Cisco ESA GUI에서 새 PKCS#12 인증서 추가/가져오기

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[문제](#)
[해결 방법](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance) GUI에서 새 PKCS(Public Key Cryptography Standards) #12 인증서를 추가/가져오는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS 7.1 이상

문제

AsyncOS 7.1.0 이상 버전부터는 이메일 어플라이언스의 GUI에서 인증서를 관리/추가할 수 있습니다.그러나 이 새 인증서의 경우 PKCS#12 형식이어야 하므로 이 요구 사항은 CA(Certificate Authority) 인증서를 받은 후 몇 가지 추가 단계를 추가합니다.

PKCS#12 인증서를 생성하려면 개인 키 인증서도 필요합니다.Cisco ESA CLI 명령 certconfig에서 CSR(Certificate Signing Request)**을** 실행하면 개인 키 인증서가 수신되지 않습니다. GUI 메뉴에서 생성한 개인 키 인증서(**메일 정책 > 서명 키**)는 CA 인증서와 함께 PKCS#12 인증서를 생성하는 데 사용할 때 유효하지 않습니다.

해결 방법

1. 워크스테이션에 OpenSSL 애플리케이션이 없는 경우 OpenSSL 애플리케이션을 설치합니다.여기서 Windows 버전을 다운로드할 수 있습니다.OpenSSL Win32에 앞서 Visual C++ 2008 재배포 가능 장치가 설치되어 있는지 확인하십시오.
2. 템플릿을 사용하여 여기에서 CSR 및 개인 키를 생성하는 스크립트를 생성합니다.스크립트는 다음과 같습니다.**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. 스크립트를 복사하여 OpenSSL 창에 붙여넣고 Enter를 **누릅니다**.

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

   출력:

   ```
   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. .CSR 파일을 사용하여 CA 인증서를 요청합니다.

5. CA 인증서를 받으면 cacert**.pem** 파일로 **저장합니다**.개인 키 파일 **test_example.key**의 이름을 **test_example.pem으로 바꿉니다**.이제 OpenSSL을 사용하여 PKCS#12 인증서를 생성할 수 있습니다.

   명령:

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

   사용된 CA 인증서와 개인 키가 올바르면 OpenSSL에서 Export Password(**비밀번호 내보내기**)**를** 입력하고 비밀번호를 다시 확인하라는 메시지를 표시합니다.그렇지 않으면 사용된 인증서와 키가 일치하지 않으며 프로세스를 진행할 수 없음을 알립니다.

   입력:

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

   출력:

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```
6. IronPort GUI 메뉴, **Network > Certificate로 이동합니다**.

Add **Certificate를 선택합니다**.
Add **Certificate** 옵션에서 Import **Certificate를** 선택합니다.
Choose(**선택**)를 선택하고 5단계에서 생성된 PKCS#12 인증서의 위치를 찾습니다.
OpenSSL에서 PKCS#12 인증서를 생성할 때 사용한 것과 동일한 비밀번호를 입력합니다(이 경우 비밀번호는 **ironport**).
Next(**다음**)를 선택하면 다음 화면에 인증서에 사용된 특성 세부사항이 표시됩니다.
제출을 **선택합니다**.

Commit **changes를 선택합니다**.

이러한 단계 후에 새 인증서가 인증서 목록에 추가되며 사용할 수 있도록 할당할 수 있습니다.