

更換安全防火牆中的故障裝置高可用性威脅防禦

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[開始之前](#)

[確定故障裝置](#)

[用備用裝置替換故障裝置](#)

[在不備份的情況下更換故障裝置](#)

[相關資訊](#)

簡介

本文說明如何更換高可用性(HA)設定中的故障Secure Firewall威脅防禦模組。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower可擴充作業系統(FXOS)
- 思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower 4110運行FXOS v2.12(0.498)
- 邏輯裝置運行Cisco安全防火牆7.2.5版

- Secure Firewall Management Center 2600運行v7.4
- 安全複製協定(SCP)知識

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。

背景資訊

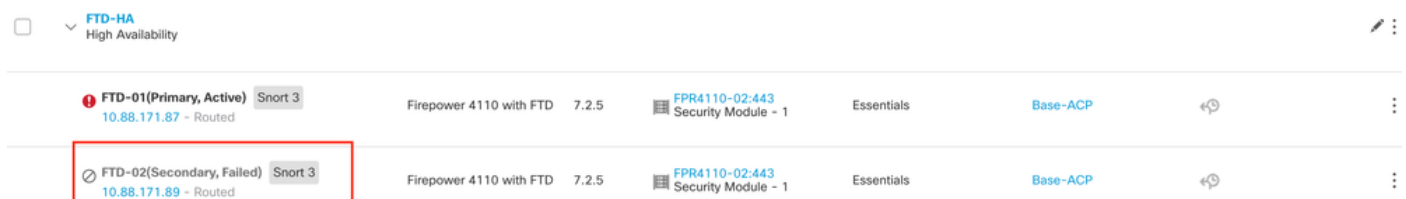
裝置支援以下過程：

- Cisco Secure Firewall 1000系列裝置
- Cisco Secure Firewall 2100系列裝置
- Cisco Secure Firewall 3100系列裝置
- Cisco Secure Firewall 4100系列裝置
- Cisco Secure Firewall 4200系列裝置
- 思科安全防火牆9300裝置
- 適用於VMWare的思科安全防火牆威脅防禦

開始之前

本文檔要求您使用相同的FXOS和FTD版本配置新裝置。

確定故障裝置



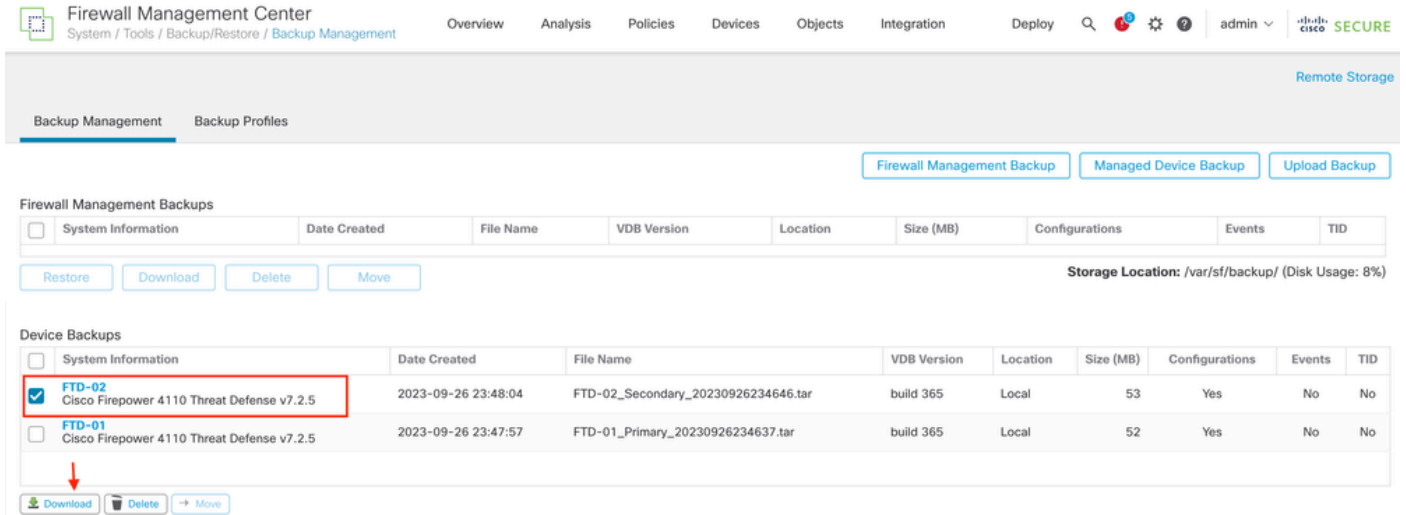
Node	Status	IP	Model	Version	Security Module	Configuration	Actions
FTD-01	Primary, Active	10.88.171.87	Firepower 4110 with FTD	7.2.5	FPR4110-02-443	Essentials, Base-ACP	⌵
FTD-02	Secondary, Failed	10.88.171.89	Firepower 4110 with FTD	7.2.5	FPR4110-02-443	Essentials, Base-ACP	⌵

在此案例中，輔助裝置(FTD-02)處於故障狀態。

用備用裝置替換故障裝置

您可以使用此過程替換主要或輔助裝置。本指南假定您有要更換的故障裝置的備份。

步驟1.從FMC下載備份檔案。導覽至System > Tools > Restore > Device Backups，然後選擇正確的備份。按一下「Download」：



步驟2.將FTD備份上傳到新FTD的/var/sf/backup/目錄：

2.1從test-pc (SCP客戶端) 將備份檔案上傳到/var/tmp/目錄下的FTD:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

2.2在FTD CLI專家模式下，將備份檔案從/var/tmp/移動到/var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

步驟3.從清潔模式應用下一個命令，以還原FTD-02備份:

```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar
```

```
Device model from backup :: Cisco Firepower 4110 Threat Defense
```

```
This Device Model :: Cisco Firepower 4110 Threat Defense
```

```
*****
```

```
Backup Details
```

```
*****
```

```
Model = Cisco Firepower 4110 Threat Defense
```

```
Software Version = 7.2.5
```

Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar

***** Caution *****

Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network

Are you sure you want to continue (Y/N)Y

Restoring device

- Added table audit_log with table_id 1
- Added table health_alarm_syslog with table_id 2
- Added table dce_event with table_id 3
- Added table application with table_id 4
- Added table rna_scan_results_tableview with table_id 5
- Added table rna_event with table_id 6
- Added table ioc_state with table_id 7
- Added table third_party_vulns with table_id 8
- Added table user_ioc_state with table_id 9
- Added table rna_client_app with table_id 10
- Added table rna_attribute with table_id 11
- Added table captured_file with table_id 12
- Added table rna_ip_host with table_id 13
- Added table flow_chunk with table_id 14
- Added table rua_event with table_id 15
- Added table wl_dce_event with table_id 16
- Added table user_identities with table_id 17
- Added table whitelist_violations with table_id 18
- Added table remediation_status with table_id 19
- Added table syslog_event with table_id 20
- Added table rna_service with table_id 21
- Added table rna_vuln with table_id 22
- Added table SRU_import_log with table_id 23
- Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

The system is going down for reboot NOW!

附註：恢復完成後，裝置將您從CLI註銷、重新啟動並自動連線到FMC。此時，裝置似乎已過時。

步驟 4. 恢復HA同步。在FTD CLI中，輸入configure high-availability resume:

```
>configure high-availability resume
```

FTD高可用性配置現在已完成：

FTD-HA High Availability									
● FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP			⋮	
● FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP			⋮	

在不備份的情況下更換故障裝置

如果沒有故障裝置的備份，可以繼續本指南。您可以替換主裝置或輔助裝置，此過程因裝置是主裝置還是輔助裝置而異。本指南中介紹的所有步驟都是要恢復有故障的輔助裝置。如果要恢復有故障的主裝置，請在步驟5中配置高可用性，即在註冊期間將現有輔助/主用裝置用作主裝置，將替換裝置用作輔助/備用裝置。

步驟1. 導航到 Device > Device Management，獲取高可用性配置的螢幕截圖（備份）。編輯正確的FTD HA配對（按一下鉛筆圖示），然後按一下High Availability選項：

The screenshot displays the 'High Availability Configuration' page for a Cisco Firepower 4110 Threat Defense device. The 'High Availability' tab is selected and highlighted with a red box. The page is divided into several sections:

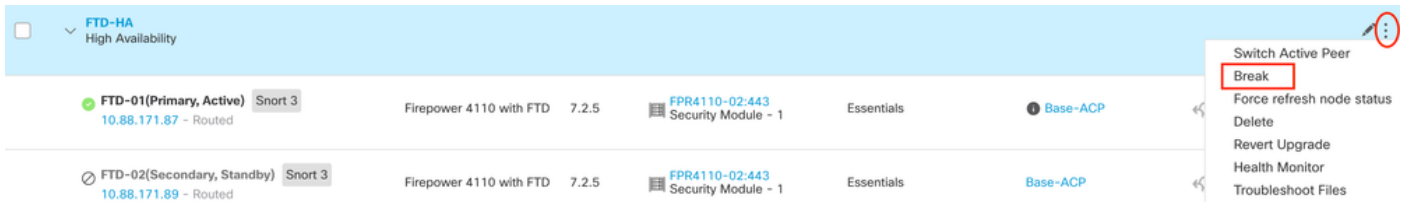
- High Availability Link:** Shows configuration for the primary link (Ethernet1/5) with Logical Name FA-LINK, Primary IP 10.10.10.1, Secondary IP 10.10.10.2, Subnet Mask 255.255.255.252, and IPsec Encryption Disabled.
- State Link:** Shows configuration for the state link (Ethernet1/5) with Logical Name FA-LINK, Primary IP 10.10.10.1, Secondary IP 10.10.10.2, and Subnet Mask 255.255.255.252.
- Monitored Interfaces:** A table listing monitored interfaces with their Active IPv4, Standby IPv4, Active IPv6 - Standby IPv6, Active Link-Local IPv6, Standby Link-Local IPv6, and Monitoring status.
- Fallover Trigger Criteria:** A table listing failure limits and various poll times.
- Interface MAC Addresses:** A table for MAC addresses, currently showing 'No records to display'.

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	192.168.30.1					🟢
diagnostic						🟢
Outside	192.168.16.1					🟢

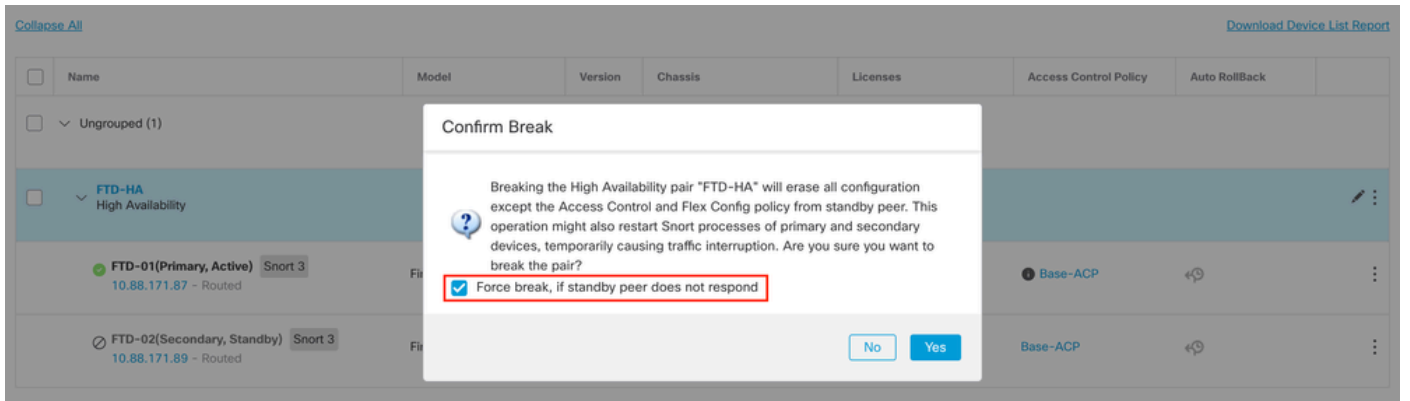
Failure Limit	Value
Failure of 1 Interfaces	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

步驟2. 中斷HA。

2.1 導航到 Devices > Device Management，然後按一下右上角的三點選單。然後按一下Break選項：



2.2. 選擇 Force break , if standby peer does not response 選項 :





附註：由於裝置無響應，您需要強制中斷HA。當您中斷高可用性對時，活動裝置將保留全部署的功能。備用裝置丟失其故障切換和介面配置，成為獨立裝置。

步驟3.刪除有故障的FTD。確定要替換的FTD，然後按一下三點式選單。按一下「Delete」：

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (2)							
<input type="checkbox"/>	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		
<input type="checkbox"/>	FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		

Delete

Packet Tracer

Packet Capture

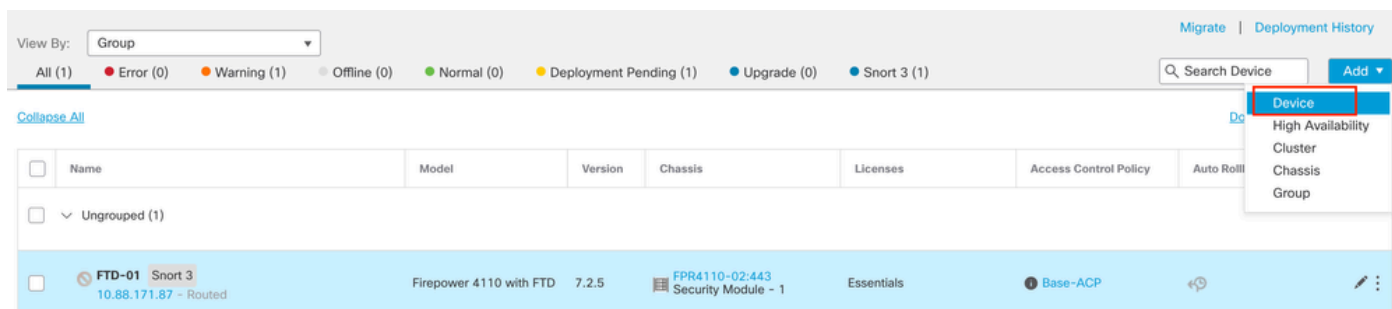
Revert Upgrade

Health Monitor

Troubleshoot Files

步驟4.新增新的FTD。

4.1. 導航到Devices > Device Management > Add，然後按一下Device:



4.2. 選擇預配方法，在本例中為Registration Key，配置Host、Display Name和Registration Key。配置Access Control Policy，然後按一下Register。

Add Device



Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

.....

Group:

None

Access Control Policy:*

Base-ACP

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

- Carrier
- Malware Defense
- IPS
- URL

Advanced

Unique NAT ID:†

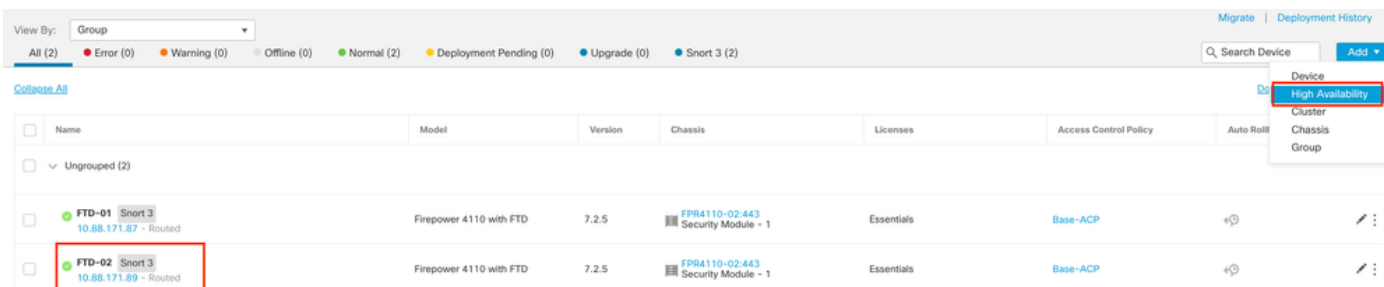
Transfer Packets

Cancel

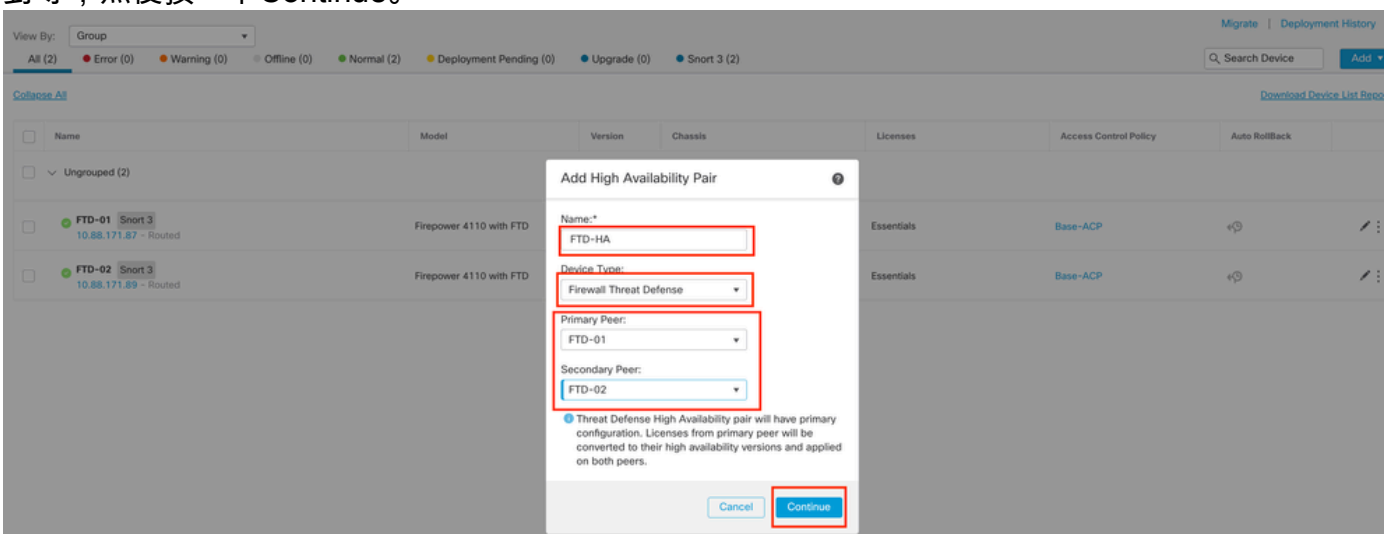
Register

步驟5. 建立HA。

5.1 導航到 Devices > Device Management > Add，然後點選 High Availability 選項。



5.2 配置新增高可用性對。配置名稱、裝置類型，選擇FTD-01作為主對等方，選擇FTD-02作為輔助對等，然後按一下Continue。





附註：請記得選擇主裝置作為仍具有配置的裝置，在本例中為FTD-01。

5.3. 確認建立HA，然後按一下Yes。

Add High Availability Pair



Name:*

FTD-HA

Warning

This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.

Do you want to continue?

Do not display this message again

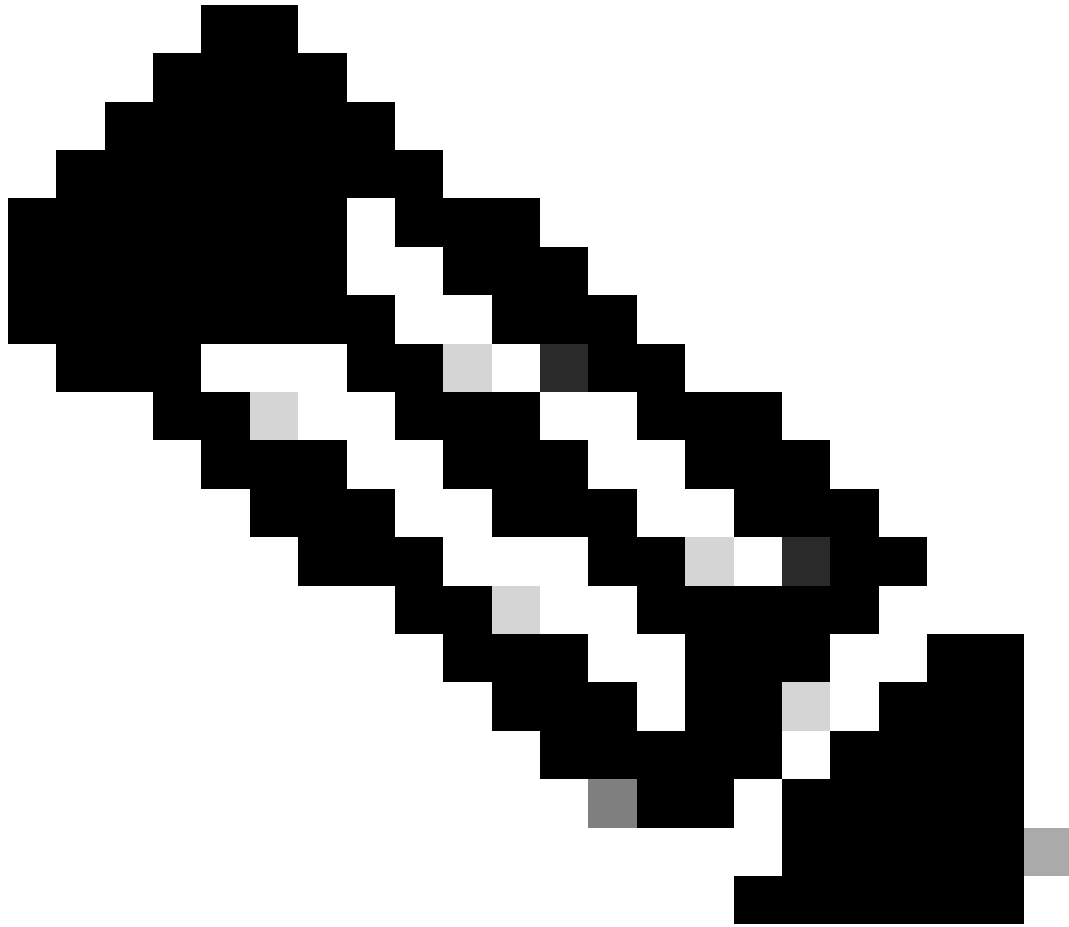
No

Yes

Configuration changes from primary peer will be converted to their high availability versions and applied on both peers.

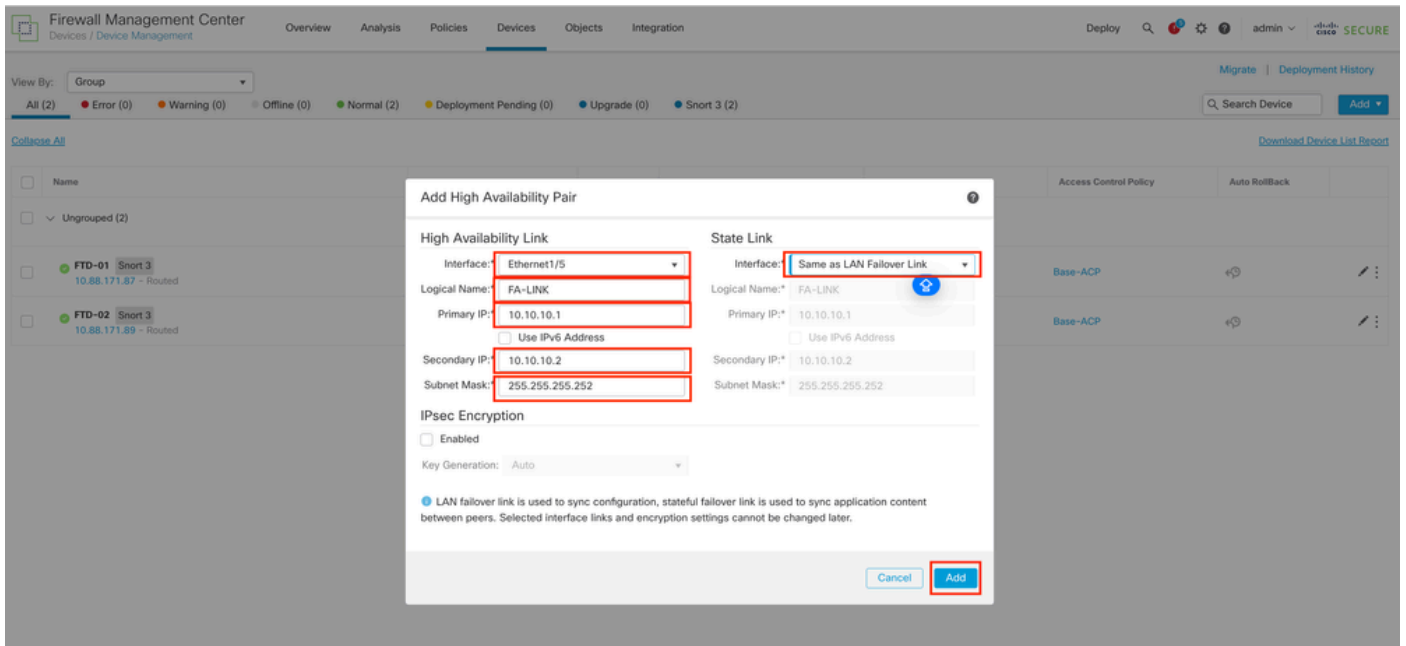
Cancel

Continue



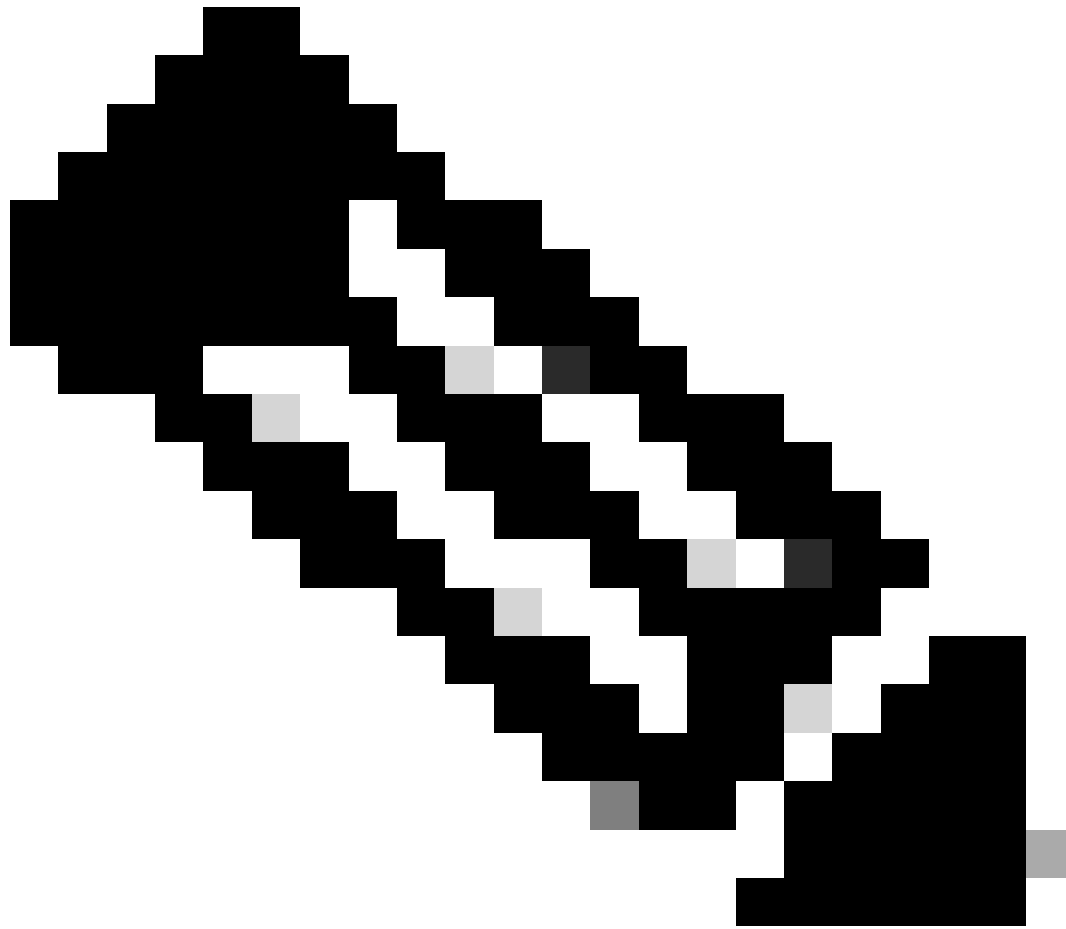
附註：配置高可用性會重新啟動兩台裝置的snort引擎，這可能會導致流量中斷。

5.4. 配置步驟2中介紹的高可用性引數，然後按一下Add選項：



6. FTD高可用性配置現在已完成：

Name	Group	Model	Version	Security Module	Policy	Actions
FTD-01(Primary, Active)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP
FTD-02(Secondary, Standby)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP



附註：如果不配置虛擬MAC地址，您需要清除相連路由器上的ARP表，以便在主裝置更換時恢復流量。有關詳細資訊，請參閱[高可用性中的MAC地址和IP地址](#)。

相關資訊

- [思科技術支援與下載](#)

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）。