

セキュアなファイアウォールとL3スイッチの冗長ソリューションの統合

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[スイッチの設定](#)

[FTD HAの設定](#)

[確認](#)

はじめに

このドキュメントでは、ハイアベイラビリティのCisco CatalystスイッチとCisco Secure Firewall間の冗長接続のベストプラクティスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール脅威対策(FTD)
- セキュアファイアウォール管理センター(FMC)
- Cisco IOS® XE
- 仮想スイッチングシステム(VSS)
- ハイアベイラビリティ(HA)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Threat Defenseバージョン7.2.5.1
- Secure Firewall Manager Center(FMC)バージョン7.2.5.1
- Cisco IOS XEバージョン16.12.08

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

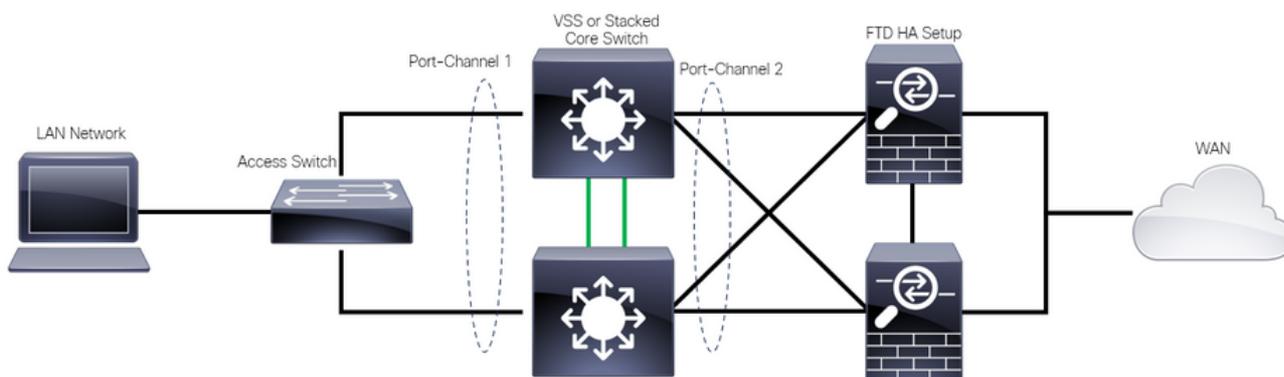
す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

HA FTDのペアに対する1つの論理Catalystスイッチ (VSSまたはスタック型) 間の単一の接続リンク (ポートチャネル) は、1つのユニットまたはリンクに障害が発生した場合に備えて完全な冗長ソリューションを用意すれば十分であると考えられるユーザーもいます。これは、VSSまたはスタックスイッチの設定が単一の論理デバイスとして動作するため、一般的な誤解です。同時に、1組のHA FTDが2つの異なる論理デバイスとして機能し、一方がアクティブ、もう一方がスタンバイになります。

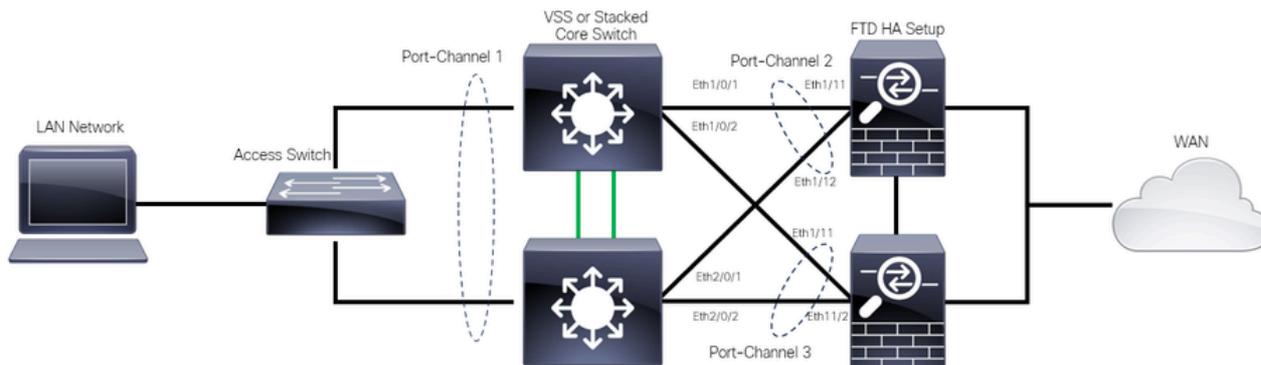
次の図は、FTD HAペアに向けて設定されたスイッチから単一のポートチャネルが設定されている無効な設計です。



無効な設計

このポートチャネルは2つの異なるデバイスに接続された単一のリンクとして動作するため、前の設定は有効ではなく、ネットワークの競合が発生し、スパニングツリープロトコル(SPT)によって、いずれかのFTDからの接続がブロックされます。

次の図は、スイッチVSSまたはスタックのメンバごとに2つの異なるポートチャネルが設定されている有効な設計です。



有効設計

コンフィギュレーション

スイッチの設定

ステップ 1: ポートチャネルをそれぞれの仮想ローカルエリアネットワーク(VLAN)で設定します。

```
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
```

ステップ 2: ポートチャネルVLANのスイッチ仮想インターフェイス(SVI)IPアドレスを設定します。

```
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
```

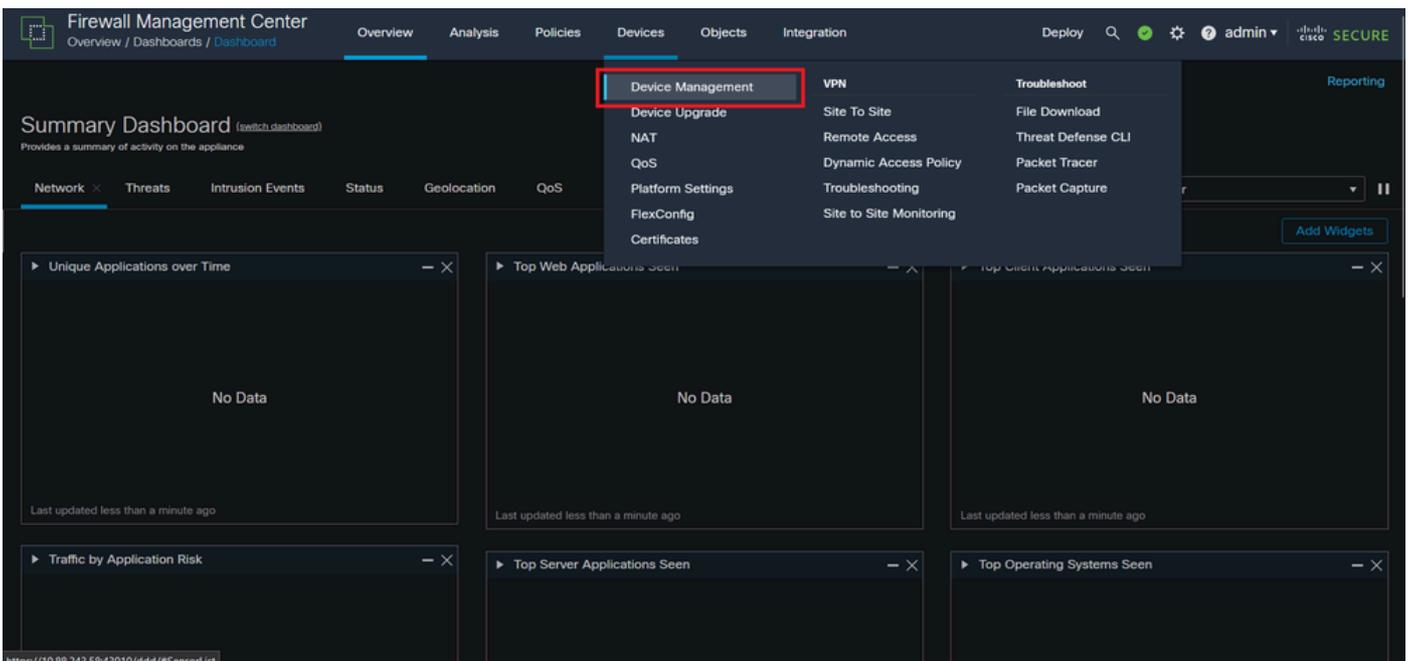
FTD HAの設定

ステップ 1 : FMCのGUIにログインします。



FMCログイン

ステップ 2 : [Device] > [Device Management]に移動します。



デバイス管理

ステップ 3 : 目的のHAデバイスを編集し、Interfaces > Add Interfaces > Ether Channel Interfaceの順に移動します。

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration Deploy admin

FTD-HA
Cisco Firepower 1150 Threat Defense

Summary High Availability Device Routing **Interfaces** Inline Sets DHCP VTEP SNMP

Search by name Sync Device **Add Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual
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

イーサチャネルの作成

ステップ 4 : インターフェイス名、Ether Channel ID、およびメンバーインターフェイスを追加します。

Add Ether Channel Interface



General

IPv4

IPv6

Hardware Configuration

Path Monitoring

Advanced

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 *:

Cancel

OK

Ether-Channel名

Add Ether Channel Interface



General

IPv4

IPv6

Hardware Configuration

Path Monitoring

Advanced

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

Add

Selected Interfaces

Ethernet1/11

Ethernet1/12

NVE Only:

Cancel

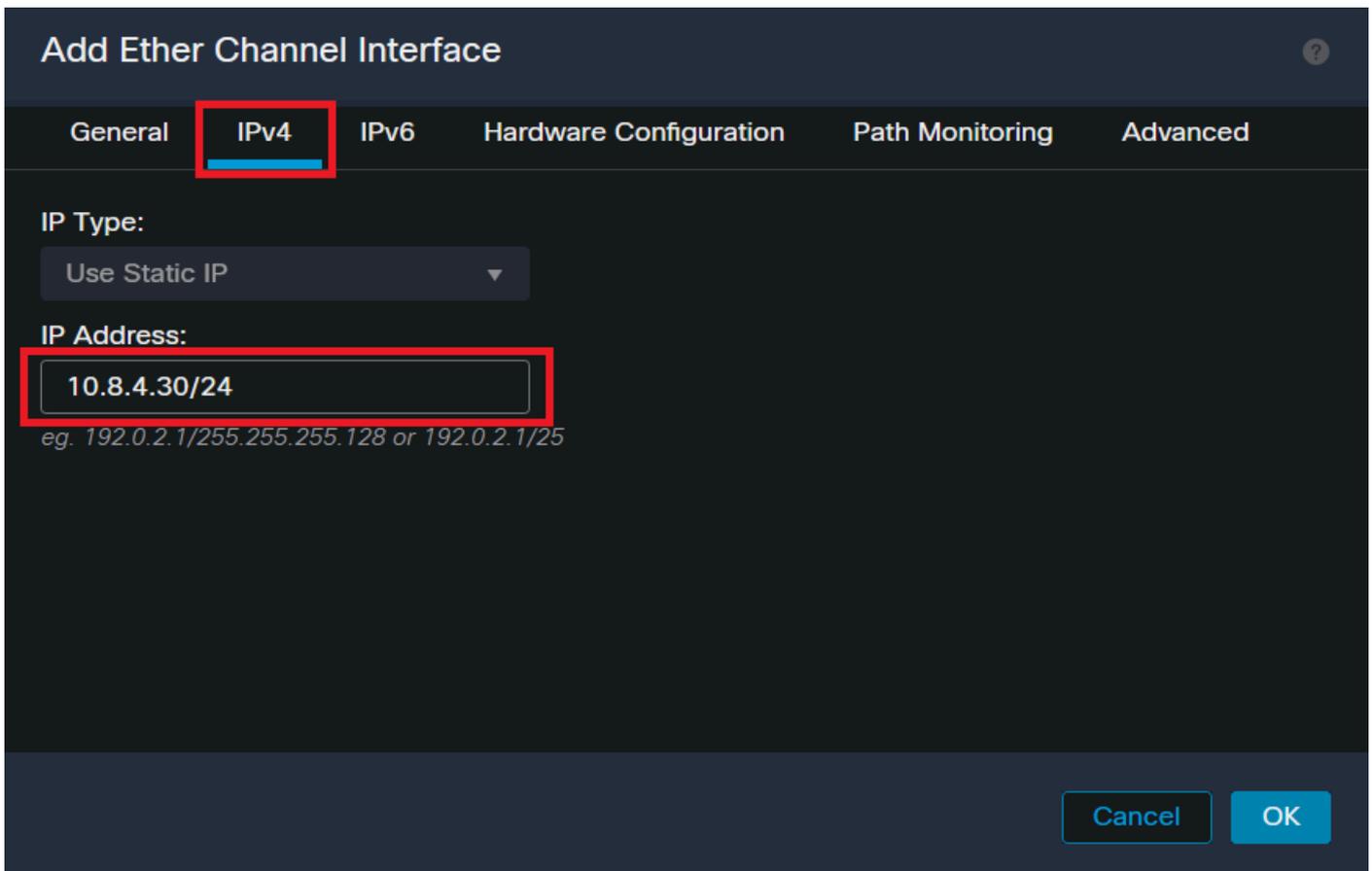
OK

Ether-Channel IDおよびメンバ



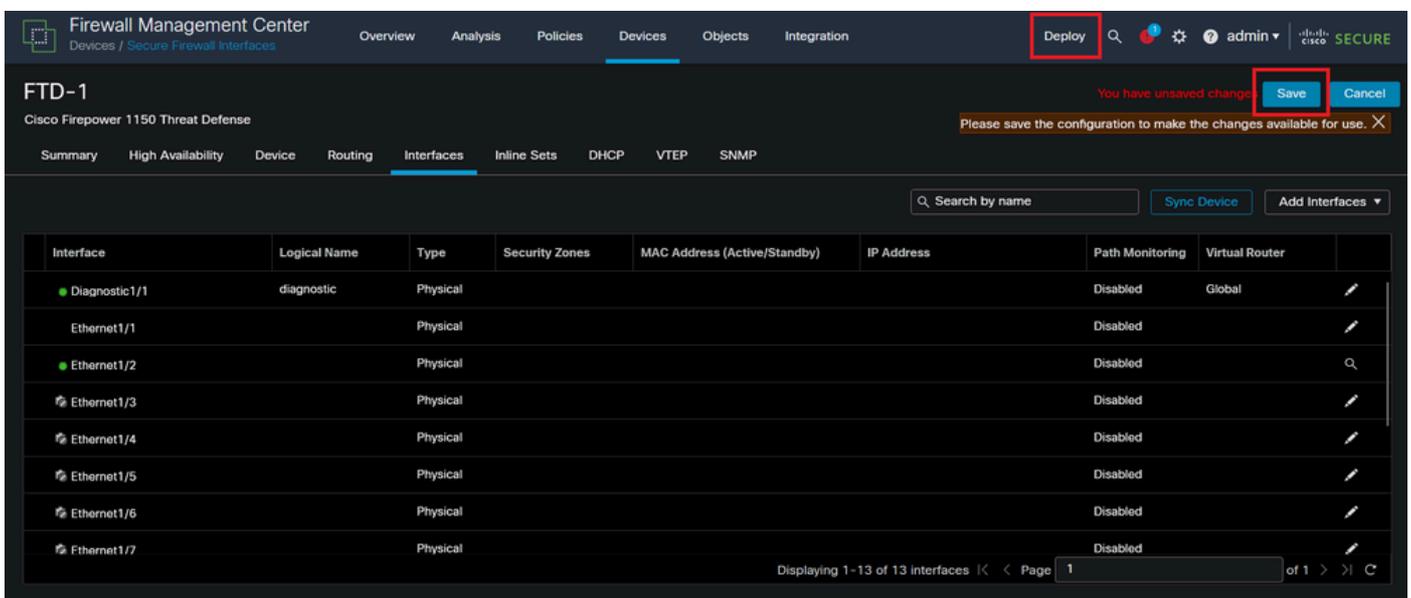
注:FTDのEther Channel IDは、スイッチのPort-Channel IDと一致する必要はありません。

ステップ 5 : IPv4タブに移動し、スイッチのVLAN 300と同じサブネット上のIPアドレスを追加します。



Ether-Channel IPアドレス

手順 6：変更を保存して展開します。



保存して展開します。

確認

ステップ 1：スイッチの観点から、VLANおよびポートチャネルインターフェイスのステータスがアップであることを確認します。

```
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
```

ステップ 2 : 両方のFTDユニットでport-channel Statusがupであることを、デバイスのコマンドラインインターフェイスにアクセスして確認します。

```
> 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***
```

ステップ 3 : スイッチSVIとFTDポートチャネルIPアドレスの間の到達可能性を確認します。

```
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 10.8.4.30, 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
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。