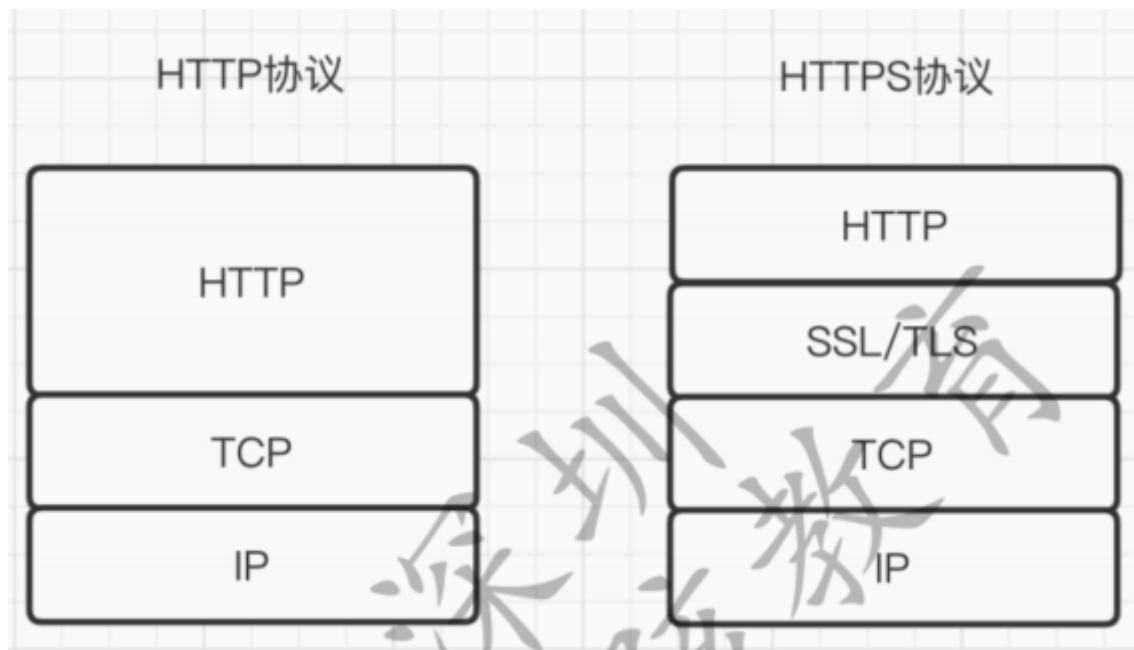


第1章 HTTPS介绍

1.什么是HTTPS协议

- 1 **HTTPS**协议不是一个独立的协议，而是**HTTP+SSL**(安全传输层协议)或**HTTP+TLS**(安全套接层)协议的组合。
- 2 合。
- 3 简单来说就是使用**SSL**或**TLS**协议对**HTTP**协议发送的文本进行加密。

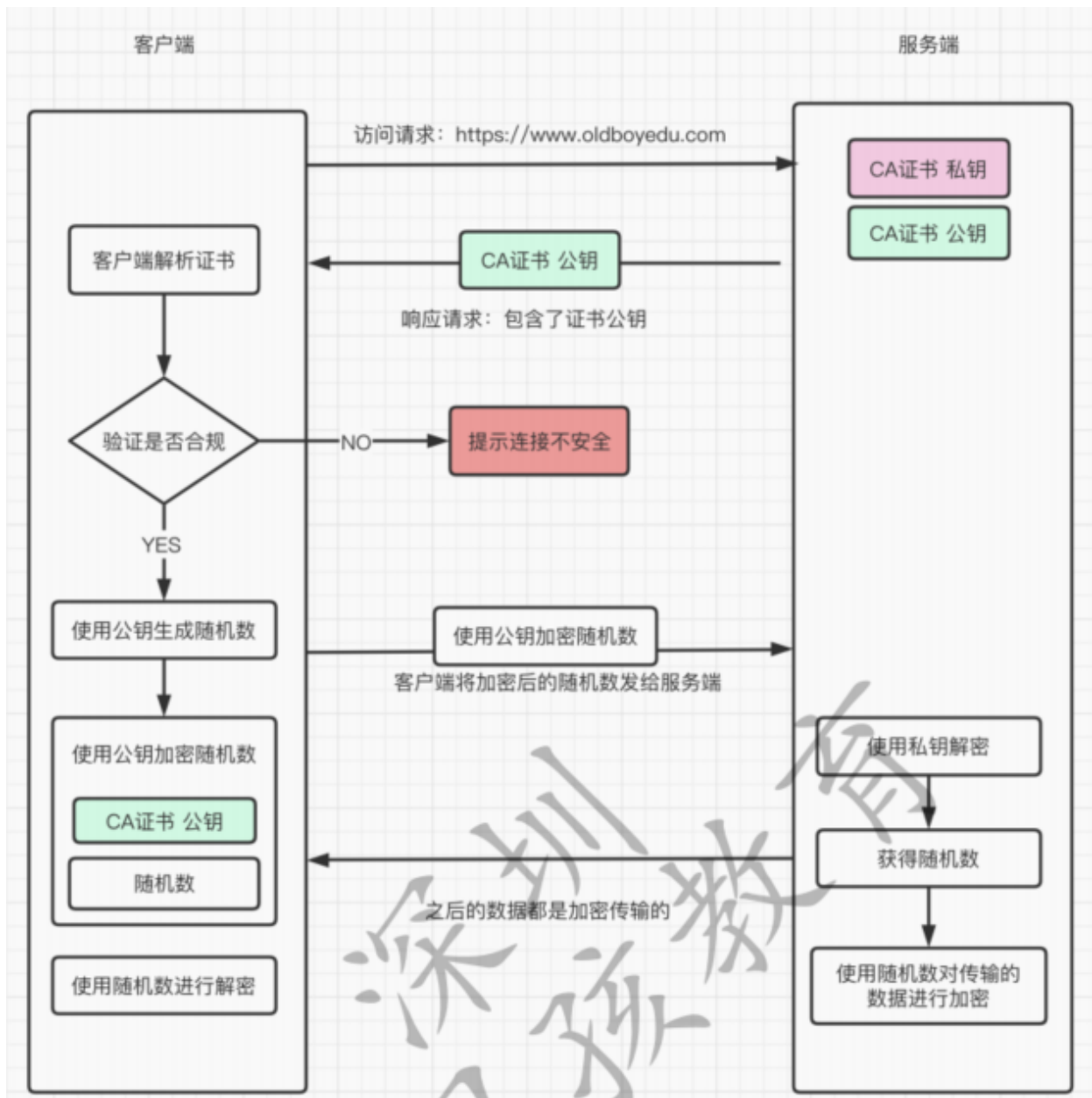


2.为什么需要HTTPS

为什么需要使用HTTPS, 因为HTTP不安全。当我们使用http网站时，经常会遇到包遭到劫持和篡改，如果采用https协议，那么数据在传输过程中是加密的，所以黑客无法窃取或者篡改数据报文信息。

3.HTTP加密流程

- 1.服务端配置有一对数字证书，包含了私钥和公钥，也称为**CA**证书，**CA**证书有专门的颁发机构，也可以自己创建，但是自己创建的证书会被浏览器认为不合法。
- 2.客户端发起**HTTPS**请求,请求的端口是**443**
- 3.服务端接收到请求后会自动将自己的**CA**证书分发给客户端
- 4.客户端收到证书后浏览器会做验证，如果是合法的就会显示**https**图标，如果是不合法的，则会提示连接不安全
- 5.客户端如果证书通过验证，就会生成一个随机数，然后使用公钥对随机数进行加密
- 6.然后客户端会将随机数发给服务端
- 7.服务端收到后使用私钥解密随机数，以后通讯就会使用随机数进行数据加密了



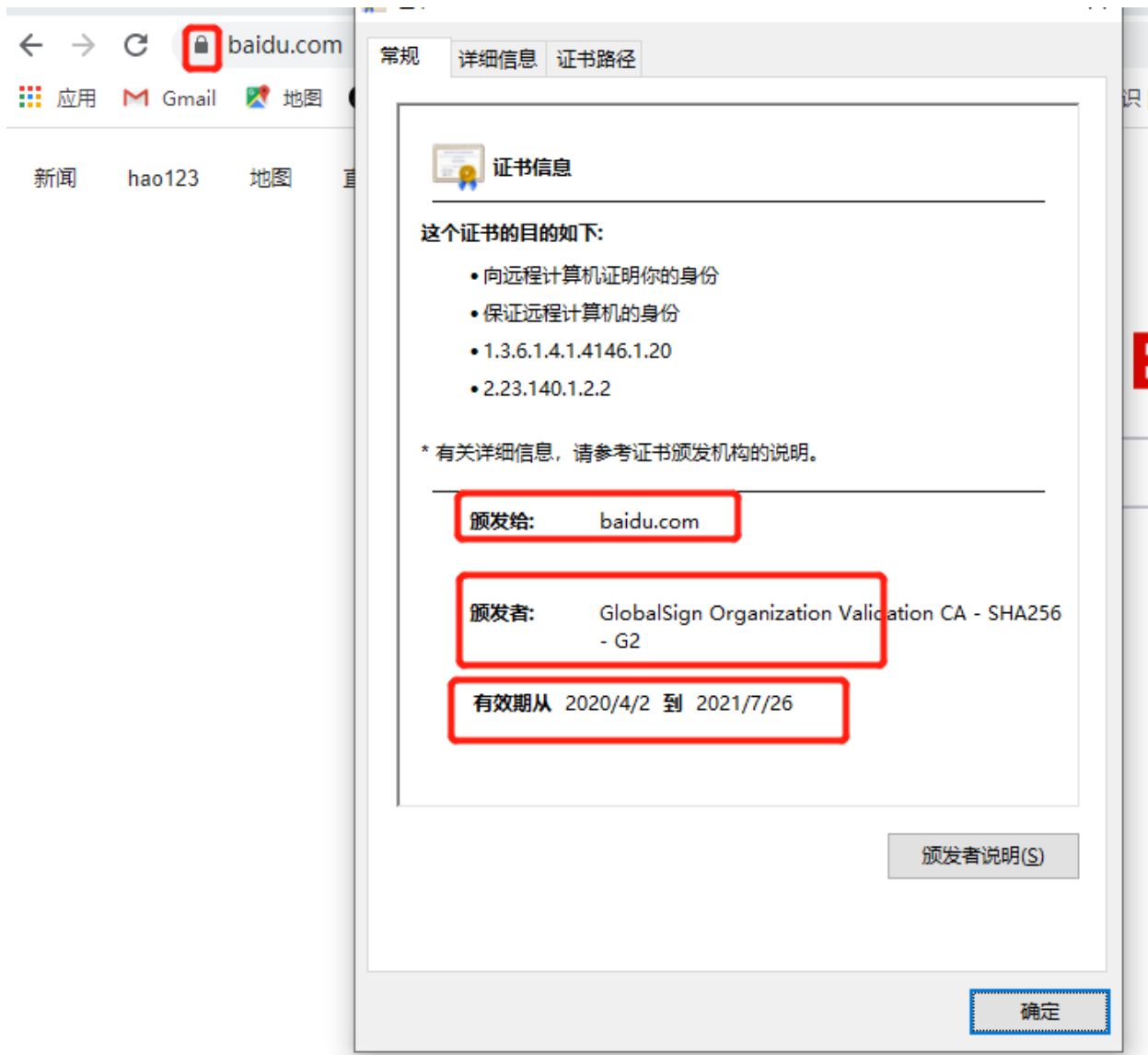
第2章 HTTPS购买以及注意事项

1. 购买平台

各大云厂商

2. 国际常见的证书颁发机构

- 1 GlobalSign
- 2 DigiCert
- 3 GeoTrust



3.证书类型

- 1 OV
- 2 EV
- 3 DV
- 4 免费

4.域名类型

- 1 单域名证书 www.mysun.com
- 2 多域名证书 www.mysun.com bbs.mysun.com blog.mysun.com
- 3 通配符域名 *.mysun.com

5.域名证书购买注意

- 1 1. 一个通配符证书只支持2级域名
- 2 2. 域名证书最多只能买3年，不持续续费，到期只能买新的
- 3 3. 域名证书到期后浏览器会提示不安全警告
- 4 4. 微信小程序必须要求配置https，不然审核不通过

6.工作中选择域名的过程

- 1 先收集好所有的域名
- 2 过滤分析一共有几种类型的域名
- 3 *.www.mysun.com
- 4 *.mysun.com

7.如何监控域名过期时间

```
1 out_time=$(echo | openssl s_client -connect www.oldboyedu.com:44
3 2>/dev/null
2 | openssl x509 -noout -dates|awk -F=" ' /notAfter/{print $2}')
3 out_time_unix=$(date +%s -d "${out_time}")
4 today=$(date +%s)
5 let out_day=($out_time_unix-$today)/86400
6 echo $out_day
```

第3章 简单nginx配置https

1.检查Nginx是否有SSL模块

```
1 nginx -V
2 --with-http_ssl_module
```

2.创建证书目录并生成证书

```
1 mkdir /etc/nginx/ssl_key
2 cd /etc/nginx/ssl_key
3 openssl genrsa -idea -out server.key 2048
4 输入密码:1234
5 确认输入密码:1234
```

```
1 openssl req -days 36500 -x509 -sha256 -nodes -newkey rsa:2048 -k
eyout server.key -out server.crt
2 -----
3 Country Name (2 letter code) [XX]:SZ
4 State or Province Name (full name) []:SZ
5 Locality Name (eg, city) [Default City]:SZ
6 Organization Name (eg, company) [Default Company Ltd]:SZ
7 Organizational Unit Name (eg, section) []:SZ
```

```
8 Common Name (eg, your name or your server's hostname) []:SZ
9 Email Address []:
```

3.确认生成了证书文件

```
1 [root@web-7 /etc/nginx/ssl_key]# ll
2 total 8
3 -rw-r--r-- 1 root root 1253 May 15 10:18 server.crt
4 -rw-r--r-- 1 root root 1704 May 15 10:18 server.key
```

4.配置nginx配置文件

```
1 cat >/etc/nginx/conf.d/ssl.conf <<EOF
2 server {
3     listen 443 ssl;
4     server_name www.oldboyedu.com;
5     ssl_certificate ssl_key/server.crt;
6     ssl_certificate_key ssl_key/server.key;
7
8     location / {
9         root /code/www;
10        index index.html;
11    }
12 }
13 EOF
```

5.检查并重启nginx

```
1 nginx -t
2 systemctl restart nginx
```

6.访问测试

```
1 cat >/etc/nginx/conf.d/ssl.conf <<EOF
2 server {
3     listen 80;
4     server_name www.oldboyedu.com;
5     rewrite ^(.*) https://$server_name$1 redirect;
6 }
7
```

```
8 server {
9     listen 443 ssl;
10    server_name www.oldboyedu.com;
11    ssl_certificate ssl_key/server.crt;
12    ssl_certificate_key ssl_key/server.key;
13    location / {
14        root /code/www;
15        index index.html;
16    }
17 }
18 EOF
```

第4章 强制http跳转到https

配置nginx配置文件

```
1 cat >/etc/nginx/conf.d/ssl.conf <<EOF
2 server {
3     listen 80;
4     server_name www.oldboyedu.com;
5     rewrite ^(.*) https://$server_name$1 redirect;
6 }
7
8 server {
9     listen 443 ssl;
10    server_name www.oldboyedu.com;
11    ssl_certificate ssl_key/server.crt;
12    ssl_certificate_key ssl_key/server.key;
13    location / {
14        root /code/www;
15        index index.html;
16    }
17 }
18 EOF
```

第5章 Nginx集群配置https

1.复制已经创建好的证书到其他的web服务器

```
1 cd /etc/nginx/  
2 scp -r ssl_key 10.0.0.8:/etc/nginx/  
3 scp -r conf.d/ssl.conf 10.0.0.8:/etc/nginx/conf.d/  
4
```

2.复制已经创建好的证书到lb服务器

```
1 cd /etc/nginx/  
2 scp -r ssl_key 10.0.0.5:/etc/nginx/
```

3.第一种情况:

lb服务器http强制跳转https

lb服务器配置:

```
1 [root@lb-5 /etc/nginx/conf.d]# cat ssl.conf  
2 upstream ssl_pools {  
3     server 172.16.1.7:443;  
4     server 172.16.1.8:443;  
5 }  
6  
7 server {  
8     listen 80;  
9     server_name ssl.oldboy.com ;  
10    rewrite ^(.*) https://$server_name$1 redirect;  
11 }  
12  
13 server {  
14     listen 443 ssl;  
15     server_name ssl.oldboy.com;  
16     ssl_certificate ssl_key/server.crt;  
17     ssl_certificate_key ssl_key/server.key;  
18     location / {  
19         proxy_pass https://ssl_pools;  
20         include proxy_params;  
21     }
```

web服务器配置:

```
1 [root@web-8 /etc/nginx/conf.d]# cat ssl.conf
2 server {
3     listen 443 ssl;
4     server_name ssl.oldboy.com;
5     ssl_certificate ssl_key/server.crt;
6     ssl_certificate_key ssl_key/server.key;
7     location / {
8         root /code;
9         index index.html;
10    }
11 }
```

4.第二种情况:

lb服务器负责https加解密, 后端web服务器还是80端口

1.lb服务器配置

```
1 [root@lb-5 ~]# cat /etc/nginx/conf.d/ssl.conf
2 upstream ssl_pools {
3     server 172.16.1.7;
4     server 172.16.1.8;
5 }
6
7 server {
8     listen 80;
9     server_name ssl.oldboy.com ;
10    rewrite ^(.*) https://$server_name$1 redirect;
11 }
12
13 server {
14     listen 443 ssl;
15     server_name ssl.oldboy.com;
16     ssl_certificate ssl_key/server.crt;
17     ssl_certificate_key ssl_key/server.key;
```



```
18 location / {
19     proxy_pass http://ssl_pools;
20     include proxy_params;
21 }
22 }
```

2.web服务器配置

```
1 [root@web-7 /etc/nginx/conf.d]# cat ssl.conf
2 server {
3     listen 80;
4     server_name ssl.oldboy.com;
5     location / {
6         root /code;
7         index index.html;
8     }
9 }
```

第6章 wordpress配置https

1.lb服务器配置

配置nginx配置文件

```
1 [root@lb-5 ~]# cat /etc/nginx/conf.d/ssl.conf
2 upstream ssl_pools {
3     server 172.16.1.7;
4     server 172.16.1.8;
5 }
6
7 server {
8     listen 80;
9     server_name blog.mysun.com;
10    rewrite ^(.*) https://$server_name$1 redirect;
11 }
12
13 server {
```

```
14 listen 443 ssl;
15 server_name blog.mysun.com;
16 ssl_certificate ssl_key/server.crt;
17 ssl_certificate_key ssl_key/server.key;
18 location / {
19     proxy_pass http://ssl_pools;
20     include proxy_params;
21 }
22 }
```

2.web服务器配置

2台web服务器都需要配置

配置fastcgi的https相关参数

```
1 echo "fastcgi_param HTTPS on;" >> /etc/nginx/fastcgi_params
```

3.web服务器nginx配置

```
1 [root@web-7 ~]# cat /etc/nginx/conf.d/blog.conf
2 server {
3     listen 80;
4     server_name blog.mysun.com;
5     root /code/wordpress;
6     index index.php index.html;
7
8     location ~ /\.php$ {
9         root /code/wordpress;
10        fastcgi_pass 127.0.0.1:9000;
11        fastcgi_index index.php;
12        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
13        include fastcgi_params;
14    }
15 }
```

4.检查语法重启nginx

```
1 nginx -t
2 systemctl restart nginx
```

第7章 阿里云配置HTTPS

阿里云https申请流程

阿里云的https证书可以申请个人免费版

【公告】4.1-4.31，2年限7折起，7.5折封顶（新老同享）：首购网站HTTPS代理7折，飞天会员全场OV证书8折

商品类型

云盾证书服务

云盾证书多年服务

网站代理https

云盾证书服务类型

云盾SSL证书

DV单域名证书【免费试用】

原DigiCert 免费单域名证书，建议用于测试、个人试用等场景，org、ip等特殊域名存在无法申请的情况。正式环境建议使用付费证书。
每个实名主体个人/企业，一个自然年内可以领取一次数量为20的云盾单域名试用证书，如需更多云盾单域名试用证书需要额外付费购买。
云盾单域名试用证书在自然年结束时，会自动清除未签发的数量（每个自然年12月31日24:00）
云盾单域名试用证书不支持续费补发时间

证书个数

20

40

50

100

每个实名主体个人/企业，一个自然年内可以领取一次数量为20的免费证书资源包
免费资源包到自然年结束时，会自动清除未签发的数量（每个自然年12月31日24:00）
证书个数是指可以签发证书的数量
例如，证书个数为1，将签发一张有效期为1年的证书
证书个数支持同时签发多张证书或者1张证书托管多年的服务