

Erneuerung des FMC-Sftunnel-CA-Zertifikats für FTD-Konnektivität

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Was geschieht nach dem Ablaufdatum?](#)

[Wie kann ich schnell überprüfen, ob das Zertifikat abgelaufen ist oder wann es abläuft?](#)

[Wie werde ich in Zukunft über ein bevorstehendes Ablaufdatum des Zertifikats informiert?](#)

[Lösung 1 - Zertifikat ist noch nicht abgelaufen \(ideales Szenario\)](#)

[Empfohlener Ansatz](#)

[Lösung 2 - Zertifikat ist bereits abgelaufen](#)

[FTDs weiterhin über Sftunnel verbunden](#)

[FTDs nicht mehr über Sftunnel verbunden](#)

[Empfohlener Ansatz](#)

[Manueller Ansatz](#)

Einleitung

Dieses Dokument beschreibt die Verlängerung des Zertifikats der FirePOWER Management Center (FMC) Sftunnel Certificate Authority (CA) in Verbindung mit der FirePOWER Threat Defense (FTD)-Verbindung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Threat Defence
- FirePOWER Management Center
- Public Key Infrastructure (PKI)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FMC und FTD kommunizieren über Sftunnel (Sourcefire-Tunnel) miteinander. Diese Kommunikation verwendet Zertifikate, um die Kommunikation über eine TLS-Sitzung sicher zu machen. Mehr Informationen über den Sftunnel und wie er sich etabliert, finden Sie unter [diesem Link](#).

Aus der Paketerfassung geht hervor, dass das FMC (in diesem Beispiel 10.48.79.232) und FTD (10.48.79.23) Zertifikate miteinander austauschen. Dabei wird überprüft, ob die Kommunikation mit dem richtigen Gerät erfolgt und ob ein Lauschangriff oder Man-In-The-Middle-Angriff (MITM) nicht stattfindet. Die Kommunikation wird mit diesen Zertifikaten verschlüsselt, und nur der Teilnehmer, dem der private Schlüssel für das Zertifikat zugeordnet ist, kann das Zertifikat erneut entschlüsseln.

The screenshot displays a network traffic capture (sftunnel.pcap) showing a TLS handshake. The top pane lists packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 99 is highlighted, showing a TLSv1.2 Record Layer: Handshake Protocol: Certificate. The bottom pane shows the detailed structure of this certificate, including fields like version, serialNumber, issuer, validity, and subject. An orange arrow points from the 'subject' field in the bottom pane to the corresponding 'Info' column in the top pane.

Zertifikat_Austausch_Server_Zertifikat

Zertifikataustausch_Clientzertifikat

Sie können sehen, dass die Zertifikate von derselben Zertifizierungsstelle (Certificate Authority, CA) der internen Zertifizierungsstelle (Issuer) signiert werden, die auf dem FMC-System eingerichtet ist. Die Konfiguration wird im FMC in der Datei /etc/sf/sftunnel.conf definiert, die Folgendes enthält:

```

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;
};

```

Dies gibt die Zertifizierungsstelle an, die zum Signieren aller Zertifikate für Sftunnel (FTD und FMC) verwendet wird, sowie das Zertifikat, das vom FMC zum Senden an alle FTDs verwendet wird. Dieses Zertifikat wird von der InternalCA signiert.

Wenn sich FTD beim FMC registriert, erstellt das FMC auch ein Zertifikat, um das FTD-Gerät zu senden, das für die weitere Kommunikation auf dem Sftunnel verwendet wird. Dieses Zertifikat wird ebenfalls vom gleichen internen Zertifizierungsstellenzertifikat signiert. Auf FMC finden Sie dieses Zertifikat (und den privaten Schlüssel) unter /var/sf/peers/<UUID-FTD-device> und möglicherweise unter dem Ordner certs_push. und heißt sftunnel-cert.pem (sftunnel-key.pem für den privaten Schlüssel). Auf FTD finden Sie diese unter /var/sf/peers/<UUID-FMC-device> mit derselben Namenskonvention.

Jedes Zertifikat hat jedoch auch eine Gültigkeitsdauer für Sicherheitszwecke. Bei der Überprüfung

des InternalCA-Zertifikats wird auch die Gültigkeitsdauer angezeigt, die 10 Jahre für die FMC InternalCA beträgt, wie aus der Paketerfassung ersichtlich.

The screenshot shows a network traffic capture tool displaying a detailed view of a certificate. The certificate is issued by Cisco Systems, Inc. and is valid until 2033-03-31 02:09:59 UTC. The subject is 'Intrusion Management System'. The certificate is part of a TLSv1.2 Record Layer: Handshake Protocol: Certificate Request.

FMC-InternalCA_Gültigkeit

Problem

Das FMC InternalCA-Zertifikat ist nur 10 Jahre gültig. Nach Ablauf der Ablaufzeit vertraut das Remote-System diesem Zertifikat (sowie von ihm signierten Zertifikaten) nicht mehr und dies führt zu Problemen bei der Sftunnel-Kommunikation zwischen FTD- und FMC-Geräten. Dies bedeutet auch, dass einige wichtige Funktionen wie Verbindungsereignisse, Malware-Suchen, identitätsbasierte Regeln, Richtlinienbereitstellungen und viele andere Dinge nicht funktionieren.

Die Geräte werden auf der FMC-Benutzeroberfläche auf der Registerkarte Devices (Geräte) > Device Management (Geräteverwaltung) als deaktiviert angezeigt, wenn der Sftunnel nicht verbunden ist. Das Problem, das mit diesem Ablauf zusammenhängt, wird unter der Cisco Bug-ID [CSCwd08098](#) nachverfolgt. Beachten Sie, dass alle Systeme betroffen sind, auch wenn Sie eine feste Version des Fehlers ausführen. Weitere Informationen zu diesem Fix finden Sie im Lösungsabschnitt.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The 'Devices' tab is selected, and a list of devices is displayed. The devices are listed with their names, models, versions, chassis, licenses, access control policies, and auto rollback status.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
BSNS-1120-3	Firepower 1120 with FTD	7.0.1	N/A	Essentials, IPS (2 more...)	Allow-Any	N/A
EMA-FPR3105-19	Firewall 3105 Threat Defense	7.4.1	Manage	Essentials	Allow-Any	+

Das FMC aktualisiert die Zertifizierungsstelle nicht automatisch und veröffentlicht die Zertifikate nicht erneut auf den FTD-Geräten. Außerdem gibt es keinen FMC-Integritätsalarm, der anzeigt, dass das Zertifikat abläuft. Die Cisco Bug-ID [CSCwd08448](#) wird in dieser Hinsicht nachverfolgt, um eine Statuswarnung für die FMC-Benutzeroberfläche bereitzustellen.

Was geschieht nach dem Ablaufdatum?

Anfänglich passiert nichts und die sftunnel Kommunikationskanäle laufen weiter wie bisher. Wenn jedoch die Sftunnel-Kommunikation zwischen FMC- und FTD-Geräten unterbrochen wird und versucht wird, die Verbindung wiederherzustellen, schlägt sie fehl, und Sie können Protokollzeilen in der Protokolldatei beobachten, die auf das Ablaufdatum des Zertifikats hinweisen.

Protokollzeilen vom FTD-Gerät aus `/ngfw/var/log/messages`:

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

Protokollzeilen von FMC-Gerät aus `/var/log/messages`:

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

Die Sftunnel-Kommunikation kann aus verschiedenen Gründen unterbrochen werden:

- Kommunikationsverlust aufgrund von Verlust der Netzwerkverbindung (möglicherweise nur vorübergehend)
- Neustart von FTD oder FMC
 - Erwartete: Manueller Neustart, Upgrades, manueller Neustart des Sftunnel-Prozesses auf FMC oder FTD (z. B. durch `pmtool restartbyid sftunnel`)

- Unerwartete: Rückverfolgung, Stromausfall

Da es so viele Möglichkeiten gibt, die die sftunnel-Kommunikation unterbrechen können, ist es sehr ratsam, die Situation so schnell wie möglich zu korrigieren, auch wenn derzeit alle FTD-Geräte trotz abgelaufenem Zertifikat ordnungsgemäß angeschlossen sind.

Wie kann ich schnell überprüfen, ob das Zertifikat abgelaufen ist oder wann es abläuft?

Am einfachsten ist es, diese Befehle in der FMC SSH-Sitzung auszuführen:

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

Hier sehen Sie die Validity-Elemente des Zertifikats. Wichtigster Teil ist hier das "notAfter", welches zeigt, dass das Zertifikat hier bis zum 5. Oktober 2034 gültig ist.

```
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
```

NichtNach

Wenn Sie die Ausführung eines einzelnen Befehls vorziehen, der Ihnen sofort die Anzahl der Tage anzeigt, für die das Zertifikat noch gültig ist, können Sie Folgendes verwenden:

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

Ein Beispiel für eine Konfiguration, bei der das Zertifikat noch mehrere Jahre gültig ist, wird angezeigt.

```

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 "\nThe certificate has expired $DAYS_EXPIRED days ago.\nIn case the sftunnel communicat
ion with the FTD is not yet lost, you need to take action immediately in renewing the certificate.\n"; elif [
"$EXPIRY_DATE_SECONDS" -le "$EXPIRY_THRESHOLD" ]; then echo -e "\nThe certificate will expire within the next
30 days!\nIt is ONLY valid for $DAYS_LEFT more days.\nIt is recommended to take action in renewing the certifi
cate as quickly as possible.\n"; else echo -e "\nThe certificate is valid for more than 30 days.\nIt is valid
for $DAYS_LEFT more days.\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# █

```

Zertifikat_Ablauf_Validierung_Befehl

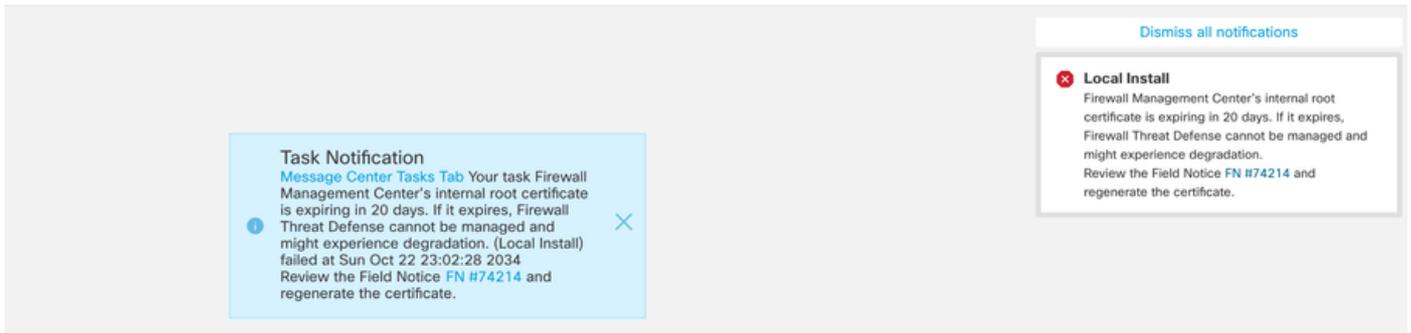
Wie werde ich in Zukunft über ein bevorstehendes Ablaufdatum des Zertifikats informiert?

Nach den letzten VDB-Updates (399 oder höher) werden Sie automatisch benachrichtigt, wenn Ihr Zertifikat innerhalb von 90 Tagen abläuft. Sie müssen dies daher nicht manuell nachverfolgen, da Sie kurz vor Ablauf der Frist benachrichtigt werden. Diese werden dann auf der FMC-Webseite in zwei Formen angezeigt. Beide Möglichkeiten finden Sie auf der [Seite mit den Feldhinweisen](#).

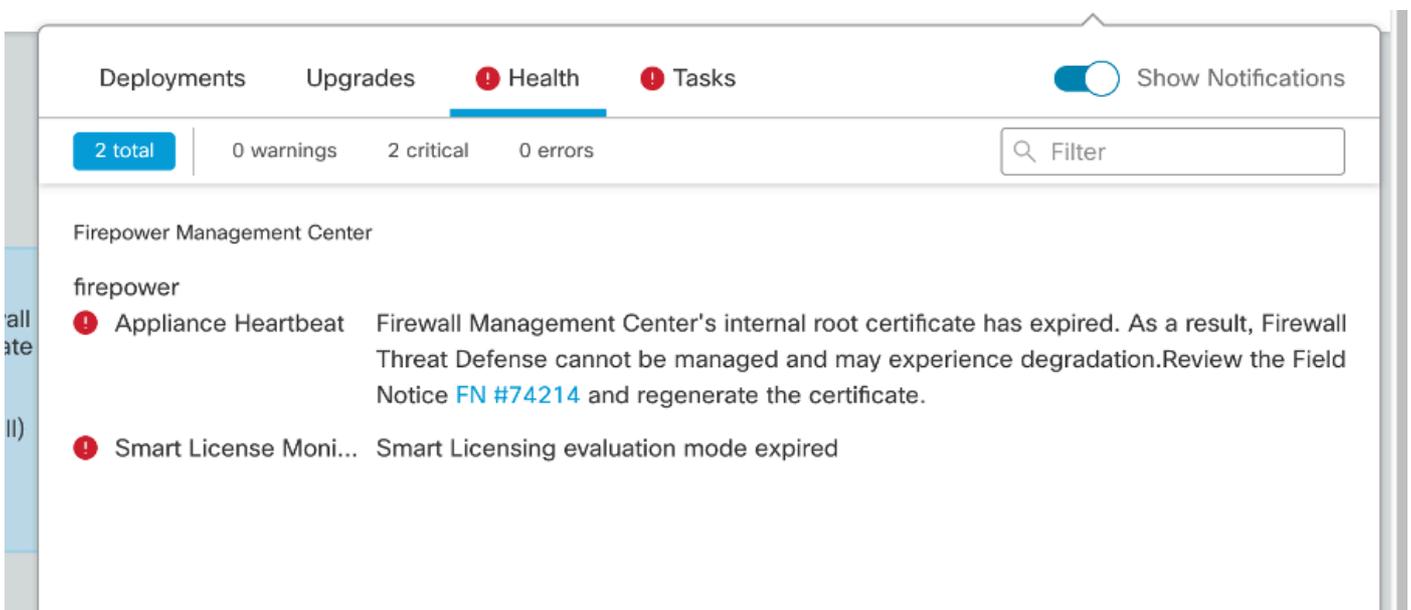
Die erste Methode wird über die Registerkarte Task ausgeführt. Diese Nachricht ist klebrig und für den Benutzer verfügbar, es sei denn, sie wird explizit geschlossen. Das Benachrichtigungs-Popup wird ebenfalls angezeigt und steht zur Verfügung, bis es vom Benutzer explizit geschlossen wird. Es wird immer als Fehler angezeigt.

The screenshot shows the 'Tasks' tab in the FMC web 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.'

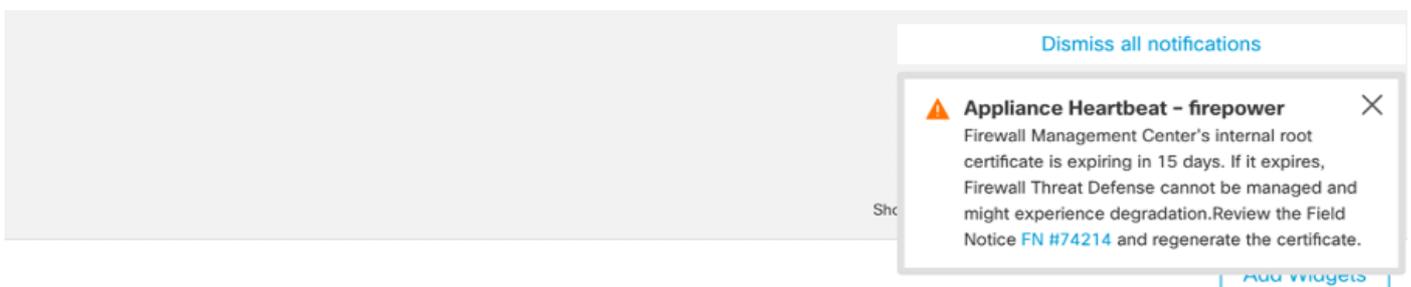
Ablaufbenachrichtigung auf Registerkarte "Vorgang"



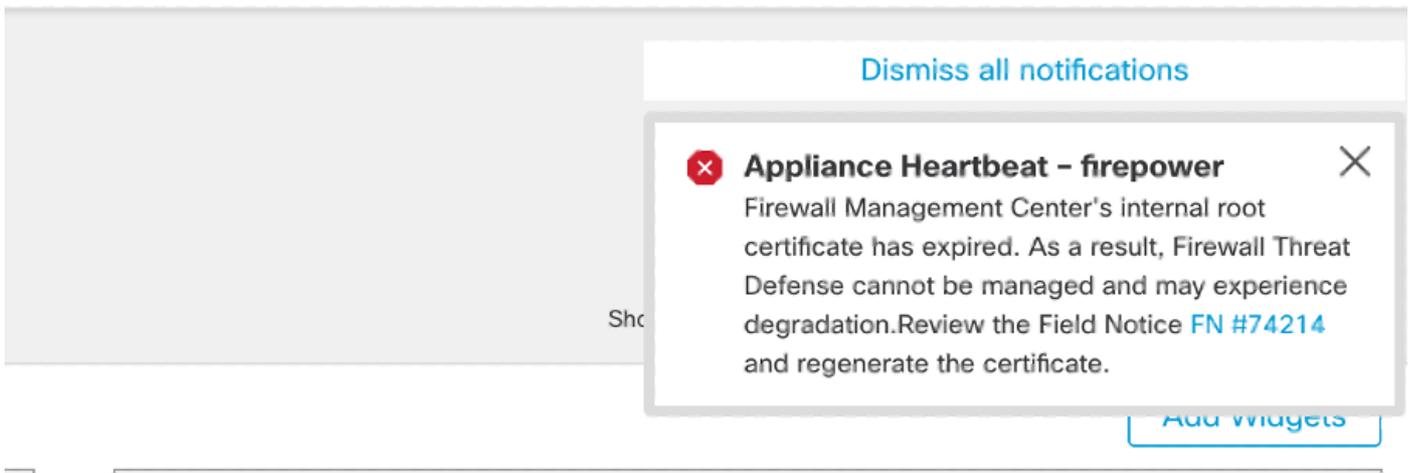
Die zweite Methode ist der Integritätsalarm. Dies wird auf der Registerkarte "Status" angezeigt, ist jedoch nicht haftbar und wird ersetzt oder entfernt, wenn der Integritätsmonitor ausgeführt wird, der standardmäßig alle 5 Minuten ausgeführt wird. Es wird auch ein Benachrichtigungs-Popup angezeigt, das vom Benutzer explizit geschlossen werden muss. Dies kann sowohl als Fehler (wenn abgelaufen) als Warnung (wenn abläuft) angezeigt werden.



Ablaufbenachrichtigung auf der Registerkarte "Status"



Warnmeldung bei Warnmeldung



Fehlerbenachrichtigung bei Systemwarnung wird angezeigt

Lösung 1 - Zertifikat ist noch nicht abgelaufen (ideales Szenario)

Dies ist die beste Situation, da wir dann je nach Ablauf des Zertifikats noch Zeit haben. Entweder verfolgen wir den vollständig automatisierten Ansatz (empfohlen), der von der FMC-Version abhängt, oder wir verfolgen einen manuellere Ansatz, der eine Interaktion mit dem TAC erfordert.

Empfohlener Ansatz

Dies ist die Situation, in der unter normalen Umständen keine Ausfallzeiten und ein geringster manueller Arbeitsaufwand zu erwarten sind.

Bevor Sie fortfahren, müssen Sie den [Hotfix](#) für Ihre spezielle Version wie hier aufgeführt installieren. Der Vorteil dabei ist, dass diese Hotfixes keinen Neustart des FMC und damit keine potenzielle unterbrochene Sftunnel-Kommunikation erfordern, wenn das Zertifikat bereits abgelaufen ist. Folgende Hotfixes stehen zur Verfügung:

- [7.0.0 - 7.0.6](#) : Hotfix FK - 7.0.6.99-9
- 7.1.x: keine feste Version als Ende der Softwarewartung
- [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

Nach der Installation des Hotfix sollte das FMC nun das Skript `generate_certs.pl` enthalten, das:

1. Regeneriert die interne Zertifizierungsstelle
2. Erstellt die von dieser neuen internen CA signierten Sftunnel-Zertifikate neu
3. Übergibt die neuen Sftunnel-Zertifikate und privaten Schlüssel an die entsprechenden FTD-Geräte (wenn der Sftunnel betriebsbereit ist)

Daher wird (wenn möglich) empfohlen:

1. Installieren Sie den entsprechenden Hotfix oben.

2. Sicherung auf dem FMC durchführen
3. Validieren Sie alle aktuellen sftunnel-Verbindungen mit dem Skript sftunnel_status.pl auf dem FMC (aus dem Expert-Modus).
4. Das Skript im Expertenmodus mit generate_certs.pl ausführen
5. Überprüfen Sie das Ergebnis, um festzustellen, ob manuelle Vorgänge erforderlich sind (wenn die Geräte nicht mit dem FMC verbunden sind) [weiter unten erläutert].
6. Führen Sie sftunnel_status.pl vom FMC aus, um zu überprüfen, ob alle Sftunnel-Verbindungen ordnungsgemäß ausgeführt werden.

```
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#
```

Generate_certs.pl-Skript



Anmerkung: Wenn FMC in Hochverfügbarkeit (HA) ausgeführt wird, müssen Sie den Vorgang zuerst auf dem primären Knoten und dann auf dem sekundären Knoten durchführen, da dieser diese Zertifikate ebenfalls für die Kommunikation zwischen den FMC-Knoten verwendet. Die interne Zertifizierungsstelle auf beiden FMC-Knoten ist unterschiedlich.

Im Beispiel hier sehen Sie, dass es eine Protokolldatei auf `/var/log/sf/sfca_generation.log` erstellt, angibt, `sftunnel_status.pl` zu verwenden, die Ablaufzeit auf der `InternalCA` angibt und angibt, ob Fehler aufgetreten sind. In diesem Fall konnten die Zertifikate beispielsweise nicht an das Gerät `BSNS-1120-1` und `EMEA-FPR3110-08` übertragen werden. Dies ist zu erwarten, da der Sftunnel für diese Geräte ausgefallen war.

Um den Sftunnel für die fehlerhaften Verbindungen zu korrigieren, führen Sie die folgenden Schritte aus:

- Öffnen Sie in der FMC-CLI die Datei FAILED_PUSH mit cat
/var/tmp/certs/1728303362/FAILED_PUSH (der Wert für die Zahl steht für die Unix-Zeit, überprüfen Sie also die Ausgabe des vorherigen Befehls in Ihrem System), die das nächste Format hat: FTD_UUID FTD_NAME FTD_IP QUELLE_Pfad_ON_FMC ZIELPFAD_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/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_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/certs_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/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807d77/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-fd927e807d77/certs_pushed//sftunnel-cert.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
root@fmcv72-stejanss:/Volume/home/admin#

```

FEHLGESCHLAGENER_PUSH

- Übertragung der neuen Zertifikate (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) vom FMC auf die FTD-Geräte
===Automatischer Ansatz===

Die Hotfix-Installation stellt außerdem die Skripte copy_sftunnel_certs.py und copy_sftunnel_certs_jumpserver.py bereit, die die Übertragung der verschiedenen Zertifikate auf Systeme automatisieren, für die der Sftunnel nicht aktiv war, während die Zertifikate neu generiert wurden. Dies kann auch für Systeme verwendet werden, bei denen die Verbindung zum SFTP-Tunnel unterbrochen wurde, da das Zertifikat bereits abgelaufen ist.

Sie können das Skript copy_sftunnel_certs.py verwenden, wenn das FMC selbst SSH-Zugriff auf die verschiedenen FTD-Systeme hat. Ist dies nicht der Fall, können Sie das Skript (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) vom FMC auf einen Jump-Server herunterladen, der SSH-Zugriff auf die FMC(s) und FTD-Geräte hat, und von dort aus das Python-Skript ausführen. Wenn dies ebenfalls nicht möglich ist, schlagen Sie vor, den als Nächstes dargestellten manuellen Ansatz auszuführen. In den folgenden Beispielen wird das verwendete Skript copy_sftunnel_certs.py veranschaulicht. Die Schritte sind jedoch für das Skript copy_sftunnel_certs_jumpserver.py identisch.

A. Erstellen Sie eine CSV-Datei auf dem FMC (oder Jump-Server), die die Geräteinformationen (Gerätename, IP-Adresse, admin_username, admin_password) enthält, die für die Herstellung der SSH-Verbindung verwendet werden.

Wenn Sie dies von einem Remote-Server ausführen, z. B. einem Jump-Server für das primäre FMC, stellen Sie sicher, dass Sie die primären FMC-Details als ersten Eintrag gefolgt von allen verwalteten FTD- und sekundären FMC-Daten hinzufügen. Wenn Sie dies von einem Remote-Server aus ausführen, z. B. einem Jump-Server für das sekundäre FMC, stellen Sie sicher, dass Sie die Details des sekundären FMC als ersten Eintrag gefolgt von


```
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

===Manueller Ansatz===

1. Drucken (cat) Sie die Ausgabe jeder Datei für jede betroffene FTD (cacert.pem / sftunnel-key.pem (nicht vollständig aus Sicherheitsgründen dargestellt) / sftunnel-cert.pem) auf der FMC-CLI, indem Sie den Dateispeicherort aus der vorherigen Ausgabe (FAILED_PUSH-Datei) kopieren.

```
root@fmcv72-stejanss:/Volume/home/admin# cat /etc/sf/ca_root/cacert.pem
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwYcxEzARBgNVBAwMck1udGVybmfS
Q0ExJDAiBgNVBAsMG0ludHJ1c2lubiBNYW5hZ2VtZW50IFN5c3R1bTEtMCsGA1UE
AwwkY2RiMTIzYzgtNDM0Ny0xMwVmlWFjYTEtZjNhYTI0MTQxMmExMRswGQYDVQK
DBJDaXNjbyBTeXN0ZW1zLkCBJmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy
MzI4WjCBhZETMBEGA1UEDAwKSW50ZXJlYXN0ZXQTEkMCIGA1UECwwbSW50cnVzaW9u
IE1hbmFnZW11bnQGU3lzdGVtMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYt
YWNhMS1mM2FhMjQxNDEyYTEXGzAZBgNVBAoMEkNpc2NvIFN5c3R1bXMsIEluYzCC
ASIWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMmUav8kVukF
xiV917W4d7/CYBb4pd1KiM0iJAep3wqxdpDUQ4KBDWnC5+p8dg+XK7Asp0W36CD
mdpRwRfqM7J51tXEUyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6VlQl+aRlAPCF
7UYpMgFPh3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXnL6Jn3rfoKbF0M77
xUtMeC0504buhfzSl+Am5J0bFuXMcPYq1N+t137r1/1etwHzmjVke7g/rfNv0y0
N+4m8i5QRN0BoghtZ0+Y/PudToSX0VmKh5Sq/i1MvOYBZEIM3Dx+Gb/DQYBWLUC
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAY2EVhEoylDdlWSu2ewdehthBtI6Q5x7e
UD187bbowmTJsd100LVGgYoU5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6
J3Q1F3hJJF0qSrIx/ST72jgL2o87ixhRIzreB/+26rHo5nns2r2tFss61KBltWN
nRZnSIYAwYhqGCjH9quiZpFDJ3N83oREGX+xfLYqFim5h3rFwk0J2q6YtaBJAuwg
0blDXGnrnWuIIV/xb0cwKbrALmtanhgGXyqT/pMYrjwLI1xVL16/PrMTV29WcQcA
IVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnstyGx8hlzRvzHz2w==
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

cacert.pem

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed/sftunn
el-key.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAQgSkAgEAAoIBAQCyc5A0xZ5N22qd
```

sftunnel-key.pem

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed/sftunn
el-cert.pem
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIBD0TANBgkqhkiG9w0BAQsFADCBhZETMBEGA1UEDAwKSW50
ZXJlYXN0ZXQTEkMCIGA1UECwwbSW50cnVzaW9uIE1hbmFnZW11bnQGU3lzdGVtMS0w
KwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYtYWNhMS1mM2FhMjQxNDEyYTEXGzAZ
BgNVBAoMEkNpc2NvIFN5c3R1bXMsIEluYzAeFw0yNDEwMTQyMzI4WhcNMzQxMDEy
MTQyMzI4WjCBhZETMBEGA1UECwwbSW50cnVzaW9uIE1hbmFnZW11bnQGU3lzdGVt
SWSjMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYtYTk5My1iOTgzMTU2NWJj
NGUxETAPBgNVBwMCHNmdHVubmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAE3MuQNMWetdtqg2k52FKHY2dQJEHc0mdUc/Y0KniUUA45iAdLbv0X819y
lQFPFdlurv4mYxgDoBDcZozLLiRBeaXcZnowoqmatv0MtMyL0TINTL+5G/KiyCr
gsz2ub03avXW/cbC2WZQGat0kQ/4Fb+LC5dnX2KA5H7m1rs0WNWEKFSpn/Y2UYGb
Zdi3bZz5wy5YHGFGQ8KK04v4mksSu02b+AWfIgoe1EaSwv5K+Wa0ssj6keaCkYfA
TP1sEiYkytFdE0F2s8mXFSfLbK+8hI+jWqAN/Q0a3D9gHD8gErrPHgLD8m30Tqp8s
kRF5JEI5UHhwlVt0FKbhWEW06906QIDAQABo0IwQDAJBgNVHRMEAjAAMBQGA1Ud
EQQNMauCCWxvY2FsaG9zdDAdBgNVHSUEFjAUBgggrBgEFBQcDAgYIKwYBBQUHAEw
DQYJKoZIhvcNAQELBQADggEBAHHAjwZHXG1nA+jAxGIaL6T/L2oYCDxuB3tcNKW
ZViILv110cUNYIvC/w7JbKlLUTLbit0aH01ff4Lcv0q6uk+SL7cAuAICXodP1EQo
ERz4E13a0MNNnvi5dt/a2fhIxzimhIq7P3zTMuKknVyblg0RqG7q8SxyEL5AT8Iy
beuhcg6+7LzCiw29/pTzCnycIrzBhBVK2ZcQ9vYtBXdCaZGK17lnYiEpk4Qi fne
9A2tQqecypKRRASd60uttEmVvpHCgMtGrC60Kb5h5SP00Ze1rGWD0V9eTj1NjIs0
+J+WXE06VApI17aYKXXhHLGF7n+esy1GaZ3Djn44mMkn8I=
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

sftunnel-cert.pem

2. Öffnen Sie die FTD-CLI der jeweiligen FTD im Expertenmodus mit Root-Berechtigungen über sudo su, und erneuern Sie die Zertifikate mit dem nächsten Verfahren.

1. Navigieren Sie zu dem Ort, der an dem hellblauen Markierungszeichen aus der Ausgabe FAILED_PUSH angezeigt wird (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1, hier zum Beispiel, aber dies ist für jede FTD anders).
2. Sichern der vorhandenen Dateien

```
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
```

Sicherungen der aktuellen Zertifikate übernehmen

3. Leere die Dateien, damit wir neue Inhalte schreiben können.

```
> 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#
```

Leerer Inhalt von vorhandenen Zertifikatsdateien

4. Schreiben Sie den neuen Inhalt (aus der FMC-Ausgabe) in jede der Dateien einzeln mit vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (separater Befehl pro Datei - Screenshots zeigen dies nur für cacert.pem, muss aber für


```

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#

```

Alle Zertifikatsdateien wurden mit Rechteinhabern und Berechtigungen aktualisiert.

3. Starten Sie den Sftunnel auf jedem FTD neu, wenn der Sftunnel nicht betriebsbereit war, damit die Änderungen im Zertifikat mit dem Befehl wirksam werden. `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. Überprüfen Sie jetzt mit der Ausgabe von `sftunnel_status.pl`, ob alle FTDs korrekt angeschlossen sind.

Lösung 2 - Zertifikat ist bereits abgelaufen

In dieser Situation haben wir zwei verschiedene Szenarien. Entweder sind alle Tunnelverbindungen noch nicht (oder nur teilweise) funktionsfähig.

FTDs weiterhin über Sftunnel verbunden

Wir können das gleiche Verfahren anwenden, wie im [Zertifikat](#) angegeben ist noch nicht abgelaufen (ideales Szenario) - Empfohlener Ansatz Abschnitt.

Führen Sie in diesem Fall jedoch KEIN Upgrade oder Neustart des FMC (oder eines FTD) durch, da es die Verbindung mit allen Sftunnel-Verbindungen unterbricht und alle Zertifikats-Updates manuell auf jedem FTD ausgeführt werden müssen. Die einzige Ausnahme sind die aufgeführten Hotfix-Versionen, da sie keinen Neustart des FMC erfordern.

Die Tunnel bleiben verbunden und die Zertifikate werden auf jedem FTD ersetzt. Falls einige Zertifikate nicht ausgefüllt werden können, werden die fehlerhaften Zertifikate angezeigt, und Sie müssen den [manuellen Ansatz](#) wie im vorherigen Abschnitt beschrieben anwenden.

FTDs nicht mehr über Sftunnel verbunden

Empfohlener Ansatz

Wir können das gleiche Verfahren anwenden, wie im [Zertifikat](#) angegeben [ist noch nicht abgelaufen \(ideales Szenario\) - Empfohlener Ansatz](#) Abschnitt. In diesem Szenario wird das neue Zertifikat auf dem FMC generiert, kann jedoch nicht auf die Geräte kopiert werden, da der Tunnel bereits ausgefallen ist. Dieser Prozess kann mit den Skripten [copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py](#) automatisiert werden.

Wenn alle FTD-Geräte vom FMC getrennt sind, können wir das FMC in diesem Fall aktualisieren, da dies keine Auswirkungen auf die Softunnel-Verbindungen hat. Wenn Sie noch einige Geräte über sftunnel verbunden haben, dann beachten Sie, dass das Upgrade des FMC alle sftunnel-Verbindungen schließt und sie nicht wieder kommen, weil das Zertifikat abgelaufen ist. Der Vorteil des Upgrades besteht darin, dass es Ihnen eine gute Anleitung für die Zertifikatsdateien bietet, die auf die einzelnen FTDs übertragen werden müssen.

Manueller Ansatz

In dieser Situation können Sie dann das Skript generate_certs.pl vom FMC ausführen, das die neuen Zertifikate generiert, Sie müssen sie jedoch [manuell](#) auf jedes FTD-Gerät übertragen. Je nach Anzahl der Geräte ist dies machbar oder kann eine mühsame Aufgabe sein. Bei Verwendung der Skripte [copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py](#) ist dies jedoch hochautomatisiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.