Toevoegen/importeren van nieuw PKCS#12-certificaat op de Cisco ESA GUI

Inhoud

Inleiding

Dit document beschrijft hoe u nieuwe PKCS (Public Key Cryptography Standards) #12 kunt toevoegen/importeren op de Cisco e-mail security applicatie (ESA) GUI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- AsyncOS 7.1 en hoger

Probleem

Sinds AsyncOS 7.1.0. en later, is het mogelijk om certificaten in de GUI van de e-mailapparaten te beheren/toe te voegen. Voor dit nieuwe certificaat moet het echter in het PKCS#12-formaat zijn, zodat aan deze eis na ontvangst van het certificaat van de certificaatinstantie (CA) enkele extra stappen worden toegevoegd.

Voor het genereren van een PKCS#12-certificaat is ook het Private Key Certificate vereist. Als u het certificaatsignaalverzoek (CSR) uitvoert vanuit Cisco ESA CLI commando **cert**, ontvangt u niet het Private Key certificaatcertificaat. Het Private Key Certificate dat is gemaakt in het GUI-menu (**Mail Policies > Signing Keys**) is niet geldig wanneer u het gebruikt om een PKCS#12-certificaat met CA-certificaat te genereren.

Werken

1. Installeer de OpenSSL-toepassing als uw werkstation deze niet heeft. U kunt de Windows-versie hier downloaden.Zorg ervoor dat visuele C++ 2008 herverdelingstabellen geïnstalleerd zijn voordat OpenSSL Win32.
2. Gebruik een sjabloon om hier een script te maken om CSR en Private Key te genereren.Het script ziet er zo uit:**openssl req -new-new-key rsa:2048 -knooppunten -out test_voorbeeldv.csr -keyout test_voorbeeldv.key -subj "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test.voorbeeld.com"**
3. Kopieer en plak het script naar OpenSSL-venster en druk op **ENTER**.

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

   Uitvoer:

   ```
   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. Gebruik het .CSR-bestand om het CA-certificaat aan te vragen.

5. Nadat u het CA-certificaat hebt ontvangen, slaat u dit op als **cacert.pem**-bestand. Hernoemen private key file **test_voorbeeld.key** voor **test_voorbeeld.pem**. U kunt nu een PKCS#12-certificaat genereren met behulp van OpenSSL.

   Opdracht:

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

   Als het CA-certificaat en de particuliere sleutel correct zijn, wordt u door OpenSSL gevraagd het **wachtwoord voor de export** in te voeren en het wachtwoord opnieuw te bevestigen. Anders adviseert het u dat het certificaat en de toets die worden gebruikt niet overeenkomen en niet met het proces kunnen doorgaan.

   Invoer:

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

   Uitvoer:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Ga naar het menu IronPort GUI, **Netwerk > certificaatnummer**.

Selecteer **Certificaat toevoegen**.
Selecteer **Invoercertificaat** in de optie **Certificaat toevoegen**.
Selecteer **Kies** en blader naar de locatie van het PKCS#12-certificaat dat in Stap 5 gegenereerd

is.
Voer het wachtwoord in dat u hebt gebruikt toen u het PKCS#12-certificaat in het OpenSSL gegenereerd hebt (in dit geval is het wachtwoord **juist**).
Selecteer **Volgende** en het volgende scherm toont de eigenschappen die voor het certificaat worden gebruikt.
Selecteer **Indienen**.
Selecteer **Commit change**.

Na deze stappen wordt het nieuwe certificaat toegevoegd aan de lijst van certificaten en kan het voor gebruik worden toegewezen.