Создайте запрос подписи сертификата на ESA

Содержание

Введение

Этот документ описывает, как создать запрос подписи сертификата (CSR) на Email Security Appliance (ESA).

Создайте CSR на ESA

С AsyncOS 7.1.1 ESA может создать подписанный сертификат для вашего собственного использования и генерировать CSR, чтобы подвергнуться центру сертификации и получить общий сертификат. Центр сертификации возвращает доверяемый общий сертификат, подписанный секретным ключом. Используйте страницу **Network> Certificates** в GUI или **certconfig** команду в CLI, чтобы создать подписанный сертификат, генерировать CSR и установить доверяемый общий сертификат.

Если вы получаете или создаете сертификат впервые, ищете Интернет "Сертификаты SSL - сервера сервисов центра сертификации" и выбираете сервис, который лучше всего удовлетворяет потребности вашей организации. Следуйте инструкциям сервиса для получения сертификата.

Действия настройки на GUI

1. Для создания подписанного сертификата **нажмите Add Сертификат** на странице Network> Certificates в GUI (или **certconfig** команда в CLI). На странице Add Certificate выберите **Create Self-Signed Certificate**.
2. Введите эту информацию для подписанного сертификата: Общее имя - полное доменное имя.Организация - Точное официальное имя организации.Подразделение - Раздел организации.Город (Местность) - Город, где по закону расположена организация.Состояние (Область) - Состояние, графство или область, где по закону расположена организация.Страна - Две буквы Международная организация по стандартизации (ISO) сокращение страны, где по закону расположена организация.Продолжительность перед истечением - число дней перед сертификатом

истекает.Размер С закрытым ключом - Размер секретного ключа для генерации для CSR. Только 2048-разрядный и 1024-разрядный поддерживаются.
3. Нажмите **Next** для просмотра сертификата и данных о подписи.
4. Введите имя для сертификата. AsyncOS назначает общее имя по умолчанию.
5. Если вы хотите отправить CSR для подписанного сертификата к центру сертификации, нажмите **Download Certificate Signing Request** для сохранения CSR в формате Privacy Enhanced Mail (PEM) к локальной или сетевой машине.
6. Нажмите **Submit**, чтобы сохранить сертификат и передать ваши изменения. При отъезде изменений незафиксированными секретный ключ потеряется, и подписанный сертификат не может быть установлен.

Когда центр сертификации возвращает доверяемый общий сертификат, подписанный секретным ключом, нажмите название сертификата на странице Certificates и введите путь к файлу на вашем локальном компьютере или сети для загрузки сертификата. Удостоверьтесь, что доверяемый общий сертификат, который вы получаете, находится в формате PEM или формате, который можно преобразовать в PEM, прежде чем это будет загружено к устройству. Программные средства для завершения этого включены с OpenSSL, открытые программные средства, доступные в http://www.openssl.org.

При загрузке сертификата от центра сертификации существующий сертификат перезаписан. Можно также загрузить промежуточный сертификат, отнесенный к подписанному сертификату. Можно использовать сертификат с общим или частным слушателем, сервисами HTTPS IP - интерфейса, интерфейсом Протокола LDAP или всеми исходящими соединениями Transport Layer Security (TLS) с целевыми доменами.

Дополнительные сведения

- Всестороннее руководство по установке для TLS на ESA
- Cisco Systems – техническая поддержка и документация