Contenu

Introduction

Ce document décrit comment ajouter/les nouveaux Certificats #12 des normes cryptographie à clé publique d'importation (PKCS) sur le GUI des appareils de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- AsyncOS 7.1 et plus tard

Problème

Depuis AsyncOS 7.1.0 et plus tard, il est possible de gérer/ajoute des Certificats dans le GUI des appliances d'email. Cependant, pour ceci le nouveau certificat, il doit être dans le format PKCS#12, ainsi cette condition requise ajoute quelques étapes supplémentaires après réception du certificat d'Autorité de certification (CA).

Générer un certificat PKCS#12 exige également le certificat de clé privée. Si vous exécutez la demande de signature de certificat (CSR) du **certconfig de** commande de Cisco ESA CLI, vous ne recevrez pas le certificat de clé privée. Le certificat de clé privée créé dans le menu GUI (**stratégies de messagerie > des clés de signature**) ne sera pas valide quand vous l'employez pour générer un certificat PKCS#12 ainsi que le certificat de CA.

Contournement

1. Installez l'application d'OpenSSL si votre poste de travail ne l'a pas. La version de Windows peut être téléchargée d'ici.Assurez-vous que Visual C++ 2008 redistribuables est installé avant l'OpenSSL Win32.

2. Utilisez un modèle pour créer un script pour générer le CSR et la clé privée dedans ici.Le script ressemblera à ceci :**req d'openssl - nouveau - newkey rsa:2048 - Noeuds - 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 d'OpenSSL et l'appuyez sur **entrent**.

   Req C:\OpenSSL-Win32\bin>openssl - nouveau - newkey rsa:2048 - Noeuds - test_example.csr - keyout test_example.key - subj « /C=AU/ST=NSW/L=Sydney/O= Cisco Systems /OU=IronPort/CN=test.example.com »

   Sortie :
4. Utilisez le fichier .CSR pour demander pour le certificat de CA.

5. Une fois que vous recevez le certificat de CA, sauvegardez-le pendant que **fichier cacert.pem**. Renommez le fichier principal privé t est_example.key à **test_example.pem. Maintenant vous** pouvez générer un certificat PKCS#12 utilisant OpenSSL.

   Commande :

   openssl pkcs12 - exportation - cacert.p12 - dans cacert.pem - inkey test_example.pem

   Si le certificat de CA et la clé privée utilisés sont corrects, OpenSSL vous incite à entrer le **mot de passe d'exportation** et à confirmer le mot de passe de nouveau. Autrement, il vous informe que le certificat et la clé qui sont utilisés ne s'assortissent pas et ne peuvent pas procéder au processus.

   Entrée :

   Sortie :
6. Allez au menu GUI d'IronPort, **réseau > certificat**.

Choisi **ajoutez le certificat**.
Certificat d'importation choisi dans l'option de **certificat d'ajouter**.
Choisi **choisissez** et parcourez à l'emplacement du certificat PKCS#12 généré dans l'étape 5.
Entrez le même mot de passe que vous avez utilisé utilisé quand vous avez généré le certificat PKCS#12 dans l'OpenSSL (dans ce cas le mot de passe est **ironport**).
Prochain choisi et l'écran suivant afficheront les détails d'attributs utilisés pour le certificat.
Sélectionnez **Submit**.
Modifications choisies de **validation**.

Après ces étapes, le nouveau certificat est ajouté aux Certificats les répertorient et peuvent être assignés pour l'usage.