FTD 연결을 위한 FMC Sftunnel CA 인증서 갱신

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

문제

- 만료일 이후에는 어떻게 됩니까?
- 인증서가 만료되었는지 또는 언제 만료되었는지 신속하게 확인하는 방법
- 향후 인증서 만료에 대한 알림을 받으려면 어떻게 해야 합니까?

솔루션 1 - 인증서가 아직 만료되지 않았습니다(이상적인 시나리오).

- 권장 접근 방식

솔루션 2 - 인증서가 이미 만료되었습니다.

- FTD가 sftunnel을 통해 계속 연결됨
- FTD가 sftunnel을 통해 더 이상 연결되지 않음
  - 권장 접근 방식
  - 수동 접근 방식

소개

이 문서에서는 FTD(Firepower Threat Defense) 연결과 관련된 FMC(Firepower Management Center) sftunnel CA(Certificate Authority) 인증서의 갱신에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 위협 방어
- Firepower 관리 센터
- PKI(Public Key Infrastructure)

사용되는 구성 요소

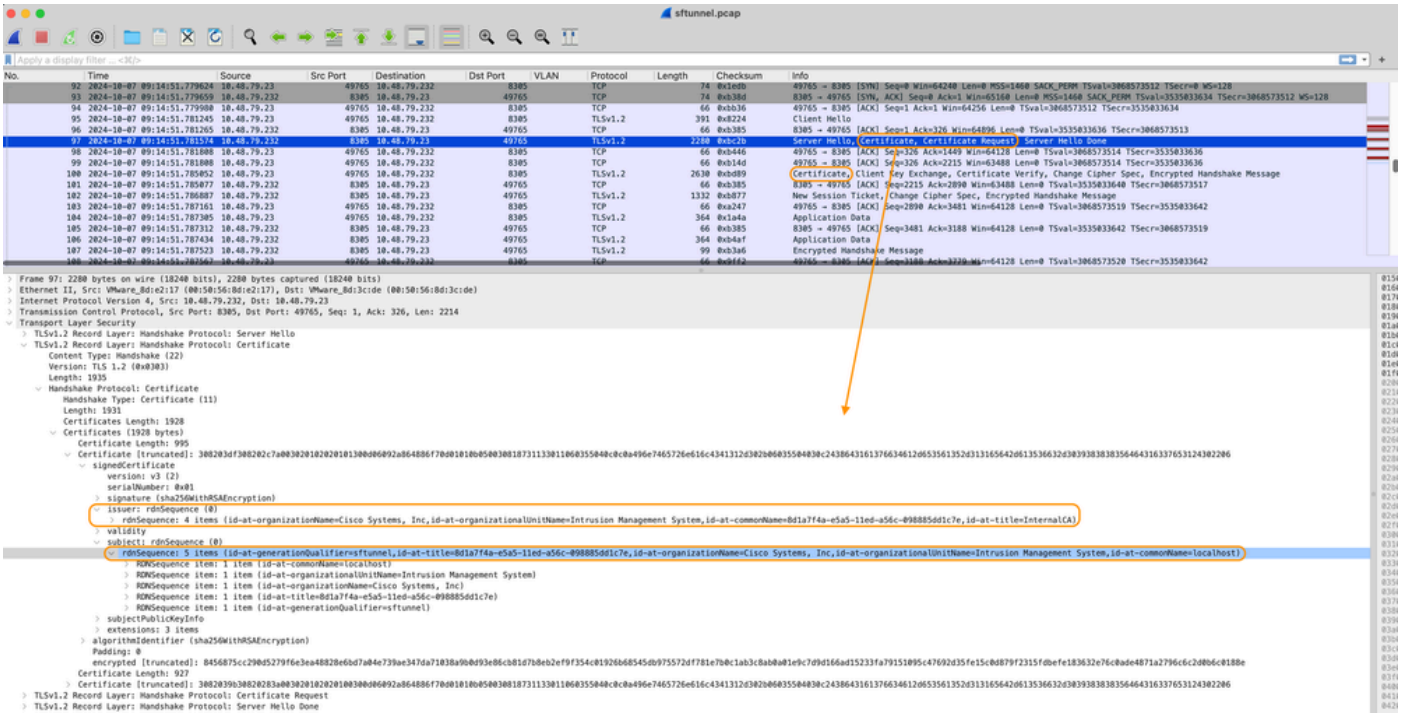
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

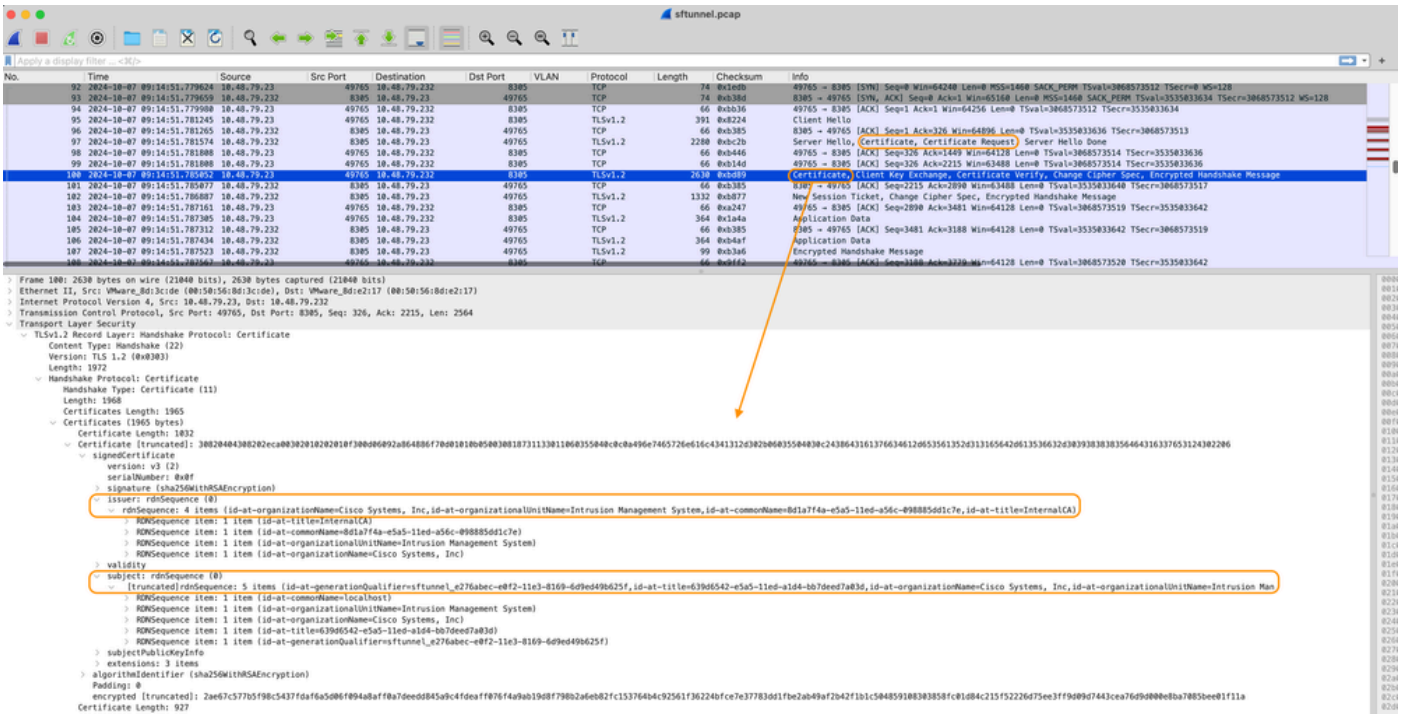
배경 정보

FMC와 FTD는 sftunnel(Sourcefire 터널)을 통해 서로 통신합니다. 이 통신에서는 인증서를 사용하여 TLS 세션을 통해 대화를 안전하게 보호합니다. sftunnel에 대한 자세한 내용 및 설정 방법은 이 링크에서 찾을 수 있습니다.

패킷 캡처에서 FMC(이 예에서는 10.48.79.232)와 FTD(10.48.79.23)가 서로 인증서를 교환하고 있음을 확인할 수 있습니다. 이들은 올바른 디바이스와 대화하고 도청이나 MITM(Man-In-The-Middle) 공격이 없음을 확인하기 위해 이 작업을 수행합니다. 이러한 인증서를 사용하여 통신이 암호화되며, 해당 인증서에 대한 연결된 개인 키가 있는 당사자만 이를 다시 해독할 수 있습니다.



Certificate_exchange_server_cert



Certificate_exchange_client_cert

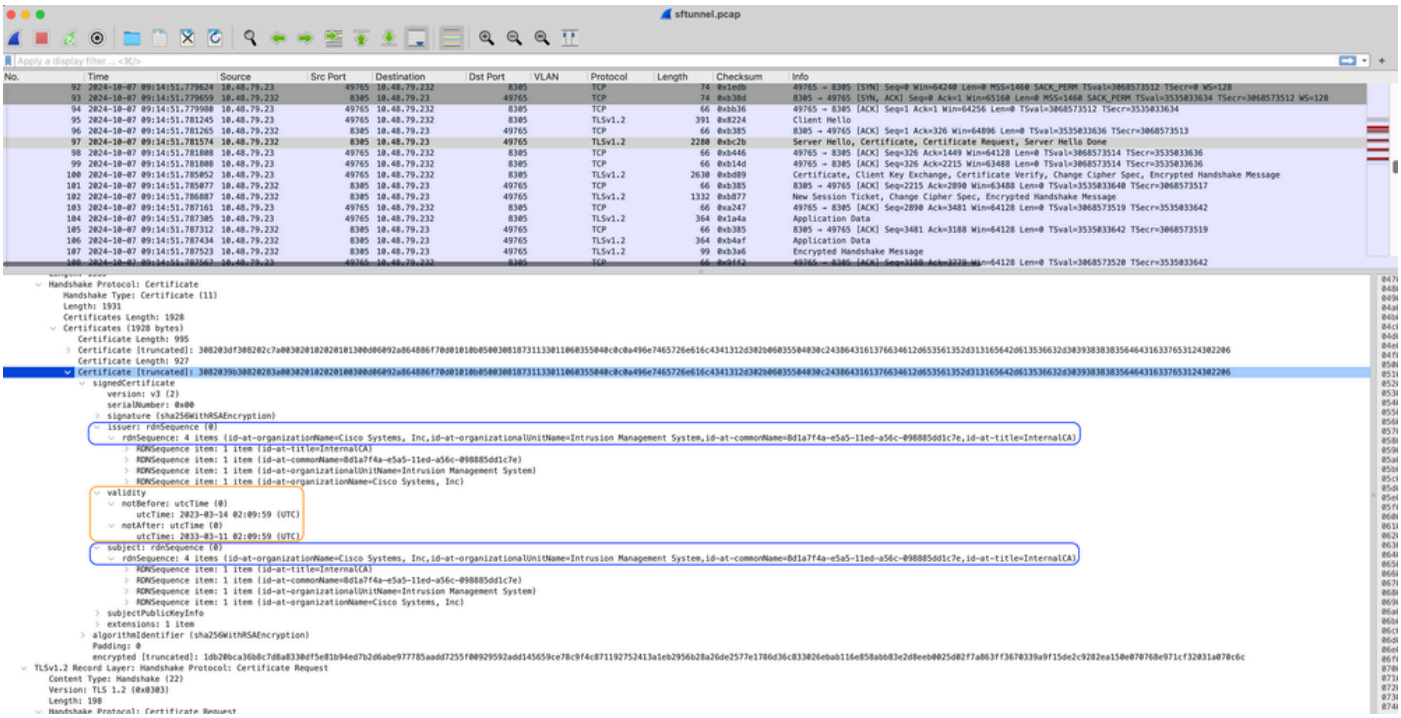
FMC 시스템에 설정된 동일한 InternalCA(Issuer) CA(Certificate Authority)에 의해 인증서가 서명된 것을 확인할 수 있습니다. 컨피그레이션은 /etc/sf/sftunnel.conf 파일의 FMC에 정의되어 있으며 다음과 같은 내용이 포함되어 있습니다.

```
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;
};
```

이는 sftunnel에 대한 모든 인증서(FTD 및 FMC 모두)에 서명하는 데 사용되는 CA와 모든 FTD에 전송하기 위해 FMC에서 사용하는 인증서를 나타냅니다. 이 인증서는 InternalCA에서 서명합니다.

FTD가 FMC에 등록되면 FMC는 sftunnel에서 추가 통신에 사용되는 FTD 디바이스에 푸시할 인증서도 생성합니다. 이 인증서는 동일한 내부 CA 인증서도 서명합니다. FMC에서 /var/sf/peers/<UUID-FTD-device> 및 잠재적으로 certs_pushed 폴더에서 해당 인증서(및 개인 키)를 찾을 수 있으며 이를 sftunnel-cert.pem(개인 키의 경우 sftunnel-key.pem)이라고 합니다. FTD에서 동일한 명명 규칙을 사용하는 /var/sf/peers/<UUID-FMC-device>를 찾을 수 있습니다.

그러나 각 인증서는 보안 목적을 위해 유효 기간이 있습니다. InternalCA 인증서를 검사할 때 패킷 캡처에서 볼 수 있는 것처럼 FMC InternalCA의 유효 기간도 10년입니다.

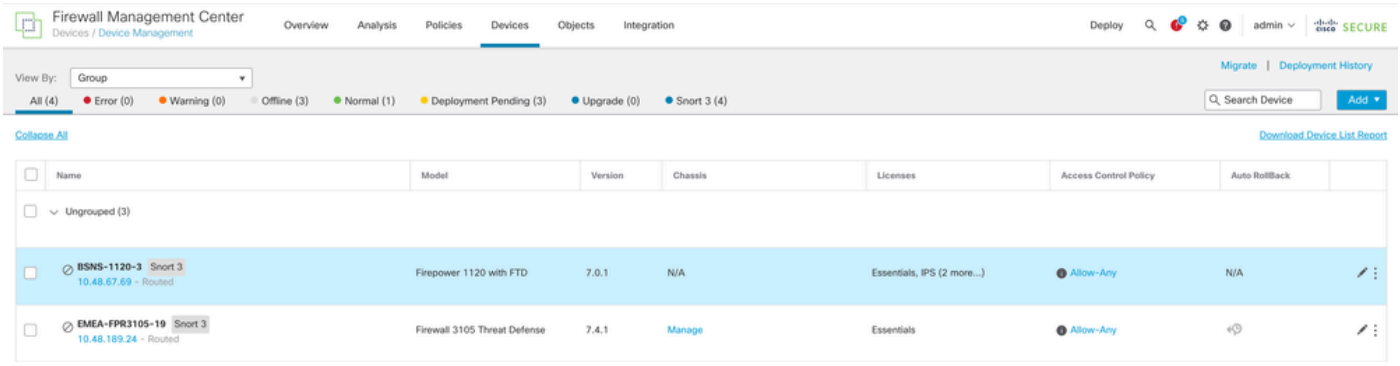


FMC-InternalCA_validity

문제

FMC InternalCA 인증서는 10년 동안만 유효합니다. 만료 시간이 지나면 원격 시스템은 더 이상 이 인증서를 신뢰하지 않으며 인증서도 서명되지 않으므로 FTD와 FMC 디바이스 간의 sftunnel 통신 문제가 발생합니다. 즉, 연결 이벤트, 악성코드 조회, ID 기반 규칙, 정책 배포 등 여러 가지 주요 기능이 작동하지 않습니다.

sftunnel이 연결되지 않은 경우 FMC UI의 Devices(디바이스) > Device Management(디바이스 관리) 탭 아래에 디바이스는 disabled(비활성화됨)로 표시됩니다. 이 만료와 관련된 문제는 Cisco 버그 ID CSCwd08098에서 추적됩니다. 고정 릴리스의 결함을 실행하는 경우에도 모든 시스템이 영향을 받는다는 점에 유의하십시오. 이 수정에 대한 자세한 내용은 솔루션 섹션을 참조하십시오.



비활성화된 디바이스

FMC는 CA를 자동으로 새로 고침하고 FTD 디바이스에 인증서를 다시 게시하지 않습니다. 또한 인증서가 만료됨을 나타내는 FMC 상태 알림도 없습니다. Cisco 버그 ID CSCwd08448은 이와 관련하여 추적되어 향후 FMC UI에 대한 상태 알림을 제공합니다.

만료일 이후에는 어떻게 됩니까?

처음에는 아무 일도 일어나지 않으며 sftunnel 통신 채널은 이전처럼 계속 작동합니다. 그러나 FMC와 FTD 디바이스 간의 sftunnel 통신이 끊기고 연결을 다시 설정하려고 하면 실패하고 메시지 로그 파일에서 인증서 만료를 가리키는 로그 라인을 관찰할 수 있습니다.

FTD 디바이스의 로그 라인 /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 ex
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
```

FMC 디바이스의 /var/log/messages에서 오는 로그 라인:

```
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: Unabl
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
```

sftunnel 통신은 여러 가지 이유로 끊어질 수 있습니다.

- 네트워크 연결 손실로 인한 통신 손실(잠재적으로 일시적인 것일 수 있음)
- FTD 또는 FMC 재부팅
  - 필요한 항목: FMC 또는 FTD에서 sftunnel 프로세스의 수동 재부팅, 업그레이드, 수동 재시작(예: pmtool restartbyid sftunnel)
  - 예기치 않은 항목: 역추적, 정전

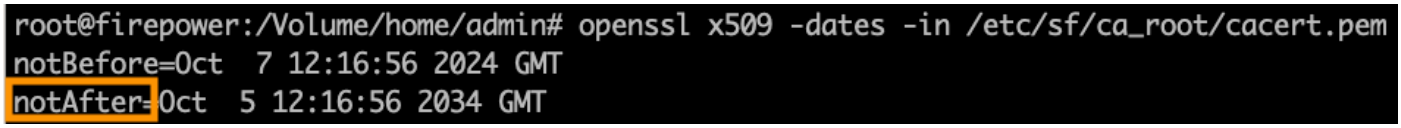
sftunnel 통신을 끊을 수 있는 가능성이 매우 많으므로, 현재 만료된 인증서에도 불구하고 모든 FTD 디바이스가 올바르게 연결된 경우에도 가능한 한 빨리 상황을 수정하는 것이 좋습니다.

인증서가 만료되었는지 또는 언제 만료되었는지 신속하게 확인하는 방법

가장 쉬운 방법은 FMC SSH 세션에서 다음 명령을 실행하는 것입니다.

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

인증서의 유효성 요소를 표시합니다. 여기서 중요한 부분은 2034년 10월 5일까지 이곳 인증서가 유효함을 보여주는 "notAfter"입니다.

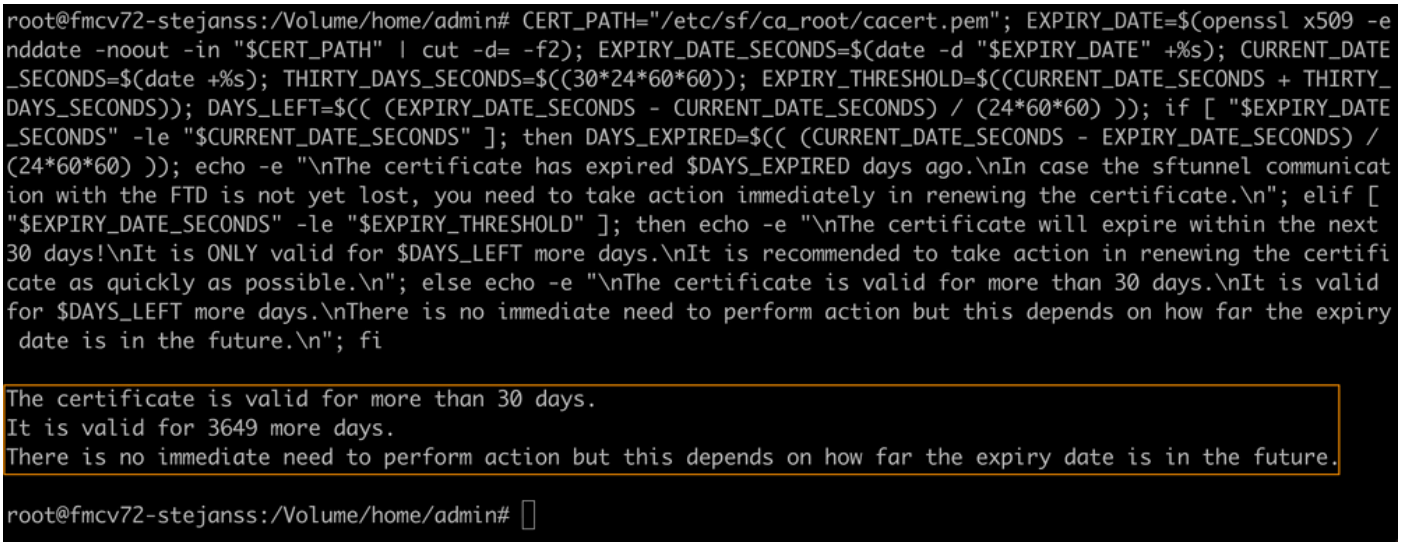


다음 이후 아님

인증서가 여전히 유효한 기간(일)을 즉시 제공하는 단일 명령을 실행하려는 경우 다음을 사용할 수 있습니다.

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

인증서가 여러 해 동안 여전히 유효한 설정의 예가 나와 있습니다.



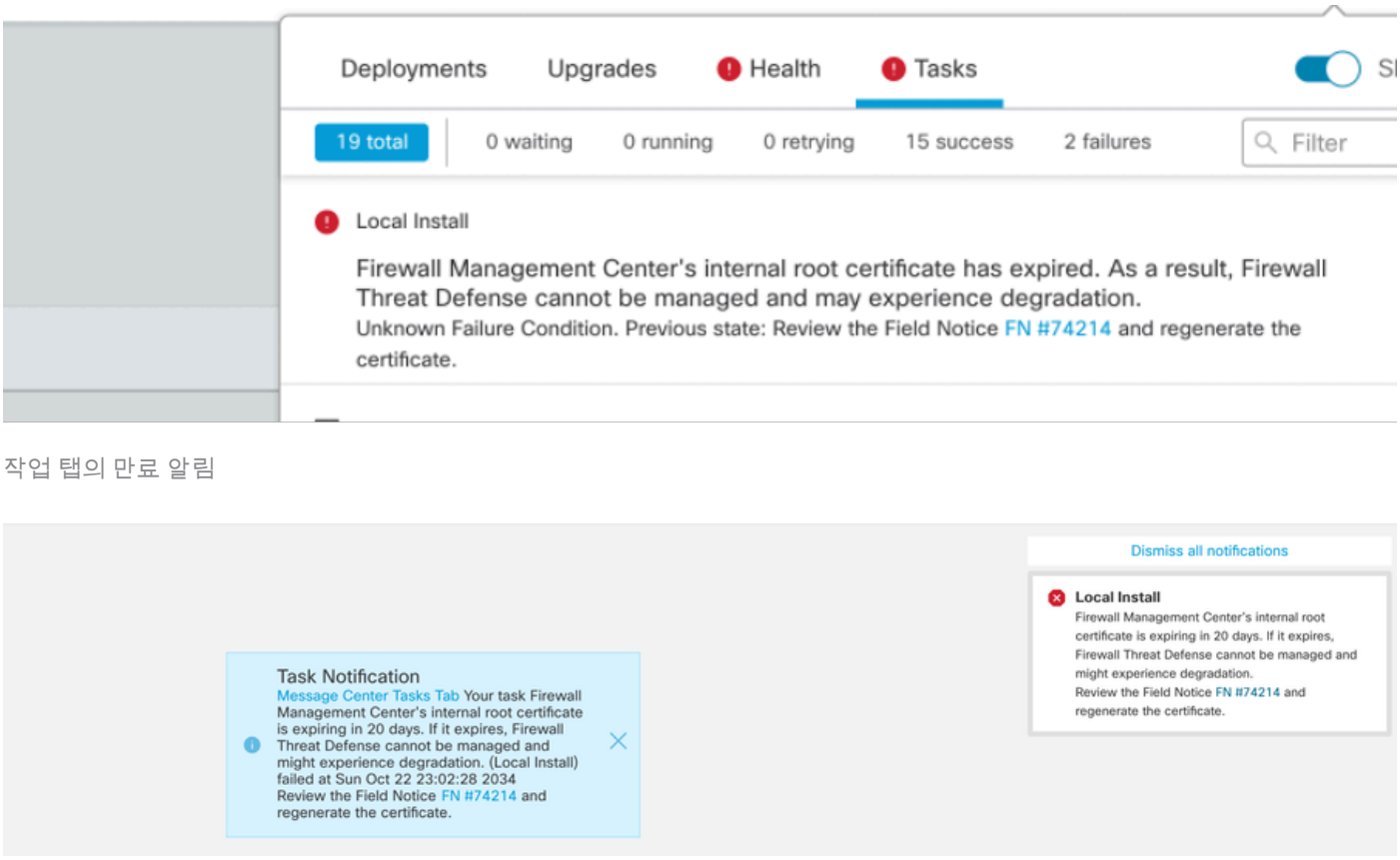
Certificate_expiry_validation_command

향후 인증서 만료에 대한 알림을 받으려면 어떻게 해야 합니까?

최근 VDB 업데이트(399 이상)를 통해 인증서가 90일 내에 만료되면 자동으로 알림을 받습니다. 따라서 만료 시간이 가까워지면 경고를 받기 때문에 수동으로 이 정보를 추적할 필요가 없습니다. 그런 다음 FMC 웹 페이지에 두 개의 양식으로 표시됩니다. 두 방법 모두 필드 알림 페이지를 참조합니다.

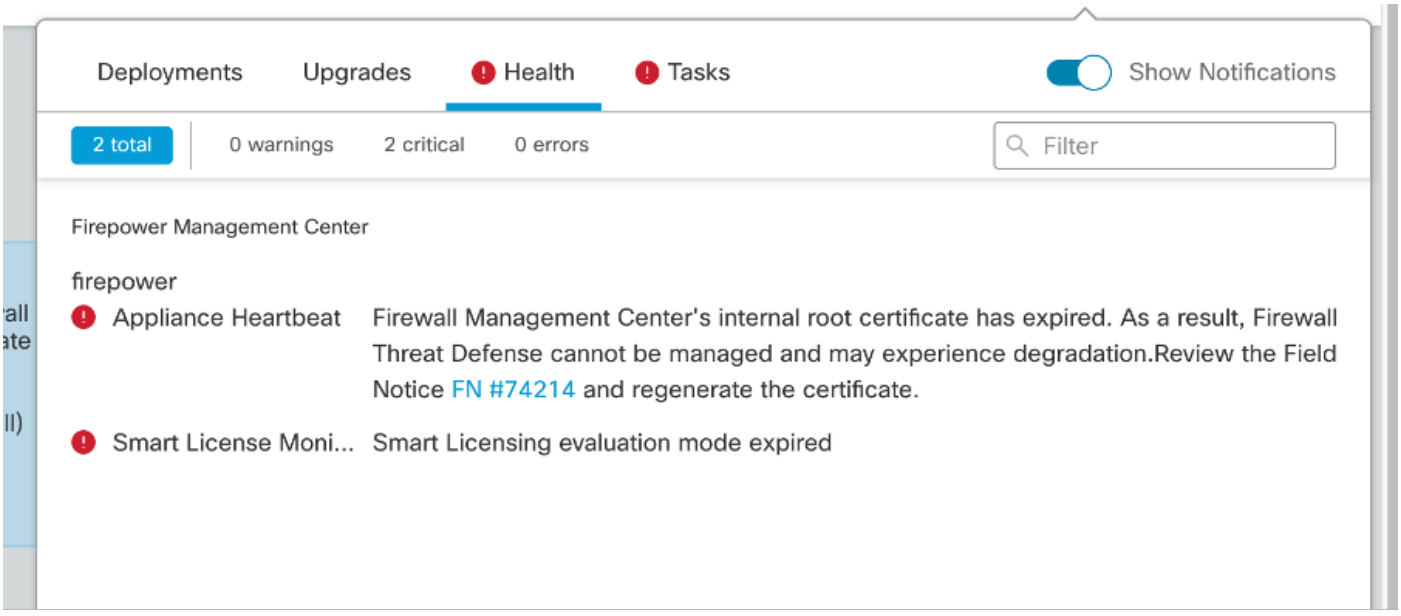
첫 번째 방법은 Task(작업) 탭을 통하는 것입니다. 이 메시지는 고정이며 명시적으로 닫지 않는 한

사용자가 사용할 수 있습니다. 알림 팝업도 표시되며 사용자가 명시적으로 닫을 때까지 사용할 수 있습니다. 항상 오류로 나타납니다.

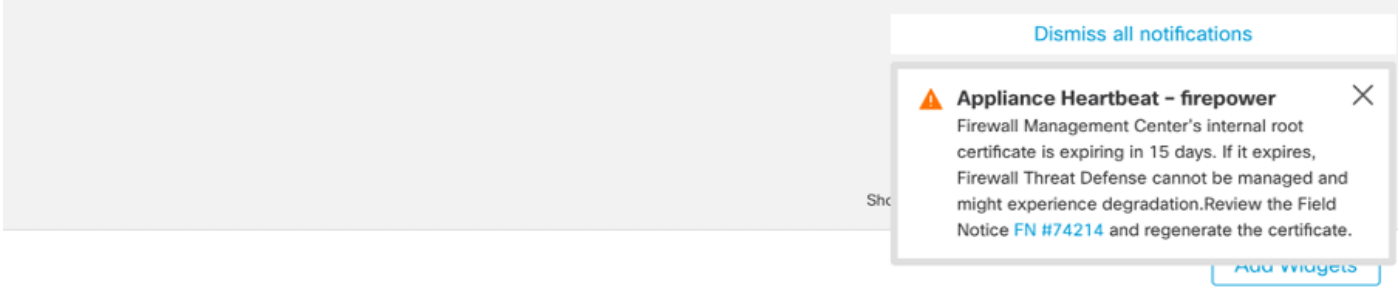


작업 탭의 만료 알림

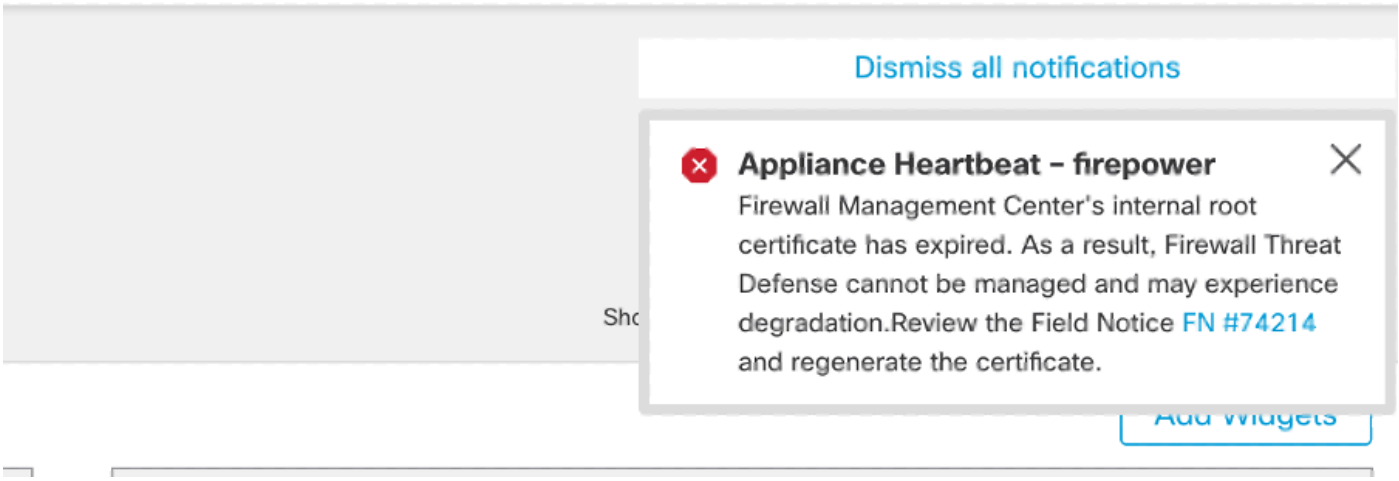
두 번째 방법은 Health Alert입니다. 이는 Health(상태) 탭에 표시되지만 스티커 현상이 없으며 상태 모니터가 실행되면 기본적으로 5분마다 교체되거나 제거됩니다. 또한 사용자가 명시적으로 닫아야 하는 알림 팝업이 표시됩니다. 이는 오류(만료될 경우)와 경고(만료될 경우)로 모두 표시될 수 있습니다.



상태 탭의 만료 알림



상태 알림 팝업에 대한 경고 알림



상태 알림 팝업에 대한 오류 알림

솔루션 1 - 인증서가 아직 만료되지 않았습니다(이상적인 시나리오).

그때 상황이 가장 좋은데, 인증서 만료에 따라 시간이 좀 남았어요. FMC 버전에 의존하는 완전히 자동화된 방식(권장)을 사용하거나, TAC 상호 작용이 필요한 좀 더 수동 방식을 사용합니다.

권장 접근 방식

정상적인 상황에서는 가동 중지 시간이 없고 수동 작업을 가장 적게 할 것으로 예상되는 상황입니다.

계속하기 전에 여기에 나열된 특정 버전에 대한 핫픽스를 설치해야 합니다. 이 경우 이러한 핫픽스는 FMC를 재부팅할 필요가 없으므로 인증서가 이미 만료되었을 때 sftunnel 통신이 끊어질 수 있습니다. 사용 가능한 핫픽스는 다음과 같습니다.

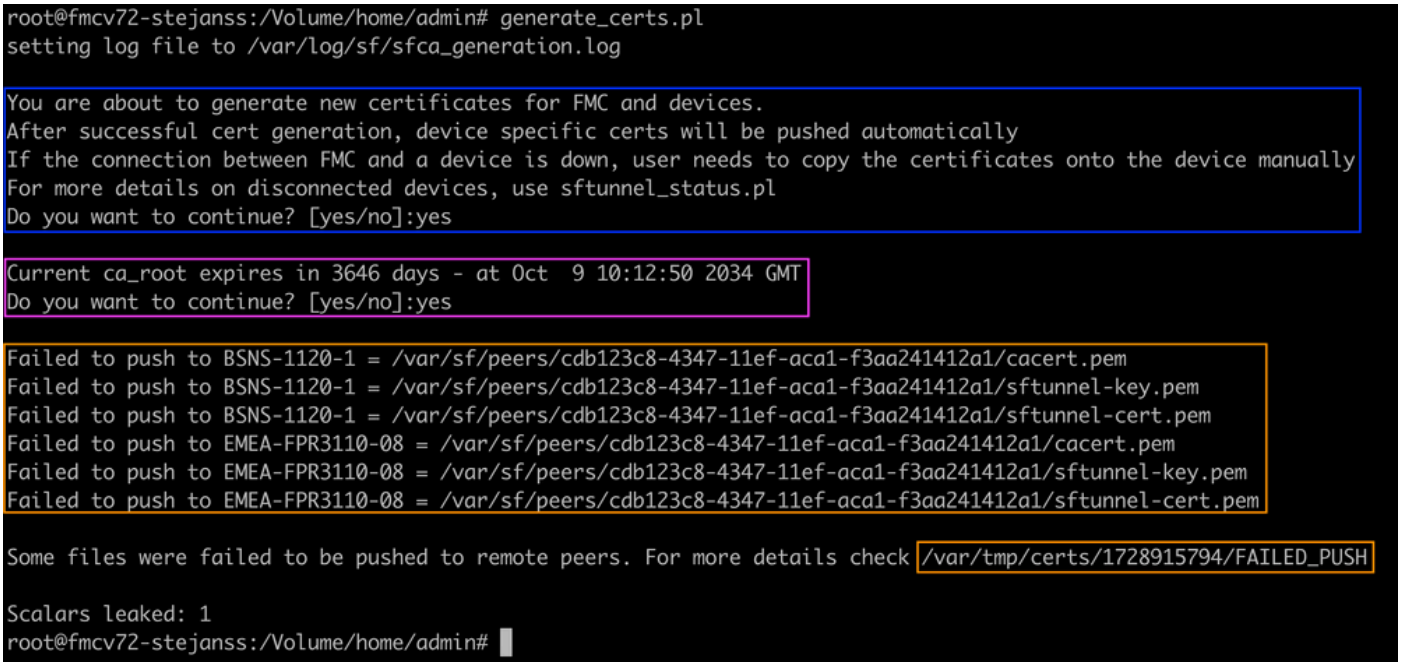
- 7.0.0~7.0.6: 핫픽스 FK - 7.0.6.99-9
- 7.1.x: 소프트웨어 유지 보수 종료로 고정 릴리스 없음
- 7.2.0 - 7.2.9: 핫픽스 FZ - 7.2.9.99-4
- 7.3.x: 핫픽스 AE - 7.3.1.99-4
- 7.4.0 - 7.4.2: 핫픽스 AO - 7.4.2.99-5
- 7.6.0 : 핫픽스 B - 7.6.0.99-5

핫픽스가 설치되면 이제 FMC에 다음과 같은 generate_certs.pl 스크립트가 포함되어야 합니다.

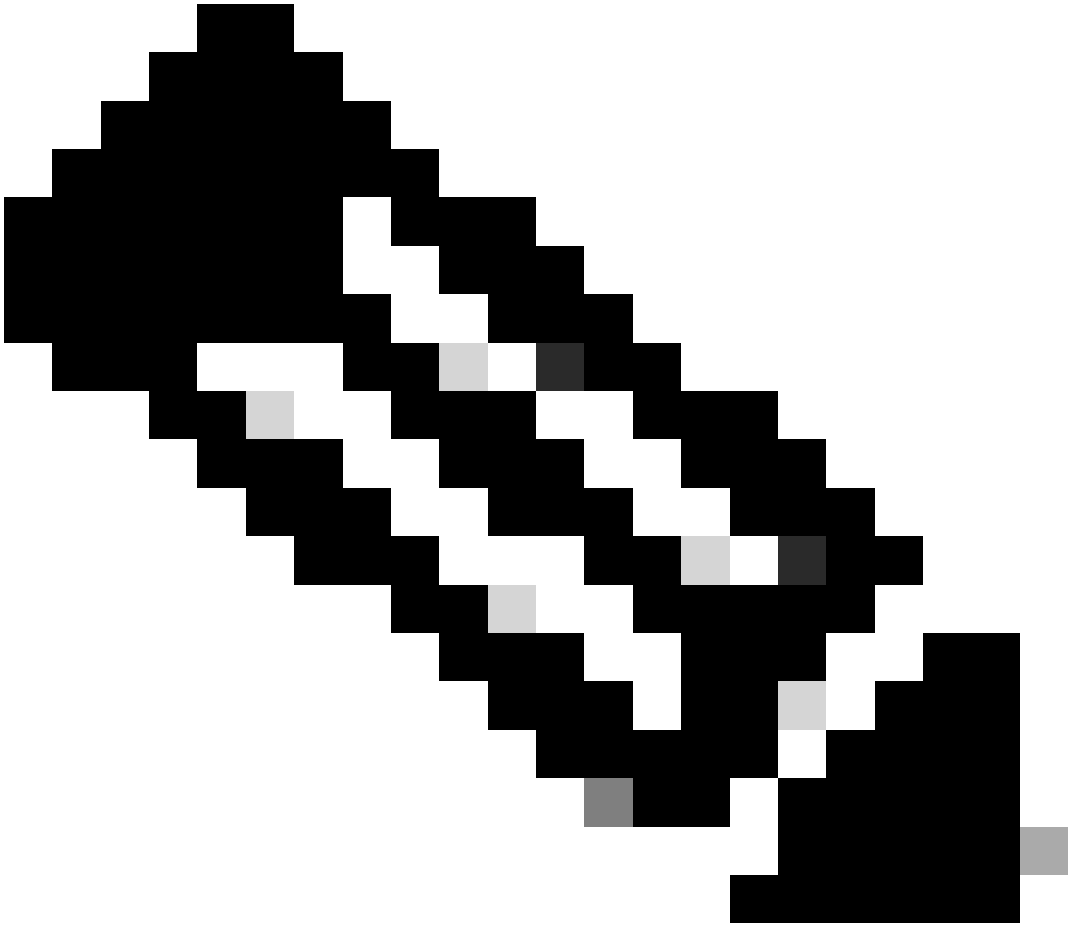
1. InternalCA를 재생성합니다.
2. 이 새 InternalCA에서 서명한 sftunnel 인증서를 다시 만듭니다.
3. 새 sftunnel 인증서 및 개인 키를 각 FTD 디바이스에 푸시합니다(sftunnel이 작동 중일 때).

따라서 (가능한 경우) 다음을 수행하는 것이 좋습니다.

1. 위에 해당하는 핫픽스를 설치합니다
2. FMC에서 백업 수행
3. FMC의 sftunnel_status.pl 스크립트를 사용하여 모든 현재 sftunnel 연결을 검증합니다
4. generate_certs.pl을 사용하여 전문가 모드에서 스크립트 실행
5. 결과를 검사하여 수동 작업이 필요한지 확인합니다(디바이스가 FMC에 연결되어 있지 않은 경우). [아래 추가 설명]
6. FMC에서 sftunnel_status.pl을 실행하여 모든 sftunnel 연결이 제대로 실행되고 있는지 확인합니다



Generate_certs.pl 스크립트



참고: FMC가 HA(고가용성)에서 실행 중인 경우, 기본 노드에서 작업을 먼저 수행한 다음 보조 노드에서 해당 인증서를 사용하여 FMC 노드 간에 통신을 수행해야 합니다. 두 FMC 노드의 InternalCA가 다릅니다.

이 예에서는 /var/log/sf/sfca_generation.log에서 로그 파일을 생성하고 sftunnel_status.pl을 사용하고 InternalCA의 만료 시간을 나타내며 오류가 발생했음을 나타냅니다. 예를 들어, 디바이스 BSNS-1120-1 및 EMEA-FPR3110-08 디바이스에 인증서를 푸시하지 못했습니다. 이 디바이스는 sftunnel이 중단되었기 때문에 이러한 문제가 발생할 것으로 예상됩니다.

실패한 연결에 대한 sftunnel을 수정하려면 다음 단계를 실행합니다.

1. FMC CLI에서 다음 형식의 cat /var/tmp/certs/1728303362/FAILED_PUSH(숫자 값은 unix 시간을 나타내므로 시스템에서 이전 명령의 출력을 확인)를 사용하여 FAILED_PUSH 파일을 엽니다. 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#
```

푸시 실패(_F)

2. FMC에서 FTD 디바이스로 새 인증서(cacert.pem / sftunnel-key.pem / sftunnel-cert.pem)를 전송합니다
   ===자동 접근 방식===

   핫픽스 설치에서는 또한 copy_sftunnel_certs.py 및 copy_sftunnel_certs_jumpserver.py 스크립트를 제공하며, 이는 인증서가 재생성되는 동안 sftunnel이 가동되지 않은 시스템에 대한 다양한 인증서의 전송을 자동화합니다. 이는 인증서가 이미 만료되었기 때문에 sftunnel 연결이 끊어진 시스템에도 사용할 수 있습니다.

   FMC 자체에서 다양한 FTD 시스템에 대한 SSH 액세스 권한이 있는 경우 copy_sftunnel_certs.py 스크립트를 사용할 수 있습니다. 그렇지 않은 경우 FMC에서 FMC 및 FTD 디바이스에 대한 SSH 액세스 권한이 있는 점프 서버로 스크립트 (/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py)를 다운로드하고 여기에서 Python 스크립트를 실행할 수 있습니다. 또한 불가능한 경우 다음에 표시된 수동 접근 방식을 실행하는 것이 좋습니다. 다음 예에서는 사용 중인 copy_sftunnel_certs.py 스크립트를 보여주지만, 단계는 copy_sftunnel_certs_jumpserver.py 스크립트와 동일합니다.

   A. SSH 연결에 사용되는 디바이스 정보(device_name, IP 주소, admin_username, admin_password)를 포함하는 CSV(또는 jump 서버)에서 CSV 파일을 생성합니다.

   기본 FMC에 대한 점프 서버와 같은 원격 서버에서 이를 실행할 경우 첫 번째 항목 다음에 모든 관리되는 FTD 및 보조 FMC를 추가하여 기본 FMC 세부 정보를 추가해야 합니다. 보조 FMC에 대한 점프 서버와 같은 원격 서버에서 이를 실행할 경우 보조 FMC 세부사항을 첫 번째 항목과 모든 관리되는 FTD로 추가해야 합니다.

   i. vi devices.csv를 사용하여 파일을 생성합니다.

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

vi devices.csv

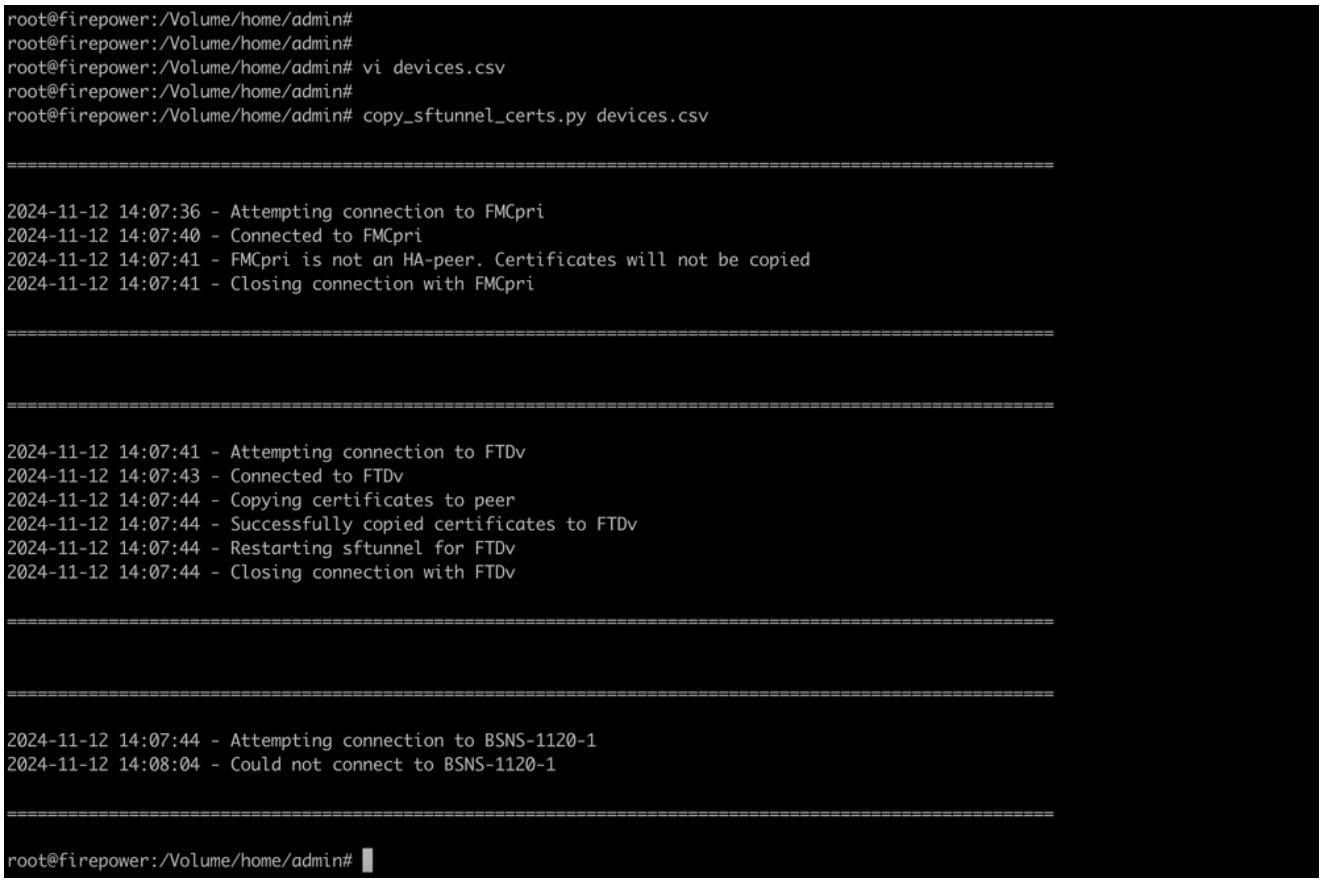
나. 그러면 빈 파일(표시되지 않음)이 열리고 키보드에서 i자를 사용하여 INTERACTIVE 모드(화면 하단에 표시됨)로 이동한 후 표시된 세부 정보를 입력합니다.

devices.csv 예

iii. 작업이 완료되면 ESC와 :wq를 차례로 사용한 다음 Enter를 사용하여 파일을 닫고 저장합니다.

devices.csv 저장

B. copy_sftunnel_certs.py devices.csv와 함께 스크립트(sudo를 사용하여 root에서)를 실행하면 결과가 표시됩니다. 여기에서는 FTDv에 대한 인증서가 올바르게 푸시되었고 BSNS-1120-1의 경우 디바이스에 SSH 연결을 설정할 수 없음을 보여줍니다.



copy_sftunnel_certs.py devices.csv

===수동 방식===

1. 이전 출력(FAILED_PUSH file)에서 파일 위치를 복사하여 FMC CLI에서 영향받는 각 FTD(cacert.pem / sftunnel-key.pem(보안을 위해 완전히 표시되지 않음) / sftunnel-cert.pem)에 대한 각 파일을 인쇄(cat)합니다.

```
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. sudo su를 통해 루트 권한으로 전문가 모드에서 각 FTD의 FTD CLI를 열고 다음 절차를 통해 인증서를 갱신합니다.
    1. FAILED_PUSH 출력에서 연한 파란색 강조 표시 위치를 찾습니다 (cd/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1 여기서 예를 들어, 이는 각 FTD마다 다릅니다).
    2. 기존 파일을 백업합니다.

```
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
```

현재 인증서 백업 수행

    3. 새 콘텐츠를 작성할 수 있도록 파일을 비웁니다.

```
> 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#
```

기존 인증서 파일의 빈 내용

    4. vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem을 사용하여 각 파일에 새 콘텐츠(FMC 출력에서)를 개별적으로 씁니다(파일당 별도의 명령 - 스크린샷은 cacert.pem에 대해서만 표시하지만 sftunnel-cert.pem 및 sftunnel-key.pem에 대해서는 반복해야 합니다).

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

vi cacert.pem

1. vi 명령을 입력한 후 빈 파일이 표시되면 i를 눌러 대화형 모드로 전환합니다.
2. 파일의 전체 내용(-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 포함)을 복사하여 붙여넣습니다.

vi에서 내용 복사(삽입 모드)

3. Esc를 누른 다음 :wq를 입력하여 파일을 닫고 입력합니다.

ESC 뒤에 :wq를 입력하여 파일에 기록합니다.

5. ls -hal을 사용하여 각 파일에 올바른 권한(chmod 644) 및 소유자(chown root:root)가 설정되어 있는지 확인합니다. 이것은 우리가 기존 파일을 업데이트할 때 실제로 올바르게 설정되어 있습니다.

```
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#
```

모든 인증서 파일이 올바른 소유자 및 권한으로 업데이트됨

3. 인증서의 변경 사항을 명령과 함께 적용하기 위해 sftunnel이 작동하지 않는 각 FTD에서 sftunnel을 다시 시작합니다 pmtool 다시 시작byid 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 다시 시작byid sftunnel

3. 이제 sftunnel_status.pl 출력을 사용하여 모든 FTD가 올바르게 연결되었는지 확인합니다

솔루션 2 - 인증서가 이미 만료되었습니다.

이 상황에서는 두 가지 시나리오가 있습니다. 모든 sftunnel 연결이 여전히 작동 중이거나 더 이상 (또는 부분적으로) 작동하지 않습니다.

FTD가 sftunnel을 통해 계속 연결됨

Certificate has not not expired (ideal scenario) - Recommended approach 섹션에서 설명한 것과 동일한 절차를 적용할 수 있습니다.

그러나 모든 sftunnel 연결을 끊고 각 FTD에서 모든 인증서 업데이트를 수동으로 실행해야 하므로

이 상황에서는 FMC(또는 FTD)를 업그레이드하거나 재부팅하지 마십시오. 단, FMC를 재부팅할 필요가 없으므로 나열된 핫픽스 릴리스는 예외입니다.

터널은 연결된 상태로 유지되며 인증서는 각 FTD에서 교체됩니다. 일부 인증서를 채우지 못할 경우 실패한 인증서를 입력하라는 메시지가 표시되며 이전 섹션에서 설명한 대로 수동 접근 방식을 취해야 합니다.

FTD가 sftunnel을 통해 더 이상 연결되지 않음

권장 접근 방식

Certificate has not not expired (ideal scenario) - Recommended approach 섹션에서 설명한 것과 동일한 절차를 적용할 수 있습니다. 이 시나리오에서 새 인증서는 FMC에서 생성되지만 터널이 이미 다운되어 디바이스에 복사할 수 없습니다. 이 프로세스는 copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py 스크립트를 사용하여 자동화할 수 있습니다

모든 FTD 디바이스가 FMC에서 연결 해제되면 sftunnel 연결에 영향을 미치지 않으므로 이 상황에서 FMC를 업그레이드할 수 있습니다. 일부 디바이스가 sftunnel을 통해 계속 연결되어 있는 경우 FMC의 업그레이드로 모든 sftunnel 연결이 닫히고 만료된 인증서로 인해 다시 나타나지 않습니다. 여기서 업그레이드를 수행하면 각 FTD로 전송해야 하는 인증서 파일에 대한 올바른 지침이 제공될 수 있습니다.

수동 접근 방식

이 경우 새 인증서를 생성하는 FMC에서 generate_certs.pl 스크립트를 실행할 수 있지만 각 FTD 디바이스에 수동으로 인증서를 푸시해야 합니다. 장치의 양에 따라 이 작업은 수행할 수 있거나 번거로운 작업이 될 수 있습니다. 그러나 copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py 스크립트를 사용할 경우 고도로 자동화됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.