Secure Firewall 및 L3 Switch를 위한 이중 솔루션 통합

목차

<u>소개</u>

<u>사전 요구 사항</u>

<u>요구 사항</u>

<u>사용되는 구성 요소</u>

<u>구성</u>

<u>네트워크 다이어그램</u>

<u>설정</u>

<u>스위치 구성</u> <u>FTD HA 컨피그레이션</u>

<u>다음을 확인합니다.</u>

소개

이 문서에서는 고가용성을 지원하는 Cisco Catalyst 스위치와 Cisco Secure Firewall 간의 중복 연결 을 위한 모범 사례에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(보안 방화벽 위협 방어)
- FMC(Secure Firewall Management Center)
- Cisco IOS® XE
- VSS(Virtual Switching System)
- 고가용성(HA)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램

한 쌍의 HA FTD를 향하는 하나의 논리적 Catalyst Switch(VSS 또는 Stacked) 간의 단일 연결 링크 (포트 채널)가 하나의 유닛 또는 링크에 장애가 발생할 경우 완전한 이중화 솔루션으로 충분하다고 생각하는 사용자가 있습니다. VSS 또는 스태킹된 스위치 설정이 단일 논리적 디바이스로 작동하기 때문에 이는 일반적인 오해입니다. 동시에 한 쌍의 HA FTD는 서로 다른 두 개의 논리적 디바이스로 작동하며, 하나는 Active로 다른 하나는 Standby로 작동합니다.

다음 다이어그램은 FTD HA 쌍으로 설정된 스위치에서 단일 포트 채널이 구성되는 잘못된 설계입 니다.



잘못된 디자인

이 포트 채널이 서로 다른 두 디바이스에 연결된 단일 링크 역할을 하여 네트워크 충돌을 일으키므 로 SPT(Spanning Tree Protocol)는 FTD 중 하나로부터의 연결을 차단하므로 이전 컨피그레이션이 유효하지 않습니다.

다음 다이어그램은 Switch VSS 또는 Stack의 각 멤버에 대해 서로 다른 두 개의 포트 채널을 구성 하는 유효한 설계입니다.



유효한 설계

스위치 구성

1단계. 각각의 VLAN(Virtual Local Area Network)으로 포트 채널을 구성합니다.

```
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
I
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
```

2단계. 포트 채널 VLAN에 대한 SVI(Switched Virtual Interface) IP 주소를 구성합니다.

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 컨피그레이션

1단계. FMC GUI에 로그인합니다.





2단계. Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysi	s Policies	Devices Objects	Integration	Deploy Q 🥏	☆ ③ admin ▼ disco SECURE
Summary Dashboard (swetch: 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	Geolocation	n QoS	Platform Settings FlexConfig	Troubleshooting Site to Site Monitoring	Packet Capture	r • II
Unique Applications over Time		- ×	 Top Web Appl 	Certificates	- ^	и тор спонтирисацона зоон	
No Data				No Data		No I	Data
Last updated less than a minute ago							
Traffic by Application Risk http://10.88.243.5843010/ddd/#SensorList		- ×	Top Server Ap	plications Seen		 Top Operating Systems Seen 	

장치 관리

3단계. 원하는 HA 디바이스를 편집하고 Interfaces(인터페이스) > Add Interfaces(인터페이스 추가) > Ether Channel Interface(이더넷 채널 인터페이스)로 이동합니다.

Firewall Management Ce Devices / Secure Firewall Interfaces	enter Overview Anal	ysis Policies D	evices Objects	Integration	Deploy	९ 📀 🔅	admin ▼
FTD-HA Cisco Firepower 1150 Threat Defense Summary High Availability Der	vice Routing Interfaces	Inline Sets DHCP	VTEP SNMP				Save Cancel
		J			Q. Search by name		Device Add Interfaces
Interface	Logical Name Type	Security Zones	MAC Address (Active/	Standby) IP Addr	ess	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
thernet1/3	Physical					Disabled	/
SEthernet1/4	Physical					Disabled	/
12 Ethernet1/5	Physical					Disabled	1
thernet1/6	Physical					Disabled	/
f Ethernet1/7	Physical			Displaying 1-13 of	13 interfaces I < Page 1	Disabled	of 1 > > C

이더 채널 생성

4단계. 인터페이스 이름, Ether Channel ID 및 멤버 인터페이스를 추가합니다.

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

Ether-Channel 이름

Add Ether Cha	annel Inte	erface						
General IP	v4 IPv6	6 Hard	ware Config	juration	Path M	Monitoring	Advar	nced
MTU: 1500 (64 - 9198) Priority: 0 Propagate Securit Ether Channel ID	ty Group Ta *:	g: 🗹	(0 - 65535)					
1								
Available Interface	es C			Selected Ir	nterface	es		
Q Search				Ethernet1/	11		Ì	
Ethernet1/9			Add	Ethernet1/	12		Ì	
Ethernet1/10								
Ethernet1/11								
Ethernet1/12								
NVE Only:								
							Cancel	ОК

Ether-Channel ID 및 멤버



참고: FTD의 Ether Channel ID는 스위치의 Port-Channel ID와 일치하지 않아도 됩니다.

5단계. IPv4 탭으로 이동하여 스위치의 VLAN 300과 동일한 서브넷에 IP 주소를 추가합니다.

1단계. VLAN 및 포트 채널 인터페이스의 상태가 스위치의 관점에서 작동 중인지 확인합니다.

다음을 확인합니다.

저장 및 배포

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis	Policies Devices Objects	Integration	Deploy Q 🧬 🛱	Ø admin ▼
FTD-1 Cisco Firepower 1150 Threat Defense			Please :	You have unsaver	t change Save Cancel the changes available for use. X
Summary High Availability Device R	touting Interfaces Inline S	ets DHCP VTEP SNMP	Q. Search by n	ame Sync	Device Add Interfaces •
Interface Logical N	ame Type Secur	ity Zones MAC Address (Activ	e/Standby) IP Address	Path Monitoring	Virtual Router
Diagnostic1/1 diagnostic	Physical			Disabled	(1004) /
Ethernet1/2 Ethernet1/3	Physical			Disabled	4
Sethernet1/5	Physical			Disabled	1
S Ethernet1/7	Physical		Displaying 1-13 of 13 interfaces	Disabled Disabled Vage 1	of 1 > > C

6단계. 변경 사항을 저장하고 구축합니다.

Ether-Channel IP 주소

Add Ether Channel Interface							
General	IPv4	IPv6	Hardware Configuration	Path Monitoring	Advanced		
IP Туре:							
Use Statio	: IP		•				
IP Address: 10.8.4.30 eg. 192.0.2.1	/24 /255.255.255	.128 or 192.(0.2.1/25				
					Cancel	ĸ	

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

2단계. 디바이스 명령줄 인터페이스에 액세스하여 포트 채널 상태가 두 FTD 유닛 모두에서 가동 중 인지 확인합니다.

> 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***

3단계. 스위치 SVI와 FTD 포트 채널 IP 주소 간의 연결성을 확인합니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.