

在高可用性下配置Secure Firewall设备管理器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[任务1.检验条件](#)

[任务2.在高可用性下配置Secure Firewall设备管理器](#)

[网络图](#)

[在主设备的安全防火墙设备管理器上启用高可用性](#)

[在辅助设备的安全防火墙设备管理器上启用高可用性](#)

[完成接口配置](#)

[任务3.验证FDM高可用性](#)

[任务4.切换故障切换角色](#)

[任务5.暂停或恢复高可用性](#)

[任务6.突破高可用性](#)

[相关信息](#)

简介

本文档介绍如何在安全防火墙上配置和验证安全防火墙设备管理器(FDM)高可用性(HA)。

先决条件

要求

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 2x思科安全防火墙2100安全设备
- 运行FDM版本7.0.5 (内部版本72)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

任务1.检验条件

任务要求：

验证两台FDM设备均符合注释要求，且可以配置为HA设备。

解决方案：

步骤1:使用SSH连接到设备管理IP并验证模块硬件。

使用show version命令验证主设备硬件和软件版本：

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

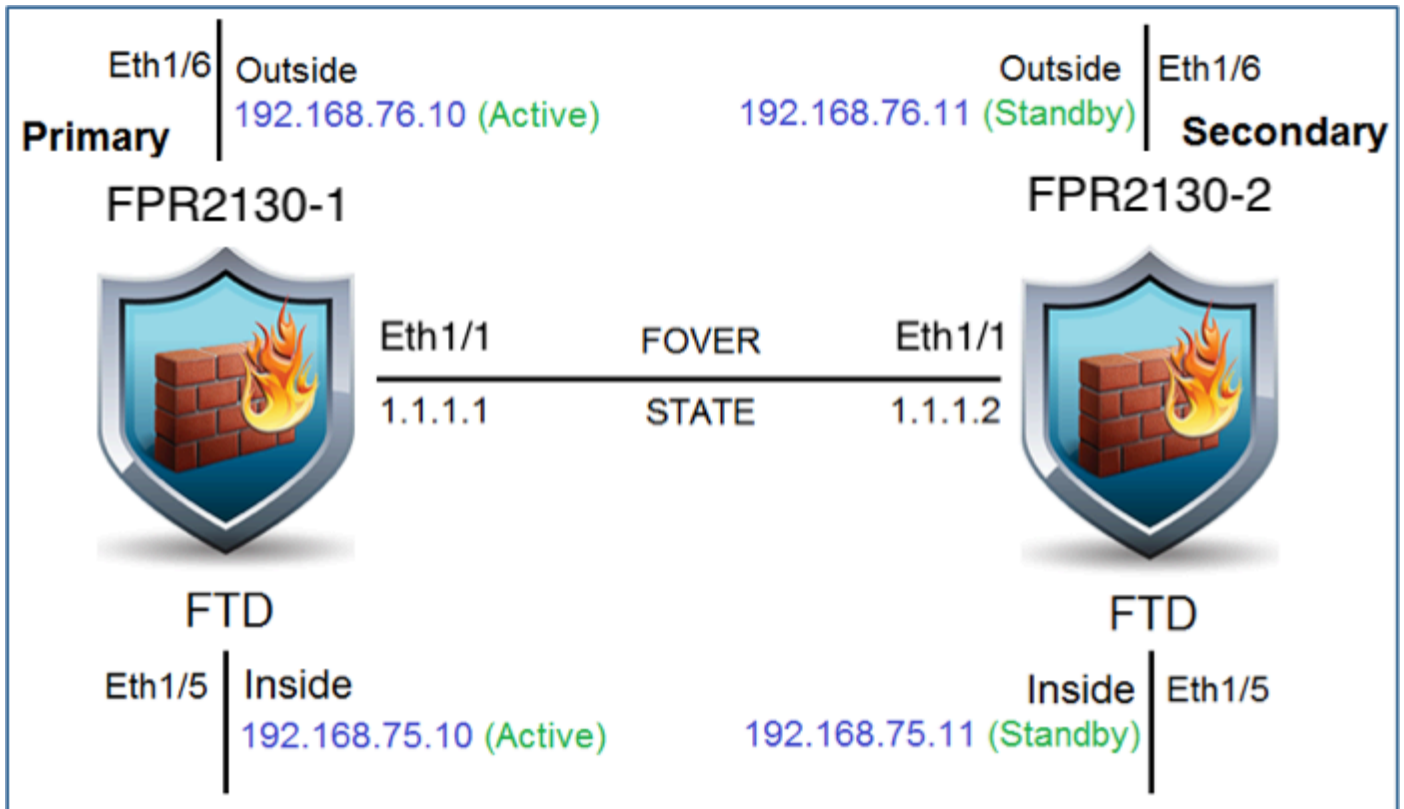
验证辅助设备的硬件和软件版本：

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

任务2.在高可用性下配置Secure Firewall设备管理器

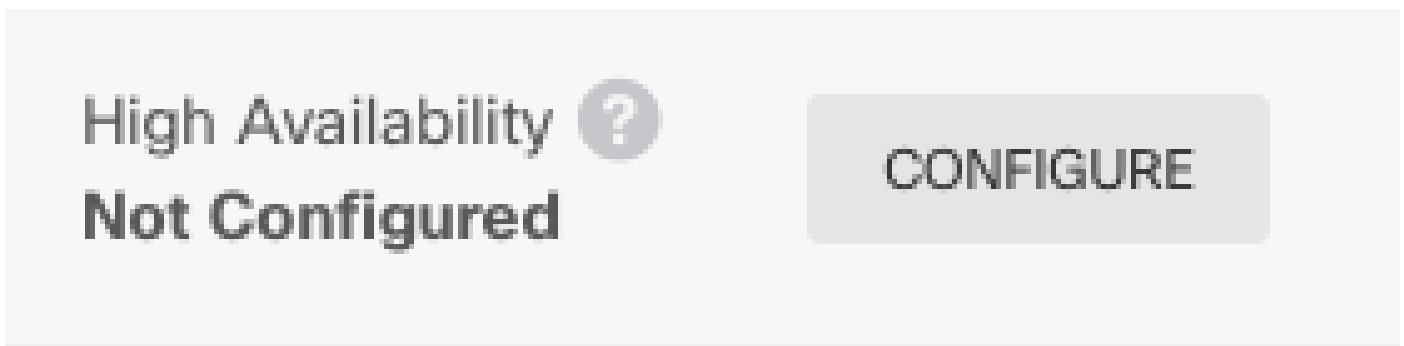
网络图

根据下图配置主用/备用高可用性(HA):

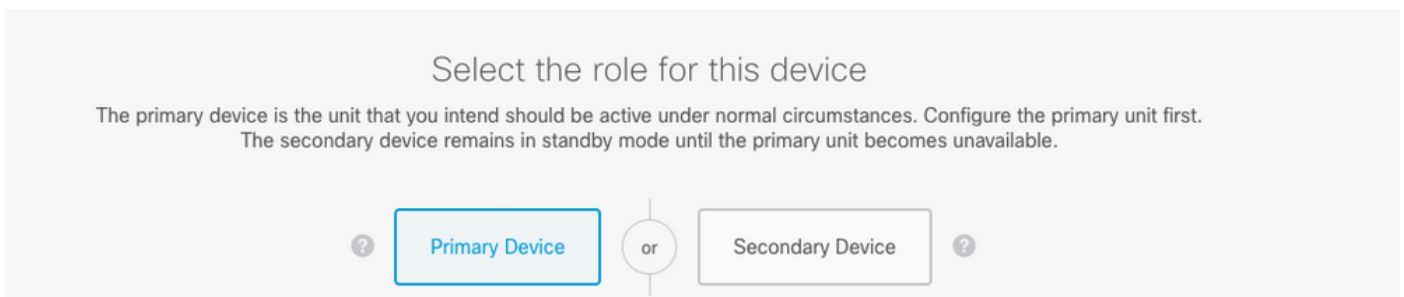


在主设备的安全防火墙设备管理器上启用高可用性

步骤1:要配置FDM故障切换，请导航到Device，然后单击High Availability组旁边的Configure:



第二步：在High Availability页面上，点击Primary Device框：



警告：确保选择正确的设备作为主要设备。所选主设备上的所有配置都将复制到所选辅助FTD设备。通过复制，可以替换辅助设备上的当前配置。

第三步：配置故障切换链路和状态链路设置：

在本示例中，状态链路和故障切换链路具有相同的设置。

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

第四步：点击Activate HA

第五步：将HA配置复制到确认消息上的剪贴板，以将其粘贴到辅助设备上。

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

系统立即将配置部署到设备。您无需启动部署作业。如果您没有看到表明您的配置已保存且部署正在进行中的消息，请滚动到页面顶部查看错误消息。

配置也会复制到剪贴板。您可以使用副本快速配置辅助设备。为增强安全性，剪贴板副本中不包含加密密钥。

此时，您必须位于High Availability页面，并且设备状态必须为“Negotiating”。即使在配置对等体之前，状态也必须转换到Active，在配置对等体之前，该状态必须显示为Failed。

High Availability

Primary Device: **Active**



Peer: **Failed**

在辅助设备的安全防火墙设备管理器上启用高可用性

将主设备配置为主用/备用高可用性后，必须配置辅助设备。登录该设备上的FDM并运行此过程。


步骤1:要配置FDM故障切换，请导航到Device，然后单击High Availability组旁边的Configure:

High Availability 
Not Configured

CONFIGURE




第二步：在High Availability页面上，点击Secondary Device框：

Device Summary
High Availability

How High Availability Works 

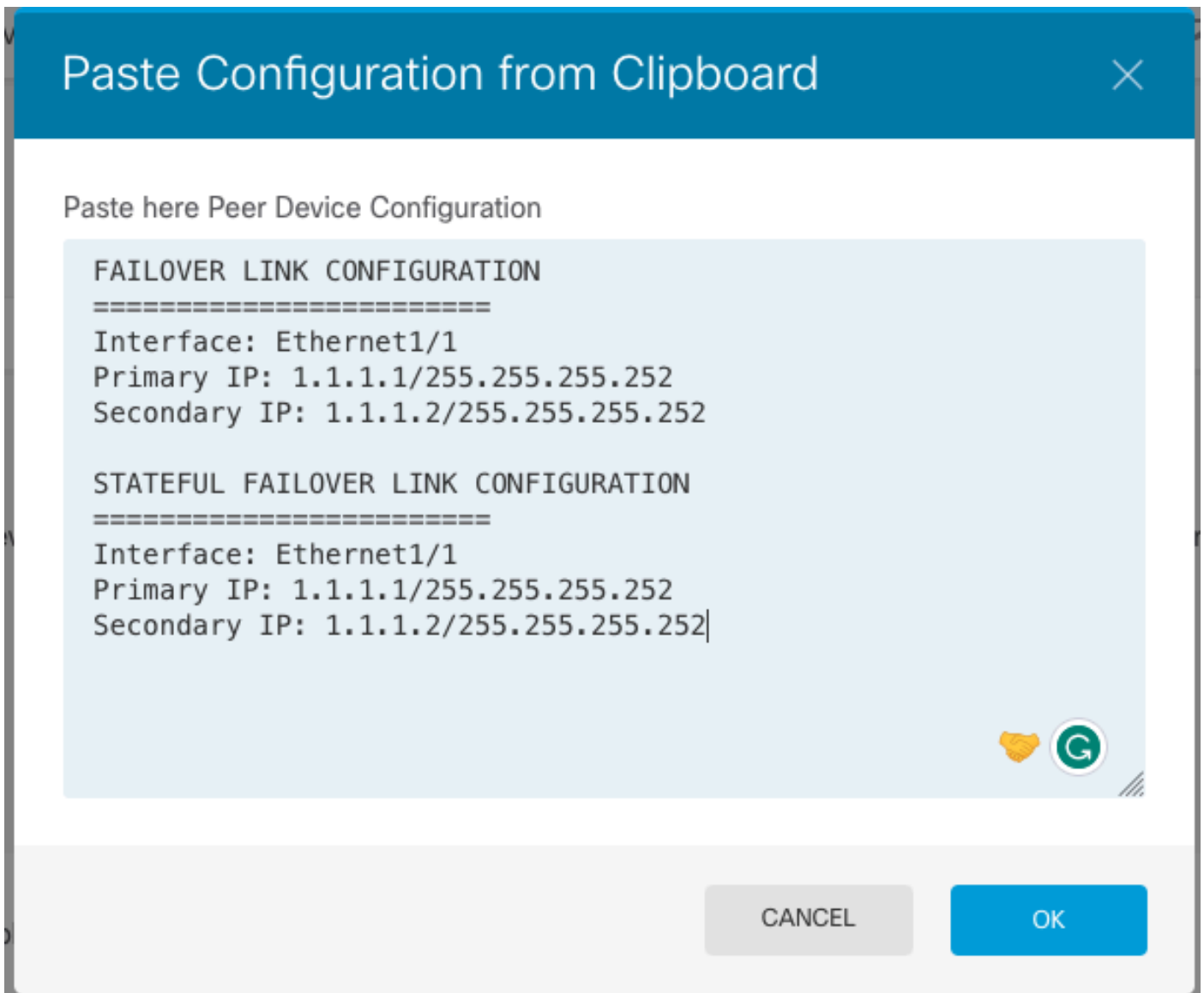
Select the role for this device

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 

第三步：选择下列选项之一：

- Easy method — 单击“Paste from Clipboard”按钮，粘贴到配置中，然后单击OK。这会使用适当的值更新字段，然后您可以进行验证。
- 手动方法 — 直接配置故障切换和有状态故障切换链路。在辅助设备上输入与在主设备上输入的完全相同的设置。

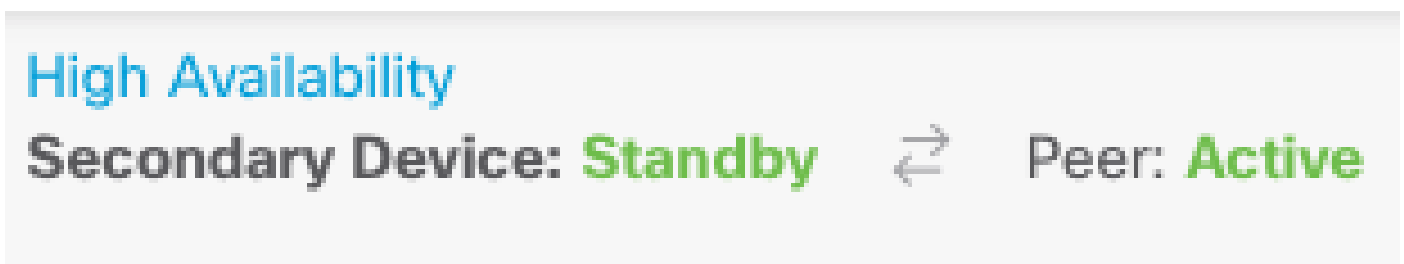


第四步：点击Activate HA

系统立即将配置部署到设备。您无需启动部署作业。如果您没有看到表明您的配置已保存且部署正在进行中的消息，请滚动到页面顶部查看错误消息。

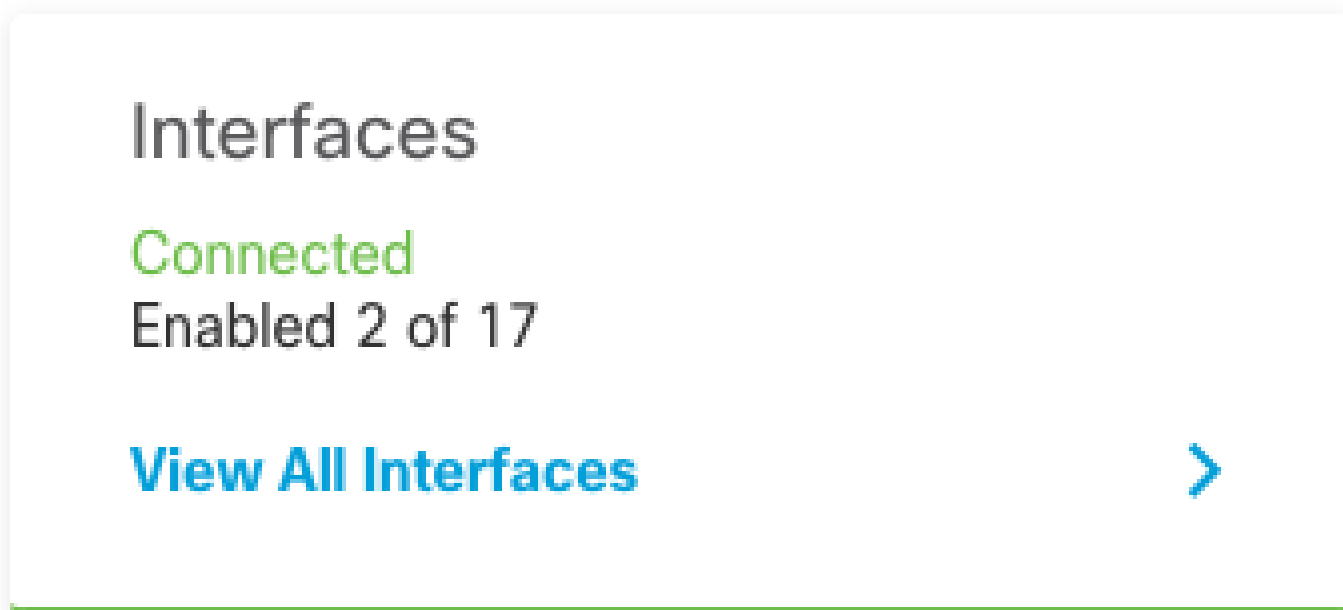
配置完成后，您将收到一条消息，表明您已配置HA。单击Got It以关闭消息。

此时，您必须位于High Availability页面，并且设备状态必须指示这是辅助设备。如果与主设备的加入成功，设备将与主设备同步，并且最终，模式必须为Standby，对等设备必须为Active。



完成接口配置

步骤1:要配置FDM接口，请导航到设备，然后单击查看所有接口：



第二步：选择并编辑接口设置，如图所示：

以太网1/5接口：

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

以太网1/6接口

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

第三步：配置更改后，单击Pending Changes



和Deploy Now。

任务3.验证FDM高可用性

任务要求：

从FDM GUI和FDM CLI验证高可用性设置。

解决方案：

步骤1:导航到设备并检查高可用性设置：

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 of failed interfaces exceeds 1-211

INTERFACE TIMING CONFIGURATION

Poll Time: 500-15000 milliseconds Hold Time: 5000-75000 milliseconds [seconds](#) [milliseconds](#)

PEER TIMING CONFIGURATION

Poll Time: 200-15000 milliseconds Hold Time: 800-45000 milliseconds [seconds](#) [milliseconds](#)

第二步：使用SSH连接到FDM主设备CLI，并使用show high-availability config命令进行验证：

```
> 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

第三步：在辅助设备上执行相同操作。

第四步：使用show failover state命令验证当前状态：

```
> 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
```

第五步：使用show running-config failover和show running-config interface从主设备检验配置：

```
> 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
```

任务4.切换故障切换角色

任务要求：

在安全防火墙设备管理器图形界面中，将故障切换角色从主/主用、辅助/备用切换为主用/备用、辅助/主用

解决方案：

步骤1:点击Device



Device: FPR2130-1

第二步：单击设备摘要右侧的High Availability链接。

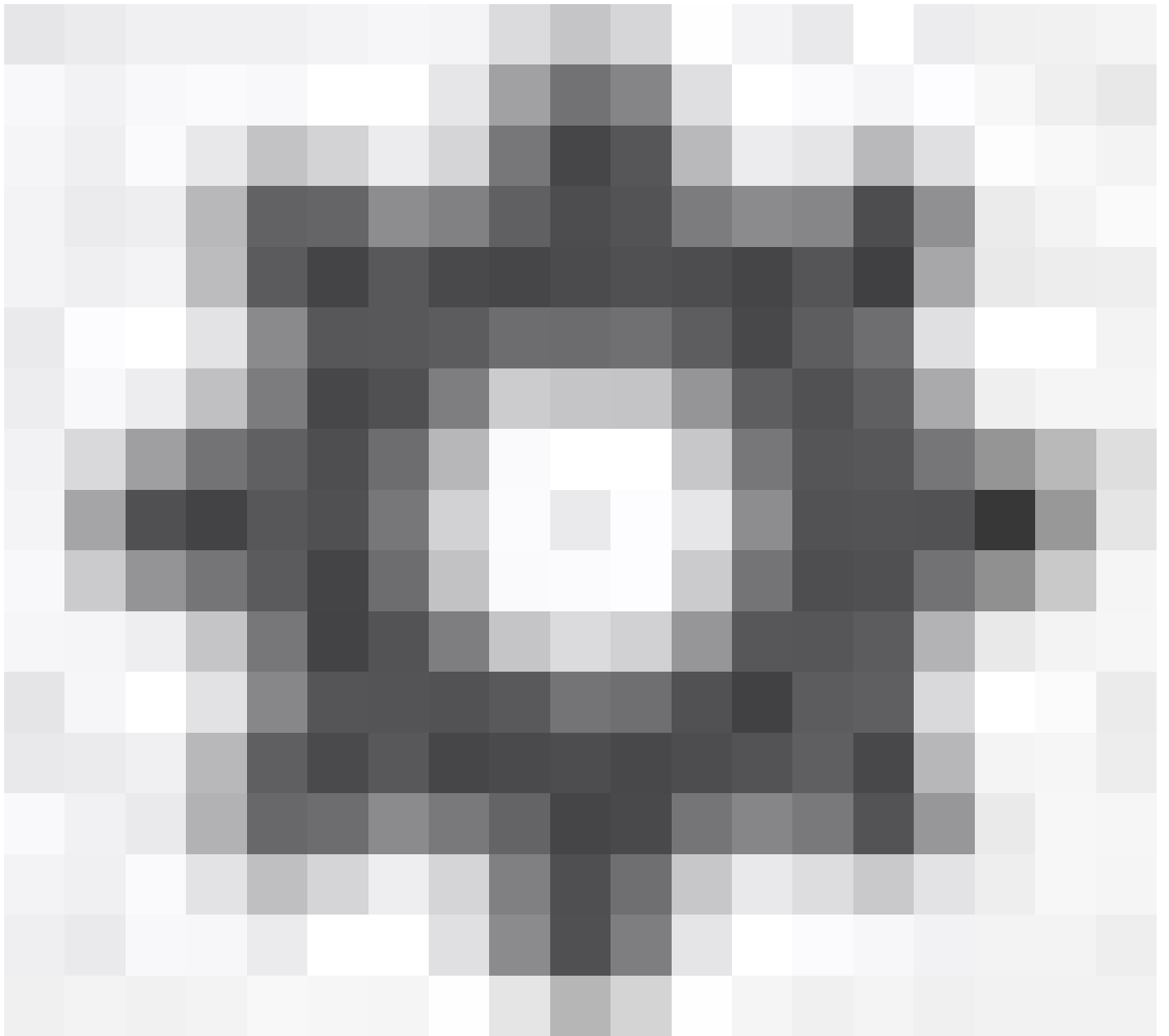
High Availability

Primary Device: **Active**

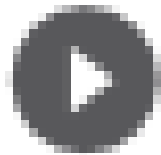
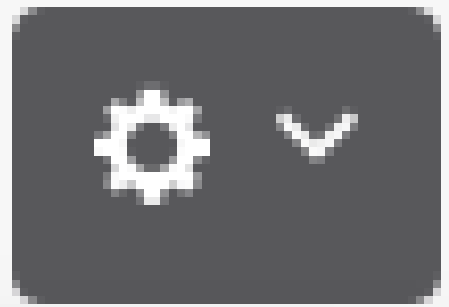


Peer: **Standby**

第三步：从齿轮图标(



) , 选择Switch Mode。



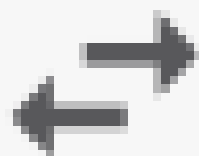
Resume HA



Suspend HA

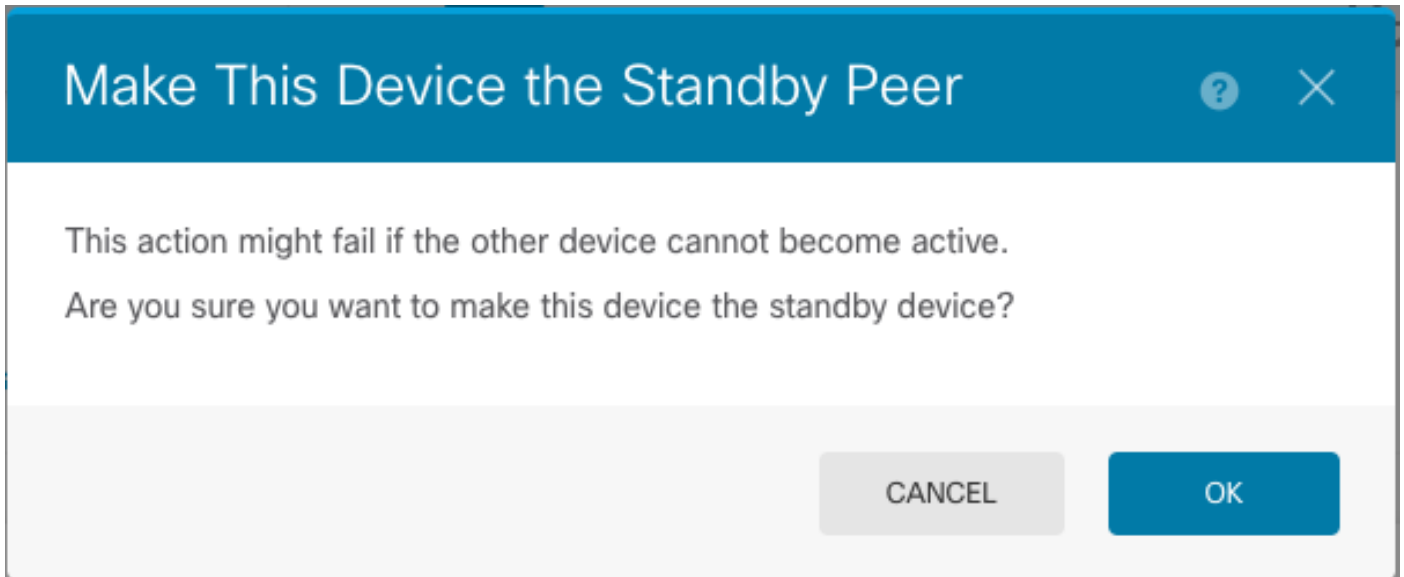


Break HA



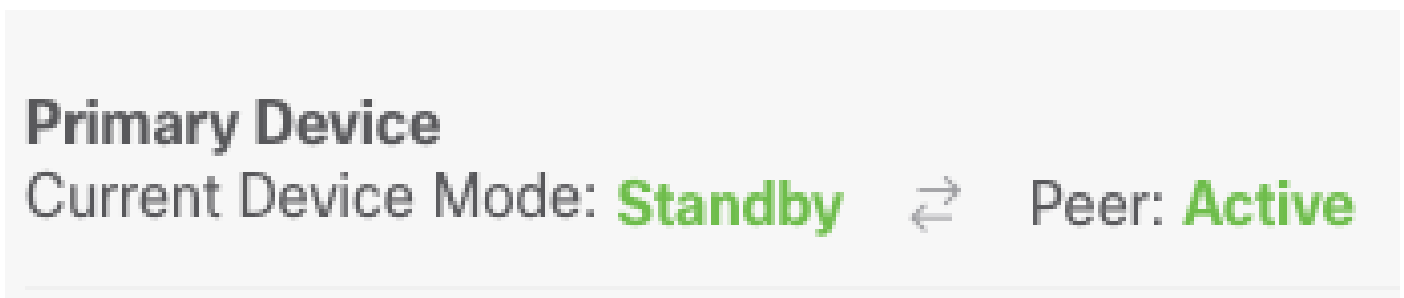
Switch Mode

第四步：阅读确认消息，然后单击OK。



系统会强制进行故障切换，使主用设备成为备用设备，而备用设备成为新的主用设备。

第五步：如图所示验证结果：



第六步：也可以使用Failover History链接进行验证，CLI控制台弹出窗口必须显示以下结果：

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=====

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=====

步骤 7.验证后，使主设备再次处于活动状态。

任务5.暂停或恢复高可用性

您可以在高可用性对中挂起设备。在以下情况下，这非常有用：

- 两台设备都处于“主用 — 主用”状态，修复故障切换链路上的通信无法解决问题。

- 您要排除主用或备用设备的故障，并且不要让这些设备在此期间进行故障转移。
- 您希望在备用设备上安装软件升级时防止故障转移。

挂起HA和中断HA之间的关键区别在于，在挂起HA设备上，保留高可用性配置。当您中断HA时，配置会被清除。因此，您可以选择在暂停的系统上恢复HA，这将启用现有配置并使两台设备再次作为故障切换对运行。

任务要求：

在安全防火墙设备管理器图形界面中，挂起主设备并在同一设备上恢复高可用性。

解决方案：

步骤1:单击Device。



Device: FPR2130-1

第二步：单击设备摘要右侧的High Availability链接。

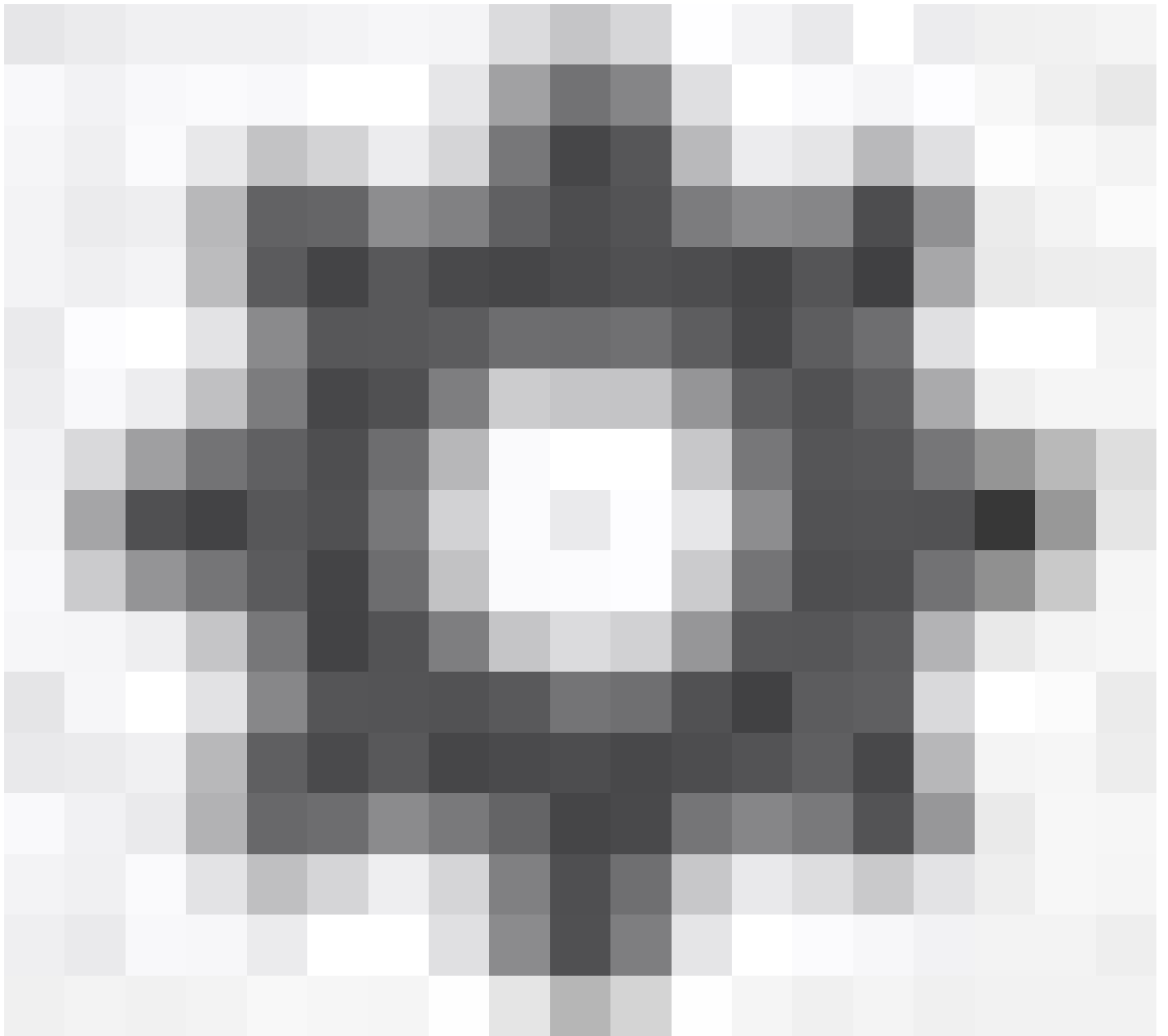
High Availability

Primary Device: **Active**

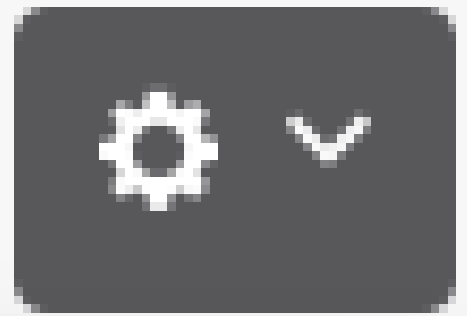


Peer: **Standby**

第三步：从齿轮图标(



) , 选择Suspend HA。



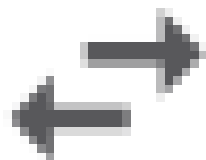
Resume HA



Suspend HA



Break HA



Switch Mode

第四步：阅读确认消息，然后单击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

第五步：如图所示验证结果：

Primary Device

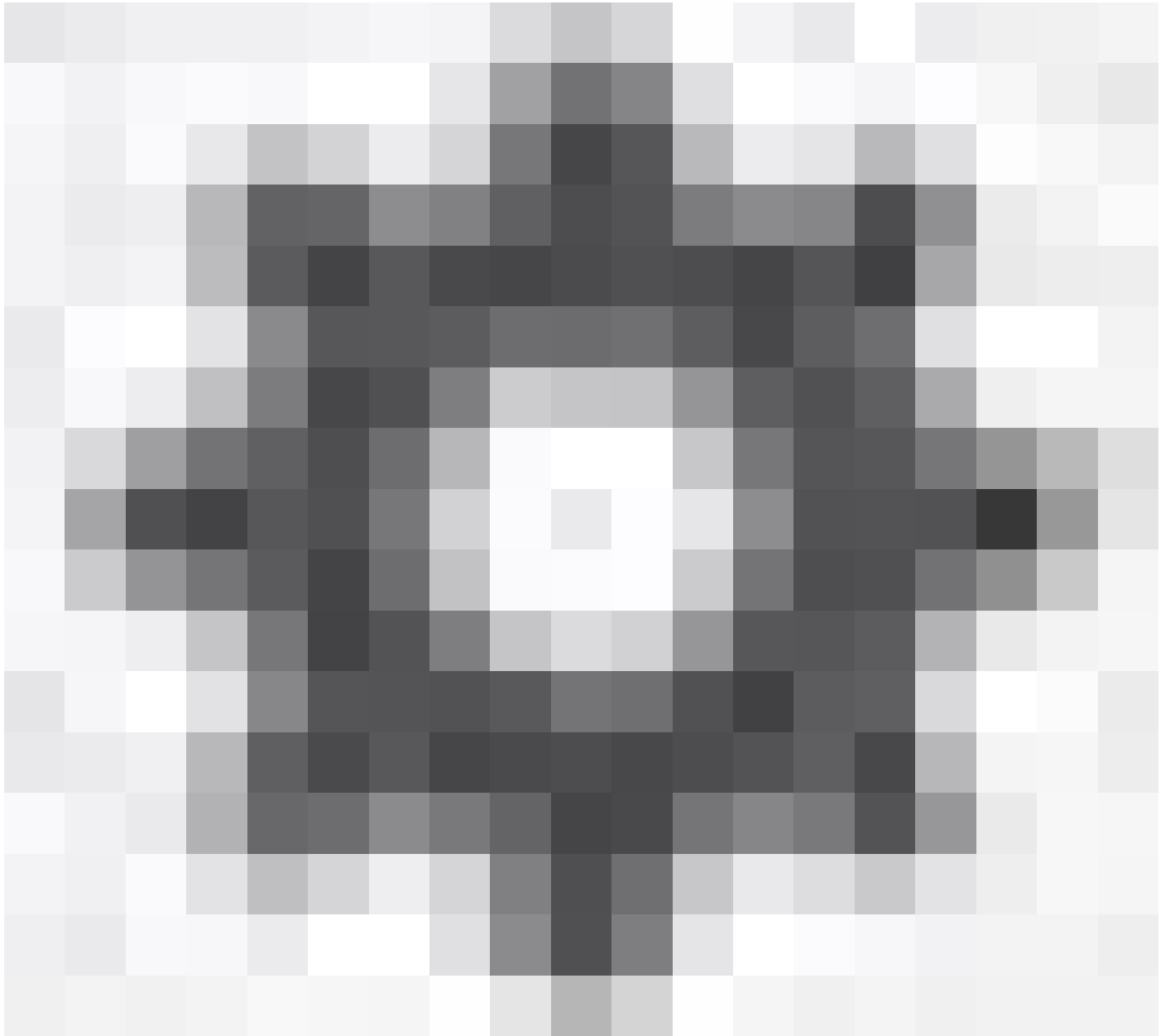
Current Device Mode: **Suspended**  Peer: **Unknown**



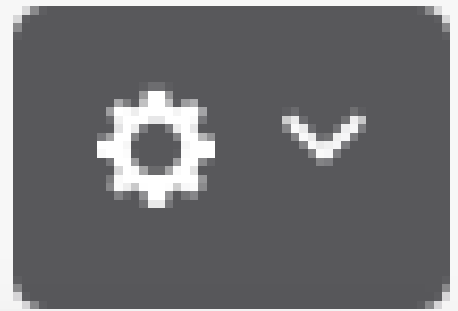
Time of event: 25 Jul 2023, 01:08:01 PM

Event description: Set by the config command

第六步：要恢复高可用性，请从齿轮图标(



) , 选择Resume HA。



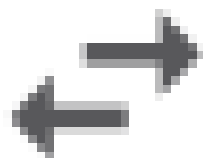
Resume HA



Suspend HA

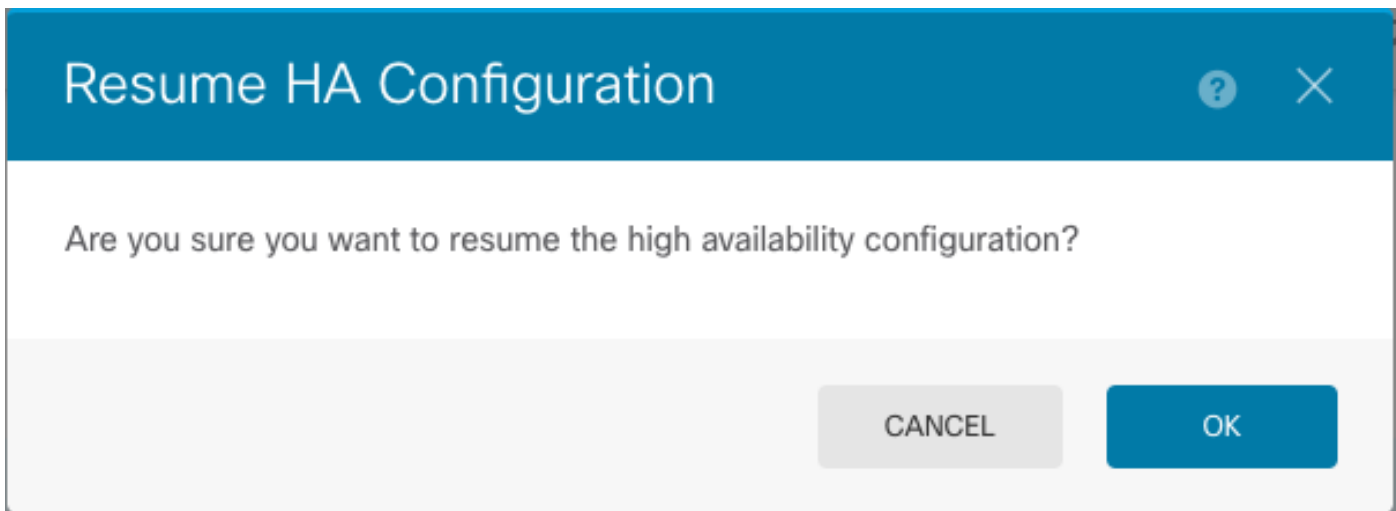


Break HA

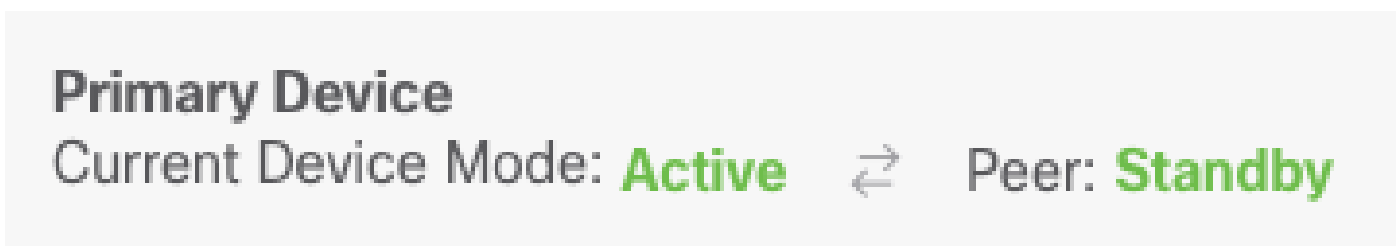


Switch Mode

步骤 7. 阅读确认消息，然后单击OK。



第五步：如图所示验证结果：



任务6.突破高可用性

如果不再希望两台设备作为高可用性对运行，则可以中断HA配置。当您中断HA时，每台设备都会成为独立设备。其配置必须更改为：

- 主用设备会保留中断前的完整配置，并删除HA配置。
- 除了HA配置之外，备用设备还删除了所有接口配置。尽管子接口未禁用，但所有物理接口都处于禁用状态。管理接口保持活动状态，因此您可以登录设备并重新配置它。

任务要求：

从安全防火墙设备管理器图形界面中断高可用性对。

解决方案：

步骤1:单击Device。



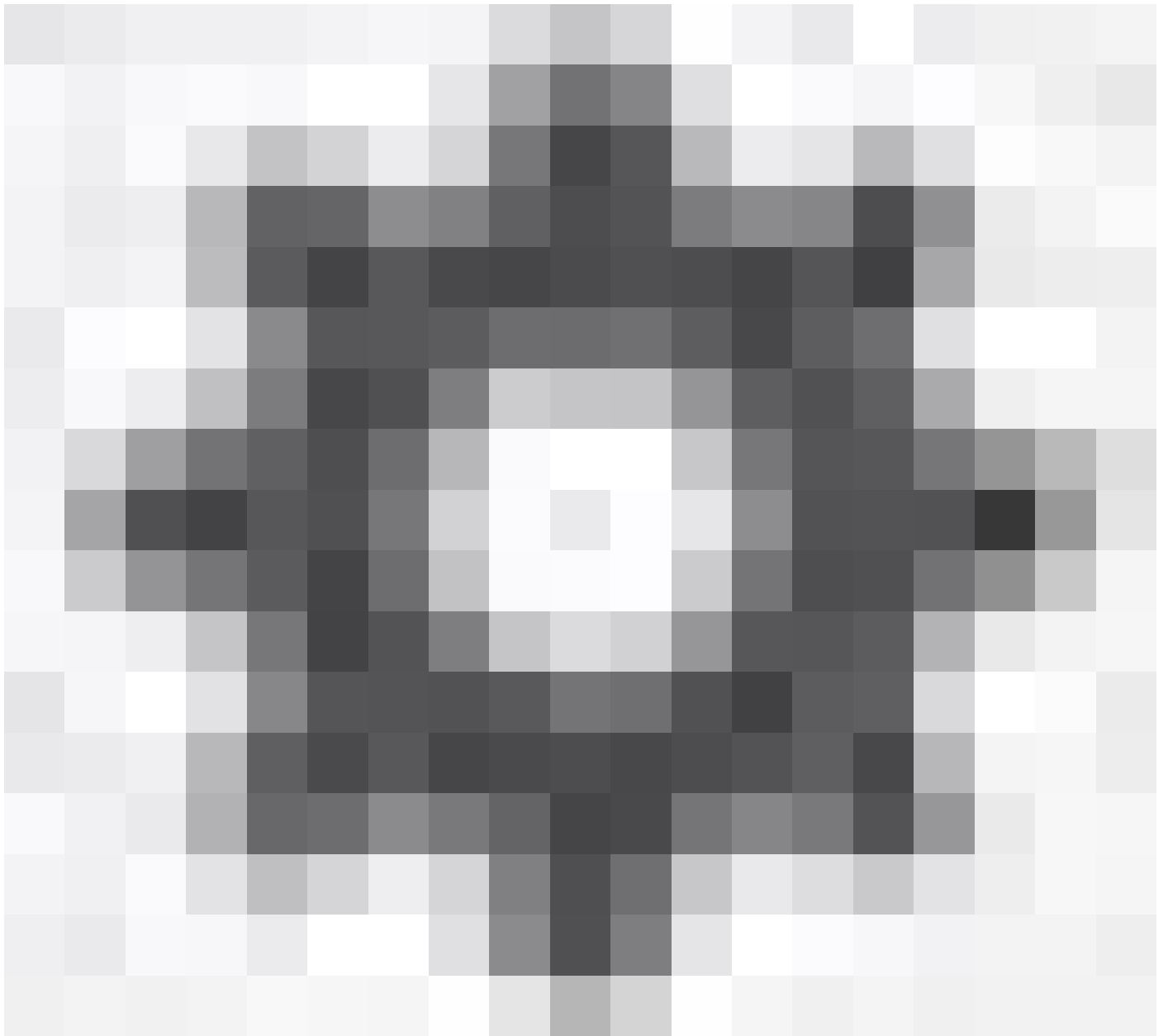
Device: FPR2130-1

第二步：单击设备摘要右侧的High Availability链接。

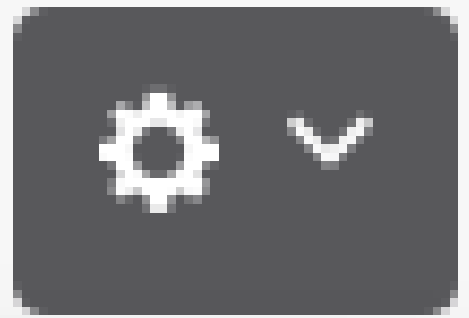
High Availability

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

第三步：从齿轮图标(



)，选择中断HA。



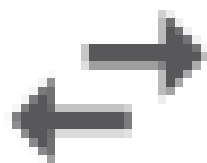
Resume HA



Suspend HA



Break HA



Switch Mode

第四步：阅读确认消息，决定是否选择禁用接口的选项，然后单击Break。

如果要从备用设备中断HA，必须选择禁用接口的选项。

系统会立即在此设备和对等设备上（如果可能）部署您的更改。每台设备上完成部署以及每台设备独立部署可能需要几分钟。

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

步骤5.检验结果，如图所示：

High Availability ? Not Configured

CONFIGURE

相关信息

- 所有版本的Cisco Secure Firewall Device Manager配置指南都可以在此处找到

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

- 思科全球技术支持中心(TAC)强烈推荐此可视化指南，以了解有关Cisco Firepower下一代安全

技术的深入实践知识：

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

- 有关Firepower技术的所有配置和故障排除技术说明

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

- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。