cd ../

使用Squid搭建HTTPS代理服务器

2015-02-25

由于经常去的一些国外网站如Google、Blogspot、Wordpress被“出现了技术问题”，访问不了，于是我在自己的DigitalOcean云主机上搭建了一个Squid代理服务器用于科学上网。Squid支持HTTP、HTTPS代理，因此能够满足日常访问国外某些网站的需求。然而如果直接使用HTTP连接Squid是明文传输的，在第一次使用时，会马上“出现技术问题”，因此需要使用stunnel加密代理通道。具体配置步骤如下，云主机的Linux发行版是Ubuntu 14.10 x32，如果你使用的是其他发行版，包管理与配置文件路径会略有不同。

安装必要的软件

安装apache2-utils用于HTTP认证文件的生成，

```
apt-get install apache2-utils -y
```

安装Squid，

```
apt-get install squid3 -y
```

安装stunnel，

```
apt-get install stunnel4 -y
```

配置Squid

生成HTTP认证文件，输入对应的密码。这个认证文件用于之后HTTP代理的认证登录，如果不需要登录认证，可以略过。

```
htpasswd -c /etc/squid3/squid.passwd <登录用户名>
```

修改Squid默认配置，配置文件位于 /etc/squid3/squid.conf 。

1. 修改监听地址与端口号

找到 TAG: http_port 注释，把其下方的

```
# Squid normally listens to port 3128
http_port 3128
```

中 http_port 修改为 127.0.0.1:3128 ，使得Squid只能被本地（127.0.0.1）访问。此处可以修改为监听其他端口号。

2. 修改访问权限与HTTP认证（可选）

若不需要添加HTTP认证，只需将 http_access deny all 修改为 http_access allow all 即可，无需下列的操作。

使用如下命令生成认证文件，

```
htpasswd -c /etc/squid3/squid.passwd <登录用户名>
```

再次打开Squid配置文件 /etc/squid3/squid.conf ， 找到 TAG: auth_param 注释，在其下方添加，

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/squic
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

找到 TAG: acl ， 在其下方添加，

```
acl ncsa_users proxy_auth REQUIRED
```

找到 TAG: http_access ， 在其下方添加，使得只允许经过认证的用户访问，

```
http_access deny !ncsa_users
http_access allow ncsa_users
```

3. 重启Squid

```
service squid3 restart
```

配置stunnel

接下来，我们需要在Squid上添加一层加密。

生成公钥和私钥

生成私钥（privatekey.pem）：

```
openssl genrsa -out privatekey.pem 2048
```

生成公钥（publickey.pem）：

```
openssl req -new -x509 -key privatekey.pem -out publickey.pem -days 1095
```

（需要注意的是， Common Name 需要与服务器的IP或者主机名一致）

合并：

```
cat privatekey.pem publickey.pem >> /etc/stunnel/stunnel.pem
```

修改stunnel配置

新建一个配置文件 /etc/stunnel/stunnel.conf ， 输入如下内容

```
client = no
[squid]
```

```
accept = 4128
connect = 127.0.0.1:3128
cert = /etc/stunnel/stunnel.pem
```

配置中指定了stunnel所暴露的HTTPS代理端口为4128，可以修改为其他的值。

修改 /etc/default/stunnel4 配置文件中 ENABLED 值为1。

```
ENABLED=1
```

重启stunnel

```
service stunnel4 restart
```

至此，服务器端已配置完成了。

本地浏览器配置

添加证书到受信任的根证书颁发机构列表中

以Windows下Chrome浏览器为例，将服务器上的公钥 publickey.pem 下载至本地，重命名至 publickey.crt，在Chrome中依次点击 “设置” - “显示高级设置” - “HTTP/SSL” - “管理证书”，在“受信任的根证书颁发机构”选项卡中“导入”这个crt证书就完成了。

代理客户端配置

将本地的代理客户端指向 https://<你的服务器IP或主机名>:4128，这里的IP或主机名和生成公钥时的 Common Name 一致，端口为stunnel的端口。如果有配置HTTP认证的话，需要在客户端中配置对应的用户名和密码。如果没有HTTP客户端的话，推荐使用Chrome的插件Proxy SwitchyOmega（使用教程可以参考Github 上的Wiki）。

评论 在线社区 隐私政策 1 登录

Favorite 15 推文 分享 评分最高

加入讨论…

通过以下方式登录

或注册一个 DISQUS 帐号 ?

姓名

David Yin • 6 年前

http://www.yinhaomin.com/

回复 • 分享 ›

Jay C • 6 年前

你好,我想问下,如果我有自己的ssl证书,分别是.crt和.key 各一份,生成公钥和私钥的步骤上需要怎样操作呢?感谢

回复 • 分享 ›

季文昊 主持 Jay C • 6 年前

crt和pem文件格式通常是一样的，具体可以参考StackOverflow上的这个问题(http://stackoverflow.com/a/... PRIVATE KEY”开头，公钥以“BEGIN CERTIFICATE”开头。

回复 • 分享 ›

luckypoem • 6 年前

hi.

你这个博客是用什么建站程序搭建的?

回复 • 分享 ›

季文昊 主持 luckypoem • 6 年前

github pages的jekyll，https://github.com/predator...

回复 • 分享 ›

唐合 • 7 年前

您好，请问按照这种设置好了之后，能在苹果手机上用吗?

回复 • 分享 ›

季文昊 主持 唐合 • 7 年前

iOS似乎不支持https代理，但是如果squid去掉ssl加密的话会造成很快被墙发现。所以目前在手机上还是只能靠VPN。

回复 • 分享 ›