Инструкция по установке TLS-сертификатов для сервера nginx

1. Скачайте промежуточный сертификат. Промежуточные сертификаты доступны для скачивания на странице сертификата.

2. Скачайте сертификат домена. Сделать это можно из разделов «Мои заказы» и «Мои сертификаты», кликнув по кнопке «Скачать» напротив соответствующего сертификата. Скачать сертификат можно также со страницы сертификата.

3. Настройте сервер nginx.

   Обращаем ваше внимание, что структура конфигурационных файлов сервера nginx может быть различной для разных операционных систем. Далее мы рассмотрим настройку типового сервера nginx.

   Требуемые конфигурационные файлы содержатся в «директивах» - блоках, выделенных фигурными скобками, которые содержат внутри параметры конфигурации сервера. В типовой конфигурации веб-сервера нужные нам блоки находятся в файле ***/etc/nginx/sites-enabled/default***

   Рекомендуется следующая конфигурация (используется для версии nginx 1.1.19 и OpenSSL 1.0.1; следует заменить имя хоста и имена директорий веб-сервера на актуальные для локальной конфигурации):

```
# HTTPS server
server {
listen 443;
server_name example.com;
root html;
index index.html index.htm;
ssl on;
ssl_certificate /etc/ssl/bundle.crt;
ssl_certificate_key /etc/ssl/my_private.key;
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers –
ALL:EECDH+aRSA+AESGCM:EDH+aRSA+AESGCM:EECDH+aRSA+AES:EDH+aRSA+AES;
ssl_prefer_server_ciphers on;
 location / {
try_files $uri $uri/ /index.html;
 }
}
```

   Для настройки сервера потребуется подготовить файл сертификатов (***/etc/ssl/bundle.crt***) и файл секретного ключа (***/etc/ssl/my_private.key***). В данном примере используются несколько файлов: файл с приватным ключом (***my_private.key***), файл с серверным сертификатом (***public.crt*** *— это сертификат, который соответствует имени сервера*) и файл с промежуточным сертификатом (***intermediate.crt***).

3.1 В первую очередь, необходимо сделать один файл из файлов с основным и промежуточным сертификатами: ***cat public.crt intermediate.crt >> bundle.crt***
Если имеются дополнительные файлы с промежуточными сертификатами, их следует добавить в этот же файл аналогичным образом.

3.2 Далее укажите правильные пути к файлам в конфигурации выше (пути должны соответствовать расположению файлов в файловой системе, то есть директориям, в которые вы скопировали файл ***bundle.crt*** и файл ***my_private.key***):

```
ssl_certificate /etc/ssl/bundle.crt;
ssl_certificate_key /etc/ssl/my_private.key;
```

3.3 Затем сохраните и закройте редактируемый файл, после чего проверьте конфигурацию командой: ***nginx –t***
Если секретный ключ защищён паролем, то потребуется ввести этот пароль. При обнаружении некорректных настроек в конфигурационном файле nginx выдаст сообщение об ошибке. Для использования команды nginx могут потребоваться права суперпользователя/ администратора (root).

3.4 Если сервер не выдал сообщений об ошибке, перезапустите сервер командой ***service nginx restart*** или ***systemctl restart nginx***, в зависимости от используемого системного окружения. Сервер попросит повторно ввести пароль, если он был задан для приватного ключа.

3.5 Если при запуске сервера не было сообщений об ошибке, вы можете проверить правильность установки сертификата, обратившись к серверу через браузер.

Значения остальных параметров ***ssl_*** в секции ***server*** приведены на странице документации nginx (на русском языке).