Integrar solução redundante para firewall seguro e switch L3

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Diagrama de Rede
Configurações
Configuração do Switch
Configuração HA de FTD
Verificar

Introdução

Este documento descreve uma prática recomendada para conexões redundantes entre Cisco Catalyst Switches e Cisco Secure Firewalls em alta disponibilidade.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças de firewall (FTD) segura
- Centro de gerenciamento seguro de firewall (FMC)
- Cisco IOS® XE
- Sistema de switching virtual (VSS)
- Alta disponibilidade (HA)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

Há usuários que acreditam que um único link de conexão (canal de porta) entre um Switch Catalyst lógico (VSS ou Empilhado) em direção a um par de FTDs HA é suficiente para ter uma solução totalmente redundante em caso de falha de uma unidade ou link. Essa é uma concepção equivocada comum, pois uma configuração de VSS ou de switch empilhado atua como um único dispositivo lógico. Ao mesmo tempo, um par de FTDs HA atua como dois dispositivos lógicos diferentes, sendo um como ativo e o outro como em standby.

O próximo diagrama é um projeto inválido no qual um único canal de porta é configurado a partir do Switch configurado em direção ao par FTD HA:



Design inválido

A configuração anterior não é válida porque esse canal de porta atua como um único link conectado a dois dispositivos diferentes, causando colisões na rede, de modo que o Spanning Tree Protocol (SPT) bloqueia conexões de um dos FTDs.

O próximo diagrama é um projeto válido no qual dois canais de porta diferentes são configurados para cada membro do Switch VSS ou da Pilha.



Configurações

Configuração do Switch

Etapa 1. Configure os canais de porta com suas respectivas VLANs (Virtual Local Area Network, rede local virtual).

```
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
```

Etapa 2. Configure um endereço IP de SVI (Switched Virtual Interface) para a VLAN de canal de porta.

```
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
```

Configuração HA de FTD

Etapa 1. Faça login na GUI do FMC.



Logon no FMC

Etapa 2. Navegue até Devices > Device Management.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integ	gration		Deploy	۹	0	¢	📀 admin 🔻	cisco SECUR	RE
Summary Dashboard (wetch.dashboard) Provides a summary of activity on the appliance				Device M Device U NAT QoS	Management Jpgrade		VPN Site To Site Remote Access Dynamic Access Polie	icy	Troubleshoot File Downloa Threat Defen Packet Trace	d se CLI r				Reportin	
Network $ imes$ Threats Intrusion Events	Status Geo	olocation	QoS	Platform	Settings		Troubleshooting		Packet Captu	ire		r			п
				FlexCon Certifica	fig tes		Site to Site Monitorin	g							
 Unique Applications over Time No Data 	->	× • T	op Web Appl	licauons ocen	No Data				αστι Αγγικαι	010	No	Data		->	×
Traffic by Application Risk https://10.88.243.58.43010/ddd/#SensorList	- >	× • T	op Server Ap	plications See	in		- ×	► Top C	Operating Syst	ems S	een			->	×

Gerenciamento de dispositivos

Etapa 3. Edite o dispositivo HA desejado e navegue até Interfaces > Add Interfaces > Ether Channel Interface.

Firewall Management Ce Devices / Secure Firewall Interfaces	enter Overview Anal	ysis Policies D	evices Objects In	tegration	Deploy Q 🥝 🛟	admin ▼ distant secure secure
FTD-HA Cisco Firepower 1150 Threat Defense		•				Save
Summary High Availability Dev	vice Routing Interfaces	Inline Sets DHCP	VTEP SNMP	Q. Search by	name Sync	Device Add Interfaces V
Interface	Logical Name Type	Security Zones	MAC Address (Active/Stand	dby) IP Address	Path Monitoring	Sub Interface VI t. Ether Channel Interface Bridge Group Interface
Diagnostic1/1	diagnostic Physical				Disabled	Glot Virtual Tunnel Interface
Ethernet1/1	Physical				Disabled	vivi intenace
Ethernet1/2	Physical				Disabled	م
thernet1/3	Physical				Disabled	/
to Ethernet1/4	Physical				Disabled	/
thernet1/5	Physical				Disabled	/
Ethernet1/6	Physical				Disabled	/
🕼 Ethernet1/7	Physical		l	Displaying 1-13 of 13 interfaces	Disabled	of 1 > > ℃

Criação de Ether-Channel

Etapa 4. Adicione um nome de interface, ID do Canal Ether e as interfaces do membro.

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

Nome do Ether-Channel

Add Ether Chanr	nel Interfac	e					
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 e membros do Ether-Channel



Observação: o ID do Ether Channel no FTD não precisa corresponder ao ID do Port-Channel no Switch.

Etapa 5. Navegue até a guia IPv4 e adicione um endereço IP na mesma sub-rede que a VLAN 300 para o Switch.

Add Ether Channel Interface										
General	IPv4	IPv6	Hardware Conf	iguration	Path Monitoring	Advanced				
IP Type:										
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	OK			

Endereço IP do Ether-Channel

Etapa 6. Salve as alterações e Implante.

Firewall Management Ce Devices / Secure Firewall Interfaces	enter _{Overview}	Analysis Policies	Devices Objects Integration	Deplo	w Q 🧬 🌣 🕜	admin 🕶 🔤 👬 🕯 secure
FTD-1 Cisco Firepower 1150 Threat Defense Summary High Availability De	vice Routing Interfa	es Inline Sets DHK	CP VTEP SNMP	Please save the cor	You have unsaved cha nfiguration to make the ch	nge Save Cancel anges available for use. X
				Q Search by name		Add Interfaces V
Interface	Logical Name Typ	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring Virt	ual Router
Diagnostic1/1	diagnostic Phys	al			Disabled Glob	oal 🖍
Ethernet1/1	Phys	al			Disabled	1
Ethernet1/2	Phys	al			Disabled	٩
to Ethernet1/3	Phys	al			Disabled	1
l Ethernet1/4	Phys	al			Disabled	/
l Ethernet1/5	Phys	al			Disabled	/
likernet1/6	Phys	al			Disabled	1
Ethernet1/7	Phys	al	Displaying 1	12 of 12 interfaces 1/ / Page 1	Disabled	
			Displaying 1-	ris of its interfaces it it page		

Salvar e implantar

Verificar

Etapa 1. Certifique-se de que o Status das interfaces VLAN e port-channel esteja ativo da perspectiva do 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

Etapa 2. Verifique se port-channel Status está ativado em ambas as unidades de FTD acessando a interface de linha de comando do 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***
```

Etapa 3. Verifique a acessibilidade entre o Switch SVI e o endereço IP do canal de porta 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.