將FTD HA（容錯移轉）遷移到另一個FMC

目錄

簡介

本檔案介紹將FTD HA從現有FMC移轉至其他FMC的程式。

有關獨立防火牆遷移至新FMC的資訊，請檢視 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

縮寫

ACP =訪問控制策略

ARP =地址解析協定

CLI =命令列介面

FMC =安全防火牆管理中心

FTD =安全防火牆威脅防禦

GARP =免費ARP

HA =高可用性

MW =維護視窗

UI =使用者介面

必要條件

開始遷移過程之前，請確保滿足以下前提條件：

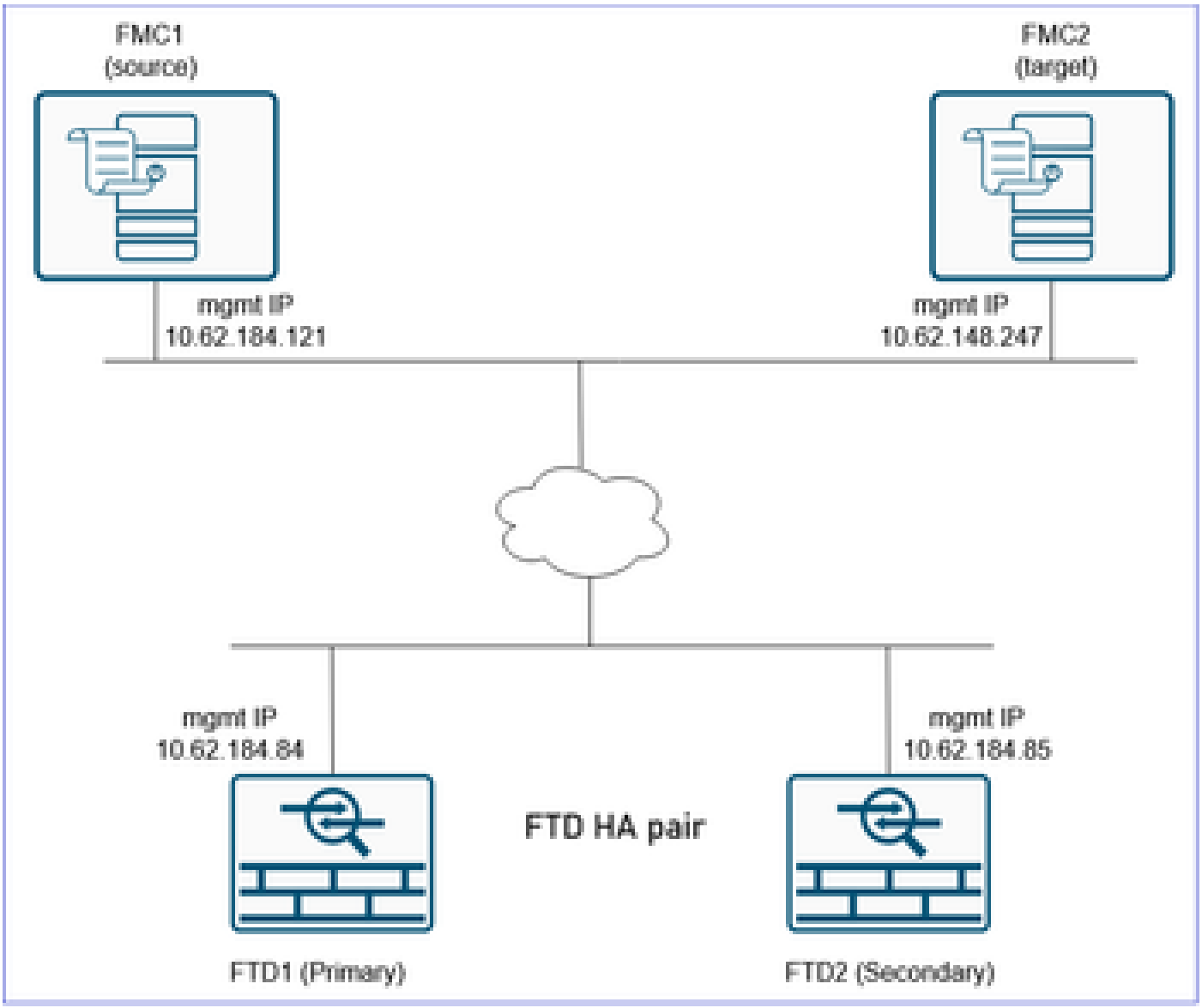
- 對源和目標FMC的UI和CLI訪問。
- FMC和防火牆的管理憑證。
- 通過控制檯訪問兩個防火牆。
- 訪問第3層上游和下游裝置（如果您需要清除ARP快取）。
- 確保目標/目標FMC的版本與源/舊FMC的版本相同。
- 確保目標/目標FMC與源/舊FMC具有相同的許可證。
- 確保您安排MW來執行遷移，因為這將影響中轉流量。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆31xx，FTD版本7.4.2.2。
- 安全防火牆管理中心版本7.4.2.2。
- 本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

拓撲



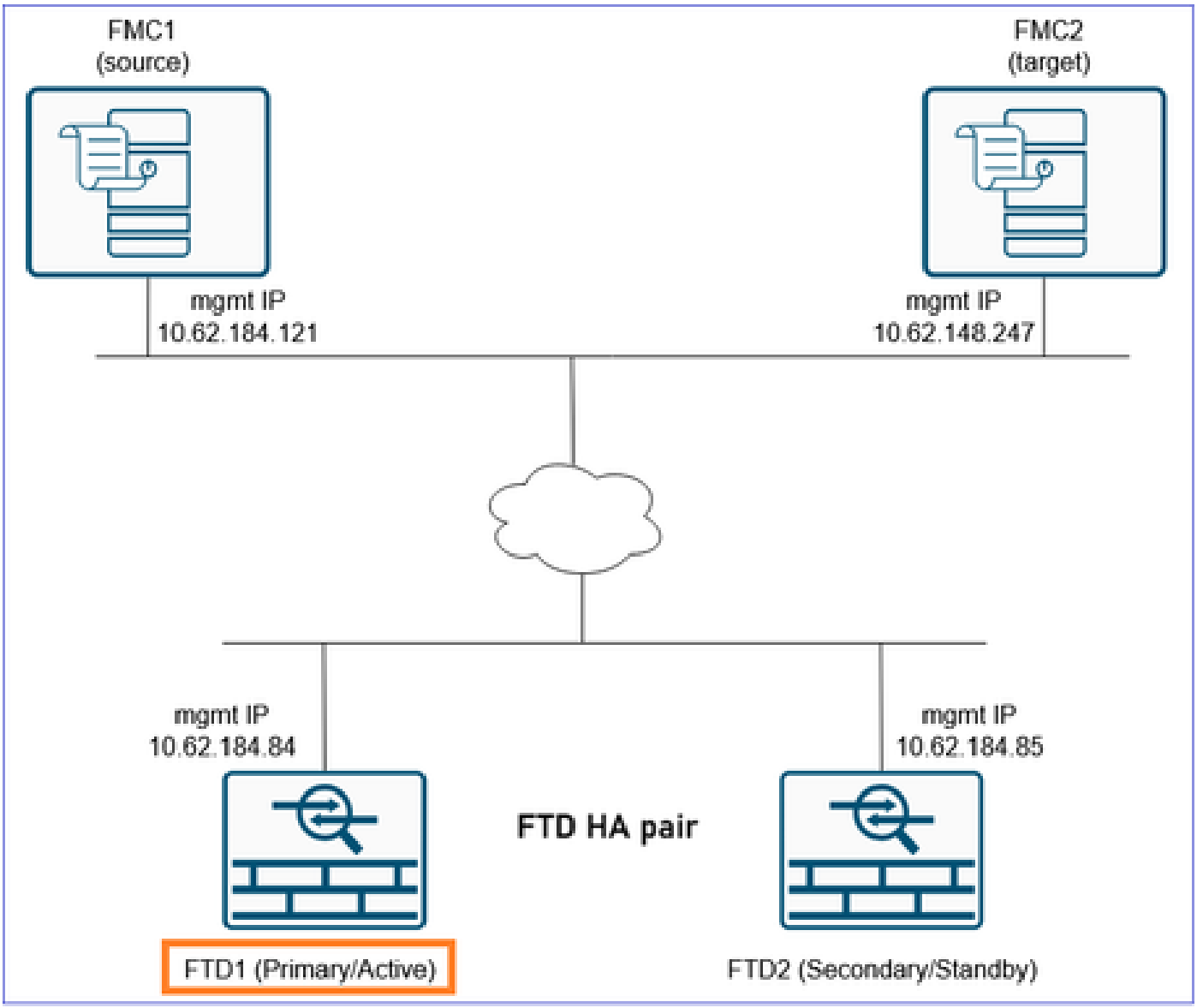
設定

遷移步驟

在此案例中，我們將考慮以下狀態：

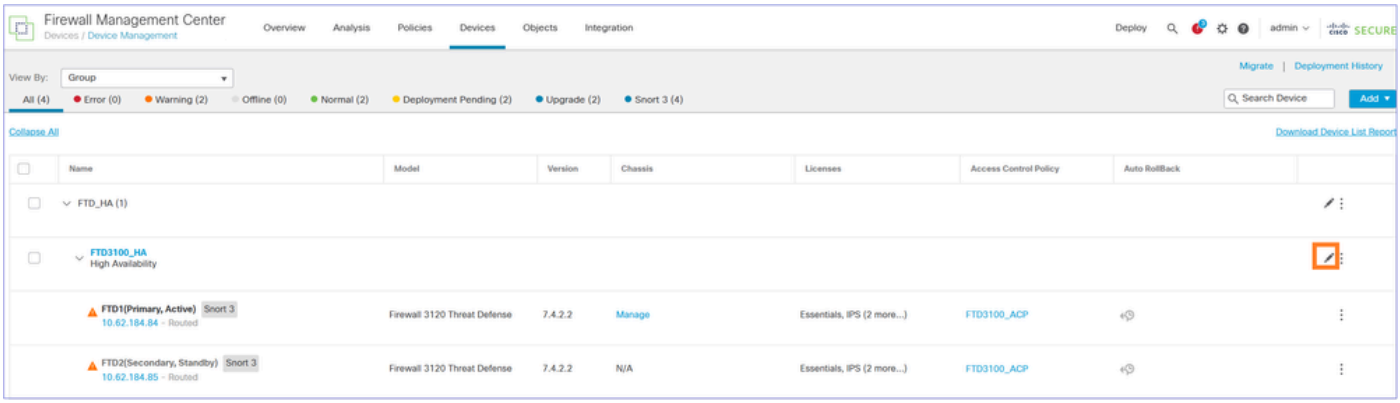
FTD1:主要/活動

FTD2:輔助/備用

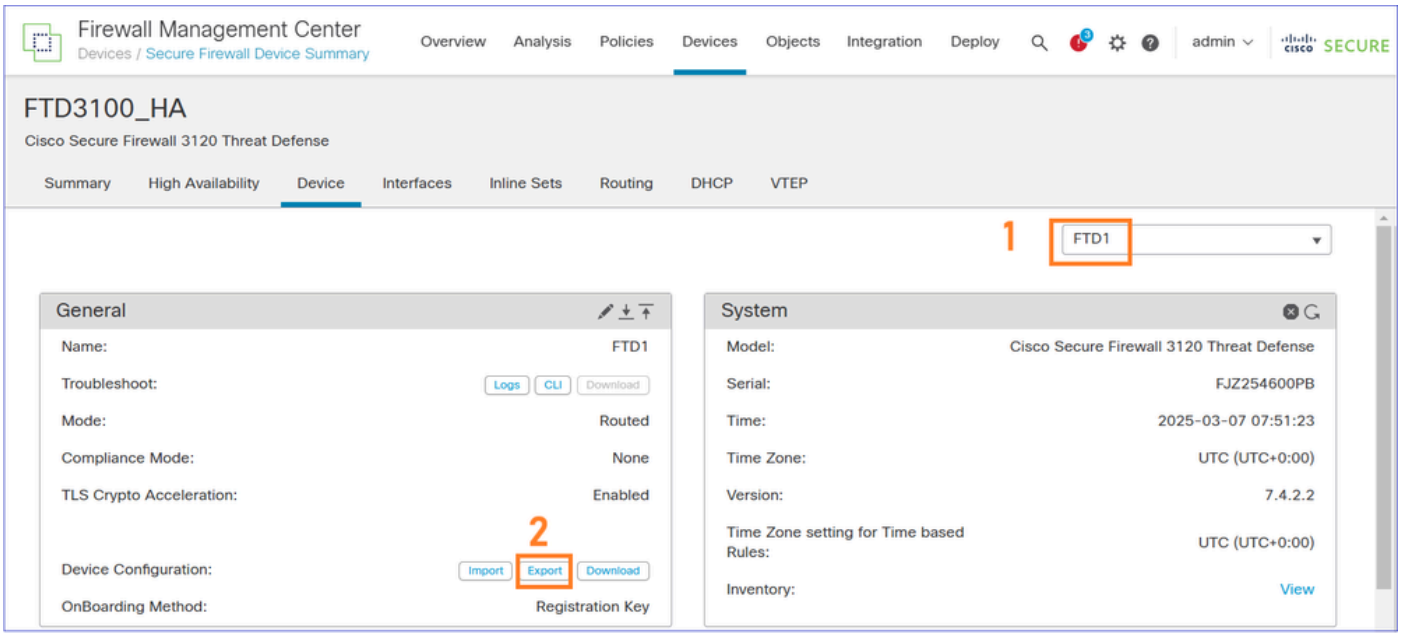


步驟1.從主防火牆匯出裝置配置

在FMC1（源FMC）上，導航至Devices > Device Management。選擇FTD HA配對，然後選擇Edit:

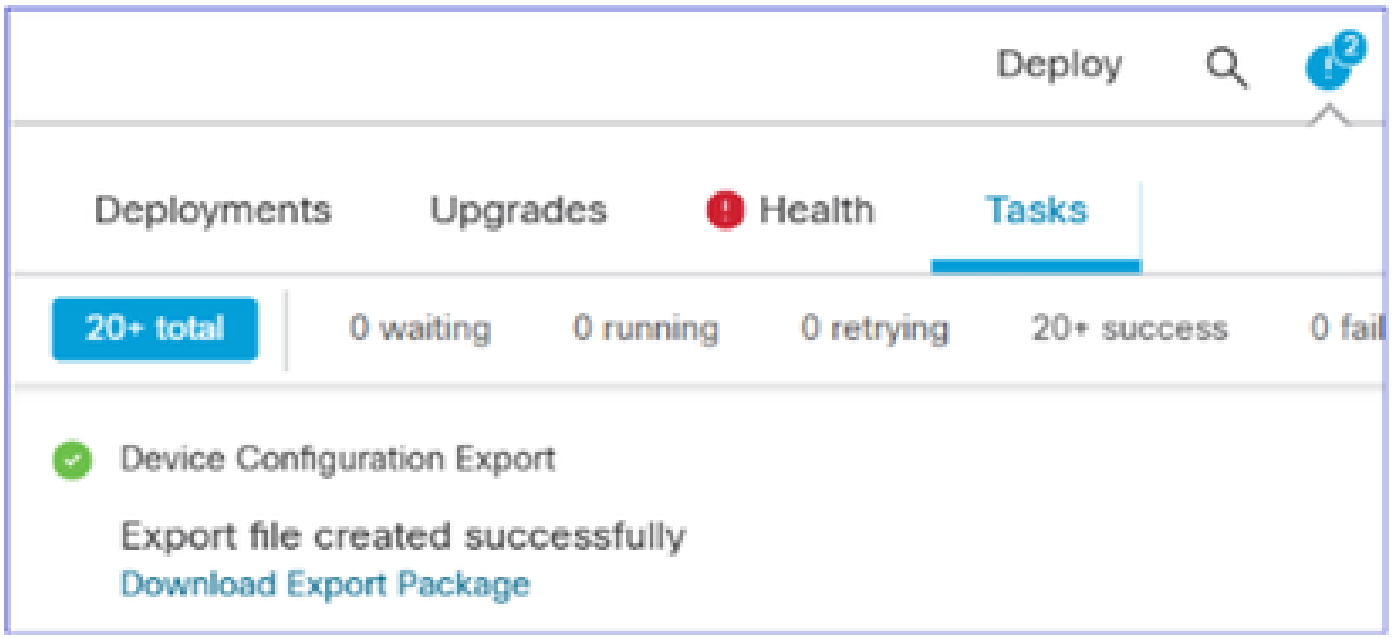


導覽至Device索引標籤。確保已選擇主/主用FTD（本例中為FTD1），然後選擇Export以匯出裝置配置：



附註：Export選項自7.1軟體版本及更高版本起可用。

您可以定位至通知>任務頁，以確保匯出已完成。然後，選擇Download Export Package:



或者，也可以按一下General區域中的Download按鈕。您將獲得sfo檔案，例如DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

檔案包含與裝置相關的配置，例如：

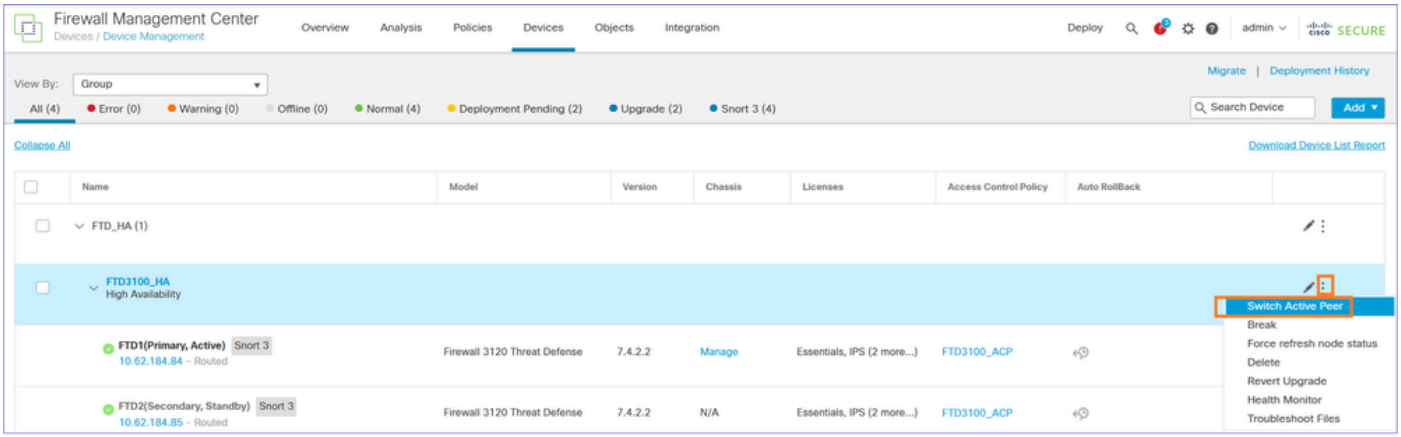
- 路由介面
- 內嵌集
- 路由
- DHCP
- VTEP
- 關聯對象

附註：匯出的配置檔案只能匯入回同一個FTD。FTD的UUID必須與匯入的sfo檔案的內容相符。可在另一個FMC上註冊相同的FTD，並可匯入sfo檔案。

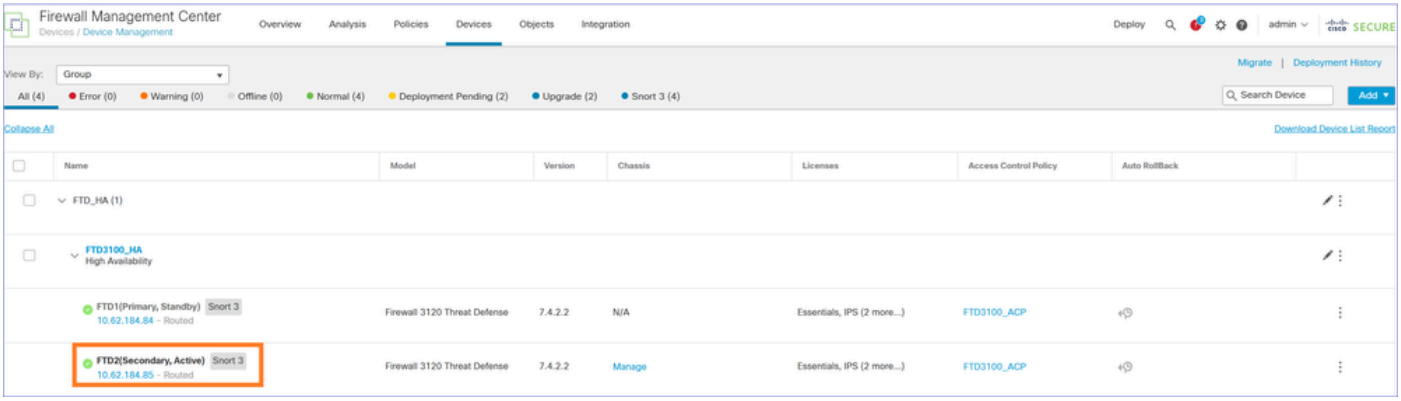
參考資料：'匯出和匯入裝置配置' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

步驟2.使次要FTD處於使用中狀態

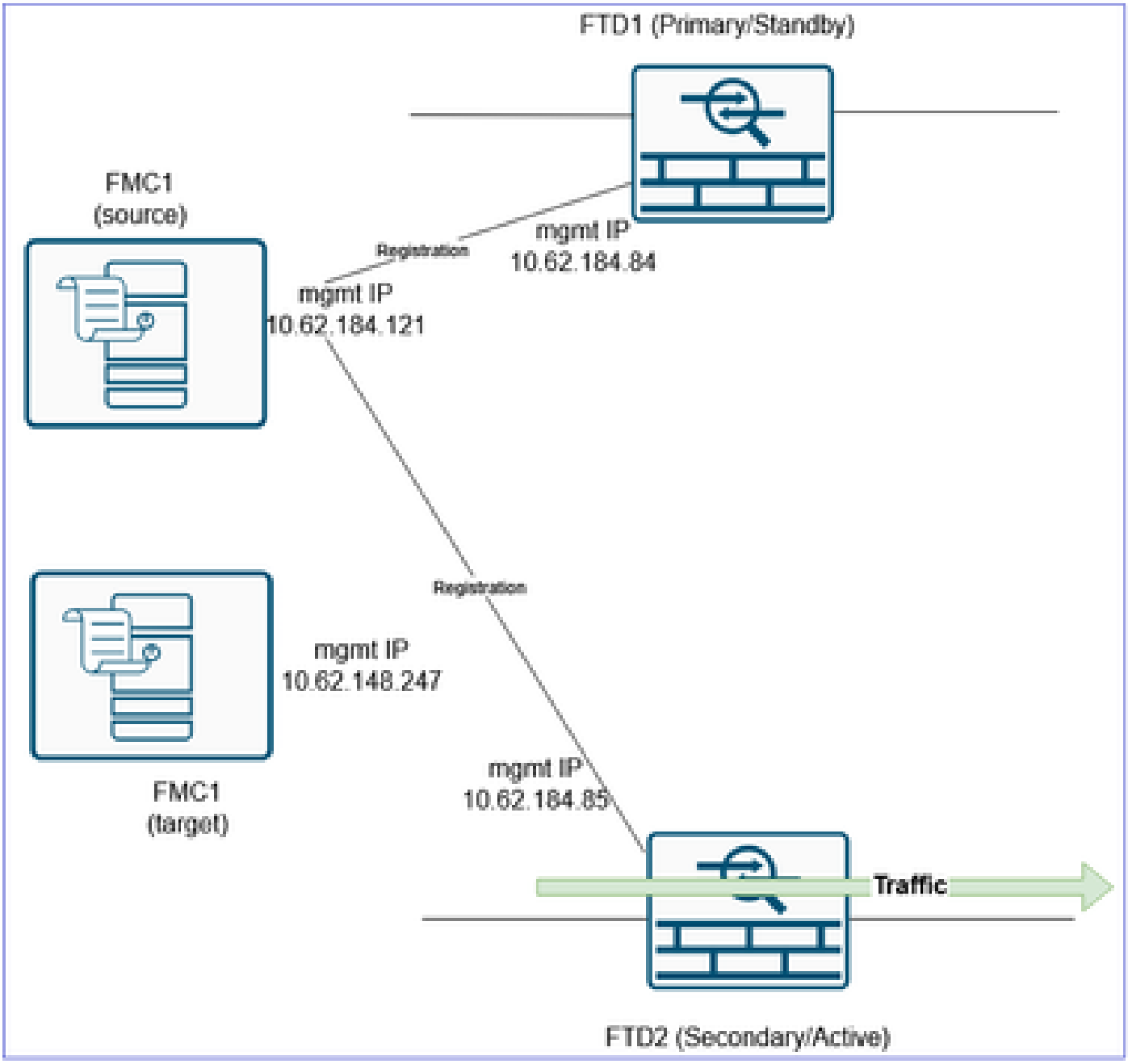
導覽至Devices > Device Management，選擇FTD HA配對，然後選擇Switch Active Pair:



結果為FTD1（主/備用）和FTD（輔助/主用）：

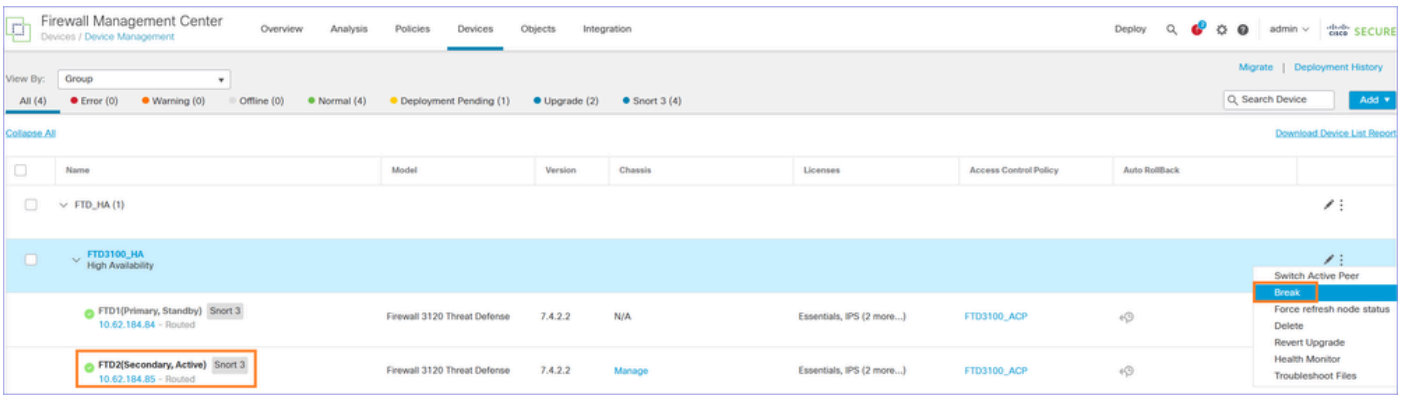


現在，流量已由輔助/主用FTD處理：

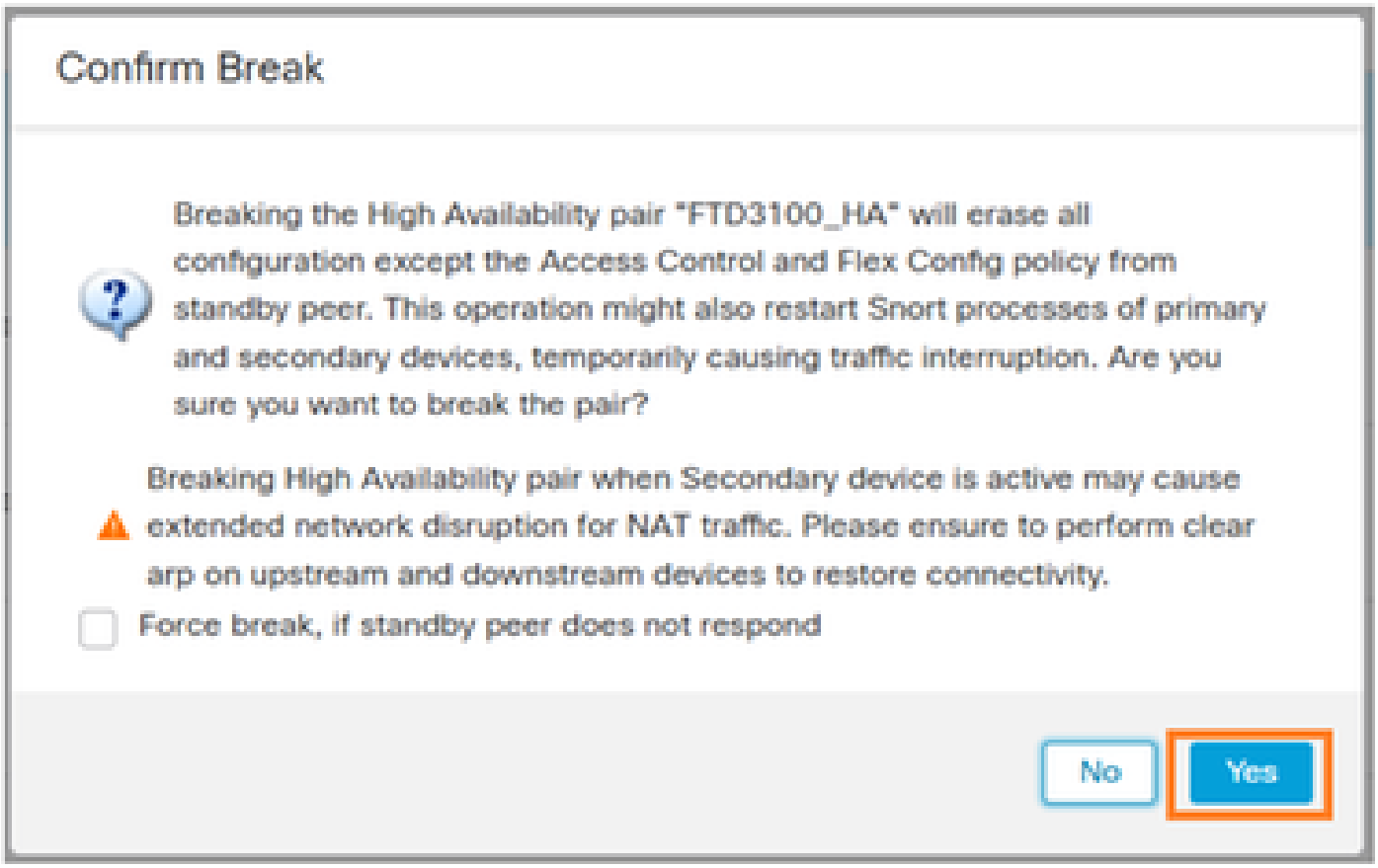


步驟3.中斷FTD HA

導覽至Devices > Device Management，然後Break FTD HA:



出現此視窗。選擇是



附註：此時您可能會遇到數秒內的流量中斷，因為Snort引擎在HA中斷期間重新啟動。此外，如消息所述，如果使用NAT並遇到長時間流量中斷，請考慮清除上游和下游裝置上的ARP快取。

中斷FTD HA後，FMC上有兩個獨立的FTD。

從配置角度來看，FTD2（非主用）仍舊有配置（與故障切換相關的配置除外），並且正在處理流量：

```
<#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
```

FTD1（非待命）已移除所有組態：

<#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#

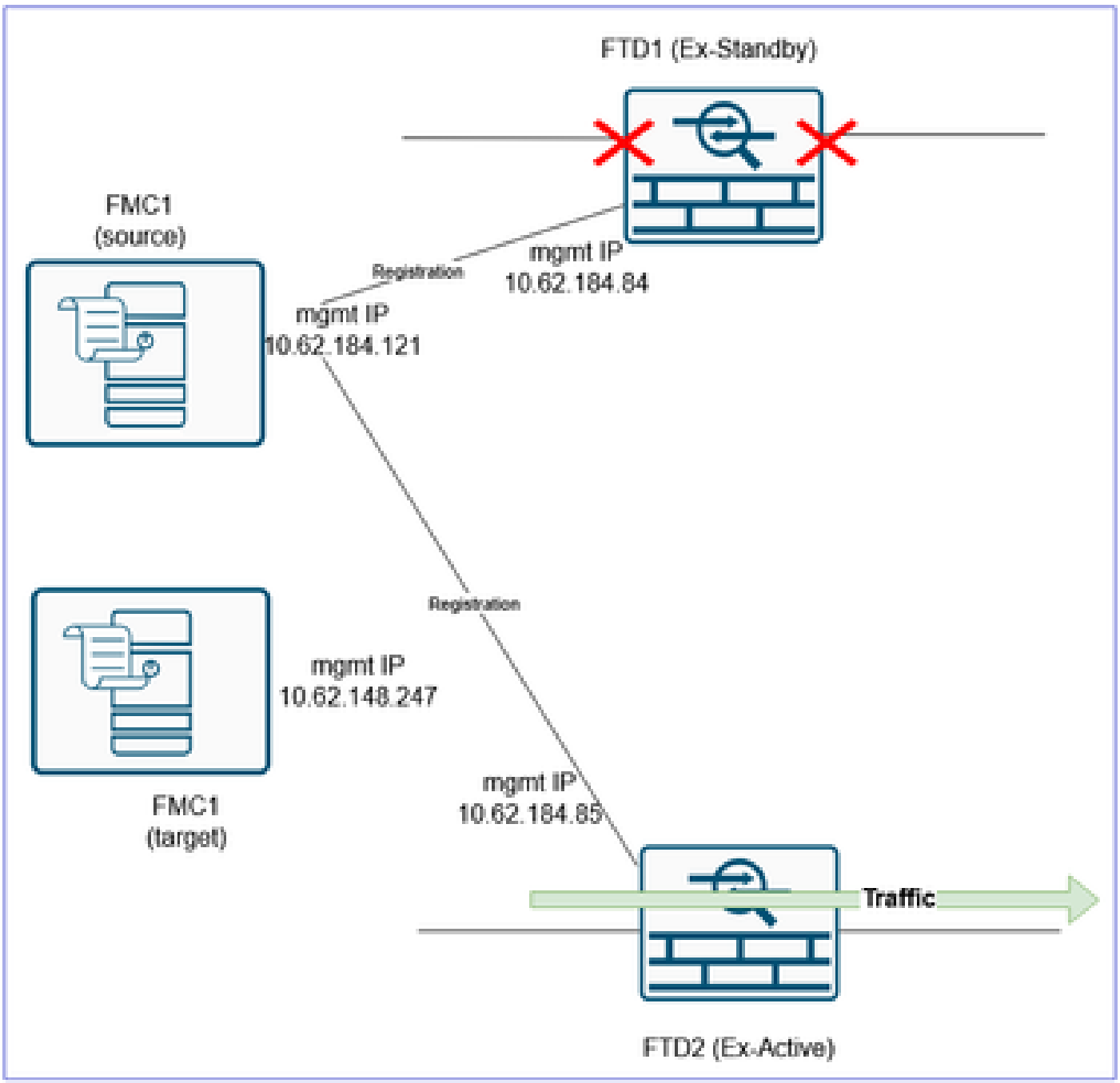
show interface ip brief

```
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
```

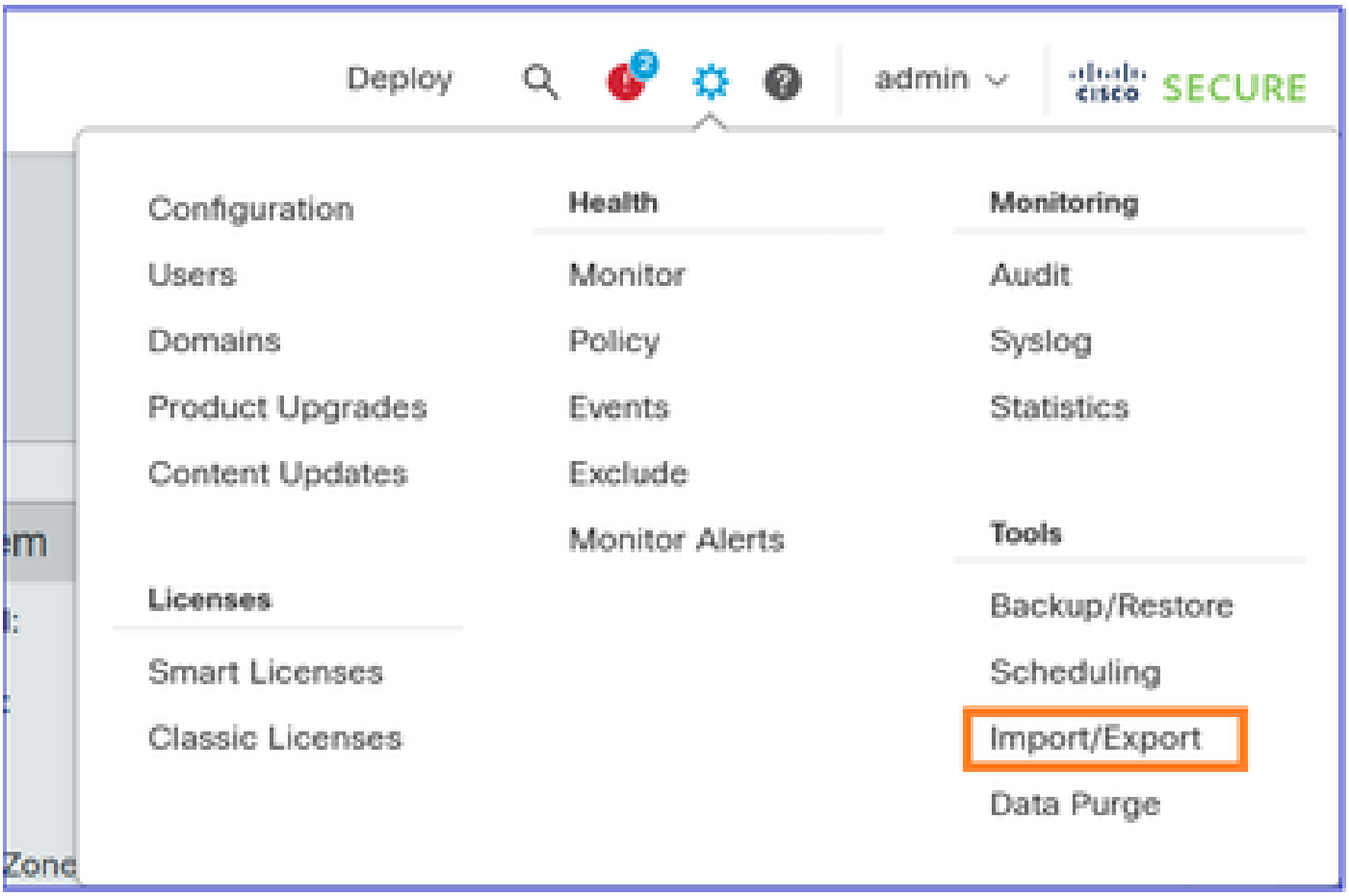
步驟4.隔離FTD1（非主要）資料介面

從FTD1(非主要)拔下資料線。 僅使FTD管理連線埠保持連線狀態。



步驟5.匯出FTD共用原則

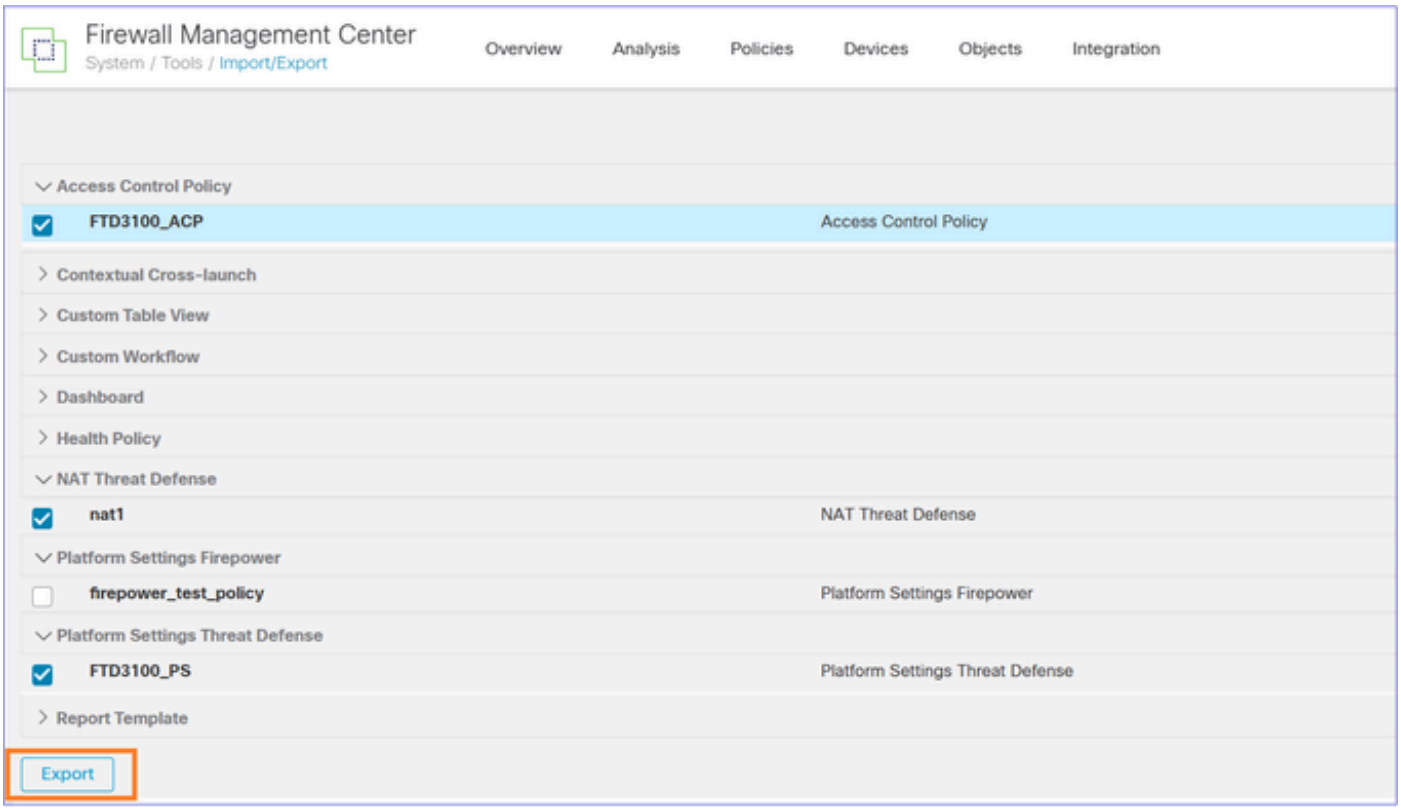
導覽至System > Tools，然後選擇Import/Export:



匯出連線到裝置的各種策略。確保匯出附加至FTD的所有原則，例如：

- 存取控制原則(ACP)
- 網路位址轉譯(NAT)原則
- 運行狀況策略（如果自定義）
- FTD平台設定

等等。



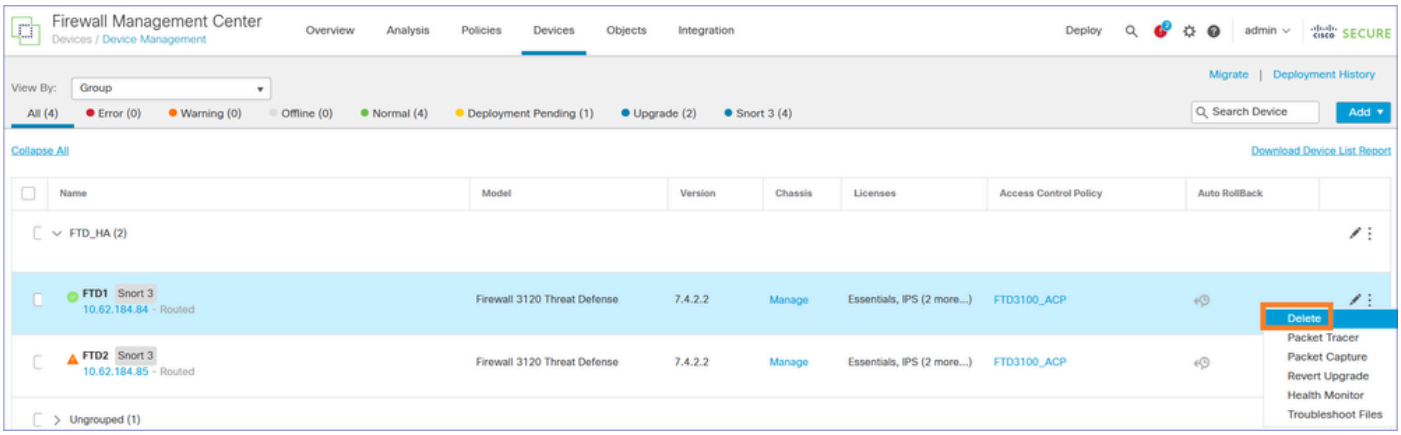
附註：在撰寫本文時，不支援匯出VPN相關的配置。裝置註冊後，您需要在FMC2（目標FMC）上手動重新配置VPN。

相關增強功能Cisco錯誤ID CSCwf05294

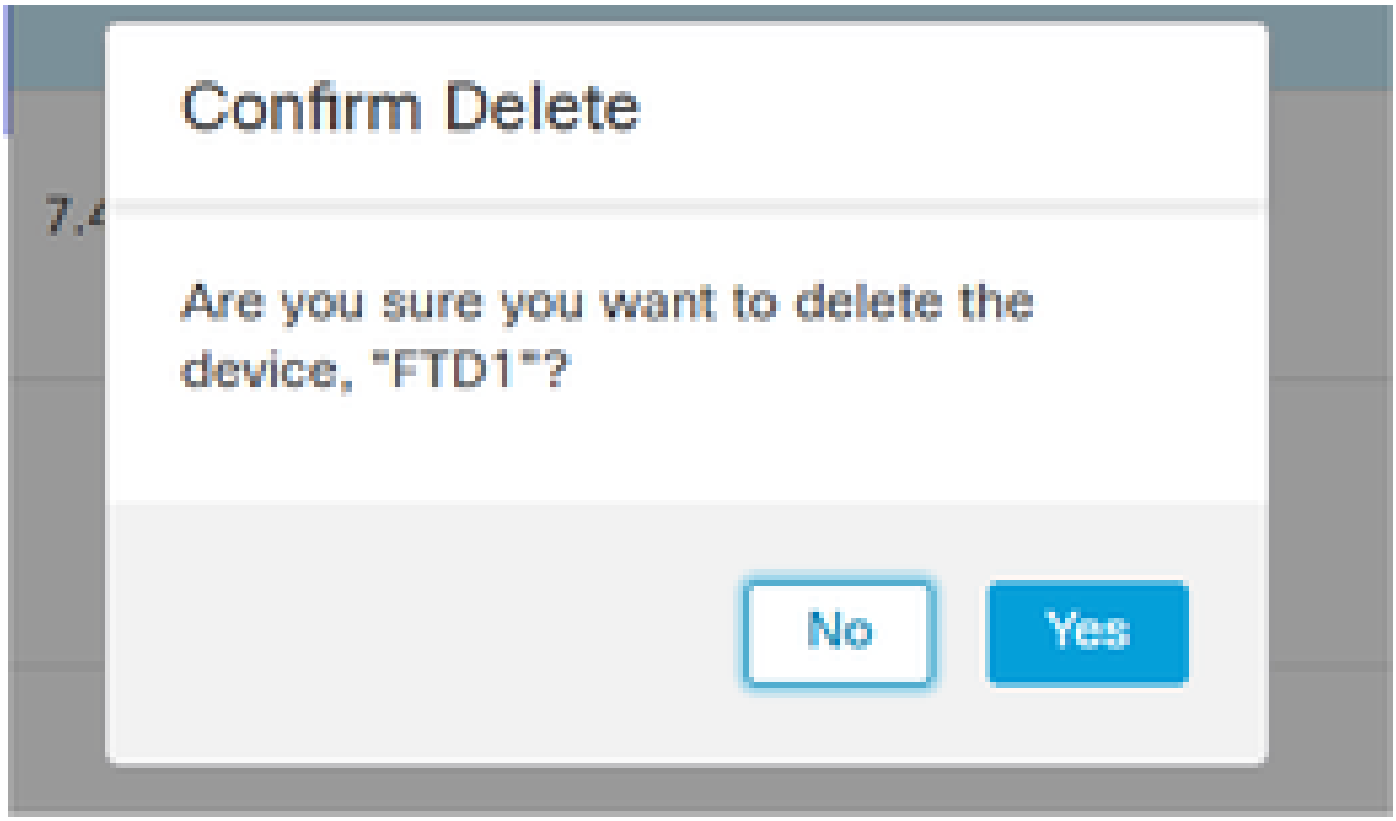
.

結果是一個.sfo檔案，例如ObjectExport_20250306082738.sfo

步驟6.從舊/來源FMC中刪除/註銷FTD1（非主要）



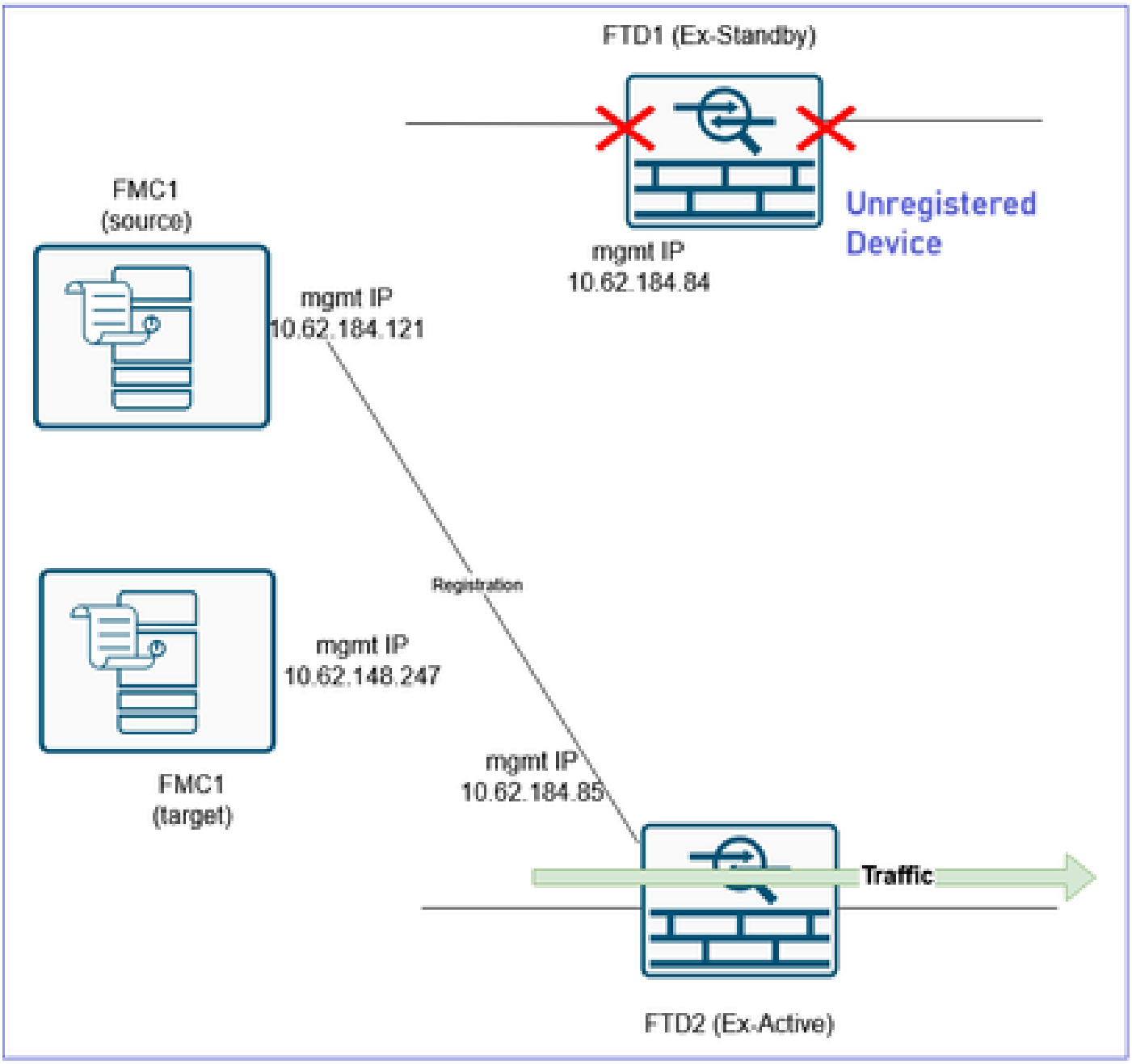
確認裝置刪除：



FTD1 CLI驗證：

```
<#root>

>

show managers

No managers configured.

>
```

FTD1裝置刪除後的目前狀態：



步驟7.將FTD原則組態物件匯入FMC2（目標FMC）

附註：本檔案將重點介紹將單個FTD HA配對移轉至新FMC的過程。另一方面，如果您計畫遷移共用相同策略（例如ACP、NAT）和對象的多個防火牆，並且希望分階段進行遷移，則需要考慮這些點。

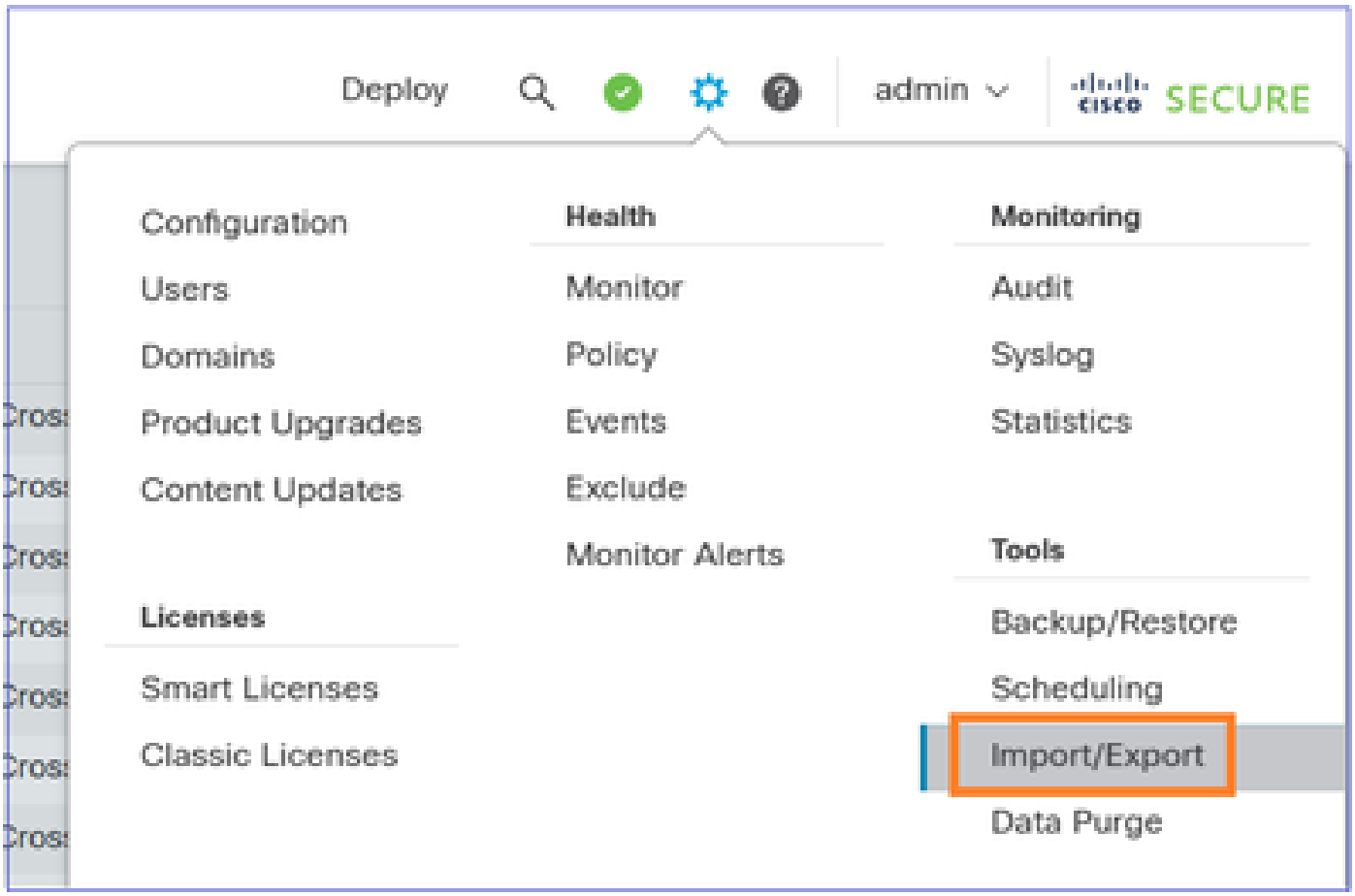
— 如果目標FMC上存在同名的現有策略，系統會詢問您是否執行以下操作：

a.要替換策略或

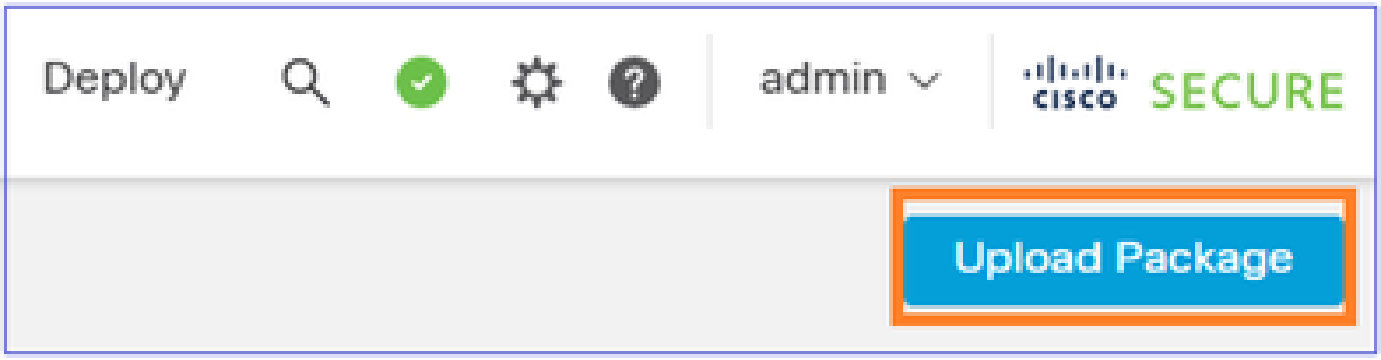
b.使用其他名稱建立一個新名稱。這將建立具有不同名稱（字尾_1）的重複對象。

— 如果您使用選項「b」，則在第9步中，確保將新建立的對象重新整理到遷移的策略（ACP安全區域、NAT安全區域、路由、平台設定等）。

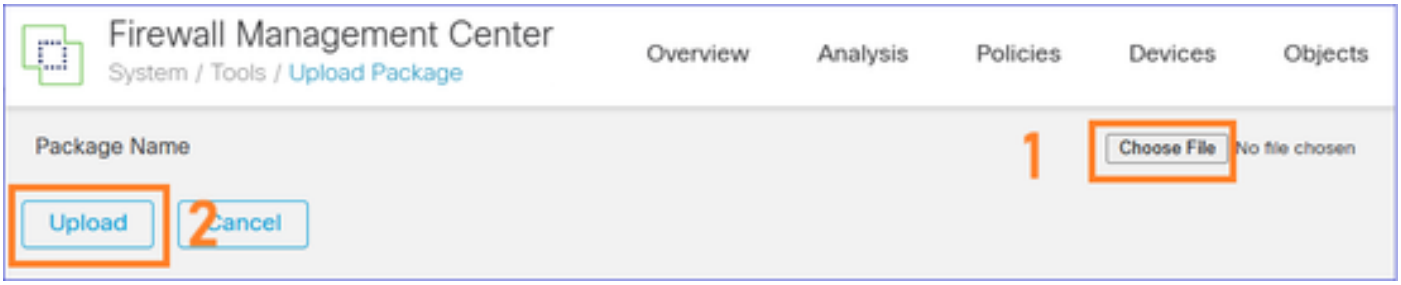
登入至FMC2（目標FMC）並匯入您在步驟5中匯出的FTD Policies證券及期貨條例對象：



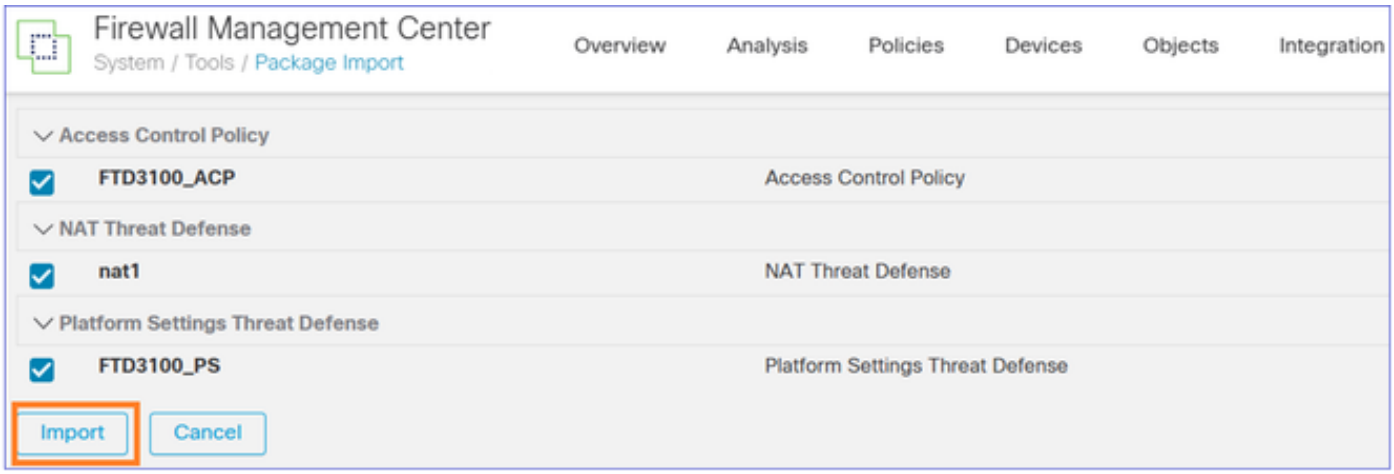
選擇Upload Package:



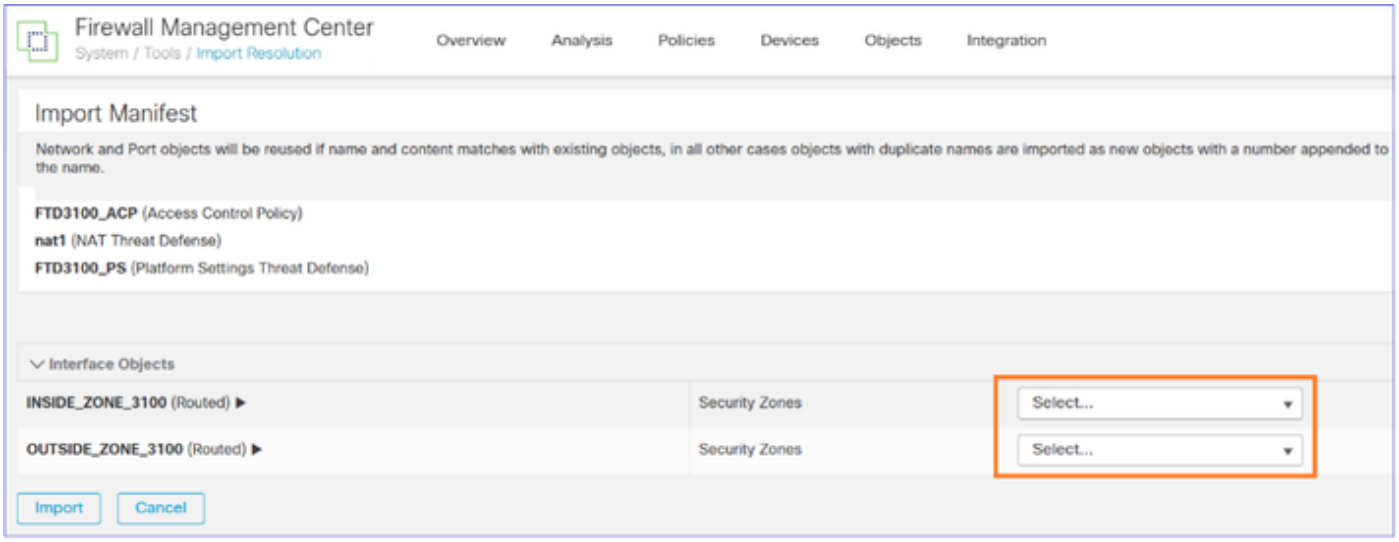
上傳檔案：



導入策略：



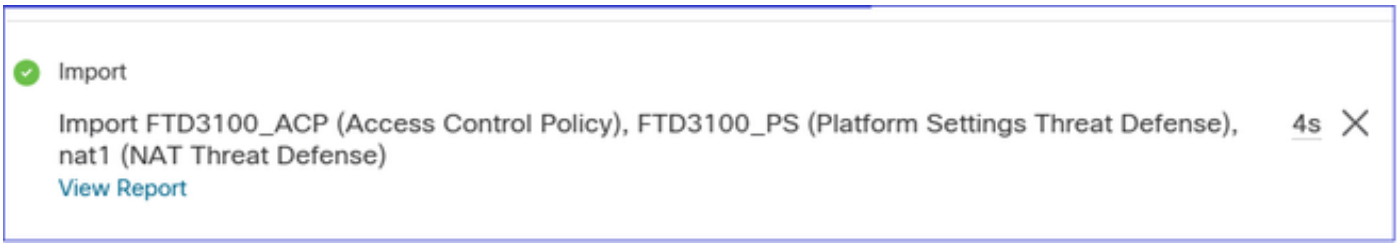
在FMC2（目標FMC）上建立介面對象/安全區域：



您可以為FMC1（來源FMC）指定相同的名稱：

選擇Import後，任務開始將相關策略匯入到FMC2（目標FMC）：

任務完成：

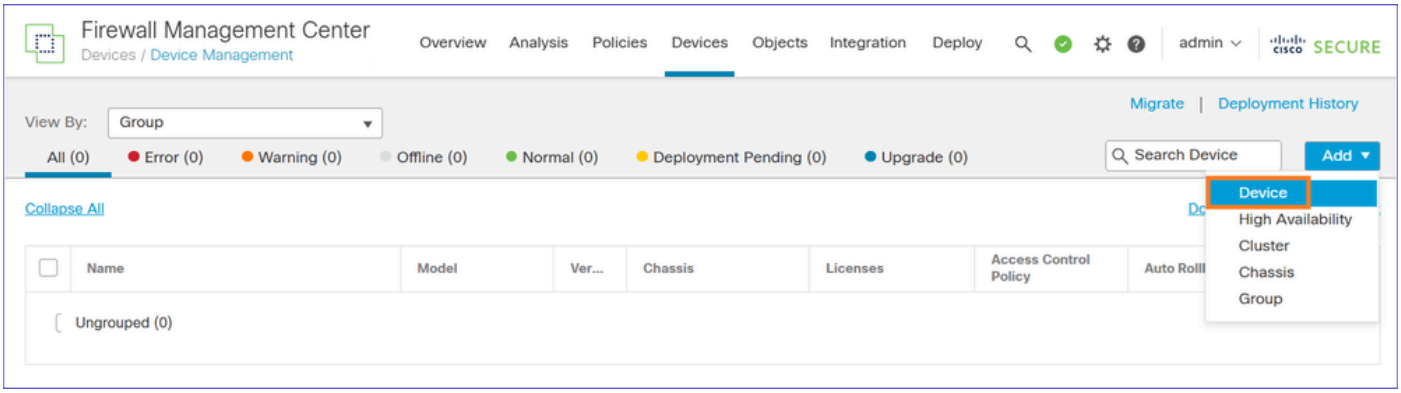


步驟8.將FTD1（非主要）註冊到FMC2

前往FTD1（非主要）CLI並設定新管理員：

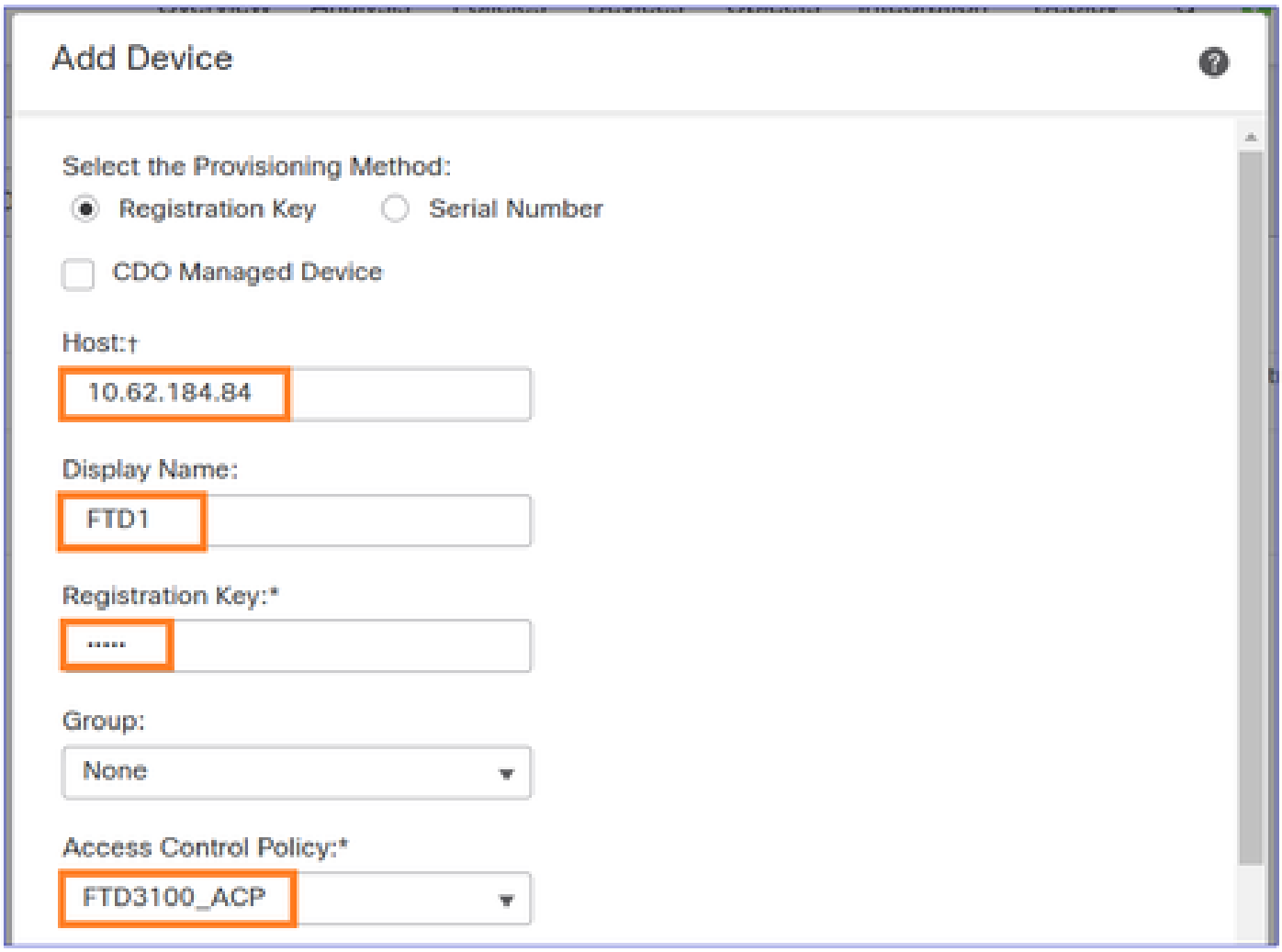
```
<#root>

>

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.

>
```

導覽至FMC2（目標FMC）UI Devices > Device Management，然後Add FTD裝置：

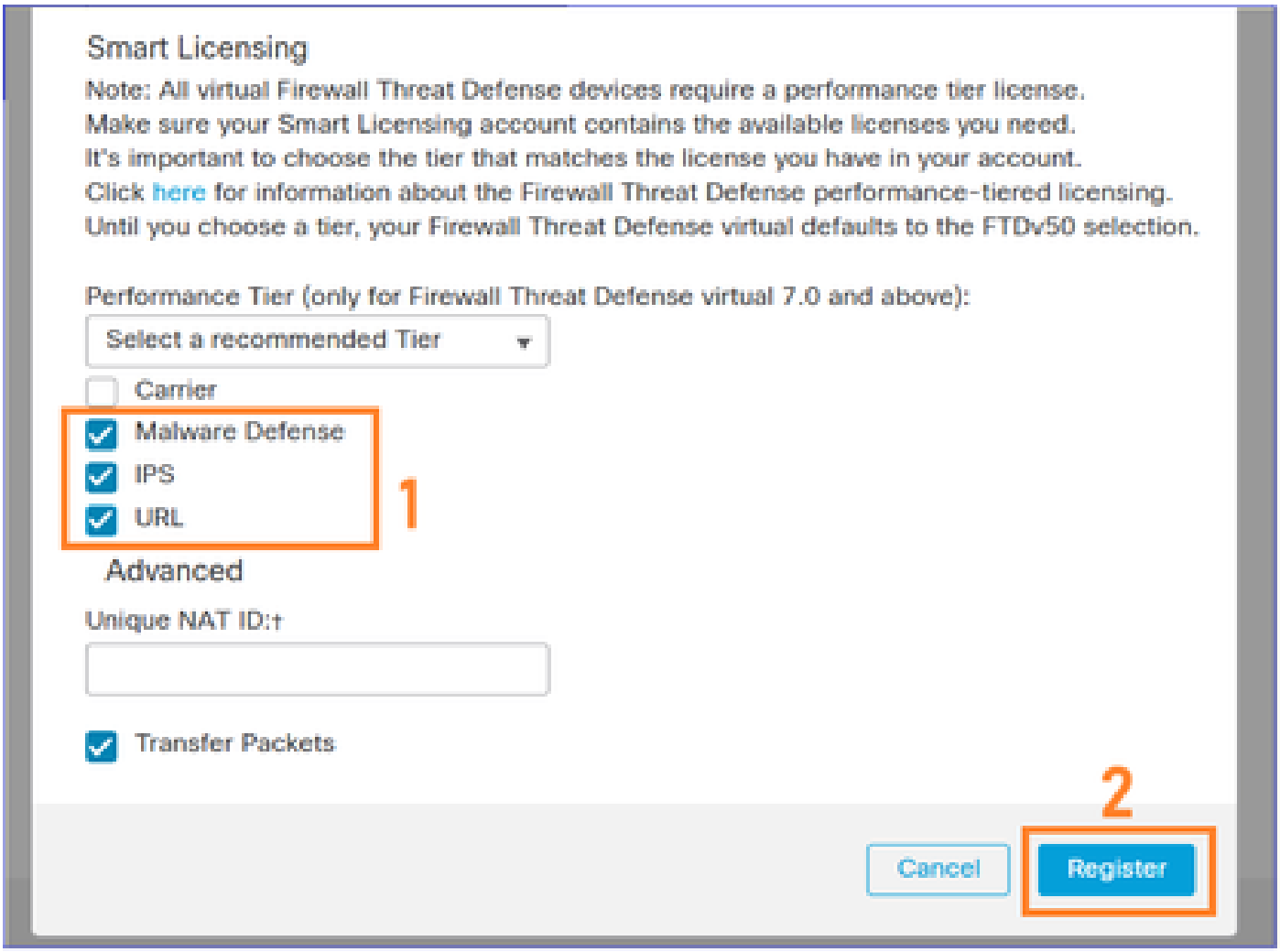


如果裝置註冊失敗，請參閱本文檔以解決問題：https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

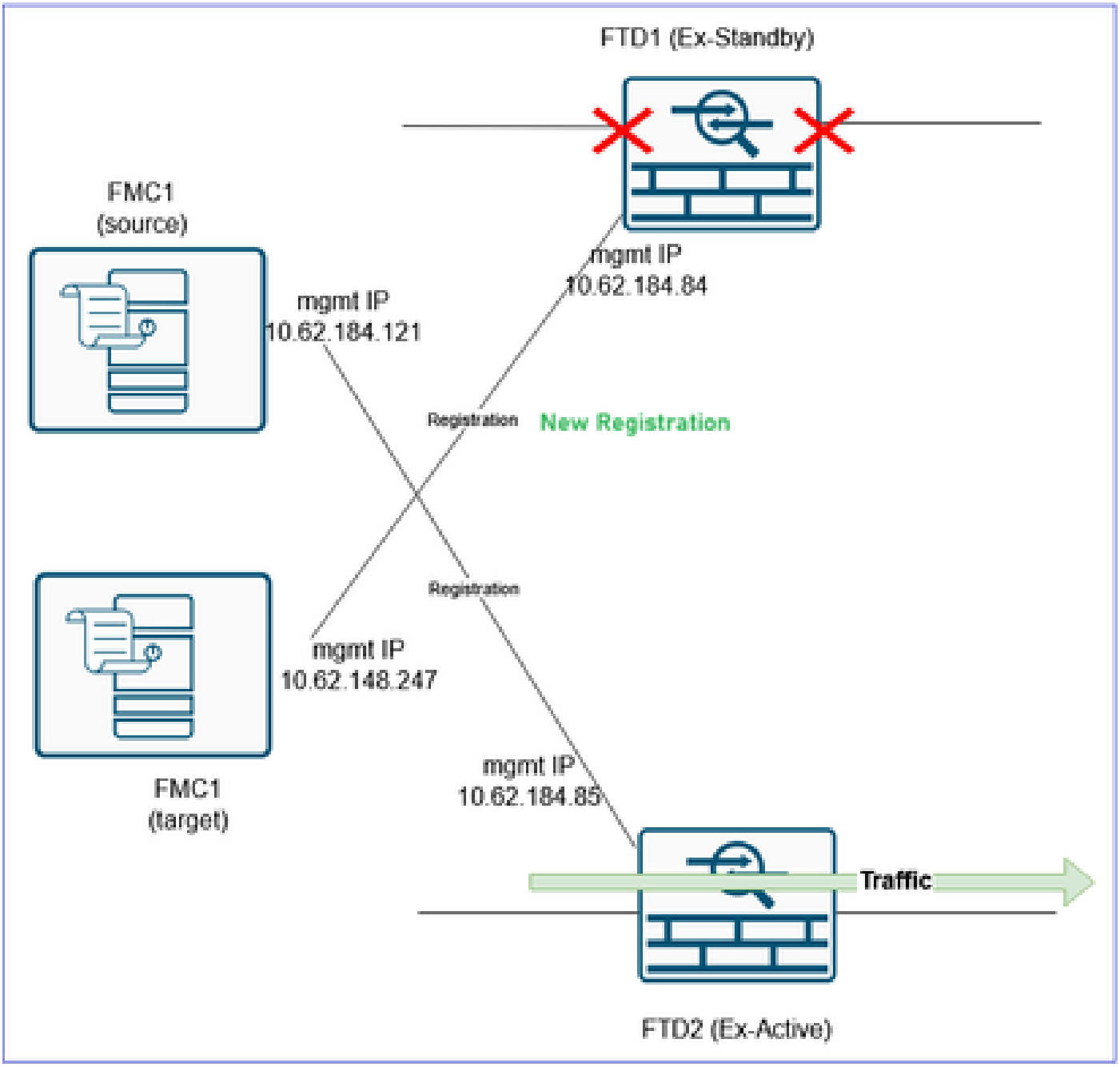
分配在上一步中匯入的訪問控制策略：



應用所需的許可證並註冊裝置：


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

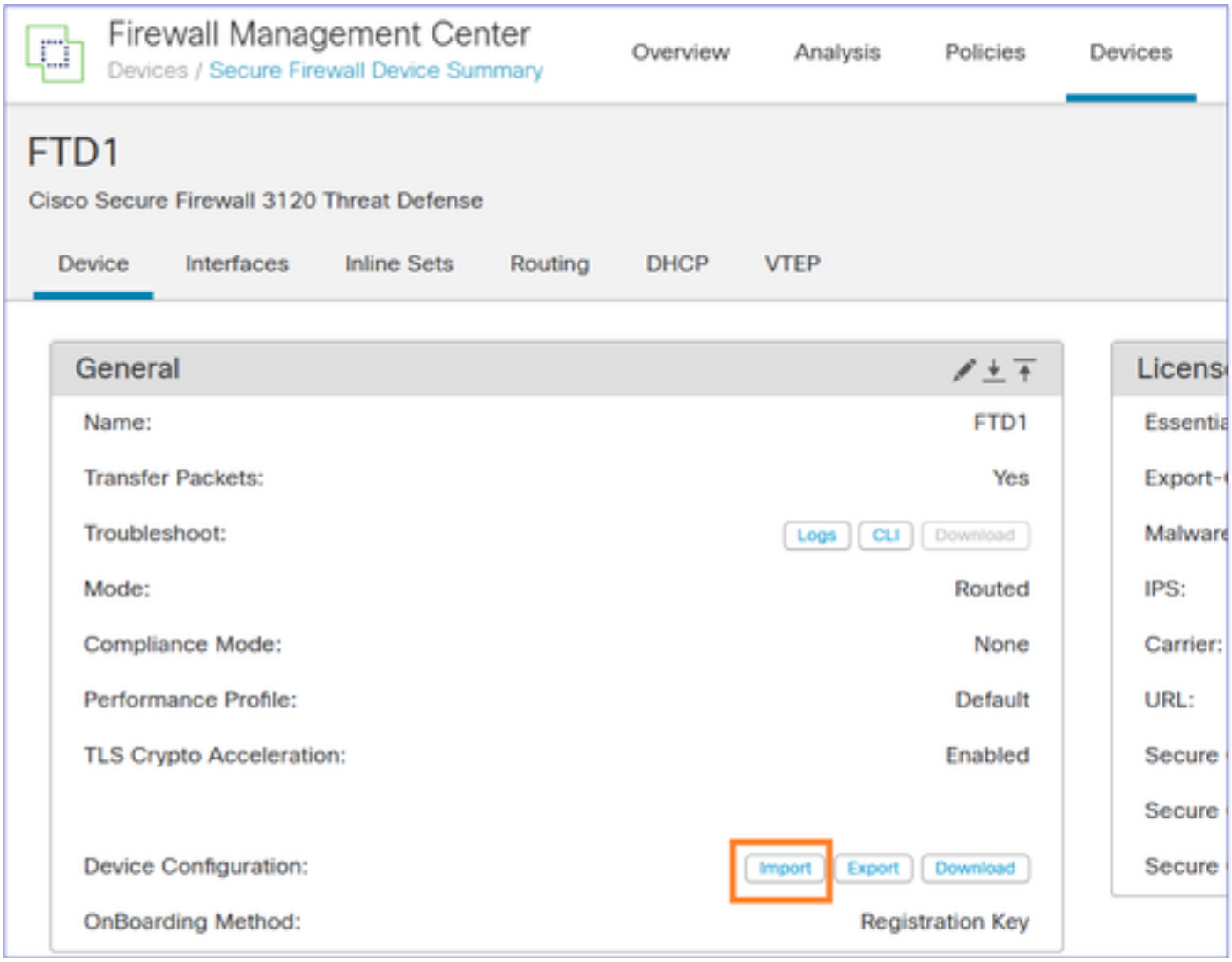
結果是：



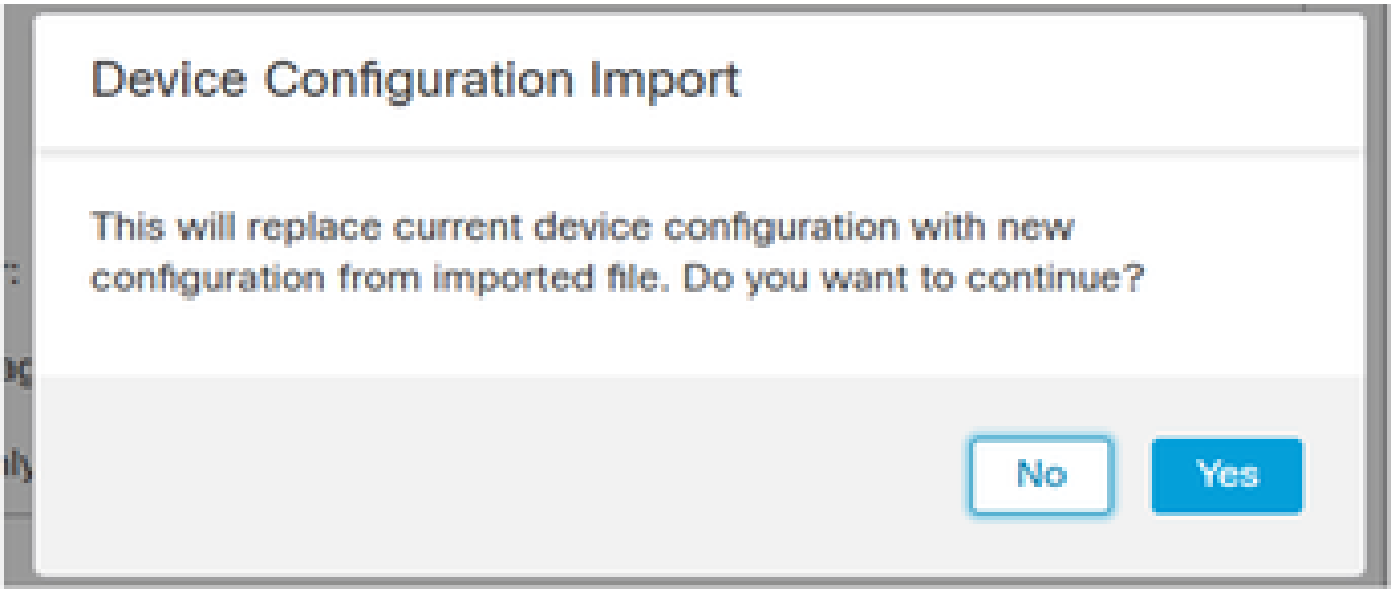
步驟9.將FTD裝置配置對象匯入FMC2（目標FMC）

登入FMC2（目標FMC），導覽至Devices > Device Management，然後導覽至Edit，然後選擇您在上一步中註冊的FTD裝置。

導覽至Device索引標籤，然後導覽至Import FTD Policies對象（已於步驟2中匯出）：

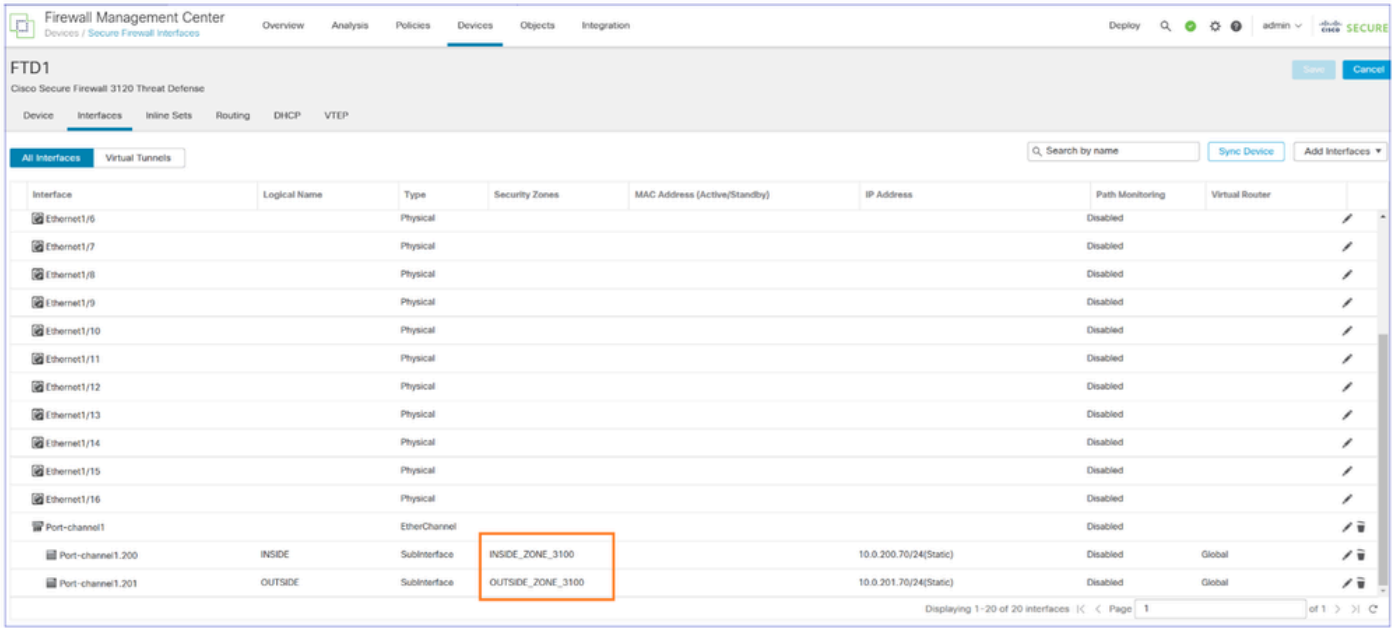


附註：如果在第7步中使用了選項「b」（建立新策略），請確保將新建立的對象重新整理到遷移的策略（ACP安全區域、NAT安全區域、路由、平台設定等）。



FMC任務已啟動。

裝置組態套用在FTD1上，例如安全區域、ACP、NAT等：



⚠ 注意：如果您的ACP擴展到許多訪問控制元素，則ACP編譯過程(tmatch compile)可能需要幾分鐘才能完成。您可以使用此命令驗證ACP編譯狀態：

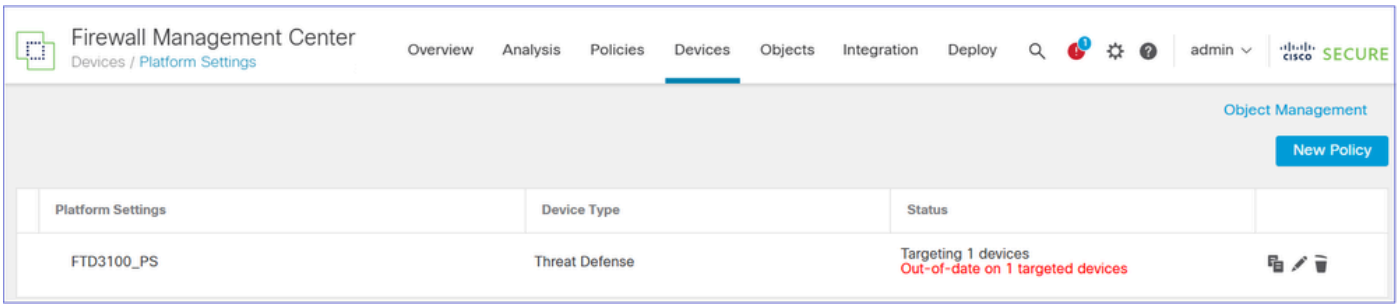
```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

步驟10.完成FTD設定

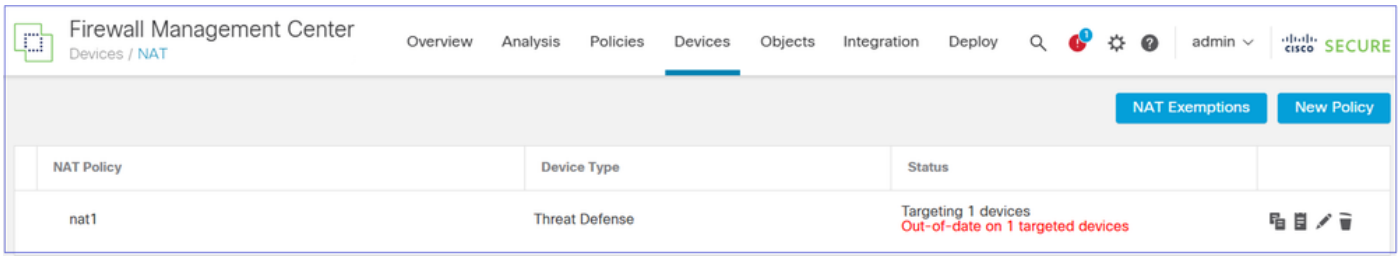
此時，目標是配置在註冊到FMC2（目標FMC）和匯入裝置策略後FTD1中仍可能丟失的所有功能。

確保NAT、平台設定、QoS等策略。已分配給FTD。您會看到，已分配策略，但部署處於掛起狀態。

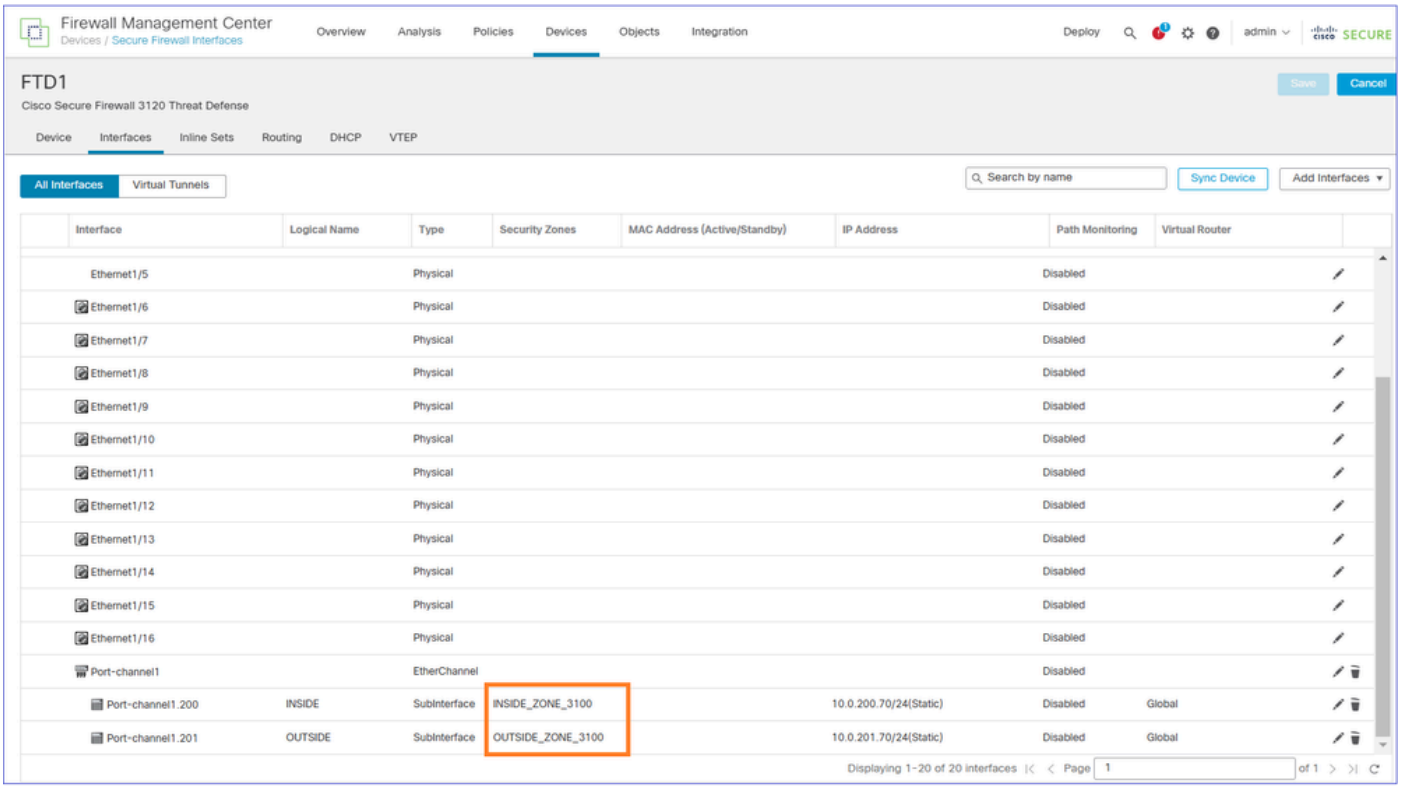
例如，平台設定被匯入並分配給裝置，但部署處於掛起狀態：



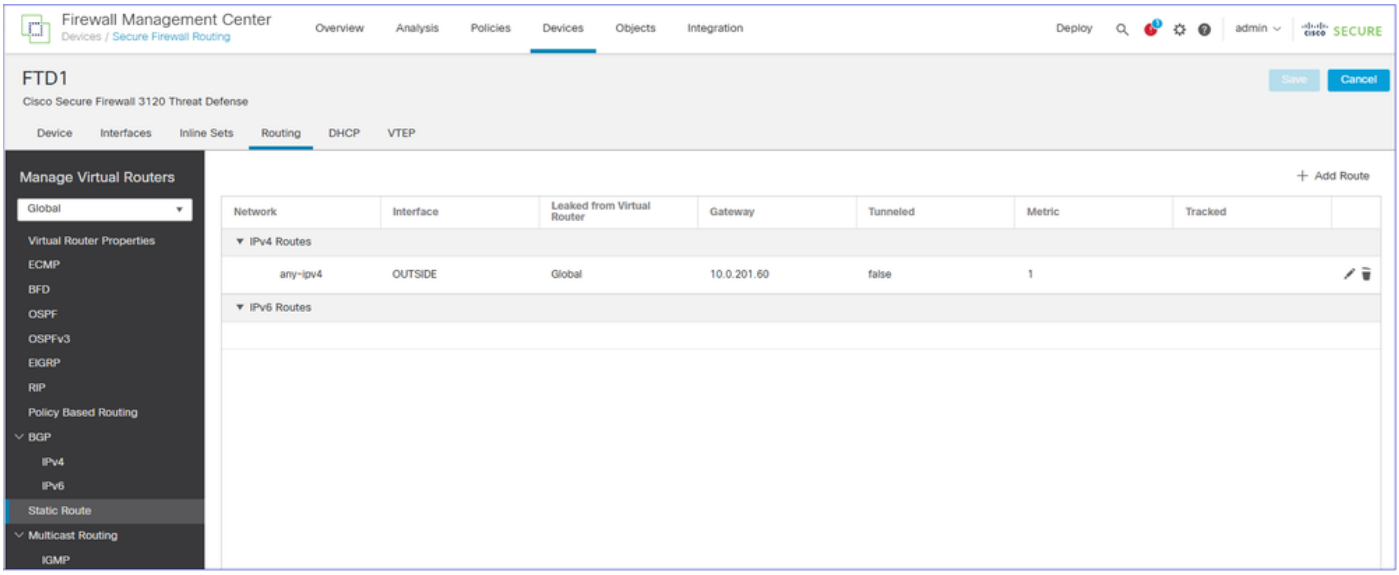
如果配置了NAT，則會匯入NAT策略並將其分配給裝置，但會等待部署：



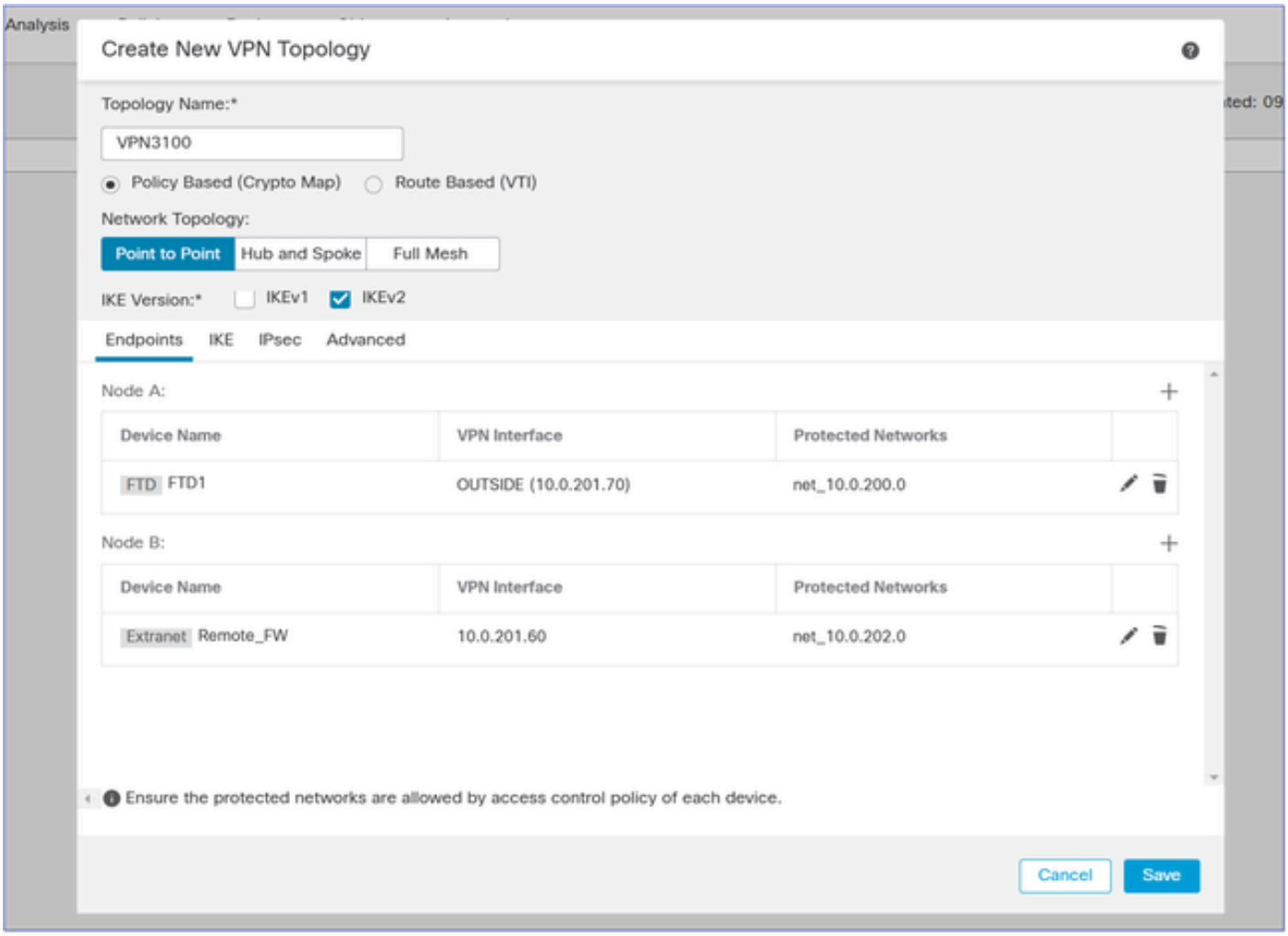
將安全區域應用到介面：



路由組態會套用到FTD裝置：

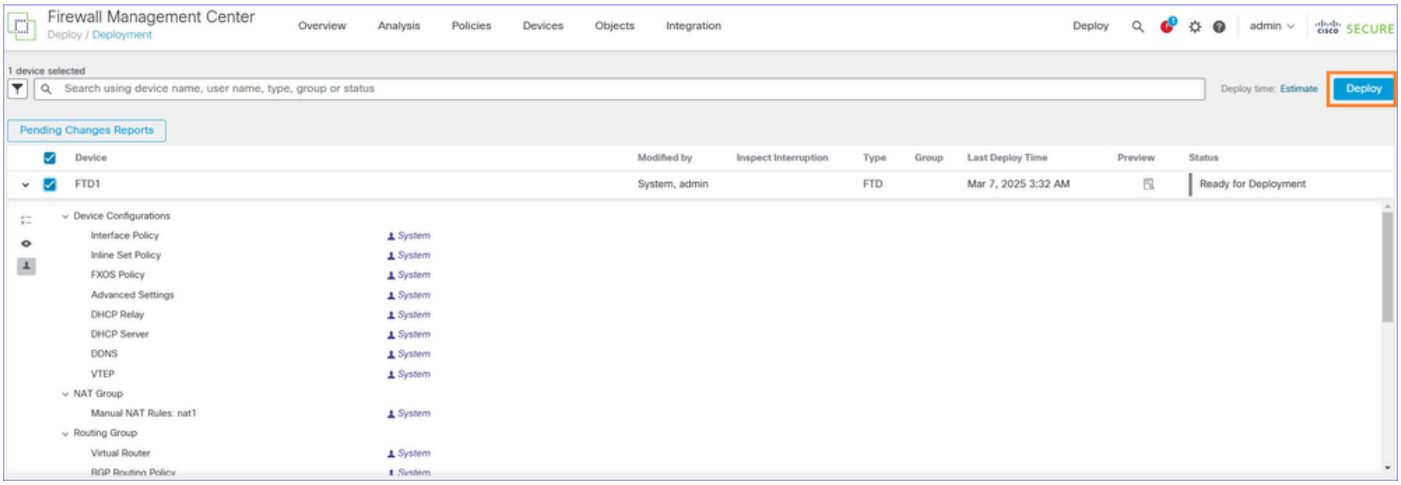


附註：現在是配置無法自動遷移的策略（例如VPN）的時候了。



附註：如果遷移的FTD具有也遷移至目標FMC的S2S VPN對等點，則必須在將所有FTD移動到目標FMC後配置VPN。

部署掛起的更改：



步驟11.驗證部署的FTD組態

此時，目標是從FTD CLI檢查所有配置是否均已就緒。

建議比較兩個FTD的「show running-config」輸出。可以使用WinMerge或diff等工具進行比較。

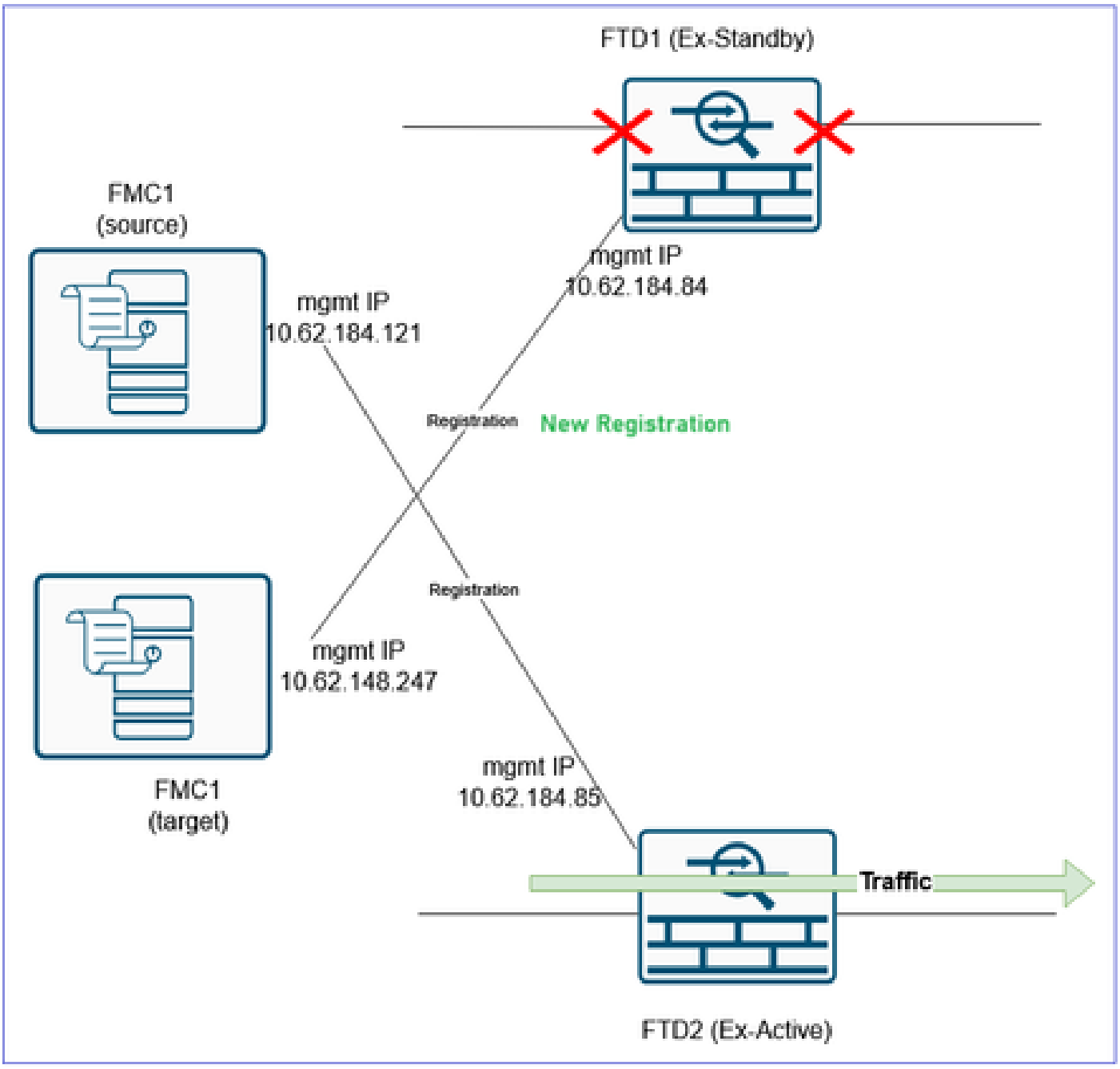
您看到的和正常情況的差異是：

- 裝置序列號
- 介面說明
- ACL rule-ids
- 配置加密校驗和

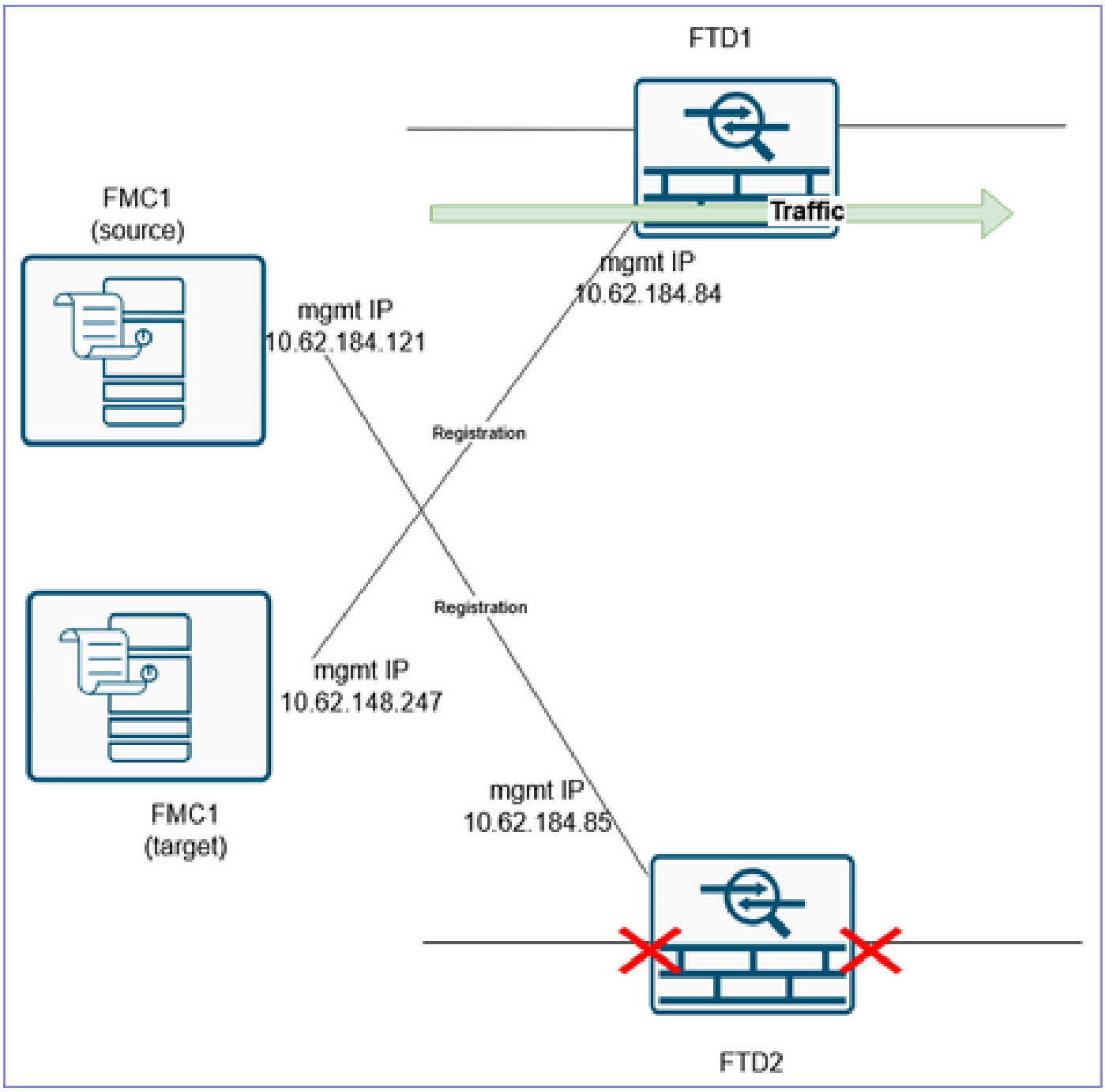
步驟12.執行切換

在此步驟中，目標是將流量從目前處理流量且仍註冊到舊/來源FMC的FTD2交換到註冊到目標FMC的FTD1。

之前：


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)

之後：



⚠ 注意：安排MW機進行切換。切換期間，您將遇到一些流量中斷，直到所有流量都轉移到FTD1,VPN重新建立，以此類推。

⚠ 注意：除非完成ACP編譯，否則請勿啟動切換（參見上述步驟10）。

⚠ 警告：確保從FTD2拔下資料線或關閉相關的交換器連線埠。否則，您最終會使用兩台裝置處理流量！

⚠ 注意：由於兩台裝置使用相同的IP配置，因此需要更新相鄰第3層裝置的ARP快取。考慮手動清除相鄰裝置的ARP快取，以加快流量切換。

提示：您還可以使用FTD CLI指令傳送GARP封包和更新相鄰裝置的ARP快取：

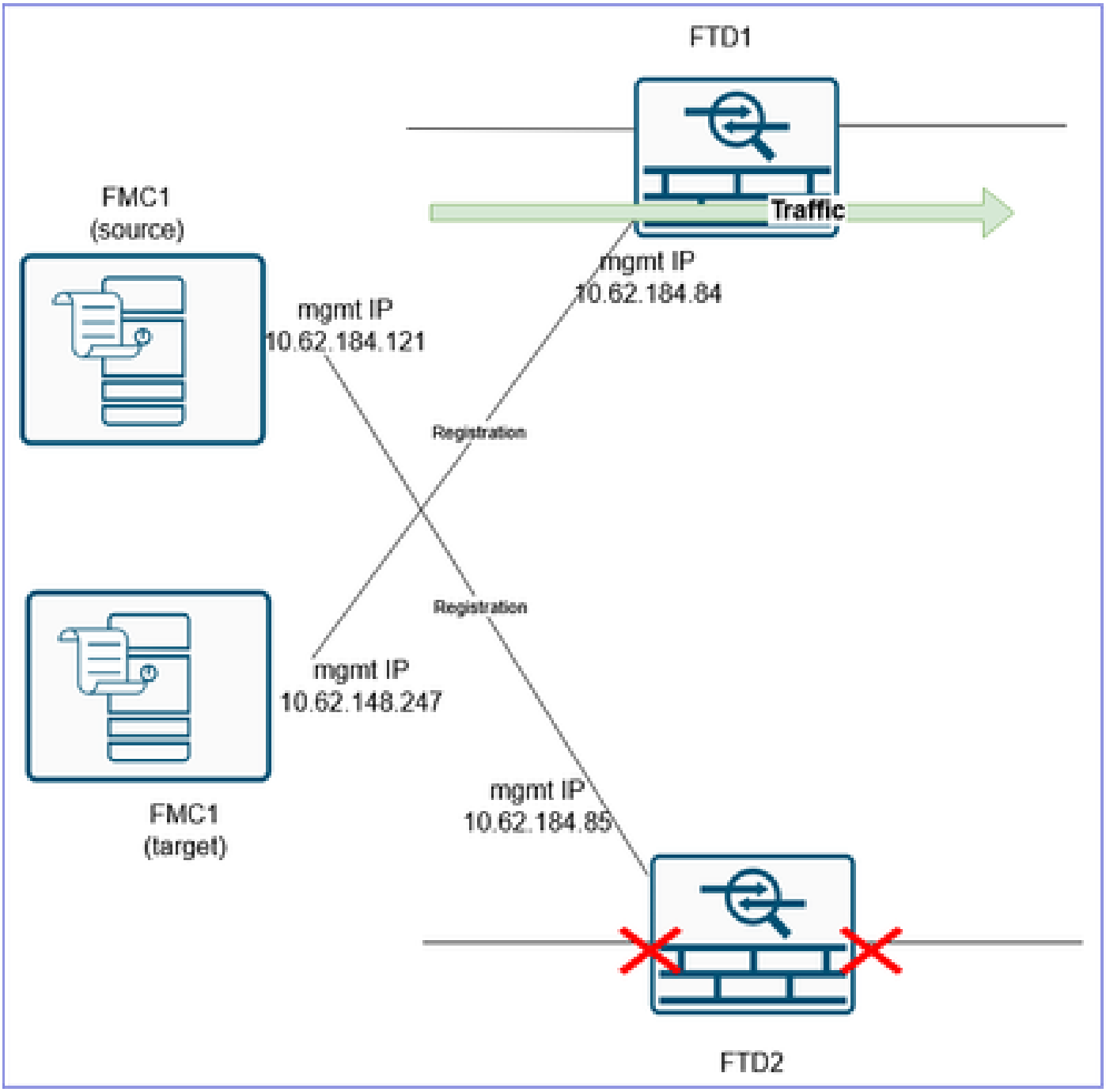
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

您必須對FW擁有的每個IP重複此命令。因此，僅清除相鄰裝置的ARP快取要比為防火牆擁有的每個IP傳送GARP資料包的速度更快。

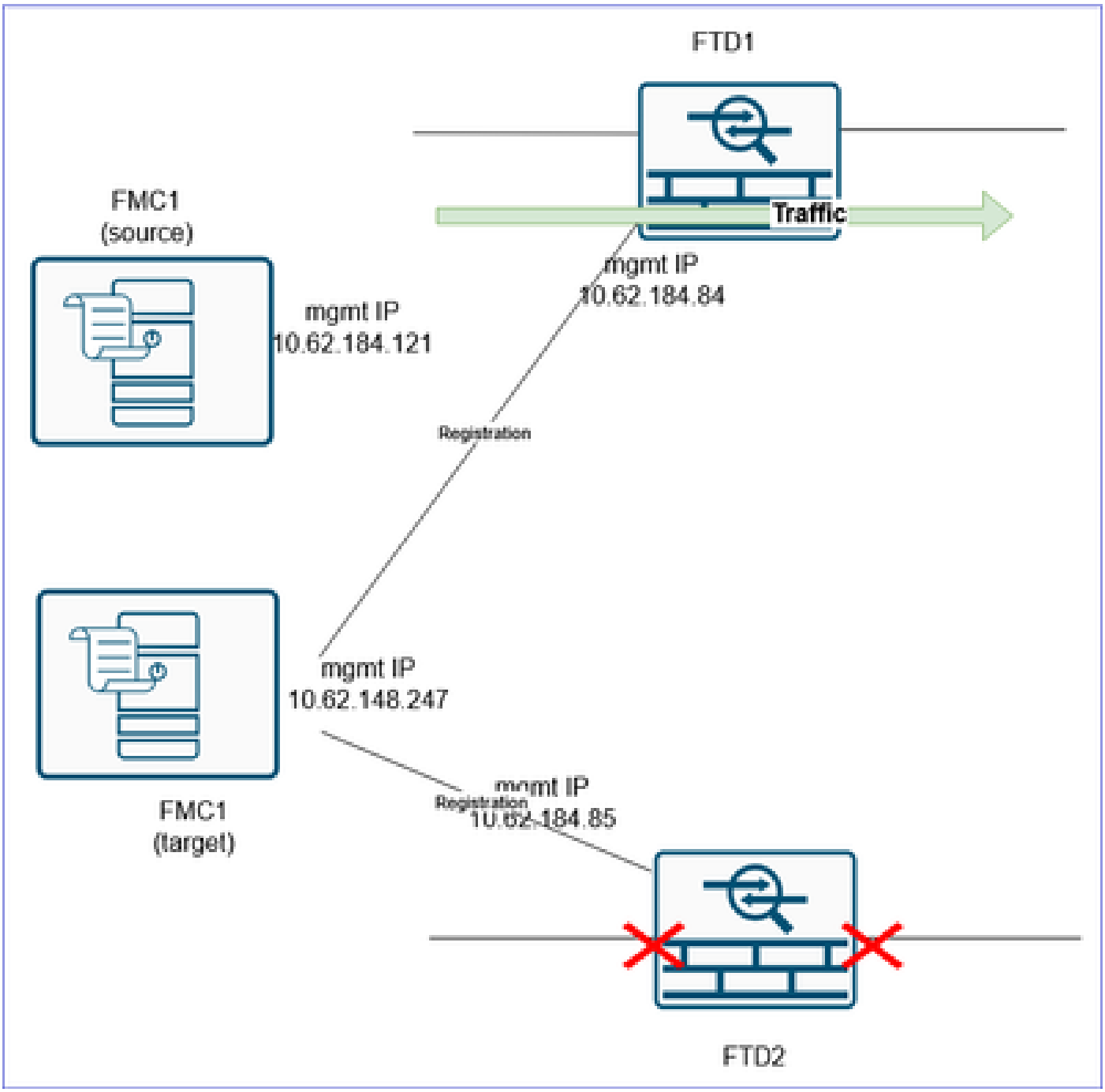
步驟13.將第二個FTD移轉到FMC2（目標FMC）

最後一項是改革HA配對。為此，首先需要從FMC1（來源FMC）中刪除FTD2，並將其註冊到FMC2（目標FMC）。

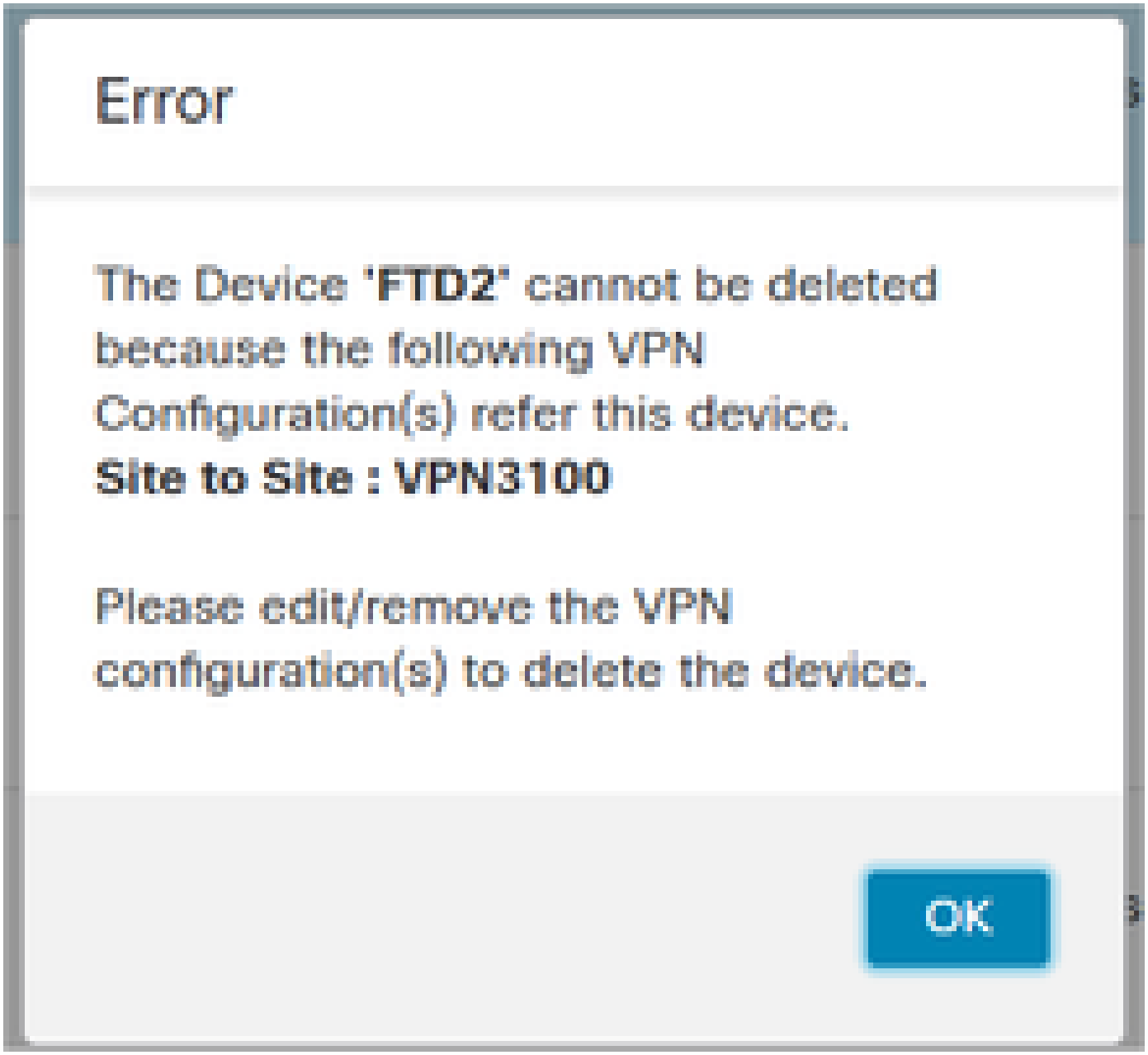
之前：


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

之後：



如果您的VPN組態連線到FTD2，則必須在刪除FTD之前先將其移除。在不同情況下，會顯示類似以下內容的消息：



CLI 驗證:

<#root>

>

show managers

No managers configured.

在將所有FTD組態註冊到目標FMC之前，將其清除是一種很好的作法。一種快速方法是在防火牆模式之間進行切換。

例如，如果您有路由模式，請切換到透明模式，然後返迴路由模式：

<#root>

>

configure firewall transparent

然後：

<#root>

>

configure firewall routed

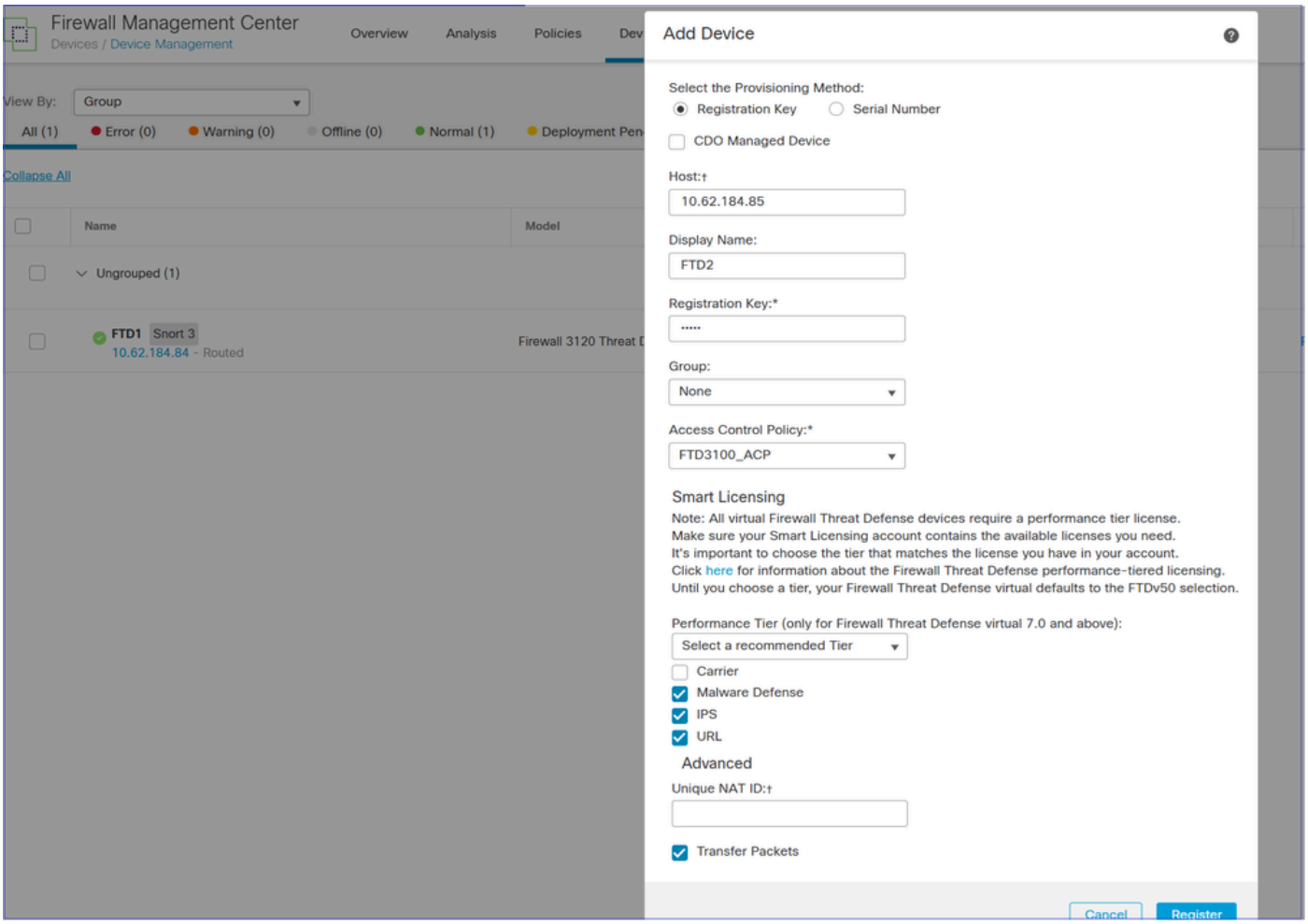
然後，將其註冊到FMC2（目標FMC）：

<#root>

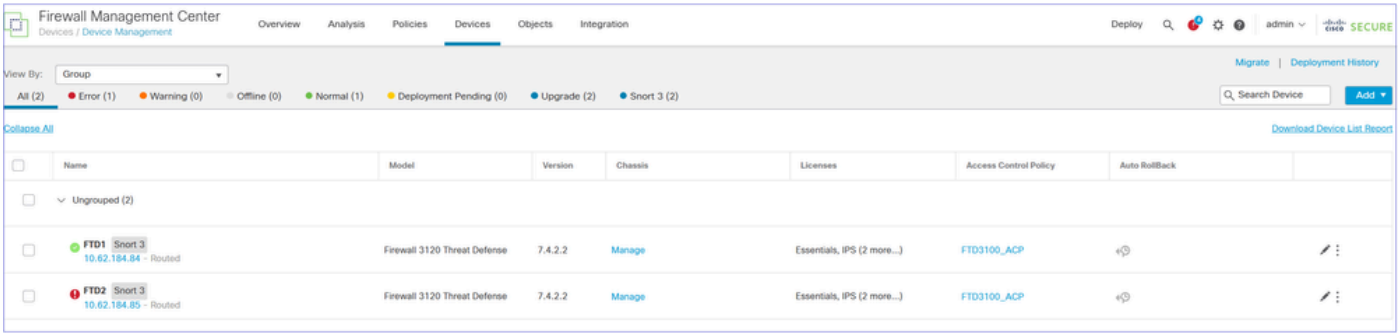
>

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.
>
```



結果是：

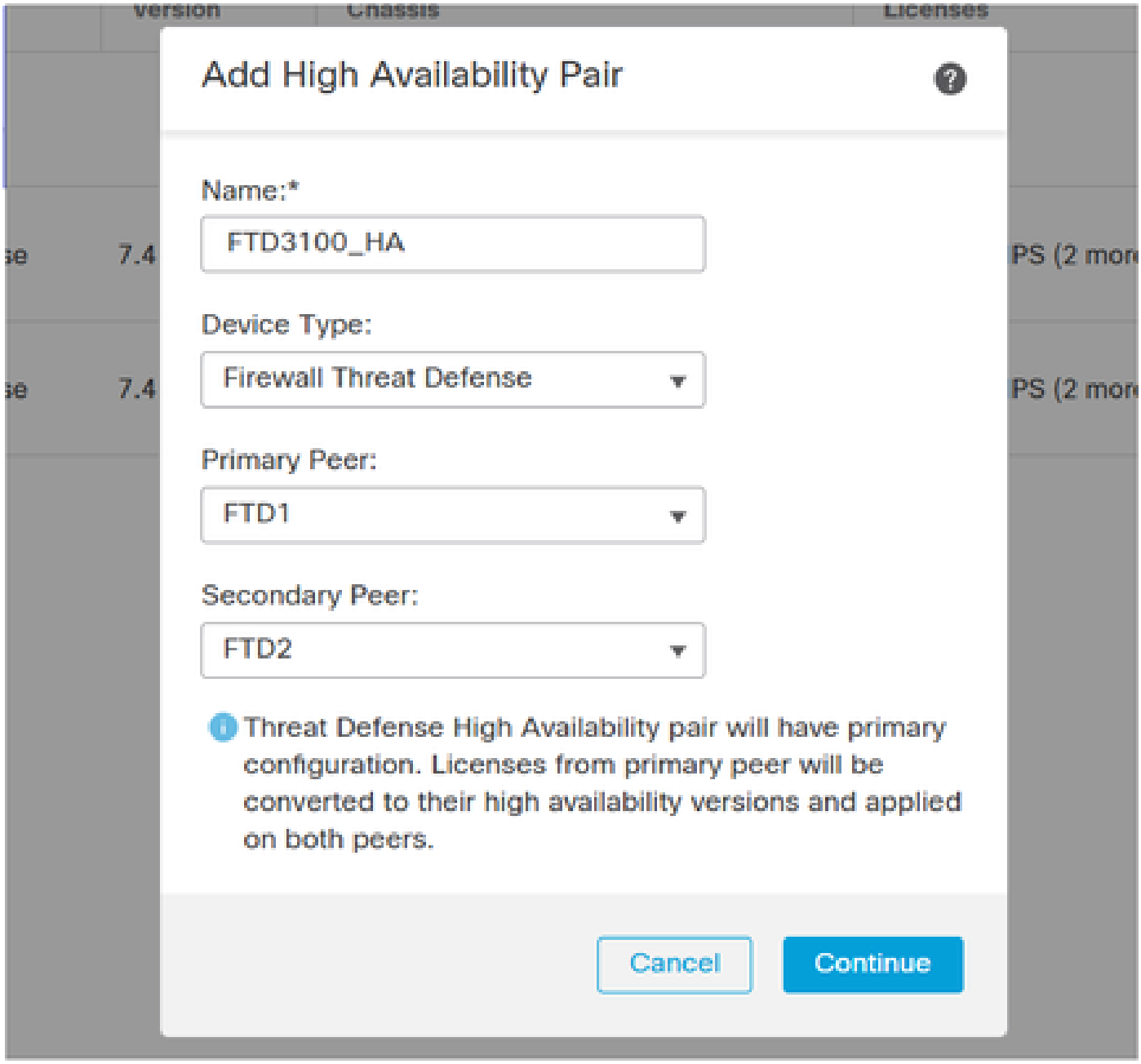


步驟14.重組FTD HA

附註：此任務（與任何與HA相關的任務一樣）也必須在MW期間執行。在HA交涉期間，資料介面關閉後，流量可能會中斷約1分鐘。

在目標FMC上，導航到Devices > Device Management和Add > High Availability。

⚠ 注意：確保選擇處理流量的FTD（在此案例中為FTD1）作為主要對等點：



重新配置HA設定，包括受監控介面、備用IP、虛擬MAC地址等。

從FTD1 CLI驗證：

```
<#root>

FTD3100-3#

show failover | include host

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

從FTD2 CLI驗證：

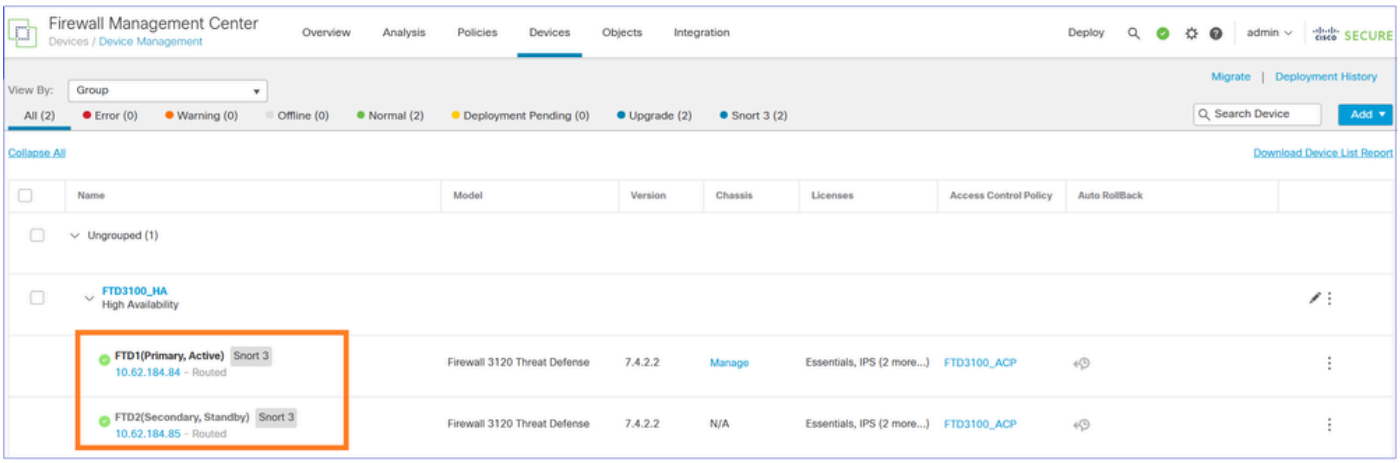
<#root>

FTD3100-3#

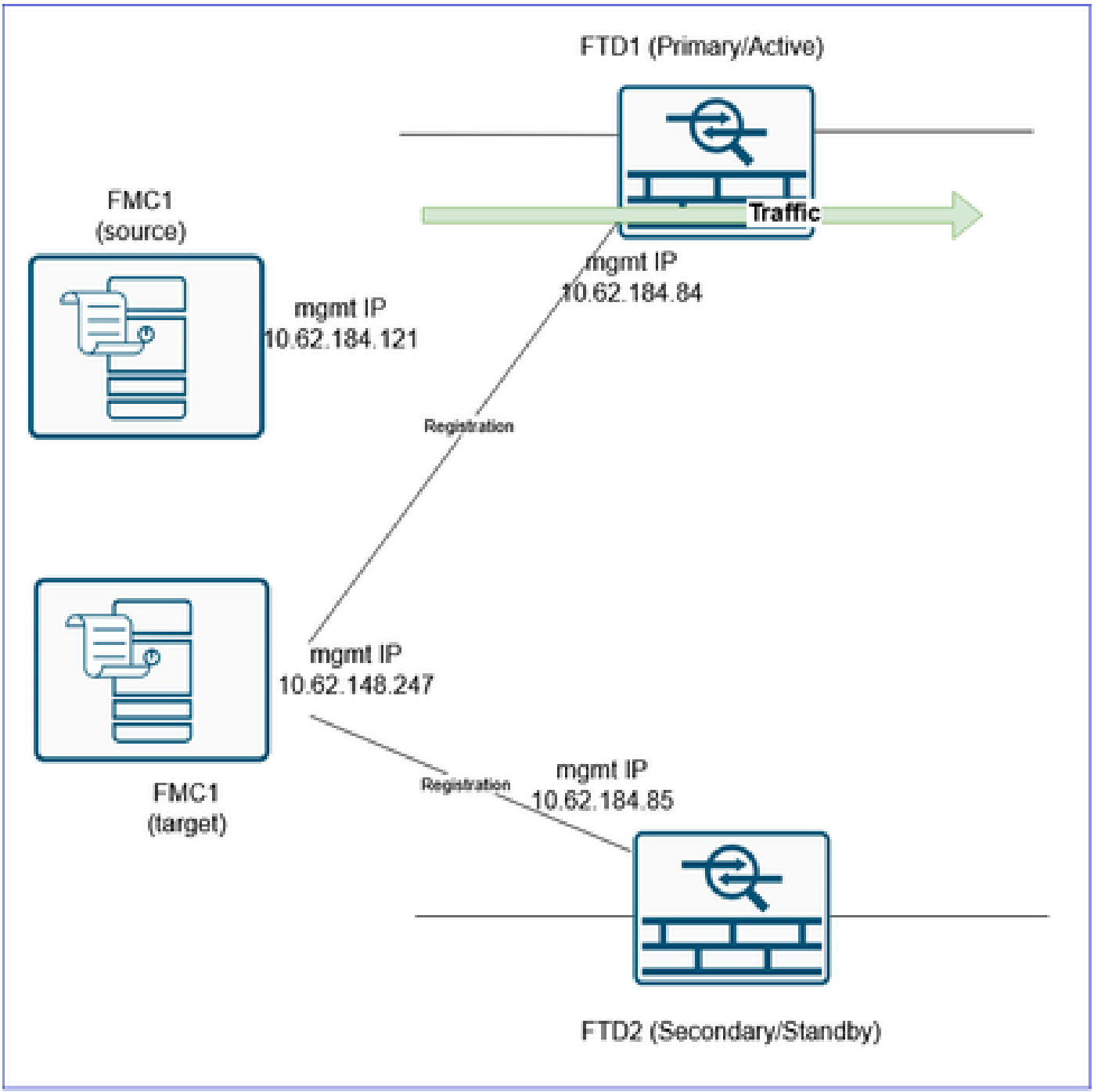
show failover | include host

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

FMC UI驗證：



最後，開啟/重新連線FTD2裝置的資料介面。



參考資料

- 匯出和匯入裝置配置
- 新增高可用性對
- 將FTD從一個FMC遷移到另一個FMC

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。