Integrate Redundant Solution for Secure Firewall and L3 Switch

Contents

Introduction

This document describes a best practice for redundant connections between Cisco Catalyst Switches and Cisco Secure Firewalls on High Availability.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)
- Cisco IOS® XE
- Virtual Switching System (VSS)
- High Availability (HA)

Components Used

The information in this document is based on these software and hardware versions:

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

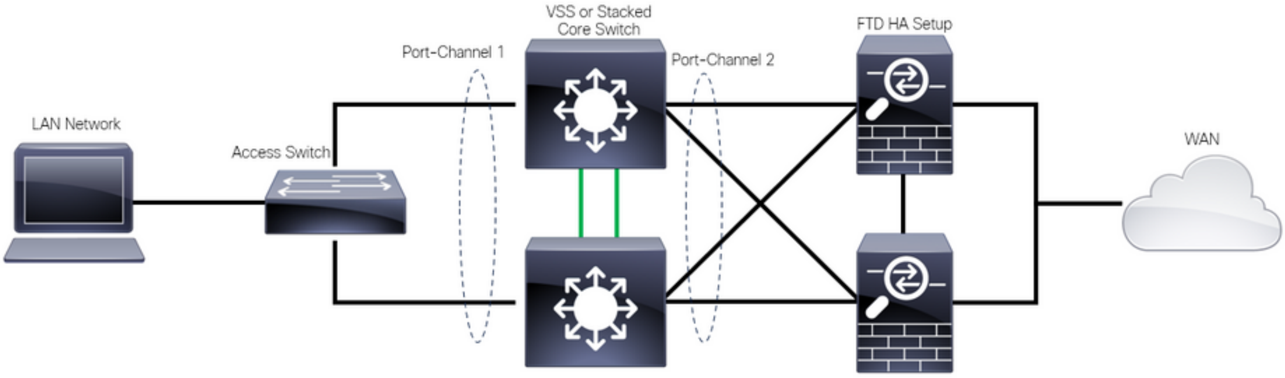
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram

There are users that believe a single connection link (port channel) between one logical Catalyst Switch (VSS or Stacked) towards a pair of HA FTDs suffices to have a full redundant solution in case one unit or link fails. This is a common misconception because a VSS or Stacked Switch setup acts as a single logical device. While at the same time, a pair of HA FTDs act as two different logical devices with one as Active and the other as Standby.

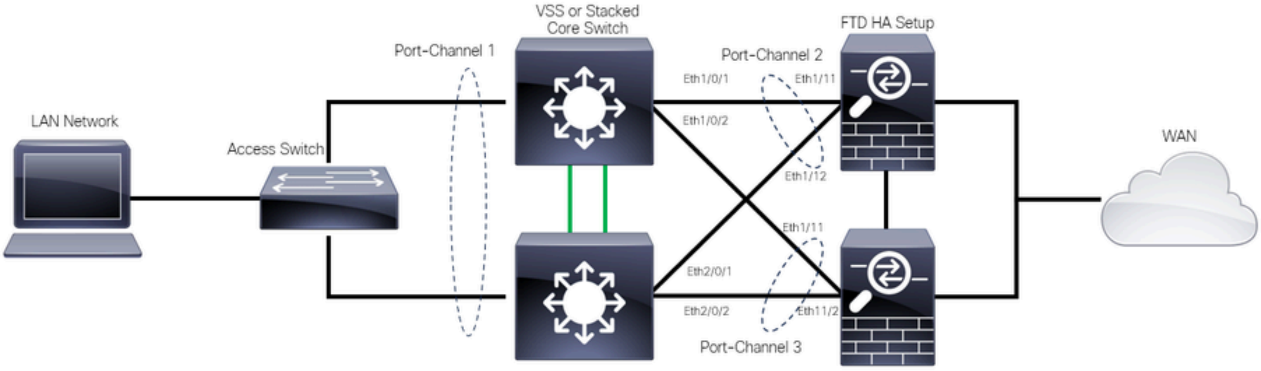
The next diagram is an invalid design in which a single Port-Channel is configured from the Switch set up towards the FTD HA pair:



Invalid Design

The previous configuration is not valid because this port-channel acts as a single link connected to two different devices, causing network collisions, so the Spanning Tree Protocol (SPT) blocks connections from one of the FTDs.

The next diagram is a valid design in which two different Port-Channels are configured for each member of the Switch VSS or Stack.



Valid Design

Configurations

Switch Configuration

Step 1. Configure port-channels with their respective Virtual Local Area Network (VLAN).

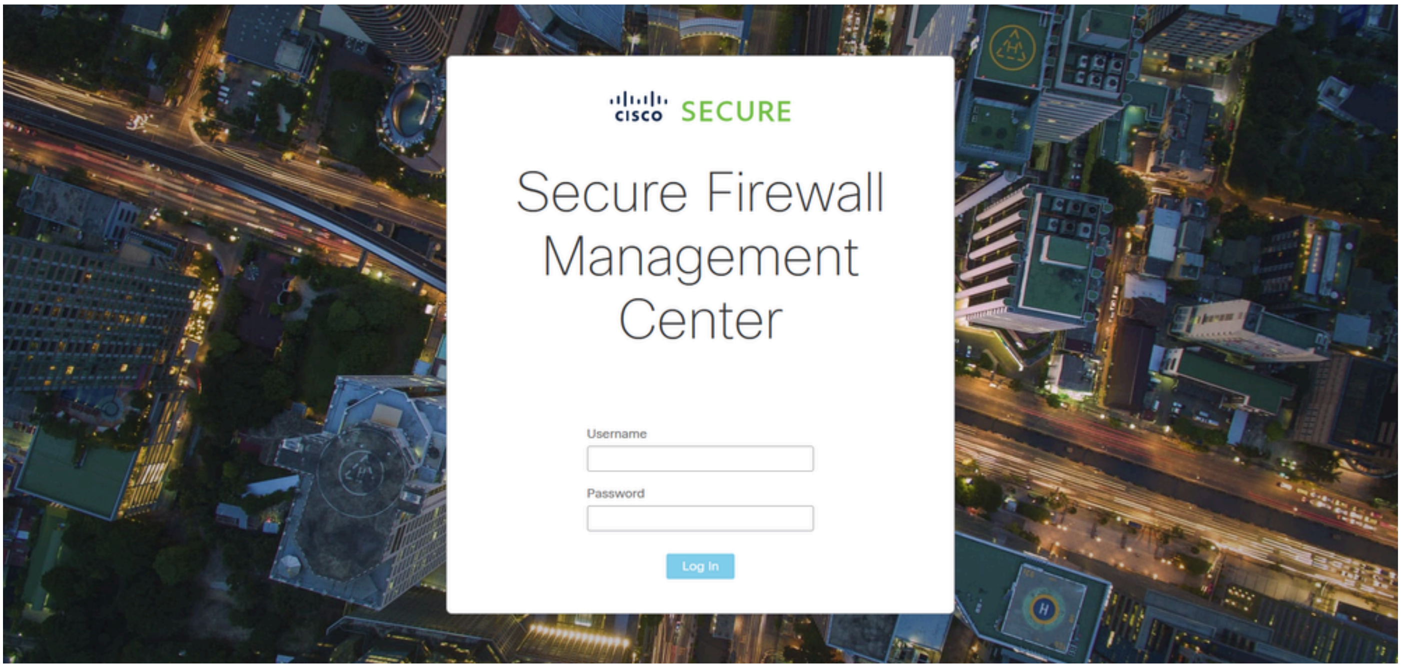
```
MXC.PS.A.06-3850-02#configure terminal
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
% Access VLAN does not exist. Creating vlan 300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

Step 2. Configure a Switched Virtual Interface (SVI) IP address for the Port-Channel VLAN.

```
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
```

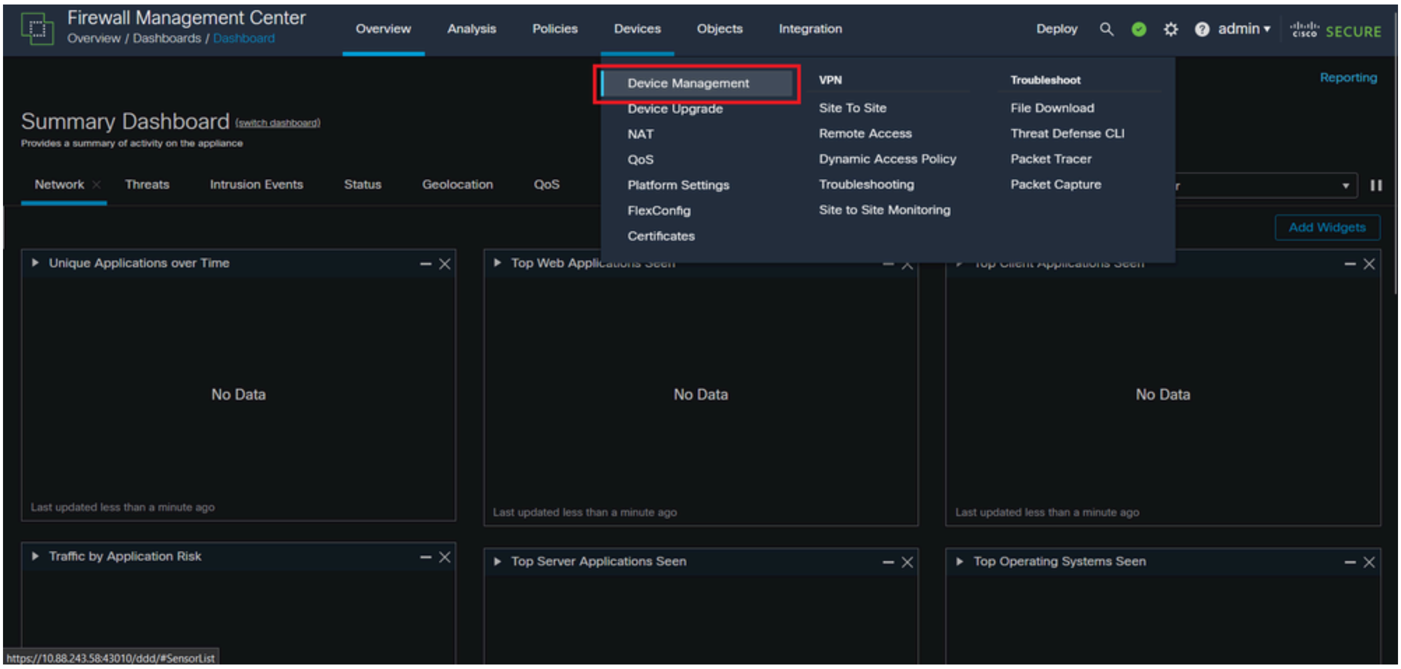
FTD HA Configuration

Step 1. Log into the FMC GUI.



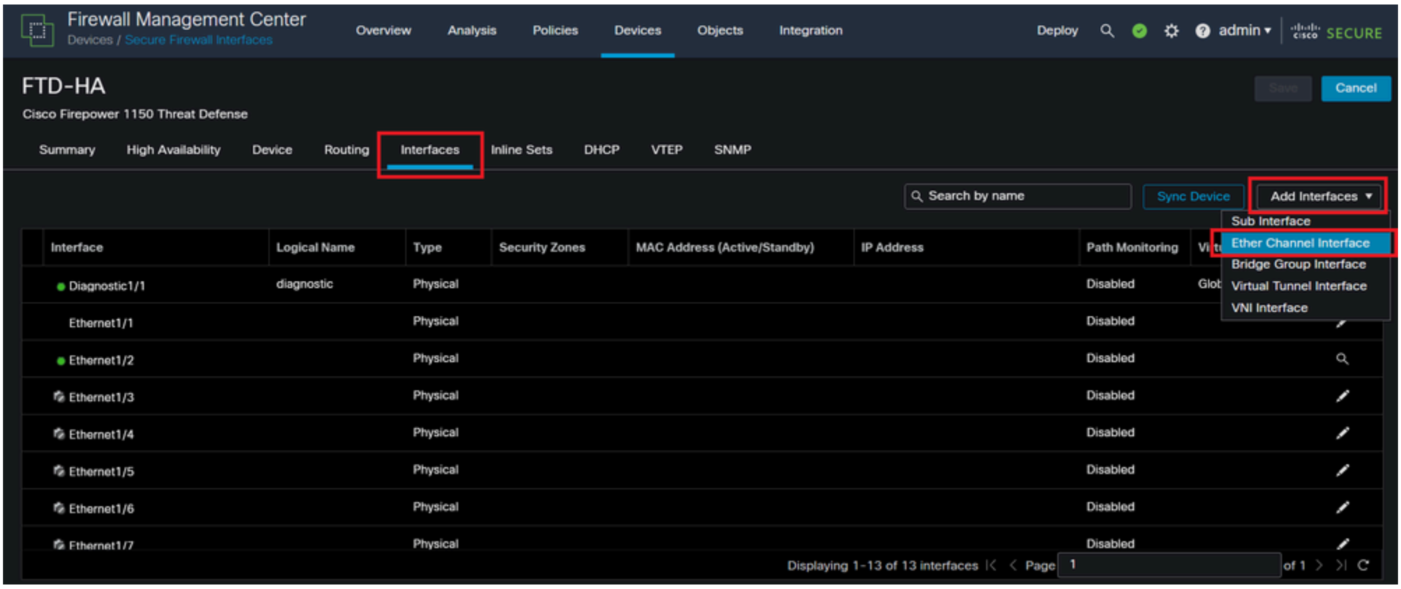
FMC Log In

Step 2. Navigate to **Devices > Device Management**.


Firewall Management Center
Overview / Dashboards / Dashboard
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
cisco SECURE
Device Management
Device Upgrade
NAT
QoS
Platform Settings
FlexConfig
Certificates
VPN
Site To Site
Remote Access
Dynamic Access Policy
Troubleshooting
Site to Site Monitoring
Troubleshoot
File Download
Threat Defense CLI
Packet Tracer
Packet Capture
Reporting
Summary Dashboard (switch dashboard)
Provides a summary of activity on the appliance
Network
Threats
Intrusion Events
Status
Geolocation
QoS
Add Widgets
Unique Applications over Time
No Data
Last updated less than a minute ago
Top Web Applications Seen
No Data
Last updated less than a minute ago
Top Client Applications Seen
No Data
Last updated less than a minute ago
Traffic by Application Risk
Top Server Applications Seen
Top Operating Systems Seen
https://10.88.243.58:43010/ddd/#SensorList

Device Management

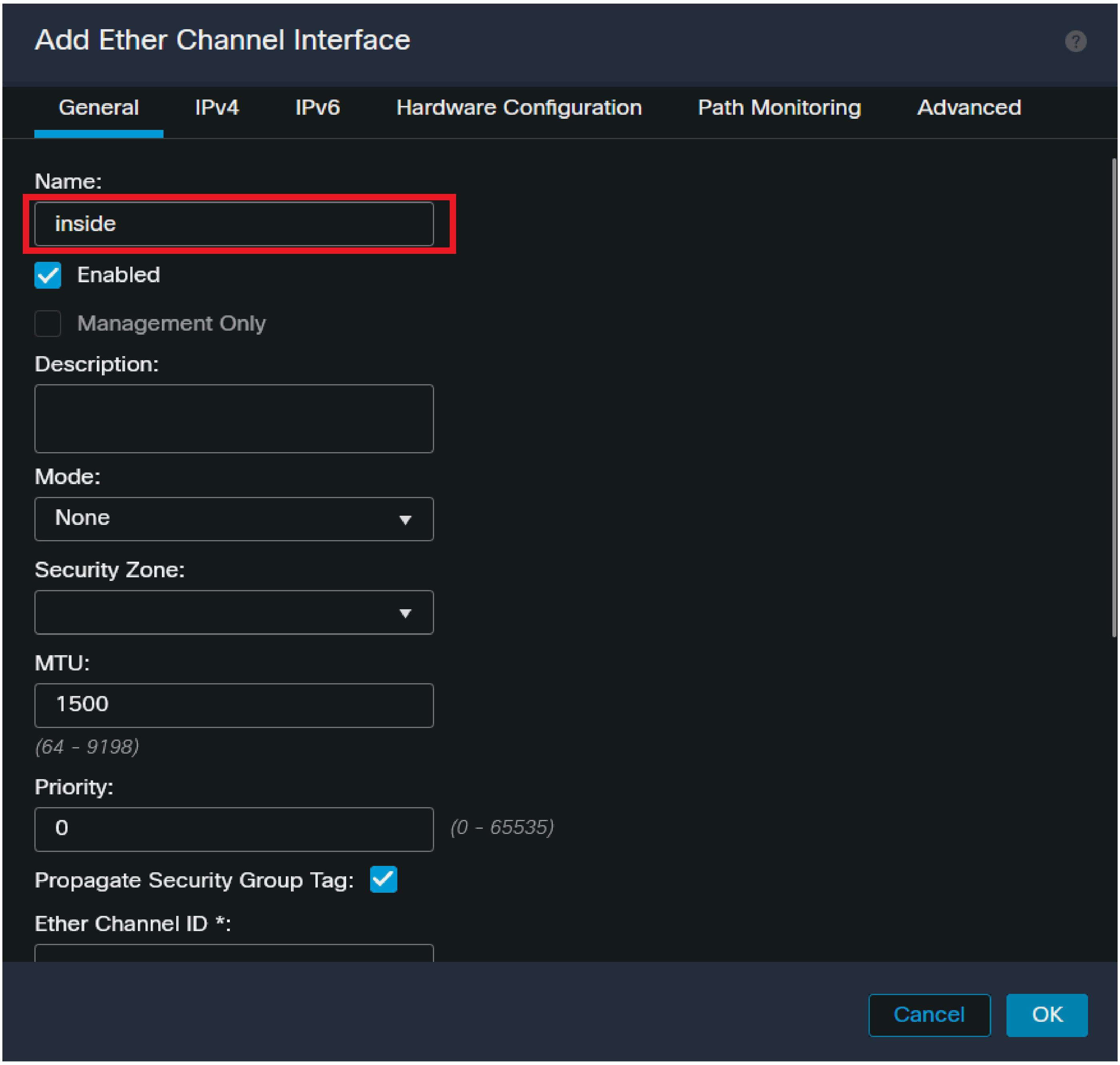
Step 3. Edit the desired HA device and navigate to **Interfaces > Add Interfaces > Ether Channel Interface**.



Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Vi
Diagnostic1/1	diagnostic	Physical				Disabled	Glob
Ethernet1/1		Physical				Disabled	
Ethernet1/2		Physical				Disabled	
Ethernet1/3		Physical				Disabled	
Ethernet1/4		Physical				Disabled	
Ethernet1/5		Physical				Disabled	
Ethernet1/6		Physical				Disabled	
Ethernet1/7		Physical				Disabled	

Ether-Channel Creation

Step 4. Add an interface name, Ether Channel ID, and the member interfaces.



Add Ether Channel Interface

Name: inside

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone:

MTU: 1500

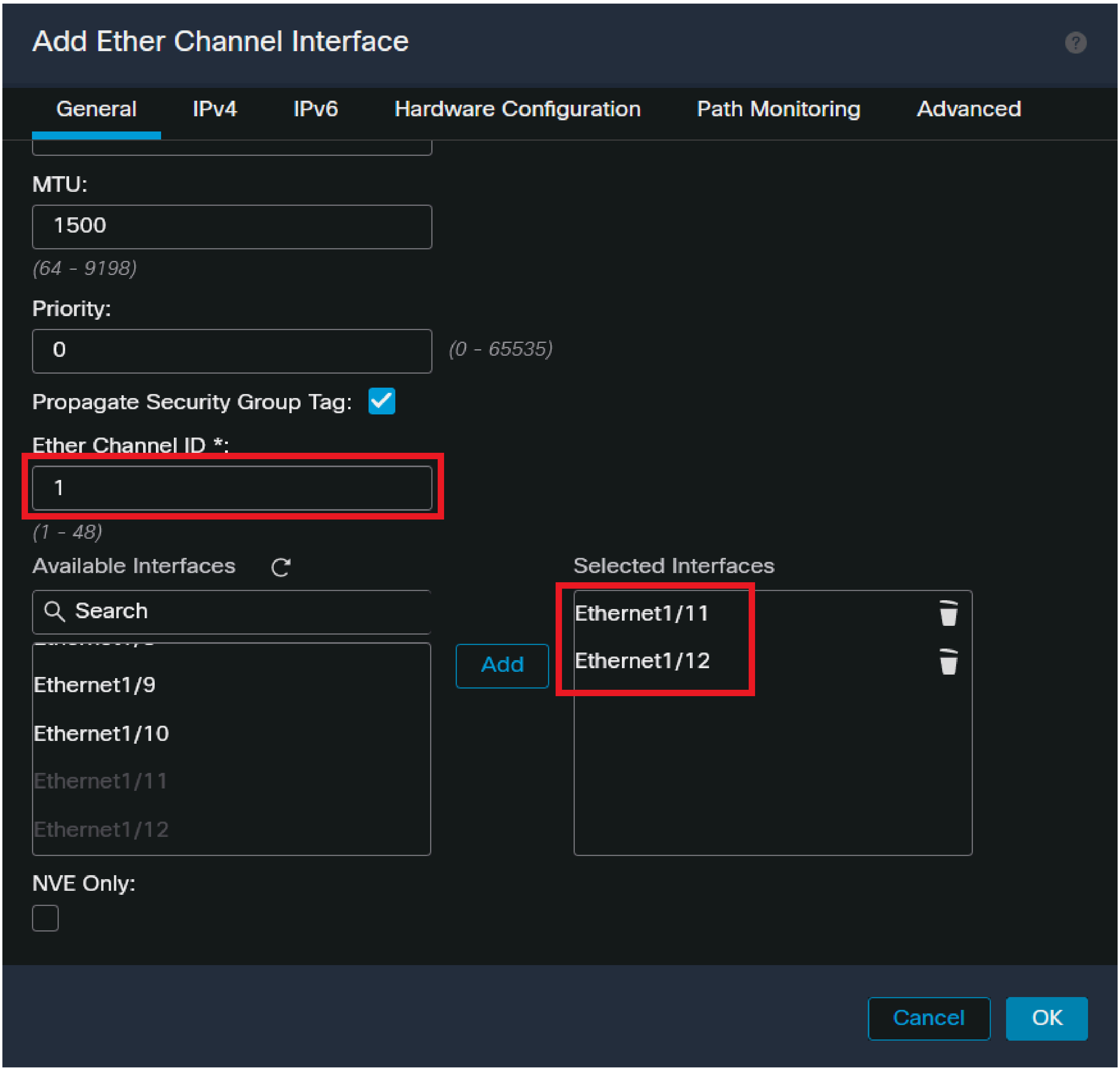
(64 - 9198)

Priority: 0 (0 - 65535)

Propagate Security Group Tag: ☑

Ether Channel ID *:

Ether-Channel Name



MTU: 1500 (64 - 9198)

Priority: 0 (0 - 65535)

Propagate Security Group Tag: ☑

Ether Channel ID *: 1 (1 - 48)

Available Interfaces

Search

Ethernet1/9

Ethernet1/10

Ethernet1/11

Ethernet1/12

Selected Interfaces

Ethernet1/11

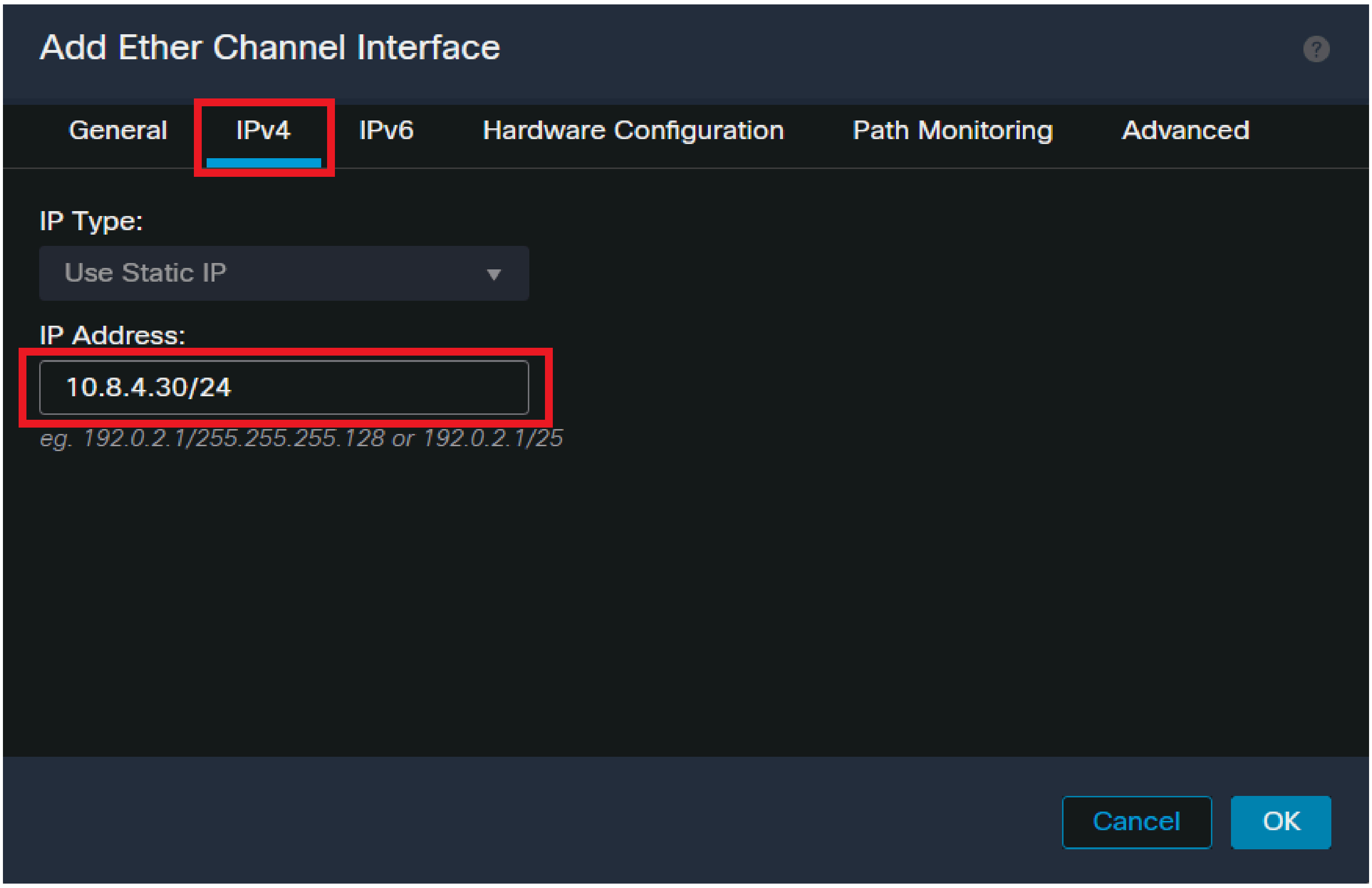
Ethernet1/12

NVE Only: □

Ether-Channel ID and Members

Note: The Ether Channel ID on the FTD does not need to match the Port-Channel ID on the Switch.

Step 5. Navigate to the **IPv4** tab and add an IP address on the same subnet as the VLAN 300 for the Switch.



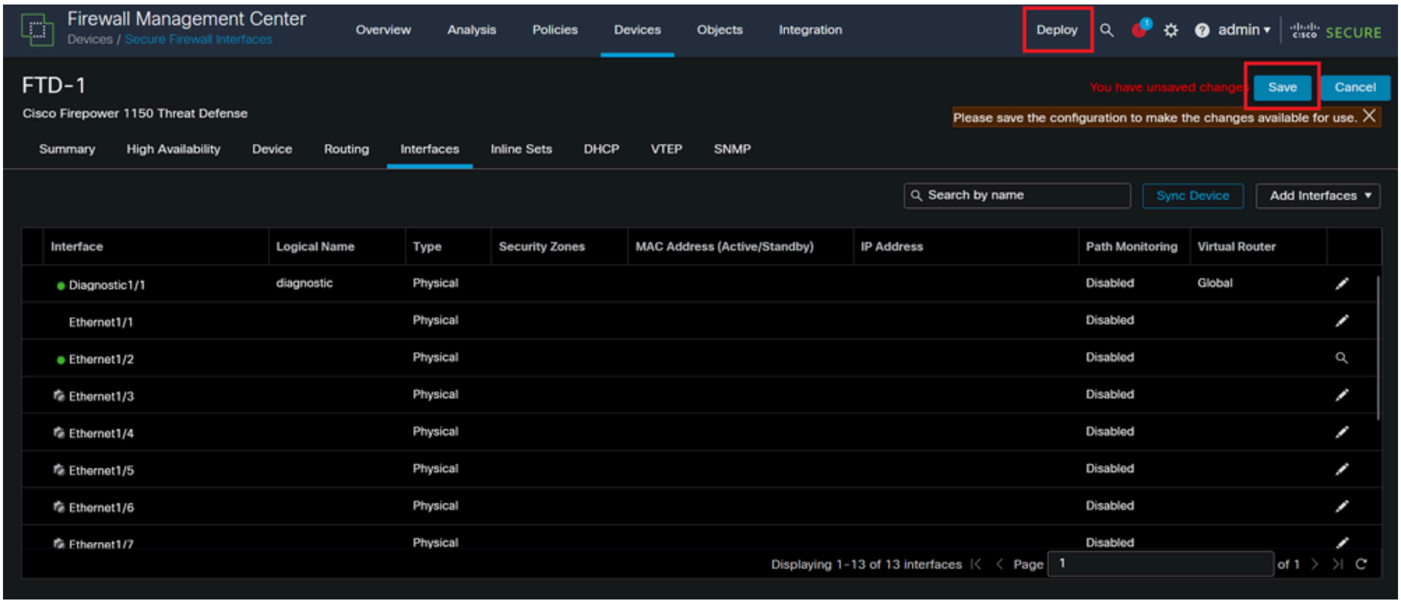
IP Type: Use Static IP

IP Address: 10.8.4.30/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Ether-Channel IP Address

Step 6. Save the changes and Deploy.



FTD-1

Cisco Firepower 1150 Threat Defense

You have unsaved changes

Please save the configuration to make the changes available for use.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
● Diagnostic1/1	diagnostic	Physical				Disabled	Global
Ethernet1/1		Physical				Disabled	
● Ethernet1/2		Physical				Disabled	
Ethernet1/3		Physical				Disabled	
Ethernet1/4		Physical				Disabled	
Ethernet1/5		Physical				Disabled	
Ethernet1/6		Physical				Disabled	
Ethernet1/7		Physical				Disabled	

Displaying 1-13 of 13 interfaces   Page 1 of 1

Save and Deploy

Verify

Step 1. Ensure the VLAN and port-channel interfaces **Status** is **up** from the Switch perspective.

```
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
```

Step 2. Check that port-channel **Status** is **up** on both FTD units by accessing the device command line interface.

```
> 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***
```

Step 3. Check reachability between the Switch SVI and the FTD Port-Channel IP address.

```
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
```