集成安全防火墙和L3交换机的冗余解决方案

目录

<u>前介</u>	
使用的组件	
<u>网络图</u>	
<u>交换机配置</u>	
FTD HA配置	
<u>à ùr</u>	

简介

本文档介绍Cisco Catalyst交换机和Cisco安全防火墙之间高可用性冗余连接的最佳实践。

先决条件

要求

Cisco 建议您了解以下主题:

- 安全防火墙威胁防御(FTD)
- 安全防火墙管理中心(FMC)
- 思科IOS® XE
- 虚拟交换系统(VSS)
- 高可用性(HA)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 安全防火墙威胁防御7.2.5.1版
- 安全防火墙管理器中心版本7.2.5.1
- 思科IOS XE版本16.12.08

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

网络图

有些用户认为,一个逻辑Catalyst交换机(VSS或堆叠)之间指向一对高可用性FTD的单个连接链路 (端口通道)足以在一个设备或链路发生故障时提供完整的冗余解决方案。这是一个常见的误解 ,因为VSS或堆叠交换机设置用作单个逻辑设备。同时,一对HA FTD充当两个不同的逻辑设备 ,其中一个作为主用,另一个作为备用。



下图是一个无效设计,其中从设置的交换机到FTD HA对配置了一个端口通道:

无效设计

之前的配置无效,因为此端口通道充当连接到两个不同设备的单个链路,从而导致网络冲突,因此 生成树协议(SPT)会阻止来自其中一个FTD的连接。

下图是一个有效的设计,其中为交换机VSS或堆栈的每个成员配置两个不同的端口通道。



有效设计

配置

交换机配置

步骤1:使用各自的虚拟局域网(VLAN)配置端口通道。

```
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 1 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

第二步:为端口通道VLAN配置交换虚拟接口(SVI) IP地址。

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配置

步骤1:登录FMC GUI。



FMC登录

第二步:导航到设备>设备管理。

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices Ob	ojects Ir	ntegration	Deploy Q 🌘	•	🕜 admin -	elsee SECURE
Summary Dashboard (switch.dashboard) Provides a summary of activity on the appliance				Device Manage Device Upgrad NAT QoS	ement de	VPN Site To Site Remote Access Dynamic Access Polic	Troubleshoot File Download Threat Defense CLI cy Packet Tracer			Reporting
Network × Threats Intrusion Events	Status Geo	olocation	QoS	Platform Settin	ngs	Troubleshooting	Packet Capture			• 11
				FlexConfig Certificates		Site to Site Monitoring	3			
Unique Applications over Time			Top Web Appl	Cauons acci		- ^	ир свенсирисацонь зее			
No Data				No Da	ata			No Dal	ta	
Last updated less than a minute ago										
Traffic by Application Risk https://10.88.243.5843010/ddd/#Sensort.ist	- >	×	Top Server Ap	plications Seen		- ×	 Top Operating Systems See 	n		- ×

设备管理

第三步:编辑所需的高可用性设备,并导航到Interfaces > Add Interfaces > Ether Channel Interface。

Firewall Management C Devices / Secure Firewall Interface	enter Overview An	ilysis Policies De	vices Objects Integ	ration	Deploy Q 🥝 🛟	admin ↓ ^{-1 1+1 +} SECURE
FTD-HA Cisco Firepower 1150 Threat Defense		-				Save
Summary High Availability De	evice Routing Interfaces	Inline Sets DHCP	VTEP SNMP	O Search by name		Davison
				d Search by hame		Sub Interface
Interface	Logical Name Type	Security Zones	MAC Address (Active/Standby) IP Address	Path Monitoring	Vi ti Ether Channel Interface
Diagnostic1/1	diagnostic Physical				Disabled	Glot Virtual Tunnel Interface
Ethernet1/1	Physical				Disabled	VNI Interface
Ethernet1/2	Physical				Disabled	م
le Ethernet1/3	Physical				Disabled	/
l Ethernet1/4	Physical				Disabled	/
12 Ethernet1/5	Physical				Disabled	/
thernet1/6	Physical				Disabled	/
🕼 Ethernet1/7	Physical		Dis	playing 1-13 of 13 interfaces $ \zeta \langle$	Disabled Page 1	of 1 > > ℃

Ether-Channel创建

第四步:添加接口名称、以太网通道ID和成员接口。

Add Ether	Channe	el Interfa	ace		
General	IPv4	IPv6	Hardware Configuration	Path Monitoring	Advanced
Name:					
inside					
🗸 Enabled					
Managem	ent Only				
Description:					
Mode:					
None			▼		
Security Zone	:				
			•		
MTU:					
1500					
(64 - 9198)					
Priority:					
0			(0 - 65535)		
Propagate Se	curity Gro	oup Tag:	V		
Ether Channe	I ID *:				
					Cancel

Ether-Channel名称

Add Ether (Channe	el Interfa	ice				
General	IPv4	IPv6	Hardware Confi	guration	Path Monit	oring Adva	nced
MTU: 1500 (64 - 9198) Priority: 0 Propagate Sec Ether Channel	curity Gr	oup Tag:	(0 - 65535) <				
1 (1 - 48) Available Inter	faces	С		Selected Ir	nterfaces		1
Q Search Ethernet1/9			Add	Ethernet1/ Ethernet1/	11 12	Ĩ	
Ethernet1/10 Ethernet1/11 Ethernet1/12							
NVE Only:							
						Cancel	ОК

Ether-Channel ID和成员



注意:FTD上的EtherChannel ID不需要与交换机上的Port-Channel ID匹配。

第五步:导航到IPv4选项卡,然后在与交换机的VLAN 300相同的子网中添加IP地址。

Add Ether Channel Interface											
General IPv4	IPv6	Hardware Configuration	Path Monitoring	Advanced							
ІР Туре:											
Use Static IP		v									
IP Address:											
10.8.4.30/24											
eg. 192.0.2.1/255.255.25	5.128 or 192.	0.2.1/25									
				Cancel	ок						

Ether-Channel IP地址

第六步:保存更改并部署。

Firewall Management Ce Devices / Secure Firewall Interface	enter ^S	w Analys	is Policies	Devices	Objects	Integration		Deploy Q	🤣 🔅	🕐 admir	n 🔻 🔤 dhalta cisco	SECURE
FTD-1 Cisco Firepower 1150 Threat Defense							Please save	You the configuration	nave unsav In to make	ed change the changes	Save available fe	Cancel or use. X
Summary High Availability De	vice Routing I	Interfaces	Inline Sets DI	HCP VTEP	P SNMP							
							Q Search by name				Add Inte	rfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC A	ddress (Active/S	itandby)	IP Address	Path	Monitoring	Virtual Ro	uter	
Diagnostic1/1	diagnostic	Physical						Disat	led	Global		1
Ethernet1/1		Physical						Disab	led			1
Ethernet1/2		Physical						Disab	led			٩
r Ethernet1/3		Physical						Disab	led			1
thernet1/4		Physical						Disab	led			/
r Ethernet1/5		Physical						Disab	led			1
thernet1/6		Physical						Disab	led			1
Ethernet1/7		Physical						Disab	led			1
						Displaying 1-	13 of 13 interfaces < < Pa	ge 1			of 1 >	×с

保存并部署

验证

步骤1:确保VLAN和端口信道接口的状态从交换机的角度为up。

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

第二步:通过访问设备命令行界面,检查两个FTD单元上的端口信道状态是否均为up。

> 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***

第三步:检查交换机SVI和FTD端口通道IP地址之间的可接通性。

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。