Migrazione di FTD HA (failover) a un altro FMC

Sommario

Introduzione

Il presente documento descrive la procedura di migrazione di un FTD HA da un CCP esistente a un altro CCP.

Per una migrazione autonoma del firewall a un nuovo FMC, visitare il sito Web all'indirizzo 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

Abbreviazioni

ACP = criteri di controllo dell'accesso

ARP = Address Resolution Protocol

CLI = Command Line Interface

FMC = Centro gestione firewall sicuro

FTD = Secure Firewall Threat Defense

GARP = ARP gratificante

HA = Alta disponibilità

MW = Finestra di manutenzione

UI = Interfaccia utente

Prerequisiti

Prima di avviare il processo di migrazione, assicurarsi di disporre dei seguenti prerequisiti:

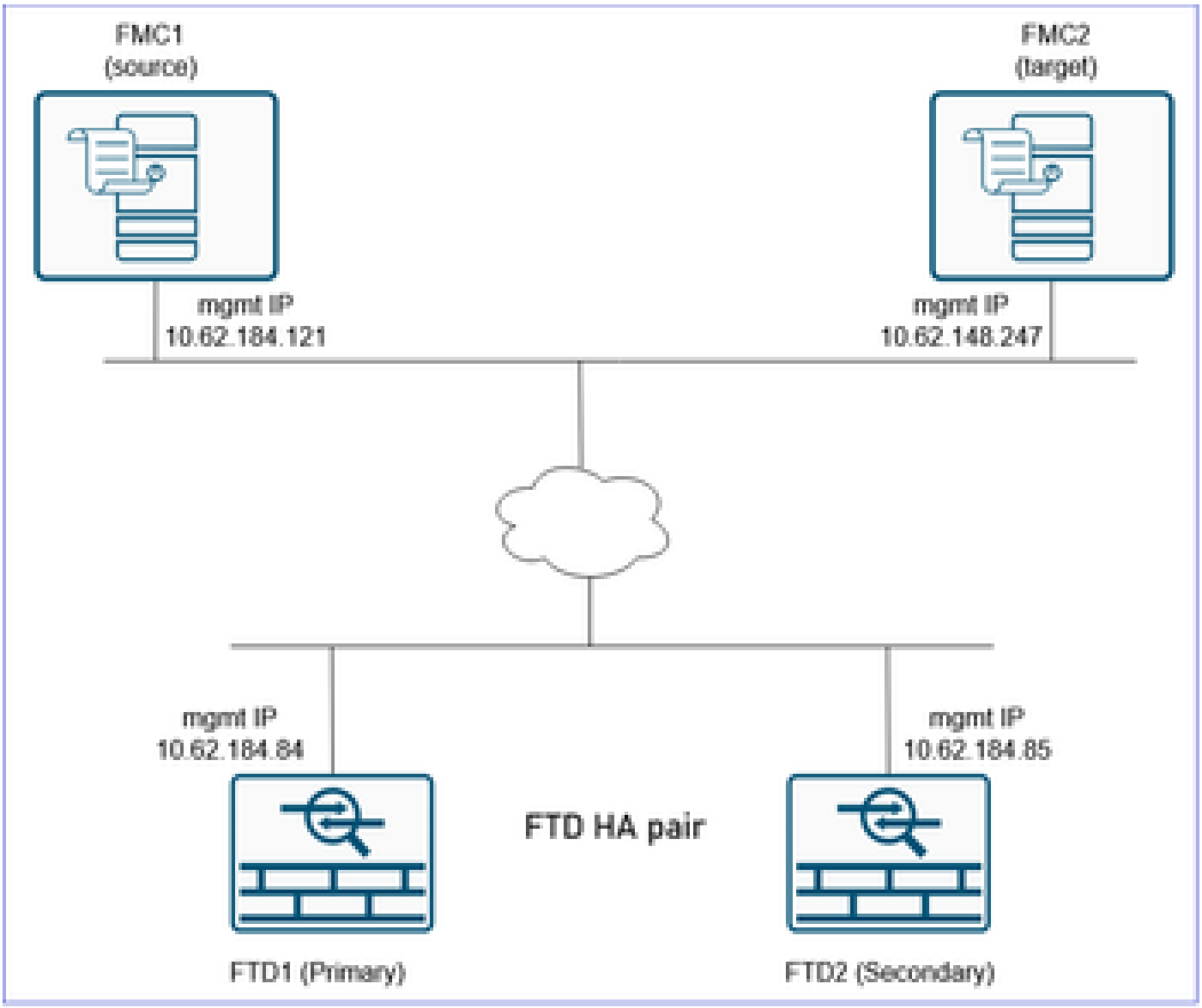
- l'accesso tramite interfaccia utente e CLI ai FMC di origine e di destinazione.
- Credenziali amministrative per i CCP e i firewall.
- Accesso da console a entrambi i firewall.
- Accesso ai dispositivi upstream e downstream L3 (nel caso sia necessario cancellare la cache ARP).
- Verificare che il CCP di destinazione abbia la stessa versione del CCP di origine/precedente.
- Verificare che il CCP di destinazione disponga delle stesse licenze del CCP di origine/precedente.
- Assicurarsi di disporre un MW per eseguire la migrazione poiché avrà un impatto sul traffico di transito.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall 31xx, FTD versione 7.4.2.2.
- Secure Firewall Management Center versione 7.4.2.2.
- Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia



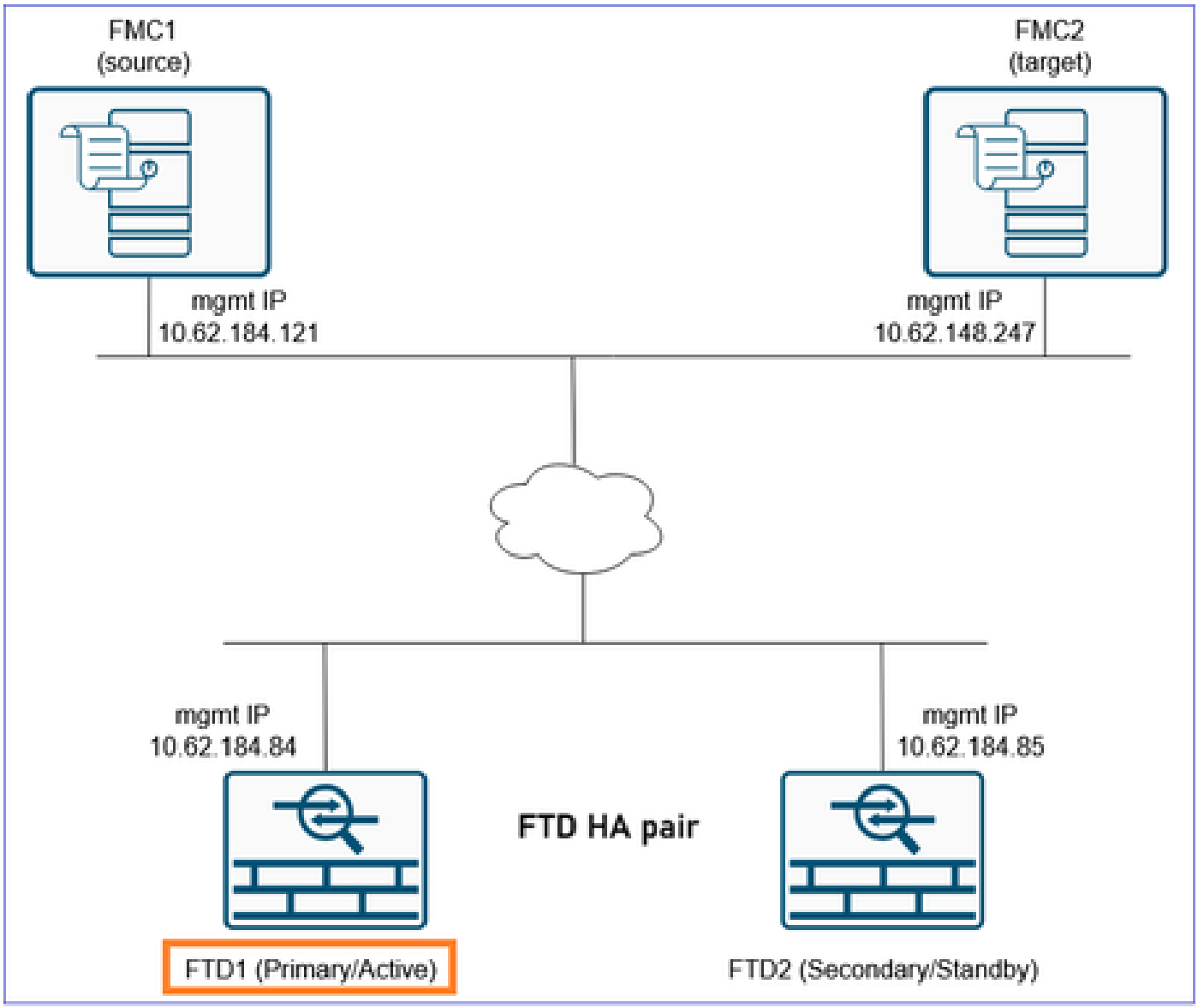
Configurazione

Fasi della migrazione

Per questo scenario si considerano i seguenti stati:

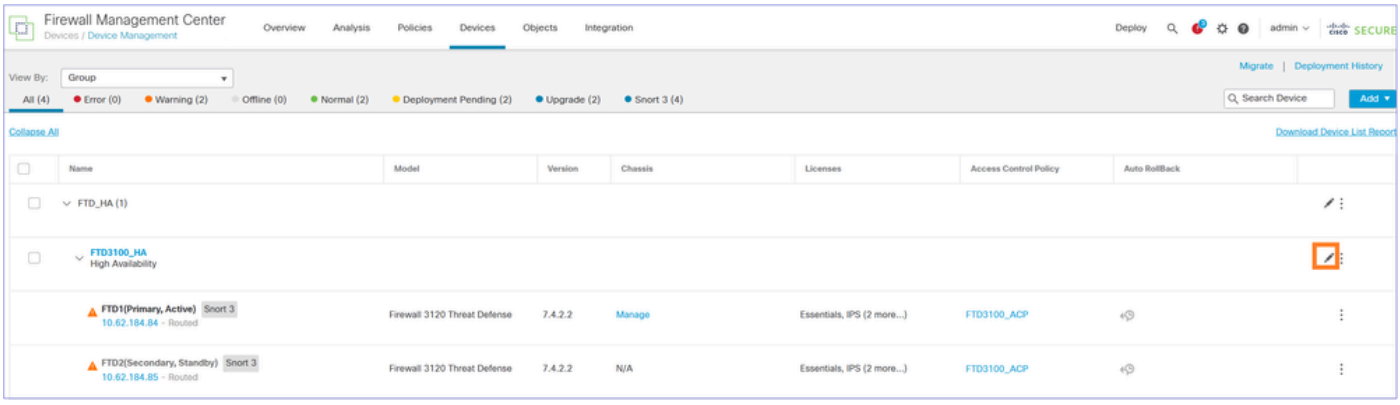
FTD1: Principale/Attivo

FTD2: Secondario/Standby

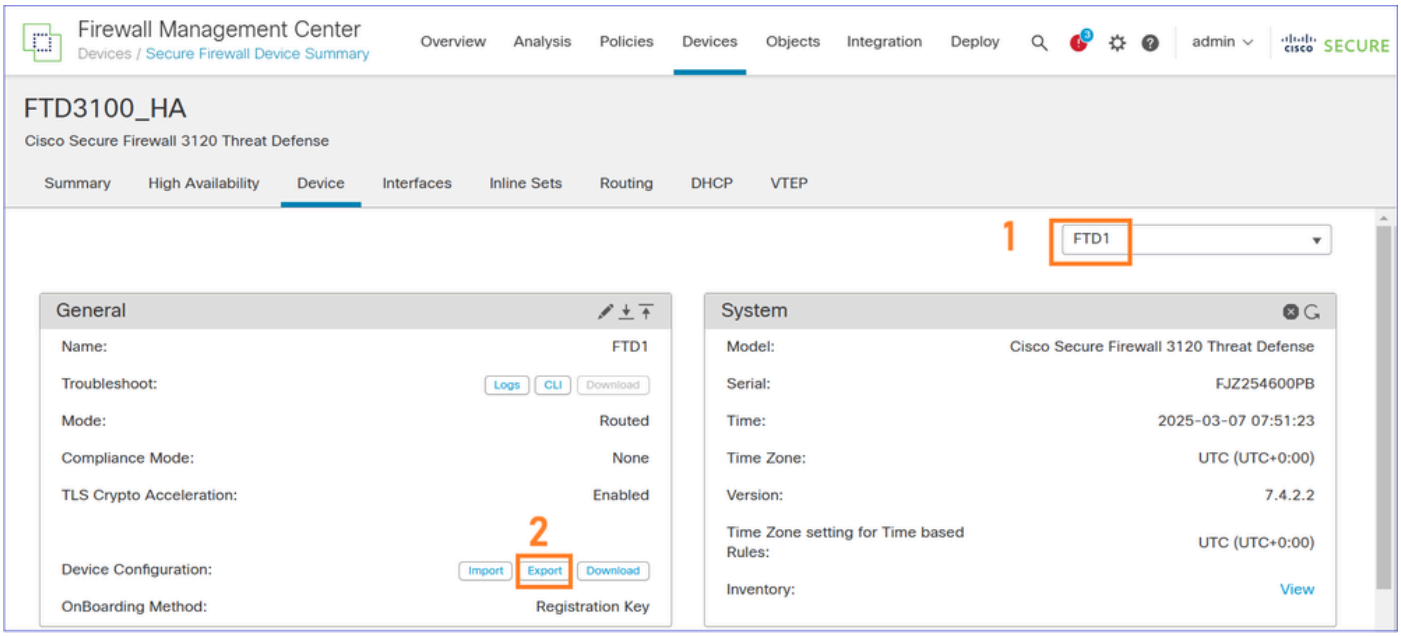


Passaggio 1. Esportare la configurazione del dispositivo dal firewall principale

Nel FMC1 (FMC di origine) passare a Dispositivi > Gestione dispositivi. Selezionare la coppia FTD HA e scegliere Modifica:

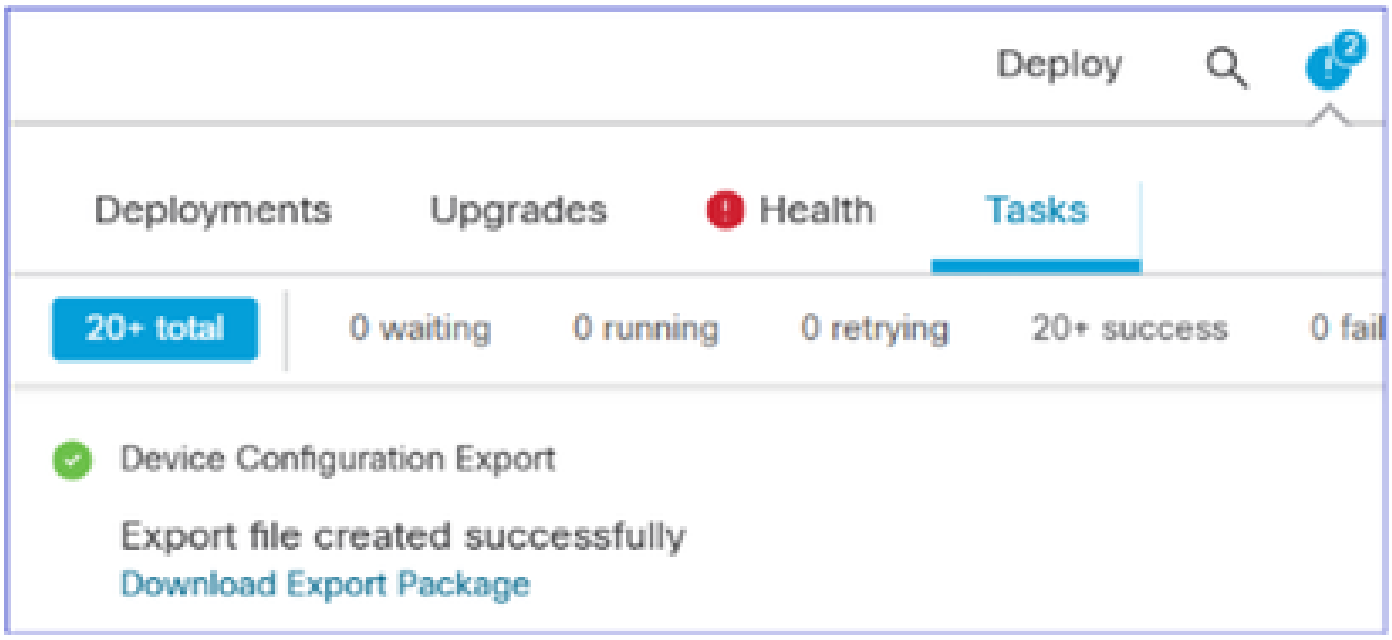


Passare alla scheda Device. Verificare che l'FTD primario/attivo (FTD1 in questo caso) sia selezionato e selezionare Esporta per esportare la configurazione del dispositivo:



Nota: L'opzione Export (Esporta) è disponibile a partire dalla versione software 7.1 e successive.

È possibile passare alla pagina Notifiche > Task per assicurarsi che l'esportazione sia stata completata. Quindi, selezionare Download Export Package (Scarica pacchetto di esportazione):



In alternativa, è possibile fare clic sul pulsante Download nell'area General. Si ottiene un file sfo, ad esempio DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

Il file contiene la configurazione relativa alla periferica, ad esempio:

- Interfacce di routing
- Insiemi non ancorati
- Routing
- DHCP

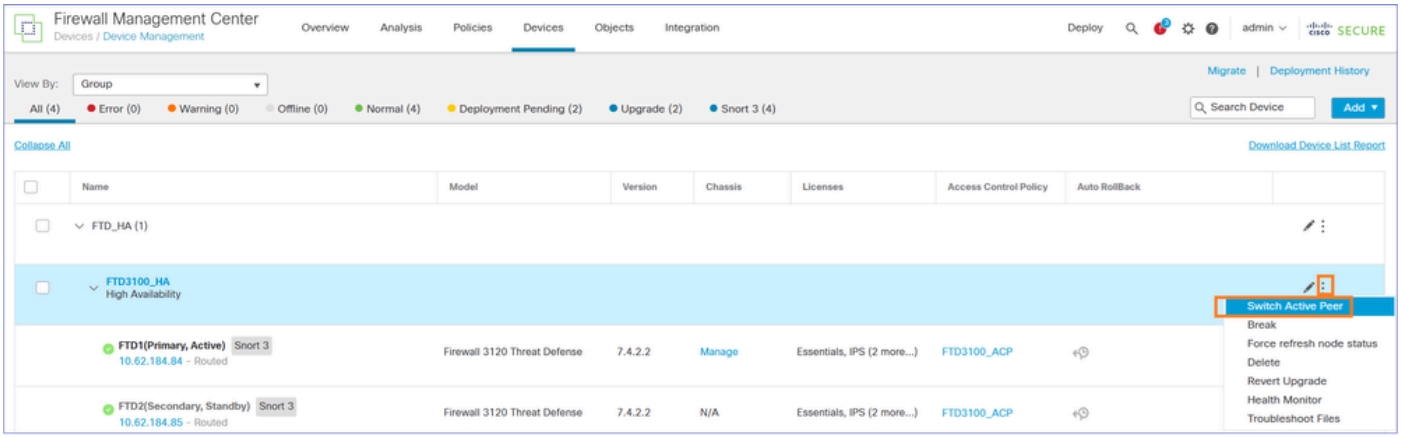
- VTEP
- Oggetti associati

Nota: Il file di configurazione esportato può essere reimportato solo nello stesso FTD. L'UUID dell'FTD deve corrispondere al contenuto del file sfo importato. Lo stesso FTD può essere registrato su un altro FMC e può essere importato un file sfo.

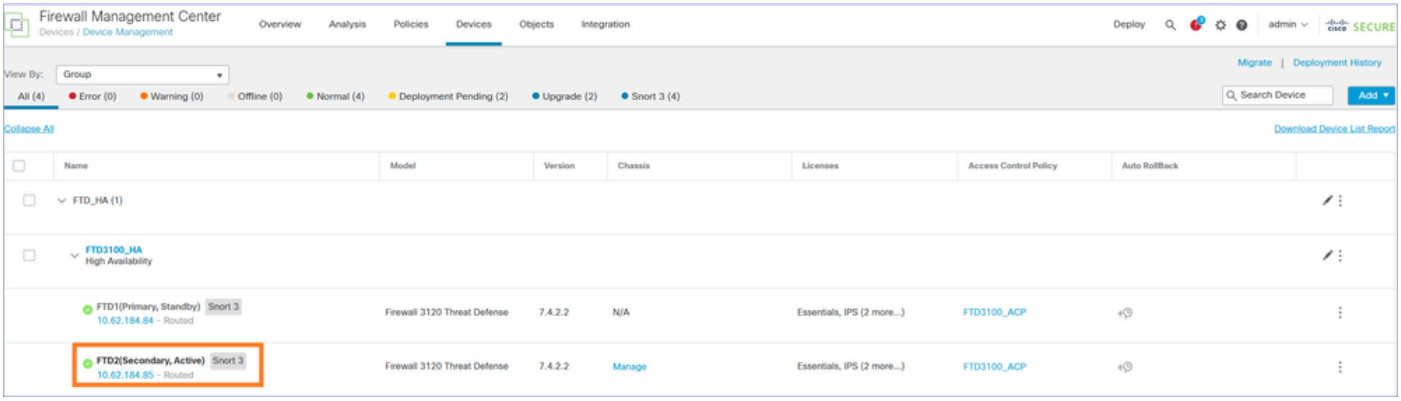
Riferimento: 'Esportare e importare la configurazione del dispositivo' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

Passaggio 2. Attivazione dell'FTD secondario

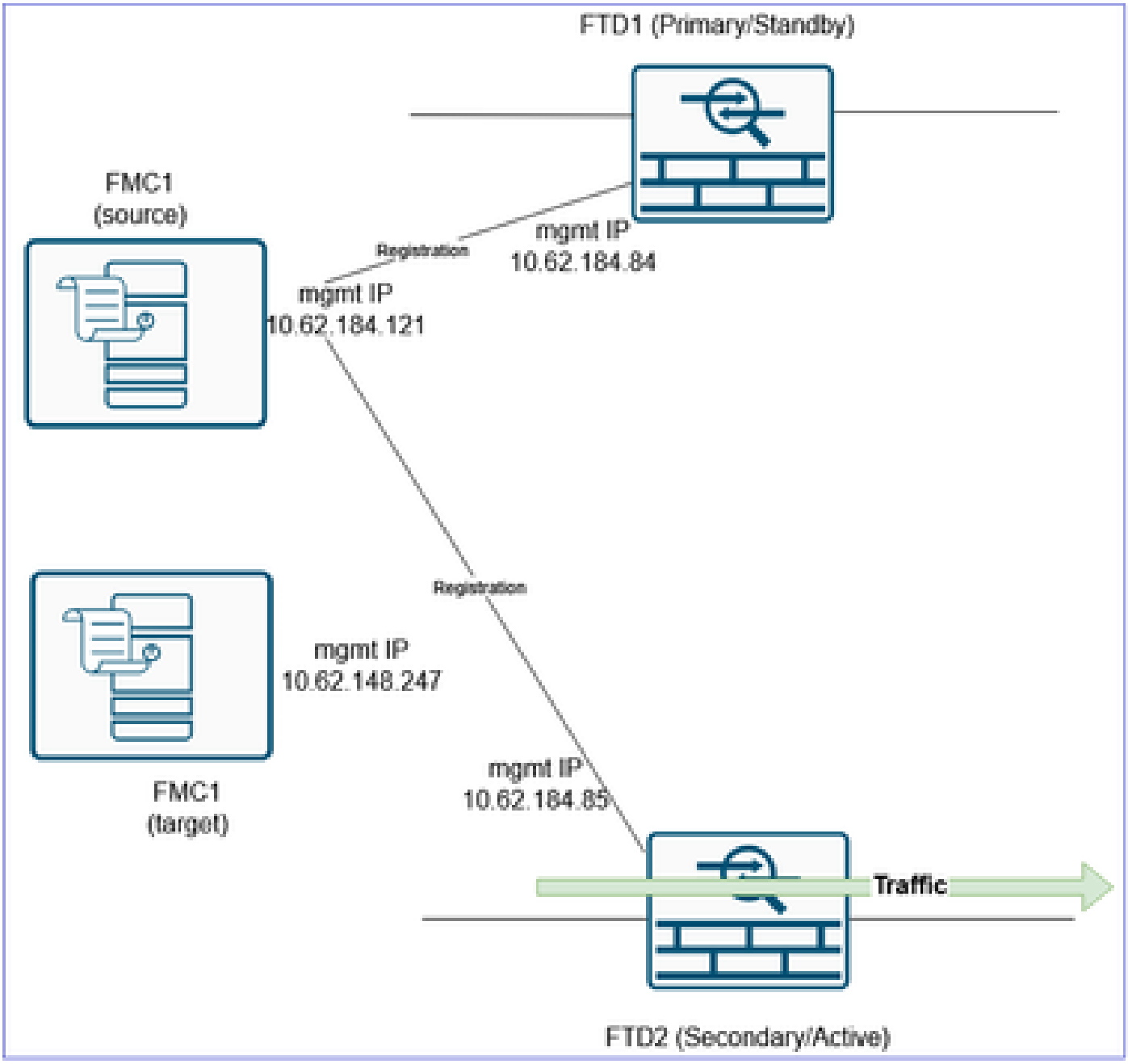
Passare a Dispositivi > Gestione dispositivi, selezionare la coppia FTD HA e selezionare Coppia switch attivo:



Il risultato è FTD1 (Principale/Standby) e FTD (Secondario/Attivo):

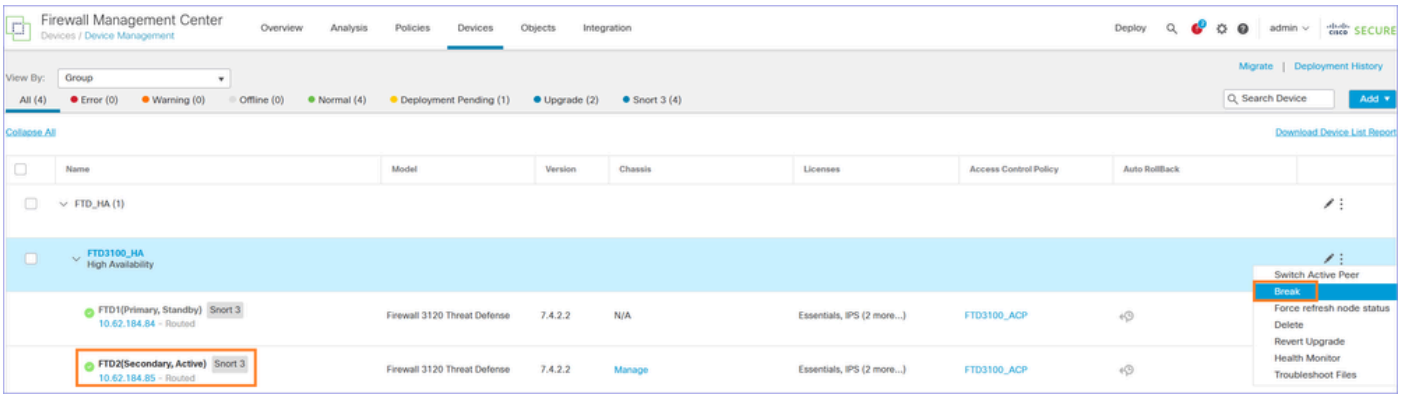


A questo punto, il traffico viene gestito dall'FTD secondario/attivo:

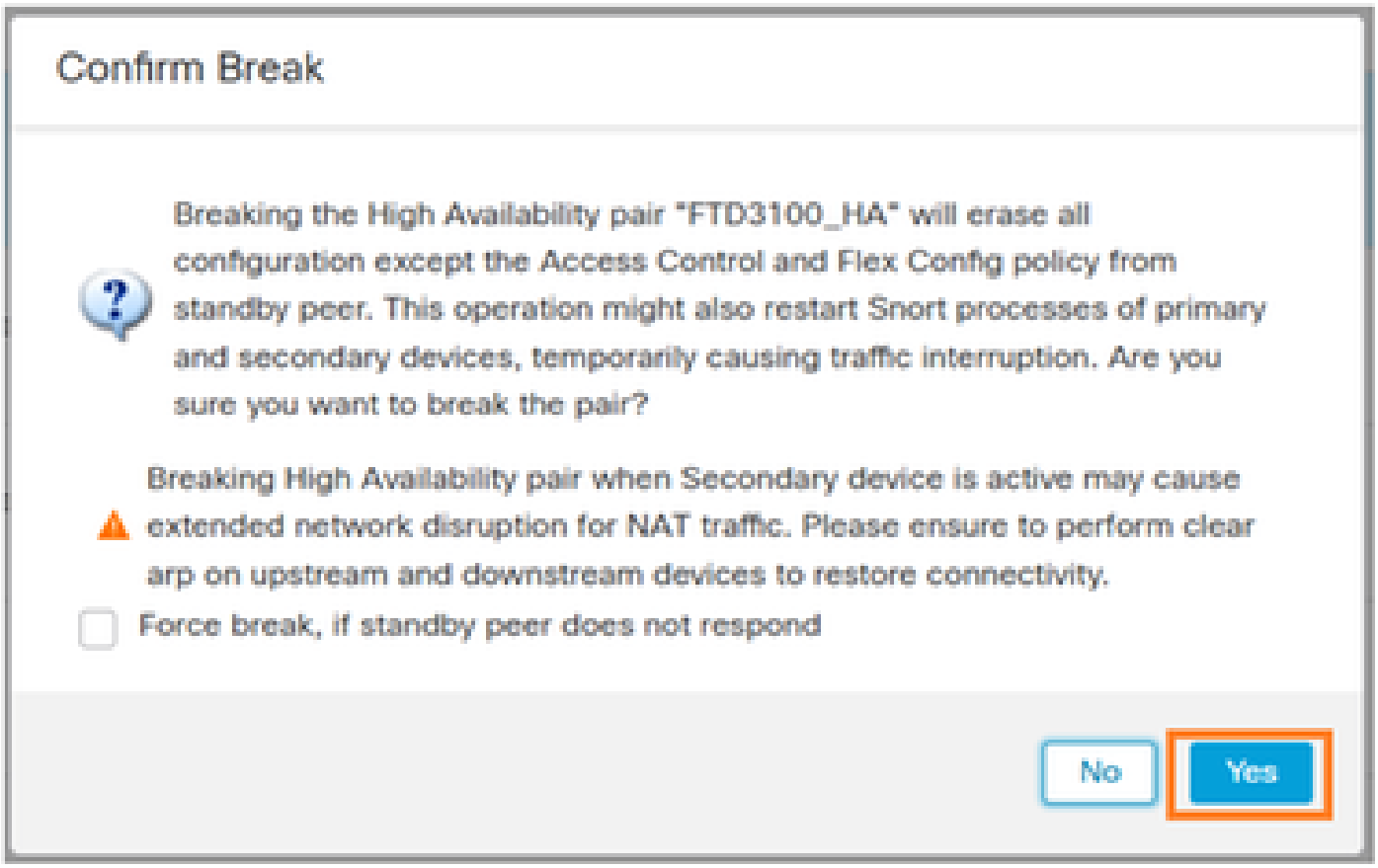


Passaggio 3. Interrompere l'FTD HA

Selezionare Devices > Device Management (Dispositivi > Gestione dispositivi) e Break the FTD HA:



Viene visualizzata questa finestra. Selezionare Sì



Nota: A questo punto è possibile riscontrare alcune interruzioni del traffico per alcuni secondi, dal momento che il motore Snort viene riavviato durante l'interruzione HA. Inoltre, come indicato nel messaggio, se si utilizza NAT e si verifica un'interruzione prolungata del traffico, valutare l'opportunità di cancellare la cache ARP sui dispositivi a monte e a valle.

Dopo aver interrotto la FTD HA, si dispone di due FTD autonomi su FMC.

Dal punto di vista della configurazione, l'FTD2 (ex-Active) dispone ancora della configurazione, ad eccezione della configurazione relativa al failover, e gestisce il traffico:

<#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
```

Nel FTD1 (ex-Standby) tutta la configurazione è stata rimossa:

<#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#

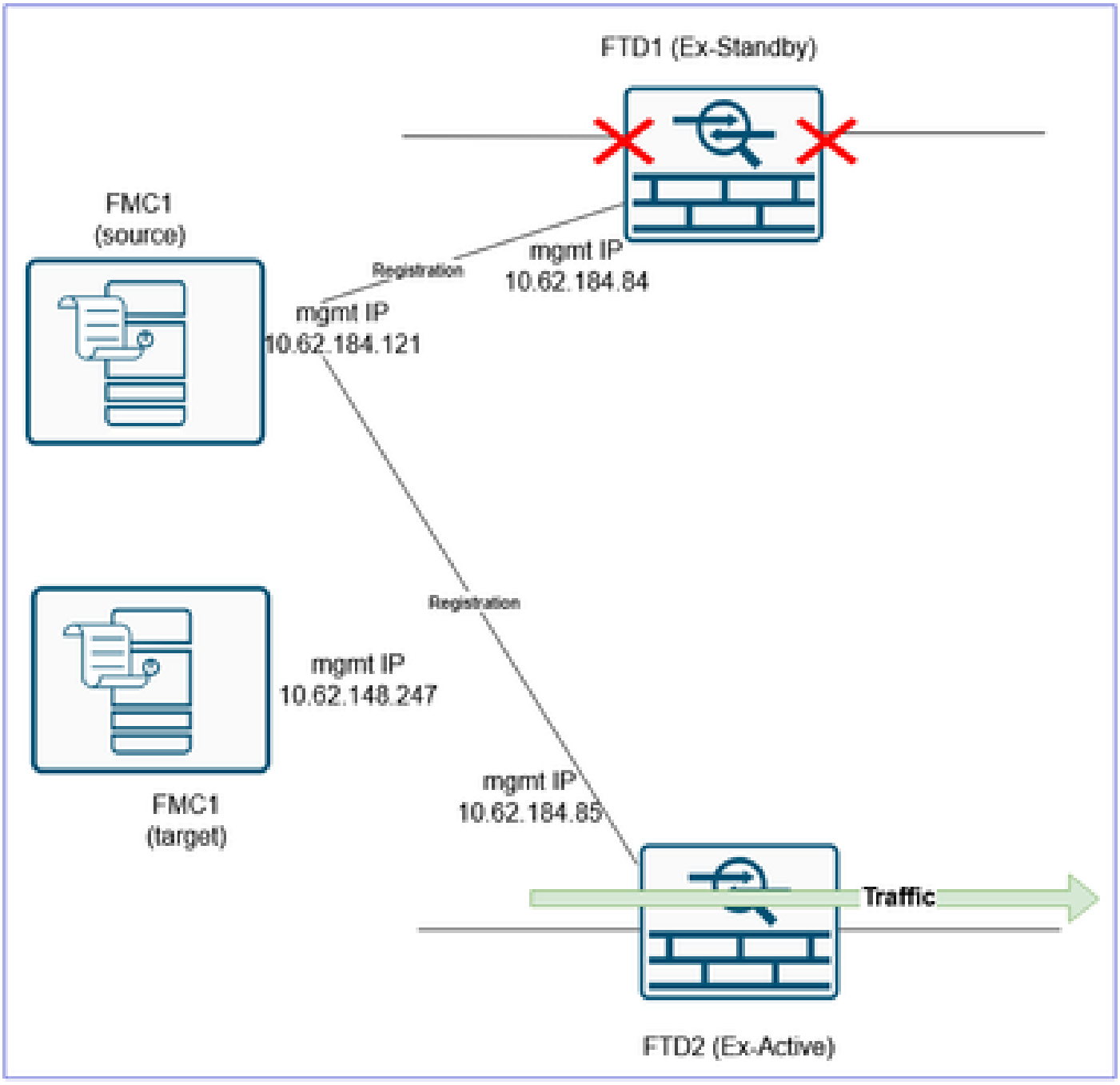
show interface ip brief

```
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
```

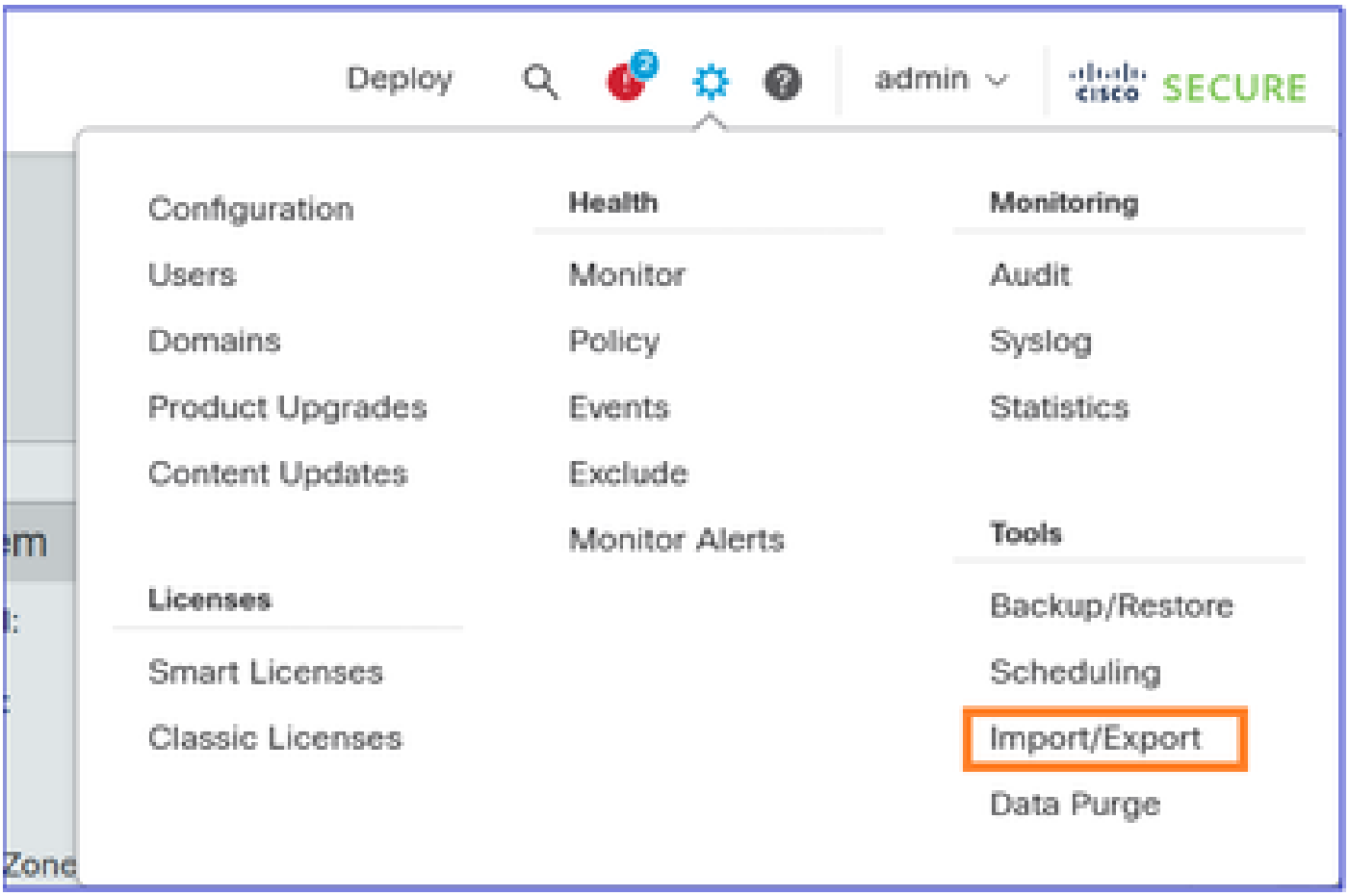
Passaggio 4. Isolare le interfacce dati FTD1 (ex primarie)

Scollegare i cavi dati dall'FTD1 (ex primario). Lasciare collegata solo la porta di gestione FTD.



Passaggio 5. Esportare i criteri condivisi FTD

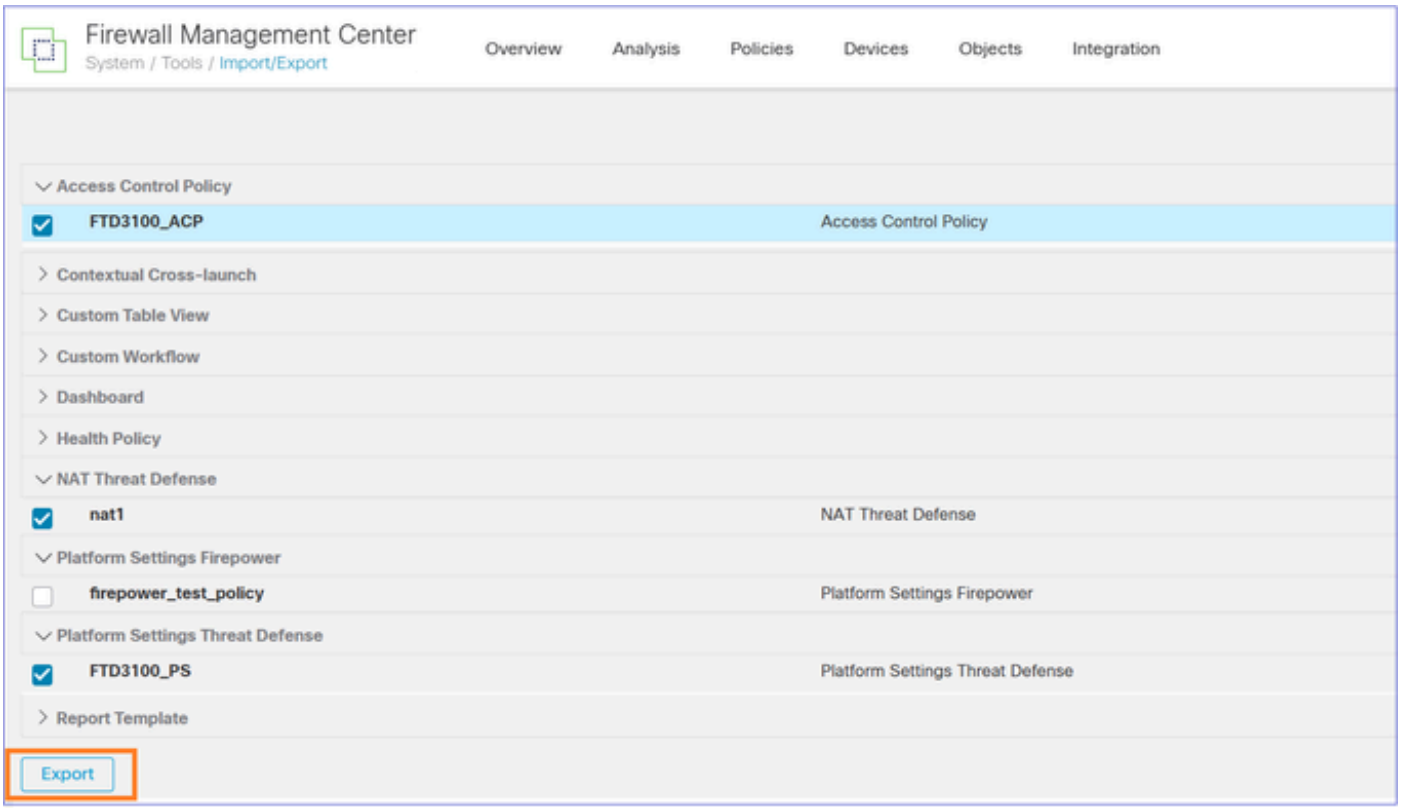
Passare a Sistema > Strumenti e selezionare Importa/Esporta:



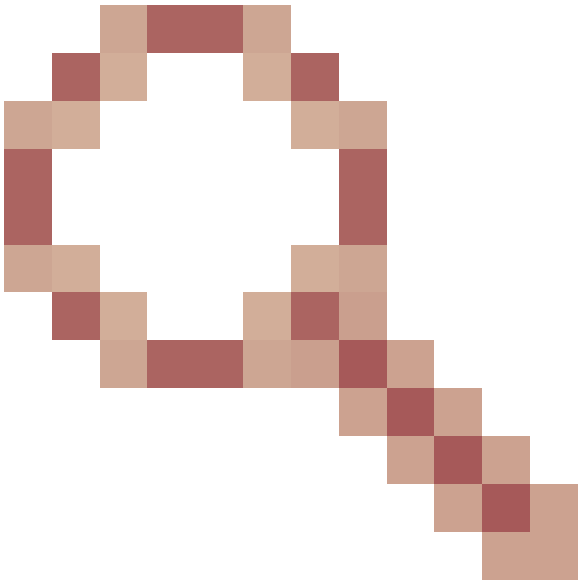
Esporta i vari criteri collegati al dispositivo. Accertarsi di esportare tutti i criteri collegati all'FTD, quali:

- Criteri di controllo di accesso (ACP)
- Criterio NAT (Network Address Translation)
- Criteri di integrità (se personalizzati)
- Impostazioni piattaforma FTD

e così via.



Nota: Al momento della scrittura, l'esportazione della configurazione relativa alla VPN non è supportata. Dopo la registrazione del dispositivo, è necessario riconfigurare manualmente la VPN nel FMC2 (FMC di destinazione).

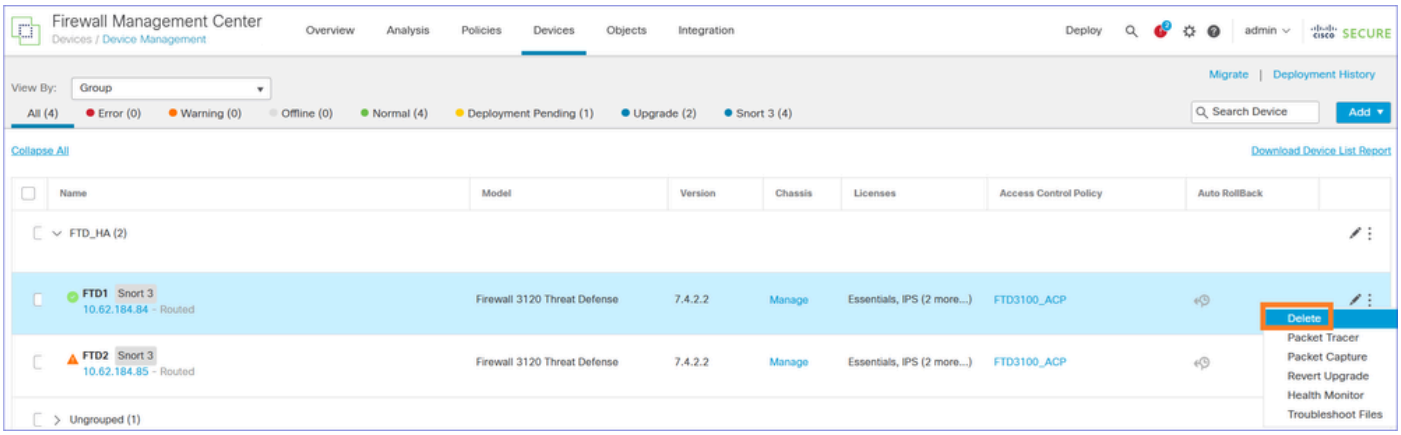


Miglioramento correlato: Cisco bug ID CSCwf05294

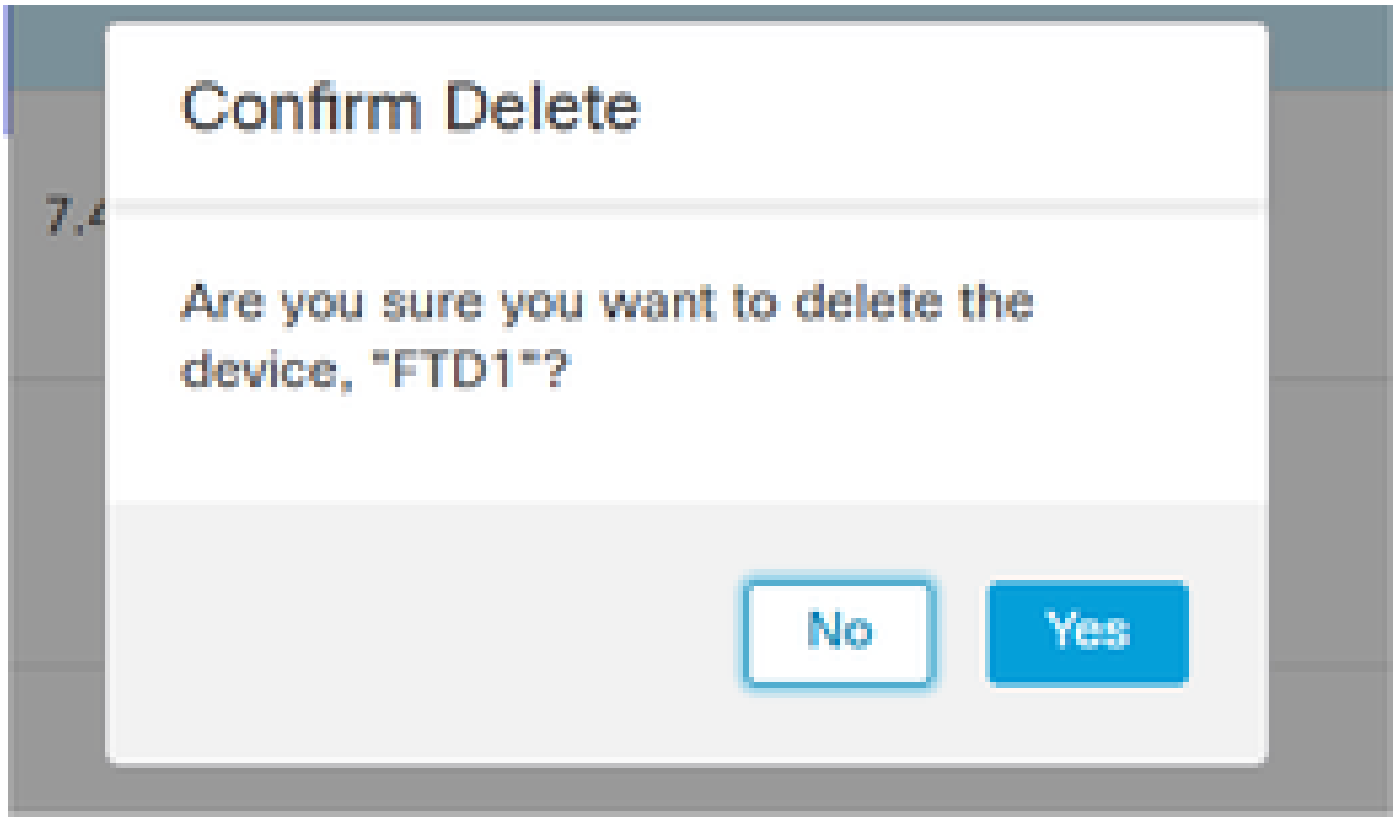
.

Il risultato è un file .sfo, ad esempio ObjectExport_20250306082738.sfo

Passaggio 6. Eliminare/annullare la registrazione dell'FTD1 (ex primario) dal CCP precedente/di origine



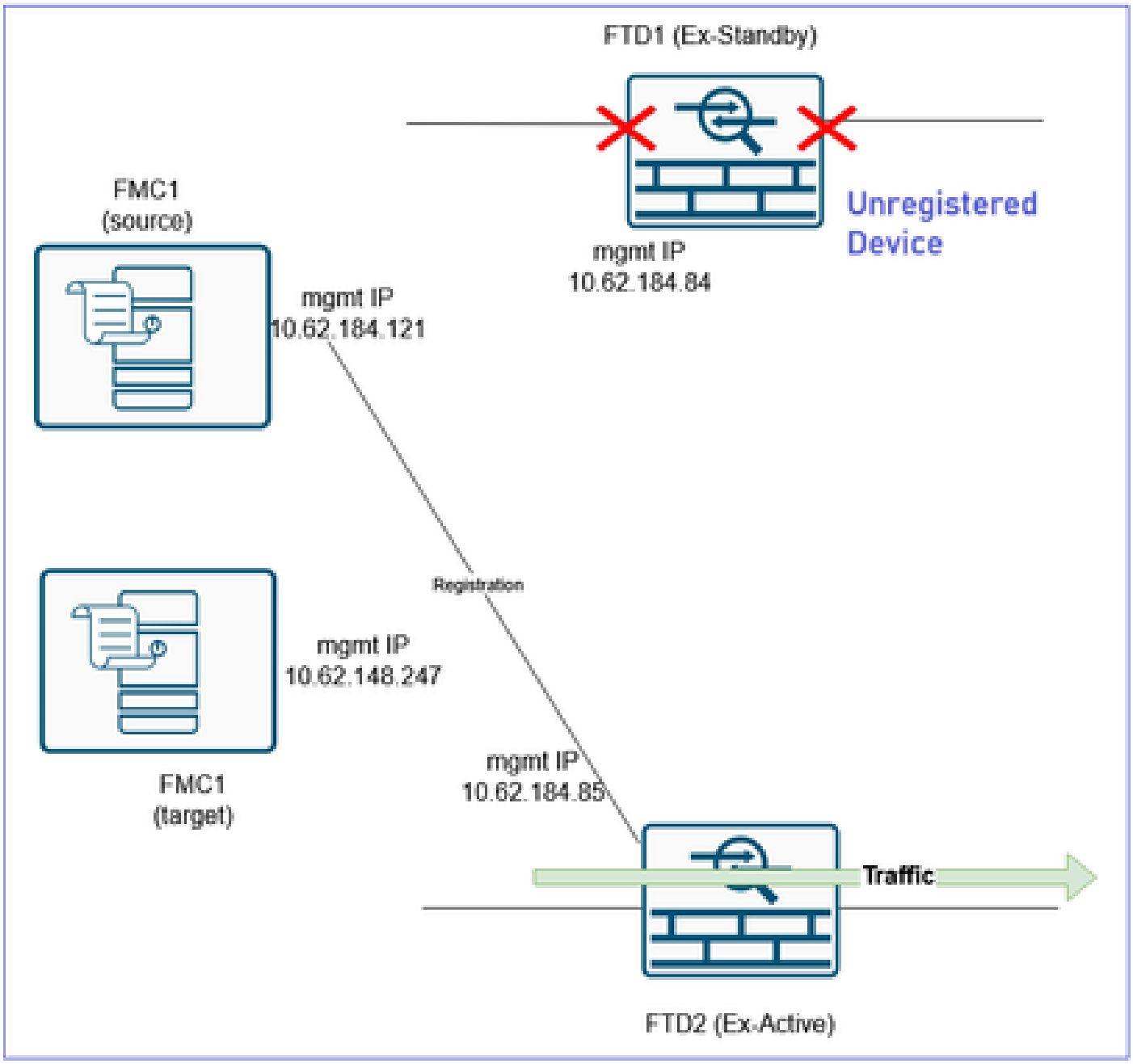
Confermare l'eliminazione del dispositivo:



Verifica CLI FTD1:

```
<#root>

>

show managers

No managers configured.

>
```

Stato corrente dopo l'eliminazione del dispositivo FTD1:



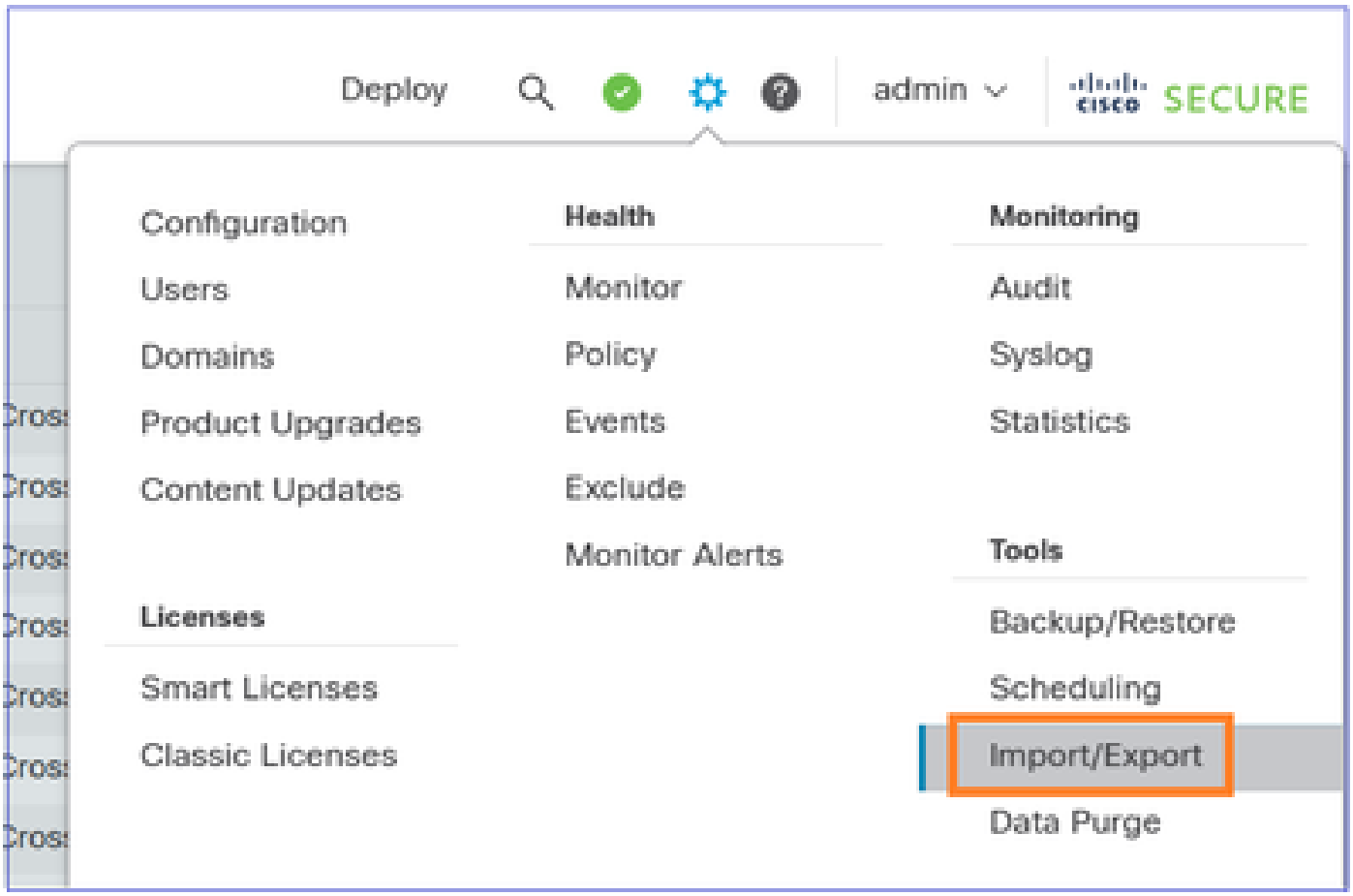
Passaggio 7. Importare l'oggetto di configurazione dei criteri FTD nel FMC2 (FMC di destinazione)

Nota: Il documento si concentra sulla migrazione di una singola coppia di HA FTD in un nuovo CCP. Se invece si intende eseguire la migrazione di più firewall che condividono gli stessi criteri (ad esempio, ACP, NAT) e gli stessi oggetti e si desidera eseguire questa operazione in più fasi, è necessario tenere conto di questi punti.
- Se nel FMC di destinazione esiste già un criterio con lo stesso nome, viene chiesto se:
r. Si desidera sostituire il criterio o
b. Crearne uno nuovo con un nome diverso. Verranno creati oggetti duplicati con nomi diversi (suffisso _1).

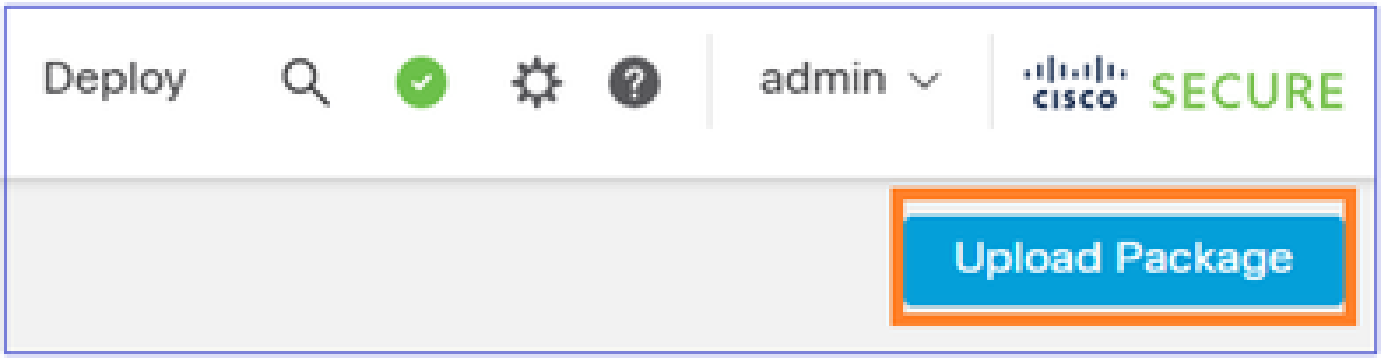
- Se si sceglie l'opzione 'b', nel passaggio 9 assicurarsi di riassegnare gli oggetti appena

creati ai criteri migrati (zone di sicurezza ACP, zone di sicurezza NAT, routing, impostazioni della piattaforma e così via).

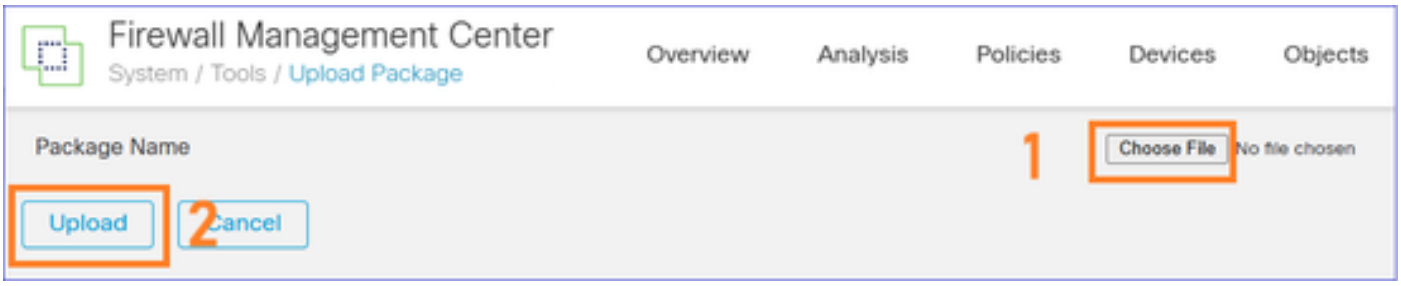
Accedere al FMC2 (FMC di destinazione) e importare l'oggetto SFO dei criteri FTD esportato nel passaggio 5:



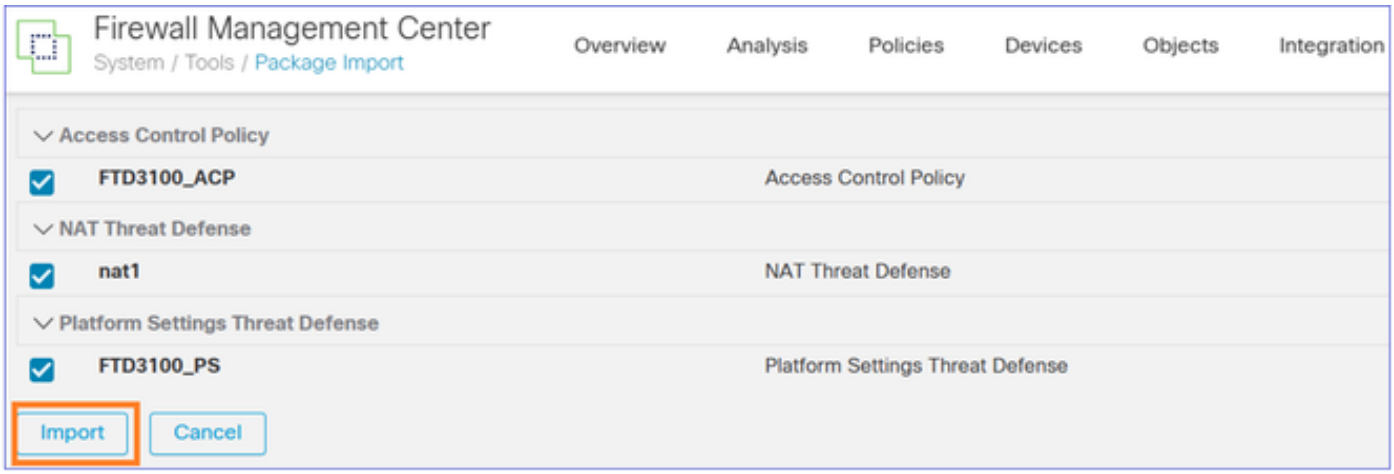
Selezionare Upload Packege:



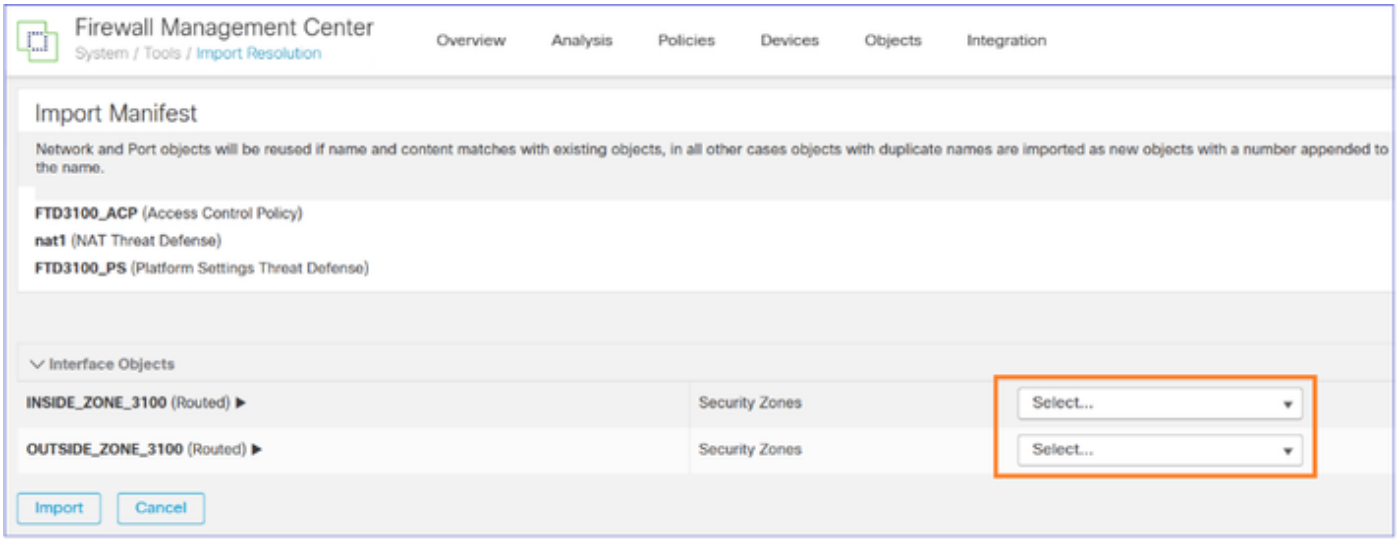
Caricare il file:



Importare i criteri:



Creare gli oggetti di interfaccia/le zone di sicurezza nel CCP2 (CCP di destinazione):



È possibile assegnare gli stessi nomi che avevano nell'FMC1 (FMC di origine):

Dopo aver selezionato Importa, un'attività inizia a importare i criteri correlati nel FMC2 (FMC di destinazione):

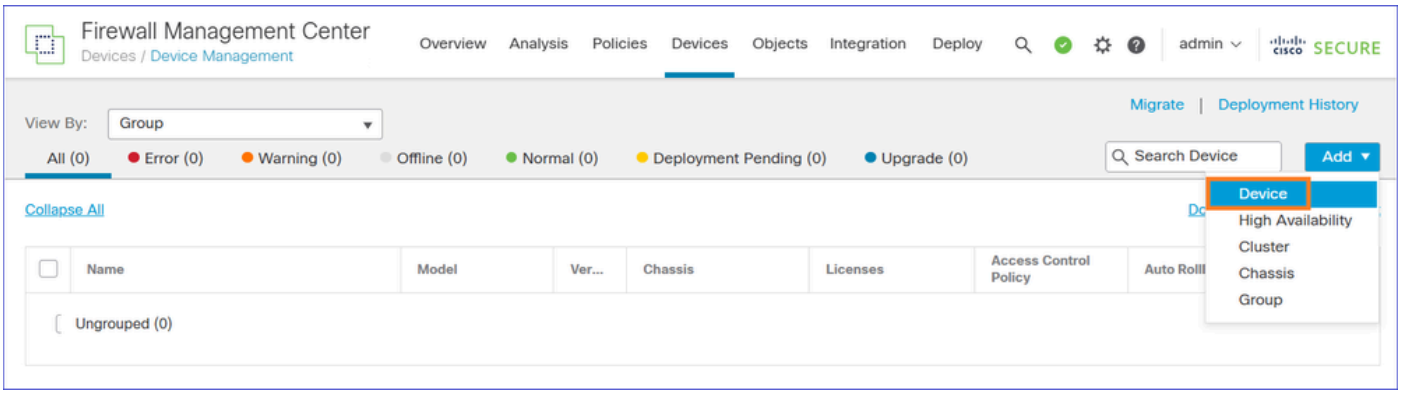
L'attività è stata completata:

Passaggio 8. Registrare l'FTD1 (ex primario) nell'FMC2

Andare alla CLI di FTD1 (ex-Primary) e configurare il nuovo manager:

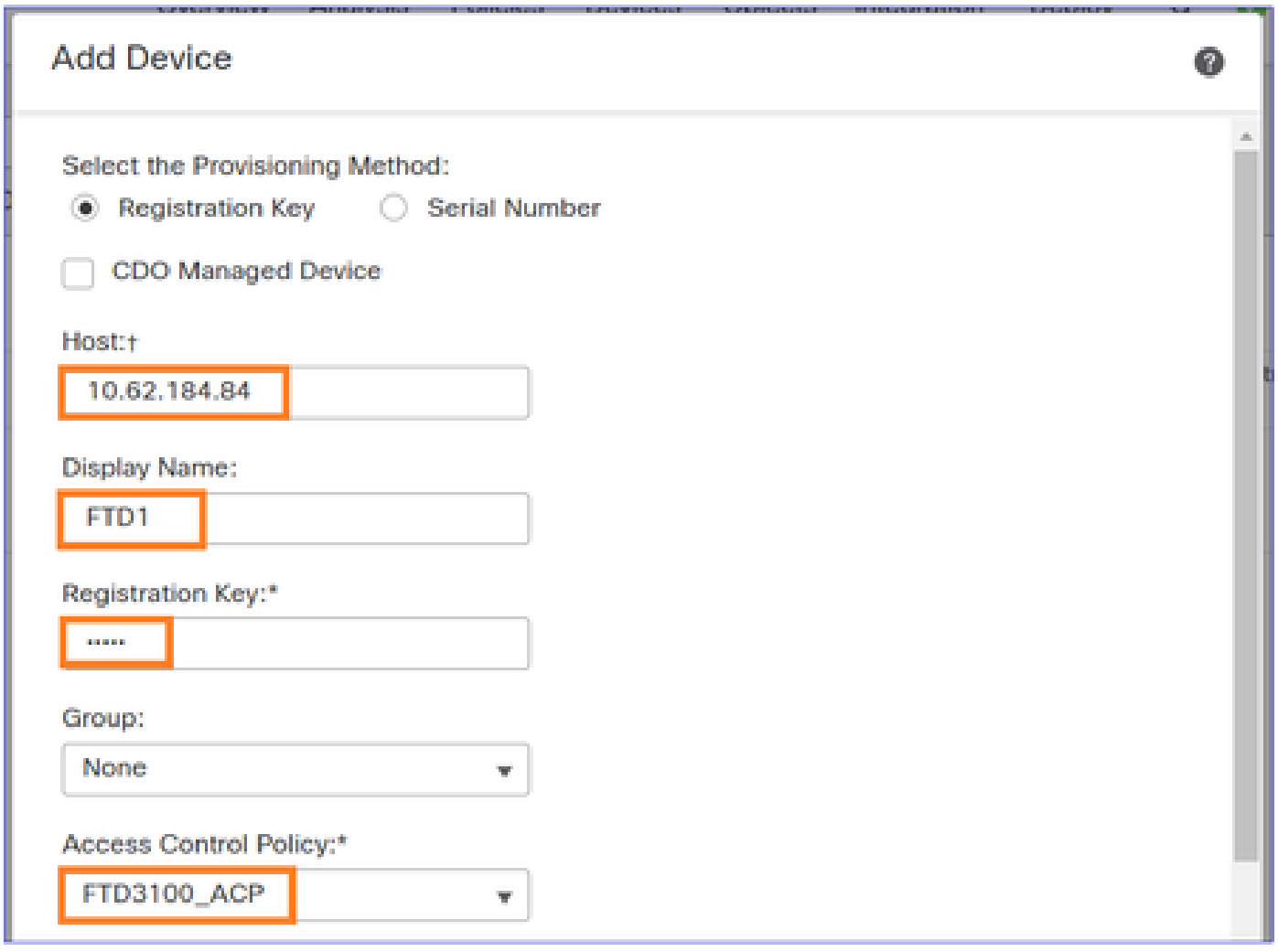
```
<#root>

>

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.

>
```

Passare a FMC2 (FMC di destinazione) UI Devices > Device Management (Gestione dispositivi) e Aggiungere il dispositivo FTD:

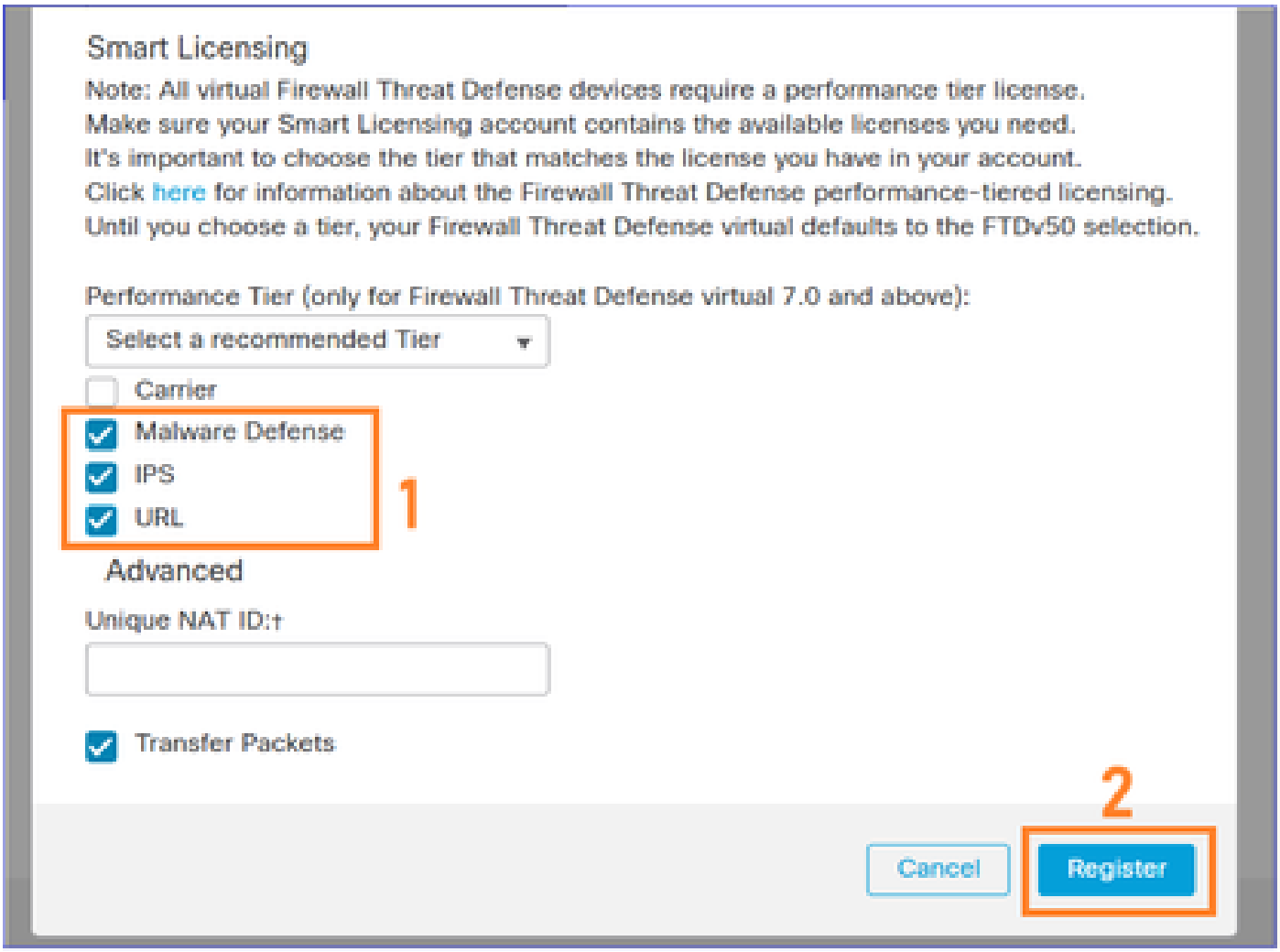


Se la registrazione del dispositivo non riesce, consultare questo documento per la risoluzione del problema: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

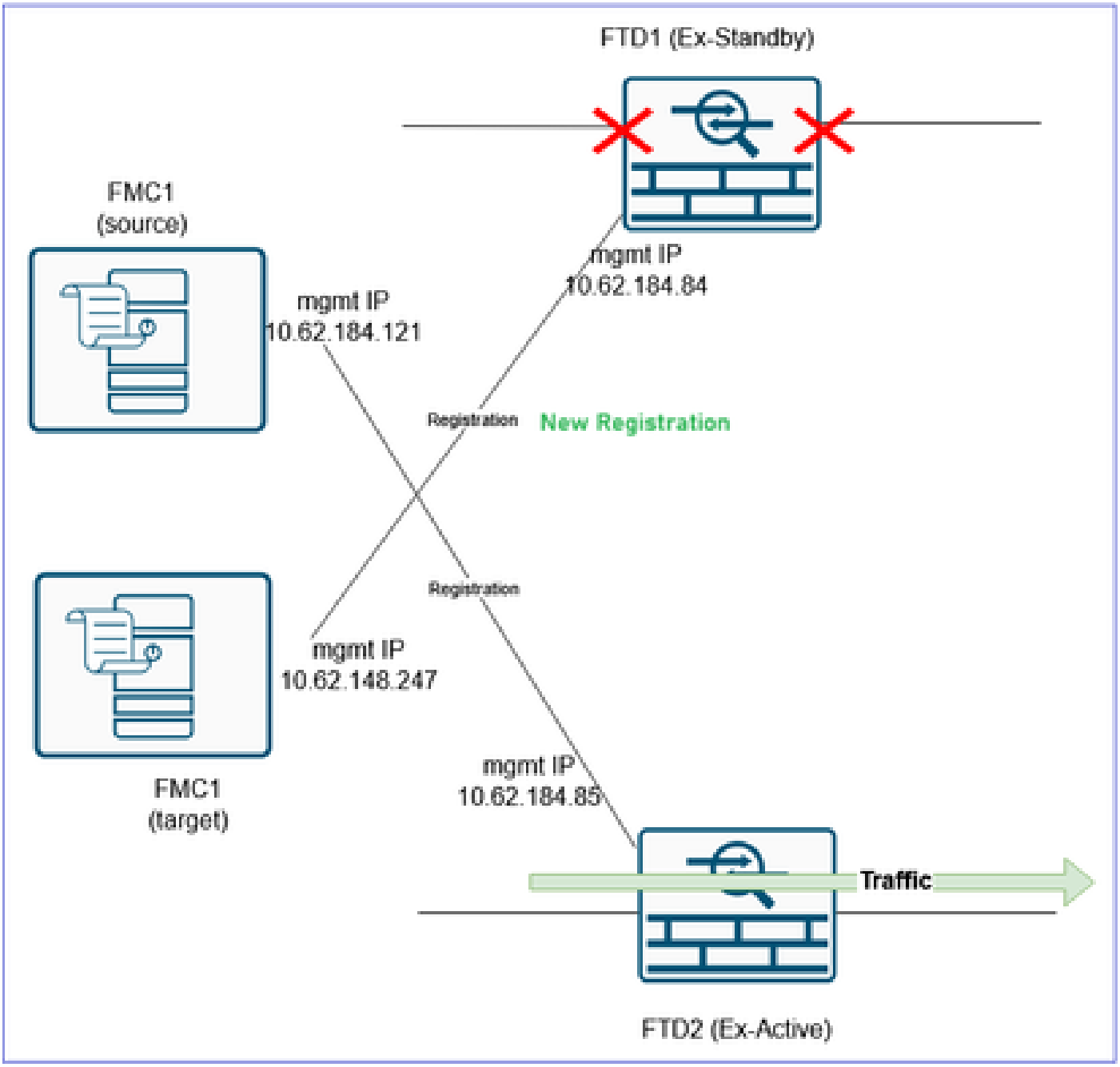
Assegnare il criterio di controllo dell'accesso importato nel passaggio precedente:



Applicare le licenze necessarie e registrare il dispositivo:



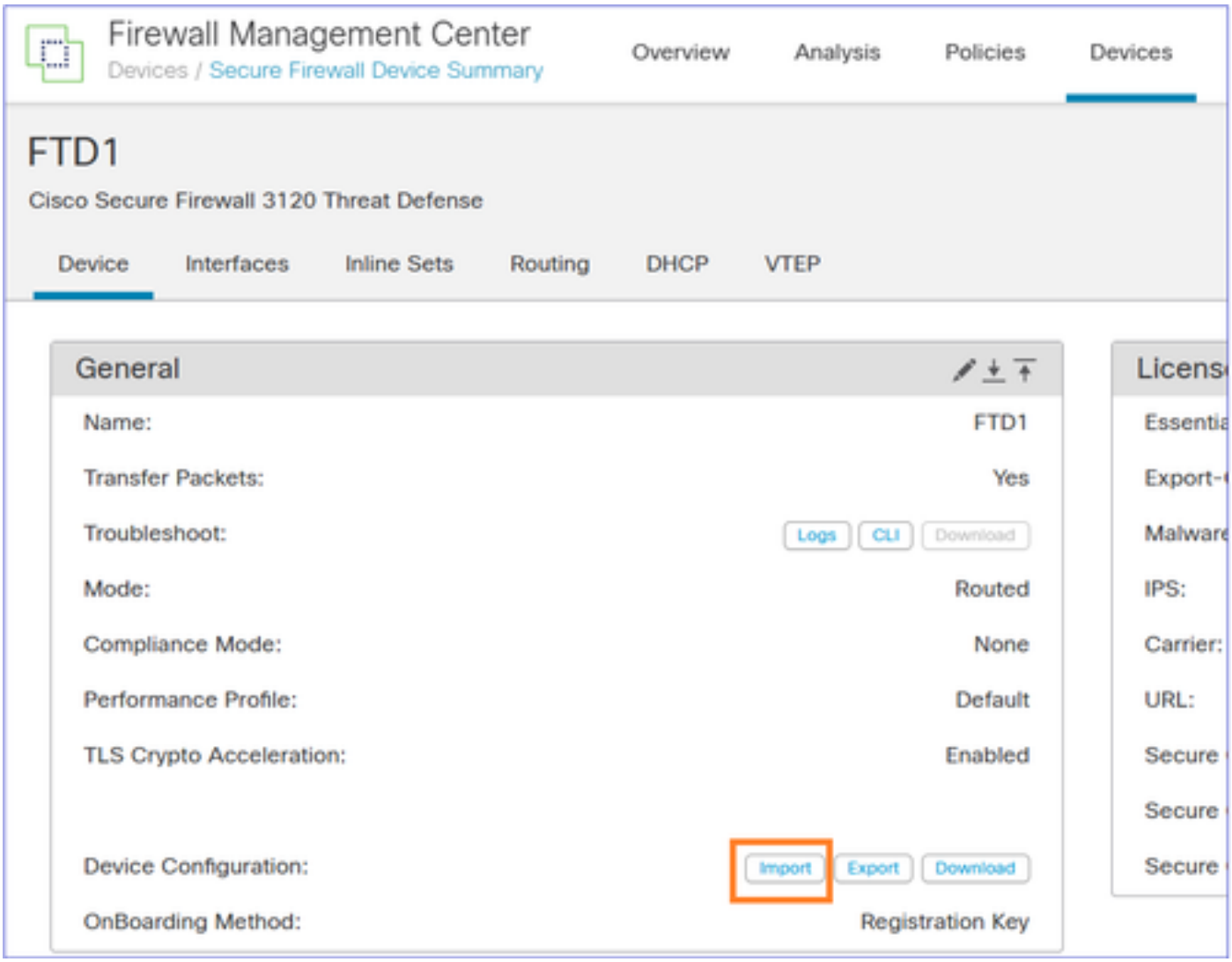
Il risultato:



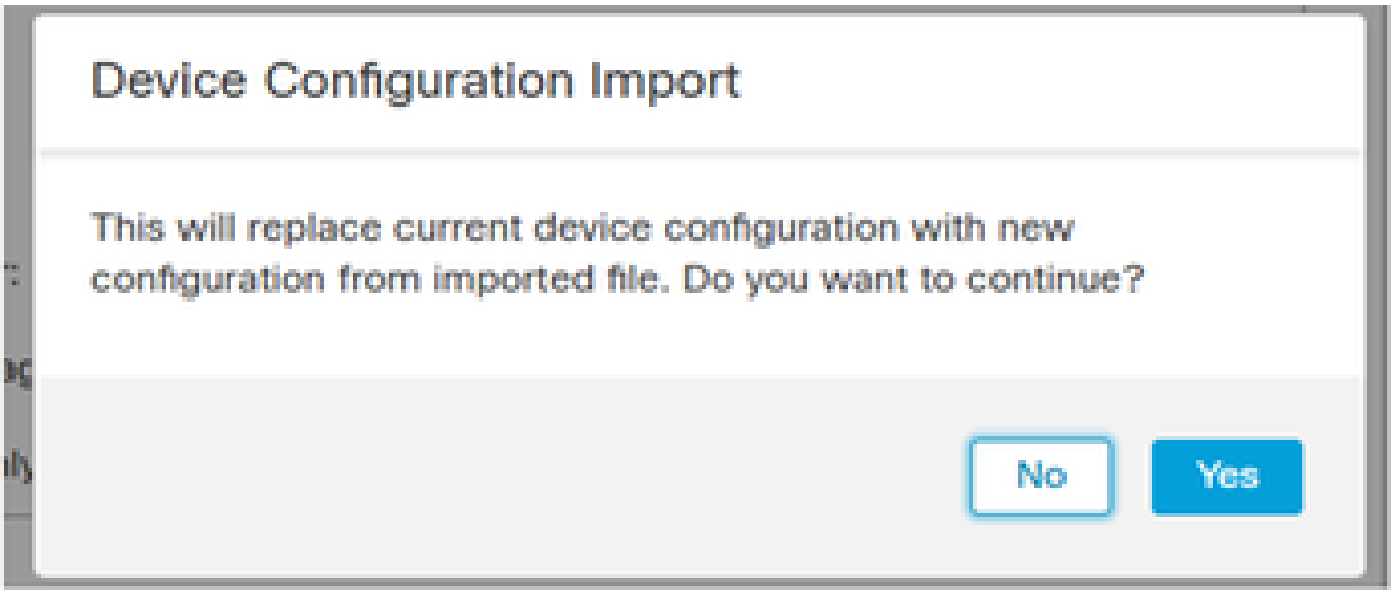
Passaggio 9. Importare l'oggetto configurazione dispositivo FTD nel FMC2 (FMC di destinazione)

Accedere al FMC2 (FMC di destinazione), selezionare Devices > Device Management (Dispositivi > Gestione dispositivi) e modificare il dispositivo FTD registrato nel passaggio precedente.

Passare alla scheda Device (Dispositivo) e Importare l'oggetto SFO dei criteri FTD esportato nel passaggio 2:

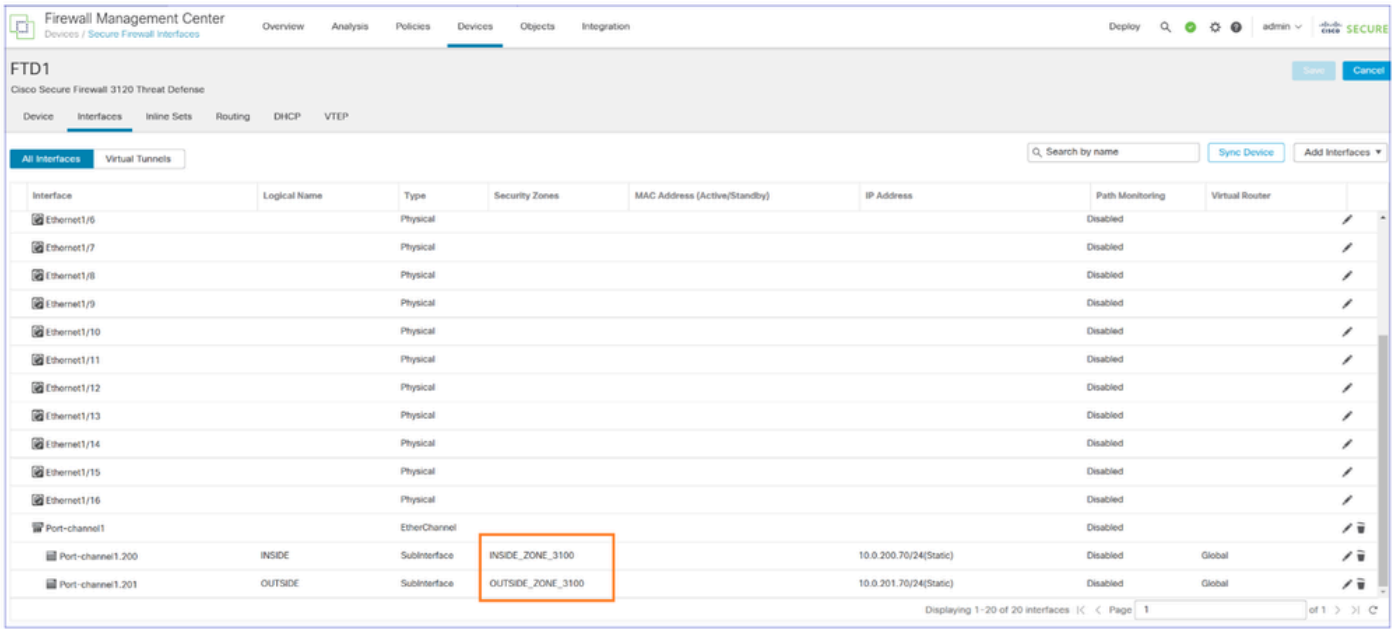


Nota: Nel caso in cui nel Passaggio 7 sia stata selezionata l'opzione 'b' (Creazione di un nuovo criterio), assicurarsi di riassegnare gli oggetti appena creati ai criteri migrati (Aree di sicurezza ACP, Aree di sicurezza NAT, Routing, Impostazioni piattaforma e così via).



Viene avviata un'operazione del CCP.

La configurazione del dispositivo viene applicata sull'FTD1, ad esempio zone di sicurezza, ACP, NAT e così via:



⚠ Attenzione: Se si dispone di un punto ACP che si espande a molti elementi di controllo dell'accesso, il completamento del processo di compilazione del punto ACP (compilazione delle corrispondenze) può richiedere diversi minuti. È possibile utilizzare questo comando per verificare lo stato della compilazione del provider di servizi di audioconferenza:

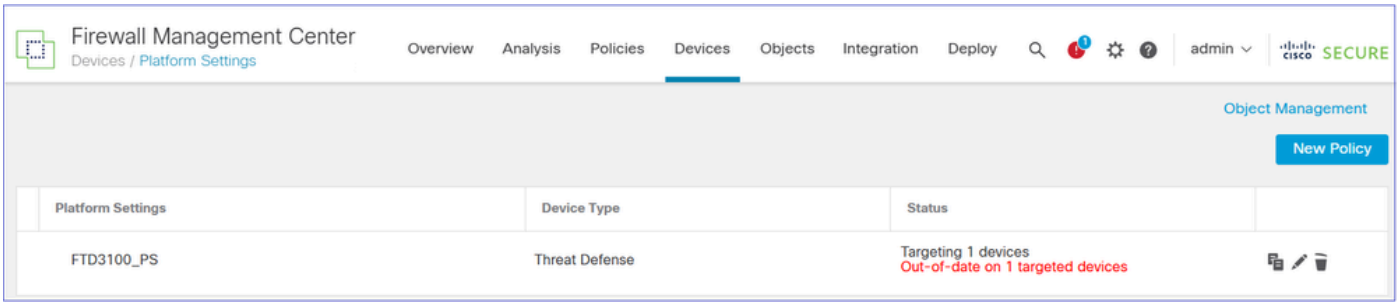
```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

Passaggio 10. Completare la configurazione FTD

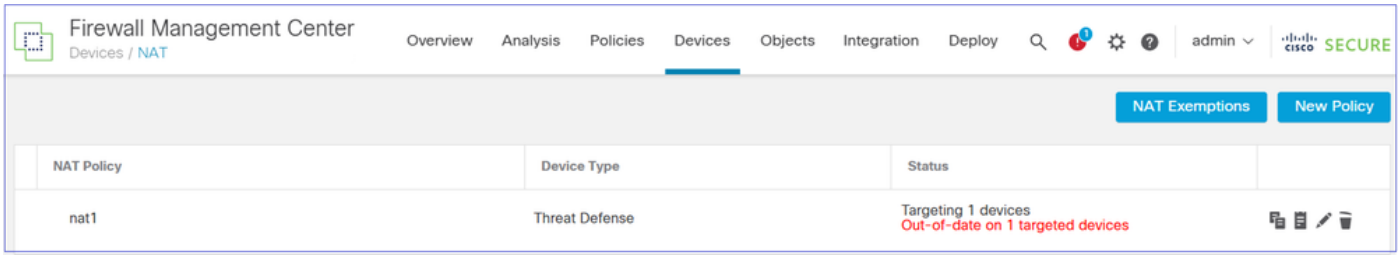
A questo punto l'obiettivo è configurare tutte le funzionalità che possono ancora mancare da FTD1 dopo la registrazione al FMC2 (FMC di destinazione) e l'importazione dei criteri del dispositivo.

Verificare che criteri quali NAT, Impostazioni piattaforma, QoS e così via siano corretti. sono assegnati all'FTD. I criteri sono assegnati ma la distribuzione è in sospeso.

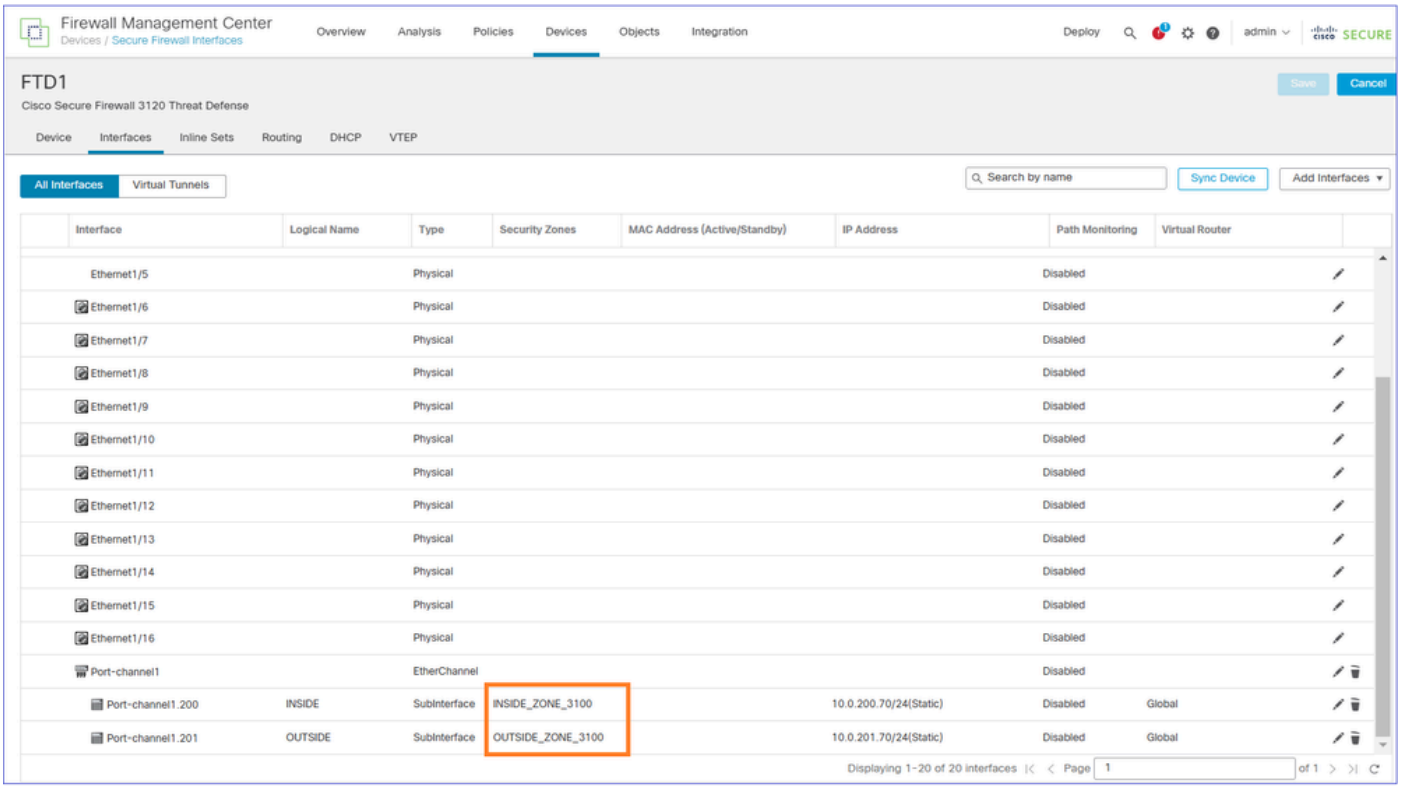
Ad esempio, le impostazioni della piattaforma vengono importate e assegnate al dispositivo, ma in attesa della distribuzione:



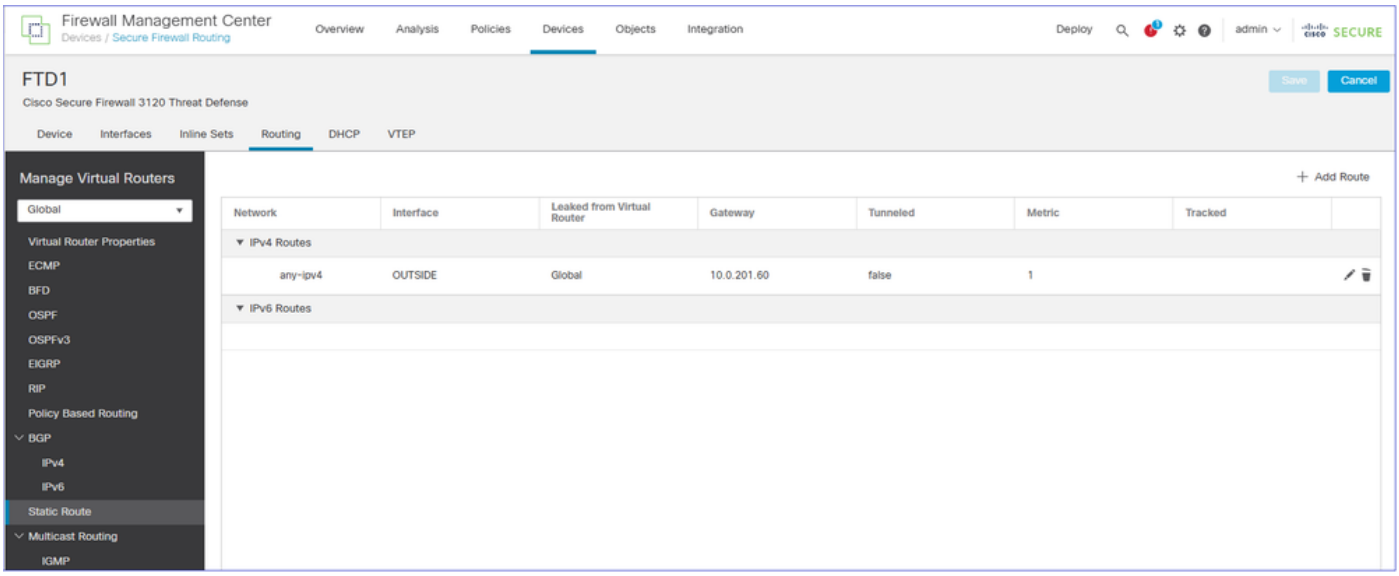
Se NAT è configurato, il criterio NAT viene importato e assegnato al dispositivo, ma in attesa della distribuzione:



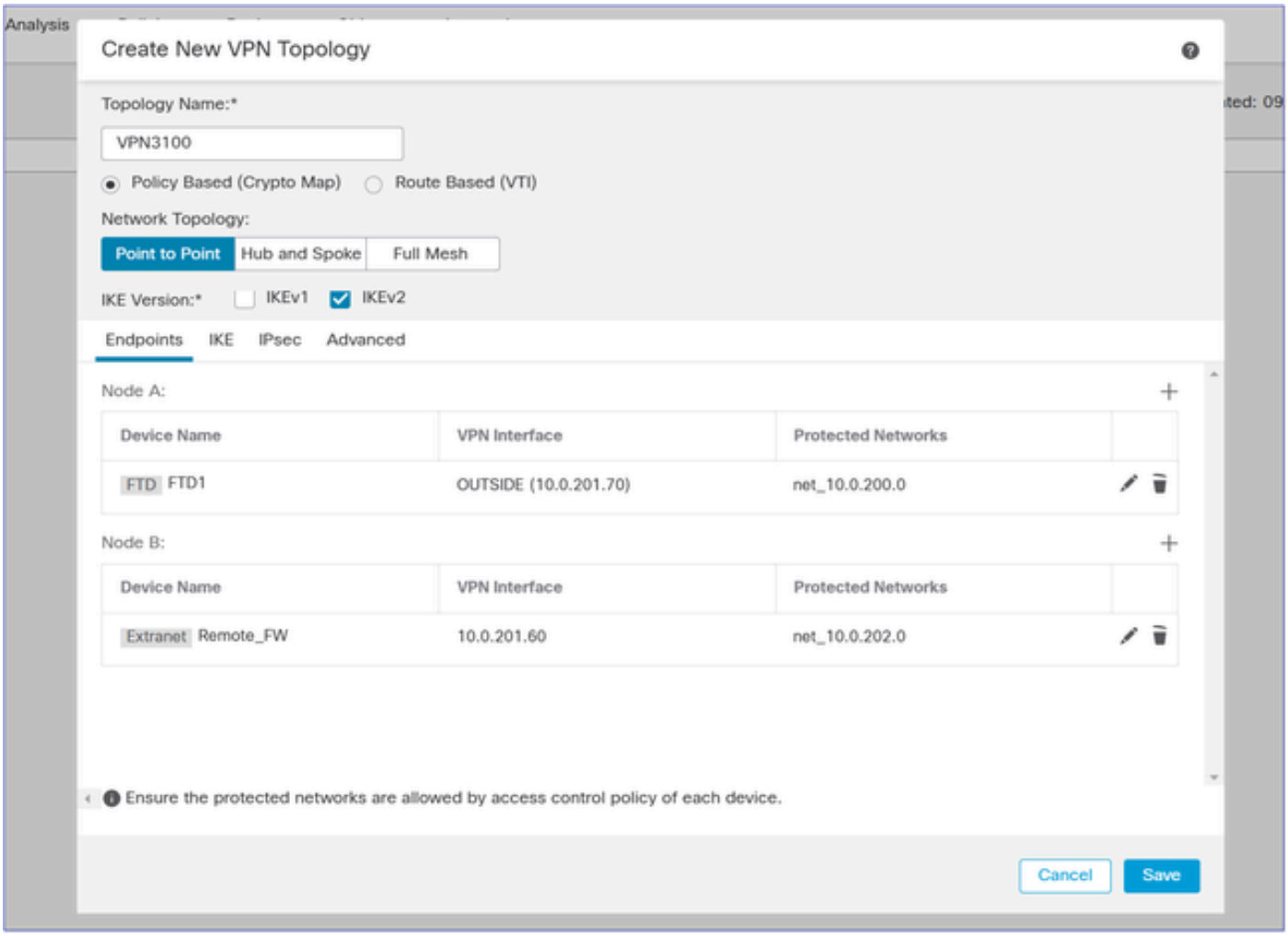
Le aree di sicurezza vengono applicate alle interfacce:



La configurazione del routing viene applicata al dispositivo FTD:



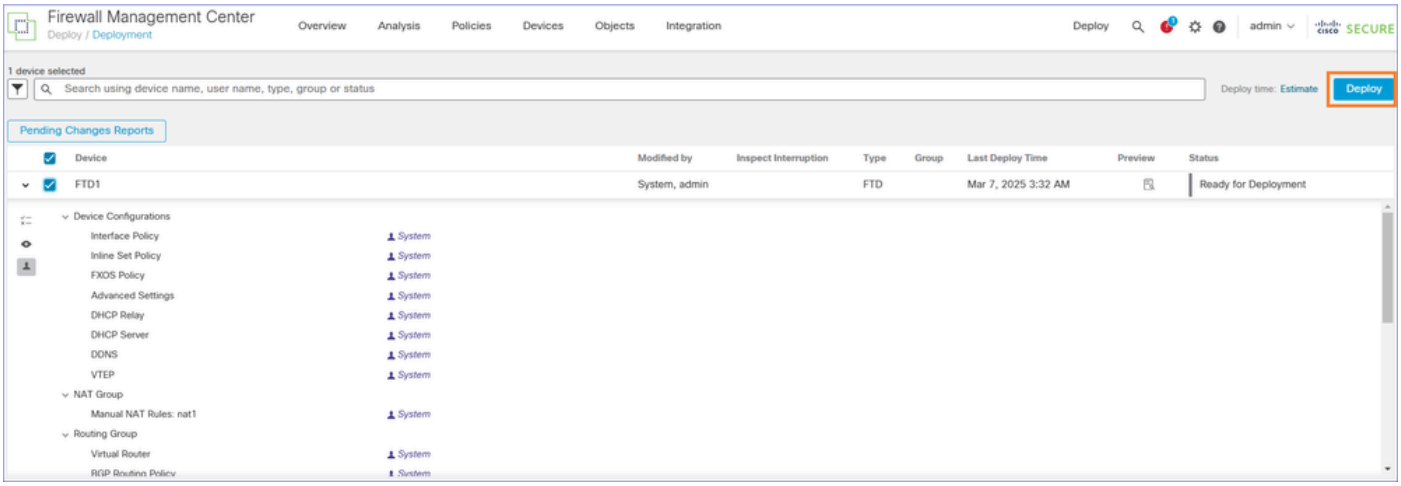
Nota: È il momento di configurare i criteri che non è stato possibile migrare automaticamente (ad esempio, le VPN).



Nota: Se l'FTD di cui è stata eseguita la migrazione dispone di peer VPN da sito a sito che

vengono anch'essi migrati nel FMC di destinazione, è necessario configurare la VPN dopo aver spostato tutti gli FTD nel FMC di destinazione.

Distribuire le modifiche in sospeso:



Passaggio 11. Verificare la configurazione FTD distribuita

A questo punto, l'obiettivo è verificare dalla CLI di FTD che tutta la configurazione sia in atto.

Il suggerimento è quello di confrontare l'output "show running-config" di entrambi gli FTD. Per il confronto è possibile utilizzare strumenti quali WinMerge o diff.

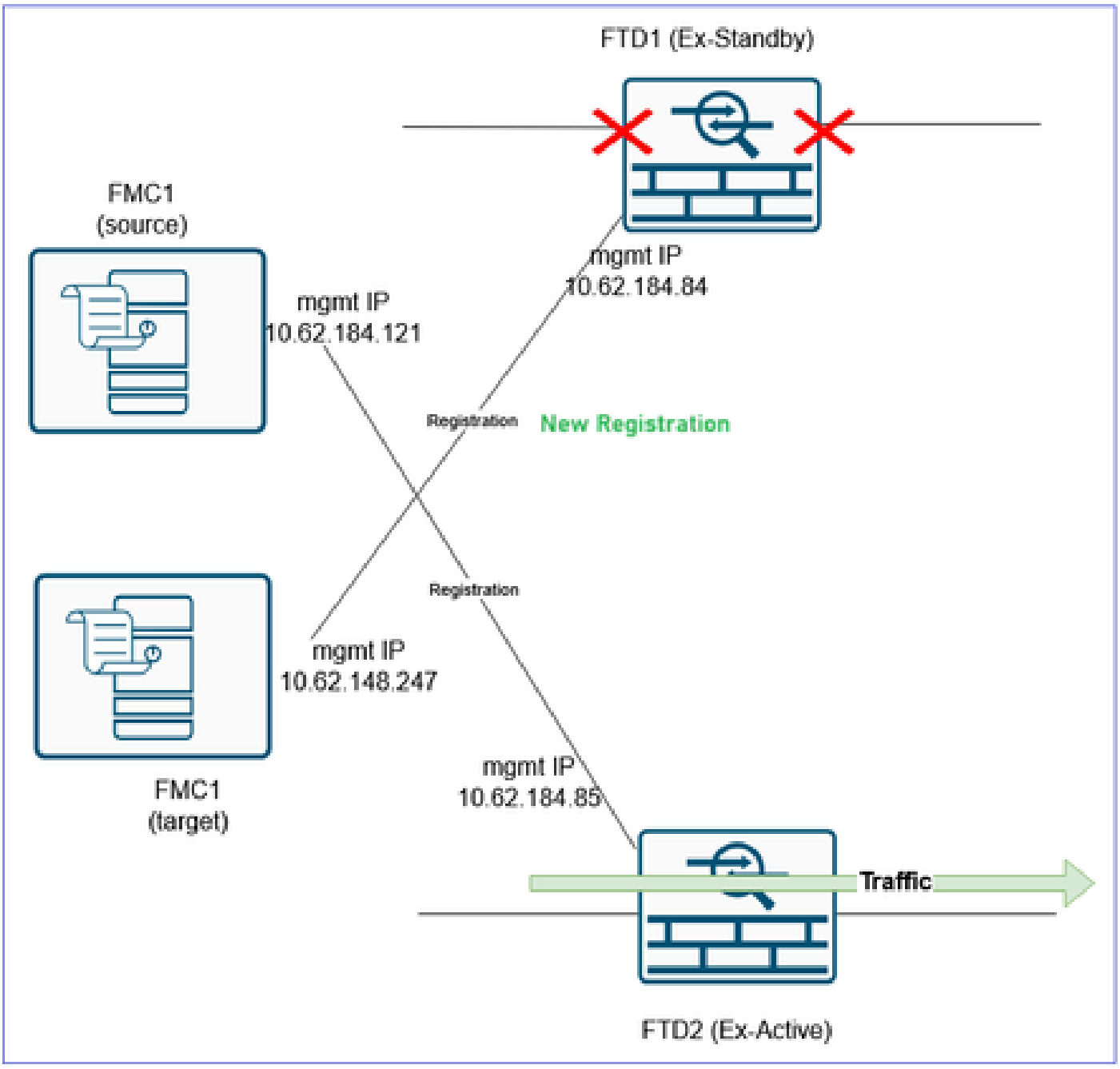
Le differenze visibili e normali sono le seguenti:

- Numero di serie del dispositivo
- Descrizioni interfaccia
- ID regole ACL
- Cryptochecksum della configurazione

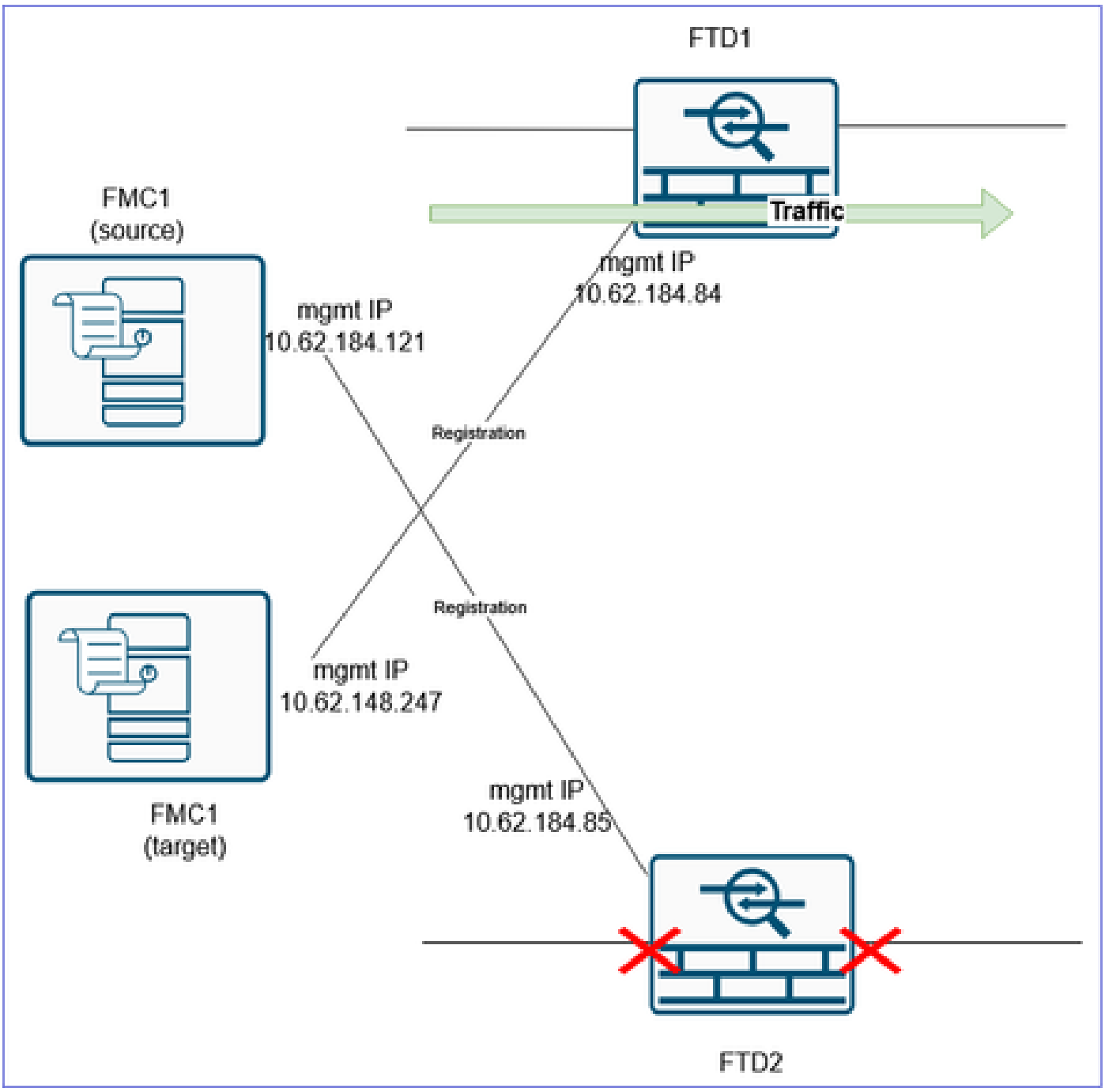
Passaggio 12. Eseguire il cutover

In questa fase, l'obiettivo è quello di far passare il traffico dall'FTD2 che sta attualmente gestendo il traffico ed è ancora registrato al FMC precedente/di origine, all'FTD1 registrato al FMC di destinazione.

Prima:


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
mgmt IP
10.62.184.85
FMC1
(target)
Traffic
FTD2 (Ex-Active)

Dopo:



⚠ Attenzione: Disporre una MW per eseguire il cutover. Durante il passaggio, si verificherà un'interruzione del traffico fino a quando tutto il traffico verrà deviato all'FTD1, le VPN verranno ristabilite e così via.

⚠ Attenzione: Non avviare il cutover a meno che la compilazione ACP non sia stata completata (vedere il passaggio 10 sopra).

⚠ Avviso: Scollegare i cavi dati dall'FTD2 o chiudere le relative porte dello switch. In caso contrario, è possibile gestire il traffico con entrambi i dispositivi.

⚠ Attenzione: Poiché entrambi i dispositivi utilizzano la stessa configurazione IP, è necessario

⚠ aggiornare la cache ARP dei dispositivi L3 adiacenti. Valutare l'opportunità di cancellare manualmente la cache ARP dei dispositivi adiacenti per accelerare il taglio del traffico.

Suggerimento: Potete anche inviare un pacchetto GARP e aggiornare la cache ARP dei dispositivi adiacenti usando il comando FTD CLI:

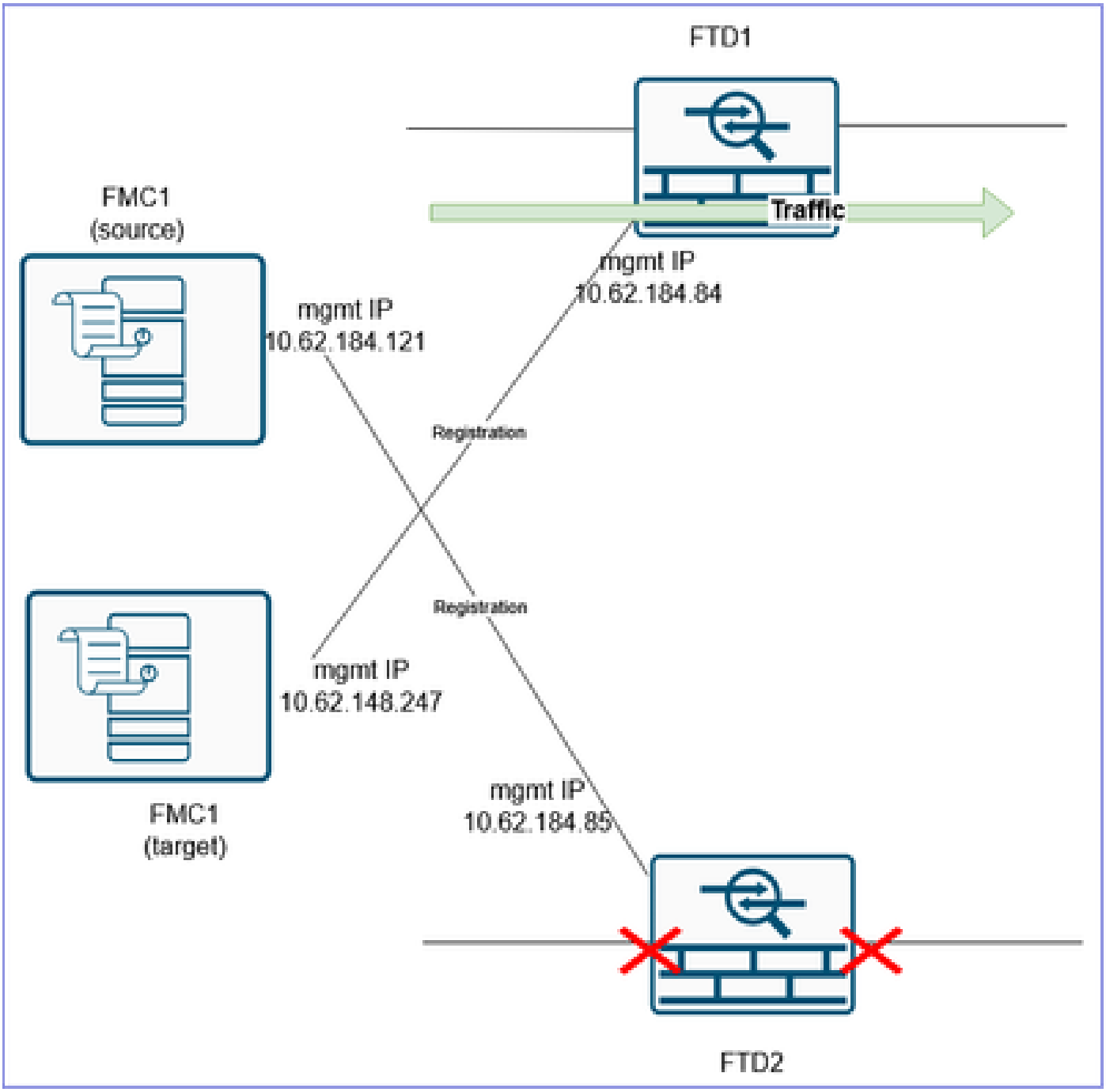
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

È necessario ripetere questo comando per ogni IP di proprietà del firmware. Pertanto, può essere più rapido cancellare la cache ARP dei dispositivi adiacenti piuttosto che inviare pacchetti GARP per ogni IP di proprietà del firewall.

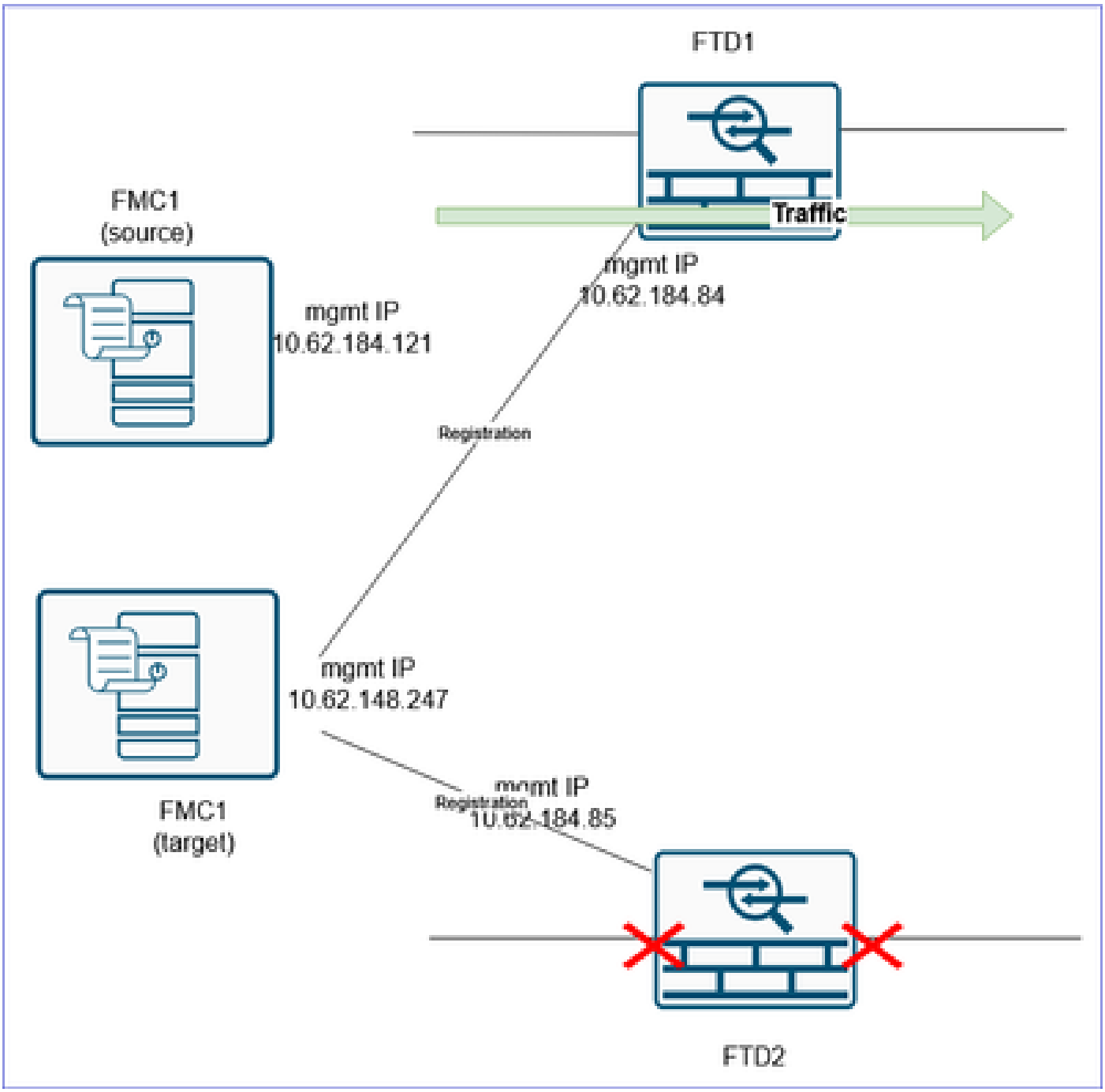
Passaggio 13. Migrare il secondo FTD al CCP2 (CCP di destinazione)

L'ultimo punto è riformare la coppia HA. A tal fine, è necessario eliminare l'FTD2 dal CCP1 (CCP di origine) e registrarlo nel CCP2 (CCP di destinazione).

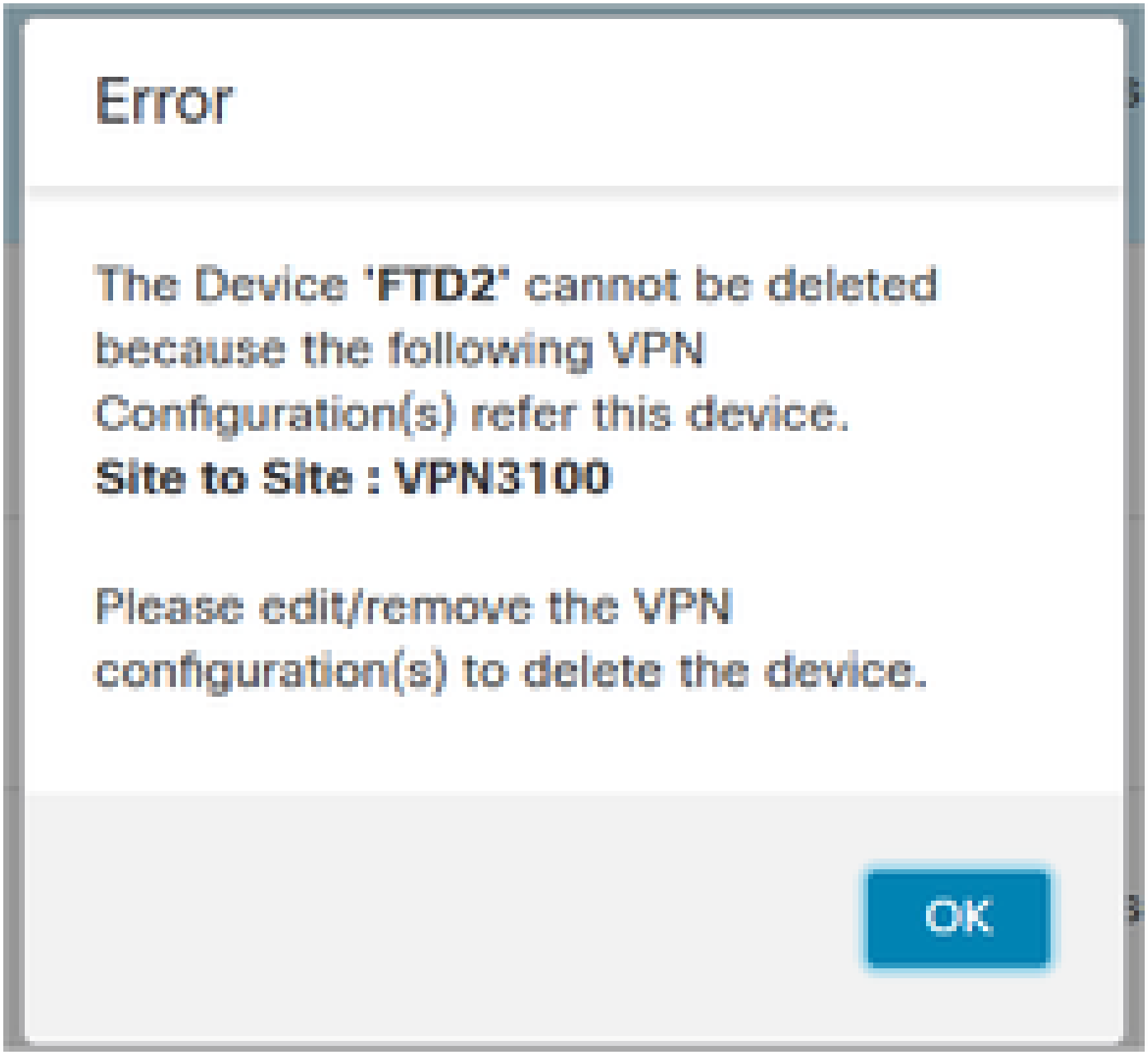
Prima:


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

Dopo:



Se all'FTD2 è collegata una configurazione VPN, è necessario rimuoverla prima di eliminare l'FTD. In altri casi, viene visualizzato un messaggio simile al seguente:



Verifica CLI:

<#root>

>

show managers

No managers configured.

È buona norma cancellare tutta la configurazione FTD prima di registrarla nel CCP di destinazione. Un modo rapido per eseguire questa operazione consiste nel passare da una modalità firewall all'altra.

Ad esempio, se è stata attivata la modalità di instradamento, passare a trasparente e quindi tornare a instradato:

<#root>

>

configure firewall transparent

E poi:

<#root>

>

configure firewall routed

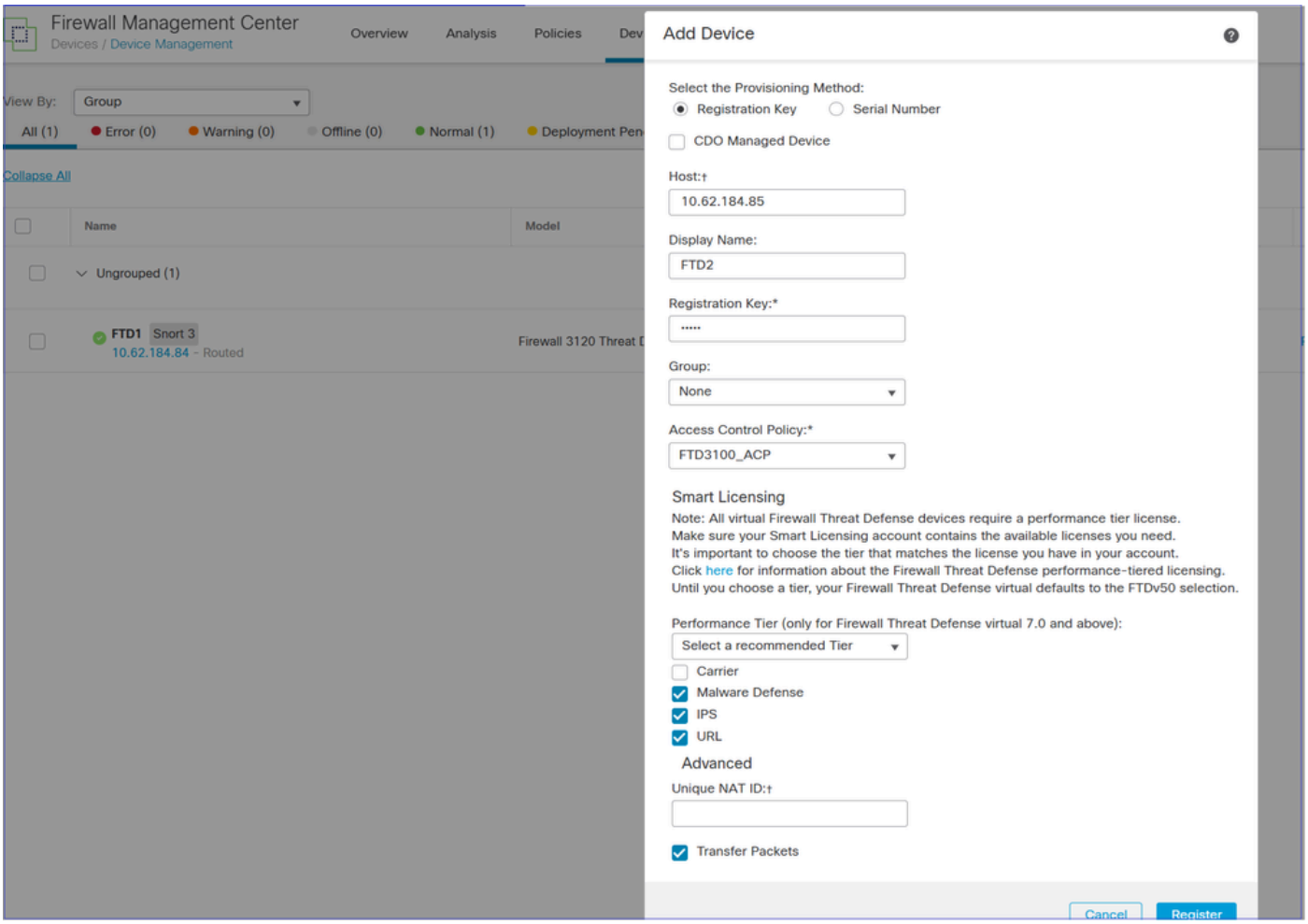
Registrarlo quindi nel CCP2 (CCP destinazione):

<#root>

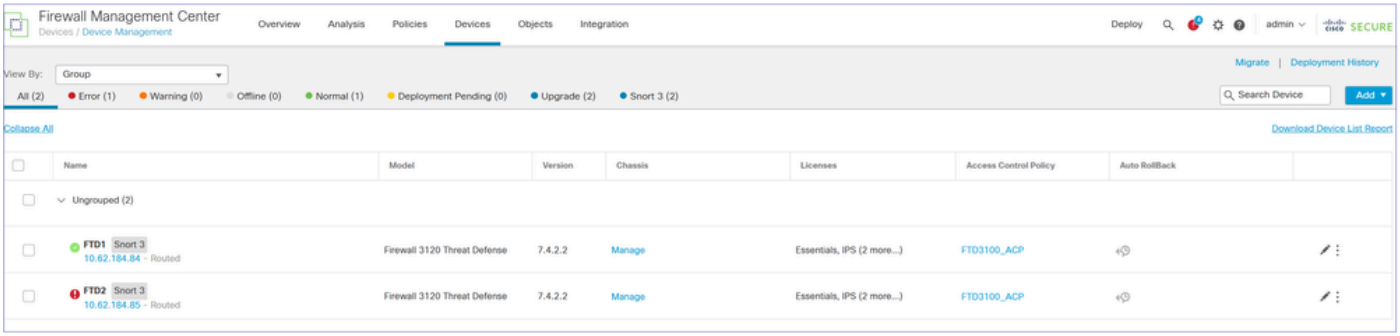
>

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.
>
```



Il risultato:

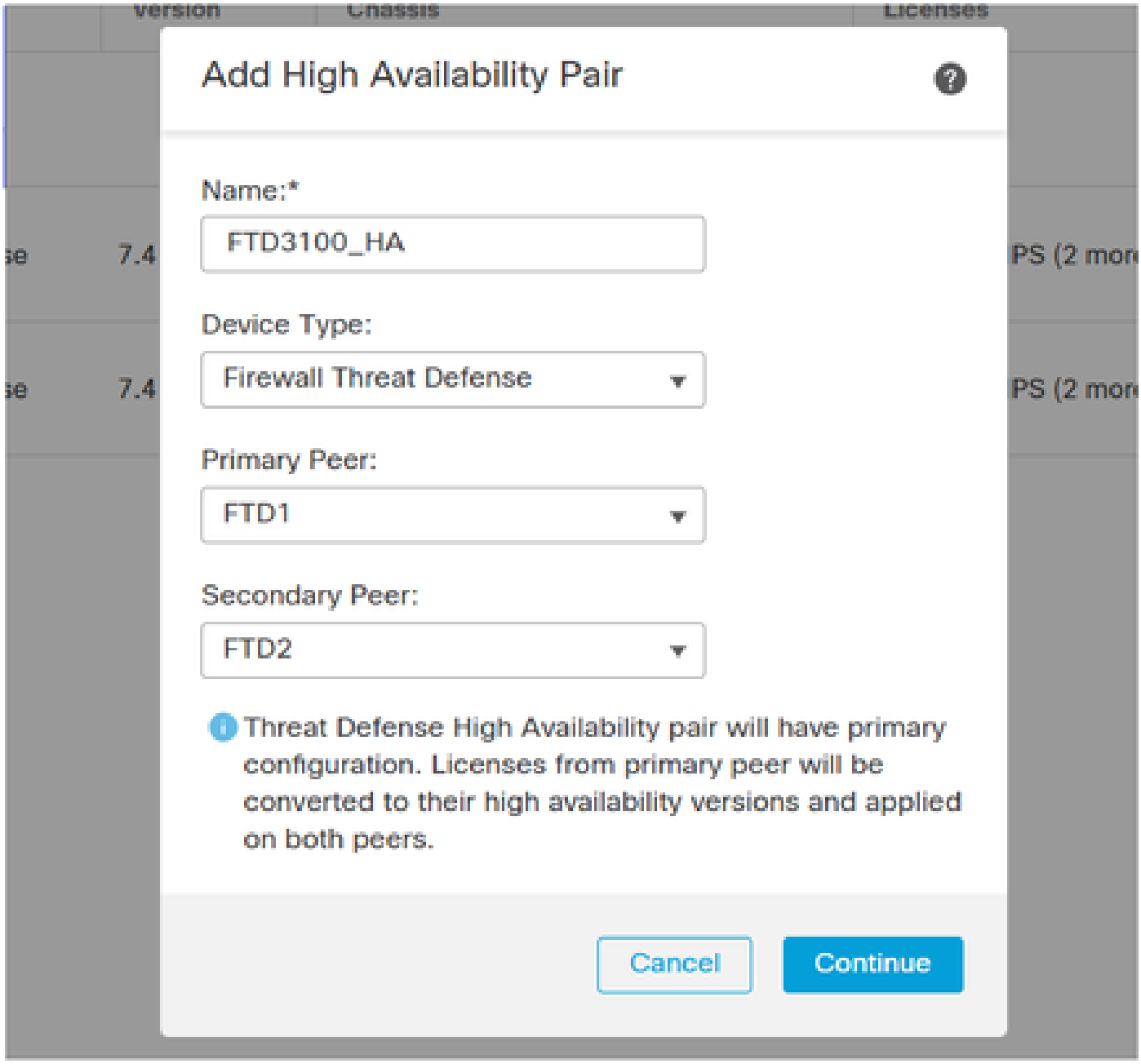


Passaggio 14. Riformare l'FTD HA

Nota: Anche questa attività (come qualsiasi attività correlata alla disponibilità elevata) deve essere eseguita durante un MW. Durante la negoziazione HA si verificherà un'interruzione del traffico di circa 1 minuto dal momento in cui le interfacce dati si interrompono.

Nel FMC di destinazione, selezionare Devices > Device Management (Dispositivi > Gestione dispositivi), quindi Add > High Availability (Aggiungi > Alta disponibilità).

⚠ Attenzione: Accertarsi di selezionare come peer principale l'FTD che gestisce il traffico (FTD1 in questo scenario):



Riconfigurare le impostazioni HA, inclusi le interfacce monitorate, gli IP in standby, gli indirizzi MAC virtuali e così via.

Verifica da CLI FTD1:

```
<#root>

FTD3100-3#

show failover | include host

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

Verifica dalla CLI FTD2:

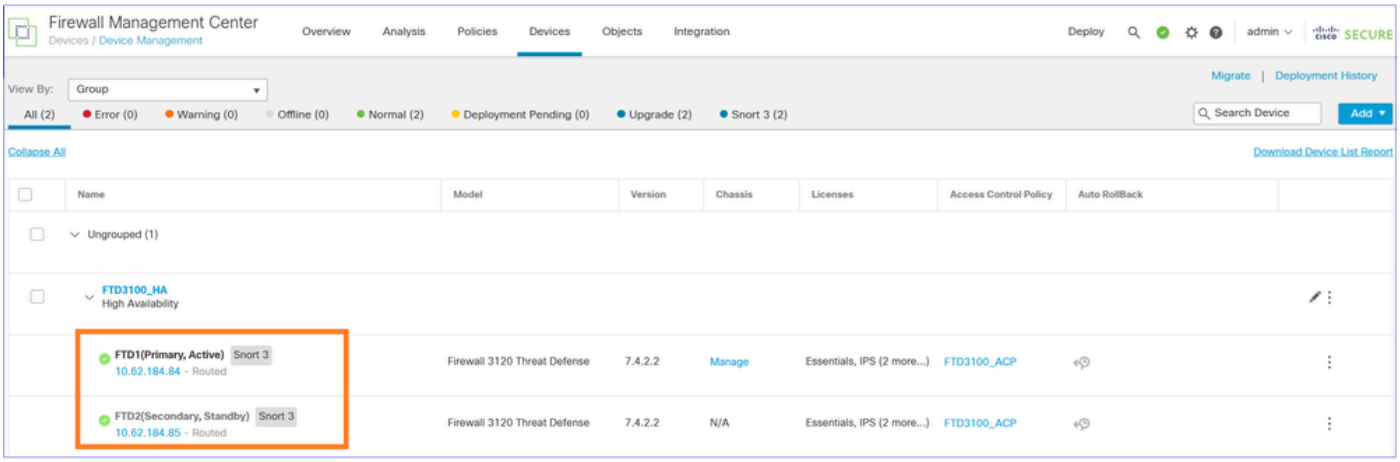
<#root>

FTD3100-3#

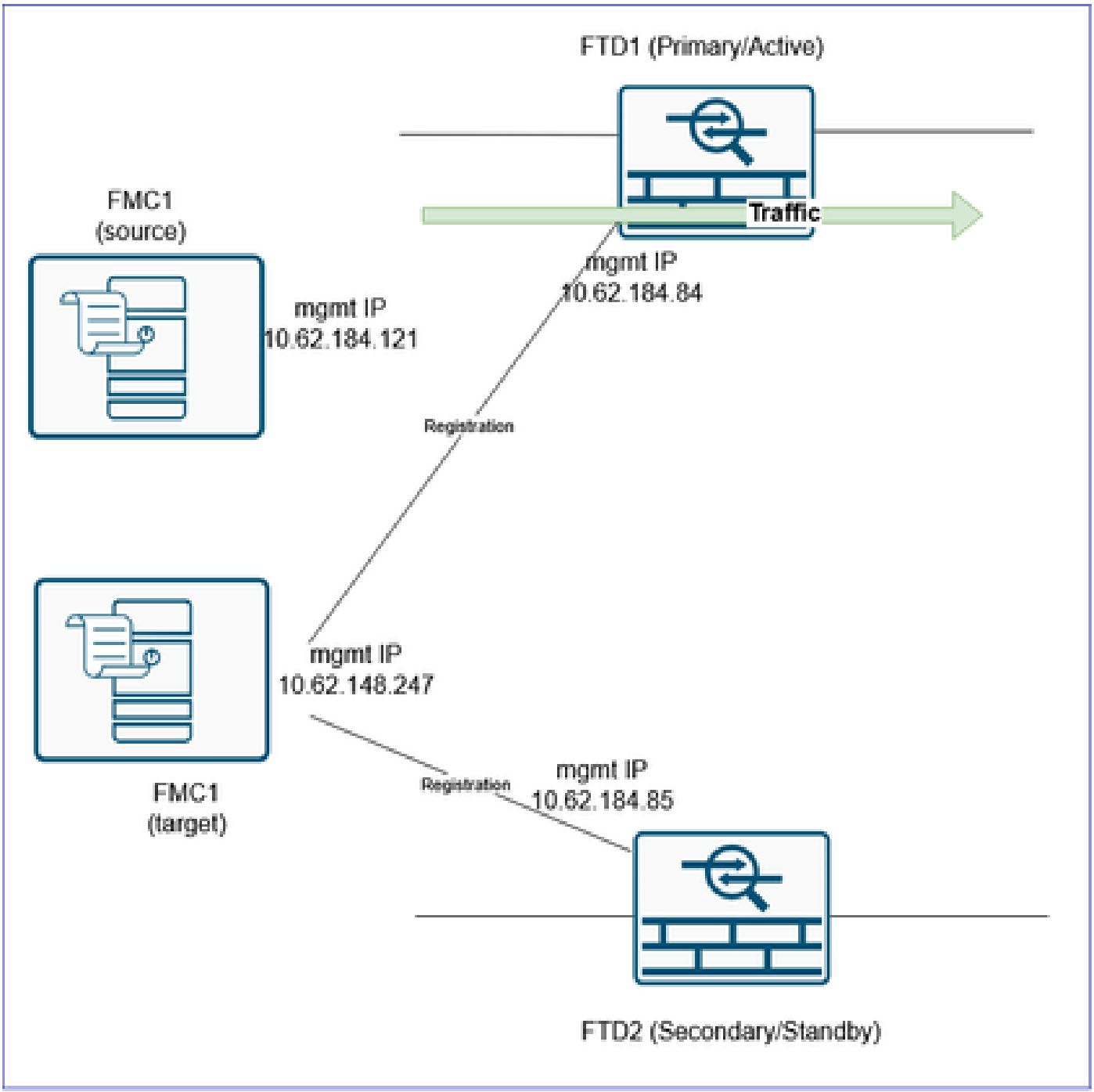
show failover | include host

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

Verifica interfaccia utente FMC:



Infine, attivare/ricollegare le interfacce dati del dispositivo FTD2.



Riferimenti

- Esportare e importare la configurazione del dispositivo
- Aggiungi una coppia ad alta disponibilità
- Migrazione di un FTD da un FMC a un altro FMC

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).