Hinzufügen/Importieren eines neuen PKCS#12-Zertifikats in der GUI der Cisco ESA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie neue PKCS (Public Key Cryptography Standards) #12-Zertifikate in der Benutzeroberfläche der Cisco E-Mail Security Appliance (ESA) hinzugefügt bzw. importiert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS 7.1 und höher

Problem

Seit AsyncOS 7.1.0. und später ist es möglich, Zertifikate in der GUI der E-Mail-Appliances zu verwalten/hinzuzufügen. Dafür muss das neue Zertifikat jedoch im PKCS#12-Format vorliegen, sodass nach Erhalt des Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) einige zusätzliche Schritte hinzugefügt werden.

Zum Generieren eines PKCS#12-Zertifikats ist auch das Private Key-Zertifikat erforderlich. Wenn Sie die CSR-Anfrage (Certificate Signing Request) mit dem Befehl **certconfig** der Cisco ESA CLI ausführen, erhalten Sie das Private Key-Zertifikat nicht. Das im GUI-Menü erstellte Private Key-Zertifikat (**Mail-Policys > Signaturschlüssel**) ist ungültig, wenn Sie es zum Generieren eines PKCS#12-Zertifikats zusammen mit dem CA-Zertifikat verwenden.

Problemumgehung

1. Installieren Sie die OpenSSL-Anwendung, wenn diese auf Ihrer Workstation nicht vorhanden ist. Die Windows-Version kann hier heruntergeladen werden.Stellen Sie sicher, dass Visual C++ 2008 Redistributables vor OpenSSL Win32 installiert ist.
2. Erstellen Sie hier mit einer Vorlage ein Skript zum Generieren von CSR und Privaten Schlüssel.Das Skript sieht wie folgt aus:**openssl req -new -newkey rsa:2048 -knoten -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. Kopieren Sie das Skript, fügen Sie es in das OpenSSL-Fenster ein, und drücken Sie die **Eingabetaste**.

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

   Ausgabe:
   ```
   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. Verwenden Sie die CSR-Datei, um das Zertifizierungsstellenzertifikat anzufordern.

5. Wenn Sie das Zertifikat der Zertifizierungsstelle erhalten haben, speichern Sie es als **cacert.pem-**Datei. Umbenennen der privaten Schlüsseldatei **test_example.key** in **test_example.pem**. Jetzt können Sie ein PKCS#12-Zertifikat mit OpenSSL generieren.

   Befehl:

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

   Wenn das CA-Zertifikat und der verwendete private Schlüssel korrekt sind, werden Sie von OpenSSL aufgefordert, das **Exportkennwort** einzugeben und das Kennwort erneut zu bestätigen. Andernfalls werden Sie darauf hingewiesen, dass das verwendete Zertifikat und der verwendete Schlüssel nicht mit dem Prozess übereinstimmen und nicht fortfahren können.

   Eingabe:

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

   Ausgabe:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Gehen Sie zum IronPort GUI-Menü **Network > Certificate**.

Wählen Sie **Zertifikat hinzufügen aus**.

Wählen Sie **Zertifikat importieren** in der Option **Zertifikat hinzufügen aus**.
Wählen Sie **Choose (Auswählen)**, und navigieren Sie zum Speicherort des in Schritt 5 generierten PKCS#12-Zertifikats.
Geben Sie das gleiche Kennwort ein, das Sie verwendet haben, als Sie das PKCS#12-Zertifikat in OpenSSL generiert haben (in diesem Fall ist das Kennwort **ironport**).
Wählen Sie **Weiter**, und im nächsten Bildschirm werden die für das Zertifikat verwendeten Attributdetails angezeigt.
Wählen Sie **Senden aus**.
Wählen Sie **Änderungen bestätigen aus**.

Nach diesen Schritten wird das neue Zertifikat der Zertifikatsliste hinzugefügt und kann zur Verwendung zugewiesen werden.