

Upgrade FTD HA Pair on Firepower Appliances

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Task 1. Verify the Prerequisites](#)

[Task 2. Upload the Software Images](#)

[Task 3. Upgrade the first FXOS chassis](#)

[Task 4. Swap the FTD Failover States](#)

[Task 5. Upgrade the second FXOS chassis](#)

[Task 6. Upgrade the FMC Software](#)

[Task 7. Upgrade the FTD HA Pair](#)

[Task 8. Deploy a Policy to the FTD HA Pair](#)

[Related Information](#)

Introduction

This document describes the upgrade process of Firepower Threat Defense (FTD) in High Availability (HA) mode on Firepower appliances.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Management Center (FMC)
- FTD
- Firepower appliances (FXOS)

Components Used

- 2 x FPR4150
- 1 x FS4000
- 1 x PC

The software image versions before the upgrade:

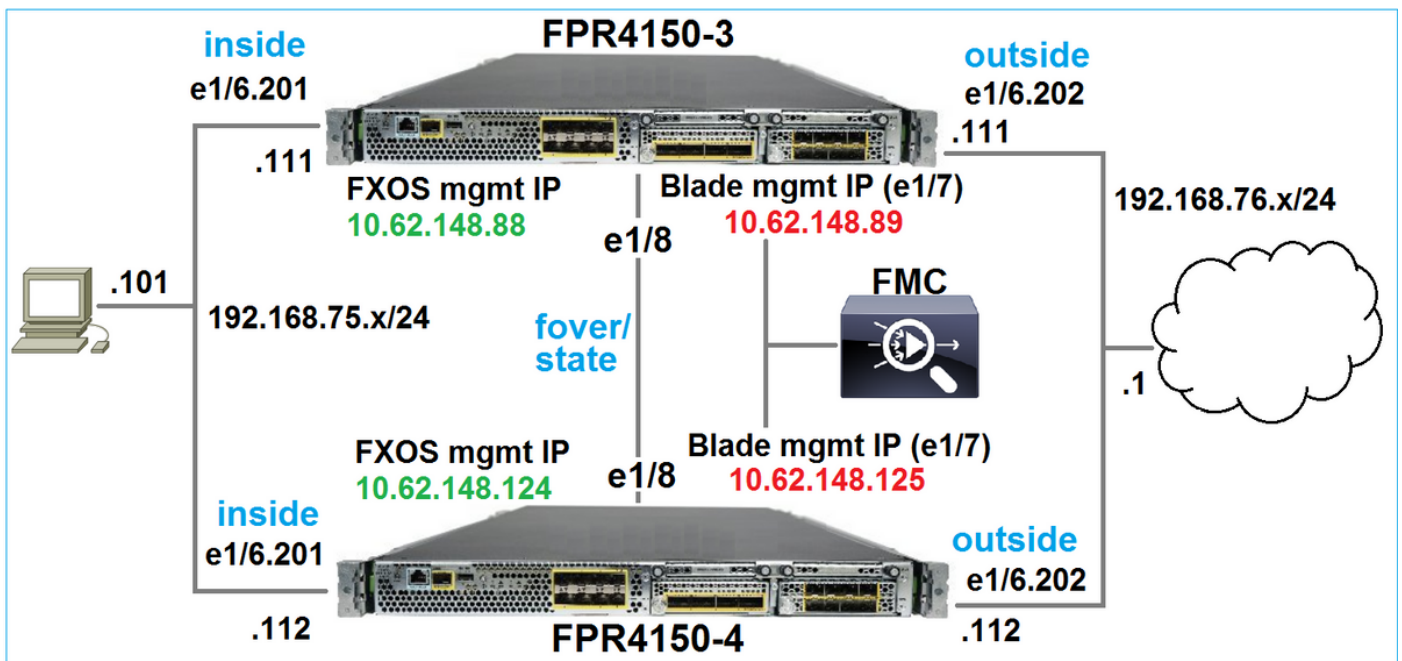
- FMC 6.1.0-330

- FTD Primary 6.1.0-330
- FTD Secondary 6.1.0-330
- FXOS Primary 2.0.1-37
- FXOS Secondary 2.0.1-37

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.

Configure

Network Diagram



Action Plan

Task 1: Verify the prerequisites

Task 2: Upload the images to FMC and SSP

Task 3: Upgrade the first FXOS chassis (2.0.1-37 -> 2.0.1-86)

Task 4: Swap the FTD failover

Task 5: Upgrade the second FXOS chassis (2.0.1-37 -> 2.0.1-86)

Task 6: Upgrade the FMC (6.1.0-330 -> 6.1.0.1)

Task 7: Upgrade the FTD HA pair (6.1.0-330 -> 6.1.0.1)

Task 8: Deploy a policy from FMC to the FTD HA pair

Task 1. Verify the Prerequisites

Consult the FXOS Compatibility Guide in order to determine the compatibility between:

- Target FTD software version and FXOS software version
- Firepower HW platform and FXOS software version

[Cisco Firepower 4100/9300 FXOS Compatibility](#)

Note: This step is not applicable to FP21xx and earlier platforms.

Check the FXOS Release Notes of the target version in order to determine the FXOS upgrade path:

[Cisco Firepower 4100/9300 FXOS Release Notes, 2.0\(1\)](#)

Note: This step is not applicable to FP21xx and earlier platforms.

Consult the FTD target version Release Notes in order to determine the FTD upgrade path:

[Firepower System Release Notes, Version 6.0.1.2](#)

Task 2. Upload the Software Images

On the two FCMs, upload the FXOS images (fxos-k9.2.0.1.86.SPA).

On the FMC, upload the FMC and FTD upgrade packages:

- For the FMC upgrade: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- For the FTD upgrade: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

Task 3. Upgrade the first FXOS chassis

Note: In case you upgrade FXOS from 1.1.4.x to 2.x, you need to first shut down the FTD logical appliance, upgrade the FXOS, and then re-enable it.

Note: This step is not applicable to FP21xx and earlier platforms.

Before the upgrade:

```
FPR4100-4-A /system # show firmware monitor
```

```
FPRM:
```

```
Package-Vers: 2.0(1.37)
```

```
Upgrade-Status: Ready
```

```
Fabric Interconnect A:
```

```
Package-Vers: 2.0(1.37)
```

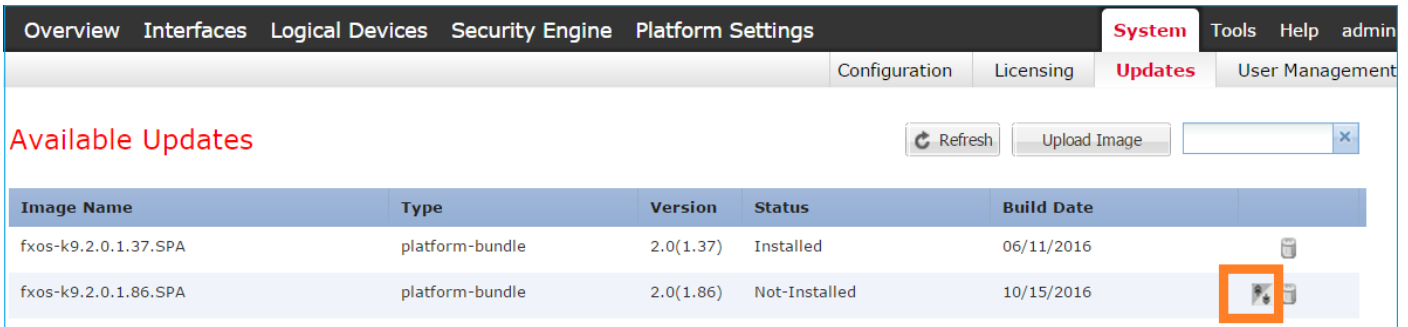
```
Upgrade-Status: Ready
```

```
Chassis 1:
```

```
Server 1:
```

Package-Vers: 2.0(1.37)
Upgrade-Status: Ready

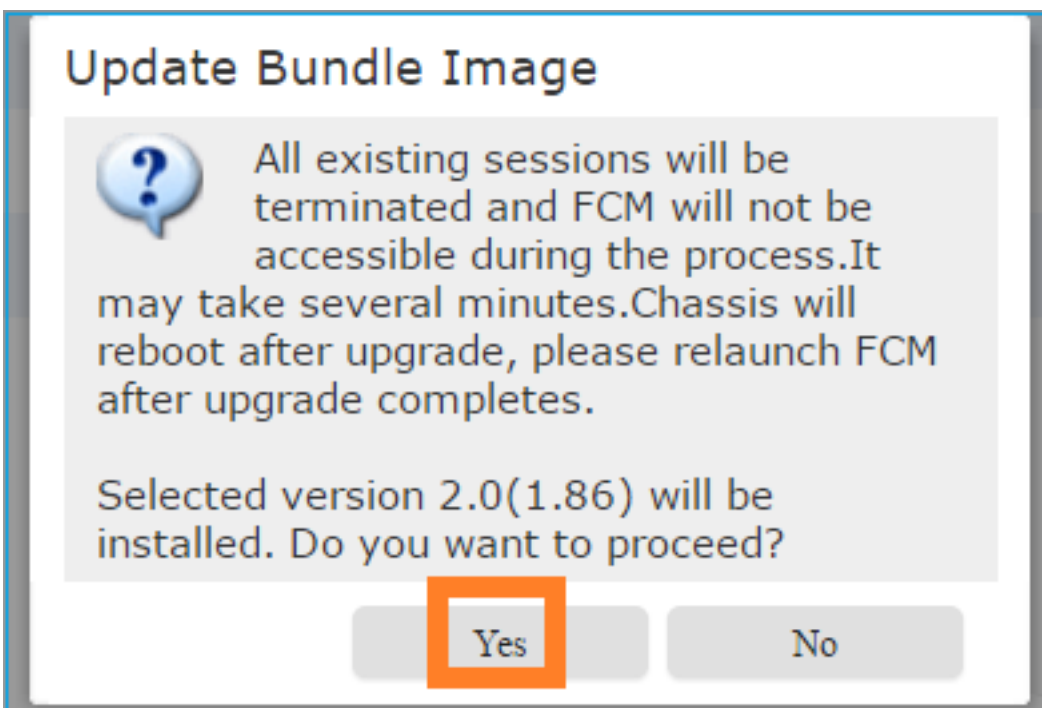
Start the FXOS upgrade:



Available Updates

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Installed	06/11/2016
fxos-k9.2.0.1.86.SPA	platform-bundle	2.0(1.86)	Not-Installed	10/15/2016

The FXOS upgrade requires a chassis reboot:



Update Bundle Image

All existing sessions will be terminated and FCM will not be accessible during the process. It may take several minutes. Chassis will reboot after upgrade, please relaunch FCM after upgrade completes.

Selected version 2.0(1.86) will be installed. Do you want to proceed?

Yes No

You can monitor the FXOS upgrade from the FXOS CLI. All three components (FPRM, fabric interconnect, and chassis) have to be upgraded:

```
FPR4100-4-A# scope system
FPR4100-4-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.37)
  Upgrade-Status: Upgrading

Fabric Interconnect A:
  Package-Vers: 2.0(1.37)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.0(1.37)
    Upgrade-Status: Ready
```

Note: A few minutes after you start the FXOS upgrade process you get disconnected from both the FXOS CLI and the GUI. You must be able to log in again after a few minutes.

After approximately five minutes the FPRM component upgrade completes:

```
FPR4100-4-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.0(1.37)
  Upgrade-Status: Upgrading

Chassis 1:
  Server 1:
    Package-Vers: 2.0(1.37)
    Upgrade-Status: Upgrading
```

After approximately 10 minutes, and as a part of the FXOS upgrade process, the Firepower device restarts:

```
Please stand by while rebooting the system...
...
Restarting system.
```

After the restart the upgrade process resumes:

```
FPR4100-4-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.0(1.37)
  Upgrade-Status: Upgrading

Chassis 1:
  Server 1:
    Package-Vers: 2.0(1.37)
    Upgrade-Status: Upgrading
```

After a total of approximately 30 minutes the FXOS upgrade completes:

```
FPR4100-4-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Chassis 1:
```

Server 1:
Package-Vers: 2.0(1.86),2.0(1.37)
Upgrade-Status: Ready

Task 4. Swap the FTD Failover States

Note: This step is not applicable to FP21xx and earlier platforms.

Before you swap the failover states, ensure that the FTD module on the chassis is fully UP:

```
FPR4100-4-A# connect module 1 console
Firepower-module1>connect ftd
Connecting to ftd console... enter exit to return to bootCLI

> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/8 (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 3 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2), Mate 9.6(2)
Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U
Last Failover at: 15:08:47 UTC Dec 17 2016
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys)
      Interface inside (192.168.75.112): Normal (Monitored)
      Interface outside (192.168.76.112): Normal (Monitored)
      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: Primary - Active
    Active time: 5163 (sec)
      Interface inside (192.168.75.111): Normal (Monitored)
      Interface outside (192.168.76.111): Normal (Monitored)
      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 Ethernet1/8 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General       65         0         68        4
sys cmd       65         0         65        0
...
```

Swap the FTD failover states. From the Active FTD CLI:

```
> no failover active
  Switching to Standby
>
```

Task 5. Upgrade the second FXOS chassis

Similar to Task 2, upgrade the FXOS appliance where the new Standby FTD is installed. This can take approximately 30 minutes or more to complete.

Note: This step is not applicable to FP21xx and earlier platforms.

Task 6. Upgrade the FMC Software

Upgrade the FMC, in this scenario from 6.1.0-330 to 6.1.0.1.

Task 7. Upgrade the FTD HA Pair

Before the upgrade:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (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 3 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2), Mate 9.6(2)
Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW
Last Failover at: 15:51:08 UTC Dec 17 2016
  This host: Primary - Standby Ready
    Active time: 0 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys)
      Interface inside (192.168.75.112): Normal (Monitored)
      Interface outside (192.168.76.112): Normal (Monitored)
      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 - Active
    Active time: 1724 (sec)
    Interface inside (192.168.75.111): Normal (Monitored)
    Interface outside (192.168.76.111): Normal (Monitored)
    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 Ethernet1/8 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General        6         0         9         0
sys cmd        6         0         6         0
...
```

From the FMC **System > Updates** menu, initiate the FTD HA upgrade process:

Overview Analysis Policies Devices Objects AMP Deploy System Help admin

Configuration Users Domains Integration **Updates** Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates Upload Update

Currently running software version: 6.1.0

Updates

Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016		No	
Cisco FTD Patch	6.1.0.1-53	Fri Dec 2 17:36:27 UTC 2016		Yes	
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016		Yes	

Ungrouped (1 total)

FTD4150-HA
Cisco Firepower 4150 Threat Defense Cluster

<input checked="" type="checkbox"/> FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09 ✕ ✔
<input checked="" type="checkbox"/> FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09 ✕ ✔

Launch Readiness Check **Install** Cancel

First, the Primary/Standby FTD is upgraded:

Deployments Health **Tasks** Settings Help admin

1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 1m 21s

Apply to FTD4150-HA.
10.62.148.89 : Initializing

The Standby FTD module reboots with the new image:

1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 7m 50s

Apply to FTD4150-HA.
10.62.148.89 : Last Message : System will now reboot. (no communication)

You can verify the FTD status from the FXOS BootCLI mode:


```

FPR4100-3-A# connect module 1 console
Firepower-module1> show services status
Services currently running:
Feature | Instance ID | State | Up Since
-----|-----|-----|-----
ftd | 001_JAD201200R4WLYCW06 | RUNNING | :00:00:33

```

The Secondary/Active FTD CLI shows a warning message due to a software version mismatch between the FTD modules:

```

firepower#
*****WARNING****WARNING****WARNING*****
Mate version 9.6(2) is not identical with ours 9.6(2)4
*****WARNING****WARNING****WARNING*****
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

```

The FMC shows that the FTD device was successfully upgraded:

1 total | 1 waiting 0 running 0 retrying 0 success 0 failures

Remote Install 16m 1s

Apply to FTD4150-HA.
10.62.148.89 : Device successfully upgraded

The upgrade of the second FTD module starts:

1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 17m 22s

Apply to FTD4150-HA.
10.62.148.125 : [1%] Running script 000_start/101_run_pruning.pl...

At the end of the process the FTD boots with the new image:

Deploy ✔ **System** Help ▾ admin

Deployments Health Tasks ⚙️ ?

2 total | 0 waiting 1 running 0 retrying 1 success 0 failures

Remote Install 24m 55s

Apply to FTD4150-HA.
10.62.148.125 : Last Message : System will now reboot. (no communication)

In the background, the FMC uses the internal user **enable_1**, swaps the FTD failover states, and temporarily removes the failover configuration from the FTD:

```

firepower# show logging
Dec 17 2016 16:40:14: %ASA-5-111008: User 'enable_1' executed the 'no failover active' command.
Dec 17 2016 16:40:14: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed
'no failover active'
Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'clear configure failover'
command.
Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed
'clear configure failover'
Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'copy /noconfirm running-
config disk0:/modified-config.cfg' command.
Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed
'copy /noconfirm running-config
disk0:/modified-config.cfg' firepower# Switching to Standby

firepower#

```

In this case the whole FTD upgrade (both units) took approximately 30 minutes.

Verification

This example shows FTD CLI verification from the Primary FTD device:

```

> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (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 3 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2)4, Mate 9.6(2)4
Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW
Last Failover at: 16:40:14 UTC Dec 17 2016
  This host: Primary - Active
    Active time: 1159 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
      Interface inside (192.168.75.111): Normal (Monitored)
      Interface outside (192.168.76.111): Normal (Monitored)
      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: 0 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
      Interface inside (192.168.75.112): Normal (Monitored)
      Interface outside (192.168.76.112): Normal (Monitored)
      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 Ethernet1/8 (up)
  Stateful Obj   xmit      xerr      rcv      rerr
  General        68         0         67         0
...
>

```

This example shows FTD CLI verification from the Secondary/Standby FTD device:

```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/8 (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 3 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2)4, Mate 9.6(2)4
Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U
Last Failover at: 16:52:43 UTC Dec 17 2016
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
      Interface inside (192.168.75.112): Normal (Monitored)
      Interface outside (192.168.76.112): Normal (Monitored)
      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: Primary - Active
    Active time: 1169 (sec)
    Interface inside (192.168.75.111): Normal (Monitored)
    Interface outside (192.168.76.111): Normal (Monitored)
    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 Ethernet1/8 (up)
Stateful Obj   xmit   xerr   rcv    rerr
General       38     0     41     0
... >
```

Task 8. Deploy a Policy to the FTD HA Pair

After the upgrade is completed, you need to deploy a policy to the HA pair. This is shown in the FMC UI:

The screenshot shows the FMC UI interface. At the top, there is a navigation bar with a 'Deploy' button, a green checkmark, 'System', 'Help', and 'admin'. Below this is a secondary navigation bar with tabs for 'Deployments', 'Health', and 'Tasks'. A summary bar indicates '2 total' deployments, with '0 waiting', '0 running', '0 retrying', '2 success', and '0 failures'. A task card titled 'Remote Install' is shown, with a message box that says 'Apply to FTD4150-HA. Please reapply policies to your managed devices.' The task duration is '28m 14s'.

Deploy the policies:

Deploy Policies Version: 2016-12-17 06:08 PM

<input checked="" type="checkbox"/>	Device
<input checked="" type="checkbox"/>	FTD4150-HA <ul style="list-style-type: none"> NGFW Settings: FTD4150 Access Control Policy: FTD4150 Intrusion Policy: Balanced Security and Connectivity DNS Policy: Default DNS Policy Prefilter Policy: Default Prefilter Policy Network Discovery Device Configuration (Details)

Verification

The upgraded FTD HA pair as it seen from the FMC UI:

Overview	Analysis	Policies	Devices	Objects	AMP	
Device Management	NAT	VPN	QoS	Platform Settings		
Name						Group
▲ Ungrouped (1)						
▲ FTD4150-HA Cisco Firepower 4150 Threat Defense High Availability						
FTD4150-3(Primary, Active) 10.62.148.89 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed						
FTD4150-4(Secondary, Standby) 10.62.148.125 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed						

The upgraded FTD HA pair as it seen from the FCM UI:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD4150-3 Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.1.53	10.62.148.89	10.62.148.1	Ethernet1/7	online

Ports:

Data Interfaces: Ethernet1/6 Ethernet1/8

Attributes:

Cluster Operational Status: not-applicable
Firepower Management IP: 10.62.148.89
Management URL : https://fs4k
UUID : 13fbc60-c378

Related Information

- [Cisco Firepower NGFW](#)
- [Technical Support & Documentation - Cisco Systems](#)