1. Выбор подходящей версии TLS

При выборе подходящих версий TLS отталкивался от TLS Cipher String Cheat Sheet, Mozilla SSL Configuration Generator. Согласно этим источникам наиболее предпочтительным с точки зрения безопасности является TLSv1.3. TLSv1.3 имеет ряд преимуществ:

- Устранение уязвимых алгоритмов и шифров (SHA-1, MD5 и т.д.).
- Улучшение процесса установки соединения (one round-trip handshake).
- Упрощенные наборы шифров (наборы шифров больше не включают алгоритмы обмена ключами и подписи).

Но TLSv1.3 поддерживается только последними версиями браузера, поэтому для охвата большего количества клиентов те ресурсы рекомендуют так же использовать TLSv1.2, но с заданным набором алгоритмов.

2. Выбор подходящих и достаточно безопасных шифров для сервера.

Для упрощения выбора алгоритмов можно выбирать из алгоритмов обозначеных в стандарте TLSv1.3 и совместимые с TLSv1.2:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

Все алгоритмы согласно TLS Cipher String Cheat Sheet являются безопасными за исключением TLS_AES_128_CCM_8_SHA256, TLS_AES_128_CCM_SHA256. Данные алгоритмы подвержены атакам и некоторые их подмножества не поддерживаются браузерами. В итоге полученный список алгоритмов (имена совместимые с OpenSSL):

- TLS_AES_256_GCM_SHA384;
- TLS_CHACHA20_POLY1305_SHA256;
- TLS_AES_128_GCM_SHA256;
- DHE-RSA-AES256-GCM-SHA384;
- DHE-RSA-AES128-GCM-SHA256;
- ECDHE-RSA-AES256-GCM-SHA384;
- ECDHE-RSA-AES128-GCM-SHA256;
- DHE-RSA-AES256-SHA256;
- DHE-RSA-AES128-SHA256;
- ECDHE-RSA-AES256-SHA384;
- ECDHE-RSA-AES128-SHA256/

3. Генерация ключей и сертификатов для настройки TLS.

Выбора алгоритмов для генерации ключей делался на основе Choosing a key algorithm. Согласно документу предпочтительными алгоритмами являются алгоритмы на основе ECDSA с длиной ключа 384-bit. Они являются такими из-за невозможностей логрифмирвания элипчтичеких кривых для нахождения праобразов за разумное время. Поэтому для создания выбрал кривую prime256v1 (NIST Curve P-256) так как она поддерживается большинством браузеров.

В целях безопасности CA sever должен быть изолированный от сети Интернет и иметь ограничения доступа к нему. Приватный CA key не должен покидать устройство. Приватный Server key так же не должен покидать пределы устройства.

Из-за отсутвия возможностей проведения этих операций согласно правил, CA файлы сгенерированы с помощью root пользователя, а Server файлы с помощью пользователя который запускает сервер.

4. Настройка reverse proxy с помощью Nginx.

Генерация конфигов для Nginx для упрощения задачи проведена с помощью NGINX Configuration Generator Tool. Были использованы дополнительные настройки кроме указаных в пункте 1 для обеспечения безопасности и производительности HTTPS. Файлы конфигураций содержат заметки относительно этих настроек.