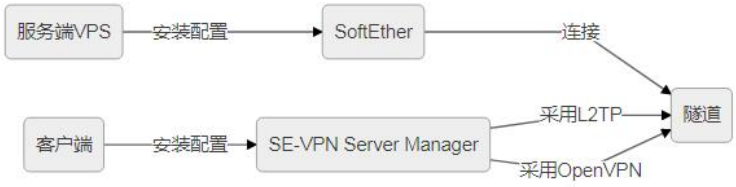
使用SoftEther搭建 VPN Server

注意：根据《中华人民共和国计算机信息网络国际联网管理暂行规定》，计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网

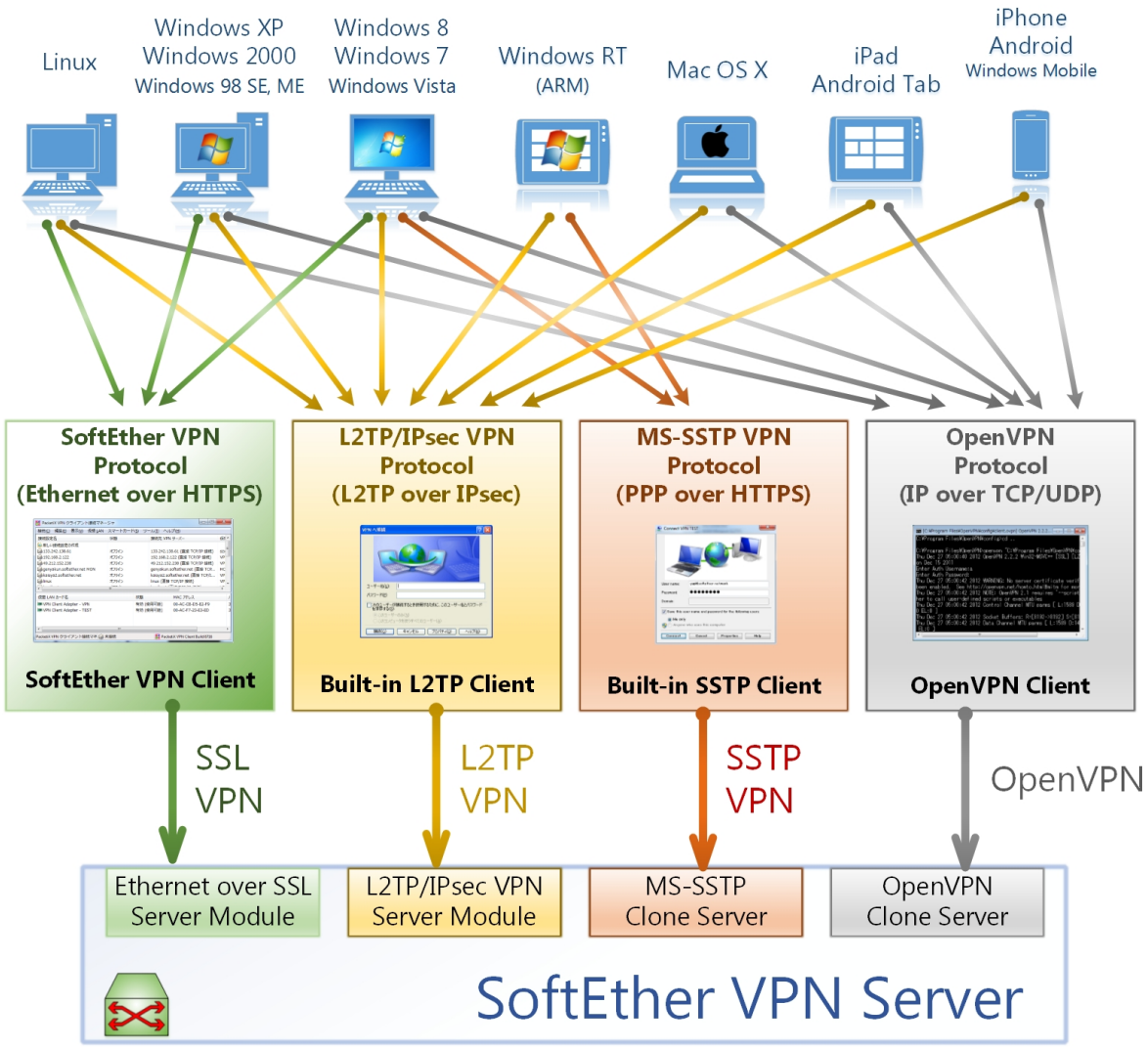
申明：本文章仅供研究学习使用，请勿用于商业、非法用途，本文禁止转载！

注意：根据《中华人民共和国计算机信息网络国际联网管理暂行规定》，计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。

[



VPN（虚拟专用网）的搭建对于新手来说尽管在网上有很详尽的教程，可是真正搭建成功还是略复杂的，在这里介绍日本筑波大学研发的分布式 VPN ——SoftEther，本文主要介绍 Linux 下的SoftEther安装及使用方法，搭建VPN Server（PPTP、L2TP、OpenVPN）。



SoftEther VPN

官网：http://www.softether-download.com/cn.aspx?product=softether 包含多种平台架构的下载地址（需科学上网）

1. SoftEther VPN Server Manager 点此下载
2. SoftEther VPN 客户端 点此下载

一、服务端安装

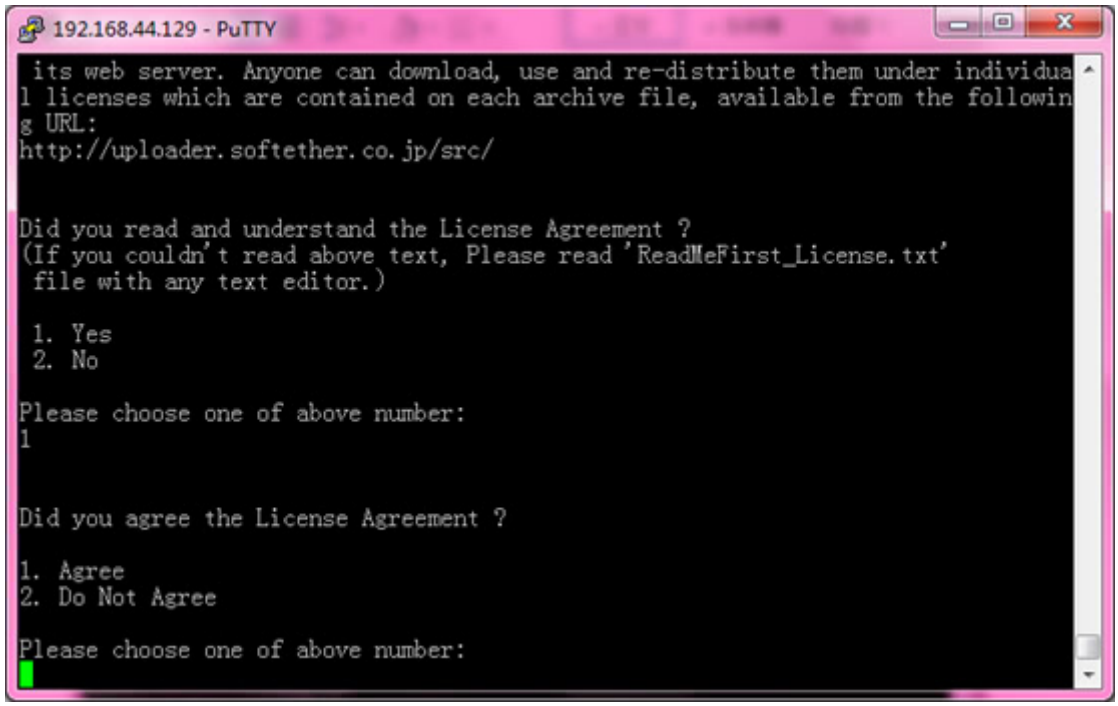
（1）安装 SoftEther

```
sudo apt-get update
sudo apt-get install build-essential

#安装 make gcc g++ 编译软件
ubuntu系统执行：  apt-get install make gcc g++  -y
cenos 系统执行：  yum install make gcc gcc-c++ -y

#32 位执行这个：
```

```
wget https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/releases/download/v4.29-9680-rtm/softether-vpnserver-v4.29-9680-rtm-2019.02.28-linux-x86-32bit.tar.gz

#64 位执行这个：
wget https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/releases/download/v4.29-9680-rtm/softether-vpnserver-v4.29-9680-rtm-2019.02.28-linux-x64-64bit.tar.gz

tar xvf softether-vpnserver-v4.29-9680-rtm-2019.02.28-linux-x64-64bit.tar.gz
#解压缩：tar xvf 文件名

cd vpnserver  #切换到解压出来的目录中

make  #安装
```

如果你的服务器在国内，可以使用Winscp软件（主要功能是在本地与远程计算机间安全地复制文件，并且可以直接编辑文件）上传到服务器。WinSCP 有两种界面可供您选择，如果您是第一次使用 WinSCP，建议选择 Windows Explorer 界面，因为 Windows 用户比较熟悉这个界面。
[点此快速下载]

- 链接：https://pan.baidu.com/s/1QpakYDLhZFIBDuQytfteSg
  提取码：gt5i



连续输入三个 1 ——> 安装完成 不要删除此目录

(2) 设置 SoftEther VPN 服务

```
./vpnserver start    #开启服务
```

```
./vpncmd              #依次 1，回车，回车    针对开启了 https 的 web 服务器，依次 1，localhost:5555，回车

ServerPasswordSet     #设置管理服务器的密码，两次确定之后，按 ctrl+C 退出管理      这里我选择不设置密码

sudo vim /etc/rc.local      #将服务器加入到开机启动项中

在 exit 0 之前写入：
/root/vpnserver/vpnserver start
```

二、部署服务端

SoftEther VPN Server Manager部署（本质上是用可视化界面部署服务端）

（1）连接到服务端

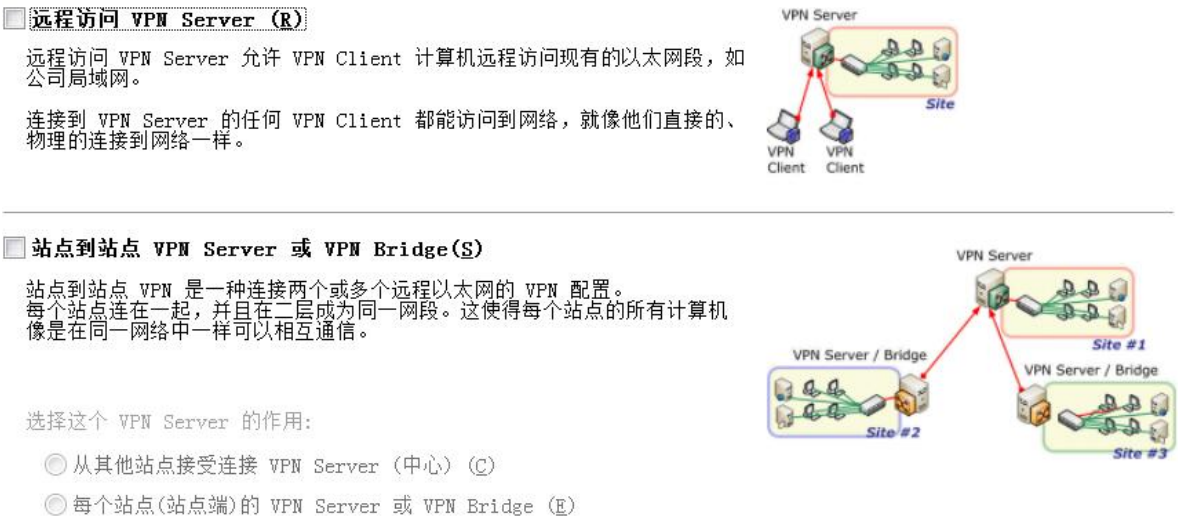
打开SE-VPN Server Manager (Tools)管理工具 ——> 点击新设置 ——> 设置（如图） ——>确定 ——> 连接

密码连接管理模式 处填写之前设置的 **管理服务器的密码** 。

针对开启了 https 的 web 服务器，之前又设置了 **管理服务器的密码** 且在 **./vpncmd** 时 依次 *1*，回车，回车 操作的，**密码连接管理模式** 处不要填写内容。

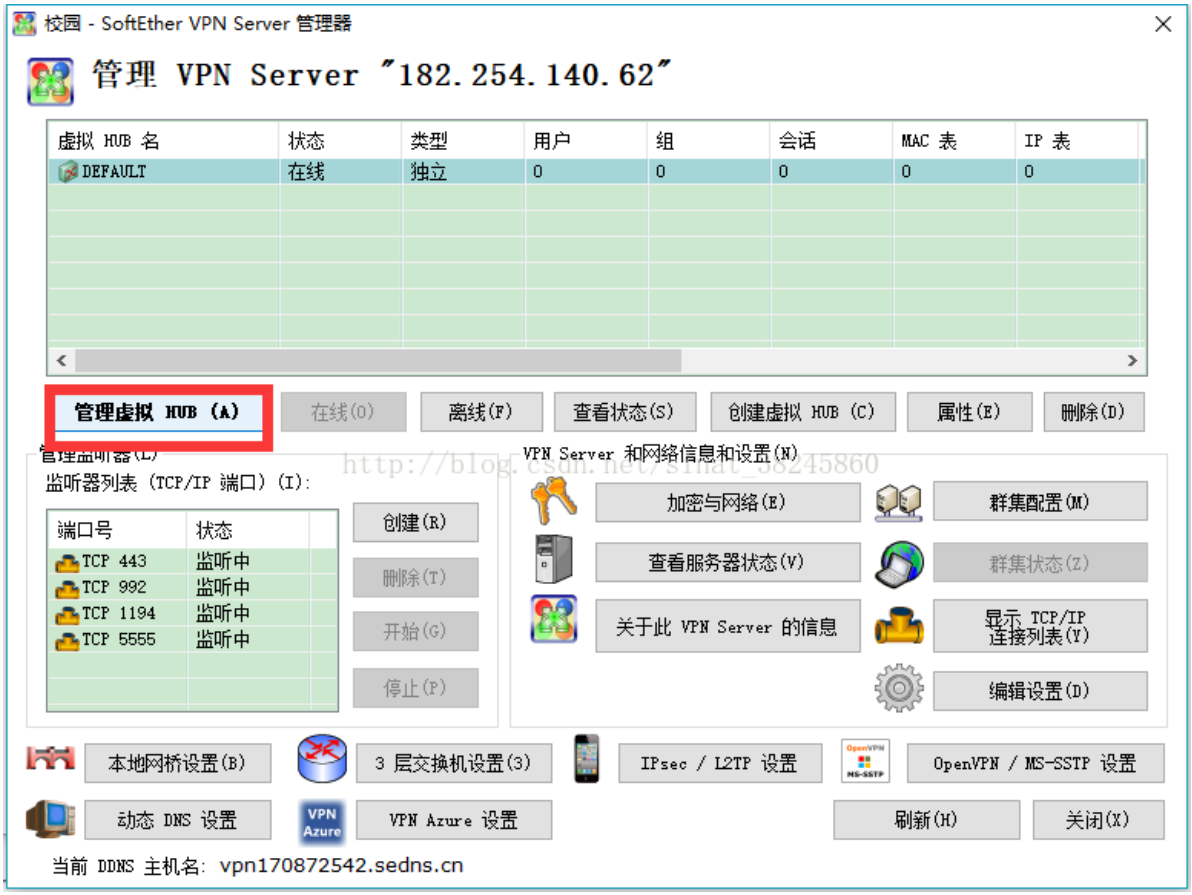
第一次连接会让你自己设定一个密码，下次就用你设定的密码登录你的VPN

连接 ——> 关闭



(2) 管理用户

弹出窗口点否 ——>点击 管理用户 ——> 点击管理HUB ——> 新建 ——> 设置 用户名 和 密码 ——> 确定

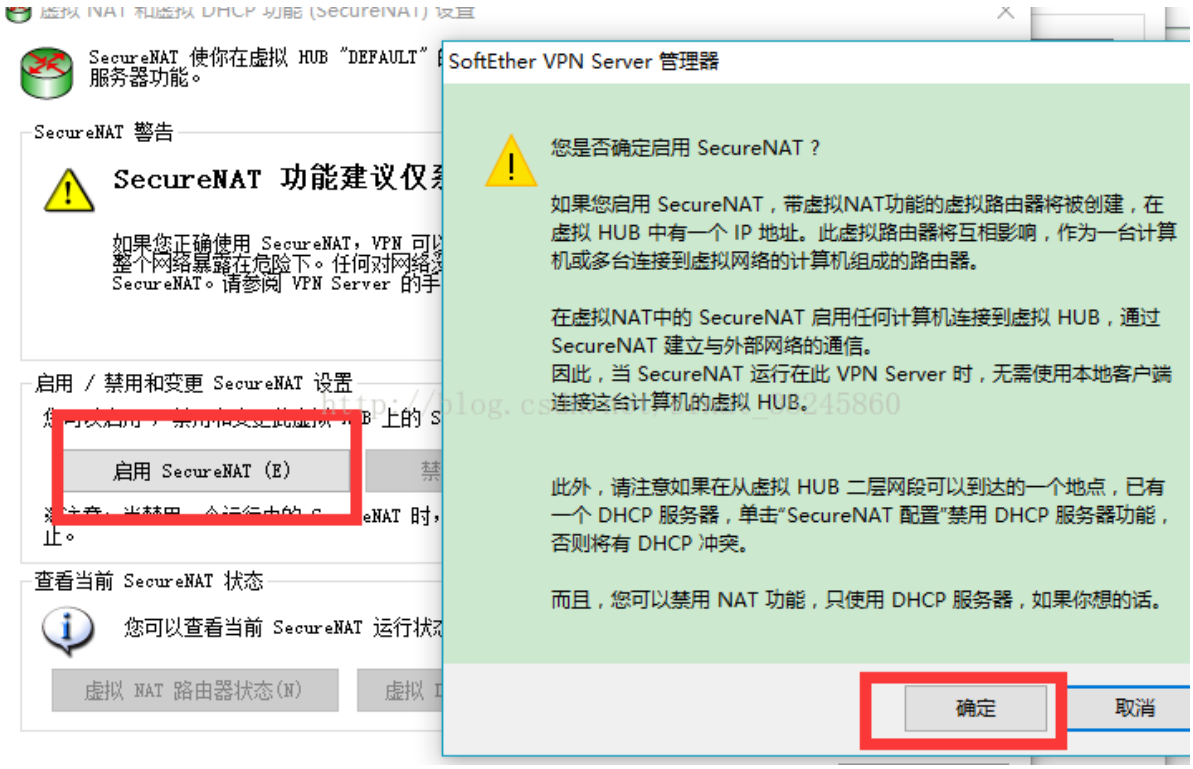



管理虚拟 HUB - DEFAULT
虚拟 HUB "DEFAULT"
管理用户(U)
添加，删除或编辑用户账户。
管理组(G)
添加，删除或编辑组。
管理访问列表(A)
添加或删除访问列表（数据包过滤规则）。
虚拟 HUB 设置(N)
虚拟 HUB 属性(P)
配置此 HUB
认证服务端设置(E)
使用外部 RADIUS 认证服务器作为用户认证。
管理级联连接(C)
在本地或远程 VPN Server 上建立到 HUB 的级联连接。
此虚拟 HUB 当前状态(R):
项目
值
虚拟 HUB 名称
DEFAULT
状态
在线
类型
独立
SecureNAT 机能
无效
会话数
0
访问列表
0
用户数
0
组数
0
MAC 表数
0
刷新(H)
其它设置(O)
日志保存设置(L)
日志文件列表(Q)
配置日志保存功能的设置。
可信的 CA 证书(T)
无效证书(K)
管理可信的 CA 证书。
虚拟 NAT 和虚拟 DHCP 服务器(V)
SecureNAT 在此虚拟 HUB 上可用。您可以运行虚拟 NAT 和虚拟 DHCP。
VPN 会话管理(I):
管理会话(S)
关闭(X)

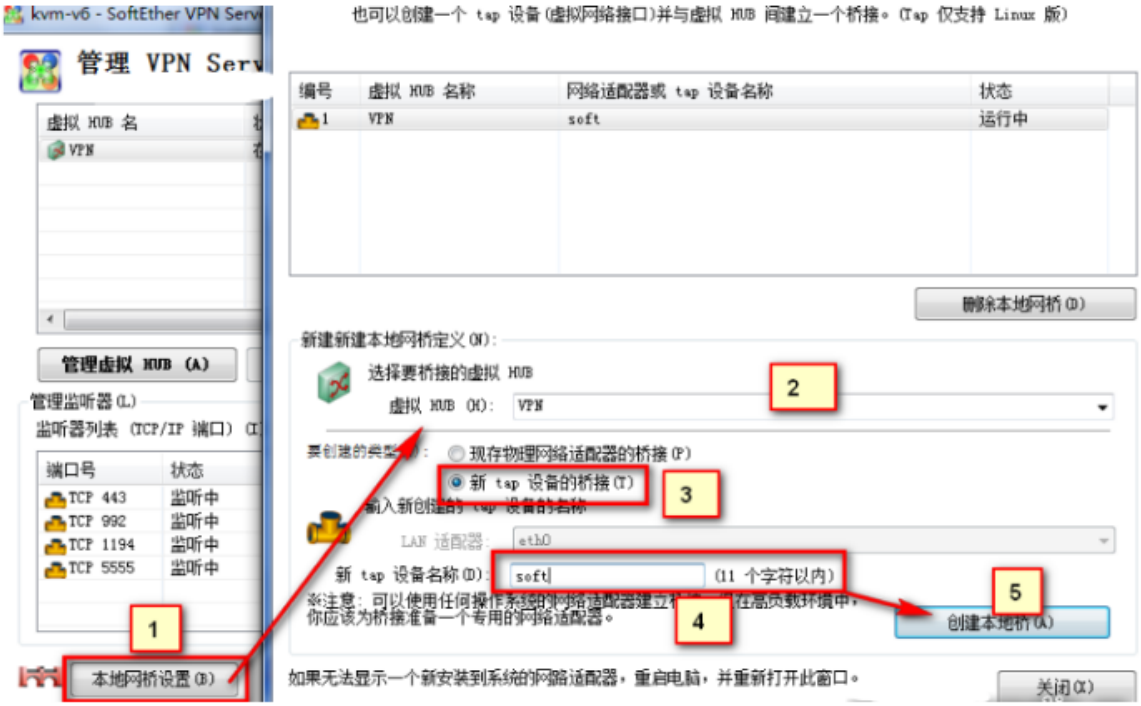

管理用户
虚拟 HUB "DEFAULT" 有如下
用户名
全名
新建(C)
管理级联连接(C)
在本地或远程 VPN Server 的级联连接。
创建新用户
用户名(U): 0
全名(F):
说明(N):
组名(可选):
浏览组(I)...
设置此账户有效期限(S)
2017年 9月19日
0:00:00
验证类型(A):
匿名身份验证
密码验证
特定证书认证
签名证书认证
RADIUS 身份验证
NT 域认证
RADIUS 或 NT 域认证设置
通过密码的登录尝试通过外部 RADIUS 服务端，Windows NT 域控制器或 Active Directory 控制器被验证。
指定认证服务器的用户名(K)
认证服务端上的用户名(W):
安全策略
设置安全策略(Y)
安全策略
密码认证设置
密码(P):
确认密码(C):
特定证书认证设置
用户使用"特定证书认证"将根据是否 SSL 客户端证书与用户事先设置的证书完整匹配而被允许或拒绝连接。
指定证书(E)
查看证书(V)
创建证书(W)
已签名证书认证设置
验证客户端证书是否已签名是基于一份由虚拟 HUB 信任的 CA 证书。
证书的 Common Name (CN) 限制值(B)
证书序列号的限制值(L)
※ 注意: 请输入十六进制数值。(例如: 0155ABCDEF)
提示:使用用户名"*"(星号)定义一个用户对象，以接受不符合任何已注册的、明确的、用户对象的登录尝试。这样一个特殊的用户将使用外部用户认证服务器验证登录。
确定(O)
取消

（3）虚拟NAT和虚拟DHCP服务器

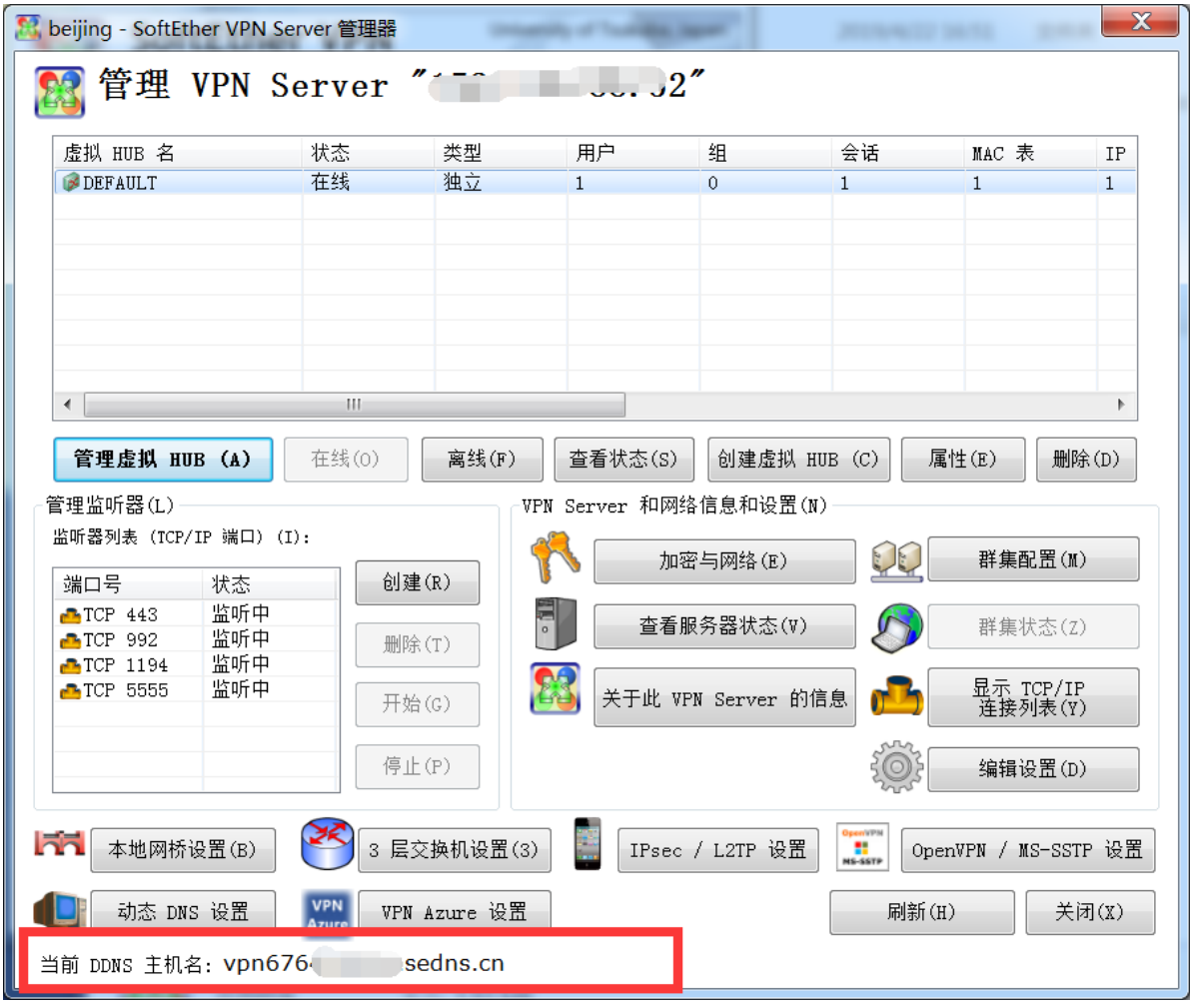
回到管理虚拟HUB界面 ——> 点击虚拟NAT和虚拟DHCP服务器 ——> 启用SecureNAT ——> 确定



> 请一定要注意，SecureNAT 和 Local Bridge（本地桥）不可以同时开启！否则会造成链路层死循环占用大量 CPU。



记下主机名，没有记住就是用公网IP，也OK!



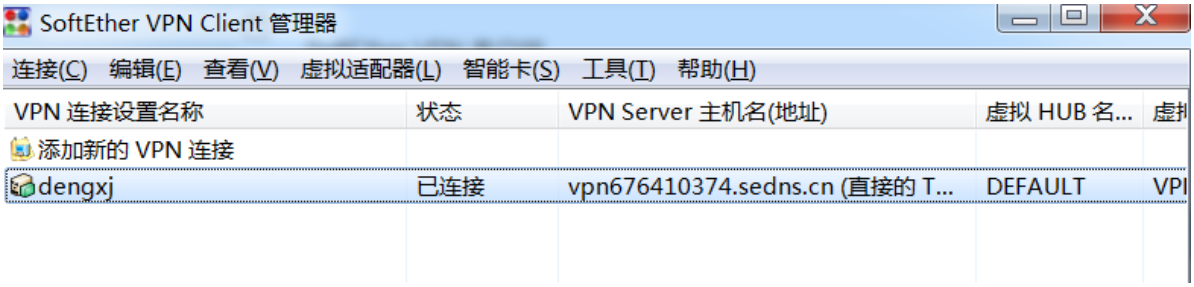
三、VPN 搭建

在这里介绍OpenVPN方法，在这种网络中，你应该使用 OpenVPN。

（1）通过SoftEther客户端连接VPN

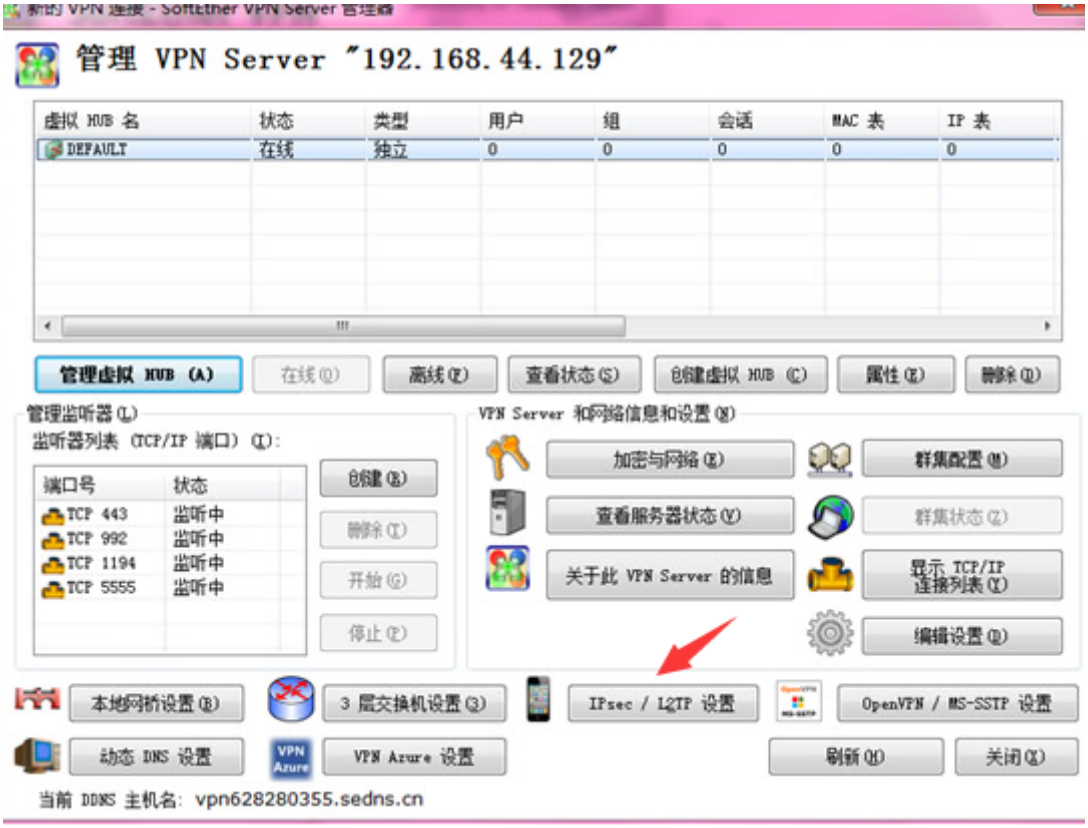
添加虚拟网络配置器 ——> 添加新的VPN连接 ——> 输入信息 ——> 确定

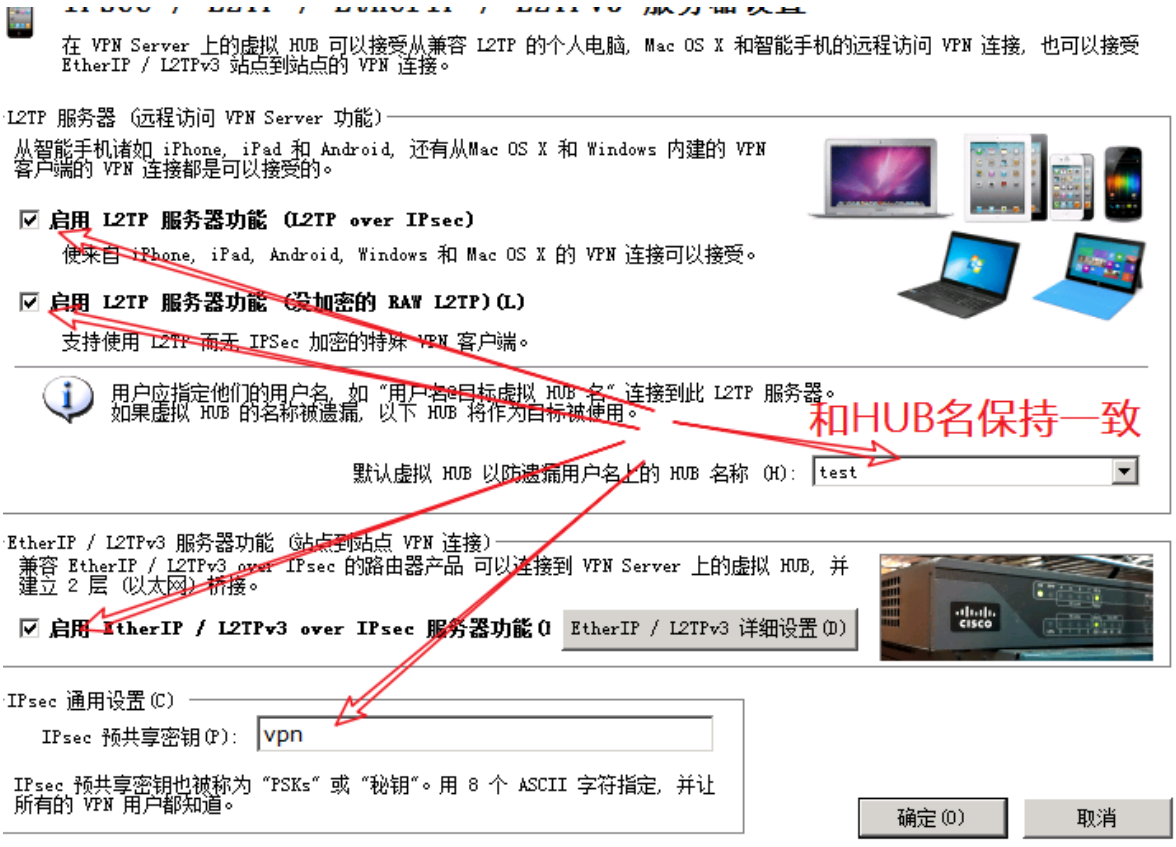
双击输入账号密码连接



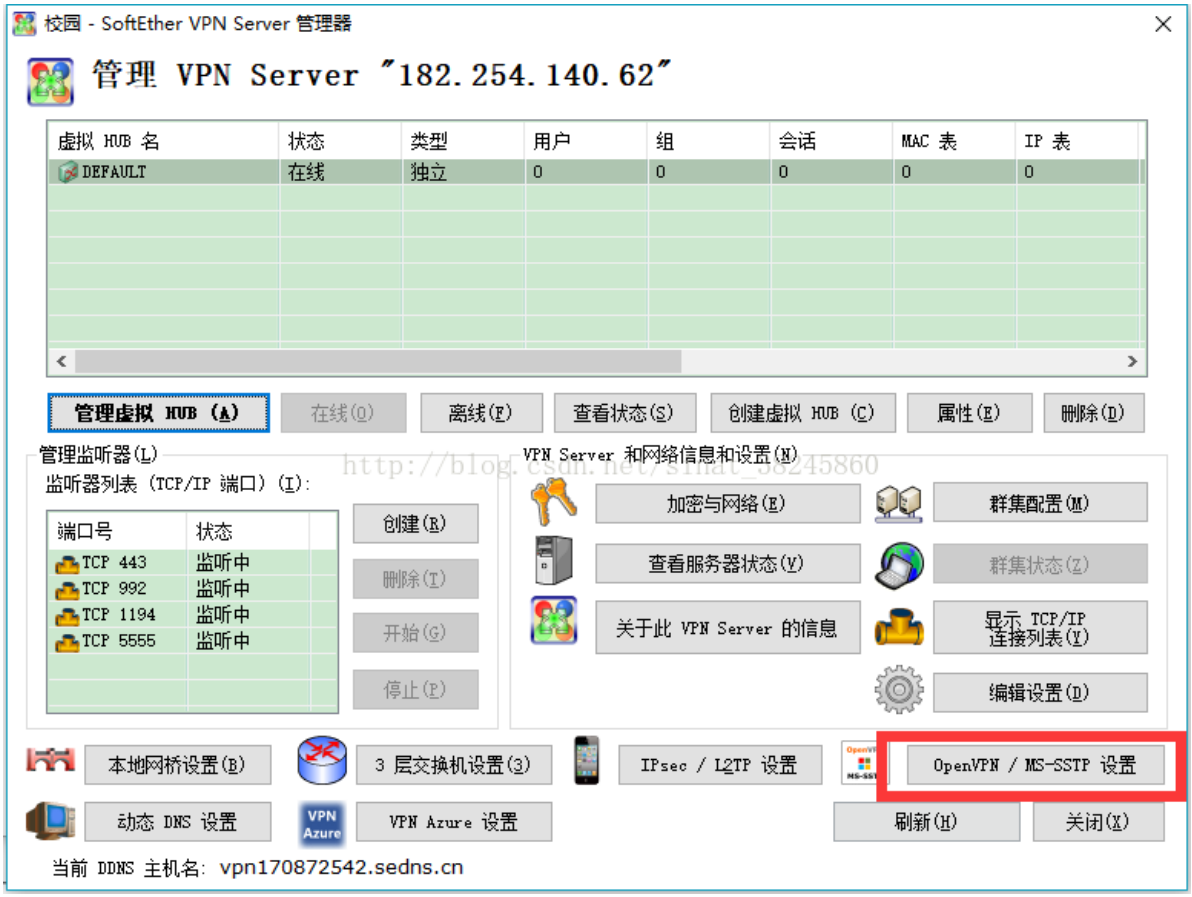
（2）搭建L2TP Over IPSec/PSK

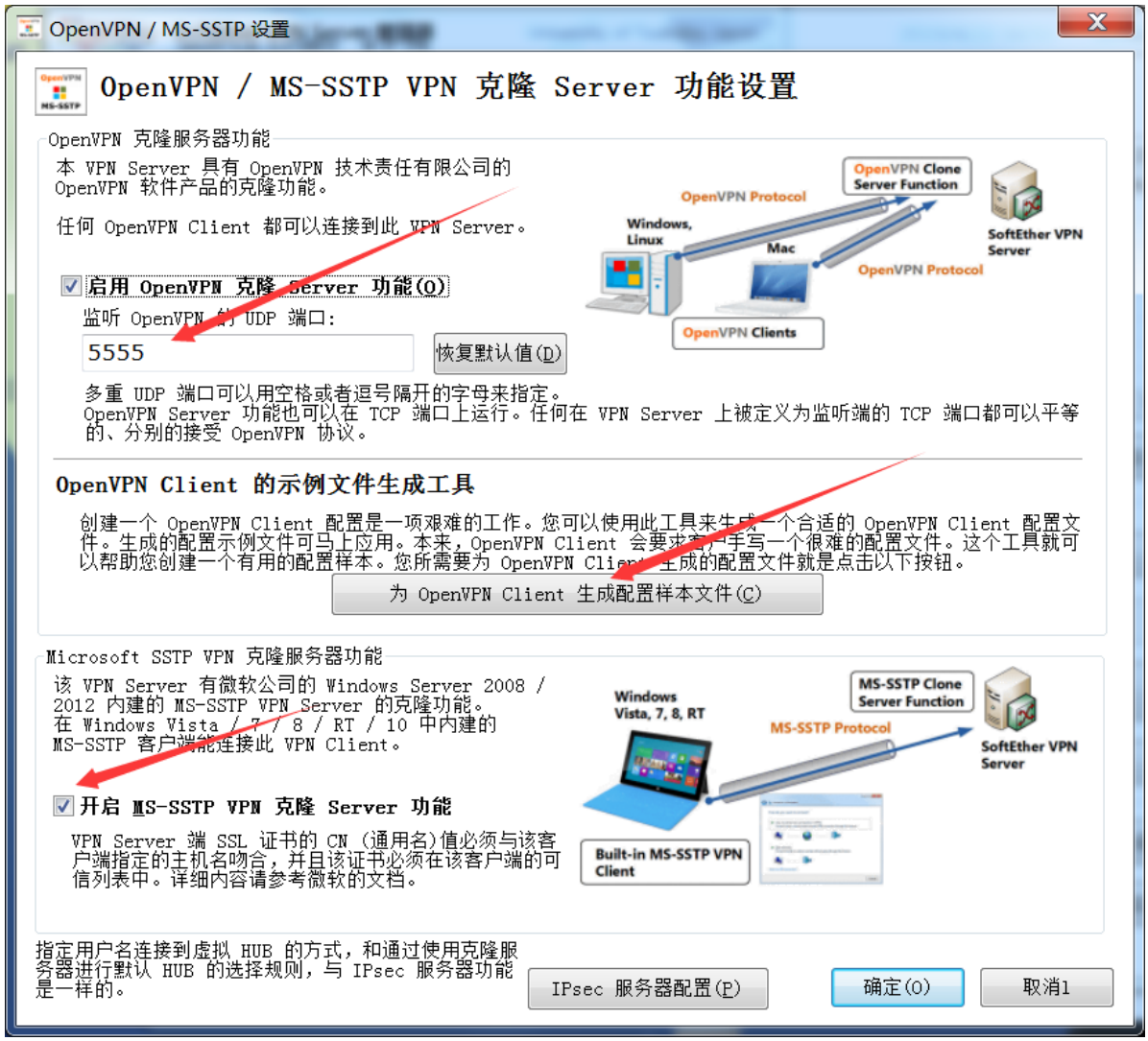
主界面点击 L2TP，勾选全部选项，设置一个预共享密钥（当成 WiFi 密码随意设置）





四、L2TP Over IPSec/PSK的客户端配置方法


校园 - SoftEther VPN Server 管理器
管理 VPN Server "182.254.140.62"
虚拟 HUB 名
状态
类型
用户
组
会话
MAC 表
IP 表
DEFAULT
在线
独立
0
管理虚拟 HUB (A)
在线(O)
离线(F)
查看状态(S)
创建虚拟 HUB (C)
属性(E)
删除(D)
管理监听器(L)
监听器列表 (TCP/IP 端口) (I):
端口号
状态
TCP 443
TCP 992
TCP 1194
TCP 5555
监听中
创建(R)
删除(T)
开始(G)
停止(P)
VPN Server 和网络信息和设置(N)
加密与网络(E)
群集配置(M)
查看服务器状态(V)
群集状态(Z)
关于此 VPN Server 的信息
显示 TCP/IP 连接列表(Y)
编辑设置(D)
本地网桥设置(B)
3 层交换机设置(3)
IPsec / L2TP 设置
OpenVPN / MS-SSTP 设置
动态 DNS 设置
VPN Azure 设置
刷新(H)
关闭(X)
当前 DDNS 主机名: vpn170872542.sedns.cn


OpenVPN / MS-SSTP 设置
OpenVPN / MS-SSTP VPN 克隆 Server 功能设置
OpenVPN 克隆服务器功能
本 VPN Server 具有 OpenVPN 技术责任有限公司的 OpenVPN 软件产品的克隆功能。
任何 OpenVPN Client 都可以连接到此 VPN Server。
OpenVPN Clone Server Function
OpenVPN Protocol
Windows, Linux
Mac
SoftEther VPN Server
OpenVPN Clients
启用 OpenVPN 克隆 Server 功能(O)
监听 OpenVPN 的 UDP 端口:
5555
恢复默认值(D)
多重 UDP 端口可以用空格或者逗号隔开的字母来指定。
OpenVPN Server 功能也可以在 TCP 端口上运行。任何在 VPN Server 上被定义为监听端的 TCP 端口都可以平等的、分别的接受 OpenVPN 协议。
OpenVPN Client 的示例文件生成工具
创建一个 OpenVPN Client 配置是一项艰难的工作。您可以使用此工具来生成一个合适的 OpenVPN Client 配置文件。生成的配置示例文件可马上应用。本来，OpenVPN Client 会要求客户手写一个很难的配置文件。这个工具就可以帮助您创建一个有用的配置样本。您所需要为 OpenVPN Client 生成的配置文件就是点击以下按钮。
为 OpenVPN Client 生成配置样本文件(C)
Microsoft SSTP VPN 克隆服务器功能
该 VPN Server 有微软公司的 Windows Server 2008 / 2012 内建的 MS-SSTP VPN Server 的克隆功能。
在 Windows Vista / 7 / 8 / RT / 10 中内建的 MS-SSTP 客户端能连接此 VPN Client。
MS-SSTP Clone Server Function
Windows Vista, 7, 8, RT
MS-SSTP Protocol
SoftEther VPN Server
Built-in MS-SSTP VPN Client
开启 MS-SSTP VPN 克隆 Server 功能
VPN Server 端 SSL 证书的 CN (通用名)值必须与该客户端指定的主机名吻合，并且该证书必须在该客户端的可信列表中。详细内容请参考微软的文档。
指定用户名连接到虚拟 HUB 的方式，和通过使用克隆服务器进行默认 HUB 的选择规则，与 IPsec 服务器功能是一样的。
IPsec 服务器配置(P)
确定(O)
取消

这里端口要注意：53/67/68，一般都可以，具体自己试一下，不过我推荐大家如果不是有特殊目的，只是单纯使用，可以直接使用之前的5555端口，因为我们至少能够保证5555端口是开放的。

> 在这里有一个坑，请务必保证你的服务器端的UDP 53端口是开放的！！！
>
> DNS的默认协议、端口是UDP 53，因此设置UDP 53端口能够绕过web认证，免验证使用网络。

把得到的文件解压，注意把生成的xxxl3.ovpn文件复制到客户端桌面上方便查找上。

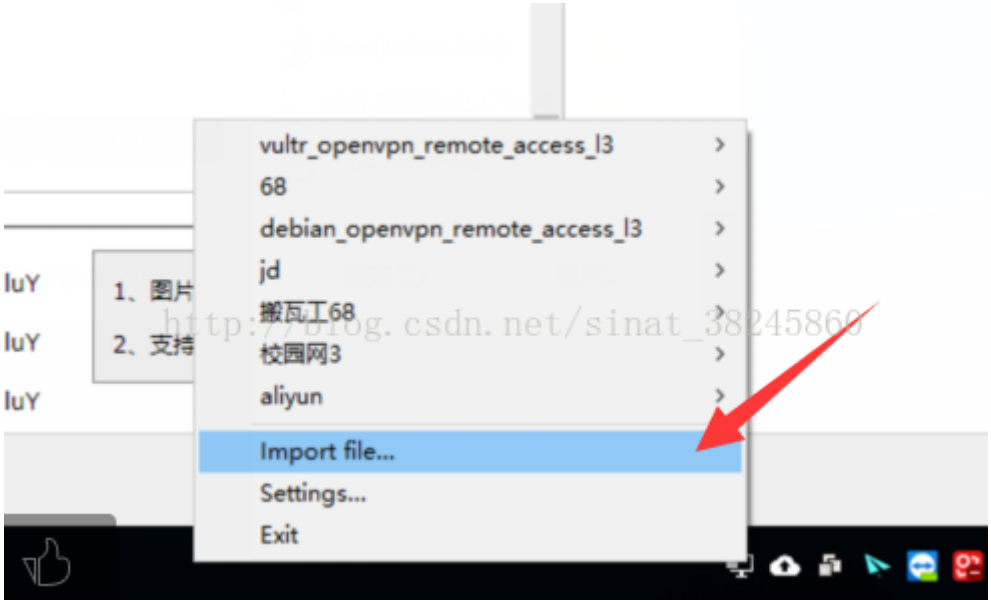
OpenVPN客户端配置方法

OpenVPN 的配置涉及到证书的生成，但是 SoftEther 同样提供了比较方便的服务器、客户端配置方法。
(使用方式可参考此文章 http://www.vpngate.net/cn/howto_openvpn.aspx)

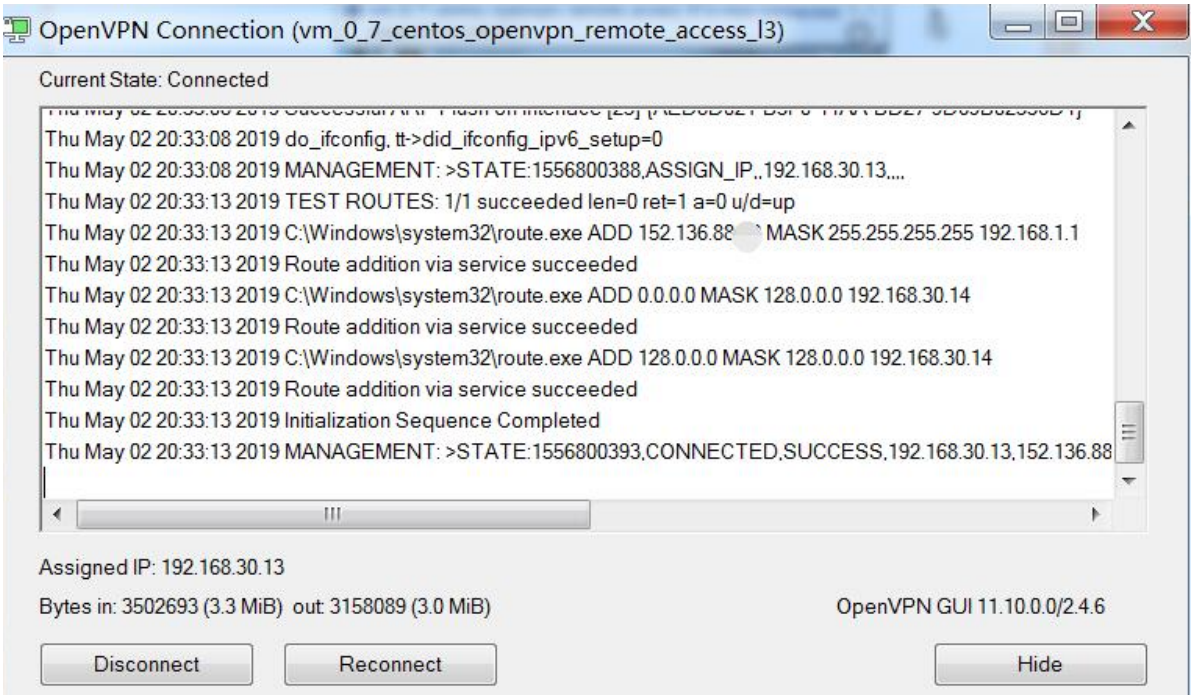
下载并安装 OpenVPN 客户端，建议先修改xl3.ovpn文件，修改成tcp**

```
34  ##############################################################################
35  # Specify the underlying protocol beyond the Internet.
36  # Note that this setting must be correspond with the listening setting on
37  # the VPN Server.
38  #
39  # Specify either 'proto tcp' or 'proto udp'.
40
41  proto tcp
42
```

打开电脑端的openvpn软件 ——>点击 settings ——> Advanced ——> 找到config路径导入xl3.ovpn文件



右下角右键选择Connect ——>输入虚拟 Hub 里设置的一对账号密码 ——> 图标变绿表示成功



五、绕过web认证，免验证使用网络方法