一．Nginx （单向配置仅在服务器端）

a) 先安装 openssl 和 openssl-devel
   i. 查看是否安装 openssl version （rpm -qa|grep ssl）
   ii. 查看路径 which openssl
b) 编译 nginx 时使用 --with-http_ssl_module 就可以支持 SSL 了
   i. 查看是否 nginx 安装/usr/sbin/nginx -V ，which nginx（查看命令路径）
c) 获取服务器证书
   i. 证书由第三提供（也可以自主生成 KEY，但是浏览器会认为不安全，商用时不可取）
   ii. 请把******.cer 和******.key 这两个文件保存到同一个目录下，
   iii. 例如放到/etc/ssl/crt/目录下。（**表示文件名）
d) 修改 nginx 配置文件
   i. 查看路径 ps aux | grep nginx （/etc/nainx/nginx.conf）
   ii. ****** nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
   iii. 修改配置（备份之前配置，修改网站 server 配置）

```
# HTTPS server
    server {
        listen          443;
        server_name     localhost;
        ssi on;
        ssi_silent_errors on;
        ssi_types text/shtml;

        ssl                     on;     # listen 443 ssl 等效  listen 443  ssl on
        ssl_certificate         /etc/ssl/crt/****.crt;
        ssl_certificate_key     /etc/ssl/crt/****.key;
        ssl_client_certificate  /etc/ssl/crt/****.crt;

        ssl_session_timeout  5m;

        ssl_protocols  SSLv2 SSLv3 TLSv1;
        ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
        ssl_prefer_server_ciphers   on;

    }
```

e) 检查配置文件
   i. /usr/sbin/nginx -t
   ii. 启动 nginx nginx 的 sbin 目录下 运行./nginx
   iii. ps -ef|grep nginx 后显示 （重启命令：./nginx -s reload）

f) 遇到问题
   i. listen 443 ssl; 等效于 listen 443; ssl on;
   ii. 启动 nginx ,等待客户连接，如果此时连接服务器，将提示 400 Bad request certification 的错误，故还需要生成客户端证书。（说明你开启客户端验证 ssl_verify_client on; #开户客户端证书验证 ）

g) 兼容 HTTP （属于域名跳转知识，百度 http 跳转到 https 即可）

i. 第一种完整配置

```
server {

        listen          443;
        listen          80;     #用户习惯用 http 访问，加上 80，后面通过 497 状态码让它自动跳到 443 端口
        server_name     ssl.bluepay.asia;   #根据自身而定

        root    /usr/share/nginx/best;
        index   index.php index.html index.htm;

        ssi on;
        ssi_silent_errors on;
        ssi_types text/shtml;

        ssl                             on;
        ssl_certificate             /etc/ssl/certs/bluepay.cer;
        ssl_certificate_key         /etc/ssl/certs/bluepay.key;
        ssl_client_certificate    /etc/ssl/certs/bluepay.cer;

        ssl_session_timeout    5m;
        ssl_verify_depth 1;

        ssl_protocols    SSLv2 SSLv3 TLSv1;
        ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
        ssl_prefer_server_ciphers     on;
        error_page 497 "https://$host$uri?$args"; #这是跳转 Http 请求到 Https

        if (!-e $request_filename) {
                rewrite ^/(.*\.(js|ico|gif|jpg|png|css|bmp|wsdl|pdf|xls)$) /public/$1 last;
                rewrite ^/(.*) /index.php?$1 last;

        }

        if ($http_user_agent ~ ApacheBench|webBench|Java/|http_load|must-revalidate|wget) {
                return 403;
        }

        error_page    404                   /404.html;
        location = /404.html {
                root    /usr/share/nginx/html;
        }

        error_page     500 502 503 504    /50x.html;
```

```
        location = /50x.html {
            root   /usr/share/nginx/html;
        }

        location ~ \.php$ {
            root           /usr/share/nginx/best;

            fastcgi_buffers 2 256k;
            fastcgi_buffer_size 128k;
            fastcgi_busy_buffers_size  256k;
            fastcgi_temp_file_write_size  256k;

            fastcgi_pass   127.0.0.1:9000;
            fastcgi_index  index.php;
            fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
            include        fastcgi_params;
        }
    }
```

ii. 第二种方法

```
server {

        listen          443;

        server_name  ssl.bluepay.asia;


        root   /usr/share/nginx/best;
        index  index.php index.html index.htm;

        ssi on;
        ssi_silent_errors on;
        ssi_types text/shtml;

        ssl                     on;
        ssl_certificate         /etc/ssl/certs/bluepay.cer;
        ssl_certificate_key     /etc/ssl/certs/bluepay.key;
        ssl_client_certificate  /etc/ssl/certs/bluepay.cer;

        ssl_session_timeout  5m;
        ssl_verify_depth 1;

        ssl_protocols  SSLv2 SSLv3 TLSv1;
        ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
```

```
        ssl_prefer_server_ciphers      on;

        if (!-e $request_filename) {
            rewrite ^/(.*\.(js|ico|gif|jpg|png|css|bmp|wsdl|pdf|xls)$) /public/$1 last;
            rewrite ^/(.*) /index.php?$1 last;

        }

        if ($http_user_agent ~ ApacheBench|webBench|Java/|http_load|must-revalidate|wget) {
            return 403;
        }

        error_page    404                    /404.html;
        location = /404.html {
            root      /usr/share/nginx/html;
        }

        error_page      500 502 503 504    /50x.html;
        location = /50x.html {
            root      /usr/share/nginx/html;
        }

        location ~ \.php$ {
            root                /usr/share/nginx/best;

            fastcgi_buffers 2 256k;
            fastcgi_buffer_size 128k;
            fastcgi_busy_buffers_size    256k;
            fastcgi_temp_file_write_size    256k;

            fastcgi_pass      127.0.0.1:9000;
            fastcgi_index    index.php;
            fastcgi_param    SCRIPT_FILENAME    $document_root$fastcgi_script_name;
            include             fastcgi_params;
        }
    }

    server {
        listen 80;
        server_name ssl.bluepay.asia;
        rewrite ^/(.*) https://$server_name$1 permanent;       #跳转到 Https
    }
```

iii. 资源找不到的小技巧（保证所有的请求都是 https 协议，包括图片，资源等）

ln -s /mnt/resource/ /usr/share/nginx/best/   #/usr/share/nginx/best/APP 根目录/mnt/resource/资源目录

二．Apache

a) 检查是否已安装 openssl
   i. 查看安装路径(which openssl)
   ii. 查看版本 openssl version
   iii. 查看安装包 rpm -qa|grep -i openssl
   iv. yum install openssl-devel
b) 查看 apache 已加载的模块
   i. /Web/apps/apache2/bin/apachectl -t -D DUMP_MODULES
c) 模块介绍
   i. Apache HTTP 服务器的 mod_ssl 模块提供了对使用安全套接层(Secure Sockets Layer)和传输层安全(Transport Layer Security)协议的 OpenSSL 库的接口。此模块和本文都是基于 Ralf S. Engelschall 的 mod_ssl 项目。
   ii. apache2 中 mod_ssl 不是单独的模块，而是放在 apache 发行包里面了，默认是不启用，启用即可

三．Apache 安装 SSL 证书需要三个配置文件

a) 由第三方安全机构提供（bluepay.cer bluepay.key ca.cer）
b) apache 生成密钥和证书（建立自己的 CA [略]）

四．修改 apache 下的 httpd.conf 文件

a) 打开 apache 安装目录下 conf 目录中的 httpd.conf 文件，找到
   i. #LoadModule ssl_module modules/mod_ssl.so
   ii. #Include conf/extra/httpd-ssl.conf
   iii. 删除行首的配置语句注释符号“#”，保存退出

五．修改 apache 下 httpd-ssl 文件

a) SSLCertificateFile "/Web/apps/apache2/etc/ssl/bluepay.cer"
   （将服务器证书公钥 bluepay.cer 配置到对应的路径）
b) SSLCertificateKeyFile "/Web/apps/apache2/etc/ssl/bluepay.key"
   （将服务器证书私钥 bluepay.cer 配置到对应的路径）
c) SSLCertificateChainFile "/Web/apps/apache2/etc/ssl/ca.cer"
   （删除行首的“#”号注释符，并将中级 CA 证书(ca.cer)配置到该路径下）
d) 报错 SSLSessionCache: 'shmcb' session cache not supported (known names:). Maybe you need to load the appropriate socache module (mod_socache_shmcb?).
   i. 开启 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

六．保存退出，并重启 Apache。重启方式：

a) 进入 Apache 安装目录下的 bin 目录，运行如下命令
   i. ./apachectl -k stop
   ii. ./apachectl -k start

七．通过 https 方式访问您的站点，测试站点证书的安装配置

a) 在地址：https://weiphp.bluepay.asia

八．为了习惯用户的操作，需要在 apache 环境下设置 url 重定向规则，使网站页面的 http 访问都自动转到 https

访问

a) 打开 url 重定向支持
   i. 打开 httpd.conf，找到 #LoadModule rewrite_module modules/mod_rewrite.so 去掉#号
   ii. <Directory "/Web/apps/apache2//htdocs">节点里面 将 AllowOverride None 改为 AllowOverride All
b) 设置重定向规则
   i. 在网站根目录下创建.htaccess

```
1. <IfModule mod_rewrite.c>
2.     RewriteEngine on
3.     RewriteBase /
4.     RewriteCond %{SERVER_PORT} !^443$
5.     RewriteRule ^.*$ https://%{SERVER_NAME}%{REQUEST_URI} [L,R]
6. </IfModule>
```

九．解决请求资源 http 方案

a) 在 HTTPS 的网站下，如果要访问 HTTP 资源，那么一般浏览器会弹出窗口询问用户是否允许加载不安全内容，为了避免出现这样干扰用户的情况，所有网页下请求的资源都都必须是 HTTPS 资源，索引使用绝对路径。
b) 判断 PHP 判断协议是否为 HTTPS （根据网站修改对应的 ROOT）

```
function is_HTTPS(){
    if(!isset($_SERVER['HTTPS']))    return FALSE;
    if($_SERVER['HTTPS'] === 1){    //Apache
        return TRUE;
    }elseif($_SERVER['HTTPS'] === 'on'){ //IIS
        return TRUE;
    }elseif($_SERVER['SERVER_PORT'] == 443){ //其他
        return TRUE;
    }
    return FALSE;
}
```