将FTD HA（故障转移）迁移到另一个FMC

目录

简介

本文档介绍将FTD HA从现有FMC迁移到其他FMC的过程。

有关到新FMC的独立防火墙迁移，请查看 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

缩写

ACP =访问控制策略

ARP = 地址解析协议

CLI =命令行界面

FMC =安全防火墙管理中心

FTD =安全防火墙威胁防御

GARP =无故ARP

HA =高可用性

MW =维护时段

UI =用户界面

先决条件

开始迁移过程之前，请确保具备以下必备条件：

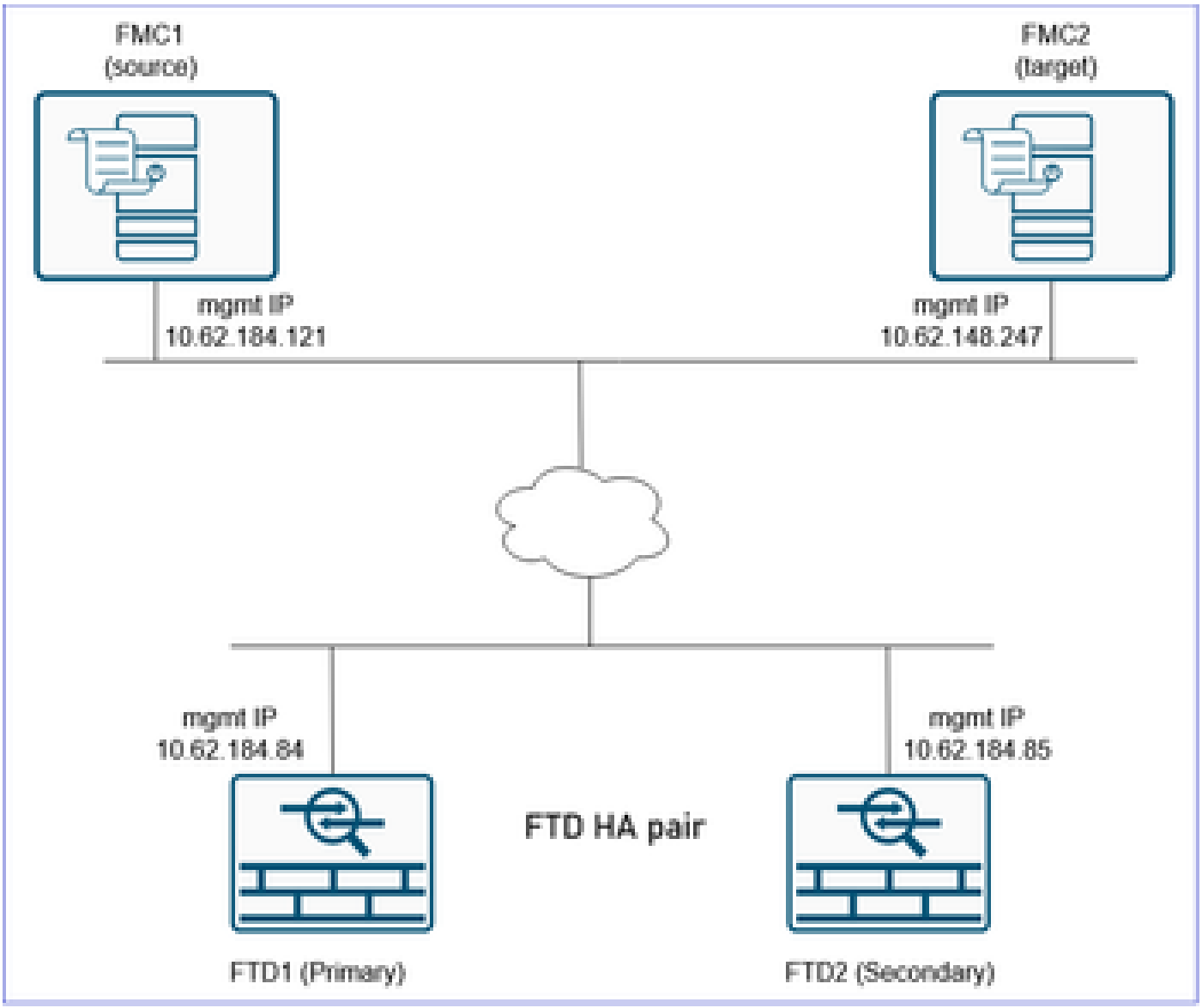
- 对源FMC和目标FMC的UI和CLI访问。
- FMC和防火墙的管理凭证。
- 通过控制台访问两个防火墙。
- 访问第3层上游和下游设备（如果需要清除ARP缓存）。
- 确保目标/目标FMC与源/旧FMC的版本相同。
- 确保目标/目标FMC与源/旧FMC具有相同的许可证。
- 确保您安排一个MW来执行迁移，因为它将影响中转流量。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure Firewall 31xx，FTD版本7.4.2.2。
- 安全防火墙管理中心版本7.4.2.2。
- 本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

拓扑



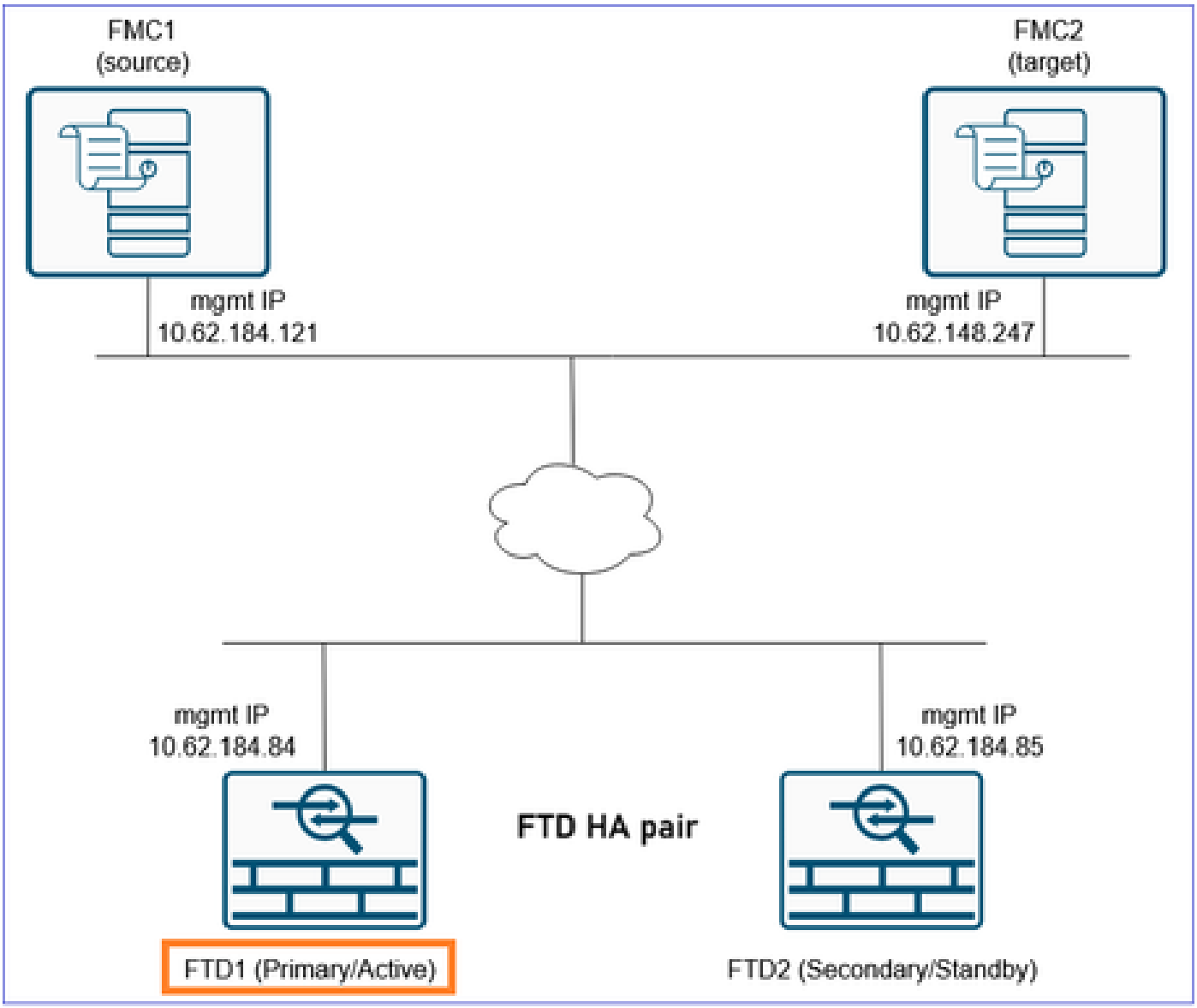
配置

迁移步骤

对于此场景，我们考虑以下状态：

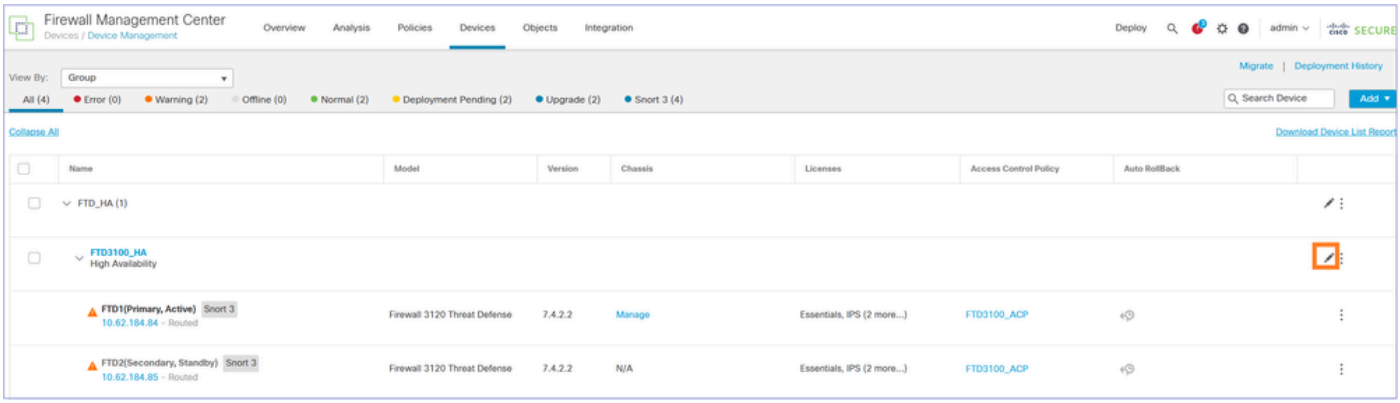
FTD1:主/主用

FTD2:辅助/备用

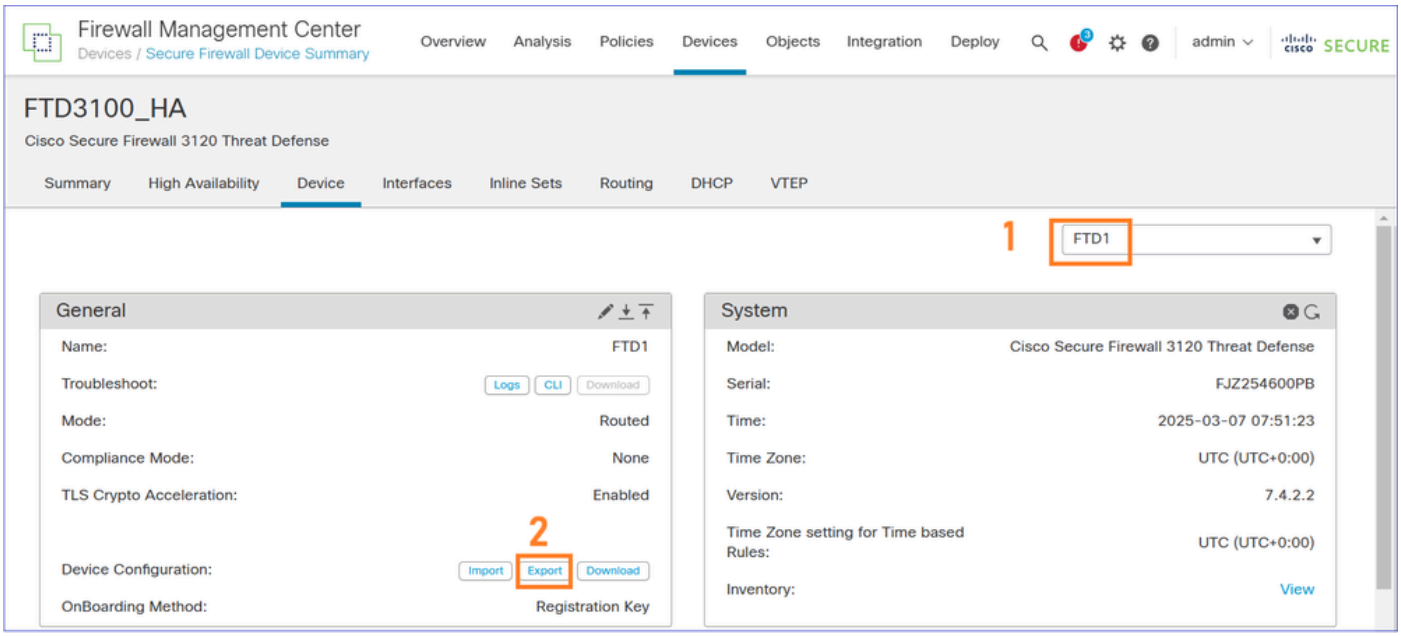


步骤1.从主防火墙导出设备配置

在FMC1（源FMC）上，导航到设备>设备管理。选择FTD HA对，然后选择Edit:

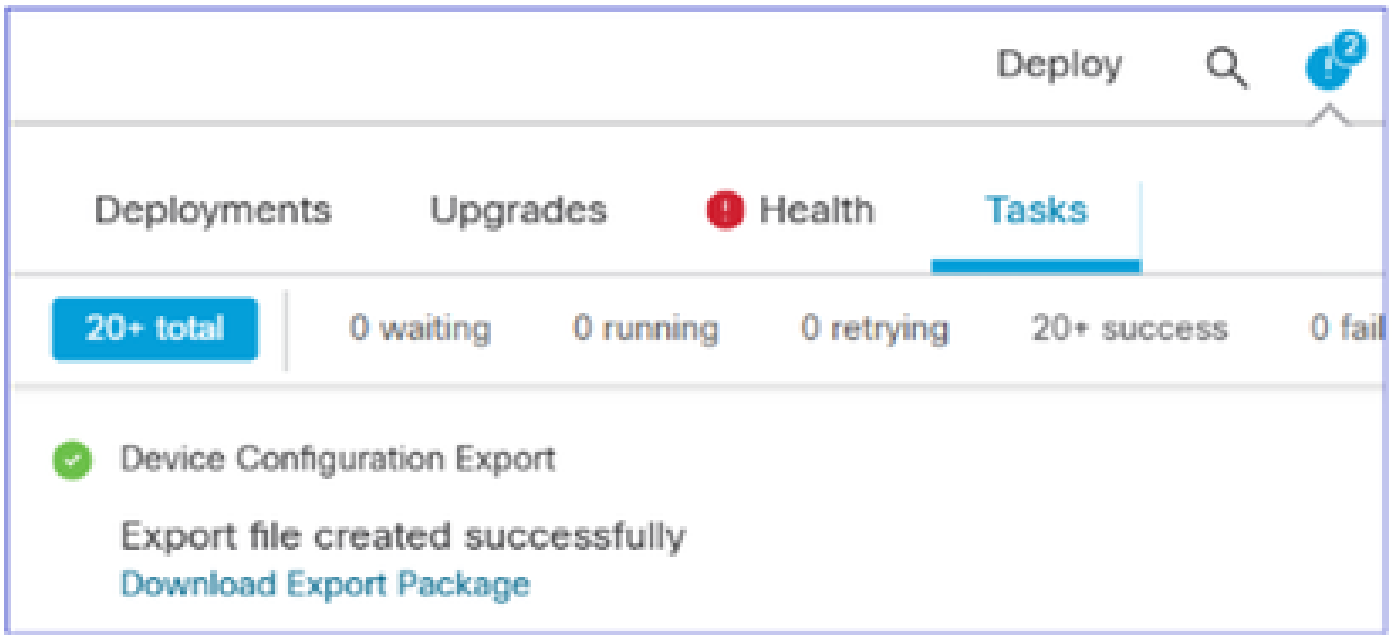


导航到Device选项卡。确保选中Primary/Active FTD（本例中为FTD1），然后选择Export以导出设备配置：



注意：Export选项在7.1软件版本及更高版本中可用。

您可以导航到通知>任务页面，以确保导出已完成。然后，选择Download Export Package:



或者，也可以单击General区域中的Download按钮。您将获得sfo文件，例如DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

该文件包含与设备相关的配置，例如：

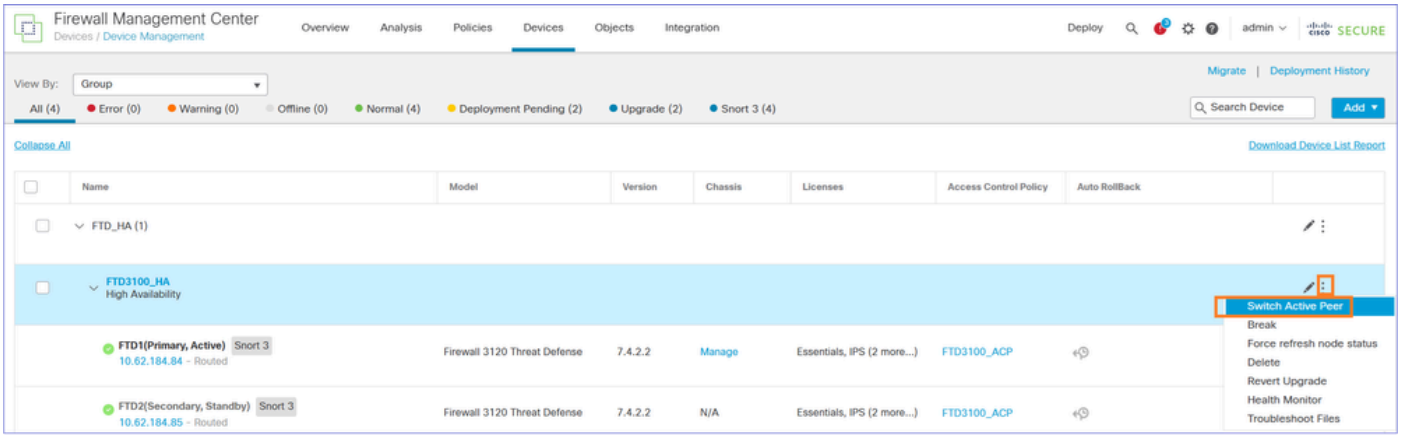
- 路由接口
- 内联集
- 路由
- DHCP
- VTEP
- 关联对象

注意：导出的配置文件只能导入回同一FTD。FTD的UUID必须与导入的sfo文件的内容匹配。同一FTD可在另一个FMC上注册，并且可导入sfo文件。

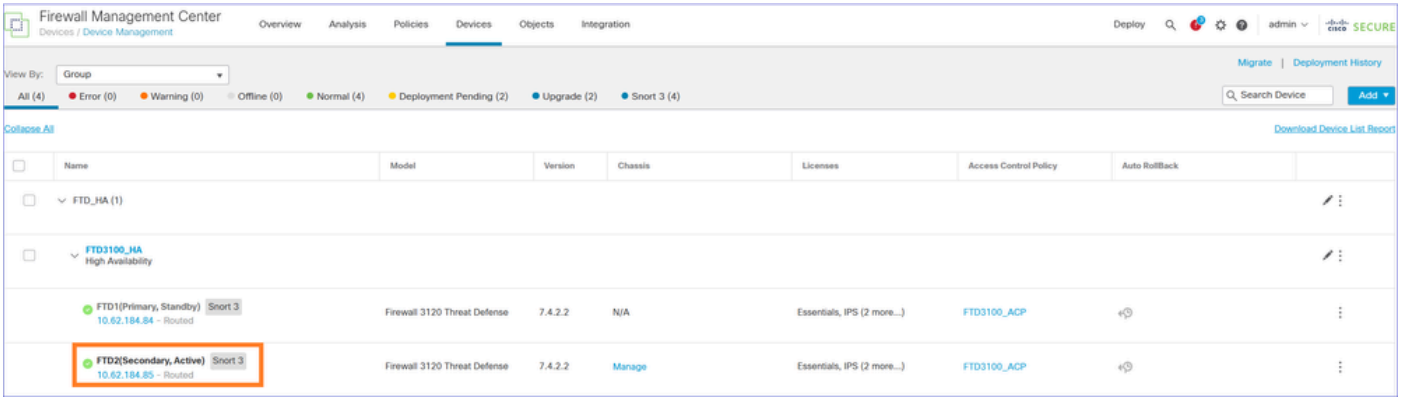
参考:'导出和导入设备配置' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

步骤2.激活辅助FTD

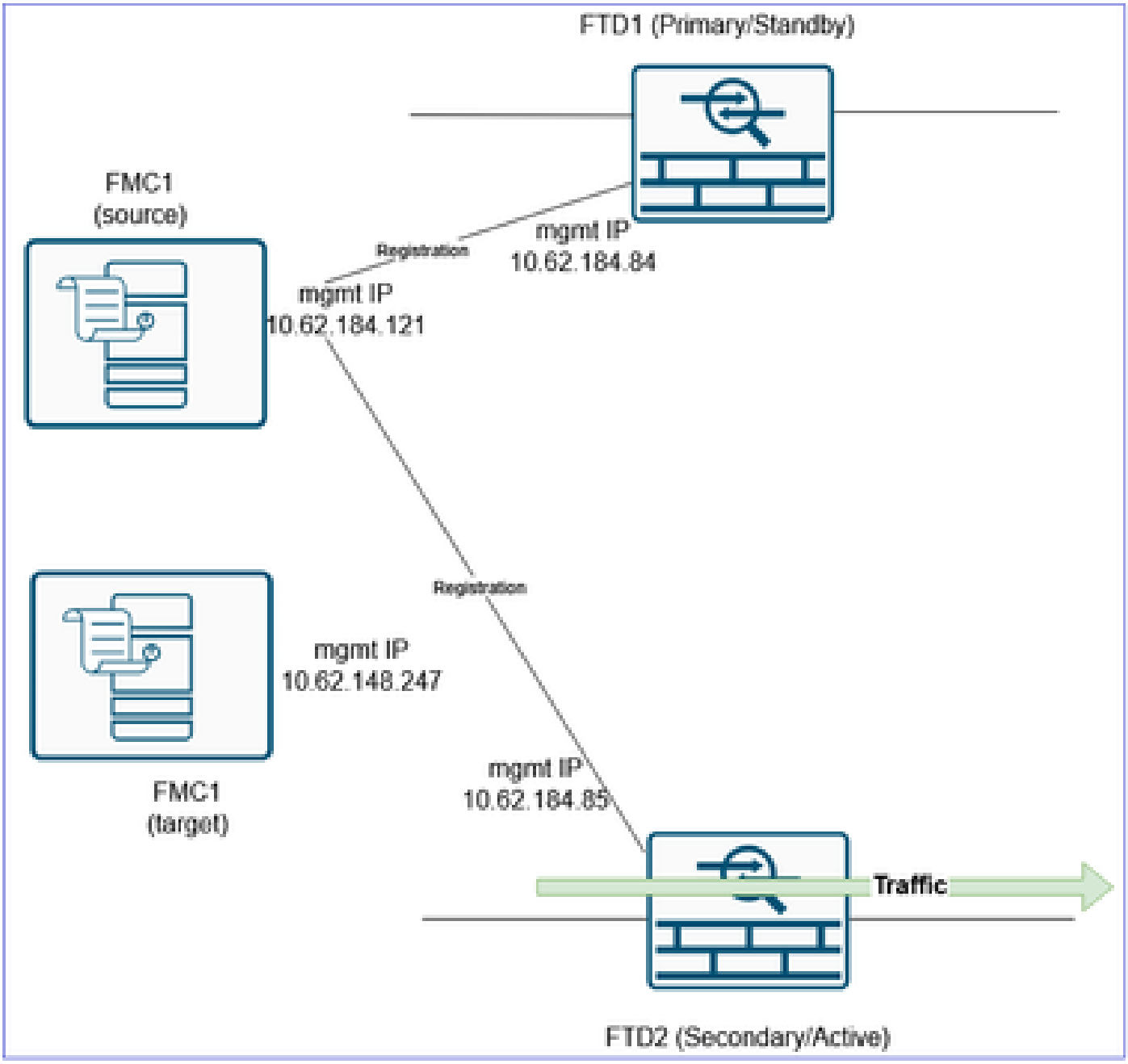
导航到Devices > Device Management，选择FTD HA对，然后选择Switch Active Pair:



结果是FTD1（主/备用）和FTD（辅助/主用）：

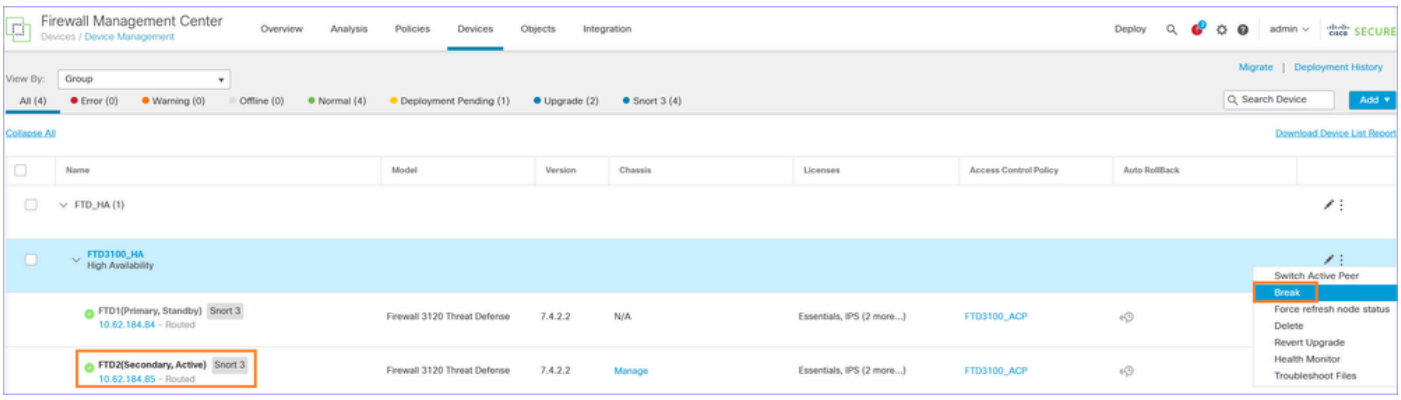


现在流量由辅助/主用FTD处理：

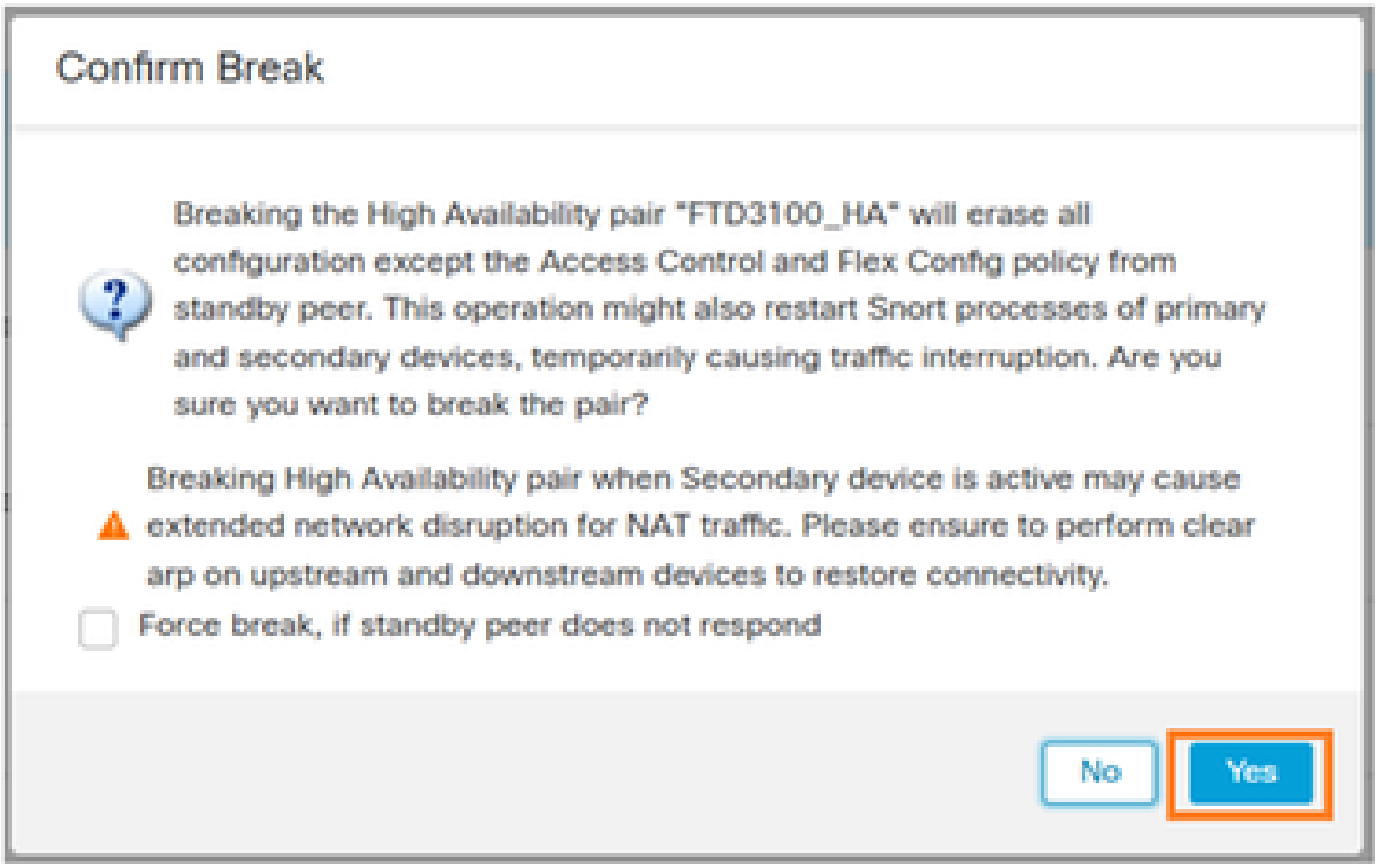


步骤3.中断FTD HA

导航到设备>设备管理并中断FTD HA:



此窗口出现。选择“是”



注意：此时，由于Snort引擎在高可用性中断期间重新启动，您可能会遇到几秒钟的流量中断。此外，如消息所述，如果使用NAT并遇到长时间流量中断，请考虑清除上游和下游设备上的ARP缓存。

中断FTD HA后，FMC上有两个独立FTD。

从配置角度来看，除故障切换相关配置外，FTD2(ex-Active)仍然具有配置，并且正在处理流量：

```
<#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（非备用）删除了所有配置：

<#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>

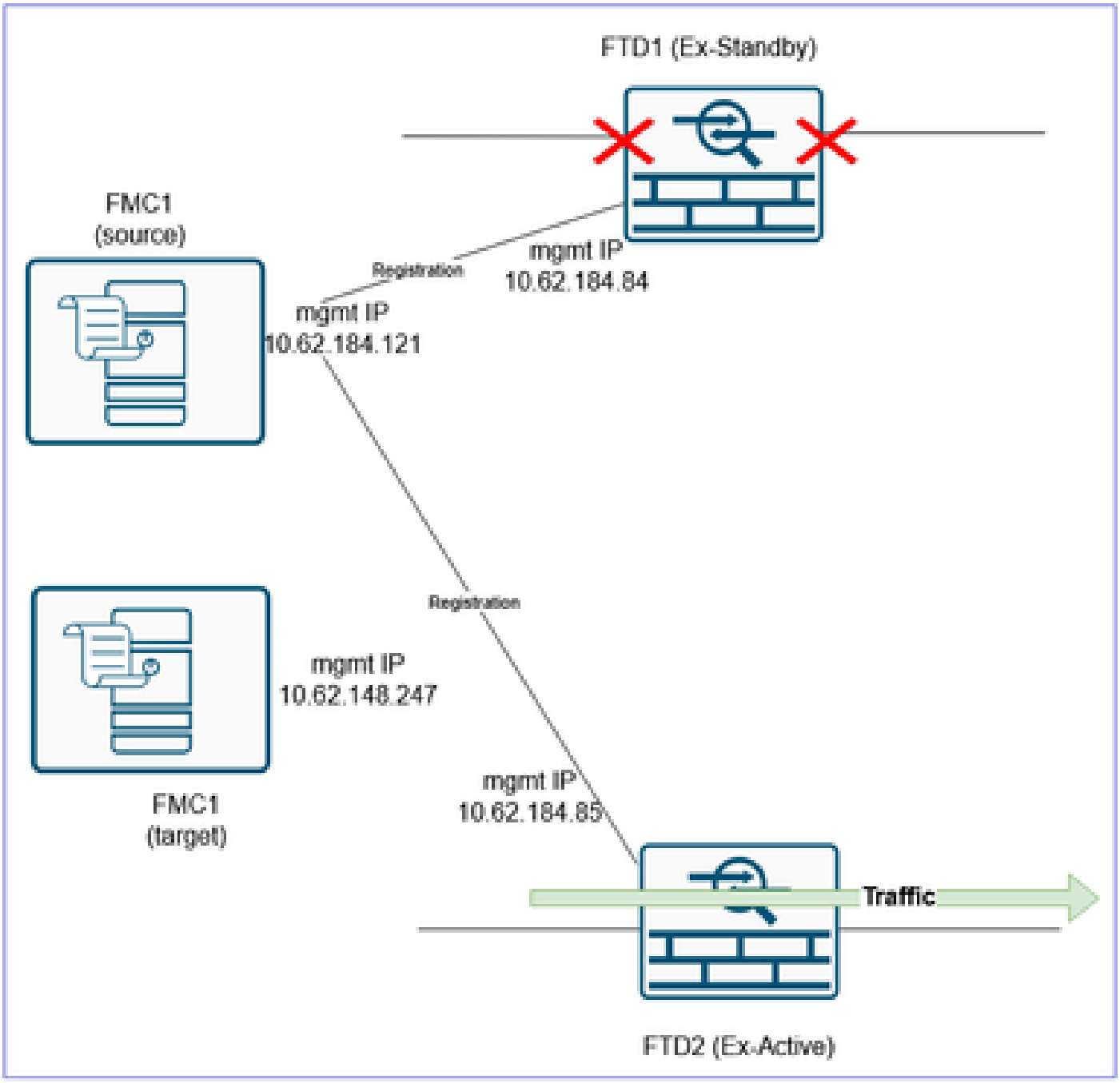
FTD3100-3#

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
```

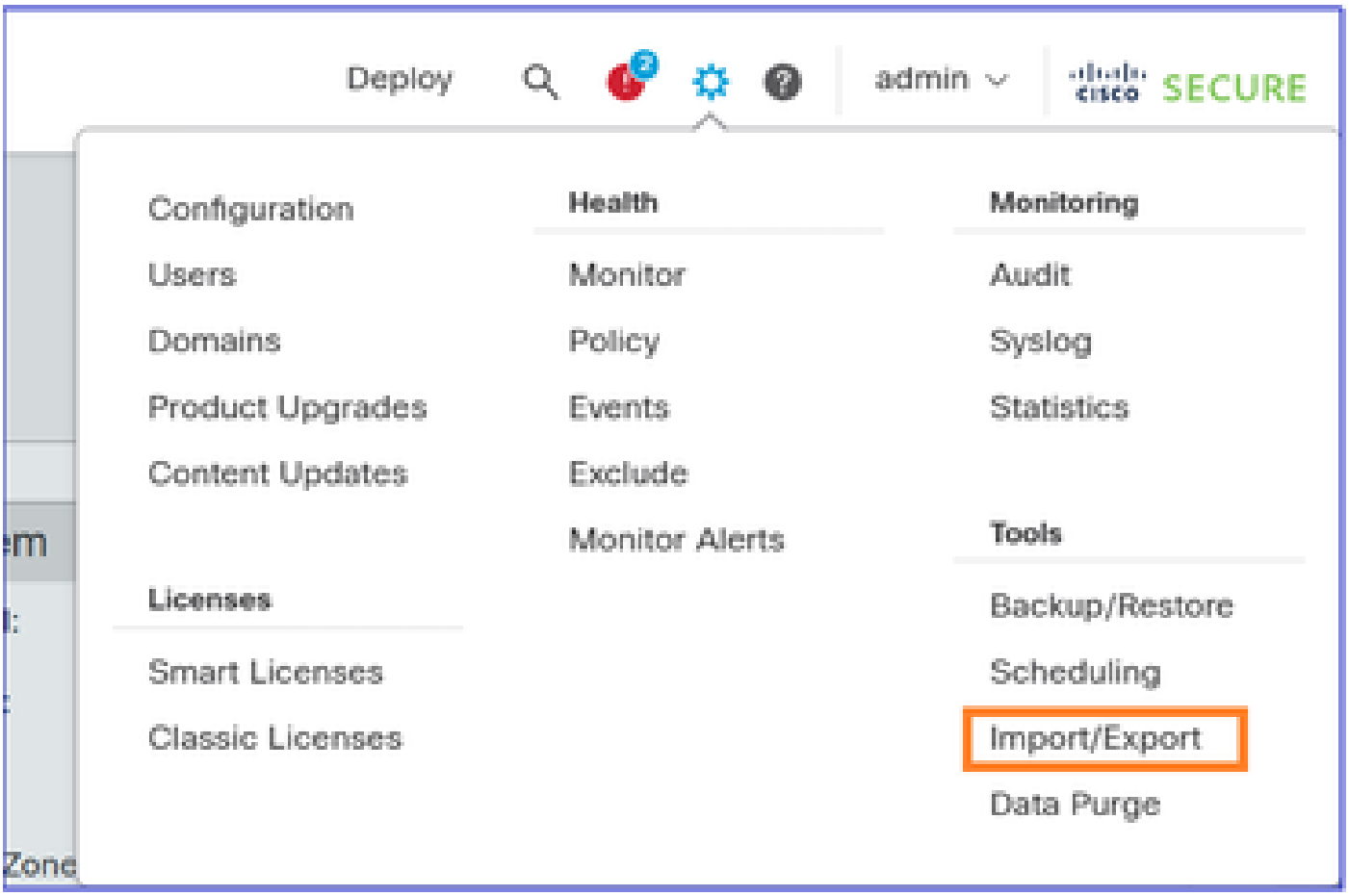
步骤4.隔离FTD1（非主要）数据接口

从FTD1(除主设备)断开数据电缆。 只连接FTD管理端口。



步骤5.导出FTD共享策略

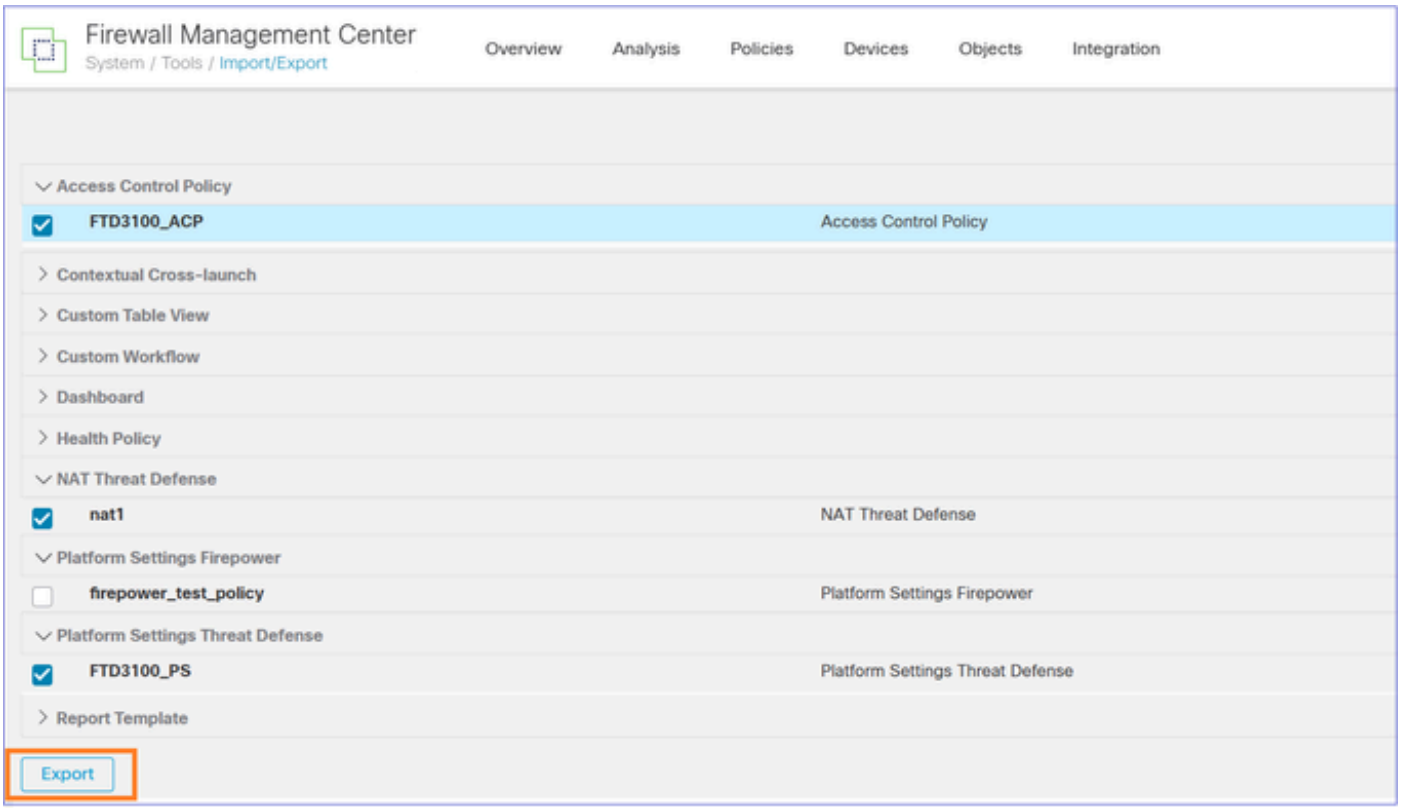
导航到System > Tools，然后选择Import/Export:



导出附加到设备的各种策略。确保导出附加到FTD的所有策略，例如：

- 访问控制策略(ACP)
- 网络地址转换(NAT)策略
- 运行状况策略（如果自定义）
- FTD平台设置

等等。



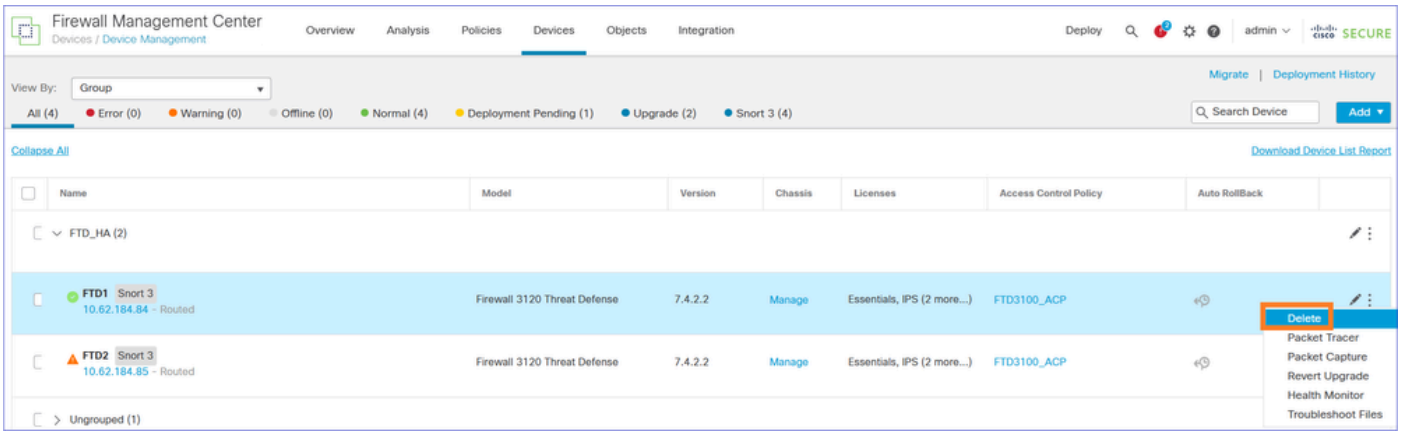
注意：在撰写本文时，不支持导出VPN相关的配置。设备注册后，您需要在FMC2（目标FMC）上手动重新配置VPN。

相关增强功能Cisco Bug ID CSCwf05294

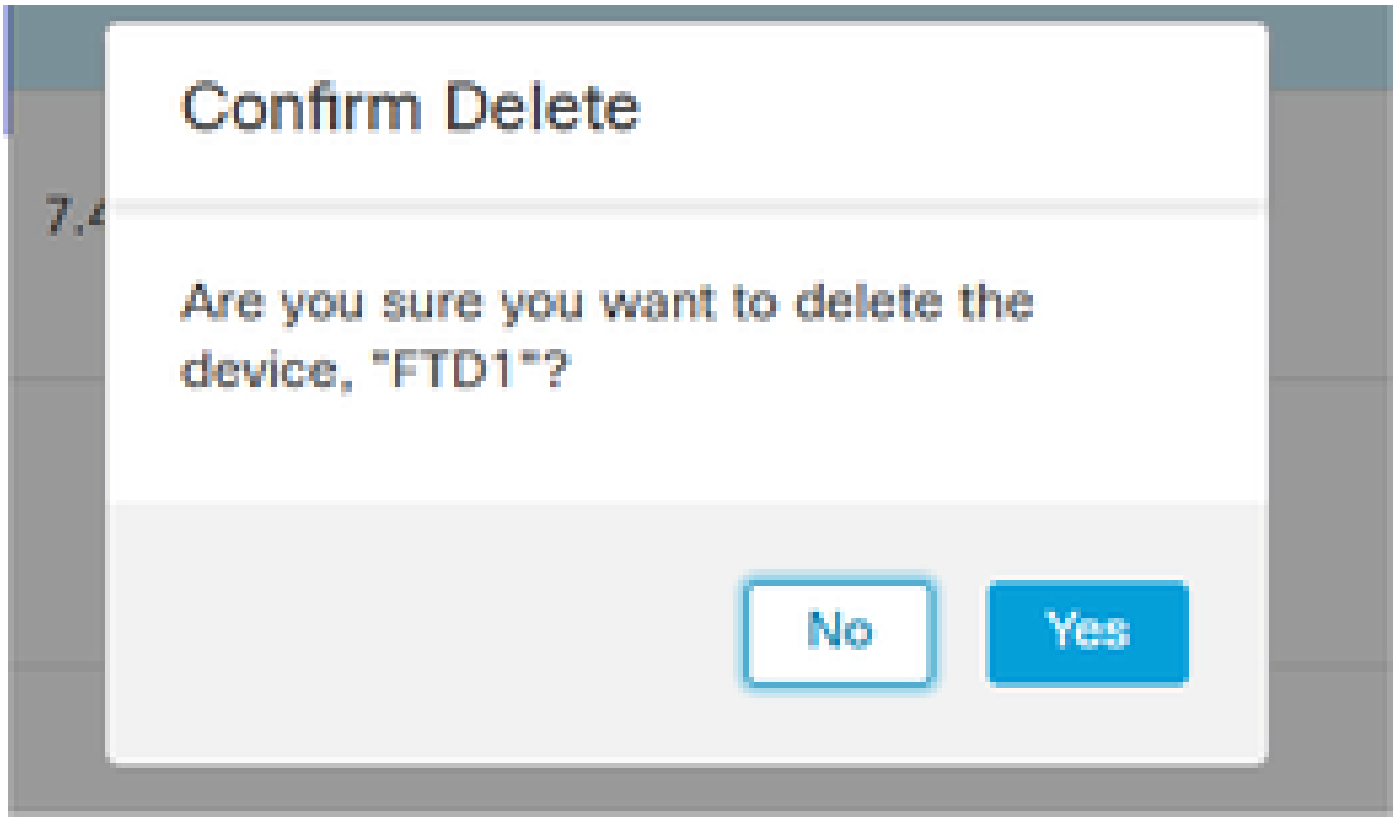
.

结果是一个.sfo文件，例如ObjectExport_20250306082738.sfo

步骤6.从旧/源FMC中删除/注销FTD1（非主要）



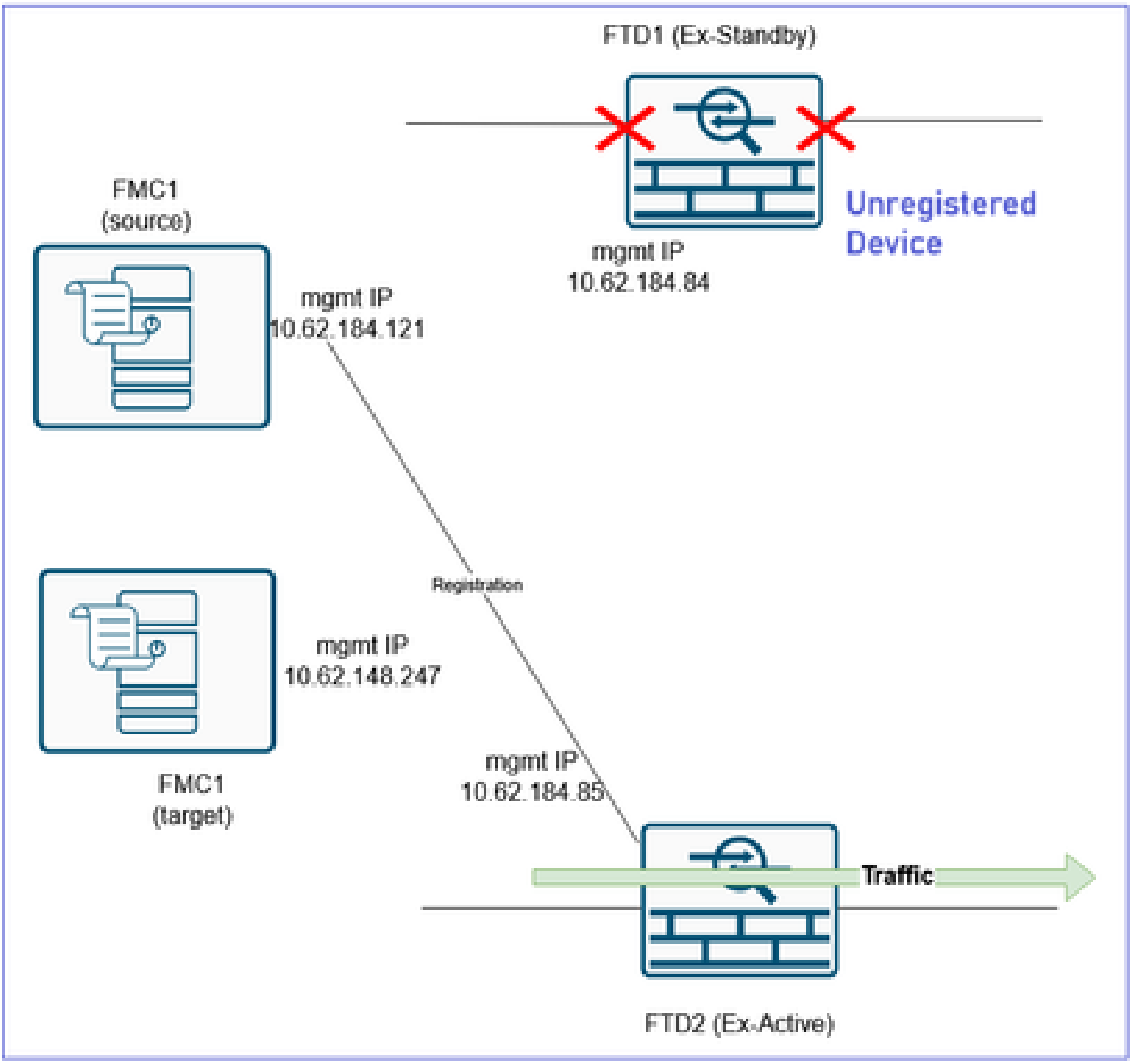
确认设备删除：



FTD1 CLI验证：

```
<#root>

>

show managers

No managers configured.

>
```

FTD1设备删除后的当前状态：



步骤7.将FTD策略配置对象导入FMC2（目标FMC）

注意：本文档重点介绍单个FTD HA对到新FMC的迁移。另一方面，如果您计划迁移多个共享相同策略（例如，ACP、NAT）和对象的防火墙，并且希望分阶段进行迁移，则需要考虑这些点。

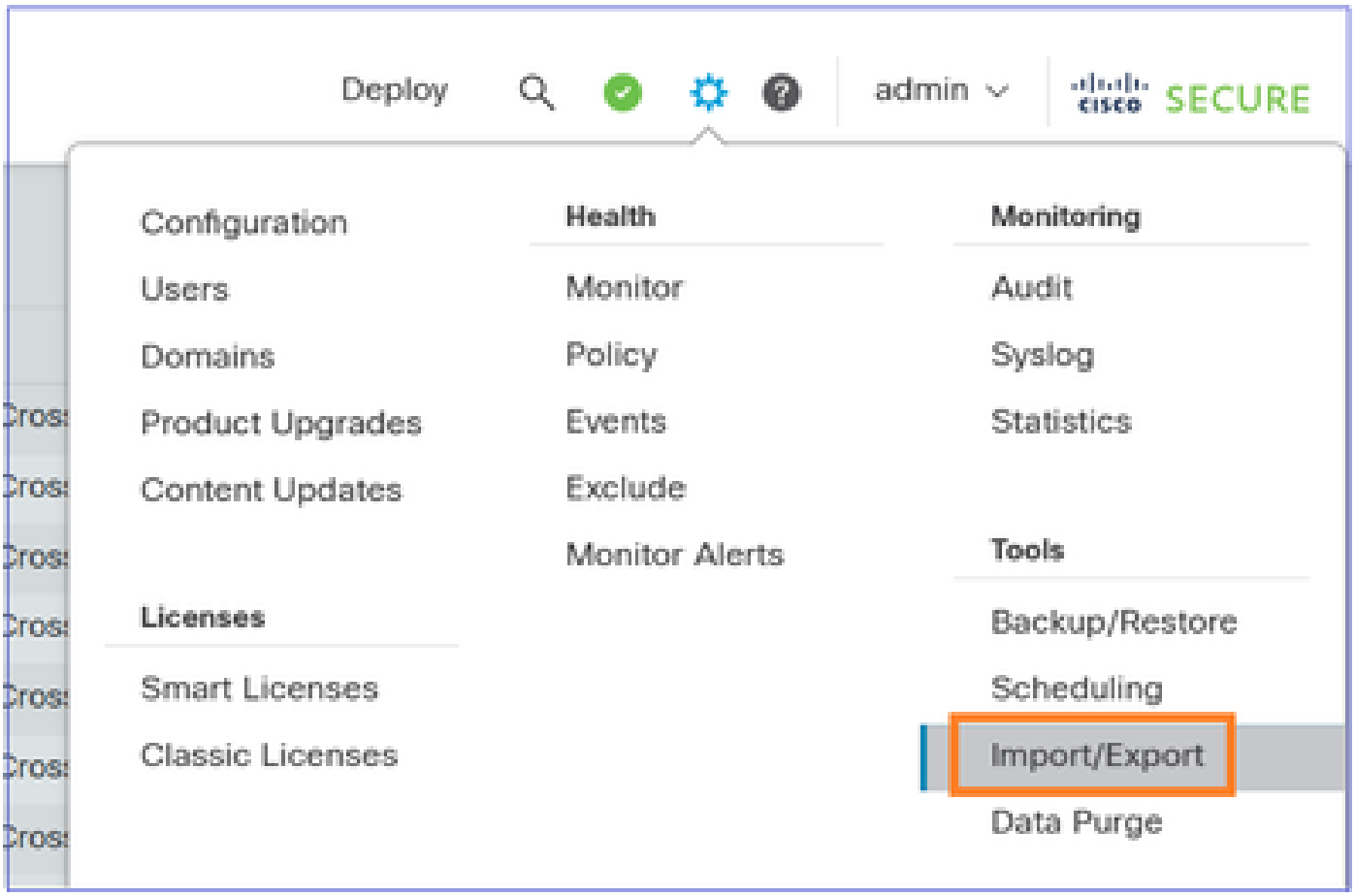
— 如果目标FMC上存在具有相同名称的现有策略，系统会询问您是否：

a.要替换策略或

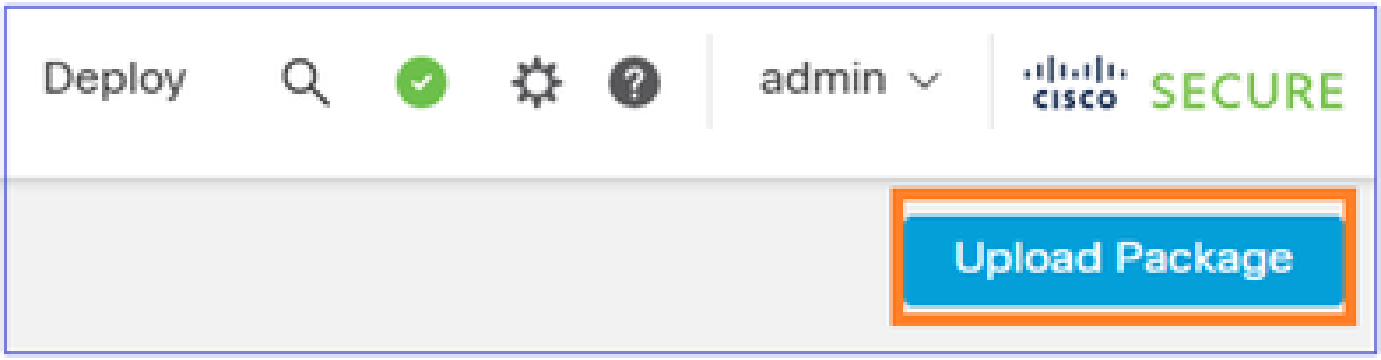
b.使用其他名称创建新名称。这将创建具有不同名称（后缀_1）的重复对象。

— 如果您使用选项“b”，则在第9步中，请确保将新创建的对象重新分配到迁移的策略（ACP安全区域、NAT安全区域、路由、平台设置等）。

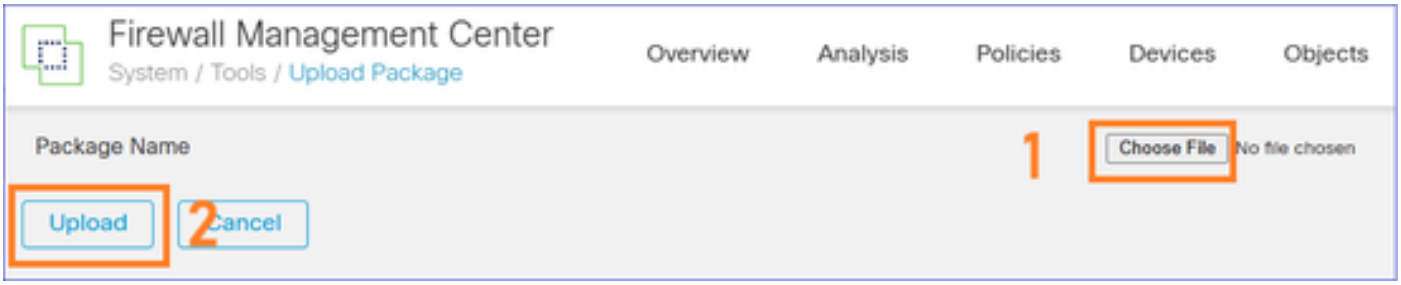
登录到FMC2（目标FMC）并导入您在第5步中导出的FTD Policies sfo对象：



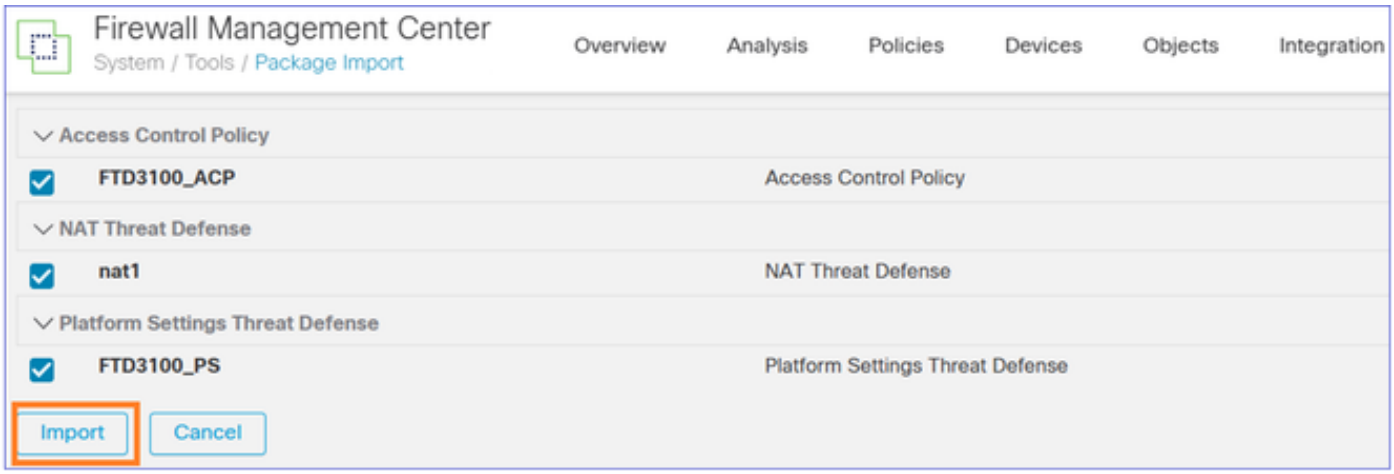
选择Upload Package:



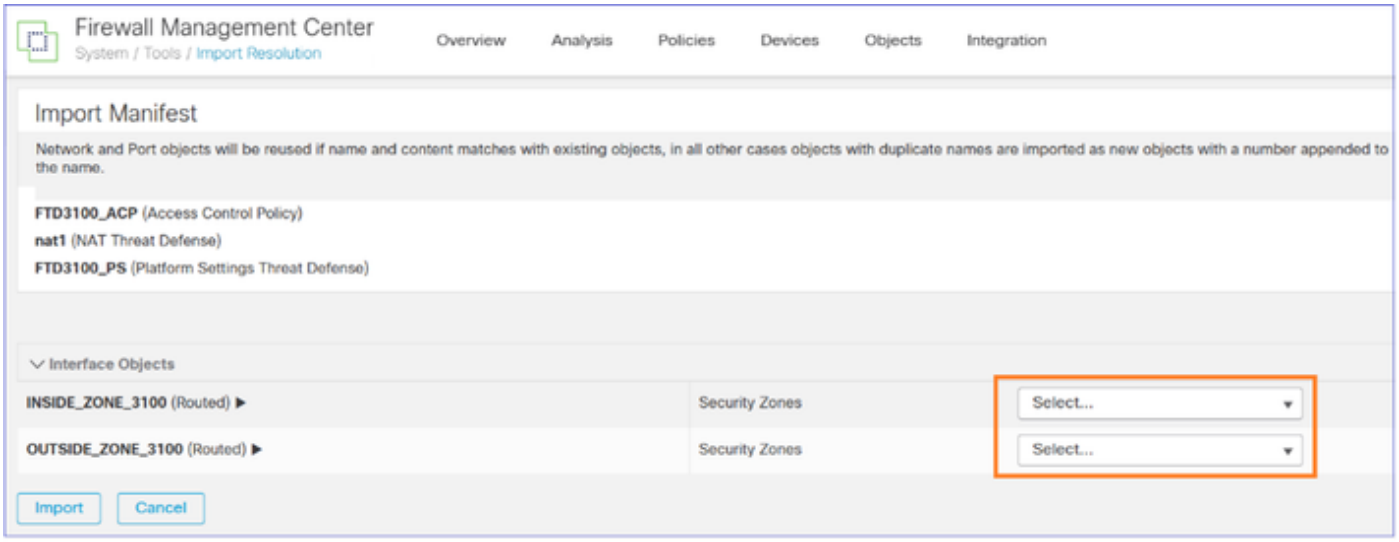
上传文件：



导入策略：



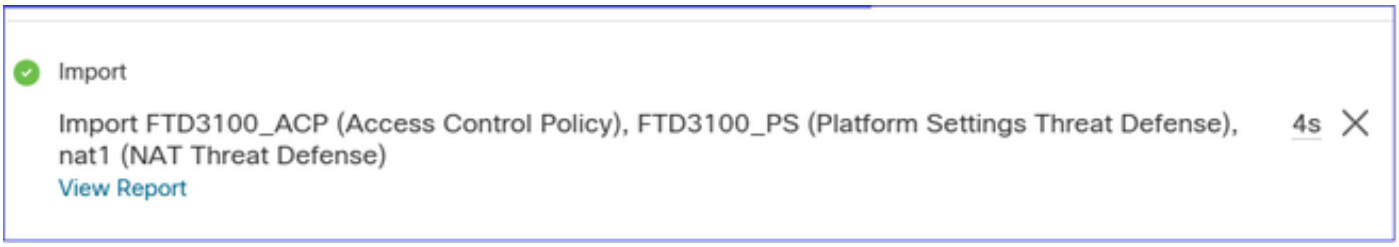
在FMC2（目标FMC）上创建接口对象/安全区域：



您可以为FMC1（源FMC）提供相同的名称：

选择Import后，任务开始将相关策略导入FMC2（目标FMC）：

任务完成：

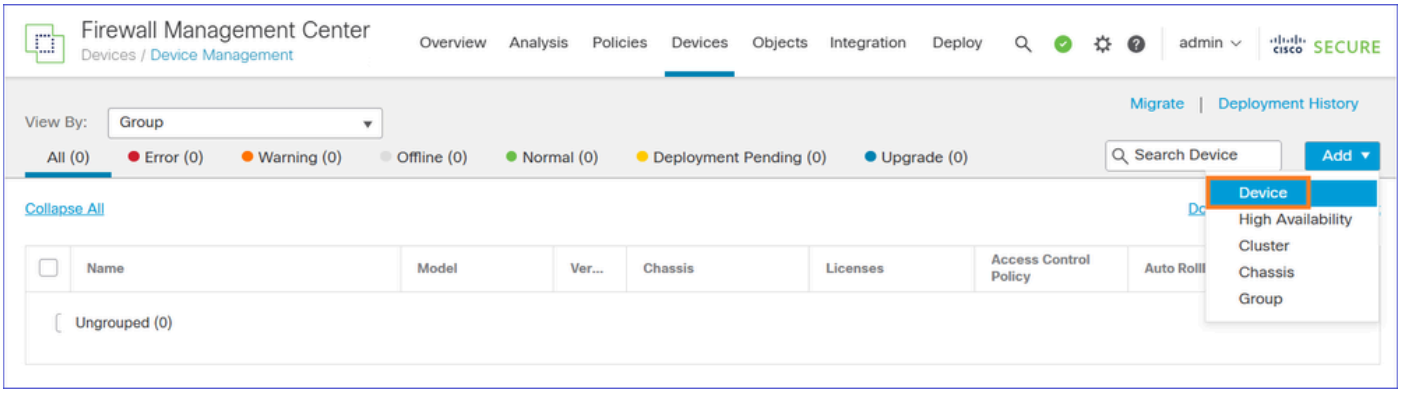


步骤8.将FTD1（非主要）注册到FMC2

转到FTD1（非主）CLI并配置新管理器：

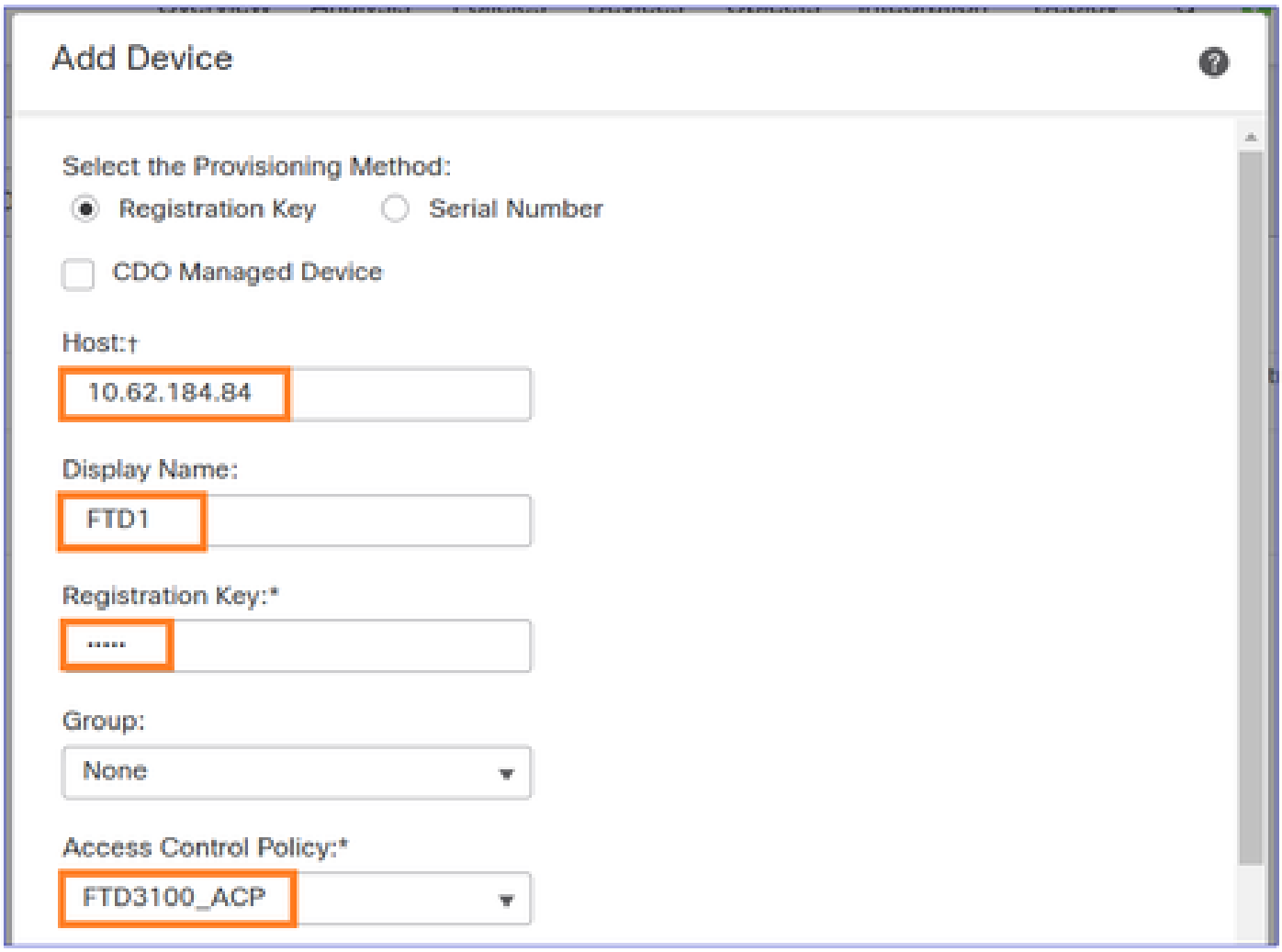
```
<#root>

>

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.

>
```

导航至FMC2（目标FMC）UI Devices > Device Management和Add the FTD device:

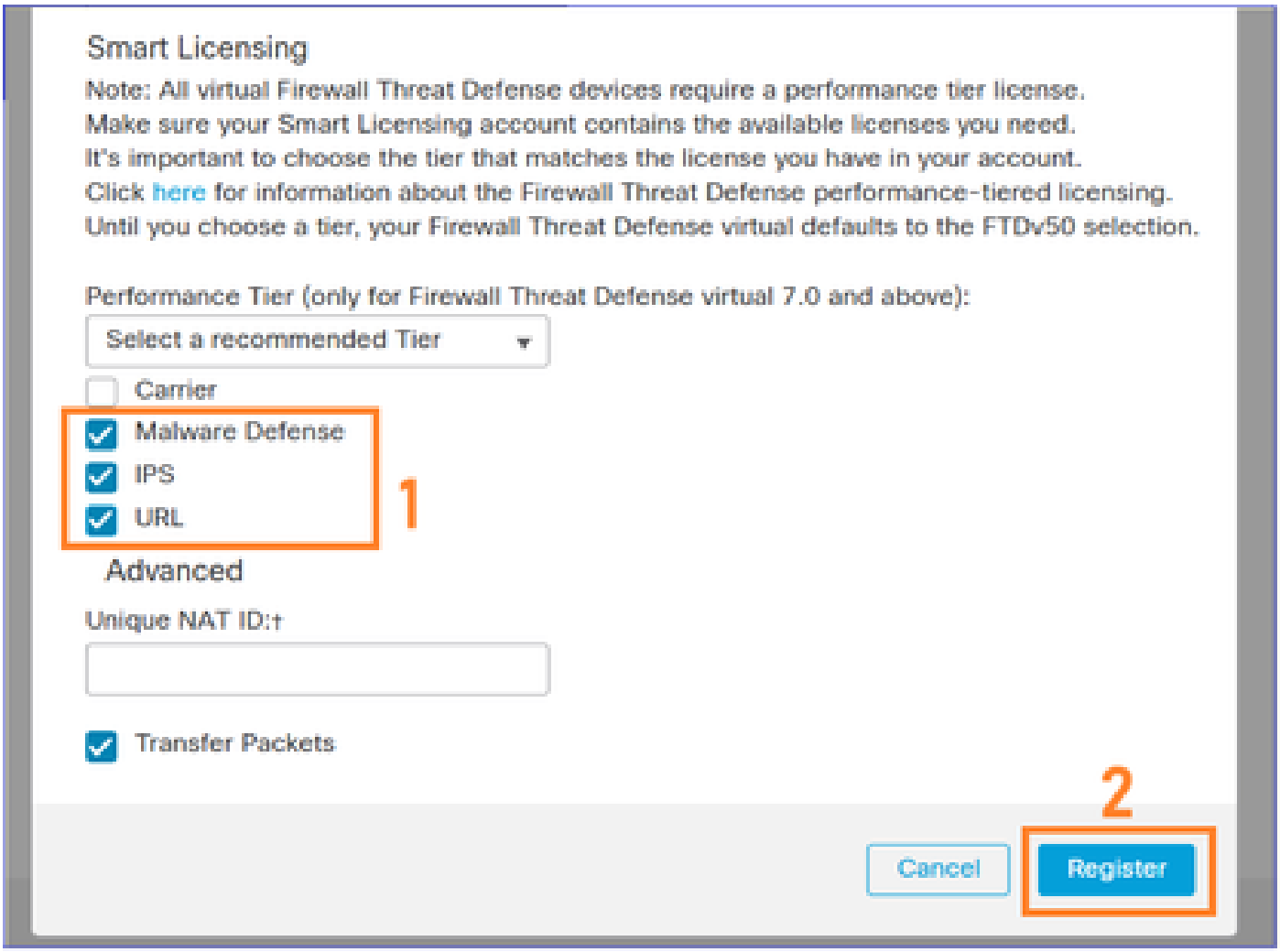


如果设备注册失败，请参阅本文档以解决问题：https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

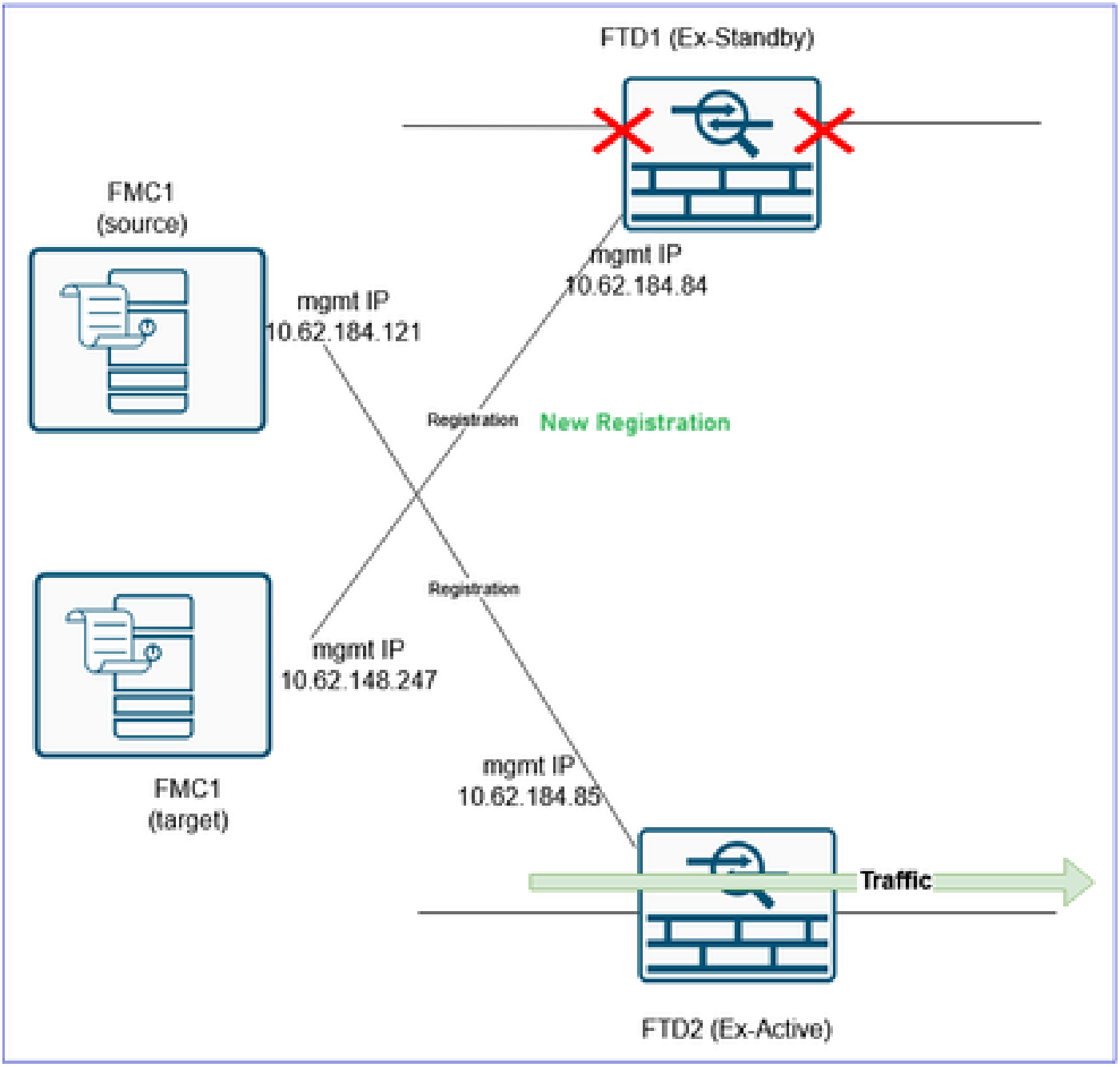
分配在上一步中导入的访问控制策略：



应用所需的许可证并注册设备：


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

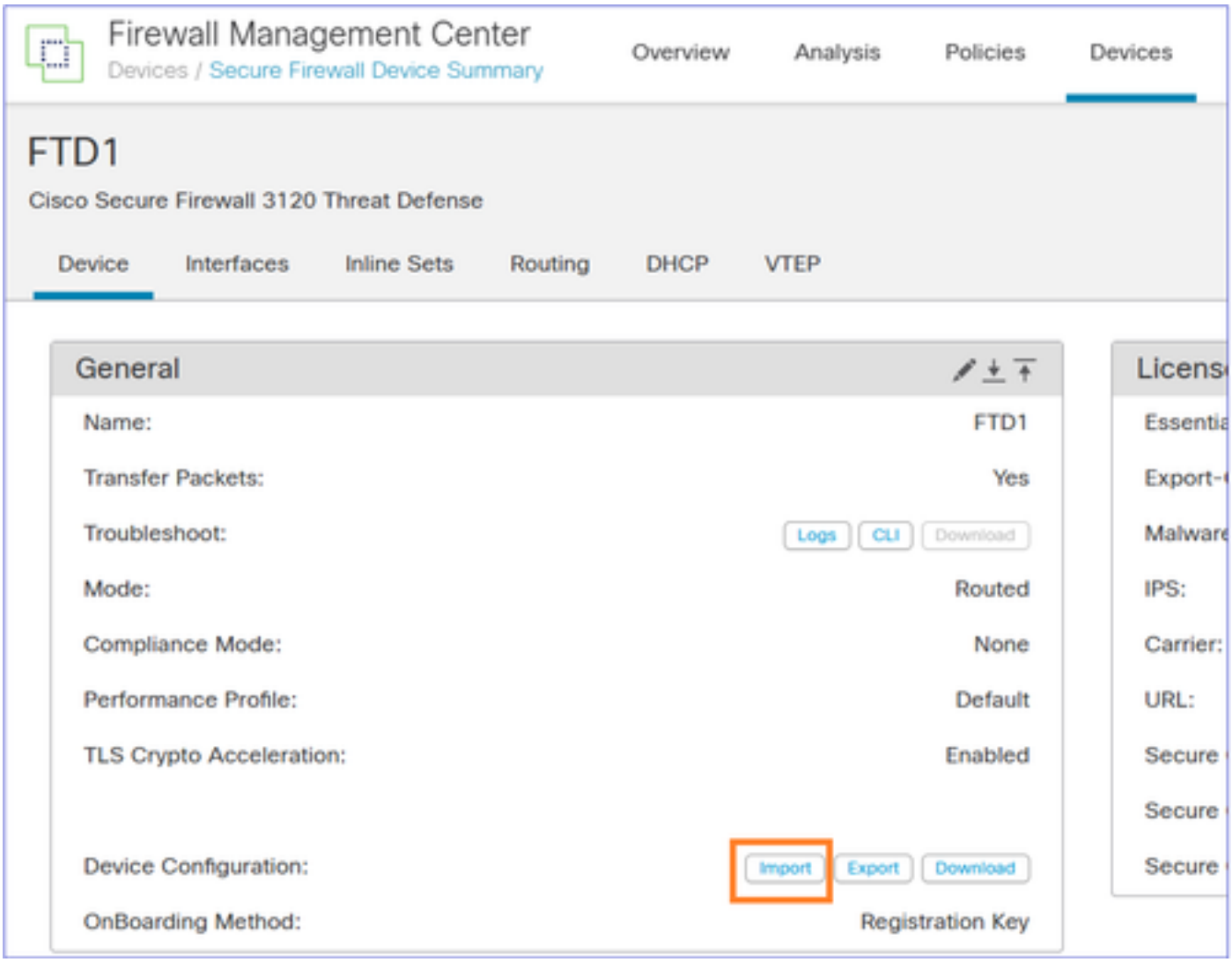
结果：



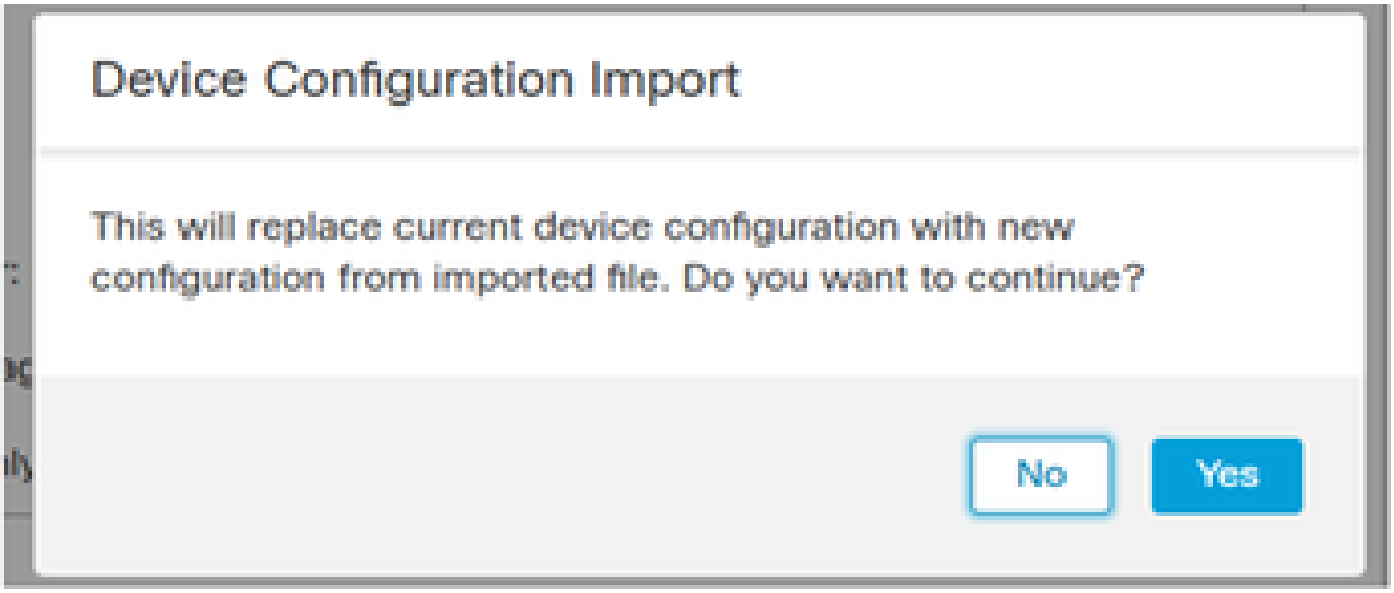
步骤9.将FTD设备配置对象导入FMC2（目标FMC）

登录FMC2（目标FMC），导航至Devices > Device Management和Edit在上一步中注册的FTD设备。

导航到Device选项卡和Import FTD Policies对象，该对象是在步骤2中导出的：

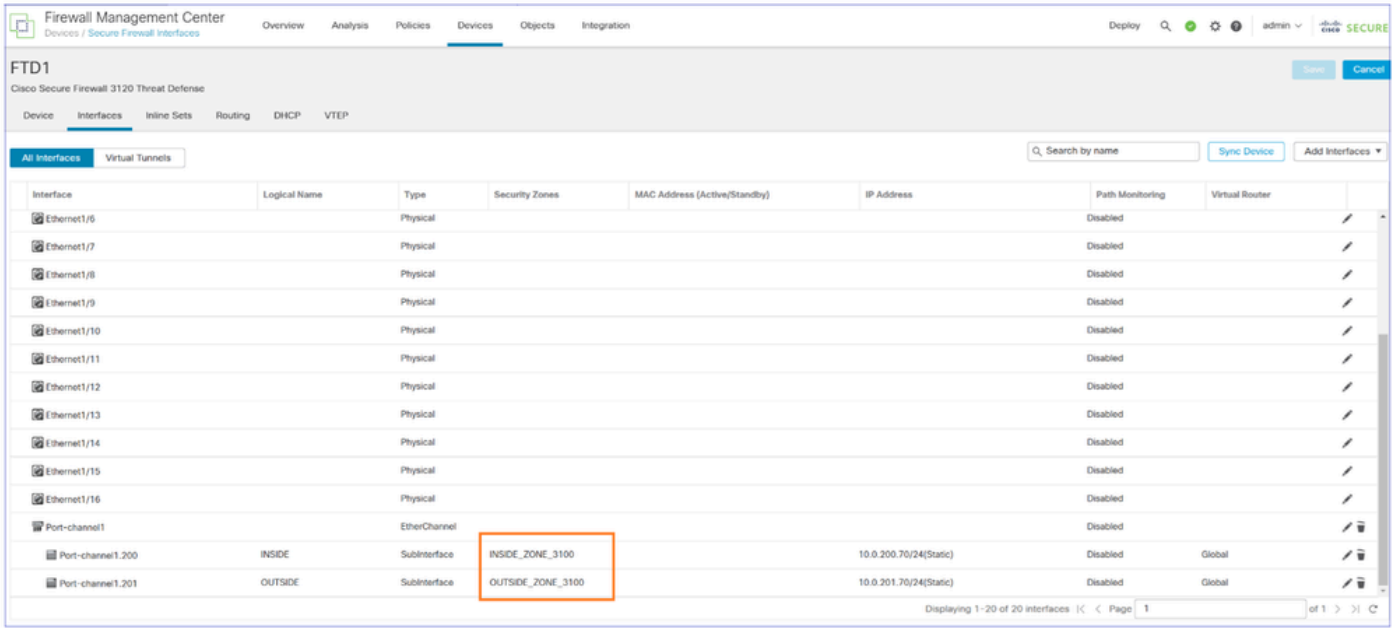


注意：如果在第7步中选择了选项“b”（创建新策略），请确保将新创建的对象重新分配到迁移的策略（ACP安全区域、NAT安全区域、路由、平台设置等）。



FMC任务已启动。

设备配置应用在FTD1上，例如安全区域、ACP、NAT等：



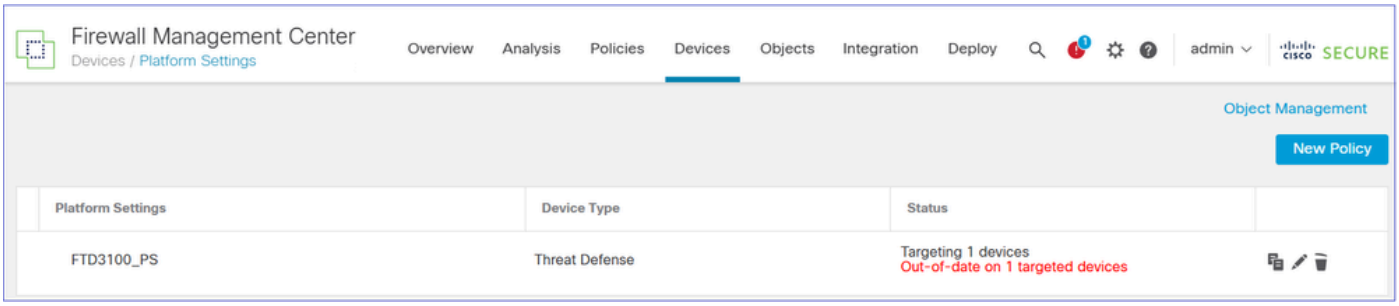
⚠ 警告：如果您的ACP扩展到了许多访问控制元素，则ACP编译过程(tmatch compile)可能需要几分钟才能完成。您可以使用此命令验证ACP编译状态：

```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

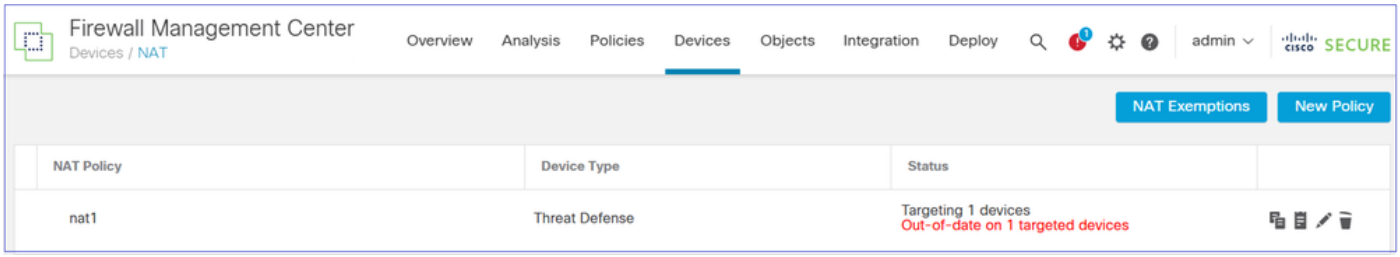
步骤10.完成FTD配置

此时，目标是配置注册到FMC2（目标FMC）并导入设备策略后FTD1中仍可能缺少的所有功能。确保NAT、平台设置、QoS等策略。分配给FTD。您会看到已分配策略，但部署处于挂起状态。

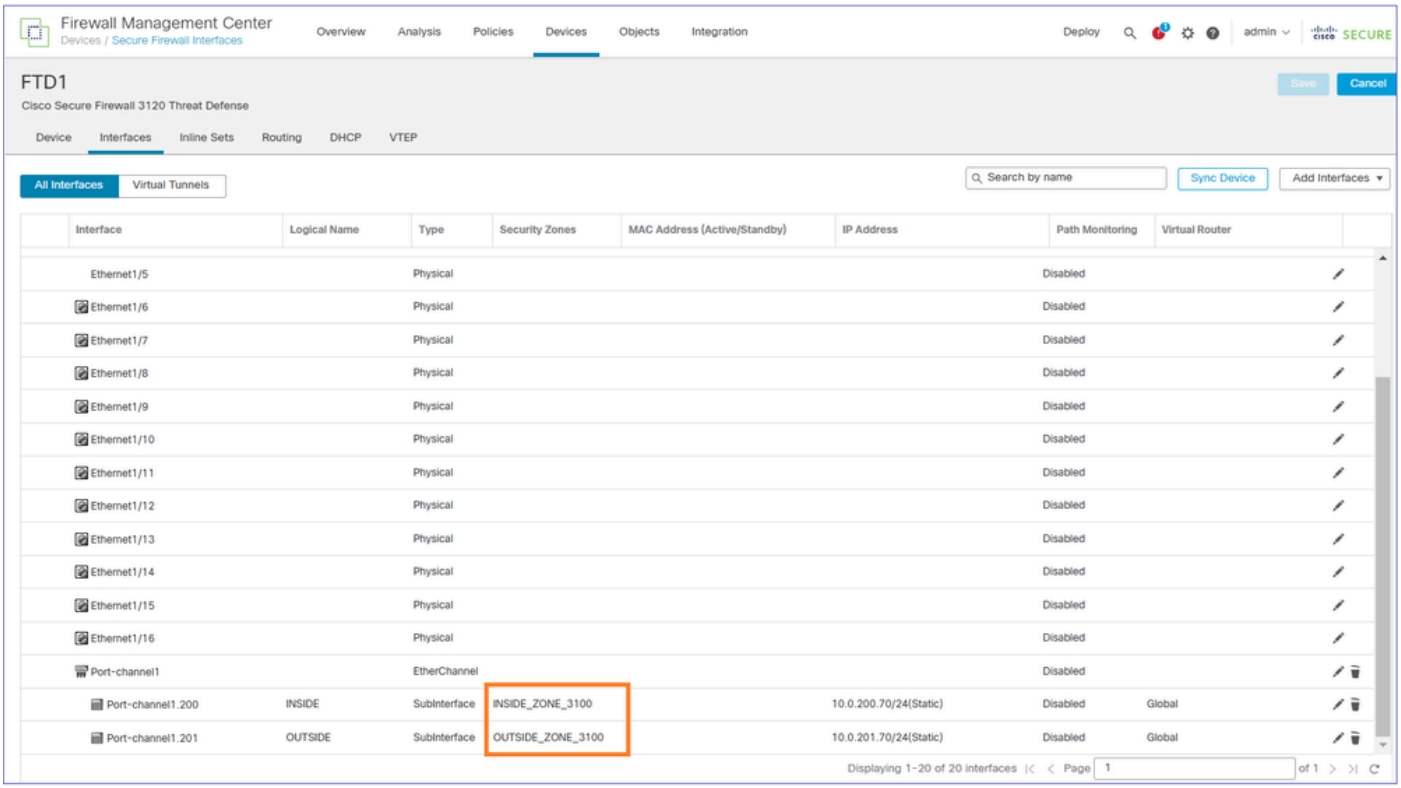
例如，平台设置已导入并分配到设备，但部署处于挂起状态：



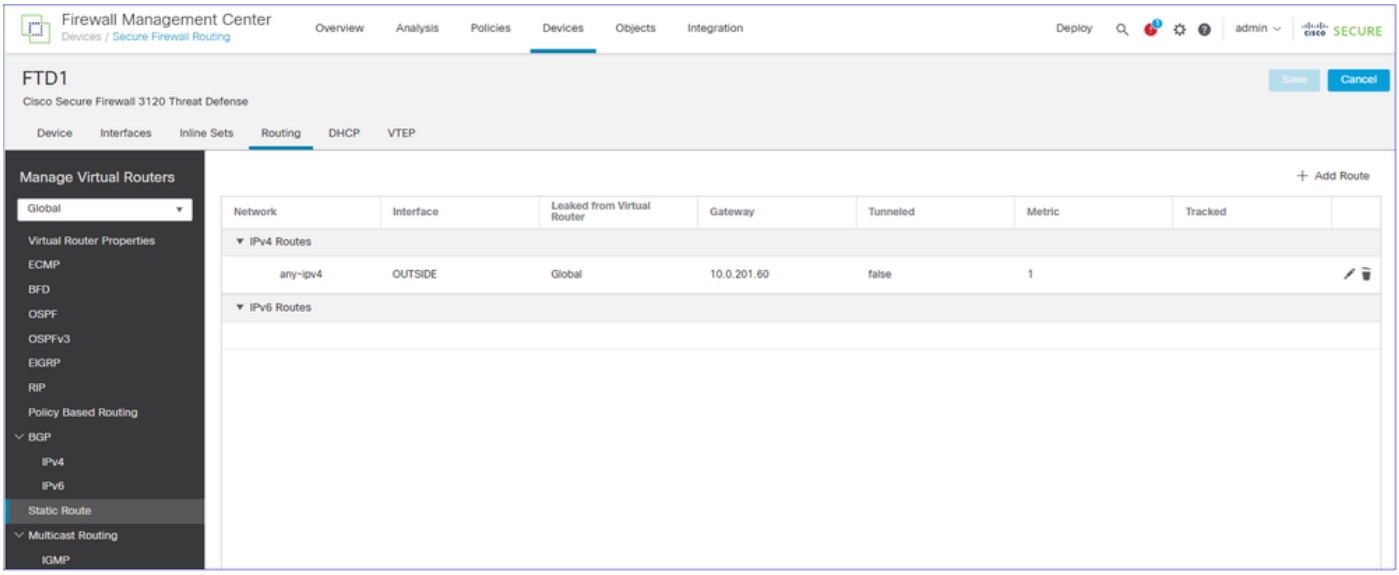
如果配置了NAT，则会导入NAT策略并将其分配给设备，但会等待部署：



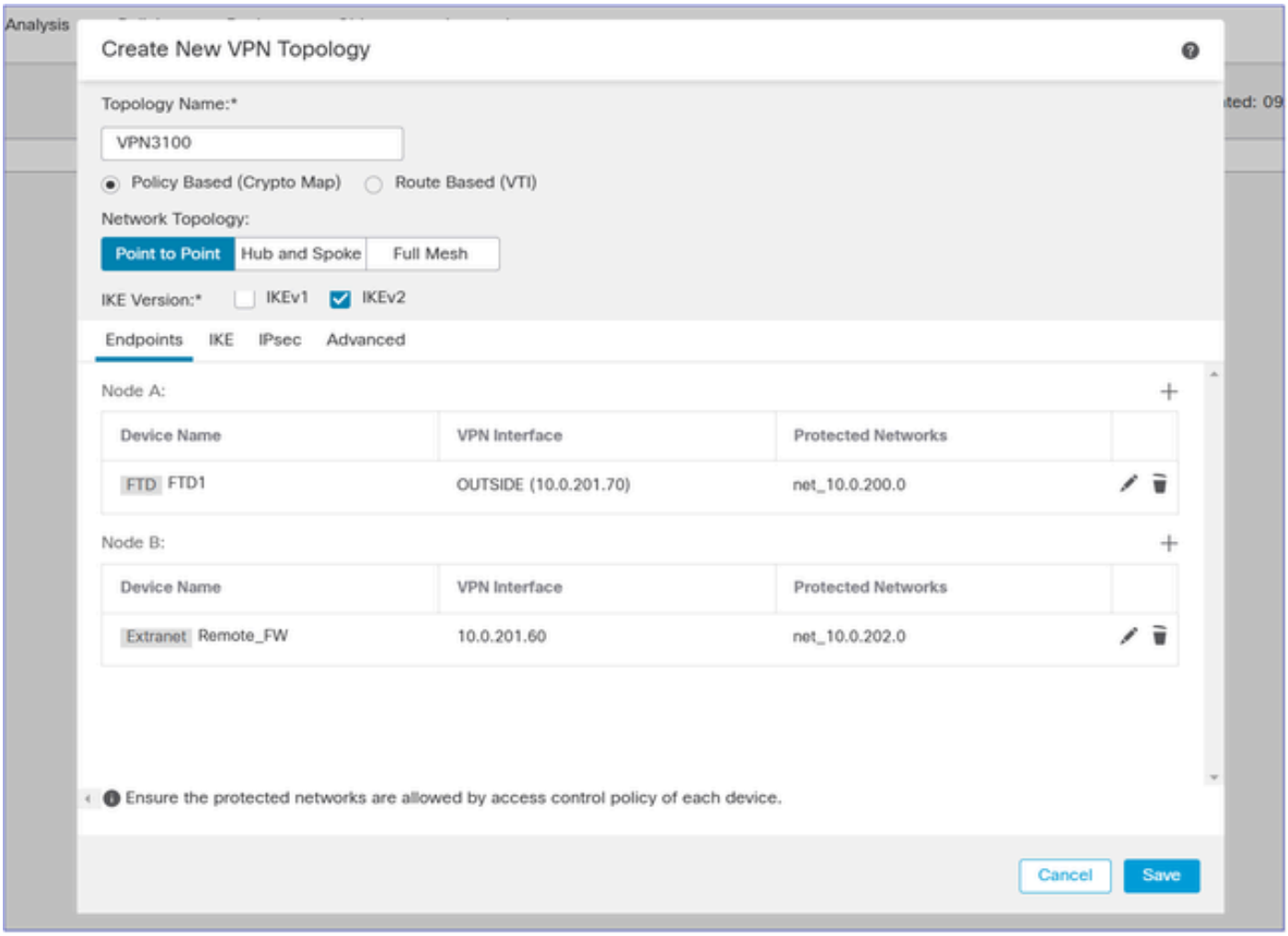
安全区域应用于接口：



路由配置应用到FTD设备：

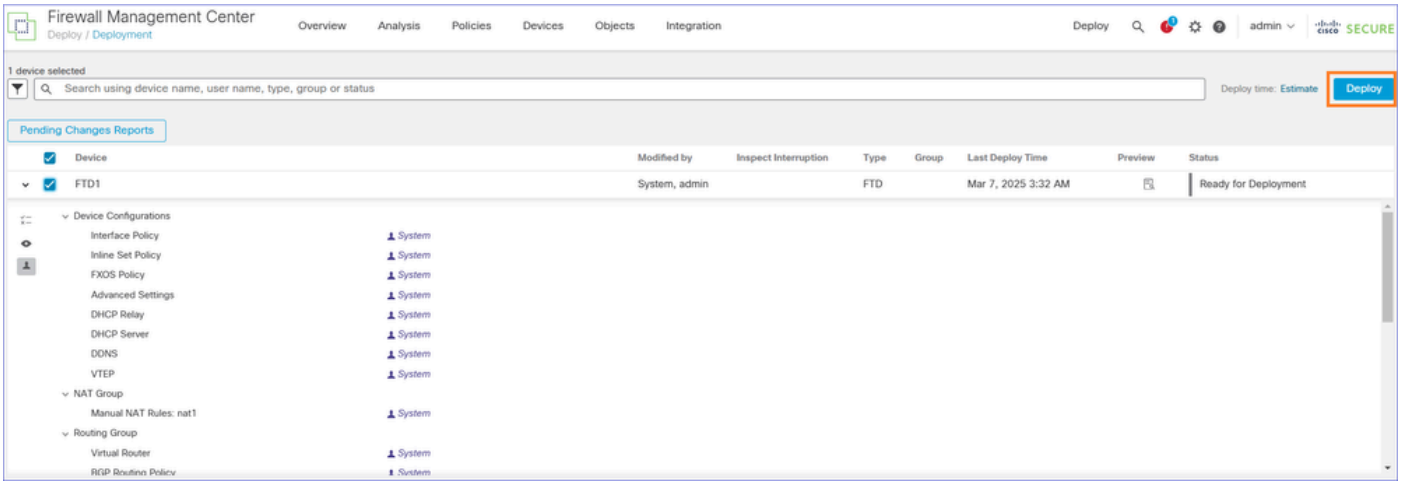


注意：现在是配置无法自动迁移的策略（例如VPN）的时候了。



注意：如果迁移的FTD具有也迁移至目标FMC的S2S VPN对等点，则必须在将所有FTD移至目标FMC后配置VPN。

部署待处理的更改：



步骤11.检验已部署的FTD配置

此时，目标是从FTD CLI检查所有配置都已就位。

建议比较两个FTD的“show running-config”输出。可以使用WinMerge或diff等工具进行比较。

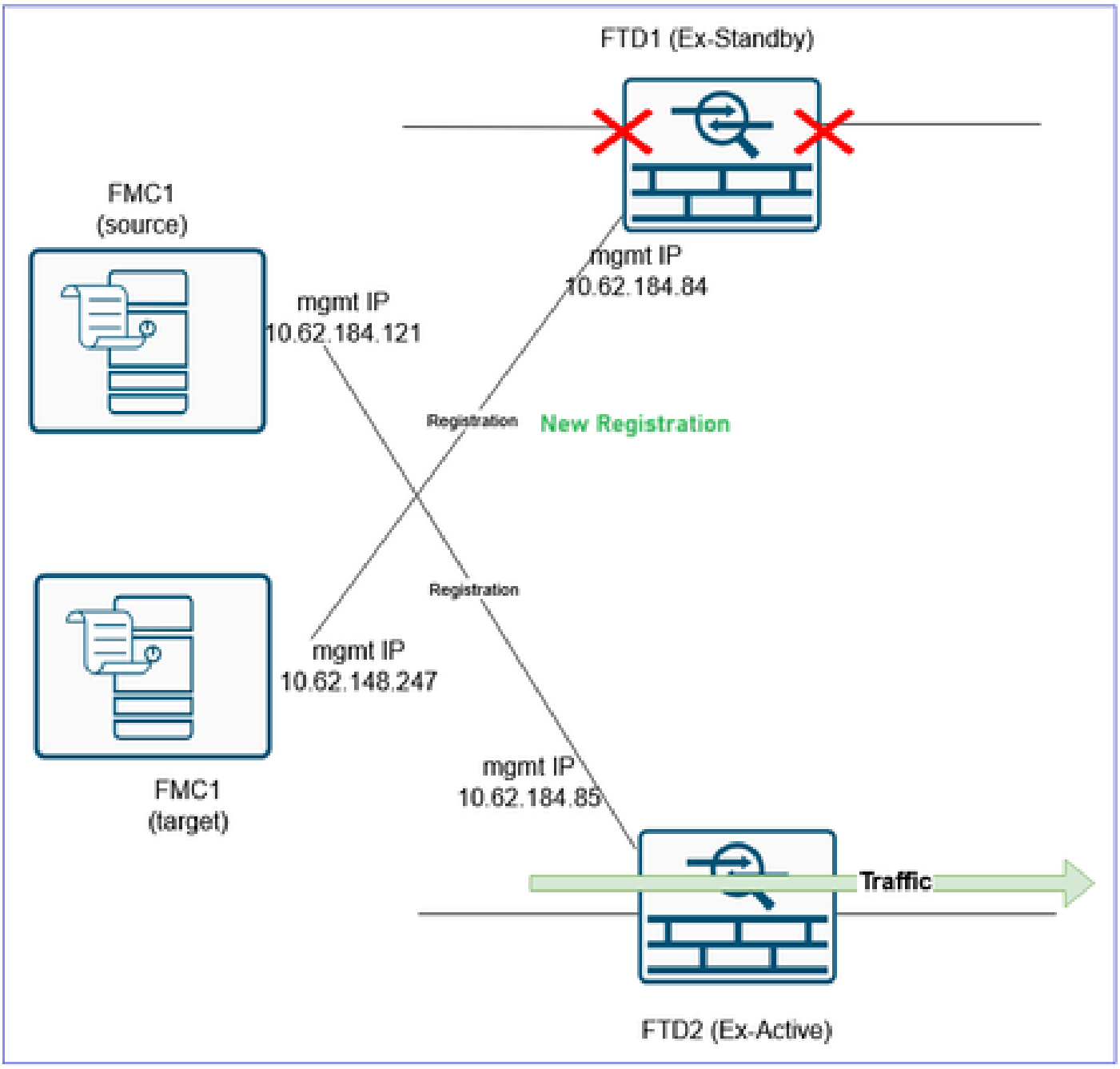
您看到的和正常的区别包括：

- 设备序列号
- 接口描述
- ACL规则ID
- 配置加密校验和

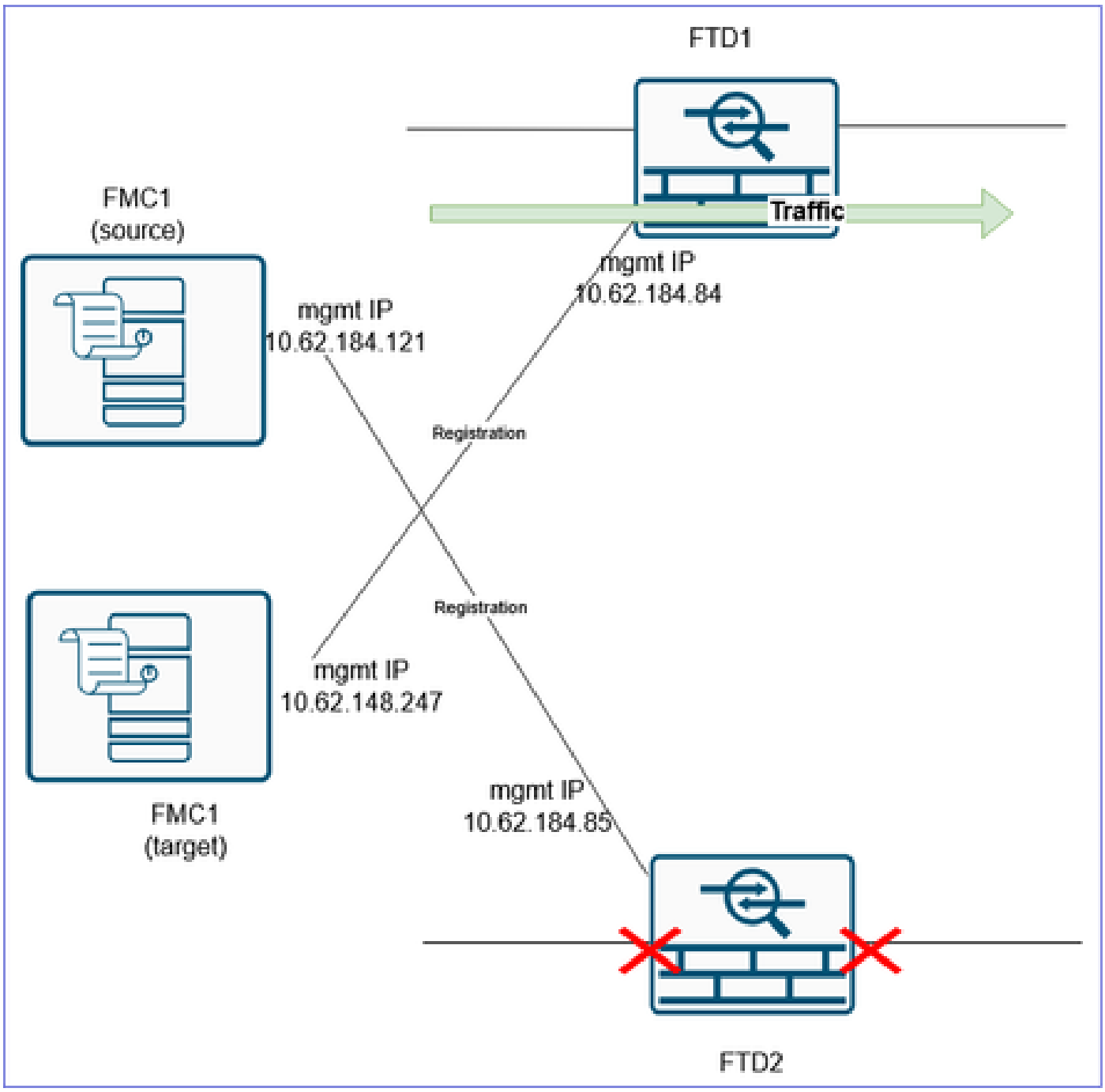
步骤12.执行切换

在此步骤中，目标是将流量从当前处理流量且仍注册到旧/源FMC的FTD2切换到注册到目标FMC的FTD1。

攻击前：


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)

在:



⚠ 警告：安排MW进行转换。切换期间，您会遇到一些流量中断，直到所有流量都转移到FTD1,VPN重新建立，等等。

⚠ 警告：除非ACP编译完成，否则请勿启动切换（参见上述步骤10）。

⚠ 警告：确保从FTD2断开数据电缆或者关闭相关的交换机端口。否则，您最终可能使用两台设备处理流量！

⚠ 警告：由于两台设备使用相同的IP配置，因此需要更新相邻L3设备的ARP缓存。考虑手动清除相邻设备的ARP缓存以加快流量转换。

提示：您还可以使用FTD CLI命令发送GARP数据包并更新相邻设备的ARP缓存：

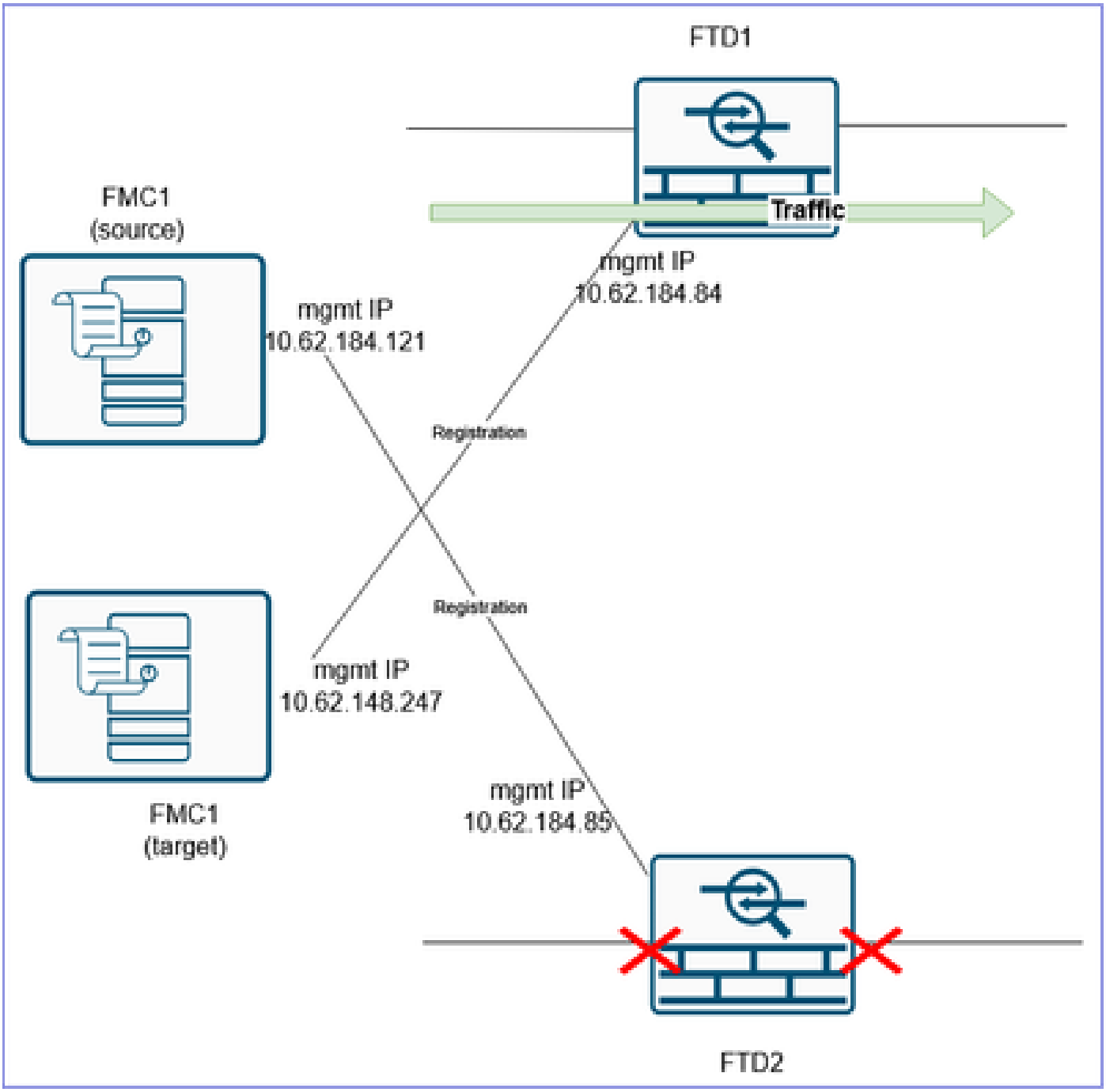
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

您必须对FW拥有的每个IP重复此命令。因此，与为防火墙拥有的每个IP发送GARP数据包相比，仅清除相邻设备的ARP缓存的速度更快。

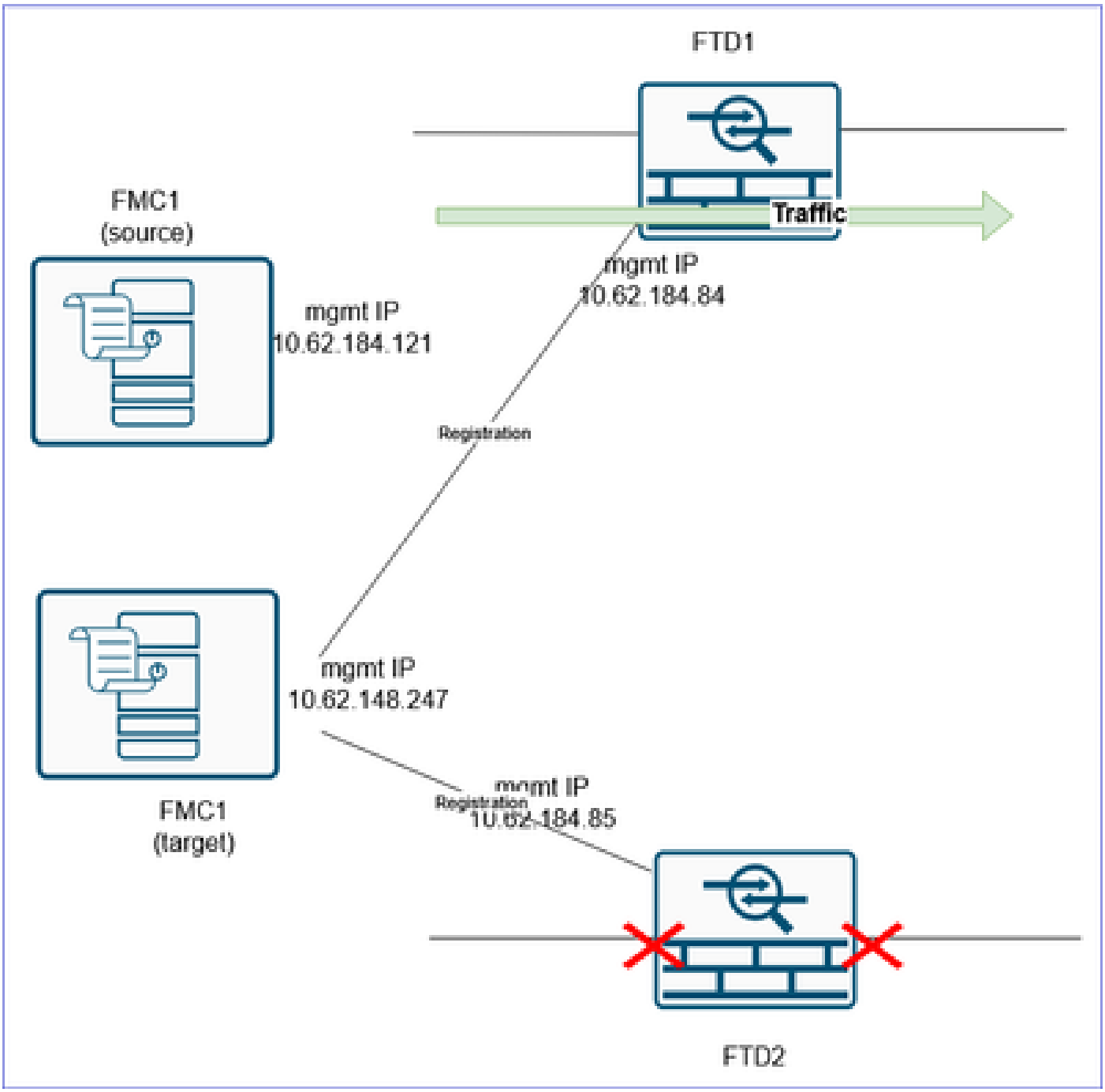
步骤13.将第二个FTD迁移到FMC2（目标FMC）

最后一项是修改HA对。为此，您首先需要从FMC1（源FMC）中删除FTD2，然后将其注册到FMC2（目标FMC）。

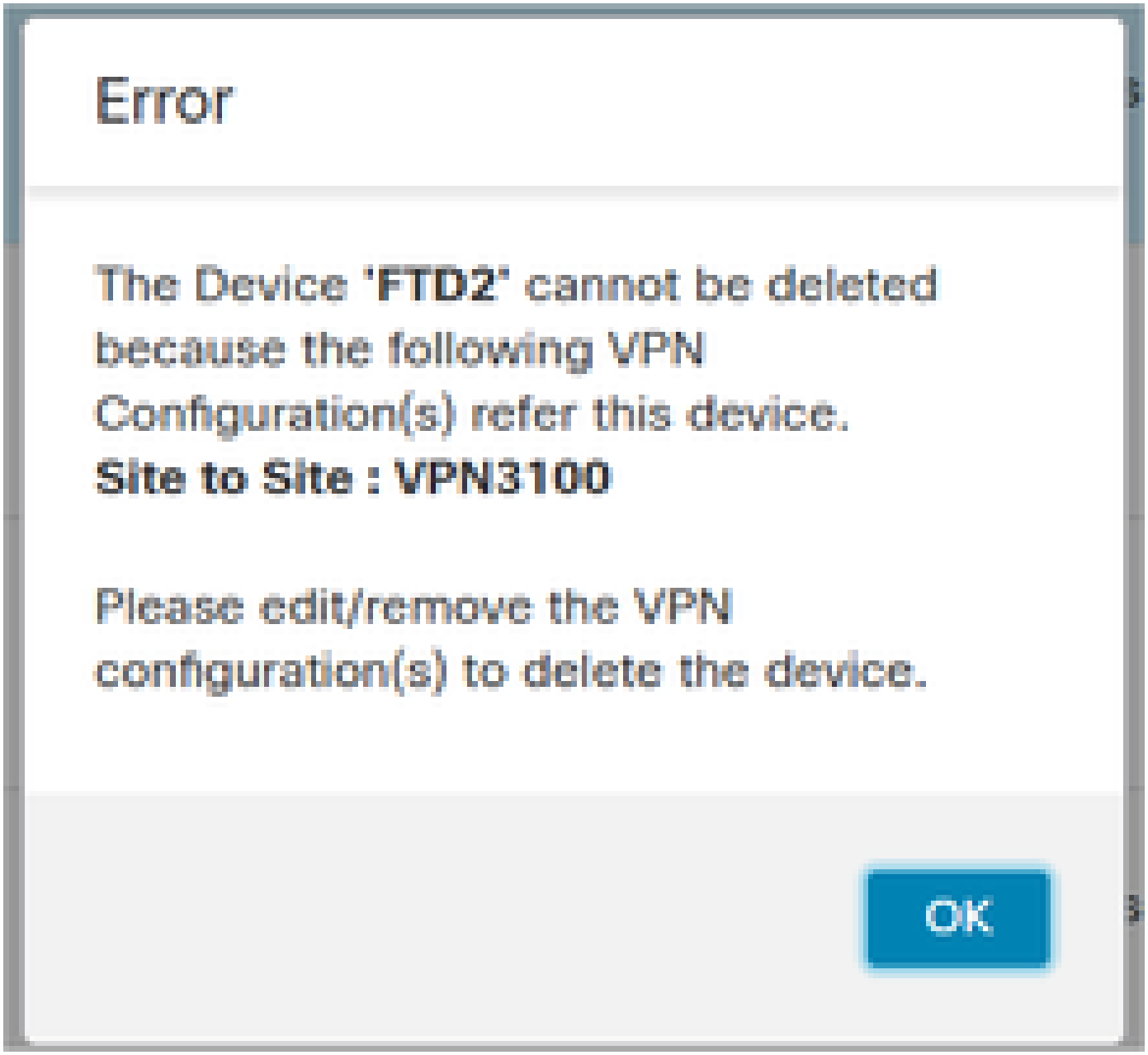
攻击前：


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

在:



如果您有连接到FTD2的VPN配置，则必须在删除FTD之前先将其删除。在不同情况下，会显示类似以下内容的消息：



CLI验证：

```
<#root>

>

show managers


No managers configured.
```

在将FTD配置注册到目标FMC之前，最好先清除所有FTD配置。一种快速的方法是在防火墙模式之间切换。

例如，如果您有路由模式，请切换到transparent，然后再切换回routed:

<#root>

>

configure firewall transparent

然后：

<#root>

>

configure firewall routed

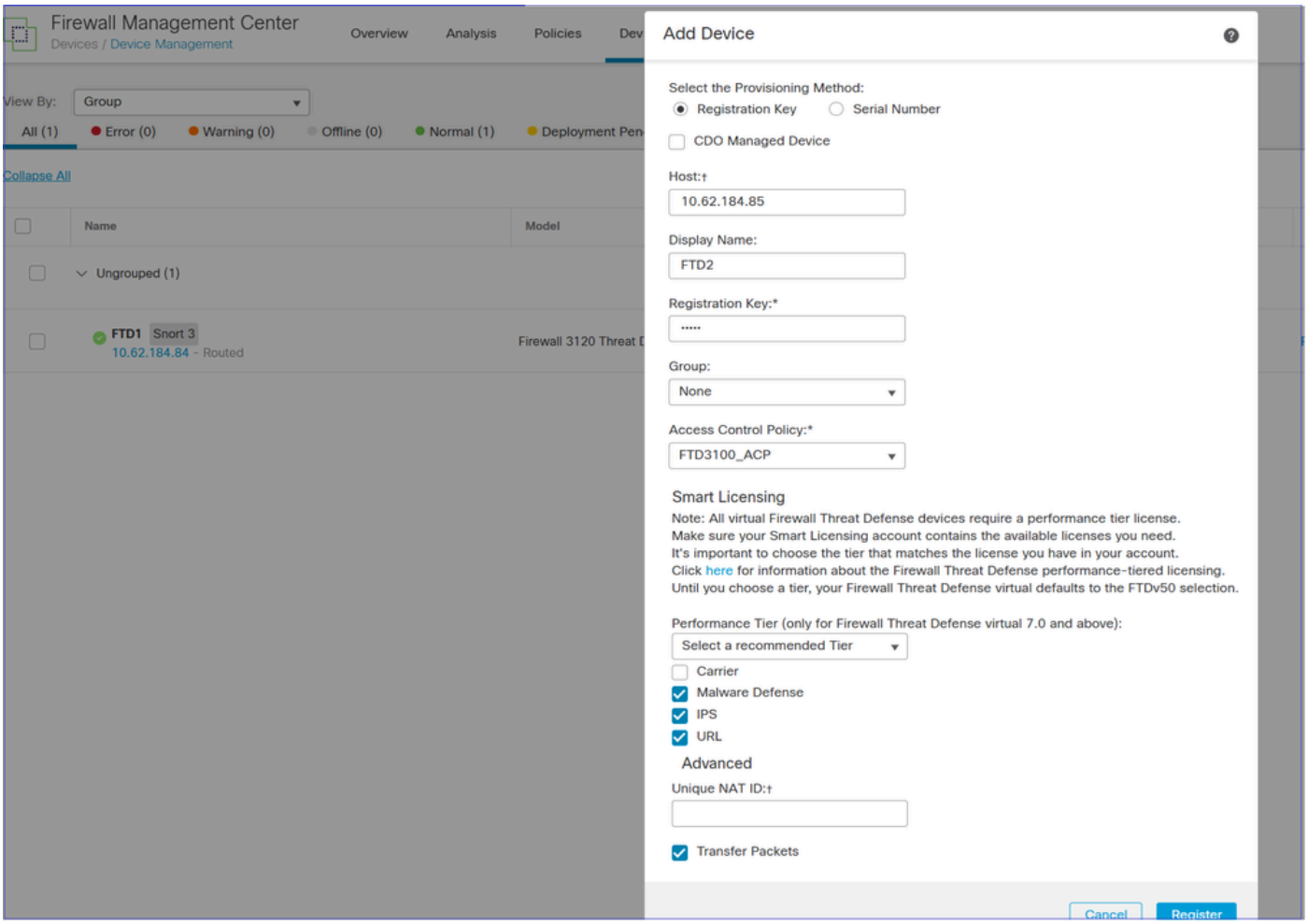
然后，将其注册到FMC2（目标FMC）：

<#root>

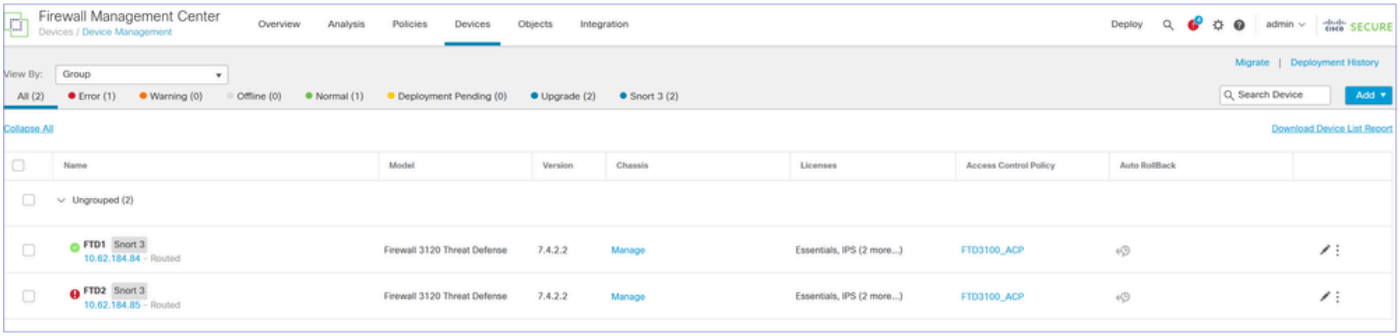
>

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.
>
```



结果：

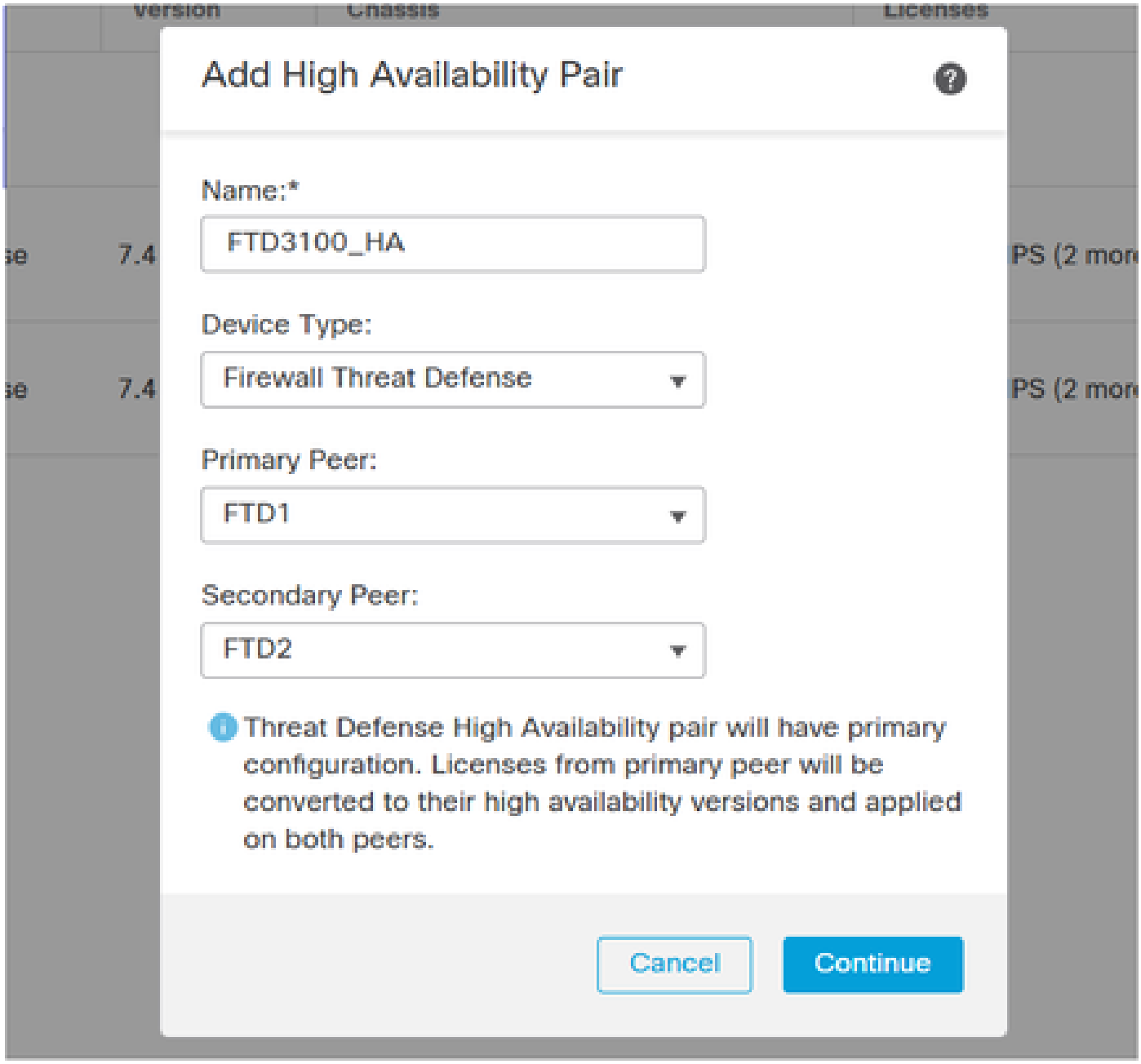


步骤14.重新形成FTD HA

注意：此任务（与任何HA相关任务一样）也必须在工作负荷期间执行。在HA协商期间，数据接口关闭后，流量将中断约1分钟。

在目标FMC上，导航到Devices > Device Management和Add > High Availability。

⚠ 警告：确保选择处理流量的FTD（本场景中的FTD1）作为主要对等体：



重新配置HA设置，包括受监控接口、备用IP、虚拟MAC地址等。

从FTD1 CLI验证：

<#root>

FTD3100-3#

show failover | include host

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

从FTD2 CLI验证：

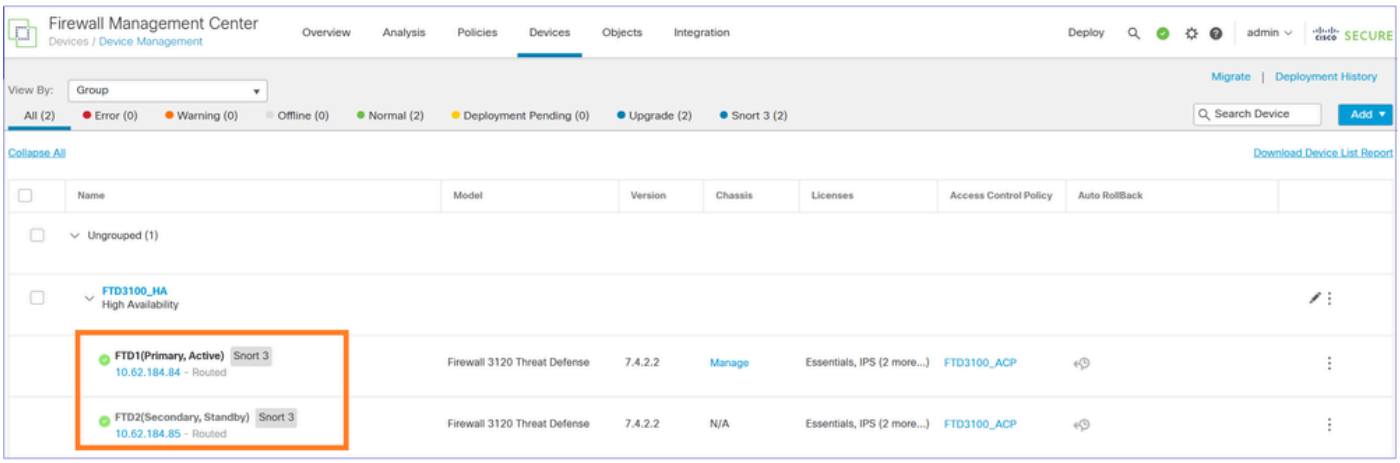
<#root>

FTD3100-3#

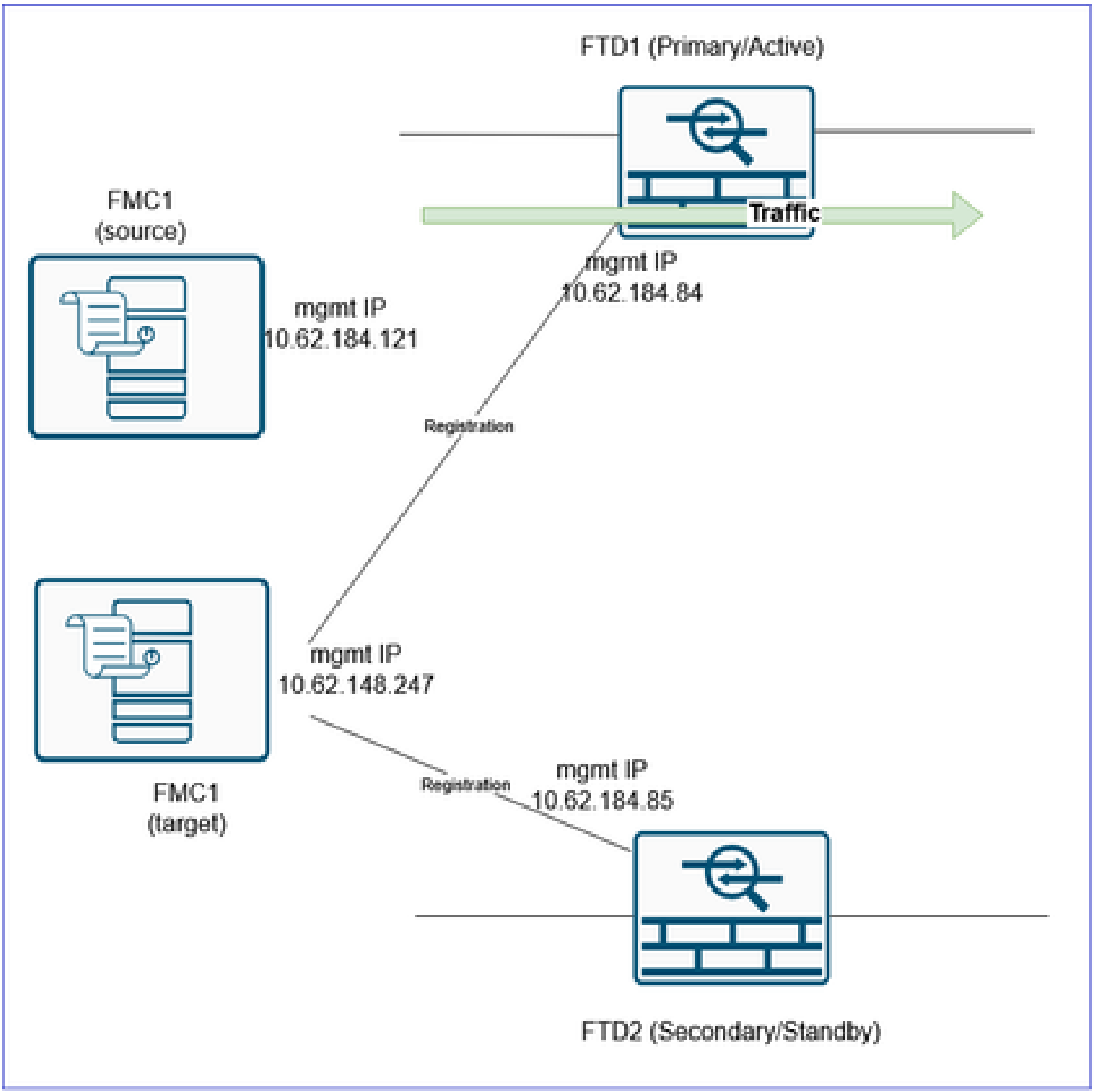
show failover | include host

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

FMC UI验证：



最后，启动/重新连接FTD2设备的数据接口。



参考

- 导出和导入设备配置
- 添加高可用性对
- 将FTD从一个FMC迁移到另一个FMC

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。