**第二十章 使用softether搭建vpn服务器**

**本节所讲内容：**

**20.1 VPN概述**

**20.2 softether vpn概述**

**20.3 在Linux系统上搭建 VPN服务器**

**20.4 在win7系统安装vpn管理端软件并创建用户**

**20.5 在win7系统上安装vpn客户端软件并连接VPN服务器**

****

**本节所使用实验环境：RHEL 7 （如有使用RHEL 6，会特别注明）**

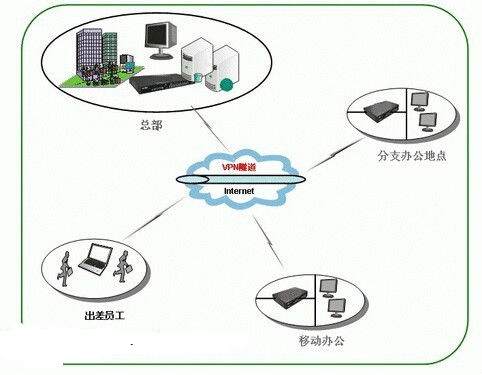
**20.1 VPN概述**

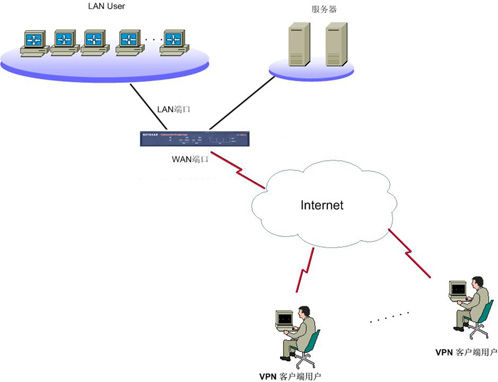
**20.1.1 VPN : Virtual Private Network 虚拟专用网络。**

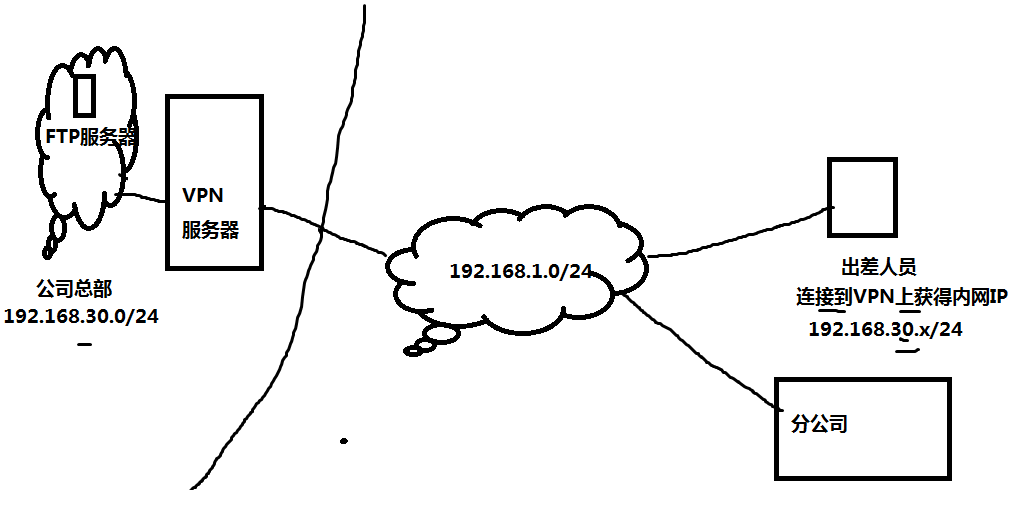
**虚拟专用网络的功能是：在公用网络上建立专用网络，进行加密通信。虚拟专用网络可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用Internet或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。**

**简单地说就是利用公用网络架设专用网络。例如某公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。**

**20.1.2 VPN的作用：**

****



****

**20.1.3 vpn分类：**

**1、按VPN的协议分类：**

**VPN的隧道协议主要有三种，PPTP、L2TP和IPSec，其中PPTP和L2TP协议工作在OSI模型的第二层，又称为二层隧道协议；IPSec是第三层隧道协议。**

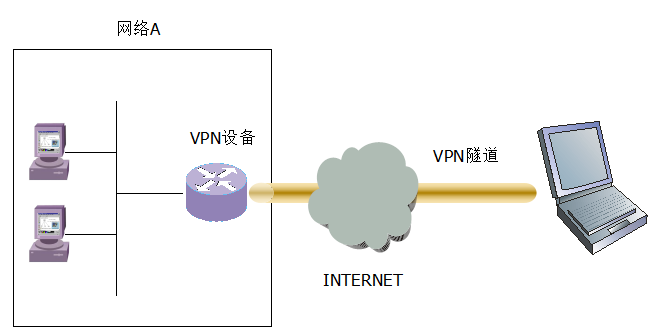
**PPTP（Point to Point Tunneling Protocol），即点对点隧道协议**

**L2TP是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如PPTP要求网络为IP网络，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**

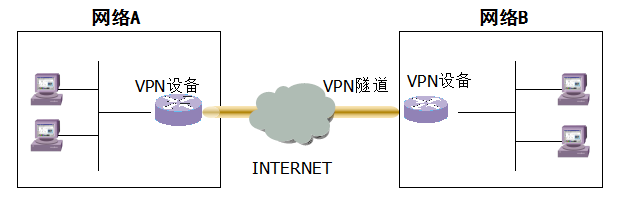
**IPSec（InternetProtocolSecurity） 是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。 在windows领域使用比较多。**

**2、按VPN的应用分类：**

**（1）Access VPN（远程接入VPN）：客户端到网关，即远程访问方式的VPN。它提供了一种安全的远程访问手段，例如，出差在外的员工，有远程办公需要的分支机构，都可以利用这种类型的VPN，实现对企业内部网络资源进行安全的远程访问。**



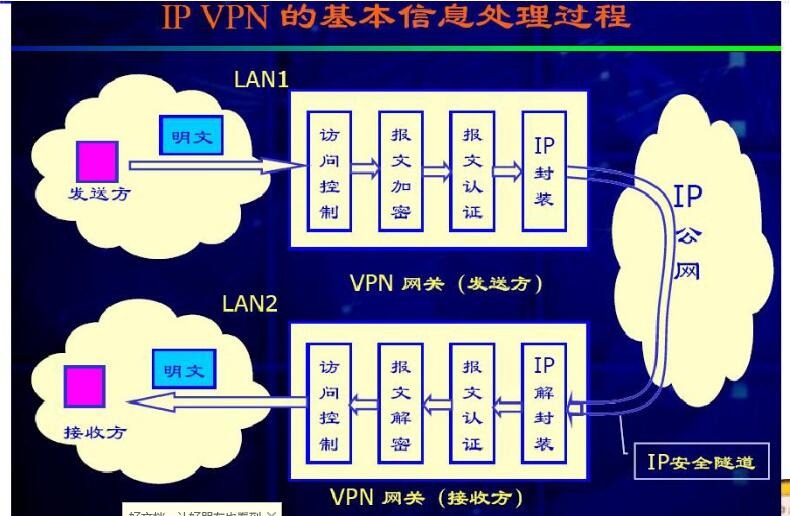
1. **Intranet VPN（内联网VPN）：网关到网关，通过公司的网络架构连接来自同公司的资源；**

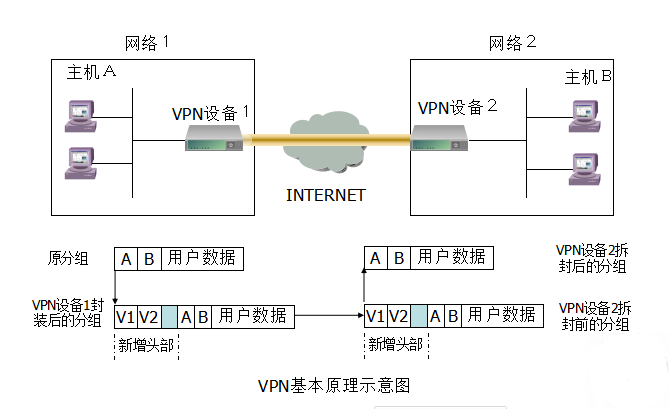


**20.1.4 vpn工作原理：**

**1、VPN网关一般采取双网卡结构，外网卡使用公网IP接入Internet。内网卡接入公司局域网。**

**2、客户端在使用vpn通信时，会先对数据包进行封装，加一个公网的IP，然后发给VPN服务器端，服务端收到数据包后，会拆去包头，还原成原始的数据包，然后进行处理。服务端通信时，也会加包头，再发出去。**

****



**1）主机A建立分组，将其IP地址作为源地址，将主机B的IP地址作为目标地址，将分组发送到VPN设备1，通常是网关。**

**（2）分组到达VPN设备1，VPN设备1在分组中增加一新头。在此分组中，将分组的源IP地址写为自己的IP地址V1，目标地址写为对等VPN设备2的IP地址V2，然后发送。**

1. **分组通过Internet到达VPN设备2，VPN设备2能够识别新增的头部，对其进行拆除，从而得到第1步由主机A生成的原分组，然后根据分组的IP地址信息，进行正常的转发。**

**20.1.5 Linux下常用的VPN软件：**

**1、OpenVPN概述：**

**OpenVPN是一款在Linux网关服务器使用的开源的VPN软件，顾名思义，其实就是用来打通一条安全的虚拟专用通道，实现用户远程办公，获取内网资源。**

**该软件可跨平台在在Linux、xBSD、Mac OS X与Windows间使用，并利用openssl作为加密库，使用加密证书或用户名/密码来实现身份验证，是一款不可多得的开源VPN解决方案。**

**2、SoftEther VPN概述：**

**SoftEther VPN是日本筑波大学的一个研究项目，是一个开放源代码的跨平台多协议VPN程序，它包括服务器端、客户端、服务器端管理工具等数个软件，支持 SSL-VPN (SoftEther VPN) 协议、 L2TP/IPsec 协议、 OpenVPN 协议和 Microsoft SSTP 协议，Windows、Linux、Android和IOS等操作系统都可以连接到SoftEther VPN服务器。**



**是日本大学。**

**http://www.tsukuba.ac.jp/chinese/**

**日本最有名的大学是什么大学？你看过的最多日本教材是什么？**

**有看过av大学的教材的同学：1 没有：2**

**一般大学4年毕业， 有的同学可能在av大学进修10年以上了。。。对吧？**

**苦海无边，回头是岸**

S{UMW`K@OQ0}9])9M5RTPN0

**20.2 实战：翻墙浏览墙外风景**

**20.2.1 运行一台腾讯云主机，可以访问外网的云主机**

**我们这里方便大家操作，直接在虚拟机上操作，系统：centos7.4上搭建**

**1、在云服务供应商申请一台云主机 qcloud.com**



**最好使用国外的云主机！**

**2、然后使用x-shell连接云主机，登陆后，使用root账户操作。**

**我这里直接本地虚拟机。**

**3、安装依赖库**

**yum -y install gcc zlib-devel openssl-devel readline-devel ncurses-devel**

**4、依赖库安装完成后，我们在安装softether server.**

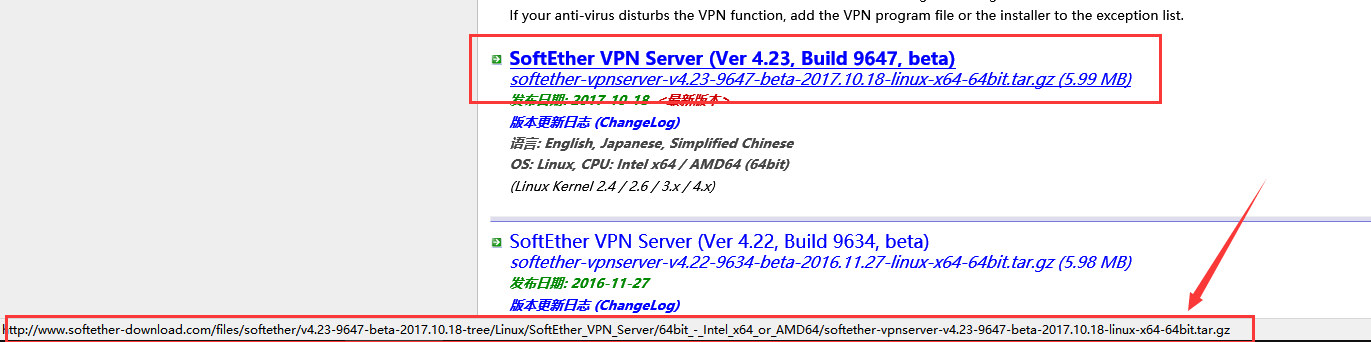
**登陆官网下载最新版本**

**<http://www.softether.org/5-download>**

****

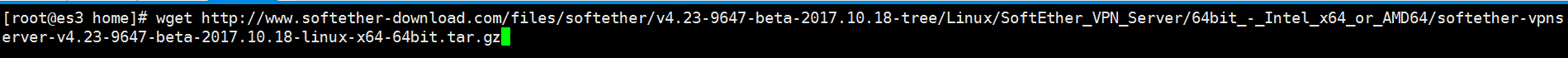
****

**这一步很关键，千万不要选择错了，不然下载的版本可能与系统不匹配，**

**点击鼠标右键，复制快捷方式。**

**<http://www.softether-download.com/files/softether/v4.23-9647-beta-2017.10.18-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.23-9647-beta-2017.10.18-linux-x64-64bit.tar.gz>**

**然后，切换到X-SHELL，输入**

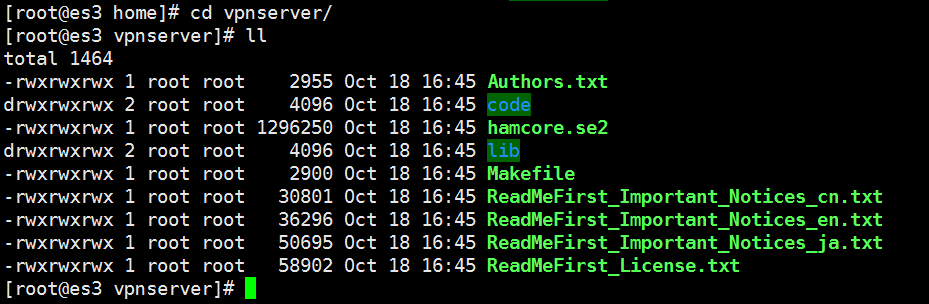
****

****

**5、下载好了，解压**

**[root@xuegod63 ~]# tar zxvf softether-vpnserver-v4.20-9608-rtm-2016.04.17-linux-x64-64bit.tar.gz**

****

****

**6、安装**

**[root@VM\_113\_253\_centos vpnserver]# make**

**--------------------------------------------------------------------**

**SoftEther VPN Server (Ver 4.20, Build 9608, Intel x64 / AMD64) for Linux Install Utility**

**Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Reserved.**

**--------------------------------------------------------------------**

**Do you want to read the License Agreement for this software ?**

**1. Yes**

**2. No**

**Did you read and understand the License Agreement ?**

**(If you couldn't read above text, Please read 'ReadMeFirst\_License.txt'**

**file with any text editor.)**

**1. Yes**

**2. No**

**Please choose one of above number: 1**

**Did you agree the License Agreement ?**

**1. Agree**

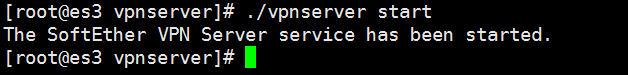
**2. Do Not Agree**

**Please choose one of above number: 1**

**或：**

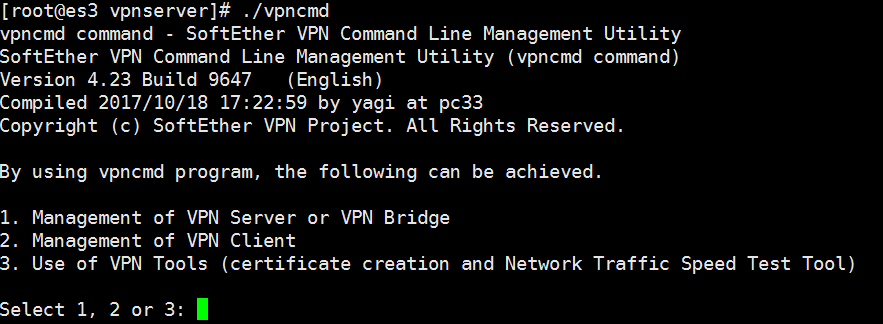
**# make i\_read\_and\_agree\_the\_license\_agreement**

**7、启动**

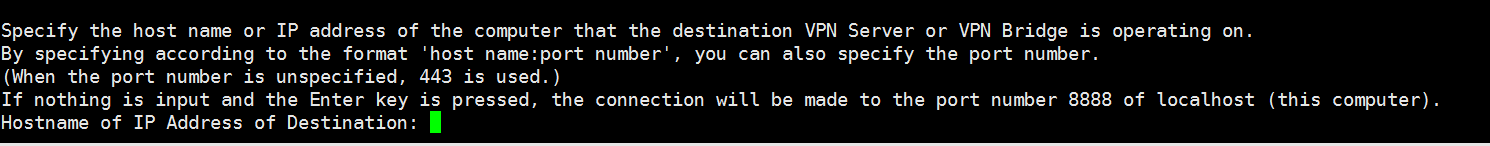
****

**8、设置管理员密码**

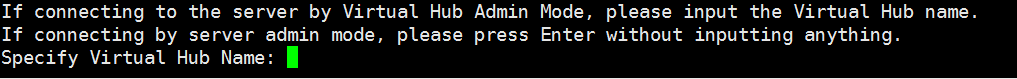
**输入./vpncmd**

****

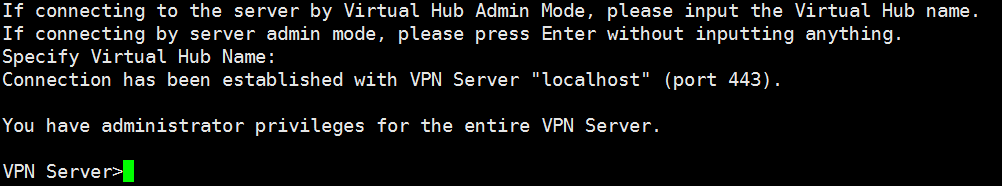
**选择1，回车**

****

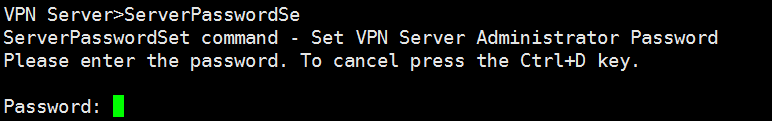
**这步直接回车**

****

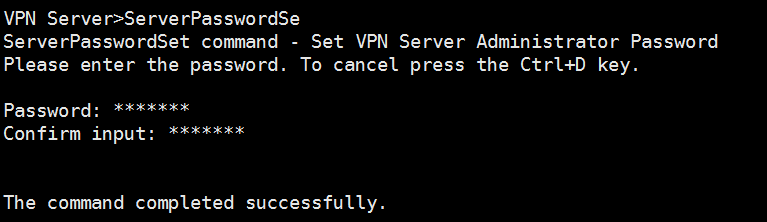
**这步也是直接回车**

****

**输入ServerPasswordSet设置VPN管理员密码（区分大小写）**

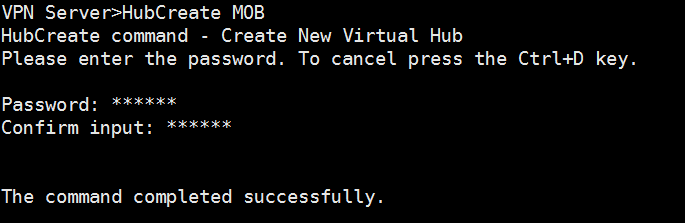
****

**输入两遍完成密码设置。**

****

**9、创建虚拟HUB**

**输入HubCreate MOB ,同时设置连接管理密码**

****

**VPN Server>exit**

**这样服务端设置就好了，**

**扩展：虚拟HUB概述**

**虚拟HUB就是我们的虚拟局域网**

**"softether"该软件是一个能虚拟网卡和集线器（HUB）的工具，只要可以访问互联网，都可以使用它来组建远程局域网。在此虚拟的局域网上能进行所有物理局域网上的操作。可以互相访问，可以联网玩只支持局网的游戏（TCP/IP）。该软件能够突破防火墙拦截，信息包都经过加密，安全上不存在问题。  
 　　SoftEther分为虚拟集线器(HUB)和虚拟网卡两部分，使用服务器/客户端的方式工作，虚拟集线器就是服务器，虚拟网卡就是客户端。连接时利用SoftEther提供的连接管理工具将虚拟网卡连接到远端的虚拟集线器上，这样你的计算机就相当于与该虚拟集线器上连接的其他计算机处于同一个局域网之内。**

**20.3 使用windows环境下的远程管理工具vpnsmgr.exe，来管理vpn服务器**

**21.3.1设置vpn客户端用户登录密码**

**这里需要用到的一个工具**

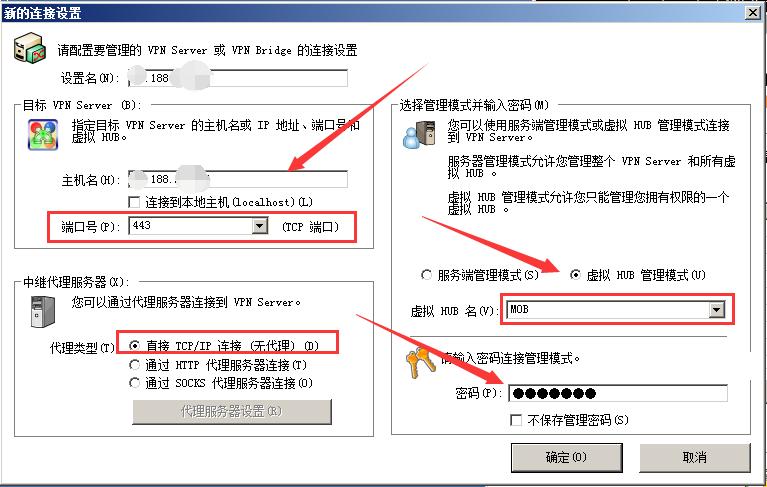
**1、解压文件后运行vpnsmgr.exe**

**2、点击【新设置】**

****

**3、在目标VPN Server的主机名输入服务器IP，端口号默认443，中继代理服务器选择TCP/IP连接，如果有代理的话，可以选择自己对应的代理服务类型，填写相关的服务器IP，端口 ，用户名，密码；**

**选择管理模式并输入密码，点击【虚拟HUB管理模式】，虚拟HUB名选择之前在服务器建好的名称，之前建立的名称是MOB，然后输入连接管理密码，【确定】。**

****

**在管理器界面，点击【连接】。**

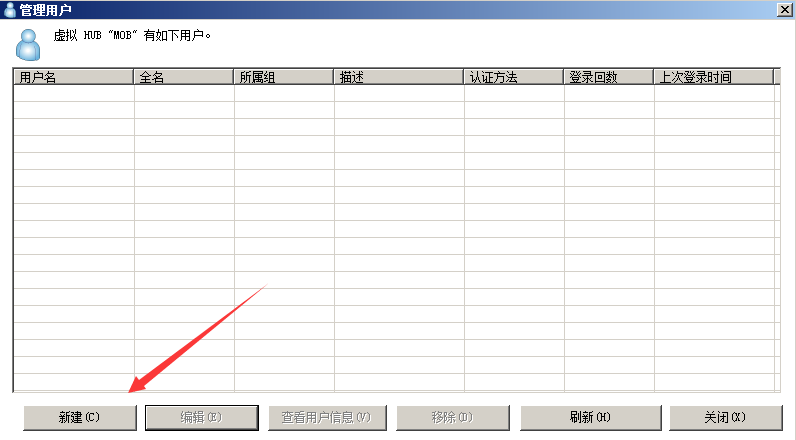
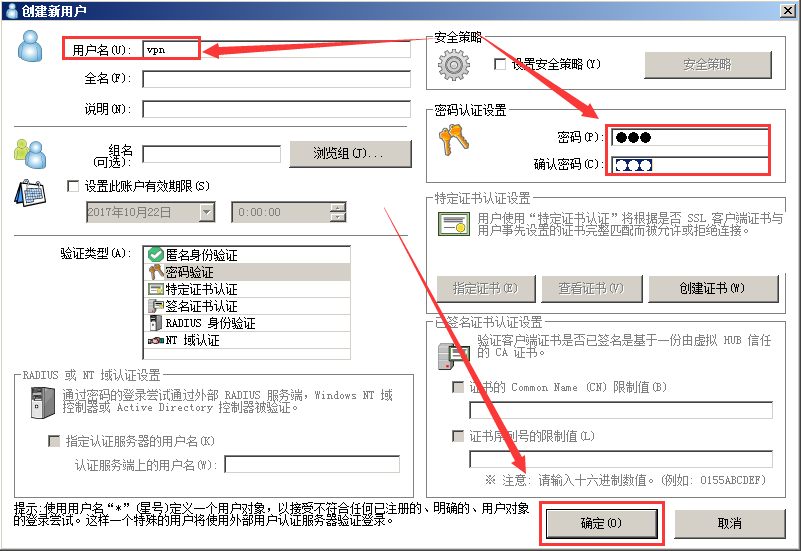
****

**在弹出的界面点击【管理虚拟HUB】**

****

**在弹出的管理虚拟HUB-MOB界面，点击【管理用户】，【新建】==》，输入用户名，密码，【确定】。**

**提示 “用户vpn已创建”。这样就把客户端登录的用户名和密码建立好了。**

**  **

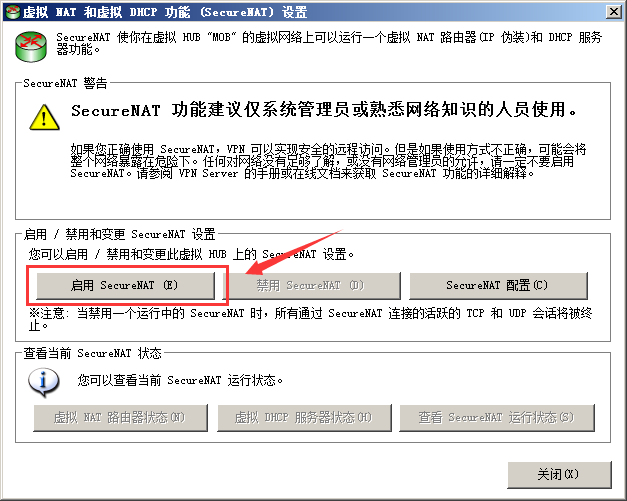
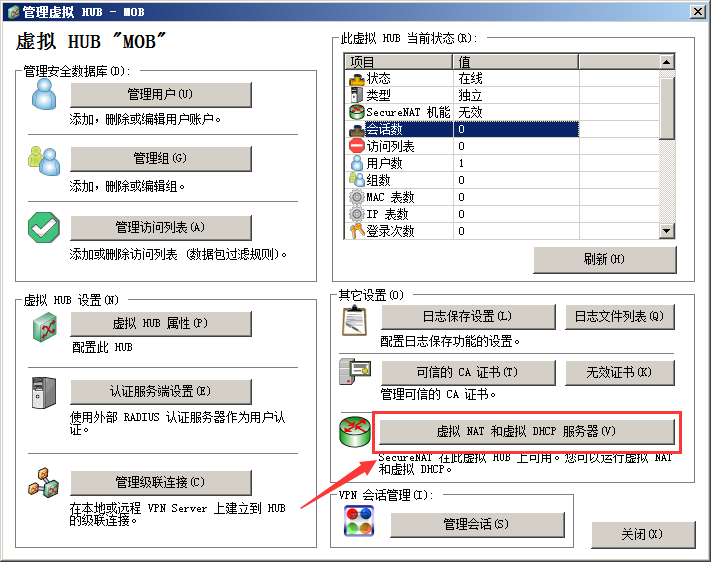
****

**5、启动SecyreNAT，开启NAT转换和DHCP服务**

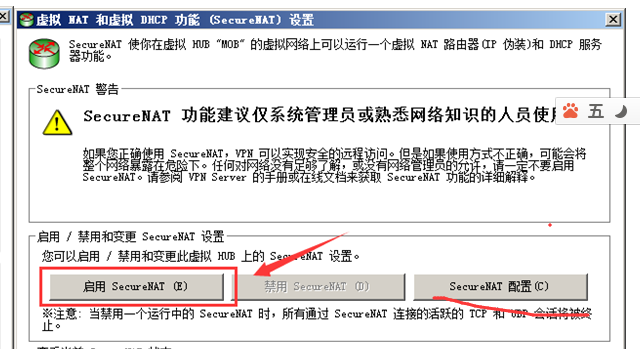
**在使用客户端登录之前，还有很关键的一步，就是需要启动SecyreNAT服务。**

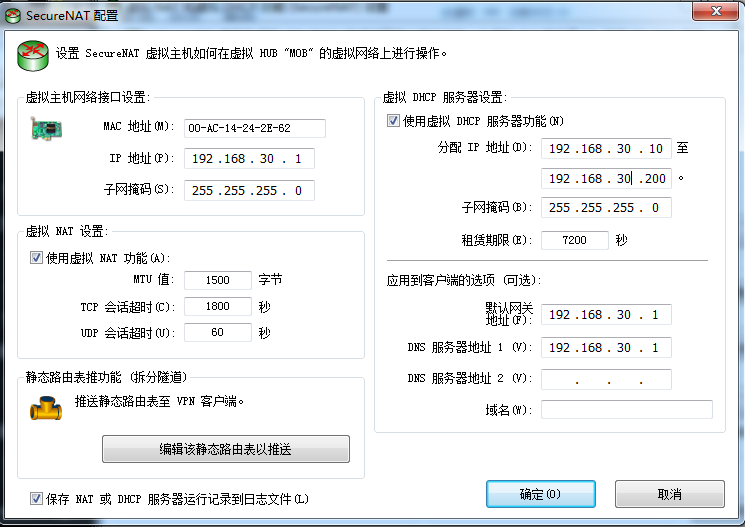
**在管理虚拟HUB-MOB界面，点击【虚拟NAT和虚拟DHCP服务器】，在弹出的设置界面点击【启用secyreNAT】即可。**

**选择“虚拟NAT和虚拟DHCP服务器”，然后选择“启用SecureDHCP”；再选择“SecureDHCP配置”。**

****

**也可以设置属性：**





**20.4 用户使用VPN Client登录VPN，访问内网并可以上网**

**20.4.1 客户端登录**

**1、这里需要下载SoftEther VPN Client 管理工具，访问<http://www.softether-download.com/cn.aspx?product=softether>**

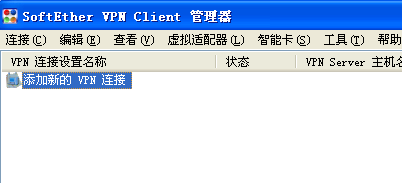
****

**2、下载好了后安装，运行SoftEther VPN Client 管理工具。双击安装，并选择： softether vpn client**



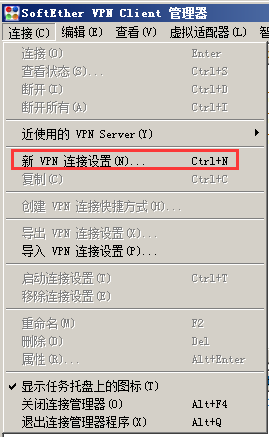
****

**3、创建新的VPN连接，运行softetheer vpn client工具：**

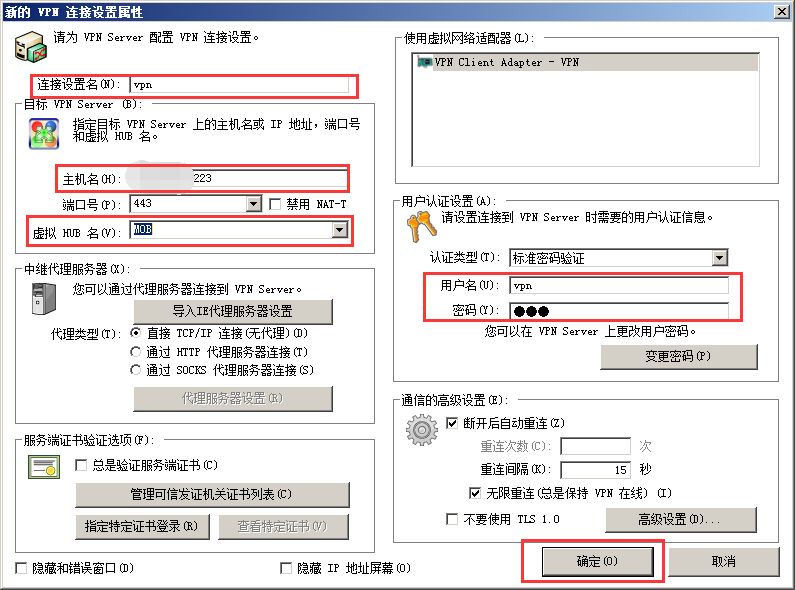


**双击新新建一个网卡设备文件。**

**然后，选中后，右击，选择 新VPN连接设置向导**

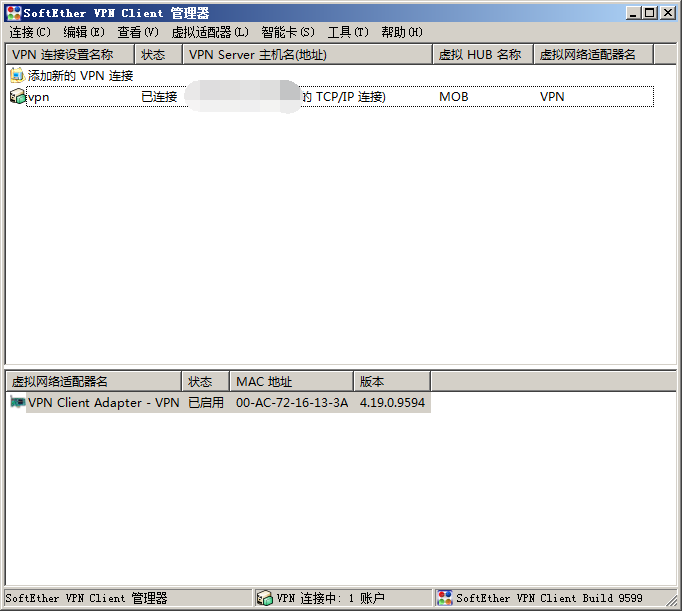
****

**4、设置VPN相关参数:**

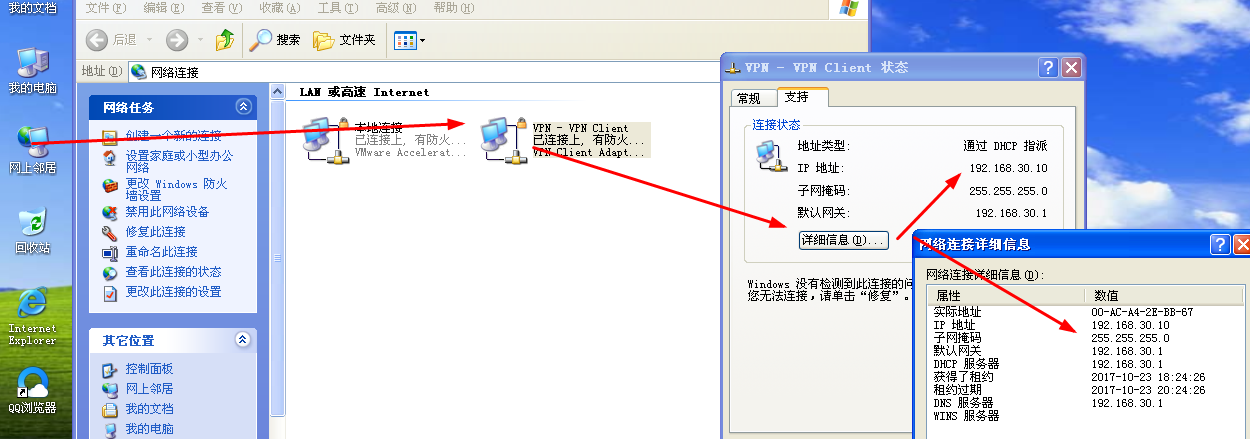
****

**5、连接VPN服务器:**

**在管理器界面,双击刚才新建好的VPN连接，提示VPN会话已建立。这样就成功登陆上VPN服务器了，开始潇洒的浏览墙外风景吧。**

****

**20.4.2 查看获得的IP地址：**

****

**总结：**

**1、VPN概述**

**2、softether vpn概述**

**3、在Linux系统上搭建 VPN服务器**

**4、在win7系统安装vpn管理端软件并创建用户**

**5、在win7系统上安装vpn客户端软件并连接VPN服务器**