Ajouter/importer un nouveau certificat PKCS#12 sur l'interface utilisateur graphique Cisco ESA

Contenu

Introduction

Ce document décrit comment ajouter/importer de nouveaux certificats PKCS (Public Key Cryptography Standards) #12 sur l'interface utilisateur graphique de l'appliance de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- AsyncOS 7.1 et versions ultérieures

Problème

Depuis AsyncOS 7.1.0. et plus tard, il est possible de gérer/ajouter des certificats dans l'interface utilisateur graphique des appliances de messagerie. Cependant, pour cela, le nouveau certificat doit être au format PKCS#12, de sorte que cette exigence ajoute quelques étapes supplémentaires après avoir reçu le certificat de l'autorité de certification (AC).

La génération d'un certificat PKCS#12 nécessite également le certificat de clé privée. Si vous exécutez la demande de signature de certificat (CSR) à partir de la commande CLI de Cisco ESA **certconfig**, vous ne recevrez pas le certificat de clé privée. Le certificat de clé privée créé dans le menu GUI (**Politiques de messagerie > Clés de signature**) ne sera pas valide lorsque vous l'utilisez pour générer un certificat PKCS#12 avec un certificat CA.

Solution de contournement

1. Installez l'application OpenSSL si votre station de travail ne l'a pas. La version de Windows peut être téléchargée ici.Assurez-vous que Redistributables Visual C++ 2008 est installé avant l'OpenSSL Win32.
2. Utilisez un modèle pour créer un script afin de générer CSR et Private Key dans cette section.Le script ressemblera à ceci :**openssl req -new -newkey rsa:2048 -noeuds -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. Copiez et collez le script dans la fenêtre OpenSSL et appuyez sur **Entrée**.

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

   Sortie :
   ```
   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. Utilisez le fichier .CSR pour demander le certificat CA.

5. Une fois que vous avez reçu le certificat de l'autorité de certification, enregistrez-le en tant que fichier **cacert.pem**. Renommez le fichier de clé privée **test_example.key** en **test_example.pem**. Vous pouvez désormais générer un certificat PKCS#12 à l'aide d'OpenSSL.

   commande :

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

   Si le certificat de l'autorité de certification et la clé privée utilisés sont corrects, OpenSSL vous invite à saisir **Exporter le mot de passe** et à confirmer à nouveau le mot de passe. Sinon, il vous indique que le certificat et la clé utilisés ne correspondent pas et ne peuvent pas poursuivre le processus.

   Entrée:

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

   Sortie :

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Accédez au menu GUI d'IronPort, **Réseau > Certificat**.

Sélectionnez **Ajouter un certificat**.
Sélectionnez **Importer un certificat** dans l'option **Ajouter un certificat**.

Sélectionnez **Choisir** et accédez à l'emplacement du certificat PKCS#12 généré à l'étape 5.
Entrez le même mot de passe que celui utilisé lors de la génération du certificat PKCS#12 dans OpenSSL (dans ce cas, le mot de passe est **ironport**).
Sélectionnez **Suivant** et l'écran suivant affiche les détails des attributs utilisés pour le certificat.
Sélectionnez **Submit**.
Sélectionnez **Valider les modifications**.

Après ces étapes, le nouveau certificat est ajouté à la liste des certificats et peut être affecté à l'utilisation.