ىلع ةديدج PKCS#12 ةداەش داريتسإ/ةفاضإ قيموسرلا مدختسملا ةەجاو Cisco ESA

المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المشكلة</u> <u>الحل</u>

المقدمة

يصف هذا وثيقة كيف أن يضيف/يستورد جديد مفتاح تشفير معايير (PKCS #12 شهادة على ال cisco بريد إلكتروني أمن تطبيق (BUI) (ESA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco ESA •
- AsyncOS 7.1 والإصدارات الأحدث

المشكلة

بما أن AsyncOS 7.1.0 والإصدارات الأحدث، من الممكن إدارة/إضافة شهادات في واجهة المستخدم الرسومية (GUI) لأجهزة البريد الإلكتروني. على أي حال، من أجل هذه الشهادة الجديدة، يجب أن تكون بتنسيق PKCS#12، لذلك فإن هذا المتطلب يضيف بعض الخطوات الإضافية بعد إستلام شهادة المرجع المصدق (CA).

يتطلب إنشاء شهادة PKCS#12 أيضا شهادة المفتاح الخاص. إذا قمت بتشغيل طلب توقيع الشهادة (CSR) من أمر واجهة سطر الأوامر Cisco ESA CLI **certconfig**، فلن تتلقى شهادة المفتاح الخاص. لن تكون شهادة المفتاح الخاص التي تم إنشاؤها في قائمة واجهة المستخدم الرسومية (**نهج البريد > مفاتيح التوقيع**) صالحة عندما تستخدمها لإنشاء شهادة PKCS#12 مع شهادة CA.

الحل

- 1. قم بتثبيت تطبيق OpenSSL إذا لم يكن في محطة العمل. يمكن تنزيل إصدار Windows من <u>هنا</u>.تأكد من تثبيت جداول إعادة التوزيع Visual C++ 2008 قبل OpenSSL Win32.
- 2. أستخدم قالبا لإنشاء برنامج نصي لإنشاء CSR ومفتاح خاص في <u>هنا</u>.سيبدو السيناريو كما يلي: **openssi req** new -new -new key rsa:2048 -node -out test_example.csr -keyout test_example.key -subj "o=Cisco Systems/OU=IronPort/CN=test.example.com"
 - 3. انسخ النص البرمجي ولصقه في نافذة OpenSSL واضغط على Enter.

```
C:\OpenSSL-Win32\bin>openssl req -new -new -new key 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
```

```
الناتج:
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
أستخدم ملف .csr لطلب شهادة CA.
```

. بمجرد أن تستلم شهادة CA، قم بحفظها على هيئة ملف **cacert.pem**. قم بإعادة تسمية ملف المفتاح الخاص. .OpenSSL إلى test_example.pem. الآن يمكنك إنشاء شهادة PKCS#12 باستخدام .

.4

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

إذا كانت شهادة CA والمفتاح الخاص المستخدمين صحيحين، يطلب منك OpenSSL إدخال **كلمة مرور التصدير** وتأكيد كلمة المرور مرة أخرى. وإلا، فإنه ينصحك بأن الشهادة والمفتاح المستخدمين لا يتطابقان ولا يمكنهما متابعة العملية.

الإدخال:

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

الناتج:

cacert.p12 (the PKCS#12 certificate). 6. انتقل إلى قائمة واجهة المستخدم الرسومية IronPorl، **الشبكة > الترخيص**. حدد **إضافة شهادة**. حدد **إضتيراد شهادة** في خيار **إضافة شهادة**. حدد **إختيار** وتصفح إلى مكان شهادة 21#PKCS المولدة في الخطوة 5. أدخل نفس كلمة المرور التي أستخدمتها عند إنشاء شهادة 21#PKCS في 2000 (في هذه الحالة تكون كلمة المرور هي ironPort). حدد **التالي** وستعرض الشاشة التالية تفاصيل السمات المستخدمة للشهادة. حدد **إرسال**.

بعد هذه الخطوات، تتم إضافة الشهادة الجديدة إلى قائمة الشهادات ويمكن تعيينها للاستخدام.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما