Agregar/importar nuevo certificado PKCS#12 en la GUI de Cisco ESA

Contenido

Introducción

Este documento describe cómo agregar/importar nuevos certificados de estándares criptográficos de clave pública (PKCS) nº 12 en la GUI de Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA de Cisco
- AsyncOS 7.1 y posterior

Problema

Desde AsyncOS 7.1.0. y posteriormente, es posible administrar/agregar certificados en la GUI de los dispositivos de correo electrónico. Sin embargo, para esto el nuevo certificado tiene que estar en formato PKCS#12, por lo que este requisito agrega algunos pasos adicionales después de recibir el certificado de la autoridad certificadora (CA).

La generación de un certificado PKCS#12 también requiere el certificado de clave privada. Si ejecuta la solicitud de firma de certificados (CSR) desde el comando CLI de Cisco ESA **certconfig**, no recibirá el certificado de clave privada. El certificado de clave privada creado en el menú GUI (**Políticas de correo > Claves de firma**) no será válido cuando lo utilice para generar un certificado PKCS#12 junto con el certificado de CA.

Solución Aternativa

1. Instale la aplicación OpenSSL si la estación de trabajo no la tiene. La versión de Windows se puede descargar desde aquí.Asegúrese de que Visual C++ 2008 Redistributables esté instalado antes de OpenSSL Win32.
2. Utilice una plantilla para crear una secuencia de comandos para generar CSR y clave privada aquí.El guión tendrá el siguiente aspecto:**openssl req -new -newkey rsa:2048 -node -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. Copie y pegue el script en la ventana OpenSSL y presione **Enter**.

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

   Salida:

   ```
   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. Utilice el archivo .CSR para solicitar el certificado de CA.

5. Una vez que reciba el certificado de CA, guárdelo como el archivo **cacert.pem**. Cambie el nombre del archivo de clave privada **test_example.key** a **test_example.pem**. Ahora puede generar un certificado PKCS#12 mediante OpenSSL.

   Comando:

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

   Si el certificado de CA y la clave privada utilizados son correctos, OpenSSL le solicita que introduzca **Export Password** y confirme la contraseña de nuevo. De lo contrario, le informa de que el certificado y la clave que se utilizan no coinciden y no pueden continuar con el proceso.

   Entrada:

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

   Salida:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Vaya al menú de la GUI de IronPort, **Network > Certificate**.

Seleccione **Agregar certificado**.
Seleccione **Importar certificado** en la opción **Agregar certificado**.
Seleccione **Choose** y busque la ubicación del certificado PKCS#12 generado en el Paso 5.

Ingrese la misma contraseña que utilizó cuando generó el certificado PKCS#12 en OpenSSL (en este caso, la contraseña es **ironport**).
Seleccione **Next** y la siguiente pantalla mostrará los detalles de atributos utilizados para el certificado.
Seleccione **Enviar**.
Seleccione **Registrar cambios**.

Después de estos pasos, el nuevo certificado se agrega a la lista de certificados y se puede asignar para su uso.