Configuración de FTD Multi-Instance High-Availability en Firepower 4100

Contenido

Introducción

Este documento describe cómo configurar la conmutación por fallas en instancias de contenedores de FTD (multiinstancia).

Prerequisites

Requirements

Cisco recomienda que conozca Firepower Management Center y Firewall Threat Defence.

Componentes Utilizados

Cisco Firepower Management Center Virtual 7.2.5
Appliance de NGFW Cisco Firepower 4145 (FTD) 7.2.5
Sistema operativo extensible (FXOS) Firepower 2.12 (0.498)
Windows 10

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.

Antes de implementar FTD Multi-Instance, es importante entender cómo puede afectar el rendimiento de su sistema y planificar en consecuencia. Consulte siempre la documentación oficial de Cisco o consulte con un representante técnico de Cisco para garantizar una implementación y configuración óptimas.

Antecedentes

Multi-Instance es una función de Firepower Threat Defence (FTD) que es similar al modo de contexto múltiple ASA. Permite ejecutar varias instancias de FTD de contenedor independientes en un único componente de hardware. Cada instancia de contenedor permite la separación de recursos físicos, la gestión de la configuración independiente, las recargas independientes, las actualizaciones de software independientes y la compatibilidad total con funciones de defensa frente a amenazas. Esto resulta especialmente útil para organizaciones que requieren diferentes políticas de seguridad para diferentes departamentos o proyectos, pero que no desean invertir en varios dispositivos de hardware independientes. Actualmente, la función de instancias múltiples es compatible con los appliances de seguridad Firepower de las series 4100 y 9300 que ejecutan FTD 6.4 y versiones posteriores.

Este documento utiliza Firepower4145, que admite un máximo de 14 instancias de contenedor. Para ver el número máximo de instancias admitidas en Firepower Appliance, consulte Número máximo de instancias y recursos de contenedor por modelo.

Diagrama de la red

Este documento presenta la configuración y verificación para HA en Multi-Instance en este diagrama.

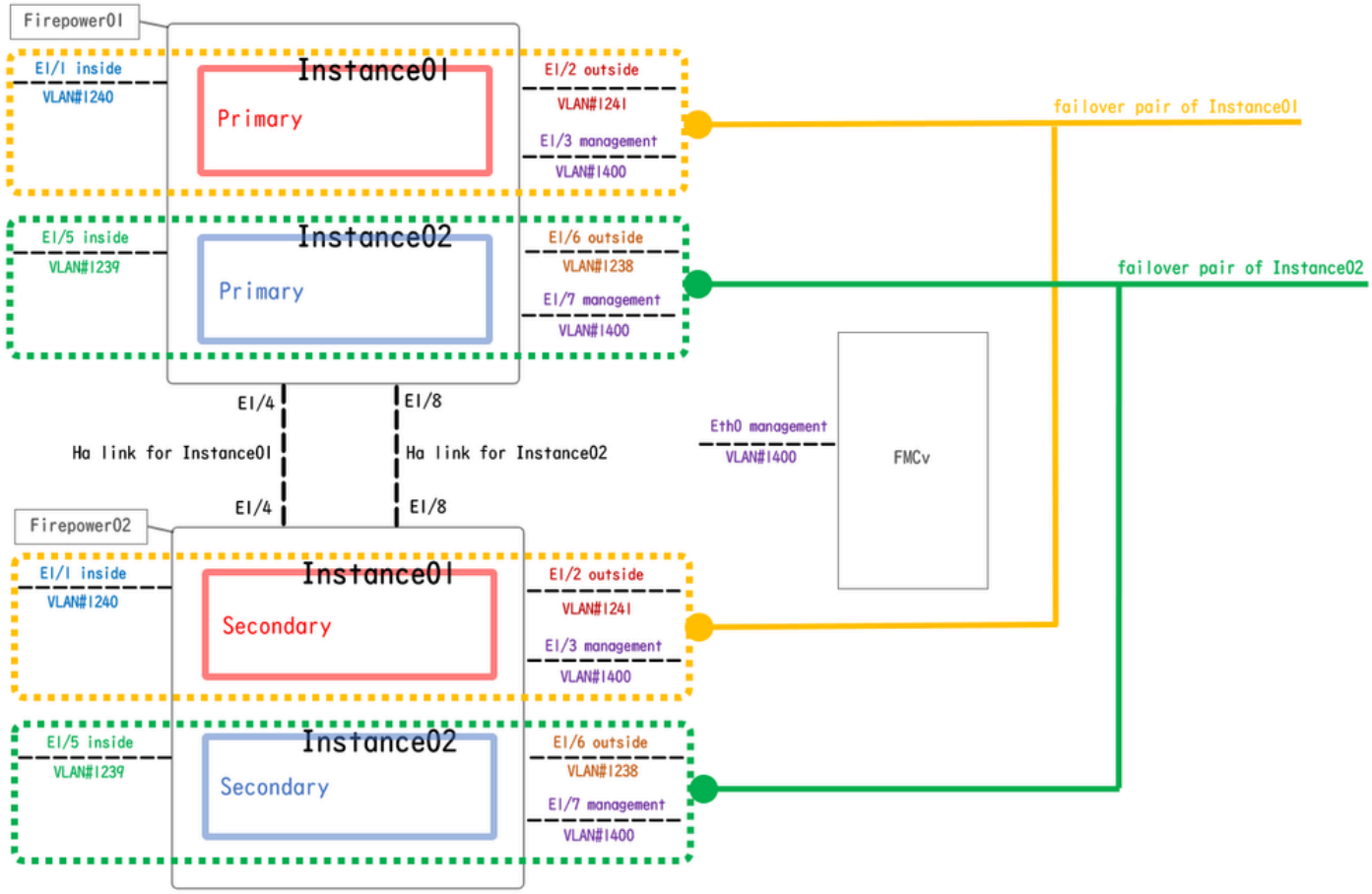


Diagrama de configuración lógica

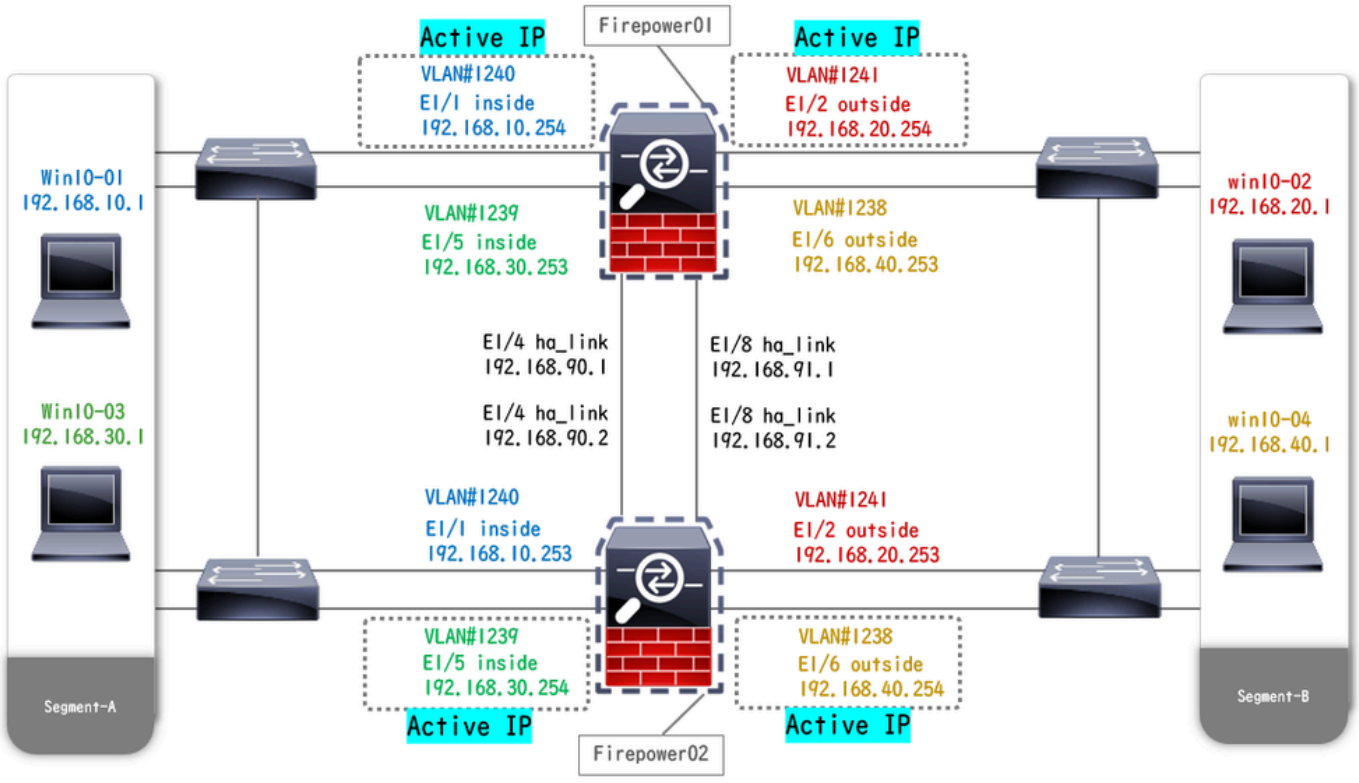
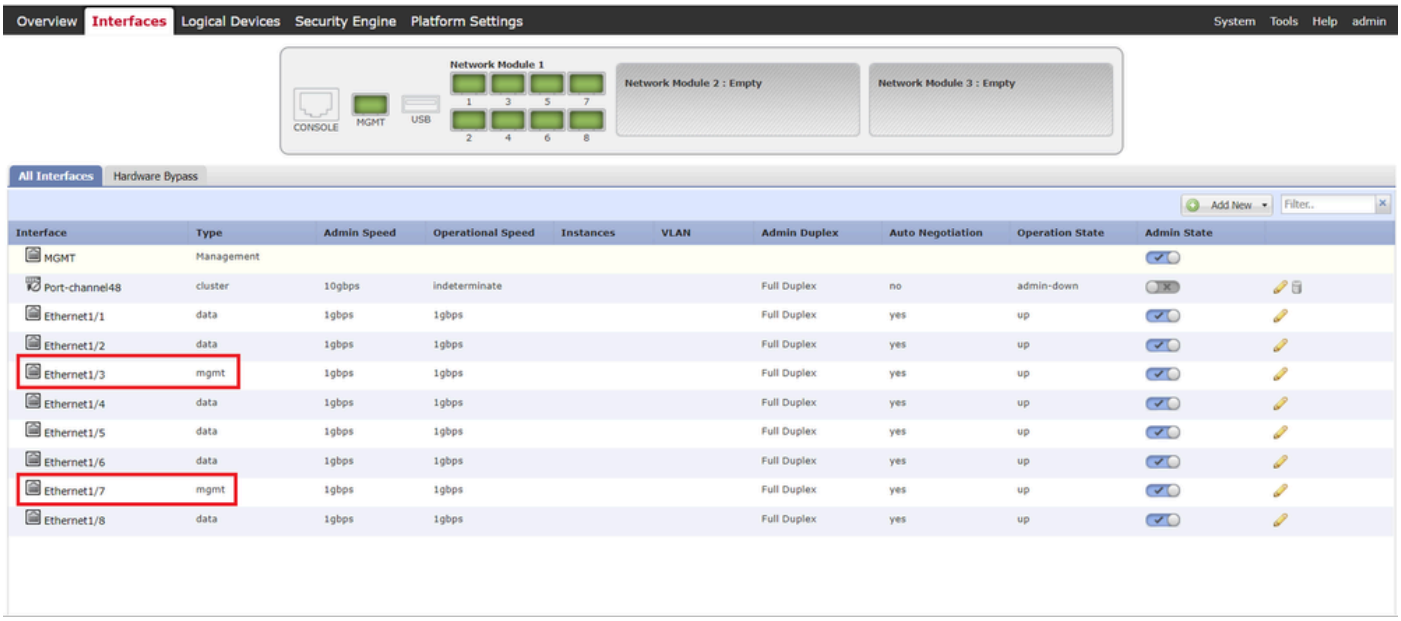


Diagrama de configuración física

Configuraciones

Paso 1. Preconfigurar interfaces

a. Navegue hasta Interfaces en FCM. Establezca 2 interfaces de gestión. En este ejemplo, Ethernet1/3 y Ethernet1/7.



Preconfigurar interfaces

Paso 2. Agregue 2 perfiles de recursos para instancias de contenedor.

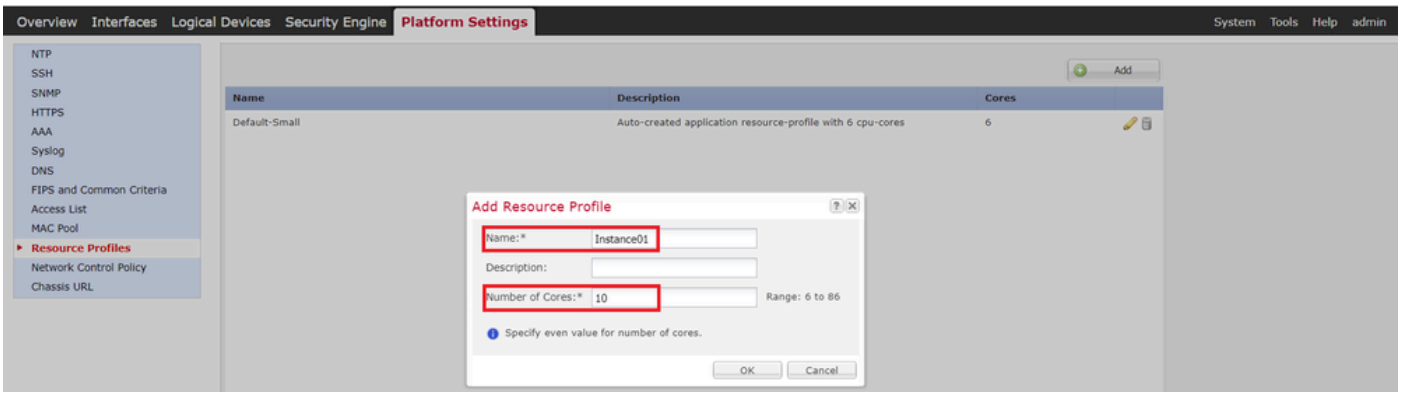
a. Navegue hasta Configuración de la plataforma > Perfiles de recursos > Agregar en FCM. Establecer el primer perfil de recursos.

En este ejemplo:
·Nombre: Instancia01
·Número de núcleos: 10

Nota: Para el HA de un par de instancias de contenedor, deben utilizar los mismos atributos de perfil de recurso.

Establezca el nombre del perfil entre 1 y 64 caracteres. Tenga en cuenta que no puede cambiar el nombre de este perfil después de agregarlo.

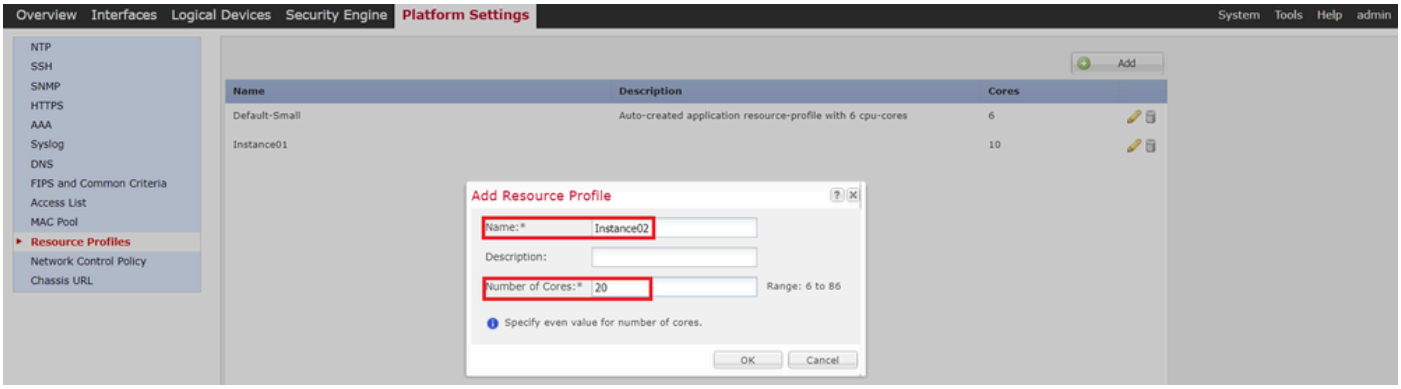
Establezca el número de núcleos para el perfil, entre 6 y el máximo.



Agregar el primer perfil de recursos

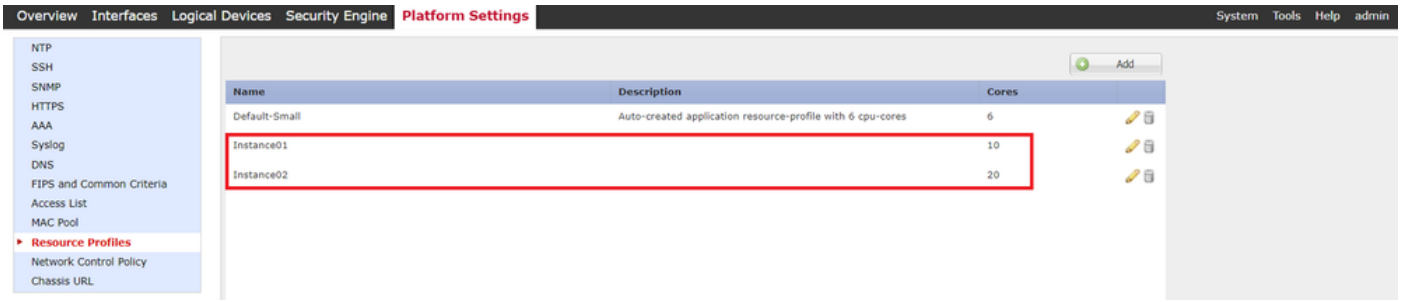
b. Repita a. en el paso 2 para configurar el segundo perfil de recursos.

En este ejemplo:
·Nombre: Instancia02
·Número de núcleos: 20



Agregar 2º perfil de recursos

c. Compruebe que 2 perfiles de recursos se han agregado correctamente.



Confirmar perfil de recurso

Paso 3. (Opcional)Agregue un Prefijo de Pool MAC de la dirección MAC virtual para las Interfaces de Instancia de Contenedor.

Puede establecer manualmente la dirección MAC virtual para la interfaz activa/en espera. Si las Direcciones MAC Virtuales no están configuradas , para la capacidad de instancias múltiples, el chasis genera automáticamente direcciones MAC para las interfaces de instancia y garantiza que una interfaz compartida en cada instancia utilice una dirección MAC única.

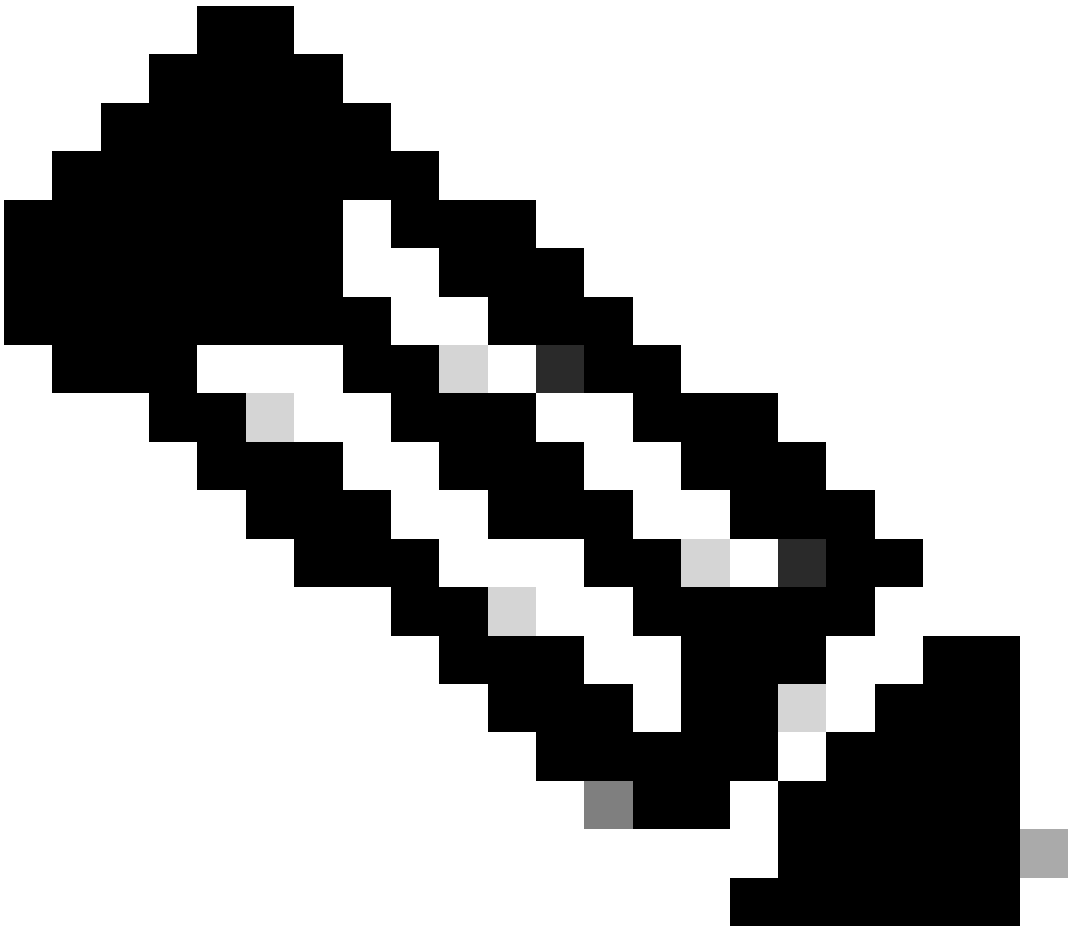
Verifique Agregar un Prefijo de Pool MAC y Ver Direcciones MAC para Interfaces de Instancia de Contenedor para obtener más detalles sobre la dirección MAC.

Paso 4. Agregue una instancia independiente.

a. Navegue hasta Dispositivos lógicos > Agregar autónomo. Establecer primera instancia.

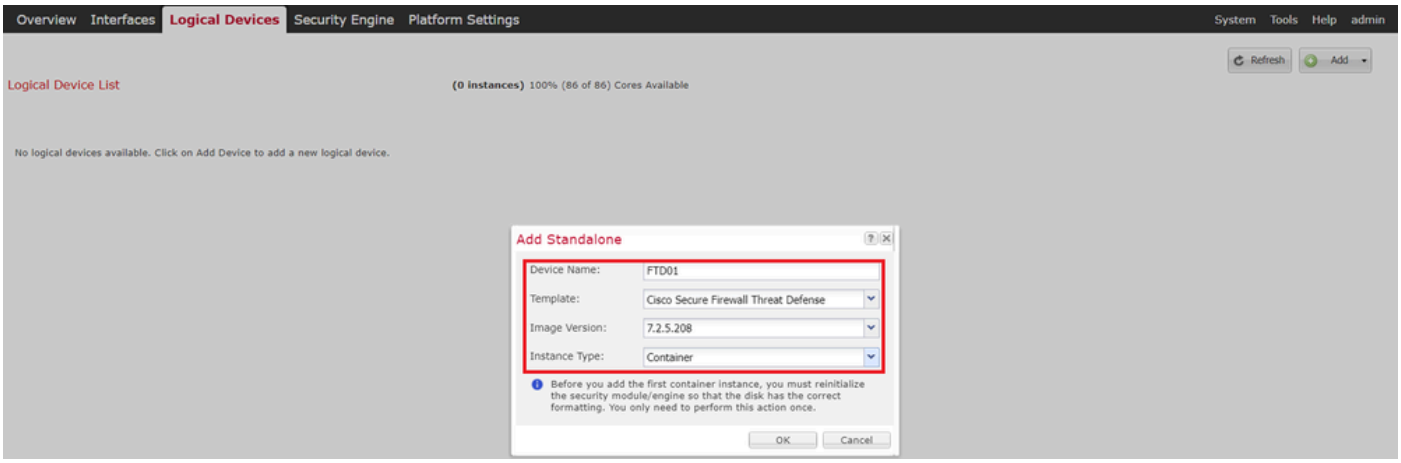
En este ejemplo:
·Nombre del dispositivo: FTD01

·Tipo de instancia: contenedor



Nota: La única forma de desplegar una aplicación contenedora es predesplegar una App-Instance con el Tipo de Instancia establecido en Contenedor. Asegúrese de seleccionar Contenedor.

No puede cambiar este nombre después de agregar el dispositivo lógico.

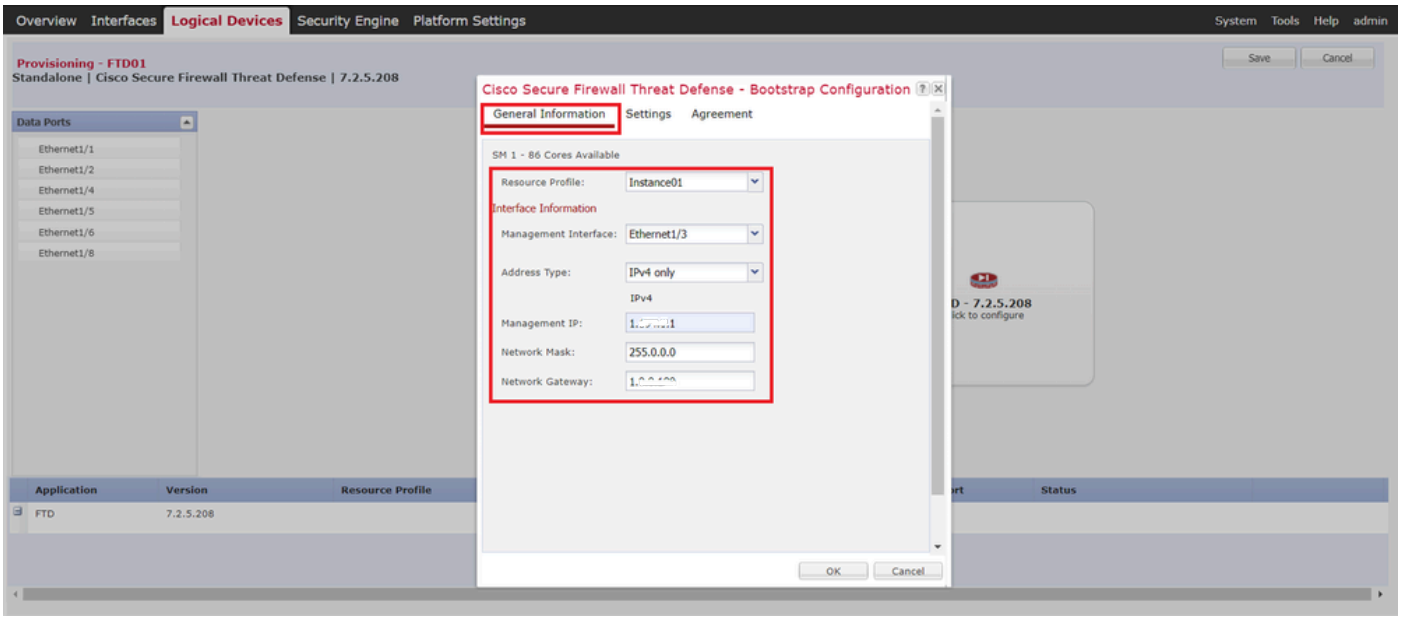


Agregar instancia

Paso 5. Configurar interfaces

a. Establezca Resource Profile, Management Interface, Management IP para Instance01.

En este ejemplo:
·Perfil de recurso: Instancia01
·Interfaz de gestión: Ethernet1/3
·IP de gestión: x.x.1.1



Configurar perfil/interfaz de gestión/IP de gestión

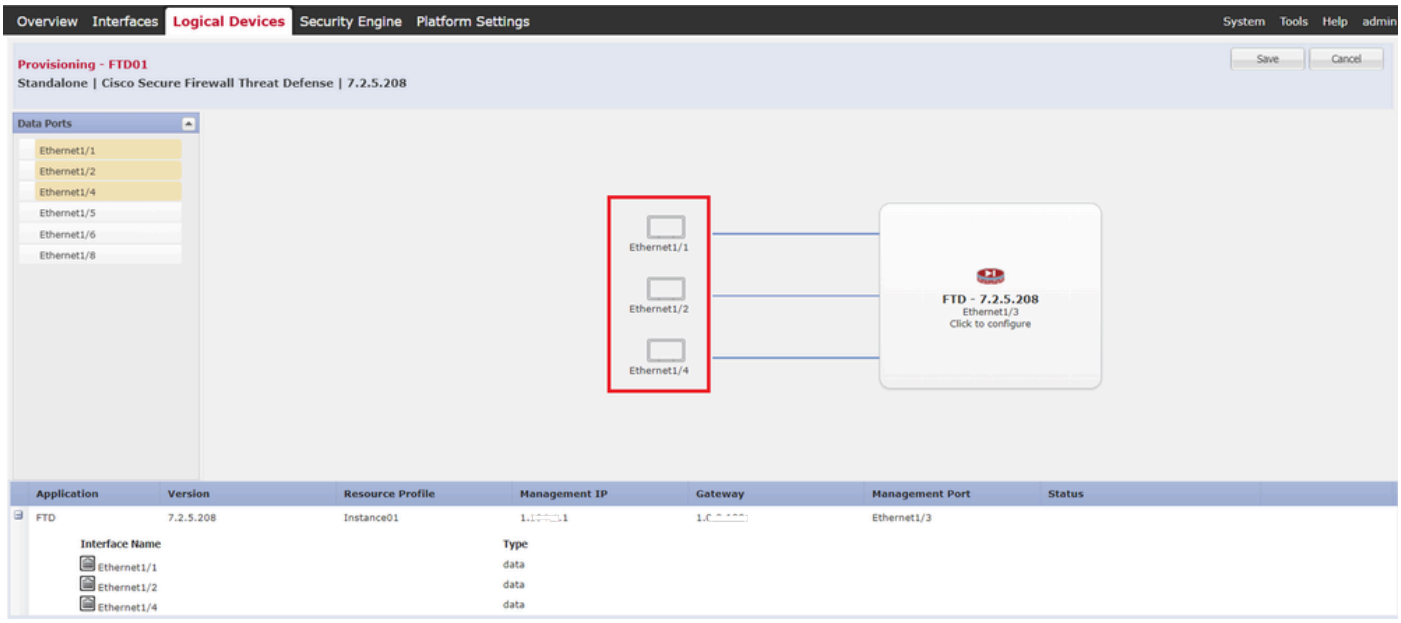
b. Establecer interfaces de datos.

En este ejemplo:

·Ethernet1/1 (se utiliza para el interior)

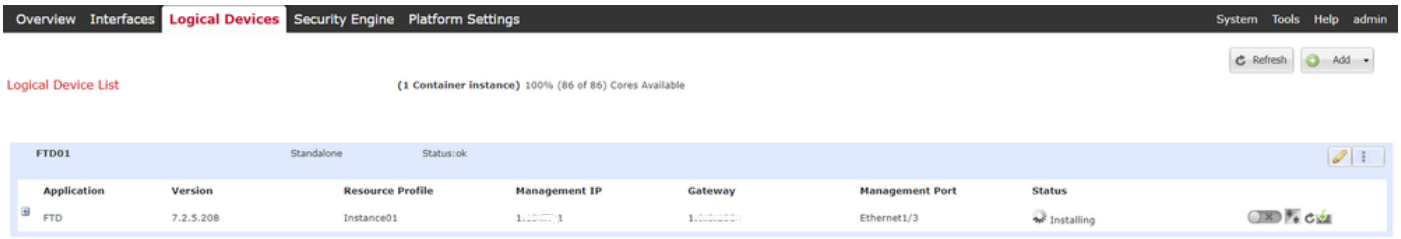
·Ethernet1/2 (utilizado para el exterior)

·Ethernet1/4 (se utiliza para el enlace HA)



Establecer interfaces de datos

c. Acceda a Dispositivos Lógicos. Esperando el inicio de la instancia.



Confirmar estado de instancia01

d. Repita a. en los pasos 4.a y 5.a a c para agregar la 2ª instancia y definir los detalles correspondientes.

En este ejemplo:

·Nombre del dispositivo: FTD11
·Tipo de instancia: contenedor

·Perfil de recursos: instancia02
·Interfaz de gestión: Ethernet1/7
·IP de gestión: x.x.10.1

·Ethernet1/5 = interior

·Ethernet1/6 = externa

·Ethernet1/8 = enlace HA

e. Confirme que dos instancias están en línea en FCM.

Confirmar El Estado De La Instancia En El Dispositivo Principal

f. (Opcional)Ejecute scope ssa y **scope slot 1** el **show app-Instance** comando para confirmar que las instancias 2 tienen el estado En línea en la CLI de Firepower.

```
<#root>

FPR4145-ASA-K9#

scope ssa

 FPR4145-ASA-K9 /ssa #

scope slot 1

 FPR4145-ASA-K9 /ssa/slot #

show app-Instance

 Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo

Online

7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11

Online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online
```

g. Haga lo mismo en el dispositivo secundario. Confirme que 2 instancias tengan el estado En línea.

Confirmar Estado De Instancia En El Dispositivo Secundario

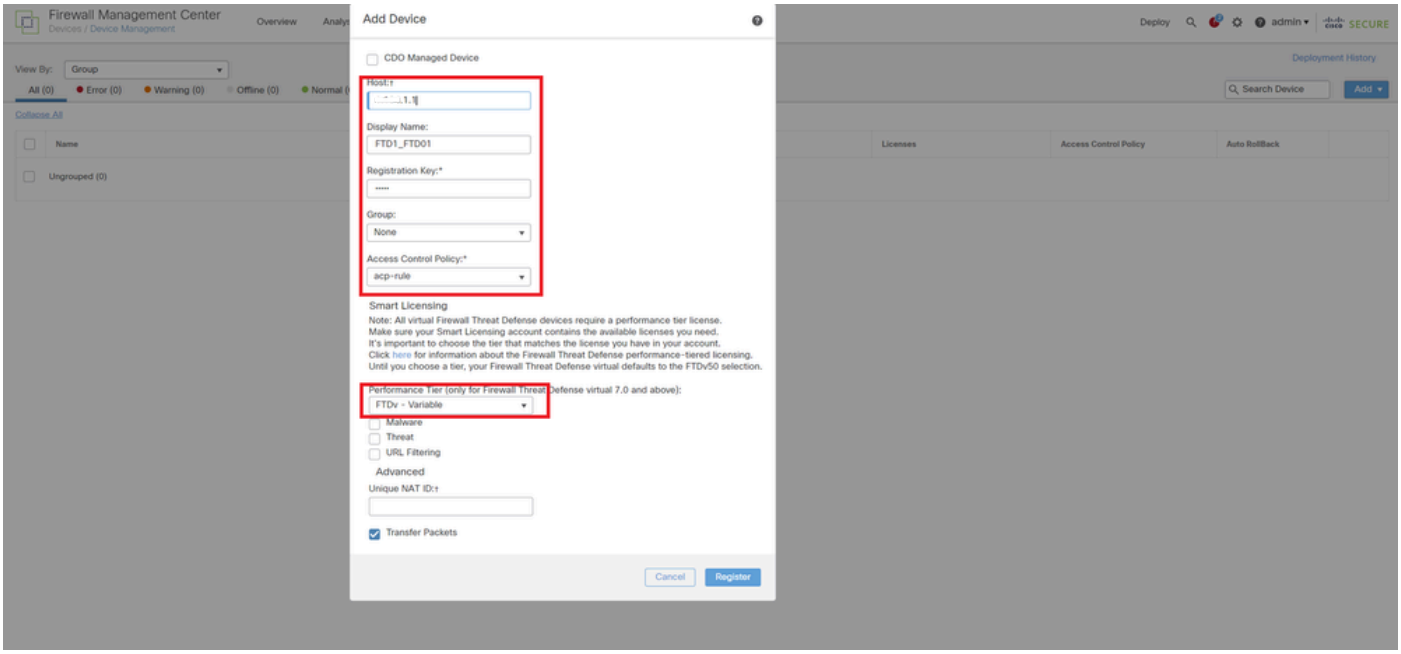
Paso 6. Agregue Un Par De Alta Disponibilidad Para Cada Instancia.

a. Navegue hasta **Dispositivos** > **Agregar dispositivo** en FMC. Agregar todas las instancias a FMC.

En este ejemplo:

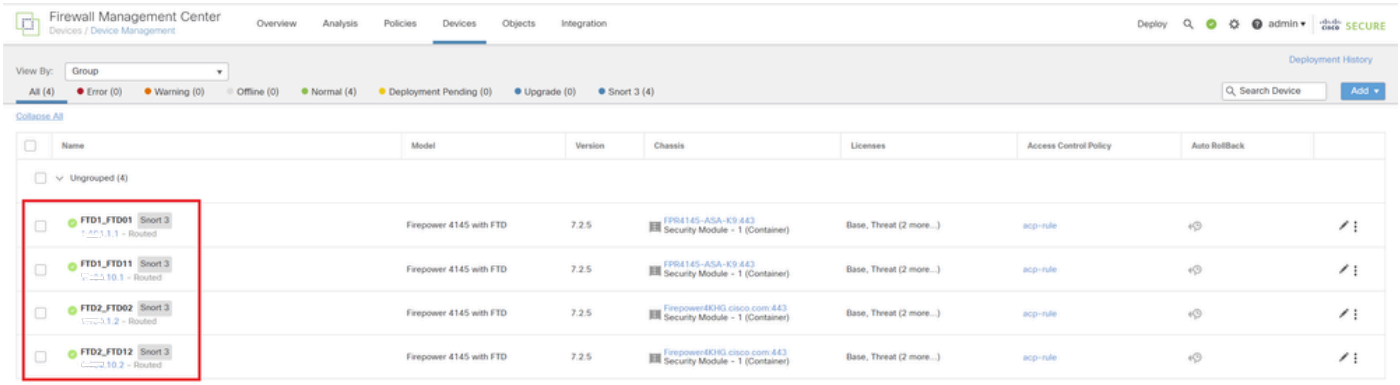
·Nombre de visualización de la instancia 01 de FTD1: FTD1_FTD01
·Nombre de visualización para la instancia 02 de FTD1: FTD1_FTD11
·Nombre de visualización de la instancia 01 de FTD2: FTD2_FTD02
·Nombre de visualización de la instancia 02 de FTD2: FTD2_FTD12

Esta imagen muestra la configuración de **FTD1_FTD01**.



Añadir instancia de FTD a FMC

b. Confirme que todas las instancias sean normales.



Confirmar estado de instancia en FMC

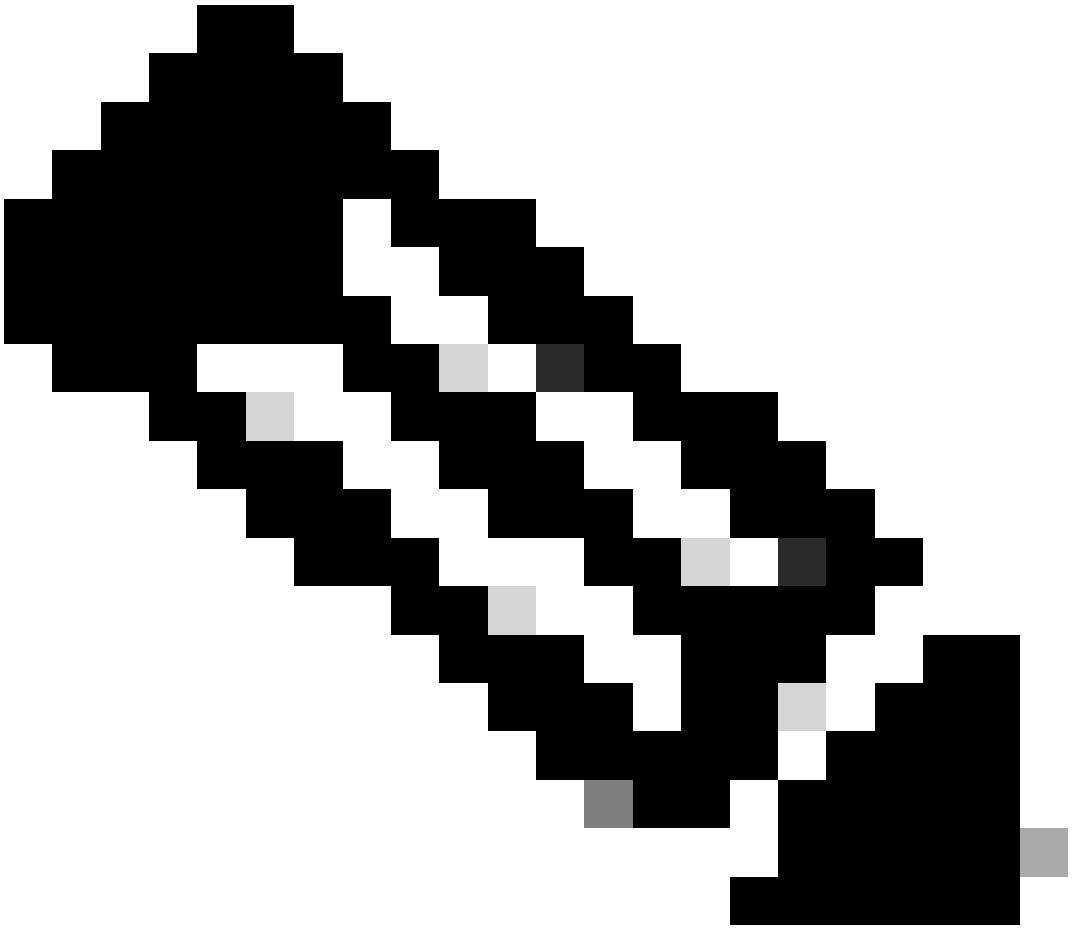
c. Vaya a **Devices** > **Add High Availability**. Establezca el primer par de conmutación por fallo.

En este ejemplo:

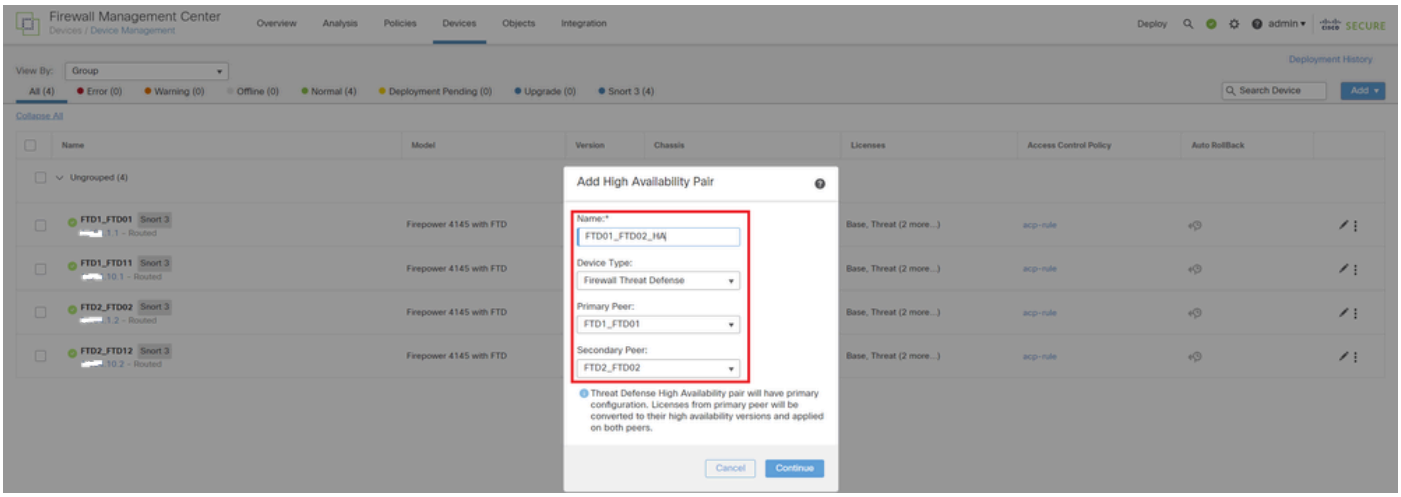
·**Nombre: FTD01_FTD02_HA**

·**Peer principal: FTD1_FTD01**

·**Peer secundario: FTD2_FTD02**



Nota: Asegúrese de seleccionar la unidad correcta como la unidad principal.



Agregar primer par de conmutación por error

d. Establezca IP para el link de failover en el primer par de failover.

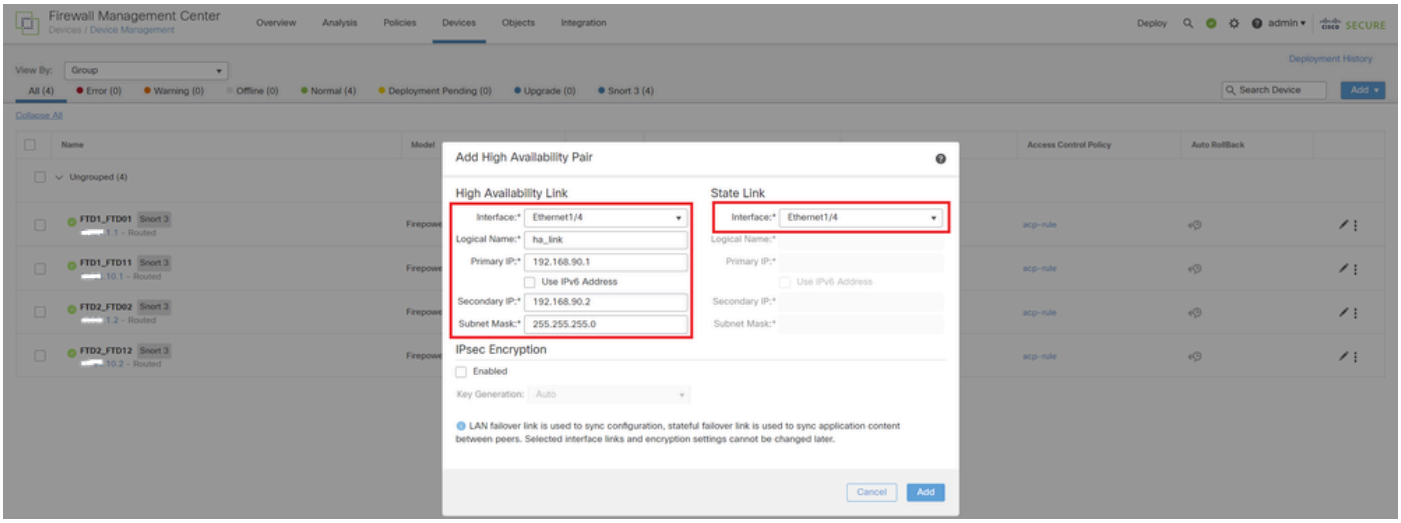
En este ejemplo:

·**Enlace de alta disponibilidad: Ethernet1/4**

·**Enlace de estado: Ethernet1/4**

·**IP principal: 192.168.90.1/24**

·**IP secundaria: 192.168.90.2/24**

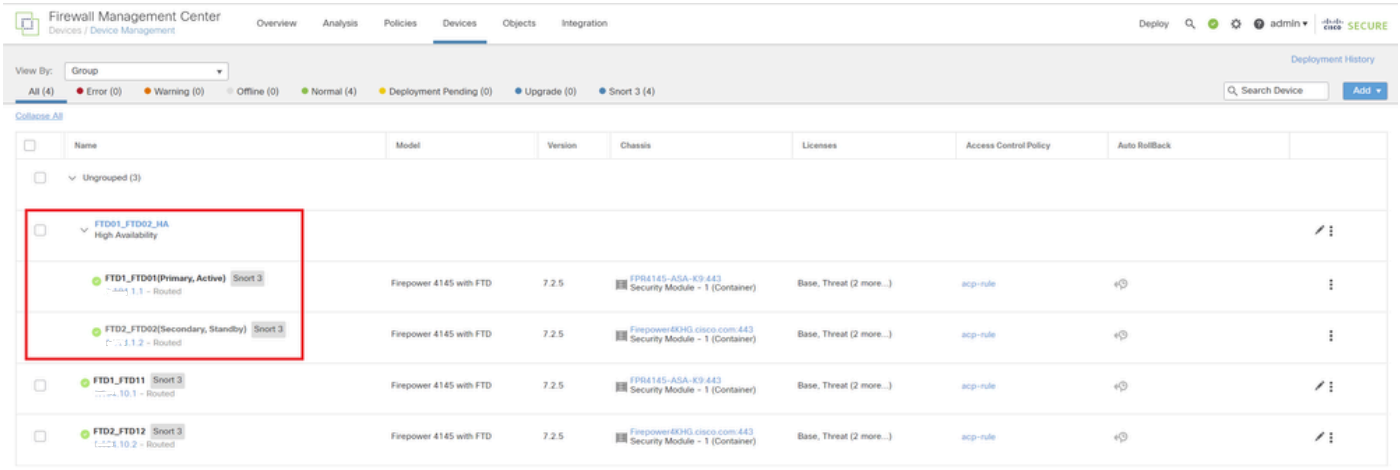


Establecer la interfaz HA y la IP para el primer par de conmutación por fallo

e. Confirmar el estado de conmutación por fallas

·**FTD1_FTD01: Principal, Activo**

·**FTD2_FTD02: Secundario, En espera**



Confirmar estado del primer par de conmutación por error

f. Vaya a **Devices** > **Click FTD01_FTD02_HA** (en este ejemplo) > **Interfaces.** Establecer IP activa para interfaz de datos.

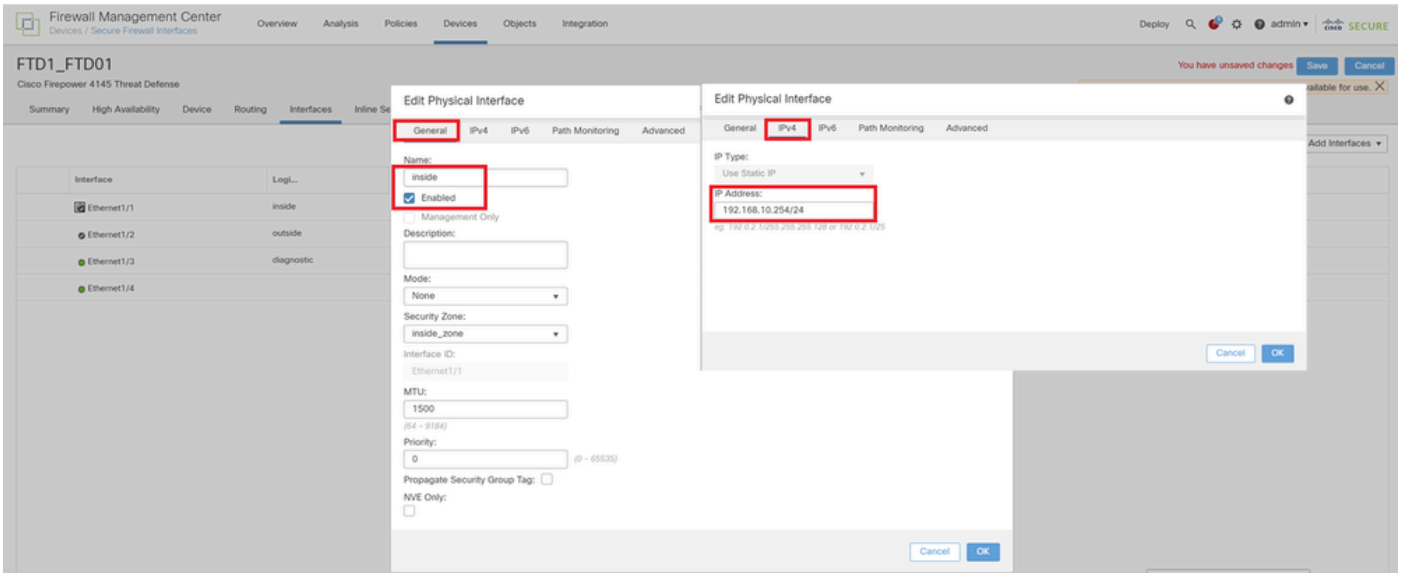
En este ejemplo:

·Ethernet1/1 (interno): 192.168.10.254/24

·Ethernet1/2 (exterior): 192.168.20.254/24

·Ethernet1/3 (diagnóstico): 192.168.80.1/24

Esta imagen muestra la configuración para la IP activa de **Ethernet1/1**.



Establecer IP activa para interfaz de datos

g. Vaya a **Devices** > **Click FTD01_FTD02_HA** (en este ejemplo) > **High Availability.** Establezca Standby IP for Data Interface.

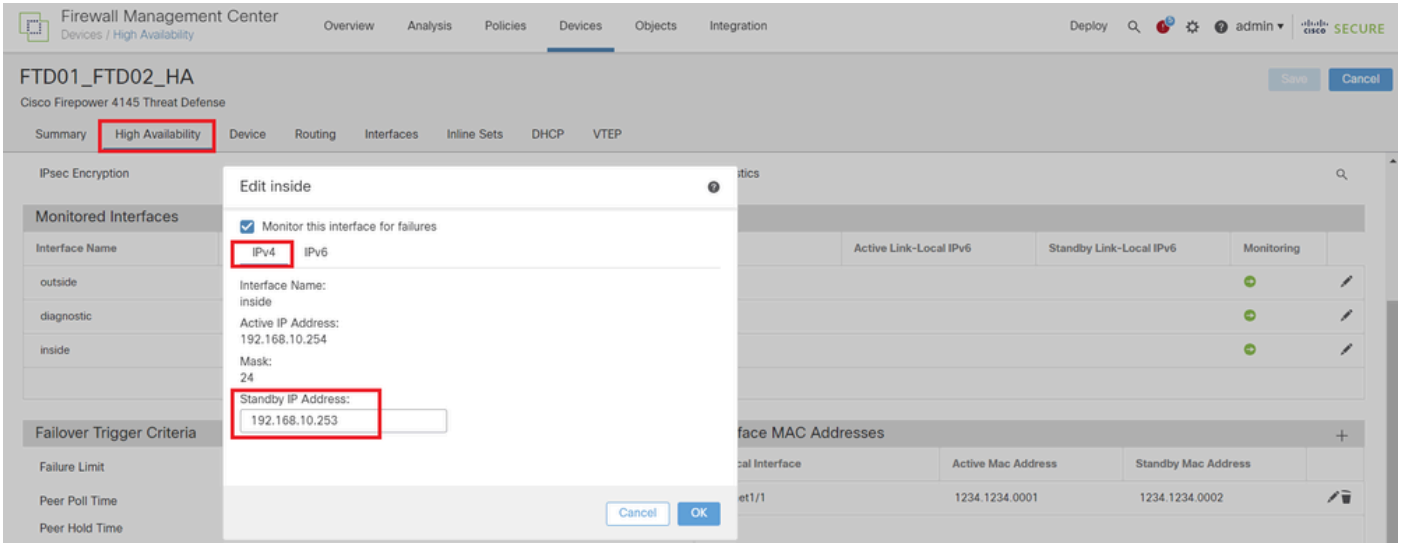
En este ejemplo:

·Ethernet1/1 (interno): 192.168.10.253/24

·Ethernet1/2 (exterior): 192.168.20.253/24

·Ethernet1/3 (diagnóstico): 192.168.80.2/24

Esta imagen muestra la configuración para la IP en espera de **Ethernet1/1**.



Establecer IP en espera para la interfaz de datos

h. Repita los pasos 6.c a g, para agregar el segundo par de conmutación por fallas.

En este ejemplo:

·Nombre: FTD11_FTD12_HA
·Par principal: FTD1_FTD11
·Par secundario: FTD2_FTD12

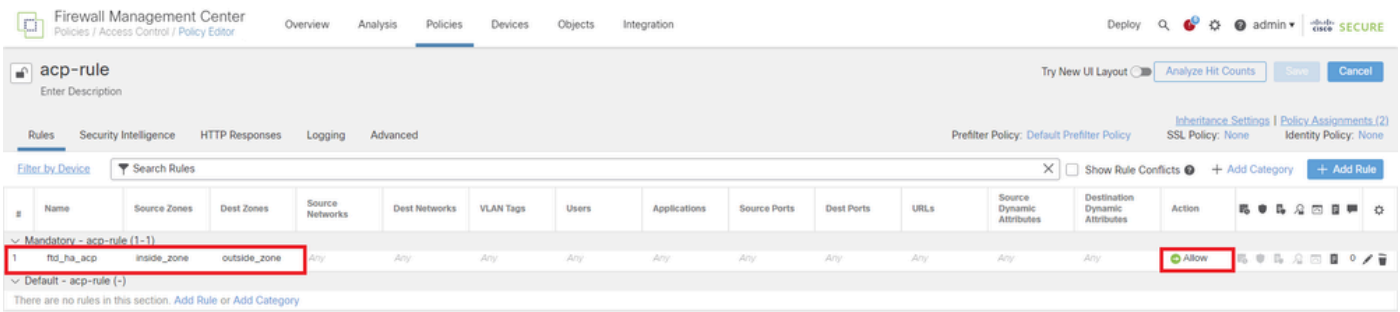
·Enlace de alta disponibilidad: Ethernet1/8
·Enlace de estado: Ethernet1/8
·Ethernet1/8 (ha_link activo): 192.168.91.1/24

·Ethernet1/5 (interna activa): 192.168.30.254/24
·Ethernet1/6 (fuera activo): 192.168.40.254/24
·Ethernet1/7 (diagnóstico activo): 192.168.81.1/24

·Ethernet1/8 (ha_link Standby): 192.168.91.2/24

·Ethernet1/5 (dentro del modo de espera): 192.168.30.253/24
·Ethernet1/6 (fuera del modo de espera): 192.168.40.253/24
·Ethernet1/7 (diagnóstico en espera): 192.168.81.2/24

i. Navegue hasta **Dispositivos lógicos** > **Agregar autónomo**. Establezca la regla ACP para permitir el tráfico desde el interior al exterior.



Establecer regla ACP

j. Despliegue el ajuste en FTD.

k. Confirmar estado de HA en CLI

El estado de HA para cada instancia también se confirma en la CLI de Firepower, que es igual que ASA.

Ejecute **show running-config failover** el **show failover** comando y confirme el estado de HA de FTD1_FTD01 (Instancia principal01) .

```
<#root>

// confrim HA status of FTD1_FTD01 (Instance01 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication htt

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host: P
...... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

Ejecute **show running-config failover** el **show failover** comando y confirme el estado de HA de FTD1_FTD11 (Instancia principal02) .

```
<#root>

// confrim HA status of FTD1_FTD11 (Instance02 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication htt

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ...... This host: P
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

Ejecute **show running-config failover** el **show failover** comando y confirme el estado de HA de FTD2_FTD02 (Instancia secundaria01) .

```
<#root>

// confrim HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

 failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

 Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host:
Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-
```

Ejecute **show running-config failover** el **show failover** comando y confirme el estado de HA de FTD2_FTD12 (Instancia secundaria02) .

<#root>

// confrim HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

```
 failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-
```

l. Confirmar el consumo de licencias

Todas las licencias se consumen por chasis/motor de seguridad y no por instancia de contenedor.

·Las licencias base se asignan automáticamente: una por motor/chasis de seguridad.

·Las licencias de funciones se asignan manualmente a cada instancia, pero solo se consume una licencia por función según el motor/chasis de seguridad. Para una licencia de función específica, solo necesita un total de 1 licencia, independientemente del número de instancias en uso.

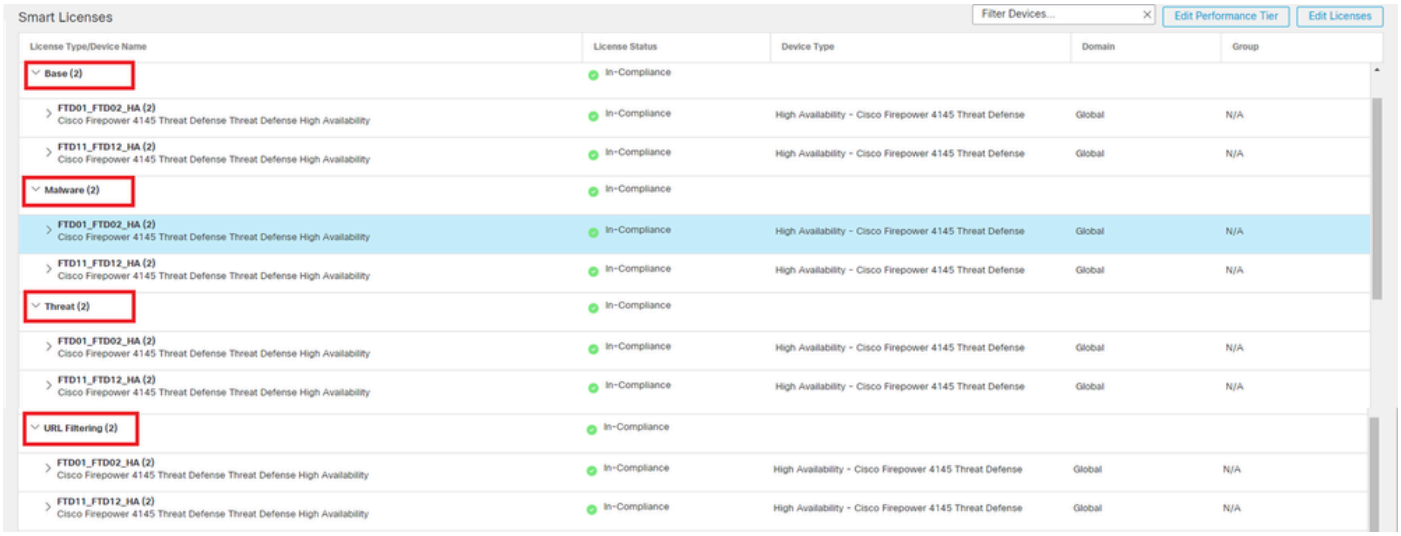
Esta tabla muestra cómo se consumen las licencias en este documento.

FPR01	Instancia01	Básico, filtrado de URL, malware y amenazas
	Instancia02	Básico, filtrado de URL, malware y amenazas
FPR02	Instancia01	Básico, filtrado de URL, malware y amenazas
	Instancia02	Básico, filtrado de URL, malware y amenazas

Número total de licencias

Base	Filtrado de URL	Malware	Amenaza
2	2	2	2

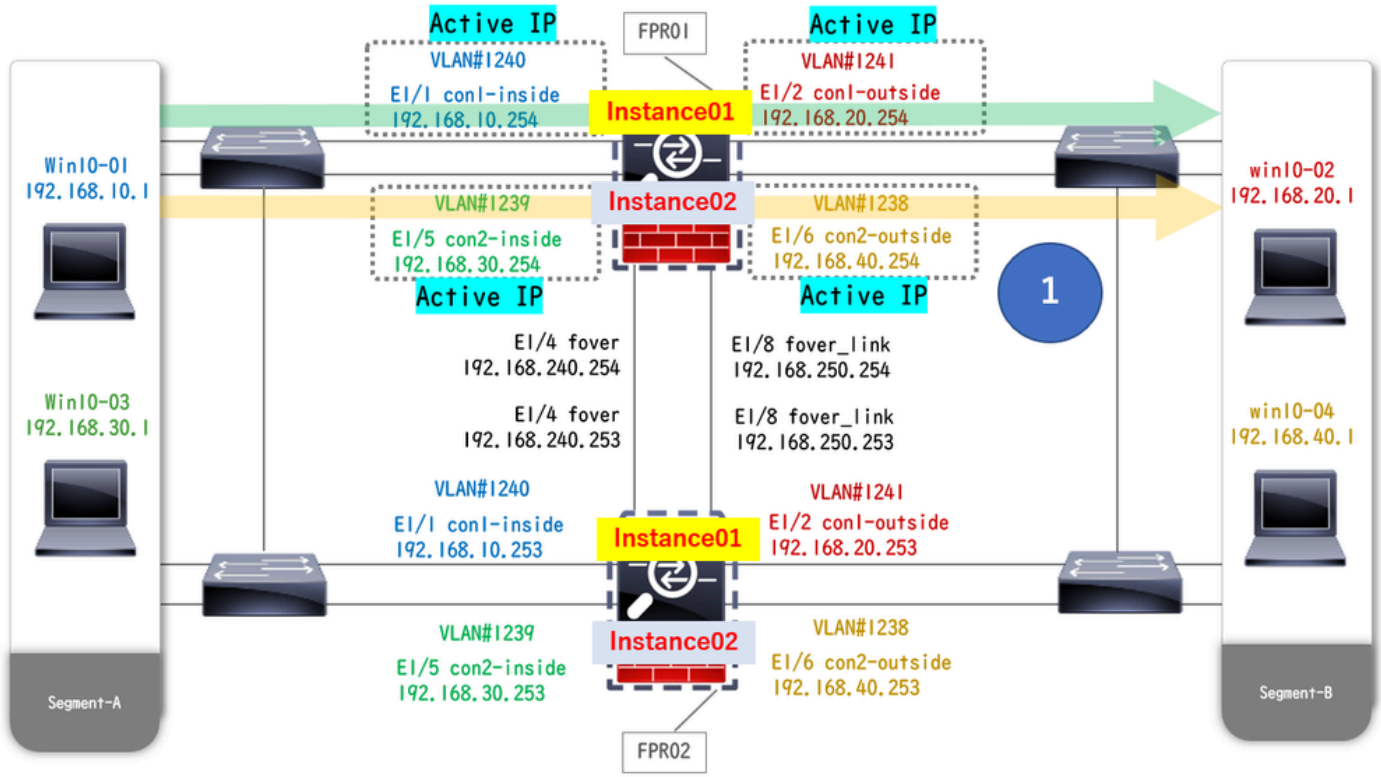
Confirme el número de licencias consumidas en la GUI de FMC.



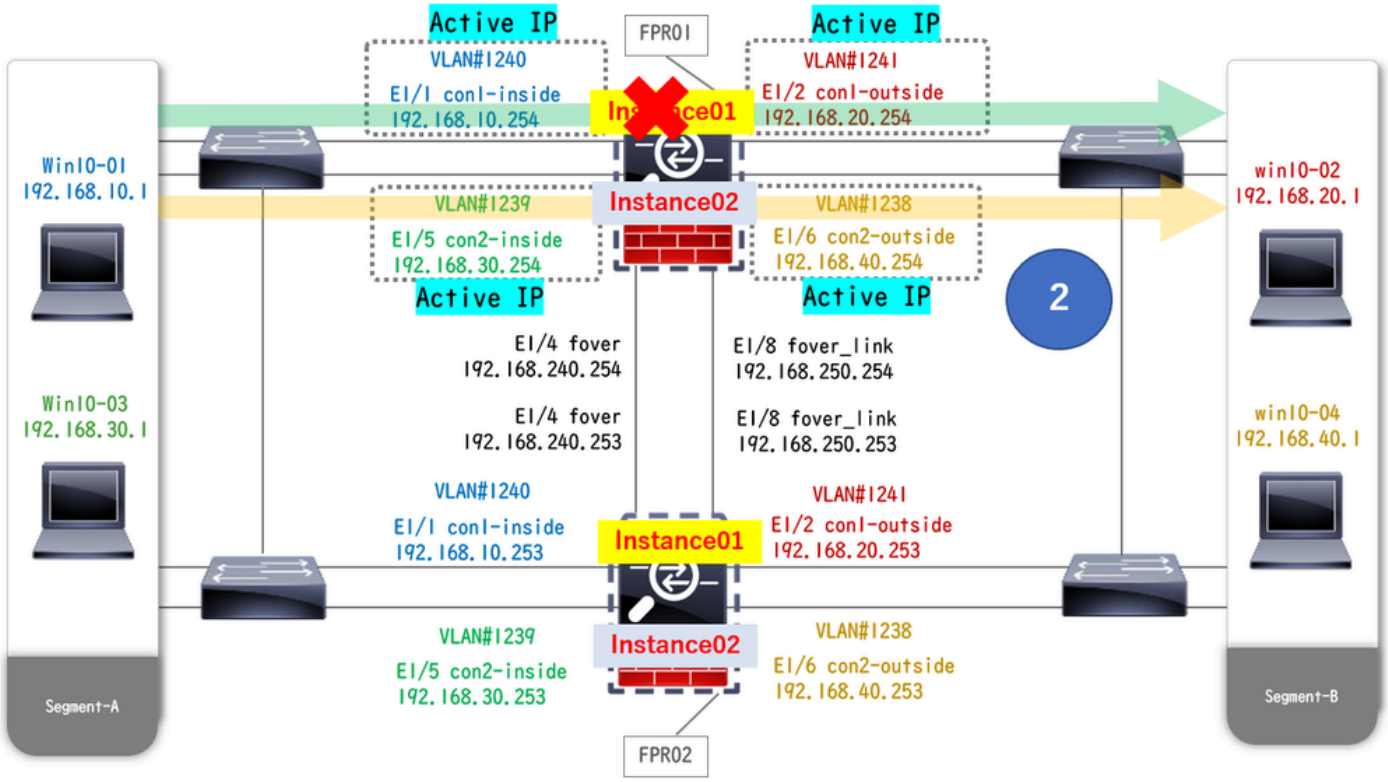
Confirmar licencias consumidas

Verificación

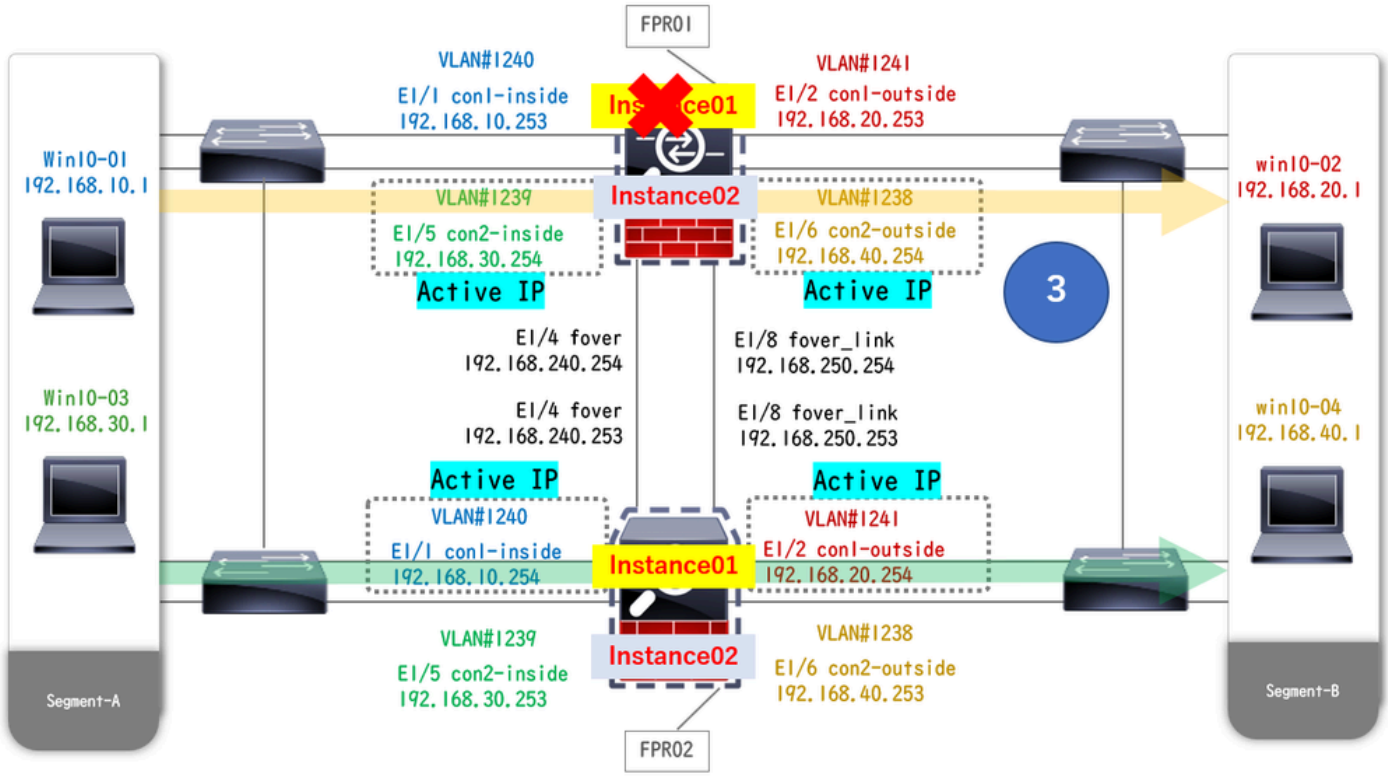
Cuando se produce un crash en FTD1_FTD01 (Instancia Primaria01), se dispara el failover de la Instancia01 y las interfaces de datos en el lado en espera se hacen cargo de la dirección IP/MAC de la Interfaz Activa original, asegurando que el tráfico (conexión FTP en este documento) sea pasado continuamente por Firepower.



Antes del desperfecto



Durante el desperfecto



Failover Activado

Paso 1. Inicie la conexión FTP de Win10-01 a Win10-02.

Paso 2. El show conn comando Run para confirmar la conexión FTP se ha establecido en Instance01.

<#root>

// Confirm the connection in Instance01 of FPR01 >

```
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1
```

Paso 3. Inicie la conexión FTP de Win10-03 a Win10-04.

Paso 4. El **show conn** comando Run para confirmar la conexión FTP se ha establecido en Instance02.

<#root>

// Confirm the connection in Instance02 of FPR01 >

```
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1
```

Paso 5. Ejecute connect ftd FTD01 y system support diagnostic-cli el comando para entrar en la CLI de ASA. Ejecute enable y el **crashinfo force watchdog** comando para forzar la caída de la Instancia01 en la unidad Primaria/Activa.

<#root>

Firepower-module1>

```
connect ftd FTD01
 >
system support diagnostic-cli
 FTD01>
enable
 Password: FTD01# FTD01#
crashinfo force watchdog
 reboot. Do you wish to proceed? [confirm]:
```

Paso 6. La conmutación por fallo se produce en Instance01 y la conexión FTP no se interrumpe. Ejecute show failover y show conn el comando para confirmar el estado de Instance01 en FPR02.

<#root>

>

show failover

**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (**

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

Paso 7. El desperfecto ocurrido en Instance01 no tuvo ningún efecto en Instance02. Ejecute show failover y show conn el comando para confirmar el estado de Instance02.

<#root>

>

show failover

**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1**

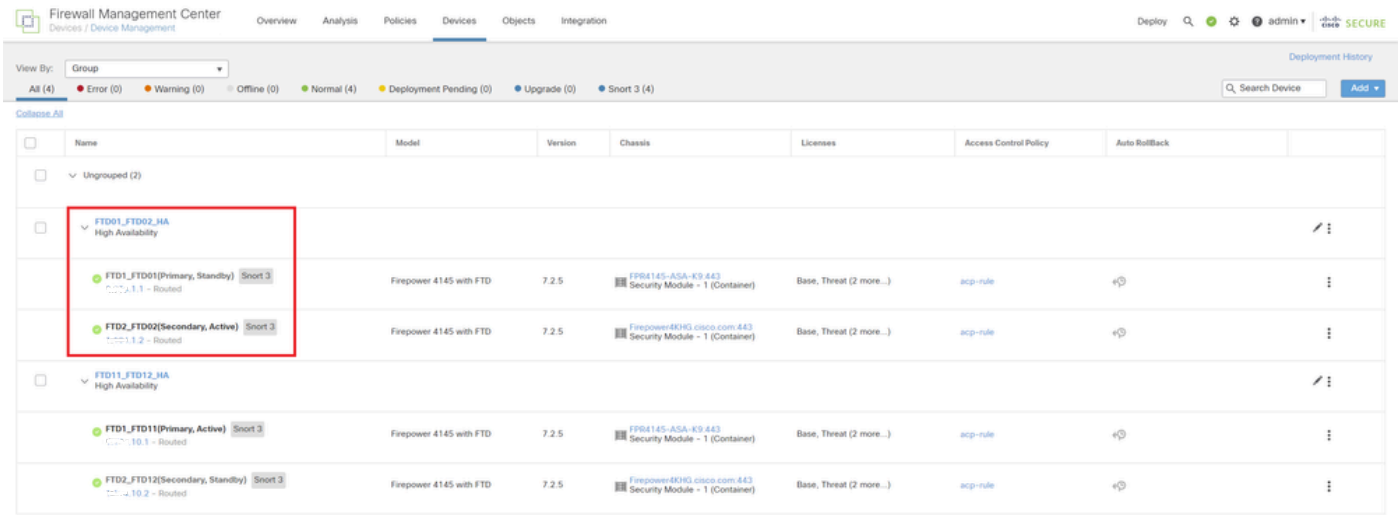
show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

Paso 8. Vaya a **Devices** > **All** en FMC. Confirme el estado de HA.

·**FTD1_FTD01: Principal, En espera**

·**FTD2_FTD02: Secundario, Activo**

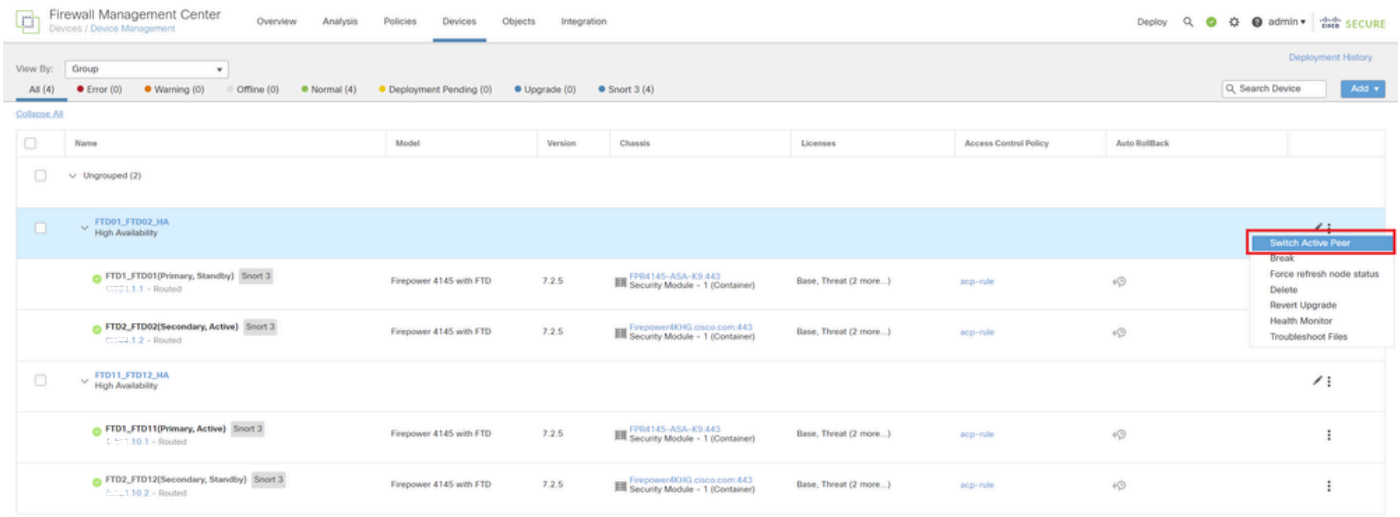


Confirmar estado de HA

Paso 9. (Opcional)Después de que el Instance01 de FPR01 vuelva a la normalidad, puede cambiar manualmente el estado de HA. Esto se puede

realizar mediante la GUI de FMC o la CLI de FRP.

En FMC, navegue hasta **Devices** > **All**. Haga clic en **Switch Active Peer** para cambiar el estado de HA para **FTD01_FTD02_HA**.



Estado de HA del switch

En Firepower CLI, ejecute connect ftd FTD01 y system support diagnostic-cli el comando para entrar en ASA CLI. Ejecute enable el **failover active** comando y cambie el HA para FTD01_FTD02_HA.

```
<#root>

Firepower-module1>

connect ftd FTD01

 >

system support diagnostic-cli

 Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of availab

enable

 firepower#

failover active
```

Troubleshoot

Para validar el estado de failover, ejecute **show failover** y **show failover history** ordene.

```
<#root>

>

show failover

 Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
```

```
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1
>
show failover history
 ========================================================================== From State To State Reason =
```

Ejecute el comando debug fover <option> para habilitar el registro de debug de failover.

<#root>

>

```
debug fover
 auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution c
```

Referencia

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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).