Ubuntu 14.04 связка Apache + Nginx

Полезные ссылки:

https://letsencrypt.org/ru/docs/ - LetsEncrypt документация (ru)

https://certbot.eff.org/lets-encrypt/ubuntubionic-apache - Инструкция по использованию Certbot для Ubuntu 18.04 + Apache

https://crt.sh - Сервис проверки по базе сертификатов.

https://tools.letsdebug.net - Онлайн инструменты для работы с базой сертификатов. Отзыв, отмена блокировки и т.д.

Альтернативные сервисы SSL Free

https://www.sslforfree.com/

https://freessl.space/

Сертификат от Lets'Encrypt

Не забываем про IPTABLES

```
iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Установка letsencrypt

```
apt-get -y install git bc
git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt
```

Получение сертификата плагином webroot

Пример для домена update.infomir.com

```
cd /opt/letsencrypt/
./letsencrypt-auto certonly --webroot -w /var/www/update.infomir.com -d
update.infomir.com
```

включаем ssl для Apache

```
sudo a2enmod ssl
```

Пример конфига хоста Apache /etc/apache2/sites-available/update.infomir.com

```
<VirtualHost *:88>
        ServerName update.infomir.com

        DocumentRoot /var/www/update.infomir.com

        <Directory /var/www/update.infomir.com>
                Options -Indexes -MultiViews
                AllowOverride ALL
                Require all granted
        </Directory>

        <Directory /var/www/update.infomir.com/im/4414>
                Order allow,deny
                Deny from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/update.infomir.com_error.log
        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        ServerSignature Off

        CustomLog ${APACHE_LOG_DIR}/update.infomir.com_access.log combined
        #CustomLog /dev/null combined
</VirtualHost>

<VirtualHost *:443>
        ServerAdmin infomiriptv@gmail.com
        ServerName update.infomir.com

#        Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains;"

        SSLEngine on
        SSLProtocol all -SSLv2 -SSLv3
        SSLHonorCipherOrder on
        SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256
EECDH+aRSA+RC4 EECDH EDH+aRSA !RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK
!SRP !DSS"
        SSLCertificateKeyFile
/etc/letsencrypt/live/update.infomir.com/privkey.pem
        SSLCertificateFile /etc/letsencrypt/live/update.infomir.com/cert.pem
        SSLCertificateChainFile
```

```
/etc/letsencrypt/live/update.infomir.com/chain.pem

        DocumentRoot /var/www/update.infomir.com

        RewriteEngine On

        <Directory /var/www/update.infomir.com>
                Options -Indexes +FollowSymLinks +Includes
                AllowOverride All
                Order allow,deny
                Allow from All
        </Directory>

        LogLevel  warn
        ErrorLog  ${APACHE_LOG_DIR}/update.infomir.com_error.log
        CustomLog ${APACHE_LOG_DIR}/update.infomir.com_access.log combined
        #CustomLog /dev/null combined

        ServerSignature Off
</VirtualHost>
```

Пример /etc/apache2/ports.conf

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 88

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Ubuntu 18.04 (пример реализации для update.infomir.com связка apache+nginx)

Метод получения сертификатов - **webroot**.

1. Установка, настройка letsencrypt, certbot
2. Конфигурация nginx, apache
3. Конфигурация iptables

4. Получение сертификатов
5. Продления сертификатов. Автоматизация

Установка, настройка letsencrypt, certbot

```
apt-get install python-certbot-apache
```

Файл /etc/letsencrypt/cli.ini приводим к виду:

cli.ini

```
# Because we are using logrotate for greater flexibility, disable the
# internal certbot logrotation.
max-log-backups = 0
authenticator = webroot
webroot-path = /var/www/letsencrypt
post-hook = systemctl reload apache2
```

Конфигурация nginx, apache

Создать каталог /var/www/letsencrypt/.well-known/

```
mkdir -p /var/www/letsencrypt/.well-known
chgrp www-data/var/www/letsencrypt
chmod g+s /var/www/letsencrypt
```

Nginx

Создать файл /etc/nginx/templates/letsencrypt.conf. При отсутствии создать каталог /etc/nginx/templates/

letsencrypt.conf

```
location ^~ /.well-known/acme-challenge/ {
   default_type "text/plain";
   root /var/www/letsencrypt;
}
location = /.well-known/acme-challenge/ {
   return 404;
```

В конфигурацию хоста, в секцию server добавить строку include /etc/nginx/templates/letsencrypt.conf;

/etc/nginx/sites-available/update.infomir.com

```
server {
        listen       80;
        server_name  update.infomir.com;

        location / {

                proxy_pass http://localhost:88/;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        }

        include /etc/nginx/templates/letsencrypt.conf;

        location ~*
\.(htm|html|jpeg|jpg|gif|png|css|js|pdf|txt|tar|mpg|avi|mkv|imageupdate
*)$ {
                root /var/www/update.infomir.com;
        }

    access_log /var/log/nginx/update.infomir.com_access.log;
    error_log /var/log/nginx/update.infomir.com_error.log error;
}
```

Apache

В этом варианте не используется безусловный редирект на HTTPS. Доступ к хосту возможен по двум протоколам.

Для безусловного редиректа раскоментировать строку `Redirect permanent / https://update.infomir.com/`

Конфигурацию хоста приводим к виду:

/etc/apache2/sites-available/update.infomir.com

```
<VirtualHost *:88>
    ServerName update.infomir.com

    DocumentRoot /var/www/update.infomir.com

    <Directory /var/www/update.infomir.com>
#       Redirect permanent / https://update.infomir.com/
      Options -Indexes -MultiViews
      AllowOverride ALL
#     Order allow,deny
#     allow from all
```

```
      Require all granted
    </Directory>

    <Directory /var/www/update.infomir.com/im/4414>
      Order allow,deny
      Deny from all
    </Directory>


        ErrorLog ${APACHE_LOG_DIR}/update.infomir.com_error.log

        # Possible values include: debug, info, notice, warn, error,
crit,
        # alert, emerg.
        LogLevel warn

        ServerSignature Off

       CustomLog ${APACHE_LOG_DIR}/update.infomir.com_access.log
combined
        #CustomLog /dev/null combined

</VirtualHost>

<VirtualHost *:443>
        ServerAdmin infomiriptv@gmail.com
        ServerName update.infomir.com

#        Header always set Strict-Transport-Security "max-age=63072000;
includeSubdomains;"

        SSLEngine on
        SSLProtocol all -SSLv2 -SSLv3
        SSLHonorCipherOrder on
        SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA !RC4 !aNULL !eNULL !LOW
!3DES !MD5 !EXP !PSK !SRP !DSS"
        SSLCertificateKeyFile
/etc/letsencrypt/live/update.infomir.com/privkey.pem
        SSLCertificateFile
/etc/letsencrypt/live/update.infomir.com/cert.pem
        SSLCertificateChainFile
/etc/letsencrypt/live/update.infomir.com/chain.pem

        DocumentRoot /var/www/update.infomir.com

        RewriteEngine On

        <Directory /var/www/update.infomir.com>
```

```
                Options -Indexes +FollowSymLinks +Includes
                AllowOverride All
                Order allow,deny
                Allow from All
        </Directory>

        LogLevel  warn
        ErrorLog  ${APACHE_LOG_DIR}/update.infomir.com_error.log
        CustomLog ${APACHE_LOG_DIR}/update.infomir.com_access.log
combined
        #CustomLog /dev/null combined

        ServerSignature Off
</VirtualHost>
```

Файл /etc/apache2/ports.conf приводим к виду:

ports.conf

```
# If you just change the port or add more ports here, you will likely
also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 88

<IfModule ssl_module>
        Listen 443
</IfModule>


<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Создать файл /etc/apache2/conf-available/certbot.conf

certbot.conf

```
Alias /.well-known /letsencrypt/.well-known
```

Включить конфигурацию

```
a2enconf certbot
```

Получение сертификатов

Используется метод **webroot**

Тестовый режим для отладки. Рекомендуется первую попытку выполнять в тестовом режиме для избежания блокировки со стороны Let'sEncrypt