Geïntegreerde redundante oplossing voor beveiligde firewall en L3 Switch

Inhoud

Inleiding

Dit document beschrijft een best practice voor redundante verbindingen tussen Cisco Catalyst Switches en Cisco Secure Firewalls op hoge beschikbaarheid.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall Threat Defence (FTD)
- Secure Firewall Management Center (FMC)
- Cisco IOS® XE
- Virtueel switchingsysteem (VSS)
- Hoge beschikbaarheid (HA)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

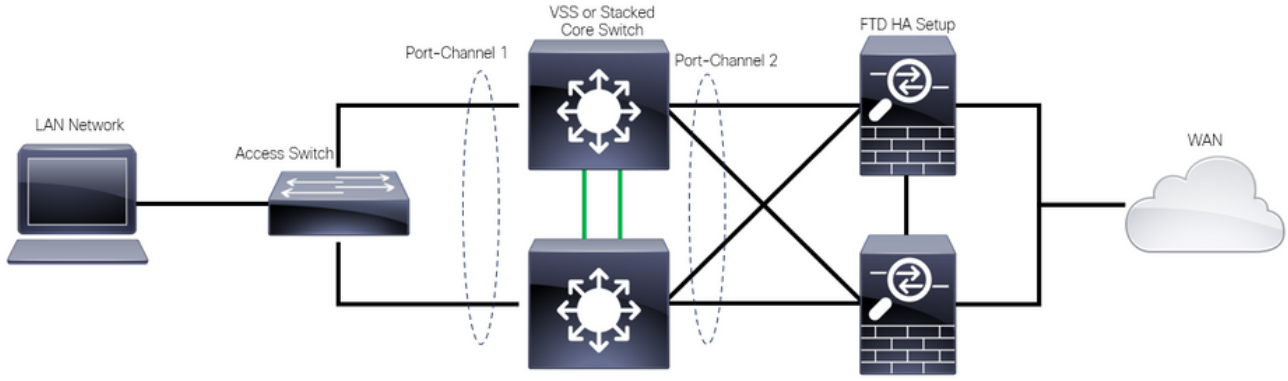
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram

Er zijn gebruikers die geloven dat één enkele verbinding (poortkanaal) tussen één logische Catalyst Switch (VSS of Stacked) naar een paar HA FTD's voldoende is om een volledige redundante oplossing te hebben voor het geval dat één unit of link uitvalt. Dit is een veel voorkomend misverstand omdat een VSS of stapelbare Switch als één logisch toestel fungeert. Tegelijkertijd fungeren twee HA FTD's als twee verschillende logische apparaten met de ene als Active en de andere als Standby.

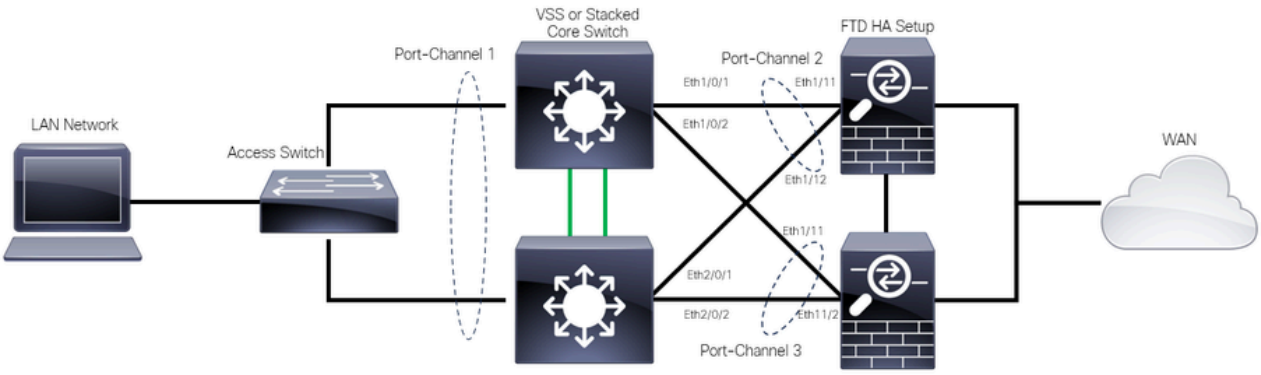
Het volgende diagram is een ongeldig ontwerp waarin één poortkanaal is geconfigureerd vanaf de Switch die is ingesteld voor het FTD HA-paar:



Ongeldig ontwerp

De vorige configuratie is niet geldig omdat dit poortkanaal fungeert als één link die is aangesloten op twee verschillende apparaten, waardoor netwerkbotsingen worden veroorzaakt. Daarom blokkeert het Spanning Tree Protocol (SPT) verbindingen van een van de FTD's.

Het volgende diagram is een geldig ontwerp waarin twee verschillende poortkanalen zijn geconfigureerd voor elk lid van de Switch VSS of Stack.



Geldig ontwerp

Configuraties

Switchconfiguratie

Stap 1. Configureer poortkanalen met hun respectievelijke 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
```

Stap 2. Configureer een Switched Virtual Interface (SVI) IP-adres voor het poortkanaal VLAN.

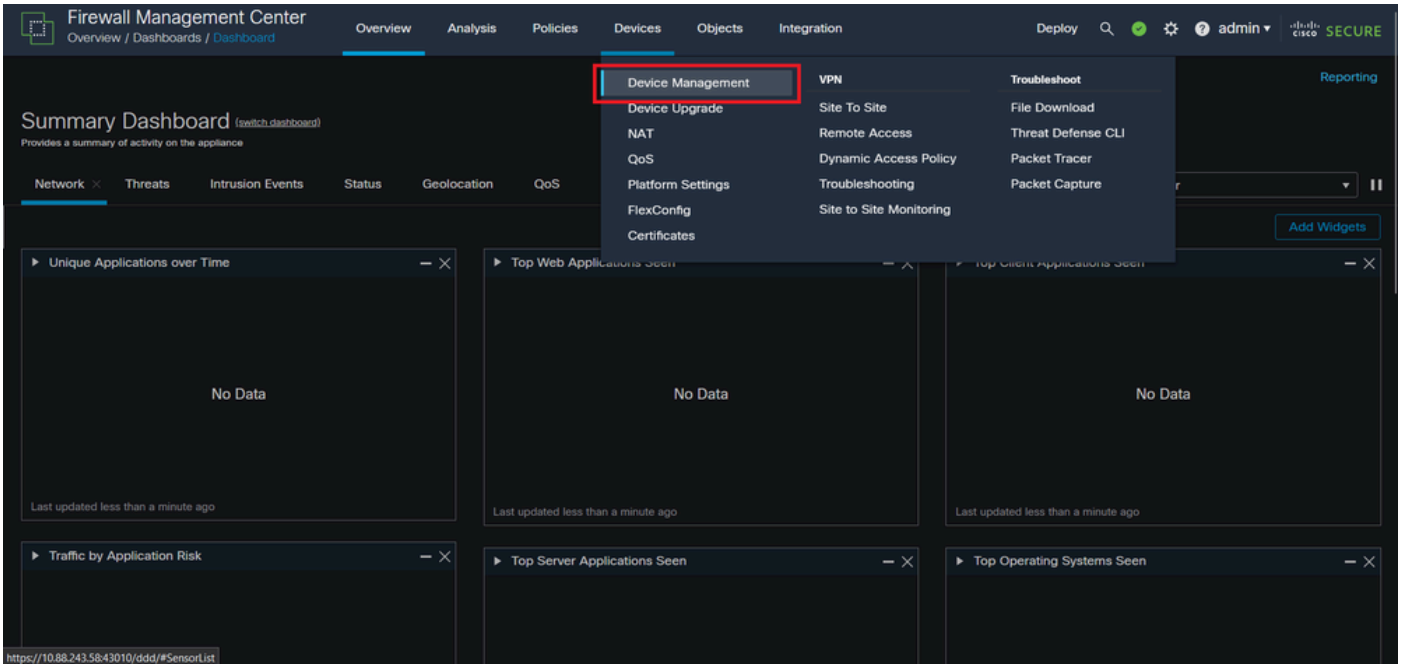
```
MXC.PS.A.06-3850-02(config-if)#exit
MXC.PS.A.06-3850-02(config)#interface VLAN 300
MXC.PS.A.06-3850-02(config-if)#ip address 10.8.4.31 255.255.255.0
MXC.PS.A.06-3850-02(config-if)#no shutdown
```

FTD HA-configuratie

Stap 1. Log in op de GUI van het VCC.

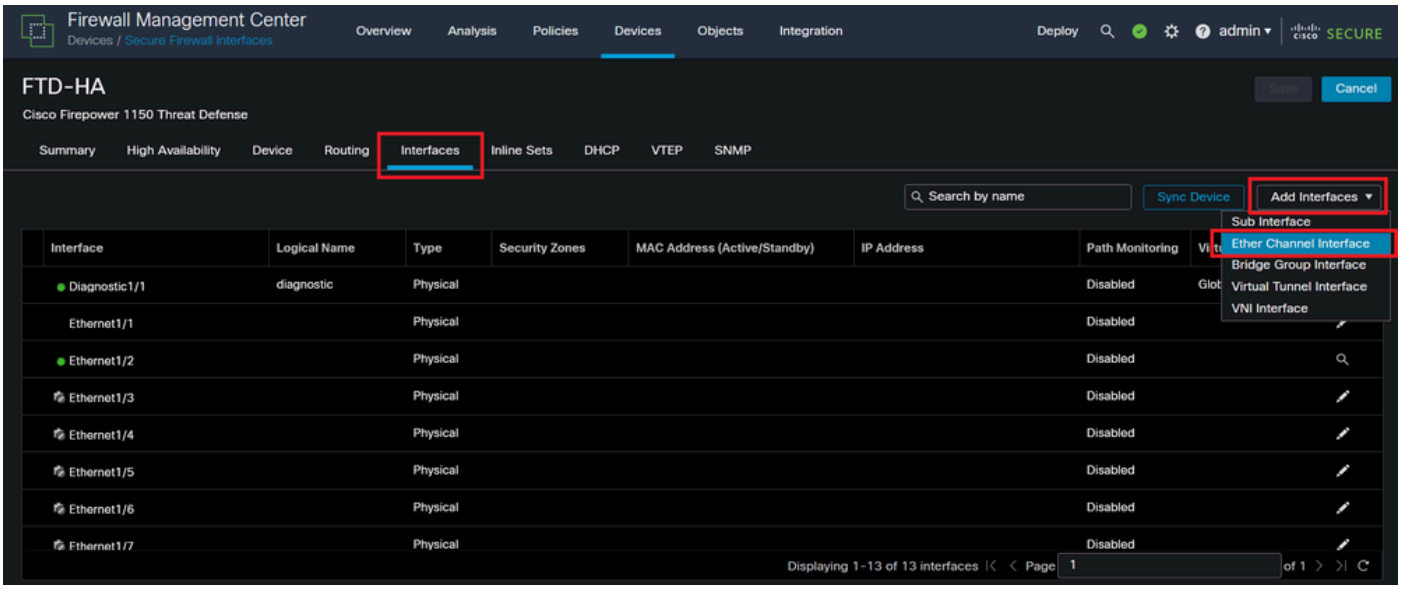
Inloggen bij VCC

Stap 2. Navigeer naar Apparaten > Apparaatbeheer.



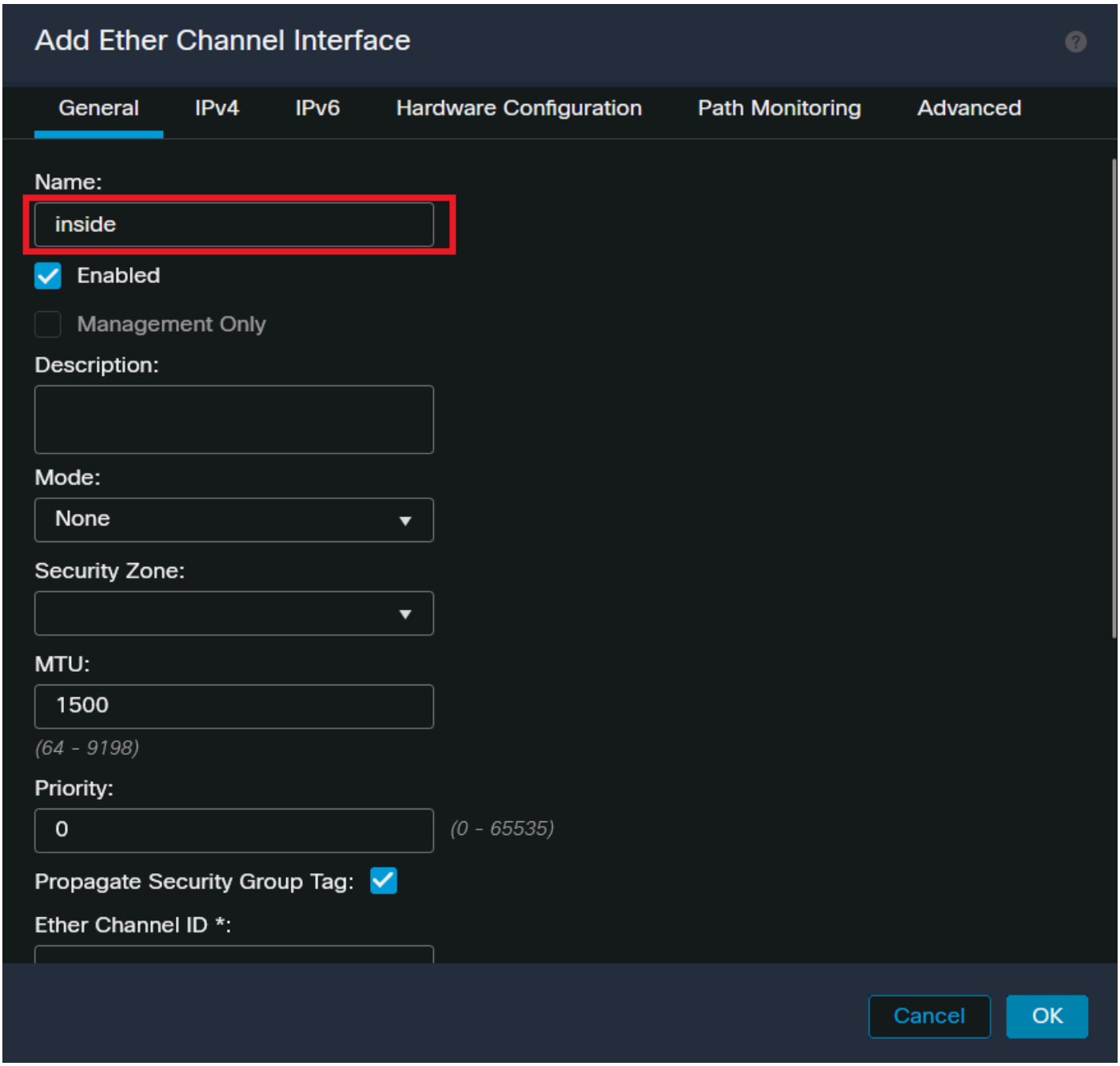
Apparaatbeheer

Stap 3. Bewerk het gewenste HA-apparaat en navigeer naar Interfaces > Add Interfaces > Ether Channel Interface.

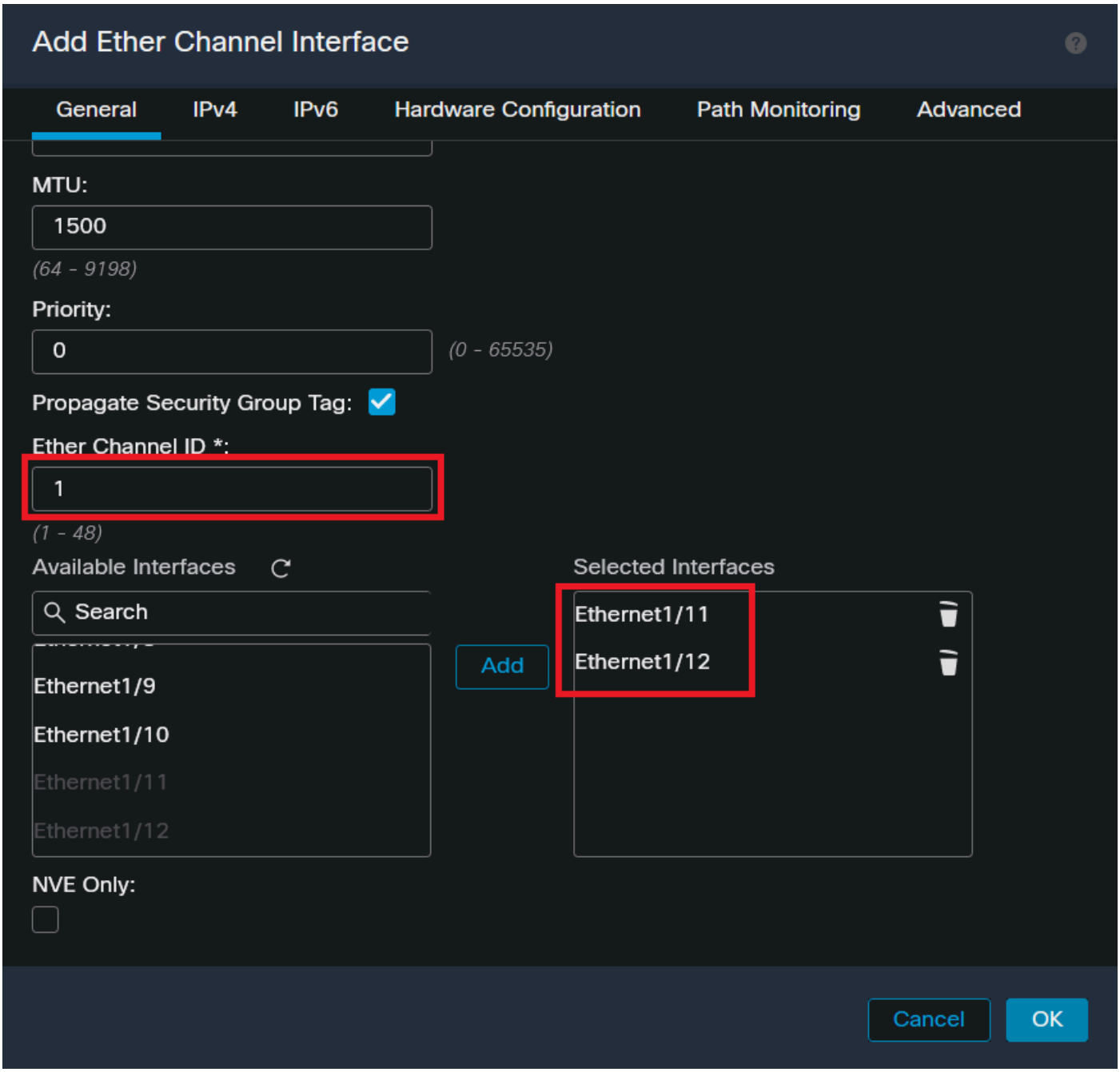


Creatie van Ether-kanaal

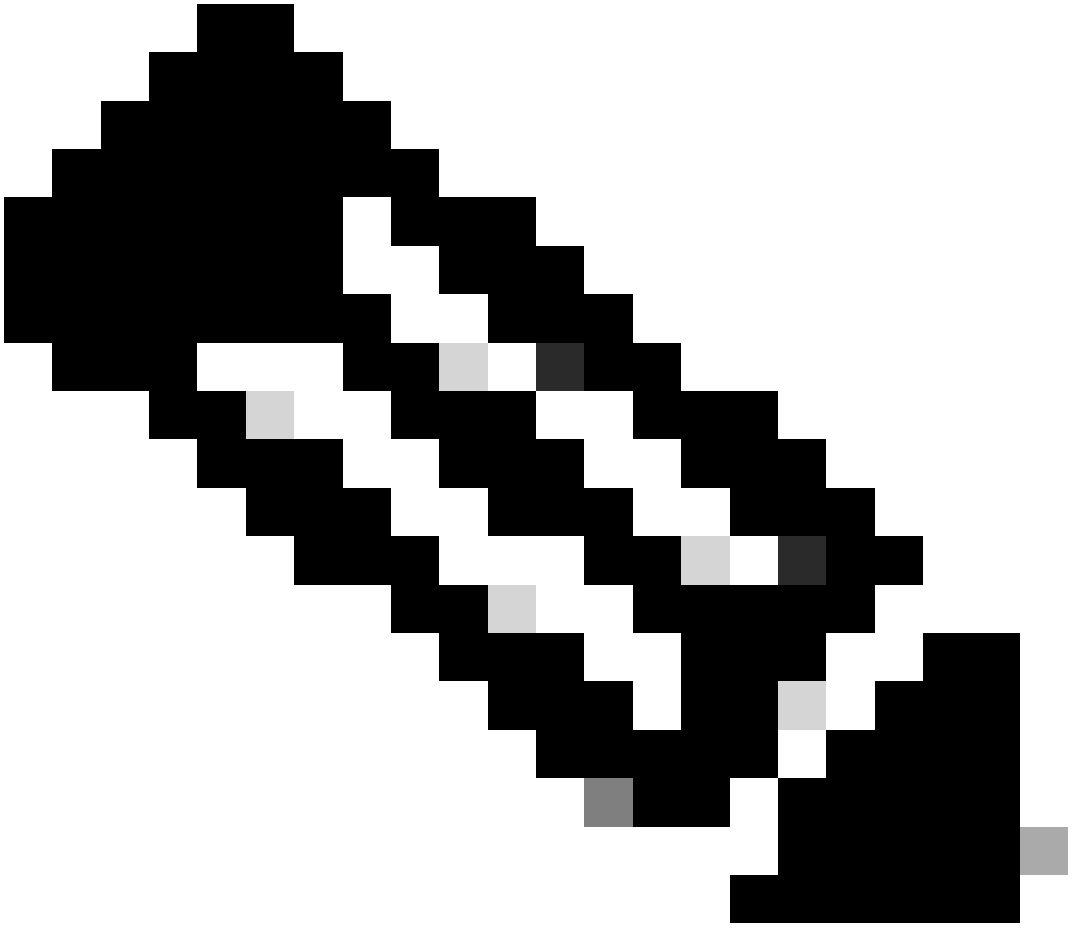
Stap 4. Voeg een interfacenaam, Ether Channel-id en de lidinterfaces toe.



Naam EtherChannel

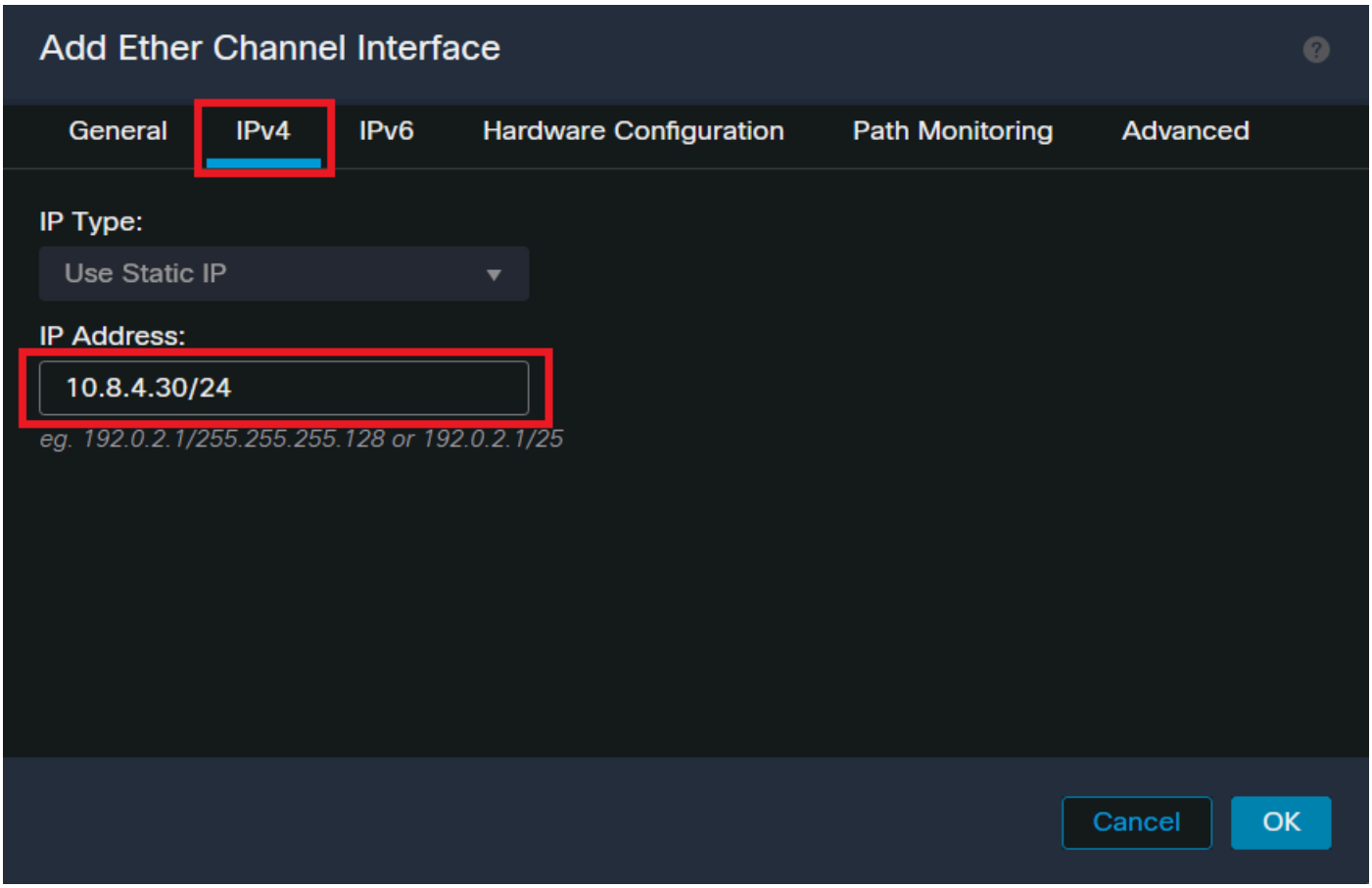


Ether-Channel ID en leden



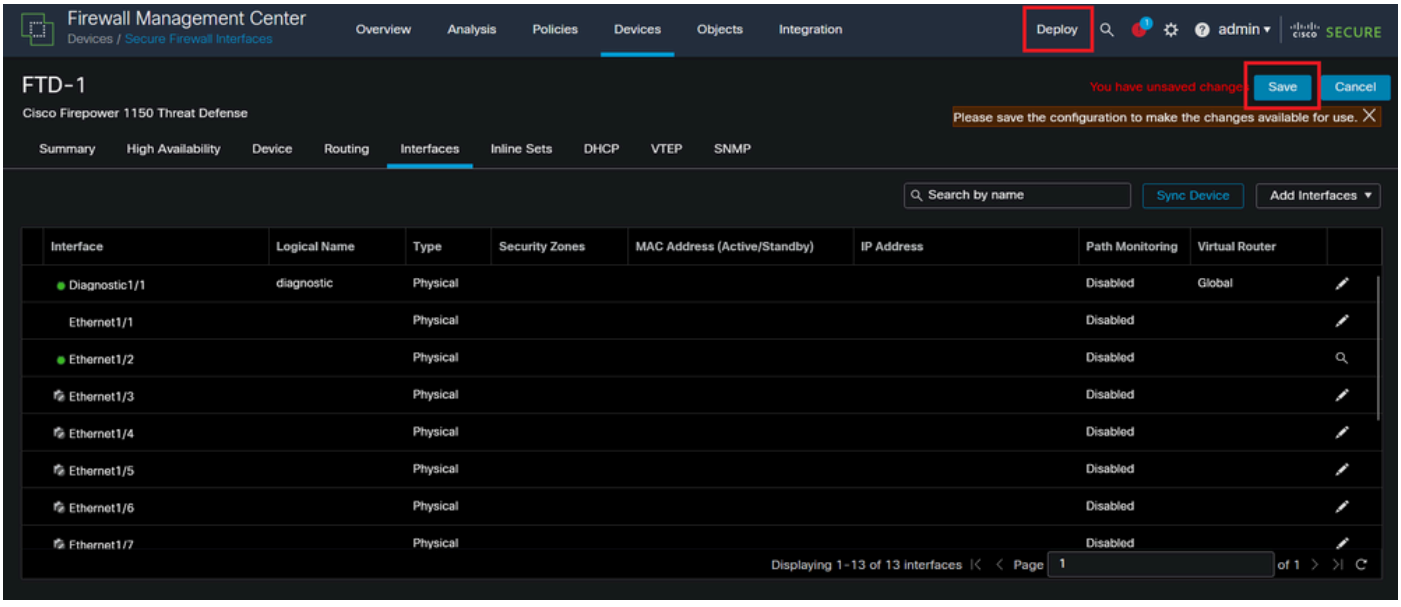
Opmerking: de Ether Channel-id op de FTD hoeft niet overeen te komen met de Port-Channel-id op de Switch.

Stap 5. Navigeer naar het tabblad IPv4 en voeg een IP-adres toe op hetzelfde subnetje als VLAN 300 voor de Switch.



Ether-Channel IP-adres

Stap 6. Sla de wijzigingen op en implementeer.



Opslaan en implementeren

Verifiëren

Stap 1. Zorg ervoor dat de status van de VLAN- en poortkanaals interfaces omhoog is vanuit het perspectief van de 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
```

Stap 2. Controleer of de poortkanaal-status op beide FTD-eenheden is ingesteld door toegang te krijgen tot de interface van de apparaatopdrachtregel.

```
> 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***
```

Stap 3. Controleer de bereikbaarheid tussen de Switch SVI en het FTD Port-Channel IP-adres.

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.