Solution redondante intégrée pour pare-feu sécurisé et commutateur de couche 3

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configurations
Configuration du commutateur
Configuration haute disponibilité FTD
Vérifier

Introduction

Ce document décrit les meilleures pratiques pour les connexions redondantes entre les commutateurs Cisco Catalyst et les pare-feu sécurisés Cisco sur la haute disponibilité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protection pare-feu contre les menaces (FTD)
- Centre de gestion du pare-feu sécurisé (FMC)
- Cisco IOS® XE
- Système de commutation virtuel (VSS)
- Haute disponibilité (HA)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu sécurisé version 7.2.5.1
- Secure Firewall Manager Center version 7.2.5.1
- Cisco IOS XE version 16.12.08

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau

Certains utilisateurs pensent qu'une liaison de connexion unique (canal de port) entre un commutateur Catalyst logique (VSS ou empilé) vers une paire de FTD HA suffit pour avoir une solution redondante complète en cas de défaillance d'une unité ou d'une liaison. Il s'agit d'une erreur courante, car la configuration d'un VSS ou d'un commutateur empilé agit comme un périphérique logique unique. En même temps, une paire de FTD HA agit comme deux périphériques logiques différents, l'un étant actif et l'autre en veille.

Le schéma suivant est une conception non valide dans laquelle un seul Port-Channel est configuré à partir du commutateur configuré vers la paire FTD HA :



Conception non valide

La configuration précédente n'est pas valide, car ce port-channel agit comme une liaison unique connectée à deux périphériques différents, provoquant des collisions réseau. Le protocole Spanning Tree (SPT) bloque donc les connexions à partir de l'un des FTD.

Le schéma suivant est une conception valide dans laquelle deux Port-Channels différents sont configurés pour chaque membre du commutateur VSS ou de la pile.



Configurations

Configuration du commutateur

Étape 1. Configurez les canaux de port avec leur réseau local virtuel (VLAN) respectif.

```
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
1
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
```

Étape 2. Configurez une adresse IP SVI (Switched Virtual Interface) pour le VLAN Port-Channel.

```
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
```

Configuration haute disponibilité FTD

Étape 1. Connectez-vous à l'interface FMC.



Connexion FMC

Étape 2. Accédez à Périphériques > Gestion des périphériques.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analys	is Policies	Devices Objects	Integration	Deploy Q 🥝 -	û @ admin ▼ disco SECURE
Summary Dashboard (witch dashboard) Provides a summary of activity on the appliance				Device Management Device Upgrade NAT QoS	VPN Site To Site Remote Access Dynamic Access Polic	Troubleshoot File Download Threat Defense CLI cy Packet Tracer	Reporting
Network $ imes$ Threats Intrusion Events	Status	Geolocatio	n QoS	Platform Settings	Troubleshooting	Packet Capture	r 🔹 🔹 🖬
				FlexConfig Certificates	Site to Site Monitoring	1	
Unique Applications over Time		- ×	Top Web Appl	Cauona accii	- ^	и тор оненсируновного осег	
No Data				No Data		No [Pata
			Last updated less th	ian a minute ago		Last updated less than a minute ago	
 Traffic by Application Risk https://10.88.243.58.43010/ddd/#Sensort.ist 		- ×	▶ Top Server Ap	pplications Seen	- ×	 Top Operating Systems Seen 	- ×

Gestion des périphériques

Étape 3. Modifiez le périphérique haute disponibilité souhaité et accédez à Interfaces > Add Interfaces > Ether Channel Interface.

Firewall Management Ce Devices / Secure Firewall Interfaces	enter Overview Anal s	ysis Policies D	evices Objects	Integration	Deploy	९ ८ ७ ३	3 admin ▼ ^{alteris} secure
FTD-HA Cisco Firepower 1150 Threat Defense		1					Save
Summary High Availability De	vice Routing Interfaces	Inline Sets DHCP	VTEP SNMP		Q Search by name		Device Add Interfaces V
Interface	Logical Name Type	Security Zones	MAC Address (Active/S	tandby) IP Ad	dress	Path Monitoring	Vi tr Ether Channel Interface
Diagnostic1/1	diagnostic Physical					Disabled	Glot Virtual Tunnel Interface
Ethernet1/1	Physical					Disabled	VNI Interface
Ethernet1/2	Physical					Disabled	م
l Ethernet1/3	Physical					Disabled	/
S Ethernet1/4	Physical					Disabled	/
S Ethernet1/5	Physical					Disabled	/
thernet1/6	Physical					Disabled	1
Sthernet1/7	Physical			Displaying 1-13 o	f 13 interfaces I < Page 1	Disabled	of 1 > > C

Création d'EtherChannel

Étape 4. Ajoutez un nom d'interface, un ID de canal Ether et les interfaces membres.

Add Ether Channel Interface										
General	IPv4	IPv6	Hardware Configur	ation Path Monito	oring Advanced					
Name: inside V Enabled										
Description:	ient Only									
Mode:										
None			•							
Security Zone	:		•							
MTU:										
1500										
(64 - 9198)										
Priority:			(0 - 65535)							
Propagate Se Ether Channe	curity Gro	oup Tag:	(0 - 03335)							
					Cancel					

Nom Ether-Channel

Add Ether Channel Interface									
General	Pv4	IPv6	Hardware Confi	guration	Path Monite	oring Adva	nced		
MTU: 1500 (64 - 9198) Priority: 0 Propagate Secu Ether Channel II	rity Gro) *:	oup Tag:	<i>(0 - 65535)</i>						
I (1 - 48) Available Interfa Q Search Ethernet1/9 Ethernet1/10	ices	C	Add	Selected Ir Ethernet1/ Ethernet1/	nterfaces 11 12	Î Î			
Ethernet1/11 Ethernet1/12 NVE Only:									
						Cancel	ОК		

ID et membres EtherChannel



Remarque : l'ID Ether Channel sur le FTD ne doit pas nécessairement correspondre à l'ID Port Channel sur le commutateur.

Étape 5. Accédez à l'onglet IPv4 et ajoutez une adresse IP sur le même sous-réseau que le VLAN 300 pour le commutateur.

Add Ether Channel Interface									
General	Pv4	IPv6	Hardware Conf	iguration	Path Monitoring	Advanced			
IP Туре:									
Use Static IP			•						
IP Address:									
10.8.4.30/24									
eg. 192.0.2.1/255.	.255.255.	.128 or 192.	0.2.1/25						
						Cancel	ок		

Adresse IP EtherChannel

Étape 6. Enregistrez les modifications et déployez.

Firewall Management Co	enter overview	Analysis	Policies	Devices Objects	Integration	Dep	nloy Q 🧬 i	🌣 🕜 admi	in 🕶 🔤 theathe SECURE
FTD-1 Cisco Firepower 1150 Threat Defense Summary High Availability De	evice Routing In	iterfaces Ir	nline Sets DHC	p vtep snmp		Please save the c	You have uns	aved change the changes	Save Cancel s available for use. X
						Q Search by name			Add Interfaces ¥
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/	Standby) IP /	Address	Path Monitoria	g Virtual Ro	outer
Diagnostic1/1	diagnostic	Physical					Disabled	Global	1
Ethernet1/1		Physical					Disabled		1
Ethernet1/2		Physical					Disabled		٩
the Ethernet1/3		Physical					Disabled		1
thernet1/4		Physical					Disabled		/
thernet1/5		Physical					Disabled		/
le Ethernet1/6		Physical					Disabled		1
12 Ethernet1/7		Physical					Disabled		
					Displaying 1-13 of	f 13 interfaces K < Page	1		of 1 > > C

Enregistrer et déployer

Vérifier

Étape 1. Assurez-vous que l'état des interfaces VLAN et port-channel est activé du point de vue du commutateur.

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

Étape 2. Vérifiez que l'état du port-channel est up sur les deux unités FTD en accédant à l'interface de ligne de commande du périphérique.

```
> 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***
```

Étape 3. Vérifiez l'accessibilité entre l'interface SVI du commutateur et l'adresse IP FTD Port-Channel.

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.