利用VPS和Shadowsocks实现翻墙

# 什么是GFW

GFW是Great Firewalls的缩写，是一种防火墙技术，目的是对中国的互联网进行全面的控制，主要表现为防止国内的网络访问一些政府不想你访问的资源，比如Google，YouTube，或者是屏蔽一些敏感的内容。实现GFW最基本的方式有两种，一是直接将它不想让你访的资源的IP地址加入黑名单，直接屏蔽所有想访问这些IP的网络请求，二是扫描网络传输的内容，检索到敏感内容再中断传输。

# 翻墙的技术实现

翻墙就是要越过GFW的封锁，自由的浏览互联网资源，要实现这个目的，我们就要解决上面的两个问题。第一，IP封锁，解决这个问题一般是通过网络代理来实现，你需要一台可以自由访问互联网的服务器，这些服务器一般都在国外，它访问互联万是不需要通过GFW的。这个服务器负责代理你的网络请求，替你访问网络资源，再将它获取到的内容传输给你。而你可以访问这个服务器，因为这个服务器的IP在GFW的黑名单外，你是可以访问到的。在这个服务器上部署代理服务就可以作为代理服务器了。

然后解决第二个问题，就是GFW不光会屏蔽IP，也会对网络内容进行扫描，一旦它扫描到敏感的内容，它也会中断网络传输。这个时候就需要加密这些信息，GFW无法知道网络传输的内容，也就没办法屏蔽了。GFW只知道你在和一台国外的服务器进行网络通信，这个服务器的IP不在黑名单，内容又进行了加密，GFW无法知道网络通信的内容，也就不能进行屏蔽了，它总不能屏蔽一切对外网络通信吧。能提供代理和加密的协议很多，以前最常用的协议是VPN，但是由于VPN协议处理过的数据的特征已经被发现，所以VPN可以很容易的被GFW屏蔽，GFW可以不解密网络传输的内容，发现内容符合VPN的特征，知道你在使用VPN，直接屏蔽，不管你到底用VPN干什么，宁可错杀一千，不能放过一个，特别是一些敏感时刻。现在最流行的协议是Shadowsocks，一个由国人开发的专门用于翻墙的协议，由于这个协议专门用于翻墙，并不需要那么严格的加密，只需要让GFW不能快速破解内容，性能比较好，而且特征目前还没被发现，所以比较安全（也许只是现在使用Shadowsocks的人还不够多吧）。

VPN不是专门用来翻墙的，它的其他内容就不在这里介绍的。

这个教程就是用VPS作为代理服务器，Shadowsocks作为代理协议的翻墙方法。

# 什么是VPS？

VPS是Virtual Private Server的首字母缩写，是一种通过虚拟化或容器技术将服务器分割成多个虚拟的专享服务器的技术。可以简单的理解为一台服务器，你拥有独立的操作系统，公网IP，磁盘空间，只是不是直接对应到相应的物理硬件上的。

由于提供给你的资源是虚拟化过后的资源，所以VPS提供商可能为了商业利益超卖，打个比方一台8核心的服务器被虚拟化成N台双核心的VPS，这个N可以是4/8/或者16，虚拟化的越多，每个VPS的可以实际使用的性能就越弱，其他的资源也是同样。

这里提供我使用的VPS的网址：<https://bwh1.net/index.php>

非官方中文网站：<https://www.bandwagonhost.net/>

Shadowsocks的网址：<https://shadowsocks.org/en/index.html>

Shadowsocks在GitHub上的地址：<https://github.com/shadowsocks>

Shadowsocks所需的教程和软件都可以在这两个地方找到

首先你要购买一个VPS服务，选一个你喜欢的VPS提供商，买一个你需要规格的VPS服务就可以了。具体内容看演示。

买了VPS服务接下来来就是在VPS上部署代理服务了，具体步骤如下：

1. 登录VPS，使用SSH登录就可以了，macOS或者Linux可以直接使用终端使用SSH命令登录。Windows上可以使用PuTTY。
2. 在VPS上安装Shadowsocks服务端软件，Shadowsocks最初是使用Python实现的，我用的也是Python版，使用pip安装。
3. 配置启动Shadowsocks服务。
4. 在你的电脑上下载Shadowsocks客户端，按照你在Shadowsocks服务端配置的参数设置Shadowsocks客户端。

这样你的电脑就可以翻墙了。

SSH登录需要的信息，远程主机的IP和SSH服务的端口，VPS上运行的操作系统（这里特指Linux）的用户名和密码，这些都可以在你购买VPS的服务提供商站点的管理系统获取。

macOS和Linux使用的SSH命令为：

ssh username@hostname -p port

然后根据提示输入密码即可

登录远程主机后你可以先升级一下系统

Ubuntu：apt update; apt upgrade

Centos: yum update; yum upgrade

后面的操作以Centos操作系统为例

升级系统后就是给Python安装pip包管理软件

curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py

python get-pip.py

安装好pip后就是安装Shadowsocks服务端了

pip install git+https://github.com/shadowsocks/shadowsocks.git@master

后面我们配置Shadowsocks要使用AEAD ciphers，你还要安装libsodium

yum install libsodium

不用知道AEAD ciphers是什么，只要知道它可以让你的翻墙更安全就可以了。

Shadowsocks服务端配置介绍，Shadowsocks可以通过JSON文件保存配置文件，JSON的文件格式是

{

"server":"my\_server\_ip",

"server\_port":8388,

"local\_port":1080,

"password":"barfoo!",

"timeout":600,

"method":"chacha20-ietf-poly1305"

}

* server：你VPS的IP地址
* server\_port：你想让Shadowsocks使用的端口
* local\_port：本地端口
* password：客户端用来进行身份验证的密码
* timeout：超时时间
* method：Shadowsocks加密内容的加密方法

填好这个JSON文件后，保存文件（假设保存为shadowsocks.json）

然后启动Shadowsocks服务

ssserver -c shadowsocks.json -d start

成功启动后Shadowsocks服务会在后台运行

Shadowsocks客户端配置介绍



填上相应的参数，address=server，address后面的是端口也就是上面的server\_port，Encryption=method，Password=password

填上这三个必要的参数就可以了。

浏览器插件

为了让你的翻墙体验更加好，你可以给Chrome或者Firefox安装SwithyOmega插件，怎么配置这个插件看我演示。