

FTD HAの別のFMCへの移行 (フェールオーバー)

内容

はじめに

略語

前提条件

使用するコンポーネント

トポロジ

設定

ステップ 1 : プライマリファイアウォールからのデバイス設定のエクスポート

ステップ 2 : セカンダリFTDをアクティブにする

ステップ 3 : FTD HAの解除

ステップ 4 : FTD1 (元プライマリ) データインターフェイスを分離します。

ステップ 5 : FTD共有ポリシーのエクスポート

手順 6 : 旧/ソースFMCからFTD1(ex-Primary)を削除/登録解除します。

手順 7 : FMC2 (ターゲットFMC) へのFTDポリシー設定オブジェクトのインポート

ステップ 8 : FTD1(ex-Primary)をFMC2に登録します。

ステップ 9 : FTDデバイス設定オブジェクトをFMC2 (ターゲットFMC) にインポートします。

ステップ 10 : FTD設定の終了

ステップ 11展開されたFTD設定の確認

ステップ 12カットオーバーの実行

ステップ 132番目のFTDをFMC2 (ターゲットFMC) に移行します。

ステップ 14 : FTD HAを再構築します。

参考資料

はじめに

このドキュメントでは、既存のFMCから別のFMCにFTD HAを移行する手順について説明します。

スタンドアロンのファイアウォールから新しいFMCへの移行については、
<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>を確認してください。

略語

ACP = Access Control Policy (アクセスコントロールポリシー)

ARP = Address Resolution Protocol (アドレス解決プロトコル)

CLI = コマンドラインインターフェイス

FMC = Secure Firewall Management Center (セキュアファイアウォールマネジメントセンター)

FTD = Secure Firewall Threat Defense (セキュアファイアウォール脅威対策)

GARP = Gratuitous ARP

HA = High Availability (高可用性)

MW = メンテナンスウィンドウ

UI = ユーザインターフェイス

前提条件

移行プロセスを開始する前に、次の前提条件が満たされていることを確認してください。

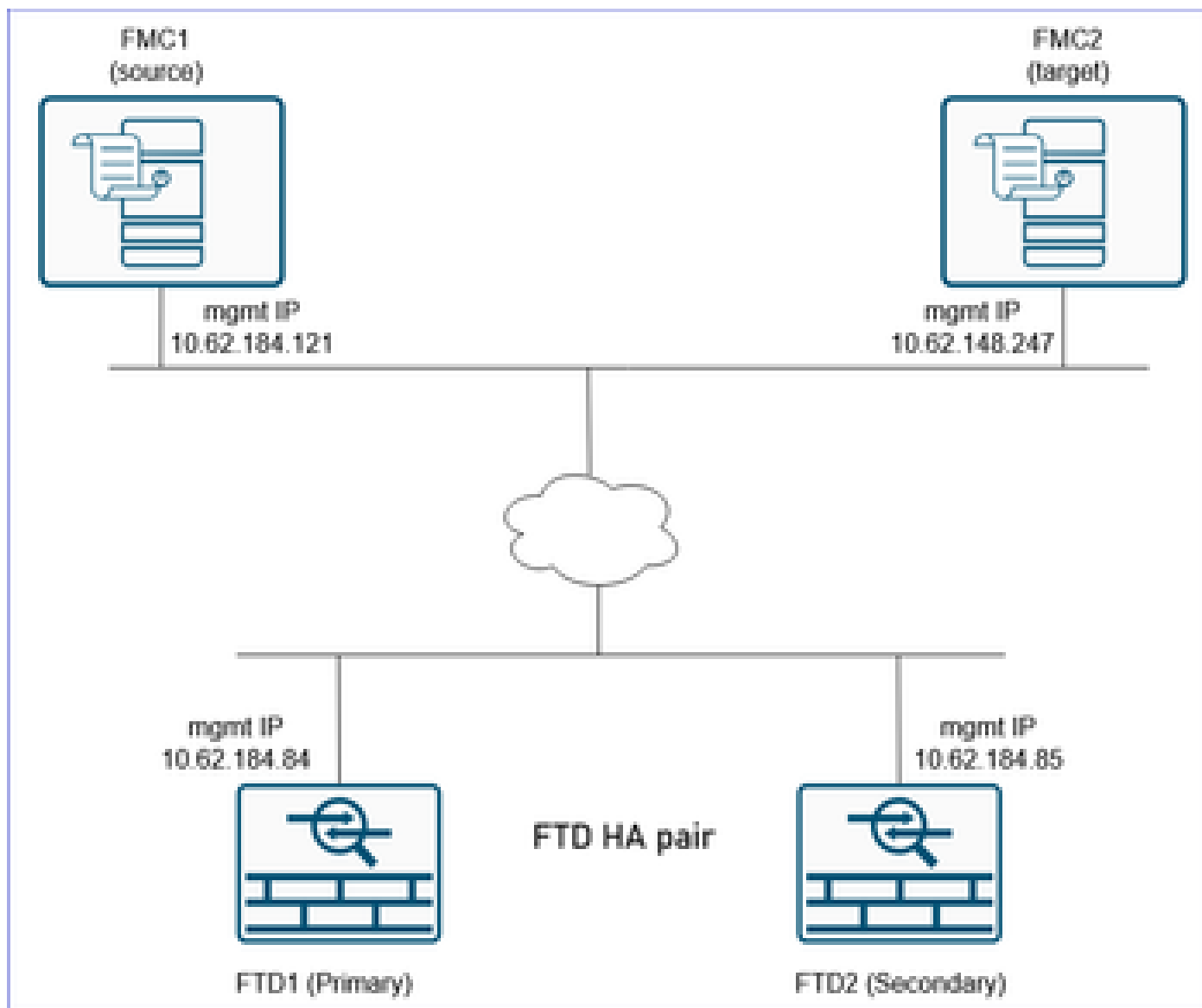
- UIおよびCLIを使用して、送信元と宛先の両方のFMCにアクセスできます。
- FMCとファイアウォールの両方の管理者クレデンシャル
- 両方のファイアウォールへのコンソールアクセス
- L3アップストリームデバイスとダウンストリームデバイスへのアクセス (ARPキャッシュをクリアする必要がある場合)。
- 宛先/ターゲットFMCのバージョンが送信元/古いFMCと同じであることを確認します。
- 宛先/ターゲットFMCのライセンスがソース/古いFMCと同じであることを確認します。
- 移行が中継トラフィックに影響を与えるため、移行を実行するメガワットを必ず配置してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall 31xx、FTDバージョン7.4.2.2
- Secure Firewall Management Centerバージョン7.4.2.2
- このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ



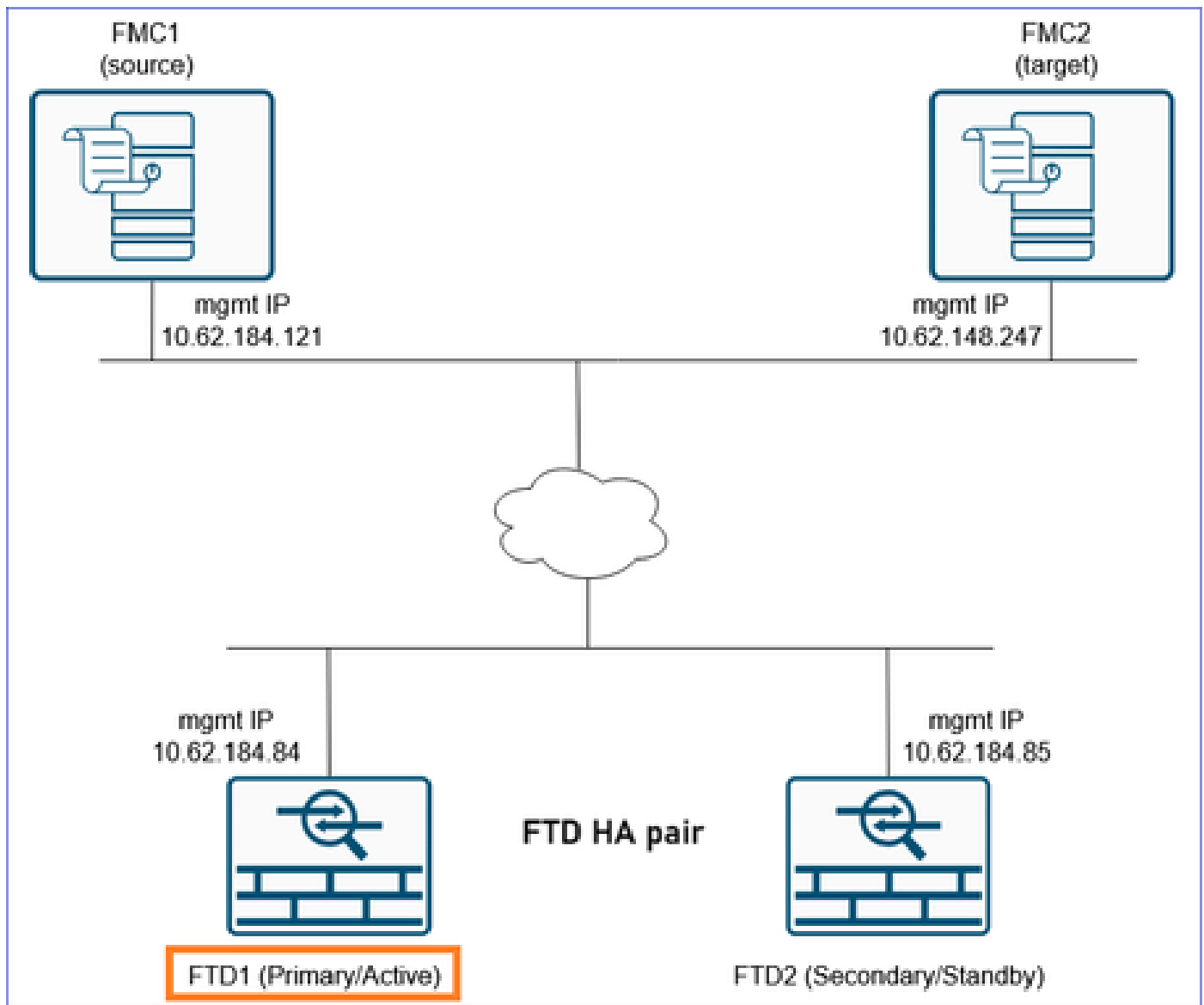
設定

移行の手順

このシナリオでは、次の状態について考えます。

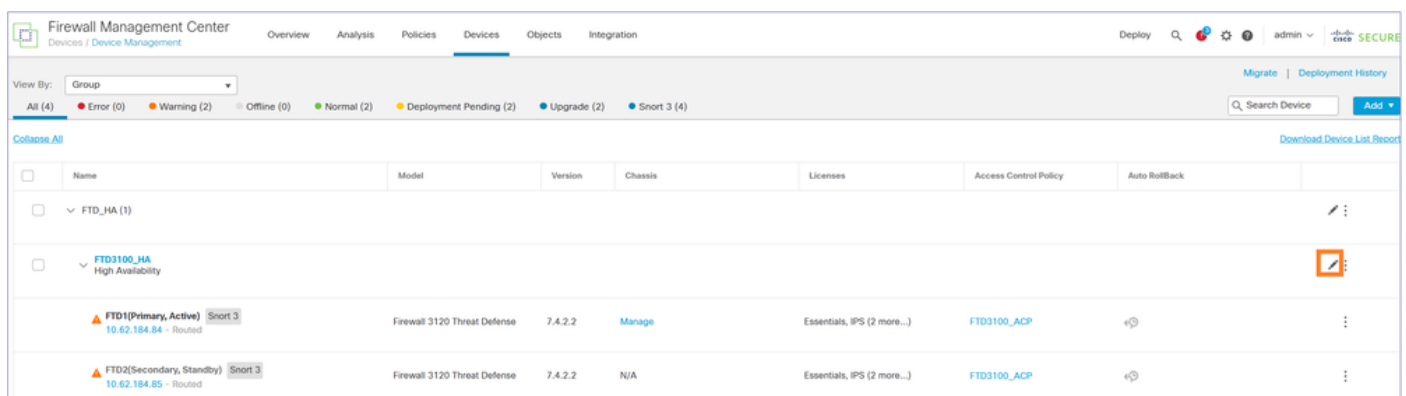
FTD1 : プライマリ/アクティブ

FTD2 : セカンダリ/スタンバイ



ステップ 1：プライマリファイアウォールからのデバイス設定のエクスポート

FMC1 (ソースFMC) で、Devices > Device Managementに移動します。FTD HAペアを選択し、Editを選択します。



Device タブに移動します。プライマリ/アクティブFTD (この場合はFTD1) が選択されていることを確認し、Exportを選択してデバイス設定をエクスポートします。

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

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



注:7.1ソフトウェアリリース以降では、エクスポートオプションを使用できます。

Notifications > Tasksページに移動して、エクスポートが完了したことを確認できます。次に、Download Export Packageを選択します。

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](#)

または、General領域にあるDownloadボタンをクリックします。sfoファイルを取得します。例：
DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

このファイルには、次のようなデバイス関連の設定が含まれています。

- ルーテッドインターフェイス
- インラインセット
- ルーティング
- DHCP
- VTEP

- 関連オブジェクト

注：エクスポートしたコンフィギュレーションファイルは、同じFTDにのみインポートできます。FTDのUUIDは、インポートされたsfoファイルの内容と一致する必要があります。同じFTDを別のFMCに登録し、sfoファイルをインポートできます。

参考：「デバイス設定のエクスポートとインポート」

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

ステップ 2：セカンダリFTDをアクティブにする

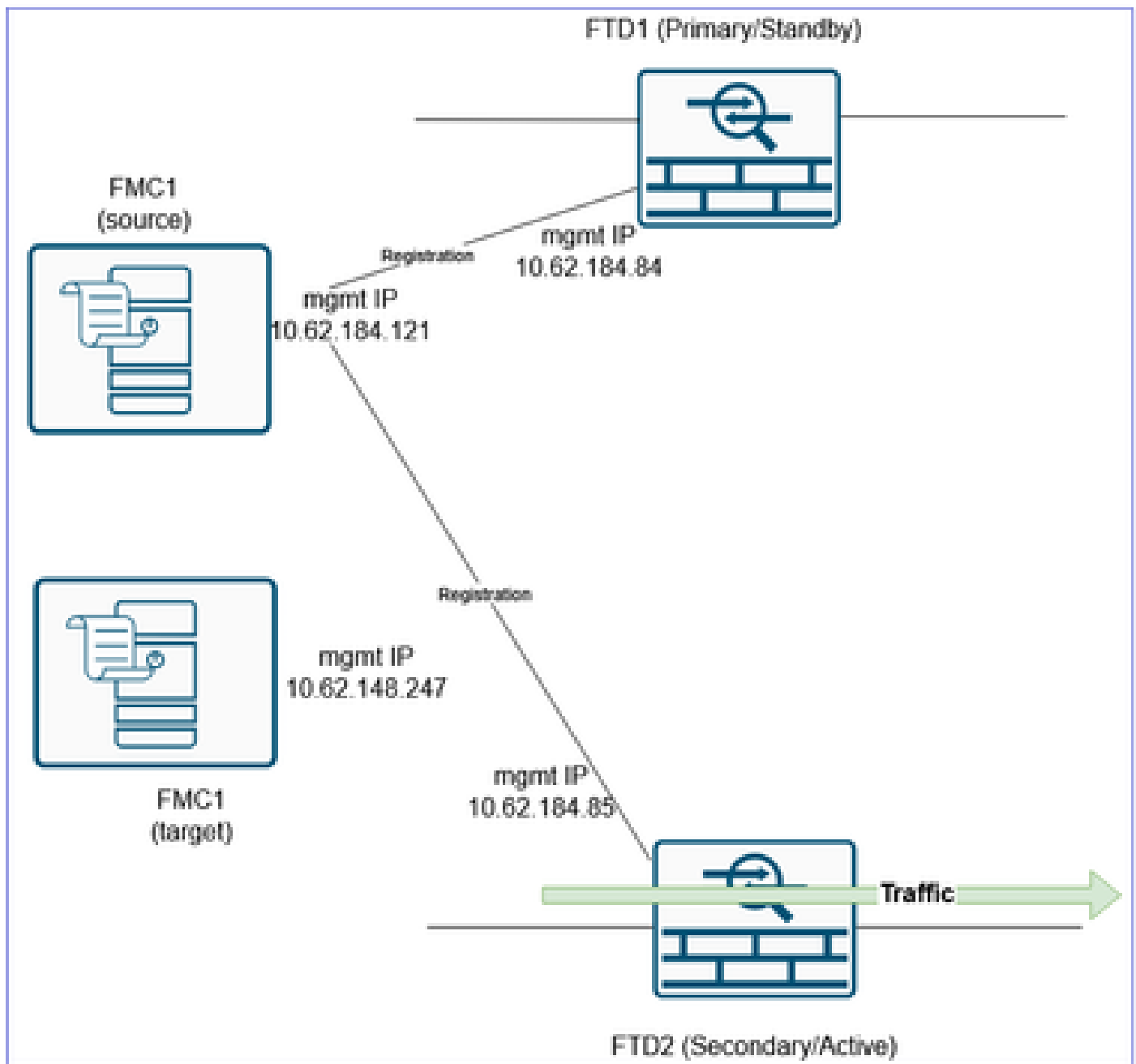
Devices > Device Managementの順に移動し、FTD HAペアを選択して、Switch Active Pair:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD100_HA (1)						
FTD100_HA High Availability						
FTD1(Primary, Standby) 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

その結果、FTD1 (プライマリ/スタンバイ) とFTD (セカンダリ/アクティブ) が作成されます。

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD100_HA (1)						
FTD100_HA High Availability						
FTD1(Primary, Standby) 10.62.184.84 - Routed	Snort 3	Firewall 3120 Threat Defense	7.4.2.2	N/A	Essentials, IPS (2 more...)	FTD3100_ACP
FTD2(Secondary, Active) 10.62.184.85 - Routed	Snort 3	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP

これで、トラフィックはセカンダリ/アクティブFTDによって処理されます。



ステップ 3 : FTD HAの解除

Devices > Device Managementに移動し、FTD HAを中断します。

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is selected, and the 'View By' dropdown is set to 'Group'. The table lists the following devices:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1 (1)						
FTD3100_HA High Availability						
FTD1(Primary, Standby) Short 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) Short 3 10.62.184.85 - Routed	Firewall 3120 Threat Defense	7.4.2.2	Manage	Essentials, IPS (2 more...)	FTD3100_ACP	+⌵

The 'FTD2(Secondary, Active)' row is highlighted, and a context menu is open showing the 'Break' option.

次のウィンドウが表示されます。[Yes] を選択します。

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

 注：この時点では、HAブレーク中にSnortエンジンが再起動されるため、数秒間トラフィックが中断される場合があります。また、メッセージで説明しているように、NATを使用しているトラフィックの停止が長く続く場合は、アップストリームデバイスとダウンストリームデバイスのARPキャッシュをクリアすることを検討してください。

FTD HAを解除した後、FMCに2つのスタンドアロンFTDがあります。

設定の観点からは、FTD2(ex-Active)はフェールオーバー関連の設定以外は引き続き設定され、トラフィックを処理しています。

<#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

FTD1(ex-Standby)の設定はすべて削除されています。

<#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#

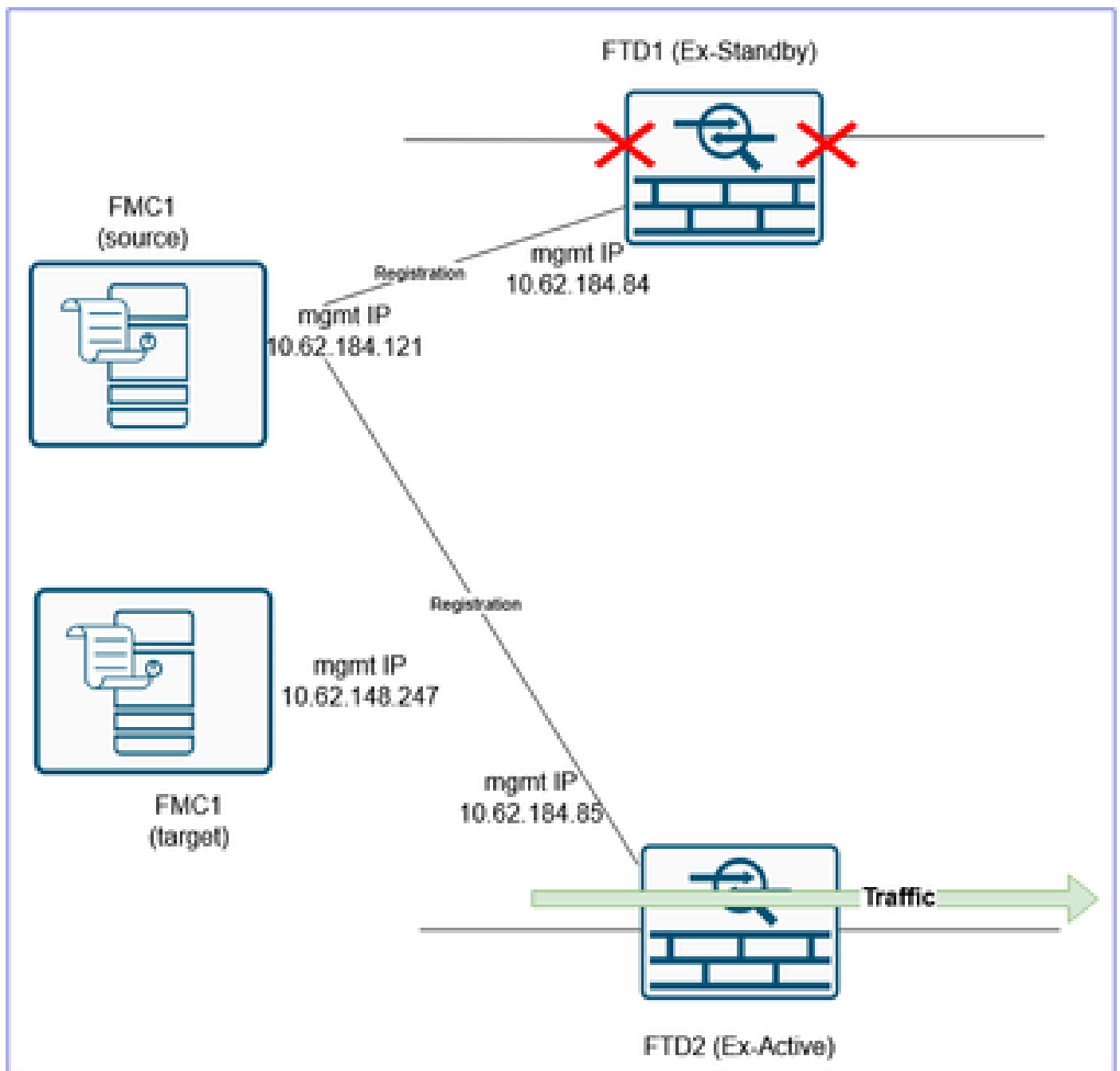
show interface ip brief

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

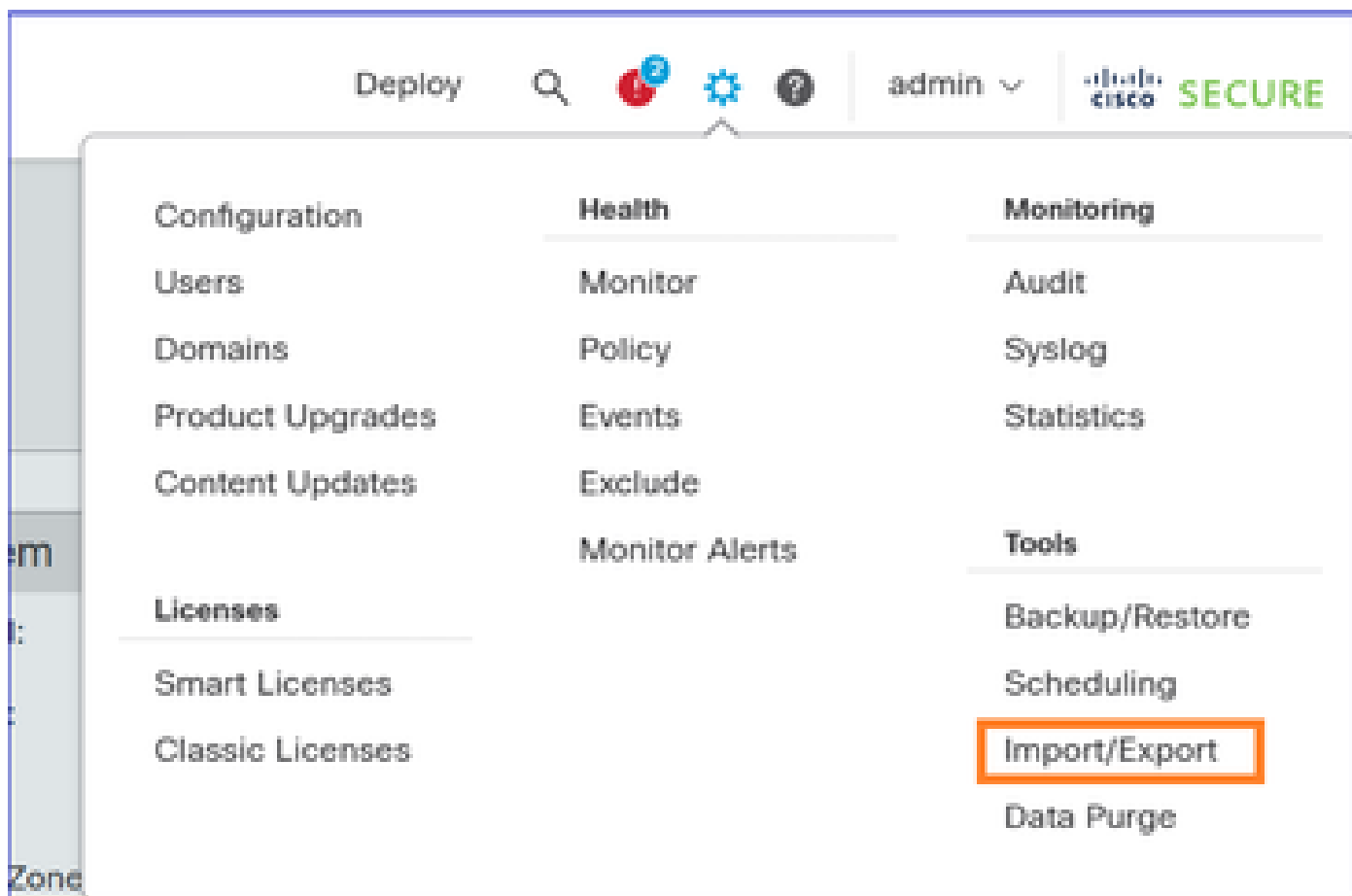
ステップ 4 : FTD1 (元プライマリ) データインターフェイスを分離します。

FTD1(ex-Primary)からデータケーブルを取り外します。 FTD管理ポートだけを接続したままにします。



ステップ 5 : FTD共有ポリシーのエクスポート

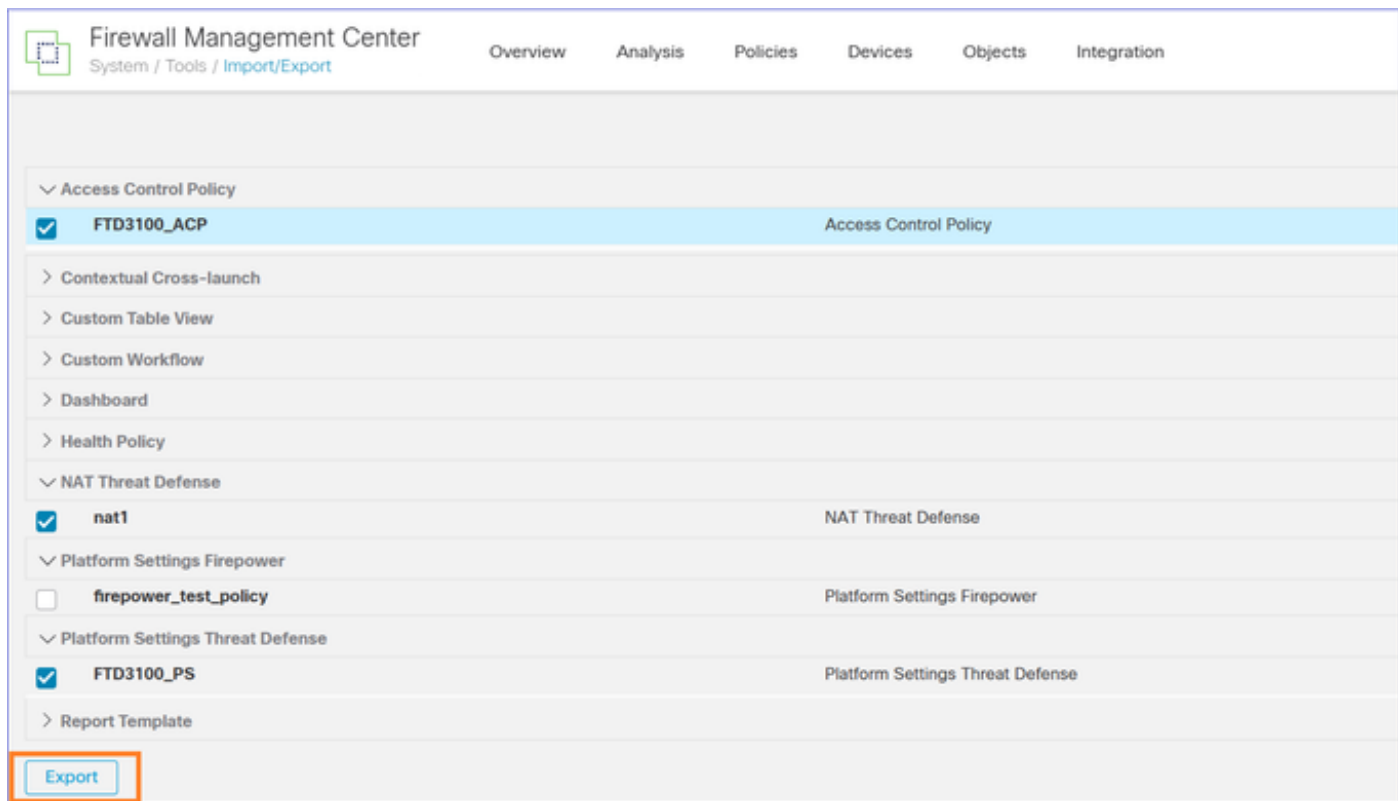
System > Toolsの順に移動し、Import/Exportを選択します。



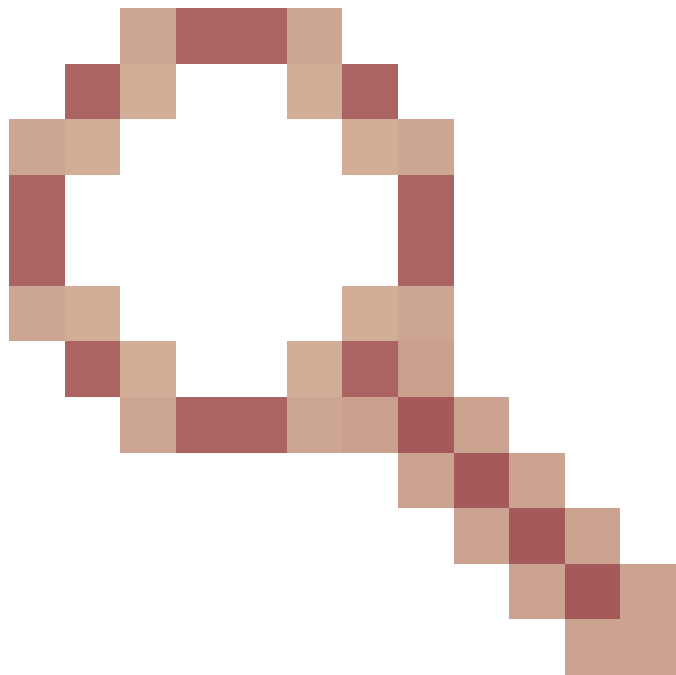
デバイスに接続されているさまざまなポリシーをエクスポートします。次のようなFTDに添付されているすべてのポリシーをエクスポートしていることを確認します。

- アクセスコントロールポリシー(ACP)
- ネットワークアドレス変換(NAT)ポリシー
- 正常性ポリシー (カスタムの場合)
- FTDプラットフォームの設定

等。



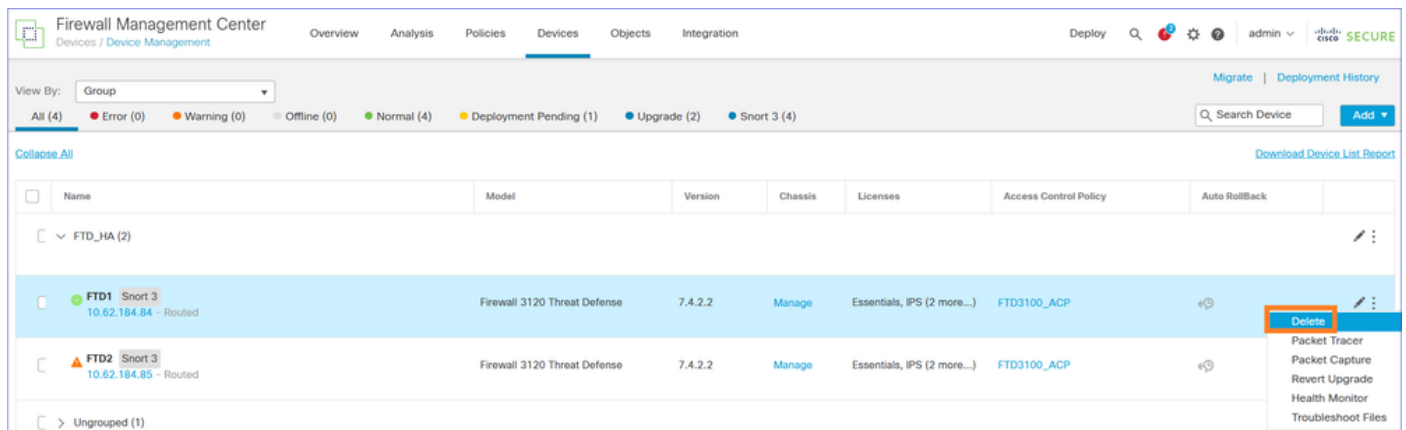
✎ 注：このドキュメントの作成時点では、VPN関連の設定のエクスポートはサポートされていません。デバイスの登録後、FMC2（ターゲットFMC）でVPNを手動で再設定する必要があります。



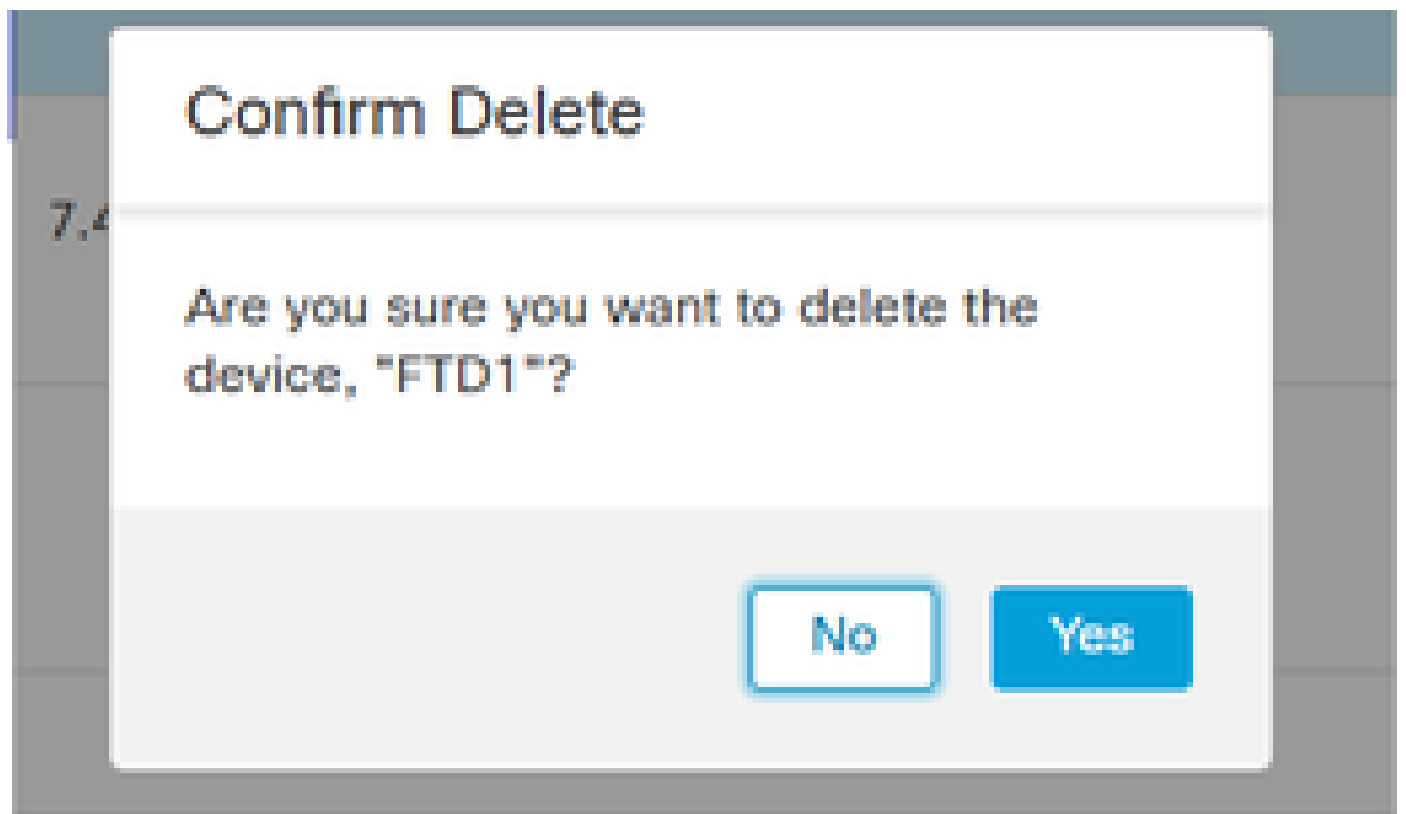
関連する機能拡張Cisco Bug ID [CSCwf05294](https://cisco.com/bug/CSCwf05294)

結果は.sfoファイルです(ObjectExport_20250306082738.sfoなど)。

手順 6：旧/ソースFMCからFTD1(ex-Primary)を削除/登録解除します。



デバイスの削除を確認します。



FTD1 CLIの確認：

```
<#root>
```

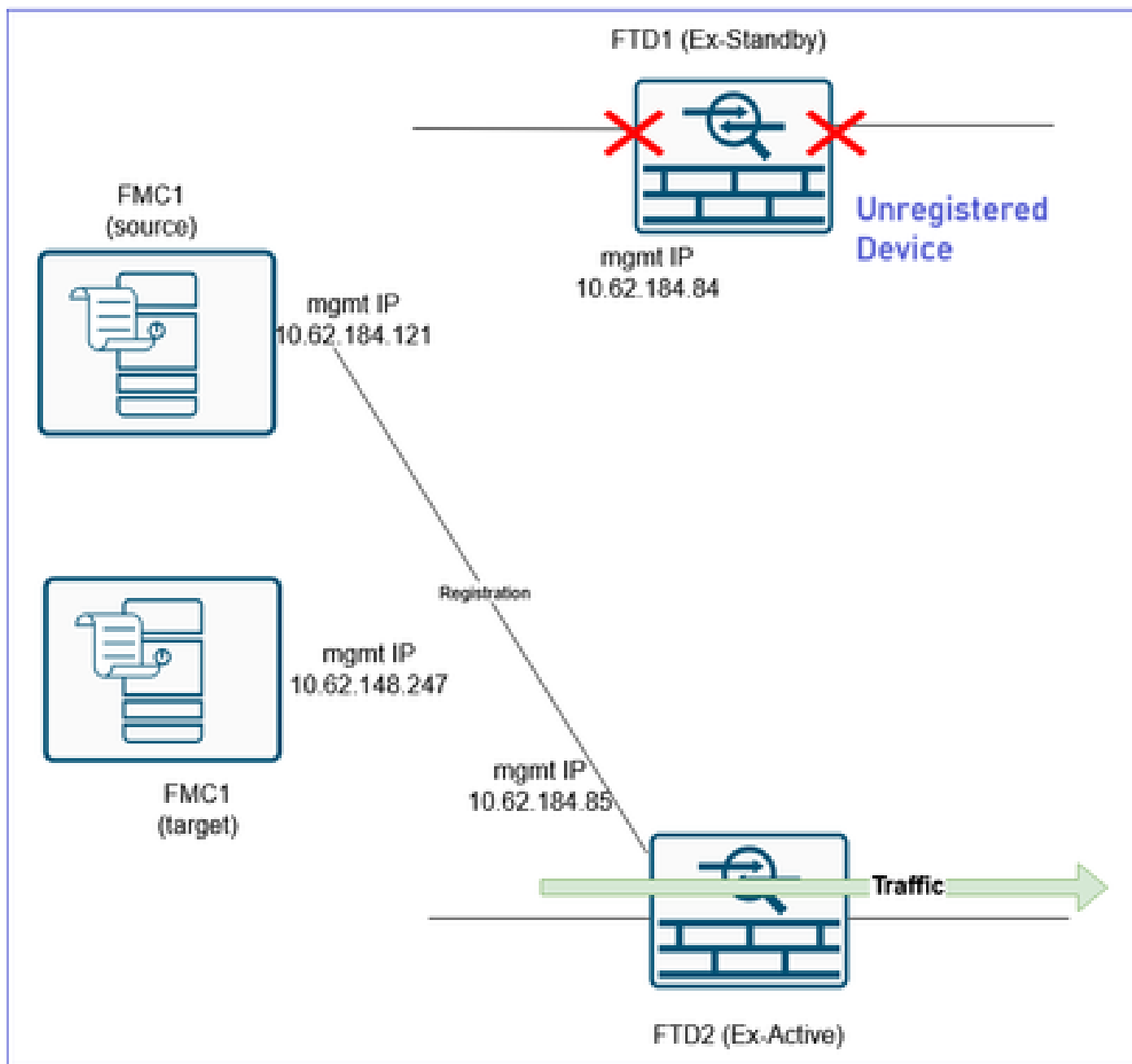
```
>
```

```
show managers
```

```
No managers configured.
```

```
>
```

FTD1デバイス削除後の現在のステータスは次のとおりです。



手順 7 : FMC2 (ターゲットFMC) へのFTDポリシー設定オブジェクトのインポート

 注：このドキュメントでは、単一のFTD HAペアの新しいFMCへの移行を中心に説明しています。一方、同じポリシー（ACP、NATなど）とオブジェクトを共有する複数のファイアウォールを移行する場合は、段階的にこの点を考慮する必要があります。

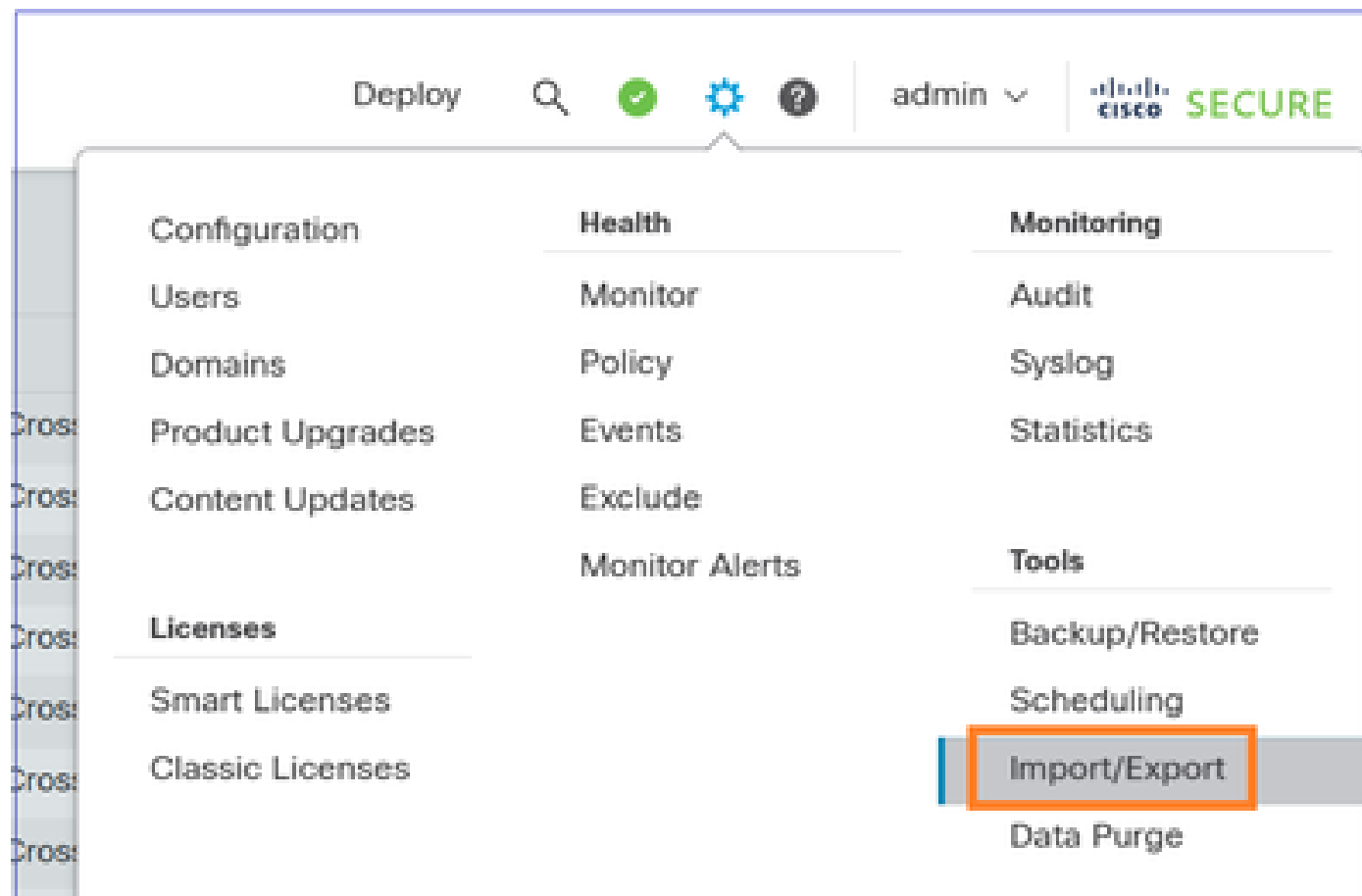
– ターゲットFMC上に同じ名前の既存のポリシーがある場合は、次の点を確認するメッセージが表示されます。

- ポリシーを置換するか、
- 別の名前で新しい名前を作成します。これにより、異なる名前（サフィックス_1）の重複オブジェクトが作成されます。

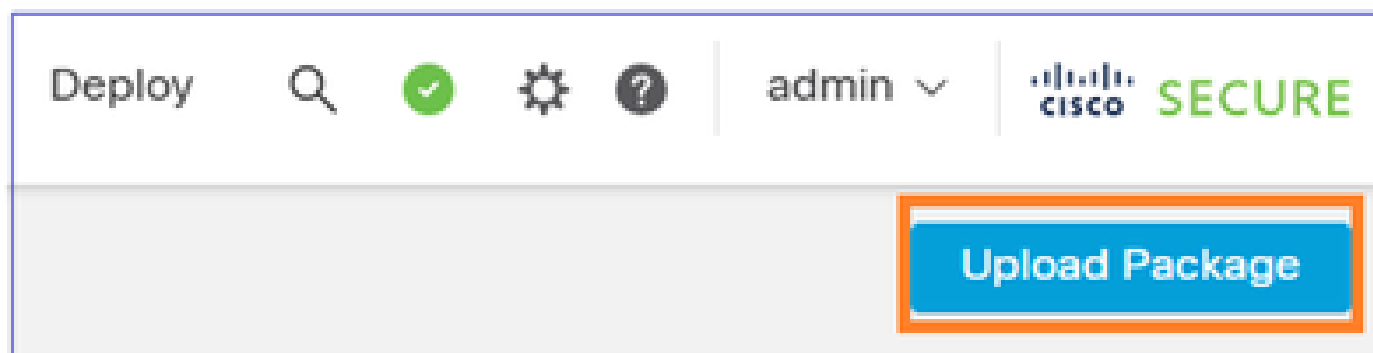
– オプション「b」を選択した場合は、ステップ9で、新しく作成したオブジェクトを移行し

✎ たポリシー（ACPセキュリティゾーン、NATセキュリティゾーン、ルーティング、プラットフォーム設定など）に割り当ててることを確認します。

FMC2（ターゲットFMC）にログインし、手順5でエクスポートしたFTDポリシーsfoオブジェクトをインポートします。



Upload Packageを選択します。



ファイルをアップロードします。

Firewall Management Center
System / Tools / Upload Package

Overview Analysis Policies Devices Objects

Package Name

1 Choose File No file chosen

2 Upload Cancel

ポリシーをインポートします。

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

FMC2 (ターゲットFMC) でインターフェイスオブジェクト/セキュリティゾーンを作成します。

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)

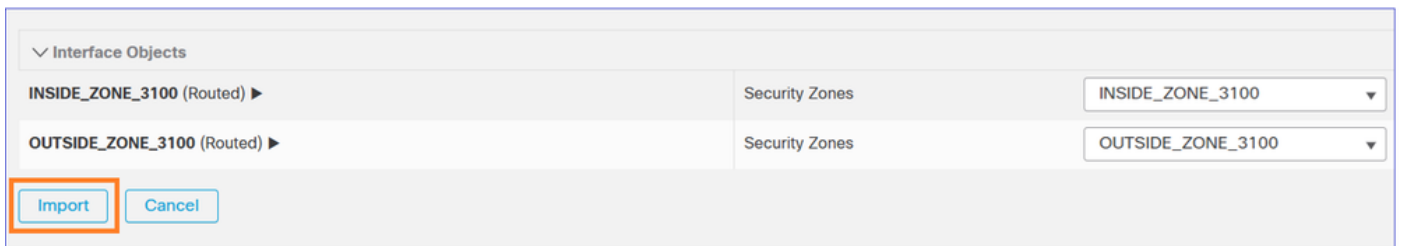
Interface Objects	
INSIDE_ZONE_3100 (Routed) ▶	Security Zones
OUTSIDE_ZONE_3100 (Routed) ▶	Security Zones

Import Cancel

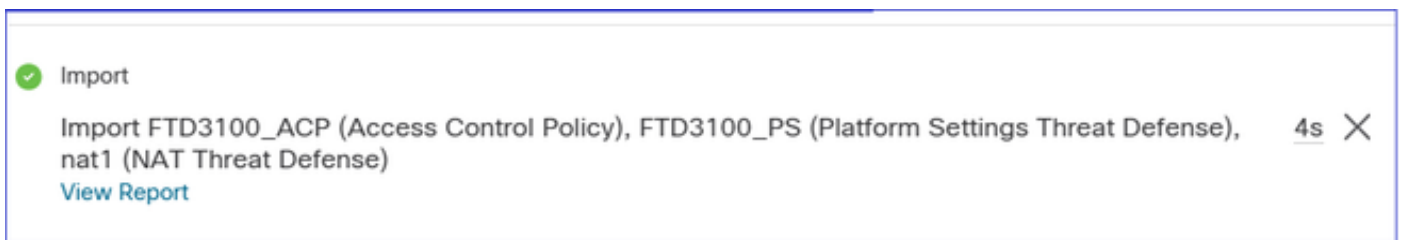
FMC1と同じ名前を付けることができます (ソースFMC) 。



Importを選択すると、タスクによって関連するポリシーがFMC2 (ターゲットFMC) にインポートされます。



タスクが完了します。



ステップ 8 : FTD1(ex-Primary)をFMC2に登録します。

FTD1(ex-Primary)CLIに移動し、新しいマネージャを設定します。

<#root>

>

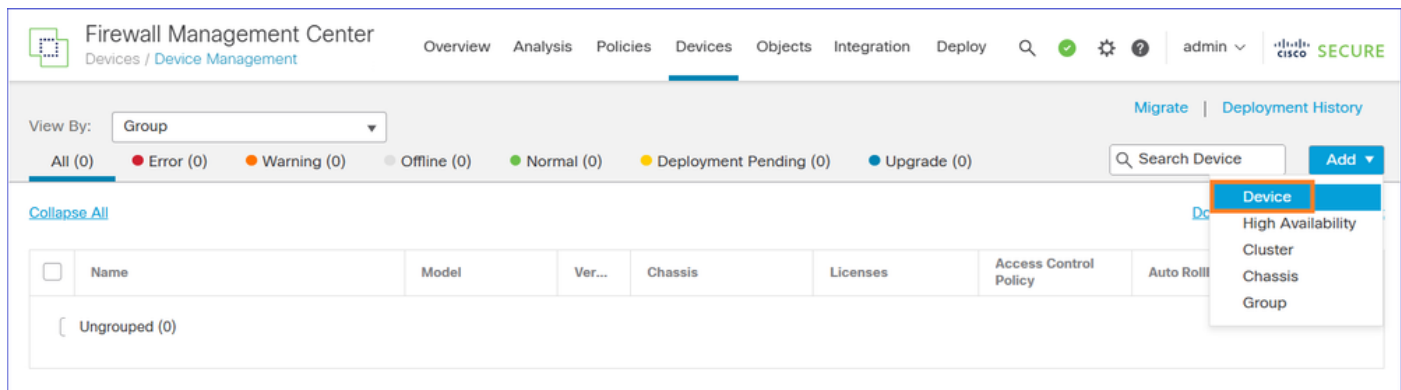
```
configure manager add 10.62.148.247 cisco
```

Manager 10.62.148.247 successfully configured.

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

>

FMC2 (ターゲットFMC) のUIでDevices > Device Managementの順に移動し、FTDデバイスを追加します。



デバイスの登録が失敗した場合は、このドキュメントで問題のトラブルシューティングを参照してください。<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html>

前の手順でインポートしたアクセスコントロールポリシーを割り当てます。

必要なライセンスを適用し、デバイスを登録します。

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:†

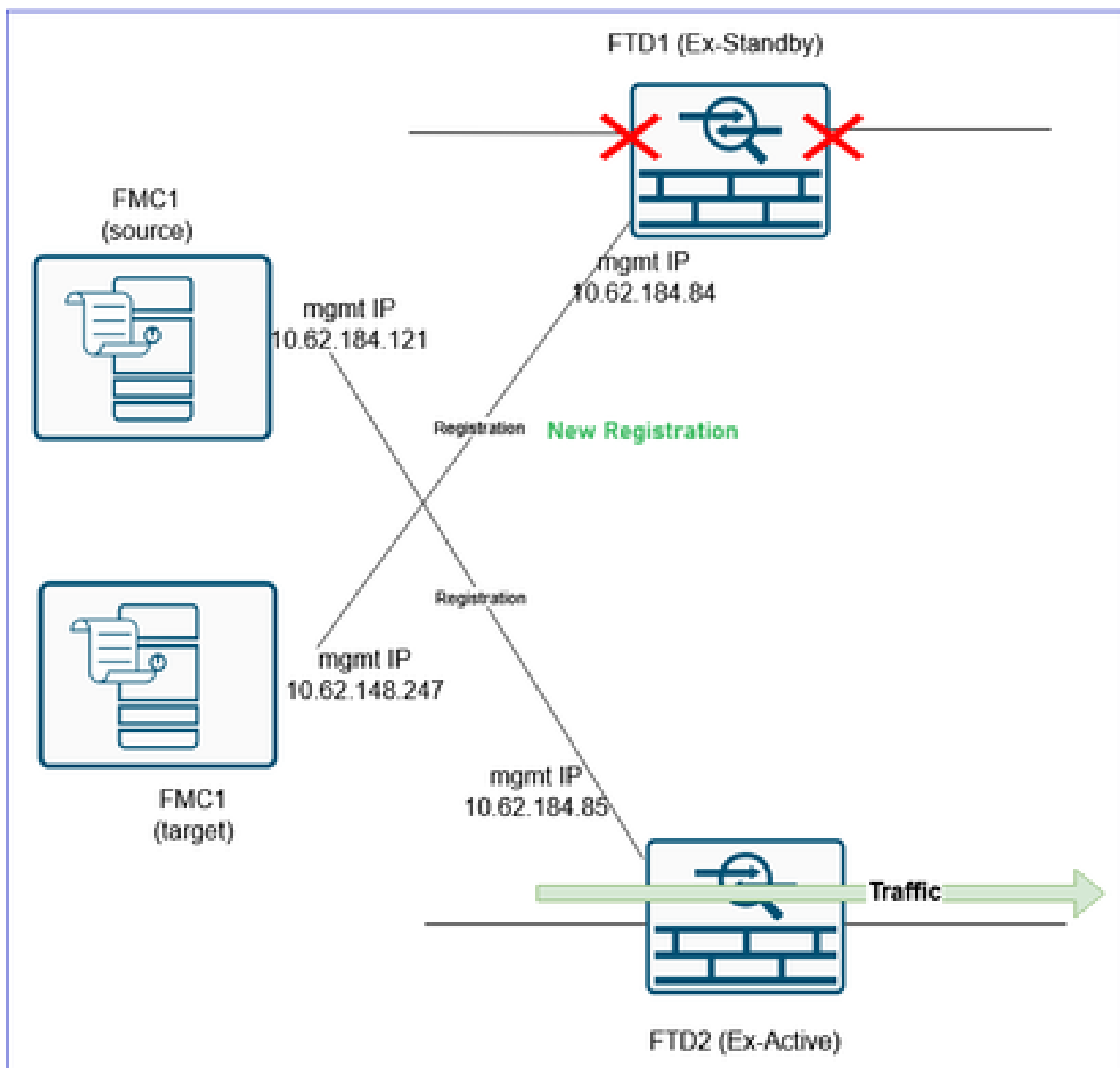
- ☒ Transfer Packets

2

Cancel

Register

結果は、次のとおりです。



ステップ 9 : FTDデバイス設定オブジェクトをFMC2 (ターゲットFMC) にインポートします。

FMC2 (ターゲットFMC) にログインし、Devices > Device Managementに移動して、前のステップで登録したFTDデバイスを編集します。

Deviceタブに移動し、手順2でエクスポートしたFTD Policiessoオブジェクトをインポートします。

 **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

 注：ステップ7で「b」オプション（新しいポリシーの作成）を選択した場合は、新しく作成したオブジェクトを移行したポリシー（ACPセキュリティゾーン、NATセキュリティゾーン、ルーティング、プラットフォーム設定など）に必ず割り当ててください。

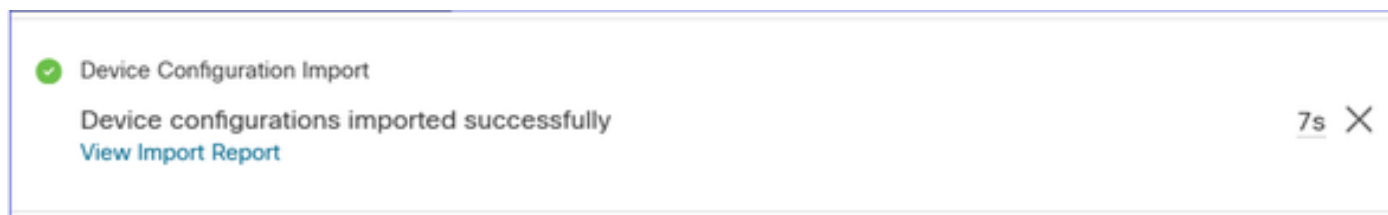
Device Configuration Import

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

No

Yes

FMCタスクが開始されます。



デバイス設定はFTD1に適用されます。たとえば、セキュリティゾーン、ACP、NATなどです。

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(Static)	Disabled	Global
Port-channel1.201	OUTSIDE	Subinterface	OUTSIDE_ZONE_3100		10.0.201.70(Static)	Disabled	Global

⚠ 注意: ACPが複数のアクセスコントロール要素(ACE)に拡張されている場合、ACPのコンパイルプロセス (tmatchコンパイル) の完了には数分かかる場合があります。次のコマンドを使用して、ACPのコンパイルステータスを確認できます。

```
<#root>
```

```
FTD3100-3#
```

```
show asp rule-engine
```

```
Rule compilation Status:
```

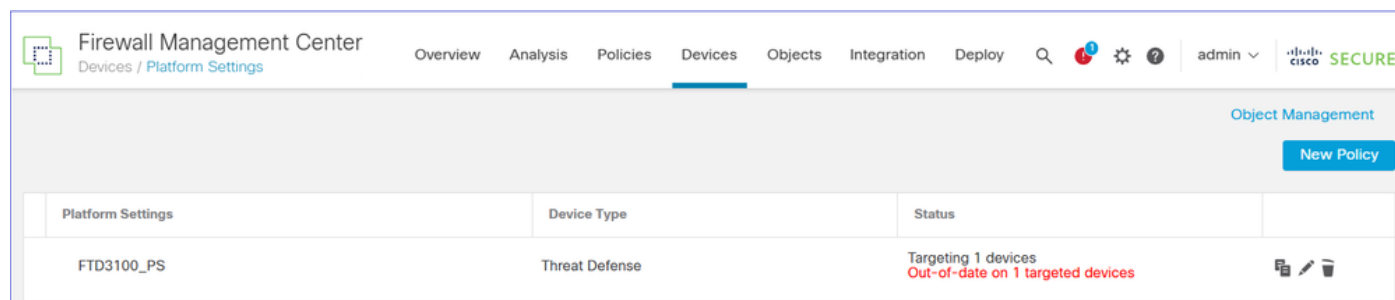
```
Completed
```

ステップ 10 : FTD設定の終了

この時点で、FMC2 (ターゲットFMC) への登録とデバイスポリシーのインポートの後もFTD1で依然として不足している可能性のあるすべての機能を設定することを目指しています。

NAT、プラットフォーム設定、QoSなどのポリシーがFTDに割り当てられていることを確認します。ポリシーは割り当てられているが、展開が保留中であることがわかります。

たとえば、プラットフォーム設定はインポートされてデバイスに割り当てられますが、展開は保留されます。



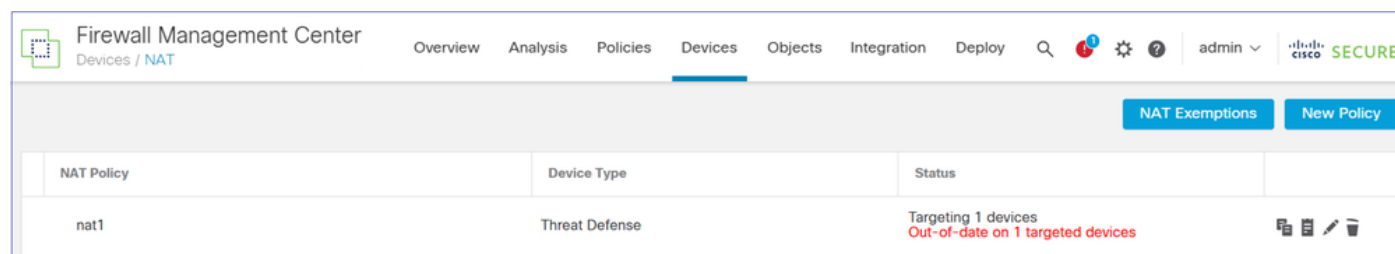
Firewall Management Center
Devices / Platform Settings

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

NATが設定されている場合、NATポリシーはインポートされてデバイスに割り当てられますが、展開は保留されます。



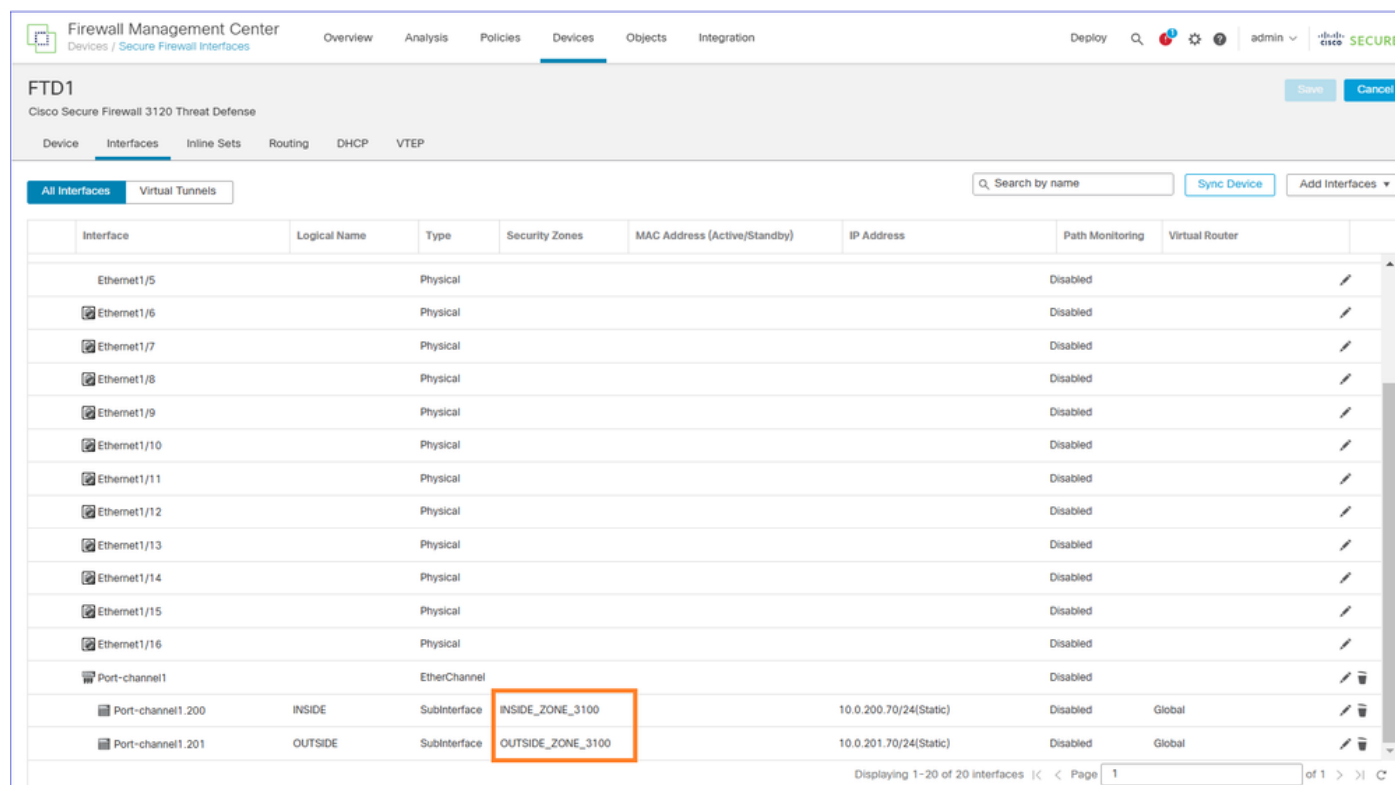
Firewall Management Center
Devices / NAT

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

セキュリティゾーンはインターフェイスに適用されます。



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

ルーティング設定がFTDデバイスに適用されます。

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

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

+ Add Route

✎ 注：ここでは、自動的に移行できなかったポリシー（VPNなど）を設定します。

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	
FTD FTD1	OUTSIDE (10.0.201.70)	net_10.0.200.0	✎ 🗑

Node B:

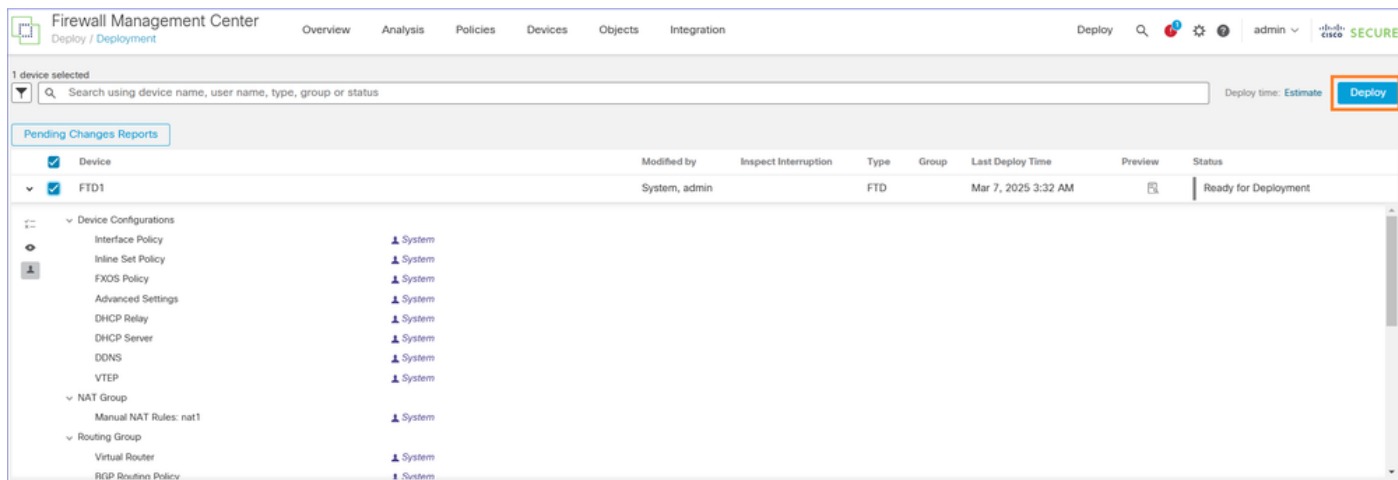
Device Name	VPN Interface	Protected Networks	
Extranet Remote_FW	10.0.201.60	net_10.0.202.0	✎ 🗑

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

Cancel Save

✎ 注：移行されるFTDに、ターゲットFMCにも移行されるS2S VPNピアがある場合は、すべてのFTDをターゲットFMCに移行した後でVPNを設定する必要があります。

保留中の変更を展開します。



ステップ 11 展開されたFTD設定の確認

この時点で、目標は、すべての設定が適切であることをFTD CLIから確認することです。

両方のFTDからの「show running-config」出力を比較することを推奨します。比較には、WinMergeやdiffなどのツールを使用できます。

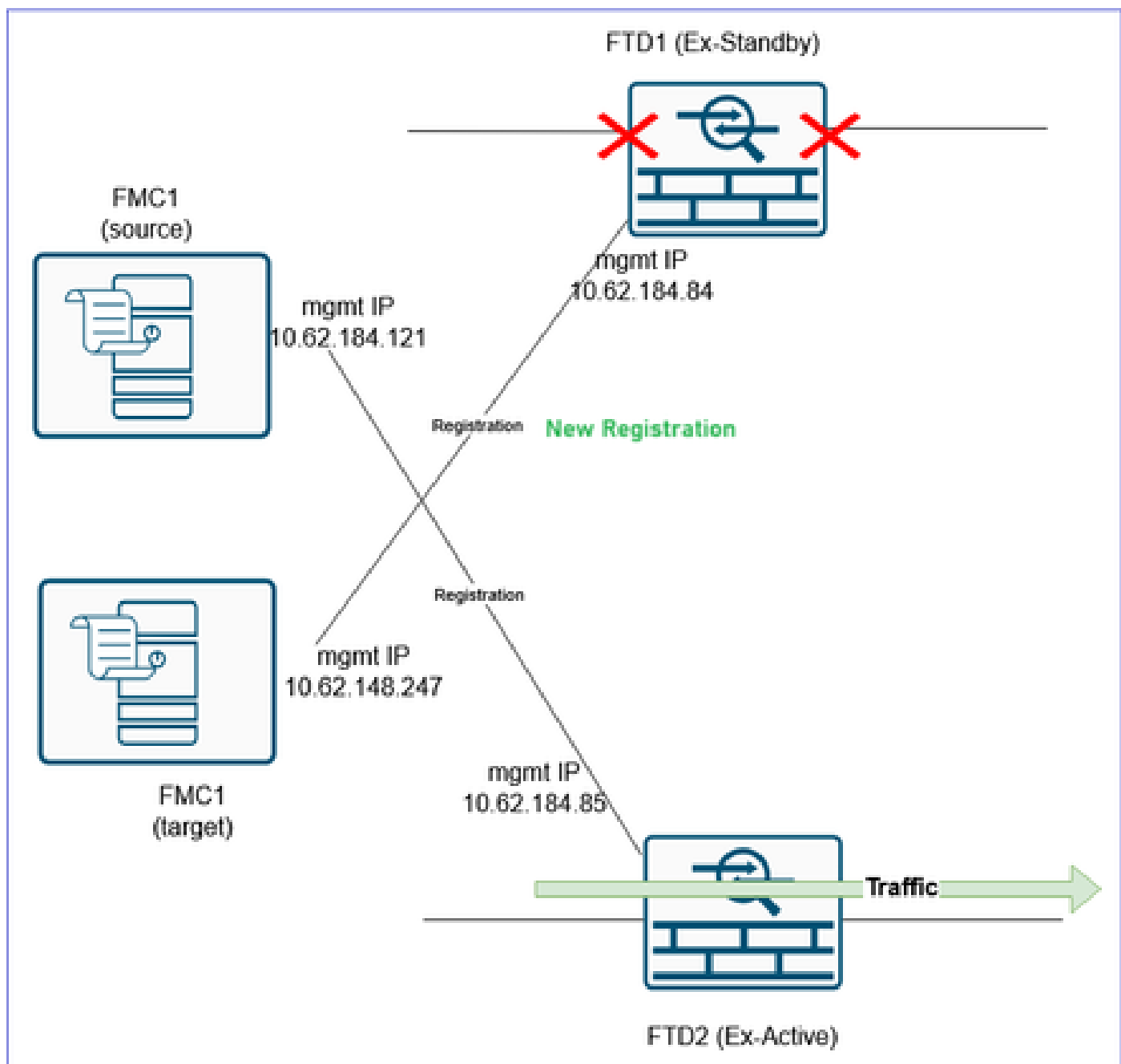
表示される通常の違いは次のとおりです。

- デバイスのシリアル番号
- インターフェイスの説明
- ACLルールID
- 設定Cryptochecksum

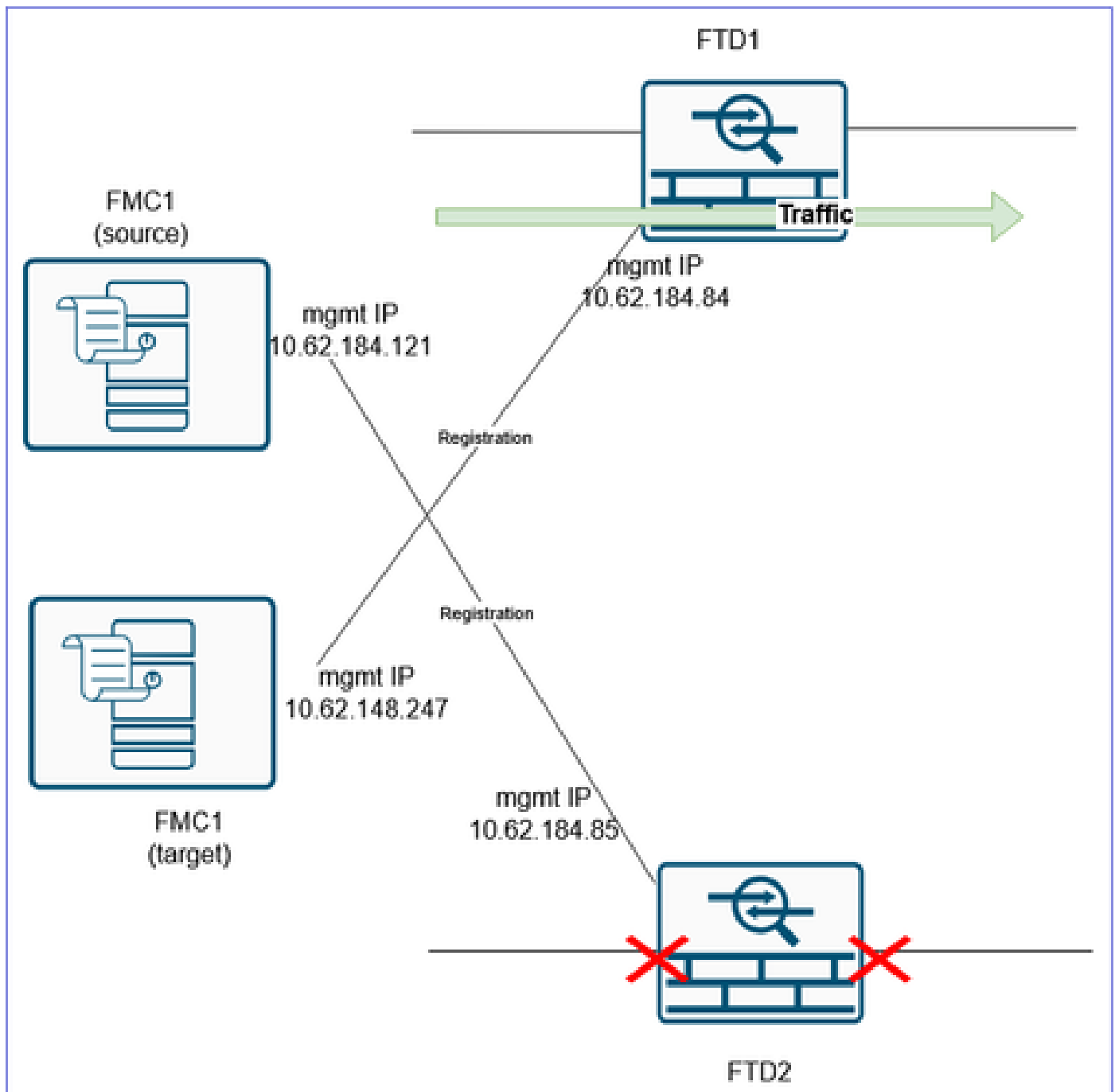
ステップ 12 カットオーバーの実行

このステップで目標とするのは、現在トラフィックを処理していて、まだ古い/ソースFMCに登録されているFTD2から、ターゲットFMCに登録されているFTD1へのトラフィックを切り替えることです。

変更前：



変更後：



⚠ 注意：カットオーバーを実行するには、MWを手配します。カットオーバー中は、すべてのトラフィックがFTD1に転送されるか、VPNが再確立されるまで、トラフィックが中断されます。

⚠ 注意：ACPのコンパイルが完了しない限り、カットオーバーを開始しないでください（上記のステップ10を参照）。

⚠ 警告：FTD2からデータケーブルを取り外すか、関連するスイッチポートをシャットダウンしてください。そうしないと、トラフィックを処理するデバイスが両方とも存在することになります。

 注意：両方のデバイスが同じIP設定を使用しているため、隣接するL3デバイスのARPキャッシュを更新する必要があります。トラフィックのカットオーバーを促進するために、隣接デバイスのARPキャッシュを手動でクリアすることを検討してください。

 ヒント:GARPパケットを送信し、FTD CLIコマンドを使用して隣接デバイスのARPキャッシュを更新することもできます。

<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

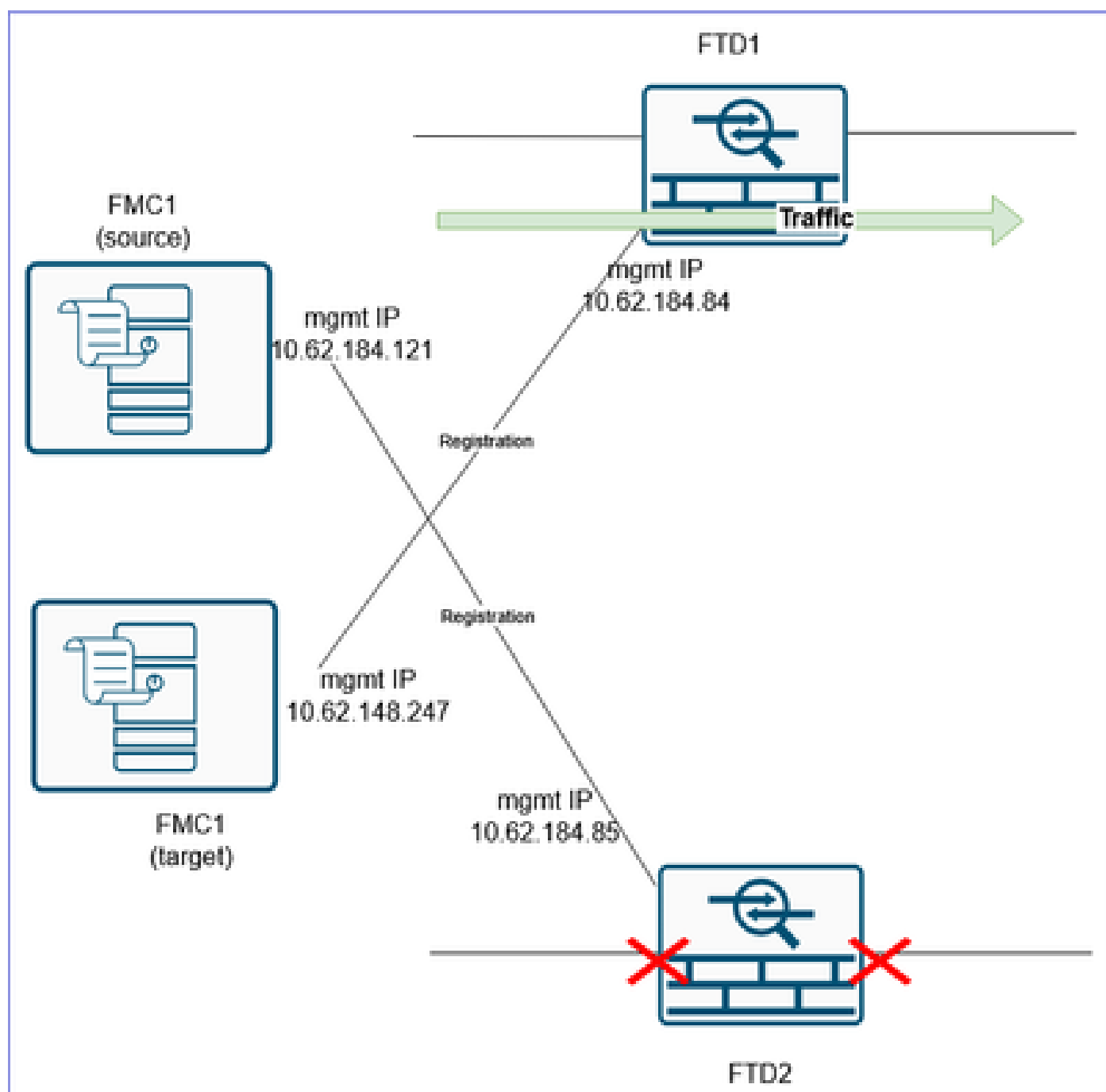
Gratuitous ARP sent for 10.0.200.70

このコマンドは、FWが所有するすべてのIPに対して繰り返す必要があります。したがって、ファイアウォールが所有するすべてのIPに対してGARPパケットを送信するよりも、隣接デバイスのARPキャッシュだけをクリアするほうが高速です。

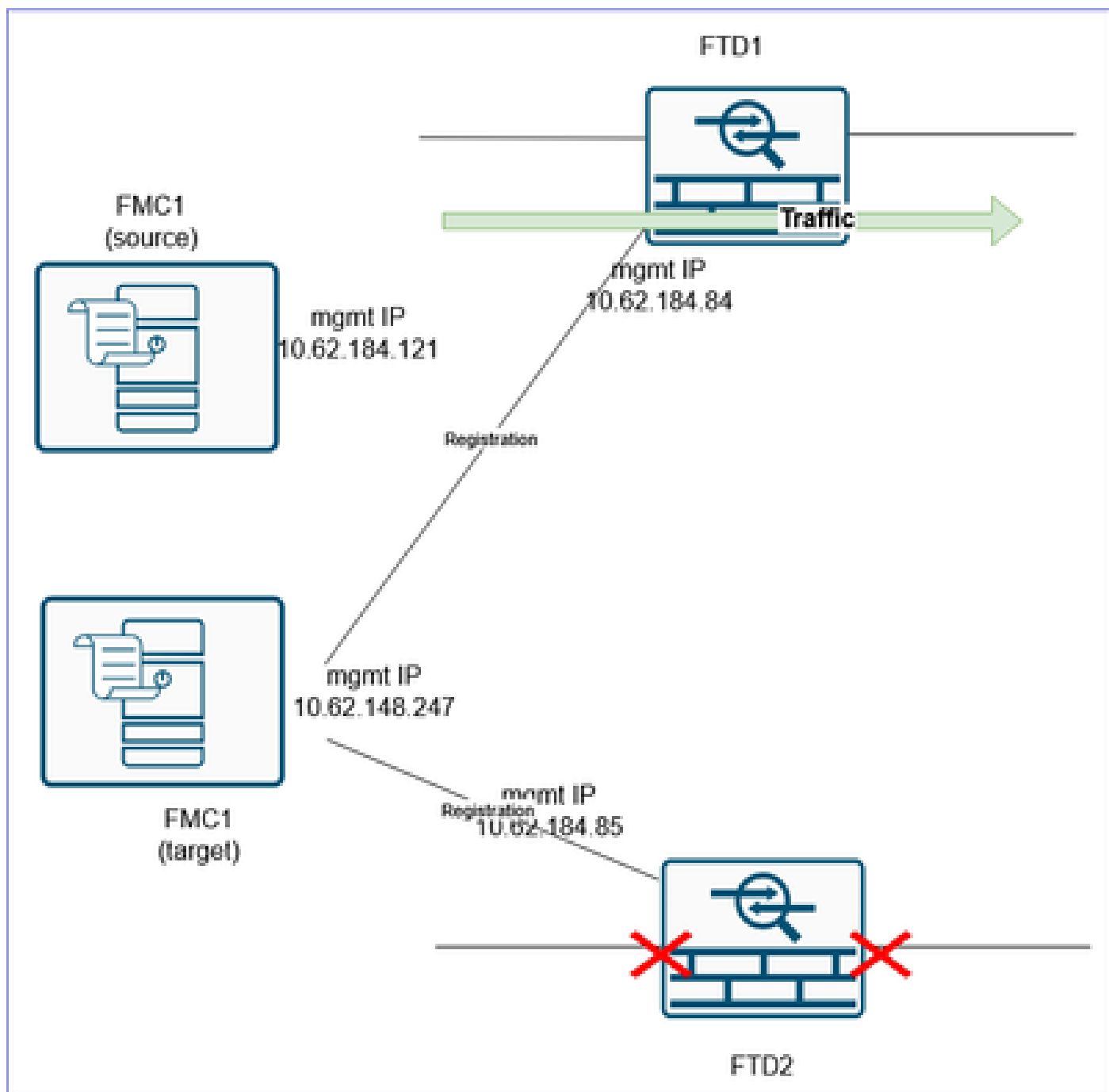
ステップ 132番目のFTDをFMC2 (ターゲットFMC) に移行します。

最後に、HAペアを改革します。これを行うには、最初にFMC1 (ソースFMC) からFTD2を削除し、FMC2 (ターゲットFMC) に登録する必要があります。

変更前：



変更後：



FTD2にVPN設定が接続されている場合は、FTDを削除する前に、まずそれを削除する必要があります。別のケースでは、次のようなメッセージが表示されます。

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 による確認:

```
<#root>
```

```
>
```

```
show managers
```

```
No managers configured.
```

ターゲットFMCに登録する前に、すべてのFTD設定を消去することを推奨します。これを簡単に行うには、ファイアウォールモードを切り替えます。

たとえば、ルーテッドモードがある場合は、トランスペアレントモードに切り替えてから、ルー

テッドモードに戻します。

```
<#root>
```

```
>
```

```
configure firewall transparent
```

次に、

```
<#root>
```

```
>
```

```
configure firewall routed
```

次に、それをFMC2 (ターゲットFMC) に登録します。

```
<#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

View By: Group

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

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

結果は、次のとおりです。

Firewall Management Center
Devices / Device Management

View By: Group

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

Devices

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

ステップ 14 : FTD HAを再構築します。

注：このタスクは（HA関連のタスクと同様に）MW中に実行する必要があります。HAネゴシエーション中、データインターフェイスがダウンしてから1分以内にトラフィックが停止します。

ターゲットFMCで、Devices > Device Management、Add > High Availabilityの順に選択します。

注意：トラフィックを処理するFTD（このシナリオではFTD1）をプライマリピアとして選択していることを確認してください。

Version Chassis Licenses

Add High Availability Pair ?

Name:*
FTD3100_HA

Device Type:
Firewall Threat Defense ▼

Primary Peer:
FTD1 ▼

Secondary Peer:
FTD2 ▼

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.

Cancel Continue

監視対象インターフェイス、スタンバイIP、仮想MACアドレスなどのHA設定を再設定します。

FTD1 CLIからの確認：

```
<#root>
```

```
FTD3100-3#
```

```
show failover | include host
```

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

FTD2 CLIからの確認：

<#root>

FTD3100-3#

show failover | include host

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

FMC UIの検証：

Firewall Management Center

Devices / Device Management

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

View By:

Group

Migrate

Deployment History

All (2)

Error (0)

Warning (0)

Offline (0)

Normal (2)

Deployment Pending (0)

Upgrade (2)

Snort 3 (2)

Search Device

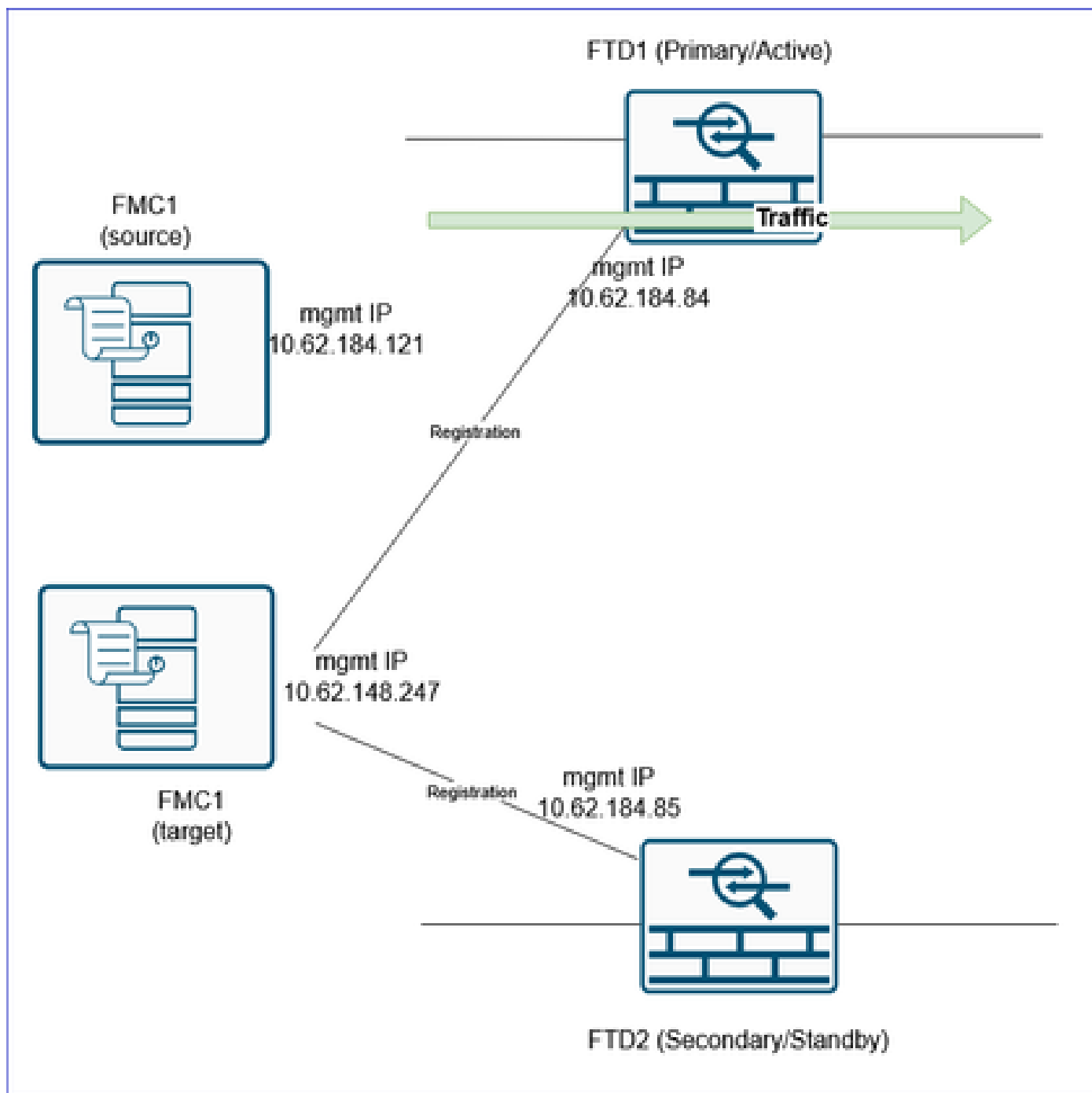
Add

Collapse All

Download Device List Report

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	Ungrouped (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	

最後に、FTD2デバイスのデータインターフェイスの起動と再接続を行います。



参考資料

- [デバイス設定のエクスポートとインポート](#)
- [ハイアベイラビリティペアの追加](#)
- [FMC間でのFTDの移行](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。