Migración de FTD HA (conmutación por fallo) a otro FMC

Contenido

Introducción

- Abreviaturas
- Prerequisites
- Componentes Utilizados
- Topología

Configurar

- Paso 1. Exportar la configuración del dispositivo desde el firewall principal
- Paso 2. Active el FTD secundario
- Paso 3. Romper el FTD HA
- Paso 4. Aislar las interfaces de datos del FTD1 (antiguo principal)
- Paso 5. Exportación de las Políticas Compartidas de FTD
- Paso 6. Eliminar/anular el registro del FTD1 (antiguo principal) del FMC antiguo/de origen
- Paso 7. Importar el objeto de configuración de la política de FTD al FMC2 (FMC de destino)
- Paso 8. Registro del FTD1 (antiguo primario) en el FMC2
- Paso 9. Importar el objeto de configuración del dispositivo FTD en el FMC2 (FMC de destino)
- Paso 10. Finalización de la configuración de FTD
- Paso 11. Verificar la configuración de FTD implementada
- Paso 12. Realice la transición
- Paso 13. Migrar el segundo FTD al FMC2 (FMC objetivo)
- Paso 14. Reforma del FTD HA

Referencias

Introducción

Este documento describe el procedimiento para migrar un FTD HA de un FMC existente a otro FMC.

Para realizar una migración de firewall independiente a un nuevo 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 control de acceso

ARP = Protocolo de resolución de direcciones

CLI = Interfaz de línea de comandos

FMC = Centro de gestión de firewall seguro

FTD = Defensa frente a amenazas de firewall seguro

GARP = ARP Gratuito

HA = alta disponibilidad

MW = ventana de mantenimiento

UI = Interfaz de usuario

Prerequisites

Antes de iniciar el proceso de migración, asegúrese de que se cumplen estos requisitos previos:

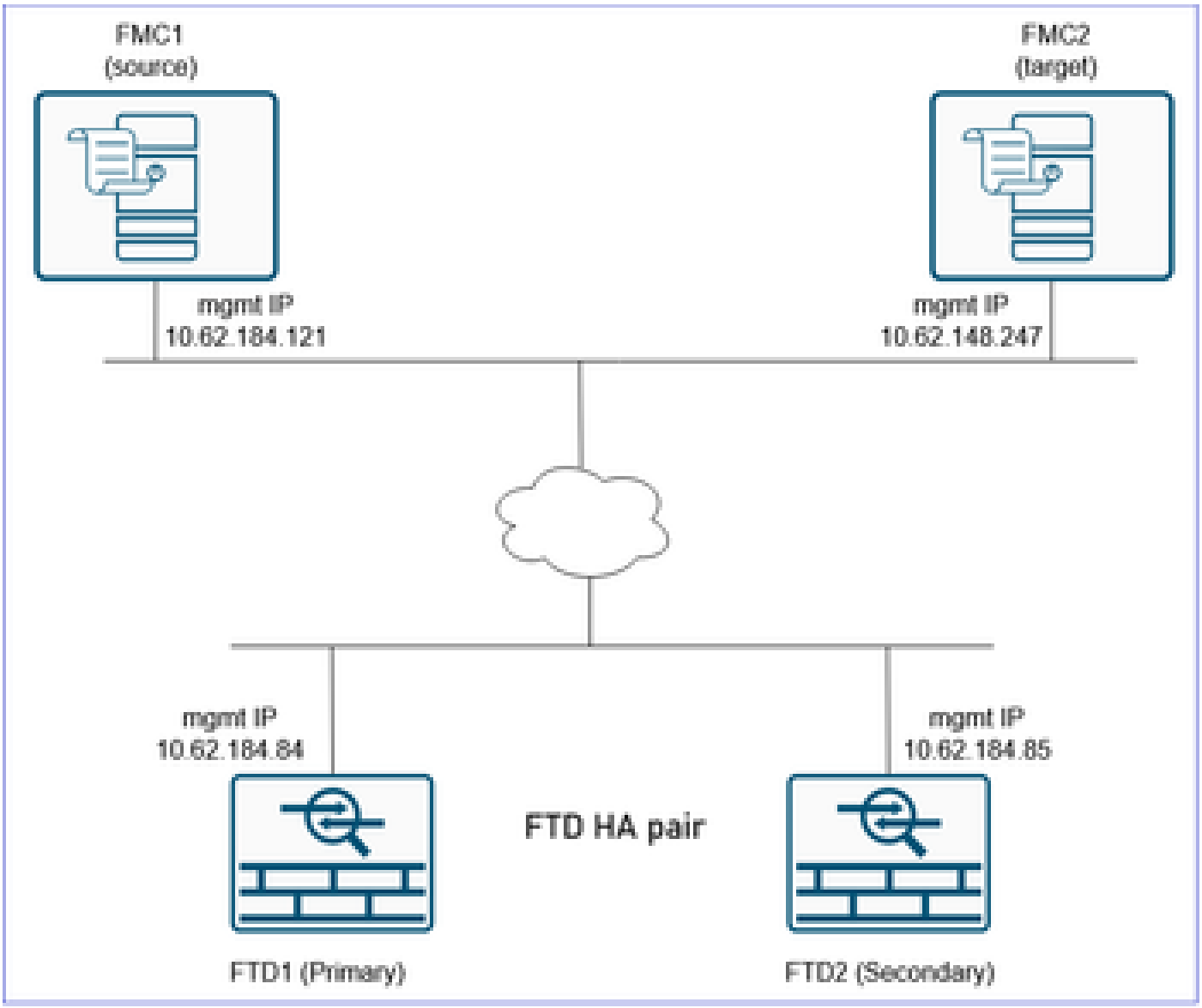
- Acceso a la interfaz de usuario y a la CLI para los CSP de origen y de destino.
- Credenciales administrativas para FMC y firewalls.
- Acceso de consola a ambos firewalls.
- Acceso a los dispositivos de flujo ascendente y descendente L3 (en caso de que necesite borrar la memoria caché ARP).
- Asegúrese de que el CSP de destino/destino tiene la misma versión que el CSP de origen/antiguo.
- Asegúrese de que el CSP de destino/destino tiene las mismas licencias que el CSP de origen/antiguo.
- Asegúrese de organizar un MW para realizar la migración, ya que afectará al tráfico de tránsito.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall 31xx, FTD versión 7.4.2.2.
- Secure Firewall Management Center versión 7.4.2.2.
- La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



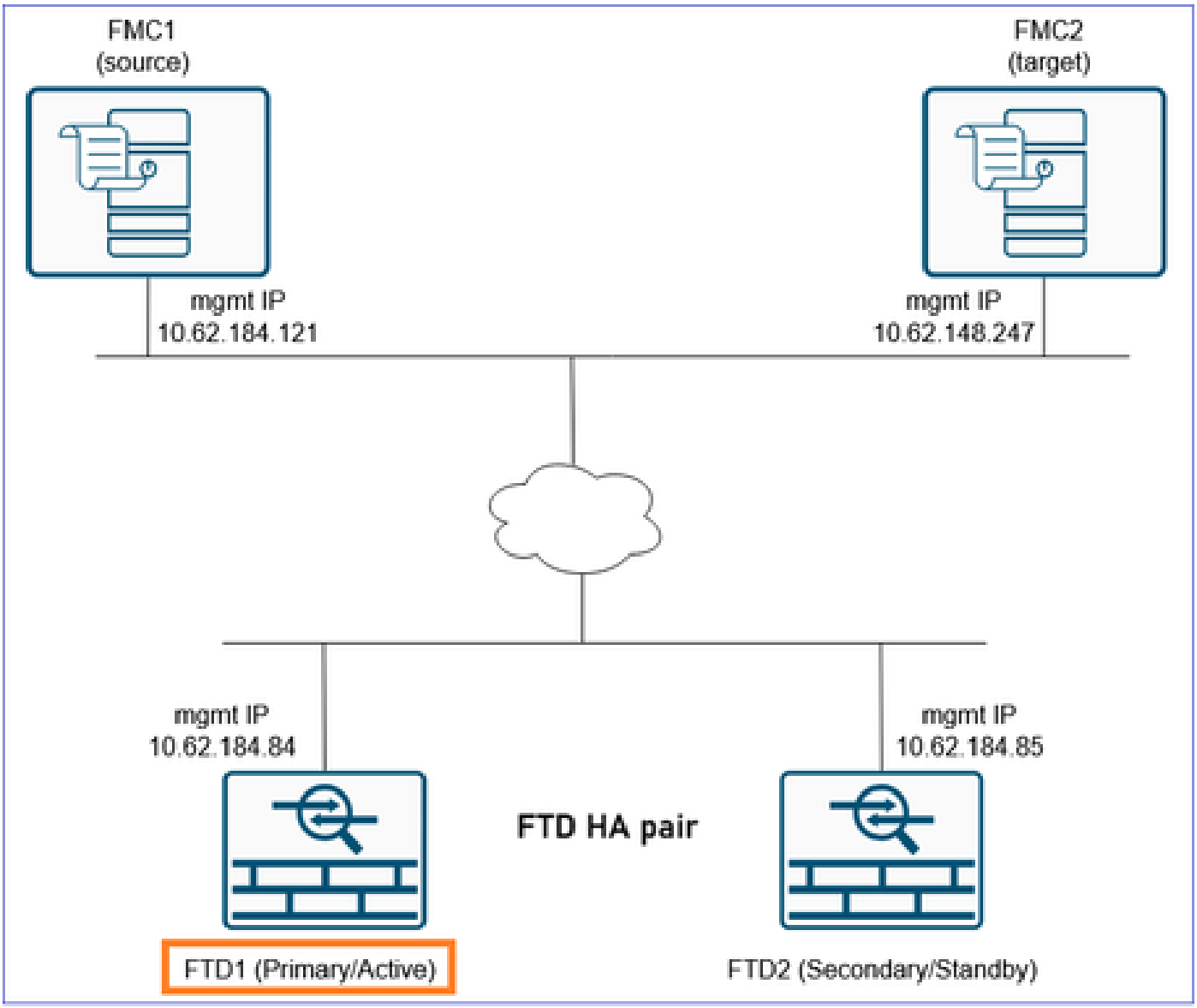
Configurar

Pasos de migración

Para este escenario, consideramos estos estados:

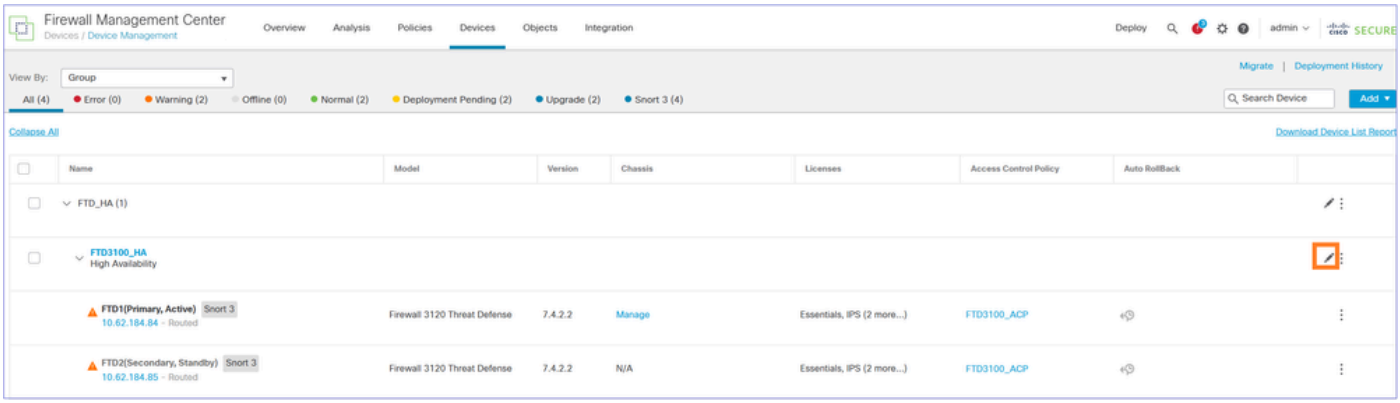
FTD1: Principal/Activo

FTD2: Secundario/En espera

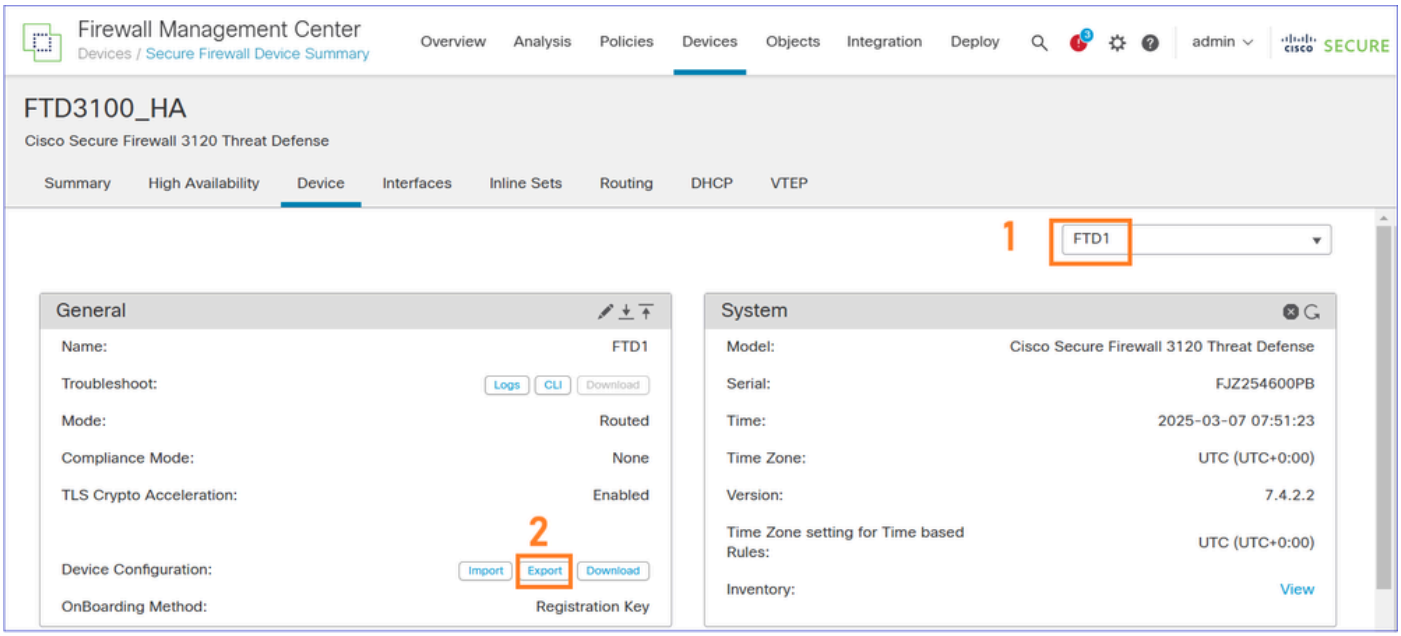


Paso 1. Exportar la configuración del dispositivo desde el firewall principal

En FMC1 (FMC de origen), vaya a Dispositivos > Administración de dispositivos. Seleccione el par FTD HA y seleccione Editar:

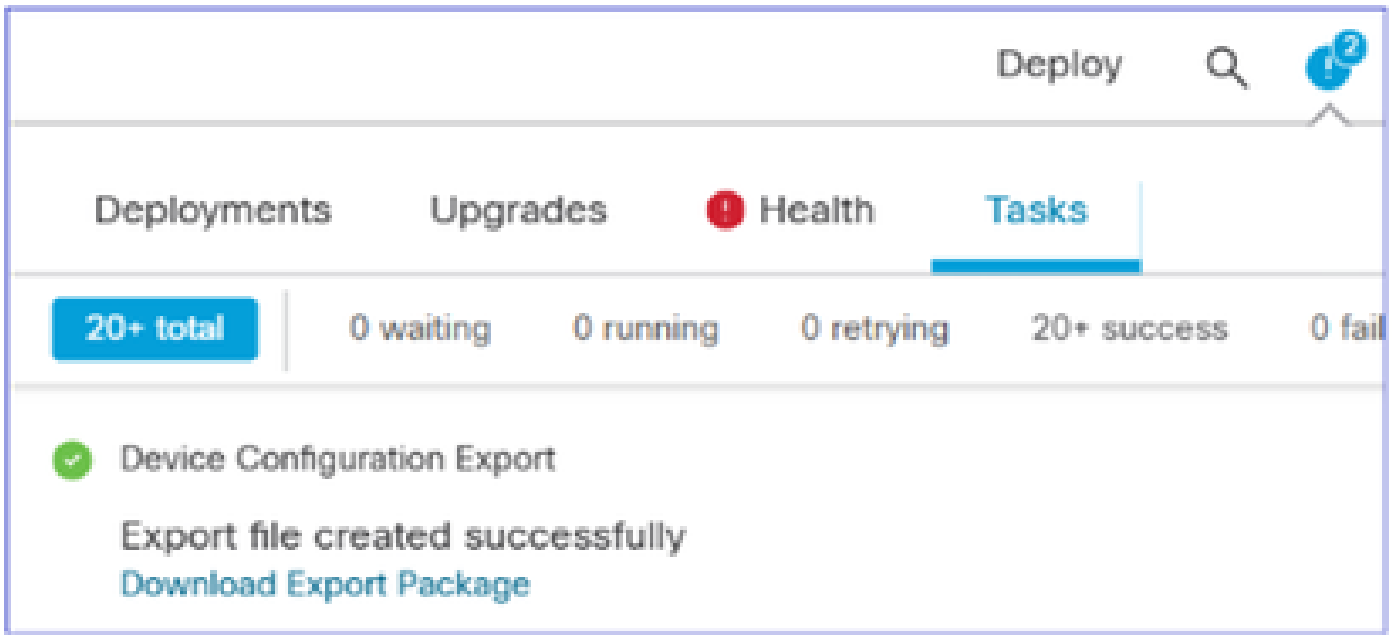


Vaya a la pestaña Device. Asegúrese de que el FTD principal/activo (FTD1 en este caso) esté seleccionado y seleccione Exportar para exportar la configuración del dispositivo:



Nota: La opción Exportar está disponible a partir de la versión de software 7.1 y posteriores.

Puede navegar hasta la página Notifications > Tasks para asegurarse de que la exportación se ha completado. A continuación, seleccione el paquete Download Export:



También puede hacer clic en el botón Download en el área General. Se obtiene un archivo sfo, por ejemplo DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

El archivo contiene una configuración relacionada con el dispositivo como:

- Interfaces enrutadas
- Conjuntos en línea
- Ruteo
- DHCP
- VTEP

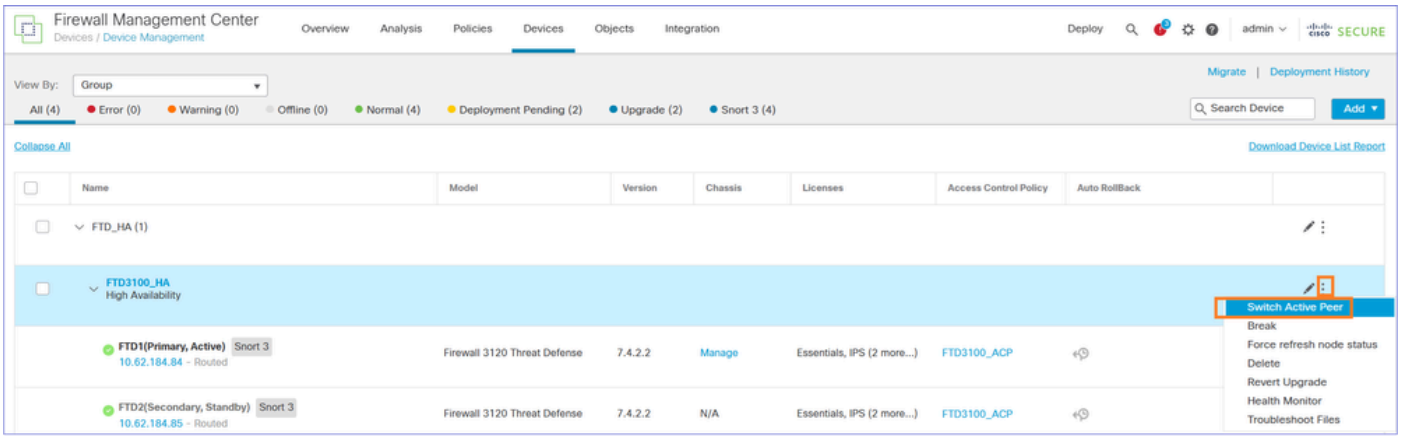
- Objetos asociados

Nota: El archivo de configuración exportado sólo se puede importar al mismo FTD. El UUID del FTD debe coincidir con el contenido del archivo sfo importado. El mismo FTD se puede registrar en otro FMC y se puede importar el archivo sfo.

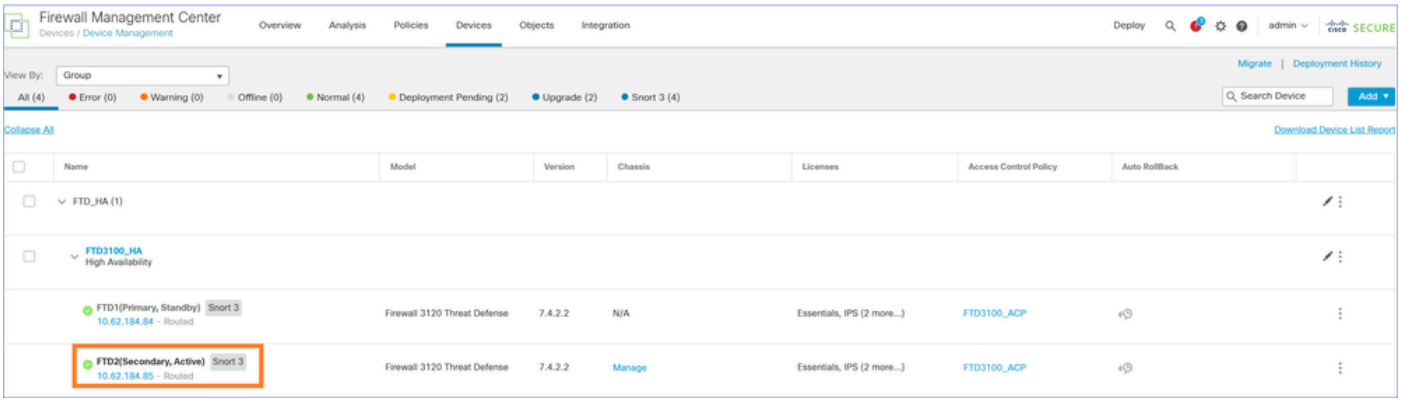
Referencia: 'Exportar e importar la configuración del dispositivo' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

Paso 2. Active el FTD secundario

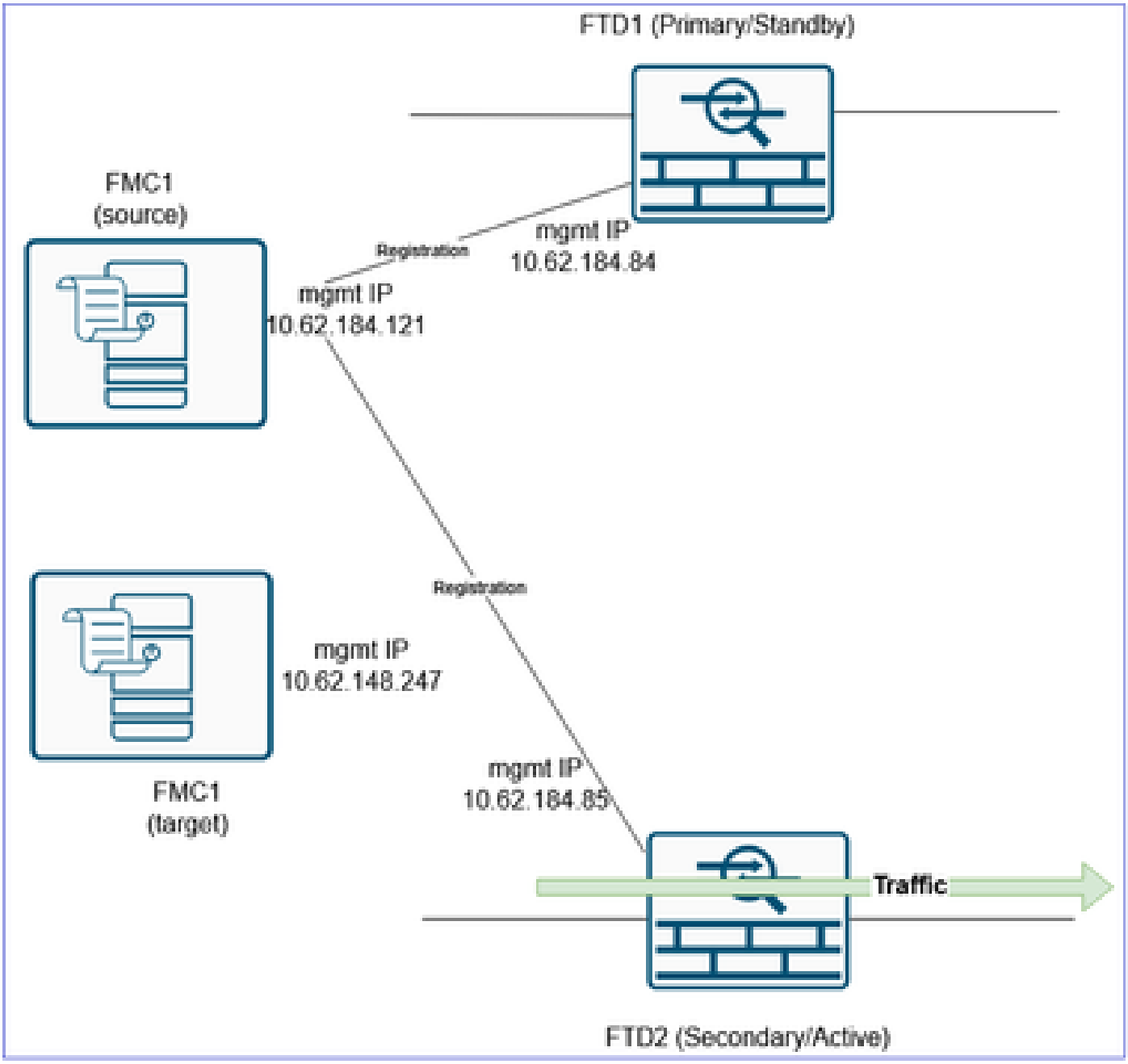
Navegue hasta Devices > Device Management, seleccione el par FTD HA y seleccione Switch Active Pair:



El resultado es FTD1 (principal/en espera) y FTD (secundario/activo):

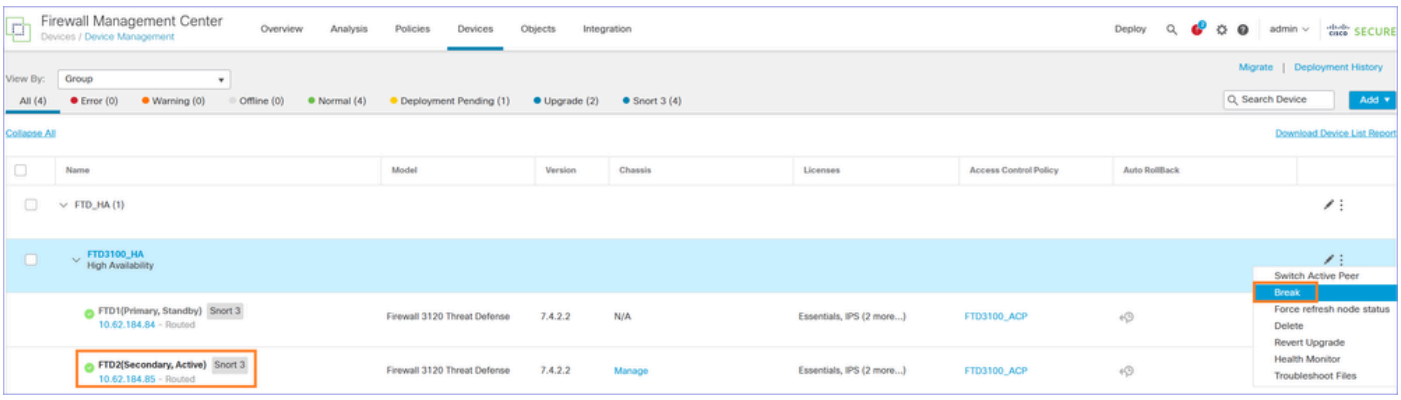


Ahora el tráfico es manejado por el FTD secundario/activo:

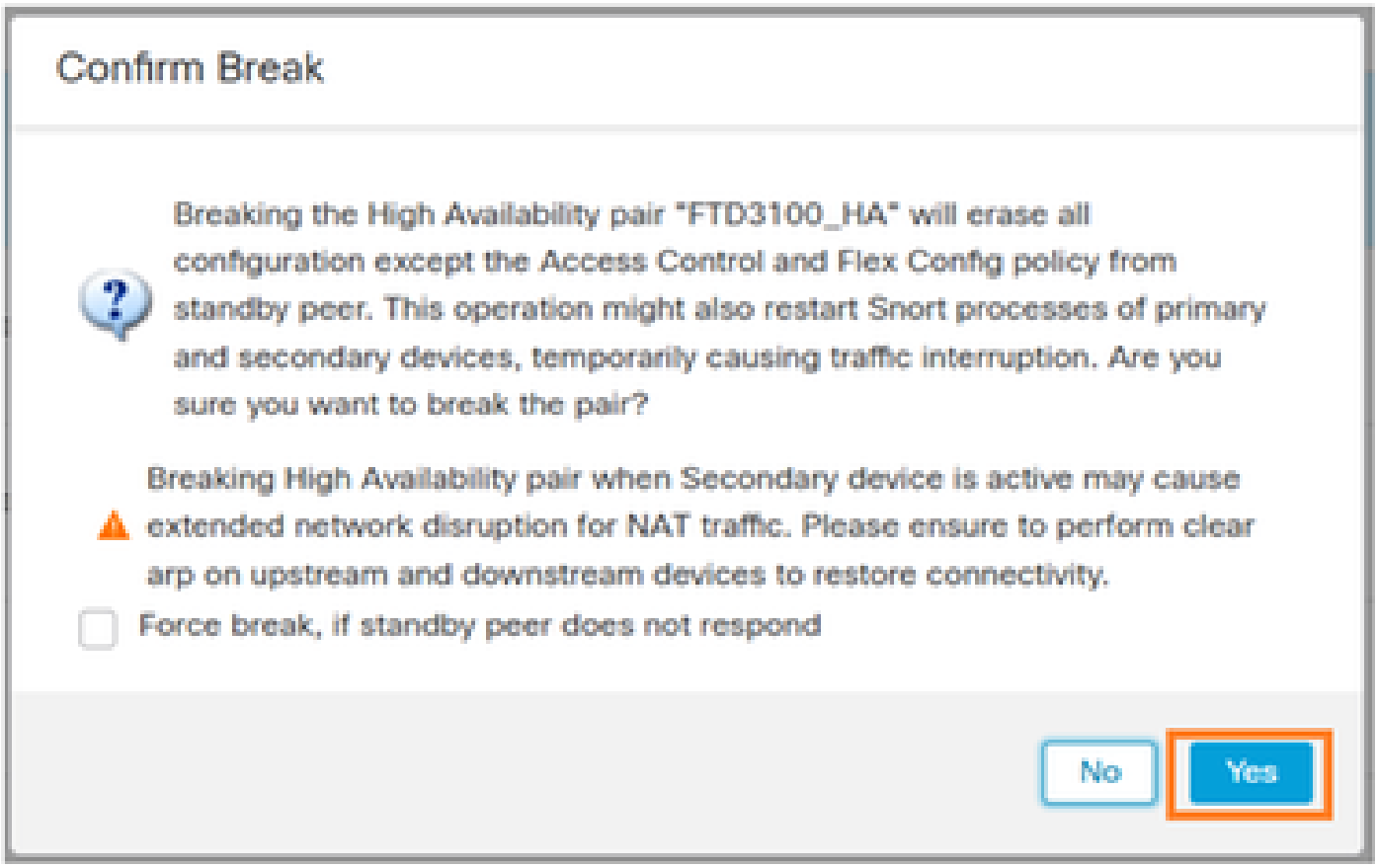


Paso 3. Romper el FTD HA

Vaya a Devices > Device Management y Break the FTD HA:



Aparecerá esta ventana. Seleccione Yes (Sí).



Nota: En este punto, puede experimentar una interrupción del tráfico durante unos segundos, ya que el motor Snort se reinicia durante la interrupción de HA. Además, como se menciona en el mensaje, si utiliza NAT y experimenta una interrupción prolongada del tráfico, considere borrar la memoria caché ARP en los dispositivos de flujo ascendente y descendente.

Después de romper el FTD HA, tiene dos FTD independientes en FMC.

Desde el punto de vista de la configuración, el FTD2 (ex-activo) todavía tiene la configuración en su lugar excepto la configuración relacionada con la conmutación por fallas y está manejando el tráfico:

<#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
```

El FTD1 (ex-Standby) tiene toda la configuración eliminada:

<#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#

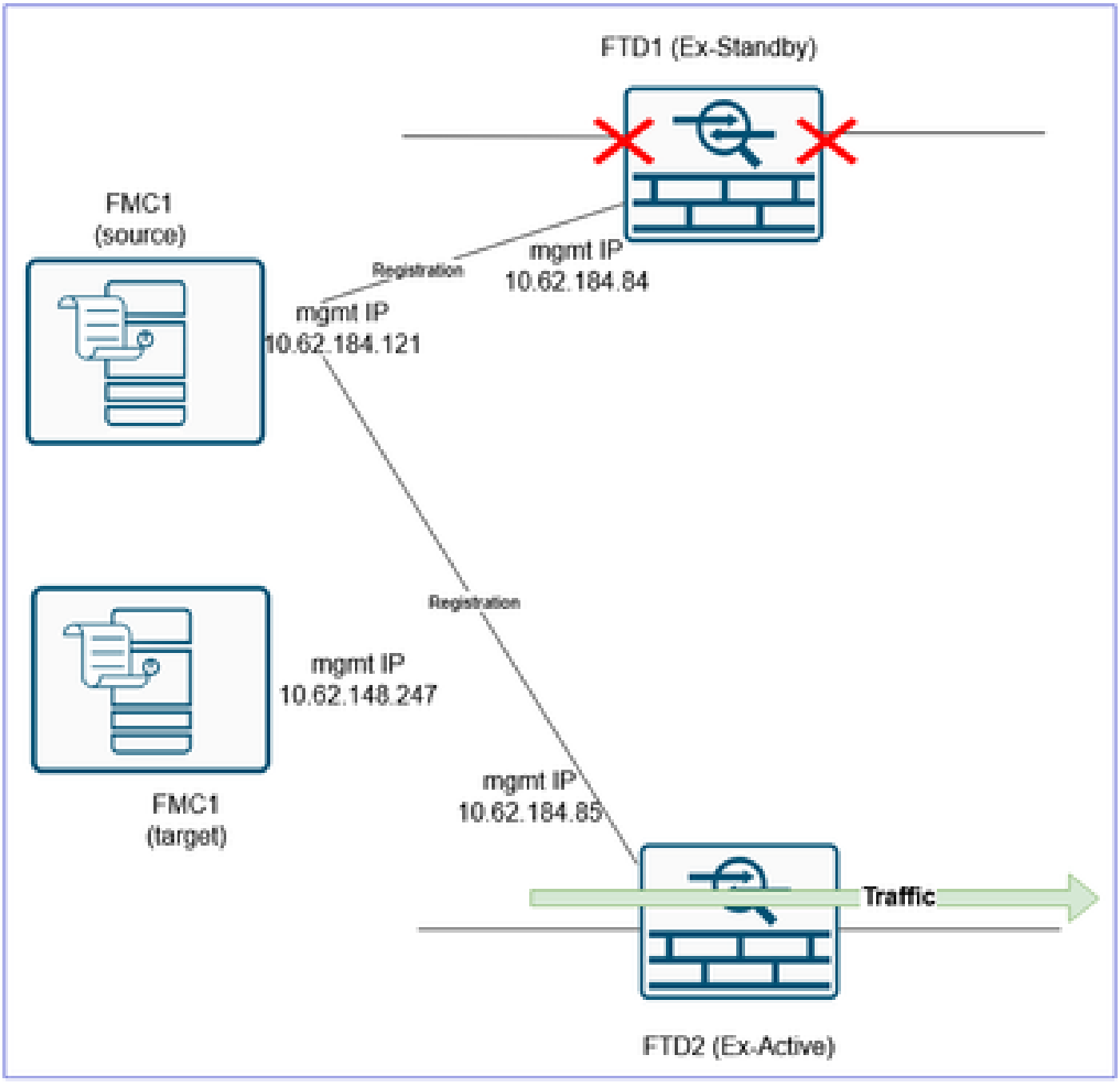
show interface ip brief

```
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
```

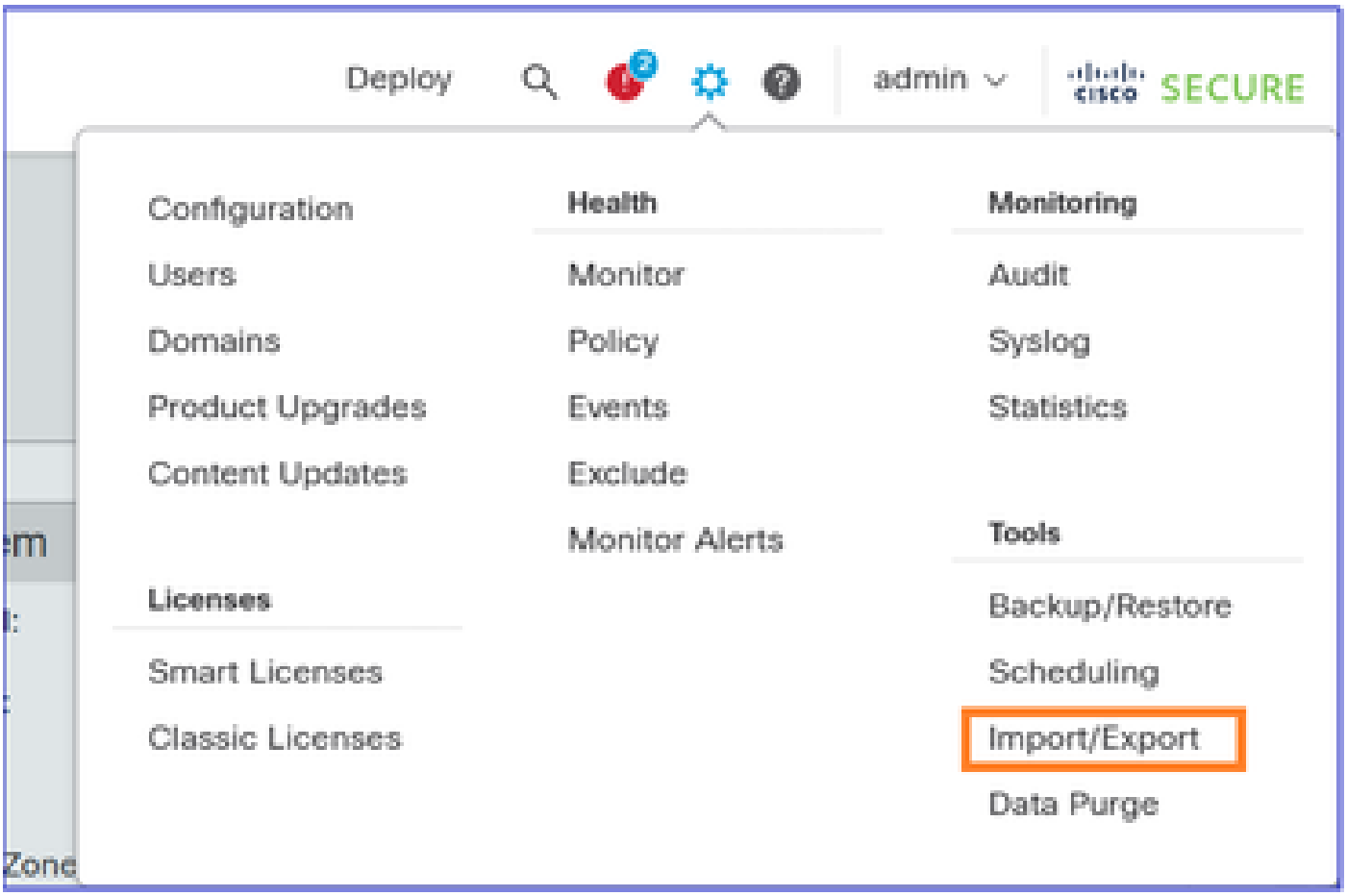
Paso 4. Aislar las interfaces de datos del FTD1 (antiguo principal)

Desconecte los cables de datos del FTD1 (antiguo primario). Deje solo conectado el puerto de administración de FTD.



Paso 5. Exportación de las Políticas Compartidas de FTD

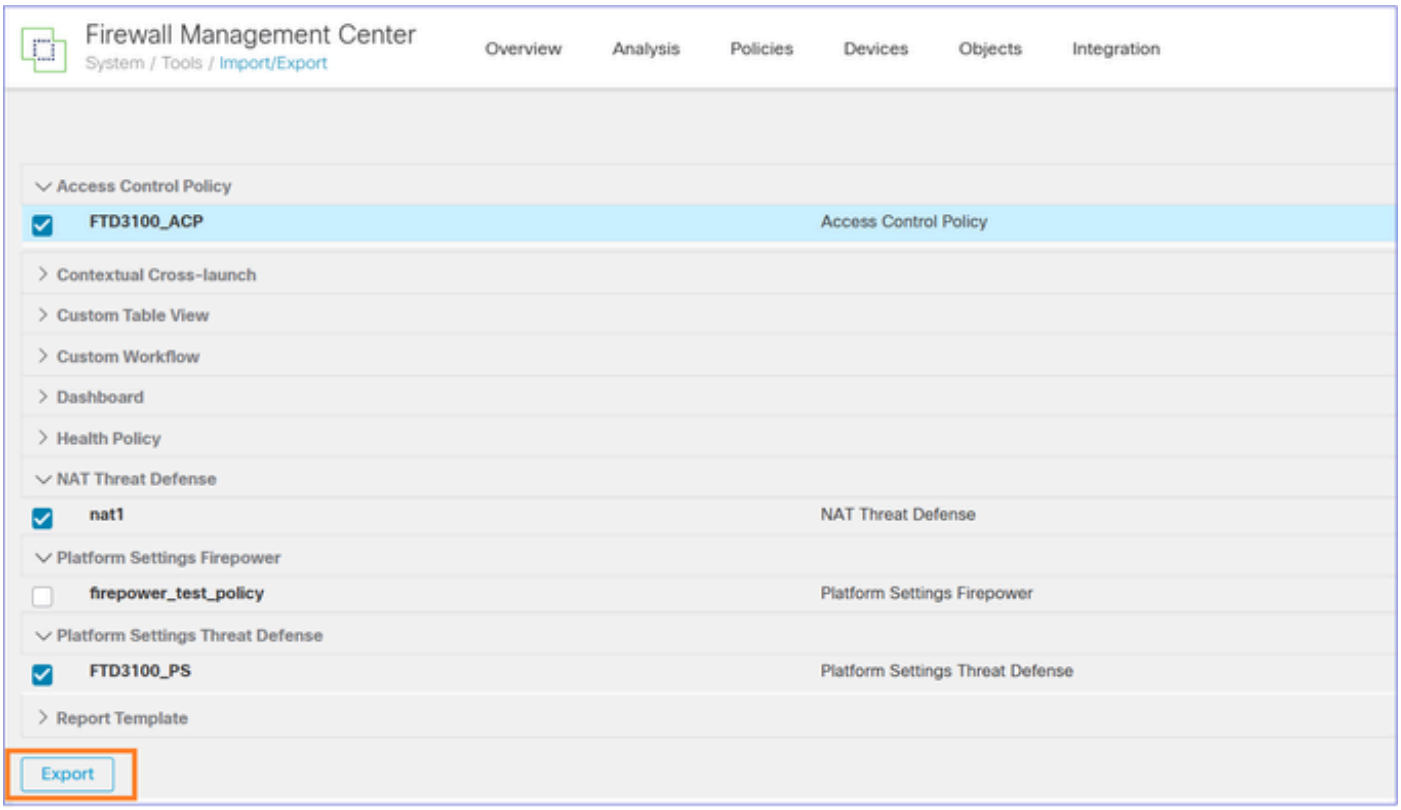
Vaya a System > Tools y seleccione Import/Export:



Exporte las distintas directivas asociadas al dispositivo. Asegúrese de exportar todas las políticas adjuntas al FTD, como:

- Política de control de acceso (ACP)
- Política de traducción de direcciones de red (NAT)
- Política de estado (si está personalizada)
- Configuración de la plataforma FTD

y más.



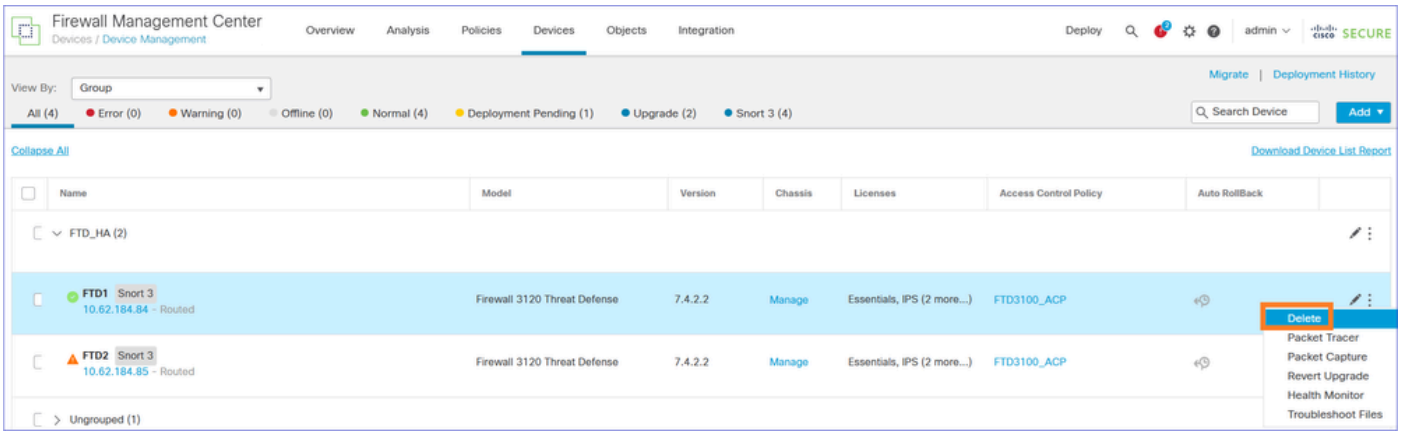
Nota: En el momento de escribir este documento, no se admite la exportación de la configuración relacionada con VPN. Debe volver a configurar manualmente la VPN en el FMC2 (FMC de destino) después del registro del dispositivo.

Mejora relacionada ID de bug de Cisco CSCwf05294

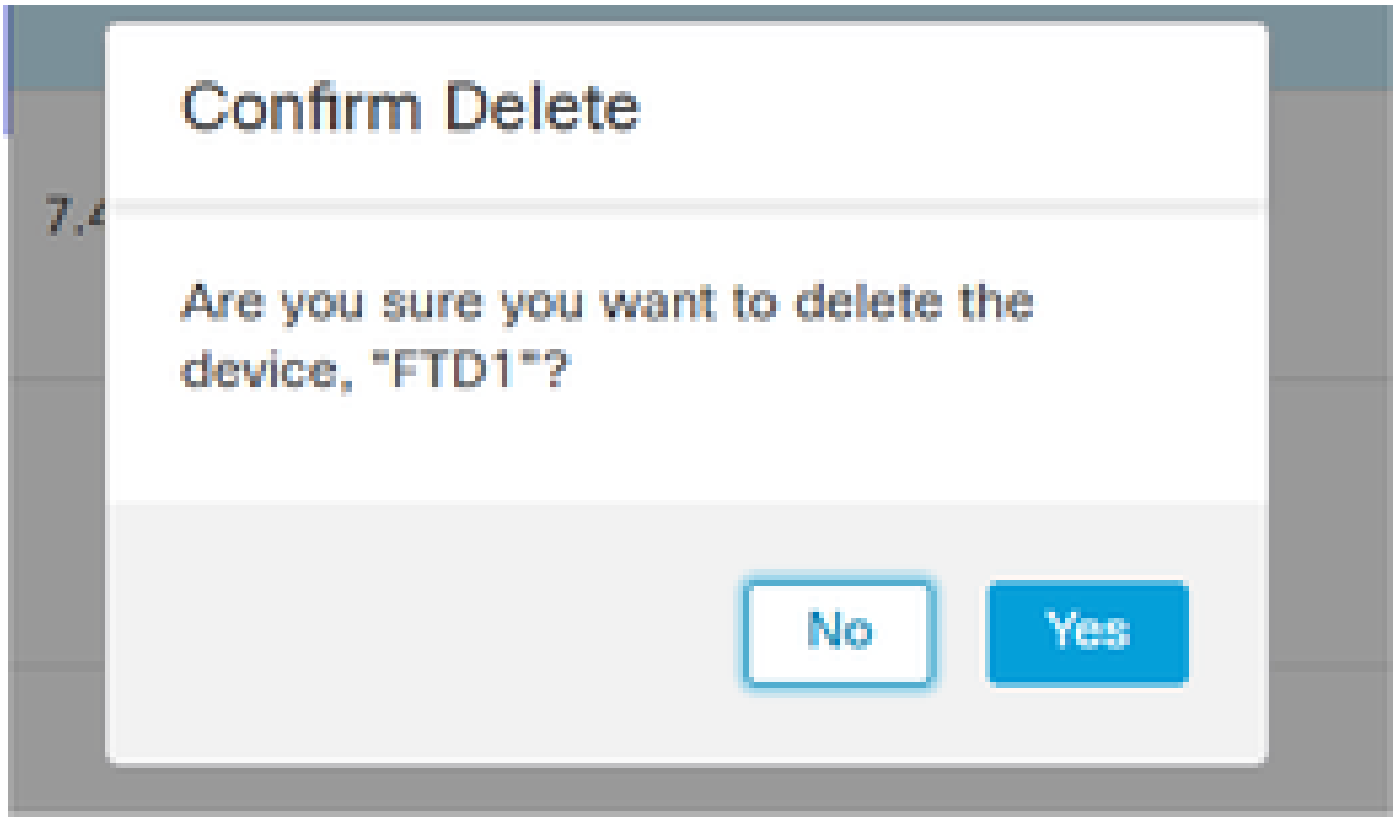
.

El resultado es un archivo .sfo; por ejemplo, ObjectExport_20250306082738.sfo

Paso 6. Eliminar/anular el registro del FTD1 (antiguo principal) del FMC antiguo/de origen



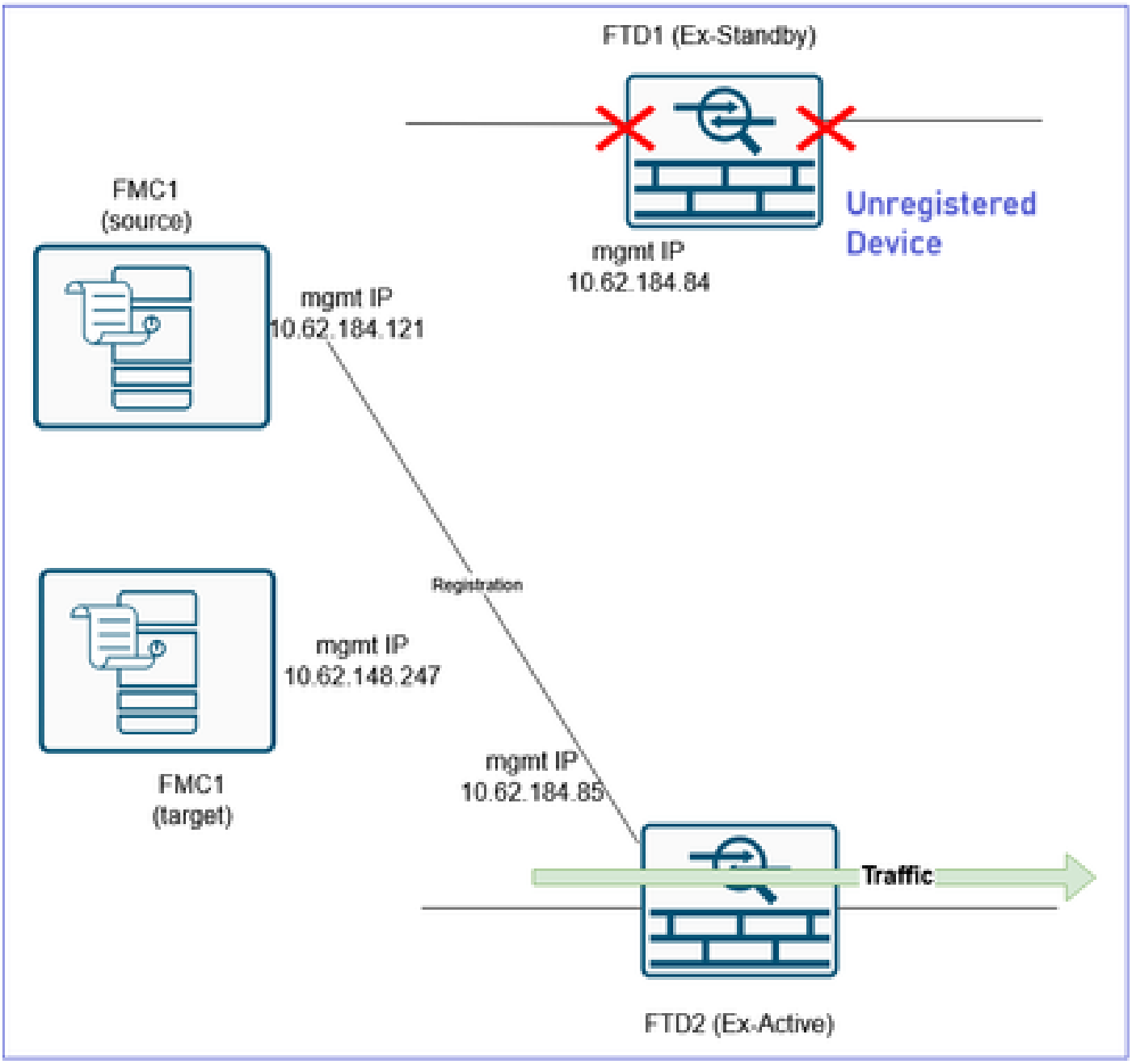
Confirme la eliminación del dispositivo:



Verificación CLI de FTD1:

```
<#root>

>

show managers

No managers configured.

>
```

Estado actual tras la eliminación del dispositivo FTD1:

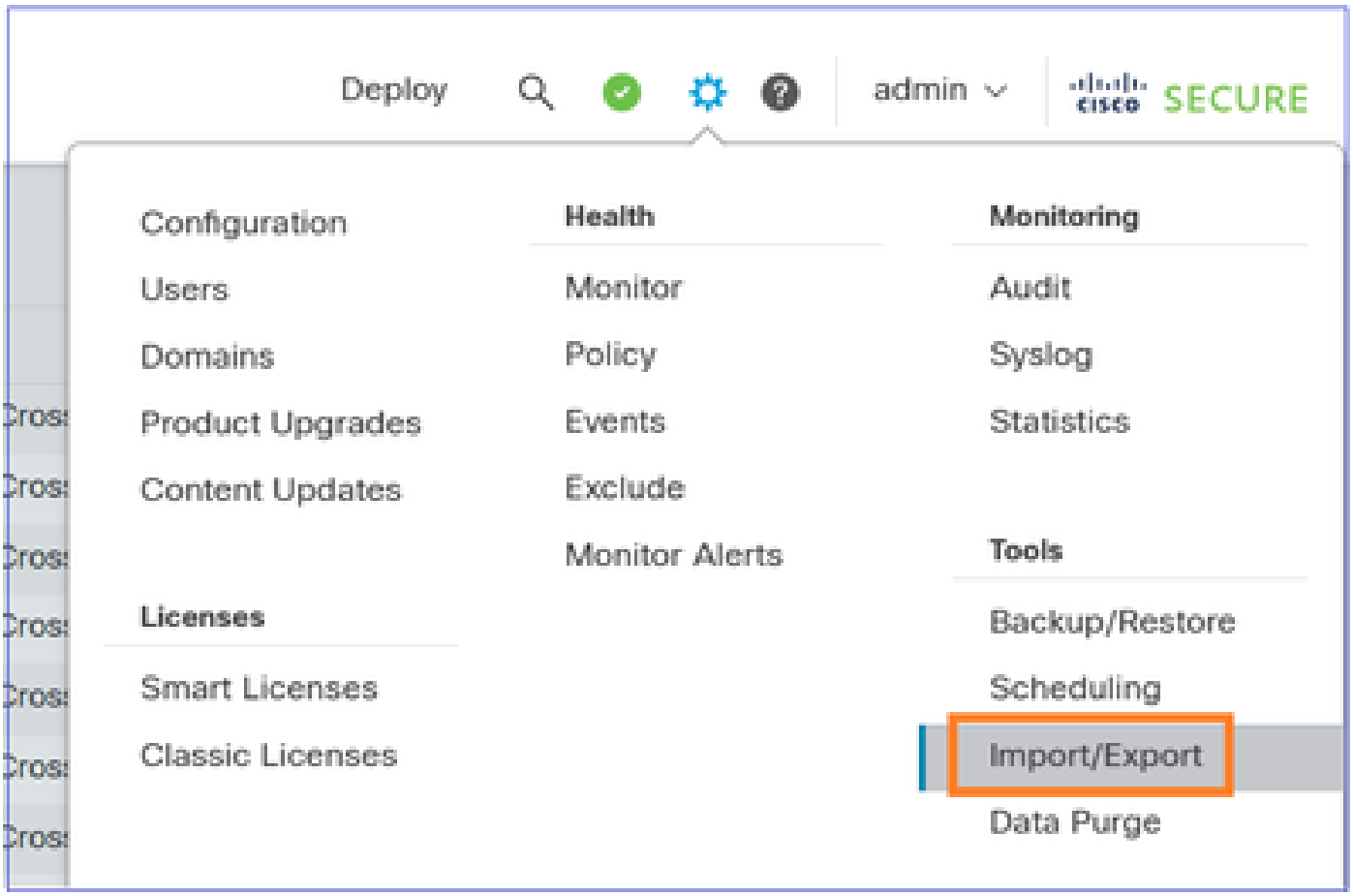


Paso 7. Importar el objeto de configuración de la política de FTD al FMC2 (FMC de destino)

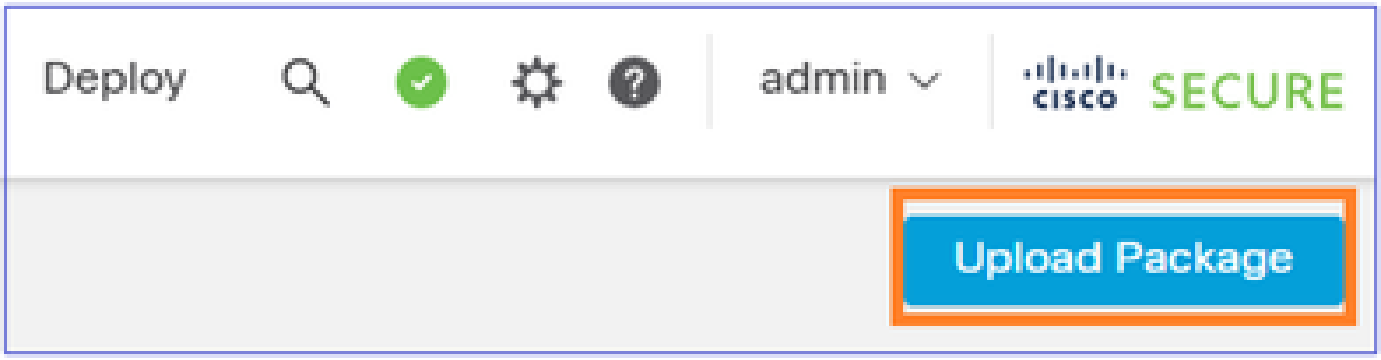
Nota: El documento se centra en la migración de un único par FTD HA a un nuevo CSP. Por otro lado, si tiene pensado migrar varios firewalls que comparten las mismas políticas (por ejemplo, ACP, NAT) y objetos y desea hacerlo por fases, debe tener en cuenta estos puntos.
- Si ya dispone de una política en el CSP de destino con el mismo nombre, se le preguntará si:
  a. ¿Desea sustituir la política o
  b. Cree uno nuevo con un nombre diferente. Esto crea objetos duplicados con nombres diferentes (sufijo _1).

- Si utiliza la opción 'b', en el paso 9 asegúrese de reasignar los objetos recién creados a las políticas migradas (zonas de seguridad ACP, zonas de seguridad NAT, enrutamiento, configuración de la plataforma, etc.).

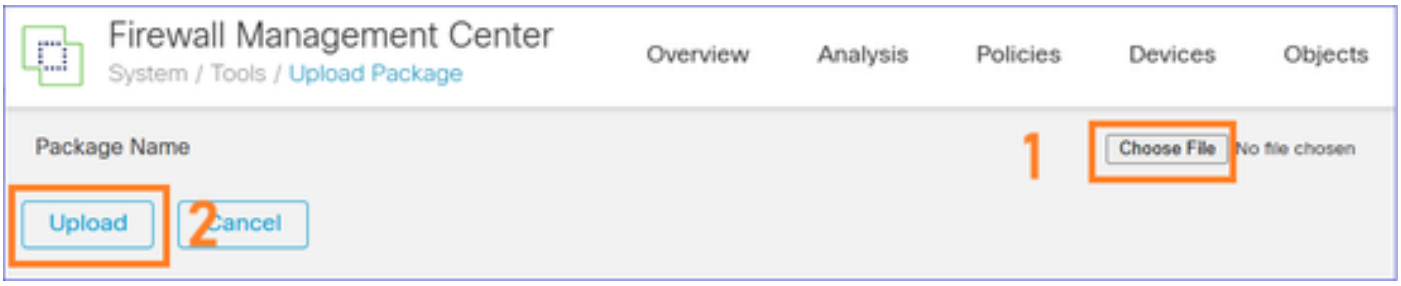
Inicie sesión en el FMC2 (FMC de destino) e importe el objeto SFO de políticas de FTD que exportó en el paso 5:



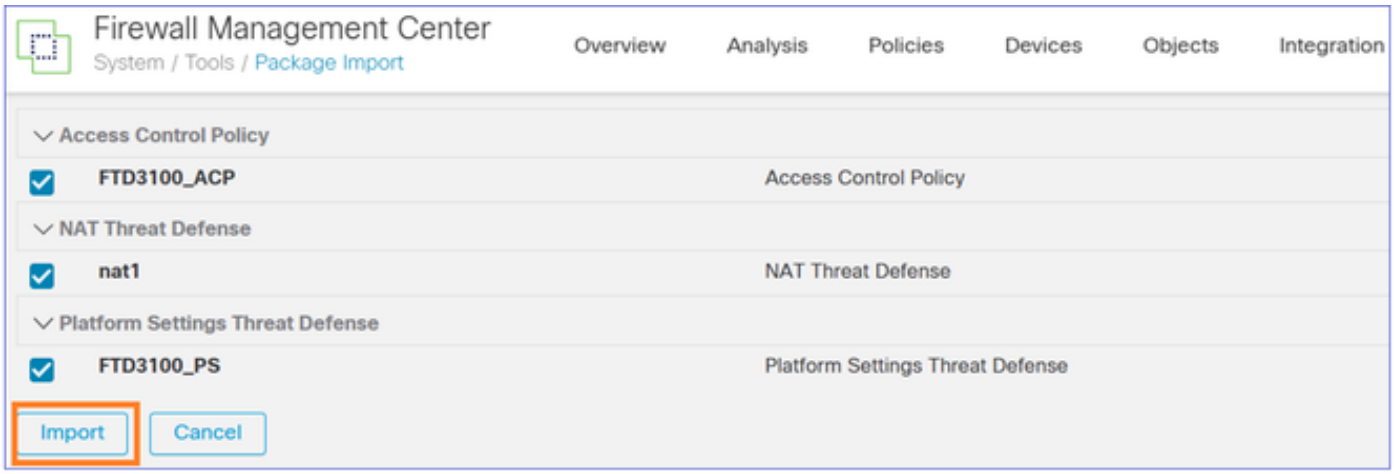
Seleccione Cargar paquete:



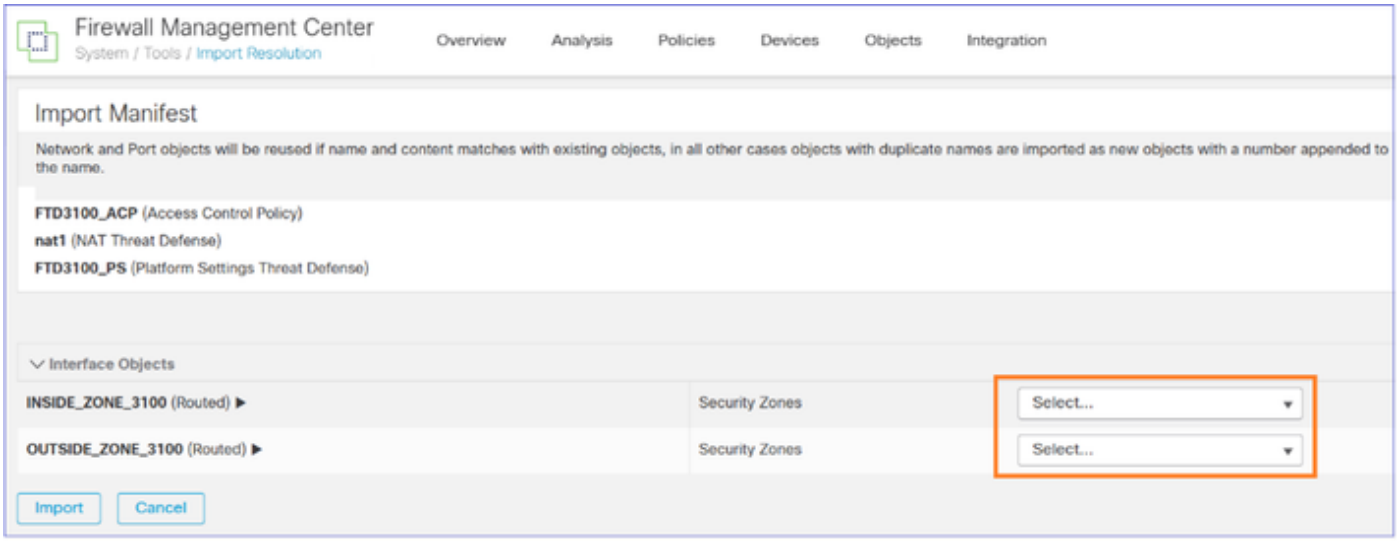
Cargue el archivo:



Importe las directivas:



Cree los objetos de interfaz/zonas de seguridad en el FMC2 (FMC de destino):



Puede dar los mismos nombres que tenían en el FMC1 (FMC de origen):

Una vez que seleccione Import (Importar), una tarea comenzará a importar las directivas relacionadas en el FMC2 (FMC de destino):

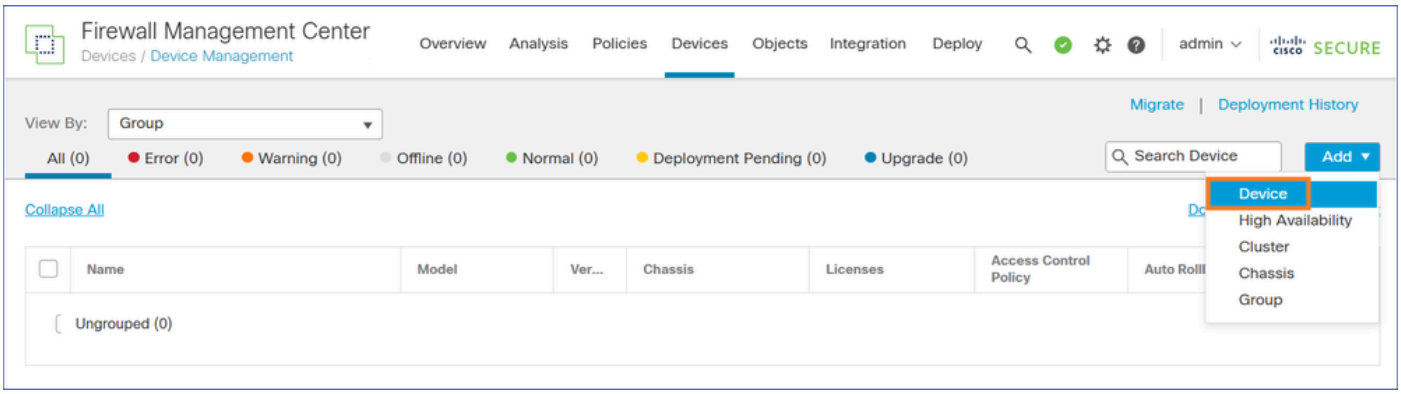
La tarea ha finalizado:

Paso 8. Registro del FTD1 (antiguo primario) en el FMC2

Vaya a la CLI de FTD1 (anterior principal) y configure el nuevo administrador:

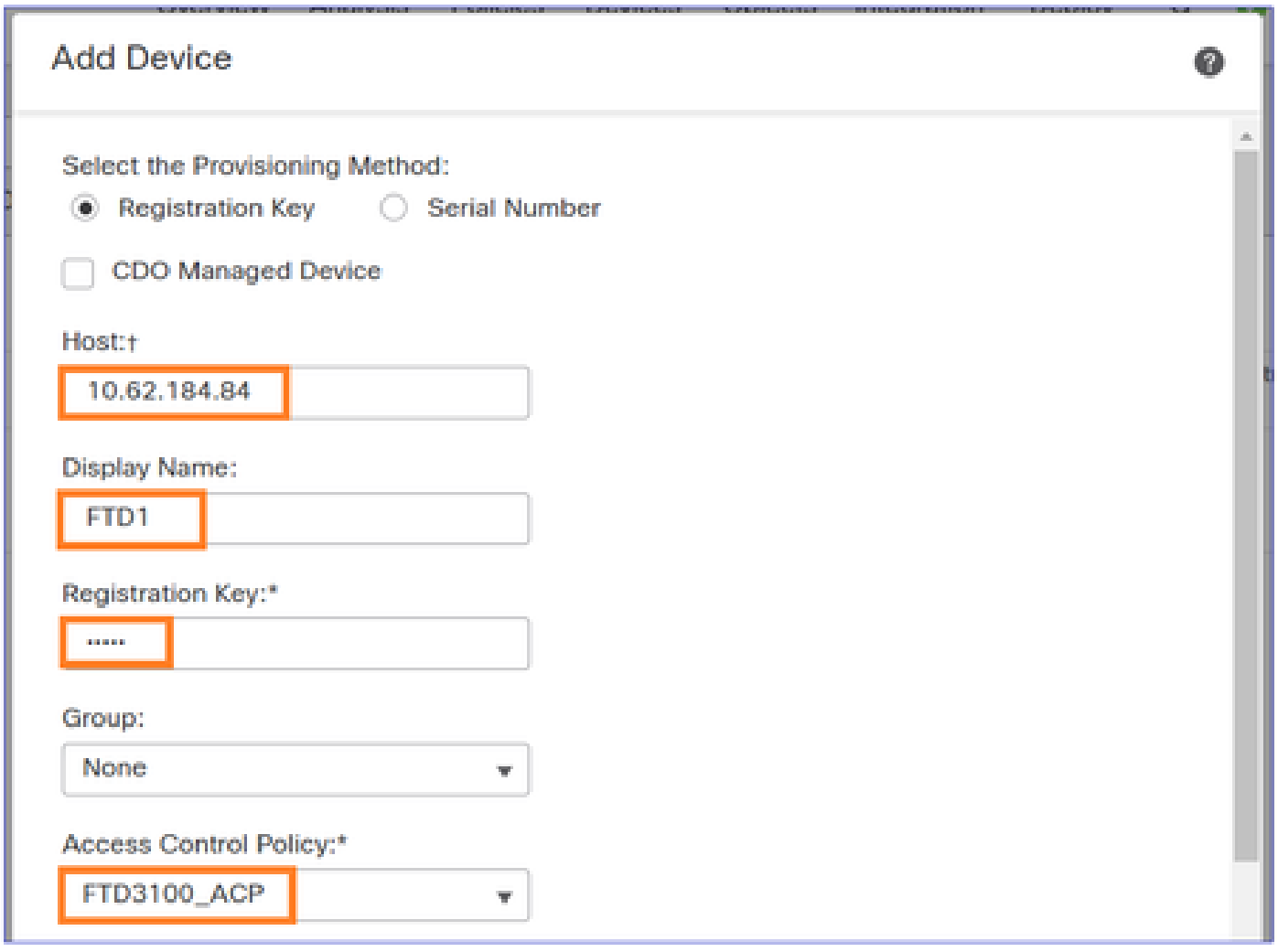
```
<#root>

>

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.

>
```

Vaya a FMC2 (FMC de destino) UI Devices > Device Management y Add the FTD device:

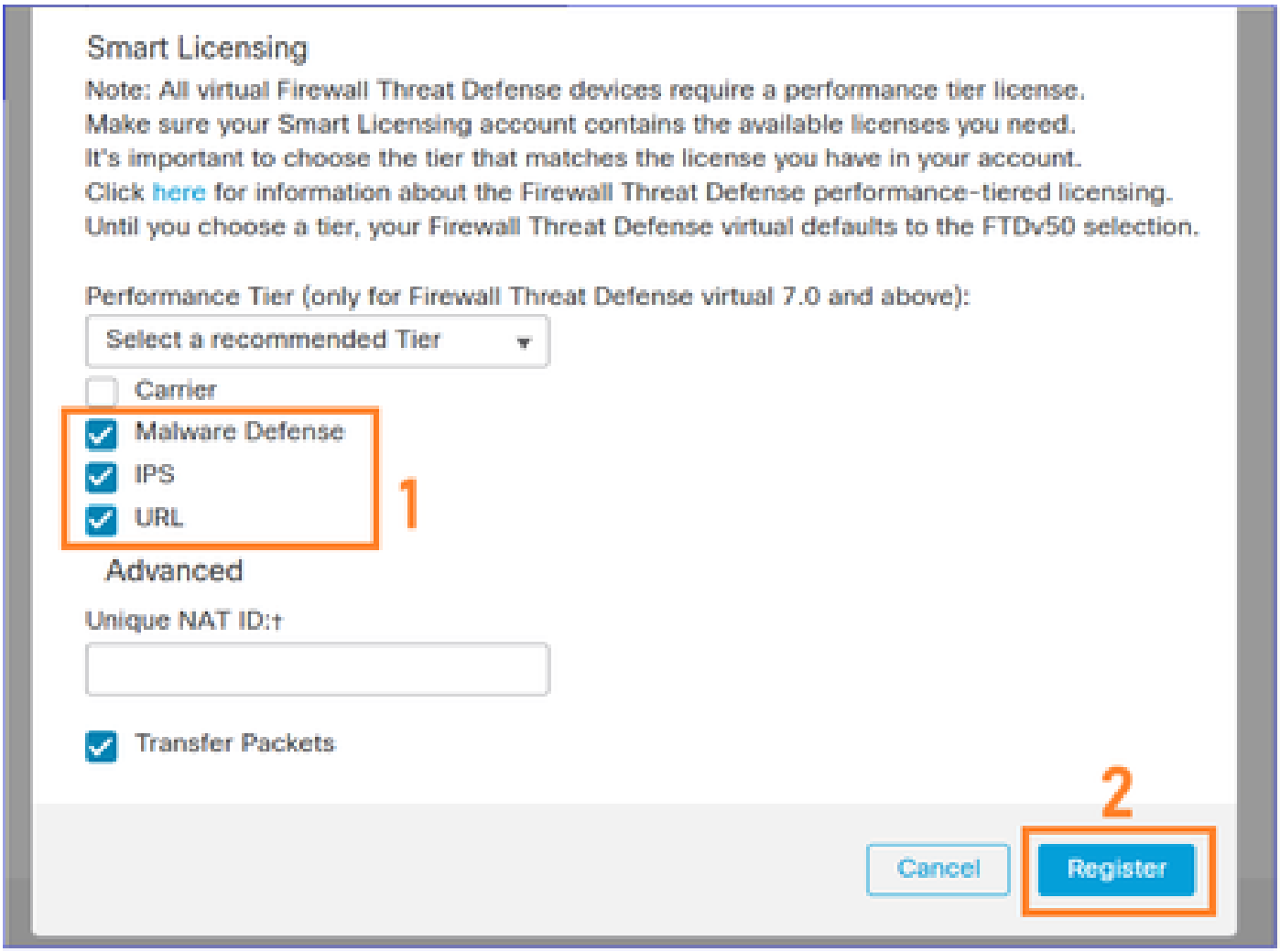


Si el registro del dispositivo falla, consulte este documento para resolver el problema: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

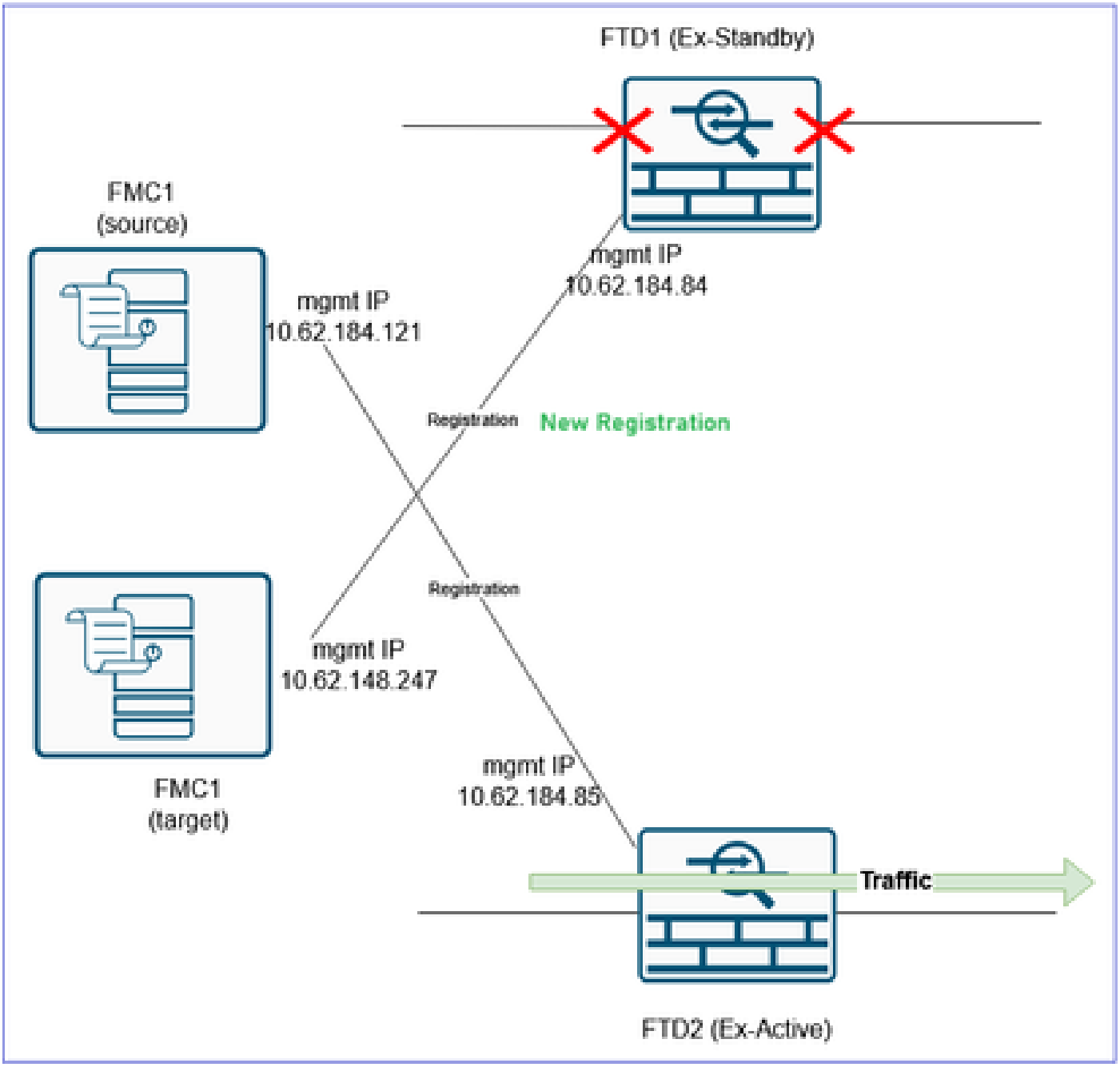
Asigne la política de control de acceso que importó en el paso anterior:



Aplique las licencias necesarias y registre el dispositivo:



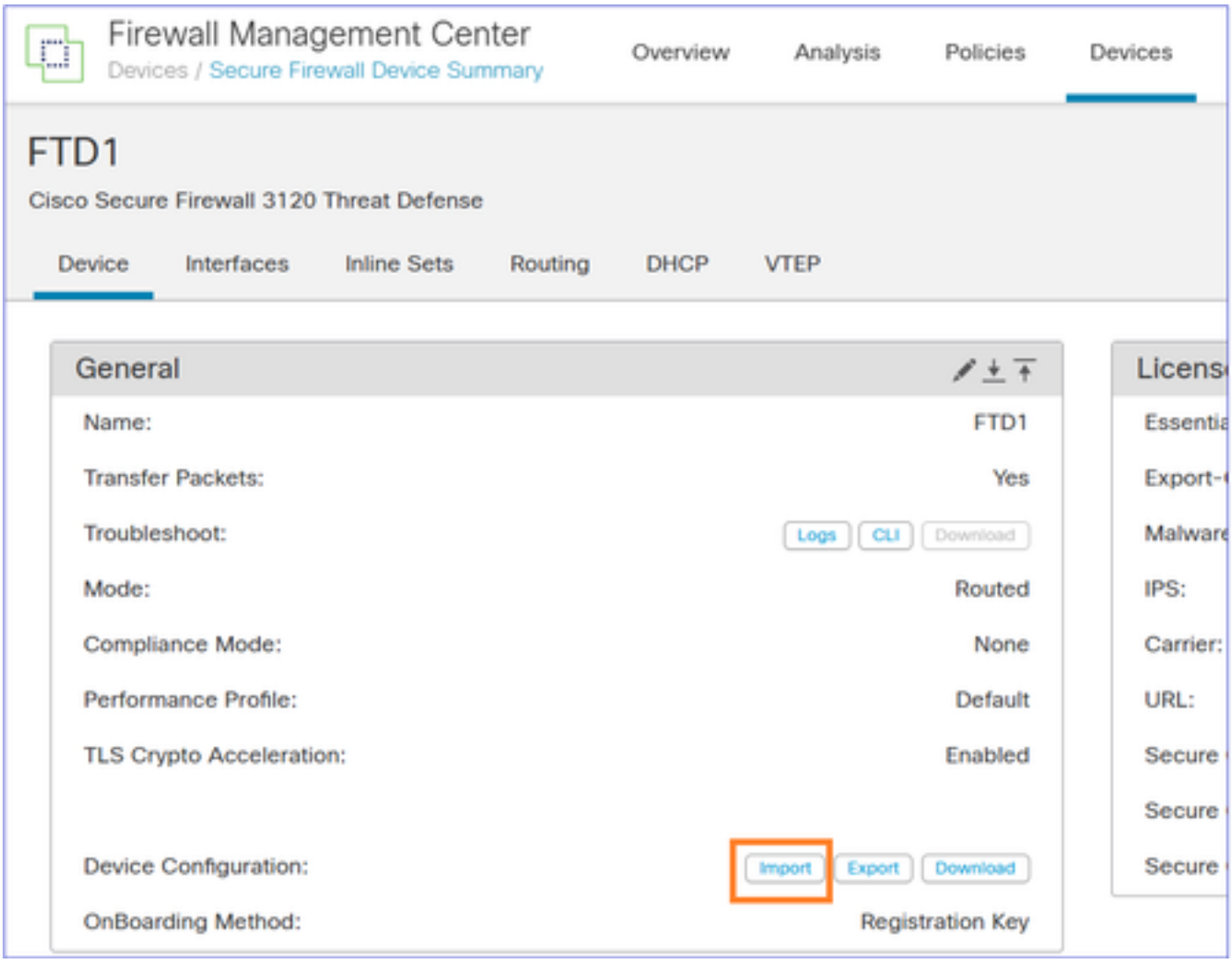
El resultado:



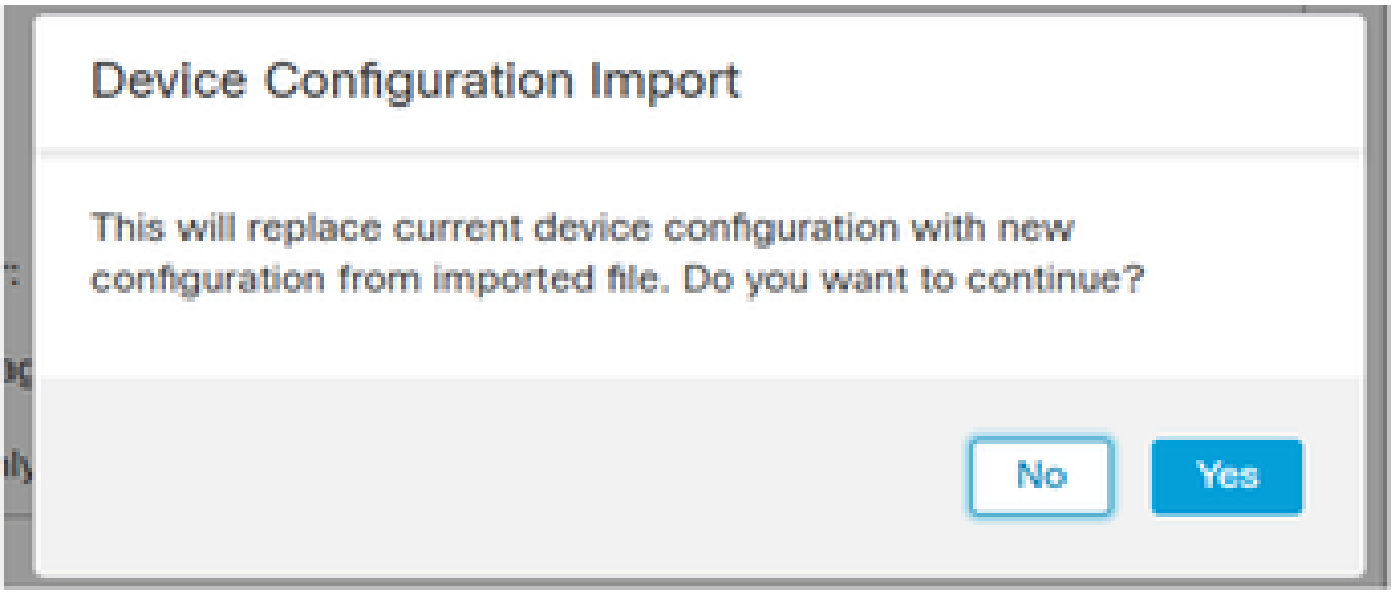
Paso 9. Importar el objeto de configuración del dispositivo FTD en el FMC2 (FMC de destino)

Inicie sesión en el FMC2 (FMC de destino), navegue hasta Devices > Device Management y Edit el dispositivo FTD que registró en el paso anterior.

Vaya a la pestaña Device e Import el objeto de información de políticas de FTD que exportó en el paso 2:

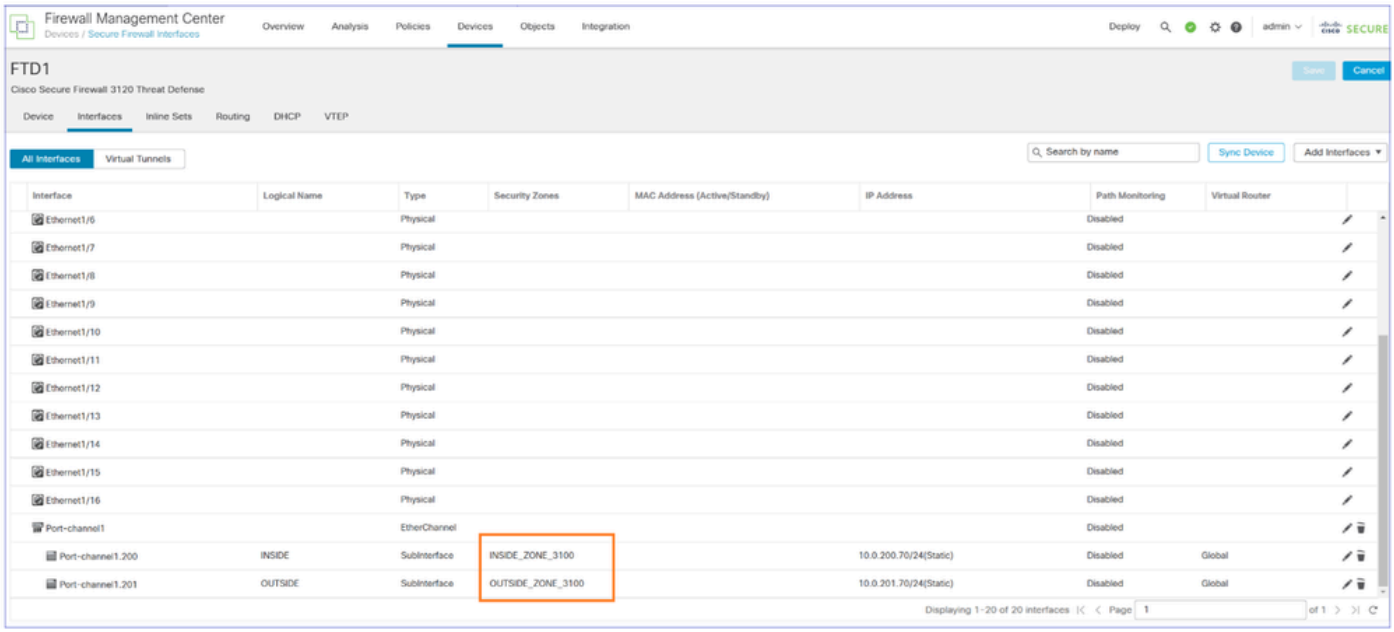


Nota: En el caso del paso 7 que utilizó la opción 'b' (Crear una nueva política), asegúrese de reasignar los objetos recién creados a las políticas migradas (zonas de seguridad ACP, zonas de seguridad NAT, enrutamiento, configuración de la plataforma, etc.).



Se inicia una tarea de CSP.

La configuración del dispositivo se aplica en el FTD1, por ejemplo, zonas de seguridad, ACP, NAT, etc.:



⚠ Precaución: Si tiene un ACP que se expande a muchos elementos de control de acceso, el proceso de compilación de ACP (compilación de coincidencia) puede tardar varios minutos en completarse. Puede utilizar este comando para verificar el estado de compilación de ACP:

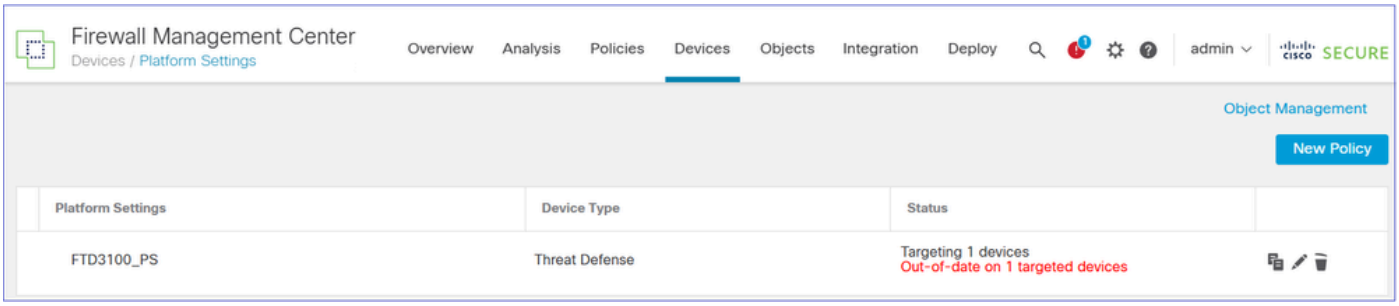
```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

Paso 10. Finalización de la configuración de FTD

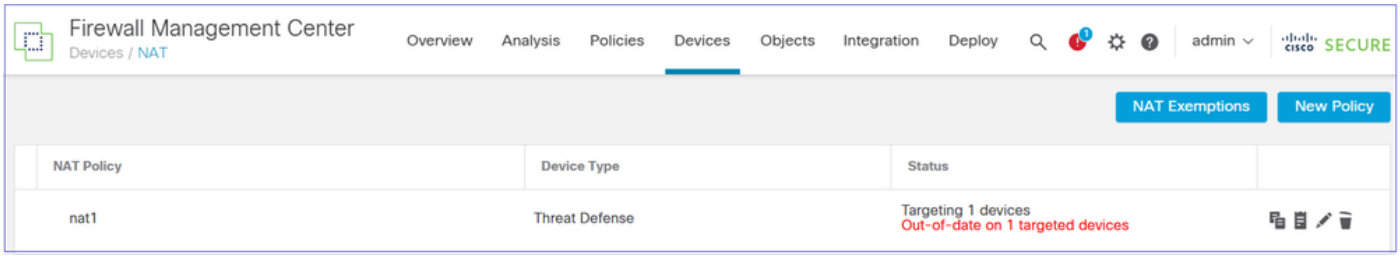
En este punto, el objetivo es configurar todas las funciones que pueden faltar en el FTD1 después del registro en el FMC2 (FMC objetivo) y la importación de la política de dispositivos.

Asegúrese de que las políticas como NAT, configuración de la plataforma, QoS, etc. están asignados al FTD. Verá que las directivas están asignadas pero pendientes de implementación.

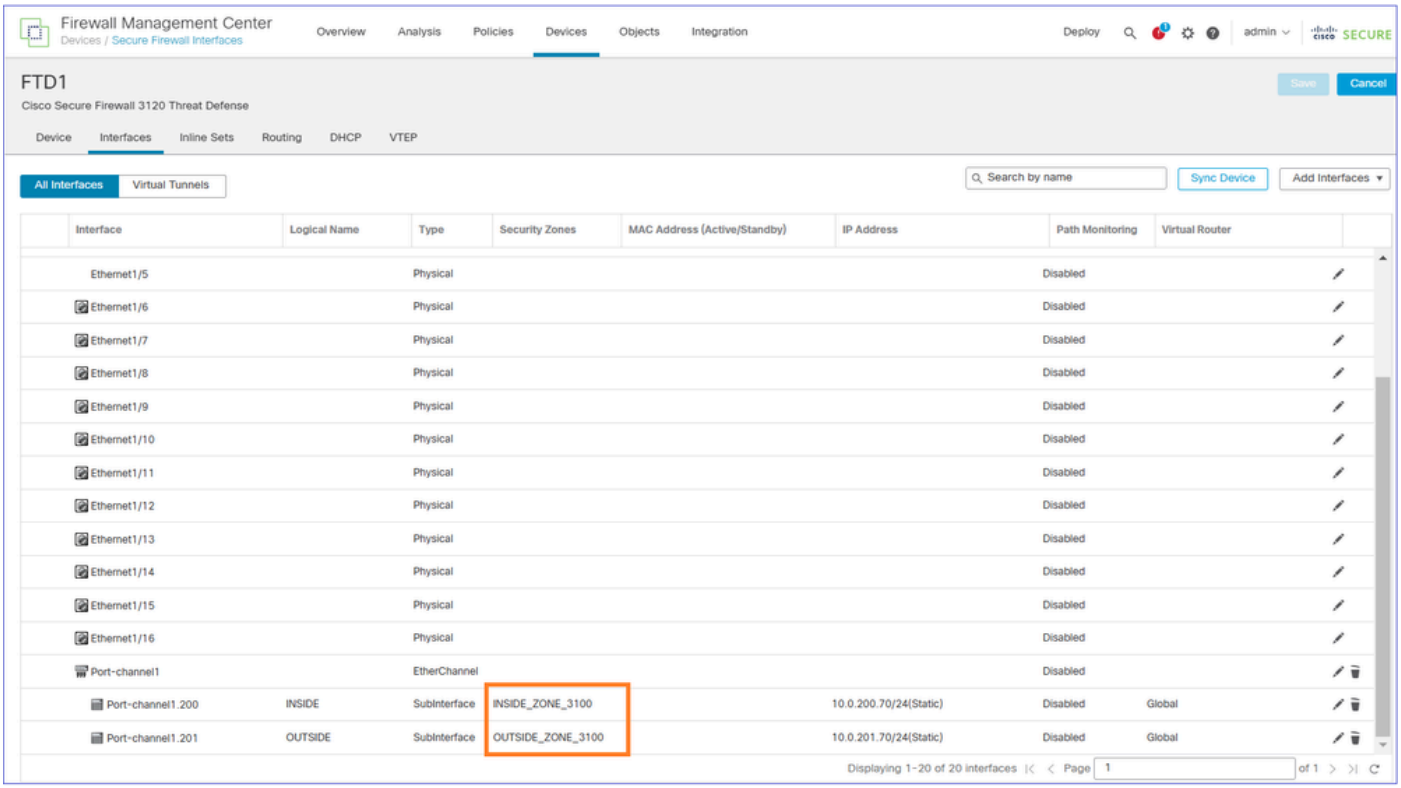
Por ejemplo, la configuración de la plataforma se importa y se asigna al dispositivo, pero a la espera de la implementación:



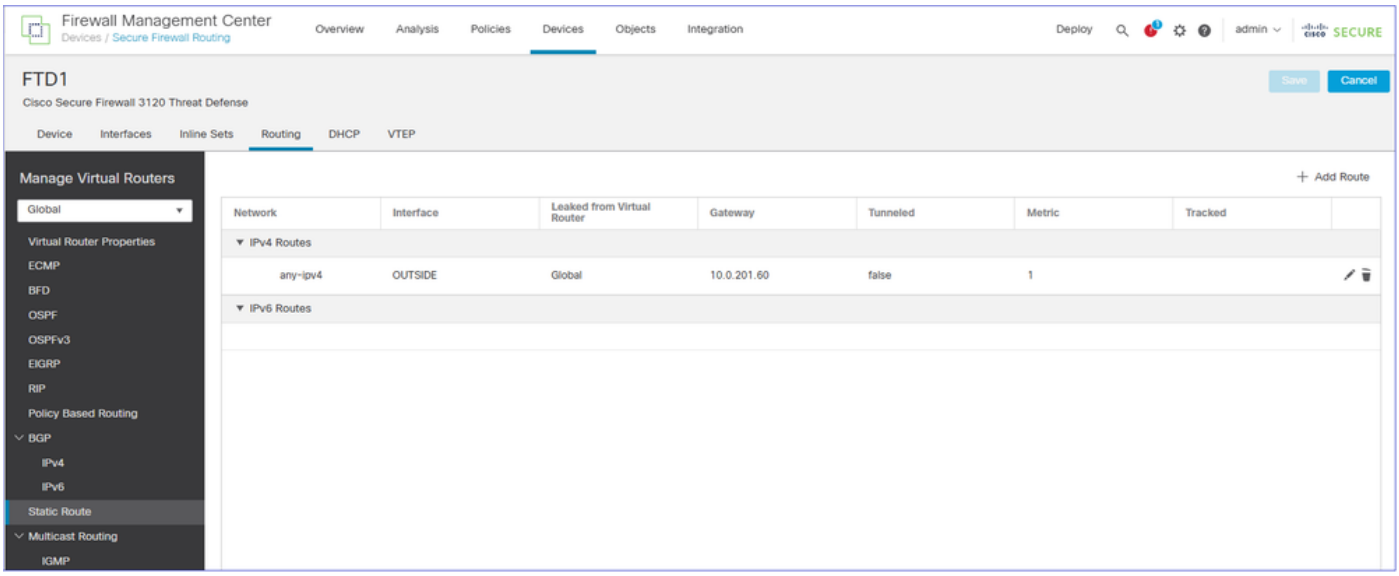
Si se configura NAT, la política NAT se importa y se asigna al dispositivo, pero está pendiente de la implementación:



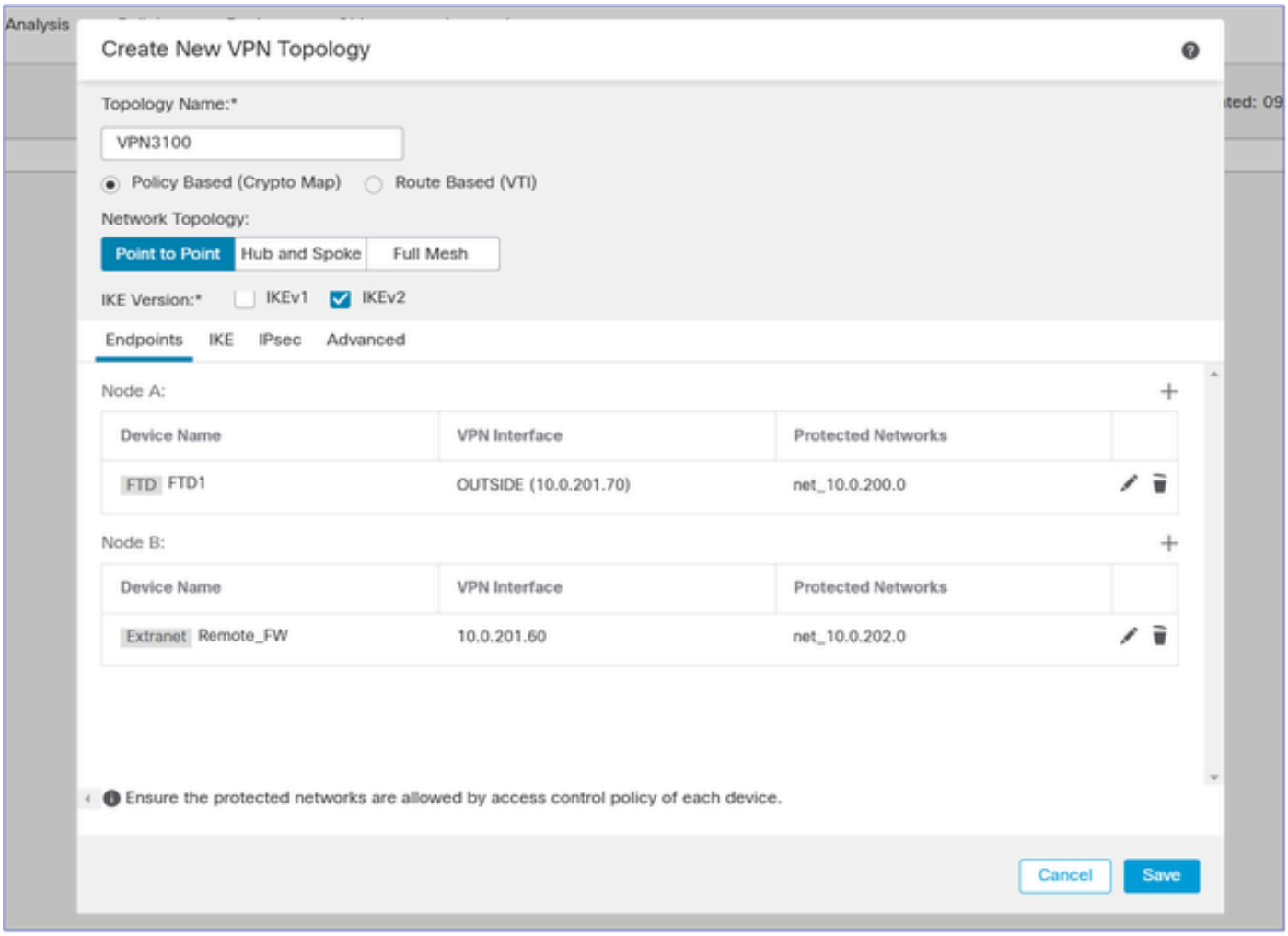
Las zonas de seguridad se aplican a las interfaces:



La configuración de ruteo se aplica al dispositivo FTD:



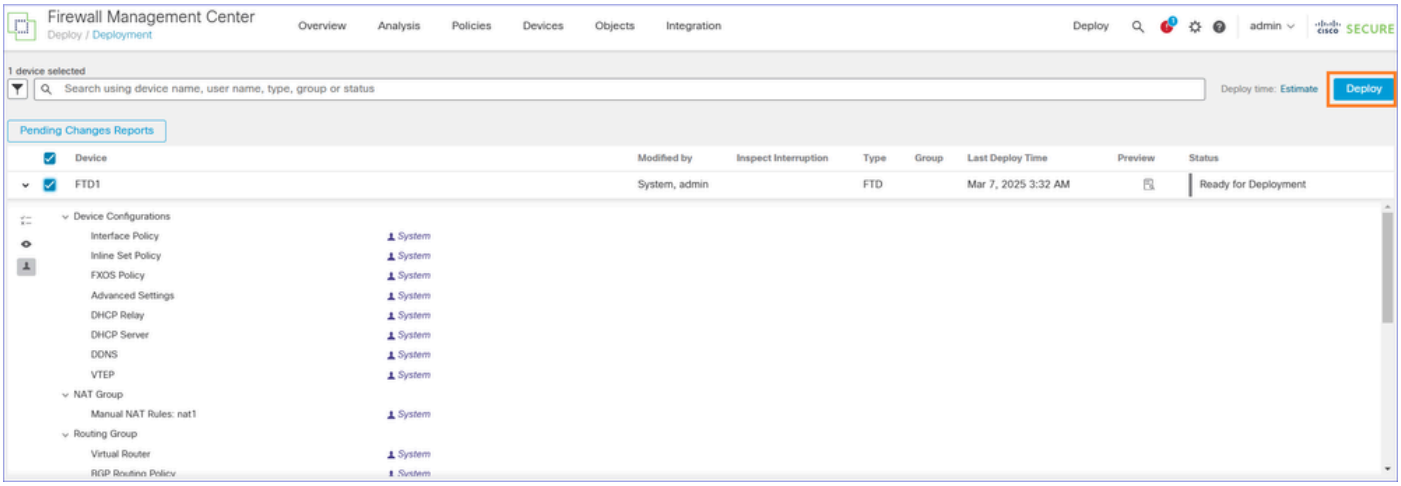
Nota: Ha llegado el momento de configurar las directivas que no se han podido migrar automáticamente (por ejemplo, VPN).



Nota: Si el FTD que se migra tiene pares VPN S2S que también se migran al FMC de

destino, debe configurar la VPN después de mover todos los FTD al FMC de destino.

Implementar los cambios pendientes:



Paso 11. Verificar la configuración de FTD implementada

En este momento, el objetivo es comprobar desde la CLI de FTD que toda la configuración está en su lugar.

La sugerencia es comparar el resultado de 'show running-config' de ambos FTD. Puede utilizar herramientas como WinMerge o diff para la comparación.

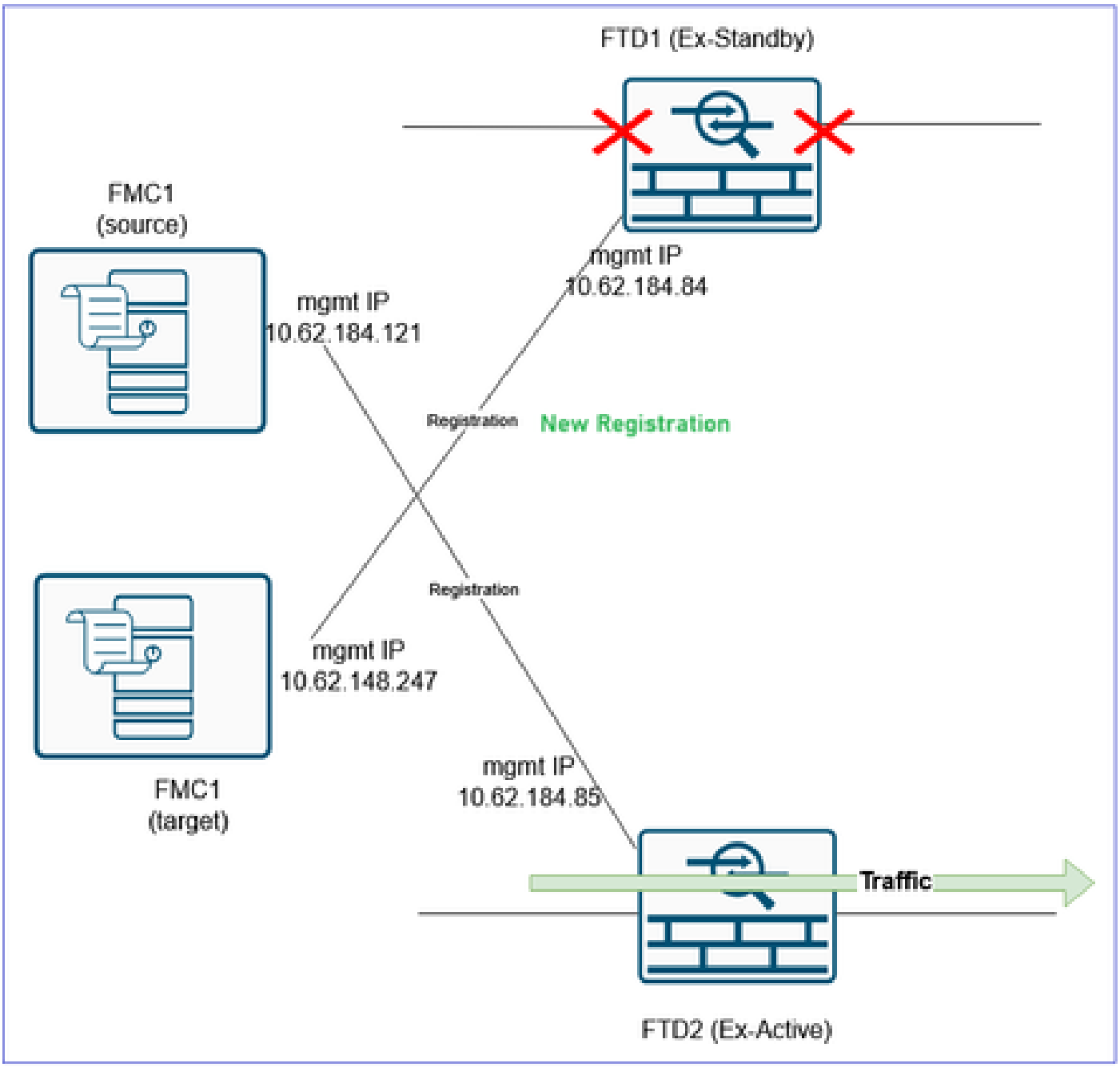
Las diferencias que ve y son normales son:

- Número de serie del dispositivo
- Descripciones de interfaz
- ACL rule-ids
- Configuración de Cryptochecksum

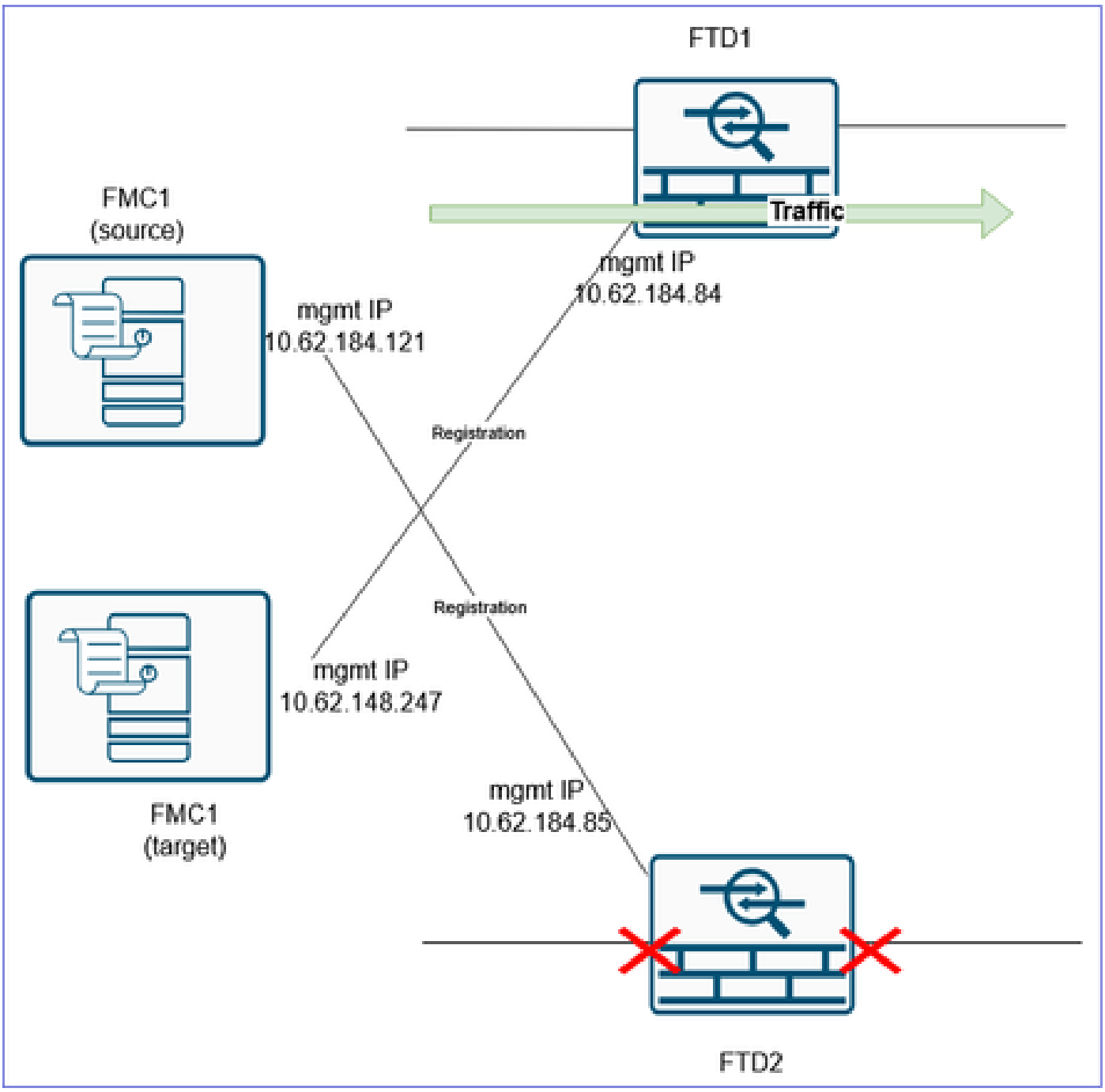
Paso 12. Realice la transición

En este paso, el objetivo es cambiar el tráfico del FTD2 que gestiona actualmente el tráfico y que sigue registrado en el FMC antiguo/de origen al FTD1 registrado en el 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)

Después de:



⚠ Precaución: Arregle un MW para hacer la transición. Durante la transición, se producirá una interrupción del tráfico hasta que todo el tráfico se desvíe al FTD1, se restablezcan las VPN, etc.

⚠ Precaución: No inicie la transición a menos que se complete la compilación ACP (véase el paso 10 anterior).

⚠ Advertencia: Asegúrese de desconectar los cables de datos del FTD2 o apagar los puertos de switch relacionados. De lo contrario, ¡puede terminar con ambos dispositivos manejando el tráfico!

⚠ Precaución: Dado que ambos dispositivos utilizan la misma configuración IP, es necesario actualizar la memoria caché ARP de los dispositivos L3 adyacentes. Considere la posibilidad de borrar manualmente la memoria caché ARP de los dispositivos adyacentes para acelerar la transición del tráfico.

Consejo: También puede enviar un paquete GARP y actualizar la memoria caché ARP de los dispositivos adyacentes mediante el comando FTD CLI:

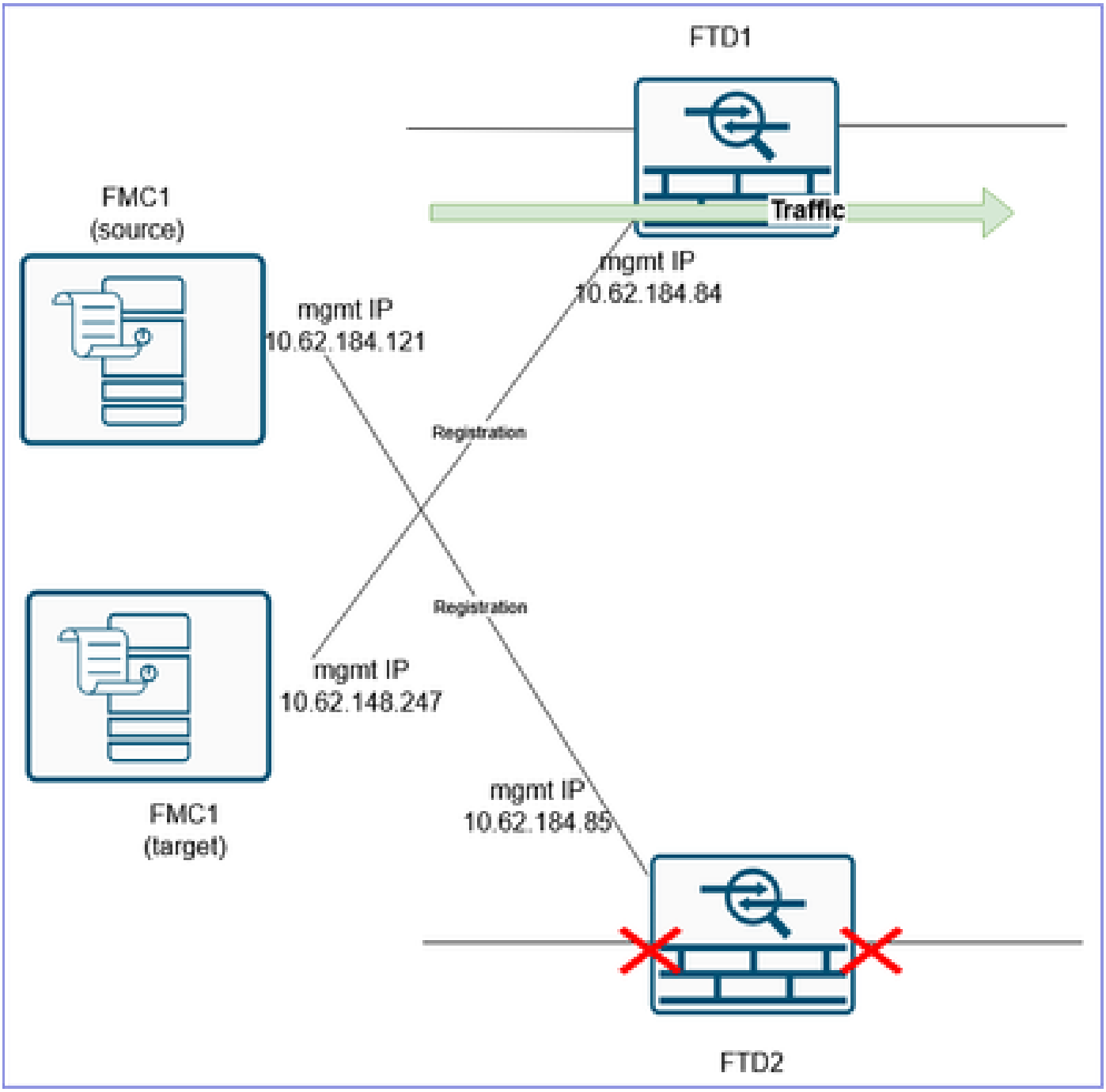
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

Tiene que repetir este comando para cada IP que posee el FW. Por lo tanto, puede ser más rápido simplemente borrar la memoria caché ARP de los dispositivos adyacentes que enviar paquetes GARP para cada IP que posee el firewall.

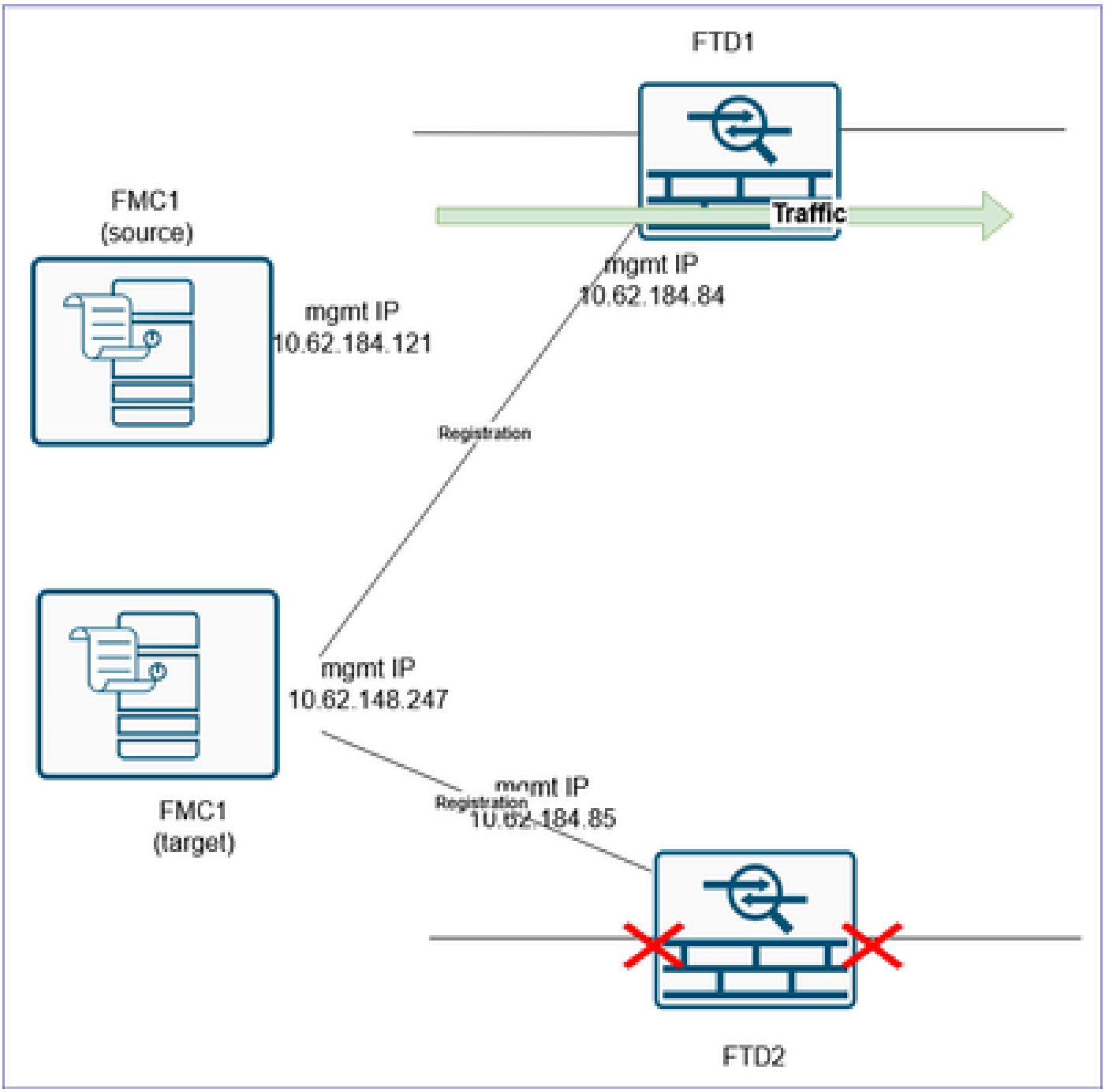
Paso 13. Migrar el segundo FTD al FMC2 (FMC objetivo)

El último punto es reformar el par HA. Para ello, primero debe eliminar el FTD2 del FMC1 (FMC de origen) y registrarlo en el FMC2 (FMC de destino).

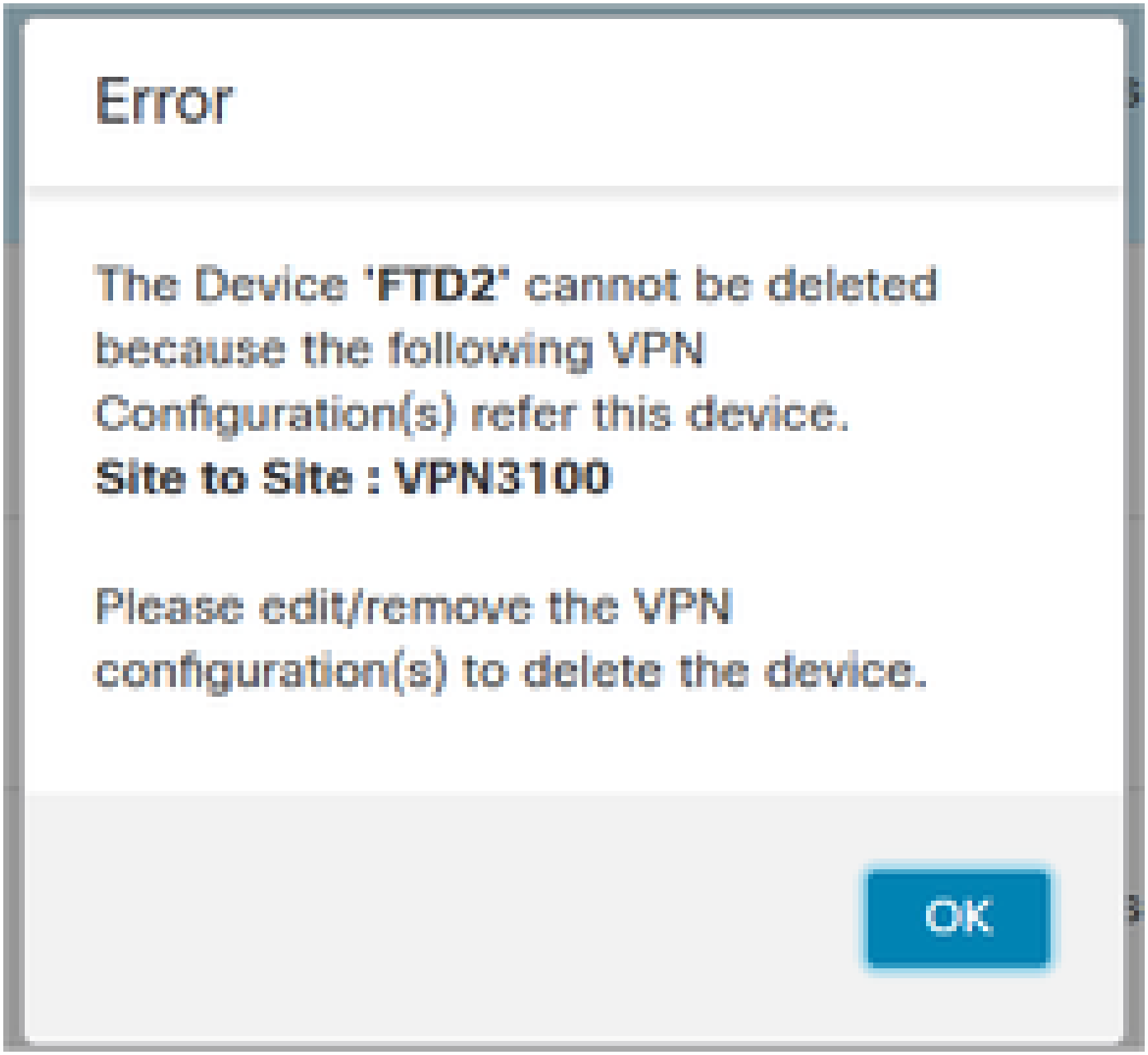
Antes:


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

Después de:



Si tiene una configuración VPN conectada al FTD2, primero debe eliminarla antes de eliminar el FTD. En otro caso, se muestra un mensaje similar a este:



Verificación de CLI:

<#root>

>

show managers

No managers configured.

Se recomienda borrar toda la configuración del FTD antes de registrarla en el FMC de destino. Una forma rápida de hacerlo es cambiar entre los modos de firewall.

Por ejemplo, si tiene el modo ruteado, cambie a transparente y luego a ruteado:

<#root>

>

configure firewall transparent

Y luego:

<#root>

>

configure firewall routed

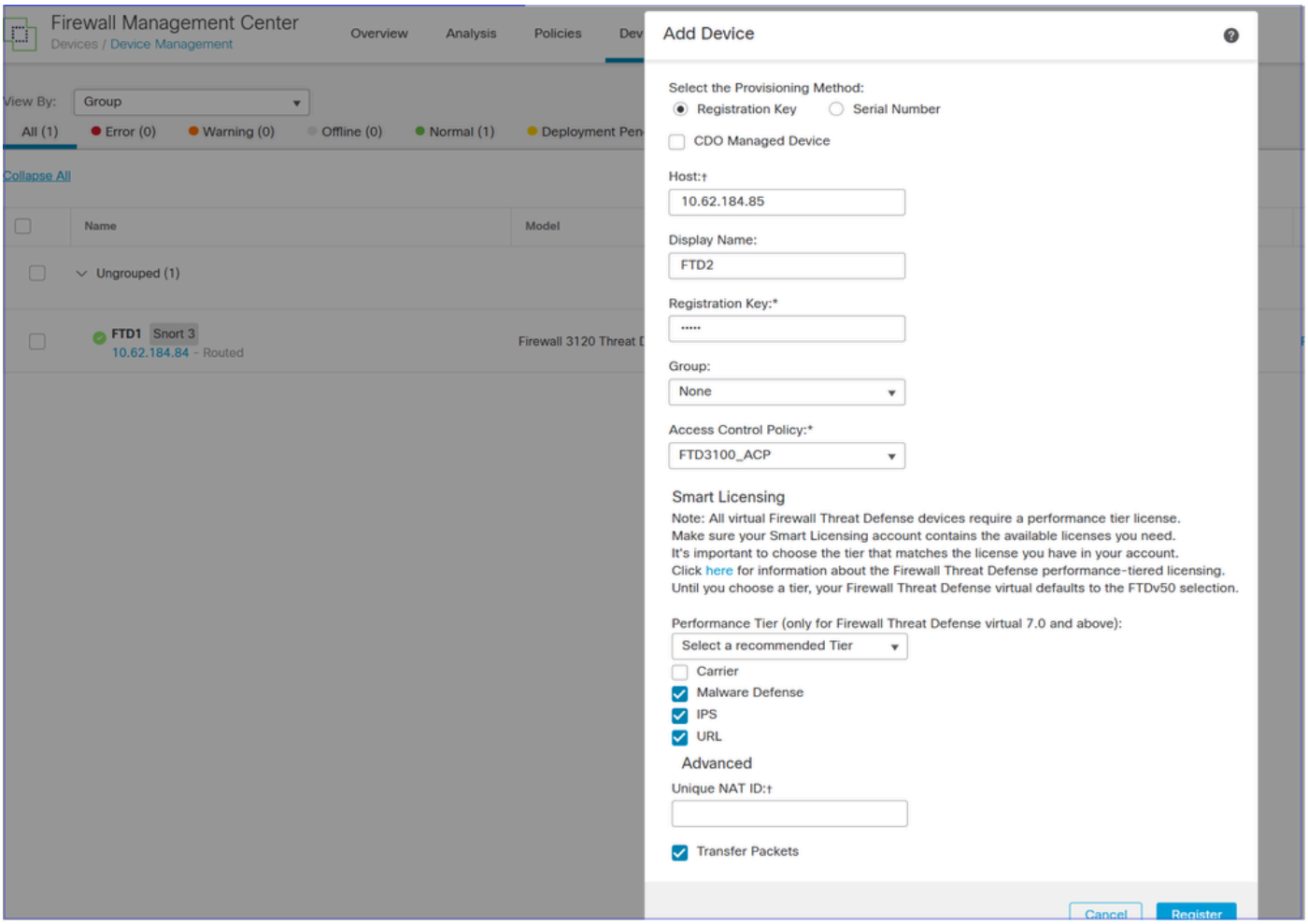
A continuación, regístrelo en el CSP2 (CSP objetivo):

<#root>

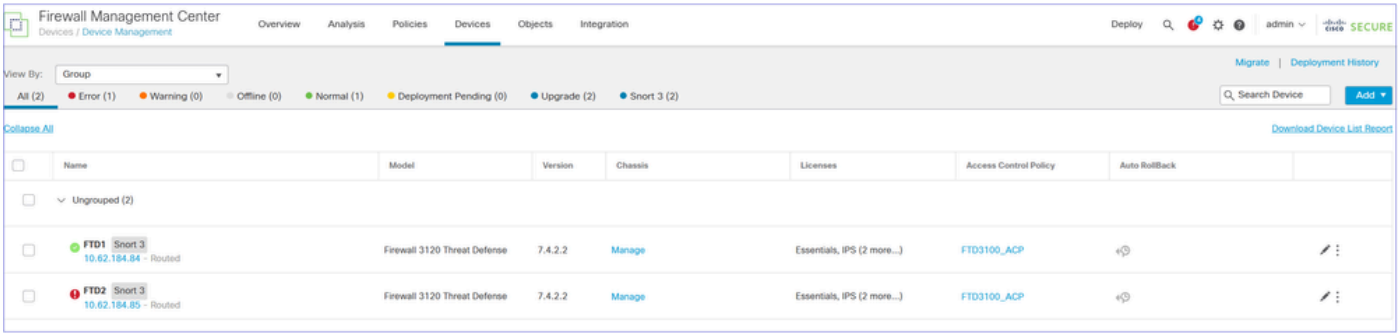
>

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.
>
```



El resultado:

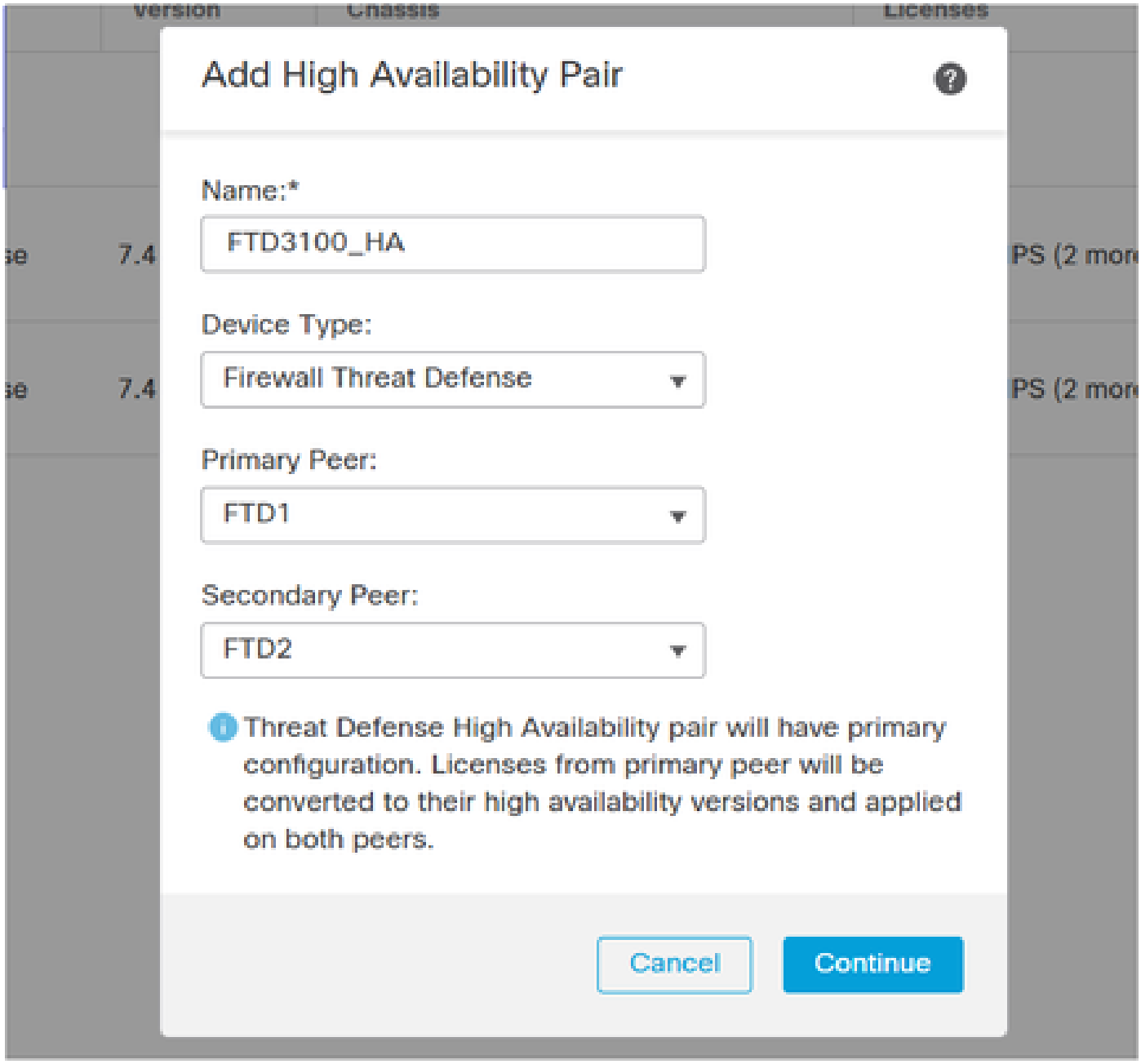


Paso 14. Reforma del FTD HA

Nota: Esta tarea (como cualquier tarea relacionada con HA) también debe realizarse durante un MW. Durante la negociación de HA, va a haber una interrupción del tráfico durante aproximadamente 1 minuto desde que las interfaces de datos se desactivan.

En el FMC de destino, navegue hasta Devices > Device Management y Add > High Availability.

⚠ Precaución: Asegúrese de seleccionar como peer primario el FTD que está manejando el tráfico (FTD1 en este escenario):



Vuelva a configurar los parámetros de HA, incluidas las interfaces supervisadas, las IP en espera, las direcciones MAC virtuales, etc.

Verificación desde FTD1 CLI:

```
<#root>

FTD3100-3#

show failover | include host

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

Verificación desde FTD2 CLI:

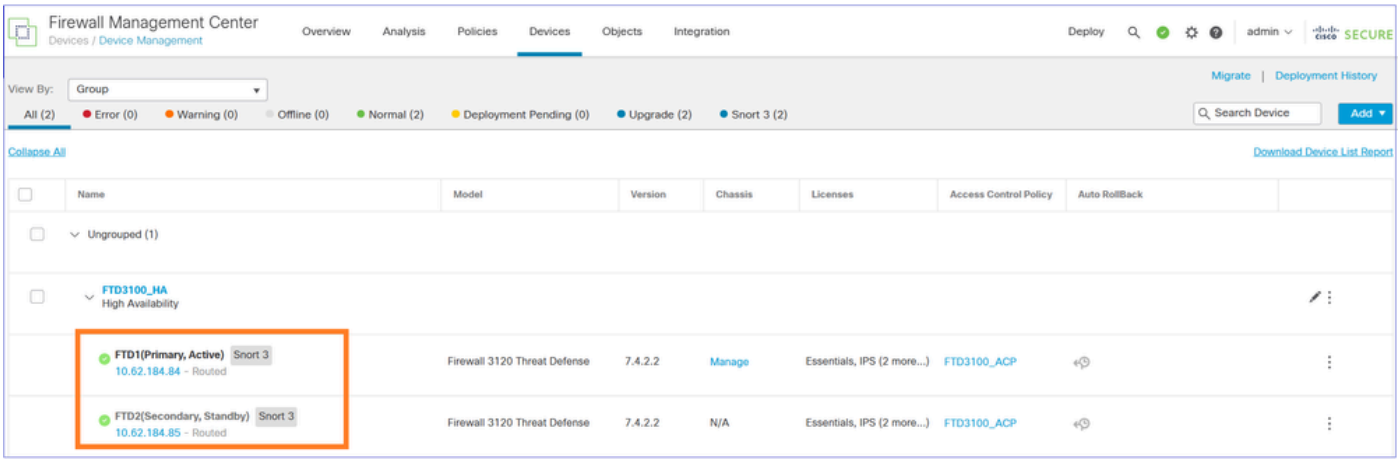
<#root>

FTD3100-3#

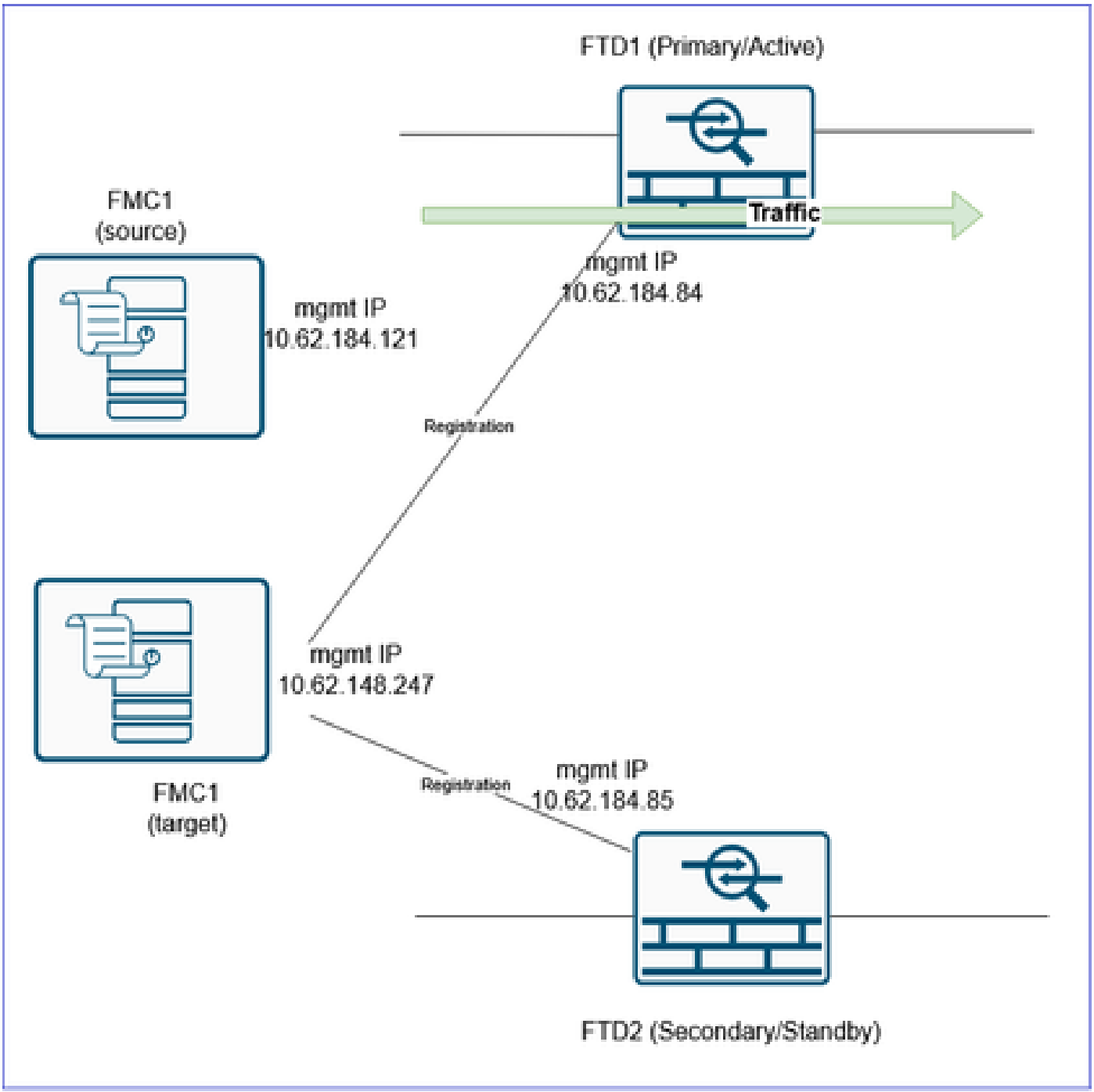
show failover | include host

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

Verificación de IU de FMC:



Por último, active o vuelva a conectar las interfaces de datos del dispositivo FTD2.



Referencias

- Exportar e importar la configuración del dispositivo
- Agregar un par de alta disponibilidad
- Migración de un FTD de un FMC a otro FMC

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).