

FTD HA (Failover) auf ein anderes FMC migrieren

Inhalt

[Einleitung](#)

[Abkürzungen](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Topologie](#)

[Konfigurieren](#)

[Schritt 1: Exportieren der Gerätekonfiguration von der primären Firewall](#)

[Schritt 2: Aktivieren des sekundären FTD](#)

[Schritt 3: Brechen Sie die FTD HA](#)

[Schritt 4: Isolieren der FTD1-Datenschnittstellen \(ex-Primary\)](#)

[Schritt 5: FTD Shared Policies exportieren](#)

[Schritt 6: Löschen/Aufheben der Registrierung des FTD1 \(ex-Primary\) aus dem alten/ursprünglichen FMC](#)

[Schritt 7: Importieren Sie das FTD Policy-Konfigurationsobjekt in das FMC2 \(Ziel-FMC\).](#)

[Schritt 8: FTD1 \(ex-Primary\) beim FMC2 registrieren](#)

[Schritt 9: FTD-Gerätekonfigurationsobjekt in FMC2 \(Ziel-FMC\) importieren](#)

[Schritt 10: Beenden der FTD-Konfiguration](#)

[Schritt 11: Überprüfen der bereitgestellten FTD-Konfiguration](#)

[Schritt 12: Umstellung durchführen](#)

[Schritt 13: Migration der zweiten FTD auf das FMC2 \(Ziel-FMC\)](#)

[Schritt 14. Umgestalten des FTD HA](#)

[Referenzen](#)

Einleitung

In diesem Dokument wird das Verfahren zur Migration eines FTD HA von einem vorhandenen FMC zu einem anderen FMC beschrieben.

Informationen zur Migration einer Standalone-Firewall zu einem neuen FMC finden Sie unter <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>

Abkürzungen

ACP = Access Control Policy

ARP = Address Resolution Protocol

CLI = Command Line Interface (Befehlszeilenschnittstelle)

FMC = Secure Firewall Management Center

FTD = Secure Firewall Threat Defense

GARP = Kostenloser ARP

HA = hohe Verfügbarkeit

MW = Wartungsfenster

UI = User Interface

Voraussetzungen

Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

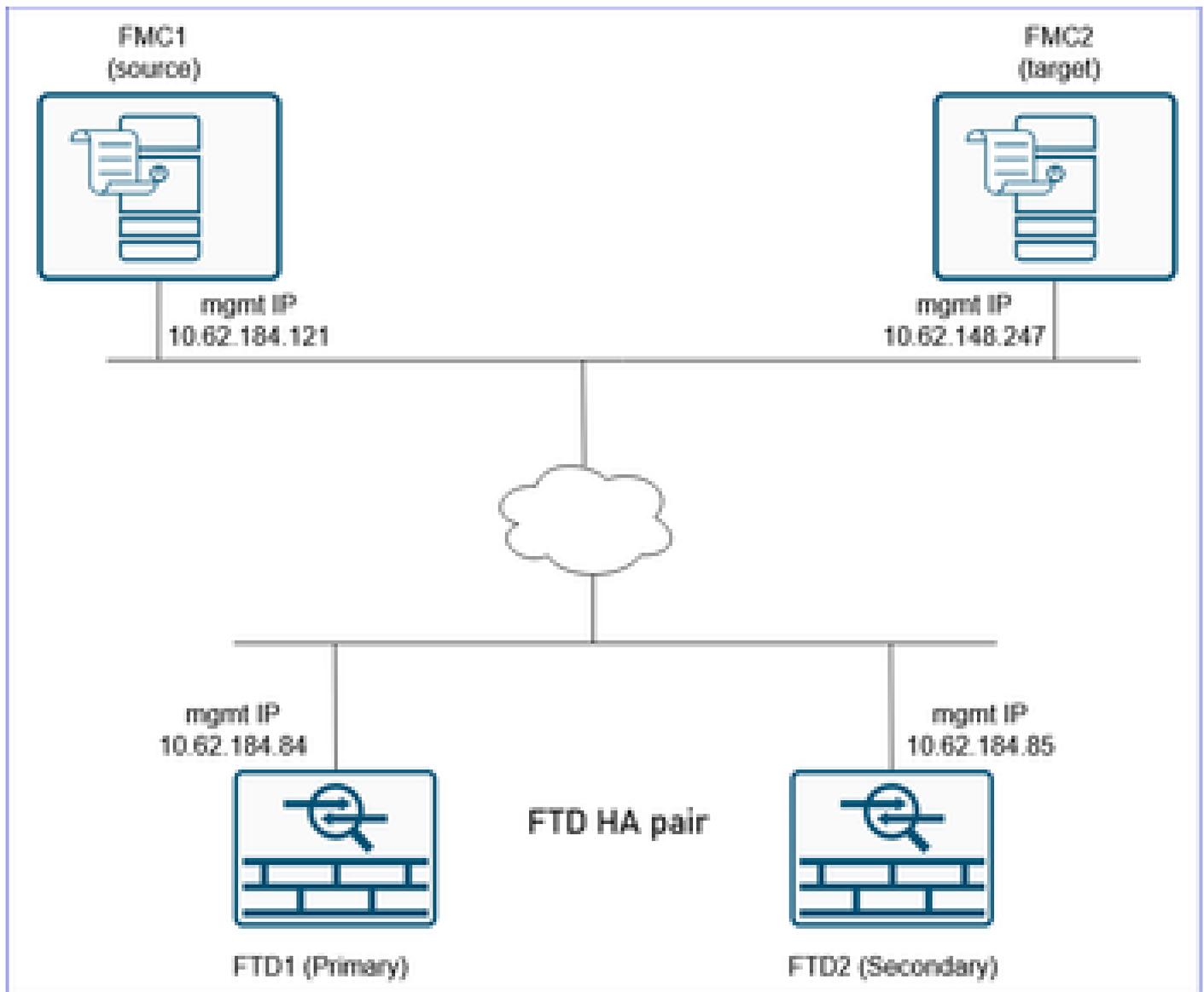
- UI- und CLI-Zugriff auf die Quell- und Ziel-FMCs.
- Administratoranmeldeinformationen für FMCs und Firewalls.
- Konsolenzugriff auf beide Firewalls
- Zugriff auf die Upstream- und Downstream-Geräte von L3 (falls Sie den ARP-Cache leeren müssen)
- Stellen Sie sicher, dass das Ziel-/Ziel-FMC dieselbe Version wie das Quell-/alte FMC verwendet.
- Stellen Sie sicher, dass das Ziel-/Ziel-FMC über dieselben Lizenzen wie das Quell-/alte FMC verfügt.
- Stellen Sie sicher, dass Sie für die Migration eine MW einrichten, da sich dies auf den Transitverkehr auswirken wird.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall 31xx, FTD-Version 7.4.2.2.
- Secure Firewall Management Center Version 7.4.2.2
- Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



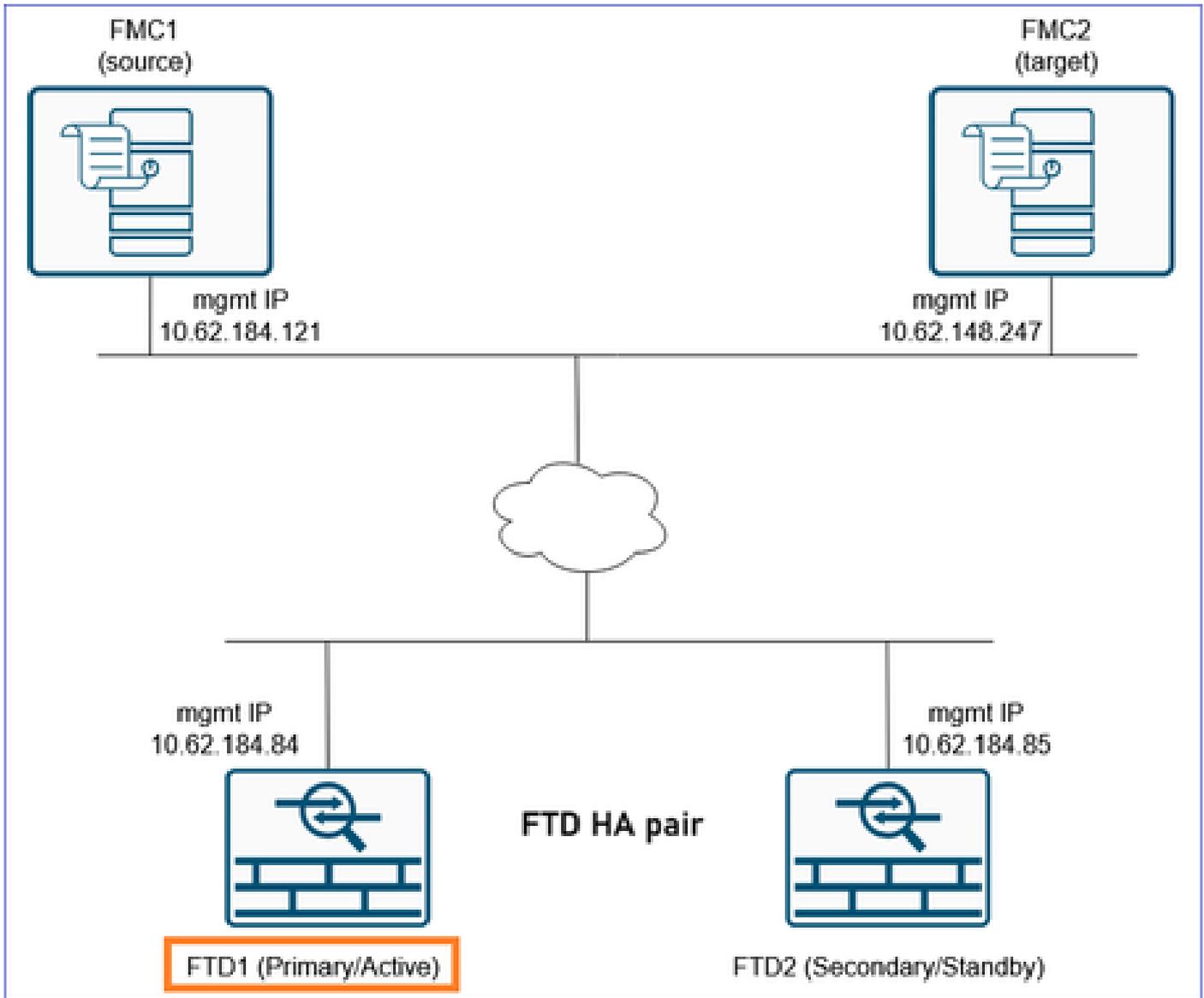
Konfigurieren

Migrationsschritte

Für dieses Szenario berücksichtigen wir folgende Zustände:

FTD1: Primär/Aktiv

FTD2: Sekundär/Standby



Schritt 1: Exportieren der Gerätekonfiguration von der primären Firewall

Navigieren Sie auf dem FMC1 (Quell-FMC) zu Devices (Geräte) > Device Management (Geräteverwaltung). Wählen Sie das FTD HA-Paar aus, und wählen Sie Bearbeiten aus:

The screenshot shows the FMC interface with the 'Devices' tab selected. The table below lists the devices in the HA pair:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (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	⊕

Navigieren Sie zur Registerkarte Gerät. Stellen Sie sicher, dass Primary/Active FTD (FTD1 in diesem Fall) ausgewählt ist, und wählen Sie Export (Exportieren) aus, um die Gerätekonfiguration zu exportieren:

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: UTC (UTC+0:00)
OnBoarding Method: Registration Key	Rules: View
	Inventory: View

Anmerkung: Die Exportoption steht ab der Softwareversion 7.1 zur Verfügung.

Sie können zur Seite Benachrichtigungen > Aufgaben navigieren, um sicherzustellen, dass der Export abgeschlossen wurde. Wählen Sie dann das 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](#)

Alternativ können Sie auch auf die Schaltfläche Download im Bereich Allgemein klicken. Sie erhalten eine sfo-Datei, zum Beispiel DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

Die Datei enthält eine gerätebezogene Konfiguration, z. B.:

- Geroutete Schnittstellen
- Inline-Sets
- Routing
- DHCP
- VTEP

- Zugeordnete Objekte

Anmerkung: Die exportierte Konfigurationsdatei kann nur in dieselbe FTD importiert werden. Die UUID des FTD muss mit dem Inhalt der importierten SFO-Datei übereinstimmen. Derselbe FTD kann auf einem anderen FMC registriert und eine sfo-Datei importiert werden.

Referenz: 'Exportieren und Importieren der Gerätekonfiguration'

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

Schritt 2: Aktivieren des sekundären FTD

Navigieren Sie zu Devices (Geräte) > Device Management (Geräteverwaltung), wählen Sie das FTD HA-Paar aus, und wählen Sie Switch Active Pair (Aktives Paar wechseln) aus:

The screenshot shows the 'Devices / Device Management' page in the Firewall Management Center. A table lists devices under the group 'FTD3100_HA High Availability'. Two devices are listed: 'FTD1(Primary, Active)' and 'FTD2(Secondary, Standby)'. A context menu is open over the 'FTD2' row, with the 'Switch Active Peer' option highlighted. Other options in the menu include Break, Force refresh node status, Delete, Revert Upgrade, Health Monitor, and Troubleshoot Files.

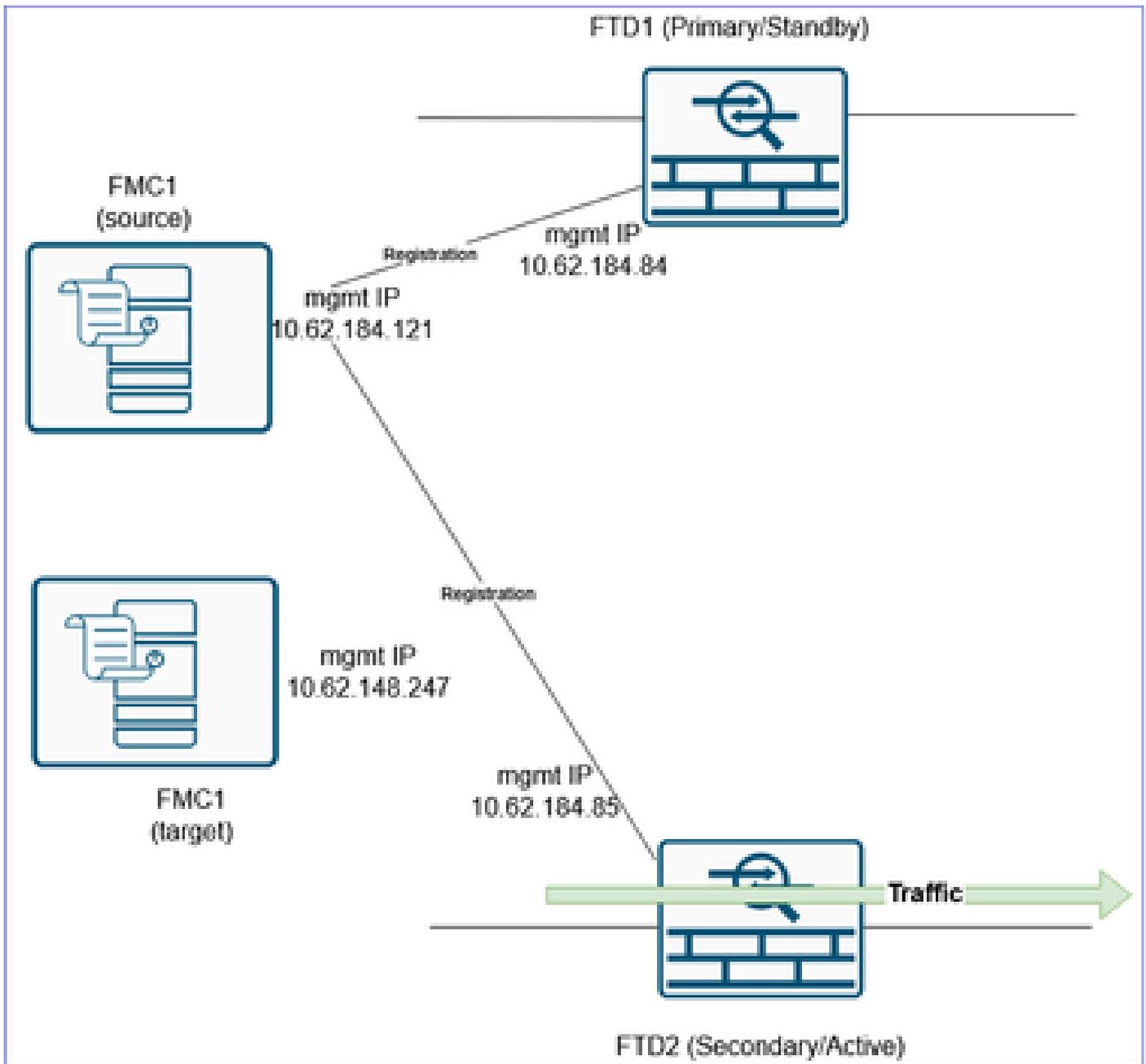
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1(Primary, Active) Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	↔
FTD2(Secondary, Standby) Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	↔

Das Ergebnis ist FTD1 (primär/Standby) und FTD (sekundär/aktiv):

The screenshot shows the same 'Devices / Device Management' page. The status of the devices has changed: 'FTD1' is now '(Primary, Standby)' and 'FTD2' is now '(Secondary, Active)'. The 'FTD2' row is highlighted with an orange box, indicating it is the active peer.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1(Primary, Standby) Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	↔
FTD2(Secondary, Active) Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	↔

Der Datenverkehr wird jetzt von der sekundären/aktiven FTD verarbeitet:



Schritt 3. Brechen Sie die FTD HA

Navigieren Sie zu Devices (Geräte) > Device Management (Gerätmanagement), und brechen Sie die Hochverfügbarkeit des FTD:

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is active, displaying a list of devices. The 'FTD3100_HA' group is expanded, showing two devices: FTD1 (Primary, Standby) and FTD2 (Secondary, Active). The 'FTD2 (Secondary, Active)' device is highlighted with a red box, and a context menu is open over it, with the 'Break' option selected.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
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	⌵

Dieses Fenster wird angezeigt. Ja auswählen

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

 Anmerkung: An diesem Punkt kann es für einige Sekunden zu einer Unterbrechung des Datenverkehrs kommen, da die Snort-Engine während der HA-Pause neu startet. Wie in der Meldung erwähnt, sollten Sie außerdem den ARP-Cache auf Upstream- und Downstream-Geräten löschen, wenn Sie NAT verwenden und es zu einem längeren Ausfall des Datenverkehrs kommt.

Nachdem Sie die FTD HA unterbrochen haben, haben Sie zwei eigenständige FTDs auf FMC.

Aus Konfigurationsperspektive verfügt FTD2 (ex-Active) über die erforderliche Konfiguration mit Ausnahme der Failover-bezogenen Konfiguration und verarbeitet den Datenverkehr:

```
<#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

Der FTD1 (ex-Standby) hat die gesamte Konfiguration entfernt:

<#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#

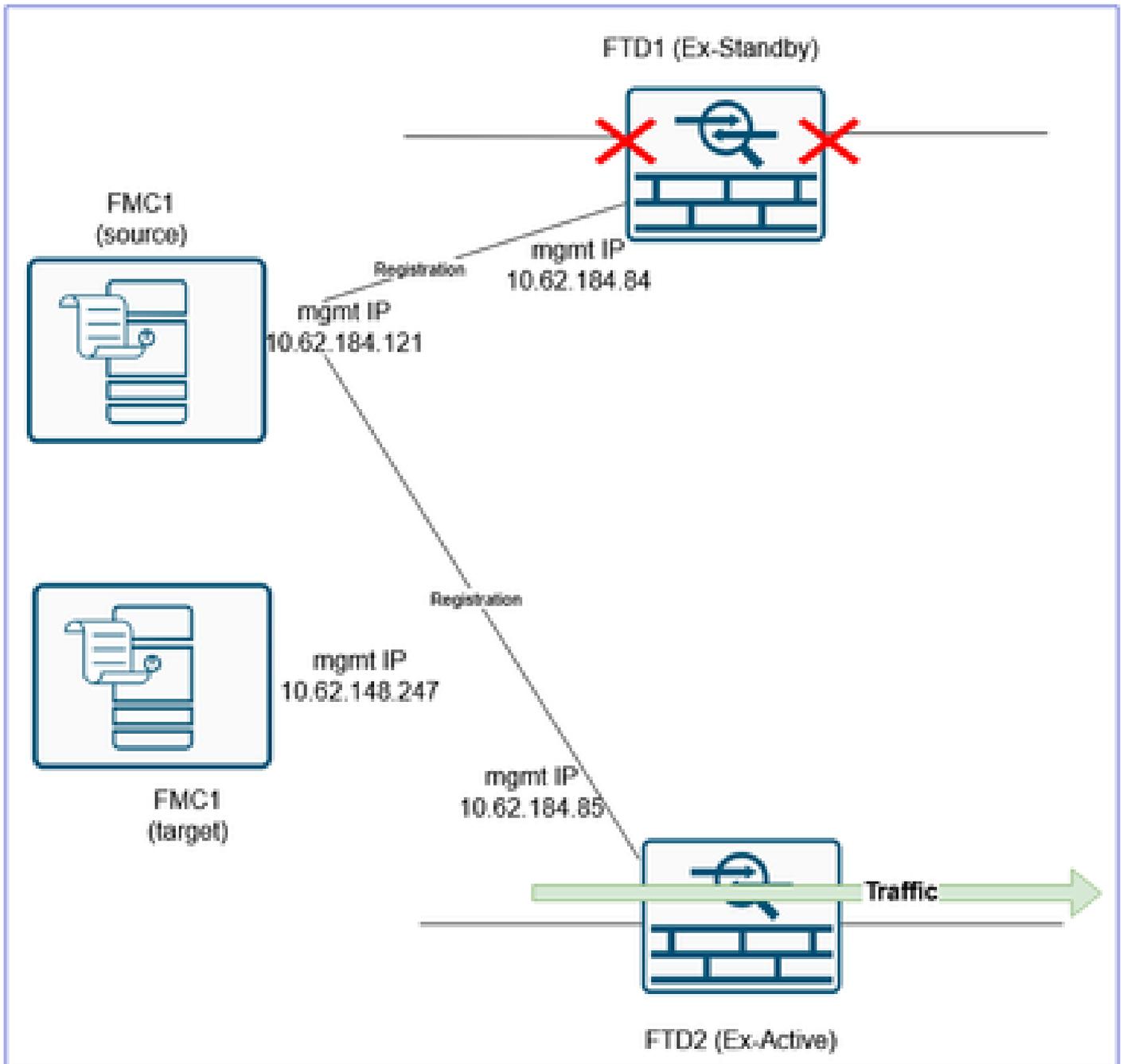
show interface ip brief

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

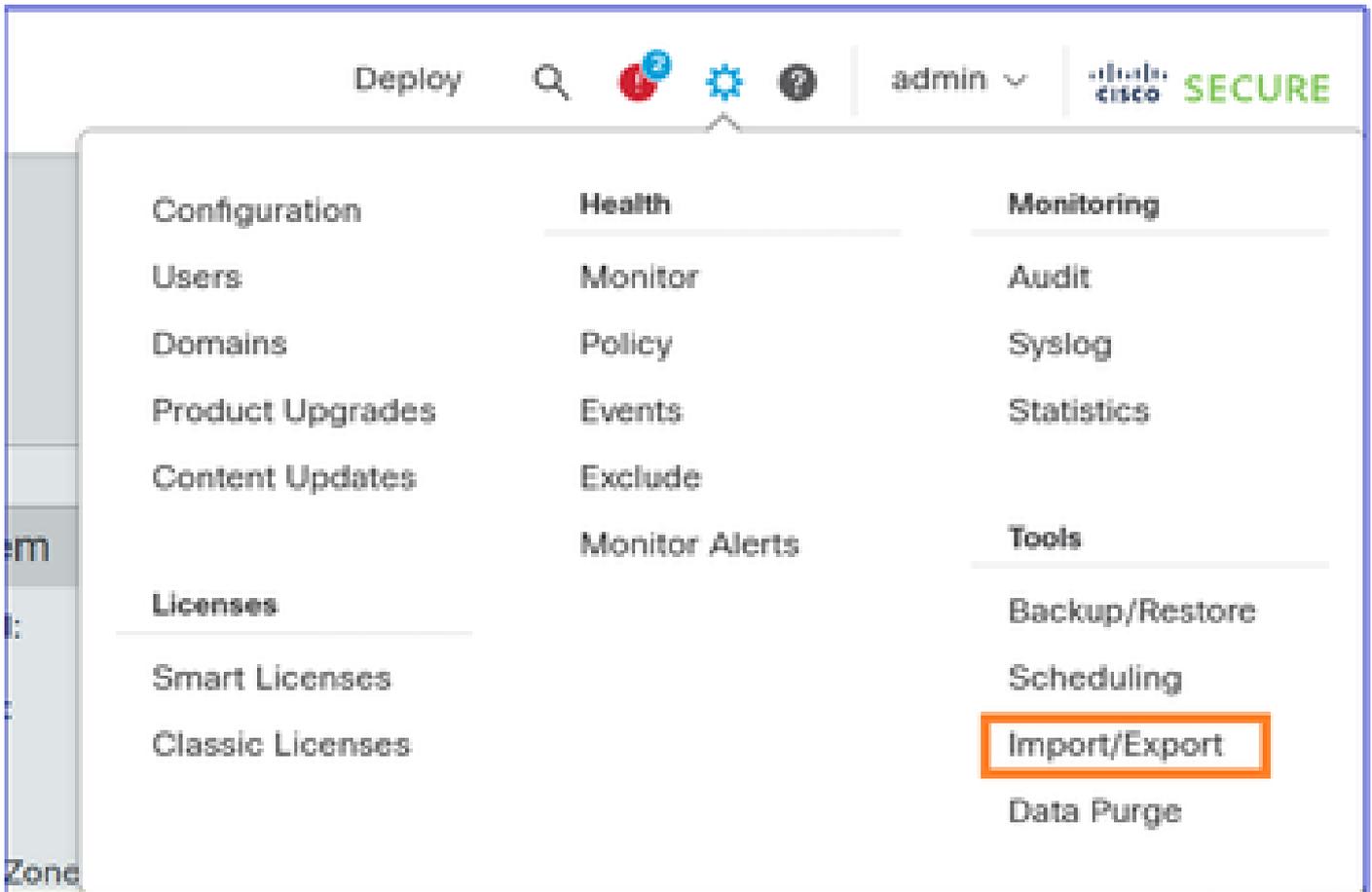
Schritt 4: Isolieren der FTD1-Datenschnittstellen (ex-Primary)

Trennen Sie die Datenkabel vom FTD1 (ex-Primary). Lassen Sie nur den FTD-Management-Port angeschlossen.



Schritt 5: FTD Shared Policies exportieren

Navigieren Sie zu System > Tools, und wählen Sie Importieren/Exportieren:



Exportieren Sie die verschiedenen Richtlinien, die mit dem Gerät verbunden sind. Stellen Sie sicher, dass Sie alle mit dem FTD verknüpften Richtlinien exportieren, z. B.:

- Zugriffskontrollrichtlinie (ACP)
- NAT-Richtlinie (Network Address Translation)
- Integritätsrichtlinie (falls benutzerdefiniert)
- FTD-Plattformeinstellungen

usw.

Firewall Management Center
System / Tools / Import/Export

Overview Analysis Policies Devices Objects Integration

Access Control Policy

- FTD3100_ACP** Access Control Policy

> Contextual Cross-launch

> Custom Table View

> Custom Workflow

> Dashboard

> Health Policy

NAT Threat Defense

- nat1** NAT Threat Defense

Platform Settings Firepower

- firepower_test_policy** Platform Settings Firepower

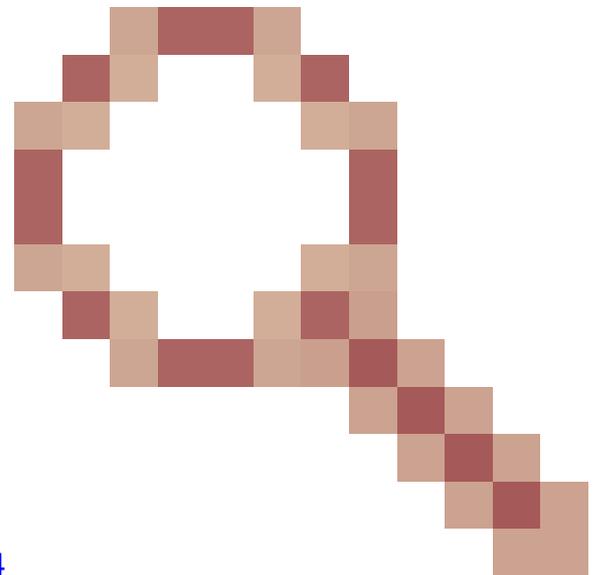
Platform Settings Threat Defense

- FTD3100_PS** Platform Settings Threat Defense

> Report Template

Export

 Anmerkung: Zum Zeitpunkt der Erstellung dieses Dokuments wird der Export einer VPN-bezogenen Konfiguration nicht unterstützt. Sie müssen das VPN auf dem FMC2 (Ziel-FMC) nach der Geräteregistrierung manuell neu konfigurieren.



Zugehörige Erweiterung Cisco Bug-ID [CSCwf05294](https://tools.cisco.com/bugcenter/bug/?bugID=CSCwf05294)

Das Ergebnis ist eine SFO-Datei, z. B. ObjectExport_20250306082738.sfo

Schritt 6: Löschen/Aufheben der Registrierung des FTD1 (ex-Primary) aus dem alten/ursprünglichen FMC

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

Migrate | Deployment History

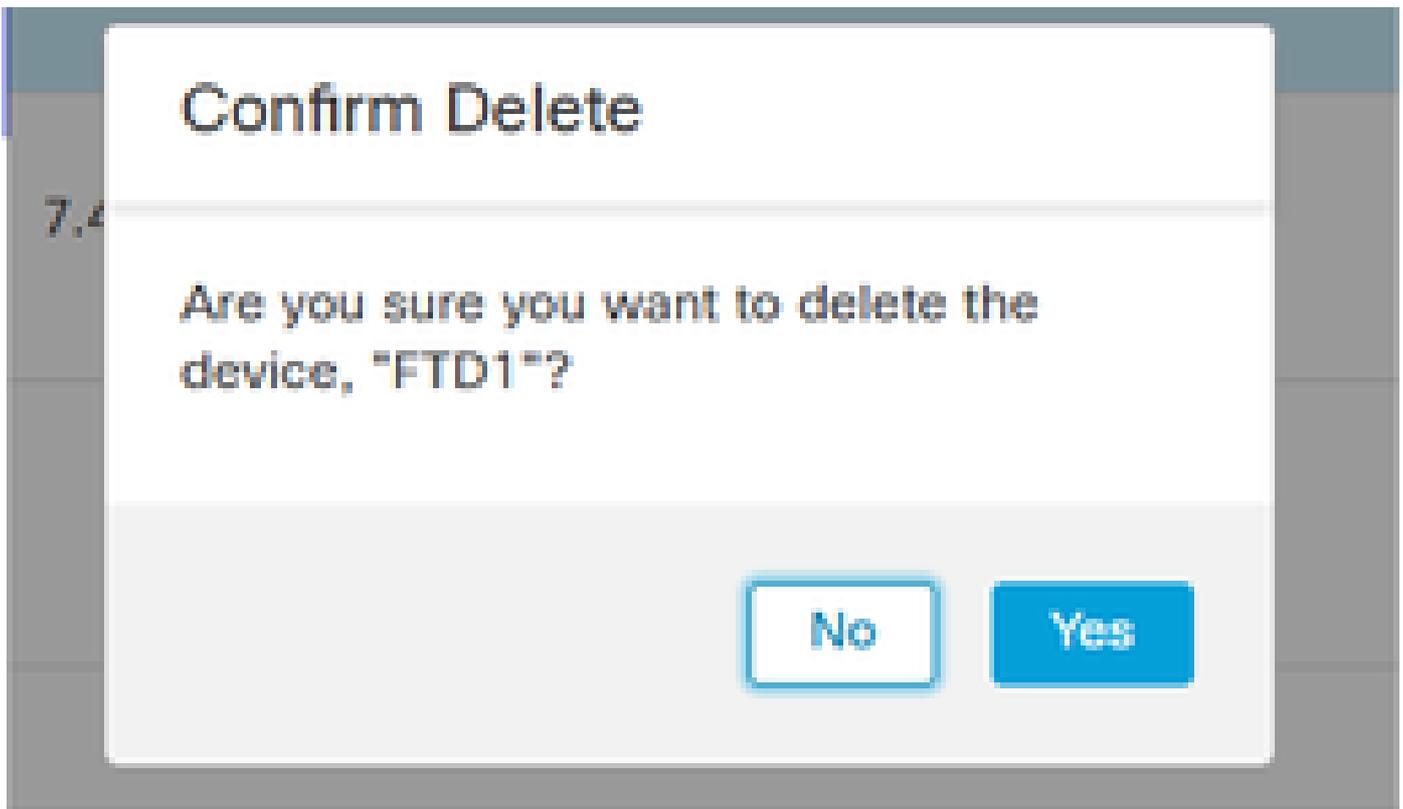
All (4) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (4) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (4)

🔍 Search Device **Add**

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	FTD_HA (2)							
<input type="checkbox"/>	FTD1 Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot Files
<input type="checkbox"/>	FTD2 Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	⊕	
<input type="checkbox"/>	Ungrouped (1)							

Löschen des Geräts bestätigen:



FTD1 CLI-Verifizierung:

```
<#root>
```

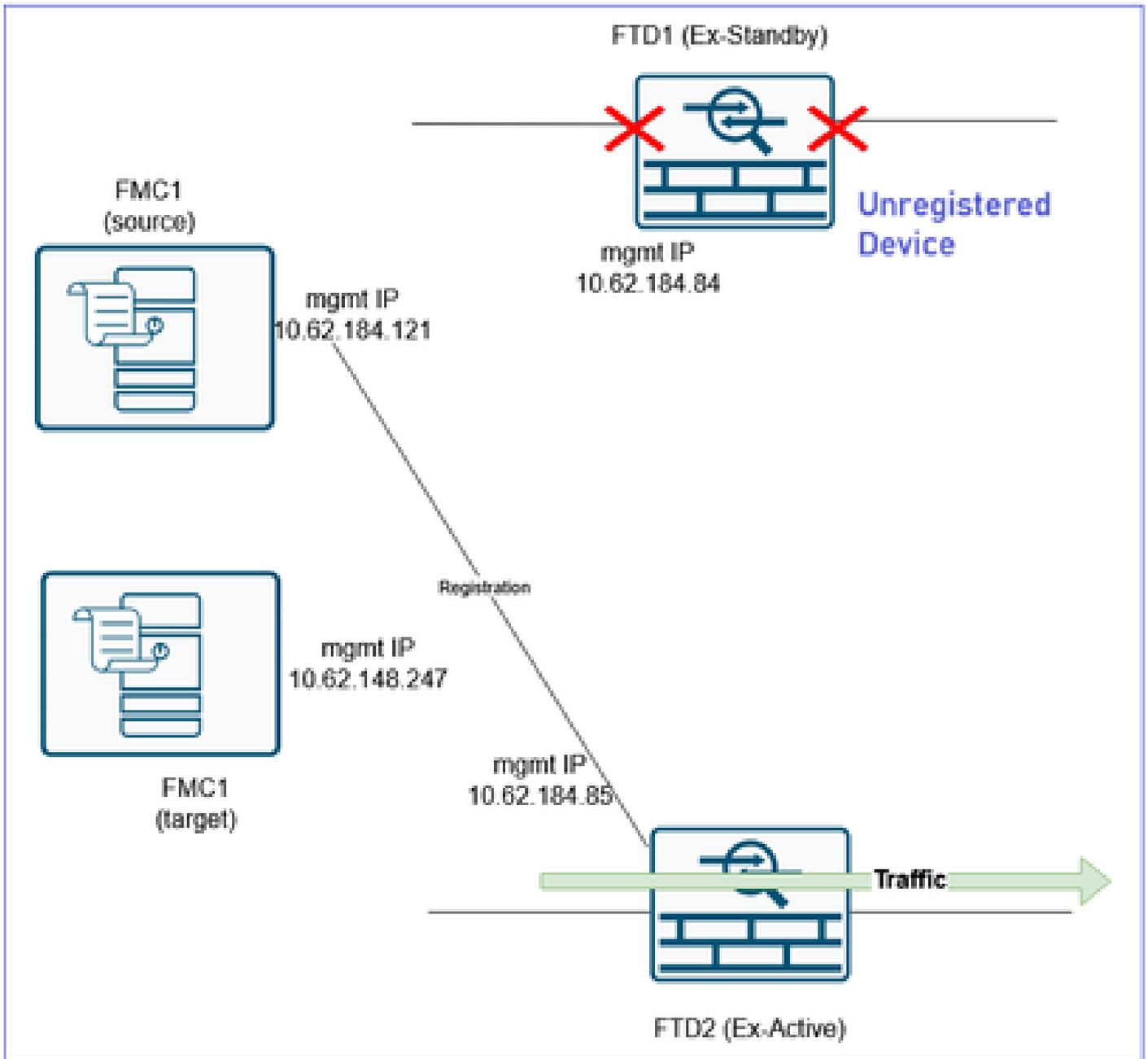
```
>
```

```
show managers
```

```
No managers configured.
```

```
>
```

Aktueller Status nach dem Löschen des FTD1-Geräts:

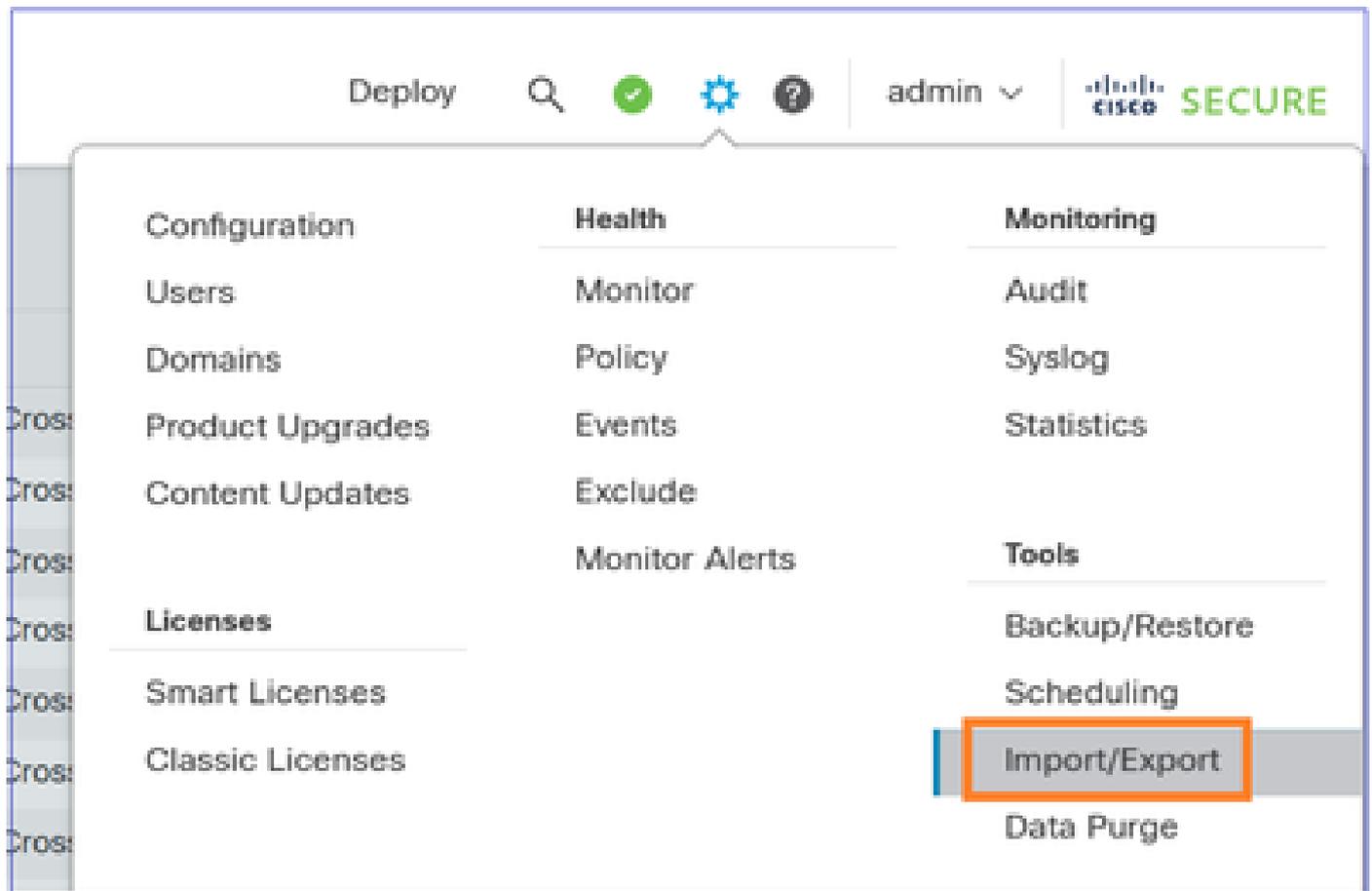


Schritt 7: Importieren Sie das FTD Policy-Konfigurationsobjekt in das FMC2 (Ziel-FMC).

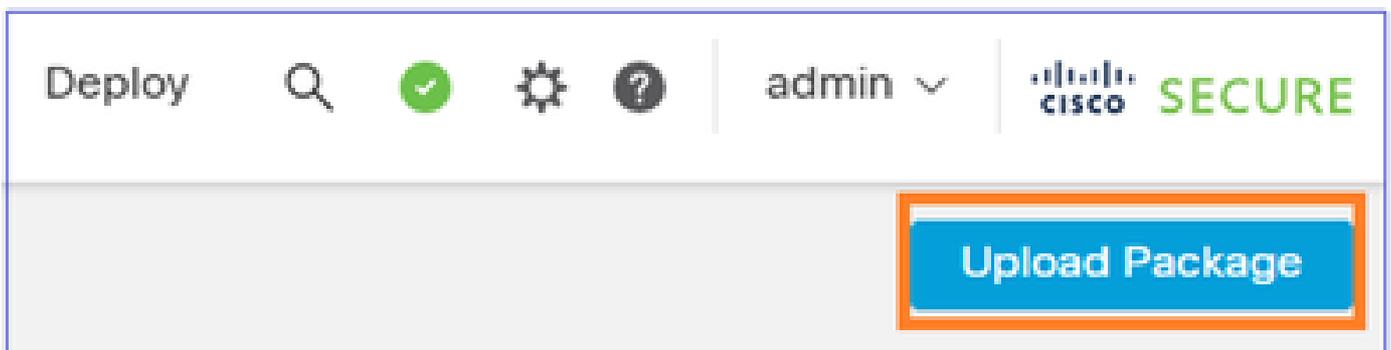
-  Anmerkung: Der Schwerpunkt des Dokuments liegt auf der Migration eines FTD HA-Paars zu einem neuen FMC. Wenn Sie jedoch mehrere Firewalls migrieren möchten, die dieselben Richtlinien (z. B. ACP, NAT) und Objekte verwenden, und dies in mehreren Phasen durchführen möchten, müssen Sie diese Punkte berücksichtigen.
- Wenn Sie bereits eine Richtlinie für das Ziel-FMC mit demselben Namen festgelegt haben, werden Sie gefragt, ob Sie:
 - antwort: die Richtlinie ersetzen möchten oder
 - b. Erstellen Sie eine neue mit einem anderen Namen. Dadurch werden doppelte Objekte mit unterschiedlichen Namen (Suffix _1) erstellt.

 - Wenn Sie Option "b" auswählen, stellen Sie in Schritt 9 sicher, dass Sie die neu erstellten Objekte den migrierten Richtlinien (ACP Security Zones, NAT Security Zones, Routing, Platform Settings usw.) erneut zuweisen.

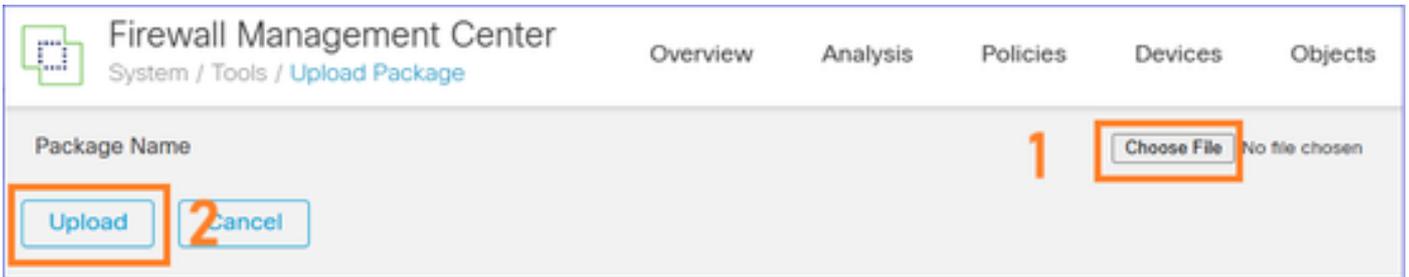
Melden Sie sich beim FMC2 (Ziel-FMC) an, und importieren Sie das FTD Policies sfo-Objekt, das Sie in Schritt 5 exportiert haben:



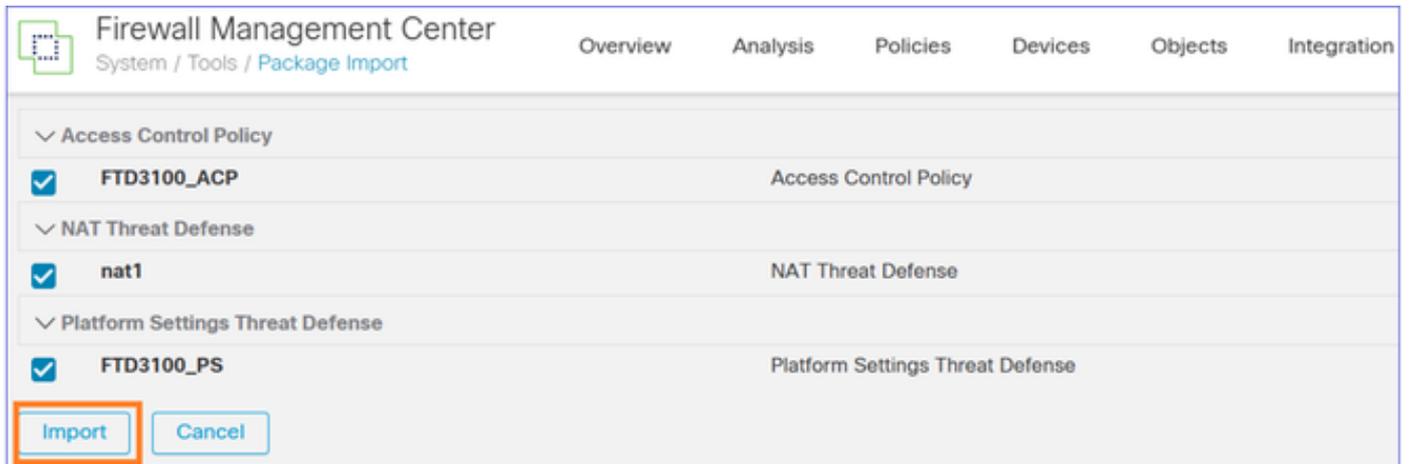
Wählen Sie Paket hochladen:



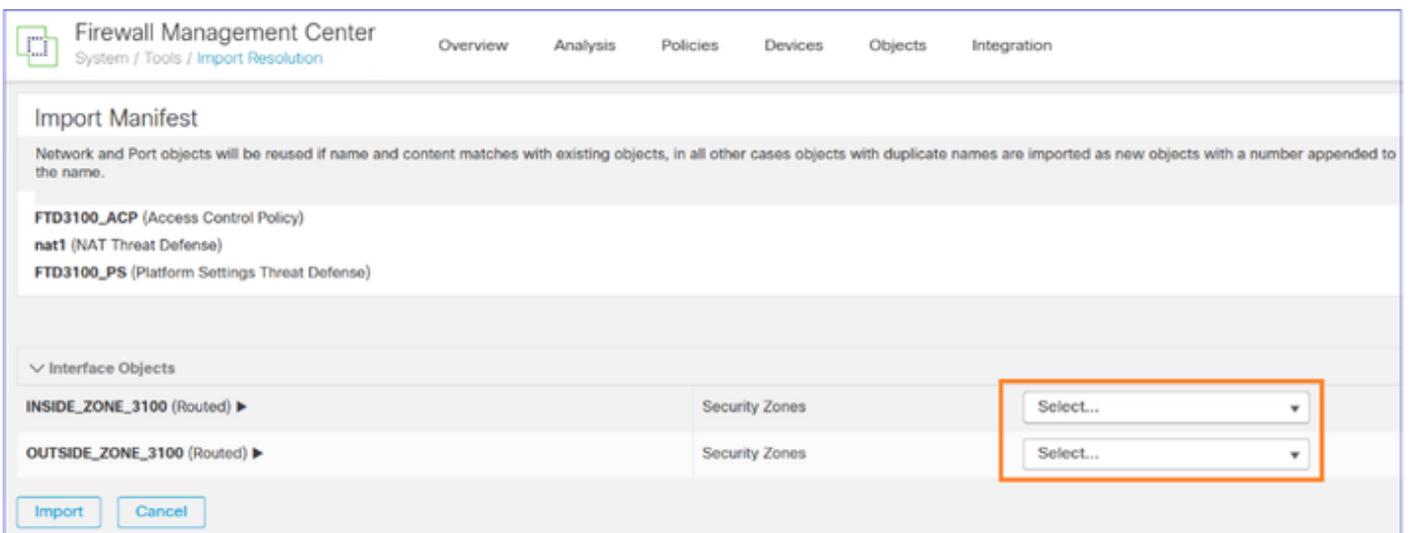
Datei hochladen:



Richtlinien importieren:



Erstellen Sie die Schnittstellenobjekte/Sicherheitszonen auf dem FMC2 (Ziel-FMC):



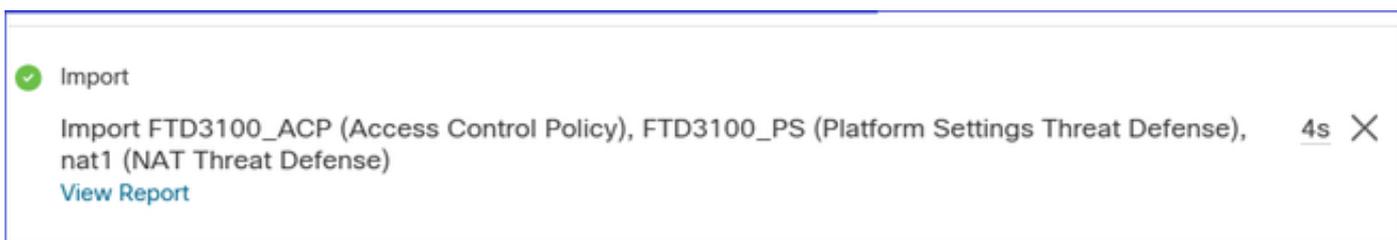
Sie können die gleichen Namen wie auf dem FMC1 (Quell-FMC) angeben:



Wenn Sie Importieren auswählen, beginnt ein Task mit dem Importieren der zugehörigen Richtlinien in das FMC2 (Ziel-FMC):



Die Aufgabe ist erledigt:



Schritt 8: FTD1 (ex-Primary) beim FMC2 registrieren

Öffnen Sie die FTD1-CLI (ex-Primary), und konfigurieren Sie den neuen 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.
```

```
>
```

Navigieren Sie zu FMC2 (target FMC) UI Devices > Device Management, und fügen Sie das FTD-Gerät hinzu:

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy

View By: Group

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

Search Device Add

Collapse All

Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto Roll
[Ungrouped (0)						

Device
High Availability
Cluster
Chassis
Group

Wenn die Geräteregistrierung fehlschlägt, finden Sie weitere Informationen zur Problembeseitigung in diesem Dokument: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html>

Weisen Sie die Zugriffskontrollrichtlinie zu, die Sie im vorherigen Schritt importiert haben:

Add Device

Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†

10.62.184.84

Display Name:

FTD1

Registration Key:*

Group:

None

Access Control Policy:*

FTD3100_ACP

Wenden Sie die erforderlichen Lizenzen an, und registrieren Sie das Gerät:

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:†

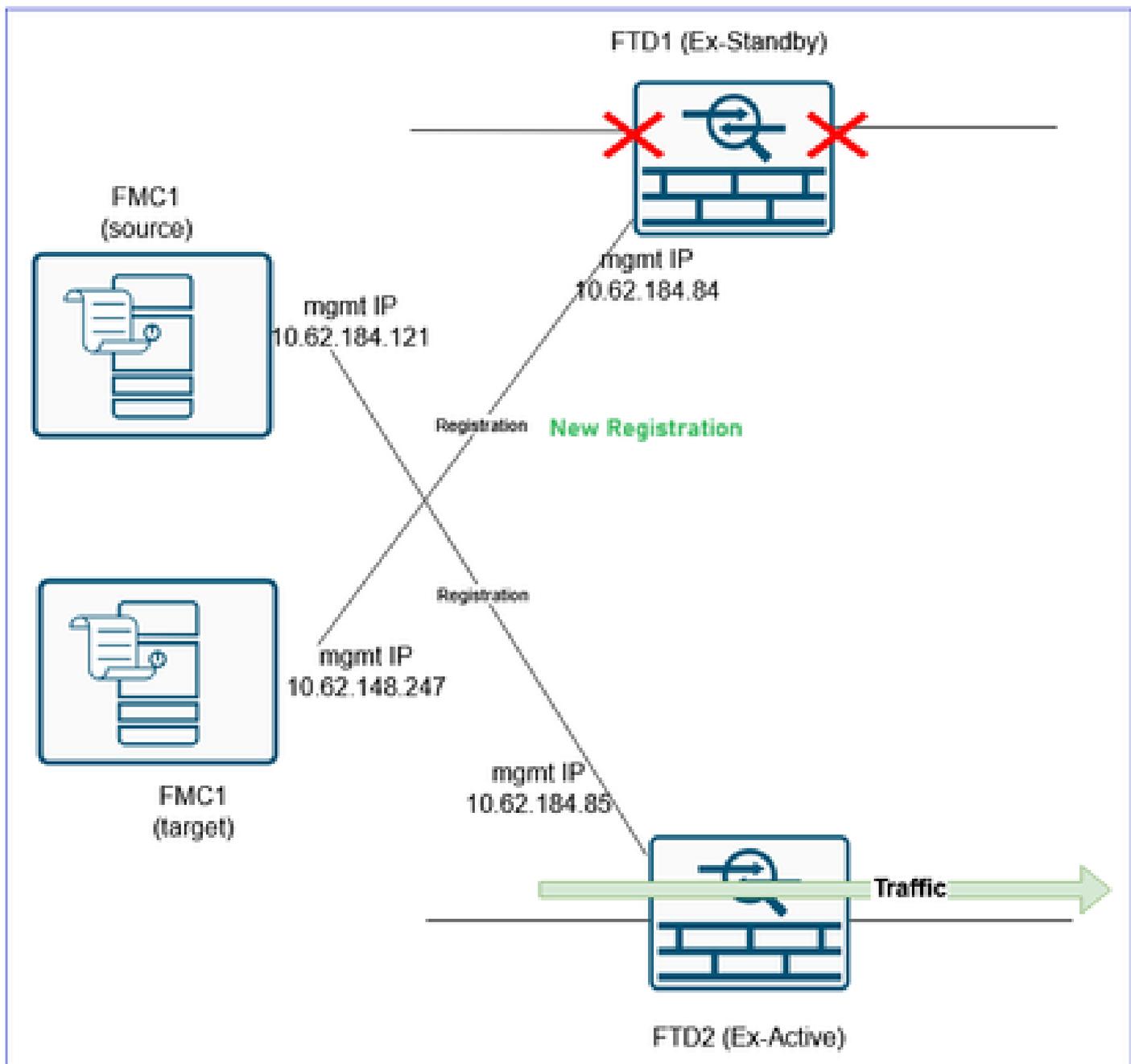
- Transfer Packets

2

Cancel

Register

Ergebnis:



Schritt 9: FTD-Gerätekonfigurationsobjekt in FMC2 (Ziel-FMC) importieren

Melden Sie sich beim FMC2 (Ziel-FMC) an, navigieren Sie zu Devices > Device Management (Geräte > Geräteverwaltung) und Bearbeiten des FTD-Geräts, das Sie im vorherigen Schritt registriert haben.

Navigieren Sie zur Registerkarte Gerät, und importieren Sie das FTD Policies-sfo-Objekt, das Sie in Schritt 2 exportiert haben:

Firewall Management Center
Devices / Secure Firewall Device Summary

Overview Analysis Policies **Devices**

FTD1

Cisco Secure Firewall 3120 Threat Defense

Device Interfaces Inline Sets Routing DHCP VTEP

General

Name: FTD1

Transfer Packets: Yes

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

Mode: Routed

Compliance Mode: None

Performance Profile: Default

TLS Crypto Acceleration: Enabled

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

OnBoarding Method: Registration Key

Licensing

Essential

Export-...

Malware

IPS:

Carrier:

URL:

Secure

Secure

Secure

 Anmerkung: Falls Sie in Schritt 7 mit Option "b" (Neue Richtlinie erstellen) gegangen sind, stellen Sie sicher, dass Sie die neu erstellten Objekte den migrierten Richtlinien (ACP Security Zones, NAT Security Zones, Routing, Plattform-Einstellungen usw.) erneut zuweisen.

Device Configuration Import

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

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

Eine FMC-Aufgabe wird initiiert.

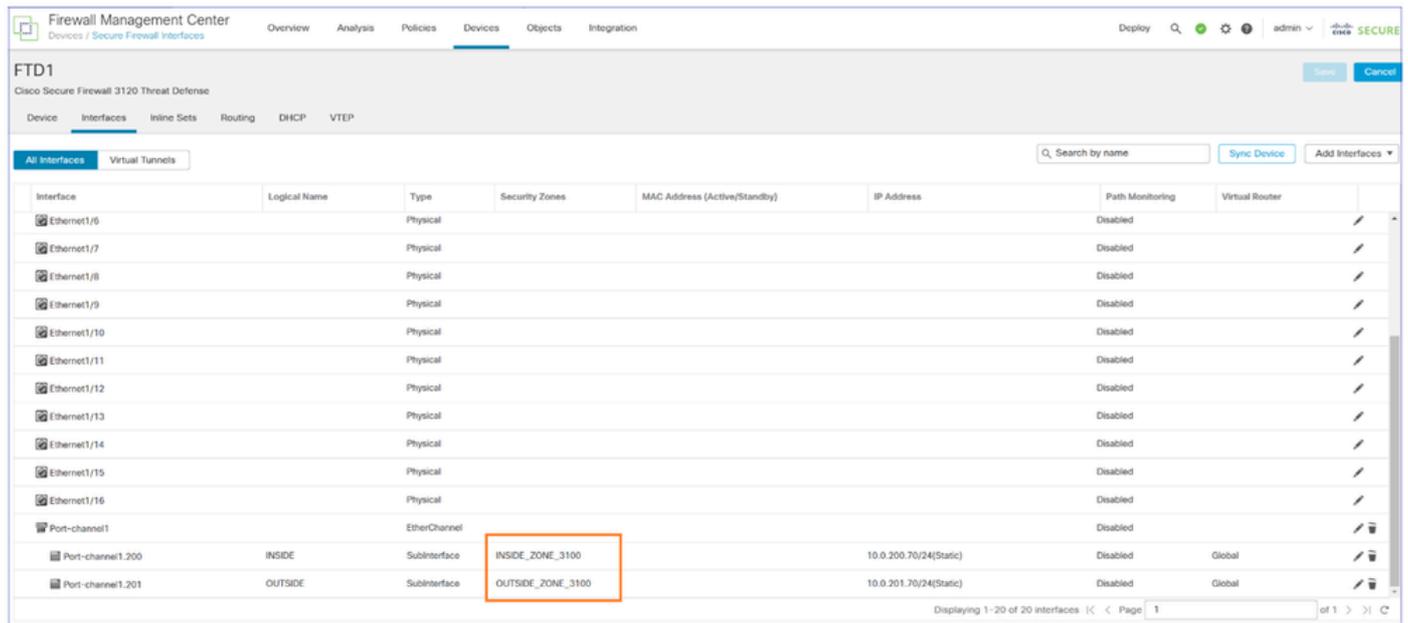
 Device Configuration Import

Device configurations imported successfully

[View Import Report](#)

7s 

Die Gerätekonfiguration wird auf FTD1 angewendet, z. B. Sicherheitszonen, ACP, NAT usw.:



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

 **Vorsicht:** Wenn Sie einen ACP haben, der auf viele Zugriffssteuerungselemente erweitert wird, kann die Kompilierung des ACP (tmatch compile) einige Minuten dauern. Mit diesem Befehl können Sie den AKP-Kompilierungsstatus überprüfen:

```
<#root>
```

```
FTD3100-3#
```

```
show asp rule-engine
```

```
Rule compilation Status:
```

```
Completed
```

Schritt 10: Beenden der FTD-Konfiguration

An diesem Punkt ist das Ziel, alle Funktionen zu konfigurieren, die nach der Registrierung beim FMC2 (Ziel-FMC) und dem Import der Geräteleitlinie in FTD1 noch fehlen können.

Stellen Sie sicher, dass Richtlinien wie NAT, Plattformeinstellungen, QoS usw. werden dem FTD zugewiesen. Sie sehen, dass die Richtlinien zugewiesen sind, aber die Bereitstellung noch aussteht.

Beispielsweise werden die Plattformeinstellungen importiert und dem Gerät zugewiesen, bis die Bereitstellung abgeschlossen ist:

Firewall Management Center
Devices / Platform Settings

Overview Analysis Policies **Devices** Objects Integration Deploy

Object Management
New Policy

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

Wenn NAT konfiguriert ist, wird die NAT-Richtlinie importiert und dem Gerät zugewiesen, bis die Bereitstellung abgeschlossen ist:

Firewall Management Center
Devices / NAT

Overview Analysis Policies **Devices** Objects Integration Deploy

NAT Exemptions New Policy

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

Sicherheitszonen werden auf die Schnittstellen angewendet:

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy

FTD1
Cisco Secure Firewall 3120 Threat Defense

Device Interfaces **Inline Sets** Routing DHCP VTEP

All Interfaces Virtual Tunnels

Search by name Sync Device Add Interfaces

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

Displaying 1-20 of 20 interfaces | Page 1 of 1

Die Routing-Konfiguration wird auf das FTD-Gerät angewendet:

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ **Secure**

FTD1

Cisco Secure Firewall 3120 Threat Defense

Device Interfaces Inline Sets **Routing** DHCP VTEP

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						

 Anmerkung: Konfigurieren Sie jetzt die Richtlinien, die nicht automatisch migriert werden konnten (z. B. VPNs).

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

Endpoints IKE IPsec Advanced

Node A:

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

Node B:

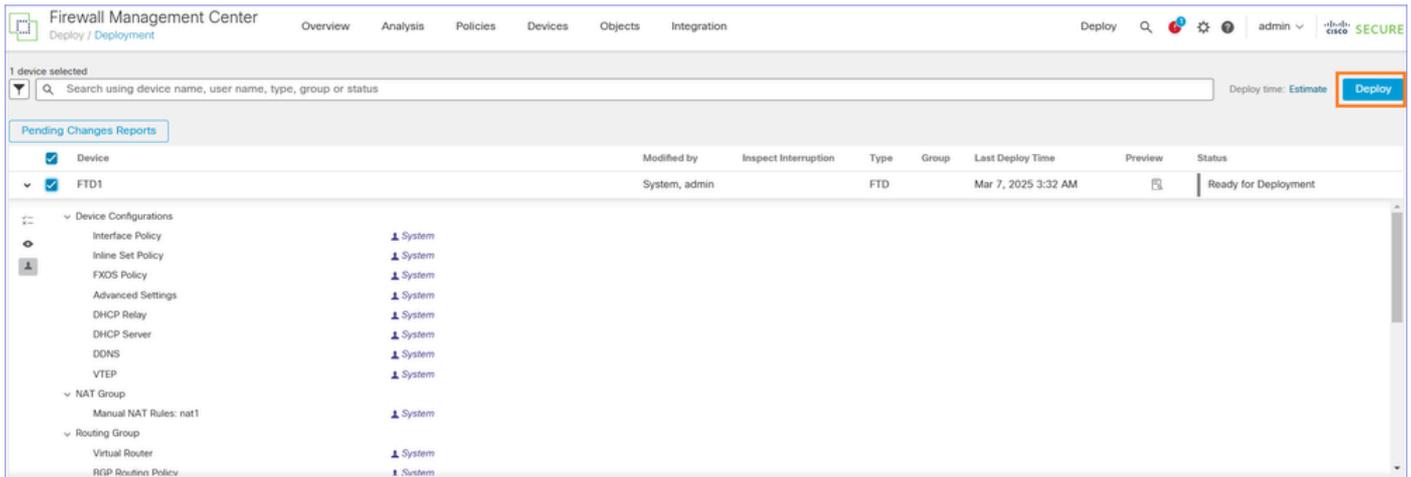
Device Name	VPN Interface	Protected Networks
Extranet Remote_FW	10.0.201.60	net_10.0.202.0

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

Cancel Save

 Anmerkung: Wenn das migrierte FTD S2S-VPN-Peers aufweist, die ebenfalls zum Ziel-FMC migriert wurden, müssen Sie das VPN konfigurieren, nachdem Sie alle FTDs zum Ziel-FMC verschoben haben.

Bereitstellen der ausstehenden Änderungen:



Schritt 11: Überprüfen der bereitgestellten FTD-Konfiguration

An diesem Punkt soll über die FTD-CLI überprüft werden, ob die gesamte Konfiguration vorhanden ist.

Es wird vorgeschlagen, die Ausgabe von "show running-config" aus beiden FTDs zu vergleichen. Sie können Tools wie WinMerge oder diff für den Vergleich verwenden.

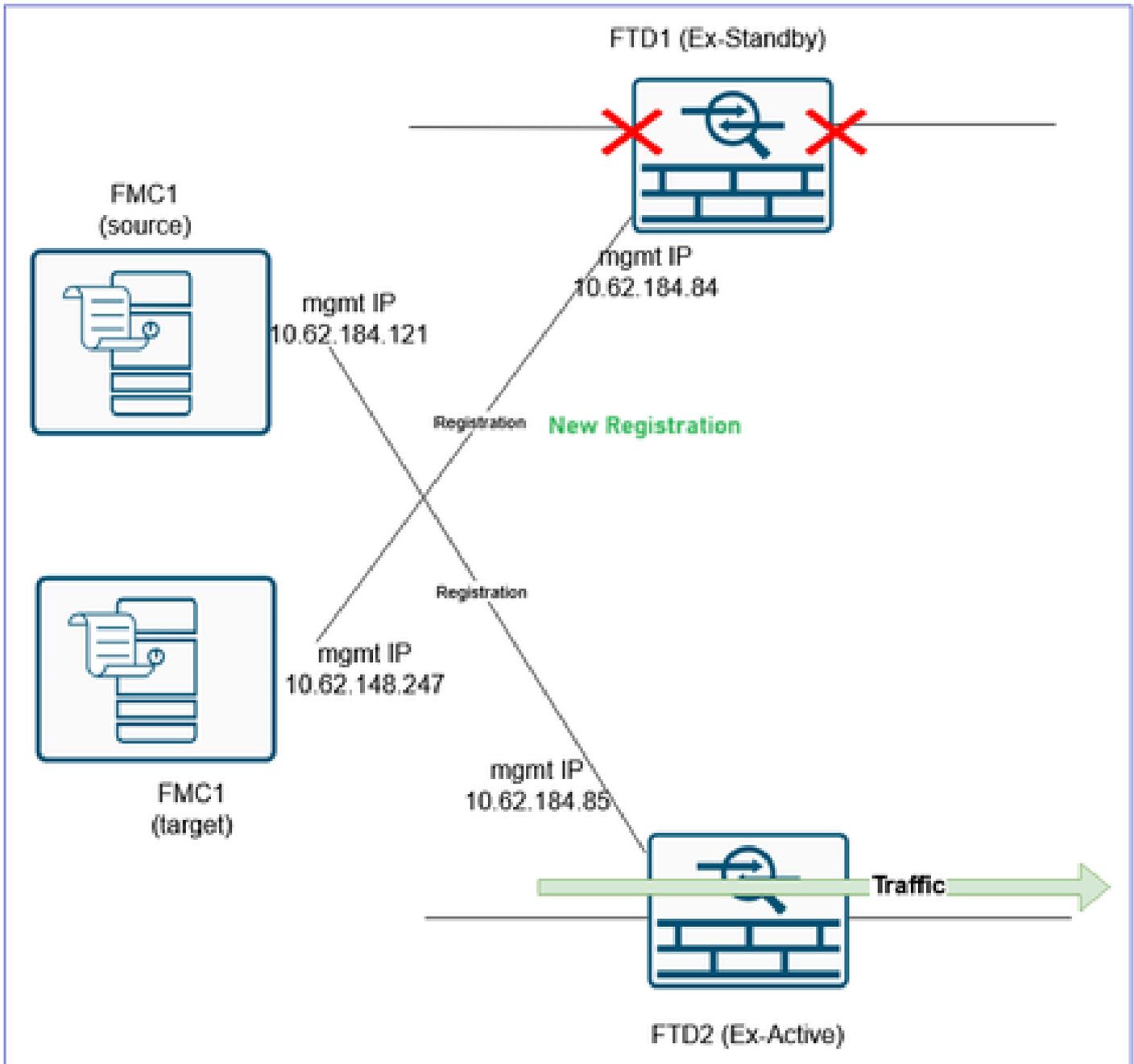
Unterschiede, die Sie sehen und die normal sind:

- Seriennummer des Geräts
- Schnittstellenbeschreibungen
- ACL-Regel-IDs
- Kryptoprüfsumme für Konfiguration

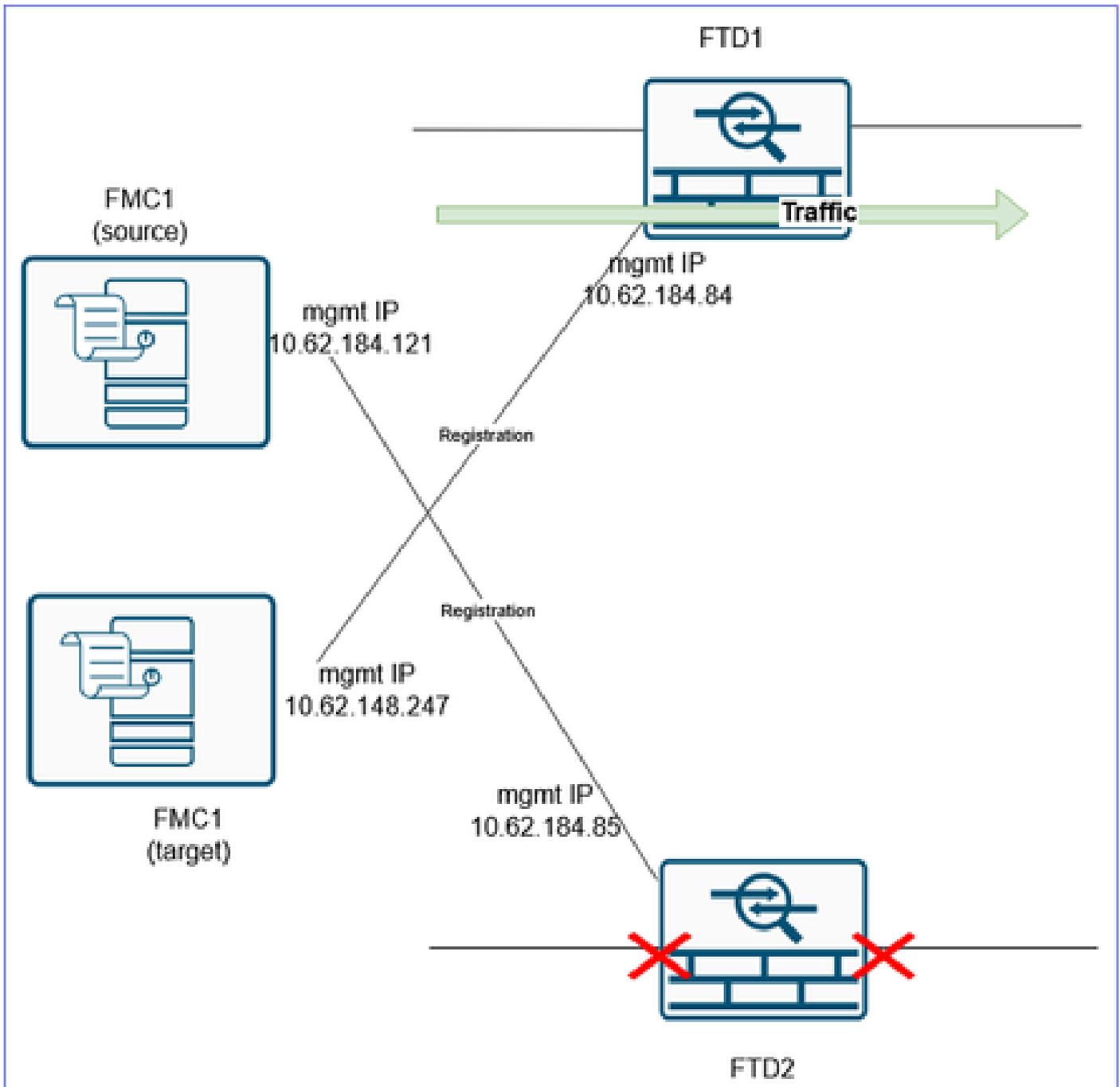
Schritt 12: Umstellung durchführen

In diesem Schritt soll der Datenverkehr von der FTD2, die derzeit den Datenverkehr verarbeitet und noch am alten Quell-FMC registriert ist, auf die FTD1, die am Ziel-FMC registriert ist, umgeleitet werden.

Vorher:



Nachher:



⚠ Vorsicht: Vereinbaren Sie eine MW für die Umstellung. Während der Umstellung wird der Datenverkehr unterbrochen, bis der gesamte Datenverkehr an die FTD1 umgeleitet wird, VPNs wiederhergestellt werden usw.

⚠ Vorsicht: Beginnen Sie die Umstellung erst, wenn die ACP-Kompilierung abgeschlossen ist (siehe Schritt 10 oben).

⚠ Warnung: Stellen Sie sicher, dass Sie entweder die Datenkabel vom FTD2 abziehen oder die entsprechenden Switch-Ports herunterfahren. Andernfalls können beide Geräte den Datenverkehr verarbeiten!

 **Vorsicht:** Da beide Geräte dieselbe IP-Konfiguration verwenden, muss der ARP-Cache der benachbarten L3-Geräte aktualisiert werden. Löschen Sie den ARP-Cache der benachbarten Geräte manuell, um die Umstellung auf den Datenverkehr zu beschleunigen.

 **Tipp:** Sie können auch ein GARP-Paket senden und den ARP-Cache der benachbarten Geräte mit dem FTD CLI-Befehl aktualisieren:

```
<#root>
```

```
FTD3100-3#
```

```
debug menu ipaddrut1 5 10.0.200.70
```

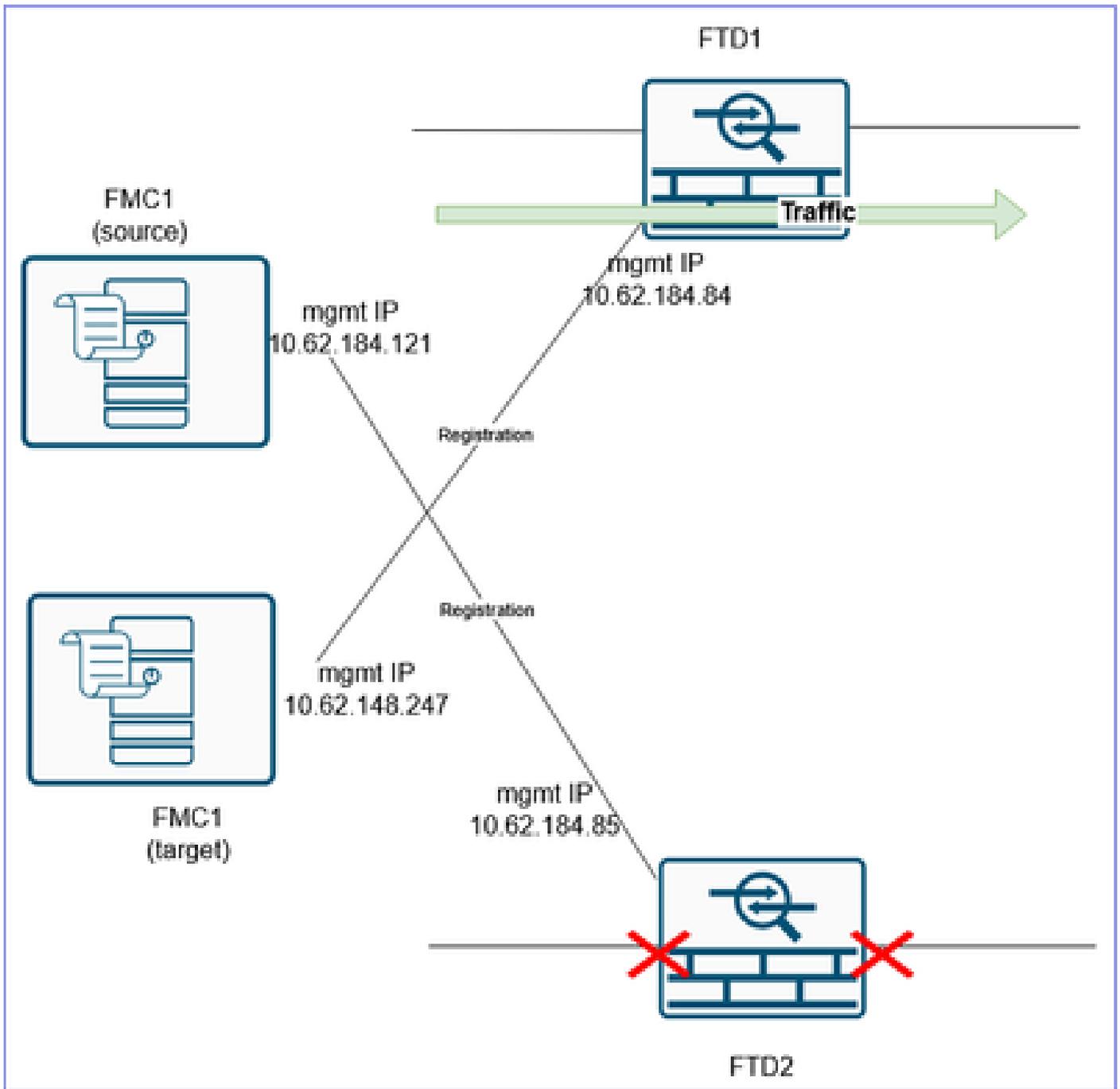
```
Gratuitous ARP sent for 10.0.200.70
```

Sie müssen diesen Befehl für jede IP wiederholen, die der FW gehört. So kann es schneller sein, nur den ARP-Cache der benachbarten Geräte zu löschen, als GARP-Pakete für jede IP zu senden, die der Firewall gehört.

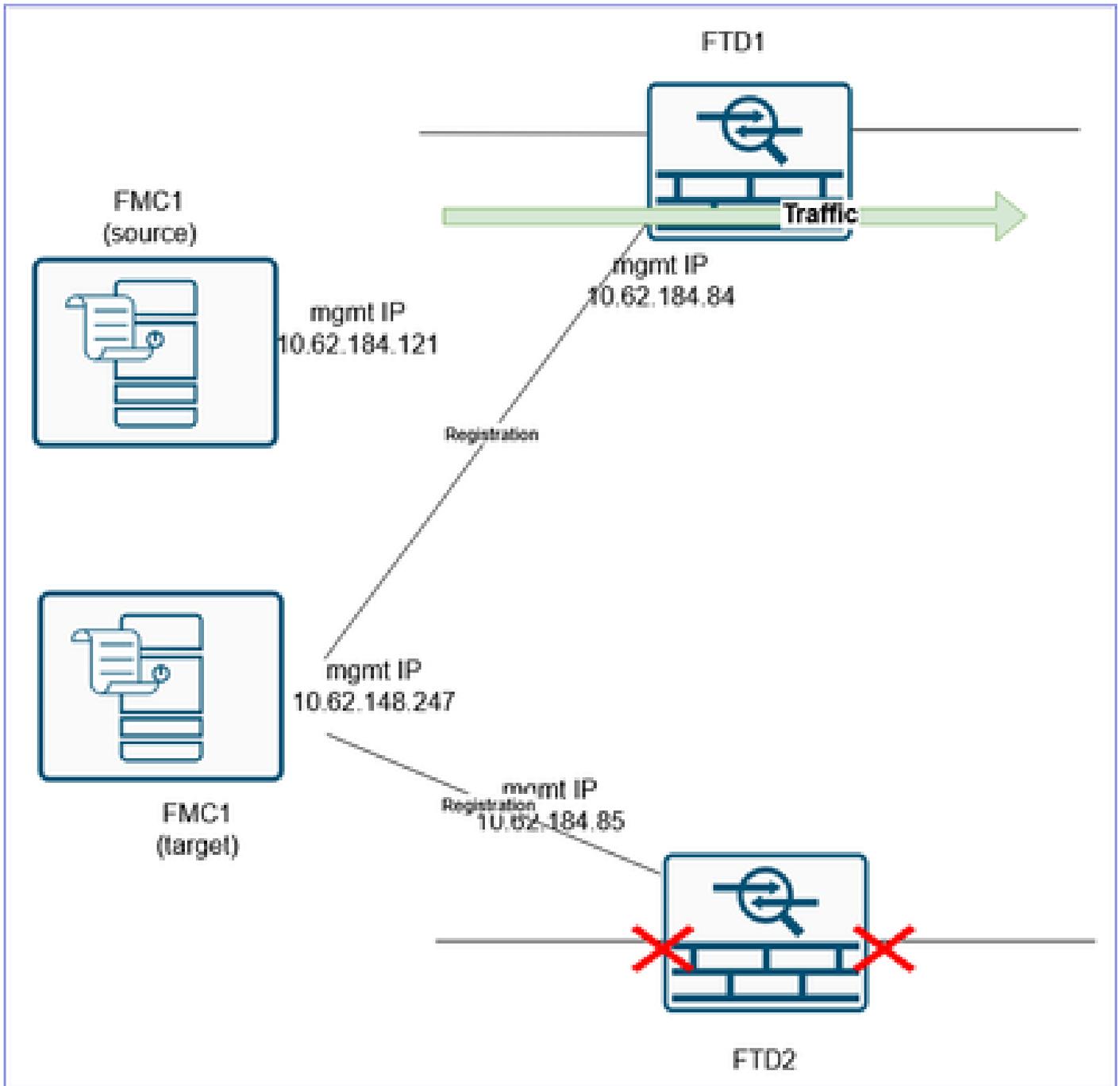
Schritt 13: Migration der zweiten FTD auf das FMC2 (Ziel-FMC)

Der letzte Punkt ist die Reform des HA-Paares. Dazu müssen Sie zunächst den FTD2 aus dem FMC1 (Quell-FMC) löschen und beim FMC2 (Ziel-FMC) registrieren.

Vorher:



Nachher:



Wenn Sie eine VPN-Konfiguration mit dem FTD2 verbunden haben, müssen Sie diese zuerst entfernen, bevor Sie das FTD löschen. In verschiedenen Fällen wird eine ähnliche Meldung angezeigt:

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-Verifizierung:

```
<#root>
```

```
>
```

```
show managers
```

```
No managers configured.
```

Es empfiehlt sich, die gesamte FTD-Konfiguration vor der Registrierung beim Ziel-FMC zu löschen. Eine schnelle Methode hierfür ist das Wechseln zwischen den Firewall-Modi.

Wenn Sie beispielsweise in den Routing-Modus gewechselt haben, wechseln Sie in den

transparenten Modus und dann zurück in den Routing-Modus:

```
<#root>
```

```
>
```

```
configure firewall transparent
```

Und dann:

```
<#root>
```

```
>
```

```
configure firewall routed
```

Dann registrieren Sie es beim FMC2 (Ziel-FMC):

```
<#root>
```

```
>
```

```
configure manager add 10.62.148.247 cisco
```

```
Manager 10.62.148.247 successfully configured.
```

```
Please make note of reg_key as this will be required while adding Device in FMC.
```

```
>
```

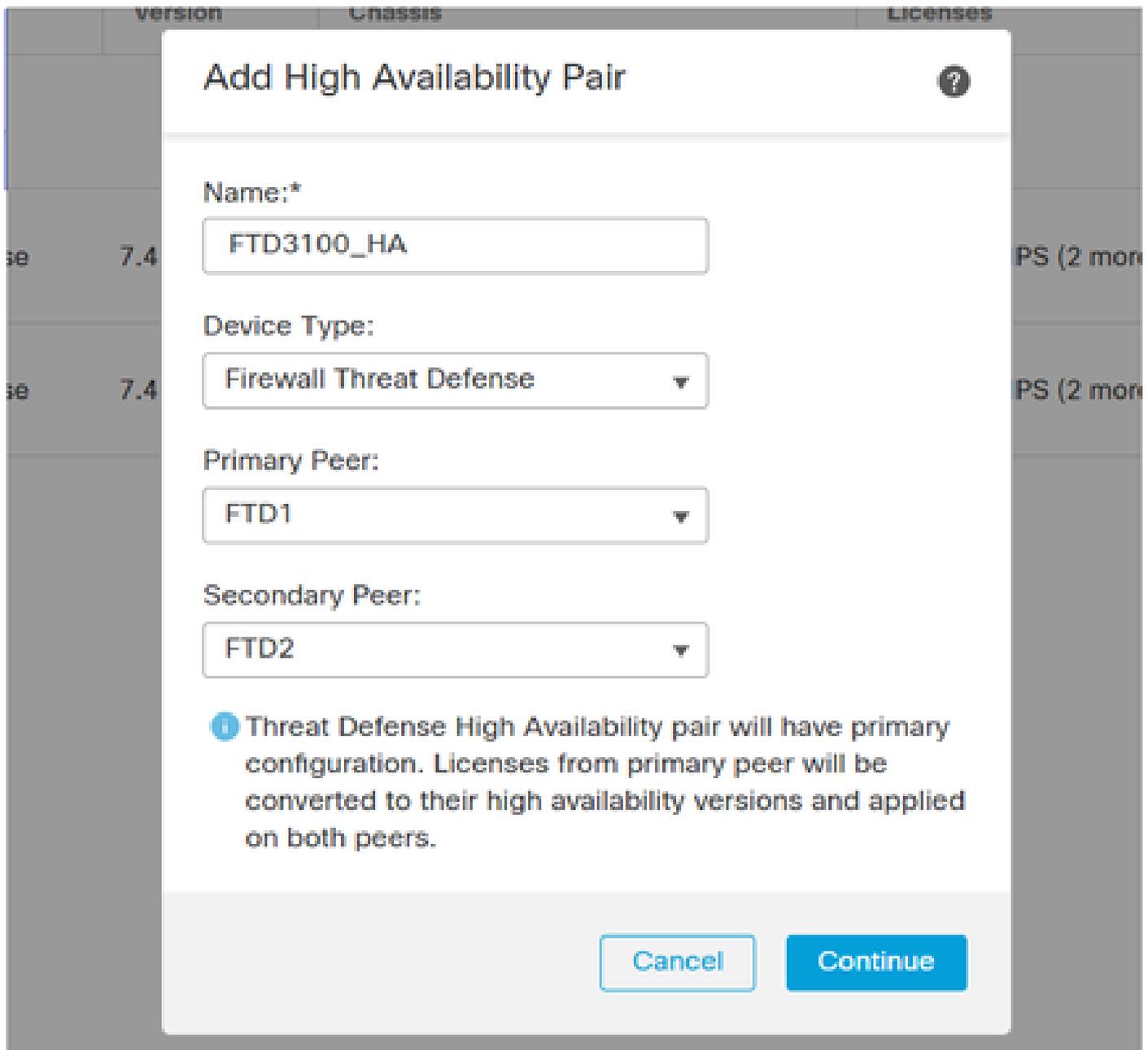
Ergebnis:

Schritt 14. Umgestalten des FTD HA

Anmerkung: Diese Aufgabe (wie jede HA-bezogene Aufgabe) muss auch während einer MW durchgeführt werden. Während der HA-Aushandlung kommt es für ca. 1 Minute zu einem Ausfall des Datenverkehrs, da die Datenschnittstellen ausfallen.

Navigieren Sie auf dem Ziel-FMC zu Devices (Geräte) > Device Management (Geräteverwaltung) und Add (Hinzufügen) > High Availability (Hochverfügbarkeit).

 **Vorsicht:** Stellen Sie sicher, dass Sie als primären Peer den FTD auswählen, der den Datenverkehr verarbeitet (FTD1 in diesem Szenario):



Neukonfiguration der HA-Einstellungen, einschließlich überwachter Schnittstellen, Standby-IPs, virtueller MAC-Adressen usw.

Überprüfung von FTD1 CLI:

```
<#root>
```

```
FTD3100-3#
```

```
show failover | include host
```

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

Überprüfung von FTD2 CLI:

```
<#root>
```

```
FTD3100-3#
```

```
show failover | include host
```

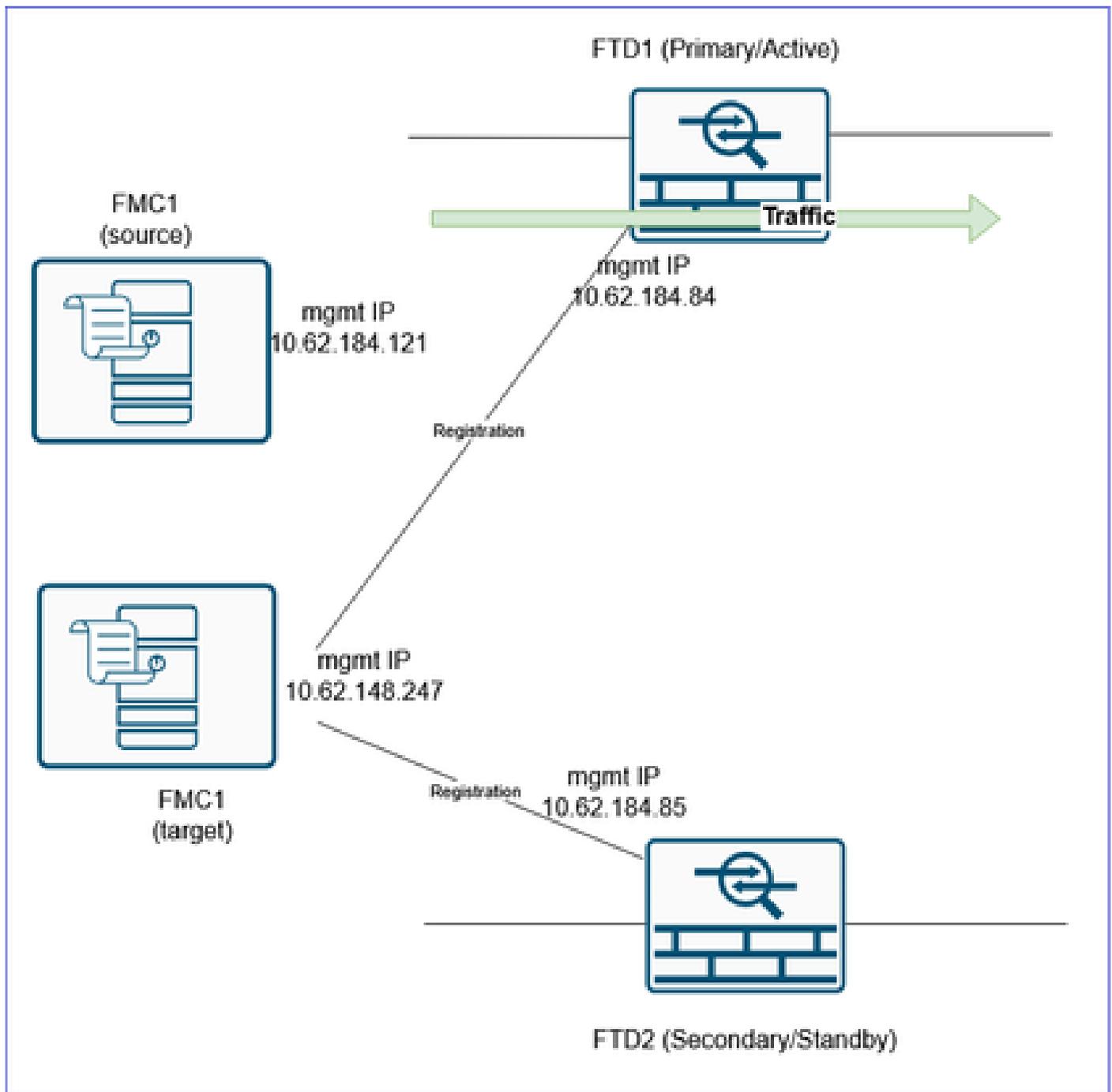
```
This host: Secondary - Standby Ready
```

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

FMC-UI-Verifizierung:

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

Schalten Sie schließlich die Datenschnittstellen des FTD2-Geräts ein bzw. wieder ein.



Referenzen

- [Exportieren und Importieren der Gerätekonfiguration](#)
- [Hochverfügbarkeitspaar hinzufügen](#)
- [FTD-Migration von einem FMC zu einem anderen FMC](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.