Migrate FTD HA (Failover) to Another FMC

Contents

Introduction

This document describes the procedure to migrate an FTD HA from an existing FMC to another FMC.

For a standalone firewall migration to a new FMC check 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

Abbreviations

ACP = Access Control Policy

ARP = Address Resolution Protocol

CLI = Command Line Interface

FMC = Secure Firewall Management Center

FTD = Secure Firewall Threat Defense

GARP = Gratuitous ARP

HA = High Availability

MW = Maintenance Window

UI = User Interface

Prerequisites

Before starting the migration process, ensure that you have these prerequisites in place:

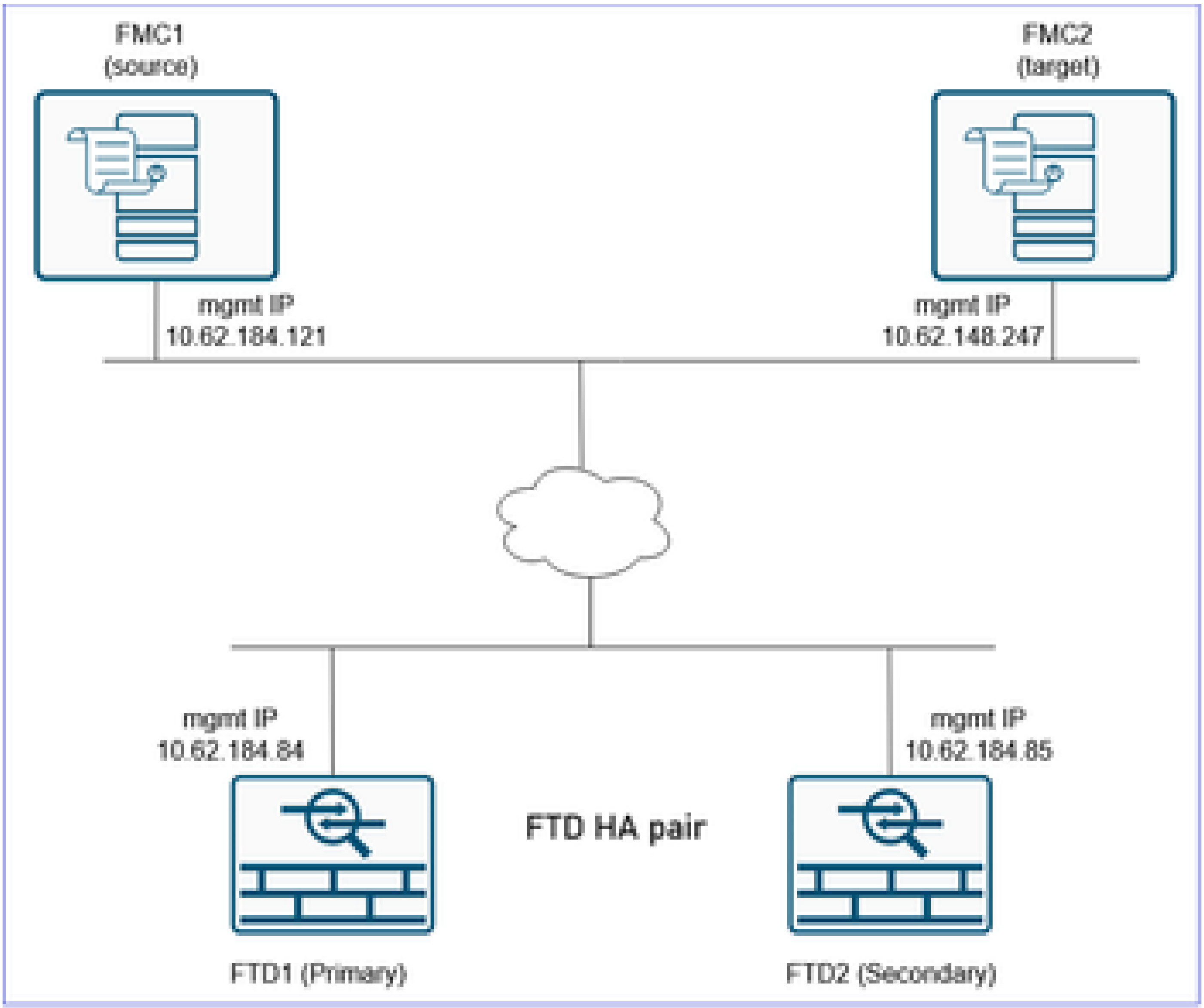
- UI and CLI access to both the source and destination FMCs.
- Administrative credentials for both FMCs and firewalls.
- Console access to both firewalls.
- Access to the L3 upstream and downstream devices (in case you need to clear the ARP cache).
- Ensure that the destination/target FMC has the same version as the source/old FMC.
- Ensure that the destination/target FMC has the same licenses as the source/old FMC.
- Ensure you arrange a MW to perform the migration since it is going to impact the transit traffic.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall 31xx, FTD version 7.4.2.2.
- Secure Firewall Management Center version 7.4.2.2.
- The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Topology



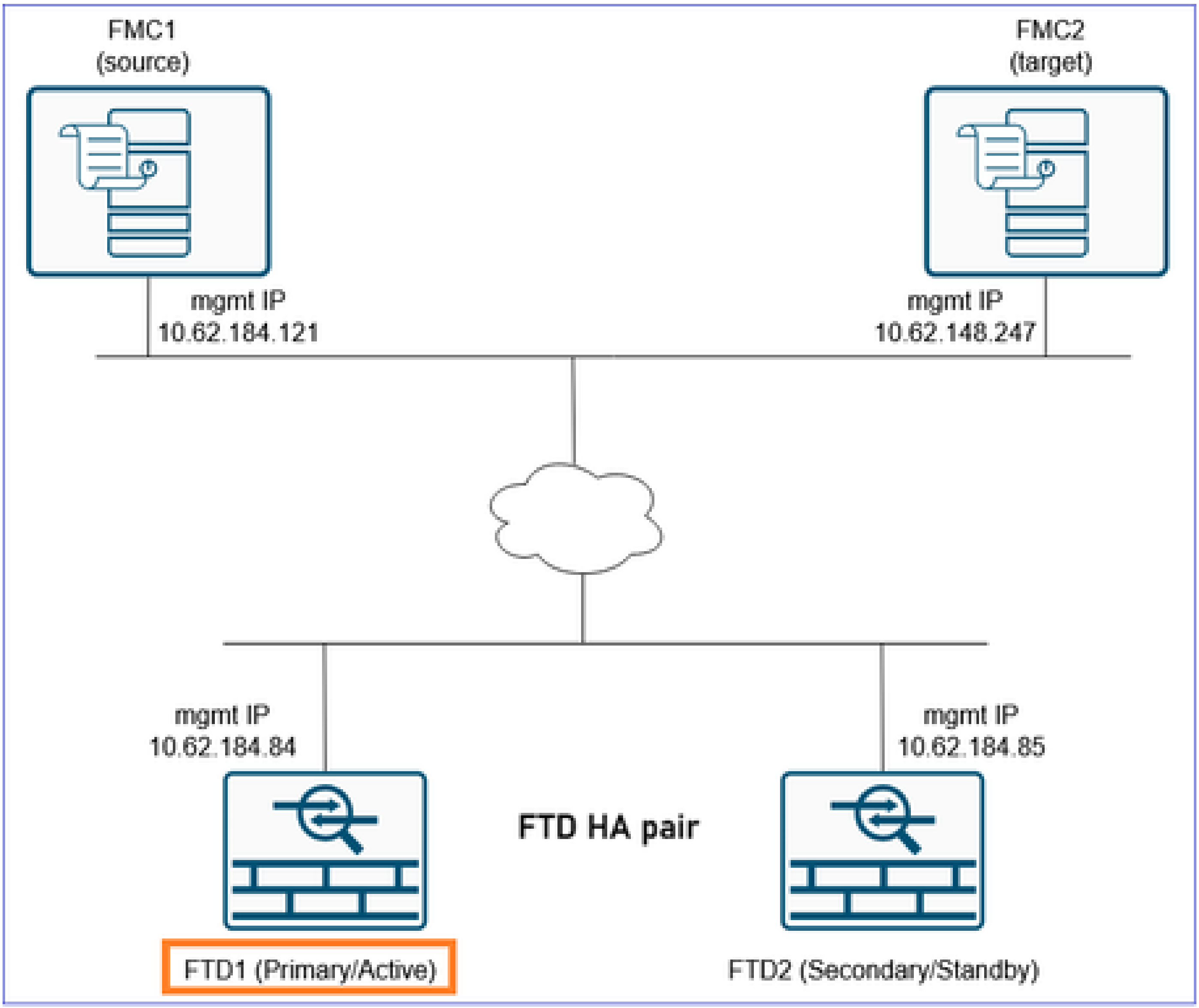
Configure

Migration Steps

For this scenario we consider these states:

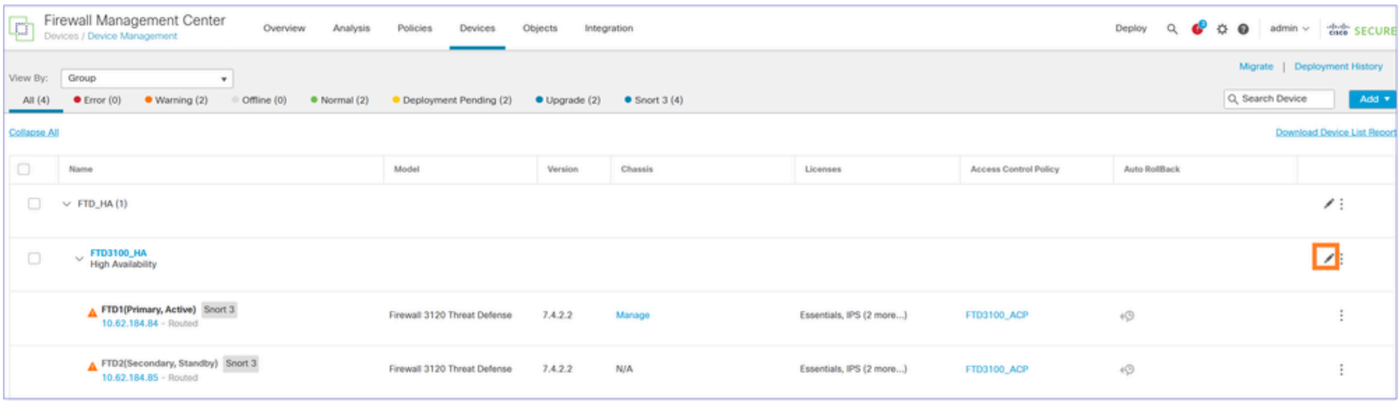
FTD1: Primary/Active

FTD2: Secondary/Standby



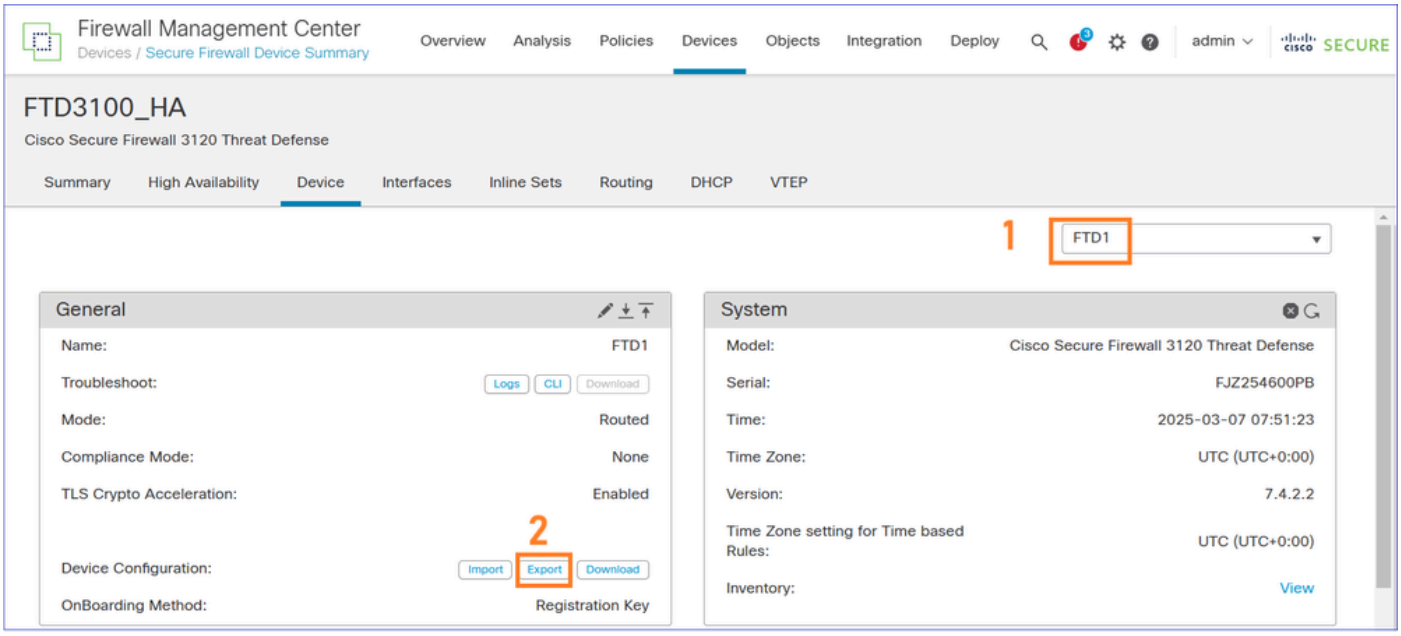
Step 1. Export the Device Configuration from the Primary Firewall

On the FMC1 (source FMC) navigate to **Devices > Device Management.** Select the FTD HA pair and select **Edit**:



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	

Navigate to the **Device** tab. Ensure that the Primary/Active FTD (FTD1 in this case) is selected and select **Export** to export the Device configuration:



FTD3100_HA

Cisco Secure Firewall 3120 Threat Defense

General

Name: FTD1

Troubleshoot: Logs CLI Download

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Enabled

Device Configuration: Import Export Download

OnBoarding Method: Registration Key

System

Model: Cisco Secure Firewall 3120 Threat Defense

Serial: FJZ254600PB

Time: 2025-03-07 07:51:23

Time Zone: UTC (UTC+0:00)

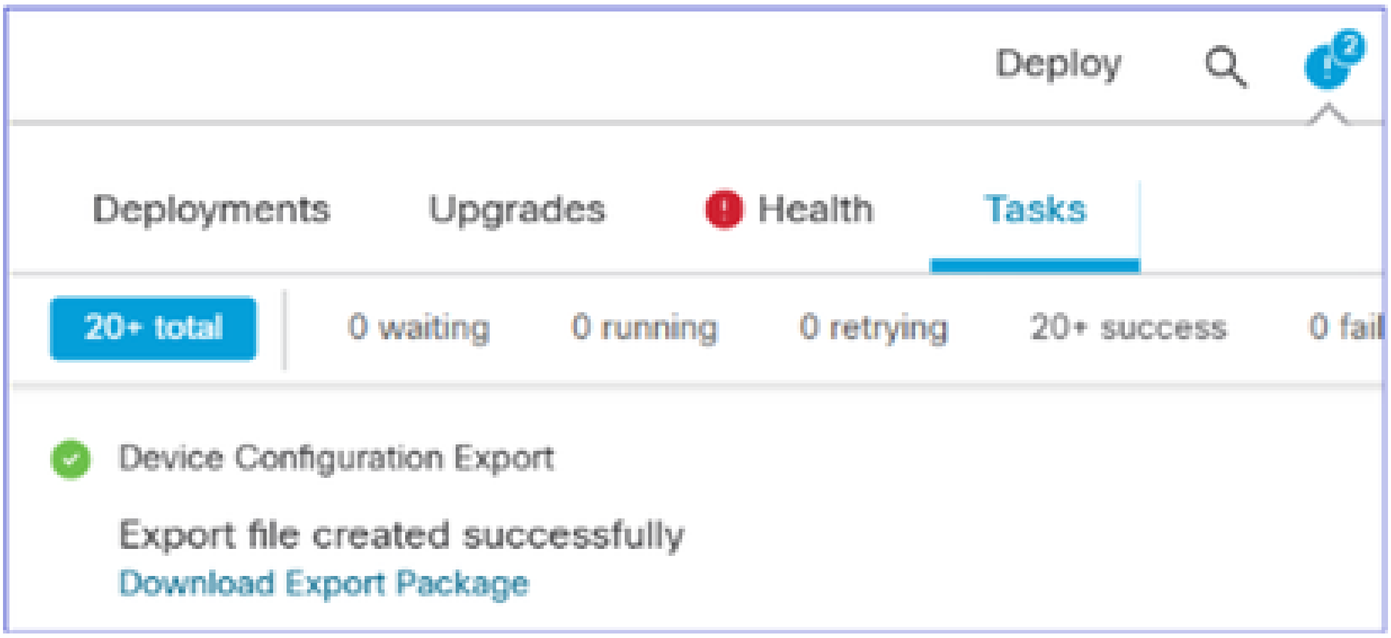
Version: 7.4.2.2

Time Zone setting for Time based Rules: UTC (UTC+0:00)

Inventory: View

Note: The Export option is available as of 7.1 software release and later.

You can navigate to **Notifications** > **Tasks** page to ensure that the export has completed. Then, select the **Download Export Package**:



Device Configuration Export

Export file created successfully

Download Export Package

Alternatively, you can click the **Download** button in the **General** area. You get an sfo file, for example DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

The file contains device-related configuration such as:

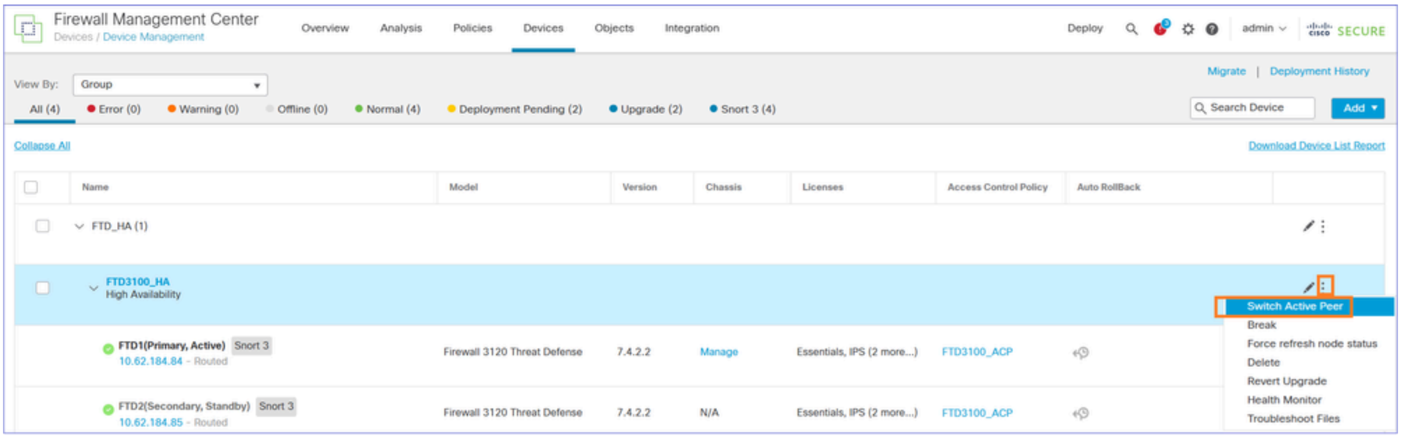
- Routed Interfaces
- Inline Sets
- Routing
- DHCP
- VTEP
- Associated objects

Note: The exported configuration file can be imported back only to same FTD. The UUID of the FTD must match with imported sfo file's content. The same FTD can be registered on another FMC and sfo file can be imported.

Reference: 'Export and Import the Device Configuration'
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

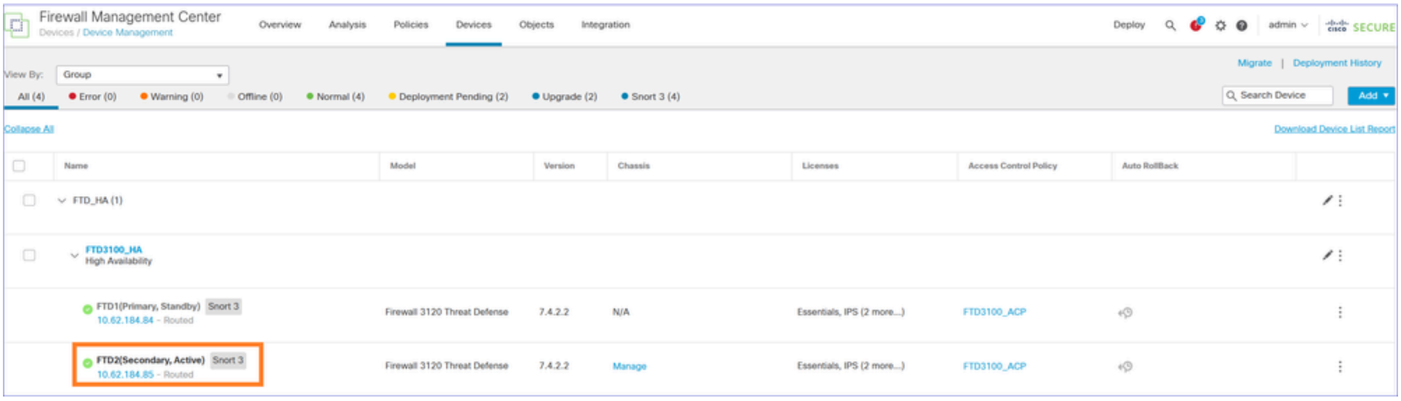
Step 2. Make the Secondary FTD Active

Navigate to **Devices** > **Device Management,** select the FTD HA pair, and select **Switch Active Pair:**



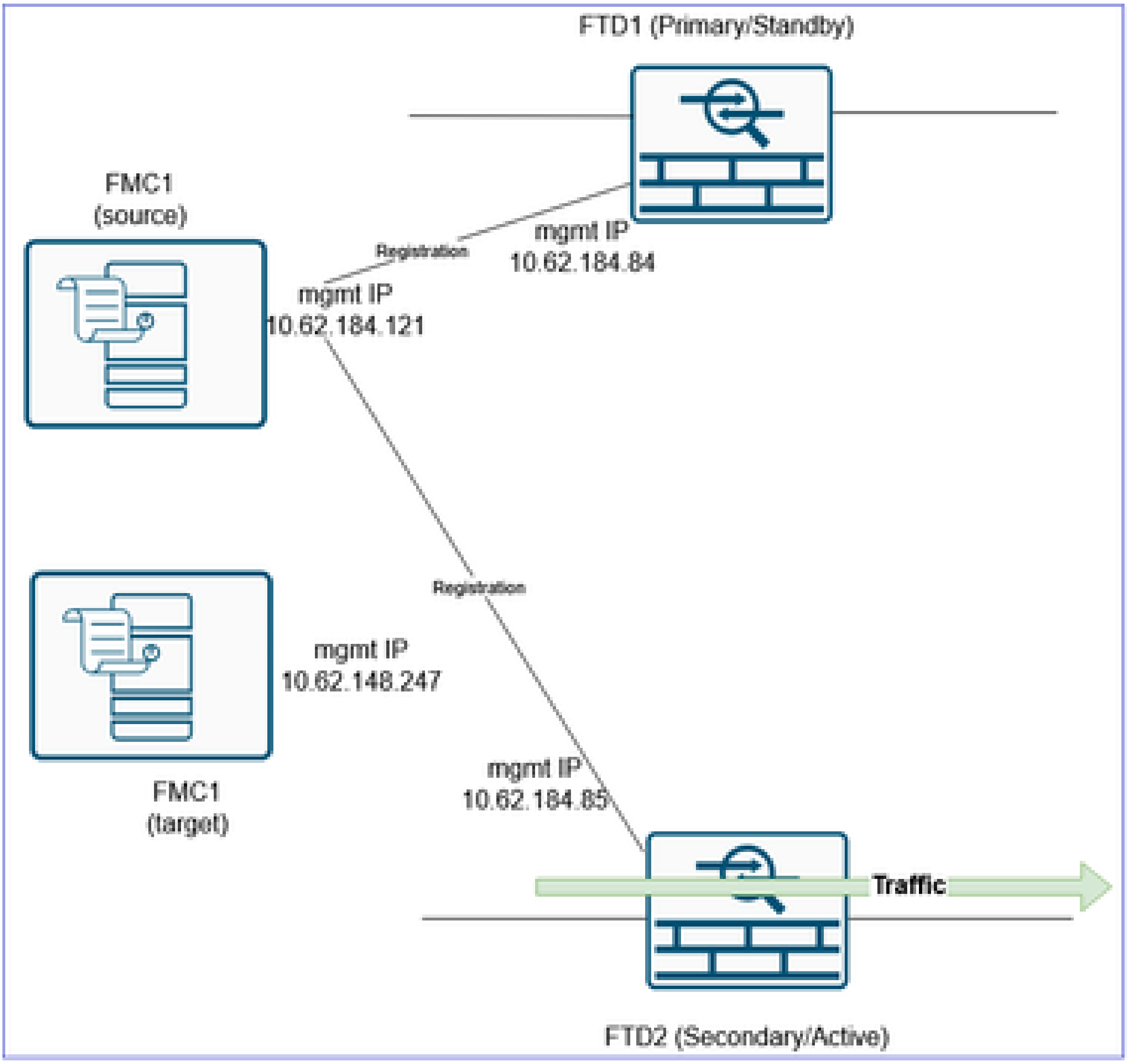
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (1)						
FTD3100_HA High Availability						
FTD1(Primary, Active) Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	
FTD2(Secondary, Standby) Snort 3 10.62.184.85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

The result is FTD1 (Primary/Standby) and FTD (Secondary/Active):



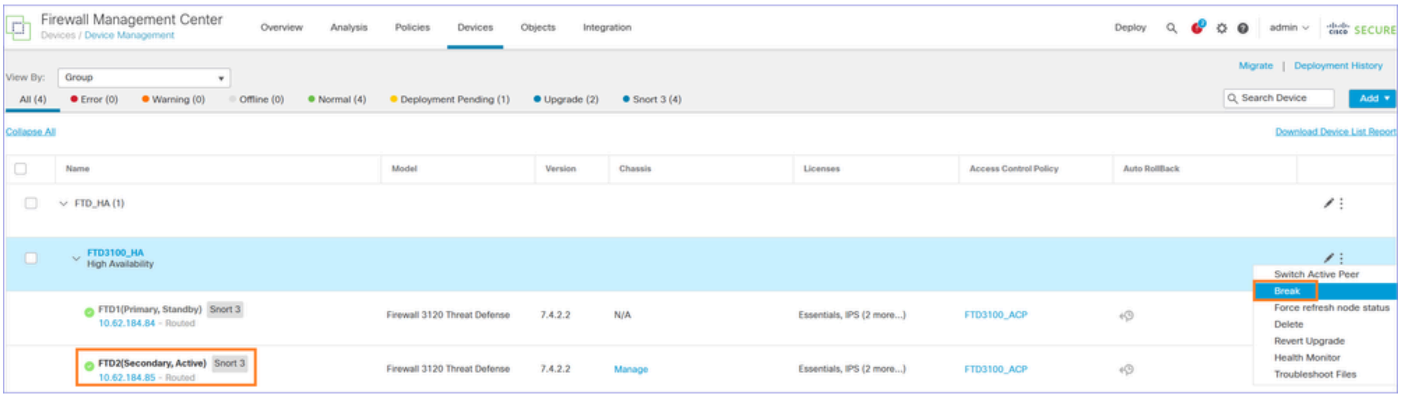
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (1)						
FTD3100_HA High Availability						
FTD1(Primary, Standby) Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP	
FTD2(Secondary, Active) Snort 3 10.62.184.85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

Now the traffic is handled by the Secondary/Active FTD:



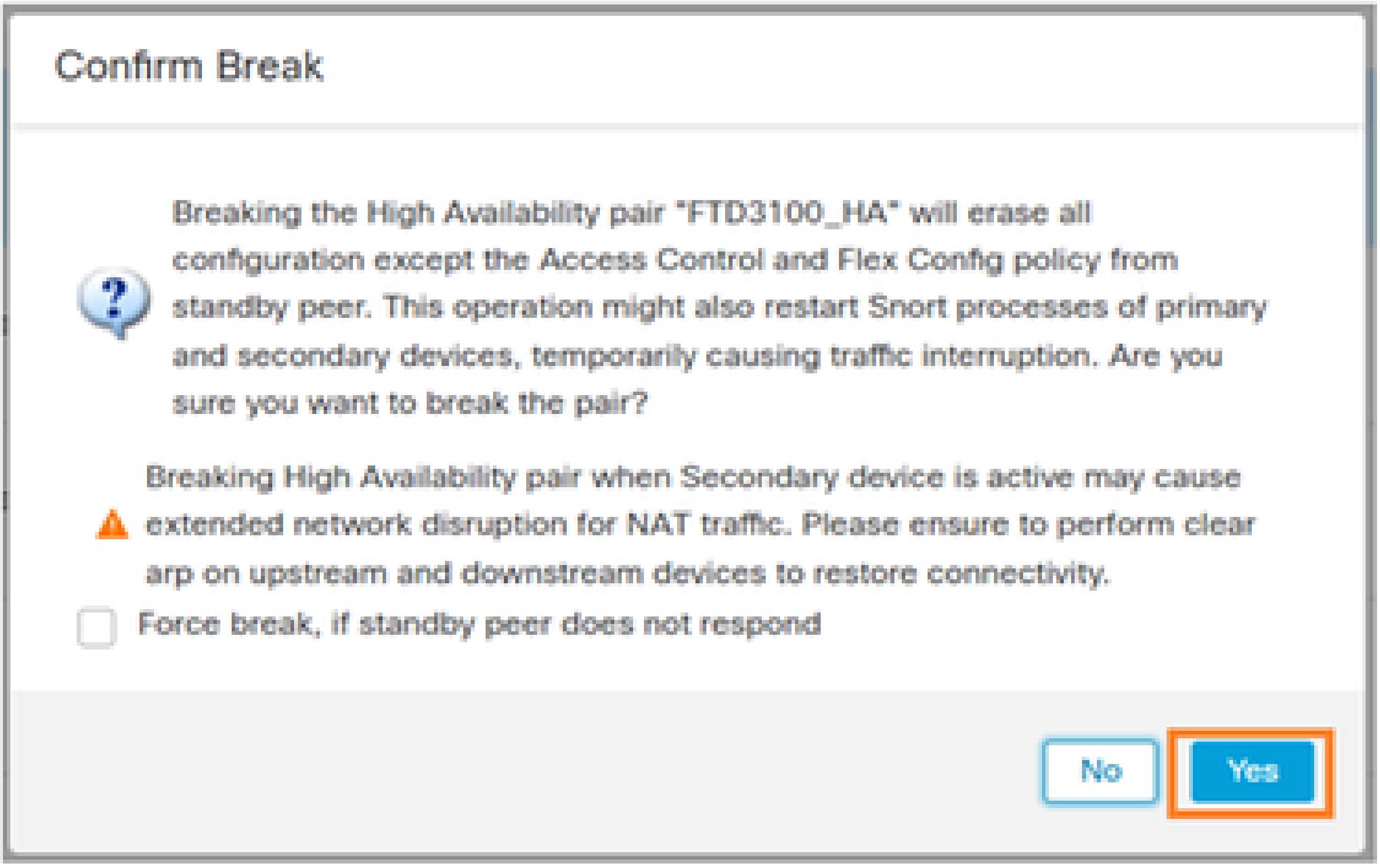
Step 3. Break the FTD HA

Navigate to **Devices > Device Management** and **Break** the FTD HA:



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (1)						
FTD3100_HA High Availability						
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	

This window appears. Select **Yes**



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

Note: At this point you can experience some traffic interruption for a few seconds since the Snort engine restarts during the HA break. Also, as the message mentions, if you use NAT and experience a prolonged traffic outage consider clearing the ARP cache on upstream and downstream devices.

After breaking the FTD HA, you have two standalone FTDs on FMC.

From configuration point of view, the FTD2 (ex-Active) still has the configuration in place except the failover-related configuration and is handling the traffic:

<#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
```

The FTD1 (ex-Standby) has all the configuration removed:

<#root>

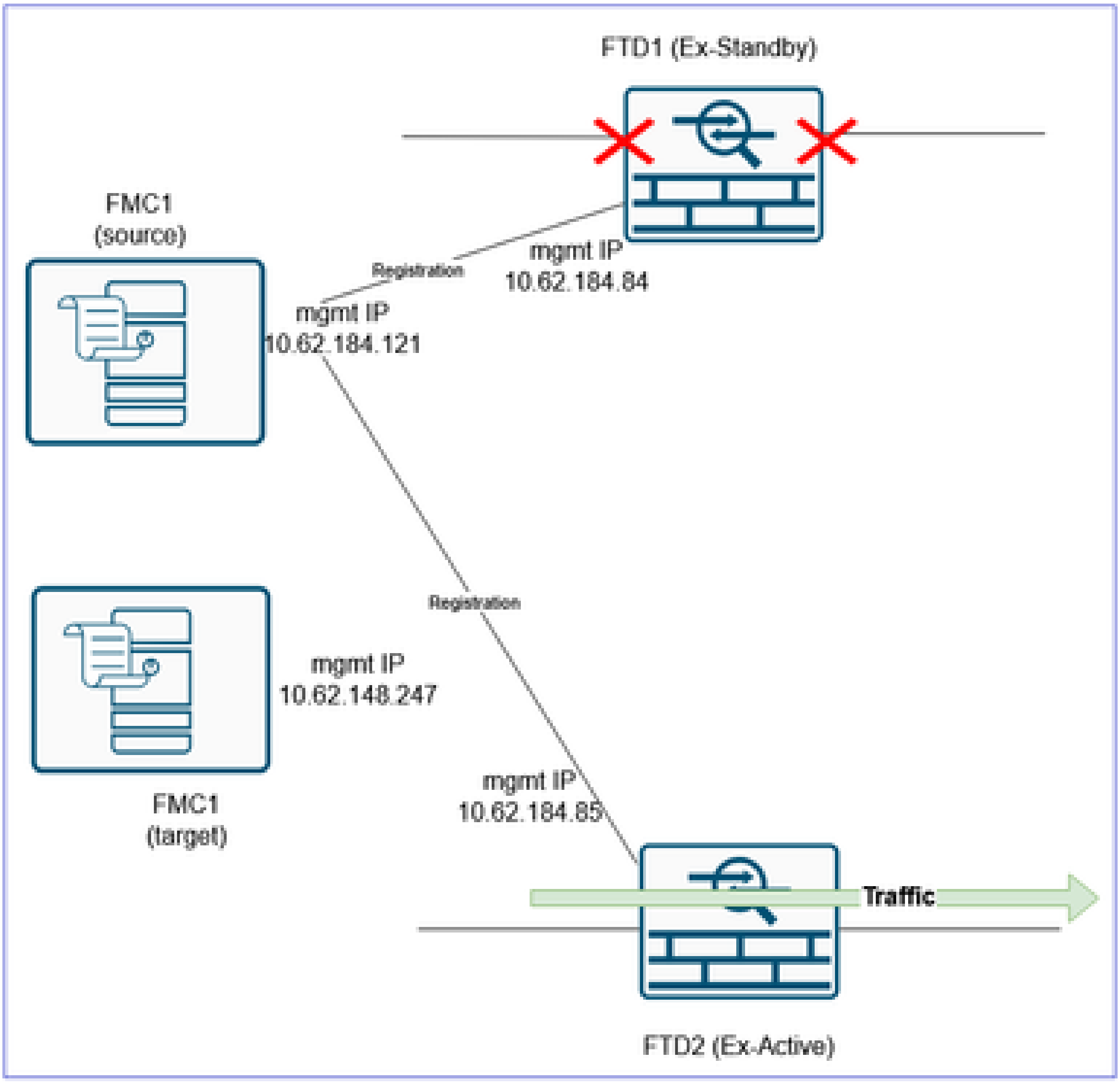
```
FTD3100-3#

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
```

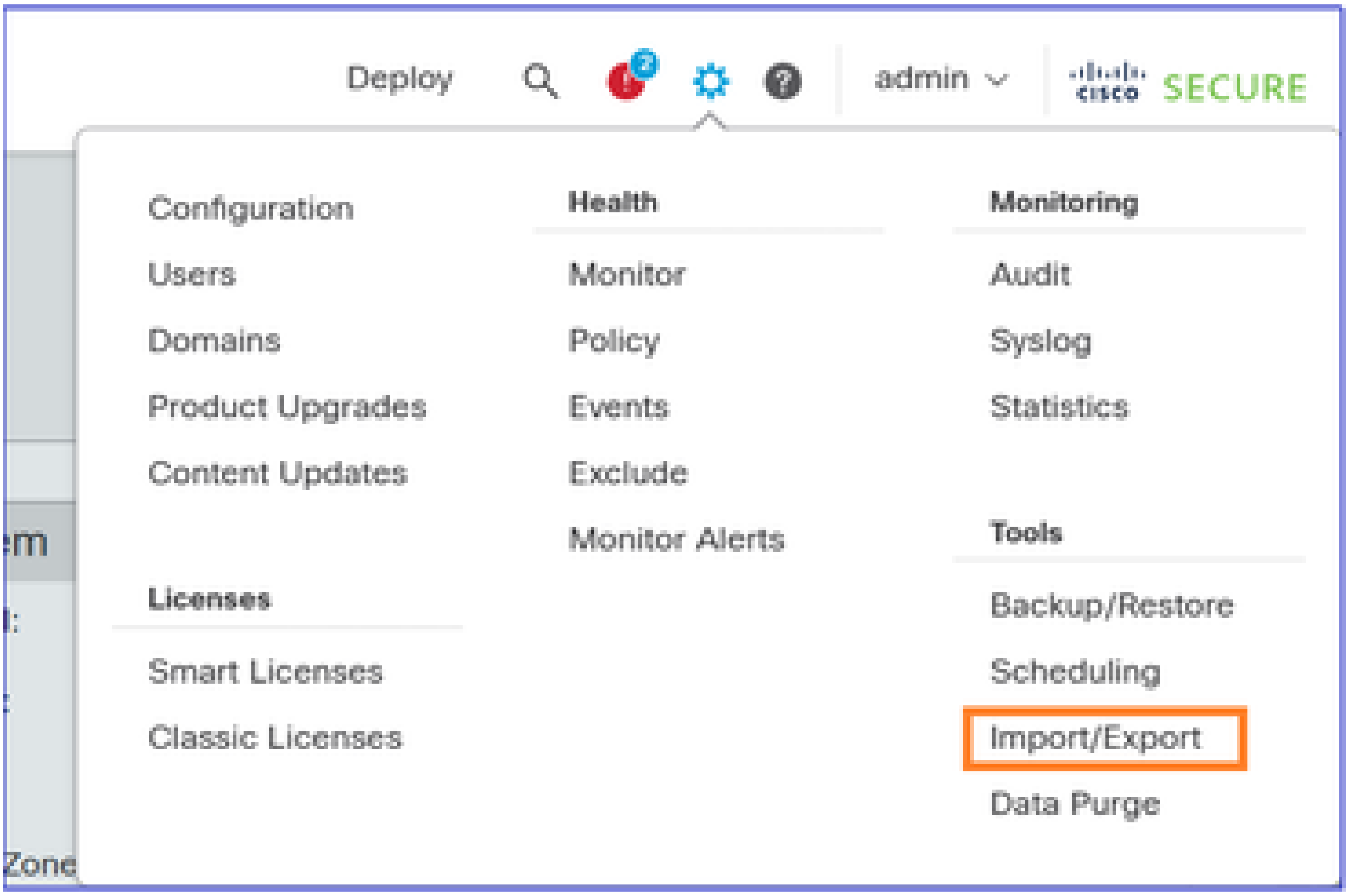
Step 4. Isolate the FTD1 (ex-Primary) data interfaces

Disconnect the **data cables** from the FTD1 (ex-Primary). Leave only the FTD management port connected.



Step 5. Export the FTD Shared Policies

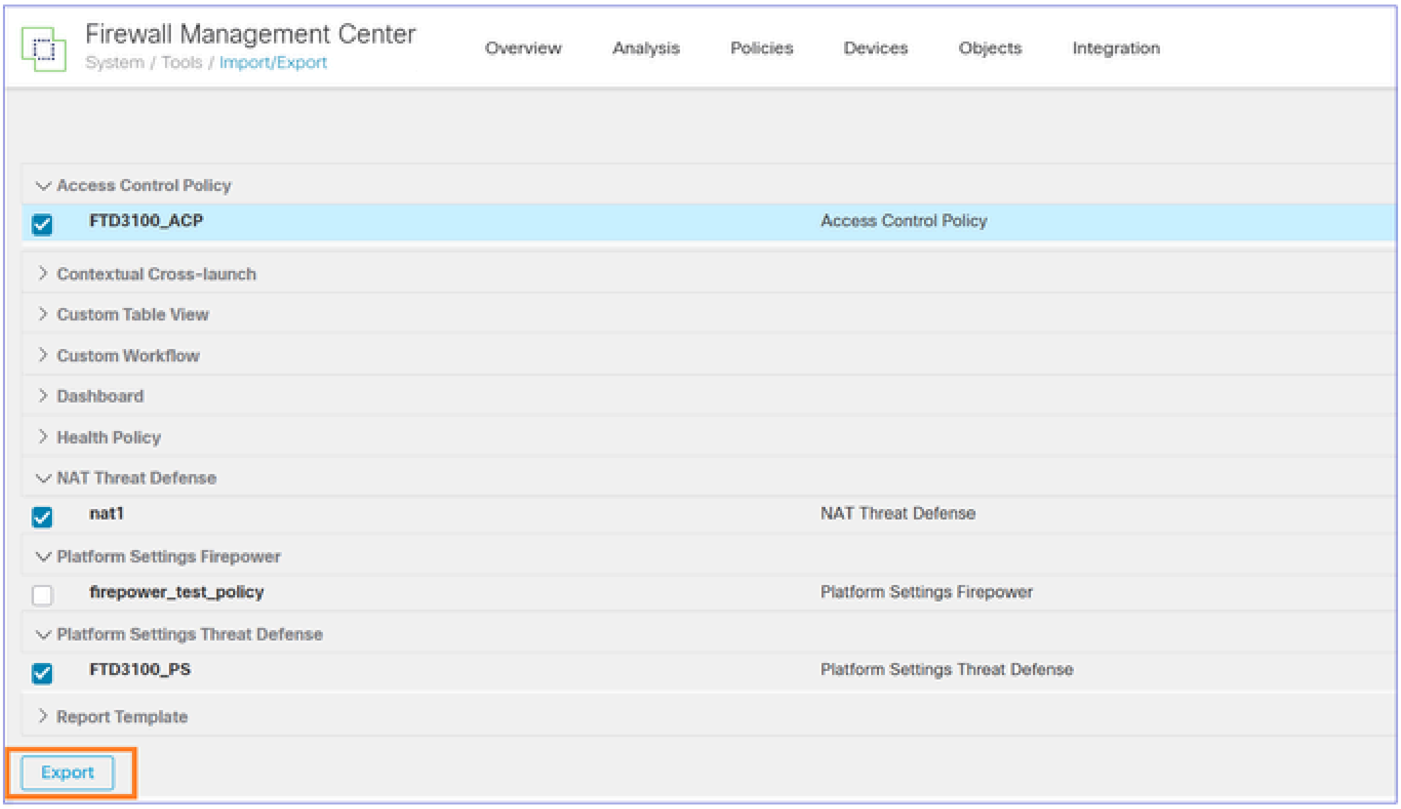
Navigate to **System** > **Tools** and select **Import/Export:**



Export the various policies attached to the device. Ensure you export all the policies attached to the FTD such as:

- Access Control Policy (ACP)
- Network Address Translation (NAT) policy
- Health Policy (if custom)
- FTD Platform Settings

and so on.



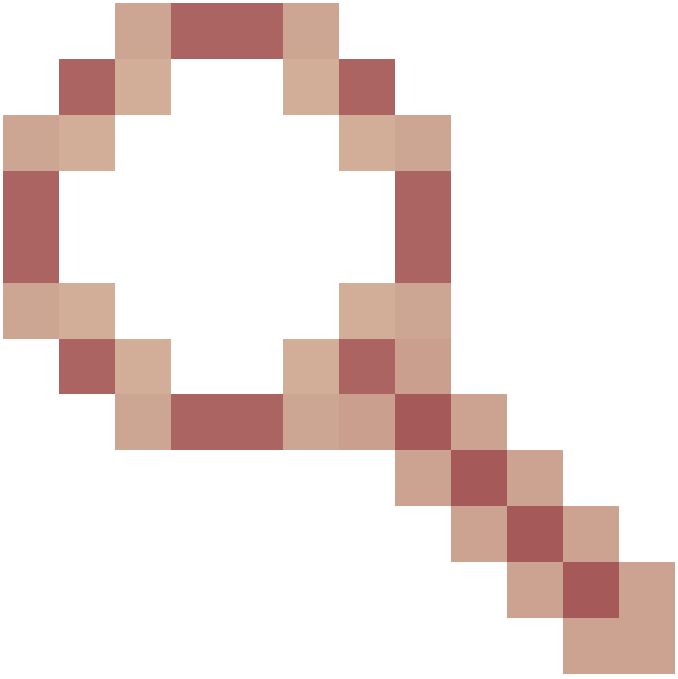
Firewall Management Center
System / Tools / Import/Export

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

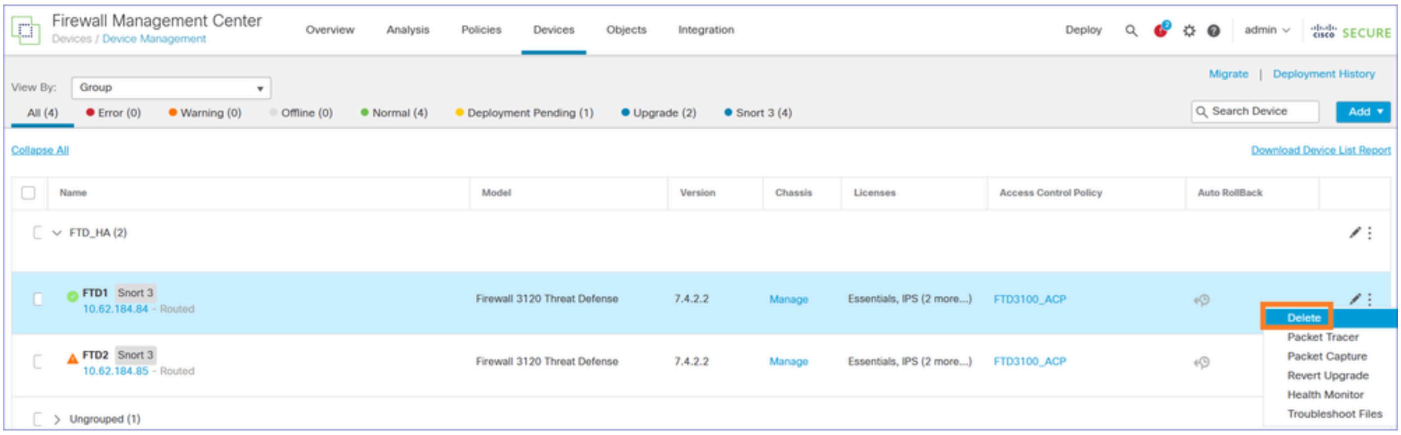
Note: At the time of this writing, exporting VPN-related configuration is not supported. You need to manually reconfigure the VPN on the FMC2 (target FMC) after the device registration.



Related enhancement Cisco bug ID CSCwf05294
.

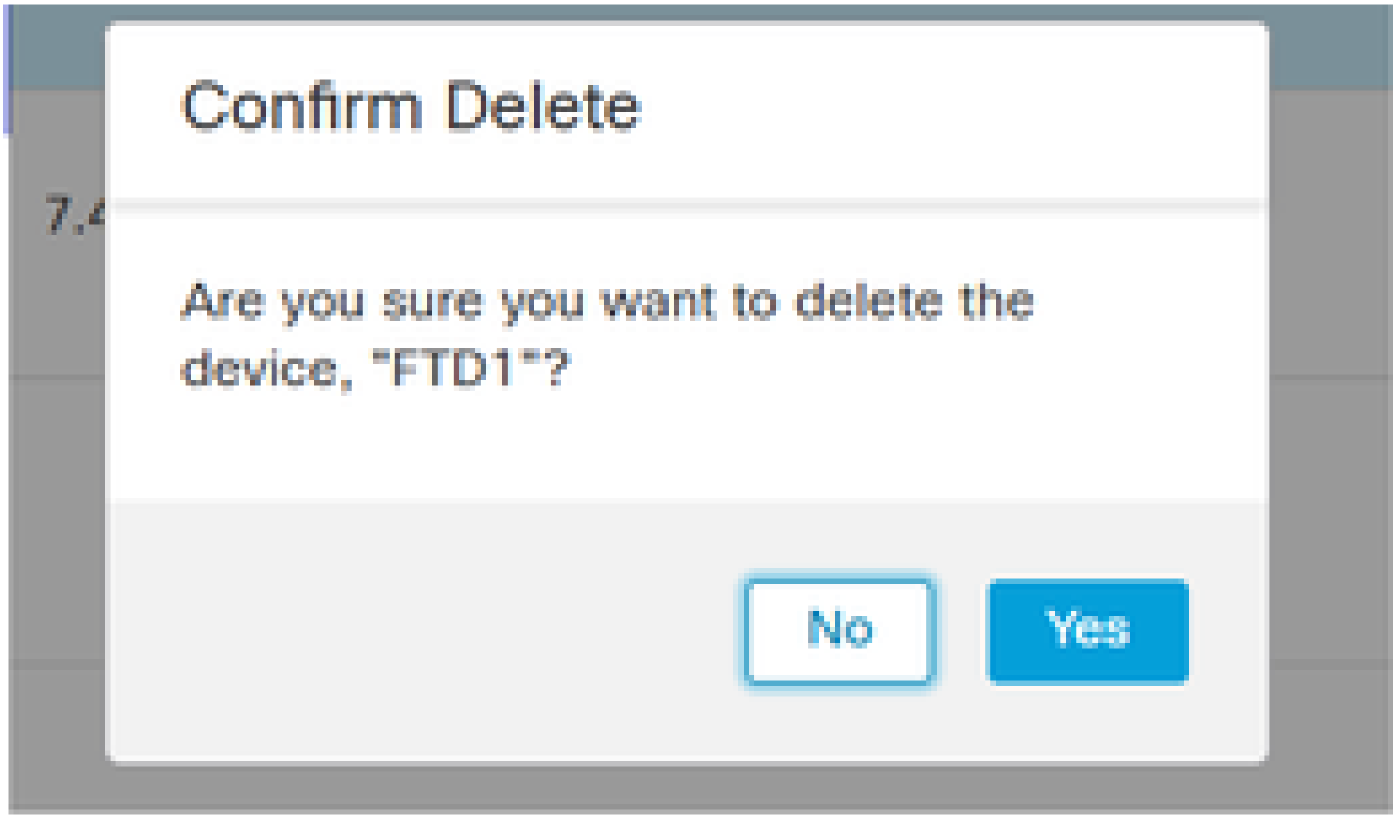
The outcome is an .sfo file, for example ObjectExport_20250306082738.sfo

Step 6. Delete/Unregister the FTD1 (ex-Primary) from the old/source FMC



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD_HA (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	
Ungrouped (1)						

Confirm the device deletion:



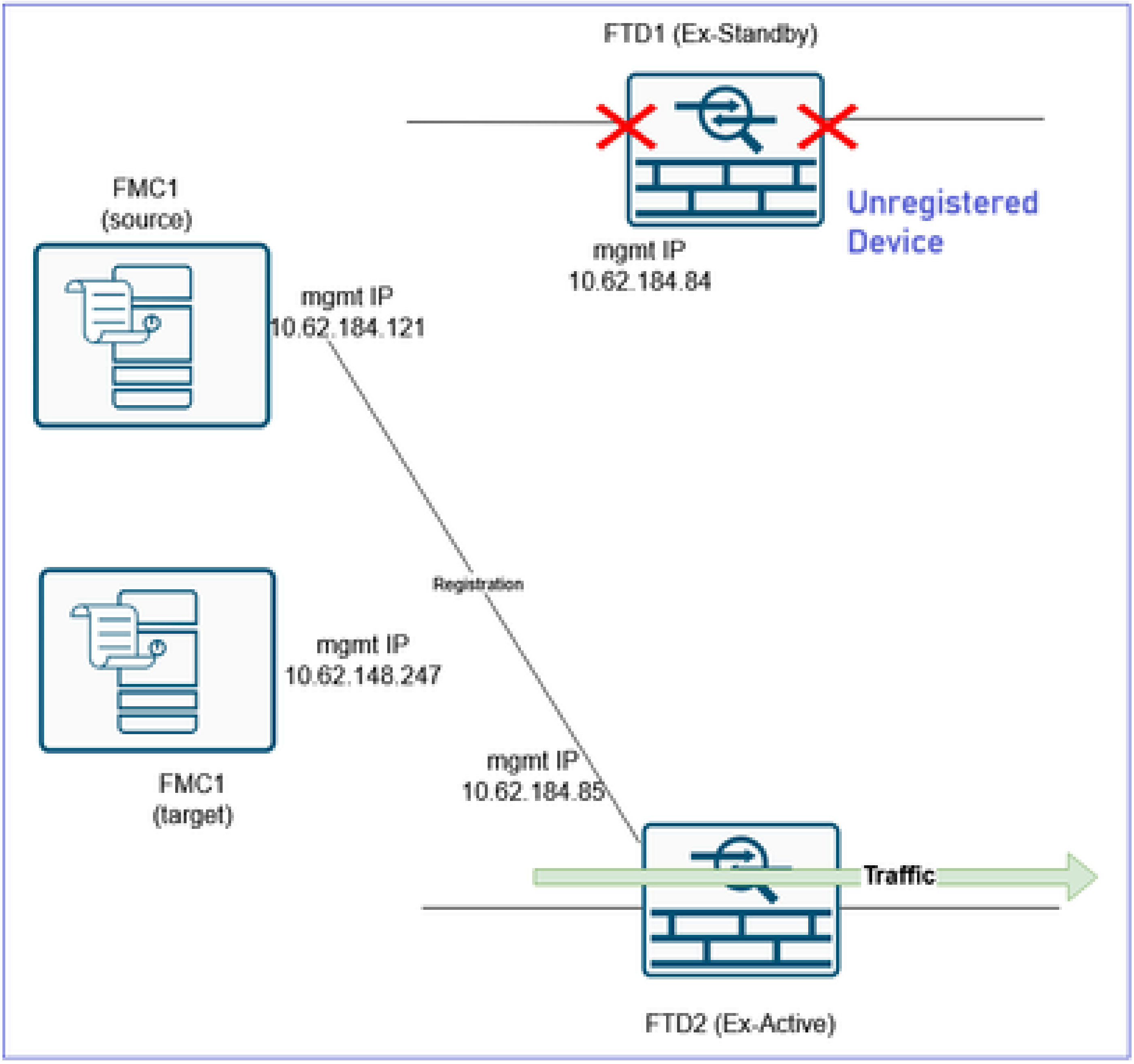
Confirm Delete

Are you sure you want to delete the device, "FTD1"?

FTD1 CLI verification:

```
<#root>
>
show managers

No managers configured.
>
```

The current status after the FTD1 device deletion:

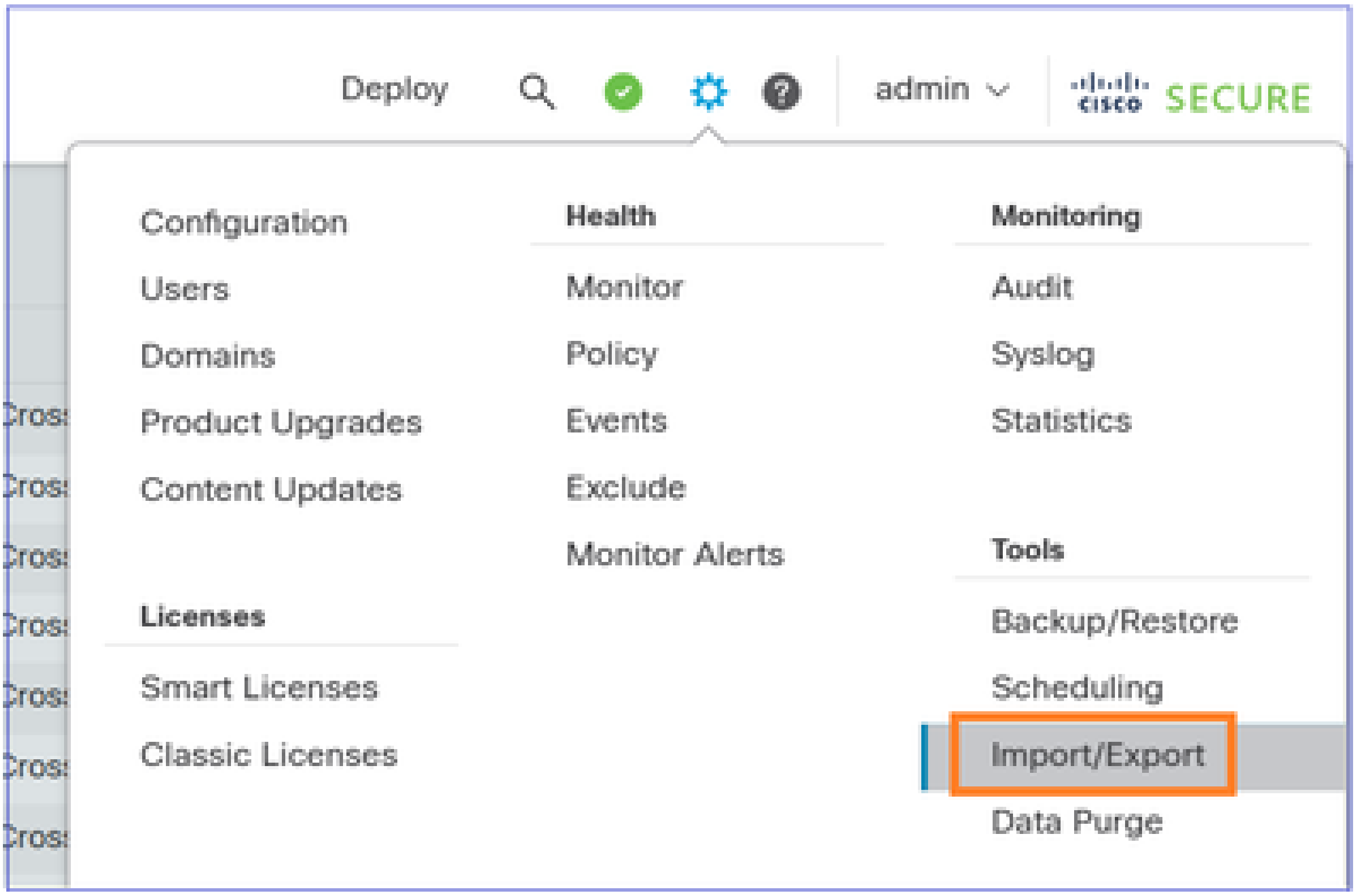


Step 7. Import the FTD Policy configuration object into the FMC2 (target FMC)

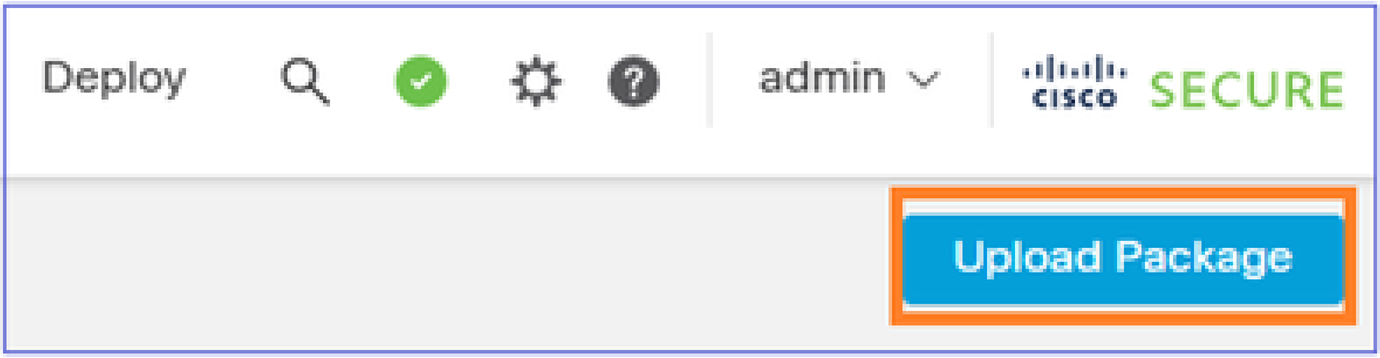
Note: The document focuses on the migration of a single FTD HA pair to a new FMC. On the other hand, if you plan to migrate multiple firewalls that share the same policies (for example, ACP, NAT) and objects and you want to do this in phases you need to consider these points.
- If you have an existing policy on the target FMC with the same name, you are asked if you:
  a. Want to replace the policy or
  b. Create a new one with a different name. This creates duplicate objects with different names (suffix _1).

- If you go with option 'b', in Step 9 ensure you reassing the newly-created objects to the migrated policies (ACP Security Zones, NAT Security Zones, Routing, Platform Settings, and so on.).

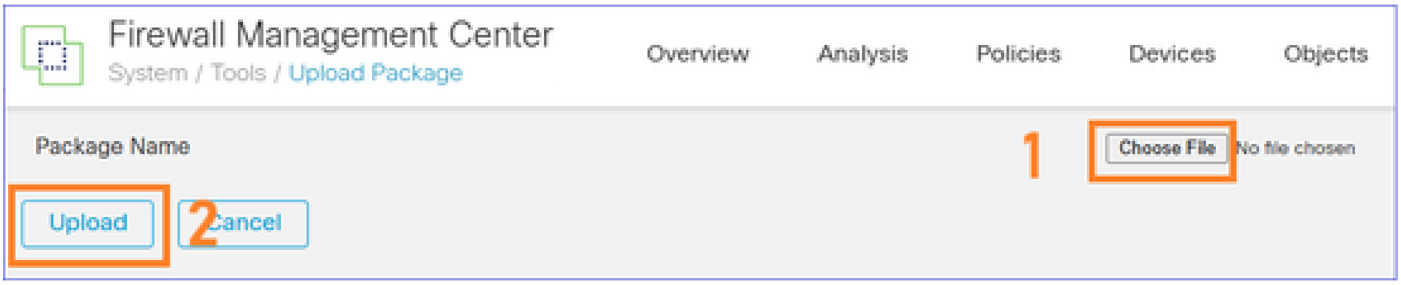
Login to the FMC2 (target FMC) and import the FTD Policies sfo object that you exported in step 5:



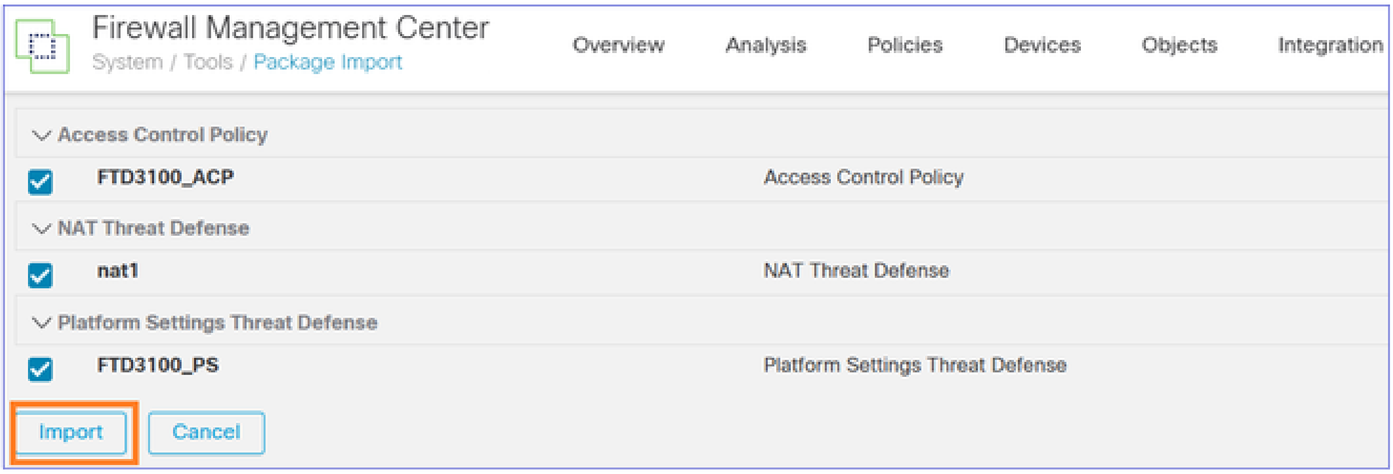
Select **Upload Packege:**



Upload the file:



Import the policies:



Access Control Policy

☑	FTD3100_ACP	Access Control Policy

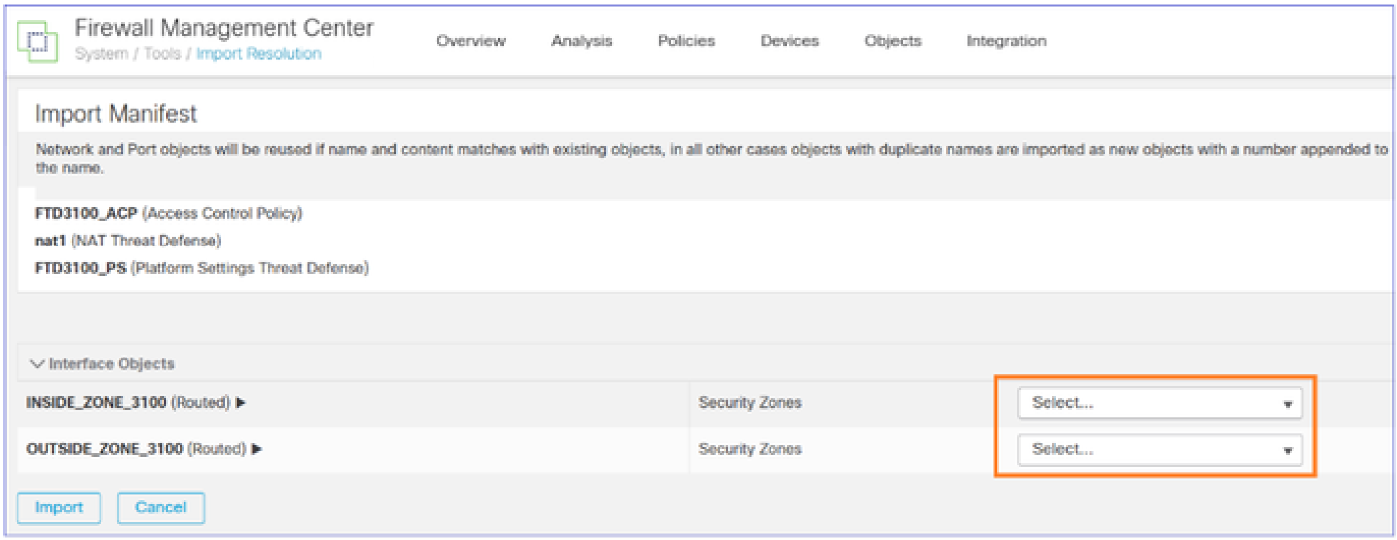
NAT Threat Defense

☑	nat1	NAT Threat Defense

Platform Settings Threat Defense

☑	FTD3100_PS	Platform Settings Threat Defense

Create the Interface Objects/Security Zones on the FMC2 (target FMC):



Import Manifest

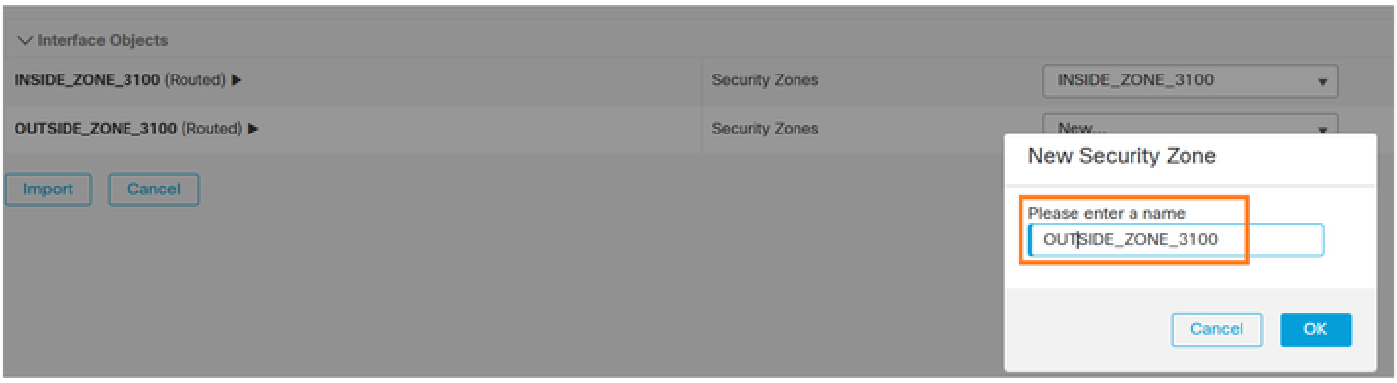
Network and Port objects will be reused if name and content matches with existing objects, in all other cases objects with duplicate names are imported as new objects with a number appended to the name.

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

Interface Objects

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

You can give the same names they had on the FMC1 (source FMC):



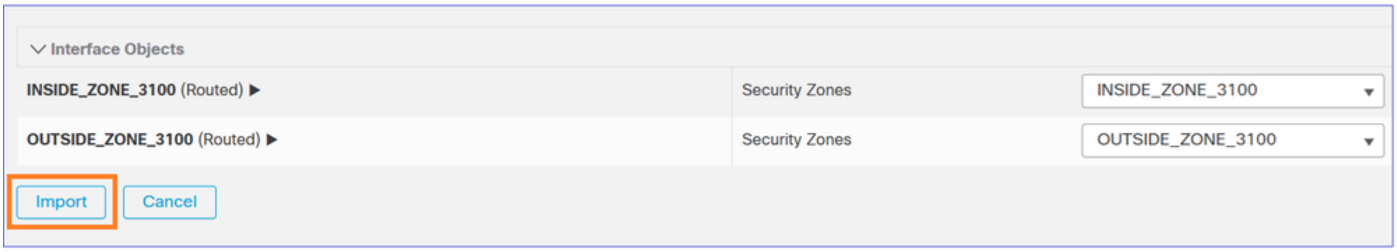
Interface Objects

INSIDE_ZONE_3100 (Routed) ▶	Security Zones	INSIDE_ZONE_3100
OUTSIDE_ZONE_3100 (Routed) ▶	Security Zones	New...

New Security Zone

Please enter a name: OUTSIDE_ZONE_3100

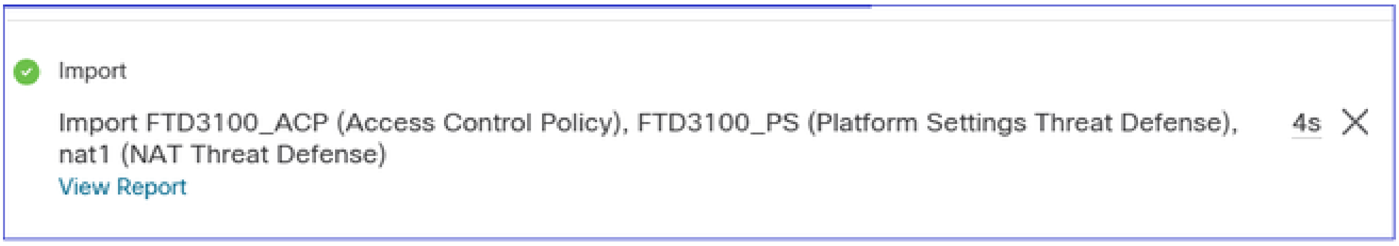
Once you select **Import,** a Task starts to import the related policies into the FMC2 (target FMC):



Interface Objects

INSIDE_ZONE_3100 (Routed) ▶	Security Zones	INSIDE_ZONE_3100
OUTSIDE_ZONE_3100 (Routed) ▶	Security Zones	OUTSIDE_ZONE_3100

The Task is done:



Import

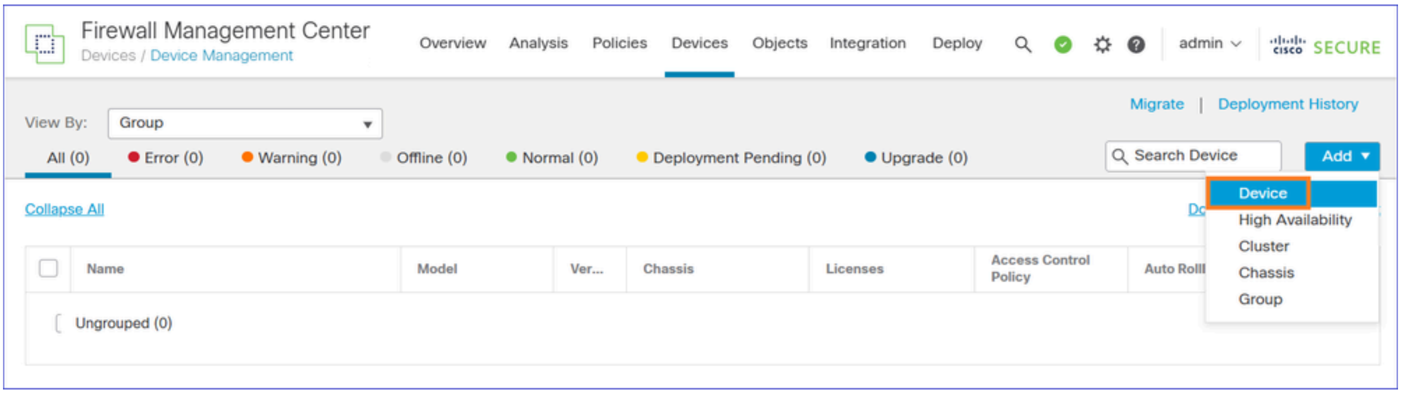
Import FTD3100_ACP (Access Control Policy), FTD3100_PS (Platform Settings Threat Defense), nat1 (NAT Threat Defense)

Step 8. Register the FTD1 (ex-Primary) into the FMC2

Go to the FTD1 (ex-Primary) CLI and configure the new manager:

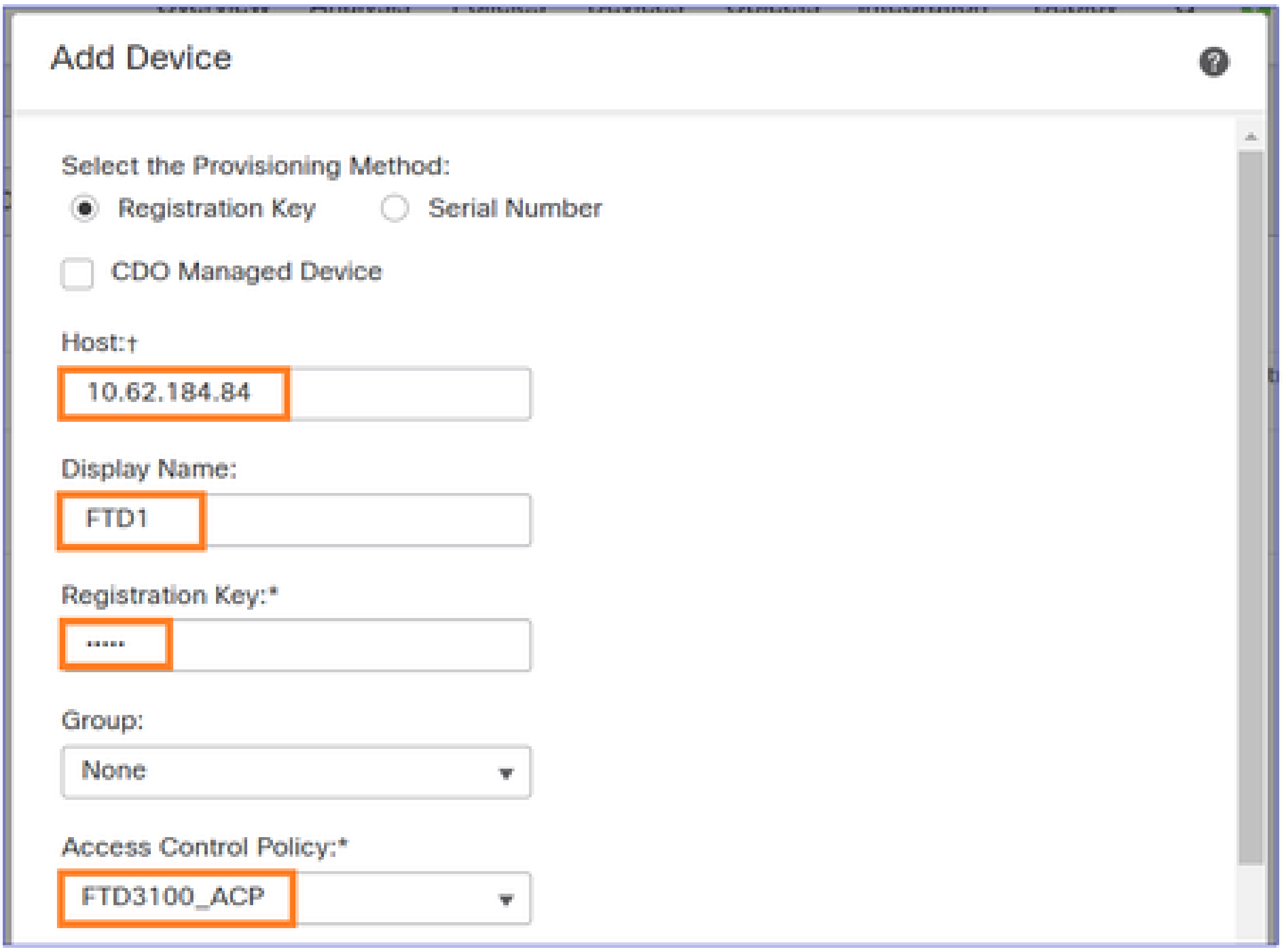
```
<#root>

>

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.

>
```

Navigate to the FMC2 (target FMC) UI **Devices** > **Device Management** and **Add** the FTD device:



If the device registration fails refer to this document to troubleshoot the problem: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

Assign the Access Control Policy you imported in the previous step:



Add Device

Select the Provisioning Method:

● Registration Key ○ Serial Number

□ CDO Managed Device

Host:†

10.62.184.84

Display Name:

FTD1

Registration Key:*

•••••

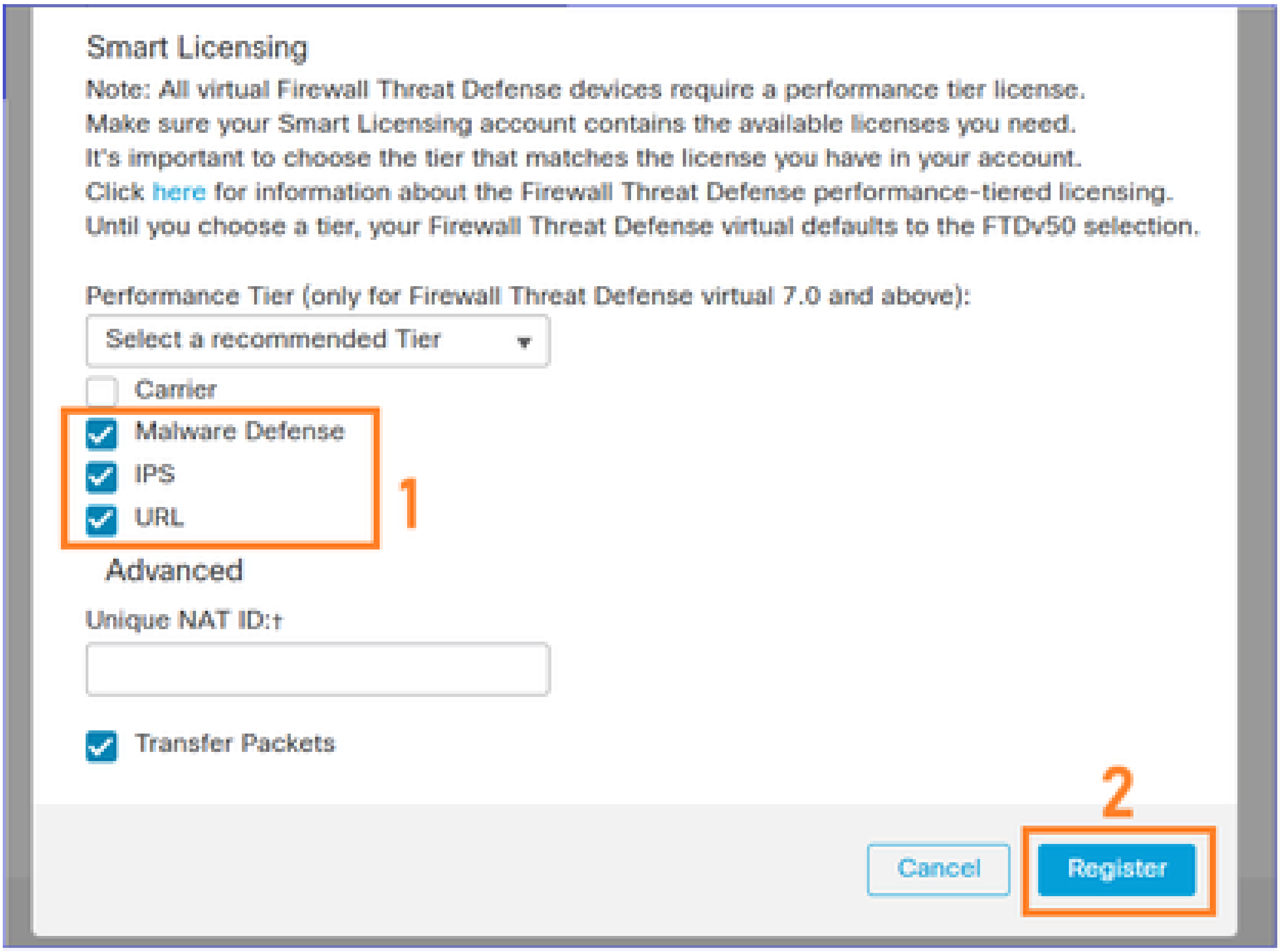
Group:

None

Access Control Policy:*

FTD3100_ACP

Apply the needed licenses and register the device:



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

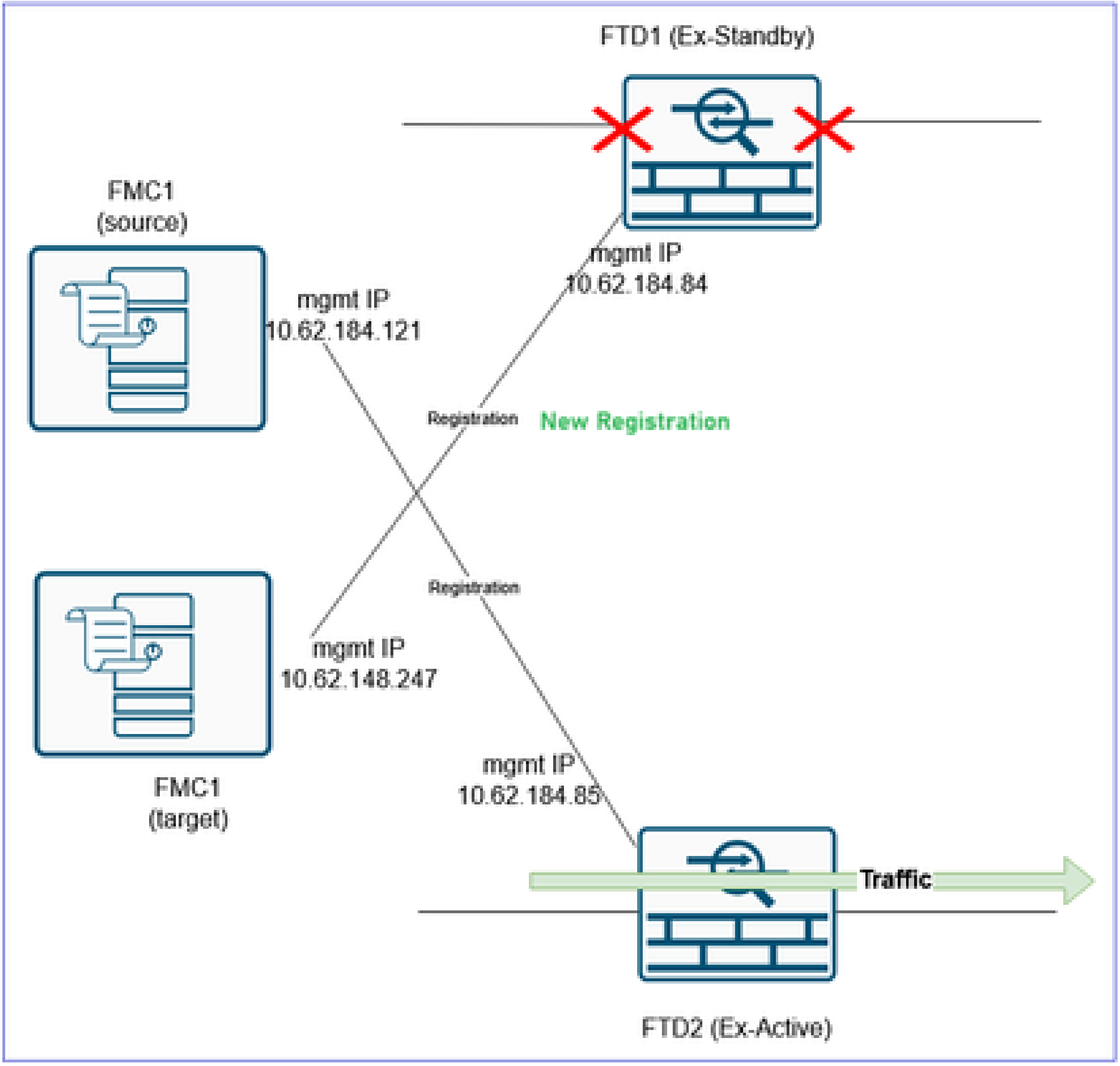
☑ URL

Advanced

Unique NAT ID:†

☑ Transfer Packets

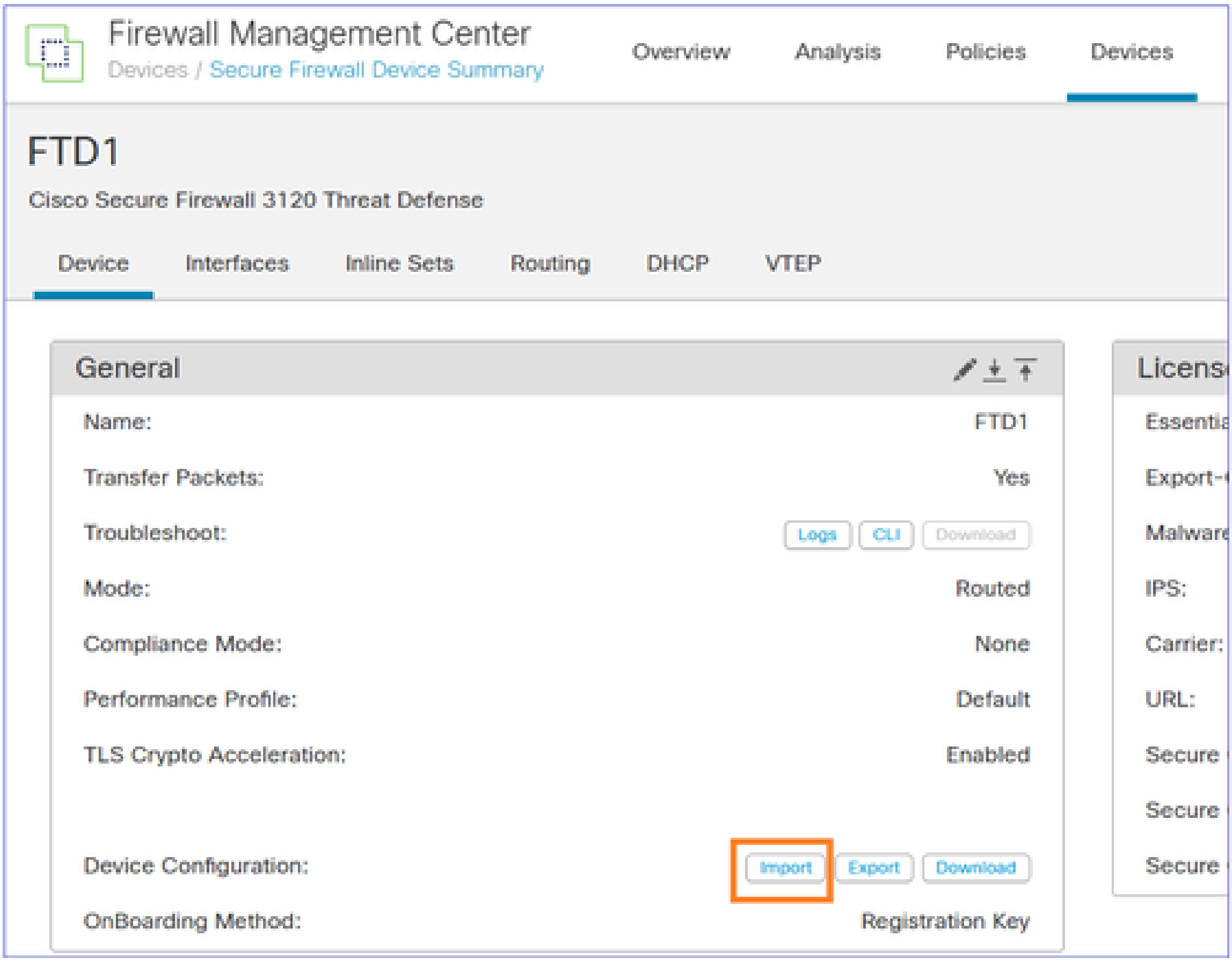
The result:



Step 9. Import the FTD Device configuration object into the FMC2 (target FMC)

Login to the FMC2 (target FMC), navigate to the **Devices** > **Device Management** and **Edit** the FTD device that you registered in the previous step.

Navigate to the **Device** tab and **Import** the FTD Policies sfo object that you exported in step 2:



Firewall Management Center

Devices / Secure Firewall Device Summary

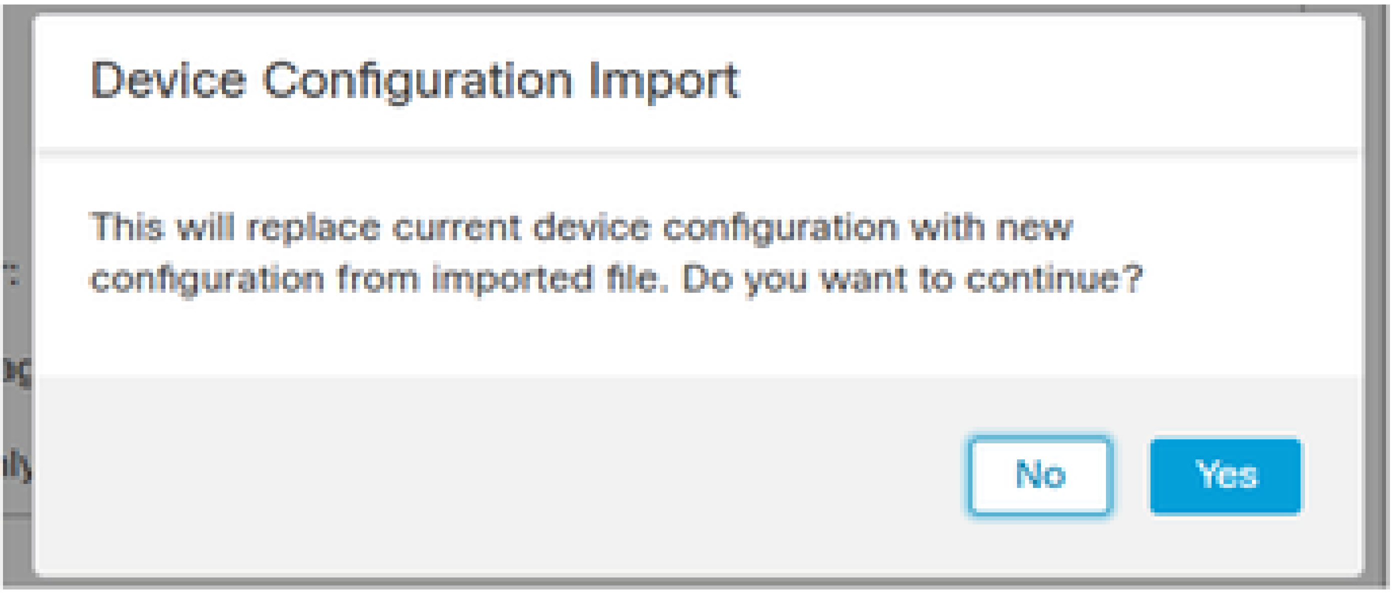
FTD1

Cisco Secure Firewall 3120 Threat Defense

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

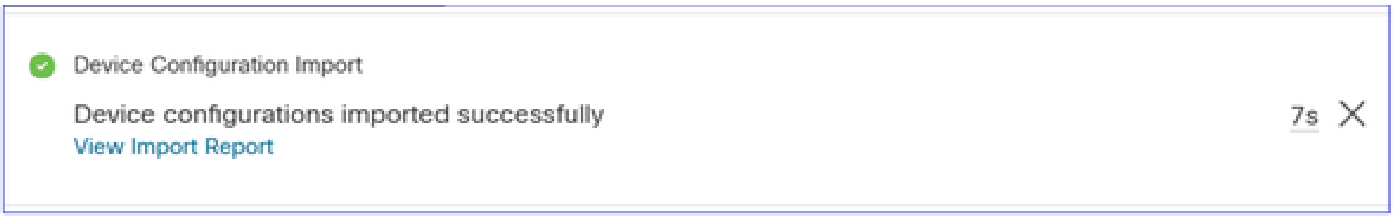
Note: In case in Step 7 you went with option 'b' (Create a new policy), ensure you reassing the newly-created objects to the migrated policies (ACP Security Zones, NAT Security Zones, Routing, Platform Settings, and so on.).



Device Configuration Import

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

An FMC task is initiated.

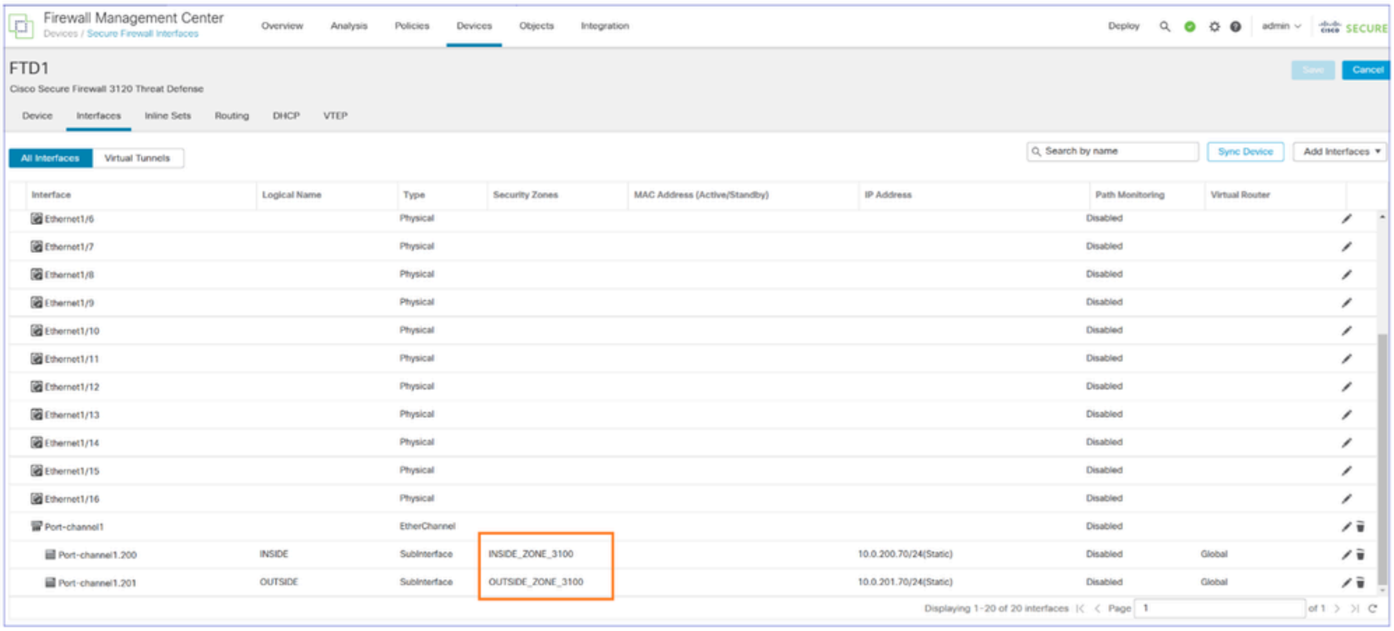


Device Configuration Import

Device configurations imported successfully

View Import Report

The device configuration is applied on the FTD1, for example, Security Zones, ACP, NAT, and so on:



FTD1

Cisco Secure Firewall 3120 Threat Defense

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

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

⚠ **Caution**: If you have an ACP that expands to many Access Control Elements, the ACP compilation process (tmatch compile) can take time several minutes to complete. You can use this command to verify the ACP compilation status:

<#root>

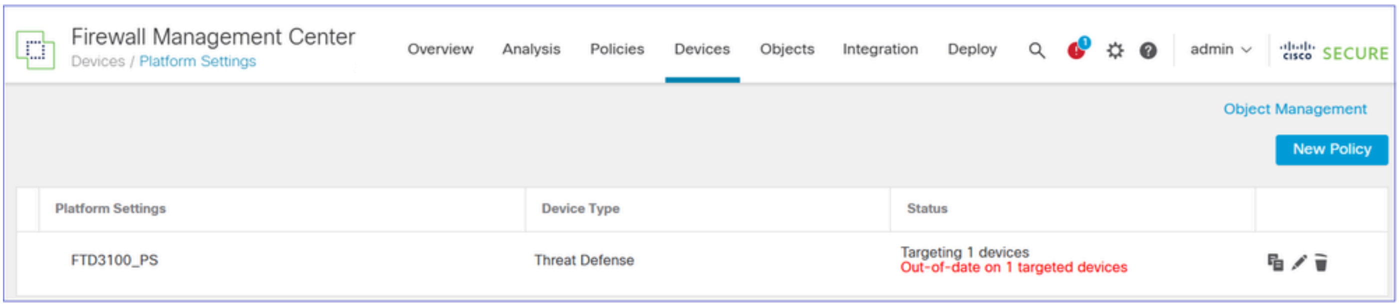
```
FTD3100-3#

show asp rule-engine


Rule compilation Status:

Completed
```

Step 10. Finish the FTD Configuration

At this point the goal is the configure all the features that can be still missing from FTD1 after the registration to the FMC2 (target FMC) and the import of the Device policy.

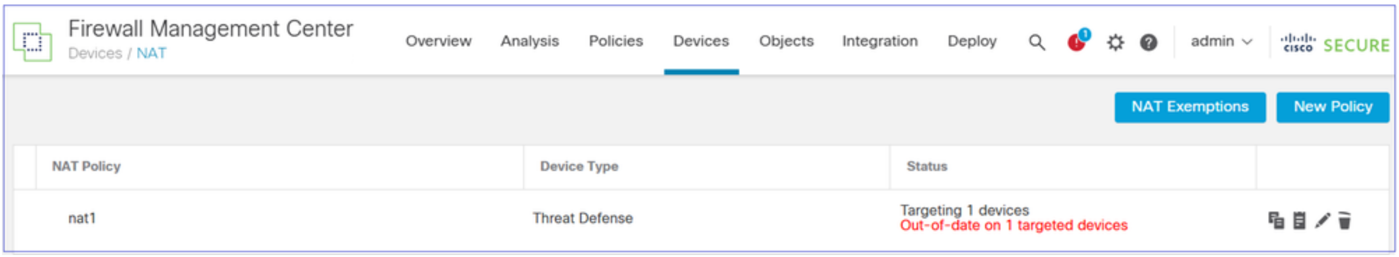
Ensure that policies like NAT, Platform Settings, QoS, and so on. are assigned to the FTD. You see that the policies are assigned but pending deployment.

For example, Platform Settings are imported and assigned to the device, but pending the deployment:



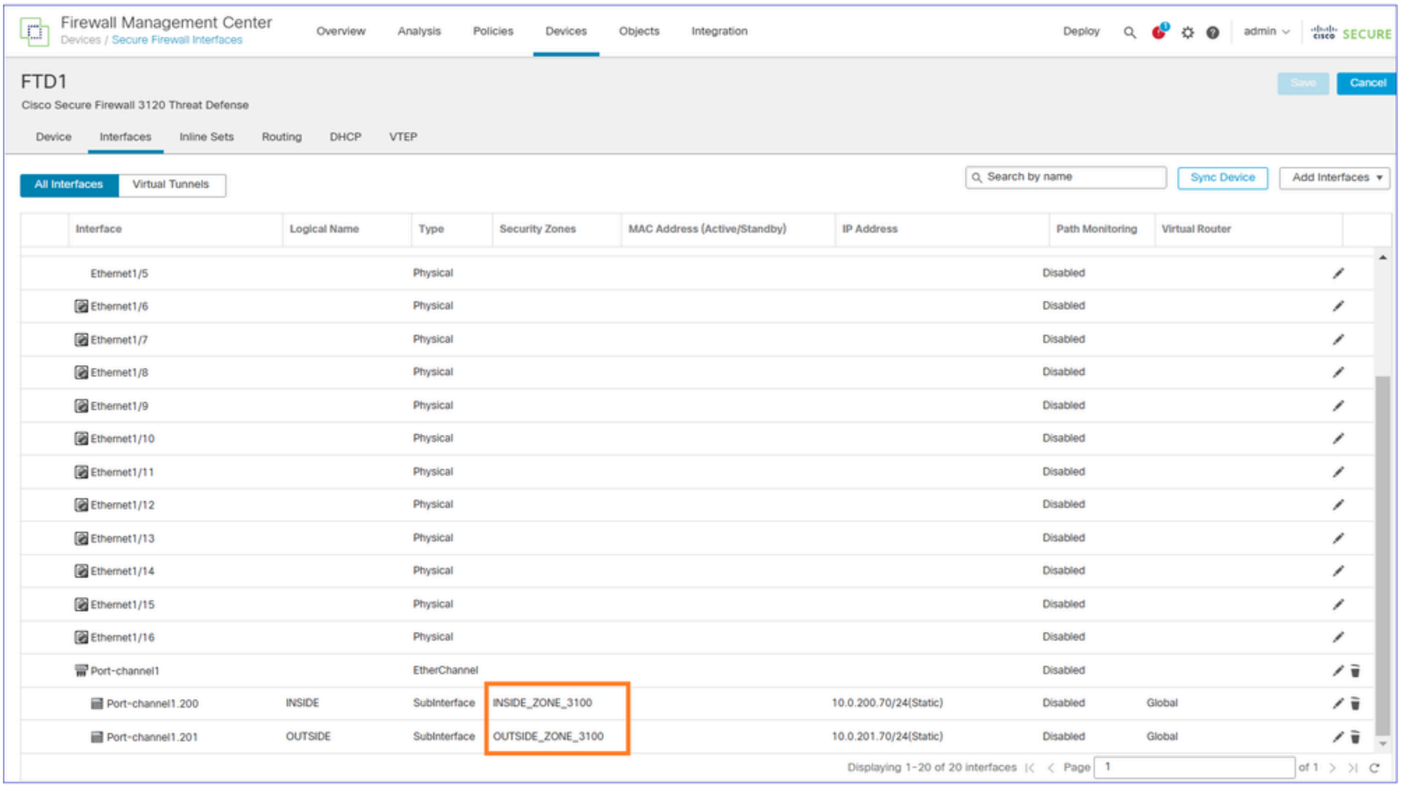
Platform Settings	Device Type	Status
FTD3100_PS	Threat Defense	Targeting 1 devices Out-of-date on 1 targeted devices

If NAT is configured, the NAT policy is imported and assigned to the device, but pending the deployment:



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

Security Zones are applied to the interfaces:



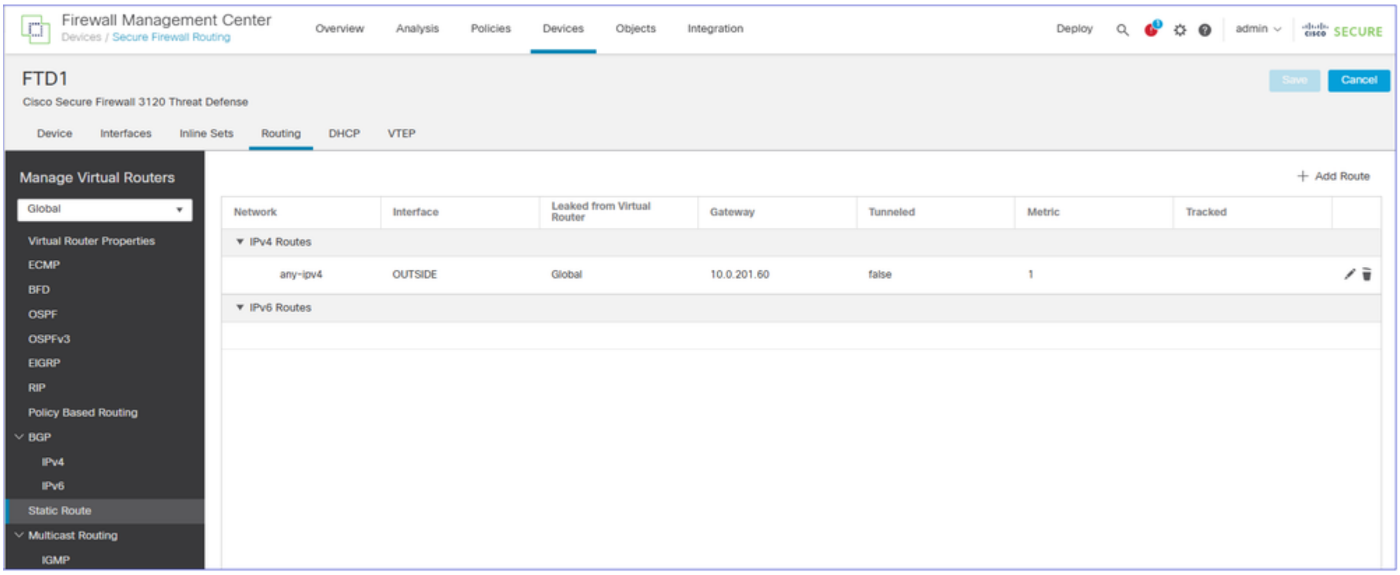
FTD1

Cisco Secure Firewall 3120 Threat Defense

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

Routing configuration is applied to the FTD device:

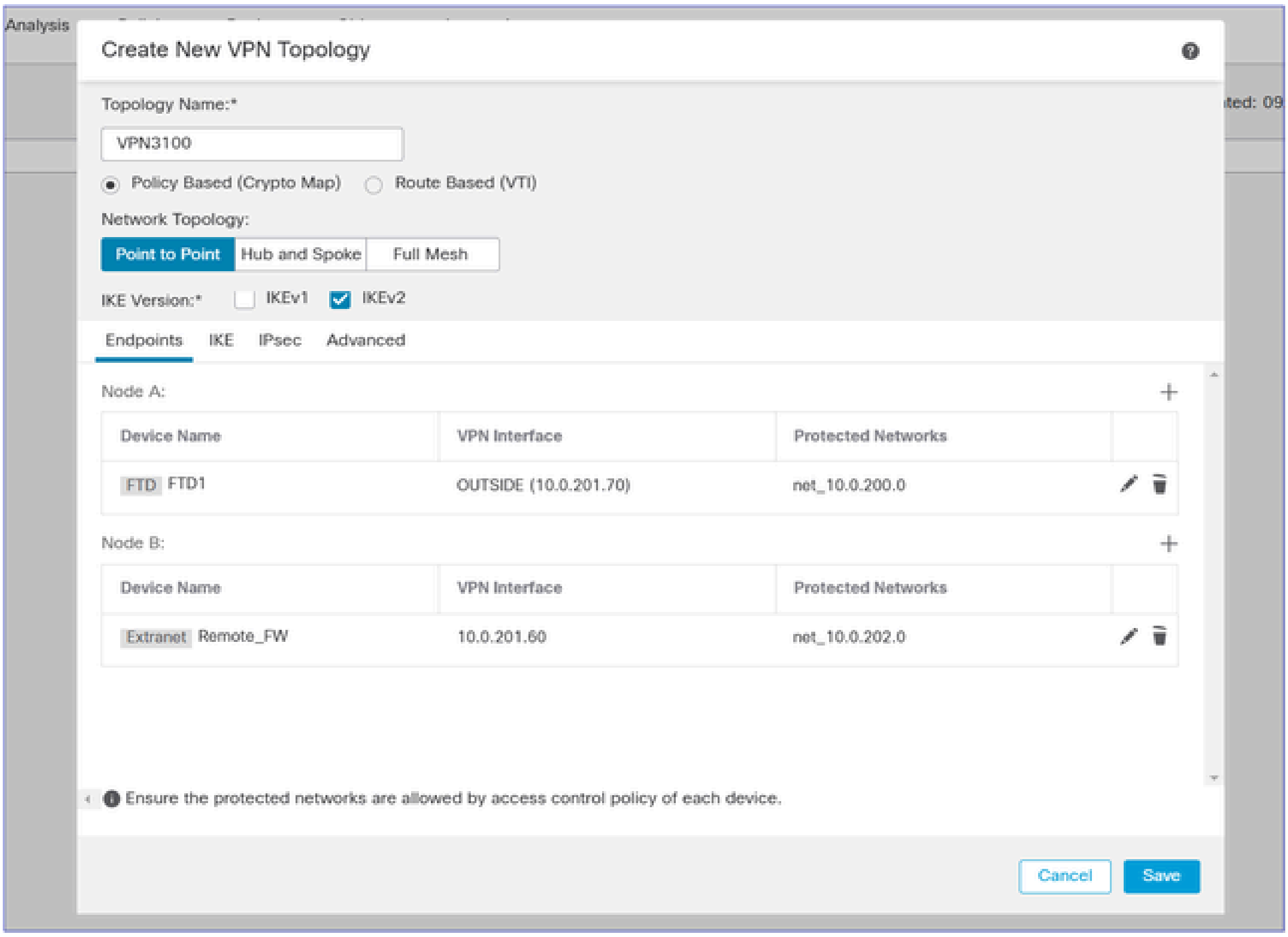


FTD1

Cisco Secure Firewall 3120 Threat Defense

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

Note: Now is the time to configure the policies that could not be migrated automatically (for example, VPNs).



Topology Name:* VPN3100

● Policy Based (Crypto Map) ○ Route Based (VTI)

IKE Version:* □ IKEv1 ☑ IKEv2

Node A:

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

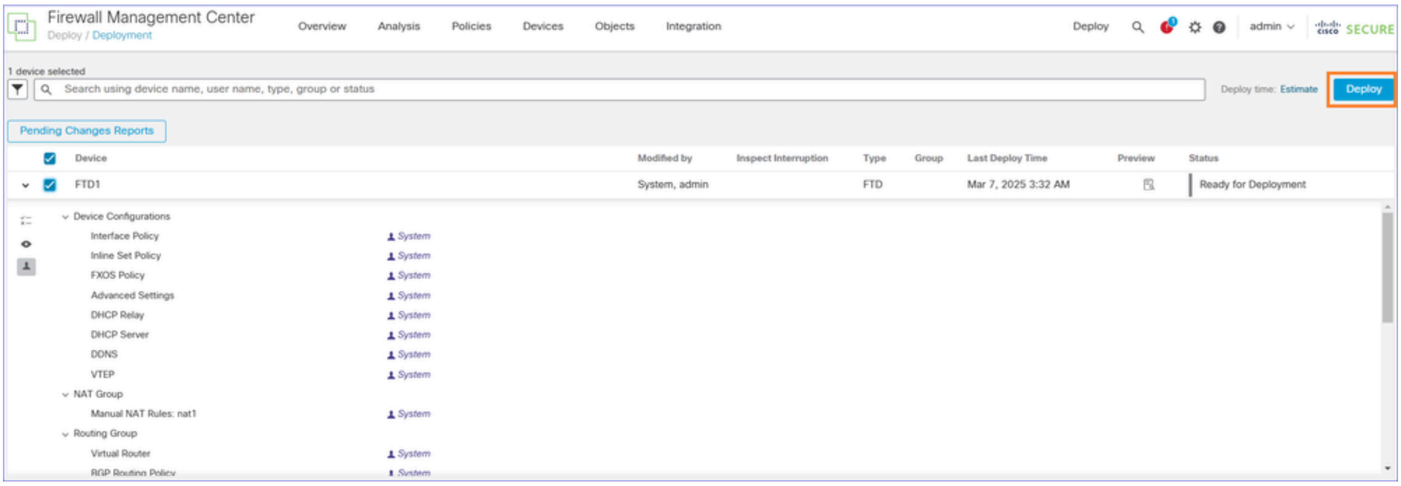
Node B:

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.

Note: If the FTD that is migrated has S2S VPN peers that are also migrated to the target FMC, you have to configure the VPN after moving all FTDs to the target FMC.

Deploy the pending changes:



	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
☑	FTD1	System, admin		FTD		Mar 7, 2025 3:32 AM		Ready for Deployment

Device Configurations	
Interface Policy	System
Inline Set Policy	System
FXOS Policy	System
Advanced Settings	System
DHCP Relay	System
DHCP Server	System
DDNS	System
VTEP	System
NAT Group	
Manual NAT Rules: nat1	System
Routing Group	
Virtual Router	System
BGP Routing Policy	System

Step 11. Verify the deployed FTD Configuration

At this point the goal is to check from the FTD CLI that all the configuration is in place.

The suggestion is to compare the ‘show running-config’ output from both FTDs. You can use tools like WinMerge or diff for the comparison.

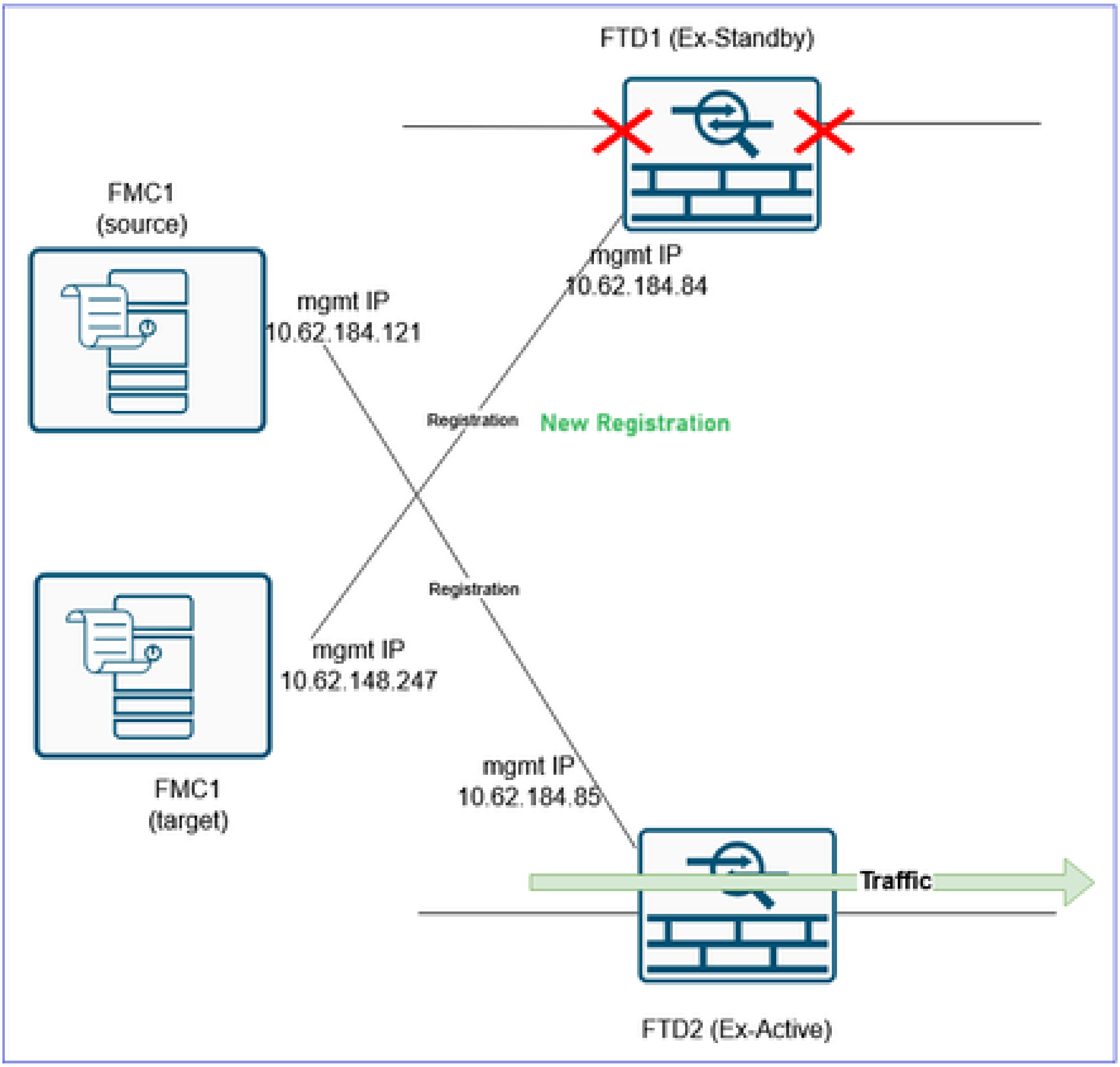
Differences that you see and are normal are:

- Device Serial Number
- Interface descriptions
- ACL rule-ids
- Configuration Cryptochecksum

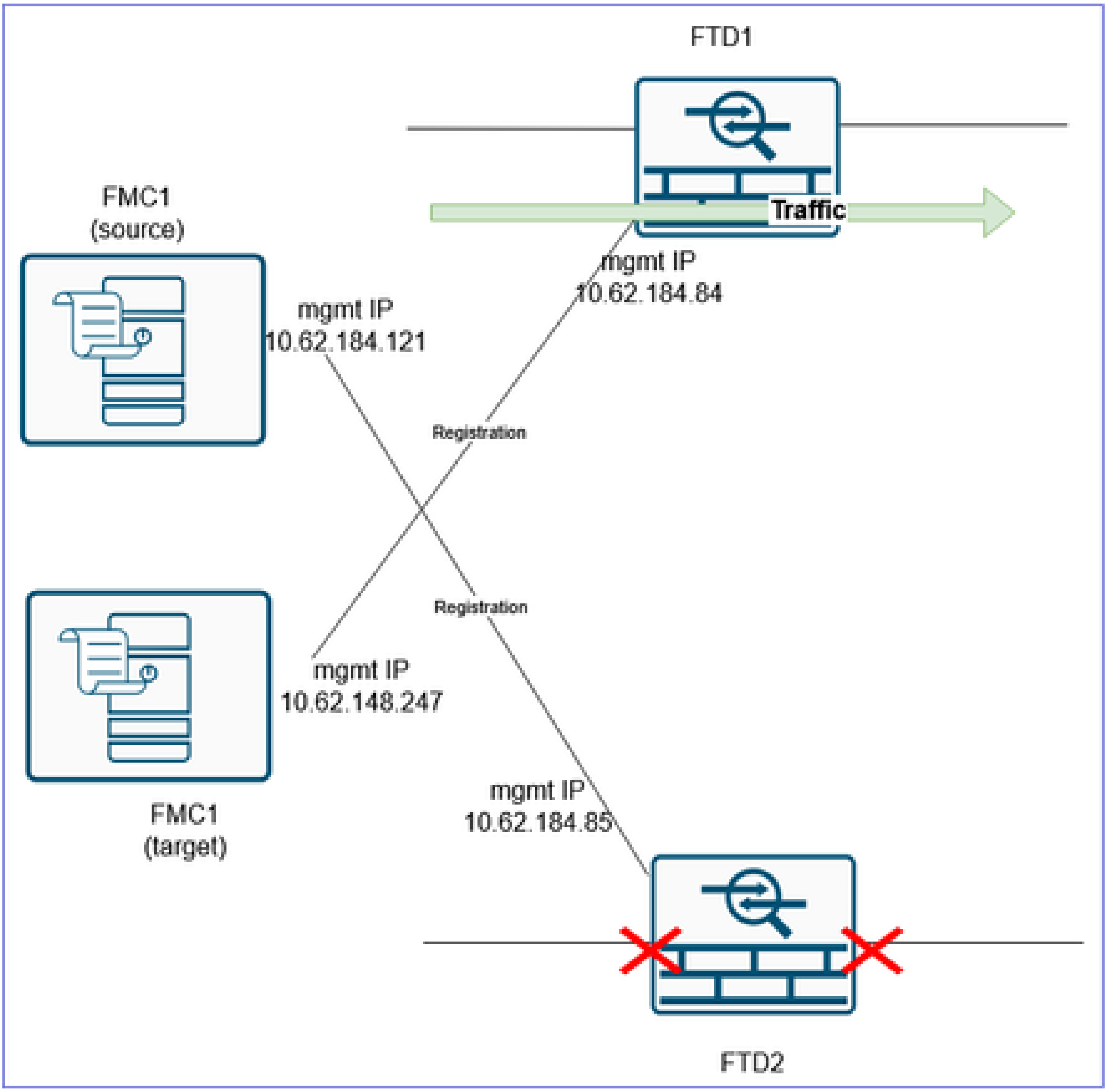
Step 12. Do the Cutover

At this step the goal is to switch the traffic from the FTD2 that is currently handling the traffic and is still registered to the old/source FMC, to the FTD1 that is registered to the target FMC.

Before:


FTD1 (Ex-Standby)
FMC1
(source)
mgmt IP
10.62.184.84
mgmt IP
10.62.184.121
Registration
New Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
Traffic
FTD2 (Ex-Active)

After:



⚠ **Caution**: Arrange a MW to do the cutover. During the cutover you are going to have some traffic interruption until all the traffic is diverted to the FTD1, VPNs are re-established, and so on.

⚠ **Caution**: Do not initiate the cutover unless the ACP compilation is completed (see step 10 above).

⚠ **Warning**: Make sure you either disconnect the data cables from the FTD2 or shutdown the related switchports. Otherwise, you can end-up with both devices handling the traffic!

⚠ **Caution**: Since both devices use the same IP configuration there is a need for the ARP cache of the adjacent L3 devices to be updated. Consider clearing manually the ARP cache of the adjacent devices to expedite the traffic cutover.

Tip: You can also send a GARP packet and update the ARP cache of the adjacent devices using the FTD CLI command:

<#root>

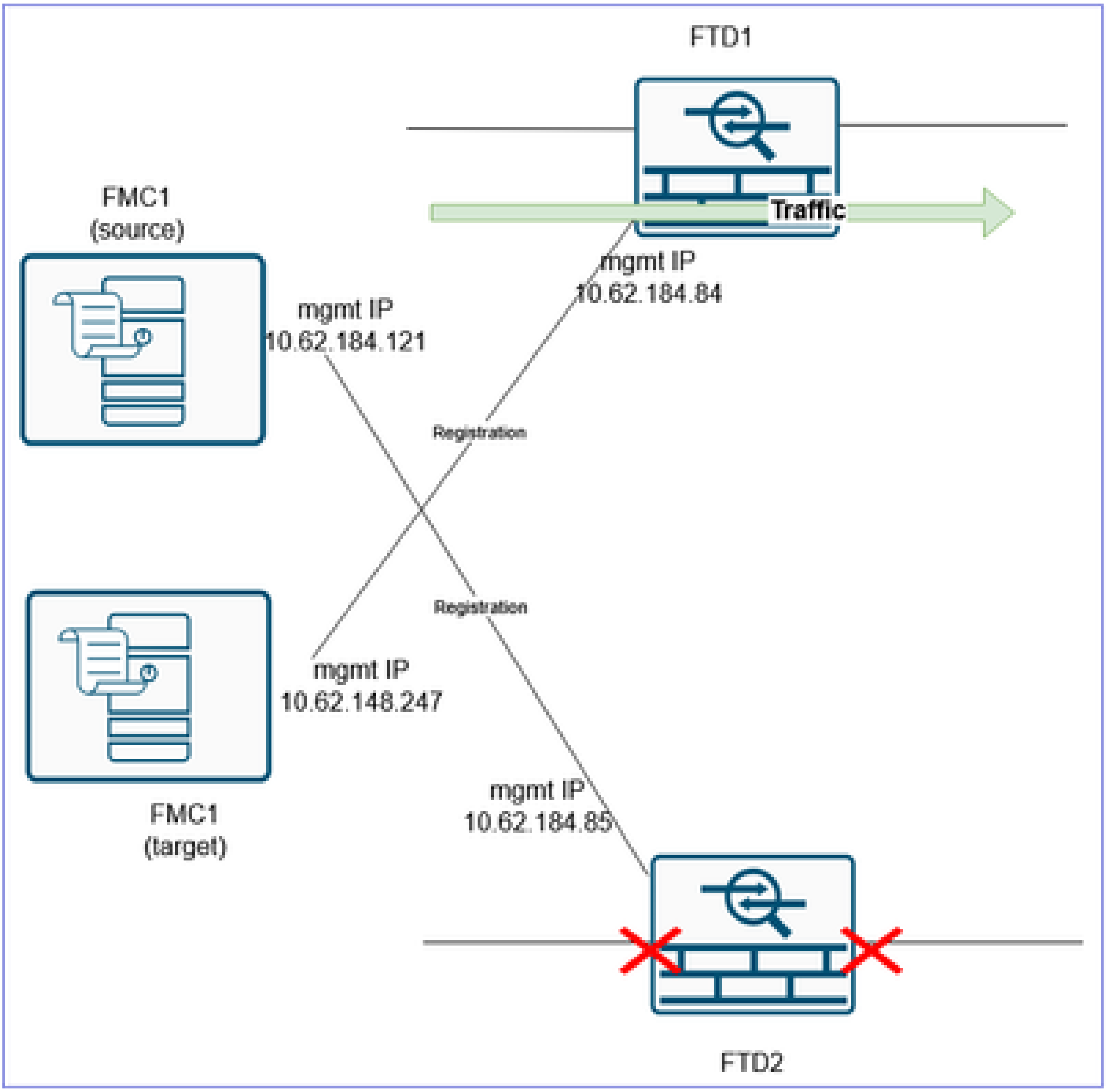
```
FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

You have to repeat this command for every IP the FW owns. Thus, it can be faster to just clear the ARP cache of the adjacent devices than sending GARP packets for every IP the firewall owns.

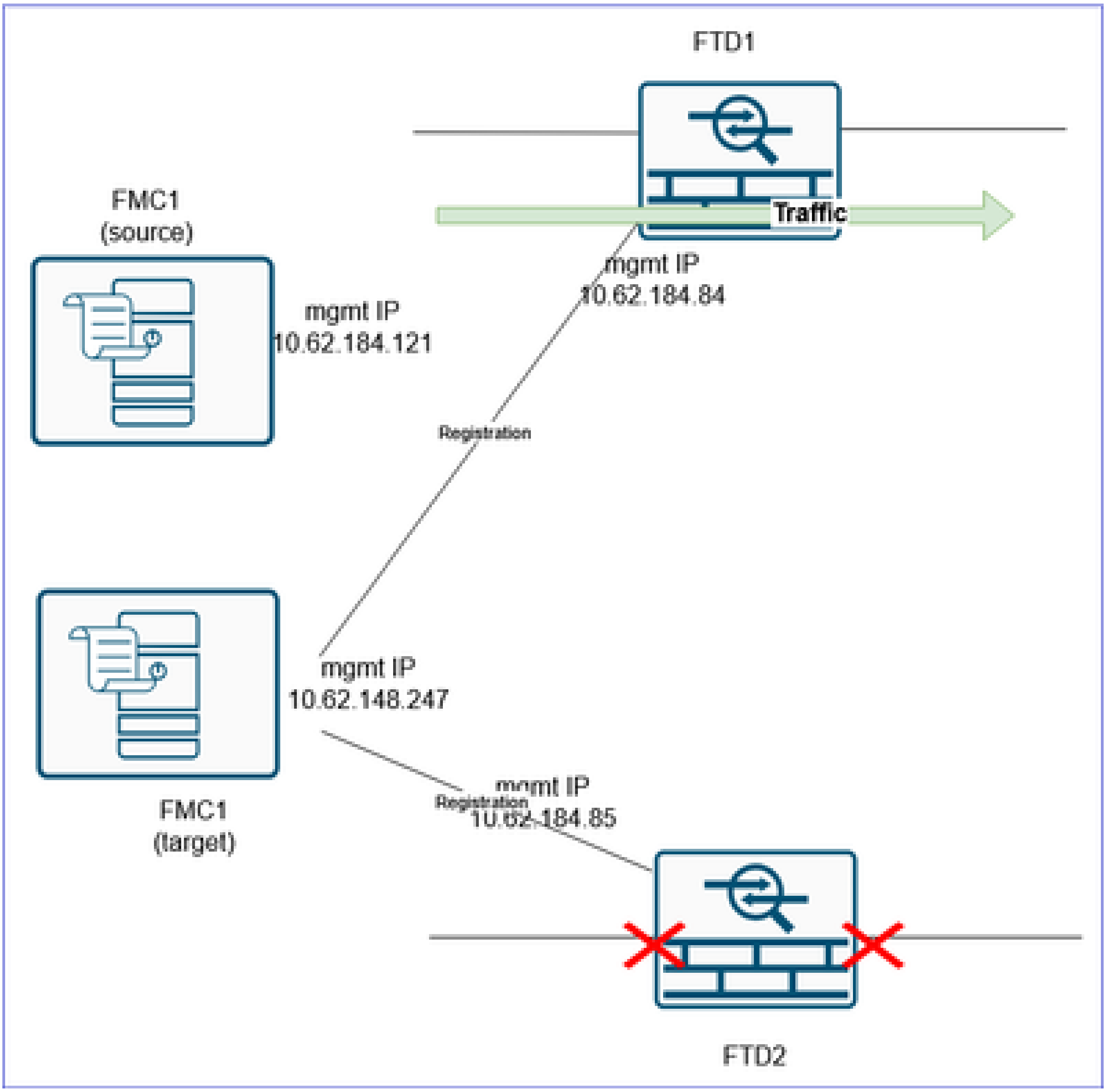
Step 13. Migrate the second FTD to the FMC2 (target FMC)

The last item is to reform the HA pair. To do this, you first need to delete the FTD2 from the FMC1 (source FMC) and register it to the FMC2 (target FMC).

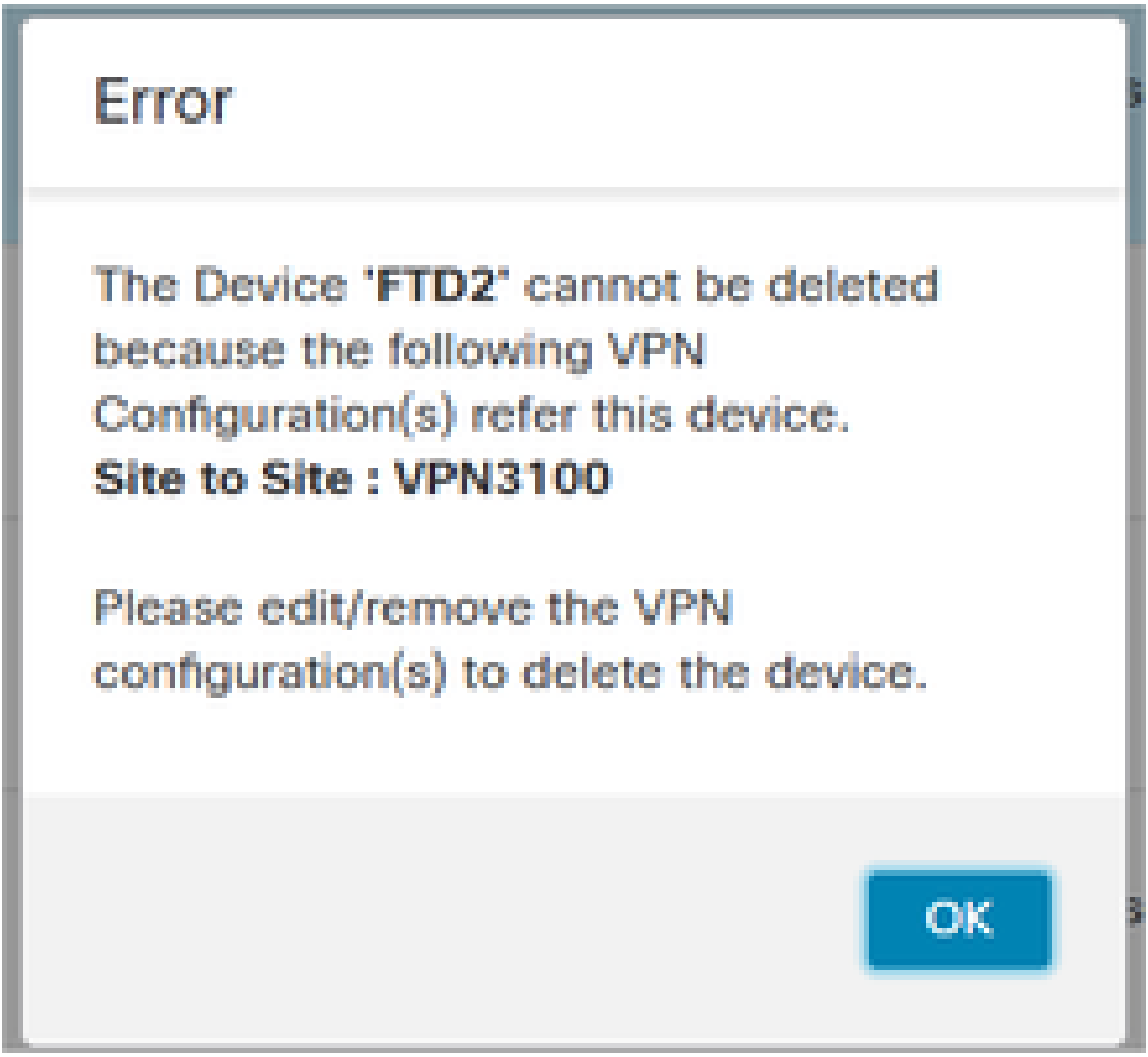
Before:


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

After:



If you have a VPN configuration attached to the FTD2, you have to remove it first before deleting the FTD. In different case, a message similar to this is shown:



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.

CLI verification:

```
<#root>

>

show managers


No managers configured.
```

It is a good practice to wipe-out all the FTD configuration before registering it to the target FMC. A quick way to do this is to switch between the firewall modes.

For example if you have routed mode, switch to transparent and then back to routed:

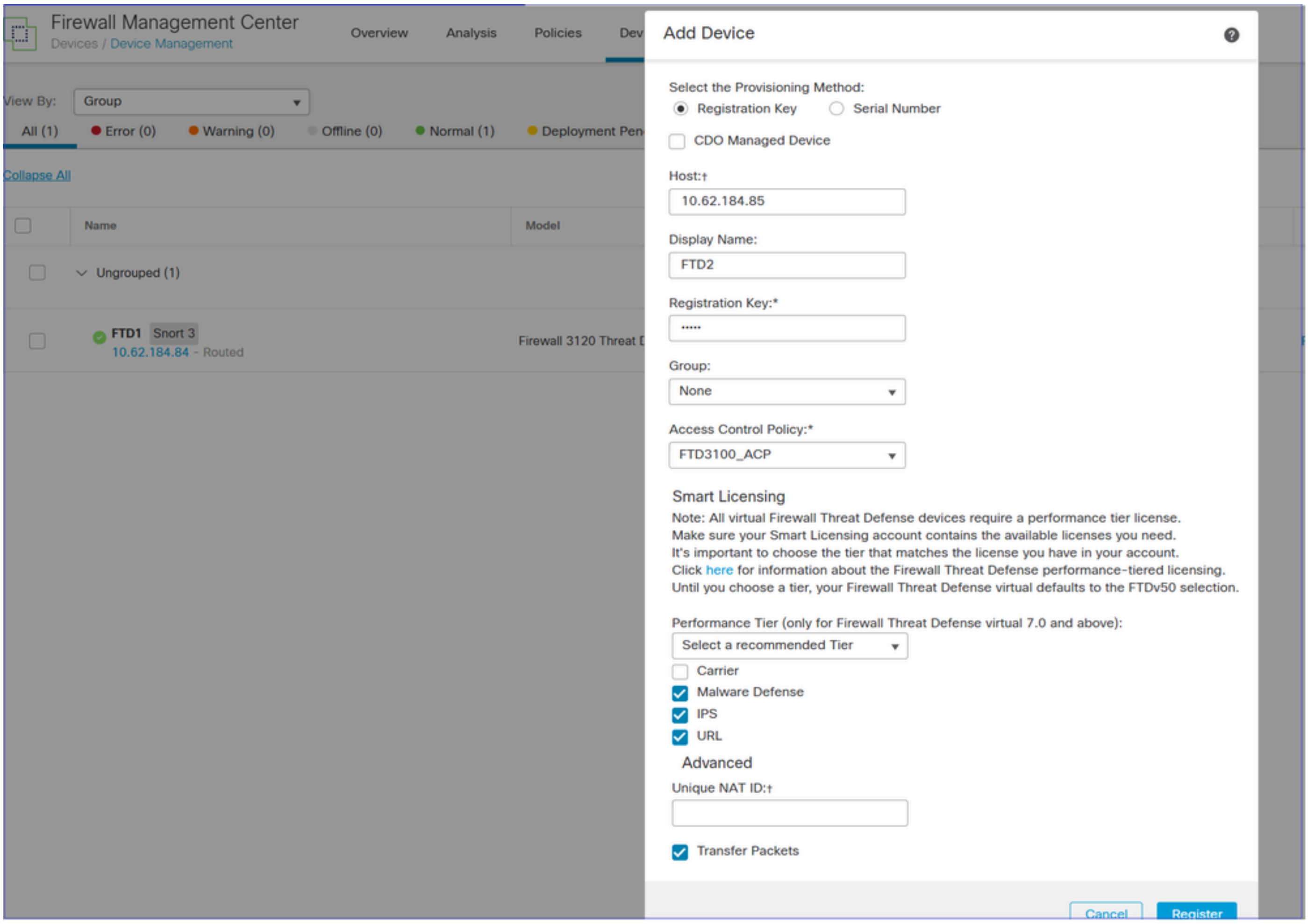
```
<#root>

>

configure firewall transparent
```

And then:

```
<#root>

>

configure firewall routed
```

Then, register it to the FMC2 (target 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.
>
```



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

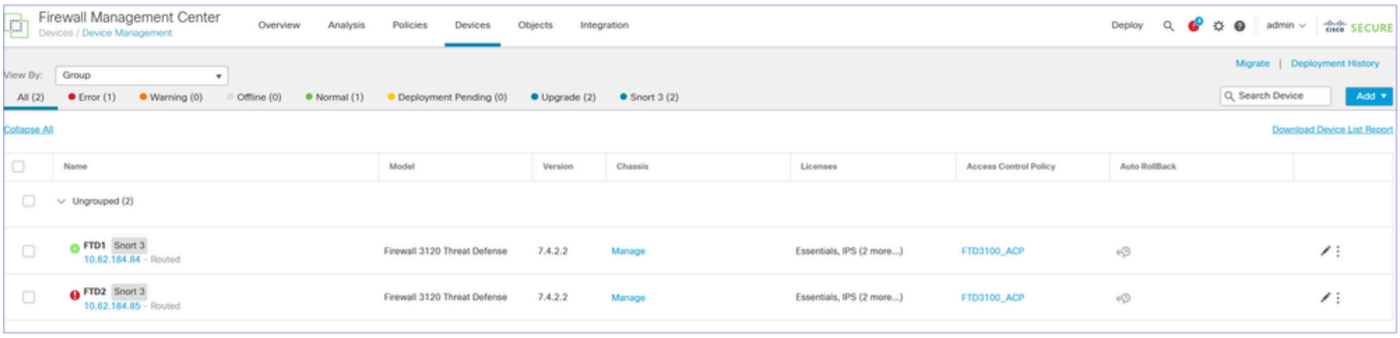
□ Carrier
☑ Malware Defense
☑ IPS
☑ URL

Advanced

Unique NAT ID:†

☑ Transfer Packets

The result:



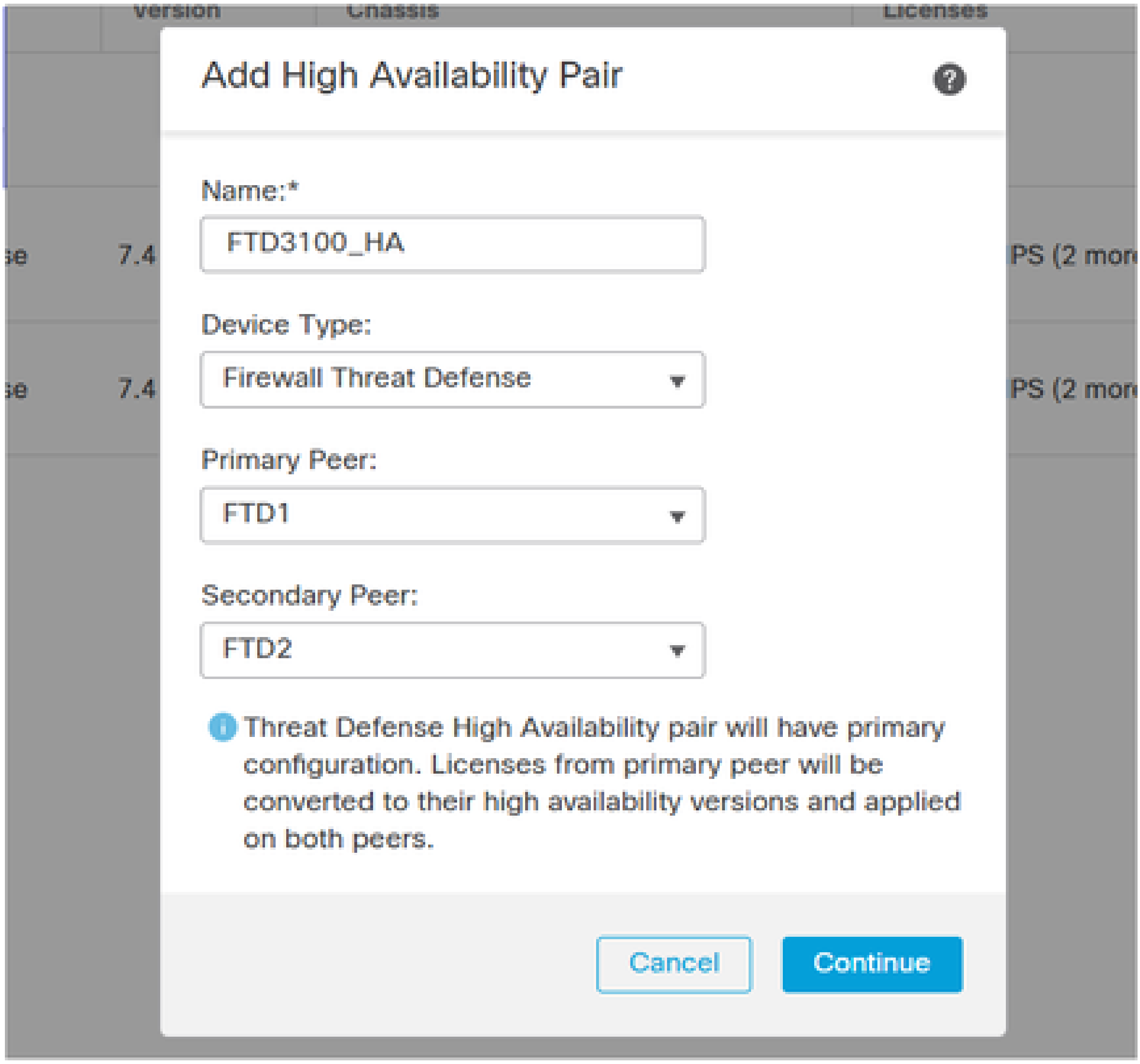
□	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
□	Ungrouped (2)							
□	FTD1 Snort 3 10.62.184.84 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP		
□	FTD2 Snort 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage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

Step 14. Re-form the FTD HA

Note: This task (as any HA-related task) must also be performed during a MW. During the HA negotiation there is going to be a traffic outage for ~1 minute since the data interfaces go down.

On the target FMC navigate to **Devices > Device Management** and **Add > High Availability**.

⚠ **Caution**: Ensure that you select as Primary Peer the FTD that is handling the traffic (FTD1 in this scenario):



Add High Availability Pair

Name:* FTD3100_HA

Device Type: Firewall Threat Defense

Primary Peer: FTD1

Secondary Peer: FTD2

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.

Reconfigure the HA settings including Monitored Interfaces, Standby IPs, virtual MAC addresses, and so on.

Verification from FTD1 CLI:

<#root>

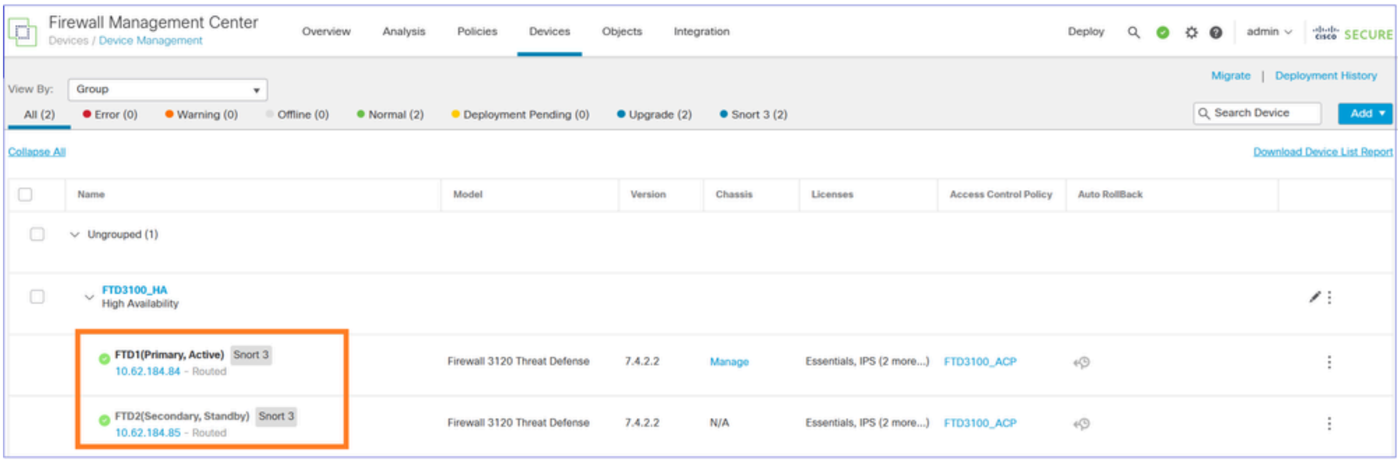
```
FTD3100-3#

show failover | include host


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

Verification from FTD2 CLI:

<#root>

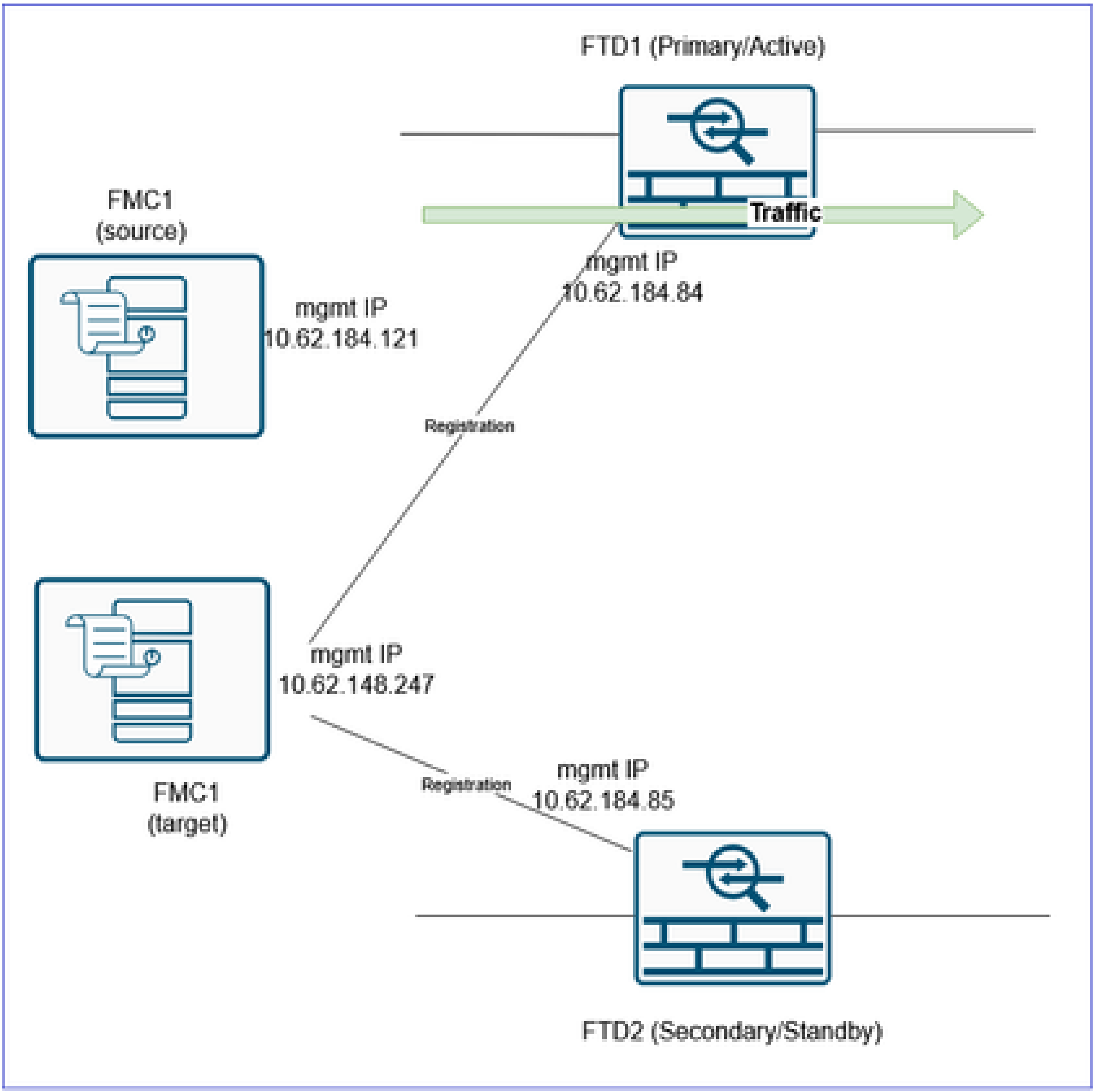
```
FTD3100-3#

show failover | include host


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

FMC UI verification:



□	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	

Finally, **bring up/reconnect the data interfaces** of the FTD2 device.



References

- Export and Import the Device Configuration
- Add a High Availability Pair
- Migrate an FTD from One FMC to another FMC