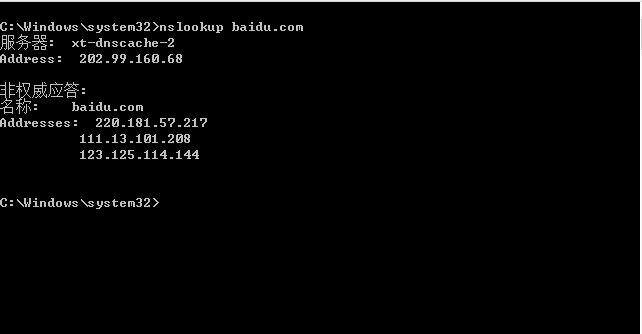


　　　如果买了联通公司的流量，会取得一个账号和密码，输入账号密码登陆后就能享用无线了，当然啦，对于爱折腾的人来说，总要想点方法绕过这个认证，不为别的，只为实现内心的一个想法。所以我就在各大技术论坛查询了一些绕过web认证的方法。网上有很多人给出了方法，这些方法大同小异，基本原理都一样，但是呢，难免有疏漏和难懂的地方。所以，接下来，我就对这个问题做一次系统的介绍。

　　首先我先讲一下原理，当我们连上校园网的无线路由器后，虽然上不了网，但是我们的计算机却分配到了IP地址（那么为什么要给我们分配IP呢？很好回答啦，不分配IP地址web认证就实现不了呀！）此时若我们进行一些上网的操作，例如访问百度主页，那么计算机的数据包将从TCP443端口上发出，校园网网关就会拦截从这个端口上发出的数据包。同理从其它端口上发出的数据包也会遭到拦截。

　　但是有一个神奇的端口，从这个端口发出的数据包不会遭到网关拦截，它就是UDP53端口。对计算机网络稍微了解的朋友应该知道在UDP53端口上运行的协议是DNS协议（域名解析协议）也就是说我们现在可以正常查询网站域名对应的IP地址。例如用Windows自带的nslookup命令查询百度的IP地址时会返回一个正确的结果：



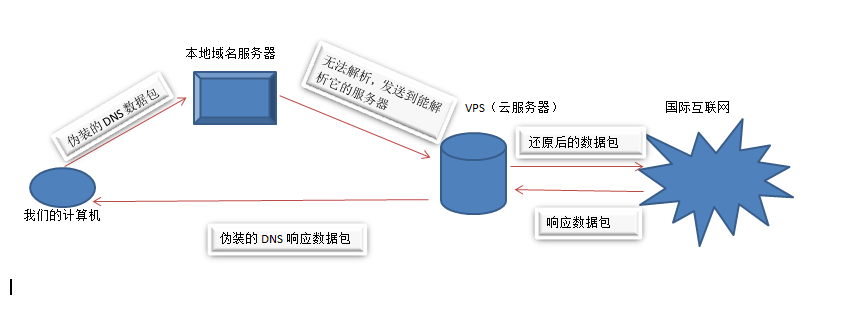
PS:接下来可能要提到一些有关域名解析原理和网络隧道方面的知识，限于篇幅，我就简单说两句，想要深入了解的朋友可以参考以下内容：

DNS原理及其解析过程【精彩剖析】: http://369369.blog.51cto.com/319630/812889/

隧道技术：https://baike.baidu.com/item/%E9%9A%A7%E9%81%93%E6%8A%80%E6%9C%AF/10774268

　　既然UDP53端口的数据包可以通过网关，那么我们可以在本地运行一个程序将其它端口的数据包伪装组成UDP53端口的数据包，然后发送到本地域名服务器，那么网关就不会进行拦截了，数据包就顺利的通过了网关，可是发送出去的数据报如何返回呢？这就需要我们做进一步的设置。

　　接下来我们需要一个VPS（云服务器）和一个域名，我了便于叙述，我给这个云服务器起名为V，域名起名为Y。我们伪装的DNS数据包要查询的域名就是Y，本地域名服务器接收到这个伪装后的数据包后，由于它无法解析这个域名Y，便将数据包进行转发，让能够解析Y的域名服务器进行解析，接下来我们将Y设置一个NS记录，用来指定Y由哪个域名服务器来进行解析，我们指定的域名服务器就是前面提到的V，所以接下来数据包会被发送到V中。此时我们在V中运行一个程序，对伪装的数据包进行还原，还原后的数据包再发送出去，这样当V接收到响应数据包后，V上运行的程序会再次对其进行伪装，伪装成一个DNS响应数据包，这个DNS响应数据包会沿着上述相反的路径发送回我们的计算机，我们的计算机再次对这个DNS响应数据包进行还原，到现在，我们真正想要得到的数据包已经到手了。也许上面的叙述有点绕，我放一张图大家就能明白了：



好了，要是看了图没明白也没有关系，只要按照下面的步骤做就可以了

接下来，到了最重要实战部分了

　　Windows上与Linux上实现方法不同，就伪装数据包的程序而言，在windows平台上推荐使用dns2tcp这个软件，而在linux平台上推荐使用iodine这个软件，关于iodine的使用，我会再写一篇文章，所以下面主要讲一下dns2tcp的使用，也就是在windows上实现绕过WEB认证，linux系统用户请移步我的另一篇文章

NO.1：

　　在本地计算机上安装dns2tcp这个软件，<它的作用是对数据包进行伪装与还原> 

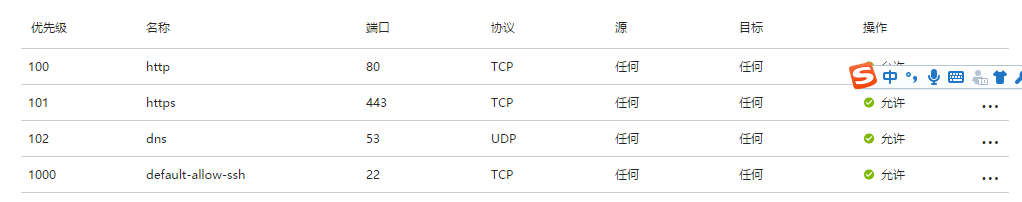
NO.2：

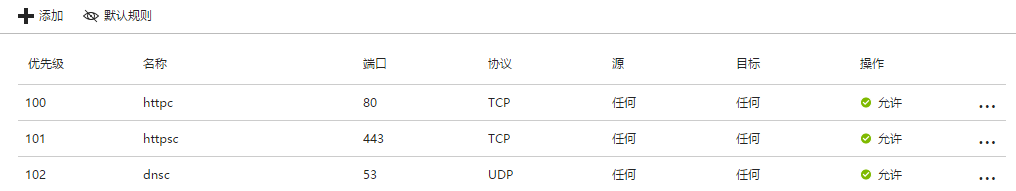
　　申请一个VPS，国内VPS服务商众多，什么阿里云啦，腾讯云啦，百度云啦。在这里我给大家推荐由世纪互联运营的微软Azure云服务器，1元体验一个月，申请与部署方式很简单，而且服务器配置与带宽很高，可惜的是就能使用一个月，其实学服务器开发的大学朋友们也可以申请一个练练手，毕竟这是一次难得的实践机会嘛！

　　有关申请与部署服务器的细节，我就不再赘述了，按照流程走就行。有不懂的地方可以参看微软给的文档和视频教程。

　　下面这个操作尤为重要，部署成功服务器后，务必参照微软的文档为服务器添加入站与出站规则，也就是哪些类型的数据包可以进出你的服务器，那些类型的数据包会被防火墙拦截，这个步骤决定着伪装的数据包是否能够进入到我们的VBS

将TCP80，TCP443，UDP53端口的数据设置为允许入站与出站，如下图所示：





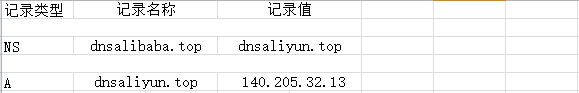
申请成功后，微软会给你一个公网IP，这个公网IP一定要牢记，接下来需要用到,现在假定你得到的公网IP为140.205.32.13

NO.3：

　　申请一个域名，推荐到阿里云申请，因为便宜，我申请的.top国际顶级域名第一年才1块钱。  
附申请地址：https://wanwang.aliyun.com/domain/yumingheji

　　申请过程请严格按照人家的流程，不过要提醒一点的是务必要用真实信息，否则人家会封掉你的域名。

　　现在假定你申请到了一个域名，假如你申请到的域名为aliyun.top,你需要进入阿里云的域名控制台，为其添加两条记录。  
　　第一条为NS记录，记录名称随便，记录值也随便，但是记录值要牢记，以后用的到。  
　　假设你添加的NS记录名称为dnsalibaba.top,记录值为dnsaliyun.top。  
　　再为申请到的域名添加一个A记录，A记录的记录名称是NS记录的记录值，A记录的记录值是你所申请到的VPS的公网IP，如下图：



　　当本地域名服务器无法解析我们伪装的数据包后，便将数据包发送给NS记录指定的服务器dnsaliyun.top,而dnsaliyun.top的IP地址已经在A记录中给出了，所以刚才原理没看懂的朋友朋友们现在应该知道为什么本地域名服务器会将数据包发送到我们的VPS中了吧

NO.4：

经过上述三步，我们所需要的资源就都具备了，这是最后一步。

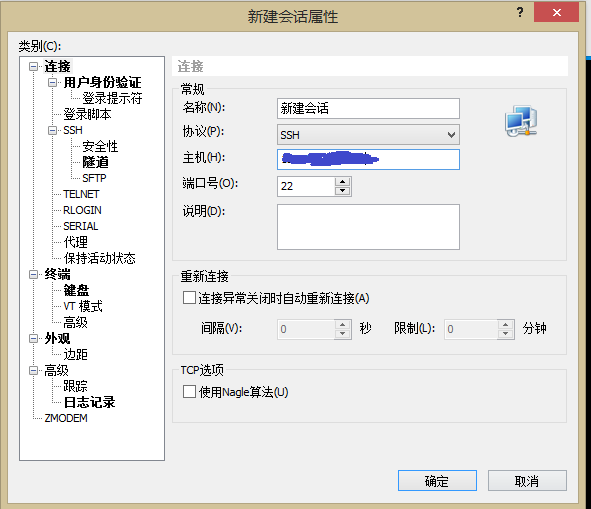
　　windows系统用户在计算机上安装一个名为xshell的软件，它用来连接我们的VPS。

　　附下载地址：http://www.downxia.com/downinfo/150560.html?fromm

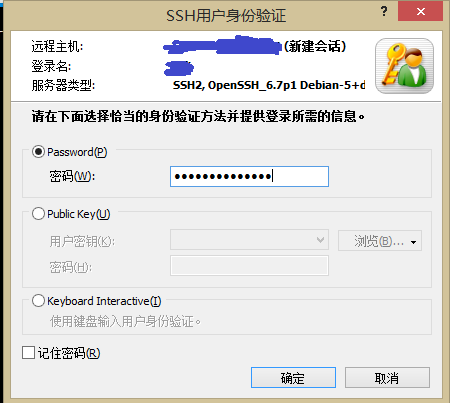
　　下载后安装，安装时选择“家庭/学校 ”版，商业版要钱，家庭版其实就能满足我们的需求了。

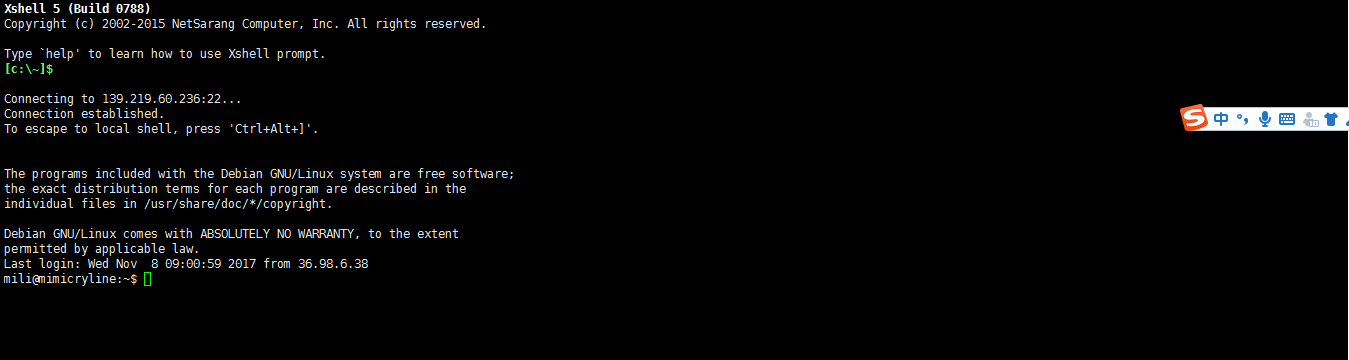
　　安装成功后，依次点击点击"文件"->"新建"。名称随意，协议选择SSH，主机名填你的VBS公网IP，端口号填22，添完后点击连接；

　　等一会弹出一个输入用户名的窗口，输入你部署服务器时设置的用户名，输入完成后点击记住用户名，点击确定。在弹出的新窗口中输入你部署服务器时设置的密码，输入完成后点击确定，不出意外，你将会连接到你的VBS,如下图：

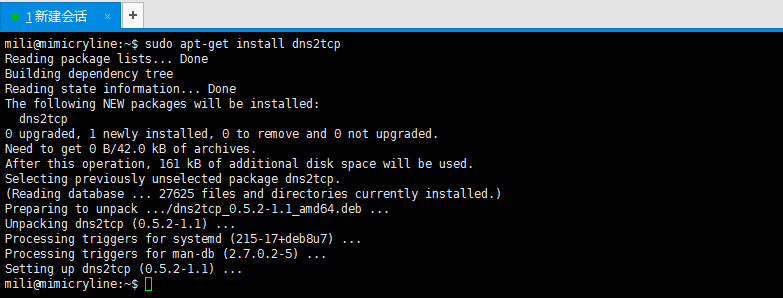








接下来在Xshell中输入sudo apt-get install dns2tcp，敲回车，这条命令用来安装dns2tcp这个软件，很快就会安装完毕

  
PS：没用过Linux的用户可能看不懂这些Linux命令，但是不懂没关系，跟着我做就行了。

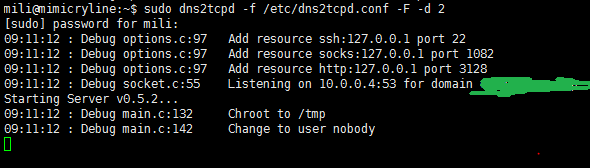
接下来配置dns2tcp

再次敲入命令：sudo vim /etc/dns2tcpd.conf ，用vim编辑器将其中的内容替换为一下内容(vim编辑器的使用教程网上有)：  
listen = 10.0.0.4     #这里写你的云服务器的内网IP，一般为10.0.0.4  
port = 53   
user = nobody   
chroot = /tmp   
domain = dnsaliyun.top         #这里写你设置的NS记录值  
resources = ssh:127.0.0.1:22,socks:127.0.0.1:1082,http:127.0.0.1:3128

配置完后按ESC键，输入“:wq”后敲回车保存配置文件

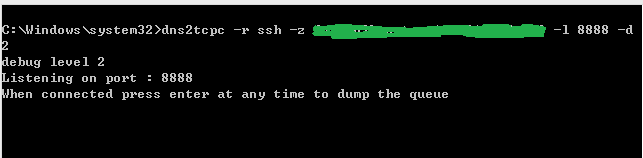
下面创建后台进程，运行dns2tcp，依次键入并执行如下命令：

screen -S dns2tcpd　　　　　　　　　    　 #创建后台会话   
dns2tcpd -f /etc/dns2tcpd.conf -F -d 2　   　 #启动dns2tcp



当出现上图显示的内容时，说明dns2tcp启动成功了，此时按下Ctrl + a+d键，让dns2tcp进程后台执行，再关闭与服务器的连接就行了

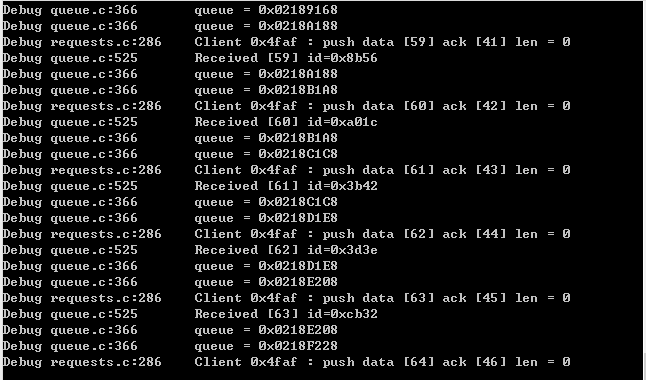
windows客户端配置：  
打开CMD，键入并执行如下命令 ： dns2tcpc -r ssh -z dnsaliyun.top 140.205.32.13  -l 8888 -d 2



当出现上图显示的内容时，代表会话已经建立了，此时最小化这个窗口【记住千万不要关闭它！！！】  
\*\*\*注：  
-r 后接服务名称<ssh/socks/http中的任意一个>  
-z 后接你设置的NS记录,和你的VPS公网ip  
-l 后接本地端口，随便一个常用端口就行  
-d 开启 Debug

现在假设你完全按照我给出的流程走的

离成功只有一步之遥了，下面用Xshell转换Socks4/5通用代理：  
　　在xshell中仿照上面新建会话：IP地址为127.0.0.1，端口为8888 ；然后点击隧道，类型选择socks4/5，端口填1080，输入完成后点击确定，若不出意外，此时CMD中会出现大量信息，这些信息代表通过dns2tcp的数据包，这就表明你的电脑已经在和服务器传输数据了。而xshell中又会提示你登录到你的服务器，仿照上文输入用户名和密码（最好选择记住用户名和密码，这样下次就不用那么麻烦了），点击确定并成功登录到你的服务器后，最小化xshell【记住，此时千万不要关闭xshell！！！】



　打开Internet选项，依次选择"连接"->"局域网设置"->"为LAN使用代理服务器"->"高级"

　在socks/套接字输入框中，要使用的代理服务器地址填127.0.0.1，端口填1080，然后点击确定。



**到此，大功告成，打开你的浏览器试试吧！！！**