為FTD連線續訂FMC Sftunnel CA憑證

目錄
<u>必要條件</u>
採用元件
<u>背景資訊</u>
<u>問題</u>
<u>到期日期後會發生什麽?</u>
如何快速驗證憑證是否已到期或何時到期?
以後如何獲得有關即將到期的證書的通知?
<u>解決方案1 — 證書尚未過期(理想情況)</u>
推薦的方法
<u>解決方案2 — 證書已過期</u>
FTD仍透過sftunnel連線
<u>FTD不再通過sftunnel連線</u>
<u>推薦的方法</u> 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
<u> </u>

簡介

_ . _

本檔案介紹有關Firepower威脅防禦(FTD)連線的Firepower管理中心(FMC)Sftunnel憑證授權單位 (CA)憑證的續訂。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower威脅防禦
- Firepower管理中心
- 公開金鑰基礎架構 (PKI)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

FMC和FTD會通過sftunnel(Sourcefire tunnel)彼此通訊。 此通訊使用證書來確保TLS會話中的會話 安全。有關sftunnel及其如何建立的詳細資訊,可在該連結上<u>找到</u>。

透過封包擷取,您可以看到FMC(本範例中為10.48.79.232)和FTD(10.48.79.23)正在相互交換憑 證。他們這樣做是為了驗證他們是否與正確的裝置進行了通訊,以及是否不存在竊聽或中間人 (MITM)攻擊。使用這些證書對通訊進行加密,只有擁有該證書的關聯私鑰的一方才能再次對其進行 解密。

• • •				🚄 sftunnel.pcap		
🖌 📕 🧷 💿 🔚 🗂 🗙 🖉 🖌 🖌	• 🕾 🛪 🔹 🗔 🗖		Ē			
Apply a display filter _<1/			lan.			+
No. Time Course	See Dort Destination	Det Dort VI AN	Drotocol	Length Chackness	linda	
92 2024-10-07 09:14:51.779624 10:48.79.23 93 2024-10-07 09:14:51.779659 10:48.79.232	49765 10.48.79.232 8385 10.48.79.23	8305 49765	TCP	74 0x1edb 74 0x1edb 74 0xb38d	49765 - 8305 [SYN] Sequé Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3068573512 TSecr=0 MS=128 8305 - 49765 [SYN, ACK] Sequé Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3535833634 TSecr=3068573512 MS=128	
94 2024-10-07 09:14:51.779980 10.48.79.23	49765 10.48.79.232	8305	TCP	66 @xbb36	49765 - 8385 [ACK] Seq=1 Ack=1 Win=64256 Len=@ TSval=3068573512 TSecr=3535833634	
95 2024-10-07 09:14:51.781245 10.40.79.23 96 2024-10-07 09:14:51.781265 10.40.79.232	49765 18.48.79.232 8385 18.48.79.23	49765	TLSV1.2 TCP	391 0x8224 66 0xb385	Client Mello 8385 + 49265 [ACK] Secril Ack=326 Win=64896 Len=0 TSval=3535833636 TSecr=3068573513	-
97 2024-10-07 09:14:51.781574 10.48.79.232	8385 10.48.79.23	49765	TL5v1.2	2280 0xbc2b	Server Hello, Certificate, Certificate Request Server Hello Done	_
98 2024-10-07 09:14:51.781808 10.48.79.23	49765 10.48.79.232	8305	TCP	66 @xb446	49765 = 8385 [ACK] Seb=325 Ack=1449 Win=64128 Len=0 TSval=3665573514 TSecr=3535835836	Ξ.
99 2824-18-87 89:14:51.781888 18.48.79.23 188 2824-18-87 89:14:51 285852 18.48 29.23	49765 10.48.79.232	8305	TCP TLSv1 2	66 @xb14d	49765 - 8385 (ACK) Sequ-326 Ack+2215 Win-65488 Lenv# Tsval-9086573514 Tsecr=3535033636 Castilicata Client Fau Erchanae Castilicata Varia Chanae Clienter Sanz Encontrat Workholm Marsanae	
101 2024-10-07 09:14:51.785077 10.48.79.232	8385 18.48.79.23	49765	TCP	66 exb385	108 - 40765 (ACK) See 2215 Ack/209 Wind 448 Leng Tsyala 535831640 Sec = 366573517	
102 2024-10-07 09:14:51.705887 10.48.79.232	8305 10.48.79.23	49765	TLSv1.2	1332 @xb877	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
103 2024-10-07 09:14:51.787161 10.48.79.23	49765 10.48.79.232	8305	TCP	66 @xa247	49765 - 8385 [ACK] Beq+2898 Ack+3481 Win+64128 Len+8 TSval=3868573519 TSecr=3535833642	
104 2024-10-07 09:14:51.787305 10.48.79.23 105 3034-10-07 09:14:51 707312 10.49 70 332	49765 10.48.79.232	8385	TLSV1.2	364 0x1a4a	Application Data 9365 _ 40256 [cmm348] Arkm3188 WinnE4128 [ann# Trus]=1515633642 Trarr=3668575510	
106 2024-10-07 09:14:51.707512 10:40.79.232	8385 10.48.79.23	49765	TLSv1.2	364 @xb4af	4201 color - 42/00 (ALA) 200-3401 ALA-3100 RIM-0420 LEM-0 1342(-3333003042 136(1-94003/3312)	
107 2024-10-07 09:14:51.707523 10.40.79.232	8305 10.48.79.23	49765	TLSv1.2	99 @xb3a6	Encrypted Handshake Message	
108 2024-10-07-09:14:51.787567 10.48.79.23	49765 10.48.79.232	8385	TCP	66 0x91/12	49765 - 8385 [ACF] See-3188 Ack+3729 Man=64128 Len=0 TSval=3068573528 TSecr=3535833642	
 Frame 97: 2280 bytes on wire (18240 bits), 2280 bytes captu Ethernet II, Src: VMware_8dre217 (00:50:56:8dre217), 0st: Intermet Protocol Version 4, Src: 10-48.79, 232, 0st: 18-48. Transmission Control Protocol, Src Port: 8305, Dst Port: 43 	red (18240 bits) VMware_8d:3c:de (00:50:56:8d:3c 79.23 765, Seq: 1, Ack: 326, Len: 2214	::de)				0154 0164 0170 0181 019
 Transport Layer Security Ti Sul 3 Record Lawer: Wandshake Protocol: Securit Hallo 						01a
 TLSv1.2 Record Layer: Handshake Protocol: Certificate 						010
Content Type: Handshake (22)						01d
Version: TLS 1.2 (0x0303)						01e
Length: 1935 Handibaba Protocol: Contificate						020
Handshake Type: Certificate (11)						821
Length: 1931					*	823
Certificates Length: 1928						824
 Certificates (1928 bytes) Certificate Length: 995 						026
 Certificate [truncated]: 308203df308202c7a00302 	01020201013003060926864886f7030	010005003081873113301100	0355040c0c0a41	6e7465726e616c4341312d382b8	#355#4#3#c;2438643161376634612d653561352d313165642d613536632d3#3938383564643163376531243#22#6	027
v signedCertificate						829
version: v3 (2)						028
signature (sha2504ith954Encryption)						820
issuer: rdnSequence (0)						@2d
> rdnSequence: 4 items (id-at-organizat)	ionName=Cisco Systems, Inc,id-at-	-organizationalUnitName=1	Intrusion Manag	pement System, id-at-commonNam	we8d1a7f4a-e5a5-11ed-a56c-098885dd1c7e,id-at-title=InternalCA)	026
> validity						030
 subjecti rensequence (0) rensequence 5 items (id-at-generation) 	dualifierusftunnel.id-at-titleu	Rd1a7fda-e5a5-11ed-a56c-d	NARRESALL 74. 1	-at-oroanizationNamesCisco	visites. Tor.id-at-organizationalUnitHamesIntrusion Management System.id-at-competibuses[aca]bost]	031
> RDNSequence item: 1 item (id-at-com	morName=localhost)					033
> RDNSequence item: 1 item (id-at-org	panizationalUnitName=Intrusion M	anagement System)				034
> RONSequence item: 1 item (id-at-org RONSequence item: 1 item (id-at-org	panizationName=Cisco Systems, Inc	c)				836
Resequence item: 1 item (id-at-der	rationDualifierusftunnel)	opericie)				037
> subjectPublicKeyInfo						039
> extensions: 3 items						03.0
> algorithmIdentifier (sha256WithRSAEncryption Reddices 0	0					830
radoing: e encrypted [truncated]: 8456875cc20845279f6e3	ka48838+63v17x84+738a+3474x71838	058493485258147584524591	1354/0102656854	5/0/075572/17781#758/1ab3/8abd	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	034
Certificate Length: 927						03e
> Certificate [truncated]: 3082039b30820283a00302	0102020100300d06092a864886170d0	10105003081873113301100	68355848c8c8a49	6e7465726e616c4341312d302b0	#35584439c24386431613766346120653561352d3131656420613536632d3#39383838356464316337653124302206	848
> TLSv1.2 Record Layer: Handshake Protocol: Certificate Re	quest					841
> ILSV1.2 Mecord Layer: mandshake Protocol: Server Hello G	ione					1 645

Certificate_exchange_server_cert

•••				🚄 sftunnel.pcap		
🚄 📕 🧶 🕥 🔚 🗂 🗙 🙆 🔍 👄	+ 2 F ± 🗔 🚍		5			
Apply a display filter <%/>					•	+
No. Time Source	Src Port Destination	Dst Port VLAN	Protocol	Length Checksum	Info	
92 2024-10-07 09:14:51.779624 10.48.79.23 93 2024-10-07 09:14:51.779659 10.48.79.232 94 2024-10-07 09:14:51.779930 10.48.79.23 95 2024-10-07 09:14:51.779508 10.48.79.23	49765 10.48.79.232 8365 10.48.79.23 49765 10.48.79.232 49765 10.48.79.232	8305 49765 8305 8305	TCP TCP TCP TLSv1.2	74 0x1edb 74 0xb38d 66 0xb36 391 0x8224	49765 - 8385 [SPN] Seevel MLm-64240 Lemit MSS-1466 SAKC_PEM TSval-3966573512 TSecre-0 %Si-128 B385 - 44795 [SPN, ACK Sequel Ackin MLm64266 Lemit MSS-1466 SAKC_PEM TSval-3355833634 TSecre-3066573512 MS-128 49765 - 8385 [ACK] Sequ1 Ackal MLm6426 Lemit TSval-396573512 TSecre-3535833634	
96 2024-10-07 09:14:51.781265 10.48.79.232 97 2024-10-07 09:14:51.781574 10.48.79.232 98 2024-10-07 09:14:51.781588 10.48.79.232	8385 10.48.79.23 8385 10.48.79.23 49765 10.48.79.23	49765 49765 8385	TCP TLSv1.2 TCP	66 0xb385 2280 0xbc2b 66 0xb46	8385 - 49765 [ACK] Seg=1 Ack=356 Winn-64896 Lenn® TSval=3353833636 TSecr=3868573513 Server Hello, [certificate, Certificate Request] Server Hello Bone 69765 - 2886 [ACK] Secol24 Ack1428 Winch1278 Lenn® Tsval=386857316 TSecr=3535813836	Ξ
99 2024-10-07 09:14:51.781808 10.48.79.23 100 2024-10-07 09:14:51.785052 10.48.79.23 101 2024-10-07 09:14:51.785072 10.48.79.232	49765 10.48.79.232 49765 10.48.79.232 8385 10.48.79.23	8305 8305 49765	TCP TLSv1.2 TCP	66 0xb14d 2630 0xbd89 66 0xb385	49765 - 8305 [ACK] Seq=326 Ack=2215 Win=63488 Len=0 TSval=3068573514 TSecr=3535033636 Certificate; Client Key Exchange, Certificate Verify, Change Cipher Seev, Encrypted Handshake Message INF - 4707 [ACK] Seev2708 United Mill Lenet Vau]133501404 [Secr=306373512	-
102 2024-10-07 09:14:51.706887 10.48.79.232 103 2024-10-07 09:14:51.787161 10.48.79.23 104 2024-10-07 09:14:51.787365 10.48.79.23	8385 10.48.79.23 49765 10.48.79.232 49765 10.48.79.232	49765 8385 8385	TLSv1.2 TCP TLSv1.2	1332 0xb877 66 0xa247 364 0x1a4a	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message 49/65 – 8365 [ACK] Seq=2898 Ack=3481 Win=64128 Len=0 TSval=3868573519 TSecr=3535833642 Abolication Bata	
105 2024-10-07 09:14:51.787312 10.48.79.232 106 2024-10-07 09:14:51.787434 10.48.79.232 107 2024-10-07 09:14:51.787531 10.48.79.232	8305 10.48.79.23 8305 10.48.79.23 8305 10.48.79.23	49765 49765 49765	TCP TLSv1.2 TLSv1.2	66 8xb385 364 8xb4a1 99 8xb1a6	8385 = 49765 [ACK] Seq=3481 Ack=3188 Win=64128 Len=0 TSval=3535833642 TSecr=3068573519 \$polication Data Encrystef Mundshake Message	
108 2024-10-07 09:14:51.787567 10.48.79.23	49765 10.48.79.232	8305	TCP	66 0x9112	49265 - 6385 [ACK] 6-02188 Ack-3729 Min-64128 Len=0 TSval=3068573520 TSecr=3535833642	
 Prame 100: 2020 bytes on wire (21040 bits), 2630 bytes cap Etherest II, Src: Whare Additate (0.055):0516:016:00; bits Internet Protocol Version 4, Src: 10.40.79.23, Dit: 10.40. Transmission Control Protocol, Src Port: 49765, Dit Port: V Transport Layer Security V TSVI.2 Record Layer: Handshake Protocol: Certificate Content Type: Handshake (22) 	tured (21040 bits) : VMwre_Mdre2:17 (00:50:56:8d:e2:1 79.232 8305, Seq: 326, Ack: 2215, Len: 256	7) 4				0001 0011 0021 0031 0051 0051 0051 0051
Version: TLS 1.2 (8x8080) Length: 1972 V Handshake Protocol: Certificate Handshake Type: Certificate (11) Length: 1968 Certificates Length: 1965						0031 0034 0034 0054 0054 0054 0064
 Certificates (1965 bytes) Certificate (expth: 1802) Certificate (truncated): 3020404308202cca0834 SignedGerificate version: v3 (2) SetabModer: 1987 SetabModer: 1987 	2010202010f3003066092a864886f70d0101	8585883881873113381186	a355848c0c0a496	e7465726e616c4341312d382b868	355844394;243864316137663461266535613552831316564266135366328398383838356464316337653124382286	0104 0111 0121 0131 0144 0154 0154
 issuer: rdsSequence (8) rdnSequence: 4 items (id-at-organizat DdSSequence item: 1 item (id-at-1) DdSSequence item: 1 item (id-at-4) DdSSequence item: 1 item (id-at-4) 	ionName=Cisco Systems, Inc,id-at-or itle=Internal(A) mmonName=8d1a?f4a=eSa5=11ed=a56c=09 rganizationalUnitName=Intrusion Mana	ganizationalUnitName=I 8885dd1c7e) gement System)	Intrusion Manage	ment System,id-at-commonName	=801a7f4a-e5a5-11e6-a56c-0900056d1c7e,id-at-title=InternalCA)	0174 0184 0194 0184 0184 0184 0164
 > Nubsquence itemi 1 item (id-at-of- validity > subject: rdnSequence (0) > [truncated]rdnSequence: 5 items (id- > EMPSequence item 1 item (id-at-of- per) 	<pre>ganizationWame=cisco Systems, inc) -at-generationQualifier=sftunnel_e27 wmonName=localhost)</pre>	6abec-e0f2-11e3-8169-6	id9ed49b625f,id-	at-title=639d6542-e5a5-11ed-	a144-b07deed7a83d,id-at-organizationNamerCisco Systems, Inc.id-at-organizationalUnitNamerIntrusion Man	01di 01di 01di 02di 02di 02di
 > RONSequence item: 1 item (id-at-or > RONSequence item: 1 item (id-at-or 	ganizationalUhiIName=Intrusion Mana ganizationName=Cisco Systems, Inc) (tle=639d6542=e5a5=1led=ald4=bb7deed merationQualifier=sftunnel_e276abec	gement System) 7a03d) -e0f2-11e3-8169-6d9ed4	196625f)			0221 0234 0244 0254 0254 0254 0254 0254 0254
 > extensions: 3 litems > algorithaldentifier (sha256withRSAEncryptic Padding: 0 encrypted [truncated]: 2ae67c577b5598c54371 Certificate Length: 927 	n) Ida16a5d061094a8aff0a7deedd845a9c4fd	eaff@76f4a9ab1968f798b	2a6eb82fc153764	b4c92561f36224bfce7e37783dd1	fbs2ab49af2b42f1b1c50485918838858fc01d84c215f52226d75es3ff9509d7443cea76d96080e8ba7085bee81f11a	8284 8294 8284 8284 8264 8264

您可以看到憑證是由在FMC系統上建立的同一InternalCA(Issuer)憑證授權單位(CA)簽署。配置在 /etc/sf/sftunnel.conf檔案上的FMC中定義,該檔案包含以下內容:

```
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;
};
```

這表示用於簽署sftunnel(FTD和FMC一)的所有憑證的CA,以及FMC用於傳送給所有FTD的憑證 。此證書由InternalCA簽名。

當FTD註冊到FMC時,FMC也會建立一個憑證以推送到FTD裝置,該憑證用於sftunnel上的進一步 通訊。此證書也由同一內部CA證書簽名。在FMC上,您可以在/var/sf/peers/<UUID-FTD-device>下 找到證書(和私鑰),也可能在certs_pused資料夾下,稱為sftunnel-cert.pem(對於私鑰,sftunnelkey.pem)。在FTD上,可以找到在/var/sf/peers/<UUID-FMC-device>下使用相同命名約定的路由器 。

但是,出於安全考慮,每個證書也有一個有效期。檢查InternalCA憑證時,我們可以看到封包擷取 中所示的FMC InternalCA的有效期為10年。



FMC-InternalCA_validity

FMC InternalCA證書的有效期僅為10年。到期時間過後,遠端系統不再信任此證書(以及由其簽名 的證書),這將導致FTD和FMC裝置之間的隧道通訊問題。這也意味著一些關鍵功能(如連線事件 、惡意軟體查詢、基於身份的規則、策略部署以及許多其他功能)無法正常工作。

當sftunnel未連線時,裝置在Devices > Device Management頁籤下的FMC UI中顯示為已禁用。在 思科錯誤ID <u>CSCwd08098</u>上,會追蹤與此過期時間相關的問題。雖然請注意,即使您執行的是錯誤 的固定版本,所有系統仍會受到影響。有關此修補程式的更多資訊,請參閱解決方案部分。

Firewall Management Center Overview Anatysis	Policies Devices Obje	cts Integrat	ion		Deploy Q 💕 🌣	admin ~ advid	SECURE
View By: Group						Migrate Deploymen	t History
All (4) • Error (0) • Warning (0) • Offline (3) • Normal (1)	 Deployment Pending (3) 	Upgrade (0)	 Snort 3 (4) 		C	& Search Device	Add 💌
Collarose All						Download Devic	e List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (3)							
O 85NS-1120-3 Short 3 10.48.67.69 - Roused	Firepower 1120 with FTD	7.0.1	N/A	Essentials, IPS (2 more)	Allow-Any	N/A	1
EMEA-FPR3105-19 Short 3 10.48.189.24 - Routed	Firewall 3105 Threat Defense	7.4.1	Manage	Essentials	Allow-Any	49	1

已禁用裝置

FMC不會自動刷新CA並將憑證重新發佈到FTD裝置。此外,也沒有指示證書到期的FMC運行狀況 警報。在此方面跟蹤思科錯誤ID <u>CSCwd08448</u>,以便將來在FMC UI上提供運行狀況警報。

到期日期後會發生什麼?

一開始什麼也沒發生,而sftunnel通訊通道繼續像以前一樣運行。但是,當FMC和FTD裝置之間的 sftunnel通訊中斷並嘗試重新建立連線時,它確實會失敗,並且您可以觀察消息日誌檔案中指向證書 到期的日誌行。

來自FTD裝置的/ngfw/var/log/messages的日誌行:

```
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [INFO] Initiating IPv4 connection
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [INFO] Wait to connect to 8305 (IP
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [INFO] Connected to 10.10.200.31 f
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] -Error with certificate at
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] issuer = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] subject = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] subject = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] err 10:certificate has e
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] Connect:SSL handshake fail
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] Connect:SSL handshake fail
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunneld:sf_ss1 [ERROR] SSL Verification status: ce
```

來自FMC裝置的日誌行,來自/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: 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: iret_
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: iret_
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: iret_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: iret_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: iret_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: iret_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: iret_Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunneld:sf_ssl
```

Sftunnel通訊可能由於多種原因而中斷:

- 由於網路連線丟失而丟失通訊(可能只是暫時的)
- 重新啟動FTD或FMC
 - ◎ 預期的:在FMC或FTD上手動重新啟動、升級、手動重新啟動sftunnel程式(例如通過 pmtool restartbyid sftunnel)
 - ◎ 意外的:回溯,斷電

由於有太多可能性會中斷sftunnel通訊,因此強烈建議儘快糾正情況,即使目前所有FTD裝置都已正 確連線(儘管憑證已過期)。

如何快速驗證憑證是否已到期或何時到期?

最簡單的方法是在FMC SSH會話上運行以下命令:

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

此處顯示憑證的「有效性」元素。此處的主要相關部分是「notAfter」,它表明此證書有效期至 2034年10月5日。

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

NotAfter

如果您偏好立即執行單一命令,並給予您憑證仍然有效的天數,則可使用以下命令:

CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=\$(openss1 x509 -enddate -noout -in "\$CERT_PATH" | c

此處範例顯示憑證仍然有效多年的設定專案。

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 certificate for \$0 and \$0 and

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_expire_validation_command

以後如何獲得有關即將到期的證書的通知?

使用最近的VDB更新(399或更高),當證書在90天內到期時,系統會自動通知您。因此,您自己 無需手動跟蹤,因為當您接近到期時間時會收到警報。然後,它以兩種形式顯示在FMC網頁上。這 兩種方式均請參閱<u>現場通知頁面</u>。

第一種方法是通過Task Tab。此消息是粘性的,除非明確關閉,否則使用者可以使用它。通知也會 彈出,直到使用者明確關閉時才可用。它始終顯示為錯誤。

Deployments Upg	grades 🛛 🔒 Health	Tasks		C si
19 total 0 waiting	0 running 0 retrying	15 success	2 failures	Q Filter
Local Install Firewall Managemen Threat Defense cann Unknown Failure Condit certificate.	t Center's internal root o ot be managed and ma on. Previous state: Review	certificate has ex y experience de the Field Notice FN	pired. As a res gradation. #74214 and rege	ult, Firewall

「任務」頁籤上的到期通知



第二種方法是通過Health Alert。這顯示在運行狀況頁籤中,但這不是粘滯狀態,在運行運行狀況監 視器時替換或刪除該資訊,預設情況下,運行狀況監視器每5分鐘運行一次。它還顯示一個通知彈出

視窗,使用者需要顯式關閉該視窗。這可以同時顯示為錯誤(過期時)和警告(即將過期時)。

Deployments Upgra	ades 🕕 Health 🌔	1 Tasks	Show Notification
2 total 0 warnings	2 critical 0 errors		् Filter
Firepower Management Center	r		
firepower			
firepower 9 Appliance Heartbeat	Firewall Management Ce	enter's internal root	certificate has expired. As a result, Firew
firepower 9 Appliance Heartbeat	Firewall Management Ce Threat Defense cannot b Notice EN #74214 and r	enter's internal root be managed and ma	certificate has expired. As a result, Firew ay experience degradation.Review the Fie
firepower Appliance Heartbeat	Firewall Management Ce Threat Defense cannot b Notice FN #74214 and re	enter's internal root be managed and ma regenerate the certi	certificate has expired. As a result, Fireway ay experience degradation.Review the Fie ficate.
firepowerAppliance HeartbeatSmart License Moni	Firewall Management Ce Threat Defense cannot b Notice FN #74214 and re Smart Licensing evaluati	enter's internal root be managed and ma regenerate the certi ion mode expired	certificate has expired. As a result, Firewa ay experience degradation.Review the Fie ficate.
firepower Appliance Heartbeat Smart License Moni	Firewall Management Ce Threat Defense cannot b Notice FN #74214 and re Smart Licensing evaluati	enter's internal root be managed and ma regenerate the certin ion mode expired	certificate has expired. As a result, Firewa ay experience degradation.Review the Fie ficate.

「健康」頁籤上的到期通知

健康警報彈出時的警告通知

	Dismiss all notifications
Shc	Appliance Heartbeat – firepower X Firewall Management Center's internal root certificate has expired. As a result, Firewall Threat Defense cannot be managed and may experience degradation.Review the Field Notice FN #74214 and regenerate the certificate.
	Auu viiugets

出現健康警報彈出錯誤通知

解決方案1 — 證書尚未過期(理想情況)

這是最佳情況,因為根據證書到期時間,我們還有時間。我們要麼採用依賴於FMC版本的全自動方 法(推薦),要麼採取需要TAC互動的更手動的方法。

推薦的方法

這種情況下,正常情況下預計不會出現停機時間和最少的人工操作。

在繼續操作之前,您必須按此處所列安裝特定版本的<u>修補程式</u>。此處的好處是,這些修補程式不要 求重新啟動FMC,因此當證書過期時,可能會中斷sftunnel通訊。可用的修補程式包括:

- 7.0.0 7.0.6:修補程式FK 7.0.6.99-9
- 7.1.x:軟體維護結束時無固定版本
- 7.2.0 7.2.9:修補程式FZ 7.2.9.99-4
- 7.3.x:修補程式AE 7.3.1.99-4
- 7.4.0 7.4.2:修補程式AO 7.4.2.99-5
- 7.6.0:修補程式B 7.6.0.99-5

安裝修補程式後,FMC現在應包含generate_certs.pl指令碼:

- 1. 重新生成內部CA
- 2. 重新建立由此新的InternalCA簽名的sftunnel證書
- 3. 將新的sftunnel憑證和私鑰推送到各自的FTD裝置(當sftunnel運作時)

因此,建議(如果可能):

- 1. 安裝上面適用的修補程式
- 2. 對FMC進行備份
- 3. 在FMC上使用sftunnel_status.pl腳本驗證所有當前的sftunnel連線(從專家模式)
- 4. 使用generate_certs.pl從專家模式運行指令碼
- 5. 檢查結果以驗證是否需要任何手動操作(當裝置未連線到FMC時)[下面將進一步說明]
- 6. 從FMC運行sftunnel_status.pl,以驗證所有sftunnel連線是否運行正常

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-key.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
```

Some files were failed to be pushed to remote peers. For more details check /var/tmp/certs/1728915794/FAILED_PUSH

Scalars leaked: 1 root@fmcv72-stejanss:/Volume/home/admin#

Generate_certs.pl指令碼



附註:當在High-Availability(HA)中運行FMC時,您需要先在主節點上執行操作,然後在輔助節點上執行操作,因為它使用這些證書並在FMC節點之間進行通訊。兩個FMC節點上的 InternalCA不同。

在此處的示例中,您看到它在/var/log/sf/sfca_generation.log上建立日誌檔案,指示使用 sftunnel_status.pl,指示InternalCA上的到期時間並指示其上的任何故障。例如,它未能將證書推送 到裝置BSNS-1120-1和EMEA-FPR3110-08裝置,這是預期的,因為這些裝置的sftunnel已關閉。

為了更正失敗連線的sftunnel,請運行以下步驟:

1. 在FMC CLI上,使用cat /var/tmp/certs/1728303362/FAILED_PUSH(number值代表unix時間 ,因此請檢查系統中上一個命令的輸出)開啟FAILED_PUSH檔案,該檔案採用以下格式: 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
<u>c8d5d5c6-87c9-11ef-a993-b9</u> 831565bc4e 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. 透過這些新憑證(cacert.pem / sftunnel-key.pem / sftunnel-cert.pem)從FMC傳輸至FTD裝置 ===自動方法===

該修補程式安裝還提供了copy_sftunnel_certs.py和copy_sftunnel_certs_jumpserver.py指令碼 ,這些指令碼可將各種證書自動傳輸到在重新生成證書時未啟動sftunnel的系統。這也可用於 由於證書已過期而導致sftunnel連線斷開的系統。

當FMC本身擁有對各種FTD系統的SSH存取權時,可以使用copy_sftunnel_certs.py指令碼。 如果情況並非如此,您可以將指令碼(/usr/local/sf/bin/copy_sftunnel_certs_jumpserver.py)從 FMC下載到具有SSH訪問FMC和FTD裝置的跳轉伺服器,並從那裡運行Python指令碼。如果 同樣不可能,則建議運行下文所示的手動方法。以下示例顯示正在使用的 copy_sftunnel_certs.py指令碼,但copy_sftunnel_certs_jumpserver.py指令碼的步驟相同。

A.在FMC(或跳轉伺服器)上建立一個CSV檔案,該檔案包含用於建立SSH連線的裝置資訊 (裝置名稱、IP地址、管理員使用者名稱、管理員密碼)。

當您從遠端伺服器(如主FMC的跳轉伺服器)運行此命令時,請確保在主FMC詳細資訊中新 增第一個條目,後跟所有託管FTD和輔助FMC。當您從遠端伺服器(如輔助FMC的跳轉伺服 器)運行此命令時,請確保將輔助FMC詳細資訊新增為第一個條目,後跟所有託管FTD。

i.使用vi devices.csv建立檔案。root@firepower:/\olume/home/admin# vi devices.csv

vi devices.csv

二。這將開啟空檔案(未顯示),並在您使用鍵盤上的i letter進入互動模式(在螢幕底部看到)後填寫詳細資訊,如圖所示。 #device_name,ipaddr,login,password FMCpri,10.48.79.125,admin,C1sc0!23 FTDv,10.48.79.25,admin,C1sc0!23 BSNS-1120-1,172.19.138.250,admin,C1sc0!23



devices.csv示例



B.使用copy_sftunnel_certs.py devices.csv運行指令碼(使用sudo從根目錄中),並顯示結果。 此處顯示已正確推送到FTDv的憑證,且對於BSNS-1120-1,無法建立到裝置的SSH連線。

copy_sftunnel_certs.py devices.csv



1. 從先前的輸出(FAILED_PUSH檔案)中複製檔案位置,在FMC CLI上列印每個受影響 的FTD(cacert.pem / sftunnel-key.pem(未出於安全目的完整顯示)/ sftunnelcert.pem)的輸出(cat)。 root@fmcv72-stejanss:/Volume/home/admin# cat /etc/sf/ca_root/cacert.pem
----BEGIN CERTIFICATE----

MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwgYcxEzARBgNVBAwMCkludGVybmFs 00ExJDAiBqNVBAsMG0ludHJ1c2lvbiBNYW5hZ2VtZW50IFN5c3RlbTEtMCsGA1UE AwwkY2RiMTIzYzgtNDM0Ny0xMWVmLWFjYTEtZjNhYTI0MTQxMmExMRswGQYDVQQK DBJDaXNjbyBTeXN0ZW1zLCBJbmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy MzI4WjCBhzETMBEGA1UEDAwKSW50ZXJuYWxDQTEkMCIGA1UECwwbSW50cnVzaW9u IE1hbmFnZW11bnQqU31zdGVtMS0wKwYDV00DDCRjZGIxMjNj0C00Mz03LTExZWYt YWNhMS1mM2FhMjQxNDEyYTExGzAZBgNVBAoMEkNpc2NvIFN5c3RlbXMsIEluYzCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMmUav8kVukF xiV917W4d7/CYBb4pd1KiMOijAEp3wqxmdpDUQ4KBDWnC5+p8dq+XK7AspOW36CD mdpRwRfqM7J51txEUyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6VlQl+aRlAPCF 7UYpMaFPh3Wp+T9tax1HabE28JktD1Nu/iism5lvxtZRadEXnL6Jn3rfoKbF0M77 xUtiMeC0504buhfzSltAm5J0bFuXMcPYq1N+t137rl/1etwHzmjVkE7q/rfNv0v0 N+4m8i5QRN0BoghtZ0+Y/PudToSX0VmKh5Sq/i1Mv0YBZEIM3Dx+Gb/DQYBWLEUC AwEAATANBgkghkiG9w0BAQsFAAOCAQEAY2EVhEoy1Dd1WSu2ewdehthBtI6Q5x7e UD187bbowmTJsdl00LVGgYoU5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6 J301F3hJJF0qSrlIx/ST72jqL2o87ixhRIzreB/+26rHo5nns2r2tFss61KBltWN nRZnSIYAwYhqGCjH9quiZpfDJ3N83oREGX+xflYqFim5h3rFwk0J2q6YtaBJAuwq 0bldXGnrnWuIIV/xbOcwKbrALmtanhgGXyqT/pMYrjwlI1xVL16/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//sftunr el-key.pem -----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDcy5A0xZ5N22qD

sftunnel-key.pem



- 2. 透過sudo su在expert模式下開啟每個相應FTD的FTD CLI,並依照下一個程式續訂憑證
 - 0
 - 瀏覽至FAILED_PUSH輸出中淺藍色突出顯示區域上顯示的位置(例如,cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1,但每個FTD的顯示位置 不同)。
 - 2. 備份現有檔案。

```
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-rr 1 root root 1.5K Oct 14 12:41 sftunnel-cert.pem
-rw-rr 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-rr 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-rr 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-rr 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-rr 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-rr 1 root root 1.3K Oct 14 12:41 cacert.pem

備份當前證書

3. 清空檔案,以便我們在其中寫入新內容。

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

現有證書檔案的內容為空

4. 使用vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem (每個檔案的單獨 命令 — 螢幕截圖僅對cacert.pem顯示此資訊,但對sftunnel-cert.pem和sftunnelkey.pem需要重複此資訊),在每個檔案中單獨寫入新內容(來自FMC輸出)。___

vi cacert.pem

- 1. 按i進入互動模式(輸入vi命令後,您會看到一個空檔案)。
- 2. 複製貼上檔案中的整-----內容-----包括-----BEGIN CERTIFICATE-----和(END

CERTIFICATE))。

-----BEGIN CERTIFICATE----MIIDhDCCAmwCAQAmDQYJKoZIhvcNAQELBQAwgYcxEzARBgNVBAwMCkludGVybmFs Q0ExJDAiBgNVBASMG0ludHJlc2lvbiBNYWShZ2Vt2W50IFNSc3RlbTetMCsGAIUE AwwkYZRiMTIzYzgtNDM0Ny0xMWVmLWFjYTEtZJNhYTI@MTQxMmExMRswGQYDVQQK DBJDaXNjbyBTeXN0ZW1zLCBJbmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy MzI4WjCBhzETMBEGA1UEDAwKSW50ZJuYWxDQTEkMCIGA1UECwwbSW50cnVza0W9u IE1hbmFnZW1lbnQgU31zdGVtMS0wKwYDVQQDDCRjZGIxMjNj0C00MzQ3LTexZWYt YWNhMSinMZFhMjQxNDEyYTExCzAZBgNVBAOMEKNpcZVIFNSc3RlbXMsIEluYzCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQocggEBANHWuapG1tBJXMmUav8kVukF xiV917W4d7/CYBb4pdIXiMDijAEp3wqxmdpDUQ4KBDWnC5+p8dg+XK7Asp0W36CD mdpRwRfqM7J51txEUyCJEmiRYFEHE0eccsUWXGSLcL18CHGjHMx6V1Q1+aRLAPCF 7UYPMgFPh3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXnL6Jn3rf6KbF0M77 xUtiMeC0504buhfzS1tAm5J0bFuXMCPYq1N+t137r1/1etwHzmjVkE7g/rfNv0y0 N+4m8i5QRN0BoghtZ0+Y/PudToSX0VMKhSSq/i1Mv0YBZEIM3Dx+Gb/DQYBUEUC AwEAATANBgkqhkiG9w0BAQ5FAA0CAQE4Y2EVh6oy1Dd1WSu2ewdehthB1E0Q5x7e UD187bbowmTJsd100LVGgY0U5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6 J3Q1F3hJJF0q5r11x/ST72jgL2087ixhRIreeB+26rHo5nns2r2tFss61KB1tWN nRZnSIYAwYhqGCjH9quiZpfDJ3N830REGX+xf1YGFim5h3rFwk0J2aGYtaBJAuwg 0b1dXGnrnWuIIV/xb0cwKbrALmtanhgGXyqT/pMYrjwI11xVL16/PrMTV29WcQcA IVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnstyGx8h1zRvzHz2w== -----END CERTIFICATE-----

- INSERT --

在vi(插入模式)中複製內容

3. 關閉並使用ESC後跟:wq寫入檔案,然後輸入。



ESC後跟:wq以寫入檔案

5. 使用ls -hal驗證是否為每份檔案設定了正確的許可權(chmod 644)和擁有者(chown root:root)。實際上在更新現有檔案時已正確設定。

root@BSNS-1	L12	20-1:/	/var/s	sf/pee	ers/o	cdb1	123c8-4	1347-11ef-aca1-f3aa241412a1# ls -hal
total 68K								
drwxr-xr-x	4	root	root	4.0K	0ct	14	15:01	
drwxr-xr-x	3	root	root	4.0K	0ct	14	15:01	
-rw-rr	1	root	root	0	0ct	14	12:42	LIGHT_REGISTRATION
-rw-rr	1	root	root	0	0ct	14	12:42	LIGHT_UNREGISTRATION
-rw-rr	1	root	root	2.0K	0ct	14	12:45	LL-caCert.pem
-rw-rr	1	root	root	2.2K	0ct	14	12:45	LL-cert.pem
-rw-rr	1	root	root	3.2K	0ct	14	12:45	LL-key.pem
-rw-rr	1	root	root	1.3K	0ct	14	14:55	cacert.pem
-rw-rr	1	root	root	1.3K	0ct	14	14:49	cacert.pem.backup
-rw-rr	1	root	root	2.3K	0ct	14	12:41	ims.conf
-rw-rr	1	root	root	221	0ct	14	12:41	peer_flags.json
drwxr-xr-x	3	root	root	19	0ct	14	12:42	proxy_config
-rw-rr	1	root	root	1.2K	0ct	14	12:42	sfipproxy.conf.json
-rw-rr	1	root	root	1.4K	0ct	14	14:59	sftunnel-cert.pem
-rw-rr	1	root	root	1.5K	0ct	14	14:49	sftunnel-cert.pem.backup
-rw-rr	1	root	root	1	0ct	14	14:21	sftunnel-heartbeat
-rw-rr	1	root	root	1.7K	0ct	14	15:01	sftunnel-key.pem
-rw-rr	1	root	root	1.7K	0ct	14	14:49	sftunnel-key.pem.backup???
-rw-rr	1	root	root	0	0ct	14	14:50	sftunnel-key.pem???
-rw-rr	1	root	root	521	0ct	14	12:41	sftunnel.json
-rw-rr	1	root	root	5	0ct	14	12:48	sw_version
drwxr-xr-x	6	root	root	90	0ct	14	12:42	sync2
root@BSNS-1	12	20-1:/	/var/s	sf/pee	ers/o	cdb1	123c8-4	1347-11ef-aca1-f3aa241412a1#

所有證書檔案已更新,具有適當的所有者和許可權

3. 在每個FTD上(其中sftunnel無法運作)重新啟動sftunnel,使憑證的變更通過指令生效 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. 使用sftunnel_status.pl輸出驗證所有FTD現在是否已正確連線

解決方案2 — 證書已過期

在這種情況下,我們面臨兩種不同的情形。所有sftunnel連線都仍然可以運行或者不再運行(或者不 完整)。

FTD仍透過sftunnel連線

我們可以應用「證書尚未過期(理想情況) — 推薦方法」一節中說明的相同步驟。

但是在這種情況下,請勿升級或重新啟動FMC(或任何FTD),因為它會斷開所有sftunnel連線 ,且我們需要手動在每個FTD上執行所有憑證更新。唯一例外是列出的修補程式版本,因為它們不 需要重新啟動FMC。

通道會保持連線狀態,且會在每個FTD上交換憑證。如果某些證書無法填充,則會提示您填充失敗 的證書,您需要採取上節前面所提到的<u>手動</u>方法。

FTD不再通過sftunnel連線

推薦的方法

我們可以應用「證書尚未過期(理想情況) — 推薦方法」一節中說明的相同步驟。在此案例中,新憑 證將產生於FMC上,但無法複製到裝置上,因為通道已關閉。可以使用<u>copy sftunnel certs.py/</u> <u>copy sftunnel certs jumpserver.py指令碼自動執行此過</u>程

如果所有FTD裝置都從FMC斷開,我們可以在此情況下升級FMC,因為它對sftunnel連線沒有影響 。如果仍有一些裝置通過sftunnel連線,則請注意,FMC的升級會關閉所有sftunnel連線,並且由於 證書過期,它們不會再次出現。此處的升級好處在於,它確實能提供需要傳輸至各個FTD的憑證檔 案的良好指南。

手動方法

在這種情況下,接著您可以從FMC執行generate_certs.pl 指令碼,此指令碼將產生新憑證,但您仍 需要手動將它們推送到各個FTD<u>裝置</u>。根據裝置數量,這是可行或繁瑣的任務。但是,使用 <u>copy_sftunnel_certs.py / copy_sftunnel_certs_jumpserver.py指令碼時,此操</u>作高度自動化。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。