**以下操作相当于给内网的防火墙上开了个洞，会给整个内网带来极其严重的安全隐患！**

**为避免产生法律问题，请在操作前务必向网络管理员咨询您的操作权限！**

**★★★★★★★★★★★★★★★★★★★**

**《基于VPS服务器的内网代理转发方案》前言**

假设我们在内网有一个自己的电脑A（运行[Win7](http://www.knowsky.com/article.asp?typeid=180)），希望在外网家中用另一台电脑B（运行Win7）访问内网资源，或伪装为内网电脑访问外网资源。

由于内网电脑没有公网[ip](http://ip.knowsky.com/)，所以外网电脑无法直接向内网电脑发起连接。为实现我们的目标，需要从内网电脑主动向一个公网服务器发起一个连接，外网电脑通过这个服务器使用这一连接，再通过内网电脑进行访问。

现在已有许多商业内网代理服务器可以实现此功能，比如花生壳、步轻云、TeamView、GoToMyCloud等等。但天下没有免费的午餐，**要使用第三方的公网服务器就必须为第三方付费**，并且这些服务器都有各种各样的限制。此外，由于数据包会流经第三方，因此对**数据安全也是一大隐患**。

随着个人VPS服务器的普及，越来越多的朋友想用自己的VPS服务器作为内网代理，这样既安全又免费。本套方案实现了这一目标，并具有以下无可替代的优势：

* **在已有VPS服务器的基础上，完全免费；**
* **用到的所有工具软件皆为开源软件；**
* **不经过任何第三方服务器，保证数据安全；**
* **外网电脑可以伪装成内网电脑，具有最高访问权限。**

如果您的方案在满足上面四个条件的基础上，比我的方案更简单，敬请指教！下文将对配置方案作详细的介绍。

**先决条件**

1. A机上可访问外网并且可以安装虚拟机。

2. 拥有一个外网的VPS服务器S（运行Debian 7.x）。推荐购买BandWagon的廉价VPS服务器（https://bandwagonhost.com/），一年100多元。

**一、建立从内网机到外网服务器的反向隧道**

1.1. 在A机上用虚拟机运行[Ubuntu](http://www.knowsky.com/article.asp?typeid=188) Server。首先安装VirtualBox虚拟机。

下载VirtualBox：https://www.virtualbox.org/wiki/Downloads

最新版的VirtualBox不用配置网络即可从本地可用的网络连接上网。

下载Ubuntu Server：http://www.ubuntu.com/download/server

在VirtualBox中安装Ubuntu Server，全部默认设置即可。

1.2. 由A机发起，建立从A到S的反向隧道连接，命令格式：

ssh -C -R <NPORT>:localhost:22 -p <RPORT> <SUSER>@<S\_IP>

* -C：允许数据压缩；
* NPORT ：指定在S机上进行侦听的端口。在S机上发往"localhost:NPORT"的数据包都将被直接转发到A机的22端口（SSH默认服务端口）；
* RPORT：S机的SSH服务端口；
* SUSER：登录S机的用户名，一般为root；
* S\_IP：S机的公网IP。

执行此命令后，可能需要输入SUSER在S机的密码。反向隧道连接建立成功以后，即远程登录到S，接下来的操作都是将在S上执行。命令举例：

ssh -C -R 876:localhost:22 -p 26131 root@14.12.83.20

1.3. 建立从S到A的SSH动态转发，可视为从S到A的SOCKS代理服务，命令格式：

ssh -C -f -N -D <SPORT> -p <NPORT> <LUSER>@localhost

* -f -N：后台连接而不登录到主机，也不执行任何脚本；
* SPORT：指定S机上SOCKS代理服务进行侦听的端口；
* NPORT：S机上侦听的反向隧道端口，在第1.2步指定；
* LUSER：登录A机的用户名。

执行此命令后，可能需要输入LUSER在A机的密码。至此，我们已将A作为S的SOCKS代理服务器。命令举例：

ssh -C -f -N -D 1080 -p 876 devymex@localhost

1.4. 用curl命令测试连接，命令格式：

curl --socks4 localhost:<SPORT> <URL>

* SPORT：S机上SOCKS代理服务进行侦听的端口，在1.3步指定；
* URL：任意网址，可指定内网资源。

此命令若执行成功，URL所指向的内容会打印在屏幕上。一般以简短的HTML页面为佳，太大的资源会很慢。命令举例：

curl --socks4 localhost:1080 www.baidu.com

如果未安装curl，需先安装：

apt-get install curl

若未找到curl包，需先更新apt-get：

apt-get update

**二、在服务器端用DeleGate实现二级HTTP代理**

接下来要将SOCKS代理转换为HTTP代理，使用的软件是DeleGate。这是一个开源软件，但目前并不被apt-get、rpm和yum支持，因此必须先下载编译。

2.1.如果没有g++需要先安装g++，命令：

apt-get install g++

2.2. 下载和解压DeleGate（http://www.delegate.org/），命令：

cd ~wget ftp://ftp.delegate.org/pub/DeleGate/delegate9.9.13.tar.gztar -xzf delegate9.9.13.tar.gz

* wget：下载[源码](http://code.knowsky.com/)包到/home目录下，当然其它具有运行程序权限的目录亦可；
* tar -xzf：/home/delegate9.9.13子目录并解压缩到此目录中。

注意，如果DeleGate发布了新版本，上面给出的下载链接和目录名可能不同，请关注DeleGate官方网站。

2.3. 编译DeleGate，命令：

cd ~/delegate9.9.13make

make命令必须在DeleGate解压后的目录中执行。如果未安装make，需先安装：

apt-get install make

make执行的过程较慢，其间会提示输入电子邮箱，任意输入，然后按Y即可。

2.4. 启动DeleGate，命令格式：

src/delegated -P<HPORT> SERVER=http SOCKS=localhost:<SPORT>

* HPORT：指定S机上HTTP代理服务进行侦听的端口；
* SPORT：S机上SOCKS代理服务进行侦听的端口，在1.3步指定。

命令举例：

delegated -P8118 SERVER=http SOCKS=localhost:1080

2.5. 用curl命令测试连接，命令格式：

curl -x localhost:<HPORT> <URL>

* HPORT：S机上HTTP代理服务进行侦听的端口，在2.4步指定。
* URL：任意网址，可指定内网资源。

命令举例：

curl -x localhost:8118 www.baidu.com

**三、在服务器端建立端口转发**

现在S机上已经有本地的HTTP代理了，接下来要将

3.1 如有必要，先清除已有nat规则，命令：

iptables -t nat -F

iptables是一个非常强大的防火墙/路由程序，用法也比较复杂，具体可参考相关文档，此处不做赘述。

3.2 建立http协议的端口转发，命令格式：

iptables -t nat -A OUTPUT -p tcp --dport 80 -j REDIRECT --to-ports <HPORT>

* HPORT：S机上HTTP代理服务进行侦听的端口，在2.4步指定。

命令执行后，由S机发出的HTTP请求（80端口）都将被转发到HPORT端口上。

命令举例：

iptables -t nat -A OUTPUT -p tcp --dport 80 -j REDIRECT --to-ports 8118

3.3. 用curl命令测试连接，命令格式：

curl <URL>

* URL：任意网址，可指定内网资源。

命令举例：

curl www.baidu.com

**四、在外网机通过SSH隧道连接到外网服务器**

1. 在B机安装Bitvise SSH客户端软件

2. 配置Bitvise SSH客户端的Login页

Host：S机的服务器IP；Port：SSH服务端口；Username：登录用户名；Initial method：pass[Word](http://www.knowsky.com/article.asp?typeid=117)；Password：登录密码。

3. 配置Bitvise SSH客户端的Services页

SOCKS/HTTP [PR](http://pr.knowsky.com/)oxy Forwarding：Enabled；Listen interface：127.0.0.1；Listen port：1080。

4. 在B机安装Privoxy。

下载地址：http://sourceforge.net/projects/ijbswa/files/

5. 配置Privoxy目录下的config.txt文件，并运行Privoxy：

listen-address 0.0.0.0:1984forward-socks5 / 127.0.0.1:1080 .

6. B机上的任意程序，以localhost:1984为HTTP代理，即可通过A机访问内网资源。

**备注**

1. kill掉delegate进程即可终止S机上的HTTP代理服务，删除delegate的目录即可完全卸载DeleGate。

2. 执行如下命令可取消80端口数据包的转发：

iptables -t nat -F

3. 断开从A机到S机的连接，即可终止S机上的SOCKS代理服务。

4. 查看侦听指定端口的进程ID，命令格式：

fuser -un tcp <PORT>

5. B机上建议使用[Firefox](http://www.knowsky.com/article.asp?typeid=151)+AutoProxy进行访问。AutoProxy下载地址：http://fxthunder.com/blog/archives/2866