Содержание

Введение

Этот документ описывает, как добавить/импортировать новые Стандарты шифрования с открытым ключом (PKCS) #12 сертификаты на Cisco GUI Email Security Appliance (ESA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- AsyncOS 7.1 и позже

Проблема

Начиная с AsyncOS 7.1.0. и позже, возможно управлять/добавлять сертификатами в GUI почтовых устройств. Однако для этого новый сертификат, это должно быть в формате PKCS#12, таким образом, это требование добавляет некоторые дополнительные шаги после получения сертификата Центра сертификации (CA).

Генерация сертификата PKCS#12 также требует Сертификата С закрытым ключом. При выполнении Запроса подписи сертификата (CSR) от команды CLI ESA Cisco **certconfig** вы не получите Сертификат С закрытым ключом. Сертификат С закрытым ключом, созданный в меню графического интерфейса пользователя (**Почтовая Политика> Ключи подписи**), не будет допустим при использовании его для генерации сертификата PKCS#12 вместе с сертификатом CA.

Обходной путь

1. Установите приложение OpenSSL, если ваша рабочая станция не имеет его. Версия Windows может быть загружена отсюда.Гарантируйте, что Visual C++ 2008 Распространяемых файлов установлен перед Win32 OpenSSL.

2. Используйте шаблон для создания сценария для генерации CSR и Секретного ключа в здесь.Сценарий будет похож на это:**req openssl - новый-newkey rsa:2048 - узлы - test_example.csr-keyout test_example.key - тема "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test. пример. com"**
3. Скопируйте и вставьте сценарий в окно OpenSSL и нажмите **Enter**.

   C : \OpenSSL-Win32\bin> openssl req - новый-newkey rsa:2048 - узлы - test_example.csr-keyout
   test_example.key - тема "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test. пример. com"

   Выходные данные:
4. Используйте.CSR файл для запроса на сертификат CA.

5. Как только вы получаете сертификат CA, сохраняете его как **cacert.pem** файл. Переименуйте файл закрытого ключа **test_example.key** к **test_example.pem**. Теперь можно генерировать сертификат PKCS#12 с помощью OpenSSL.

   Команда:

   pkcs12 openssl - экспорт - cacert.p12 - в cacert.pem-inkey test_example.pem

   Если сертификат CA и используемый секретный ключ корректны, OpenSSL побуждает вас вводить **Пароль Экспорта** и подтверждать пароль снова. В противном случае это советует вам, с которыми сертификат и ключ, которые используются, не совпадают и не могут продолжить процесс.

   Ввод:

   Выходные данные:
6. Перейдите к меню графического интерфейса пользователя IronPort, **Сеть> Сертификат**.

Выберите **Add Certificate**.
Выберите **Import Certificate** в опции **Add Certificate**.
Выберите **Choose** и перейдите к местоположению сертификата PKCS#12, генерируемого в Шаге 5.
Введите тот же пароль, который вы использовали используемый при генерации сертификата PKCS#12 в OpenSSL (в этом случае, пароль является **ironport**).
Выберите **Next**, и следующий экран отобразит подробные данные атрибутов, используемые для сертификата.
Выберите **Submit**.
Выберите **изменения Commit**.

После этих шагов новый сертификат добавлен к списку сертификатов и может быть назначен для использования.