



05. Nginx 리버스 프록시 & TLS

```
# MQTT over TLS 포트인 8883번을 제외하고 모두 닫기
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

```
services:
  spring:
    ports:
      - "127.0.0.1:8080:8080"
  fastapi:
    ports:
      - "127.0.0.1:8000:8000"
  jenkins:
    ports:
      - "127.0.0.1:13570:13570"
  emqx:
    ports:
      - "127.0.0.1:18083:18083"
```

```
# /etc/nginx/conf.d/siseon.conf

upstream spring_app { server 127.0.0.1:8080; }
upstream fastapi_app { server 127.0.0.1:8000; }
upstream jenkins_app { server 127.0.0.1:13570; }
upstream emqx_app { server 127.0.0.1:18083; }

map $http_upgrade $connection_upgrade { default upgrade; "" close; }

server {
  listen 80;
```

```

server_name i13b101.p.ssafy.io;

location /.well-known/acme-challenge/ { root /var/www/certbot; }
location / { return 301 https://$host$request_uri; }
}

server {
    listen 443 ssl http2;
    server_name i13b101.p.ssafy.io;

    ssl_certificate /etc/letsencrypt/live/i13b101.p.ssafy.io/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/i13b101.p.ssafy.io/privkey.pem;

    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;

    location /siseon/ {
        proxy_http_version 1.1;
        proxy_read_timeout 60s;
        rewrite ^/siseon/?(.*)$ /$1 break;
        proxy_pass http://spring_app;
    }

    location /chat/ {
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_read_timeout 60s;
        rewrite ^/chat/?(.*)$ /$1 break;
        proxy_pass http://fastapi_app;
    }

    location /jenkins/ {
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;

```

```

    proxy_read_timeout 3600s;
    proxy_buffering off;
    client_max_body_size 100m;
    proxy_pass http://jenkins_app/jenkins/;
}

location /emqx/ {
    proxy_http_version 1.1;
    proxy_read_timeout 60s;
    rewrite ^/emqx/?(.*)$ /$1 break;
    proxy_pass http://emqx_app;
}
}

```

443 서버블록(SSL) 잠깐 비활성화

```
/etc/nginx/conf.d/siseon.conf
```

에서 **443 서버블록 전체**를 주석 처리하거나 삭제하고, **80 포트 블록만** 남겨둡니다.

```

sudo nginx -t
sudo systemctl reload nginx

```

certbot로 인증서 발급(nginx 플러그인 사용)

```

sudo apt-get install -y certbot python3-certbot-nginx
sudo certbot --nginx -d i13b101.p.ssafy.io --redirect

```

- 이 명령이 **인증서를 발급**하고, 자동으로 **443 서버블록과 ssl_certificate 경로를 conf**에 추가/갱신.
- 발급이 끝나면 `nginx -t && systemctl reload nginx`

갱신 리허설 (90일 만료 후 TLS)

```
sudo certbot renew --dry-run
```

