Configure FTD High Availability on Firepower Appliances

Contents

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 running 2.0(1.23)
- FTD running 6.0.1.1 (build 1023)
- Firepower Management Center (FMC) running 6.0.1.1 (build 1023)

Lab completion time: 1 hour

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 a 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 it 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.

```
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-FPR9K-1-A#
```

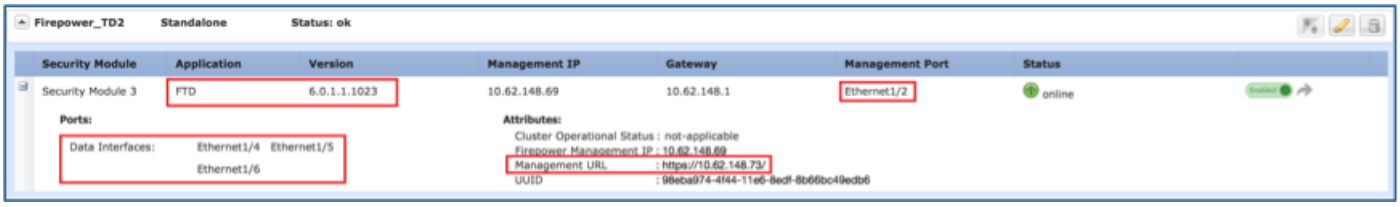
Verify the FPR9300-2 hardware.

```
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-FPR9K-2-A#
```

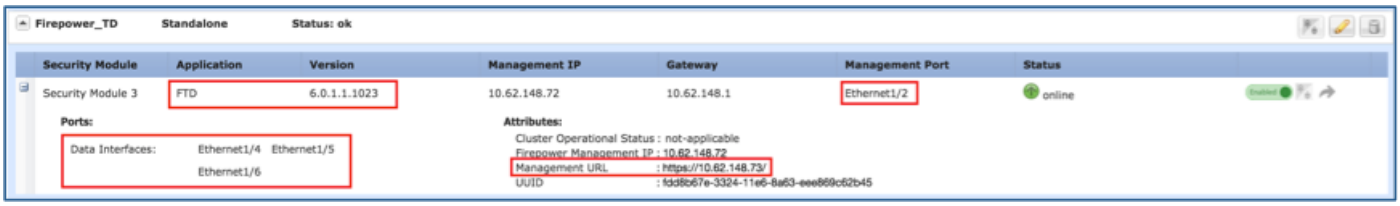
Step 2. Log into the FPR9300-1 Chassis Manager and navigate to Logical Devices.

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

FPR9300-1



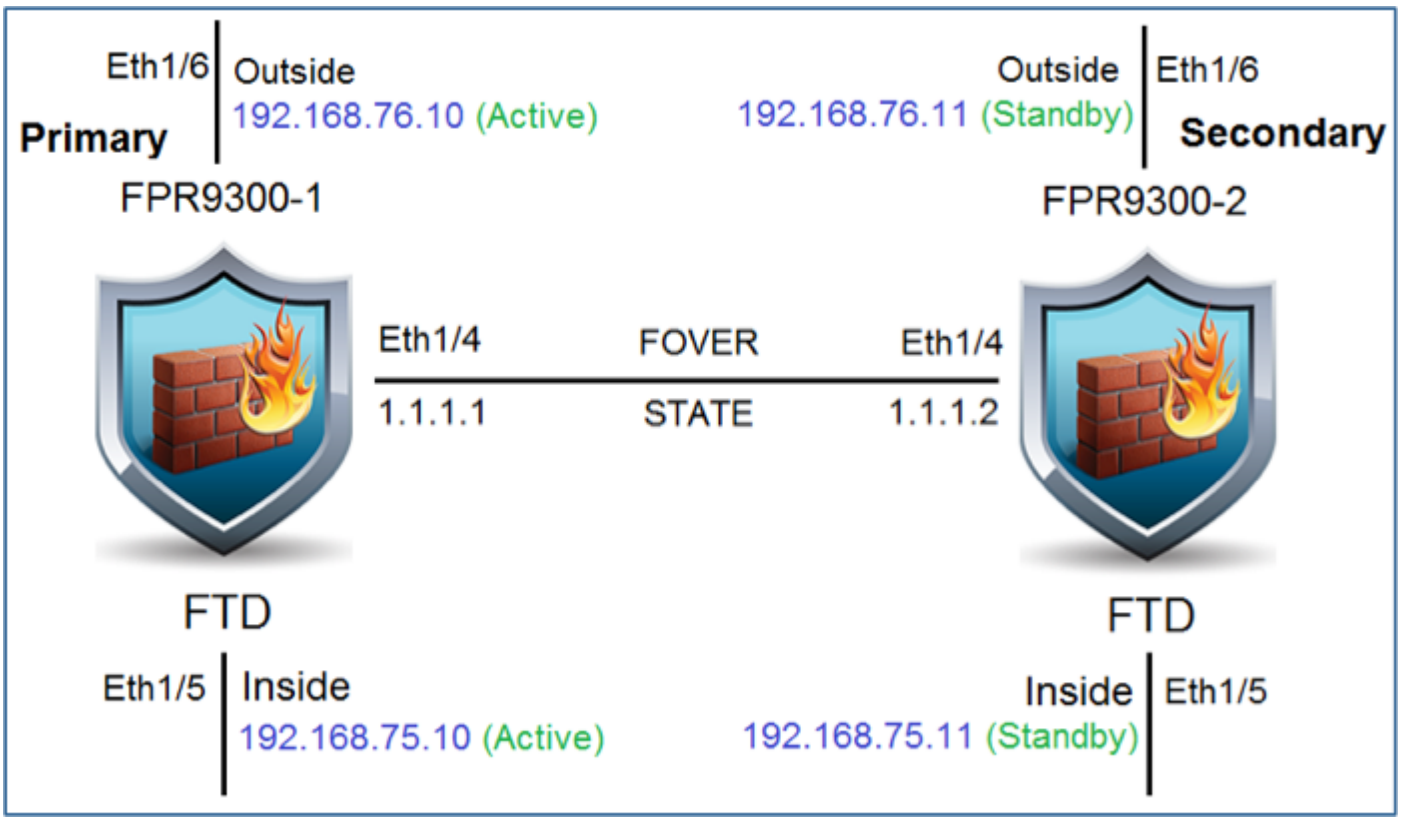
FPR9300-2



Task 2. Configure FTD HA on FPR9300

Task requirement:

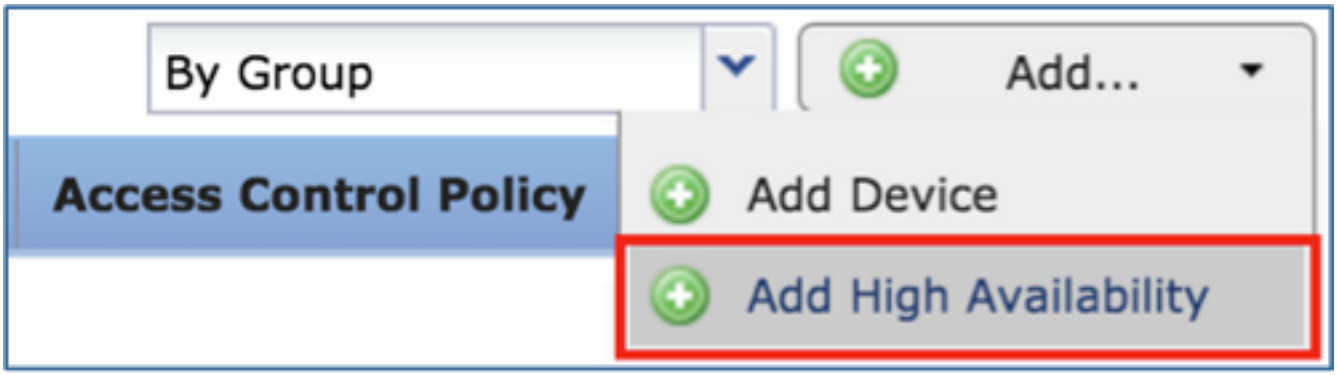
Configure Active/Standby failover (HA) as per this diagram.



Solution:

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

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



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

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 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 that 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.
- 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 go to FTD CLI and run this command:

```
firepower# show chassis-management-url

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

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

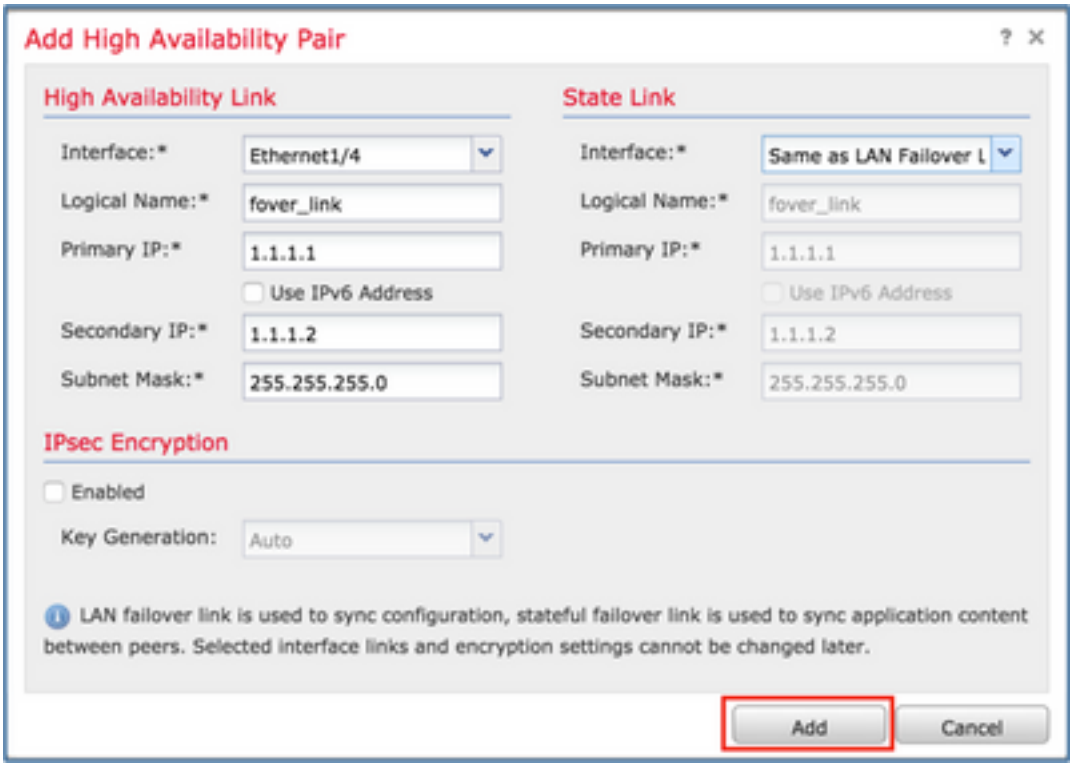
```
KSEC-FPR9K-1-A# scope system
KSEC-FPR9K-1-A /system # set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* # commit-buffer
FPR9K-1-A /system # exit
FPR9K-1new-A#
```

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.

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

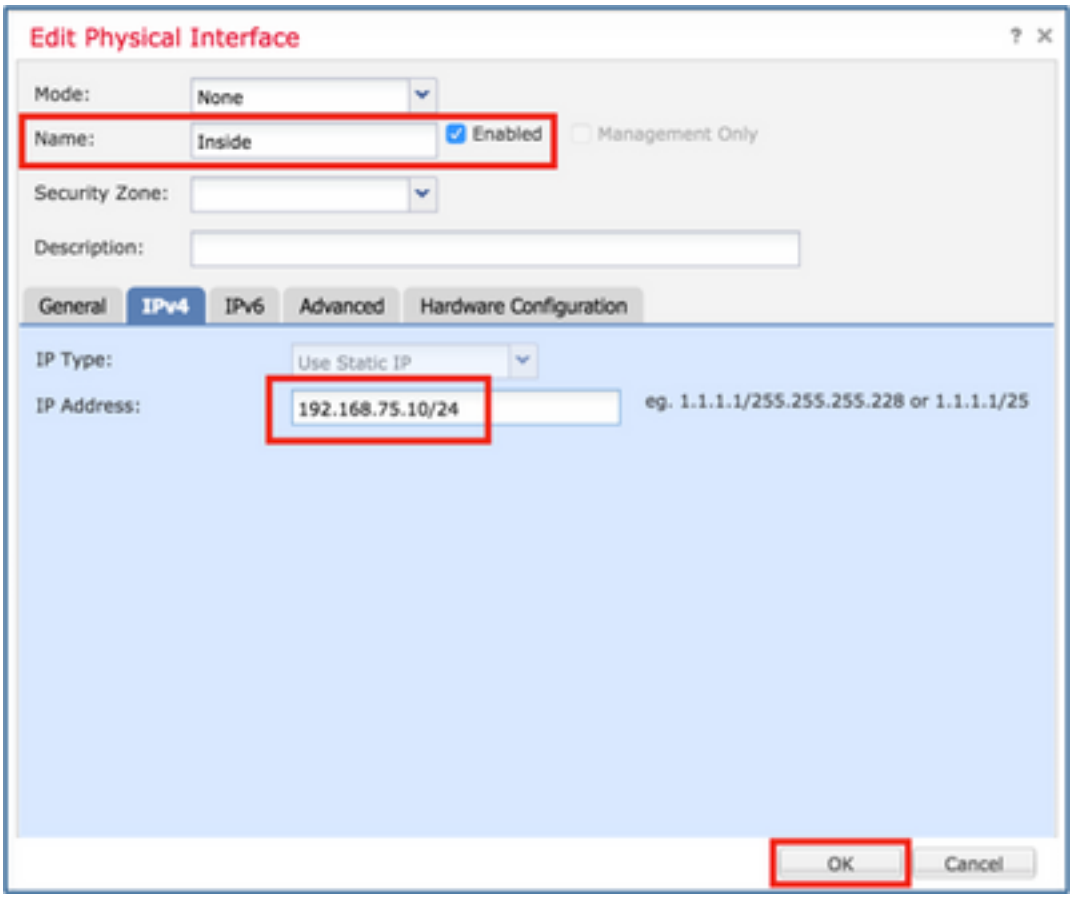


Step 4. Configure the Data interfaces (primary and standby IP addresses)

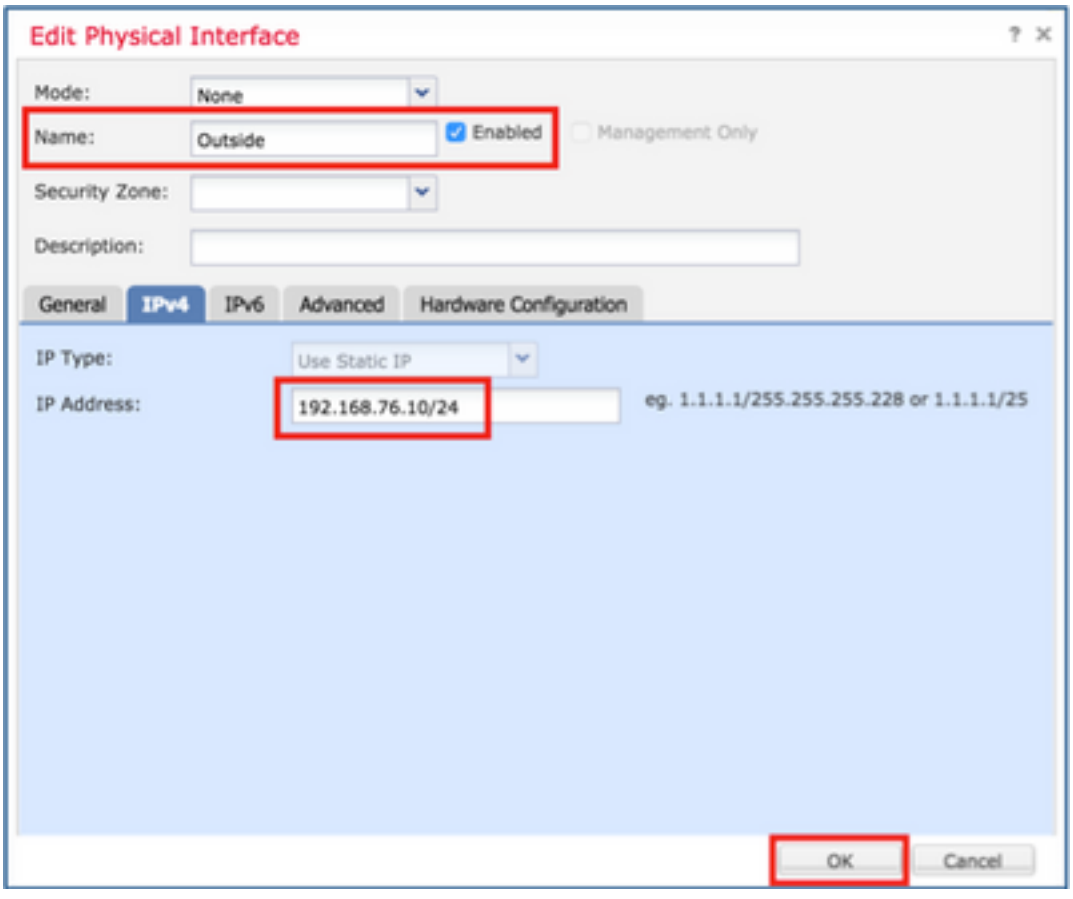
From the FMC GUI, click on the HA **Edit** as shown in the image.

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

Ethernet 1/5 interface.

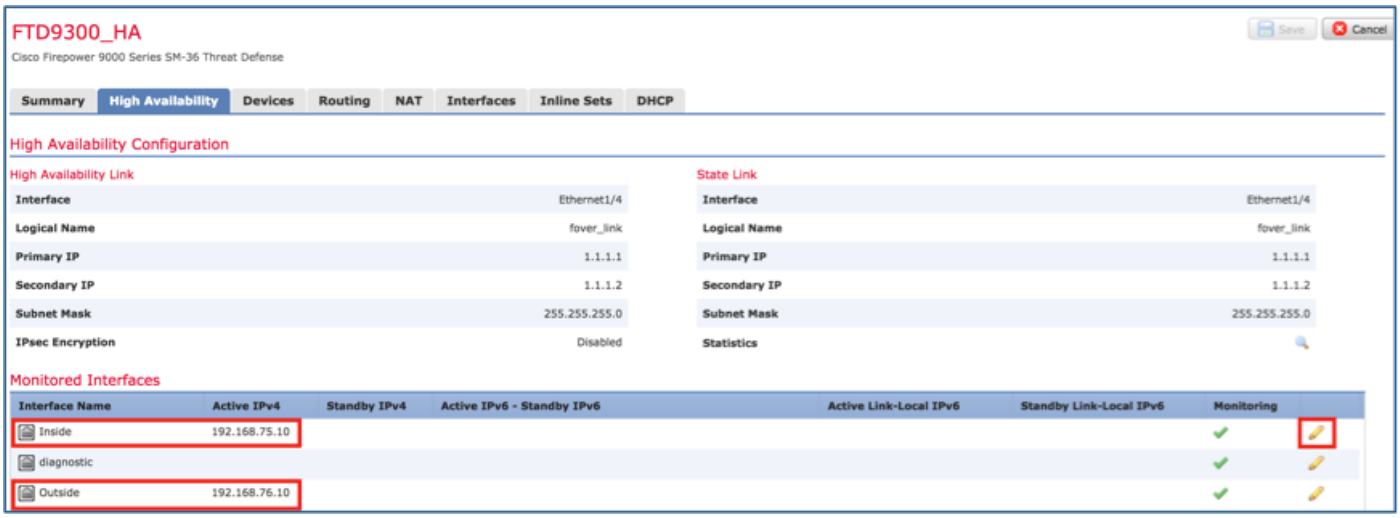


Ethernet 1/6 interface.

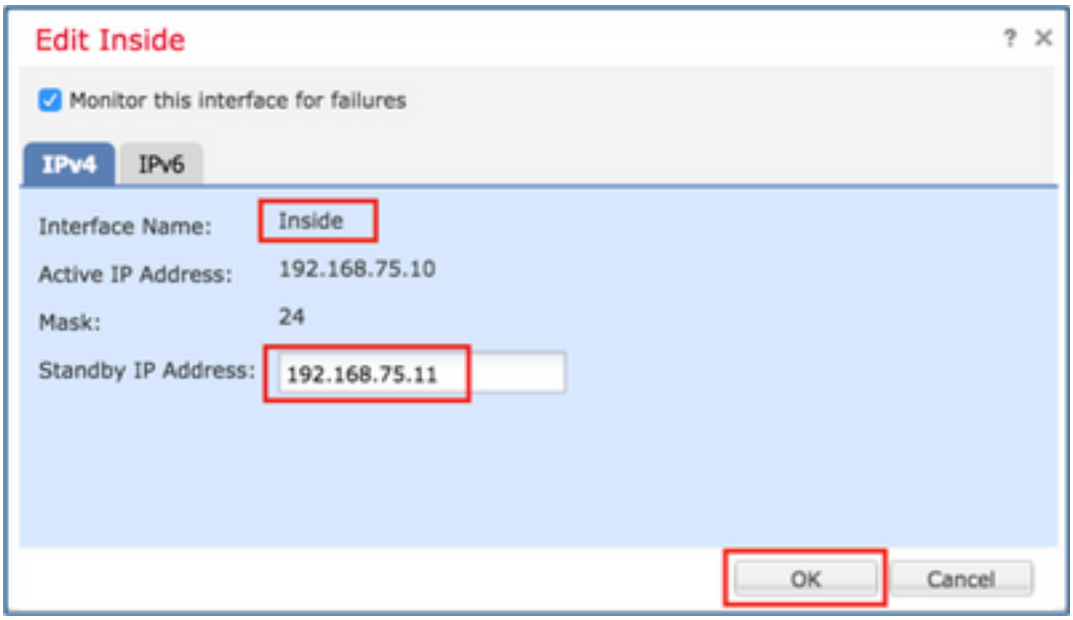


Step 6. Navigate to **High Availability** and click on the Interface Name **Edit** to add the standby IP

addresses as shown in the image.

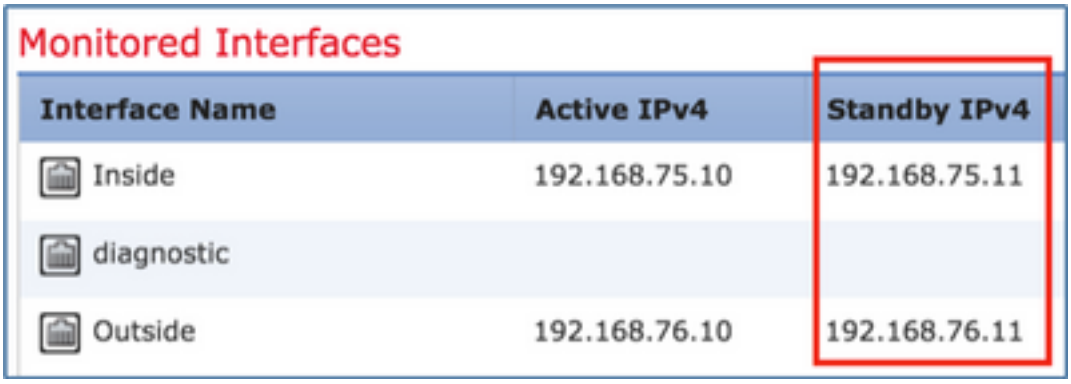


Step 7. For the Inside interface as shown in the image.

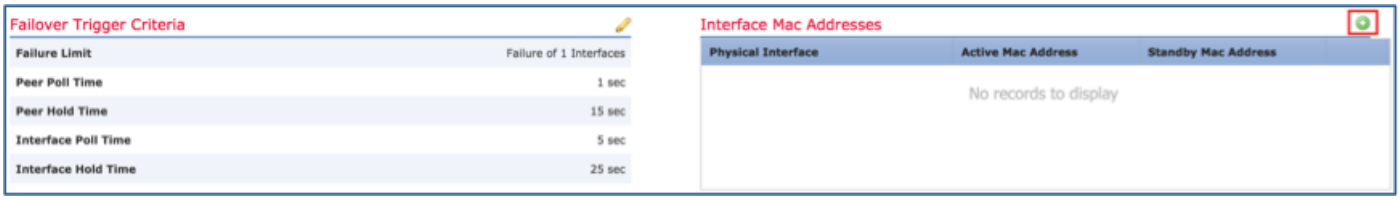


Step 8. Do the same for the Outside interface.

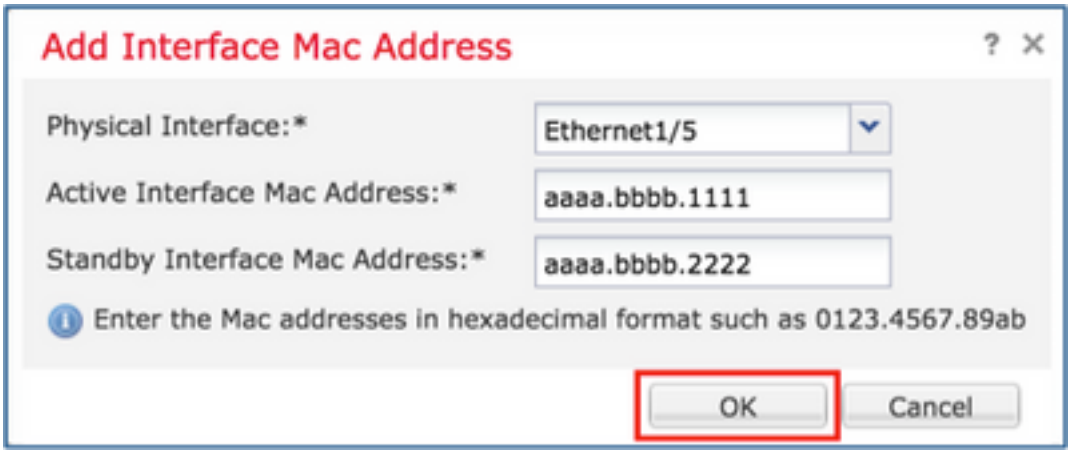
Step 9. Verify the result as shown in the image.



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



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



Step 12. Do the same for the Outside interface.

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

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

Task 3. Verify FTD HA and Licensing

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.

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

```
> 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
UDP conn 0          0          0          0
ARP tbl  0          0          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
VPN IKEv2 SA 0          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
SIP Session 0          0          0          0
SIP Tx 0          0          0          0
```

```
SIP Pinhole 0          0          0          0
Route Session 0          0          0          0
Router ID 0          0          0          0
User-Identity 1          0          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 Queue Information
  Cur Max Total
Recv Q: 0 10 416
Xmit Q: 0 11 2118

>
```

Step 3. Do the same on the Secondary device.

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

```
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   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

firepower#
```

Step 5. Verify the running configuration from the Primary unit (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 1.1.1.1 255.255.255.0 standby 1.1.1.2
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. Switching Failover Roles

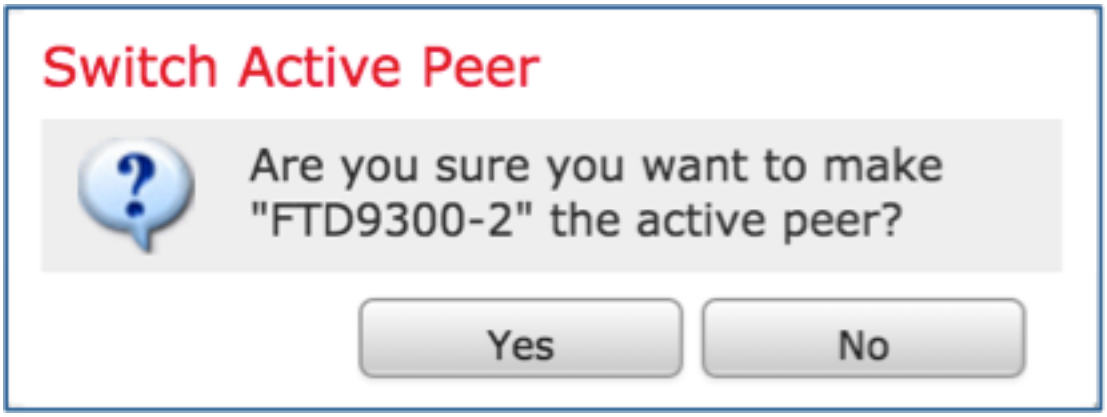
Task requirement:

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

Solution:

Step 1. Click on 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:

```
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'
```

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

```
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. Breaking HA Pair

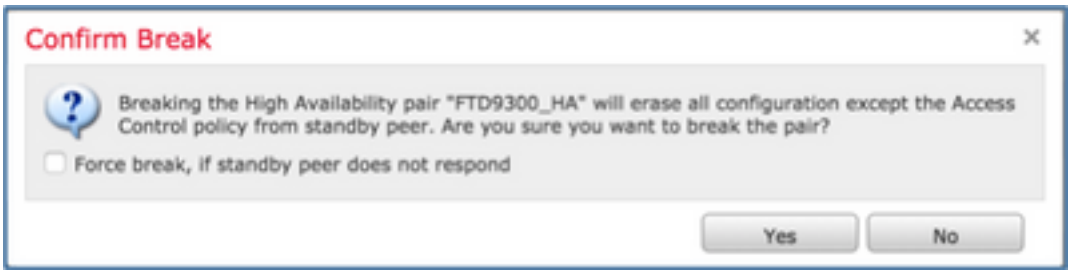
Task requirement:

From the FMC, break the failover pair.

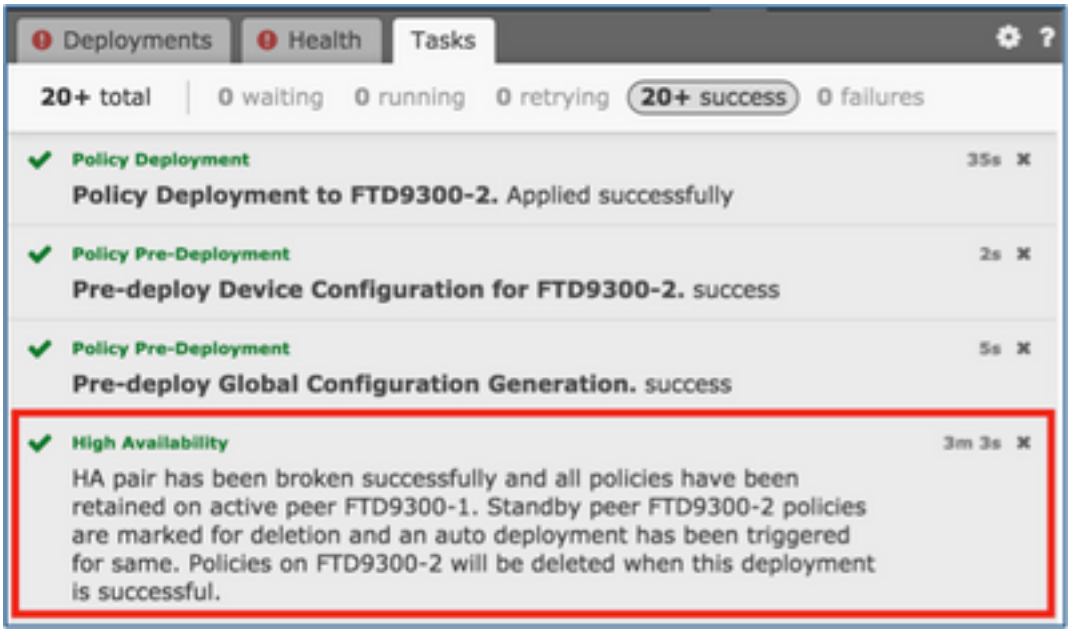
Solution:

Step 1. Click on the icon as shown in the image.

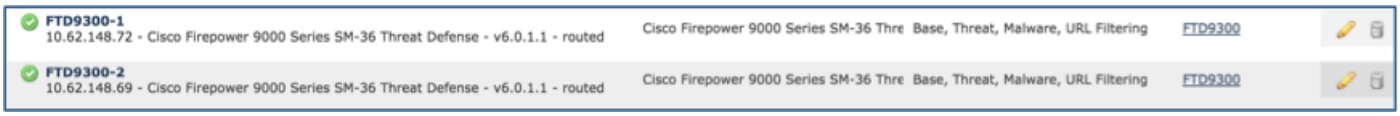
Step 2. Check the notification as shown in the image.



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 breaking the HA:

Before HA Break

```
firepower# sh run
: Saved
:
: Serial Number: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5
series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 6.0.1.1
!
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
!
ftp mode passive
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 268447744: L4
RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any any
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 268441600: L4
```

After HA Break

```
firepower# sh run
: Saved
:
: Serial Number: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB
series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 6.0.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 enc
names
!
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
no nameif
no security-level
no ip address
!
interface Ethernet1/5
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0
192.168.75.11
!
interface Ethernet1/6
nameif Outside
security-level 0
ip address 192.168.76.10 255.255.255.0
192.168.76.11
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-i
ACCESS POLICY: FTD9300 - Mandatory
access-list CSM_FW_ACL_ remark rule-i
RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced pe
rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-i
```

RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600
!
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 1.1.1.1 255.255.255.0 standby 1.1.1.2
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

ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-i
RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced pe
268441600
!
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
0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h22
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uau
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 authe
linkdown coldstart warmstart
crypto ipsec security-association pmtu-ag
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 DfltAccess

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/DDCEService
destination address email callhome@cisco.com
destination transport-method http
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_
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_OPTI
class class-default
set connection advanced-options UM_ST
!
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/s
destination address email callhome@cisc
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodi
subscribe-to-alert-group configuration per
subscribe-to-alert-group telemetry periodi
Cryptochecksum:fb6f5c369dee730b9125
: end

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:933c594fc0264082edc0f24bad358031
: end
firepower#

firepower#

show running-config on the Secondary unit before and after breaking the HA is 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 series 2294 MHz, 2 CPUs (72 cores)
:	:
NGFW Version 6.0.1.1	NGFW Version 6.0.1.1
!	!
hostname firepower	hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted	enable password 8Ry2YjIyt7RRXU24 enc
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 192.168.75.11	**interface Ethernet1/5**
!	**shutdown**
interface Ethernet1/6	**no nameif**
nameif Outside	**no security-level**
security-level 0	**no ip address**
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	**!**
!	**interface Ethernet1/6**
ftp mode passive	**shutdown**
ngips conn-match vlan-id	**no nameif**
access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1	**no security-level**
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP	**no ip address**
	!
	ftp mode passive
	ngips conn-match vlan-id
	access-list CSM_FW_ACL_ remark rule-i

access-list CSM_FW_ACL_ advanced permit icmp any any 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 268441600: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600
!
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 secondary
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 1.1.1.1 255.255.255.0 standby 1.1.1.2
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
user-identity default-domain LOCAL

ACCESS POLICY: FTD9300 - Mandatory
access-list CSM_FW_ACL_ remark rule-i
RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced pe
rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-i
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-i
RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced pe
268441600
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 255 allow
urgent-flag allow
!
no pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu diagnostic 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
0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h22
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uau
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
aaa proxy-limit disable
no snmp-server location

```
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
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
no snmp-server contact
no snmp-server enable traps snmp authe
linkdown coldstart warmstart
crypto ipsec security-association pmtu-ag
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 DfltAccess
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_
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_OPTI
class class-default
set connection advanced-options UM_ST
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
```

profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService 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:e648f92dd7ef47ee611f2aaa5c6cbd84 : end firepower#	destination address http https://tools.cisco.com/its/service/oddce/s destination address email callhome@cisc destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodi subscribe-to-alert-group configuration per subscribe-to-alert-group telemetry periodi Cryptochecksum:08ed87194e9f5cd9149f : end firepower#

Main points to note for breaking the HA:

Primary FTD	Secondary FTD
All failover configuration is removed Standby IP's remain	All configuration is removed

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

Task 6. Disable HA pair

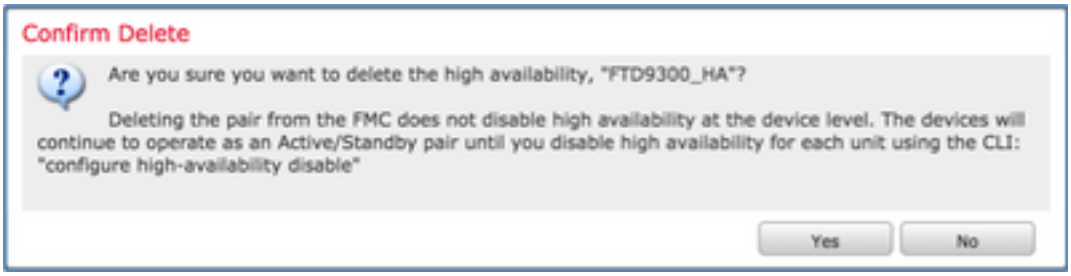
Task requirement:

From the FMC, disable the failover pair.

Solution:

Step 1. Click on 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:

Primary Unit	Secondary Unit

```
firepower# sh run
: Saved
:
: Serial Number: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5
series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 6.0.1.1
!
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
!
ftp mode passive
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 268447744: L4
RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any any
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 268441600: L4
RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id
268441600
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 255 allow
urgent-flag allow
```

```
firepower# sh run
: Saved
:
: Serial Number: FLM19206H7T
: Hardware:   FPR9K-SM-36, 135841 MB
series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 6.0.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 enc
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
192.168.75.11
!
interface Ethernet1/6
nameif Outside
security-level 0
ip address 192.168.76.10 255.255.255.0
192.168.76.11
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-i
ACCESS POLICY: FTD9300 - Mandatory
access-list CSM_FW_ACL_ remark rule-i
RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced pe
rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-i
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-i
RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced pe
268441600
!
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 1.1.1.1 255.255.255.0 standby 1.1.1.2
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
!

!
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 secondary
failover lan interface fover_link Ethern
failover replication http
failover mac address Ethernet1/5 aaaa
aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa
aaaa.bbbb.4444
failover link fover_link Ethernet1/4
failover interface ip fover_link 1.1.1.1 2
standby 1.1.1.2
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
0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h22
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uau
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 authe
linkdown coldstart warmstart
crypto ipsec security-association pmtu-ag
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 DfltAccess

```
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/DDCEService
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:933c594fc0264082edc0f24bad358031
: end
firepower#
```

```
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_
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_OPTI
class class-default
set connection advanced-options UM_ST
!
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/s
destination address email callhome@cisc
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodi
subscribe-to-alert-group configuration per
subscribe-to-alert-group telemetry periodi
Cryptochecksum:e648f92dd7ef47ee611f2
: end
```

firepower#

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

```
> show managers
No managers configured.
```

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

```
> 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.
```

Main points to note for disabling the HA:

Primary FTD	Secondary FTD
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 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 by typing **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.
```

Step 2. Verify the changes on Primary unit:

```
> 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:

```
> 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:

```
> configure high-availability resume
Successfully resumed high-availablity.

> .

No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>

> 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:

```
> ..

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
>
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

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

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

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

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfId-121950

- Cisco Global Technical Assistance Center (TAC) strongly recommends this visual guide for in-depth practical knowledge on Cisco Firepower Next Generation Security Technologies, including the ones mentioned in this article.

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

- For all Configuration and Troubleshooting TechNotes that pertains to the Firepower technologies

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

- Technical Support & Documentation - Cisco Systems