Шифрование данных устройства безопасности содержания с SSL и TLS

Содержание

Введение

Этот документ предоставляет определения для методов шифрования Уровня защищенных сокетов (SSL) и Transport Layer Security (TLS) и описывает, как они используются.

SSL и обзор TLS

SSL и методы шифрования TLS являются двумя наиболее высоко используемыми методами для шифрования данных по сетевому потоку или транспортируют сеанс.

Метод шифрования SSL был первоначально разработан Netscape для обеспечения Связей HTTP, которые пересекли Интернет во время его широко распространенного принятия в 1990-х. Версия SSL 2.0 была первым релизом общего пользования, придерживавшимся вскоре Версией SSL 3.0, которая была обновлена для адресации к некоторым серьезным дефектам безопасности в предыдущей версии.

Версия TLS 1.0 была преемником Версии SSL 3.0. Это предложило алгоритм безопасности, предупреждение и усовершенствования спецификации. Несмотря на то, что изменения были тонкими, они были достаточно решительными для создания этих двух протоколов несовместимыми друг с другом. Метод шифрования TLS был с тех пор улучшен с дополнительными наборами шифров, такими как Расширенный стандарт шифрования (AES) и более безопасные алгоритмы генерации ключа. Актуальнейшей версией в это время является Версия TLS 1.2.

> **Примечание:** С AsyncOS 8.5.6 только поддерживается v1 TLS. V1.1 TLS, 1.2 еще не поддерживаются. Рассмотрите **sslconfig** от CLI и выберите **GUI**, **INBOUND** или **OUTBOUND** для просмотра доступных методов шифрования.

SSL и использование TLS

Сегодня, большинство программ клиент-сервер, которые используют безопасные транспорты, такие как Протокол SMTP и транзакции HTTPS, основывается на Версии SSL 3.0 и Версии TLS 1. x . Несмотря на то, что много приложений имеют встроенную поддержку для безопасных транспортов как SSL и TLS, любую программу можно нести по безопасным туннелям. Много новых приложений развились поэтому, такие как безопасная телефонная связь как Протокол SIP и VPN, которые используют модифицированный метод шифрования TLS, который несут по пакетам IP типа UDP (DTL).

В то время как SSL сроков и TLS иногда используются взаимозаменяемо, протоколы не идентичны. Основные различия вращаются вокруг наборов шифров (типы шифрования), о которых выполняет согласование клиент и сервер, а также методы, которыми они выбирают те шифры. По существу TLS является предпочтительными средствами для шифрования передач по сети, поскольку его разработка более открыта и устойчива и была стандартизирована IETF.

Примечание: См. RFC 5246 для подробных данных о спецификациях Версии TLS 1.2 и интернет-Проекте SSL для получения информации о Версии SSL 3.0.