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 - 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-FPR9K-1-A#
```

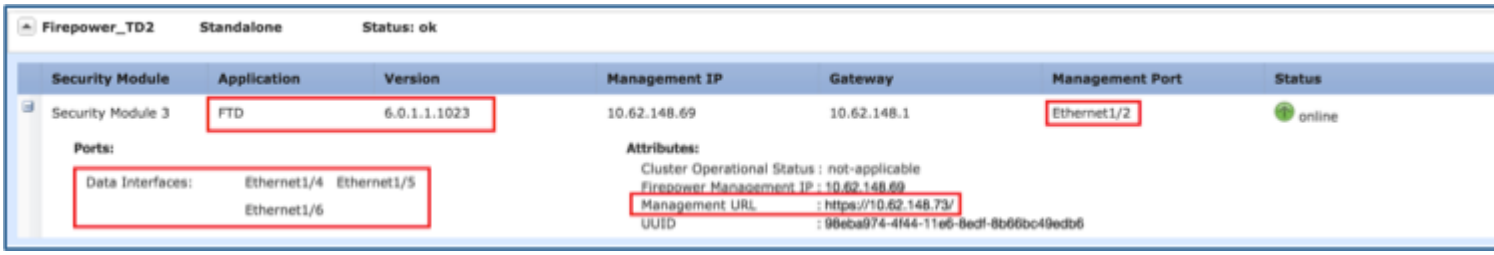
Verify the FPR9300-2 hardware.

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

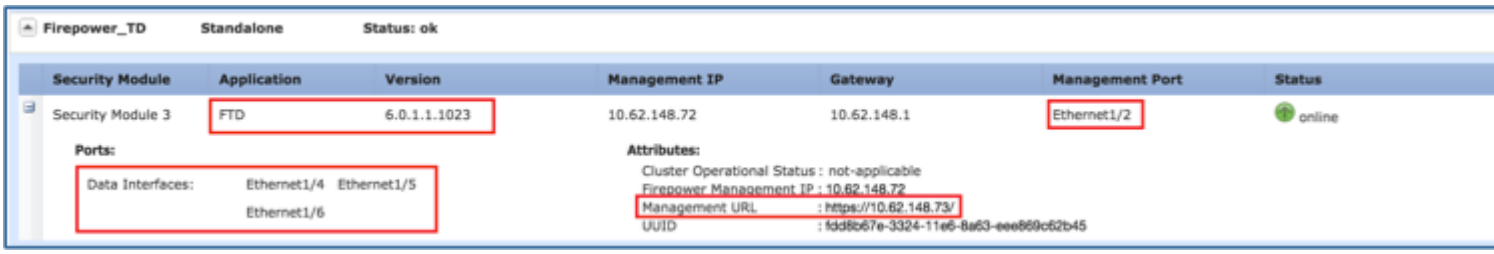
Step 2. Log into the FPR9300-1 Chassis Manager and navigate to **Logical Devices**.

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

FPR9300-1



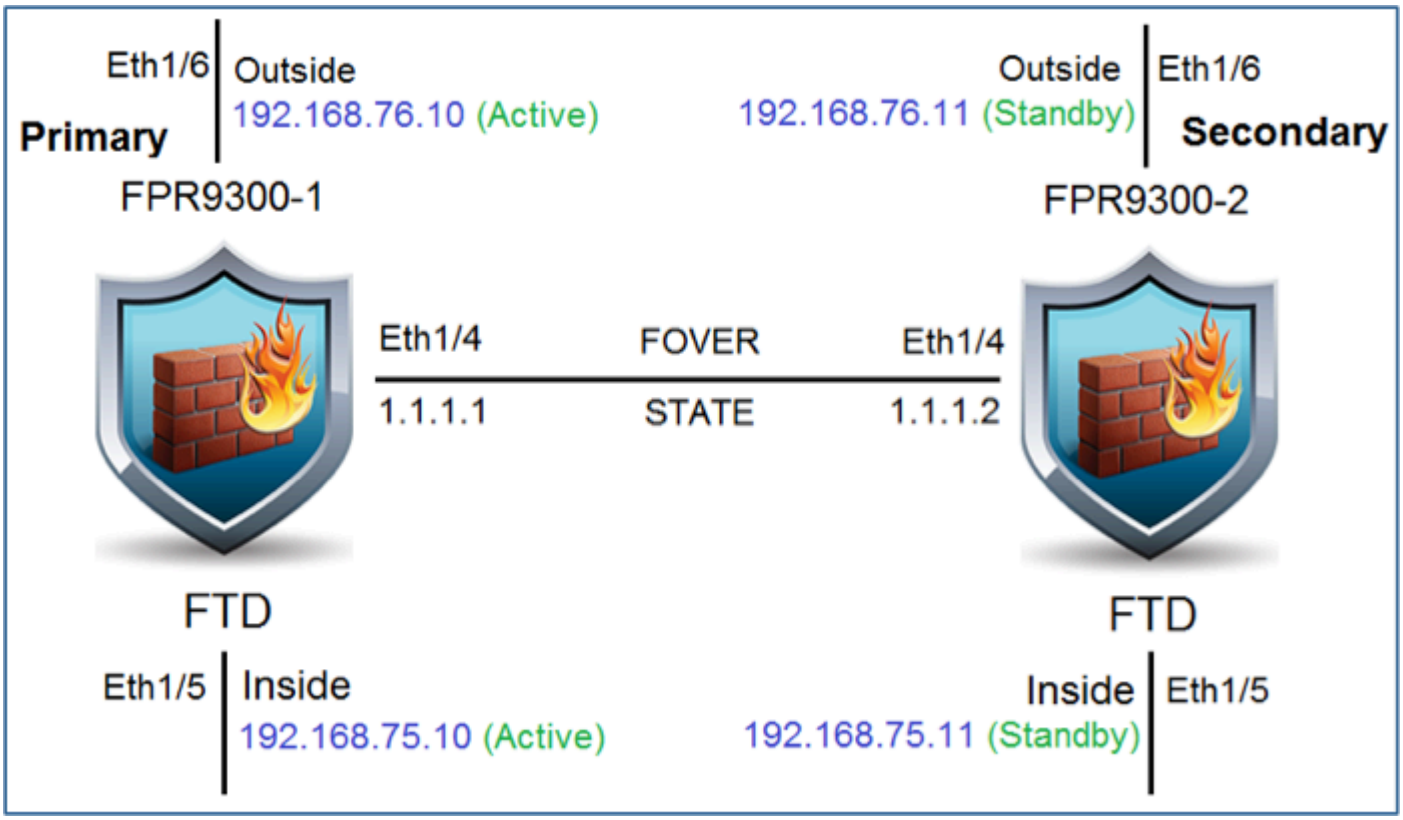
FPR9300-2



Task 2. Configure FTD HA on FPR9300

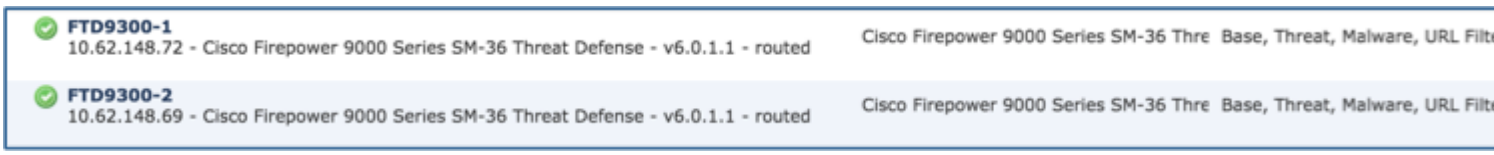
Task requirement:

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

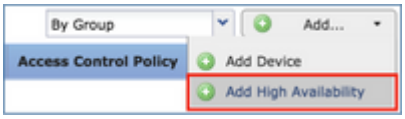


Solution:

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 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.

> **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               : 192.0.2.1
Chassis Serial Number    : JMX12345678
Security 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

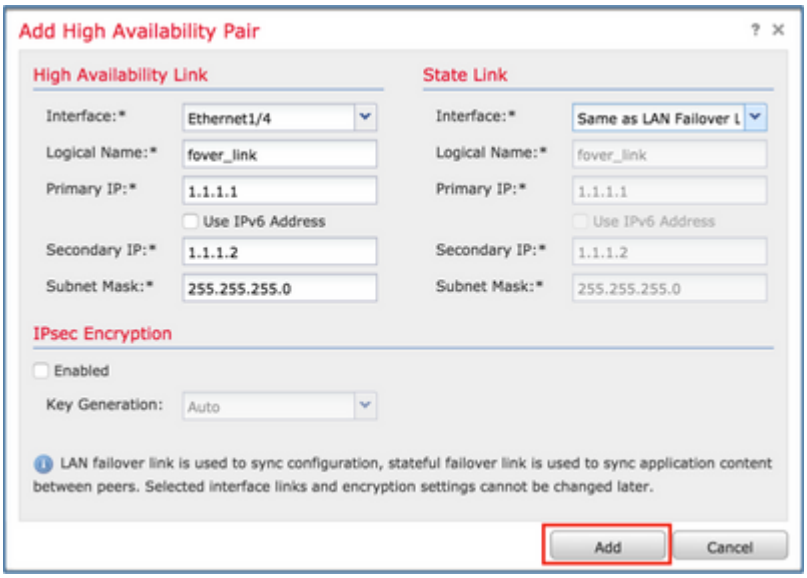
#

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.

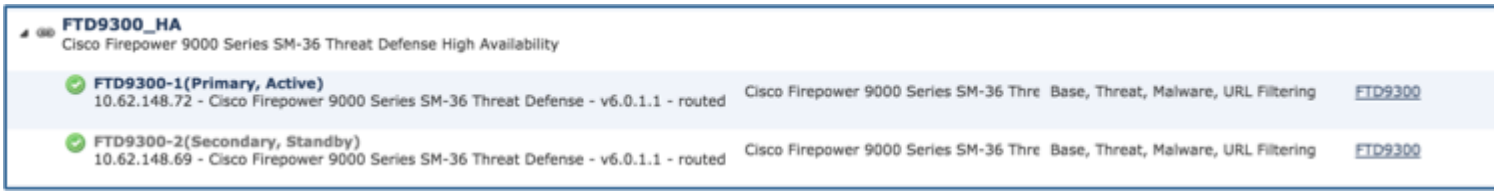
In your case, the state link has the same settings as the High Availability Link.

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



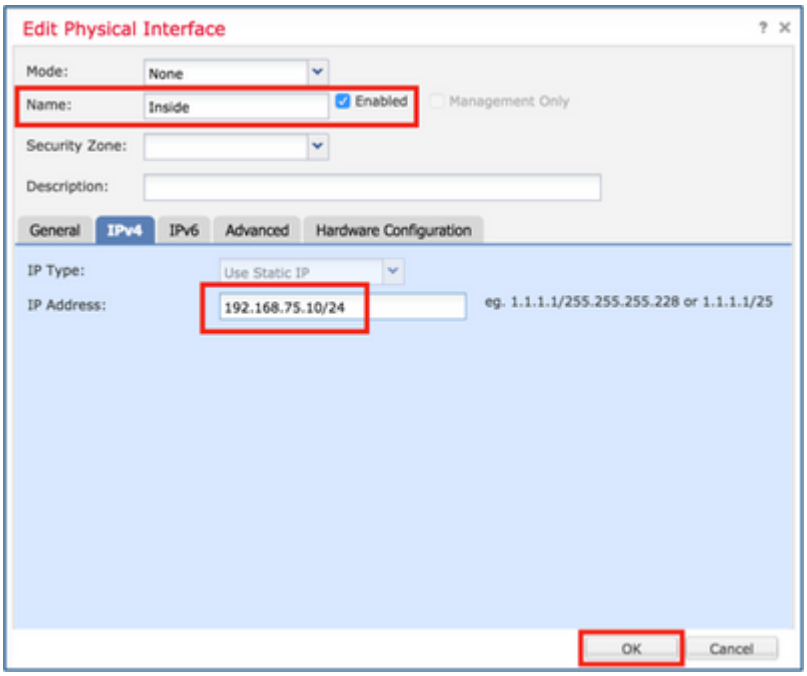
Step 4. Configure the Data interfaces (primary and standby IP addresses)

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

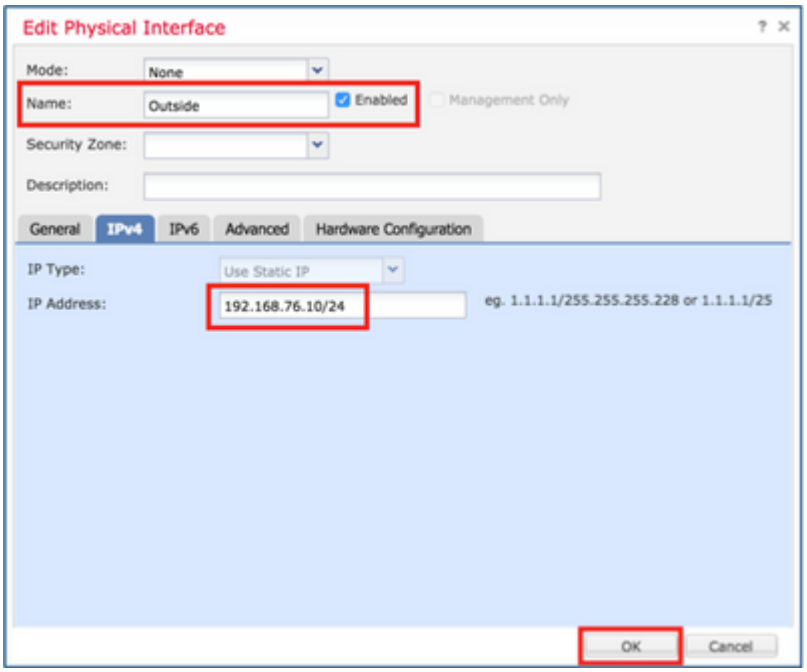


Step 5. Configure the Interface settings as shown in the images.

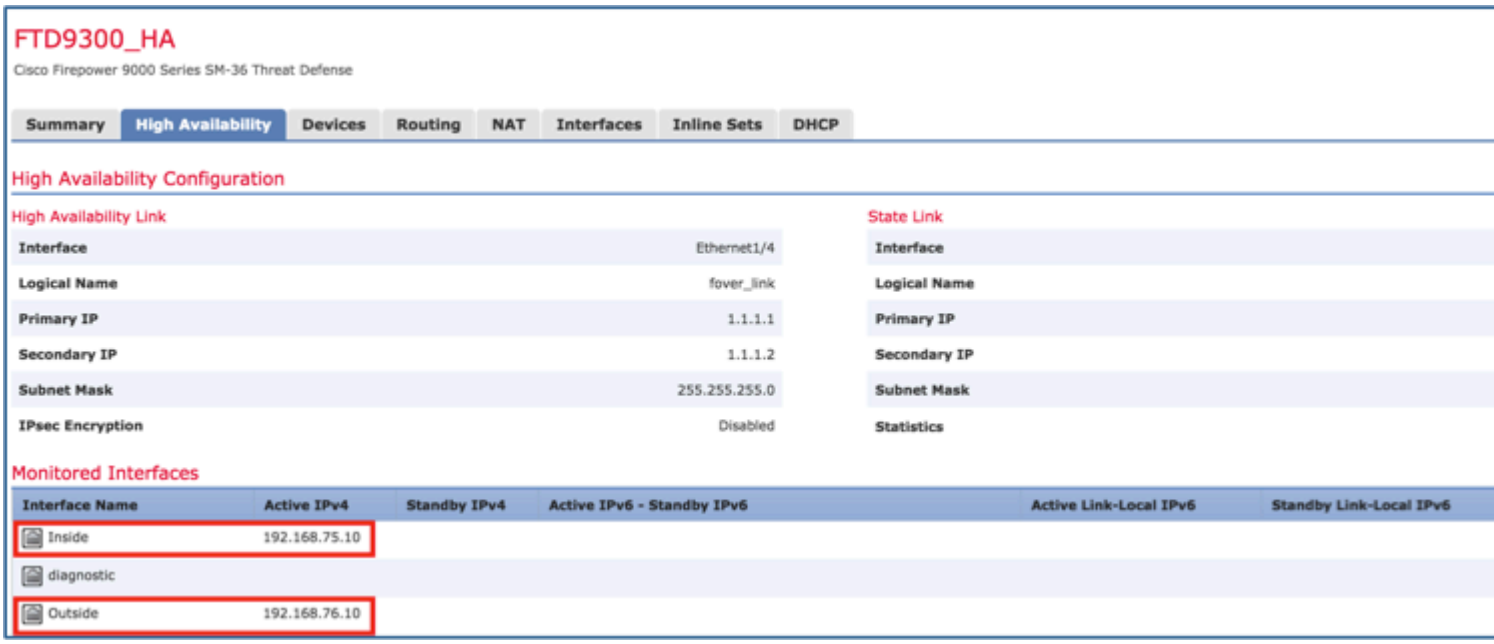
Ethernet 1/5 interface.



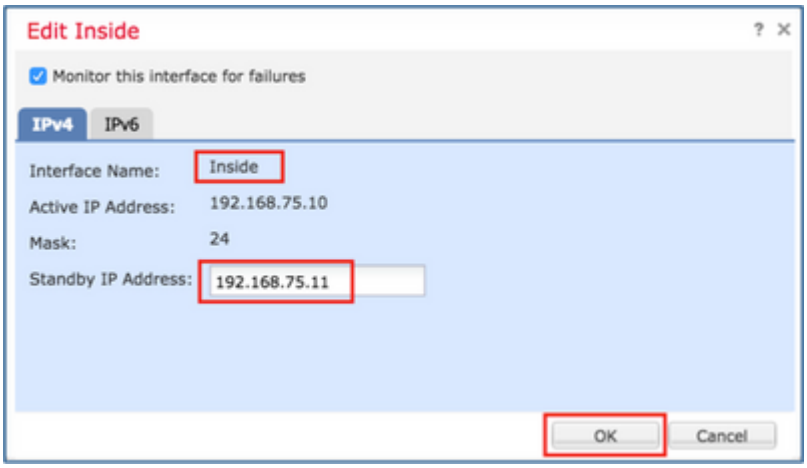
Ethernet 1/6 interface.



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

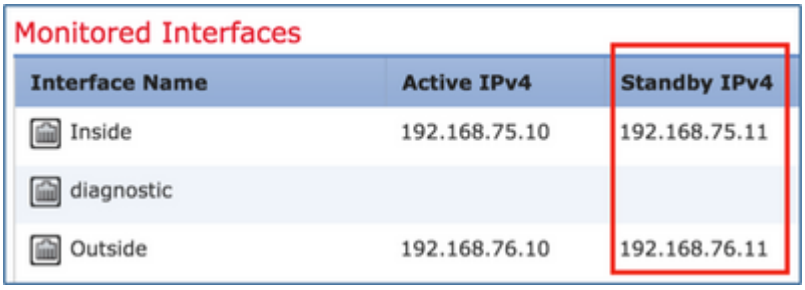


Step 7. For the Inside interface as shown in the image.

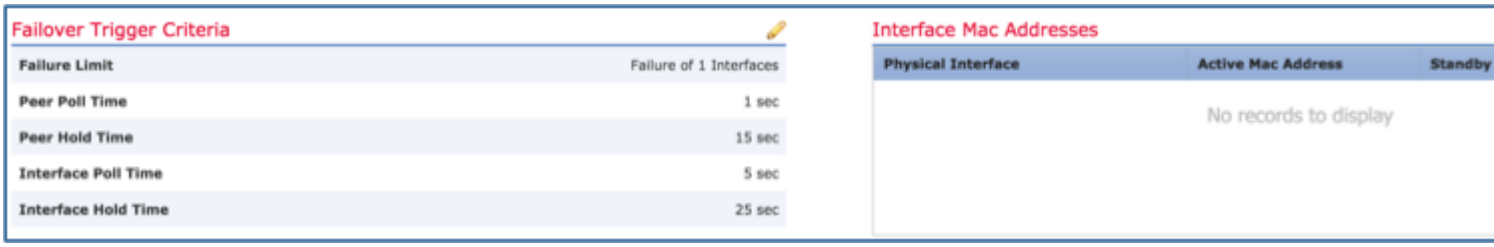


Step 8. Do the same for the Outside interface.

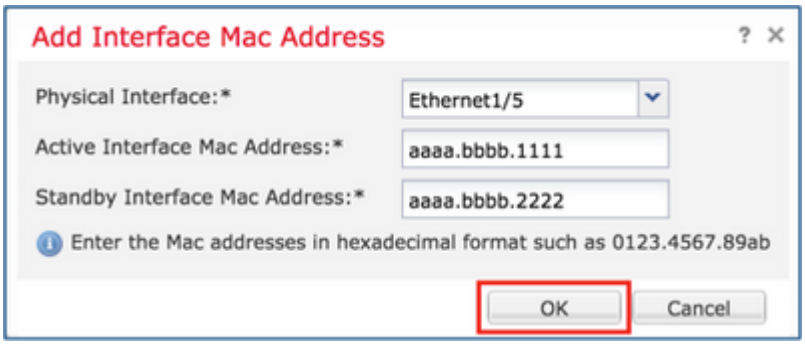
Step 9. Verify the result as shown in the image.



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

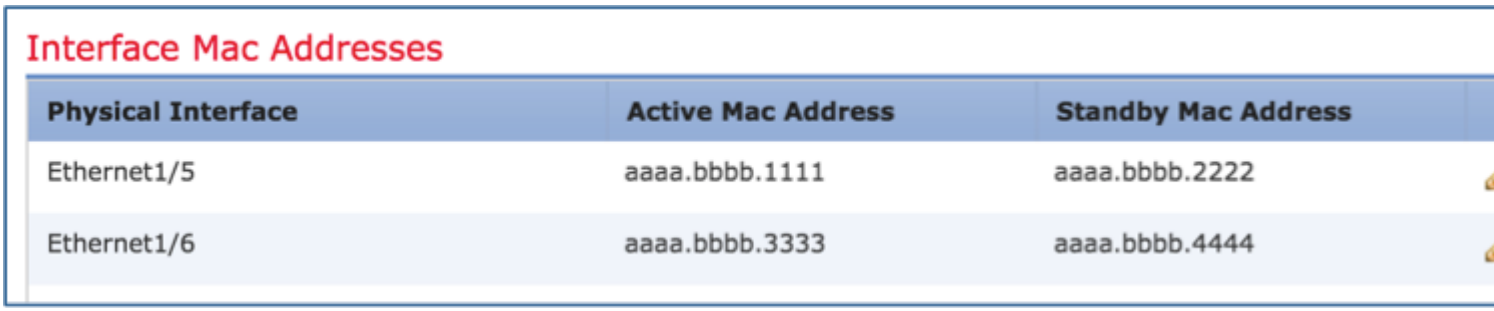


Step 11. For the Inside Interface is as shown in the image.



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, choose **Save** and **Deploy**.

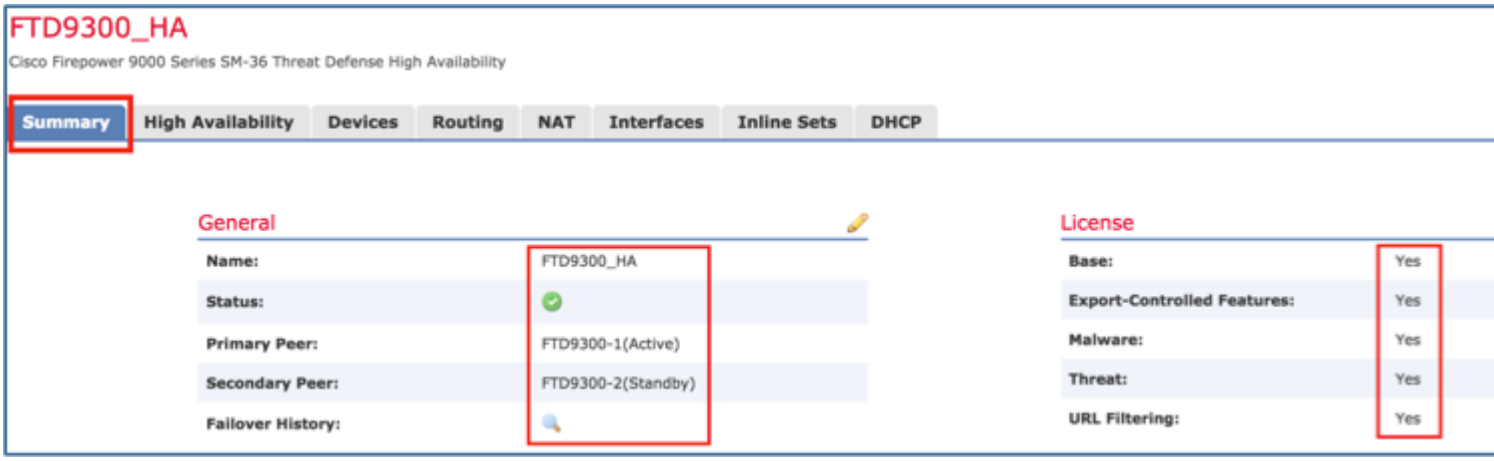
Task 3. Verify FTD HA and License

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.



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       xerr       rcv        rerr
    General        417        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:

```
<#root>

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 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#
```

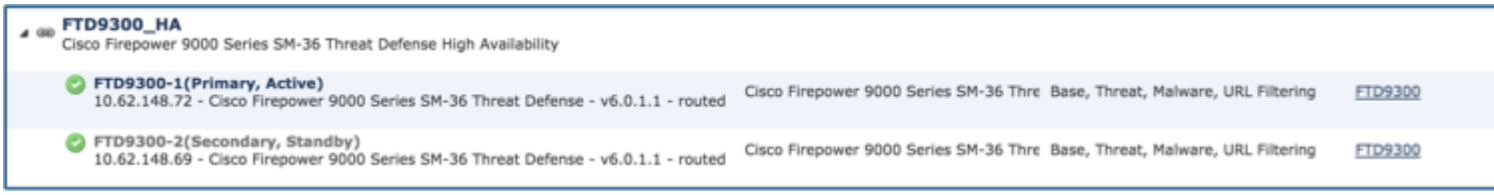
Task 4. Switch the Failover Roles

Task requirement:

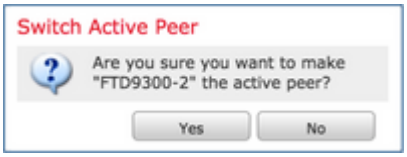
From the FMC, switch the failover roles from Primary/Active, Secondary/Standby to Primary/Standby, Secondary/Active

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.

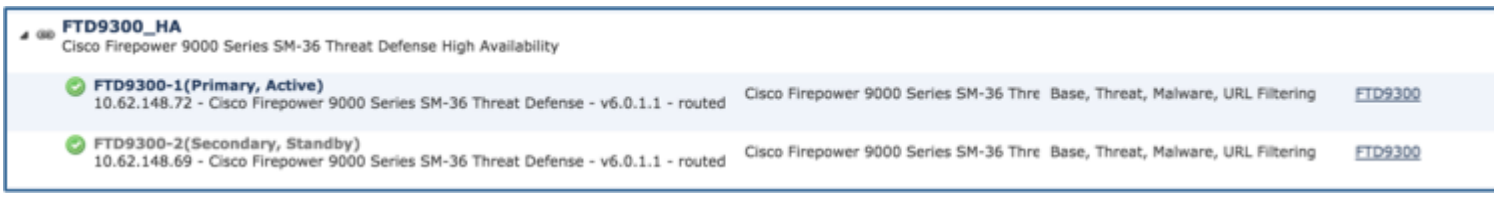
Task 5. Break the HA Pair

Task requirement:

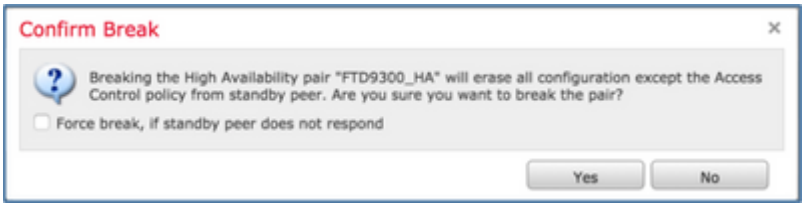
From the FMC, break the failover pair.

Solution:

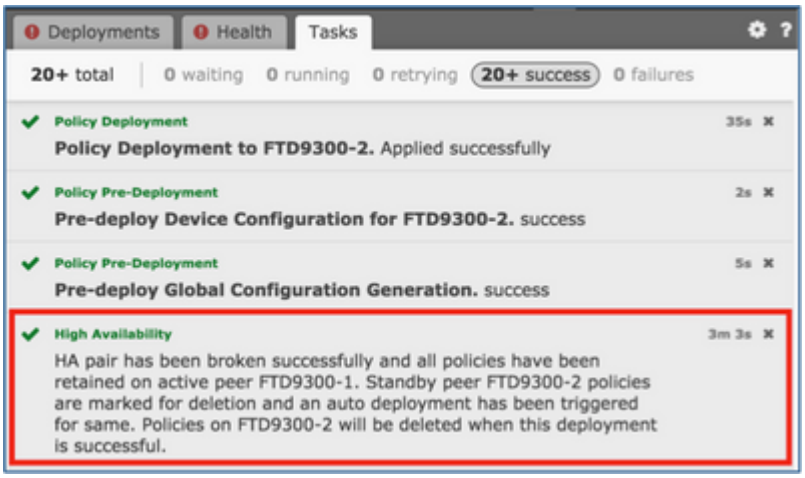
Step 1. Select the icon as shown in the image.



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



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 : Saved : : Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon 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	firepower# sh run : Saved : : Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CI 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	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 192
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 192
ngips conn-match vlan-id	!
access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1	ftp mode passive
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP	ngips conn-match vlan-id
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 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 rule-id 268447744 event-log both
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600	access-list CSM_FW_ACL_ remark rule-id 268441 ACCESS POLICY: FTD9300 - Default/1
!	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 ! 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

access-group CSM_FW_ACL_ global

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:00:30

timeout floating-conn 0:00:00

aaa proxy-limit disable

no snmp-server location

no snmp-server contact

no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

dynamic-access-policy-record DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

!

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 r
0:05:00 mgcp-pat 0:05:00

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 0:05:0

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 lin
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

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

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_MA

class class-default

set connection advanced-options UM_STATIC_TC

!

service-policy global_policy global

prompt hostname context

call-home

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#	profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/DI 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 mon subscribe-to-alert-group telemetry periodic daily Cryptochecksum:fb6f5c369dee730b9125650517dbb : 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 : Saved : : Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores) :	firepower# sh run : 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	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 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:	**no security-level**
	no ip address

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

!

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

!

ftp mode passive

ngips conn-match vlan-id

access-list CSM_FW_ACL_ remark rule-id 268447
ACCESS POLICY: FTD9300 - Mandatory/1

access-list CSM_FW_ACL_ remark rule-id 268447
RULE: Allow_ICMP

access-list CSM_FW_ACL_ advanced permit icmp
rule-id 268447744 event-log both

access-list CSM_FW_ACL_ remark rule-id 268441
ACCESS POLICY: FTD9300 - Default/1

access-list CSM_FW_ACL_ remark rule-id 268441
RULE: DEFAULT ACTION RULE

access-list CSM_FW_ACL_ advanced permit ip any
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

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

failover replication http	**no logging message 302017**
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	**no logging message 302016**
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444	**no logging message 302021**
failover link fover_link Ethernet1/4	**no logging message 302020**
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	mtu diagnostic 1500
icmp unreachable rate-limit 1 burst-size 1	**no failover**
no asdm history enable	**no monitor-interface service-module**
arp timeout 14400	icmp unreachable rate-limit 1 burst-size 1
no arp permit-nonconnected	no asdm history enable
access-group CSM_FW_ACL_ global	arp timeout 14400
timeout xlate 3:00:00	no arp permit-nonconnected
timeout pat-xlate 0:00:30	access-group CSM_FW_ACL_ global
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout xlate 3:00:00
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout pat-xlate 0:00:30
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:0 0:02:00 icmp 0:00:02
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 0:05:00 mgcp-pat 0:05:00
timeout tcp-proxy-reassembly 0:00:30	timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:0 disconnect 0:02:00
timeout floating-conn 0:00:00	timeout sip-provisional-media 0:02:00 uauth 0:05:0
user-identity default-domain LOCAL	timeout tcp-proxy-reassembly 0:00:30
aaa proxy-limit disable	timeout floating-conn 0:00:00
no snmp-server location	aaa proxy-limit disable
no snmp-server contact	no snmp-server location
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	no snmp-server contact
crypto ipsec security-association pmtu-aging infinite	no snmp-server enable traps snmp authentication lin linkdown coldstart warmstart
crypto ca trustpool policy	crypto ipsec security-association pmtu-aging infinite
	crypto ca trustpool policy
	telnet timeout 5

```
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
```

```
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 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:

Primary Unit	**Secondary Unit**
All failover configuration is removed. Standby IP addresses remain.	All configuration is removed.

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

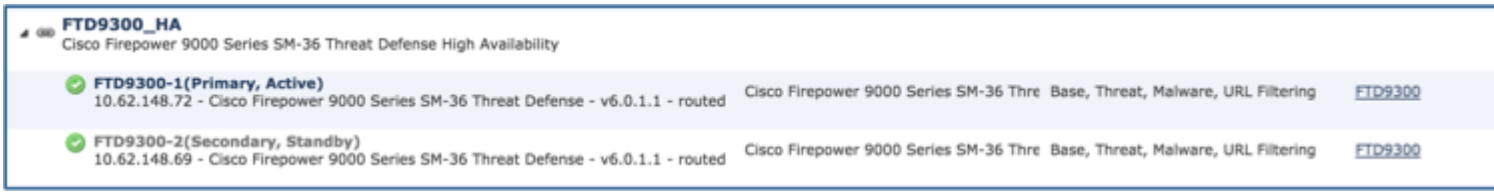
Task 6. Disable HA pair

Task requirement:

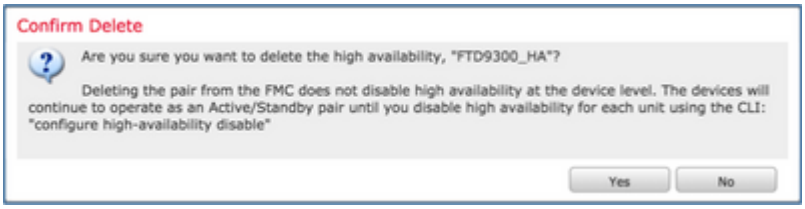
From the FMC, disable the failover pair.

Solution:

Step 1. 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:

Primary Unit	**Secondary Unit**
firepower# sh run : Saved	firepower# sh run : Saved

:	:
: Serial Number: FLM19267A63	: Serial Number: FLM19206H7T
: Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Hardware: FPR9K-SM-36, 135841 MB RAM, CI 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	description LAN/STATE Failover Interface
!	!
interface Ethernet1/5	interface Ethernet1/5
nameif Inside	nameif Inside
security-level 0	security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	**ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11**
!	!
interface Ethernet1/6	interface Ethernet1/6
nameif Outside	nameif Outside
security-level 0	security-level 0
ip address 192.168.76.10 255.255.255.0 standby	**ip address 192.168.76.10 255.255.255.0 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 any 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 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 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	no snmp-server enable traps snmp authentication lin 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 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_MAP	inspect ip-options UM_STATIC_IP_OPTIONS_MA
class class-default	class class-default
set connection advanced-options UM_STATIC_TCP_MAP	set connection advanced-options UM_STATIC_TC
!	!
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/DDCEService	destination address http https://tools.cisco.com/its/service/oddce/services/DI
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 monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:933c594fc0264082edc0f24bad358031 : end firepower#	subscribe-to-alert-group configuration periodic mon subscribe-to-alert-group telemetry periodic daily Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbc : end 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. No configuration is removed from the FTD device.	The device is removed from the FMC. 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 failover** **Failover Off (pseudo-Standby)** Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/3.205 (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 0 of 1041 maximum MAC Address Move Notification Interval not set failover replication http >

Primary	**Secondary**
firepower# show run ! hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted names arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 ! interface GigabitEthernet1/1 nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 **ip address 10.1.1.1 255.255.255.0 <-- standby IP was**	firepower# show run ! hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted names arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 ! interface GigabitEthernet1/1 shutdown no nameif no security-level no ip address ! interface GigabitEthernet1/2

removed

!

interface GigabitEthernet1/2

nameif inside

cts manual

propagate sgt preserve-untag

policy static sgt disabled trusted

security-level 0

ip address 192.168.1.1 255.255.255.0 <-- standby IP was removed

!

interface GigabitEthernet1/3

description LAN Failover Interface

!

interface GigabitEthernet1/4

description STATE Failover Interface

!

interface GigabitEthernet1/5

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/6

shutdown

no nameif

no security-level

no ip address

!

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/3

description LAN Failover Interface

!

interface GigabitEthernet1/4

description STATE Failover Interface

!

interface GigabitEthernet1/5

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/6

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/7

shutdown

no nameif

no security-level

no ip address

!

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

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

access-list CSM_FW_ACL_ remark rule-id 268435456: ACCESS POLICY: FTD_HA - Default/1

access-list CSM_FW_ACL_ remark rule-id 268435456: L4 RULE: DEFAULT ACTION RULE

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435456

!

tcp-map UM_STATIC_TCP_MAP

tcp-options range 6 7 allow

tcp-options range 9 18 allow

tcp-options range 20 255 allow

tcp-options md5 clear

urgent-flag allow

!

no pager

logging enable

logging timestamp

logging buffered debugging

logging flash-minimum-free 1024

logging flash-maximum-allocation 3076

no logging message 106015

no logging message 313001

no logging message 313008

no logging message 106023

no logging message 710005

no logging message 710003

no logging message 106100

access-list CSM_FW_ACL_ advanced permit ip any
id 268435456

!

tcp-map UM_STATIC_TCP_MAP

tcp-options range 6 7 allow

tcp-options range 9 18 allow

tcp-options range 20 255 allow

tcp-options md5 clear

urgent-flag allow

!

no pager

logging enable

logging timestamp

logging buffered debugging

logging flash-minimum-free 1024

logging flash-maximum-allocation 3076

no logging message 106015

no logging message 313001

no logging message 313008

no logging message 106023

no logging message 710005

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 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 outside 1500
mtu inside 1500
mtu diagnostic 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
access-group CSM_FW_ACL_ global
00 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu diagnostic 1500
no failover
failover lan unit secondary
failover lan interface FOVER GigabitEthernet1/3
failover replication http
failover link STATE GigabitEthernet1/4
failover interface ip FOVER 10.10.1.1 255.255.255.
10.10.1.2
failover interface ip STATE 10.10.2.1 255.255.255.
10.10.2.2
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
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
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 r
0:05:00 mgcp-pat 0:05:00
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
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
user-identity default-domain LOCAL
aaa proxy-limit disable
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
inspect netbios
  inspect tftp
  inspect icmp
```

```
snmp-server host outside 192.168.1.100 community
version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
```

inspect 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:768a03e90b9d3539773b9d7af66b3452	inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_M class class-default set connection advanced-options UM_STATIC_TC ! 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/DI 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 monthl subscribe-to-alert-group configuration periodic mo subscribe-to-alert-group telemetry periodic daily Cryptochecksum:ac9b8f401e18491fee653f4cfe0ce1

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 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 timeout conn-holddown 0:00:15 aaa proxy-limit disable snmp-server host outside	• Interface configurations are removed. • The device goes into Pseudo-Standby mode.

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.

> .

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

>
```

<#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>

```
> ..


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.

>
```

<#root>

```
>

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
>
```

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 R
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_6
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACCE
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4 R
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:
```

```
write memory        <--
```

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 startup-config:

```
<#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 192.0.2.1 255.255.255.0 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:

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)

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

Cisco Secure Firewall Management Center

- Technical Support & Documentation - Cisco Systems