Contenido

Introducción

Este documento describe cómo agregar/los nuevos Certificados #12 de los estándares del Cifrado de clave pública de la importación (PKCS) en el dispositivo de seguridad del correo electrónico de Cisco (ESA) GUI.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ESA
- AsyncOS 7.1 y posterior

Problema

Desde AsyncOS 7.1.0 y posterior, es posible manejar/agrega los Certificados en el GUI de los dispositivos del correo electrónico. Sin embargo, para esto el nuevo certificado, tiene que estar en el formato del PKCS-12, así que este requisito agrega algunos pasos adicionales después de recibir el certificado del Certificate Authority (CA).

La generación de un certificado del PKCS-12 también requiere el certificado de la clave privada. Si usted ejecuta el pedido de firma de certificado (CSR) del **certconfig del** comando CLI de Cisco ESA, usted no recibirá el certificado de la clave privada. El certificado de la clave privada creado en el menú GUI (**directivas del correo > las claves de firma**) no será válido cuando usted lo utiliza para generar un certificado del PKCS-12 así como el certificado de CA.

Solución Aternativa

1. Instale la aplicación del OpenSSL si su puesto de trabajo no la tiene. La versión de Windows se puede descargar de aquí.Asegúrese de que Visual C++ 2008 Redistributables esté instalado antes del OpenSSL Win32.

2. Utilice una plantilla para crear un script para generar el CSR y la clave privada adentro aquí.El script parecerá esto:**req del openssl - nuevo - newkey rsa:2048 - Nodos - hacia fuera test_example.csr - keyout test_example.key - subj "/C=AU/ST=NSW/L=Sydney/O= Cisco Systems /OU=IronPort/CN=test.example.com"**
3. La copia y pega el script en la ventana y el Presione ENTER del OpenSSL.

   Req C:\OpenSSL-Win32\bin>openssl - nuevo - newkey rsa:2048 - Nodos - hacia fuera test_example.csr - keyout
   test_example.key - subj "/C=AU/ST=NSW/L=Sydney/O= Cisco Systems /OU=IronPort/CN=test.example.com"

   Salida:
4. Utilice el archivo .CSR para petición el certificado de CA.

5. Una vez que usted recibe el certificado de CA, sálvelo mientras que **archivo cacert.pem**. Retitule el archivo de clave privado t est_example.key a **test_example.pem. Ahora usted** puede generar un certificado del PKCS-12 usando el OpenSSL.

   Comando:

   pkcs12 del openssl - exportación - hacia fuera cacert.p12 - en cacert.pem - inkey test_example.pem

   Si el certificado de CA y la clave privada usados están correctos, el OpenSSL le indica a que ingrese la **contraseña de la exportación** y confirme la contraseña otra vez. Si no, le aconseja que el certificado y la clave se utilizan que no hagan juego y no puedan proceder con el proceso.

   Entrada:

   Salida:
6. Van al menú GUI de IronPort, la **red > el certificado**.

Selecto **agregue el certificado**.
Seleccione **Import Certificate (Importar certificado)** en la opción del **certificado del agregar**.
Selecto **elija** y hojee a la ubicación del certificado del PKCS-12 generado en el paso 5.
Ingrese la misma contraseña que usted utilizó utilizado cuando usted generó el certificado del PKCS-12 en el OpenSSL (en este caso la contraseña es **ironport**).
Seleccione **después** y la siguiente pantalla visualizará los detalles de los atributos usados para el certificado.
Seleccione **Enviar**.
Seleccione los **cambios del cometer**.

Después de estos pasos, el nuevo certificado se agrega a los Certificados enumera y se puede asignar para el uso.