

Migration de FTD HA (basculement) vers un autre FMC

Table des matières

[Introduction](#)

[Abréviations](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Topologie](#)

[Configurer](#)

[Étape 1 : exportation de la configuration du périphérique à partir du pare-feu principal](#)

[Étape 2 : activation du FTD secondaire](#)

[Étape 3. Interrompre la haute disponibilité du FTD](#)

[Étape 4. Isolation des interfaces de données FTD1 \(ex-Primary\)](#)

[Étape 5. Exportation des stratégies partagées FTD](#)

[Étape 6. Suppression/annulation de l'enregistrement du FTD1 \(ex-Primary\) de l'ancien FMC source](#)

[Étape 7. Importez l'objet de configuration de la stratégie FTD dans FMC2 \(FMC cible\)](#)

[Étape 8. Enregistrement du FTD1 \(ex-Primary\) dans le FMC2](#)

[Étape 9. Importez l'objet de configuration du périphérique FTD dans FMC2 \(FMC cible\)](#)

[Étape 10. Terminer la configuration FTD](#)

[Étape 11. Vérification de la configuration FTD déployée](#)

[Étape 12. Effectuez le basculement](#)

[Étape 13. Migration du deuxième FTD vers FMC2 \(FMC cible\)](#)

[Étape 14. Reformez la haute disponibilité FTD](#)

[Références](#)

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 :

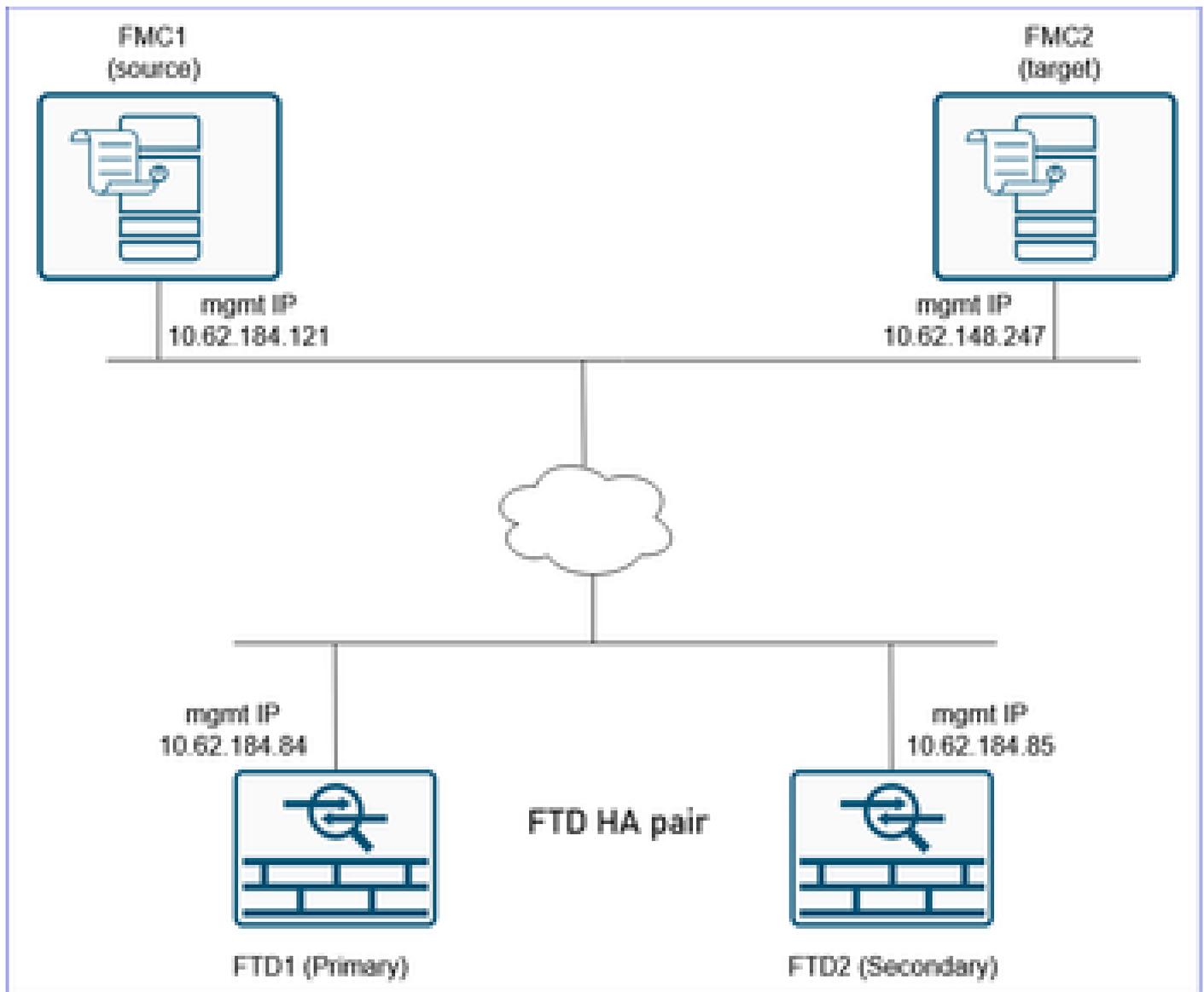
- L'interface utilisateur et l'interface de ligne de commande accèdent aux FMC source et de destination.
- Informations d'identification administratives pour les FMC et les pare-feu.
- Accès console aux deux pare-feu.
- Accès aux périphériques amont et aval de couche 3 (au cas où vous auriez besoin d'effacer 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



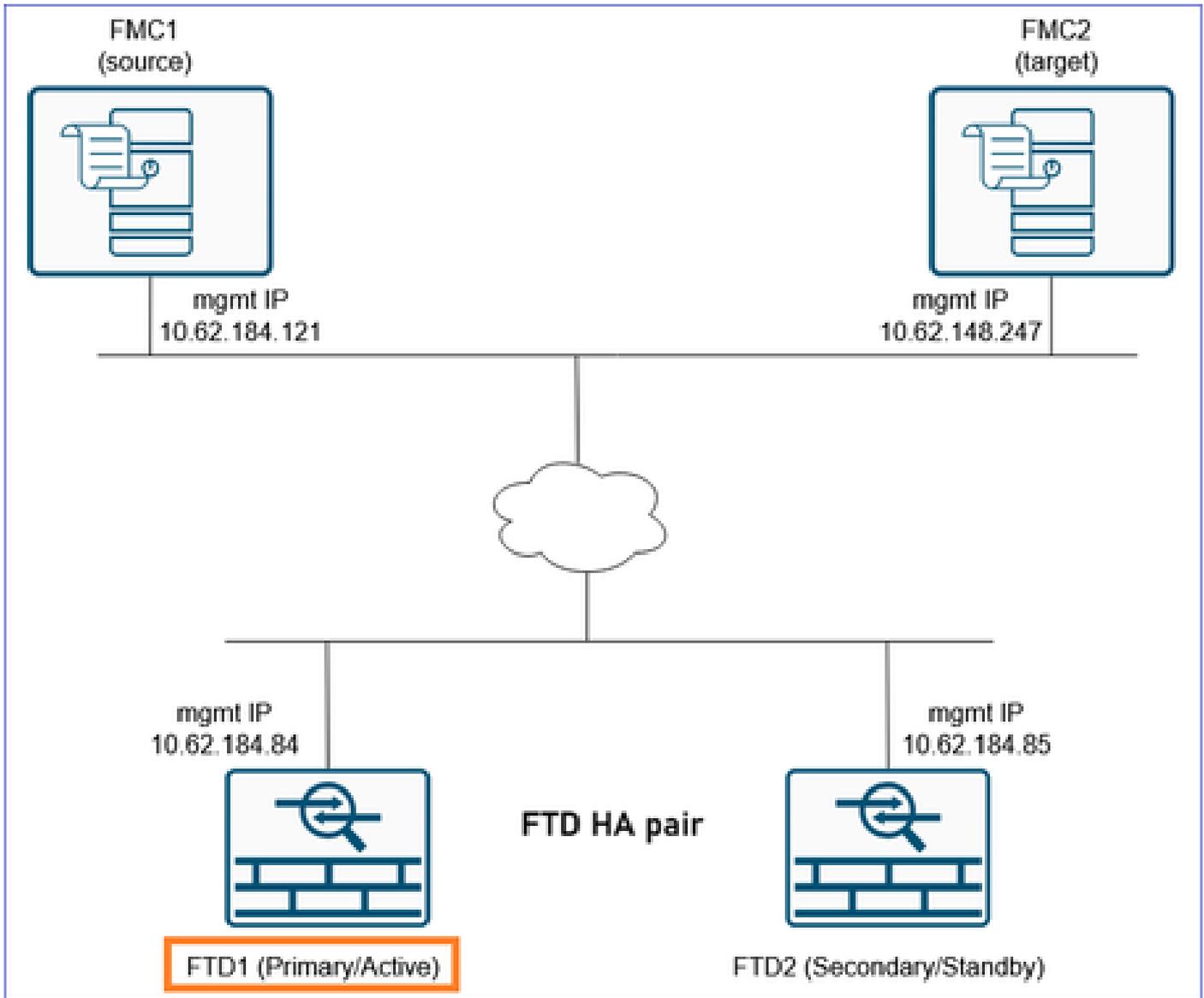
Configurer

Étapes de migration

Pour ce scénario, nous considérons les états suivants :

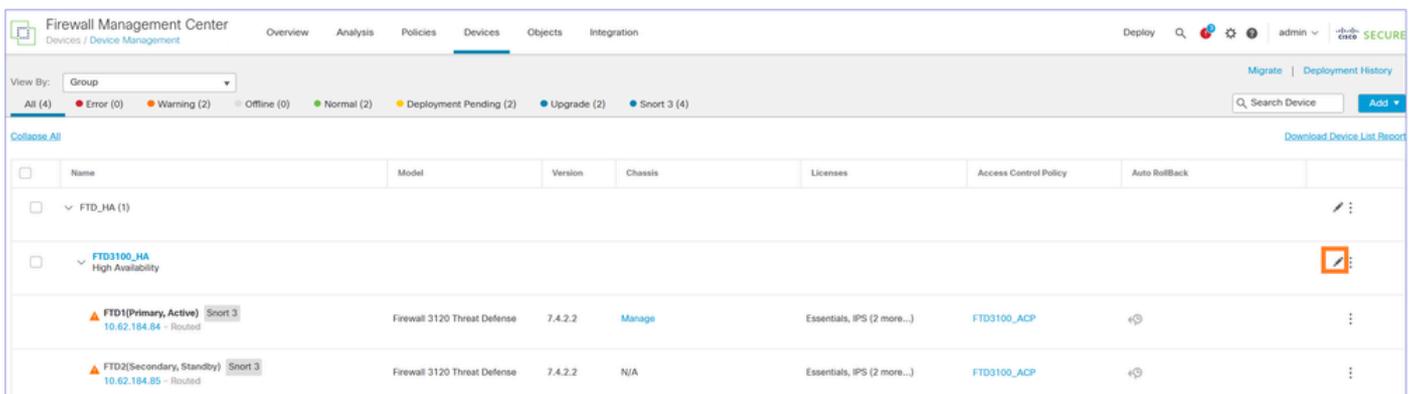
FTD1 : Principal/actif

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 :

The screenshot shows the Cisco Firewall Management Center interface for device FTD1. The 'General' section is visible, with the 'Export' button highlighted by a red box and a red number '2'. The 'System' section is also visible, showing details like Model, Serial, Time, and Version. A red number '1' is placed near the device name dropdown menu.

 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:

The screenshot shows the 'Tasks' page in the Cisco Firewall Management Center. The 'Tasks' tab is selected, and a notification for 'Device Configuration Export' is displayed, indicating that the export file was created successfully. A 'Download Export Package' link is visible.

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-ecccc8b72b7c8

Étape 2 : activation du FTD secondaire

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

The screenshot shows the Firewall Management Center interface. The 'Devices' tab is active, displaying a list of devices. A 'High Availability' pair is expanded, showing two FTDs: 'FTD1(Primary, Active)' and 'FTD2(Secondary, Standby)'. A context menu is open over the 'FTD2' entry, with the 'Switch Active Peer' option highlighted in orange. Other options in the menu include Break, Force refresh node status, Delete, Revert Upgrade, Health Monitor, and Troubleshoot Files.

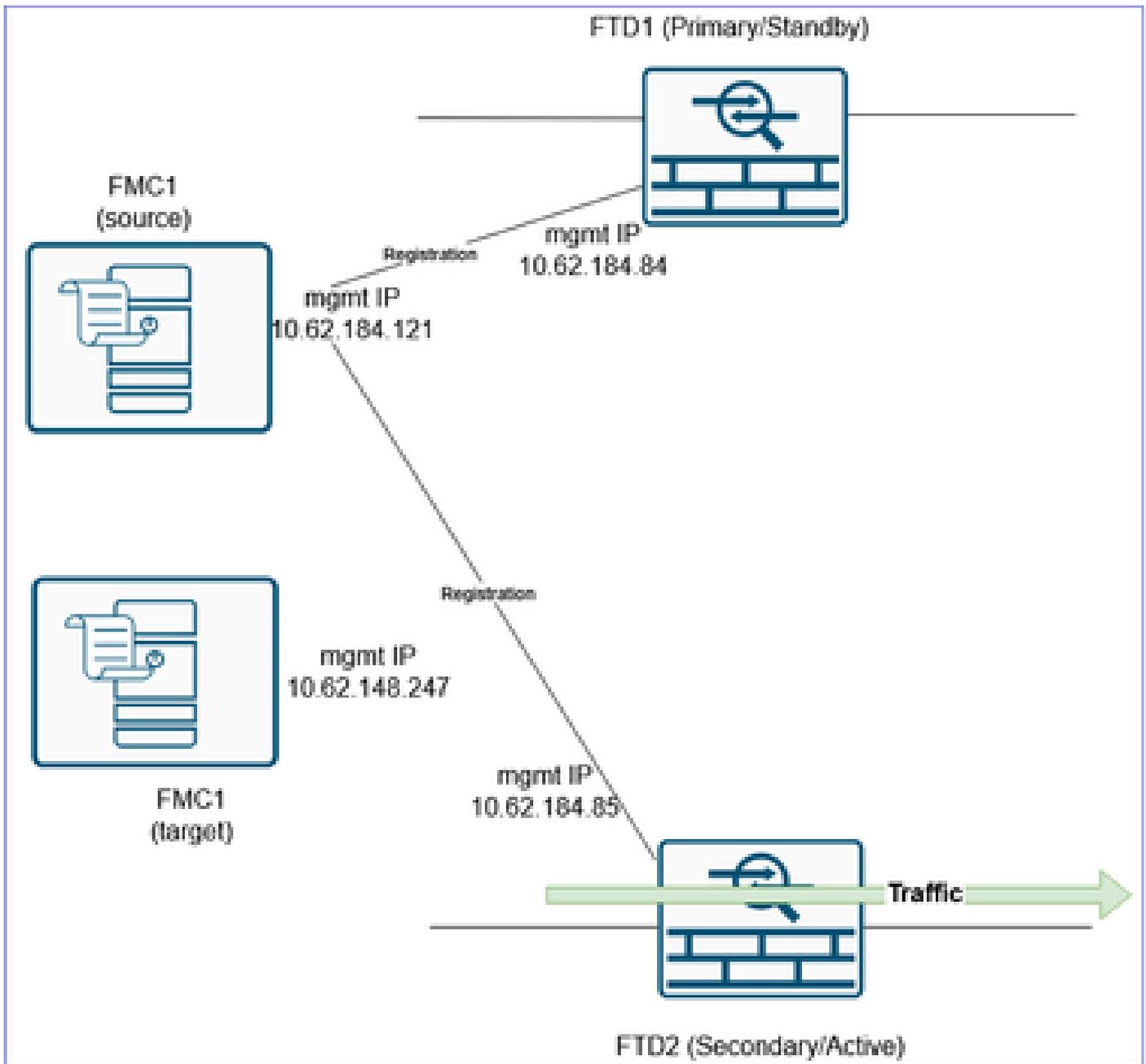
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
FTD3100_HA High Availability							
FTD1(Primary, Active)	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	
FTD2(Secondary, Standby)	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	

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

The screenshot shows the Firewall Management Center interface after the configuration change. The 'High Availability' pair is still expanded, but now 'FTD2(Secondary, Active)' is highlighted with an orange box, indicating it is the active peer. 'FTD1' is now in a 'Standby' state.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
FTD3100_HA High Availability							
FTD1(Primary, Standby)	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	
FTD2(Secondary, Active)	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	

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:

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is active, displaying a list of devices under the 'FTD3100_HA High Availability' group. The following table summarizes the visible device information:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD1(Primary, Standby)	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	+⊖
FTD2(Secondary, Active)	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+⊖

A context menu is open over the 'FTD2(Secondary, Active)' device, with the 'Break' option highlighted. Other options in the menu include 'Switch Active Peer', 'Force refresh node status', 'Delete', 'Revert Upgrade', 'Health Monitor', and 'Troubleshoot Files'.

Cette fenêtre apparaît . Sélectionnez oui

Confirm Break

 Breaking the High Availability pair "FTD3100_HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair?

 Breaking High Availability pair when Secondary device is active may cause extended network disruption for NAT traffic. Please ensure to perform clear arp on upstream and downstream devices to restore connectivity.

Force break, if standby peer does not respond

 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#

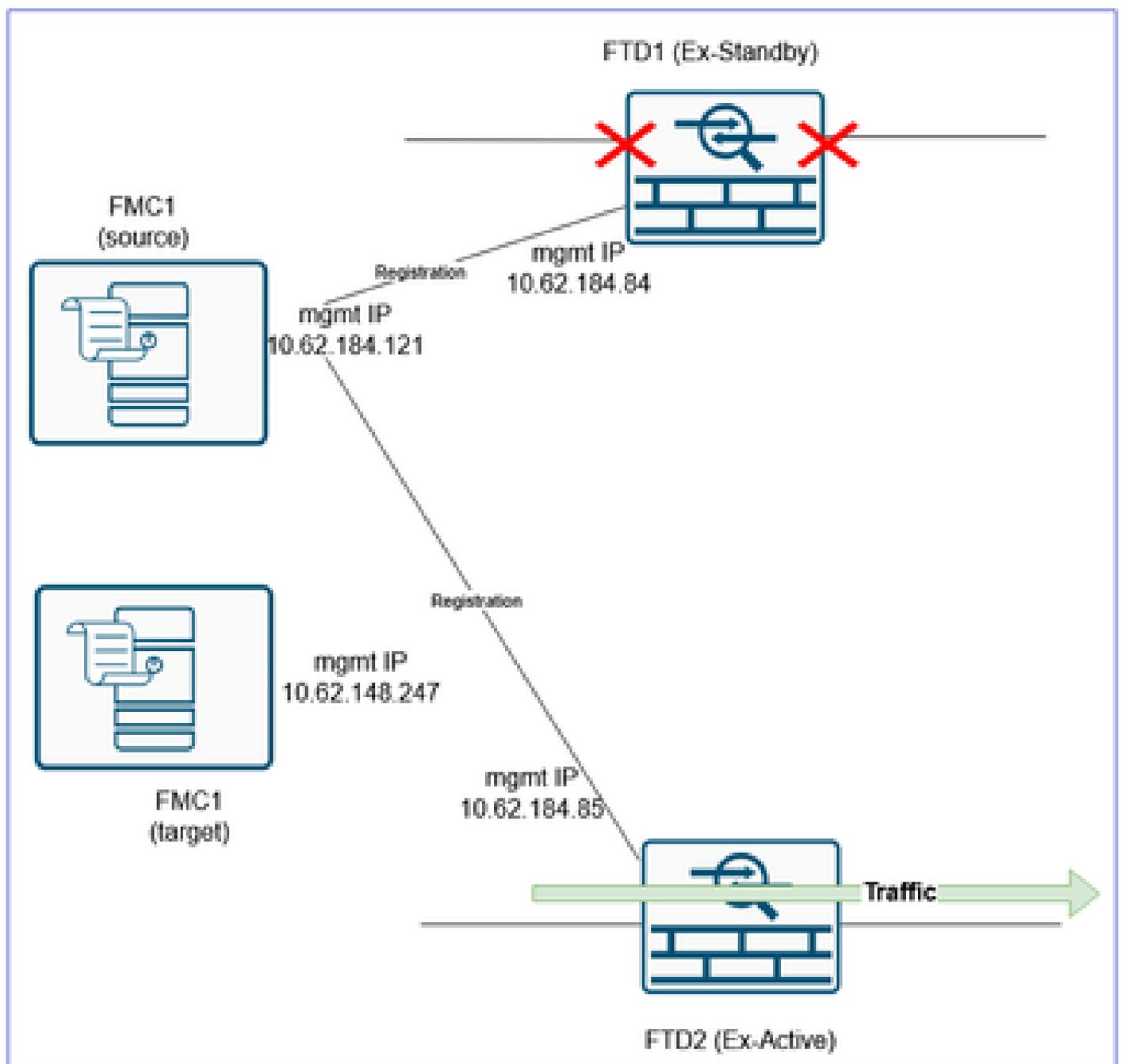
show interface ip brief

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

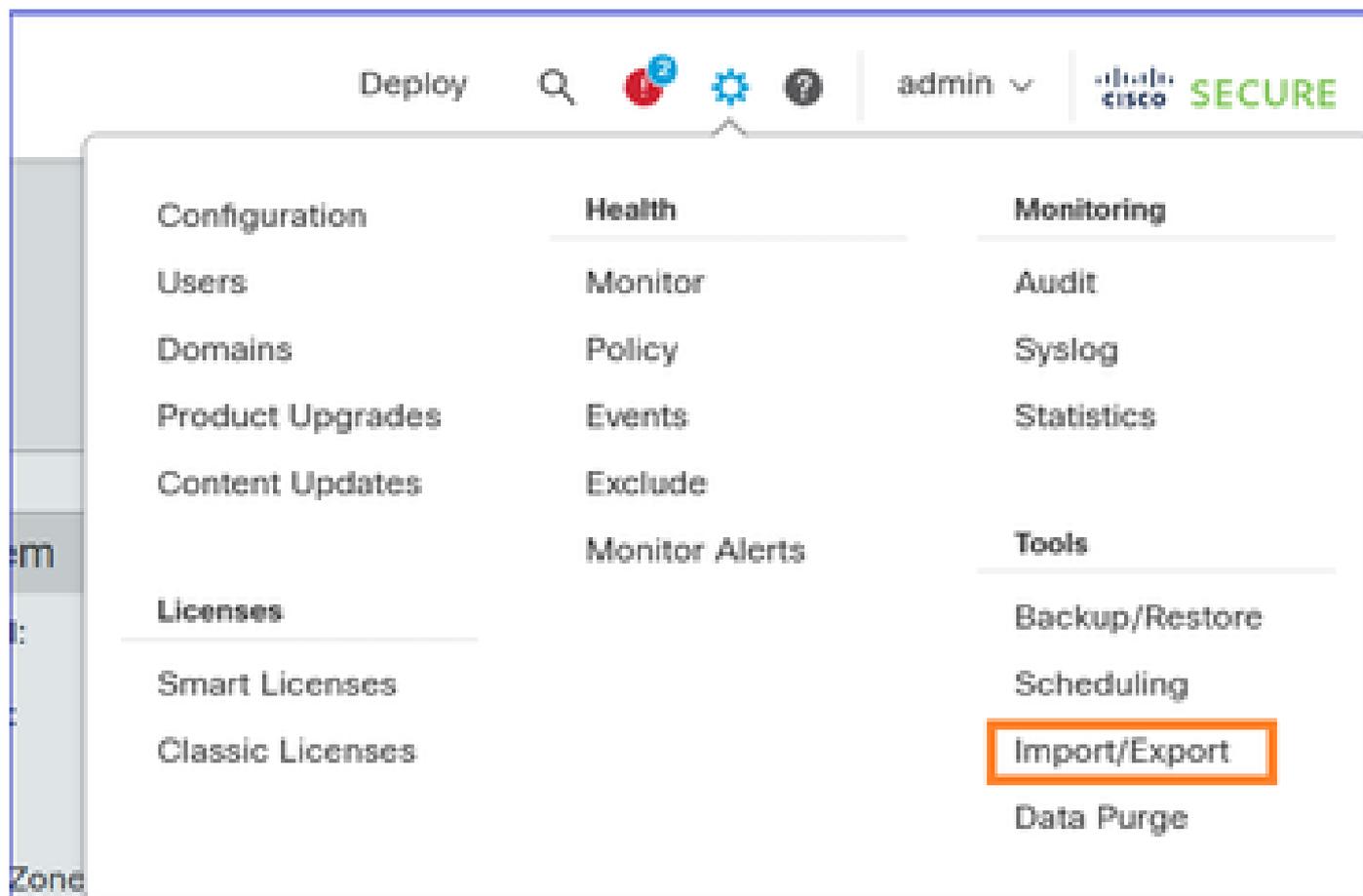
Étape 4. Isolation des interfaces de données FTD1 (ex-Primary)

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



Étape 5. Exportation des stratégies partagées FTD

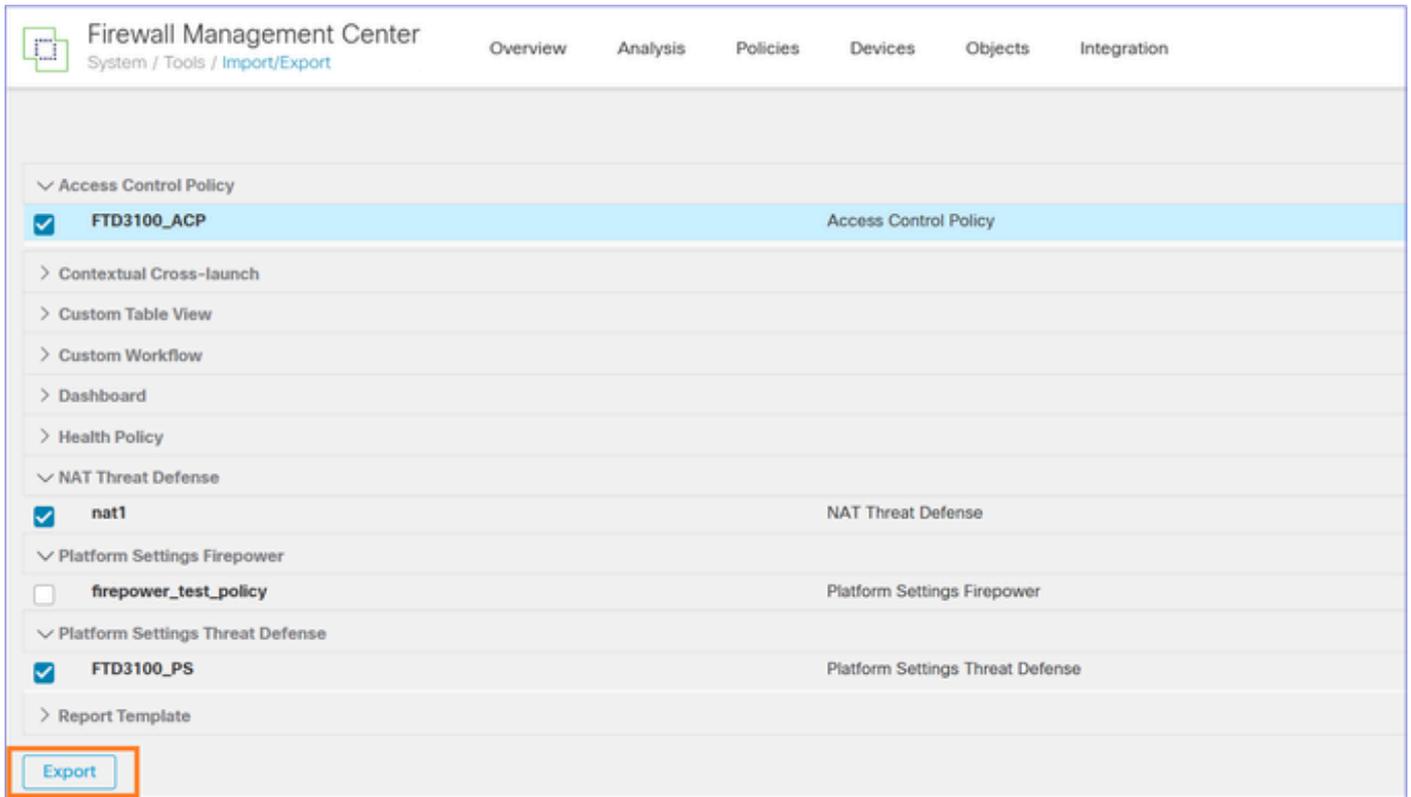
Accédez à System > Tools et sélectionnez Import/Export :



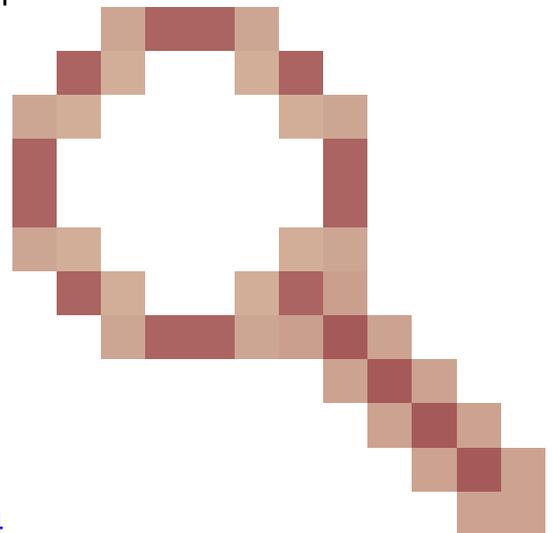
Exportez les différentes stratégies associées au périphérique. Assurez-vous d'exporter toutes les stratégies associées au FTD, telles que :

- 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](https://www.cisco.com/cisco/web/bugtools/bugdetail.do?moduleId=3&bugtype=bug&bugid=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

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

Migrate | Deployment History

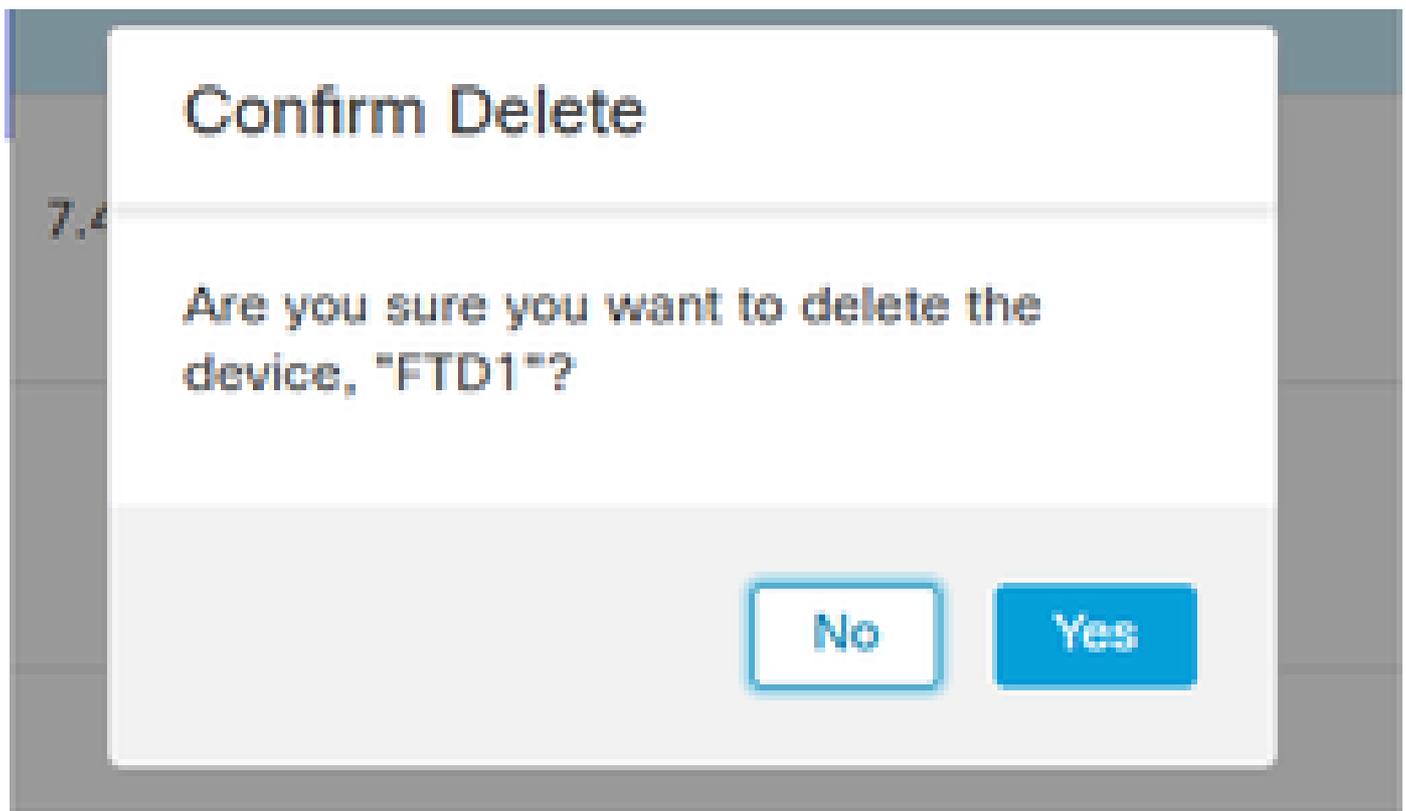
All (4) Error (0) Warning (0) Offline (0) Normal (4) Deployment Pending (1) Upgrade (2) Snort 3 (4)

Search Device Add

Collaps All Download Device List Report

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
FTD_HA (2)							
FTD1 Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP		<ul style="list-style-type: none"> Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot Files
FTD2 Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP		
Un grouped (1)							

Confirmez la suppression du périphérique :



Vérification CLI FTD1 :

```
<#root>
```

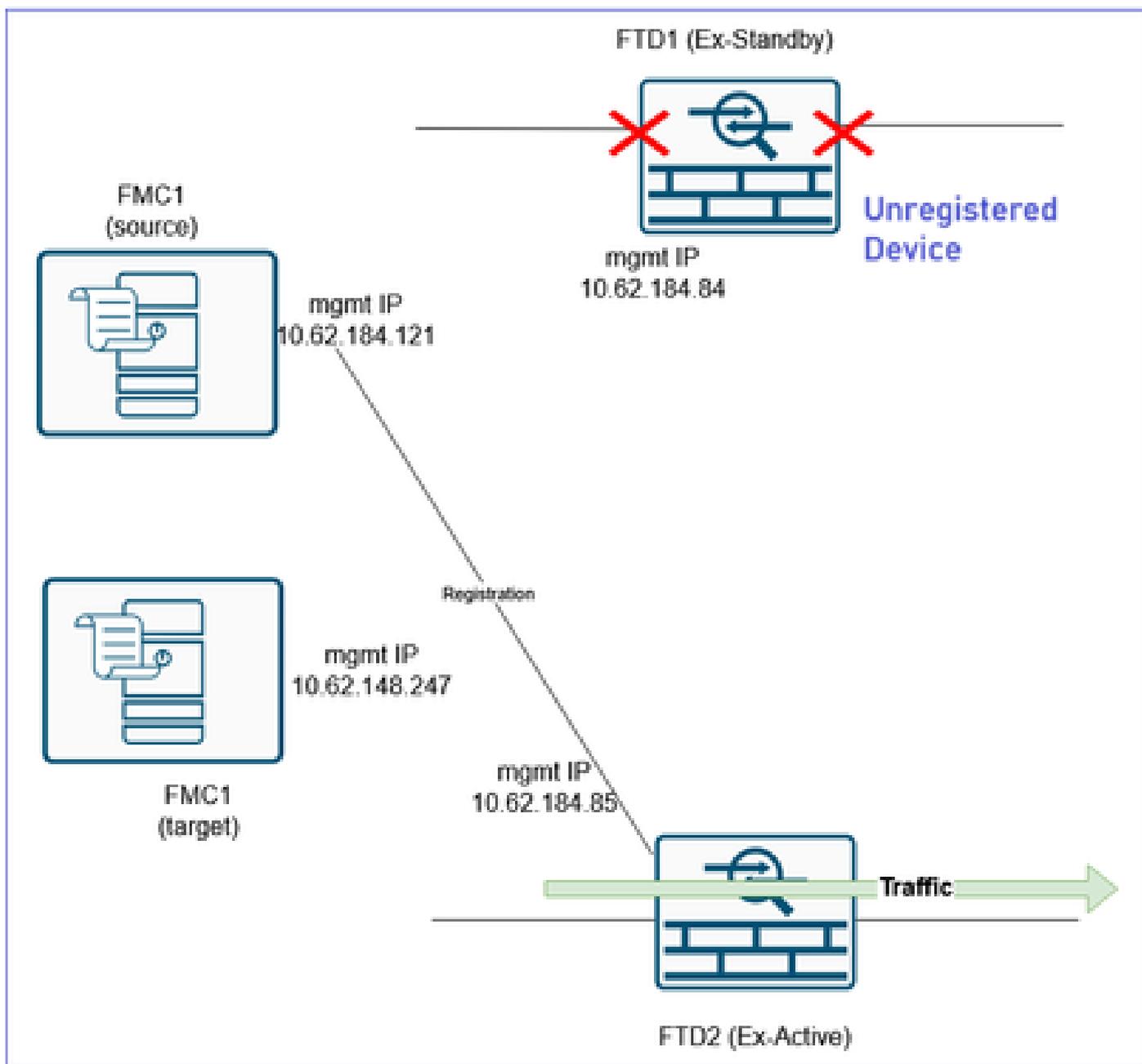
```
>
```

```
show managers
```

```
No managers configured.
```

```
>
```

État actuel après la suppression du périphérique FTD1 :

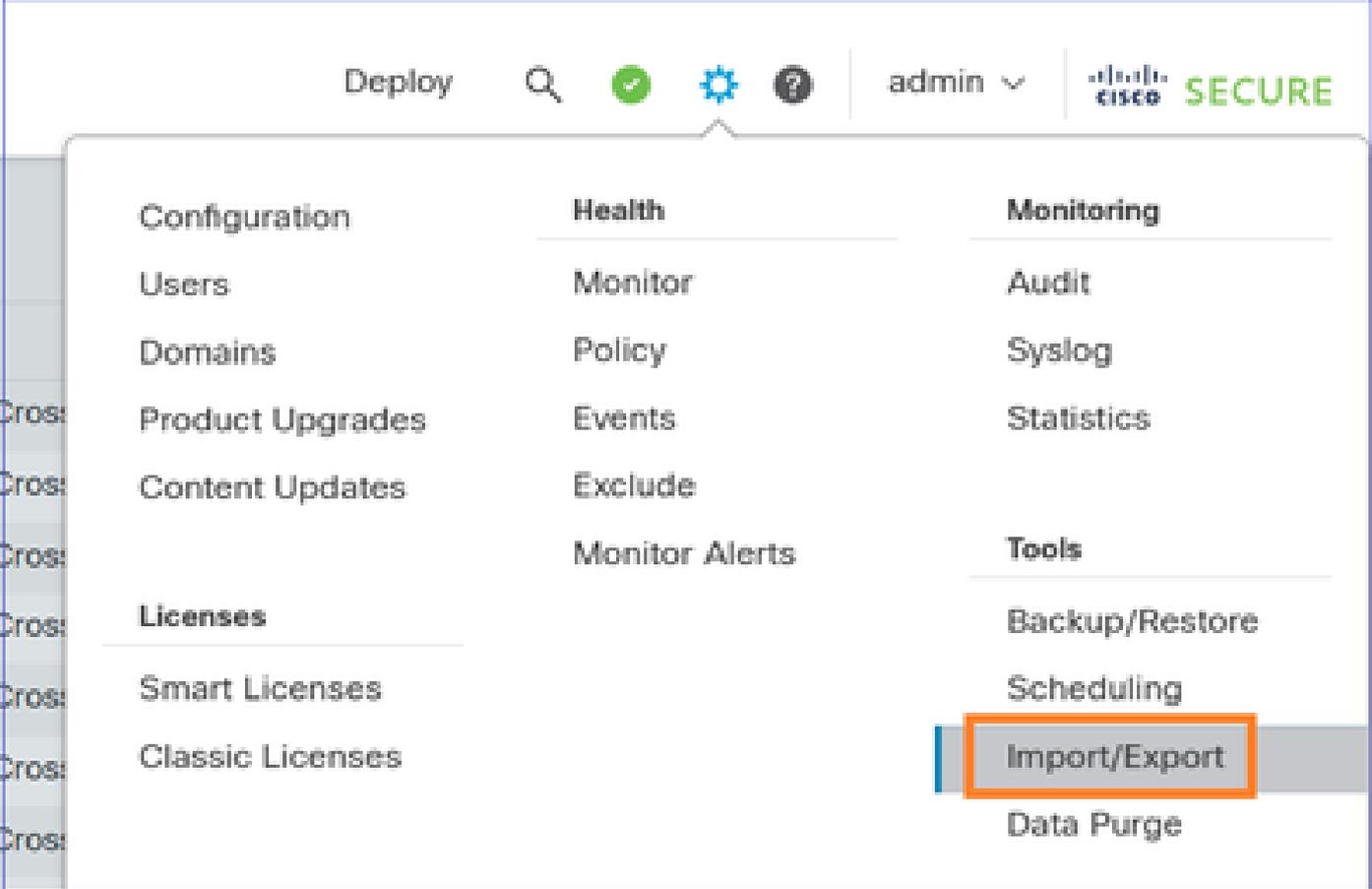


Étape 7. Importez l'objet de configuration de la stratégie FTD dans FMC2 (FMC cible)

-  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).

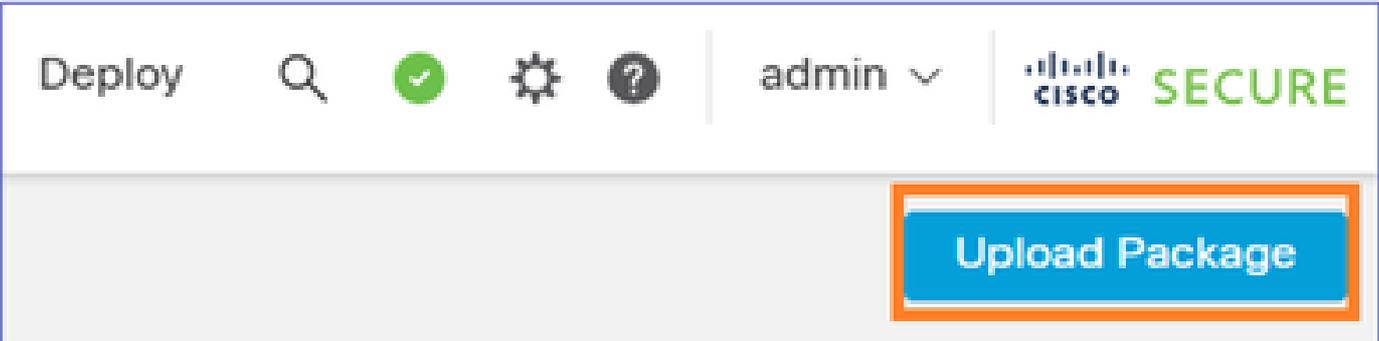
 - Si vous choisissez l'option 'b', à l'étape 9, assurez-vous de réaffecter les objets nouvellement créés aux stratégies migrées (zones de sécurité ACP, zones de sécurité NAT, routage, paramètres de plate-forme, etc.).

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



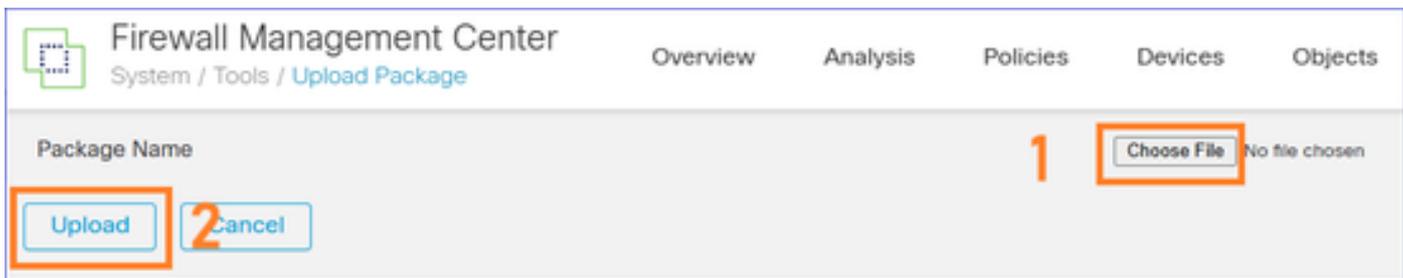
The screenshot shows the Cisco Secure FMC2 interface. The top navigation bar includes 'Deploy', a search icon, a green checkmark, a gear icon, a question mark icon, a user dropdown menu labeled 'admin', and the Cisco Secure logo. A dropdown menu is open, displaying three columns: 'Configuration', 'Health', and 'Monitoring'. The 'Tools' section is expanded, and the 'Import/Export' option is highlighted with an orange box. Other options in the 'Tools' section include 'Backup/Restore', 'Scheduling', and 'Data Purge'.

Sélectionnez Charger le paquet :

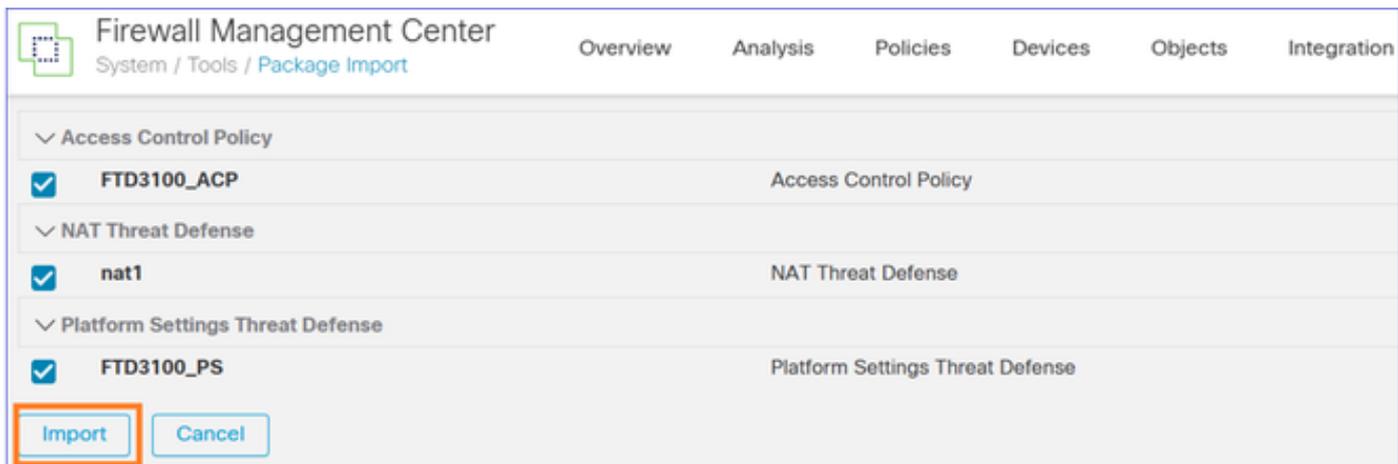


The screenshot shows the Cisco Secure FMC2 interface. The top navigation bar is the same as in the previous screenshot. A large blue button labeled 'Upload Package' is highlighted with an orange box.

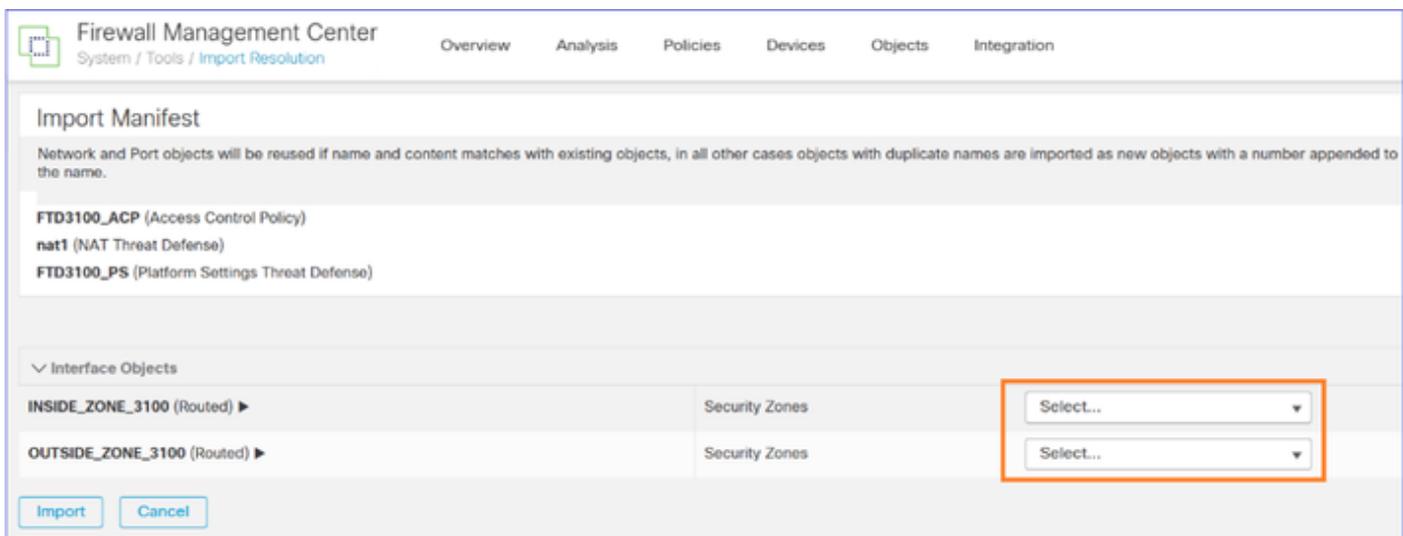
Téléchargez le fichier :



Importez les stratégies :



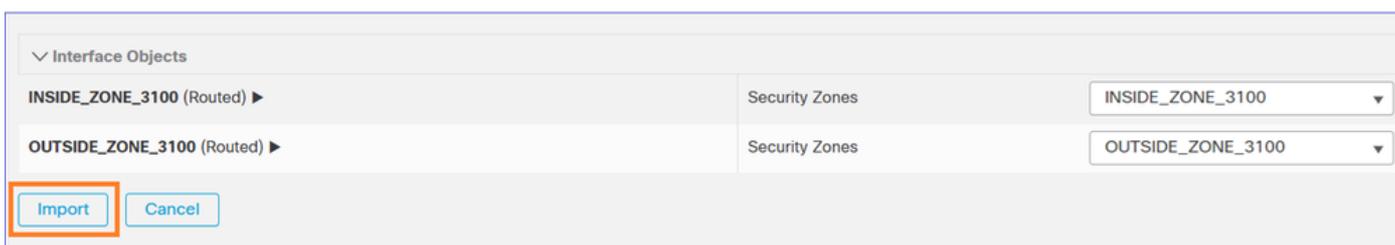
Créez les objets d'interface/zones de sécurité sur le FMC2 (FMC cible) :



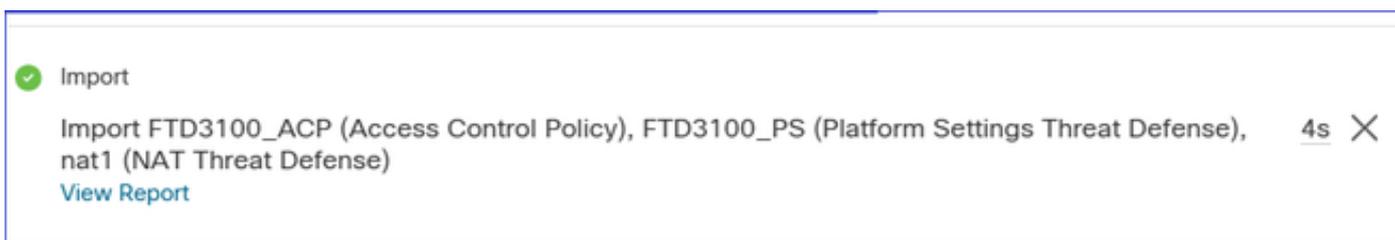
Vous pouvez donner les mêmes noms qu'ils avaient sur le FMC1 (source FMC) :



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>
```

```
>
```

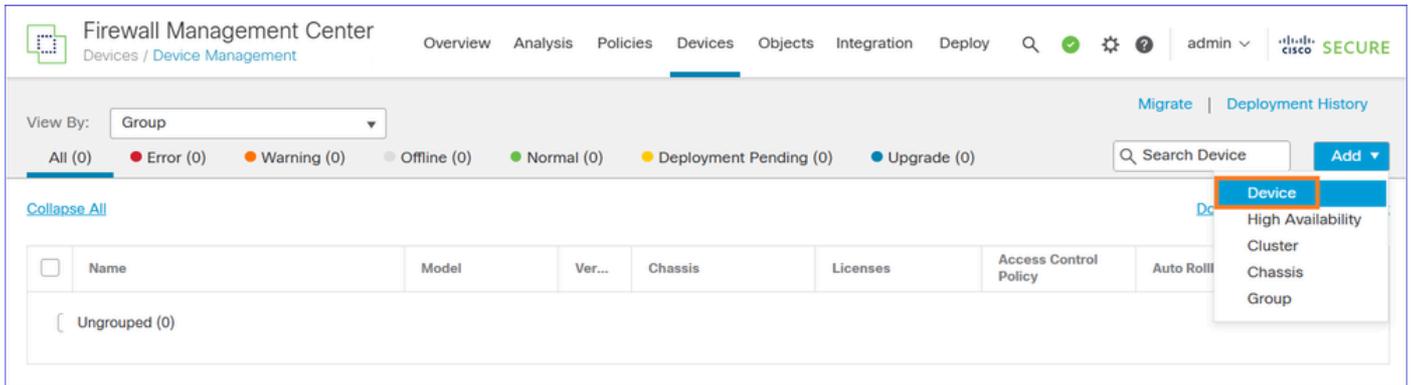
```
configure manager add 10.62.148.247 cisco
```

```
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 :

The screenshot shows the 'Add Device' configuration page. The 'Select the Provisioning Method:' section has 'Registration Key' selected with a radio button. Below it, 'CDO Managed Device' is unchecked. The 'Host:' field contains '10.62.184.84'. The 'Display Name:' field contains 'FTD1'. The 'Registration Key:*' field contains '****'. The 'Group:' dropdown menu is set to 'None'. The 'Access Control Policy:*' dropdown menu is set to 'FTD3100_ACP'. A question mark icon is visible in the top right corner of the form area.

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:†

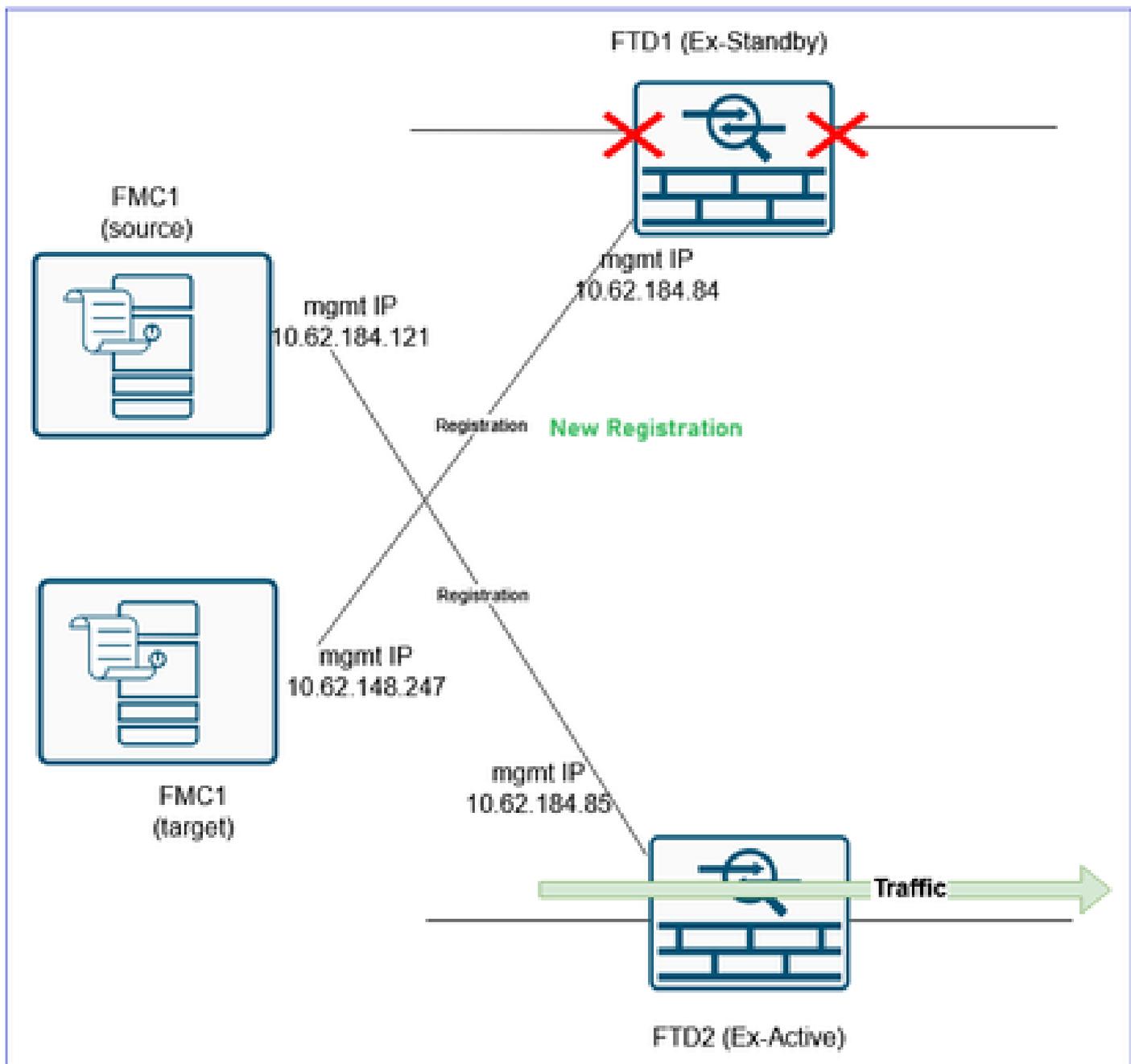
Transfer Packets

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 :

Firewall Management Center
Devices / Secure Firewall Device Summary

Overview Analysis Policies **Devices**

FTD1

Cisco Secure Firewall 3120 Threat Defense

Device Interfaces Inline Sets Routing DHCP VTEP

General

Name: FTD1

Transfer Packets: Yes

Troubleshoot: [Logs](#) [CLI](#) [Download](#)

Mode: Routed

Compliance Mode: None

Performance Profile: Default

TLS Crypto Acceleration: Enabled

Device Configuration: [Import](#) [Export](#) [Download](#)

OnBoarding Method: Registration Key

Licensing

Essential

Export-Only

Malware

IPS:

Carrier:

URL:

Secure

Secure

Secure

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

Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

[No](#) [Yes](#)

Une tâche FMC est lancée.



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

The screenshot shows the Firewall Management Center (FMC) interface for a Cisco Secure Firewall 3120 Threat Defense device (FTD1). The "Interfaces" tab is selected, showing a table of interfaces. The table has columns for Interface, Logical Name, Type, Security Zones, MAC Address (Active/Standby), IP Address, Path Monitoring, and Virtual Router. Two subinterfaces are highlighted with orange boxes: "Port-channel1.200" with logical name "INSIDE" and security zone "INSIDE_ZONE_3100", and "Port-channel1.201" with logical name "OUTSIDE" and security zone "OUTSIDE_ZONE_3100".

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Ethernet1/6		Physical				Disabled	
Ethernet1/7		Physical				Disabled	
Ethernet1/8		Physical				Disabled	
Ethernet1/9		Physical				Disabled	
Ethernet1/10		Physical				Disabled	
Ethernet1/11		Physical				Disabled	
Ethernet1/12		Physical				Disabled	
Ethernet1/13		Physical				Disabled	
Ethernet1/14		Physical				Disabled	
Ethernet1/15		Physical				Disabled	
Ethernet1/16		Physical				Disabled	
Port-channel1		EtherChannel				Disabled	
Port-channel1.200	INSIDE	Subinterface	INSIDE_ZONE_3100		10.0.200.70/24(Static)	Disabled	Global
Port-channel1.201	OUTSIDE	Subinterface	OUTSIDE_ZONE_3100		10.0.201.70/24(Static)	Disabled	Global

⚠ 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 :

The screenshot shows the Firewall Management Center interface. The breadcrumb is 'Devices / Platform Settings'. The 'Devices' tab is active. A table lists platform settings for device 'FTD3100_PS'. The 'Device Type' is 'Threat Defense' and the 'Status' is 'Targeting 1 devices' with a sub-note 'Out-of-date on 1 targeted devices'. There are icons for edit, delete, and refresh.

Platform Settings	Device Type	Status	
FTD3100_PS	Threat Defense	Targeting 1 devices Out-of-date on 1 targeted devices	

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

The screenshot shows the Firewall Management Center interface. The breadcrumb is 'Devices / NAT'. The 'Devices' tab is active. A table lists NAT policies for device 'nat1'. The 'Device Type' is 'Threat Defense' and the 'Status' is 'Targeting 1 devices' with a sub-note 'Out-of-date on 1 targeted devices'. There are icons for edit, delete, and refresh.

NAT Policy	Device Type	Status	
nat1	Threat Defense	Targeting 1 devices Out-of-date on 1 targeted devices	

Les zones de sécurité sont appliquées aux interfaces :

The screenshot shows the Firewall Management Center interface for device 'FTD1'. The breadcrumb is 'Devices / Secure Firewall Interfaces'. The 'Interfaces' tab is active. A table lists interfaces and their security zones. The 'Security Zones' column is highlighted with an orange box. The zones are 'INSIDE_ZONE_3100' for 'Port-channel1.200' and 'OUTSIDE_ZONE_3100' for 'Port-channel1.201'. There are icons for edit, delete, and refresh.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Ethernet1/5		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/6		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/7		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/8		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/9		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/10		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/11		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/12		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/13		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/14		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/15		Physical				Disabled		
<input checked="" type="checkbox"/> Ethernet1/16		Physical				Disabled		
Port-channel1		EtherChannel				Disabled		
<input checked="" type="checkbox"/> Port-channel1.200	INSIDE	Subinterface	INSIDE_ZONE_3100		10.0.200.70/24(Static)	Disabled	Global	
<input checked="" type="checkbox"/> Port-channel1.201	OUTSIDE	Subinterface	OUTSIDE_ZONE_3100		10.0.201.70/24(Static)	Disabled	Global	

La configuration du routage est appliquée au périphérique FTD :

The screenshot shows the Firewall Management Center interface for device FTD1. The 'Routing' tab is selected, and the 'Static Route' configuration page is displayed. A table lists the configured routes:

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	OUTSIDE	Global	10.0.201.60	false	1	
▼ IPv6 Routes						

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

The screenshot shows the 'Create New VPN Topology' dialog box. The configuration is as follows:

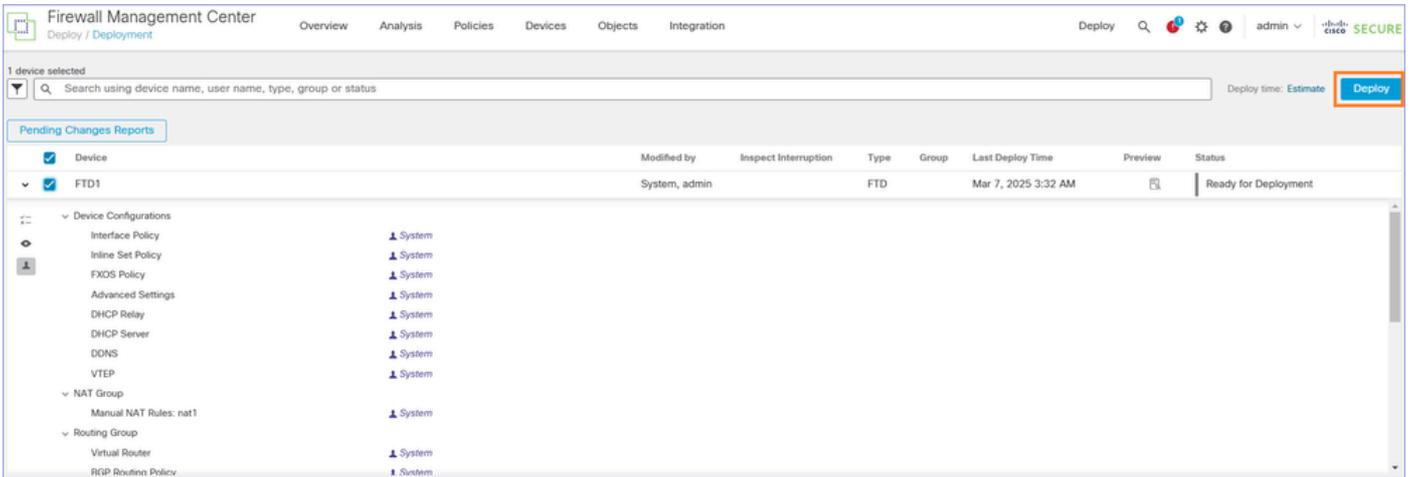
- Topology Name: VPN3100
- Policy Based (Crypto Map) is selected.
- Network Topology: Point to Point is selected.
- IKE Version: IKEv2 is selected.
- Endpoints tab is active.
- Node A: Device FTD1, VPN Interface OUTSIDE (10.0.201.70), Protected Networks net_10.0.200.0.
- Node B: Device Extranet Remote_FW, VPN Interface 10.0.201.60, Protected Networks net_10.0.202.0.

A note at the bottom states: "Ensure the protected networks are allowed by access control policy of each device."

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 :



The screenshot displays the Firewall Management Center (FMC) interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and Integration. A search bar is present with the text "Search using device name, user name, type, group or status". A "Deploy" button is highlighted in orange. Below the search bar, there is a section for "Pending Changes Reports" with a table of pending changes. The table has columns for Device, Modified by, Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status. The first row shows FTD1, modified by System, admin, with a status of "Ready for Deployment". Below the table, there is a tree view of configurations for FTD1, including Interface Policy, Inline Set Policy, FXOS Policy, Advanced Settings, DHCP Relay, DHCP Server, DNS, VTEP, NAT Group, Manual NAT Rules: nat1, Routing Group, Virtual Router, and RGP Routem Policy.

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.

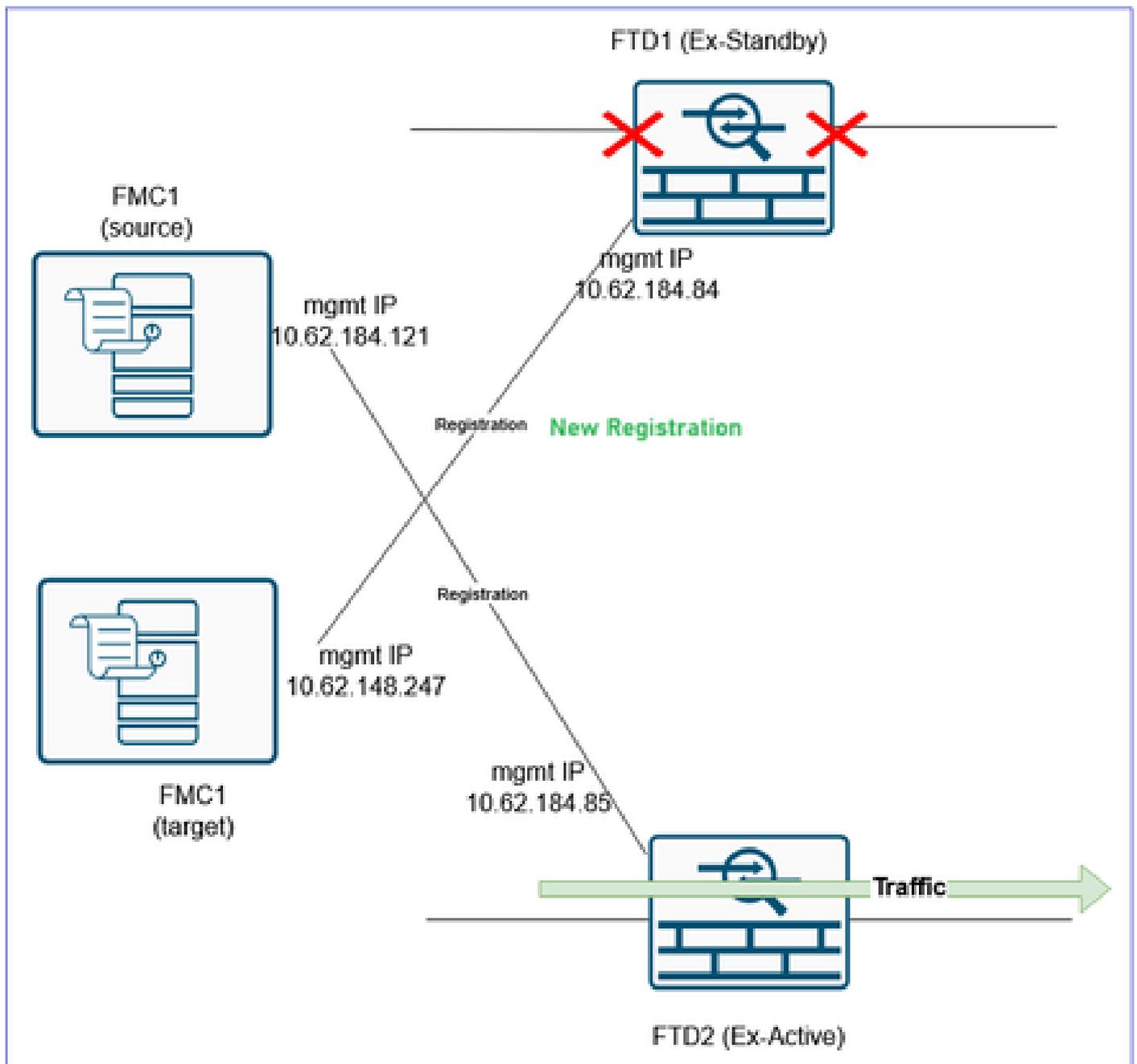
Les différences que vous voyez et qui sont normales sont les suivantes :

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

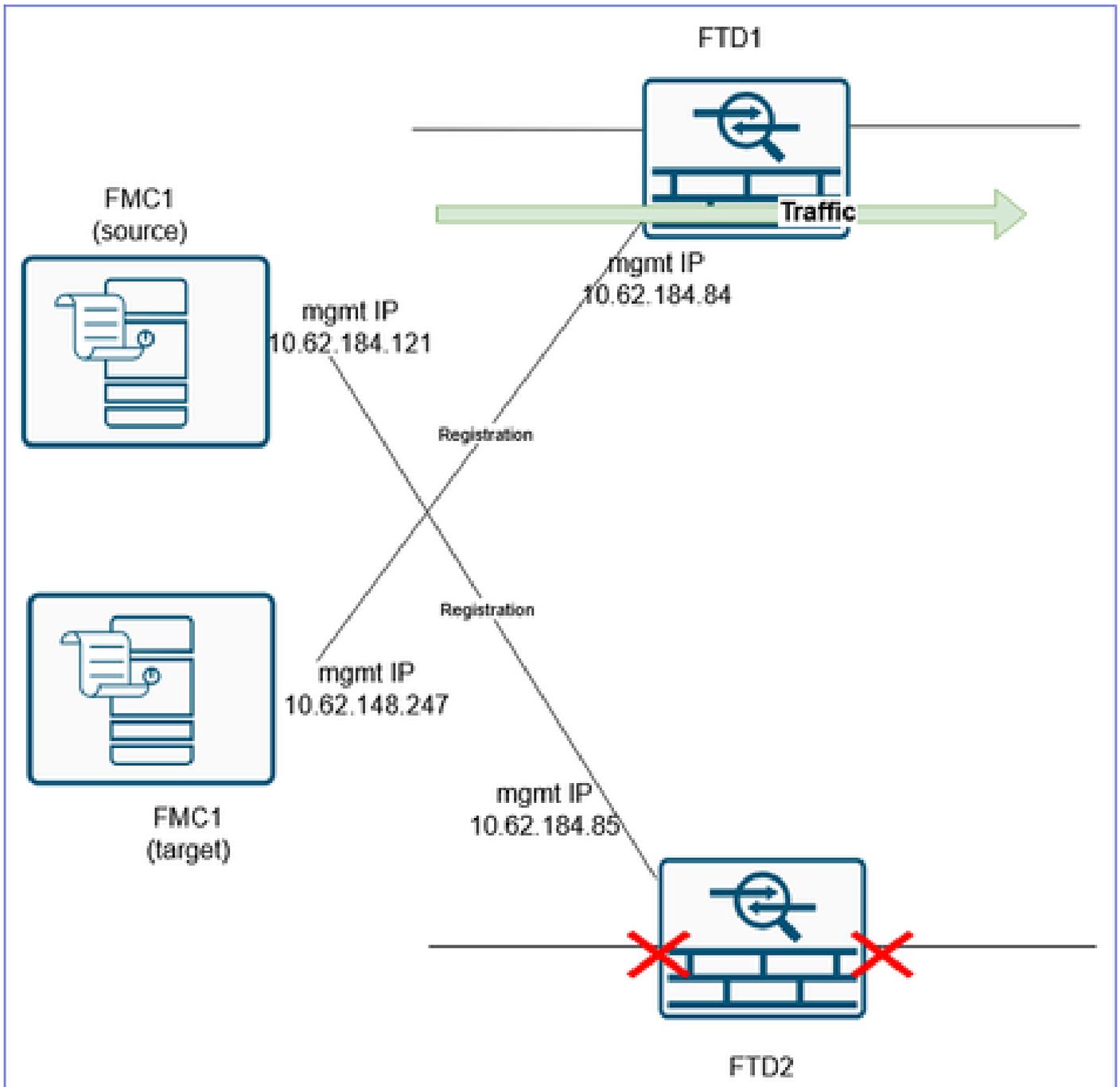
Étape 12. Effectuez le basculement

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 :



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 ipaddrut1 5 10.0.200.70
```

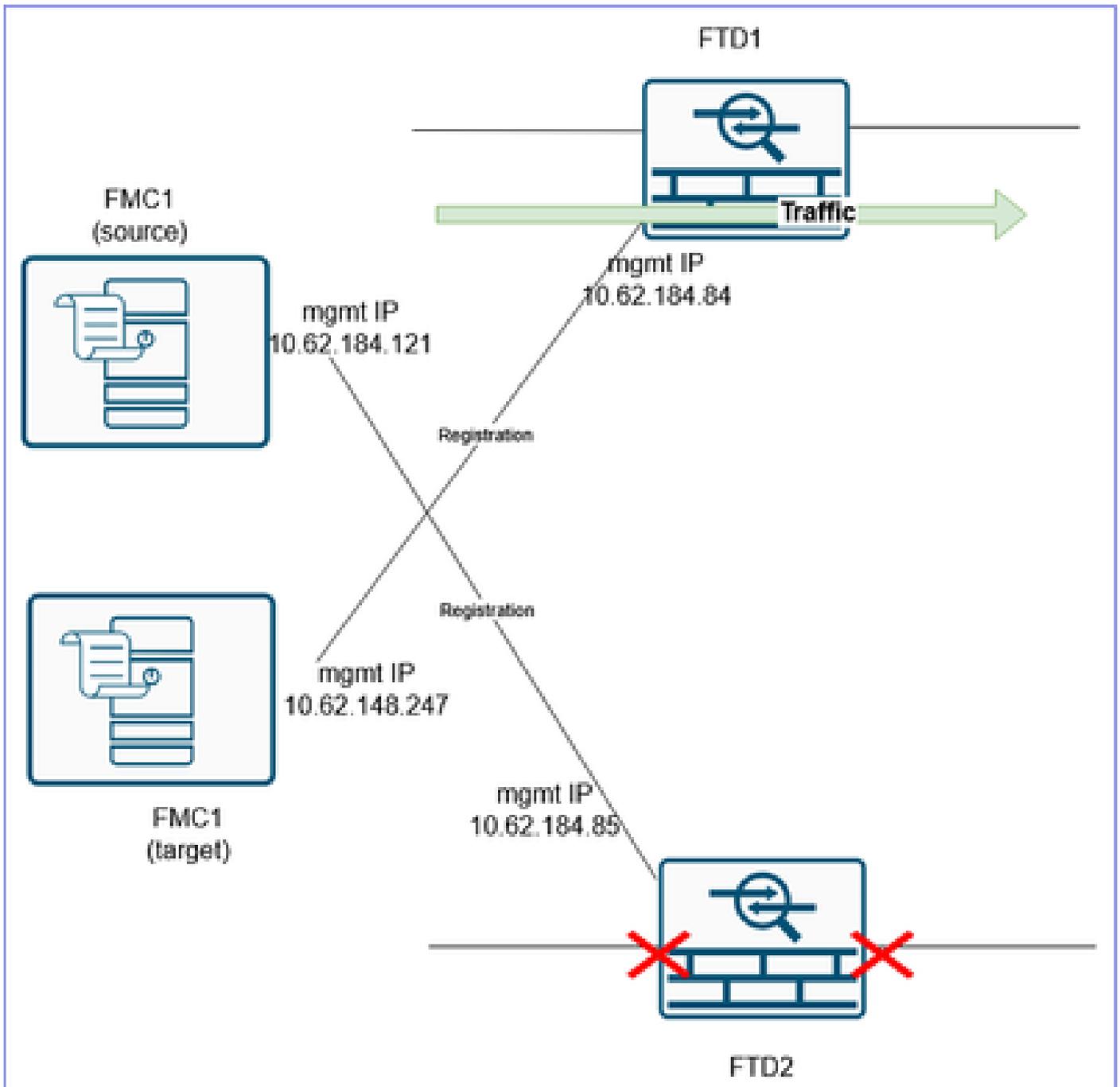
```
Gratuitous ARP sent for 10.0.200.70
```

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.

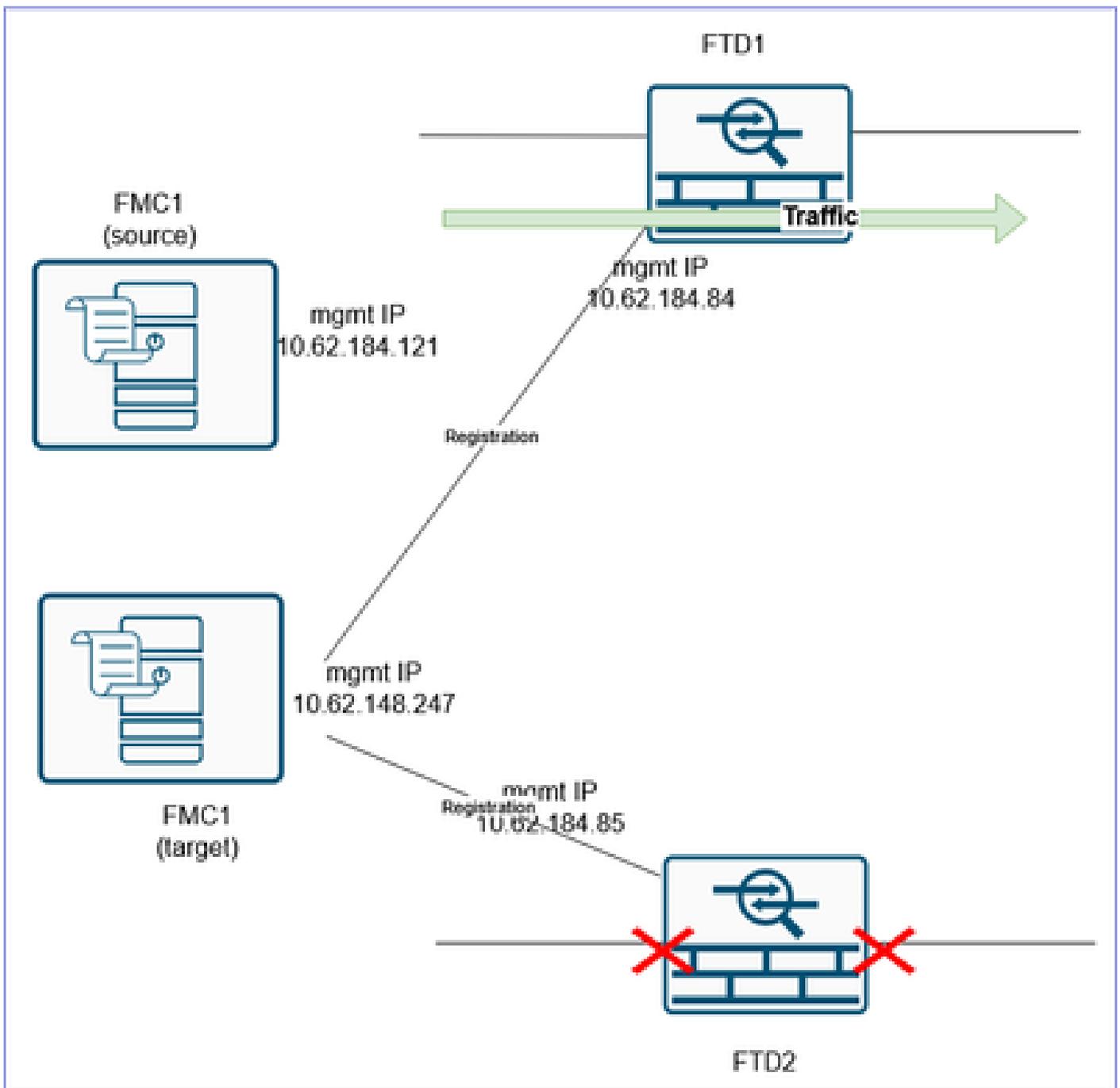
Étape 13. Migration du deuxième FTD vers FMC2 (FMC cible)

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 :



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 :

Error

The Device 'FTD2' cannot be deleted because the following VPN Configuration(s) refer this device.

Site to Site : VPN3100

Please edit/remove the VPN configuration(s) to delete the device.

OK

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.
```

```
>
```

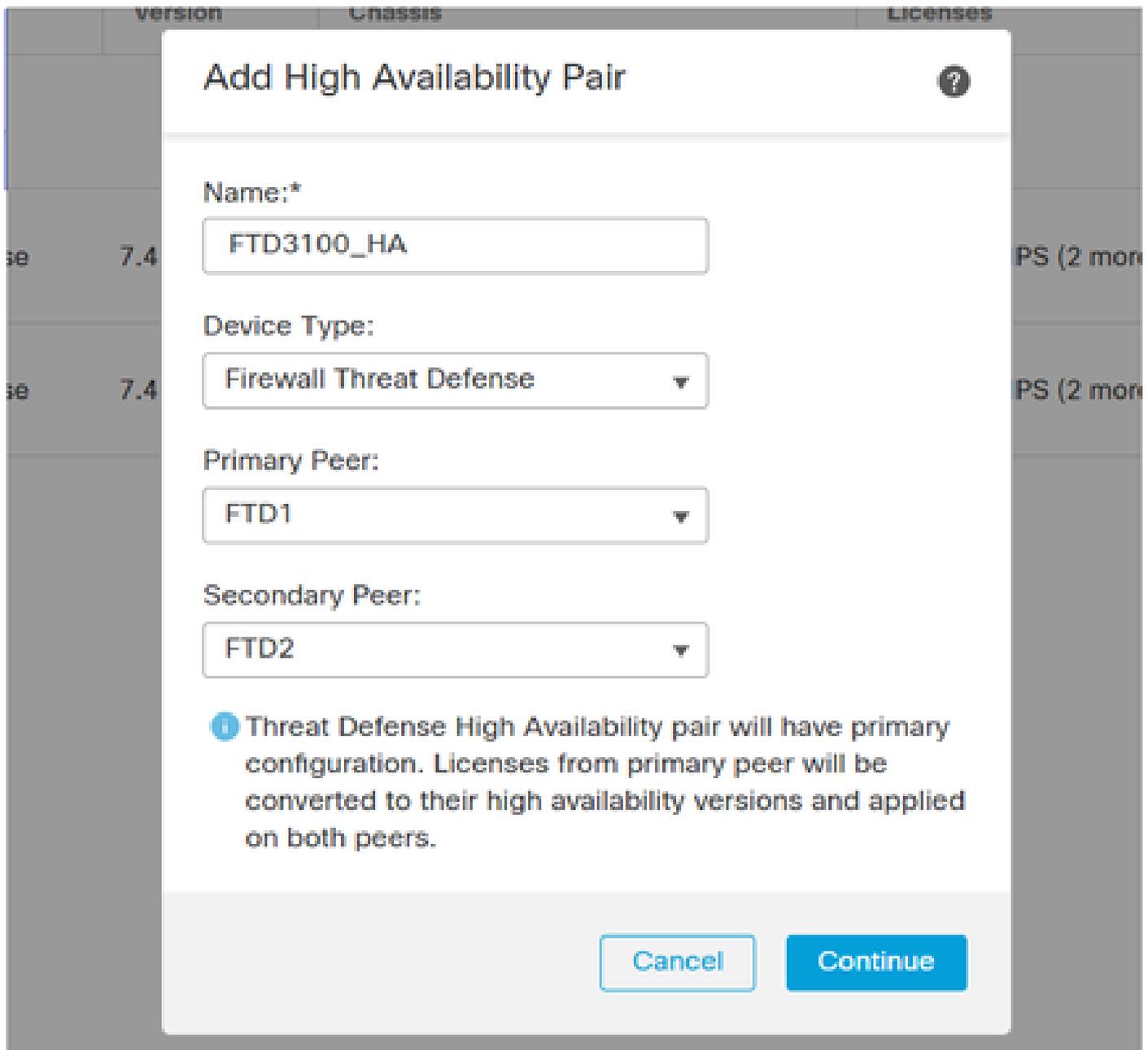
Le résultat :

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>
```

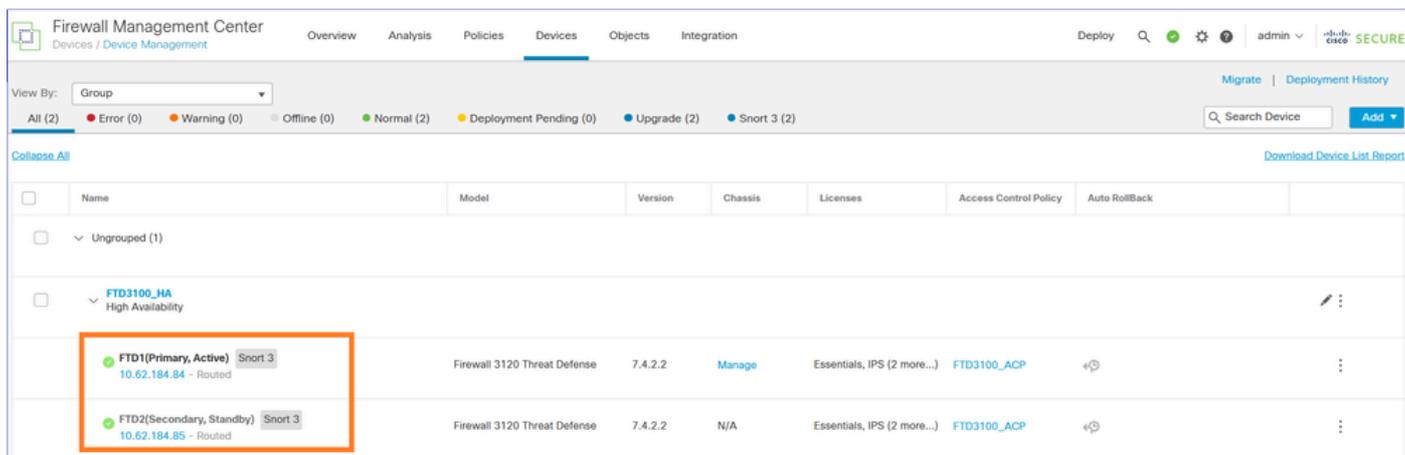
```
FTD3100-3#
```

```
show failover | include host
```

```
This host: Secondary - Standby Ready
```

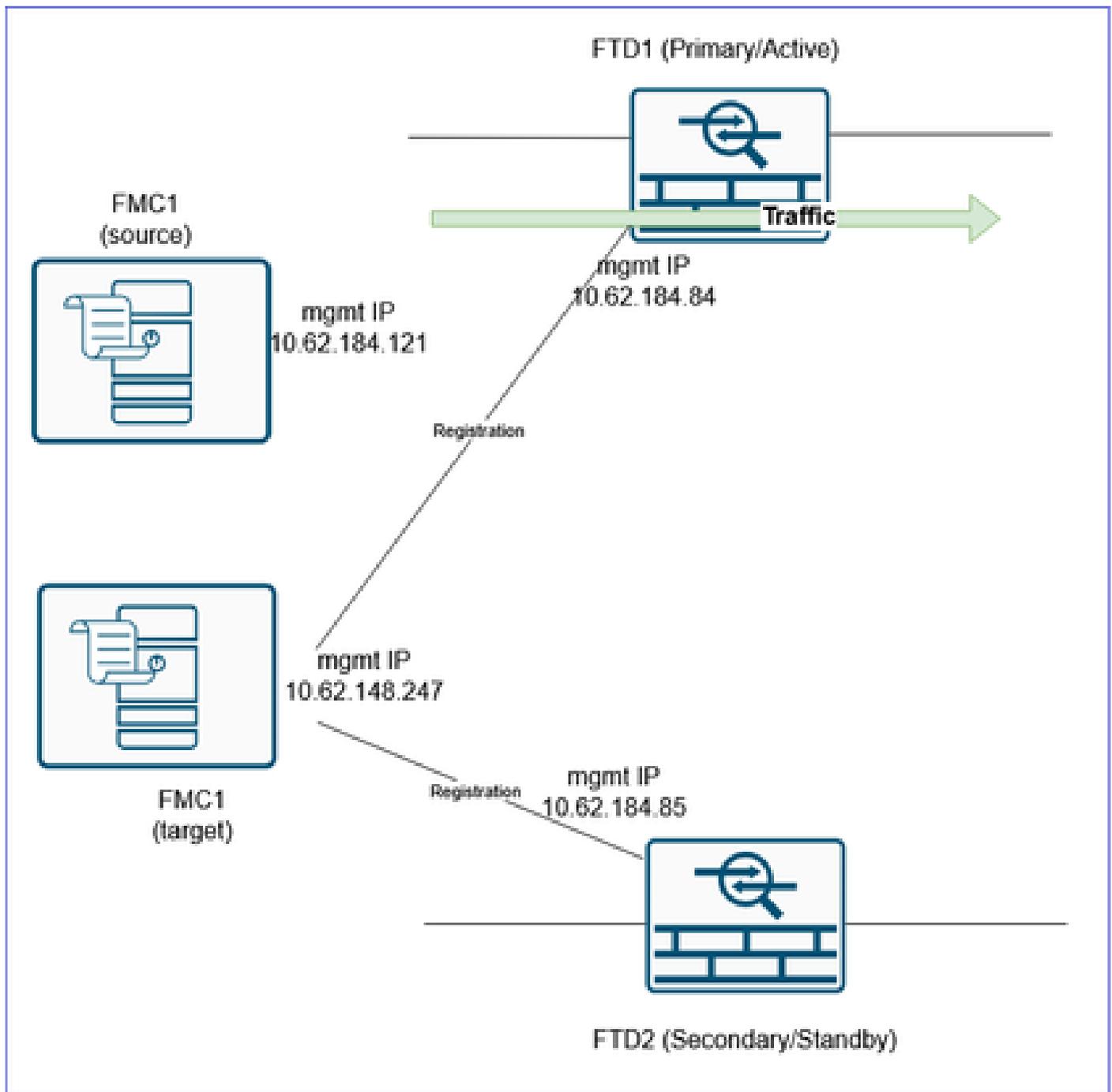
```
Other host: Primary - Active
```

Vérification de l'interface FMC :



	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
<input type="checkbox"/>	Ungrouped (1)						
<input type="checkbox"/>	FTD3100_HA High Availability						
<input type="checkbox"/>	FTD1(Primary, Active) Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	↺
<input type="checkbox"/>	FTD2(Secondary, Standby) Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	↺

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.