Secure Firewall 및 L3 Switch를 위한 이중 솔루션 통합

목차

소개

이 문서에서는 고가용성을 지원하는 Cisco Catalyst 스위치와 Cisco Secure Firewall 간의 중복 연결을 위한 모범 사례에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(보안 방화벽 위협 방어)
- FMC(Secure Firewall Management Center)
- Cisco IOS® XE
- VSS(Virtual Switching System)
- 고가용성(HA)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

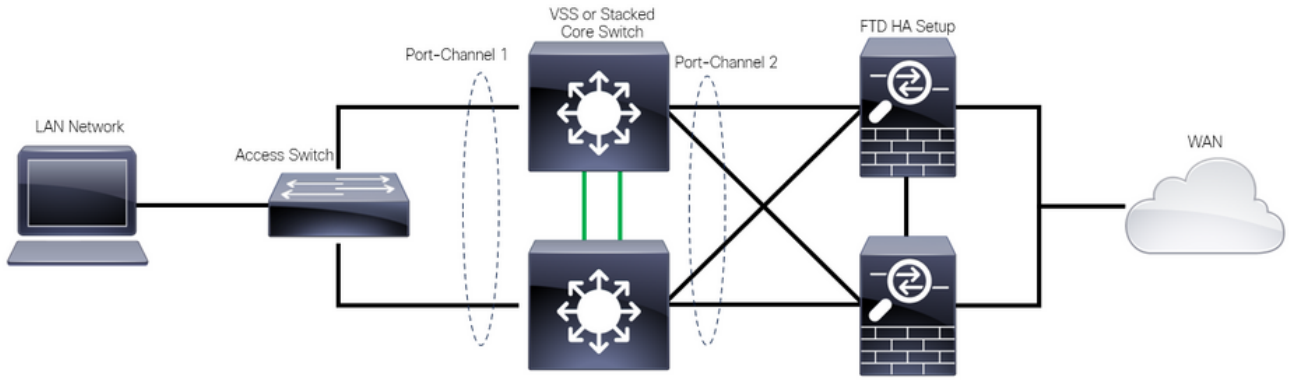
명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램

한 쌍의 HA FTD를 향하는 하나의 논리적 Catalyst Switch(VSS 또는 Stacked) 간의 단일 연결 링크(포트 채널)가 하나의 유닛 또는 링크에 장애가 발생할 경우 완전한 이중화 솔루션으로 충분하다고 생각하는 사용자가 있습니다. VSS 또는 스태킹된 스위치 설정이 단일 논리적 디바이스로 작동하기 때문에 이는 일반적인 오해입니다. 동시에 한 쌍의 HA FTD는 서로 다른 두 개의 논리적 디바이스로 작동하며, 하나는 Active로 다른 하나는 Standby로 작동합니다.

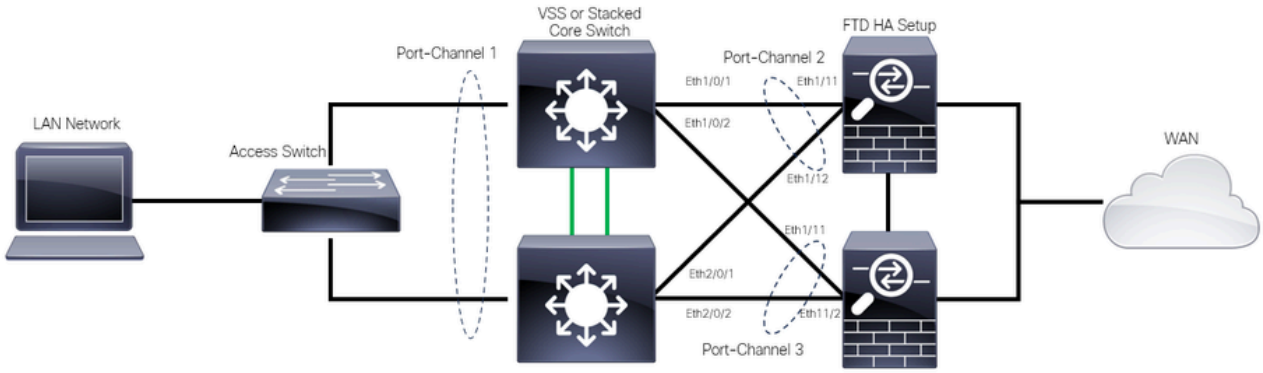
다음 다이어그램은 FTD HA 쌍으로 설정된 스위치에서 단일 포트 채널이 구성되는 잘못된 설계입니다.



잘못된 디자인

이 포트 채널이 서로 다른 두 디바이스에 연결된 단일 링크 역할을 하여 네트워크 충돌을 일으키므로 SPT(Spanning Tree Protocol)는 FTD 중 하나로부터의 연결을 차단하므로 이전 컨피그레이션이 유효하지 않습니다.

다음 다이어그램은 Switch VSS 또는 Stack의 각 멤버에 대해 서로 다른 두 개의 포트 채널을 구성하는 유효한 설계입니다.



유효한 설계

설정

스위치 구성

1단계. 각각의 VLAN(Virtual Local Area Network)으로 포트 채널을 구성합니다.

```
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
```

2단계. 포트 채널 VLAN에 대한 SVI(Switched Virtual Interface) IP 주소를 구성합니다.

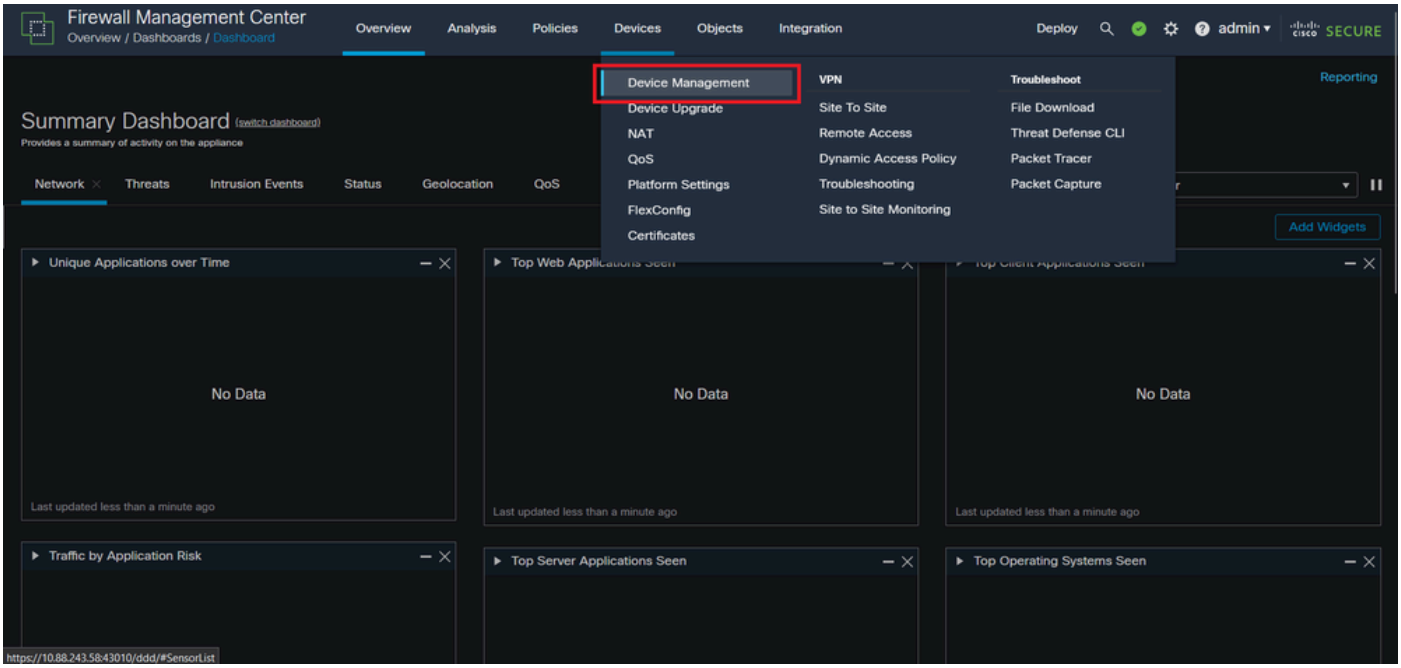
```
MXC.PS.A.06-3850-02(config-if)#exit
MXC.PS.A.06-3850-02(config)#interface VLAN 300
MXC.PS.A.06-3850-02(config-if)#ip address 10.8.4.31 255.255.255.0
MXC.PS.A.06-3850-02(config-if)#no shutdown
```

FTD HA 컨피그레이션

1단계. FMC GUI에 로그인합니다.

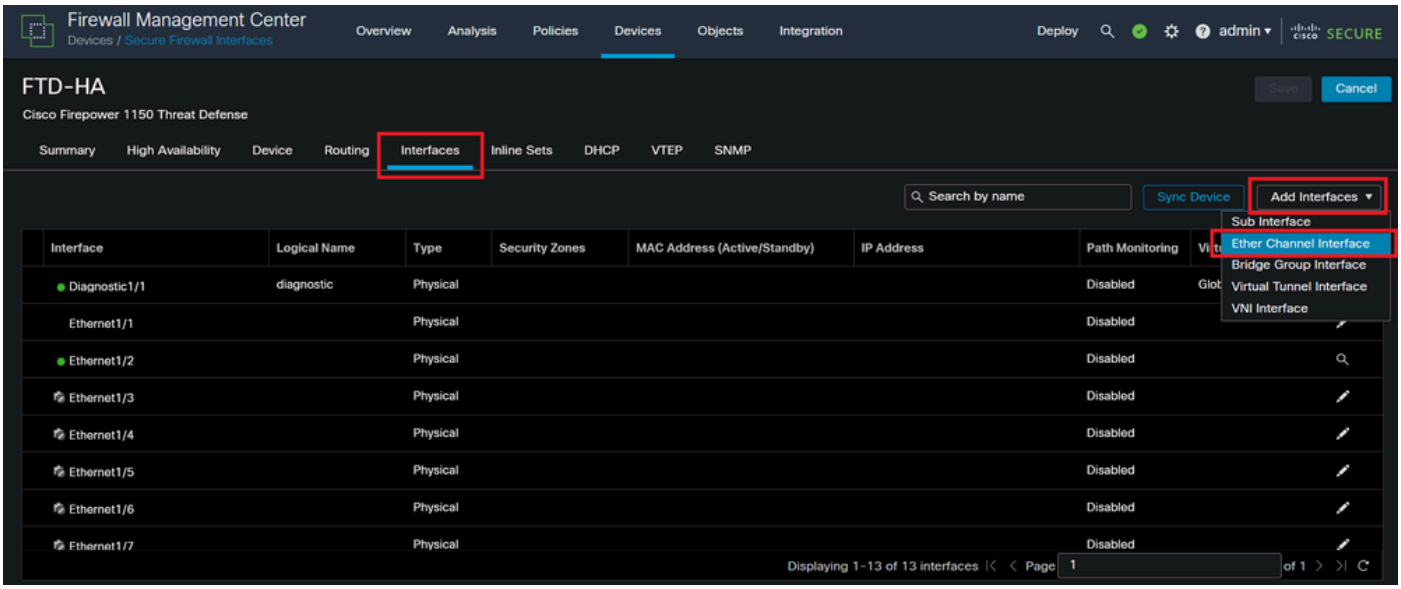
FMC 로그인

2단계. Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다.



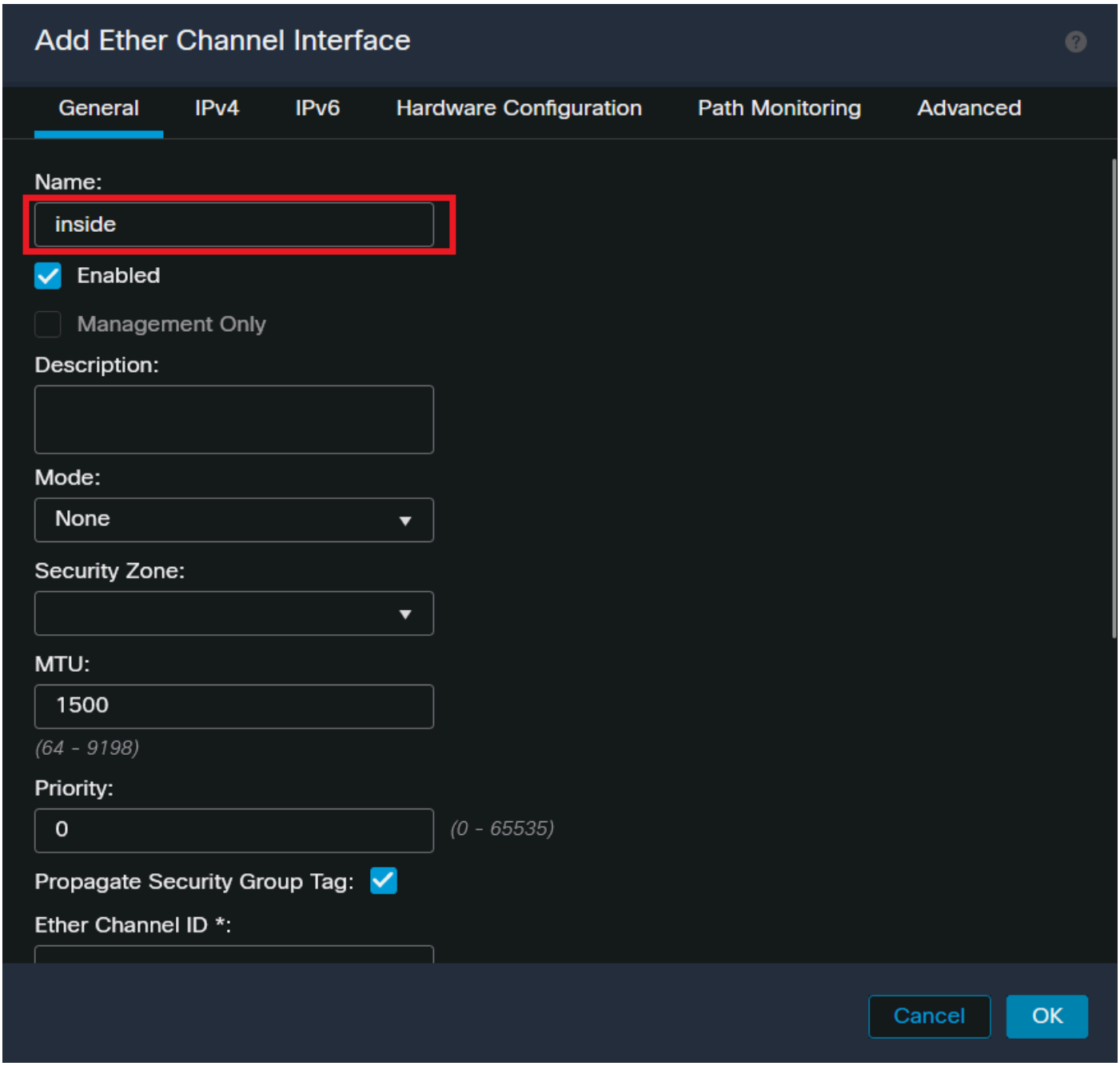
장치 관리

3단계. 원하는 HA 디바이스를 편집하고 Interfaces(인터페이스) > Add Interfaces(인터페이스 추가) > Ether Channel Interface(이더넷 채널 인터페이스)로 이동합니다.

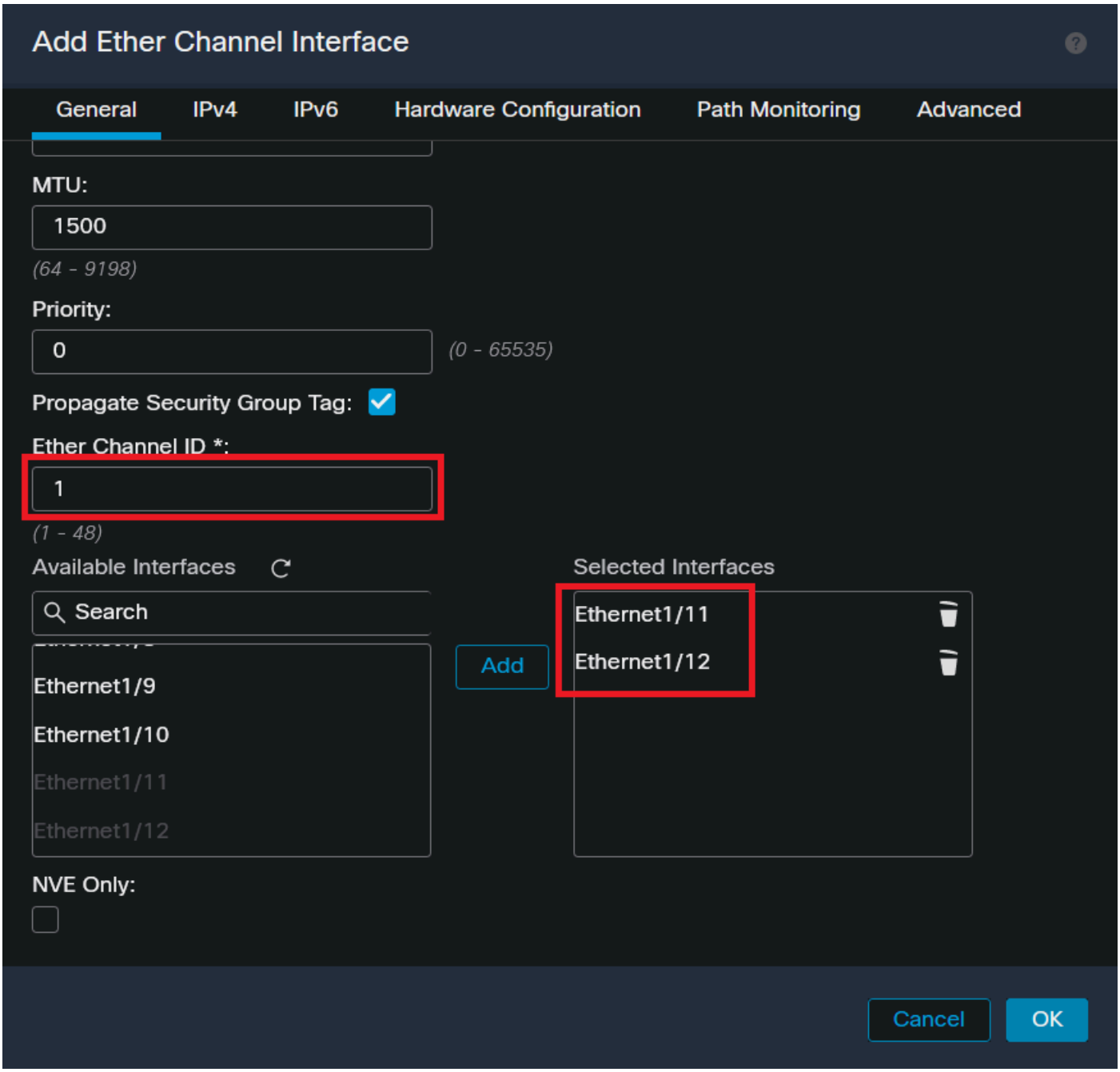


이더 채널 생성

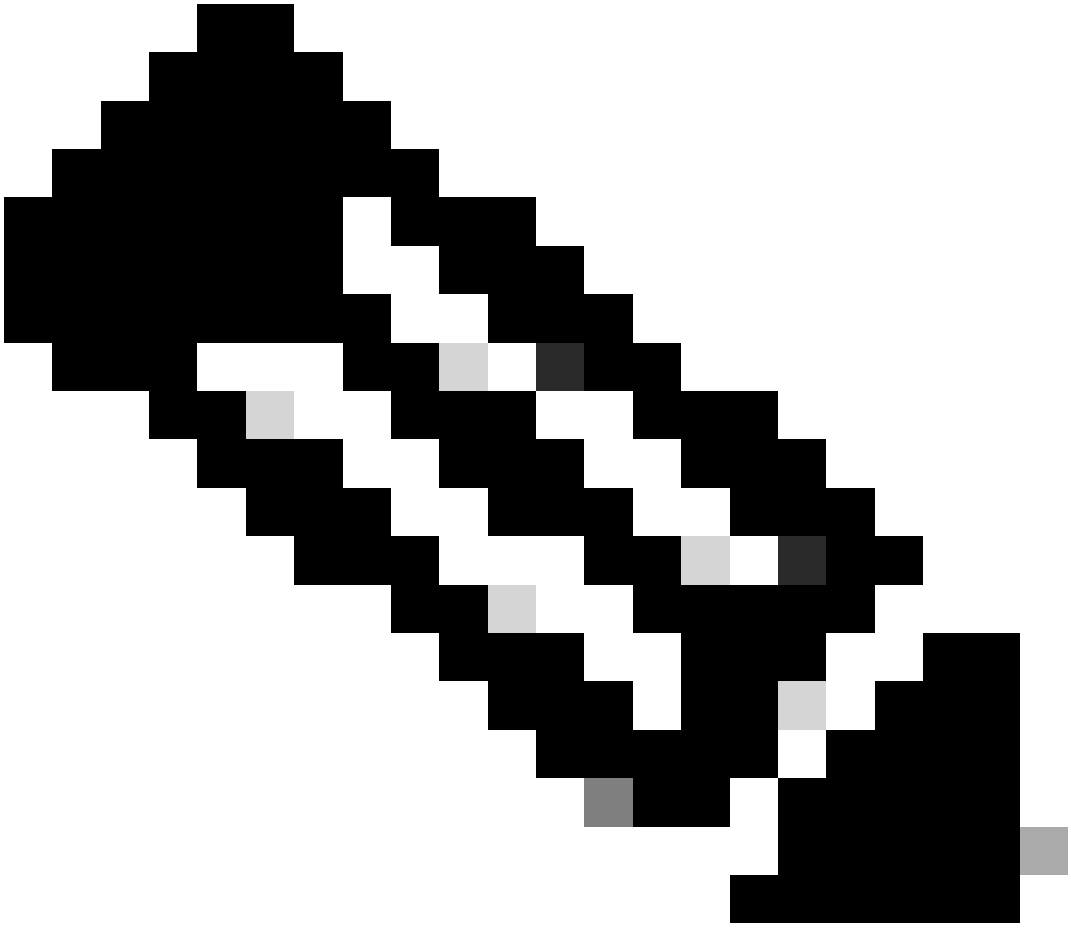
4단계. 인터페이스 이름, Ether Channel ID 및 멤버 인터페이스를 추가합니다.



Ether-Channel 이름

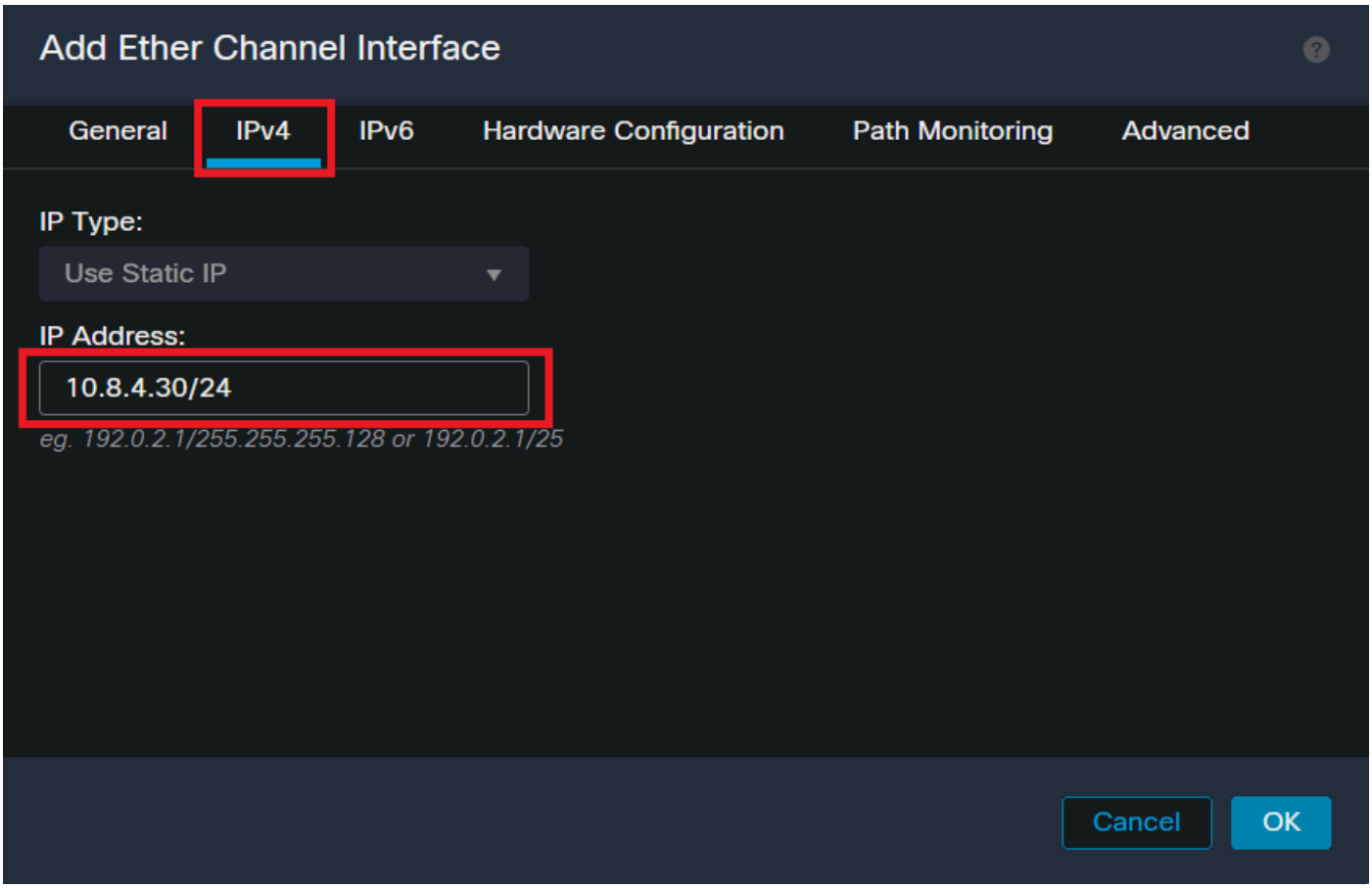


Ether-Channel ID 및 멤버



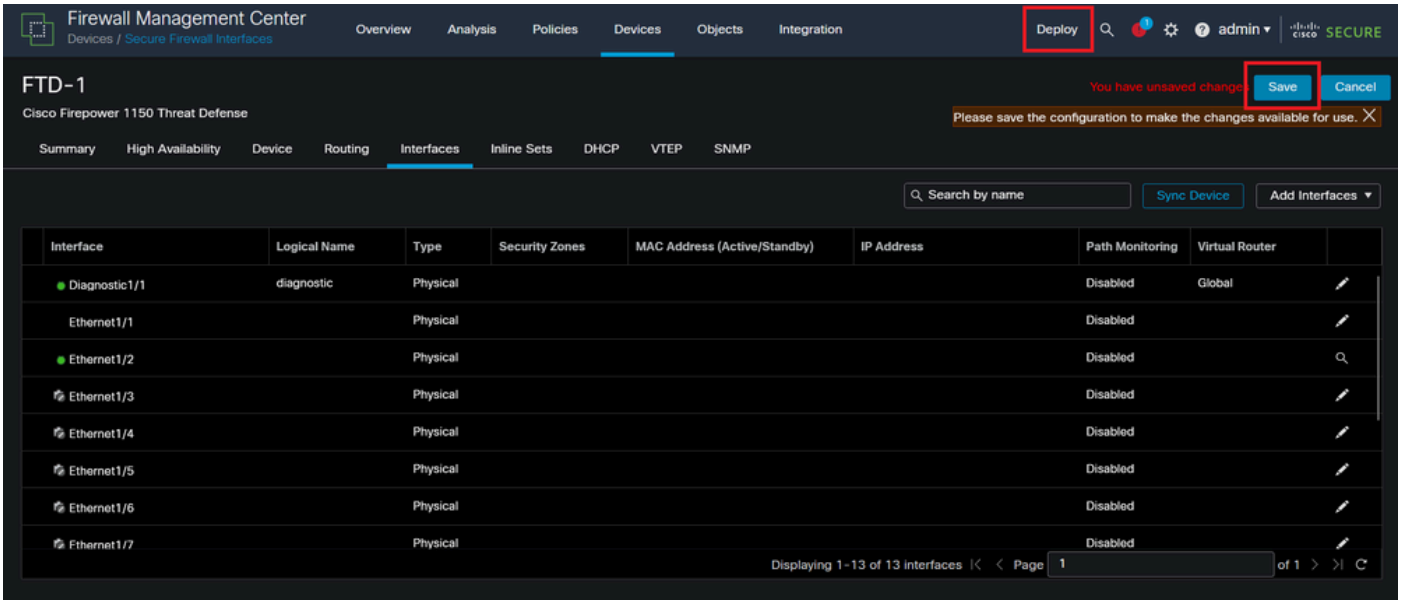
참고: FTD의 Ether Channel ID는 스위치의 Port-Channel ID와 일치하지 않아도 됩니다.

5단계. IPv4 탭으로 이동하여 스위치의 VLAN 300과 동일한 서브넷에 IP 주소를 추가합니다.



Ether-Channel IP 주소

6단계. 변경 사항을 저장하고 구축합니다.



저장 및 배포

다음을 확인합니다.

1단계. VLAN 및 포트 채널 인터페이스의 상태가 스위치의 관점에서 작동 중인지 확인합니다.

```
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
```

2단계. 디바이스 명령줄 인터페이스에 액세스하여 포트 채널 상태가 두 FTD 유닛 모두에서 가동 중인지 확인합니다.

```
> 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***
```

3단계. 스위치 SVI와 FTD 포트 채널 IP 주소 간의 연결성을 확인합니다.

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.