Integrazione della soluzione ridondante per Secure Firewall e switch L3

Sommario

Introduzione

In questo documento viene descritta una best practice per le connessioni ridondanti tra switch Cisco Catalyst e Cisco Secure Firewall su alta disponibilità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Threat Defense (FTD)
- Centro gestione firewall protetto (FMC)
- Cisco IOS® XE
- VSS (Virtual Switching System)
- Alta disponibilità (HA)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

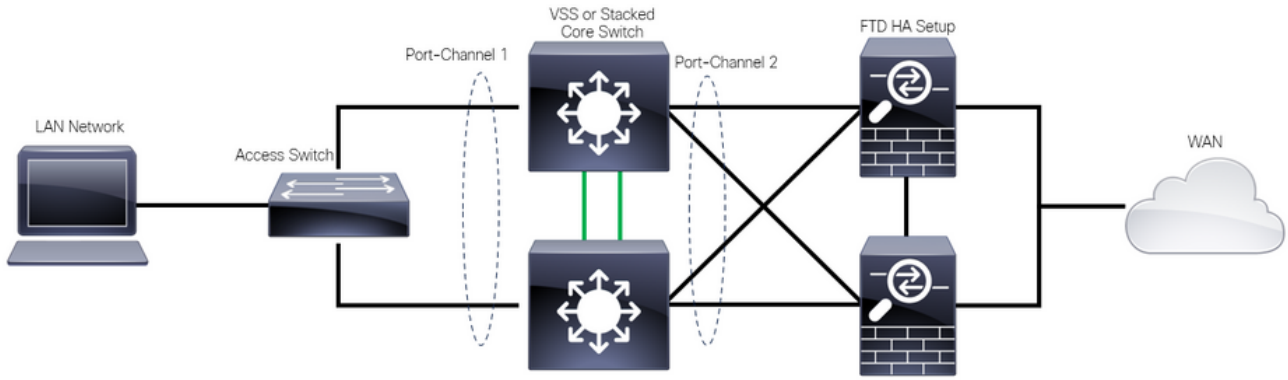
ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Alcuni utenti ritengono che un singolo collegamento di connessione (canale della porta) tra uno switch Catalyst logico (VSS o in stack) e una coppia di FTD HA sia sufficiente per ottenere una soluzione completamente ridondante in caso di guasto di un'unità o di un collegamento. Si tratta di un errore comune, in quanto l'installazione di un servizio VSS o di uno switch in stack funziona come un unico dispositivo logico. Mentre allo stesso tempo, una coppia di FTD HA agisce come due dispositivi logici diversi con uno come Attivo e l'altro come Standby.

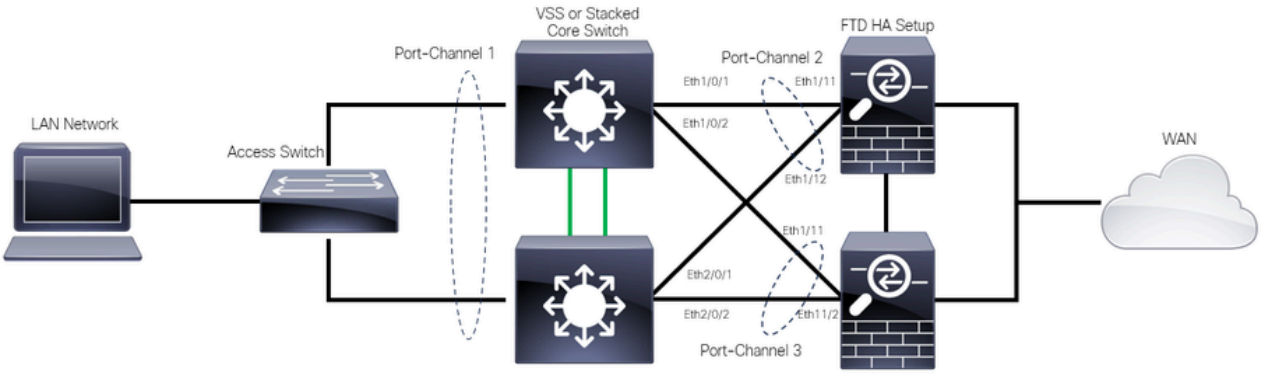
Il diagramma successivo è un progetto non valido in cui viene configurato un singolo canale porta dallo switch configurato verso la coppia FTD HA:



Progettazione non valida

La configurazione precedente non è valida perché questo canale di porta funziona come un singolo collegamento connesso a due dispositivi diversi, causando collisioni di rete, quindi lo Spanning Tree Protocol (SPT) blocca le connessioni da uno degli FTD.

Nel diagramma successivo viene illustrato un modello valido in cui due canali porte diverse vengono configurate per ciascun membro dello switch VSS o dello stack.



Configurazioni

Configurazione degli switch

Passaggio 1. Configurare i canali porta con la rispettiva VLAN (Virtual Local Area Network).

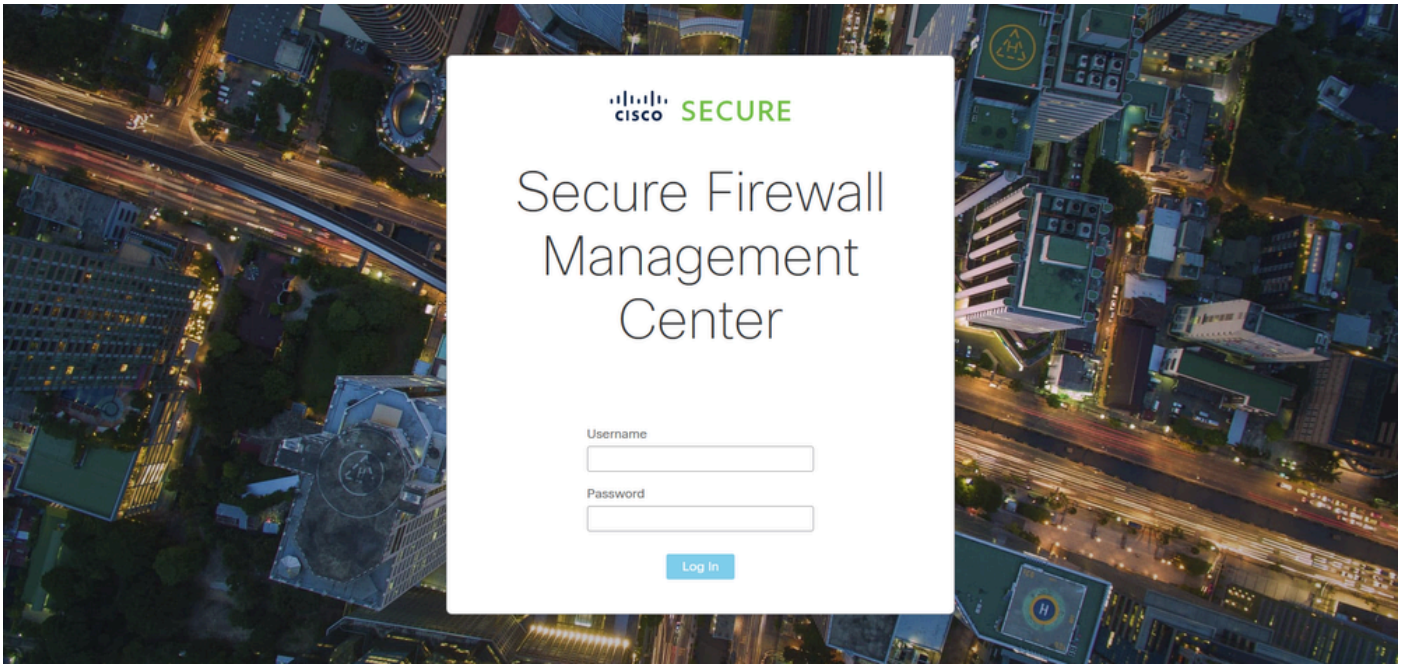
```
MXC.PS.A.06-3850-02#configure terminal
MXC.PS.A.06-3850-02(config)#interface GigabitEthernet 1/0/1
MXC.PS.A.06-3850-02(config-if)#shutdown
MXC.PS.A.06-3850-02(config-if)#switchport mode access
MXC.PS.A.06-3850-02(config-if)#switchport access vlan 300
% Access VLAN does not exist. Creating vlan 300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

Passaggio 2. Configurare un indirizzo IP dell'interfaccia virtuale commutata (SVI) per la VLAN del canale della 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
```

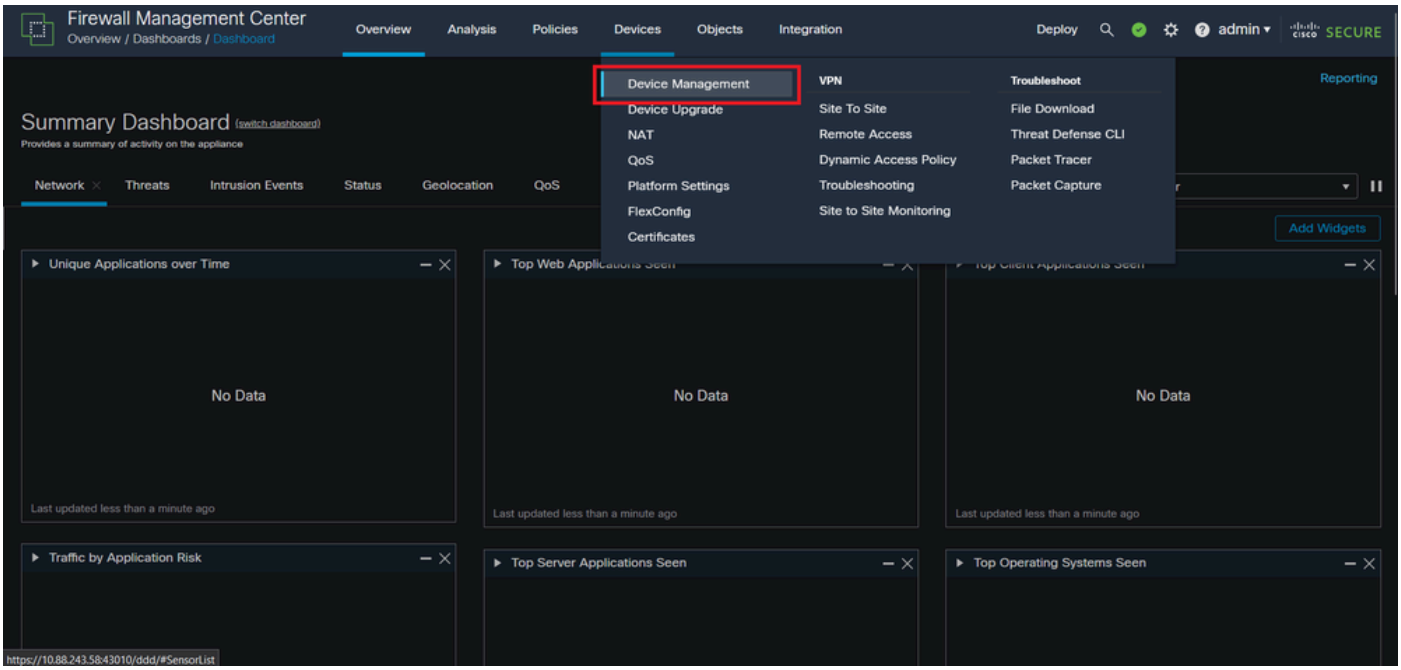
Configurazione FTD HA

Passaggio 1. Accedere all'interfaccia utente di FMC.



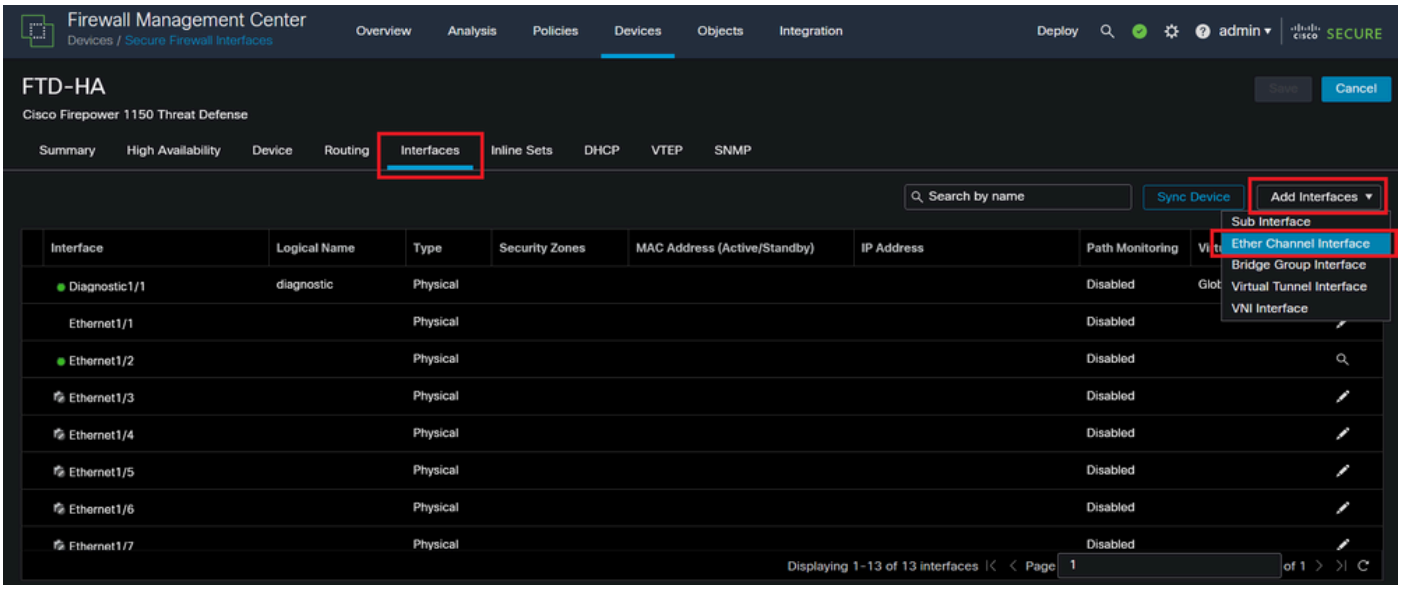
Log In di FMC

Passaggio 2. Selezionare Dispositivi > Gestione dispositivi.



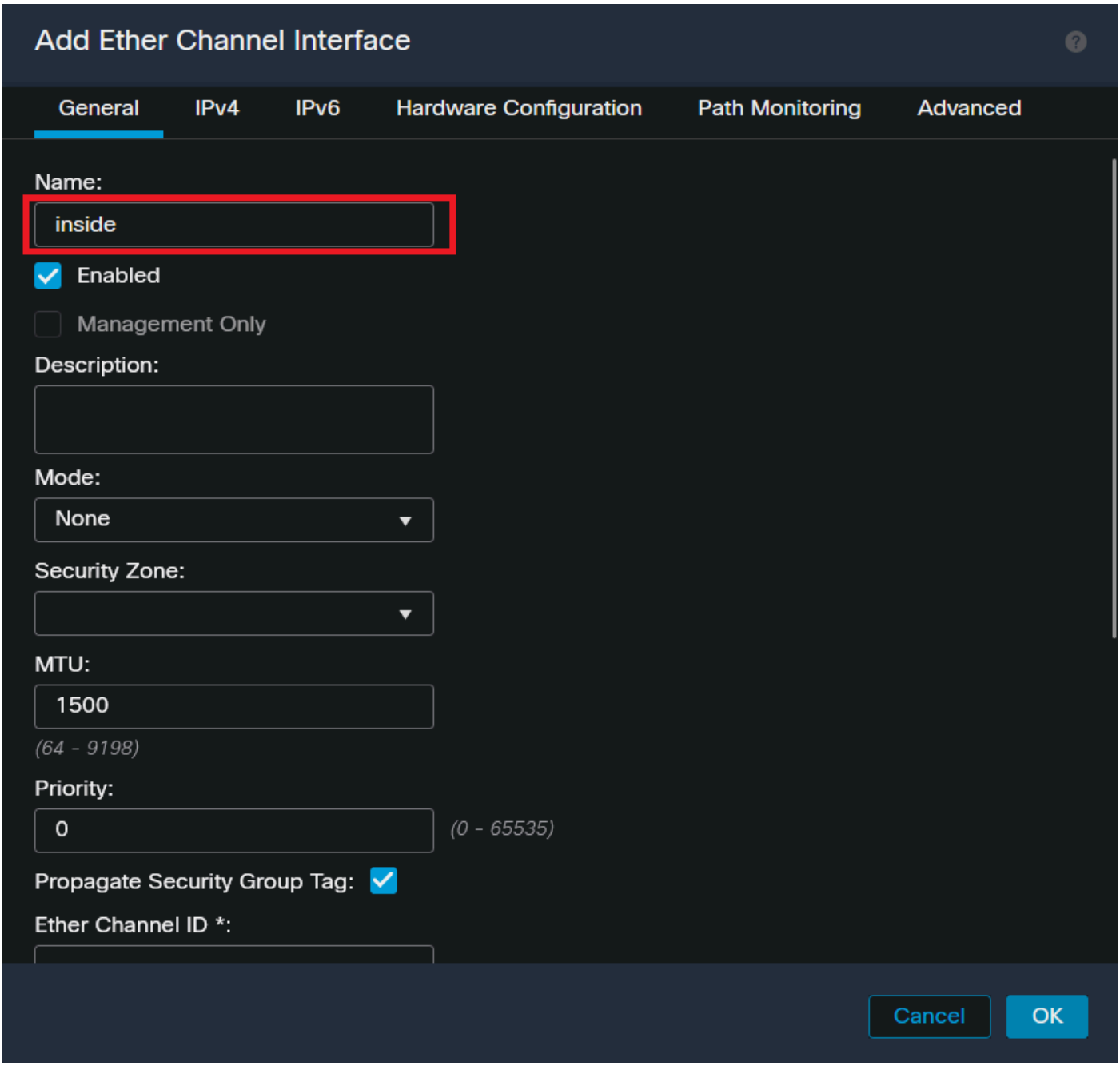
Gestione dispositivi

Passaggio 3. Modificare il dispositivo HA desiderato e selezionare Interfacce > Aggiungi interfacce > Interfaccia Ether Channel.

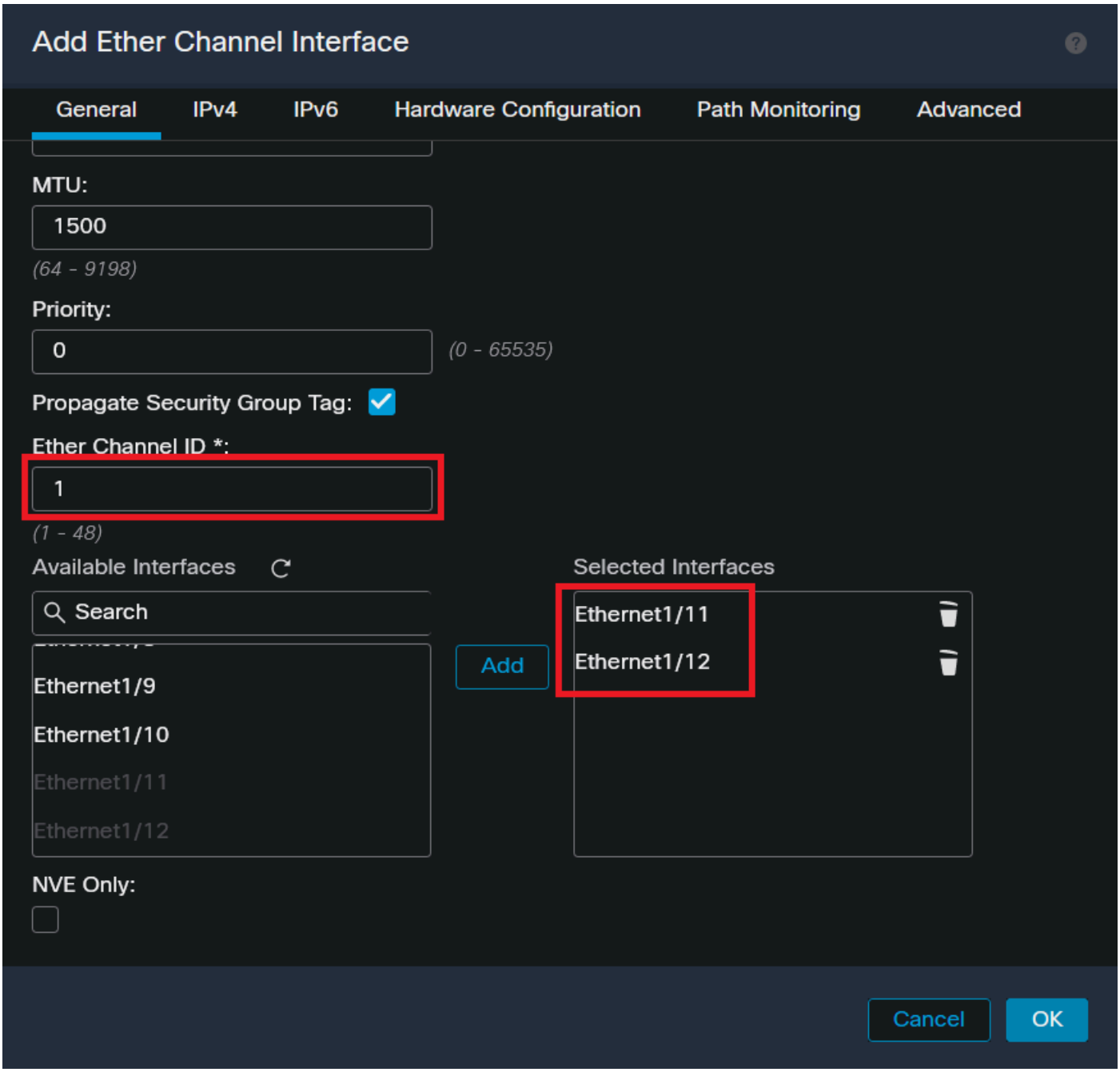


Creazione di Ether-Channel

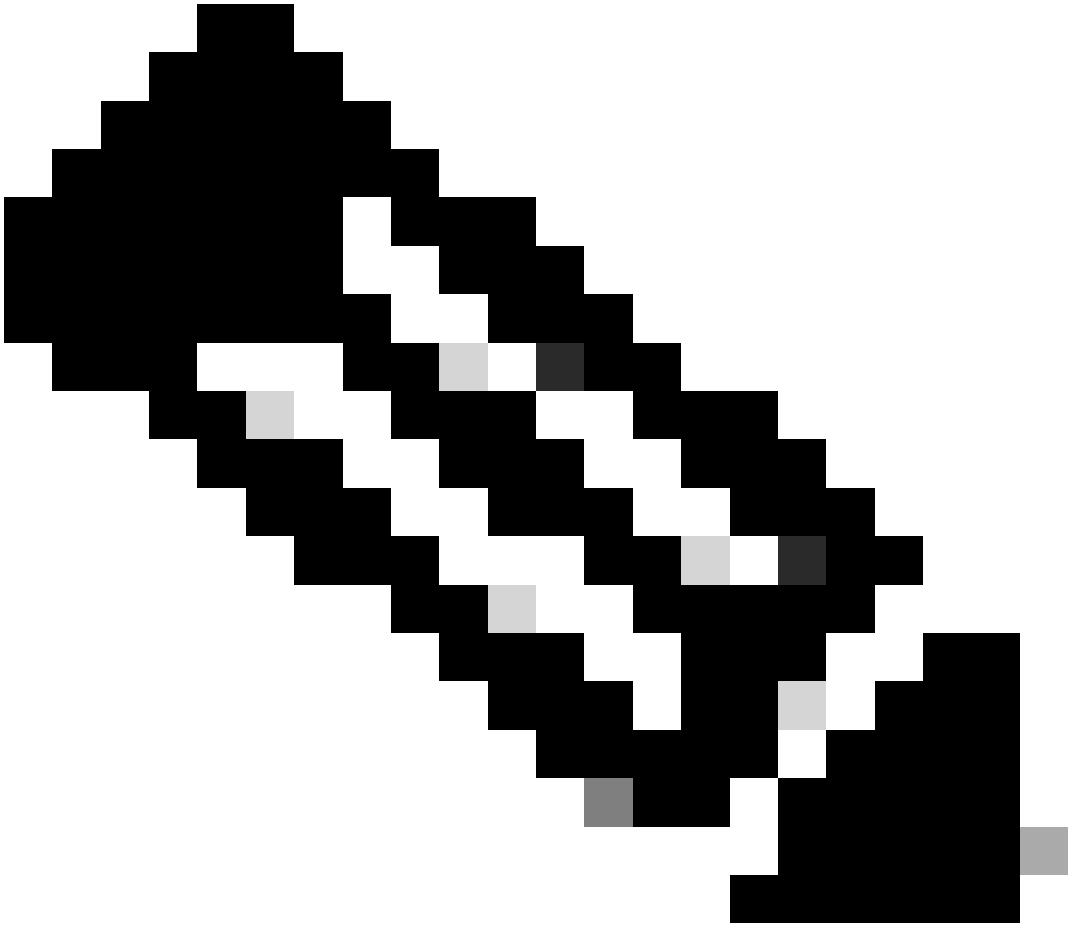
Passaggio 4. Aggiungere il nome di un'interfaccia, l'ID di Ether Channel e le interfacce membro.



Nome Ether-Channel

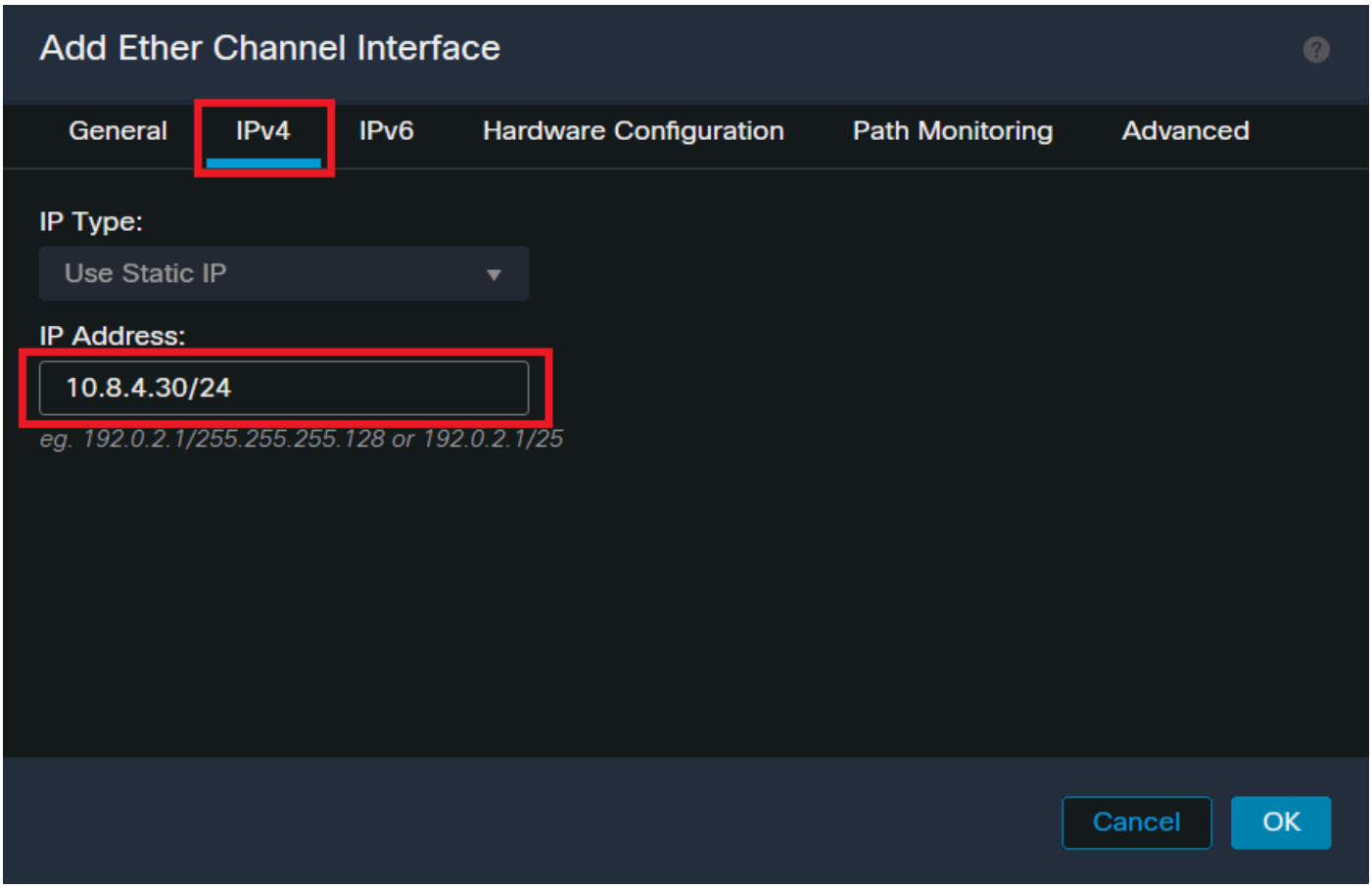


ID e membri Ether-Channel



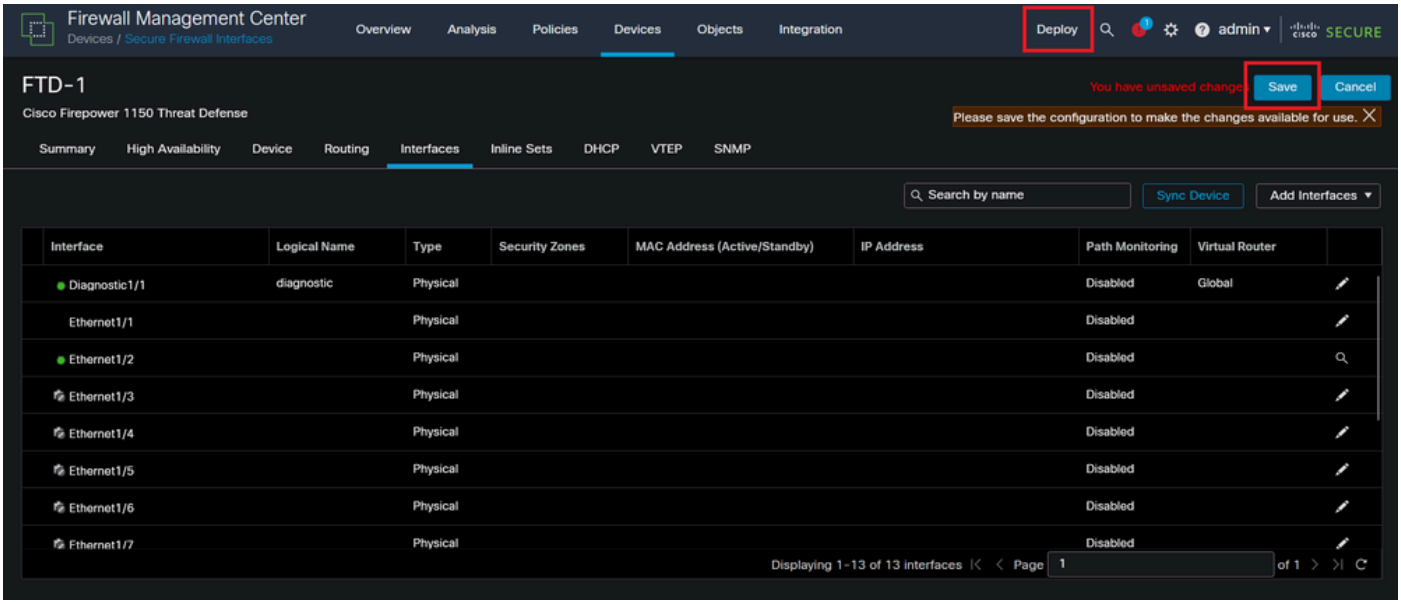
Nota: l'ID Ether Channel sull'FTD non deve corrispondere all'ID Port-Channel sullo switch.

Passaggio 5. Passare alla scheda IPv4 e aggiungere un indirizzo IP sulla stessa subnet della VLAN 300 per lo switch.



Indirizzo IP di Ether-Channel

Passaggio 6. Salvare le modifiche e distribuire.



Salva e distribuisci

Verifica

Passaggio 1. Verificare che lo stato della VLAN e delle interfacce del canale della porta sia attivo dalla prospettiva dello 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
```

Passaggio 2. Verificare che lo stato del canale della porta sia attivo su entrambe le unità FTD accedendo all'interfaccia della riga di comando del 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***
```

Passaggio 3. Verificare la raggiungibilità tra lo switch SVI e l'indirizzo IP del canale della 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).