تجديد شهادة FMC Sftunnel CA لاتصال FTD

المحتويات

المقدمة

يصف هذا المستند تجديد شهادة المرجع المصدق (CA) لمركز إدارة FirePOWER (FMC) فيما يتعلق باتصال "الدفاع عن تهديد جدار الحماية (FTD)".

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Firepower Threat Defense
- مركز إدارة Firepower
- البنية الأساسية للمفتاح العام (PKI)

المكونات المستخدمة

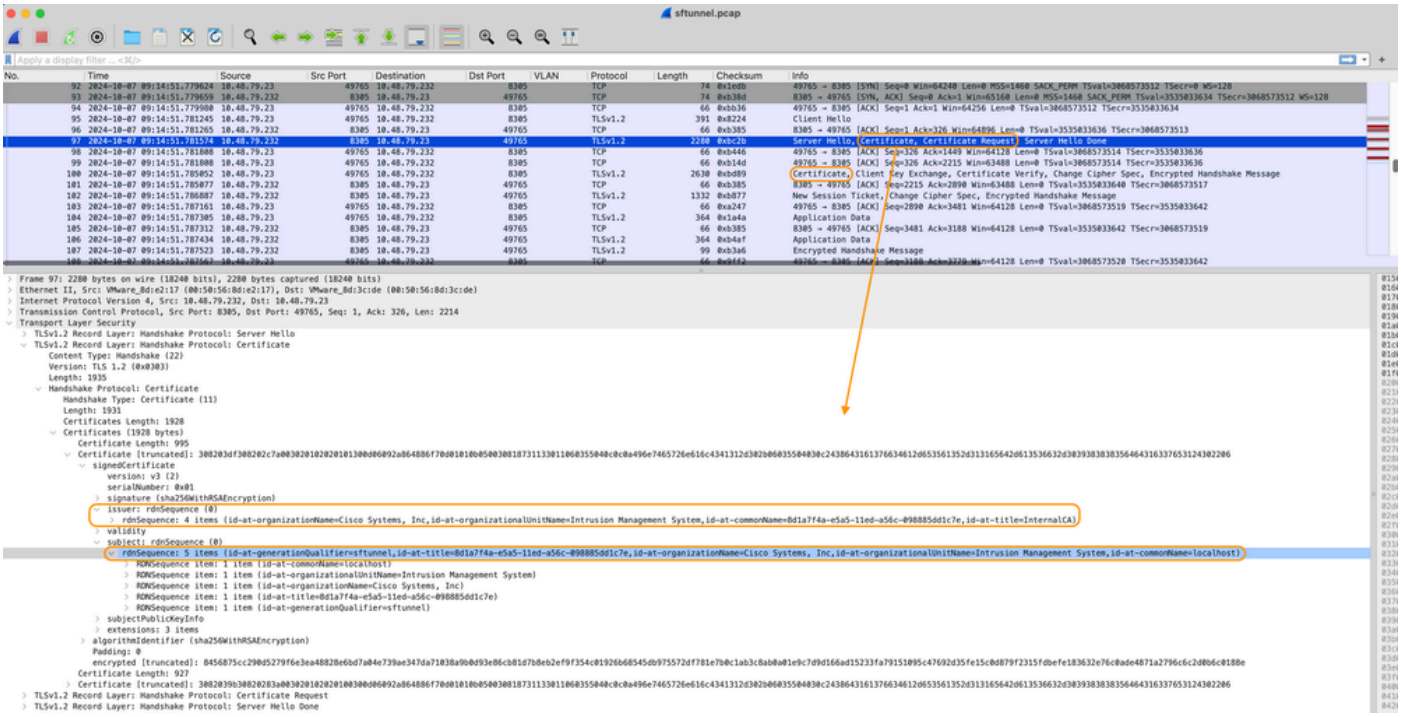
لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

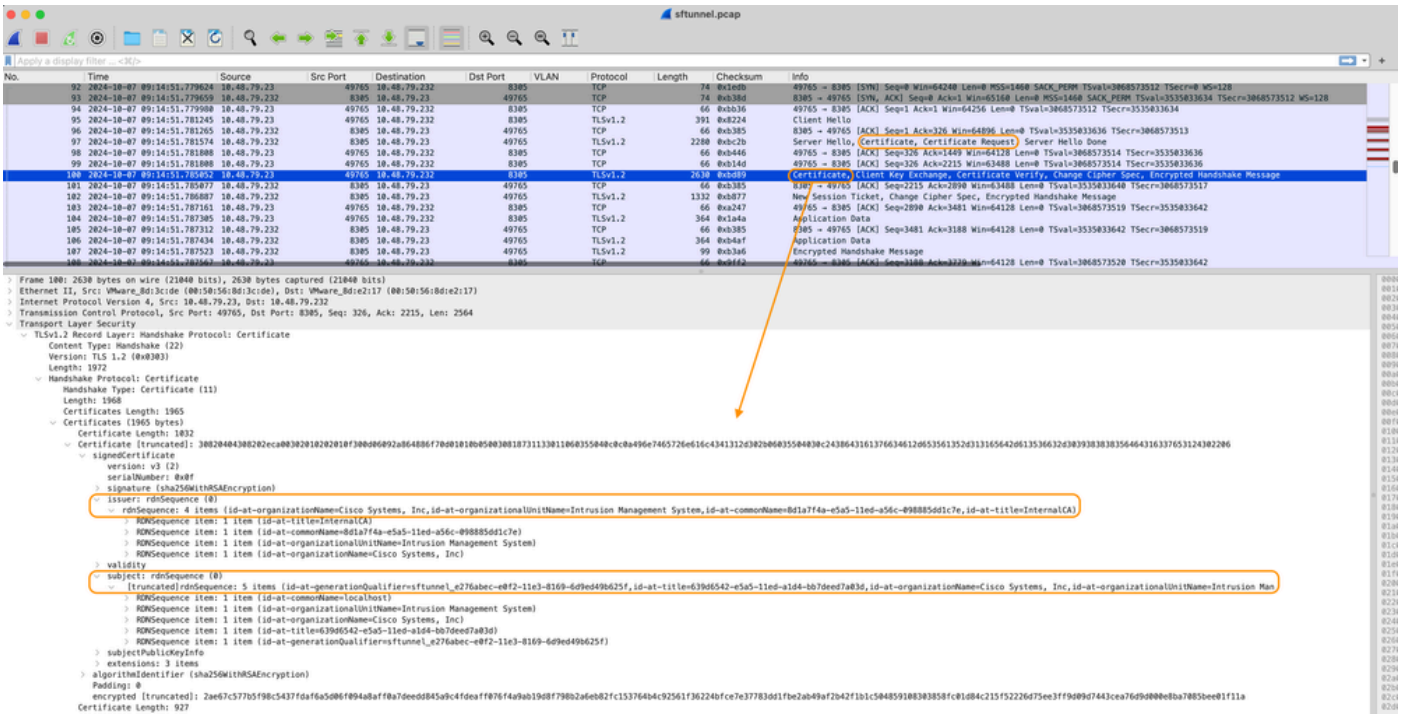
معلومات أساسية

تتصل FMC و FTD مع كل مفتاح عبر SFTUNNEL (نفق Sourcefire). يستخدم هذا الاتصال الشهادات لجعل المحادثة آمنة عبر جلسة TLS. يمكن العثور على مزيد من المعلومات حول كيفية إنشاء SFtunnel [على هذا الارتباط].

من التقاط الحزمة، أنت يستطيع رأيت أن ال FMC (10.48.79.232 في هذا مثال) و FTD (10.48.79.23) يتبادل شهادات مع كل آخر. وهم يفعلون ذلك للتأكد من أنهم يتحدثون مع الجهاز الصحيح، وليس هناك أي تنصت أو هجوم ضد "الدخيل". يتم تشفير الاتصال باستخدام هذه الشهادات، والطرف الذي لديه المفتاح الخاص المقترن لتلك الشهادة فقط هو الذي يمكنه فك تشفيرها مرة أخرى.



CERTIFICATE_EXCHANGE_SERVER_CERT



CERTIFICATE_EXCHANGE_CLIENT_CERT

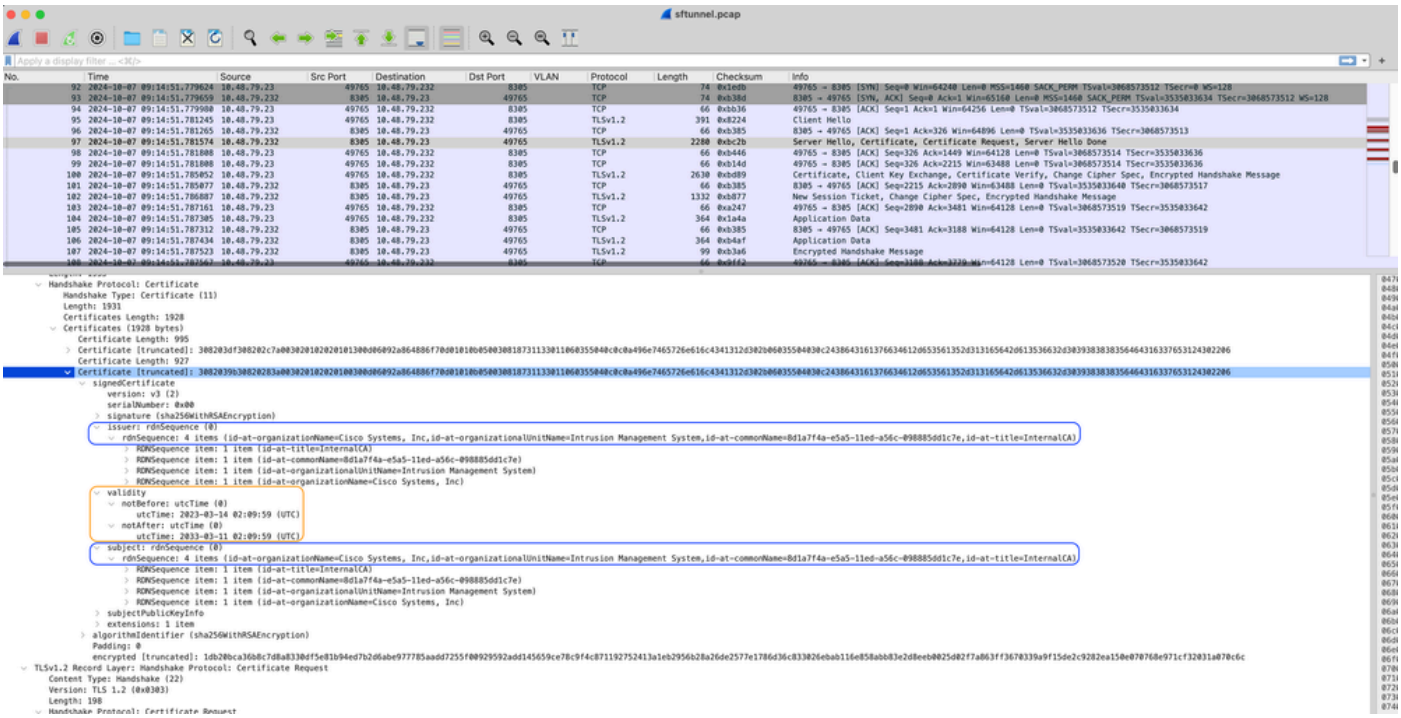
يمكنك أن ترى أن الشهادات موقعة من قبل نفس المرجع المصدق الداخلي (المصدر) الذي تم إعداده على نظام FMC. يتم تحديد التكوين على وحدة التحكم في إدارة اللوحة الأساسية (FMC) في الملف /etc/sf/sftunnel.conf الذي يحتوي على ما يلي:

```
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;
};
```

وهذا يشير إلى المرجع المصدق الذي يتم إستخدامه لتوقيع جميع الشهادات ل sftunnel (كل من FTD و FMC one) والشهادة التي تستخدمها FMC لإرسال إلى جميع FTDs. تم توقيع هذه الشهادة من قبل InternalCA.

عندما يقوم FTD بالتسجيل إلى FMC، تقوم FMC أيضا بإنشاء شهادة للدفع إلى جهاز FTD يتم إستخدامها لمزيد من الاتصال على FTTUNNEL. هذه الشهادة موقعة أيضا بنفس شهادة CA الداخلية. على FMC، يمكنك العثور على تلك الشهادة (والمفاتيح الخاص) تحت /var/sf/peers/<UUID-FTD-device>وتحتمل أن تكون أسفل مجلد certs_pushed وتسمى sftunnel-cert.pem (sftunnel-key.pem للمفاتيح الخاص). في FTD، يمكنك العثور على الأجهزة الموجودة تحت /var/sf/peers/<UUID-FMC-device>ذات اصطلاح التسمية نفسه.

بيد أن لكل شهادة أيضا فترة صلاحية لأغراض الضمان. عند فحص شهادة InternalCA، يمكننا أن نرى أيضا فترة الصلاحية وهي 10 سنوات ل FMC InternalCA كما هو موضح من التقاط الحزمة.

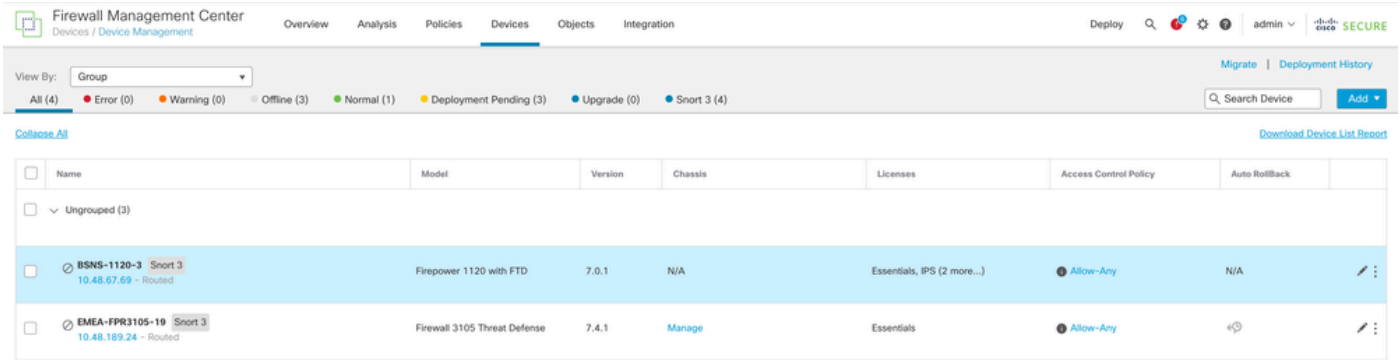


صلاحية FMC-InternalCA_VALIDITY

المشكلة

شهادة FMC InternalCA صالحة لمدة 10 سنوات فقط. بعد وقت انتهاء الصلاحية، لم يعد النظام البعيد يثق في هذه الشهادة بعد الآن (بالإضافة إلى الشهادات الموقعة منها) وهذا يؤدي إلى حدوث مشاكل في اتصال FastTunnel بين أجهزة FTD و FMC. وهذا يعني أيضا أن العديد من الوظائف الأساسية مثل أحداث الاتصال وعمليات البحث عن البرامج الضارة والقواعد المستندة إلى الهوية وعمليات نشر السياسات والعديد من الأشياء الأخرى لا تعمل.

تظهر الأجهزة معطلة على واجهة مستخدم FMC ضمن الأجهزة > عالمة تبويب إدارة الأجهزة عندما يكون Sftunnel غير متصل. يتم تعقب الإصدار الذي يتعلق بانتهاء صلاحية هذا على معرف تصحيح الأخطاء من Cisco CSCwd08098. لاحظ أن جميع الأنظمة تتأثر، حتى عند تشغيل إصدار ثابت من العيب. تم العثور على مزيد من المعلومات حول هذه الإصلاح في قسم "الحل".



الأجهزة المعطلة

لا تقوم FMC بتحديث CA تلقائيا وإعادة نشر الشهادات إلى أجهزة FTD. كما لا يوجد أي تنبيه صحي FMC يشير إلى انتهاء صلاحية الشهادة. يتم تعقب معرف تصحيح الأخطاء

من Cisco CSCwd08448 في هذا الصدد لتوفير تنبيه صحة على واجهة مستخدم FMC في المستقبل.

ماذا يحدث بعد تاريخ انتهاء الصلاحية؟

مبدئيا ما يصير شي وتستمر قنوات الاتصال متل ما كانت. ومع ذلك، عند قطع اتصال FTD بين أجهزة FMC و FTD ويحاول إعادة إنشاء الاتصال، فإنه يفشل ويمكنك ملاحظة أسطر السجل في ملف سجل الرسائل الذي يشير إلى انتهاء صلاحية الشهادة.

تسجيل الخطوط من جهاز FTD من /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 faile
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ssl [WARN] SSL Verification status: ce
```

تسجيل الخطوط من جهاز FMC من /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: Faile
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: Faile
```

قد يتم قطع اتصال SfTunnel لأسباب مختلفة:

- فقد الاتصال بسبب فقدان الاتصال بالشبكة (قد يكون هذا الاتصال مؤقتا فقط)
- إعادة تمهيد FTD أو FMC
  - المتوقع منها: إعادة التشغيل اليدوية والترقيات وإعادة التشغيل اليدوي لعملية SFTUNNEL على FMC أو FTD (على سبيل المثال بواسطة PMTOOL restartbyid sftunnel)
  - غير متوقعين: خطوط خلفية، انقطاع التيار الكهربائي

نظرا لوجود العديد من الاحتمالات التي يمكنها قطع اتصال SFtunnel، فمن المستحسن تصحيح الموقف بأسرع ما يمكن، حتى في الوقت الحالي الذي تكون فيه جميع أجهزة FTD

متصلة بشكل صحيح بالرغم من الشهادة منتهية الصلاحية.

كيف يمكنك التحقق بسرعة من انتهاء صلاحية الشهادة أو تاريخ انتهاء صلاحيتها؟

أسهل طريقة هي تشغيل هذه الأوامر على جلسة FMC SSH:

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

يظهر لك هذا عناصر الصحة من الشهادة. الجزء الرئيسي ذو الصلة هنا هو "notAfter" الذي يظهر أن الشهادة هنا صالحة حتى 5 تشرين الأول/أكتوبر 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
```

ليس بعد

إذا كنت تفضل تشغيل أمر واحد يمنحك على الفور مقدار الأيام التي لا تزال الشهادة صالحة لها، يمكنك إستخدام هذا:

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

يتم عرض مثال على إعداد حيث لا تزال الشهادة صالحة لعدة سنوات.

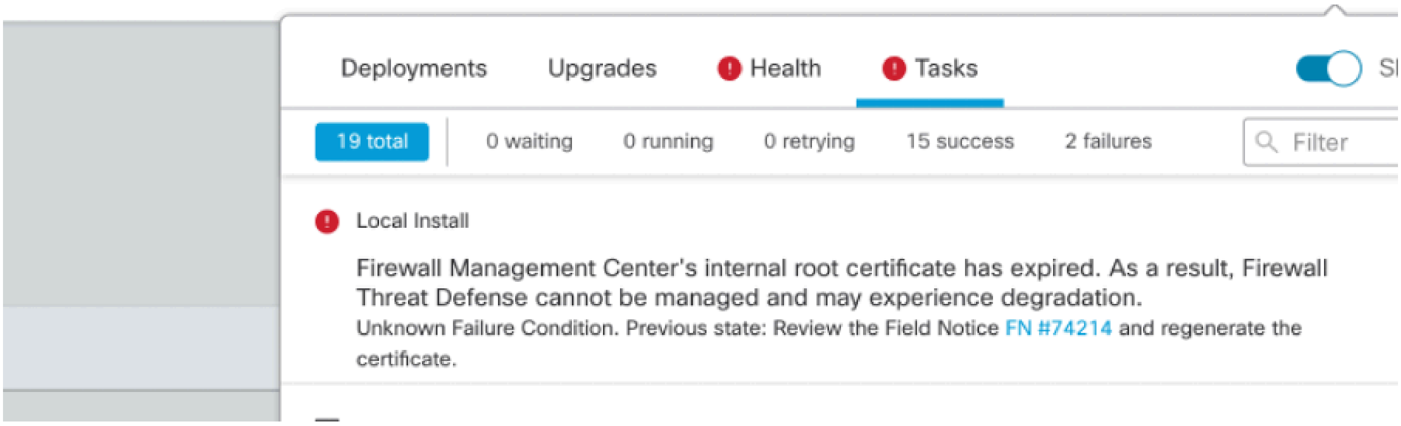
```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -e
nddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE
_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS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

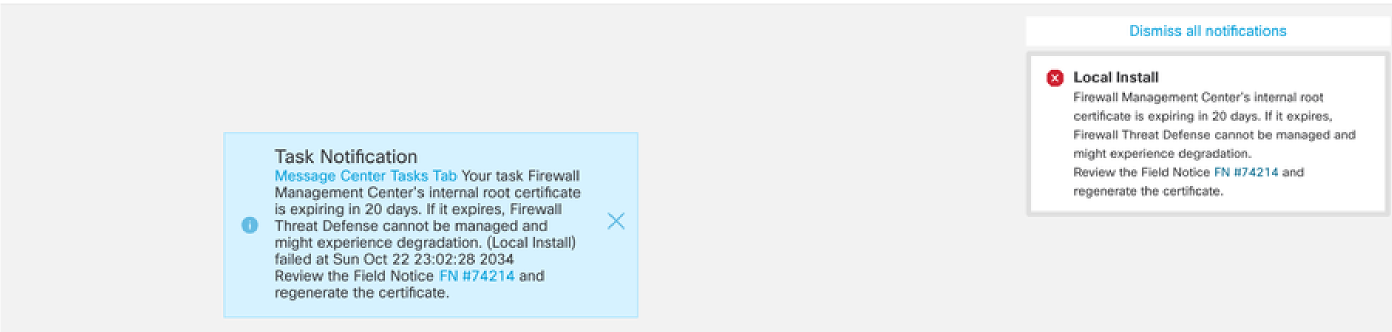
كيف يتم إعلامي في المستقبل حول انتهاء صلاحية الشهادة القادمة؟

مع تحديثات VDB الأخيرة (399 أو أعلى)، يتم تنبيهك تلقائيا عندما تنتهي صلاحية شهادتك في غضون 90 يوما. لذلك أنت لا تحتاج أن تتبع يدويا على هذا بنفسك كما تنبه عندما تكون قريب من وقت انتهاء الصلاحية. يظهر هذا بعد ذلك على صفحة ويب FMC في نموذجين. يشير كلا الطريقتين إلى صفحة إشعار الحقل.

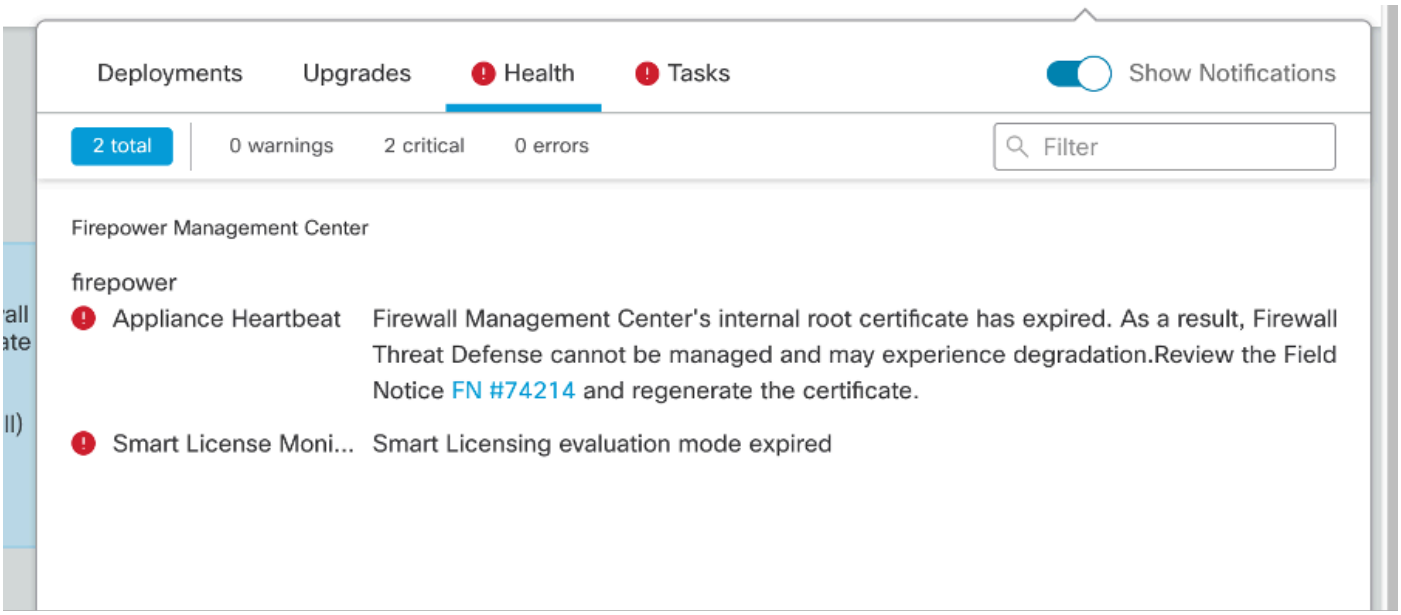
الطريقة الأولى هي من خلال علامة تبويب مهمة. هذه الرسالة ملصقة ومتاحة للمستخدم ما لم يتم إغلاقها بشكل صريح. يظهر الإخطار أيضا ويكون متاحا حتى يتم إغلاقه بشكل صريح من قبل المستخدم. تظهر دائما كخطأ.



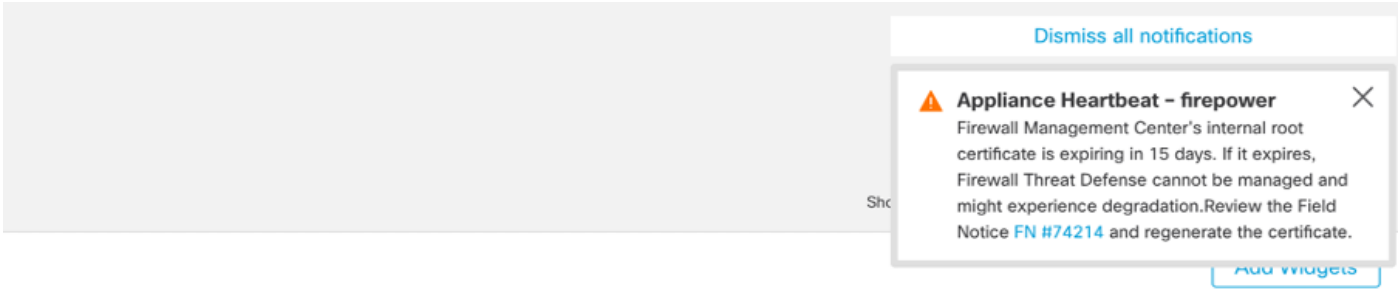
إعلام انتهاء الصلاحية في علامة تبويب المهمة



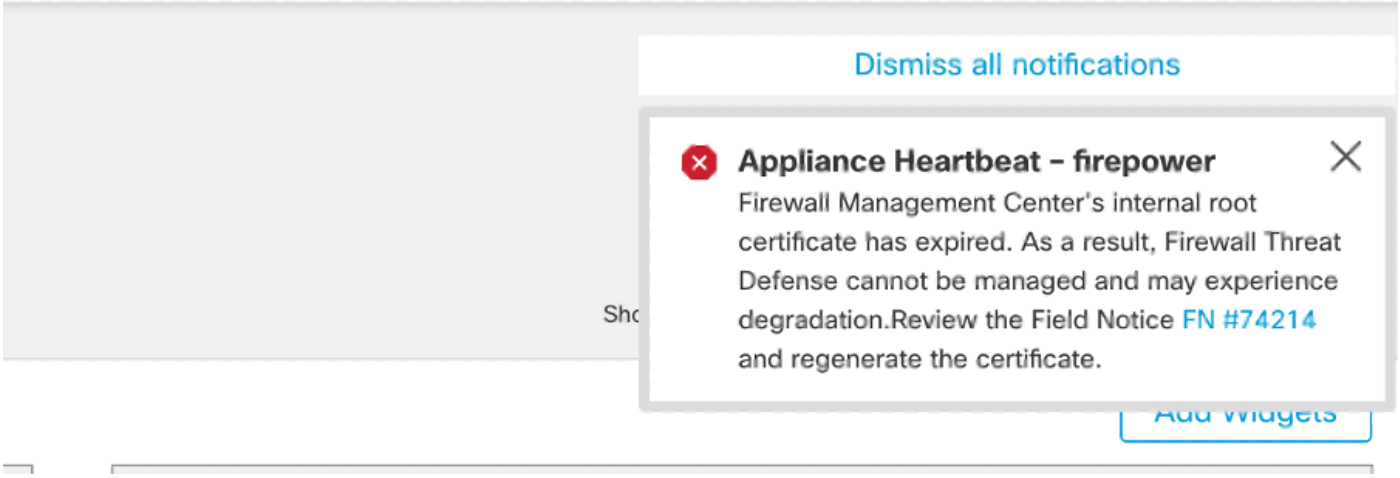
الطريقة الثانية هي من خلال تنبيه الصحة. يظهر هذا في علامة التبويب "صحة" على أي حال، هذا غير جزء ويستبدل أو يزيل عندما يتم تشغيل "مراقبة الحماية" والتي تكون كل 5 دقائق بشكل افتراضي. كما يعرض أيضا إخطارا منبثق يجب إغلاقه بشكل صريح من قبل المستخدم. يمكن أن يظهر هذا كخطأ (عندما تنتهي صلاحيته) كتحذير (عندما تنتهي صلاحيته).



إعلام انتهاء الصلاحية في علامة التبويب "صحة"



إعلام تحذير منبثق للتنبيه الصحي



الإعلام بالخطأ في قائمة التنبيه الخاص بالصحة المنبثقة

الحل 1 - لم تنته صلاحية الشهادة بعد (السيناريو المثالي)

هاد أحلى موقف على حسب انتهاء صلاحية الشهادة ومع هيك عنا وقت. إما أن تتبنى المنهج الأوتوماتيكي الكامل (الموصى به) الذي يعتمد على نسخة FMC أو أن تتبع نهج يدوي أكثر يتطلب تفاعل TAC.

نهج موصى به

هذا هو الوضع الذي ال يتوقع فيه في الظروف العادية أي وقت للانتهاء من العمل أو أقل قدر من العمليات اليدوية.

قبل المتابعة، يجب تثبيت الإصلاح العاجل لإصدارك المحدد كما هو مدرج هنا. الميزة هنا هي أن هذه الإصلاحات العاجلة ال تتطلب إعادة تشغيل FMC وبالتالي إمكانية قطع اتصال SfTunnel عند انتهاء صلاحية الشهادة بالفعل. الإصلاحات العاجلة المتوفرة هي:

- 7. 0. 0 - 7. 0. 6 : Hotfix FK - 7.0.6.99-9
- 7. 1.x : ال يوجد إصدار ثابت كنهاية لصيانة البرامج
- 7-2-0-7-2-9 : Hotfix FZ - 7.2.9.99-4
- 7. 3.x : AE - 7.3.1.99-4
- 7-4-0-7-4-2 : Hotfix AO - 7.4.2.99-5
- 7.6.0 : الإصلاح العاجل B - 7.6.0.99-5

بمجرد تثبيت الإصلاح العاجل، يجب أن تحتوي FMC الآن على البرنامج النصي generate_certs.pl الذي:

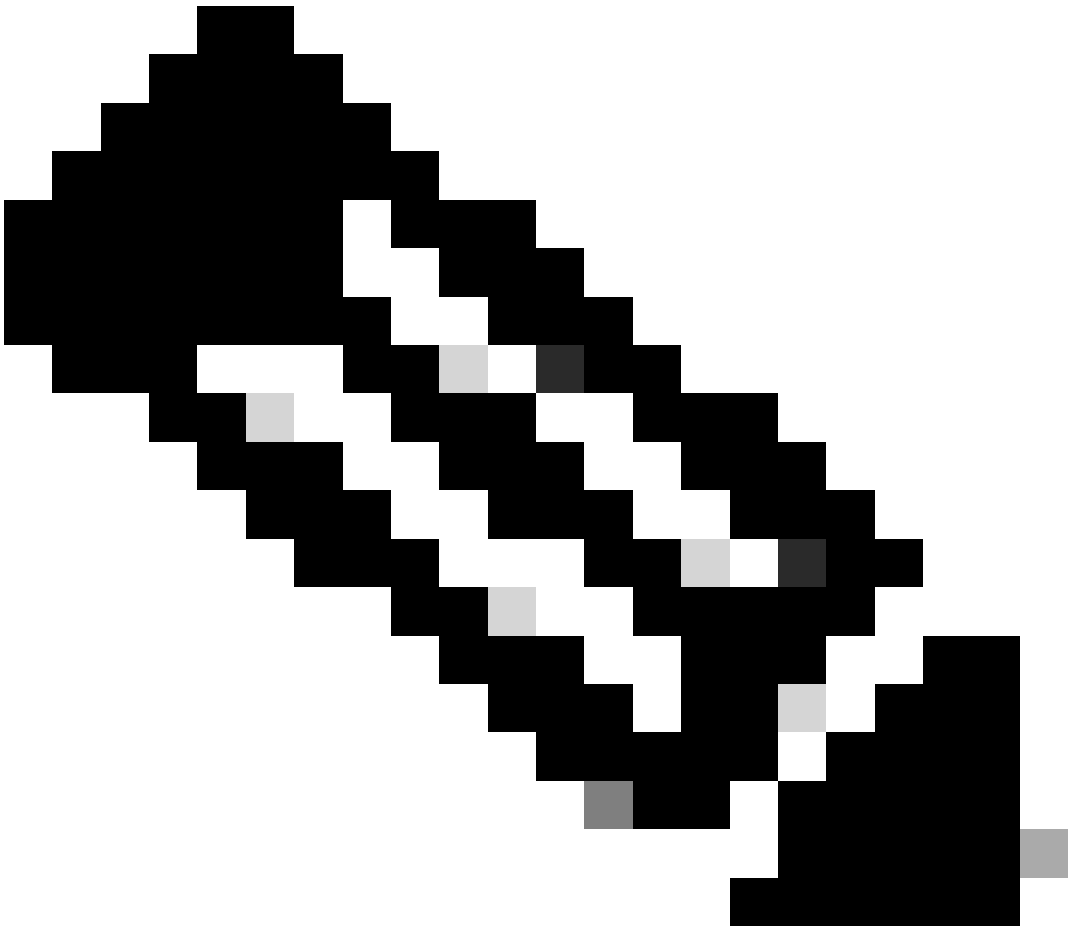
1. إعادة إنشاء InternalCA
2. إعادة إنشاء شهادات sftunnel الموقعة من قبل InternalCA الجديد
3. يدفع شهادات sftunnel الجديدة والمفاتيح الخاصة إلى أجهزة FTD المعنية (عند تشغيل SFTTUNNEL)

ولذلك يوصى (إن أمكن) بما يلي:

1. تثبيت الإصلاح العاجل القابل للتطبيق أعلاه
2. احصل على نسخة احتياطية من وحدة التحكم في إدارة اللوحة الأساسية (FMC)
3. التحقق من صحة جميع اتصالات sftunnel الحالية باستخدام البرنامج النصي sftunnel_status.pl على FMC (من وضع الخبير)
4. تشغيل البرنامج النصي من وضع الخبير باستخدام generate_certs.pl
5. فحص النتيجة للتحقق من ما إذا كانت هناك حاجة إلى أي عمليات يدوية (عندما ال تكون الأجهزة متصلة بوحدة التحكم في إدارة الهيكل (FMC)) [يتم شرح ذلك أدناه بشكل إضافي]
6. قم بتشغيل sftunnel_status.pl من FMC للتحقق من أن جميع اتصالات sftunnel تعمل بشكل جيد

```
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#
```

إنشاء_certs.pl برمجية



ملاحظة: عندما يكون لديك FMC يعمل في حالة توفر عال (HA)، يلزمك إجراء العملية الوأ على العقدة الأساسية ثم على العقدة الثانوية لأنها تستخدم هذه الشهادات أيضا للاتصال بين عقد FMC. يختلف CA الداخلي على كل عقدتي FMC.

على المثال هنا ترى أنه ينشئ ملف سجل على /var/log/sf/sfca_generation.log، ويشير إلى إستخدام sftunnel_status.pl، ويشير إلى قوة انتهاء الصلاحية على InternalCA ويشير إلى أي حالات فشل عليه. هنا على سبيل المثال، فشل في دفع الشهادات إلى جهاز BSNS-1120-1 وجهاز EMEA-FPR3110-08، المتوقع أن يكون بسبب تعطل SFTUNNEL لتلك الأجهزة.

من أجل تصحيح SFtunnel للاتصالات الفاشلة، يمكنك تشغيل الخطوات التالية:

1. على FMC CLI، افتح الملف failed_PUSH باستخدام cat /var/tmp/certs/1728303362/failed_PUSH (تمثل قيمة الرقم وقت unix، لذلك تحقق من إخراج الأمر السابق في نظامك) الذي له التنسيق التالي: FTD_UUID FTD_NAME FTD_IP SOURCE_PATH_ON_FMC DESTINATION_PATH_ON_FTD

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

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

Failed_Push

2. قم بالتحويل عبر تلك الشهادات الجديدة (cacert.pem / sftunnel-key.pem / sftunnel-cert.pem) من وحدة التحكم FMC إلى أجهزة FTD
====النهج التلقائي====

كما يوفر تثبيت الإصلاح العاجل البرامج النصية copy_sftunnel_certs.py وcopy_sftunnel_certs_jumpserver.py التي تقوم بأتمتة نقل الشهادات المختلفة إلى الأنظمة التي لم يتم تشغيل SFTUNNEL لها أثناء إعادة إنشاء الشهادات. كما يمكن إستخدام هذا النظام للنظم التي تم قطع اتصال Sftunnel بها نظرا لانتهاء صلاحية الشهادة بالفعل.

يمكنك إستخدام البرنامج النصي copy_sftunnel_certs.py عندما يكون لوحدة التحكم FMC نفسها وصول SSH إلى أنظمة FTD المختلفة. إذا لم يكن هذا هو الحال، يمكنك تنزيل البرنامج النصي (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py) من FMC إلى خادم الانتقال السريع الذي لديه وصول SSH إلى كل من أجهزة FMC (FTD) و FTD

وتشغيل البرنامج النصي Python من هناك. وإذا لم يكن ذلك ممكنا أيضا، فاقترح تطبيق النهج اليدوي الذي يظهر بعد ذلك. تظهر الأمثلة التالية النص البرمجي copy_sftunnel_certs.py الذي يتم إستخدامه، لكن الخطوات هي نفسها للنص copy_sftunnel_certs_jumpserver.py.

أ. قم بإنشاء ملف CSV على FMC (أو خادم الانتقال السريع) الذي يحتوي على معلومات الجهاز (device_name، عنوان IP، admin_username، admin_password) التي يتم إستخدامها لإنشاء اتصال SSH.

عندما تقوم بتشغيل هذا من خادم بعيد مثل خادم الانتقال السريع ل FMC أساسي، تأكد من إضافة تفاصيل FMC الأساسية كأول إدخال يليه كل FTD المدار و FMC الثانوي. عندما تقوم بتشغيل هذا من خادم بعيد مثل خادم الانتقال السريع ل FMC الثانوي، تأكد من إضافة تفاصيل FMC الثانوية كأول إدخال يليه كل FTD المدار.

ط. إنشاء ملف باستخدام vi devices.csv. 

أجهزة vi.csv

ثانيا. يؤدي ذلك إلى فتح الملف الفارغ (غير معروض) وتقوم بتعبئة التفاصيل كما هو موضح بعد إستخدام I Letter على لوحة المفاتيح للانتقال إلى الوضع التفاعلي (يظهر في أسفل الشاشة).

مثال devices.csv

ثالثا. عندما تنتهي تماما، توقف إلغاء وحفظ الملف باستخدام ESC يتبعه :wq ثم قم بإدخال.

حفظ الأجهزة.csv

ب. قم بتشغيل البرنامج النصي (من الجذر باستخدام sudo) باستخدام copy_sftunnel_certs.py devices.csv، وسيظهر لك الناتج. هنا يوضح أن الشهادة إلى FTDv قد تم دفعها بشكل صحيح وأنه لم يتمكن من إجراء اتصال SSH بالجهاز بالنسبة لـ BSNS-1120-1.

```
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

<u>====النهج اليدوي====</u>

1. قم بطباعة (cat) المخرجات لكل ملف من ملفات FTD المتأثرة (cacert.pem / sftunnel-key.pem (غير معروض بالكامل لأغراض الأمان) / sftunnel-cert.pem) على واجهة سطر أوامر (CLI) FMC عن طريق نسخ وقوع الملف من الإخراج السابق (ملف 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. افتح واجهة سطر أوامر (CLI) خاصة ب FTD على وضع خبير مع امتيازات جذر من خلال sudo su وتجديد الشهادات باستخدام الإجراء التالي.
   1. استعرض إلى الموقع الذي يظهر على إبراز الأزرق الفاتح من إخراج FAILED_PUSH (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 هنا على سبيل المثال ولكنه يختلف لكل FTD).
   2. إجراء عمليات نسخ إحتياطي للملفات الموجودة.

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

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

إجراء عمليات نسخ إحتياطي للشهادات الحالية

3. قم بإفراغ الملفات حتى نتمكن من كتابة محتوى جديد فيها.

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

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-cert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-key.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1ls -hal sftunnel*
-rw-r--r-- 1 root root    0 Oct 14 14:50 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root    1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root    0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root  521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1ls -hal cacert.pem
-rw-r--r-- 1 root root 0 Oct 14 14:50 cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

محتويات فارغة من ملفات الشهادات الموجودة

4. اكتب المحتوى الجديد (من إخراج FMC) في كل ملف على حدة باستخدام vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (الأمر المنفصل لكل ملف - ظهر لقطات الشاشة هذه فقط ل cacert.pem ولكن يلزم تكرار ه ل sftunnel-cert.pem و sftunnel-key.pem).

vi cacert.pem

1. اضغط i للانتقال إلى الوضع التفاعلي (بعد إدخال الأمر vi ورؤية ملف فارغ).
2. انسخ لصق المحتوى بأكمله (بما في ذلك —بدء الشهادة— و —نهاية الشهادة—) في الملف.

نسخ المحتوى في VI (وضع الإدراج)

3. قم بإغلاق الملف والكتابة إليه باستخدام ESC ثم :wq ثم أدخل.

ESC متبوعة ب: wq للكتابة إلى ملف

5. تحقق من أن الأذونات الصحيحة (chmod 644) والمالكين (الجذر:root) قد تم تعيينها لكل ملف باستخدام ls -hal. يتم تعيين هذا بشكل صحيح عند تحديث الملف الموجود.

```
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#
```

تم تحديث كافة ملفات الشهادات بواسطة المالكين المناسبين والأذونات

3. قم بإعادة تشغيل النفق على كل FTD خاص حيث لم يكن SFtunnel قيد التشغيل لتفعيل التغييرات في الشهادة باستخدام الأمر نفق Pmtool restartbyid

```
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#
```

نفق Pmtool restartbyid

3. تحقق من أن جميع ملفات FTD متصلة بشكل صحيح الآن باستخدام إخراج sftunnel_status.pl

الحل 2 - انتهت صلاحية الشهادة بالفعل

في هذه الحالة، لديك سيناريوهان مختلفان. إما أن جميع إتصالات SFTUNNEL لا تزال قيد التشغيل أو لم تعد تعمل (أو جزئية).

لا يزال FTDs متصل من خلال SFTUNNEL

يمكنك تطبيق الإجراء نفسه كما هو موضح في الشهادة التي لم تنته صلاحيتها بعد (السيناريو المثالي) - قسم النهج الموصى به.

عمو ذلك، ال تقوم بترقية أو إعادة تشغيل FMC (أو أي FTD) في هذه الحالة حيث أنها تقطع جميع إتصالات SFTUNNEL وتحتاج إلى تشغيل جميع تحديثات الشهادات يدويا على كل FTD. الاستثناء الوحيد لهذه الخطوة، وهو إصدارات "الإصلاح العاجل" المدرجة أدناه التي تتطلب إعادة تمهيد ل FMC.

ظل الأنفاق متصلة ويتم إستبدال الشهادات على كل واحد من FTD. في حالة فشل علم بعض الشهادات، فإنها تطلب منك الشهادات التي فشلت وتحتاج إلى اتباع النهج اليدوي كما هو مشار إليه سابقا في القسم السابق.

لم يعد FTDs متصلا من خلال sftunnel

نهج موصى به

يمكنني تطبيق الإجراء نفسه كما هو موضح في الشهادة التي لم تنتهي صلاحيتها بعد (السيناريو المثالي) - قسم النهج الموصى به. في هذا السيناريو، سيتم إنشاء الشهادة الجديدة على FMC ولكن ال يمكن نسخها إلى الأجهزة حيث إن النفق معطل بالفعل. يمكن أتمتة هذه العملية باستخدام النصوص التنفيذية copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py

إذا تم قطع اتصال جميع أجهزة FTD من FMC، يمكنني ترقية FMC في هذه الحالة لأنه ال يؤثر على إتصالات SFTTUNNEL. إذا كان ال يزال لديك بعض الأجهزة متصلة من خلال sftunnel، فكن على علم بأن ترقية FMC تغلق جميع إتصالات FMC والتي تأتي مرة أخرى بسبب الشهادة التي انتهت صلاحيتها. تتمثل فائدة الترقية هنا في أنها توفر لك إرشادا جيدا حول ملفات الشهادات التي يجب نقلها إلى كل ملف من ملفات FTD.

أسلوب يدوي

في هذه الحالة، يمكنك بعد ذلك تشغيل البرنامج النصي generate_certs.pl من FMC الذي يولد الشهادات الجديدة ولكن ال تزال بحاجة إلى دفعها إلى كل من أجهزة FTD يدويا. اعتمادا على كمية الأجهزة، يمكن القيام بذلك أو يمكن أن يكون مهمة مضنية. ومع ذلك عند إستخدام البرامج النصية copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py يكون هذا الأمر مؤتمتا للغاية.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).