# Renovação do certificado CA do FMC Sftunnel para conectividade do FTD

## Contents



## Introdução

Este documento descreve a renovação do certificado da CA (Certificate Authority, Autoridade de certificação) do túnel do Firepower Management Center (FMC) em relação à conectividade do Firepower Threat Defense (FTD).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### Componentes Utilizados

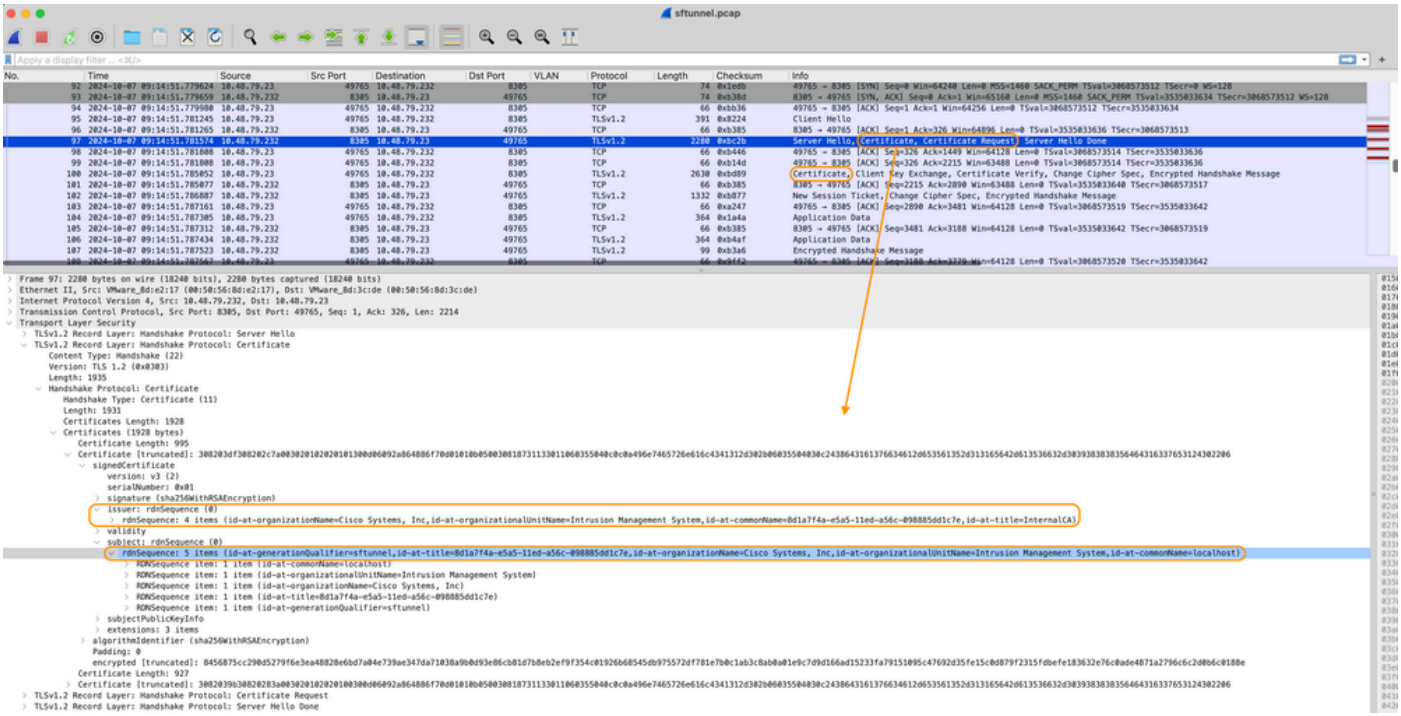
Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

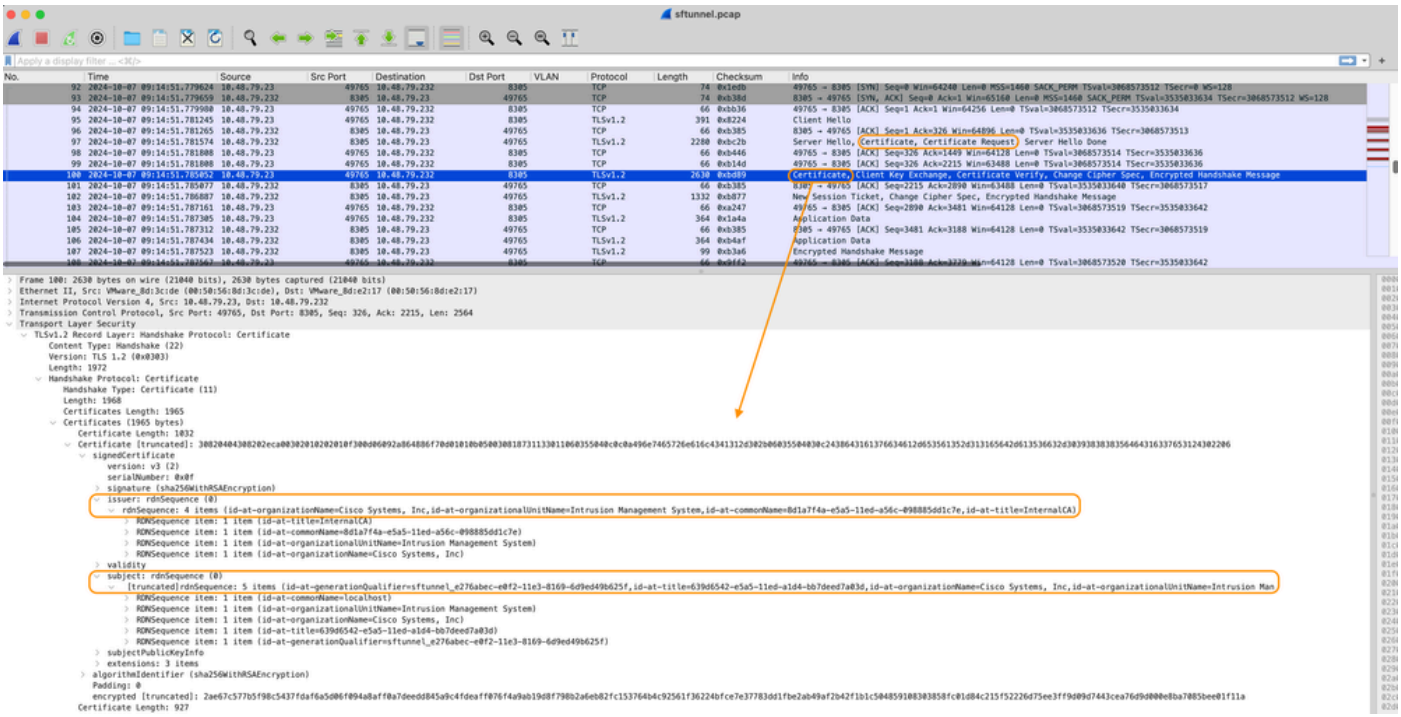
# Informações de Apoio

O FMC e o FTD comunicam-se entre si através do túnel sfl (túnel Sourcefire). Essa comunicação usa certificados para tornar a conversação segura em uma sessão TLS. Mais informações sobre o túnel sf e como ele é estabelecido podem ser encontradas neste link.

Na captura de pacotes, você pode ver que o FMC (10.48.79.232 neste exemplo) e o FTD (10.48.79.23) estão trocando certificados. Eles fazem isso para confirmar que conversam com o dispositivo correto e que não há interceptação nem ataque Man-In-The-Middle (MITM). A comunicação é criptografada usando esses certificados e somente a parte que tem a chave privada associada para esse certificado pode descriptografá-la novamente.




Certificate_exchange_server_cert




Certificate_exchange_client_cert

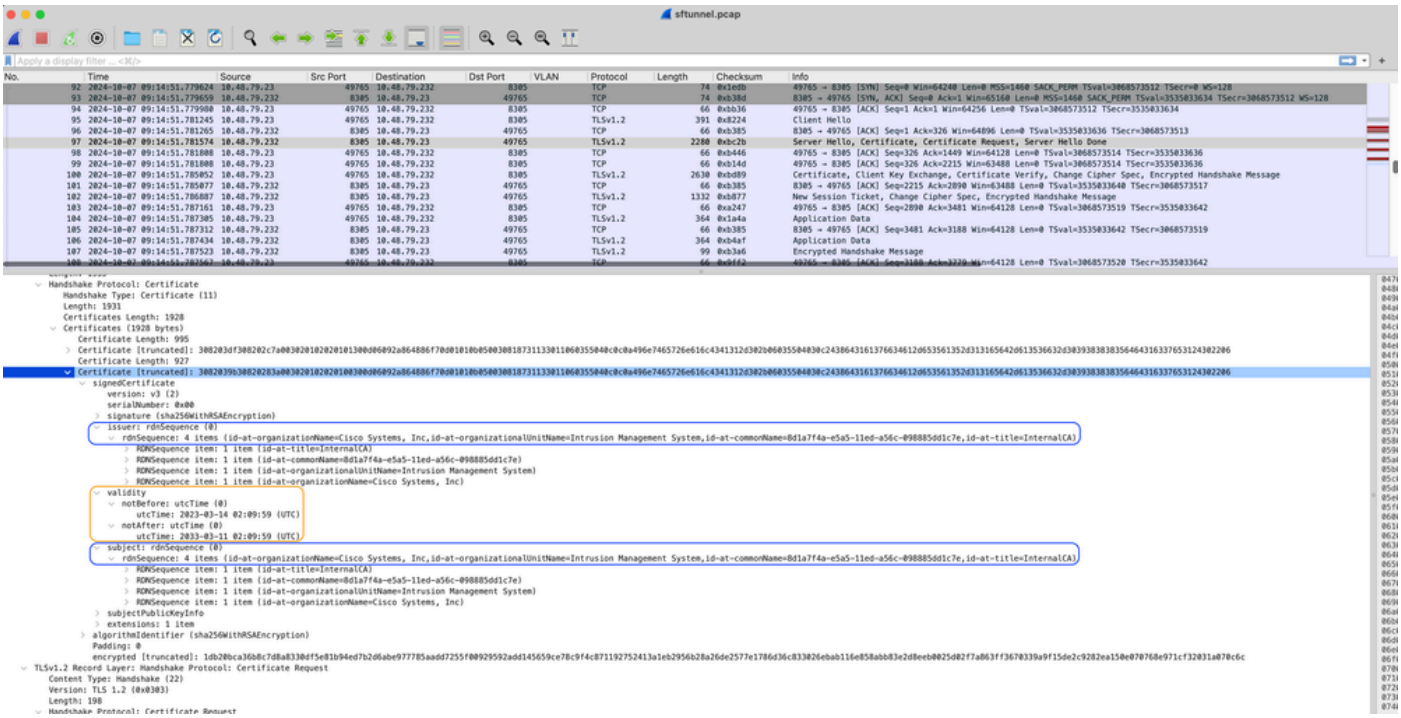
Você pode ver que os certificados são assinados pela mesma Autoridade de Certificação (CA) interna (emissor) que está configurada no sistema FMC. A configuração é definida no arquivo FMC em /etc/sf/sftunnel.conf que contém algo como:

```
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;
};
```

Indica a autoridade de certificação que é utilizada para assinar todos os certificados de túnel duplo (tanto o FTD como o FMC) e o certificado utilizado pelo FMC para enviar a todos os FTD. Este certificado é assinado pela InternalCA.

Quando o FTD se registra no FMC, o FMC também cria um certificado para enviar para o dispositivo FTD que é usado para a comunicação posterior no túnel sf. Este certificado também é assinado pelo mesmo certificado CA interno. No FMC, você pode encontrar esse certificado (e a chave privada) em /var/sf/peers/<UUID-FTD-device> e possivelmente na pasta certs_push e é chamado sftunnel-cert.pem (sftunnel-key.pem para a chave privada). No FTD, você pode encontrá-los em /var/sf/peers/<UUID-FMC-device> com a mesma convenção de nomenclatura.

No entanto, cada certificado também tem um período de validade para fins de segurança. Ao inspecionar o certificado InternalCA, podemos ver também o período de validade, que é de 10 anos para o FMC InternalCA, conforme mostrado na captura de pacotes.

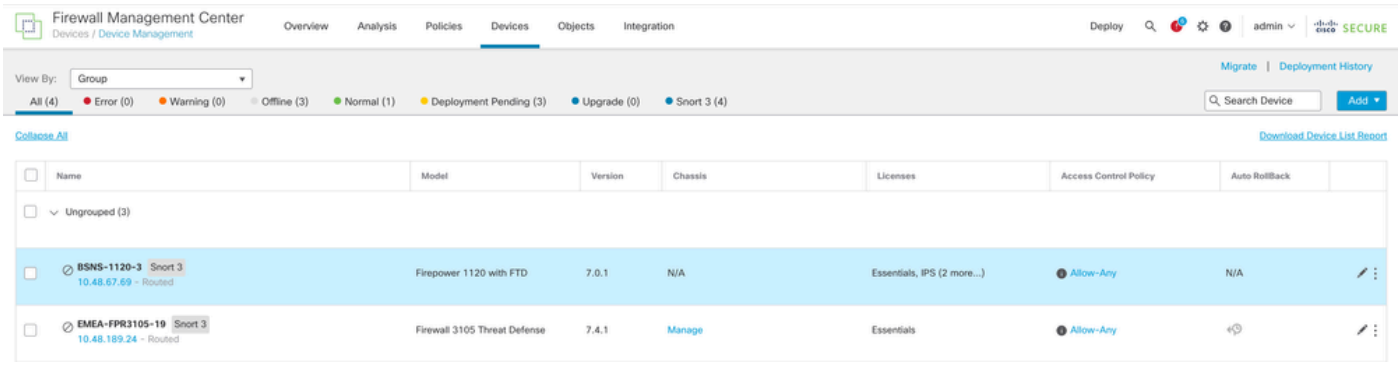



FMC-InternalCA_valid

# Problema

O certificado InternalCA do FMC só é válido por dez anos. Após o prazo de validade, o sistema remoto deixa de confiar neste certificado (bem como nos certificados por ele assinados), o que dá origem a problemas de comunicação sftunnel entre o FTD e os dispositivos do FMC. Isso também significa que várias funcionalidades importantes, como eventos de conexão, pesquisas de malware, regras baseadas em identidade, implantações de políticas e muitas outras coisas não estão funcionando.

Os dispositivos aparecem como desativados na interface do usuário do FMC na guia Devices > Device Management quando o sftunnel não está conectado. O problema relacionado a essa expiração é rastreado na ID de bug da Cisco CSCwd08098. Observe que todos os sistemas são afetados, mesmo quando você executa uma versão fixa do defeito. Mais informações sobre essa correção podem ser encontradas na seção Solução.




Dispositivos desativados

O FMC não atualiza automaticamente a CA nem republica os certificados nos dispositivos de

FTD. Além disso, não existe qualquer alerta sanitário do CVP que indique que o certificado expira. A ID de bug da Cisco CSCwd08448 é rastreada a este respeito para fornecer um alerta de integridade na interface do usuário do FMC no futuro.

## O que acontece após a data de expiração?

Inicialmente, nada acontece e os canais de comunicação do sftunnel continuam a operar como antes. No entanto, quando a comunicação sftunnel entre os dispositivos FMC e FTD é interrompida e tenta restabelecer a conexão, ela falha e você pode observar linhas de registro no arquivo de registro de mensagens que apontam para a expiração do certificado.

Linhas de log do dispositivo FTD de /ngfw/var/log/messages:

```
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
```

Linhas de registro do dispositivo FMC de /var/log/messages:

```
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
```

A comunicação sftunnel pode ser interrompida por vários motivos:

- Perda de comunicação devido à perda de conectividade de rede (possivelmente apenas temporária)
- Reinicialização do FTD ou do FMC
  - Os esperados: reinicialização manual, atualizações, reinicialização manual do processo sftunnel no FMC ou FTD (por exemplo, por pmtool restartbyid sftunnel)
  - Inesperados: retornos de rastreamento, queda de energia

Como há tantas possibilidades que podem interromper a comunicação do túnel, é altamente aconselhável corrigir a situação o mais rápido possível, mesmo quando atualmente todos os dispositivos FTD estão conectados corretamente, apesar do certificado expirado.

## Como verificar rapidamente se o certificado expirou ou quando ele expira?

A maneira mais fácil é executar esses comandos na sessão SSH do FMC:

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

Mostra os elementos de Validade do certificado. A parte principal relevante aqui é o "notAfter" que mostra que o certificado aqui é válido até 5 de outubro 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
```

NãoDepois

Se você preferir que um único comando seja executado que forneça imediatamente a quantidade de dias para os quais o certificado ainda é válido, você poderá usar:

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

Um exemplo de uma configuração em que o certificado ainda é válido por vários anos é mostrado.

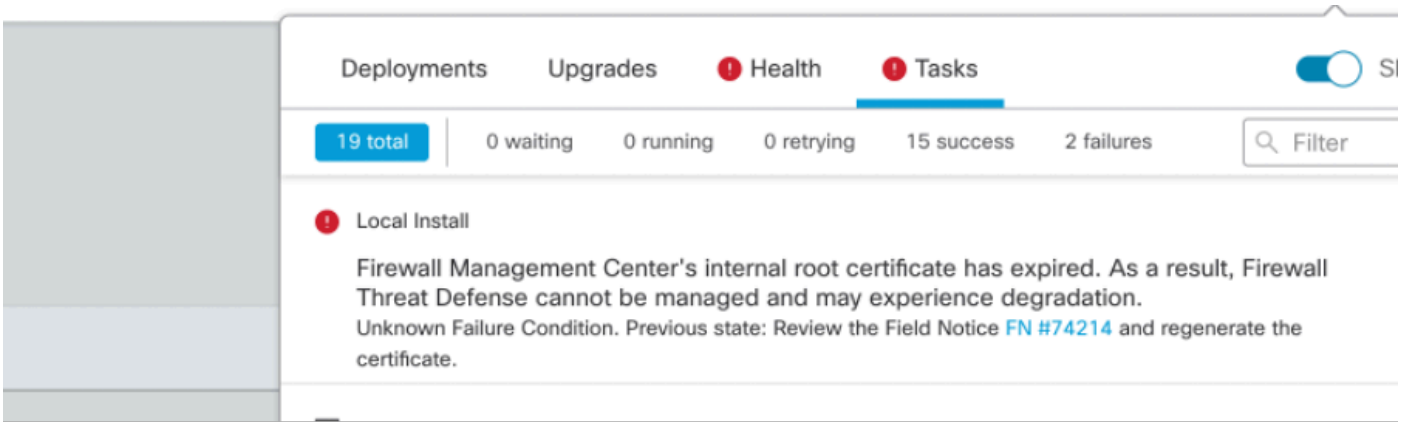
```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS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

Certificate_expiry_validation_command

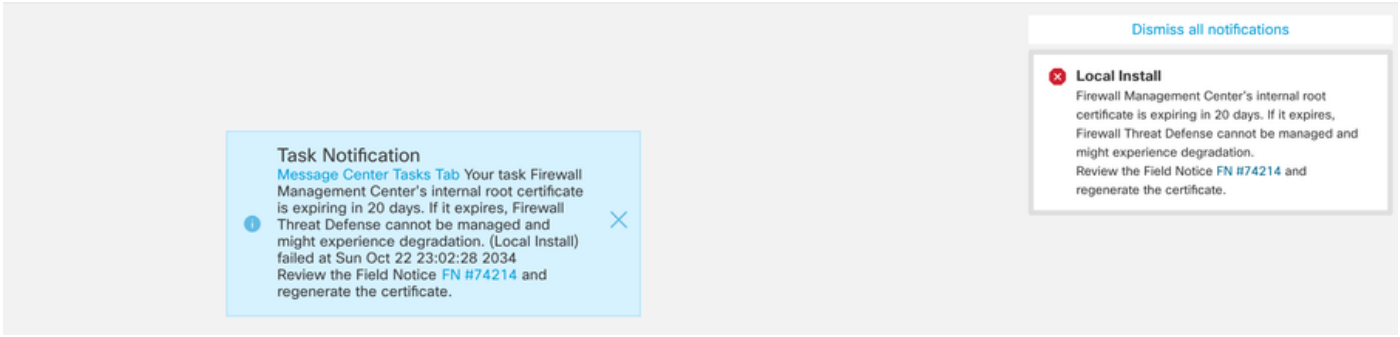
## Como posso ser notificado futuramente sobre a expiração de um certificado?

Com atualizações recentes do VDB (399 ou superior), você é alertado automaticamente quando seu certificado expira em 90 dias. Portanto, você não precisa rastrear isso manualmente, pois é alertado quando está próximo do tempo de expiração. Em seguida, ele é exibido na página da Web do FMC em dois formulários. Ambas as formas se referem à página de notificação de campo.

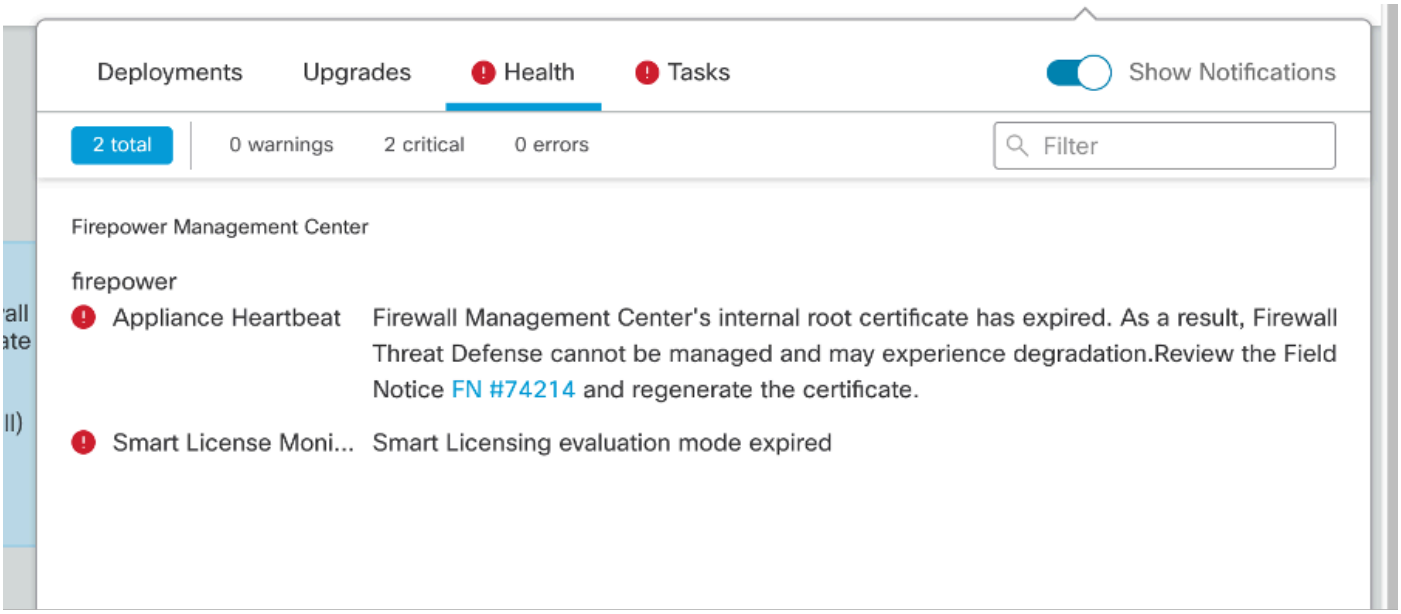
O primeiro método é através da Guia Tarefa. Essa mensagem é fixa e está disponível para o usuário, a menos que seja explicitamente fechada. O pop-up de notificação também é exibido e fica disponível até que seja explicitamente fechado pelo usuário. Ele sempre aparece como um erro.



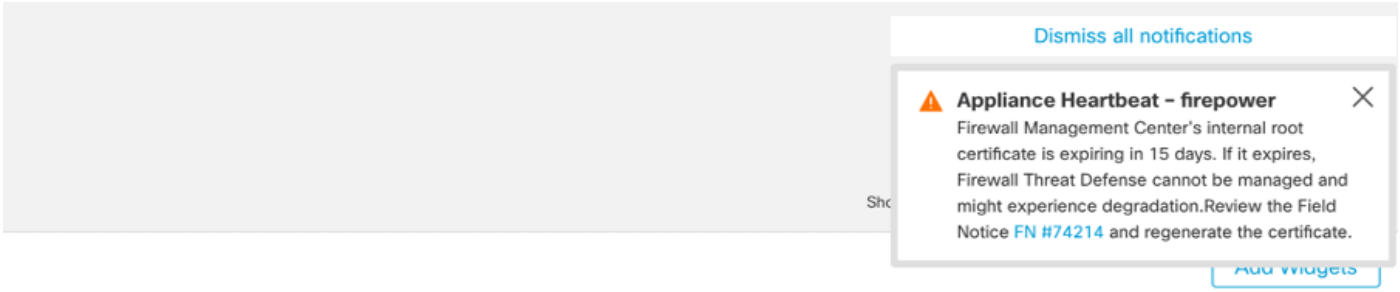

Notificação de vencimento na guia Tarefa



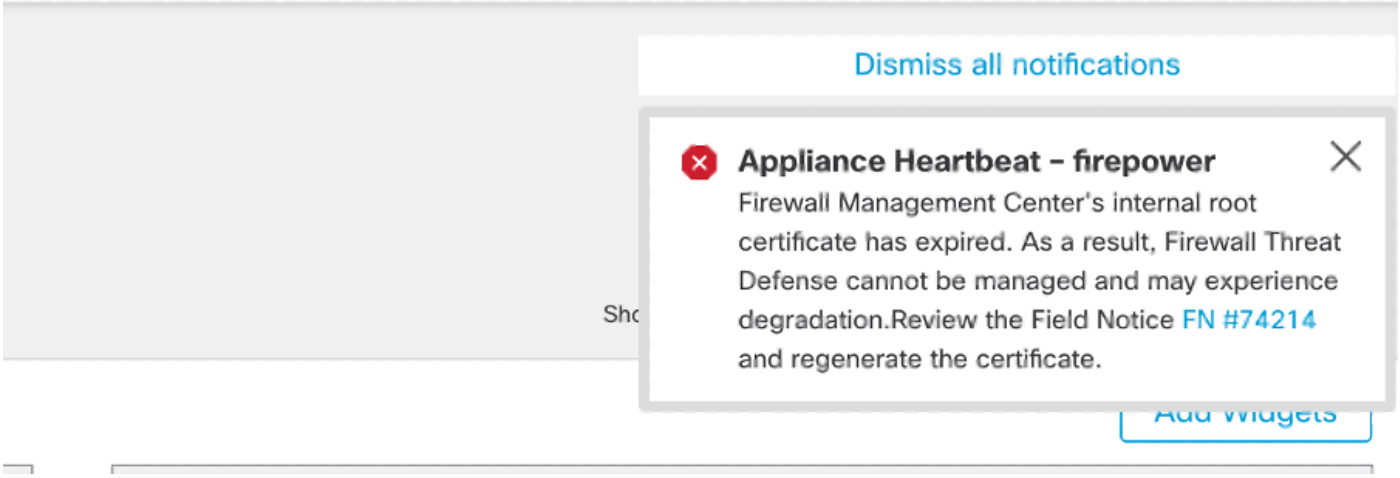

O segundo método é através do Health Alert. Isso aparece na guia Integridade, mas não é difícil e substitui ou remove quando o monitor de integridade é executado, o que por padrão é a cada 5 minutos. Ele também mostra um pop-up de notificação que precisa ser fechado explicitamente pelo usuário. Isso pode aparecer como erro (quando expirado) como um aviso (quando expirará).




Notificação de vencimento na guia Integridade




Notificação de aviso no Pop-up de Alerta de Integridade




Notificação de erro no pop-up de alerta de integridade

## Solução 1 - O certificado ainda não expirou (cenário ideal)

Essa é a melhor situação, pois, dependendo da expiração do certificado, ainda temos tempo. Ou adotamos a abordagem totalmente automatizada (recomendada), que depende da versão do FMC, ou adotamos uma abordagem mais manual, que requer interação com o TAC.

## Método recomendado

Esta é a situação em que não se espera nenhum tempo de inatividade e a menor quantidade de operações manuais em circunstâncias normais.

Antes de continuar, você deve instalar o hotfix para sua versão específica, conforme listado aqui. A vantagem aqui é que esses hotfixes não exigem uma reinicialização do FMC e, portanto, uma possível comunicação sftunnel interrompida quando o certificado já expirou. Os hotfixes disponíveis são:

- 7.0.0 - 7.0.6 : Hotfix FK - 7.0.6.99-9
- 7.1.x: nenhuma versão fixa como fim da manutenção de software
- 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

Depois que o hotfix for instalado, o FMC deverá conter o script generate_certs.pl que:

1. Regenera a CA interna
2. Recria os certificados sftunnel assinados por esta nova InternalCA
3. Envia por push os novos certificados sftunnel e as chaves privadas para os respectivos dispositivos FTD (quando o sftunnel estiver operacional)

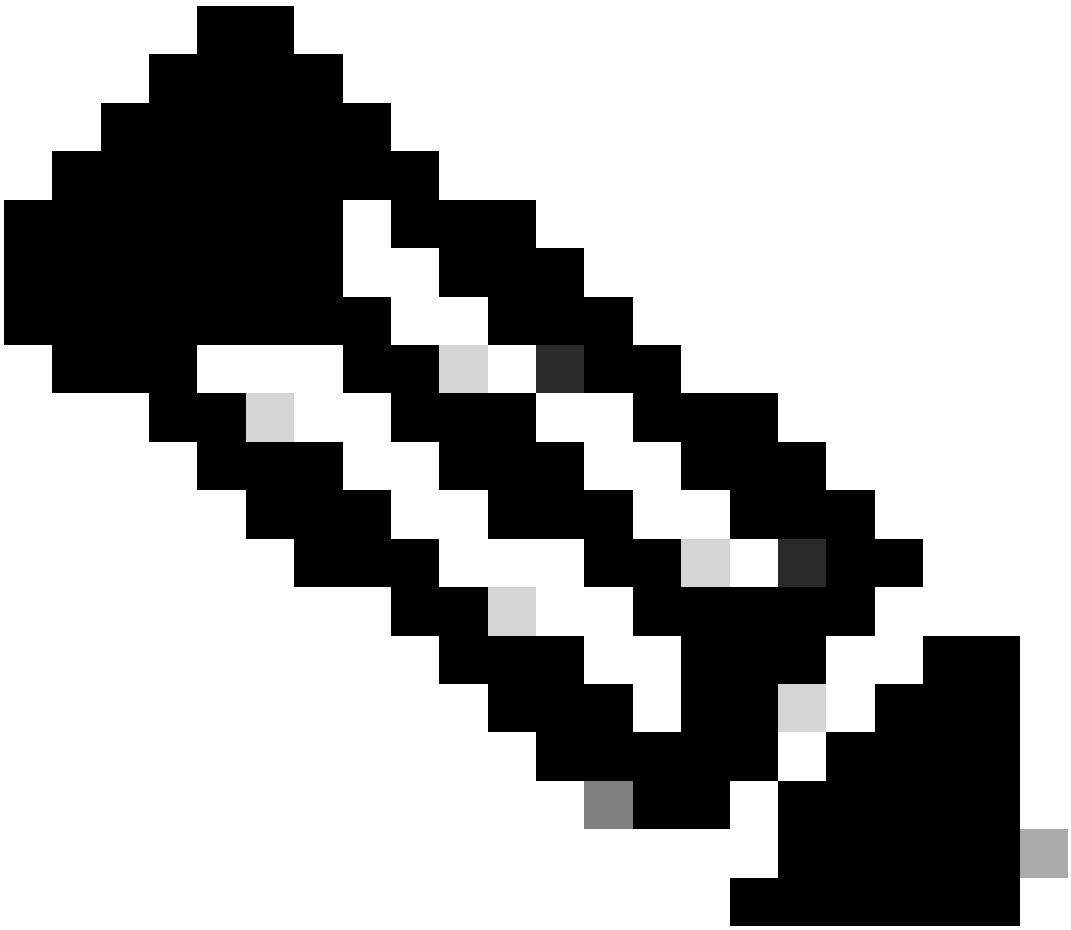
Por conseguinte, recomenda-se (se possível):

1. Instale o hotfix aplicável acima
2. Fazer um backup no FMC
3. Valide todas as conexões sftunnel atuais usando o script sftunnel_status.pl no FMC (no modo expert)
4. Execute o script a partir do modo especialista usando generate_certs.pl
5. Inspecionar o resultado para validar se são necessárias quaisquer operações manuais (quando os dispositivos não estão ligados ao CVP) [explicado mais adiante]
6. Execute o sftunnel_status.pl do FMC para validar se todas as conexões do sftunnel estão funcionando corretamente

```
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#
```

Script Generate_certs.pl

---



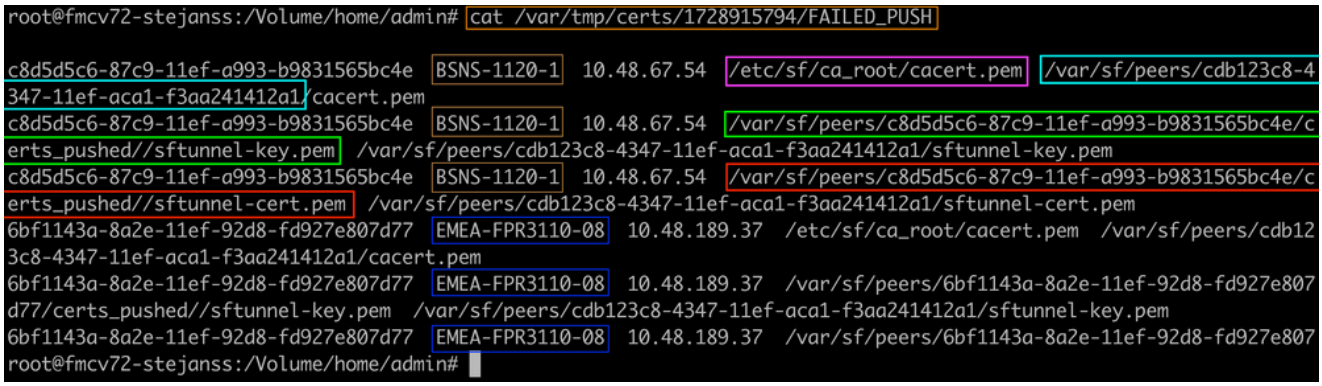
---

Note: Quando o FMC estiver em execução no High-Availability (HA), você precisará executar a operação primeiro no nó primário e depois no nó secundário, pois ele também usa esses certificados para se comunicar entre os nós do FMC. A InternalCA em ambos os nós do FMC é diferente.

No exemplo aqui, você vê que ele cria um arquivo de log em /var/log/sf/sfca_generation.log, indica para usar sftunnel_status.pl, indica o tempo de expiração em InternalCA e indica para quaisquer falhas nele. Aqui, por exemplo, ele falhou ao enviar os certificados para o dispositivo BSNS-1120-1 e EMEA-FPR3110-08, o que é esperado porque o sftunnel estava inoperante para esses dispositivos.

Para corrigir o sftunnel das conexões com falha, execute as próximas etapas:

1. Na CLI do FMC, abra o arquivo FAILED_PUSH usando cat /var/tmp/certs/1728303362/FAILED_PUSH (o valor do número representa o tempo UNIX, portanto, verifique a saída do comando anterior em seu sistema) que tem o próximo formato: FTD_UUID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINATION_PATH_ON_FTD




FAILED_PUSH

2. Transferir esses novos certificados (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) do FMC para os dispositivos do FTD
   ===Aproximação automática===

   A instalação do hotfix também fornece os scripts copy_sftunnel_certs.py e copy_sftunnel_certs_jumpserver.py que automatizam a transferência dos vários certificados para sistemas para os quais o sftunnel não estava ativo enquanto os certificados eram regenerados. Isso também pode ser usado para sistemas que tiveram uma conexão sftunnel interrompida porque o certificado já expirou.

   Você pode usar o script copy_sftunnel_certs.py quando o próprio FMC tiver acesso SSH aos

vários sistemas FTD. Se não for o caso, você pode fazer o download do script (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) do FMC para um servidor de salto que tenha acesso SSH aos dispositivos FMC e FTD e executar o script Python a partir daí. Se isso também não for possível, sugira executar a abordagem manual mostrada a seguir. Os exemplos a seguir mostram o script copy_sftunnel_certs.py sendo usado, mas as etapas são as mesmas para o script copy_sftunnel_certs_jumpserver.py .

A. Crie um arquivo CSV no FMC (ou servidor de salto) que contenha as informações do dispositivo (nome_do_dispositivo, endereço IP, nome_do_usuário admin, senha_admin) que são usadas para fazer a conexão SSH.

Ao executar isso a partir de um servidor remoto, como um servidor de salto para o FMC primário, certifique-se de adicionar os detalhes do FMC primário como a primeira entrada seguida por todos os FTD gerenciados e FMC secundário. Ao executar isso a partir de um servidor remoto, como um servidor de salto para o FMC secundário, certifique-se de adicionar os detalhes do FMC secundário como a primeira entrada seguida por todos os FTD gerenciados.

i. Crie um arquivo usando vi devices.csv. 


vi devices.csv

ii) Isso abre o arquivo vazio (não mostrado) e você preenche os detalhes como mostrado depois de usar i letra no teclado para entrar no modo INTERATIVO (visto na parte inferior da tela).


exemplo de devices.csv

iii) Quando terminar, feche e salve o arquivo usando ESC seguido por :wq e, em seguida, Enter.


Salve o device.csv

B. Execute o script (a partir da raiz usando sudo) com copy_sftunnel_certs.py devices.csv e ele mostrará o resultado. Aqui, ele mostra que o certificado para FTDv foi enviado corretamente e que para BSNS-1120-1 ele não pôde fazer a conexão SSH com o dispositivo.

```
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 dispositivos.csv

===Aproximação manual===

1. Imprima (cat) a saída de cada um dos arquivos para cada FTD afetado (cacert.pem / sftunnel-key.pem (não mostrado completamente para fins de segurança) / sftunnel-cert.pem) na CLI do FMC copiando o local do arquivo da saída anterior (arquivo FAILED_PUSH).

```
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
```

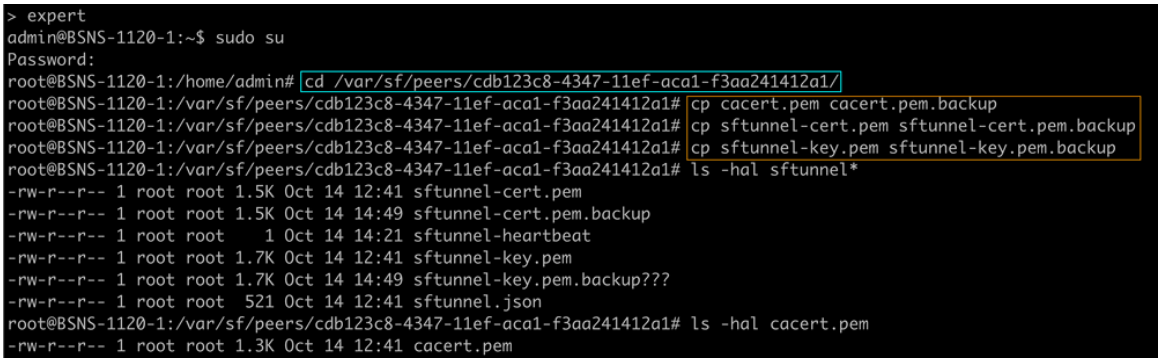
sftunnel-key.pem

```
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. Abra o FTD CLI de cada FTD respectivo no modo especialista com privilégios de raiz através do sudo su e renove os certificados com o próximo procedimento.
    1. Navegue até o local visto no realce azul claro da saída FAILED_PUSH (cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 aqui por exemplo, mas isso é diferente para cada FTD).
    2. Fazer backups dos arquivos existentes.

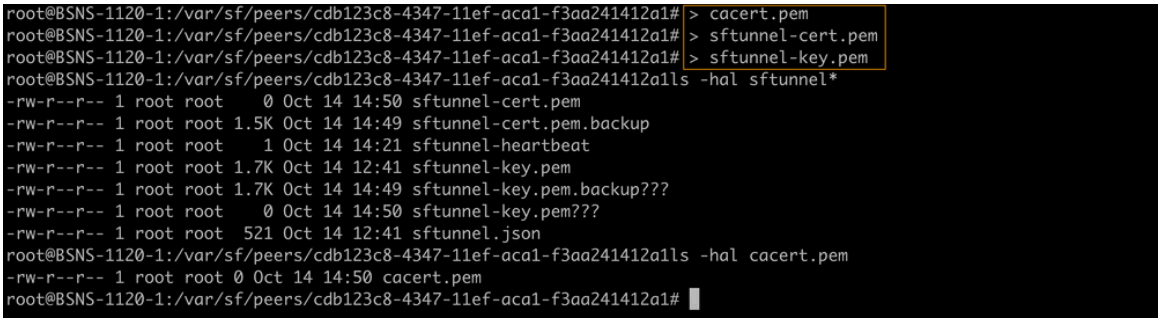
```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```




Fazer backups dos certificados atuais

    3. Esvazie os arquivos para que possamos gravar novo conteúdo neles.

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




Conteúdo vazio de arquivos de certificado existentes

    4. Escreva o novo conteúdo (da saída FMC) em cada um dos arquivos individualmente usando vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (comando separado por arquivo - capturas de tela mostram isso apenas para cacert.pem, mas precisam ser repetidas para sftunnel-cert.pem e sftunnel-

key.pem).

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

vi cacert.pem

1. Pressione i para entrar no modo interativo (depois que o comando vi for inserido e um arquivo vazio for exibido).
2. Copie e cole o conteúdo inteiro (incluindo -----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----) no arquivo.


Copiar conteúdo no vi (modo INSERT)

3. Feche e grave no arquivo com ESC seguido por :wq e insira.


ESC seguido por :wq para gravar no arquivo

5. Valide se as permissões corretas (chmod 644) e os proprietários (chown root:root) estão definidos para cada um dos arquivos usando ls -hal. Isso é definido corretamente na verdade quando atualizamos o arquivo 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 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#
```

Todos os arquivos de certificado atualizados com permissões e proprietários de direitos

3. Reinicie o sftunnel em cada FTD respectivo onde o sftunnel não estava operacional para que as alterações no certificado entrem em vigor com o 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 se todos os FTDs estão conectados corretamente agora usando a saída sftunnel_status.pl

# Solução 2 - O certificado já expirou

Nesta situação, temos dois cenários diferentes. Ou todas as conexões sftunnel ainda estão operacionais ou não estão mais (ou parciais).

## FTDs ainda conectados por meio de sftunnel

Podemos aplicar o mesmo procedimento indicado na seção Certificado ainda não expirou (cenário ideal) - Abordagem recomendada.

No entanto, NÃO atualize nem reinicialize o FMC (ou qualquer FTD) nesta situação, pois ele desconecta todas as conexões sftunnel e precisamos executar manualmente todas as atualizações de certificado em cada FTD. A única exceção a esta, são as versões de Hotfix listadas, pois não exigem uma reinicialização do FMC.

Os túneis permanecem conectados e os certificados são substituídos em cada um dos FTD. Caso alguns certificados falhem ao serem preenchidos, ele o avisa com os que falharam e você precisa fazer a abordagem manual conforme indicado anteriormente na seção anterior.

## Os FTDs não estão mais conectados por meio do sftunnel

Método recomendado

Podemos aplicar o mesmo procedimento indicado na seção Certificado ainda não expirou (cenário ideal) - Abordagem recomendada. Neste cenário, o novo certificado será gerado no FMC, mas não poderá ser copiado para os dispositivos, pois o túnel já está inoperante. Esse processo pode ser automatizado com os scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py

Se todos os dispositivos do FTD estiverem desconectados do FMC, podemos atualizá-lo nessa situação, pois isso não afeta as conexões de sftunnel. Se ainda houver alguns dispositivos conectados por meio do sftunnel, lembre-se de que a atualização do FMC fecha todas as conexões do sftunnel e elas não são ativadas novamente devido ao certificado expirado. O benefício da atualização aqui seria que ela fornece uma boa orientação sobre os arquivos de certificado que precisam ser transferidos para cada um dos FTDs.

Abordagem manual

Nessa situação, você pode executar o script generate_certs.pl no FMC que gera os novos certificados, mas ainda é necessário enviá-los para cada um dos dispositivos do FTD manualmente. Dependendo da quantidade de dispositivos, isso pode ser feito ou pode ser uma tarefa entediante. No entanto, ao usar os scripts copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py, isso é altamente automatizado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.