

FTD HA (failover) migreren naar een ander FMC

Inhoud

[Inleiding](#)

[Afkortingen](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Topologie](#)

[Configureren](#)

[Stap 1. Exporteer de apparaatconfiguratie vanuit de primaire firewall](#)

[Stap 2. Maak het secundaire FTD actief](#)

[Stap 3. Breek de FTD HA](#)

[Stap 4. Isoleer de FTD1 \(ex-Primair\) data-interfaces](#)

[Stap 5. Exporteer het FTD gedeelde beleid](#)

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

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

[Stap 8. Registreer het FTD1 \(ex-Primair\) in het FMC2](#)

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

[Stap 10. De FTD-configuratie voltooien](#)

[Stap 11. Controleer de geïmplementeerde FTD-configuratie](#)

[Stap 12. Voer de cutover uit](#)

[Stap 13. Migreren van het tweede FTD naar het FMC2 \(doel-FMC\)](#)

[Stap 14. Hervorm de FTD HA](#)

[Referenties](#)

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:

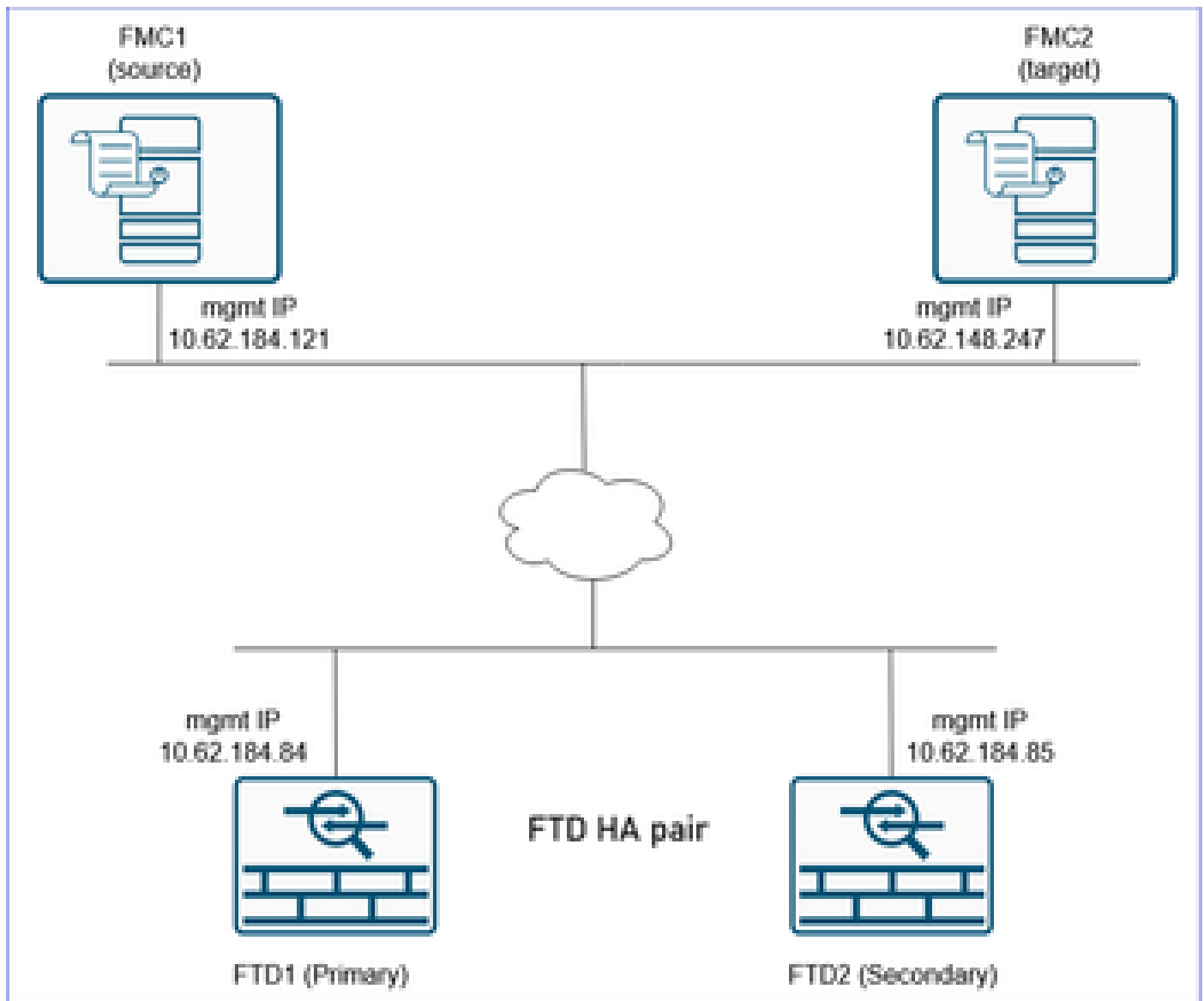
- UI- en CLI-toegang tot zowel de FMC's van herkomst als van bestemming.
- Administratieve referenties voor zowel VCC's als firewalls.
- De toegang van de console tot beide firewalls.
- Toegang tot de L3 upstream en downstream apparaten (voor het geval dat je de ARP cache moet wissen).
- Zorg ervoor 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



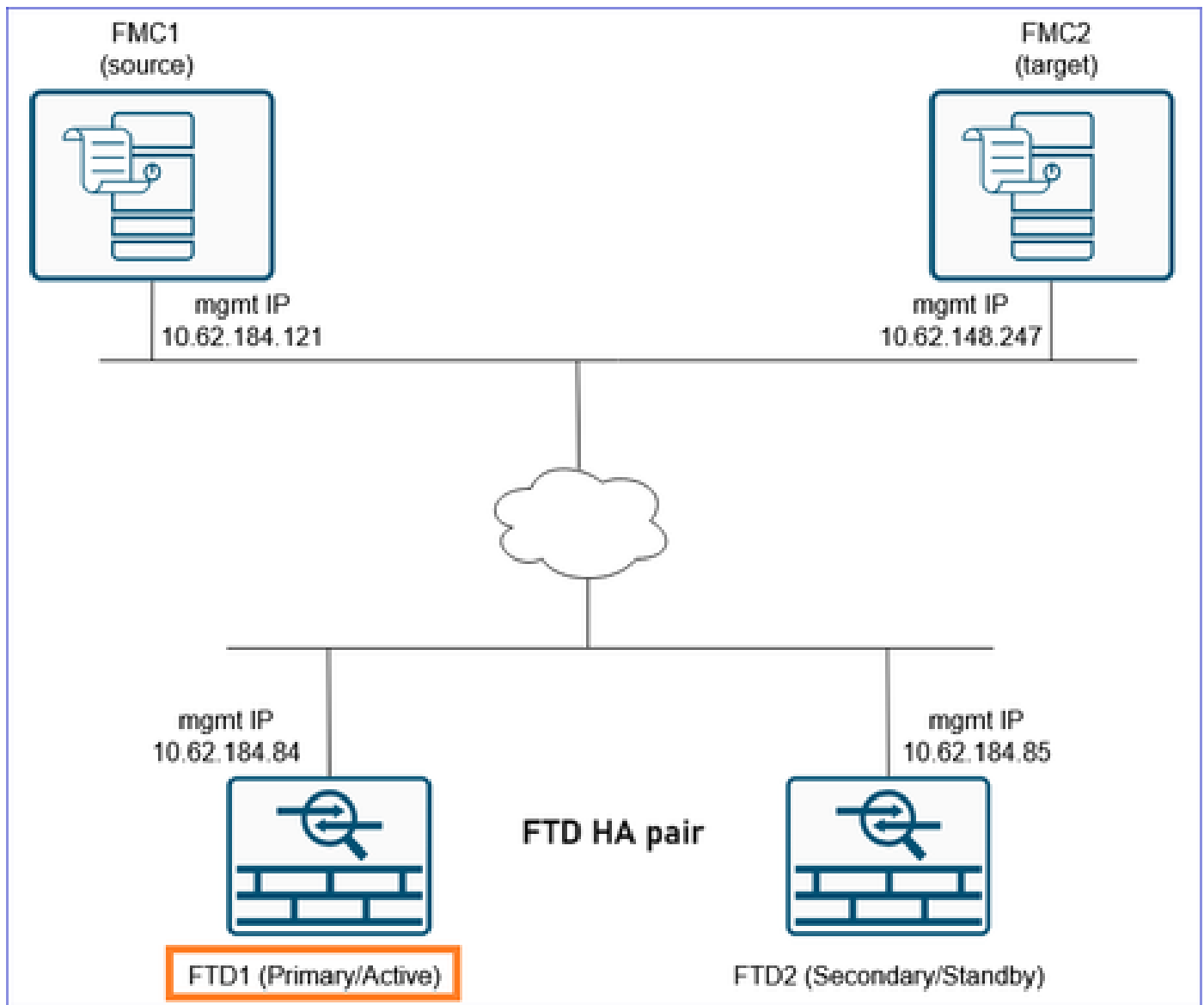
Configureren

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:

Firewall Management Center								
Devices / Device Management								
Overview Analysis Policies Devices Objects Integration								
Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE								
View By: Group								
All (4) Error (0) Warning (2) Offline (0) Normal (2) Deployment Pending (2) Upgrade (2) Snort 3 (4)								
Collapse All								
☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	FTD_HA (1)							
☐	FTD3100_HA High Availability							
▲	FTD1(Primary, Active) 10.62.184.84 - Routed	Snort 3	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	⌵
▲	FTD2(Secondary, Standby) 10.62.184.85 - Routed	Snort 3	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	⌵

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:

Firewall Management Center
Devices / Secure Firewall Device Summary

Overview Analysis Policies **Devices** Objects Integration Deploy

FTD3100_HA
Cisco Secure Firewall 3120 Threat Defense

Summary High Availability **Device** Interfaces Inline Sets Routing DHCP VTEP

1 FTD1

General	System
Name: FTD1	Model: Cisco Secure Firewall 3120 Threat Defense
Troubleshoot: Logs CLI Download	Serial: FJZ254600PB
Mode: Routed	Time: 2025-03-07 07:51:23
Compliance Mode: None	Time Zone: UTC (UTC+0:00)
TLS Crypto Acceleration: Enabled	Version: 7.4.2.2
Device Configuration: Import Export Download	Time Zone setting for Time based Rules: UTC (UTC+0:00)
OnBoarding Method: Registration Key	Inventory: View

2

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:

Deploy

Deployments Upgrades **Health** **Tasks**

20+ total 0 waiting 0 running 0 retrying 20+ success 0 fail

Device Configuration Export

Export file created successfully

[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

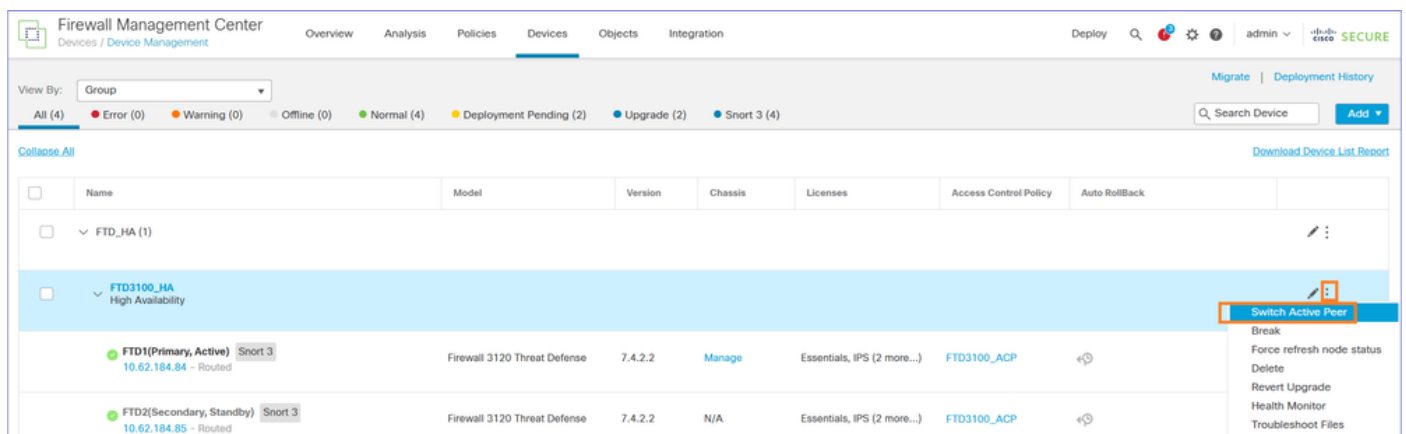
Opmerking: Het geëxporteerde configuratiebestand kan alleen terug naar dezelfde FTD worden geïmporteerd. De UUID van de FTD moet overeenkomen met de inhoud van het geïmporteerde Sfo-bestand. Hetzelfde FTD kan worden geregistreerd in een ander FMC en sfo-bestand kan worden geïmporteerd.

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-ecccc8b72b7c8

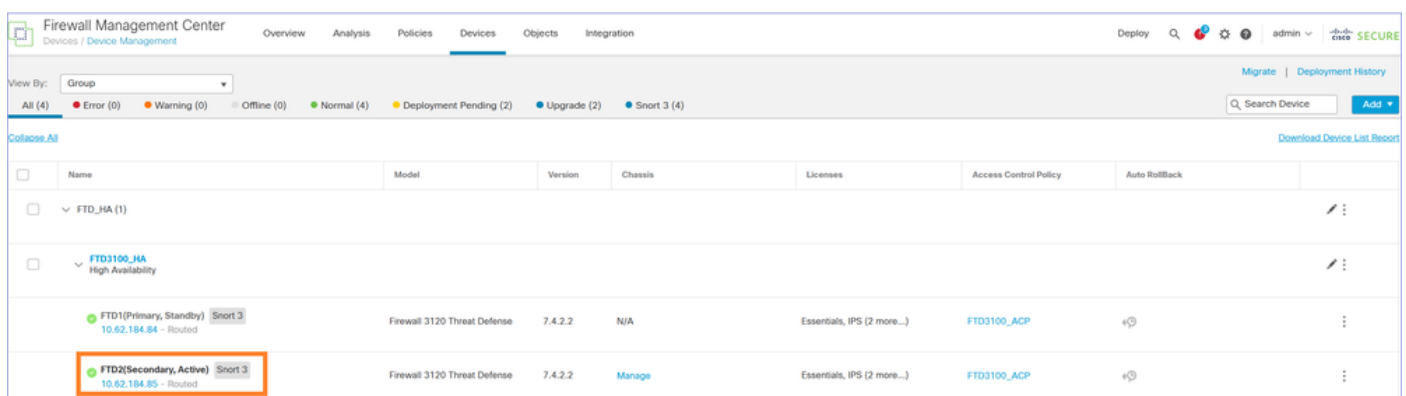
Stap 2. Maak het secundaire FTD actief

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



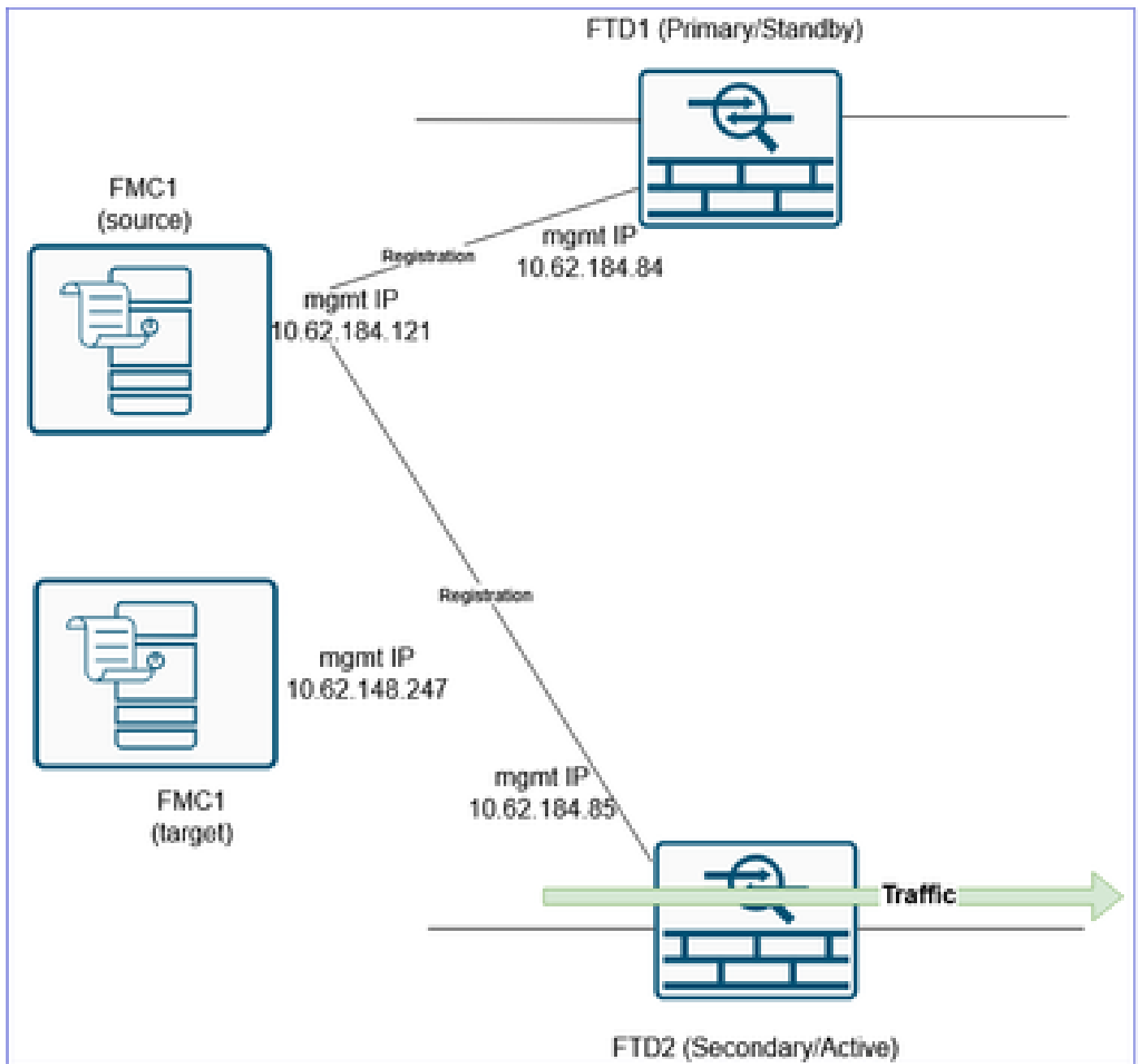
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (1)						
FTD3100_HA High Availability						
FTD1(Primary, Active) 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+⌵
FTD2(Secondary, Standby) 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	+⌵

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



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (1)						
FTD3100_HA High Availability						
FTD1(Primary, Standby) 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	+⌵
FTD2(Secondary, Active) 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+⌵

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:

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is selected, displaying a table of devices. The table has columns for Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The table lists two devices: FTD1 (Primary, Standby) and FTD2 (Secondary, Active). A context menu is open for FTD2, with the 'Break' option highlighted.

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	+⌵

Dit venster verschijnt. Selecteer Ja

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

 **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#

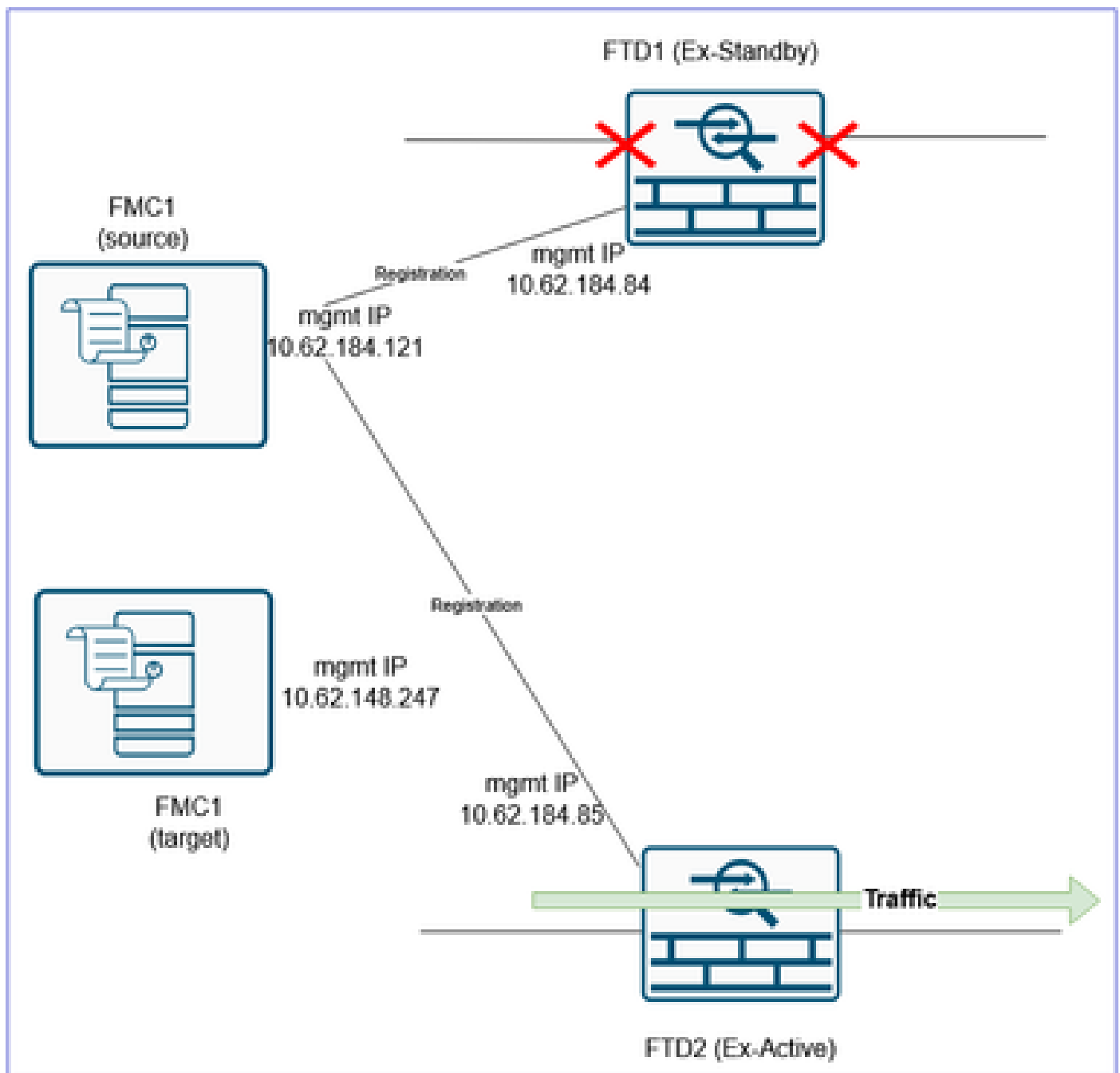
show interface ip brief

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

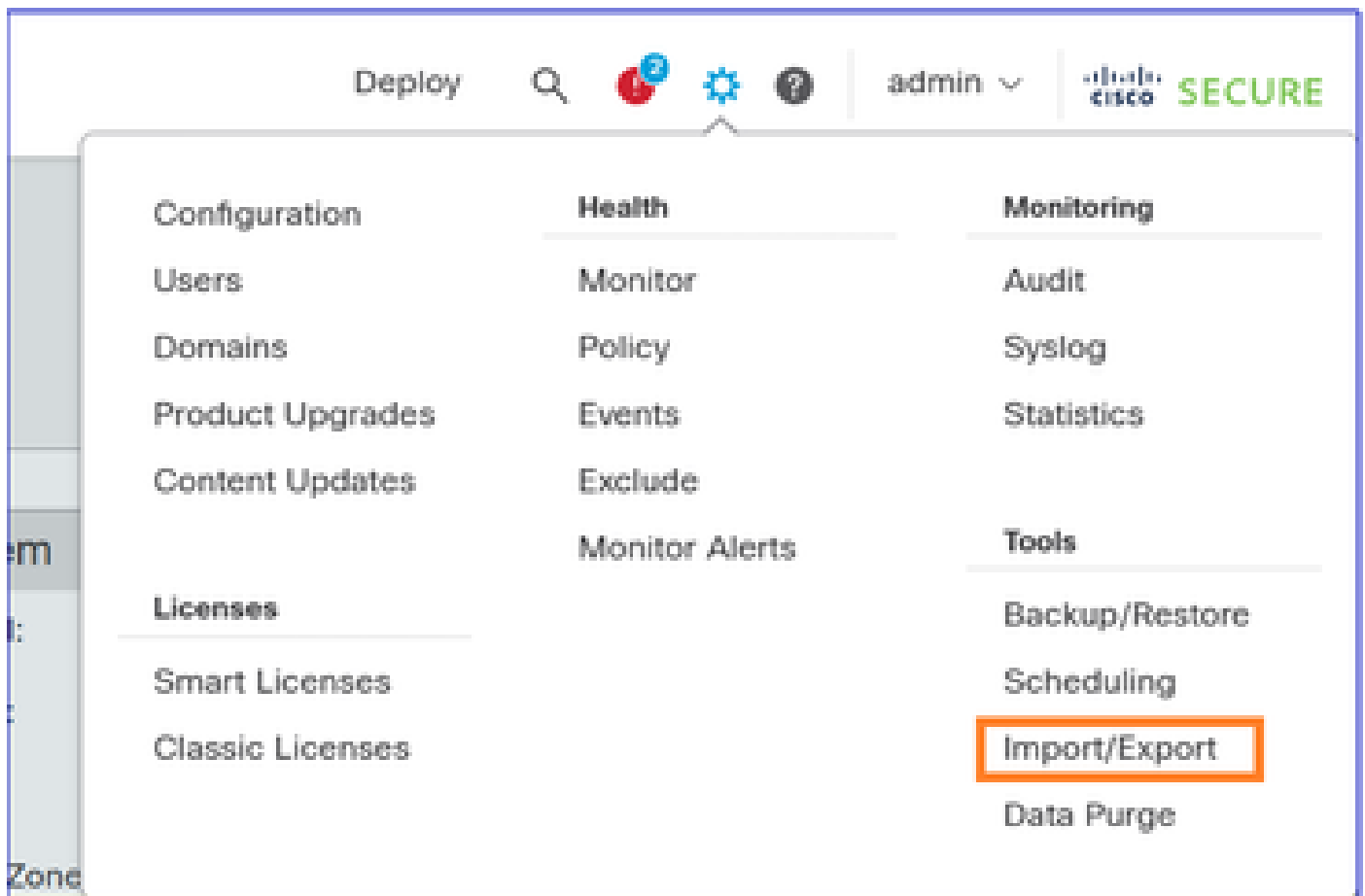
Stap 4. Isoleer de FTD1 (ex-Primair) data-interfaces

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



Stap 5. Exporteer het FTD gedeelde beleid

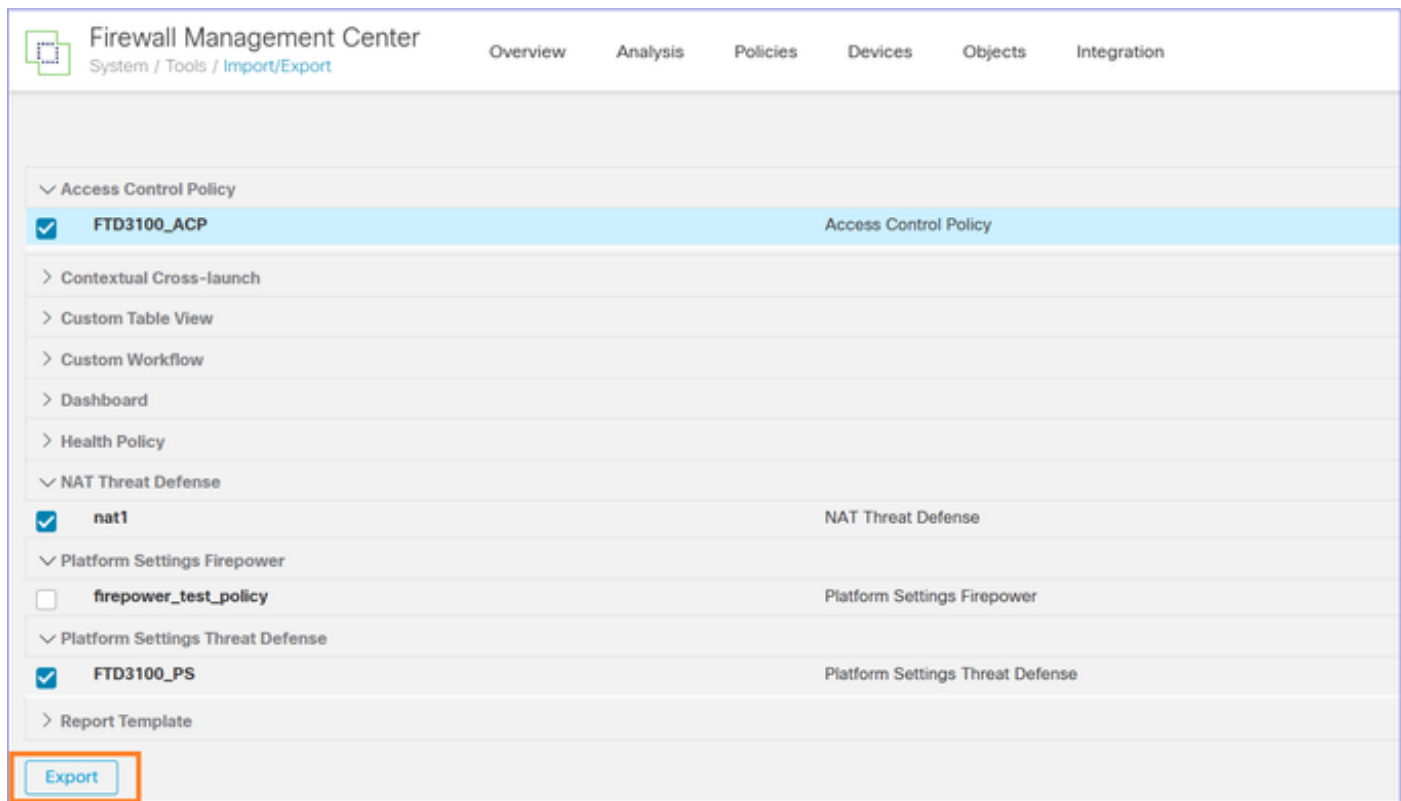
Navigeer naar Systeem > Tools en selecteer Importeren/Exporteren:



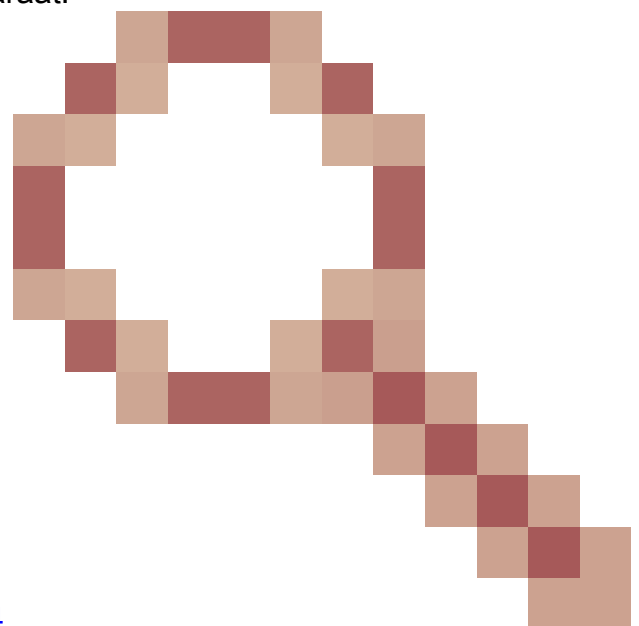
Exporteer de verschillende beleidsregels die aan het apparaat zijn gekoppeld. Zorg ervoor dat u alle aan de FTD gehechte beleidslijnen exporteert, zoals:

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

en ga zo maar door.



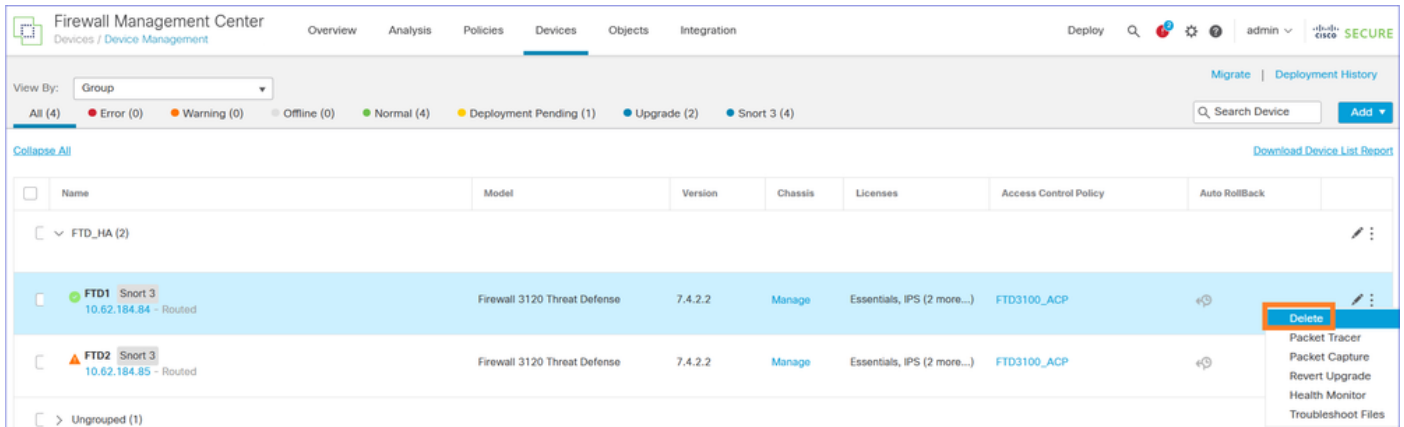
Opmerking: Op het moment van schrijven wordt de export van VPN-gerelateerde configuratie niet ondersteund. U moet de VPN handmatig opnieuw configureren op het FMC2 (doel-FMC) na de registratie van het apparaat.



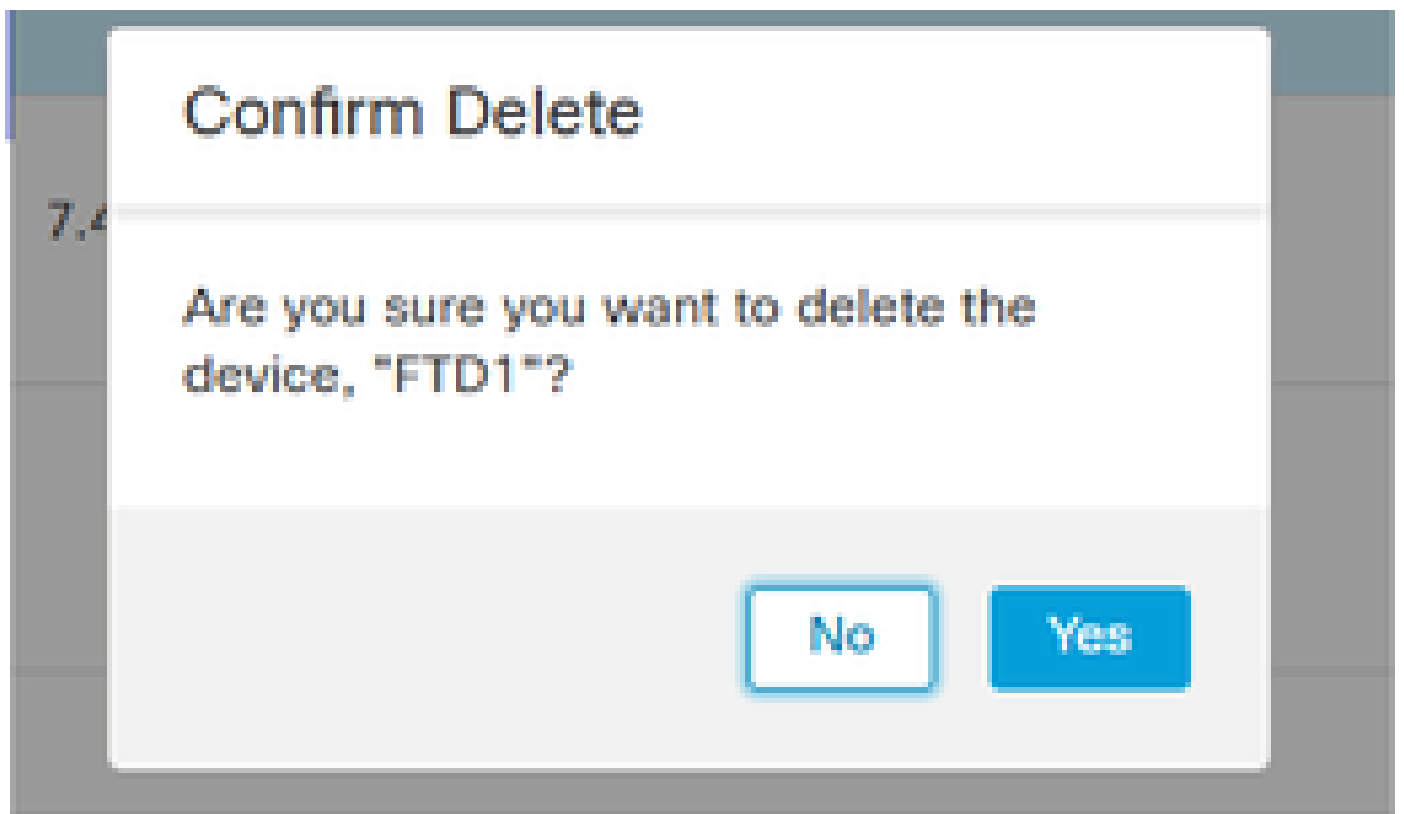
Verwante verbetering Cisco bug-id [CSCwf05294](https://tools.cisco.com/bugcenter/bug/?bugID=CSCwf05294)

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>
```

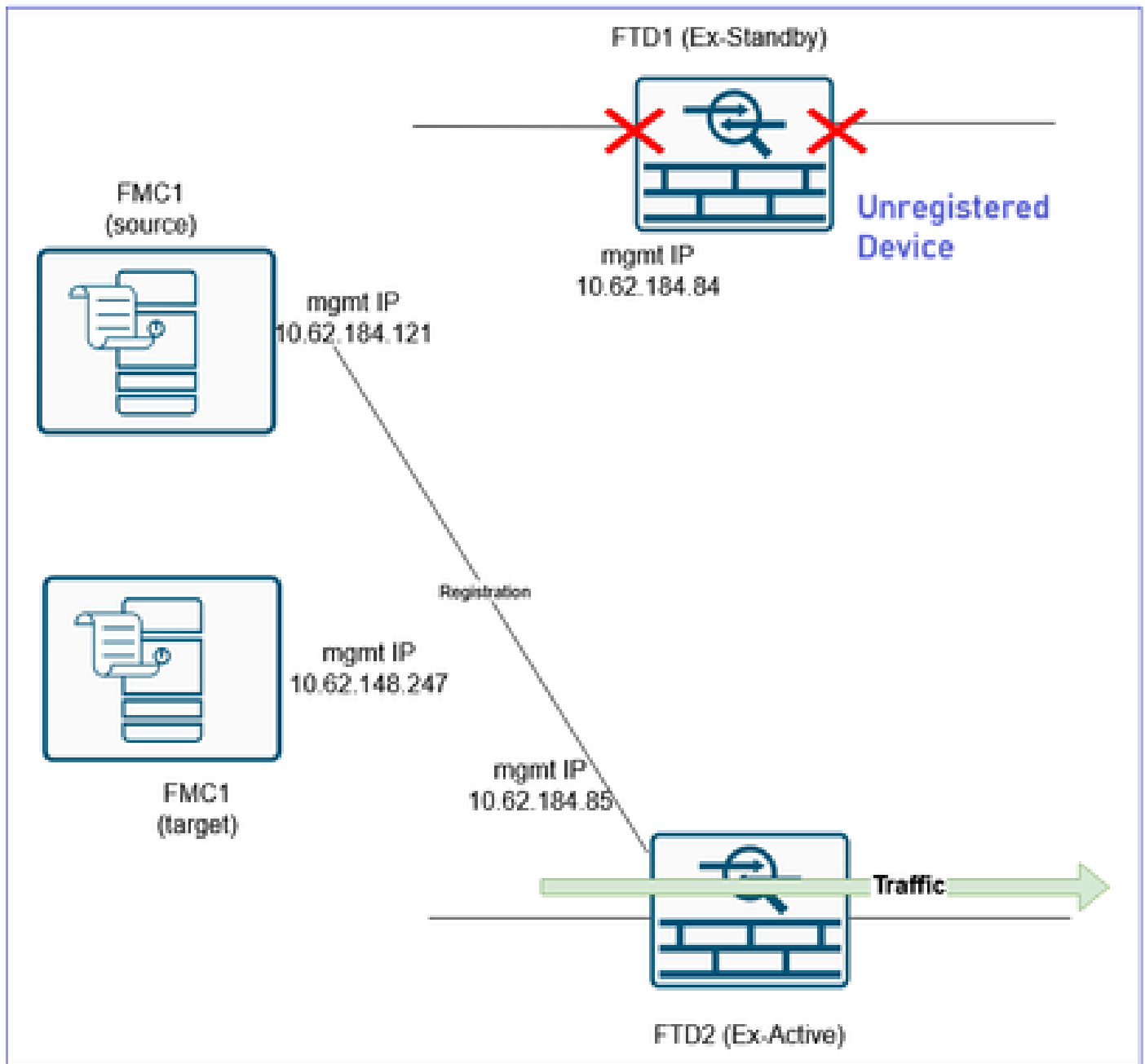
```
>
```

```
show managers
```

```
No managers configured.
```

```
>
```

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

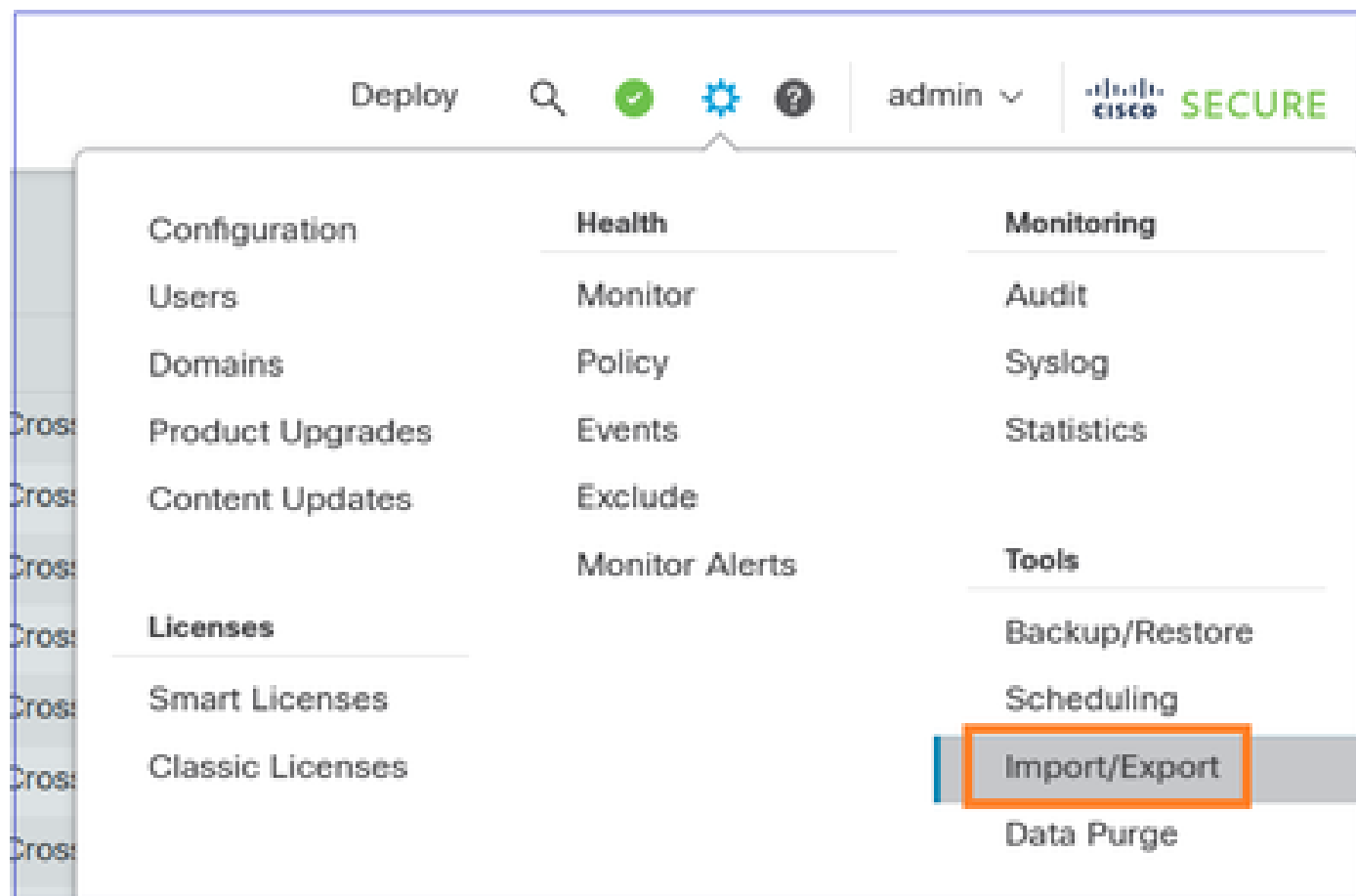


Stap 7. Importeer het configuratieobject van het FTD Policy in het FMC2 (doel-FMC)

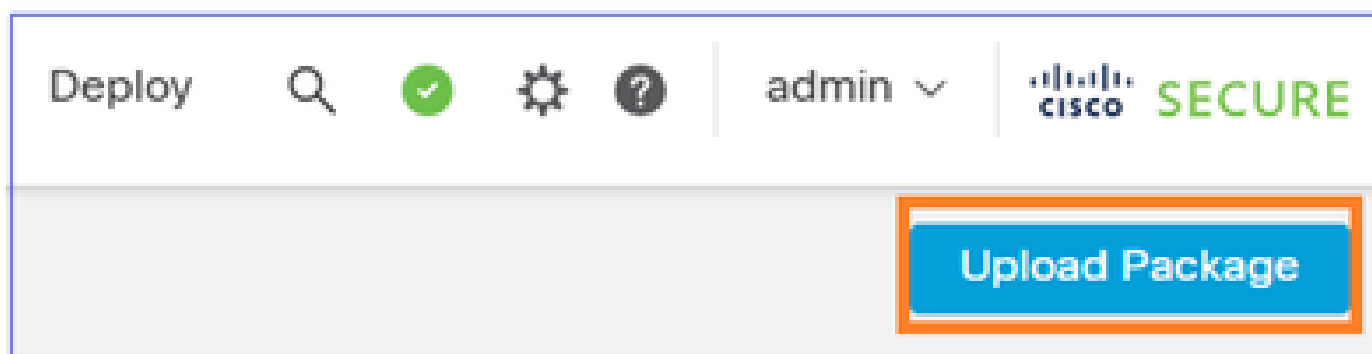
-  **Opmerking:** Het document richt zich op de migratie van één FTD HA-paar naar een nieuw FMC. Aan de andere kant, als u van plan bent om te migreren meerdere firewalls die hetzelfde beleid (bijvoorbeeld, ACS, NAT) en objecten delen en u wilt dit doen in fasen moet u deze punten overwegen.
- Indien 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:

Firewall Management Center
System / Tools / Upload Package

Overview Analysis Policies Devices Objects

Package Name Choose File No file chosen

Upload 2 Cancel

Importeer de beleidslijnen:

Firewall Management Center
System / Tools / Package Import

Overview Analysis Policies Devices Objects Integration

Access Control Policy

☒ FTD3100_ACP Access Control Policy

NAT Threat Defense

☒ nat1 NAT Threat Defense

Platform Settings Threat Defense

☒ FTD3100_PS Platform Settings Threat Defense

Import Cancel

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

Firewall Management Center
System / Tools / Import Resolution

Overview Analysis Policies Devices Objects Integration

Import Manifest

Network and Port objects will be reused if name and content matches with existing objects, in all other cases objects with duplicate names are imported as new objects with a number appended to the name.

FTD3100_ACP (Access Control Policy)
nat1 (NAT Threat Defense)
FTD3100_PS (Platform Settings Threat Defense)

Interface Objects

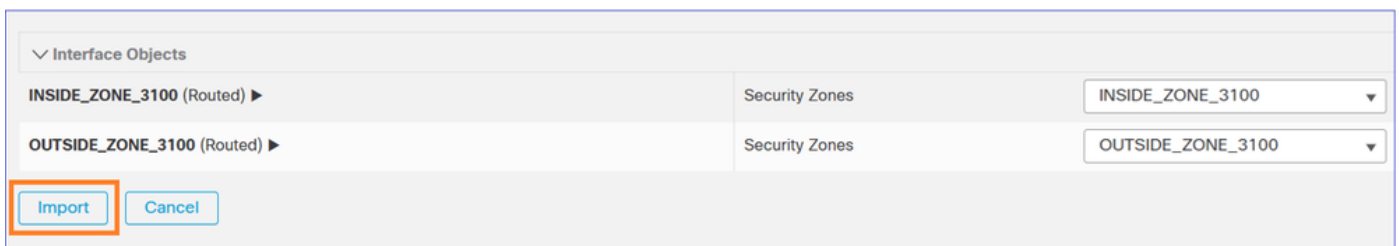
Object Name	Security Zones
INSIDE_ZONE_3100 (Routed) ▶	Select...
OUTSIDE_ZONE_3100 (Routed) ▶	Select...

Import Cancel

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>
```

```
>
```

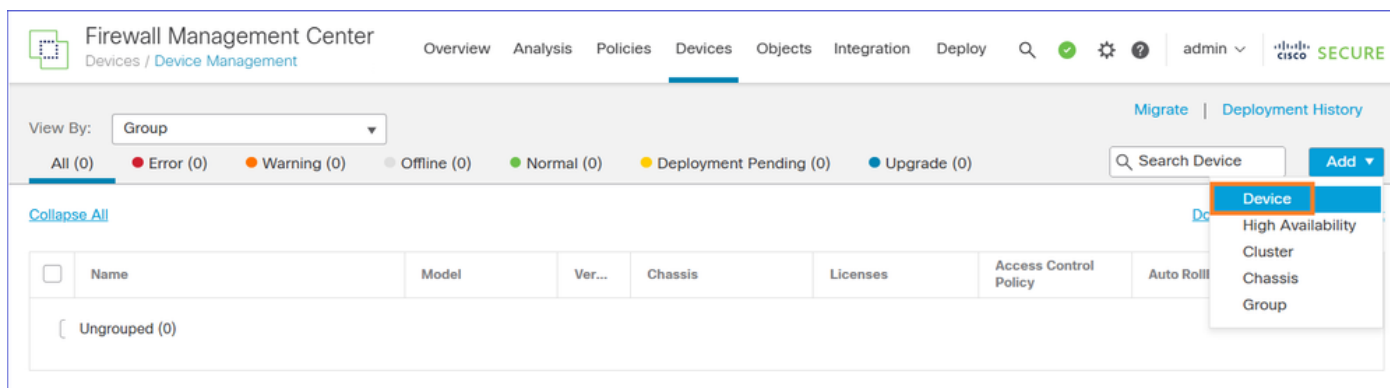
```
configure manager add 10.62.148.247 cisco
```

```
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:

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:†

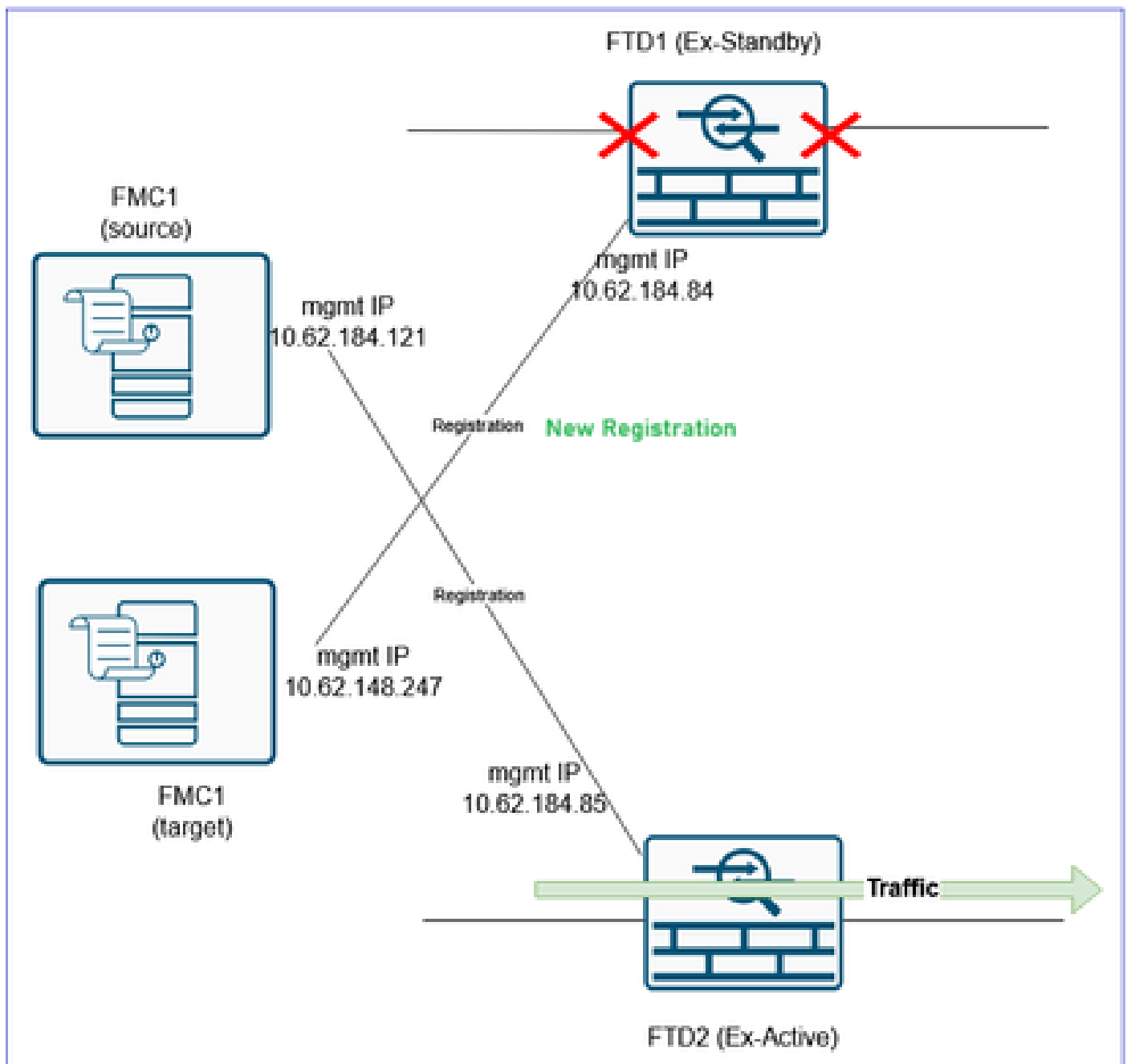
- ☒ Transfer Packets

2

Cancel

Register

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:

 **Firewall Management Center**
Devices / Secure Firewall Device Summary

OverviewAnalysisPolicies**Devices**

FTD1
Cisco Secure Firewall 3120 Threat Defense

Device**Interfaces**Inline SetsRoutingDHCPVTEP

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

 **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).

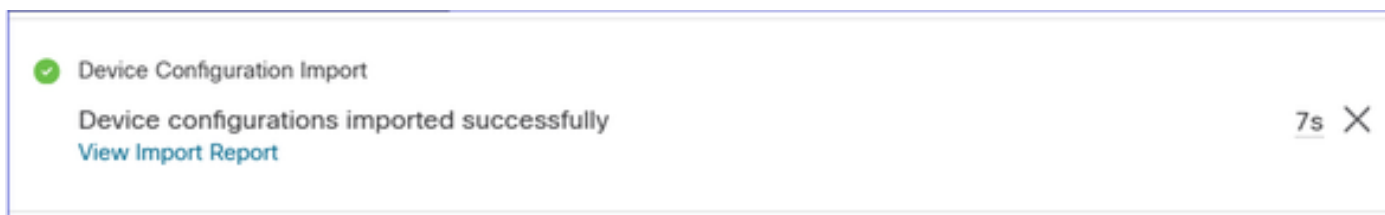
Device Configuration Import

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

No

Yes

Een VCC-taak wordt gestart.



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

The screenshot shows the "Firewall Management Center" interface for device "FTD1". The "Interfaces" tab is selected. A table lists 20 interfaces. The last two rows are highlighted with an orange box:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
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

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
```

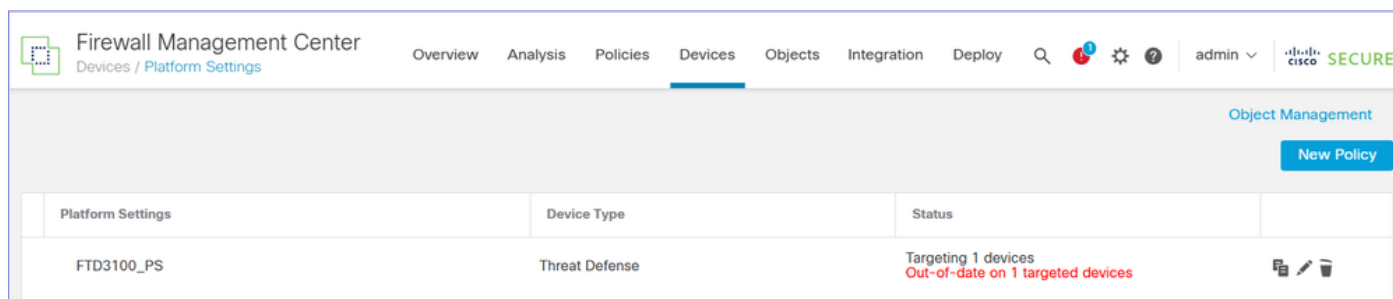
Stap 10. De FTD-configuratie voltooien

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.

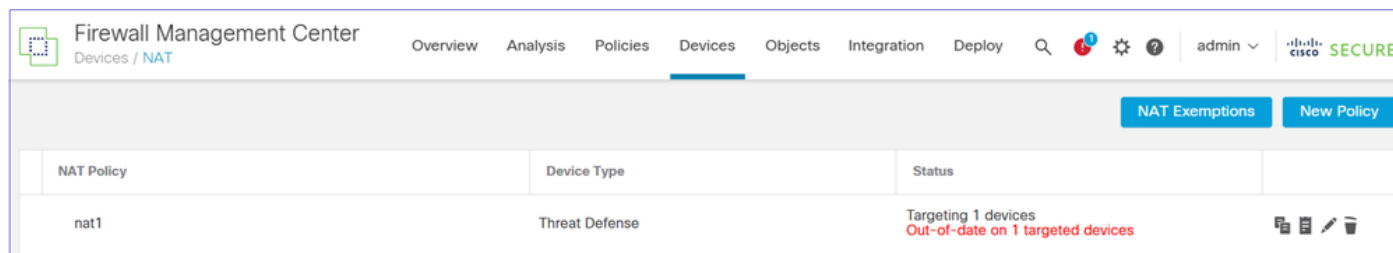
Platform-instellingen worden bijvoorbeeld geïmporteerd en toegewezen aan het apparaat, maar in afwachting van de implementatie:



The screenshot shows the 'Firewall Management Center' interface with the 'Devices' tab selected. Under 'Platform Settings', the device 'FTD3100_PS' is listed with a 'Threat Defense' device type. The status indicates it is 'Targeting 1 devices' and 'Out-of-date on 1 targeted devices'.

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

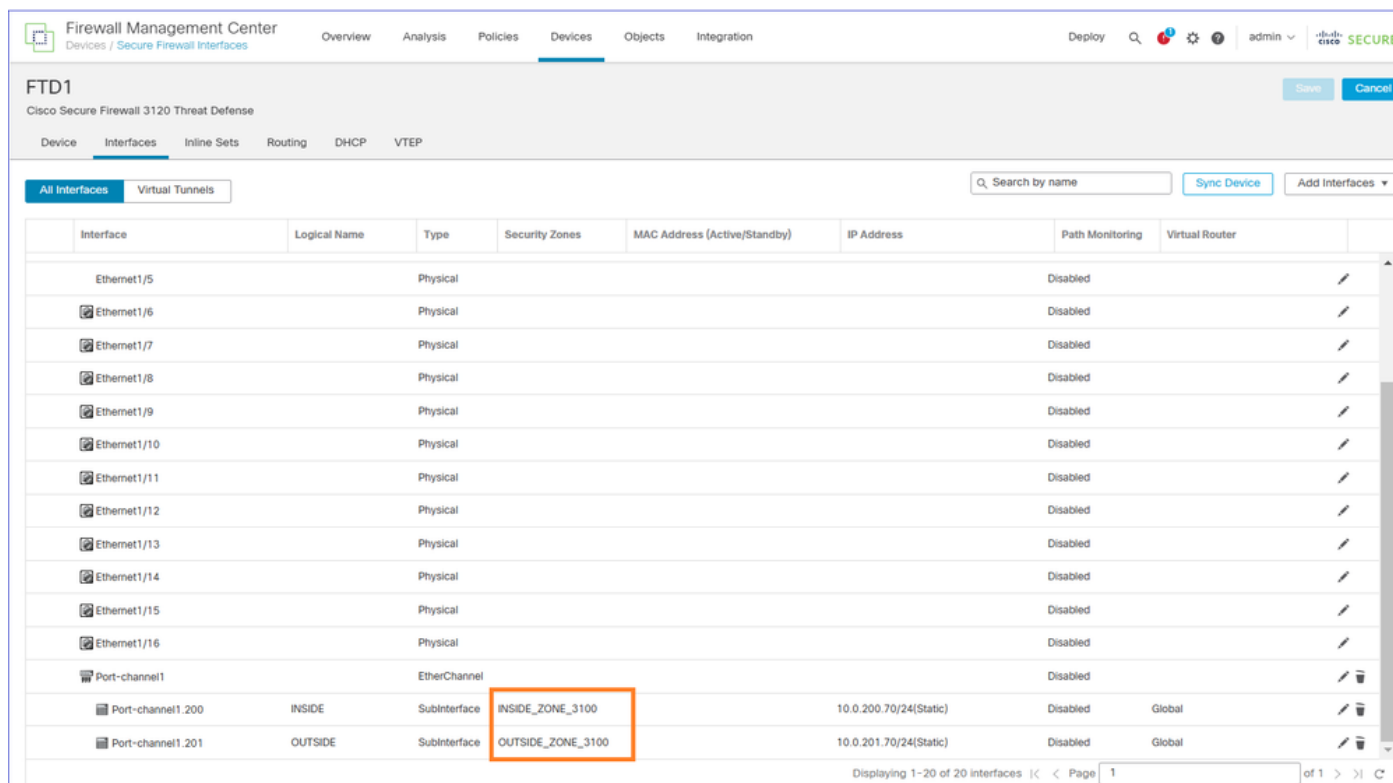
Als NAT is geconfigureerd, wordt het NAT-beleid geïmporteerd en aan het apparaat toegewezen, maar in afwachting van de implementatie:



The screenshot shows the 'Firewall Management Center' interface with the 'Devices' tab selected. Under 'NAT Policy', the policy 'nat1' is listed with a 'Threat Defense' device type. The status indicates it is 'Targeting 1 devices' and 'Out-of-date on 1 targeted devices'.

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

Security Zones worden toegepast op de interfaces:



The screenshot shows the 'Firewall Management Center' interface with the 'Devices' tab selected. Under 'Secure Firewall Interfaces', the device 'FTD1' is shown. The 'Interfaces' sub-tab is active, displaying a table of interfaces and their assigned security zones. The 'INSIDE_ZONE_3100' and 'OUTSIDE_ZONE_3100' zones are highlighted with orange boxes.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Ethernet1/5		Physical				Disabled	
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

Routing-configuratie wordt toegepast op het FTD-apparaat:

Firewall Management Center

Devices / Secure Firewall Routing

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 ⚙️ ⓘ admin 🔒 **SECURE**

FTD1

Cisco Secure Firewall 3120 Threat Defense

SaveCancel

DeviceInterfacesInline Sets**Routing**DHCPVTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

+ Add Route

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

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

Analysis

Create New VPN Topology

Topology Name:*

VPN3100

☒ Policy Based (Crypto Map) ☐ Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

☐ IKEv1 ☒ IKEv2

EndpointsIKEIPsecAdvanced

Node A:

Device Name	VPN Interface	Protected Networks	
FTD1	OUTSIDE (10.0.201.70)	net_10.0.200.0	

Node B:

Device Name	VPN Interface	Protected Networks	
Remote_FW	10.0.201.60	net_10.0.202.0	

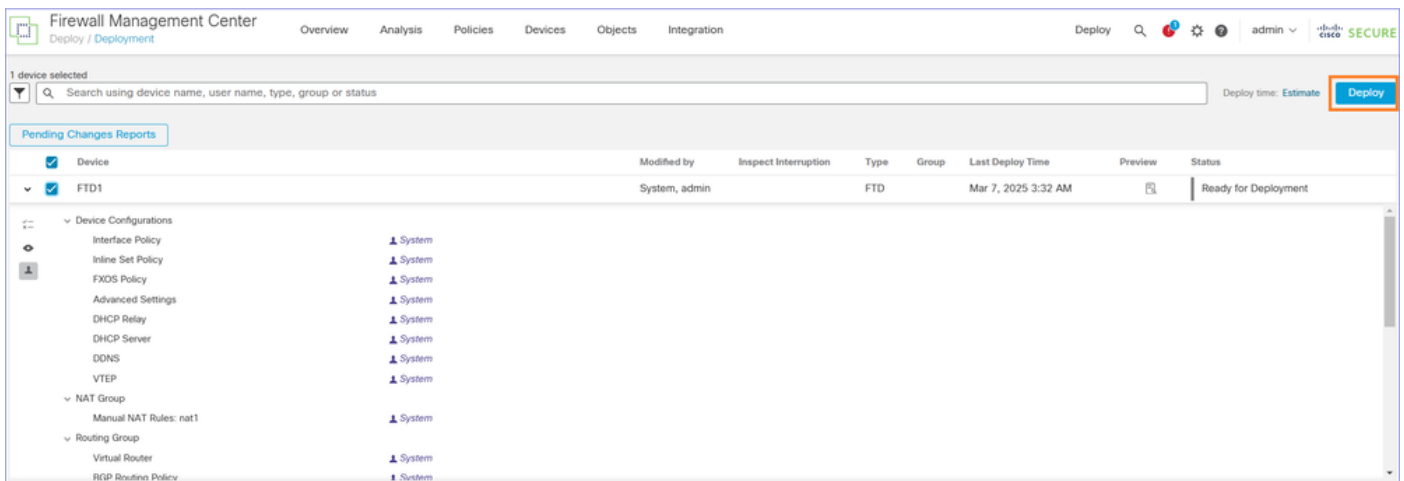
ⓘ Ensure the protected networks are allowed by access control policy of each device.

CancelSave

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.

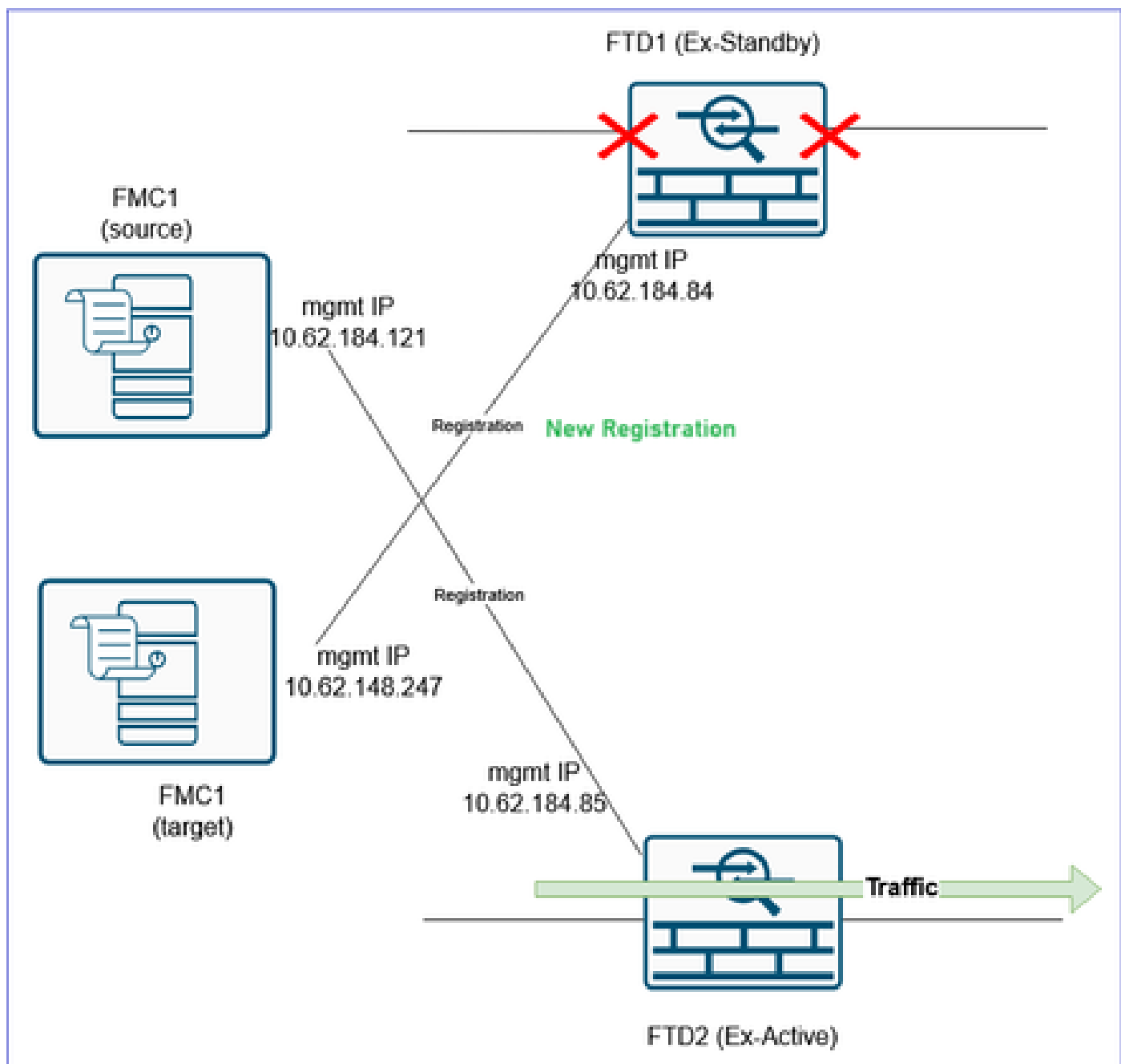
Verschillen die u ziet en die normaal zijn, zijn:

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

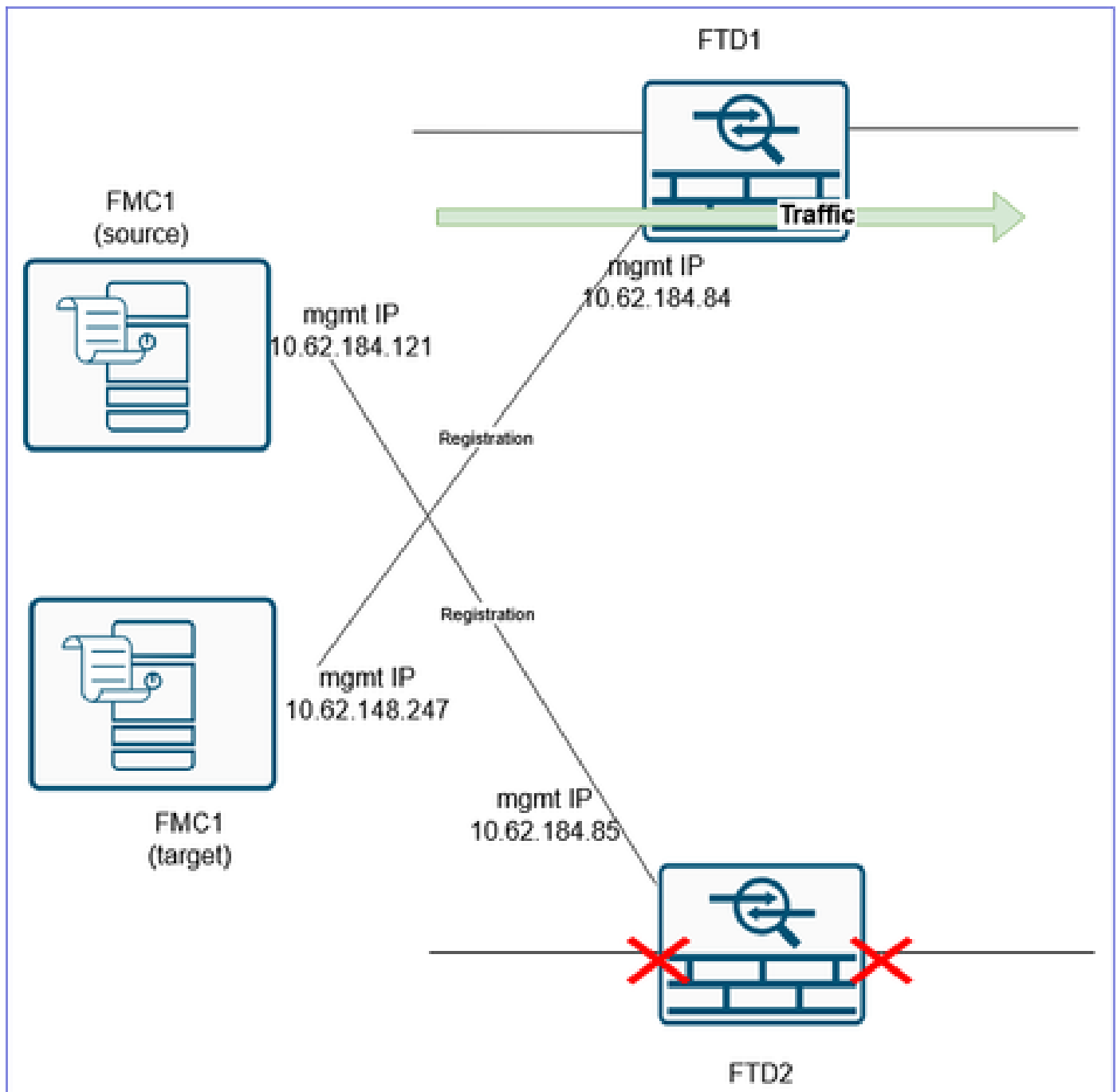
Stap 12. Voer de cutover uit

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:



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 ipaddrut1 5 10.0.200.70

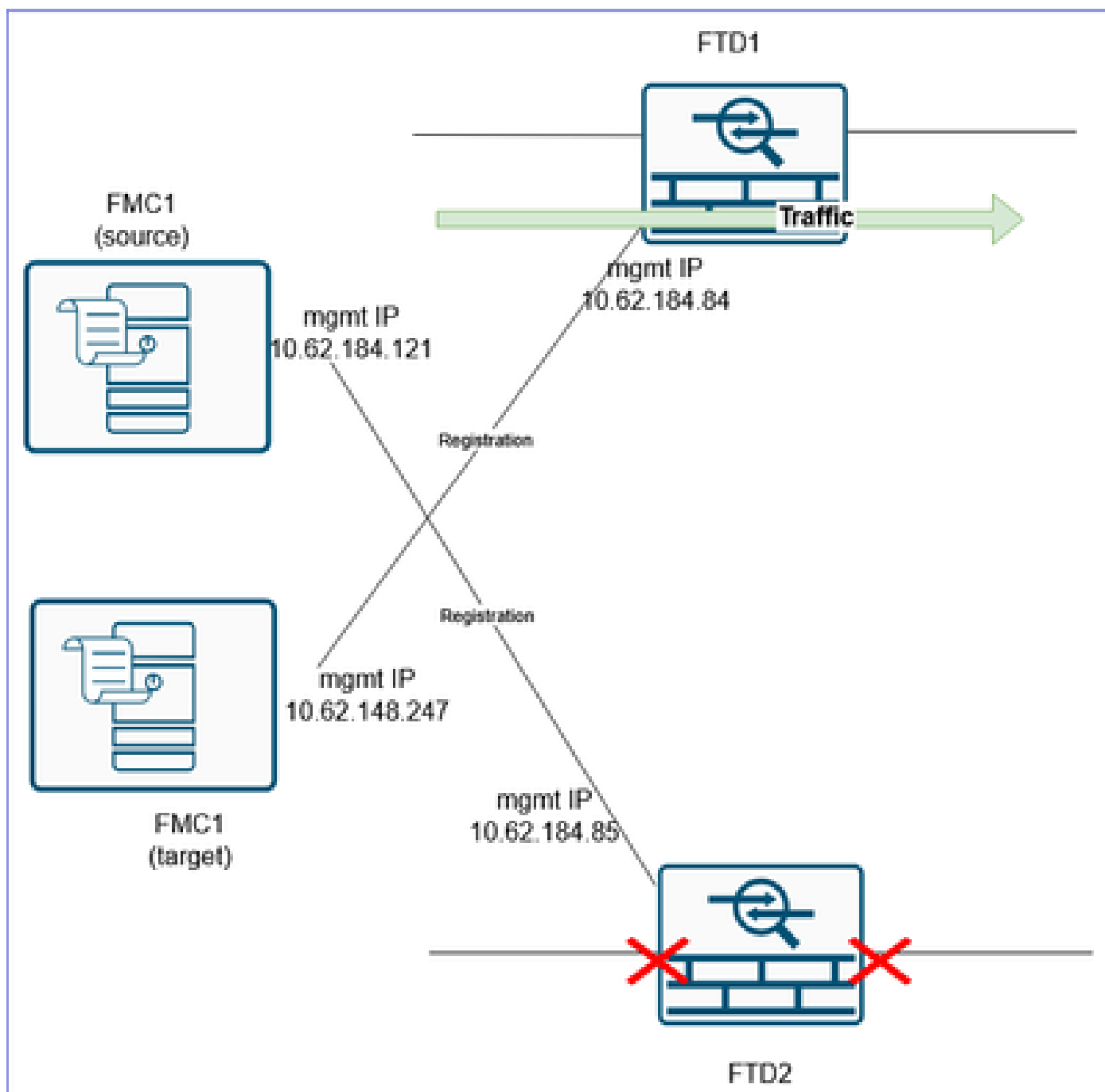
Gratuitous ARP sent for 10.0.200.70

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.

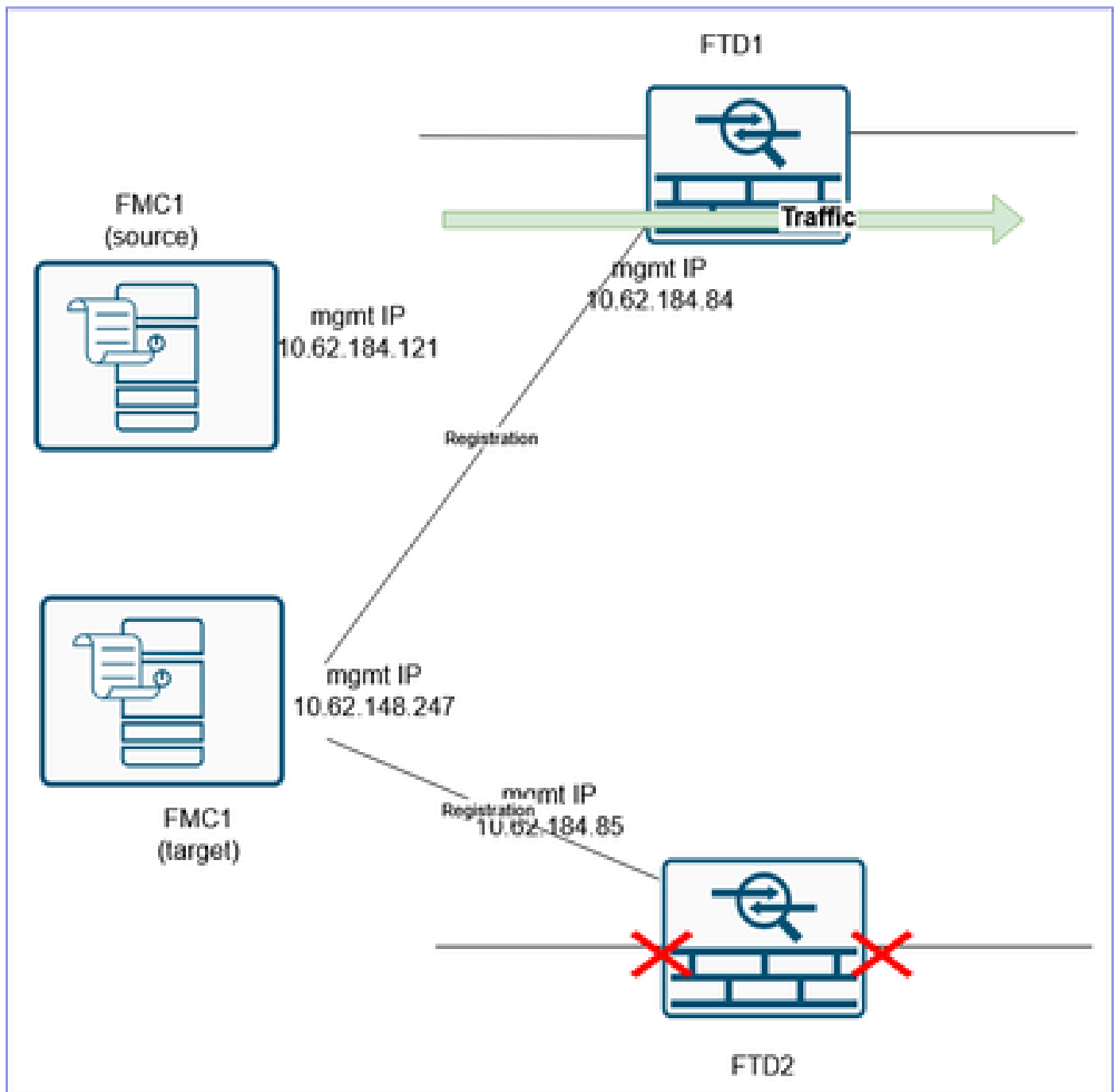
Stap 13. Migreren van het tweede FTD naar het FMC2 (doel-FMC)

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:



Na:



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

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

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 switchen 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.

```
>
```

Firewall Management Center
Devices / Device Management

Overview Analysis Policies Dev

View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (0)

Collapse All

Name	Model
Ungrouped (1)	
FTD1 Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense

Add Device

Select the Provisioning Method:
☒ Registration Key ☐ Serial Number

☐ CDO Managed Device

Host:†
10.62.184.85

Display Name:
FTD2

Registration Key:†

Group:
None

Access Control Policy:†
FTD3100_ACP

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

Advanced
 Unique NAT ID:†

☒ Transfer Packets

Cancel Register

Het resultaat:

Firewall Management Center
Devices / Device Management

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings admin admin

Migrate Deployment History

View By: Group

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

Search Device Add

Download Device List Report

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (2)						
FTD1 Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+
FTD2 Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+

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):

Version	Chassis	Licenses
se	7.4	PS (2 more
se	7.4	PS (2 more

Add High Availability Pair ?

Name:*

Device Type:

Primary Peer:

Secondary Peer:

i Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

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>
```

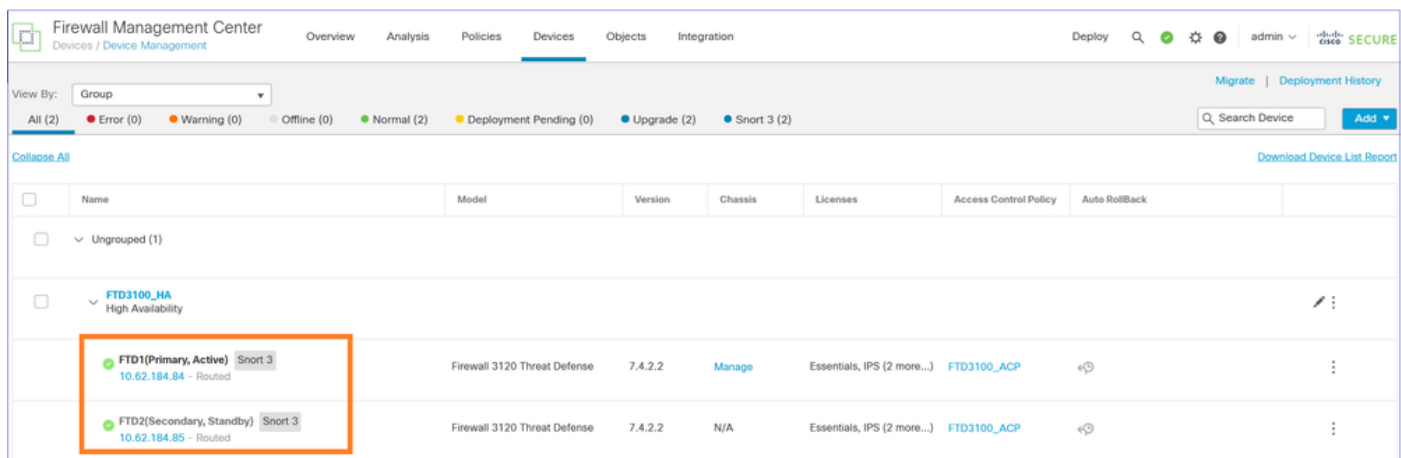
```
FTD3100-3#
```

```
show failover | include host
```

This host: Secondary - Standby Ready

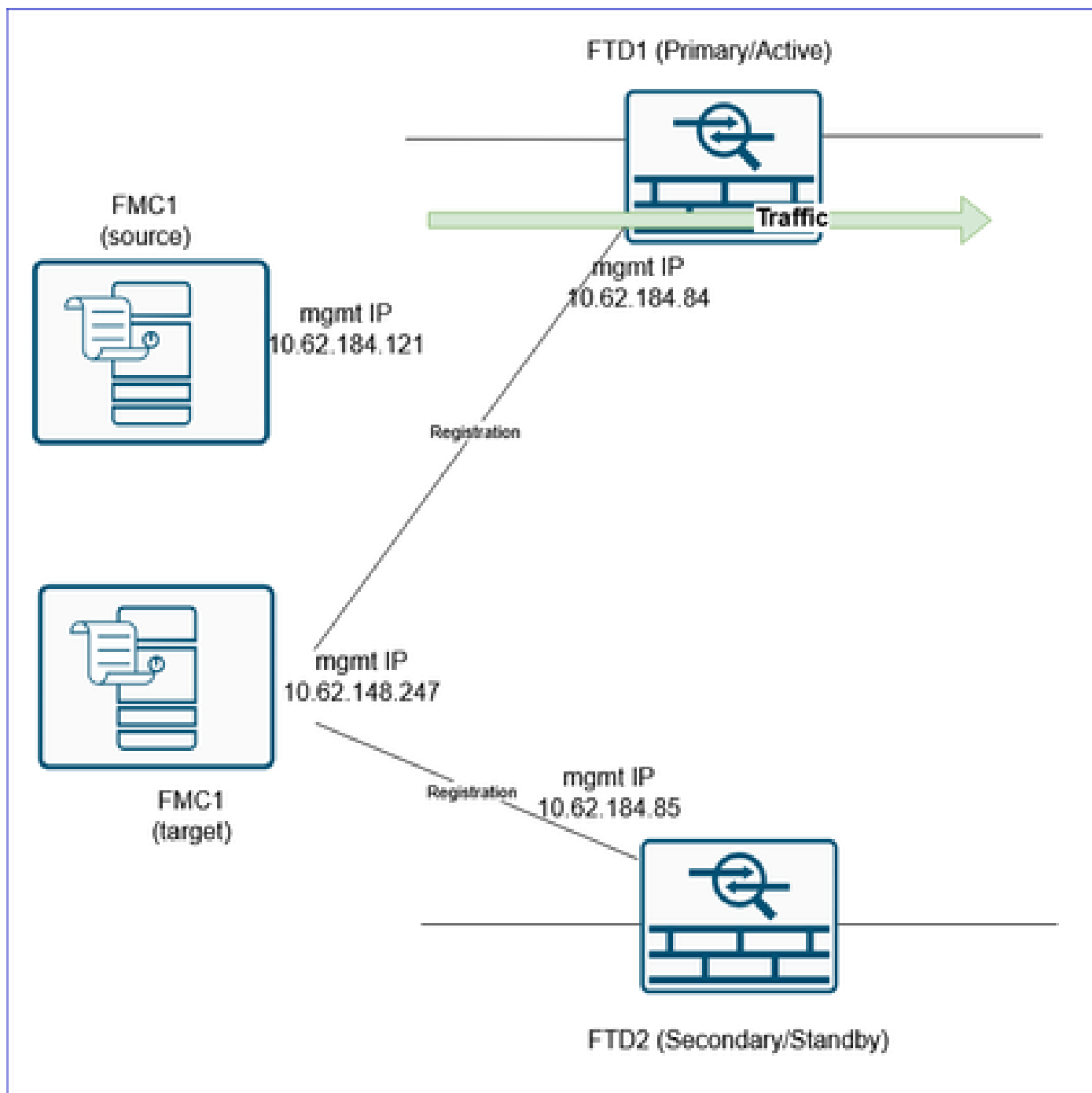
Other host: Primary - Active

Controle van de FMC UI:



	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
☐	Ungrouped (1)						
☐	FTD3100_HA High Availability						
☐	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	+ ⓘ
☐	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	+ ⓘ

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.