Configuración de alta disponibilidad de FTD mediante FDM

Contenido

Introducción

Este documento describe cómo configurar un par de alta disponibilidad (HA) activo/en espera de defensa frente a amenazas de firewall (FTD) gestionado localmente.

Prerequisites

Requirements

Se recomienda tener conocimiento de estos temas:

- Configuración inicial de Cisco Secure Firewall Threat Defence mediante GUI o shell.

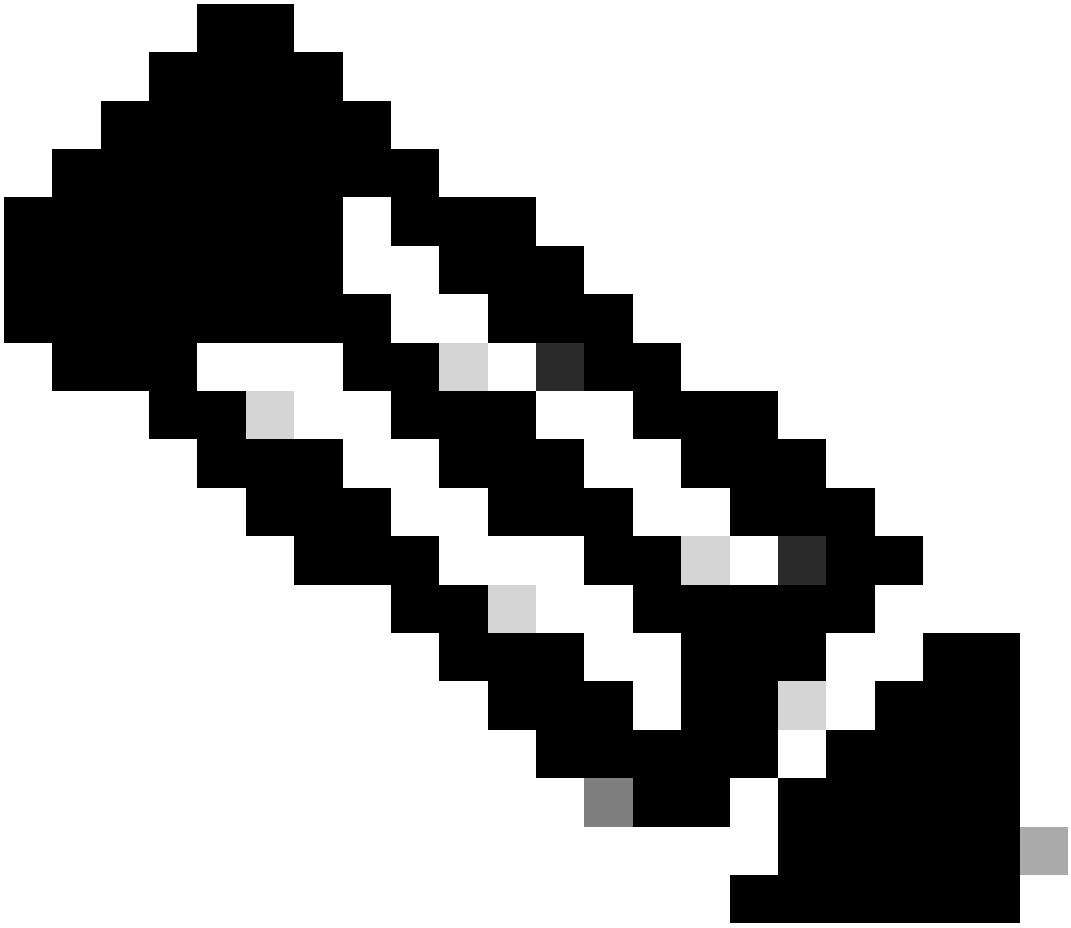
Componentes Utilizados

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

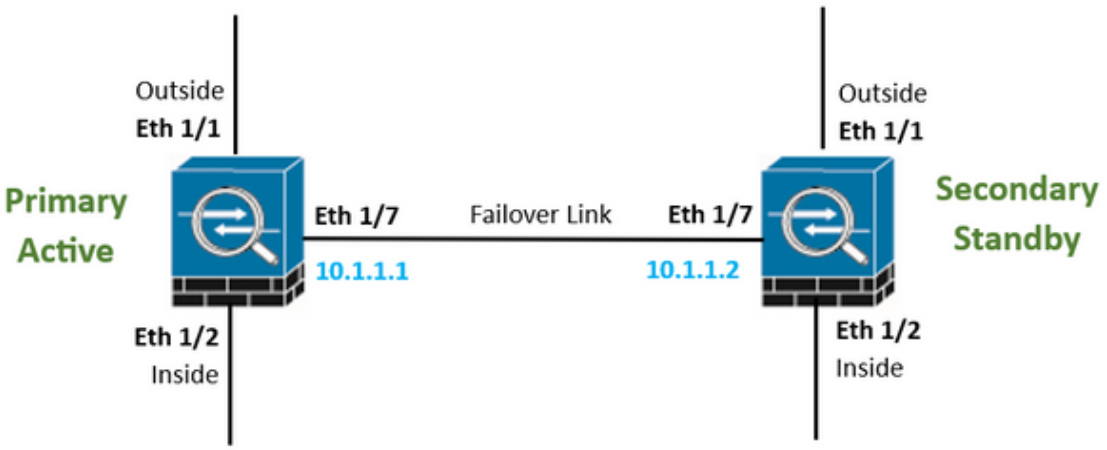
- FPR2110 versión 7.2.5 administrada localmente por Firepower Device Manager (FDM)

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 de red



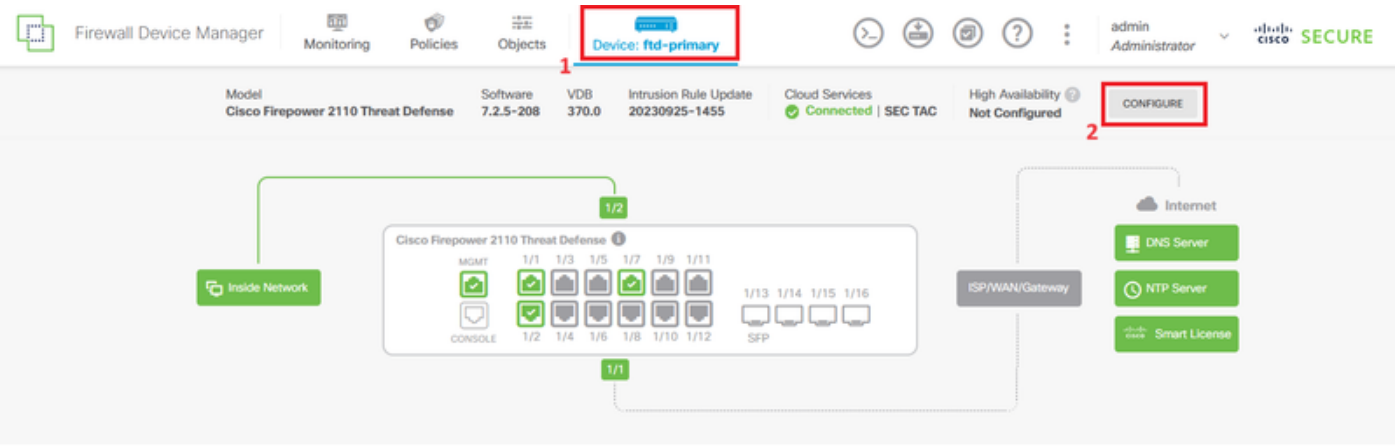
Nota: El ejemplo descrito en este documento es uno de los varios diseños de red recomendados. Refiérase a la guía de configuración Evitar Failover Interrumpido y Enlaces de Datos para obtener más opciones.



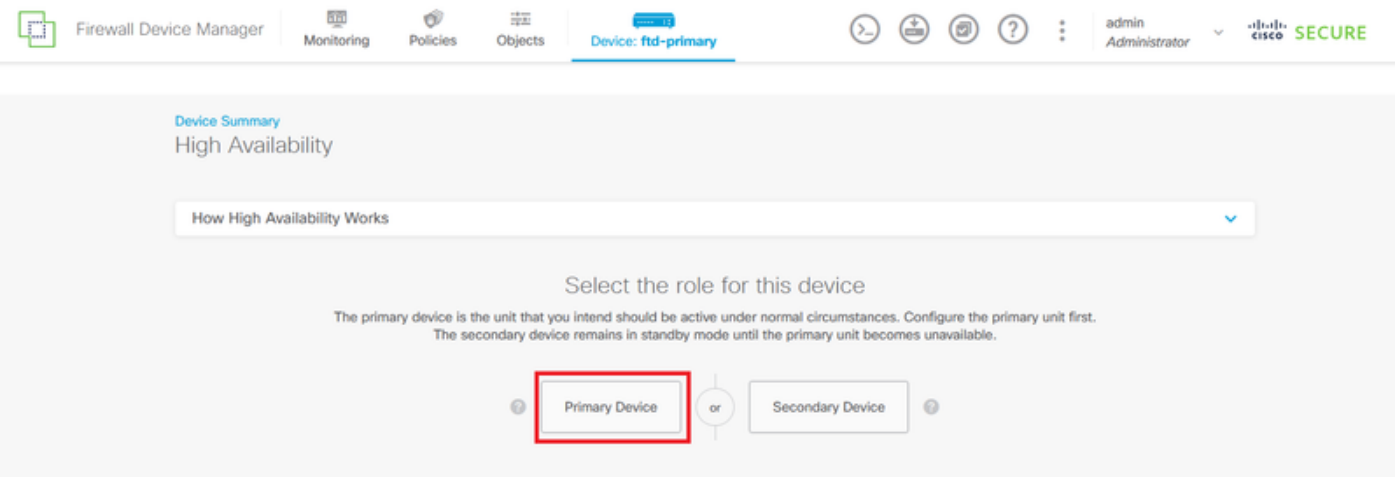
Configurar

Configuración de la unidad principal para alta disponibilidad

Paso 1. Haga clic en Device y presione el botón Configure ubicado en la esquina superior derecha, junto al estado High Availability.



Paso 2. En la página Alta disponibilidad, haga clic en el cuadro Dispositivo principal.



Paso 3. Configure las propiedades Failover Link.

Seleccione la interfaz que ha conectado directamente a su firewall secundario y establezca la dirección IP primaria y secundaria, así como la máscara de red de subred.

Marque la casilla de verificación Use the same interface as the Failover Link para el Stateful Failover Link.

Desactive el cuadro Clave de cifrado IPSec y haga clic en Activar HA para guardar los cambios.

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD

FAILOVER LINK

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.10.1

Secondary IP

10.1.1.2

e.g. 192.168.10.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

STATEFUL FAILOVER LINK

Use the same interface as the Failover Link

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.11.1

Secondary IP

10.1.1.2

e.g. 192.168.11.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

IPSec Encryption Key *(optional)*

For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA.
You will need to manually enter the key when you configure HA on the peer device.

IMPORTANT

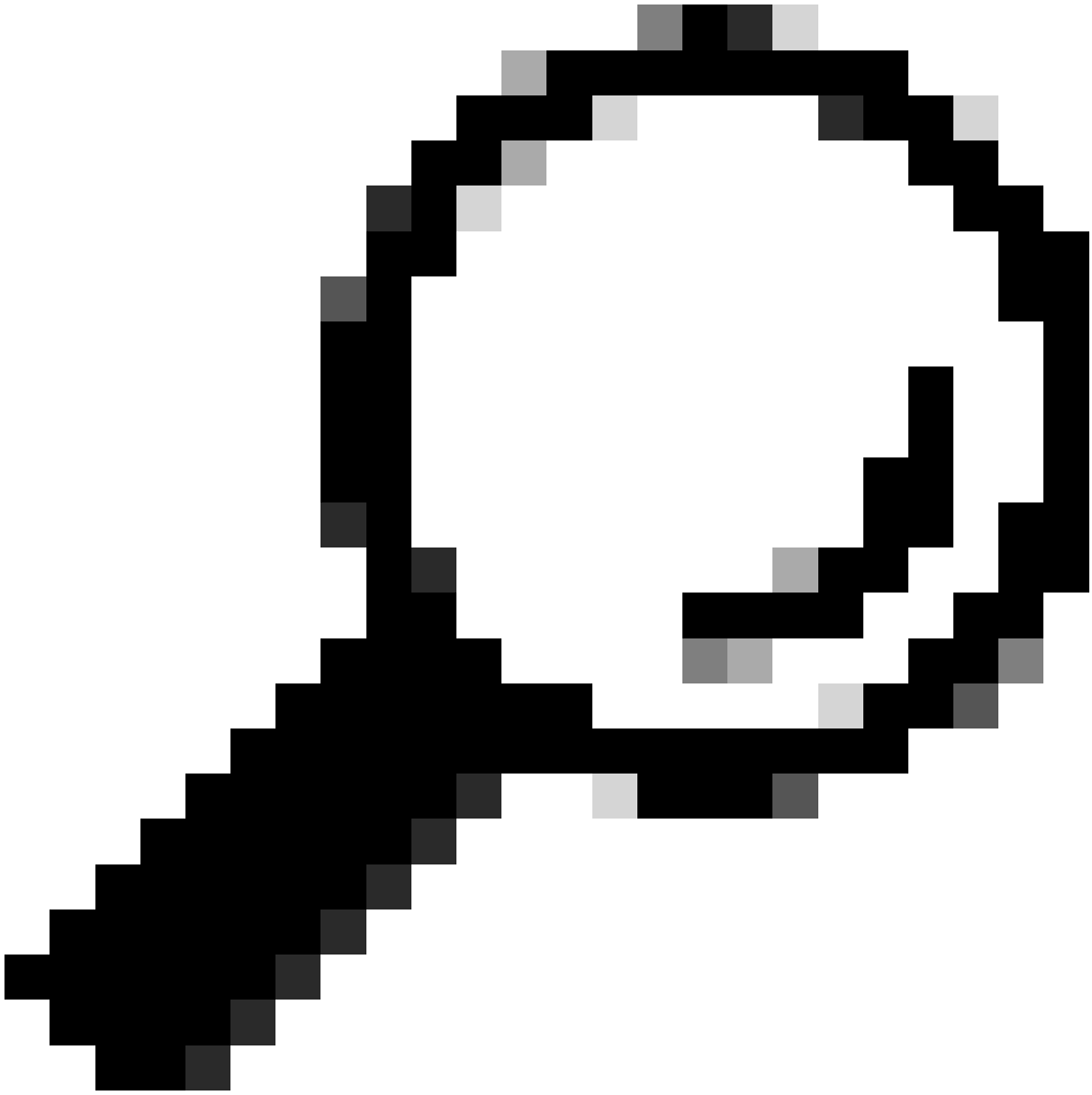
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

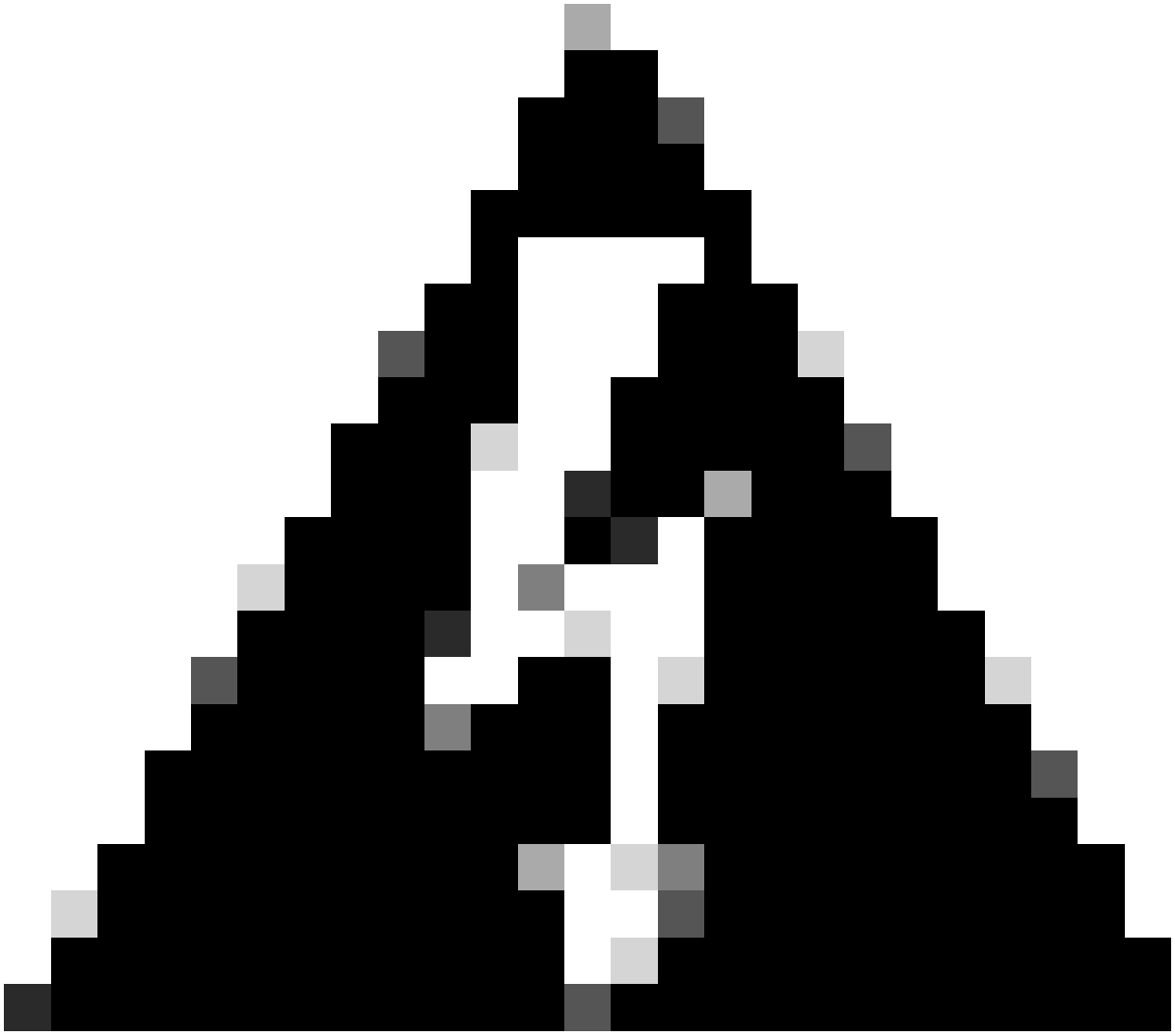
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

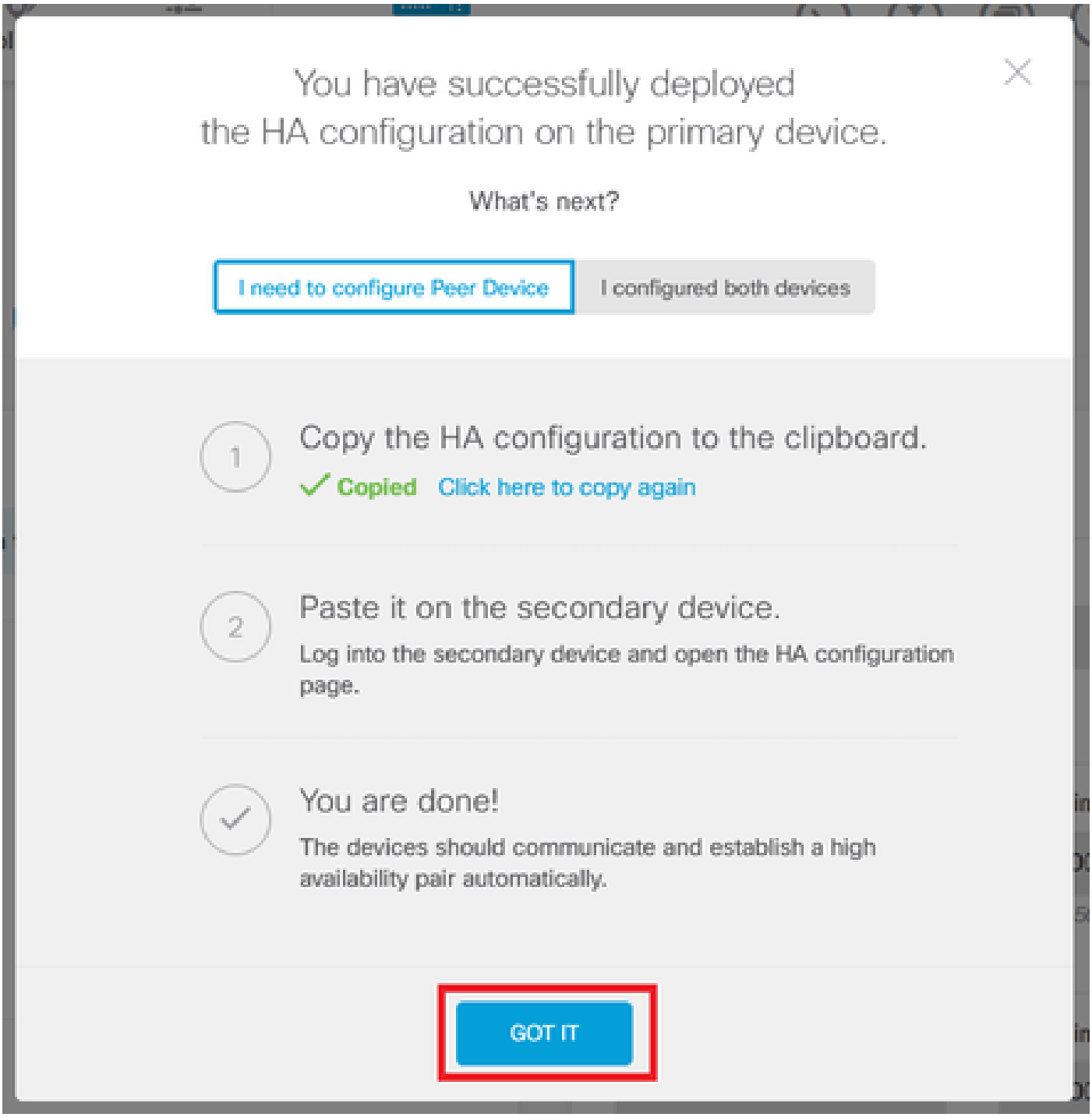


Sugerencia: utilice una pequeña subred de máscaras, dedicada únicamente al tráfico de conmutación por fallo para evitar en la medida de lo posible las infracciones de seguridad o los problemas de red.



Advertencia: el sistema implementa inmediatamente la configuración en el dispositivo. No es necesario iniciar un trabajo de implementación. Si no ve ningún mensaje que indique que la configuración se ha guardado y la implementación está en curso, desplácese a la parte superior de la página para ver los mensajes de error. La configuración también se copia en el portapapeles. Puede utilizar la copia para configurar rápidamente la unidad secundaria. Para mayor seguridad, la clave de cifrado (si la define) no se incluye en la copia del portapapeles.

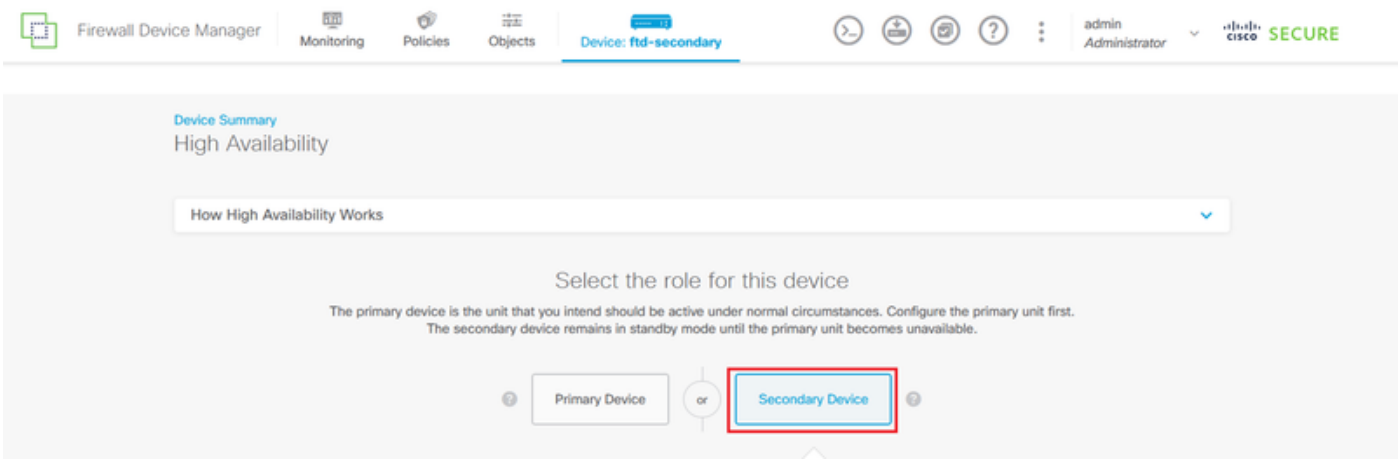
Paso 4. Una vez finalizada la configuración, aparece un mensaje que explica los siguientes pasos. Haga clic en Got It después de leer la información.



Configuración de la unidad secundaria para alta disponibilidad

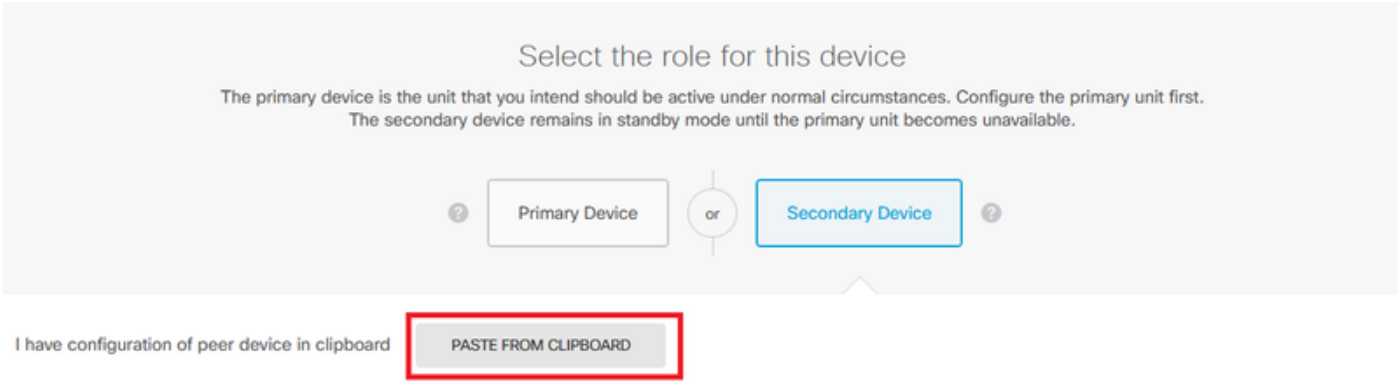
Paso 1. Haga clic en Device y presione el botón Configure ubicado en la esquina superior derecha, junto al estado High Availability.

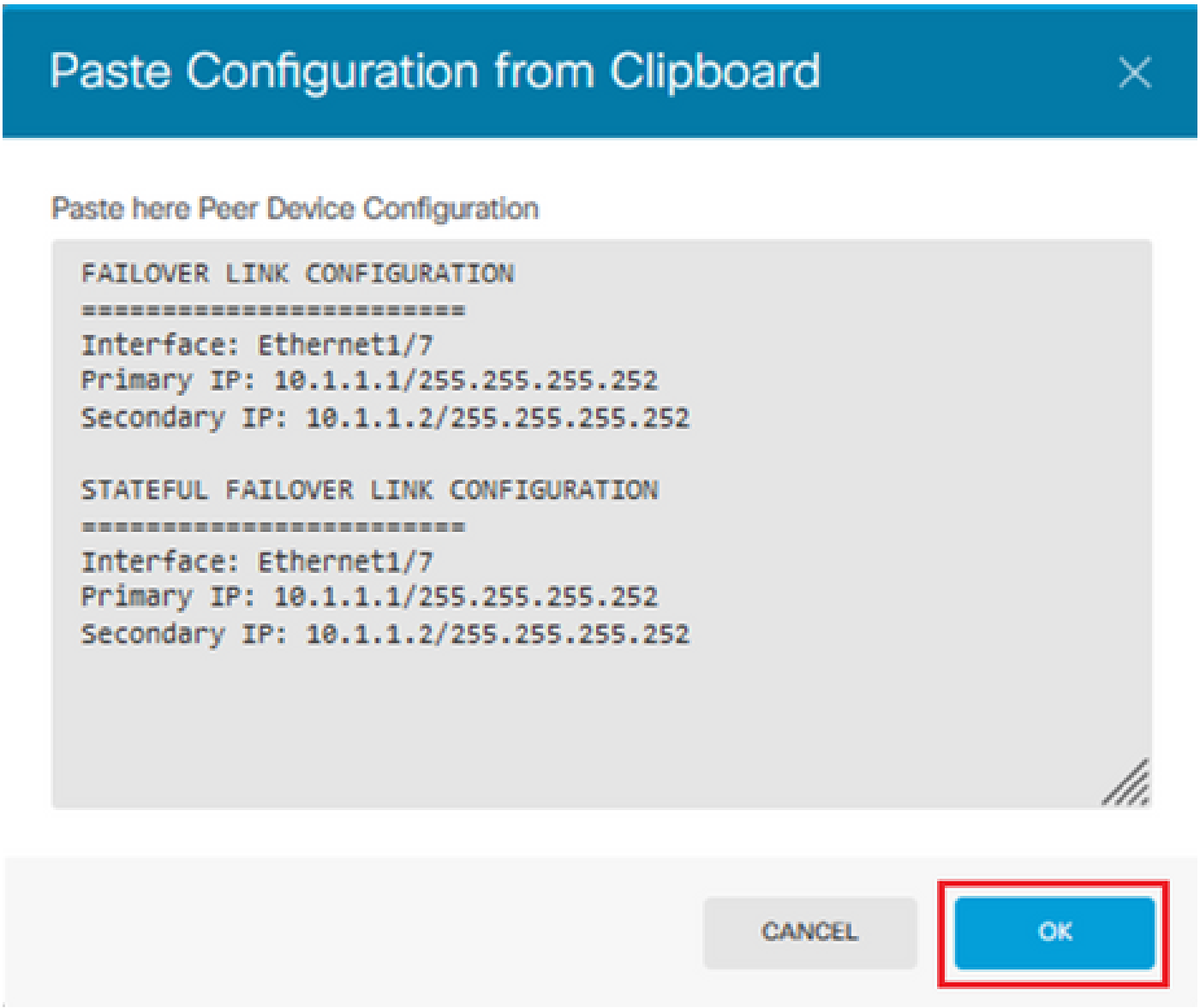
Paso 2. En la página Alta disponibilidad, haga clic en el cuadro Dispositivo secundario.



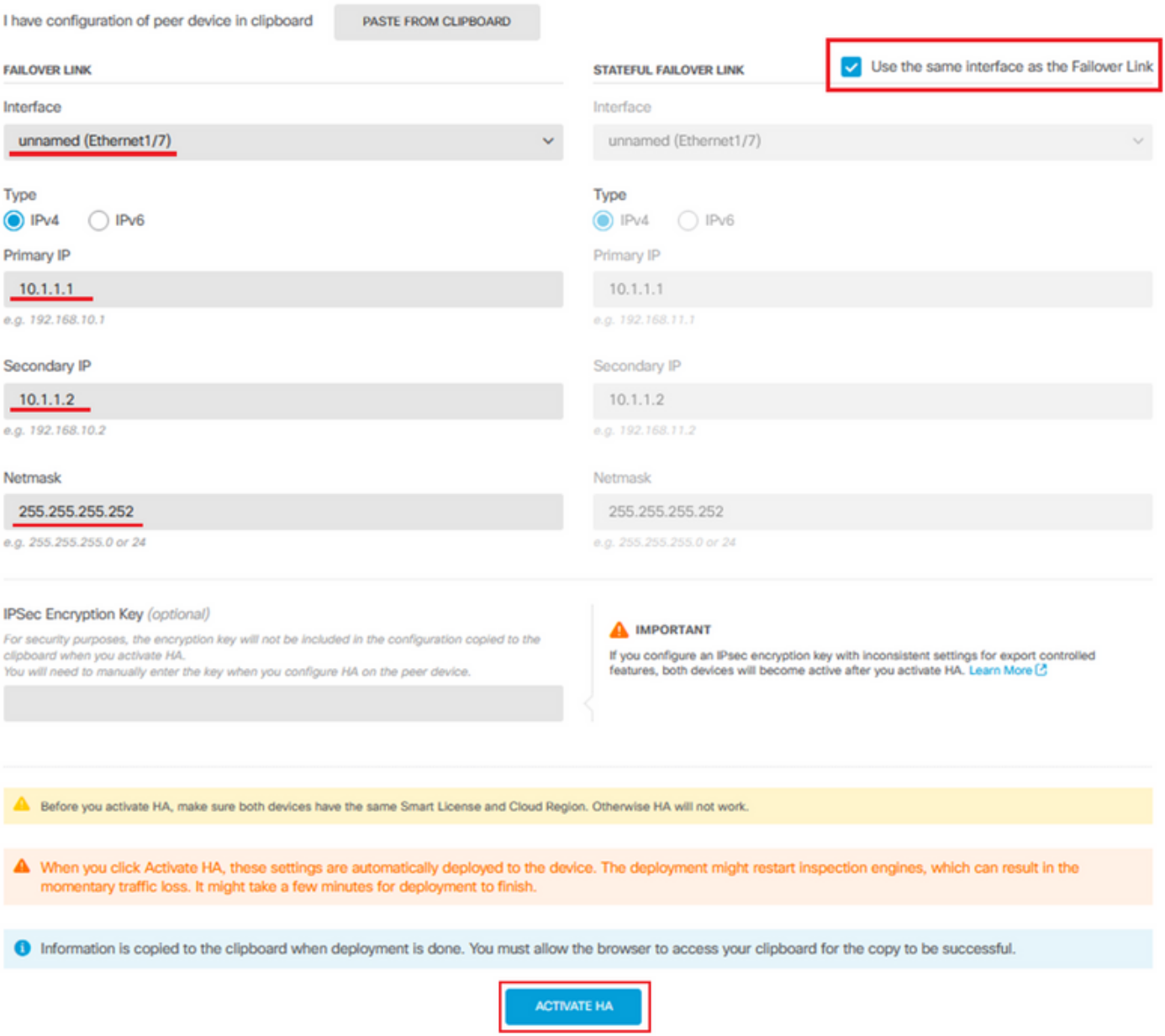
Paso 3. Configure las propiedades Failover Link. Puede pegar los parámetros almacenados en el portapapeles después de configurar el FTD principal, o puede continuar manualmente.

Paso 3.1. Para pegar desde el portapapeles simplemente haga clic en el botón Pegar desde el portapapeles, pegue la configuración (presione las teclas Ctrl+v simultáneamente) y haga clic en Aceptar.

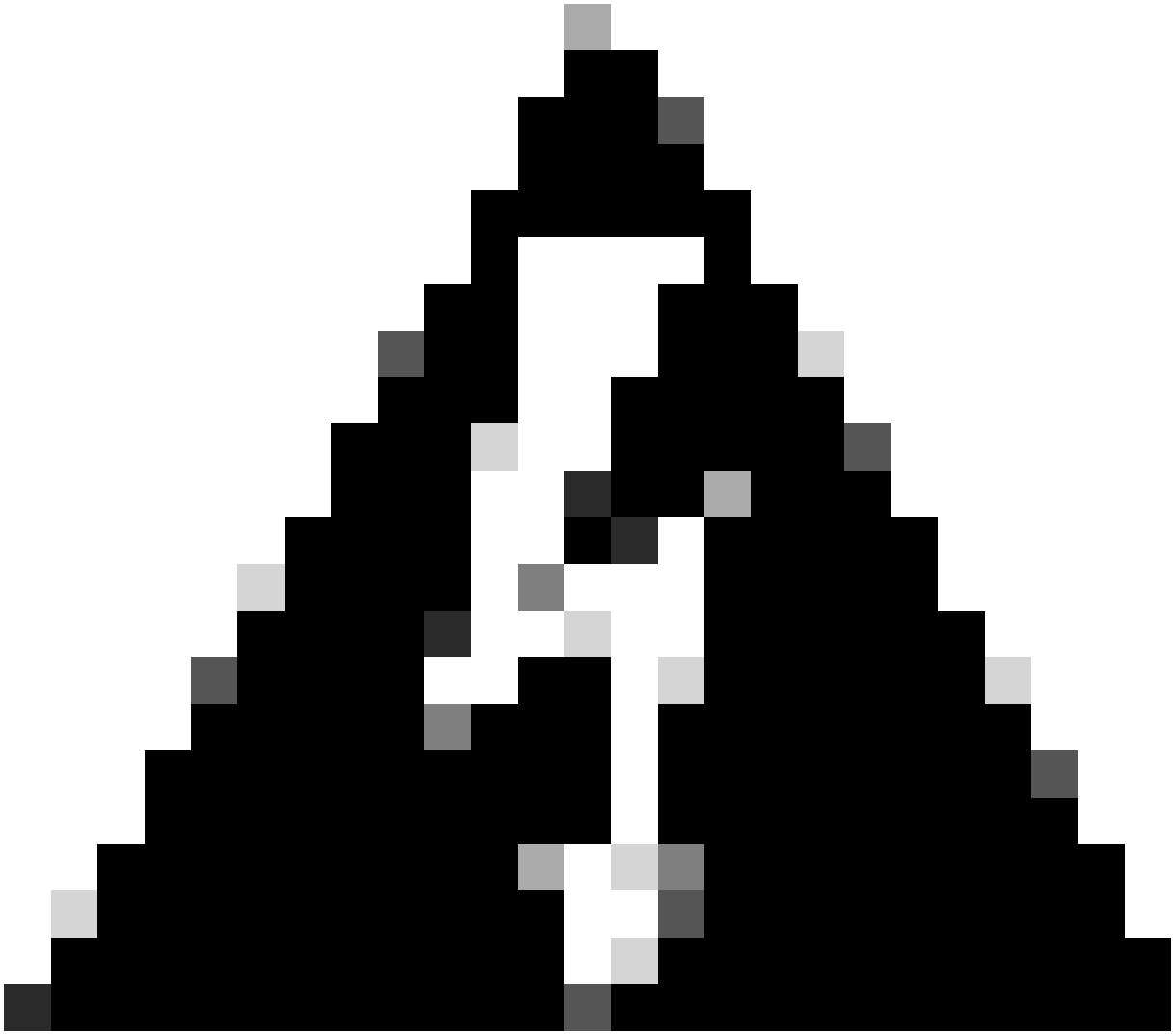




Paso 3.2. Para continuar manualmente, seleccione la interfaz que ha conectado directamente a su firewall secundario y establezca la dirección IP primaria y secundaria, así como la máscara de red de subred. Marque la casilla de verificación Use the same interface as the Failover Link para el Stateful Failover Link.

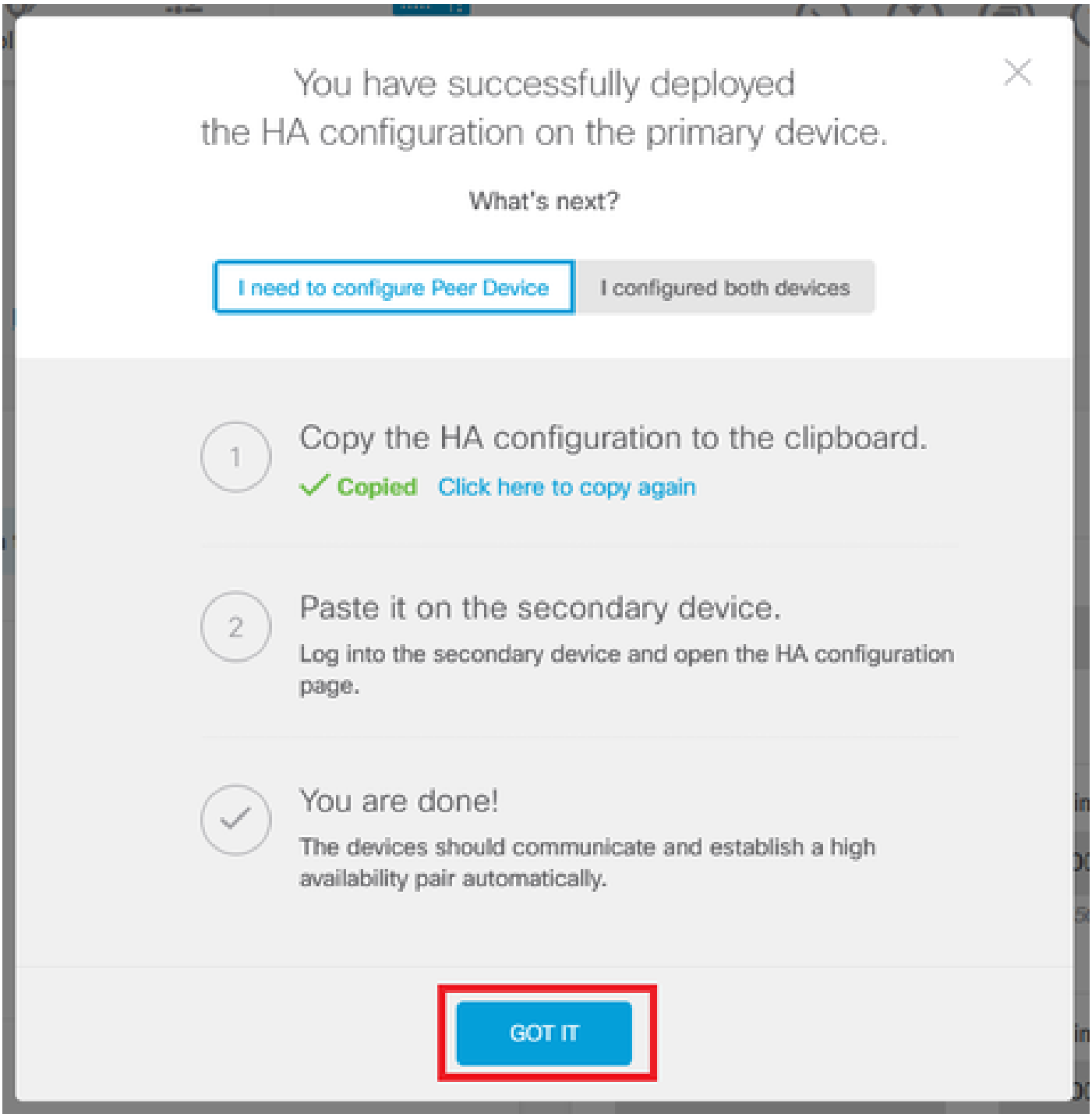


Paso 4. Desactive el cuadro Clave de cifrado IPSec y haga clic en Activar HA para guardar los cambios.



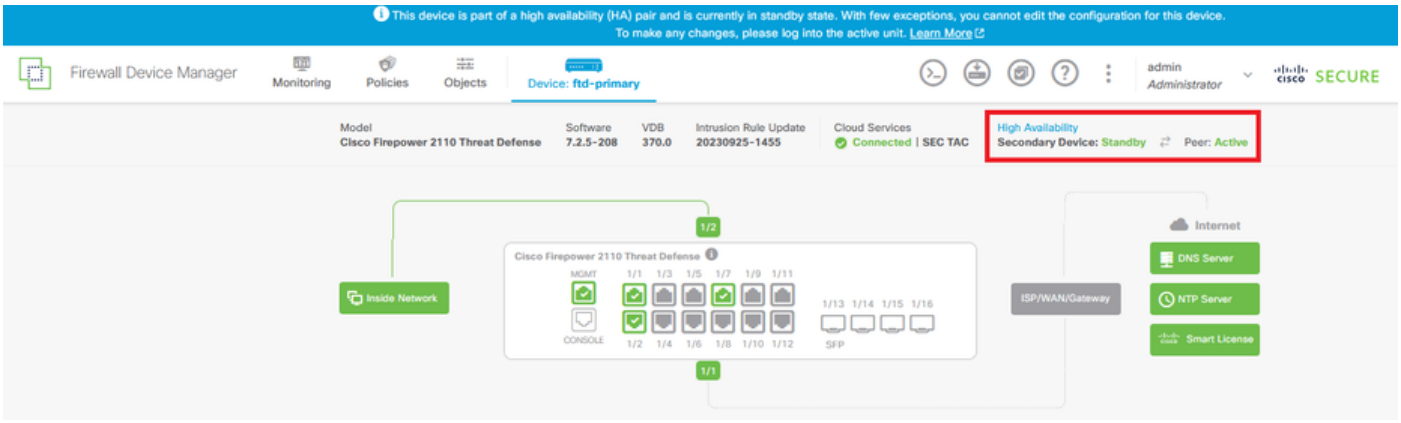
Advertencia: el sistema implementa inmediatamente la configuración en el dispositivo. No es necesario iniciar un trabajo de implementación. Si no ve ningún mensaje que indique que la configuración se ha guardado y la implementación está en curso, desplácese a la parte superior de la página para ver los mensajes de error.

Paso 5. Una vez finalizada la configuración, aparece un mensaje en el que se explican los siguientes pasos que debe realizar. Haga clic en Got It después de leer la información.

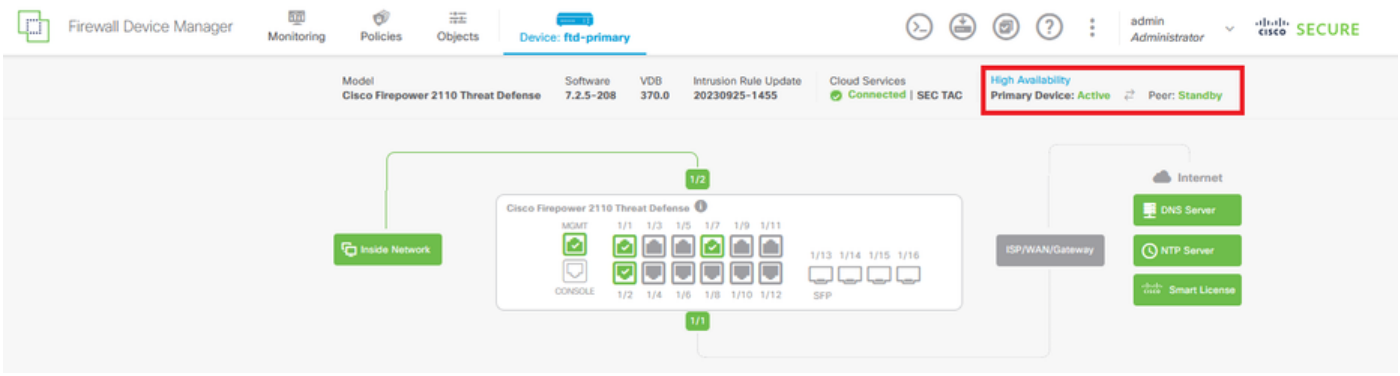


Verificación

- En este momento, el estado del dispositivo indica que se trata del dispositivo secundario de la página Alta disponibilidad. Si la unión con el dispositivo principal se realizó correctamente, el dispositivo comienza a sincronizarse con el dispositivo principal y, finalmente, el modo cambia a En espera y el par a Activo.



- El FTD principal debe mostrar también el estado Alta disponibilidad, pero como Activo y Par: En espera.



- Abra una sesión SSH al FTD primario y ejecute el comando show running-config failover para verificar la configuración.

```
> show running-config failover
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/7
failover replication http
failover link failover-link Ethernet1/7
failover interface ip failover-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

- Valide el estado actual del dispositivo con el comando show failover state.

```
> show failover state

              State          Last Failure Reason      Date/Time
This host  -  Primary
              Active         None
Other host -  Secondary
              Standby Ready  None

====Configuration State===
====Communication State===
        Mac set

>
```

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).