

Configure o Gerenciador de dispositivos do Secure Firewall em alta disponibilidade

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Tarefa 1. Verificar condições](#)

[Tarefa 2. Configure o Gerenciador de dispositivos do Secure Firewall em alta disponibilidade](#)

[Diagrama de Rede](#)

[Habilitar alta disponibilidade no Gerenciador de dispositivos de firewall seguro na unidade primária](#)

[Ative a alta disponibilidade no Gerenciador de dispositivos de firewall seguro na unidade secundária](#)

[Concluir A Configuração Das Interfaces](#)

[Tarefa 3. Verificar a Alta Disponibilidade do FDM](#)

[Tarefa 4. Alternar entre as funções de failover](#)

[Tarefa 5. Suspendendo ou retomando a alta disponibilidade](#)

[Tarefa 6. Quebrando a alta disponibilidade](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e verificar o Gerenciador de Dispositivos de Firewall Seguro (FDM) Alta Disponibilidade (HA) em Dispositivos de Firewall Seguro.

Pré-requisitos

Requisitos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 2xDispositivo de segurança Cisco Secure Firewall 2100
- Executando o FDM versão 7.0.5 (compilação 72)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Tarefa 1. Verificar condições

Requisito da tarefa:

Verifique se os dois dispositivos do FDM atendem aos requisitos de nota e podem ser configurados como unidades de HA.

Solução:

Etapa 1. Conecte ao IP de gerenciamento do equipamento usando SSH e verifique o hardware do módulo.

Verifique com o comando `show version` a versão de hardware e software do dispositivo primário:

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

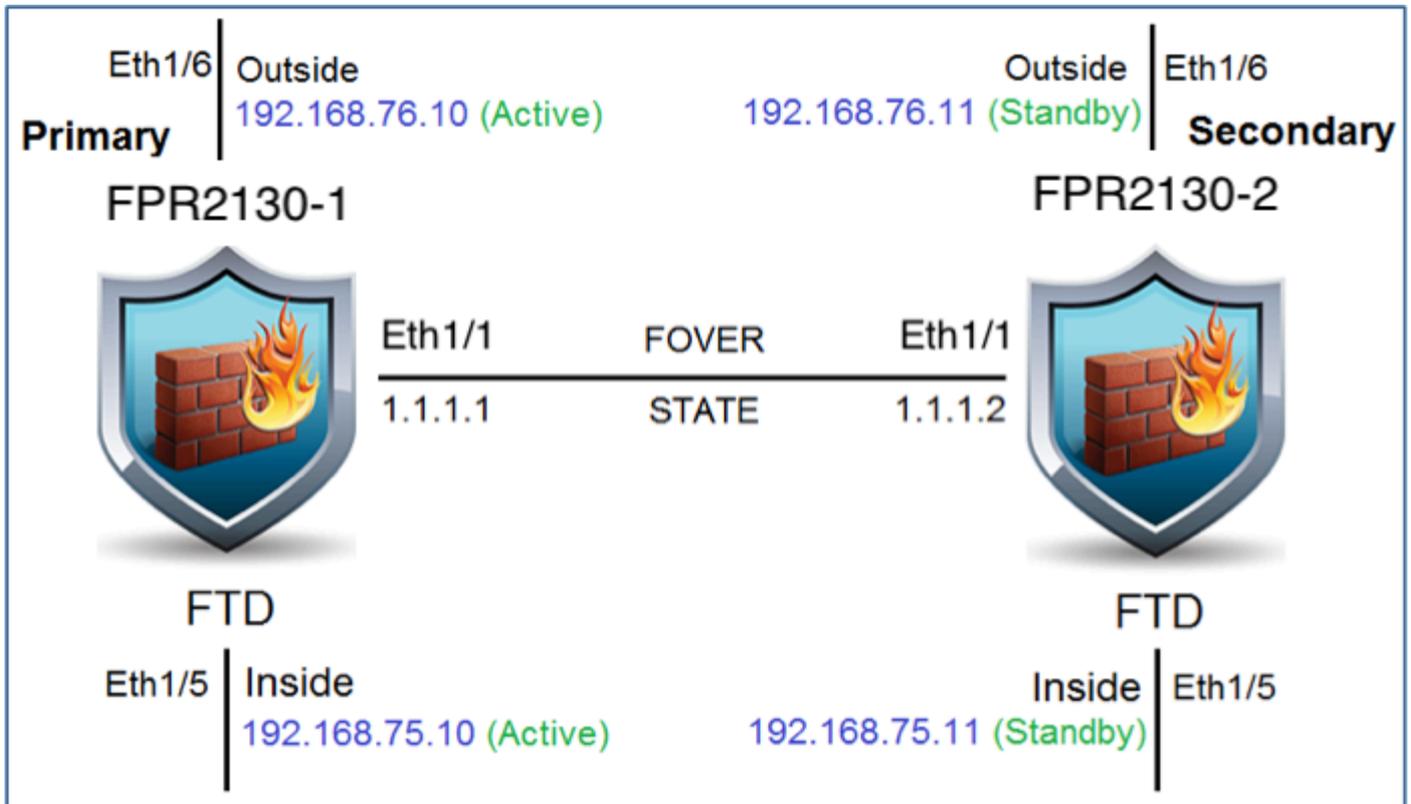
Verifique a versão do hardware e do software do dispositivo secundário:

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

Tarefa 2. Configure o Gerenciador de dispositivos do Secure Firewall em alta disponibilidade

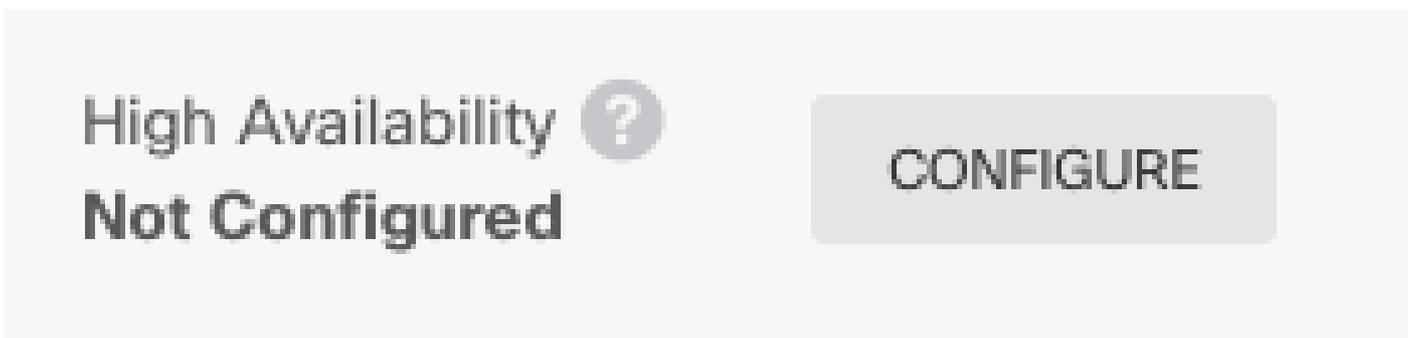
Diagrama de Rede

Configure a alta disponibilidade (HA) ativa/em standby de acordo com este diagrama:

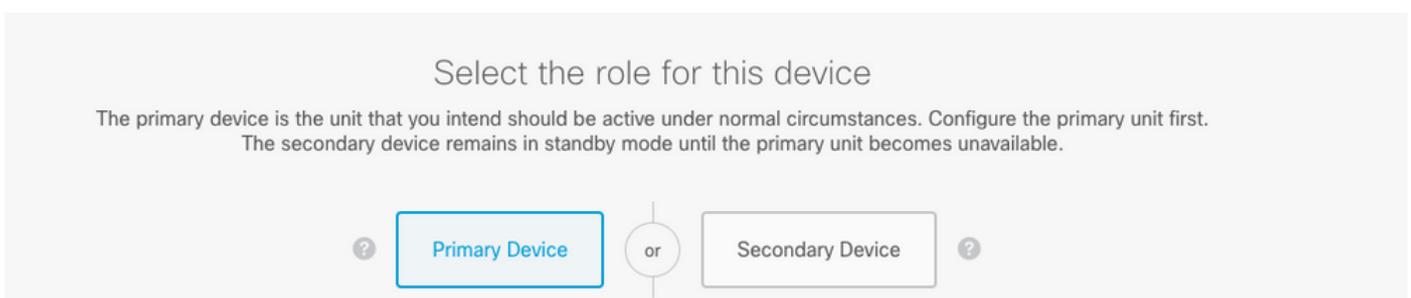


Habilitar alta disponibilidade no Gerenciador de dispositivos de firewall seguro na unidade primária

Etapa 1. Para configurar o Failover do FDM, navegue para Dispositivo e clique em Configurar ao lado do grupo Alta Disponibilidade:



Etapa 2. Na página Alta disponibilidade, clique na caixa Dispositivo primário:



Aviso: Selecione a unidade correta como a unidade principal. Todas as configurações na

unidade primária selecionada são replicadas na unidade FTD secundária selecionada. Como resultado da replicação, a configuração atual na unidade secundária pode ser substituída.

Etapa 3. Defina as configurações de link de failover e link de estado:

Neste exemplo, o link de estado tem as mesmas configurações que o link de failover.

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 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

Etapa 4. Clique em Ativar HA

Etapa 5. Copie a configuração de alta disponibilidade para a área de transferência na mensagem de confirmação para colá-la na unidade secundária.

✕

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

O sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro.

A configuração também é copiada para a área de transferência. Você pode usar a cópia para configurar rapidamente a unidade secundária. Para maior segurança, a chave de criptografia não é incluída na cópia da área de transferência.

Nesse ponto, você deve estar na página Alta disponibilidade e o status do dispositivo deve ser "Negociando". O status deve mudar para Ativo antes mesmo de você configurar o peer, que deve aparecer como Falha até que você o configure.

High Availability

Primary Device: **Active**



Peer: **Failed**

Ative a alta disponibilidade no Gerenciador de dispositivos de firewall seguro na unidade secundária

Depois de configurar o dispositivo primário para alta disponibilidade ativa/em espera, você deve configurar o dispositivo secundário. Efetue login no FDM nesse dispositivo e execute este procedimento.

Etapa 1. Para configurar o Failover do FDM, navegue para Dispositivo e clique em Configurar ao lado do grupo Alta Disponibilidade:

High Availability 
Not Configured

CONFIGURE

Etapa 2. Na página Alta disponibilidade, clique na caixa Dispositivo secundário:

Device Summary

High Availability

How High Availability Works

Select the role for this device

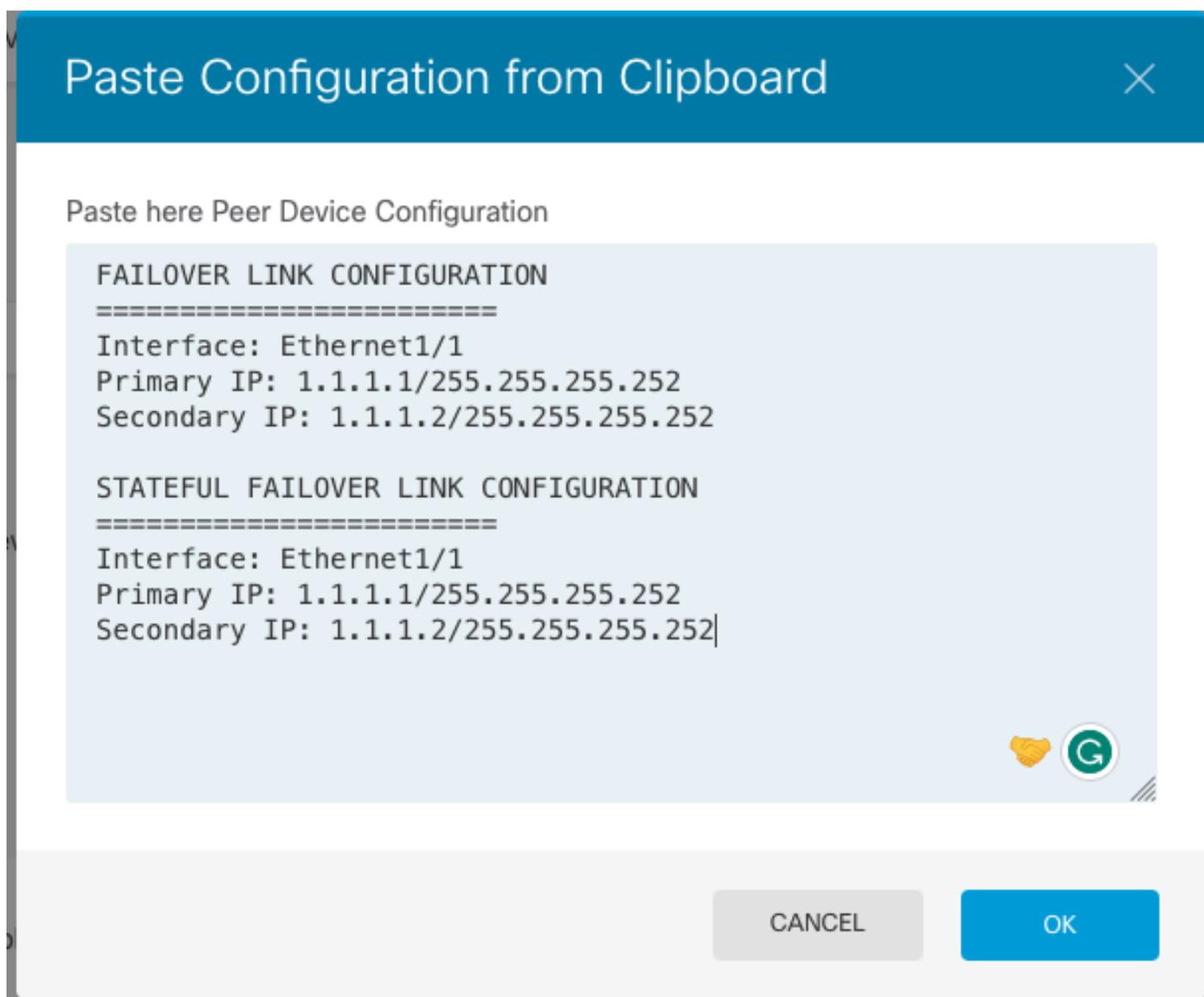
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first.
The secondary device remains in standby mode until the primary unit becomes unavailable.

Primary Device or Secondary Device

Etapa 3. Escolha uma destas opções:

- Método fácil — Clique no botão Colar da área de transferência, cole na configuração e clique em OK. Isso atualiza os campos com os valores apropriados, que podem ser verificados.
- Método manual — Configure os links de failover dinâmico e de failover de estado

diretamente. Insira exatamente as mesmas configurações no dispositivo secundário que você inseriu no dispositivo primário.



Etapa 4. Clique em Ativar HA

O sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro.

Depois que a configuração for concluída, você receberá uma mensagem informando que configurou o HA. Clique em Got It para descartar a mensagem.

Nesse momento, você deve estar na página Alta disponibilidade e o status do dispositivo deve indicar que esse é o dispositivo secundário. Se a junção com o dispositivo primário tiver sido bem-sucedida, o dispositivo sincronizará com o primário e, eventualmente, o modo deverá ser Standby e o peer deverá ser Ative.

High Availability

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

Concluir A Configuração Das Interfaces

Etapa 1. Para configurar as Interfaces do FDM, navegue até Dispositivo e clique em Exibir Todas as Interfaces:

Interfaces

Connected

Enabled 2 of 17

View All Interfaces



Etapa 2. Selecione e edite as configurações de interfaces como mostrado nas imagens:

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

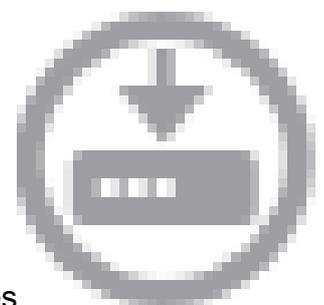
/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK



Etapa 3. Depois de configurar as alterações, clique em Alterações Pendentes e implantar agora.

Tarefa 3. Verificar a Alta Disponibilidade do FDM

Requisito da tarefa:

Verifique as configurações de Alta Disponibilidade na GUI do FDM e na CLI do FDM.

Solução:

Etapa 1. Navegue até Device e verifique as configurações de alta disponibilidade:

Device Summary
High Availability

Primary Device
Current Device Mode: **Active** Peer: **Standby** [Failover History](#) [Deployment History](#)

High Availability Configuration

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

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
Number of failed interfaces exceeds	1

INTERFACE TIMING CONFIGURATION

Poll Time	Hold Time	
5000	25000	seconds milliseconds
<small>500-15000 milliseconds</small>	<small>5000-75000 milliseconds</small>	

PEER TIMING CONFIGURATION

Poll Time	Hold Time	
1000	15000	seconds milliseconds
<small>200-15000 milliseconds</small>	<small>800-45000 milliseconds</small>	

SAVE

Etapa 2. Conecte-se à CLI do Dispositivo Primário do FDM usando SSH e valide com o 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

```

Etapa 3. Faça o mesmo no dispositivo secundário.

Etapa 4. Valide o estado atual com o 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
```

Etapa 5. Verifique a configuração a partir da unidade Primária com o comando show running-config failover e 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
```

Tarefa 4. Alternar entre as funções de failover

Requisito da tarefa:

Na interface gráfica do Secure Firewall Device Manager, alterne as funções de failover de Principal/Ativo, Secundário/Em espera para Principal/Em espera, Secundário/Ativo

Solução:

Etapa 1. Clique em Dispositivo



Device: FPR2130-1

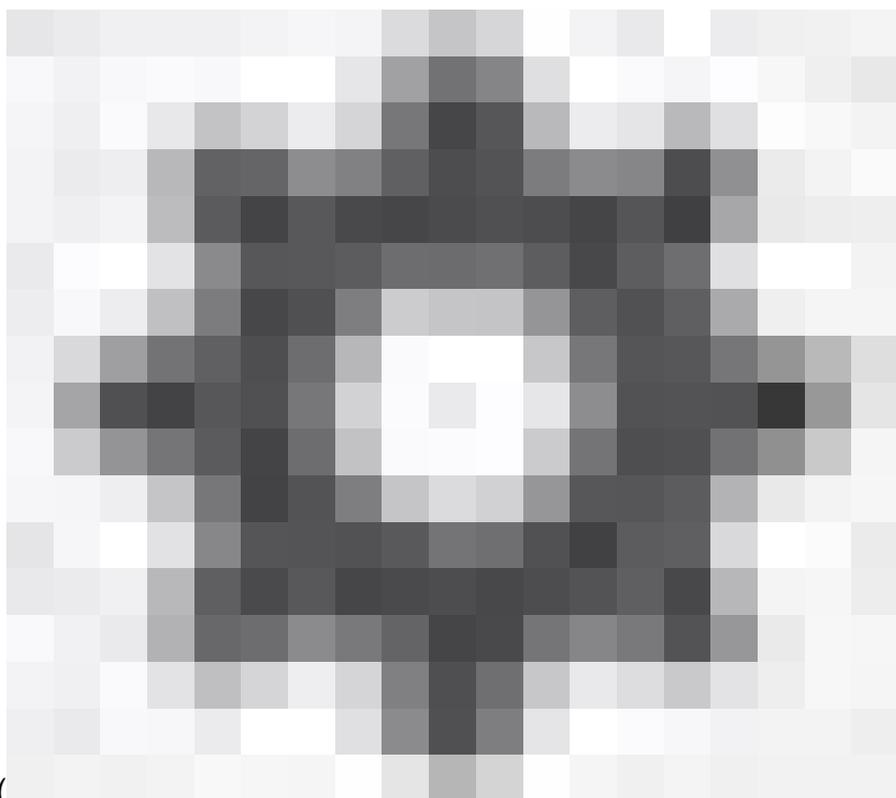
Etapa 2. Clique no link High Availability no lado direito do resumo do dispositivo.

High Availability

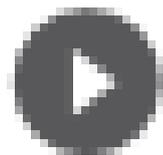
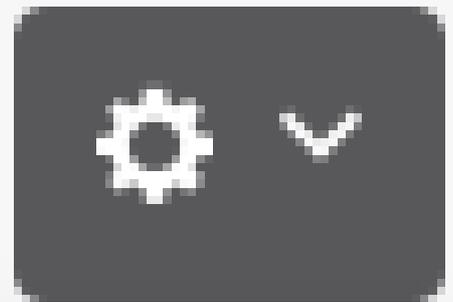
Primary Device: **Active**



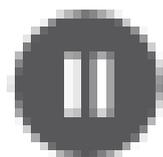
Peer: **Standby**



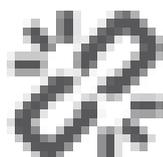
Etapa 3. Do ícone de engrenagem (), seleccione Switch Mode.



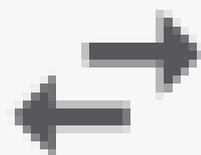
Resume HA



Suspend HA

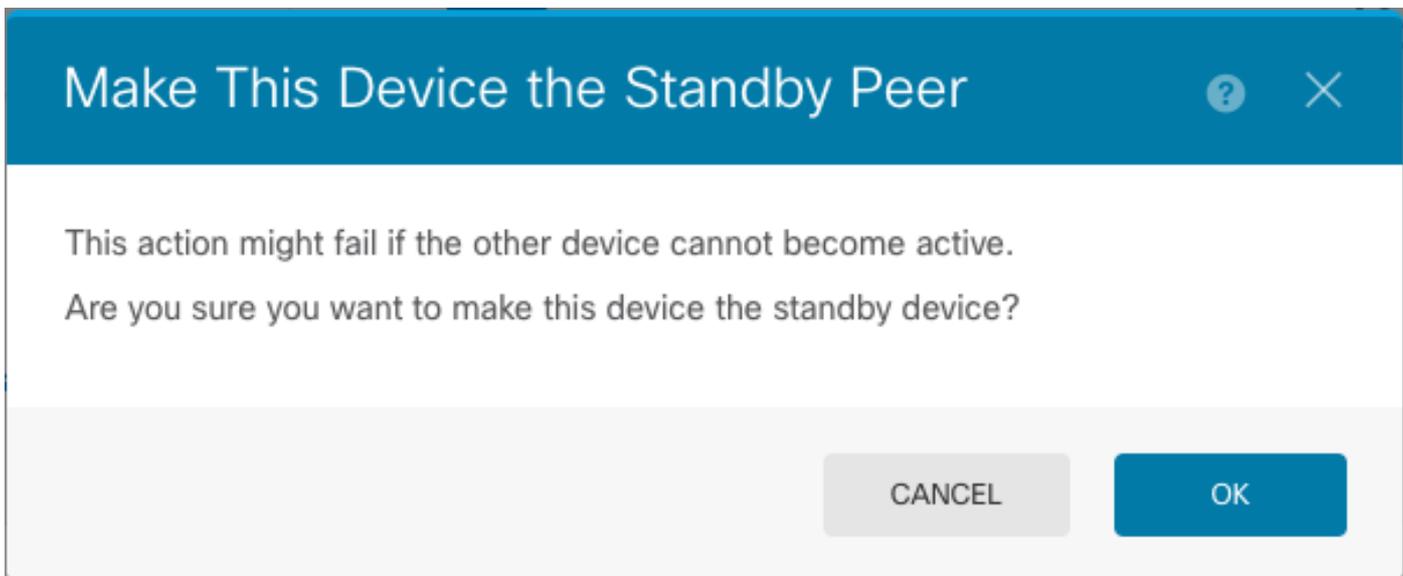


Break HA



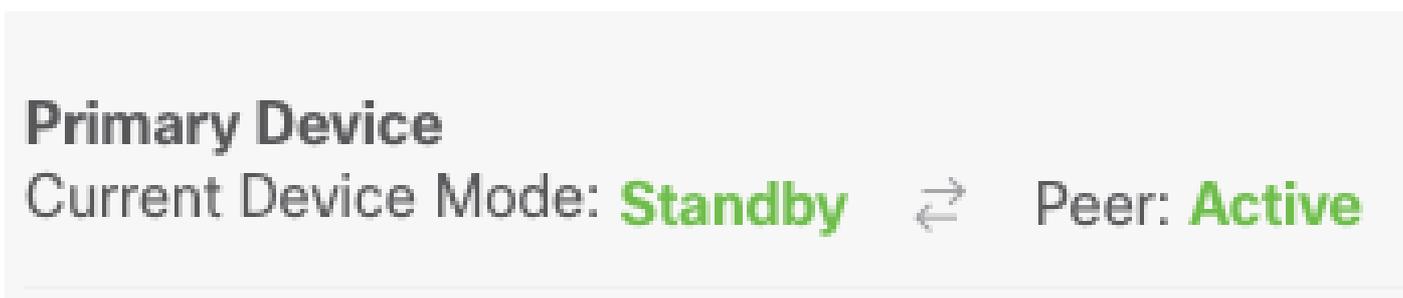
Switch Mode

Etapa 4. Leia a mensagem de confirmação e clique em OK.



O sistema força o failover para que a unidade ativa se torne em espera e a unidade em espera se torne a nova unidade ativa.

Etapa 5. Verifique o resultado conforme mostrado na imagem:



Etapa 6. Também é possível verificar usando o link Histórico de Failover e o pop-up Console CLI deve mostrar os 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=====

```

Passo 7. Após a verificação, ative a unidade primária novamente.

Tarefa 5. Suspendendo ou retomando a alta disponibilidade

Você pode suspender uma unidade em um par de alta disponibilidade. Isso é útil quando:

- As duas unidades estão em uma situação ativo-ativo e corrigir a comunicação no link de failover não corrige o problema.
- Você deseja solucionar problemas de uma unidade ativa ou em espera e não deseja que as unidades falhem durante esse período.
- Você deseja impedir o failover durante a instalação de um upgrade de software no dispositivo de standby.

A principal diferença entre suspender o HA e interromper o HA é que em um dispositivo HA suspenso, a configuração de alta disponibilidade é mantida. Quando você quebra o HA, a configuração é apagada. Assim, você tem a opção de retomar o HA em um sistema suspenso, o que ativa a configuração existente e faz com que os dois dispositivos funcionem como um par de failover novamente.

Requisito da tarefa:

Na interface gráfica do Gerenciador de dispositivos do Secure Firewall, suspenda a unidade principal e reinicie a alta disponibilidade na mesma unidade.

Solução:

Etapa 1. Clique em Device.



Device: FPR2130-1

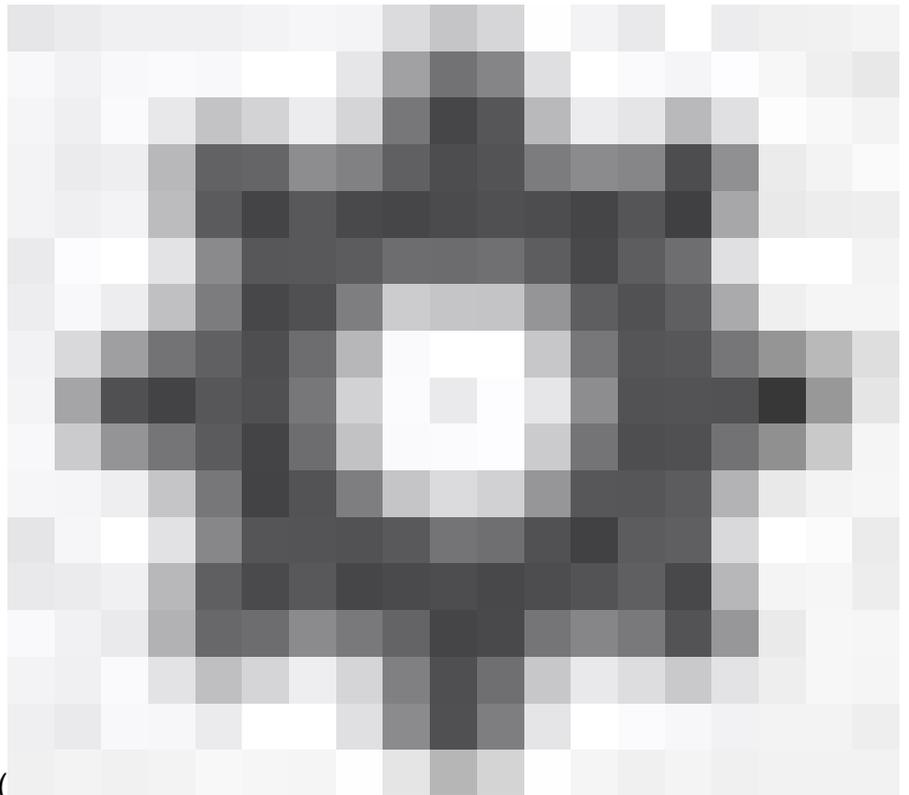
Etapa 2. Clique no link High Availability no lado direito do resumo do dispositivo.

High Availability

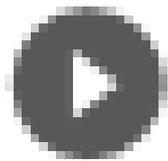
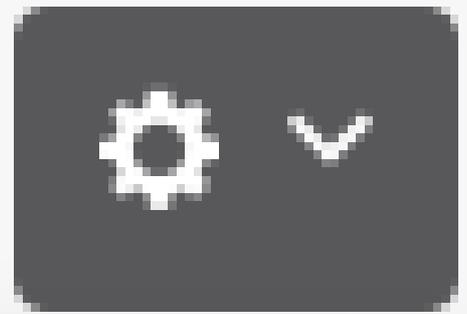
Primary Device: **Active**



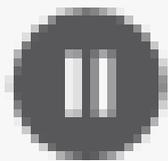
Peer: **Standby**



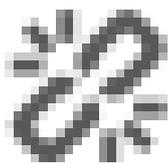
Etapa 3. Do ícone de engrenagem (), escolha Suspend HA.



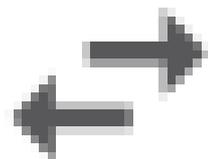
Resume HA



Suspend HA



Break HA



Switch Mode

Etapa 4. Leia a mensagem de confirmação e clique em 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

Etapa 5. Verifique o resultado conforme mostrado na imagem:

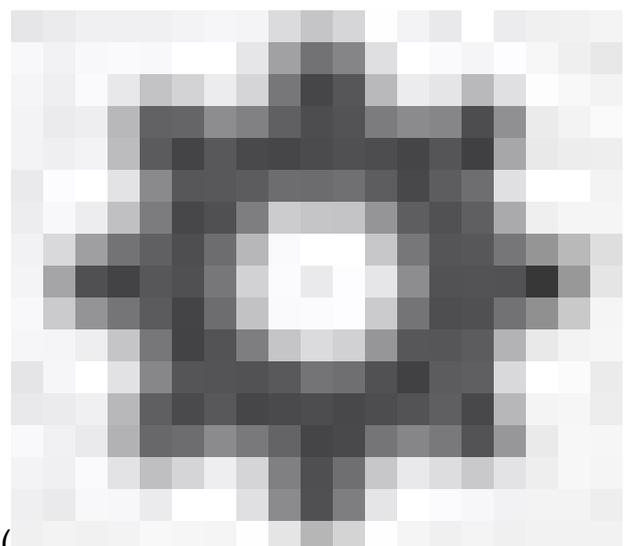
Primary Device

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

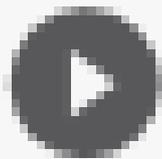
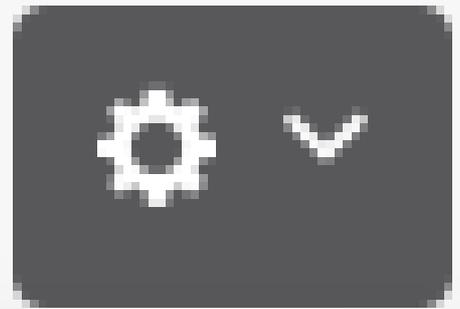


Time of event: 25 Jul 2023, 01:08:01 PM

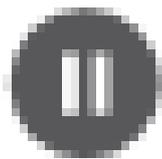
Event description: Set by the config command



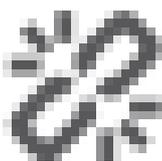
Etapa 6. Para retomar o HA, no ícone da engrenagem (), escolha Retomar HA.



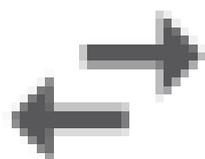
Resume HA



Suspend HA

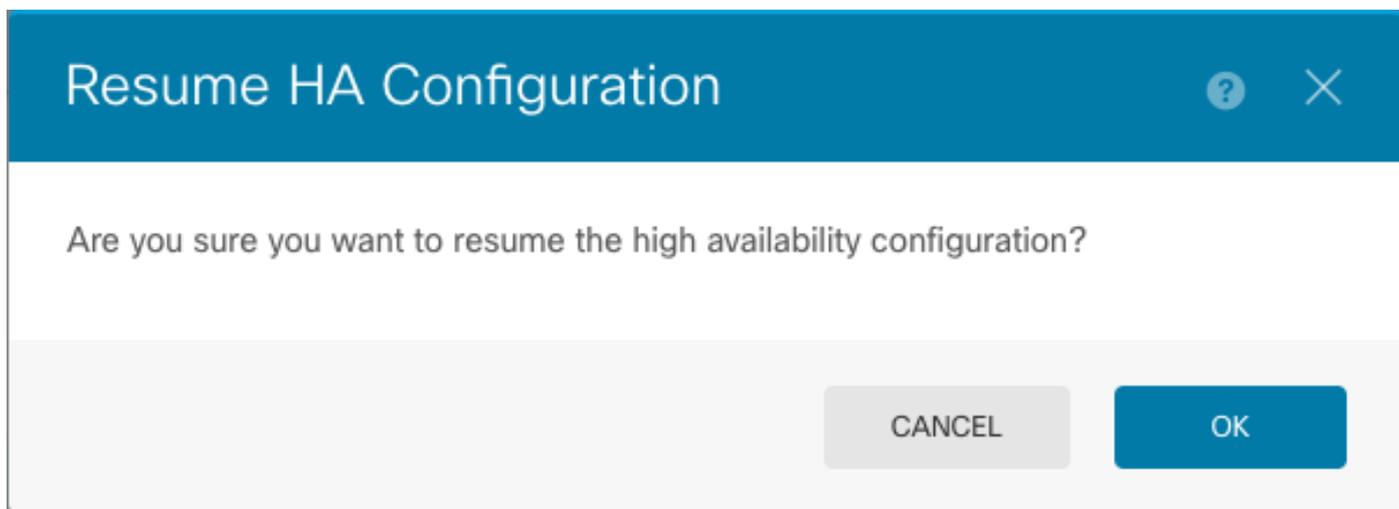


Break HA

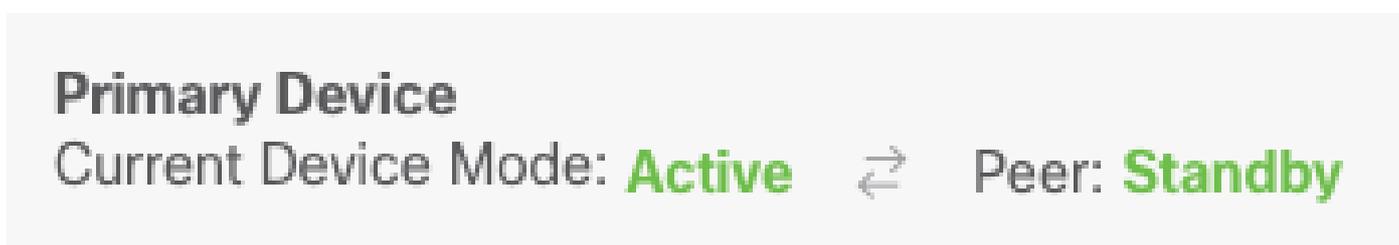


Switch Mode

Passo 7. Leia a mensagem de confirmação e clique em OK.



Etapa 5. Verifique o resultado conforme mostrado na imagem:



Tarefa 6. Quebrando a alta disponibilidade

Se não quiser mais que os dois dispositivos operem como um par de alta disponibilidade, você pode quebrar a configuração de HA. Quando você quebra o HA, cada dispositivo se torna um dispositivo autônomo. Suas configurações devem ser alteradas como:

- O dispositivo ativo mantém a configuração completa como antes da interrupção, com a configuração de HA removida.
- O dispositivo em standby tem todas as configurações de interface removidas, além da configuração de HA. Todas as interfaces físicas estão desabilitadas, embora as subinterfaces não estejam desabilitadas. A interface de gerenciamento permanece ativa, assim você pode fazer login no dispositivo e reconfigurá-lo.

Requisito da tarefa:

Na interface gráfica do Gerenciador de dispositivos do Secure Firewall, quebre o par de alta disponibilidade.

Solução:

Etapa 1. Clique em Device.



Device: FPR2130-1

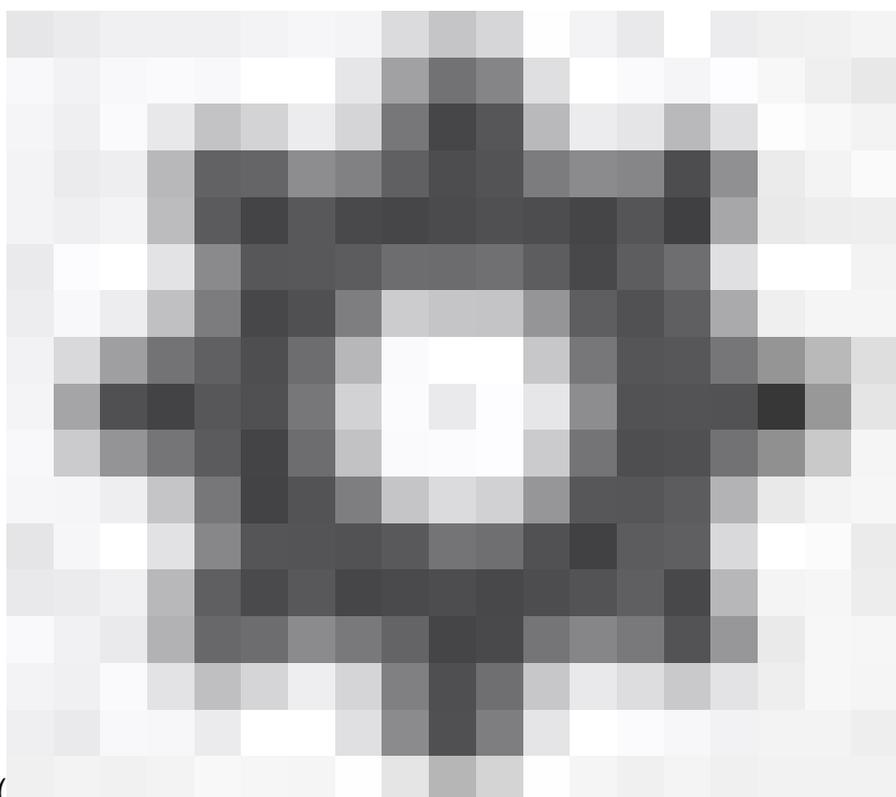
Etapa 2. Clique no link High Availability no lado direito do resumo do dispositivo.

[High Availability](#)

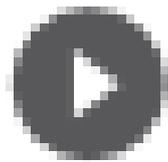
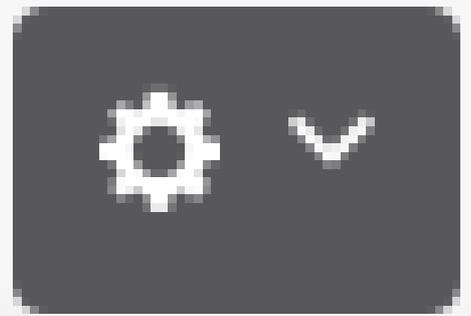
Primary Device: **Active**



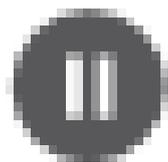
Peer: **Standby**



Etapa 3. Do ícone de engrenagem (), escolha Quebrar HA.



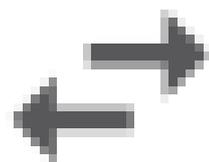
Resume HA



Suspend HA



Break HA



Switch Mode

Etapa 4. Leia a mensagem de confirmação, decida se deseja selecionar a opção para desativar interfaces e clique em Break.

Você deve selecionar a opção para desativar as interfaces se estiver quebrando o HA da unidade

de standby.

O sistema implementa imediatamente suas alterações neste dispositivo e no dispositivo par (se possível). Pode levar alguns minutos para que a implantação seja concluída em cada dispositivo e para que cada dispositivo se torne independente.

Confirm Break HA ? ×

⚠ Deployment might require the restart of inspection engines, which will result in a momentary traffic loss.

Are you sure you want to break the HA configuration?

When you break HA from the active unit, the HA configuration is cleared on both the active and standby unit, and the interfaces on the standby unit are disabled. When you break HA from the standby unit (which must be in the suspended state), the HA configuration is removed from that unit and interfaces must be disabled.

Disable interfaces on this unit.

CANCEL BREAK

Etapa 5. Verifique o resultado conforme mostrado na imagem:

High Availability ?
Not Configured

CONFIGURE

Informações Relacionadas

- Todas as versões do guia de configuração do Cisco Secure Firewall Device Manager podem ser encontradas aqui

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

- O Cisco Global Technical Assistance Center (TAC) recomenda enfaticamente este guia visual para conhecimento prático aprofundado sobre as tecnologias de segurança de próxima geração Cisco Firepower:

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

- Para todas as Notas técnicas de configuração e solução de problemas que pertencem às tecnologias Firepower

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

- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.