Rinnovo del certificato CA del tunnel SFC del CCP per la connettività FTD

Sommario

Introduzione

In questo documento viene descritto il rinnovo del certificato CA (Certification Authority) di Firepower Management Center (FMC) in relazione alla connettività Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

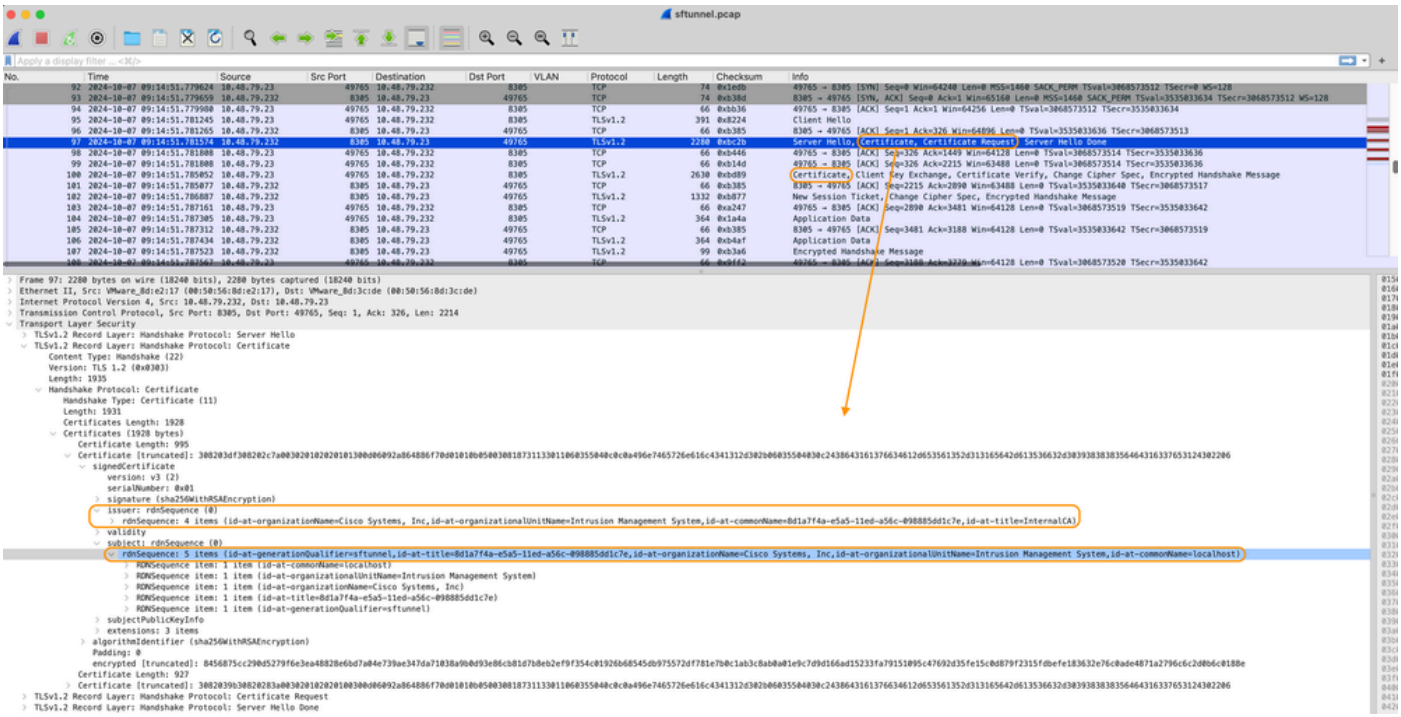
Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

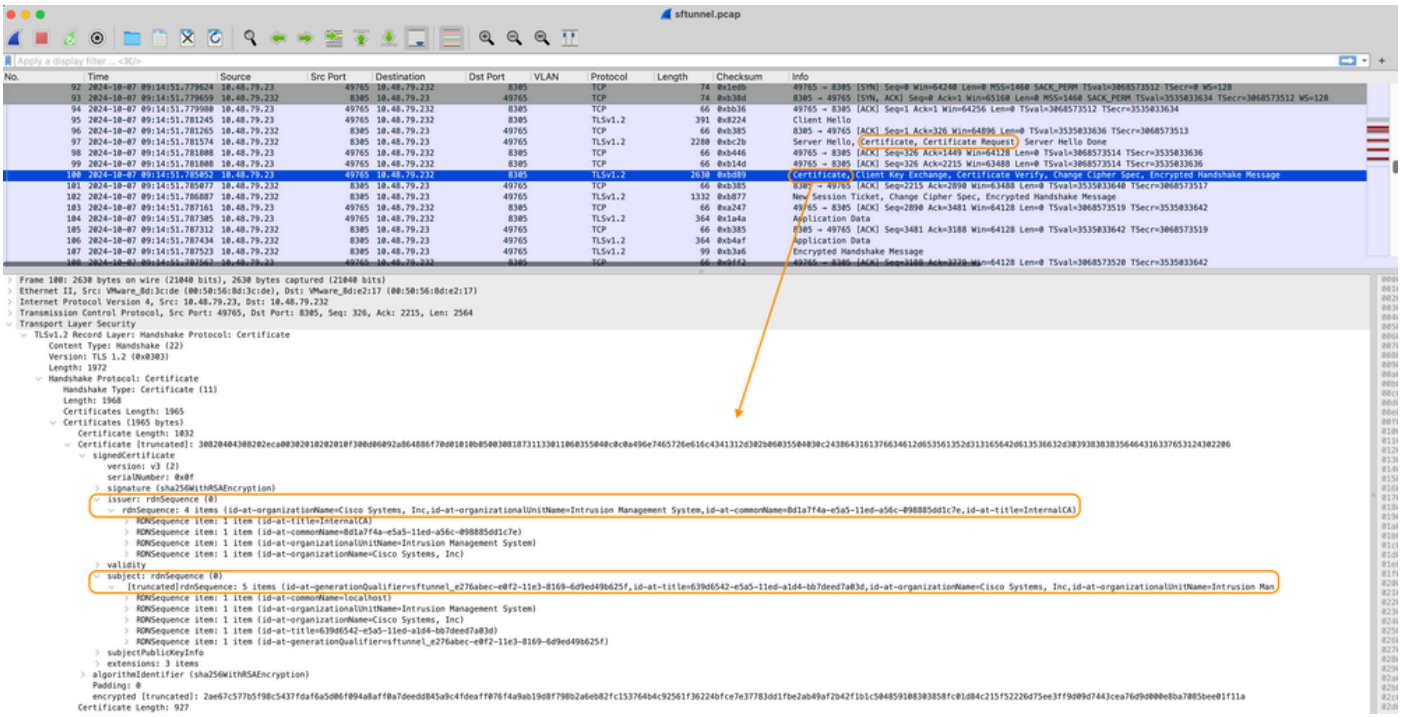
Premesse

Il FMC e l'FTD comunicano tra loro attraverso il tunnel Sourcefire. In questa comunicazione vengono utilizzati i certificati per proteggere la conversazione in una sessione TLS. Per maggiori informazioni su sftunnel e su come viene stabilito, cliccare su questo link.

Dall'acquisizione dei pacchetti è possibile notare che i due FMC (10.48.79.232 nell'esempio) e FTD (10.48.79.23) si scambiano certificati. Lo fanno per convalidare che parlano con il dispositivo corretto e non c'è alcun tipo di intercettazione o attacco Man-In-The-Middle (MITM). La comunicazione viene crittografata utilizzando tali certificati e solo la parte che dispone della chiave privata associata per il certificato è in grado di decrittografarla nuovamente.



Certificato_scambio_server_cert



Certificato_scambio_client_cert

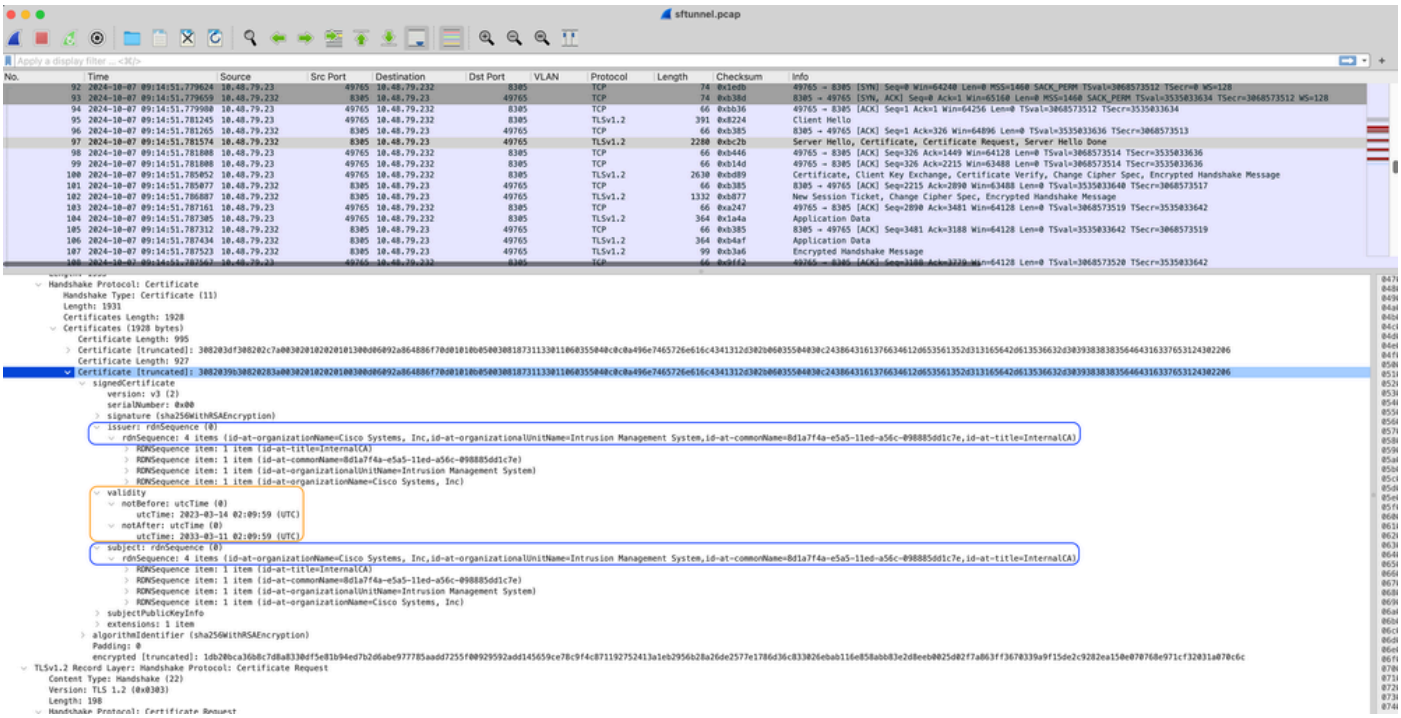
È possibile visualizzare i certificati firmati dalla stessa CA interna (autorità di certificazione) impostata nel sistema FMC. La configurazione è definita nel file /etc/sf/sftunnel.conf del FMC che contiene:

```
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 l'autorità di certificazione utilizzata per firmare tutti i certificati per sftunnel (FTD e FMC uno) e il certificato utilizzato dal FMC per inviare tutti i FTD. Il certificato è firmato dalla CA interna.

Quando un FTD si registra nel FMC, quest'ultimo crea anche un certificato da inviare al dispositivo FTD utilizzato per le successive comunicazioni nel tunnel sfc. Il certificato è firmato anche dallo stesso certificato CA interno. In FMC, il certificato (e la chiave privata) si trovano nella cartella /var/sf/peers/<UUID-FTD-device> e potenzialmente nella cartella certs_pushed ed è denominato sftunnel-cert.pem (sftunnel-key.pem per la chiave privata). Su FTD, è possibile trovare quelli sotto /var/sf/peers/<UUID-FMC-device> con la stessa convenzione di denominazione.

Ogni certificato ha tuttavia anche un periodo di validità a fini di sicurezza. Quando si controlla il certificato InternalCA, è possibile verificare anche il periodo di validità che è di 10 anni per l'InternalCA FMC, come mostrato dall'acquisizione del pacchetto.

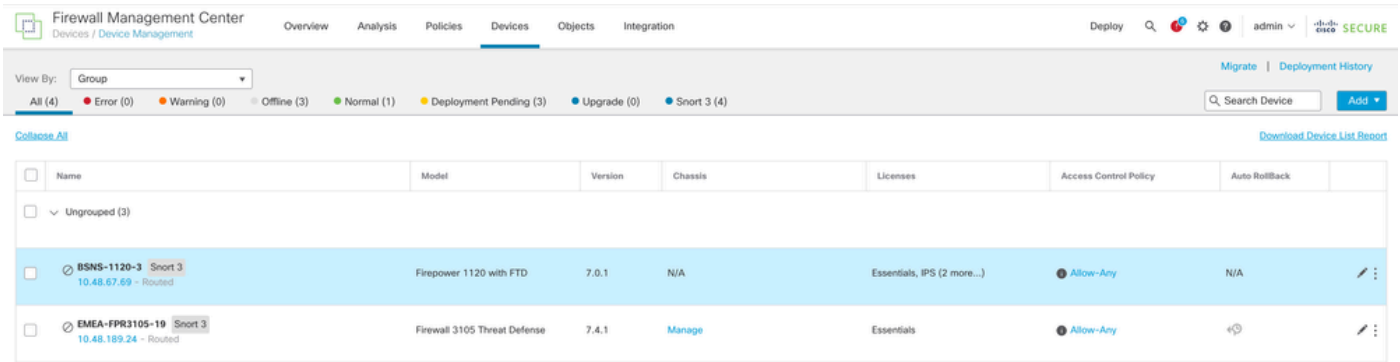


FMC-ValiditàCA_interna

Problema

Il certificato CA interna del CCP è valido solo per 10 anni. Dopo la scadenza, il sistema remoto non considera più attendibile il certificato (e i certificati da esso firmati) e ciò comporta problemi di comunicazione del tunnel tra i dispositivi FTD e FMC. Questo significa anche che diverse funzionalità chiave come gli eventi di connessione, le ricerche di malware, le regole basate sull'identità, le distribuzioni di criteri e molti altri elementi non funzionano.

I dispositivi vengono visualizzati come disattivati nell'interfaccia utente di FMC nella scheda Dispositivi > Gestione dispositivi quando sftunnel non è connesso. Il problema relativo alla scadenza viene registrato nell'ID bug Cisco CSCwd08098. Si noti tuttavia che il problema interessa tutti i sistemi, anche se si esegue una versione fissa del problema. Per ulteriori informazioni su questa correzione, vedere la sezione Soluzione.



Periferiche disabilitate

Il FMC non aggiorna automaticamente la CA e ripubblica i certificati sui dispositivi FTD. Non è inoltre presente alcun avviso di integrità del CCP che indica che il certificato scade. A questo

proposito, viene registrato l'ID bug Cisco CSCwd08448 per fornire un avviso sullo stato di salute sull'interfaccia utente del Cisco in futuro.

Cosa succede dopo la data di scadenza?

Inizialmente non accade nulla e i canali di comunicazione sftunnel continuano a funzionare come prima. Tuttavia, quando la comunicazione sftunnel tra i dispositivi FMC e FTD si interrompe e tenta di ristabilire la connessione, non riesce ed è possibile osservare le righe di registro nel file di registro dei messaggi che indicano la scadenza del certificato.

Righe di registro dal dispositivo FTD da /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
```

Righe di registro dal dispositivo FMC da /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
```

La comunicazione con il tunnel alternativo può essere interrotta per diversi motivi:

- Perdita di comunicazione a causa della perdita di connettività di rete (potenzialmente solo temporanea)
- Riavvio di FTD o FMC
  - Previsti: riavvio manuale, aggiornamenti, riavvio manuale del processo sftunnel su FMC o FTD (ad esempio tramite pmtool restartbyid sftunnel)
  - Quelli imprevisti: traceback, interruzione dell'alimentazione

Poiché ci sono così tante possibilità che possono interrompere la comunicazione sftunnel, si

consiglia vivamente di correggere sulla situazione il più rapidamente possibile, anche quando attualmente tutti i dispositivi FTD sono correttamente collegati nonostante il certificato scaduto.

Come verificare rapidamente se il certificato è scaduto o quando scade?

Il modo più semplice è eseguire questi comandi sulla sessione SSH del FMC:

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

Vengono visualizzati gli elementi Validità del certificato. La parte principale qui rilevante è il "notAfter" che mostra che il certificato qui è valido fino al 5 ottobre 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
```

NonDopo

Se si preferisce eseguire un unico comando che fornisca immediatamente il numero di giorni per cui il certificato è ancora valido, è possibile utilizzare quanto segue:

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

Viene visualizzato un esempio di installazione in cui il certificato è ancora valido per più anni.

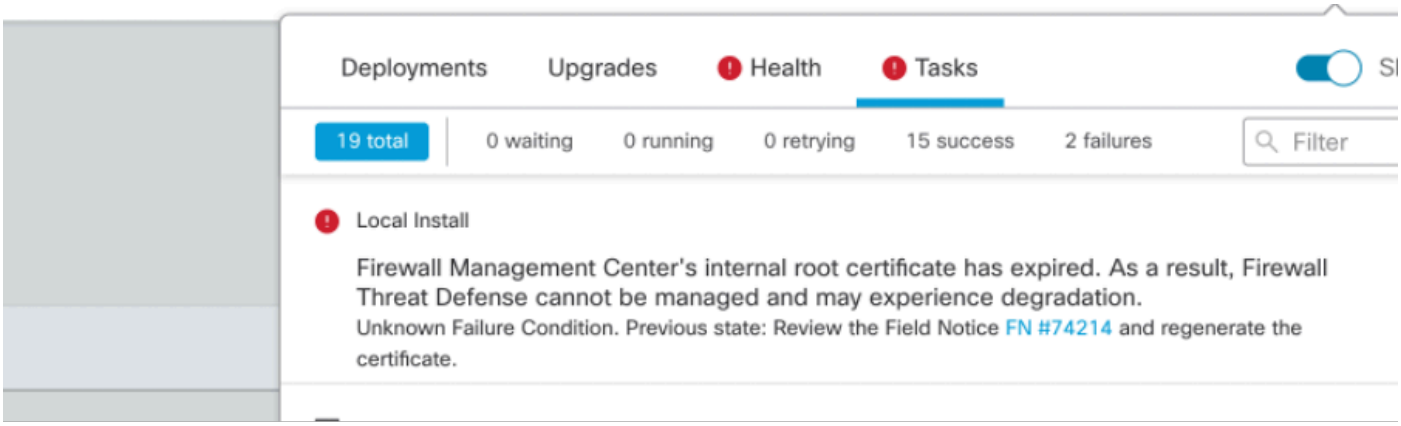
```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS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

Comando_convalida_scadenza_certificato

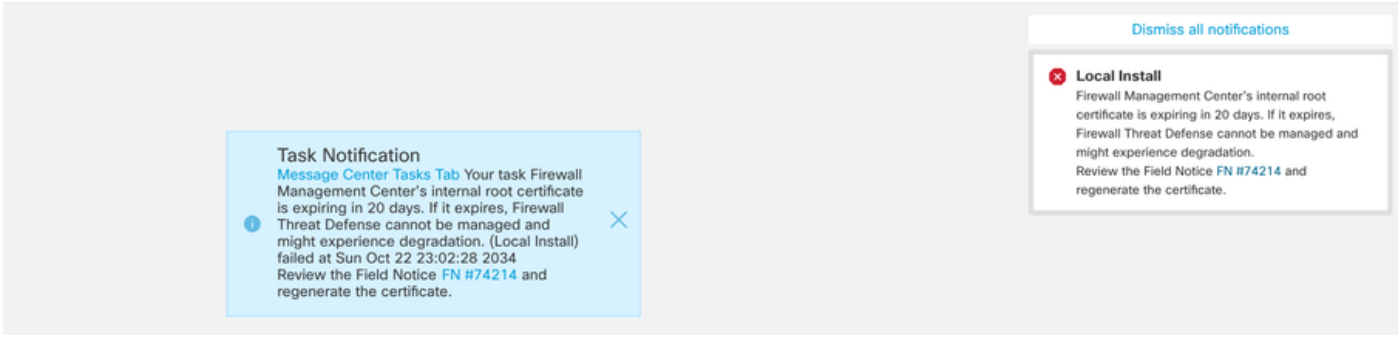
Come si riceve in futuro una notifica relativa alla prossima scadenza di un certificato?

Con gli aggiornamenti recenti di VDB (399 o versione successiva), viene visualizzato automaticamente un avviso quando il certificato scade entro 90 giorni. Pertanto, non è necessario tenere traccia manualmente della situazione da soli, in quanto si viene avvisati quando si è vicini alla scadenza. Questo viene visualizzato nella pagina Web del CCP in due forme. In entrambi i casi si fa riferimento alla pagina di notifica.

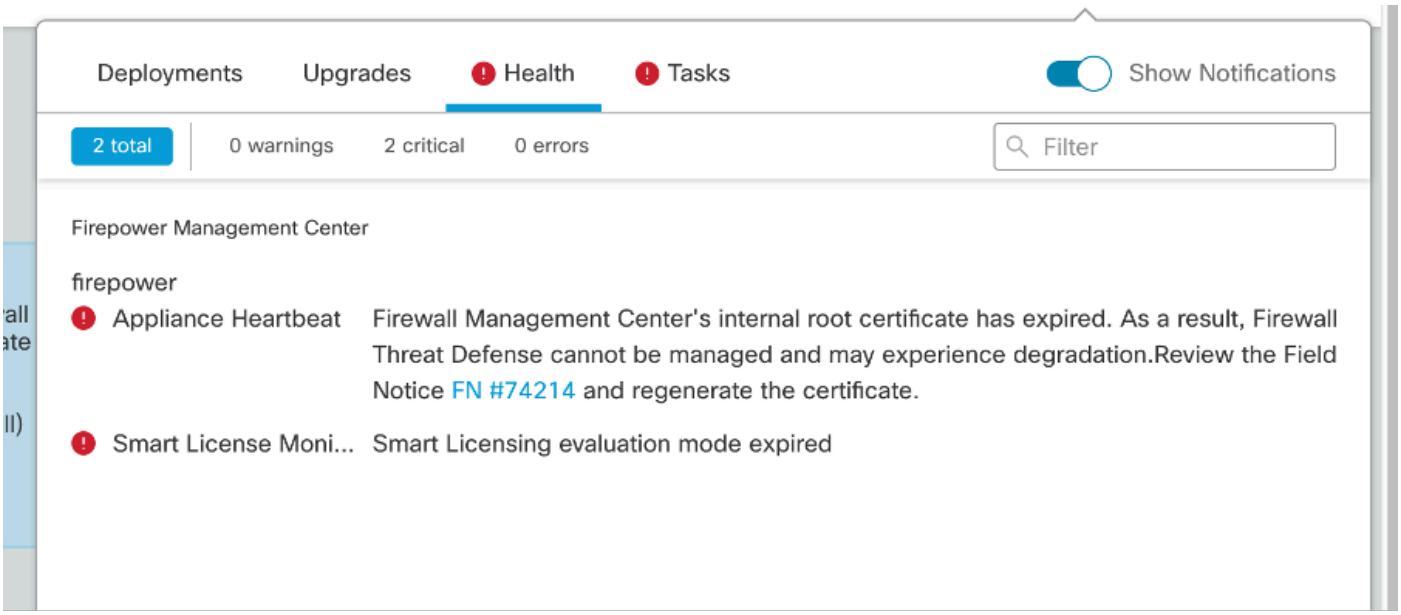
Il primo metodo consiste nell'utilizzare la scheda Task. Questo messaggio è permanente e disponibile per l'utente a meno che non sia stato esplicitamente chiuso. Viene visualizzata anche la finestra popup di notifica, disponibile fino alla chiusura esplicita da parte dell'utente. Viene sempre visualizzato come un errore.



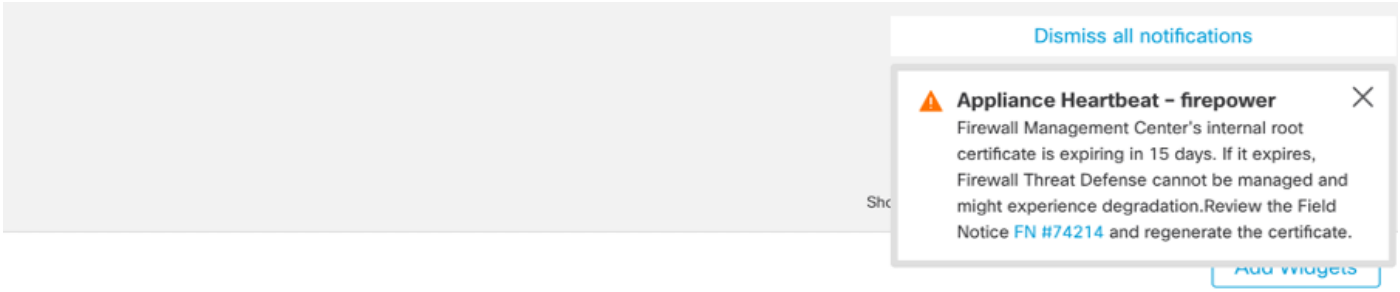
Notifica di scadenza nella scheda Task



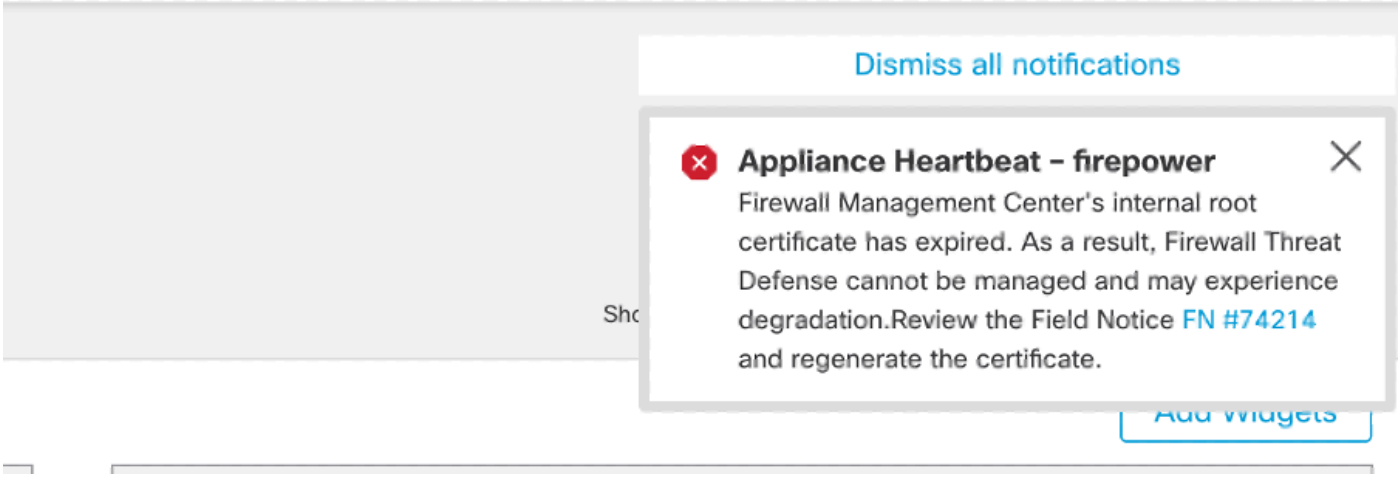
Il secondo metodo è tramite Health Alert. Questa opzione viene visualizzata nella scheda Integrità ma non è permanente e sostituisce o rimuove quando si esegue Health Monitor che, per impostazione predefinita, è ogni 5 minuti. Viene inoltre visualizzato un popup di notifica che deve essere chiuso esplicitamente dall'utente. Ciò può essere visualizzato come errore (se scaduto) come avviso (se sta per scadere).



Notifica di scadenza nella scheda Integrità



Notifica di avviso all'apertura dell'avviso di stato



Notifica di errore durante la visualizzazione dell'avviso di stato

Soluzione 1 - Il certificato non è ancora scaduto (scenario ideale)

Questa è la situazione migliore perché, a seconda della scadenza del certificato, abbiamo ancora tempo. O adottiamo l'approccio completamente automatizzato (consigliato) che dipende dalla versione FMC o un approccio più manuale che richiede l'interazione TAC.

Approccio consigliato

Questa è la situazione in cui non si prevedono tempi di inattività e si prevede un minor numero di operazioni manuali in circostanze normali.

Prima di procedere, è necessario installare l'aggiornamento rapido per la versione in uso, come indicato di seguito. Il vantaggio è che tali aggiornamenti rapidi non richiedono il riavvio del FMC e quindi la potenziale interruzione della comunicazione con il tunnel quando il certificato è già scaduto. Gli aggiornamenti rapidi disponibili sono:

- 7.0.0 - 7.0.6 : Aggiornamento rapido FK - 7.0.6.99-9
- 7.1.x : nessuna versione fissa alla fine della manutenzione del software
- 7.2.0 - 7.2.9 : Aggiornamento rapido FZ - 7.2.9.99-4
- 7.3.x : Aggiornamento rapido - 7.3.1.99-4
- 7.4.0 - 7.4.2 : Aggiornamento rapido AO - 7.4.2.99-5
- 7.6.0 : Aggiornamento rapido B - 7.6.0.99-5

Una volta installato l'aggiornamento rapido, il FMC deve ora contenere lo script generate_certs.pl che:

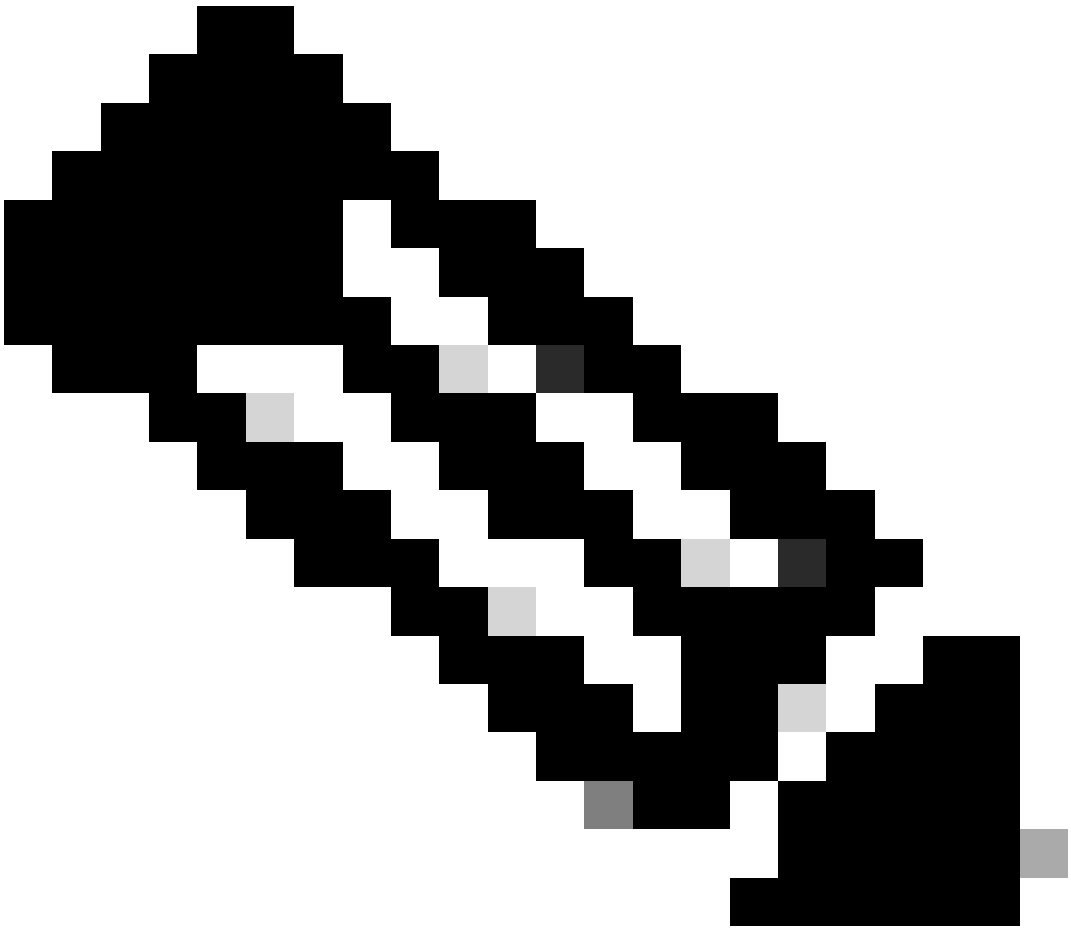
1. Rigenera la CA interna
2. Ricrea i certificati sftunnel firmati da questa nuova CA interna
3. Invia i nuovi certificati sftunnel e le nuove chiavi private ai rispettivi dispositivi FTD (quando il sftunnel è operativo)

Si raccomanda pertanto (se possibile) di:

1. Installare l'aggiornamento rapido desiderato
2. Eseguire un backup sul CCP
3. Convalida tutte le connessioni sftunnel correnti utilizzando lo script sftunnel_status.pl nel FMC (dalla modalità Expert)
4. Eseguire lo script dalla modalità Expert utilizzando generate_certs.pl
5. Esaminare il risultato per verificare se sono necessarie operazioni manuali (quando i dispositivi non sono collegati al CCP) [ulteriori informazioni]
6. Eseguire il file sftunnel_status.pl dalla console Gestione configurazione server per verificare che tutte le connessioni sftunnel funzionino correttamente

```
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



Nota: Se FMC è in esecuzione in modalità High-Availability (HA), è necessario eseguire l'operazione prima sul nodo primario e quindi sul nodo secondario, poiché utilizza anche tali certificati per comunicare tra i nodi FMC. La CA interna di entrambi i nodi FMC è diversa.

Nell'esempio riportato di seguito viene indicato che viene creato un file di log in /var/log/sf/sfca_generation.log, che indica di utilizzare sftunnel_status.pl, che indica l'ora di scadenza dell'autorità di certificazione interna e di eventuali errori. In questo caso, ad esempio, non è stato possibile inviare i certificati ai dispositivi BSNS-1120-1 e EMEA-FPR3110-08, come previsto perché lo sftunnel non era attivo per tali dispositivi.

Per correggere lo sftunnel per le connessioni non riuscite, eseguire la procedura seguente:

1. Dalla CLI di FMC, aprire il file FAILED_PUSH utilizzando cat /var/tmp/certs/1728303362/FAILED_PUSH (il valore numerico rappresenta l'ora univoca, quindi controllare l'output del comando precedente nel sistema) nel formato successivo: FTD_UUID NOME_FTD FTD_IP PERCORSO_ORIGINE SU FMC PERCORSO_DESTINAZIONE SU FTD

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/tmp/certs/1728915794/FAILED_PUSH

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

PUSH_NON RIUSCITO

2. Trasferire i nuovi certificati (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) dal FMC ai dispositivi FTD
   ===Approccio automatico==

   L'installazione dell'aggiornamento rapido fornisce inoltre gli script copy_sftunnel_certs.py e copy_sftunnel_certs_jumpserver.py che automatizzano il trasferimento dei vari certificati ai sistemi per cui sftunnel non era attivo durante la rigenerazione dei certificati. Questa opzione può essere utilizzata anche per i sistemi con una connessione sftunnel interrotta perché il certificato è già scaduto.

   È possibile utilizzare lo script copy_sftunnel_certs.py quando il CCP stesso ha accesso SSH

ai vari sistemi FTD. In caso contrario, è possibile scaricare lo script (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) dal CCP su un server di collegamento che disponga di accesso SSH ai CCP e ai dispositivi FTD ed eseguire lo script Python da tale server. Se anche questo non è possibile, consigliare di eseguire l'approccio manuale indicato di seguito. Negli esempi seguenti viene illustrato lo script copy_sftunnel_certs.py in uso, ma i passaggi sono gli stessi per lo script copy_sftunnel_certs_jumpserver.py.

A. Creare un file CSV sul FMC (o sul server di collegamento) contenente le informazioni sul dispositivo (nome_dispositivo, indirizzo IP, nome_utente_amministratore, password_amministratore) usate per stabilire la connessione SSH.

Quando si esegue questa operazione da un server remoto come un server di collegamento per il CCP primario, assicurarsi di aggiungere i dettagli del CCP primario come prima voce, seguita da tutti i CCP gestito e secondario. Quando si esegue questa operazione da un server remoto come un server di collegamento per un FMC secondario, assicurarsi di aggiungere i dettagli del FMC secondario come prima voce seguita da tutti i FTD gestiti.

i. Creare un file utilizzando vi devices.csv.

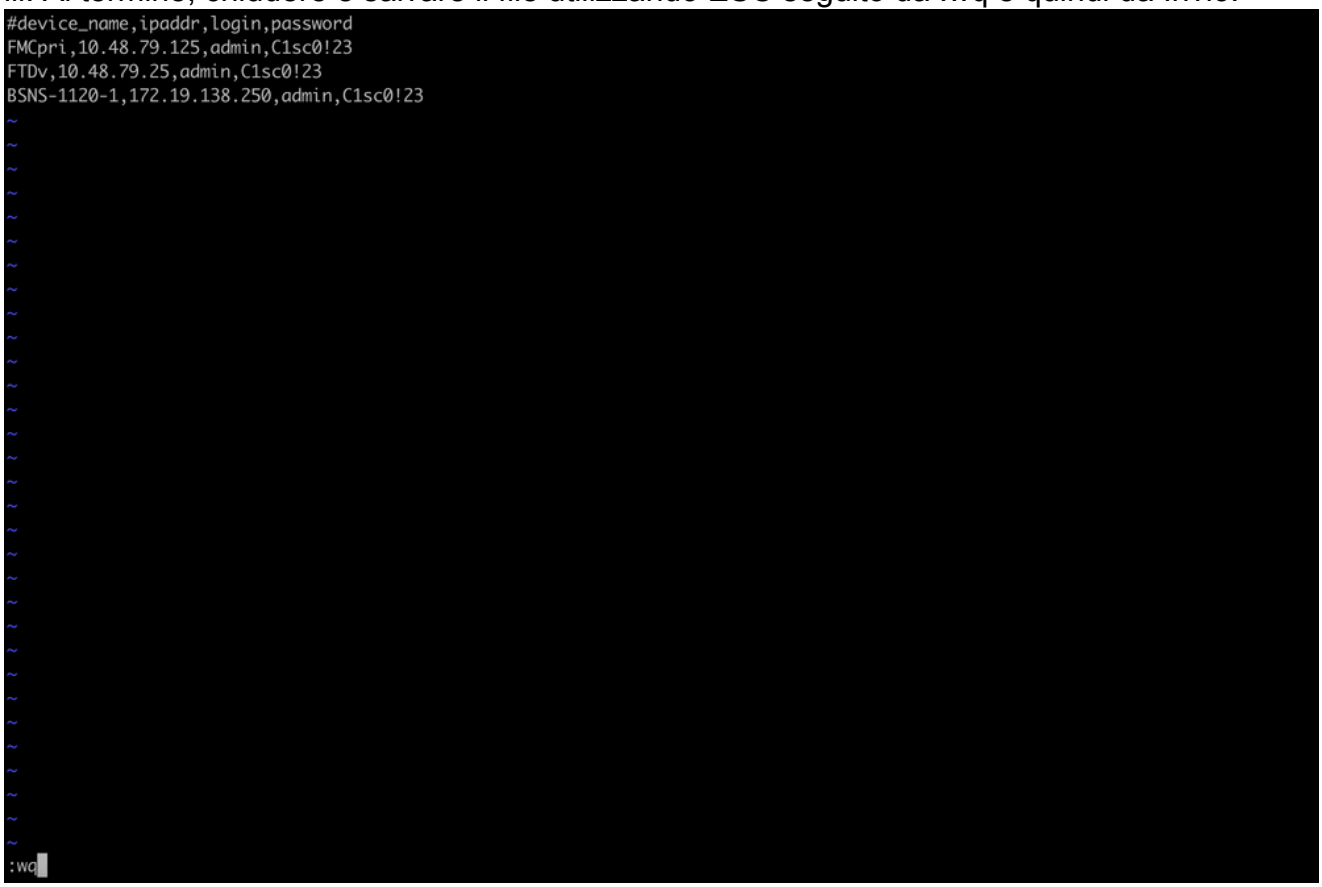
```
root@firepower:/Volume/home/admin# vi devices.csv
```

vi devices.csv

ii. In questo modo si apre il file vuoto (non visualizzato) e si inseriscono i dettagli come mostrato dopo aver utilizzato i caratteri sulla tastiera per passare alla modalità INTERATTIVA (visibile nella parte inferiore dello schermo).

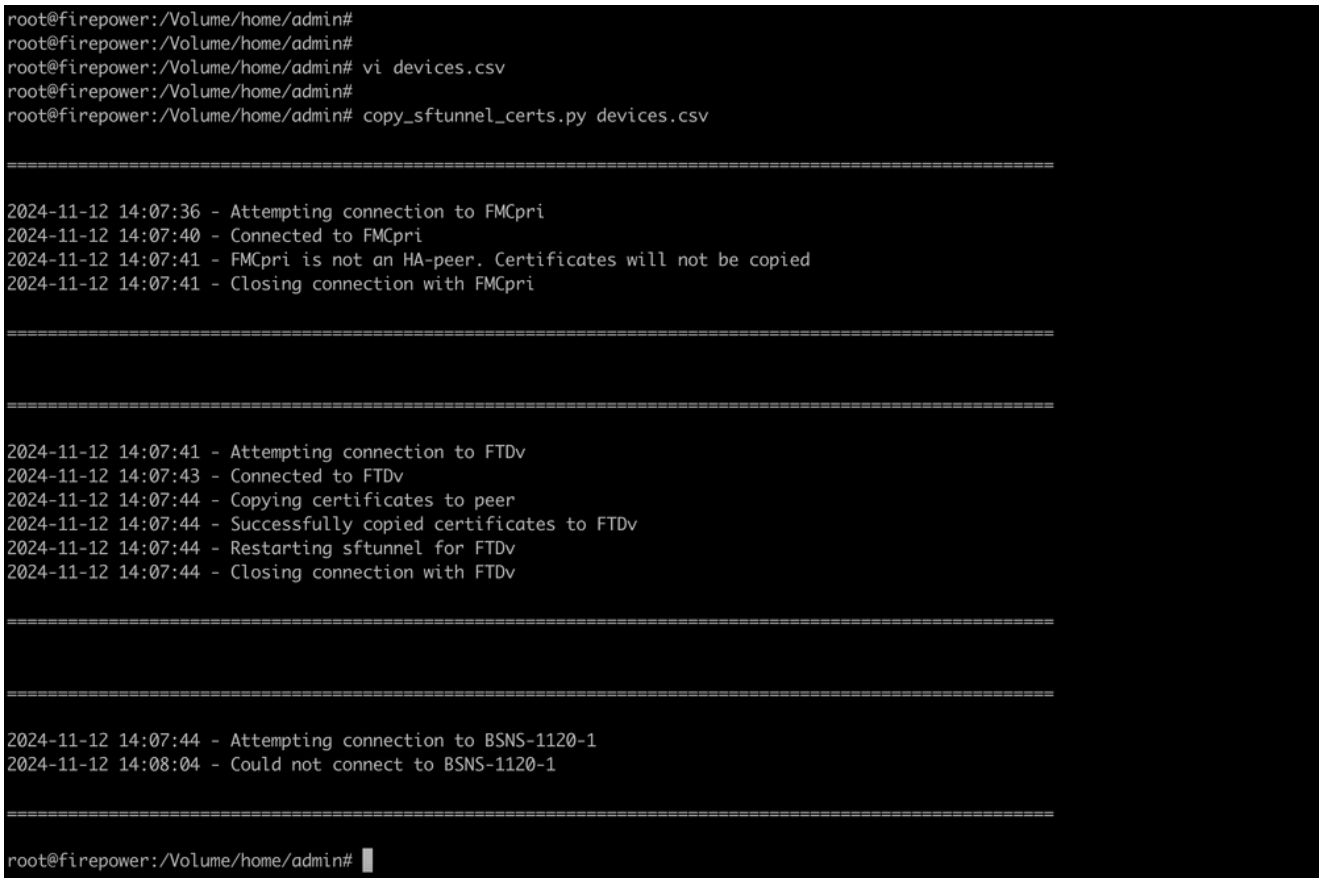
esempio di devices.csv

iii. Al termine, chiudere e salvare il file utilizzando ESC seguito da :wq e quindi da Invio.



Salvare il file devices.csv

B. Eseguire lo script (dalla directory principale utilizzando sudo) con copy_sftunnel_certs.py devices.csv e viene visualizzato il risultato. Qui mostra che il certificato per FTDv è stato inserito correttamente e che per BSNS-1120-1 non poteva effettuare la connessione SSH al dispositivo.



copy_sftunnel_certs.py dispositivi.csv

===Approccio manuale==

1. Stampa (cat) l'output di ciascuno dei file di ciascun FTD interessato (cacert.pem / sftunnel-key.pem (non visualizzato completamente per motivi di sicurezza) / sftunnel-cert.pem) sulla CLI di FMC copiando il percorso del file dall'output precedente (file 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
```

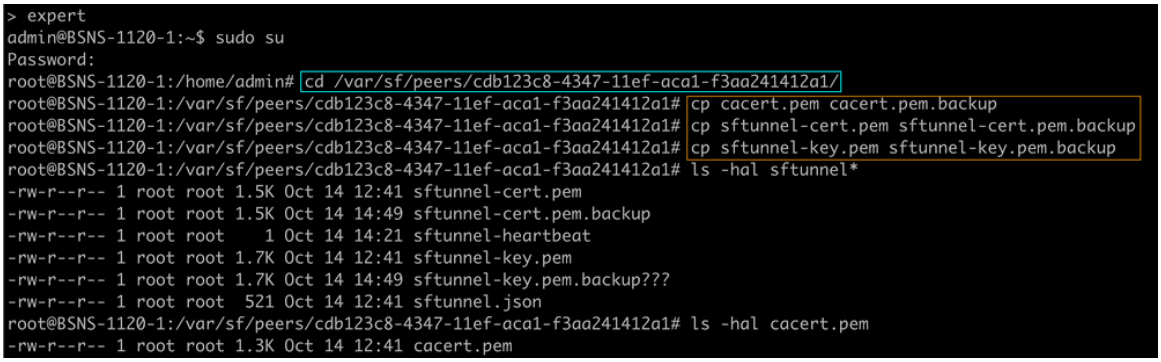
sftunnel-key.pem

```
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. Aprire la CLI FTD di ciascun FTD in modalità Expert con privilegi root tramite sudo su e rinnovare i certificati con la procedura successiva.
    1. Individuare la posizione visualizzata nella luce blu chiara dell'output FAILED_PUSH (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 ad esempio, ma questa è diversa per ogni FTD).
    2. Eseguire il backup dei file esistenti.

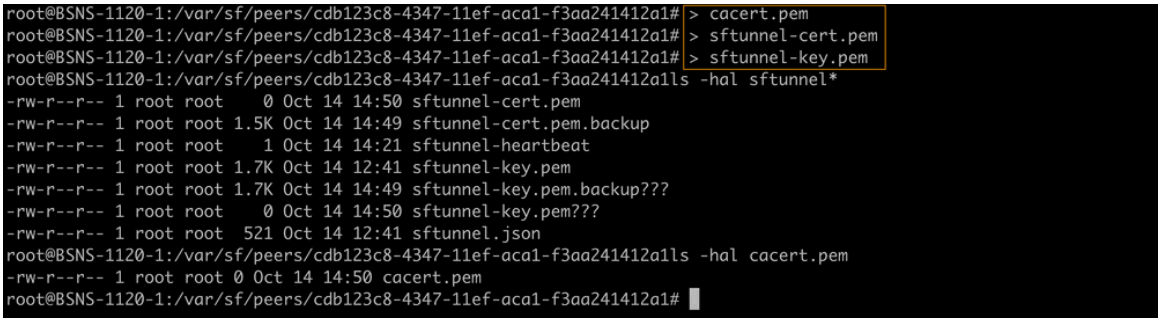
```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```



Esegui backup dei certificati correnti

3. Svuotare i file in modo che sia possibile scrivere nuovo contenuto al loro interno.

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



Contenuto vuoto dei file di certificato esistenti

4. Scrivere il nuovo contenuto (dall'output FMC) in ciascuno dei file singolarmente utilizzando vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (comando separato per file - gli screenshot mostrano questo solo per cacert.pem ma devono essere ripetuti per sftunnel-cert.pem e sftunnel-key.pem).

vi cacert.pem

1. Premere i per passare alla modalità interattiva (dopo l'immissione del comando vi viene visualizzato un file vuoto).
2. Copiare e incollare l'intero contenuto (inclusi —BEGIN CERTIFICATE— e —END CERTIFICATE—) nel file.

Copiare il contenuto in vi (modalità INSERT)

3. Chiudere e scrivere nel file con ESC seguito da :wq e quindi immettere.

ESC seguito da :wq per scrivere nel file

5. Verificare che le autorizzazioni corrette (chmod 644) e i proprietari (chown root:root) siano impostati per ogni file utilizzando ls -hal. L'impostazione è corretta quando si aggiorna il file esistente.

```
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#
```

Tutti i file di certificato aggiornati con i proprietari e le autorizzazioni corretti

3. Riavviare il sftunnel su ciascun FTD in cui il sftunnel non era operativo per rendere effettive le modifiche nel certificato con il 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. Verificare che tutti i FTD siano collegati correttamente utilizzando l'output sftunnel_status.pl

Soluzione 2 - Il certificato è già scaduto

In questa situazione, abbiamo due diversi scenari. Tutte le connessioni sftunnel sono ancora operative oppure non sono più (o sono parziali).

FTD ancora connessi tramite sftunnel

È possibile applicare la stessa procedura indicata nella sezione Certificato non ancora scaduto (scenario ideale) - Metodo consigliato.

Tuttavia, NON aggiornare o riavviare il FMC (o qualsiasi FTD) in questa situazione in quanto

disconnette tutte le connessioni sftunnel e dobbiamo eseguire manualmente tutti gli aggiornamenti dei certificati su ogni FTD. L'unica eccezione è rappresentata dalle versioni degli aggiornamenti rapidi elencate, che non richiedono il riavvio del FMC.

Le gallerie restano collegate e i certificati sono sostituiti su ciascuno FTD. Nel caso in cui alcuni certificati non possano essere compilati, viene richiesto se si sono verificati errori ed è necessario adottare l'approccio manuale indicato in precedenza nella sezione precedente.

FTD non più connessi tramite sftunnel

Approccio consigliato

È possibile applicare la stessa procedura indicata nella sezione Certificato non ancora scaduto (scenario ideale) - Metodo consigliato. In questo scenario, il nuovo certificato verrà generato nel FMC ma non potrà essere copiato nei dispositivi perché il tunnel è già inattivo. Questo processo può essere automatizzato con gli script copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py

Se tutti i dispositivi FTD sono scollegati dal CCP, è possibile aggiornare il CCP in questa situazione in quanto non ha alcun impatto sulle connessioni del tunnel. Se si dispone ancora di alcuni dispositivi connessi tramite sftunnel, tenere presente che l'aggiornamento della console Gestione configurazione FMC chiude tutte le connessioni sftunnel e che tali dispositivi non vengono visualizzati di nuovo a causa del certificato scaduto. Il vantaggio di questo aggiornamento è che fornisce una buona guida sui file di certificato che devono essere trasferiti a ciascuno degli FTD.

Approccio manuale

In questo caso, è possibile eseguire lo script generate_certs.pl dal FMC che genera i nuovi certificati, ma è comunque necessario eseguirne il push manualmente in ciascun dispositivo FTD. A seconda della quantità di dispositivi, questa operazione è fattibile o può essere noiosa. Tuttavia, quando si utilizzano gli script copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py, questa operazione è altamente automatizzata.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).