集成安全防火墙和L3交换机的冗余解决方案

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 配置
  - 交换机配置
  - FTD HA配置

验证

简介

本文档介绍Cisco Catalyst交换机和Cisco安全防火墙之间高可用性冗余连接的最佳实践。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全防火墙威胁防御(FTD)
- 安全防火墙管理中心(FMC)
- 思科IOS® XE
- 虚拟交换系统(VSS)
- 高可用性(HA)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙威胁防御7.2.5.1版
- 安全防火墙管理器中心版本7.2.5.1
- 思科IOS XE版本16.12.08

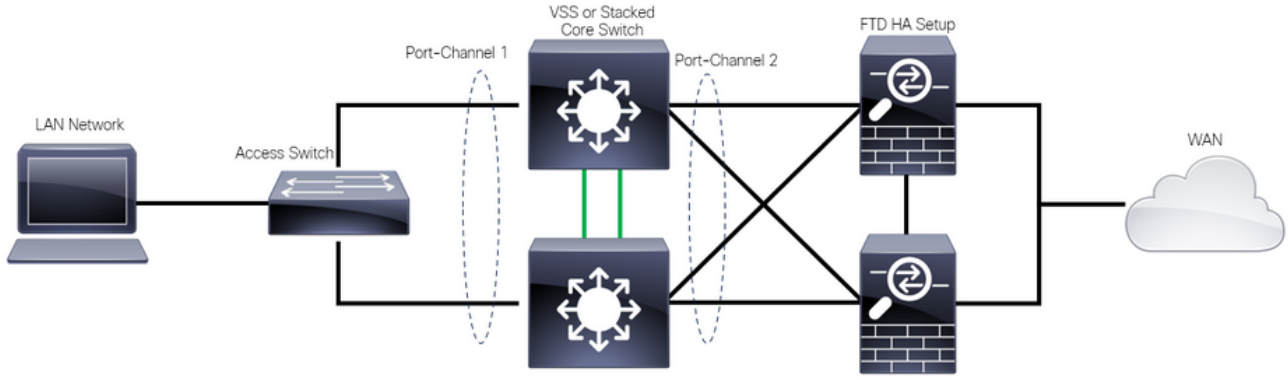
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

有些用户认为，一个逻辑Catalyst交换机（VSS或堆叠）之间指向一对高可用性FTD的单个连接链路（端口通道）足以在一个设备或链路发生故障时提供完整的冗余解决方案。这是一个常见的误解，因为VSS或堆叠交换机设置用作单个逻辑设备。同时，一对HA FTD充当两个不同的逻辑设备，其中一个作为主用，另一个作为备用。

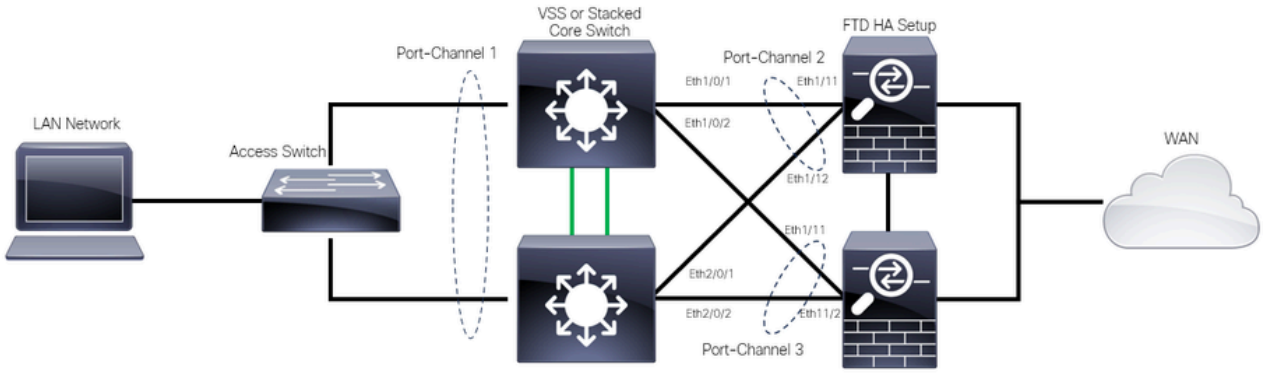
下图是一个无效设计，其中从设置的交换机到FTD HA对配置了一个端口通道：



无效设计

之前的配置无效，因为此端口通道充当连接到两个不同设备的单个链路，从而导致网络冲突，因此生成树协议(SPT)会阻止来自其中一个FTD的连接。

下图是一个有效的设计，其中为交换机VSS或堆栈的每个成员配置两个不同的端口通道。



有效设计

配置

交换机配置

步骤1:使用各自的虚拟局域网(VLAN)配置端口通道。

```
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
```

第二步：为端口通道VLAN配置交换虚拟接口(SVI) IP地址。

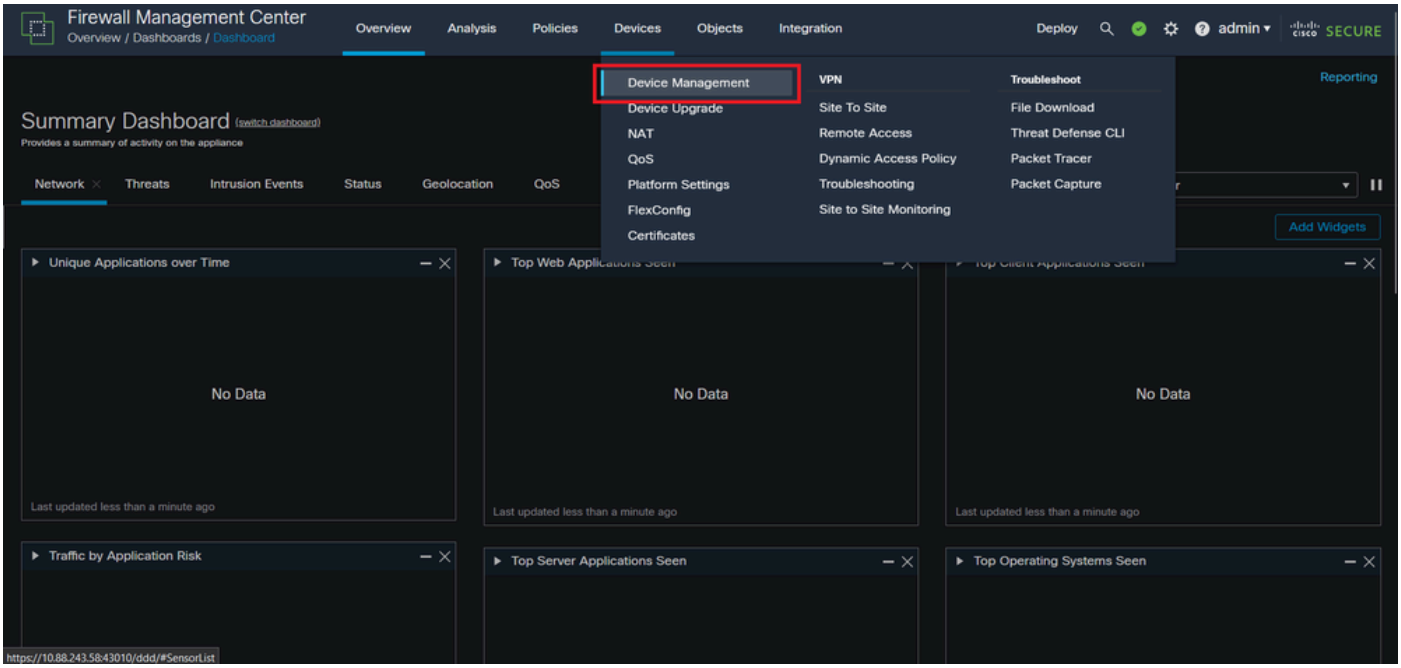
```
MXC.PS.A.06-3850-02(config-if)#exit
MXC.PS.A.06-3850-02(config)#interface VLAN 300
MXC.PS.A.06-3850-02(config-if)#ip address 10.8.4.31 255.255.255.0
MXC.PS.A.06-3850-02(config-if)#no shutdown
```

FTD HA配置

步骤1:登录FMC GUI。

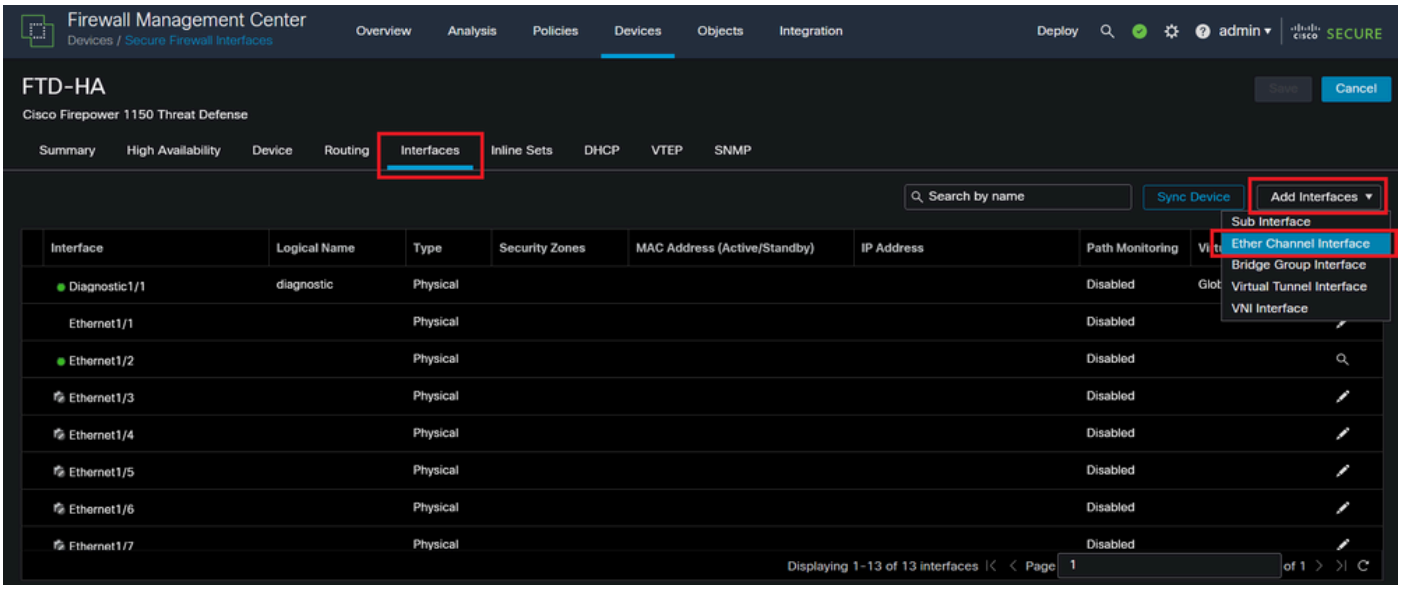
FMC登录

第二步：导航到设备>设备管理。



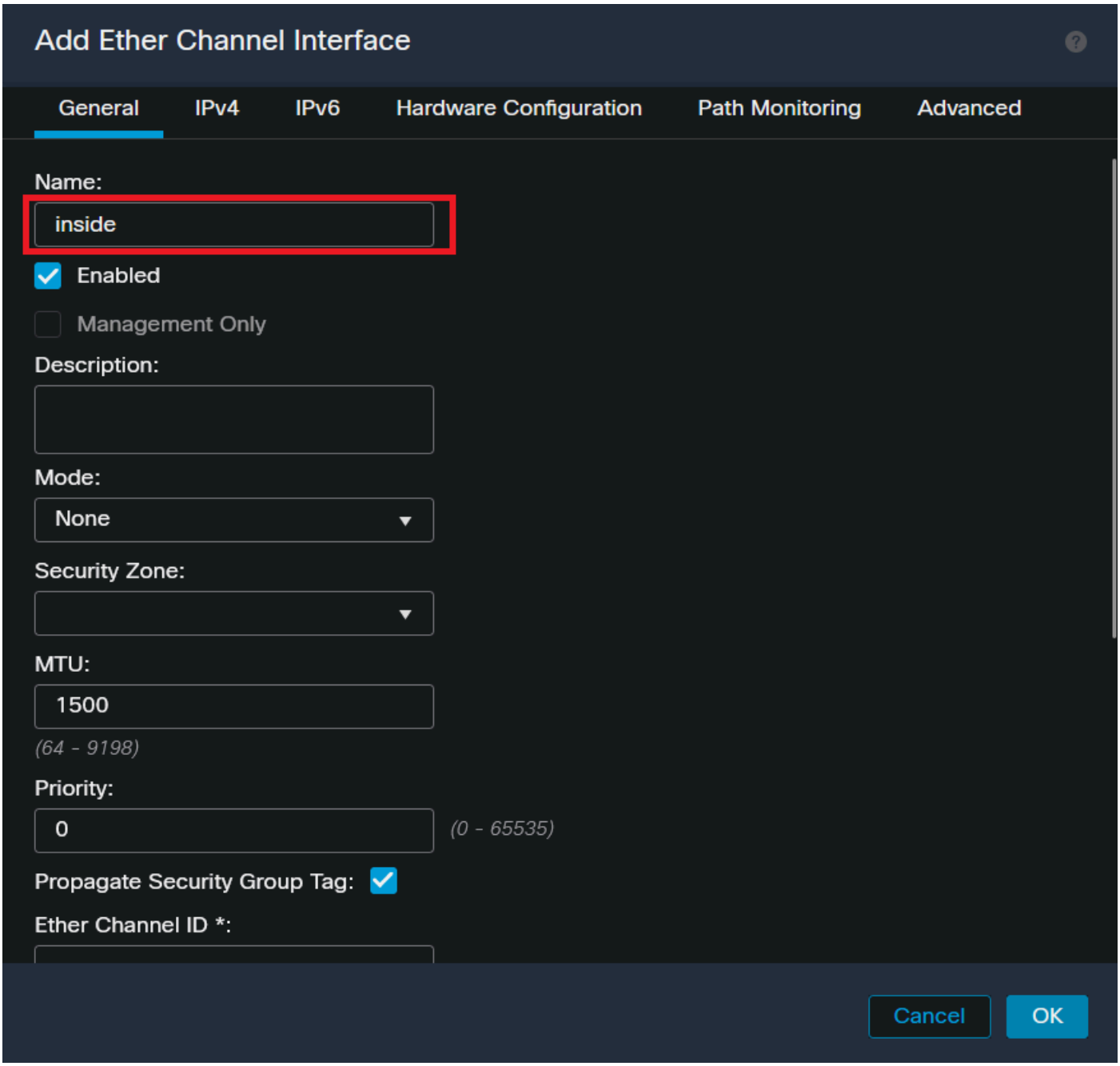
设备管理

第三步：编辑所需的高可用性设备，并导航到Interfaces > Add Interfaces > Ether Channel Interface。

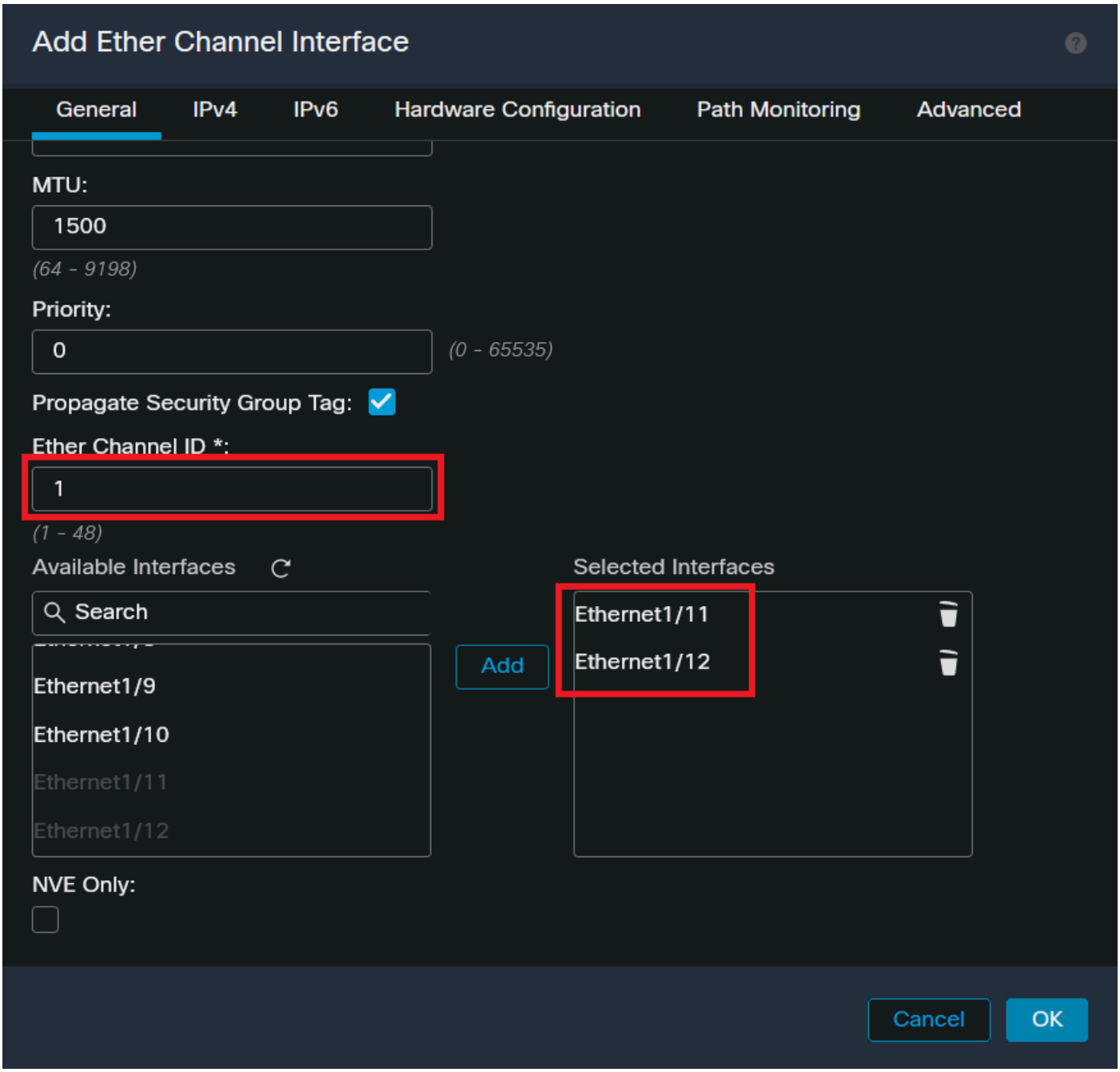


Ether-Channel创建

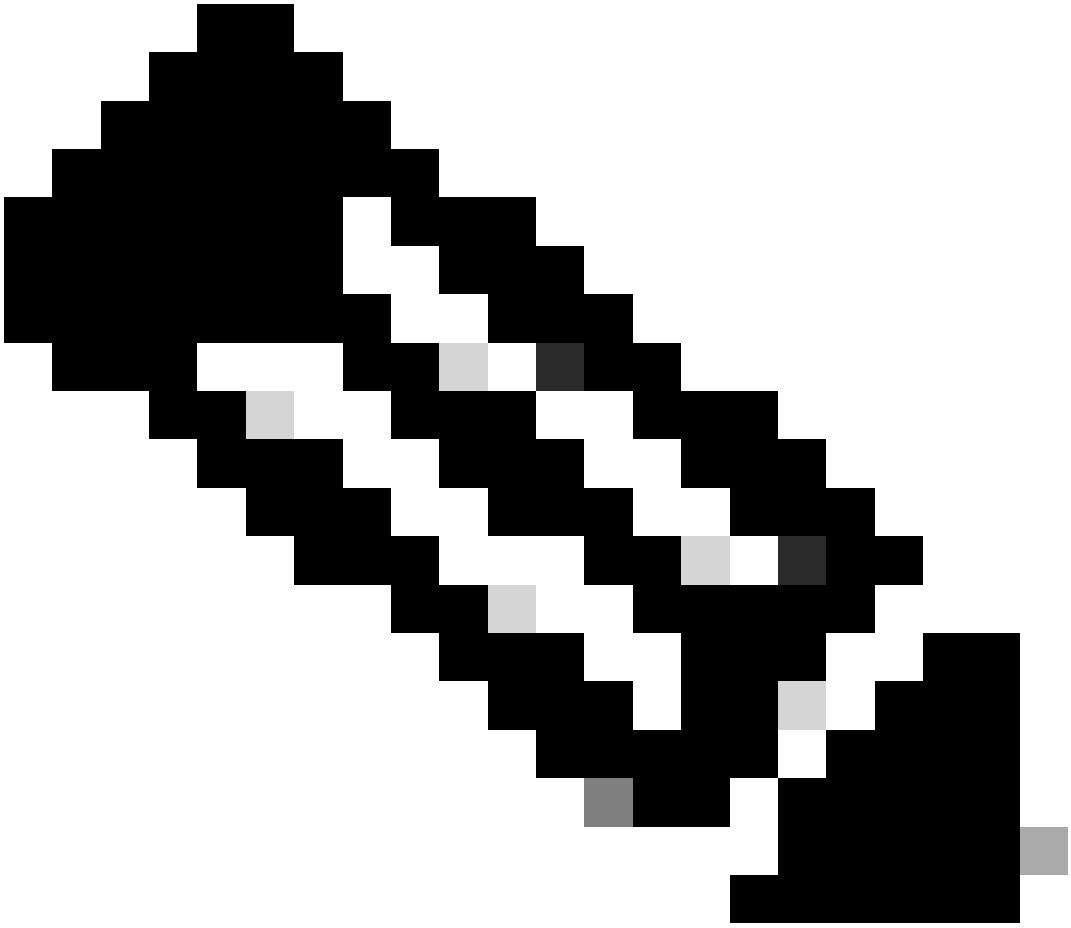
第四步：添加接口名称、以太网通道ID和成员接口。



Ether-Channel名称

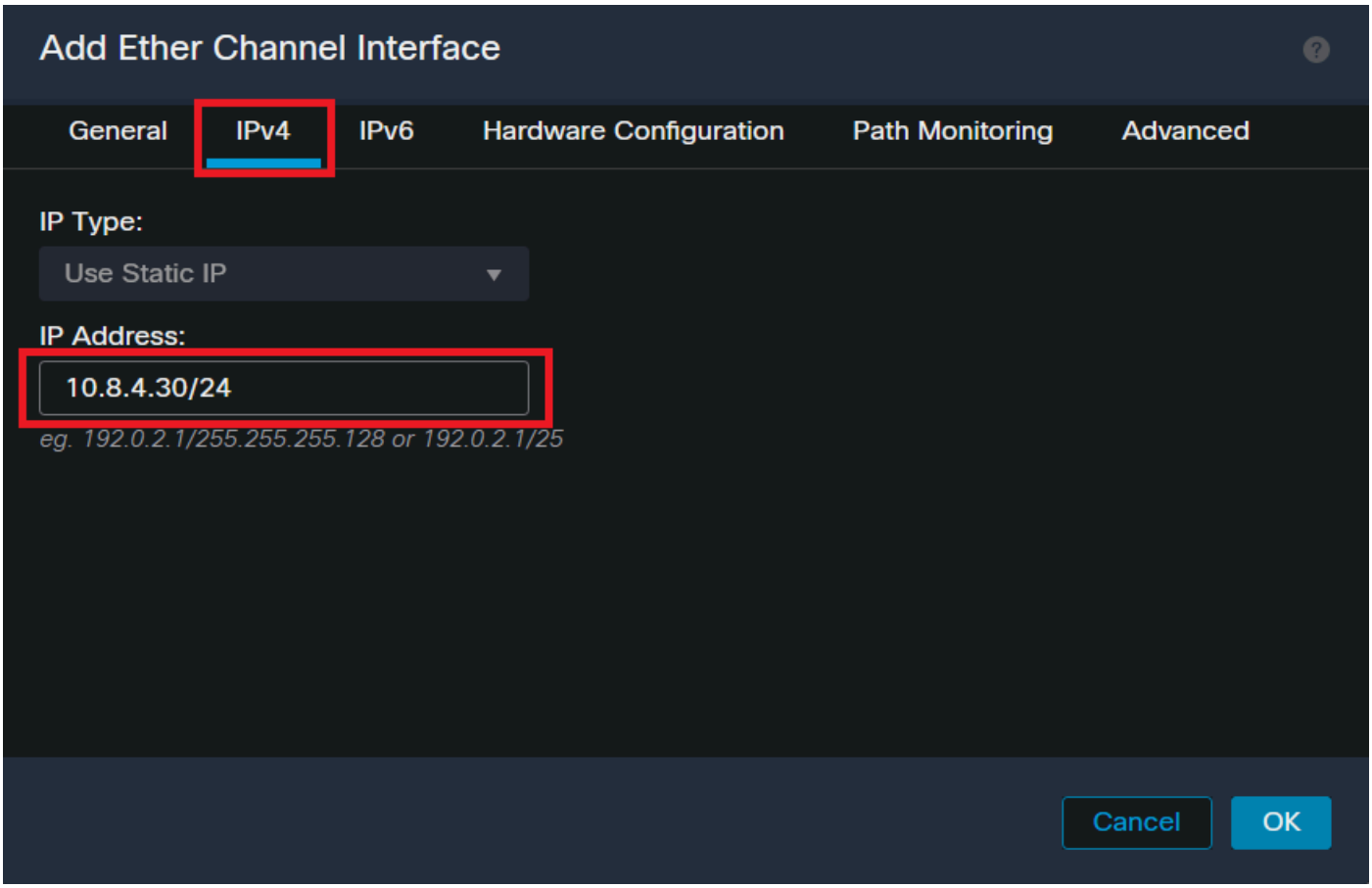


Ether-Channel ID和成员



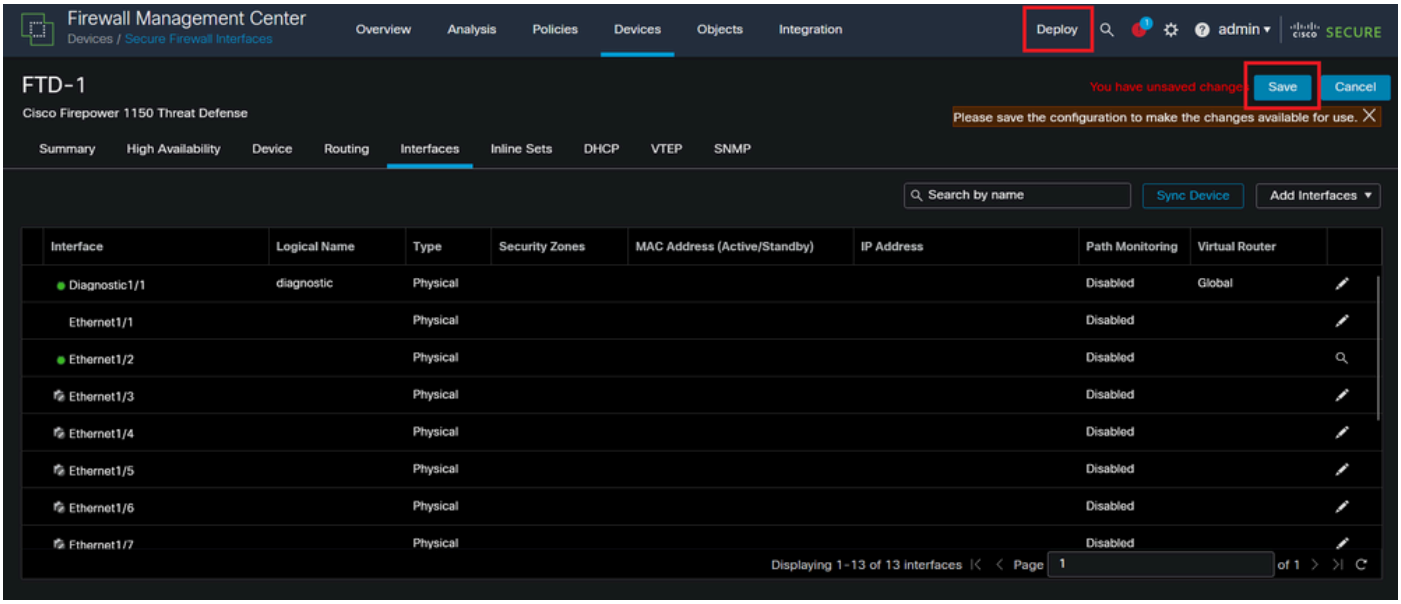
注意：FTD上的EtherChannel ID不需要与交换机上的Port-Channel ID匹配。

第五步：导航到IPv4选项卡，然后在与交换机的VLAN 300相同的子网中添加IP地址。



Ether-Channel IP地址

第六步：保存更改并部署。



保存并部署

验证

步骤1:确保VLAN和端口信道接口的状态从交换机的角度为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
```

第二步：通过访问设备命令行界面，检查两个FTD单元上的端口信道状态是否均为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***
```

第三步：检查交换机SVI和FTD端口通道IP地址之间的可接通性。

```
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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。