Hoge beschikbaarheid van FTD op Firepowerapplicaties configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Taak 1. Voorwaarden controleren Taak 2. FTD HA op FPR9300 configureren Voorwaarden Taak 3. FTD HA en licentie verifiëren Taak 4. Failover-rollen wisselen Taak 5. HA-paar verbreken Taak 5. HA-paar verbreken Taak 6. HA-paar uitschakelen Taak 7. HA opschorten Veelgestelde vragen (FAQ) Gerelateerde informatie

Inleiding

In dit document wordt beschreven hoe u hoge beschikbaarheid (HA) van Firepower Threat Defense (FTD) (Active/Standby failover) configureert en verifieert op de FPR9300.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- 2x Cisco Firepower 9300 security applicatie FXOS-software 2.0(1.23)
- FTD versie 10.10.1.1 (build 1023)
- Firepower Management Center (FMC) SW 10.10.1.1 (build 1023)

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. **Opmerking:** Op een FPR9300 apparaat met FTD, kunt u alleen inter-chassis HA configureren. De twee eenheden in een HA-configuratie moeten voldoen aan de hier genoemde voorwaarden.

Taak 1. Voorwaarden controleren

Taakvereiste:

Controleer of beide FTD-apparaten voldoen aan de notitievereisten en kunnen worden geconfigureerd als HA-eenheden.

Oplossing:

Stap 1. Maak verbinding met het beheer-IP-adres van de FPR9300 en controleer de hardware van de module.

Controleer de FPR9300-1 hardware.

KSEC-FI	PR9K-1-A# s	how server	inventory		
Server Cores	Equipped P	ID Equipped	l VID Equipped Serial	(SN) Slot Status	Ackd Memory (MB) Ackd
1/1	FPR9K-SM-	-36 V01	FLM19216KK6	Equipped	262144
36					
1/2	FPR9K-SM-	-36 V01	FLM19206H71	Equipped	262144
36					
1/3	FPR9K-SM-	-36 V01	FLM19206H7T	Equipped	262144
36					
KSEC-FI	PR9K-1-A#				
-					

Controleer de FPR9300-2 hardware.

KSEC-FPF	R9K-2-A# show	server invent	ory		
Server Cores	Equipped PID	Equipped VID	Equipped Serial (SN)	Slot Status	Ackd Memory (MB) Ackd
1/1	FPR9K-SM-36	V01	FLM19206H9T	Equipped	262144
36					
1/2	FPR9K-SM-36	V01	FLM19216KAX	Equipped	262144
36					
1/3	FPR9K-SM-36	V01	FLM19267A63	Equipped	262144
36					
KCEC-EDE	0V-2-7#				

Stap 2. Log in bij de FPR9300-1 Chassis Manager en ga naar Logical Devices (logische apparaten).

Controleer de softwareversie, het aantal en het type interfaces zoals in de afbeeldingen wordt weergegeven.

FPR9300-1

۲	Firepower_TD2	Standalone	Status: ok					M 🥒 B
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
	Security Module 3	FTD	6.0.1.1.1023	10.62.148.69	10.62.148.1	Ethernet1/2	Online	Contract 🕒 🥕
	Ports: Attributes: Data Interfaces: Ethernet1/4 Ethernet1/5 Ethernet1/6 UIID : 10.62.148.69 UIID : 99eba974-4144-11e6-BedF-8b68bo49edb6							

FPR9300-2

۲	Firepower_TD	Standalone	Status: ok					F. 23
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
8	Security Module 3	FTD	6.0.1.1.1023	10.62.148.72	10.62.148.1	Ethernet1/2	online	(trainer 🕒 🎼 🏞
	Ports: Attributes: Data Interfaces: Ethernet1/4 Ethernet1/5 Ethernet1/6 Cluster Operational Status : not-applicable Firepower Management IP: 10.62.148.72 Management URL : https://10.82.148.73 UUID : \$1048676-3324-1166-8a63-eee869c62b45							

Taak 2. FTD HA op FPR9300 configureren

Taakvereiste:

Configureer Active/Standby failover (HA) aan de hand van dit diagram.



Oplossing:

Beide FTD-apparaten zijn al geregistreerd op het FMC, zoals in de afbeelding is weergegeven.



Stap 1. Om de FTD-failover te configureren gaat u naar **Devices > Device Management** (Apparaten > Apparaatbeheer) en selecteert u **Add High Availability** (Hoge beschikbaarheid toevoegen), zoals in de afbeelding is weergegeven.

By Group	▼ 🔾 Add •
Access Control Policy	Add Device
	Add High Availability

Stap 2. Voer de **Primary Peer** (primaire peer) en de **Secondary Peer** (secundaire peer) in en selecteer **Doorgaan** zoals in de afbeelding is weergegeven.

Add High Availability Pair ?							
Name:*	FTD9300_HA						
Device Type:	Firepower Threat Defense	~					
Primary Peer:	FTD9300-1	~					
Secondary Peer:	FTD9300-2	~					
Threat Defense High Availability pair will have primary device configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.							
	Continue	ancel					

Waarschuwing: Zorg ervoor dat u de juiste eenheid als **primaire** eenheid selecteert. Alle configuraties op de geselecteerde primaire eenheid worden gerepliceerd naar de geselecteerde secundaire FTD-eenheid. Als gevolg van replicatie kan de huidige configuratie op de secundaire eenheid worden **vervangen**.

Voorwaarden

Om een HA tussen 2 FTD-apparaten te creëren, moet aan deze voorwaarden worden voldaan:

- Hetzelfde model
- Dezelfde versie (dit geldt voor FXOS en voor FTD (hoofdversie (eerste getal), onderversie (tweede getal) en revisieversie (derde getal) moeten hetzelfde zijn))
- Hetzelfde aantal interfaces
- Hetzelfde type interfaces
- Beide apparaten als deel van dezelfde groep/domein in het VCC
- Identieke NTP-configuratie (Network Time Protocol)
- Zijn volledig geïmplementeerd op het FMC zonder niet-doorgevoerde wijzigingen
- Gebruiken dezelfde firewallmodus: gerouteerd of transparant.
- Dit moet op beide FTD-apparaten en de GUI van het FMC worden gecontroleerd, aangezien de FTD's dezelfde modus kunnen hebben zonder dat dit wordt weerspiegeld door het FMC.
- Heeft geen DHCP/Point-to-Point Protocol over Ethernet (PPPoE) geconfigureerd in een van de interfaces
- Verschillende hostnamen (Fully Qualified Domain Name (FQDN)) voor beide chassis. Om te

controleren of het chassis hostname navigeer naar FTD CLI en voer deze opdracht uit:

firepower# show chassis-management-url

```
https://KSEC-FPR9K-1.cisco.com:443//
```

Opmerking: In FTD-versies recenter dan 6.3, gebruikt u de opdracht 'show chassis detail'

firepower# show chassis	detail
Chassis URL	: https://KSEC-FPR4100-1:443//
Chassis IP	: 192.0.2.1
Chassis Serial Number	: JMX12345678
Security Module	: 1

Als beide chassis dezelfde naam hebben, verander dan de naam van één chassis met behulp van deze opdrachten:

KSEC-FPR9K-1-A# scope system
KSEC-FPR9K-1-A /system # set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* # commit-buffer
FPR9K-1-A /system # exit
FPR9K-1new-A#

Nadat u de chassisnaam heeft gewijzigd, verwijdert u de registratie van FTD van het FMC en voert u de registratie opnieuw uit. Ga daarna door met het maken van het HA-paar.

Stap 3. Configureer de HA en voer de linkinstellingen in.

In uw geval heeft de State Link dezelfde instellingen als de High Availability Link.

Selecteer Add (toevoegen) en wacht enkele minuten tot het HA-paar is geïmplementeerd, zoals in de afbeelding is weergegeven.

Interface:*	Ethernet1/4	*	Interface:*	Same as LAN Failover L
Logical Name:*	fover_link		Logical Name:*	fover_link
Primary IP:*	1.1.1.1		Primary IP:*	1.1.1.1
	Use IPv6 Address	1		Use IPv6 Address
Secondary IP:*	1.1.1.2		Secondary IP:*	1.1.1.2
Subnet Mask:*	255.255.255.0		Subnet Mask:*	255.255.255.0
Sec Encryption				
Key Generation:	Auto	*		
				ad to a second textile a second

Stap 4. Configureer de data-interfaces (primaire en stand-by-IP-adressen)

Selecteer vanuit de FMC GUI de optie HA Edit, zoals weergegeven in de afbeelding.



Stap 5. Configureer de interface-instellingen, zoals weergegeven in de afbeeldingen.

Ethernet 1/5 interface.

Edit Physical	Interface	? ×
Mode:	None	
Name:	Inside C Enabled Management Only	
Security Zone:	×	
Description:		
General IPv4	IPv6 Advanced Hardware Configuration	
IP Type: IP Address:	Use Static IP v 192.168.75.10/24 eg. 1.1.1.1/2	255.255.255.228 or 1.1.1.1/25
		OK Cancel

Ethernet 1/6 interface.

Edit Physical	Interface	? ×
Mode:	None	
Name:	Outside Chabled Management Only	
Security Zone:	×	
Description:		
General IPv4	IPv6 Advanced Hardware Configuration	
IP Type: IP Address:	Use Static IP v 192.168.76.10/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/	25
	OK Cancel	

Stap 6. Ga naar **High Availability** (hoge beschikbaarheid) en selecteer **Edit** (bewerken) voor de interfacenaam om de stand-by-IP-adressen toe te voegen zoals in de afbeelding is weergegeven.

FTD9300_HA Cisco Firepower 9000 Series SM-36 Threat Defense											Save	Cancel
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP					
High Availability Configuration												
High Availabilit	y Link							State Link				
Interface						Ethernet1/4		Interface			Ethernet1/	4
Logical Name						fover_link		Logical Name			fover_lin	ik
Primary IP						1.1.1.1		Primary IP			1.1.1	1
Secondary IP						1.1.1.2		Secondary IP			1.1.1	2
Subnet Mask						255.255.255.0		Subnet Mask			255.255.255	0
IPsec Encrypti	ion					Disabled		Statistics				L
Monitored In	nterfaces											
Interface Nam	ne Act	tive IPv4	Standby 1	IPv4	Active IPv6 - S	tandby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
📄 Inside	192	2.168.75.10									×	0
iagnostic											1	8
Outside	192	2.168.76.10									×	1

Stap 7. Voor de inside-interface zoals weergegeven in de afbeelding.

Edit Inside	? ×
Monitor this interface for failures	
IPv4 IPv6	
Interface Name: Inside	
Active IP Address: 192.168.75.10	
Mask: 24	
Standby IP Address: 192.168.75.11	
	OK Cancel

Stap 8. Doe hetzelfde voor de outside-interface.

Stap 9. Controleer het resultaat zoals weergegeven in de afbeelding.

Monitored Interfaces					
Interface Name	Active IPv4	Standby IPv4			
📾 Inside	192.168.75.10	192.168.75.11			
iagnostic					
Outside	192.168.76.10	192.168.76.11			

Stap 10. Blijf op het tabblad High Availability en configureer virtuele MAC-adressen zoals in de afbeelding is weergegeven.

Failover Trigger Criteria	1	Interface Mac Addresses	Interface Mac Addresses	Interface Mac Addresses
Failure Limit	Failure of 1 Interfaces	Physical Interface	Physical Interface Active Mac Address	Physical Interface Active Mac Address Standby Mac Address
Peer Poll Time	1 sec		No records to display	No records to display
Peer Hold Time	15 sec		no records to display	no records to display
Interface Poll Time	5 sec			
Interface Hold Time	25 sec			

Stap 11. De afbeelding toont de instellingen voor de inside-interface.

Add Interface Mac Address			? ×
Physical Interface:*	Ethernet1/5	~	
Active Interface Mac Address:*	aaaa.bbbb.1111		
Standby Interface Mac Address:*	aaaa.bbbb.2222		
Inter the Mac addresses in hexad	lecimal format such as	0123.45	67.89ab
	ок	Ca	incel

Stap 12. Doe hetzelfde voor de outside-interface.

Stap 13. Controleer het resultaat zoals weergegeven in de afbeelding.

1	Interface Mac Addresses			٢
	Physical Interface	Active Mac Address	Standby Mac Address	
	Ethernet1/5	aaaa.bbbb.1111	aaaa.bbbb.2222	J 🖉
	Ethernet1/6	aaaa.bbbb.3333	aaa.bbbb.4444	a 🖉

Stap 14. Nadat u de wijzigingen heeft geconfigureerd, selecteert u **Save** (opslaan) en Deploy (implementeren).

Taak 3. FTD HA en licentie verifiëren

Taakvereiste:

Controleer de FTD HA-instellingen en actieve licenties van de FMC GUI en van de FTD CLI.

Oplossing:

Stap 1. Ga naar **Summary** (overzicht) en controleer de HA-instellingen en actieve licenties, zoals weergegeven in de afbeelding.

FTD9300_HA										
Cisco Firepower	9000 Series SM-36 Thre	at Defense Hig	h Availability							
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP			
	•									
	General						P	License		0
	Name:			FTD93	00_HA			Base:	Yes	
	Status:			0				Export-Controlled Feature	s: Yes	
	Primary Pee	r:		FTD93	00-1(Active)			Malware:	Yes	
	Secondary P	eer:		FTD93	00-2(Standby)			Threat:	Yes	
	Failover Hist	ory:		۹,				URL Filtering:	Yes	

Stap 2. Voer vanaf de FTD CLISH CLI de volgende opdrachten uit:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours FLM19267A63, Mate FLM19206H7T
Last Failover at: 18:32:38 EEST Jul 21 2016
This host: Primary - Active
Active time: 3505 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
 Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Standby Ready
Active time: 172 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Stateful Failover Logical Update Statistics
```

Link : fover_link Ethernet1/4 (up) Stateful Obj xmit xerr rcv rerr General417 0 416 0 sys cmd 416 0 416 0 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 0 UDP conn 0 0 0 0 0 ARP tbl 0 0 Xlate_Timeout 0 0 0 0 IPv6 ND tbl 0 0 0 0 VPN IKEv1 SA 0 0 0 0 VPN IKEv1 P2 0 0 0 0 0 VPN IKEv2 SA 0 0 0 VPN IKEv2 P2 0 0 0 0 VPN CTCP upd 0 0 0 0 VPN SDI upd 0 0 0 0 VPN DHCP upd 0 0 0 0 0 SIP Session 0 0 0 SIP Tx 0 0 0 0

SIP Pinhole O	0	0	0
Route Session 0	0	0	
Router ID 0	0	0	0
User-Identity 1	0	0	
CTS SGTNAME 0	0	0	0
CTS PAC 0	0	0	0
TrustSec-SXP 0	0	0	0
IPv6 Route 0	0	0	0
STS Table 0	0	0	0
Logical Update Queu	le Informa	ation	
Cur Max Total			
Recv Q: 0 10 416			
Xmit Q: 0 11 2118			

>

Stap 3. Doe hetzelfde op het secundaire apparaat.

Stap 4. Voer de opdracht show failover state uit vanaf de LINA CLI:

```
firepower# show failover state

Active Last Failure Reason Date/Time

Primary

Active None

Other host - Secondary

Standby Ready Comm Failure 18:32:56 EEST Jul 21 2016

====Configuration State===

Sync Done

====Communication State===

Mac set
```

0

0

```
firepower#
Stap 5. Controleer de configuratie vanaf de primaire eenheid (LINA CLI):
```

```
firepower# show running-config failover
failover
failover lan unit primary
failover lan interface fover_link Ethernet1/4
failover replication http
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2
firepower#
firepower# show running-config interface
1
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
1
interface Ethernet1/4
description LAN/STATE Failover Interface
1
interface Ethernet1/5
nameif Inside
```

```
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
interface Ethernet1/6
nameif Outside
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
firepower#
```

Taak 4. Failover-rollen wisselen

Taakvereiste:

Vanuit het FMC wisselt u de failover-rollen van Primary/Active, Secondary/Standby in Primary/Standby, Secondary/Active

Oplossing:

Stap 1. Selecteer het pictogram, zoals weergegeven in de afbeelding.



Stap 2. Bevestig de actie in het pop-upvenster, zoals weergegeven in de afbeelding.



Stap 3. Controleer het resultaat zoals weergegeven in de afbeelding.



Vanaf de LINA CLI kunt u zien dat de opdracht **no failover active** is uitgevoerd op de Primary/Active (primaire/actieve) eenheid:

```
Jul 22 2016 10:39:26: %ASA-5-111008: User 'enable_15' executed the 'no failover active' command. Jul 22 2016 10:39:26: %ASA-5-111010: User 'enable_15', running 'N/A' from IP 0.0.0.0, executed 'no failover active'
```

U kunt dit ook verifiëren in de output van de opdracht show failover history:

firepower# show failover history

From StateTo StateReason10:39:26 EEST Jul 22 2016Standby ReadySet by the config commandActiveStandby ReadySet by the config commandStap 4. Na de verificatie maakt u de primaire eenheid weer actief.

Taak 5. HA-paar verbreken

Taakvereiste:

Verbreek het failover-paar vanaf het FMC.

Oplossing:

Stap 1. Selecteer het pictogram, zoals weergegeven in de afbeelding.



Stap 2. Controleer de melding zoals weergegeven in de afbeelding.

Confirm	n Break		×
 Ford 	Breaking the High Availability pair "FTD9300_HA' Control policy from standby peer. Are you sure y te break, if standby peer does not respond	' will erase all configuration except ou want to break the pair?	the Access
		Yes	No

Stap 3. Bekijk de melding, zoals weergegeven in de afbeelding.



Stap 4. Controleer het resultaat in de GUI van het FMC, zoals weergegeven in de afbeelding.



show running-config op de primaire eenheid vóór en na het verbreken van HA:

Voorafgaand aan verbreken van HA	Na verbreken van HA
firepower# sh run	firepower# sh run
: Saved	: Saved
Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Serial Number: FLM19267A63 Hardware: FPR9K-SM-36, 135839 MB RAM, C Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
NGFW Version 10.10.1.1	NGFW Version 10.10.1.1
hostname firepower	hostname firepower
enable password 8Ry2Yjlyt7RRXU24 encrypted	enable password 8Ry2Yjlyt7RRXU24 encrypted
names	names
interface Ethernet1/2	interface Ethernet1/2
management-only	management-only
nameif diagnostic	nameif diagnostic
security-level 0	security-level 0
no ip address	no ip address
interface Ethernet1/4 description LAN/STATE Failover Interface	interface Ethernet1/4 no nameif no security-level
interface Ethernet1/5	no ip address
nameif Inside	interface Ethernet1/5
security-level 0	nameif Inside
ip address 192.168.75.10 255.255.255.0 standby	security-level 0
192.168.75.11	ip address 192.168.75.10 255.255.255.0 standby
nameif Outside security-level 0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! ftp mode passive	Interface Ethernet1/6 nameif Outside security-level 0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
ngips conn-match vlan-id	!
access-list CSM_FW_ACL_ remark rule-id 268447744:	ftp mode passive
ACCESS POLICY: FTD9300 - Mandatory/1	ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744:	access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: Allow_ICMP	ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ advanced permit icmp any	access-list CSM_FW_ACL_ remark rule-id 26844
any rule-id 268447744 event-log both	L4 RULE: Allow_ICMP
access-list CSM_FW_ACL_ remark rule-id 268441600:	access-list CSM_FW_ACL_ advanced permit icm
ACCESS POLICY: FTD9300 - Default/1	any rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 268441600:	access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: DEFAULT ACTION RULE	ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ advanced permit ip any	access-list CSM_FW_ACL_ remark rule-id 26844
any rule-id 268441600	L4 RULE: DEFAULT ACTION RULE
!	access-list CSM_FW_ACL_ advanced permit ip a
tcp-map UM_STATIC_TCP_MAP	any rule-id 268441600
tcp-options range 6 7 allow	!
tcp-options range 9 255 allow	tcp-map UM_STATIC_TCP_MAP
urgent-flag allow	tcp-options range 6 7 allow
!	tcp-options range 9 255 allow
no pager	urgent-flag allow
logging enable logging timestamp logging standby	no pager logging enable

logging buffer-size 100000 logging buffered debugging logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 mtu diagnostic 1500 mtu Inside 1500 mtu Outside 1500 failover failover lan unit primary failover lan interface fover_link Ethernet1/4 failover replication http failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222 failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444 failover link fover_link Ethernet1/4 failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2 icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 aaa proxy-limit disable no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM STATIC IP OPTIONS MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map

logging timestamp logging standby loğğinğ buffer-size 100000 logging buffered debugging logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 mtu diagnostic 1500 mtu Inside 1500 mtu Outside 1500 no failover no monitor-interface service-module icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:0 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 aaa proxy-limit disable no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infin crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM STATIC IP OPTIONS MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc

inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/DDC **EService** destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly 9 subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily firepower# Cryptochecksum:933c594fc0264082edc0f24bad35803

inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_M class class-default set connection advanced-options UM STATIC TCP MAP service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/ **EService** destination address email callhome@cisco.com destination transport-method http

subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic month subscribe-to-alert-group configuration periodic mo subscribe-to-alert-group telemetry periodic daily Cryptochecksum:fb6f5c369dee730b9125650517

1

: end firepower#

show running-config op de secundaire eenheid vóór en na het verbreken van HA, zoals weergegeven in deze tabel.

Voorafgaand aan verbreken van HA	Na verbreken van HA
firepower# sh run	firepower# sh run
: Saved	: Saved
: Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, 0 Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
NGFW Version 10.10.1.1	NGFW Version 10.10.1.1
hostname firepower	hostname firepower
enable password 8Ry2Yjlyt7RRXU24 encrypted	enable password 8Ry2Yjlyt7RRXU24 encrypted
names	names
interface Ethernet1/2	interface Ethernet1/2
management-only	management-only
nameif diagnostic	nameif diagnostic
security-level 0	security-level 0
no ip address	no ip address
interface Ethernet1/4	interface Ethernet1/4
description LAN/STATE Failover Interface	shutdown
!	no nameif

end

interface Ethernet1/5 no security-level nameif Inside no ip address security-level 0 ip address 192.168.75.10 255.255.255.0 standby interface Ethernet1/5 shutdown 192.168.75.11 no nameif no security-level interface Ethernet1/6 no ip address nameif Outside security-level 0 interface Ethernet1/6 ip address 192.168.76.10 255.255.255.0 standby shutdown 192.168.76.11 no nameif no security-level ftp mode passive no ip address ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 268447744: ftp mode passive ACCESS POLICY: FTD9300 - Mandatory/1 ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 268447744: access-list CSM_FW_ACL_ remark rule-id 26844 L4 RULE: Allow_ICMP ACCESS POLICY: FTD9300 - Mandatory/1 access-list CSM_FW_ACL_ advanced permit icmp any access-list CSM_FW_ACL_ remark rule-id 26844 any rule-id 268447744 event-log both L4 RULE: Allow ICMP access-list CSM_FW_ACL_ remark rule-id 268441600: access-list CSM_FW_ACL_ advanced permit icm ACCESS POLICY: FTD9300 - Default/1 any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: access-list CSM_FW_ACL_ remark rule-id 26844 L4 RULE: DEFAULT ACTION RULE ACCESS POLICY: FTD9300 - Default/1 access-list CSM_FW_ACL_ advanced permit ip any access-list CSM_FW_ACL_ remark rule-id 26844 L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip a any rule-id 268441600 tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow any rule-id 268441600 tcp-options range 9 255 allow tcp-map UM_STATIC_TCP_MAP urgent-flag allow tcp-options range 6 7 allow tcp-options range 9 255 allow no pager urgent-flag allow logging enable logging timestamp no pager logging standby no logging message 106015 logging buffer-size 100000 no logging message 313001 logging buffered debugging no logging message 313008 logging flash-minimum-free 1024 no logging message 106023 logging flash-maximum-allocation 3076 no logging message 710003 mtu diagnostic 1500 no logging message 106100 mtu Inside 1500 no logging message 302015 mtu Outside 1500 no logging message 302014 failover no logging message 302013 failover lan unit secondary no logging message 302018 failover lan interface fover_link Ethernet1/4 no logging message 302017 failover replication http no logging message 302016 failover mac address Ethernet1/5 aaaa.bbbb.1111 no logging message 302021 aaaa.bbbb.2222 no logging message 302020 failover mac address Ethernet1/6 aaaa.bbbb.3333 mtu diagnostic 1500 no failover aaaa.bbbb.4444 no monitor-interface service-module failover link fover_link Ethernet1/4 icmp unreachable rate-limit 1 burst-size 1 failover interface ip fover_link 10.10.1.1 no asdm history enable 255.255.255.0 standby 10.10.1.2 arp timeout 14400 icmp unreachable rate-limit 1 burst-size 1 no arp permit-nonconnected no asdm history enable access-group CSM_FW_ACL_ global arp timeout 14400 timeout xlate 3:00:00 no arp permit-nonconnected access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:0 sctp 0:02:00 icmp 0:00:02 timeout pat-xlate 0:00:30 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 mgcp 0:05:00 mgcp-pat 0:05:00 sctp 0:02:00 icmp 0:00:02 timeout sip 0:30:00 sip_media 0:02:00 sip-invite timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 0:03:00 sip-disconnect 0:02:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 user-identity default-domain LOCAL aaa proxy-limit disable no shmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM STATIC IP OPTIONS MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM STATIC IP OPTIONS MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/DDC **EService** destination address email callhome@cisco.com

timeout sip-provisional-media 0:02:00 uauth 0:05 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 aaa proxy-limit disable no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infin crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicv class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset dns map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM STATIC IP OPTIONS M class class-default set connection advanced-options UM STATIC TCP MAP service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/ **EService** destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment

destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic daily Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd8 4 : end firepower#

subscribe-to-alert-group inventory periodic month subscribe-to-alert-group configuration periodic mo subscribe-to-alert-group telemetry periodic daily Cryptochecksum:08ed87194e9f5cd9149fab3c0e9

3 : end firepower#

Belangrijkste punten voor het verbreken van HA:

Primaire eenheidSecundaire eenheidAlle failover-configuraties worden verwijderdAlle configuraties worden verwijderdIP-adressen in stand-by blijvenAlle configuraties worden verwijderd

Stap 5. Nadat deze taak is voltooid, maakt u het HA-paar opnieuw.

Taak 6. HA-paar uitschakelen

Taakvereiste:

Schakel het failover-paar vanaf het FMC.

Oplossing:

Stap 1. Selecteer het pictogram, zoals weergegeven in de afbeelding.



Stap 2. Controleer de melding en bevestig deze, zoals weergegeven in de afbeelding.



Stap 3. Nadat u de HA heeft verwijderd, wordt de registratie van beide apparaten ongedaan gemaakt (verwijderd) vanaf het FMC.

show running-config resultaat van de LINA CLI is zoals weergegeven in deze tabel:

Primaire eenheid	Secundaire eenheid
firepower# sh run : Saved	firepower# sh run : Saved
: Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Serial Number: FLM19206H7T Hardware: FPR9K-SM-36, 135841 MB RAM, C Xeon E5 series 2294 MHz, 2 CPUs (72 cores)

NGFW Version 10.10.1.1 NGFW Version 10.10.1.1 hostname firepower hostname firepower enable password 8Ry2Yjlyt7RRXU24 encrypted enable password 8Ry2Yjlyt7RRXU24 encrypted names names interface Ethernet1/2 interface Ethernet1/2 management-only management-only nameif diagnostic nameif diagnostic security-level 0 security-level 0 no ip address no ip address interface Ethernet1/4 interface Ethernet1/4 description LAN/STATE Failover Interface description LAN/STATE Failover Interface interface Ethernet1/5 interface Ethernet1/5 nameif Inside nameif Inside security-level 0 security-level 0 ip address 192.168.75.10 255.255.255.0 stands ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11 192.168.75.11 interface Ethernet1/6 interface Ethernet1/6 nameif Outside nameif Outside security-level 0 security-level 0 ip address 192.168.76.10 255.255.255.0 standby ip address 192.168.76.10 255.255.255.0 stands 192.168.76.11 192.168.76.11 ftp mode passive ftp mode passive ngips conn-match vlan-id ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 268447744: access-list CSM_FW_ACL_ remark rule-id 26844 ACCESS POLICY: FTD9300 - Mandatory/1 ACCESS POLICY: FTD9300 - Mandatory/1 access-list CSM_FW_ACL_ remark rule-id 268447744: access-list CSM_FW_ACL_ remark rule-id 26844 L4 RULE: Allow_ICMP L4 RULE: Allow_ICMP access-list CSM_FW_ACL_ advanced permit icmp any access-list CSM_FW_ACL_ advanced permit icm any rule-id 268447744 event-log both any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: access-list CSM_FW_ACL_ remark rule-id 26844 ACCESS POLICY: FTD9300 - Default/1 ACCESS POLICY: FTD9300 - Default/1 access-list CSM_FW_ACL_ remark rule-id 268441600: access-list CSM_FW_ACL_ remark rule-id 26844 L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip a L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600 any rule-id 268441600 tcp-map UM_STATIC_TCP_MAP tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 6 7 allow tcp-options range 9 255 allow tcp-options range 9 255 allow urgent-flag allow urgent-flag allow no pager no pager logging enable logging enable logging timestamp logging timestamp logging standby logging standby logging buffer-size 100000 logging buffer-size 100000 logging buffered debugging logging flash-minimum-free 1024 logging buffered debugging loğğinğ flash-minimum-free 1024 logging flash-maximum-allocation 3076 logging flash-maximum-allocation 3076 mtu diagnostic 1500 mtu diagnostic 1500 mtu Inside 1500 mtu Inside 1500 mtu Outside 1500 mtu Outside 1500 failover failover failover lan unit primary failover lan unit secondary failover lan interface fover_link Ethernet1/4 failover lan interface fover_link Ethernet1/4 failover replication http failover replication http failover mac address Ethernet1/5 aaaa.bbbb.1111 failover mac address Ethernet1/5 aaaa.bbbb.1 aaaa.bbbb.2222 aaaa.bbbb.2222 failover mac address Ethernet1/6 aaaa.bbbb.3333 failover mac address Ethernet1/6 aaaa.bbbb.3

aaaa.bbbb.4444 failover link fover_link Ethernet1/4 failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2 icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 aaa proxy-limit disable no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM STATIC IP OPTIONS MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc

aaaa.bbbb.4444 failover link fover_link Ethernet1/4 failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2 icmp unreachable rate-limit 1 -size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:0 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 user-identity default-domain LOCAL aaa proxy-limit disable no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infin crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error

inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_MAP inspect ip-options UM_STATIC_IP_OPTIONS_M class class-default class class-default set connection advanced-options set connection advanced-options UM_STATIC_TCP_MAP UM STATIC TCP MAP service-policy global_policy global service-policy global_policy global prompt hostname context prompt hostname context call-home call-home profile CiscoTAC-1 profile CiscoTAC-1 no active no active destination address http destination address http https://tools.cisco.com/its/service/oddce/services/DDC https://tools.cisco.com/its/service/oddce/services/ **EService** EService destination address email callhome@cisco.com destination address email callhome@cisco.com destination transport-method http destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic month subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:933c594fc0264082edc0f24bad35803 subscribe-to-alert-group configuration periodic mo subscribe-to-alert-group telemetry periodic daily Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6 1 4 : end end firepower# firepower#

Stap 4. De registratie van beide FTD-apparaten is ongedaan gemaakt vanaf het FMC:

> show managers

No managers configured.

Belangrijkste punten om rekening mee te houden voor de optie HA uitschakelen in het FMC:

Primaire eenheid

Het apparaat wordt uit het FMC verwijderd. Er wordt geen configuratie verwijderd van het FTDapparaat

Secundaire eenheid

Het apparaat wordt uit het FMC verwijderd. Er wordt geen configuratie verwijderd van het FTI apparaat

Stap 5. Voer deze opdracht uit om de failover-configuratie te verwijderen van de FTD-apparaten:

> configure high-availability disable High-availability will be disabled. Do you really want to continue? Please enter 'YES' or 'NO': yes Successfully disabled high-availability.

Opmerking: U moet de opdracht op beide eenheden uitvoeren

Het resultaat:

Primaire eenheid >show failover Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Secundaire eenheid >show failover Failover Off (pseudo-Standby) Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/3.205 Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 secor Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1 Monitored Interfaces 2 of 1041 maximum MAC Address Move Notification Interval not set

Primair

firepower# show run hostname firepower enable password 8Ry2Yjlyt7RRXU24 encrypted names arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 interface GigabitEthernet1/1 nameif outside cts manual propagate sgt preserve-untag policy static sqt disabled trusted security-level 0 ip address 10.1.1.1 255.255.255.0 <-- standby IP was removed interface GigabitEthernet1/2 nameif inside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.1 255.255.255.0 <-- standby IP was removed interface GigabitEthernet1/3 description LAN Failover Interface interface GigabitEthernet1/4 description STATE Failover Interface interface GigabitEthernet1/5 shutdown no nameif no security-level no ip address interface GigabitEthernet1/6 shutdown no nameif no security-level no ip address interface GigabitEthernet1/7 shutdown no nameif no security-level no ip address interface GigabitEthernet1/8 shutdown no nameif no security-level no ip address interface Management1/1 management-only nameif diagnostic cts manual

Interface Policy 1 Monitored Interfaces 0 of 1041 maximum MAC Address Move Notification Interval not set failover replication http > Secundair firepower# show run hostname firepower enable password 8Ry2Yjlyt7RRXU24 encrypted names arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 interface GigabitEthernet1/1 shutdown no nameif no security-level no ip address interface GigabitEthernet1/2 shutdown no nameif no security-level no ip address interface GigabitEthernet1/3 description LAN Failover Interface interface GigabitEthernet1/4 description STATE Failover Interface interface GigabitEthernet1/5 shutdown no nameif no security-level no ip address interface GigabitEthernet1/6 shutdown no nameif no security-level no ip address interface GigabitEthernet1/7 shutdown no nameif no security-level no ip address interface GigabitEthernet1/8 shutdown no nameif no security-level no ip address interface Management1/1 management-only nameif diagnostic cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 no ip address ftp mode passive

ngips conn-match vlan-id propagate sgt preserve-untag policy static sgt disabled trusted access-list CSM_FW_ACL_ remark rule-id 9998: security-level 0 PREFILTER POLICY: Default Tunnel and Priority no ip address Policy access-list CSM_FW_ACL_ remark rule-id 9998: ftp mode passive RULE: DEFAULT TUNNEL ACTION RULE ngips conn-match vlan-id access-list CSM_FW_ACL_ advanced permit ipir access-list CSM_FW_ACL_ remark rule-id 9998: any any rule-id 9998 PREFILTER POLICY: Default Tunnel and Priority access-list CSM_FW_ACL_ advanced permit 41 Policy anv rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 9998: access-list CSM_FW_ACL_ advanced permit gre RULE: DEFAULT TUNNEL ACTION RULE any rule-id 9998 access-list CSM_FW_ACL_ advanced permit ipinip access-list CSM_FW_ACL_ advanced permit udp any any rule-id 9998 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any access-list CSM_FW_ACL_ remark rule-id 26843 any rule-id 9998 ACCESS POLICY: FTD_HA - Default/1 access-list CSM_FW_ACL_ remark rule-id 26843 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit udp any access-list CSM_FW_ACL_ advanced permit ip a any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268435456: any rule-id 268435456 ACCESS POLICY: FTD_HA - Default/1 access-list CSM_FW_ACL_ remark rule-id 268435456: tcp-map UM_STATIC_TCP_MAP L4 RULE: DEFAULT ACTION RULE tcp-options range 9 18 allow access-list CSM_FW_ACL_ advanced permit ip any tcp-options range 20 255 allow tcp-options md5 clear any rule-id 268435456 urgent-flag allow tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow no pager tcp-options range 9 18 allow tcp-options range 20 255 allow logging enable logging timestamp tcp-options md5 clear logging buffered debugging logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 urgent-flag allow no logging message 106015 no logging message 313001 no pager logging enable logging timestamp no logging message 313008 logging buffered debugging logging flash-minimum-free 1024 no logging message 106023 no logging message 710005 no logging message 710003 logging flash-maximum-allocation 3076 no logging message 106100 no logging message 106015 no logging message 313001 no logging message 302015 no logging message 313008 no logging message 302014 no logging message 106023 no loğğinğ messağe 302013 no logging message 710005 no logging message 710003 no logging message 302018 no loğğinğ messağe 302017 no logging message 106100 no logging message 302016 no logging message 302015 no logging message 302021 no logging message 302014 no logging message 302020 no logging message 302013 mtu outside 1500 mtu inside 1500 no logging message 302018 no logging message 302017 mtu diagnostic 1500 no logging message 302016 no failover no logging message 302021 failover lan unit secondary failover lan interface FOVÉR GigabitEthernet1 no logging message 302020 mtu outside 1500 failover replication http mtu inside 1500 failover link STATE GigabitEthernet1/4 failover interface ip FOVER 10.10.1.1 255.255.2 mtu diagnostic 1500 no failover standby 10.10.1.2 icmp unreachable rate-limit 1 burst-size 1 failover interface ip STATE 10.10.2.1 255.255.2 no asdm history enable access-group CSM_FW_ACL_ global standby 10.10.2.2 icmp unreachable rate-limit 1 burst-size 1 timeout xlate 3:00:00 no asdm history enable access-group CSM_FW_ACL_ global timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 timeout xlate 3:00:00 sctp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 timeout conn-holddown 0:00:15 aaa proxy-limit disable snmp-server host outside 192.168.1.100 community ***** version 2c no snmp-server location no snmp-server contact ***** snmp-server community service sw-reset-button crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet timeout 5 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 no tcp-inspection policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esintp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http

timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:0 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 timeout conn-holddown 0:00:15 user-identity default-domain LOCAL aaa proxy-limit disable snmp-server host outside 192.168.1.100 commun ***** version 2c no snmp-server location no snmp-server contact snmp-server community ***** service sw-reset-button crypto ipsec security-association pmtu-aging infin crypto ca trustpool policy telnet timeout 5 console timeout 0 dynamic-access-policy-record DfltAccessPolicy class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum client auto message-length maximum 512 no tcp-inspection policy-map type inspect ip-options UM STATIC IP OPTIONS MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM STATIC IP OPTIONS I class class-default set connection advanced-options UM STATIC TCP MAP service-policy global_policy global prompt hostname context

https://tools.cisco.com/its/service/oddce/services/DDC EService destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:768a03e90b9d3539773b9d7af66b34 52	profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/ <u>EService</u> destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic mont subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:ac9b8f401e18491fee653f4cfe00
Delevery illete envetere even velvere envetere te berndere verere	de entie LIA witeeleelee weret de CTD

call-home

Belangrijkste punten om rekening mee te houden voor de optie HA uitschakelen vanaf de FTD CLI:

Primaire eenheid

Secundaire eenheid

Failover-configuratie en stand-by IPadressen worden verwijderd

- Interface-configuraties worden verwijderd
- - Het apparaat gaat naar de pseudo-stand-bymodus

Stap 6. Nadat u de taak heeft voltooid, registreert u de apparaten bij het FMC en schakelt u het HA-paar in.

Taak 7. HA opschorten

Taakvereiste:

Schort de HA op vanaf de FTD CLISH CLI

Oplossing:

Stap 1. Voer de opdracht uit op de primaire FTD en bevestig (typ YES).

> configure high-availability suspend Please ensure that no deployment operation is in progress before suspending high-availability. Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to abort: YES Successfully suspended high-availability. Stap 2. Verifieer de wijzigingen op de primaire eenheid:

> show high-availability config Failover Off Failover unit Primary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set

failover replication http Stap 3. Het resultaat op de secundaire eenheid:

> show high-availability config Failover Off (pseudo-Standby)

Failover unit Secondary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set failover replication http

Stap 4. Hervat HA op de primaire eenheid:

> configure high-availability resume Cuggogafully required high availablity

Successfully resumed high-availablity.

> .

>

> show high-availability config

Failover On

Failover unit Primary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set failover replication http

Stap 5. Het resultaat op de secundaire eenheid nadat HA is hervat:

> ..

Detected an Active mate Beginning configuration replication from mate.

WARNING: Failover is enabled but standby IP address is not configured for this interface. WARNING: Failover is enabled but standby IP address is not configured for this interface. End configuration replication from mate.

>

> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

Veelgestelde vragen (FAQ)

Als de configuratie wordt gerepliceerd, wordt deze dan onmiddellijk opgeslagen (per regel) of wanneer de replicatie is beëindigd?

Aan het einde van de replicatie. Het bewijs bevindt zich aan het einde van de output van de opdracht debug fover sync, waar de config/command-replicatie wordt getoond:

cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RULE: ACP_Rule_500 cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group group_10 eq 48894 object-group group_10 eq 23470 vlan eq 1392 rule-id 268442578 cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS POLICY: mzafeiro_500 - Default cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RULE: DEFAULT ACTION RULE cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_2 eq 32881 object-group group_433 eq 39084 vlan eq 1693 rule-id 268442076 cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACCESS POLICY: mzafeiro_ACP1500 - Mandatory cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7 RULE: ACP_Rule_1500 cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_6 eq 8988 object-group group_311 eq 32433 vlan eq 619 rule-id 268442077 cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACCESS POLICY: mzafeiro_ACP1500 - Default cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4 RULE: DEFAULT ACTION RULE cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078 event-log flow-start cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311 cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433 cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6 cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2 cli_xml_server: frep_write_cmd: Cmd: write memory <--</pre>

Wat gebeurt er als een eenheid zich in een pseudo-Standby-staat bevindt (failover uitgeschakeld) en u het opnieuw laadt terwijl de andere eenheid failover ingeschakeld is en actief is? U komt terecht in een Active/Active-scenario (hoewel dit technisch gezien Active/Failover-off is). Zodra de eenheid is geactiveerd, wordt de failover uitgeschakeld, maar de eenheid gebruikt dezelfde IP-adressen als de actieve eenheid. Er is dus effectief sprake van de volgende toestand:

- Eenheid-1: Active
- Eenheid-2: failover is uitgeschakeld. De unit gebruikt dezelfde gegevens-IP's als unit-1, maar verschillende MAC-adressen.

Wat gebeurt er met de failover-configuratie als u de failover handmatig uitschakelt ('configure high-availability suspend') en het apparaat vervolgens opnieuw laadt?

Wanneer u de failover uitschakelt, is dit geen permanente wijziging (wordt niet opgeslagen in de startup-config tenzij u dit expliciet doet). U kunt de eenheid op twee manieren opnieuw opstarten/opnieuw laden, en bij de tweede manier moet u extra zorgvuldig te werk gaan:

Situatie 1. Opnieuw opstarten vanaf CLISH

Bij opnieuw opstarten vanaf CLISH wordt er niet om een bevestiging gevraagd. De configuratiewijziging wordt dus niet opgeslagen in startup-config:

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you
wish to abort: YES
Successfully suspended high-availability.
```

Het in bedrijf stellen-configureren heeft de failover uitgeschakeld. In dit geval was de unit stand-by en kwam in de pseudo-stand-by-stand zoals verwacht om een actief/actief scenario te voorkomen:

firepower# show failover | include Failover
Failover Off (pseudo-Standby)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)

Het opstarten-config heeft de failover nog toegelaten:

```
firepower# show startup | include failover
failover
failover
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Start het apparaat opnieuw op vanaf CLISH (opdracht reboot):

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81_ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

Aangezien failover is ingeschakeld, zal zodra de eenheid actief is, het apparaat naar de onderhandelingsfase voor de failover gaan om te proberen de externe peer te detecteren:

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
```

Type help or '?' for a list of available commands. firepower> .

Detected an Active mate

Situatie 2. Opnieuw opstarten vanaf LINA CLI Bij opnieuw opstarten vanuit LINA (opdracht **reload**) wordt om een bevestiging gevraagd. Als u in dit geval [Y] 'ja' kiest, wordt de configuratiewijziging opgeslagen in startup-config:

firepower# reload System config has been modified. Save? [Y]es/[N]o: Y <-- Be careful. This will disable the failover in the startup-config Cryptochecksum: 31857237 8658f618 3234be7c 854d583a 8781 bytes copied in 0.940 secs Proceed with reload? [confirm] firepower# show startup | include failover no failover failover lan unit secondary failover lan interface FOVER Ethernet1/1 failover replication http failover link FOVER Ethernet1/1 failover interface ip FOVER 192.0.2.1 255.255.0 standby 192.0.2.2 failover ipsec pre-shared-key *****

Zodra de eenheid actief is, wordt de failover uitgeschakeld:

```
firepower# show failover | include Fail
Failover Off
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Opmerking: Om dit scenario te vermijden zorg ervoor dat wanneer u wordt gevraagd u niet de veranderingen in het opstarten -opstarten -opstarten -configureren.

Gerelateerde informatie

Alle versies van de Cisco Firepower Management Center-configuratiehandleiding vindt u hier https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

 Alle versies van de FXOS Chassis Manager- en CLI-configuratiehandleidingen vindt u hier <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfld-121950</u>

 Cisco Global Technical Assistance Center (TAC) raadt deze visuele handleiding ten zeerste aan voor diepgaande praktische kennis over Cisco Firepower Security Technologies van de volgende generatie:

http://www.ciscopress.com/title/9781587144806

• TechNotes voor alle configuratie en probleemoplossing die betrekking hebben op de Firepower-technologieën

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-serieshome.html

• Technische ondersteuning en documentatie – Cisco Systems

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.