Migrar FTD HA (Failover) para outro FMC

Contents

Introdução

O presente documento descreve o procedimento de migração de um FTD HA de um CVP existente para outro CVP.

Para obter uma migração de firewall autônomo para um novo FMC, consulte 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

Abreviaturas

ACP = Política de Controle de Acesso

ARP = Address Resolution Protocol (Protocolo de Resolução de Endereços)

CLI = Interface de linha de comando

FMC = Secure Firewall Management Center (Centro de gerenciamento de firewall seguro)

FTD = Secure Firewall Threat Defense (Defesa contra ameaças de firewall seguro)

GARP = ARP Gratuito

HA = alta disponibilidade

MW = Janela de manutenção

IU = Interface do usuário

Pré-requisitos

Antes de iniciar o processo de migração, certifique-se de que estes pré-requisitos estejam em vigor:

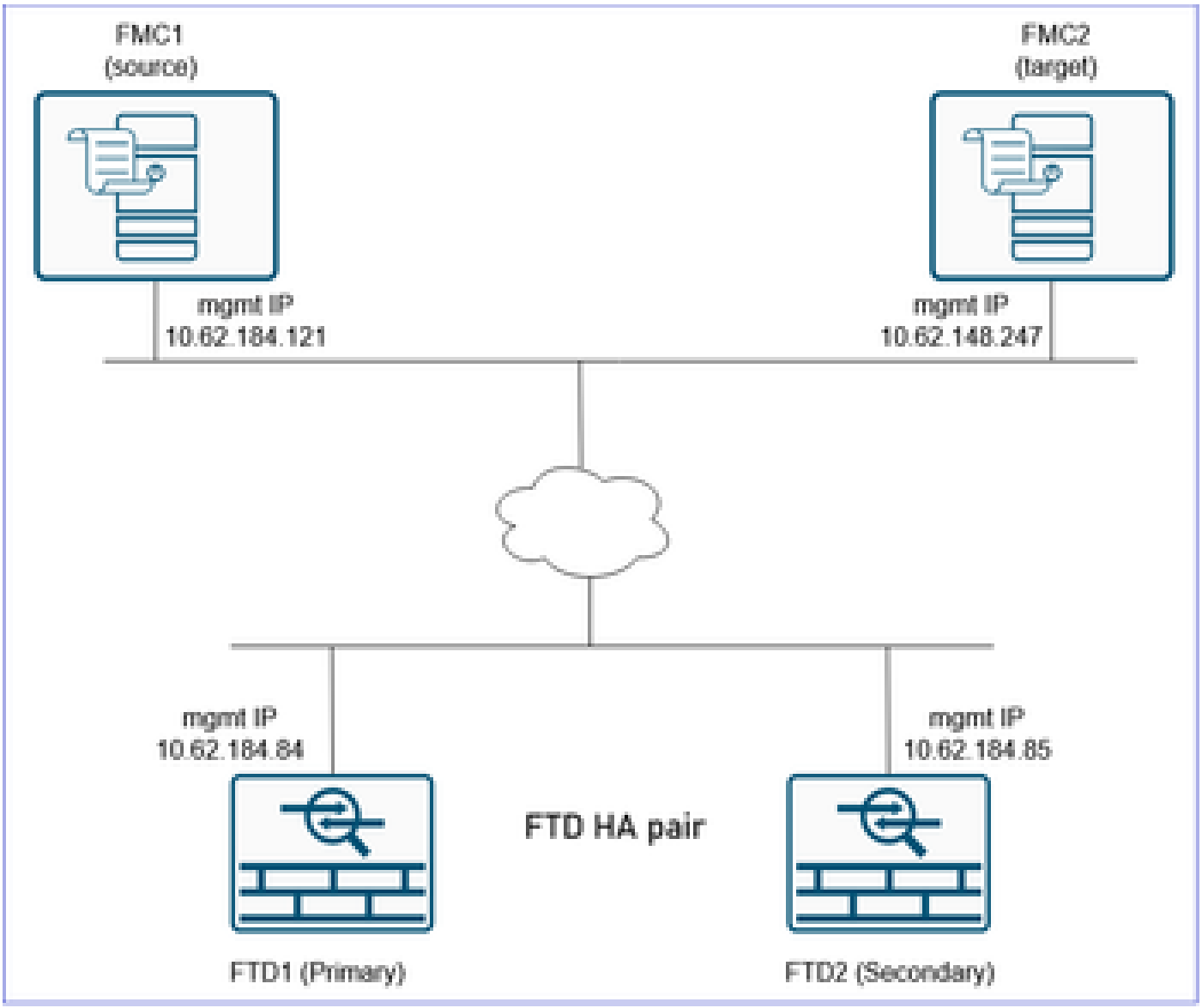
- Acesso de interface do usuário e CLI aos FMCs de origem e de destino.
- Credenciais administrativas para FMC e firewalls.
- Acesso de console a ambos os firewalls.
- Acesso aos dispositivos de upstream e downstream de L3 (caso seja necessário limpar a cache ARP).
- Assegurar que o CVP de destino/de destino tem a mesma versão que o CVP de origem/antigo.
- Assegurar que o CVP de destino/de destino tem as mesmas licenças que o CVP de origem/antigo.
- Organize uma MW para executar a migração, já que ela afetará o tráfego de trânsito.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall 31xx, FTD versão 7.4.2.2.
- Secure Firewall Management Center versão 7.4.2.2.
- As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia



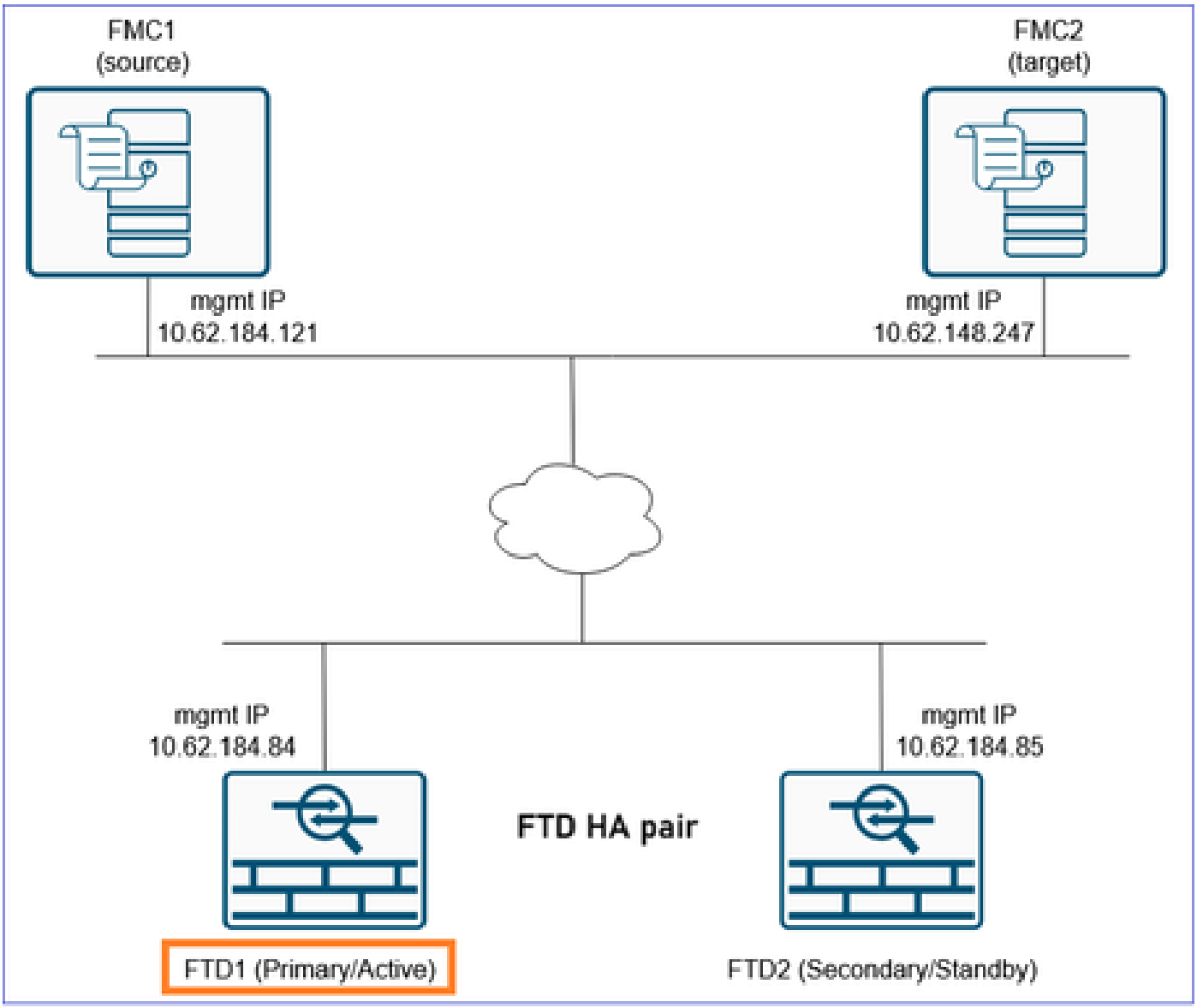
Configurar

Etapas da migração

Para esse cenário, consideramos os seguintes estados:

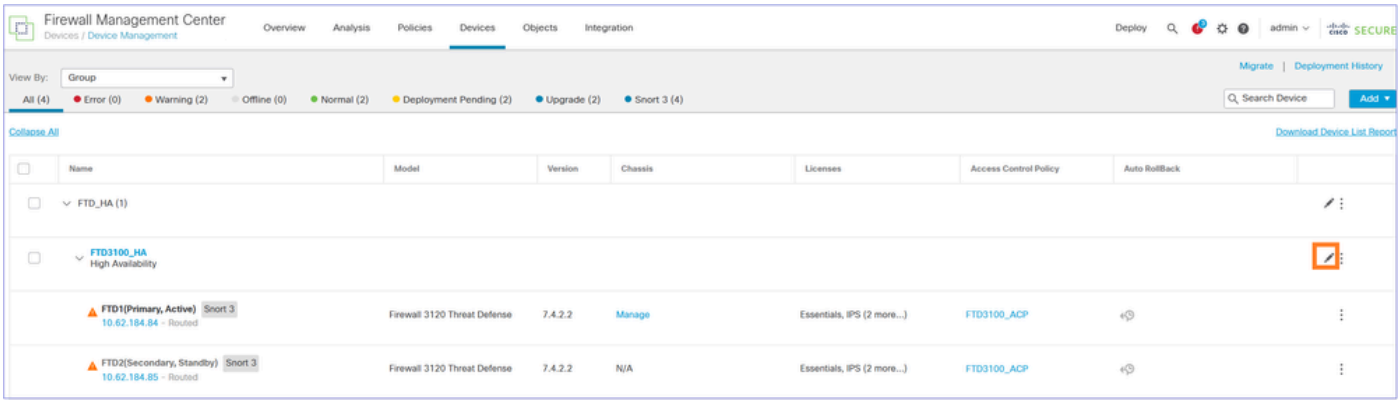
FTD1: Principal/Ativo

FTD2: Secundário/Em Espera

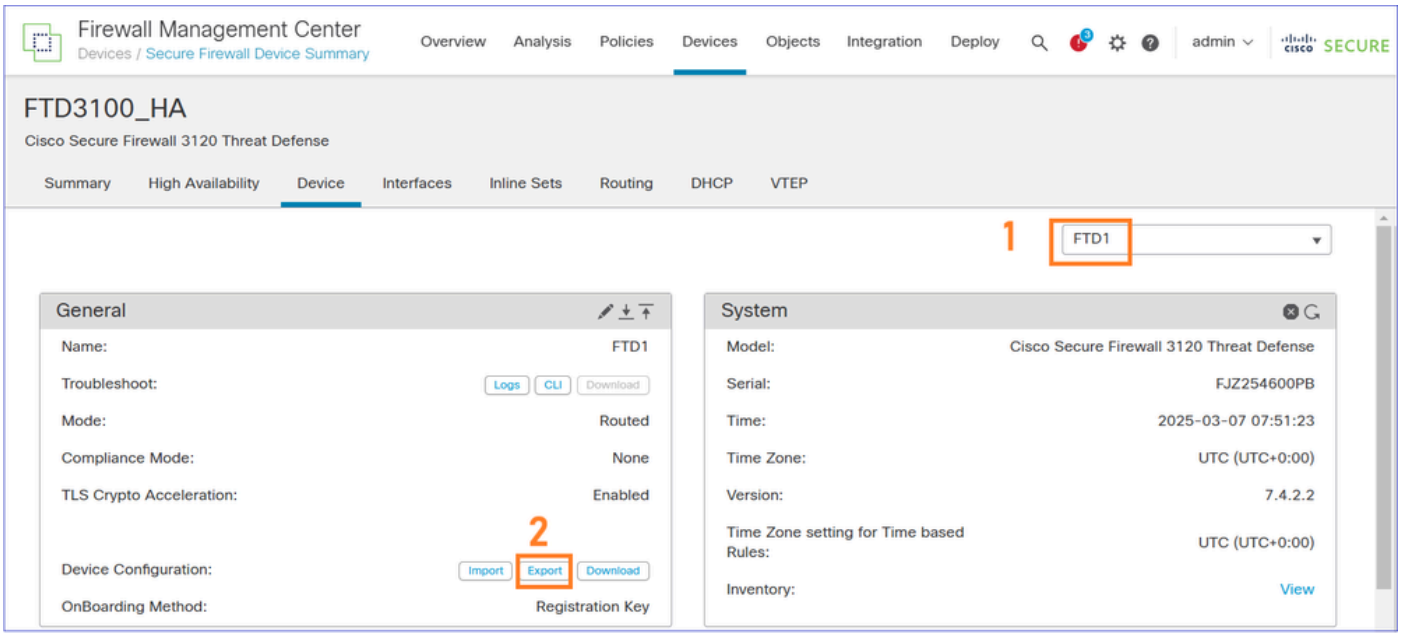


Etapa 1. Exportar a configuração do dispositivo do firewall primário

No FMC1 (FMC de origem), navegue até Devices > Device Management. Selecione o par HA FTD e selecione Editar:

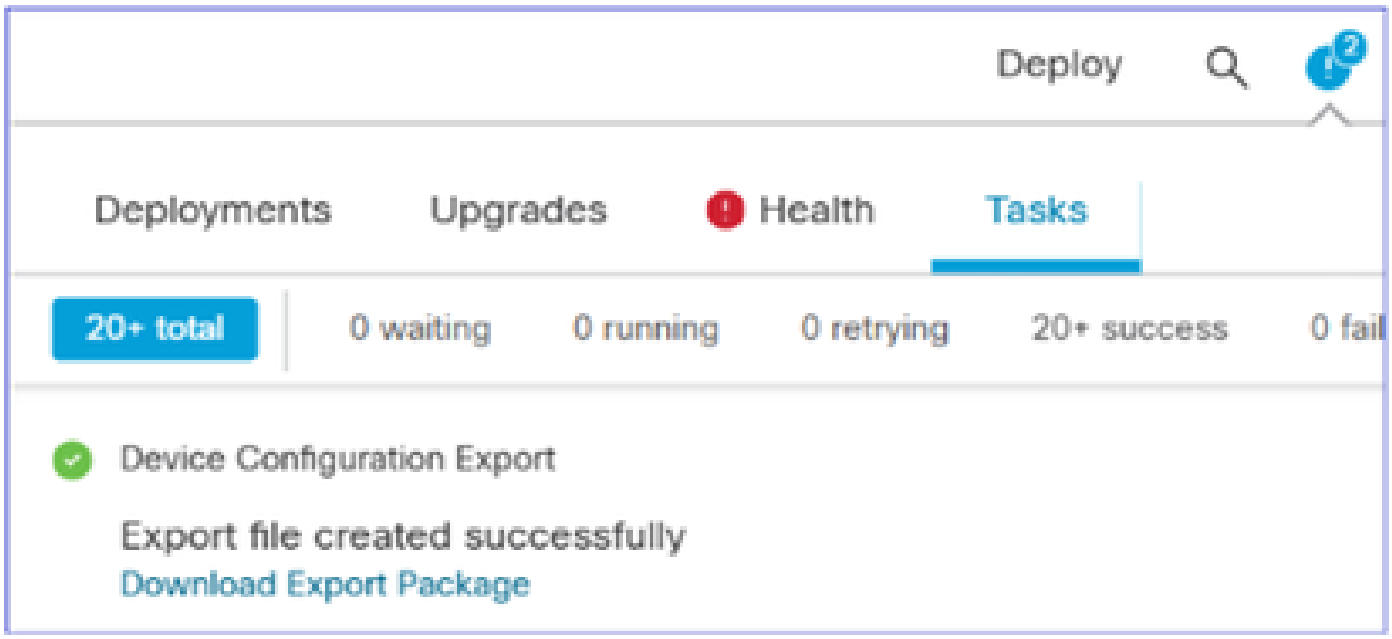


Navegue até a guia Device. Verifique se o FTD principal/ativo (FTD1, neste caso) está selecionado e selecione Exportar para exportar a configuração do dispositivo:



Note: A opção Exportar está disponível a partir da versão de software 7.1 e posterior.

Você pode navegar até a página Notificações > Tarefas para garantir que a exportação foi concluída. Em seguida, selecione o Pacote Download Export:



Como alternativa, você pode clicar no botão Download na área Geral. Você obtém um arquivo sfo, por exemplo DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

O arquivo contém configurações relacionadas ao dispositivo, como:

- Interfaces roteadas
- Conjuntos em linha
- Roteamento
- DHCP
- VTEP

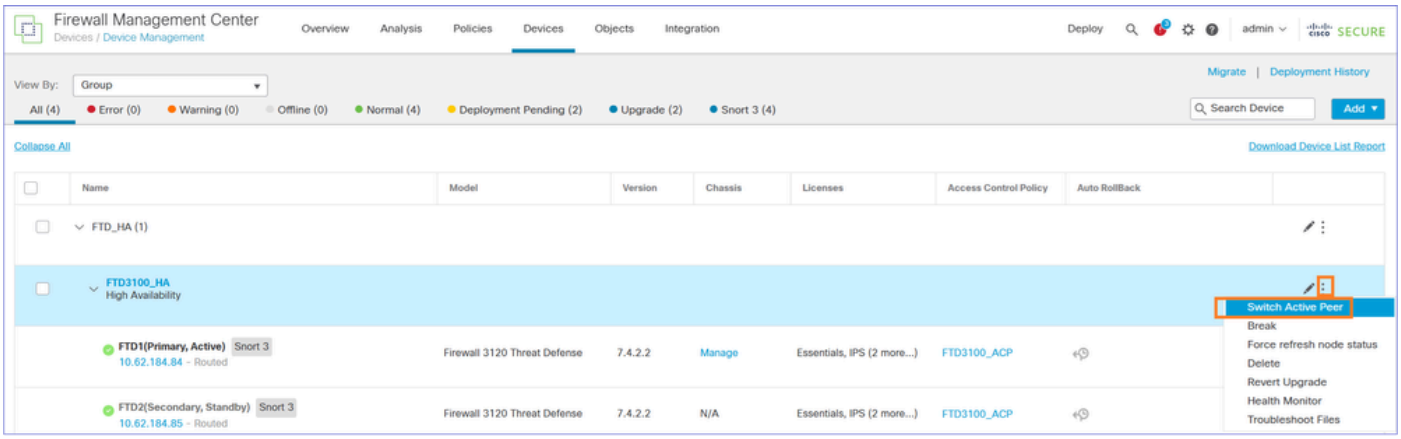
- Objetos associados

Note: O arquivo de configuração exportado pode ser importado de volta somente para o mesmo FTD. O UUID do FTD deve corresponder ao conteúdo do arquivo sfo importado. O mesmo FTD pode ser registrado em outro FMC e o arquivo sfo pode ser importado.

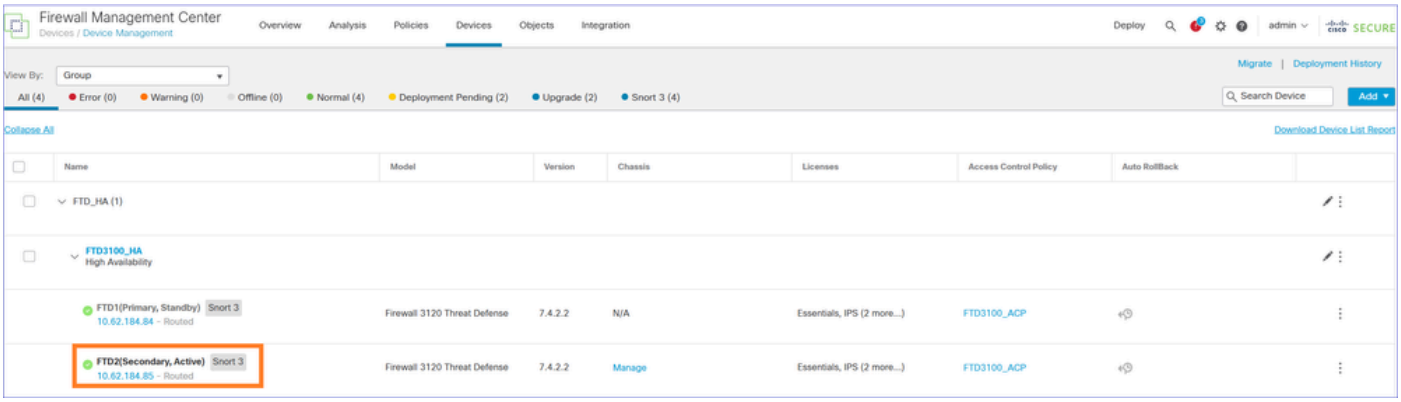
Referência: 'Exportar e importar a configuração do dispositivo' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

Etapa 2. Ativar o FTD Secundário

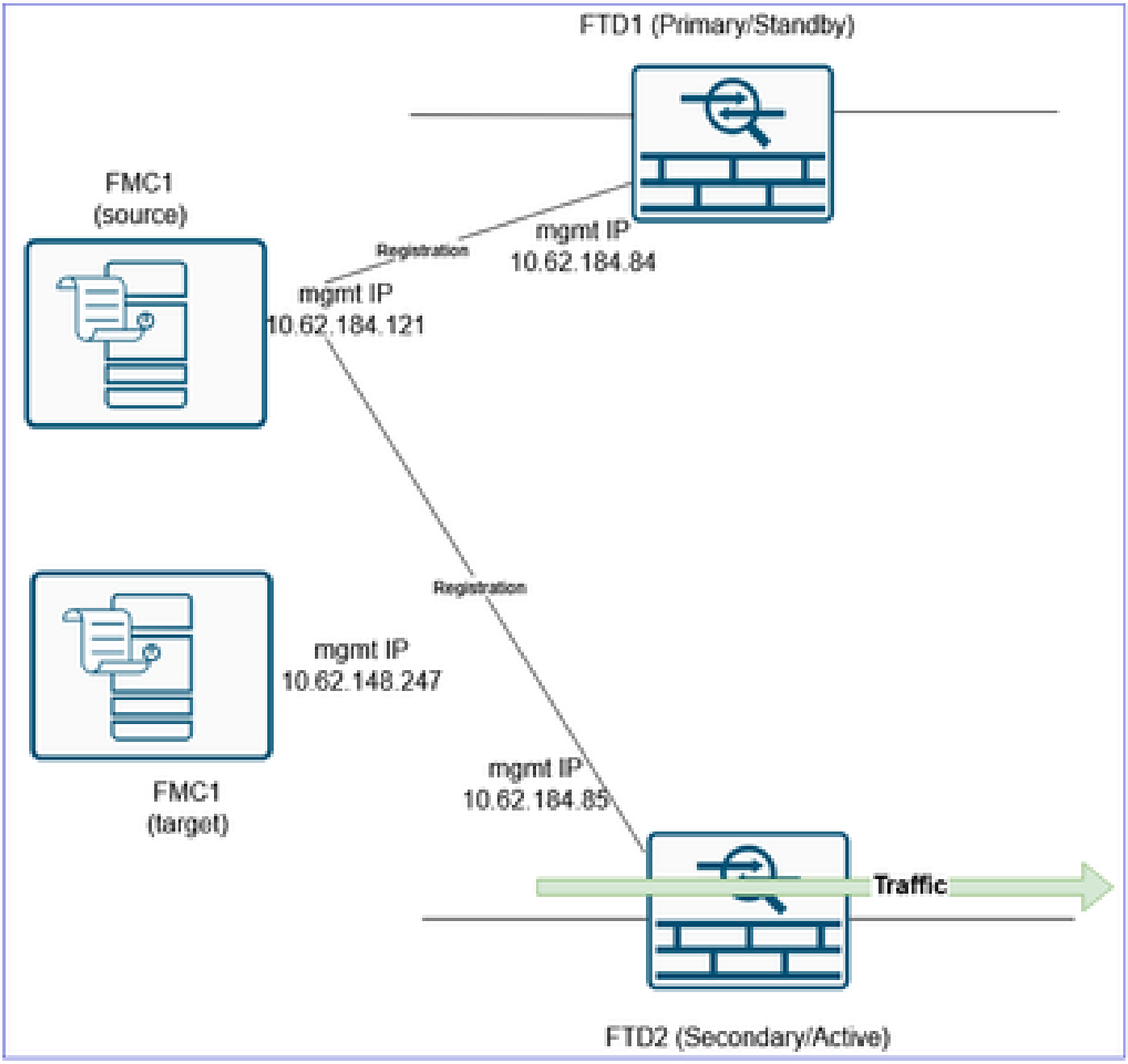
Navegue até Devices > Device Management, selecione o par FTD HA e selecione Switch Ative Pair:



O resultado é FTD1 (Principal/Standby) e FTD (Secundário/Ativo):

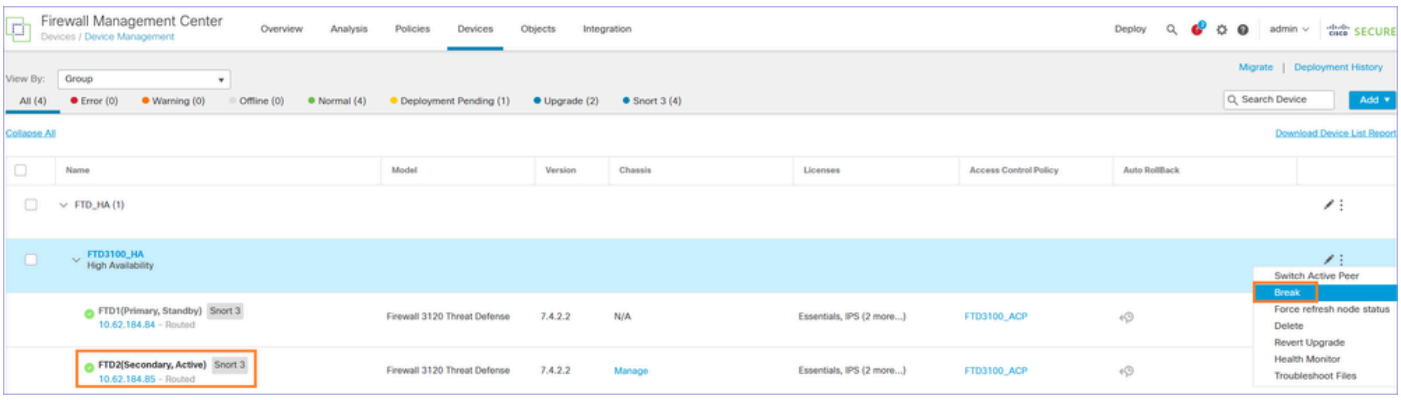


Agora o tráfego é processado pelo FTD secundário/ativo:

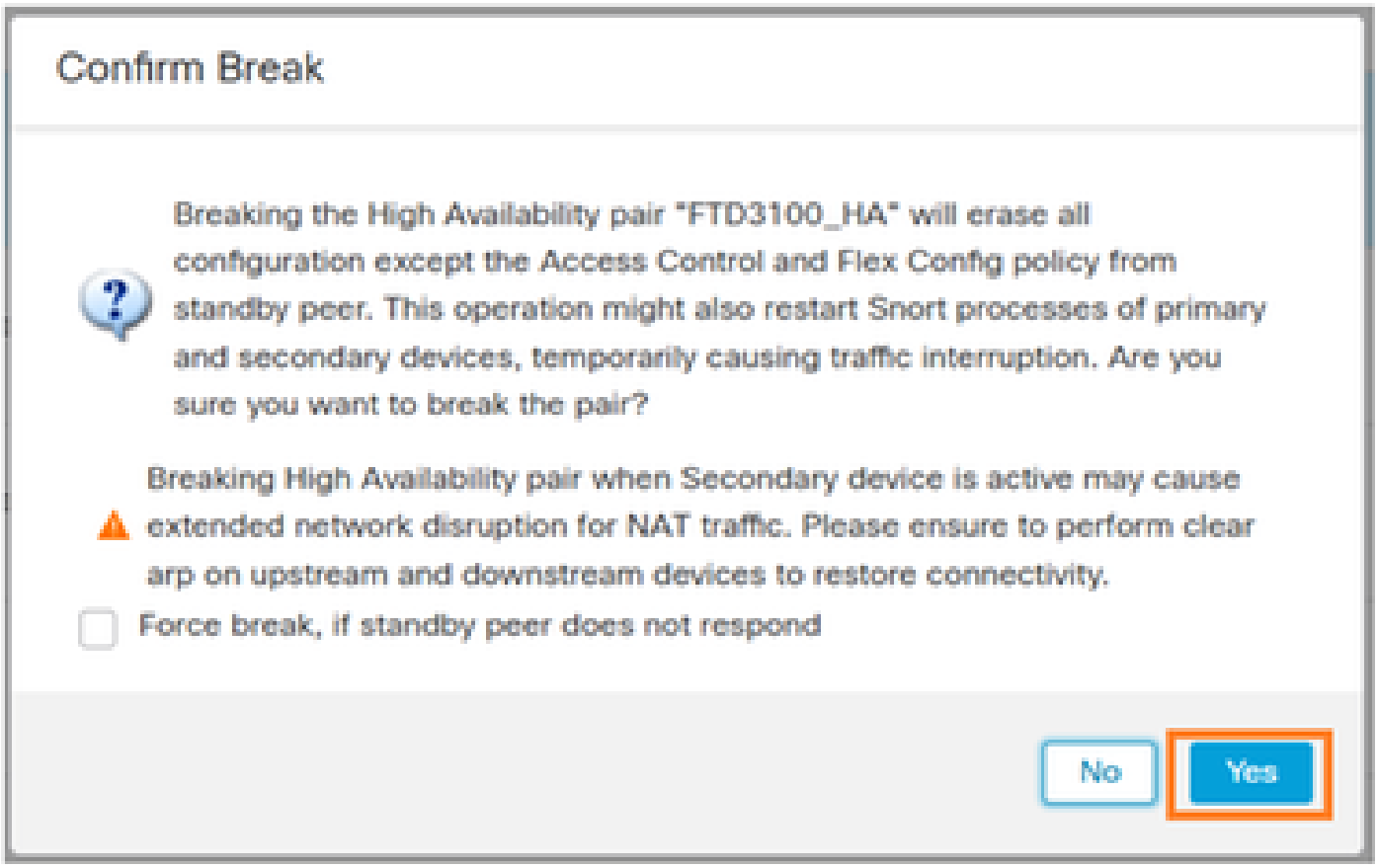


Etapa 3. Quebrar o HA do FTD

Navegue até Devices > Device Management e Break o FTD HA:



Essa janela é exibida. Selecione sim



Note: Neste ponto, você pode experimentar alguma interrupção de tráfego por alguns segundos, desde que o mecanismo Snort reinicie durante a interrupção de HA. Além disso, como a mensagem menciona, se você usar o NAT e experimentar uma interrupção de tráfego prolongada, considere limpar o cache ARP em dispositivos upstream e downstream.

Após quebrar o HA do FTD, você tem dois FTDs independentes no FMC.

Do ponto de vista da configuração, o FTD2 (ex-Ativo) ainda tem a configuração em vigor, exceto a configuração relacionada a failover e está tratando do tráfego:

<#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
```

O FTD1 (ex-Standby) tem todas as configurações removidas:

<#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#

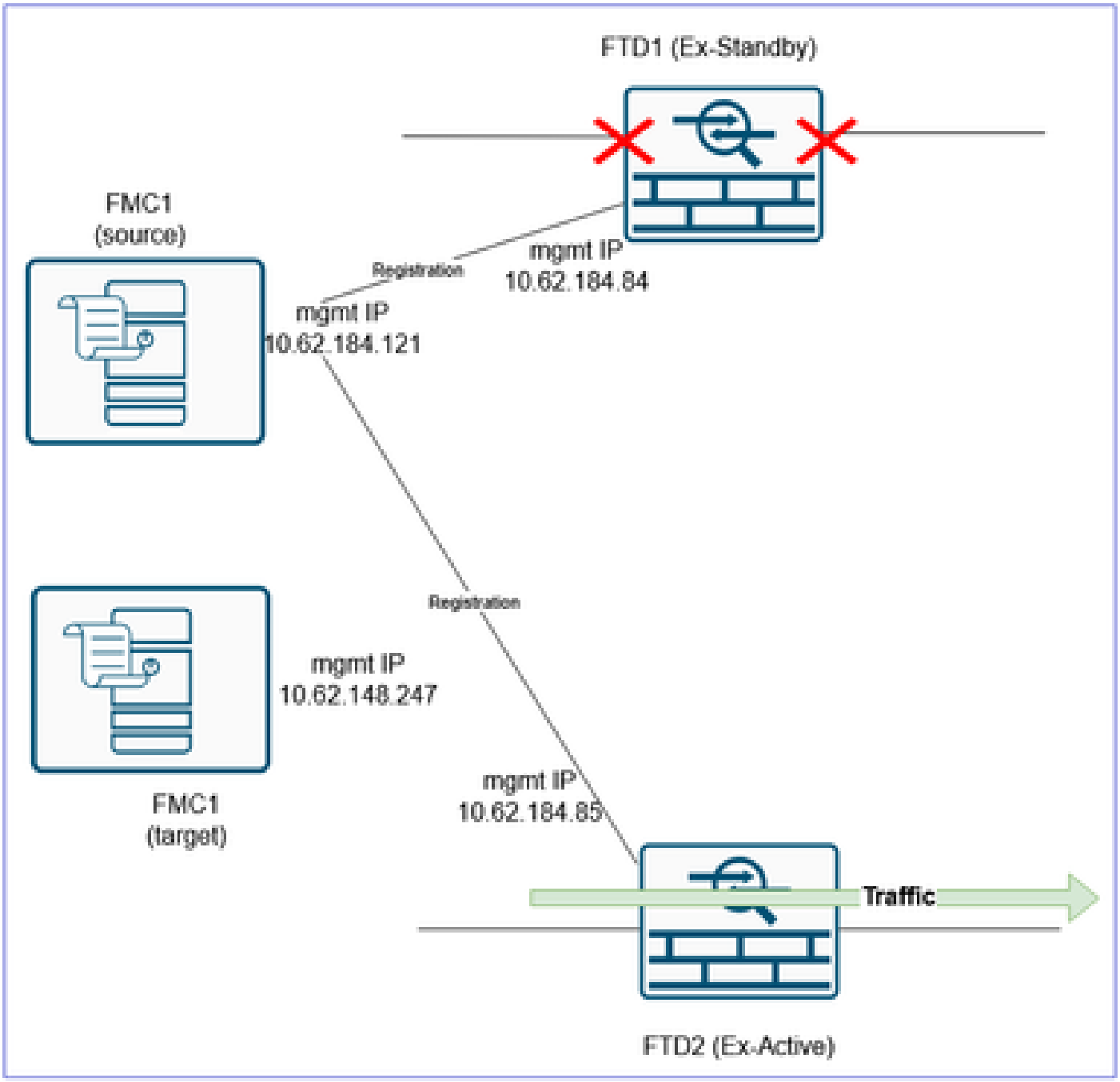
show interface ip brief

```
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
```

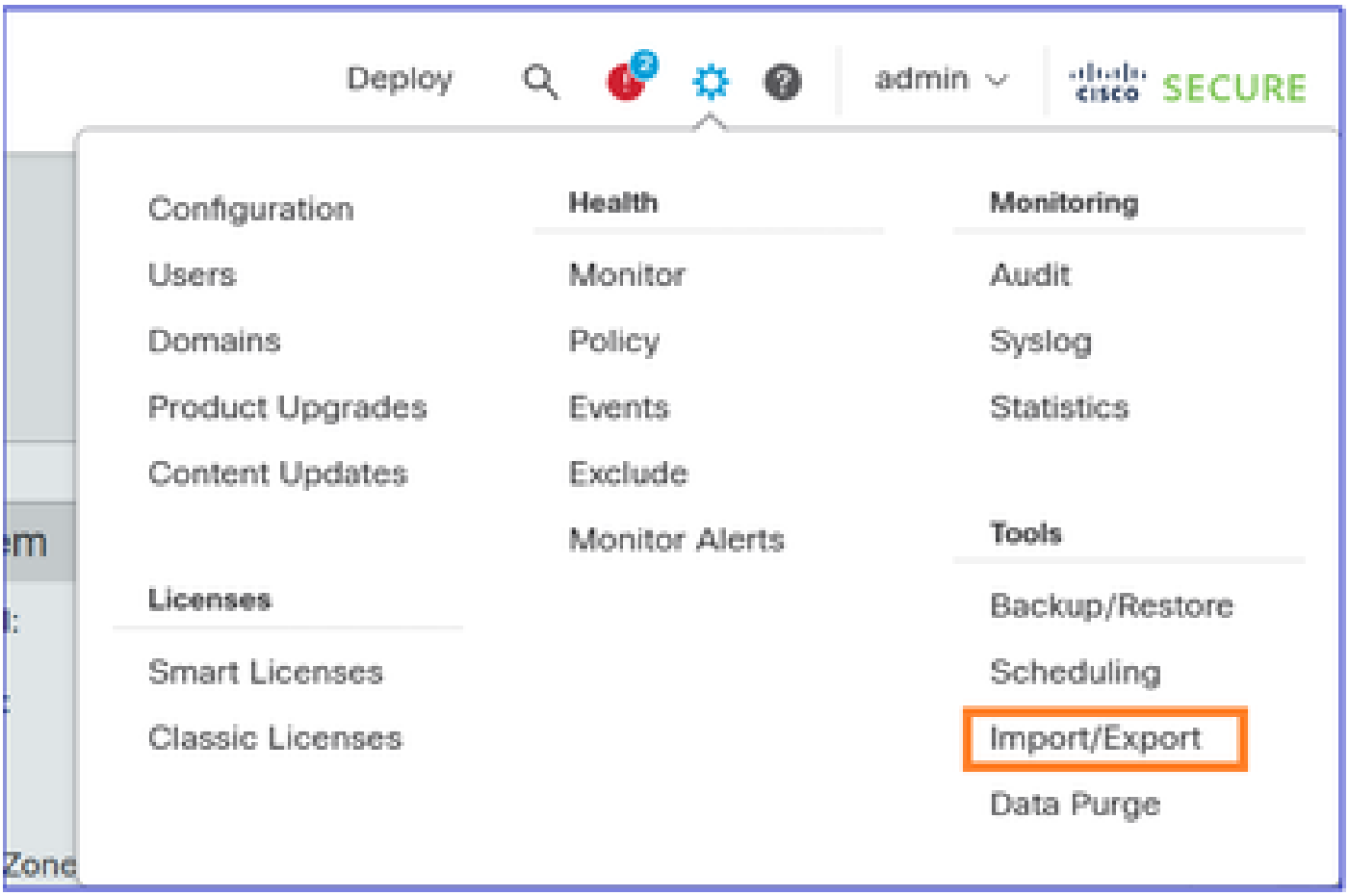
Etapa 4. Isolar as interfaces de dados FTD1 (ex-Primário)

Desconecte os cabos de dados do FTD1 (ex-Primário). Deixe apenas a porta de gerenciamento do FTD conectada.



Etapa 5. Exportar as Políticas Compartilhadas de FTD

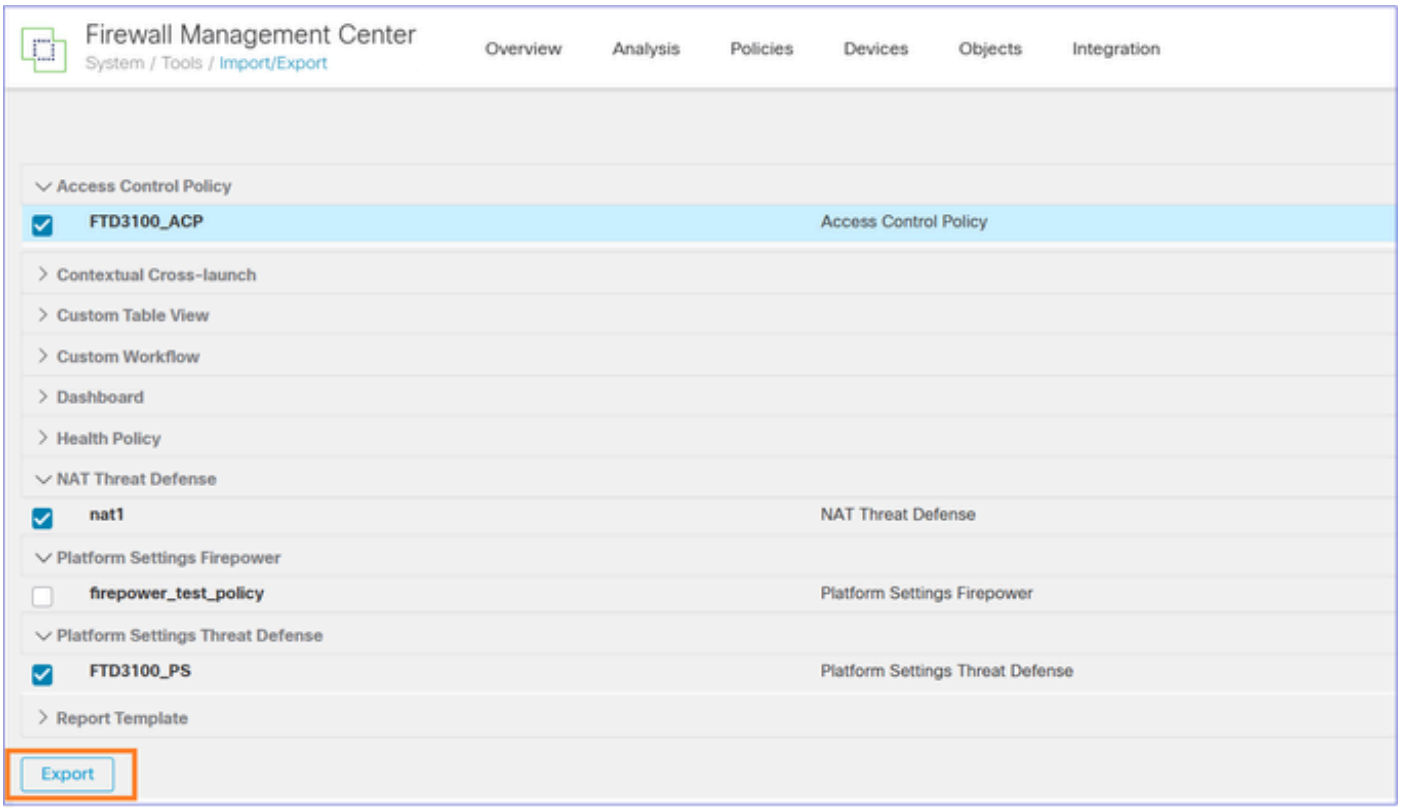
Navegue até System > Tools e selecione Import/Export:



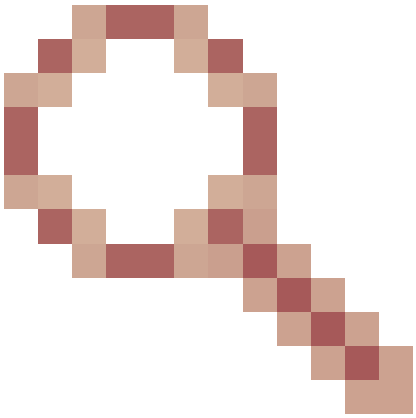
Exporte as várias políticas anexadas ao dispositivo. Certifique-se de exportar todas as políticas anexadas ao FTD, como:

- Política de Controle de Acesso (ACP)
- Política de conversão de endereço de rede (NAT)
- Política de Integridade (se personalizada)
- Configurações da plataforma FTD

etc.



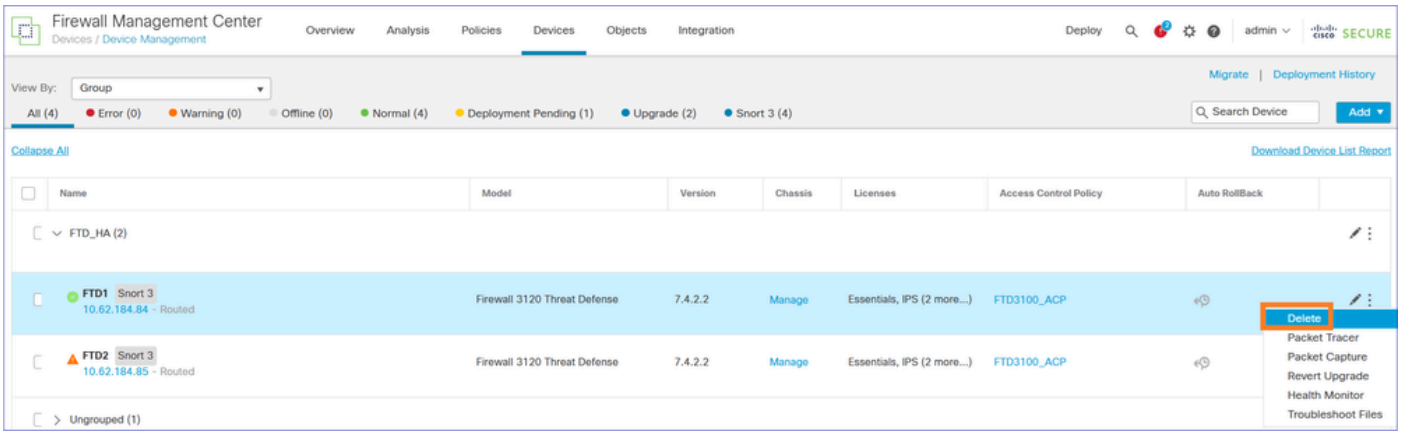
Note: No momento em que este texto foi escrito, não há suporte para a exportação de configuração relacionada à VPN. Você precisa reconfigurar manualmente a VPN no FMC2 (FMC de destino) após o registro do dispositivo.



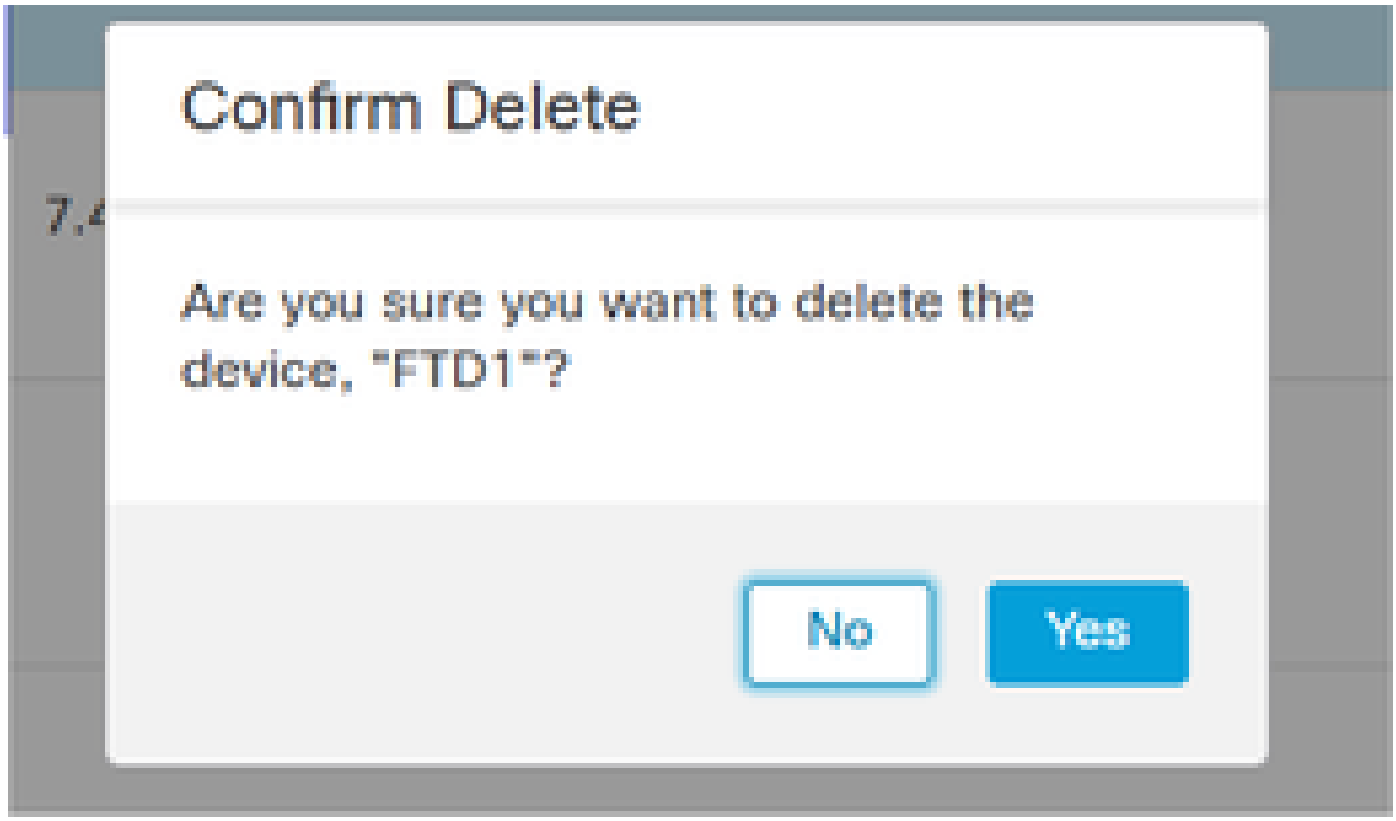
Aprimoramento relacionado à ID de bug da Cisco CSCwf05294
.

O resultado é um arquivo .sfo, por exemplo ObjectExport_20250306082738.sfo

Etapa 6. Excluir/cancelar o registro do FTD1 (ex-primário) do FMC antigo/de origem



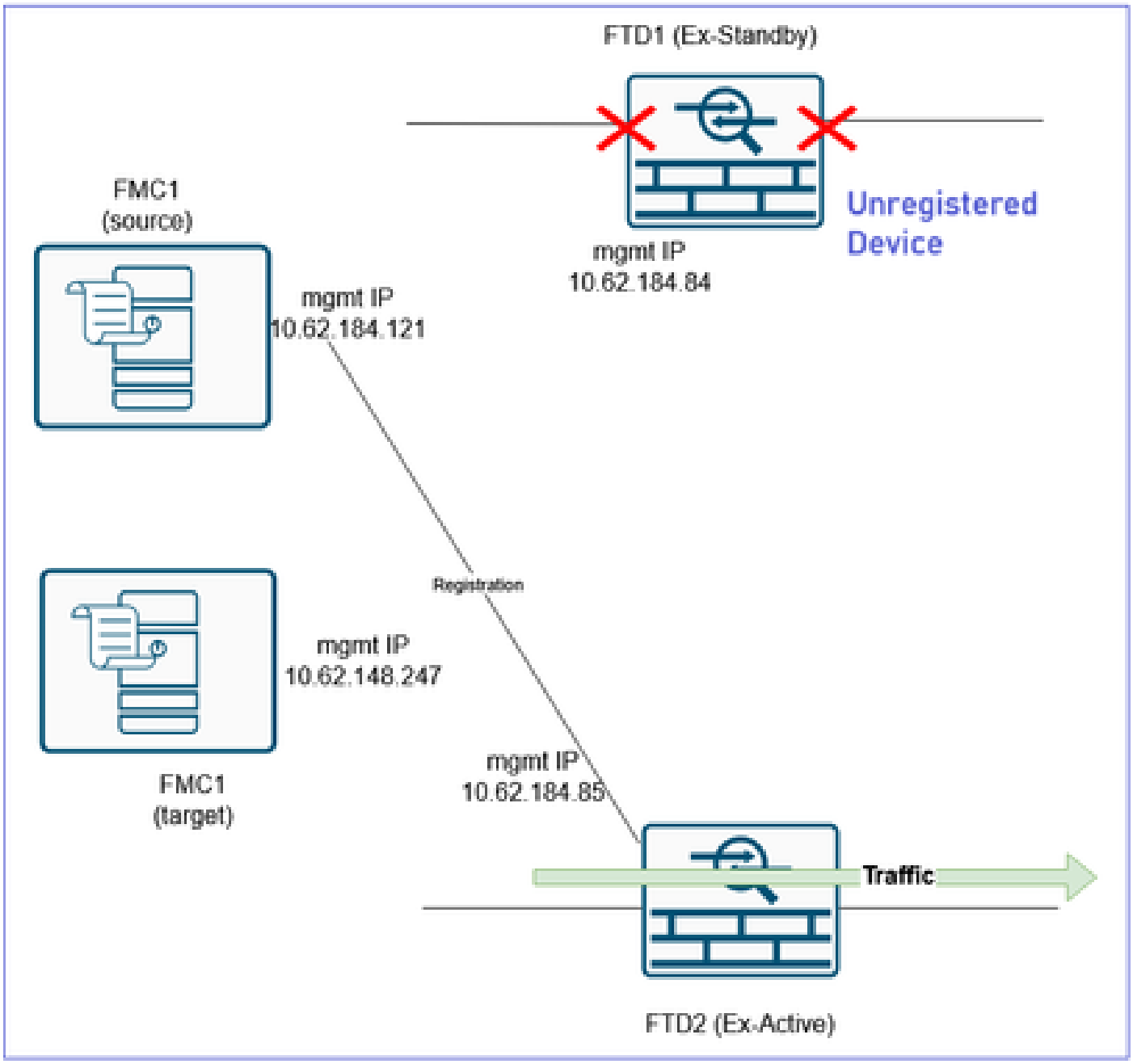
Confirme a exclusão do dispositivo:



Verificação CLI FTD1:

```
<#root>

>

show managers

No managers configured.

>
```

O status atual após a exclusão do dispositivo FTD1:

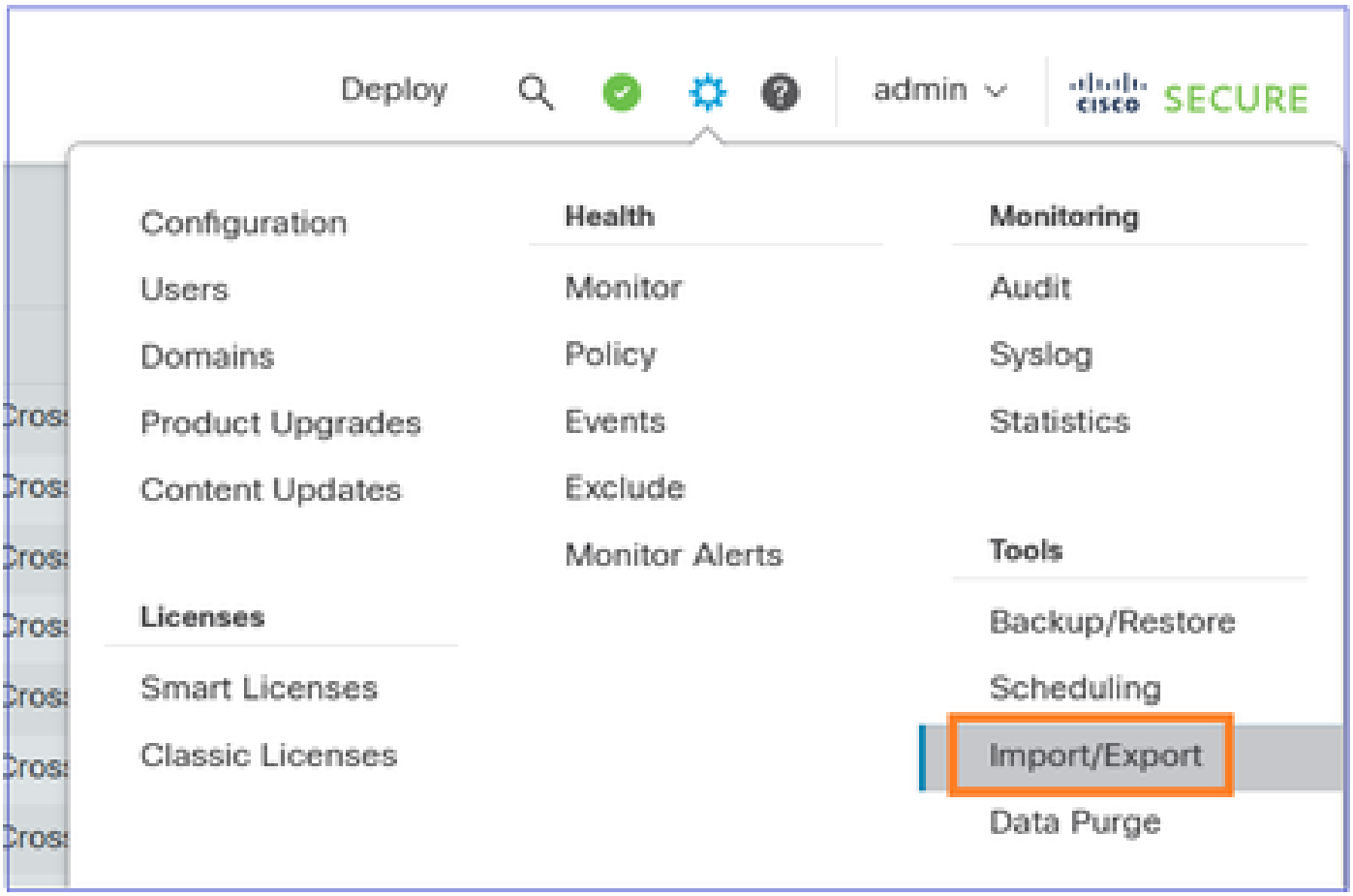


Etapa 7. Importar o objeto de configuração da política de FTD para o FMC2 (FMC de destino)

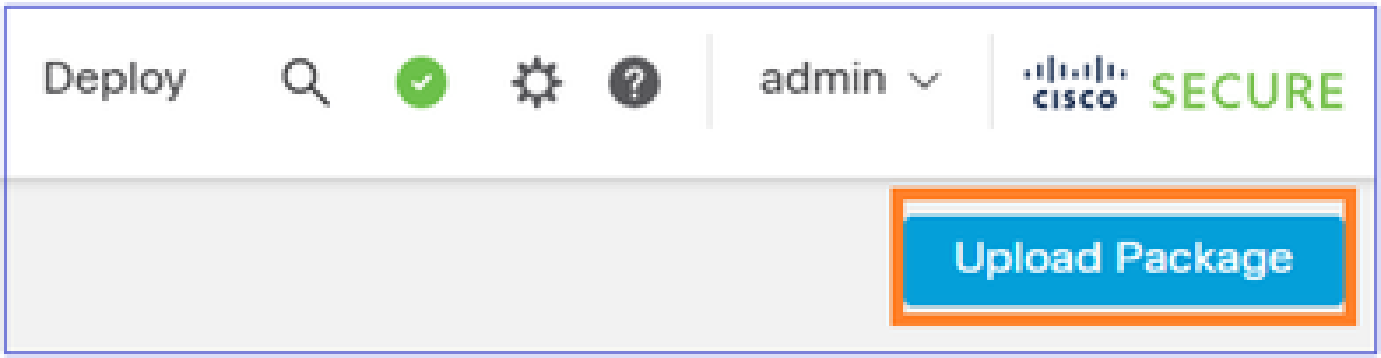
Note: O documento centra-se na migração de um único par de FTD HA para um novo CVP. Por outro lado, se você planeja migrar vários firewalls que compartilham as mesmas políticas (por exemplo, ACP, NAT) e objetos e deseja fazer isso em fases, é necessário considerar esses pontos.
- Se você tiver uma política existente no FMC de destino com o mesmo nome, será perguntado se:
  a. Desejar substituir a política ou
  b. Crie um novo com um nome diferente. Isso cria objetos duplicados com nomes diferentes (sufixo _1).

- Se você for com a opção 'b', na Etapa 9, certifique-se de reorganizar os objetos recém-criados para as políticas migradas (Zonas de segurança ACP, Zonas de segurança NAT, Roteamento, Configurações de plataforma, etc.).

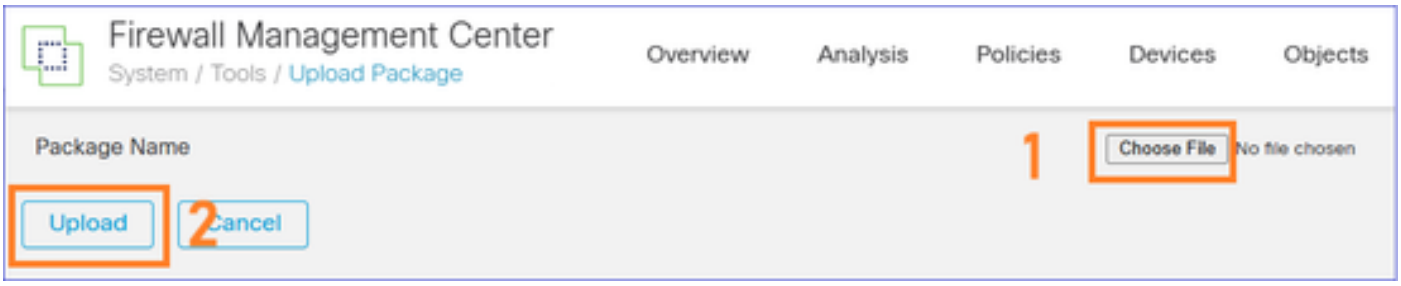
Faça login no FMC2 (FMC de destino) e importe o objeto SFO de Políticas de FTD que você exportou na etapa 5:



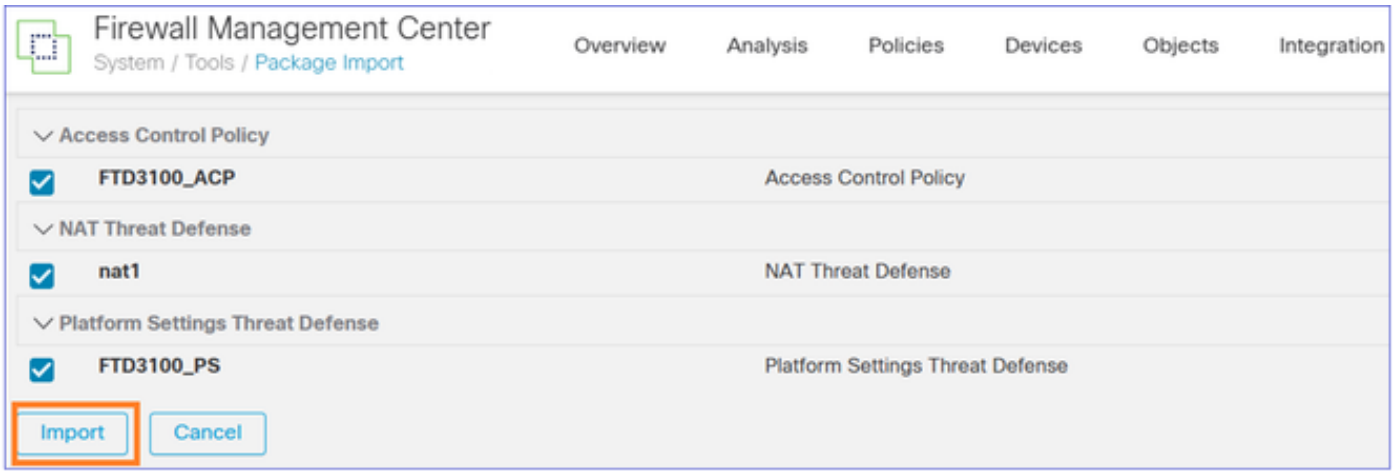
Selecione Carregar pacote:



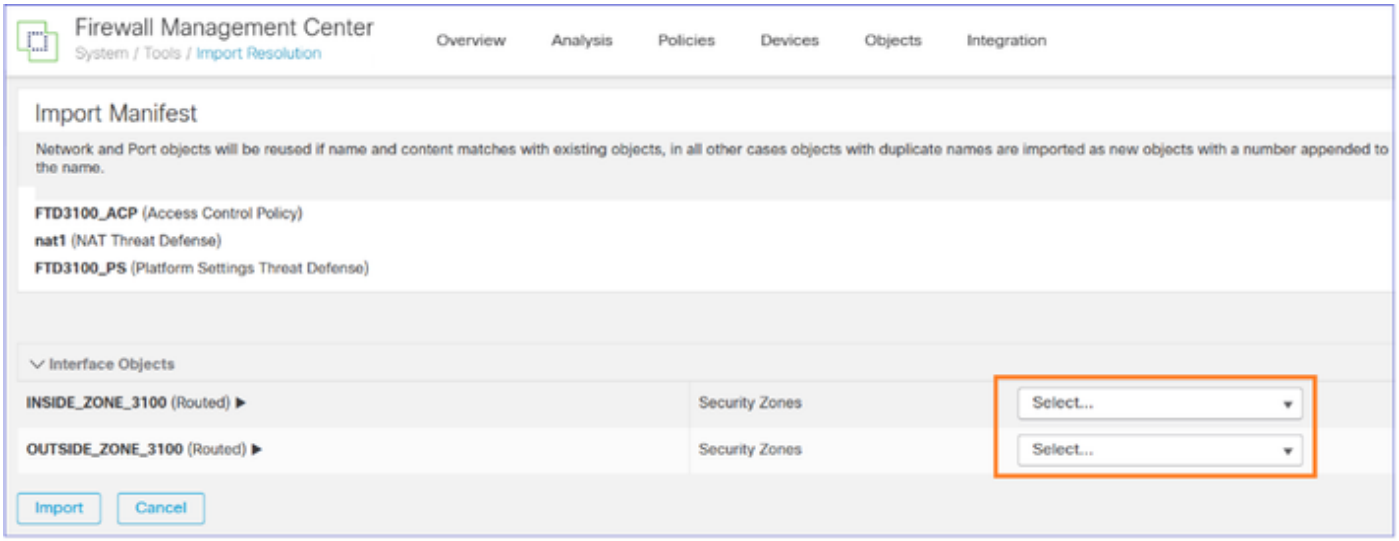
Carregue o arquivo:



Importar as diretivas:



Crie os objetos de interface/zonas de segurança no FMC2 (FMC de destino):



Você pode dar os mesmos nomes que eles tinham no FMC1 (FMC de origem):

Depois de selecionar Import, uma tarefa começa a importar as políticas relacionadas no FMC2 (FMC de destino):

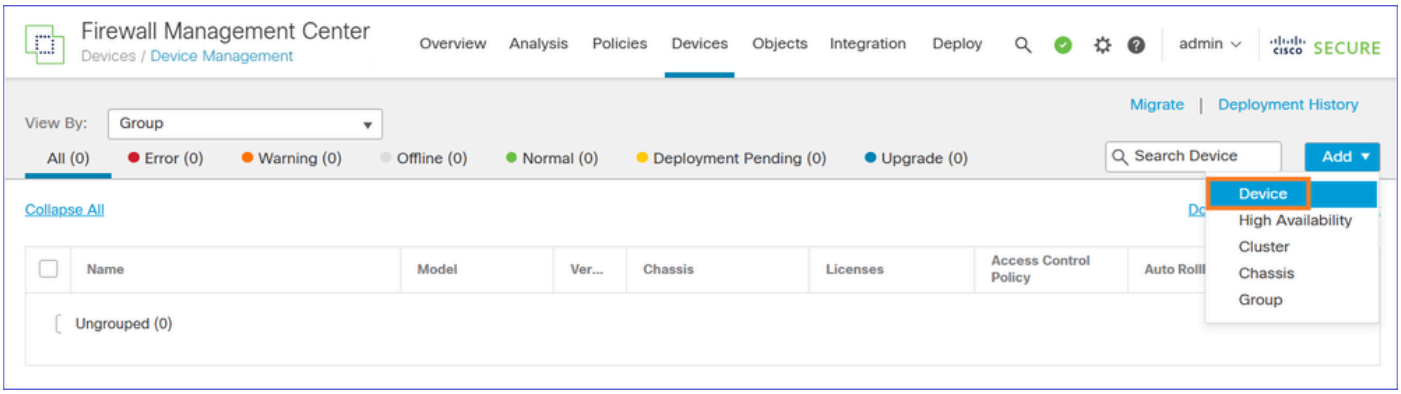
A tarefa está concluída:

Etapa 8. Registrar o FTD1 (ex-Primário) no FMC2

Vá para a CLI FTD1 (ex-Primary) e configure o novo gerenciador:

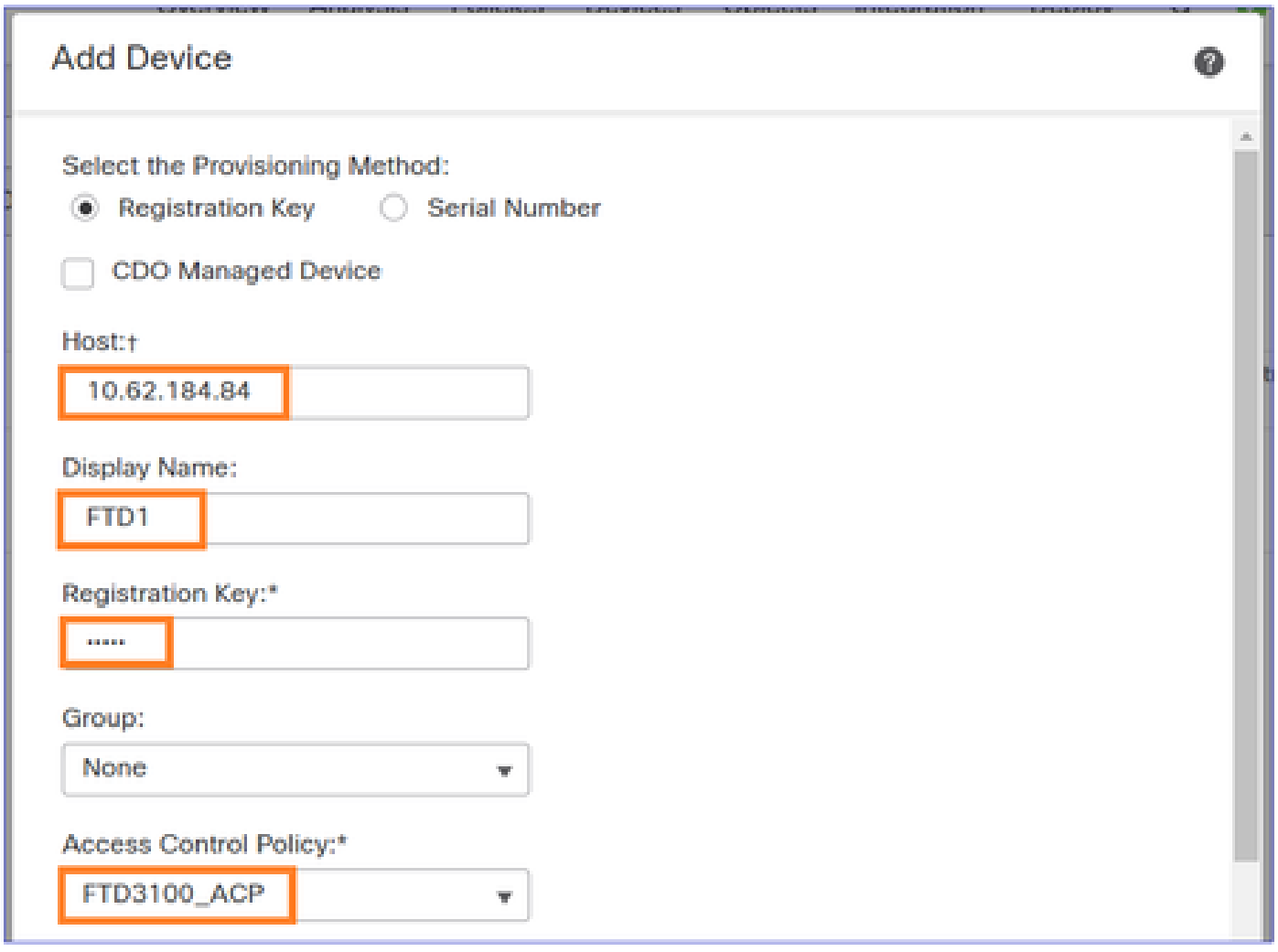
```
<#root>

>

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.

>
```

Navegue até FMC2 (FMC de destino) UI Devices > Device Management e Add o dispositivo FTD:

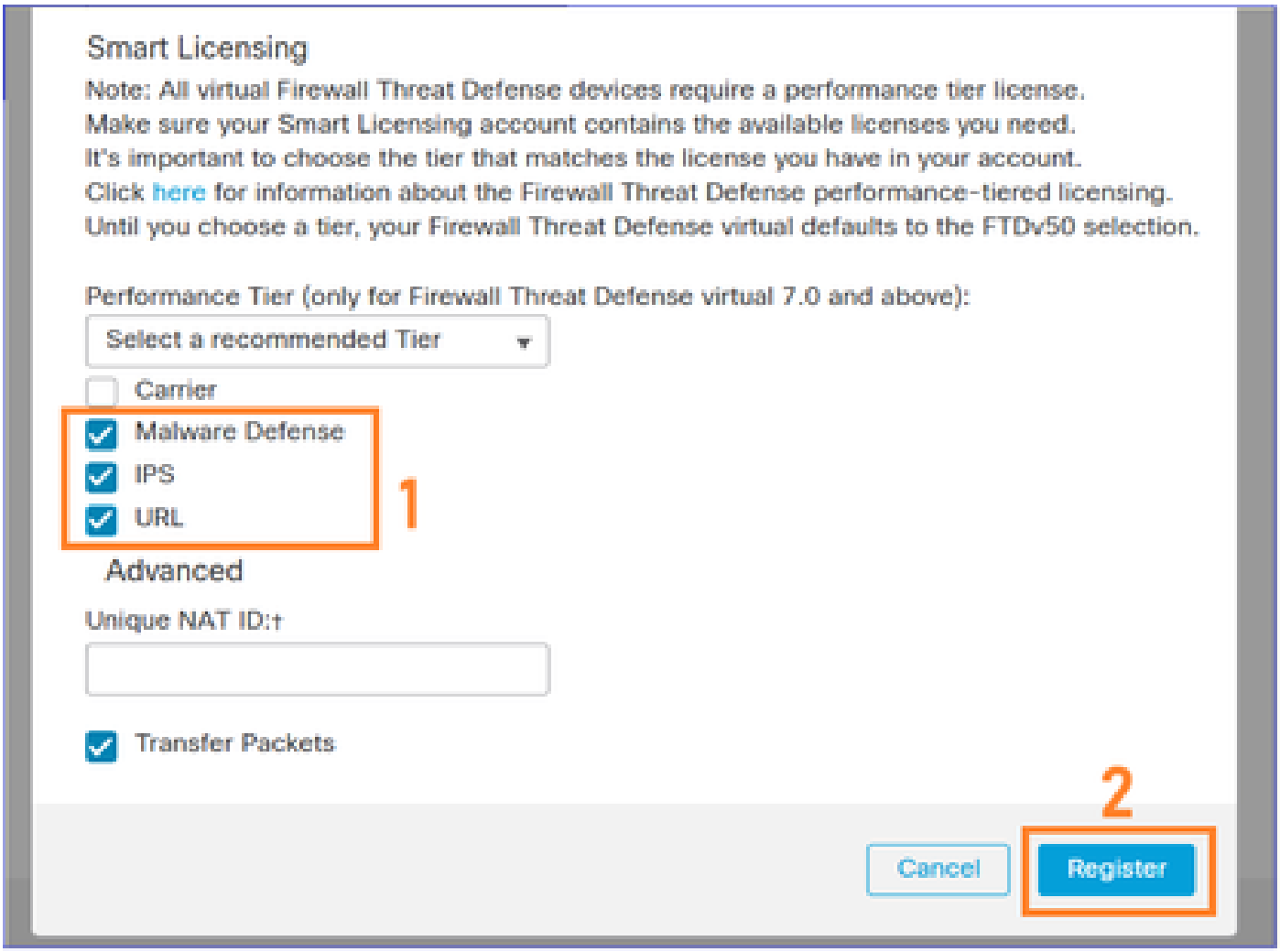


Se o registro do dispositivo falhar, consulte este documento para solucionar o problema: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

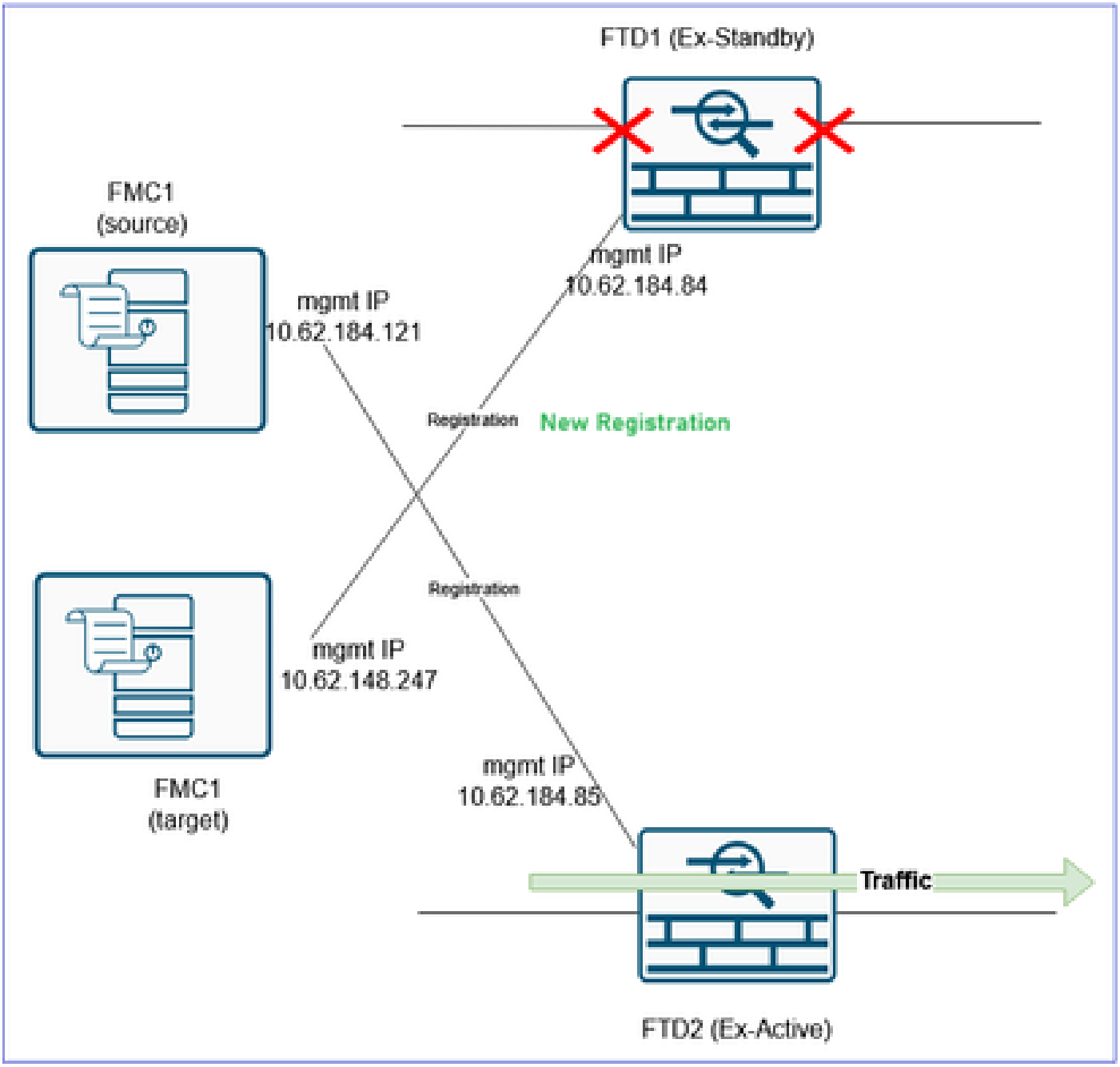
Atribua a Política de Controle de Acesso que você importou na etapa anterior:



Aplique as licenças necessárias e registre o dispositivo:


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

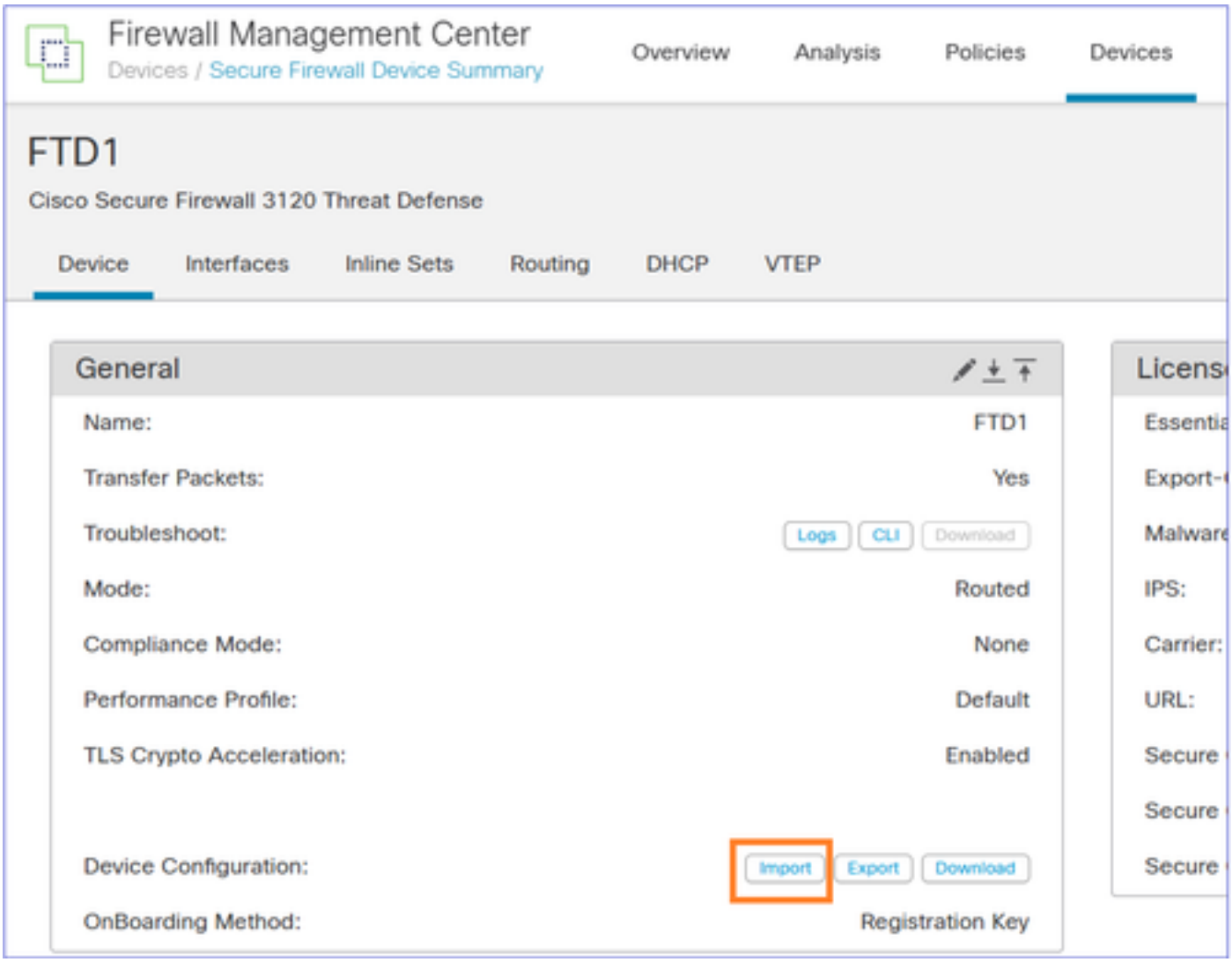
O resultado:



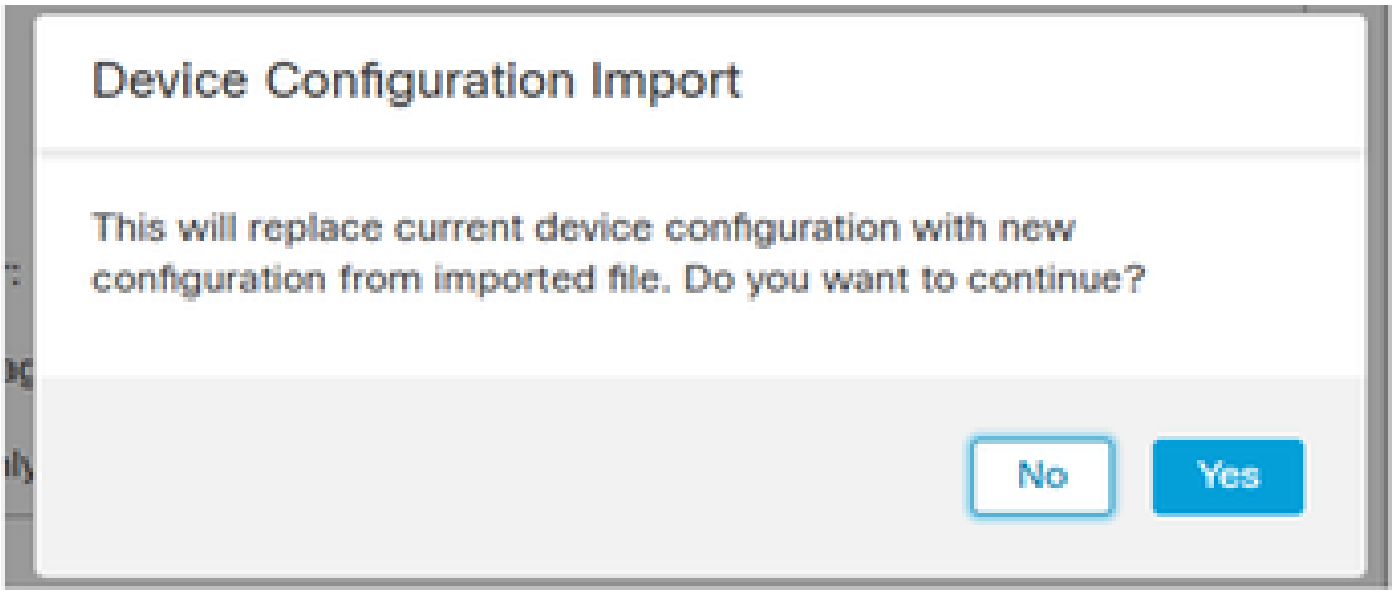
Etapa 9. Importar o objeto de configuração do dispositivo FTD para o FMC2 (FMC de destino)

Faça login no FMC2 (FMC de destino), navegue para Devices > Device Management e Edit o dispositivo FTD que você registrou na etapa anterior.

Navegue até a guia Device e Import o objeto SFO FTD Policies que você exportou na etapa 2:

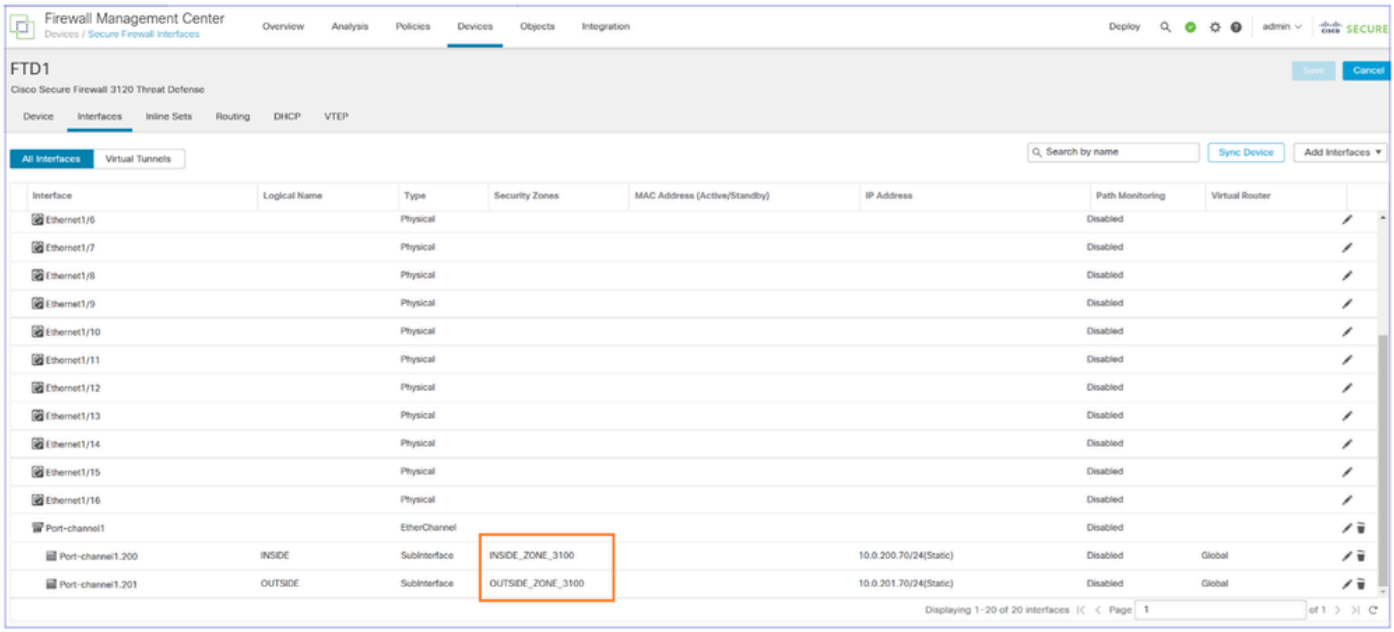


Note: Caso na Etapa 7 você tenha optado pela opção 'b' (Criar uma nova política), assegure-se de reatribuir os objetos recém-criados para as políticas migradas (Zonas de segurança do ACP, Zonas de segurança do NAT, Roteamento, Configurações da plataforma, etc.).



Uma tarefa do FMC é iniciada.

A configuração do dispositivo é aplicada no FTD1, por exemplo, Zonas de Segurança, ACP, NAT e assim por diante:



Caution: Se você tiver um ACP que se expande para muitos Elementos de Controle de Acesso, o processo de compilação do ACP (compilação de correspondência) pode levar vários minutos para ser concluído. Você pode usar este comando para verificar o status de compilação do ACP:

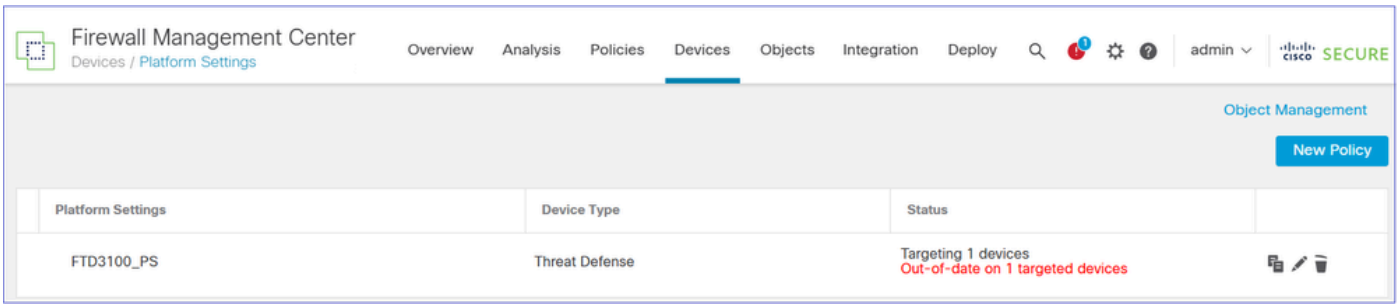
```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

Etapa 10. Finalizar a Configuração do FTD

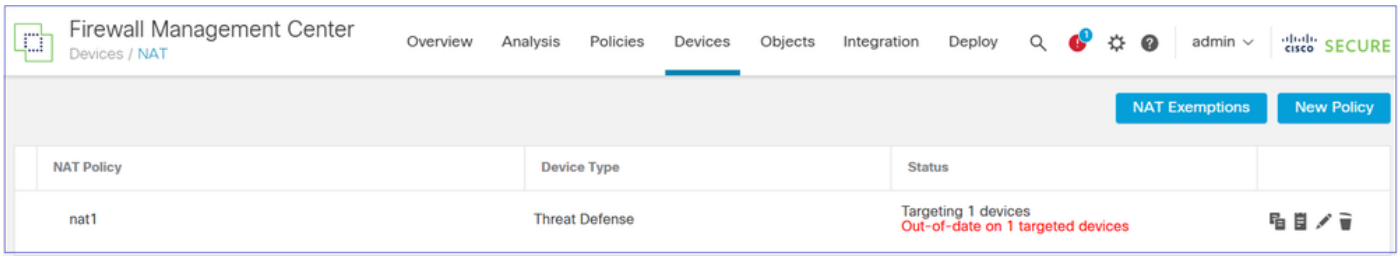
Neste ponto, o objetivo é configurar todos os recursos que ainda podem estar ausentes do FTD1 após o registro no FMC2 (FMC de destino) e a importação da política do dispositivo.

Assegure-se de que as políticas como NAT, configurações de plataforma, QoS, etc. são atribuídos ao DTF. Você verá que as políticas foram atribuídas, mas a implantação está pendente.

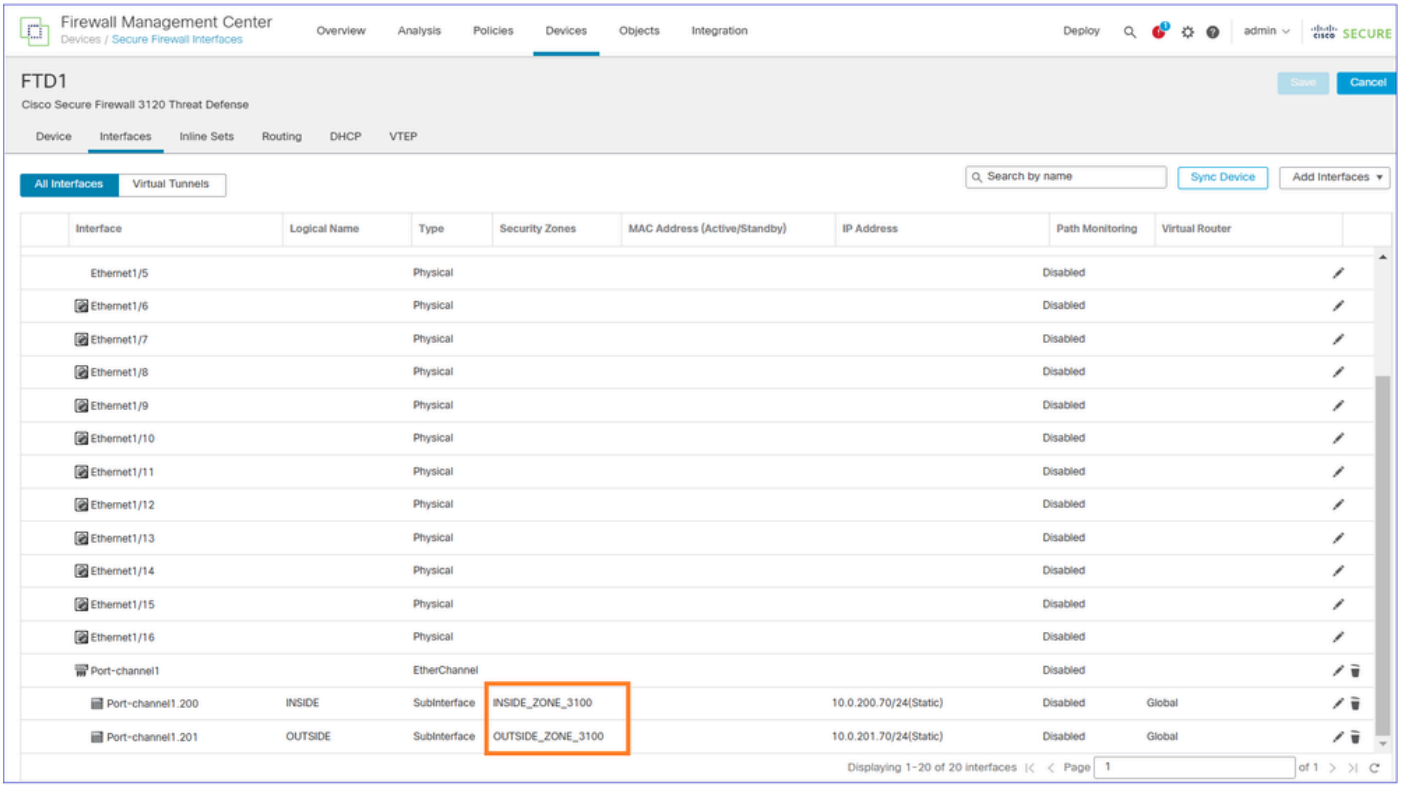
Por exemplo, as configurações da plataforma são importadas e atribuídas ao dispositivo, mas a implantação está pendente:



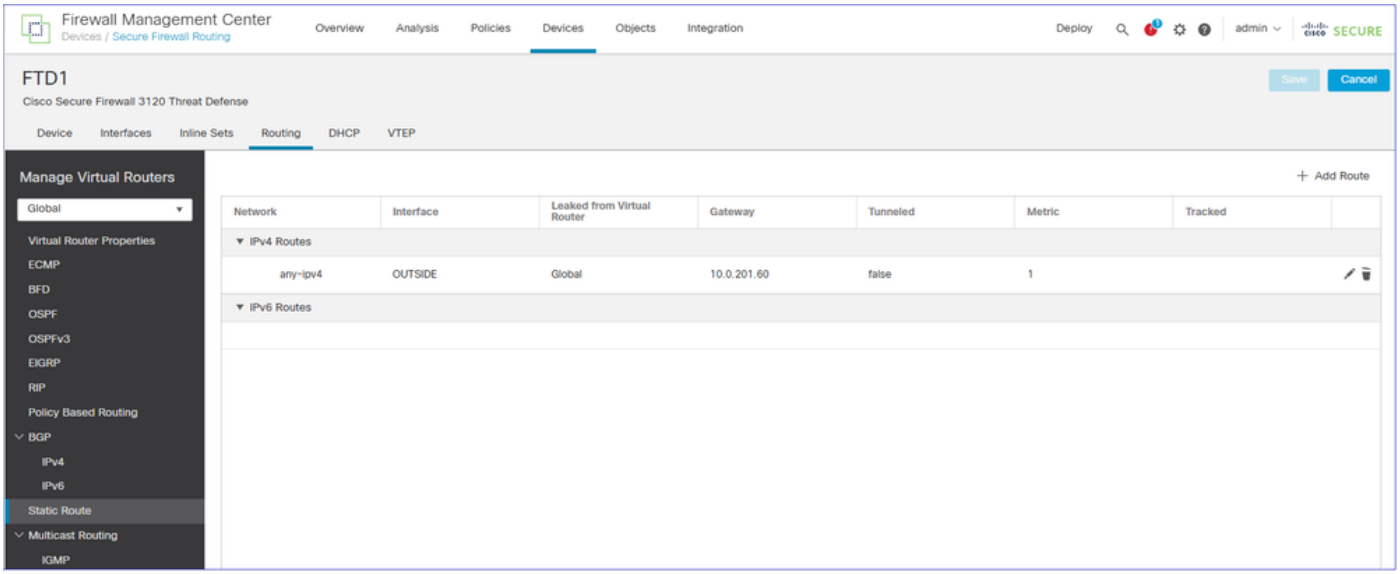
Se o NAT estiver configurado, a política NAT será importada e atribuída ao dispositivo, mas a implantação estará pendente:



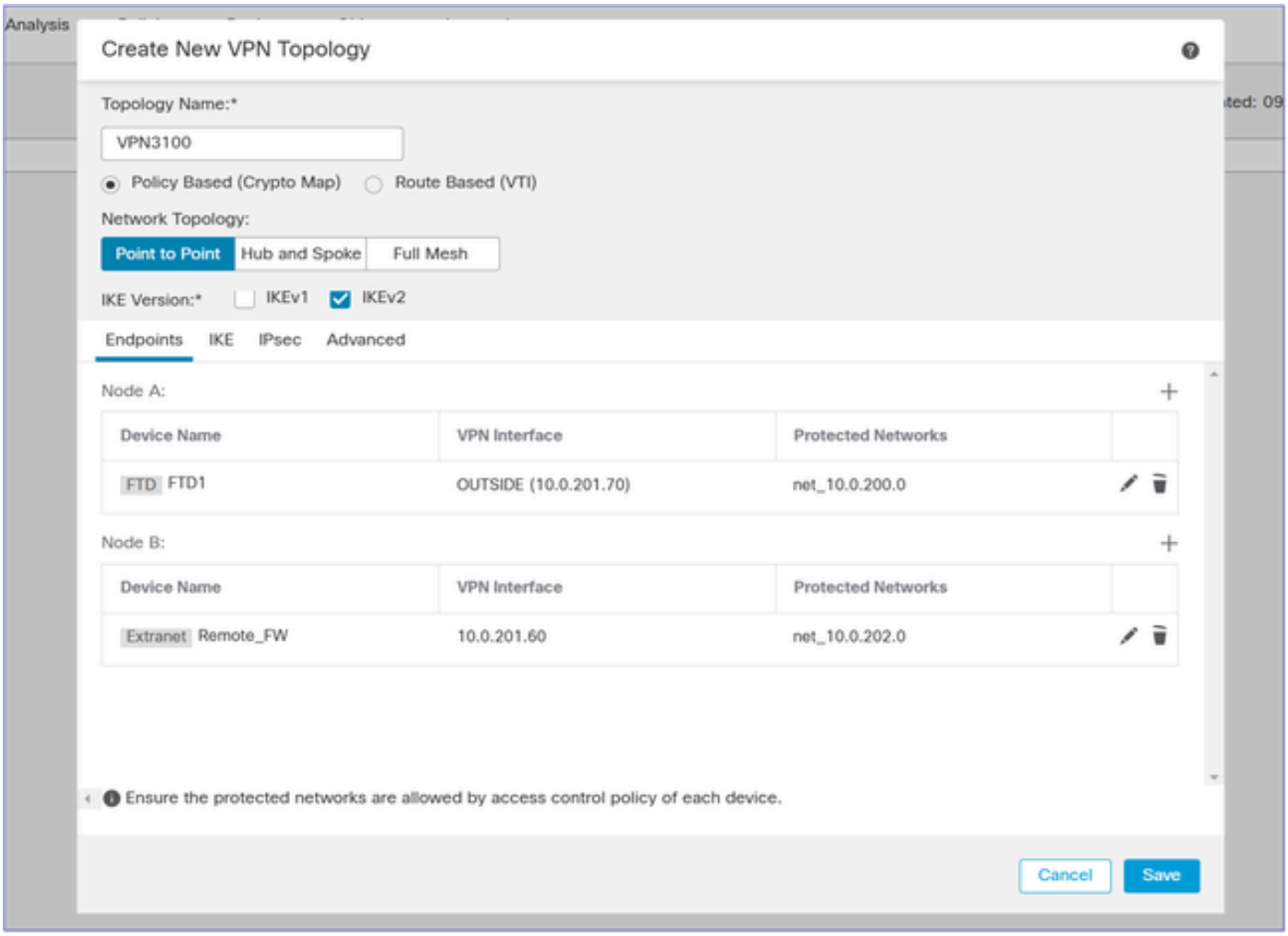
As zonas de segurança são aplicadas às interfaces:



A configuração de roteamento é aplicada ao dispositivo FTD:

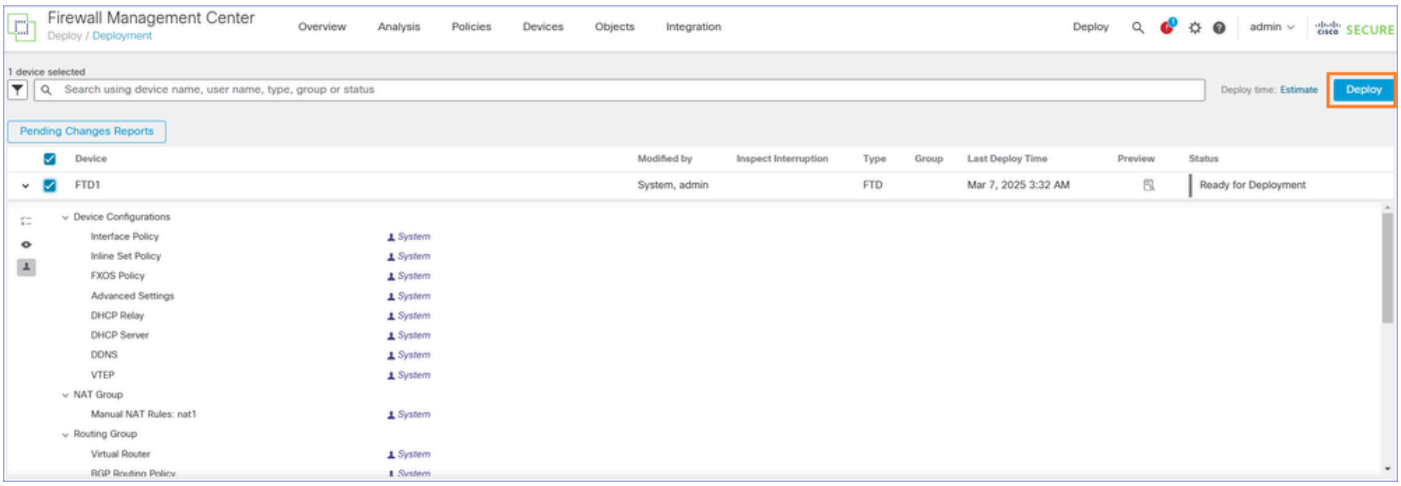


Note: Agora é a hora de configurar as políticas que não podem ser migradas automaticamente (por exemplo, VPNs).



Note: Se o FTD migrado tiver pares VPN S2S que também são migrados para o FMC de destino, você terá que configurar o VPN depois de mover todos os FTDs para o FMC de destino.

Implantar as alterações pendentes:



Etapa 11. Verificar a Configuração do FTD disponibilizado

Neste ponto, o objetivo é verificar a partir da CLI do FTD se toda a configuração está em vigor.

A sugestão é comparar a saída ‘show running-config’ de ambos os FTDs. Você pode usar ferramentas como WinMerge ou diff para a comparação.

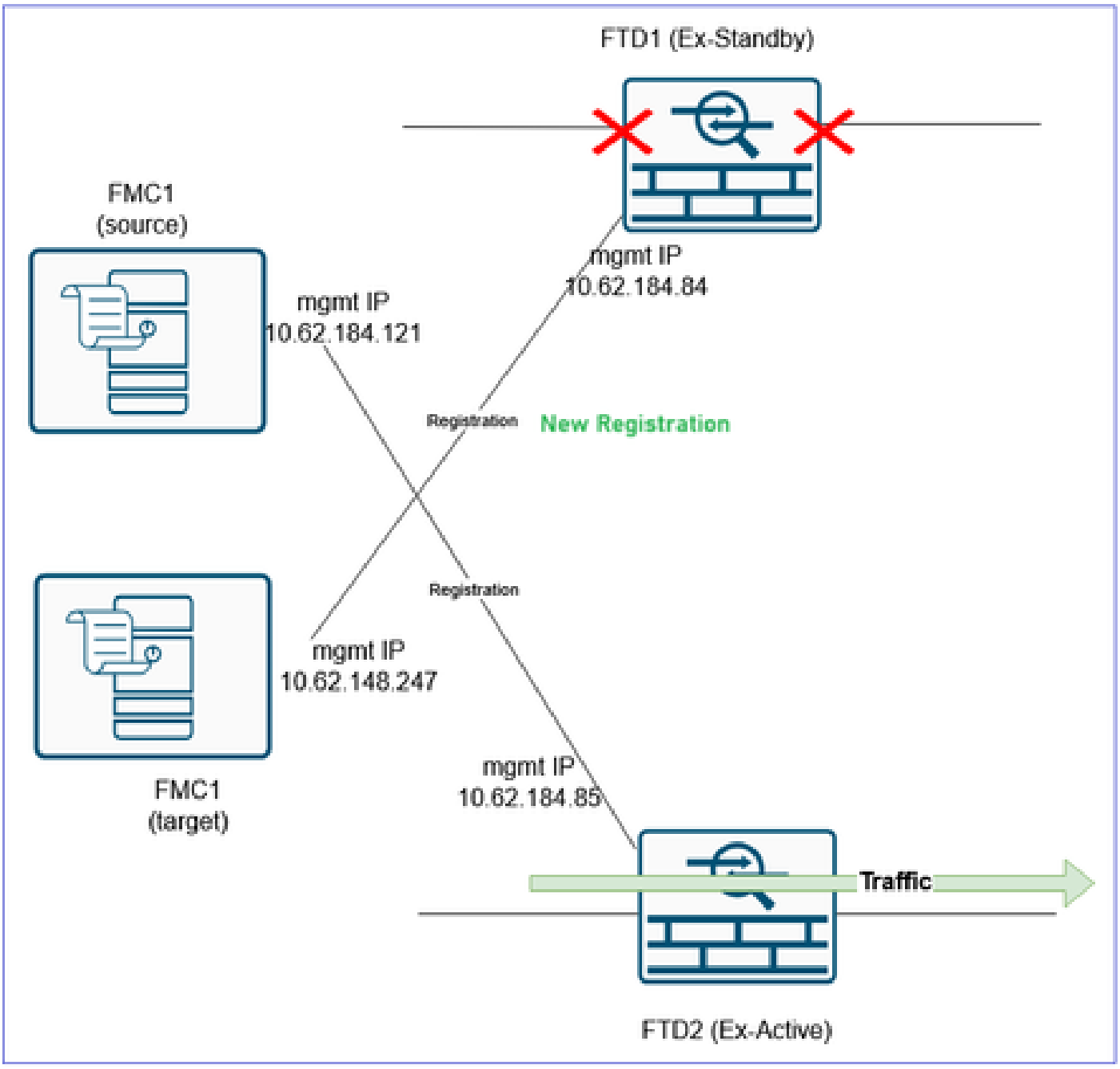
As diferenças que você vê e são normais são:

- Número de série do dispositivo
- Descrições de interface
- ACL rule-ids
- Configuração Cryptochecksum

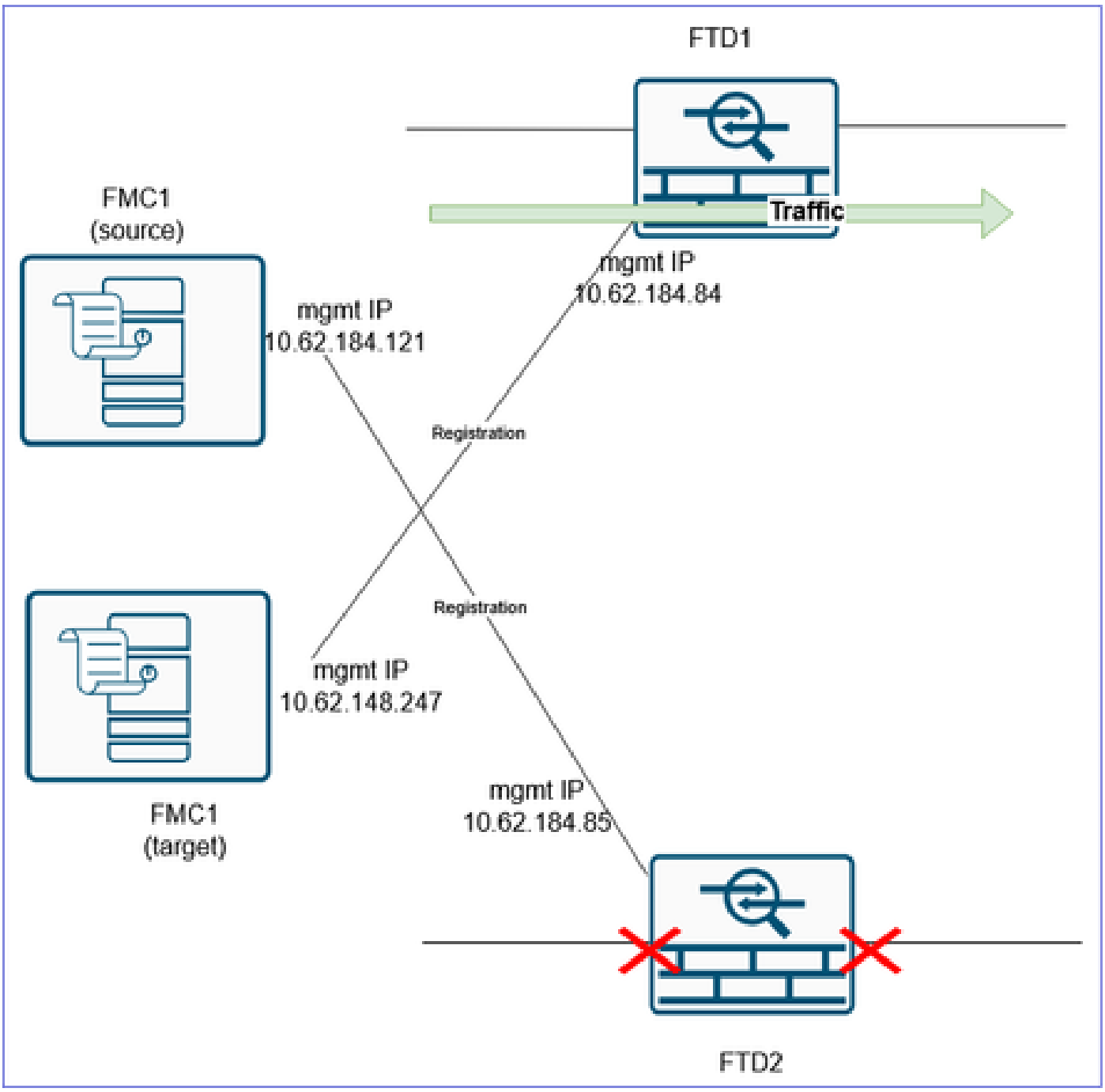
Etapa 12. Fazer a transição

Nesta etapa, o objetivo é transferir o tráfego do FTD2 que está atualmente a processar o tráfego e ainda está registrado para o FMC antigo/de origem para o FTD1 que está registrado para o FMC de destino.

Antes:


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)

Após:



⚠ Caution: Organize um MW para fazer a transição. Durante a transição, você terá alguma interrupção de tráfego até que todo o tráfego seja desviado para o FTD1, as VPNs sejam restabelecidas e assim por diante.

⚠ Caution: Não inicie a transição, a menos que a compilação do ACP seja concluída (consulte a etapa 10 acima).

⚠ aviso: Certifique-se de desconectar os cabos de dados do FTD2 ou de desligar as portas do switch relacionadas. Caso contrário, você pode acabar com os dois dispositivos lidando com o tráfego!

⚠ Caution: Como ambos os dispositivos usam a mesma configuração IP, há uma necessidade de atualizar o cache ARP dos dispositivos L3 adjacentes. Considere limpar manualmente o cache ARP dos dispositivos adjacentes para agilizar a transferência de tráfego.

Tip: Você também pode enviar um pacote GARP e atualizar o cache ARP dos dispositivos adjacentes usando o comando CLI FTD:

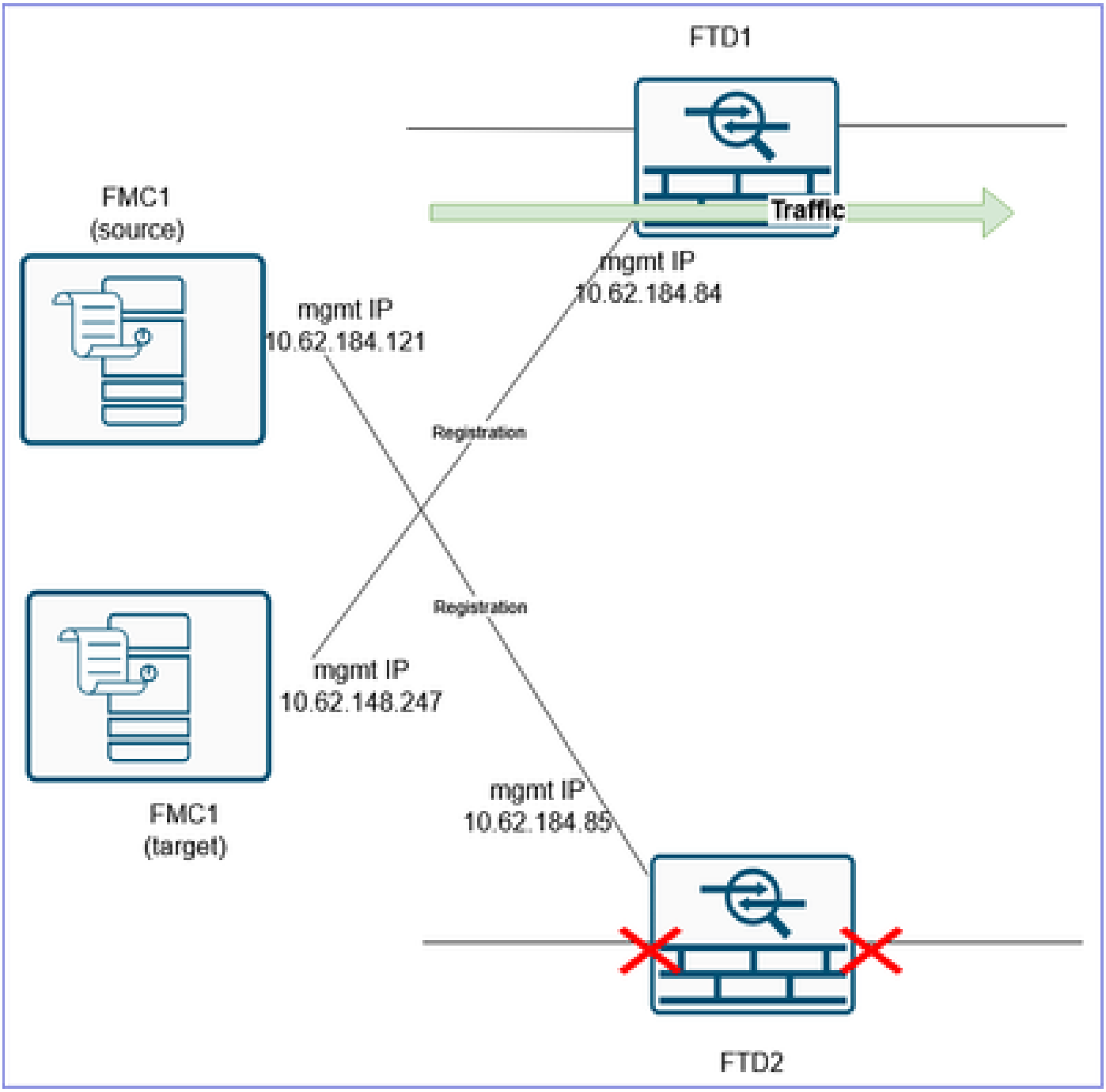
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

Você tem que repetir esse comando para cada IP que o FW possui. Assim, pode ser mais rápido simplesmente limpar o cache ARP dos dispositivos adjacentes do que enviar pacotes GARP para cada IP que o firewall possui.

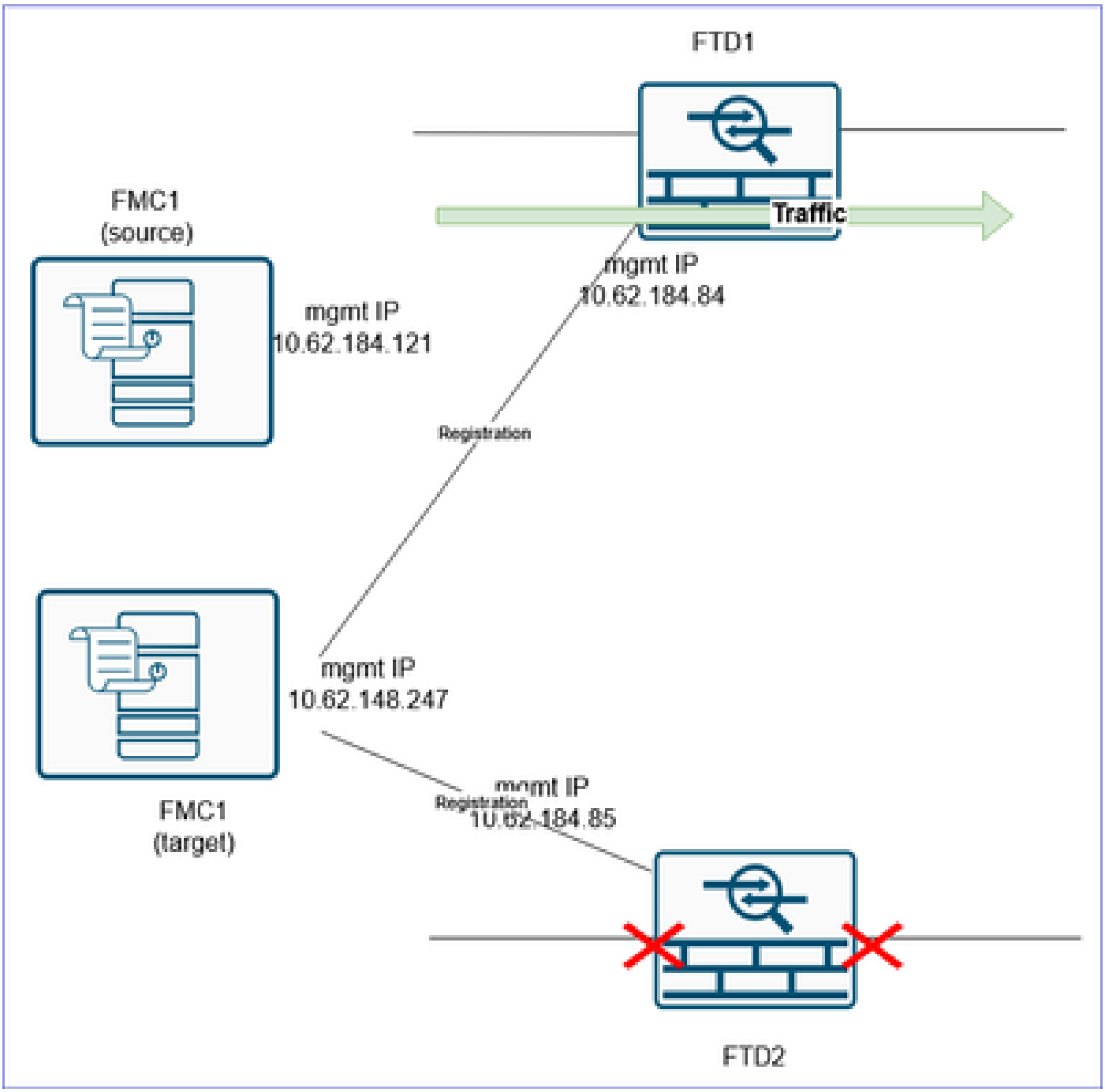
Etapa 13. Migrar o segundo FTD para o FMC2 (FMC de destino)

O último item é reformar o par HA. Para isso, é preciso primeiro excluir o FTD2 do FMC1 (FMC de origem) e registrá-lo no FMC2 (FMC de destino).

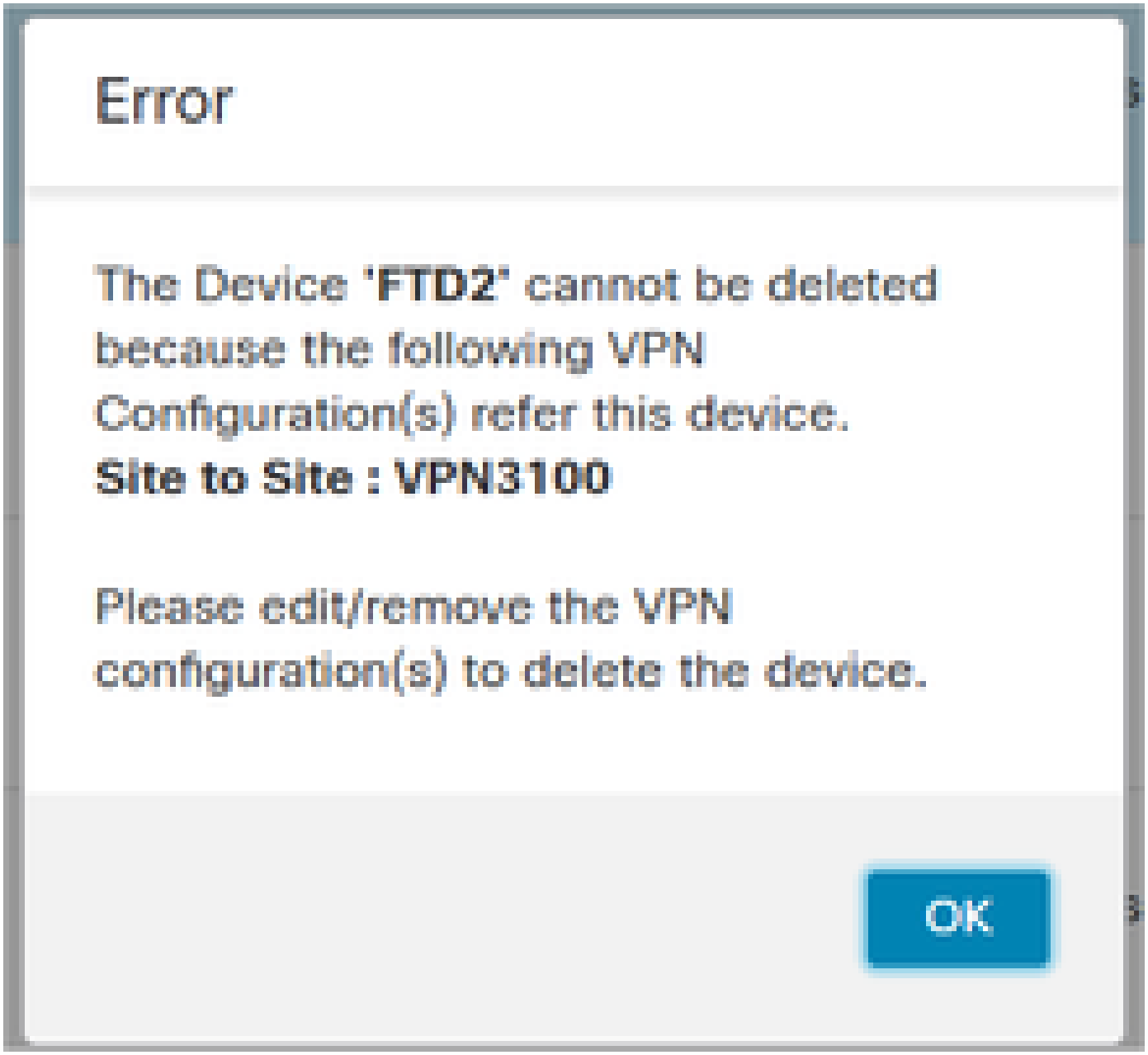
Antes:


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

Após:



Se você tiver uma configuração de VPN anexada ao FTD2, terá que removê-la primeiro antes de excluir o FTD. Em casos diferentes, uma mensagem semelhante a esta é mostrada:



Verificação da CLI:

<#root>

>

show managers

No managers configured.

É uma boa prática apagar toda a configuração do FTD antes de registrá-lo no FMC de destino. Uma maneira rápida de fazer isso é alternar entre os modos do firewall.

Por exemplo, se você tiver o modo roteado, mude para transparente e, em seguida, de volta para

roteado:

<#root>

>

configure firewall transparent

E então:

<#root>

>

configure firewall routed

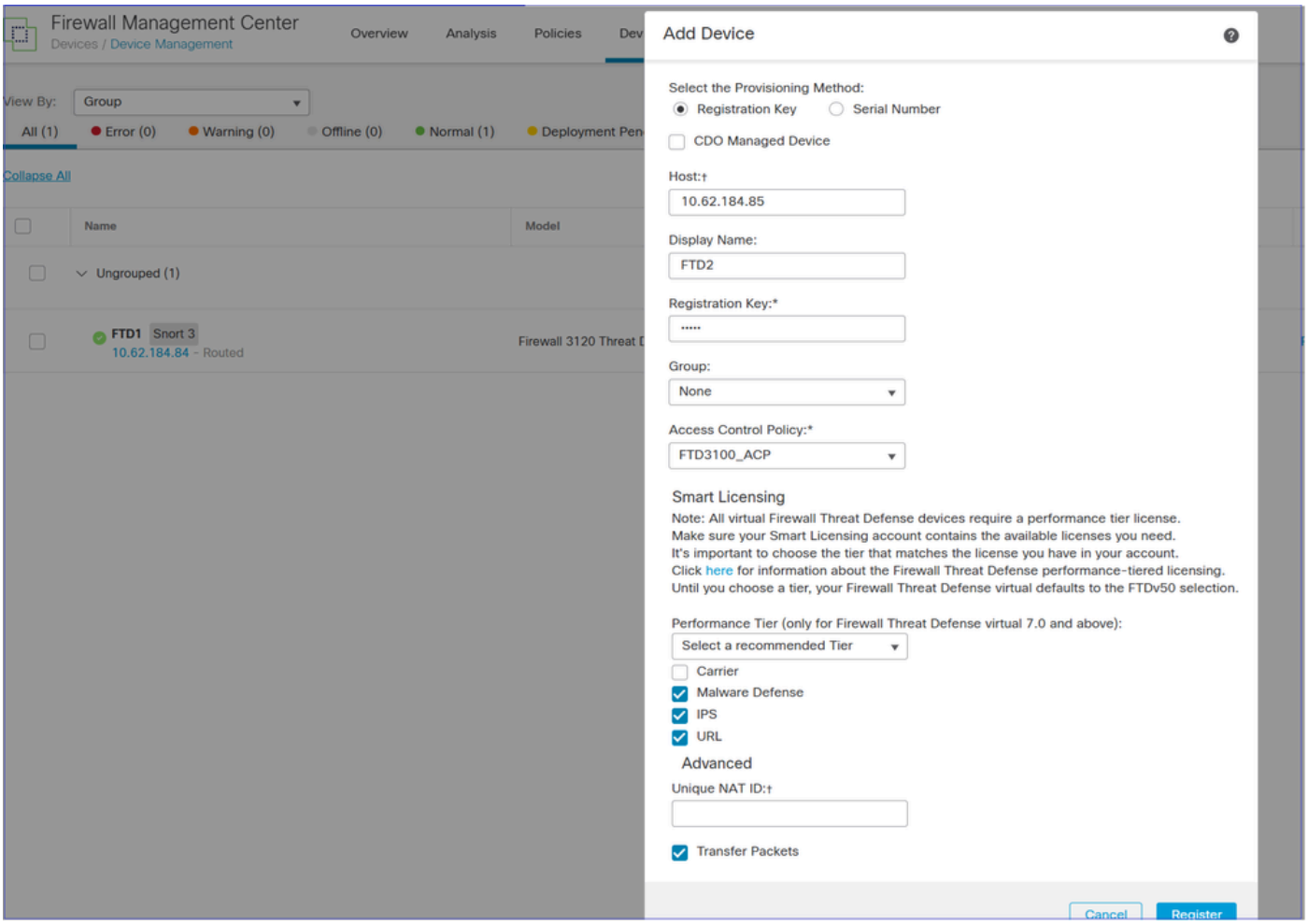
Em seguida, registre-o no FMC2 (FMC de destino):

<#root>

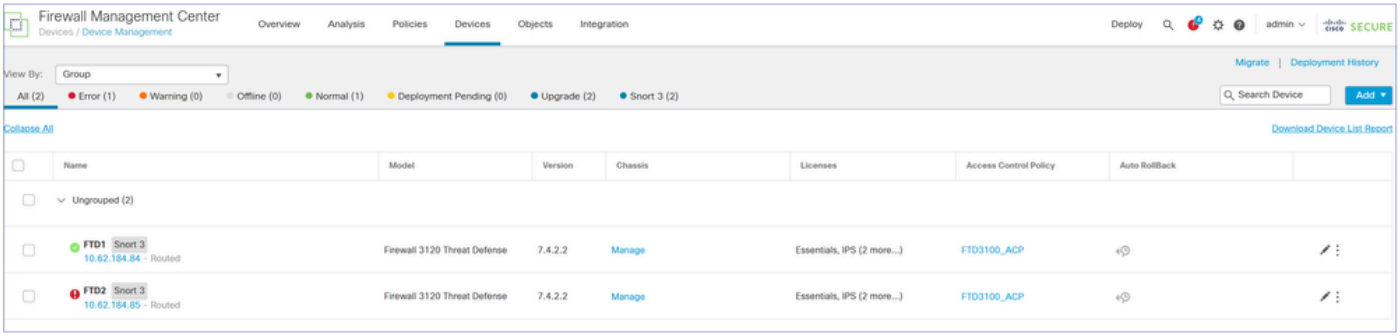
>

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.
>
```



O resultado:

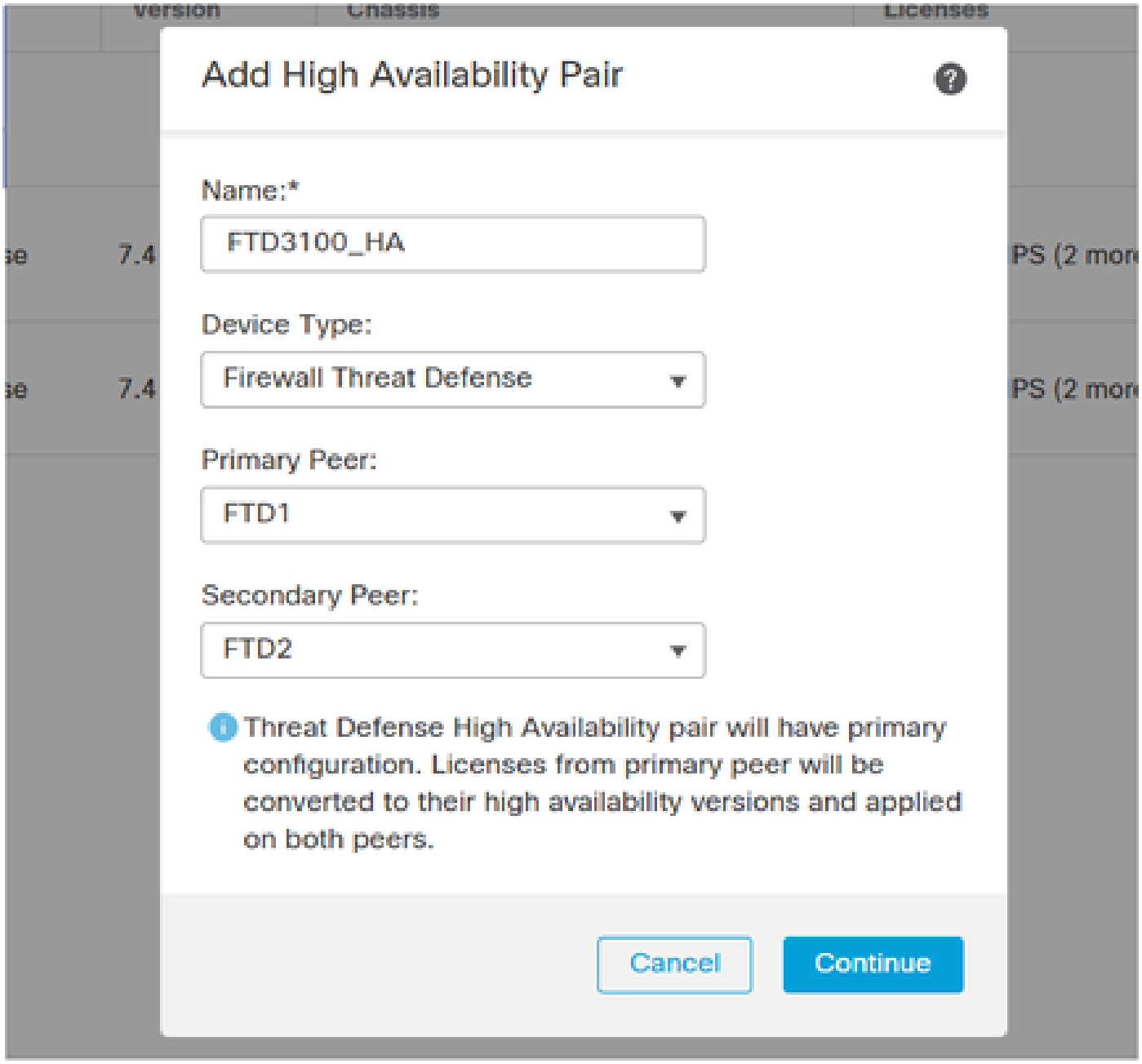


Etapa 14. Reformar o HA do FTD

Note: Essa tarefa (como qualquer tarefa relacionada ao HA) também deve ser executada durante uma MW. Durante a negociação de HA, haverá uma interrupção de tráfego por ~1 minuto, já que as interfaces de dados ficarão inativas.

No FMC de destino, navegue para Devices > Device Management e Add > High Availability.

⚠ Caution: Certifique-se de selecionar como Par Primário o FTD que está tratando o tráfego (FTD1 neste cenário):



Reconfigure as configurações de HA, incluindo interfaces monitoradas, IPs em espera, endereços MAC virtuais e assim por diante.

Verificação do CLI FTD1:

```
<#root>

FTD3100-3#

show failover | include host

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

Verificação do CLI do FTD2:

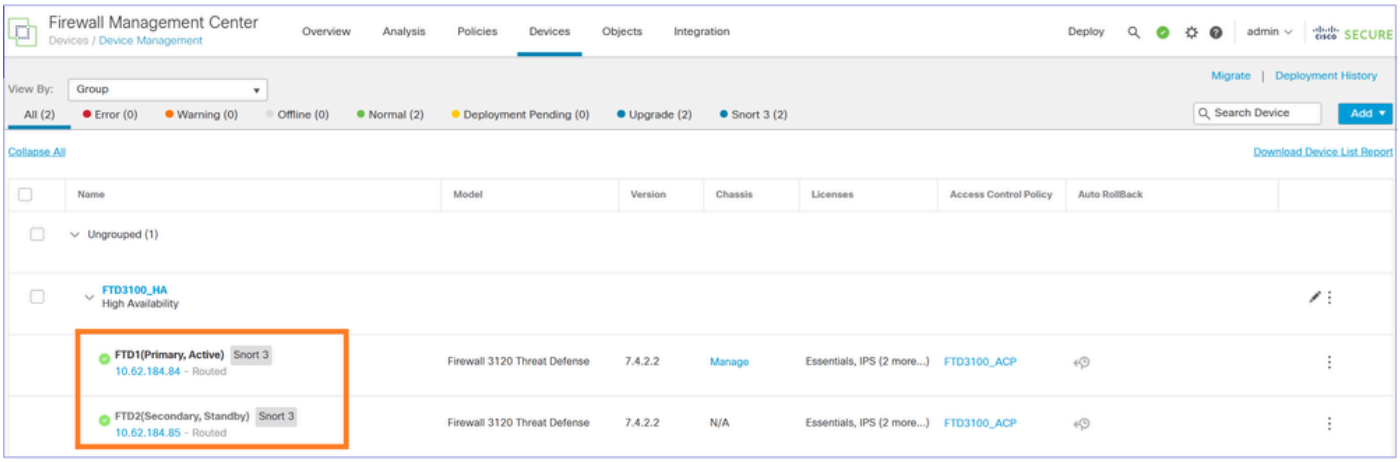
<#root>

FTD3100-3#

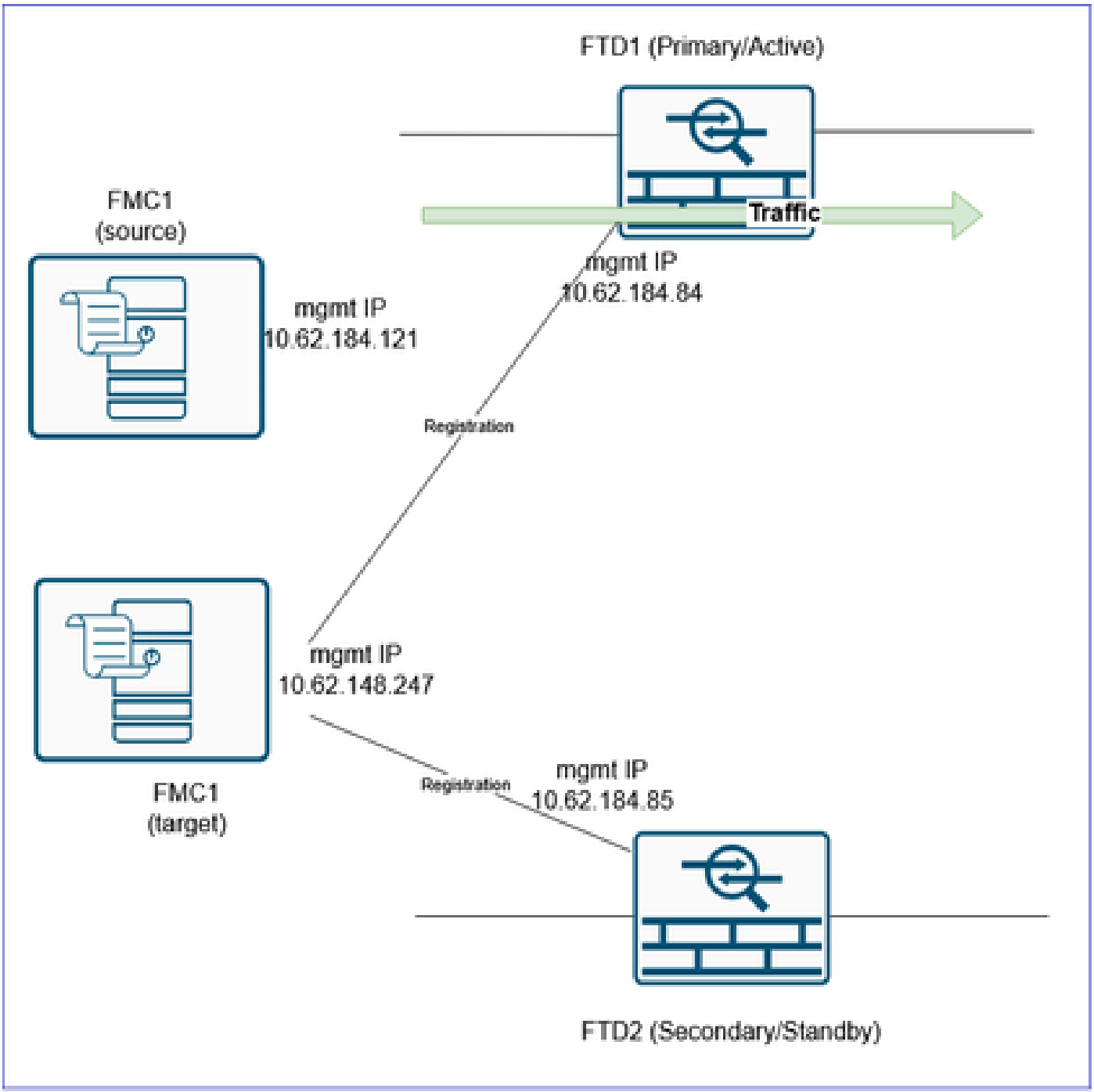
show failover | include host

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

Verificação da interface do usuário do FMC:



Finalmente, ative/reconecte as interfaces de dados do dispositivo FTD2.



Referências

- Exportar e importar a configuração do dispositivo
- Adicionar um par de alta disponibilidade
- Migrar um FTD de um CVP para outro CVP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.