Содержание

Вопрос

Как проверить, что сертификат SSL был подписан связанным, включают Устройство Безопасности электронной почты Cisco?

Среда: Cisco Email Security Appliance (ESA), все версии AsyncOS

Эта статья Базы Знаний ссылается на программное обеспечение, которое не поддерживается Cisco. Информация предоставлена как любезность для вашего удобства. Для дальнейшей поддержки свяжитесь с поставщиком программного обеспечения.

Установка сертификатов SSL является предпосылкой к шифрованию получения/доставки через TLS и безопасного доступа LDAP. Сертификаты установлены через команду CLI 'certconfig'. Сертификат/пара ключей, который вы намереваетесь установить, должен включить ключ, который подписал сертификат. Не соответствие этому приведет к сбою для установки сертификата/пары ключей.

Следующие шаги помогают проверять, был ли сертификат подписан с связанным ключом. Предположите, что у вас есть секретный ключ в файле, названном 'server.key' и сертификатом в 'server.cer'.

1. Удостоверьтесь, что поля экспоненты сертификата и ключа являются тем же. Если дело обстоит не так, то ключ не является подписывающим лицом. Следующие команды (работает на любой стандартной машине Unix с openssl) помогут проверять это.

   Удостоверьтесь, что поле экспоненты в сертификате и ключе является тем же. Ключ экспоненты должен быть равен 65537.

2. Выполните хэш MD5 на модуле и сертификата и ключа, чтобы гарантировать, что они - то же.

Если два хэша MD5 подобны, то вас можно уверить, что ключ подписал сертификат.

Ссылки по теме

http://www.modssl.org/docs/2.8/ssl_faq.html