Установка https без сертификации (самоподписной сертификат)

При использовании самоподписного сертификата, ничего не требуется, однако:

- Соединение не является безопасным
- Браузер будет выдавать предупреждения, необходимо добавить исключение
- Нельзя использовать CSP, как PWA приложение
- Использовать CSP Client можно полноценно

Самоподписной сертификат

```
export MYSITE=csp
mkdir -p /etc/nginx/ssl/${MYSITE}
openssl req -x509 -nodes -days 3650 -subj /C=CA/ST=None/L=NB/O=None/CN=${MYSITE} -newkey rsa:2048 -keyout /etc/nginx/ssl/${MYSITE}/ssl.key -out /etc/nginx/ssl/${MYSITE}/cert.crt
```

В MYSITE можно указать свой домен (напр. mysite.ru)

Установка nginx

```
apt install nginx
rm /etc/nginx/sites-enabled/default
```

Создать файл /etc/nginx/sites-enabled/csp

```
 server {
   listen 80;
   listen [::]:80;

   error_log /var/log/nginx/csp-error.log warn;

   location / {
     #Websocket support
     proxy_set_header Upgrade $http_upgrade;
     proxy_set_header Connection $http_connection;
     proxy_http_version 1.1;

     #Proxy
```

```
    client_max_body_size 100m;
    add_header       X-Served-By $host;
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-Scheme $scheme;
    proxy_set_header X-Forwarded-Proto  $scheme;
    proxy_set_header X-Forwarded-For    $proxy_add_x_forwarded_for;
    proxy_set_header X-Real-IP          $remote_addr;
    proxy_pass       http://127.0.0.1:8080;
  }

  location ^~ /.well-known/acme-challenge/ {
     default_type "text/plain";
     root /var/www/acme;
  }

  listen 443 ssl;
  listen [::]:443 ssl;

  ssl_certificate /etc/nginx/ssl/csp/cert.crt;
  ssl_certificate_key /etc/nginx/ssl/csp/ssl.key;
}
```

```
ln -s /etc/nginx/sites-available/csp /etc/nginx/sites-enabled/csp
service nginx restart
```

Revision #8
Created 30 May 2025 10:40:07 by Admin
Updated 7 August 2025 16:16:44 by Admin