Sustitución de la unidad defectuosa en Firewall seguro Defensa frente a amenazas de alta disponibilidad

Contenido

Introducción

En este documento se describe cómo sustituir un módulo de Secure Firewall Threat Defence defectuoso que forme parte de una configuración de alta disponibilidad (HA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)
- Sistema operativo extensible (FXOS) Cisco Firepower
- Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

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

- Firepower 4110 ejecuta FXOS v2.12(0.498)
- El dispositivo lógico ejecuta Cisco Secure Firewall v7.2.5
- Secure Firewall Management Center 2600 ejecuta la versión 7.4
- Conocimiento del protocolo de copia segura (SCP)

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.

Antecedentes

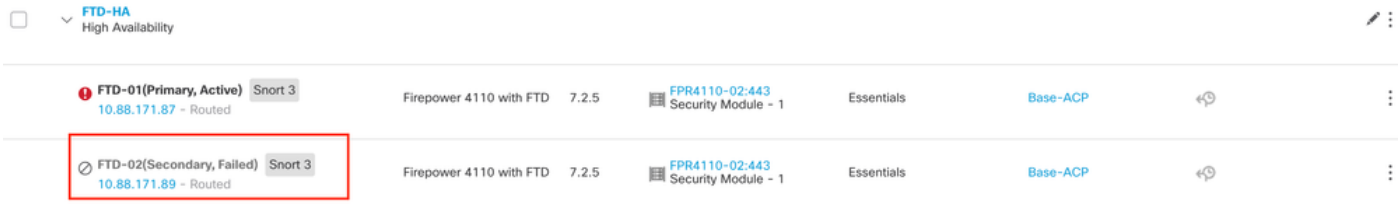
Este procedimiento es compatible con los dispositivos:

- Dispositivos Cisco Secure Firewall serie 1000
- Dispositivos Cisco Secure Firewall serie 2100
- Dispositivos Cisco Secure Firewall serie 3100
- Dispositivos Cisco Secure Firewall serie 4100
- Dispositivos Cisco Secure Firewall serie 4200
- Dispositivo Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defence para VMWare

Antes de comenzar

Este documento requiere que tenga la nueva unidad configurada con las mismas versiones FXOS y FTD.

Identifique la unidad defectuosa

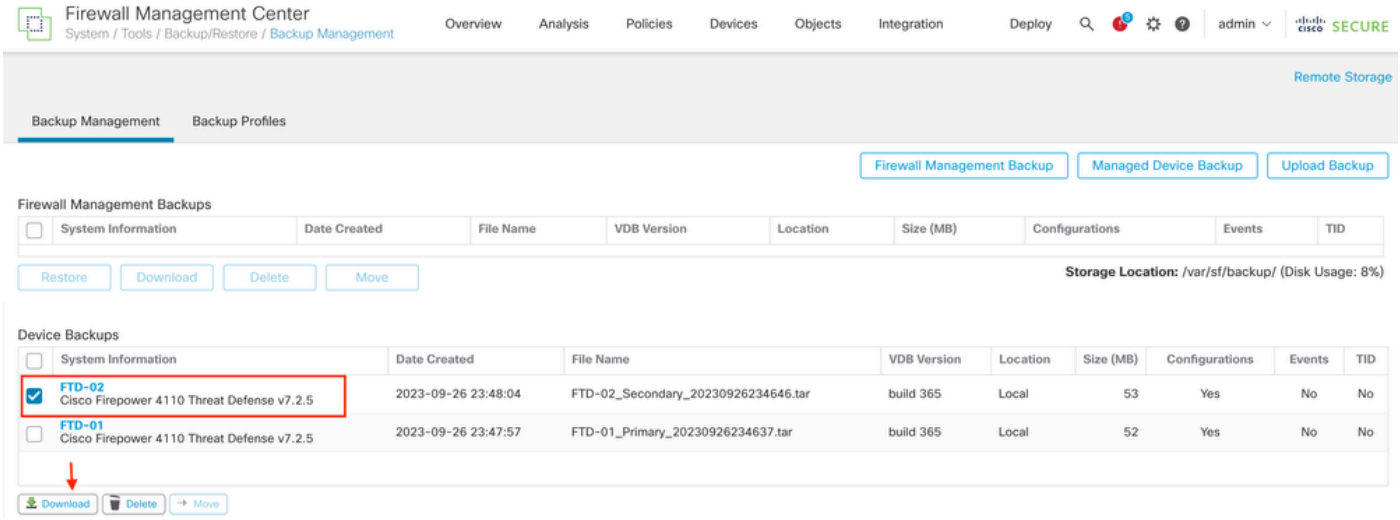


En esta situación, la unidad secundaria (FTD-02) se encuentra en estado de fallo.

Sustitución de una unidad defectuosa por una unidad auxiliar

Puede utilizar este procedimiento para sustituir la unidad primaria o secundaria. En esta guía se da por hecho que se dispone de una copia de seguridad de la unidad defectuosa que se va a sustituir.

Paso 1. Descargue el archivo de copia de seguridad de FMC. Vaya a System > Tools > Restore > Device Backups y seleccione la copia de seguridad correcta. Haga clic en Descargar:



Paso 2. Cargue la copia de seguridad del FTD en el directorio /var/sf/backup/ del nuevo FTD:

2.1 Desde test-pc (cliente SCP), cargue el archivo de copia de seguridad en el FTD bajo el directorio /var/tmp/:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

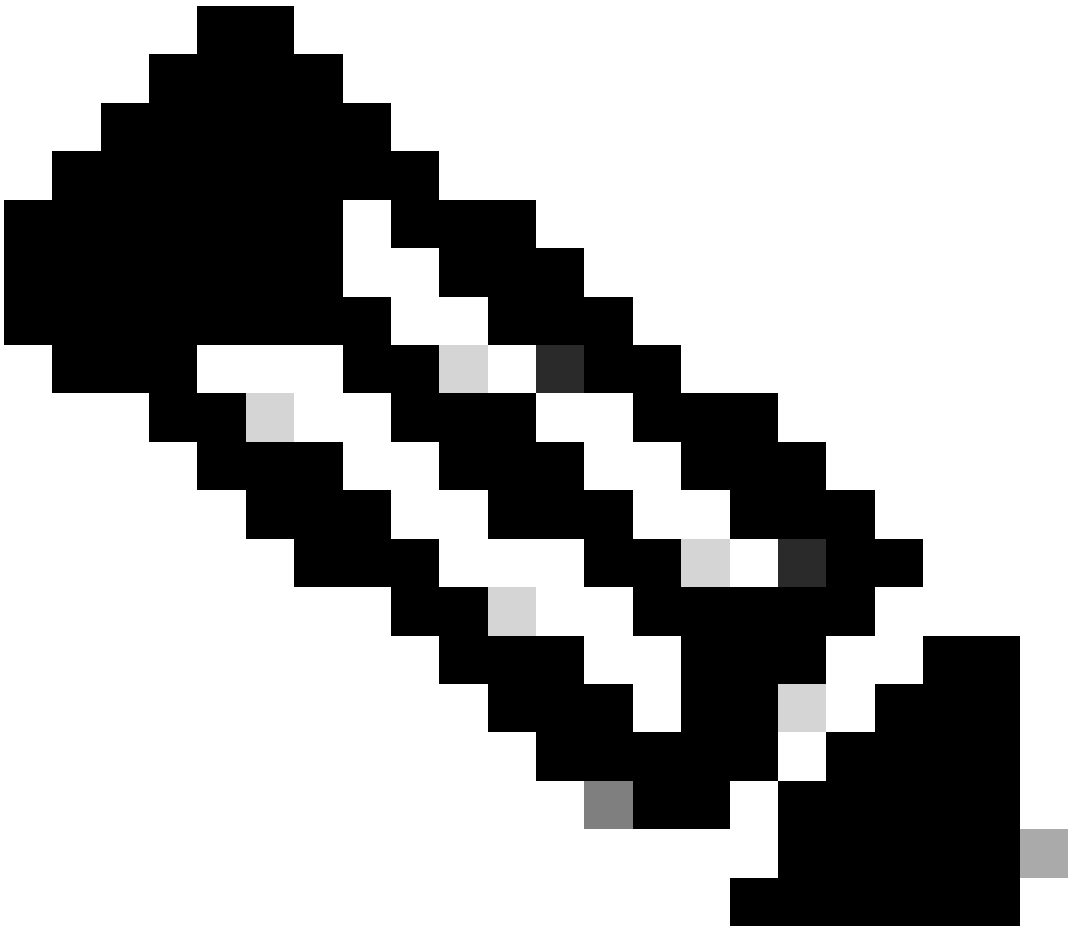
2.2 Desde el modo experto de CLI de FTD, mueva el archivo de copia de seguridad de /var/tmp/ a /var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

Paso 3. Restaure la copia de seguridad del FTD-02, aplicando el siguiente comando desde el modo clish:

```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model  :: Cisco Firepower 4110 Threat Defense
************************************************
Backup Details
************************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
************************************************

******************** Caution ***************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network
********************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
```

```
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

The system is going down for reboot NOW!
```

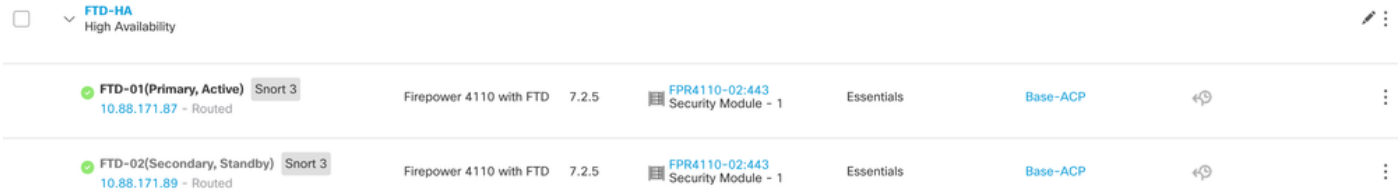


> Nota: Una vez finalizada la restauración, el dispositivo cierra la sesión de la CLI, se reinicia y se conecta automáticamente a la FMC. En este momento, el dispositivo va a aparecer desactualizado.

Paso 4. Reanude la sincronización HA. Desde la CLI de FTD, ingrese configure high-availability resume:

```
>configure high-availability resume
```

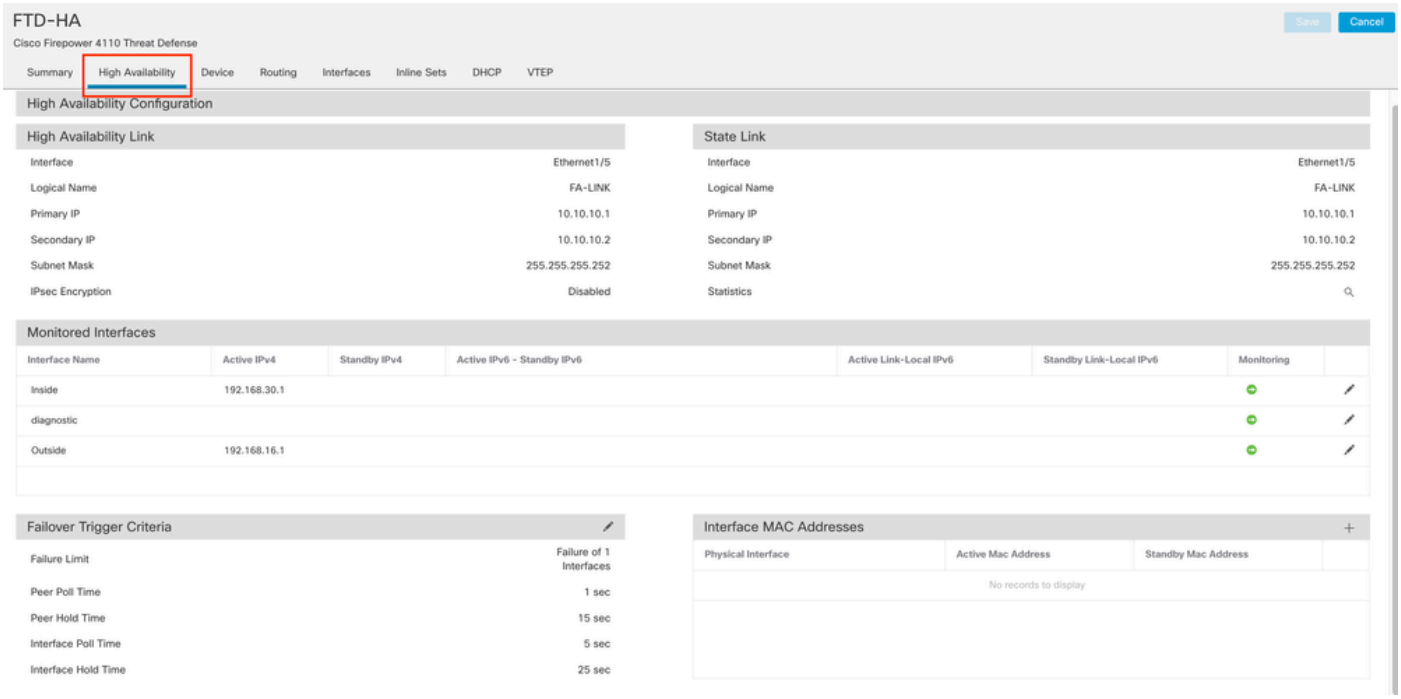
La configuración de alta disponibilidad de FTD ha finalizado:



Sustituya una unidad defectuosa sin apoyo

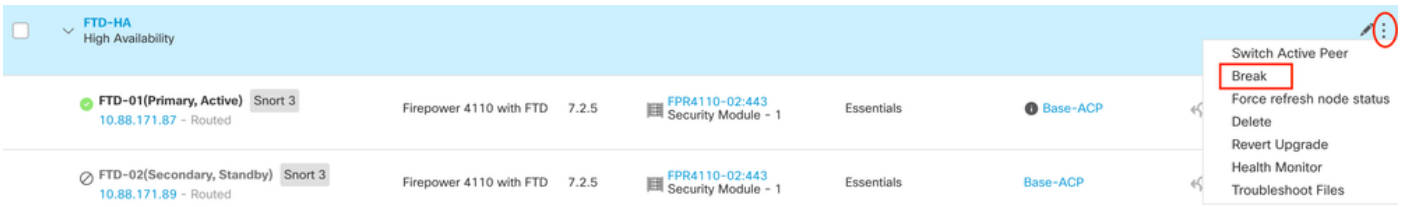
Si no dispone de una copia de seguridad del dispositivo que ha fallado, puede continuar con esta guía. Puede sustituir la unidad primaria o secundaria, oEl proceso varía dependiendo de si el dispositivo es primario o secundario. Todos los pasos descritos en esta guía son para restaurar una unidad secundaria defectuosa. Si desea restaurar una unidad primaria defectuosa, en el paso 5, configure la alta disponibilidad utilizando la unidad secundaria/activa existente como dispositivo principal y el dispositivo de reemplazo como dispositivo secundario/en espera durante el registro.

Paso 1. Realice una captura de pantalla (copia de seguridad) de la configuración de alta disponibilidad navegando hasta Device > Device Management. Edite el par FTD HA correcto (haga clic en el icono del lápiz) y, a continuación, haga clic en la opción High Availability:

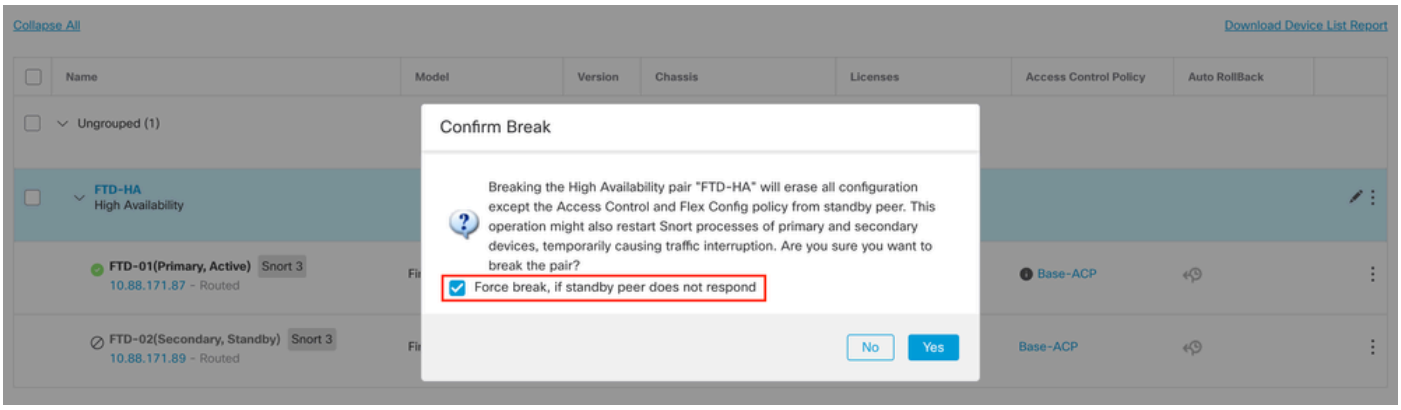


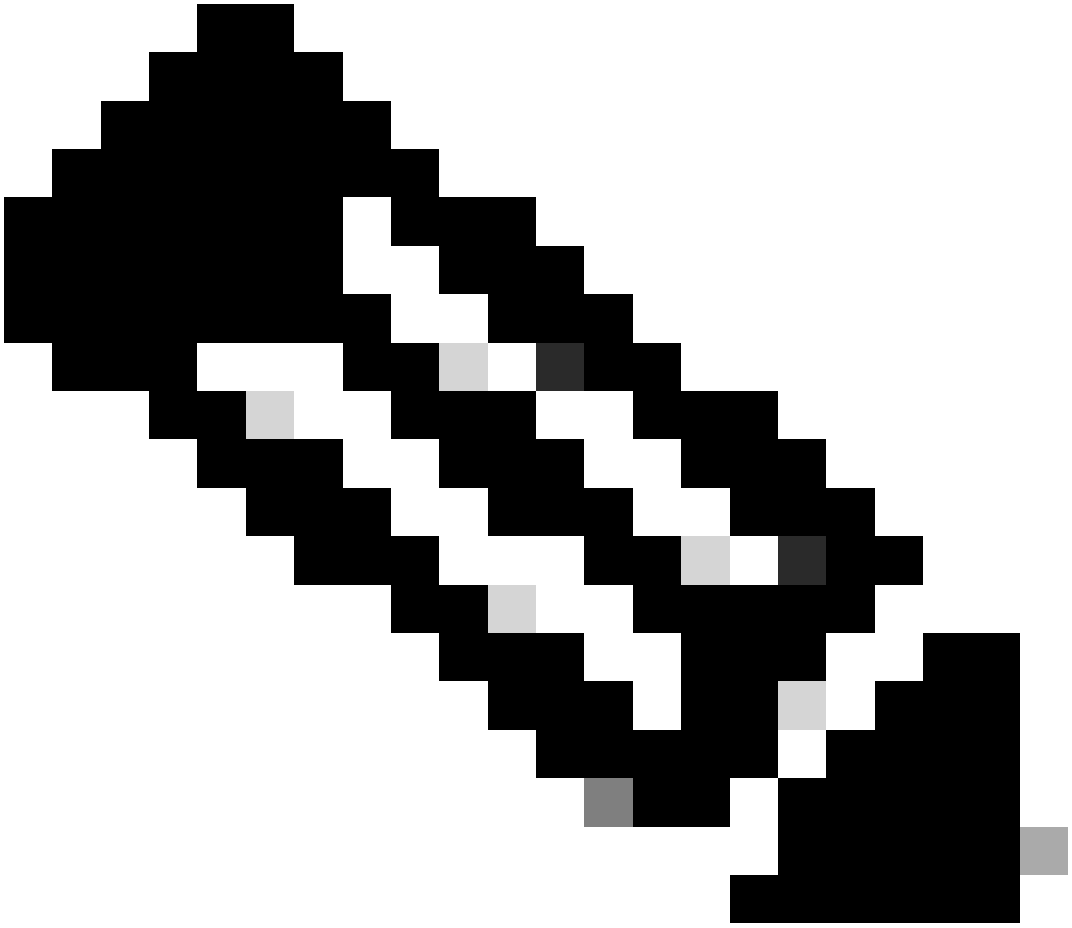
Paso 2. Rompa el HA.

2.1 Navegue hasta Devices > Device Management y luego haga clic en el menú de tres puntos en la esquina superior derecha. A continuación, haga clic en la opción Break:



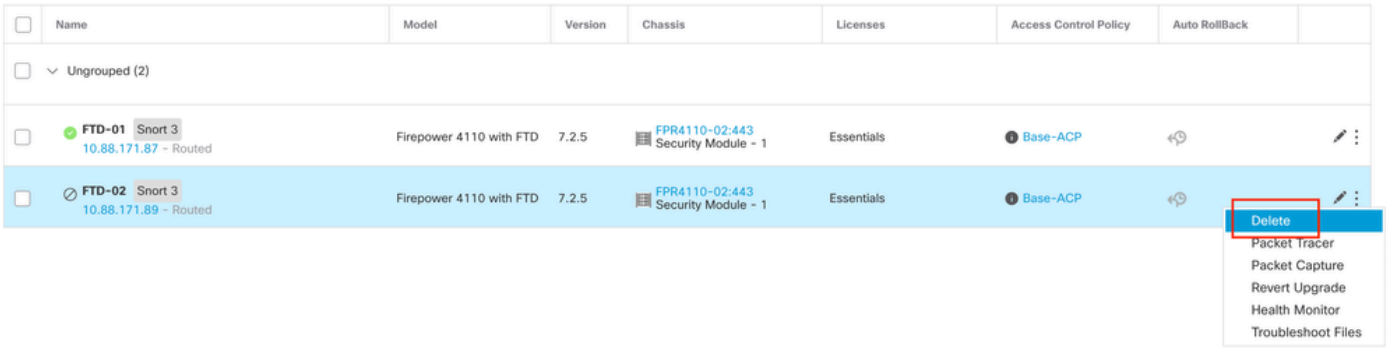
2.2. Seleccione Force break, si el par en espera no responde opción:





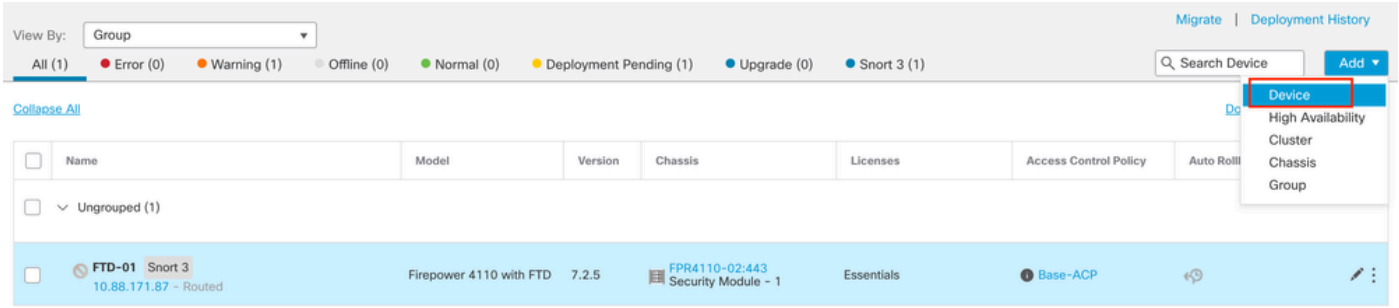
Nota: Debido a que la unidad no responde, debe forzar la interrupción del HA. Cuando interrumpe un par de alta disponibilidad, el dispositivo activo conserva toda la funcionalidad implementada. El dispositivo en espera pierde sus configuraciones de failover e interfaz y se convierte en un dispositivo autónomo.

Paso 3. Suprimir FTD defectuoso. Identifique el FTD que desea reemplazar y, a continuación, haga clic en el menú de tres puntos. Haga clic en Eliminar:



Paso 4. Agregue el nuevo FTD.

4.1. Navegue hasta Dispositivos > Administración de dispositivos > Agregar y luego haga clic en Dispositivo:



4.2. Seleccione el método de aprovisionamiento, en este caso, Clave de registro, configure Host, Mostrar nombre, Clave de registro. Configure una Política de control de acceso y haga clic en Registrar.

Add Device

Select the Provisioning Method:

(•) Registration Key ( ) Serial Number

[ ] CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

Base-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

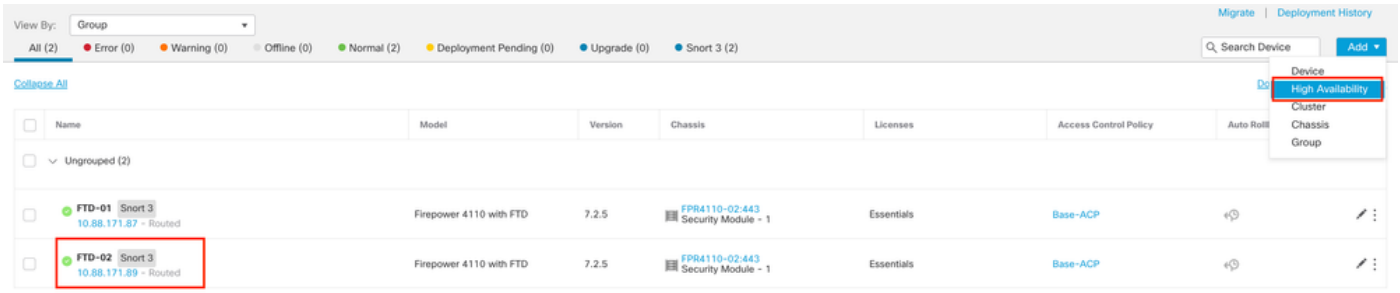
Unique NAT ID:†

[ ] Transfer Packets

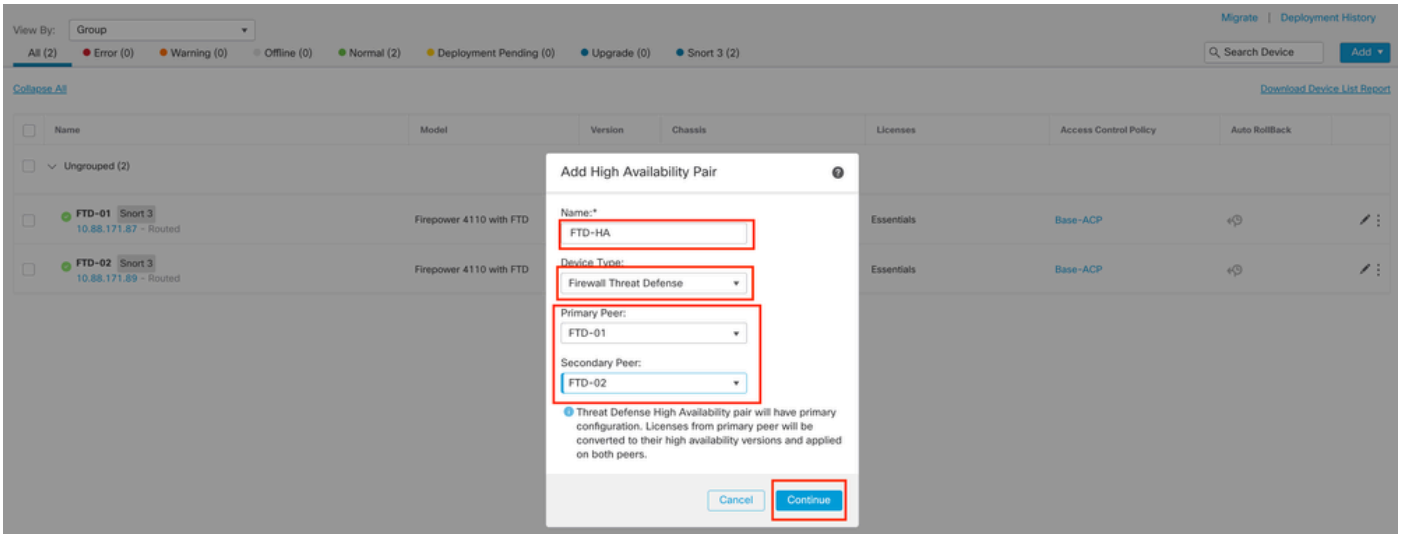
Cancel Register

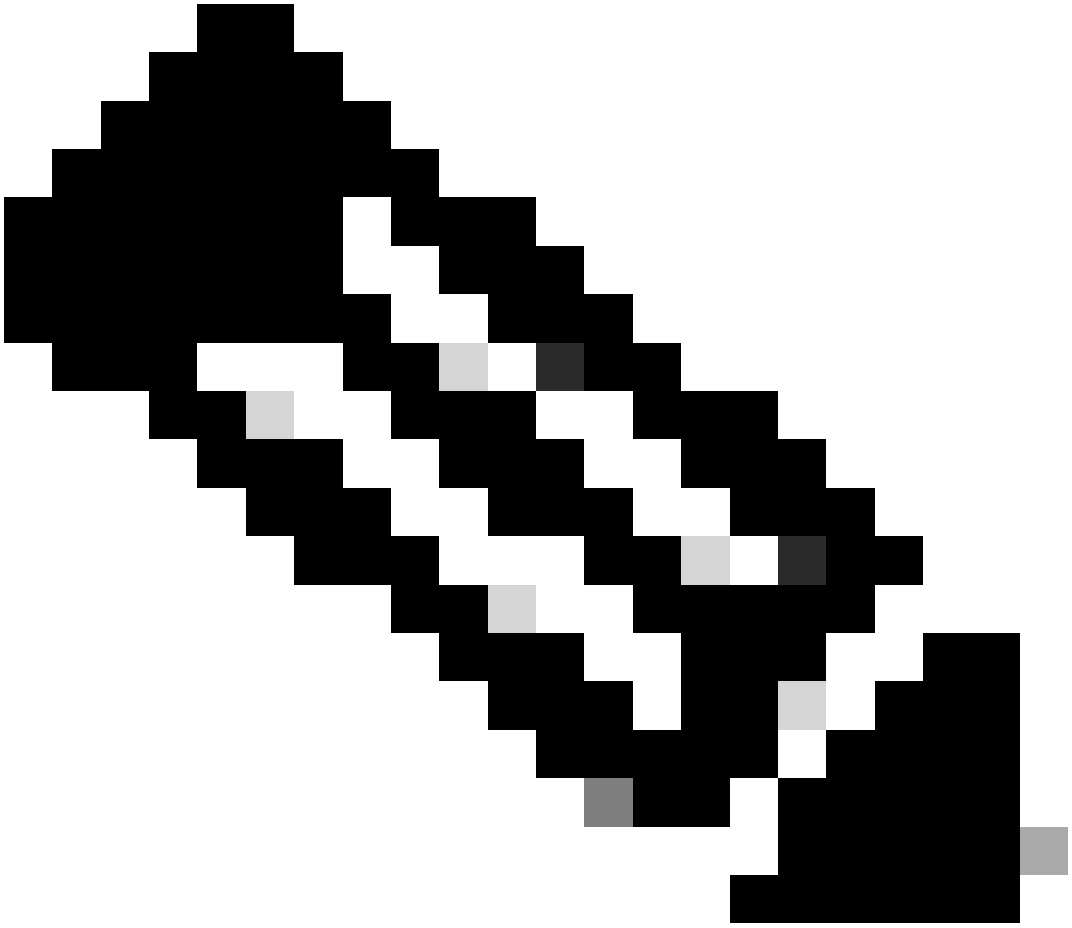
Paso 5. Cree el HA.

5.1 Navegue hasta Devices > Device Management > Add y haga clic en la opción High Availability.



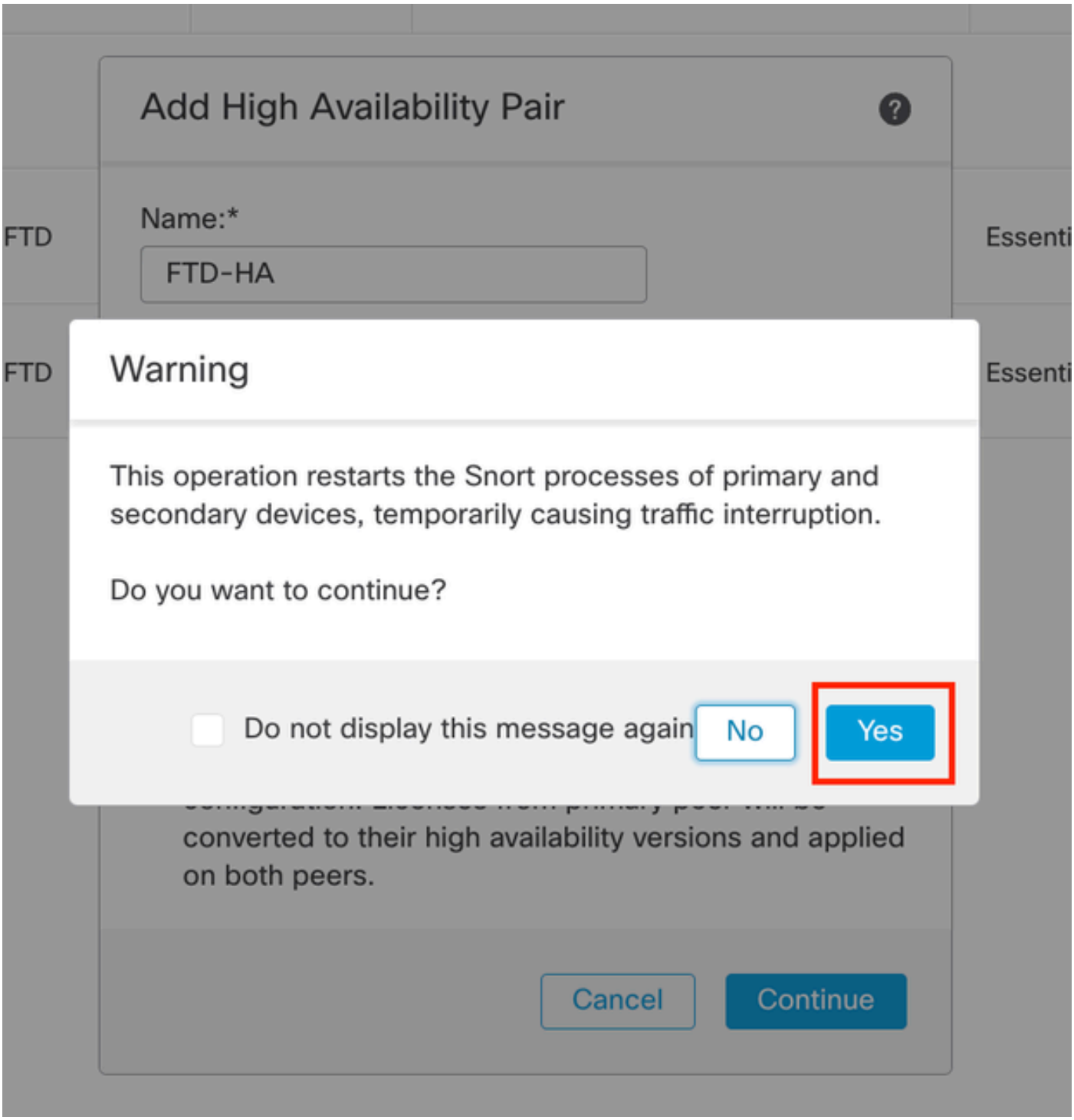
5.2. Configure el par Agregar alta disponibilidad. Configure el nombre, el tipo de dispositivo, seleccione FTD-01 como el par principal y FTD-02 como el par secundario y, a continuación, haga clic en Continuar.

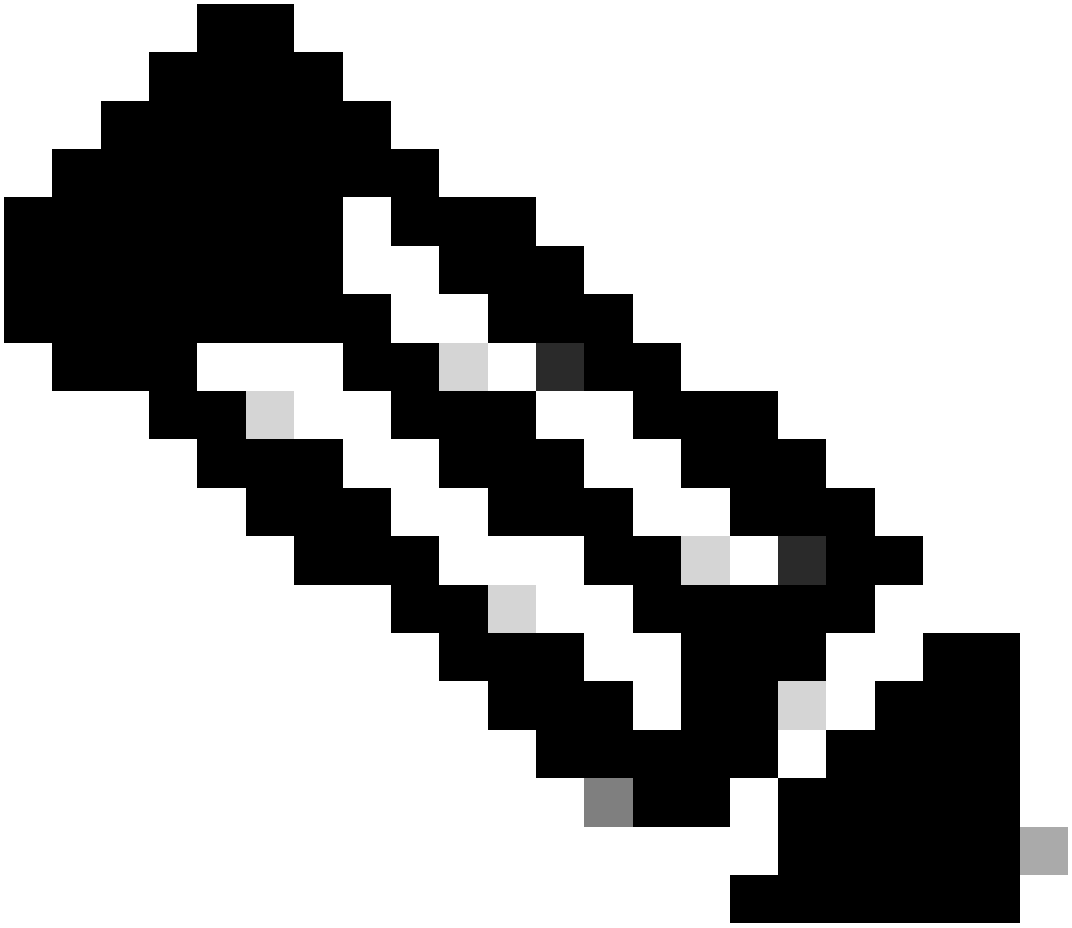




Nota: Recuerde seleccionar la unidad primaria como el dispositivo que aún tiene la configuración, en este caso, FTD-01.

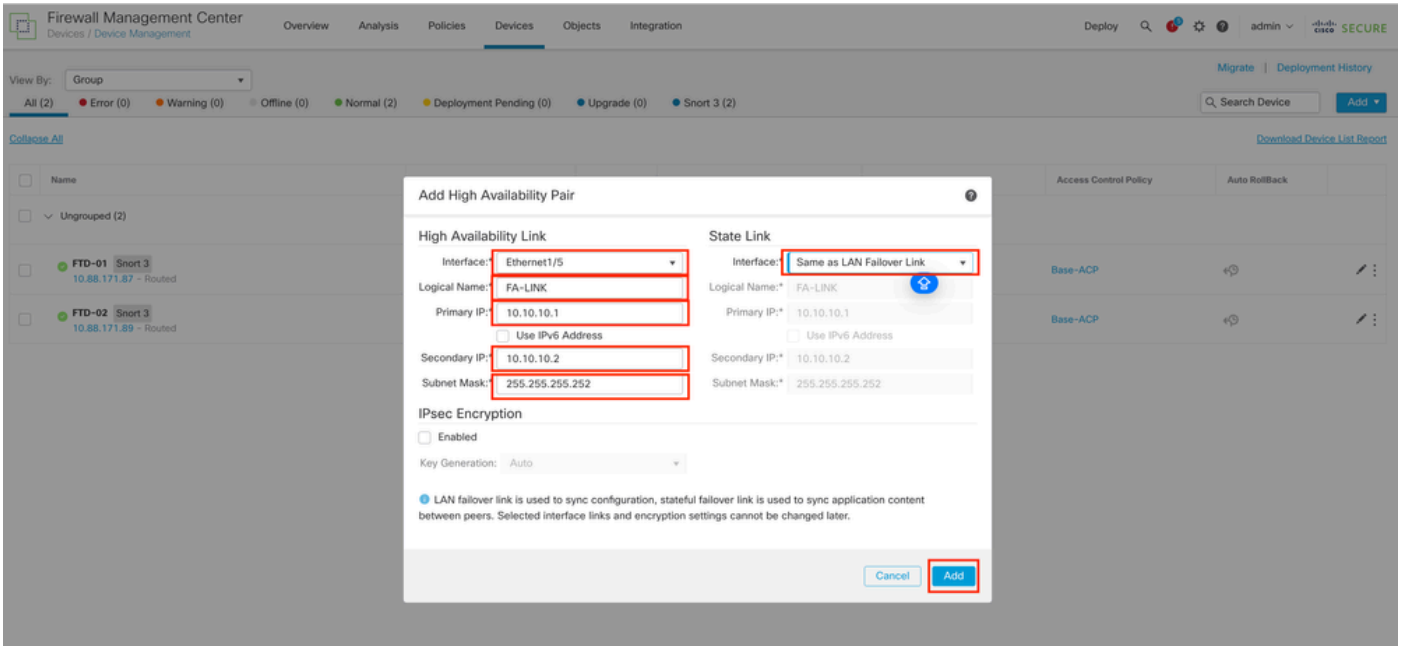
5.3. Confirme la creación de HA y, a continuación, haga clic en Sí.


Add High Availability Pair
Name:*
FTD-HA
FTD
Essenti
FTD
Essenti
Warning
This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.
Do you want to continue?
Do not display this message again
No
Yes
converted to their high availability versions and applied on both peers.
Cancel
Continue

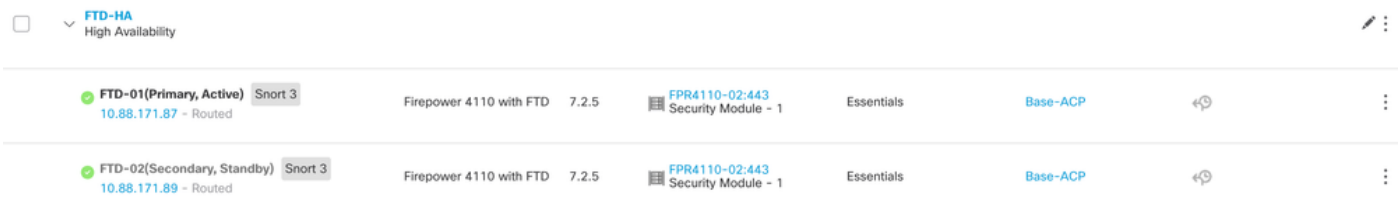


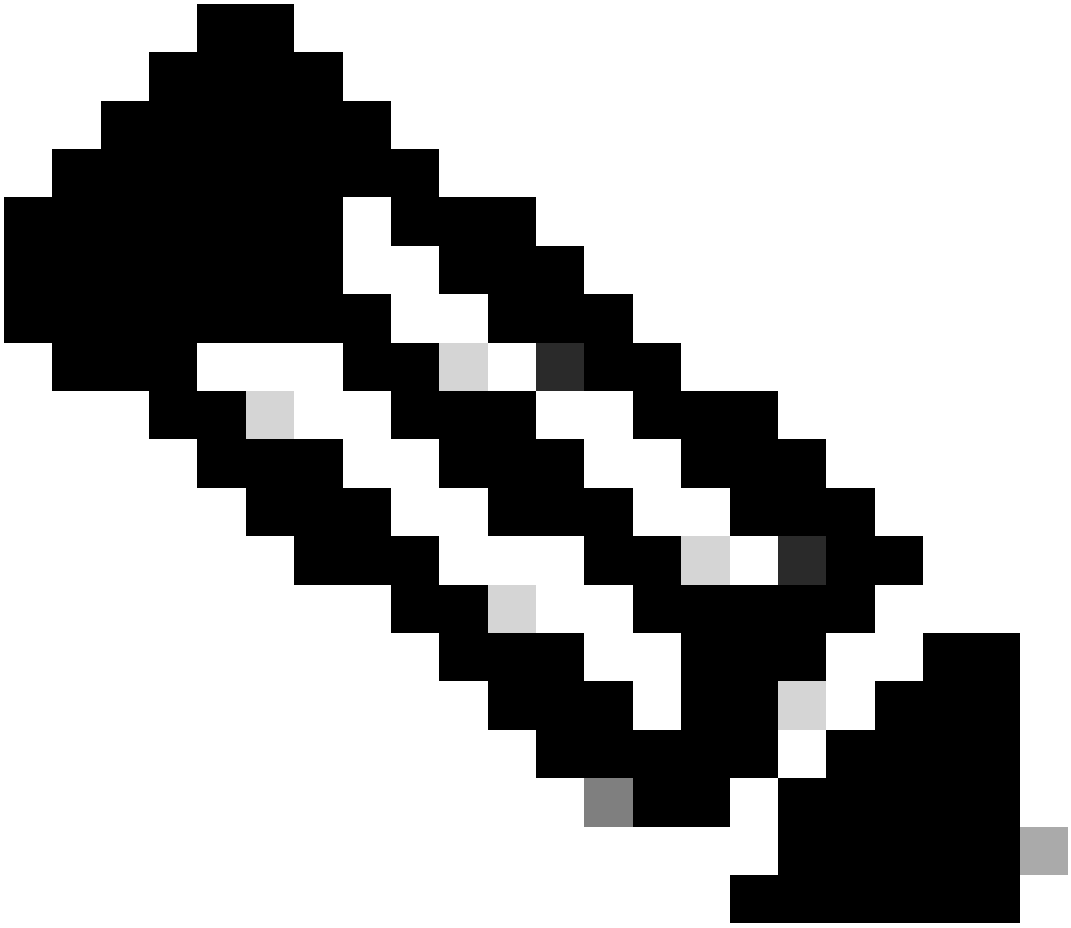
Nota: La configuración de la alta disponibilidad reinicia el motor de snort de ambas unidades y esto puede causar la interrupción del tráfico.

5.4. Configure los parámetros de alta disponibilidad realizados en el paso 2 y, a continuación, haga clic en la opción Add:



6. La configuración de alta disponibilidad de FTD se ha completado:





Nota: Si no configura las direcciones MAC virtuales, debe borrar las tablas ARP en los routers conectados para restaurar el flujo de tráfico en caso de reemplazo de la unidad primaria. Para obtener más información, consulte Direcciones MAC y Direcciones IP en alta disponibilidad.

Información Relacionada

- Soporte técnico y descargas de Cisco

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).