Configure FTD High Availability on Firepower Appliances

Contents

Introduction Prerequisites Requirements Components Used Task 1. Verify Conditions Task 2. Configure FTD HA on FPR9300 Conditions Task 3. Verify FTD HA and License Task 4. Switch the Failover Roles Task 5. Break the HA Pair Task 6. Disable HA pair Task 7. Suspend HA Frequently Asked Questions (FAQ) Related Information

Introduction

This document describes how to configure and verify Firepower Threat Defense (FTD) High Availability (HA) (Active/Standby failover) on FPR9300.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- 2xCisco Firepower 9300 Security Appliance FXOS SW 2.0(1.23)
- FTD version 10.10.1.1 (build 1023)
- Firepower Management Center (FMC) SW 10.10.1.1 (build 1023)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: On an FPR9300 appliance with FTD, you can configure only inter-chassis HA. The two units in a HA configuration must meet the conditions mentioned here.

Task 1. Verify Conditions

Task requirement:

Verify that both FTD appliances meet the note requirements and can be configured as HA units.

Solution:

Step 1. Connect to the FPR9300 Management IP and verify the module hardware.

Verify the FPR9300-1 hardware.

<#root>

KSEC-FPR9K-1-A#

show server inventory

Server	Equipped PID	Equipped	VID Equipped Serial	(SN) Slot Status	Ackd Memory (MB) Ackd	Cores
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#					

Verify the FPR9300-2 hardware.

<#root>

KSEC-FPR9K-2-A#

show server inventory

Server	Equipped PID	Equipped VID	Equipped Serial (SN)	Slot Status	Ackd Memory (MB)	Ackd Cores
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
KSEC-FPF	R9K-2-A#					

Step 2. Log into the FPR9300-1 Chassis Manager and navigate to Logical Devices.

Verify the software version, number, and type of interfaces as shown in the images.

FPR9300-1

۲	Firepower_TD2	Standalone	Status: ok				
	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	6 online
	Ports: Data Interfaces	: Ethernet1/4 Ethernet1/6	Ethernet1/5	Attributes: Cluster Operational Status Firepower Management IP Management URL UUID	: not-applicable <u>: 10.62.148.69</u> : https://10.62.148.73/ : 98eba974-4f44-11e6-8edf-8b66b	c49edbő	

FPR9300-2

۲	Firepo	wer_TD	Standalone	Status: ok				
	Secu	rity Module	Application	Version	Management IP	Gateway	Management Port	Status
	Secur	ity Module 3	FTD	6.0.1.1.1023	10.62.148.72	10.62.148.1	Ethernet1/2	ine online
	Po	orts: Data Interfaces:	Ethernet1/4 E Ethernet1/6	thernet1/5	Attributes: Cluster Operational Status : Firepower Management IP : Management URL UUID :	: not-applicable :10.62.148.72 https://10.62.148.73/ fdd8b67e-3324-11e6-8a63-eee	869c62b45	

Task 2. Configure FTD HA on FPR9300

Task requirement:

Configure Active/Standby failover (HA) as per this diagram.



Solution:

Both FTD devices are already registered on the FMC as shown in the image.

0	FTD9300-1 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Fi	ilt
0	FTD9300-2 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Fi	ilte

Step 1. In order to configure FTD failover, navigate to **Devices > Device Management** and choose **Add High Availability** as shown in the image.



Step 2. Enter the **Primary Peer** and the **Secondary Peer** and choose **Continue** as shown in the image.

Add High Availabil	ity Pair	? X	5			
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	incel				

Warning: Ensure to select the correct unit as the primary unit. All configurations on the selected primary unit are replicated to the selected secondary FTD unit. As a result of replication, the current configuration on the secondary unit can be replaced.

Conditions

In order to create an HA between 2 FTD devices, these conditions must be met:

- Same model
- Same version- this applies to FXOS and to FTD major (first number), minor (second number), and maintenance (third number) must be equal.
- Same number of interfaces
- Same type of interfaces
- Both devices as part of the same group/domain in FMC.
- Have identical Network Time Protocol (NTP) configuration.
- Be fully deployed on the FMC without uncommitted changes.
- Be in the same firewall mode: routed or transparent.

Note: This must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.

- Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interfaces.
- Different hostname [Fully Qualified Domain Name (FQDN)] for both chassis. In order to check the chassis hostname, navigate to **FTD CLI** and run this command:

<#root>

firepower#

show chassis-management-url

https://

KSEC-FPR9K-1.cisco.com

:443//

Note: In post-6.3 FTD use the command show chassis detail.

<#root>

firepower#

```
show chassis detail
```

```
Chassis URL: https://KSEC-FPR4100-1:443//Chassis IP: 192.0.2.1Chassis Serial Number: JMX12345678Security Module: 1
```

If both chassis have the same name, change the name in one of them with the use of these commands:

<#root> 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
```

#

After you change the chassis name, unregister the FTD from the FMC and register it again. Then, proceed with the HA Pair creation.

Step 3. Configure the HA and state the links settings.

In your case, the state link has the same settings as the High Availability Link.

Choose Add and wait for a few minutes for the HA pair to be deployed as shown in the image.

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 Addres	s		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	1			
Key Generation:	Auto	~		

Step 4. Configure the Data interfaces (primary and standby IP addresses)

From the FMC GUI, choose the HA Edit as shown in the image.



Step 5. Configure the Interface settings as shown in the images.

Ethernet 1/5 interface.

Edit Physical	Interfac	ce .					? >
Mode:	None		*				
Name:	Inside		C Enabled	Man	agement Only		
Security Zone:			*				
Description:]	
General IPv4	IPv6	Advanced	Hardware Con	figuration			
IP Type: IP Address:	[Use Static II 192.168.75	p ¥		eg. 1.1.1.1/255.	255.255.228	or 1.1.1.1/25
						ОК	Cancel

Ethernet 1/6 interface.

Edit Physical	Interfac	e					? ×
Mode:	None		*	_			
Name:	Outside		🕑 Enab	led 🗌 Mar	agement Only		
Security Zone:			*				
Description:]	
General IPv	IPv6	Advanced	Hardware (Configuration			
IP Type:		Use Static I	P	*			
IP Address:		192.168.76	10/24		eg. 1.1.1.1/255.	255.255.228	or 1.1.1.1/25
						OK	Cancel

Step 6. Navigate to **High Availability** and choose the Interface Name **Edit** to add the standby IP addresses as shown in the image.

FTD9300 Cisco Firepower)_HA 9000 Series SM-36 Three	at Defense								
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP			
High Availat	oility Configuration	1								
High Availabilit	ty Link							State Link		
Interface						Ethernet1/4		Interface		
Logical Name						fover_link		Logical Name		
Primary IP						1.1.1.1		Primary IP		
Secondary IP						1.1.1.2		Secondary IP		
Subnet Mask						255.255.255.0		Subnet Mask		
IPsec Encrypt	ion					Disabled		Statistics		
Monitored I	nterfaces									
Interface Nam	me Act	tive IPv4	Standby I	Pv4	Active IPv6 - S	itandby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6
🚔 Inside	192	2.168.75.10								
diagnostic										
Outside	192	2.168.76.10								

Step 7. For the Inside interface as shown in the image.

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	
ОК Са	ncel

Step 8. Do the same for the Outside interface.

Step 9. Verify the result as shown in the image.

Monitored Interfaces								
Interface Name	Active IPv4	Standby IPv4						
🛍 Inside	192.168.75.10	192.168.75.11						
iagnostic								
Dutside	192.168.76.10	192.168.76.11						

Step 10. Stay on the High Availability tab, and configure Virtual MAC addresses as shown in the image.

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

Step 11. For the Inside Interface is as shown in the image.

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	decimal format such as	0123.	4567.89ab
	ок		Cancel

Step 12. Do the same for the Outside interface.

Step 13. Verify the result as shown in the image.

Interface Mac Addresses			
Physical Interface	Active Mac Address	Standby Mac Address	
Ethernet1/5	aaaa.bbbb.1111	aaaa.bbbb.2222	4
Ethernet1/6	aaaa.bbbb.3333	aaaa.bbbb.4444	6

Step 14. After you configure the changes, choose Save and Deploy.

Task 3. Verify FTD HA and License

Task requirement:

Verify the FTD HA settings and enabled Licenses from the FMC GUI and from FTD CLI.

Solution:

Step 1. Navigate to Summary and check the HA settings and enabled Licenses as shown in the image.

FTD9300	_HA										
Cisco Firepower	9000 Series SM-36 Three	at Defense Hig	h Availability								
Summary	High Availability	Devices	Routing	NAT	Interfaces	Inline Sets	DHCP				
	General						0	License			
	Name:			FTD93	AH_00		_	Base:	٢	Yes	
	Status:			0				Export-Controlled Feat	tures: Y	Yes	
	Primary Peer	r:		FTD93	00-1(Active)			Malware:	۲	Yes	
	Secondary P	eer:		FTD93	00-2(Standby)			Threat:	Y	Yes	
	Failover Hist	ory:		۹,				URL Filtering:	۲	Yes	

Step 2. From the FTD CLISH CLI, run these commands:

<#root>
>
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 rcv rerr xerr General sys cmd up time **RPC** services TCP conn UDP conn ARP tbl Xlate Timeout IPv6 ND tbl VPN IKEv1 SA VPN IKEv1 P2 VPN IKEv2 SA VPN IKEv2 P2 VPN CTCP upd VPN SDI upd VPN DHCP upd SIP Session SIP Tx SIP Pinhole Route Session Router ID User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table Logical Update Queue Information Cur Max Total Recv Q: Xmit Q:

Step 3. Do the same on the Secondary device.

>

Step 4. Run the show failover state command from the LINA CLI:

<#root>

firepower#

show failover state

 State
 Last Failure Reason
 Date/Time

 This host Primary Active
 None
 None

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

 ====Configuration State=== Sync Done ====Communication State=== Mac set
 Kaster

firepower#

Step 5. Verify the configuration from the Primary unit (LINA CLI):

<#root>

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
```

```
!
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
description LAN/STATE Failover Interface
!
```

```
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#
```

Task 4. Switch the Failover Roles

Task requirement:

From the FMC, switch the failover roles from Primary/Active, Secondary/Standby to Primary/Standby, Secondary/Active

Solution:

Step 1. Select the icon as shown in the image.



Step 2. Confirm the action on the pop-up window as shown in the image.



Step 3. Verify the result as shown in the image.



From the LINA CLI, you can see that the command **no failover active** was executed on the Primary/Active unit:

<#root>

```
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 failo
```

You can also verify it in the show failover history command output:

<#root>				
firepower#				
show failover history				
From State	To State	Reason		
10:39:26 EEST Jul 22 2016 Active	Standby Ready	Set by the config command		

Step 4. After the verification, make the Primary unit Active again.

Task 5. Break the HA Pair

Task requirement:

From the FMC, break the failover pair.

Solution:

Step 1. Select the icon as shown in the image.



Step 2. Check the notification as shown in the image.

Confin	m Break	×
2 - For	Breaking the High Availability pair "FTD9300_HA" will erase all configuration except the Acce Control policy from standby peer. Are you sure you want to break the pair? ce break, if standby peer does not respond	55
	Yes No	

Step 3. Note the message as shown in the image.



Step 4. Verify the result from the FMC GUI as shown in the image.



show running-config on the Primary unit before and after the HA break:

Before HA Break	After HA Break
firepower# sh run	firepower# sh run
: Saved	: Saved
:	:
: Serial Number: FLM19267A63	: Serial Number: FLM19267A63
: Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Hardware: FPR9K-SM-36, 135839 MB RAM, C 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 8Ry2YjIyt7RRXU24 encrypted	enable password 8Ry2YjIyt7RRXU24 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	no nameif
!	no security-level
interface Ethernet1/5	no ip address
nameif Inside	!
security-level 0	interface Ethernet1/5
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	nameif Inside
!	security-level 0
interface Ethernet1/6	ip address 192.168.75.10 255.255.255.0 standby 19
nameif Outside	!
security-level 0	interface Ethernet1/6
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	nameif Outside
!	security-level 0
ftp mode passive	ip address 192.168.76.10 255.255.255.0 standby 19
ngips conn-match vlan-id	!
access-list CSM_FW_ACL_ remark rule-id 268447744:	ftp mode passive
ACCESS FOLICT. FTD9500 - Mandatory/T	ngips conn-match vlan-id
RULE: Allow_ICMP	access-list CSM_FW_ACL_ remark rule-id 268447
access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both	access-list CSM_FW_ACL_ remark rule-id 268447 RULE: Allow ICMP
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1	access-list CSM_FW_ACL_ advanced permit icmp rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE	access-list CSM_FW_ACL_ remark rule-id 268441 ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ advanced permit ip any any rule- id 268441600	access-list CSM_FW_ACL_ remark rule-id 268441 RULE: DEFAULT ACTION RULE
!	

tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow urgent-flag allow no pager logging enable logging timestamp logging standby 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

access-list CSM_FW_ACL_ advanced permit ip any id 268441600 ۱ tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow urgent-flag allow no pager logging enable logging timestamp logging standby 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 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 0:02:0 0:02:00 icmp 0:00:02

no arp permit-nonconnected	timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
access-group CSM_FW_ACL_ global	
timeout xlate 3:00:00	timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:0 disconnect 0:02:00
timeout pat-xlate 0:00:30	timeout sip-provisional-media 0:02:00 uauth 0:05:0
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout tcp-proxy-reassembly 0:00:30
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout floating-conn 0:00:00 aaa proxy-limit disable
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip- disconnect 0:02:00	no snmp-server location
timeout sin-provisional-media 0:02:00 yauth 0:05:00 absolute	no snmp-server contact
timeout tcp-proxy-reassembly 0:00:30	no snmp-server enable traps snmp authentication lir linkdown coldstart warmstart
timeout floating-conn 0:00:00	crypto ipsec security-association pmtu-aging infinit
aaa proxy-limit disable	crypto ca trustpool policy
no snmp-server location	telnet timeout 5
no snmp-server contact	ssh stricthostkeycheck
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	ssh timeout 5
crypto ipsec security-association pmtu-aging infinite	ssh key-exchange group dh-group1-sha1
crypto ca trustpool policy	console timeout 0
telnet timeout 5	dynamic-access-policy-record DfitAccessPolicy
ssh stricthostkeycheck	
ssh timeout 5	class-map inspection_default
ssh key-exchange group dh-group1-sha1	match default-inspection-traffic
console timeout 0	!
dynamic-access-policy-record DfltAccessPolicy	!
!	policy-map type inspect dns preset_dns_map
class-man inspection default	parameters
match default increation traffic	message-length maximum client auto
	message-length maximum 512
· !	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

policy-map type inspect dns preset_dns_map	parameters
parameters	eool action allow
message-length maximum client auto	nop action allow
message-length maximum 512	router-alert action allow
policy-map type inspect ip-options	policy-map global_policy
DW_STATIC_II_OFTIONS_WAT	class inspection_default
eool action allow	inspect dns preset_dns_map
non action allow	inspect ftp
nop action allow	inspect h323 h225
router-alert action allow	inspect h323 ras
policy-map global_policy	inspect rsh
class inspection_default	inspect rtsp
inspect dns preset_dns_map	inspect sqlnet
inspect ftp	inspect skinny
inspect h323 h225	inspect sunrpc
inspect h323 ras	inspect xdmcp
inspect rsh	inspect sip
inspect rtsp	inspect netbios
inspect sqlnet	inspect tftp
inspect skinny	inspect icmp
inspect sunrpc	inspect icmp error
inspect xdmcp	inspect dcerpc
inspect sip	inspect ip-options UM_STATIC_IP_OPTIONS_M
inspect netbios	class class-default
inspect tftp	set connection advanced-options UM STATIC TO
inspect icmp	!
inspect icmp error	service-policy global policy global
inspect dcerpc	prompt hostname context
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	call-home

class class-default	profile CiscoTAC-1
set connection advanced-options UM_STATIC_TCP_MAP	no active
! service-policy global_policy global prompt hostname context	destination address http https://tools.cisco.com/its/service/oddce/services/Dl destination address email callhome@cisco.com
call-home	destination transport-method http subscribe-to-alert-group diagnostic
profile CiscoTAC-1 no active	subscribe-to-alert-group environment
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService	subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic mor
destination address email callhome@cisco.com	subscribe-to-alert-group telemetry periodic daily
destination transport-method http	Cryptochecksum:fb6f5c369dee730b9125650517dbl
subscribe-to-alert-group diagnostic	: end
subscribe-to-alert-group environment	firepower#
subscribe-to-alert-group inventory periodic monthly	
subscribe-to-alert-group configuration periodic monthly	
subscribe-to-alert-group telemetry periodic daily	
Cryptochecksum:933c594fc0264082edc0f24bad358031	
: end	
firepower#	

show running-config on the Secondary unit before and after the HA break as shown in the table here.

Before HA Break	After HA Break
firepower# sh run	firepower# sh run
: Saved	: Saved
:	:
: Serial Number: FLM19206H7T	: Serial Number: FLM19206H7T
: Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Hardware: FPR9K-SM-36, 135841 MB RAM, C 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 8Ry2YjIyt7RRXU24 encrypted	enable password 8Ry2YjIyt7RRXU24 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
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
172.100.73.11	shutdown
: intorfaga Ethornat1/6	no nameif
namoif Outsida	no security-level
socurity loyal 0	no ip address
in address 192 168 76 10 255 255 255 0 standby	!
192.168.76.11	interface Ethernet1/6
!	shutdown
ftp mode passive	no nameif
ngips conn-match vlan-id	no security-level
access-list CSM_FW_ACL_ remark rule-id 268447744:	no ip address

ACCESS POLICY: FTD9300 - Mandatory/1	!
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow ICMP	ftp mode passive
	ngips conn-match vlan-id
rule-id 268447744 event-log both	access-list CSM_FW_ACL_ remark rule-id 268447 ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1	access-list CSM_FW_ACL_ remark rule-id 268447 RULE: Allow ICMP
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE	access-list CSM_FW_ACL_ advanced permit icmp
access-list CSM FW ACL advanced permit ip any any rule-	rule-1d 268447744 event-log both
id 268441600	access-list CSM_FW_ACL_ remark rule-id 268441 ACCESS POLICY: FTD9300 - Default/1
tcp-map UM_STATIC_TCP_MAP	access-list CSM_FW_ACL_ remark rule-id 268441 RULE: DEFAULT ACTION RULE
tcp-options range 6 7 allow	access-list CSM_FW_ACL_ advanced permit ip an id 268441600
tcp-options range 9 255 allow	
urgent-flag allow	
!	tcp-map UM_STATIC_TCP_MAP
no pager	tcp-options range 6 7 allow
	tcp-options range 9 255 allow
logging enable	urgent-flag allow
logging timestamp	,
logging standby	
logging buffer-size 100000	no pager
logging buffered debugging	no logging message 106015
logging flash-minimum-free 1024	no logging message 313001
logging flach maximum allocation 2076	no logging message 313008
logging mash-maximum-anocation 5070	no logging message 106023
mtu diagnostic 1500	no logging message 710003
mtu Inside 1500	no logging message 106100
mtu Outside 1500	no logging moscogo 202015
failover	no logging message 502015
failover lan unit secondary	no logging message 302014
failover lan interface fover link Ethernet1/4	no logging message 302013
	no logging message 302018

failover replication http	no logging message 302017
failover mac address Ethernet1/5 aaaa.bbbb.1111	no logging message 302016
	no logging message 302021
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444	no logging message 302020
failover link fover_link Ethernet1/4	mtu diagnostic 1500
failover interface ip fover_link 10.10.1.1 255.255.255.0	no failover
standby 10.10.1.2	no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1	icmp unreachable rate-limit 1 burst-size 1
no asdm history enable	no asdm history enable
arp timeout 14400	arp timeout 14400
no arp permit-nonconnected	no arp permit-nonconnected
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
timeout xlate 3:00:00	timeout xlate 3:00:00
timeout pat-xlate 0:00:30	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 conn 1:00:00 half-closed 0:10:00 udp 0:02: 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 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 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 0:30:00 sip_media 0:02:00 sip-invite 0:0 disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout sip-provisional-media 0:02:00 uauth 0:05:0
timeout tcp-proxy-reassembly 0:00:30	timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00	timeout floating-conn 0:00:00
user-identity default-domain LOCAL	aaa proxy-limit disable
aaa proxy-limit disable	no snmp-server location
no snmp-server location	no snmp-server contact
no snmp-server contact	no sump-server enable trans sump authentication lir
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite	crypto ipsec security-association pmtu-aging infinit
crypto ca trustpool policy	crypto ca trustpool policy

telnet timeout 5	ssh stricthostkeycheck
ssh stricthostkeycheck	ssh timeout 5
ssh timeout 5	ssh key-exchange group dh-group1-sha1
ssh key-exchange group dh-group1-sha1	console timeout 0
console timeout 0	dynamic-access-policy-record DfltAccessPolicy
dynamic-access-policy-record DfltAccessPolicy	!
!	class-map inspection_default
class-map inspection_default	match default-inspection-traffic
match default-inspection-traffic	!
!	!
!	policy-map type inspect dns preset_dns_map
policy-map type inspect dns preset_dns_map	parameters
parameters	message-length maximum client auto
message-length maximum client auto	message-length maximum 512
message-length maximum 512	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	parameters
parameters	eool action allow
eool action allow	nop action allow
nop action allow	router-alert action allow
router-alert action allow	policy-map global_policy
policy-map global_policy	class inspection_default
class inspection_default	inspect dns preset_dns_map
inspect dns preset_dns_map	inspect ftp
inspect ftp	inspect h323 h225
inspect h323 h225	inspect h323 ras
inspect h323 ras	inspect rsh
inspect rsh	inspect rtsp
inspect rtsp	inspect sqlnet

inspect sqlnet	inspect skinny
inspect skinny	inspect sunrpc
inspect sunrpc	inspect xdmcp
inspect xdmcp	inspect sip
inspect sip	inspect netbios
inspect netbios	inspect tftp
inspect tftp	inspect icmp
inspect icmp	inspect icmp error
inspect icmp error	inspect dcerpc
inspect dcerpc	inspect ip-options UM_STATIC_IP_OPTIONS_MA
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	class class-default
class class-default	set connection advanced-options UM_STATIC_TC
set connection advanced-options 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 https://tools.cisco.com/its/service/oddce/services/DI
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService	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 monthly
subscribe-to-alert-group inventory periodic monthly	subscribe-to-alert-group configuration periodic mon
subscribe-to-alert-group configuration periodic monthly	subscribe-to-alert-group telemetry periodic daily
subscribe-to-alert-group telemetry periodic daily	Cryptochecksum:08ed87194e9f5cd9149fab3c0e9ce
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84	: end

: end	firepower#
firepower#	

Main points to note for the HA break:

figuration is removed.

Step 5. After you finish this task, recreate the HA pair.

Task 6. Disable HA pair

Task requirement:

From the FMC, disable the failover pair.

Solution:

Step 1. Choose the icon as shown in the image.



Step 2. Check the notification and confirm as shown in the image.



Step 3. After you delete the HA, both devices are unregistered (removed) from the FMC.

show running-config result from the LINA CLI is as shown in the table here:

Pr	rimary Unit	Secondary Unit
fir	epower# sh run	firepower# sh run
: S	Saved	: Saved

:
: Serial Number: FLM19206H7T
: Hardware: FPR9K-SM-36, 135841 MB RAM, C E5 series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 10.10.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
description LAN/STATE Failover Interface
!
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	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 POLICY: FTD9300 - Mandatory/1	access-list CSM_FW_ACL_ remark rule-id 268447 ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP	access-list CSM_FW_ACL_ remark rule-id 268447 RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both	access-list CSM_FW_ACL_ advanced permit icmp rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1	access-list CSM_FW_ACL_ remark rule-id 268441 ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE	access-list CSM_FW_ACL_ remark rule-id 268441 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule- id 268441600	access-list CSM_FW_ACL_ advanced permit ip an 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 buffered debugging
logging flash-minimum-free 1024	logging 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 aaaa.bbbb.2222	failover mac address Ethernet1/5 aaaa.bbbb.111 aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444	failover mac address Ethernet1/6 aaaa.bbbb.333 aaaa.bbbb.4444
failover link fover_link Ethernet1/4	failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	failover interface ip fover_link 10.10.1.1 255.255. standby 10.10.1.2
icmp unreachable rate-limit 1 burst-size 1	icmp unreachable rate-limit 1 -size 1
no asdm history enable	no asdm history enable
arp timeout 14400	arp timeout 14400
no arp permit-nonconnected	no arp permit-nonconnected
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
timeout xlate 3:00:00	timeout xlate 3:00:00
timeout pat-xlate 0:00:30	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 conn 1:00:00 half-closed 0:10:00 udp 0:02: 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 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 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 0:30:00 sip_media 0:02:00 sip-invite 0:0 disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout sip-provisional-media 0:02:00 uauth 0:05:0
timeout tcp-proxy-reassembly 0:00:30	timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00	timeout floating-conn 0:00:00
aaa proxy-limit disable	user-identity default-domain LOCAL
no snmp-server location	aaa proxy-limit disable
no snmp-server contact	no snmp-server location
no snmp-server enable traps snmp authentication linkup	no snmp-server contact

linkdown coldstart warmstart	no snmp-server enable traps snmp authentication lir
crypto ipsec security-association pmtu-aging infinite	arupto insee security association protu aging infinit
crypto ca trustpool policy	
telnet timeout 5	crypto ca trustpool policy
ssh stricthostkeycheck	telnet timeout 5
ssh timeout 5	ssh stricthostkeycheck
ssh key-exchange group dh-group1-sha1	ssh timeout 5
console timeout 0	ssh key-exchange group dh-group1-sha1
dynamic-access-policy-record DfltAccessPolicy	console timeout 0
	dynamic-access-policy-record DfltAccessPolicy
class man inspection default	!
match default increation traffic	class-map inspection_default
match default-inspection-traffic	match default-inspection-traffic
!	!
!	!
policy-map type inspect dns preset_dns_map	policy-map type inspect dns preset dns map
parameters	parameters
message-length maximum client auto	message-length maximum client auto
message-length maximum 512	message length maximum 512
policy-map type inspect ip-options	message-iengui maximum 512
UM_STATIC_IP_OPTIONS_MAP	UM_STATIC_IP_OPTIONS_MAP
parameters	parameters
eool action allow	eool action allow
nop action allow	nop action allow
router-alert action allow	router-alert action allow
policy-map global_policy	policy man global policy
class inspection_default	poncy-map grobal_poncy
inspect dns preset_dns_map	
inspect ftp	Inspect dns preset_dns_map
inspect h323 h225	inspect ftp
	inspect h323 h225

ſ

_		
i	nspect h323 ras	inspect h323 ras
i	nspect rsh	inspect rsh
i	nspect rtsp	inspect rtsp
i	nspect sqlnet	inspect sqlnet
i	nspect skinny	inspect skinny
i	nspect sunrpc	inspect sunrpc
i	nspect xdmcp	inspect xdmcp
i	nspect sip	inspect sip
i	nspect netbios	inspect netbios
i	nspect tftp	inspect tftp
i	nspect icmp	inspect icmp
i	nspect icmp error	inspect icmp error
i	nspect dcerpc	inspect dcerpc
i	nspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect ip-options UM_STATIC_IP_OPTIONS_M
с	lass class-default	class class-default
s	et connection advanced-options UM_STATIC_TCP_MAP	set connection advanced-options UM_STATIC_TC
!		!
s	ervice-policy global_policy global	service-policy global_policy global
p	rompt hostname context	prompt hostname context
с	all-home	call-home
p	rofile CiscoTAC-1	profile CiscoTAC-1
n	o active	no active
d h	estination address http https://tools.cisco.com/its/service/oddce/services/DDCEService	destination address http https://tools.cisco.com/its/service/oddce/services/D
d	estination address email callhome@cisco.com	destination address email callhome@cisco.com
d	estination transport-method http	destination transport-method http
s	ubscribe-to-alert-group diagnostic	subscribe-to-alert-group diagnostic
s	ubscribe-to-alert-group environment	subscribe-to-alert-group environment
s	ubscribe-to-alert-group inventory periodic monthly	subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly	subscribe-to-alert-group configuration periodic mon
subscribe-to-alert-group telemetry periodic daily	subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:933c594fc0264082edc0f24bad358031	Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbc
: end	: end
firepower#	firepower#
	·

Step 4. Both FTD devices were unregistered from the FMC:

<#root>

> show managers

No managers configured.

Main points to note for the Disable HA option in FMC:

Primary Unit	Secondary Unit
The device is removed from the FMC.	The device is removed from the FMC.
No configuration is removed from the FTD device.	No configuration is removed from the FTD device.

Step 5. Run this command to remove the failover configuration from the FTD devices:

<#root>

>

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.

Note: You have to run the command on both units

The result:

Primary Unit	Secondary Unit

> 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 Interface Policy 1 Monitored Interfaces 2 of 1041 maximum MAC Address Move Notification Interval not set >	> show fa Failover Failover Failover (up) Reconnect Unit Poll Interface seconds Interface Monitore MAC Ad failover r	ailover Off (pseudo-Standby) unit Secondary LAN Interface: FOVER Ethernet1/3.205 et timeout 0:00:00 frequency 1 seconds, holdtime 15 seconds Poll frequency 5 seconds, holdtime 25 Policy 1 d Interfaces 0 of 1041 maximum dress Move Notification Interval not set eplication http	
Primary		Secondary	
firepower# show run		firepower# show run	
!		!	
hostname firepower		hostname firepower	
enable password 8Ry2YjIyt7RRXU24 encrypted		enable password 8Ry2YjIyt7RRXU24 encry	pted
names		names	
arp timeout 14400		arp timeout 14400	
no arp permit-nonconnected		no arp permit-nonconnected	
arp rate-limit 16384		arp rate-limit 16384	
!		!	
interface GigabitEthernet1/1		interface GigabitEthernet1/1	
nameif outside		shutdown	
cts manual		no nameif	
propagate sgt preserve-untag		no security-level	
policy static sgt disabled trusted		no ip address	
security-level 0		!	
ip address 10.1.1.1 255.255.255.0 < standby IP v	was	interface GigabitEthernet1/2	

removed	shutdown
!	no nameif
interface GigabitEthernet1/2	no security-level
nameif inside	no ip address
cts manual	!
propagate sgt preserve-untag	interface GigabitEthernet1/3
policy static sgt disabled trusted	description LAN Failover Interface
security-level 0	!
ip address 192.168.1.1 255.255.255.0 < standby IP was	interface GigabitEthernet1/4
removed	description STATE Failover Interface
: interface GigabitEthernet1/3	!
description I AN Failover Interface	interface GigabitEthernet1/5
	shutdown
interface GigabitEthernet1/4	no nameif
description STATE Failover Interface	no security-level
	no ip address
interface GigabitEthernet1/5	!
shutdown	interface GigabitEthernet1/6
no nameif	shutdown
no security-level	no nameif
no in address	no security-level
!	no ip address
interface GigabitEthernet1/6	!
shutdown	interface GigabitEthernet1/7
no nameif	shutdown
no security-level	no nameif
no ip address	no security-level
!	no ip address
	!

interface GigabitEthernet1/7	interface GigabitEthernet1/8
shutdown	shutdown
no nameif	no nameif
no security-level	no security-level
no ip address	no ip address
!	!
interface GigabitEthernet1/8	interface Management1/1
shutdown	management-only
no nameif	nameif diagnostic
no security-level	cts manual
no ip address	propagate sgt preserve-untag
!	policy static sgt disabled trusted
interface Management1/1	security-level 0
management-only	no ip address
nameif diagnostic	!
cts manual	ftp mode passive
propagate sgt preserve-untag	ngips conn-match vlan-id
policy static sgt disabled trusted	access-list CSM_FW_ACL_ remark rule-id 9998: F
security-level 0	POLICY: Default Tunnel and Priority Policy
no ip address	DEFAULT TUNNEL ACTION RULE
!	access-list CSM_FW_ACL_ advanced permit ipini
ftp mode passive	rule-1d 9998
ngips conn-match vlan-id	access-list CSM_FW_ACL_ advanced permit 41 ar id 9998
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy	access-list CSM_FW_ACL_ advanced permit gre a id 9998
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE	access-list CSM_FW_ACL_ advanced permit udp a 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998	access-list CSM_FW_ACL_ remark rule-id 268435 ACCESS POLICY: FTD_HA - Default/1
access-list CSM_FW_ACL_ advanced permit 41 any any rule- id 9998	access-list CSM_FW_ACL_ remark rule-id 268435 RULE: DEFAULT ACTION RULE

access-list CSM_FW_ACL_ advanced permit gre any any rule- id 9998	access-list CSM_FW_ACL_ advanced permit ip an id 268435456
access-list CSM_FW_ACL_ advanced permit udp any any eq 3544 rule-id 9998	!
access-list CSM_FW_ACL_ remark rule-id 268435456: ACCESS POLICY: FTD_HA - Default/1	tcp-options range 6 7 allow
access-list CSM_FW_ACL_ remark rule-id 268435456: L4 RULE: DEFAULT ACTION RULE	tcp-options range 9 18 allow
access-list CSM_FW_ACL_ advanced permit ip any any rule- id 268435456	tcp-options md5 clear
!	urgent-flag allow
tcp-map UM_STATIC_TCP_MAP	!
tcp-options range 6 7 allow	no pager
tcp-options range 9 18 allow	logging enable
tcp-options range 20 255 allow	logging timestamp
tcp-options md5 clear	logging buffered debugging
urgent-flag allow	logging flash-minimum-free 1024
!	logging flash-maximum-allocation 3076
no pager	no logging message 106015
logging enable	no logging message 313001
logging timestamp	no logging message 313008
logging buffered debugging	no logging message 106023
logging flash-minimum-free 1024	no logging message 710005
logging flash-maximum-allocation 3076	no logging message 710003
no logging message 106015	no logging message 106100
no logging message 313001	no logging message 302015
no logging message 313008	no logging message 302014
no logging message 106023	no logging message 302013
no logging message 710005	no logging message 302018
no logging message 710003	no logging message 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
no logging message 302018	mtu inside 1500
no logging message 302017	mtu diagnostic 1500
no logging message 302016	no failover
no logging message 302021	failover lan unit secondary
no logging message 302020	failover lan interface FOVER GigabitEthernet1/3
mtu outside 1500	failover replication http
mtu inside 1500	failover link STATE GigabitEthernet1/4
mtu diagnostic 1500	failover interface ip FOVER 10.10.1.1 255.255.255 10.10.1.2
icmp unreachable rate-limit 1 burst-size 1	failover interface ip STATE 10.10.2.1 255.255.255 10.10.2.2
no asdm history enable	icmp unreachable rate-limit 1 burst-size 1
access-group CSM_FW_ACL_ global	no asdm history enable
00 community ***** version 2c	access-group CSM_FW_ACL_ global
no snmp-server location	timeout xlate 3:00:00
no snmp-server contact	timeout pat-xlate 0:00:30
snmp-server community ****	timeout conn 1:00:00 half-closed 0:10:00 udp 0:02: 0:02:00 icmp 0:00:02
crypto ipsec security-association pmtu-aging infinite	timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 0:05:00 mgcp-pat 0:05:00
crypto ca trustpool policy	timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:
telnet timeout 5	
console timeout 0	timeout sip-provisional-media 0:02:00 uauth 0:05:0
dynamic-access-policy-record DfltAccessPolicy	timeout tcp-proxy-reassembly 0:00:30
!	timeout floating-conn 0:00:00
class-map inspection_default	timeout conn-holddown 0:00:15
match default-inspection-traffic	user-identity default-domain LOCAL
!	aaa proxy-limit disable
1	

!	snmp-server host outside 192.168.1.100 community version 2c
policy-map type inspect dns preset_dns_map	no snmp-server location
parameters	no snmp-server contact
message-length maximum client auto	snmp-server community ****
message-length maximum 512	service sw reset button
no tcp-inspection	service sw-reset-button
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	crypto ca trustpool policy
parameters	telnet timeout 5
eool action allow	console timeout 0
nop action allow	dynamic-access-policy-record DfltAccessPolicy
router-alert action allow	!
policy-map global_policy	class-map inspection_default
class inspection_default	match default-inspection-traffic
inspect dns preset_dns_map	!
inspect ftp	!
inspect h323 h225	policy-map type inspect dns preset_dns_map
inspect h323 ras	parameters
inspect rsh	message-length maximum client auto
inspect rtsp	message-length maximum 512
inspect esmtp	no tcp-inspection
inspect sqlnet	policy-map type inspect ip-options
inspect skinny	UM_STATIC_IP_OPTIONS_MAP
inspect sunrpc	parameters
inspect xdmcp	eool action allow
inspect sip	nop action allow
inspect netbios	router-alert action allow
inspect tftp	policy-map global_policy
inspect icmp	class inspection_default
	inspect dns preset_dns_map

inspect icmp error	inspect ftp
inspect dcerpc	inspect h323 h225
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect h323 ras
class class-default	inspect rsh
set connection advanced-options UM_STATIC_TCP_MAP	inspect rtsp
!	inspect esmtp
service-policy global_policy global	inspect sqlnet
prompt hostname context	inspect skinny
call-home	inspect sunrpc
profile CiscoTAC-1	inspect xdmcp
no active	inspect sip
destination address http	inspect netbios
https://tools.cisco.com/its/service/oddce/services/DDCEService	inspect tftp
destination address email callhome@cisco.com	inspect icmp
destination transport-method http	inspect icmp error
subscribe-to-alert-group diagnostic	inspect dcerpc
subscribe-to-alert-group environment	inspect ip-options UM_STATIC_IP_OPTIONS_N
subscribe-to-alert-group inventory periodic monthly	class class-default
subscribe-to-alert-group configuration periodic monthly	set connection advanced-options UM_STATIC_T
subscribe-to-alert-group telemetry periodic daily	!
Cryptochecksum:768a03e90b9d3539773b9d7af66b3452	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/D
	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:ac9b8f401e18491fee653f4cfe0ce2
I

Main points to note for the Disable HA from FTD CLI:

Primary Unit	Secondary Unit
Failover configuration and standby IPs aretimeout 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	• Interface configurations are removed.
sip-invite 0:03:00 sip-disconnect 0:02:00	The device goes into Pseudo- Standby mode.
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	

192.168.1.1 removed.	
----------------------	--

Step 6. After you finish the task, register the devices to the FMC and enable HA pair.

Task 7. Suspend HA

Task requirement:

Suspend the HA from the FTD CLISH CLI

Solution:

Step 1. On the Primary FTD, run the command and confirm (type YES).

<#root>

> 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 a
```

YES

Successfully suspended high-availability.

Step 2. Verify the changes on Primary unit:

<#root>

>

```
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
```

Step 3. The result on Secondary unit:

<#root>

>

```
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
```

Step 4. Resume HA on Primary unit:

<#root>

>

configure high-availability resume

```
Successfully resumed high-availablity.
```

> .

>

<#root>

>

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
```

Step 5. The result on the Secondary unit after you resume HA:

<#root>

> ..

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 >

Frequently Asked Questions (FAQ)

When the configuration is replicated, is it saved immediately (line-by-line) or at the end of the replication?

At the end of the replication. The evidence is at the end of the **debug fover sync** command output which shows the config/command replication:

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RULE
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RULE
. . .
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_2
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACCE
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7 F
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_(
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4 F
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
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:
```

What happens if a unit is in a pseudo-Standby state (failover disabled) and then you reload it while the other unit has failover enabled and is Active?

You end up in an Active/Active scenario (although technically it is an Active/Failover-off). Specifically, once the unit comes UP the failover is disabled, but the unit uses the same IPs as the Active unit. So effectively, you have:

- Unit-1: Active
- Unit-2: failover is off. The unit uses the same data IPs as Unit-1, but different MAC addresses.

What happens to the failover configuration if you manually disable the failover (configure high-availability suspend), and then you reload the device?

When you disable the failover, it is not a permanent change (not saved in the startup-config unless you decide to do this explicitly). You can reboot/reload the unit in 2 different ways and with the second way you must be careful:

Case 1. Reboot from CLISH

Reboot from CLISH does not ask for confirmation. Thus, the configuration change is not saved into startupconfig:

<#root>

>

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 a

YES

```
Successfully suspended high-availability.
```

The running-config has the failover disabled. In this case, the unit was Standby and got into the pseudo-Standby state as expected in order to avoid an Active/Active scenario:

<#root>

firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

```
)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

The startup-config has the failover still enabled:

<#root>

firepower#

show startup | include 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 *****

Reboot the device from CLISH (reboot command):

<#root>

>

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 ...
```

Once the unit is UP, since the failover is enabled, the device enters the failover Negotiation phase and tries to detect the remote peer:

<#root>

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

Case 2. Reboot from LINA CLI

Reboot from LINA (**reload** command) asks for confirmation. Thus, in case you select **Y** (Yes) the configuration change is saved into startup-config:

<#root> 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 192.0.2.1 255.255.255.0 standby 192.0.2.2 failover ipsec pre-shared-key *****

Once the unit is UP the failover is disabled:

<#root>

firepower#

show failover | include Fail

Failover Off

```
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Note: To avoid this scenario, ensure that when you are prompted, you do not save the changes to the startup-config.

Related Information

• All versions of the Cisco Firepower Management Center configuration guide can be found here

Navigating the Cisco Secure Firewall Threat Defense Documentation

• All versions of the FXOS Chassis Manager and CLI configuration guides can be found here

Navigating the Cisco Firepower 4100/9300 FXOS Documentation

• Cisco Global Technical Assistance Center (TAC) strongly recommends this visual guide for in-depth practical knowledge on Cisco Firepower Next-Generation Security Technologies:

<u>Cisco Firepower Threat Defense (FTD): Configuration and Troubleshooting Best Practices for the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP)</u>

• For all Configuration and Troubleshoot TechNotes that pertain to the Firepower technologies

Cisco Secure Firewall Management Center

<u>Technical Support & Documentation - Cisco Systems</u>