

Renovación del certificado de CA FMC Sftunnel para conectividad FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[¿Qué ocurre después de la fecha de caducidad?](#)

[¿Cómo se puede comprobar rápidamente si el certificado ha caducado o cuándo lo hace?](#)

[¿Cómo puedo recibir notificaciones en el futuro sobre el vencimiento de un certificado?](#)

[Solución 1: el certificado aún no ha caducado \(situación ideal\)](#)

[Enfoque recomendado](#)

[Solución 2: el certificado ya ha caducado](#)

[FTD aún conectados a través de sftunnel](#)

[FTD no conectados más a través de sftunnel](#)

[Enfoque recomendado](#)

[Enfoque manual](#)

Introducción

Este documento describe la renovación del certificado de autoridad de certificación (CA) sftunnel de Firepower Management Center (FMC) en relación con la conectividad de Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense
- Centro de administración FirePOWER
- Public Key Infrastructure (PKI)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

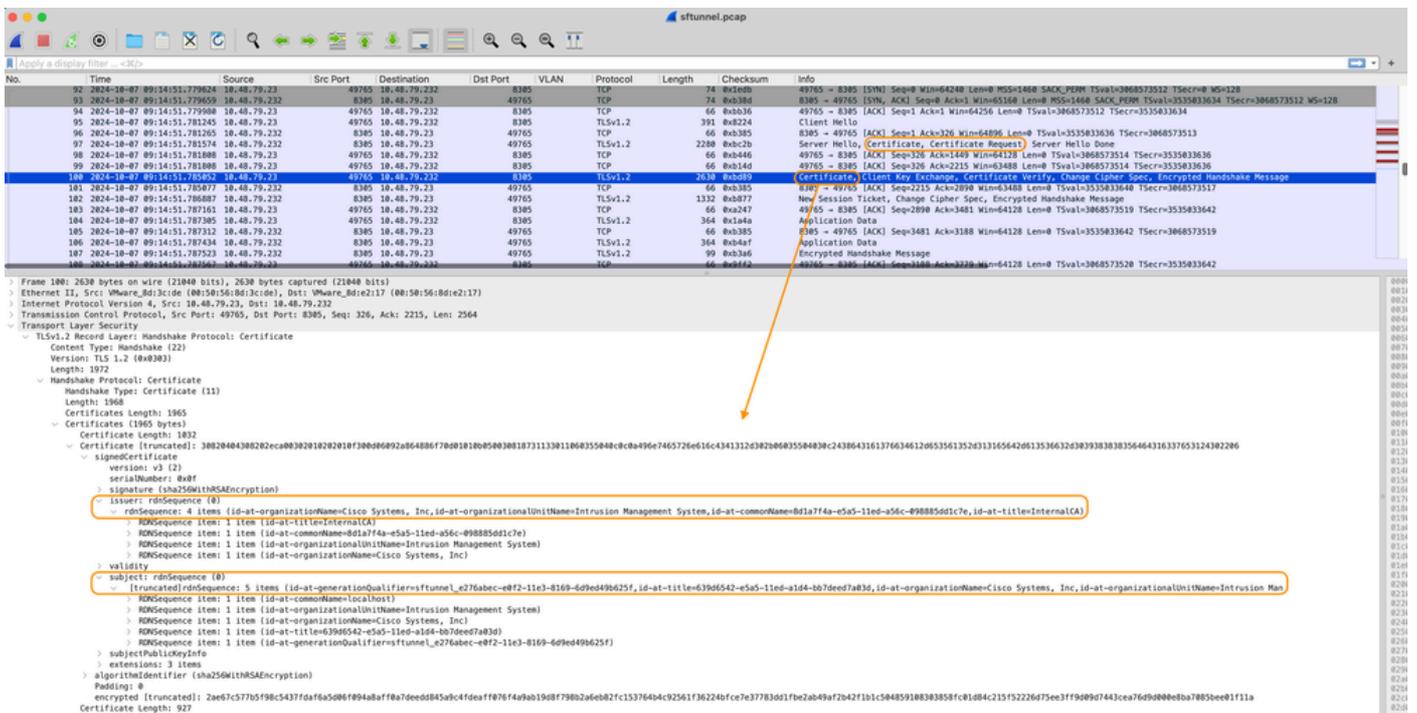
FMC y FTD se comunican entre sí a través de sftunnel (túnel de Sourcefire). Esta comunicación utiliza certificados para asegurar la conversación a través de una sesión TLS. Más información sobre el sftunnel y cómo se establece se puede encontrar en [este link](#).

En la captura de paquetes, puede ver que FMC (10.48.79.232 en este ejemplo) y FTD (10.48.79.23) intercambian certificados entre sí. Lo hacen para confirmar que hablan con el dispositivo correcto y que no hay intercepciones ni ataques de intrusos (MITM). La comunicación se cifra utilizando esos certificados y sólo la parte que tiene la clave privada asociada para ese certificado puede descifrarla de nuevo.

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of packets, with packet 97 selected. The bottom pane provides a hierarchical view of the selected packet's structure:

- Frame 97: 2288 bytes on wire (18240 bits), 2288 bytes captured (18240 bits)
- Ethernet II, Src: VMware_Bd3:17 (08:50:56:0d:e2:17), Dst: VMware_Bd3:17 (08:50:56:0d:e2:17)
- Internet Protocol Version 4, Src: 10.48.79.232, Dst: 10.48.79.23
- Transmission Control Protocol, Src Port: 8385, Dst Port: 49765, Seq: 1, Ack: 326, Len: 2214
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Context Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 1935
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1931
 - Certificate Length: 1928
 - Certificates (1928 bytes)
 - Certificate Length: 995
 - Certificate [truncated]: 380293903802823a083020102020100300069928646867700101005083081873113811060355848c0ba496e746572616c4341312c02006035584830c243864316137663461206533613526313656426133366324083938383835646431637653124302206
 - signatureCertificate
 - version: v3 (2)
 - serialNumber: 0x0
 - signature (sha256withRSAEncryption)
 - issuer: rdnSequence (0)
 - rdnSequence: 4 items (id-at-organizationName=Cisco Systems, Inc,id-at-organizationalUnitName=Intrusion Management System,id-at-commonName=01a774a-e5a5-11e0-a56c-998855d01c7e,id-at-title=InternalCA)
 - validity
 - subject: rdnSequence (0)
 - rdnSequence: 5 items (id-at-generationQualifiers=sftunnel,id-at-title=01a774a-e5a5-11e0-a56c-998855d01c7e,id-at-organizationName=Cisco Systems, Inc,id-at-organizationalUnitName=Intrusion Management System,id-at-commonName=localhost)
 - rdnSequence item: 1 item (id-at-commonName=localhost)
 - rdnSequence item: 1 item (id-at-organizationalUnitName=Intrusion Management System)
 - rdnSequence item: 1 item (id-at-organizationName=Cisco Systems, Inc)
 - rdnSequence item: 1 item (id-at-title=01a774a-e5a5-11e0-a56c-998855d01c7e)
 - rdnSequence item: 1 item (id-at-generationQualifiers=sftunnel)
 - subjectPublicKeyInfo
 - extensions: 3 items
 - algorithmIdentifier (sha256withRSAEncryption)
 - padding: 0
 - encrypted [truncated]: 8456875c290d5279f6e3a48828e6d734e739e347da71038a0b0e93c86c801d70eb2e7f9354c0192606545097527f71e70bc1ab3c0ba081e9c709166a052337a1591055c47692025fe15e080792315f0e0ef183632e76bade4871a2796c2d086c8188e

Certificate_exchange_server_cert



Certificate_exchange_client_cert

Puede ver que los certificados están firmados por la misma autoridad de certificación (CA) CA interna (emisor) configurada en el sistema FMC. La configuración se define en el FMC en el archivo /etc/sf/sftunnel.conf que contiene algo como:

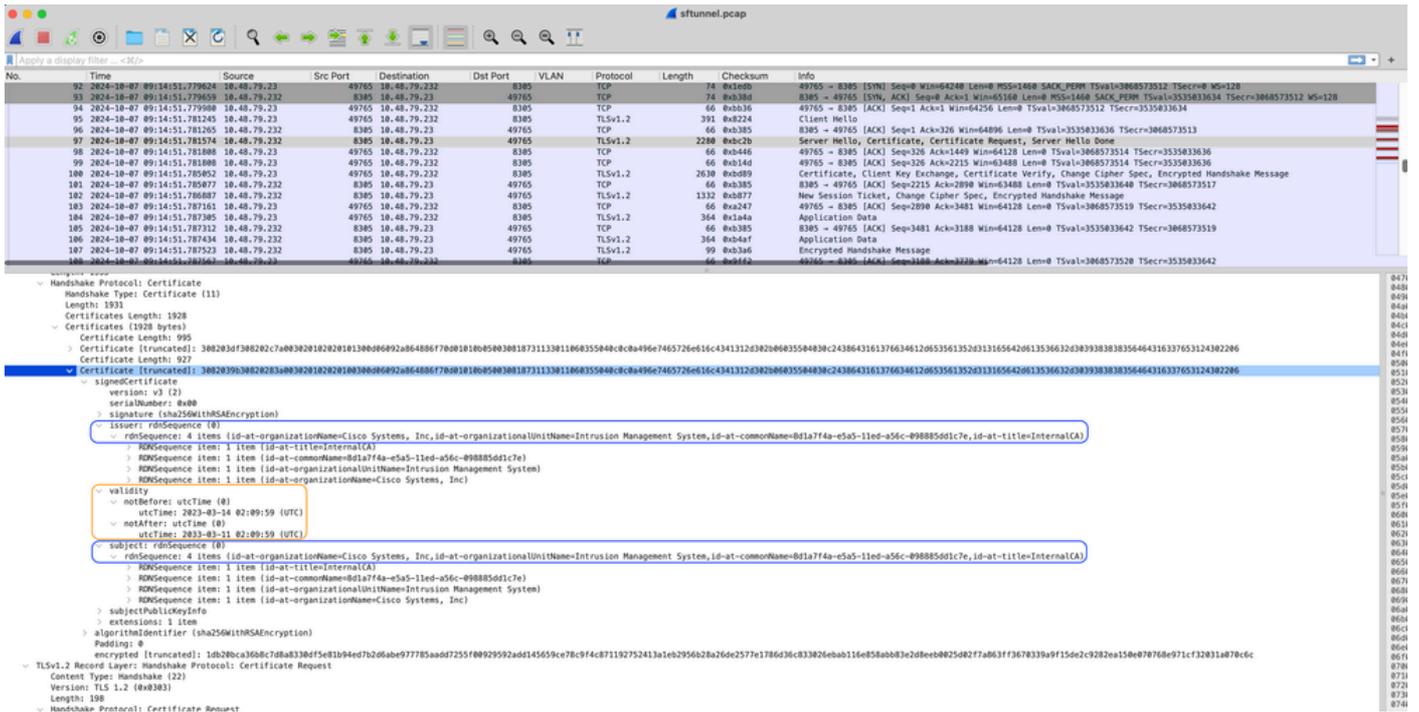
```
proxys1 {
  proxy_cert /etc/sf/keys/sftunnel-cert.pem;          ----> Certificate provided by FMC to FTD
  proxy_key /etc/sf/keys/sftunnel-key.pem;
  proxy_cacert /etc/sf/ca_root/cacert.pem;           ----> CA certificate (InternalCA)
  proxy_cr1 /etc/sf/ca_root/cr1.pem;
  proxy_cipher 1;
  proxy_tls_version TLSv1.2;
};
```

Indica la CA que se utiliza para firmar todos los certificados para sftunnel (tanto el FTD como el FMC) y el certificado que utiliza el FMC para enviar a todos los FTD. Este certificado está firmado por la CA interna.

Cuando el FTD se registra en el FMC, el FMC también crea un certificado para enviar al dispositivo FTD que se utiliza para la comunicación posterior en el sftunnel. Este certificado también está firmado por el mismo certificado de CA interna. En FMC, puede encontrar ese certificado (y la clave privada) en /var/sf/peers/<UUID-FTD-device> y posiblemente en la carpeta certs_push y se denomina sftunnel-cert.pem (sftunnel-key.pem para la clave privada). En FTD, puede encontrarlos en /var/sf/peers/<UUID-FMC-device> con la misma convención de nomenclatura.

Sin embargo, cada certificado tiene también un período de validez por motivos de seguridad. Al inspeccionar el certificado de CA interna, también podemos ver el período de validez que es de

10 años para la CA interna de FMC, como se muestra en la captura de paquetes.

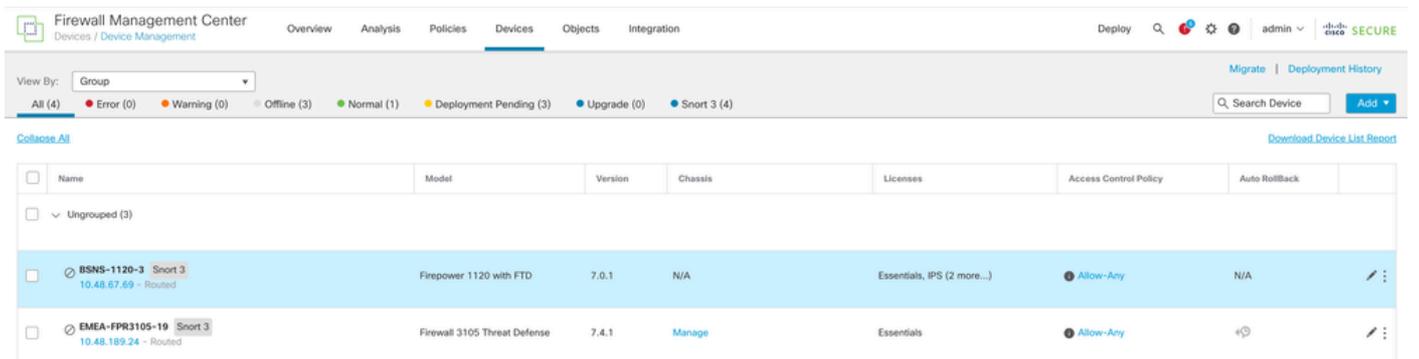


FMC-InternalCA_valid

Problema

El certificado de CA interna FMC solo es válido durante 10 años. Una vez transcurrido el tiempo de caducidad, el sistema remoto ya no confía en este certificado (así como en los certificados firmados por él), lo que provoca problemas de comunicación de túnel seguro entre los dispositivos FTD y FMC. Esto también significa que varias funciones clave, como los eventos de conexión, las búsquedas de malware, las reglas basadas en identidad, las implementaciones de políticas y muchas otras cosas, no funcionan.

Los dispositivos aparecen como inhabilitados en la interfaz de usuario de FMC en la pestaña Devices > Device Management cuando el sftunnel no está conectado. El problema relacionado con este vencimiento se rastrea en el Id. de error de Cisco [CSCwd08098](#). Tenga en cuenta que todos los sistemas están afectados, incluso cuando ejecuta una versión corregida del defecto. Encontrará más información sobre esta solución en la sección Solución.



Disabled-devices

El FMC no actualiza automáticamente la CA y vuelve a publicar los certificados en los dispositivos FTD. Tampoco hay ninguna alerta sanitaria del CSP que indique que el certificado ha caducado. A este respecto, se realiza un seguimiento del error de ID de Cisco [CSCwd08448](#) para proporcionar una alerta de estado en la interfaz de usuario de FMC en el futuro.

¿Qué ocurre después de la fecha de caducidad?

Inicialmente no sucede nada y los canales de comunicación sftunnel continúan funcionando como antes. Sin embargo, cuando se interrumpe la comunicación sftunnel entre los dispositivos FMC y FTD e intenta restablecer la conexión, se produce un error y se pueden observar líneas de registro en el archivo de registro de mensajes que apuntan a la expiración del certificado.

Líneas de registro del dispositivo FTD desde /ngfw/var/log/messages:

```
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [INFO] Initiating IPv4 connection
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [INFO] Wait to connect to 8305 (IP
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [INFO] Connected to 10.10.200.31 f
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] -Error with certificate at
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] issuer = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] subject = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] err 10:certificate has e
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [ERROR] Connect:SSL handshake fail
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunne1d:sf_ssl [WARN] SSL Verification status: ce
```

Líneas de registro desde el dispositivo FMC desde /var/log/messages:

```
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [INFO] VERIFY ssl_verify_callback_in
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [ERROR] SSL_renegotiate error: 1: er
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [INFO] establishConnectionUtil: Fail
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [ERROR] establishSSLConnection: Unab
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [ERROR] establishSSLConnection: ret_
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [ERROR] establishSSLConnection: iret
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunne1d:sf_ssl [ERROR] establishSSLConnection: Fail
```

La comunicación sftunnel se puede interrumpir por varias razones:

- Pérdida de comunicación debido a la pérdida de conectividad de red (potencialmente solo temporal)
- Reinicio de FTD o FMC
 - Esperados: reinicio manual, actualizaciones, reinicio manual del proceso sftunnel en FMC o FTD (por ejemplo, mediante pmtool restartbyid sftunnel)
 - Inesperados: rastreos, interrupción del suministro eléctrico

Debido a que hay muchas posibilidades que pueden interrumpir la comunicación sftunnel, se recomienda encarecidamente corregir la situación lo más rápidamente posible, incluso cuando actualmente todos los dispositivos FTD están conectados correctamente a pesar del certificado caducado.

¿Cómo se puede comprobar rápidamente si el certificado ha caducado o cuándo lo hace?

La manera más fácil es ejecutar estos comandos en la sesión SSH de FMC:

```
expert
sudo su
cd /etc/sf/ca_root
openssl x509 -dates -noout -in cacert.pem
```

Muestra los elementos de validez del certificado. La parte principal relevante aquí es el "notAfter" que muestra que el certificado aquí es válido hasta el 5 de octubre de 2034.

```
root@firepower:/Volume/home/admin# openssl x509 -dates -in /etc/sf/ca_root/cacert.pem
notBefore=Oct  7 12:16:56 2024 GMT
notAfter=Oct  5 12:16:56 2034 GMT
```

NotAfter

Si prefiere que se ejecute un solo comando que le proporcione inmediatamente la cantidad de días para los que el certificado sigue siendo válido, puede utilizar lo siguiente:

```
CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -enddate -noout -in "$CERT_PATH" | c
```

Se muestra un ejemplo de una configuración en la que el certificado sigue siendo válido durante varios años.

```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS + THIRTY_
DAYS_SECONDS)); DAYS_LEFT=$(( (EXPIRY_DATE_SECONDS - CURRENT_DATE_SECONDS) / (24*60*60) )); if [ "$EXPIRY_DATE
_SECONDS" -le "$CURRENT_DATE_SECONDS" ]; then DAYS_EXPIRED=$(( (CURRENT_DATE_SECONDS - EXPIRY_DATE_SECONDS) /
(24*60*60) )); echo -e "\n\nThe certificate has expired $DAYS_EXPIRED days ago.\n\nIn case the sftunnel communicat
ion with the FTD is not yet lost, you need to take action immediately in renewing the certificate.\n"; elif [
"$EXPIRY_DATE_SECONDS" -le "$EXPIRY_THRESHOLD" ]; then echo -e "\n\nThe certificate will expire within the next
30 days!\n\nIt is ONLY valid for $DAYS_LEFT more days.\n\nIt is recommended to take action in renewing the certifi
cate as quickly as possible.\n"; else echo -e "\n\nThe certificate is valid for more than 30 days.\n\nIt is valid
for $DAYS_LEFT more days.\n\nThere is no immediate need to perform action but this depends on how far the expiry
date is in the future.\n"; fi
```

```
The certificate is valid for more than 30 days.
It is valid for 3649 more days.
There is no immediate need to perform action but this depends on how far the expiry date is in the future.
```

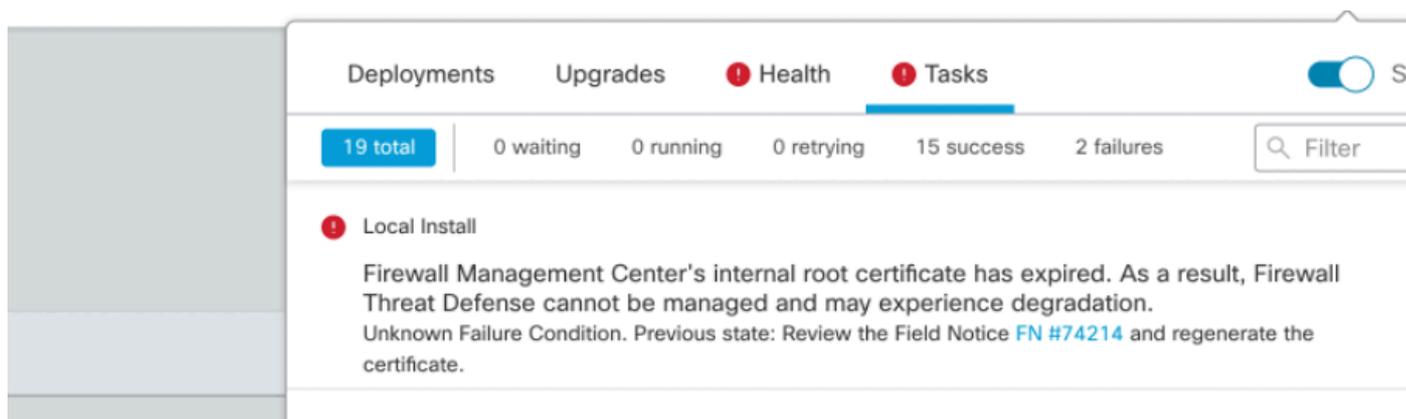
```
root@fmcv72-stejanss:/Volume/home/admin#
```

Comando_validación_vencimiento_certificado

¿Cómo puedo recibir notificaciones en el futuro sobre el vencimiento de un certificado?

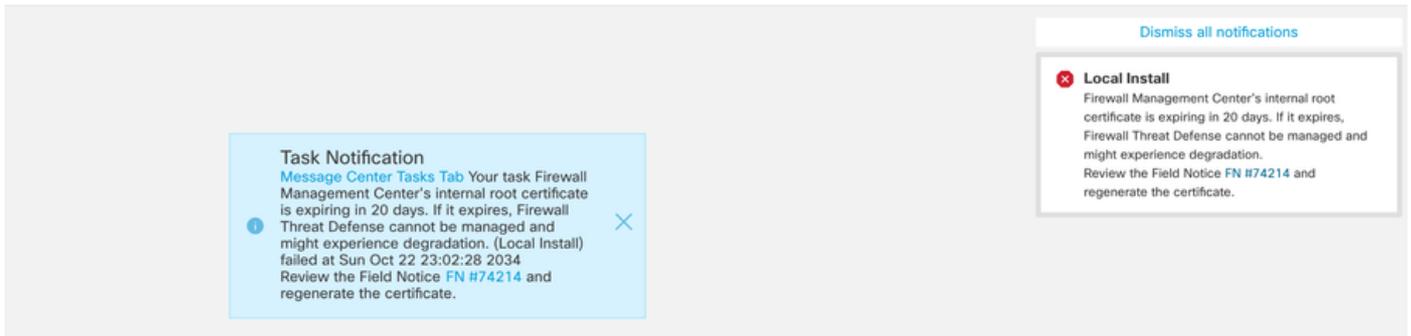
Con las actualizaciones recientes de VDB (399 o superiores), recibirá una alerta automáticamente cuando su certificado caduque en 90 días. Por lo tanto, no es necesario que realice un seguimiento manual de esta información, ya que se le avisará cuando se aproxime el momento de vencimiento. A continuación, se muestra en la página web del CSP de dos formas. Ambos métodos hacen referencia a la [página de avisos de campo](#).

El primer método es a través de la Ficha Tarea. Este mensaje es persistente y está disponible para el usuario a menos que se cierre explícitamente. La notificación emergente también aparece y está disponible hasta que el usuario la cierre explícitamente. Siempre aparece como un error.

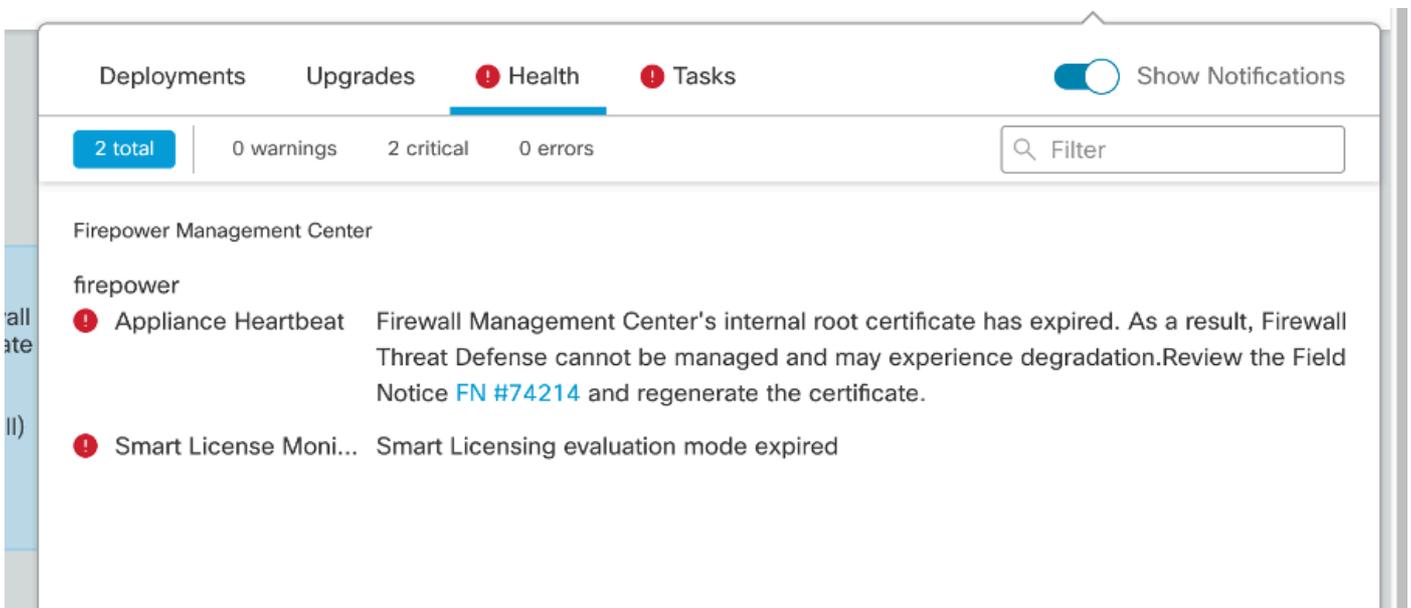


The screenshot shows the 'Tasks' tab in the Firewall Management Center interface. The 'Tasks' tab is active, showing 19 total tasks, with 15 successful and 2 failures. A notification for 'Local Install' is displayed, stating: 'Firewall Management Center's internal root certificate has expired. As a result, Firewall Threat Defense cannot be managed and may experience degradation. Unknown Failure Condition. Previous state: Review the Field Notice FN #74214 and regenerate the certificate.'

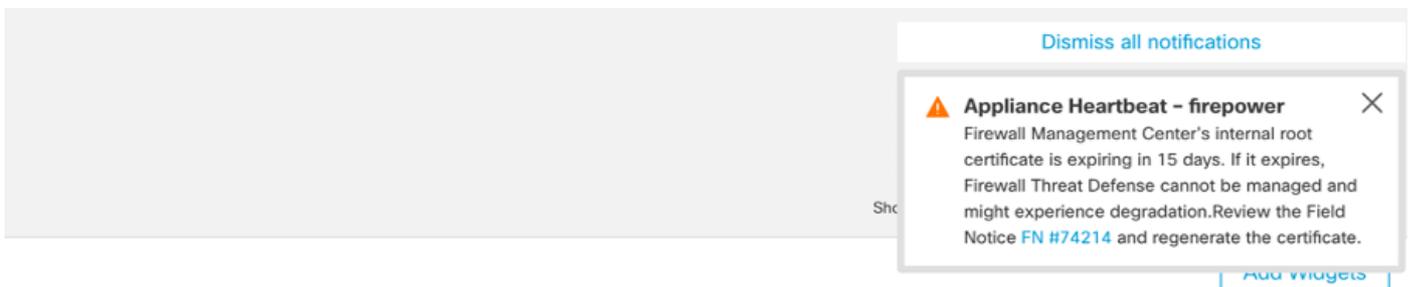
Notificación de vencimiento en la ficha Tarea



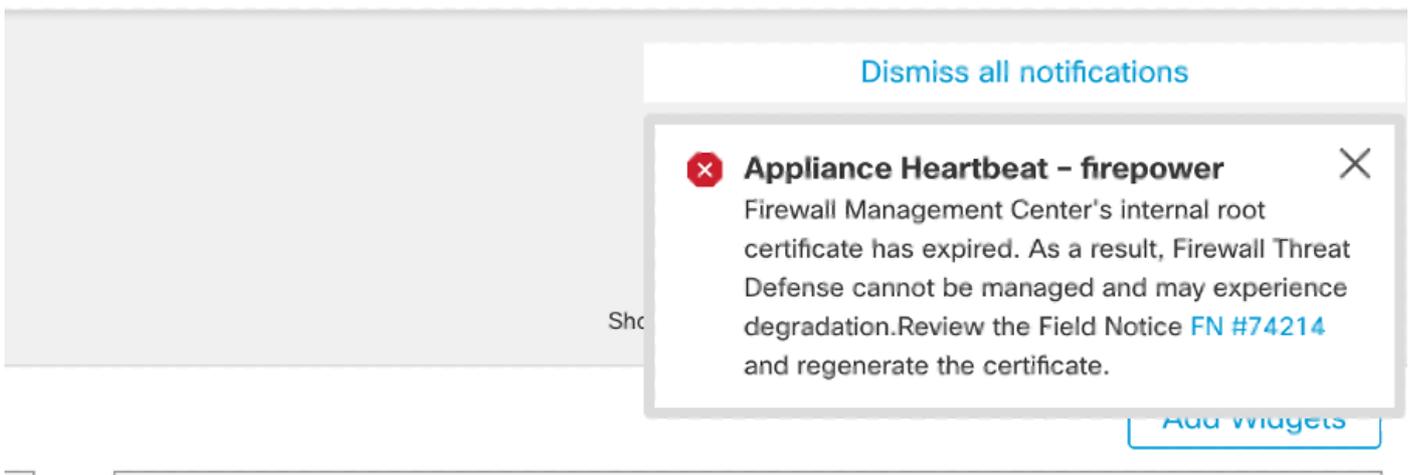
El segundo método es a través de Health Alert. Esto se muestra en la ficha Estado; sin embargo, no es fijo y se reemplaza o quita cuando se ejecuta el monitor de estado, que de forma predeterminada es cada 5 minutos. También muestra una notificación emergente que el usuario debe cerrar de forma explícita. Esto puede aparecer como error (cuando caducó) y como advertencia (cuando caducará).



Notificación de vencimiento en la ficha Estado



Aviso de advertencia en la ventana emergente Alerta de estado



Notificación de error en la ventana emergente Alerta de estado

Solución 1: el certificado aún no ha caducado (situación ideal)

Esta es la mejor situación ya que entonces dependiendo de la expiración del certificado, todavía tenemos tiempo. O bien tomamos el enfoque totalmente automatizado (recomendado) que depende de la versión de FMC o adoptamos un enfoque más manual que requiere la interacción del TAC.

Enfoque recomendado

Se trata de una situación en la que, en circunstancias normales, no se espera tiempo de inactividad ni la menor cantidad de operaciones manuales.

Antes de continuar, debe instalar la [revisión](#) para su versión en particular, como se indica aquí. La ventaja aquí es que esas revisiones no requieren un reinicio del FMC y, por lo tanto, la comunicación potencial de sftunnel interrumpida cuando el certificado ya ha caducado. Las revisiones disponibles son:

- [7.0.0 - 7.0.6](#) : Hotfix FK - 7.0.6.99-9
- 7.1.x: no fixed release as end of software maintenance
- [7.2.0 - 7.2.9](#) : Hotfix FZ - 7.2.9.99-4
- [7.3.x](#): Hotfix AE - 7.3.1.99-4
- [7.4.0 - 7.4.2](#) : Hotfix AO - 7.4.2.99-5
- [7.6.0](#) : Hotfix B - 7.6.0.99-5

Una vez instalada la revisión, el FMC debe contener la secuencia de comandos `generate_certs.pl` que:

1. Regenera la CA interna
2. Vuelve a crear los certificados sftunnel firmados por esta nueva CA interna
3. Envía los nuevos certificados y claves privadas de sftunnel a los dispositivos FTD respectivos (cuando sftunnel está operativo)

Por lo tanto, se recomienda (si es posible):

1. Instale la revisión correspondiente arriba
2. Realice una copia de seguridad en el FMC
3. Valide todas las conexiones sftunnel actuales mediante el script sftunnel_status.pl en el FMC (desde el modo experto)
4. Ejecute el script desde el modo experto mediante generate_certs.pl
5. Examine el resultado para comprobar si se requiere alguna operación manual (cuando los dispositivos no están conectados al FMC) [se explica más adelante]
6. Ejecute sftunnel_status.pl desde el FMC para validar que todas las conexiones sftunnel funcionan correctamente

```
root@fmcv72-stejanss:/Volume/home/admin# generate_certs.pl
setting log file to /var/log/sf/sfca_generation.log

You are about to generate new certificates for FMC and devices.
After successful cert generation, device specific certs will be pushed automatically
If the connection between FMC and a device is down, user needs to copy the certificates onto the device manually
For more details on disconnected devices, use sftunnel_status.pl
Do you want to continue? [yes/no]:yes

Current ca_root expires in 3646 days - at Oct 9 10:12:50 2034 GMT
Do you want to continue? [yes/no]:yes

Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem

Some files were failed to be pushed to remote peers. For more details check /var/tmp/certs/1728915794/FAILED_PUSH

Scalars leaked: 1
root@fmcv72-stejanss:/Volume/home/admin# █
```

Archivo de comandos Generate_certs.pl



Nota: Cuando FMC se está ejecutando en alta disponibilidad (HA), primero debe realizar la operación en el nodo principal y, a continuación, en el secundario, ya que también utiliza esos certificados para comunicarse entre los nodos FMC. La CA interna en ambos nodos FMC es diferente.

En el ejemplo aquí se ve que crea un archivo de registro en `/var/log/sf/sfca_generation.log`, indica que se debe utilizar `sftunnel_status.pl`, indica el tiempo de vencimiento en InternalCA e indica que no hay fallas en ella. Aquí, por ejemplo, no pudo enviar los certificados al dispositivo BSNS-1120-1 y al dispositivo EMEA-FPR3110-08, lo que se espera debido a que el sftunnel no funcionaba para esos dispositivos.

Para corregir el sftunnel para las conexiones fallidas, ejecute los siguientes pasos:

1. En la CLI de FMC, abra el archivo FAILED_PUSH mediante `cat /var/tmp/certs/1728303362/FAILED_PUSH` (el valor numérico representa la hora unix, por lo

que debe comprobar el resultado del comando anterior en su sistema), que tiene el siguiente formato: FTD_UUID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINATION_PATH_ON_FTD

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/tmp/certs/1728915794/FAILED_PUSH
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /etc/sf/ca_root/cacert.pem /var/sf/peers/cdb123c8-4
347-11ef-aca1-f3aa241412a1/cacert.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-key.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-cert.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /etc/sf/ca_root/cacert.pem /var/sf/peers/cdb12
3c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
d77/certs_pushed//sftunnel-key.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
root@fmcv72-stejanss:/Volume/home/admin#
```

FAILED_PUSH

- Transferir estos nuevos certificados (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) desde el FMC a los dispositivos FTD
===Aproximación automática===

La instalación de la revisión también proporciona los scripts copy_sftunnel_certs.py y copy_sftunnel_certs_jumpserver.py que automatizan la transferencia de los diversos certificados a sistemas para los cuales sftunnel no estaba activo mientras se regeneraban los certificados. Esto también se puede utilizar para sistemas que tenían una conexión sftunnel interrumpida porque el certificado ya había caducado.

Puede utilizar el script copy_sftunnel_certs.py cuando el FMC tiene acceso SSH a los diversos sistemas FTD. Si no es así, puede descargar el script (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) del FMC a un servidor de salto que tenga acceso SSH tanto al FMC(s) como a los dispositivos FTD y ejecutar el script Python desde allí. Si esto tampoco es posible, sugiera ejecutar el enfoque manual que se muestra a continuación. Los siguientes ejemplos muestran el script copy_sftunnel_certs.py que se está utilizando, pero los pasos son los mismos para el script copy_sftunnel_certs_jumpserver.py.

R. Cree un archivo CSV en el FMC (o servidor de salto) que contenga la información del dispositivo (nombre_dispositivo, dirección IP, nombre_usuario_administrador, contraseña_administrador) que se utiliza para realizar la conexión SSH.

Cuando ejecute esto desde un servidor remoto como un servidor de salto para el FMC principal, asegúrese de agregar los detalles del FMC principal como la primera entrada seguida por todos los FTD gestionados y el FMC secundario. Cuando ejecute esto desde un servidor remoto como un servidor de salto para FMC secundario, asegúrese de agregar los detalles de FMC secundario como la primera entrada seguida de todo FTD administrado.

- Cree un archivo usando vi devices.csv. `root@firepower:/Volume/home/admin# vi devices.csv`


```
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin# vi devices.csv
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin# copy_sftunnel_certs.py devices.csv

=====

2024-11-12 14:07:36 - Attempting connection to FMCpri
2024-11-12 14:07:40 - Connected to FMCpri
2024-11-12 14:07:41 - FMCpri is not an HA-peer. Certificates will not be copied
2024-11-12 14:07:41 - Closing connection with FMCpri

=====

2024-11-12 14:07:41 - Attempting connection to FTDv
2024-11-12 14:07:43 - Connected to FTDv
2024-11-12 14:07:44 - Copying certificates to peer
2024-11-12 14:07:44 - Successfully copied certificates to FTDv
2024-11-12 14:07:44 - Restarting sftunnel for FTDv
2024-11-12 14:07:44 - Closing connection with FTDv

=====

2024-11-12 14:07:44 - Attempting connection to BSNS-1120-1
2024-11-12 14:08:04 - Could not connect to BSNS-1120-1

=====

root@firepower:/Volume/home/admin# █
```

copy_sftunnel_certs.py devices.csv

===Aproximación manual===

1. Imprima (cat) la salida de cada uno de los archivos de cada FTD afectado (cacert.pem / sftunnel-key.pem (no se muestra completamente por motivos de seguridad) / sftunnel-cert.pem) en la CLI de FMC copiando la ubicación del archivo de la salida anterior (archivo FAILED_PUSH).

2. Abra la CLI de FTD de cada FTD respectivo en el modo experto con privilegios raíz a través de sudo su y renueve los certificados con el siguiente procedimiento.

1. Busque la ubicación que aparece en el resaltado azul claro de la salida FAILED_PUSH (cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 aquí, por ejemplo, pero esto es diferente para cada FTD).
2. Realice copias de seguridad de los archivos existentes.

```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```

```
> expert
admin@BSNS-1120-1:~$ sudo su
Password:
root@BSNS-1120-1:/home/admin# cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp cacert.pem cacert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-cert.pem sftunnel-cert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-key.pem sftunnel-key.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal sftunnel*
-rw-r--r-- 1 root root 1.5K Oct 14 12:41 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 12:41 cacert.pem
```

Realizar copias de seguridad de los certificados actuales

3. Vacía los archivos para que podamos escribir nuevo contenido en ellos.

```
> cacert.pem
> sftunnel-cert.pem
> sftunnel-key.pem
```

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-cert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-key.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal sftunnel*
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal cacert.pem
-rw-r--r-- 1 root root 0 Oct 14 14:50 cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

Contenido vacío de los archivos de certificado existentes

4. Escriba el nuevo contenido (a partir de la salida de FMC) en cada uno de los archivos individualmente mediante vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (comando separado por archivo: las capturas de pantalla solo muestran esto para cacert.pem, pero debe repetirse para sftunnel-cert.pem y

```
sftunnel-key.pem).root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# vi cacert.pem
```

```
vi cacert.pem
```

1. Presione **i** para entrar al modo interactivo (después de ingresar el comando **vi** y de ver un archivo vacío).
2. Copie y pegue todo el contenido (incluidos **-----BEGIN CERTIFICATE-----** y **-----END CERTIFICATE-----**) en el archivo.

```
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwYcxzEzARBgNVBAwMck1udGvYmFz
Q0EwJDAiBgNVBAsMG01udHJ1c2lubiBNYW5hZ2VtZW50IFN5c3RlbnRlc3R1e
AwwkY2RiMTIzYzgtNDM0Ny0xMwVmlWFjYTEtZjNhYTl0MTQxMmExMRswGQYDVQ
DBJDaXNjb3R1eXN0ZW1zLmVudG91bnR1eXN0ZW1zLmVudG91bnR1eXN0ZW1z
MzI4WjBhZEMBEGA1UEDAwKSjUwYXN0ZTEkMCIgA1UECwwbSW50cnVzaW9u
IE1hbmFnZW1lbnQGU3ZldGVtMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZ
WNhMS1mZmMjQxNDEyYTYxGzAZBgNVBAoMEkNpc2NvIFN5c3RlbnR1eXN0ZW1
zASUwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMMUav8k
VukFxiV917W4d7/CYBb4pd1KiM0iJAep3wqmdpDUQ4KBDWnCS+p8dg+XK7Asp
0W36CDmdpRwRfQm7J51txEuyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6V
LQ1+aR1APCF7UYpMgFPH3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXn
L6Jn3rfoKbF0M77xUtiMc0504buhfzS1tAm5J0bFuXMcPYq1N+t137rL/1etw
HzmjVke7g/rfnv0y0N+4m8i5QRN0BoghtZ0+Y/PudToSX0VmKh5Sq/i1Mv0Y
BZEIM3Dx+Gb/DQYBWLWUcAwEAATANBgkqhkiG9w0BAQsFAAOCQAQAY2EVhEoy
1DdlWSu2ewdehthBtI6Q5x7eUD187bbowmTJsdl00LVGgYoU5qUFDh3NAqSxrDHEu
/NsLUbrRiA30RI8WEA1o/S6J3Q1F3hJF0qSrLIx/ST72jgL2o87ixhRIZreB/+26r
Ho5nns2r2tFss61KB1tWNnRZnSIYAwyhGcJH9quiZpFDJ3N83oREGX+xfLYqF
im5h3rFwk0J2q6YtaBjAuw0bldXGnrnWuIIV/xb0cwKbrALmtanhgGXyqT/pMYrjw
lI1xVL16/PrMTV29wCqAIVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnsty
Gx8hlzRvzHz2w==
-----END CERTIFICATE-----
~
~
~
~
~
~
-- INSERT --
```

Copiar contenido en vi (modo INSERT)

3. Cierre y escriba en el archivo con **ESC** seguido de **:wq** y, a continuación, escriba.

```
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwYcxzEzARBgNVBAwMck1udGvYmFz
Q0EwJDAiBgNVBAsMG01udHJ1c2lubiBNYW5hZ2VtZW50IFN5c3RlbnRlc3R1e
AwwkY2RiMTIzYzgtNDM0Ny0xMwVmlWFjYTEtZjNhYTl0MTQxMmExMRswGQYDVQ
DBJDaXNjb3R1eXN0ZW1zLmVudG91bnR1eXN0ZW1zLmVudG91bnR1eXN0ZW1z
MzI4WjBhZEMBEGA1UEDAwKSjUwYXN0ZTEkMCIgA1UECwwbSW50cnVzaW9u
IE1hbmFnZW1lbnQGU3ZldGVtMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZ
WNhMS1mZmMjQxNDEyYTYxGzAZBgNVBAoMEkNpc2NvIFN5c3RlbnR1eXN0ZW1
zASUwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMMUav8k
VukFxiV917W4d7/CYBb4pd1KiM0iJAep3wqmdpDUQ4KBDWnCS+p8dg+XK7Asp
0W36CDmdpRwRfQm7J51txEuyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6V
LQ1+aR1APCF7UYpMgFPH3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXn
L6Jn3rfoKbF0M77xUtiMc0504buhfzS1tAm5J0bFuXMcPYq1N+t137rL/1etw
HzmjVke7g/rfnv0y0N+4m8i5QRN0BoghtZ0+Y/PudToSX0VmKh5Sq/i1Mv0Y
BZEIM3Dx+Gb/DQYBWLWUcAwEAATANBgkqhkiG9w0BAQsFAAOCQAQAY2EVhEoy
1DdlWSu2ewdehthBtI6Q5x7eUD187bbowmTJsdl00LVGgYoU5qUFDh3NAqSxrDHEu
/NsLUbrRiA30RI8WEA1o/S6J3Q1F3hJF0qSrLIx/ST72jgL2o87ixhRIZreB/+26r
Ho5nns2r2tFss61KB1tWNnRZnSIYAwyhGcJH9quiZpFDJ3N83oREGX+xfLYqF
im5h3rFwk0J2q6YtaBjAuw0bldXGnrnWuIIV/xb0cwKbrALmtanhgGXyqT/pMYrjw
lI1xVL16/PrMTV29wCqAIVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnsty
Gx8hlzRvzHz2w==
-----END CERTIFICATE-----
~
~
~
~
~
~
:wq
```

ESC seguida de **:wq** para escribir en el archivo

5. Valide que los permisos (**chmod 644**) y propietarios (**chown root:root**) correctos estén establecidos para cada uno de los archivos mediante **ls -hal**. Esto se configura correctamente cuando actualizamos el archivo existente.

```

root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal
total 68K
drwxr-xr-x 4 root root 4.0K Oct 14 15:01 .
drwxr-xr-x 3 root root 4.0K Oct 14 15:01 ..
-rw-r--r-- 1 root root 0 Oct 14 12:42 LIGHT_REGISTRATION
-rw-r--r-- 1 root root 0 Oct 14 12:42 LIGHT_UNREGISTRATION
-rw-r--r-- 1 root root 2.0K Oct 14 12:45 LL-caCert.pem
-rw-r--r-- 1 root root 2.2K Oct 14 12:45 LL-cert.pem
-rw-r--r-- 1 root root 3.2K Oct 14 12:45 LL-key.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:55 cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:49 cacert.pem.backup
-rw-r--r-- 1 root root 2.3K Oct 14 12:41 ims.conf
-rw-r--r-- 1 root root 221 Oct 14 12:41 peer_flags.json
drwxr-xr-x 3 root root 19 Oct 14 12:42 proxy_config
-rw-r--r-- 1 root root 1.2K Oct 14 12:42 sfiproxy.conf.json
-rw-r--r-- 1 root root 1.4K Oct 14 14:59 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 15:01 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
-rw-r--r-- 1 root root 5 Oct 14 12:48 sw_version
drwxr-xr-x 6 root root 90 Oct 14 12:42 sync2
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# █

```

Todos los archivos de certificado actualizados con los propietarios y permisos adecuados

3. Reinicie el sftunnel en cada FTD respectivo donde el sftunnel no estaba operativo para que los cambios en el certificado tengan efecto con el comando `pmtool restartbyid sftunnel`

```

root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# pmtool restartbyid sftunnel
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# █

```

`pmtool restartbyid sftunnel`

3. Valide que todos los FTD estén conectados correctamente ahora mediante la salida `sftunnel_status.pl`

Solución 2: el certificado ya ha caducado

En esta situación, tenemos dos escenarios diferentes. Todas las conexiones sftunnel siguen operativas o ya no lo están (o son parciales).

FTD aún conectados a través de sftunnel

Podemos aplicar el mismo procedimiento que se indica en la sección [El certificado aún no ha caducado \(situación ideal\) - Enfoque recomendado](#).

Sin embargo, NO actualice ni reinicie el FMC (ni ningún FTD) en esta situación, ya que desconecta todas las conexiones sftunnel y necesitamos ejecutar manualmente todas las actualizaciones de certificados en cada FTD. La única excepción a esta, son las versiones de revisión enumeradas, ya que no requieren un reinicio del FMC.

Los túneles permanecen conectados y los certificados se sustituyen en cada uno de los FTD. En caso de que algunos certificados no se rellenen, se le indican los que han fallado y debe seguir el [enfoque manual](#) como se ha indicado anteriormente en la sección anterior.

FTD no conectados más a través de sftunnel

Enfoque recomendado

Podemos aplicar el mismo procedimiento que se indica en la sección [El certificado aún no ha caducado \(situación ideal\) - Enfoque recomendado](#). En esta situación, el nuevo certificado se generará en el FMC pero no se puede copiar en los dispositivos porque el túnel ya está inactivo. Este proceso se puede automatizar con los scripts [copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py](#)

Si todos los dispositivos FTD están desconectados del FMC, podemos actualizar el FMC en esta situación ya que no tiene un impacto en las conexiones sftunnel. Si todavía tiene algunos dispositivos conectados a través de sftunnel, tenga en cuenta que la actualización de FMC cierra todas las conexiones sftunnel y no vuelven a aparecer debido al certificado caducado. La ventaja de la actualización sería que proporciona una buena orientación sobre los archivos de certificados que deben transferirse a cada uno de los FTD.

Enfoque manual

En esta situación, puede ejecutar la secuencia de comandos generate_certs.pl desde el FMC que genera los nuevos certificados, pero aún así tendrá que enviarlos [manualmente](#) a cada uno de los dispositivos FTD. Dependiendo de la cantidad de dispositivos, esto es factible o puede ser una tarea tediosa. Sin embargo, cuando se utilizan los scripts [copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py](#), esto es altamente automatizado.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).