**1. Cài đặt domain**

Bên Server:

- Sửa file /etc/hosts

127.0.0.1 domai.com

- Sửa file /etc/apache2/apache2.conf thêm vào dòng 70

ServerName [www.domain.com](http://www.domain.com/)

- sửa file /etc/apache2/conf-available/security.conf sửa ServerTokens

Từ On sang Prod

- Sửa file /etc/apache2/sites-available/domain.com.conf (tạo mới hoặc sửa file mặc định và đổi tên) và sửa như sau:

<VirtualHost \*:80>

ServerAdmin webmaster@localhost

ServerName domai.com

ServerAlias www.domain.com

DocumentRoot “Đường dẫn đến file web” (Có thể dùng đường dẫn mặc định là /var/www/html)

ErrorLog /home/domain.com/logs/error.log (Tạo đường dẫn hoặc dùng file mặc định trong /var/log)

CustomLog /home/domain.com/logs/access.log combined (Tạo đường dẫn hoặc dùng file mặc định trong /var/log)

<Directory “Đường dẫn đến file web”>

AllowOverride AuthConfig FileInfo Limit Options=IncludesNOEXEC,MultiViews,SymLinksIfOwnerMatch,FollowSymLinks,None

Options -ExecCGI -Includes +IncludesNOEXEC -Indexes

</Directory>

</VirtualHost>

- Có thể xóa file mặc định cũ của apache hoặc chỉnh sửa file đó hay tạo file mới và tắt file mặc định bằng câu lệnh sau:

#sudo a2dissite <file mặc định>

- Gõ các lệnh sau:

#sudo a2enmod rewrite

#sudo a2ensite domain.com.conf

#sudo service apache2 restart

Bên Client:

- Sửa file /etc/hosts

IP\_Server domai.com

- Tiến hành truy cập theo link: “http://domain.com”

Tài liệu tham khảo: <https://sanvu88.net/cai-dat-apache-tren-ubuntu.html?fbclid=IwAR19AiHpUSf6QbE2MlODezefw-S87KhulVN87-hoMPJBVP3h1h8NOkPcMEU>

**2. Cài đặt https**

- Tạo chứng chỉ SSL bằng các câu lệnh sau:

openssl genrsa -out domain.com.key 2048

openssl req -new -key domain.com.key -out domain.com.csr

openssl x509 -req -days 365 -in domain.com.csr -signkey domain.com.key -out domain.com.crt

- Copy các self-certificate vào đường dẫn /etc/ssl/certs và private bằng câu lệnh cp

- Kích hoạt https chúng ta cần

#sudo ufw allow ‘Apache Full’

#sudo ufw delete allow ‘Apache’

- Cấu hình thêm SSL và chỉnh sửa file /etc/apache2/sites-avalable/domain-ssl.conf (tạo mới hoặc chỉnh sửa file mặc định và đổi tên) và sửa như sau:

ServerName www.chimrio.com

DocumentRoot “Đường dẫn đến file web”

SSLEngine on

SSLProtocol all

SSLCertificateFile /etc/ssl/certs/domain.com.crt

SSLCertificateKeyFile /etc/ssl/private/domain.com.key

- Gõ tiếp các lệnh sau:

#sudo a2enmod ssl

#sudo a2enmod headers

#sudo a2ensite domain-ssl.conf

- Sau đó check cấu hình của file chúng ta đã tạo domain-ssl.conf hoặc chỉnh sửa file mặc định bằng câu lệnh sau:

#sudo apache2ctl configtest

- Chỉnh sửa file /etc/apache2/sites-available/domain.com.conf bằng cách Redirect từ http sang https. Câu lệnh:

….

Redirect "/" "<https://your_domain_or_IP/>"

….

- Tiến hành truy cập theo link: “https://domain.com”

Tài liệu tham khảo: <https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-18-04>

**3. Cài đặt Proxy (Dùng Nginx làm Reverse Proxy)**

**A. Reverse Proxy với http**

- Tạo file /etc/apt/sources.list.d/nginx.list với nội dung sau:

deb http://nginx.org/packages/mainline/O5/ bionic nginx

deb-src http://nginx.org/packages/mainline/O5/ bionic nginx

- Sau đó cập nhập direction và tải ứng dụng về bằng các câu lênh sau:

# wget <http://nginx.org/keys/nginx_signing.key>

# apt-key add nginx\_signing.key

# apt-get update

# apt-get install -y nginx

- Do apache và nginx đều chạy mặc định ở cổng 80 nên để không bị đè lên nhau thì chúng ta cần phải đổi cổng của apache bằng cách sửa các file sau:

/etc/apache2/port.conf từ port 80 sang port 8080,port 443 sang port 4433

/etc/apache2/sites-available/domain.com.conf từ port 80 sang port 8080

/etc/apache2/sites-available/domain-ssl.conf từ port 443 sang port 4433

- Chỉnh sửa file /etc/nginx/conf.d/default.conf

server {

….

server\_name domain.com;

….

location / {

….

proxy\_pass [http://domain.com:8080](http://domain.com:8080/);

}

….

}

- Restart lại 2 service: apache và nginx

- Tiến hành truy cập theo link: “http://domain.com”

**B. Reverse Proxy với https**

- Tạo chứng chỉ SSL bằng các câu lệnh sau:

openssl genrsa -out domain.com.key 2048

openssl req -new -key domain.com.key -out domain.com.csr

openssl x509 -req -days 365 -in domain.com.csr -signkey domain.com.key -out domain.com.crt

- Copy các self-certificate vào đường dẫn /etc/nginx bằng câu lệnh cp

- Sau đó tạo hoặc chỉnh sửa file ở đường dẫn /etc/nginx/conf.d và sửa file như sau:

server {

listen 80;

return 301 https://$host$request\_uri;

}

server {

listen 443;

server\_name chimrio.com;

ssl\_certificate /etc/nginx/chimrio.com.crt;

ssl\_certificate\_key /etc/nginx/chimrio.com.key;

ssl on;

ssl\_session\_cache builtin:1000 shared:SSL:10m;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;

ssl\_prefer\_server\_ciphers on;

….

location / {

….

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_set\_header X-Forwarded-Proto $scheme;

proxy\_pass http://chimrio.com:8080;

proxy\_read\_timeout 60;

}

….

}

- Tiến hành truy cập theo link: “https://domain.com”

Tài liệu tham khảo: <https://secure.vinahost.vn/ac/knowledgebase/257/Cu-hinh-SSL-cho-Nginx-lam-Reverse-Proxy.html?fbclid=IwAR0wnJxM7MCe51Ko1yQUUxXCob61CzZnzcSVJ4vmjFKO4SBFk27t3VZBY-w>