Integración de una solución redundante para un firewall seguro y un switch L3

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Configurar

- Diagrama de la red
- Configuraciones
  - Configuración del switch
  - Configuración de FTD HA

Verificación

Introducción

Este documento describe una práctica recomendada para conexiones redundantes entre switches Catalyst de Cisco y firewalls seguros de Cisco en alta disponibilidad.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protección frente a amenazas de firewall (FTD)
- Centro de gestión de firewall seguro (FMC)
- Cisco IOS® XE
- Sistema de switching virtual (VSS)
- Alta disponibilidad (HA)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Firewall Threat Defence versión 7.2.5.1
- Secure Firewall Manager Center versión 7.2.5.1
- Cisco IOS XE versión 16.12.08

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

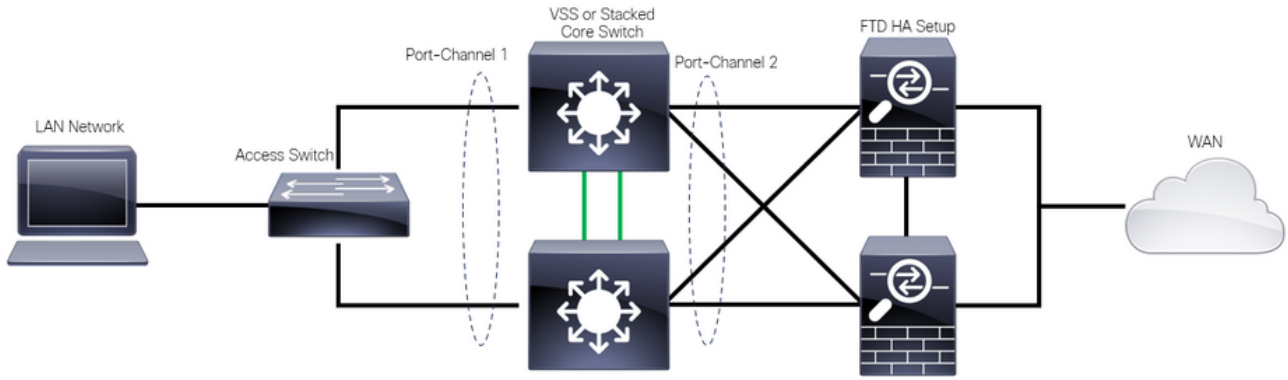
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

Hay usuarios que creen que un único enlace de conexión (canal de puerto) entre un switch Catalyst lógico (VSS o apilado) y un par de FTD de HA es suficiente para tener una solución redundante completa en caso de que una unidad o un enlace falle. Se trata de un error habitual, ya que una configuración de VSS o switch apilado actúa como un único dispositivo lógico. Mientras que al mismo tiempo, un par de FTD de HA actúan como dos dispositivos lógicos diferentes con uno como activo y el otro como en espera.

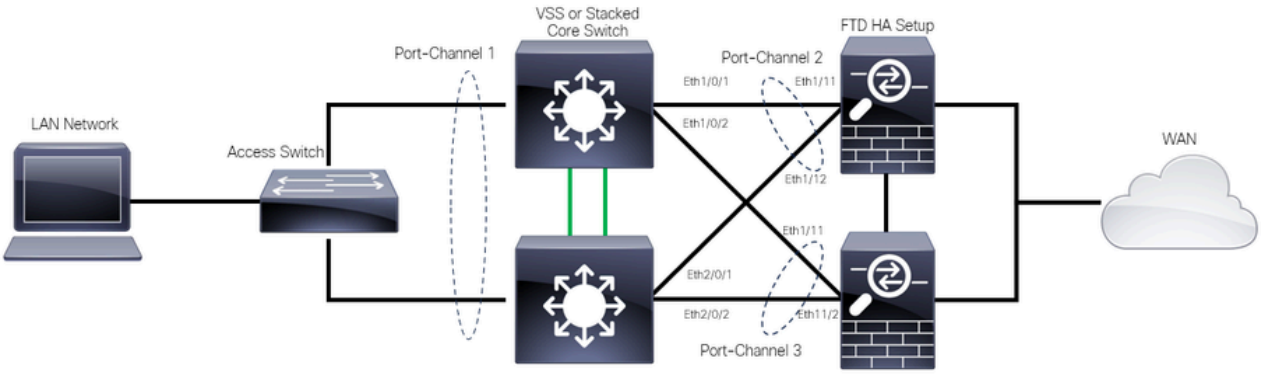
El siguiente diagrama es un diseño no válido en el que se configura un solo canal de puerto desde el switch configurado hacia el par FTD HA:



Diseño no válido

La configuración anterior no es válida porque este canal de puerto actúa como un único enlace conectado a dos dispositivos diferentes, lo que provoca colisiones de red, por lo que el protocolo de árbol de extensión (SPT) bloquea las conexiones de uno de los FTD.

El siguiente diagrama es un diseño válido en el que se configuran dos Port-Channels diferentes para cada miembro del VSS o la pila del switch.



Configuraciones

Configuración del switch

Paso 1. Configure los canales de puerto con sus respectivas redes de área local virtual (VLAN).

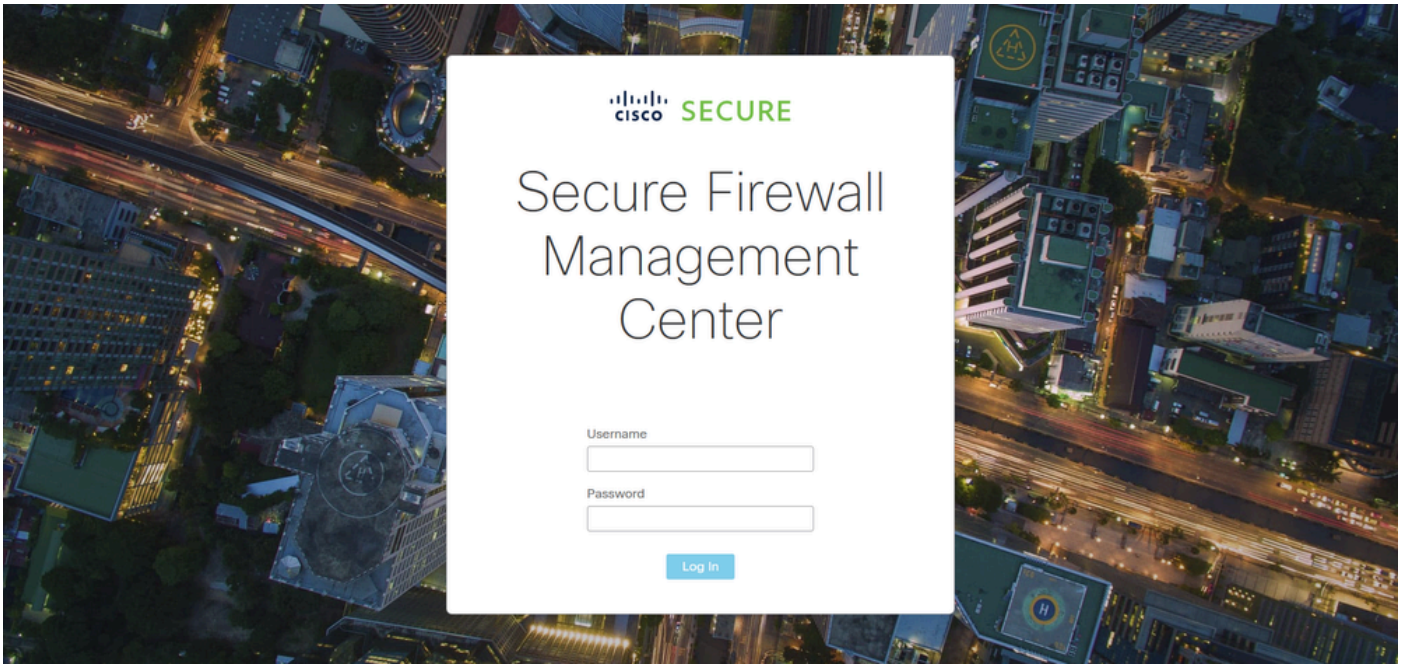
```
MXC.PS.A.06-3850-02#configure terminal
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
% Access VLAN does not exist. Creating vlan 300
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
```

Paso 2. Configure una dirección IP de interfaz virtual conmutada (SVI) para la VLAN de canal de puerto.

```
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
```

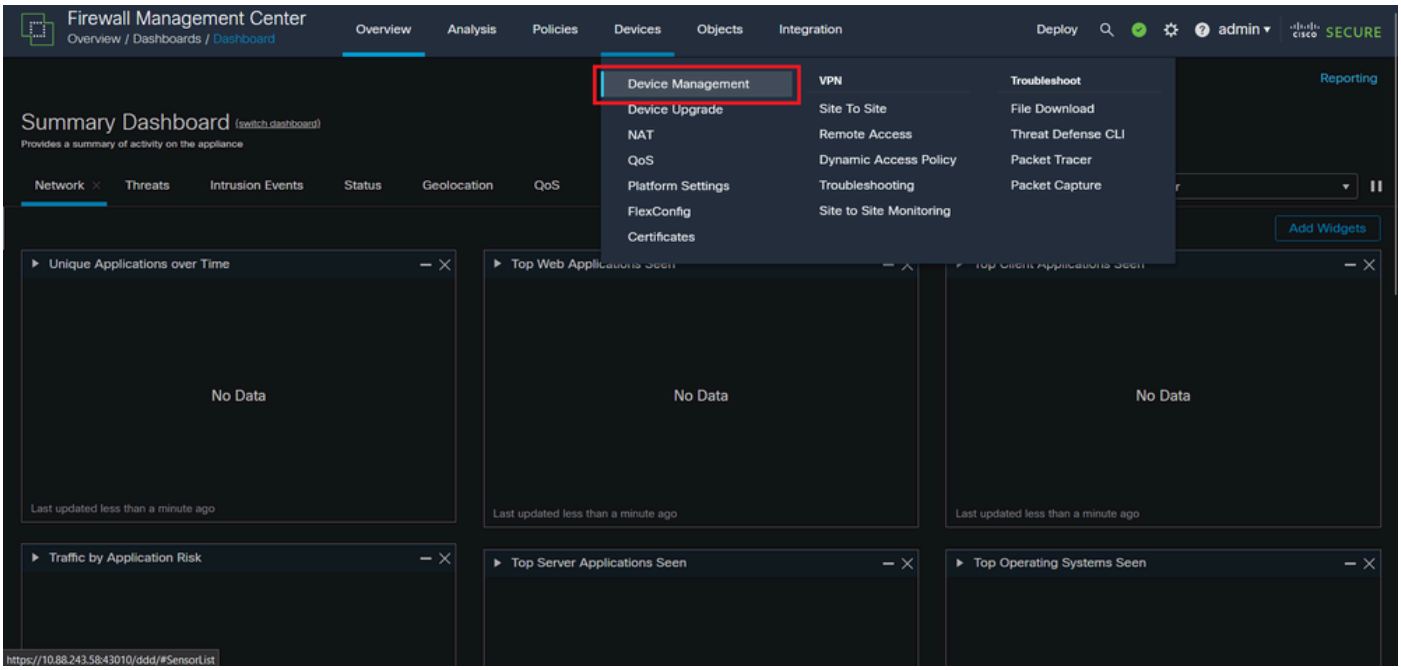
Configuración de FTD HA

Paso 1. Inicie sesión en la GUI de FMC.



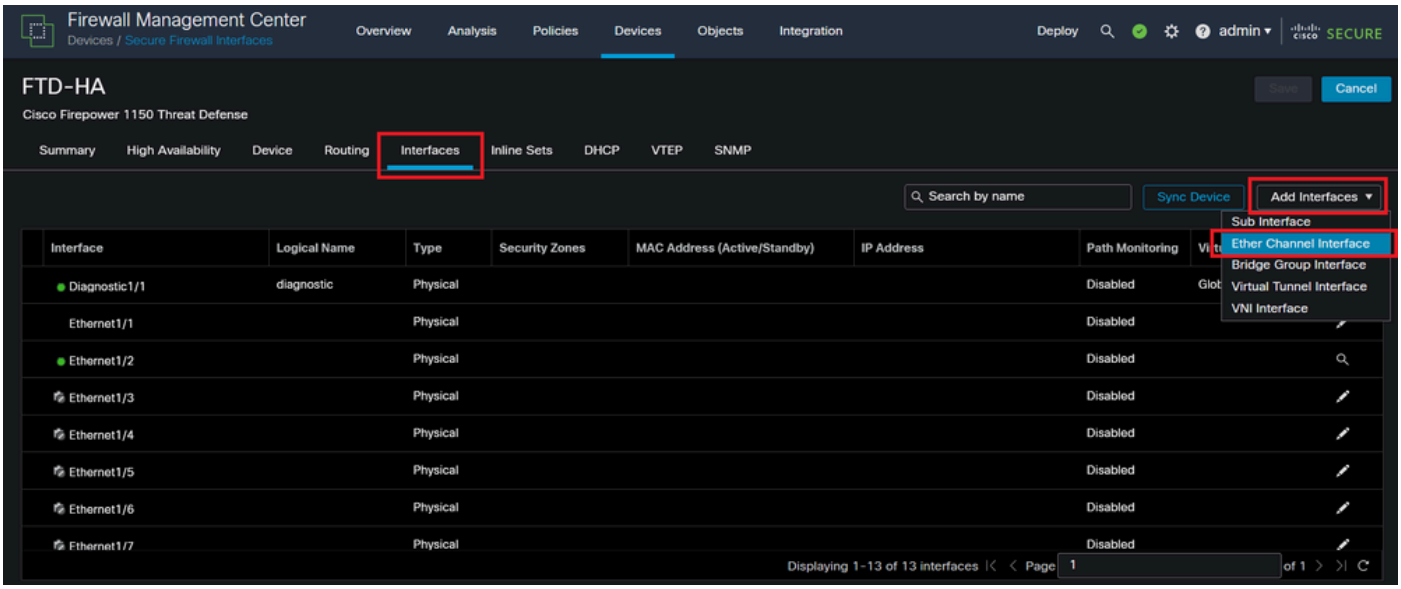
Inicio de sesión en FMC

Paso 2. Vaya a Devices > Device Management.



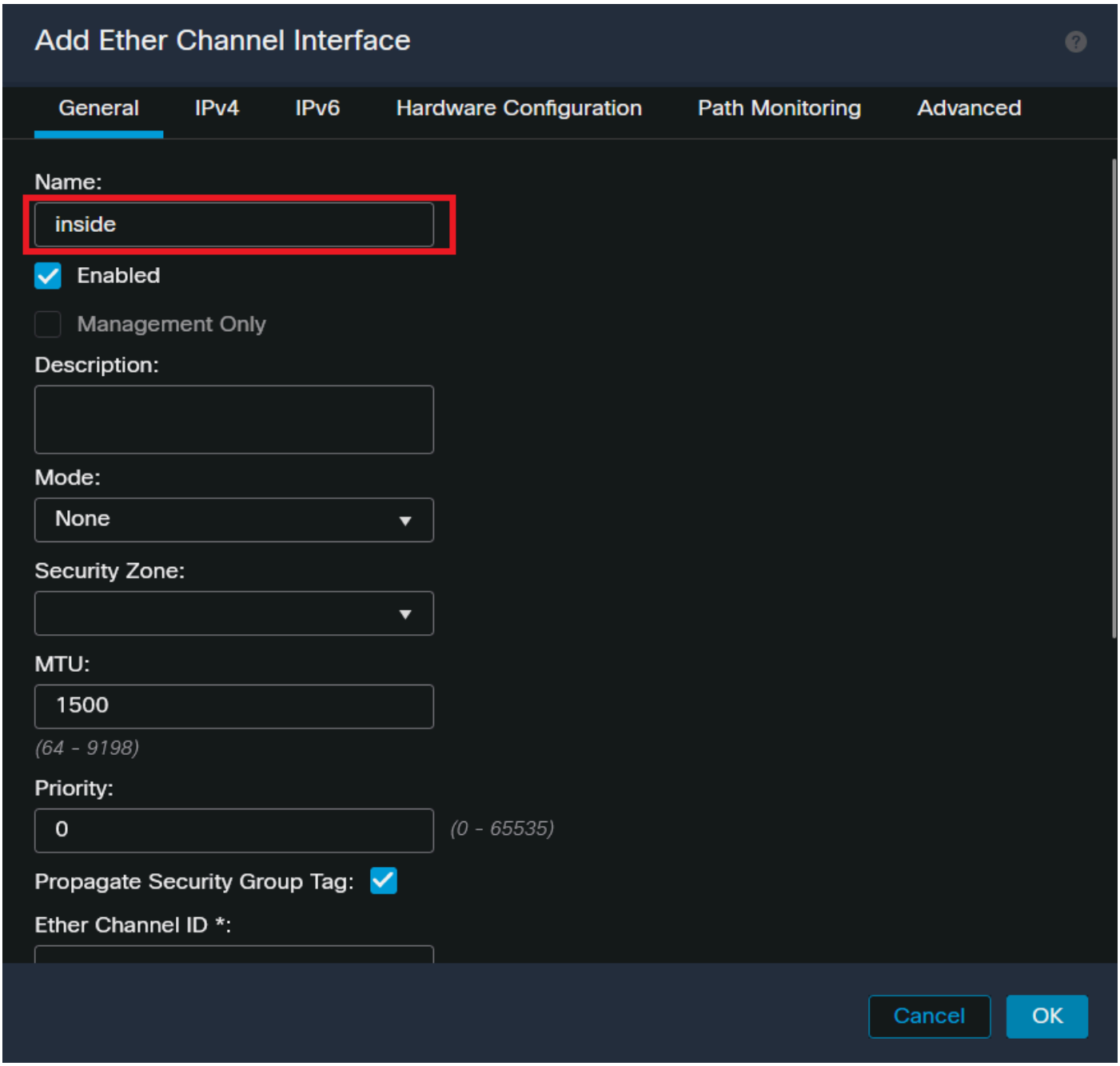
Gestión de dispositivos

Paso 3. Edite el dispositivo HA deseado y navegue hasta Interfaces > Add Interfaces > Ether Channel Interface.

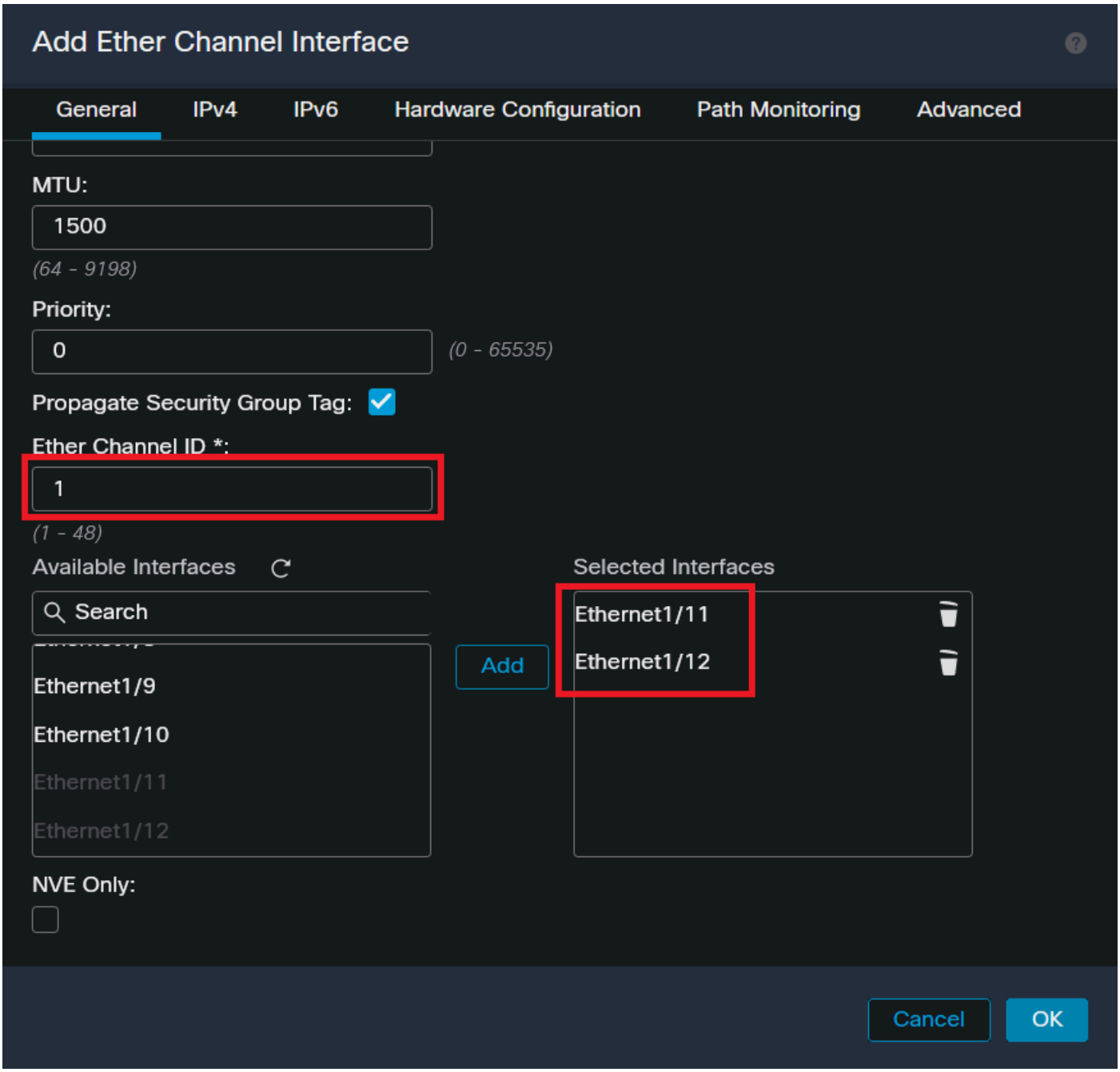


Creación de Ether-Channel

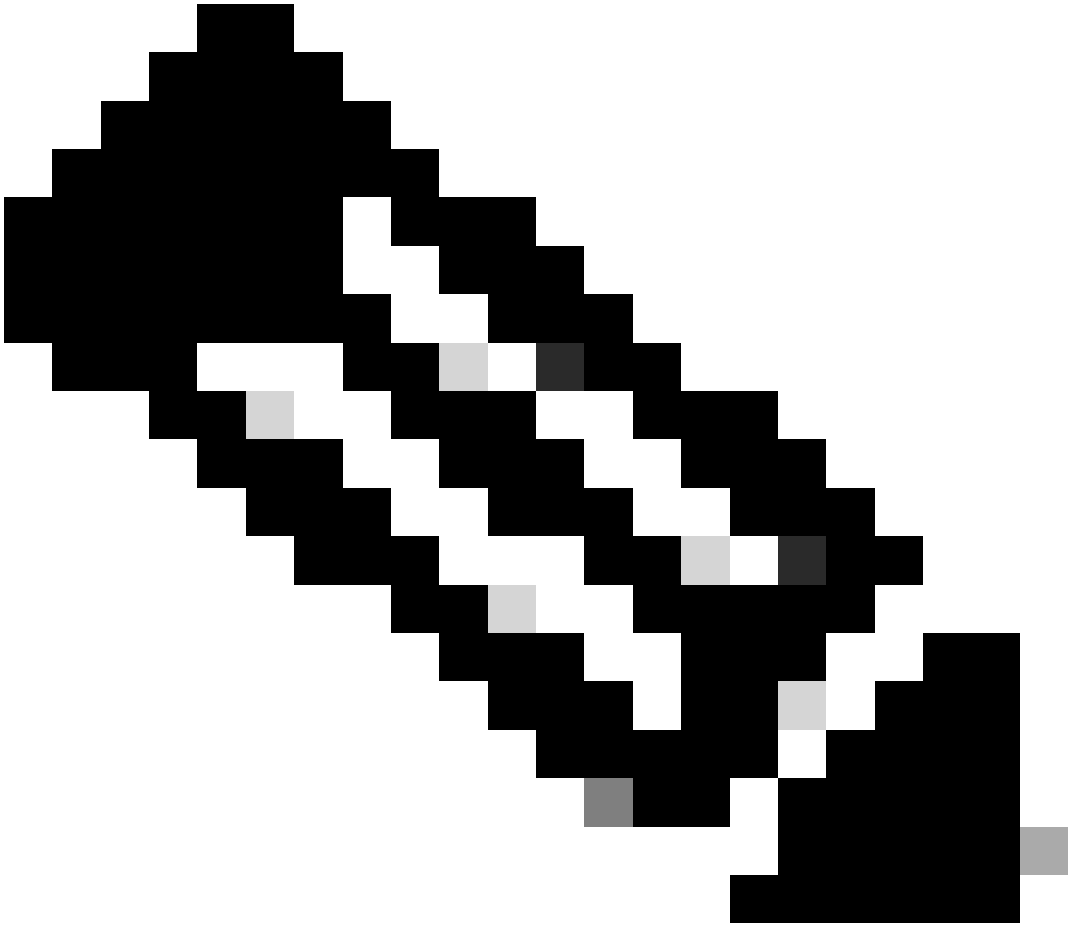
Paso 4. Agregue un nombre de interfaz, un ID de canal Ether y las interfaces de miembro.



Nombre de canal Ethernet

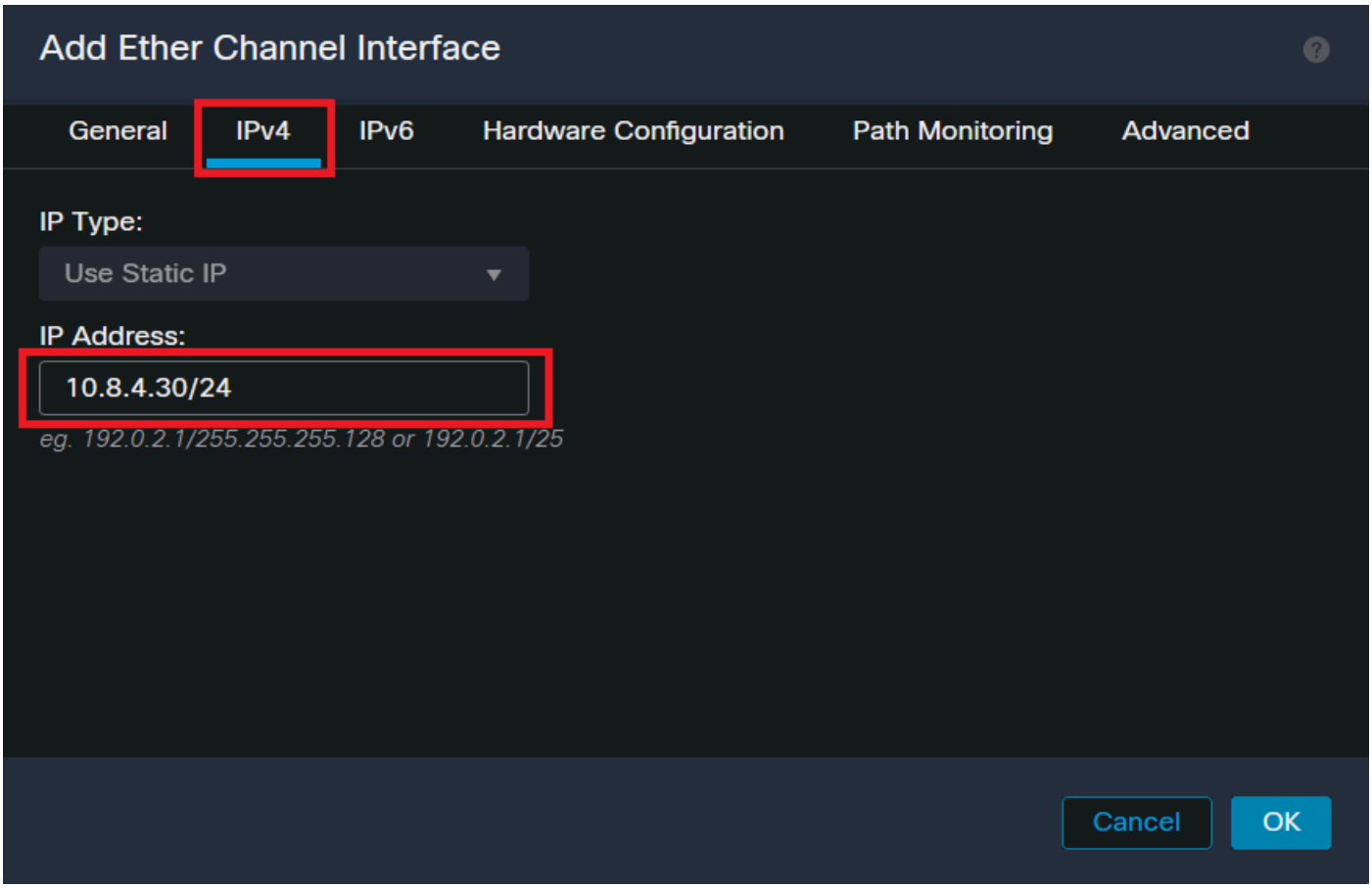


ID y miembros de Ether-Channel



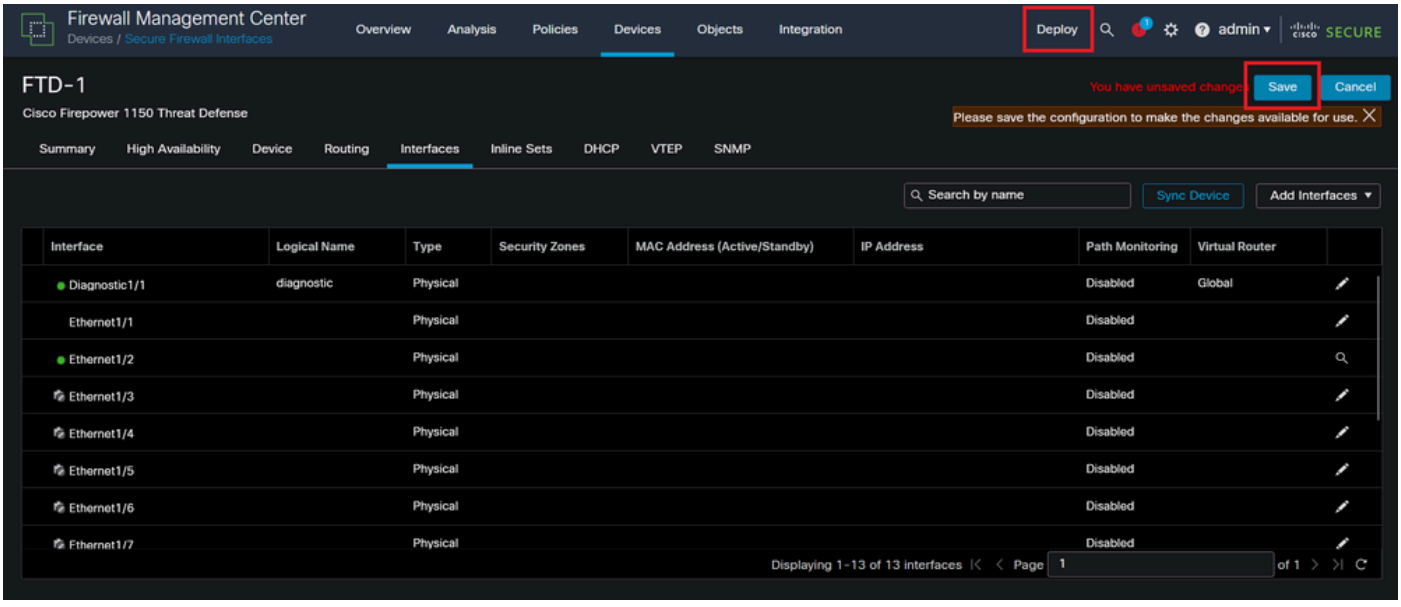
Nota: El ID de canal Ether en el FTD no necesita coincidir con el ID de canal de puerto en el switch.

Paso 5. Vaya a la pestaña IPv4 y agregue una dirección IP en la misma subred que la VLAN 300 para el switch.



Dirección IP de Ether-Channel

Paso 6. Guarde los cambios e impleméntelo.



Guardar e implementar

Verificación

Paso 1. Asegúrese de que el Estado de las interfaces VLAN y de canal de puerto esté activo desde la perspectiva del switch.

```
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
```

Paso 2. Verifique que el Estado del canal de puerto esté activo en ambas unidades FTD accediendo a la interfaz de línea de comandos del dispositivo.

```
> 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***
```

Paso 3. Compruebe la disponibilidad entre la SVI del switch y la dirección IP del canal de puerto FTD.

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).