在思科ESA GUI上添加/导入新PKCS#12证书

目录

简介

本文档介绍如何在思科邮件安全设备(ESA)GUI上添加/导入新的公钥加密标准(PKCS)#12证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ESA
- AsyncOS 7.1及更高版本

问题

自AsyncOS 7.1.0.及更高版本以来，可以在电子邮件设备的GUI中管理/添加证书。但是，对于此新证书，它必须采用PKCS#12格式，因此此要求在收到证书颁发机构(CA)证书后添加一些额外步骤。

生成PKCS#12证书也需要私钥证书。如果从Cisco ESA CLI命令**certconfig**运行证书签名请求(CSR)，您将不会收到私钥证书。在GUI菜单(**Mail Policies > Signing Keys**)中创建的私钥证书在与PKCS#12证书一起生成时将无效CA证书。

解决方法

1. 如果工作站没有OpenSSL应用，请安装它。可以从此处下载Windows[版本](#)。确保在OpenSSL Win32之前安装了Visual C++ 2008可重分发文件。
2. 使用模板创建脚本，在此处生成CSR和私[钥](#)。脚本如下所示：**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. 将脚本复制并粘贴到OpenSSL窗口，然后按**Enter**。

   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"

   输出：

   ```
   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. 使用.CSR文件请求CA证书。

5. 收到CA证书后，将其另存为**cacert.pem文**件。将私钥文**件test_example.key重**命名为**test_example.pem**。现在，您可以使用OpenSSL生成PKCS#12证书。

   命令:

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

   如果使用的CA证书和私钥正确，OpenSSL会提示您输入**导出密**码并再次确认密码。否则，它建议您使用的证书和密钥不匹配，无法继续该过程。

   输入:

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

   输出：

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```

6. 转到IronPort GUI菜单，网络**>证书**。

选择“**添加证书**”。
在“添**加证书”**选项中**选择导入**证书。
选择**Choose**并浏览到第5步中生成的PKCS#12证书的位置。
输入在OpenSSL中生成PKCS#12证书时使用的密码(在本例中，密码为**ironport**)。
选择**Next**，下一个屏幕将显示用于证书的属性详细信息。
选择 **Submit**。
选择“**提交更改**”。

执行这些步骤后，新证书将添加到证书列表中，并可以分配给使用。