

# Secure Firewall Device Manager configureren in hoge beschikbaarheid

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Taak 1. Controleer de voorwaarden](#)

[Taak 2. Secure Firewall Device Manager configureren in hoge beschikbaarheid](#)

[Netwerkdigram](#)

[Hoge beschikbaarheid inschakelen voor Secure Firewall Device Manager in primaire eenheid](#)

[Hoge beschikbaarheid inschakelen voor Secure Firewall Device Manager in Secundaire eenheid](#)

[De configuratie van de interfaces voltooien](#)

[Taak 3. Controleer de hoge beschikbaarheid van FDM](#)

[Taak 4. De failover-rollen switches](#)

[Taak 5. Hoge beschikbaarheid opschorten of hervatten](#)

[Taak 6. Brekende hoge beschikbaarheid](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u Secure Firewall Device Manager (FDM) High Availability (HA) kunt configureren en verifiëren op beveiligde firewallapparaten.

## Voorwaarden

### Vereisten

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 2xCisco Secure Firewall 2100 security applicatie
- FDM-versie 7.0.5 uitvoeren (build 72)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Taak 1. Controleer de voorwaarden

Taakvereiste:

Controleer dat beide FDM-apparaten voldoen aan de notatievereisten en kunnen worden geconfigureerd als HA-eenheden.

Oplossing:

Stap 1. Sluit de IP-telefoon met apparaatbeheer aan op SSH en controleer de hardware van de module.

Controleer met de **opdracht show version** de primaire hardware en softwareversie van het apparaat:

```
> 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
-----
```

Controleer de hardware en softwareversie van het secundaire apparaat:

```
> 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
-----
```

## **Taak 2. Secure Firewall Device Manager configureren in hoge beschikbaarheid**

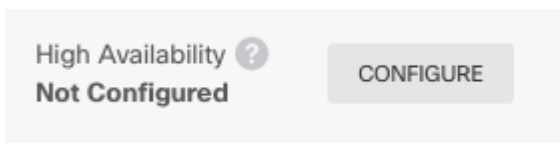
### **Netwerkdigram**

Active/Standby High Availability (HA) configureren volgens dit diagram:

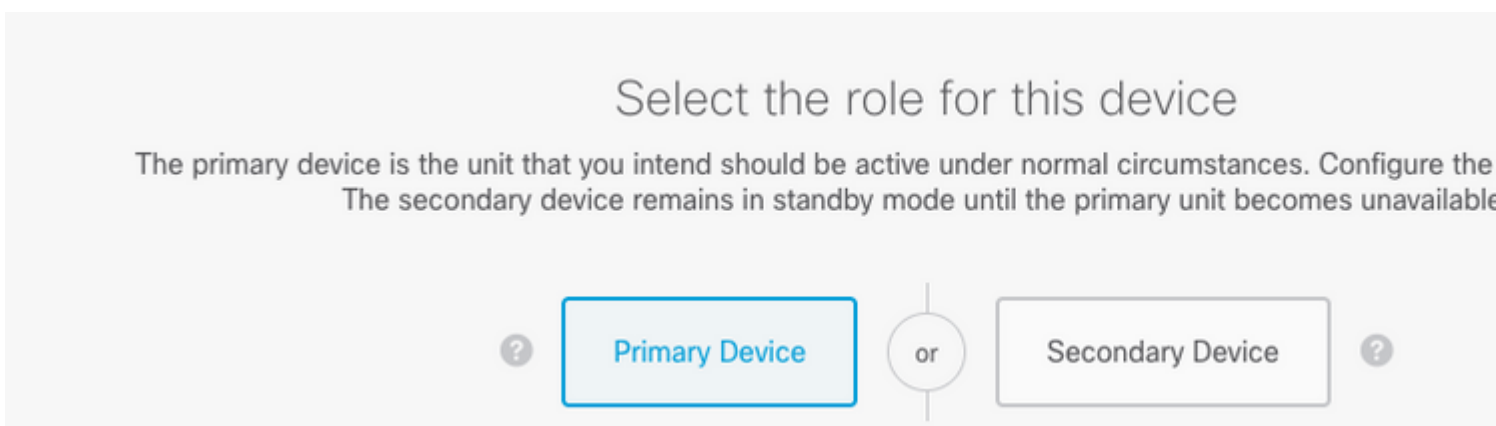


## Hoge beschikbaarheid inschakelen voor Secure Firewall Device Manager in primaire eenheid

Stap 1. Om FDM failover te configureren, navigeer naar **apparaat** en klik op **Configureren** naast de groep met **hoge beschikbaarheid**:



Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Primair apparaat:



**Waarschuwing:** Zorg ervoor dat u de juiste eenheid als de **primaire** eenheid selecteert. Alle configuraties op de geselecteerde primaire eenheid worden gerepliceerd naar de geselecteerde secundaire FTD-eenheid. Als gevolg van replicatie kan de huidige configuratie op de secundaire eenheid worden **vervangen**.

Stap 3. Configureer de failover link en de instellingen van de state link:

In dit voorbeeld heeft de koppeling status dezelfde instellingen als de koppeling 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>	
<b>IMPORTANT</b> If you configure an IPsec encryption key with in features, both devices will become active after	

Stap 4. Klik op Activeren HA

Stap 5. Kopieer de HA-configuratie naar het klembord op het bevestigingsbericht, om het op de Secundaire eenheid te plakken.

✕

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

What's next?

I need to configure Peer Device

I 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

Het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatetaak te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien.

De configuratie wordt ook naar het klembord gekopieerd. U kunt met deze kopie de secundaire eenheid snel configureren. Voor extra veiligheid is de coderings sleutel niet in het klembord-exemplaar opgenomen.

Op dit punt moet u op de pagina Hoge beschikbaarheid staan en moet uw apparaatstatus "Onderhandelen" zijn. De status moet overgaan naar Actief, zelfs voordat u de peer configureert. Deze moet verschijnen als Mislukt totdat u het configureert.

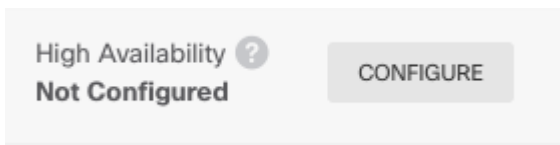
High Availability

Primary Device: Active Peer: ✕ Failed

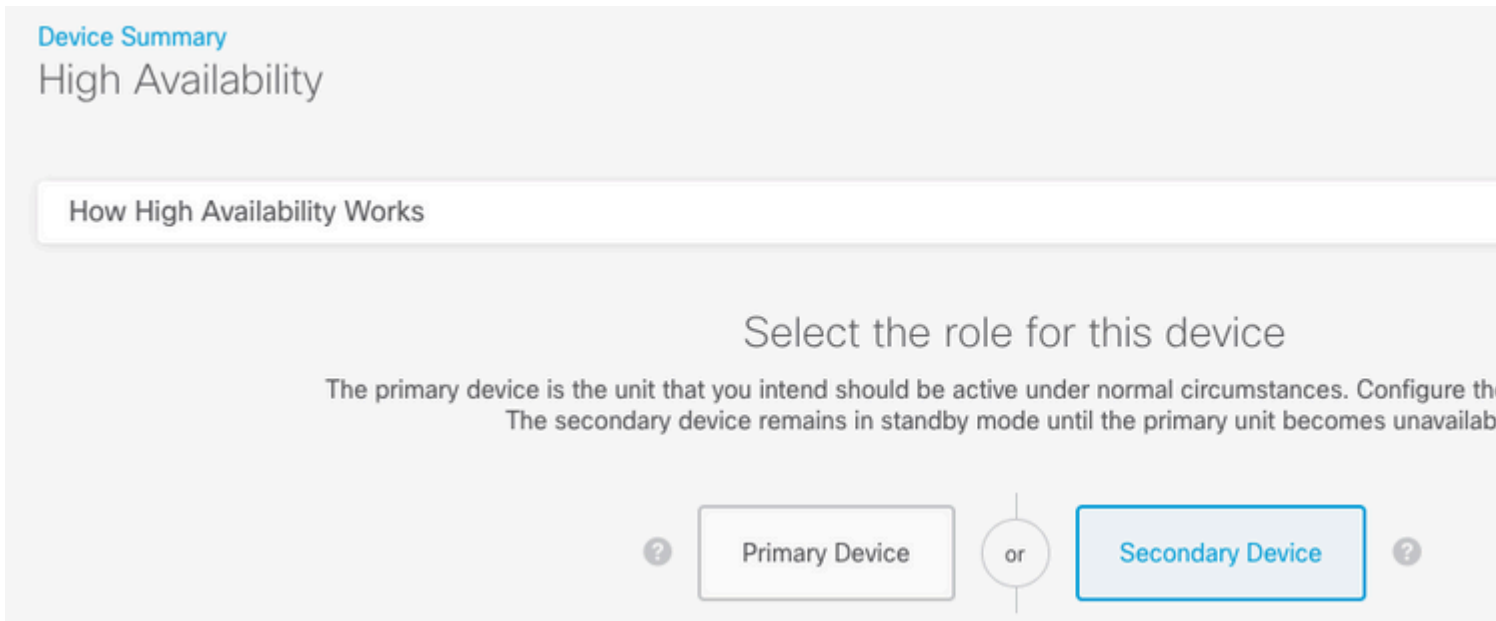
## Hoge beschikbaarheid inschakelen voor Secure Firewall Device Manager in Secundaire eenheid

Nadat u het primaire apparaat voor actieve/stand-by hoge beschikbaarheid configureert, moet u vervolgens het secundaire apparaat configureren. Log in de FDM op dat apparaat en voer deze procedure uit.

Stap 1. Om FDM failover te configureren, navigeer naar **apparaat** en klik op **Configureren** naast de groep met **hoge beschikbaarheid**:

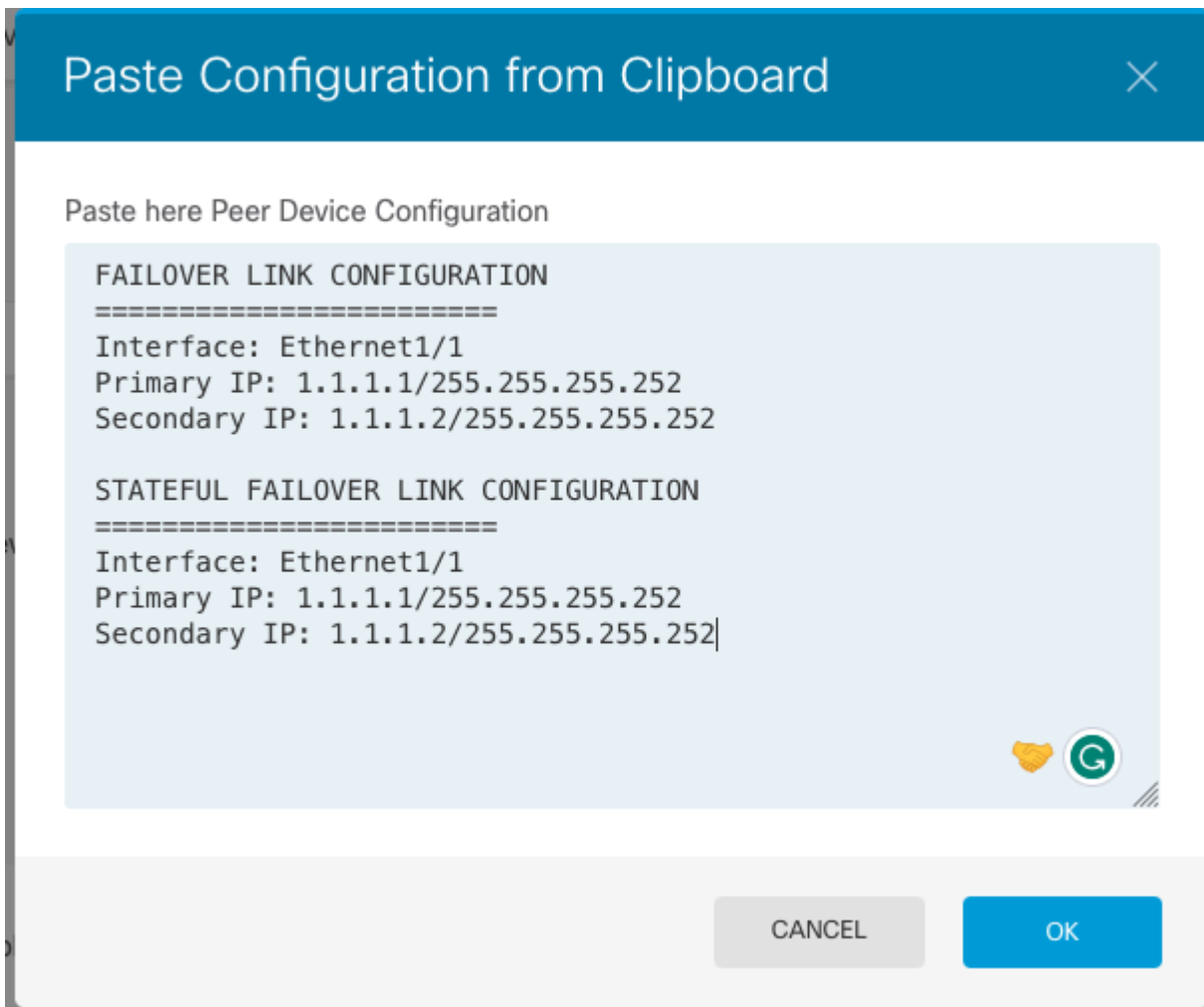


Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Secundair apparaat:



Stap 3. Kies een van de volgende opties:

- Gemakkelijk methode – Klik op de knop Plakken vanaf klembord, plak in de configuratie en klik op OK. Hiermee worden de velden met de juiste waarden bijgewerkt. Deze waarden kunt u vervolgens controleren.
- Handmatig methode: stel de failover en stateful failover links direct in. Voer exact dezelfde instellingen in voor het secundaire apparaat dat u op het primaire apparaat hebt ingevoerd.

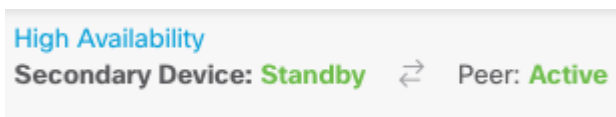


Stap 4. Klik op HA activeren

Het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatietask te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien.

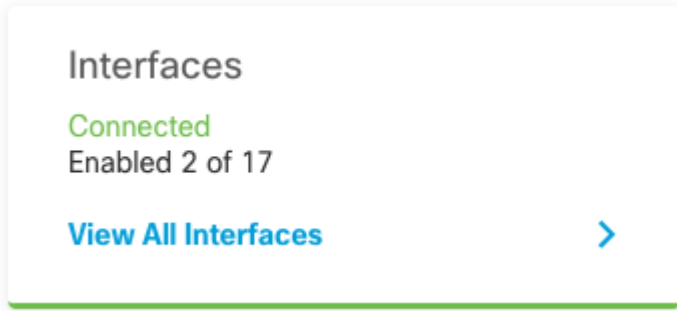
Nadat de configuratie is voltooid, krijgt u een bericht waarin staat dat u HA hebt geconfigureerd. Klik op Got It om het bericht te negeren.

Op dit punt, moet u op de pagina Hoge beschikbaarheid zijn, en uw apparatenstatus moet erop wijzen dat dit het secundaire apparaat is. Als de verbinding met het primaire apparaat succesvol was, synchroniseert het apparaat met het primaire, en uiteindelijk, moet de modus stand-by zijn en moet de peer actief zijn.



## De configuratie van de interfaces voltooien

Stap 1. Om FDM-interfaces te configureren navigeer je naar **apparaat** en klik je op **Alle interfaces weergeven**:



Stap 2. Selecteer de instellingen voor interfaces en bewerk deze zoals in de afbeeldingen:

Ethernet 1/5 interface:



# 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

Ethernet 1/6 interface

## Ethernet1/6 Edit Physical Interface



Interface Name

outside

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

Stap 3. Nadat u de wijzigingen hebt geconfigureerd, klikt u op **Hangende wijzigingen**  en **nu implementeren**.

### Taak 3. Controleer de hoge beschikbaarheid van FDM

Taakvereiste:

Controleer de instellingen voor hoge beschikbaarheid van de FDM GUI en van FDM CLI.

Oplossing:

Stap 1. Navigeer naar **apparaat** en controleer de instellingen voor **hoge beschikbaarheid**:

The screenshot displays the 'High Availability Configuration' page for a Cisco Firepower 2130 Threat Defense device. The page is divided into several sections:

- Device Summary:** Shows 'High Availability' status, 'Primary Device' (Current Device Mode: Active, Peer: Standby), and links for 'Failover History' and 'Deployment History'.
- High Availability Configuration:**
  - GENERAL DEVICE INFORMATION:** Model: Cisco Firepower 2130 Threat Defense, Software: 7.0.5-72, VDB: 338.0, Intrusion Rule Update: 20210503-2107.
  - FAILOVER LINK:** Interface: Ethernet1/1, Type: IPv4, Primary IP/Netmask: 1.1.1.1/255.255.255.252, Secondary IP/Netmask: 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:** Poll Time: 5000 (500-15000 milliseconds), Hold Time: 25000 (5000-75000 milliseconds).
  - PEER TIMING CONFIGURATION:** Poll Time: 1000 (200-15000 milliseconds), Hold Time: 15000 (800-45000 milliseconds).
  - SAVE** button.

Stap 2. Verbind met de FDM Primaire Apparaat CLI met behulp van SSH en bevestig met de opdracht **hoge beschikbaarheid**:

```
> 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
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

Stap 3. Doe dit ook met het Secundaire apparaat.

Stap 4. Bevestig de huidige staat met het bevel van de **show failover staat**:

```
> 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
```

Stap 5. Controleer de configuratie van de primaire eenheid met de show in werking stelt -in werking stellen-configuratiefailover en toon in werking stellen-configuratieinterface:

```
> 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
```

## Taak 4. De failover-rollen switches

Taakvereiste:

Switch vanuit de grafische interface van Secure Firewall Device Manager de failoverrollen van Primary/Active, Secondary/Standby naar Primary/Standby, Secondary/Active

Oplossing:

Stap 1. Klik op **apparaat**



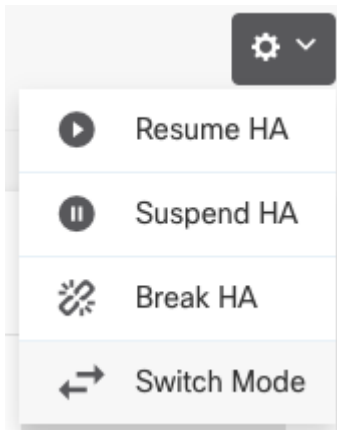
Device: **FPR2130-1**

Stap 2. Klik op de link **Hoge beschikbaarheid** rechts in het apparaatoverzicht.

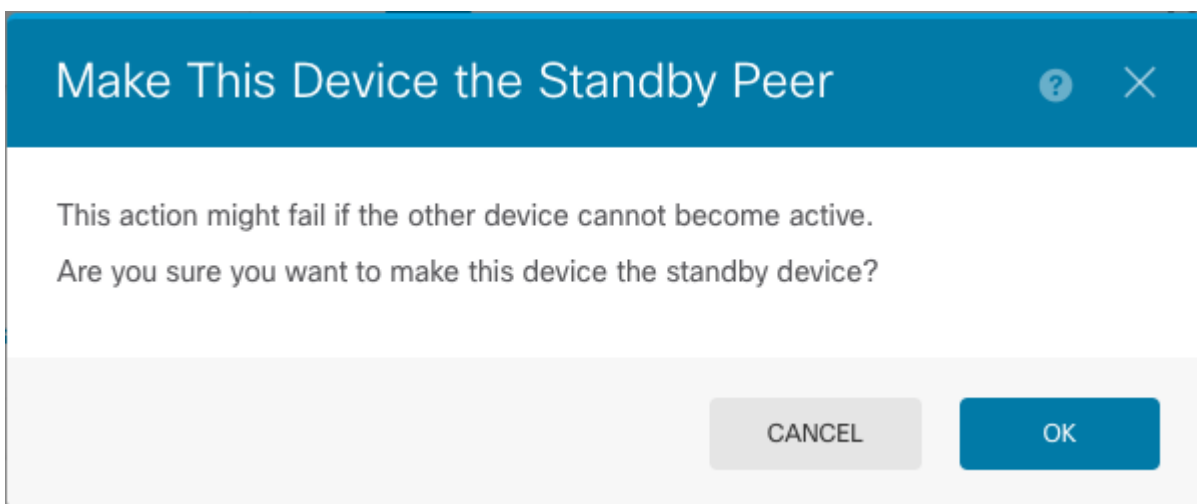
High Availability

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

Stap 3. Van het tandwiel pictogram (⚙️), kies **Switch Mode**.

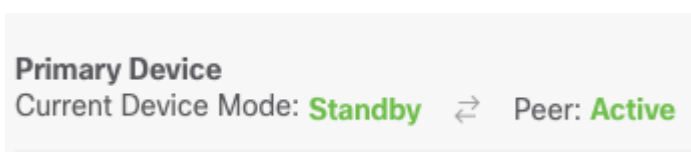


Stap 4. Lees het bevestigingsbericht en klik op **OK**.



Het systeem forceert de failover zodat de actieve eenheid stand-by wordt en de standby-eenheid de nieuwe actieve eenheid wordt.

Stap 5. Controleer het resultaat zoals in de afbeelding:



Stap 6. Het is ook mogelijk om te verifiëren met behulp van de koppeling failover historie en de CLI-console pop-up moet de resultaten tonen:

```
=====
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=====



Stap 7. Voer na de verificatie de primaire eenheid opnieuw in.

## Taak 5. Hoge beschikbaarheid opschorten of hervatten

U kunt een eenheid in een paar met hoge beschikbaarheid opschorten. Dit is nuttig wanneer:

- Beide eenheden bevinden zich in een actief-actieve situatie en het verhelpen van de communicatie via de failover-link lost het probleem niet op.
- U wilt problemen oplossen met een actieve of stand-by unit en wilt niet dat de eenheden gedurende die tijd failliet gaan.
- U wilt failover voorkomen tijdens het installeren van een software upgrade op het stand-by apparaat.

Het belangrijkste verschil tussen het opschorten van HA en het breken van HA is dat op een opgeschort HA apparaat, de hoge beschikbaarheid configuratie wordt behouden. Wanneer u HA breekt, wordt de configuratie gewist. Zo hebt u de optie om HA op een opgeschort systeem te hervatten, dat de bestaande configuratie toelaat en de twee apparaten weer als failover-paar laat functioneren.

Taakvereiste:

Schakel de grafische interface van Secure Firewall Device Manager uit om de primaire eenheid te onderbreken en de hoge beschikbaarheid op dezelfde eenheid te hervatten.

Oplossing:

Stap 1. Klik op **Apparaat**.

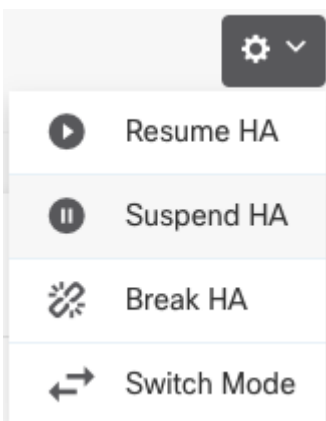


Device: FPR2130-1

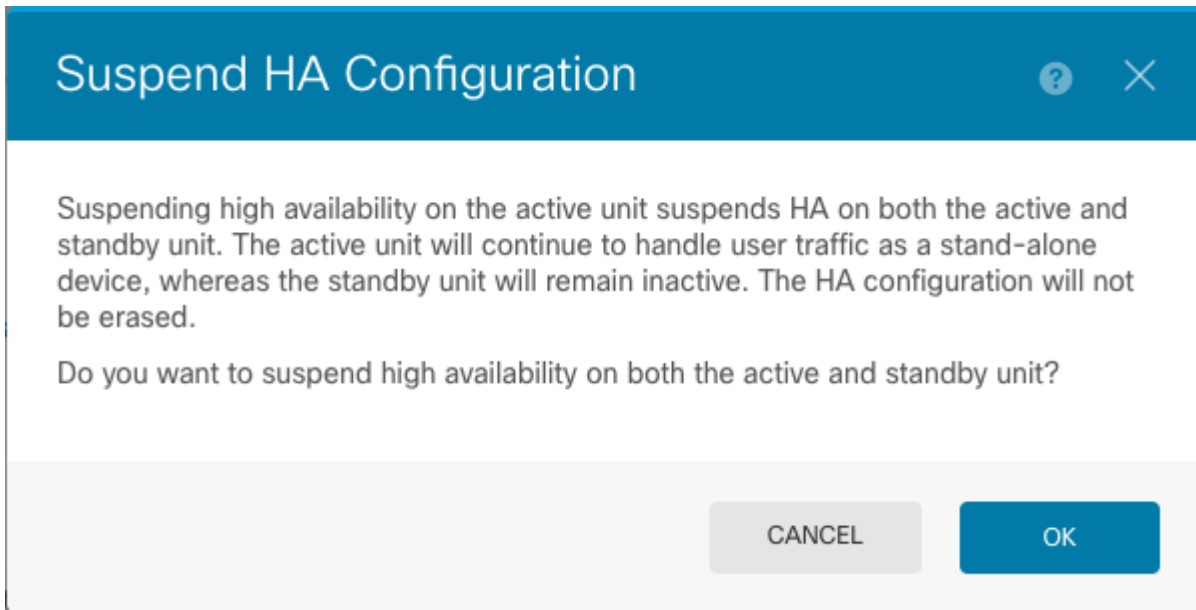
Stap 2. Klik op de link **Hoge beschikbaarheid** rechts in het apparaatoverzicht.

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

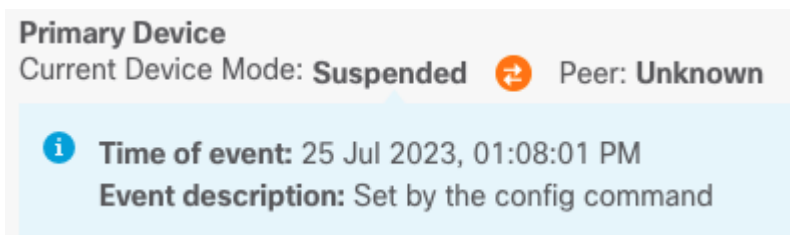
Stap 3. Van het tandwiel pictogram (⚙️), kies **Suspend HA**.



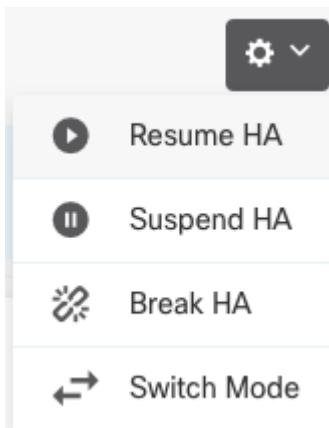
Stap 4. Lees het bevestigingsbericht en klik op **OK**.



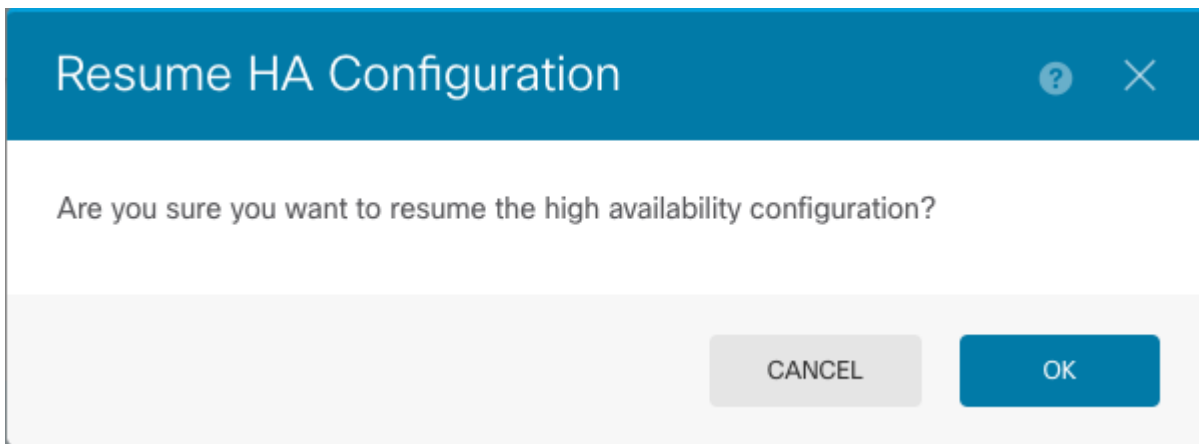
Stap 5. Controleer het resultaat zoals in de afbeelding:



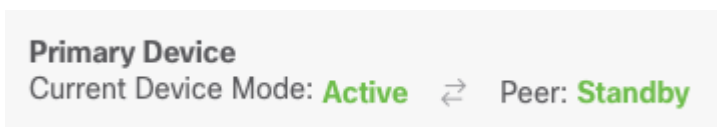
Stap 6. Hervatten van de HA, vanaf het tandwiel pictogram (⚙️), kies **Hervat HA**.



Stap 7. Lees het bevestigingsbericht en klik op **OK**.



Stap 5. Controleer het resultaat zoals in de afbeelding:



## Taak 6. Brekende hoge beschikbaarheid

Als u niet langer wilt dat de twee apparaten functioneren als een paar met hoge beschikbaarheid, kunt u de HA-configuratie breken. Wanneer u HA breekt, wordt elk apparaat een standalone apparaat. Hun configuraties moeten als volgt worden gewijzigd:

- Het actieve apparaat behoudt de volledige configuratie zoals het is voorafgaand aan de breuk, met de HA-configuratie verwijderd.
- Het standby-apparaat heeft alle interfaceconfiguraties verwijderd naast de HA-configuratie. Alle fysieke interfaces zijn uitgeschakeld, hoewel subinterfaces niet zijn uitgeschakeld. De beheerinterface blijft actief, zodat u zich bij het apparaat kunt aanmelden en het opnieuw kunt configureren.

Taakvereiste:

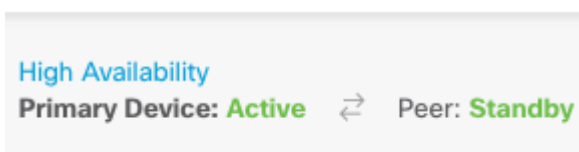
Breek het paar Hoge Beschikbaarheid via de grafische interface van Secure Firewall Device Manager.

Oplossing:

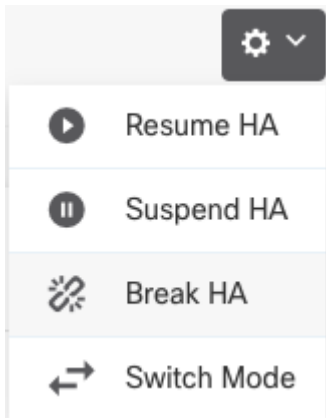
Stap 1. Klik op **Apparaat**.



Stap 2. Klik op de link **Hoge beschikbaarheid** rechts in het apparaatoverzicht.



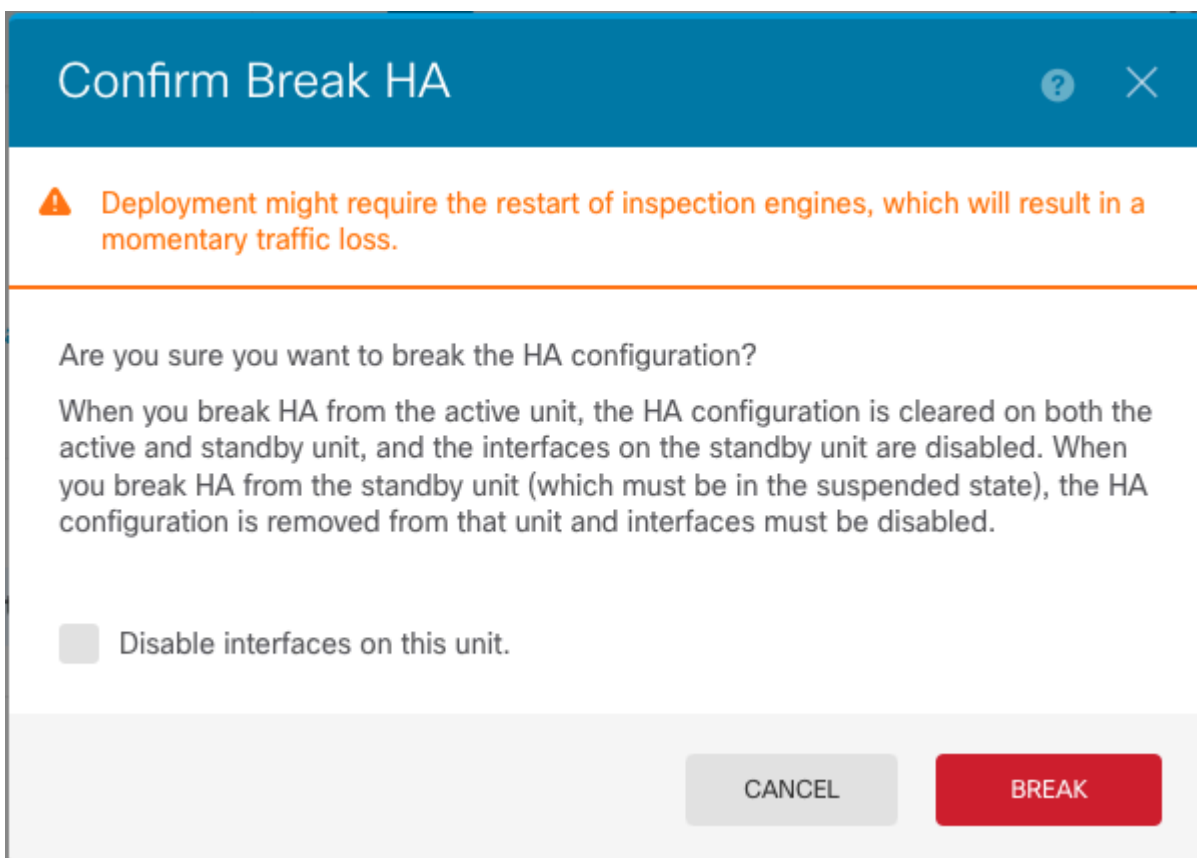
Stap 3. Van het tandwielpictogram (⚙️), kies **Break HA**.



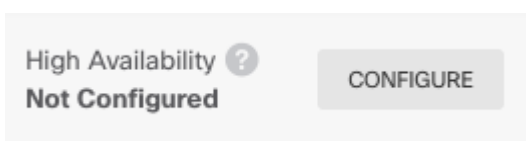
Stap 4. Lees het bevestigingsbericht, beslis of u de optie wilt selecteren om interfaces uit te schakelen en klik op **Onderbreken**.

U moet de optie selecteren om interfaces uit te schakelen als u HA uit de standby-eenheid breekt.

Het systeem implementeert onmiddellijk uw wijzigingen op zowel dit apparaat als het peer-apparaat (indien mogelijk). Het kan een paar minuten duren voor de implementatie op elk apparaat is voltooid en voor elk apparaat om onafhankelijk te worden.



Stap 5. Controleer het resultaat zoals in de afbeelding:



## Gerelateerde informatie

- Alle versies van de configuratiehandleiding voor Cisco Secure Firewall Device Manager zijn hier te vinden

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

- Cisco Global Technical Assistance Center (TAC) raadt deze visuele handleiding ten zeerste aan voor diepgaande praktische kennis over Cisco Firepower Security Technologies van de volgende generatie:

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

- TechNotes voor alle configuratie en probleemoplossing die betrekking hebben op de FirePOWER-technologieën

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

- [Technische ondersteuning en documentatie](#) â€™ Cisco Systems

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.