

# Configuración del administrador de dispositivos de firewall seguro en alta disponibilidad

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Tarea 1. Verificar las condiciones](#)

[Tarea 2. Configuración del administrador de dispositivos de firewall seguro en alta disponibilidad](#)

[Diagrama de la red](#)

[Habilitación de la alta disponibilidad en el administrador de dispositivos de firewall seguro en la unidad principal](#)

[Habilitación de la alta disponibilidad en el administrador de dispositivos de firewall seguro en la unidad secundaria](#)

[Complete La Configuración De Las Interfaces](#)

[Tarea 3. Verificar alta disponibilidad de FDM](#)

[Tarea 4. Cambiar los roles de conmutación por error](#)

[Tarea 5. Suspensión o reanudación de alta disponibilidad](#)

[Tarea 6. Alta disponibilidad rompedora](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar y verificar la alta disponibilidad (HA) del administrador de dispositivos de firewall seguro (FDM) en los dispositivos de firewall seguro.

## Prerequisites

## Requirements

## Componentes Utilizados

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

- 2 dispositivos de seguridad Cisco Secure Firewall 2100
- Ejecución de FDM versión 7.0.5 (compilación 72)

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.

## Tarea 1. Verificar las condiciones

Tarea requerida:

Verifique que ambos appliances de FDM cumplan los requisitos de la nota y se puedan configurar como

unidades de HA.

Solución:

Paso 1. Conéctese a la IP de administración del dispositivo mediante SSH y verifique el hardware del módulo.

Verifique con el comando **show version** la versión de hardware y software del dispositivo primario:

```
> show version
-----[ FPR2130-1 ]-----
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6197946e-2747-11ee-9b20-ead7c72f2631
VDB version : 338
-----
```

Verifique la versión del hardware y software del dispositivo secundario:

```
> show version
-----[ FPR2130-2 ]-----
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6ba86648-2749-11ee-b7c9-c9e434a6c9ab
VDB version : 338
-----
```

## **Tarea 2. Configuración del administrador de dispositivos de firewall seguro en alta disponibilidad**

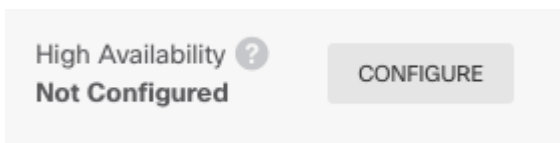
### **Diagrama de la red**

Configure la alta disponibilidad (HA) activa/en espera según este diagrama:

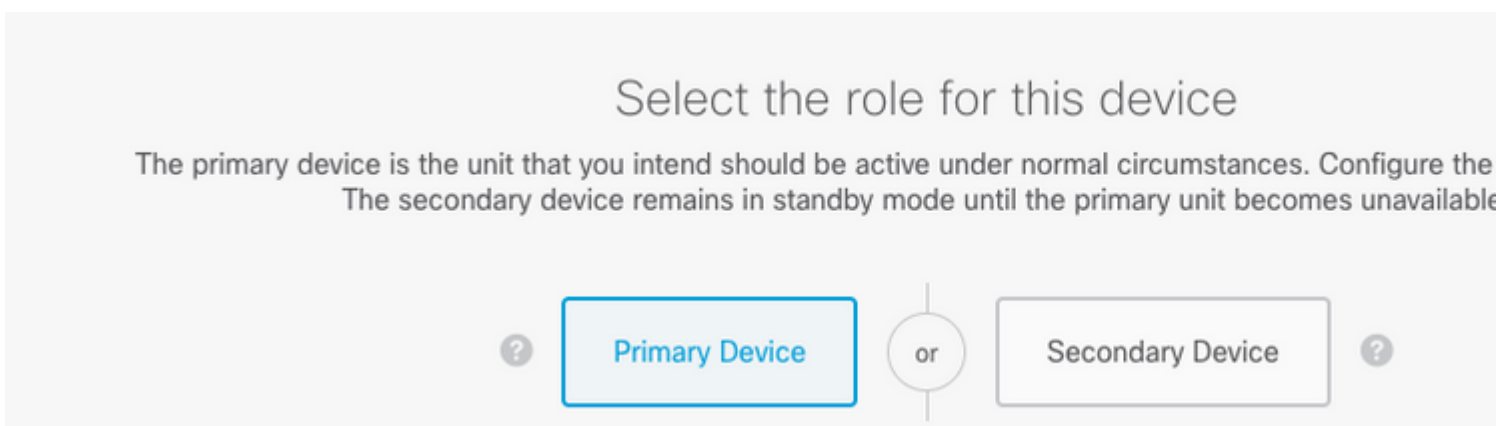


## Habilitación de la alta disponibilidad en el administrador de dispositivos de firewall seguro en la unidad principal

Paso 1. Para configurar la conmutación por fallas de FDM, navegue hasta **Device** y haga clic en **Configure** junto al grupo **High Availability**:



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



**Advertencia:** Asegúrese de seleccionar la unidad correcta como la unidad **principal**. Todas las configuraciones de la unidad principal seleccionada se replican en la unidad FTD secundaria seleccionada. Como resultado de la replicación, la configuración actual en la unidad secundaria puede ser **reemplazada**.

Paso 3. Configure los parámetros del link de failover y del link de estado:

En este ejemplo, el link de estado tiene la misma configuración que el link de failover.

FAILOVER LINK	STATEFUL FAILOVER LINK <input checked="" type="checkbox"/>
<b>Interface</b> unnamed (Ethernet1/1) <input type="text"/>	<b>Interface</b> unnamed (Ethernet1/1) <input type="text"/>
<b>Type</b> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	<b>Type</b> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Primary IP</b> 1.1.1.1 <input type="text"/> <small>e.g. 192.168.10.1</small>	<b>Primary IP</b> 1.1.1.1 <input type="text"/> <small>e.g. 192.168.11.1</small>
<b>Secondary IP</b> 1.1.1.2 <input type="text"/> <small>e.g. 192.168.10.2</small>	<b>Secondary IP</b> 1.1.1.2 <input type="text"/> <small>e.g. 192.168.11.2</small>
<b>Netmask</b> 255.255.255.252 <input type="text"/> <small>e.g. 255.255.255.0 or 24</small>	<b>Netmask</b> 255.255.255.252 <input type="text"/> <small>e.g. 255.255.255.0 or 24</small>
<b>IPSec Encryption Key (optional)</b> <small>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.</small> <input type="text"/>	
<b>IMPORTANT</b> If you configure an IPsec encryption key with in features, both devices will become active after	

Paso 4. Haga clic en Activar HA

Paso 5. Copie la configuración de HA en el portapapeles del mensaje de confirmación para pegarla en la unidad secundaria.

✕

You have successfully deployed  
the HA configuration on the primary device.

What's next?

I need to configure Peer DeviceI configured both devices

- 1

Copy the HA configuration to the clipboard.

✓ Copied [Click here to copy again](#)
- 2

Paste it on the secondary device.

Log into the secondary device and open the HA configuration page.
- ✓

You are done!

The devices should communicate and establish a high availability pair automatically.

GOT IT

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 no se incluye en la copia del portapapeles.

En este momento, debe estar en la página Alta disponibilidad y el estado del dispositivo debe ser "Negociando". El estado debe pasar a Activo incluso antes de configurar el par, que debe aparecer como Fallido hasta que lo configure.

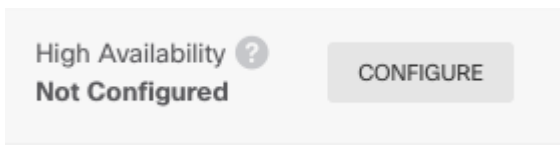
High Availability

Primary Device: Active ↻ Peer: ✕ Failed

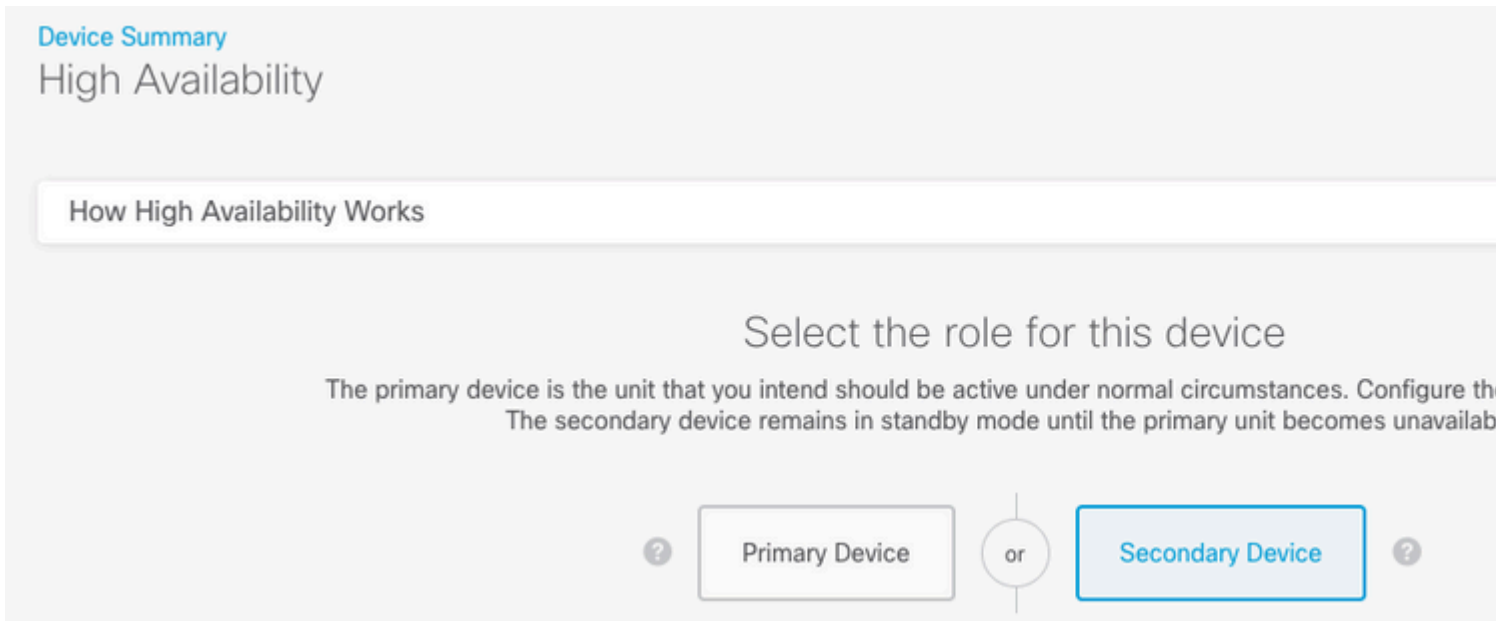
## Habilitación de la alta disponibilidad en el administrador de dispositivos de firewall seguro en la unidad secundaria

Después de configurar el dispositivo principal para la alta disponibilidad activa/en espera, debe configurar el dispositivo secundario. Inicie sesión en FDM en ese dispositivo y ejecute este procedimiento.

Paso 1. Para configurar la conmutación por fallas de FDM, navegue hasta **Device** y haga clic en **Configure** junto al **grupo High Availability**:

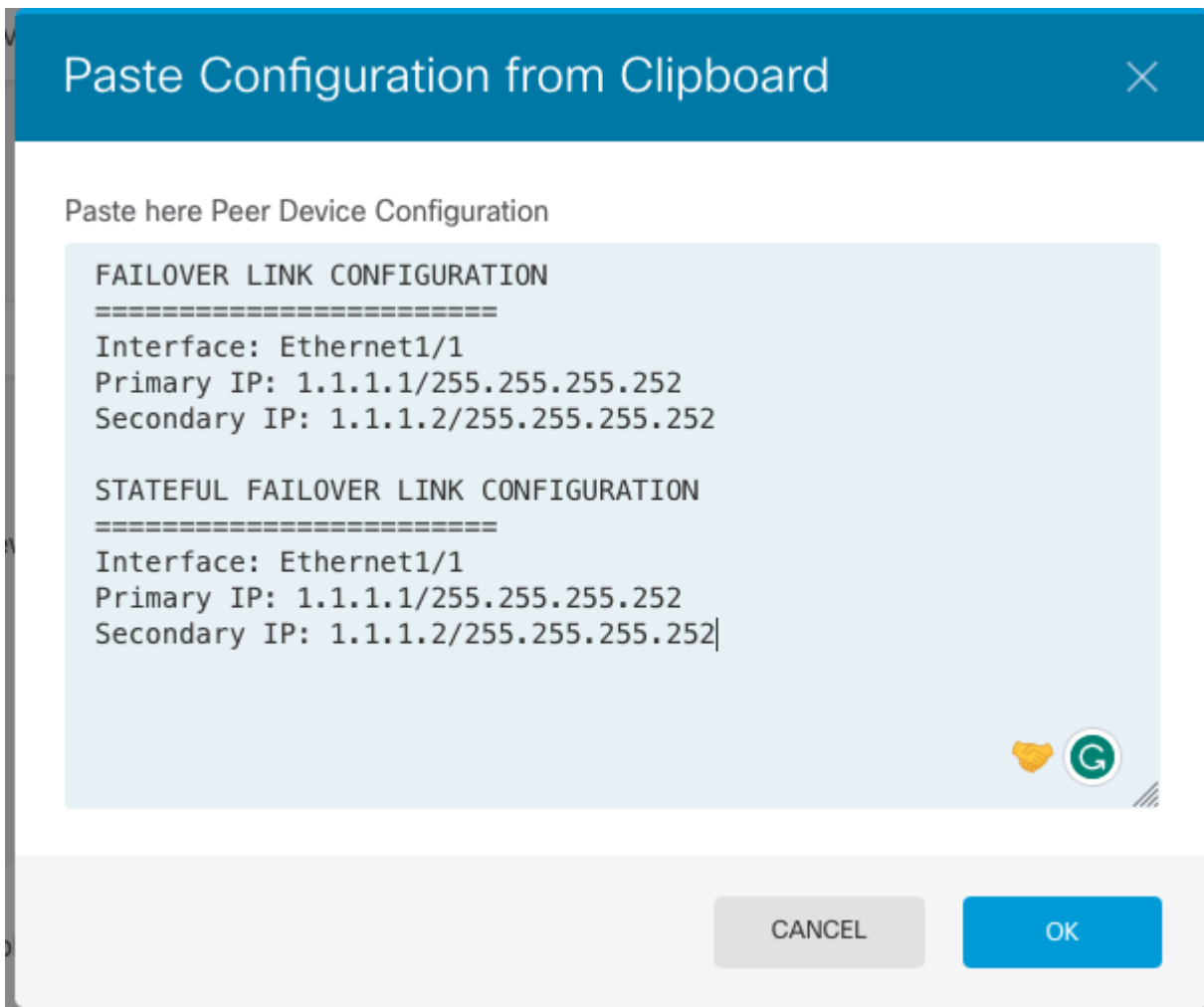


Paso 2. En la página Alta disponibilidad, haga clic en el cuadro Dispositivo secundario:



Paso 3. Elija una de estas opciones:

- Método sencillo: haga clic en el botón Pegar desde el portapapeles, pegue la configuración y haga clic en Aceptar. De este modo, se actualizan los campos con los valores adecuados, que puede comprobar a continuación.
- Método manual: configure los links de failover y stateful failover directamente. Introduzca exactamente los mismos parámetros en el dispositivo secundario que introdujo en el dispositivo principal.

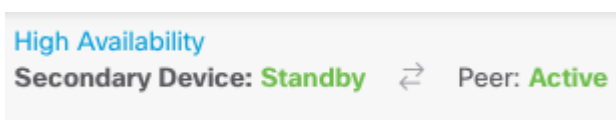


Paso 4. Haga clic en Activar HA

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.

Una vez finalizada la configuración, aparece un mensaje que indica que ha configurado HA. Haga clic en Got It para descartar el mensaje.

En este momento, debe encontrarse en la página High Availability y el estado de su dispositivo debe indicar que se trata del dispositivo secundario. Si la unión con el dispositivo principal se realizó correctamente, el dispositivo se sincroniza con el dispositivo principal y, finalmente, el modo debe estar en espera y el par debe estar activo.



## Complete La Configuración De Las Interfaces

Paso 1. Para configurar las interfaces de FDM, navegue hasta **Device** y haga clic en **View All Interfaces:**

## Interfaces

Connected

Enabled 2 of 17

[View All Interfaces](#)



Paso 2. Seleccione y edite la configuración de las interfaces como se muestra en las imágenes:

Interfaz ethernet 1/5:



# Ethernet1/5

## Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



*Most features work with named interfaces only, although some require unnamed interfaces.*

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

192.168.75.10

/

255.255.255.0

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

Standby IP Address and Subnet Mask

192.168.75.11

/

255.255.255.0

*e.g. 192.168.5.16*

CANCEL

OK

Интерфаз ethernet 1/6

Ethernet1/6
? ×

Edit Physical Interface

**Interface Name**

**Mode**

Routed
▼

**Status**

*Most features work with named interfaces only, although some require unnamed interfaces.*

**Description**

IPv4 Address
IPv6 Address
Advanced

**Type**

Static
▼

**IP Address and Subnet Mask**

192.168.76.10

/

255.255.255.0

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

**Standby IP Address and Subnet Mask**

192.168.76.11


/

255.255.255.0

*e.g. 192.168.5.16*

CANCEL

OK

Paso 3. Después de configurar los cambios, haga clic en **Pending Changes**  e **Impleméntelo ahora**.

### Tarea 3. Verificar alta disponibilidad de FDM

Tarea requerida:

Verifique la configuración de alta disponibilidad desde la GUI de FDM y desde la CLI de FDM.

Solución:

Paso 1. Navegue hasta **Device** y verifique la configuración de **High Availability**:

## Device Summary

# High Availability

### Primary Device

Current Device Mode: **Active** ⇌ Peer: **Standby**

[Failover History](#)

[Deployment History](#)

## High Availability Configuration

**i** Select and configure the peer device based on the following characteristics.

### GENERAL DEVICE INFORMATION

<b>Model</b>	Cisco Firepower 2130 Threat Defense
<b>Software</b>	7.0.5-72
<b>VDB</b>	338.0
<b>Intrusion Rule Update</b>	20210503-2107

### FAILOVER LINK

<b>Interface</b>	Ethernet1/1
<b>Type</b>	IPv4
<b>Primary IP/Netmask</b>	1.1.1.1/255.255.255.252
<b>Secondary IP/Netmask</b>	1.1.1.2/255.255.255.252

### STATEFUL FAILOVER LINK

*The same as the Failover Link.*

**IPSEC ENCRYPTION KEY: NOT CONFIGURED**

## Failover Criteria

### INTERFACE FAILURE THRESHOLD

Failure Criteria

Number of failed interfaces exceeds

### INTERFACE TIMING CONFIGURATION **i**

Poll Time

5000

500-15000 milliseconds

Hold Time

25000

5000-75000 milliseconds

### PEER TIMING CONFIGURATION **i**

Poll Time

1000

200-15000 milliseconds

Hold Time

15000

800-45000 milliseconds

SAVE

Paso 2. Conéctese a la CLI del dispositivo principal de FDM mediante SSH y realice la validación con el comando **show high-availability config**:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover-link Ethernet1/1 (up)
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 4 of 1293 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(4)200, Mate 9.16(4)200
Serial Number: Ours JAD231510ZT, Mate JAD2315110V
Last Failover at: 00:01:29 UTC Jul 25 2023
This host: Primary - Active
```

```

Active time: 4927 (sec)
slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  Interface eth2 (0.0.0.0): Link Down (Shutdown)
  Interface inside (192.168.75.10): No Link (Waiting)
  Interface outside (192.168.76.10): No Link (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  Interface eth2 (0.0.0.0): Link Down (Shutdown)
  Interface inside (192.168.75.11): No Link (Waiting)
  Interface outside (192.168.76.11): No Link (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)

```

#### Stateful Failover Logical Update Statistics

```

Link : failover-link Ethernet1/1 (up)
Stateful Obj    xmit      xerr      rcv        rerr
General         189        0         188        0
sys cmd         188        0         188        0
up time         0          0          0          0
RPC services    0          0          0          0
TCP conn        0          0          0          0
UDP conn        0          0          0          0
ARP tbl         0          0          0          0
Xlate_Timeout   0          0          0          0
IPv6 ND tbl     0          0          0          0
VPN IKEv1 SA    0          0          0          0
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA    0          0          0          0
VPN IKEv2 P2    0          0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0
SIP Session     0          0          0          0
SIP Tx 0        0          0          0          0
SIP Pinhole     0          0          0          0
Route Session   0          0          0          0
Router ID       0          0          0          0
User-Identity   1          0          0          0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
STS Table       0          0          0          0
Rule DB B-Sync  0          0          0          0
Rule DB P-Sync  0          0          0          0
Rule DB Delete  0          0          0          0

```

#### Logical Update Queue Information

```

          Cur      Max      Total
Recv Q:      0      10      188
Xmit Q:      0      11      957

```

Paso 3. Haga lo mismo en el dispositivo secundario.

Paso 4. Valide el estado actual 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	Comm Failure	00:01:45 UTC Jul 25 2023

```
====Configuration State====
```

```
    Sync Done
```

```
====Communication State====
```

```
    Mac set
```

Paso 5. Verifique la configuración desde la unidad primaria con el comando `show running-config failover` y `show running-config interface`:

```
> show running-config failover
```

```
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 1.1.1.1 255.255.255.252 standby 1.1.1.2
```

```
> show running-config interface
```

```
!
interface Ethernet1/1
  description LAN/STATE Failover Interface
  ipv6 enable
!
interface Ethernet1/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/5
  nameif inside
  security-level 0
  ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
interface Ethernet1/6
  nameif outside
  security-level 0
  ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
```

```
!  
interface Ethernet1/7  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Management1/1  
  management-only  
  nameif diagnostic  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  no ip address
```

## Tarea 4. Cambiar los roles de conmutación por error

Tarea requerida:

Desde la interfaz gráfica del administrador de dispositivos de firewall seguro, cambie las funciones de conmutación por fallo de Primario/Activo, Secundario/En espera a Primario/En espera, Secundario/Activo

Solución:

Paso 1. Haga clic en **Dispositivo**

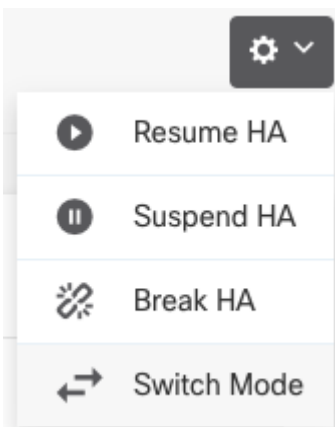


Device: FPR2130-1

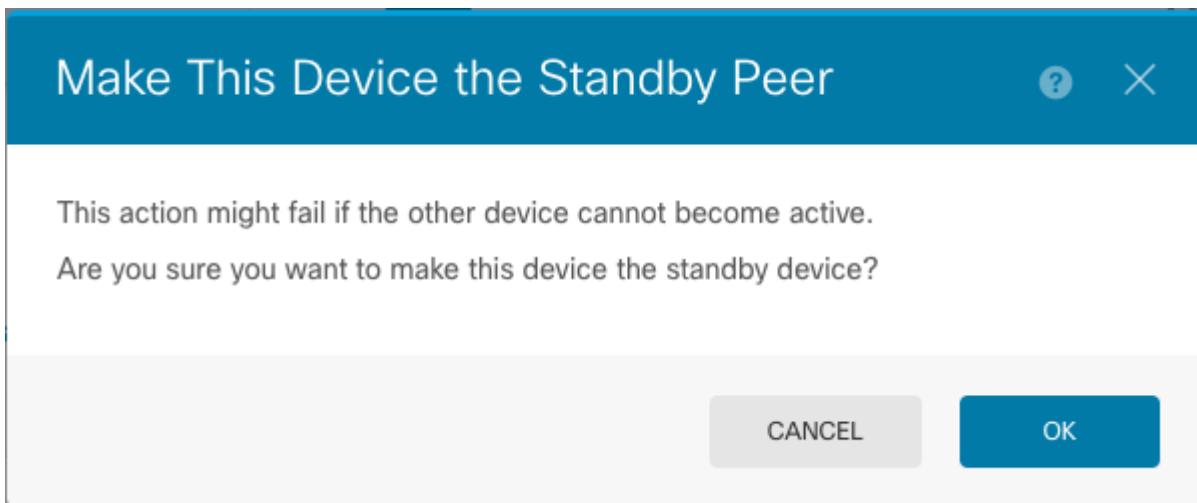
Paso 2. Haga clic en el enlace **High Availability** en el lado derecho del resumen del dispositivo.

High Availability  
Primary Device: **Active** ↔ Peer: **Standby**

Paso 3. Desde el icono del engranaje (⚙️), elija **Switch Mode**.

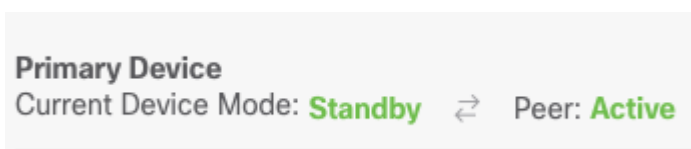


Paso 4. Lea el mensaje de confirmación y haga clic en **Aceptar**.



El sistema fuerza la conmutación por fallas de modo que la unidad activa pase a estar en espera y la unidad en espera pase a ser la nueva unidad activa.

Paso 5. Verifique el resultado como se muestra en la imagen:



Paso 6. También es posible verificar mediante el enlace Failover History (Historial de fallas) y la ventana emergente de la consola CLI debe mostrar los resultados:

From State	To State	Reason
21:55:37 UTC Jul 20 2023 Not Detected	Disabled	No Error
00:00:43 UTC Jul 25 2023 Disabled	Negotiation	Set by the config command
00:01:28 UTC Jul 25 2023 Negotiation	Just Active	No Active unit found
00:01:29 UTC Jul 25 2023 Just Active	Active Drain	No Active unit found
00:01:29 UTC Jul 25 2023 Active Drain	Active Applying Config	No Active unit found
00:01:29 UTC Jul 25 2023 Active Applying Config	Active Config Applied	No Active unit found
00:01:29 UTC Jul 25 2023 Active Config Applied	Active	No Active unit found
18:51:40 UTC Jul 25 2023 Active	Standby Ready	Set by the config command

```

=====
PEER History Collected at 18:55:08 UTC Jul 25 2023
=====PEER-HISTORY=====
From State          To State          Reason
=====PEER-HISTORY=====
22:00:18 UTC Jul 24 2023
Not Detected        Disabled          No Error

00:52:08 UTC Jul 25 2023
Disabled            Negotiation       Set by the config command

00:52:10 UTC Jul 25 2023
Negotiation         Cold Standby      Detected an Active mate

00:52:11 UTC Jul 25 2023
Cold Standby        App Sync          Detected an Active mate

00:53:26 UTC Jul 25 2023
App Sync            Sync Config       Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync Config         Sync File System  Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync File System    Bulk Sync         Detected an Active mate

01:00:23 UTC Jul 25 2023
Bulk Sync           Standby Ready     Detected an Active mate

18:45:01 UTC Jul 25 2023
Standby Ready       Just Active       Other unit wants me Active

18:45:02 UTC Jul 25 2023
Just Active         Active Drain      Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Drain        Active Applying Config Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Applying Config Active Config Applied Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Config Applied Active             Other unit wants me Active
=====PEER-HISTORY=====

```

Paso 7. Después de la verificación, vuelva a activar la unidad principal.

## Tarea 5. Suspensión o reanudación de alta disponibilidad

Puede suspender una unidad en un par de alta disponibilidad. Esto es útil cuando:

- Ambas unidades están en una situación activa-activa y la corrección de la comunicación en el link de failover no corrige el problema.
- Usted desea resolver problemas de una unidad activa o en espera y no quiere que las unidades conmuten por error durante ese tiempo.



- Desea evitar la conmutación por error al instalar una actualización de software en el dispositivo en espera.

La diferencia clave entre suspender HA y romper HA es que en un dispositivo HA suspendido, se conserva la configuración de alta disponibilidad. Cuando interrumpe HA, la configuración se borra. Por lo tanto, tiene la opción de reanudar HA en un sistema suspendido, lo que habilita la configuración existente y hace que los dos dispositivos funcionen como un par de failover nuevamente.

Tarea requerida:

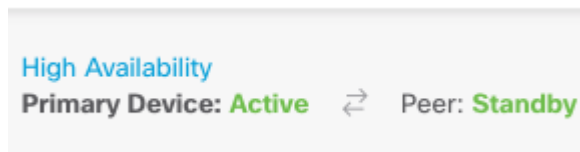
En la interfaz gráfica del administrador de dispositivos de firewall seguro, suspenda la unidad principal y reanude la alta disponibilidad en la misma unidad.

Solución:

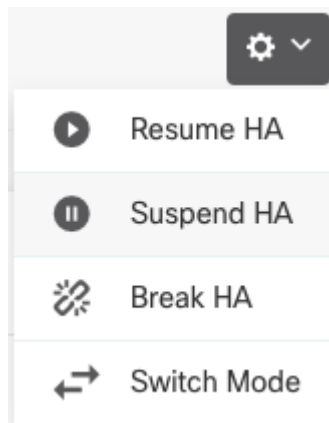
Paso 1. Haga clic en **Device**.



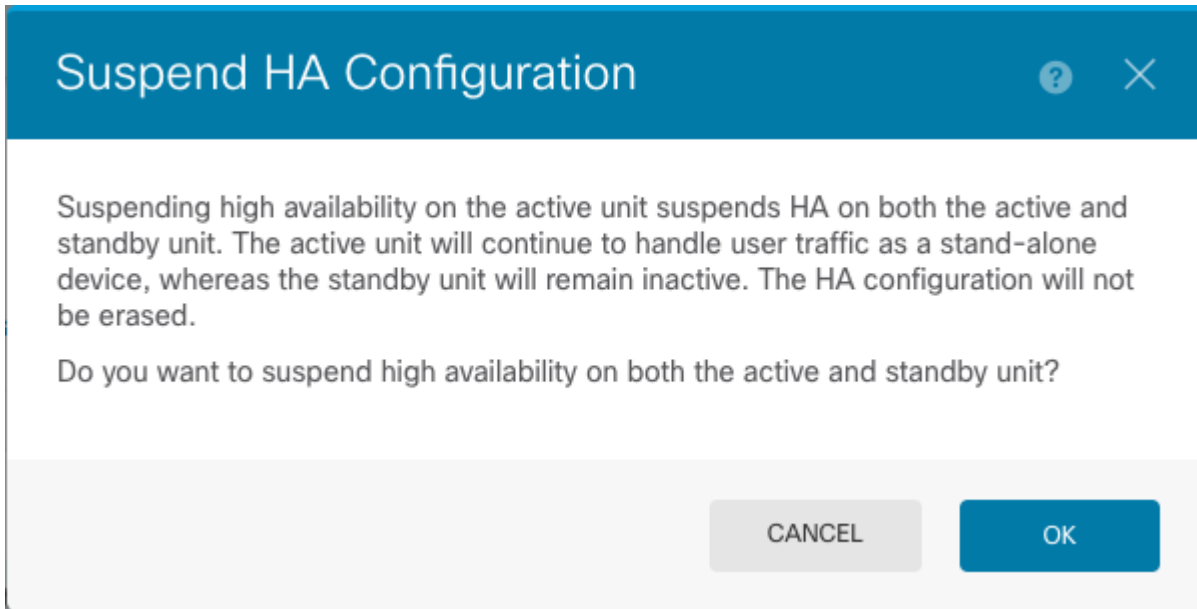
Paso 2. Haga clic en el enlace **High Availability** en el lado derecho del resumen del dispositivo.



Paso 3. Desde el icono del engranaje (⚙️), elija **Suspend HA**.



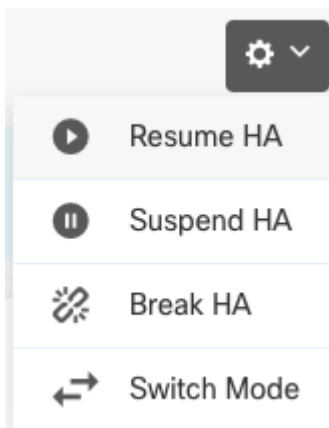
Paso 4. Lea el mensaje de confirmación y haga clic en **Aceptar**.



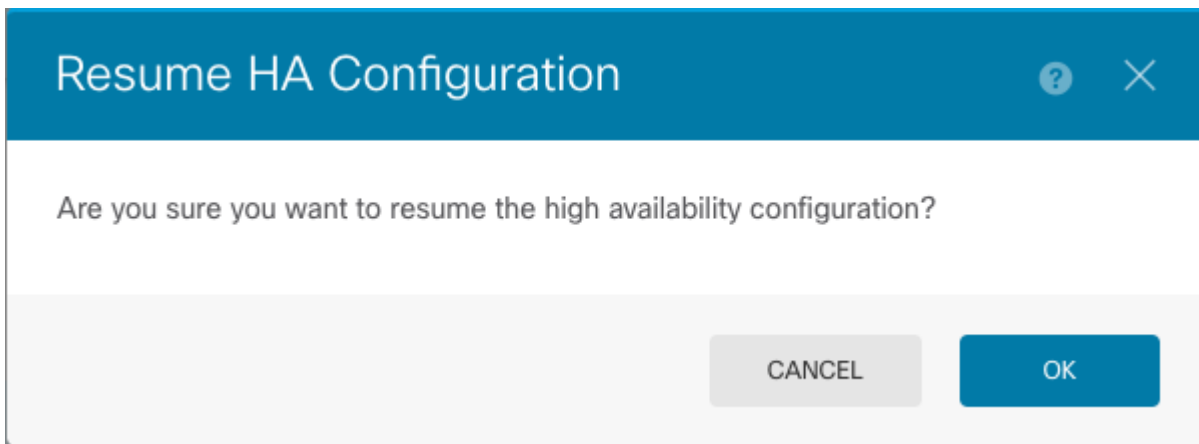
Paso 5. Verifique el resultado como se muestra en la imagen:



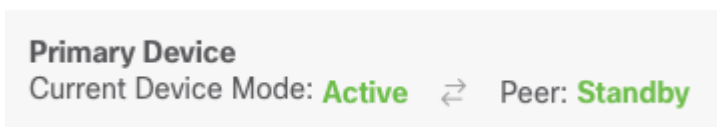
Paso 6. Para reanudar el HA, en el icono del engranaje (⚙️), elija **Reanudar HA**.



Paso 7. Lea el mensaje de confirmación y haga clic en **Aceptar**.



Paso 5. Verifique el resultado como se muestra en la imagen:



## Tarea 6. Alta disponibilidad rompedora

Si ya no desea que los dos dispositivos funcionen como un par de alta disponibilidad, puede interrumpir la configuración de HA. Cuando interrumpe HA, cada dispositivo se convierte en un dispositivo independiente. Sus configuraciones deben cambiar de la siguiente manera:

- El dispositivo activo conserva la configuración completa tal y como está antes de la interrupción, con la configuración de alta disponibilidad eliminada.
- El dispositivo en espera tiene todas las configuraciones de interfaz removidas además de la configuración HA. Todas las interfaces físicas están desactivadas, aunque las subinterfaces no lo están. La interfaz de administración permanece activa, por lo que puede iniciar sesión en el dispositivo y volver a configurarlo.

Tarea requerida:

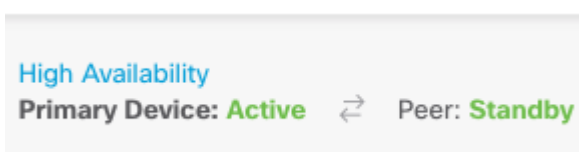
Desde la interfaz gráfica del administrador de dispositivos de firewall seguro, rompa el par de alta disponibilidad.

Solución:

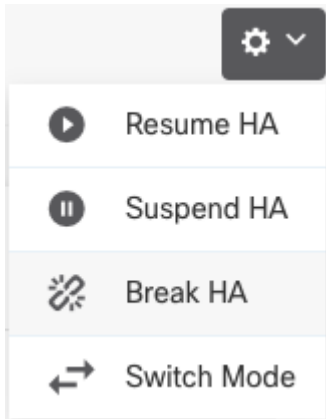
Paso 1. Haga clic en **Device**.



Paso 2. Haga clic en el enlace **High Availability** en el lado derecho del resumen del dispositivo.



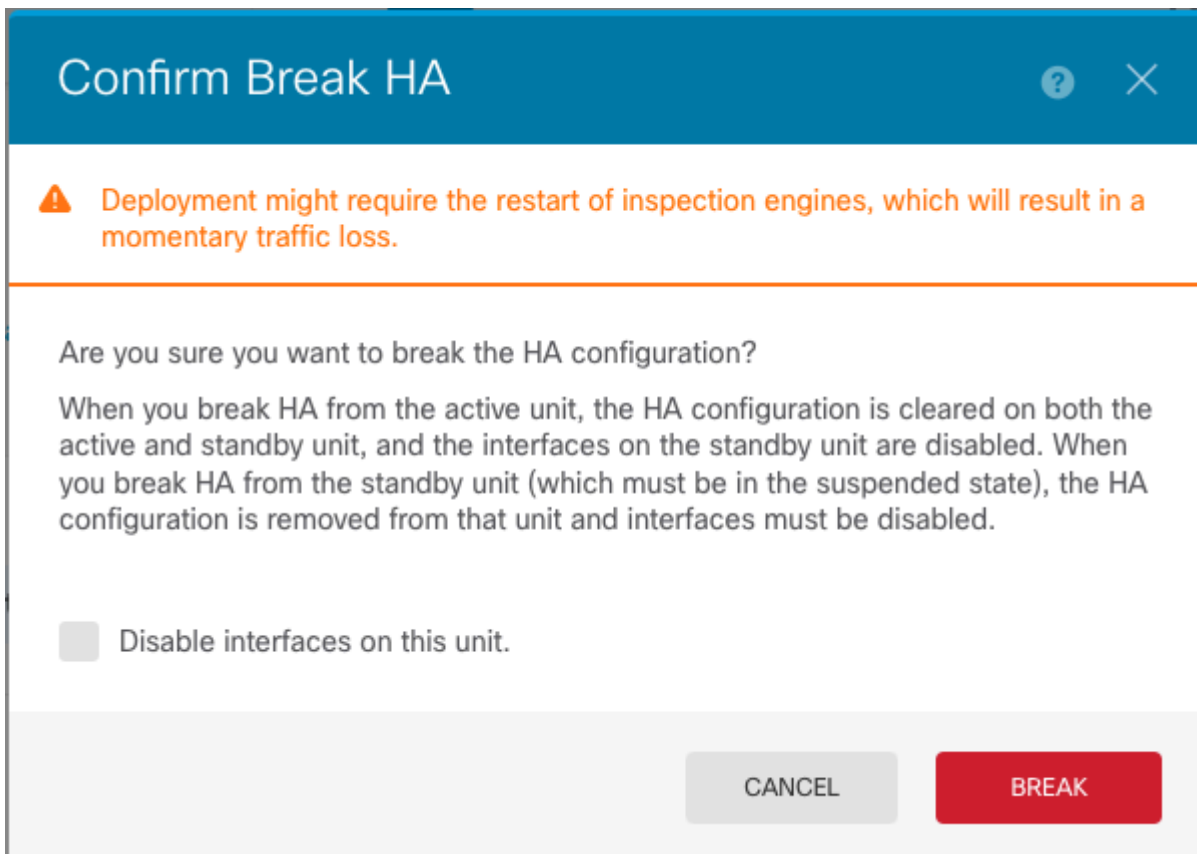
Paso 3. Desde el icono del engranaje (⚙️), elija **Break HA**.



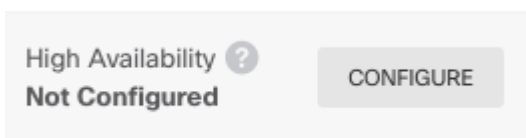
Paso 4. Lea el mensaje de confirmación, decida si selecciona la opción para desactivar las interfaces y haga clic en **Break**.

Debe seleccionar la opción para inhabilitar las interfaces si está interrumpiendo HA de la unidad en espera.

El sistema implementa inmediatamente los cambios tanto en este dispositivo como en el dispositivo par (si es posible). La implementación puede tardar varios minutos en completarse en cada dispositivo y, además, cada dispositivo puede pasar a ser independiente.



Paso 5. Verifique el resultado como se muestra en la imagen:



## Información Relacionada

- Puede encontrar todas las versiones de la guía de configuración del administrador de dispositivos de Cisco Secure Firewall aquí

<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html>

- Cisco Global Technical Assistance Center (TAC) recomienda encarecidamente esta guía visual para obtener un conocimiento práctico en profundidad de las tecnologías de seguridad de última generación de Cisco Firepower:

<https://www.ciscopress.com/store/cisco-firepower-threat-defense-ftd-configuration-and-9781587144806>

- Para todas las notas técnicas de configuración y solución de problemas relacionadas con las tecnologías Firepower

<https://www.cisco.com/c/en/us/support/security/defense-center/series.html>

- [Soporte Técnico y Documentación - Cisco Systems](#)

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).