整合安全防火牆與L3交換器的備援解決方案

目錄

簡介

本文檔介紹Cisco Catalyst交換機和Cisco安全防火牆之間高可用性冗餘連線的最佳實踐。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆威脅防禦(FTD)
- 安全防火牆管理中心(FMC)
- Cisco IOS® XE
- 虛擬交換系統(VSS)
- 高可用性(HA)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆威脅防禦7.2.5.1版
- 安全防火牆管理器中心版本7.2.5.1
- Cisco IOS XE版本16.12.08

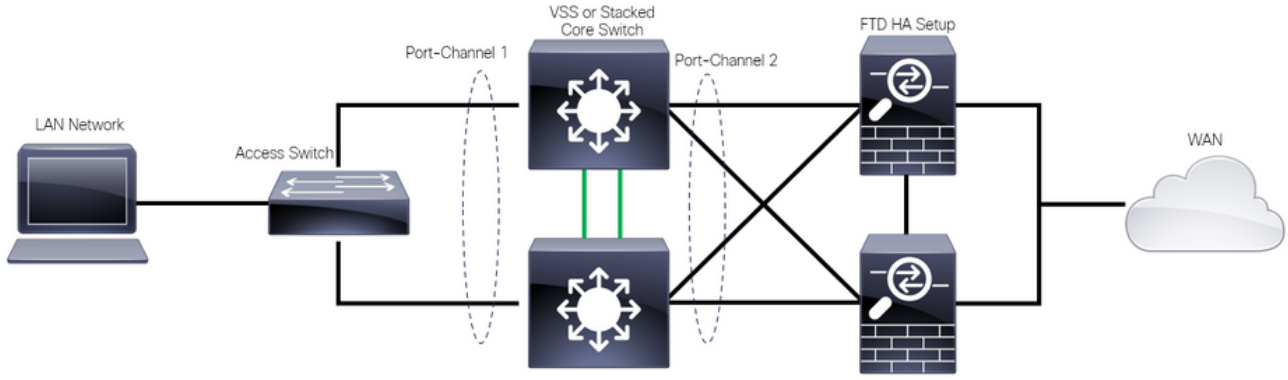
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

有些使用者相信，一個邏輯Catalyst交換器（VSS或堆疊）之間朝向一對HA FTD的單一連線連結（連線埠通道）就足以提供一個完整的備援解決方案，以防一個單元或連結失敗。這是一個常見的誤解，因為VSS或堆疊交換機設定充當單個邏輯裝置。同時，一對HA FTD充當兩個不同的邏輯裝置，其中一個充當作用中，另一個充當待命。

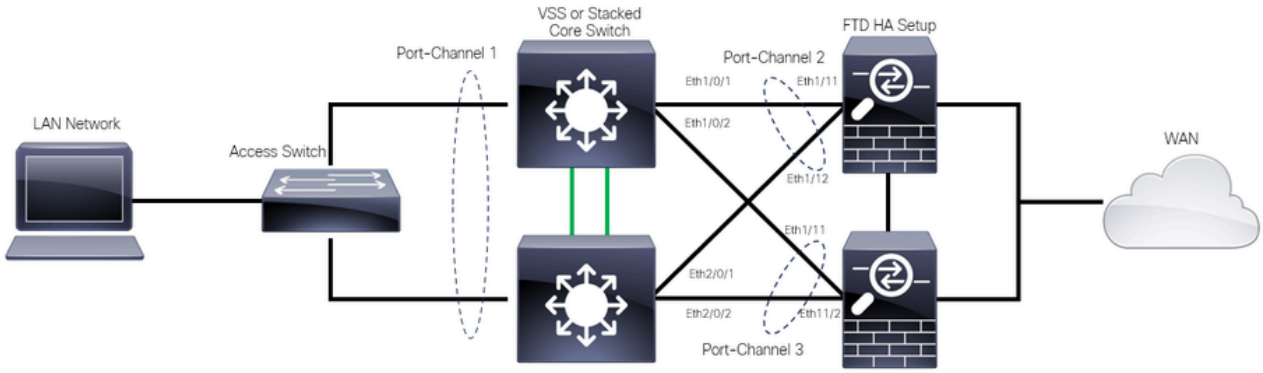
下一個圖表是無效設計，其中從設定的交換器向FTD HA配對設定單一連線埠通道：



設計無效

先前的設定無效，因為此連線埠通道作為連線到兩個不同裝置的單一連結，會造成網路衝突，因此跨距樹狀目錄通訊協定(SPT)會封鎖來自其中一個FTD的連線。

下圖是有效的設計，其中為交換機VSS或堆疊的每個成員配置了兩個不同的埠通道。



有效設計

組態

交換機配置

步驟 1.使用各自的虛擬區域網路(VLAN)設定連線埠通道。

```
MXC.PS.A.06-3850-02#configure terminal
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
```

```
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
% Access VLAN does not exist. Creating vlan 300
MXC.PS.A.06-3850-02(config-if)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
MXC.PS.A.06-3850-02(config-if)#no shutdown
MXC.PS.A.06-3850-02(config-if)#exit
!
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 2/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
MXC.PS.A.06-3850-02(config-if)#channel-group 2 mode active
MXC.PS.A.06-3850-02(config-if)#exit
!
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/2
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
MXC.PS.A.06-3850-02(config-if)#channel-group 3 mode active
Creating a port-channel interface Port-channel 3
MXC.PS.A.06-3850-02(config-if)#no shutdown
MXC.PS.A.06-3850-02(config-if)#exit
!
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 2/0/2
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
MXC.PS.A.06-3850-02(config-if)#channel-group 3 mode active
```

步驟 2.為連線埠通道VLAN設定交換虛擬介面(SVI) IP位址。

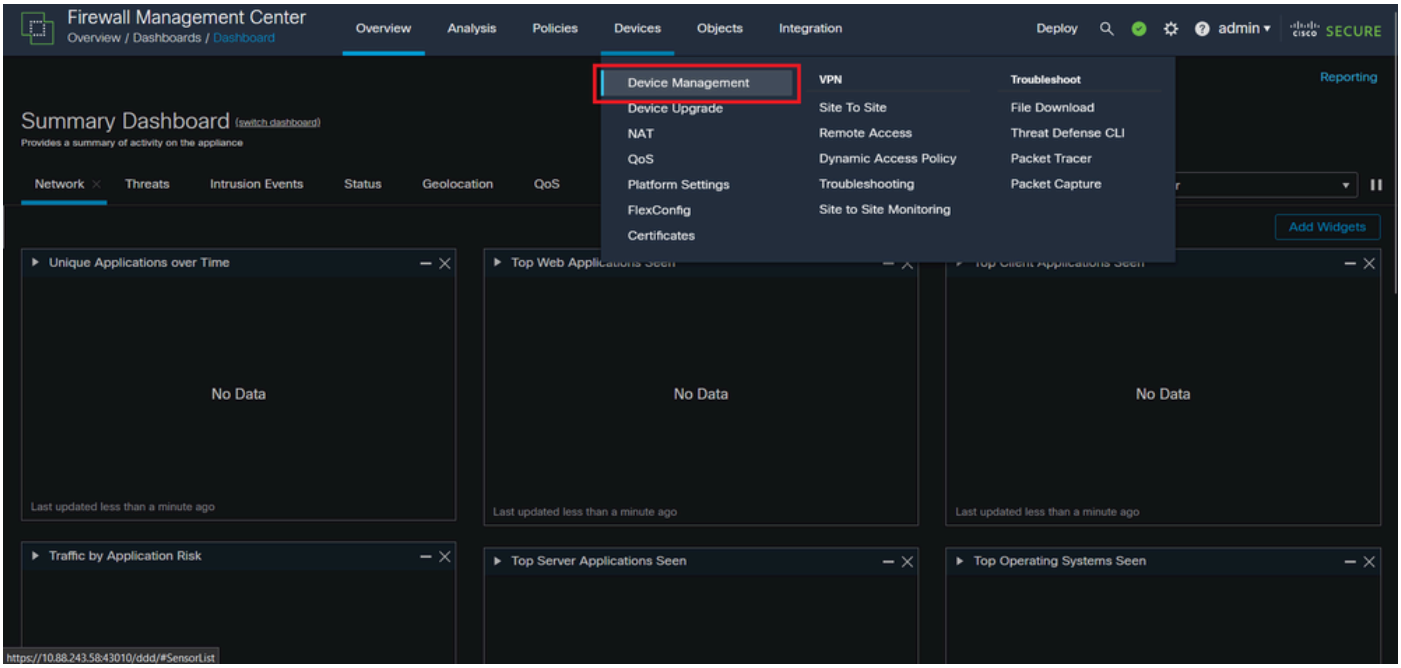
```
MXC.PS.A.06-3850-02(config-if)#exit
MXC.PS.A.06-3850-02(config)#interface VLAN 300
MXC.PS.A.06-3850-02(config-if)#ip address 10.8.4.31 255.255.255.0
MXC.PS.A.06-3850-02(config-if)#no shutdown
```

FTD HA組態

步驟 1.登入FMC GUI。

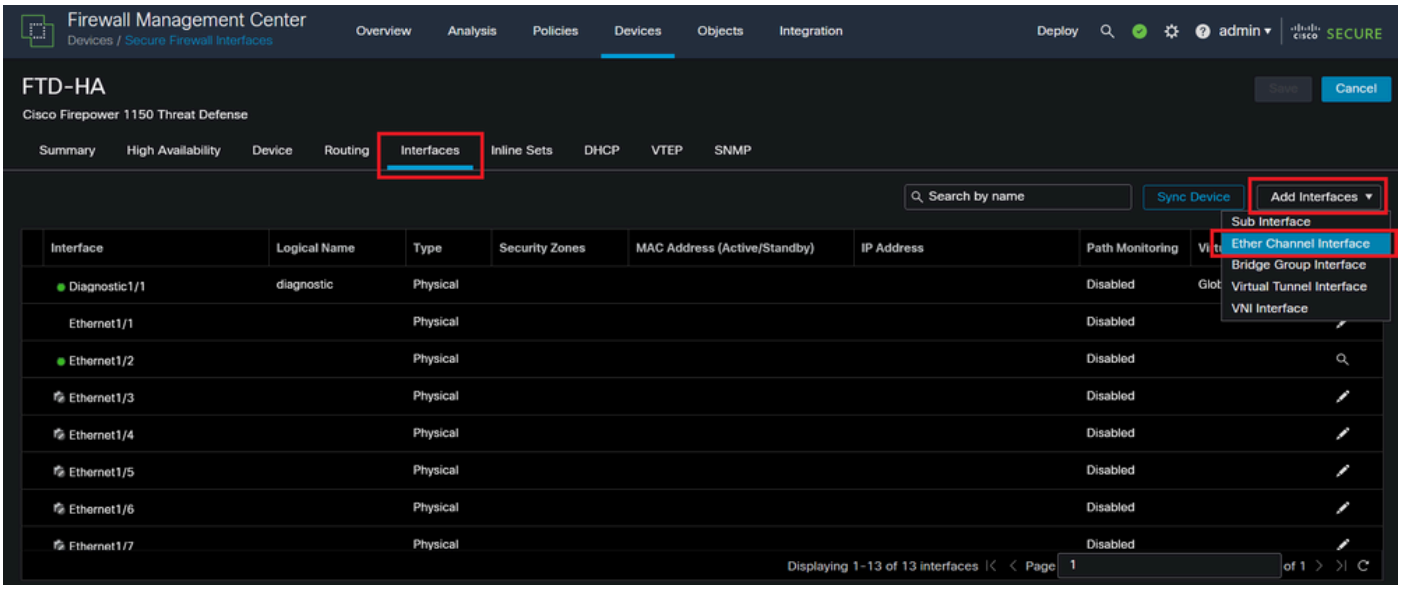
FMC登入

步驟 2.導航到裝置>裝置管理。



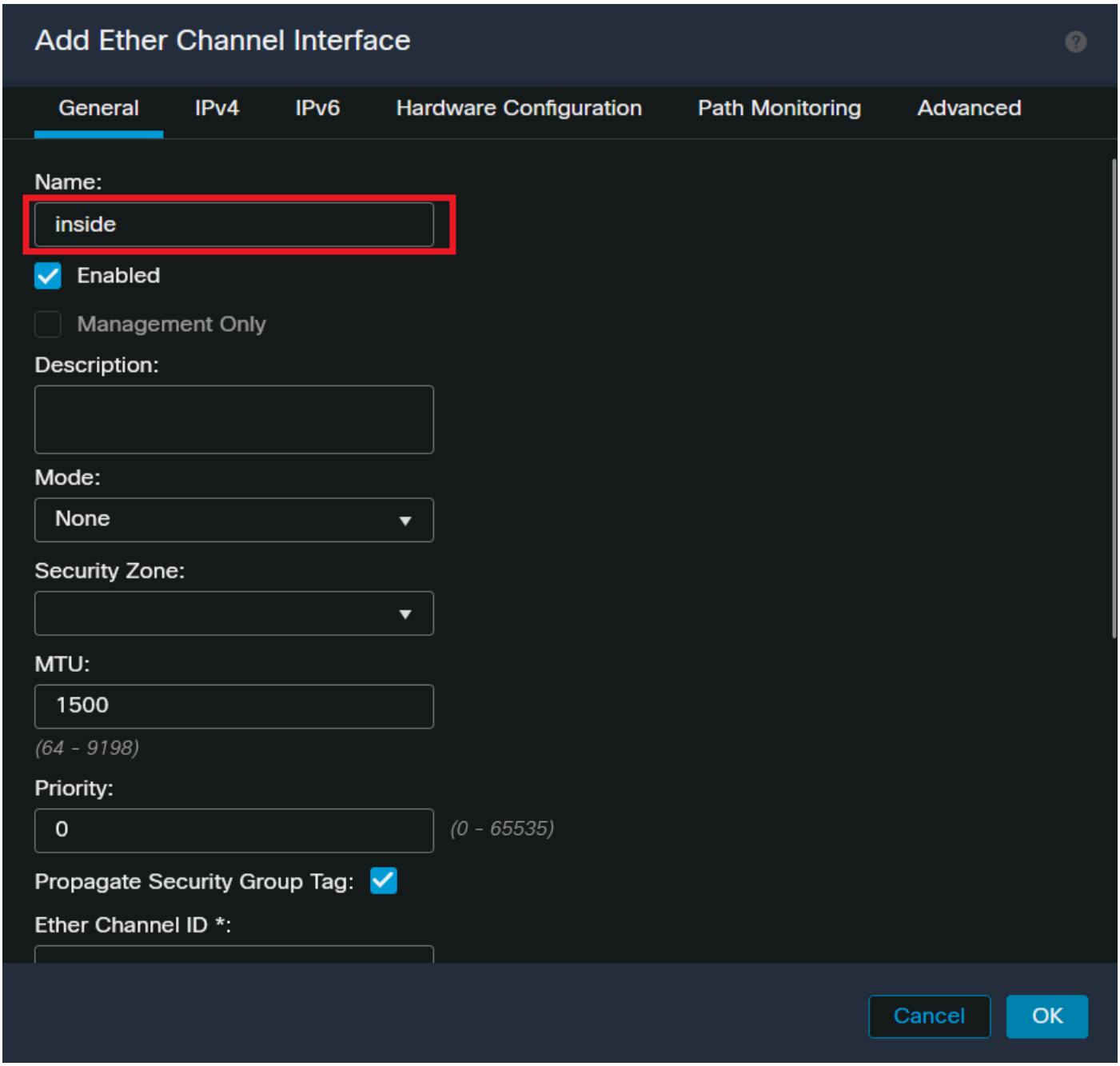
裝置管理

步驟 3.編輯所需的HA裝置，然後導航到Interfaces > Add Interfaces > Ether Channel Interface。

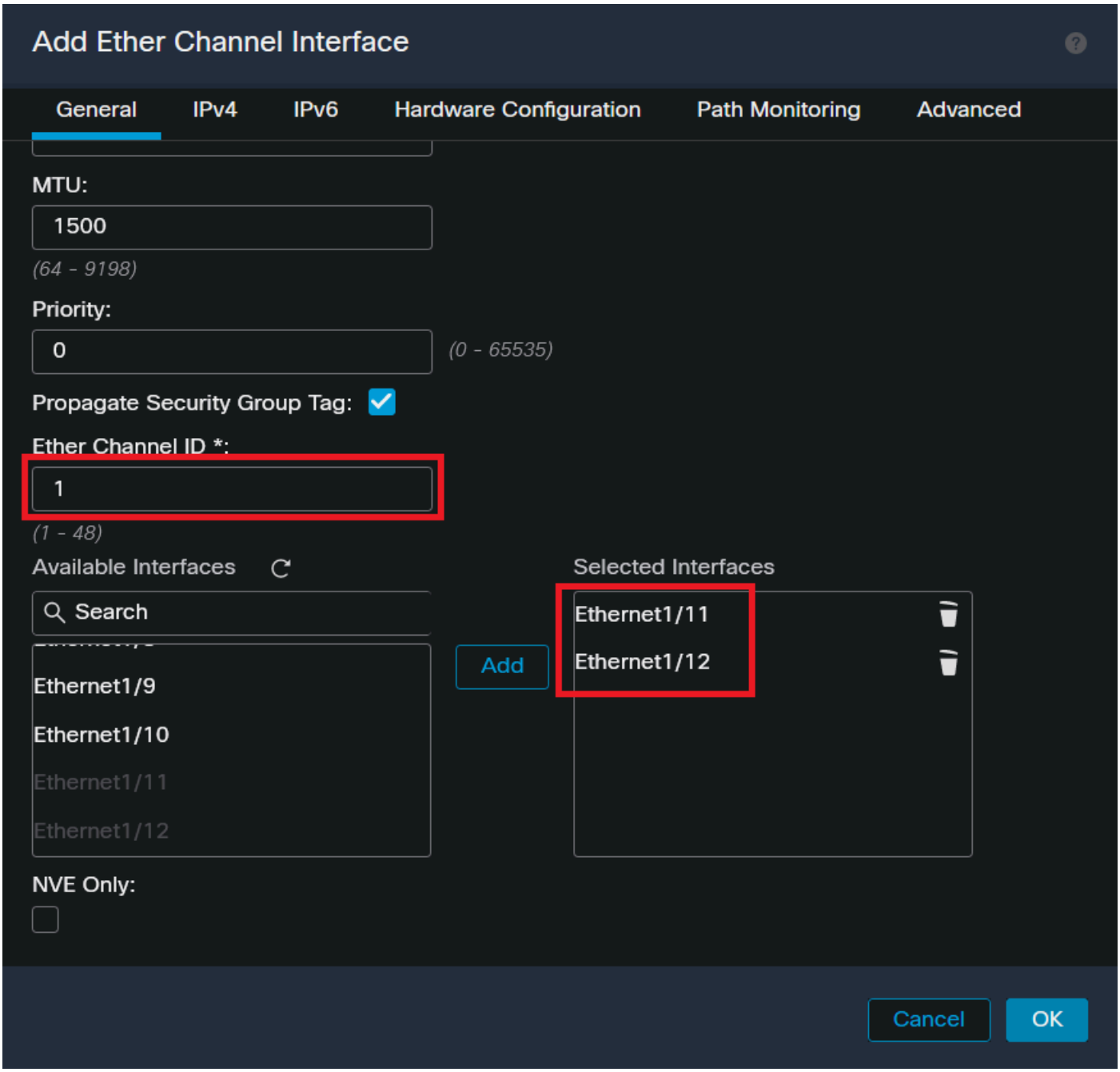


Ether-Channel建立

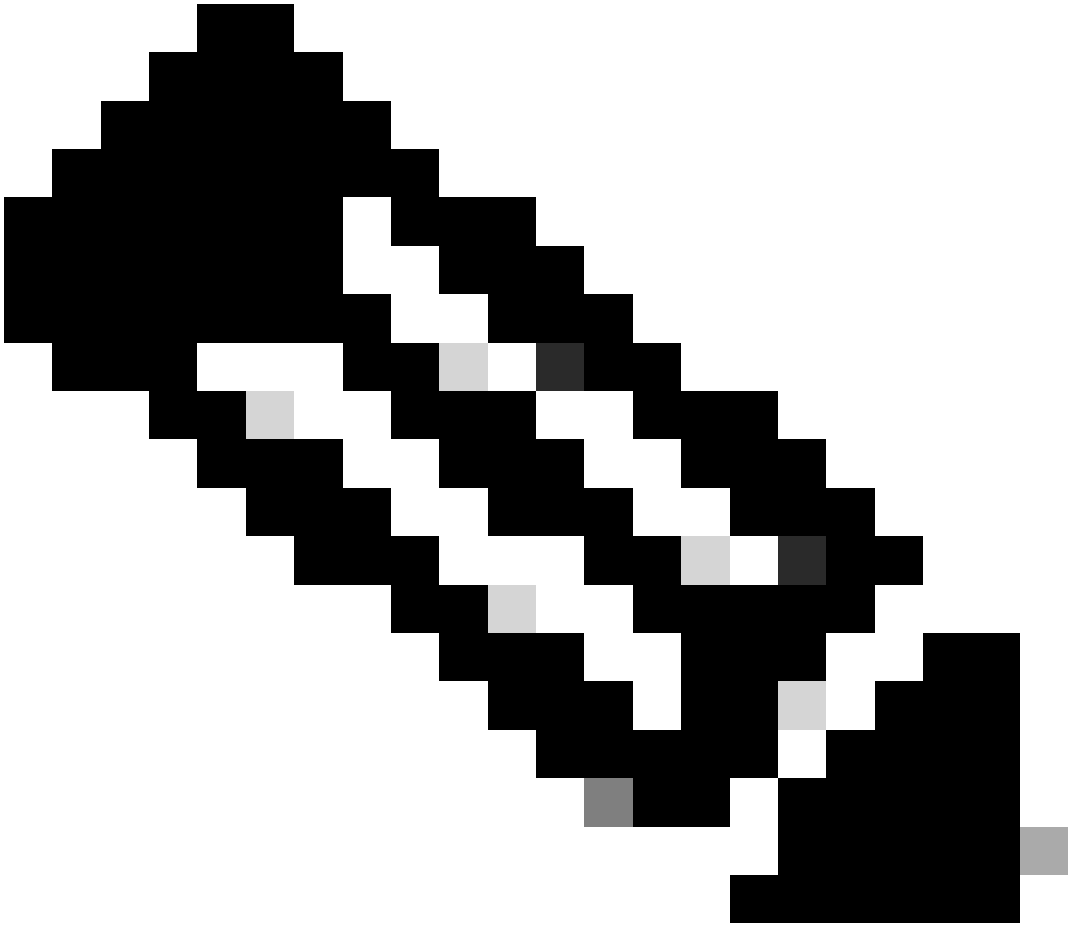
步驟 4.增加介面名稱、乙太網通道ID和成員介面。



Ether-Channel名稱

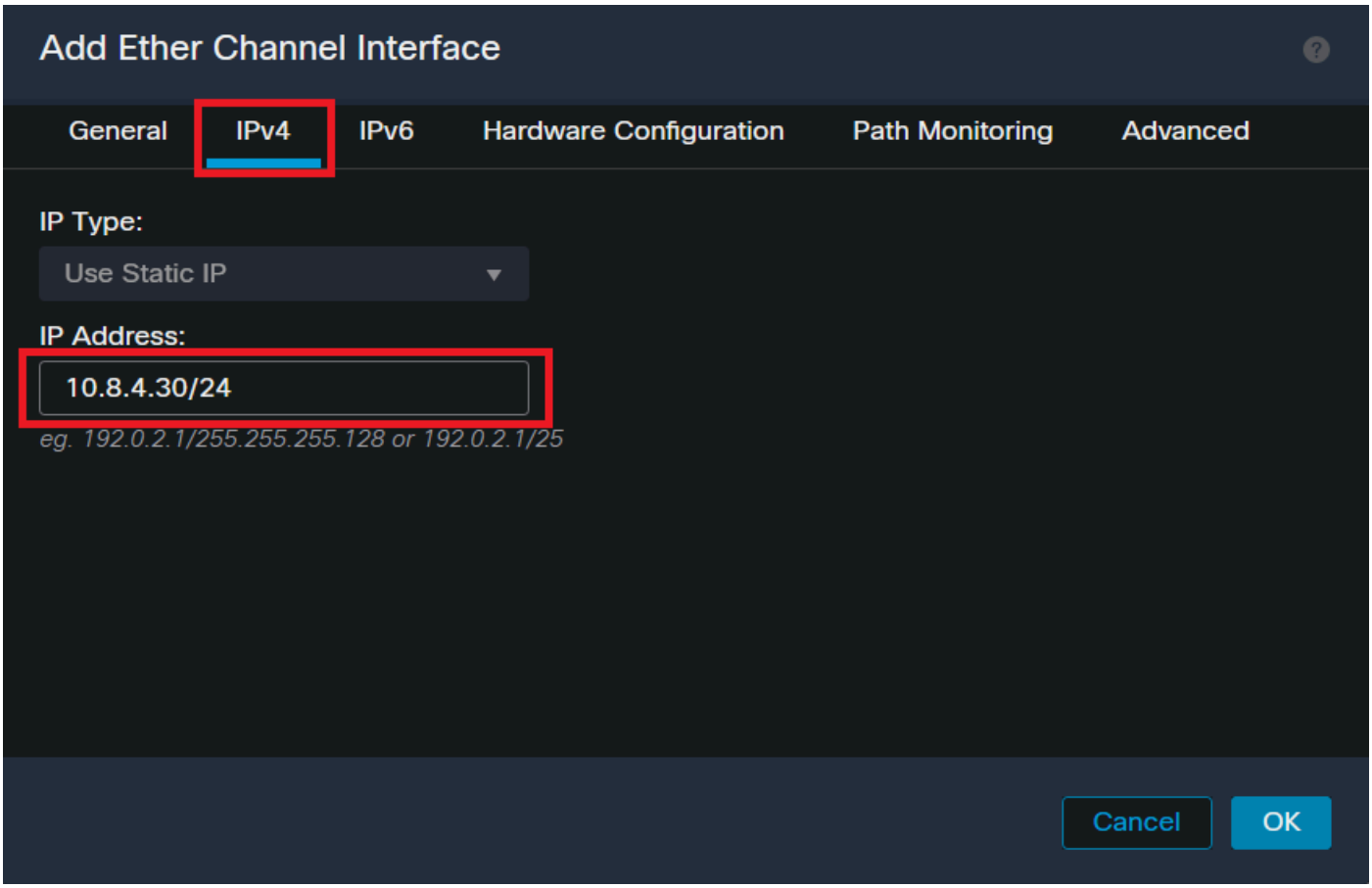


Ether-Channel ID和成員



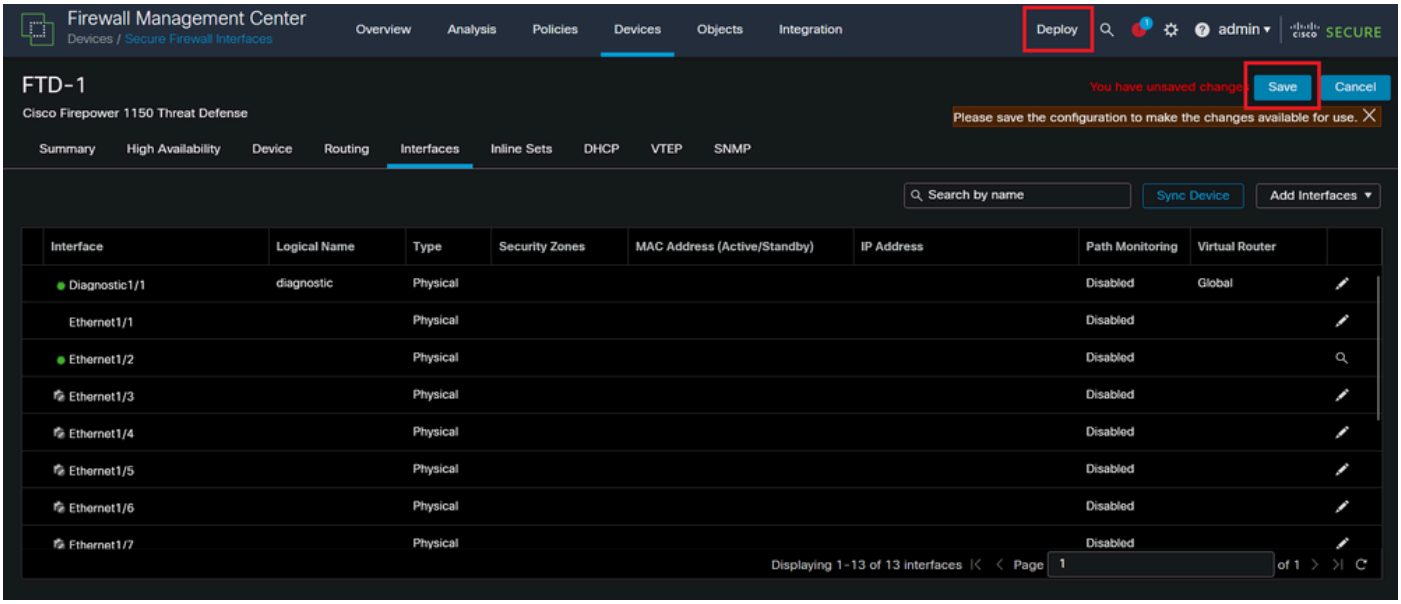
注意：FTD上的乙太通道ID不需要與交換器上的連線埠通道ID相符。

步驟 5.導航到IPv4頁籤，然後在與交換機的VLAN 300相同的子網中增加一個IP地址。



Ether-Channel IP地址

步驟 6.儲存變更並進行部署。



儲存與部署

驗證

步驟 1.確保VLAN和埠通道介面的Status從交換機的角度為up。

```
MXC.PS.A.06-3850-02#show ip interface brief
Interface IP-Address OK? Method Status Protocol
***OUTPUT OMITTED FOR BREVITY***
Vlan300 10.8.4.31 YES manual up up
***OUTPUT OMITTED FOR BREVITY***
Port-channel2 unassigned YES unset up up
Port-channel3 unassigned YES unset up up
```

步驟 2.透過訪問裝置命令列介面，檢查兩個FTD單元上的埠通道Status是否均為up。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# show interface ip brief
***OUTPUT OMITTED FOR BREVITY***
Port-channel1 10.8.4.30 YES unset up up
***OUTPUT OMITTED FOR BREVITY***
```

步驟 3.檢查交換器SVI和FTD連線埠通道IP位址之間的連線能力。

```
MXC.PS.A.06-3850-02#ping 10.8.4.30 source vlan 300
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.4.34, timeout is 2 seconds:
Packet sent with a source address of 10.8.4.31
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

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）。