Verlenging van FMC Sftunnel CA-certificaat voor FTD-connectiviteit

Inhoud

Inleiding

In dit document wordt de verlenging beschreven van het certificaat van de Firepower Management Center (FMC) Sftunnel Certificate Authority (CA) in relatie tot de FTD-connectiviteit (Firepower Threat Defence).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

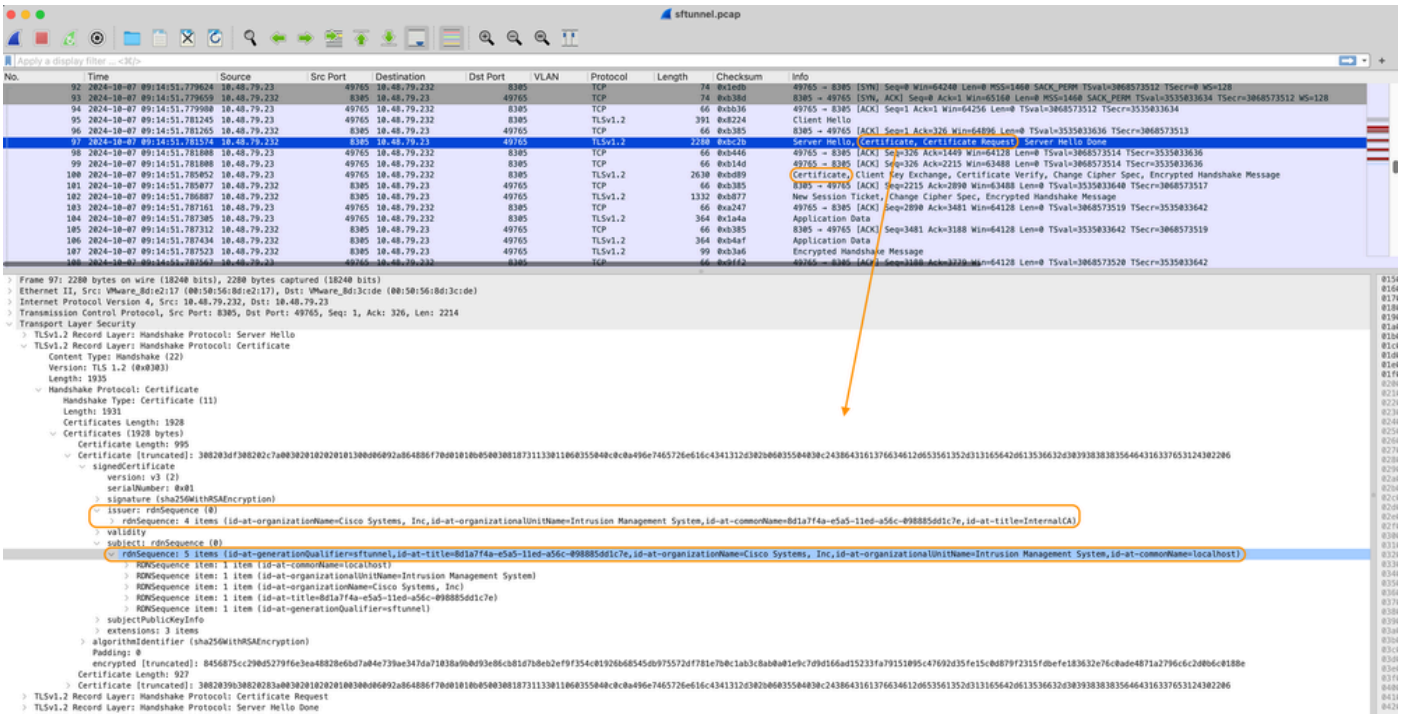
Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

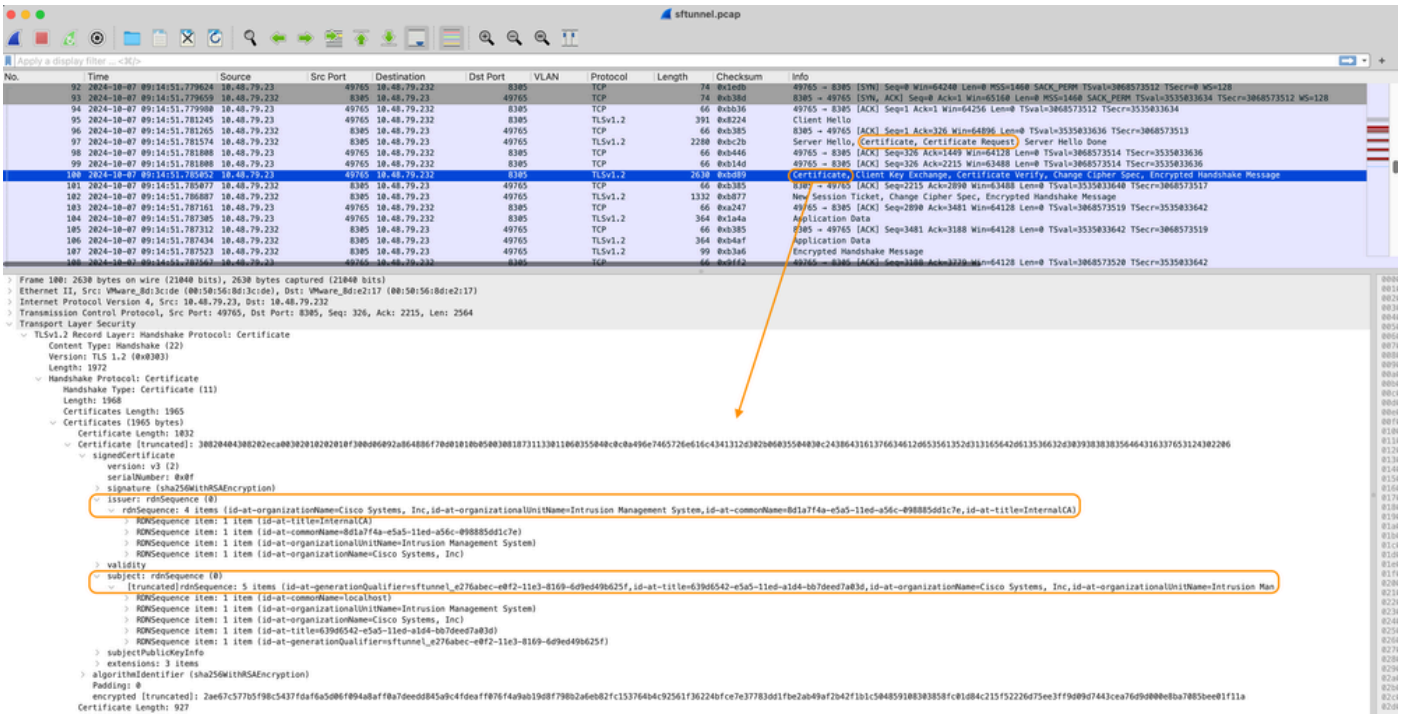
Achtergrondinformatie

FMC en FTD communiceren met elkaar via sftunnel (Sourcefire-tunnel). Deze communicatie maakt gebruik van certificaten om het gesprek veilig te maken via een TLS-sessie. Meer informatie over de sftunnel en hoe deze zich heeft gevestigd, vindt u op deze link.

Uit de pakketopname kunt u zien dat de FMC (10.48.79.232 in dit voorbeeld) en FTD (10.48.79.23) certificaten met elkaar uitwisselen. Ze doen dit om te controleren of ze met het juiste apparaat praten en er geen afluisterapparatuur of Man-In-The-Middle (MITM)-aanval is. De communicatie wordt versleuteld met die certificaten en alleen de partij die de bijbehorende privésleutel voor dat certificaat heeft, kan het opnieuw ontsleutelen.



Certificate_exchange_server_cert



Certificate_exchange_client_cert

U kunt zien dat de certificaten worden ondertekend door dezelfde Interne certificeringsinstantie (CA) die is ingesteld op het VCC. De configuratie is gedefinieerd in het FMC op /etc/sf/sftunnel.conf bestand dat zoiets bevat als:

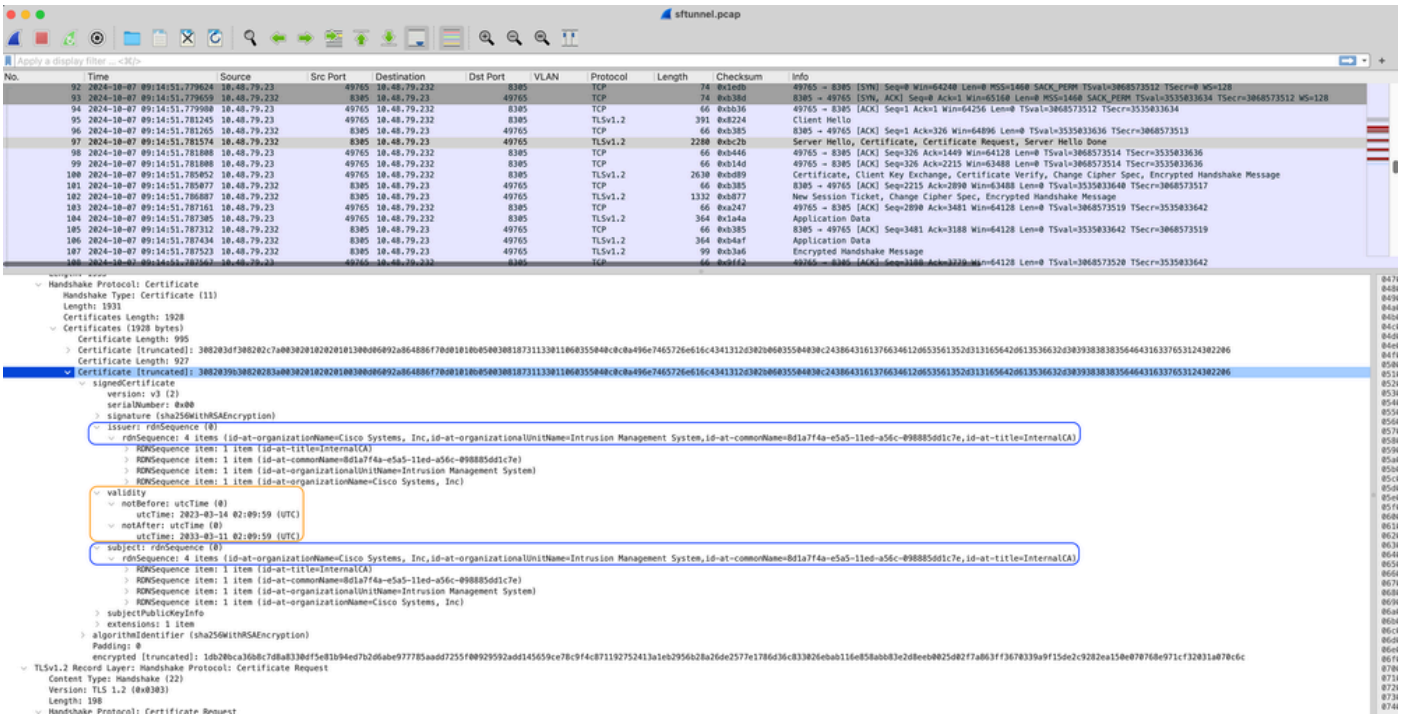
```
proxyssl {
  proxy_cert   /etc/sf/keys/sftunnel-cert.pem;              ---> Certificate provided by FMC to FTD f
  proxy_key    /etc/sf/keys/sftunnel-key.pem;
  proxy_cacert /etc/sf/ca_root/cacert.pem;                  ---> CA certificate (InternalCA)
  proxy_crl    /etc/sf/ca_root/crl.pem;
  proxy_cipher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

Dit geeft de CA aan die wordt gebruikt voor de ondertekening van alle certificaten voor de sftunnel (zowel het FTD als het FMC) en het certificaat dat door het FMC wordt gebruikt om alle FTD's toe te zenden. Dit certificaat is ondertekend door de Interne CA.

Wanneer het FTD zich bij het FMC registreert, stelt het FMC tevens een certificaat op om het FTD-apparaat te activeren dat wordt gebruikt voor de verdere communicatie over de sftunnel. Dit certificaat wordt ook ondertekend door hetzelfde interne CA-certificaat. Op FMC, kunt u dat certificaat (en privé sleutel) onder /var/sf/peers/<UUID-FTD-device> en mogelijk onder certs_pushed map vinden en heet sftunnel-cert.pem (sftunnel-key.pem voor private sleutel). Op FTD kunt u de bestanden onder /var/sf/peers/<UID-FMC-device> met dezelfde naamgevingsconventie vinden.

Elk certificaat heeft echter ook een geldigheidstermijn voor veiligheidsdoeleinden. Bij de inspectie van het certificaat van InternCA zien we ook de geldigheidsperiode van 10 jaar voor het VCC

InternCA, zoals blijkt uit de pakketvastlegging.

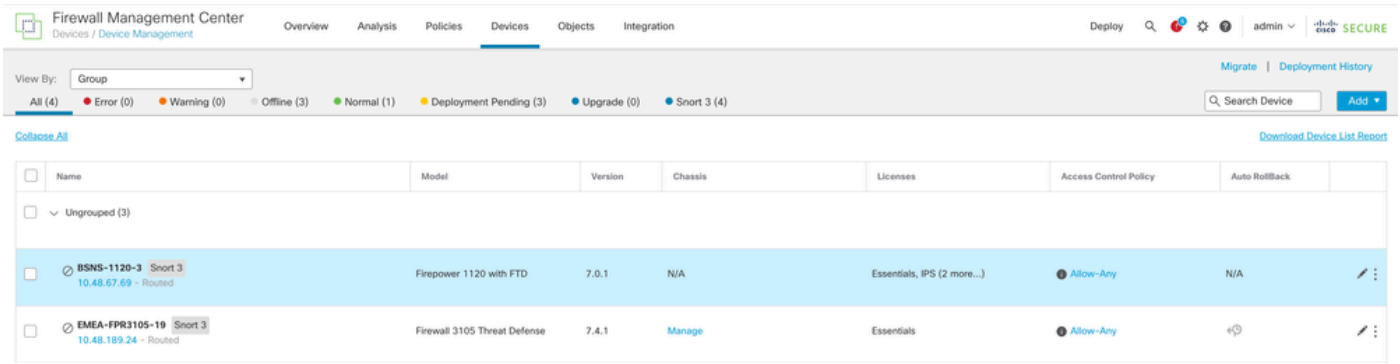


FMC-InternalCA_validiteit

Probleem

Het interne certificaat van het VCC is slechts 10 jaar geldig. Na de vervaltijd vertrouwt het systeem op afstand dit certificaat niet meer (evenals de door het systeem ondertekende certificaten) en dit leidt tot problemen met de sftunnelcommunicatie tussen FTD- en FMC-apparaten. Dit betekent ook dat verschillende belangrijke functionaliteiten zoals verbindingsgebeurtenissen, malware zoeken, op identiteit gebaseerde regels, beleidsimplementaties en vele andere dingen niet werken.

De apparaten verschijnen niet als uitgeschakeld op de FMC UI onder het tabblad Apparaten > Apparaatbeheer wanneer de sftunnel niet is verbonden. Het probleem dat betrekking heeft op deze vervaldatum, wordt getraceerd op Cisco-fout-id CSC08098. Houd er echter rekening mee dat alle systemen getroffen zijn, zelfs wanneer u een vaste release van het defect uitvoert. Meer informatie over deze oplossing vindt u in het gedeelte Oplossing.



Uitgeschakelde apparaten

Het VCC vernieuwt de CA niet automatisch en geeft de certificaten opnieuw uit aan de FTD-apparatuur. Er is ook geen gezondheidswaarschuwing van het VCC waaruit blijkt dat het certificaat vervalt. Cisco bug-id CSCwd08448 wordt in dit opzicht gevolgd om in de toekomst een gezondheidswaarschuwing voor de FMC UI te geven.

Wat gebeurt er na de vervaldatum?

Aanvankelijk gebeurt er niets en de communicatiekanalen voor de veilige tunnel blijven functioneren zoals voorheen. Wanneer echter de sftunnelcommunicatie tussen FMC en FTD-apparaten wordt verbroken en de verbinding opnieuw tot stand wordt gebracht, is het mislukt en kunt u logregels waarnemen op het berichtenlogbestand dat naar het verlopen van het certificaat wijst.

Loglijnen van FTD-apparaat van /ngfw/var/log/message:

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

Loglijnen van FMC-apparaat van /var/log/berichten:

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

De sftunnelcommunicatie kan om verschillende redenen worden verbroken:

- Communicatieverlies door verlies van netwerkconnectiviteit (potentieel slechts tijdelijk)
- Herstart van het FTD of het FMC
  - Verwachte: handmatige herstart, upgrades, handmatige herstart van sftunnelproces op FMC of FTD (bijvoorbeeld door pmtool restartbyid sftunnel)
  - Onverwachte: terugtracebacks, stroomuitval

Omdat er zo veel mogelijkheden zijn die de sftunnelcommunicatie kunnen doorbreken, is het zeer aan te raden om zo snel mogelijk op de situatie te corrigeren, zelfs wanneer momenteel alle FTD-apparaten goed zijn aangesloten ondanks het verlopen certificaat.

Hoe om snel te verifiëren als het certificaat is verlopen of wanneer het verloopt?

De gemakkelijkste manier is om deze opdrachten uit te voeren in de SSH-sessie van het FMC:

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

Dit toont u de Geldigheid elementen van het certificaat. Het belangrijkste relevante deel hier is de "notAfter", waaruit blijkt dat het certificaat hier geldig is tot 5 oktober 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
```

Niet meer na

Als u wilt dat er één opdracht wordt uitgevoerd die u onmiddellijk de hoeveelheid dagen geeft waarvoor het certificaat nog geldig is, kunt u dit gebruiken:

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

Er wordt een voorbeeld getoond van een installatie waarbij het certificaat nog meerdere jaren geldig is.

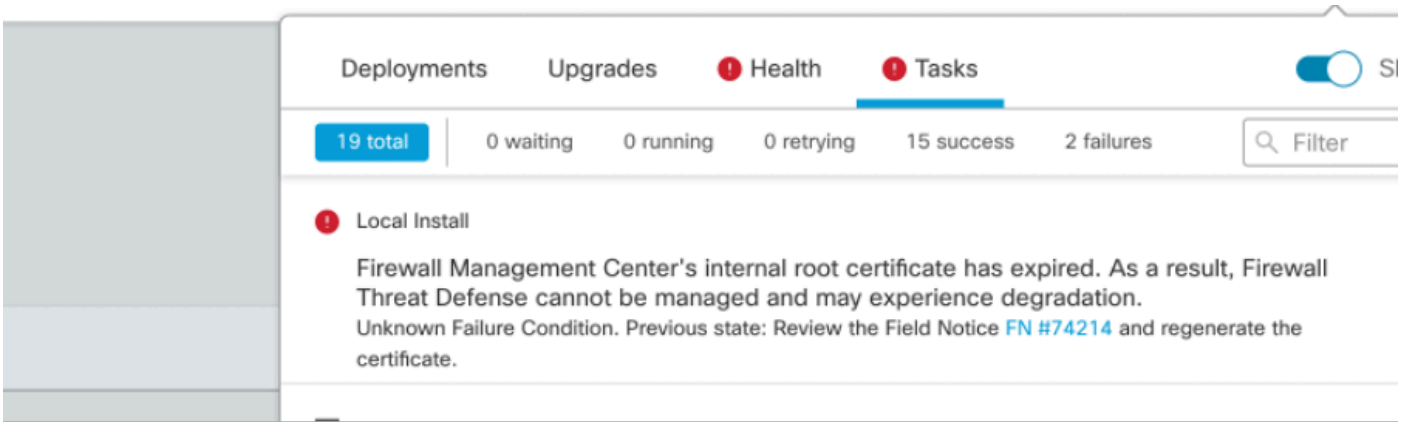
```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS + THIRTY_
DAYS_SECONDS)); DAYS_LEFT=$(( (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#
```

Certificaat_expiratie_opdracht

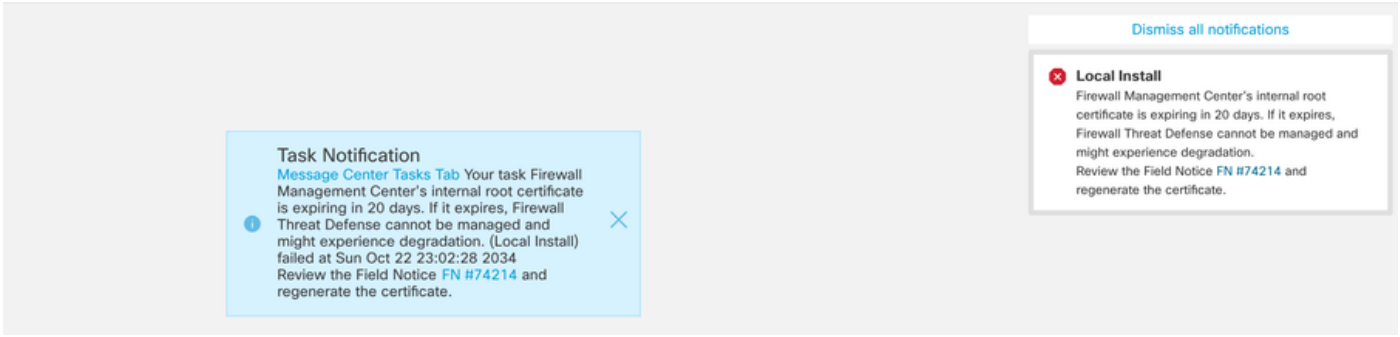
Hoe krijg ik in de toekomst bericht over een aanstaande certificaatvervaldatum?

Bij recente VDB-updates (399 of hoger) wordt u automatisch gewaarschuwd wanneer uw certificaat binnen 90 dagen vervalt. Daarom hoeft u dit niet zelf handmatig bij te houden, aangezien u wordt gewaarschuwd wanneer u dicht bij de vervaltijd bent. Dit verschijnt dan op de FMC-webpagina in twee vormen. Beide manieren verwijzen naar de pagina van de gebiedsbericht.

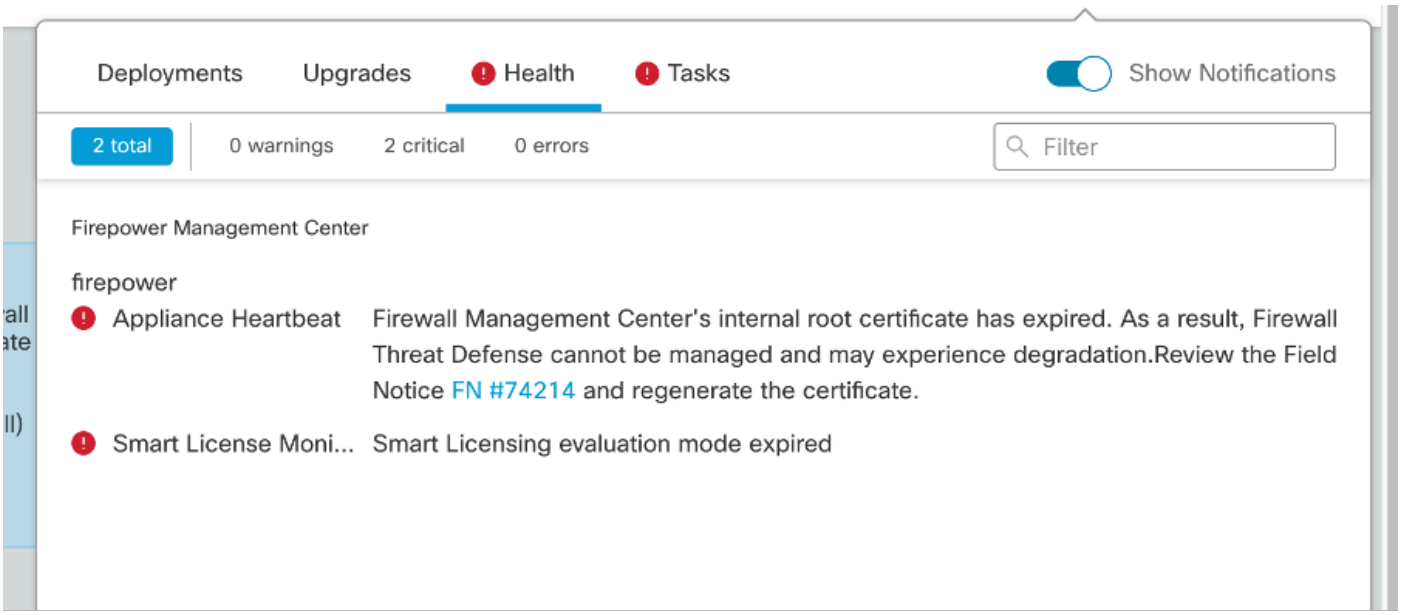
De eerste methode is via het tabblad Taak. Dit bericht is plakkerig en beschikbaar voor de gebruiker tenzij expliciet gesloten. Het melding pop-up verschijnt ook en is beschikbaar tot expliciet gesloten door de gebruiker. Het verschijnt altijd als een fout.



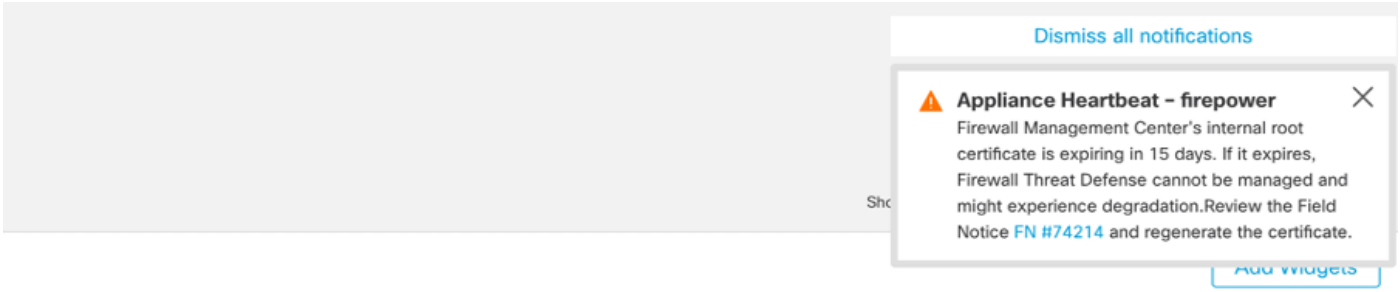
Melding bij afloop van taak tabblad



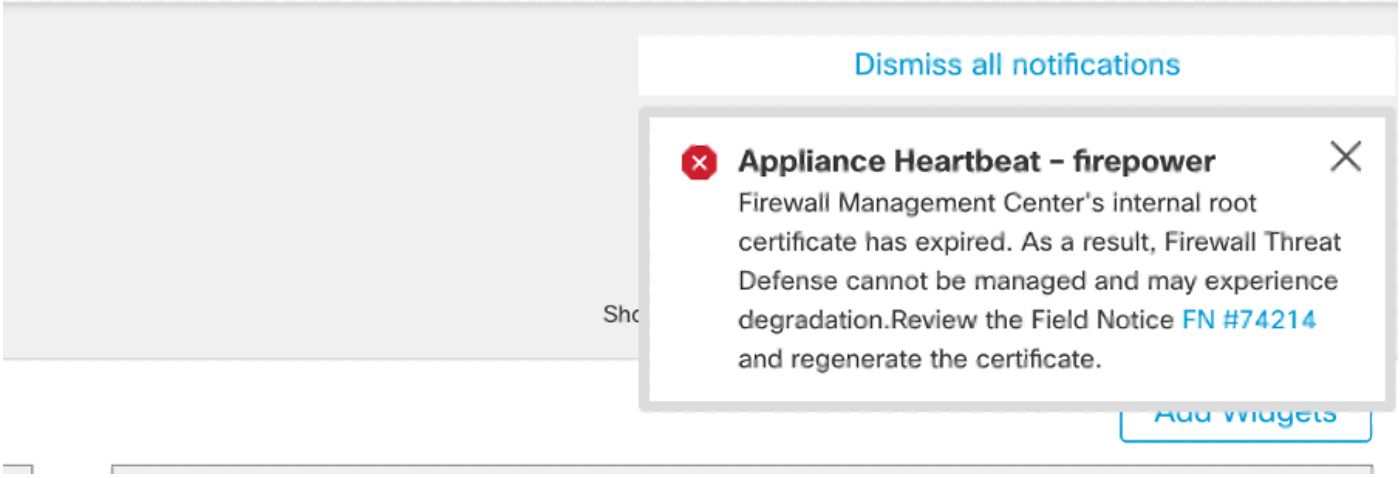
De tweede methode is via Health Alert. Dit verschijnt in het tabblad Gezondheid, maar dit is niet kleverig en vervangt of verwijdert als de gezondheidsmonitor wordt uitgevoerd, wat standaard elke 5 minuten is. Het toont ook een melding pop-up die expliciet door de gebruiker moet worden gesloten. Dit kan zowel als fout (wanneer verlopen) als waarschuwing (wanneer het verlopen is) weergeven.



Bericht bij verlopen op het tabblad Gezondheid



Waarschuwingsmelding bij pop-up van gezondheidswaarschuwing



Foutmelding bij pop-up van gezondheidswaarschuwing

Oplossing 1 - Het certificaat is nog niet verlopen (ideaal scenario)

Dit is de beste situatie omdat we, afhankelijk van het verstrijken van het certificaat, nog tijd hebben. Ofwel kiezen we voor de volledig geautomatiseerde aanpak (aanbevolen) die afhankelijk is van de FMC-versie, ofwel kiezen we voor een meer handmatige aanpak die TAC-interactie vereist.

Aanbevolen aanpak

Dit is de situatie waarin onder normale omstandigheden geen uitvaltijd en de minste hoeveelheid handmatige handelingen wordt verwacht.

Alvorens verder te gaan, moet u de hotfix voor uw bepaalde versie installeren zoals hier vermeld. Het voordeel is dat deze hotfixes geen reboot van het VCC en dus potentiële kapotte sftunnelcommunicatie vereisen wanneer het certificaat al is verlopen. De beschikbare hotfixes zijn:

- 7.0.0-7.0.6 : Hotfix FK - 7.0.6.99-9
- 7.1.x. : geen vaste release als einde van softwareonderhoud
- 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

Zodra de hotfix is geïnstalleerd, moet het VCC nu het script generation_certs.pl bevatten dat:

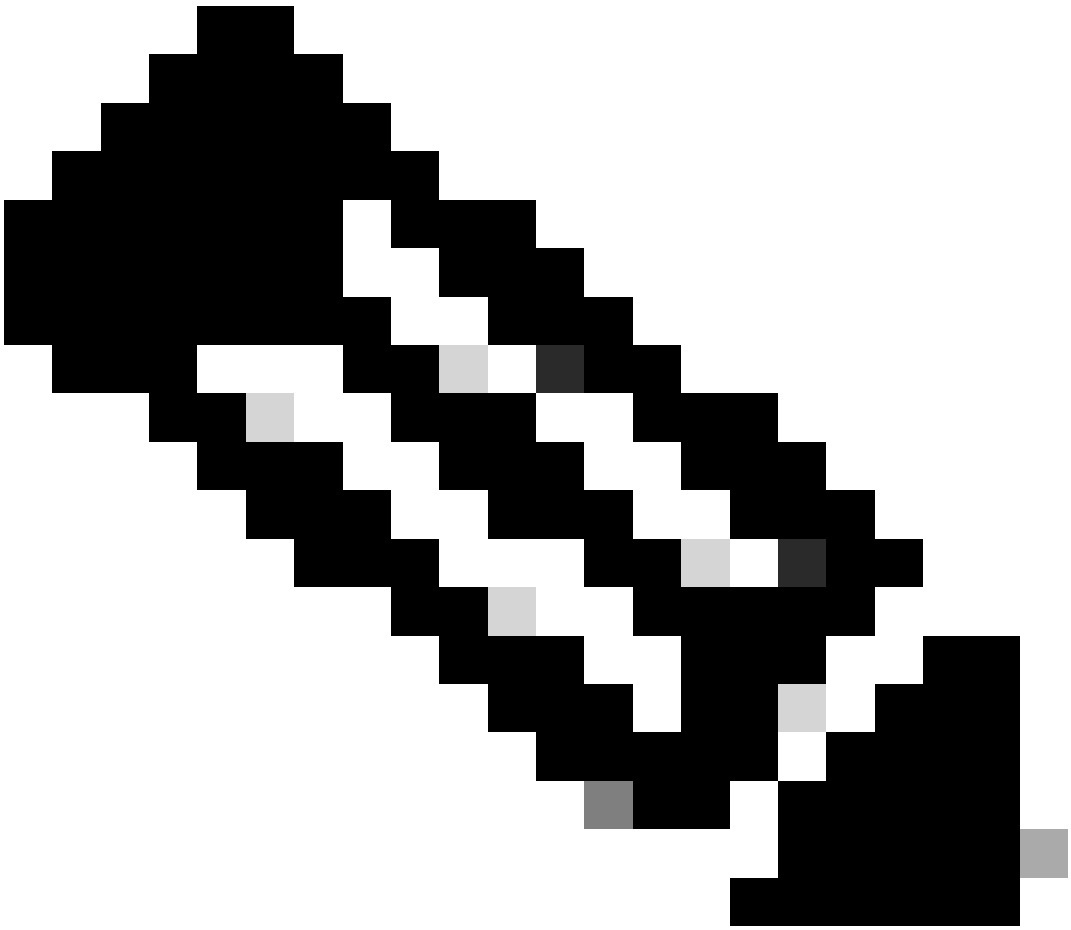
1. Hiermee wordt de interne CA hersteld
2. Herstelt de sftunnelcertificaten die zijn ondertekend door dit nieuwe InternalCA
3. Duw de nieuwe sftunnelcertificaten en privésleutels over naar de respectieve FTD-apparaten (wanneer de sftunnel operationeel is)

Daarom wordt aanbevolen (indien mogelijk):

1. Installeer de toepasselijke hotfix hierboven
2. Maak een back-up op het VCC
3. Valideer alle huidige Sftunnelverbindingen met behulp van het script sftunnel_status.pl in het VCC (van expert mode)
4. Draai het script vanuit de expert mode met generation_certs.pl
5. Inspecteer het resultaat om te valideren of handmatige handelingen nodig zijn (wanneer de apparatuur niet met het VCC is verbonden) [zie verder hieronder]
6. Voer sftunnel_status.pl uit vanuit het VCC om te controleren of alle sftunnelverbindingen goed lopen

```
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 script

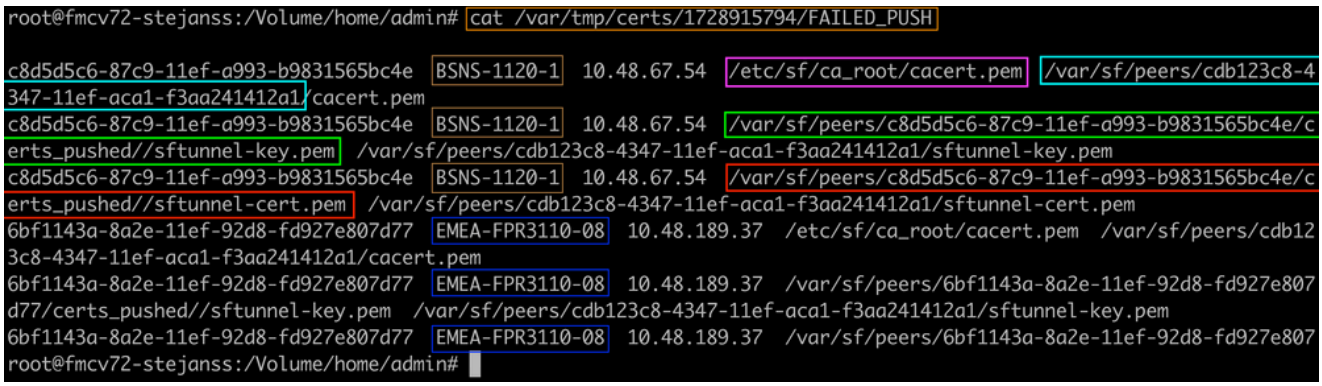


Opmerking: Wanneer FMC in High-Availability (HA) wordt uitgevoerd, moet u de handeling eerst op het primaire knooppunt uitvoeren en vervolgens op het secundaire knooppunt, aangezien het deze certificaten ook gebruikt om te communiceren tussen de FMC-knooppunten. De interne CA op beide FMC-knooppunten is verschillend.

In het voorbeeld hier ziet u dat het maakt een logbestand op /var/log/sf/sfca_generation.log, geeft aan sftunnel_status.pl te gebruiken, geeft de verlooptijd aan op de InternalCA en geeft aan of er fouten zijn opgetreden. Hier is het er bijvoorbeeld niet in geslaagd om de certificaten over te brengen naar apparaat BSNS-1120-1 en EMEA-FPR3110-08, wat wordt verwacht omdat de sftunnelbuis was neergehaald voor die apparaten.

U voert de volgende stappen uit om de tunnel voor de mislukte verbindingen te corrigeren:

1. Open op FMC CLI het bestand MISLUKTE_PUSH met cat /var/tmp/certs/1728303362/FAIL_PUSH (number value vertegenwoordigt unix time, dus controleer de uitvoer van de vorige opdracht in uw systeem) die het volgende formaat heeft: FTD_UID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINY_PATH_ON_FTD



MISLUKTE_DRUK

2. Overdracht van die nieuwe certificaten (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) van het FMC naar de FTD-apparaten
   ===Automatische nadering===

   De hotfix installatie biedt ook de scripts copy_sftunnel_certs.py en copy_sftunnel_certs_jumpserver.py die de overdracht van de verschillende certificaten naar systemen automatiseren waarvoor de sftunnel niet omhoog was terwijl de certificaten werden geregenereerd. Dit kan ook worden gebruikt voor systemen die een verbroken verbinding hadden omdat het certificaat al was verlopen.

   U kunt het script copy_sftunnel_certs.py gebruiken wanneer het FMC zelf SSH-toegang heeft tot de verschillende FTD-systemen. Als dat niet het geval is, kunt u het script

(/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) van het FMC downloaden naar een springserver die SSH-toegang heeft tot zowel het FMC (de FMC's) als de FTD-apparaten en het Python-script vanaf daar uitvoeren. Als dat ook niet mogelijk is, stel dan voor om de handmatige benadering uit te voeren die hieronder wordt getoond. De volgende voorbeelden tonen het script copy_sftunnel_certs.py dat gebruikt wordt, maar de stappen zijn hetzelfde voor het script copy_sftunnel_certs_jumpserver.py.

A. Maak een CSV-bestand op het FMC (of springserver) dat de apparaatinfo bevat (device_name, IP-adres, admin_username, admin_password) die gebruikt wordt om de SSH-verbinding te maken.

Wanneer u dit uitvoert vanaf een externe server zoals een springserver voor Primary FMC, zorg er dan voor dat u de primaire FMC-gegevens toevoegt als de eerste vermelding, gevolgd door alle beheerde FTD en secundaire FMC. Wanneer u dit uitvoert vanaf een externe server zoals een springserver voor secundair FMC, zorg er dan voor dat u de secundaire FMC-gegevens toevoegt als de eerste vermelding gevolgd door alle beheerde FTD.

i. Maak een bestand met vi devices.csv. 

vi-apparaten.csv

ii. Hiermee wordt het lege bestand geopend (niet weergegeven) en u vult de details in zoals weergegeven nadat u in de letter op het toetsenbord hebt gebruikt om naar de INTERACTIEVE modus te gaan (zie onder op het scherm).

devices.csv voorbeeld

iii. Als u klaar bent, sluit u het bestand en slaat u het op met behulp van ESC gevolgd door :wq en vervolgens ENTER.

De apparaten opslaan.csv

B. Start het script (vanaf root met behulp van sudo) met copy_sftunnel_certs.py devices.csv en het toont je het resultaat. Hier toont het aan dat het certificaat naar FTDv correct werd geduwd en dat voor BSNS-1120-1 het de verbinding van SSH met het apparaat niet kon maken.

```
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

===Handmatige nadering===

1. Druk (cat) de uitvoer van elk van de bestanden voor elke FTD beïnvloed (cacert.pem / sftunnel-key.pem (niet volledig getoond voor veiligheidsdoeleinden) / sftunnel-cert.pem) op de FMC CLI af door de bestandslocatie van de vorige uitvoer te kopiëren (ERROR_PUSH-bestand).

```
root@fmcv72-stejanss:/Volume/home/admin# cat /etc/sf/ca_root/cacert.pem
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwgYcxEzARBgNVBAwMCkludGVybmFs
Q0ExJDAiBgNVBAsMG0ludHJ1c2lvbiBNYW5hZ2VtZW50IFN5c3RlbTEtMCsGA1UE
AwwkY2RiMTIzYzgtNDM0Ny0xMWVmLWFjYTEtZjNhYTI0MTQxMmExMRswGQYDVQQK
DBJDaXNjbyBTeXN0ZW1zLCBJbmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy
MzI4WjCBhzETMBEGA1UEDAwKSW50ZXJuYWxDQTEkMCIGA1UECwwbSW50cnVzaW9u
IE1hbmFnZW1lbnQgU3lzdGVtMS0wKwYDVQQDDCRjZGIxMjNjOC00MzQ3LTExZWYt
YWNhMS1mM2FhMjQxNDEyYTExGzAZBgNVBAoMEkNpc2NvIFN5c3RlbXMsIEluYzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMmUav8kVukF
xiV917W4d7/CYBb4pd1KiMOijAEp3wqxmdpDUQ4KBDWnC5+p8dg+XK7AspOW36CD
mdpRwRfqM7J51txEUyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6VlQl+aRlAPCF
7UYpMgFPh3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXnL6Jn3rfoKbF0M77
xUtiMeC05O4buhfzSltAm5J0bFuXMcPYq1N+t137rl/1etwHzmjVkE7g/rfNv0yO
N+4m8i5QRN0BoghtZO+Y/PudToSX0VmKh5Sq/i1MvOYBZEIM3Dx+Gb/DQYBWLEUC
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAY2EVhEoylDdlWSu2ewdehthBtI6Q5x7e
UD187bbowmTJsdlOOLVGgYoU5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6
J3Q1F3hJJFOqSrlIx/ST72jgL2o87ixhRIzreB/+26rHo5nns2r2tFss61KBltWN
nRZnSIYAwYhqGCjH9quiZpfDJ3N83oREGX+xflYqFim5h3rFwk0J2q6YtaBJAuwg
0bldXGnrnWuIIV/xbOcwKbrALmtanhgGXyqT/pMYrjwlI1xVLl6/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//sftunnel-key.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDcy5A0xZ5N22qD
```

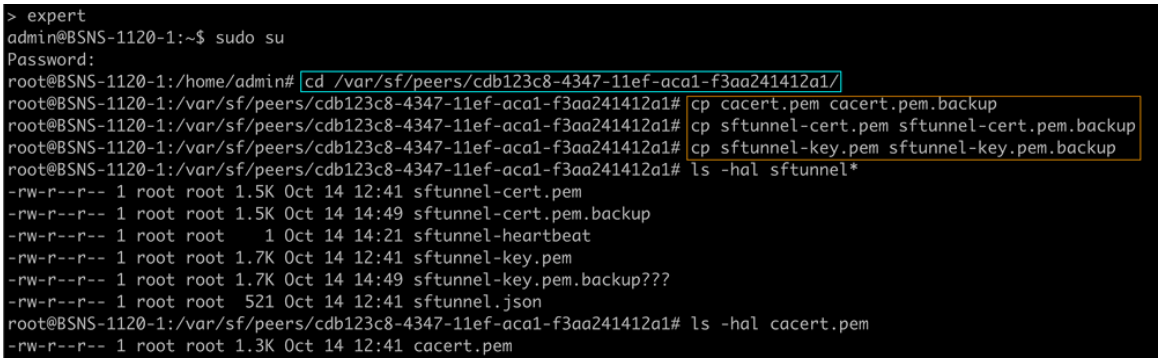
sftunnel-key.pem

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed//sftunnel-cert.pem
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIBDTANBgkqhkiG9w0BAQsFADCBhzETMBEGA1UEDAwKSW50
ZXJuYWxDQTEkMCIGA1UECwwbSW50cnVzaW9uIE1hbmFnZW1lbnQgU3lzdGVtMS0w
KwYDVQQDDCRjZGIxMjNjOC00MzQ3LTExZWYtYWNhMS1mM2FhMjQxNDEyYTExGzAZ
BgNVBAoMEkNpc2NvIFN5c3RlbXMsIEluYzAeFw0yNDEwMTMxNDIzMzFaFw0zNDEw
MTIxNDIzMzFaMIGZMRIwEAYDVQQDDAlsb2NhbGhvc3QxJDAiBgNVBAsMG0ludHJ1
c2lvbiBNYW5hZ2VtZW50IFN5c3RlbTEbMBkGA1UECgwSQ2lzY28gU3lzdGVtcywg
SW5jMS0wKwYDVQQMDCRjOGQ1ZDVjNi04N2M5LTExZWYtYTk5My1iOTgzMTU2NWJj
NGUxETAPBgNVBCwMCHNmdHVubmVsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA3MuQNMWeTdtqg2k52FKHY2dQJEHc0mdUc/YOKniUUa45iAdLBv0X8l9y
lQFPFdlurv4mYxgDoBDCzoZLLiRBeaaXcZnowoqmatvOMtMyL0ITNTL+5G/KiyCr
gsz2ub03avXW/cbC2WZQGat0kQ/4Fb+LC5dnX2KA5H7m1rsOWNWEKFspn/Y2UYGb
Zdi3bZz5wy5YHGGFQ8KKO4v4mksSu02b+AWfIgOe1EaSwv5K+Wa0ssj6keaCkYfA
TP1sEiYkytFdE0f2s8mXfSfLbK+8hI+jWqAN/QOa3D9gHD8gErPHgLDBm30Tqp8s
kRf5JEIsU5HHwlvT0FKbhWEW069O6QIDAQABo0IwQDAJBgNVHRMEAjAAMBQGA1Ud
EQQNMAuCCWxvY2FsaG9zdDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
DQYJKoZIhvcNAQELBQADggEBAAHHAjwZHXG1nA+jAxGIaL6T/L2oYCDxuB3tcNKW
ZViILv11OcUNYIvC/w7JbKllUTLbit0aH01ff4lcv0q6uk+SL7cAuAIcXodP1EQo
ERz4E13a0MNNnvi5dT/a2fhIxzimhIq7P3zTMuKknVyblg0RqG7q8SxyEL5AT8Iy
beuhcg6+7LZcIw29/pTzCnycIrzBhBVK2ZcQ9vYtBXxDCaZGK17lnYiEpK4Qifne
9A2tQQecypKRRA5d60uttEmVvpHCgMtGrC6OKb5h5SPO0Ze1rGWDoV9eTj1NJis0
+J+WXE06VApIl7aYKWXXhHLGF7n+esy1GaZ3Djn44mMkn8I=
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

sftunnel-cert.pem

2. Open FTD CLI van elke respectieve FTD op deskundige wijze met wortelvoorrechten door sudo su en vernieuw de certificaten met de volgende procedure.
    1. Blader naar de locatie op het lichtblauwe hoogtepunt van DE OUTPUT VAN FAILLIET_PUSH (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3a241412a1 hier bijvoorbeeld, maar dit is anders voor elke FTD).
    2. Maak een back-up van de bestaande bestanden.

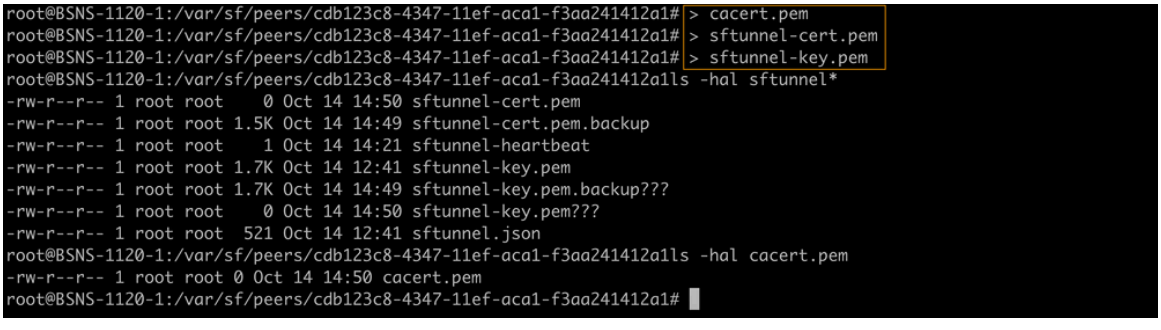
```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```



Maak een back-up van de huidige certificaten

    3. Leeg de bestanden zodat we nieuwe inhoud in ze kunnen schrijven.

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



Lege inhoud van bestaande certificaatbestanden

    4. Schrijf de nieuwe inhoud (van FMC-uitvoer) in elk van de bestanden afzonderlijk met behulp van vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (afzonderlijke opdracht per bestand - screenshots tonen dit alleen voor cacert.pem maar moet worden herhaald voor sftunnel-cert.pem en sftunnel-

key.pem).

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

vi cacert.pem

1. Druk op deze om in de interactieve modus te gaan (nadat de vi-opdracht is ingevoerd en u een leeg bestand ziet).
2. Kopieer de gehele inhoud (inclusief -----BEGIN CERTIFICAAT----- en -----END CERTIFICAAT-----) in het bestand.

Kopieert inhoud in vi (INSERT mode).

3. Sluit het bestand en schrijf naar het bestand met ESC gevolgd door :wq en voer het vervolgens in.

ESC gevolgd door :wq om naar bestand te schrijven

5. Bevestig dat de juiste rechten (chmod 644) en eigenaars (chown root:root) zijn ingesteld voor elk van de bestanden met ls -hal. Dit is correct ingesteld eigenlijk wanneer we het bestaande bestand updaten.

```
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 sfipproxy.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 certificaatbestanden bijgewerkt met de juiste eigenaars en machtigingen

3. Start de sftunnel opnieuw op elk FTD in het geval dat de sftunnel niet operationeel was, zodat de wijzigingen in het certificaat van kracht worden met de opdracht 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. Controleer of alle FTD's nu correct zijn aangesloten met behulp van sftunnel_status.pl uitvoer

Oplossing 2 - Het certificaat is al verlopen

In deze situatie hebben we twee verschillende scenario's. Ofwel alle tunnelverbindingen zijn nog steeds operationeel of ze zijn niet meer (of gedeeltelijk) operationeel.

FTD's nog steeds verbonden via sftunnel

We kunnen dezelfde procedure toepassen als aangegeven in het certificaat is nog niet verlopen (ideaal scenario) - Aanbevolen aanpak sectie.

Echter niet upgraden of opnieuw opstarten van het FMC (of een FTD) in deze situatie als het verbroken alle sftunnelverbindingen en we moeten alle certificaten updates handmatig uitvoeren op elk FTD. De enige uitzondering hierop zijn de vermelde Hotfix-releases, aangezien ze geen herstart van het VCC vereisen.

De tunnels blijven met elkaar verbonden en de certificaten worden op elk van de FTD's vervangen. In het geval dat sommige certificaten niet worden ingevuld, wordt u gevraagd om de certificaten die niet zijn ingevuld en moet u de handmatige aanpak te volgen zoals eerder aangegeven in de vorige sectie.

FTD's niet meer verbonden via sftunnel

Aanbevolen aanpak

We kunnen dezelfde procedure toepassen als aangegeven in het certificaat is nog niet verlopen (ideaal scenario) - Aanbevolen aanpak sectie. In dit scenario zal het nieuwe certificaat worden gegenereerd op het VCC, maar kan niet worden gekopieerd naar de apparatuur, aangezien de tunnel reeds is ingeklapt. Dit proces kan worden geautomatiseerd met de scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py

Indien alle FTD-apparatuur wordt losgekoppeld van het FMC, kunnen we het FMC in deze situatie verbeteren, aangezien het geen invloed heeft op de verbindingen in de sftunnels. Als u nog steeds bepaalde apparaten hebt aangesloten door sftunnel, dan moet u zich ervan bewust zijn dat de upgrade van de FMC alle sftunnelverbindingen sluit en ze komen niet weer boven als gevolg van het verlopen certificaat. Het voordeel van de upgrade hier zou zijn dat het geeft u een goede leidraad over de certificaatbestanden die moeten worden overgedragen naar elk van de FTD's.

Handmatige nadering

In deze situatie kunt u het script generation_certs.pl uitvoeren vanuit het FMC dat de nieuwe certificaten genereert, maar u moet ze nog steeds handmatig naar elk FTD-apparaat duwen. Afhankelijk van de hoeveelheid apparaten, is dit doenbaar of kan een vervelende taak zijn. Bij gebruik van de scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py is dit echter sterk geautomatiseerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.