FTD HA (failover) migreren naar een ander FMC

Inhoud

Inleiding

In dit document wordt de procedure beschreven om een FTD HA van een bestaand FMC naar een ander FMC te migreren.

Voor een standalone firewall-migratie naar een nieuw VCC, surf naar 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

Afkortingen

ACS = beleid inzake toegangscontrole

ARP = Protocol voor adresoplossing

CLI = Command Line Interface

FMC = Secure Firewall Management Center

FTD = Secure Firewall Threat Defence

GARP = vrij ARP

HA = hoge beschikbaarheid

MW = Onderhoudsvenster

UI = gebruikersinterface

Voorwaarden

Zorg er voordat u het migratieproces start voor dat u over deze voorwaarden beschikt:

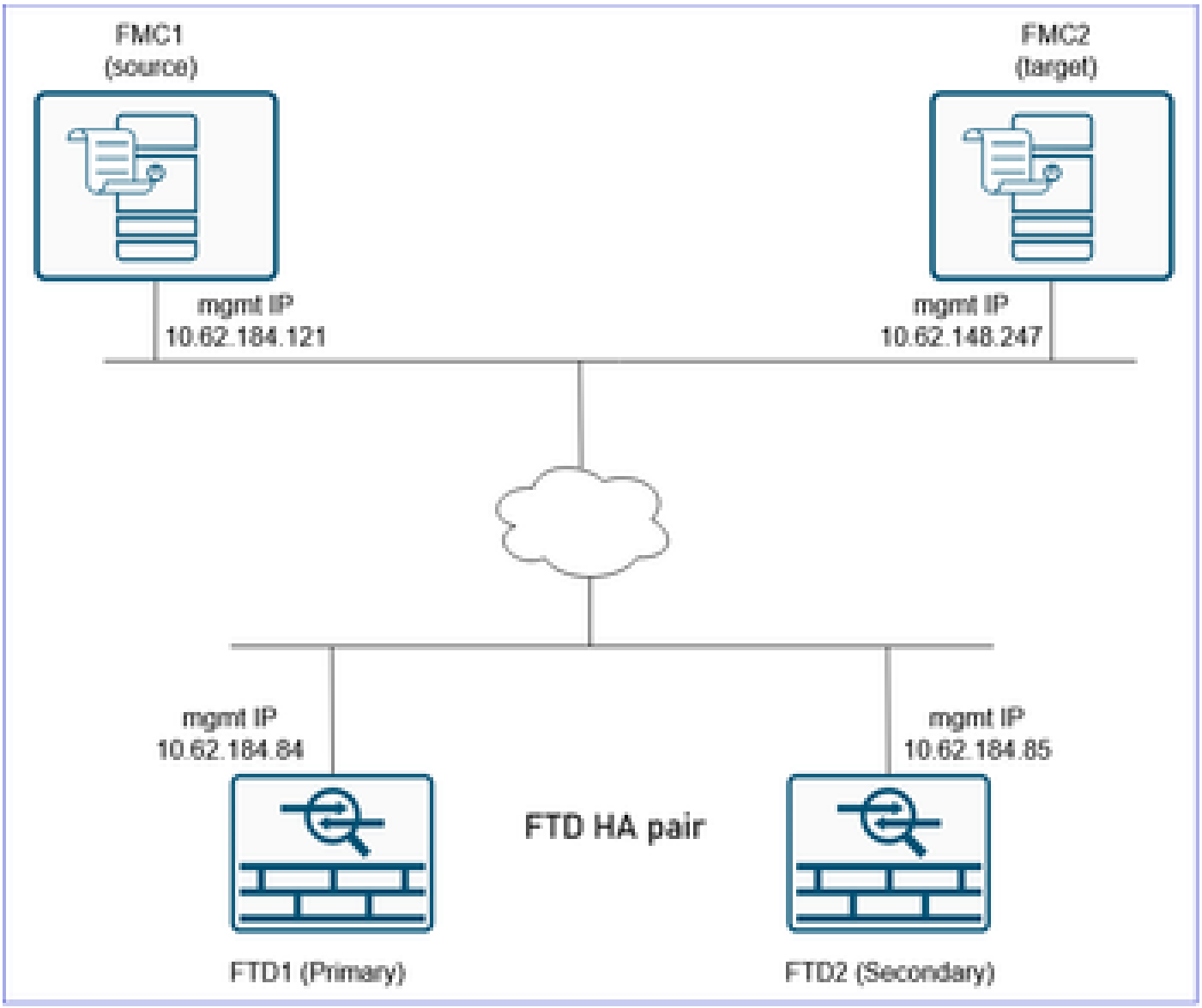
- UI- en CLI-toegang tot zowel de FMC's van herkomst als van bestemming.
- Administratieve referenties voor zowel VCC's als firewalls.
- De toegang van de console tot beide firewalls.
- Toegang tot de L3 upstream en downstream apparaten (voor het geval dat je de ARP cache moet wissen).
- Zorg ervoor dat het VCC van bestemming/doel dezelfde versie heeft als het VCC van herkomst/van bestemming.
- Zorg ervoor dat het VCC van bestemming/doel over dezelfde vergunningen beschikt als het VCC van herkomst/van bestemming.
- Zorg ervoor dat u een MW instelt om de migratie uit te voeren, omdat dit invloed zal hebben op het transitoverkeer.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall 31x, FTD versie 7.4.2.2.
- Secure Firewall Management Center versie 7.4.2.2.
- De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



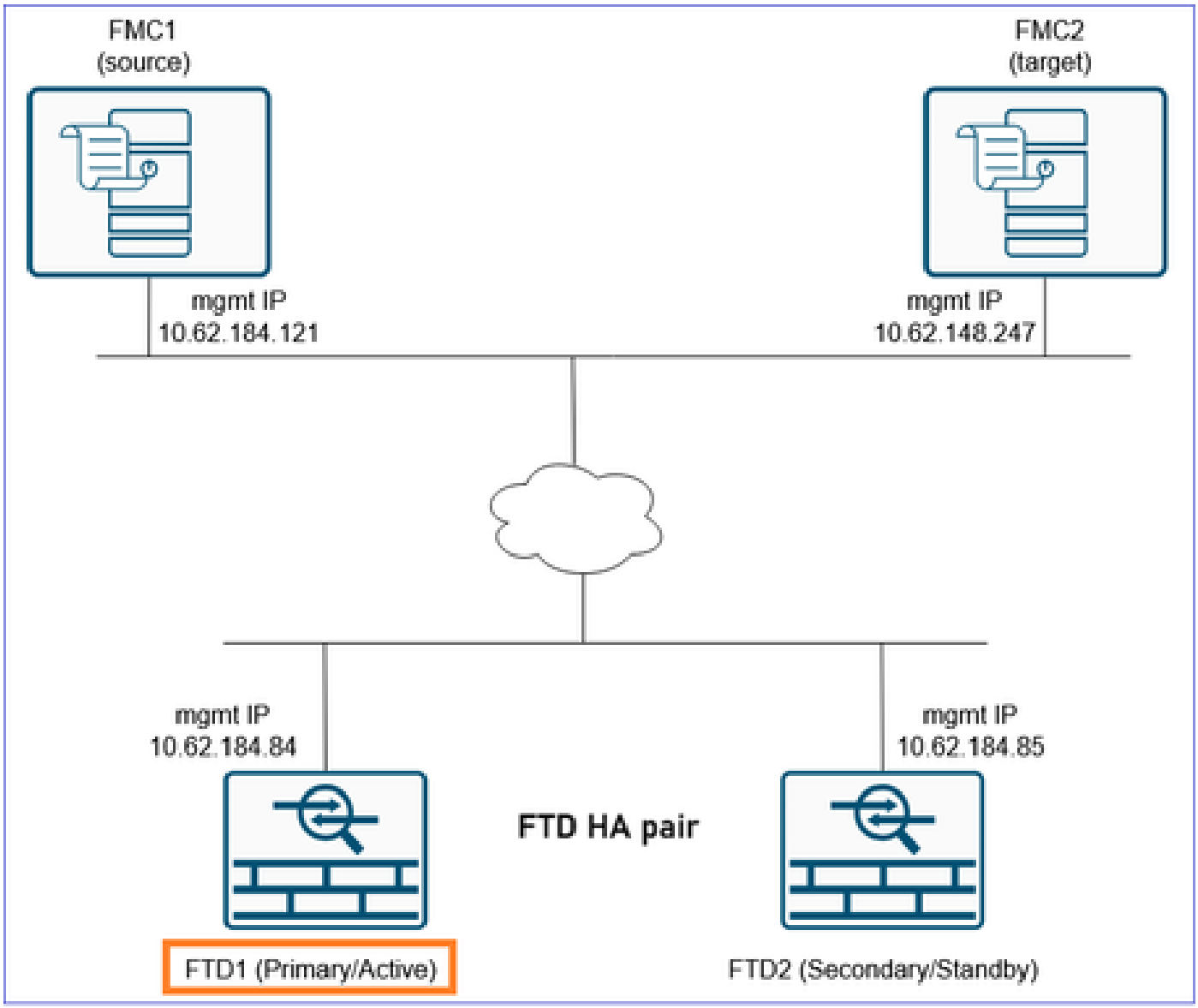
Configureren

Migratiestappen

Voor dit scenario denken we aan de volgende staten:

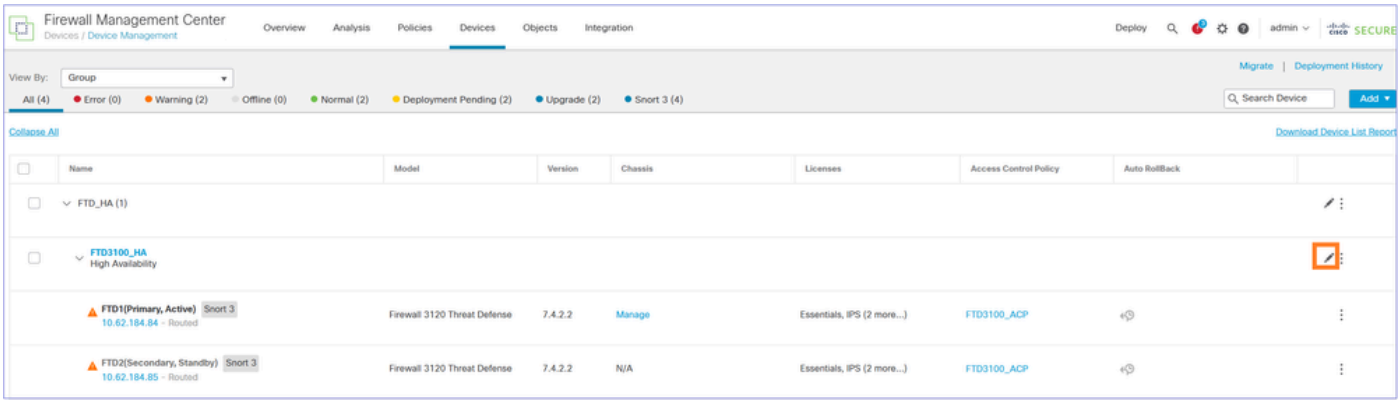
FTD1: Primair/actief

FTD2: Secundair/stand-by

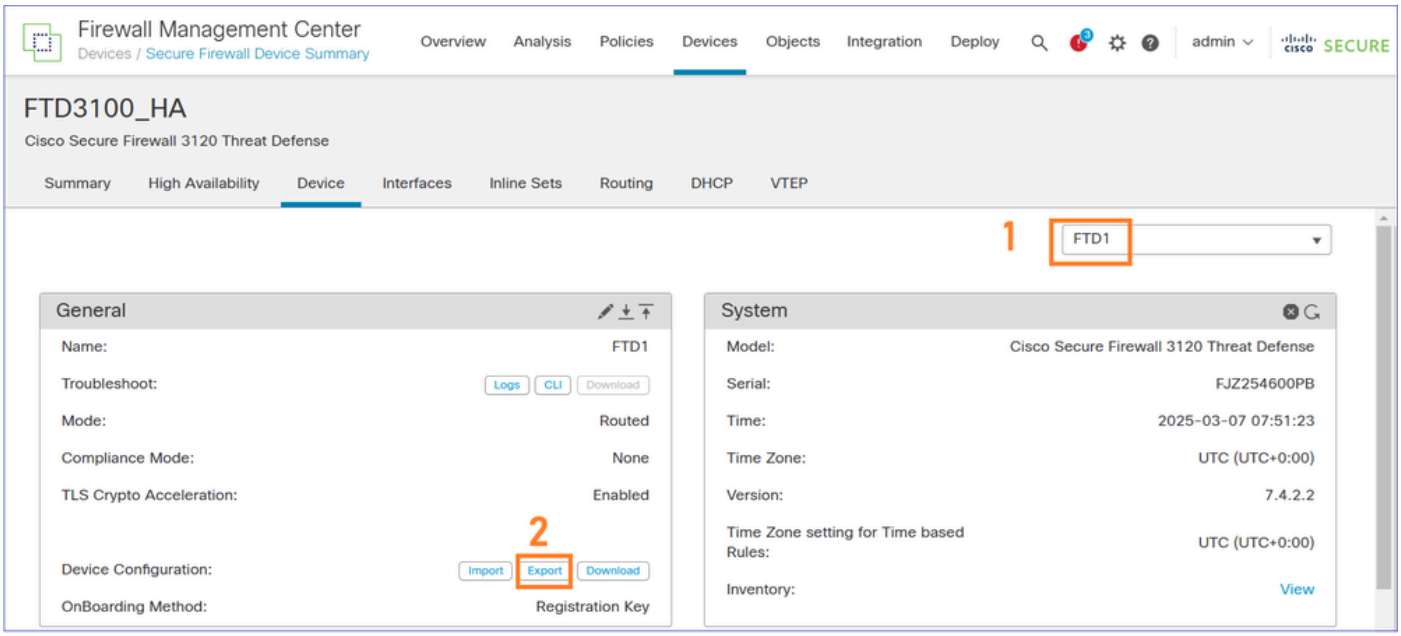


Stap 1. Exporteer de apparaatconfiguratie vanuit de primaire firewall

Navigeer in het VCC1 (bron-VCC) naar Apparaten > Apparaatbeheer. Selecteer het FTD HA-paar en selecteer Bewerken:

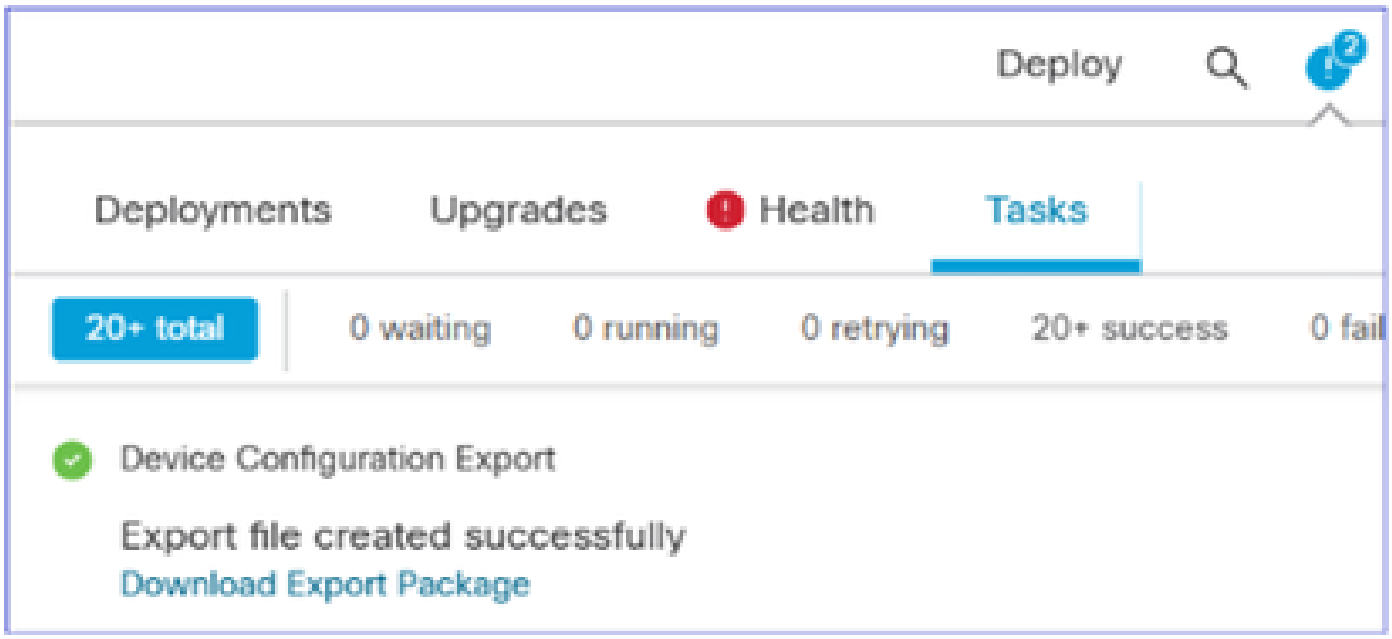


Ga naar het tabblad Apparaat. Zorg ervoor dat de primaire/actieve FTD (in dit geval FTD1) is geselecteerd en selecteer Exporteren om de apparaatconfiguratie te exporteren:



Opmerking: De Exportoptie is beschikbaar vanaf 7.1-softwarerelease en hoger.

U kunt naar de pagina Kennisgevingen > Taken navigeren om er zeker van te zijn dat de export is voltooid. Selecteer vervolgens het Download Export Package:



U kunt ook op de knop Downloaden klikken in het gedeelte Algemeen. U krijgt een sfo-bestand, bijvoorbeeld DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

Het bestand bevat apparaatgerelateerde configuratie zoals:

- Routed Interfaces
- Inline sets
- Routing
- DHCP
- VTEP

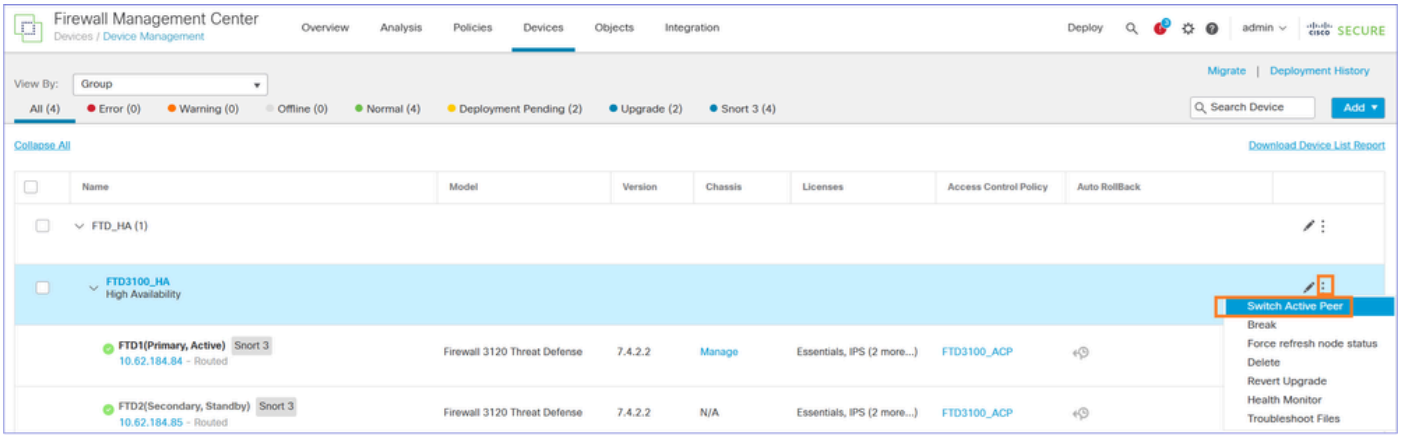
- Verwante objecten

Opmerking: Het geëxporteerde configuratiebestand kan alleen terug naar dezelfde FTD worden geïmporteerd. De UUID van de FTD moet overeenkomen met de inhoud van het geïmporteerde Sfo-bestand. Hetzelfde FTD kan worden geregistreerd in een ander FMC en sfo-bestand kan worden geïmporteerd.

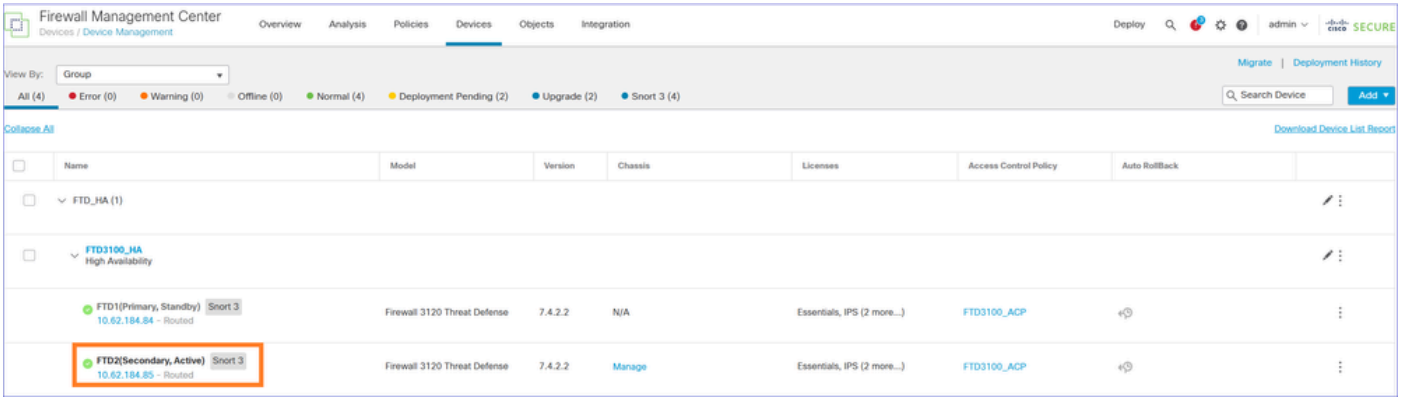
Referentie: 'De apparaatconfiguratie exporteren en importeren' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

Stap 2. Maak het secundaire FTD actief

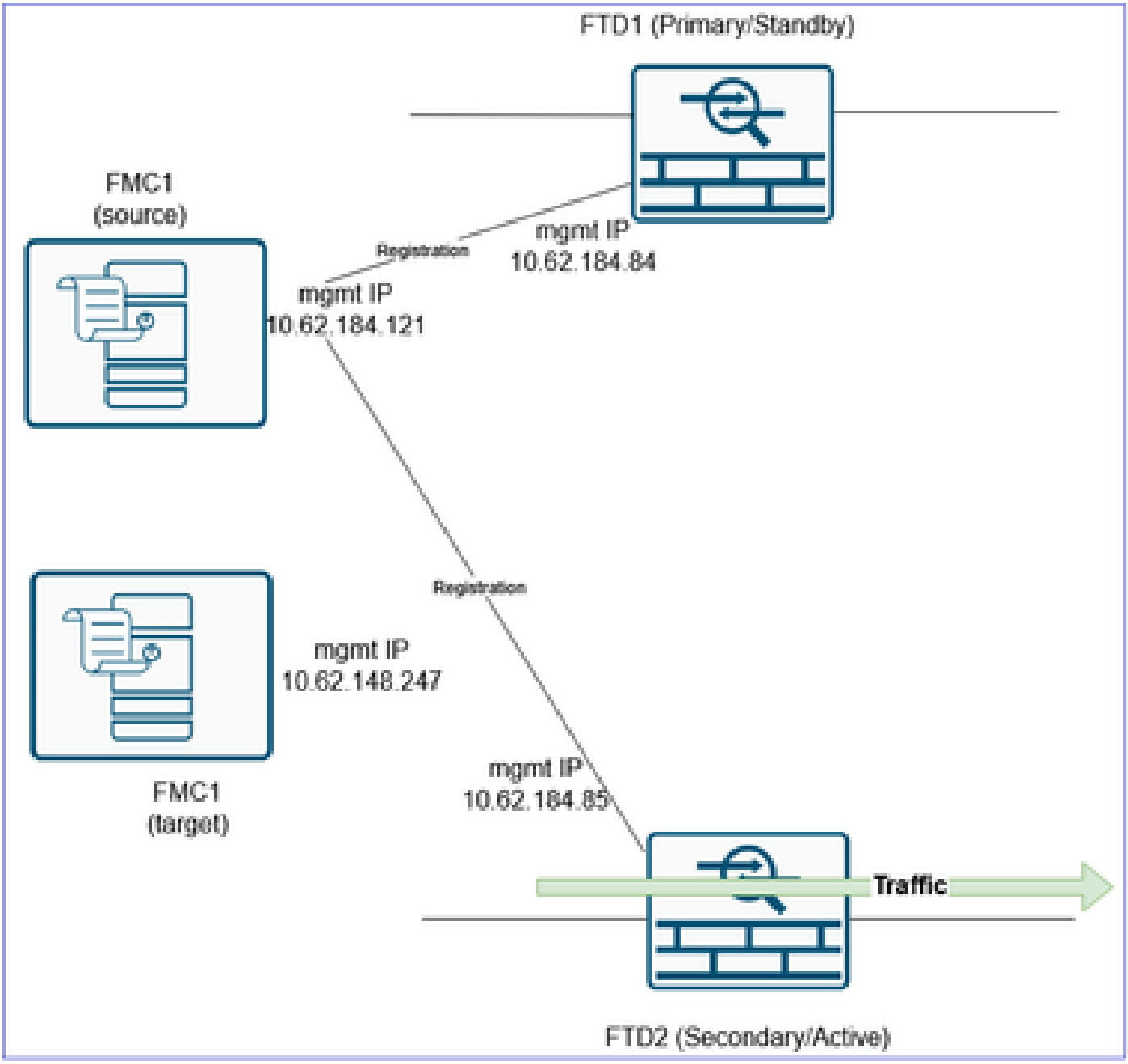
Navigeren naar Apparaten > Apparaatbeheer, selecteer het FTD HA-paar en selecteer Switch Active Pair:



Het resultaat is FTD1 (Primair/stand-by) en FTD (Secundair/actief):

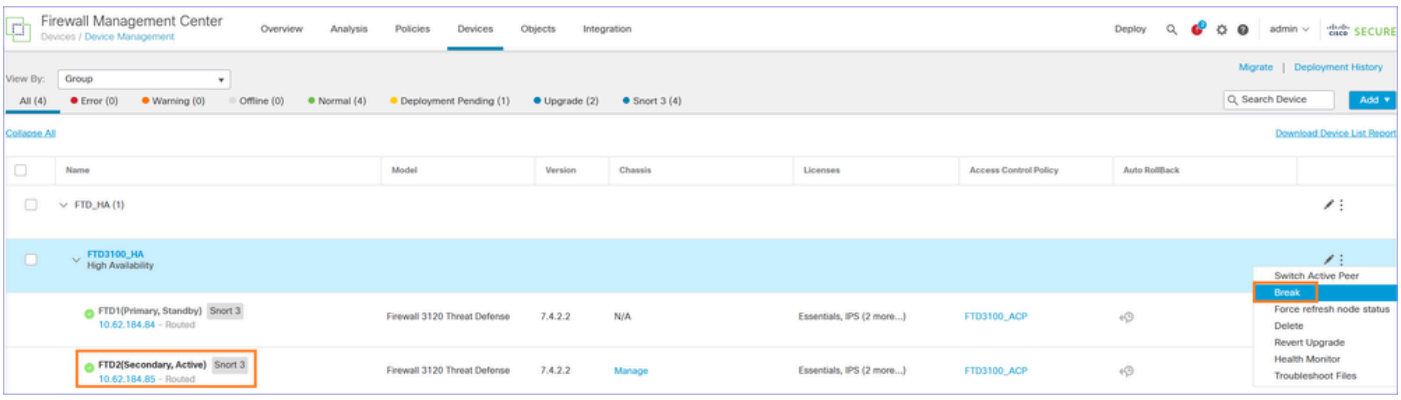


Het verkeer wordt nu verwerkt door het secundaire/actieve FTD:

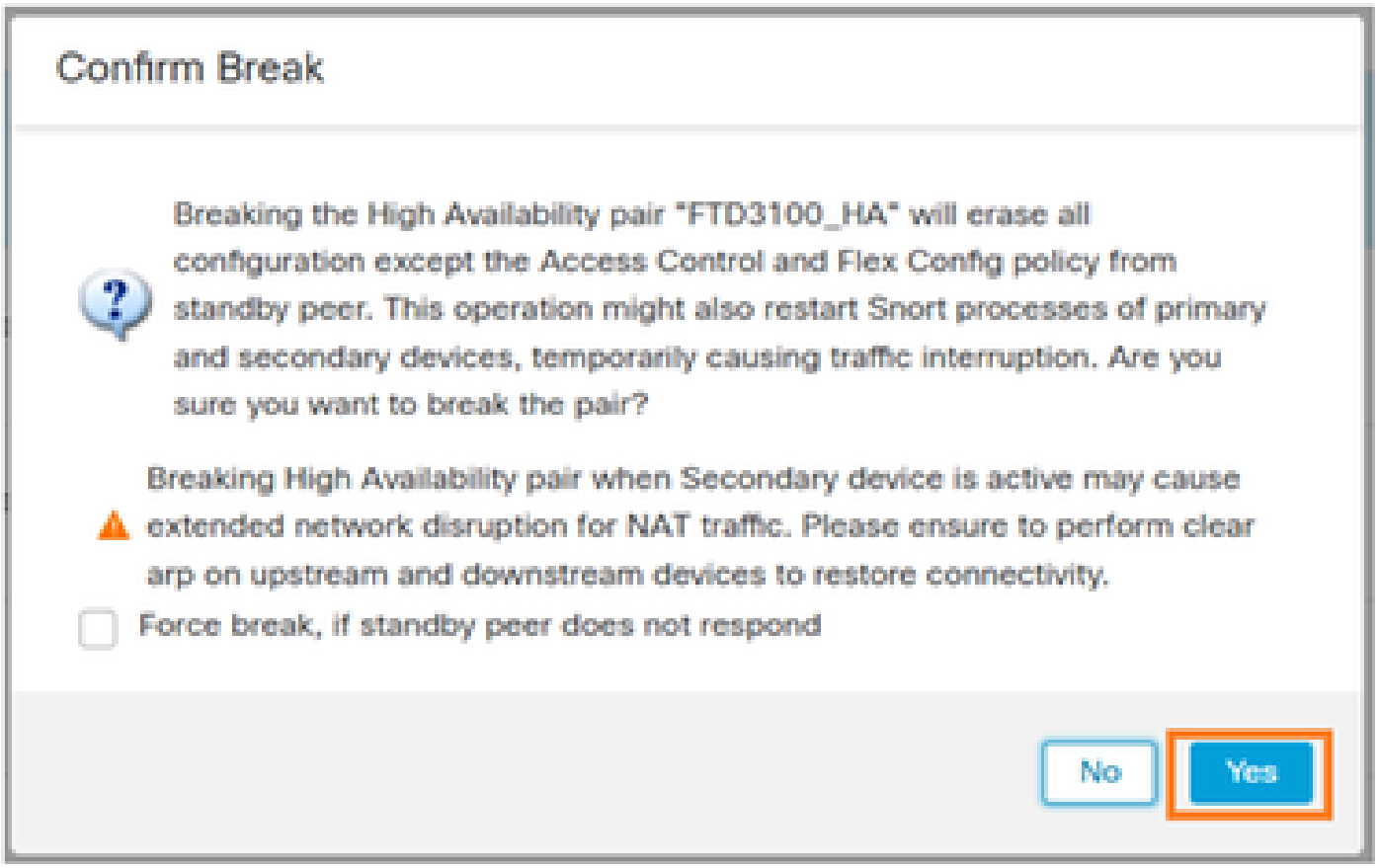


Stap 3. Breek de FTD HA

Ga naar Apparaten > Apparaatbeheer en breek de FTD HA:



Dit venster verschijnt. Selecteer Ja



Opmerking: Op dit punt kunt u enige verkeersonderbreking voor een paar seconden ervaren aangezien de Snort-motor tijdens de HA-onderbreking opnieuw begint. Ook, zoals het bericht vermeldt, als u NAT gebruikt en een langdurige verkeersstroomonderbreking ervaart, overweeg dan het verwijderen van het ARP cache op upstream en downstream apparaten.

Na het breken van de FTD HA, heb je twee standalone FTDs op FMC.

Vanuit configuratieoogpunt heeft de FTD2 (ex-Active) nog steeds de configuratie op zijn plaats, behalve de failover-gerelateerde configuratie, en verwerkt hij het verkeer:

```
<#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
```

De FTD1 (ex-Standby) heeft alle configuratie verwijderd:

<#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#

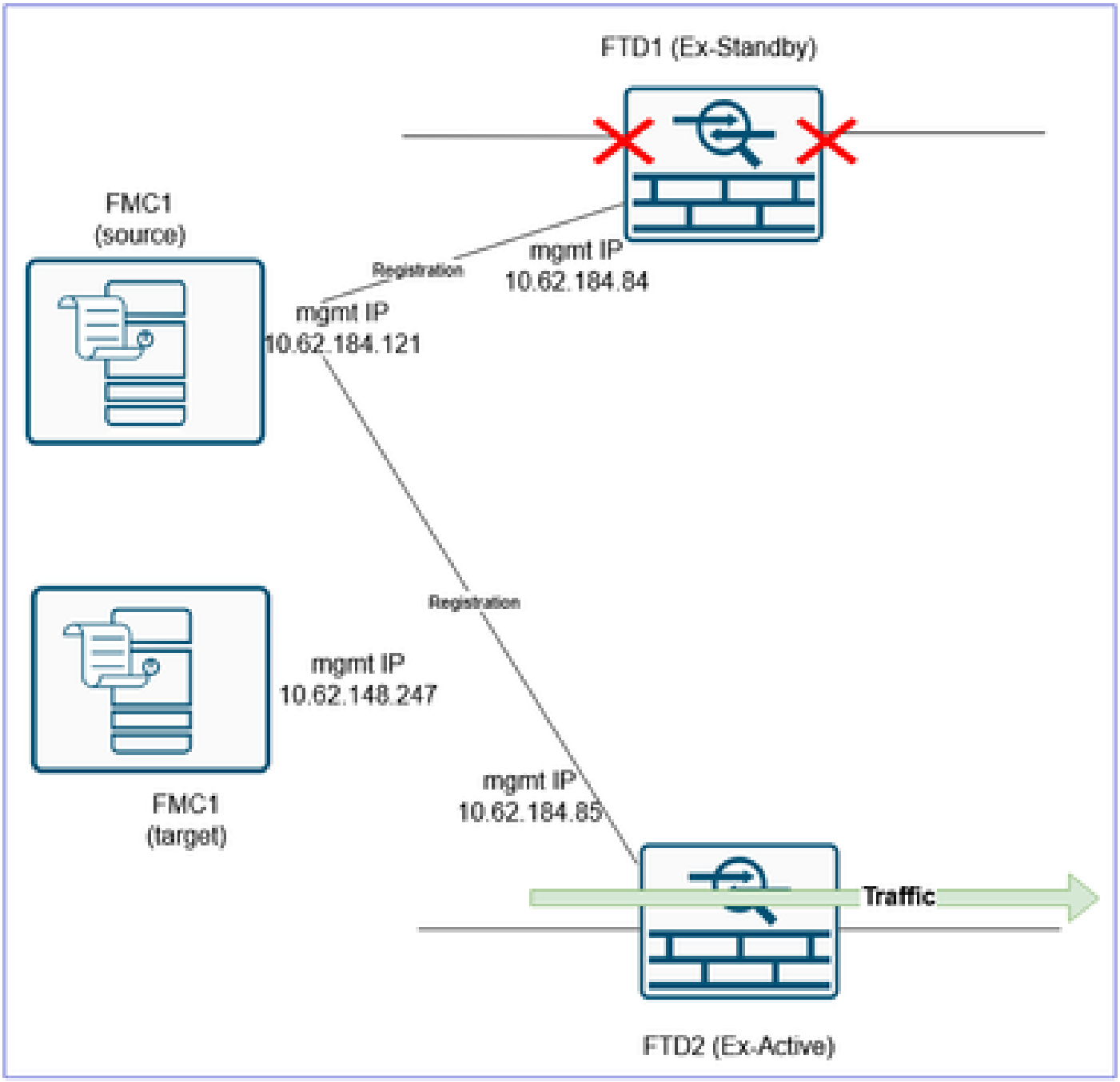
show interface ip brief

```
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
```

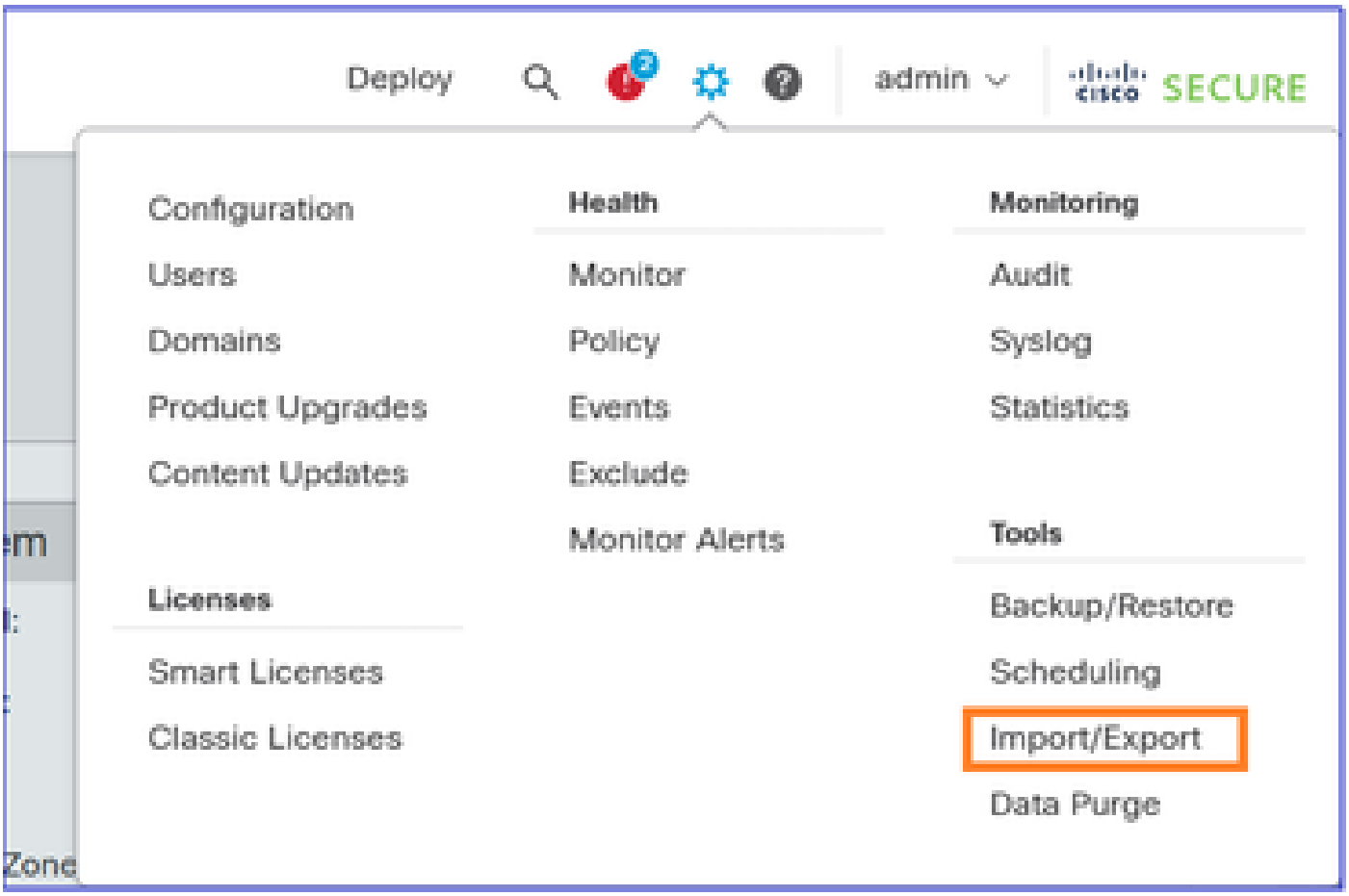
Stap 4. Isoleer de FTD1 (ex-Primair) data-interfaces

Koppel de gegevenskabels los van de FTD1 (ex-Primair). Laat alleen de FTD-beheerpoort aangesloten.



Stap 5. Exporteer het FTD gedeelde beleid

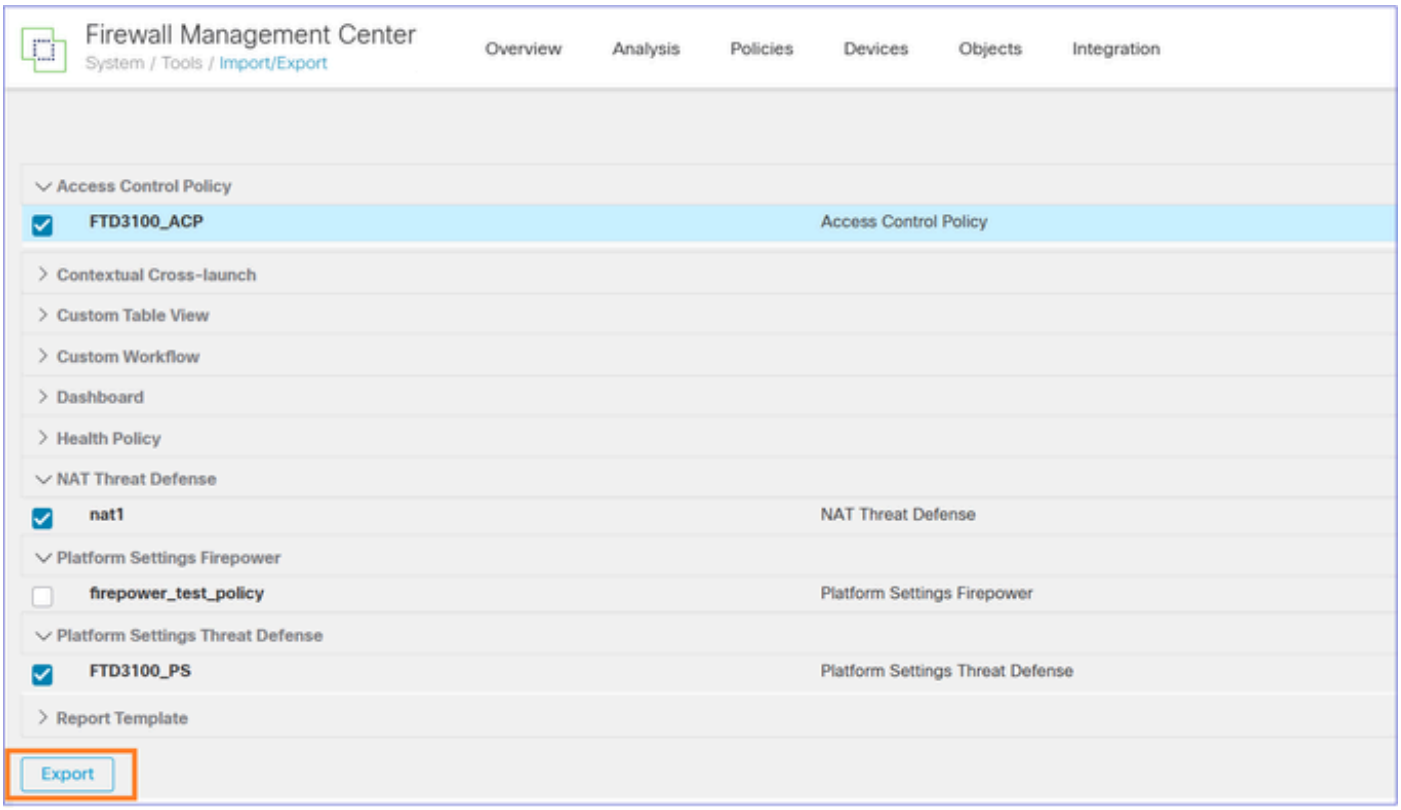
Navigeer naar Systeem > Tools en selecteer Importeren/Exporteren:



Exporteer de verschillende beleidsregels die aan het apparaat zijn gekoppeld. Zorg ervoor dat u alle aan de FTD gehechte beleidslijnen exporteert, zoals:

- Toegangscontrolebeleid (ACS)
- Beleid voor netwerkadresomzetting (NAT)
- Gezondheidsbeleid (indien van toepassing)
- FTD-platforminstellingen

en ga zo maar door.

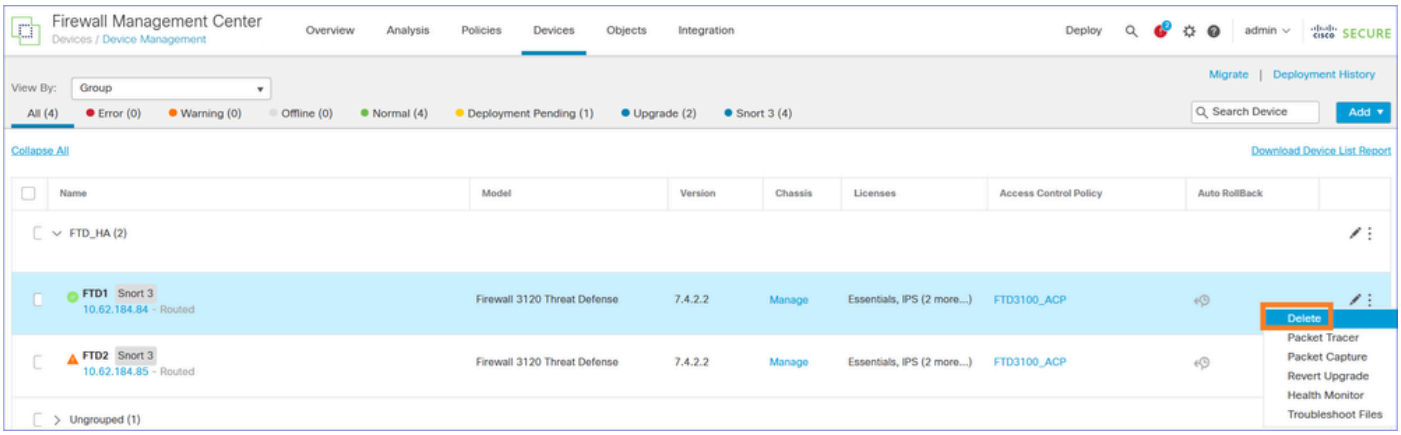


Opmerking: Op het moment van schrijven wordt de export van VPN-gerelateerde configuratie niet ondersteund. U moet de VPN handmatig opnieuw configureren op het FMC2 (doel-FMC) na de registratie van het apparaat.

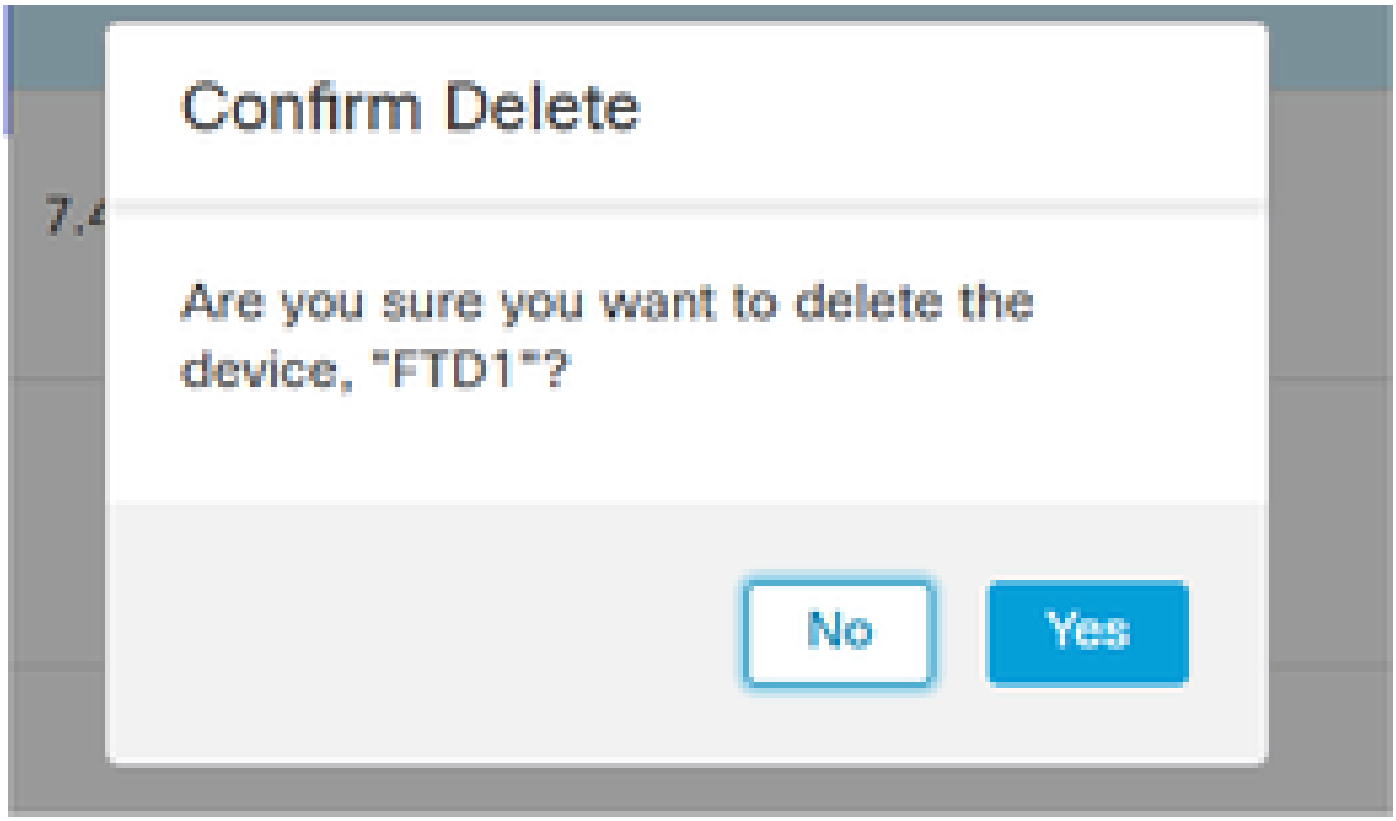
Verwante verbetering Cisco bug-id CSCwf05294
.

Het resultaat is een .sfo bestand, bijvoorbeeld ObjectExport_20250306082738.sfo

Stap 6. Verwijder/deregistreer het FTD1 (ex-Primair) van het oude VCC/het VCC van de bron



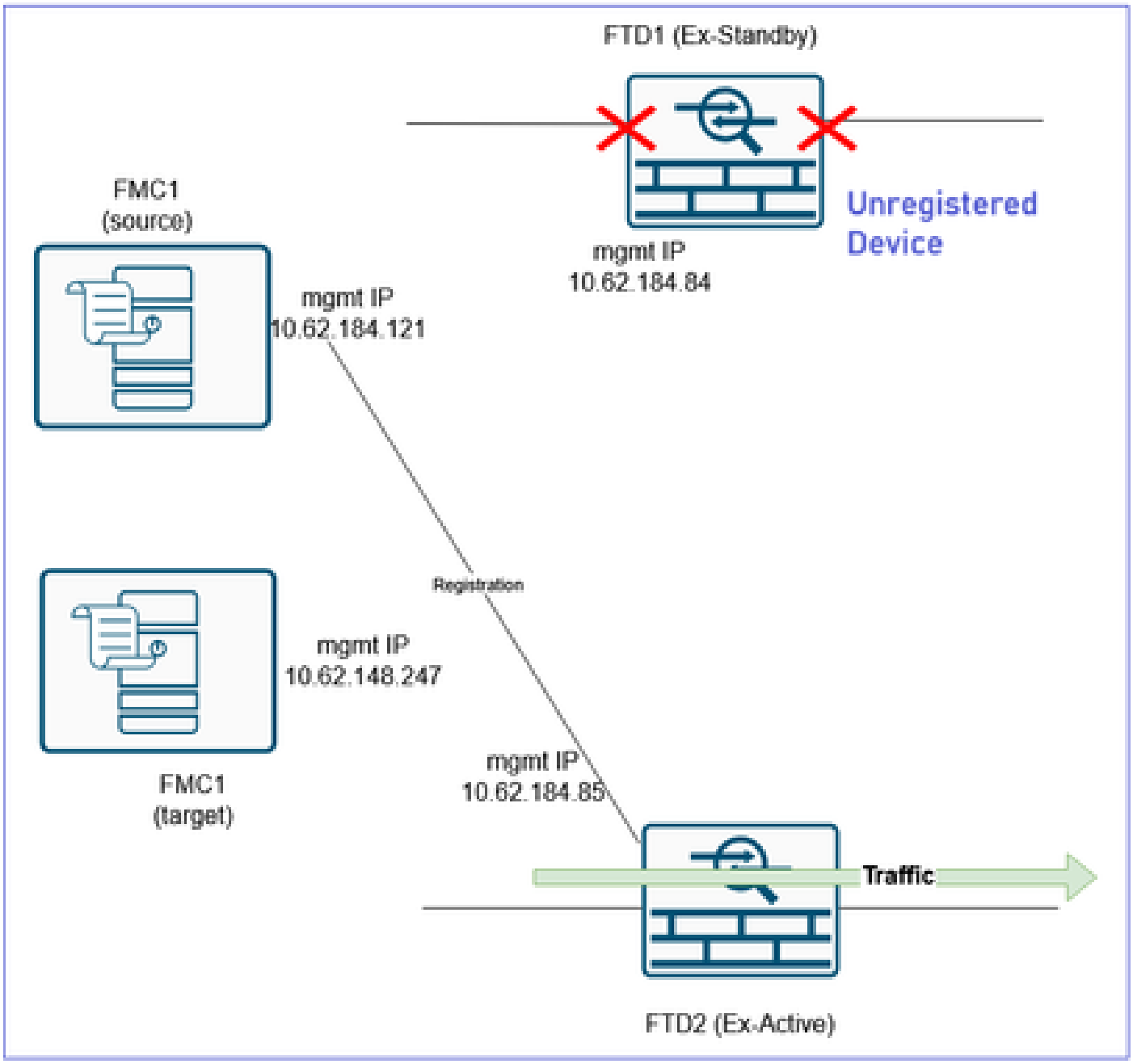
Bevestig het wissen van het apparaat:



FTD1 CLI-verificatie:

```
<#root>

>

show managers

No managers configured.

>
```

De huidige status na het wissen van het FTD1-apparaat:

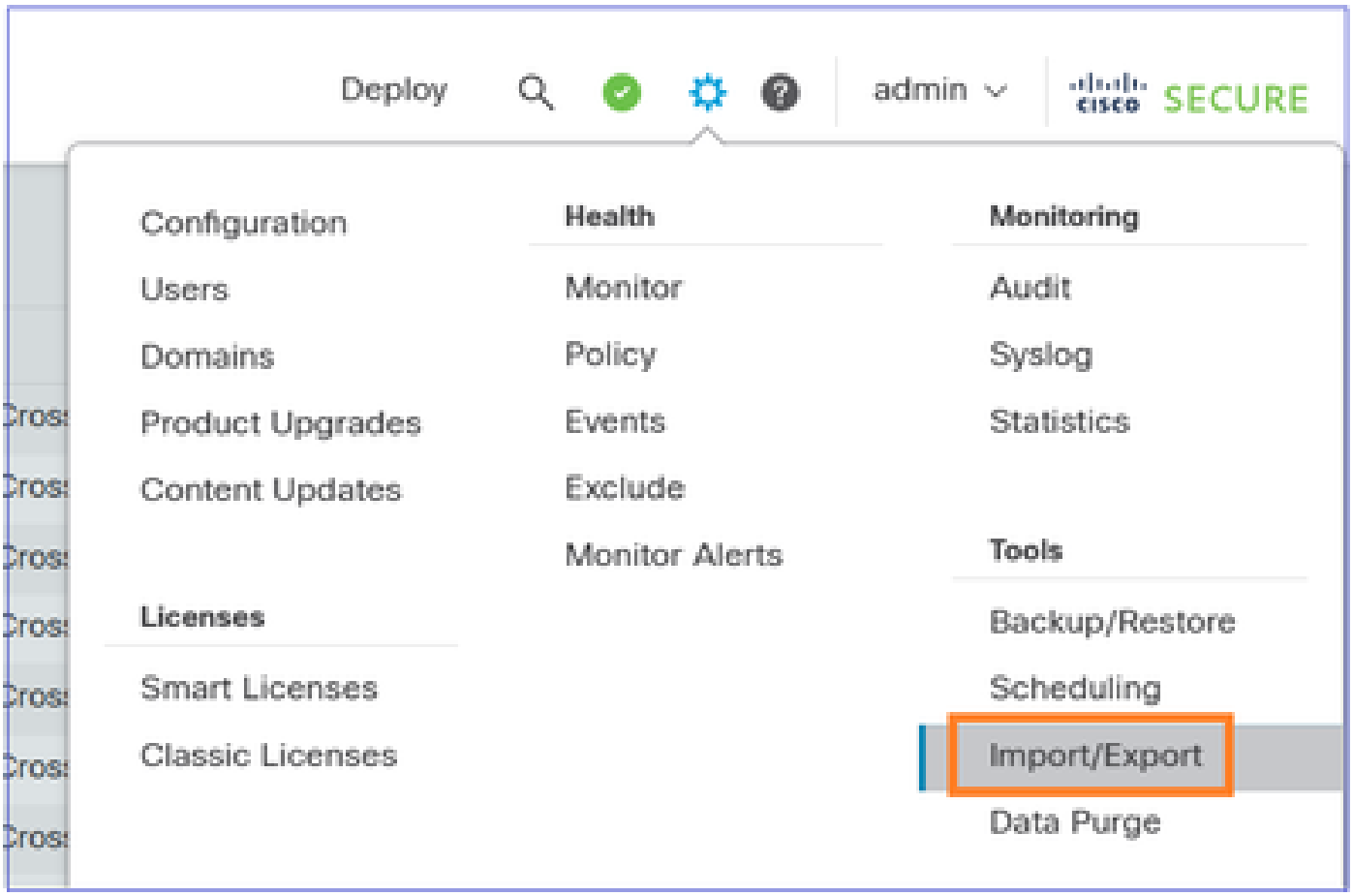


Stap 7. Importeer het configuratieobject van het FTD Policy in het FMC2 (doel-FMC)

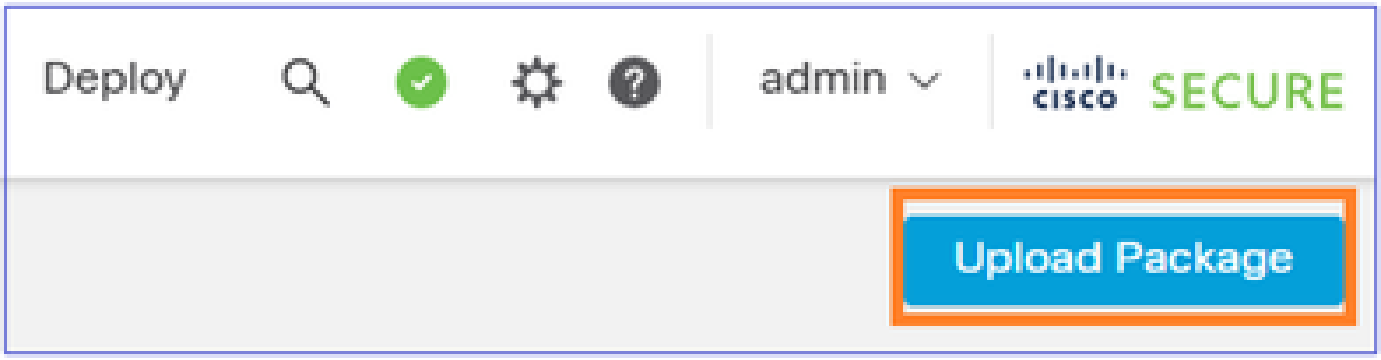
Opmerking: Het document richt zich op de migratie van één FTD HA-paar naar een nieuw FMC. Aan de andere kant, als u van plan bent om te migreren meerdere firewalls die hetzelfde beleid (bijvoorbeeld, ACS, NAT) en objecten delen en u wilt dit doen in fasen moet u deze punten overwegen.
- Indien u een bestaand beleid heeft met betrekking tot het VCC met dezelfde naam, wordt u gevraagd:
a. Wil de polis vervangen of
b. Maak een nieuwe met een andere naam. Hierdoor worden dubbele objecten met verschillende namen gemaakt (achtervoegsel _1).

- Als u met optie 'b' gaat, zorgt u er in stap 9 voor dat u de nieuw gemaakte objecten op het gemigreerde beleid afstemt (ACS-beveiligingszones, NAT-beveiligingszones, routing, platforminstellingen, enzovoort).

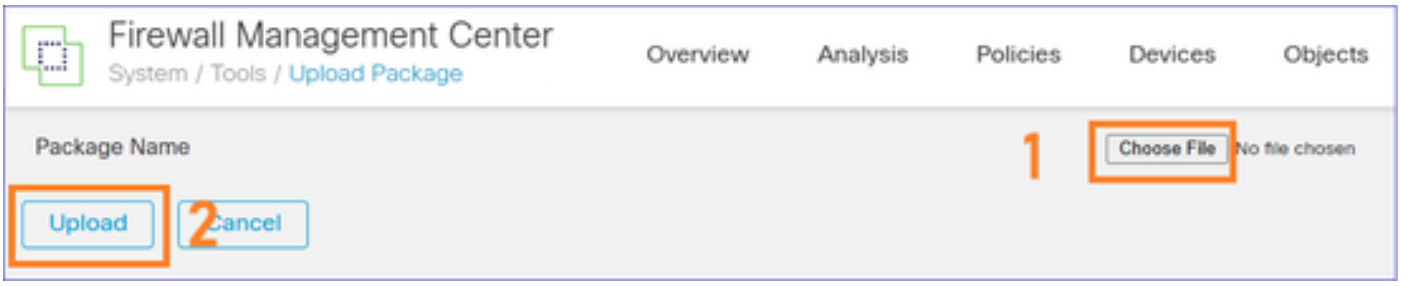
Meld u aan bij het FMC2 (doel-FMC) en importeer het Sfo-object FTD Policies dat u in stap 5 hebt geëxporteerd:



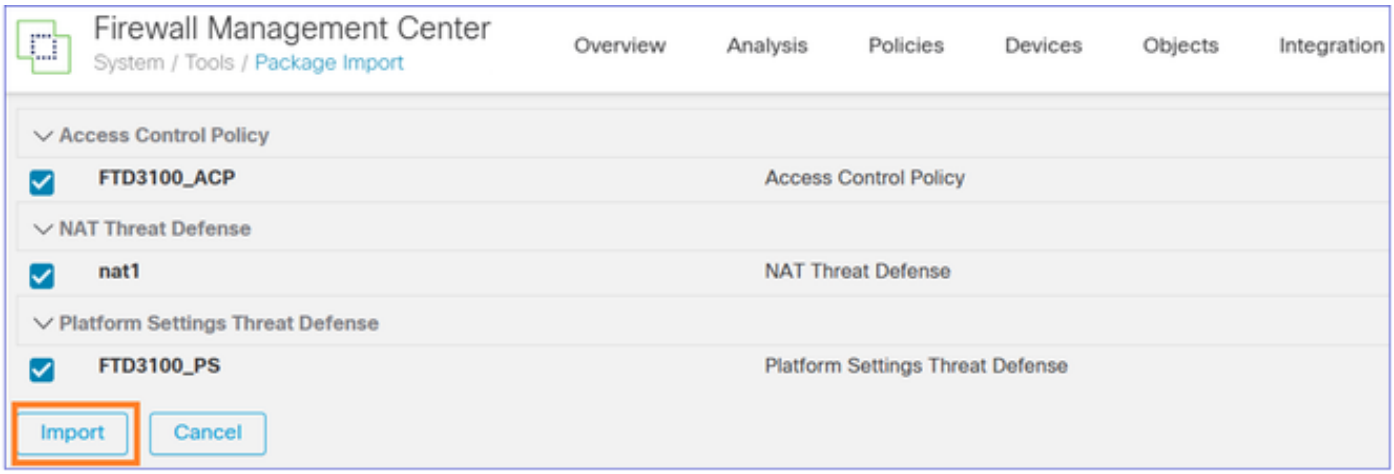
Selecteer Uploadpakket:



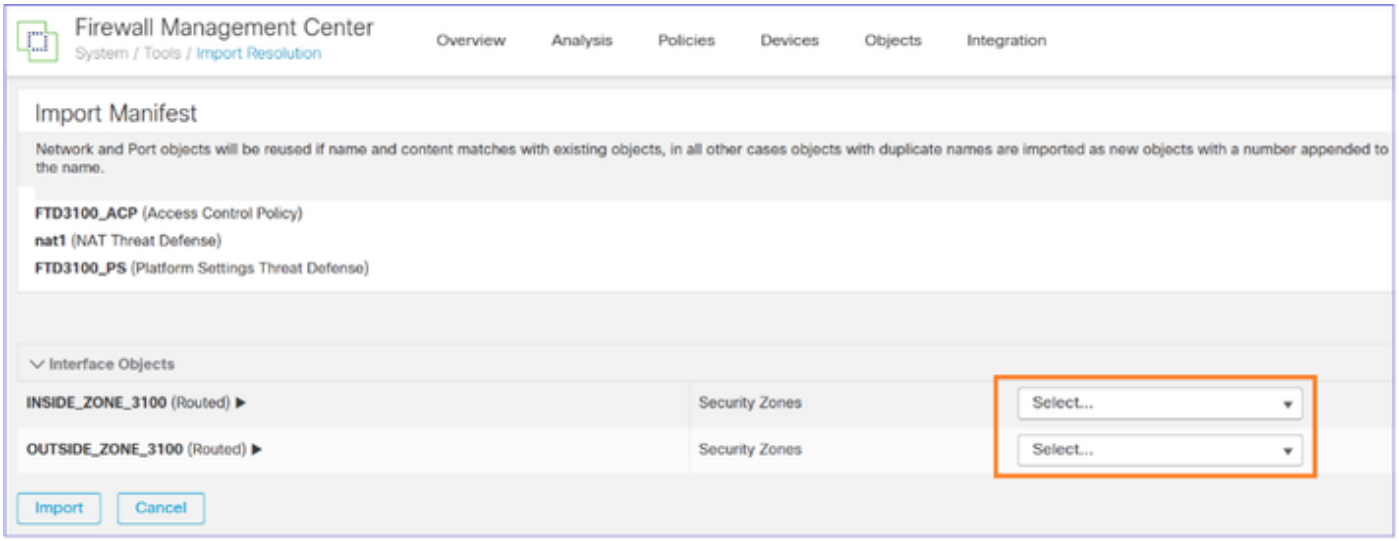
Upload het bestand:



Importeer de beleidslijnen:



Maak de interface-objecten/beveiligingszones aan in het VCC2 (doel-VCC):



U kunt dezelfde namen geven als bij het VCC1 (bron-VCC):

Zodra u Importeren hebt geselecteerd, wordt een taak gestart met het importeren van het betreffende beleid in het VCC2 (doel-VCC):

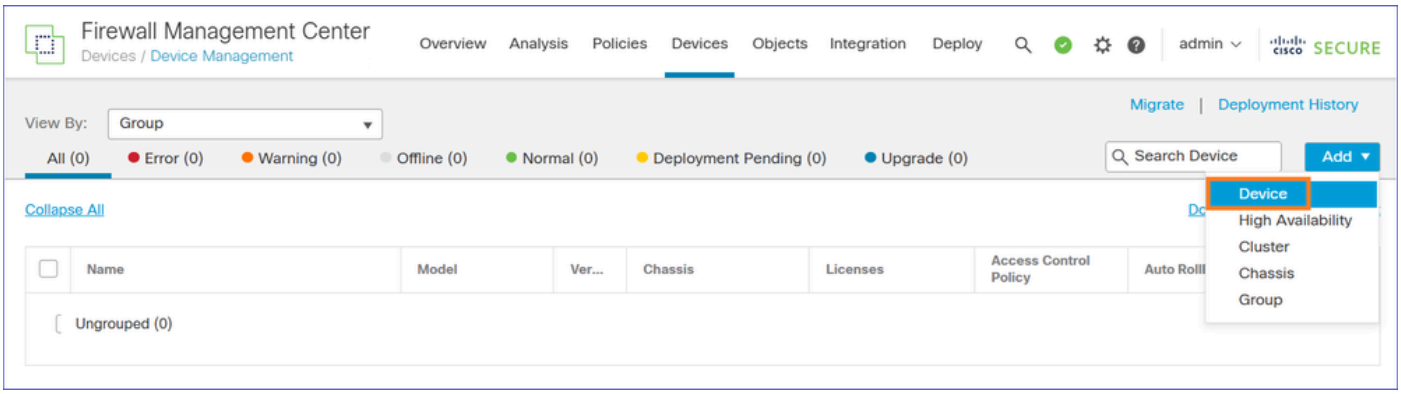
De taak is voltooid:

Stap 8. Registreer het FTD1 (ex-Primair) in het FMC2

Ga naar de FTD1 (ex-Primary) CLI en configureer de nieuwe beheerder:

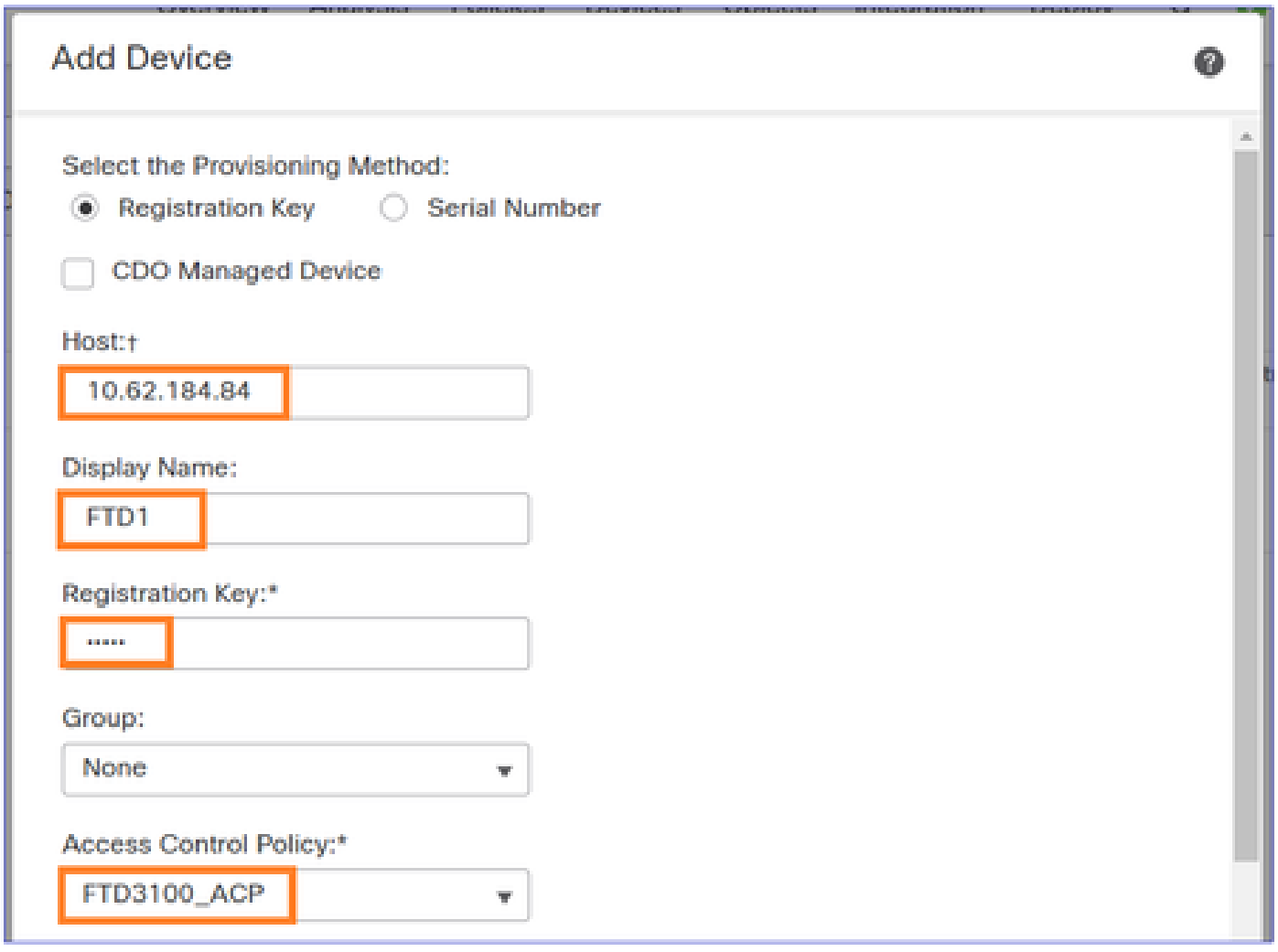
```
<#root>

>

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.

>
```

Ga naar de FMC2 (target FMC) UI Devices > Apparaatbeheer en voeg het FTD-apparaat toe:

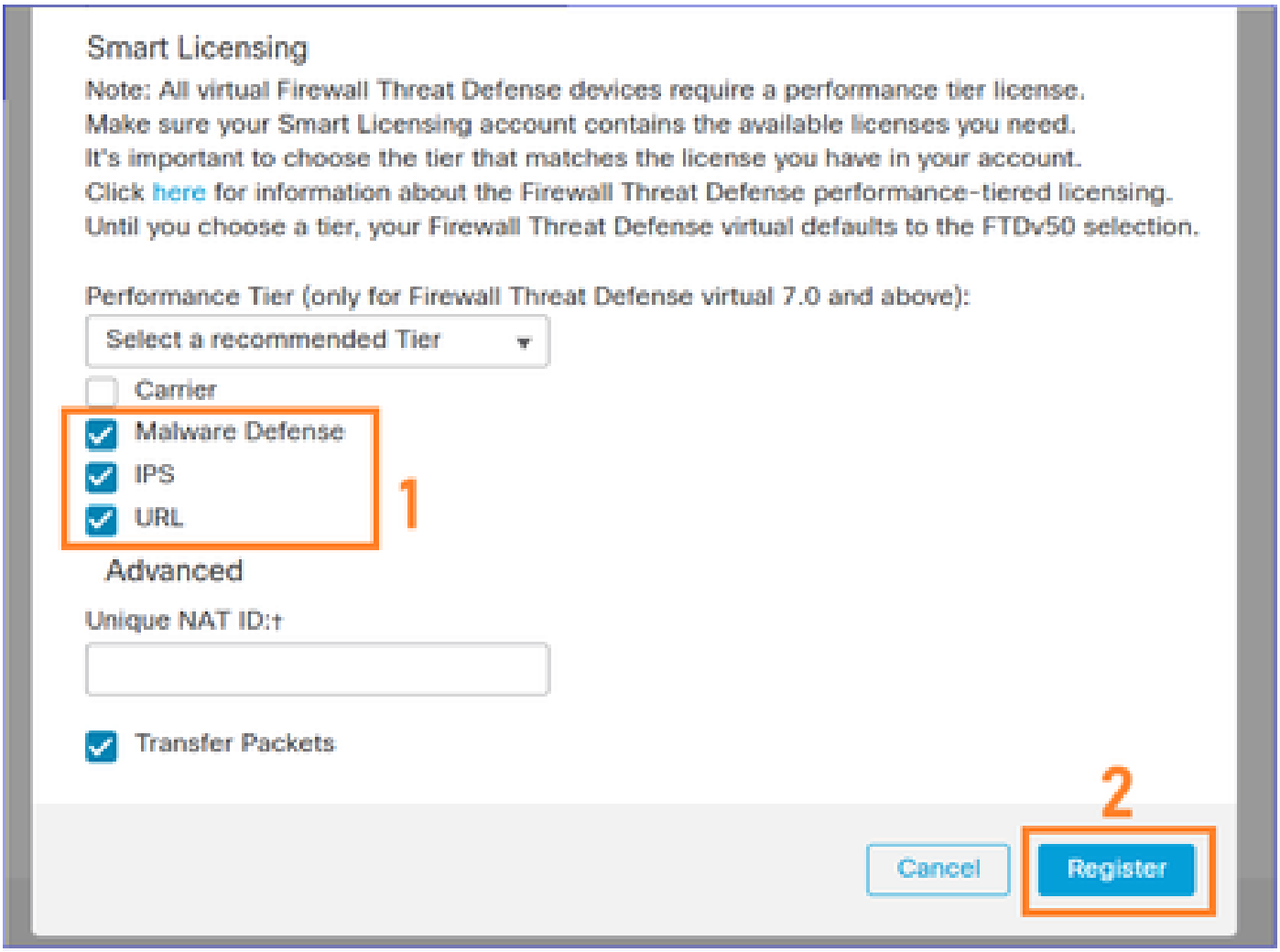


Als de apparaatregistratie mislukt, raadpleegt u dit document om het probleem op te lossen: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

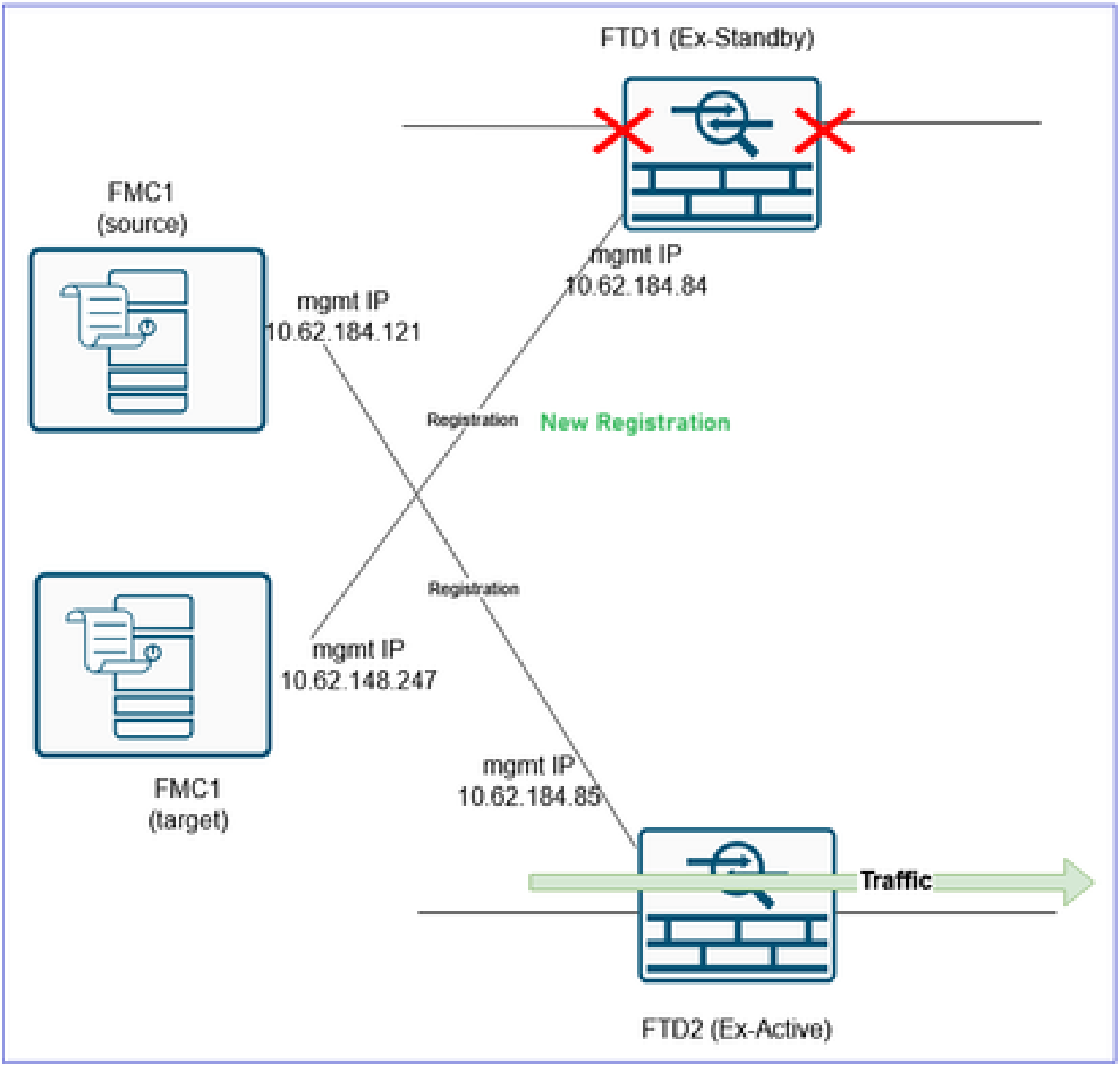
Wijs het toegangscontrolebeleid toe dat u in de vorige stap hebt geïmporteerd:



Pas de benodigde licenties toe en registreer het apparaat:



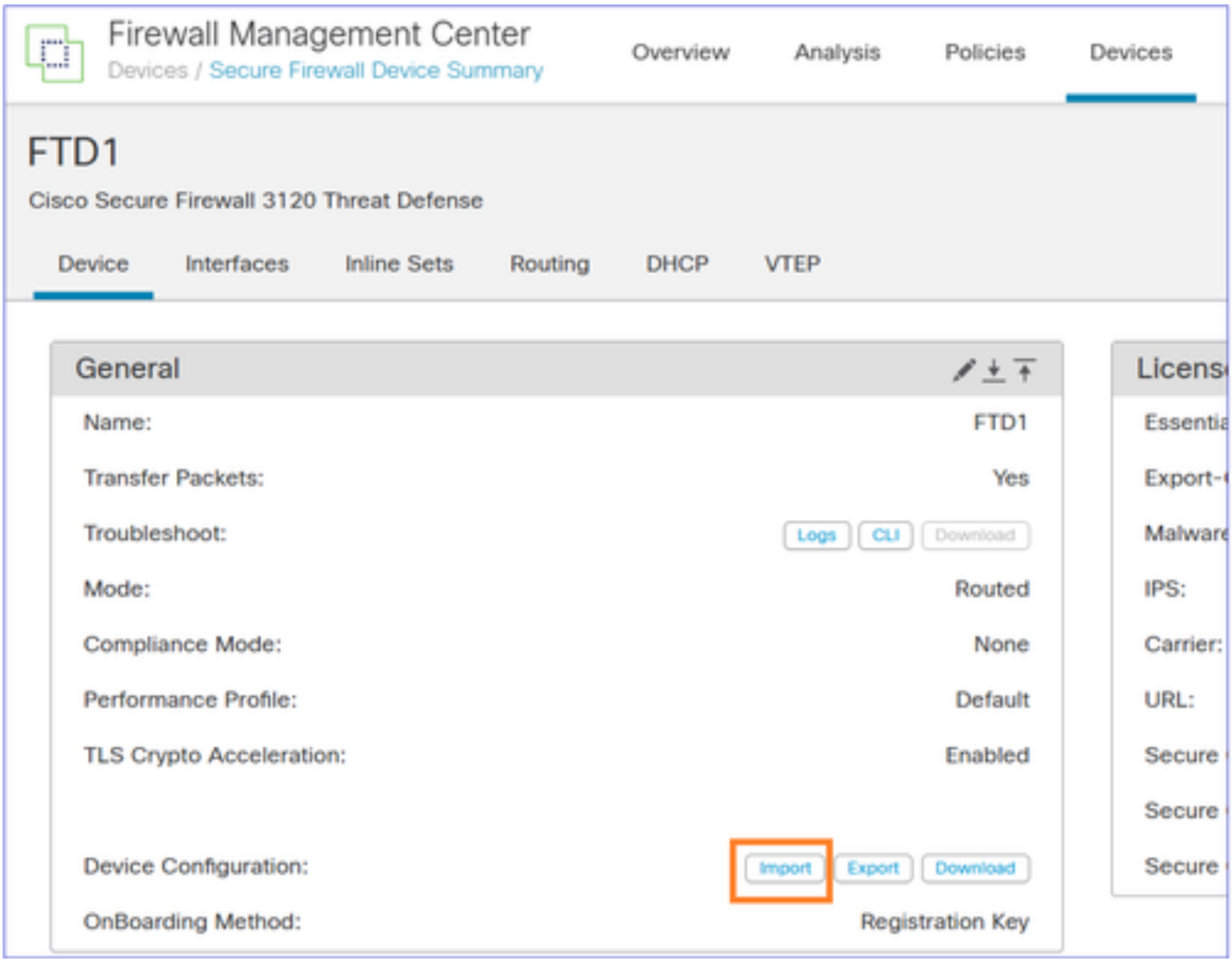
Het resultaat:



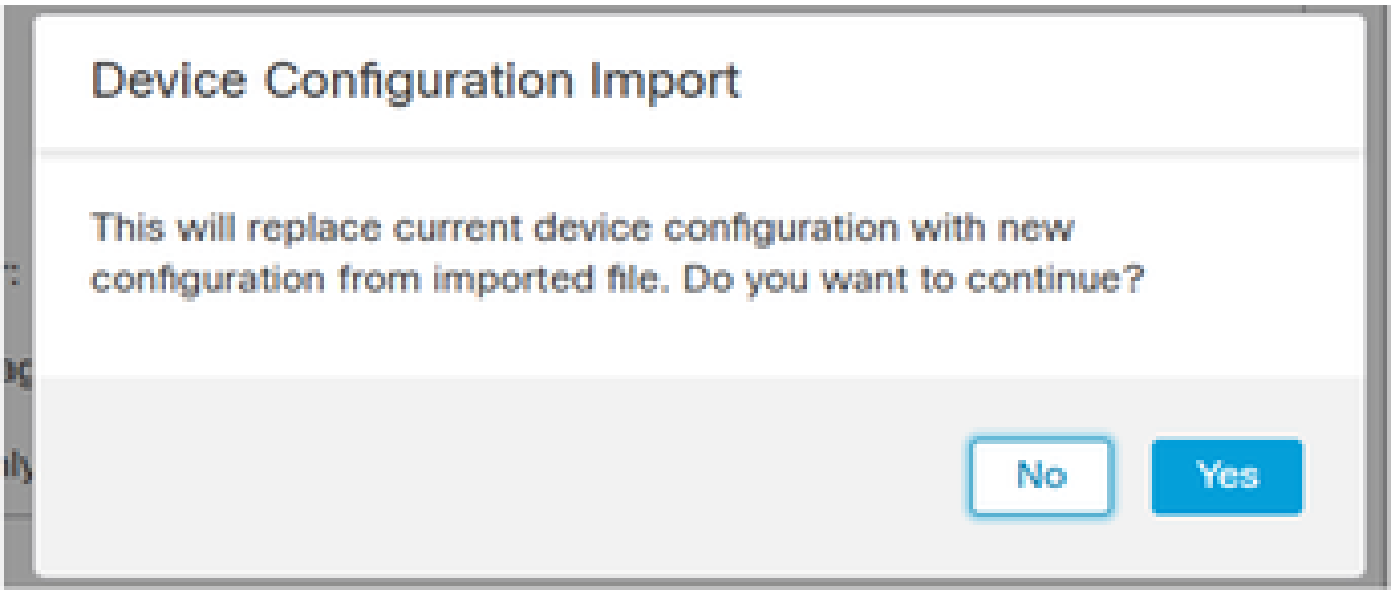
Stap 9. Importeer het configuratieobject van het FTD-apparaat in het FMC2 (doel-FMC)

Log in bij het FMC2 (doel-FMC), navigeer naar de Apparaten > Apparaatbeheer en bewerk het FTD-apparaat dat u in de vorige stap hebt geregistreerd.

Navigeer naar het tabblad Apparaat en importeer het sfeerobject FTD Policies dat u in stap 2 hebt geëxporteerd:

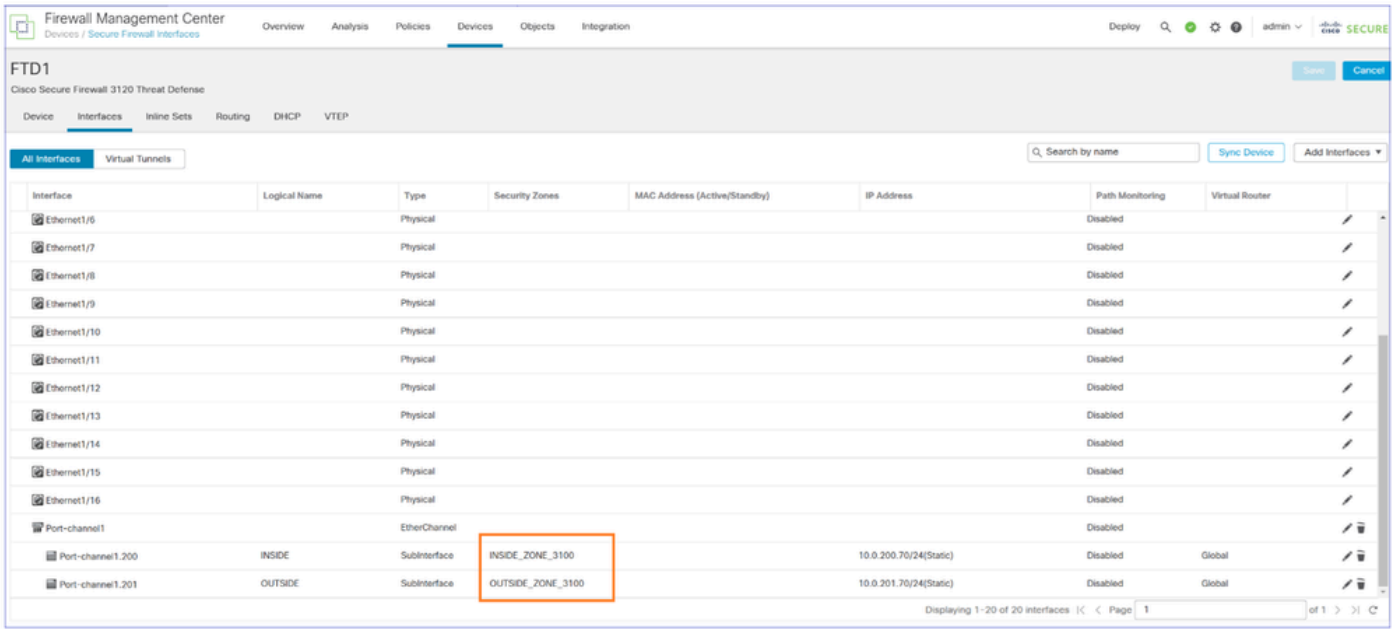


Opmerking: In het geval in Stap 7 ging u met optie 'b' (Maak een nieuw beleid), zorg ervoor dat u de nieuw gecreëerde objecten aan het gemigreerde beleid (ACS-beveiligingszones, NAT-beveiligingszones, routing, platforminstellingen, enzovoort).



Een VCC-taak wordt gestart.

De apparatenconfiguratie wordt toegepast op FTD1, bijvoorbeeld, de Zones van de Veiligheid, ACS, NAT, etc.:



⚠ Voorzichtig: Als u een ACS hebt die zich uitbreidt tot vele Access Control Elements, kan het ACS-compilatieproces (tmatch compileren) enkele minuten duren om te voltooien. U kunt deze opdracht gebruiken om de ACS-compilatiestatus te verifiëren:

```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

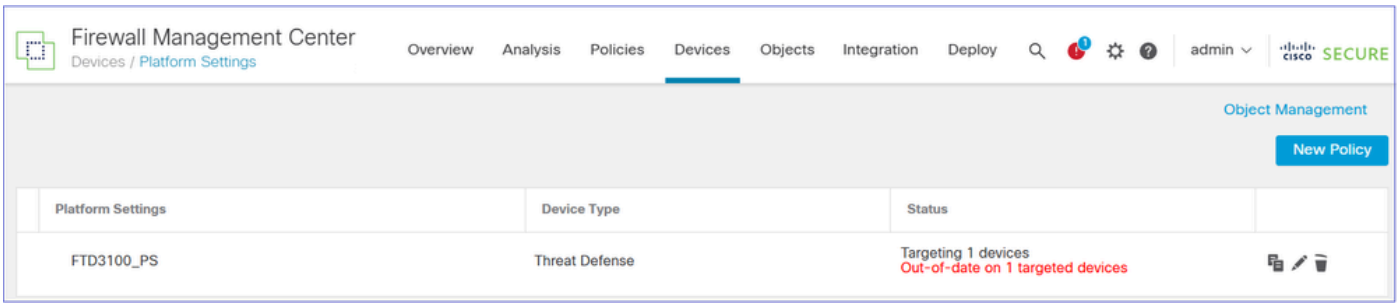
Stap 10. De FTD-configuratie voltooien

Op dit punt is het doel het configureren van alle functies die nog kunnen ontbreken in FTD1 na de

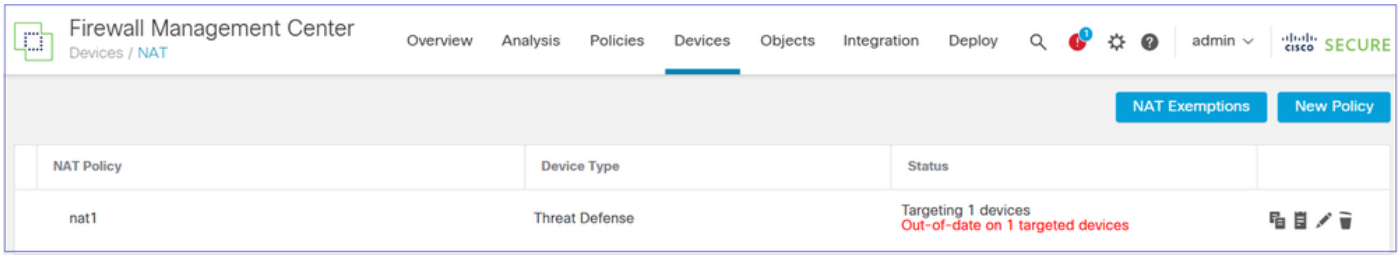
registratie in het FMC2 (doel FMC) en de import van het apparaatbeleid.

Zorg ervoor dat beleid zoals NAT, de Instellingen van het Platform, QoS, etc. worden toegewezen aan het FTD. U ziet dat de beleidsregels zijn toegewezen maar in behandeling zijn.

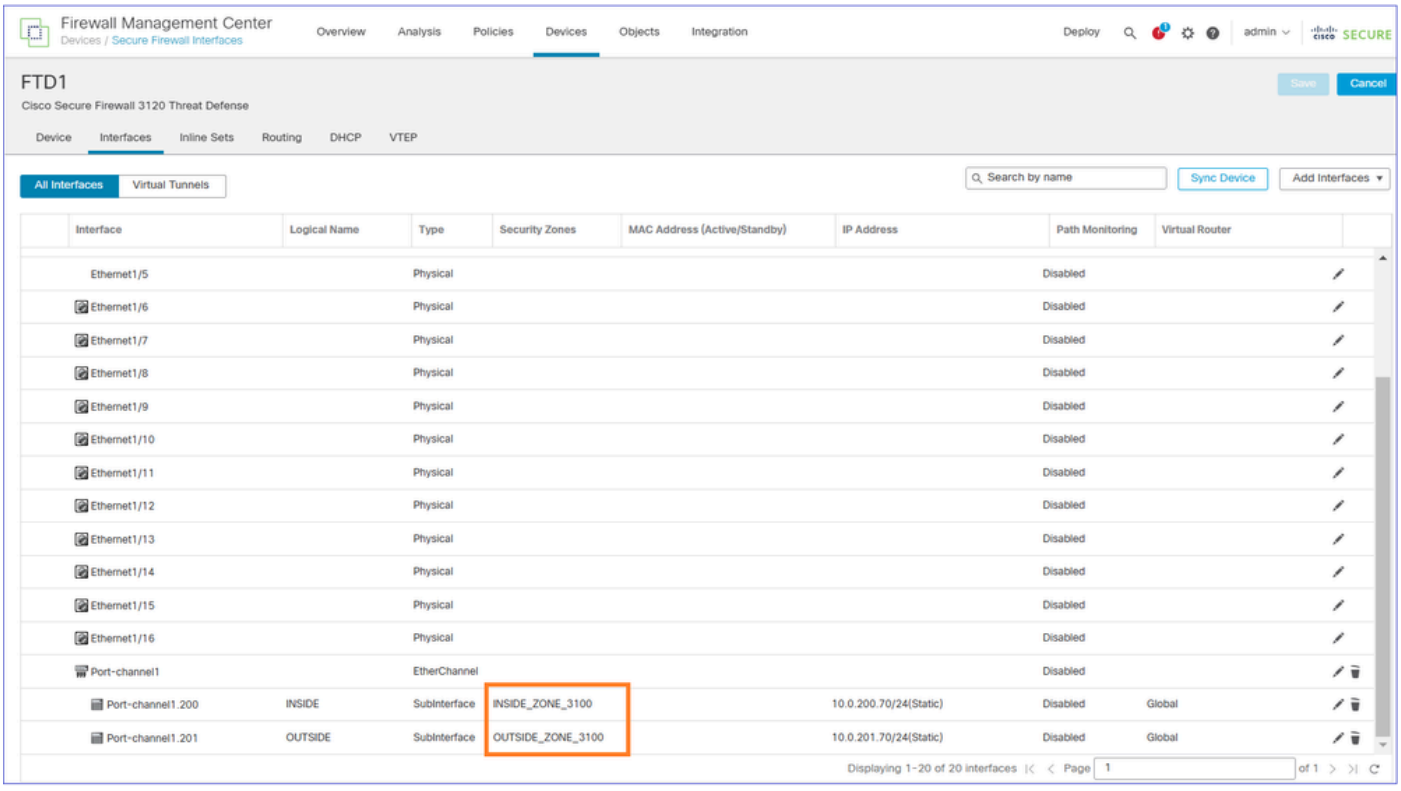
Platform-instellingen worden bijvoorbeeld geïmporteerd en toegewezen aan het apparaat, maar in afwachting van de implementatie:



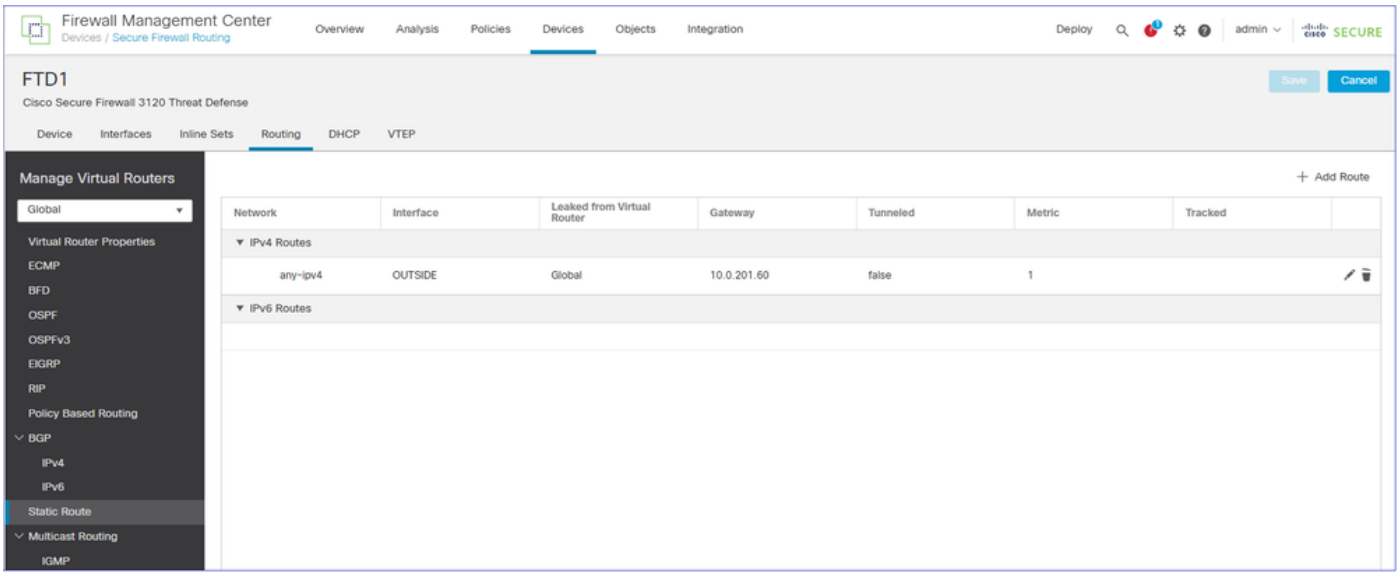
Als NAT is geconfigureerd, wordt het NAT-beleid geïmporteerd en aan het apparaat toegewezen, maar in afwachting van de implementatie:



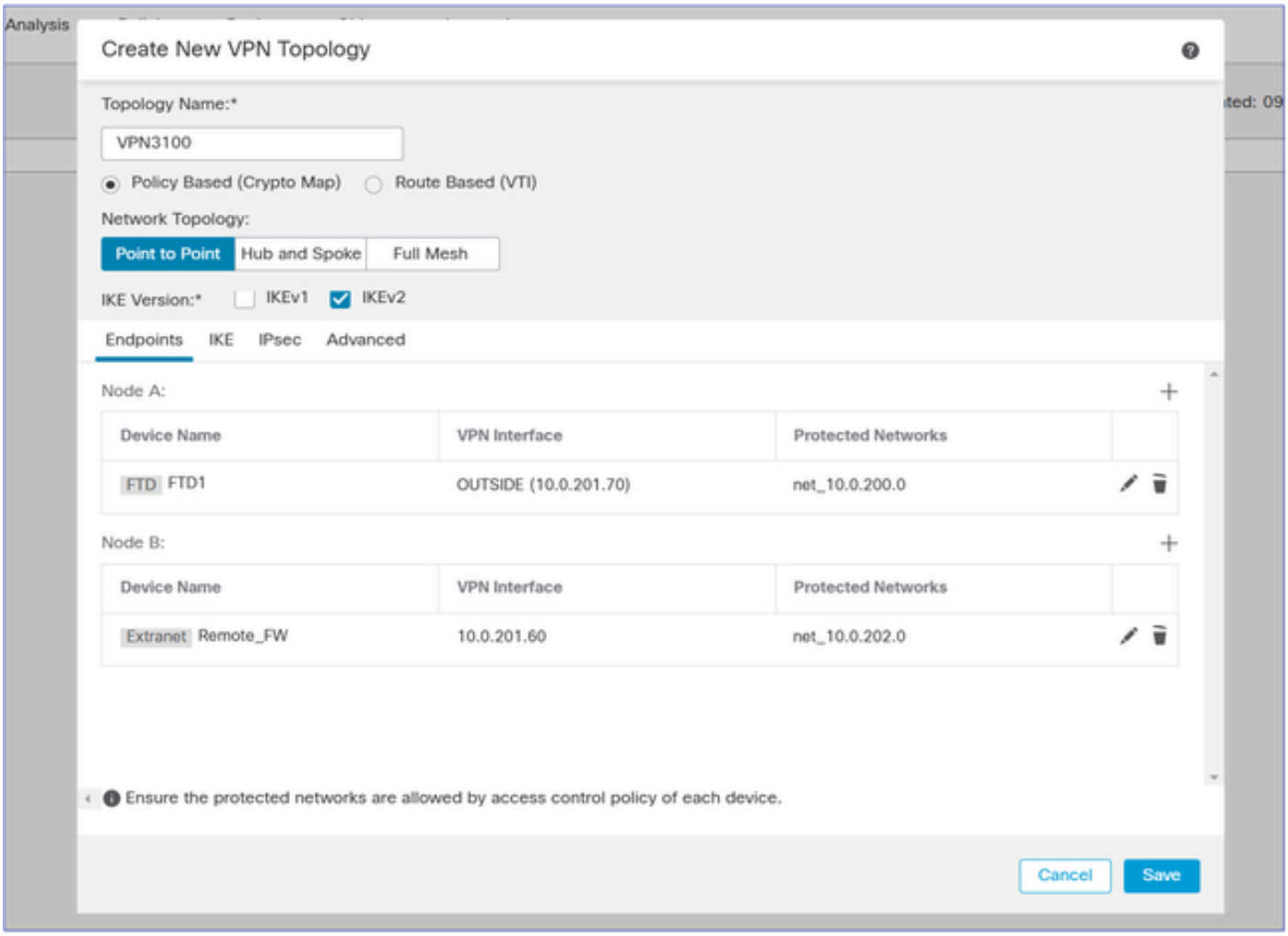
Security Zones worden toegepast op de interfaces:



Routing-configuratie wordt toegepast op het FTD-apparaat:



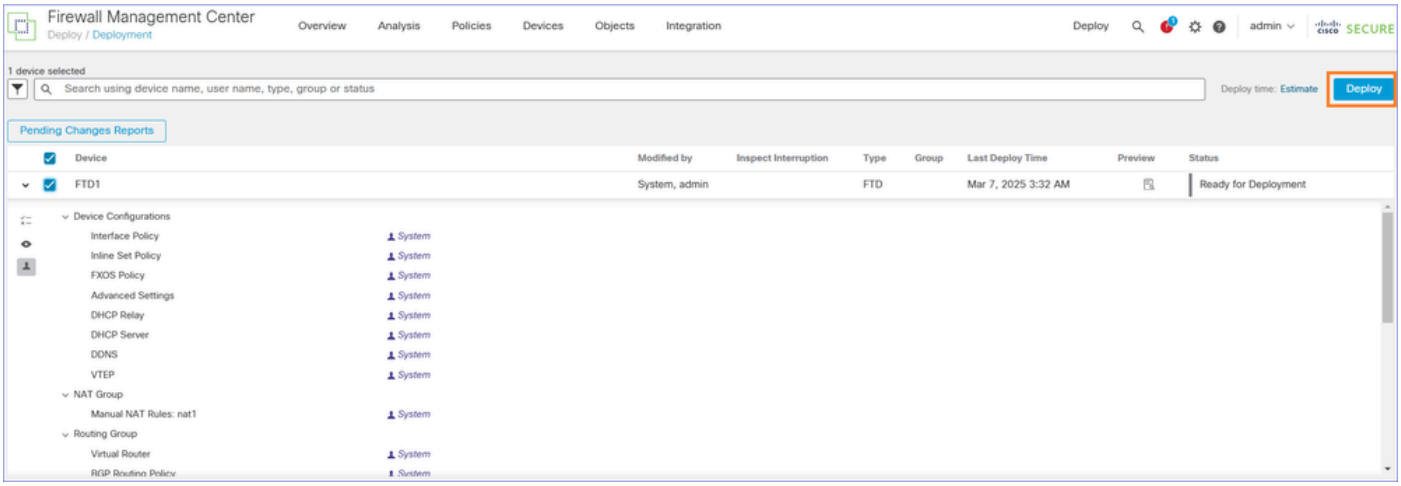
Opmerking: Nu is het tijd om het beleid te configureren dat niet automatisch kan worden gemigreerd (bijvoorbeeld VPN's).



Opmerking: Indien de FTD die gemigreerd is, beschikt over S2S VPN-peers die ook naar het

doel-FMC zijn gemigreerd, moet u de VPN configureren na alle FTD's naar het doel-FMC te hebben verplaatst.

Breng de hangende veranderingen in:



Stap 1. Controleer de geïmplementeerde FTD-configuratie

Op dit punt is het doel om vanuit de FTD CLI te controleren of alle configuratie aanwezig is.

De suggestie is om de 'show running-config' uitvoer van beide FTDs te vergelijken. U kunt tools zoals WinMerge of diff gebruiken voor de vergelijking.

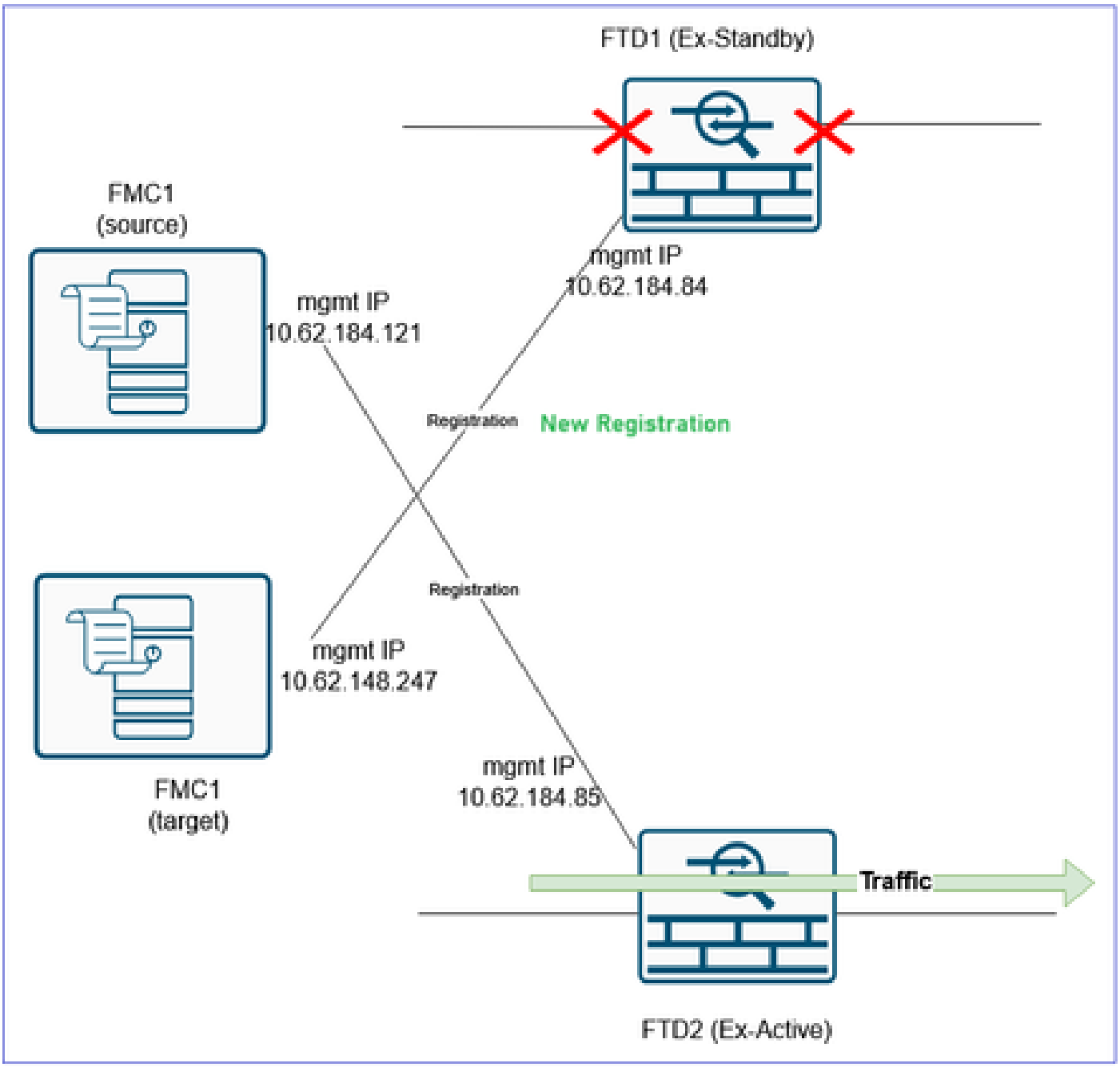
Verschillen die u ziet en die normaal zijn, zijn:

- Serienummer van apparaat
- Interfacebeschrijvingen
- ACL-regel-id's
- Configuration Cryptochecksum

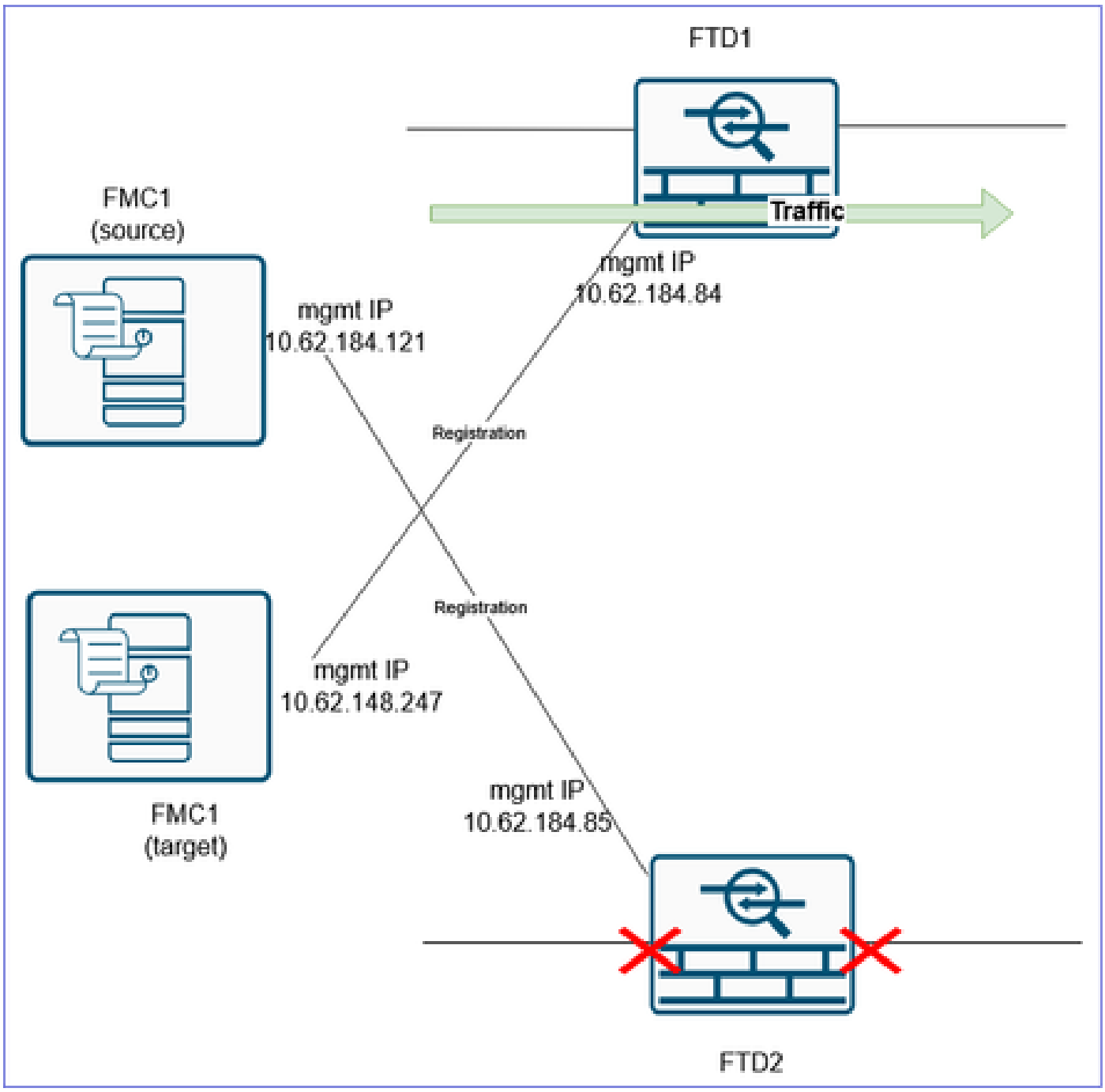
Stap 12. Voer de cutover uit

In deze stap is het doel het verkeer te switches van het FTD2 dat momenteel het verkeer verwerkt en nog steeds geregistreerd is naar het FTD1 dat bij het beoogde FMC is geregistreerd.

Voor:


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)

Na:



⚠ Voorzichtig: Schik een MW om de cutover te doen. Tijdens de cutover krijg je wat verkeersonderbreking totdat al het verkeer is omgeleid naar de FTD1, VPN's zijn hersteld, enzovoort.

⚠ Voorzichtig: Start de cutover niet tenzij de ACS-compilatie is voltooid (zie stap 10 hierboven).

⚠ Waarschuwing: Zorg ervoor dat u de gegevenskabels loskoppelt van de FTD2 of de gerelateerde switchpoorten uitschakelt. Anders kunt u eindigen met beide apparaten die het verkeer afhandelen!

⚠ Voorzichtig: Aangezien beide apparaten dezelfde IP-configuratie gebruiken, moet het ARP-

⚠ cache van de aangrenzende L3-apparaten worden bijgewerkt. Overweeg de arp cache van de aangrenzende apparaten handmatig te verwijderen om de traffic cutover te versnellen.

Tip: U kunt ook een GARP-pakket verzenden en de ARP-cache van de aangrenzende apparaten bijwerken met de FTD CLI-opdracht:

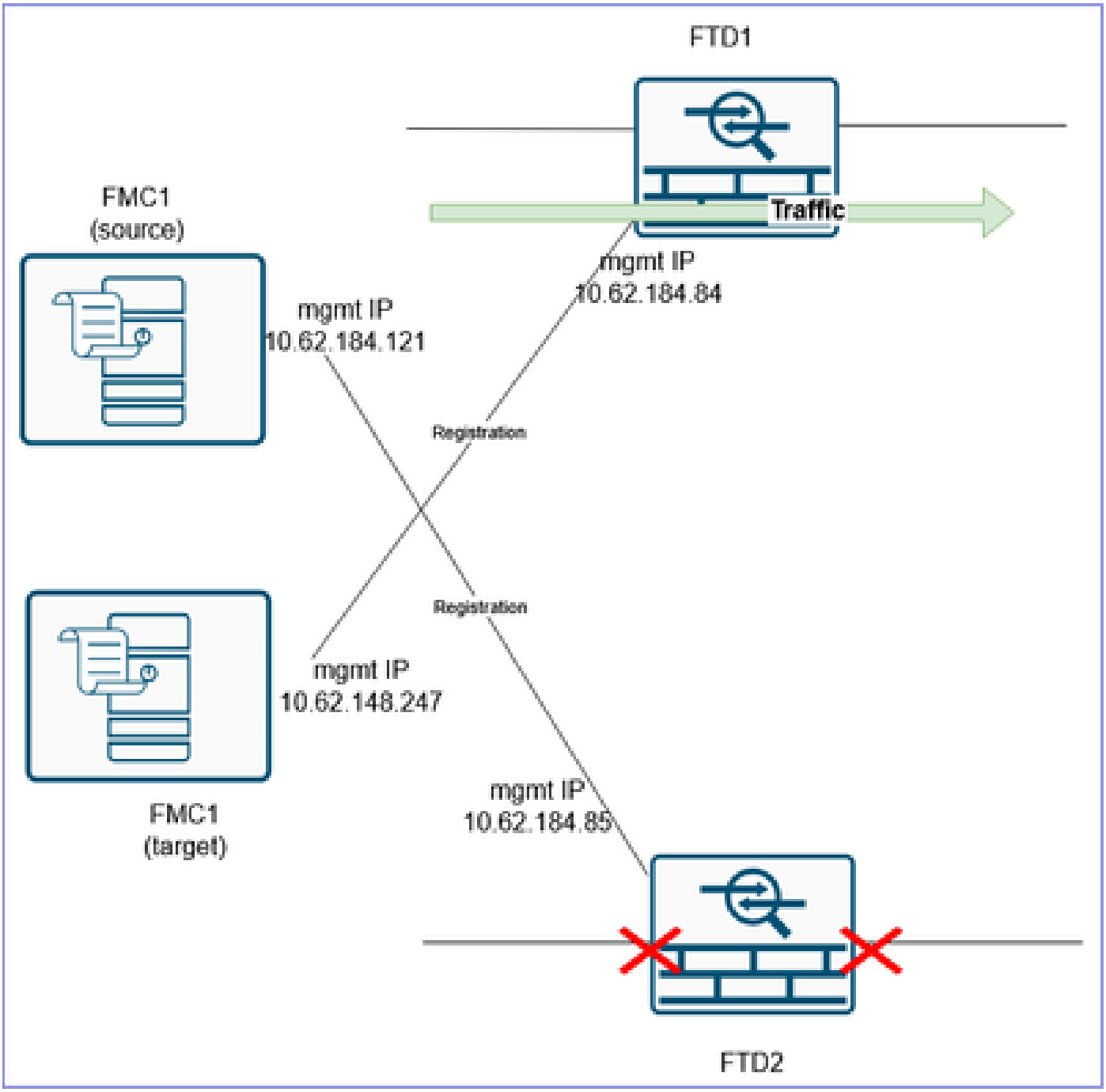
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

U moet deze opdracht herhalen voor elke IP die de FW bezit. Aldus, kan het sneller zijn om het ARP geheim voorgeheugen van de aangrenzende apparaten enkel te ontruimen dan het verzenden van pakketten GARP voor elke IP de firewall bezit.

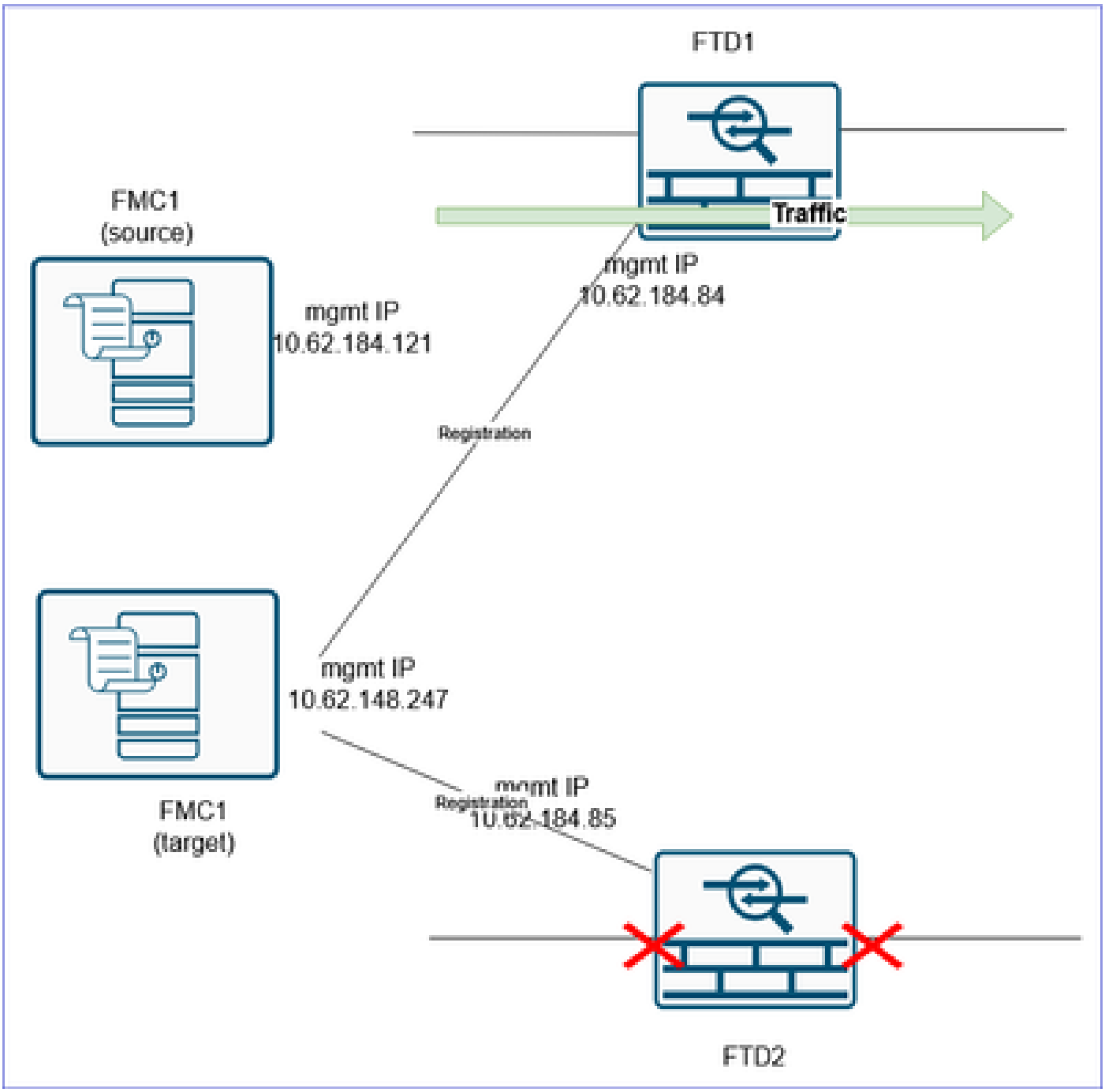
Stap 13. Migreren van het tweede FTD naar het FMC2 (doel-FMC)

Het laatste punt is het hervormen van het HA-paar. Hiertoe moet u eerst het FTD2 uit het FMC1 (bron-FMC) verwijderen en registreren bij het FMC2 (doel-FMC).

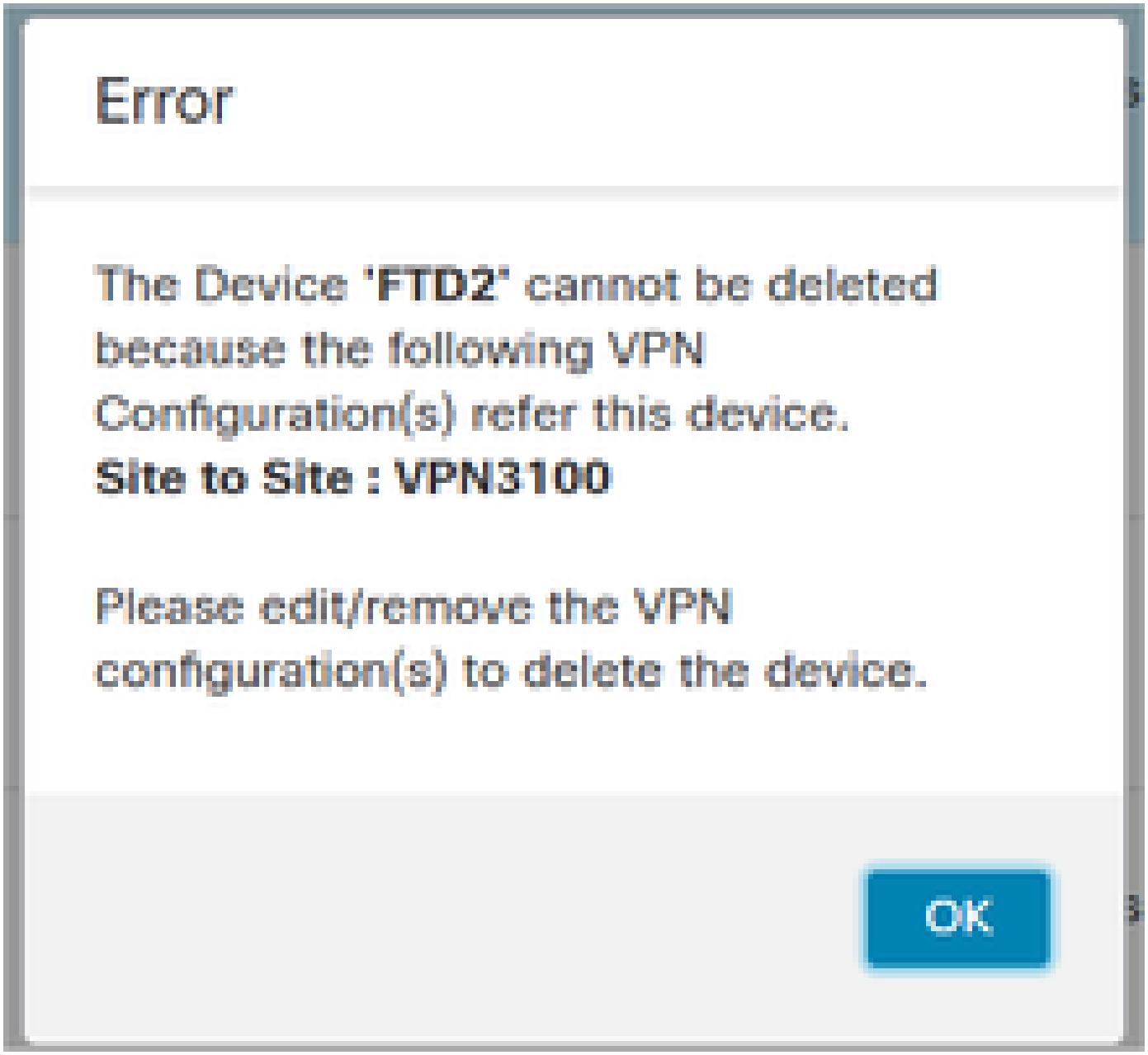
Voor:


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

Na:



Als u een VPN-configuratie hebt die aan de FTD2 is gekoppeld, moet u deze eerst verwijderen voordat u de FTD verwijdert. In andere gevallen wordt een soortgelijk bericht getoond:



CLI-verificatie:

<#root>

>

show managers

No managers configured.

Het is een goede gewoonte om alle FTD-configuratie te verwijderen voordat deze in het beoogde FMC wordt geregistreerd. Een snelle manier om dit te doen is door te switches tussen de firewallmodi.

Als u bijvoorbeeld de modus hebt gerouteerd, gaat u van switch naar transparant en vervolgens terug naar routed:

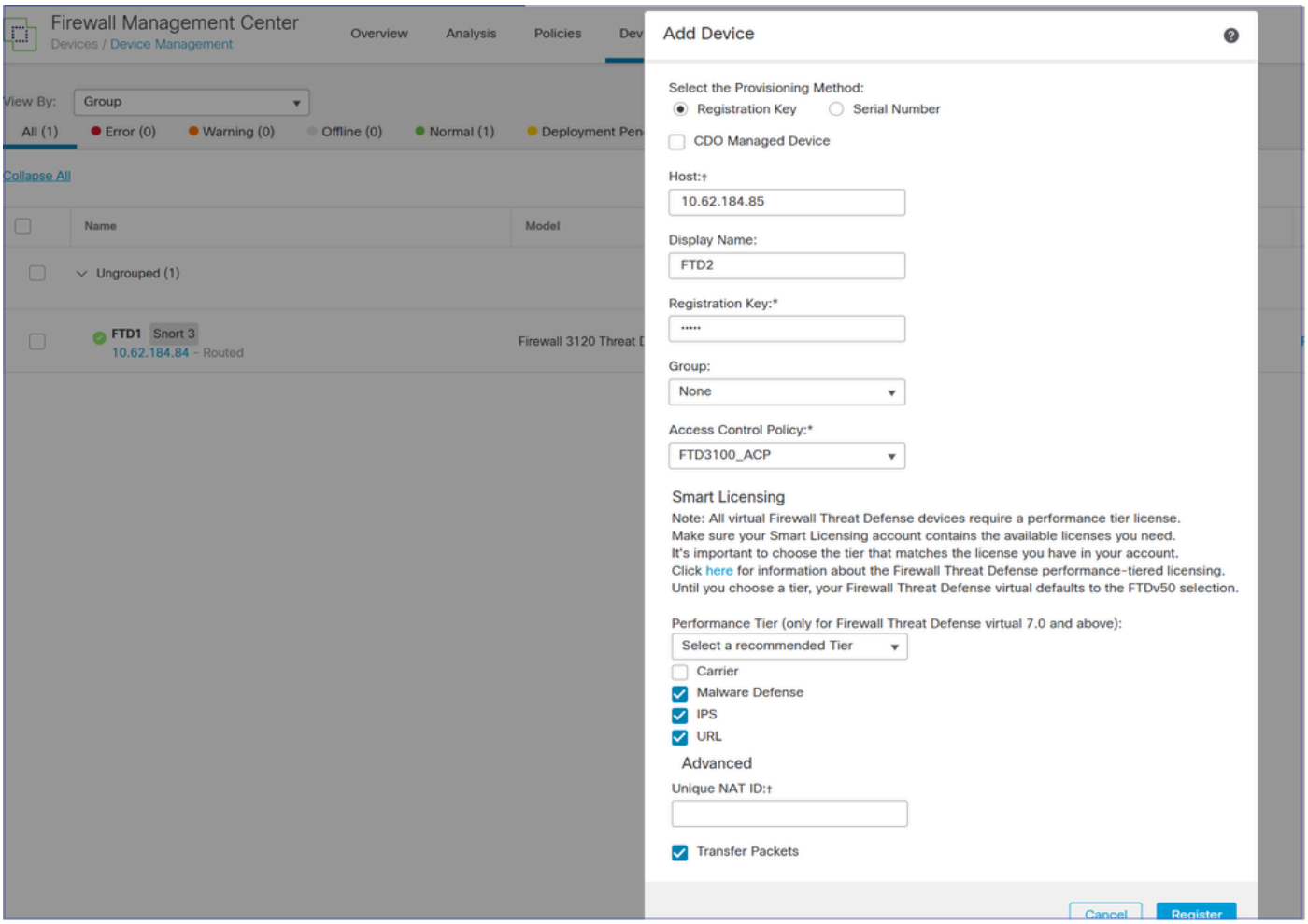
```
<#root>

>

configure firewall transparent
```

En dan:

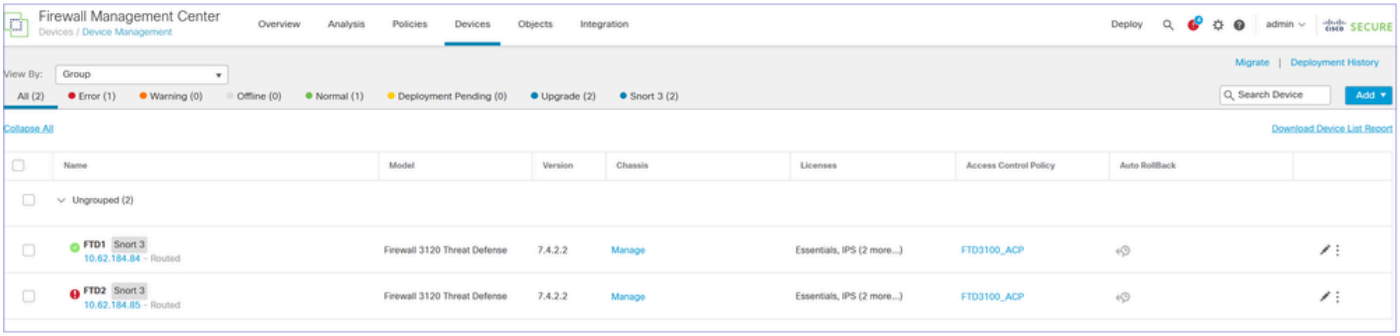
```
<#root>

>

configure firewall routed
```

Registreer dit vervolgens bij het VCC2 (doel-VCC):

```
<#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.
>
```



Het resultaat:

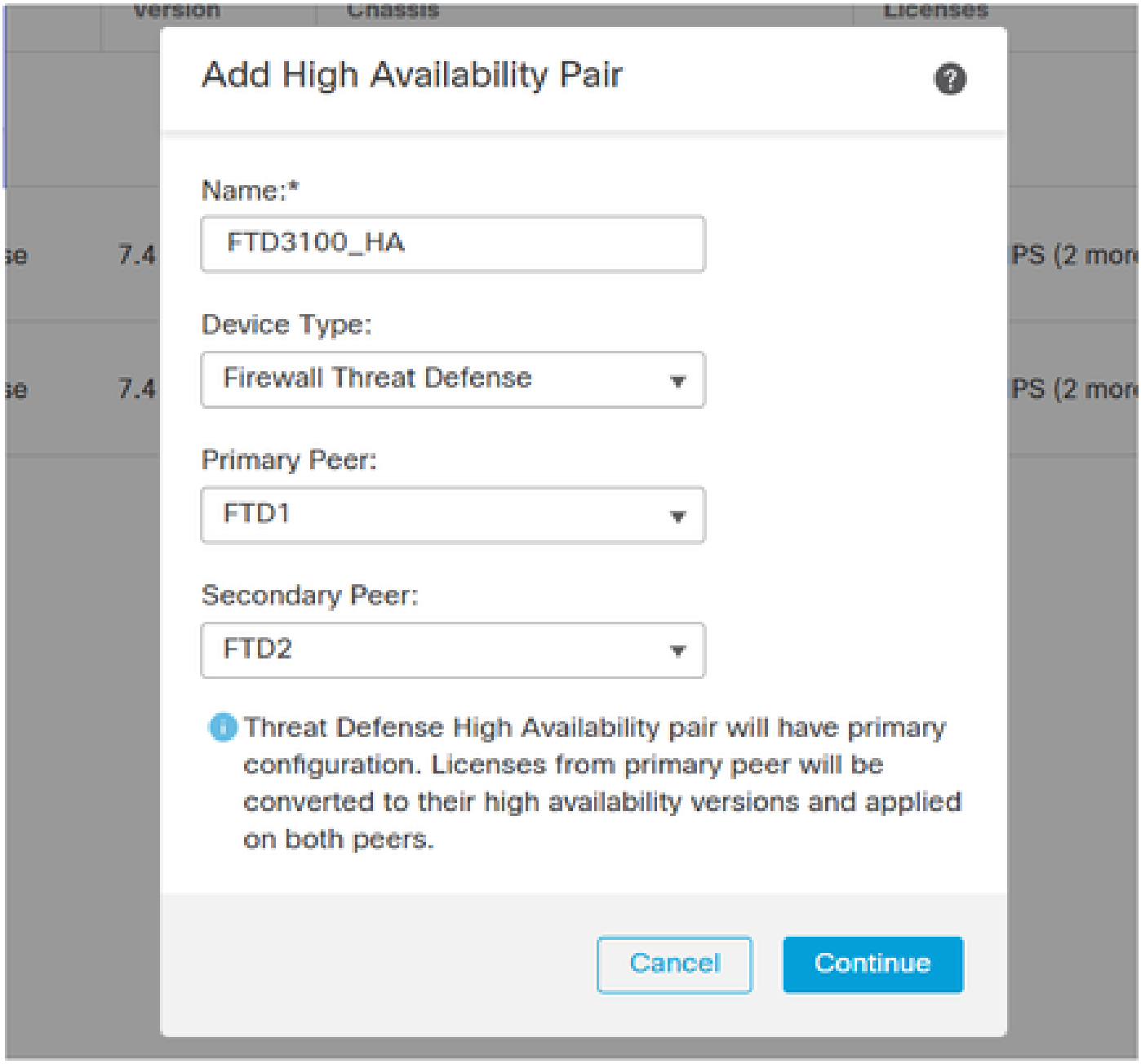


Stap 14. Hervorm de FTD HA

Opmerking: Deze taak (zoals elke HA-gerelateerde taak) moet ook worden uitgevoerd tijdens een MW. Tijdens de HA-onderhandeling is er een verkeersstoring voor ~1 minuut sinds de data-interfaces dalen.

Op het doel navigeren FMC naar Apparaten > Apparaatbeheer en toevoegen > Hoge beschikbaarheid.

⚠ Voorzichtig: Zorg ervoor dat u de FTD die het verkeer verwerkt, als primaire peer selecteert (FTD1 in dit scenario):



Herstel de HA-instellingen met inbegrip van bewaakte interfaces, stand-by IP's, virtuele MAC-adressen, enzovoort.

Verificatie via FTD1 CLI:

```
<#root>

FTD3100-3#

show failover | include host

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

Verificatie via FTD2 CLI:

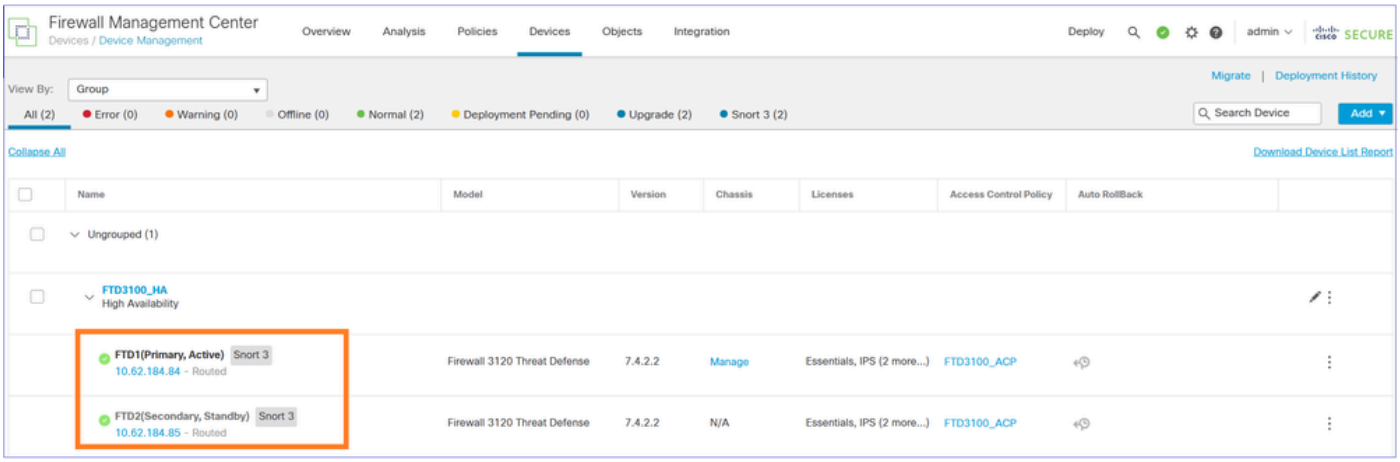
<#root>

FTD3100-3#

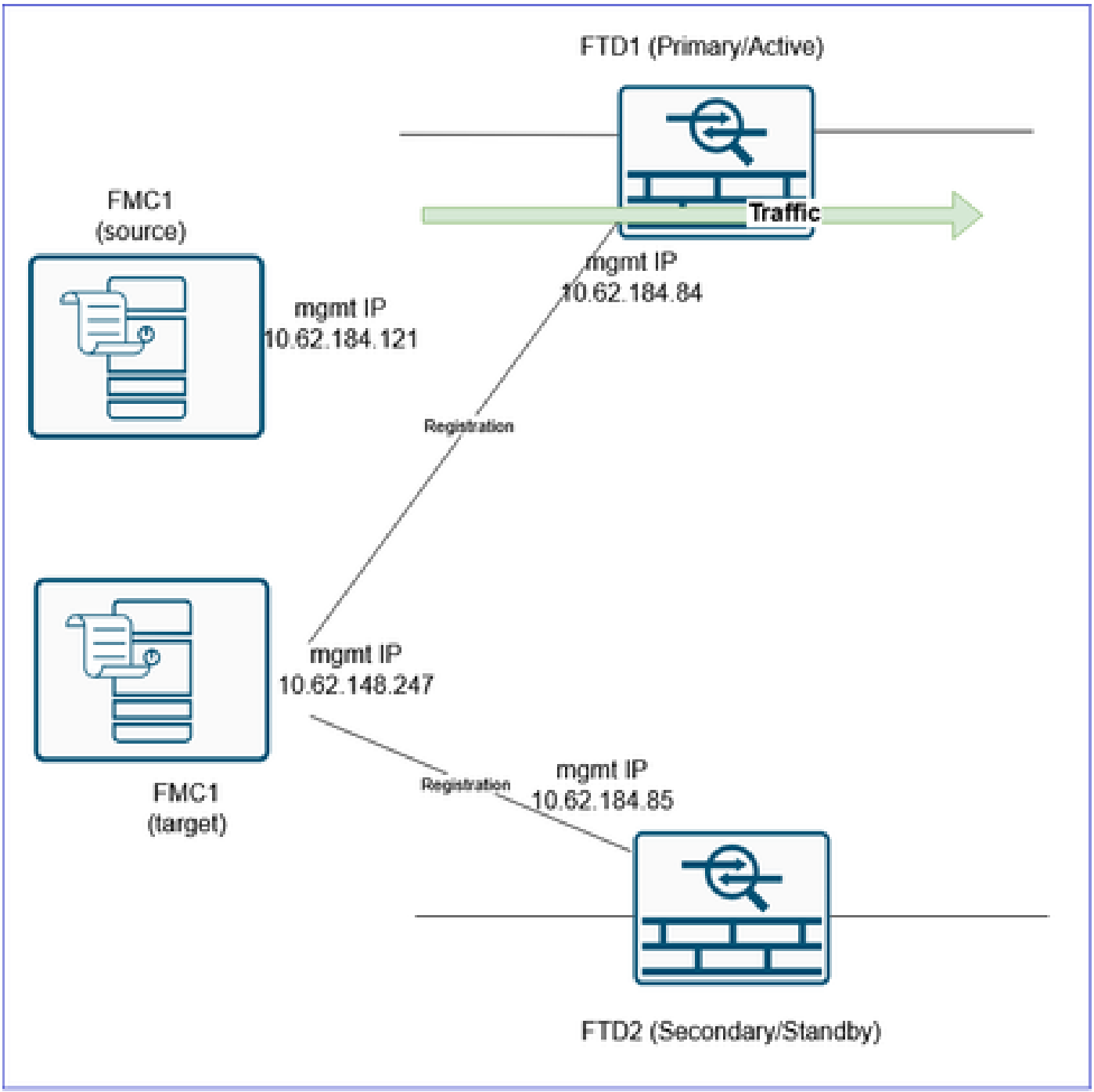
show failover | include host

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

Controle van de FMC UI:



Ten slotte de datainterfaces van het FTD2 apparaat samenbrengen/opnieuw aansluiten.



Referenties

- De apparaatconfiguratie exporteren en importeren
- Voeg een paar met hoge beschikbaarheid toe
- Migratie van een VHK van het ene VCC naar een ander VCC

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.