Integrar solução redundante para firewall seguro e switch L3

Contents

Introdução

Este documento descreve uma prática recomendada para conexões redundantes entre Cisco Catalyst Switches e Cisco Secure Firewalls em alta disponibilidade.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças de firewall (FTD) segura
- Centro de gerenciamento seguro de firewall (FMC)
- Cisco IOS® XE
- Sistema de switching virtual (VSS)
- Alta disponibilidade (HA)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Firewall Threat Defense versão 7.2.5.1
- Secure Firewall Manager Center versão 7.2.5.1
- Cisco IOS XE versão 16.12.08

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

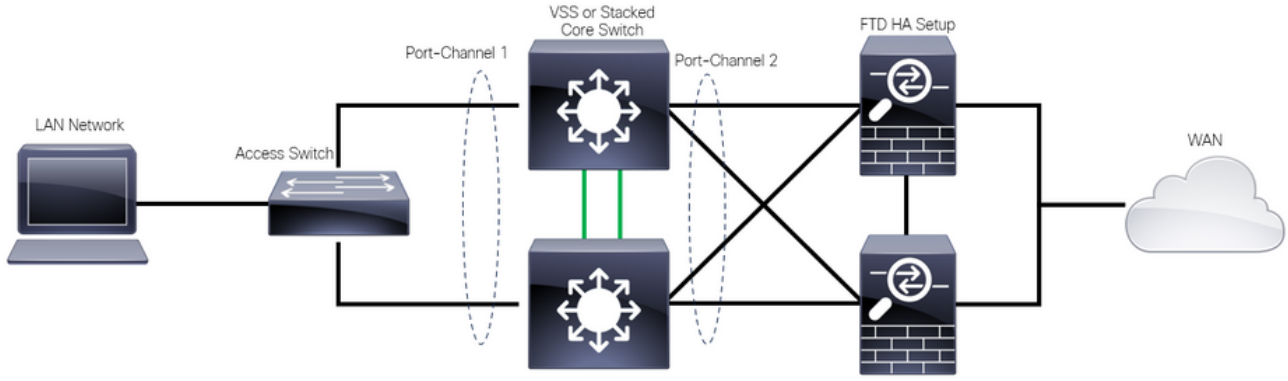
configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

Há usuários que acreditam que um único link de conexão (canal de porta) entre um Switch Catalyst lógico (VSS ou Empilhado) em direção a um par de FTDs HA é suficiente para ter uma solução totalmente redundante em caso de falha de uma unidade ou link. Essa é uma concepção equivocada comum, pois uma configuração de VSS ou de switch empilhado atua como um único dispositivo lógico. Ao mesmo tempo, um par de FTDs HA atua como dois dispositivos lógicos diferentes, sendo um como ativo e o outro como em standby.

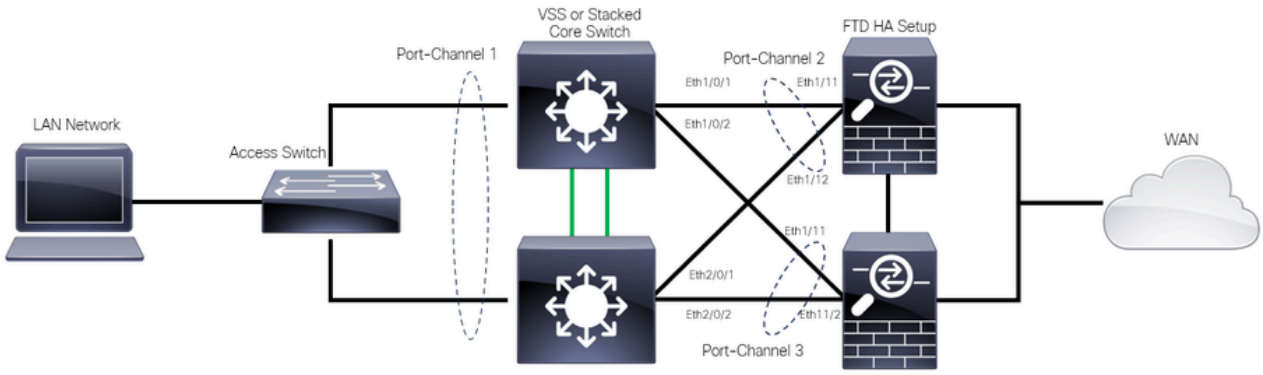
O próximo diagrama é um projeto inválido no qual um único canal de porta é configurado a partir do Switch configurado em direção ao par FTD HA:



Design inválido

A configuração anterior não é válida porque esse canal de porta atua como um único link conectado a dois dispositivos diferentes, causando colisões na rede, de modo que o Spanning Tree Protocol (SPT) bloqueia conexões de um dos FTDs.

O próximo diagrama é um projeto válido no qual dois canais de porta diferentes são configurados para cada membro do Switch VSS ou da Pilha.



Design Válido

Configurações

Configuração do Switch

Etapa 1. Configure os canais de porta com suas respectivas VLANs (Virtual Local Area Network, rede local virtual).

```
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
```

Etapa 2. Configure um endereço IP de SVI (Switched Virtual Interface) para a VLAN de canal de porta.

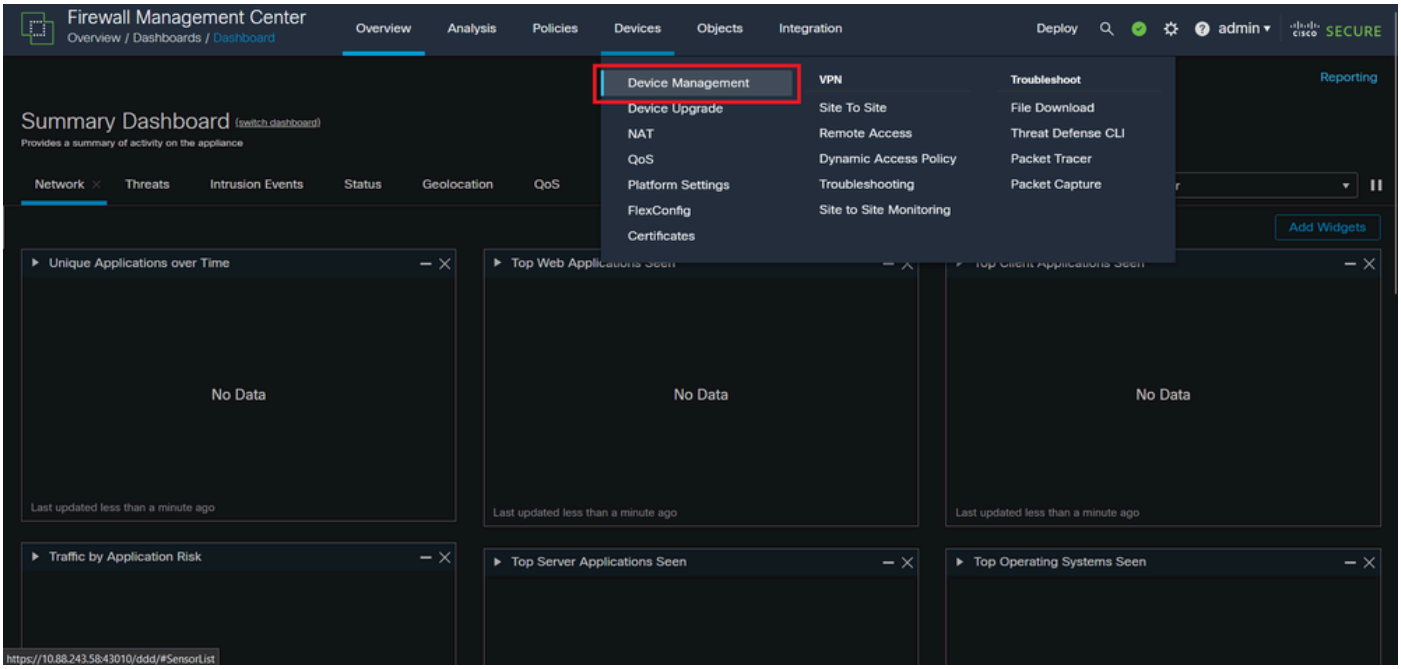
```
MXC.PS.A.06-3850-02(config-if)#exit
MXC.PS.A.06-3850-02(config)#interface VLAN 300
MXC.PS.A.06-3850-02(config-if)#ip address 10.8.4.31 255.255.255.0
MXC.PS.A.06-3850-02(config-if)#no shutdown
```

Configuração HA de FTD

Etapa 1. Faça login na GUI do FMC.

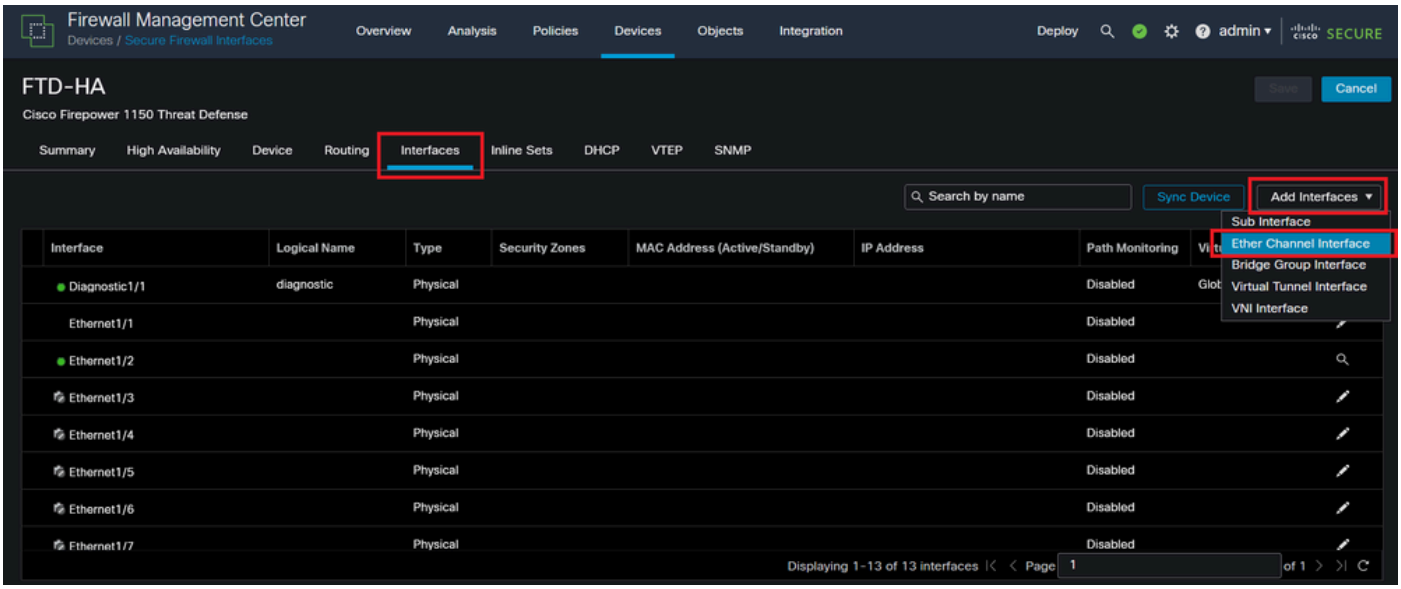
Logon no FMC

Etapa 2. Navegue até Devices > Device Management.



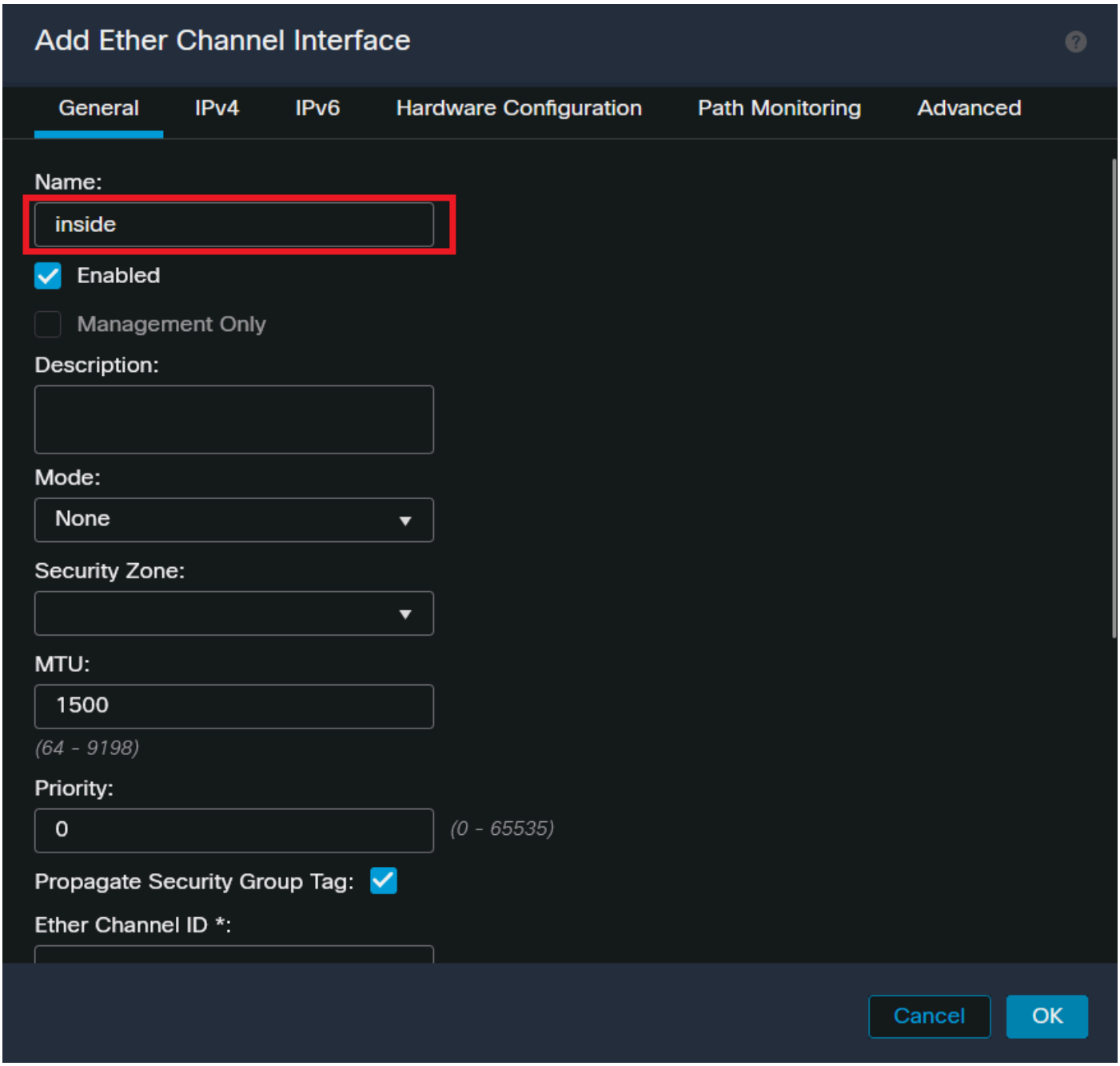
Gerenciamento de dispositivos

Etapa 3. Edite o dispositivo HA desejado e navegue até Interfaces > Add Interfaces > Ether Channel Interface.

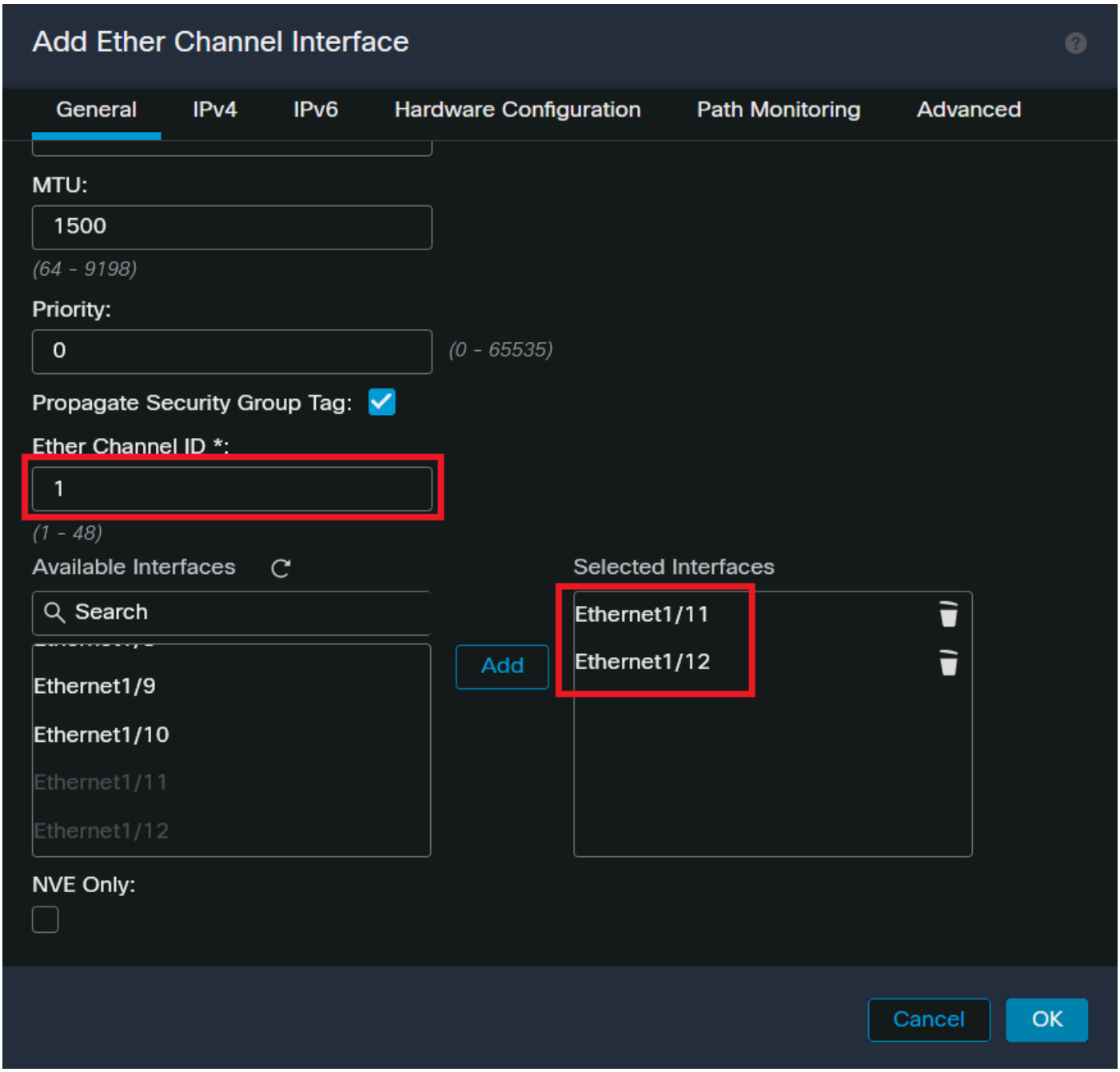


Criação de Ether-Channel

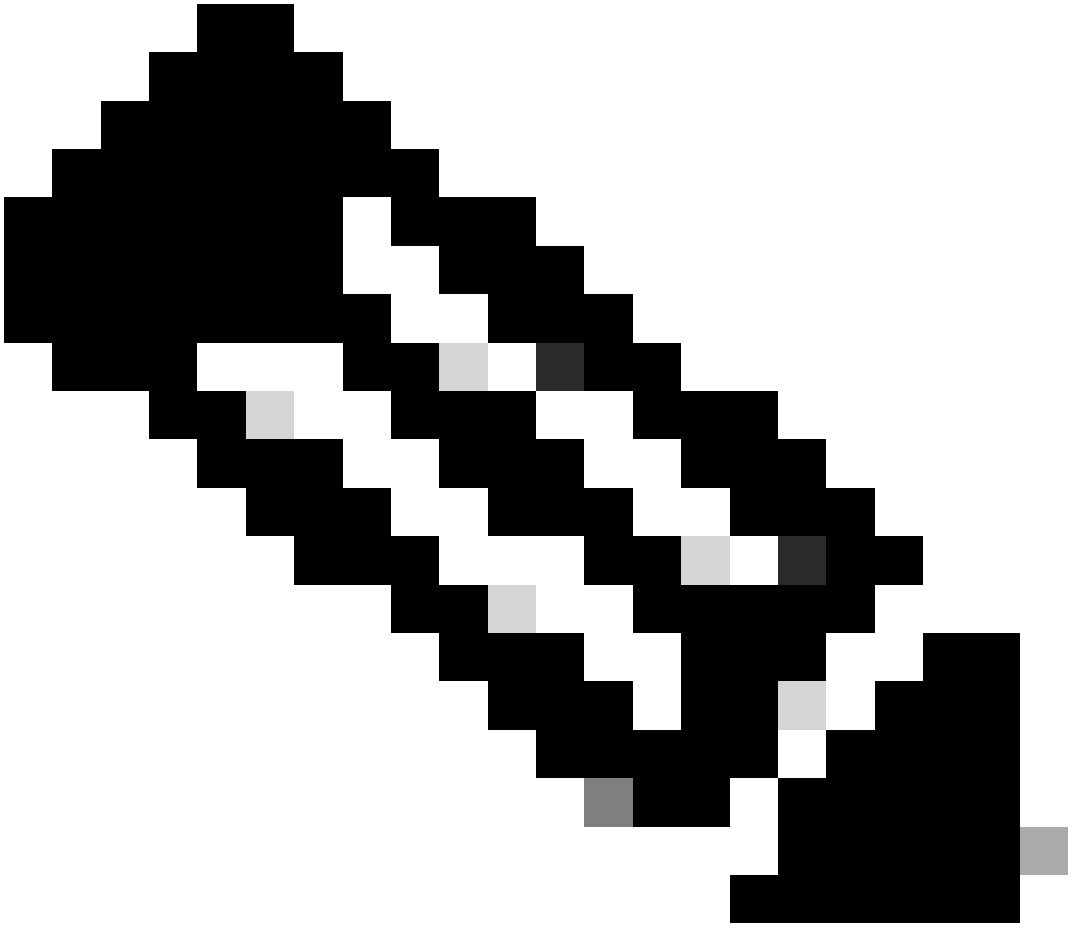
Etapa 4. Adicione um nome de interface, ID do Canal Ether e as interfaces do membro.



Nome do Ether-Channel

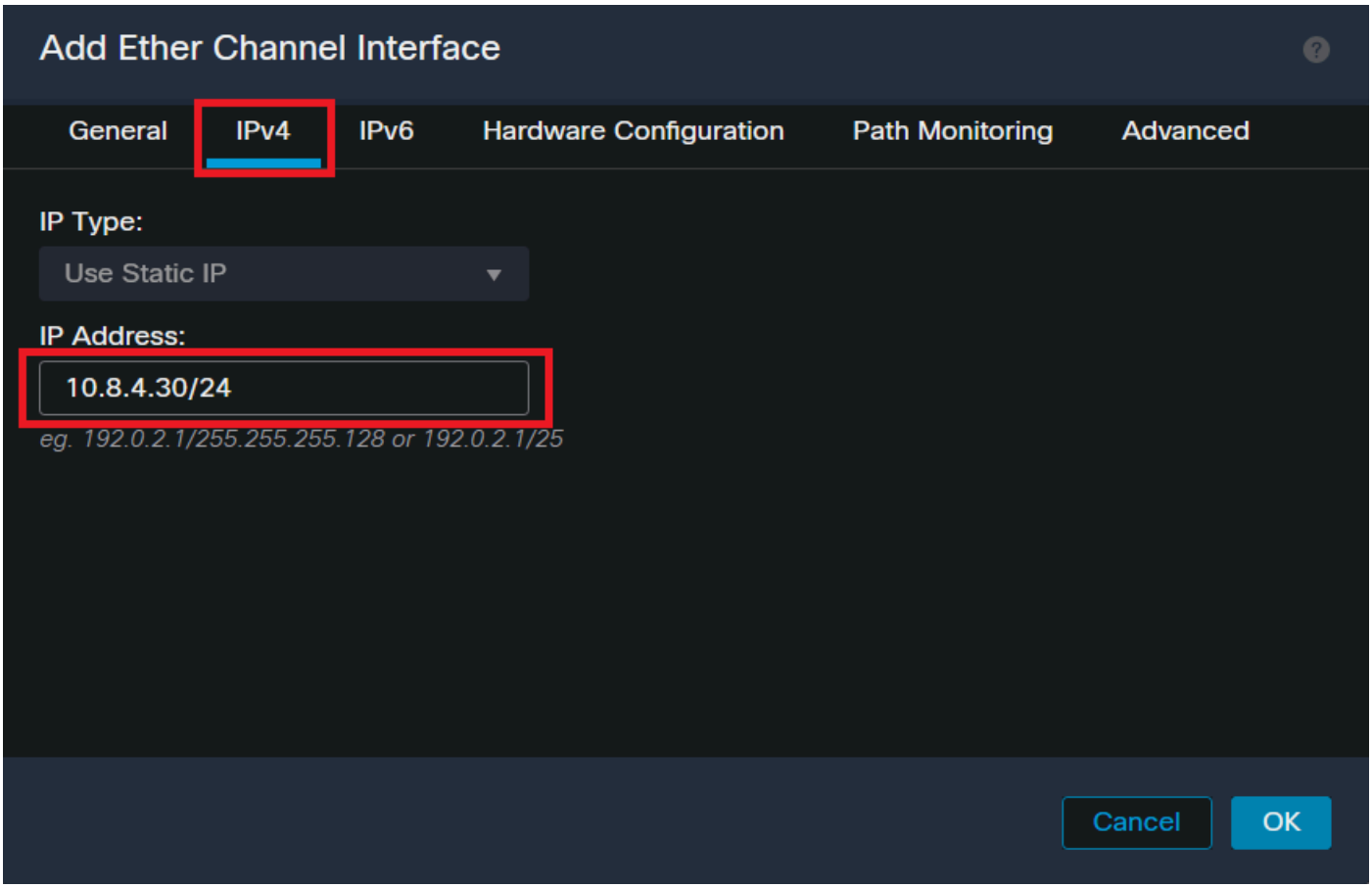


ID e membros do Ether-Channel



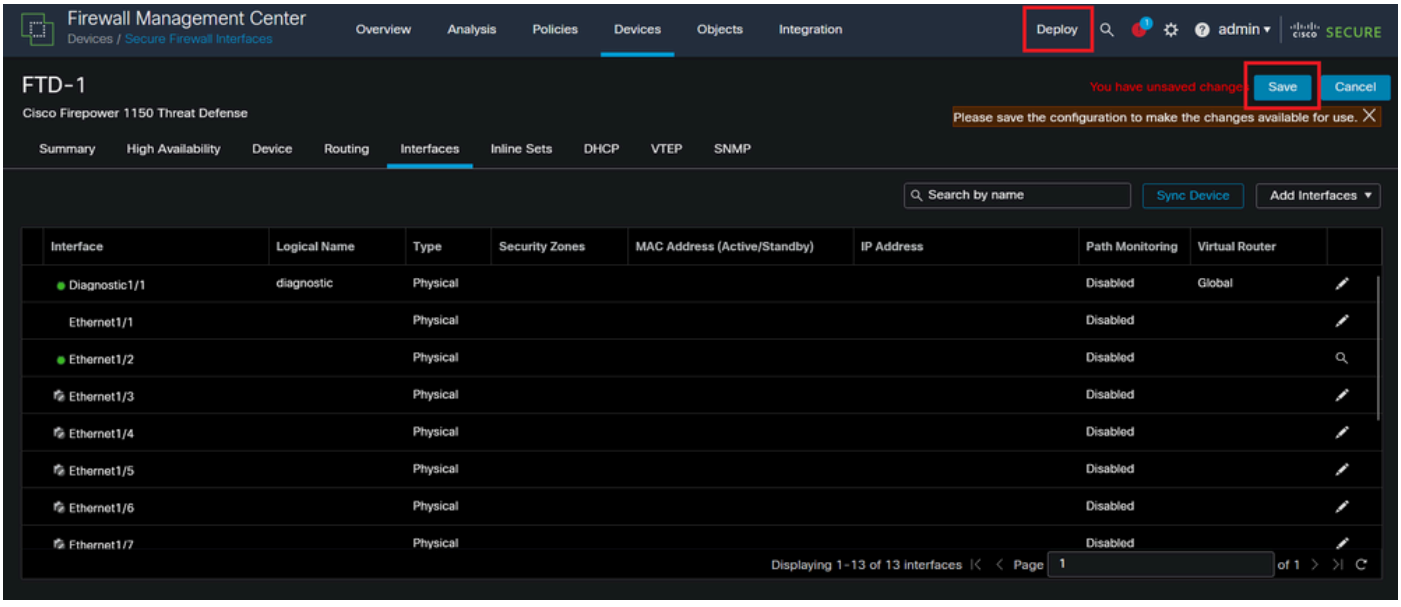
Observação: o ID do Ether Channel no FTD não precisa corresponder ao ID do Port-Channel no Switch.

Etapa 5. Navegue até a guia IPv4 e adicione um endereço IP na mesma sub-rede que a VLAN 300 para o Switch.



Endereço IP do Ether-Channel

Etapa 6. Salve as alterações e Implante.



Salvar e implantar

Verificar

Etapa 1. Certifique-se de que o Status das interfaces VLAN e port-channel esteja ativo da perspectiva do 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
```

Etapa 2. Verifique se port-channel Status está ativado em ambas as unidades de FTD acessando a interface de linha de comando do 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***
```

Etapa 3. Verifique a acessibilidade entre o Switch SVI e o endereço IP do canal de porta 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.