Инструкция по установке веб сервера nginx, ЦС и клиента с поддержкой mTLS.

Для установки вебсервера и клиента необходимо:

1. Скачать архив install.tar.xz на локальную машину.

2. Любым удобным способом (ftp, ssh...) закачать архив на стенд в любую папку.

3. Распаковать архив - tar -xvf install.tar.xz

4. Дать права на скрипты - sudo chmod 777 install.sh keys.sh

5. Для первоначальной установки nginx и создания ключей пользоваться скриптом install.sh - sudo ./install.sh

6. Для удаления ключей и сертификатов или повторного создания использовать скрипт keys.sh - sudo ./keys.sh

В процессе создания сертификатов, необходимо заполнить следующие поля:

Country Name (2 letter code) [XX]: - Код страны (2 буквы код).

State or Province Name (full name) []: - Область или регион.

Locality Name (eg, city) [Default City]: - Название города.

Organization Name (eg, company) [Default Company Ltd]: - Наименование организации.

Organizational Unit Name (eg, section) []: - Наименование подразделения или отдела организации.

Common Name (eg, your name or your server's hostname) []: - Днс имя. Если настроен днс или ip адресс.

Email Address []: - почтовый адрес.

Так же при создании сертификата можно заполнить следующие поля:

A challenge password []: - Пароль

An optional company name []: - Дополнительное название компании.

При создании .p12 сертификата для клиентской части (например для браузера) может потребоваться ввести два поля паролей. Это пароли на разархивацию сертификата.

В конец файла /*etc/*hosts прописываем 127.0.0.1 localhost.localdomain.com (sudo nano /etc/hosts)

Проверить работу сертификата можно следующей командой:

sudo curl -v -k --key /etc/httpd/certs/client.key --cert /etc/httpd/certs/client.crt --capath /etc/httpd/certs/ca.crt --url https://192.168.111.21:443

Вместо localhost необходимо прописать свой домен или ip адрес (то что указывали в ) Common Name.

Для создания самоподписного сертификата Common name CA и server, cleint должны совпадать.

Если надо создать доверенный сертификат, то Common name CA и остальных сертификатов должны быть разные.

Для доступа к сайту необходимо из сервера (из /etc/httpd/certs) скачать сертификат клиентской части client.p12 и установить в браузер. Обычно в браузере надо зайти в Настройки — безопасность — управление сертификатами. Но для каждого браузера установка сертификатов осуществляется по-своему. Лучше уточнить в google.com

Внимание!!!

В связи с особенностями работы с сертификатами в ФаерФокс, данный браузер работать не будет. Тестирование необходимо проводить на любых других браузерах: Опера, Хром, Эдж, Яндекс браузер...