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		
<u>はじめに</u>		
<u>前提条件</u>		
<u>要件</u>		
<u>使用するコンポーネント</u>		
<u>設定</u>		
<u>ネットワーク図</u>		
<u>コンフィギュレーション</u>		
<u>スイッチの設定</u>		
<u>FTD HAの設定</u>		
<u>確認</u>		

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るユーザもいます。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。



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 1 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

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。

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integr	ration		Deploy	۹	0	¢	🕜 admin 🔻	cisco SECU	
			[Device N	Management		VPN		Troubleshoot					Report	
Summary Dashboard (switch dashboard)				Device U	pgrade		Site to Site		Threat Defen						
Provides a summary of activity on the appliance				NAT OoS			Dynamic Access Polic	ev .	Packet Trace	ise CLI					
Network × Threats Intrusion Events	Status Geo	olocation	OoS	Platform	Settings		Troubleshooting	cy i	Packet Capti	ire		-		-	
	000		400	FlexCont	fia		Site to Site Monitoring	a	r uskor oupti						
				Certificat	tes			- -							
Unique Applications over Time	- ×	X 🕨 1	Top Web Appli	Caucita OCCII					понсмррноа						×
No Data Last updated less than a minute ago				f an a minute ago	No Data						No I	Data			
Traffic by Application Risk Interpret/10.88.243.58.43010/ddd/#Sensort.ixt	- >	×	Top Server Ap	plications See	n		- ×	► Top O	perating Syst	terns Si	ten			-	×

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 Q 🥝 🔅 🕻	admin ▼ ^{-thtalt} SECURE
FTD-HA Cisco Firepower 1150 Threat Defense				Save
Summary High Availability Device Rout	ing Interfaces Inline Sets D	HCP VTEP SNMP		
		Q 8	earch by name Sync De	evice Add Interfaces V
Interface Logical Name	e Type Security Zones	MAC Address (Active/Standby) IP Address	Path Monitoring	Sub Interface
Diagnostic1/1 diagnostic	Physical		Disabled	Glot Virtual Tunnel Interface
Ethernet1/1	Physical		Disabled	VNI Interface
Ethernet1/2	Physical		Disabled	م
thernet1/3	Physical		Disabled	1
thernet1/4	Physical		Disabled	1
the Ethernet1/5	Physical		Disabled	1
thernet1/6	Physical		Disabled	1
🏂 Ethernet 1/7	Physical	Displaying 1-13 of 13 inte	Disabled erfaces < < 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	Channe	el Interfa	ace		
General	IPv4	IPv6	Hardware Configuration	on Path Monitoring	Advanced
Name: inside					
 Enabled Managerr Description: 	ent Only				
Mode: None			▼		
MTU:			•		
1500 (64 - 9198) Priority:					
0 Propagate Se Ether Channe	curity Gro	oup Tag:	(0 - 65535)		
					Cancel OK

Ether-Channel名

Add Ether Channel Interface						
General IPv4 IPv6 Har	dware Config	guration	Path	Monitoring	Advan	ced
MTU:						
1500						
(64 - 9198)						
Priority:						
0	(0 - 65535)					
Propagate Security Group Tag: 🧹						
Ether Channel ID *:						
1						
(1 - 48)						
Available Interfaces C		Selected Ir	nterfac	es		
Q Search		Ethernet1/	11			
Ethernet1/9	Add	Ethernet1/	12		Ì	
				l		
Ethernet1/10						
Ethernet1/11						
Ethernet1/12						
NVE Only:						
					Cancel	ОК

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。

Add Ether Channel Interface General IP 4 IP Type: Use Static IP IP Address: 10.8.4.30/24 eg. 192.0.2.1/255.255.128 or 192.0.2.1/25					
General IPv4	IPv6	Hardware Configuration	Path Monitoring	Advanced	
ІР Туре:					
Use Static IP		•			
IP Address:					
10.8.4.30/24					
eg. 192.0.2.1/255.255.255	5.128 or 192.	0.2.1/25			
				Cancel	ок

Ether-Channel IPアドレス

手順6:変更を保存して展開します。

Ę	Firewall Management Ce Devices / Secure Firewall Interfaces	onter _{Overvie}	sw Analys	sis Policies	Devices	Objects In	ntegration		Deploy	٩	e 🔹	🕜 adm	in • albal	SECURE
F] cis	TD-1 co Firepower 1150 Threat Defense Summary High Availability De	vice Routing	Interfaces	Inline Sets DHC	P VTEP	P SNMP		Please save	the config	You ha	ve unsavi to make (ed change he change	Save s available t	Cancel for use. X
								Q Search by name					Add Int	erfaces 🔻
	Interface	Logical Name	Туре	Security Zones	MAC Ad	dress (Active/Stan	ndby)	IP Address		Path Mo	onitoring	Virtual Ro	outer	
	Diagnostic1/1	diagnostic	Physical							Disable	đ	Global		1
	Ethernet1/1		Physical							Disable	d			1
	Ethernet1/2		Physical							Disable	d			۹
	12 Ethernet1/3		Physical							Disable	d			1
	12 Ethernet1/4		Physical							Disable	d			1
	12 Ethernet1/5		Physical							Disable	d			1
	12 Ethernet1/6		Physical							Disable	d			1
	12 Ethernet1/7		Physical			0			1	Disable	d			1
						Dis	splaying 1-1	3 of 13 interfaces < < Pa	396 1				of 1	2 7 C

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 10.8.4.34, 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

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。