Как генерировать и установить цифровой сертификат на SMA?

Содержание

Введение

Этот документ описывает, как генерировать сертификат на Email Security Appliance (ESA), который может использоваться на устройстве управления безопасностью (SMA).

Как генерировать и установить цифровой сертификат на SMA?

Общие сведения

SMA не поддерживает генерирующиеся сертификаты на самом устройстве. Вместо этого возможно генерировать сам подписанный сертификат на ESA. Это может использоваться в качестве обходного пути для создания сертификата для SMA, который будет импортироваться и использоваться.

Создайте и экспортируйте сертификат на ESA

1. Создайте сам подписанный сертификат под **GUI: Сеть> Сертификаты> Добавляет Сертификат.** Это важно, при создании сам подписанный сертификат, для Общего имени (CN) для использования имени хоста SMA а не ESA, так, чтобы мог должным образом использоваться сертификат. Отправьте и передайте изменения.
2. **GUI** использования**: Сеть> Сертификаты> Сертификаты Экспорта** для экспортирования сертификата. Дайте ему имя файла (например, mycert) и пароль, который будет использоваться при преобразовании сертификата.

Преобразуйте экспортируемый сертификат

Экспортируемый сертификат будет в формате **.pfx**. SMA только поддерживает формат **.pem** для импорта, таким образом, должен быть преобразован этот сертификат. Для преобразования сертификата от формата .pfx до формата .pem используйте следующий синтаксис OpenSSL.

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

После преобразования сертификата к правильному формату оба должны присутствовать сертификат и соответствующий секретный ключ в формате .pem. Важно иметь certifcate **и** availabe с закрытым ключом. Только certifcate без секретного ключа не может быть импортировано в SMA. Рекомендуется подписать сертификат доверенным центром сертификации (CA). Cisco не рекомендует, чтобы определенный CA. Для подписания выбрал **"Download certificate signing request"** на GUI ESA и отправил его доверяемому предпочтительному CA.

Сертификат импорта к SMA - Опция 1

Подписанный сертификат CA или сам подписанный сертификат и секретный ключ в формате .pem, может быть импортирован теперь в SMA. Чтобы изучить, как сделать это, считайте TechNote, "Как я устанавливаю сертификаты на SMA?" как отнесено ниже.

Сертификат импорта к SMA - Опция 2

Вместо того, чтобы преобразовать сертификат из .pfx в .pem можно просто сохранить файл конфигурации, не маскируя пароли на ESA. Откройте XML-файл и ищите <сертификат> метку. Вы уже найдете сертификат и секретный ключ в формате PEM. Скопируйте сертификат и секретный ключ для импорта того же в SMA, как описано в TechNote, "Как я устанавливаю сертификаты на SMA?" как отнесено ниже.

> **Примечание:** Если вы идете для опции 2 и если вам подписал сертификат CA, сначала необходимо импортировать подписанный сертификат назад к ESA прежде, чем сохранить файл конфигурации на то, что он сделал копию сертификата и секретного ключа. Импорт может быть сделан путем щелчка по названию сертификата на GUI ESA и опции "Upload Signed Certificate" использования.

Проверьте импортированный сертификат

1. Обратитесь к GUI SMA через HTTPS (https://<IP SMA или имя хоста>) и вставьте свои учетные данные
2. Рядом с URL в строке адреса на вашем браузере нажмите значок Блокировки и проверьте законность сертификата, истечения, и т.д.
3. Щелкните по Пути сертификации для проверки цепочки сертификатов

Дополнительные сведения

- Как я устанавливаю сертификаты на SMA?
- Онлайновый преобразователь SSL