FIPS非準拠のPBEアルゴリズムによるPKCS#12ファイルのインストール障害のトラブルシューティング

内容

概要

このドキュメントでは、Cisco Firepower Management Center(FMC)を介してPublic Key Cryptography Standards(PKCS)#12ファイルとNon-Federal Information Processing Standard(FIPS)準拠のパスワードベース暗号化(PBE)のインストール障害をトラブルシューティングする方法について方法を説明します。 これを識別し、OpenSSLで新しい準拠バンドルを作成する手順について説明します。

背景説明

Cisco Firepower Threat Defense(FTD)は、管理対象デバイスでCommon Criteria(CC)またはUnified Capabilities Approved Products List(UAP)モードを有効にすると、FIPS 140への準拠をサポートします。この設定は、FMCプラットフォーム設定ポリシーの一部です。適用後、FTDの**show running-config**出力にfips enableコマンドが表示されます。

PKCS#12は、秘密キーとそれぞれのID証明書をバンドルするために使用されるファイル形式を定義します。検証チェーンに属するルート証明書または中間証明書を含めることもできます。PBEアルゴリズムは、PKCS#12ファイルの証明書と秘密キー部分を保護します。メッセージ認証方式(MD2/MD5/SHA1)と暗号化方式(RC2/RC4/DES)の組み合わせにより、複数のPBEアルゴリズムが存在しますが、FIPSに準拠しているのはPBE-SHA1-3DESだけです。

> **注**：シスコ製品のFIPSの詳細については、FIPS 140を参照してください。

> **注**：FTDおよびFMCで利用可能なセキュリティ認定基準の詳細については、『FMC Configuration Guide』の「**Security Certifications Compliance**」の章を参照してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 公開キー インフラストラクチャ（PKI）
- OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCv - 6.5.0.4（ビルド57）
- FTDv - 6.5.0（ビルド115）

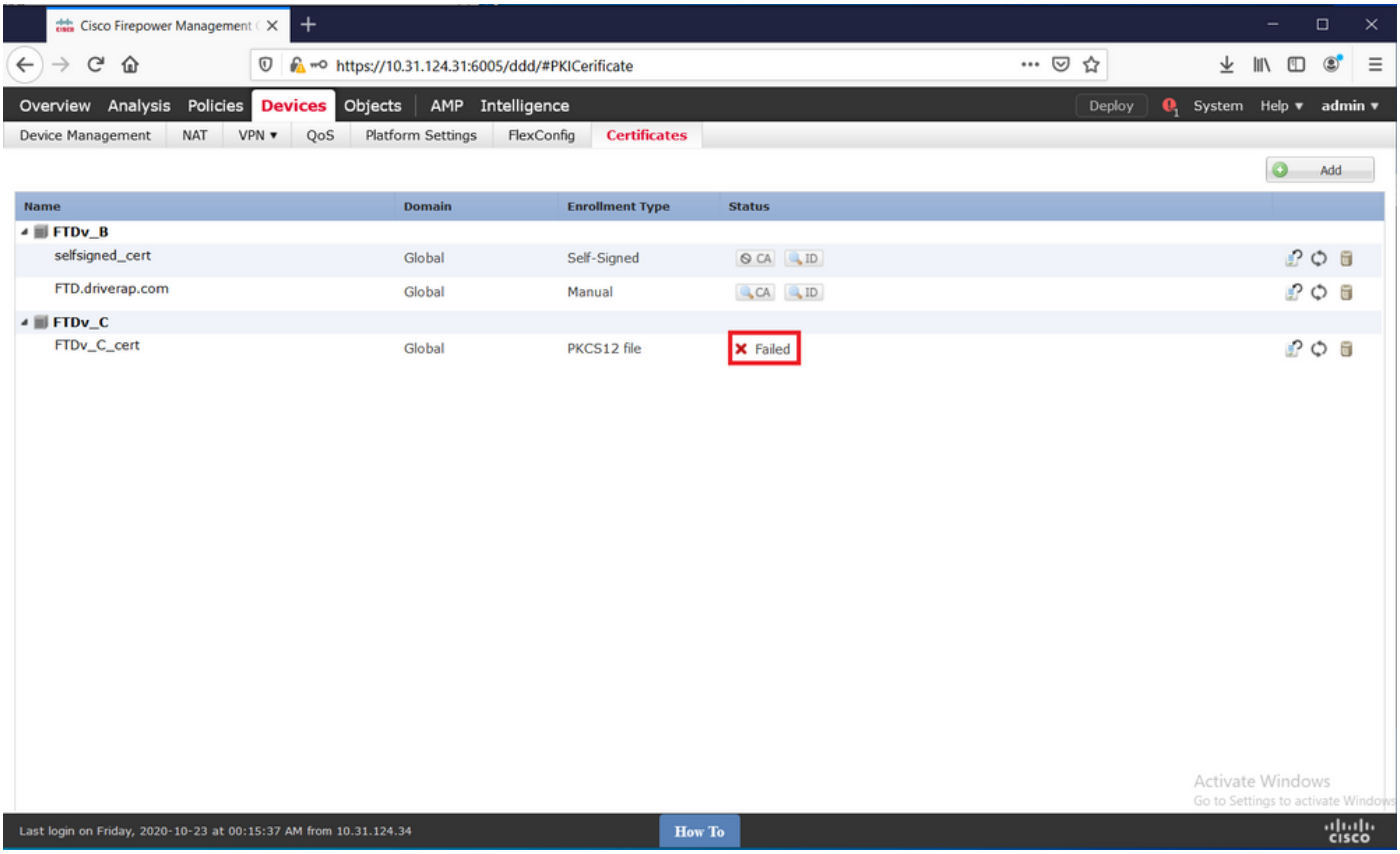
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

> **注：**このドキュメントで説明するアプローチは、Cisco適応型セキュリティアプライアンス(ASA)などの同様の問題を持つ他のプラットフォームに実装できます。これは、証明書がFIPS非準拠であるためです。

> **注：**このドキュメントでは、PKCS#12コンポーネント自体がRivest、Shamir、Adleman(RSA)キー長や、ID証明書の署名に使用される署名アルゴリズムなどの他の理由によって準拠していない状況については説明しません。このような場合、FIPSに準拠するために証明書を再発行する必要があります。

問題

FTDでFIPSモードが有効になっている場合、PKCS#12ファイルの保護に使用されるPBEアルゴリズムがFIPSに準拠していないと、証明書のインストールが失敗する可能性があります。



注：FMCが管理するFTDでの証明書のインストールと更新のPKCS12登録セクションのFMCを使用してPKCS#12ファイルをインストールする方法について手順を追って説明します。

この理由で証明書のインストールが失敗すると、PKIデバッグでは次のエラーが出力されます。

```
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
```

また、OpenSSLで、手元のPKCS#12に準拠していないFIPS PBEアルゴリズムが含まれていることを確認できます。

```
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
```

前の出力では、pbeWithSHA1And40BitRC2-CBCとpbeWithSHA1And3-KeyTripleDES-CBCの2つのPBEアルゴリズムがあり、それぞれ証明書と秘密キーを保護します。1つ目はFIPSに準拠していません。

解決方法

解決策は、PBE-SHA1-3DESアルゴリズムを証明書と秘密鍵の両方の保護に設定することです。上記の例では、証明書アルゴリズムだけを変更する必要があります。まず、OpenSSLを利用して元のPKCS#12ファイルのPrivacy-Enhanced Mail(PEM)バージョンを入手する必要があります。

```
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:
```

最後に、次のコマンドを前の手順で取得したPEMファイルを使用してFIPS準拠のPBEアルゴリズムで使用し、新しいPKCS#12ファイルを生成する必要があります。

```
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'
```

> **注：秘密キーを保護するアルゴリズムも変更する必要がある場合は、PBE-SHA1-3DESの後に続く – keybeキーワードを同じコマンドに追加できます。pkcs12 -certpbe PBE-SHA1-3DES -keybe PBE-SHA1-3DES -export -in -out *<PKCS12 cert file>*。**

確認

同じOpenSSLコマンドを使用して、PKCS#12ファイル構造に関する情報を取得し、FIPSアルゴリズムが使用されていることを確認します。

```
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
```

証明書のインストールが成功すると、PKIデバッグの出力が次のように表示されます。

```
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
```

最後に、FMCは使用可能なCA証明書とID証明書の両方を表示します。