

En améliorant un FTD ha appareillez sur des appliances de FirePOWER

Contenu

[Introduction](#)

[But](#)

[Composants de laboratoire](#)

[Topologie](#)

[Le processus de mise à niveau FTD ha](#)

[Étape 1 : Vérifiez les conditions préalables](#)

[Étape 2 : Téléchargez les images](#)

[Étape 3 : Améliorez le FXOS secondaire](#)

[Étape 4 : Permutez les états de Basculement FTD](#)

[Étape 5 : Améliorez l'appliance primaire FXOS](#)

[Étape 6 : Améliorez le logiciel FMC](#)

[Étape 7 : Améliorez les paires FTD ha](#)

[Étape 8 : Déployez une stratégie vers les paires FTD ha](#)

[Documents connexes](#)

Introduction

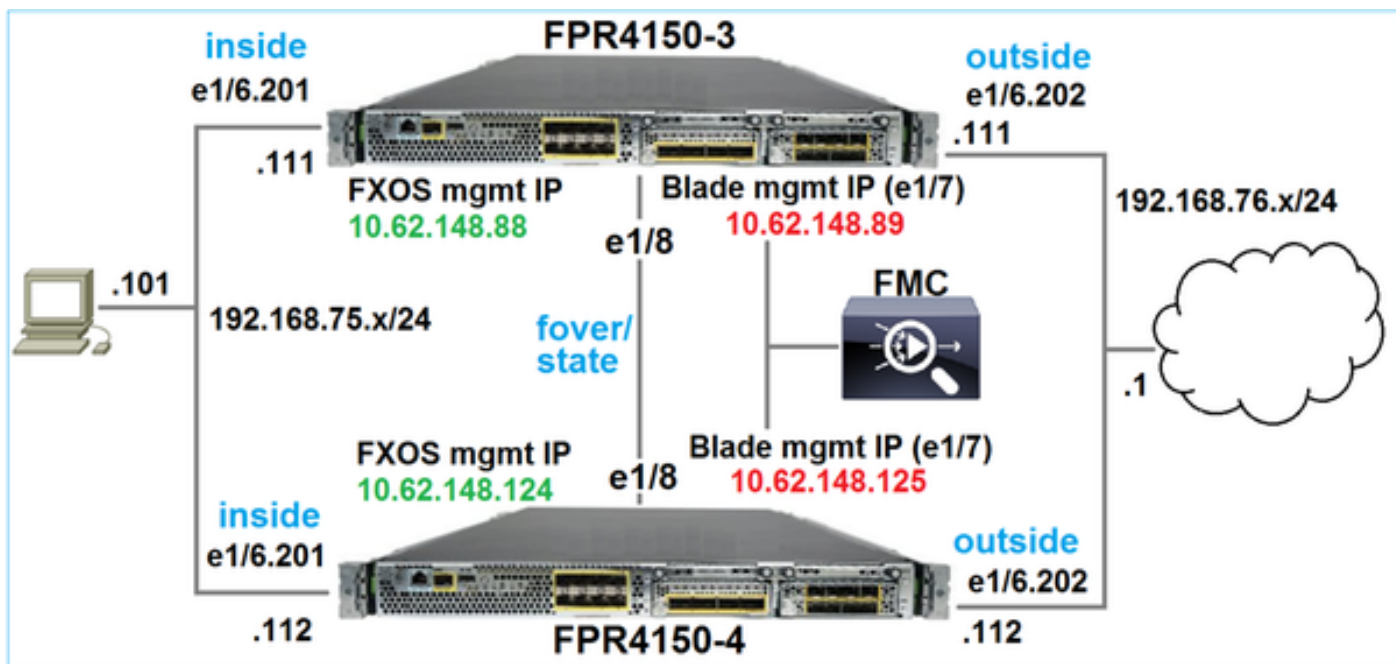
But

Le but de ce document est d'expliquer le processus de mise à niveau de la défense contre des menaces de FirePOWER (FTD) en mode facilement disponible sur des appliances de FirePOWER.

Composants de laboratoire

- 2 x FP4150
- 1 x FS4000
- 1 PC

Topologie



Les versions d'image logicielle avant de commencer l'activité :

- Centre de Gestion de FirePOWER (FMC) 6.1.0-330
- FTD 6.1.0-330 primaires
- FTD 6.1.0-330 secondaires
- FXOS 2.0.1-37 primaires
- FXOS 2.0.1-37 secondaires

Plan d'action

Étape 1 : Vérifiez les conditions préalables

Étape 2 : Téléchargez les images à FMC et à SSP

Étape 3 : Améliorez le FXOS secondaire 2.0.1-37 - > 2.0.1-86

Étape 4 : Permutez le Basculement FTD (vous aurez primaire/standby, secondaire/Active)

Étape 5 : Améliorez le FXOS primaire 2.0.1-37 - > 2.0.1-86

Étape 6 : Améliorez le FMC 6.1.0-330 - > 6.1.0.1

Étape 7 : Améliorez les paires 6.1.0-330 FTD ha - > 6.1.0.1

Étape 8 : Déployez une stratégie de FMC vers les paires FTD ha

Le processus de mise à niveau FTD ha

Étape 1 : Vérifiez les conditions préalables

Consultez le guide de compatibilité FXOS pour déterminer la compatibilité entre :

- Version de logiciel de la cible FTD et version de logiciel FXOS
- Plate-forme de FirePOWER HW et version de logiciel FXOS

<http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#pgfld-136544>

Vérifiez les notes de mise à jour FXOS de la version cible pour déterminer le chemin de mise à niveau FXOS :

http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos201/release/notes/fxos201_rn.html#pgfld-141076

Consultez les notes de mise à jour en version cible FTD pour déterminer le chemin de mise à niveau FTD :

<http://www.cisco.com/c/en/us/td/docs/security/firepower/601/6012/relnotes/firepower-system-release-notes-version-6012.html#pgfld-378288>

Étape 2 : Téléchargez les images

Sur les 2 FCMs téléchargez les images FXOS (fxos-k9.2.0.1.86.SPA)

Sur le téléchargement FMC la mise à jour FMC et FTD empaquette :

- Pour la mise à jour FMC : Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- Pour la mise à jour FTD : Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

Étape 3 : Améliorez le FXOS secondaire

Avant la mise à jour :

```
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

Commencez la mise à jour FXOS :

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

La mise à jour FXOS exigera une réinitialisation de châssis :

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

Vous pouvez surveiller la mise à jour FXOS du FXOS CLI. Chacun des 3 composants (FPRM, interconnexion de matrice et châssis) doit être mis à jour :

```
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 – Peu de minutes après avoir commencé le processus de mise à niveau FXOS vous pourriez être déconnecté de FXOS CLI et de GUI. Vous devriez pouvoir ouvrir une session de nouveau après peu de secondes.

Après la minute ~5 la mise à jour composante FPRM se termine :

```
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
```

Après ~10 minimum et comme partie du processus de mise à niveau FXOS le périphérique secondaire de FirePOWER redémarre :

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

Après la reprise les reprises de processus de mise à niveau :

```
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
```

Après le total de la minute ~30 la mise à jour FXOS se termine :

```
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
```

Étape 4 : Permutez les états de Basculement FTD

Avant la permutation les états de failover s'assurent que le module FTD sur le châssis secondaire est entièrement EN HAUSSE :

```
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
...
```

Permutez les états de Basculement FTD. Du FTD actif CLI :

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

Note - En ce moment vous pourriez faire lâcher le paquet ~1 du trafic de transit FTD

Étape 5 : Améliorez l'appliance primaire FXOS

Semblable à la mise à jour d'étape 2 l'appliance FXOS où le FTD primaire est installé - cette étape peut prendre ~30 minutes ou plus pour se terminer.

Étape 6 : Améliorez le logiciel FMC

Améliorez le FMC, dans ce scénario de 6.1.0-330 à 6.1.0.1.

Étape 7 : Améliorez les paires FTD ha

Avant la mise à jour :

```
> 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
...

```

Du menu de **système** > de mises à jour FMC initiez le processus de mise à niveau FTD ha :

The screenshot shows the Cisco FTD management console interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Deploy', 'System', 'Help', and 'admin'. Below this, there are tabs for 'Configuration', 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health', 'Monitoring', and 'Tools'. The 'Updates' tab is active, and within it, 'Product Updates' is selected. A 'Upload Update' button is visible. The current software version is 6.1.0. The 'Updates' section contains a table with the following data:

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	

Sur option vous pouvez lancer le contrôle de préparation de mise à jour FTD qui inclut un contrôle d'intégrité de DB FTD :

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

Currently running software version: 6.1.0

Selected Update

Type Cisco FTD SSP Patch
 Version 6.1.0.1-53
 Date Fri Dec 2 17:37:52 UTC 2016
 Release Notes
 Reboot Yes

By Group

▼ Ungrouped (1 total)

<input checked="" type="checkbox"/>	FTD4150-HA Cisco Firepower 4150 Threat Defense Cluster	Health Policy Initial Health Policy 2016-11-21 12:21:09	X	✓
<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	X	✓
<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	X	✓

Launch Readiness Check Install Cancel

Le contrôle a pris ~5 minimum et était réussi :

Deployments Health **Tasks** Settings ?

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

✓ **Remote Install** 5m 2s X

Apply to FTD4150-HA.
 Readiness Check To 10.62.148.125 Success

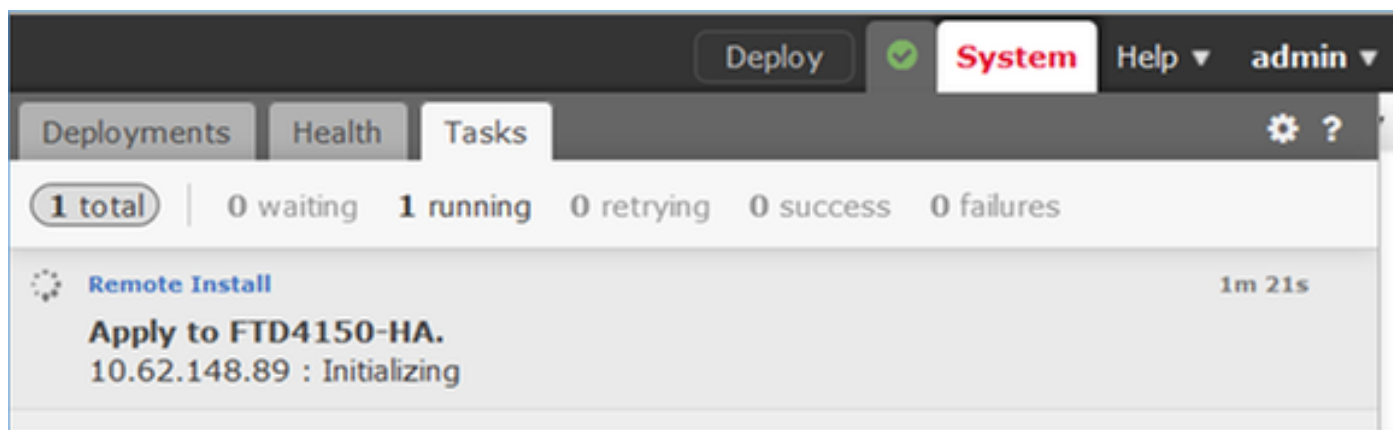
Initiez le processus d'installation :

▼ Ungrouped (1 total)

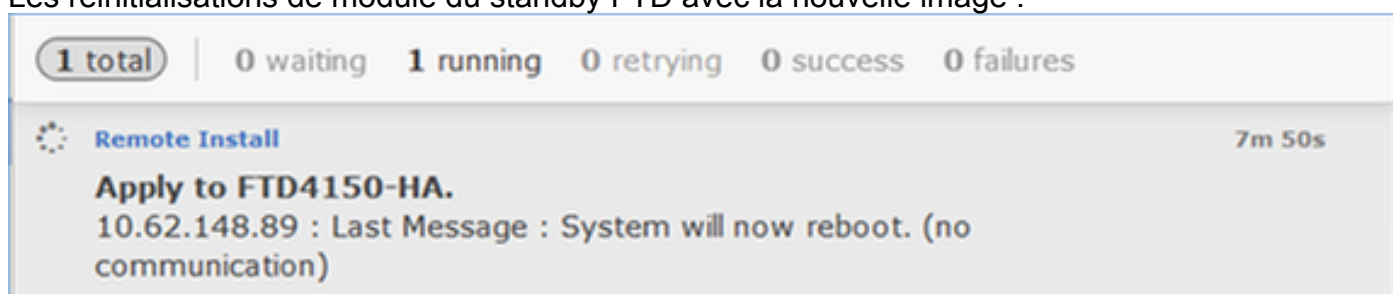
<input checked="" type="checkbox"/>	FTD4150-HA Cisco Firepower 4150 Threat Defense Cluster	Health Policy Initial Health Policy 2016-11-21 12:21:09	X	✓
<input checked="" type="checkbox"/>	FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy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

Launch Readiness Check Install Cancel

D'abord le primaire/standby FTD est mis à jour :



Les réinitialisations de module du standby FTD avec la nouvelle image :



Vous pouvez vérifier l'état FTD du mode FXOS BootCLI :

```
FPR4100-3-A# connect module 1 console
Firepower-module1> show services status
Services currently running:
Feature | Instance ID | State | Up Since
-----|-----|-----|-----
ftd | 001_JAD201200R4WLYCWO6 | RUNNING | :00:00:33
```

FTD secondaire/actif CLI affiche un message d'avertissement dû à la non-concordance de version de logiciel entre les modules FTD :

```
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
```

Le FMC prouve que le périphérique FTD a été avec succès mis à jour :

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

La mise à jour du deuxième module FTD commence :

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...

À la fin de l'opération le FTD secondaire démarre avec la nouvelle 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)

Au fond le FMC, utilisant l'utilisateur interne « enable_1 », permute les états de Basculement FTD et retire temporairement la configuration de Basculement du FTD secondaire :

```
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#
```

Note - En ce moment vous pourriez voir la perte de paquets ~1 due à la permutation d'état de Basculement

Dans ce cas la mise à jour entière FTD (les deux unités) a pris ~30 minutes :

Vérification

Vérification FTD CLI du périphérique primaire FTD :

```
> 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
...
>
```

Du périphérique secondaire FTD :

```

> 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
... >

```

Étape 8 : Déployez une stratégie vers les paires FTD ha

Après que la mise à jour soit terminée il y a le besoin de déployer une stratégie vers les paires ha. Ceci est affiché dans le FMC UI :

Deploy System Help admin

Deployments Health Tasks ?

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

✓ Remote Install 28m 14s ✕

Apply to FTD4150-HA.
Please reapply policies to your managed devices.

Déployez les stratégies :

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

Device

FTD4150-HA

- 🕒 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](#))

Vérification

Les paires mises à jour FTD ha en tant que lui vu du FMC UI :

Overview Analysis Policies **Devices** Objects AMP

Device Management NAT VPN QoS Platform Settings

Name	Group
<ul style="list-style-type: none"> Ungrouped (1) <ul style="list-style-type: none"> FTD4150-HA <ul style="list-style-type: none"> Cisco Firepower 4150 Threat Defense High Availability <ul style="list-style-type: none"> FTD4150-3(Primary, Active) <ul style="list-style-type: none"> 10.62.148.89 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed FTD4150-4(Secondary, Standby) <ul style="list-style-type: none"> 10.62.148.125 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed 	

Les paires mises à jour FTD ha en tant que lui vu du 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 : 13fcb60-c378

Documents connexes

[Cisco FirePOWER NGFW](#)