FTD Multi-Instance High-Availability instellen op Firepower 4100

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie **Netwerkdiagram Configuraties** Stap 1. Interfaces vooraf configureren Stap 2. Voeg 2 resourceprofielen toe voor containerinstanties. Stap 3. (Optioneel) Voeg een MAC Pool Prefix van virtueel MAC-adres toe voor Container Instance Interfaces. Stap 4. Voeg een standalone instantie toe. Stap 5. Interfaces configureren Stap 6. Voeg een hoog beschikbaarheidspaar toe voor elke instantie. Verifiëren Problemen oplossen Referentie

Inleiding

Dit document beschrijft hoe u failover kunt configureren in FTD-containerinstanties (Multi-Instance).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Firepower Management Center en Firewall Threat Defence.

Gebruikte componenten

Cisco Firepower Management Center Virtual 7.2.5 Cisco FirePOWER 4145 NGFW-applicatie (FTD) 7.2.5 Firepower eXtensible Operating System (FXOS) 2.12 (0.498) Windows 10 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.

Alvorens FTD Multi-Instance te implementeren, is het belangrijk om te begrijpen hoe het uw systeemprestaties kan beïnvloeden en dienovereenkomstig te plannen. Raadpleeg altijd de officiële documentatie van Cisco of neem contact op met een technische vertegenwoordiger van Cisco om een optimale implementatie en configuratie te garanderen.

Achtergrondinformatie

Multi-Instance is een functie van Firepower Threat Defence (FTD) die vergelijkbaar is met ASA multiple context mode. Het stelt u in staat om meerdere, aparte container Instanties van FTD op een enkel stuk hardware uit te voeren. Elke container instantie staat harde middelenscheiding, afzonderlijk configuratiebeheer, afzonderlijke herladingen, afzonderlijke software-updates, en volledige ondersteuning van bedreigingsverdediging. Dit is met name nuttig voor organisaties die verschillende beveiligingsmaatregelen voor verschillende afdelingen of projecten nodig hebben, maar niet willen investeren in meerdere afzonderlijke hardwareapparatuur. De Multi-Instance optie wordt momenteel ondersteund op het FirePOWER 4100 en 9300 Series security apparaat waarop FTD 6.4 en hoger wordt uitgevoerd.

Dit document gebruikt Firepower4145 die maximaal 14 Container-instanties ondersteunt. Raadpleeg voor de maximale aantal instanties die in FirePOWER-applicatie worden ondersteund <u>Maximum aantal containerinstanties en -bronnen per model.</u>

Netwerkdiagram

Dit document introduceert de configuratie en verificatie voor HA in Multi-Instance op dit diagram.



Logisch configuratiediagram



Diagram van fysieke configuratie

Configuraties

Stap 1. Interfaces vooraf configureren

a. Navigeren naar interfaces op FCM. Set 2 beheerinterfaces. In dit voorbeeld Ethernet1/3 en Ethernet1/7.

Overview Inte	erfaces Logical Devices	Security Engine	Platform Settings						Syster	n Tools Help	admin
			Network Module 1	5 7	Network Module 2 :	Empty	Network Module 3 : Em	pty			
An Interfaces	taroware bypass								Add Nes	N - Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
MGMT	Management										
Port-channel48	8 cluster	10gbps	indeterminate			Full Duplex	no	admin-down	(IX)	6	
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up	\frown	0	
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up		0	

Interfaces vooraf configureren

Stap 2. Voeg 2 resourceprofielen toe voor containerinstanties.

a. Navigeer naar Platform Instellingen > Resource Profiles > Add on FCM. Stel 1e resourceprofiel in.

In dit voorbeeld : ·Naam: Instance01 ·Aantal kernen: 10



Opmerking: voor HA van het containerinstantiepaar moeten ze dezelfde eigenschappen van het resourceprofiel gebruiken.

Stel de naam van het profiel in tussen 1 en 64 tekens. Merk op dat u de naam van dit profiel niet kunt wijzigen nadat u het hebt toegevoegd.

Stel het aantal kernen voor het profiel in, tussen de 6 en het maximum.

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH				O Add	
SNMP	Name	Description	Cores		
HTTPS AAA Syslog DNS FIPS and Common Criteria	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	<i>2</i> 3	
Access List		Add Resource Profile			
MAC Pool Resource Profiles		Name: * Instance01			
Network Control Policy Chassis URL		Description: Number of Cores:* 10 Range: 6 to 86 Specify even value for number of cores.			
		OK. Cancel			

1e resourceprofiel toevoegen

b. Herhaal a. in stap 2 om het tweede resourceprofiel te configureren.

In dit voorbeeld : ·Naam : instantie02 ·Aantal kernen: 20

Overview Interfaces Log	cal Devices Security Engine	Platform Settings	·		System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	Ø 🕄	
Syslog	Instance01		10	/ 6	
DNS					
FIPS and Common Criteria		Add Dessures Desfile			
Access List		Add Resource Profile			
MAC Pool		Name:* Instance02			
Resource Profiles					
Network Control Policy		Description:			
Chassis URL		Number of Cores:* 20 Range: 6 to 86			
		O Specify even value for number of cores.			
		OK			

2e resourceprofiel toevoegen

c. Controleer of er twee resourceprofielen zijn toegevoegd.

Oven	view Interfaces Log	ical Devices Security Engine	Platform Settings				System Tools Help a	admin
NTP	• •					0 MI		
SNN	1 MP	Name		Description	Cores			
AAA	'PS	Default-Small		Auto-created application resource-profile with 6 cp	u-cores 6	/ 6		
Sys	log	Instance01			10	<i>🖉</i> 🗐		
FIP	s S and Common Criteria	Instance02			20	<i>~</i> 1		
Acc MAG	ess List C Pool							
 Res 	source Profiles							
Cha	work Control Policy Issis URL							

Resourceprofiel bevestigen

Stap 3. (Optioneel)Voeg een MAC Pool Prefix van virtueel MAC-adres toe voor Container Instance Interfaces.

U kunt het virtuele MAC-adres voor de Active/Stanby-interface handmatig instellen. Als de Virtuele Adressen van MAC niet, voor multi-instantie vermogen worden geplaatst, produceert het chassis automatisch de adressen van MAC voor de interfaces van de Instantie, en garandeert dat een gedeelde interface in elke Instantie een uniek adres van MAC gebruikt.

Contr. <u>Een MAC Pool Prefix toevoegen en MAC-adressen bekijken voor Container Instance</u> <u>Interfaces</u> voor meer details over MAC-adres.

Stap 4. Voeg een standalone instantie toe.

a. Navigeer naar logische apparaten > Standalone toevoegen. Eerste instantie instellen.

In dit voorbeeld : ·Apparaatnaam : FTD01

·Type instantie: container



Opmerking: de enige manier om een containerapplicatie te implementeren is door een App-Instance vooraf te implementeren met Instance Type ingesteld op Container. Verzeker u ervan dat u Container selecteert.

U kunt deze naam niet wijzigen nadat u het logische apparaat hebt toegevoegd.

Overview Interfaces Logical Devices Security Engine	Platform Settings			System Tools He	lp admin
Logical Device List	(0 instances) 100% (86 of 86) Core	is Available		C Refresh	Add •
No logical devices available. Click on Add Device to add a new logical device.					
	Add Standalone		(?)×		
	Device Name:	FTD01			
	Template:	Cisco Secure Firewall Threat Defense	~		
	Image Version:	7.2.5.208	×		
	Instance Type:	Container	~		
	Before you add the security modiformatting. You o	he first container instance, you must reinitia ule/engine so that the disk has the correct nly need to perform this action once.	lize		
		ок	ancel		

Instantie toevoegen

Stap 5. Interfaces configureren

a. Stel Resource Profile, Management Interface, Management IP in voor Instance01.

In dit voorbeeld : ·Resourceprofiel: Instance01 ·Beheerinterface: Ethernet1/3 ·ManagementIP: x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform	Settings	System Tools Help admin
Provisioning - FTD01 Standalone Cisco Secure Firewall Threat Defense 7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration TX	Save Cancel
Data Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/8	Settings Agreement SM 1 - 86 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 Address Type: IPv4 Management ID: 1.000000000000000000000000000000000000	
Application Version Resource Profile	rt Status	
FTD 7.2.5.208		
	OK Cancel	,

Profielen/beheerinterface/IP-beheer configureren

b. Stel data-interfaces in.

In dit voorbeeld :

·Ethernet1/1 (gebruikt voor binnenkant)

·Ethernet1/2 (gebruikt voor buitengebruik)

·Ethernet1/4 (gebruikt voor HA-link)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools	Help admin
P S	rovisioning - FTD01 itandalone Cisco Sec	ure Firewall Threat Defense	7.2.5.208					Save	Cancel
D	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Ethernet I Ethernet I]/1]/2]/4	FTD - 7.2.5.208 Ethernet1/3 Click to configure			
ļ	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
•	FTD	7.2.5.208	Instance01	1.10001	1.0	Ethernet1/3			
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4	2		Type data data data					

Gegevensinterfaces instellen

c. Navigeer naar logische apparaten. Wachten op bijv. bootup.

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	S				System Tools	Help	admin
Lo	gical Devic	e List		0	1 Container instance	a) 100% (86 of 86) Cores Availab	le			C Refresh	 Add 	d •
	FTD01			Standalone	Status:ok						I	11
	Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status			
	FTD		7.2.5.208	Instance01		1	1.0-0	Ethernet1/3	😽 Installing		¢	

Status van instantie bevestigen01

d. Herhaal a. in stap 4.a en stap 5.a tot en met c om de tweede instantie toe te voegen en geef er een detail voor in te stellen.

In dit voorbeeld :

·Apparaatnaam: FTD11 ·Type instantie: Container

•Resourceprofiel: Instance02 •Beheerinterface: Ethernet1/7 •ManagementIP: x.x.10.1

·Ethernet1/5 = binnenkant

•Ethernet1/6 = buiten

·Ethernet1/8 = HA-link

e. Bevestig 2 Instanties zijn online status op FCM.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devic	ce List			2 Container instan	ces) 66% (56 of 86) Cor	es Available			C Refresh 🔘 Add •
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02]	.10.1	1.0.0.000	Ethernet1/7	Online	🕶 🕅 c 🖄
FTD01			Standalone	Status:ok					/ I
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01]	Carlani	1.0	Ethernet1/3	Online	💌 🕅 Cái

Instantiestatus op primair apparaat bevestigen

f. (optioneel) Start scope ssa, scope slot 1 en show app-Instance bevestig 2 instanties zijn online status op Firepower CLI.

<#root>
FPR4145-ASA-K9#
scope ssa
FPR4145-ASA-K9 /ssa #
scope slot 1
FPR4145-ASA-K9 /ssa/slot #
show app-Instance
Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo
online
7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11
online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g. Doe dit ook met het secundaire apparaat. Bevestig 2 Instanties zijn online status.

Ove	erview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logic	al Devio	e List			(2 Container instan	ces) 66% (56 of 86) Co	res Available			C Refresh 🕢 Add •
	FTD12			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance02]	10.2	1.	Ethernet1/7	Online	💌 🕅 💌
E	FTD02			Standalone	Status:ok					/ :
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance01			1.6	Ethernet1/3	Online	🚾 🌆 C 🖄

Instantiestatus op secundair apparaat bevestigen

Stap 6. Voeg een hoog beschikbaarheidspaar toe voor elke instantie.

a. Ga naar Apparaten > Apparaat toevoegen op VCC. Voeg alle instanties toe aan het VCC.

In dit voorbeeld :

·Naam weergeven voor Instance01 van FTD1: FTD1_FTD01
·Naam weergeven voor Instance02 van FTD1: FTD1_FTD11
·Naam weergeven voor Instance01 van FTD2: FTD2_FTD02
·Naam weergeven voor Instance02 van FTD2: FTD2_FTD12

Dit beeld toont de instelling voor **FTD1_FTD01**.



FTD-instantie toevoegen aan FMC

b. Controleer of alle exemplaren normaal zijn.

Firewall Management Center Devices / Device Management	31 Overview Analysis Policies	Devices Objects Into	egration			Deploy	Q 🥝 🌣 🚱 admin 🔹 ;	dode SECURE
View By: Group	•						Deploym	nent History
All (4) • Error (0) • Warning (0)	Offline (0) Normal (4) Deployment	nt Pending (0) • Upgrade (0) • Snort 3 (4	1)			Q, Search Device	Add 🔻
Collapse All								
Name	Model	4	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)								
FTD1_FTD01_Snort 3 1_21_3.1.1 - Routed	Firepov	wer 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1
C FTD1_FTD11 Snort 3	Firepov	wer 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1:
FTD2_FTD02 Snort 3 Smot.1.2 - Routed	Firepor	wer 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD12 Snort 3 Gonz 10.2 - Routed	Firepov	wer 4145 with FTD	7.2.5	Firepower4KHG cisco com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1:

Instantiestatus in VCC bevestigen

c. Navigeer naar **apparaten** > **Hoge beschikbaarheid toevoegen**. Stel 1e failover-paar in.

In dit voorbeeld :

·Naam: FTD01_FTD02_HA

·Primaire peer: FTD1_FTD01



Opmerking: Zorg ervoor dat u de juiste eenheid als primaire eenheid selecteert.

Firewall Management Center Overview Analysis Pol	licies Devices Objects	Integration		Deploy	Q 📀 🌣 😧 admin 🕶	tiste SECURE
View By: Group					Deploy	ment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4) • D	eployment Pending (0)	(0) • Snort 3 (4)			Q, Search Device	Add 🔻
Collacse All						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availability Pair				
FID1_FID01_Snort_3	Firepower 4145 with FTD	Name:* FTD01_FTD02_H4	Base, Threat (2 more)	acp-rule	*Ø	1
FID1_FID11 Snort 3	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-role	*©	1
FTD2_FTD02_Snort.3 1.2 - Routed	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01 *	Base, Threat (2 more)	acp-rule	*9	1
FTD2_FTD12_Snort.3 10.2 - Routed	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 v	Base, Threat (2 more)	acp-rule	4Q	1
		Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.				
		Cancel Continue				

1e failover-paar toevoegen

d. Stel IP voor failover link in als 1e failover-paar.

In dit voorbeeld :

·High Availability Link: Ethernet1/4

•Statuslink: Ethernet1/4

·Primair IP-adres: 192.168.90.1/24

·Secundair IP-adres: 192.168.90.2/24

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q 💿 🗘										
Mew Br. Group					Depk	yment History				
All (4) Error (0) Warning (0) Offline (0) Normal (4)	Deployment	Pending (0)			Q, Search Device	Add •				
Collacos Al										
Name Name	Model	Add Mich Availability Pair		Access Control Policy	Auto RollBack					
Ungrouped (4)		Ava high Availability Fail								
		High Availability Link	State Link							
FTD1_FTD01 Snot 3 I 1 - Routed	Firepow	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	4©	11				
		Logical Name:* ha_link	Logical Name:*							
FTD1_FTD11 Snort 3 I0.1 - Routed	Firepow	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	*9	11				
		Secondary IP-1 102 169 00 2	Geroportany ID-1							
FTD2_FTD02 Snort 3 1.2 - Routed	Firepowe	Subnet Mask.* 255.255.0	Subnet Mask:*	acp-rule	*9	1				
FTD2 FTD12 Seed 3		IPsec Encryption								
10.2 - Routed	Firepow	Enabled		acp-rule	\$P	1				
		Key Generation: Auto v								
		LAN failover link is used to sync configuration, state between peers. Selected interface links and encryption	ful failover link is used to sync application content settings cannot be changed later.							
			Cancel Add							

HA-interface en IP instellen voor 1e failover-paar

e. Bevestig de status van failover

·FTD1_FTD01: Primair, actief

·FTD2_FTD02: Secundair, stand-by

E Fire	ewall Management Center Overview Analysis ces / Device Management	Policies Devices Object	is Integration	1			Deploy Q 🥝	🔅 🔞 admin	cisco SECURE			
View By:	Group +							Dep	oloyment History			
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	 Deployment Pending (0) 	lpgrade (0)	Snort 3 (4)				Q, Search Device	Add 👻			
Collapse All	Zallaces All											
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack					
	□											
	FTD01_FTD02_HA High Availability								11			
	FTD1_FTD01(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40		I			
	FTD2_FTD02(Secondary, Standby) Snort 3 CT3.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower/KCHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q		I			
	C FTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢Ø		11			
	C FTD2_FTD12 Snort 3 (Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø		1			

Status van eerste failover-paar bevestigen

f. Navigeren naar apparaten > Klik op FTD01_FTD02_HA (in dit voorbeeld) > Interfaces. Stel actieve IP voor data-interface in.

In dit voorbeeld :

·Ethernet1/1 (binnenkant): 192.168.10.254/24

·Ethernet1/2 (buiten): 192.168.20.254/24

·Ethernet1/3 (diagnostisch): 192.168.80.1/24

Dit beeld toont de instelling voor Active IP van Ethernet1/1.

Firewall Management Center Devices / Secure Frewall Interfaces	rview Analysis Po	vicies Devices Objects Integration				Deplo	y Q 🗳 🌣 🔕 admin	• deades SECURE
FTD1_FTD01							You have unsaved changes	Save Cancel
Cisco Firepower 4145 Threat Defense Summary High Availability Device Routing	Interfaces Inline Se	Edit Physical Interface		Edit Physical Interface			0	vailable for use. X
		General IPv4 IPv6 Path Monitorin	ng Advanced	General IPv4 IPv6 Path	Monitoring Advanced			Add Interfaces +
Interface	.ogi	Name:		IP Type: Use Static IP v				
Ethernet1/1 inc	nside	Enabled Management Only		IP Address: 192.168.10.254/24	-			
© Ethernet1/2 or	utside faceatis	Description:		- 92. 196.0.2. 19209-200-200-120 07 196.0.2. 02				
© Ethernet1/4	agavan.	Mode:						
		Security Zone:						
		Interface ID:					Cancel OK	
		Ethernet1/1 MTU:						
		(64 - 9184)						
		Priority: 0 (0 - 6553)	9					
		Propagate Security Group Tag:						
					Cancel OK			

Actieve IP voor data-interface instellen

Ga naar Apparaten > Klik op FTD01_FTD02_HA (in dit voorbeeld) > High Availability. Stel stand-by IP voor data-interface in.

In dit voorbeeld :

Ethernet1/1 (binnenkant): 192.168.10.253/24
Ethernet1/2 (buiten): 192.168.20.253/24
Ethernet1/3 (diagnostisch): 192.168.80.2/24

Dit beeld toont de instelling voor Standby IP van Ethernet1/1.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q 🗳 🌣 @ admin 🗸 the secure												
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	e Device Routing Interfaces Inline Sets DHCP VT	ГЕР						Savo Cancel				
IPsec Encryption	Edit inside	0	itics					٩				
Monitored Interfaces Interface Name	Monitor this interface for failures IPv4 IPv6			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitori	ing				
outside	Interface Name:						٥	1				
diagnostic	Active IP Address:				٢	/						
inside	192.168.10.254 Mask:				0	1						
	24 Standby IP Address:											
Failover Trigger Criteria	192.106.10.233		face MAC Add	resses				+				
Failure Limit			cal Interface	Active Mac Ac	Idress	Standby M	ac Address					
Peer Poll Time		Cancel	et1/1	1234.1234.00	01	1234.1234	1.0002	/1				
Peer Hold Time												

Standby IP voor data-interface instellen

h. Herhaal stap 6.c tot en met g om het tweede failover-paar toe te voegen.

In dit voorbeeld :

·Naam : FTD11_FTD12_HA
·Primaire peer: FTD1_FTD11
·Secundaire peer: FTD2_FTD12

·High Availability Link: Ethernet1/8
·State Link: Ethernet1/8
·Ethernet1/8 (ha_link actief): 192.168.91.1/24

·Ethernet1/5 (in actief): 192.168.30.254/24

·Ethernet1/6 (buiten actief): 192.168.40.254/24

·Ethernet1/7 (diagnostisch actief): 192.168.81.1/24

·Ethernet1/8 (ha_link Standby): 192.168.91.2/24

·Ethernet1/5 (in standby): 192.168.30.253/24

·Ethernet1/6 (buiten Standby): 192.168.40.253/24

·Ethernet1/7 (diagnostische stand-by): 192.168.81.2/24

i. Navigeren naar **logische apparaten** > **Standalone toevoegen**. Stel de ACS-regel in om het verkeer van binnen naar buiten toe mogelijk te maken.

Ę	Firewall Ma Policies / Acces	anagement C Is Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🗳 🕸	Ø ad	min •	diste	SECU	RE
•	acp-rule Try New UI Layout (Analyze Hit Counts Sees Carcel Enter Description																			
F	Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: None Identity Policy: None																			
Eih	er by Device	Search Rules											×	Show Rule Con	flicts 🛛 +	Add Cat	egory	+ A	dd Rul	e
	Name	Source Zones	Dest Zones	Source Networks	De	est Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	F6 0	B , <u>A</u>	•		¢
$\sim M$	landatory - acp-rule	(1-1)		_																
1	ftd_ha_acp	inside_zone	outside_zone	Any	A		Any	Any	Any	Any	Any	Any	Any	Any	C Allow	15 O	B .2	0	0 /	1
$\sim D$	V Default - acp-rule (-)																			
The	re are no rules in thi	s section. Add Ru	le or Add Cate	gory																

j. Stel de instelling in op FTD.

k. Bevestig de HA-status in CLI

De HA status voor elke instantie wordt ook bevestigd in Firepower CLI die hetzelfde is als ASA.

Start show running-config failover en show failover opdracht om de HA-status van FTD1_FTD01 (Primaire instantie01) te bevestigen.

<#root>

// confrim HA status of FTD1_FTD01 (Instance01 of Primary Device) >

show running-config failover

failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication htt

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: P Other host: Secondary - Standby Ready <---- InstanceO1 of FPRO2 is Standby Interface diagnostic

Uitvoeren show running-config failover en show failover opdracht om de HA-status van FTD1_FTD11 te bevestigen (Primaire instantie02)

<#root>

// confrim HA status of FTD1_FTD11 (Instance02 of Primary Device) >

show running-config failover

failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication htt

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: P Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16

Doorlopen **show running-config failover** en **show failover** opdracht geven om de HA-status van FTD2_FTD02 te bevestigen (Secundaire instantie01).

<#root>

// confrim HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host:

Start show running-config failover en show failover opdracht om de HA-status van FTD2_FTD12 (Secundaire instantie02) te bevestigen.

<#root>

// confrim HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

1. Bevestig het verbruik van de vergunning

Alle licenties worden verbruikt per beveiligingsmotor/chassis en niet per container instantie.

·Basislicenties worden automatisch toegewezen: één per beveiligingsmotor/chassis.

·Licenties voor functies worden handmatig toegewezen aan elke instantie, maar u verbruikt slechts één licentie per voordeelmotor/chassis. Voor een specifieke functielicentie hebt u slechts in totaal 1 licentie nodig, ongeacht het aantal gebruikte instanties.

In deze tabel wordt aangegeven hoe de licenties in dit document worden verbruikt.

FPR01	Instantie01	Basis, URL-filtering, malware, bedreiging
	Instantie02	Basis, URL-filtering, malware, bedreiging
FPR02	Instantie01	Basis, URL-filtering, malware, bedreiging
	Instantie02	Basis, URL-filtering, malware, bedreiging

Totaal aantal licenties

Basis	URL-filtering	Malware	dreigement
2	2	2	2

Bevestig het aantal verbruikte licenties in de FMC GUI.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
∨ Base (2)	 In-Compliance 					^
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	_
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	_
V Mabware (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	aat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
✓ Threat (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
✓ URL Filtering (2)	In-Compliance					- 1
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Frepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	

Bevestig verbruikte licenties

Verifiëren

Wanneer de crash plaatsvond op FTD1_FTD01 (Primary Instance01), wordt de failover van Instance01 geactiveerd en nemen de gegevensinterfaces aan de Standby-zijde het IP/MAC-adres van de oorspronkelijke Active Interface over, waardoor het verkeer (FTP-verbinding in dit document) continu door Firepower wordt doorgegeven.



Voor de botsing



failover is geactiveerd

Stap 1. Start FTP verbinding van Win10-01 naar Win10-02.

Stap 2. De show conn opdracht Uitvoeren om de FTP-verbinding te bevestigen is in beide gevallen vastgelegd.

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

Stap 3. Start FTP verbinding van Win10-03 naar Win10-04.

Stap 4. De show conn opdracht Uitvoeren om de FTP-verbinding te bevestigen is in beide gevallen vastgelegd.

<#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

Stap 5. Start connect ftd FTD01 en system support diagnostic-cli opdracht om ASA CLI te starten. Start enableen **crashinfo force watchdog** commando om crash Instance01 in primaire/actieve eenheid te forceren.

<#root>

Firepower-module1>

connect ftd FTD01

```
>
```

```
system support diagnostic-cli
```

FTD01>

enable

Password: FTD01# FTD01#

crashinfo force watchdog

```
reboot. Do you wish to proceed? [confirm]:
```

Stap 6. Failover treedt op in Instance01 en de FTP-verbinding wordt niet onderbroken. Draai show failover en show conn commando om de status van Instance01 in FPR02 te bevestigen.

<#root>

```
>
```

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

Stap 7. De crash in Instance01 had geen effect op Instance02. Draai show failover en show conn commando om de status van Instance02 te bevestigen.

<#root>

```
>
```

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

show conn

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1
```

Stap 8. Ga naar Apparaten > Alles op FMC. Bevestig de HA-status.

·FTD1_FTD01: Primair, stand-by

·FTD2_FTD02: Secundair, actief

Fin Dev	rewall Management Center Overview Analysis	Policies Devices Object	s Integration	n			Deploy Q	admin • 🕴 🕹				
View By:	Group							Deployment History				
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	Deployment Pending (0) U	pgrade (0)	Snort 3 (4)				Q, Search Device Add +				
Collapse All	lasse Al											
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack					
	✓ Ungrouped (2)											
	✓ FTD01_FTD02_HA High Availability							×1				
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	EPRA145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1				
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1				
	✓ FTD11_FTD12_HA ∀ High Availability							1				
	FTD1_FTD11(Primary, Active) Short 3 Circ ¹ 10.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:				
	FTD2_FTD12(Secondary, Standby) Short 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4D	I				

HA-status bevestigen

Stap 9. (Optioneel)Nadat de Instance01 van FPR01 terugkeert naar normaal, kunt u de status van HA handmatig switches. Dit kan door FMC

GUI of FRP CLI worden gedaan.

Ga in het VCC naar Apparaten > Alle. Klik op Switch Active Peer to switch HA status voor FTD01_FTD02_HA.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deptoy Q O 🌣 🕢 admin												
View By All (4	Group • • Error (0) • Warning (0) • Offline (0) • Normal (4)	Deployment Pending (0) Upgrade (0)	0) Snort 3 (4)			Q	Deployment History Search Device Add •					
Collapse	Al											
	Name	Model Version	n Chassis	Licenses	Access Control Policy	Auto RollBack						
	 Ungrouped (2) 											
	FTD01_FTD02_HA High Availability						Switch Active Peer					
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD 7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ф	Force refresh node status Delete Revert Upgrade					
	FTD2_FTD02(Secondary, Active) Short 3 FTD2_FTD2_FTD2(Secondary, Active)	Firepower 4145 with FTD 7.2.5	Firepower401G.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ęģ	Health Monitor Troubleshoot Files					
	FTD11_FTD12_HA High Availability						1					
	FTD1_FTD11(Primary, Active) Short 3 Com(10.1 - Routed	Firepower 4145 with FTD 7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	42	:					
	FD2_FTD12(Secondary, Standby) Snort 3 Elig3.10.2 - Routed	Firepower 4145 with FTD 7.2.5	Erepower4043.cisco.com/443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					

Switch HA-status

Op Firepower CLI, Start connect ftd FTD01 en system support diagnostic-cli opdracht om ASA CLI in te voeren. Start enableen **failover** active commando naar switch HA voor FTD01_FTD02_HA.

<#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available

enable

firepower#

failover active

Problemen oplossen

Om de status van failover te valideren, voert u show failover de show failover history opdracht uit.

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) This host:

Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (2

>

show failover history

Start de opdracht debug fover <optie> om debug-logbestand van failover in te schakelen.

<#root>

>

debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution of

Referentie

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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.