對FMC上的證書錯誤「需要匯入身份證書」進行 故障排除

目錄

簡介
必要條件
需求
採用元件
背景資訊
問題
解決方案
步驟1。產生CSR(可選)
步驟2.簽署CSR
步驟3.驗證並分離憑證
步驟4.合併PKCS12中的證書
步驟5.匯入FMC中的PKCS12證書
驗證

簡介

本文說明如何排解和修正由Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)裝置上的「需要身份證書匯入」錯誤。

必要條件

需求

思科建議您瞭解以下主題:

- 公開金鑰基礎架構 (PKI)
- FMC
- FTD
- OpenSSL

採用元件

文中使用的資訊是根據以下軟體版本:

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

背景資訊

附註:在FTD裝置上,需要先取得憑證授權單位(CA)憑證,才能產生憑證簽署請求(CSR)。

如果在外部伺服器(例如Windows Server或OpenSSL)中產生CSR,則手動註冊方法會失敗,因為FTD不支援手動金鑰註冊。必須使用其他方法,例如PKCS12。

問題

在FMC中匯入證書並收到一個錯誤,說明需要身份證書才能繼續進行證書註冊。

案例 1

- 已選擇手動註冊
- CSR是從外部生成的(Windows Server、OpenSSL等),您沒有(或知道)私鑰資訊
- •以前的CA證書用於填充CA證書資訊,但不知道此證書是否負責證書簽名

In progress

案例 2

- 已選擇手動註冊
- CSR是從外部生成的(Windows Server、OpenSSL)
- 您有來自CA的憑證檔案,用於簽署我們的CSR

兩個程式都會上傳憑證,並顯示進度指示,如下圖所示。

Manual

FPR1k-172.204.204.66 wildcart-cert-2020

幾秒鐘後,FMC仍宣告需要ID證書:

Global

FPR1k-172.204.204.66 wildcart-cert-2020

上一個錯誤指出CA憑證與ID憑證中的頒發者資訊不相符,或是私鑰與FTD中預設產生的私鑰不相符 。

CA A ID 🛕 Identity certificate import required

208

20 8

解決方案

要使此證書註冊生效,您必須具有ID證書的相應金鑰。使用OpenSSL可產生PKCS12檔案。

步驟1。產生CSR(可選)

您可以使用稱為CSR generator(csrgenerator.com)的第三方工具取得CSR及其私密金鑰。

在相應填寫證書資訊後,選擇**生成CSR**選項。



Generate a Certificate Signing Request

Complete this form to generate a new CSR and private key.

Country			
US			
State			
Texas			
Locality			
San Antonio			
Organization			
Big Bob's Beepers			
Organizational Unit			
Marketing			
Common Name			
example.com			
Key Size			
Generate CSR			

這提供了CSR +私鑰以便我們傳送到證書頒發機構:

👱 IIN 💷 🔲 😖



Close

步驟2.簽署CSR

tingsPolicyList

CSR需要由第三方CA(GoDaddy、DigiCert)簽署,一旦簽署CSR,便會提供一個zip檔案,其中包括 :

• 身份證書

• CA套件組合(中間憑證+根憑證)

步驟3.驗證並分離憑證

使用文字編輯器(例如記事本)驗證和分隔檔案。 為私密金鑰(key.pem)、身分識別憑證 (ID.pem)和CA憑證(CA.pem)建立具有可輕易識別名稱的檔案。 如果CA套件組合檔案具有超過2個憑證(1個根CA、1個子CA),則需要移除根CA,ID憑證發出者 是子CA,因此,在此案例中與具有根CA無關。

名為CA.pem的檔案的內容:

Bag Attributes

localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8 subject=/C=US/ST=Texas/L=San Antonio/O=Cisco/OU=VPN/CN=*.cisco.com issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU= Corp Certificate Authority/CN=Corp Intermediate CA -BEGIN CERTIFICATE-MIIFojCCA4qgAwIBAgICEBowDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCTVgx DTALBgNVBAgMBENETVgxEjAQBgNVBAoMCVVuZ3UgQ29ycDEoMCYGA1UECwwfVW5n dSBDb3JwIEN1cnRpZmljYXRlIEF1dGhvcml0eTEiMCAGA1UEAwwZVW5ndSBDb3Jw IEludGVybWVkaWF0ZSBDQTAeFw0yMDAyMjcwNjE1MjRaFw0yMTAzMDgwNjE1MjRa MGcxCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVUZXhhczEUMBIGA1UEBwwLU2FuIEFu dG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANWUE4xFDASBgNVBAMMCyou Y21zY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsrPghHA3 7r/ShqU7Hj016muESBwmeDYTb0SBDz6T30E95T67Ey0ra8/sxyorCMzTHSPr6adF o7xbrjm1onhneeJv+6sUbF1FnZnyNjrjAd/6u8BCJcXPdHESp4kvFGv8fuNAE01s gjfuj+Ap1iPbWUjsxs1CDlq208H/NyPn+mvu2Kvo1sJZls5VAAk6D2FxSpwos4tV sXUn711ymzyArhDMQ0sGib8s8oOPqnBYPhy12+AWECqHTccMbsVxC3S11hHQMPCi LAEC/ijQeISMOxdR/p4CpjbuNJTIQQw8CRqjSvkY2DGZs3slLo56RrHpRJdcukD5 zKGRLrKCt0jvyQIDAQABo4IBPzCCATswCQYDVR0TBAIwADARBglghkgBhvhCAQEE BAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIFNlcnZlciBD ZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUzED6CQ5u/wcK7y+GYz9ccDkrUigwgaEGA1Ud IwSBmTCBloAUT8MBVNLJSgdOEG3GW+KnUvRMRCihegR4MHYxCzAJBgNVBAYTAk1Y MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDA1Vbmd1IENvcnAxKDAmBgNVBAsMH1Vu Z3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxGjAYBgNVBAMMEVVuZ3UgQ29y cCBSb290IENBggIQADAOBgNVHQ8BAf8EBAMCBaAwEwYDVR01BAwwCgYIKwYBBQUH AwEwDQYJKoZIhvcNAQELBQADggIBAJuAihWxJ44ug/vEhZaUapUtYSqKWzMLZbBr un1IMsL8I8AhuWM93PPmHX2Tm2XwQlo9PBN3aNacUz/FneZ/NNfQwC1GfJCTHJVE K4+GWDNIeVznY7hbMppt5iJNuBMR/EoYoQ0xdqPtnLEqt92WgGjn6kvjVLw6eJKB Ph75RDyr5DQz86Agn1/JzjvpeLR10eqMTCxgQJbY0eUrZCRNDWaV/ahpvmZ9xPV6 MB1la6GipT5EcFe16WPNiqQa+3f+y8nsnsMDNE8UXW8nSqZwdTdA8THxkpogcPTb isw8a9CkindzZhI6rtoCI0QXmgkw6uXPWcw5PnTT08TnSQoMJnC/Hvaa/tiiFA3F dkaPLePgDScFZED2nPIFsbXfb2zFRCN2YLirose/k9wc8rX1Z639uVCXN4yYmx9b ADrqqQdkUXCGCGrQjXzWRNCORZihfTKg+ANoEaWgBsgInqtV5R/nsSkeibva9rBG vHPUkZB70Xz2AuINod70aPDiQCabEpVTcV5dr8+r9L1h5UQCIim+wPqBAQzG9Bz9 JM5RHriNhdmKQkvjDbqcKx8V3tjYpDNHgWAlwnaoICEoDKbSoiLdWgaPt4F1kipW 2RImd7X9wPetswGe0pI3q39mBtgQ1eAARXVB373i12WvxEWnjfBa9V4GAZcoMjpx 92xpoxS1 -END CERTIFICATE-

名為key.pem的檔案的內容:

Bag Attributes

localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8 Key Attributes: <No Attributes>

----BEGIN ENCRYPTED PRIVATE KEY---

MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI9vQUkrE10MMCAggA MBQGCCqGSIb3DQMHBAjnRV9YTIYsSwSCBMjqflLhs3v0RL0DHkvi7yvWSd3xWLMn jt1hg0LsU1TDmBAWp/LXpqSP27c4XCQiZcOeiFDqm8aKw9xTDjgkEUBVactZs+Sz vCE1gcG6NRH91ZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlywfAtrAcQk E5tJniCaNTppwfVOfLpd/oHa2tFOkBMVVjS3HyxAXEfNThmzMwKRygsLPUKShtfb iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZ071H3DW0HamtPw3InUuvYuzv SM08x+NJi6uo7gtrQ6Rld2z5fN6vTtAw3xl0AHjxm+vf0xt95zXhABYkMg2zHaQg 0djTHYFWdHwpdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v PzUwIDWs6kt0rxp0v82001mqSKD6C4UnD1Vf2hH7AyMuwRpYamOEIuPtg8GgeiHJ 6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTGyR08AE56ig2+XiBkwIoUai QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXxXcH3mHPaMU/Nhdldn8fpx+ phTzULmdtIpD3rlHknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhuf0I7vtPp rQqXNo6JleXuBteWSIHDqFynrtIdLyUVhK5QwF40m9+0vGkXNuqMDv4fH4+7nv91 KqK2NS4yUXW1KjbAFe+Cxz9E7stt4Nyvwx561/FpYLHymYDjQA3kFrC3tPHeULjT fp95fJ+6g2ROnr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA TZLj/BDxIc40Q6A0RATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTNcQD nmaFYykWVxYCzsvQAgwkvyzzZw2mPNQpj3lVIOVRdZy8NWVkKCBLpq2XTSA6AQIK mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwkP/KhEHKmipEoHS8b5 MLby4tL7grA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxgaY Int7b6p90i1r0LpielhUUrEvbu0CudM4sLDyXg8Fgf9G5u8dMuchCjXrEPGhmf4Y ZhTfQF3xxQYtLBbLfWeQUFt6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa bcT868DNME+UQxoT825SLwsFFPcj0pixn21FSm6baig6QWvTV9+5797+AEPnG23i 1x/KKsvTEuwyHGgAX6p9Z0bfPOVcikMZkO9MvMDU5MOUm0lbnb0zINrrblG0qmRX SYNNoL71J3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWx0SAszRMkneptiR VCm5UvzbYiMIAOrJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN 2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM C1dBcaJLWdpdTmrg2WNiao/rv3A20JjPOzAOeUwRo9r5OS0oF9ez1ghBpAAtehyi FGY=

----END ENCRYPTED PRIVATE KEY-----

名為ID.pem的檔案的內容:

---BEGIN CERTIFICATE----

MIIFtzCCA5+gAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwgZIxCzAJBgNVBAYTAk1Y MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDAlVbmd1IENvcnAxMjAwBgNVBAsMKUFu eWNvbm51Y3QgaG9sZ3VpbnMgQ2VvdG1maWNhdGUgQXV0aG9vaXR5MSwwKgYDVQQD DCNBbnljb25uZWN0IGhvbGd1aW5zIEludGVybWVkaWF0ZSBDQTAeFw0yMDA0MDUy MjI3NDhaFw0yMDA0MjUyMjI3NDhaMGcxCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVU ZXhhczEUMBIGA1UEBwwLU2FuIEFudG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYD VQQLDANWUE4xFDASBgNVBAMMCyouY21zY28uY29tMIIBIjANBgkqhkiG9w0BAQEF AAOCAQ8AMIIBCgKCAQEAxcrtoc7qbNIqPD5jwxTZRZPTQJbDE9y/WIySZWQ0CEL9 AwFSziHOsuXpivM4Q5Lx1TOPhHaPS7lligmIfca4m2/5E6n4kMqUMn1PTR+7QGT7 j+0872AA0Rr0tag7XmdBSw7V66aTodkYhrJoUxHsCdey5D1xdapyvzl2hHcYqemi HZtXthVq1XTfeC2LGESvz1cb0++MKcraeZgykM6Ho3aaOG52w1xzF1FGUe2nkKaT I6WcuD4dnQLXFiWDGmh7foQ30biFyJ4MjT4QZBCQdW080axeYCQbR38Qn28tFzuU /xj33kUKyExuJeSFuZoKcuwhrPgwekcvYxw4NzMOuQIDAQABo4IBPzCCATswCQYD VR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5T U0wgR2VuZXJhdGVkIFNlcnZlciBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQURWLK5NOS K1NN/LPU6E0Q/SVp/K0wgaEGA1UdIwSBmTCBloAUzMVIA+G1XbnwtEZX0syJQGUq jeahegR4MHYxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDA1V bmd1IENvcnAxKDAmBgNVBAsMH1VuZ3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3Jp dHkxGjAYBgNVBAMMEVVuZ3UgQ29ycCBSb290IENBggIQAjAOBgNVHQ8BAf8EBAMC BaAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBAJtmMncK 3iF+q31fE8/m3gghNjfkqrvyCkILnwuw2vx2CHCMgGzU4MT5AodGJfJJZNq2Cbhy VaPGm7/X010gW5dfbeHPLvyWqdK4nQLtw2kr1pRznoeEk16qumPBrHVmWUZQoWpV elDzSigzhbv+vFMP40F0lbMYHDSAcolLedCS7KuQ/c0soGNR1oGSA2hUYM60MEiW ezBgT7R/XK+Rh5zwlok4mje8R1rY7qUIn/hrKUDf/JNiBNFUvD6vDYLHJA3W2s10 ou3vdLy7z57Lj4WbtheHXQsmD6n9N+ANxmHpgpWPPD94YRalvpDbefU2hYrHx7fn 1jSdpzyOmw6JluxWbW0kp+BER+5Ya3rqIpBtljfbhZ18C17Hhb5oixSqBwL6oGa9 vOu6mhVHQBrPLeg+A/Pfkmpwq/wr19iUOLW+tJ8Lc7/Qlst7kCEjncub4SNvb6cx RRzi53fE3MVVqL6pBpBm4Pgt552ku7Lr3254haAmIczQ6Lxhq28Wo/Sq6bND1XBh Wg8ZfjpwraAloKStUPYPQyHuz6POuPGybaBjyjChkTooO3CkBpl1YIZdttZMtFHC bmKJMQ45LsaF5aGcuL0sr4YB2EyJBVU4vAWnVJ7j1SZOnntPFNebfRKV/hjZ4k+g ViWh5GmceXBbcTQ7wbVxpbYFnXtYge780zUz ---END CERTIFICATE----

步驟4.合併PKCS12中的證書

將CA證書與ID證書和.pfx檔案中的私鑰合併。您必須使用密碼保護此檔案。

openssl pkcsl2 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx HOLGUINS-M-Q3UV:tshoot hugoolguin\$ openssl pkcsl2 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx Enter pass phrase for key.pem: Enter Export Password: Verifying - Enter Export Password: HOLGUINS-M-Q3UV:tshoot hugoolguin\$

步驟5.匯入FMC中的PKCS12證書

在FMC中,導覽至Device > Certificates,然後將憑證匯入所需的防火牆:

Add Cert Enrollment

Name*	new-cert-pfx	
Description		
CA Information	Certificate Parameters Key	Revocation
Enrollment Type:	PKCS12 File	~
PKCS12 File*:	new-cert.pfx	Browse PKCS12 File
Passphrase:	••••••	
Allow Overrides		
		Save Cancel

驗證

若要確認憑證狀態以及CA和ID資訊,您可以選擇圖示並確認其已成功匯入:

 rew-cert-pfx
 Global
 PKCS12 file
 CA
 LD
 2 ♥ 目

選擇ID**圖**標:

Identity Certificate

- Serial Number : 101a
- Issued By :

Common Name : Ungu Corp Intermediate CA Organization Unit : Ungu Corp Certificate Authority Organization : Ungu Corp State : CDMX Country Code : MX

Issued To :

Common Name : *.cisco.com Organization Unit : VPN Organization : Cisco Locality : San Antonio State : Texas

Close

? 🔺 🗙

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)。