# Integración de una solución redundante para un firewall seguro y un switch L3

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Configuraciones
Configuración del switch
Configuración de FTD HA
Verificación

# Introducción

Este documento describe una práctica recomendada para conexiones redundantes entre switches Catalyst de Cisco y firewalls seguros de Cisco en alta disponibilidad.

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protección frente a amenazas de firewall (FTD)
- Centro de gestión de firewall seguro (FMC)
- Cisco IOS® XE
- Sistema de switching virtual (VSS)
- Alta disponibilidad (HA)

## **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Firewall Threat Defence versión 7.2.5.1
- Secure Firewall Manager Center versión 7.2.5.1
- Cisco IOS XE versión 16.12.08

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configurar

## Diagrama de la red

Hay usuarios que creen que un único enlace de conexión (canal de puerto) entre un switch Catalyst lógico (VSS o apilado) y un par de FTD de HA es suficiente para tener una solución redundante completa en caso de que una unidad o un enlace falle. Se trata de un error habitual, ya que una configuración de VSS o switch apilado actúa como un único dispositivo lógico. Mientras que al mismo tiempo, un par de FTD de HA actúan como dos dispositivos lógicos diferentes con uno como activo y el otro como en espera.

El siguiente diagrama es un diseño no válido en el que se configura un solo canal de puerto desde el switch configurado hacia el par FTD HA:



Diseño no válido

La configuración anterior no es válida porque este canal de puerto actúa como un único enlace conectado a dos dispositivos diferentes, lo que provoca colisiones de red, por lo que el protocolo de árbol de extensión (SPT) bloquea las conexiones de uno de los FTD.

El siguiente diagrama es un diseño válido en el que se configuran dos Port-Channels diferentes para cada miembro del VSS o la pila del switch.



#### Configuraciones

#### Configuración del switch

Paso 1. Configure los canales de puerto con sus respectivas redes de área local virtual (VLAN).

```
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
I
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
```

Paso 2. Configure una dirección IP de interfaz virtual conmutada (SVI) para la VLAN de canal de puerto.

```
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
```

### Configuración de FTD HA

Paso 1. Inicie sesión en la GUI de FMC.



Inicio de sesión en FMC

Paso 2. Vaya a Devices > Device Management.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Inte	gration		Deploy	۹	⊘ ⊀	¢	🕑 admin 🔻	cisco SECU	
Summary Dashboard (switch.dastboard) Provides a summary of activity on the appliance				Device M Device U NAT QoS	Aanagement Jpgrade		VPN Site To Site Remote Access Dynamic Access Polic	≂y	Troubleshoot File Downlos Threat Defer Packet Trace	ad hse CLI ar				Reporti	
Network X Threats Intrusion Events	Status G	eolocation	QoS	Platform FlexConf Certificat	Settings fig tes		Troubleshooting Site to Site Monitoring	3	Packet Capt	ure		r			•
Unique Applications over Time     No Data		×	<ul> <li>Top Web Appl</li> </ul>	Kaluns Joen	No Data		- ^	Γυρια	нон Арриса	с анон	No D	vata			
Last updated less than a minute ago															
Traffic by Application Risk  https://10.88.243.58.43010/ddd/#SensorList	-	×	Top Server Ap	plications See	in		- x	► Top C	perating Sys	tems S	een			_	×

Gestión de dispositivos

Paso 3. Edite el dispositivo HA deseado y navegue hasta Interfaces > Add Interfaces > Ether Channel Interface.

Firewall Management Ce Devices / Secure Firewall Interface	enter Overview Anal s	ysis Policies De	vices Objects	Integration	Deploy	९ <b>२ 📀 🌣</b>	admin
FTD-HA Cisco Firepower 1150 Threat Defense Summary High Availability De	rvice Routing Interfaces	Inline Sets DHCP	VTEP SNMP				Save
		1			Q Search by name		Device Add Interfaces V
Interface	Logical Name Type	Security Zones	MAC Address (Active/S	tandby) IP Add	ress	Path Monitoring	Vi t Ether Channel 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	/
thernet1/4	Physical					Disabled	/
12 Ethernet1/5	Physical					Disabled	/
thernet1/6	Physical					Disabled	1
1/7 Ethernet1/7	Physical			Displaying 1-13 of	13 interfaces I < Page 1	Disabled	of 1 > >  C

Creación de Ether-Channel

Paso 4. Agregue un nombre de interfaz, un ID de canal Ether y las interfaces de miembro.

Add Ether Channel Interface											
General	IPv4	IPv6	Hardware Conf	iguration	Path Monitoring	Advanced					
Name: inside											
<ul> <li>Enabled</li> <li>Managem</li> <li>Description:</li> </ul>	nent Only										
Mode:											
Security Zone	:		• •								
MTU:											
(64 - 9198) Priority:											
0 Propagate Se Ether Channe	curity Gro	oup Tag: 🛔	(0 - 65535)								
						Cancel	ОК				

Nombre de canal Ethernet

Add Ether Channel Interface										
General IPv4	IPv6	Hardware Confi	guration	Path N	lonitoring	Advanc	ed			
MTU: 1500										
(64 - 9798) Priority:										
0		(0 - 65535)								
Propagate Security G	roup Tag: 🔽	]								
Ether Channel ID *:										
1										
(1 - 48)										
Available Interfaces	C		Selected Ir	nterface	s					
Q Search			Ethernet1/	11						
Ethernet1/9		Add	Ethernet1/	12		Ī				
Ethernet1/10										
Ethernet1/11										
Ethernet1/12										
NVE Only:										
						Cancel	ОК			

ID y miembros de Ether-Channel



Nota: El ID de canal Ether en el FTD no necesita coincidir con el ID de canal de puerto en el switch.

Paso 5. Vaya a la pestaña IPv4 y agregue una dirección IP en la misma subred que la VLAN 300 para el switch.

Add Ether Channel Interface											
General	IPv4	IPv6	Hardware Config	juration	Path Monitoring	Advanced					
IP Туре:		•									
Use Static	IP		-								
IP Address:											
10.8.4.30/2	24										
eg. 192.0.2.1/2	255.255.255	5.128 or 192	.0.2.1/25								
						Cancel	ОК				

Dirección IP de Ether-Channel

## Paso 6. Guarde los cambios e impleméntelo.

Firewall Management C Devices / Secure Firewall Interface	enter Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹	¢ 🎙	🕜 admir	1 ▼   -iliali cisco	SECURE
FTD-1 Cisco Firepower 1150 Threat Defense Summary High Availability D	evice Routing Int	terfaces In	nline Sets DHC	CP VTEF	P SNMP			Please save	e the config	You hav	e unsave o make ti	d change he changes	Save available f	Cancel for use. X
								୍ Search by nam	8				Add Inte	erfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC Ad	idress (Active/S	tandby)	IP Addre	55		Path Mo	nitoring	Virtual Ro	ıter	
Diagnostic1/1	diagnostic F	Physical								Disabled		Global		1
Ethernet1/1	1	Physical								Disabled				1
Ethernet1/2	1	Physical								Disabled				٩
thernet1/3	1	Physical								Disabled				1
thernet1/4	1	Physical								Disabled				1
thernet1/5	1	Physical								Disabled				1
thernet1/6		Physical								Disabled				1
Ethernet1/7	1	Physical				Dission	10 - ( 12 -	1	<b>1</b>	Disabled				1
						Displaying 1-1	13 of 13 ir	nternaces I < < F	age				of 1	

Guardar e implementar

# Verificación

Paso 1. Asegúrese de que el Estado de las interfaces VLAN y de canal de puerto esté activo desde la perspectiva del 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

Paso 2. Verifique que el Estado del canal de puerto esté activo en ambas unidades FTD accediendo a la interfaz de línea de comandos 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***
```

Paso 3. Compruebe la disponibilidad entre la SVI del switch y la dirección IP del canal de puerto 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

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).