**病毒检测与入侵第三次作业**

赵文博 201492078 软网1404

上次作业中我们分析了hosts文件的工作原理并与ipv6进行了关联，这次我们主要介绍翻墙的第二种也是最为流行的方法，VPN翻墙。

首先科普一下什么是VPS和VPN。VPN指的是虚拟专用网络。其功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN网关通过对[数据包](http://baike.baidu.com/view/25880.htm)的加密和数据包目标地址的转换实现[远程访问](http://baike.baidu.com/view/183974.htm)。而VPS指的是virtual private server，即虚拟私人服务器。VPN翻墙实现的原理实际上非常简单，就是将外国的服务器作为代理服务器访问网页。这样一来，DNS解析，发出请求等都是有境外的服务器完成的，GFW就毫无办法了。

一般而言，我们本机访问我们境外的服务器会采用隧道技术，主要是因为以下的原因：

1.将数据流强制送到特定的地址。 2. 隐藏私有的[网络地址](https://www.baidu.com/s?wd=%E7%BD%91%E7%BB%9C%E5%9C%B0%E5%9D%80&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Yzuhwbm1KBnHKBmHn3ujc0IAYqnWm3PW64rj0d0AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtznHfkn1bznW03P1mLnHRkPWm3)。

3. 在IP网上传递非IP数据包。 4. 提供[数据安全](https://www.baidu.com/s?wd=%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Yzuhwbm1KBnHKBmHn3ujc0IAYqnWm3PW64rj0d0AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtznHfkn1bznW03P1mLnHRkPWm3)支持。

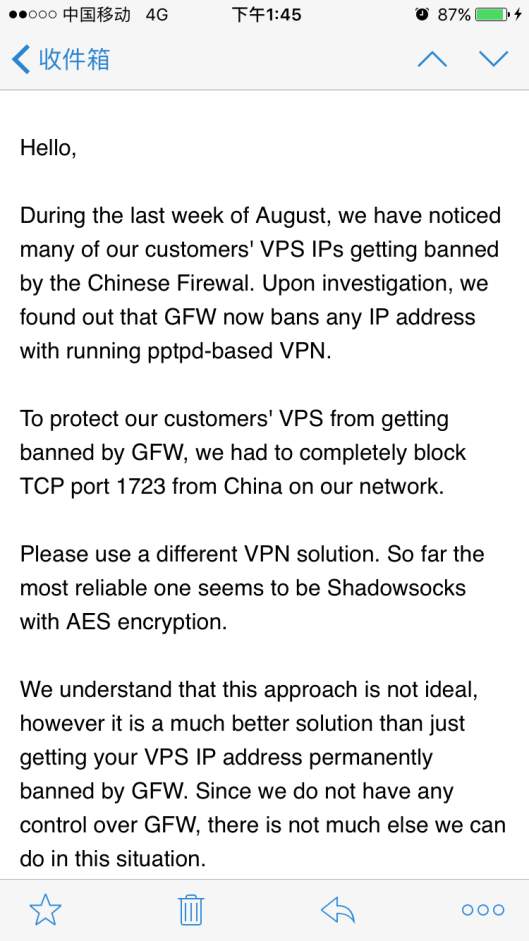
目前市面上采用的主要有以下两种协议，PPTP协议，L2TP协议，二者都用到的PPP（点对点传输协议），主要区别如下。PPTP要求网络为[IP网络](http://baike.baidu.com/view/4256808.htm)，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道；L2TP提供包头压缩、隧道验证，而PPTP不支持。而且PPTP通常与IPSEC结合使用，安全性可以更高。为了方便，我们在用自己的VPS搭建VPN是选择使用PPTP协议。

下面是本次的实验过程：

首先我们需要选择VPS，由于价格原因，我选择的是搬瓦工的VPS, 当然便宜自然有其原因，搬瓦工的vps是基于openVZ架构的，OpenVZ为不完全虚拟化技术，每个VPS账户共享母机内核，易受同一母机下其他VPS的影响，几乎不能单独修改内核。而其他市面上的一些较贵的vps是基于xen和kvm架构的。Xen和KVM为完全虚拟化技术，各VPS之间互相独立，基本互不影响，而且可以任意修改内核。

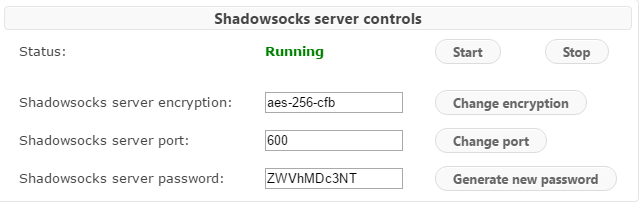
之后我们需要配置我们的vps, 实行pptp协议。主要步骤如下：1. 使用SSH登陆VPS,运行下面命令安装PPP和Iptables 2. 安装pptpd服务 3. VPN相关配置问题 4. 设置转发规则 5. 启动VPN （具体安装步骤请看<http://www.jianshu.com/p/b21c12bf86e8>）

然而事情没有那么顺利的进行，启用pptp之后，我的主机并不能连接上我的服务器，我百思不得其解，在调试了许久之后，我给vps的客服发了一封邮件询问，得到了如下回复



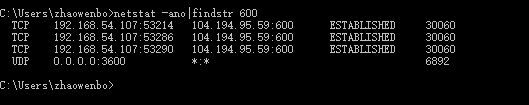
**原来是搬瓦工把端口封掉了。那时我的内心是崩溃的。。。PPTP告一段落。**

于是我又开始转向socks 5代理。Socks代理需要相应的软件，比如Shadow socks, 搬瓦工很良心的给出服务器端的一键安装，使用其他服务器的朋友们可以参考<http://bbs.ihei5.com/thread-344353-1-1.html>，在此就不赘述了。



然后安装客户端，按照上表填写就没啥问题了。

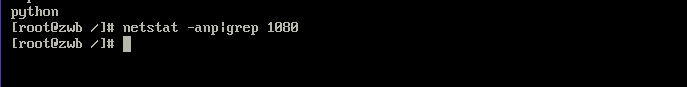
然后我在客户端和服务端进行了端口查看





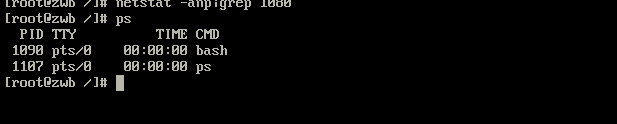
可以看到，客户端通过服务器的600端口进行通信。

另：Shadow socks 里面有一个代理端口，默认是1080，我不是很理解这个端口的作用，于是又在服务器端查看这个端口



却发现没人在用，这个真的很让我困惑。

更让人奇怪的是，我用ps命令查看进程，没有发现pid为1001的进程。



以上两个问题还在思索中，无法给出解释。。