Solucione problemas de falha de instalação de arquivo PKCS#12 com algoritmos PBE não compatíveis com FIPS

Contents

Introduction

Este documento descreve como solucionar problemas de falha de instalação de um arquivo PKCS (Public Key Cryptography Standards)#12 com algoritmos PBE (Password-Based Encryption - Criptografia Baseada em Senha) compatíveis com FIPS (Non-Federal Information Processing Standard) via Cisco Firepower Management Center (FMC). Ele explica um procedimento para identificá-lo e criar um novo pacote compatível com o OpenSSL.

Informações de Apoio

O Cisco Firepower Threat Defense (FTD) oferece suporte à conformidade com o FIPS 140 quando você habilita o modo Common Criteria (CC) ou Unified Capabilities Approved Products List (UCAP) em um dispositivo gerenciado. Essa configuração faz parte de uma política de configurações da plataforma FMC. Depois de aplicado, o comando **fips enable** aparece na saída **show running-config** do FTD.

PKCS#12 define um formato de arquivo usado para agrupar uma chave privada e o respectivo certificado de identidade. Há a opção de incluir qualquer certificado raiz ou intermediário que também pertença à cadeia de validação. Os algoritmos PBE protegem os certificados e partes de chave privada do arquivo PKCS#12. Como resultado da combinação do esquema de autenticação de mensagens (MD2/MD5/SHA1) e do esquema de criptografia (RC2/RC4/DES), há vários algoritmos PBE, mas o único compatível com FIPS é PBE-SHA1-3DES.

> **Note**: Para saber mais sobre o FIPS em produtos da Cisco, navegue até FIPS 140.

> **Note**: Para saber mais sobre os padrões de certificações de segurança disponíveis para FTD e FMC, navegue até o capítulo **Conformidade com certificações de segurança** do Guia de Configuração do FMC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Public Key Infrastructure (PKI)
- OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- FMCv - 6.5.0.4 (build 57)
- FTDv - 6.5.0 (build 115)

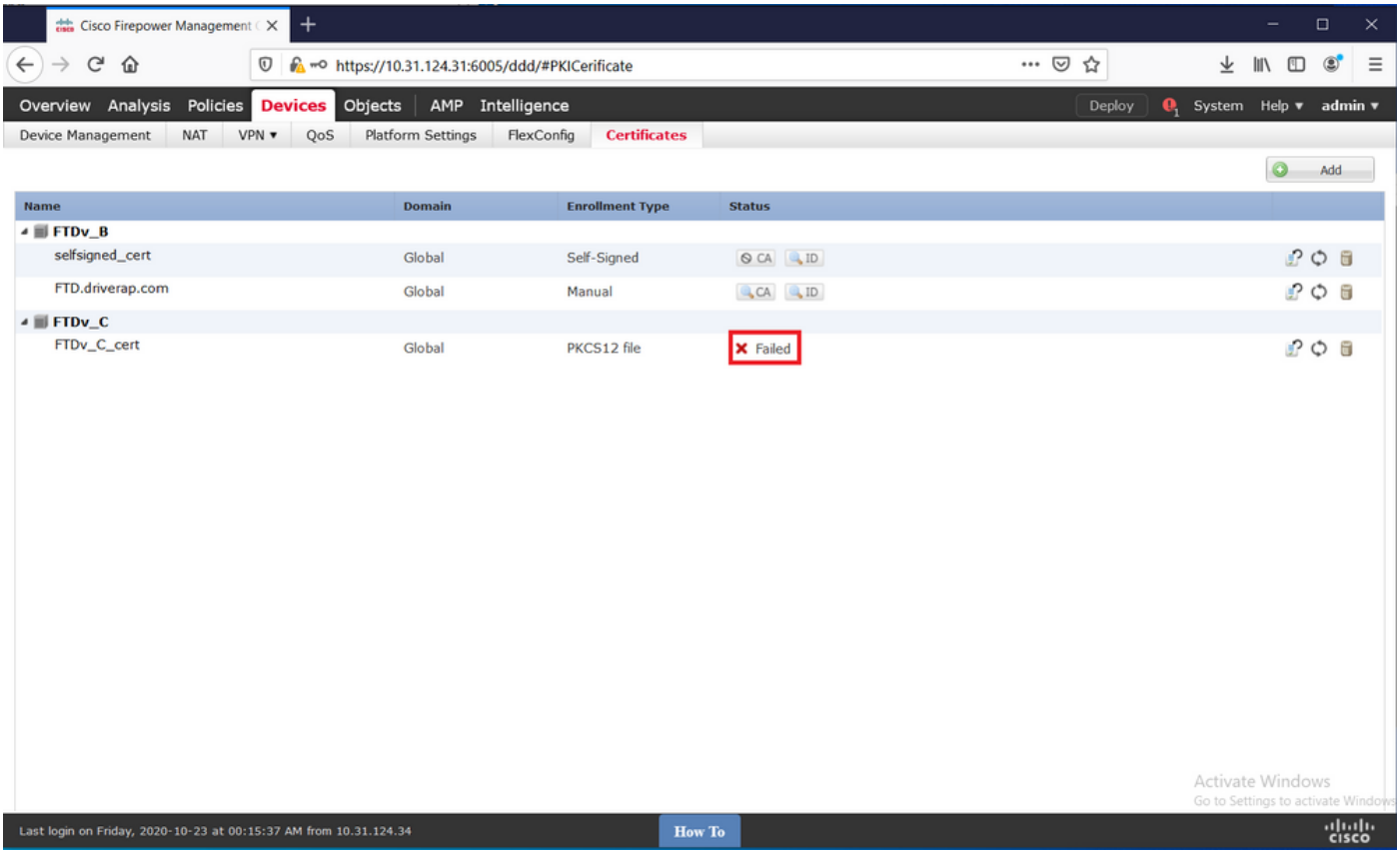
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Note**: A abordagem descrita neste documento pode ser implementada em qualquer outra plataforma com um problema semelhante, por exemplo, um Cisco Adaptive Security Appliance (ASA), já que o problema está no certificado não compatível com FIPS.

> **Note**: Este documento não aborda a condição em que os próprios componentes PKCS#12 não são compatíveis por qualquer outra razão, como o comprimento da chave Rivest, Shamir, Adleman (RSA) ou o algoritmo de assinatura usado para assinar o certificado de identidade. Nesses casos, os certificados devem ser reemitidos para serem conformes com o FIPS.

Problema

Quando o modo FIPS está habilitado no FTD, a instalação do certificado pode falhar se os algoritmos PBE usados para proteger o arquivo PKCS#12 não forem compatíveis com FIPS.



Note: Localize um procedimento passo a passo sobre como instalar um arquivo PKCS#12 usando o FMC na seção **Registro PKCS12** de Instalação e renovação de certificado no FTD gerenciado pelo FMC.

Se a instalação do certificado falhar por esse motivo, as depurações de PKI imprimirão um erro abaixo:

```
firepower# debug crypto ca 14
firepower# show debug
debug crypto ca enabled at level 14
Conditional debug filters:
Conditional debug features:

firepower# PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[4]: Error unpacking pkcs7 encrypted data
PKI[1]: error:060A60A3:digital envelope routines:FIPS_CIPHERINIT:disabled for fips in fips_enc.c
line 143.
PKI[1]: error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure in evp_pbe.c
line 203.
PKI[1]: error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error in
p12_decr.c line 93.
PKI[1]: error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:pkcs12 pbe crypt error in
p12_decr.c line 145.
PKI[4]: pkcs7 encryption algorithm may not be fips compliant
PKI[4]: Error unpacking pkcs12 struct to extract keys and certs
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list is NULL
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
```

```
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
```

Você também pode confirmar com o OpenSSL que o PKCS#12 em mãos inclui algoritmos FIPS PBE não compatíveis.

```
OpenSSL> pkcs12 -info -in ftdv_C_.p12 -noout
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

Na saída anterior há dois algoritmos PBE, pbeWithSHA1And40BitRC2-CBC e pbeWithSHA1And3-KeyTripleDES-CBC, que protegem os certificados e a chave privada respectivamente. O primeiro não é compatível com FIPS.

Solução

A solução é configurar o algoritmo PBE-SHA1-3DES para proteção de certificado e chave privada. No exemplo acima, apenas o algoritmo de certificado precisa ser alterado. Primeiro, você precisa obter a versão do Privacy-Enhanced Mail (PEM) do arquivo PKCS#12 original utilizando o OpenSSL.

```
OpenSSL> pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Por último, você precisa usar o comando abaixo com o algoritmo PBE compatível com FIPS usando o arquivo PEM obtido na etapa anterior para gerar um novo arquivo PKCS#12:

```
OpenSSL> pkcs12 -certpbe PBE-SHA1-3DES -export -in ftdv_C_.pem -out ftdv_C_FIPS_compliant.p12
Enter pass phrase for ftdv_C_.pem:
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'
```

> **Note**: Se o algoritmo para proteger a chave privada também precisar ser alterado, você pode adicionar a palavra-chave **-keypbe** seguida de **PBE-SHA1-3DES** ao mesmo comando: **pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out *<arquivo de certificado PKCS12>***.

Verificação

Use o mesmo comando OpenSSL para obter informações sobre a estrutura de arquivos PKCS#12 para confirmar se os algoritmos FIPS estão em uso:

```
OpenSSL> pkcs12 -info -in ftdv_C_FIPS_compliant.p12 -noout
```

```
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

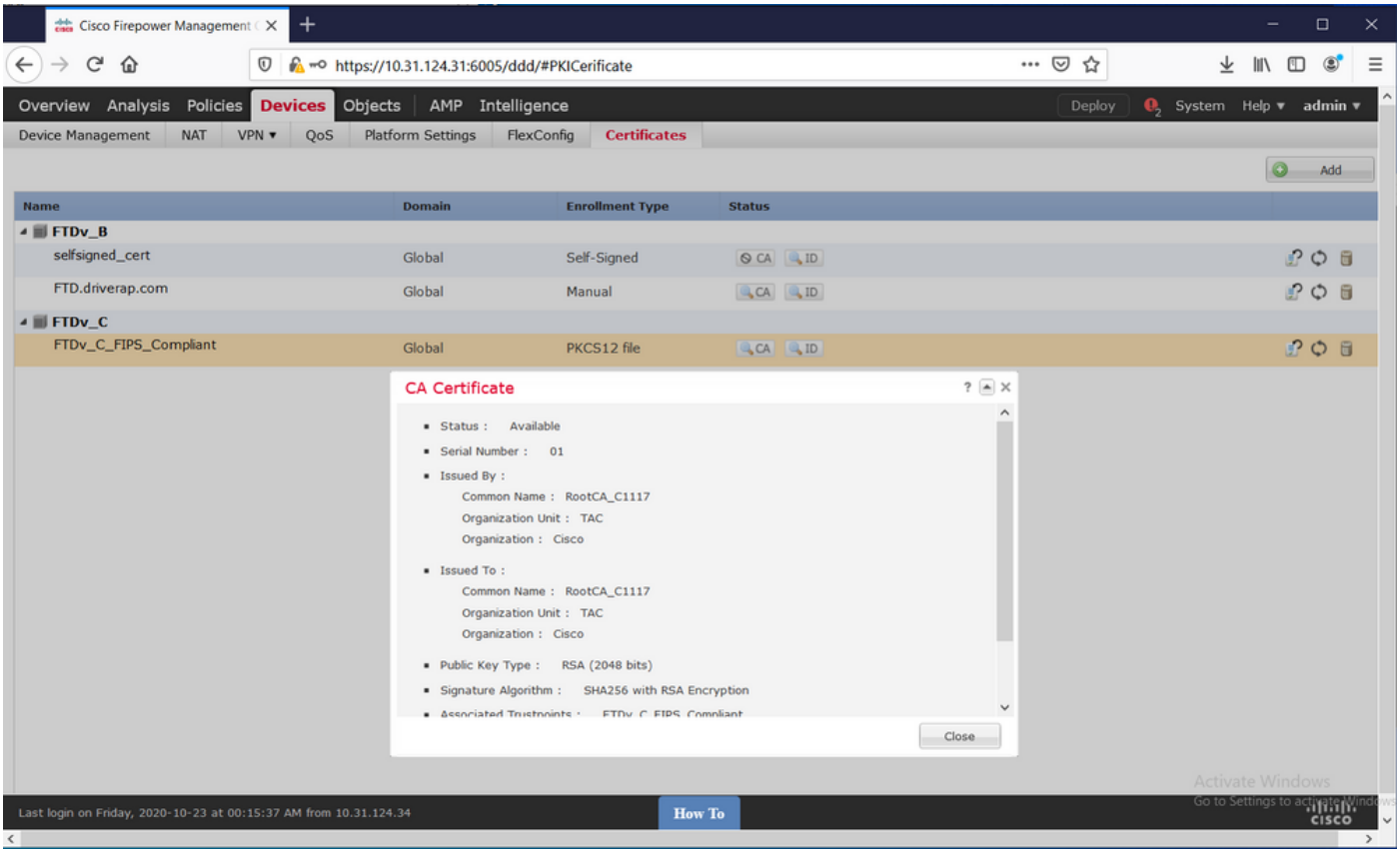
Agora, as depurações PKI mostram a saída abaixo quando a instalação do certificado for bem-sucedida.

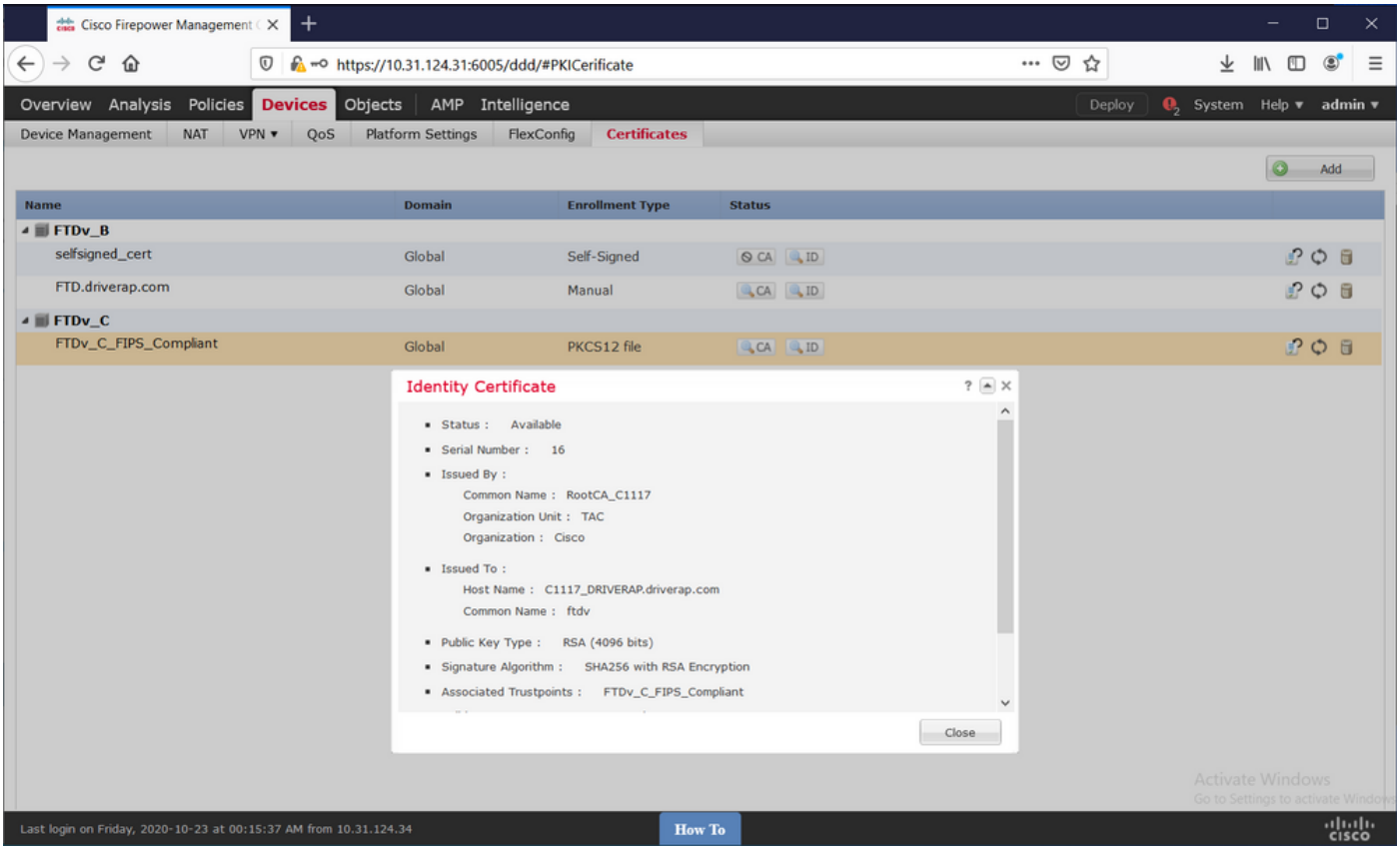
```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_key, pki_ossl_pkcs12.c:1252
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[14]: compare_key_ids, pki_ossl_pkcs12.c:1150
PKI[12]: transfer_p12_contents_to_asa, pki_ossl_pkcs12.c:375
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list is NULL

CRYPTO_PKI: examining router cert:
CRYPTO_PKI: issuerName=/O=Cisco/OU=TAC/CN=RootCA_C1117
CRYPTO_PKI: subjectname=/CN=ftdv/unstructuredName=C1117_DRIVERAP.driverap.com
CRYPTO_PKI: key type is RSAPKI[13]: GetKeyUsage, pki_ossl_pkcs12.c:278

CRYPTO_PKI: bitValue of ET_KEY_USAGE = a0
CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
CRYPTO_PKI: adding RSA Keypair
CRYPTO_PKI: adding as a router certificate.
CRYPTO_PKI: InsertCertData: subject name =

30 3b 31 0d 30 0b 06 03 55 04 03 13 04 66 74 64 76 31 2a 30
28 06 09 2a 86 48 86 f7 0d 01 09 02 16 1b 43 31 31 31 37 5f
44 52 49 56 45 52 41 50 2e 64 72 69 76 65 72 61 70 2e 63 6f
6d
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
```

```
PKI[9]: Starting to build the PKI cache
PKI[4]: No identity cert found for TP: FTDv_C_FIPS_Compliant
PKI[4]: Failed to cache certificate chain for the trustpoint FTDv_C_FIPS_Compliant or none
available
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[4]: Failed to retrieve trusted issuers list or no trustpoint configured
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_add_sync_record, pki_ossl_pkcs12.c:144
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: ID cert in trustpoint FTDv_C_FIPS_Compliant successfully validated with CA cert.

CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

CRYPTO_PKI: trustpoint FTDv_C_FIPS_Compliant authentication status = 0

CRYPTO_PKI: InsertCertData: subject name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 01 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
17 9d 0e b0 15 9d cd a2 5a 01 95 bf c6 8c 4f 2e | ........Z.....O.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.
PKI[7]: Get Certificate Chain: number of certs returned=2
PKI[13]: CERT_GetDNbyBuffer, vpn3k_cert_api.c:993
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[7]: Built trustpoint cache for FTDv_C_FIPS_Compliant
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[9]: Added 1 issuer hashes to cache.
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_free_sync_record, pki_ossl_pkcs12.c:113
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
```

```
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI: certificate data
<omitted output>
CRYPTO_PKI: status = 0: failed to get extension from cert

CRYPTO_PKI: certificate data
<omitted output>
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
```

Por último, o CVP mostra certificados de CA e de identidade disponíveis:




Cisco Firepower Management
https://10.31.124.31:6005/ddd/#PKICerificate
Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates
Add
Name Domain Enrollment Type Status
FTDv_B
selfsigned_cert Global Self-Signed CA ID
FTD.driverap.com Global Manual CA ID
FTDv_C
FTDv_C_FIPS_Compliant Global PKCS12 file CA ID
Identity Certificate
Status : Available
Serial Number : 16
Issued By :
Common Name : RootCA_C1117
Organization Unit : TAC
Organization : Cisco
Issued To :
Host Name : C1117_DRIVERAP.driverap.com
Common Name : ftdv
Public Key Type : RSA (4096 bits)
Signature Algorithm : SHA256 with RSA Encryption
Associated Trustpoints : FTDv_C_FIPS_Compliant
Close
Activate Windows
Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34
How To