تثبيت الدفاع عن تهديد FirePOWER وترقيته على أجهزة ASA 55xx-X

المحتويات

المقدمة

يصف هذا المستند إجراءات تثبيت "الدفاع عن تهديد الطاقة النارية (FTD)" وترقيته وتسجيله على أجهزة ASA55xx-X.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA5508-X
- ASA الطراز X-5512
- FireSIGHT Management Center (FMC) يشغل الإصدار 6.0.1 (بنية 1213)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يُعدّ FTD أحد صور البرامج المُوحّدة التي يمكن تثبيتها على هذه الأنظمة الأساسية:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100 و FPR9300
- VMware (ESXi)
- Amazon Web Services (AWS)
- لوحة المفاتيح والفيديو والماوس
- الوحدة النمطية لموجه ISR Router Module

الهدف من هذا المستند هو توضيح ما يلي:

- تثبيت الإصدار 6.0.0 من FTD على النظام الأساسي ASA5508-X و ASA5512-X
- إجراء ترقية FTD من الإصدار 6.0.0 إلى 6.0.1
- تسجيل مركز إدارة Firepower (FMC) والتراخيص الأساسية

التكوين

الرسم التخطيطي للشبكة
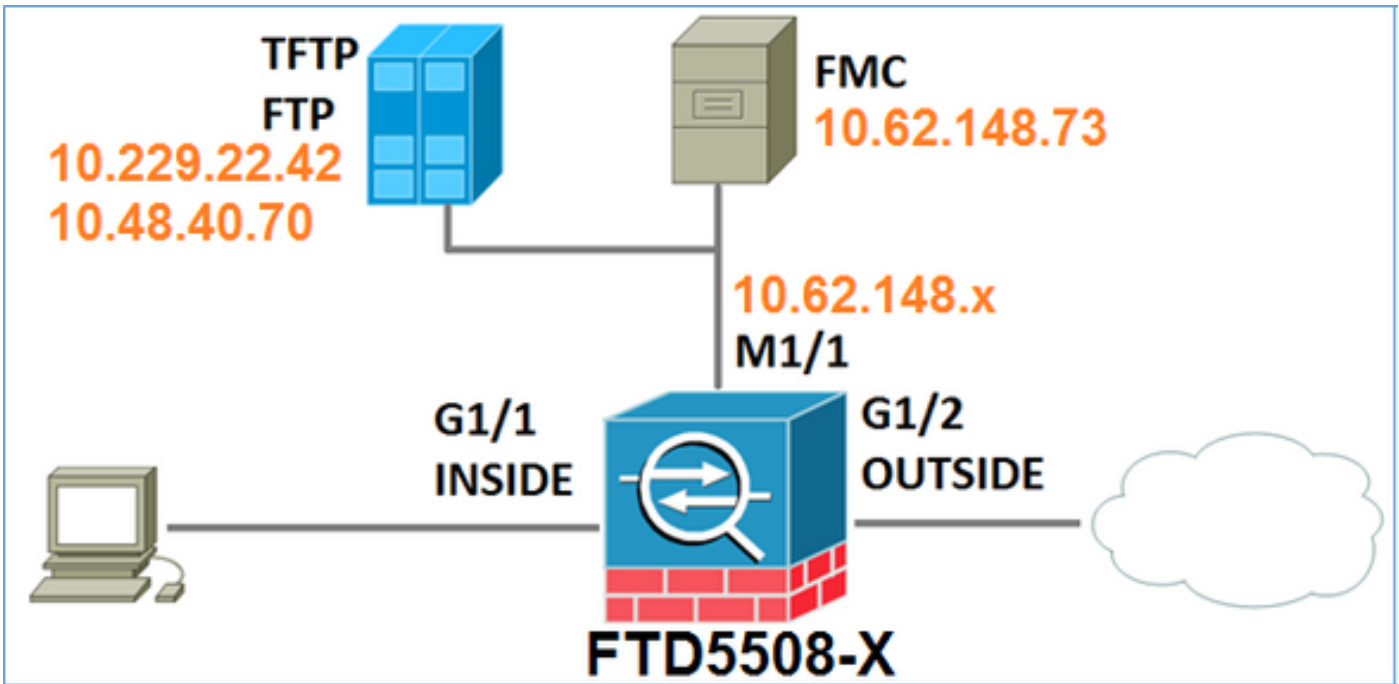
تنزيل برنامج FTD

انتقل إلى الجيل التالي من جدران الحماية (ASA > NGFW) مع خدمات ASA 5508-X > FirePOWER مع خدمات FirePOWER وحدد برنامج الدفاع ضد تهديد FirePOWER:

وعلى نحو مماثل لبرنامج ASA5512-X.

المهمة 1. التحقق من المتطلبات الأساسية

تحقق من المتطلبات الأساسية قبل تثبيت FTD.

الحل:

لتثبيت FTD، يمكنك إستخدام صورتين:

1. صورة OS (AKA Boot Image) - بالنسبة للدفاع ضد تهديد FirePOWER على ASA5506-X و ASA5506H-X و ASA5506W-X و ASA5508-X و ASA5516-X هو ملف lfbff.*. بالنسبة للدفاع عن تهديد FirePOWER على ASA5512-X، ASA5515-X، ASA5525-X، ASA5545-X، ASA5555-X) Salyn) هو ملف cdisk.*.
2. صورة النظام - هذا ملف pkg.
قبل متابعة تثبيت FTD، تحقق مما يلي:

- يجب أن يحتوي ذاكرة ASA المؤقتة على مساحة حرة لا تقل عن 3. 1 جيجابايت (3 جيجابايت بايت + حجم صورة التمهيد)
- يتم تحميل صورة التمهيد إلى خادم TFTP
- يتم تحميل صورة النظام إلى خادم HTTP أو FTP
- OnASA5506/08/16 يكون ROMMON إصدارا 1.1.8 على الأقل

تحقق من المساحة الخالية:

```
FTD5508X# show flash | i free
(bytes total (4273819648 bytes free 7859437568
```

تحقق من هذه الصور:

اسم الملف	الوصف
ftd-boot-9.6.1.0.lfbff	صورة تمهيد الدفاع ضد تهديد الحماية ضد Firepower لـ 5516/5508/5506. هذه هي صورة التمهيد للتثبيت النظيف على 5516/5508/5506
ftd-boot-9.6.1.0.cdisk	V6. 0. 1 صورة تمهيد الدفاع ضد تهديد Firepower لـ ASA

5512/5515/5525/554 5/5555. هذه هي صورة التمهيد للتثبيت النظيف على 554/5525/5515/5512 5555/5 الدفاع ضد تهديد Firepower لجميع أجهزة ASA المدعومة: 551/5512/5508/5506 55/5545/5525/5516/5 555. هذه صورة النظام للتثبيت النظيف	FTD-6.0.0-1005.pkg

المهمة 2. ترقية ASA5508-X ROMMON

كما هو مذكور في المتطلبات الأساسية، يجب أن تكون أجهزة ASA5506-X و ASA5508-X و ASA5516-X على
ROMMON v1.1.8. إذا لم تكن كذلك، قم بتثبيت ASA5500-FIRMWARE-1108.SPA (متوفر في صفحة تنزيل
Cisco ASA).

متطلبات المهمة:

ترقية ASA5508 ROMMON من 1.1.1 إلى 1.1.8.

الحل:

يتم وصف الإجراء في دليل ترقية ASA ROMMON.

الخطوة 1. التحقق من إصدار ROMMON الموجود:

```
                                                   FTD5508X# show module
 Mod  Card Type                                    Model            Serial No.
 ----------- ----------------- ------------------------------------------ ----
 ASA 5508-X with FirePOWER services, 8GE, AC, ASA5508        JAD192100SZ 1
 sfr FirePOWER Services Software Module        ASA5508          JAD192100SZ

     Mod  MAC Address Range           Hw Version  Fw Version  Sw Version
 --------------- ----------- ----------- ------------------------------- ----
     (188b.9d1e.ca7c to 188b.9d1e.ca84  1.0        1.1.1       9.5(2 1
     sfr 188b.9d1e.ca7b to 188b.9d1e.ca7b  N/A        N/A        5.4.1-211
```

الخطوة 2.تنزيل البرامج الثابتة ROMMON في ذاكرة ASA flash:

```
FTD5508X# copy ftp://10.48.40.70/ANG/mzafeiro/asa5500-firmware-1108.SPA disk0:asa5500-firmware-
                                                                      1108.SPA
                                   Address or name of remote host [10.48.40.70]?

              Source filename [ANG/mzafeiro/asa5500-firmware-1108.SPA]?

                   Destination filename [asa5500-firmware-1108.SPA]?

                      Accessing ftp://10.48.40.70/ANG/mzafeiro/asa5500-firmware-
                      1108.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Done!
```

```
Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
eefe8f182491652ee4c05e6e751f7a4f
5cdea28540cf60acde3ab9b65ff55a9f
4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
eefe8f182491652ee4c05e6e751f7a4f
5cdea28540cf60acde3ab9b65ff55a9f
4e0cfb84b9e2317a856580576612f4af
```

Digital signature successfully validated
```
...Writing file disk0:/asa5500-firmware-1108.SPA
!!!!!!!!!!
(bytes copied in 18.890 secs (513411 bytes/sec 9241408
```

الخطوة 3. ترقية صورة ASA ROMMON:

```
FTD5508X# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
eefe8f182491652ee4c05e6e751f7a4f
5cdea28540cf60acde3ab9b65ff55a9f
4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
eefe8f182491652ee4c05e6e751f7a4f
5cdea28540cf60acde3ab9b65ff55a9f
4e0cfb84b9e2317a856580576612f4af
```

Digital signature successfully validated
```
File Name                       : disk0:/asa5500-firmware-1108.SPA
               Image type                     : Release
                             Signer Information
               Common Name            : abraxas
           Organization Unit    : NCS_Kenton_ASA
          Organization Name     : CiscoSystems
             Certificate Serial Number : 55831CF6
               Hash Algorithm        : SHA2 512
             Signature Algorithm     : 2048-bit RSA
                  Key Version          : A
```
.Verification successful
```
System config has been modified. Save? [Y]es/[N]o: Y
Cryptochecksum: cb47de8a cad3b773 7fc07212 3e76ef4f

bytes copied in 0.260 secs 2804
```
[Proceed with reload? [confirm

```
                                          ***
            --- START GRACEFUL SHUTDOWN --- ***
                                          ***
                :Message to all terminals ***
                                          ***
```
.Performing upgrade on rom-monitor *
```
          Shutting down License Controller
               Shutting down File system

                                          ***
            --- SHUTDOWN NOW --- ***
```

```
                                                                      ***
                                            :Message to all terminals ***
                                                                      ***
                                      .Performing upgrade on rom-monitor ***
                                                   Process shutdown finished
                                                            .....Rebooting
                                     INIT: Sending processes the TERM signal
                                .Deconfiguring network interfaces... done
                                   ...Sending all processes the TERM signal
                                   ...Sending all processes the KILL signal
                                                     ...Deactivating swap
                                        ...Unmounting local filesystems
                                                              ...Rebooting
                                             Rom image verified correctly


                          Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
                              .Copyright (c) 1994-2014  by Cisco Systems, Inc
                              Compiled Mon 10/20/2014 15:59:12.05 by builder



                                         Current image running: Boot ROM0
                                     Last reset cause: PowerCycleRequest
                                                 DIMM Slot 0 : Present
                                                 DIMM Slot 1 : Present
                                (INFO: Rommon upgrade state: ROMMON_UPG_START (1
                                              INFO: Reset code: 0x00002000


        Firmware upgrade step 1... Looking for file 'disk0:asa5500-firmware-1108.SPA' Located 'asa5500-
                                              .firmware-1108.SPA' @ cluster 856765


        #####################################################################################
                                          Image base 0x77014018, size 9241408
                                                      .LFBFF signature verified
                                    (Objtype: lfbff_object_rommon (0x800000 bytes @ 0x77014238
                                     (Objtype: lfbff_object_fpga (0xd0100 bytes @ 0x77814258
                                       INFO: FPGA version in upgrade image: 0x0202
                                      INFO: FPGA version currently active: 0x0202
                                            .INFO: The FPGA image is up-to-date
        .INFO: Rommon version currently active: 1.1.01. INFO: Rommon version in upgrade image: 1.1.08
                                       Active ROMMON: Preferred 0, selected 0, booted 0
                                            .Switching SPI access to standby rommon 1
            Please DO NOT reboot the unit, updating ROMMON................... INFO: Duplicating machine
        state...... Reloading now as step 1 of the rommon upgrade process... Toggling power on system
                                              board... Rom image verified correctly

                          Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
                              .Copyright (c) 1994-2014  by Cisco Systems, Inc
                              Compiled Mon 10/20/2014 15:59:12.05 by builder



                                         Current image running: Boot ROM0
                                           Last reset cause: RP-Reset
                                                 DIMM Slot 0 : Present
                                                 DIMM Slot 1 : Present
                                (INFO: Rommon upgrade state: ROMMON_UPG_START (1
                                              INFO: Reset code: 0x00000008
                                     Active ROMMON: Preferred 0, selected 0, booted 0


                                                       ...Firmware upgrade step 2
                  Detected current rommon upgrade is available, continue rommon upgrade process
                                              Rommon upgrade reset 0 in progress
                                ...Reloading now as step 2 of the rommon upgrade process
```

```
                                               Rom image verified correctly


                       Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
                              .Copyright (c) 1994-2015  by Cisco Systems, Inc
                              Compiled Thu 06/18/2015 12:15:56.43 by builders


                   Current image running: *Upgrade in progress* Boot ROM1
                                        Last reset cause: BootRomUpgrade
                                              DIMM Slot 0 : Present
                                              DIMM Slot 1 : Present
                        (INFO: Rommon upgrade state: ROMMON_UPG_START (1
                                        INFO: Reset code: 0x00000010
                                        PROM B: stopping boot timer
                            Active ROMMON: Preferred 0, selected 0, booted 1
                              INFO: Rommon upgrade state: ROMMON_UPG_TEST


          !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
          !! Please manually or auto boot ASAOS now to complete firmware upgrade !!
          !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


                              Platform ASA5508 with 8192 Mbytes of main memory
                                      MAC Address: 18:8b:9d:1e:ca:7c


                                   .Use BREAK or ESC to interrupt boot
                                   .Use SPACE to begin boot immediately


                                  .Located '.boot_string' @ cluster 859024

                                                                           #
                       "Attempt autoboot: "boot disk0:/asa952-lfbff-k8.SPA
                          .Located 'asa952-lfbff-k8.SPA' @ cluster 818273

##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
                                  ####################################
                                        .LFBFF signature verified
                                        INIT: version 2.88 booting
                                                Starting udev
                                   .Configuring network interfaces... done
                                             Populating dev cache
                                    dosfsck 2.11, 12 Mar 2005, FAT32, LFN
                     .There are differences between boot sector and its backup
                                        (Differences: (offset:original/backup
                                                           65:01/00
                                        .Not automatically fixing this
                                             .Starting check/repair pass
                                                    csco_config/
                                   .is missing. Can't fix this yet "."
                                                    csco_config/
                                   .is missing. Can't fix this yet ".."
                                             .Starting verification pass
                                                    csco_config/
                                   .is missing. Can't fix this yet "."
```

```
                                                                    csco_config/
                                           .is missing. Can't fix this yet ".."
                                  dev/sdb1: 182 files, 849380/1918808 clusters/
                                                    dosfsck(/dev/sdb1) returned 0
                                                            IO Memory Nodes: 1
                                          IO Memory Per Node: 499122176 bytes

                         Global Reserve Memory Per Node: 314572800 bytes Nodes=1

                                                Processor memory 3807834603
         LCMB: got 499122176 bytes on numa-id=0, phys=0x1b8000000, virt=0x2aaaaae00000
          LCMB: HEAP-CACHE POOL got 314572800 bytes on numa-id=0, virt=0x2aaac8a00000

                                       Compiled on Sat 28-Nov-15 00:16 PST by builders

                                                            Total NICs found: 13
            i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: 188b.9d1e.ca7c
             ivshmem rev03 Backplane Data Interface    @ index 09 MAC: 0000.0001.0002
             en_vtun rev00 Backplane Control Interface @ index 10 MAC: 0000.0001.0001
    en_vtun rev00 Backplane Int-Mgmt Interface    @ index 11 MAC: 0000.0001.0003
    en_vtun rev00 Backplane Ext-Mgmt Interface    @ index 12 MAC: 0000.0000.0000
                                       .Rom-monitor was successfully upgraded
                                                                           ...
```

التحقق من الصحة:

يمكنك إستخدام الأمر show module للتحقق من إصدار برنامج ROMMON:

```
                                                               FTD5508X> enable
                                                                     :Password
                                                           FTD5508X# show module

 .Mod  Card Type                                       Model            Serial No
----------- ----------------- ------------------------------------------- ----
ASA 5508-X with FirePOWER services, 8GE, AC, ASA5508         JAD192100SZ 1
sfr FirePOWER Services Software Module       ASA5508          JAD192100SZ

    Mod  MAC Address Range              Hw Version  Fw Version  Sw Version
-------------- ------------ ------------ ------------------------------- ----
    (188b.9d1e.ca7c to 188b.9d1e.ca84  1.0        1.1.8      9.5(2 1
   sfr 188b.9d1e.ca7b to 188b.9d1e.ca7b  N/A        N/A        5.4.1-211
```

المهمة 3. تثبيت صورة تمهيد FTD على ASA55xx-X

متطلبات المهمة:

قم بتثبيت صورة تمهيد FTD-boot-9.6.1.0.lfbff على ASA5508-X.

الحل:

هناك أكثر من طريقة للقيام بذلك. هنا أول واحد:

الطريقة 1. من موقع ROMMON

الخطوة 1. أعد تحميل ASA وأدخل وضع ROMmon:

```
                                              FTD5508X# reload
                                   [Proceed with reload? [confirm
                                                        #FTD5508X

                                                              ***
                       --- START GRACEFUL SHUTDOWN --- ***
                                         Shutting down isakmp
                                         Shutting down webvpn
                                      Shutting down sw-module
                            Shutting down License Controller
                                    Shutting down File system


                                                              ***
                                    --- SHUTDOWN NOW --- ***
                                   Process shutdown finished
                                          .....Rebooting
                      INIT: Sending processes the TERM signal
                    .Deconfiguring network interfaces... done
                   ...Sending all processes the TERM signal
                   ...Sending all processes the KILL signal
                                  ...Deactivating swap
                           ...Unmounting local filesystems
                                       Rebooting... ÿ
                               Rom image verified correctly


              Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
                      .Copyright (c) 1994-2015  by Cisco Systems, Inc
                      Compiled Thu 06/18/2015 12:15:56.43 by builders


                                 Current image running: Boot ROM1
                           Last reset cause: PowerCycleRequest
                                       DIMM Slot 0 : Present
                                       DIMM Slot 1 : Present

                      Platform ASA5508 with 8192 Mbytes of main memory
                            MAC Address: 18:8b:9d:1e:ca:7c


                           .Use BREAK or ESC to interrupt boot
                           .Use SPACE to begin boot immediately
                                    .Boot interrupted

                                          < rommon 1
```

الخطوة 2. تكوين إعدادات الشبكة الأساسية:

```
                          rommon 1 > ADDRESS=10.62.148.29
                           rommon 2 > SERVER=10.229.22.42
                           rommon 3 > GATEWAY=10.62.148.1
                 rommon 4 > IMAGE=ftd-boot-9.6.1.0.1fbff
                        rommon 5 > netmask 255.255.255.128
                            rommon 6 > ping 10.229.22.42
    Sending 10, 32-byte ICMP Echoes to 10.229.22.42 timeout is 4 seconds
                                           !!!!!!!!!!?
                            (Success rate is 90 percent (9/10
                                     rommon 7 > sync
                                  rommon 8 > tftpdnld
                          ADDRESS: 10.62.148.29
                          NETMASK: 255.255.255.128
                          GATEWAY: 10.62.148.1
```

```
                                        SERVER: 10.229.22.42
                              IMAGE: ftd-boot-9.6.1.0.lfbff
                               MACADDR: 18:8b:9d:1e:ca:7c
                                      VERBOSITY: Progress
                                              RETRY: 40
                                       PKTTIMEOUT: 7200
                                          BLKSIZE: 1460
                                         CHECKSUM: Yes
                                            PORT: GbE/1
                                  PHYMODE: Auto Detect
                             Receiving ftd-boot-9.6.1.0.lfbff from
10.229.22.42!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                             .. !!!!!!!!!!!!!!!!!!!!!!!! .. output omitted
         !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                                           .File reception completed
                                          Boot buffer bigbuf=348bd018
                            Boot image size = 100308208 (0x5fa94f0) bytes
                                         image size]       100308208]
                   MD5 signaure]     781dde41844d750f8c0db1cd1e1e164f]
                                            .LFBFF signature verified
                                          INIT: version 2.88 booting
                                                       Starting udev
                            .Configuring network interfaces... done
                                           Populating dev cache
                                           .Detected PID ASA5508
                            .Found device serial number JAD192100SZ
                                    Found USB flash drive /dev/sdb
                                    Found hard drive(s):  /dev/sda
                                    fsck from util-linux 2.23.2
                              dosfsck 2.11, 12 Mar 2005, FAT32, LFN
       dev/sdb1: 47 files, 24618/1919063 clusters ==============================================/
       Launching boot CLI ... Configuring network interface using static IP Bringing up network
    interface. Depending on your network, this might take a couple of minutes when using DHCP...
                      ifup: interface lo already configured Using IPv4 address: 10.62.148.62
                            Using IPv6 address: fe80::1a8b:9dff:fe1e:ca7b
                                    Using DNS server: 10.62.145.72
                                 Using default gateway: 10.62.148.100
                           .INIT: Starting system message bus: dbus
                         Starting OpenBSD Secure Shell server: sshd
                                    ...generating ssh RSA key
                                    ...generating ssh ECDSA key
                                    ...generating ssh DSA key
                                                      .done
                  .Starting Advanced Configuration and Power Interface daemon: acpid
                                         acpid: starting up

                                         acpid: 1 rule loaded

                              acpid: waiting for events: event logging is off

                                           Starting ntpd: done
                                         .:Starting syslog-ng
                                         Starting crond: OK


                              (.Cisco FTD Boot 6.0.0 (9.6.1
                             Type ? for list of commands
                                             <firepower-boot
```

في ASA5512/15/25/45/55 يكون الإجراء هو نفسه مع أختلاف فقط في اسم صورة التمهيد:

```
rommon #0> ADDRESS=10.62.148.10
rommon #1> SERVER=10.229.22.42
rommon #2> GATEWAY=10.62.148.1
rommon #3> IMAGE=ftd-boot-9.6.1.0.cdisk
```

الطريقة 2. من وضع ASA

الخطوة 1. من وضع ASA EXEC (لا ROMMON) انسخ صورة تمهيد FTD إلى ذاكرة ASA flash:

```
ciscoasa# copy ftp://10.48.40.70/ANG/mzafeiro/ftd-boot-9.6.1.0.lfbff flash
```
الخطوة 2. احذف أي صور ASA من القرص:

```
*ciscoasa# delete flash:asa
```
محتويات Flash بعد أن تقوم بحذف صور ASA:

```
ciscoasa# show flash
--#--   path--      -----date/time------      length--
131   33      .boot_string      May 20 2016 09:27:28
11    4096    log                Mar 03 2016 11:48:34
154   16767   log/asa-appagent.log      May 20 2016 09:23:48
155   465     log/asa-ssp_ntp.log      Mar 03 2016 11:54:58
21    4096    crypto_archive      Jun 10 2015 06:45:42
22    4096    coredumpinfo      Jun 10 2015 06:46:00
23    59      coredumpinfo/coredump.cfg      Jun 10 2015 06:46:00
134   25627616 asdm-752.bin      Dec 01 2015 04:01:58
135   52563   system.cfg      Feb 09 2016 02:49:58
136   25028660 asdm-751-112.bin      Feb 09 2016 02:50:28
137   38409858 anyconnect-win-3.1.10010-k9.pkg      Feb 09 2016 02:51:14
138   25629676 asdm-752-153.bin      Feb 09 2016 04:38:10
--> May 20 2016 09:39:57 ftd-boot-9.6.1.0.lfbff 100308208 151
```
الخطوة 3.إعادة تحميل ASA. يتم تمهيده من صورة تمهيد FTD:

```
Located 'ftd-boot-9.6.1.0.lfbff' @ cluster 45093.
######################################################################
..
LFBFF signature verified.
INIT: version 2.88 booting
..

Cisco FTD Boot 6.0.0 (9.6.1).)
Type ? for list of commands
firepower-boot>
```

المهمة 4. تثبيت صورة نظام FTD على ASA55xx-X

تثبيت صورة نظام FTD على ASA5508-X.

الحل

```
firepower-boot> setup
```

```
                                Welcome to Cisco FTD Setup
                                  [hit Ctrl-C to abort]
                                [] Default values are inside

                                      Enter a hostname [firepower]: FTD5508
                :[Do you want to configure IPv4 address on management interface?(y/n) [Y
      Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]: N
                                            Enter an IPv4 address: 10.62.148.29
                                          Enter the netmask: 255.255.255.128
                                          Enter the gateway: 10.62.148.1
  Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]: Enter
         an IPv4 address [10.62.148.29]: Enter the netmask [255.255.255.128]: Enter the gateway
    [10.62.148.1]: Do you want to configure static IPv6 address on management interface?(y/n) [N]:
  Stateless autoconfiguration will be enabled for IPv6 addresses. Enter the primary DNS server IP
                                          address: 173.38.200.100
                    Do you want to configure Secondary DNS Server? (y/n) [n]: y
                    Enter the secondary DNS server IP address: 144.254.71.184
                         :[Do you want to configure Local Domain Name? (y/n) [n
                         :[Do you want to configure Search domains? (y/n) [n
                               :[Do you want to enable the NTP service? [Y
           Enter the NTP servers separated by commas [203.0.113.126]: 171.68.38.65
                                     :Please review the final configuration
                           Hostname:              FTD5508
                           Management Interface Configuration

                                  IPv4 Configuration:       static
                            IP Address:       10.62.148.29
                          Netmask:          255.255.255.128
                           Gateway:          10.62.148.1

                      IPv6 Configuration:       Stateless autoconfiguration

                                           :DNS Configuration
                                           :DNS Server
                            173.38.200.100
                            144.254.71.184

                                           :NTP configuration
                            171.68.38.65
                                                  :CAUTION
      You have selected IPv6 stateless autoconfiguration, which assigns a global address
      based on network prefix and a device identifier. Although this address is unlikely
                .to change, if it does change, the system will stop functioning correctly
                          .We suggest you use static addressing instead

                                           :[Apply the changes?(y,n) [Y
                            !Configuration saved successfully
                            ...Applying
                            .Done
                            ...Press ENTER to continue
                            <firepower-boot
```

التحقق من الاتصال بخادم FTP:

```
                            firepower-boot> ping 10.229.22.42
              .PING 10.229.22.42 (10.229.22.42) 56(84) bytes of data
      bytes from 10.229.22.42: icmp_seq=1 ttl=124 time=1.30 ms 64
      bytes from 10.229.22.42: icmp_seq=2 ttl=124 time=1.32 ms 64
      bytes from 10.229.22.42: icmp_seq=3 ttl=124 time=1.45 ms 64
                                                  C^
```

```
                                    --- ping statistics 10.229.22.42 ---
packets transmitted, 3 received, 0% packet loss, time 2002ms 3
                            rtt min/avg/max/mdev = 1.302/1.360/1.458/0.075 ms
```

تثبيت حزمة النظام:

```
firepower-boot> system install ftp://10.229.22.42/ftd-6.0.0-1005.pkg

############################ WARNING ########################
# !The content of disk0: will be erased during installation #
############################################################

                                    Do you want to continue? [y/N] y
                                                    ... Erasing disk0
                                                            Verifying

                            Enter credentials to authenticate with ftp server
                                                        Username: ftp
                                                             :Password
(Verifying Downloading Extracting                 <-- Here give it some time (~10 min
                                                        Package Detail
            Description:                     Cisco ASA-NGFW 6.0.0-1005 System Install
                                Requires reboot:            Yes

            Do you want to continue with upgrade? [y]:    <-- Press Enter
                .Warning: Please do not interrupt the process or turn off the system
                                    .Doing so might leave system in unusable state

                                                    ... Starting upgrade process
                    (Populating new system image       <-- Here give it some time (~5 min

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system. <-- Press Enter


        Broadcast message from root@firepowStopping OpenBSD Secure Shell server: sshdstopped
                                                    (/usr/sbin/sshd (pid 1963
                                                                    .
(Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 1967
                                                            acpid: exiting

                                                                    .acpid
                                            .Stopping system message bus: dbus
            (Stopping ntpd: stopped process in pidfile '/var/run/ntp.pid' (pid 2055
                                                                    done
                                                    Stopping crond: OK
                                    .Deconfiguring network interfaces... done
                                    ...Sending all processes the TERM signal
                                    ...Sending all processes the KILL signal
                                                ...Deactivating swap
                                        ...Unmounting local filesystems
                                                    Rebooting... ÿ
                                        Rom image verified correctly


                        Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
                            .Copyright (c) 1994-2015  by Cisco Systems, Inc
                            Compiled Thu 06/18/2015 12:15:56.43 by builders


                                        Current image running: Boot ROM1
                                    Last reset cause: PowerCycleRequest
                                                DIMM Slot 0 : Present
                                                DIMM Slot 1 : Present
```

```
                              Platform ASA5508 with 8192 Mbytes of main memory
                                        MAC Address: 18:8b:9d:1e:ca:7c


                                   .Use BREAK or ESC to interrupt boot
                                   .Use SPACE to begin boot immediately


                              .Located '.boot_string' @ cluster 186016

                                                                      #
                                  "Attempt autoboot: "boot disk0:os.img
                                     .Located 'os.img' @ cluster 160001

                              #######################################
                                             .LFBFF signature verified
                                           INIT: version 2.88 booting
                                                        Starting udev
                                .Configuring network interfaces... done
                                             Populating dev cache
                                              .Detected PID ASA5508
                                .Found device serial number JAD192100SZ
                                       Found USB flash drive /dev/sdb
                                       Found hard drive(s):  /dev/sda
                                           fsck from util-linux 2.23.2
                                    dosfsck 2.11, 12 Mar 2005, FAT32, LFN
                              dev/sdb1: 7 files, 26064/1919063 clusters/


                              ===============================================
                              .Use ESC to interrupt boot and launch boot CLI
                                 .Use SPACE to launch Cisco FTD immediately
                                         ... Cisco FTD launch in 20 seconds
                                                      Running on kenton
                                            ... Mounting disk partitions
[  Initializing Threat Defense ...                                    [  OK
[  Starting system log daemon...                                      [  OK
          Flushing all current IPv4 rules and user defined chains: ...success
          Clearing all current IPv4 rules and user defined chains: ...success
                                       :Applying iptables firewall rules
                                            'Flushing chain `PREROUTING
                                               'Flushing chain `INPUT
                                              'Flushing chain `FORWARD
                                               'Flushing chain `OUTPUT
                                            'Flushing chain `POSTROUTING
                                               'Flushing chain `INPUT
                                              'Flushing chain `FORWARD
                                               'Flushing chain `OUTPUT
                                              Applying rules successed
          Flushing all current IPv6 rules and user defined chains: ...success
          Clearing all current IPv6 rules and user defined chains: ...success
                                      :Applying ip6tables firewall rules
                                            'Flushing chain `PREROUTING
                                               'Flushing chain `INPUT
                                              'Flushing chain `FORWARD
                                               'Flushing chain `OUTPUT
                                            'Flushing chain `POSTROUTING
                                               'Flushing chain `INPUT
                                              'Flushing chain `FORWARD
                                               'Flushing chain `OUTPUT
                                              Applying rules successed
                                                   ...Starting nscd
[  mkdir: created directory '/var/run/nscd'                           [  OK
```

```
              Starting , please wait...grep: /ngfw/etc/motd: No such file or directory
                                                                       .complete...
                                                   Firstboot detected, executing scripts
[ Executing S01reset_failopen_if                                                 [  OK
[ Executing S04fix-httpd.sh                                                      [  OK
[ Executing S05set-mgmnt-port                                                    [  OK
[ Executing S06addusers                                                          [  OK
[ Executing S07uuid-init                                                         [  OK
[ Executing S09configure_mysql                                                   [  OK


                                          ********* Attention ************

                     Initializing the configuration database.  Depending on available
                 system resources (CPU, memory, and disk), this may take 30 minutes
                                                                 .or more to complete

                                          ********* Attention ************

                   [  Executing S10database                                      [  OK
                   [  Executing S12install_infodb                                 [  OK
                   [  Executing S15set-locale.sh                                  [  OK
                   [  Executing S16update-sensor.pl                               [  OK
                   [  Executing S19cert-tun-init                                  [  OK
                   [  Executing S20cert-init                                      [  OK
                   [  Executing S21disable_estreamer                              [  OK
                   [  Executing S25create_default_des.pl                          [  OK
                   [  Executing S30init_lights_out_mgmt.pl                        [  OK
                   [  Executing S40install_default_filters.pl                     [  OK
                   [  Executing S42install_default_dashboards.pl                  [  OK
                   [  Executing S43install_default_report_templates.pl            [  OK
                   [  Executing S44install_default_app_filters.pl                 [  OK
                   [  Executing S45install_default_realms.pl                      [  OK
                   [  Executing S47install_default_sandbox_EO.pl                  [  OK
                   [  Executing S50install-remediation-modules                    [  OK
                   [  Executing S51install_health_policy.pl                       [  OK
                   [  Executing S52install_system_policy.pl                       [  OK
                   [  Executing S53change_reconciliation_baseline.pl              [  OK
                   [  Executing S70update_sensor_objects.sh                       [  OK
                   [  Executing S85patch_history-init                             [  OK
                   [  Executing S90banner-init                                    [  OK
                   [  Executing S95copy-crontab                                   [  OK
                   [  Executing S96grow_var.sh                                    [  OK


                                         ********** Attention **********

                   Initializing the system's localization settings.  Depending on available
                        system resources (CPU, memory, and disk), this may take 10 minutes
                                                                      .or more to complete

                                         ********** Attention **********
[ Executing S96localize-templates                                                [  OK
[ Executing S96ovf-data.pl                                                       [  OK
[ Executing S97compress-client-resources                                         [  OK
[ Executing S97create_platinum_forms.pl                                          [  OK
[ Executing S97install_cloud_support.pl                                          [  OK
[ Executing S97install_geolocation.pl                                            [  OK
[ Executing S97install_ssl_inspection.pl                                         [  OK
[ Executing S97update_modprobe.pl                                                [  OK
[ Executing S98check-db-integrity.sh                                             [  OK
[ Executing S98htaccess-init                                                     [  OK
[ Executing S99correct_ipmi.pl                                                   [  OK
[ Executing S99start-system                                                      [  OK
[ Executing S99z_db_restore                                                      [  OK
                                                           .Firstboot scripts finished
```

```
                   [  Configuring NTP...                                      [  OK
                                      Model reconfigure detected, executing scripts
                                                                    Pinging mysql
                                                              Found mysql is running
                   [  Executing 45update-sensor.pl                            [  OK
                   [  Executing 55recalculate_arc.pl                          [  OK
                                                                 :Starting xinetd
                                                       Mon Mar 14 18:28:11 UTC 2016
                                                                ...Starting MySQL
                                                                    Pinging mysql
                                                              Pinging mysql, try 1
                                                              Found mysql is running
                                                       ...Running initializeObjects
                                                                 ...Stopping MySQL
                                                       Killing mysqld with pid 10993
                                                          Wait for mysqld to exit\c
                                                                             done
                                                       Mon Mar 14 18:28:21 UTC 2016
                   [  Starting sfifd...                                       [  OK
                        !Starting Cisco ASA5508-X Threat Defense, please wait...No PM running
                                                                      .started...
                                              .INIT: Starting system message bus: dbus
                                     Starting OpenBSD Secure Shell server: sshd
                                                          ...generating ssh RSA key
                                                        ...generating ssh ECDSA key
                                                          ...generating ssh DSA key
                                                                            .done
                    .Starting Advanced Configuration and Power Interface daemon: acpid
                                                               Starting crond: OK
Mar 14 18:28:26 ciscoasa SF-IMS[11490]: [11490] init script:system [INFO] pmmon Setting affinity
                                                                        ...to 5-7
                                              pid 11486's current affinity list: 0-7
                                                 pid 11486's new affinity list: 5-7
      Mar 14 18:28:26 ciscoasa SF-IMS[11492]: [11492] init script:system [INFO] pmmon The Process
                                                          ...Manager is not running
    Mar 14 18:28:26 ciscoasa SF-IMS[11493]: [11493] init script:system [INFO] pmmon Starting the
                                                               ...Process Manager
            Mar 14 18:28:26 ciscoasa SF-IMS[11494]: [11494] pm:pm [INFO] Using model number 75K


                                        (Cisco ASA5508-X Threat Defense v6.0.0 (build 1005
                                                                   :ciscoasa login
                                            Compiled on Sat 07-Nov-15 16:13 PST by builders


                                                             Total NICs found: 13
                 i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: 188b.9d1e.ca7c
                ivshmem rev03 Backplane Data Interface     @ index 09 MAC: 0000.0001.0002
               en_vtun rev00 Backplane Control Interface  @ index 10 MAC: 0000.0001.0001
         en_vtun rev00 Backplane Int-Mgmt Interface       @ index 11 MAC: 0000.0001.0003
         en_vtun rev00 Backplane Ext-Mgmt Interface       @ index 12 MAC: 0000.0000.0000


                                        INFO: Unable to read firewall mode from flash
                              Writing default firewall mode (single) to flash

                                        INFO: Unable to read cluster interface-mode from flash
                                      Writing default mode "None" to flash
                              ...Verify the activation-key, it might take a while
                                        .Failed to retrieve permanent activation key
          Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
                       :The Running Activation Key is not valid, using default settings


                                                     :Licensed features for this platform
                      Maximum Physical Interfaces        : Unlimited       perpetual
                      Maximum VLANs                       : 50              perpetual
                      Inside Hosts                        : Unlimited       perpetual
```

```
Failover                         : Active/Active  perpetual
Encryption-DES                   : Enabled        perpetual
Encryption-3DES-AES              : Disabled       perpetual
Security Contexts                : 2              perpetual
GTP/GPRS                         : Disabled       perpetual
AnyConnect Premium Peers         : 4              perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                  : 100            perpetual
Total VPN Peers                  : 100            perpetual
Shared License                   : Disabled       perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
Total UC Proxy Sessions          : 320            perpetual
Botnet Traffic Filter            : Disabled       perpetual
Cluster                          : Disabled       perpetual
VPN Load Balancing               : Enabled        perpetual

(Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1

Cisco Adaptive Security Appliance Software Version 99.1(3)194

****************************** Warning ******************************
This product contains cryptographic features and is
subject to United States and local country laws
.governing, import, export, transfer, and use
Delivery of Cisco cryptographic products does not
,imply third-party authority to import, export
,distribute, or use encryption. Importers, exporters
distributors and users are responsible for compliance
with U.S. and local country laws. By using this
product you agree to comply with applicable laws and
.regulations. If you are unable to comply with U.S
.and local laws, return the enclosed items immediately

A summary of U.S. laws governing Cisco cryptographic
:products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by
.sending email to export@cisco.com
****************************** Warning ******************************

... output omitted ...
...Reading from flash
!
Cryptochecksum (changed): 6129864f 6298b553 75f279ea e547792b

.INFO: Power-On Self-Test in process
......................
.INFO: Power-On Self-Test complete

...INFO: Starting HW-DRBG health test
.INFO: HW-DRBG health test passed

...INFO: Starting SW-DRBG health test
.INFO: SW-DRBG health test passed

(Cisco ASA5508-X Threat Defense v6.0.0 (build 1005
firepower login: admin
Password:      <-- Admin123
.You must accept the EULA to continue
Press
```

```
                                         EULA is displayed - output is omitted ...
                                                    END USER LICENSE AGREEMENT
                                    :Please enter 'YES' or press to AGREE to the EULA

                                           .System initialization in progress.  Please stand by
                                          .You must change the password for 'admin' to continue
                                                                          :Enter new password
                                                                        :Confirm new password
                                                 .You must configure the network to continue
                                                 .You must configure at least one of IPv4 or IPv6
            :[Do you want to configure IPv4? (y/n) [y]: Do you want to configure IPv6? (y/n) [n
                                           :[Configure IPv4 via DHCP or manually? (dhcp/manual) [manual
       Enter an IPv4 address for the management interface [192.168.45.45]: 10.62.148.29
       Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.128
              Enter the IPv4 default gateway for the management interface []: 10.62.148.1
                   Enter a fully qualified hostname for this system [firepower]: FTD5508
   Enter a comma-separated list of DNS servers or 'none' []: 173.38.200.100,144.254.71.184
                         :[] 'Enter a comma-separated list of search domains or 'none
                    .If your networking information has changed, you will need to reconnect
                         'For HTTP Proxy configuration, run 'configure network http-proxy

                                   :[Configure firewall mode? (routed/transparent) [routed
                                              ... Configuring firewall mode


                                             Update policy deployment information
                                                    add device configuration -

               You can register the sensor to a Firepower Management Center and use the
         Firepower Management Center to manage it. Note that registering the sensor
            to a Firepower Management Center disables on-sensor Firepower Services
                                                     .management capabilities

                When registering the sensor to a Firepower Management Center, a unique
         alphanumeric registration key is always required.  In most cases, to register
         a sensor to a Firepower Management Center, you must provide the hostname or
                              .the IP address along with the registration key
                    '[ configure manager add [hostname | ip address ] [registration key'

            However, if the sensor and the Firepower Management Center are separated by a
         NAT device, you must enter a unique NAT ID, along with the unique registration
                                                                               .key
                          '[ configure manager add DONTRESOLVE [registration key ] [ NAT ID'

            Later, using the web interface on the Firepower Management Center, you must
         use the same registration key and, if necessary, the same NAT ID when you add
                                     .this sensor to the Firepower Management Center
                                                                                <
```

تلميح: يمكنك إستخدام خيار **عدم التأكيد** لتثبيت الصورة. وفي هذه الحالة، لا يطلب منك أثناء التثبيت.


```
firepower-boot>system install noconfirm ftp://10.229.22.42/ftd-6.0.0-1005.pkg
```


في FTD 6.1.x وأعلى، يتم مطالبتك بوضع الإدارة (محلي مقابل بعيد).


```
                         'For HTTP Proxy configuration, run 'configure network http-proxy
```

```
                                   Manage the device locally? (yes/no) [yes]: no
                             :[Configure firewall mode? (routed/transparent) [routed
```

الوضع المحلي = قابل للتطبيق فقط على أجهزة ASA55xx-X. إنك تدير FTD من FirePOWER Device
Manager (FDM).

الوضع البعيد = إدارة FTD من FMC

التحقق

```
                                                        show version <
             --------------------[ FTD5508 ]------------------
(Model     : Cisco ASA5508-X Threat Defense (75) Version 6.0.0 (Build 1005
UUID                  : 8c3f4b7e-ea11-11e5-94f1-f3a55afb51a3
                    Rules update version    : 2015-10-01-001-vrt
                        VDB version              : 252
             ----------------------------------------------------

                                                                <
```

تثبيت صورة النظام على ASA5512/15/25/45/55 هو نفسه المذكور أعلاه.

المهمة 5. تسجيل FTD في FMC

تسجيل FTD إلى خادم FMC باستخدام الإعدادات التالية:

مضيف	10.62.148.29
اسم العرض	FTD5508
مفتاح التسجيل	cisco
بلا مجموعة	
سياسة التحكم في الوصول	FTD5508
سياسة قاعدة سياسة التحكم بالوصول	None
الإجراء الافتراضي لسياسة التحكم بالوصول	حظر كل حركة المرور

الحل

الخطوة 1.في FTD حدد خادم FMC:

```
                              configure manager add 10.62.148.73 cisco <
                                             .Manager successfully configured
            .Please make note of reg_key as this will be required while adding Device in FMC

                                                          show managers <
                        Host                    : 10.62.148.73
                          **** :        Registration Key
                    Registration              : pending
                                   :          RPC Status
                    Type                      : Manager
                        Host                    : 10.62.148.73
                    Registration              : Pending
```

الخطوة 2.قبل إضافة FTD، يلزمك تسجيل FMC باستخدام خادم الترخيص الذكي. إذا حاولت إضافة جهاز FTD بدون وجود ترخيص ذكي، ستحصل على الخطأ التالي:
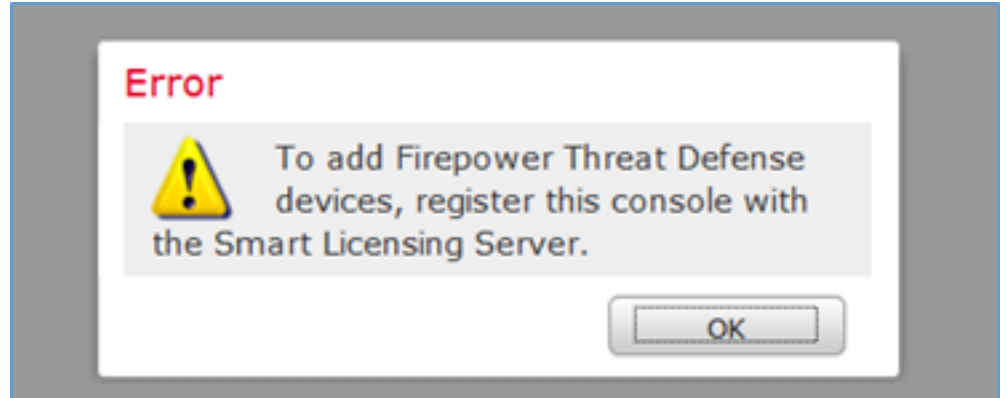
يمكنك إختيار وضع التقييم. وهذا يتيح لك إستخدام بروتوكول FTD لمدة 90 يوما دون وجود ميزات تتطلب تشفيرا قويا (على سبيل المثال، VPN).

الخطوة 3. في FMC، قم أولا بإنشاء نهج التحكم في الوصول الذي سيتم إستخدامه من قبل FTD. انتقل إلى
السياسات > التحكم في الوصول وحدد سياسة جديدة:

ثم أضف جهاز FTD:
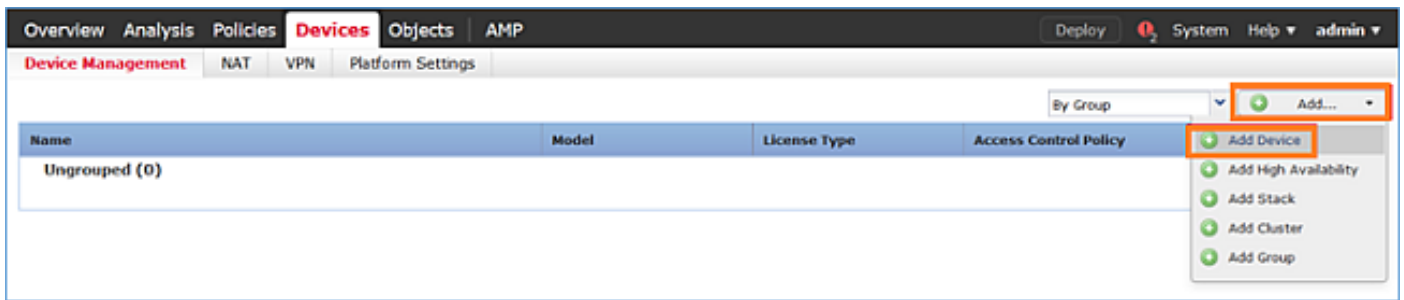
في نهاية إضافة FTD يتم نشر سياسة:
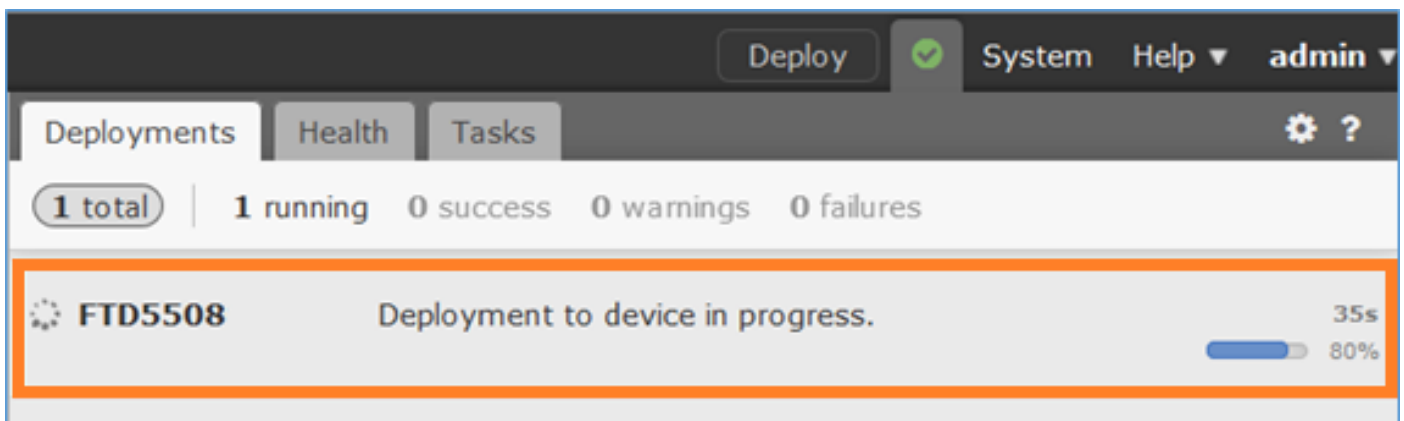
للتحقق من ما يحدث في الخلفية أثناء إضافة جهاز FTD، قم بتمكين **Pigtail** على كل من FMC و FTD.

في FMC:

```
admin@fs4k:~$ sudo pigtail
```

```
********************************************************************
  ***************************
  Displaying logs: ACTQ HTTP DCSM VMSS MOJO NGFW NGUI VMSB TCAT DEPL MSGS USMS **
********************************************************************
  ***************************
```

في FTD:

```
pigtail <
```

```
********************************************************************
  Displaying logs: HTTP ACTQ DCSM VMSS MOJO NGUI NGFW TCAT VMSB DEPL USMS MSGS **
********************************************************************
```

ملاحظة: إذا كانت حالة واجهة إدارة FTD معطلة، فتأكد من أن قيمة confreg هي 0x1.

المهمة 6. ترقية FTD

في هذه المهمة قم بترقية FTD من 6. 0.0 إلى 6. 0.1.

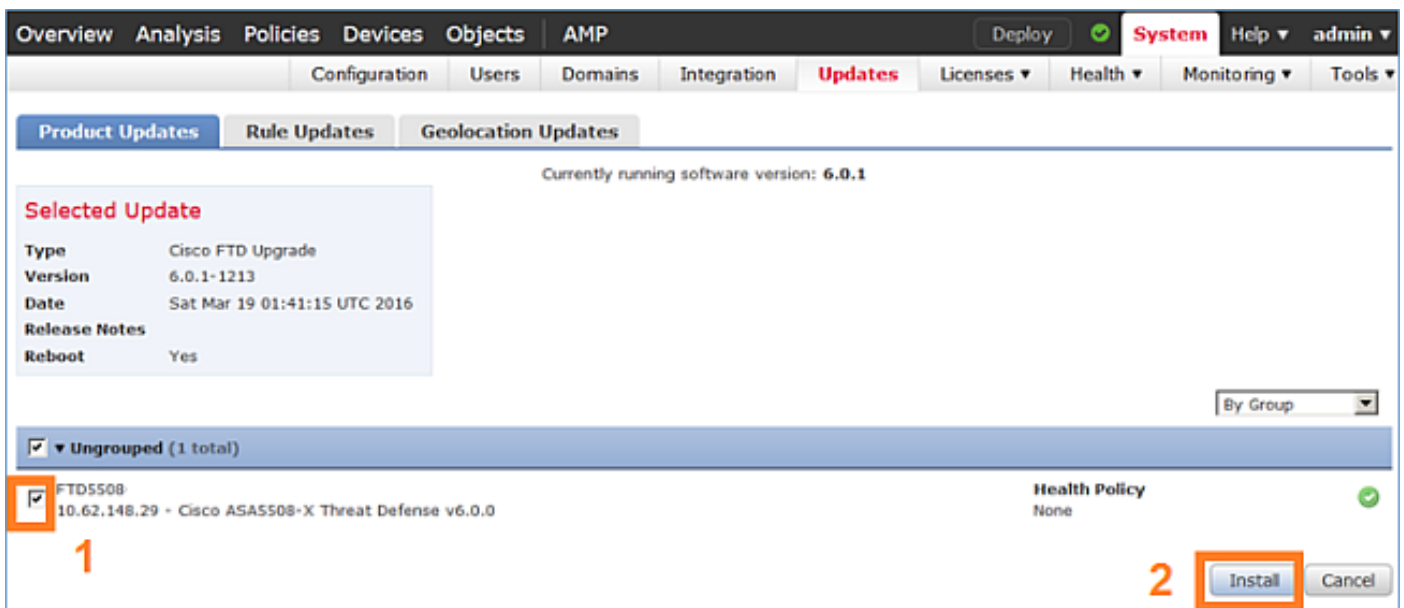|	الإصدار	اسم الملف
صورة FTD أولية	الإصدار 6.0.0 (Build 1005)	FTD-6.0.0-1005.pkg
صورة FTD الهدف	الإصدار 6.0.1 (Build 1213)	Cisco_FTD_UPGRADE-6.0.1-1213.sh

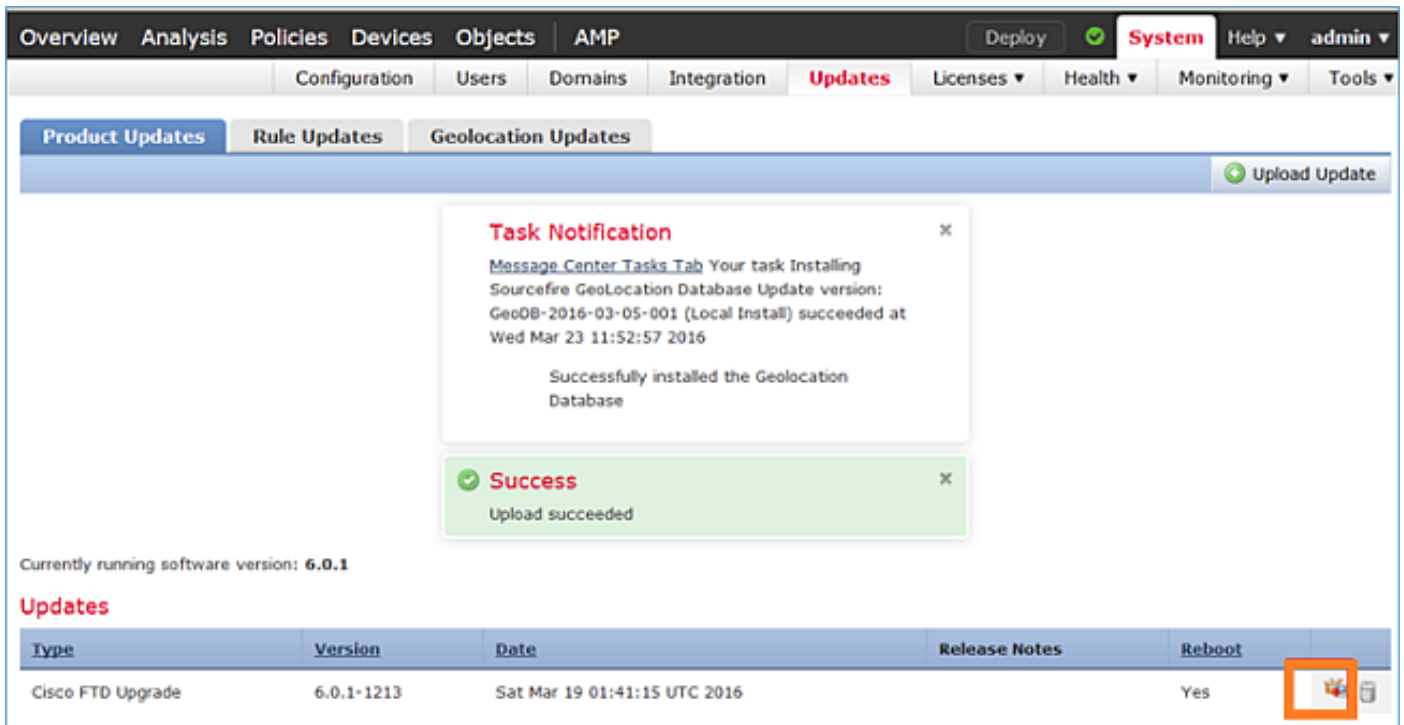## الحل

الخطوة 1. تحميل صورة FTD إلى FMC:
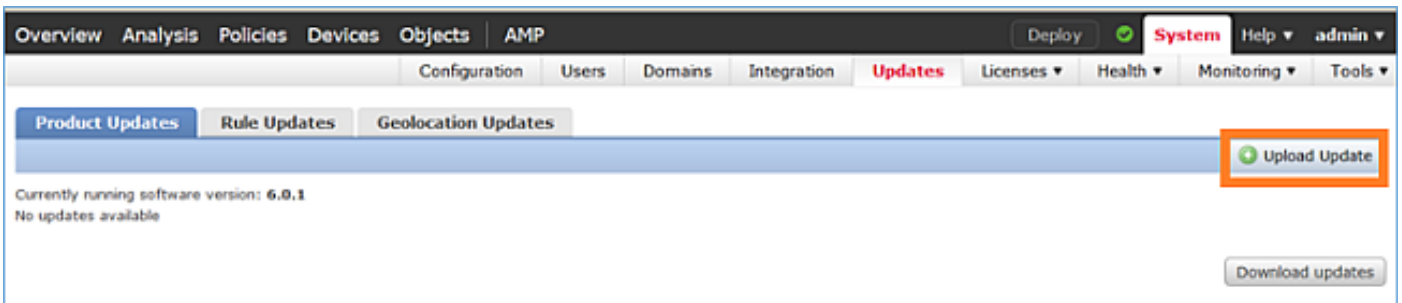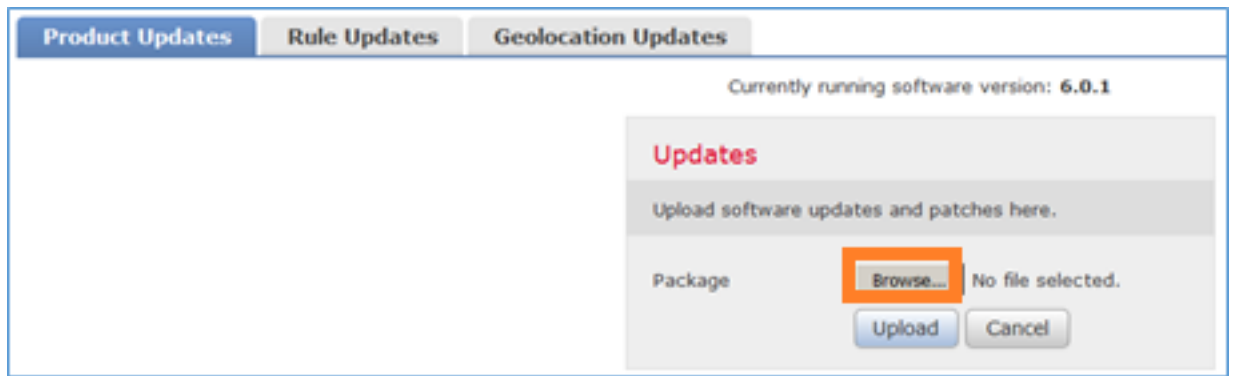
الخطوة 2. تثبيت صورة FTD:

يتم عرض تحذير حول إعادة تحميل FTD:
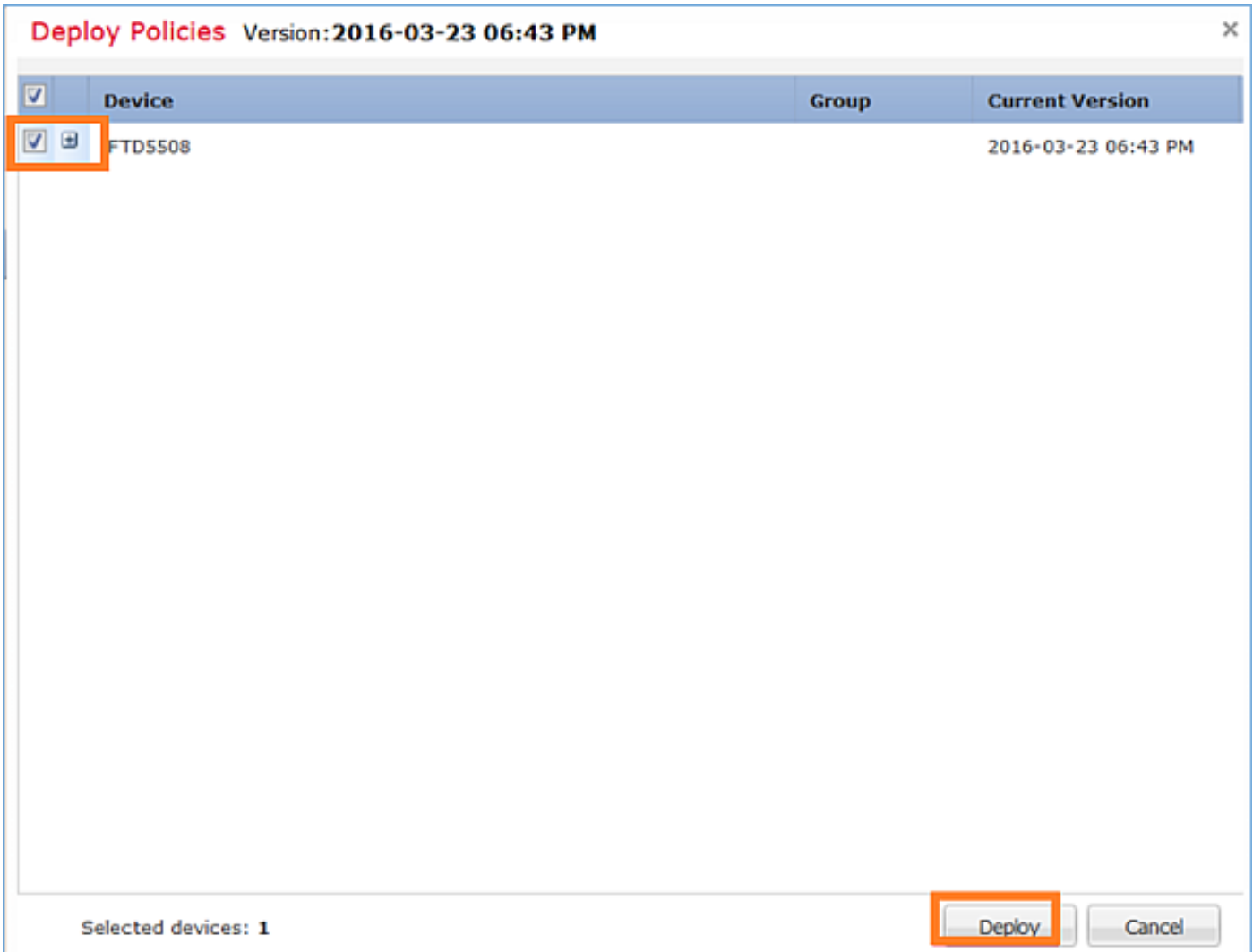
Update installation will reboot the system(s). Are you sure you want to continue?

التحقق

OK   Cancel
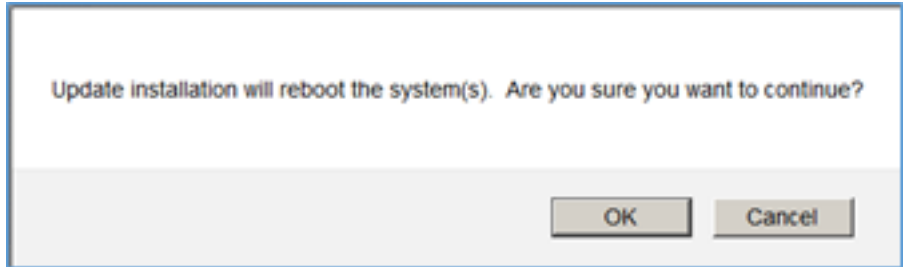
استغرقت الترقية في هذه الحالة حوالي 35 دقيقة. وكما هو موضح أدناه، هناك حاجة إلى إعادة تطبيق السياسة:
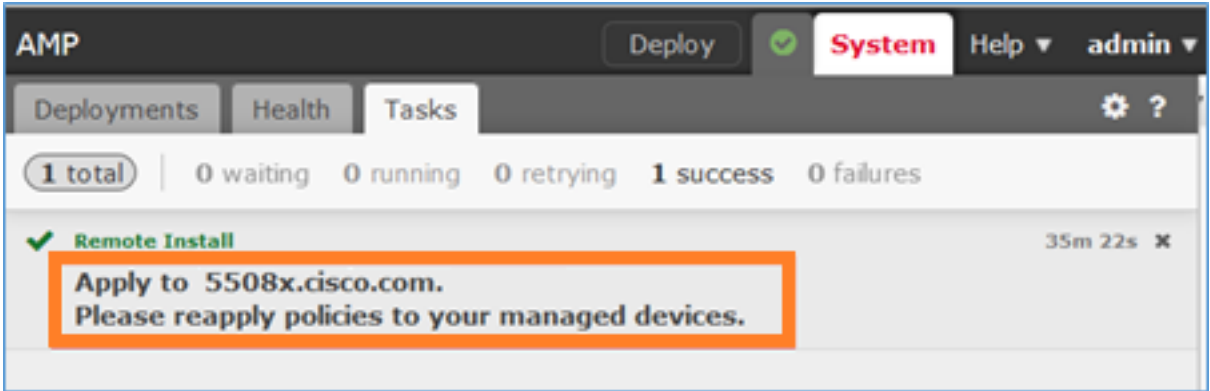
نشر النهج:

التحقق

بعد ترقية FTD:

```
> show version
-------------------[ FTD5508 ]-------------------
Model                : Cisco ASA5508-X Threat Defense (75) Version 6.0.1 (Build 1213)
UUID                 : 53b44806-f0f4-11e5-88cc-c72c24d24877
Rules update version : 2016-03-04-001-vrt
VDB version          : 259
-------------------------------------------------

>
```

المهمة 7. الاتصال والفصل من وضع واجهة سطر الأوامر (CLI) لمحرك LINA

أدخل إلى وضع واجهة سطر الأوامر (CLI) لـ LINA، ثم افصل عنه.

الحل

من وضع FTD، اكتب الأمر التالي:

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>
firepower> enable
Password:  <-- by default empty (null)
firepower#
```

كما ورد ذكره في الرسالة أعلاه، لقطع الاتصال (الانفصال) عن نوع وحدة تحكم a + CTRL في برنامج FTD Lina ثم الضغط على D:

```
firepower#  'Ctrl+a then d' Console connection detached.
admin@FTD5508:~$
```

المهمة 8. إعادة تكوين تثبيت FTD موجود

المتطلبات

إعادة تكوين صورة FTD الموجودة وتثبيت الإصدار 330-6.1.0

الحل

تفترض هذه المهمة وجود جهاز FTD يشغل الرمز x.6.0.1 ولأية أسباب كانت هناك حاجة لإعادة تصوره (على سبيل المثال، تلف قاعدة البيانات غير القابل للاسترداد، عيب فادح لا يسمح بترقية البرامج وما إلى ذلك).

ملخص الخطوات

1. التحقق من التوافق.
2. إلغاء تسجيل FTD من FMC.
3. قم بإعادة تحميل جهاز FTD وأدخل واجهة سطر الأوامر (BootCLI).
4. قم بتشغيل معالج الإعداد.
5. قم بتثبيت صورة نظام FTD.
6. تسجيل FTD في FMC.

الخطوات التفصيلية

الخطوة 1. تحقق من ملاحظات إصدار FirePOWER وتأكد من أن صورة FTD التي تريد إستخدامها متوافقة مع FMC. إذا لم تقم بترقية FMC أولا.

الخطوة 2. إلغاء تسجيل (حذف) FTD من FMC. هذه الخطوة مطلوبة بعد أن يقوم FTD بإعادة تكوين UUID الخاص به ولا يمكن تسجيله مرة أخرى، ولكن يجب إضافته من البداية.

الخطوة 3. قم بإعادة تحميل جهاز FTD وأدخل واجهة سطر الأوامر (BootCLI). نظرا لوجود صورة FTD موجودة بالفعل، يمكن تخطي تثبيت صورة بدء تشغيل FTD:

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': YES

Broadcast messagStopping Cisco ASA5506-X Threat Defense......ok
Shutting down sfifd...                                              [  OK  ]
Clearing static routes
Unconfiguring default route                                        [  OK  ]
Unconfiguring address on br1                                       [  OK  ]
Unconfiguring IPv6                                                 [  OK  ]
Downing interface                                                  [  OK  ]
Stopping nscd...                                                   [  OK  ]
Stopping system log daemon...                                      [  OK  ]
Stopping Threat Defense ...
cp: cannot stat '/etc/ssh': No such file or directory
Stopping system message bus: dbus.
rmdir: failed to remove directory '/etc': Directory not empty      [  OK  ]
Un-mounting disk partitions ...
…
Device root is still in use.
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted filesystem or
```

```
                                                            ?active volume group
              (Stopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd (pid 4209
                                                                                         .
    (Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 4213
                                                                              acpid: exiting

                                                                                    .acpid
                                                    .Stopping system message bus: dbus
                    Deconfiguring network interfaces... ifdown: interface br1 not configured
                                                                                      .done
                                              ...Sending all processes the TERM signal
                                              ...Sending all processes the KILL signal
                                                                    ...Deactivating swap
                                                     ...Unmounting local filesystems
                                                                     Rebooting... ÿ
                                                   Rom image verified correctly


                               Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
                                       .Copyright (c) 1994-2015  by Cisco Systems, Inc
                                       Compiled Thu 06/18/2015 12:15:56.43 by builders


                                                   Current image running: Boot ROM0
                                                 Last reset cause: PowerCycleRequest
                                                           DIMM Slot 0 : Present

                                       Platform ASA5506 with 4096 Mbytes of main memory
                                                    MAC Address: 84:3d:c6:1a:cf:39


                                                 .Use BREAK or ESC to interrupt boot
                                                 .Use SPACE to begin boot immediately


                                              .Located '.boot_string' @ cluster 260275

                                                                                       #
                                               ":Attempt autoboot: "boot disk0
                                              .Located 'os.img' @ cluster 235457

################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
                              ##########################
                                              .LFBFF signature verified
                                              INIT: version 2.88 booting
                                                          Starting udev
                                     .Configuring network interfaces... done
                                                   Populating dev cache
                                                  .Detected PID ASA5506
                                     .Found device serial number JAD2034008E
                                            Found USB flash drive /dev/sdb
                                            Found hard drive(s):  /dev/sda
                                               fsck from util-linux 2.23.2
                                         dosfsck 2.11, 12 Mar 2005, FAT32, LFN
                                       dev/sdb1: 42 files, 24805/1798467 clusters/
```

```
==============================================
Use ESC to interrupt boot and launch boot CLI.
Use SPACE to launch Cisco FTD immediately.
Cisco FTD launch in 23 seconds ...          Press ESC to enter BootCLI >
Launching boot CLI ...
Configuring network interface using DHCP
Bringing up network interface.
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv6 address: fe80::863d:c6ff:fe1a:cf38
IPv4 address not assigned. Run 'setup' before installation.
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
generating ssh RSA key...
generating ssh ECDSA key...
generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up

acpid: 1 rule loaded

acpid: waiting for events: event logging is off

Starting ntpd: done
Starting syslog-ng:[2017-01-14T11:20:33.699619] Connection failed; fd='15',
server='AF_INET(127.128.254.1:514)', local='AF_INET(0.0.0.0:0)', error='Network is unreachable
(101))'
[2017-01-14T11:20:33.699704] Initiating connection failed, reconnecting; time_reopen='60'
.
Starting crond: OK




Cisco FTD Boot 6.0.0 (9.6.2.)
Type ? for list of commands
firepower-boot>
```

الخطوة 4. قم بتشغيل معالج الإعداد وتعيين معلمات الشبكة الأساسية:


```
firepower-boot>setup

Welcome to Cisco FTD Setup
[hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [firepower]: FTD5506
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]: n
Enter an IPv4 address: 10.48.66.83
Enter the netmask: 255.255.255.128
Enter the gateway: 10.48.66.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 192.168.0.1
Do you want to configure Secondary DNS Server? (y/n) [n]: n
```

```
                           Do you want to configure Local Domain Name? (y/n) [n]: n
                          Do you want to configure Search domains? (y/n) [n]:  n
                            Do you want to enable the NTP service? [Y]: n
                                      :Please review the final configuration
                                Hostname:            FTD5506
                             Management Interface Configuration

                                     IPv4 Configuration:      static
                               IP Address:      10.48.66.83
                               Netmask:         255.255.255.128
                               Gateway:           10.48.66.1

                             IPv6 Configuration:      Stateless autoconfiguration

                                                 :DNS Configuration
                               DNS Server:       192.168.0.1

                                    NTP configuration:       Disabled

                                                           :CAUTION
            You have selected IPv6 stateless autoconfiguration, which assigns a global address
            based on network prefix and a device identifier. Although this address is unlikely
                      .to change, if it does change, the system will stop functioning correctly
                            .We suggest you use static addressing instead

                                    Apply the changes?(y,n) [Y]:      Y
                                     !Configuration saved successfully
                                                 ...Applying
                                    ...Restarting network services
                                                          .Done
                                     ...Press ENTER to continue
                                            <firepower-boot
```

<div dir="rtl">

الخطوة 5.التحقق من الاتصال بالخادم (FTP و HTTP وما إلى ذلك) الذي يحتوي على صورة نظام FTD وبدء
التثبيت:

</div>

```
                                    firepower-boot>ping 10.48.40.70
                               .PING 10.48.40.70 (10.48.40.70) 56(84) bytes of data
                           bytes from 10.48.40.70: icmp_seq=1 ttl=64 time=555 ms 64
                          bytes from 10.48.40.70: icmp_seq=2 ttl=64 time=0.465 ms 64
                          bytes from 10.48.40.70: icmp_seq=3 ttl=64 time=0.511 ms 64
                                      --- ping statistics 10.48.40.70 ---
                   packets transmitted, 3 received, 0% packet loss, time 2000ms 3
                          rtt min/avg/max/mdev = 0.465/185.466/555.424/261.599 ms

firepower-boot > system install noconfirm ftp://anonymous:cisco@10.48.40.70/ftd-6. 1.0-330.pkg

                          ############################# WARNING #######################
                          # !The content of disk0: will be erased during installation #
                          ###########################################################

                                            Do you want to continue? [y/N] y
                                                    ... Erasing disk0
                                                    Verifying
                                                    Downloading
                                                    Extracting
                                                    Package Detail
            Description:                    Cisco ASA-FTD 6.1.0-330 System Install
```

```
                                  Requires reboot:              Yes

              .Warning: Please do not interrupt the process or turn off the system
                                  .Doing so might leave system in unusable state

                                               ... Starting upgrade process
                                               Populating new system image

                                                    ... output omitted ...
                                      Firstboot detected, executing scripts
[  Executing S01reset_failopen_if                                    [  OK
[  Executing S01virtual-machine-reconfigure                          [  OK
[  Executing S02aws-pull-cfg                                         [  OK
[  Executing S02configure_onbox                                      [  OK
[  Executing S04fix-httpd.sh                                         [  OK
[  Executing S05set-mgmnt-port                                       [  OK
[  Executing S06addusers                                             [  OK
[  Executing S07uuid-init                                            [  OK
[  Executing S08configure_mysql                                      [  OK

                                          ********* Attention ************

                 Initializing the configuration database.  Depending on available
              system resources (CPU, memory, and disk), this may take 30 minutes
                                               .or more to complete

                                          ********* Attention ************

[  Executing S09database-init                                        [  OK
[  Executing S11database-populate                                    [  OK
[  Executing S12install_infodb                                       [  OK
[  Executing S15set-locale.sh                                        [  OK
[  Executing S16update-sensor.pl                                     [  OK
[  Executing S19cert-tun-init                                        [  OK
[  Executing S20cert-init                                            [  OK
[  Executing S21disable_estreamer                                    [  OK
[  Executing S25create_default_des.pl                                [  OK
[  Executing S30init_lights_out_mgmt.pl                              [  OK
[  Executing S40install_default_filters.pl                           [  OK
[  Executing S42install_default_dashboards.pl                        [  OK
[  Executing S43install_default_report_templates.pl                  [  OK
[  Executing S44install_default_app_filters.pl                       [  OK
[  Executing S45install_default_realms.pl                            [  OK
[  Executing S47install_default_sandbox_EO.pl                        [  OK
[  Executing S50install-remediation-modules                          [  OK
[  Executing S51install_health_policy.pl                             [  OK
[  Executing S52install_system_policy.pl                             [  OK
[  Executing S53change_reconciliation_baseline.pl                    [  OK
[  Executing S70remove_casuser.pl                                    [  OK
[  Executing S70update_sensor_objects.sh                             [  OK
[  Executing S85patch_history-init                                   [  OK
[  Executing S90banner-init                                          [  OK
[  Executing S95copy-crontab                                         [  OK
[  Executing S96grow_var.sh                                          [  OK
[  Executing S96install_vmware_tools.pl                              [  OK

                                          ********** Attention **********

                 Initializing the system's localization settings.  Depending on available
                  system resources (CPU, memory, and disk), this may take 10 minutes
                                               .or more to complete

                                          ********** Attention **********
[  Executing S96localize-templates                                   [  OK
```

```
[   Executing S96ovf-data.pl                                                    [   OK
[   Executing S97compress-client-resources                                      [   OK
[   Executing S97create_platinum_forms.pl                                       [   OK
[   Executing S97install_cas                                                    [   OK
[   Executing S97install_cloud_support.pl                                       [   OK
[   Executing S97install_geolocation.pl                                         [   OK
[   Executing S97install_ssl_inspection.pl                                      [   OK
[   Executing S97update_modprobe.pl                                             [   OK
[   Executing S98check-db-integrity.sh                                          [   OK
[   Executing S98htaccess-init                                                  [   OK
[   Executing S98is-sru-finished.sh                                             [   OK
[   Executing S99correct_ipmi.pl                                                [   OK
[   Executing S99start-system                                                   [   OK
[   Executing S99z_db_restore                                                   [   OK
[   Executing S99_z_cc-integrity.sh                                             [   OK
                                                          .Firstboot scripts finished
[   Configuring NTP...                                                          [   OK
        fatattr: can't open '/mnt/disk0/.private2': No such file or directory
                fatattr: can't open '/mnt/disk0/.ngfw': No such file or directory
                                    Model reconfigure detected, executing scripts
                                                                  Pinging mysql
                                                          Found mysql is running
[   Executing 45update-sensor.pl                                                [   OK
[   Executing 55recalculate_arc.pl                                              [   OK
                                                               :Starting xinetd
                                                   Sat Jan 14 12:07:35 UTC 2017
                                                             ...Starting MySQL
                                                                  Pinging mysql
                                                        Pinging mysql, try 1
                                                        Pinging mysql, try 2
                                                        Found mysql is running
                                                  ...Running initializeObjects
                                                            ...Stopping MySQL
                                                  Killing mysqld with pid 22354
                                                  Wait for mysqld to exit\c
                                                                          done
                                                   Sat Jan 14 12:07:57 UTC 2017
[   Starting sfifd...                                                           [   OK
         !Starting Cisco ASA5506-X Threat Defense, please wait...No PM running
                                                                  .started...
```
... output omitted ...
```
                                                         firepower login: admin
                                                         Password:    < Admin123
                                            .You must accept the EULA to continue
                                             :Press <ENTER> to display the EULA
                                                     END USER LICENSE AGREEMENT

                                                                              …

                         :Please enter 'YES' or press <ENTER> to AGREE to the EULA

                                  .System initialization in progress.  Please stand by
                                  .You must change the password for 'admin' to continue
                                                             :Enter new password
                                                           :Confirm new password
                                         .You must configure the network to continue
                                         .You must configure at least one of IPv4 or IPv6
                                         :[Do you want to configure IPv4? (y/n) [y
                                         :[Do you want to configure IPv6? (y/n) [n
                                 :[Configure IPv4 via DHCP or manually? (dhcp/manual) [manual
        Enter an IPv4 address for the management interface [192.168.45.45]: 10.48.66.83
   Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.128
Enter the IPv4 default gateway for the management interface [192.168.45.1]: 10.48.66.1
           Enter a fully qualified hostname for this system [firepower]: FTD5506
```

```
                  Enter a comma-separated list of DNS servers or 'none' []: 192.168.0.1
                                 :[] 'Enter a comma-separated list of search domains or 'none
                  .If your networking information has changed, you will need to reconnect
                            'For HTTP Proxy configuration, run 'configure network http-proxy

                                        Manage the device locally? (yes/no) [yes]: no
                        :[Configure firewall mode? (routed/transparent) [routed
                                             ... Configuring firewall mode

                                        Update policy deployment information
                                            add device configuration -
                                              add network discovery -
                                                 add system policy -

               You can register the sensor to a Firepower Management Center and use the
            Firepower Management Center to manage it. Note that registering the sensor
              to a Firepower Management Center disables on-sensor Firepower Services
                                             .management capabilities

                   When registering the sensor to a Firepower Management Center, a unique
                 alphanumeric registration key is always required.  In most cases, to register
                a sensor to a Firepower Management Center, you must provide the hostname or
                                       .the IP address along with the registration key
                      '[ configure manager add [hostname | ip address ] [registration key'

              However, if the sensor and the Firepower Management Center are separated by a
             NAT device, you must enter a unique NAT ID, along with the unique registration
                                                                                       .key
                          '[ configure manager add DONTRESOLVE [registration key ] [ NAT ID'

                Later, using the web interface on the Firepower Management Center, you must
                use the same registration key and, if necessary, the same NAT ID when you add
                                        .this sensor to the Firepower Management Center
```

الخطوة 6. تسجيل FTD في FMC

```
                                     configure manager add 10.62.148.50 cisco <
                                                     .Manager successfully configured
                 .Please make note of reg_key as this will be required while adding Device in FMC

                                                                    show managers <
                    Host                                  : 10.62.148.50
                               **** :            Registration Key
                         Registration                      : pending
                                    :                       RPC Status
```

على FMC، انتقل إلى **الأجهزة > إدارة الأجهزة** لإضافة جهاز FTD.

بعد إضافة برنامج الإرسال فائق السرعة (FTD) إلى وحدة التحكم في إدارة الهيكل (FMC)، يلزمك ما يلي:

• أعد تكوين إعدادات الجهاز مثل الواجهات والتوجيه
• قم بإعادة تكوين السياسات مثل VPN و QoS

• أعد تطبيق السياسات والإعدادات المطبقة سابقا مثل إعدادات سياسة التحكم بالوصول، NAT، والنظام الأساسي

معلومات ذات صلة

- [أدلة المميزات](#)
- [إعادة تكوين جهاز الدفاع عن تهديد Cisco ASA أو FirePOWER](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم. تخلي Cisco Systems مسؤوليتها عن دقة هذه الترجمات وتوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).