NginX 보안서버인증서 설치 가이드

보안서버인증서 구성파일 안내

Private.key	**개인키** (예스닉에 CSR 생성을 요청하신 경우에만 제공됩니다)
도메인명_crt.pem	**보안서버인증서** (CRT 파일)
ChainCA.crt	**체인인증서 번들** (ChinCA1+ChainCA2)
RootCA.crt	**루트인증서**
CSR.pem	**CSR** (인증서 신청 시 사용된 CSR 값)

예스닉 보안서버인증서는 기본적으로 PEM 형식으로 제공되고 있으며,
NginX 서버에 인증서를 설치하는 경우 인증서 번들파일과, 복호화된 개인키가 필요합니다.

먼저, 예스닉에서 제공된 인증서 구성파일을 NginX 서버 내 임의의 인증서 폴더에 업로드 하고,
cat 명령어로 보안서버인증서+체인인증서+루트인증서 번들파일을 생성합니다.

```
cat 도메인명_crt.pem ChainCA.crt RootCA.crt > 도메인명_bundle.pem
```

예스닉에 CSR 생성을 요청하셨다면, 아래 단계를 통해 비암호화 개인키로 변환합니다. -OpenSSL 이 설치된 서버에서 진행
(직접 CSR을 생성하여 암호화된 개인키를 보유하고 계신다면, 참고하여 비암호화 개인키로 변환 필요합니다.)

```
openssl rsa -des3 -in Private.key -out Private_pass.key
openssl rsa -in Private_pass.key -out Private_nopass.key
```

위 과정을 직접 진행하기 어려운 경우, 1:1 친절상담이나 메일로 NginX용 인증서 구성파일 제공을 요청하세요.
(직접 CSR을 생성하신 경우엔 인증서 비밀번호와 함께 개인키 파일을 첨부하여 요청해 주세요.)

NginX용 인증서 번들파일을 생성하고 복호화한 개인키로 변환을 완료했다면,
아래 내용을 참고하여 설정 파일을 수정합니다.

1. 서버 설정파일 수정 (일반적으로 NginX 홈/conf/**nginx.conf**)
   아래 구문을 찾아 인증서 설치포트, 파일경로 등 내용을 수정합니다.

   (1) NginX 1.14 이하 버전

```
server{
listen 443;
server_name (인증서 적용할 도메인명)
ssl_certificate_key /(인증서 파일 업로드 경로)/Private_nopass.key;
ssl_certificate /(인증서 파일 업로드 경로)/도메인명_bundle.pem;
ssl_protocols TLSv1.2;
ssl on; ssl_prefer_server_ciphers on;    (서버 환경에 따라 제공되는 기본 값 참고하여 적용)
}
```

   (2) NginX 1.15 이상 버전

```
server{
listen 443 ssl;
server_name (인증서 적용할 도메인명)
ssl_certificate_key /(인증서 파일 업로드 경로)/Private_nopass.key;
ssl_certificate /(인증서 파일 업로드 경로)/도메인명_bundle.pem;
ssl_protocols TLSv1.2;
}
```

2. 수정을 완료하면 NginX 웹서버를 재시작하여 적용되었는지 확인합니다.

적용 과정에 오류가 있는 경우 오류내용, 로그, 스크린샷 등을 첨부하여 **1:1 친절상담**이나 **메일**로 문의해 주세요.