

Configurer le Gestionnaire de périphériques de pare-feu sécurisé en haute disponibilité

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Tâche 1. Vérifier les conditions](#)

[Tâche 2. Configurer le Gestionnaire de périphériques de pare-feu sécurisé en haute disponibilité](#)

[Diagramme du réseau](#)

[Activer la haute disponibilité sur le Gestionnaire de périphériques de pare-feu sécurisé dans l'unité principale](#)

[Activer la haute disponibilité sur le Gestionnaire de périphériques de pare-feu sécurisé dans l'unité secondaire](#)

[Terminer La Configuration Des Interfaces](#)

[Tâche 3. Vérification de la haute disponibilité FDM](#)

[Tâche 4. Modifier les rôles de basculement](#)

[Tâche 5. Suspension ou reprise de la haute disponibilité](#)

[Tâche 6. Une haute disponibilité exceptionnelle](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer et vérifier la haute disponibilité (HA) de Secure Firewall Device Manager (FDM) sur les périphériques Secure Firewall.

Conditions préalables

Exigences

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 2 appliances de sécurité Cisco Secure Firewall 2100
- Exécution de FDM version 7.0.5 (build 72)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Tâche 1. Vérifier les conditions

Exigence de la tâche :

Vérifiez que les deux appareils FDM répondent aux exigences de la note et peuvent être configurés en tant qu'unités haute disponibilité.

Solution :

Étape 1. Connectez-vous à l'adresse IP de gestion de l'appliance via SSH et vérifiez le matériel du module.

Vérifiez à l'aide de la commande `show version` la version matérielle et logicielle du périphérique principal :

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

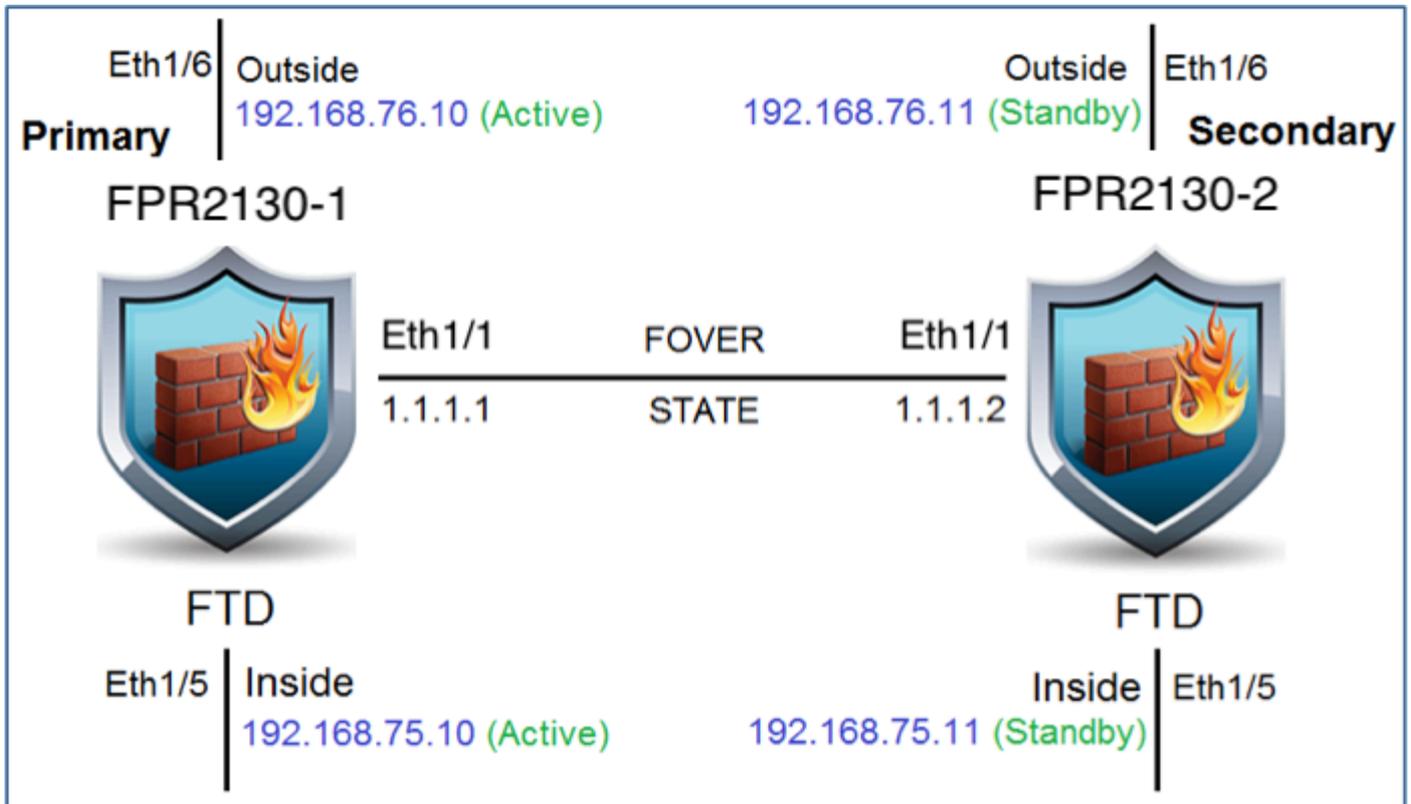
Vérifiez la version matérielle et logicielle du périphérique secondaire :

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

Tâche 2. Configurer le Gestionnaire de périphériques de pare-feu sécurisé en haute disponibilité

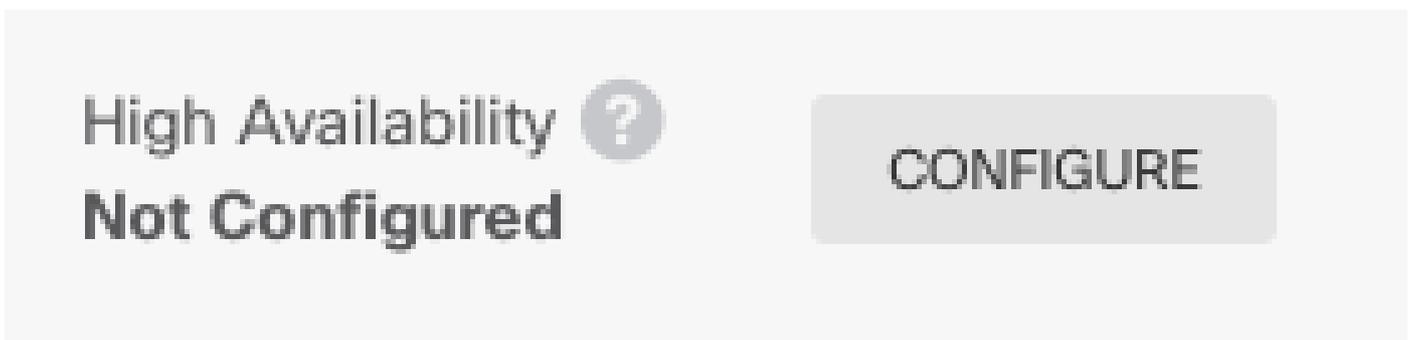
Diagramme du réseau

Configurez la haute disponibilité active/veille (HA) selon le schéma suivant :

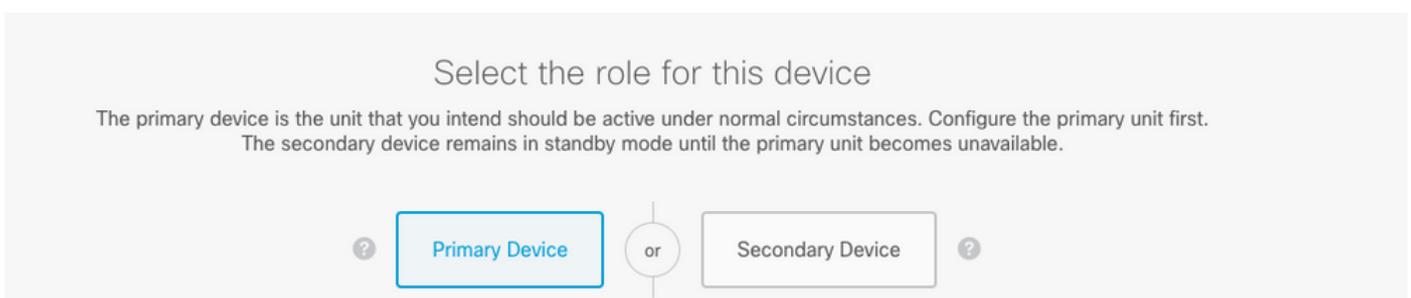


Activer la haute disponibilité sur le Gestionnaire de périphériques de pare-feu sécurisé dans l'unité principale

Étape 1. Afin de configurer le basculement de FDM, naviguez vers Device et cliquez sur Configurer à côté du groupe High Availability :



Étape 2. Sur la page High Availability, cliquez sur la zone Primary Device :



Avertissement : assurez-vous de sélectionner l'unité appropriée comme unité principale.

Toutes les configurations de l'unité principale sélectionnée sont répliquées sur l'unité FTD secondaire sélectionnée. Suite à la réplication, la configuration actuelle de l'unité secondaire peut être remplacée.

Étape 3. Configurez le lien de basculement et les paramètres du lien d'état :

Dans cet exemple, le lien d'état possède les mêmes paramètres que le lien de basculement.

| FAILOVER LINK | STATEFUL FAILOVER LINK <input checked="" type="checkbox"/> Use the same interface as the Failover Link |
|---|--|
| Interface unnamed (Ethernet1/1) | Interface unnamed (Ethernet1/1) |
| Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 | Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| Primary IP 1.1.1.1 <small>e.g. 192.168.10.1</small> | Primary IP 1.1.1.1 <small>e.g. 192.168.11.1</small> |
| Secondary IP 1.1.1.2 <small>e.g. 192.168.10.2</small> | Secondary IP 1.1.1.2 <small>e.g. 192.168.11.2</small> |
| Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small> | Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small> |
| IPSec Encryption Key (optional) <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> | IMPORTANT <small>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</small> |

Étape 4. Cliquez sur Activer HA

Étape 5. Copiez la configuration haute disponibilité dans le Presse-papiers du message de confirmation, pour la coller sur l'unité secondaire.

✕

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

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si aucun message indiquant que votre configuration a été enregistrée et que le déploiement est en cours ne s'affiche, faites défiler la page jusqu'en haut pour afficher les messages d'erreur.

La configuration est également copiée dans le Presse-papiers. Vous pouvez utiliser la copie pour configurer rapidement l'unité secondaire. Pour plus de sécurité, la clé de cryptage n'est pas incluse dans la copie du Presse-papiers.

À ce stade, vous devez être sur la page Haute disponibilité, et l'état de votre périphérique doit être « Négociation ». L'état doit passer à Actif avant même que vous configuriez l'homologue, qui doit apparaître comme Échec jusqu'à ce que vous le configuriez.

High Availability

Primary Device: **Active**



Peer: **Failed**

Activer la haute disponibilité sur le Gestionnaire de périphériques de pare-feu sécurisé dans l'unité secondaire

Après avoir configuré le périphérique principal pour la haute disponibilité active/en veille, vous devez configurer le périphérique secondaire. Connectez-vous au FDM sur ce périphérique et exécutez cette procédure.

Étape 1. Afin de configurer le basculement de FDM, naviguez vers Device et cliquez sur Configurer à côté du groupe High Availability :

High Availability 
Not Configured

CONFIGURE

Étape 2. Sur la page High Availability, cliquez sur la zone Secondary Device :

Device Summary
High Availability

How High Availability Works 

Select the role for this device

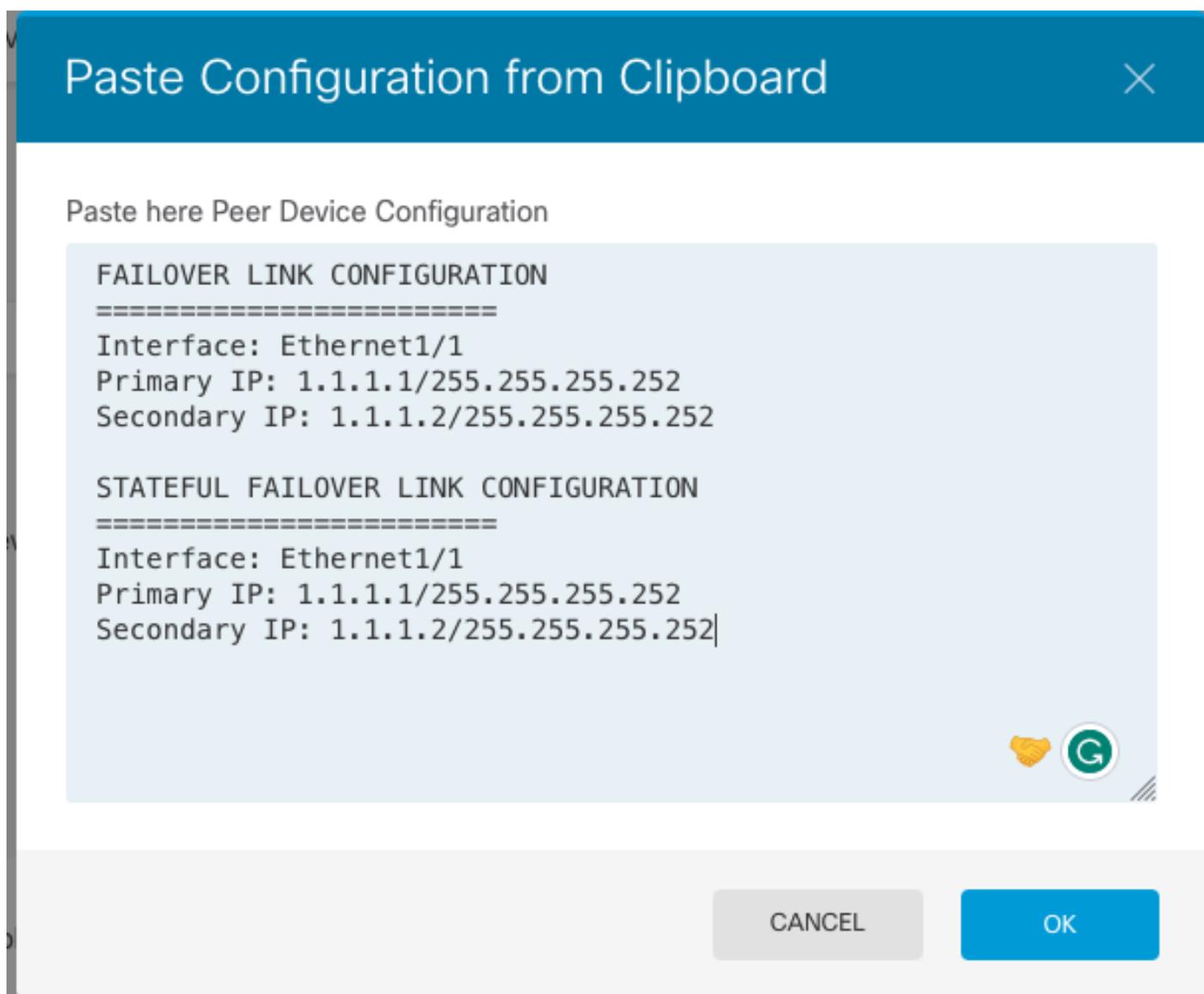
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first.
The secondary device remains in standby mode until the primary unit becomes unavailable.

 Primary Device  Secondary Device 

Étape 3. Choisissez l'une des options suivantes :

- Méthode facile : cliquez sur le bouton Coller à partir du Presse-papiers, collez la configuration, puis cliquez sur OK. Les champs sont mis à jour avec les valeurs appropriées, que vous pouvez ensuite vérifier.
- Méthode manuelle : configurez directement les liaisons de basculement et de basculement

dynamique. Saisissez exactement les mêmes paramètres sur le périphérique secondaire que sur le périphérique principal.



Étape 4. Cliquez sur Activer HA

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si aucun message indiquant que votre configuration a été enregistrée et que le déploiement est en cours ne s'affiche, faites défiler la page jusqu'en haut pour afficher les messages d'erreur.

Une fois la configuration terminée, vous recevez un message indiquant que vous avez configuré la haute disponibilité. Cliquez sur Got It pour rejeter le message.

À ce stade, vous devez vous trouver sur la page Haute disponibilité, et l'état de votre périphérique doit indiquer qu'il s'agit du périphérique secondaire. Si la jonction avec le périphérique principal a réussi, le périphérique se synchronise avec le périphérique principal et, finalement, le mode doit être Veille et l'homologue doit être Actif.

High Availability

Secondary Device: **Standby** ↔ Peer: **Active**

Terminer La Configuration Des Interfaces

Étape 1. Afin de configurer les interfaces FDM, accédez à Device et cliquez sur View All Interfaces :

Interfaces

Connected

Enabled 2 of 17

View All Interfaces



Étape 2. Sélectionnez et modifiez les paramètres des interfaces comme indiqué dans les images :

Interface 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

Interface Ethernet 1/6

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

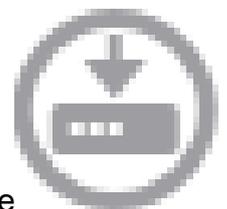
/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK



Étape 3. Après avoir configuré les modifications, cliquez sur Modifications en attente et Déployer maintenant.

Tâche 3. Vérification de la haute disponibilité FDM

Exigence de la tâche :

Vérifiez les paramètres de haute disponibilité à partir de l'interface utilisateur graphique et de

l'interface de ligne de commande FDM.

Solution :

Étape 1. Accédez à Device et vérifiez les paramètres High Availability :

The screenshot displays the 'High Availability Configuration' page in the FDM interface. It is divided into two main sections: 'High Availability Configuration' on the left and 'Failover Criteria' on the right.

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 (dropdown)
 - Number: 1
- 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)

A 'SAVE' button is visible at the bottom of the Failover Criteria section.

Étape 2. Connectez-vous à l'ILC du périphérique principal FDM à l'aide de SSH et validez avec la commande 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

```

Étape 3. Faites de même sur le périphérique secondaire.

Étape 4. Validez l'état actuel avec la commande 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
```

Étape 5. Vérifiez la configuration de l'unité principale à l'aide des commandes show running-config failover et 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
```

Tâche 4. Modifier les rôles de basculement

Exigence de la tâche :

À partir de l'interface graphique du Gestionnaire de périphériques de pare-feu sécurisé, passez des rôles de basculement principal/actif, secondaire/veille à principal/veille, secondaire/actif

Solution :

Étape 1. Cliquez sur Device



Device: FPR2130-1

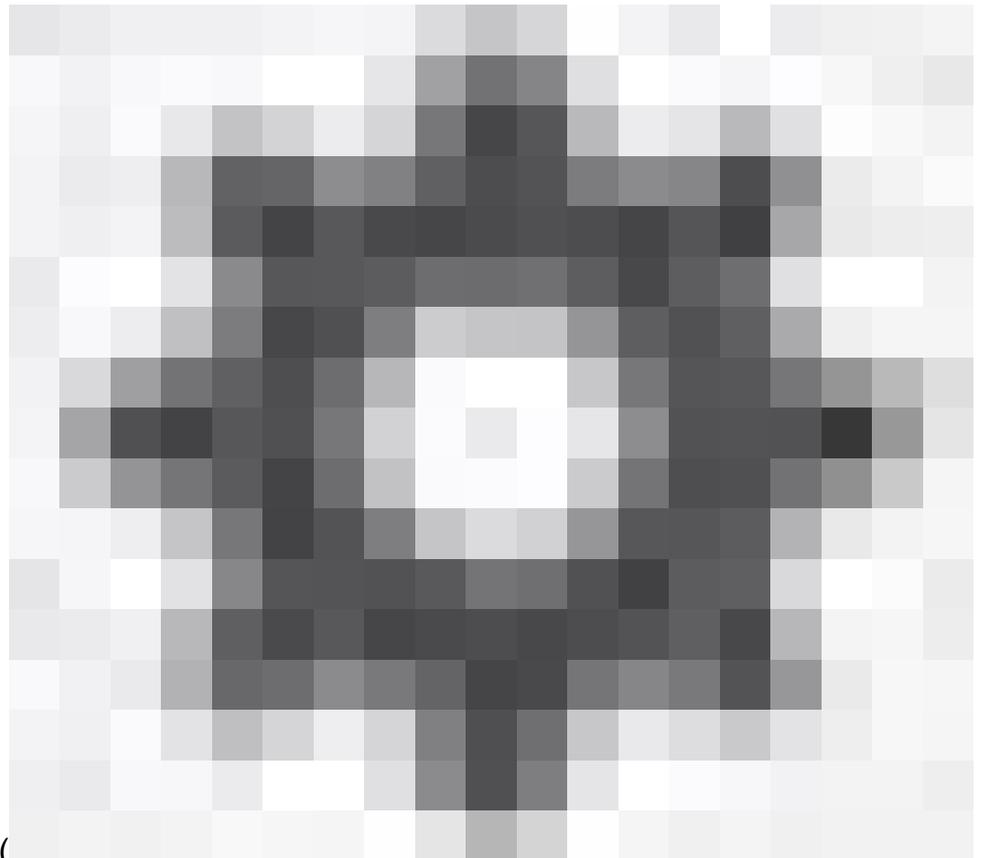
Étape 2. Cliquez sur le lien High Availability sur le côté droit du résumé du périphérique.

High Availability

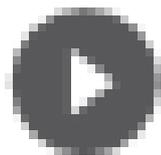
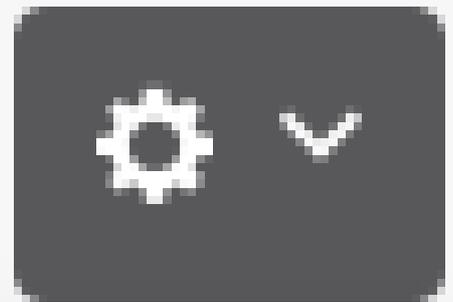
Primary Device: **Active**



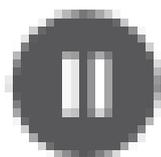
Peer: **Standby**



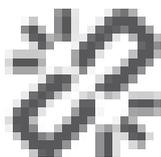
Étape 3. De l'icône de pignon (), choisissez Switch Mode.



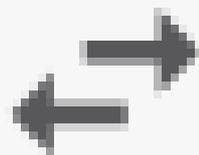
Resume HA



Suspend HA

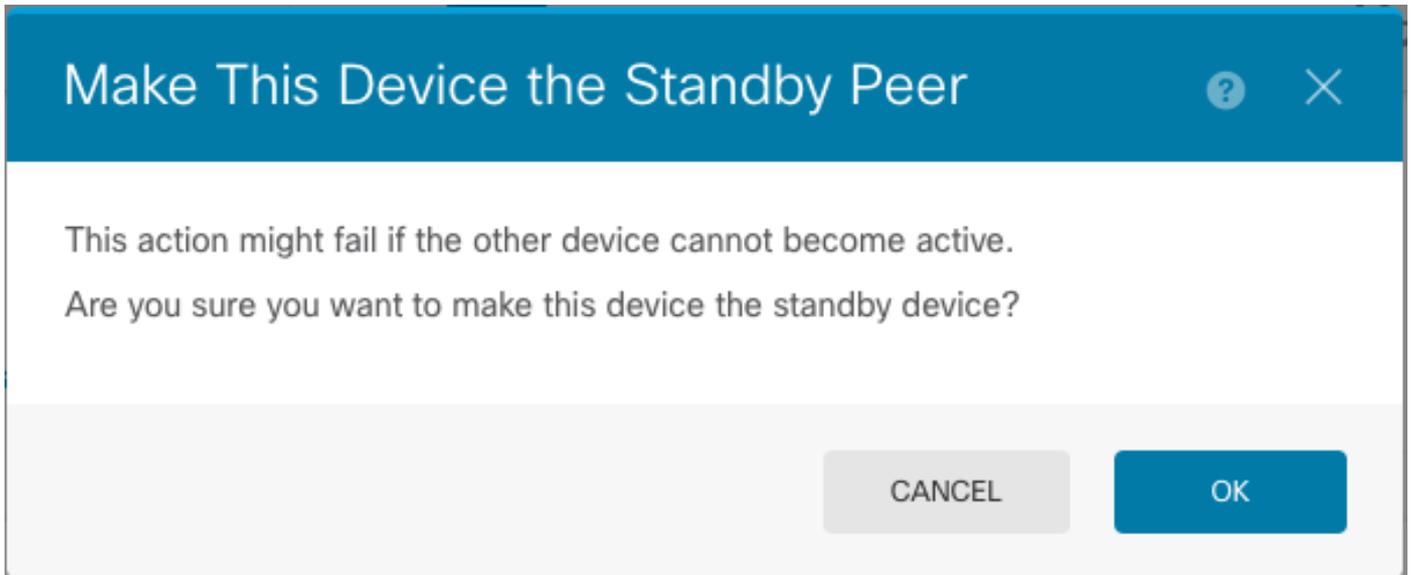


Break HA



Switch Mode

Étape 4. Lisez le message de confirmation et cliquez sur OK.



Le système force le basculement de sorte que l'unité active devienne en veille et que l'unité en veille devienne la nouvelle unité active.

Étape 5. Vérifiez que le résultat est le même que celui sur l'image:



Étape 6. Il est également possible de vérifier à l'aide du lien Historique de basculement et la fenêtre contextuelle de la console CLI doit afficher les résultats suivants :

| 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=====

```

Étape 7. Après la vérification, réactivez l'unité principale.

Tâche 5. Suspension ou reprise de la haute disponibilité

Vous pouvez suspendre une unité dans une paire haute disponibilité. Ceci est utile lorsque :

- Les deux unités sont dans une situation active-active et la résolution de la communication sur la liaison de basculement ne résout pas le problème.
- Vous voulez dépanner une unité active ou en veille et ne voulez pas que les unités basculent pendant ce temps.
- Vous souhaitez empêcher le basculement lors de l'installation d'une mise à niveau logicielle sur le périphérique de secours.

La principale différence entre la suspension de la haute disponibilité et la rupture de la haute disponibilité réside dans le fait que la configuration de haute disponibilité est conservée sur un périphérique à haute disponibilité suspendu. Lorsque vous interrompez la haute disponibilité, la configuration est effacée. Ainsi, vous avez la possibilité de reprendre la haute disponibilité sur un système suspendu, ce qui active la configuration existante et permet aux deux périphériques de fonctionner à nouveau comme une paire de basculement.

Exigence de la tâche :

À partir de l'interface graphique de Secure Firewall Device Manager, suspendez l'unité principale et reprenez la haute disponibilité sur la même unité.

Solution :

Étape 1. Cliquez sur Périphérique.



Device: FPR2130-1

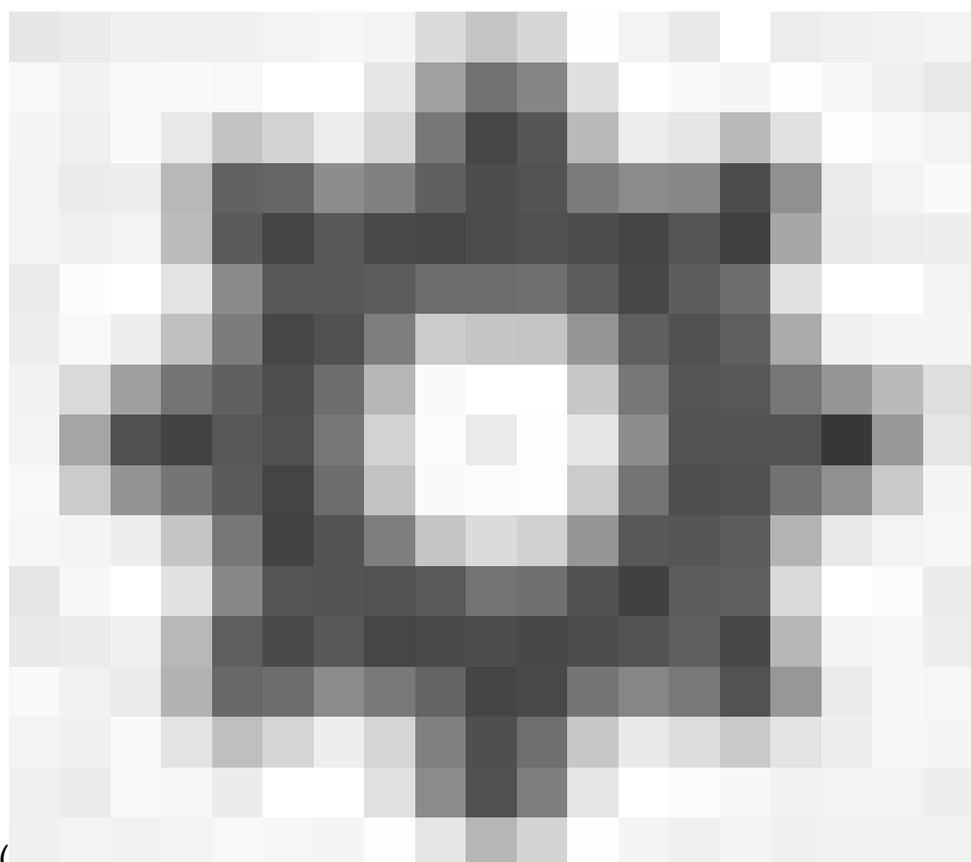
Étape 2. Cliquez sur le lien High Availability sur le côté droit du résumé du périphérique.

High Availability

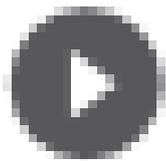
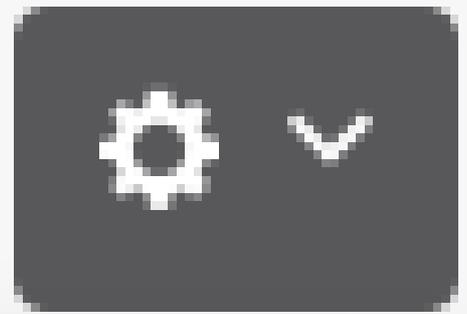
Primary Device: **Active**



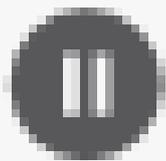
Peer: **Standby**



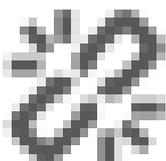
Étape 3. De l'icône de pignon (), sélectionnez Suspendre HA.



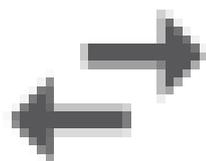
Resume HA



Suspend HA



Break HA



Switch Mode

Étape 4. Lisez le message de confirmation et cliquez sur OK.

Suspend HA Configuration



Suspending high availability on the active unit suspends HA on both the active and standby unit. The active unit will continue to handle user traffic as a stand-alone device, whereas the standby unit will remain inactive. The HA configuration will not be erased.

Do you want to suspend high availability on both the active and standby unit?

CANCEL

OK

Étape 5. Vérifiez que le résultat est le même que celui sur l'image:

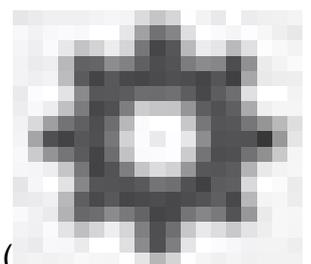
Primary Device

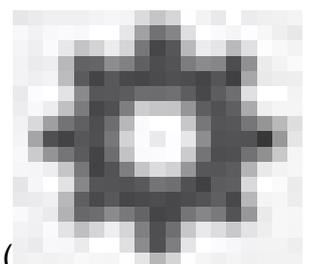
Current Device Mode: **Suspended**  Peer: **Unknown**

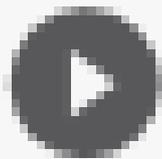
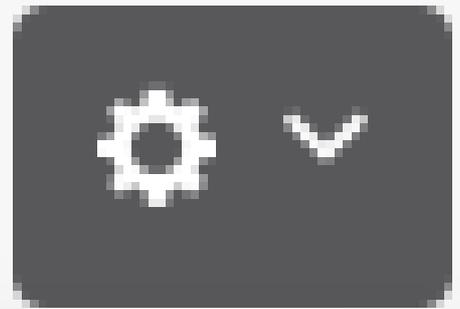


Time of event: 25 Jul 2023, 01:08:01 PM

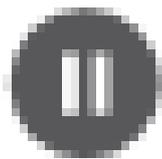
Event description: Set by the config command



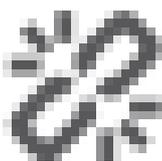
Étape 6. Pour reprendre la haute disponibilité, à partir de l'icône d'engrenage (), sélectionnez Reprendre HA.



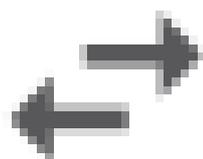
Resume HA



Suspend HA

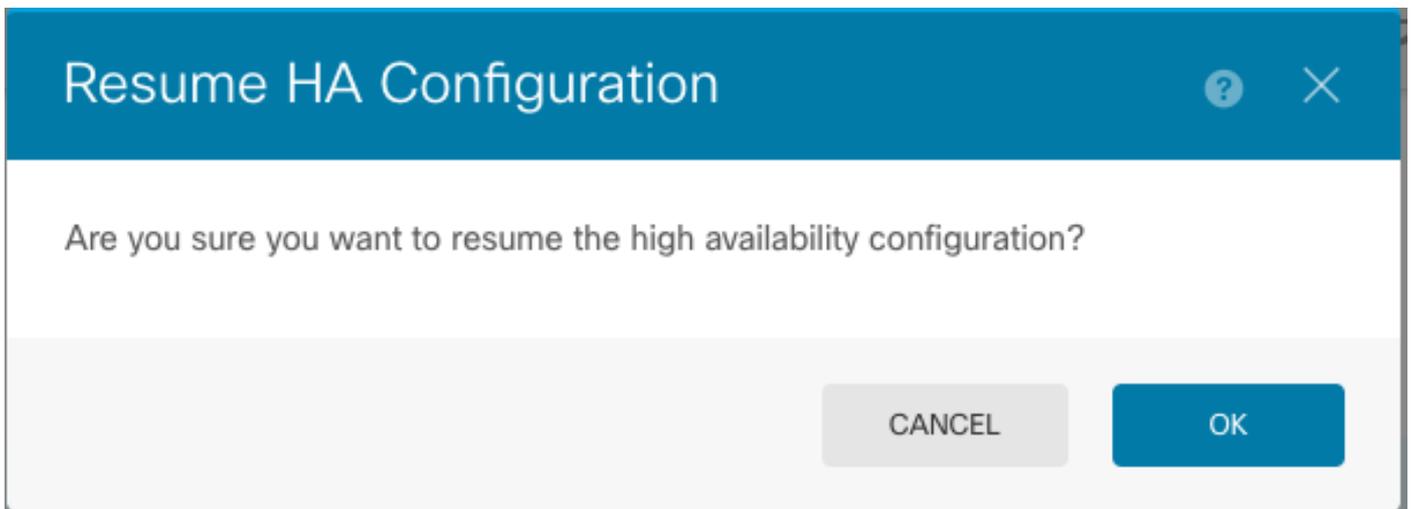


Break HA



Switch Mode

Étape 7. Lisez le message de confirmation et cliquez sur OK.



Étape 5. Vérifiez que le résultat est le même que celui sur l'image:



Tâche 6. Une haute disponibilité exceptionnelle

Si vous ne souhaitez plus que les deux périphériques fonctionnent comme une paire haute disponibilité, vous pouvez interrompre la configuration haute disponibilité. Lorsque vous interrompez la haute disponibilité, chaque périphérique devient un périphérique autonome. Leurs configurations doivent changer comme suit :

- Le périphérique actif conserve la configuration complète telle qu'elle était avant l'interruption, la configuration haute disponibilité étant supprimée.
- Toutes les configurations d'interface sont supprimées du périphérique de secours, en plus de la configuration haute disponibilité. Toutes les interfaces physiques sont désactivées, mais pas les sous-interfaces. L'interface de gestion reste active, ce qui vous permet de vous connecter au périphérique et de le reconfigurer.

Exigence de la tâche :

À partir de l'interface graphique du Gestionnaire de périphériques Secure Firewall, cassez la paire Haute disponibilité.

Solution :

Étape 1. Cliquez sur Périphérique.

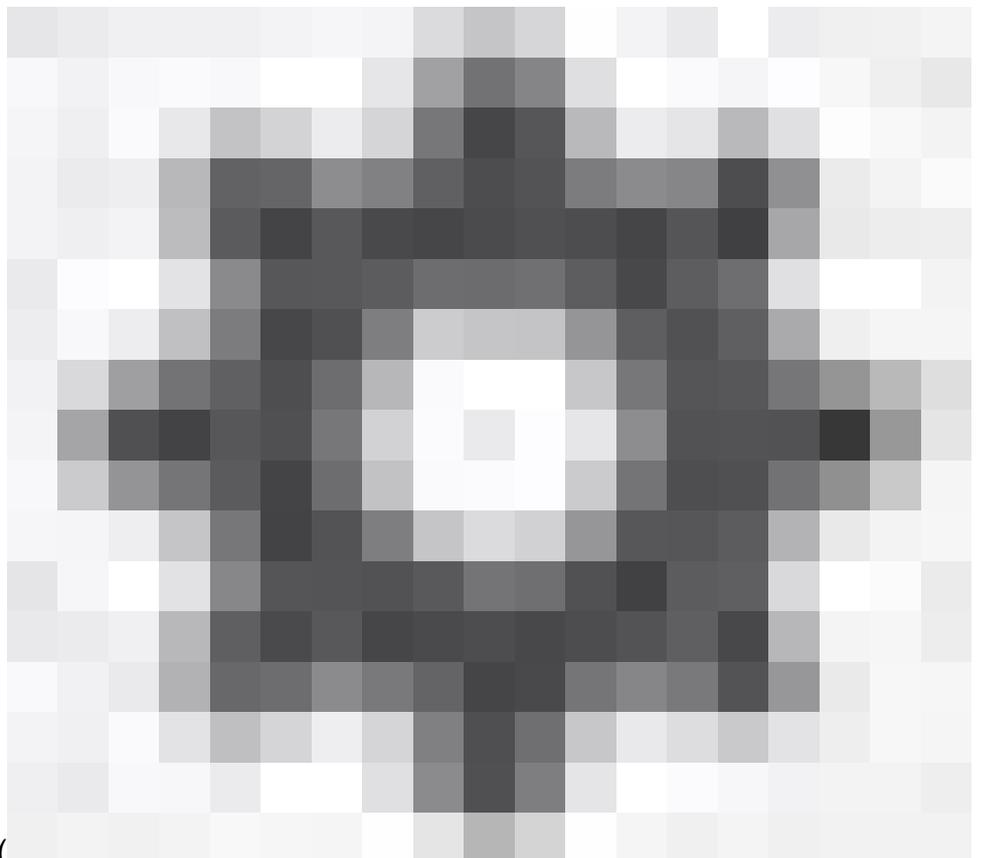


Device: FPR2130-1

Étape 2. Cliquez sur le lien High Availability sur le côté droit du résumé du périphérique.

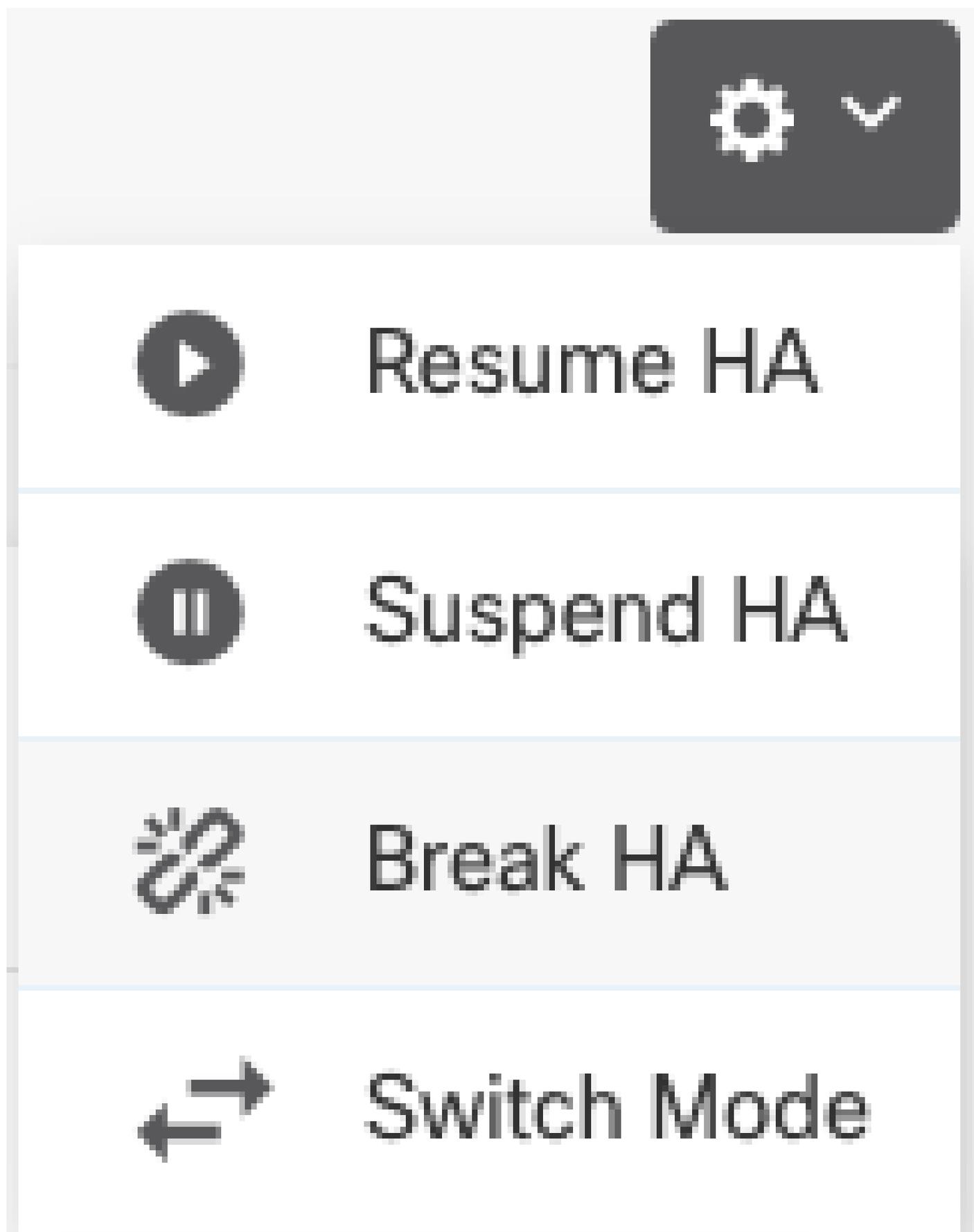
[High Availability](#)

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



Étape 3. De l'icône de pignon (

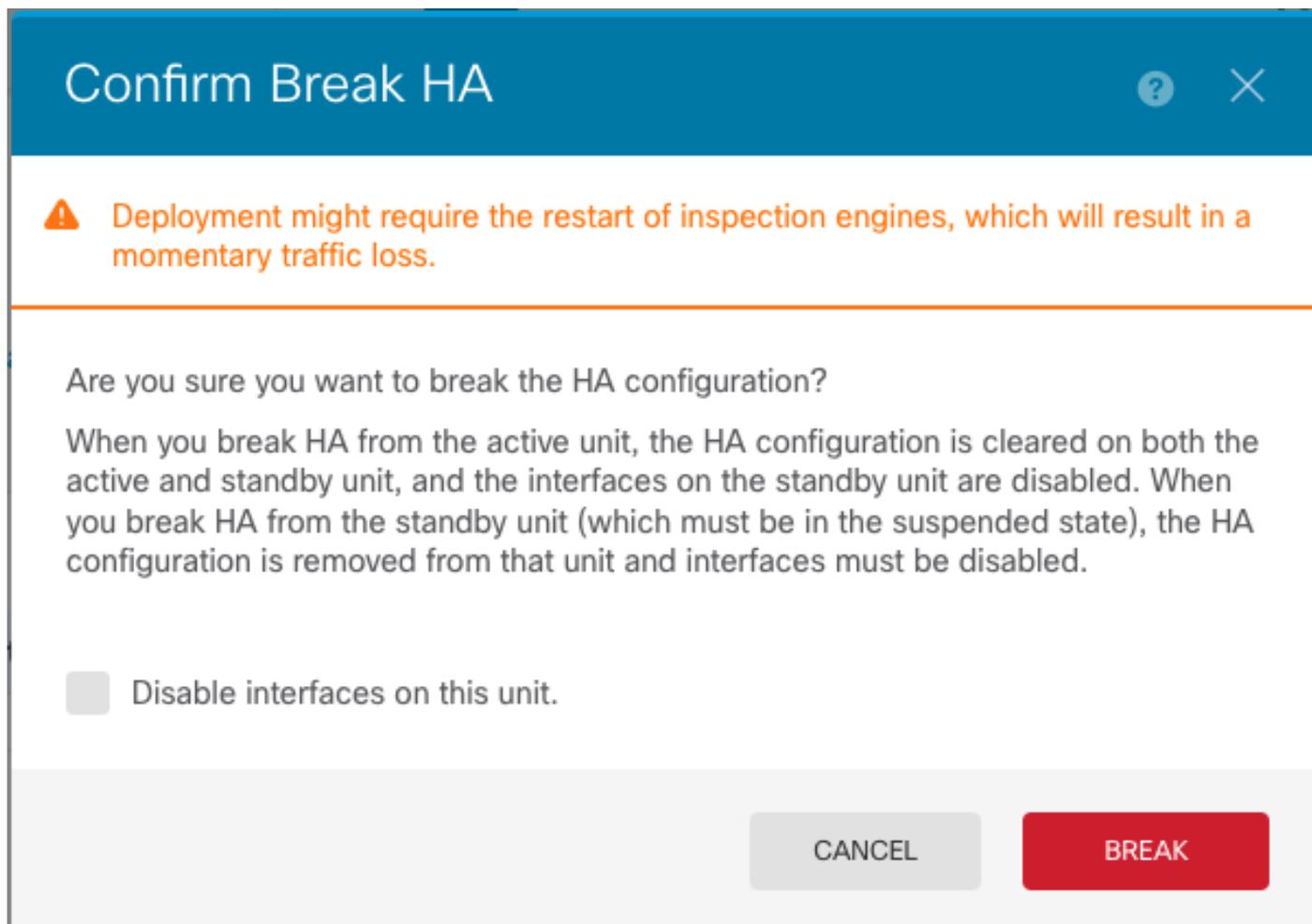
), choisissez Break HA.



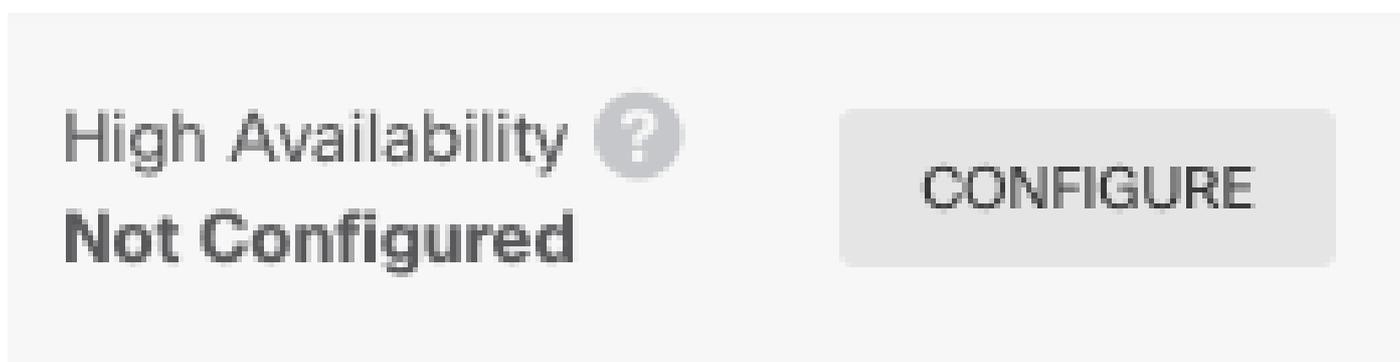
Étape 4. Lisez le message de confirmation, décidez si vous souhaitez sélectionner l'option pour désactiver les interfaces, et cliquez sur Break.

Vous devez sélectionner l'option permettant de désactiver les interfaces si vous interrompez la haute disponibilité à partir de l'unité en veille.

Le système déploie immédiatement vos modifications sur ce périphérique et sur le périphérique homologue (si possible). Le déploiement peut prendre quelques minutes pour s'effectuer sur chaque périphérique et pour que chaque périphérique devienne indépendant.



Étape 5. Vérifiez le résultat comme indiqué dans l'image :



Informations connexes

- Toutes les versions du guide de configuration de Cisco Secure Firewall Device Manager sont disponibles ici

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

- Le centre d'assistance technique international (TAC) de Cisco recommande vivement ce guide visuel pour des connaissances pratiques approfondies sur les technologies de sécurité nouvelle génération Cisco Firepower :

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

- Pour toutes les notes techniques de configuration et de dépannage relatives aux technologies Firepower

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

- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.