Migration de FTD HA (basculement) vers un autre FMC

Table des matières

Introduction

Ce document décrit la procédure de migration d'un FTD HA d'un FMC existant vers un autre FMC.

Pour une migration de pare-feu autonome vers un nouveau FMC, consultez la page https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/222480-migrate-an-ftd-from-one-fmc-to-another-f.html

Abréviations

ACP = Politique de contrôle d'accès

ARP = protocole de résolution d'adresse

CLI = interface de ligne de commande

FMC = Secure Firewall Management Center

FTD = Protection pare-feu sécurisée contre les menaces

GARP = ARP gratuit

HA = Haute disponibilité

MW = Fenêtre de maintenance

Interface utilisateur = Interface utilisateur

Conditions préalables

Avant de commencer le processus de migration, assurez-vous que les conditions suivantes sont réunies :

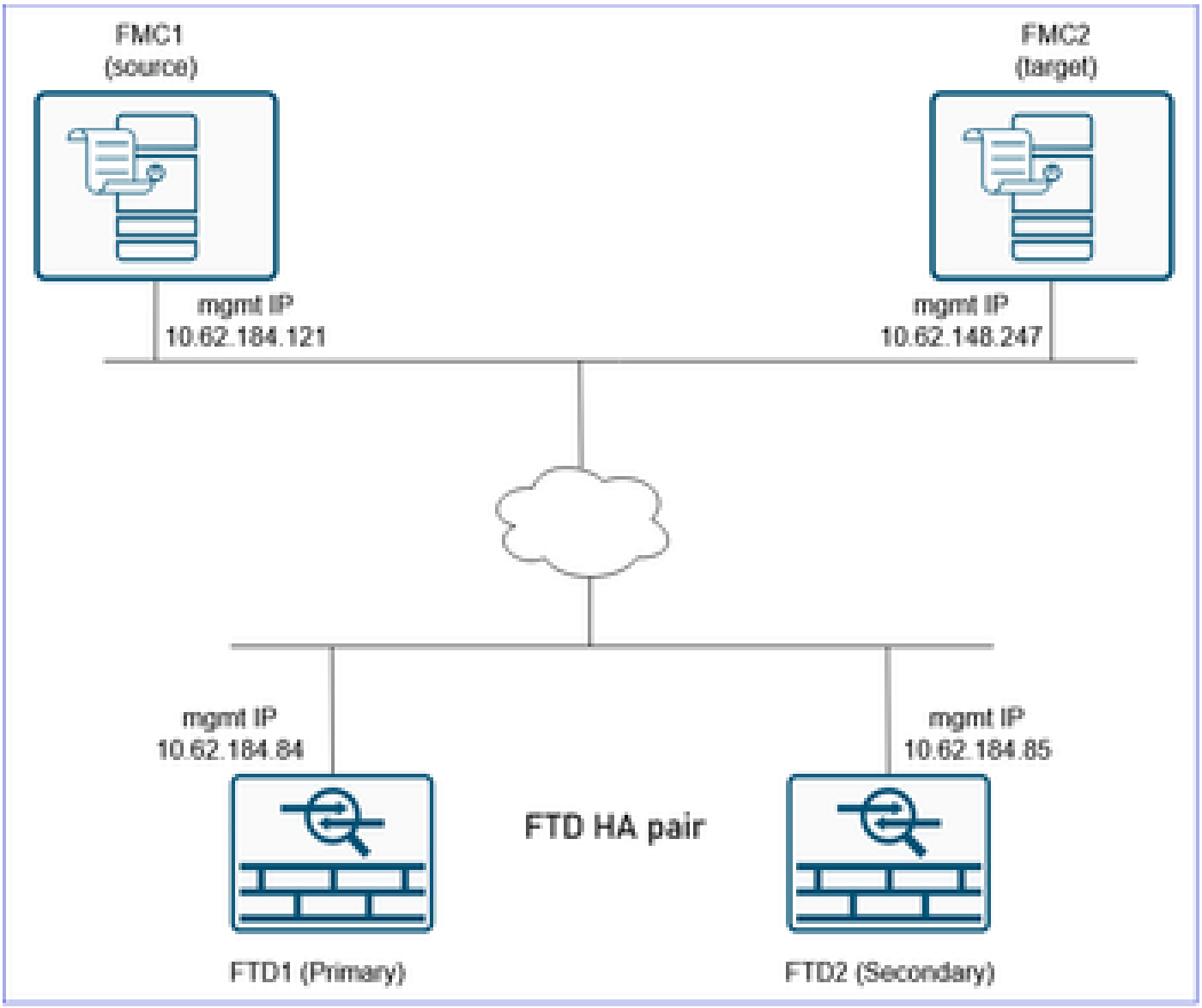
- L'interface utilisateur et l'interface de ligne de commande accèdent aux FMC source et de destination.
- Informations d'identification administratives pour les FMC et les pare-feu.
- Accès console aux deux pare-feu.
- Accès aux périphériques amont et aval de couche 3 (au cas où vous auriez besoin d'effacer le cache ARP).
- Assurez-vous que le FMC de destination/cible a la même version que le FMC source/ancien.
- Assurez-vous que le FMC cible/de destination possède les mêmes licences que le FMC source/ancien.
- Veillez à organiser un MW pour effectuer la migration, car elle aura un impact sur le trafic de transit.

Composants utilisés

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

- Cisco Secure Firewall 31xx, FTD version 7.4.2.2.
- Secure Firewall Management Center version 7.4.2.2.
- 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.

Topologie



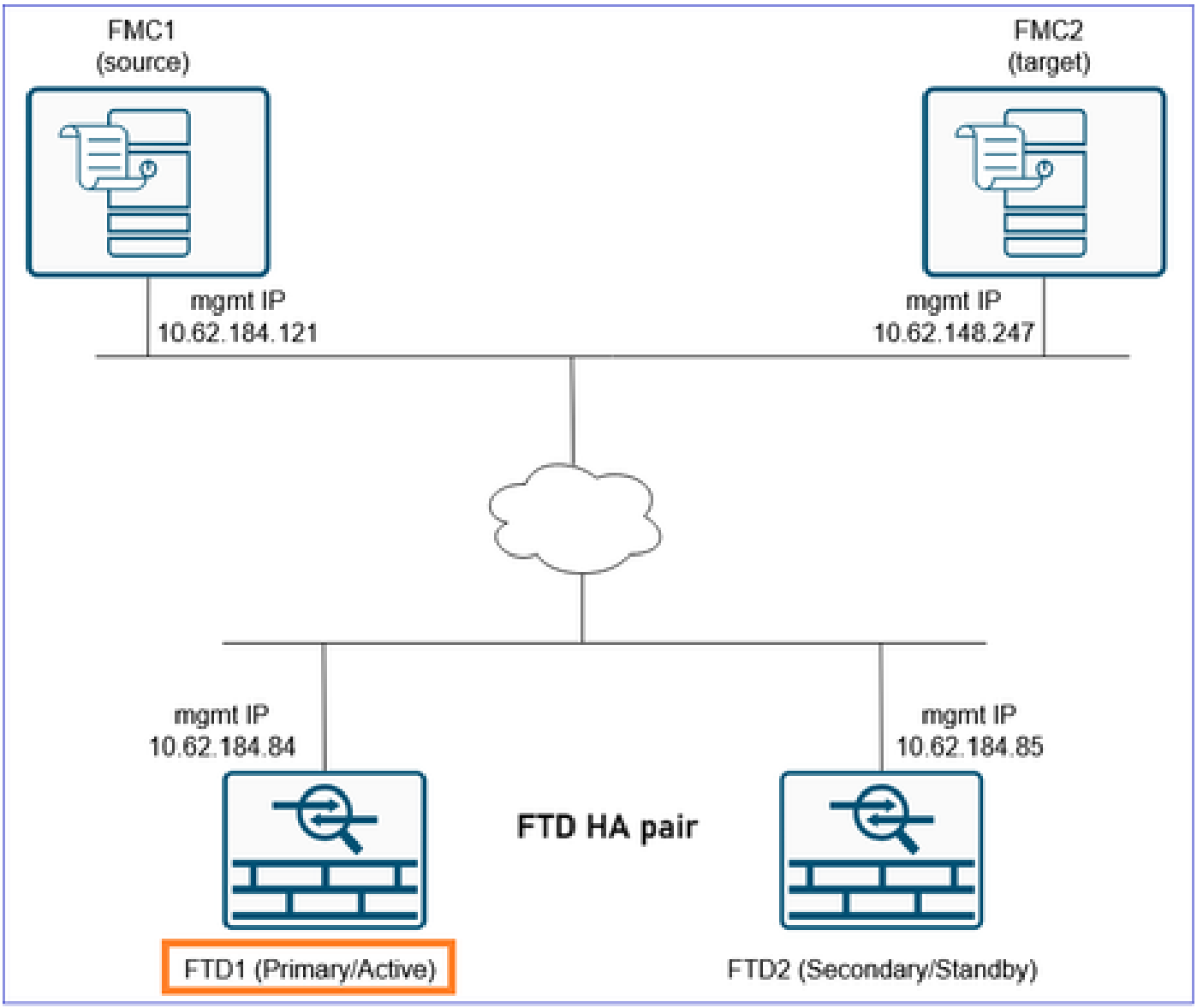
Configurer

Étapes de migration

Pour ce scénario, nous considérons les états suivants :

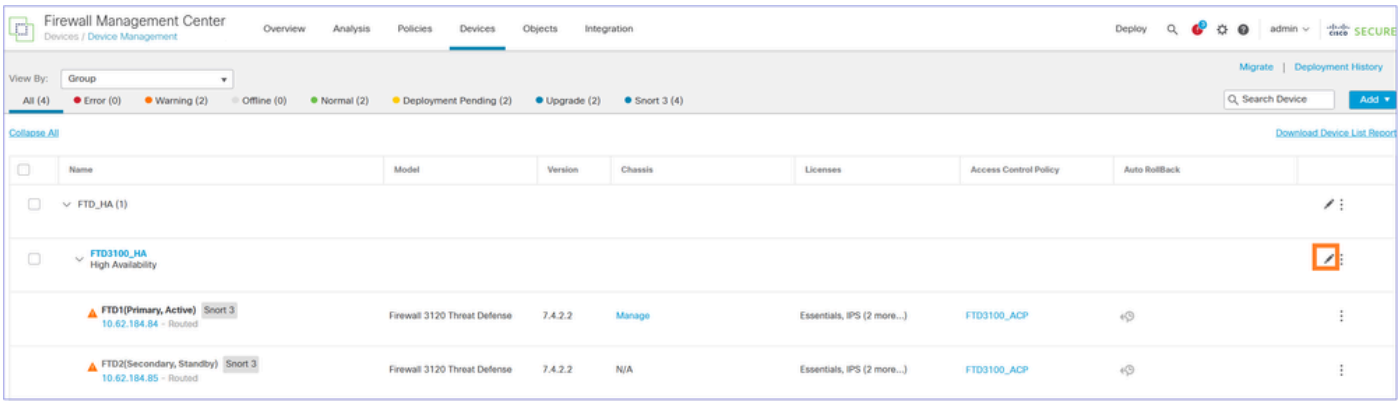
FTD1 : Principal/actif

FTD2 : Secondaire/En veille



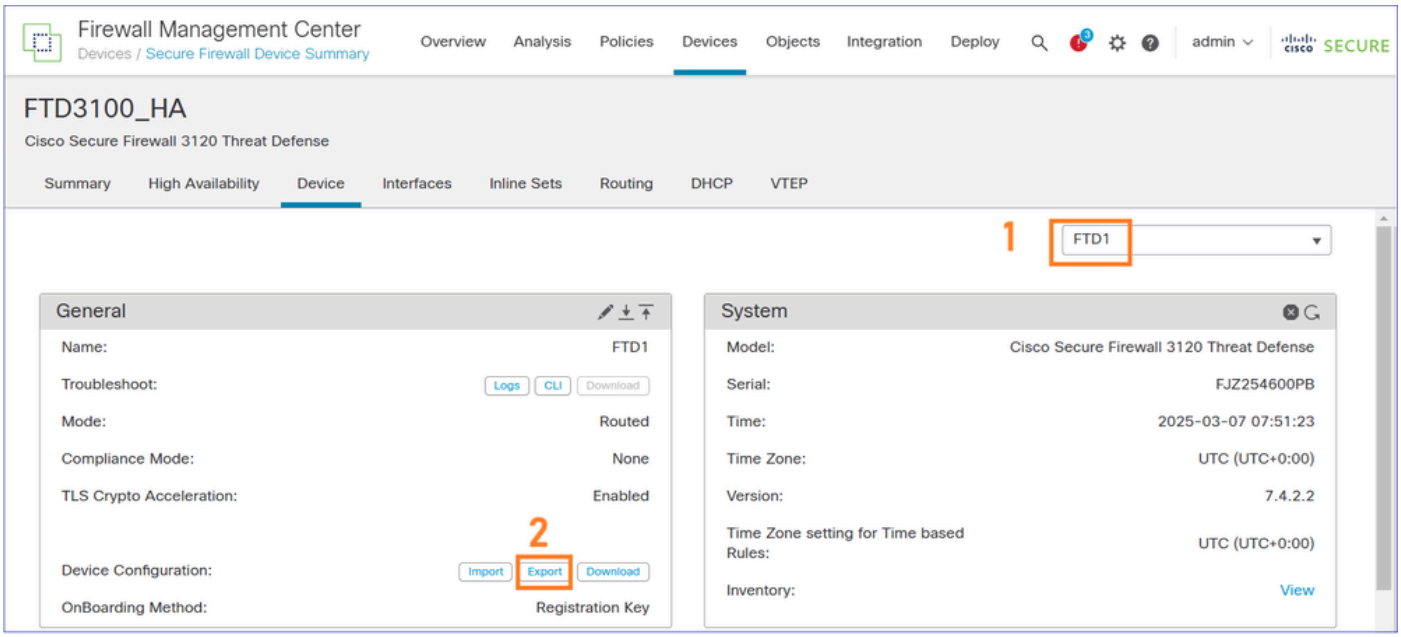
Étape 1 : exportation de la configuration du périphérique à partir du pare-feu principal

Sur le FMC1 (FMC source), accédez à Périphériques > Gestion des périphériques. Sélectionnez la paire FTD HA et sélectionnez Edit :



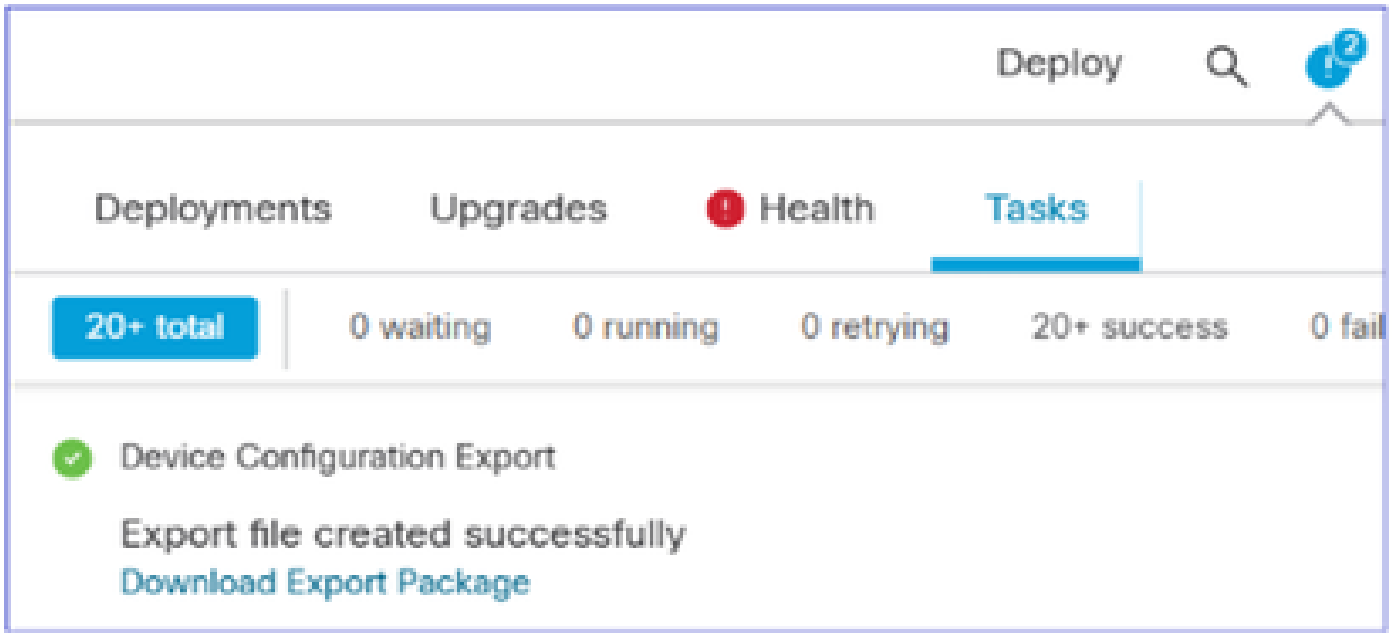
Accédez à l'onglet Device. Assurez-vous que le FTD principal/actif (FTD1 dans ce cas) est

sélectionné et sélectionnez Export pour exporter la configuration du périphérique :



Remarque : L'option Exporter est disponible à partir de la version 7.1 du logiciel et des versions ultérieures.

Vous pouvez accéder à la page Notifications > Tâches pour vous assurer que l'exportation est terminée. Ensuite, sélectionnez Download Export Package:



Vous pouvez également cliquer sur le bouton Download (Télécharger) dans la zone General (Général). Vous obtenez un fichier sfo, par exemple DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

Le fichier contient une configuration relative au périphérique, telle que :

- Interfaces routées

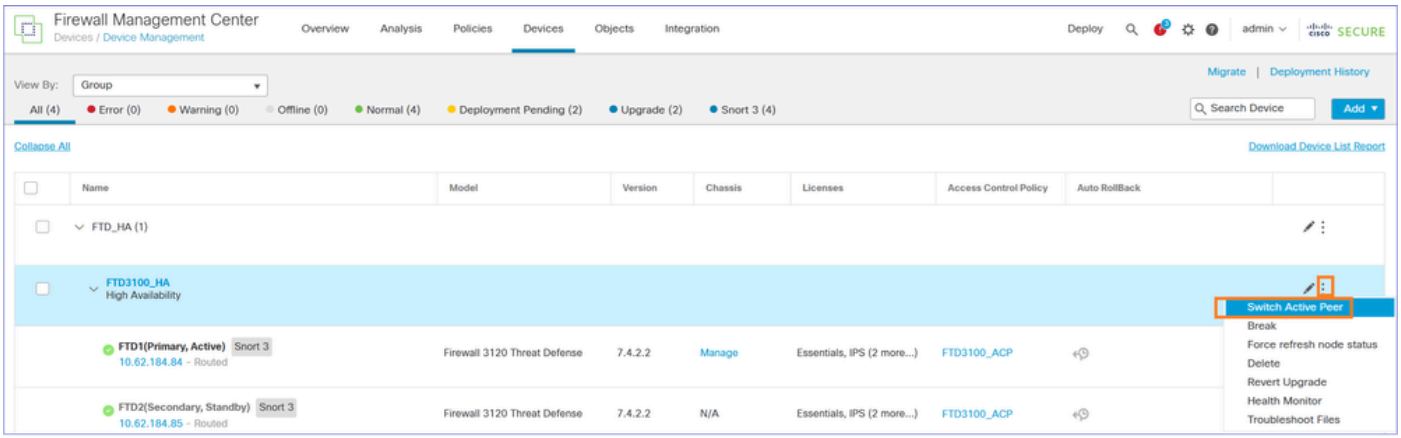
- Jeux en ligne
- Routage
- DHCP
- VTEP
- Objets associés

Remarque : Le fichier de configuration exporté ne peut être réimporté que vers le même FTD. L'UUID du FTD doit correspondre au contenu du fichier SFO importé. Le même FTD peut être enregistré sur un autre FMC et le fichier sfo peut être importé.

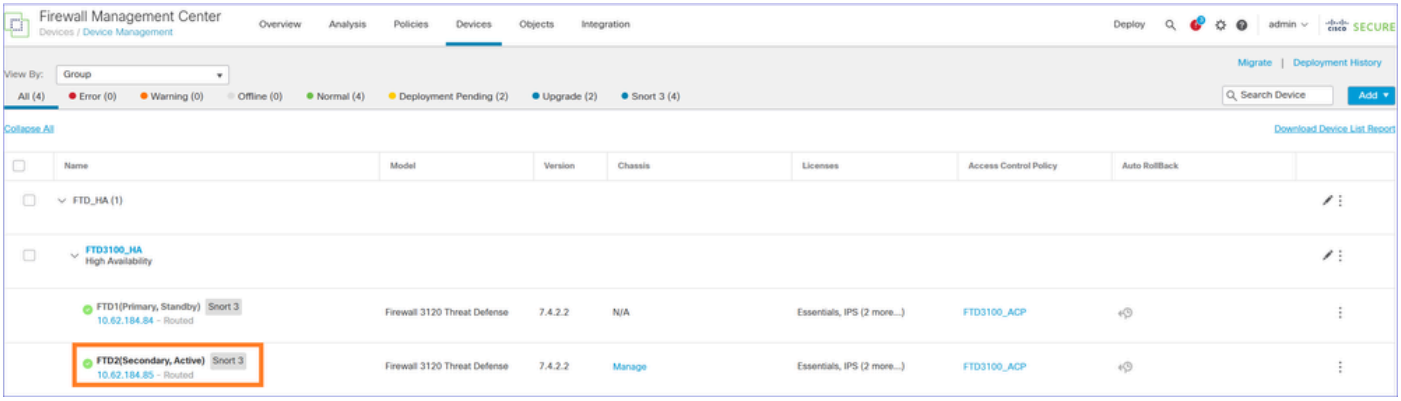
Référence: 'Export and Import the Device Configuration' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

Étape 2 : activation du FTD secondaire

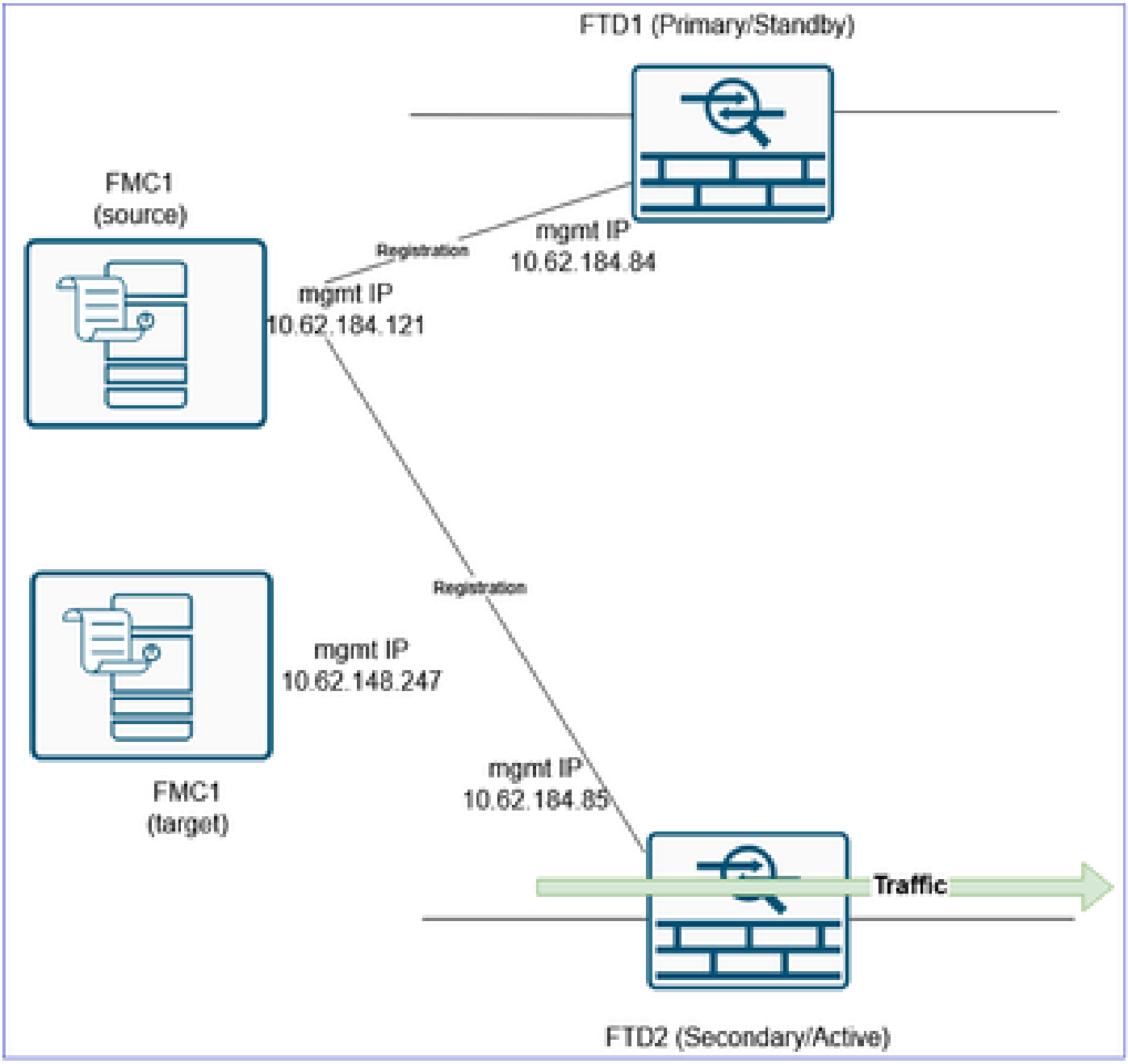
Accédez à Devices > Device Management, sélectionnez la paire FTD HA et sélectionnez Switch Active Pair:



Le résultat est FTD1 (principal/veille) et FTD (secondaire/actif) :

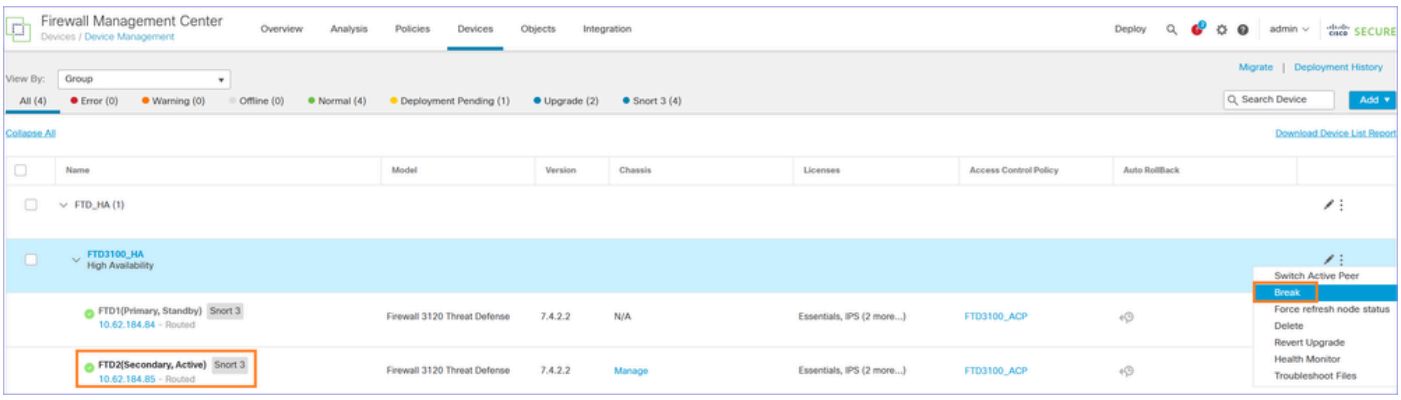


Maintenant, le trafic est géré par le FTD secondaire/actif :

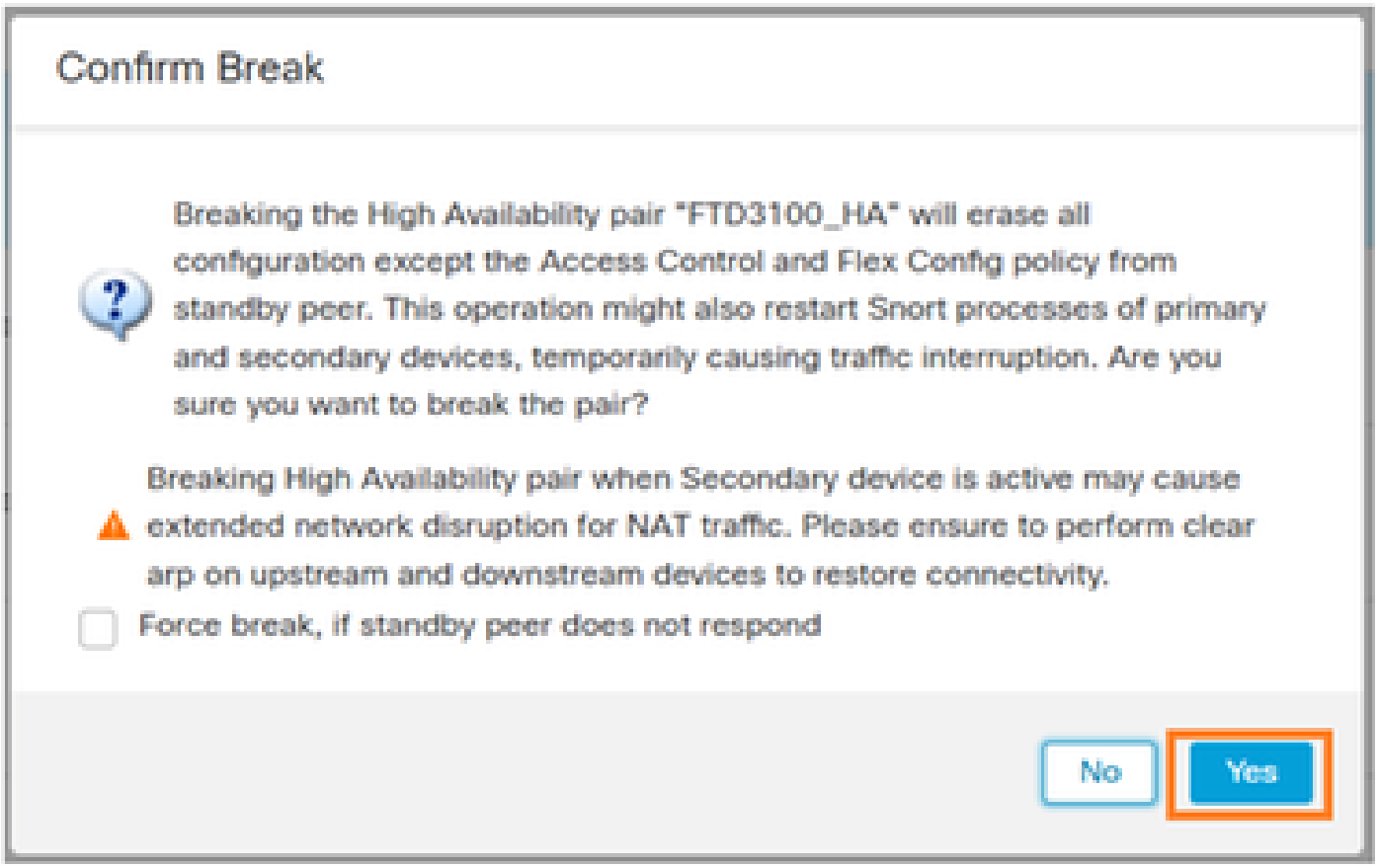


Étape 3. Interrompre la haute disponibilité du FTD

Accédez à Devices > Device Management et Break the FTD HA:



Cette fenêtre apparaît . Sélectionnez oui



Remarque : À ce stade, vous pouvez rencontrer une interruption du trafic pendant quelques secondes, puisque le moteur Snort redémarre pendant la pause HA. En outre, comme le message le mentionne, si vous utilisez la fonction NAT et que vous subissez une interruption prolongée du trafic, pensez à effacer le cache ARP sur les périphériques en amont et en aval.

Après la rupture de la haute disponibilité du FTD, vous disposez de deux FTD autonomes sur FMC.

Du point de vue de la configuration, le FTD2 (ex-Active) a toujours la configuration en place à l'exception de la configuration liée au basculement et gère le trafic :

<#root>

```
FTD3100-4#
show failover


Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
```

```
Monitored Interfaces 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

<#root>

FTD3100-4#

show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Port-channel1              unassigned      YES           unset  up          up
Port-channel1.200          10.0.200.70     YES           manual up          up
Port-channel1.201          10.0.201.70     YES           manual up          up
```

La configuration du FTD1 (hors veille) a été supprimée :

<#root>

FTD3100-3#

show failover

```
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

<#root>

FTD3100-3#

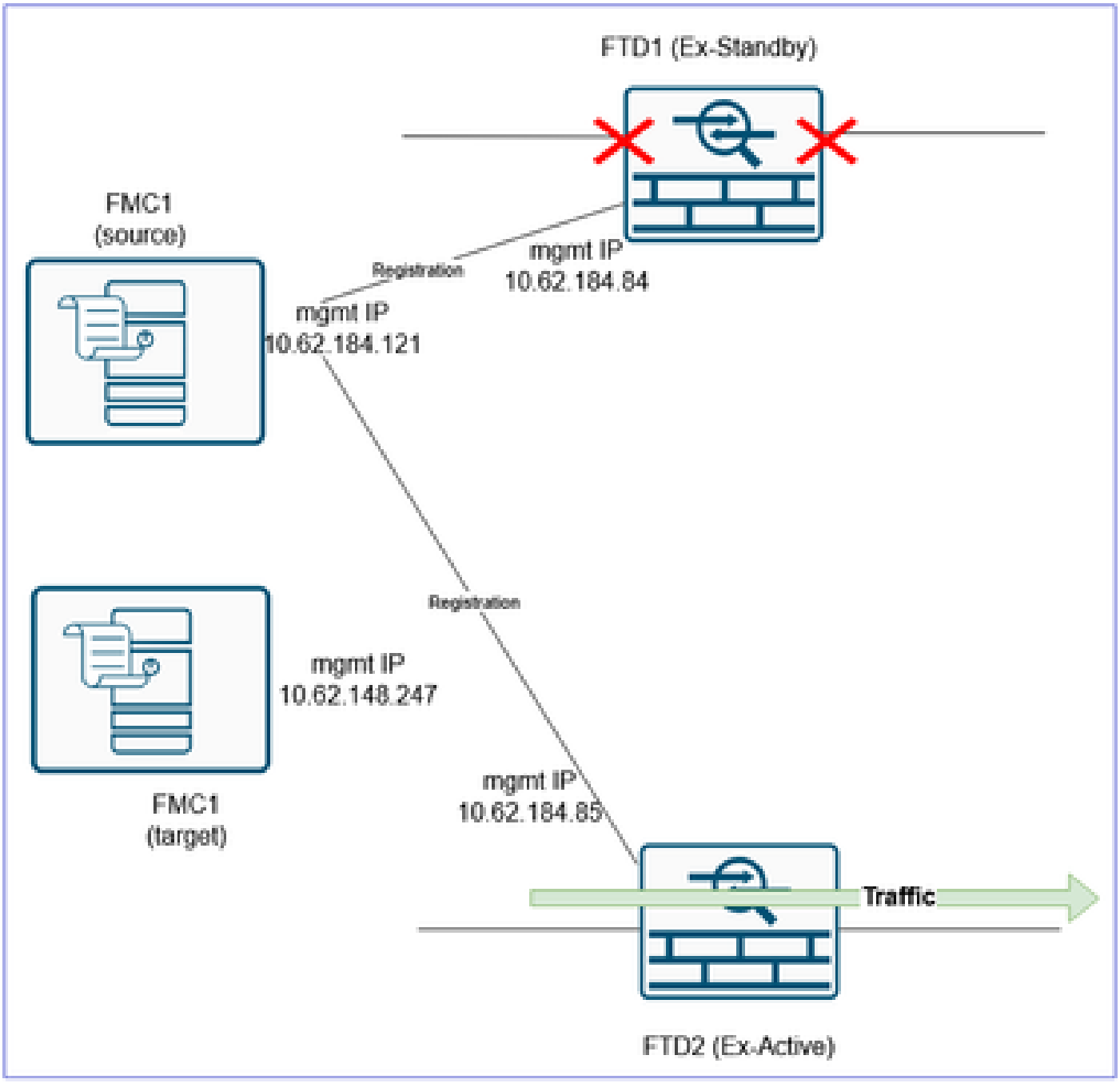
show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Ethernet1/1                unassigned      YES           unset  admin down  down
Ethernet1/2                unassigned      YES           unset  admin down  down
Ethernet1/3                unassigned      YES           unset  admin down  down
Ethernet1/4                unassigned      YES           unset  admin down  down
Ethernet1/5                unassigned      YES           unset  admin down  down
Ethernet1/6                unassigned      YES           unset  admin down  down
Ethernet1/7                unassigned      YES           unset  admin down  down
Ethernet1/8                unassigned      YES           unset  admin down  down
Ethernet1/9                unassigned      YES           unset  admin down  down
Ethernet1/10               unassigned      YES           unset  admin down  down
```

```
Ethernet1/11                unassigned      YES           unset  admin down  down
Ethernet1/12                unassigned      YES           unset  admin down  down
Ethernet1/13                unassigned      YES           unset  admin down  down
Ethernet1/14                unassigned      YES           unset  admin down  down
Ethernet1/15                unassigned      YES           unset  admin down  down
Ethernet1/16                unassigned      YES           unset  admin down  down
```

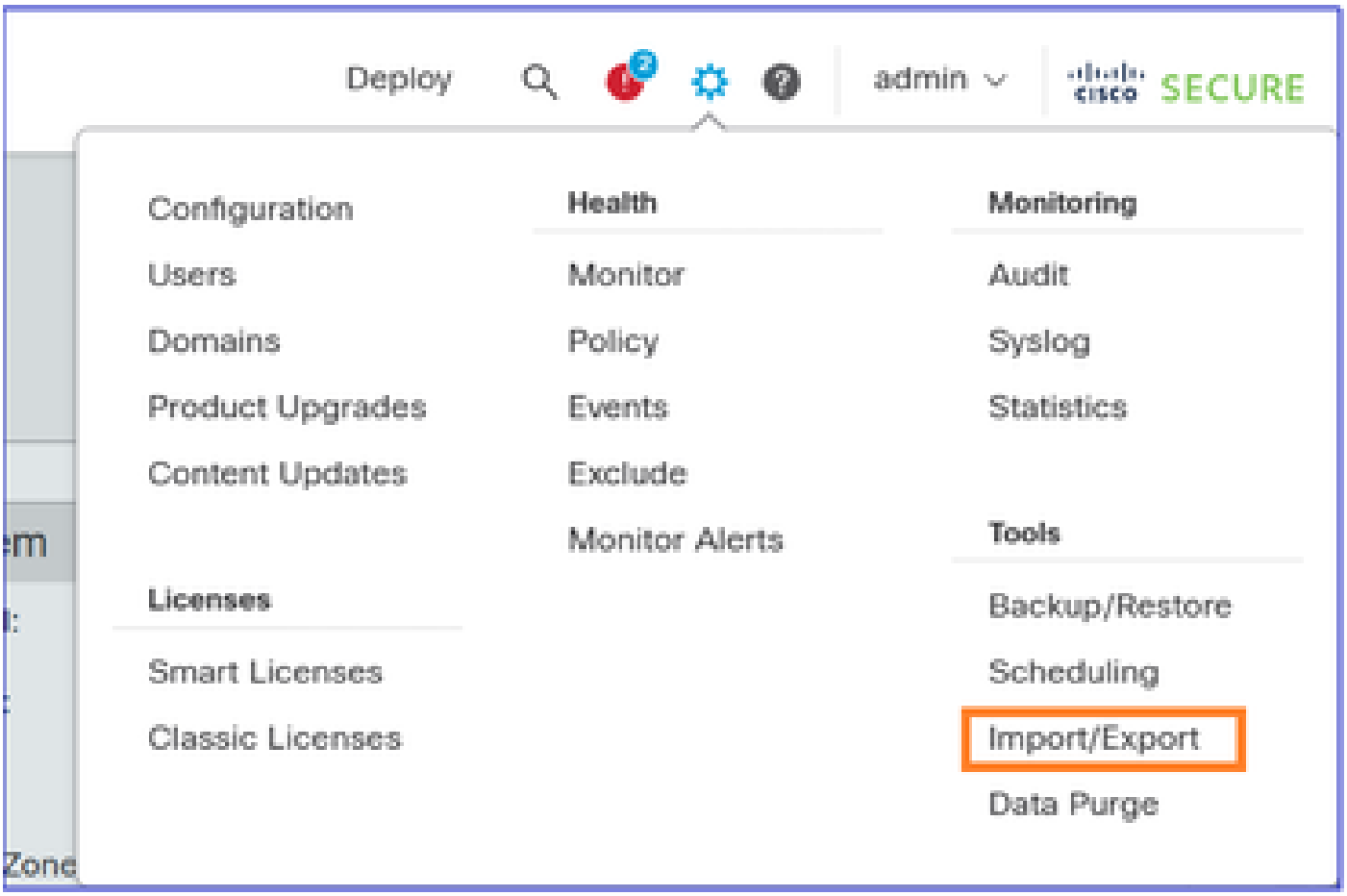
Étape 4. Isolation des interfaces de données FTD1 (ex-Primary)

Déconnectez les câbles de données du FTD1 (ex-primaire). Laissez uniquement le port de gestion FTD connecté.



Étape 5. Exportation des stratégies partagées FTD

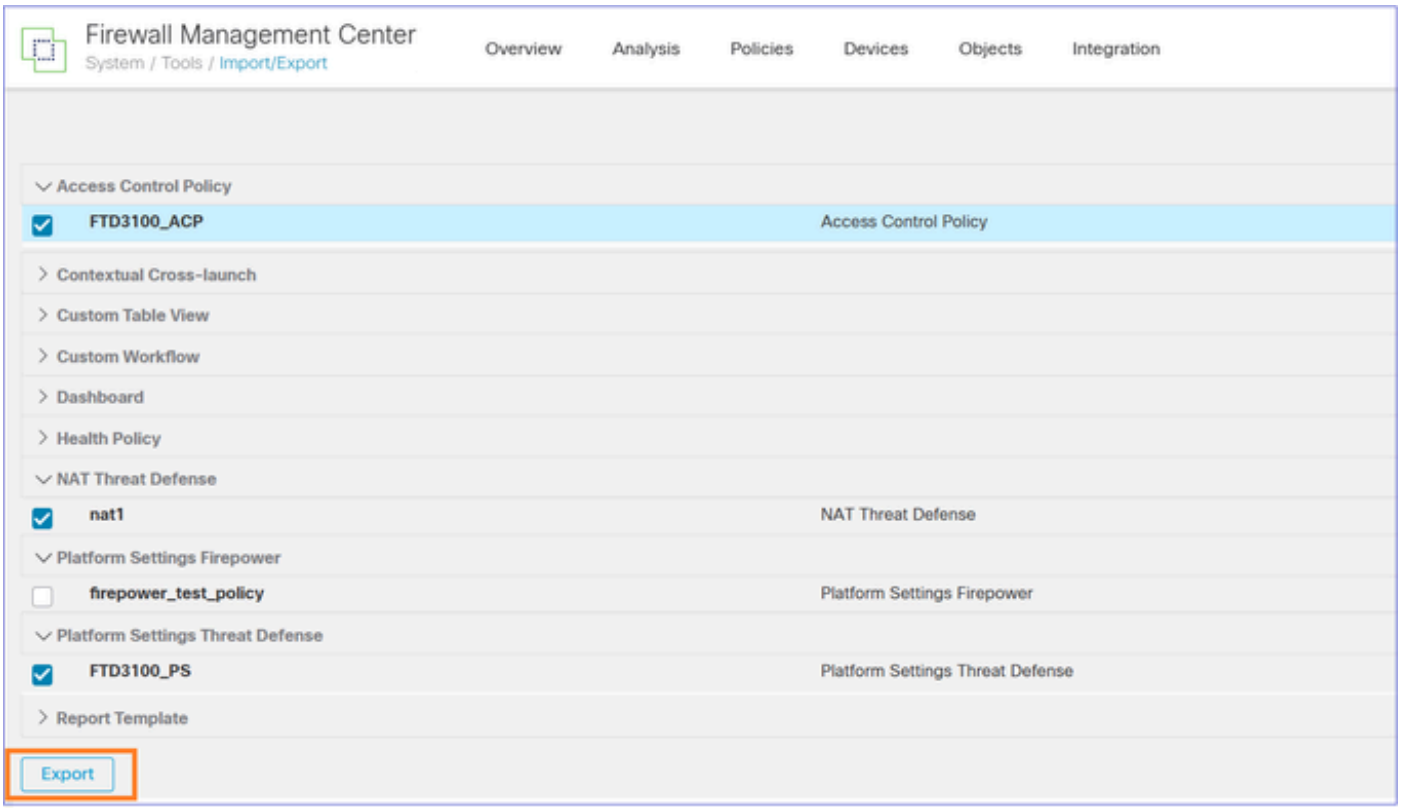
Accédez à System > Tools et sélectionnez Import/Export :



Exportez les différentes stratégies associées au périphérique. Assurez-vous d'exporter toutes les stratégies associées au FTD, telles que :

- Politique de contrôle d'accès (ACP)
- Politique NAT (Network Address Translation)
- Politique d'intégrité (si personnalisée)
- Paramètres de plateforme FTD

etc.



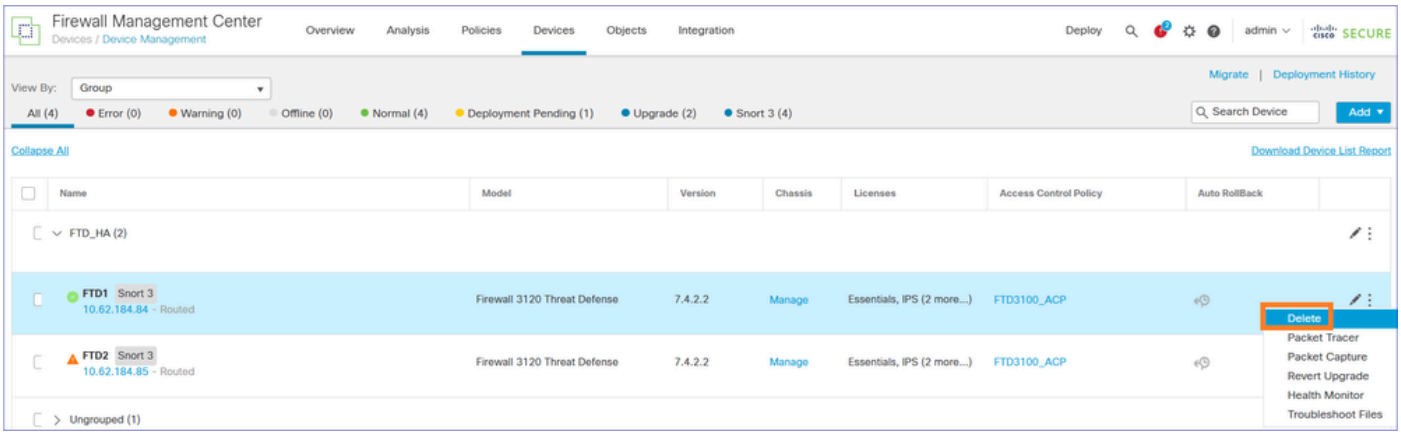
Remarque : Au moment de la rédaction de ce document, l'exportation de la configuration liée au VPN n'est pas prise en charge. Vous devez reconfigurer manuellement le VPN sur le FMC2 (FMC cible) après l'enregistrement du périphérique.

Amélioration connexe ID de bogue Cisco CSCwf05294

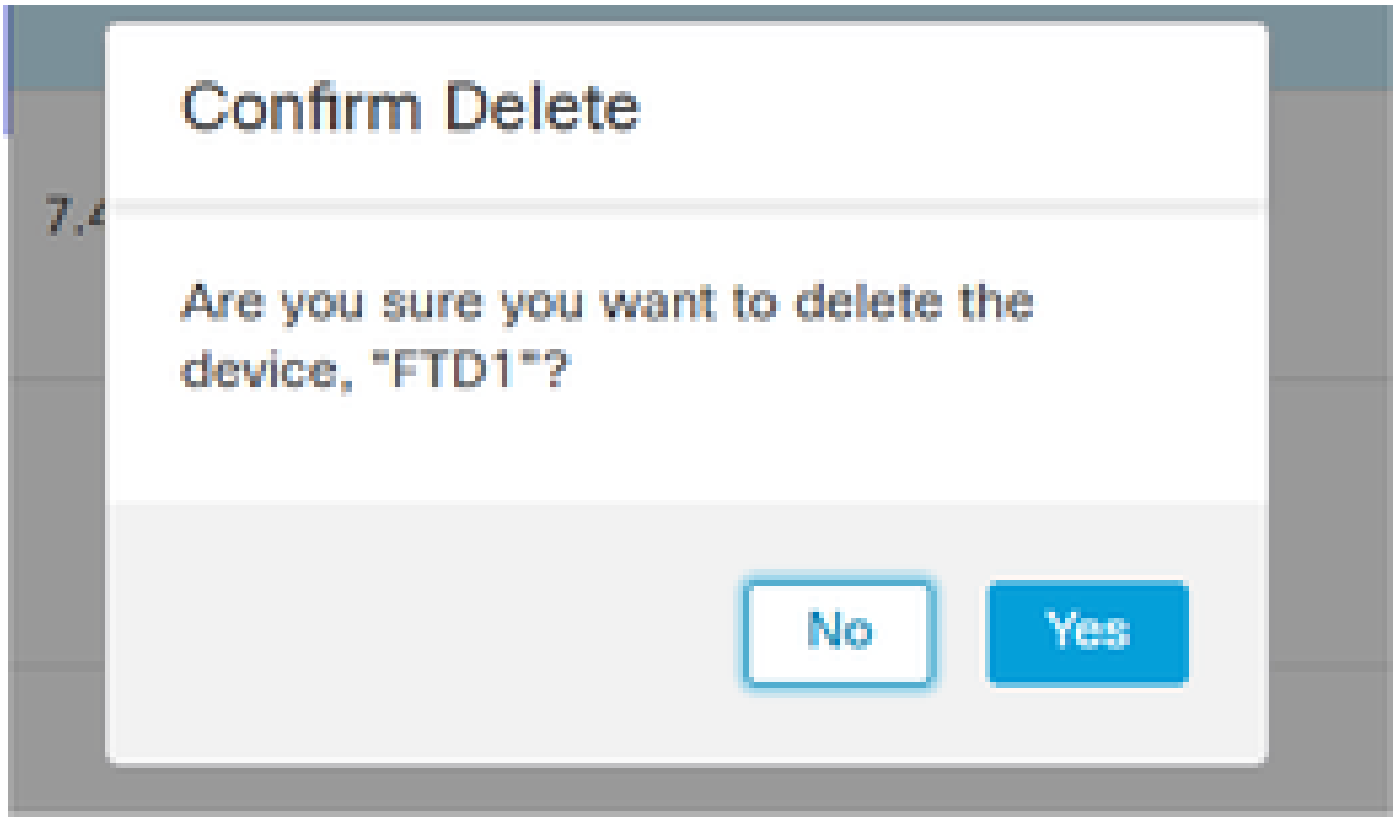
.

Le résultat est un fichier .sfo, par exemple ObjectExport_20250306082738.sfo

Étape 6. Suppression/annulation de l’enregistrement du FTD1 (ex-Primary) de l’ancien FMC source



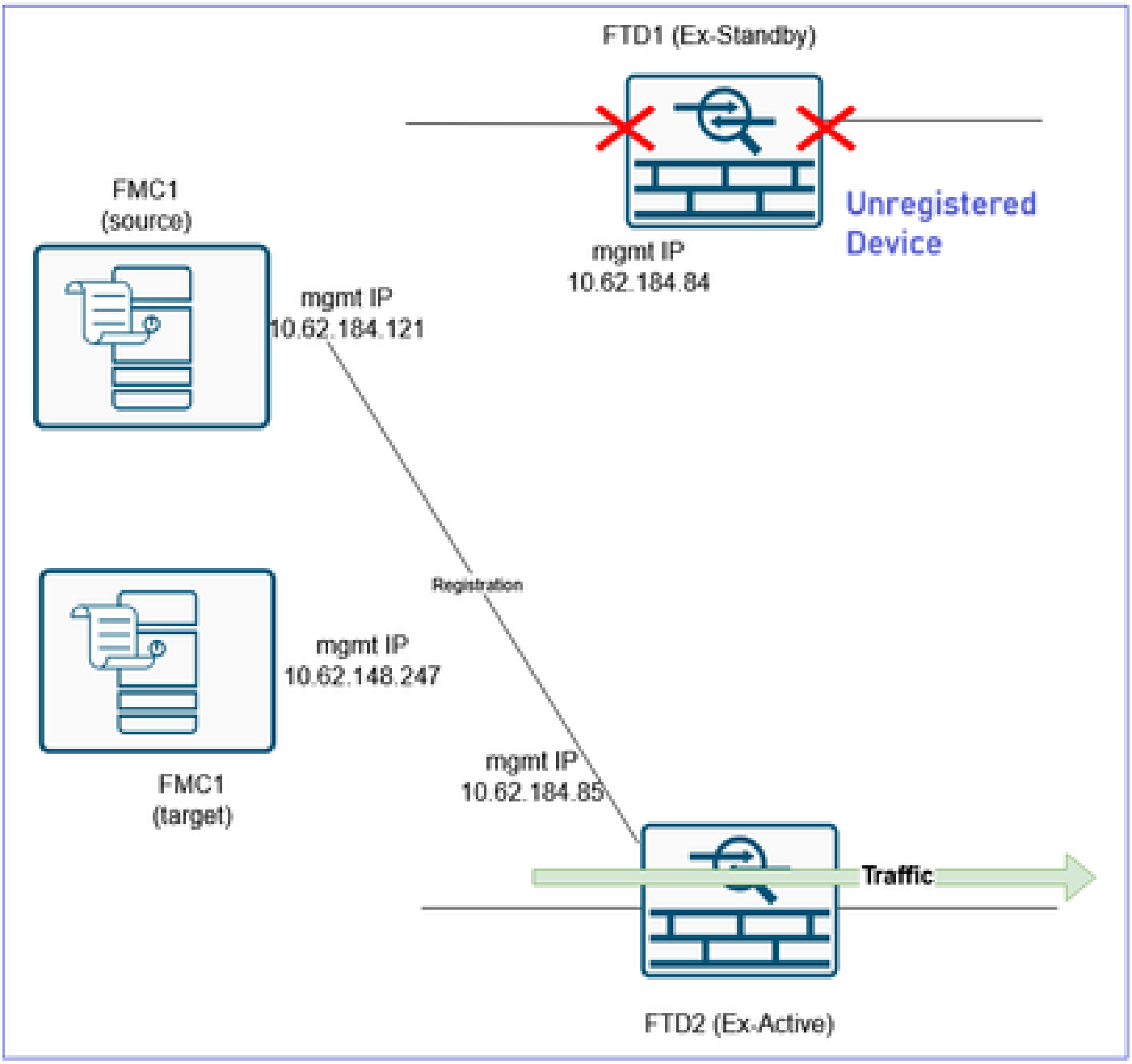
Confirmez la suppression du périphérique :



Vérification CLI FTD1 :

```
<#root>

>

show managers

No managers configured.

>
```

État actuel après la suppression du périphérique FTD1 :

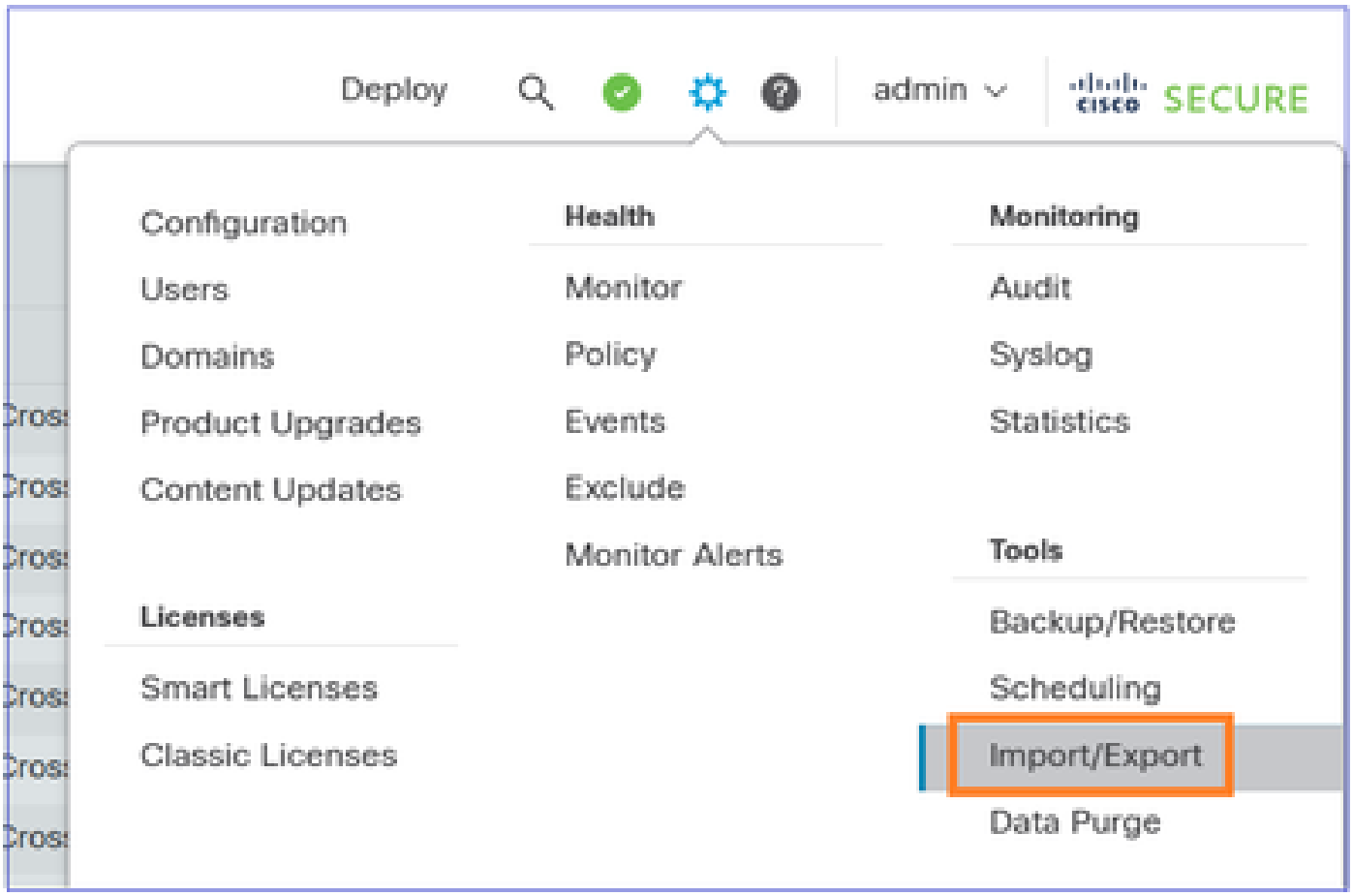


Étape 7. Importez l’objet de configuration de la stratégie FTD dans FMC2 (FMC cible)

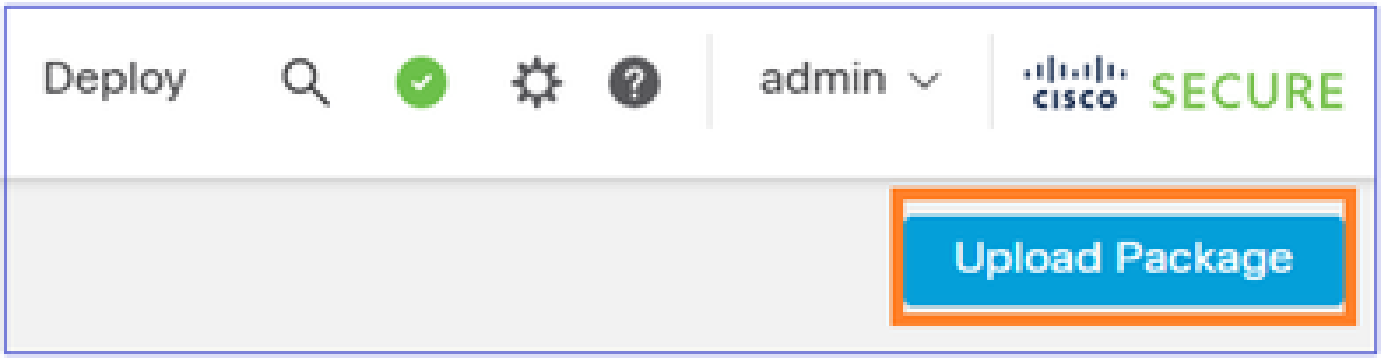
Remarque : Le document se concentre sur la migration d'une seule paire FTD HA vers un nouveau FMC. D'autre part, si vous prévoyez de migrer plusieurs pare-feu qui partagent les mêmes politiques (par exemple, ACP, NAT) et objets et que vous souhaitez effectuer cette opération par phases, vous devez tenir compte de ces points.
- Si vous avez une stratégie existante sur le FMC cible portant le même nom, vous êtes invité à :
  a. Vous souhaitez remplacer la stratégie ou
  b. Créez-en un nouveau avec un nom différent. Ceci crée des objets dupliqués avec des noms différents (suffixe _1).

- Si vous choisissez l'option 'b', à l'étape 9, assurez-vous de réaffecter les objets nouvellement créés aux stratégies migrées (zones de sécurité ACP, zones de sécurité NAT, routage, paramètres de plate-forme, etc.).

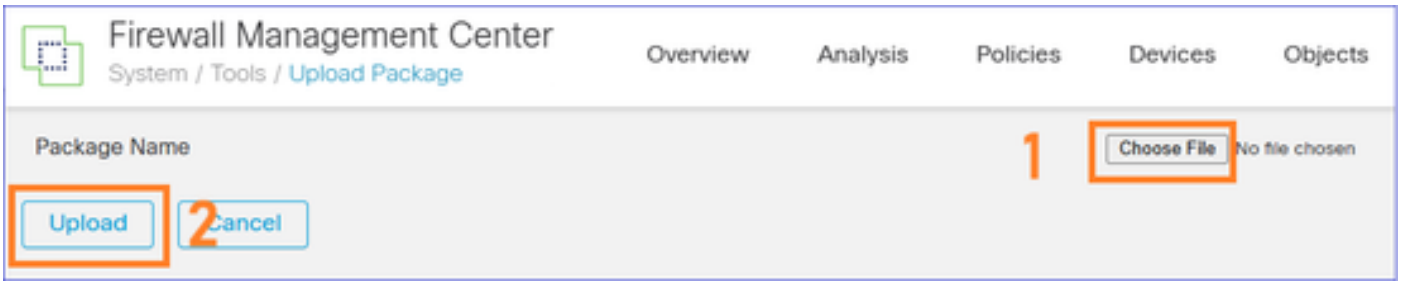
Connectez-vous au FMC2 (FMC cible) et importez l'objet de configuration FTD Policies que vous avez exporté à l'étape 5 :



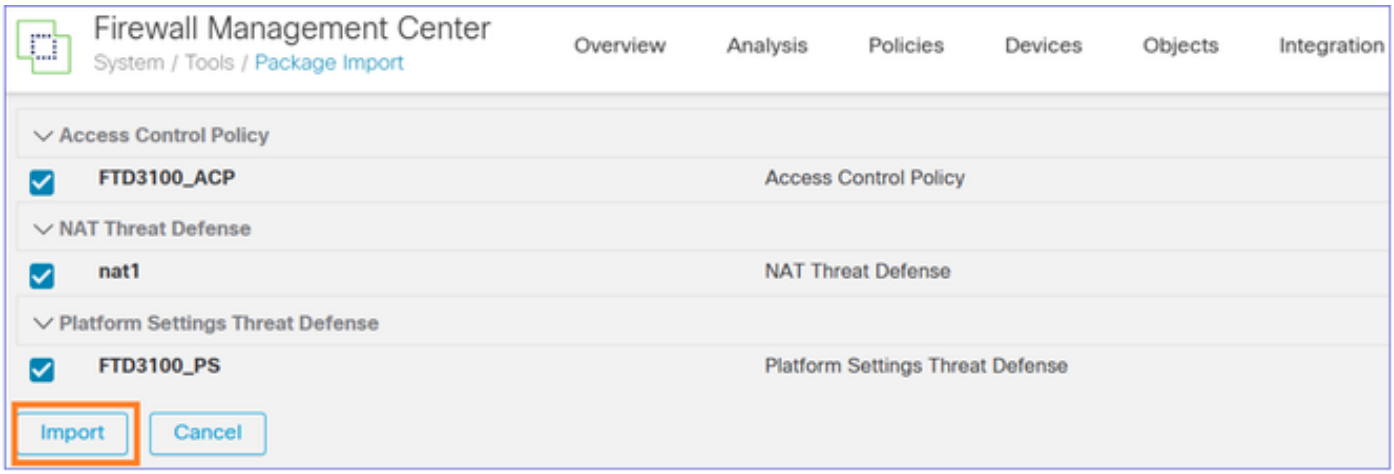
Sélectionnez Charger le paquet :



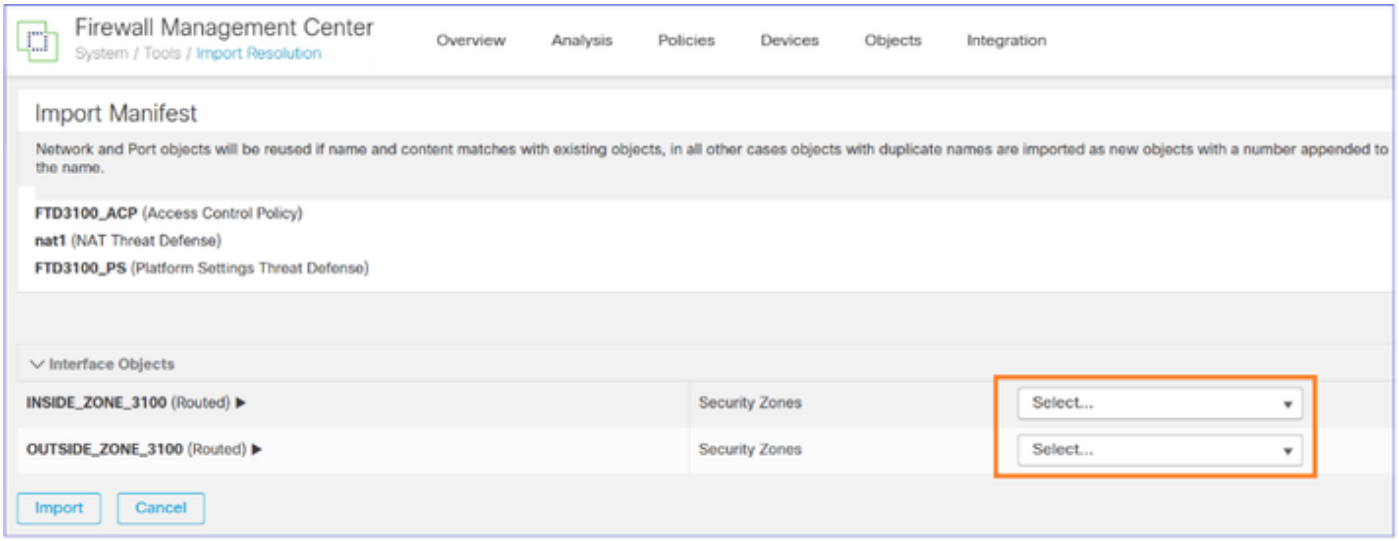
Téléchargez le fichier :



Importez les stratégies :



Créez les objets d'interface/zones de sécurité sur le FMC2 (FMC cible) :



Vous pouvez donner les mêmes noms qu'ils avaient sur le FMC1 (source FMC) :

Une fois que vous avez sélectionné Import, une tâche commence à importer les stratégies associées dans FMC2 (FMC cible) :

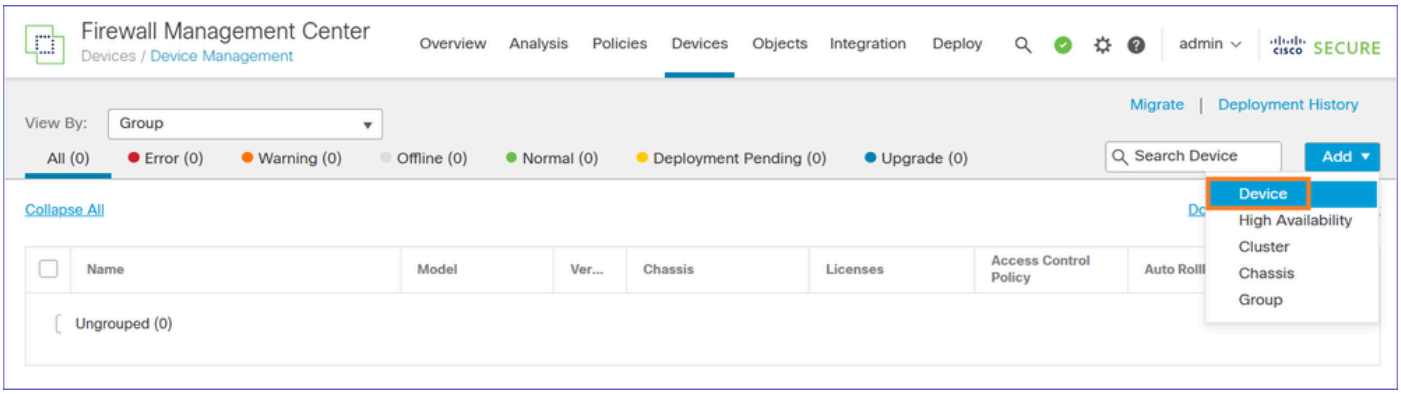
La tâche est effectuée :

Étape 8. Enregistrement du FTD1 (ex-Primary) dans le FMC2

Accédez à l'interface de ligne de commande FTD1 (ex-Primary) et configurez le nouveau gestionnaire :

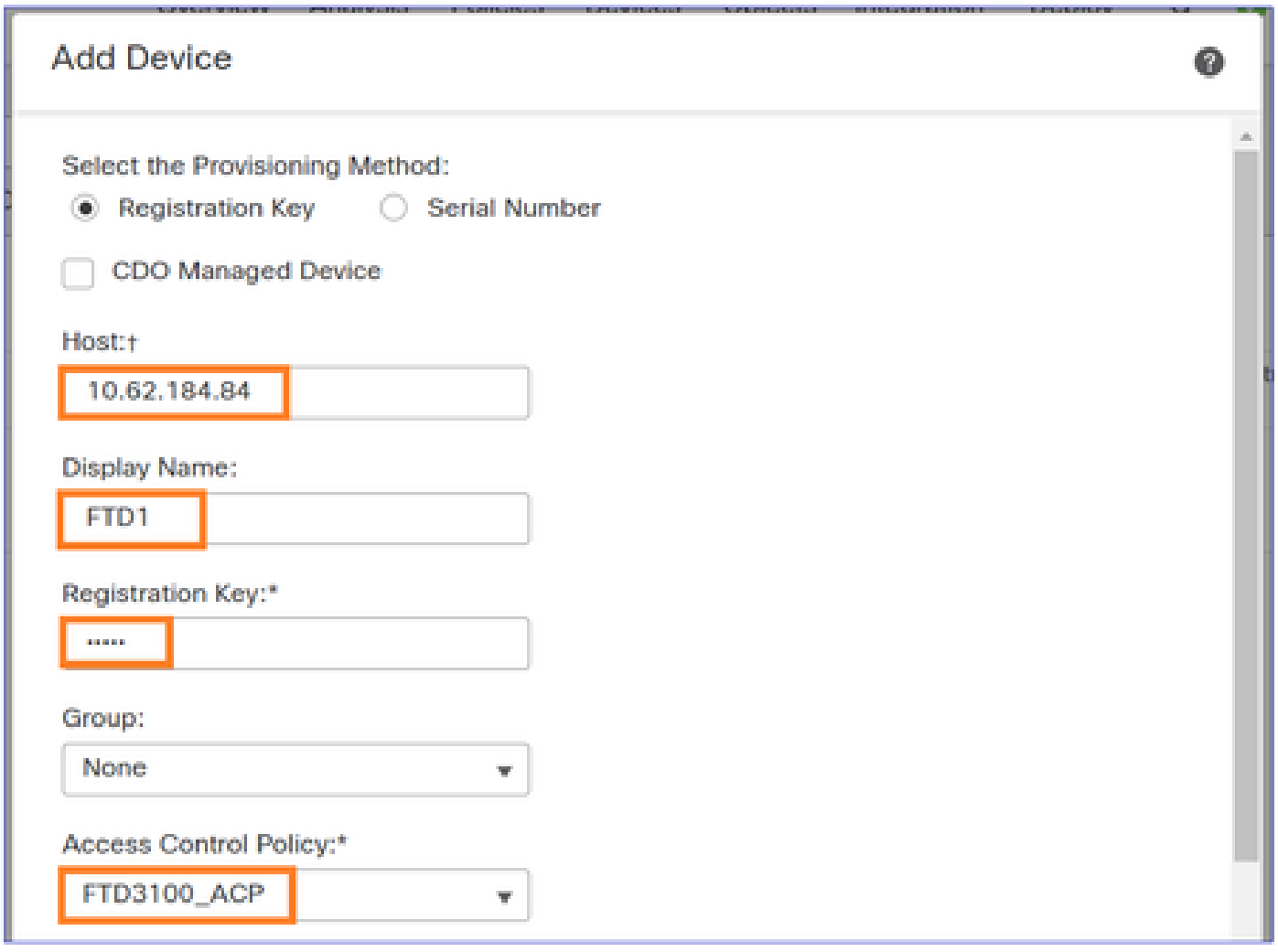
```
<#root>

>

configure manager add 10.62.148.247 cisco


Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

Accédez à l'interface utilisateur FMC2 (FMC cible) Périphériques > Gestion des périphériques et ajoutez le périphérique FTD :

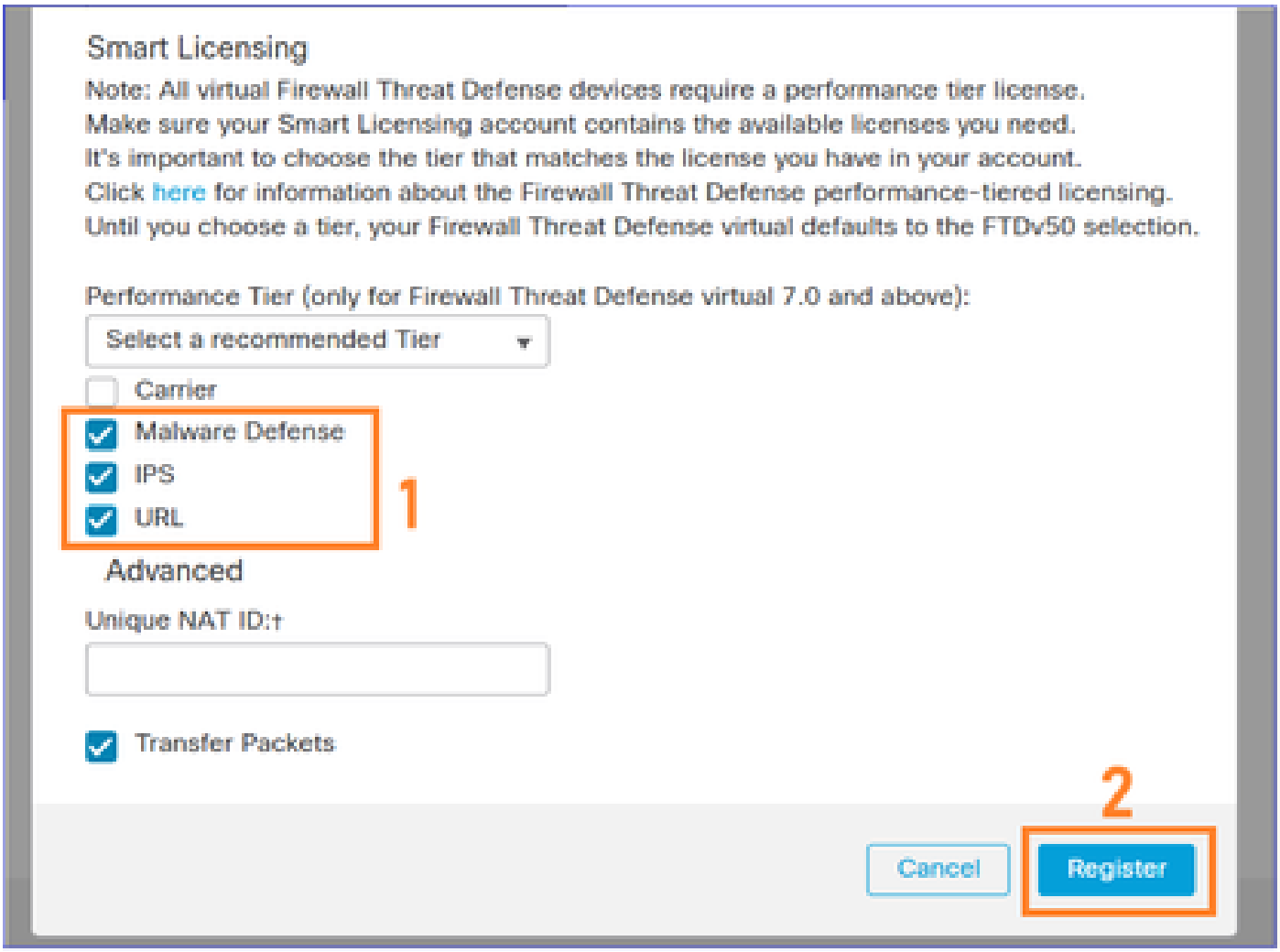


Si l'enregistrement du périphérique échoue, reportez-vous à ce document pour résoudre le problème : https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

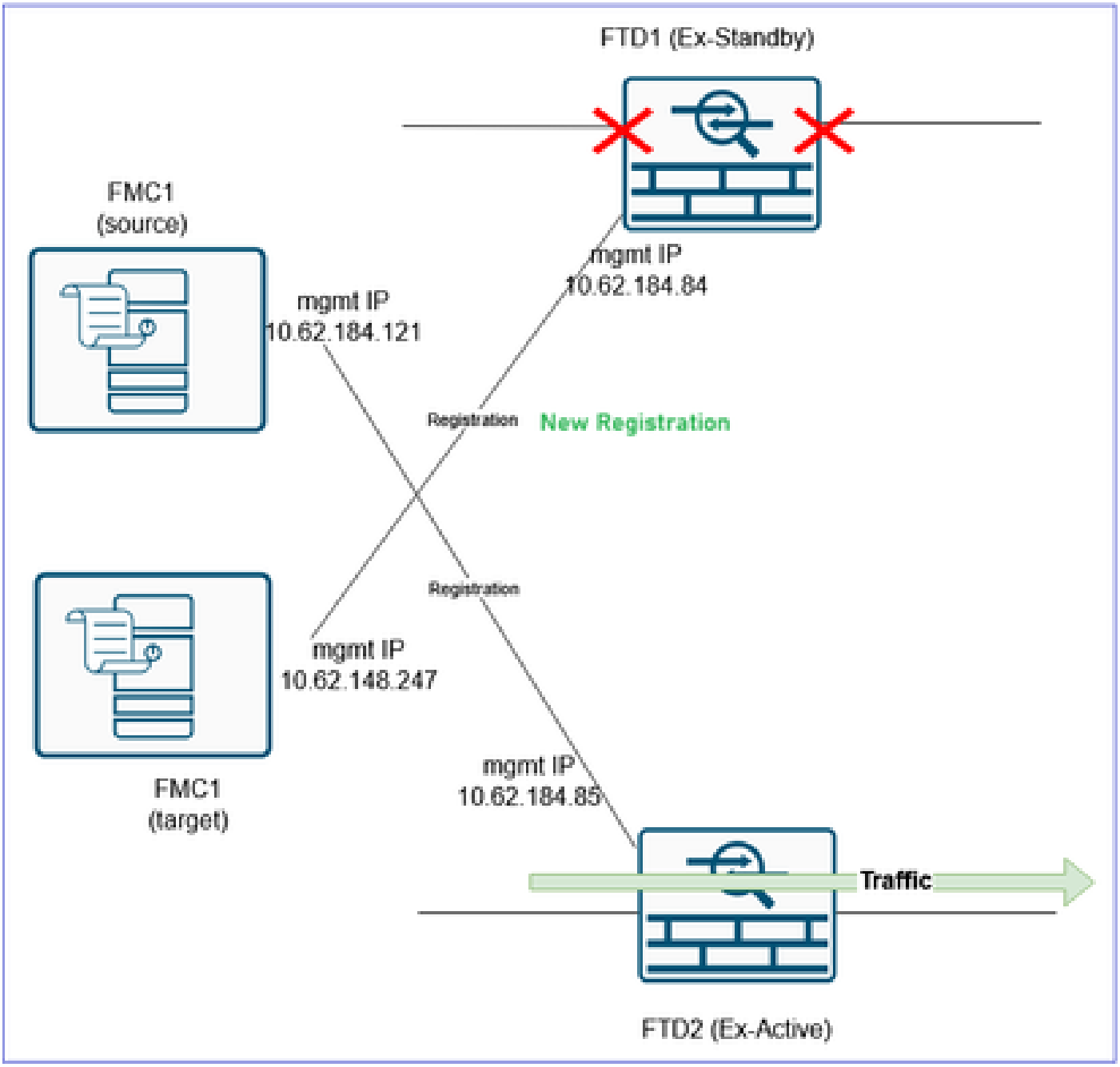
Attribuez la stratégie de contrôle d'accès que vous avez importée à l'étape précédente :



Appliquez les licences nécessaires et enregistrez le périphérique :


Smart Licensing
Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.
Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
Select a recommended Tier
Carrier
Malware Defense
IPS
URL
1
Advanced
Unique NAT ID:†
Transfer Packets
2
Cancel
Register

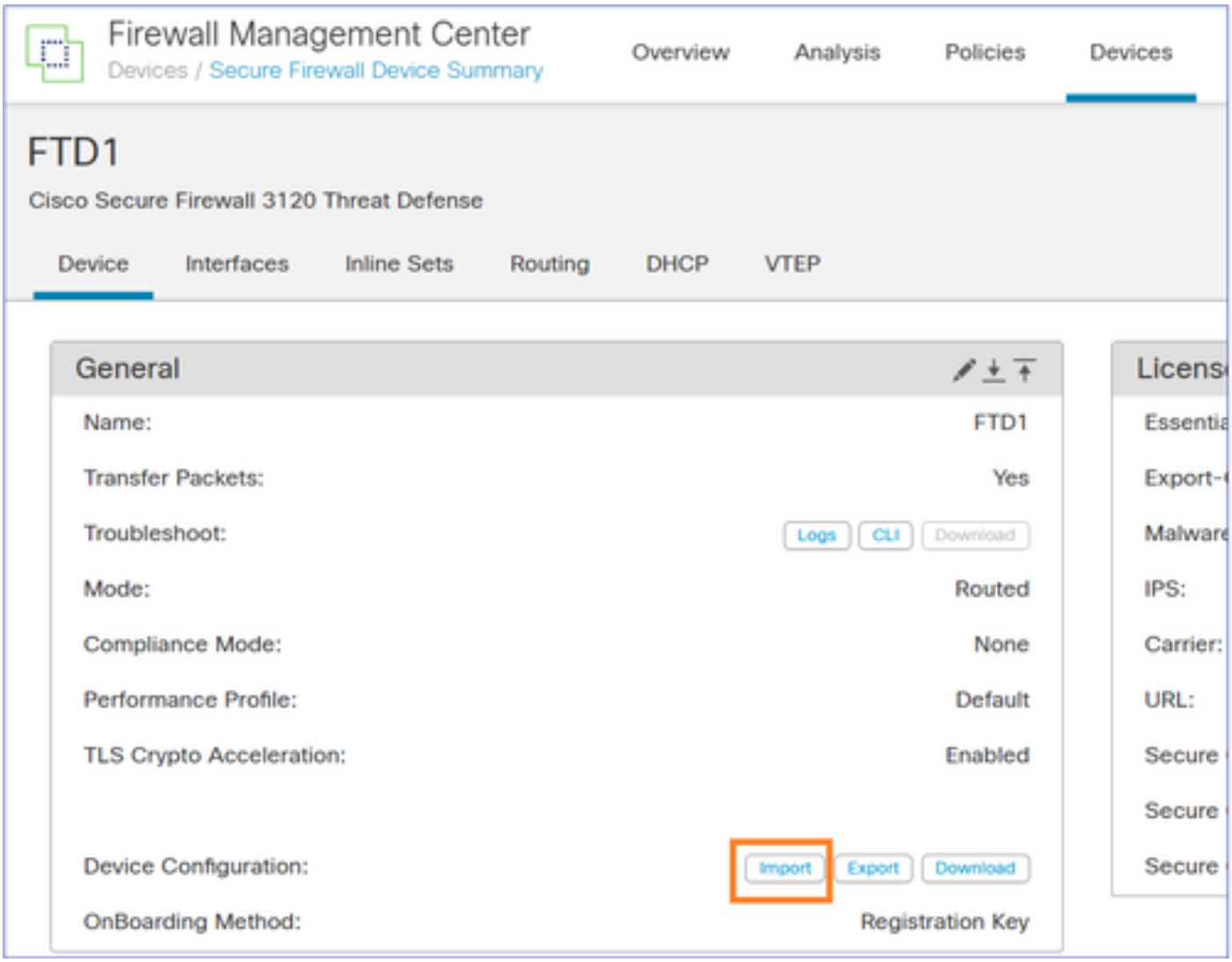
Le résultat :



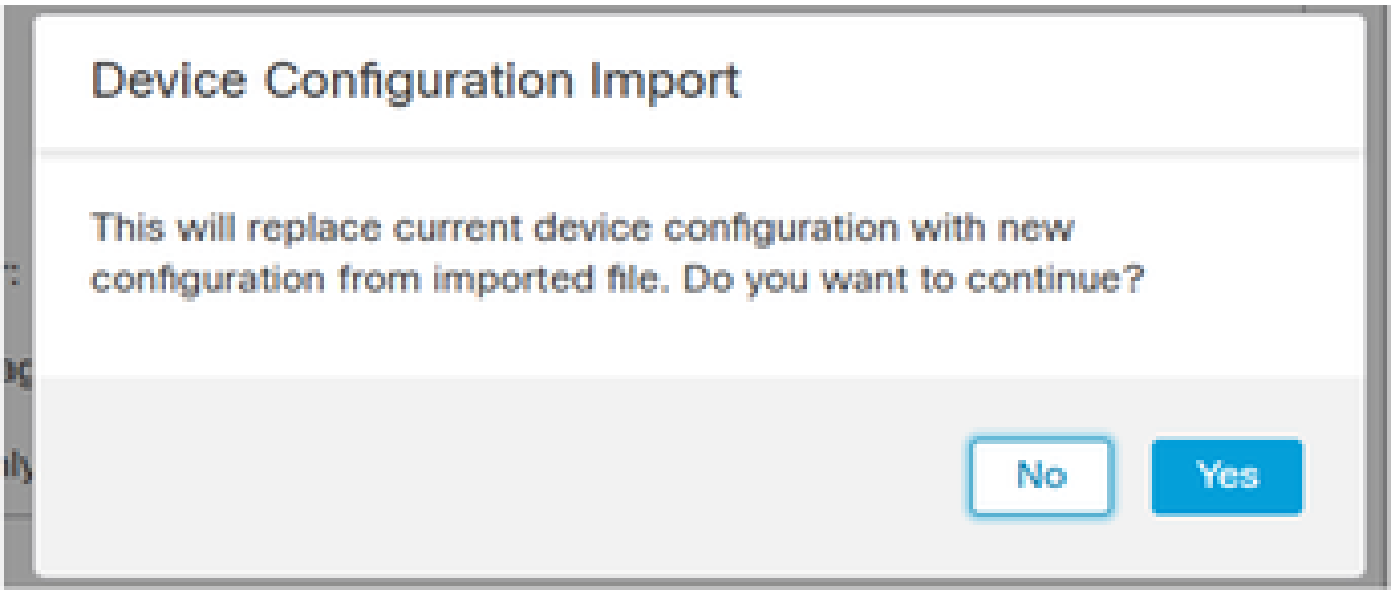
Étape 9. Importez l’objet de configuration du périphérique FTD dans FMC2 (FMC cible)

Connectez-vous au FMC2 (FMC cible), accédez à Devices > Device Management et Edit the FTD device that you registered in the previous step.

Accédez à l'onglet Device et Importez l'objet logiciel FTD Policies que vous avez exporté à l'étape 2 :

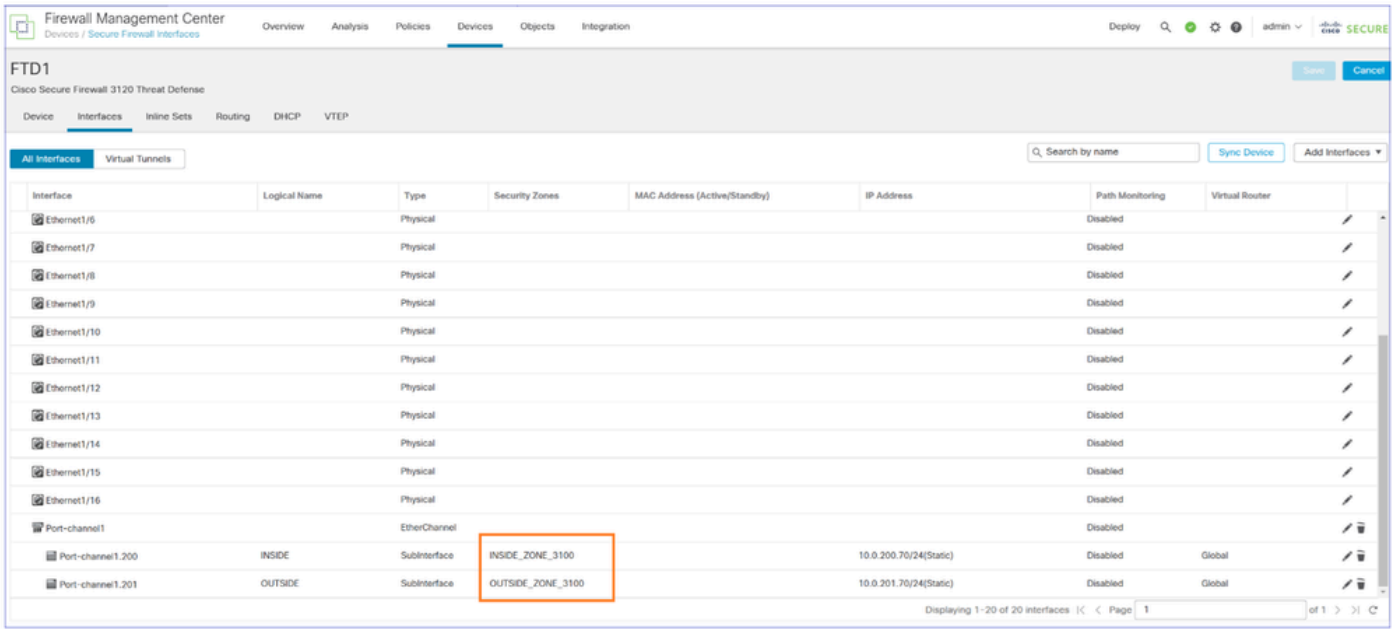


Remarque : Si, à l'étape 7, vous avez choisi l'option « b » (Créer une nouvelle stratégie), veillez à réaffecter les objets nouvellement créés aux stratégies migrées (Zones de sécurité ACP, Zones de sécurité NAT, Routage, Paramètres de plateforme, etc.).



Une tâche FMC est lancée.

La configuration du périphérique est appliquée sur le FTD1, par exemple, les zones de sécurité, ACP, NAT, etc. :



⚠ Mise en garde : Si vous avez un ACP qui s'étend à de nombreux éléments de contrôle d'accès, le processus de compilation de l'ACP (tmatch compile) peut prendre plusieurs minutes. Vous pouvez utiliser cette commande pour vérifier l'état de compilation ACP :

<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed

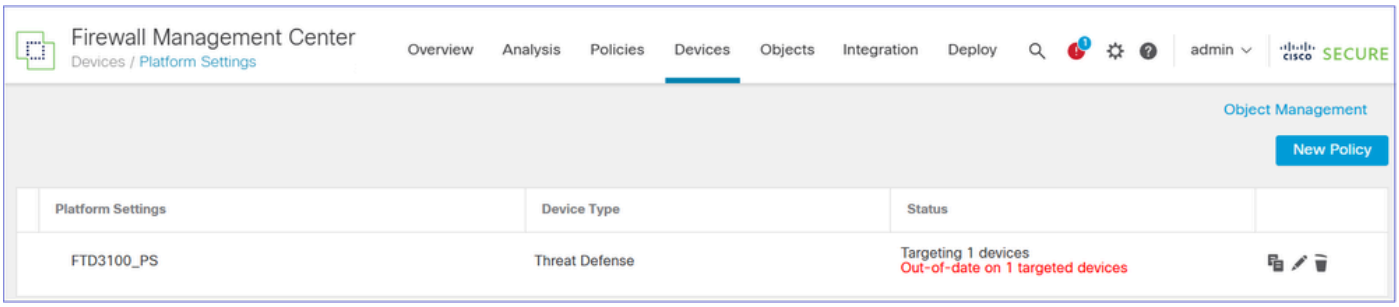
Étape 10. Terminer la configuration FTD

À ce stade, l'objectif est de configurer toutes les fonctionnalités qui peuvent encore manquer dans

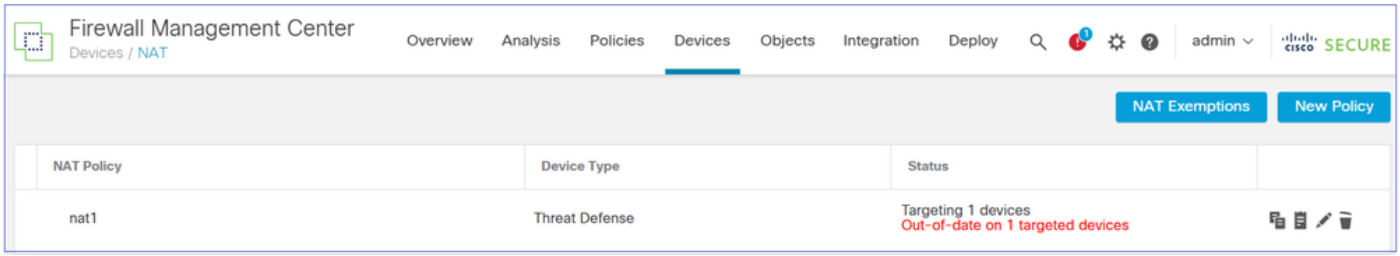
FTD1 après l'enregistrement sur FMC2 (FMC cible) et l'importation de la stratégie de périphérique.

Assurez-vous que les stratégies telles que NAT, les paramètres de plate-forme, la QoS, etc. sont affectés au FTD. Vous voyez que les stratégies sont attribuées mais en attente de déploiement.

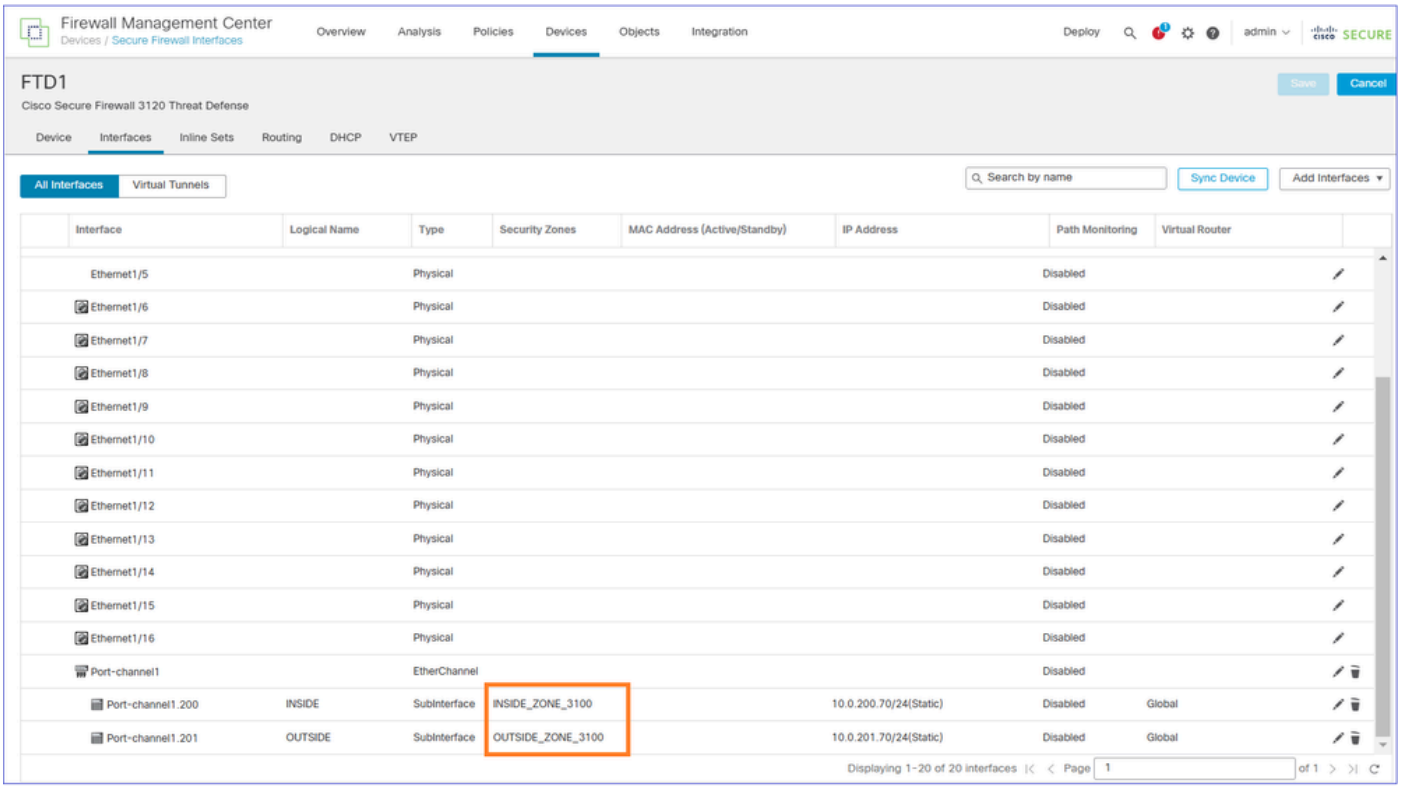
Par exemple, les paramètres de plate-forme sont importés et affectés au périphérique, mais en attente du déploiement :



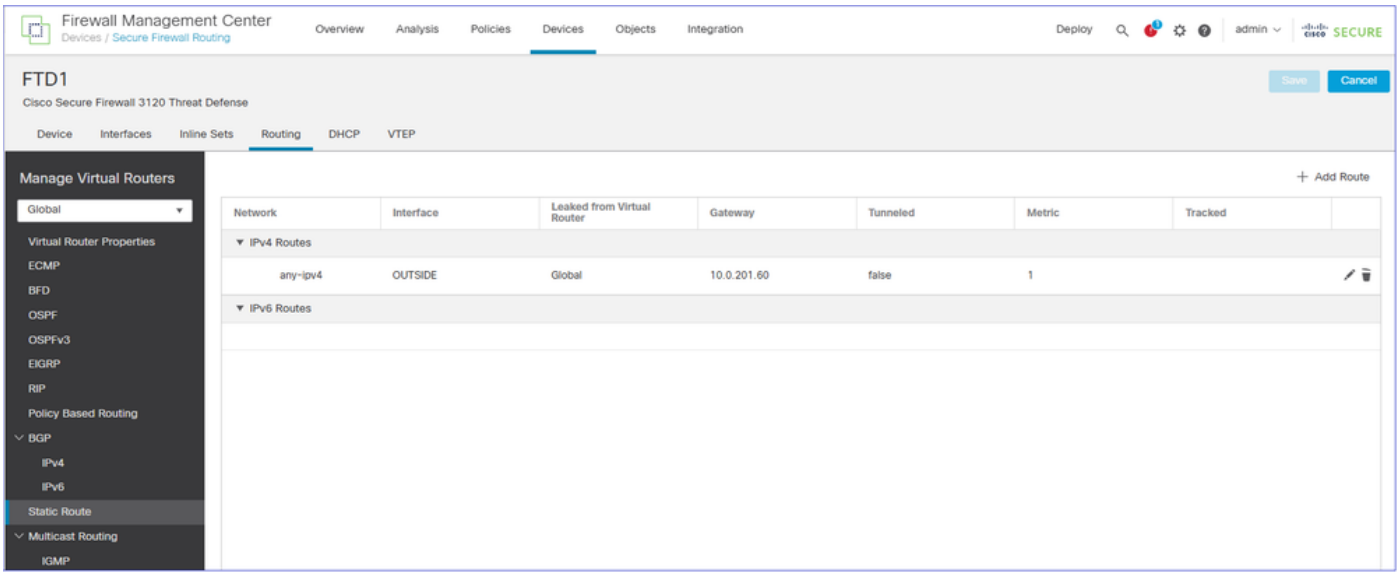
Si la NAT est configurée, la stratégie NAT est importée et attribuée au périphérique, mais en attente du déploiement :



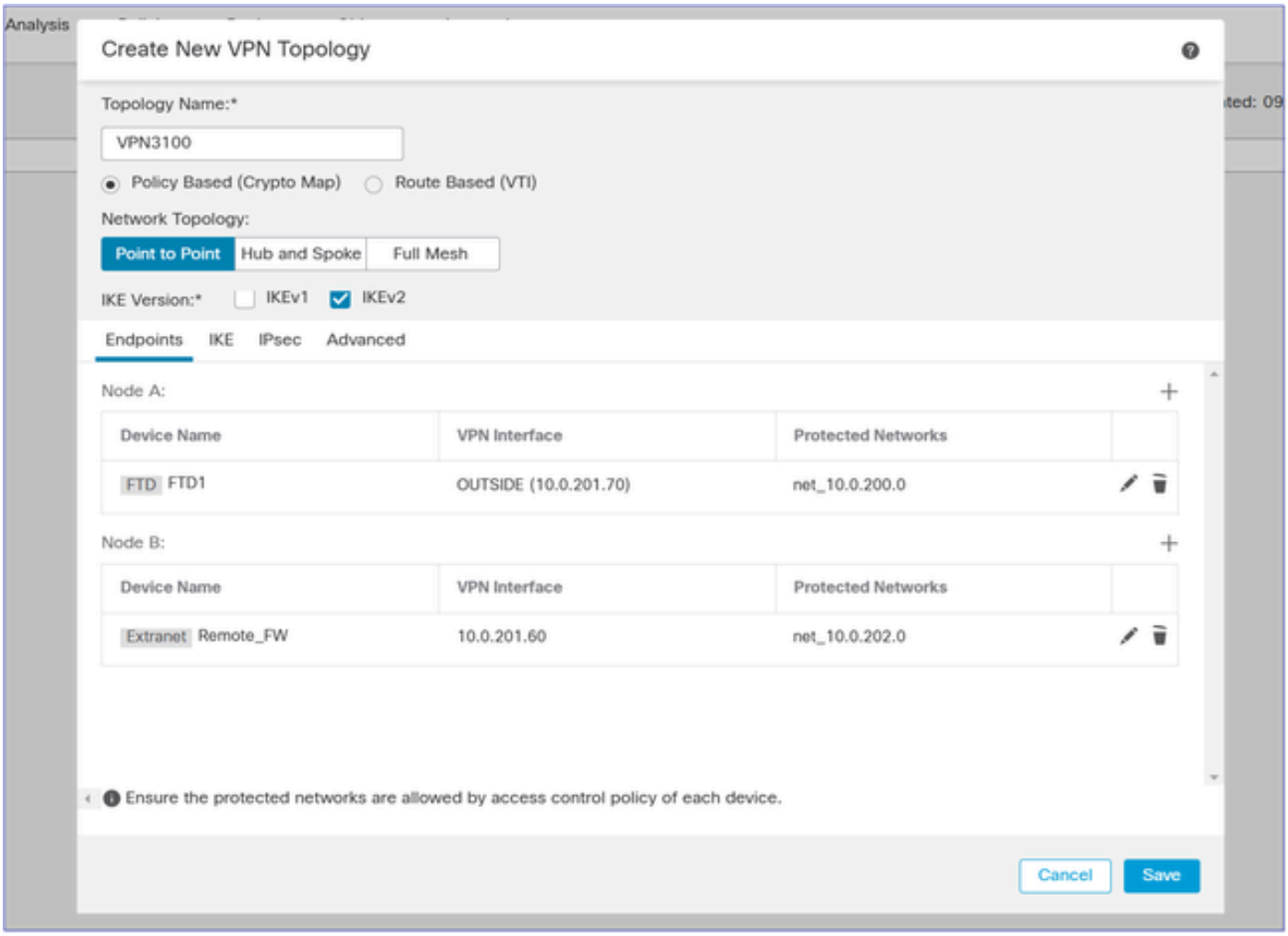
Les zones de sécurité sont appliquées aux interfaces :



La configuration du routage est appliquée au périphérique FTD :



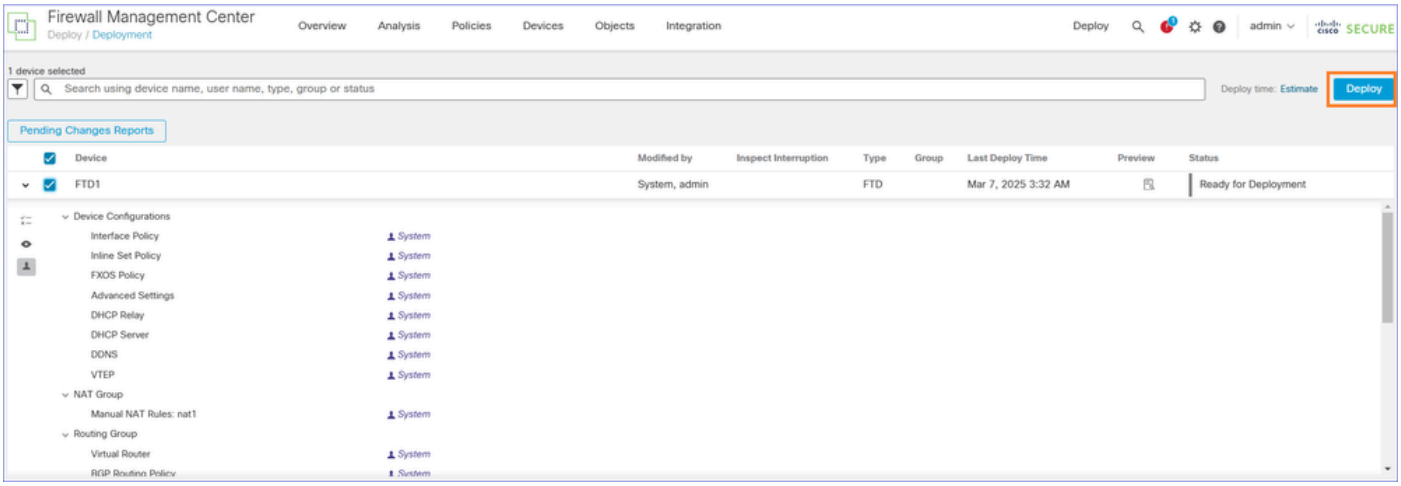
Remarque : C'est le moment de configurer les stratégies qui n'ont pas pu être migrées automatiquement (par exemple, les VPN).



Remarque : Si le FTD qui est migré a des homologues VPN S2S qui sont également migrés

vers le FMC cible, vous devez configurer le VPN après avoir déplacé tous les FTD vers le FMC cible.

Déployez les modifications en attente :



Étape 11. Vérification de la configuration FTD déployée

À ce stade, l'objectif est de vérifier à partir de l'interface de ligne de commande FTD que toute la configuration est en place.

La suggestion consiste à comparer le résultat de la commande « show running-config » des deux FTD. Vous pouvez utiliser des outils comme WinMerge ou diff pour la comparaison.

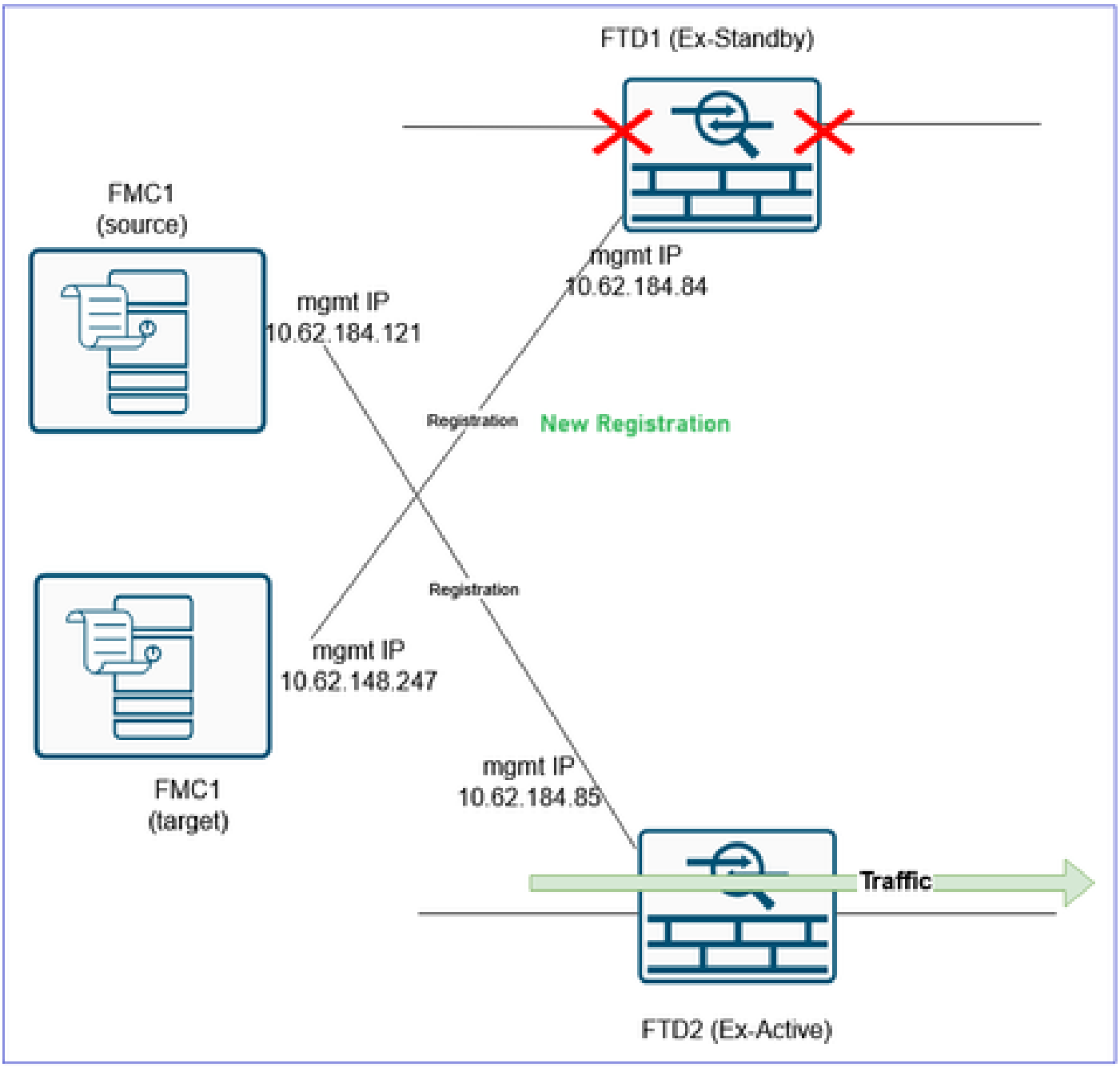
Les différences que vous voyez et qui sont normales sont les suivantes :

- Numéro de série du périphérique
- Descriptions des interfaces
- ID règle ACL
- Cryptochecksum de configuration

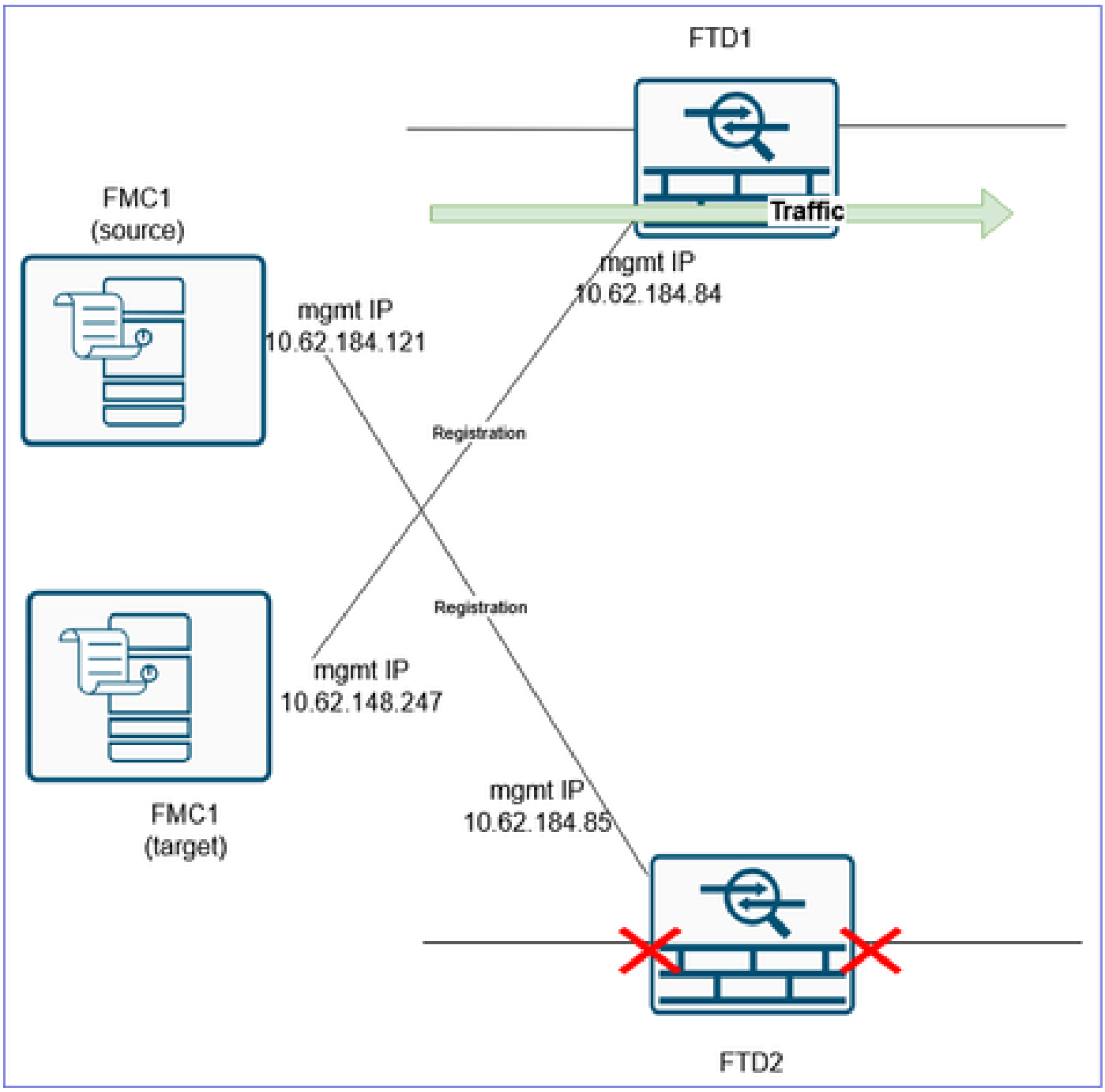
Étape 12. Effectuez le basculement

À cette étape, l'objectif est de commuter le trafic du FTD2 qui traite actuellement le trafic et qui est toujours enregistré vers l'ancien FMC/FMC source, vers le FTD1 qui est enregistré vers le FMC cible.

Avant :


FTD1 (Ex-Standby)
FMC1
(source)
mgmt IP
10.62.184.84
mgmt IP
10.62.184.121
Registration
New Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
Traffic
FTD2 (Ex-Active)

Après :



⚠ Mise en garde : Disposez d'un MW pour effectuer la transition. Pendant le basculement, vous allez avoir une interruption du trafic jusqu'à ce que tout le trafic soit transféré vers le FTD1, les VPN sont rétablis, et ainsi de suite.

⚠ Mise en garde : Ne lancez pas la mise en service à moins que la compilation ACP ne soit terminée (voir l'étape 10 ci-dessus).

⚠ Avertissement : Veillez à déconnecter les câbles de données du FTD2 ou à arrêter les ports de commutation associés. Sinon, vous pouvez vous retrouver avec les deux périphériques qui gèrent le trafic !

⚠ Mise en garde : Les deux périphériques utilisant la même configuration IP, le cache ARP des périphériques L3 adjacents doit être mis à jour. Envisagez d'effacer manuellement le cache ARP des périphériques adjacents pour accélérer le transfert du trafic.

Conseil : Vous pouvez également envoyer un paquet GARP et mettre à jour le cache ARP des périphériques adjacents à l'aide de la commande CLI FTD :

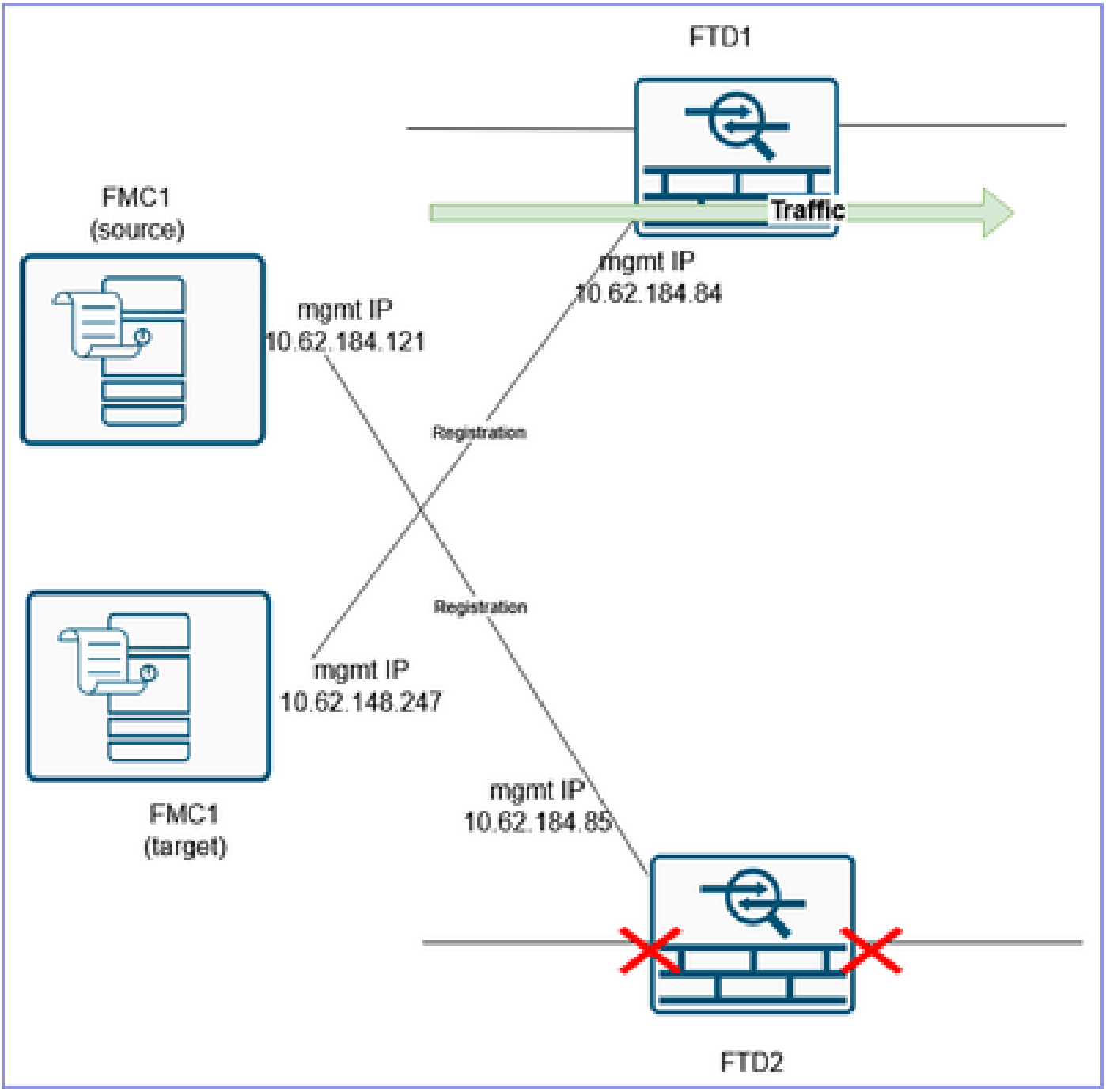
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

Vous devez répéter cette commande pour chaque adresse IP appartenant au pare-feu. Par conséquent, il peut être plus rapide d'effacer simplement le cache ARP des périphériques adjacents que d'envoyer des paquets GARP pour chaque IP appartenant au pare-feu.

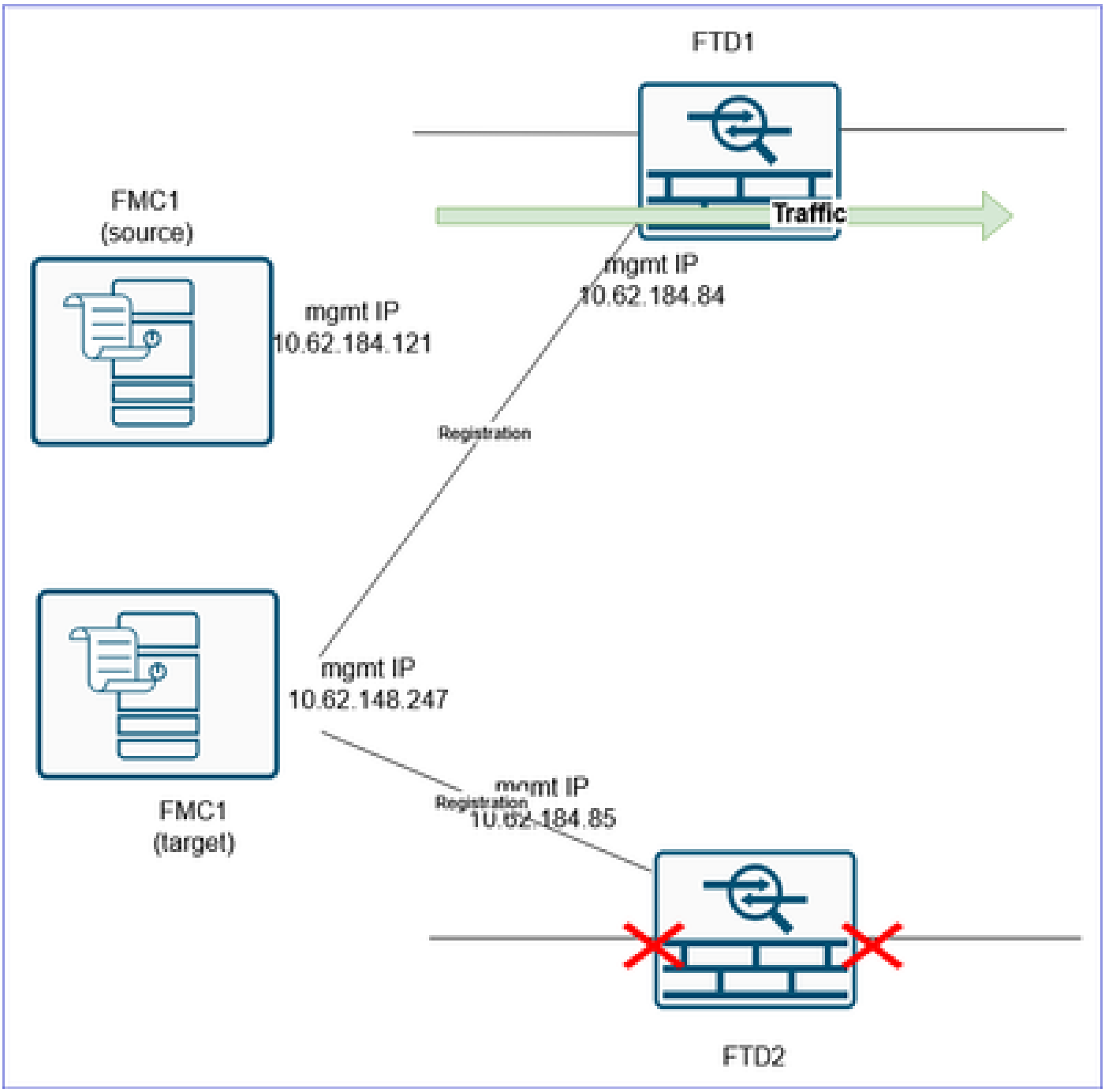
Étape 13. Migration du deuxième FTD vers FMC2 (FMC cible)

Le dernier point concerne la réforme de la paire haute disponibilité. Pour ce faire, vous devez d'abord supprimer le FTD2 du FMC1 (FMC source) et l'enregistrer sur le FMC2 (FMC cible).

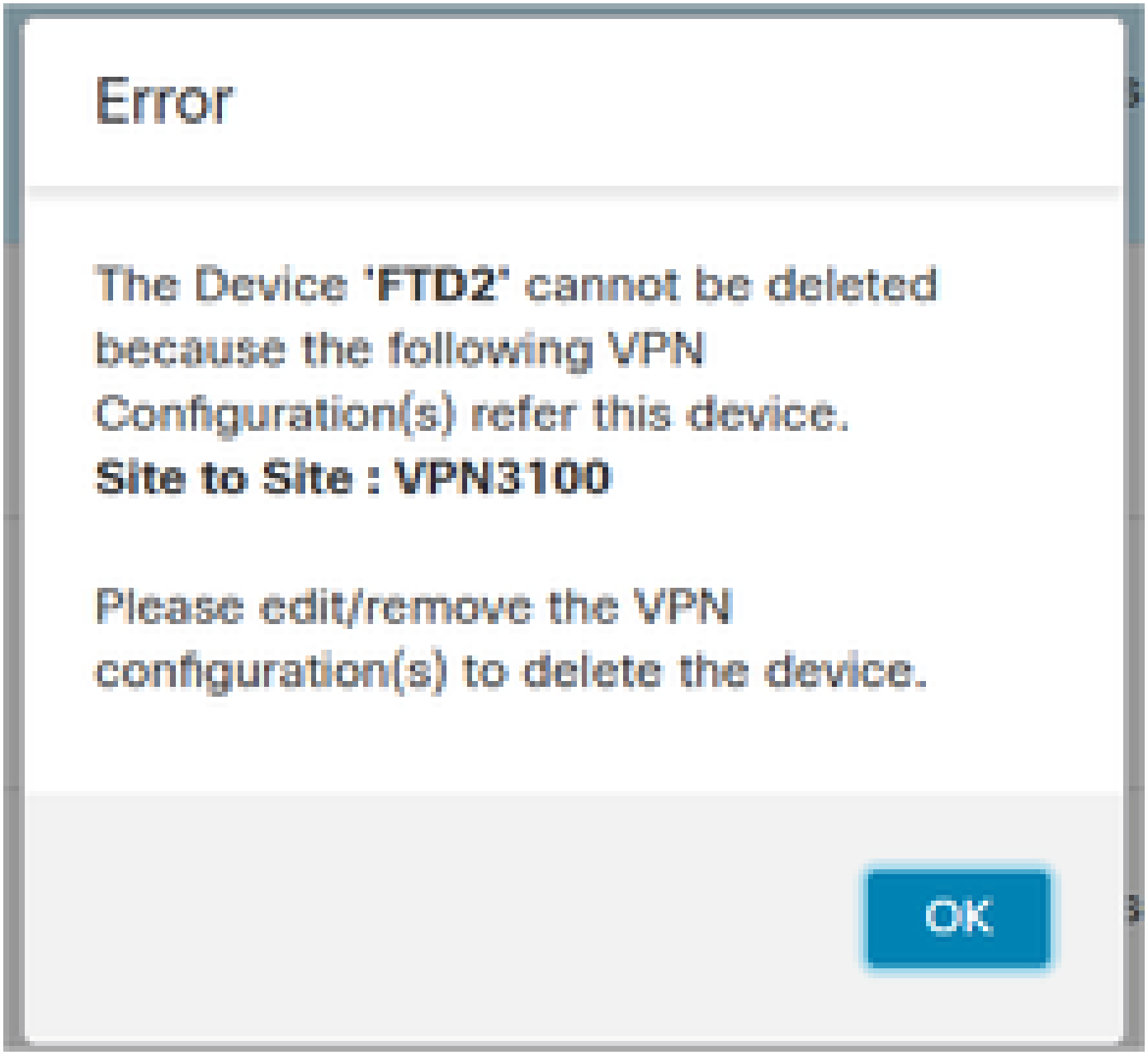
Avant :


FTD1
Traffic
mgmt IP
10.62.184.84
FMC1
(source)
mgmt IP
10.62.184.121
Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
FTD2

Après :



Si une configuration VPN est associée au FTD2, vous devez d'abord la supprimer avant de supprimer le FTD. Dans d'autres cas, un message similaire à celui-ci s'affiche :



Vérification CLI :

<#root>

>

show managers

No managers configured.

Il est recommandé d'effacer toute la configuration FTD avant de l'enregistrer auprès du FMC cible. Pour ce faire, passez rapidement d'un mode de pare-feu à l'autre.

Par exemple, si vous avez le mode routé, passez en mode transparent, puis revenez en mode

routé :

<#root>

>

configure firewall transparent

Et ensuite :

<#root>

>

configure firewall routed

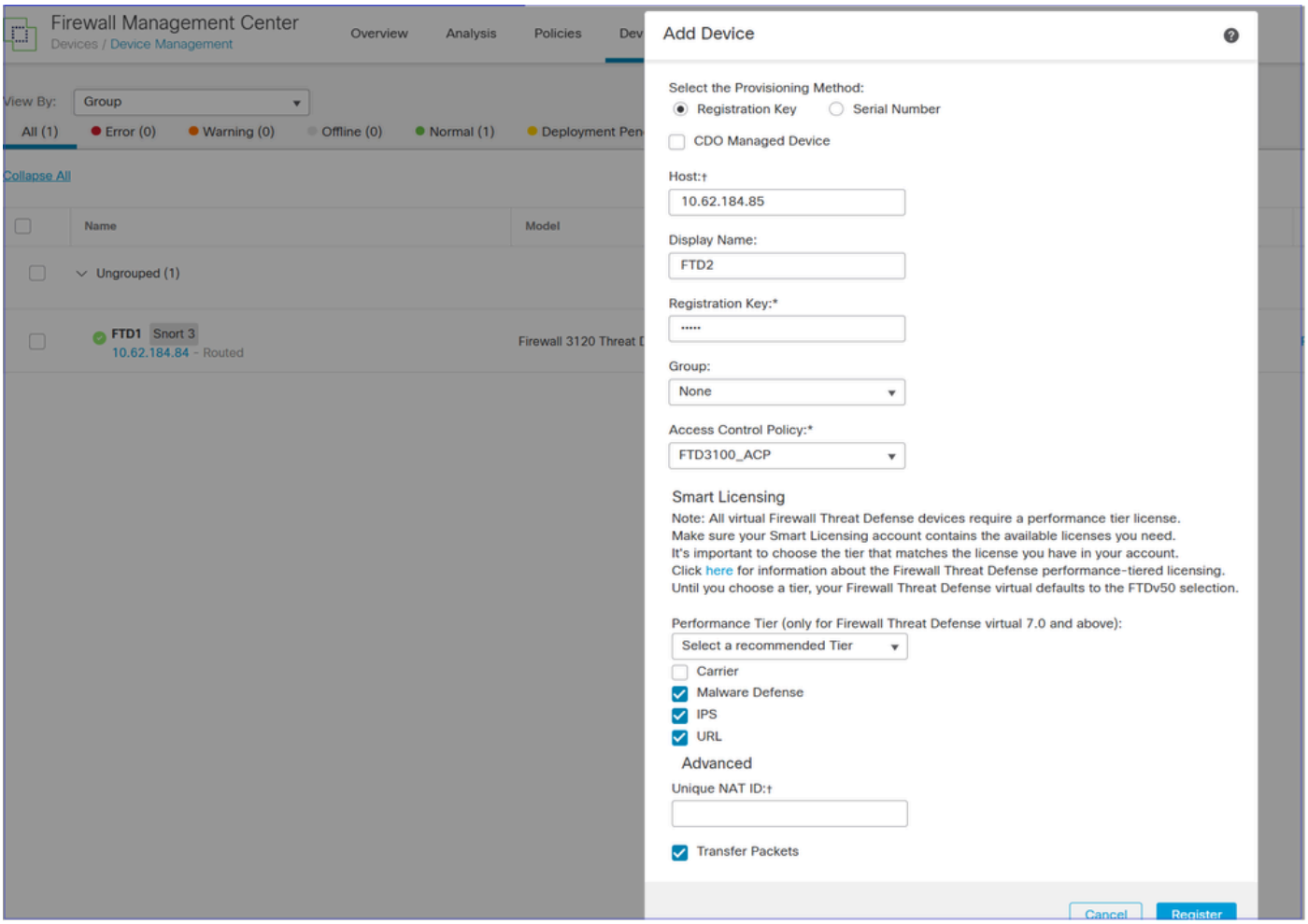
Ensuite, enregistrez-le sur le FMC2 (FMC cible) :

<#root>

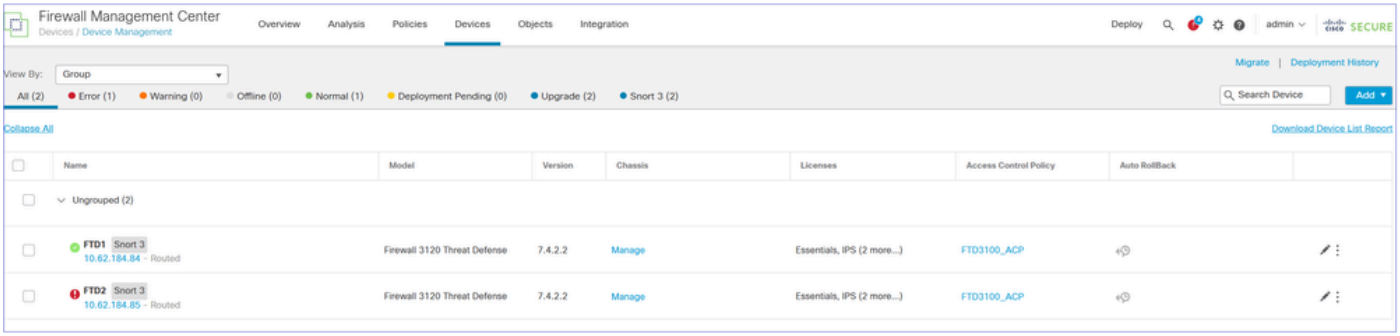
>

configure manager add 10.62.148.247 cisco

```
Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```



Le résultat :

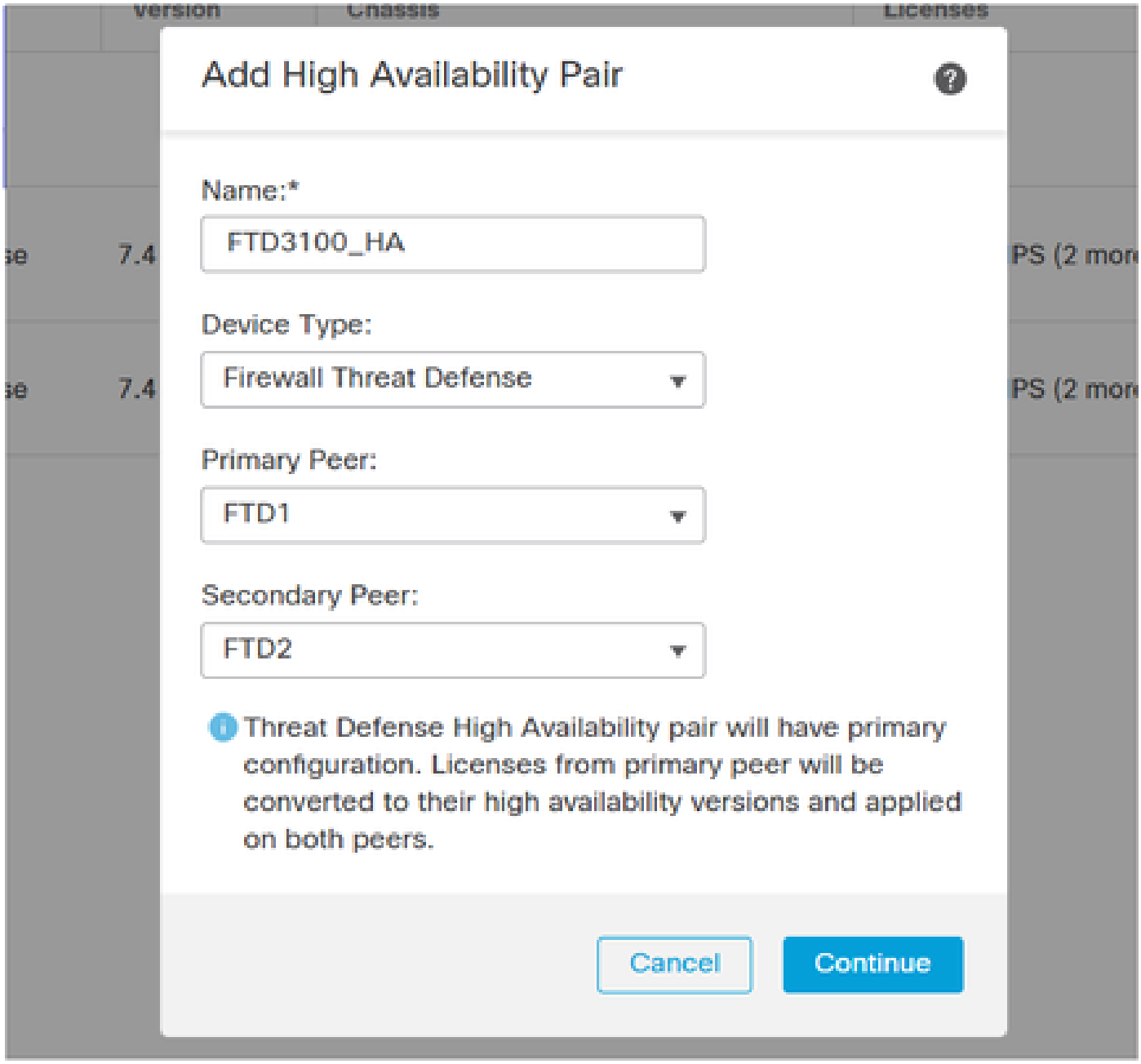


Étape 14. Reformez la haute disponibilité FTD

Remarque : Cette tâche (comme toute tâche liée à la haute disponibilité) doit également être exécutée pendant un MW. Pendant la négociation de haute disponibilité, il va y avoir une interruption du trafic d'environ 1 minute depuis que les interfaces de données sont hors service.

Sur le FMC cible, accédez à Devices > Device Management et Add > High Availability.

⚠ Mise en garde : Assurez-vous de sélectionner comme homologue principal le FTD qui gère le trafic (FTD1 dans ce scénario) :



Reconfigurer les paramètres de haute disponibilité, notamment les interfaces surveillées, les adresses IP de secours, les adresses MAC virtuelles, etc.

Vérification à partir de FTD1 CLI :

<#root>

```
FTD3100-3#
show failover | include host

        This host: Primary - Active
        Other host: Secondary - Standby Ready
```

Vérification à partir de FTD2 CLI :

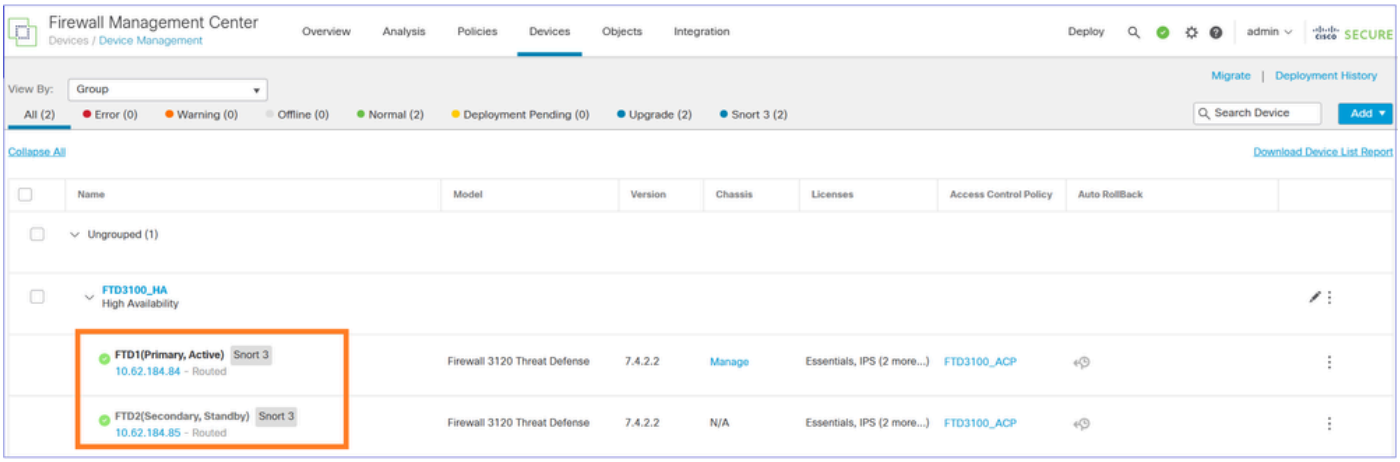
<#root>

FTD3100-3#

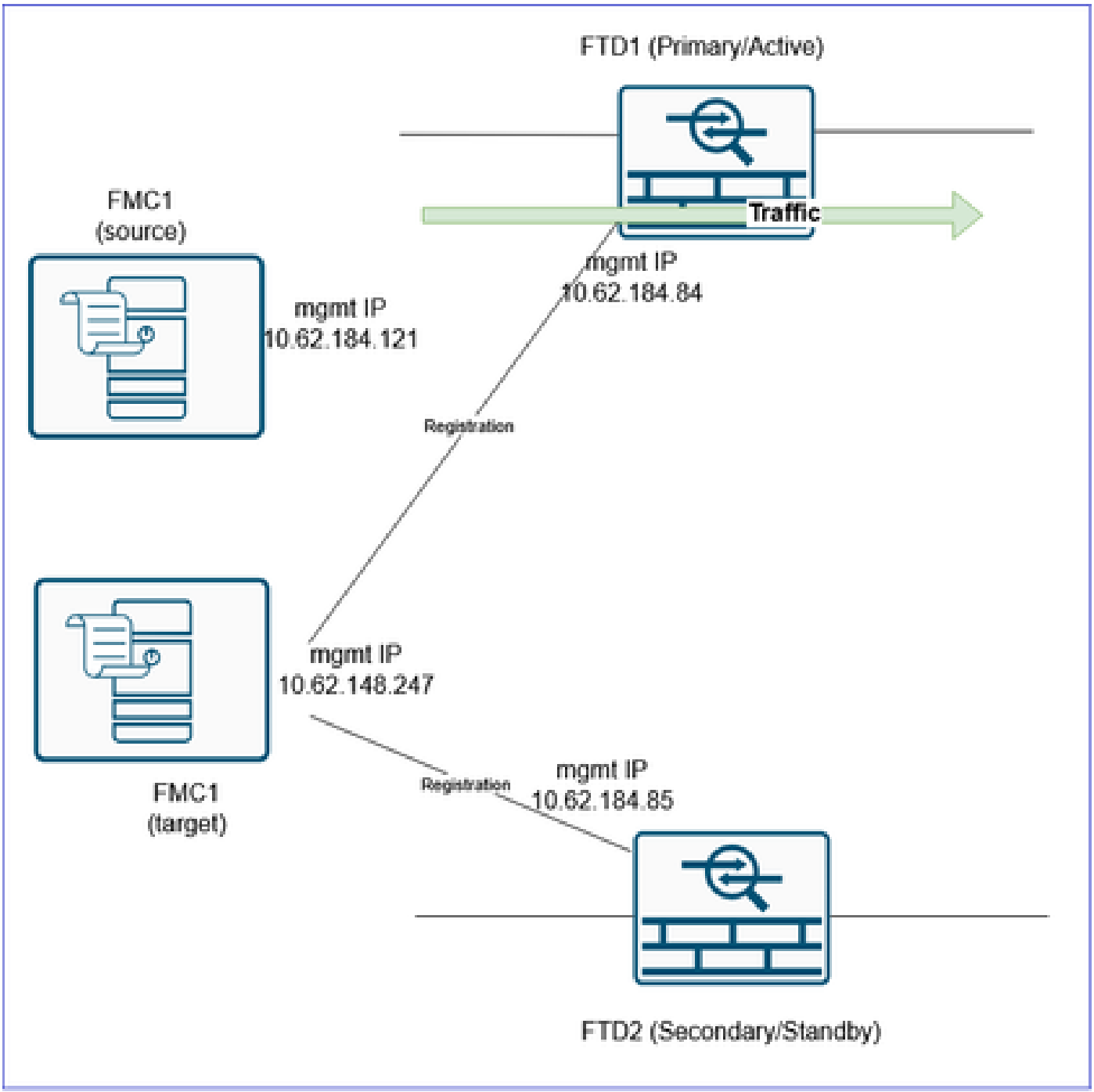
show failover | include host

```
        This host: Secondary - Standby Ready
        Other host: Primary - Active
```

Vérification de l'interface FMC :



Enfin, activez/reconnectez les interfaces de données du périphérique FTD2.



Références

- Exportation et importation de la configuration du périphérique
- Ajouter une paire haute disponibilité
- Migration d'un FTD d'un FMC vers un autre FMC

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.