Instalación y actualización de Firepower Threat Defense en dispositivos ASA 55xx-X

Contenido

Introducción

Este documento describe los procedimientos de instalación, actualización y registro de Firepower Threat Defense (FTD) en dispositivos ASA55xx-X.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA5508-X
- ASA5512-X
- FireSIGHT Management Center (FMC), ejecución 6.0.1 (compilación 1213)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

FTD es una imagen de software unificada que se puede instalar en estas plataformas:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Amazon Web Services (AWS)
- KVM
- Módulo de router ISR

El objetivo de este documento es demostrar:

- La instalación de la versión 6.0.0 de FTD en las plataformas ASA5508-X y ASA5512-X
- El procedimiento de actualización de FTD de la versión 6.0.0 a 6.0.1
- Registro en Firepower Management Center (FMC) y licencias básicas

Configurar

Diagrama de la red
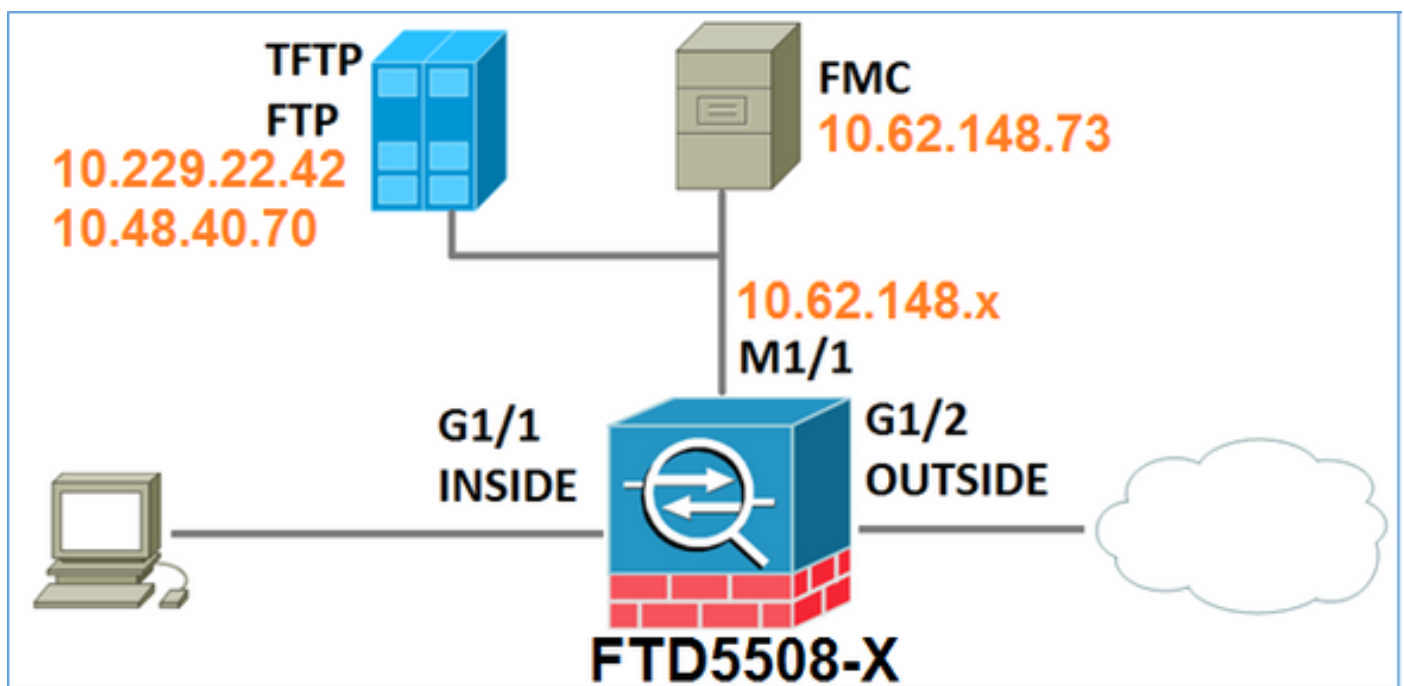
Descarga de software FTD

Vaya a **Firewalls de última generación (NGFW) > ASA con FirePOWER Services > ASA 5508-X con FirePOWER Services** y seleccione **Firepower Threat Defense Software**:

Del mismo modo para el software ASA5512-X.

Tarea 1. Verificar los requisitos previos

Verifique los requisitos previos antes de la instalación de FTD.

Solución:

Para la instalación de FTD utiliza dos imágenes:

1. Imagen de sistema operativo (también conocida como imagen de inicio): para Firepower Threat Defense en ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X y ASA5516-X es un archivo *.lfbff. Para Firepower Threat Defense en Saleen (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA555-X) es un archivo *.cdisk.
2. Imagen del sistema: es un archivo .pkg.

Antes de continuar con la instalación de FTD, verifique lo siguiente:

- La memoria flash ASA debe tener al menos 3,1 GBytes (3 GBytes + tamaño de la imagen de inicio) de espacio libre
- La imagen de inicio se carga en un servidor TFTP
- La imagen del sistema se carga en un servidor HTTP o FTP
- OnASA5506/08/16 el ROMMON es al menos 1.1.8 versión

Verifique el espacio libre:

```
FTD5508X# show flash | i free
7859437568 bytes total (4273819648 bytes free)
```
Verifique estas imágenes:

Nombre del archivo	Descripción
ftd-boot-9.6.1.0.lfbff	imagen de inicio de Firepower Threat Defense v6.0.1 para 5506/5508/5516. Esta es la imagen de inicio para la instalación limpia en 5506/5508/5516
ftd-boot-9.6.1.0.cdisk	Imagen de inicio de Firepower Threat Defense v6.0.1 para ASA 5512/5515/5525/5545/5555. Esta es la imagen de inicio para la instalación limpia en 5512/5515/5525/5545/5555
ftd-6.0.0-1005.pkg	Firepower Threat Defense v6.0.0 para todos los ASA compatibles: 5506/5508/5512/5515/5516/5525/5545/5555.

Esta es la imagen del sistema para la instalación limpia

Tarea 2. Actualización del ROMMON ASA5508-X

Como se menciona en los requisitos previos, los dispositivos ASA5506-X, ASA5508-X y ASA5516-X deben estar en ROMMON v1.1.8. Si no, instale asa5500-firmware-1108.SPA (disponible en la página de descarga de Cisco ASA).

Requisito de tarea:

Actualice ASA5508 ROMMON de 1.1.1 a 1.1.8.

Solución:

El procedimiento se describe en la [Guía de actualización de ASA ROMMON](#).

Paso 1. Verifique la versión ROMMON existente:

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

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

Paso 2.Descargue el firmware ROMMON en la memoria flash del ASA:

```
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...
!!!!!!!!!!
9241408 bytes copied in 18.890 secs (513411 bytes/sec)
```

Paso 3. Actualización de la imagen ROMMON de ASA:

```
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

2804 bytes copied in 0.260 secs
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.
...
```

Controle lo siguiente:

Puede utilizar el comando **show module** para verificar la versión del software ROMMON:

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

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

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

Tarea 3. Instale la imagen de inicio de FTD en ASA55xx-X

Requisito de tarea:

Instale la imagen de inicio FTD ftd-boot-9.6.1.0.lfbff en ASA5508-X.

Solución:

Hay más de un método para hacerlo. He aquí el primero:

Método 1. De ROMMON

Paso 1. Recargue el ASA e ingrese al modo 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 >
```

Paso 2. Configuración de los parámetros básicos de red:

```
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.lfbff
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>
```

En ASA5512/15/25/45/55 el procedimiento es el mismo con la única diferencia en el nombre de la imagen de inicio:

```
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
```

Método 2. Desde el modo ASA

Paso 1. Desde el modo de ejecución ASA (sin ROMMON) copie la imagen de inicio FTD en la

memoria flash ASA:

```
ciscoasa# copy ftp://10.48.40.70/ANG/mzafeiro/ftd-boot-9.6.1.0.lfbff flash
```
Paso 2. Elimine cualquier imagen ASA del disco:

```
ciscoasa# delete flash:asa*
```
El contenido de la memoria flash después de eliminar imágenes ASA:

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

Tarea 4. Instale la imagen del sistema FTD en ASA55xx-X

Instale la imagen del sistema FTD en ASA5508-X.

Solución

```
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>
```

Verifique la conectividad con el servidor FTP:

```
firepower-boot> ping 10.229.22.42
PING 10.229.22.42 (10.229.22.42) 56(84) bytes of data.
64 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
^C
--- 10.229.22.42 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.302/1.360/1.458/0.075 ms
```

Instale el paquete del sistema:

```
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.
>
```

> **Consejo:** Puede utilizar la opción **noconfirm** para instalar la imagen. En ese caso, no se le solicitará durante la instalación.

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

En FTD 6.1.x y superiores, se le solicita el modo de administración (local frente a remoto).

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

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

Modo local = Aplicable sólo en dispositivos ASA55xx-X. Gestiona el FTD desde Firepower Device Manager (FDM).

Modo remoto = Gestiona el FTD desde FMC

Verificación

```
> 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
--------------------------------------------------

>
```

La instalación de la imagen del sistema en ASA5512/15/25/45/55 es la misma que la anterior.

Tarea 5. Registre el FTD en FMC

Registrar FTD en el servidor FMC utilizando la siguiente configuración:

Host	10.62.148.29
Mostrar nombre:	FTD5508
Clave de registro	Cisco
Grupo Ninguno	
Política de control de acceso	FTD5508
Política de base de políticas de control de acceso	Ninguno
Acción predeterminada de la política de control de acceso	Bloquear todo el tráfico

Solución

Paso 1.En FTD, especifique el servidor 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

>
```
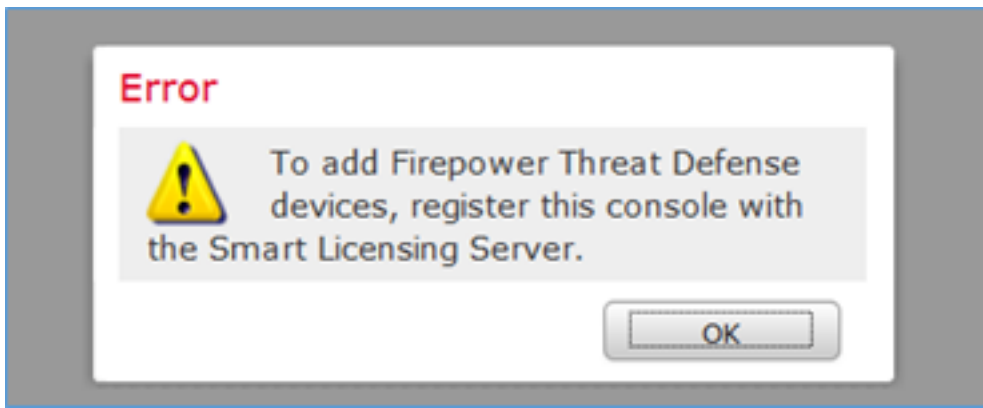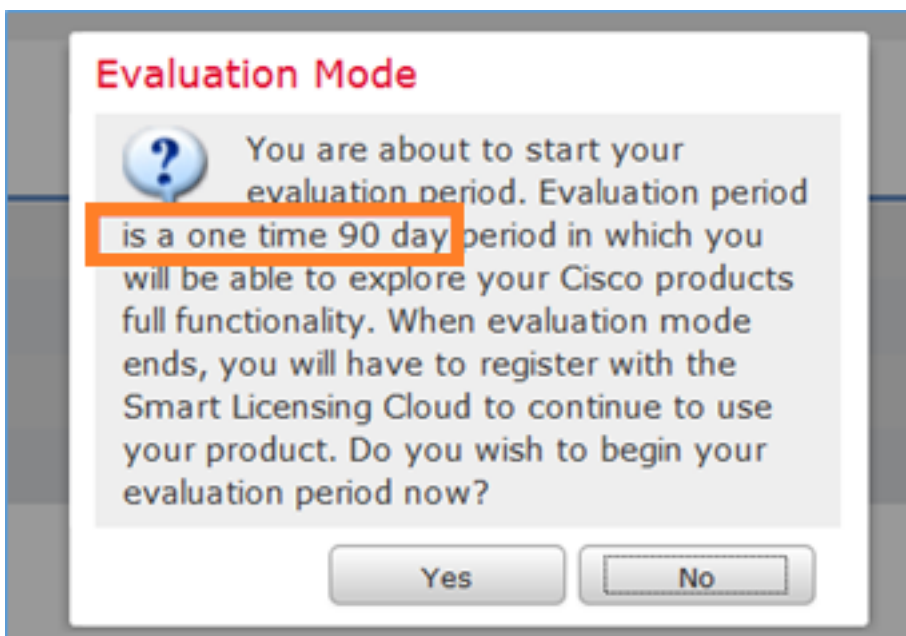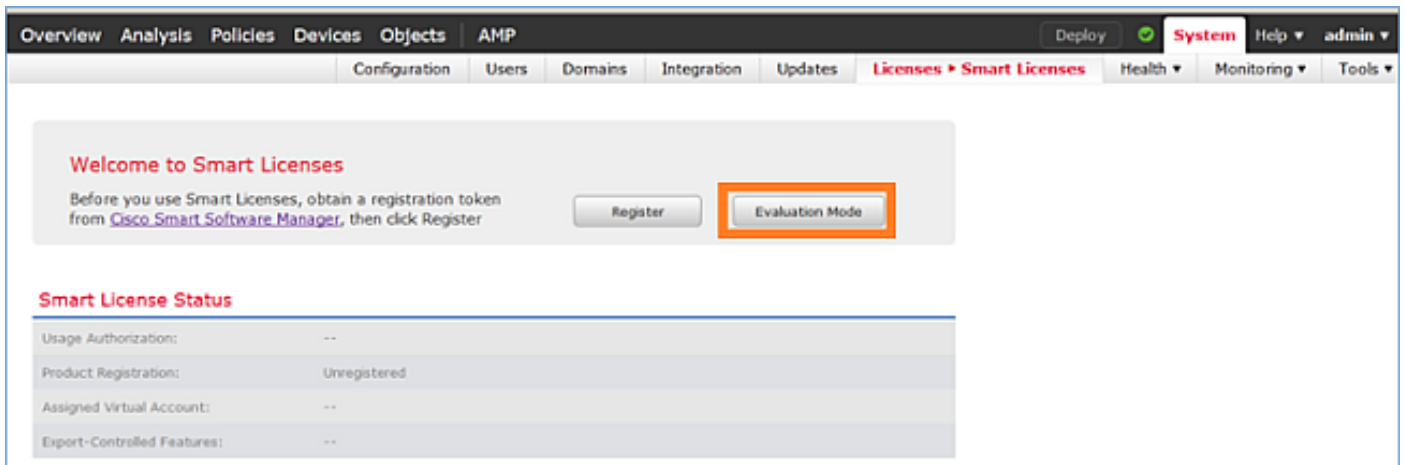
Paso 2.Antes de agregar el FTD, debe registrar el FMC con Smart Licensing Server. Si intenta agregar un dispositivo FTD sin tener una licencia inteligente, se producirá el siguiente error:

Error

To add Firepower Threat Defense devices, register this console with the Smart Licensing Server.

OK

Puede elegir el modo de evaluación. Esto le permite utilizar FTD durante 90 días sin funciones que requieran un cifrado seguro (por ejemplo, VPN).

Overview   Analysis   Policies   Devices   Objects   AMP   Deploy   ⊘   **System**   Help ▾   admin ▾

Configuration   Users   Domains   Integration   Updates   **Licenses ▸ Smart Licenses**   Health ▾   Monitoring ▾   Tools ▾

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Register   Evaluation Mode

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--

Evaluation Mode

You are about to start your evaluation period. Evaluation period is a one time 90 day period in which you will be able to explore your Cisco products full functionality. When evaluation mode ends, you will have to register with the Smart Licensing Cloud to continue to use your product. Do you wish to begin your evaluation period now?

Yes   No

Paso 3. En FMC, cree primero la política de control de acceso que utilizará FTD. Navegue hasta **Políticas > Control de acceso** y seleccione **Nueva política**:

A continuación, agregue el dispositivo FTD:
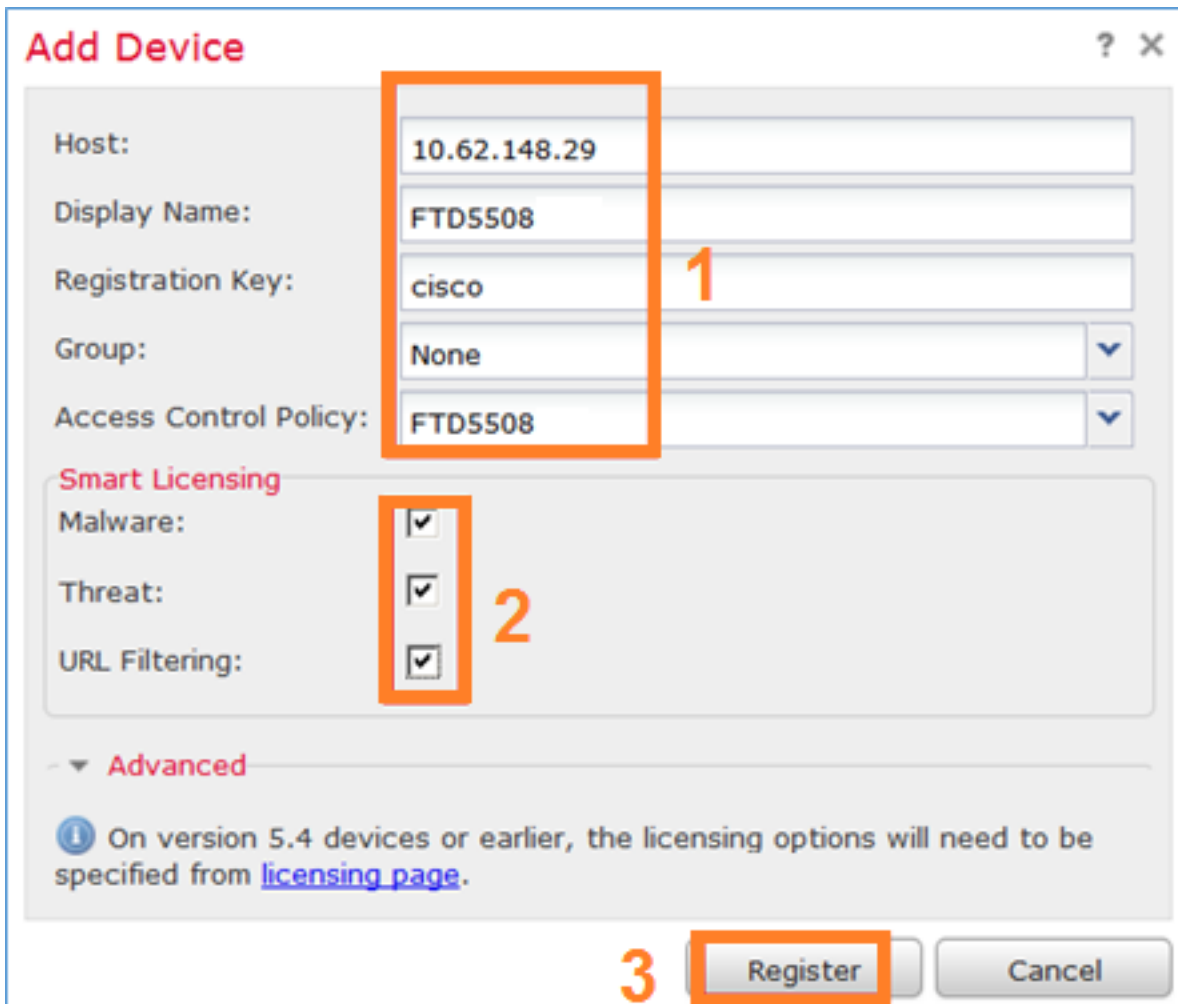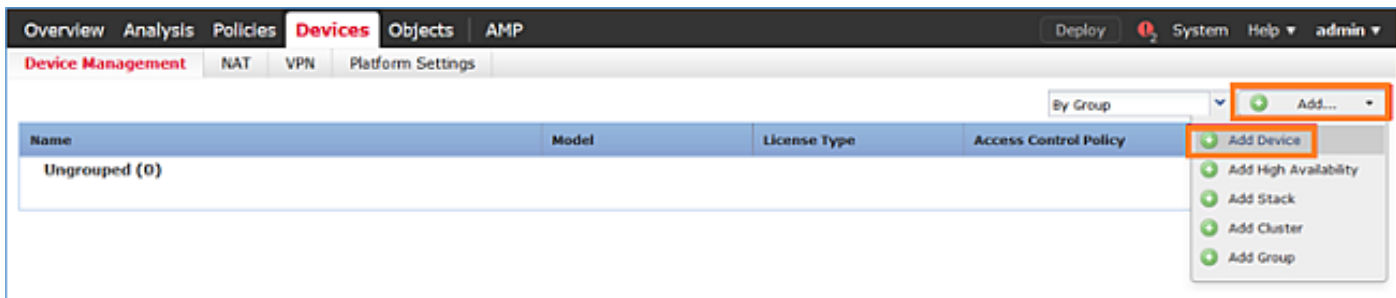
Al final de la adición de FTD se implementa una política:
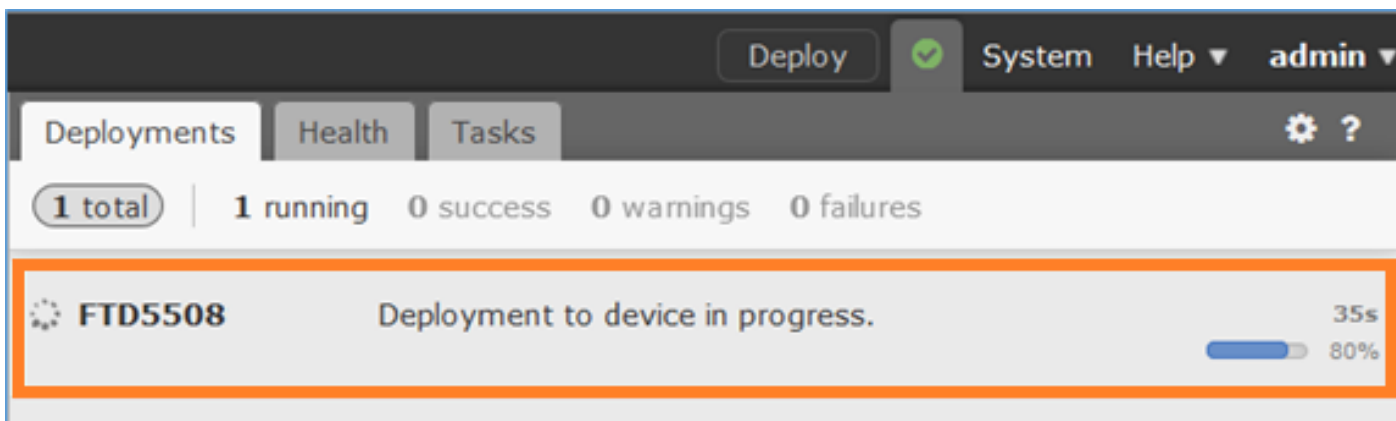
Para comprobar lo que está sucediendo en segundo plano mientras se agrega el dispositivo FTD, active **pigtail** tanto en FMC como en FTD.

En FMC:

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

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

En FTD:

```
> pigtail
```

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

Nota: Si el estado de la Interfaz de administración de FTD está inactivo, asegúrese de que el valor de la conferencia sea 0x1.

Tarea 6. Actualización del FTD

En esta tarea, actualice FTD de 6.0.0 a 6.0.1.

	Versión	Nombre del archivo
Imagen inicial de FTD	Versión 6.0.0 (Compilación 1005)	ftd-6.0.0-1005.pkg
Imagen FTD objetivo	Versión 6.0.1 (Compilación 1213)	Cisco_FTD_Upgrade-6.0.1-1213.sh

Solución

Paso 1. Cargue la imagen FTD en FMC:
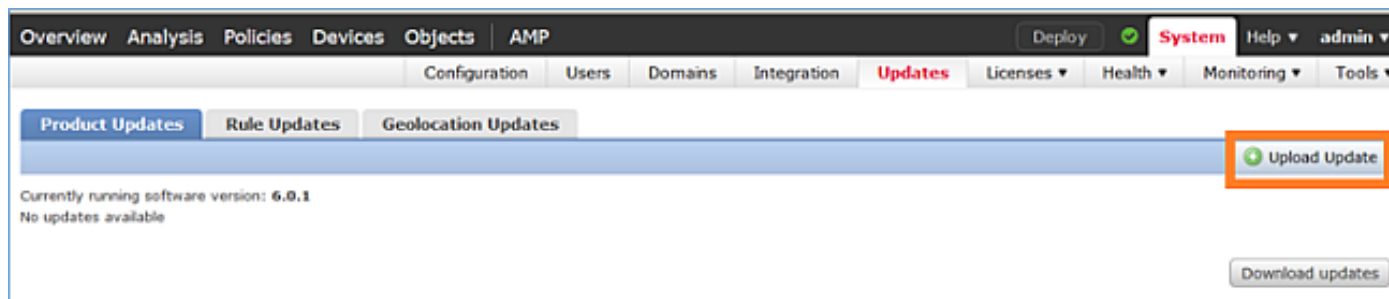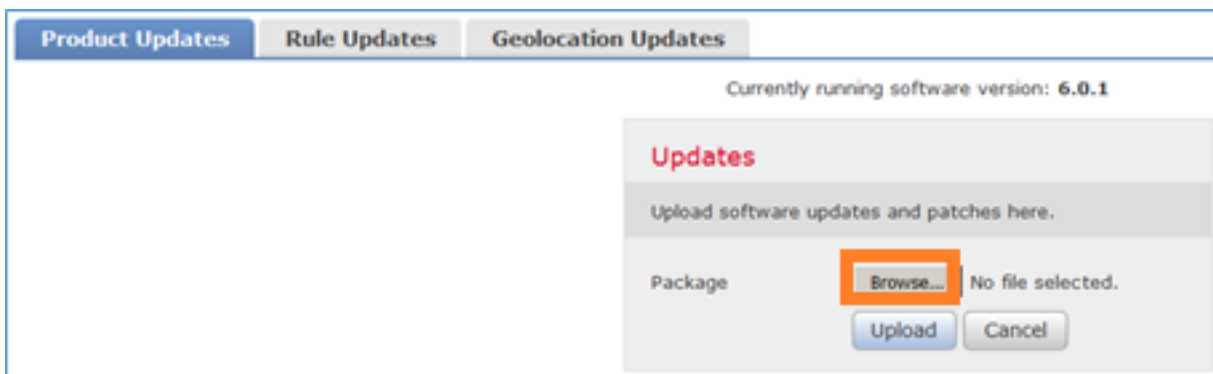
Paso 2. Instale la imagen FTD:
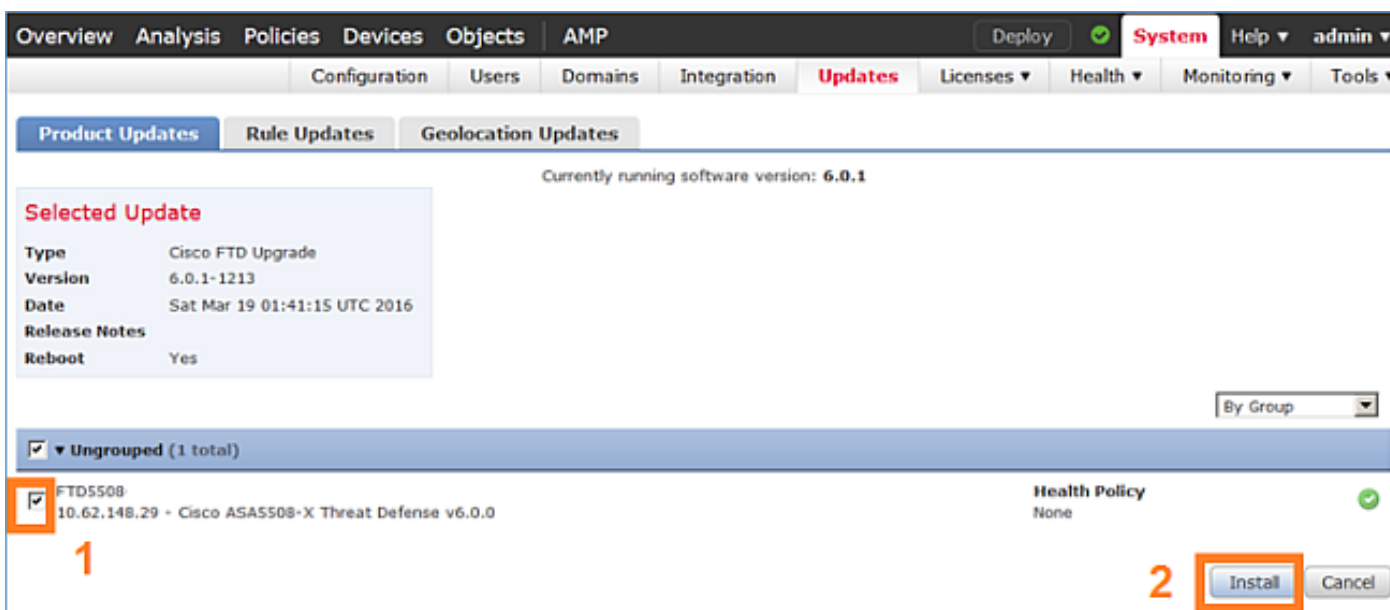
Se muestra una advertencia sobre la recarga de FTD:

Update installation will reboot the system(s). Are you sure you want to continue?

OK   Cancel
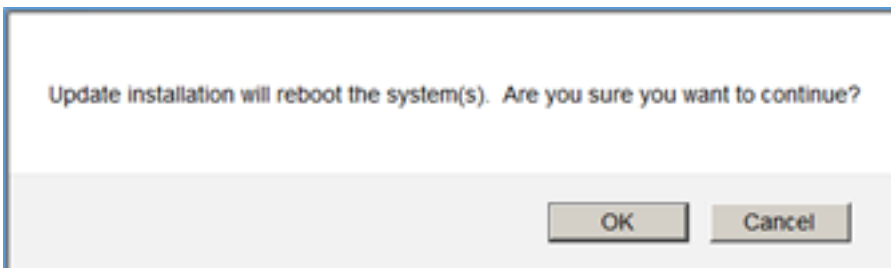
La actualización en este caso llevó unos 35 minutos. Como se muestra a continuación, es necesario volver a aplicar la política:
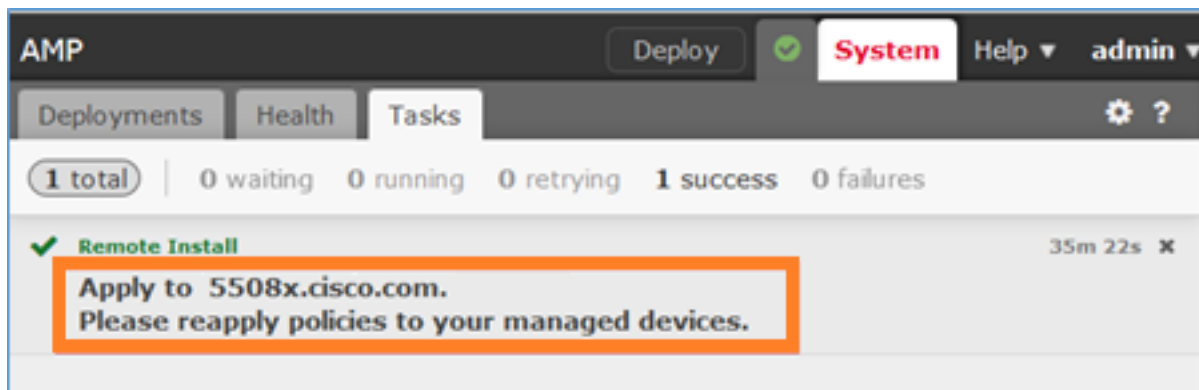
Implemente las políticas:
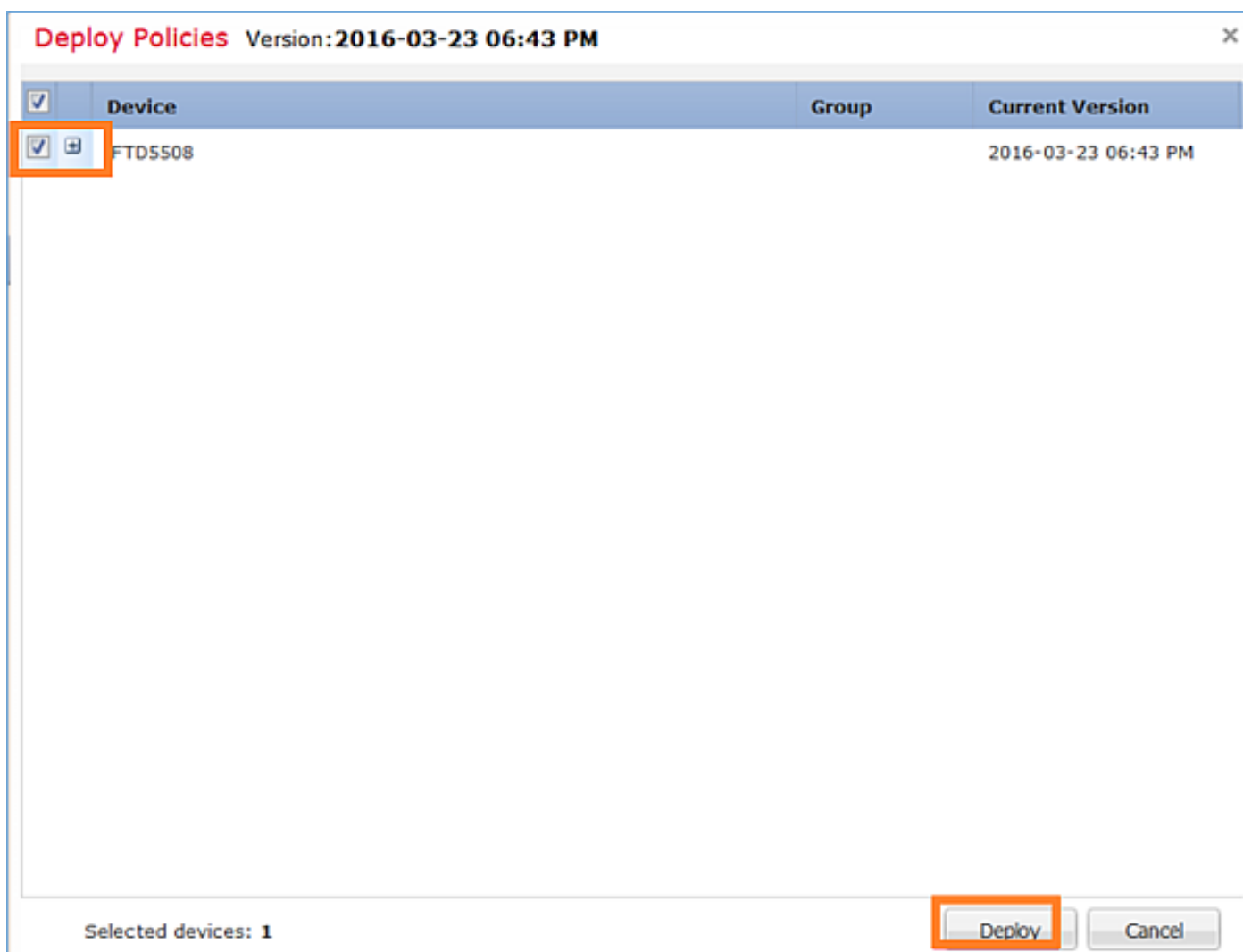
Verificación

Después de la actualización de 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
---------------------------------------------------

>
```

Tarea 7. Conexión y desconexión del modo CLI del motor LINA

Entre en el modo CLI de LINA y desconéctese de él.

Solución

Desde el modo FTD CLISH, escriba el siguiente comando:

```
> 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#
```
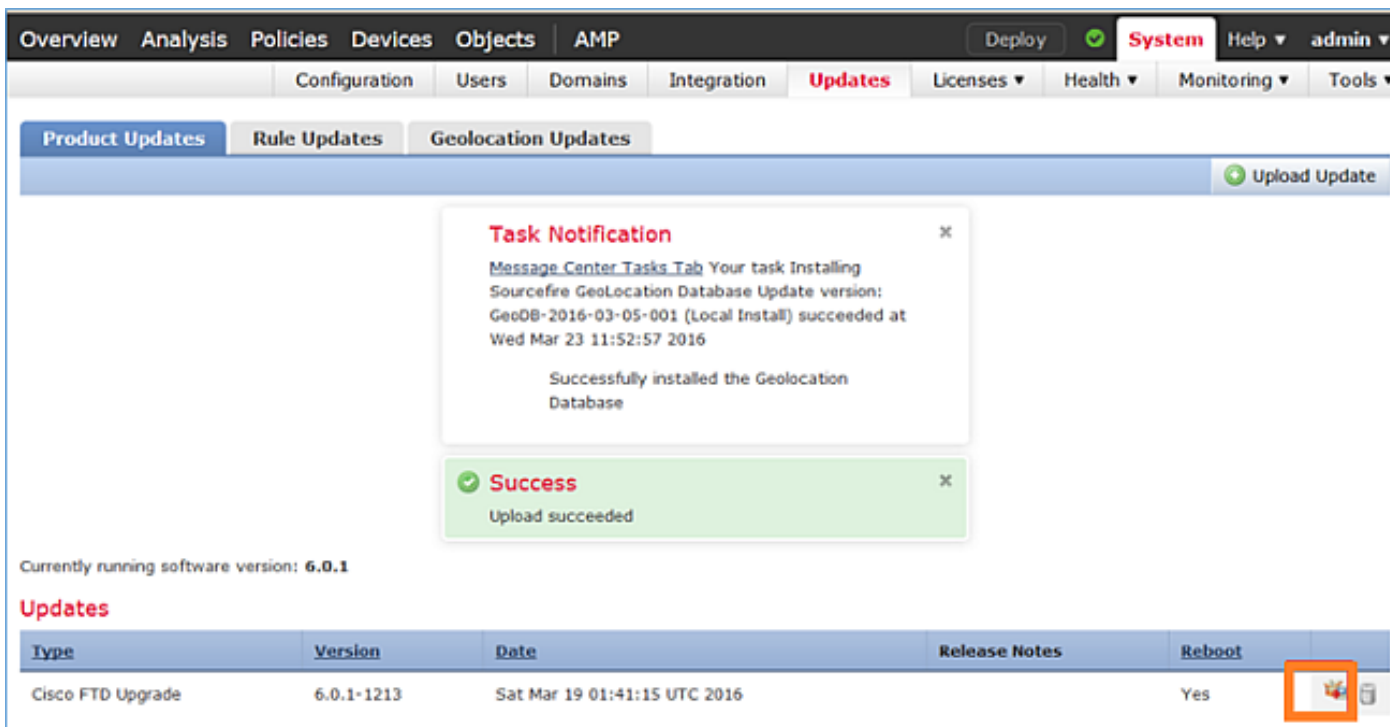
Como se menciona en el mensaje anterior, para desconectar (desconectar) de la consola de FTD LINA, escriba CTRL + a y, a continuación, presione d:

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

Tarea 8. Recrear imagen de una instalación FTD existente

Requisito

Vuelva a crear una imagen FTD existente e instale la versión 6.1.0-330

Solución

Esta tarea supone que hay un dispositivo FTD que ejecuta código 6.0.1.x y por las razones que sean necesarias para recrear la imagen (por ejemplo, corrupción de la base de datos irrecuperable, defecto catastrófico que no permite la actualización del software, etc.).

Resumen de pasos

1. Comprobación de compatibilidad.
2. Anule el registro de FTD de FMC.
3. Recargue el dispositivo FTD e ingrese BootCLI.
4. Ejecute el asistente de configuración.
5. Instale la imagen del sistema FTD.
6. Registre FTD en FMC.

PASOS DETALLADOS

Paso 1. Verifique las notas de la versión de Firepower y asegúrese de que la imagen FTD que desea utilizar sea compatible con el FMC. Si no actualiza primero el FMC.

Paso 2. Anule el registro (eliminación) de FTD de FMC. Este paso es necesario ya que después de la recreación de imágenes de FTD su UUID cambia y no se puede registrar de nuevo, pero se debe agregar desde el principio.

Paso 3. Recargue el dispositivo FTD e ingrese BootCLI. Dado que ya existe una imagen FTD instalada, se puede omitir la instalación de la imagen de inicio 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>
```

Paso 4.Ejecute el asistente de configuración y establezca los parámetros básicos de red:

```
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>
```

Paso 5. Verifique la conectividad con el servidor (FTP, HTTP, etc.) que contiene la imagen del sistema FTD e inicie la instalación:

```
firepower-boot>ping 10.48.40.70
PING 10.48.40.70 (10.48.40.70) 56(84) bytes of data.
64 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
--- 10.48.40.70 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
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.
```

Paso 6. Registrar FTD en 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              :
```

En FMC navegue a **Dispositivos > Administración de dispositivos** para agregar el dispositivo FTD.

Después de agregar FTD a FMC, debe:

- Reconfigure la configuración del dispositivo, como las interfaces y el enrutamiento

- Reconfigure políticas como VPN y QoS
- Vuelva a aplicar las políticas y configuraciones aplicadas anteriormente, como la política de control de acceso, NAT y configuración de plataforma

Información Relacionada

- [Guías de instalación y actualización](#)
- [Recreación de la imagen de Cisco ASA o del dispositivo de defensa frente a amenazas Firepower](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)