# Geïntegreerde redundante oplossing voor beveiligde firewall en L3 Switch

# Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Configureren
Netwerkdiagram
Configuraties
Switchconfiguratie
FTD HA-configuratie
Verifiëren

# Inleiding

Dit document beschrijft een best practice voor redundante verbindingen tussen Cisco Catalyst Switches en Cisco Secure Firewalls op hoge beschikbaarheid.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall Threat Defence (FTD)
- Secure Firewall Management Center (FMC)
- Cisco IOS® XE
- Virtueel switchingsysteem (VSS)
- Hoge beschikbaarheid (HA)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Configureren

## Netwerkdiagram

Er zijn gebruikers die geloven dat één enkele verbinding (poortkanaal) tussen één logische Catalyst Switch (VSS of Stacked) naar een paar HA FTD's voldoende is om een volledige redundante oplossing te hebben voor het geval dat één unit of link uitvalt. Dit is een veel voorkomend misverstand omdat een VSS of stapelbare Switch als één logisch toestel fungeert. Tegelijkertijd fungeren twee HA FTD's als twee verschillende logische apparaten met de ene als Active en de andere als Standby.

Het volgende diagram is een ongeldig ontwerp waarin één poortkanaal is geconfigureerd vanaf de Switch die is ingesteld voor het FTD HA-paar:



Ongeldig ontwerp

De vorige configuratie is niet geldig omdat dit poortkanaal fungeert als één link die is aangesloten op twee verschillende apparaten, waardoor netwerkbotsingen worden veroorzaakt. Daarom blokkeert het Spanning Tree Protocol (SPT) verbindingen van een van de FTD's.

Het volgende diagram is een geldig ontwerp waarin twee verschillende poortkanalen zijn geconfigureerd voor elk lid van de Switch VSS of Stack.



### Configuraties

#### Switchconfiguratie

Stap 1. Configureer poortkanalen met hun respectievelijke Virtual Local Area Network (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
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
```

Stap 2. Configureer een Switched Virtual Interface (SVI) IP-adres voor het poortkanaal VLAN.

```
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-configuratie

Stap 1. Log in op de GUI van het VCC.



Inloggen bij VCC

#### Stap 2. Navigeer naar Apparaten > Apparaatbeheer.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices Ot	bjects Ir	ntegration	Deploy Q	•	🕑 admin 🕇	cisco SECURE
Summary Dashboard (switch disatilitioard) Provides a summary of activity on the appliance				Device Manag Device Upgrad NAT QoS	jement de	VPN Site To Site Remote Access Dynamic Access Policy	Troubleshoot File Download Threat Defense CLI Packet Tracer			Reporting
Network × Threats Intrusion Events	Status G	ieolocation	QoS	Platform Settir FlexConfig Certificates	ngs	Troubleshooting Site to Site Monitoring	Packet Capture			Add Widgets
<ul> <li>Unique Applications over Time</li> <li>No Data</li> </ul>			Top Web Appl	No Da	ata		r - Top Chichi Paphicalonia Jen	No Da	ta	
Last updated less than a minute ago										
Traffic by Application Risk     https://10.88.243.58.43010/ddd/#SensorList	-	• × •	Top Server Ap	plications Seen		- ×	<ul> <li>Top Operating Systems Se</li> </ul>	en		- ×

Apparaatbeheer

Stap 3. Bewerk het gewenste HA-apparaat en navigeer naar Interfaces > Add Interfaces > Ether Channel Interface.

Firewall Management Ce Devices / Secure Firewall Interface	enter <sub>Overview</sub> Anal s	ysis Policies D	evices Objects I	Integration	Deploy Q 🥝 🛱	admin      ↓ <sup>-thalt</sup> secure     SECURE
FTD-HA Cisco Firepower 1150 Threat Defense			V770 0140			Save Cancel
Sumimary nign Availability De	nice Routing interfaces	inline sets DHCP		Q Search	a by name Sync	Device Add Interfaces V
Interface	Logical Name Type	Security Zones	MAC Address (Active/Sta	indby) 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
SEthernet1/3	Physical				Disabled	/
Sethernet1/4	Physical				Disabled	1
SEthernet1/5	Physical				Disabled	/
le Ethernet1/6	Physical				Disabled	1
f Ethernet1/7	Physical			Displaying 1-13 of 13 interface	Disabled es I< < Page 1	of 1 > >  C

Creatie van Ether-kanaal

Stap 4. Voeg een interfacenaam, Ether Channel-id en de lidinterfaces toe.

Add Ether	Channe	l Interfa	ce				
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

Naam EtherChannel

Add Ether Ch	anne	l Interfac	ce					
General IP	v4	IPv6	Hardware Confi	guration	Path M	Monitoring	Advand	ced
MTU: 1500								
(64 - 9198)								
Priority:								
0			(0 - 65535)					
Propagate Securi	ity Gro	up Tag: 🧹	4					
Ether Channel ID	*:							
1								
(1 - 48)								
Available Interfac	es (	<b>7</b> )	1	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 en leden



Opmerking: de Ether Channel-id op de FTD hoeft niet overeen te komen met de Port-Channel-id op de Switch.

Stap 5. Navigeer naar het tabblad IPv4 en voeg een IP-adres toe op hetzelfde subnetje als VLAN 300 voor de Switch.

Add Ether Channel Interface											
General IPv4	IPv6	Hardware Configuration	Path Monitoring	Advanced							
ІР Туре:											
Use Static IP		<b>v</b>									
IP Address:											
10.8.4.30/24											
eg. 192.0.2.1/255.255.255	5.128 or 192	.0.2.1/25									
				Cancel	K						

Ether-Channel IP-adres

## Stap 6. Sla de wijzigingen op en implementeer.

Firewall Management Ce Devices / Secure Firewall Interfaces	overview	Analysis	· Policies	Devices	Objects	Integration		Deploy	۹	¢	🕜 admi	n <del>v</del>   aladi cisco	SECURE
FTD-1 Cisco Firepower 1150 Threat Defense Summary High Availability De	vice Routing In	terfaces li	nline Sets DHC	P VTEP	SNMP		Please save t	the configu	You hav	e unsave to make ti	d change he changes	Save available f	Cancel or use. X
							Q Search by name					Add Inte	erfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC Ad	dress (Active/Sta	andby)	IP Address	F	Path Mo	nitoring	Virtual Ro	uter	
Diagnostic1/1	diagnostic	Physical						ſ	Disabled		Global		1
Ethernet1/1		Physical						ſ	Disabled				1
Ethernet1/2		Physical						ι	Disabled				۹
Ethernet1/3		Physical						ſ	Disabled				1
SEthernet1/4		Physical						c	Disabled				1
r Ethernet1/5		Physical						c	Disabled				1
Ethernet1/6		Physical						C	Disabled				1
S Ethernet1/7		Physical							Disabled				1
					0	isplaying 1-1	13 of 13 interfaces   < < Pa	ge 1				of 1 >	> c

Opslaan en implementeren

# Verifiëren

Stap 1. Zorg ervoor dat de status van de VLAN- en poortkanaals interfaces omhoog is vanuit het perspectief van de 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

Stap 2. Controleer of de poortkanaal-status op beide FTD-eenheden is ingesteld door toegang te krijgen tot de interface van de apparaatopdrachtregel.

```
> 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***
```

Stap 3. Controleer de bereikbaarheid tussen de Switch SVI en het FTD Port-Channel IP-adres.

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

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.