Configure FTD High Availability on Firepower Appliances

Contents

Introduction
Prerequisites
Requirements
Components Used
Task 1. Verify Conditions
Task 2. Configure FTD HA on FPR9300
Conditions
Task 3. Verify FTD HA and Licensing
Task 4. Switching Failover Roles
Task 5. Breaking HA Pair
Task 6. Disable HA pair
Task 7. Suspend HA
Verify
Troubleshoot
Related Information

Introduction

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

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- 2xCisco Firepower 9300 Security Appliance 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
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.
- 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 go to FTD CLI and run this command:

```
firepower# show chassis-management-url
```

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

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

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

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 redeploy 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
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
General1417 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 IKV1 SA 0 0 0 0
VPN IKV1 P2 0 0 0 0
VPN IKV2 SA 0 0 0 0
VPN IKV2 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 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

<table>
<thead>
<tr>
<th>State</th>
<th>Last Failure Reason</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>This host</td>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Other host</td>
<td>Secondary</td>
<td></td>
</tr>
</tbody>
</table>

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

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/Standy to Primary/Standy, 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-5-111010: 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

```bash
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 8Ry2Yjlt7RRXU24 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 event-log both
```

After HA Break

```bash
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 8Ry2Yjlt7RRXU24 encrypted
names
!
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
!
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 event-log both
```
access-list CSM_FW_ACL_global
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
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

RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_global
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
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 0:02:00 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
cryptochecksum:fb6f5c369dee730b9125650517dbb059

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
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic
subscribe-to-alert-group telemetry periodic
Cryptochecksum:fb6f5c369dee730b9125650517dbb059
:end
firepower#
show running-config on the Secondary unit before and after breaking the HA is as shown in the table here.

<table>
<thead>
<tr>
<th>Before HA Break</th>
<th>After HA Break</th>
</tr>
</thead>
<tbody>
<tr>
<td>firepower# sh run</td>
<td>firepower# sh run</td>
</tr>
<tr>
<td>Saved</td>
<td>Saved</td>
</tr>
<tr>
<td>: Serial Number: FLM19206H7T</td>
<td>: Serial Number: FLM19206H7T</td>
</tr>
<tr>
<td>: Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)</td>
<td>: Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)</td>
</tr>
<tr>
<td>NGFW Version 6.0.1.1</td>
<td>NGFW Version 6.0.1.1</td>
</tr>
<tr>
<td>hostname firepower</td>
<td>hostname firepower</td>
</tr>
<tr>
<td>enable password 8Ry2Yjlyt7RRUX24 encrypted names</td>
<td>enable password 8Ry2Yjlyt7RRUX24 encrypted names</td>
</tr>
<tr>
<td>interface Ethernet1/2</td>
<td>interface Ethernet1/2</td>
</tr>
<tr>
<td>management-only</td>
<td>management-only</td>
</tr>
<tr>
<td>nameif diagnostic</td>
<td>nameif diagnostic</td>
</tr>
<tr>
<td>security-level 0</td>
<td>security-level 0</td>
</tr>
<tr>
<td>no ip address</td>
<td>no ip address</td>
</tr>
<tr>
<td>interface Ethernet1/4</td>
<td>interface Ethernet1/4</td>
</tr>
<tr>
<td>description LAN/STATE Failover Interface</td>
<td>description LAN/STATE Failover Interface</td>
</tr>
<tr>
<td>interface Ethernet1/5</td>
<td>interface Ethernet1/5</td>
</tr>
<tr>
<td>nameif Inside</td>
<td>nameif Inside</td>
</tr>
<tr>
<td>security-level 0</td>
<td>security-level 0</td>
</tr>
<tr>
<td>ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11</td>
<td>ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11</td>
</tr>
<tr>
<td>interface Ethernet1/6</td>
<td>interface Ethernet1/6</td>
</tr>
<tr>
<td>nameif Outside</td>
<td>nameif Outside</td>
</tr>
<tr>
<td>security-level 0</td>
<td>security-level 0</td>
</tr>
<tr>
<td>ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11</td>
<td>ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11</td>
</tr>
<tr>
<td>ftp mode passive</td>
<td>ftp mode passive</td>
</tr>
<tr>
<td>ngips conn-match vlan-id</td>
<td>ngips conn-match vlan-id</td>
</tr>
<tr>
<td>access-list CSM_FW_ACL_remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1</td>
<td>access-list CSM_FW_ACL_remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1</td>
</tr>
<tr>
<td>access-list CSM_FW_ACL_remark rule-id 268447744: L4 RULE: Allow ICMP</td>
<td>access-list CSM_FW_ACL_remark rule-id 268447744: L4 RULE: Allow ICMP</td>
</tr>
<tr>
<td>access-list CSM_FW_ACL_remark advanced permit icmp any any rule-id 268447744 event-log both</td>
<td>access-list CSM_FW_ACL_remark advanced permit icmp any any rule-id 268447744 event-log both</td>
</tr>
</tbody>
</table>
access-list CSM_FW_ACL_ remark rule-id 268441600:
ACCESS POLICY: FTD9300 - Default/1
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
ingress timestamp
ingress standby
logging buffer-size 100000
logging buffered debugging
logging flush-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
aaa proxy-limit disable
no snmp-server location
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
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 buffer-size 100000
logging buffered debugging
logging flush-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
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authen
no snmp-server contact
no snmp-server enable traps snmp authentication linkup
linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
! 
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http

https://tools.cisco.com/its/service/oddce/s
Main points to note for breaking the HA:

<table>
<thead>
<tr>
<th>Primary Unit</th>
<th>Secondary Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>All failover configuration is removed</td>
<td>All configuration is removed</td>
</tr>
<tr>
<td>Standby IP’s remain</td>
<td></td>
</tr>
</tbody>
</table>

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.

![Image](image1.png)

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

![Image](image2.png)

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:

<table>
<thead>
<tr>
<th>Primary Unit</th>
<th>Secondary Unit</th>
</tr>
</thead>
</table>
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 8Ry2Yjlyt7RRXU24 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 RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
: NGFW Version 6.0.1.1
!
hostname firepower
enable password 8Ry2Yjlyt7RRXU24 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
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
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 ftp
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/lts/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
Crytochecksum:933c594fc0264082edc0f24bad358031
: end
firepower#
Step 4. Both FTD devices were unregistered from the FMC:

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

Main points to note for disabling the HA from FMC:

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

**Secondary Unit**  
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:

```
> 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 above command on both units

After doing the above:

**Primary 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
```

**Secondary Unit**

```
> 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
```

```
firepower# show run
!
hostname firepower
enable password 8Ry2Yjlty7RRXU24 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
```

```
firepower# show run
!
hostname firepower
enable password 8Ry2Yjlty7RRXU24 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
```
security-level 0
ip address 10.1.1.1 255.255.255.0  <-- standby IP was removed
!
interface GigabitEthernet1/2
nameif inside
ccts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.1 255.255.255.0  <-- standby IP was removed
!
interface GigabitEthernet1/3
description LAN Failover Interface
!
interface GigabitEthernet1/4
description STATE Failover Interface
!
interface GigabitEthernet1/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface Management1/1
management-only
nameif diagnostic
ccts 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

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
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
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
failover lan unit secondary
failover lan interface FOVER GigabitEthernet1
failover replication http
failover link STATE GigabitEthernet1/4
failover interface ip FOVER 1.1.1.1 255.255.255.0
standby 1.1.1.2

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
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
!
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 0:02:00
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
aaa proxy-limit disable
snmp-server host outside 192.168.1.100 community
***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
close timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp

failover interface ip STATE 2.2.2.1 255.255.255.0
standby 2.2.2.2
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 0:02:00
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
user-identity default-domain LOCAL
aaa proxy-limit disable
snmp-server host outside 192.168.1.100 community
***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
close timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
Main points to note for disabling the HA from FTD CLI:

<table>
<thead>
<tr>
<th>Primary Unit</th>
<th>Secondary Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover configuration and standby IPs are removed</td>
<td>Interface configurations are removed</td>
</tr>
<tr>
<td></td>
<td>The device goes into Pseudo-Standby mode</td>
</tr>
</tbody>
</table>

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-availability.

> .

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

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

- 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

- Technical Support & Documentation - Cisco Systems