Integration einer redundanten Lösung für eine sichere Firewall und einen L3-Switch

Inhalt

Einleitung

Dieses Dokument beschreibt eine Best Practice für redundante Verbindungen zwischen Cisco Catalyst Switches und Cisco Secure Firewalls bei hoher Verfügbarkeit.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Firewall-Bedrohungsabwehr (FTD)
- Secure Firewall Management Center (FMC)
- Cisco IOS® XE
- Virtual Switching System (VSS)
- Hohe Verfügbarkeit

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

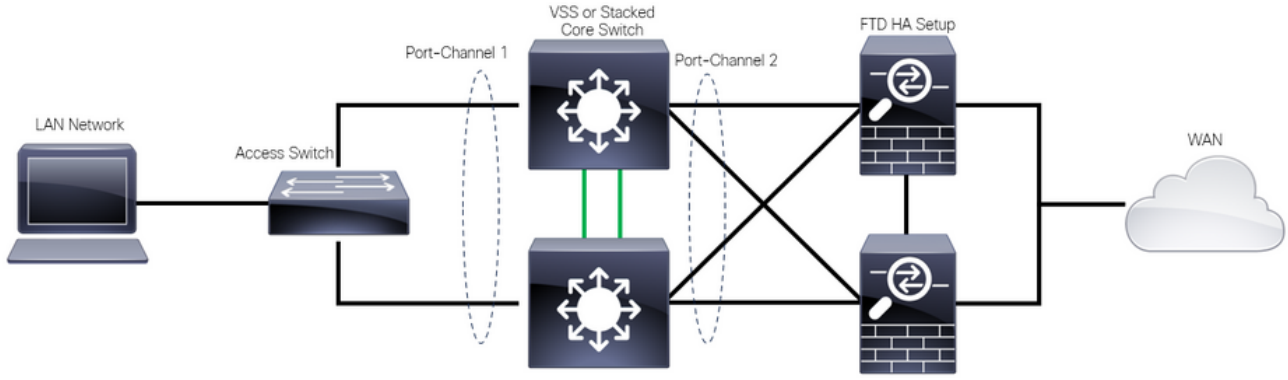
Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

Es gibt Benutzer, die der Ansicht sind, dass eine einzelne Verbindungsverbindung (Port-Channel) zwischen einem logischen Catalyst Switch (VSS oder Stacked Switch) und einem Paar hochverfügbarer FTDs ausreicht, um eine vollständig redundante Lösung bereitzustellen, falls eine Einheit oder Verbindung ausfällt. Dies ist ein weit verbreitetes Missverständnis, da eine VSS- oder Stack Switch-Konfiguration als einzelnes logisches Gerät fungiert. Gleichzeitig fungieren zwei Hochverfügbarkeits-FTDs als zwei verschiedene logische Geräte, von denen das eine als Aktiv und das andere als Standby-Geräte fungiert.

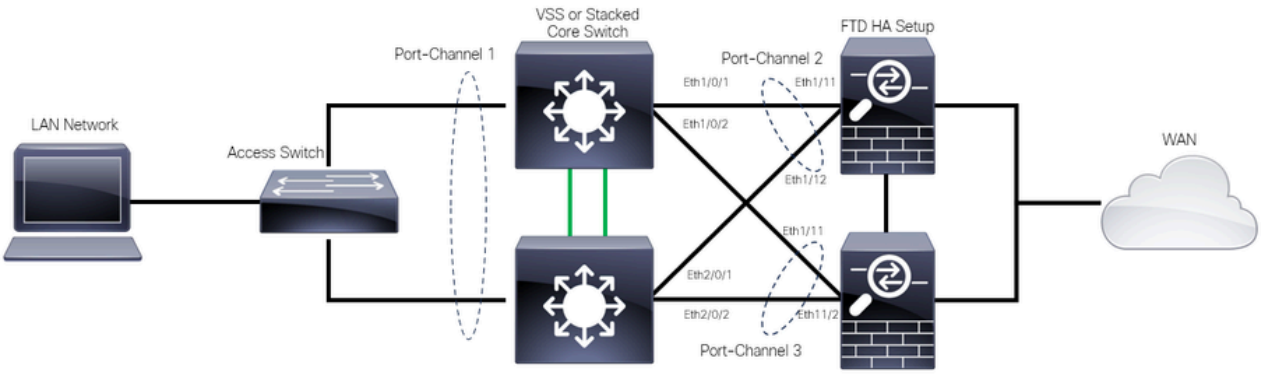
Das nächste Diagramm zeigt ein ungültiges Design, bei dem ein einzelner Port-Channel vom Switch für das Hochverfügbarkeitspaar des FTD konfiguriert wird:



Ungültiges Design

Die vorherige Konfiguration ist ungültig, da dieser Port-Channel als eine Verbindung mit zwei verschiedenen Geräten agiert und Netzwerkkollisionen verursacht. Daher blockiert das Spanning Tree Protocol (SPT) Verbindungen von einem FTD.

Das nächste Diagramm zeigt ein gültiges Design, bei dem zwei verschiedene Port-Channels für jedes Element des Switch-VSS oder -Stacks konfiguriert werden.



Konfigurationen

Switch-Konfiguration

Schritt 1: Konfigurieren Sie Port-Channels mit dem entsprechenden Virtual Local Area Network (VLAN).

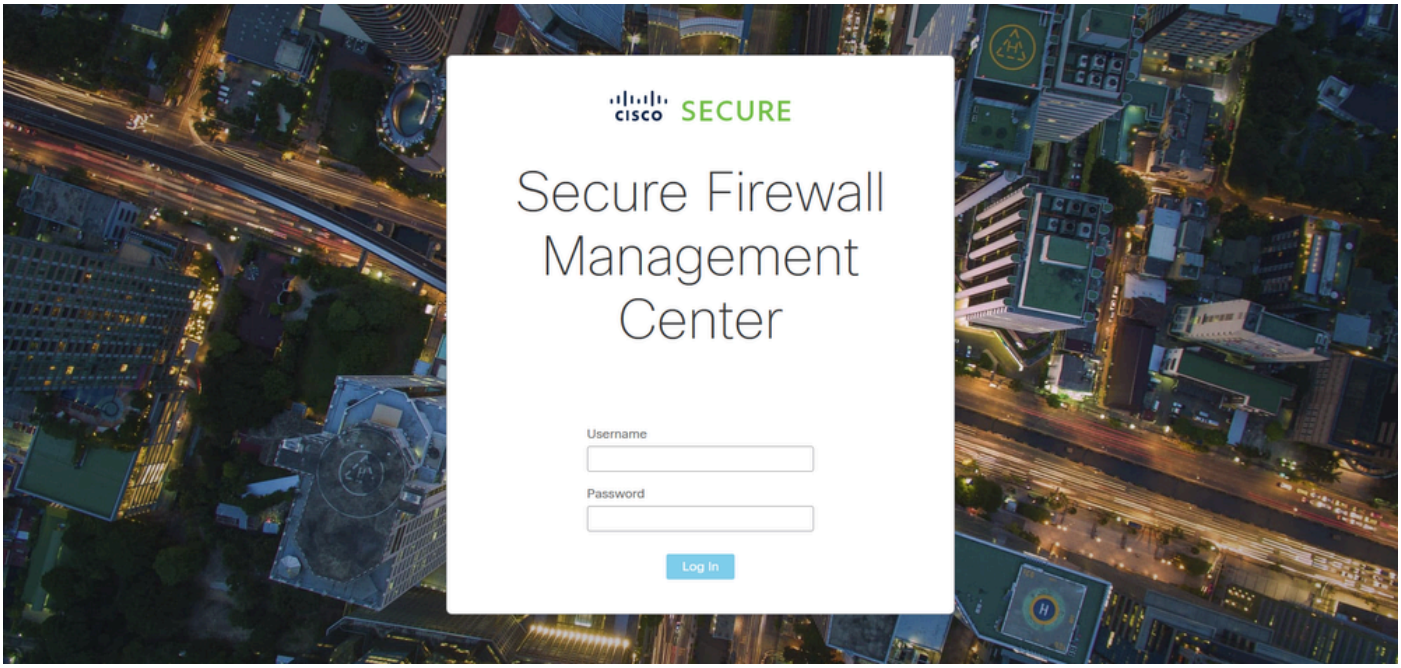
```
MXC.PS.A.06-3850-02#configure terminal
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
% Access VLAN does not exist. Creating vlan 300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

Schritt 2: Konfigurieren Sie eine SVI-IP-Adresse (Switched Virtual Interface) für das 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
```

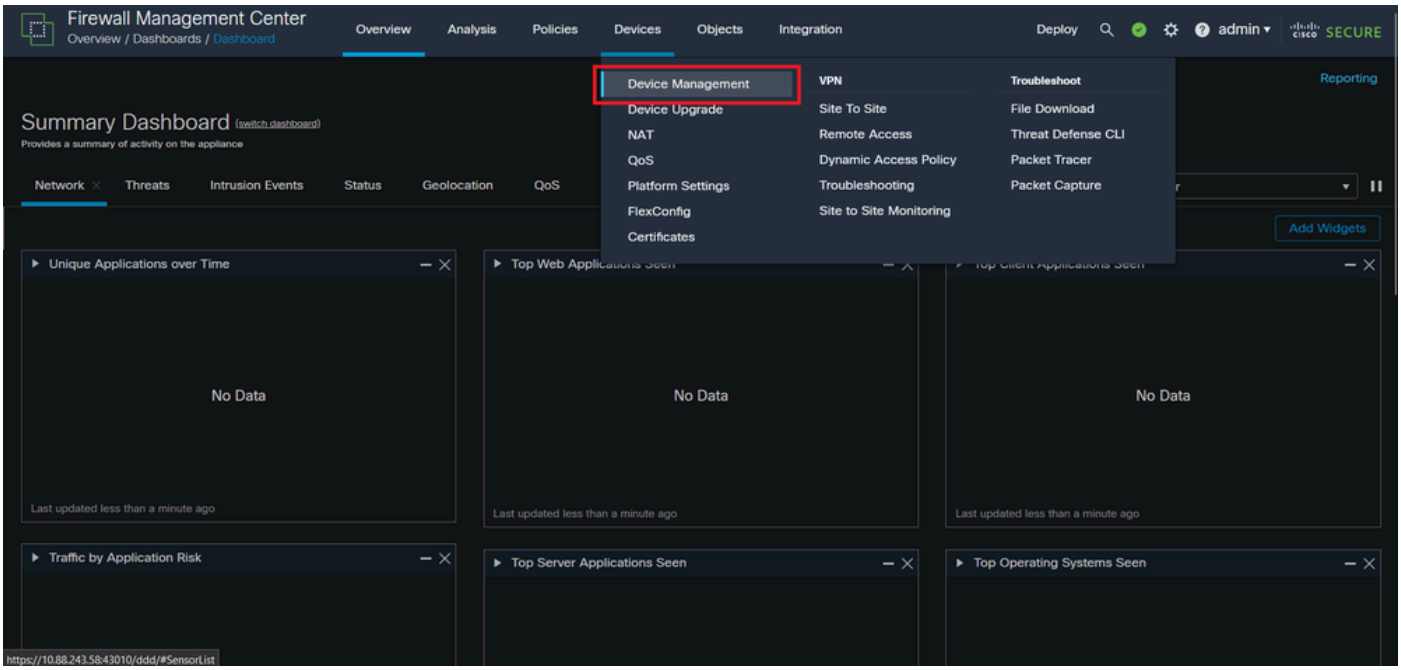
FTD HA-Konfiguration

Schritt 1: Melden Sie sich bei der FMC-GUI an.



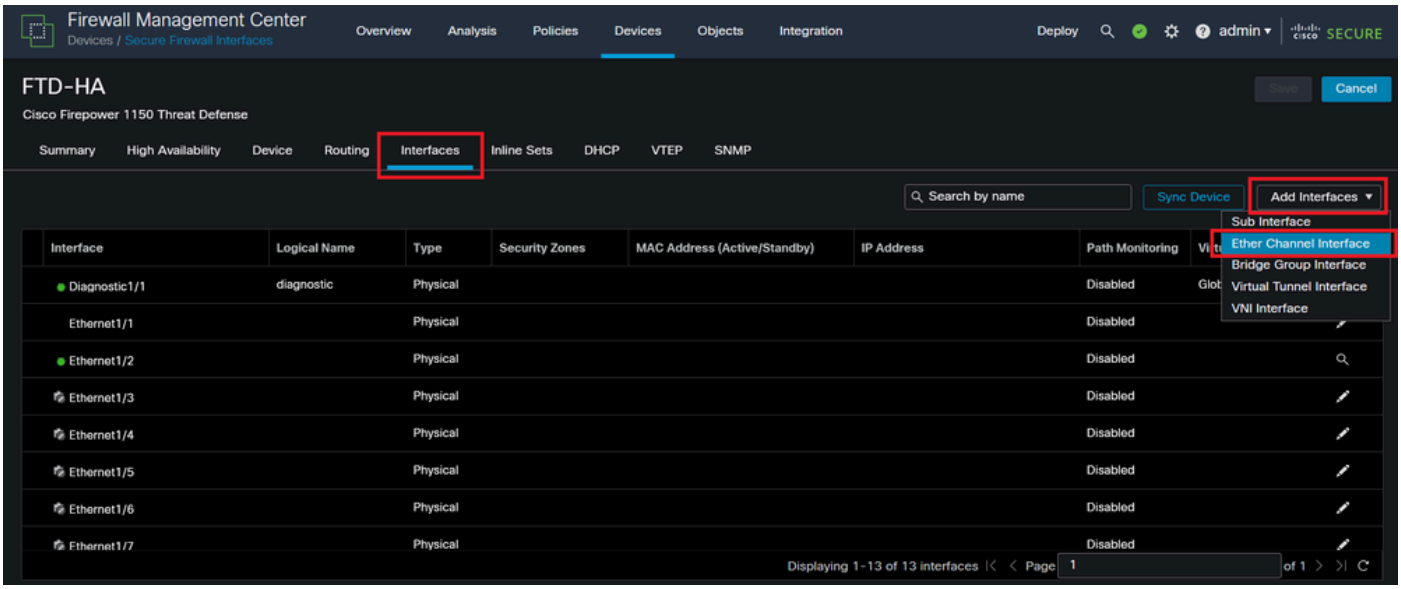
FMC-Anmeldung

Schritt 2: Navigieren Sie zu Geräte > Geräteverwaltung.



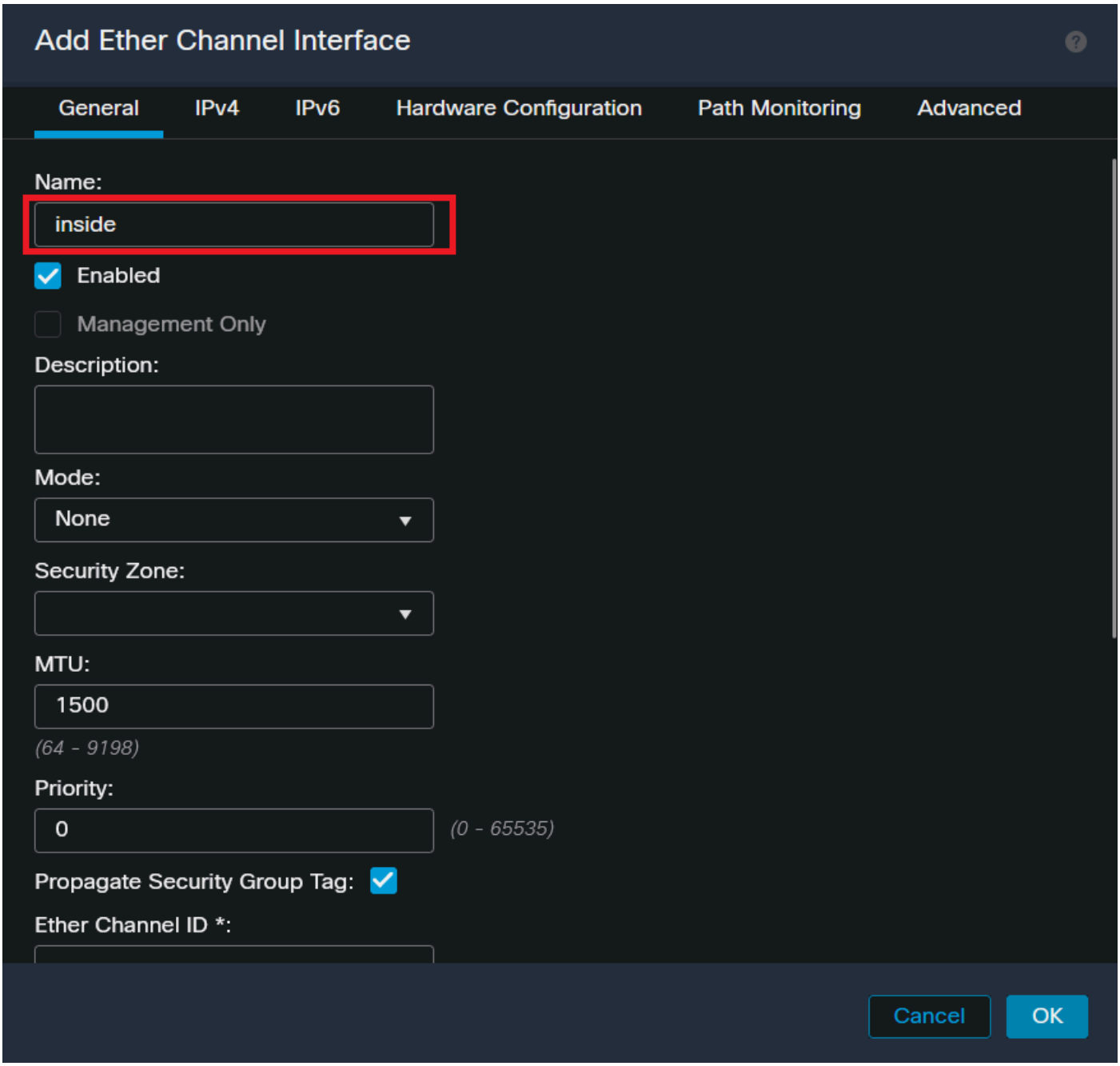
Gerätemanagement

Schritt 3: Bearbeiten Sie das gewünschte HA-Gerät, und navigieren Sie zu Interfaces > Add Interfaces > Ether Channel Interface (Schnittstellen > Schnittstellen hinzufügen > EtherChannel-Schnittstelle).

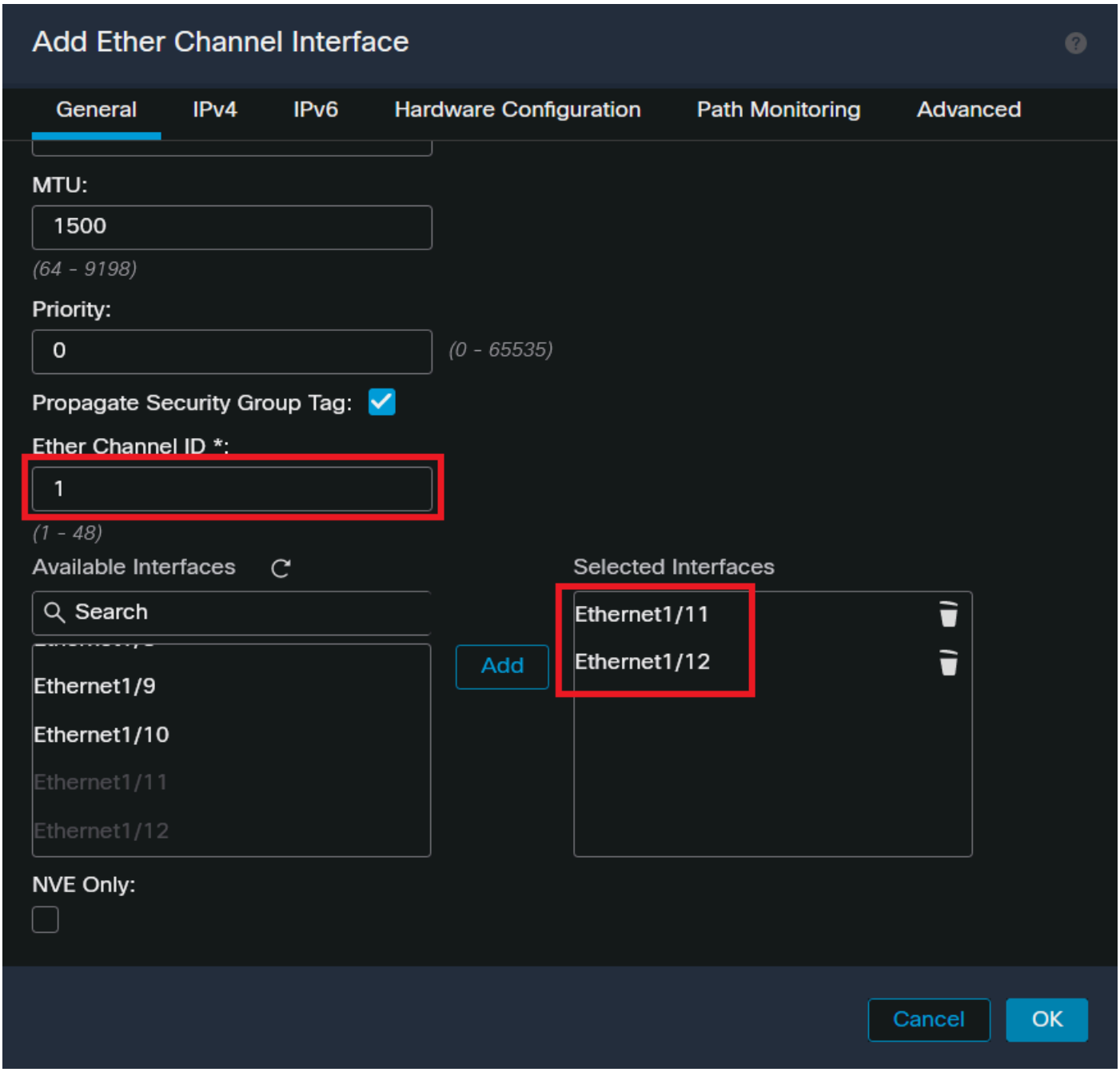


EtherChannel-Erstellung

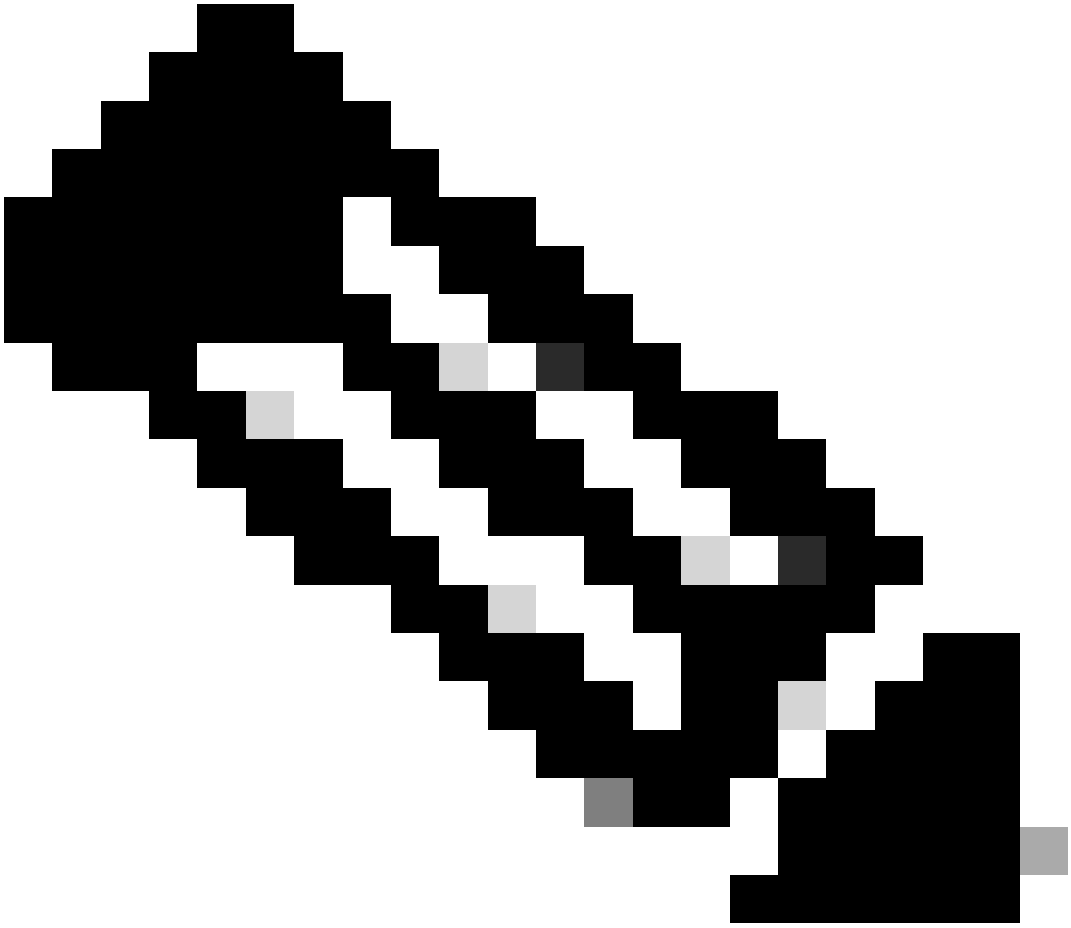
Schritt 4: Fügen Sie einen Schnittstellennamen, eine EtherChannel-ID und die Mitgliedsschnittstellen hinzu.



EtherChannel-Name

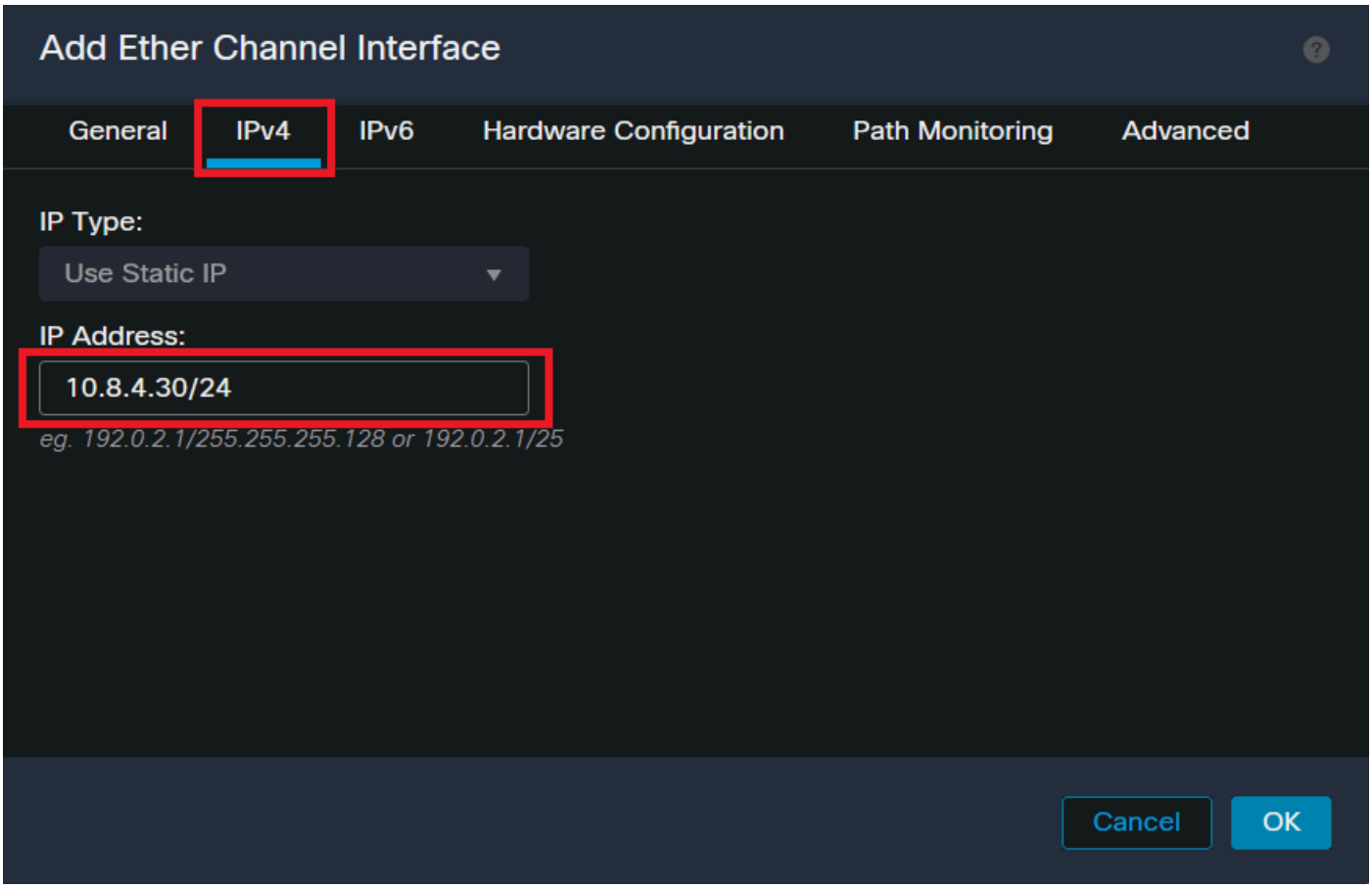


EtherChannel-ID und Mitglieder



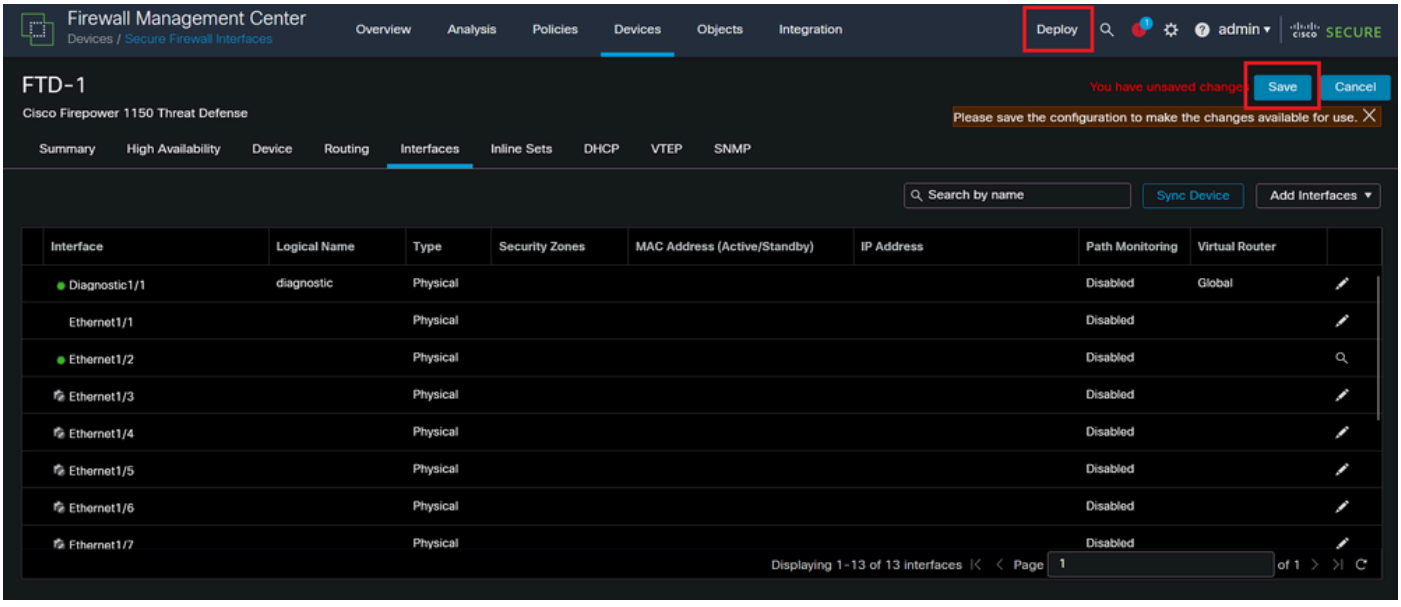
Hinweis: Die EtherChannel-ID auf dem FTD muss nicht mit der Port-Channel-ID auf dem Switch übereinstimmen.

Schritt 5: Navigieren Sie zur Registerkarte IPv4, und fügen Sie eine IP-Adresse im gleichen Subnetz wie VLAN 300 für den Switch hinzu.



EtherChannel-IP-Adresse

Schritt 6: Speichern Sie die Änderungen, und stellen Sie sie bereit.



Speichern und Bereitstellen

Überprüfung

Schritt 1: Stellen Sie sicher, dass der Status der VLAN- und Port-Channel-Schnittstellen aus Switch-Sicht aktiv ist.

```
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
```

Schritt 2: Überprüfen Sie, ob der Port-Channel-Status auf beiden FTD-Einheiten aktiv ist, indem Sie auf die Befehlszeilenschnittstelle des Geräts zugreifen.

```
> 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***
```

Schritt 3: Überprüfen Sie die Erreichbarkeit zwischen der Switch-SVI und der FTD-Port-Channel-IP-Adresse.

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.