Aggiunta/importazione di un nuovo certificato PKCS#12 sull'interfaccia utente di Cisco ESA

Sommario

Introduzione

In questo documento viene descritto come aggiungere/importare nuovi certificati PKCS (Public Key Cryptography Standards) n. 12 sull'interfaccia utente di Cisco Email Security Appliance (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- AsyncOS 7.1 e versioni successive

Problema

Da AsyncOS 7.1.0 e versioni successive, è possibile gestire/aggiungere certificati nella GUI degli accessori di posta elettronica. Tuttavia, per questo nuovo certificato, deve essere in formato PKCS#12, quindi questo requisito aggiunge alcuni passaggi aggiuntivi dopo la ricezione del certificato CA (Certification Authority).

La generazione di un certificato PKCS#12 richiede anche il certificato della chiave privata. Se si esegue il comando **certconfig** di Cisco ESA CLI Request (CSR), non si riceverà il certificato della chiave privata. Il certificato della chiave privata creato nel menu della GUI (**Mail Policies > Signing Keys**) non sarà valido quando si utilizza il certificato PKCS#12 con il certificato CA.

Soluzione alternativa

1. Installare l'applicazione OpenSSL se la workstation non dispone di tale applicazione. La versione per Windows può essere scaricata da qui.Verificare che Visual C++ 2008 Redistributables sia installato prima di OpenSSL Win32.
2. Qui è possibile utilizzare un modello per creare uno script per generare CSR e chiave privata.Lo script avrà il seguente aspetto:**openssl req -new -newkey rsa:2048 -nodes -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. Copiare e incollare lo script nella finestra OpenSSL e premere **Invio**.

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

   Uscita:
   ```
   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. Utilizzare il file CSR per richiedere il certificato CA.

5. Dopo aver ricevuto il certificato CA, salvarlo come file **cacert.pem**. Rinominare il file della chiave privata **test_example.key** in **test_example.pem**. È ora possibile generare un certificato PKCS#12 utilizzando OpenSSL.

   Comando:

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

   Se il certificato CA e la chiave privata utilizzati sono corretti, OpenSSL richiede di immettere **Export Password** e confermare nuovamente la password. In caso contrario, viene segnalato che il certificato e la chiave utilizzati non corrispondono e non possono procedere con il processo.

   Ingresso:

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

   Uscita:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. Andare al menu dell'interfaccia utente di IronPort, **Rete > Certificato**.

Selezionare **Aggiungi certificato**.
Selezionare **Importa certificato** nell'opzione **Aggiungi certificato**.
Selezionare **Choose** (Scegli) e individuare il percorso del certificato PKCS#12 generato nel

passaggio 5.
Immettere la stessa password utilizzata al momento della generazione del certificato PKCS#12 in OpenSSL (in questo caso la password è **ironport**).
Selezionare **Avanti** e nella schermata successiva verranno visualizzati i dettagli degli attributi utilizzati per il certificato.
Selezionare **Invia**.
Selezionare **Conferma modifiche**.

Al termine della procedura, il nuovo certificato verrà aggiunto all'elenco dei certificati e potrà essere assegnato per l'utilizzo.