

在高可用性中配置Secure Firewall裝置管理器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[任務1.驗證條件](#)

[任務2.在高可用性中配置Secure Firewall裝置管理器](#)

[網路圖表](#)

[在主裝置的安全防火牆裝置管理器上啟用高可用性](#)

[在輔助裝置的安全防火牆裝置管理器上啟用高可用性](#)

[完成介面配置](#)

[任務3.驗證FDM高可用性](#)

[任務4.切換故障切換角色](#)

[任務5.暫停或恢復高可用性](#)

[任務6.突破高可用性](#)

[相關資訊](#)

簡介

本文描述如何在安全防火牆裝置上配置和驗證Secure Firewall裝置管理器(FDM)高可用性(HA)。

必要條件

需求

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 2x思科安全防火牆2100安全裝置
- 運行FDM版本7.0.5 (內部版本72)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

任務1.驗證條件

工作需求：

驗證兩個FDM裝置是否滿足註釋要求，以及是否可以配置為HA裝置。

解決方案：

步驟1.使用SSH連線到裝置管理IP並驗證模組硬體。

使用show version命令驗證主裝置的硬體和軟體版本：

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

驗證輔助裝置硬體和軟體版本：

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

任務2.在高可用性中配置Secure Firewall裝置管理器

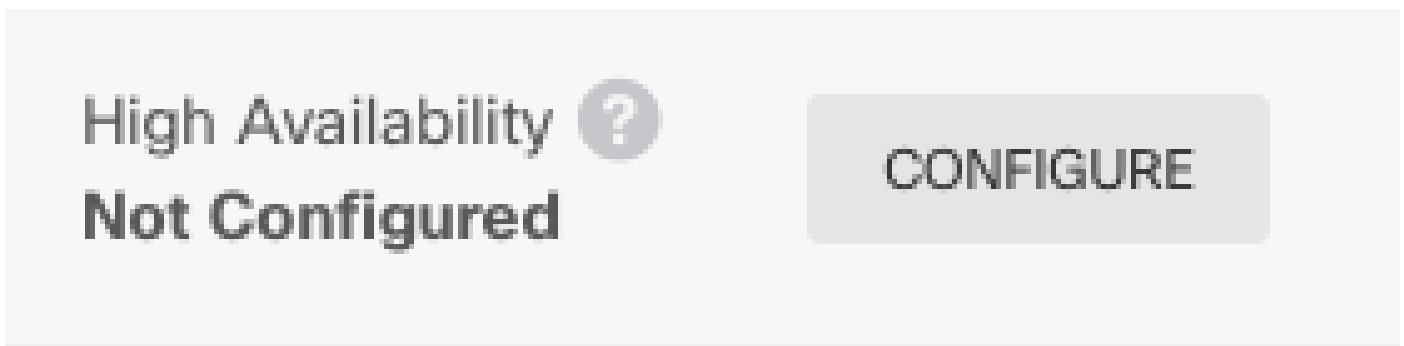
網路圖表

根據下圖配置活動/備用高可用性(HA):

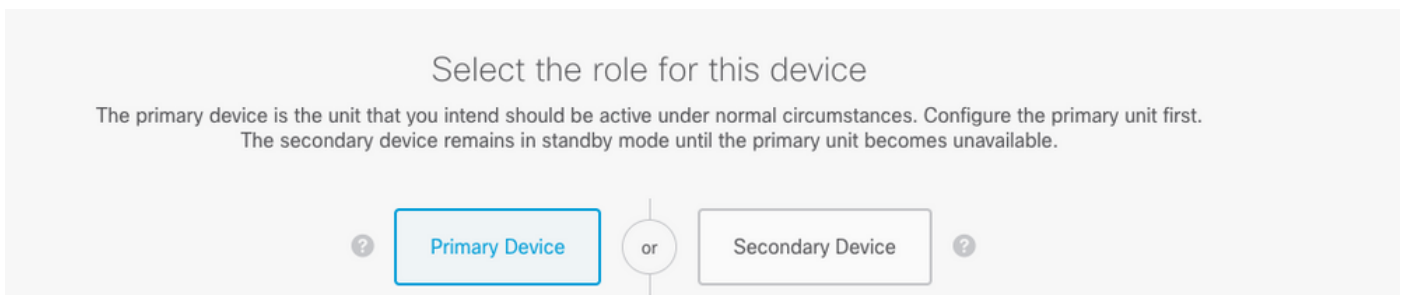


在主裝置的安全防火牆裝置管理器上啟用高可用性

步驟1.要配置FDM故障轉移，請導航到Device，然後按一下High Availability組旁邊的Configure:



步驟2.在High Availability頁面上，按一下Primary Device框：



警告：確保選擇正確的裝置作為主要裝置。所選主裝置上的所有配置都將複製到所選輔助FTD裝置。通過複製，可以替換輔助裝置上的當前配置。

步驟3.配置故障切換鏈路和狀態鏈路設定：

在本示例中，狀態鏈路的設定與故障切換鏈路的設定相同。

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

步驟4.點選啟用HA(Activate HA)

步驟5.將HA配置複製到確認消息上的剪貼簿，以將其貼上到輔助裝置上。

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

系統會立即將配置部署到裝置。您無需啟動部署作業。如果您沒有看到表明配置已儲存且部署正在進行中的消息，請滾動到頁面頂部以檢視錯誤消息。

系統也會將組態複製到剪貼簿。您可以使用該副本快速配置輔助裝置。為了增強安全性，剪貼簿副本中不包含加密金鑰。

此時，您必須位於High Availability頁面，並且裝置狀態必須為「Negotiating」。即使在配置對等體之前，狀態也必須轉換為「活動」，配置對等體之前，狀態必須顯示為「失敗」。

High Availability

Primary Device: **Active**



Peer: **Failed**

在輔助裝置的安全防火牆裝置管理器上啟用高可用性

將主裝置配置為主用/備用高可用性後，必須配置輔助裝置。登入該裝置上的FDM並運行此過程。


步驟1.要配置FDM故障轉移，請導航到Device，然後按一下High Availability組旁邊的Configure:

High Availability 
Not Configured

CONFIGURE




步驟2.在High Availability (高可用性) 頁面上，按一下Secondary Device (輔助裝置) 框：

Device Summary
High Availability

How High Availability Works 

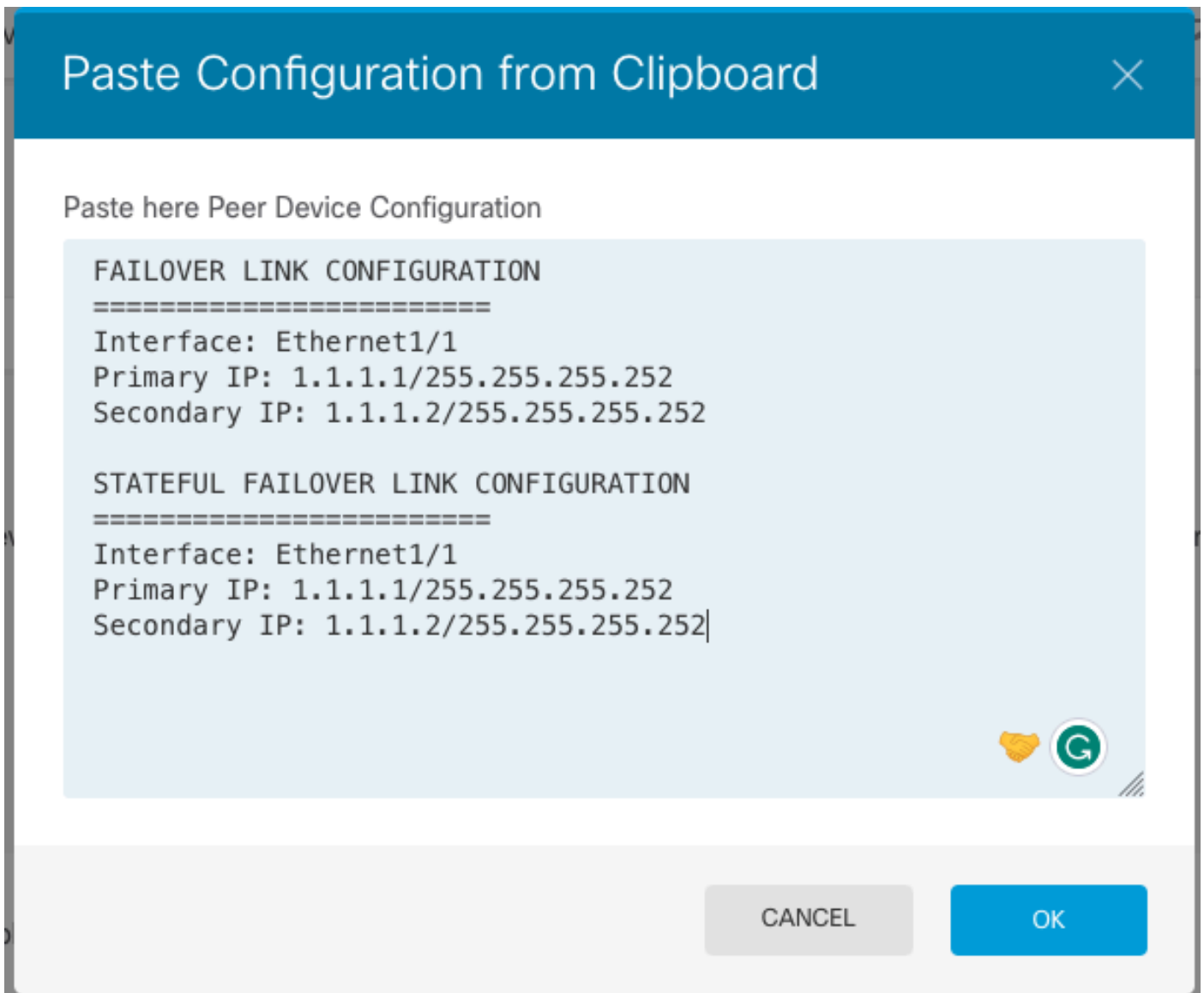
Select the role for this device

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 

步驟3.選擇以下選項之一：

- Easy method — 按一下「Paste from Clipboard」按鈕，貼上配置，然後按一下OK。這將用適當的值更新欄位，然後您可以進行驗證。
- 手動方法 — 直接配置故障切換和有狀態故障切換鏈路。在輔助裝置上輸入與您在主裝置上輸入的設定完全相同的設定。

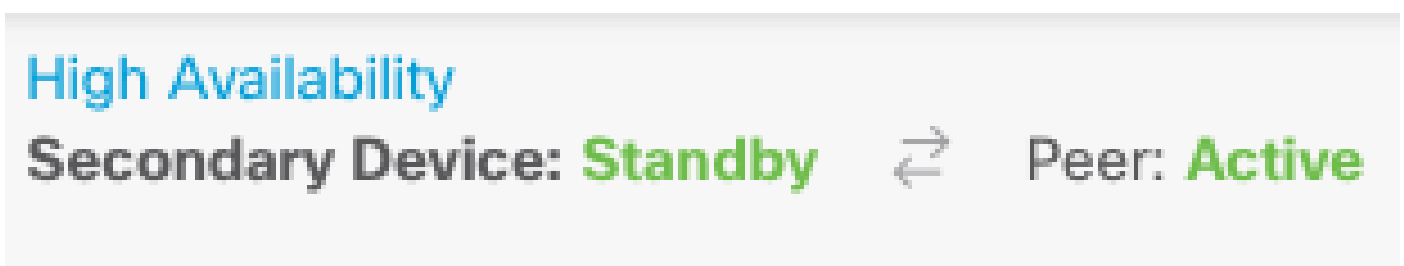


步驟4. 點選啟用HA(Activate HA)

系統會立即將配置部署到裝置。您無需啟動部署作業。如果您沒有看到表明配置已儲存且部署正在進行中的消息，請滾動到頁面頂部以檢視錯誤消息。

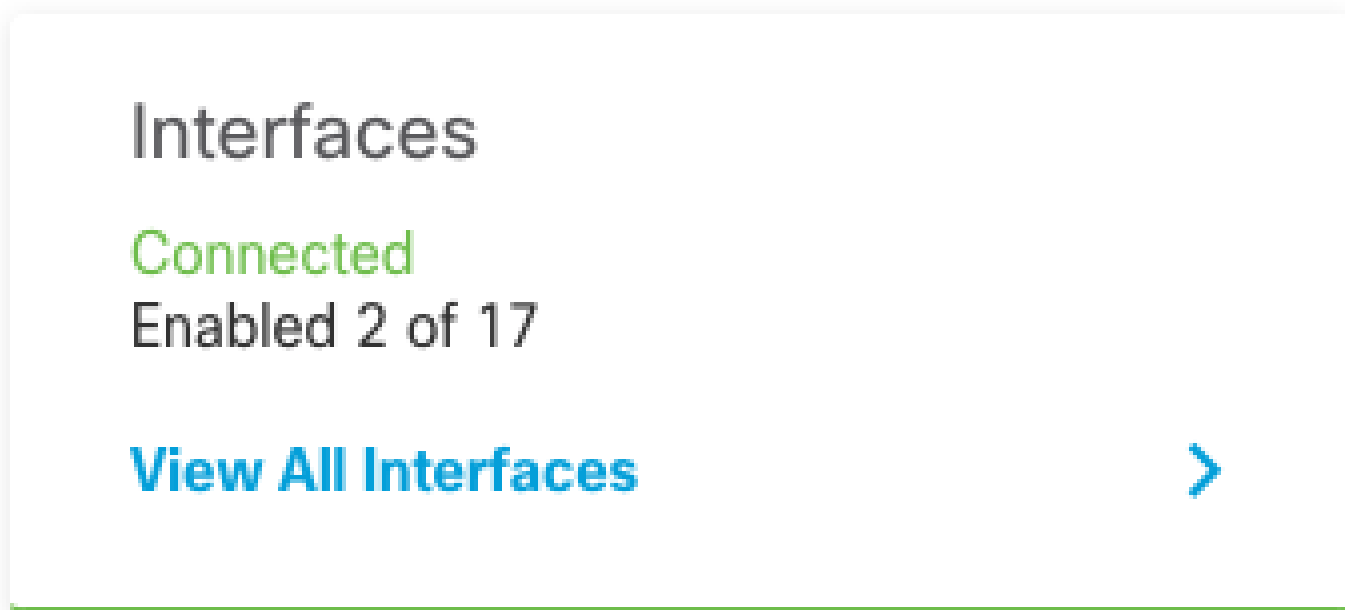
配置完成後，您將收到一條消息，通知您已配置HA。按一下Got It以關閉郵件。

此時，您必須位於High Availability頁面，並且裝置狀態必須指示這是輔助裝置。如果與主裝置的連線成功，則裝置將與主裝置同步，最後，模式必須為Standby，對等裝置必須為Active。



完成介面配置

步驟1.要配置FDM介面，請導航到裝置，然後按一下檢視所有介面：



步驟2.選擇並編輯介面設定，如下圖所示：

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 介面

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

步驟3.配置更改後，按一下Pending Changes



和Deploy Now。

任務3. 驗證FDM高可用性

工作需求：

從FDM GUI和FDM CLI驗證高可用性設定。

解決方案：

步驟1. 導覽至Device，然後檢查High Availability設定：

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](#)

SAVE

步驟2.使用SSH連線到FDM主裝置CLI，並使用show high-availability config命令進行驗證：

```
> 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

步驟3.在輔助裝置上執行相同操作。

步驟4.使用show failover state 命令驗證當前狀態：

```
> 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
```

步驟5.使用show running-config failover和show running-config interface從主裝置驗證配置：

```
> 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
```

任務4. 切換故障切換角色

工作需求：

從Secure Firewall Device Manager Graphic Interface (安全防火牆裝置管理器圖形介面)，將故障切換角色從主/主用、輔助/備用切換為主用/備用、輔助/主用

解決方案：

步驟1. 按一下Device (裝置)



Device: FPR2130-1

步驟2. 按一下裝置摘要右側的High Availability連結。

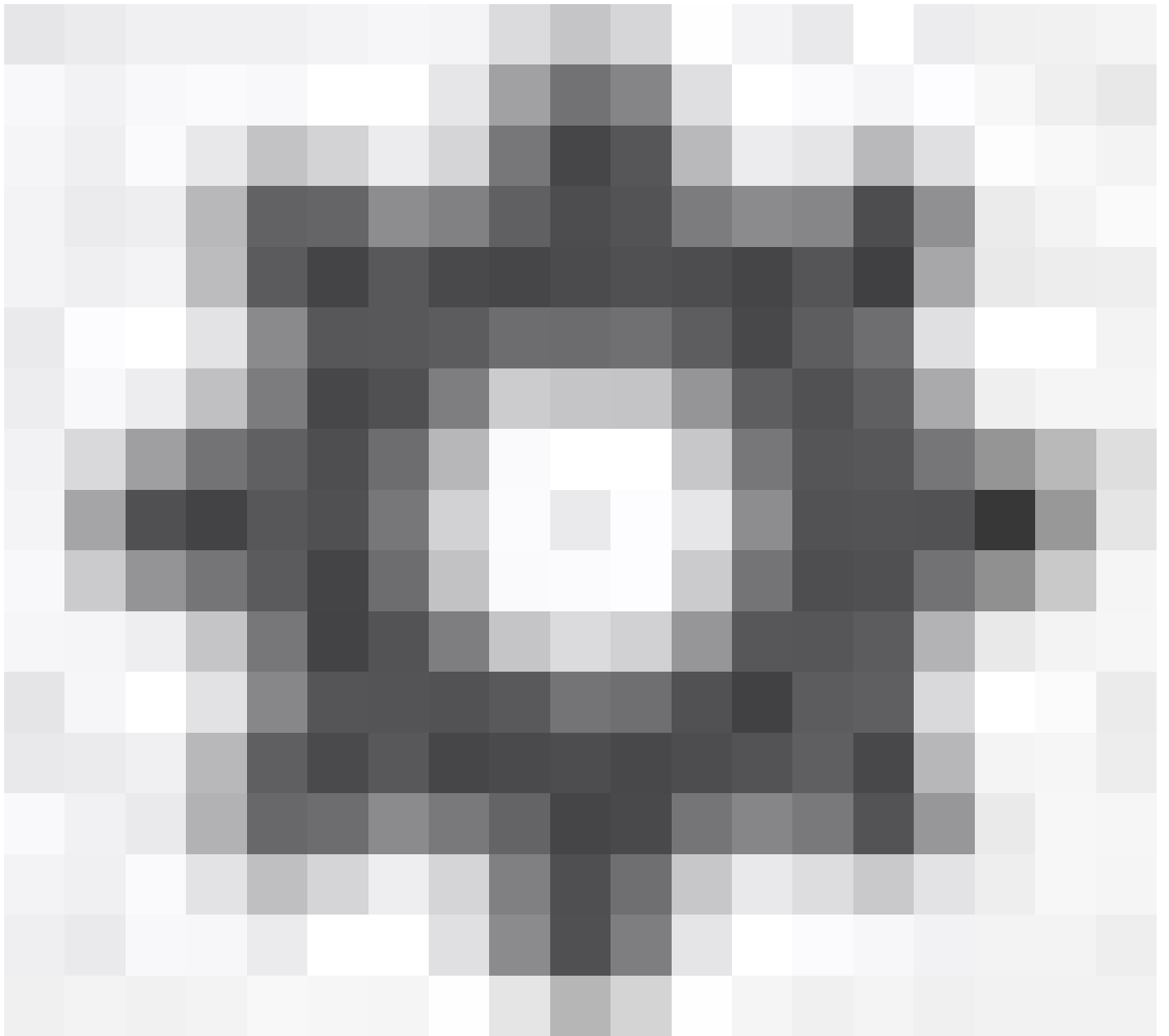
High Availability

Primary Device: **Active**

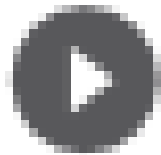
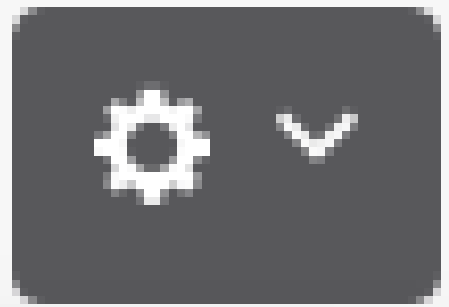


Peer: **Standby**

步驟3. 從齒輪圖示(



, 選擇Switch Mode。



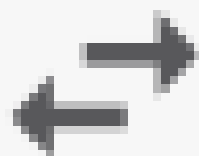
Resume HA



Suspend HA

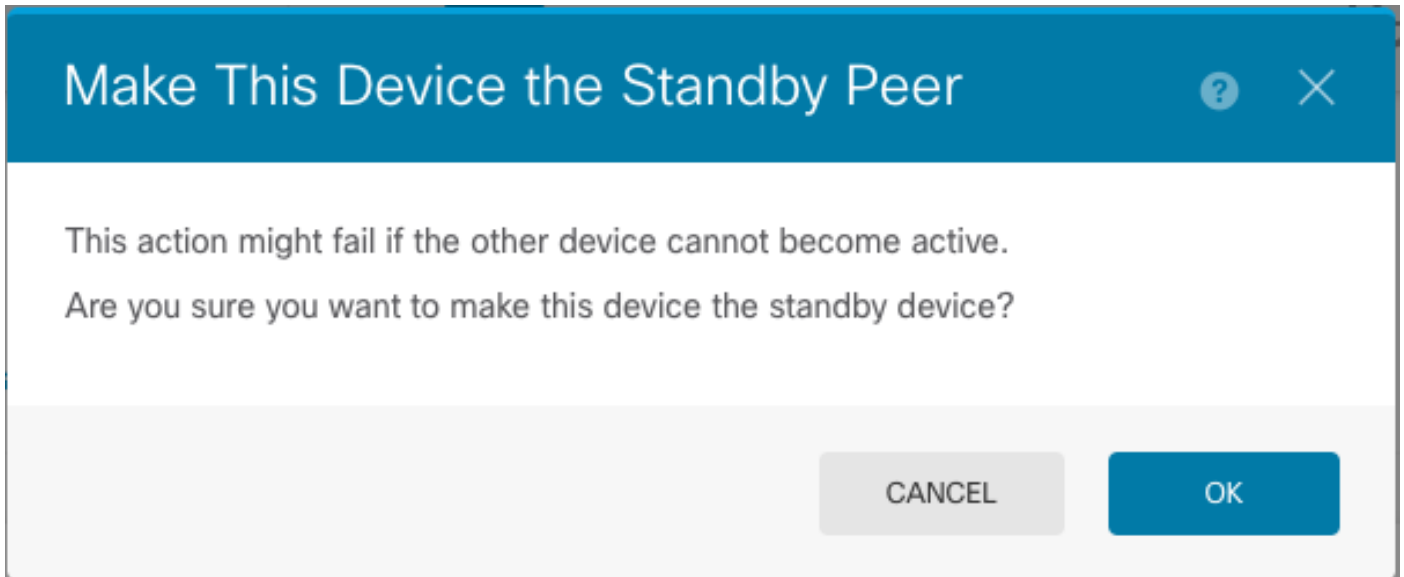


Break HA



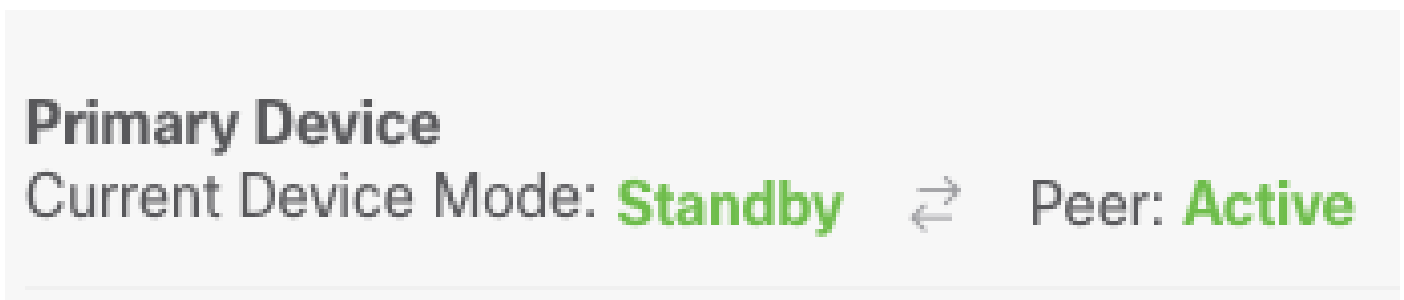
Switch Mode

步驟4.閱讀確認消息，然後按一下OK。



系統強制進行故障切換，以便主用裝置成為備用裝置，而備用裝置成為新的主用裝置。

步驟5.驗證結果，如下圖所示：



步驟6.也可以使用Failover History (故障轉移歷史記錄) 連結進行驗證，並且CLI Console (CLI控制檯) 彈出視窗必須顯示結果：

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 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=====

```

步驟7.驗證後，使主裝置再次處於活動狀態。

任務5.暫停或恢復高可用性

您可以在高可用性對中暫停設備。在以下情況下，這非常有用：

- 兩台裝置都處於主用 — 主用狀態，修復故障轉移鏈路上的通訊無法解決問題。
- 您要對主用或備用裝置進行故障排除，並且不希望這些裝置在此期間發生故障轉移。
- 您希望在備用裝置上安裝軟體升級時防止故障轉移。

掛起HA和中斷HA之間的關鍵區別在於，在掛起HA裝置上，保留高可用性配置。中斷HA時，配置會被清除。因此，您可以選擇在掛起的系統上恢復HA，這將啟用現有配置，並使兩台裝置再次作為故障轉移對運行。

工作需求：

從Secure Firewall Device Manager Graphic Interface (安全防火牆裝置管理器圖形介面)，暫停主裝置並在同一裝置上恢復高可用性。

解決方案：

步驟1.按一下「Device」。



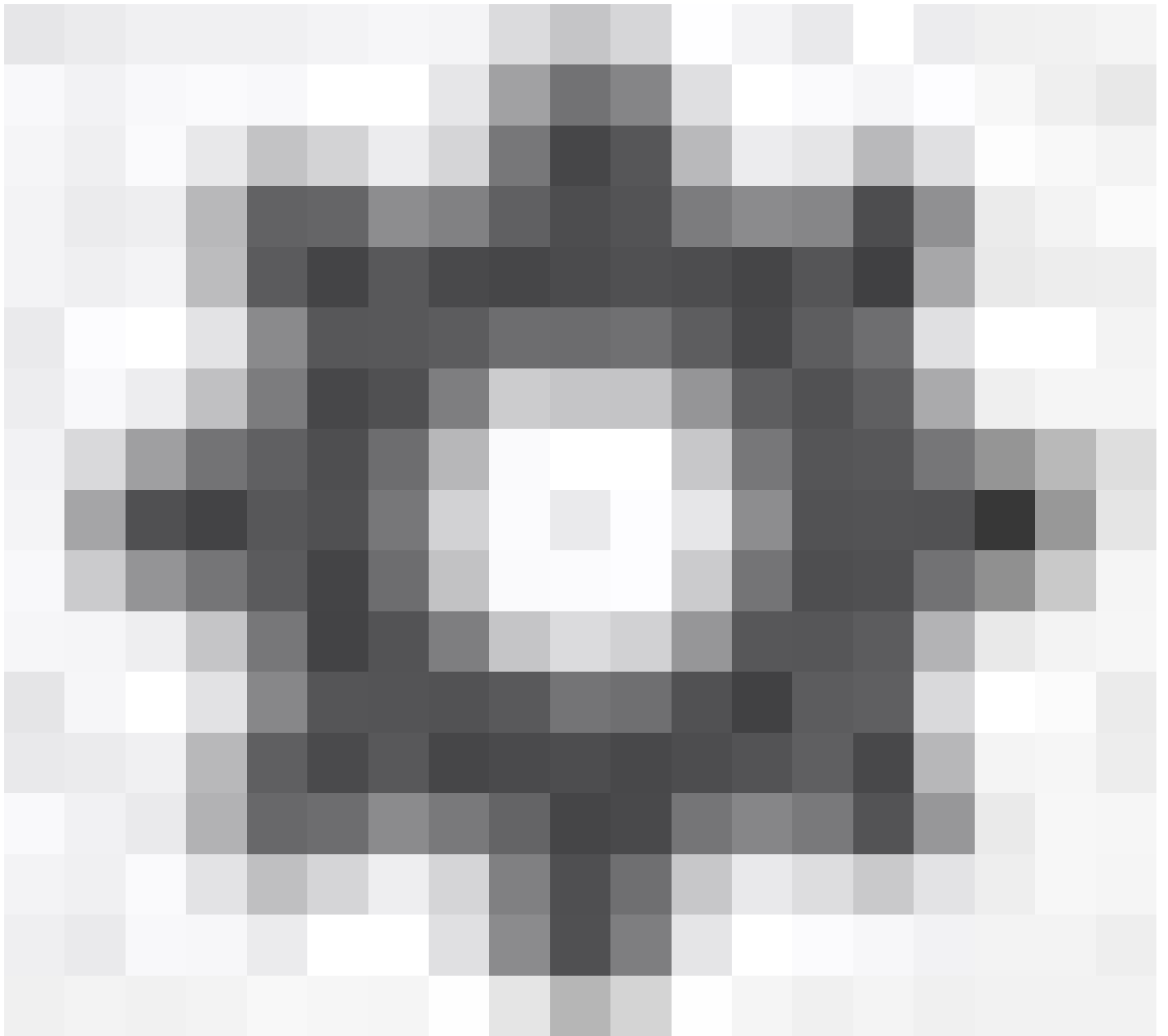
Device: FPR2130-1

步驟2.按一下裝置摘要右側的High Availability連結。

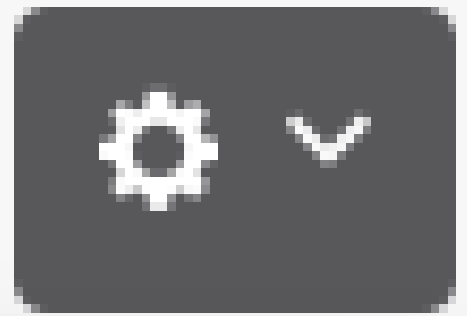
High Availability

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

步驟3.從齒輪圖示(



, 選擇Suspend HA。



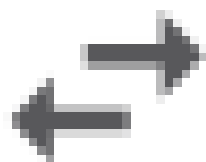
Resume HA



Suspend HA



Break HA



Switch Mode

步驟4.閱讀確認消息，然後按一下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

步驟5.驗證結果，如下圖所示：

Primary Device

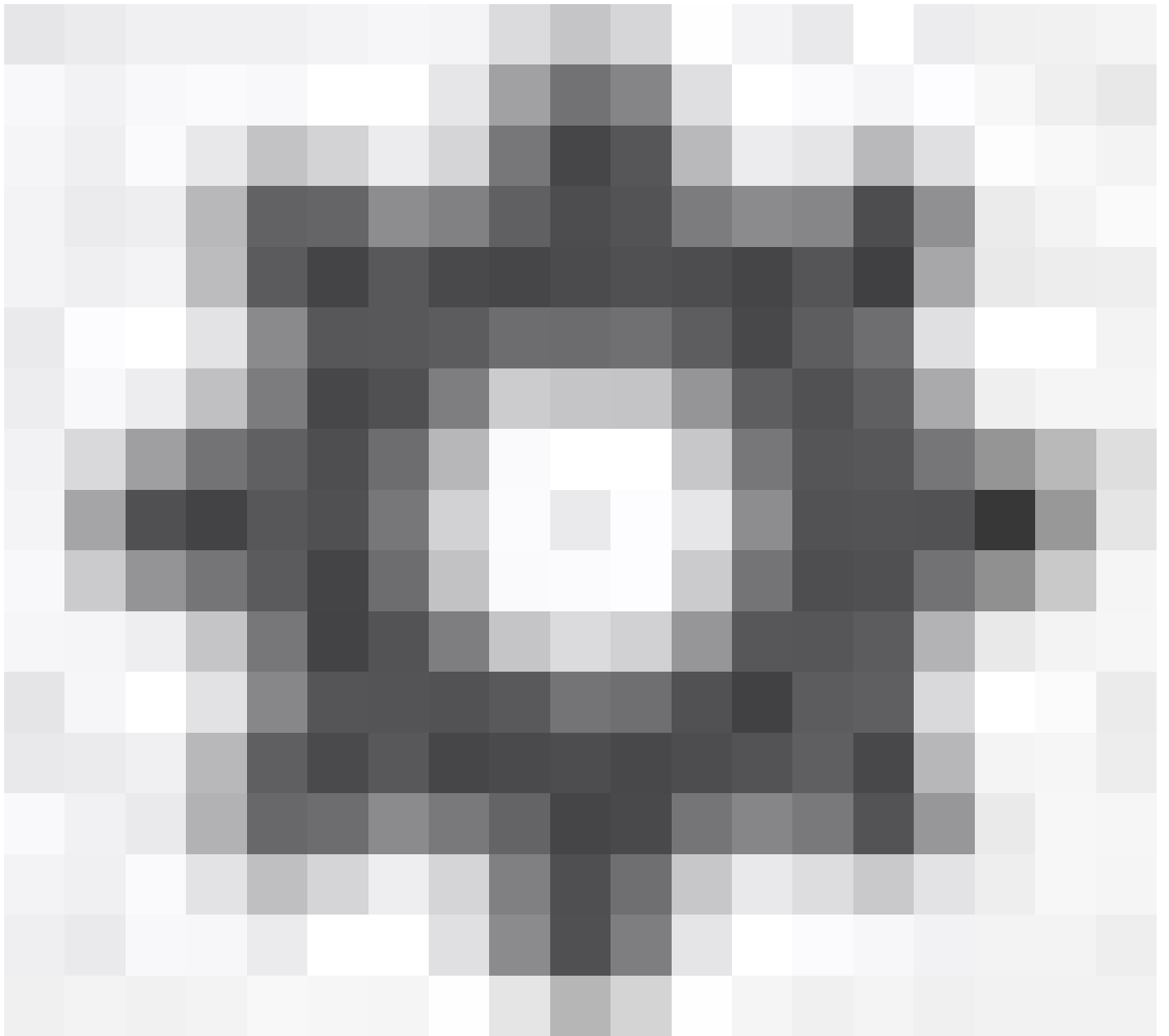
Current Device Mode: **Suspended**  Peer: **Unknown**



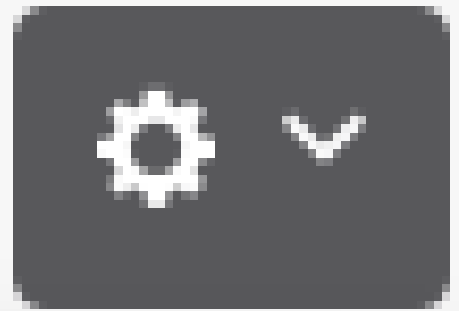
Time of event: 25 Jul 2023, 01:08:01 PM

Event description: Set by the config command

步驟6.要恢復HA，請從齒輪圖示(



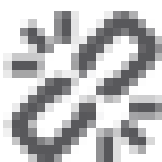
, 選擇Resume HA。



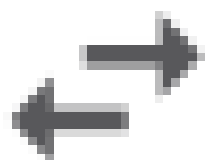
Resume HA



Suspend HA

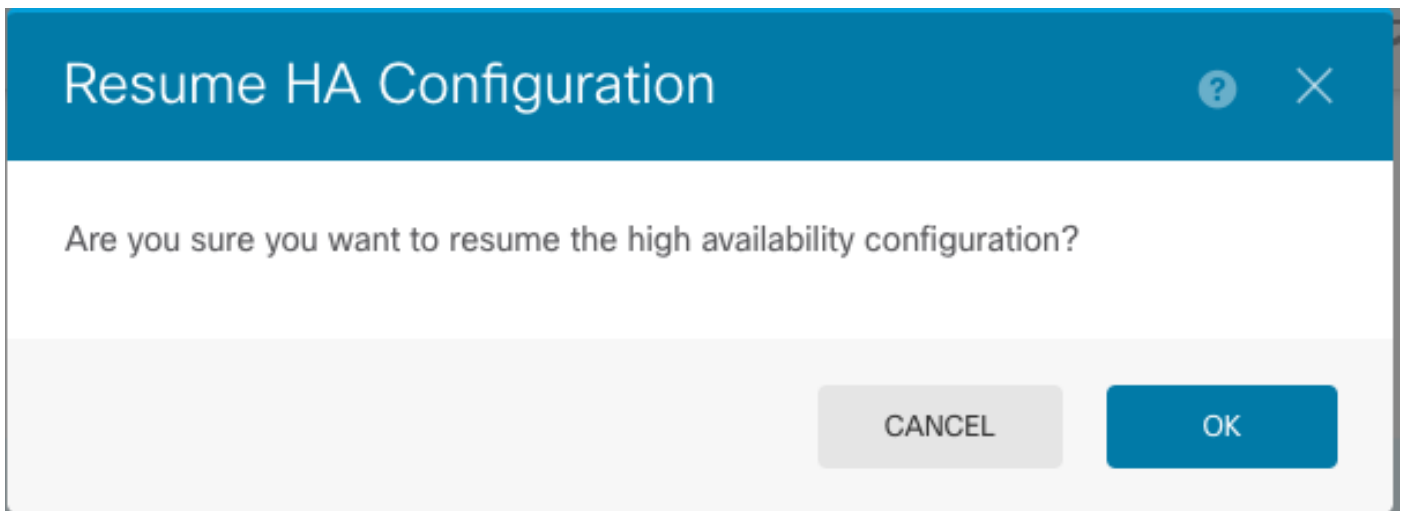


Break HA

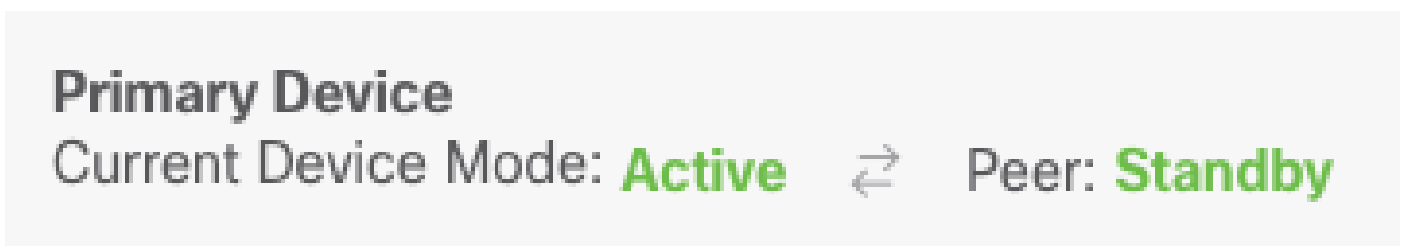


Switch Mode

步驟7.閱讀確認消息，然後按一下OK。



步驟5.驗證結果，如下圖所示：



任務6.突破高可用性

如果不想讓兩台裝置作為高可用性對運行，可以中斷HA組態。當中斷HA時，每台裝置都將成為獨立裝置。其配置必須更改為：

- 活動裝置會保留中斷前的完整配置，同時會刪除HA配置。
- 除了HA配置之外，備用裝置還刪除了所有介面配置。儘管子介面未禁用，但所有物理介面都處於禁用狀態。管理介面保持活動狀態，因此您可以登入裝置並重新配置裝置。

工作需求：

從安全防火牆裝置管理器圖形介面中斷高可用性對。

解決方案：

步驟1.按一下「Device」。



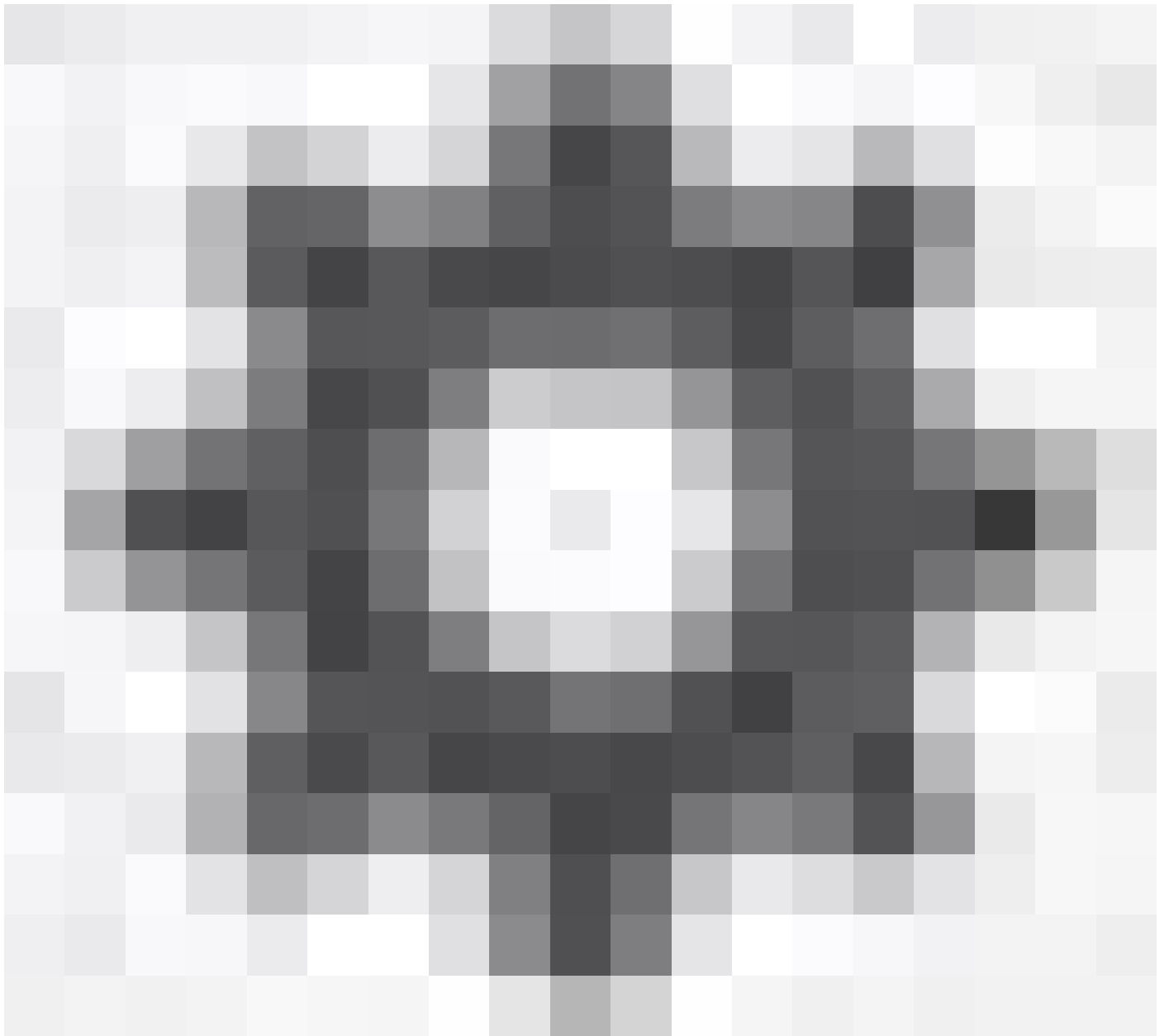
Device: FPR2130-1

步驟2. 按一下裝置摘要右側的High Availability連結。

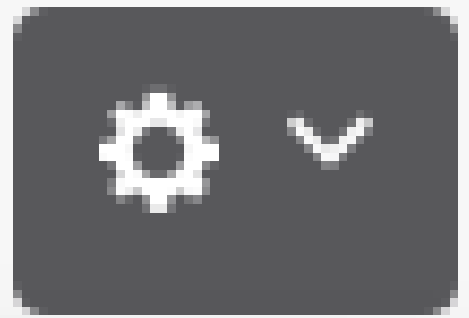
High Availability

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

步驟3. 從齒輪圖示(



, 選擇Break HA。



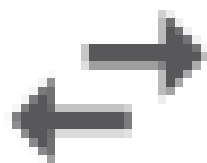
Resume HA



Suspend HA



Break HA

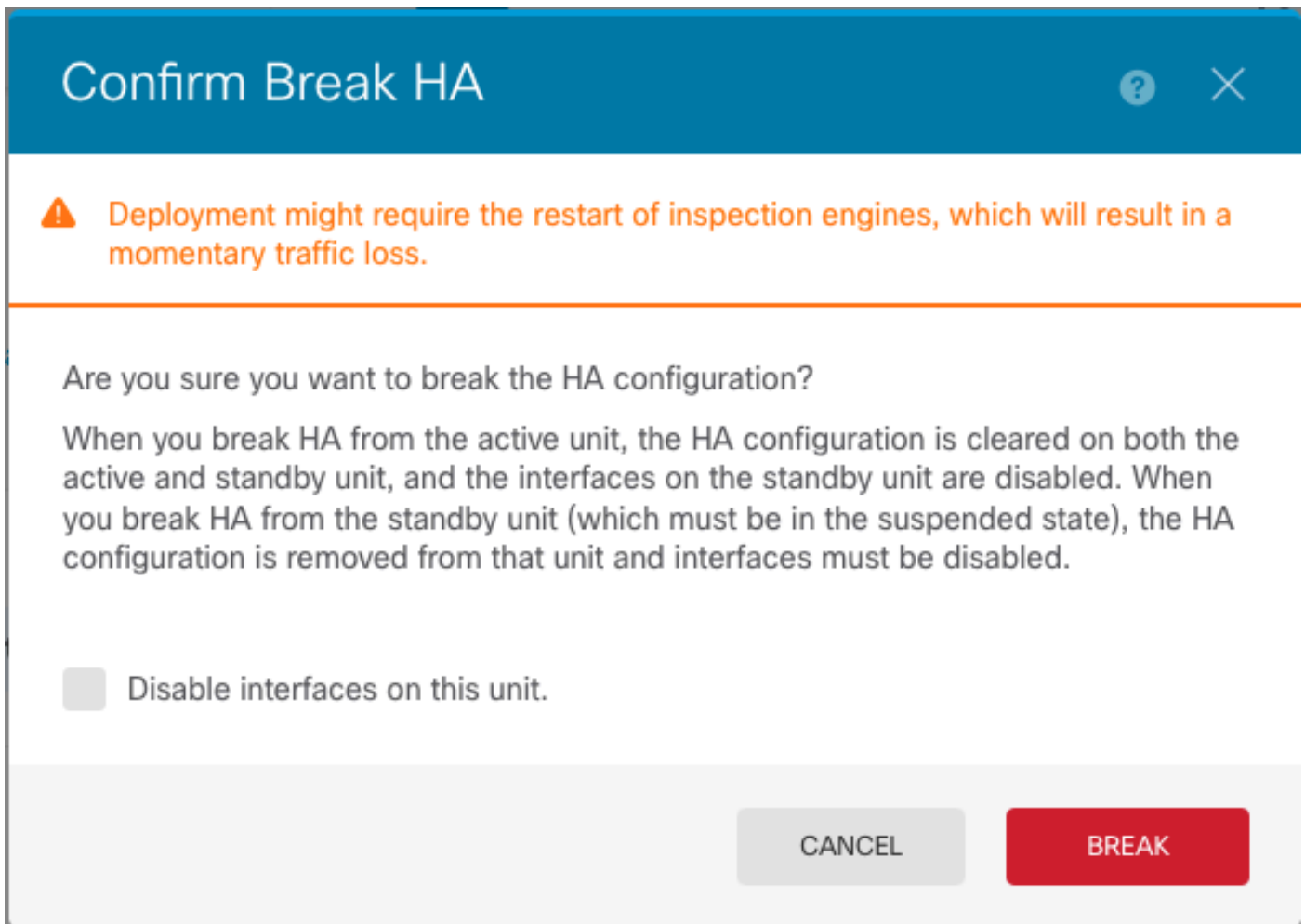


Switch Mode

步驟4. 閱讀確認消息，決定是否選擇禁用介面的選項，然後按一下Break。

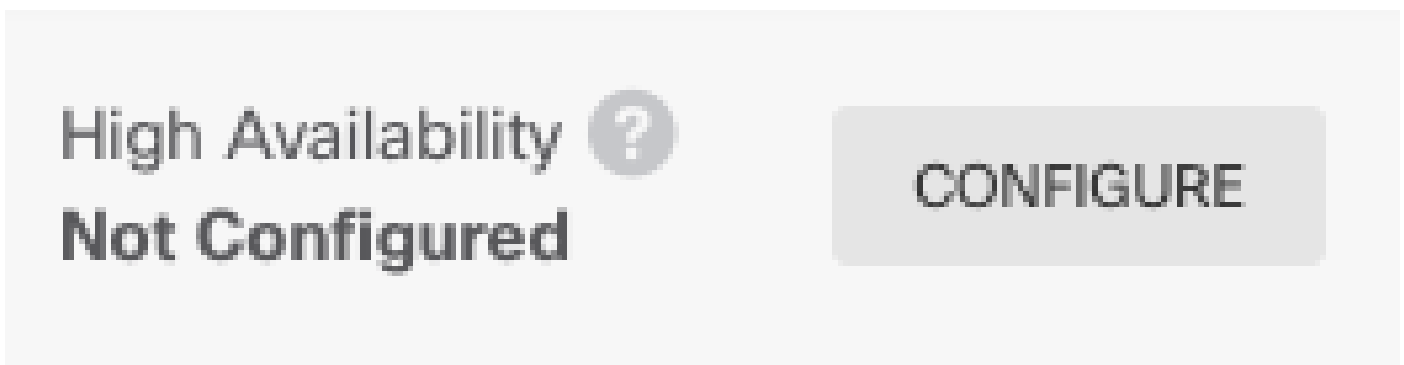
如果要從備用裝置斷開HA，必須選擇禁用介面的選項。

系統會立即在此裝置和對等裝置上部署您的更改（如果可能）。在每台裝置上完成部署以及每台裝置獨立部署可能需要幾分鐘時間。



The image shows a 'Confirm Break HA' dialog box. At the top, there is a blue header with the title 'Confirm Break HA' and a close button (X) and a help icon (?). Below the header, there is an orange warning icon and text: 'Deployment might require the restart of inspection engines, which will result in a momentary traffic loss.' The main body of the dialog asks 'Are you sure you want to break the HA configuration?' and provides detailed instructions: '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.' There is a checkbox labeled 'Disable interfaces on this unit.' At the bottom, there are two buttons: 'CANCEL' and 'BREAK'.

步驟5.驗證結果，如下圖所示：



The image shows a status message: 'High Availability Not Configured' with a help icon (?). To the right of the text is a large grey button labeled 'CONFIGURE'.

相關資訊

- 此處可以找到所有版本的Cisco Secure Firewall Device Manager配置指南

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

- 思科全球技術協助中心(TAC)強烈建議使用以下視覺指南，以瞭解有關Cisco Firepower下一代

安全技術的深入實用知識：

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

- 有關Firepower技術的所有配置和故障排除技術說明

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

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。