Certificado novo do PKCS-12 adicionar/importação em Cisco ESA GUI

Índice

Introdução

Este documento descreve como adicionar/os Certificados #12 novos dos padrões criptografia de chave pública da importação (PKCS) na ferramenta de segurança do email de Cisco (ESA) GUI.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS 7.1 e mais atrasado

Problema

Desde AsyncOS 7.1.0 e mais atrasado, é possível controlar/adiciona Certificados no GUI dos dispositivos do email. Contudo, para este o certificado novo, tem que estar no formato do PKCS-12, assim que esta exigência adiciona algumas etapas extras após ter recebido o certificado do Certificate Authority (CA).

Gerar um certificado do PKCS-12 igualmente exige o certificado da chave privada. Se você executa a solicitação de assinatura de certificado (CSR) do **certconfig do** comando CLI de Cisco ESA, você não receberá o certificado da chave privada. O certificado da chave privada criado no menu GUI (**políticas do correio > chaves de assinatura**) não será válido quando você o usa para gerar um certificado do PKCS-12 junto com o certificado de CA.

Solução

1. Instale o aplicativo do OpenSSL se sua estação de trabalho não o tem. A versão do Windows pode ser transferida de aqui.Assegure-se de que Visual C++ 2008 Redistributables esteja instalado antes do OpenSSL Win32.
2. Use um molde para criar um script para gerar dentro o CSR e a chave privada aqui.O script olhará como este:**req do OpenSSL - novo - newkey rsa:2048 - Nós - para fora test_example.csr - keyout test_example.key - subj "Cisco Systems /OU=IronPort/CN=test.example.com /C=AU/ST=NSW/L=Sydney/O="**
3. A cópia e cola o script no indicador do OpenSSL e pressiona-o **entra**.

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

   Saída:
   ```
   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. Use o arquivo .CSR para pedir para o certificado de CA.

5. Uma vez que você recebe o certificado de CA, salvar o enquanto **arquivo cacert.pem**. Rebatize o arquivo-chave privado t est_example.key a **test_example.pem. Agora você** pode gerar um certificado do PKCS-12 usando o OpenSSL.

   Comando:

   pkcs12 do OpenSSL - exportação - para fora cacert.p12 - em cacert.pem - inkey test_example.pem

   Se o certificado de CA e a chave privada usados estão corretos, o OpenSSL alerta-o incorporar a **senha da exportação** e confirmar outra vez a senha. Se não, recomenda-o que o certificado e a chave que são usados não combinam e não podem continuar com o processo.

   Entrada:

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

   Saída:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Vão ao menu GUI de IronPort, a **rede > o certificado**.

Seleto **adicionar o certificado**.
Selecione o **certificado de importação na** opção do **certificado adicionar**.

Seleto **escolha** e consulte ao lugar do certificado do PKCS-12 gerado na etapa 5.
Incorpore a mesma senha que você usou usado quando você gerou o certificado do PKCS-12 no OpenSSL (neste caso a senha é **ironport**).
Selecione **em seguida** e a tela seguinte indicará os detalhes dos atributos usados para o certificado.
Selecione **Submit**.
Seleto **comprometa mudanças**.

Após estas etapas, o certificado novo é adicionado aos Certificados alista e pode ser atribuído para o uso.