Cisco ESA/GUI への新しい PKCS#12 証明書の追加/インポート

目次

概要

このドキュメントでは、新しい公開キー暗号化標準規格（PKCS）#12 の証明書を Cisco E メール セキュリティ アプライアンス（ESA）の GUI で追加またはインポートする方法を説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco ESA
- AsyncOS 7.1 以降

問題

AsyncOS 7.1.0 以降では、E メール アプライアンスの GUI で証明書の管理と追加ができます。しかし、この新しい証明書は PKCS#12 形式である必要があります。それで、認証局（CA）の証明書を受け取った後、いくらかの追加手順が必要です。

また、PKCS#12 証明書の生成には秘密キー証明書が必要です。 Cisco ESA CLI コマンド **certconfig** で証明書署名要求（CSR）を実行する場合、秘密キー証明書を受け取りません。 GUI メニュー [Mail Policies] > [Signing Keys] から秘密キー証明書を生成できますが、それを CA 証明書とともに PKCS#12 証明書の生成に使用しても無効です。

回避策

1. ワークステーションに OpenSSL アプリケーションをまだインストールしていなければ、インストールします。 Windows バージョンはここからダウンロードできます。OpenSSL Win32 のインストールの前に Visual C++ 2008 再頒布可能パッケージがインストールされていることを確認します。
2. ここにあるテンプレートを使用して、CSR と秘密キーを生成するスクリプトを作成します。次のようなスクリプトになります。**openssl req -new -newkey rsa:2048 -nodes -out test_example.csr -keyout test_example.key -subj "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test.example.com"**
3. スクリプトを OpenSSL のウィンドウに貼り付け、Enter を押します。

   C:\OpenSSL-Win32\bin>openssl req -new -newkey rsa:2048 -nodes -out test_example.csr -keyout
   test_example.key -subj "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test.example.com"

   出力：
   ```
   test_example.csr and test_example.key in the C:\OpenSSL-Win32\bin or in the
   'bin' folder where OpenSSL is installed
   test_example.csr = Certificate Signing Request
   example.key = private key
   ```
4. CA 証明書を要求するために .CSR ファイルを使用します。

5. CA 証明書を受け取ったら、それを **cacert.pem ファイル**として保存します。 秘密キーファイル test_example.key を **test_example.pem** という名前に変更します。 ここで OpenSSL を使用して PKCS#12 証明書を生成できます。

   コマンド：

   openssl pkcs12 -export -out cacert.p12 -in cacert.pem -inkey test_example.pem

   使用する CA 証明書と秘密キーが正しければ、OpenSSL は **Export Password** を入力するようにプロンプトを表示し、さらに再入力してパスワードを確認するように求めます。 もし正しくなければ、証明書とキーが一致せずプロセスを続行できないことが表示されます。

   Input :

   ```
   cacert.pem = CA certificate
   test_example.pem = private key
   Export password: ironport
   ```

   出力：

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. IronPort GUI メニューの [Network] > [Certificate] に移動します。

[Add Certificate] を選択します。
[Add Certificate] の [Import Certificate] オプションを選択します。
[Choose] を選択し、ステップ 5 で生成された PKCS#12 証明書の場所を参照してファイルを選択してください。
OpenSSL の PKCS#12 証明書を生成したときに使用したパスワードを入力します。（この例ではパスワードは **ironport** です）。

[Next] をクリックします。次の画面には、証明書に使用されている属性の詳細が表示されます。
Submit を選択します。
[Commit Changes] を選択します。

これらの手順を完了すると、新しい証明書が証明書一覧に追加されて使用可能になります。