中神通大地
EDR&DNS&URL&VPN
云控管系统
用户指南

武汉中神通信息技术有限公司

目录

免责声明/Disclaimers

请合法使用本软件，因违法使用而产生的责任与本软件及其开发者无关。

Please use this software legally, the responsibility of illegal use has nothing to do with the developer.

1 DNS 服务器设置

1.1 Windows 10 系统下的 DNS 设置

Windows DNS 服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/network/windows_dns.html

1）打开“网络连接”窗口，选择与网络相连的网卡，打开其“属性”窗口，如图 1-1 所示。

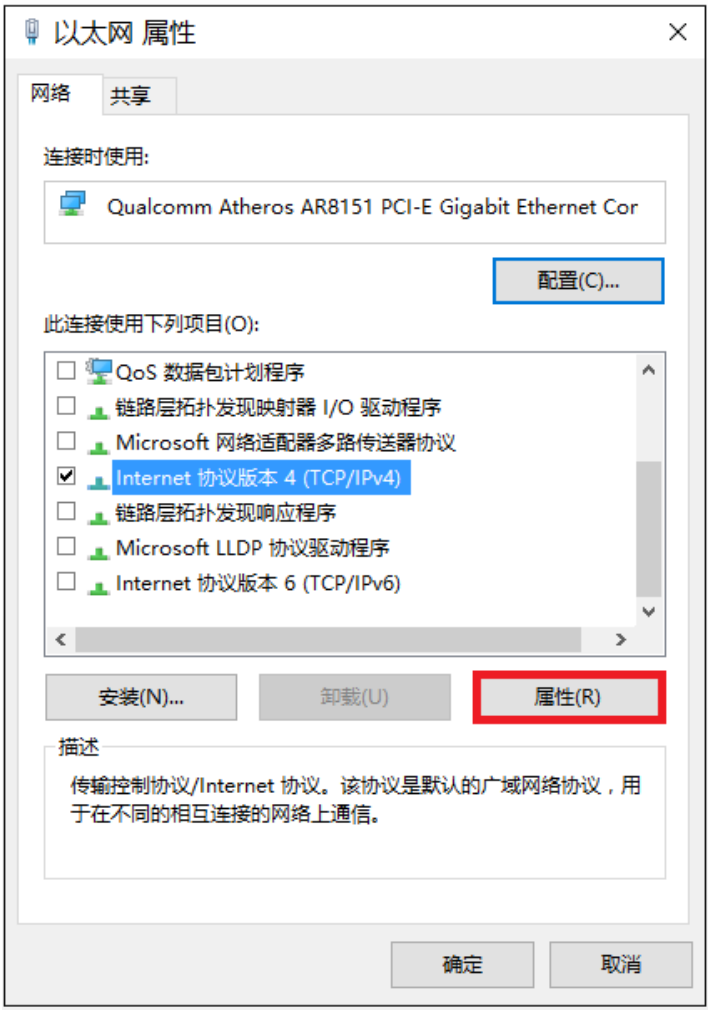


图 1-1 网卡的属性窗口

2）选择“Internet 协议 4（TCP / IPv4）”项，出现 TCP / IP 属性窗口，如图 1-2 所示。

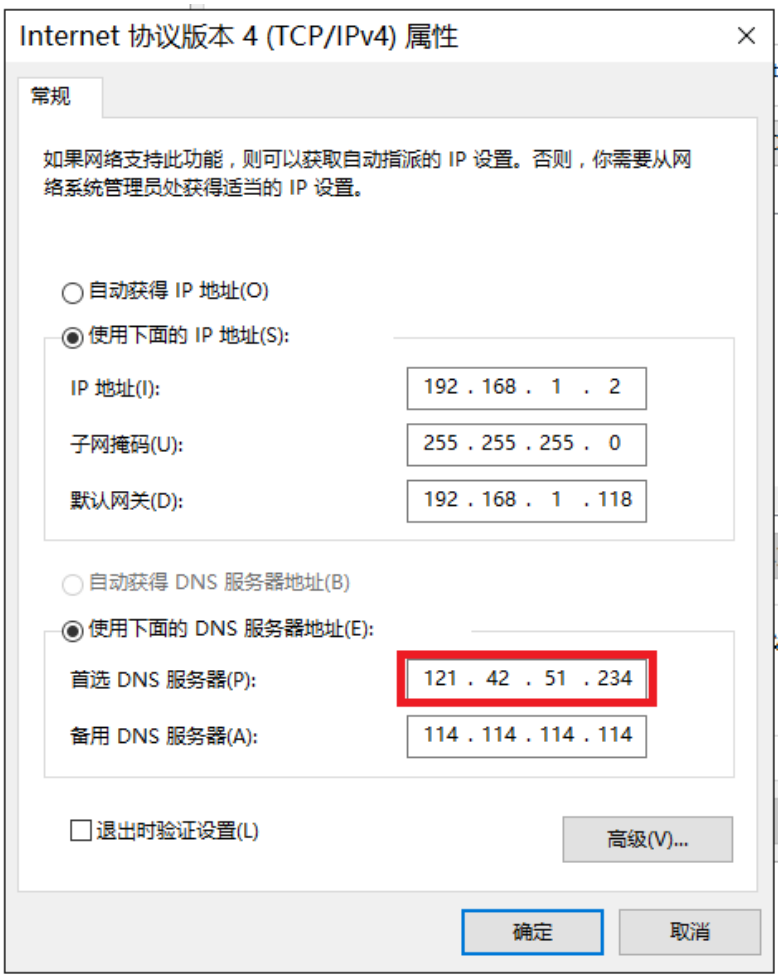


图 1-2 TCP / IP 属性窗口

DNS 服务器地址可以通过 DHCP 方式获得，也可以手工指定多个有效的 DNS 服务器地址，Windows 按先后顺序查询域名。某些时候，默认网关也提供 DNS 服务，则 DNS 服务器地址之一就是默认网关的地址，但这要得到管理员的确认。

3）在 DOS 窗口中，运行 ipconfig/all 命令，确认当前网络配置生效，如图 1-3 所示。

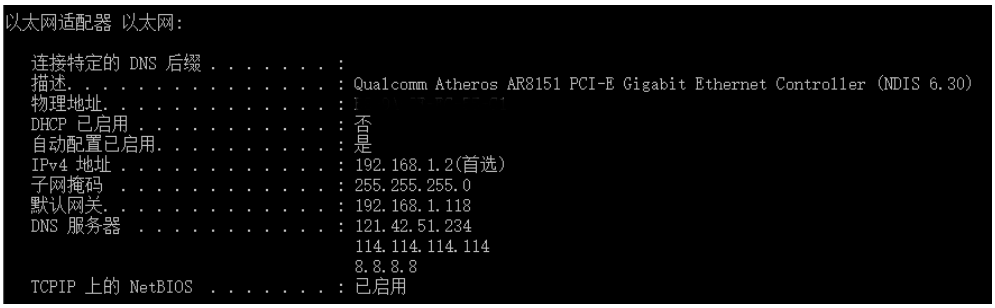


图 1-3 ipconfig/all 命令输出

4）在 DOS 窗口中，运行 nslookup www.baidu.com 命令，及运行 nslookup hm.baidu.com 命令，确认当前 DNS 服务器配置生效，如图 1-4 所示。

图 1-4 nslookup 命令输出

用户在遇到网络不通等故障时，请先运行 ping [网关 IP]，netstat -nr（查看路由），tracert（跟踪路由），telnet（查看 TCP 端口连通性）等。

注意：

1）使用 DNS 服务器上 Google 等国外网站时，URL 需要加 https://，类似：https://www.google.com

2）为防止用户更改 DNS 服务器 IP，可以以管理员的身份添加普通账号，让用户以普通账号使用 Windows

1.2 Android 系统下的 DNS 设置

安卓系统 DNS 服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/network/android_dns.html

1.2.1 安卓系统 WIFI 下 DNS 设置

打开安卓系统的“设置”界面，选择“WLAN”栏目，如果之前已有建立的无

线连接，可以长按该连接名称，选择“修改网络”，如图 1-5-1 所示。

图 1-5-1 安卓系统修改已有的无线连接

对于新连接，输入密码，再勾选“显示高级选项”，选择“IP”类型为“静态”，填写正确的“IP 地址”、“网关”和“域名 1”等值，再点击“连接”按钮即可。如图 1-5-2 所示。

图 1-5-2 安卓系统设置 WIFI 下 DNS 服务器设置

参考：http://jingyan.baidu.com/article/8ebacdf0cae95649f75cd57c.html

1.2.2 安卓系统 WIFI 及数据流量下 DNS 设置

不 root，不改 hosts 文件，安装第三方 APP 或 VPN 拨号可以实现修改 DNS 服务器。

下载安装 DNS Changer APP（有广告），地址是：

https://play.google.com/store/apps/details?id=com.burakgon.dnschanger

https://apkpure.com/dns-changer-mobile-data-wifi-ipv4-ipv6/com.burakgon.dnschanger

或者下载安装 dnspipe（无广告），地址是：

https://play.google.com/store/apps/details?id=com.frostnerd.dnschanger

https://apkpure.com/dnspipe-an-ipv4-ipv6-dns-changer-without-root/com.frostnerd.dnschanger

为了避免 53 端口的 DNS 劫持、污染、上网审计，可以使用非 53 端口服务器，需要在 dnspipe APP 的“设置>高级设置”里启用“自定义端口”选项，再在服务器地址栏中输入“120.92.16.207:666”这样的 IP 及端口字符串，再点击“开始”按钮，如下图 1-6 所示。

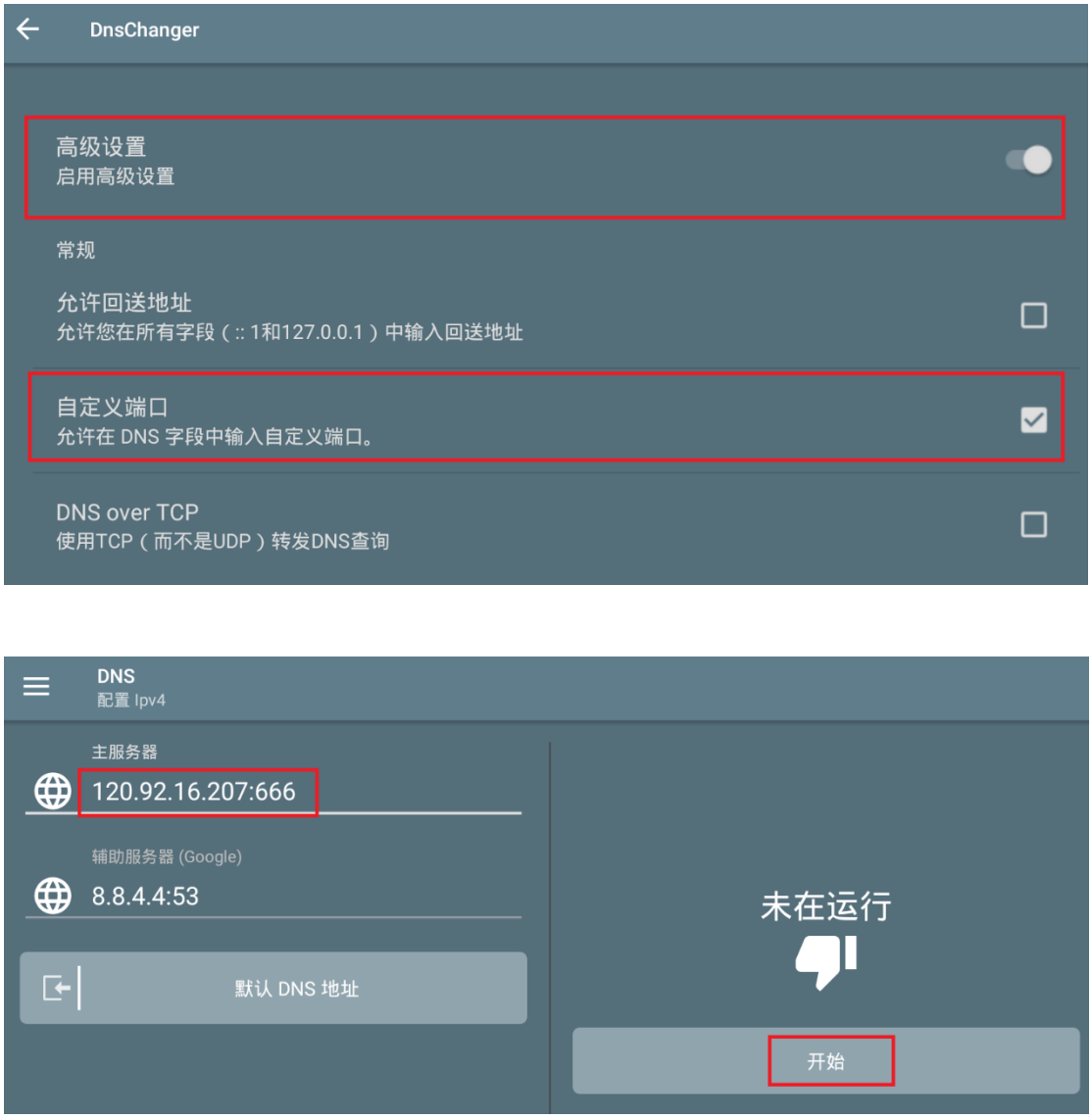


图 1-6 安卓系统设置 WIFI 及数据流量下 DNS 服务器设置

另外，还可以通过连接一个特殊设置的 VPN 服务器，实现在 WIFI 及移动网

络数据流量下修改 DNS 服务器的目的，该 VPN 服务器不做上网网关用，只是分配 DNS 服务器，所有流量仍然走原来的网络。DNS Changer 和 dnspipe APP 就是连接虚拟的本机 VPN 服务器，实际用来设置 DNS 服务器。

为了在重新打开系统时 VPN 不中断,DNS 服务器仍能用,需要在电池设置中，启用“休眠时始终保持网络连接”选项。

1.2.3 安卓 9+系统下加密 DNS 设置

DNS over TLS（DOT）使用 853/TCP 端口，客户端使用时，先由系统 DNS 服务器解析 DOT 加密服务器域名，之后再用 DOT 服务器解析所有域名。Android 9 及以上的版本，你可以前往“设置>更多连接>加密 DNS”（与只修改 WIFI 的 DNS 服务器不同),选择“指定加密 DNS 服务”(部分设备上可能被命名为:私人 DNS)，输入服务器的域名 即可，如图 1-7 所示。

例如:

中神通：ipv4.ddns.group

阿里云：dns.alidns.com

谷歌 ： dns.google.com

IBM ： dns.quad9.net

红鱼 ： dns.rubyfish.cn

注意：连接麦当劳、肯德基等公共 WIFI 时，需要额外的 WEB 认证，要事先停用“加密 DNS”，WEB 认证过后，可以再启用“加密 DNS”。

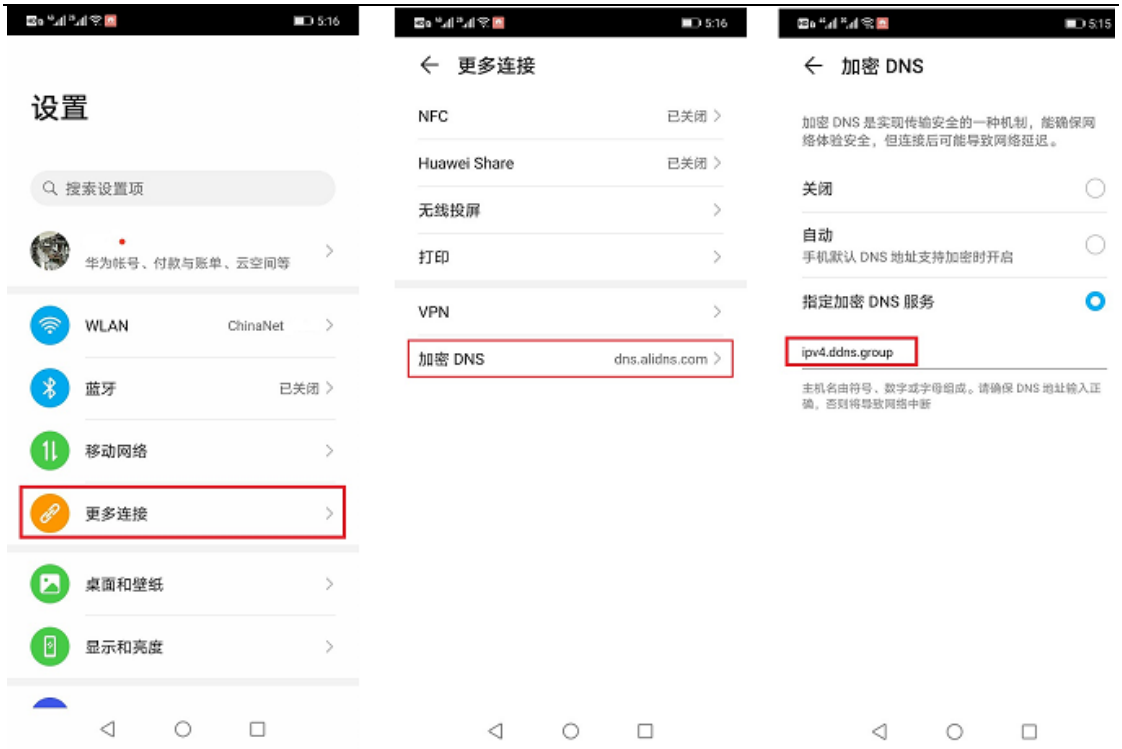


图 1-7 安卓系统设置加密 DNS

1.3 iOS 系统下的 DNS 设置

iOS 系统 DNS 服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/network/ios_dns.html

1.3.1 iOS 系统 WIFI 下 DNS 设置

在“设置”界面中，选择“无线局域网”栏目，点击现有的无线连接，在右边的“IP 地址”栏中，修改“DNS”项为正确的值即可。如图 1-8 所示。

图 1-8 iOS 系统 WIFI 下设置 DNS 服务器

1.3.2 iOS 系统 WIFI 及数据流量下 DNS 设置

不 root，不改 hosts 文件，安装第三方（DNS Change）APP 或 VPN 拨号可以实现修改 DNS 服务器。

可以通过连接一个特殊设置的 VPN 服务器，实现在 WIFI 及移动网络数据流量下修改 DNS 服务器的目的，该 VPN 服务器不做上网网关用，只是分配 DNS 服务器，所有流量仍然走原来的网络。

2 WEB 在线代理

WEB 在线代理使用示例

http://www.trustcomputing.com.cn/help/cn/dadi/proxy/online_proxy.html

2.1 使用 WEB 在线代理

WEB 在线代理不需要事先做设置，直接打开浏览器就可以用，如图 2-1 所示，再在输入框中输入网址，点击“Go”按钮，就可以浏览。可以在 WEB 在线代理界面中输入下载链接，再配合 IDM 下载，这样可以不用在 IDM 中设置代理服务器。

HTTP 协议缺省有两个端口可以用，一个是 80，另一个是 99（可修改），URL 类似“http://121.42.51.234/www”，或者“http://121.42.51.234:99/www”。

HTTPS 协议缺省有两个端口可以用，一个是 443，另一个是 100（可修改），URL 类似“https://121.42.51.234/www”，或者“https://121.42.51.234:100/www”。

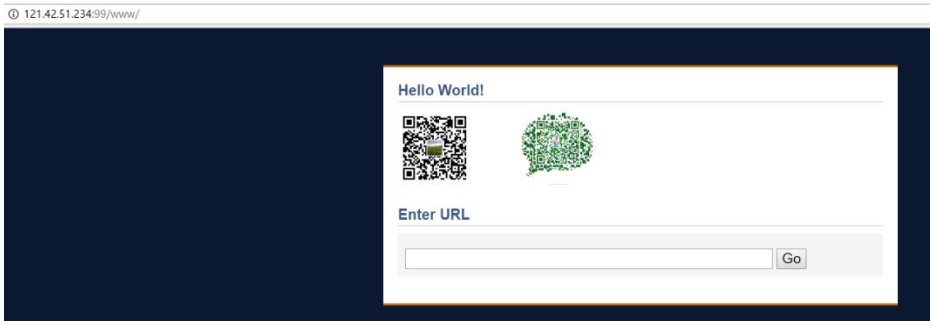


图 2-1 WEB 在线代理界面

另外一个使用方法是直接指定网址浏览，URL 类似“http://121.42.51.234:99/www/index.php?jump=https://www.google.com”。

如果无法正常浏览（输入 URL 后无反应或无限循环但是不显示内容），可以清除浏览器缓存及 Cooike 再试。

如有乱码，请切换浏览器的编码，Chrome 浏览器可以下载安装“Set Character Encoding”插件，下载地址是 https://chrome.google.com/webstore/detail/set-character-encoding/bpojelgakakmcfmjfilgdlmhefphglae

对于 https 类型的 URL，而且服务器地址没有真实域名证书时，只能使用自签名证书，缺省 CommonName/Subject Alternative Name/SAN 是“zstdadi.com”，还需要在浏览器中导入自签名 CA 根证书，才能消除使用

https 链接时的证书安全提示，具体参见以下内容。

某些网站 https 证书配置错误或已被撤消（https://mawenjian.net/），无法使用 chrome 浏览器直接查看，可以使用 WEB 在线代理强制查看。

2.2 导入 CA 证书

对于 https 类型的 URL（WEB 用户门户），而且服务器地址没有真实域名证书时，只能使用自签名证书，可以通过 WEB 用户门户资源页面、电子邮件、聊天软件、U 盘等方式得到自签名 CA 证书，也可以通过在线下载的方式得到，URL 类似 http://121.42.51.234/myca.crt，需要输入用户名和（初始）密码。

不同应用对于服务器证书认证的情形不一样，有的必须满足“服务器地址”和服务器证书的 CommonName/Subject Alternative Name/SAN 一致，否则不能连接，例如：Windows 文件管理器挂载 WebDAV、SSTP VPN、IKEV2 VPN，有的可以选择忽略警告继续连接(可能会受到中间人攻击)，具体情形详见下表：

✔代表强制检查，✘代表非强制

	OS 及应用	说明
DNS over TLS（DOT）	✔	安卓系统必须用正式 CA 证书，Linux 系统可以用自签名 CA 证书
WebDAV	✔ Windows 文件管理器	其它应用非强制，有的应用，例如 winscp，没有警告；有的有警告，但是可以选择忽略继续连接
WEB 在线代理等其它 https URL	✘	有警告，但是可以选择忽略继续连接
HTTP 代理+解密 HTTPS	✔	只能使用自签名 CA 证书

IKEV2 VPN	✔ 所有 OS 应用	
OCSERV VPN	✘	有警告，但是可以选择忽略继续连接
PPTP VPN	✘	没有证书认证功能
OpenVPN	✘	服务器和客户端的 CA 证书必须一致，但对“服务器地址”没有要求
SoftEther VPN	✘	可选服务器证书验证
RAW L2TP VPN	✘	没有证书认证功能
L2TP/IPSEC VPN	✔	和 IKEV2 VPN 要求一样
SSTP VPN	✔Windows 内置 VPN 拨号	

2.2.1.1 Windows 系统的证书导入

IE/Chrome 浏览器、WebDAV 服务以及 IKEV2/OCSERV/SSTP VPN 等软件使用 Windows 系统内置的证书。

1）使用 certutil 命令行方式导入证书

管理员：certutil -addstore root C:\Users\xxx\Downloads\myca.crt

普通用户：certutil -user -addstore root C:\Users\xxx\Downloads\myca.crt

2）交互式方式导入

双击 myca.crt 证书文件，出现“证书”窗口，如下图 2-2 所示。

图 2-2 “证书”窗口

点击“安装证书”按钮，出现“证书导入向导”窗口 1，如下图 2-3-1 所示。

图 2-3-1 “证书导入窗口” 1

“存储位置”一定要选择“**本地计算机**”项，否则在 IKEV2 拨号中，会出现“IKE 身份验证凭证不可接受”的错误；HTTPS 代理显示“ERR_PROXY_CERTIFICATE_INVALID”错误。再点击“下一步”按钮，出现“证书导入向导”窗口 2，如下图 2-3-2 所示。

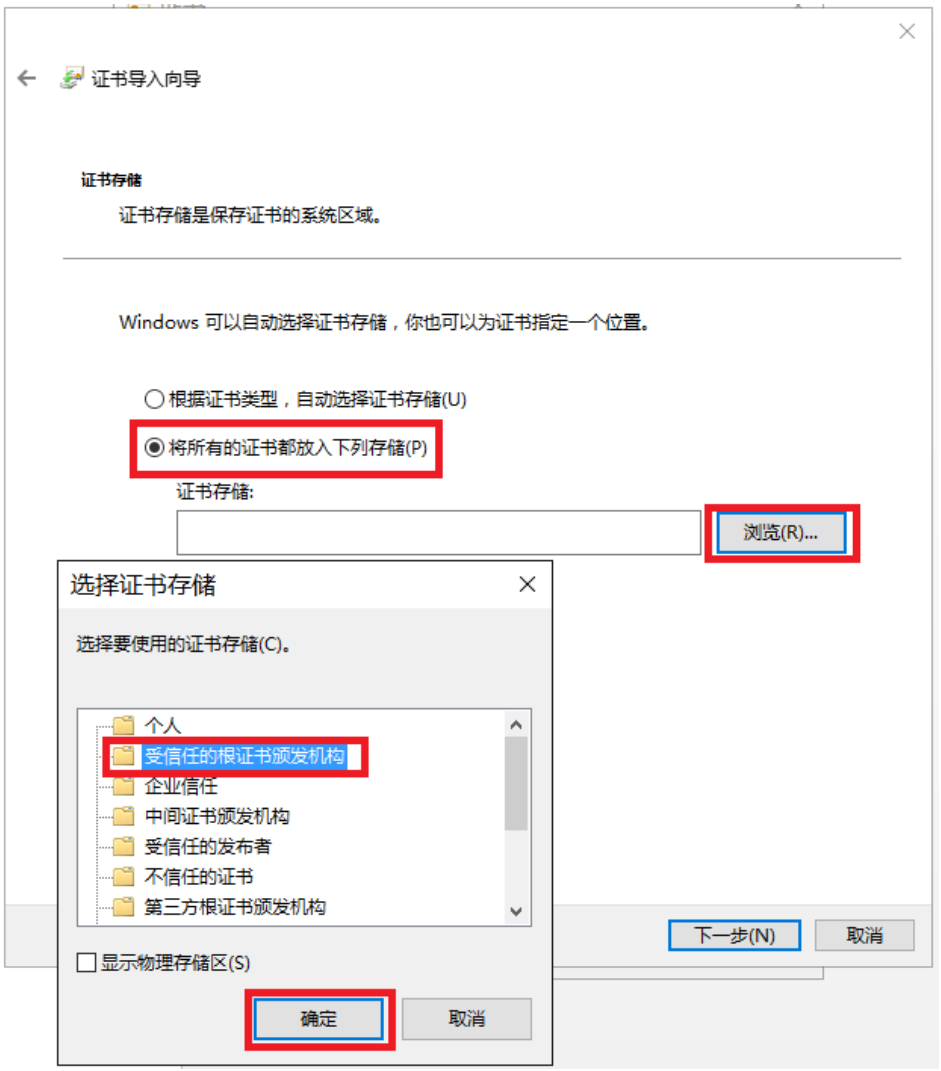


图 2-3-2 “证书导入窗口”2

选择“将所有的证书都放入下列存储”项，再点击“浏览”按钮，出现“选择证书存储”窗口，选择“**受信任的根证书颁发机构**”项目，再点击“确定”按钮，之后，再点击窗口的“下一步”、“完成”按钮，最终会弹出导入成功窗口，如下图 2-4 所示，点击“确定”按钮关闭。

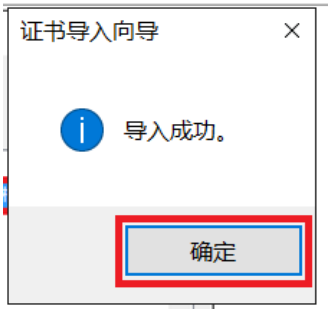


图 2-4 “导入成功”窗口

2.2.1.2 编辑 hosts 文件

导入证书后，如果证书的 CommonName/Subject Alternative Name/SAN 是 IP，就不用域名解析或编辑 hosts 文件，直接使用“https://12.12.23.34/xxx”这样的链接。

如果是域名，要么修改 DNS 服务器配置，将该域名解析成对应的 IP，客户端的 DNS 服务器还要能检索到该 DNS 服务器；要么修改 Windows 本地的 hosts 文件，即以管理员的身份编辑“C:\Windows\System32\drivers\etc\hosts”文件，

加入“12.12.23.34 zstdadi.com”这样的域名 IP 解析，保存文件后就可以使用“https://zstdadi.com/xxx”这样的带域名的链接，而不再出现证书安全提示了。

为了检验 CA 证书安装是否成功，可以打开测试 URL“https://服务器地址”，如果没有安全警告，而且查看证书是有效的，如下图 2-5 所示，就表明 CA 证书安装成功。

图 2-5 检验 CA 证书有效性

如果正常安装了自签名 CA 证书、修改了 hosts 文件后，浏览器仍然报错，可以清除 SSL 状态，或者重启浏览器再试。还可以运行 certmgr 证书管理器，如下图 2-6 所示，在“受信任的根证书颁发机构”证书中，找到名称（颁发者、颁发给）为 IP 地址的证书，全部删除后，重新安装自签名 CA 证书，再重启浏览器做测试。

访问纯 IP 的 https 地址不需要安装自签名 CA 证书，可以选择忽略错误并打开网页，如果浏览器报错（例如“您目前无法访问 xxx，因为此网站发送了

Google Chrome 无法处理的杂乱凭据”等），并且无法进一步访问，可以删除名称（颁发者、颁发给）为 IP 地址的证书再试。

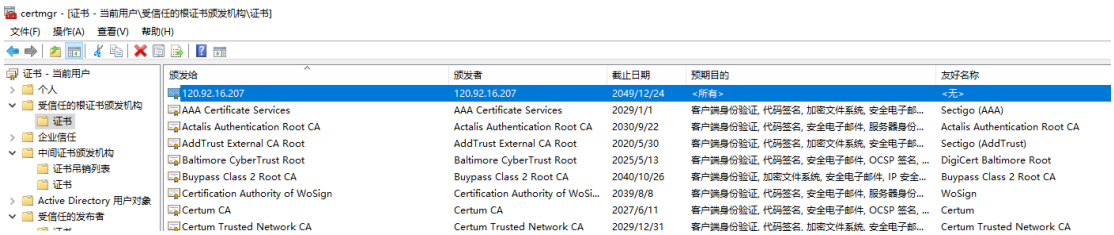


图 2-6 certmgr 证书管理器

2.2.2 安卓系统的证书导入

可以通过（quickmark APP 扫描二维码，再通过 chrome 浏览器）从 VPN 服务器上下载得到，URL 类似“http://121.42.51.234/myca.crt” ，需要输入用户名和（初始）密码 。crt 文件下载完成后，自动弹出窗口，如下图 2-7 所示。

图 2-7 安卓系统安装 CA 证书窗口

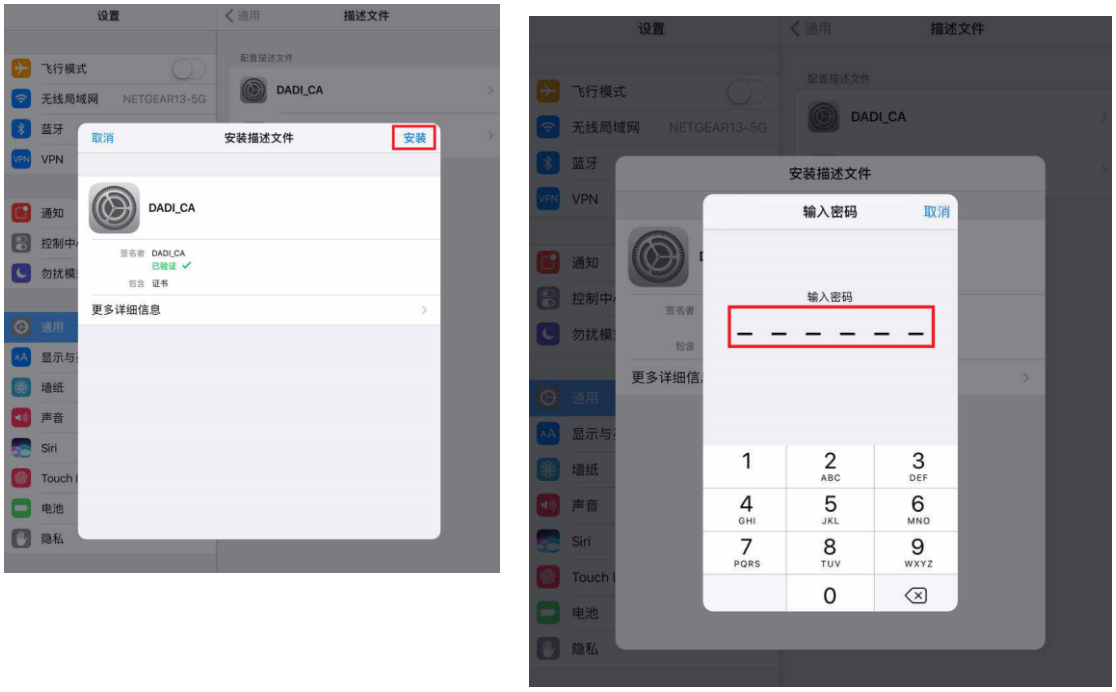
输入证书名称，并点击“确定”按钮，系统会提示“xxx 安装成功”。

如果点击 crt 文件，提示错误“无法安装该证书，因为无法读取该证书文件”，可以打开“设置—WiFi—高级设置—安装证书”，选择下载的 crt 文件安装。

普通用户在安卓系统下无法编辑 hosts 文件，需要 DNS 服务器配合才能使用域名形式的“服务器地址”，所以尽量使用 IP 地址形式或有 SSL 证书的真实域名的“服务器地址”。

2.2.3 iOS 系统的证书导入

通过浏览器下载并安装 CA 证书，URL 类似“http://121.42.51.234/myca.crt”，需要输入用户名和（初始）密码，下载成功后，打开“设置>通用>描述文件”（如果没有自动弹出“安装描述文件”窗口），选择待安装的文件，点击右上角的“安装”按钮，安装过程中需要输入 iOS 的解锁密码，如下图 2-8 所示。



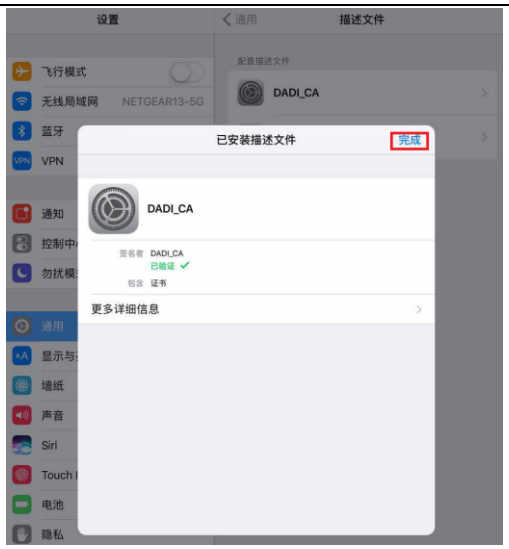


图 2-8 iOS 系统安装 CA 证书窗口

普通用户在 iOS 系统下无法编辑 hosts 文件，需要 DNS 服务器配合才能使用域名形式的“服务器地址”，所以尽量使用 IP 地址形式或有 SSL 证书的真实域名的“服务器地址”。

2.2.4 Firefox 的证书导入

1、Windows 系统

Firefox 浏览器需要单独导入 CA 证书，地址栏输入“about:preferences#privacy”，或依次打开“选项>隐私与安全>证书>查看证书”，点击“证书颁发机构”TAB，点击下方的“导入”按钮，选择 myca.crt 证书文件导入，最后再点击“确定”按钮，参见图 2-9 所示。

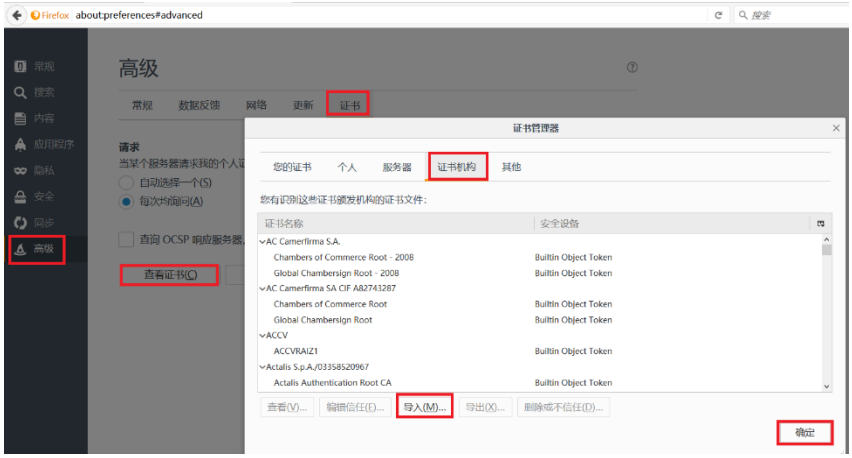


图 2-9 Firefox 浏览器证书导入

如果遇到“SEC_ERROR_BAD_SIGNATURE”等证书错误的提示，可以在“证书

机构”中删除证书名称是“dadi”的所有证书，再重新导入新证书；或者删除 cert9.db 文件（帮助>故障排除信息>配置文件夹>打开文件夹，about:support），再重启 firefox 浏览器。

2、安卓系统

安卓系统下 Firefox 浏览器没有证书设置界面，打开 Firefox 浏览器，请求 https://xxx/myca.crt，输入用户名密码，再导入 CA 证书，再重启 Firefox 浏览器。

3 WebDAV 服务

WebDAV 服务可以让用户挂载远程目录到文件管理器，在本地串流播放（VLC 等）、查找、创建、编辑、删除远程文件，不需要下载、上传，自动同步内容，WebDAV 服务分为可读可写和只读，需要用户认证和不需要用户认证，WebDAV 服务的 URL 分为 http 和 https 两种类型，一般使用 https 类型，但是需要事先安装 CA 证书。保存的远程文件都是 WEB 服务器的一个 URL 链接，根据存储的位置，可能需要或不需要用户认证。

注意：

1）上传的文件均只能作为普通文件打开，不能作为 cgi 程序执行

2）如果知道子目录 dir 的名称，可以以 https://ip 或域名/web/dir 的方式挂载

3）上传文件如果大于 WebDAV 目录所在文件系统的容量，将会出错，可能需要断开连接，重新连接后才能再用

3.1 Windows 系统下使用 WebDAV 服务

Windows 下可以使用 RaiDrive、GoodSync、Air Explorer、Cyberduck、CarotDAV、Hopic Explorer、TeamFile、WinSCP、PotPlayer、wget/curl（用于自动备份）等软件。

Windows 下使用 WebDAV 服务示例

http://www.trustcomputing.com.cn/help/cn/dadi/webserver/webdav_windows.html

Windows 系统下使用 WebDAV 服务分为两个步骤：下载安装自签名 CA 证书、映射网络驱动器。注意：当管理员为服务器地址申请了真实域名 SSL 证书后，可不必再下载安装自签名 CA 证书。

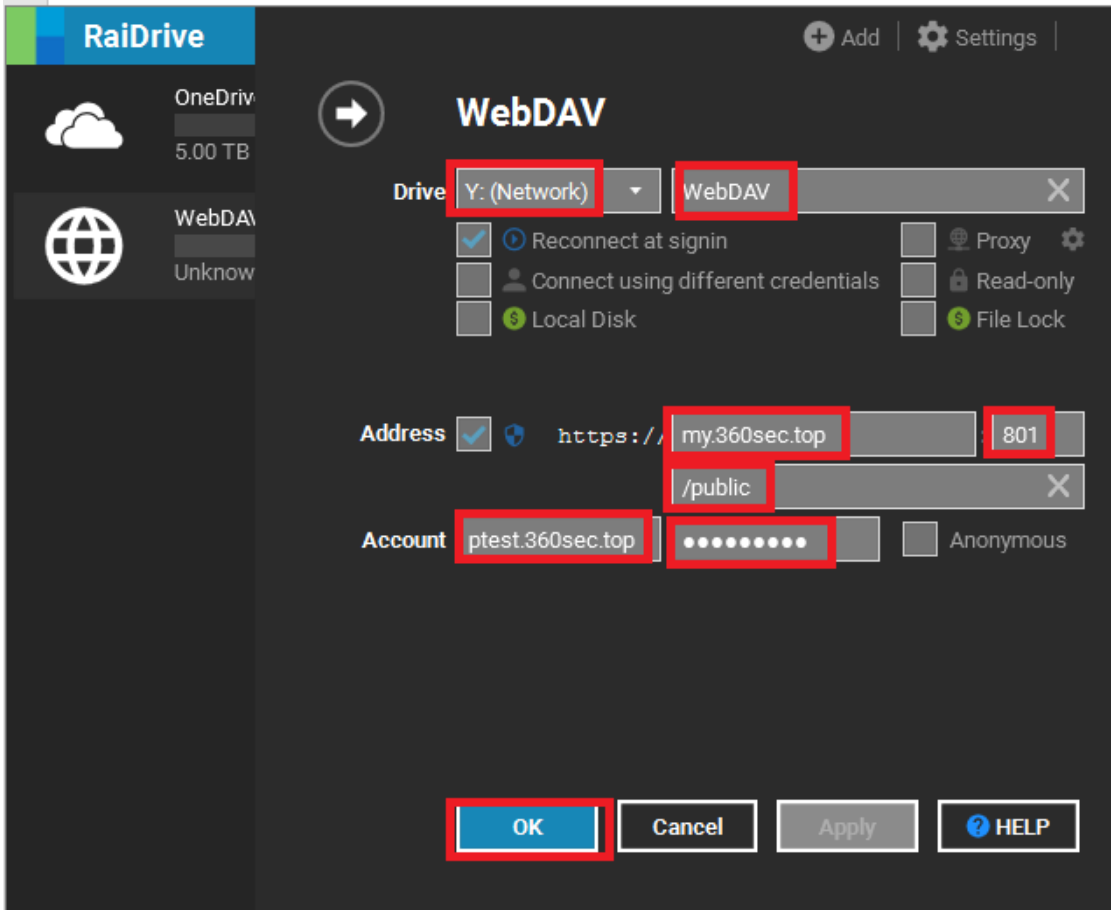
1）下载安装自签名 CA 证书

对于 https 类型的 WebDAV 服务 URL，而且服务器地址没有真实域名证书时，需要事先安装并验证 CA 证书：参见“**2.2.1 Windows 系统的证书导入**”。

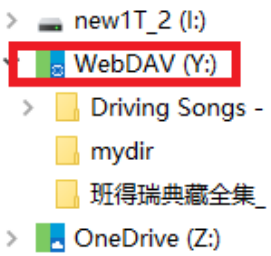
2）映射网络驱动器

Windows 下推荐使用 RaiDrive 软件挂载 WebDAV 资源，网址是：https://www.raidrive.com/Download

对于 WebDAV 资源“https://my.360sec.top:801/public”的挂载，输入参数如下图所示。



成功后，会在文件管理器中挂载该网盘，以后对文件、目录的操作和本地磁盘一样，public 目录下文件将成为公开的 WEB URL 资源，如下图所示。



注意：

1）可以匿名挂载/public 目录，权限是只读

2）用户密码输入错误仍可以挂载，但权限是只读

3）WEB、VPN 用户输入正确密码挂载后，可以创建子目录、文件，但只有 WEB 用户可以删除自己的子目录、文件

以下再以 Windows 自带的文件管理器为例说明（Windows 下还是推荐使用 RaiDrive 软件挂载 WebDAV 资源）。

打开文件管理器，找到“网络”图标，在其上按鼠标右键，选择“映射网络驱动器(N)”项，如图 3-1 所示。

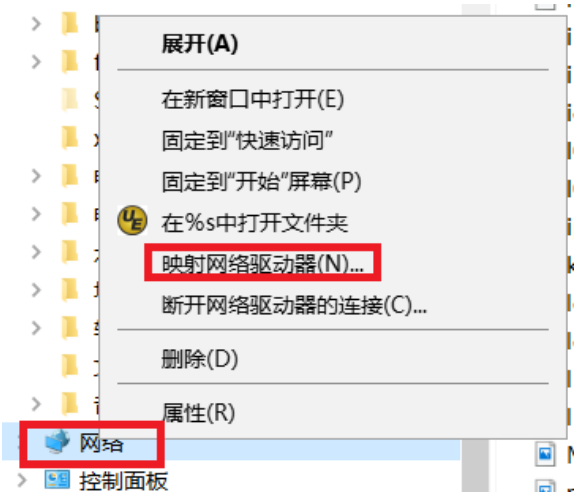


图 3-1 映射网络驱动器挂载 WebDAV 服务 1

在打开的“映射网络驱动器”窗口中，如图 3-2 所示，选择“驱动器”盘符，并在 “文件夹”栏填写服务器 URL，例如：https://11.22.33.44/public 或 https://giga.com/web，点击“完成”按钮；如果要以可写方式挂载，需要勾选“使用其它凭据连接”项，用于切换用户/强制用户认证，输入用户名和密码，再点击“确定”按钮完成挂载操作。

注意：此服务器 URL 主机名部分“11.22.33.44”或“giga.com”必须和 CA 证书的 SAN 服务器名一致，如果是域名的形式，还要确保能解析成正确的 IP 地址，如果不是真实的域名，还要以管理员的身份修改“C:\Windows\System32\drivers\etc\hosts”文件，具体参考“**2.2.5 编辑**

hosts 文件”。

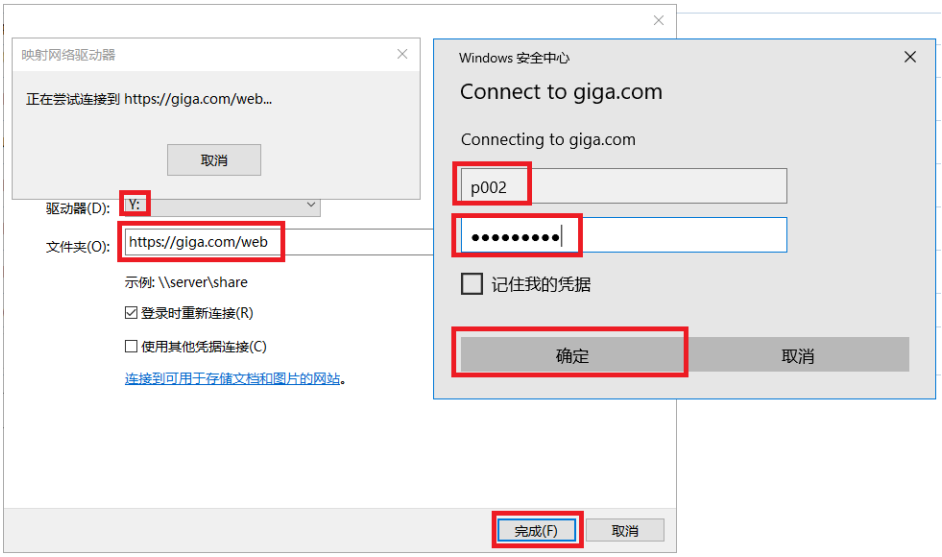


图 3-2 映射网络驱动器挂载 WebDAV 服务 2

映射成功后，会在文件管理器中显示网络驱动器的盘符，如图 3-3 所示。之后就可以在本地操作其中的文件，根据 WebDAV 的类型，可能是可读可写的或只读的。在此盘符图标上按鼠标右键，选择“断开连接(D)”项可以取消映射。

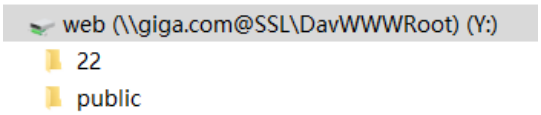


图 3-3 映射完成后的网络驱动器

另外，还可以在 DOS 命令提示符窗口中使用命令行映射或取消网络驱动器，对于 https URL 事先也需要安装 CA 证书，如图 3-4 所示。

- 映射网络驱动器: net use * https://giga.com/web /user:xxx
  或 net use * \\giga.com@SSL\public
- 取消映射网络驱动器: net use * /delete
- 查看网络驱动器: net use

图 3-4 DOS 命令提示符窗口中使用命令行映射或取消网络驱动器

注意：挂载/public 目录不需要用户认证，但是是只读的；如果需要写入，则挂载时需要加上用户认证，即 /user:xxx 。

Windows 文件管理器删除无用的、此网络连接不存在的网络驱动器的方法：

1）打开注册表软件 regedit，搜索该网络位置、网络驱动器的 URL，一般在\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\下，删除下面的子项；

2）关闭 Windows 资源管理器/文件管理器，运行任务管理器，杀掉所有的“Windows 资源管理器”进程，再运行“explorer”恢复

部分多媒体播放器支持 WebDAV 资源，例如，PotPlayer 播放器可以使用“打开远程连接”来查看 WebDAV 资源，如图 3-5 所示。

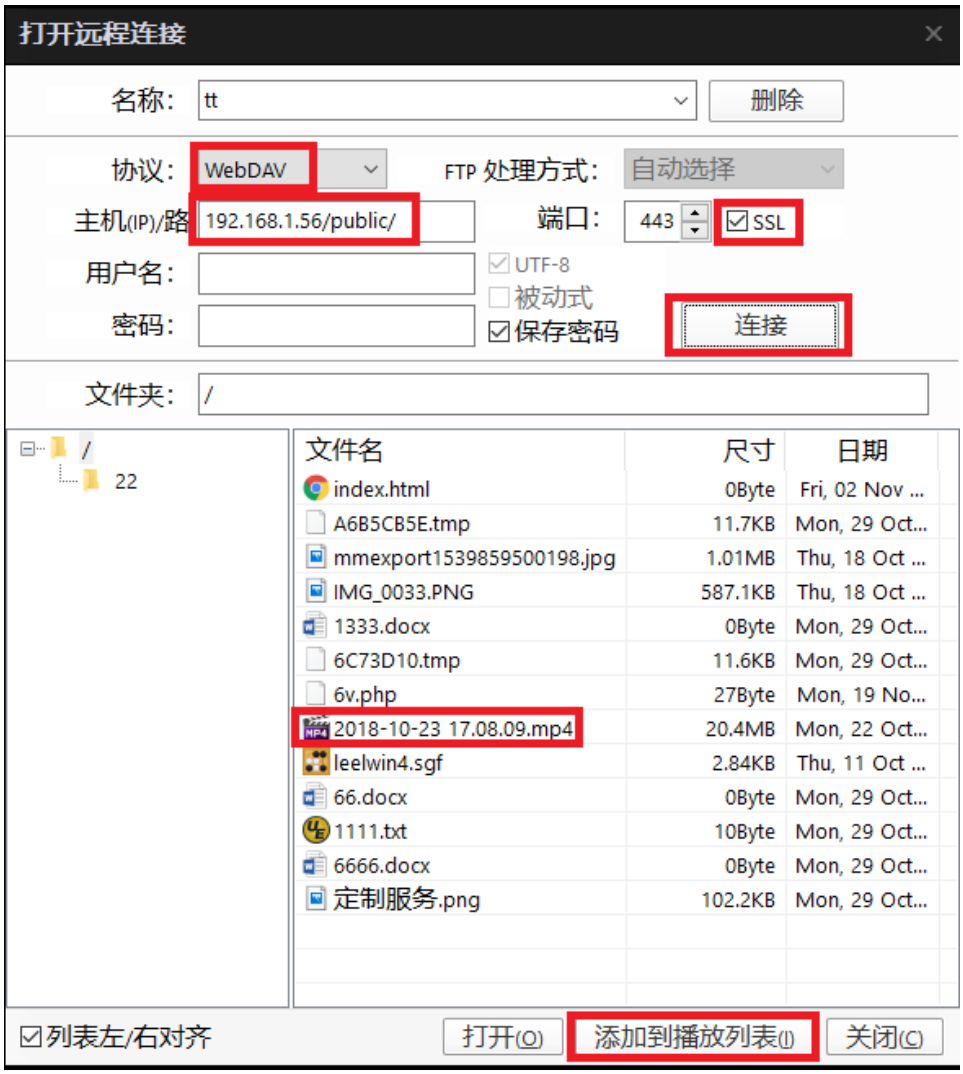


图 3-5 PotPlayer 播放器打开 WebDAV 远程连接

注意：

1）WebDAV 上传的文件均只能作为普通文件打开，不能作为 cgi 程序执行

2）最好先创建子目录 dir，再以 https://giga.com/web/登录账号/dir 的方式挂载 WebDAV 资源进行上传文件的操作

3）在小带宽互联网上下载、上传、直接打开网络驱动器中的大文件时，Windows 文件管理器进度条显示有问题，PotPlayer 播放器也打开慢，最好使用其它软件，或先查询得到文件的 URL，再以 WEB 浏览器的方式下载、上传、在线播放文件

4）在某些版本的 Windows 操作系统中，从 WebDAV 驱动器下载的最大文件大小被限制为 50MB，上传并没有限制。如果拷贝超过 50MB 大小的文件，

Windows 就会显示“文件大小超出允许的限制”的错误提示。可以通过修改注册表来消除这个限制，将注册表中位于 HKLM\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\FileSizeLimitInBytes 处的键值由 50000000 (50MB) 修改为更大的数值，最大修改为：4294967295（0xffffffff）字节，即 4G。之后要重启 WebClient 服务，重新挂载 WebDAV 驱动器才能生效

5）如果 https 方式不好用，可以换成 http 的方式，但需要修改注册表键值 HKLM\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\BasicAuthLevel 为 2，之后要重启 WebClient 服务(net stop webclient; net start webclient)，重新挂载 WebDAV 驱动器才能生效。http 方式会泄露用户名密码信息，请谨慎使用。如果 Windows 文件管理器不好用，可以换成 WinSCP\RaiDrive 等第三方软件挂载 WebDAV 资源

6）VPN 拨号后，对于不真实的域名，即使在 hosts 文件中有记录的域名，WebDAV 也可能会连接不成功，需要断开 VPN 再连接

7）IPV6 IP 需要转换成 ipv6-literal.net 结尾的 literal address 才能用于挂载，例如：2001:470:c:1cb::2 转换后是 2001-470-c-1cb--2.ipv6-literal.net，再通过命令 net use * http://2001-470-c-1cb--2.ipv6-literal.net/public 挂载，在线转换工具可以用 https://ipv6-literal.com

3.2 安卓系统下使用 WebDAV 服务

安卓下可以使用 Flashlight + Clock Filemanager、Cx File Explorer、X-plore、ES 文件浏览器等软件，以下以 X-plore 和 ES 文件浏览器为例说明操作步骤。

安卓下使用 WebDAV 服务示例

http://www.trustcomputing.com.cn/help/cn/dadi/webserver/webdav_android.html

安卓系统下使用 WebDAV 服务可以不需要下载安装自签名 CA 证书，直接挂载 WebDAV 目录，如有必要可以先下载并安装自签名 CA 证书，参考“**2.2.2 安卓系**

统的证书导入”。以下以 X-plore 和 ES 文件浏览器为例说明挂载 WebDAV 的方法。

1、X-plore App

图 3-6-1

图 3-6-2

图 3-6-3

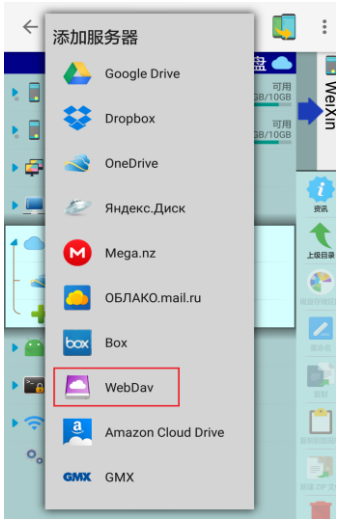


图 3-6-4

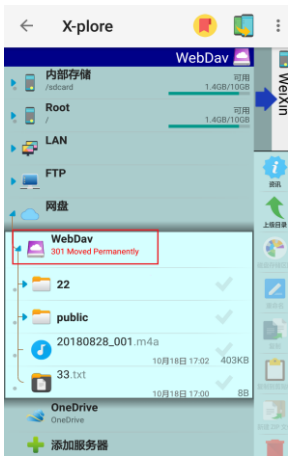


图 3-6-5　　图 3-6-6

使用 X-plore 挂载 WebDAV 资源的步骤如系列图 3-6 所示，具体描述如下：

1）如果没有“网盘”项，需要在“显示”项中启用“网盘”项；

2）在“网盘”项最下方，点击“添加服务器”，并选择“WebDav”项；

3）在“编辑服务器”窗口，填写“用户名”、“密码”和“服务器”栏内容，再点击“保存”按钮；

4）返回主界面后，点击“网盘”>“WebDav”项查看挂载的远程目录的内容；之后就可以进行文件操作。

2、ES 文件浏览器 App

图 3-7-1

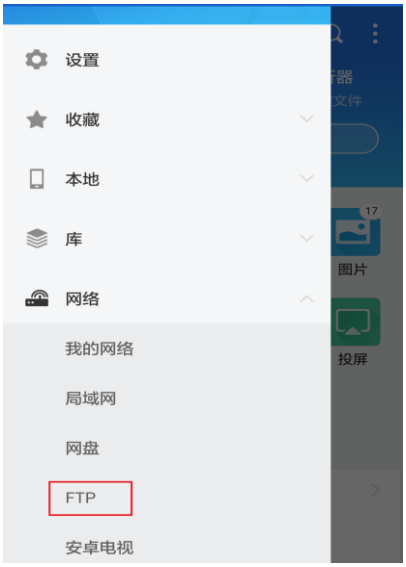


图 3-7-2

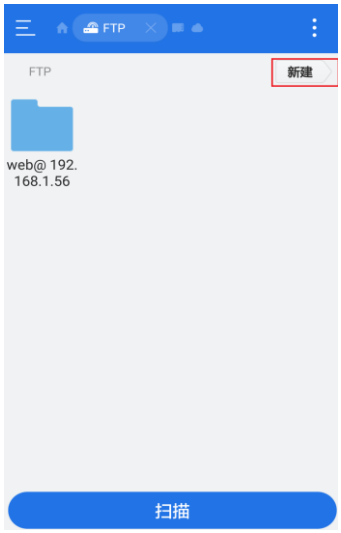


图 3-7-3

图 3-7-4

图 3-7-5

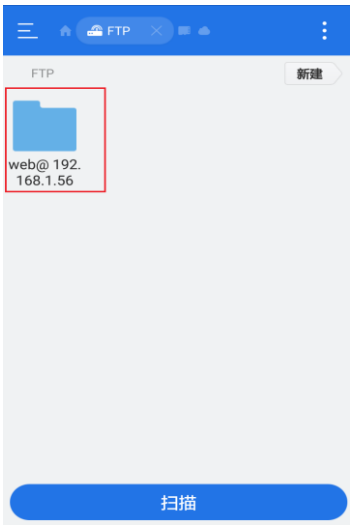


图 3-7-6

使用 ES 文件浏览器挂载 WebDAV 资源如系列图 3-7 所示，具体描述如下:

1）点击左上角图符，选择“FTP”项；

2）在“FTP”界面右上角，点击“新建”按钮；

3）在“新建 WEBDAV 服务器”窗口，填写“服务器”、“端口”、“用户名”、“密码”栏的内容，勾选“加密(https)”项，再点击“确定”按钮；

4）返回“FTP”界面后，点击新建的图符，查看挂载的远程目录的内容；之后就可以进行文件操作。

3.3 iOS 系统下使用 WebDAV 服务

iOS 下可以使用 Documents by Readdle、OverTheAir、GoodReader、PhotoSync、WebDAV Navigator、Keynote、Pages 等软件，以下以 Keynote 和 Documents 为例说明操作步骤。

iOS 下使用 WebDAV 服务示例

http://www.trustcomputing.com.cn/help/cn/dadi/webserver/webdav_ios.html

iOS 系统下使用 WebDAV 服务可以不需要下载安装自签名 CA 证书，直接挂载 WebDAV 目录，如有必要可以先下载并安装自签名 CA 证书，参考“**2.2.3 iOS 系统的证书导入**”。以下以 iWork 系列 App 和 Documents App 为例说明挂载 WebDAV

的方法。

1、iWork 系列 App

图 3-8

使用 i-Work 系列 App 挂载 WebDAV 资源如图 3-8 所示，具体描述如下:

1）点击“位置”右上“编辑”按钮，再新界面中启用“WebDAV”项；

2）返回“位置”界面后，点击“WebDAV”项；

3）在“WebDAV”窗口，填写“服务器地址”、 “用户名”、“密码”栏的内容，再点击“登录”按钮；之后就可以查看挂载的远程目录的内容，再进行文件操作。

2、Documents App

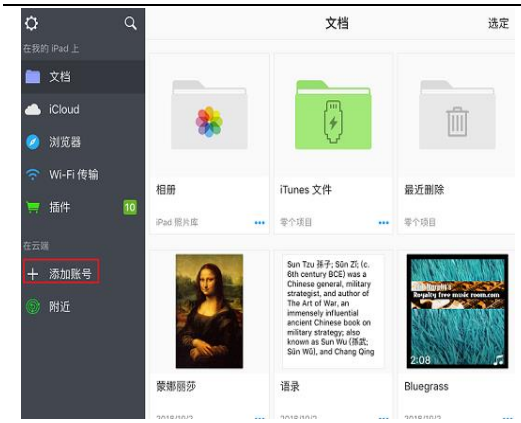


图 3-9-1

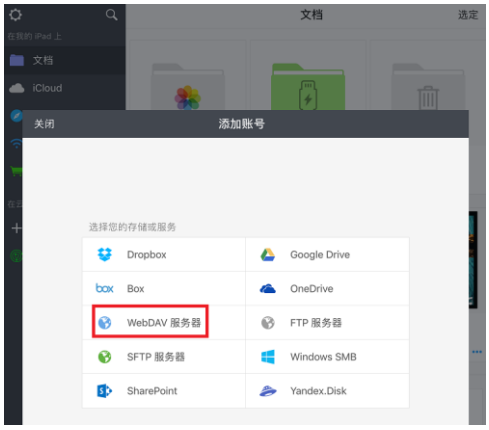


图 3-9-2

图 3-9-3

图 3-9-4

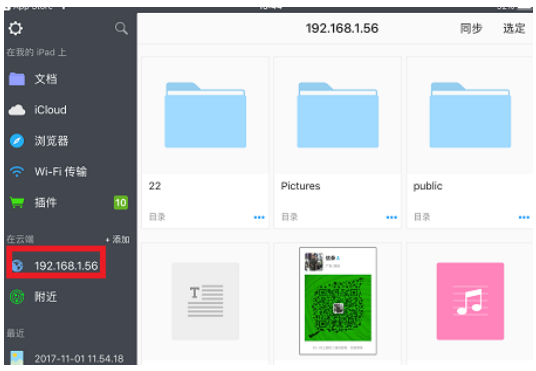


图 3-9-5

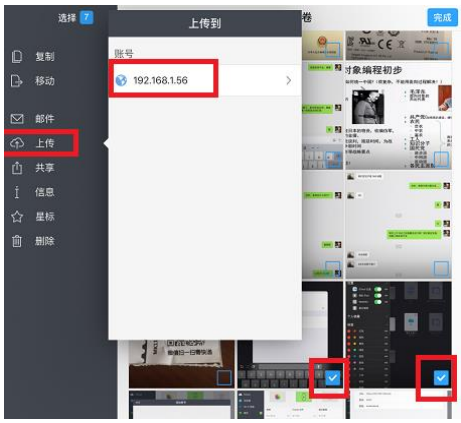


图 3-9-6

使用 Documents App 挂载 WebDAV 资源如系列图 3-9 所示，具体描述如下:

1）点击左边“添加账号”按钮，再新界面中选择“WebDAV 服务器”项；

2）在“WebDAV 服务器”窗口，填写“URL”、 “登录”、“密码”栏的内容，再点击“保存”按钮；

3）如果没有安装 CA 证书，就会出现“无法验证服务器身份”的警告窗口，点击“继续”按钮；

4）返回主界面后，点击左边新建的图符，之后就可以查看挂载的远程目录的内容，再进行文件操作。

3.4 MacOS 系统下使用 WebDAV 服务

MacOS 下可以使用 GoodSync、Air Explorer、Cyberduck、Dreamweaver 等软件，以下以 MacOS 自带的 Finder 为例说明操作步骤。

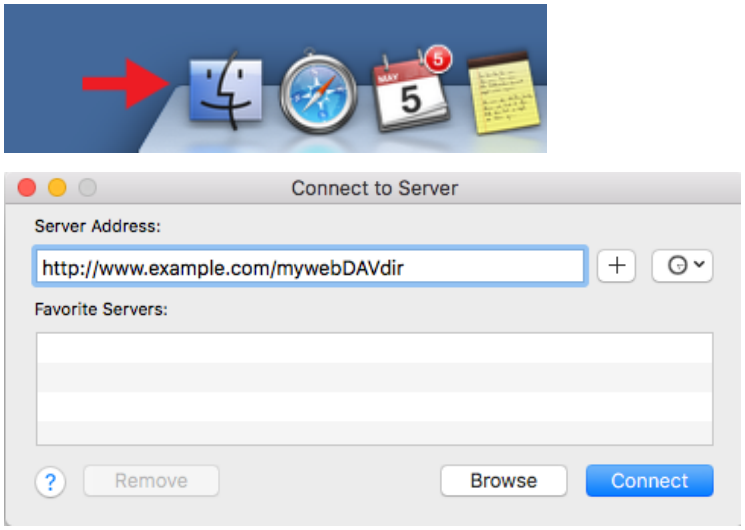


图 3-10

MacOS 系统下挂载 WebDAV 资源如图 3-10 所示，具体描述如下:

1）点击下方“Finder”图符，选择“Go > Connect”菜单项；

2）在“Connect to Server”窗口中，填写“Server Address”栏的内容，再点击“Connect”按钮；

3）如果有用户认证，就会弹出认证窗口，输入用户名密码，点击“OK”按钮；

4）成功后就可以查看挂载的远程目录的内容，再进行文件操作。

3.5 Linux 系统下使用 WebDAV 服务

Linux 下可以使用 wget/curl（用于自动备份）、cadaver、davfs2 等软件，以下以 Ubuntu 图形化文件管理器和命令行为例说明操作步骤。

1、Ubuntu 图形化文件管理器

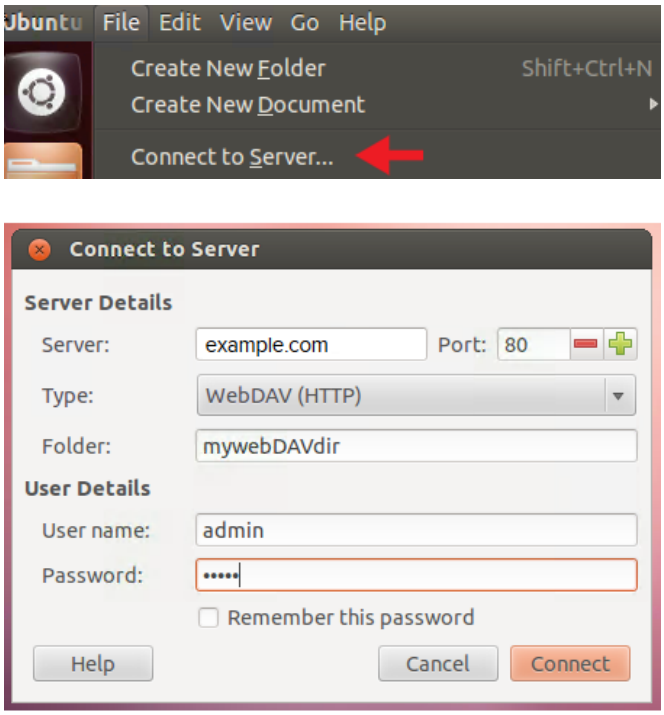


图 3-11

Linux 系统下通过图形界面挂载 WebDAV 资源如图 3-11 所示，具体描述如下：

1）进入桌面，点击上方菜单，选择“File > Connect”菜单项；

2)在“Connect to Server”窗口中，填写“Server”等栏的内容，再点击“Connect”按钮；

3）成功后就可以查看挂载的远程目录的内容，再进行文件操作。

2、Linux 命令行挂载 WebDAV 目录

1）安装软件包

apt-get install davfs2 或 yum install davfs2

2）创建挂载目录

mkdir /mnt/dav

3）挂载 WebDAV 目录

mount -t davfs https://192.168.1.56/web /mnt/dav

4）查看已挂载的目录

df -h

5）卸载已挂载的目录

umount /mnt/dav

3.6 WEB 浏览器使用 WebDAV 服务

通过浏览器可以以 WEB GUI 的形式使用远程的 WebDAV 服务，这样可以不需要安装软件，Windows、安卓、iOS、MacOS、Linux 等 OS 下都可以使用，一般 URL 是“https://服务器地址/pan”或“https://服务器地址/pan/#https://服务器地址/web/登录账号/public”，界面如图 3-12 所示，如果服务器地址是域名，而且没有真实域名证书，需要下载安装自签名 CA 证书，参考“**2.2 导入 CA 证书**”。查看、下载不需要用户认证，上传、写入、删除需要用户认证。在线编辑文件需要先用户认证，一开始请求的 URL 是“https://服务器地址/pan/#https://服务器地址/web/登录账号”

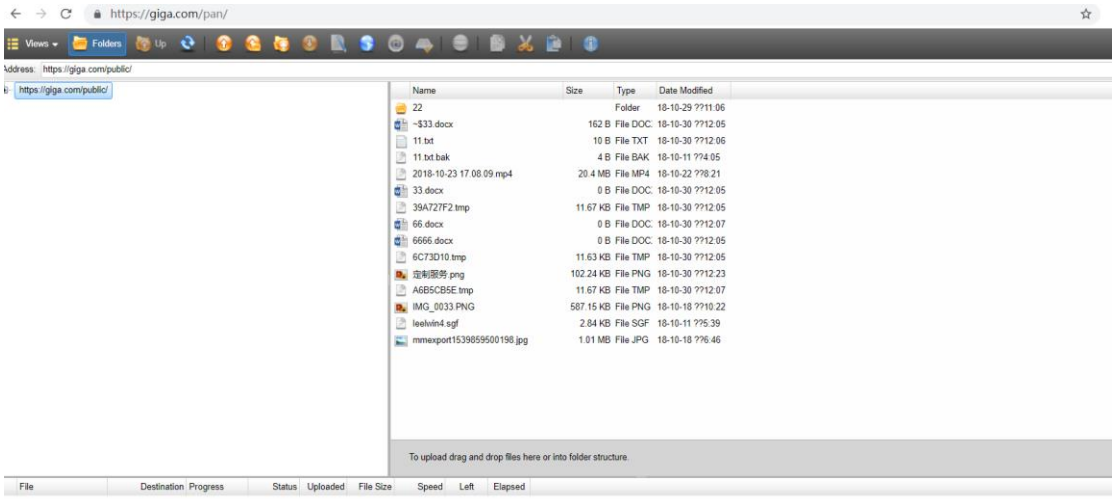


图 3-12 WEB GUI 的形式使用远程的 WebDAV 服务

4 代理服务器设置

4.1 Windows 系统下代理服务器的设置

4.1.1 Windows 系统设置 HTTP 代理

Windows 代理服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/proxy/windows_proxy.html

1）打开 IE 浏览器，点击上方的“**工具**”菜单项，选择最下方的“Internet 选项”，如图 4-1 所示；

图 4-1 IE 浏览器设置 1

2）在弹出的“Internet 选项”对话框中，切换到“**连接**”选项卡，点击“**局域网设置**”按钮，如图 4-2 所示；

图 4-2 IE 浏览器设置 2

3）在弹出的“局域网（LAN）设置”对话框中，勾选“**为 LAN 使用代理服务器**”选项，并填写地址：“**121.42.51.234**”，端口：“**8081**”，如图 4-3 所示。以后如果不想使用代理，则取消这个“**为 LAN 使用代理服务器**”选项。

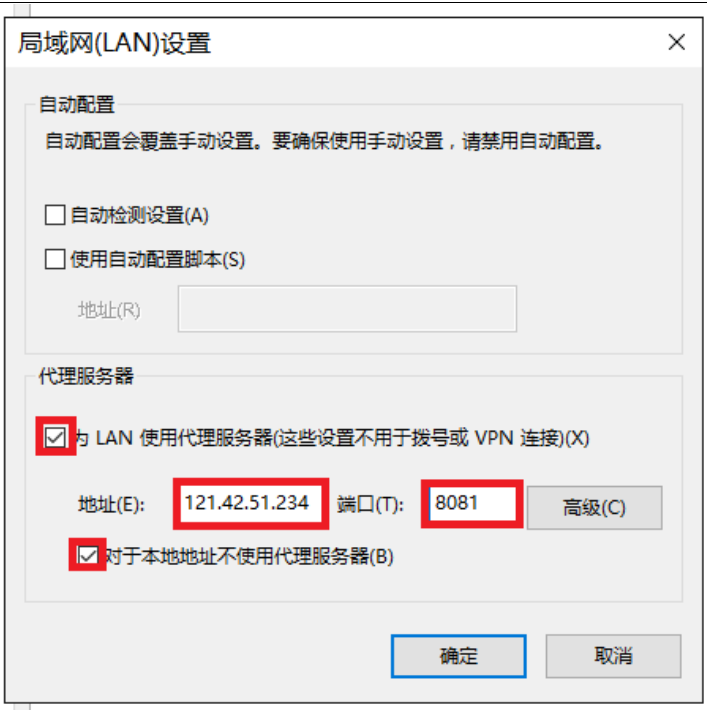


图 4-3 IE 浏览器设置 3

4）为了避免连接路由器等本地 IP 时也使用代理，需要设置一下例外，点击图 4-3 中的“**高级**”按钮，弹出“**代理设置**”对话框，如图 4-4 所示，在“**例外**”栏里输入本地网段，例如：***192.168.1.****，如果代理服务器在国外，需要将国内的域名作为例外，例如：****.qq.com,*.baidu.com,*.jd.com***，之后一路点击“**确定**”按钮，即可上网浏览。

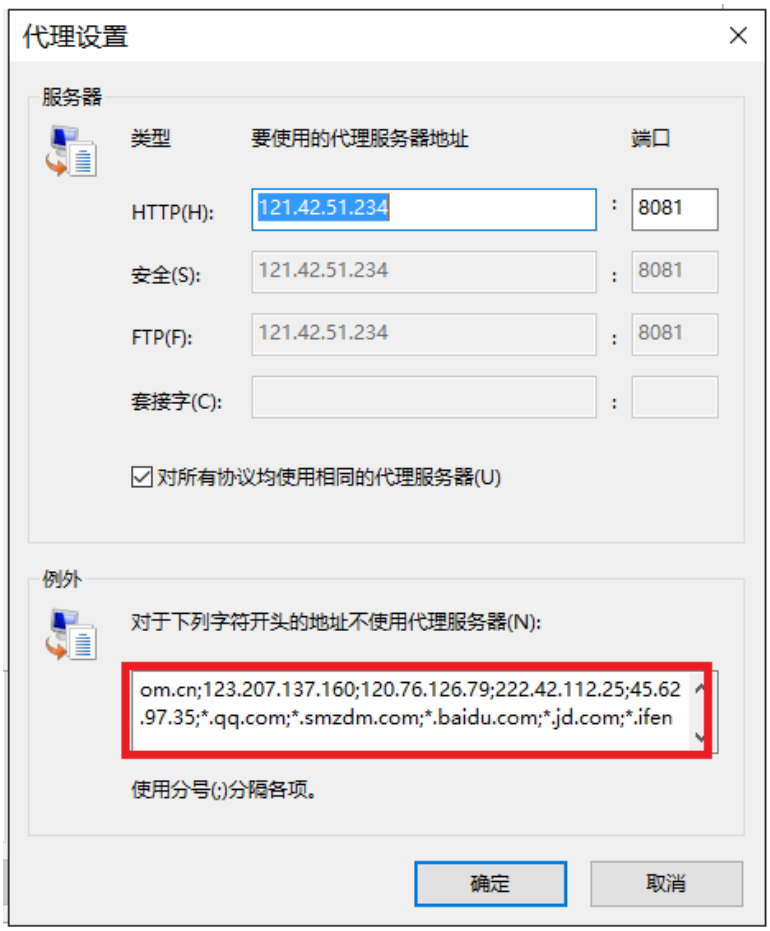


图 4-4 IE 浏览器设置 4

如果代理服务器要求用户认证，则会弹出对话框，输入正确的用户名和口令，即可继续浏览，如果输入错误，会被系统阻拦，请等待一分钟之后再试。如果使用 chrome、firefox 浏览器，安装了 SwitchOmega 插件，需要事先输入用户名密码，并保存、应用配置，如下图所示：

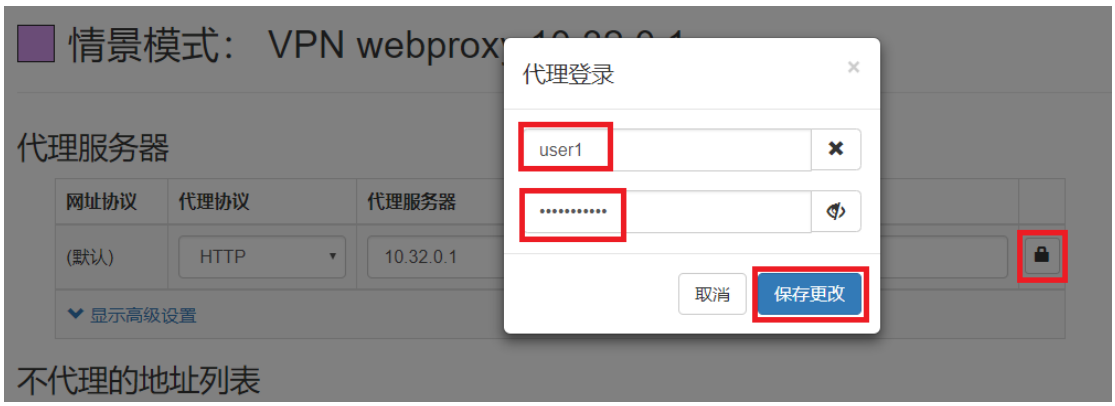


图 4-5 SwitchOmega 设置用户认证

注意：

1）为了使用 HTTP 代理的“解密 HTTPS”的功能，客户端必须事先下载安装自签名 CA 证书，具体参见“**2.2.1 Windows 系统的证书导入**”

2）Windows 下，用户连接 PPTP VPN 后，将忽略此处 IE 设置的代理服务器，直接通过 VPN 隧道访问远程网络

3）SSTP VPN 连接时会首先使用此处 IE 设置的代理服务器，所以，如不必要，请停用此处的代理服务器再连接 SSTP VPN

4）SS/SSR 客户端启用系统代理后，会自动修改此处的代理服务器为套接字（Socks）127.0.0.1 8080，如果 SS/SSR 未运行，则要在此处停用其设置的代理服务器

为了避免 HTTP 代理明文流量被中间网络监听及阻拦，可以在（PC 或 VPS）客户端利用 SSH 客户端软件启用 SSH 正向端口代理功能，以 SecureCRT 软件为例，具体设置如下图 4-5 所示。建立 SSH 连接后，（PC）客户端设置 127.0.0.1:8086 为本机浏览器的 HTTP 代理服务器 IP 及端口，实际连接的是 SSH 服务器所在主机的 WEB 代理服务器的 25 端口，这样 HTTP 代理的流量首先经过 SSH 的加密保护，可以不再受到中间网络的监听及阻拦。其它自启动等设置请参考“**13.1 Windows 系统下设置 SSH 客户端**”。还可以使用 HTTPS 代理。

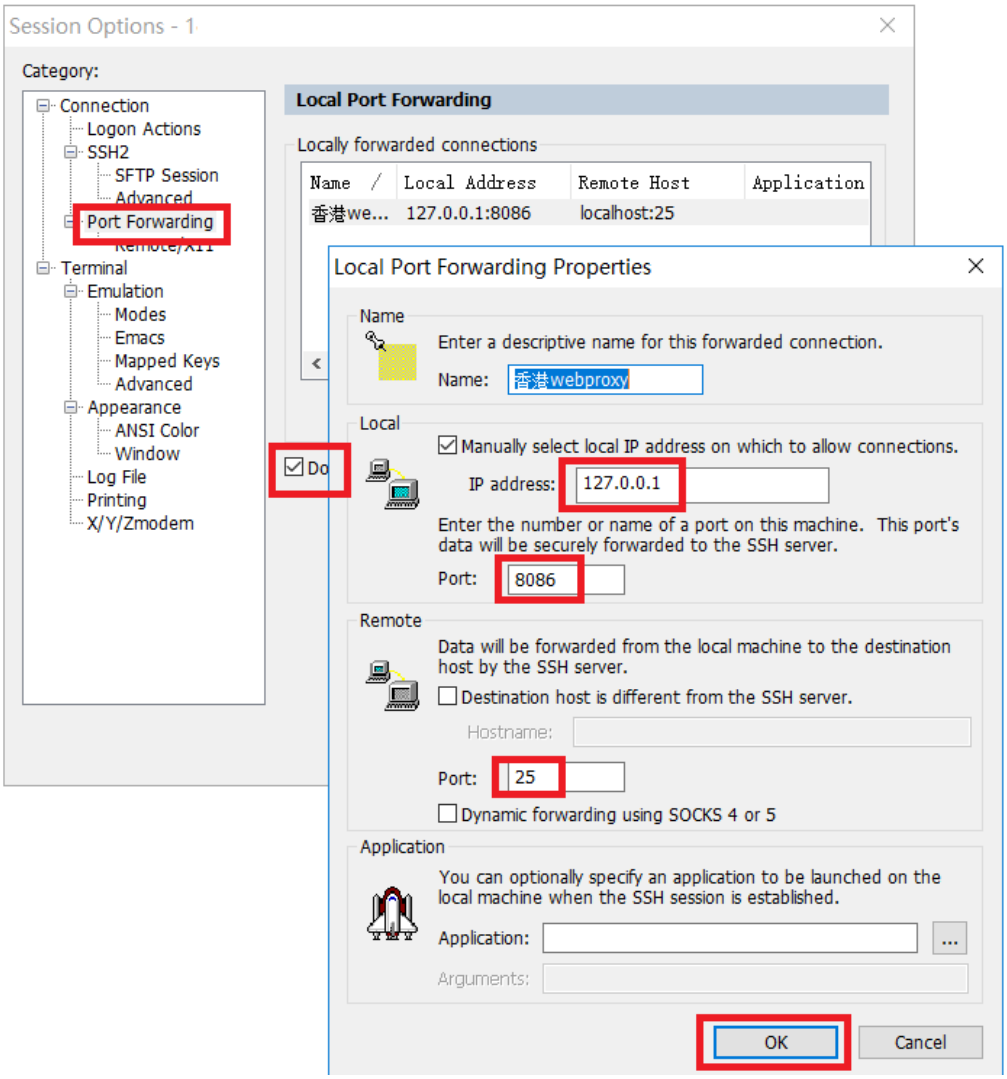


图 4-5 SSH 客户端正向端口代理设置

4.1.2 Windows 系统设置 Socks、HTTPS 代理

浏览器方面，Windows 系统自带的 IE 浏览器对 Socks5、HTTPS 代理支持不好，Edge 浏览器不支持 HTTPS 代理，Firefox 无法直接使用 HTTPS 代理，都可以使用在线 PAC 文件间接使用 Socks5、HTTPS 代理，IE、Firefox 浏览器需要没有用户认证的在线 PAC 文件，最好先导入 CA 证书再使用 https URL 的 pac 文件。

可以使用 netch 软件的进程模式，选择浏览器的.exe 文件，使得浏览器可以透明使用 socks 代理服务。

HTTPS 代理没有明文的请求，可以避免流量被中间网络监听及阻拦，比 HTTP 代理更安全。系统级的 Socks 代理客户端软件有 Proxifier、SocksCap64 等。

日常使用推荐 Chrome 浏览器及 Proxy SwitchyOmega 插件的组合。

SwitchyOmega 插件下载链接

https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif

http://www.trustcomputing.com.cn/tools/SwitchyOmega.crx

打开 Chrome 浏览器选项菜单  ，选择“更多工具>扩展程序”项，或者在地址栏中输入“chrome://extensions/”，再把 SwitchyOmega.crx 文件用鼠标拖到新窗口中，再依提示安装 Proxy SwitchyOmega 插件。安装好后，进行具体设置：

1）右键点击 Chrome 浏览器右上角的圆环图符  ，选择“选项”项，弹出设定窗口；

2）再点击左下角的“新建情景模式...”项，在弹出的窗口中输入情景模式名称，例如：阿里云 socks 代理，类型是“代理服务器”，再点击“创建”按钮；

3）在该情景设置窗口中，选择代理协议为“SOCKS5”，再填写代理服务器域名或 IP 地址、端口以及不代理地址列表，再点击左下角的“应用选项”项，如下图 4-6 所示；

4）左键点击 Chrome 浏览器右上角圆环图符  ，选择刚刚创建的项目，例如：阿里云 socks 代理，就是使用该代理设置进行浏览了。

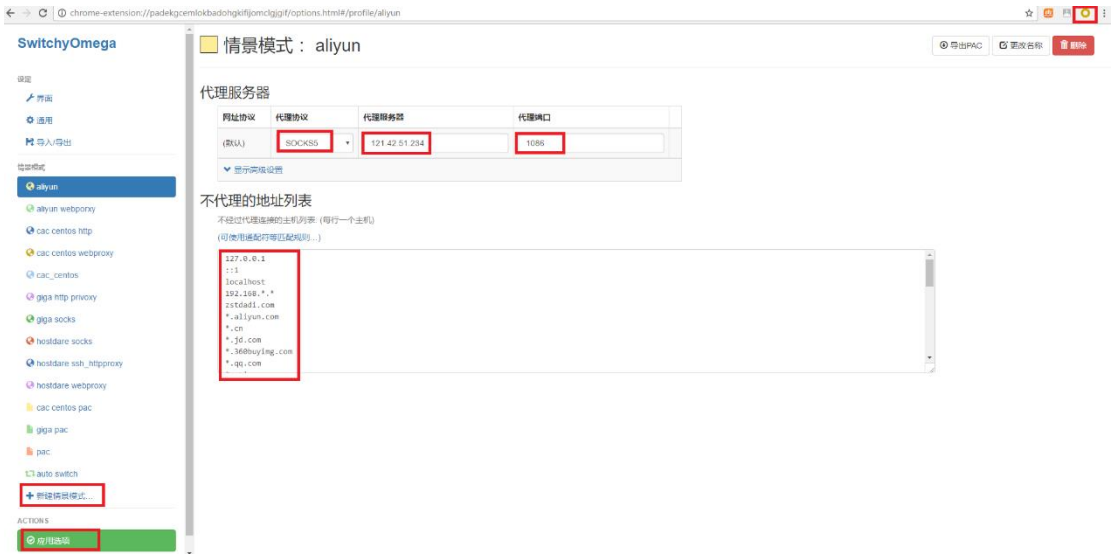


图 4-6 Chrome 浏览器 SwitchyOmega 插件设置

Chrome 浏览器的其它设置：

1、Chrome 浏览器的快捷方式，在“目标”栏后添加命令行选项，可以指定 HTTPS 代理

chrome --proxy-server=https://secure-proxy.example.com:443

或

chrome --proxy-pac-url=http://ip/proxy.pac

pac 文件内容为：

function FindProxyForURL(url, host) { return "HTTPS secure-proxy.example.com:443"; }

2、Chrome 浏览器的快捷方式，在“目标”栏后可以加“ --ignore-certificate-errors ”命令行选项，可以忽略证书问题。如果 Chrome 浏览器设置了没有安装 CA 证书的 HTTPS 代理服务器，会出现 ERR_PROXY_CERTIFICATE_INVALID 错误

3、关闭 Chrome 对 QUIC 协议支持，避免 UDP 协议被 QoS，以提高视频播放性能。需要开关测试后确定。

1） Chrome 地址栏输入 chrome://flags

2）搜索栏输入 quic，会显示 “Experimental QUIC protocol” 项

3）将下拉框展开，值改为 Disabled

4）重新启动浏览器，配置生效

4.2 Android 系统下代理服务器的设置

安卓系统有自带的代理服务器的设置，另外，也可以安装使用 Postern 等第三方全局代理软件。

4.2.1 安卓系统设置 HTTP 代理

安卓系统代理服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/proxy/android_proxy.html

打开安卓系统的“设置”界面，选择“WLAN”栏目，如果之前已有建立的无线连接，可以长按该连接名称，选择“修改网络”，如图 4-7 所示。

图 4-7 安卓系统修改已有的无线连接

对于新连接，输入密码，再勾选“显示高级选项”，选择“代理”类型为“手动”，“服务器主机名”和“服务器端口”填写正确的值，再点击“连接”按钮即可。如图 4-8 所示。

图 4-8 安卓系统 WIFI 连接时设置手工代理服务器

注意：

1）为了使用 HTTP 代理的“解密 HTTPS”的功能，客户端必须事先下载安装自签名 CA 证书，具体参见“**2.2.2 安卓系统的证书导入**”

4.2.2 安卓系统设置 Socks、HTTPS 代理

1）系统代理（全局代理）

安卓系统（6.0+）下可以通过设置 WIFI 的代理类型为“自动”即 PAC 自动检测代理来使用 Socks、HTTPS 代理，具体操作过程参见上节所述，主要的改变是代理选择“自动”项，并填写 PAC URL，如下图 4-9 所示。

图 4-9 安卓系统 WIFI 连接时设置自动 PAC 代理服务器

注意：安卓系统自带的浏览器不支持 Socks 系统代理，但安卓 Chrome、安卓 Firefox 等浏览器 App 支持。安卓 Chrome 没有手工或自动代理设置，只能使用系统代理，可以通过 chrome://net-internals/#proxy 查看，也不能安装插件。

2）Socks 代理 App

安卓系统下可以通过第三方 App 功能实现 Socks 代理功能，例如：Postern（HTTP 代理可能不兼容安卓高版本，SSH 兼容好）、Drony（未验证）或 ProxyDroid(需要 root)，下载链接如下。

- Postern 安卓 App 下载链接

https://play.google.com/store/apps/details?id=com.tunnelworkshop.postern

http://www.trustcomputing.com.cn/tools/Postern_v3.1.3.apk

- Drony 安卓 App 下载链接

https://play.google.com/store/apps/details?id=org.sandroproxy.drony

http://www.trustcomputing.com.cn/tools/org.sandroproxy.drony_1.3.112.apk

- ProxyDroid 安卓 App 下载链接

https://play.google.com/store/apps/details?id=org.proxydroid

http://www.trustcomputing.com.cn/tools/org.proxydroid_2.7.7.apk

3）浏览器 App

有一些可以使用 Chrome 插件的浏览器 App，例如：Kiwi 浏览器、Via 浏览器、Yandex 浏览器等，可以安装 SwitchyOmega 插件，再设置 HTTP、HTTPS 代理服务器，但是只能使用域名形式的代理服务器，HTTPS 代理需要真实域名的 SSL 证书。

安卓系统下 Firefox 浏览器没有网络代理设置界面，要通过 about:config 的方式修改浏览器配置以使用 Socks 或 HTTP、HTTPS 代理，Socks 代理具体参数如下：

network.proxy.socks: xx.xx.xx.xx

network.proxy.socks_port: 1080

network.proxy.socks_remote_dns: true

network.proxy.type: 1 (缺省是 5，即系统代理，1 是指定的手工代理)

使用 PAC 自动检测代理间接使用 HTTP、HTTPS 代理，具体参数如下：

network.proxy.autoconfig_url: http://xx.xx.xx.xx/http.js?t=001

network.proxy.type: 2

注意：Firefox 使用的 PAC 文件必须是无用户认证，js 结尾的 URL 没有用户认证，pac 结尾的 URL 有用户认证，最好先导入 CA 证书（打开 Firefox 浏览器，请求 https://xxx/myca.crt，输入用户名密码，再导入 CA 证书，再重启 Firefox 浏览器），再使用 https URL 的 pac 文件及 HTTPS 代理（https://xx.xx.xx.xx/https.js）。

4.3 iOS 系统下代理服务器的设置

4.3.1 iOS 系统设置 HTTP 代理

iOS 系统代理服务器设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/proxy/ios_proxy.html

在“设置”界面中，选择“无线局域网”栏目，点击现有的无线连接，在右下方的“HTTP 代理”子项中，选择“手动”项，并填写正确“服务器”和“端口”值。如果需要用户认证，就打开“鉴定”开关，填写正确的用户名和密码。如图 4-10 所示。

图 4-10 iOS 系统下设置手动代理服务器

注意:

1）为了使用 HTTP 代理的“解密 HTTPS”的功能，客户端必须事先下载安装自签名 CA 证书，具体参见“**2.2.3 iOS 系统的证书导入**”

4.3.2 iOS 系统设置 Socks、HTTPS 代理

iOS 系统下可以通过设置 WIFI 的代理类型为“自动”类型来使用 Socks、

HTTPS 代理，如下图 4-11 所示。

图 4-11 iOS 系统下设置 PAC 代理服务器

在“设置”界面中，选择“无线局域网”栏目，点击现有的无线连接，在右下方的“HTTP 代理”子项中，选择“自动”项，并填写正确的 URL。

4.4 其它系统下代理服务器的设置

4.4.1 任天堂 switch 系统设置 HTTP 代理

任天堂 switch 只能使用 HTTP 代理，如下图 4-12 所示。

图 4-12 任天堂 switch 系统下设置 HTTP 代理服务器

5 IKE VPN 客户端设置

5.1 Windows 系统下设置 IKE VPN

IKE VPN 分为两个版本，IKE V1 VPN 即 IPSEC VPN，主要用于网关到网关 VPN 的连接，Windows 没有集成 IPSEC VPN 拨号设置，需要安装 CISCO VPN Client、ShrewSoft VPN 等专门的客户端软件；IKEV2 VPN 是最新的版本，安全性以及性能有很大的提高，主要用于客户端到网关以及网关到网关的 VPN 连接，Win10 系统集成有 IKEV2 VPN 拨号设置，因此不需要专门的软件。以下分别进行介绍。

5.1.1 Windows10 内置的 IKEV2 VPN 设置

Windows10 下使用 IKEV2 VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/ikev2/windows_ikev2.html

注意：

1）为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”；可以通过安装特定的软件实现 Windows 内置的 VPN 拨号随机启动自动拨号,无需人工交互输入，适用于无人值守或普通用户无感知的情形

2）Windows 内置的 IKEV2/SSTP/L2TP/PPTP VPN 连接成功后，浏览器的连接将忽视原有 IE 的代理设置，使用 Proxy SwitchyOmega 插件的 Chrome 浏览器不受影响，如果要设置代理，需要单独给每个 VPN 连接设置代理。

3）新建的 IKEV2 VPN 连接缺省不使用 VPN 隧道作为连接后的默认网关，如需启用，请依次打开“控制面板\网络和 Internet\网络连接>[IKEV2 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>在远程网络上使用默认网关”并启用。

Windows 系统下设置 IKEV2 VPN 分为三个步骤：建立 VPN 连接、修改网络的默认网关属性以及下载安装自签名 CA 证书。注意：当管理员为服务器地址申请了真实域名证书后，可不必再下载安装自签名 CA 证书。

1）建立 VPN 连接

鼠标双击右下角“网络”图标，弹出 VPN 列表，如下图 5-1 所示，点击任意项目，弹出“网络和 INTERNET”窗口，如图 5-2 所示。

图 5-1 鼠标双击右下角“网络”图标

图 5-2“网络和 INTERNET”窗口

点击最上面的“添加 VPN 连接”项目，出现“添加 VPN 连接”窗口，如下图 5-3 所示。依次输入正确的内容，最后点击“保存”按钮，其中“服务器名称或地址”栏可以是 IP 或域名。

注意：

I、IKEV2 VPN 的“服务器名称或地址”需要和 VPN 服务器的服务器证书中的 CN 值保持一致（由管理端决定），而 VPN 服务器的 CA 证书需要安装到客户端 Windows 系统中。

II、如果内容是域名（缺省是 zstdadi.com），且不是真实的域名，那么还要将域名解析成 IP，可以通过修改 C:\Windows\System32\drivers\etc\hosts 文件，或者设置专门的 DNS 服务器做解析。

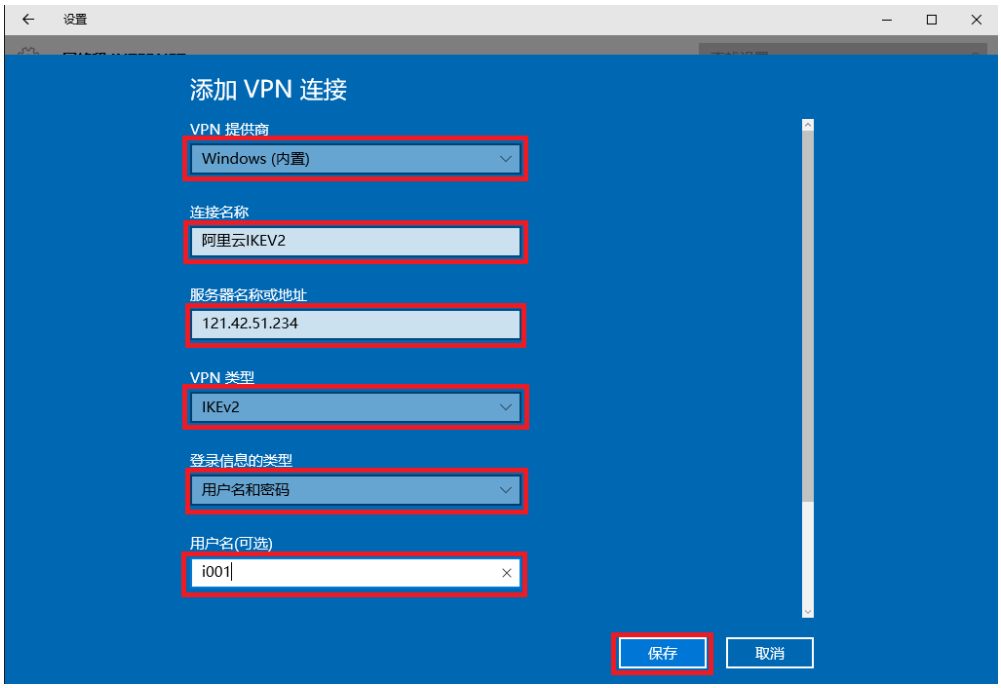


图 5-3“添加 VPN 连接”窗口

添加成功后，返回列表，在末尾找到新添加的连接名称，需要连接时可以点击该项，再点击下方的“连接”按钮，就可以连接 VPN 了，如下图 5-4 所示。

图 5-4 连接 VPN

2）修改网络的默认网关属性

VPN 连通后，只能访问 10.32.0.1，为了能访问 10.32.0.0/24 网络及其它公网 IP，需要使 VPN 连接成为缺省路由，即需要对该 VPN 连接的网络属性进行修改。具体过程如下图 5-5-1、2、3、4、5 所示。

图 5-5-1 修改 VPN 连接的默认网关的网络属性 1

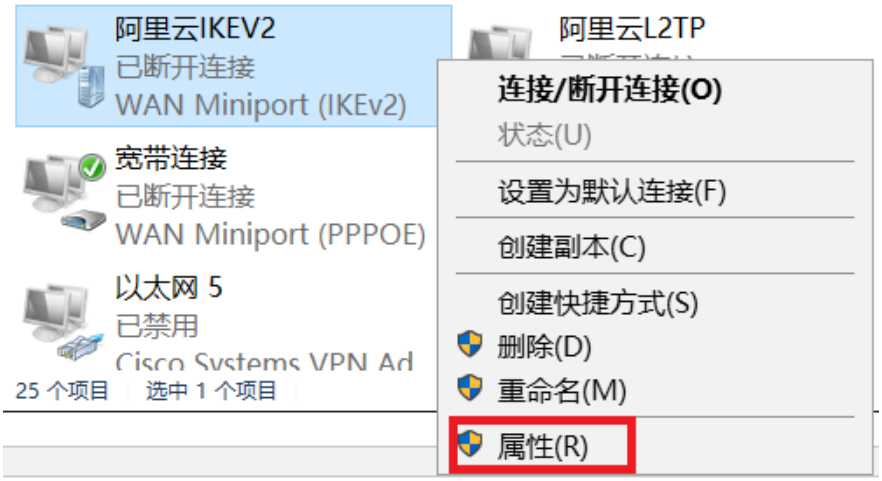


图 5-5-2 修改 VPN 连接的默认网关的网络属性 2

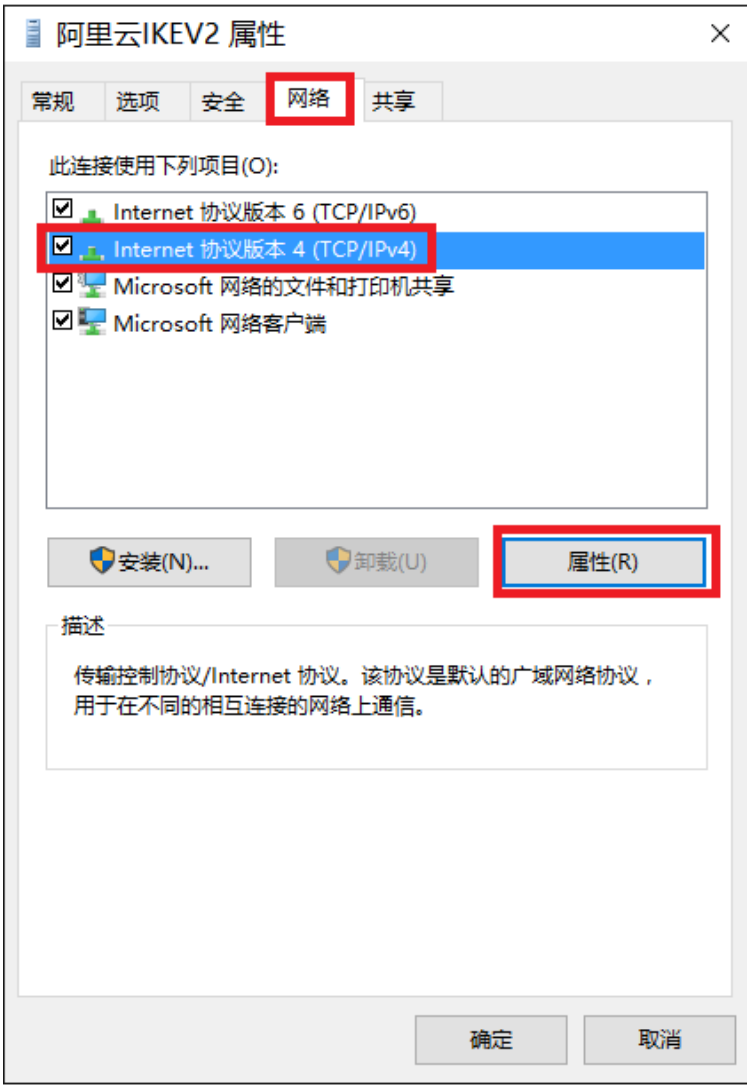


图 5-5-3 修改 VPN 连接的默认网关的网络属性 3

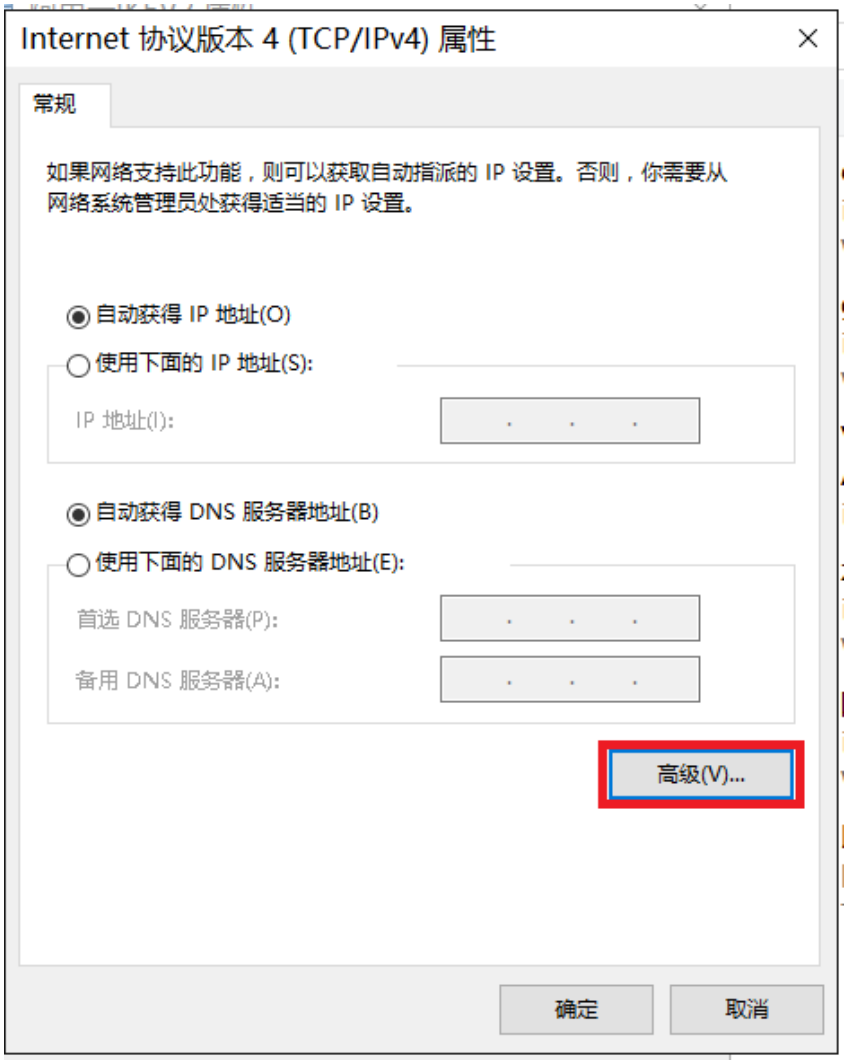


图 5-5-4 修改 VPN 连接的默认网关的网络属性 4

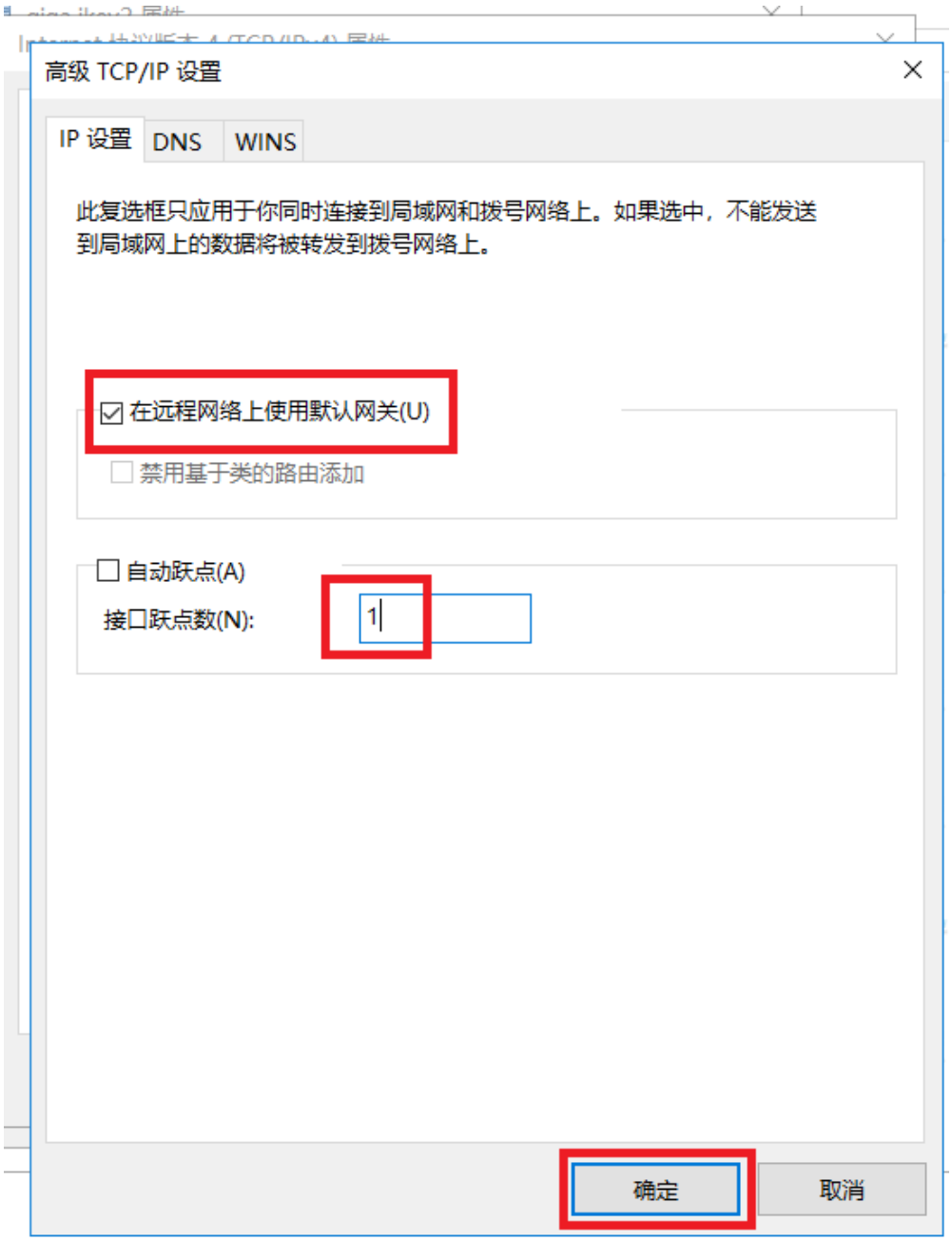
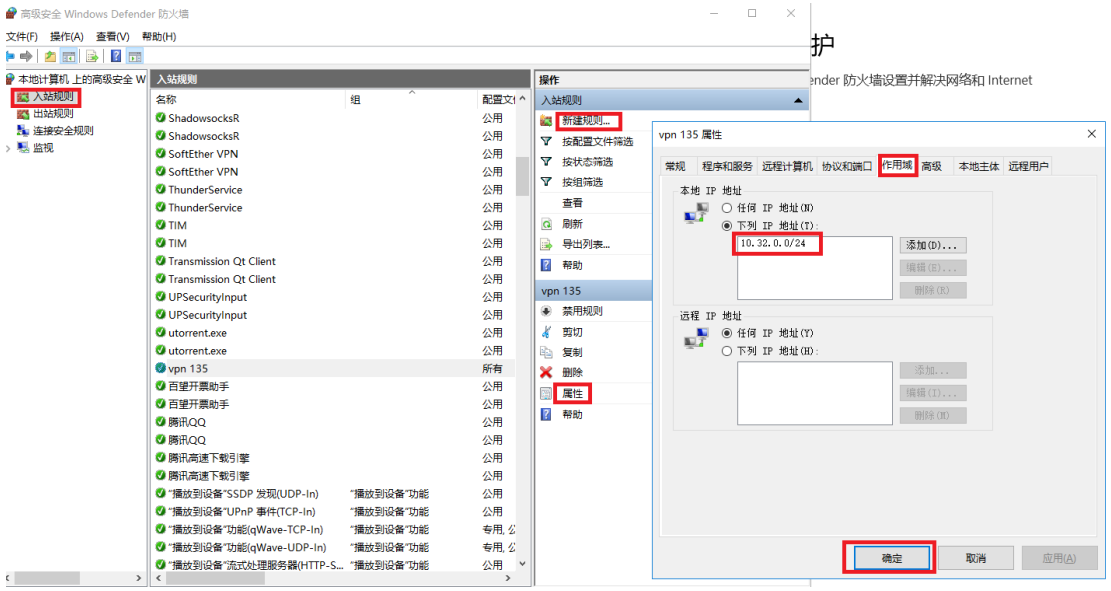


图 5-5-5 修改 VPN 连接的默认网关的网络属性 5

打开网络连接控制面板，找到 VPN 连接，按右键，选择“属性”项，弹出属性窗口，切换到“网络”TAB，选择“Internet 协议版本 4（TCP/IPv4）”项，点击下方的“属性”按钮，在弹出的窗口中点击“高级”按钮，在弹出的窗口中勾选“在远程网络上使用默认网关”项；同时为了避免不必要的 DNS 污染，在“接口跃点数”（Metric）中输入“1”，再一路点击“确定”按钮，保存配置。

3）修改防火墙规则

VPN 连接后，为了能让 VPN 虚拟网络（10.32.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“10.32.0.0/24”，如下图 5-5-6 所示。



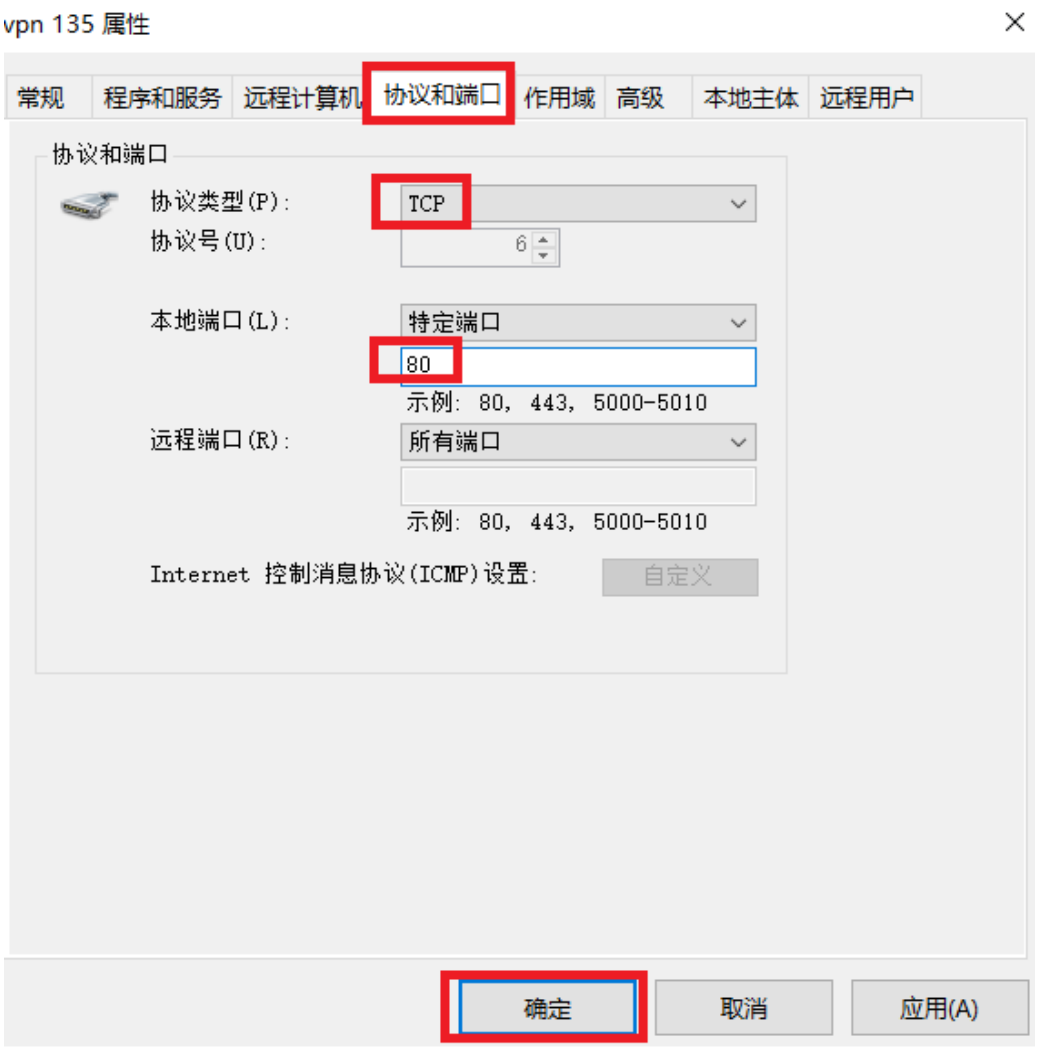
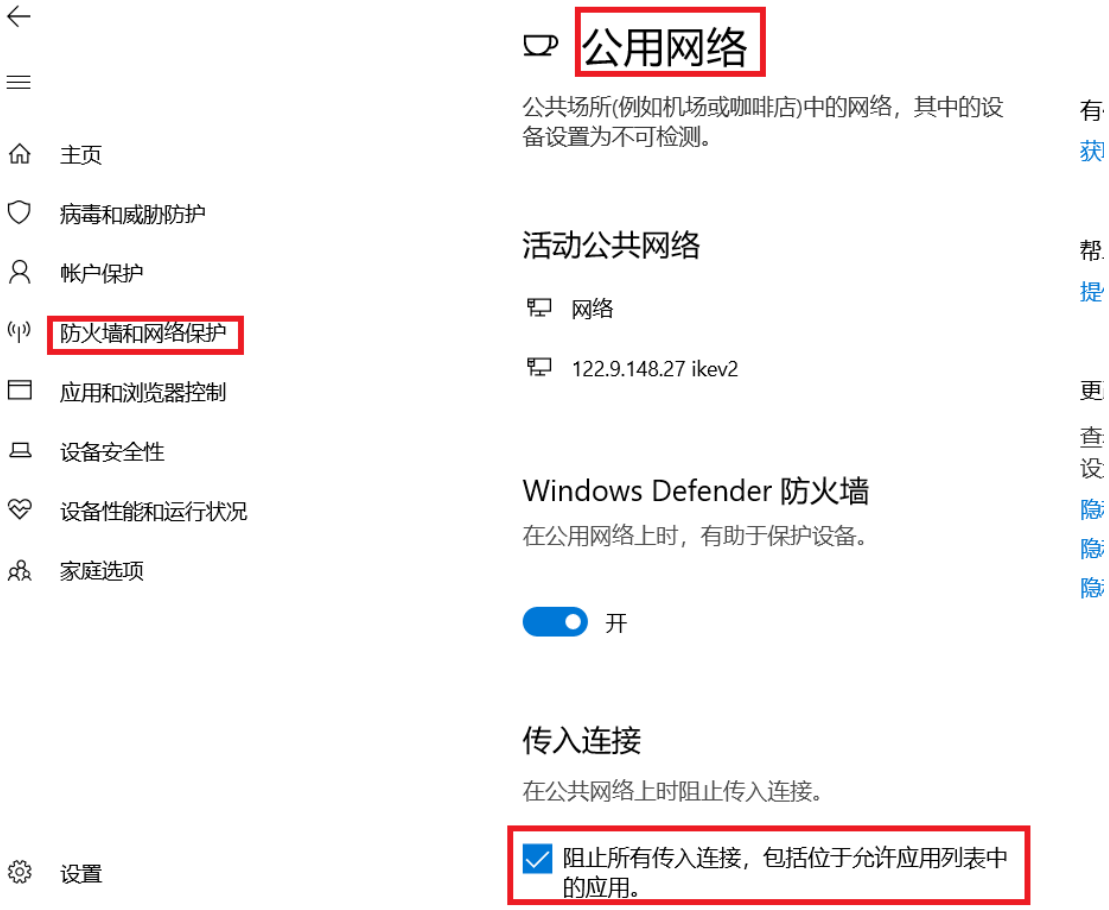


图 5-5-6 修改防火墙策略



另外，还可以一键关闭所有打开的端口，如上图所示。

4）下载安装自签名 CA 证书

对于 IKEV2/OCSERV/SSTP VPN 还需要在连接 VPN 前安装并验证 VPN 服务器的 CA 证书：参见“**2.2.1 Windows 系统的证书导入**”。

导入成功后，才能进行 IKEV2/OCSERV/SSTP VPN 拨号，具体过程如图 5-4 所示。

注意：如果 IKEV2 VPN 有异常，请检查“Remote Access Connection Manager”服务是否启用，参见图 5-6。如有异常，可以停用再启用该服务再试；如果提示“管理员警报”，可以重启 Windows 再试。

图 5-6 与 IKEV2 VPN 有关的服务

注意：

IKEV2 VPN 客户端拨号成功后，缺省设置 VPN 虚拟网卡 10.32.0.1 为 DNS 服务器，但 Windows 的 DNS 查询会同时从 VPN 隧道和物理网卡上发出，并选择响应最快的作为查询结果，而后者会被 ISP 等劫持污染，即存在 DNS 泄露的问题，所以要正确设置物理网卡的 DNS 服务器，例如：用 1.1.1.1，而不用 8.8.8.8，或者删除所有 DNS 服务器只保留 10.32.0.1，但中断 VPN 连接后，又要恢复原 DNS 服务器设置，比较麻烦，可以在 chrome 浏览器打开两个 TAB，一个输入“https://www.google.com”，另一个输入“chrome://net-internals/#dns”，查看 www.google.com 的解析来判断是否存在 DNS 污染。

另外还可以使用 VPN 虚拟网卡 10.32.0.1 的 WEB、Socks 代理服务器上网，让 DNS 解析通过 VPN 隧道在远程解析，这样就没有 DNS 泄露，没有 DNS 污染了，而且不需要修改 IKEV2 VPN 网卡的默认网关属性。

Windows 下其它 VPN 拨号客户端存在同样的 DNS 泄露问题，可以参考上述内容解决。

5.1.2 CISCO VPN Client 安装及使用

注意：CISCO VPN Client 软件是收费软件，目前已经不再更新，官方称只支持到 Win7 系统。

Cisco VPN Client Windows 软件下载链接

软件下载：

http://download.ascensionhealth.org/cisco_vpn_client/ (选择 32 位或 64 位之一)

http://download.ascensionhealth.org/cisco_vpn_client/vpnclient-winx64-msi-5.0.07.0440-k9.exe

Win10 补丁：

http://cisco.techygeekshome.info/windows-10 （步骤）

http://blog.techygeekshome.info/wpdm-package/cisco-vpn-client-fix-for-windows-10-package/?wpdmdl=1372

下载并安装 CISCO VPN Client 软件，对于 Win10 系统还需要安装补丁，依次运行 WinFix.exe、DNEUpdatex64.msi、CiscoVPNClientFixx64.exe，具体过程参考 http://cisco.techygeekshome.info/windows-10。

再运行 CISCO VPN Client 软件，缺省是“C:\Program Files (x86)\Cisco Systems\VPN Client\vpngui.exe”文件，程序主界面如下图 5-7 所示。

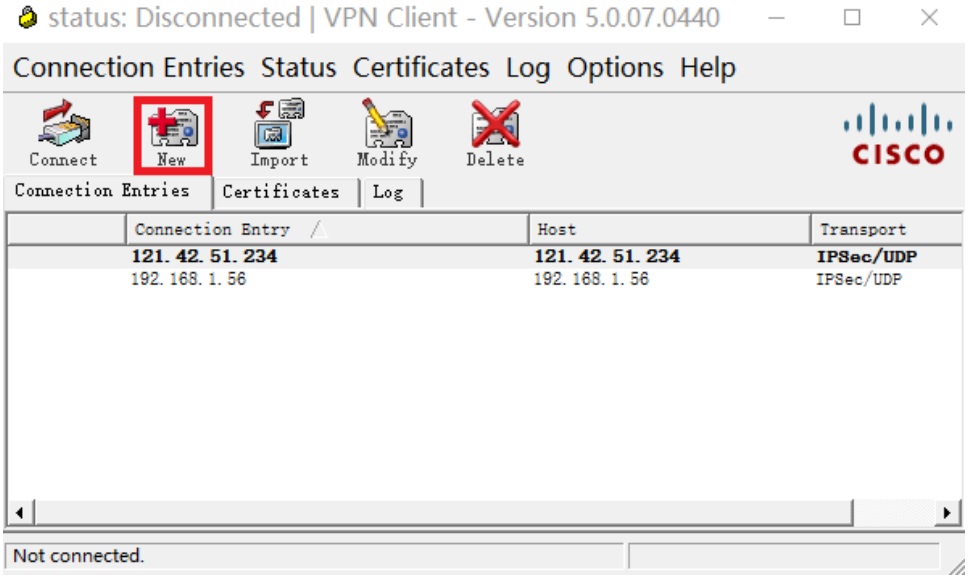


图 5-7 CISCO VPN Client 软件主窗口

点击“New”按钮新建一个 VPN 连接，弹出参数窗口，如下图 5-8 所示。

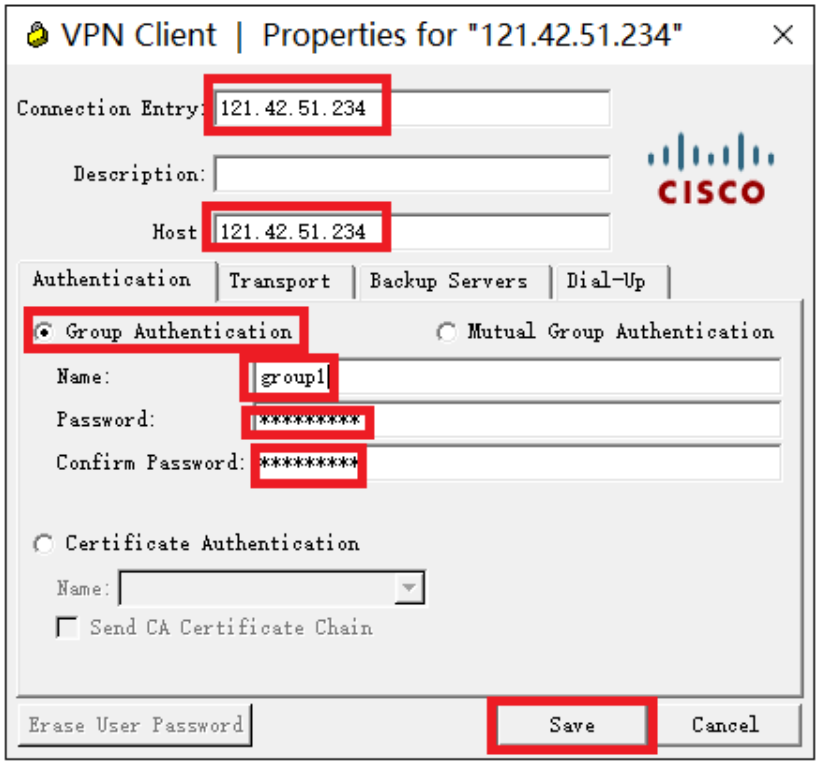


图 5-8 CISCO VPN Client 软件参数窗口 1

依次填写各栏目，最后点击“Save”按钮。其中 Name 栏填写“group1”，Password 栏填写“myPSKkey”。

再点击“Transport”TAB，勾选“Allow Local LAN Access”选项，最后点击“Save”按钮，如下图 5-9 所示。

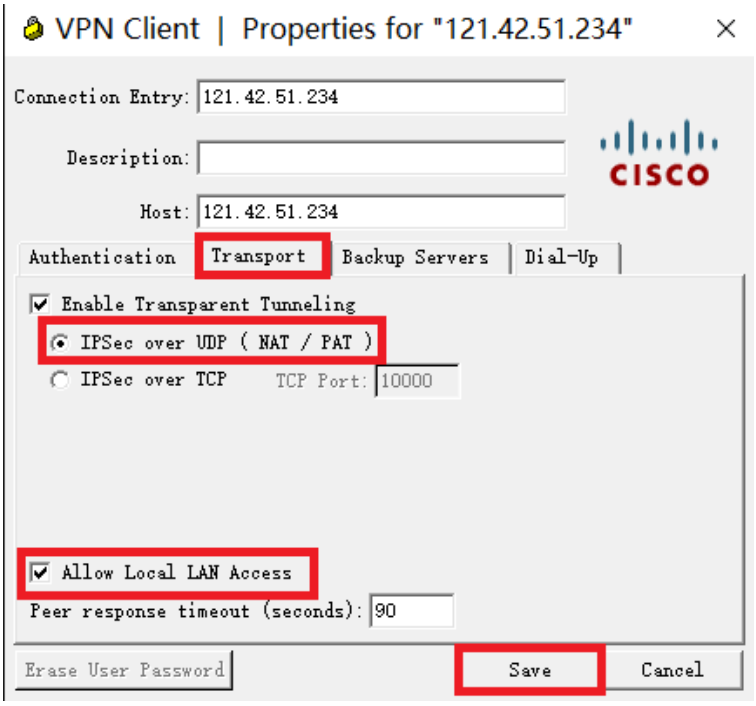


图 5-9 CISCO VPN Client 软件参数窗口 2

返回主界面，双击条目，弹出用户认证窗口，如下图 5-10 所示。

图 5-10 CISCO VPN Client 软件用户认证窗口

输入正确的用户名和密码，连接成功后主窗口关闭，需要到右下角任务栏图标中找到图标，右键点击图标弹出菜单项，点击“Disconnect”中断连接。

5.1.3 ShrewSoft VPN 安装及使用

ShrewSoft VPN Windows 客户端软件下载链接

https://www.shrew.net/download/vpn/vpn-client-2.2.2-release.exe

下载并安装 ShrewSoft VPN 软件，相比 CISCO VPN Client 软件，其在 Win8/Win10 系统下不需要另外安装补丁也可以运行，是免费软件。

安装成功后，在物理网卡的属性里有一项“Shrew Soft Lightweight Filter”，必须是启用状态才能正常使用 ShrewSoft VPN 软件，如下图 5-11 所示。

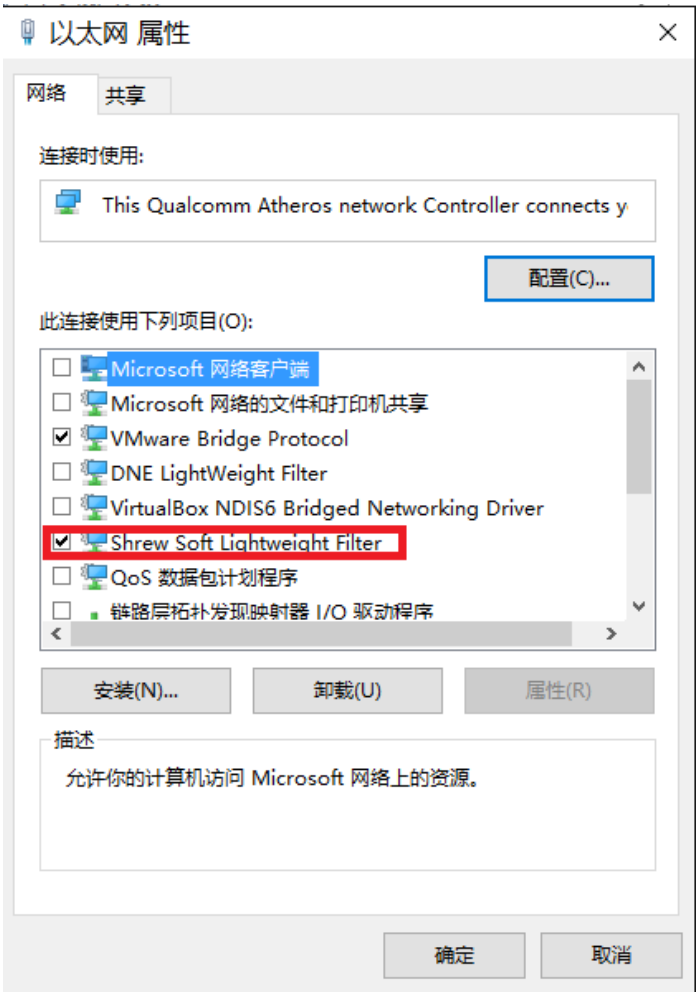


图 5-11 物理网卡与 ShrewSoft VPN 有关的属性

双击桌面的“VPN Access Manager”程序图符，对应 d 文件是“C:\Program Files\ShrewSoft\VPN Client\ipseca.exe”文件，运行 ShrewSoft VPN 软件，程序主界面如下图 5-12 所示。

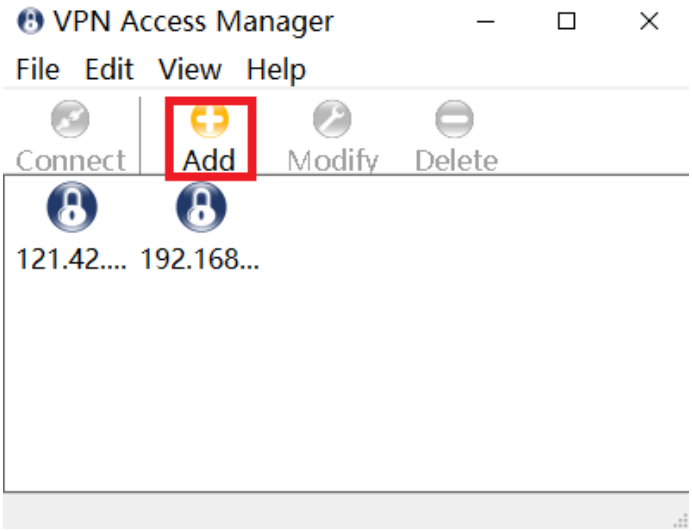


图 5-12 ShrewSoft VPN 软件主窗口

填写各个参数窗口的设置，如下图 5-13-1、2、3、4、5、6、7、8、9 所示。

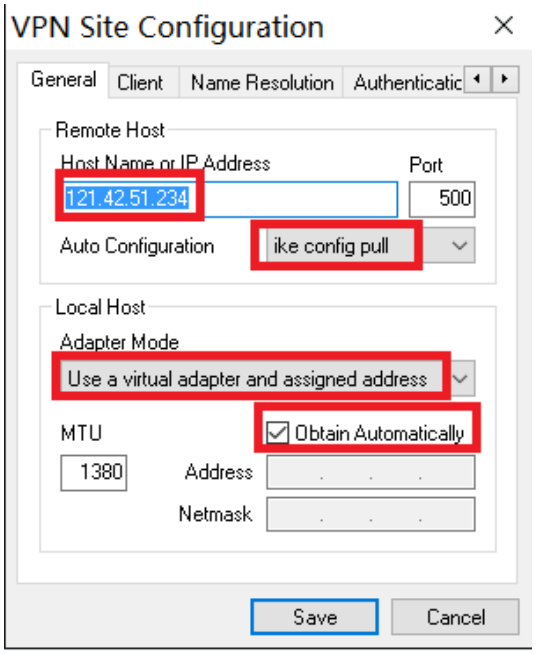


图 5-13-1 ShrewSoft VPN 软件参数窗口 1

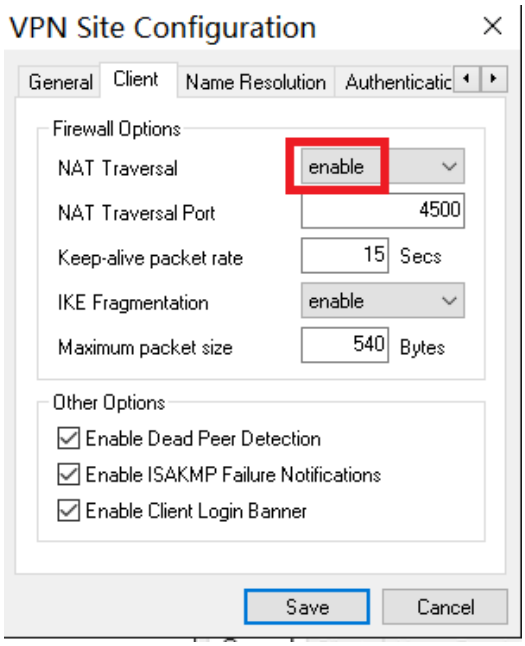


图 5-13-2 ShrewSoft VPN 软件参数窗口 2

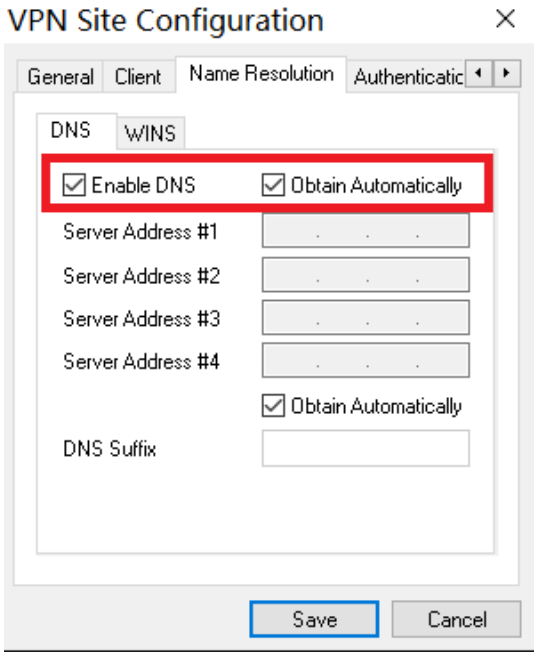


图 5-13-3 ShrewSoft VPN 软件参数窗口 3

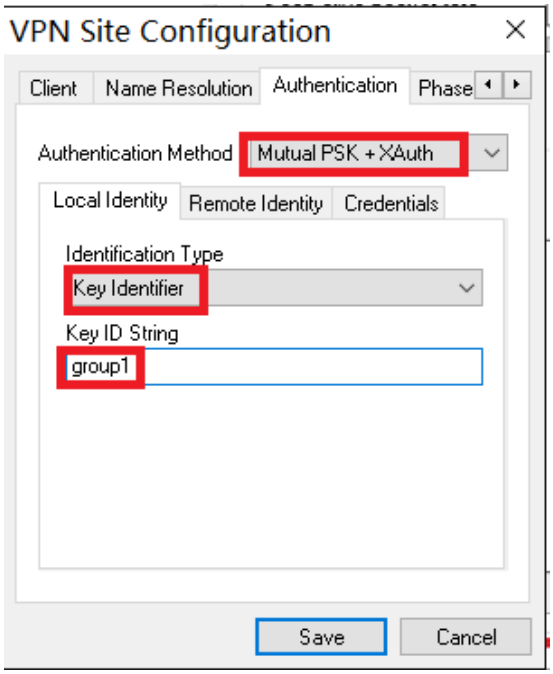


图 5-13-4 ShrewSoft VPN 软件参数窗口 4

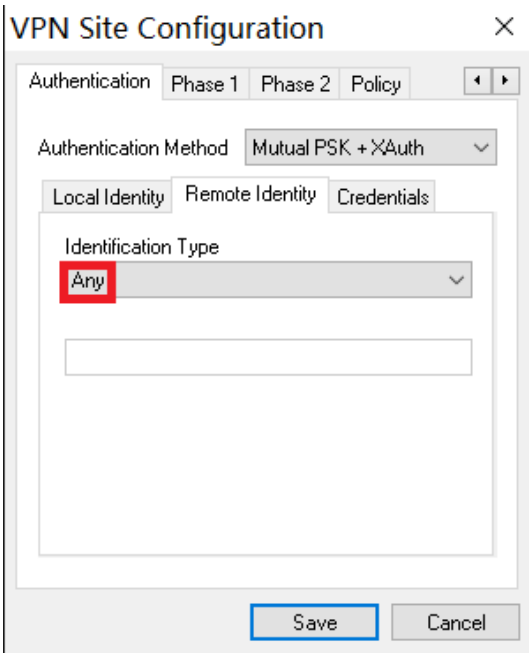


图 5-13-5 ShrewSoft VPN 软件参数窗口 5

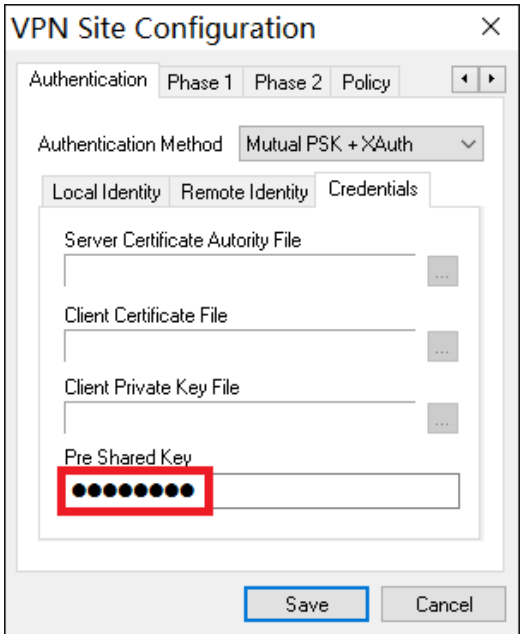


图 5-13-6 ShrewSoft VPN 软件参数窗口 6

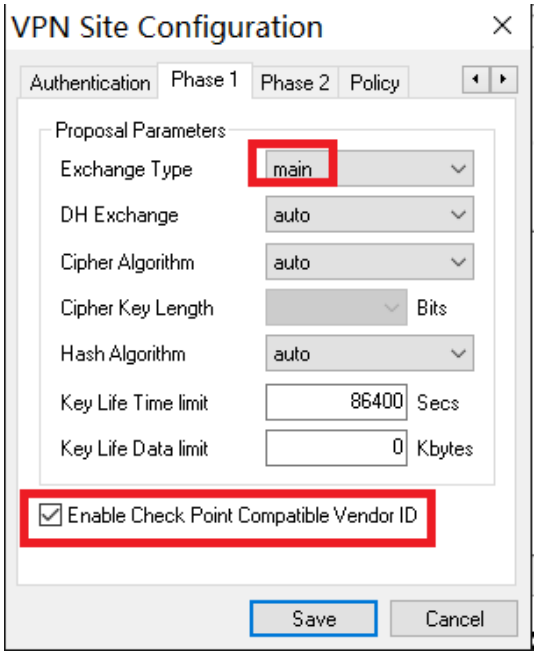


图 5-13-7 ShrewSoft VPN 软件参数窗口 7

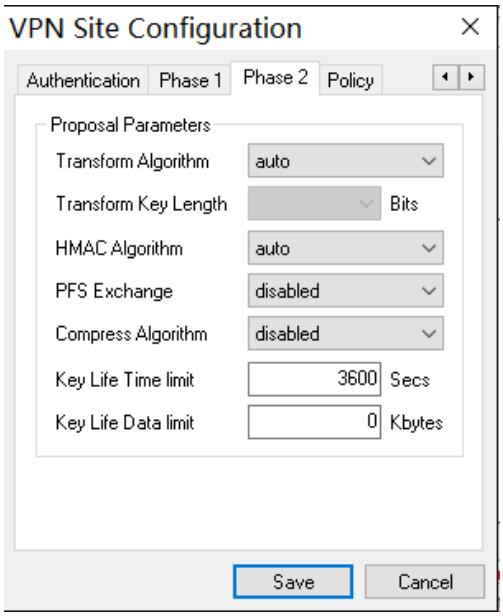


图 5-13-8 ShrewSoft VPN 软件参数窗口 8

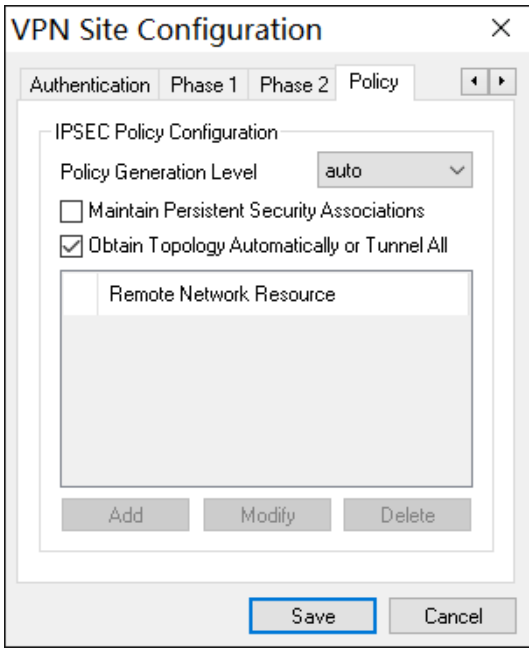


图 5-13-9 ShrewSoft VPN 软件参数窗口 9

其中，图 5-13-4 中的 Key ID String 栏填写“group1”，图 5-13-6 中的 Pre Shared Key 栏填写“myPSKkey”，图 5-13-7 中的 Exchange Type 选择“main”选项。最后点击“Save”按钮，保存设置。

返回主界面，双击图标，弹出用户认证窗口，如下图 5-14 所示。

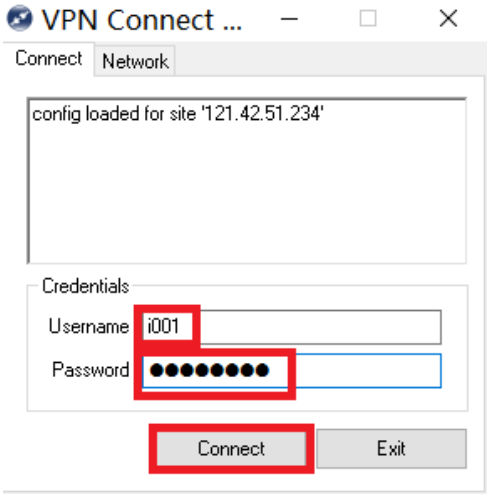


图 5-14 ShrewSoft VPN 软件用户认证窗口

输入正确的用户名和密码，点击“Connect”按钮连接，连接成功后信息栏显示“tunnel enabled”，点击“Disconnect”按钮中断连接。

5.2 Android 系统下设置 IKE VPN

5.2.1 安卓系统内置的 IKE VPN 设置

安卓系统 IPSEC VPN 设置示例
http://www.trustcomputing.com.cn/help/cn/dadi/ikev2/android_ipsec.html

安卓系统内置的 VPN 拨号连接有 IKEV1 VPN 即 IPSEC VPN，但没有 IKEV2 VPN（12+），而且华为、荣耀部分手机/系统存在问题，可以连通但不能获得虚拟 IP。具体操作分为两个步骤：下载安装自签名 CA 证书以及建立 VPN 连接。注意：当管理员为服务器地址申请了真实域名证书后，可不必再下载安装自签名 CA 证书。

为了在重新打开系统时 VPN 不中断，需要在“电池”设置中，启用“休眠时始终保持网络连接”选项。

1、下载安装自签名 CA 证书

对于 IKEV2 VPN（非 PSK）需要在连接 VPN 前安装 VPN 服务器的 CA 证书：可以通过电子邮件、聊天软件、U 盘等方式得到 CA 证书，也可以通过（quickmark APP 扫描二维码，再通过 chrome 浏览器）在线下载的方式得到，具体说明参考“2.2.2 安卓系统的证书导入”。

2、建立 VPN 连接

1）点击桌面齿轮性“设置”图标，进入“设置”页面；

2）点击“更多”项，进入“无线和网络”页面；

3）点击“VPN”项，进入“VPN”页面；

4）点击底部的“添加 VPN 网络”按钮，进入“编辑 VPN 网络”页面，依次填写各项内容，其中，类型选择“IPSec Xauth PSK”项，IPSec 标识符填写“group1”，IPSec 预共享密钥填写“myPSKkey”，安卓 IPSec VPN 可能无法实现自定义 VPN 路由（如果不想让 VPN 连接成为缺省路由，就打开“显示高级选项”开关，在“转发路线”栏中填写“10.32.0.0/24” ，相当于只是修改 DNS 服务器，其它流量还是走原来的 WIFI 或移动数据流量网络）；

5）最后点击“保存”按钮，返回“VPN”页面；

6）再点击 VPN 项，弹出用户认证窗口，输入用户名和密码，就可以连接 VPN 了。

如下图 5-15-1、2、3、4、5、6 所示。

图 5-15-1

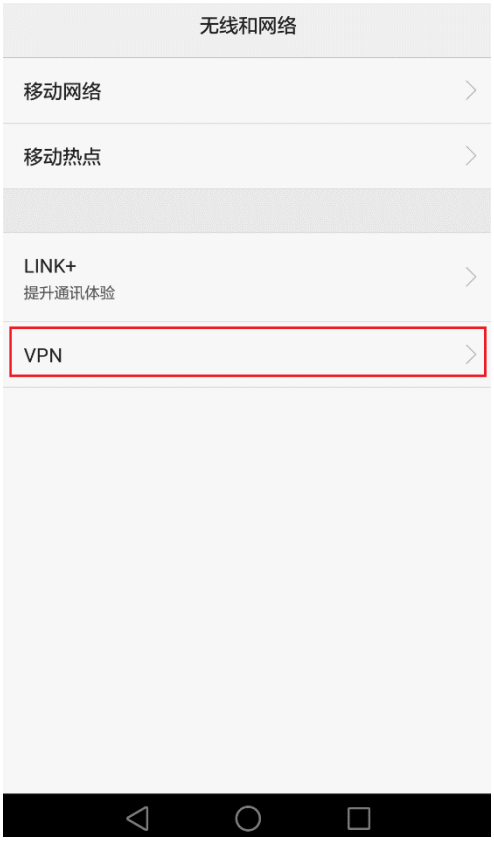


图 5-15-2

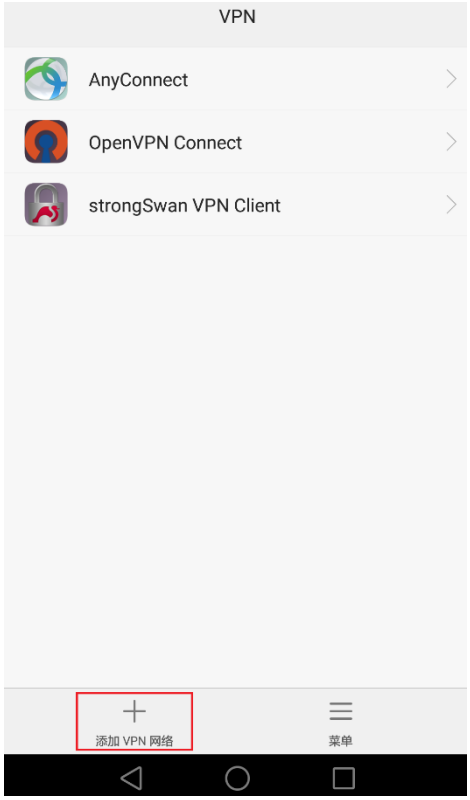


图 5-15-3

图 5-15-4

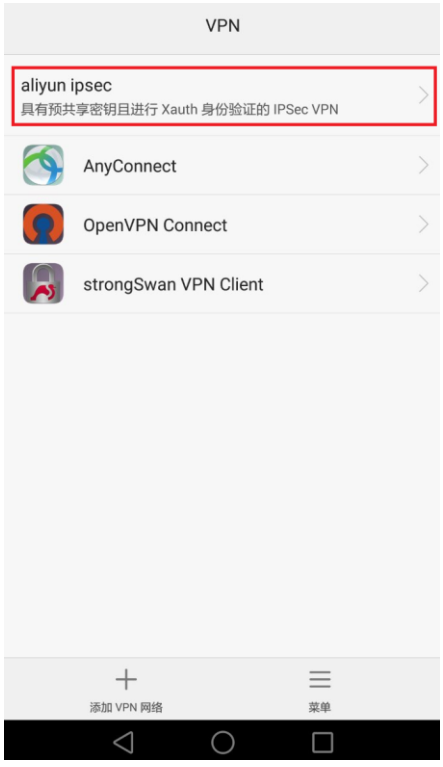


图 5-15-5

图 5-15-6

图 5-15-A 安卓系统自带的 PSK IPSEC VPN 设置

类型还可以选择“IPSec Hybrid RSA”项，事先需要安装 CA 证书，不同之处见下图所示：

图 5-15-7

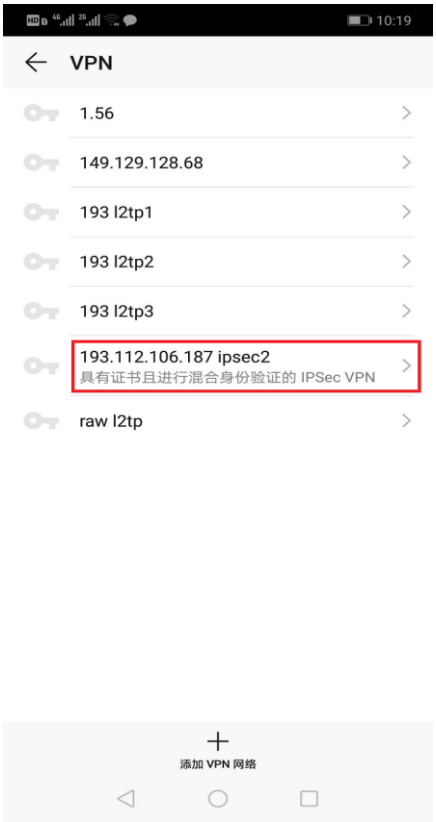


图 5-15-8

图 5-15-B 安卓系统自带的 Hyper RSA IPSEC VPN 设置

5.2.2 strongSwan VPN client 安装及使用

strongSwan VPN client 安卓软件下载链接

https://play.google.com/store/apps/details?id=org.strongswan.android

https://apkpure.com/strongswan-vpn-client/org.strongswan.android

http://www.trustcomputing.com.cn/tools/strongSwan VPN Client_v2.3.0.apk

strongSwan VPN client 软件是安卓系统下的专门的 IKEV2 VPN 客户端软件，具有断线重连、锁屏仍保持连接等高可用性功能。

下载 strongSwan VPN client 软件，安装后，点击桌面的 strongSwan VPN client 程序图符，运行 strongSwan VPN client 软件，如图 5-16 所示。

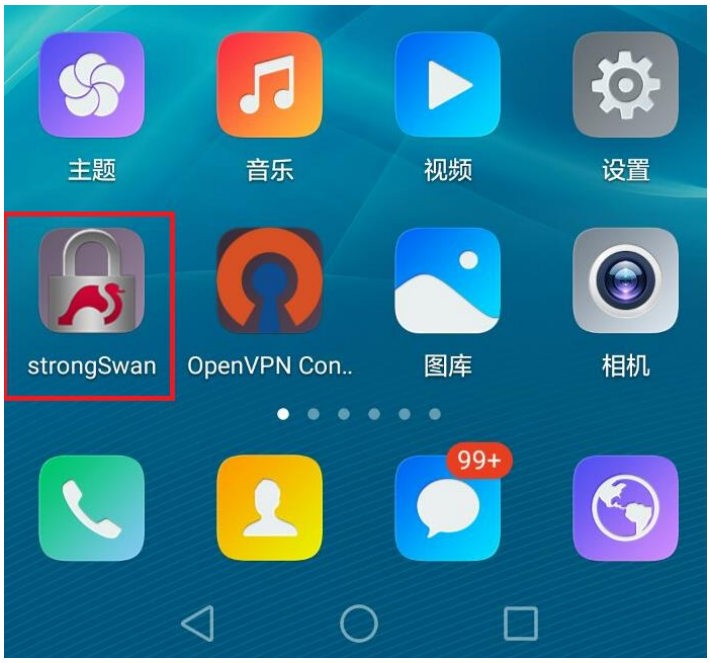


图 5-16 桌面上的 strongSwan VPN client 安卓软件图标

具体设置过程如图 5-17-1、2、3、4、5、6 所示。

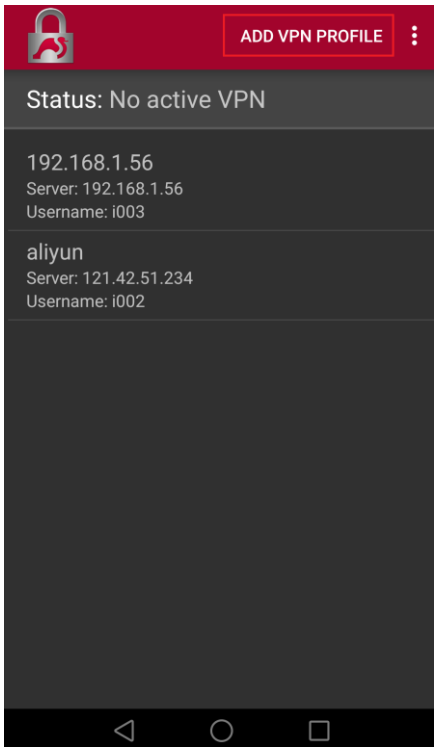


图 5-17-1

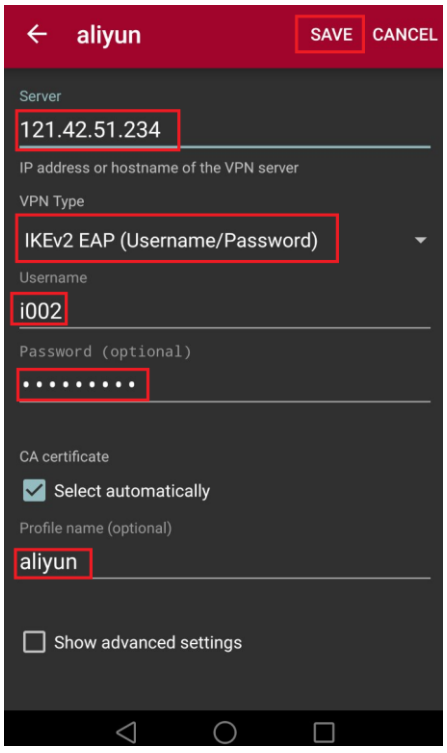


图 5-17-2

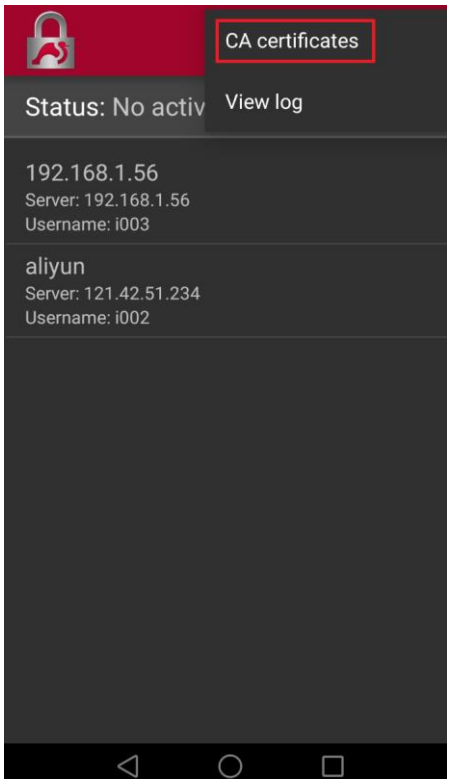


图 5-17-3

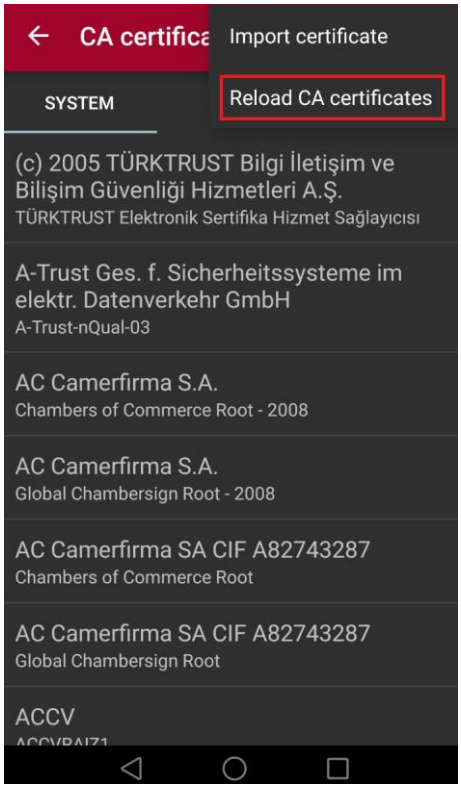


图 5-17-4

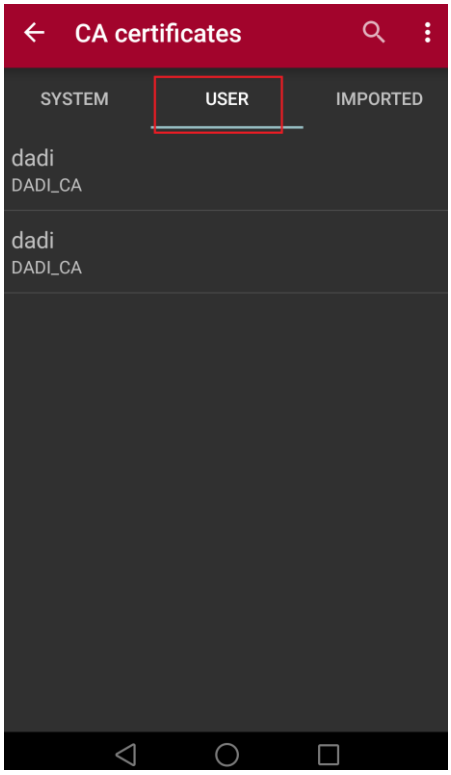


图 5-17-5

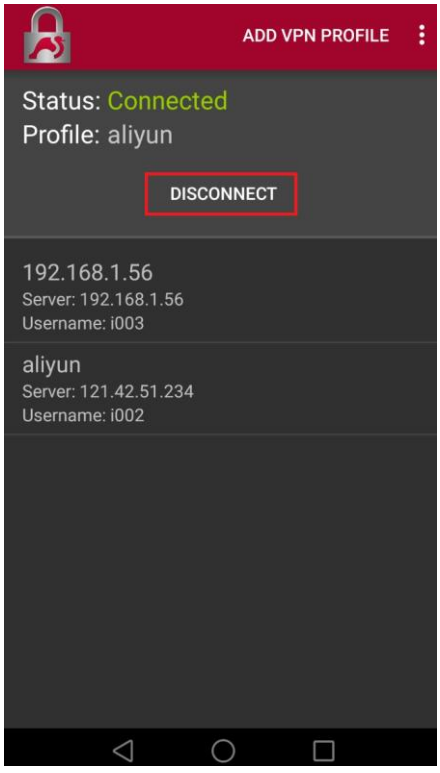


图 5-17-6

图 5-17 strongSwan VPN client 安卓软件界面

安卓系统下 strongSwan VPN client 软件具体设置过程描述如下：

1）点击右上方的“ADD VPN PROFILE”按钮，在弹出的窗口中依次输入内容，最后点击“SAVE”按钮；

2）通过 chrome 浏览器下载安装自签名 CA 证书，URL 类似“http://121.42.51.234/myca.crt”这样，具体过程参考“**2.2.2 安卓系统的证书导入**”内容；

3）再点击右上方的“  ”按钮，选择“CA certificates”项，再点击右上方的“  ”按钮，选择“Reload CA certificates”项，再切换到“USER”TAB，可以看到添加了新的证书；

4)返回主界面,点击 VPN 名称,就可以连接 VPN 了,连通后,点击“DISCONNECT”按钮，退出 VPN 连接。

注意：

1、 如果不需要让 VPN 成为默认网关，而只需要连接 10.32.0.0/24 虚拟网络，则可以在“拆分隧道”的“Custom subnets”栏中填写“10.32.0.0/24”；

2、 如果用户能拨号成功，但无法使用网络，则要求管理员重新设置一个绑定 IP（10.32.0.11 可能有问题）再重新拨号试试；

3、为了在重新打开系统时 VPN 不中断，需要：

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2)手机管家--应用启动管理--找到应用,不让它自动管理,选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

5.3 iOS 系统下设置 IKEV2 VPN

iOS 系统 IKEV2 VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/ikev2/ios_ikev2.html

iOS 系统下设置 IKEV2 VPN 过程描述如下：

1）点击桌面的“设置”图符，再点击“通用”菜单项，再点击右下方的“VPN”菜单项，如果已经有了 VPN 设置，则在左上方就有 VPN 菜单项；

2）再点击右边下方的“添加 VPN 配置…”菜单项，选择类型为“IKEv2”或“IPSec”，输入“描述”、“服务器”、“远程 ID”、“密钥”、“用户名”、“密码”，其中，“服务器”、“远程 ID”均为 VPN 服务器的 IP 或域名，IPSec 的“密钥”是“myPSKkey”，再点击右上角的“完成”按钮；

3）服务器非真实域名时，需要事先通过浏览器下载并安装 CA 证书，参考“**2.2.3 iOS 系统的证书导入**”；

4）返回 VPN 界面后，勾选 VPN 连接，再点击“状态”栏“未连接”开关。详见下组图 5-18 所示。

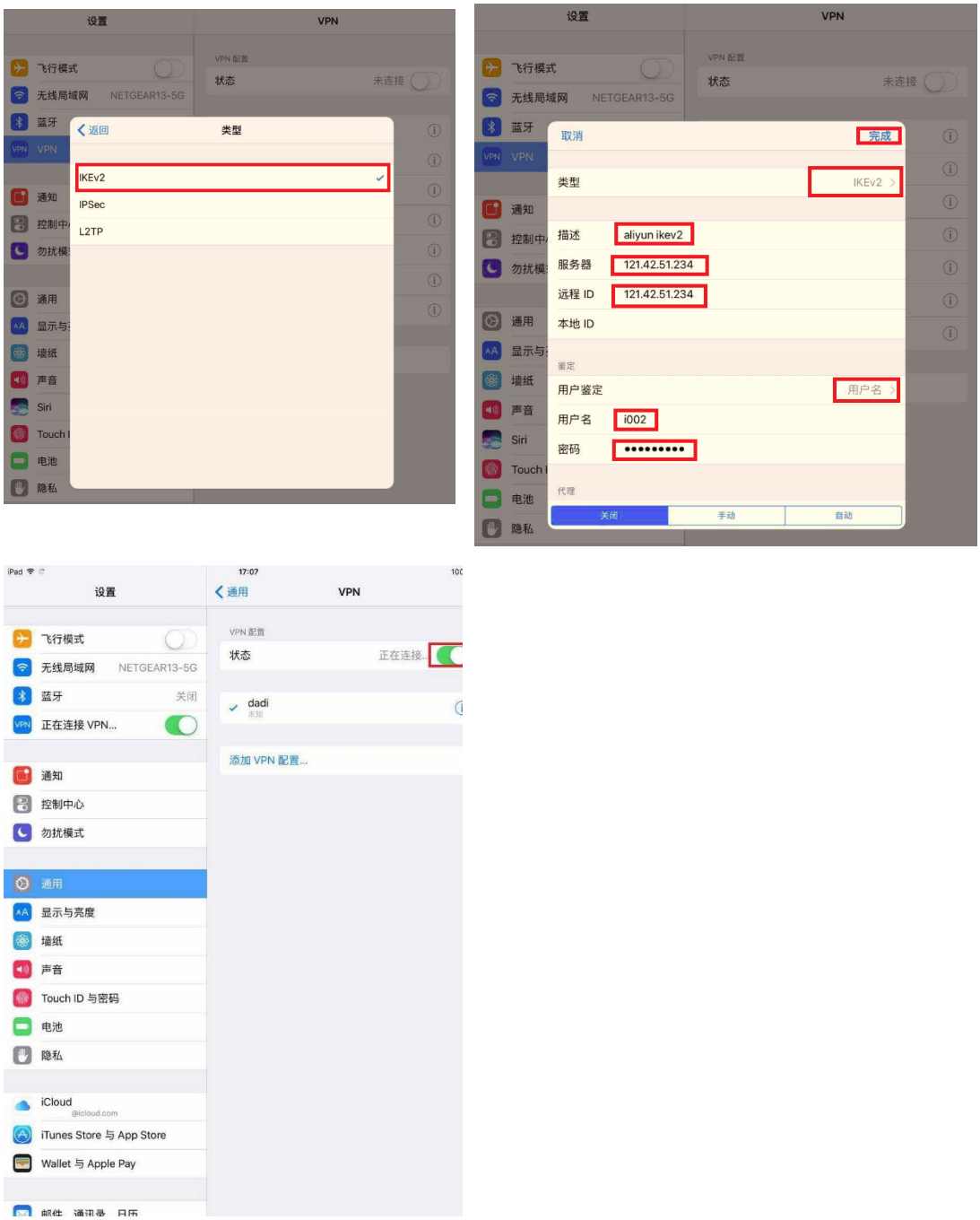


图 5-18 iOS 系统下新建 IKEV2 VPN 连接

6 Cisco AnyConnect VPN 客户端设置

6.1 Windows 系统下设置 Cisco AnyConnect VPN 客户端

OCSERV VPN 客户端软件全称是“Cisco AnyConnect Secure Mobility

Client”，它是 CISCO 公司开发的最新的 VPN 客户端软件，是收费软件。

Windows 安装使用 Cisco AnyConnect VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/ocserv/windows_ocserv.html

注意：Cisco AnyConnect VPN 连接成功后，如果原来设置了系统代理，则浏览器仍然通过原来的代理进行连接。

Cisco AnyConnect VPN Windows 客户端软件下载链接

https://software.cisco.com/download/home/283000185

https://www.itechtics.com/download-anyconnect-4-7/

下载并安装 Cisco AnyConnect VPN 客户端软件，文件名类似“anyconnect-win-4.7.01076-core-vpn-predeploy-k9.msi”，双击桌面的“Cisco AnyConnect Secure Mobility Client”程序图符，对应的文件是"C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe"，程序主界面如下图 6-1 所示。

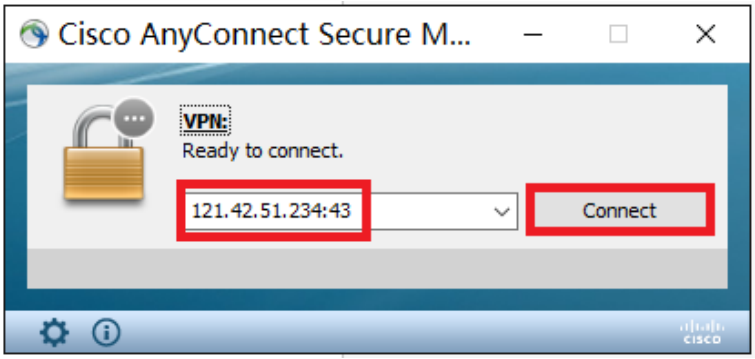


图 6-1 Cisco AnyConnect VPN 客户端软件主界面

在输入框中输入 VPN 服务器域名或 IP 及端口，中间以冒号:隔离，再点击“Connect”按钮，如果非真实域名且没有安装 CA 证书就会弹出警告窗口 1，如下图 6-2 所示。

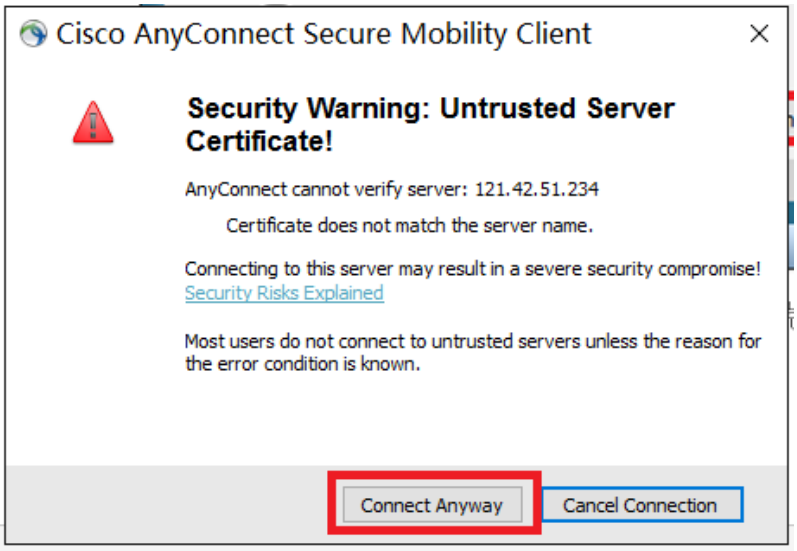


图 6-2 Cisco AnyConnect VPN 客户端软件警告窗口

点击“Connect Anyway”按钮，弹出用户认证窗口 1，如下图 6-3-1 所示。

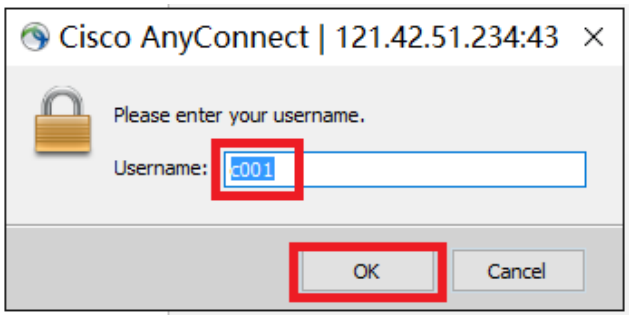


图 6-3-1 Cisco AnyConnect VPN 客户端软件用户认证窗口 1

输入用户名，再点击“OK”按钮，弹出用户认证窗口 2，如下图 6-3-2 所示。

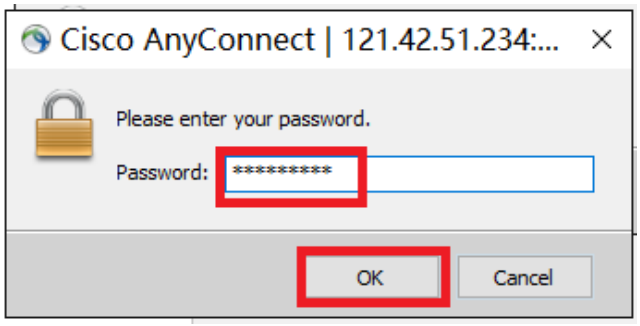


图 6-3-2 Cisco AnyConnect VPN 客户端软件用户认证窗口 2

输入密码，再点击“OK”按钮，如果没有安装 CA 证书会弹出警告窗口 2，如下图 6-4 所示。

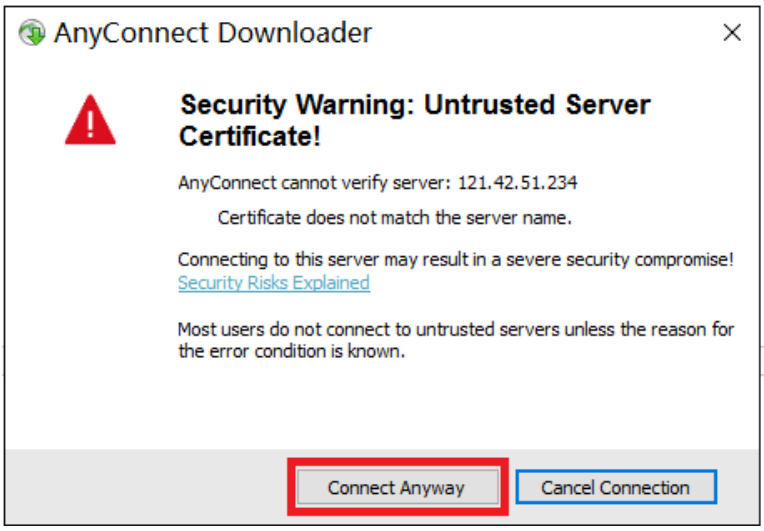


图 6-4 Cisco AnyConnect VPN 客户端软件警告窗口 2

点击“Connect Anyway”按钮，如果一切正常，VPN 连接建立，程序退到右下角的任务栏里。

如果没有显示，则需要设置任务栏属性，右键单击右下角的时间和日期，选择最下面的“属性”项，在弹出来的窗口中点击“选择在任务栏上显示哪些图标”项，再将“Cisco AnyConnect User Interface”项设置为“开”，这样就可以在任务栏里长久显示图标，如下图 6-5 所示。

图 6-5 选择在任务栏上显示 VPN 程序图符

右键点击 Cisco AnyConnect VPN 客户端软件任务栏图标，弹出菜单，如下图 6-6 所示。

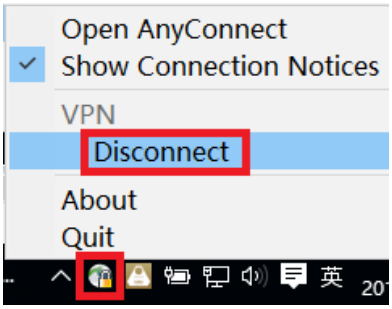


图 6-6 Cisco AnyConnect VPN 客户端软件任务栏图标及菜单

选择“Disconnect”项退出 VPN 连接，选择“Open AnyConnect”打开主界面，如下图 6-7-1 所示。

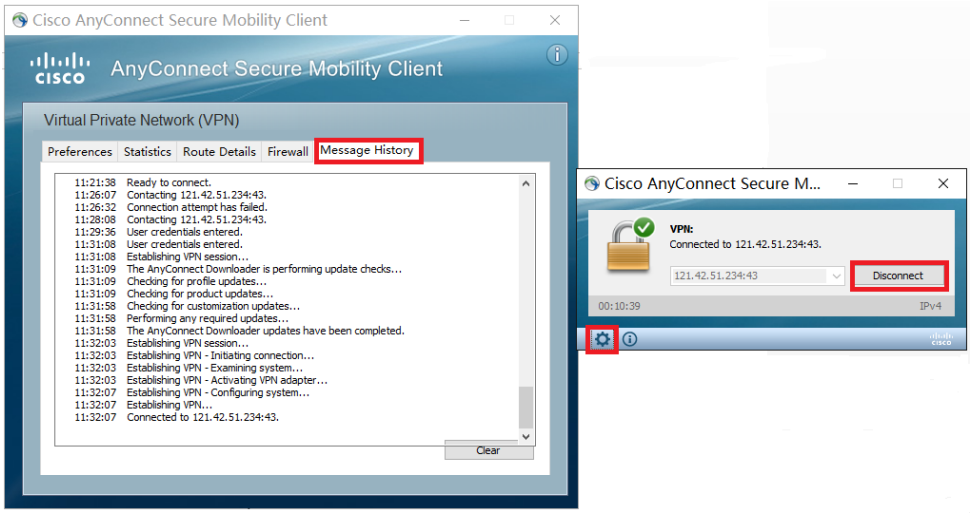


图 6-7-1 Cisco AnyConnect VPN 客户端软件主界面及信息窗口

点击“Disconnect”按钮退出 VPN 连接。点击齿轮按钮，弹出信息查看窗口，切换到“Message History”TAB，可以查看连接过程中显示的信息。

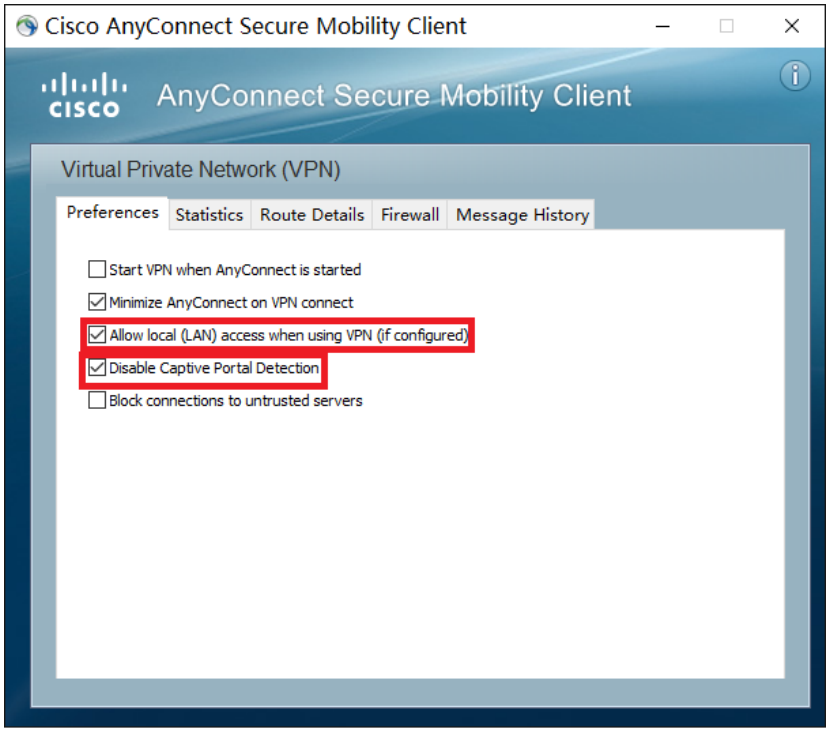


图 6-7-2 Cisco AnyConnect VPN 客户端软件参数窗口

为确保连接成功，需要在 Preferences 参数窗口中勾选“Allow local(LAN)access when using VPN(if configured)”和“Disable Captive Portal Detection”选项，如上图 6-7-2 所示。

为了防止不必要的 DNS 污染，依次打开“控制面板\网络和 Internet\网络连接>Cisco AnyConnect Secure Mobility Client Connection>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>接口跃点数（Metric）”，将“自动跃点”改成“1”。

VPN 连接后，为了能让 VPN 虚拟网络（10.12.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“10.12.0.0/24”，参考图 5-5-6 所示。

OCSERV VPN 客户端无法选择 VPN 路由，只能接受 VPN 服务器下发的路由。

6.2 Android 系统下设置 Cisco AnyConnect VPN 客户端

安卓系统安装使用 Cisco AnyConnect VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/ocserv/android_ocserv.html

Cisco AnyConnect VPN 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf

https://dl.xxshe.com/cisco_anyconnect/com.cisco.anyconnect.vpn.android.avf-4.0.05062.apk

下载 CISCO AnyConnect 客户端软件，安装后，点击桌面的 CISCO AnyConnect 程序图符，运行 CISCO AnyConnect 客户端软件，如图 6-8 所示。

图 6-8 桌面上的 CISCO AnyConnect 安卓客户端软件图标

具体设置过程如图 6-9-1、2、3、4、5、6、7、8 所示。

图 6-9-1

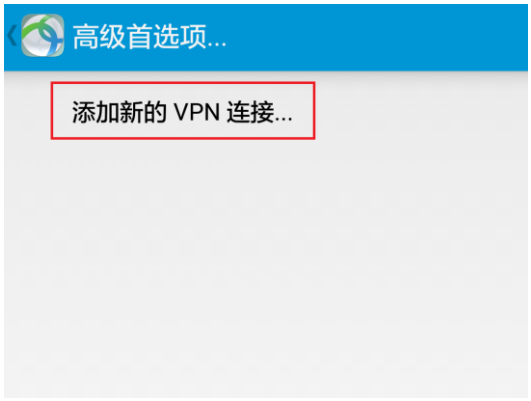


图 6-9-2

图 6-9-3

图 6-9-4

图 6-9-5

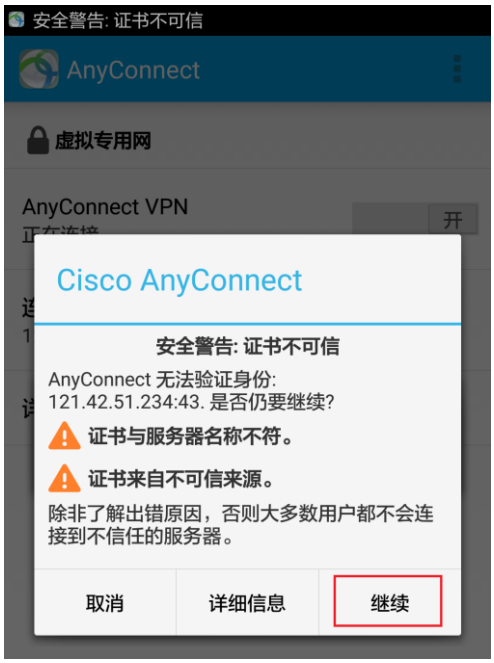


图 6-9-6

图 6-9-7

图 6-9-8

图 6-9 CISCO AnyConnect 安卓客户端软件界面

安卓系统下 CISCO AnyConnect 客户端软件具体设置过程描述如下：

1）点击中间的“连接”项，在新窗口中点击“添加新的 VPN 连接”项；

2）在新窗口中点击“服务器地址”项，在弹出的窗口中输入服务器 IP 及端口，中间以冒号:隔离，再点击“确定”按钮；

3）返回主界面，点击“关”按钮，在弹出的警告窗口中点击“继续”按钮，在之后的窗口中分别输入用户名和密码并点击“连接”按钮，就可以连接 VPN 了，连通后，点击“开”按钮，退出 VPN 连接。

另外，还可以查看诊断信息：

点击主界面右上方的“ ”按钮，选择第一项“诊断”项，再选择最后一项“登陆和系统消息”项，再切换到“系统”TAB，可以查看“接口信息”、“路由信息”和“所有路由表”等信息。

OCSERV VPN 客户端无法选择 VPN 路由，只能接受 VPN 服务器下发的路由。为了在重新打开系统时 VPN 不中断，需要

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

6.3 iOS 系统下设置 Cisco AnyConnect VPN 客户端

iOS 系统安装及使用 Cisco AnyConnect VPN 示例
http://www.trustcomputing.com.cn/help/cn/dadi/ocserv/ios_ocserv.html

Cisco AnyConnect VPN iOS 客户端软件下载链接
https://itunes.apple.com/us/app/cisco-anyconnect/id392790924

下载 CISCO AnyConnect 客户端软件，安装后，点击桌面的 CISCO AnyConnect 程序图符，运行 CISCO AnyConnect 客户端软件，如图 6-10 所示。

图 6-10 桌面上的 CISCO AnyConnect iOS 客户端软件图标

具体设置过程如图 6-11-1、2、3、4、5、6、7、8 所示。


AnyConnect
VPN 连接
虚拟专用网
AnyConnect VPN
添加 VPN 连接...
连接
无连接
详细信息
已断开连接
通用
设置
诊断
关于

图 6-11-1


AnyConnect
VPN 连接
虚拟专用网
AnyConnect VPN
添加 VPN 连接...
连接
无连接
详细信息
通用
设置
诊断
关于
取消
添加 VPN 连接
保存
说明
可选
服务器地址
121.42.51.234:43
高级

图 6-11-2


AnyConnect
设置
虚拟专用网
AnyConnect VPN
连接
121.42.51.234:43
详细信息
通用
设置
诊断
关于
外部控制
已禁用
阻止不信任的服务器
不信任的服务器
AnyConnect 无法验证服务器的身份:
DADI-Server
连接到此服务器可能会导致严重的安全损害!
已说明安全风险
AnyConnect 在默认情况下配置为封锁不信任的服务器。大多数用户都选择保留此设置。
如果更改此设置，AnyConnect 将不再自动阻止连接到潜在的恶意网络设备。
保护我的安全
更改设置

图 6-11-3


AnyConnect
设置
虚拟专用网
AnyConnect VPN
连接
121.42.51.234:43
详细信息
已断开连接
通用
设置
诊断
关于
外部控制
已禁用
阻止不信任的服务器
VPN FIPS 模式
Please modify Settings only when instructed by your system administrator.

图 6-11-4

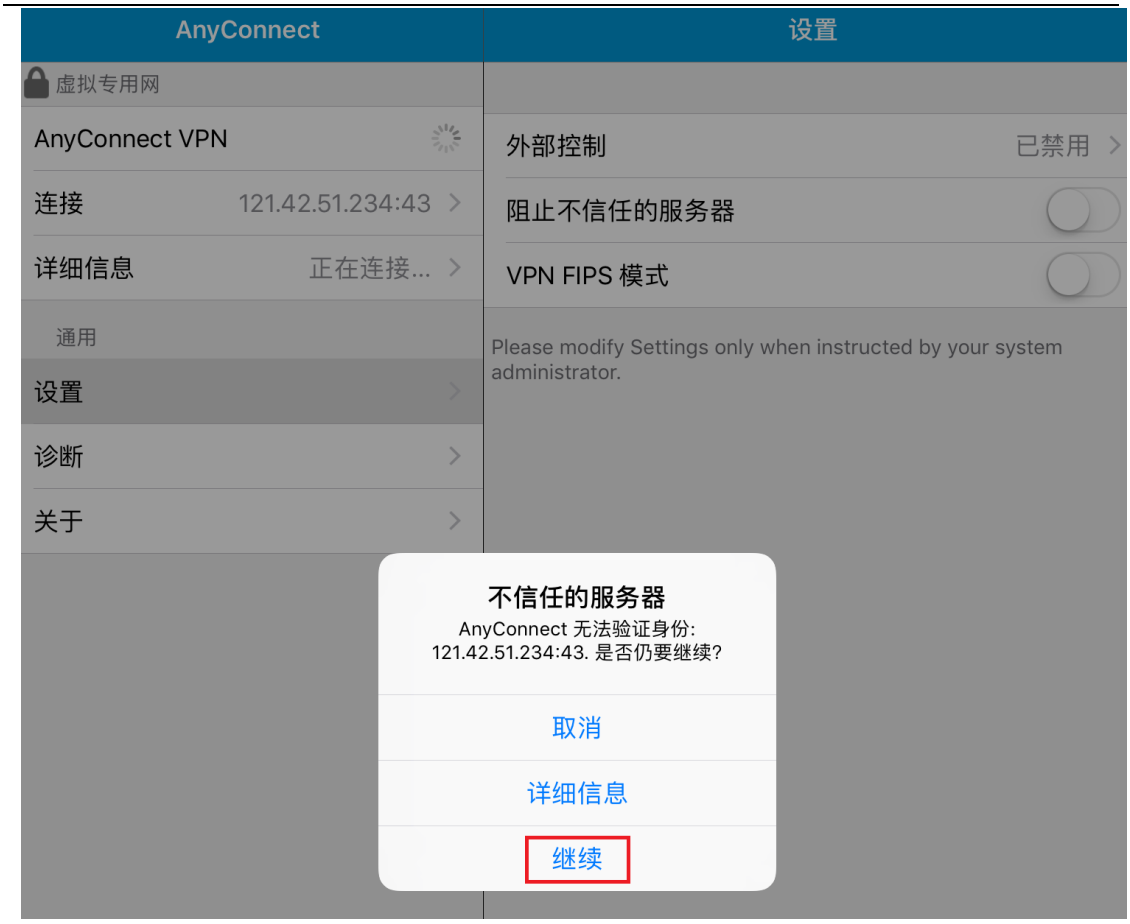

AnyConnect
设置
虚拟专用网
AnyConnect VPN
连接
121.42.51.234:43
详细信息
正在连接...
通用
设置
诊断
关于
外部控制
已禁用
阻止不信任的服务器
VPN FIPS 模式
Please modify Settings only when instructed by your system administrator.
不信任的服务器
AnyConnect 无法验证身份:
121.42.51.234:43. 是否仍要继续?
取消
详细信息
继续

图 6-11-5

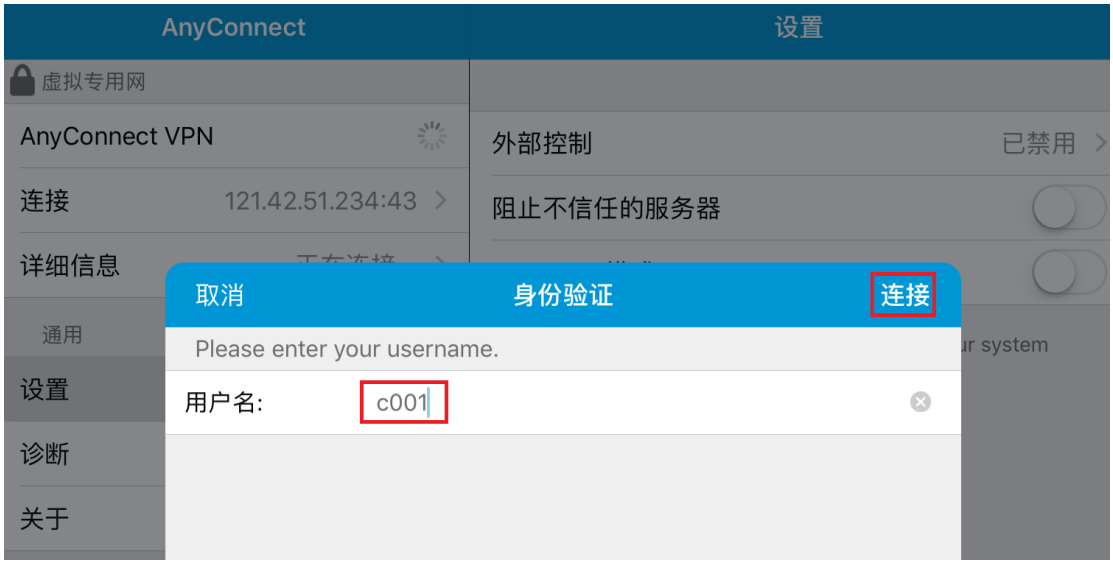

AnyConnect
设置
虚拟专用网
AnyConnect VPN
连接
121.42.51.234:43
详细信息
通用
设置
诊断
关于
外部控制
已禁用
阻止不信任的服务器
取消
身份验证
连接
Please enter your username.
用户名:
c001

图 6-11-6

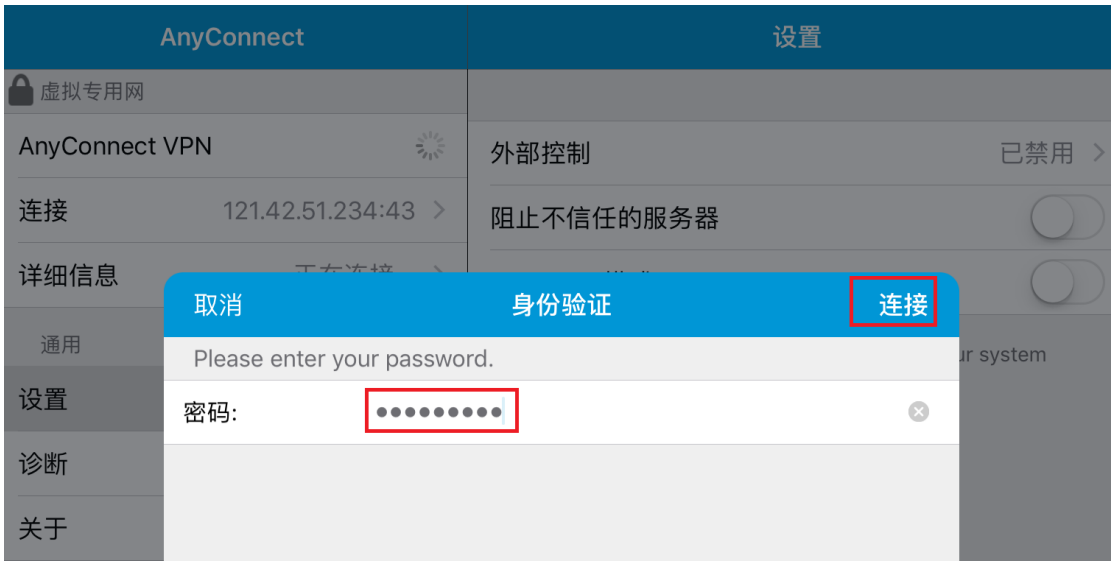


图 6-11-7

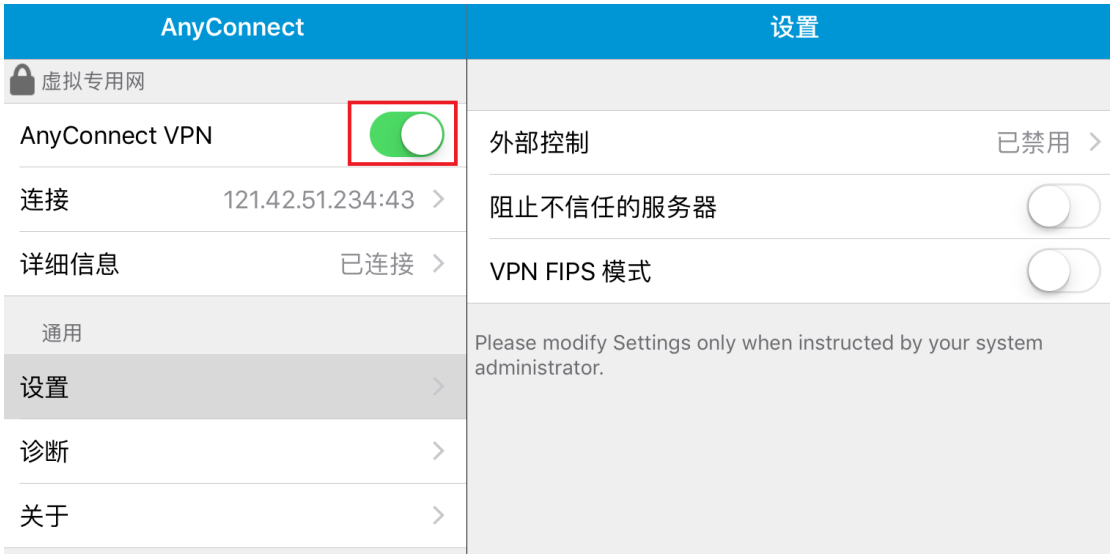


图 6-11-8

图 6-11 iOS 系统下 CISCO AnyConnect 客户端软件界面

iOS 系统下 CISCO AnyConnect 客户端软件具体设置过程描述如下：

1）点击左边的“连接”项，在右边窗口中点击“添加 VPN 连接”项；

2）在弹出的窗口中输入服务器 IP 及端口，中间以冒号:隔离，再点击右上角“保存”按钮；

3）返回主界面，点击“开关”按钮，在弹出的警告窗口中点击右下角的“更改设置”按钮，在主界面右边窗口中关闭“阻止不信任的服务器”选项；

4）主界面左边窗口中，再点击“开关”按钮，在弹出的警告窗口中点击“继

续”按钮，在之后的窗口中分别输入用户名和密码并点击右上角的“连接”按钮，就可以连接 VPN 了，连通后，点击“开关”按钮，退出 VPN 连接。

OCSERV VPN 客户端无法选择 VPN 路由，只能接受 VPN 服务器下发的路由。

6.4 下载安装自签名 CA 证书

如果不想在连接过程中出现证书警告窗口，则需要在连接 OCSERV VPN 前安装 VPN 服务器的 CA 证书（和 IKEV2 VPN 共一套 CA 证书，由 IKEV2 VPN 具体设置），具体安装验证流程参考“**2.2.1 Windows 系统的证书导入**”、“**2.2.2 安卓系统的证书导入**”和“**2.2.3 Windows 系统的证书导入**”。

CA 证书文件在线下载的 URL 类似“http://121.42.51.234/myca.crt”这样，Windows 下证书安装到“本地计算机”“受信任的根证书颁发机构”项目中。

注意：当管理员为服务器地址申请了真实域名证书后，可不必再下载安装自签名 CA 证书。

7 PPTP VPN 客户端设置

7.1 Windows 系统下设置 PPTP VPN

Windows 新建 PPTP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/pptp/windows_pptp.html

注意：

1）为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”；可以通过安装特定的软件实现 Windows 内置的 VPN 拨号随机启动自动拨号，无需人工交互输入，适用于无人值守或普通用户无感知的情形

2）Windows 内置的 PPTP VPN 连接成功后，浏览器的连接将忽视原有 IE 的代理设置，使用 Proxy SwitchyOmega 插件的 Chrome 浏览器不受影响，如果要设置

代理，需要单独给每个 VPN 连接设置代理。

3）新建的 PPTP VPN 连接缺省使用 VPN 隧道作为连接后的默认网关，如需取消，即只使用 VPN 服务器虚拟网络上的服务，请依次打开“控制面板\网络和 Internet\网络连接>[PPTP 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>在远程网络上使用默认网关”并取消。

4）为了防止不必要的 DNS 污染，依次打开“控制面板\网络和 Internet\网络连接>[PPTP 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>接口跃点数（Metric）”，将“自动跃点”改成“1”。

以下以 Windows XP 为例做说明，之后还有针对 Windows 10 的说明。

打开“网络连接”窗口，如图 7-1 所示。

图 7-1 “网络连接”窗口

选择“创建一个新的连接”项，出现新建连接向导窗口，如图 7-2 所示。

图 7-2 新建连接向导窗口

选择“下一步”，出现网络连接类型窗口，如图 7-3 所示。

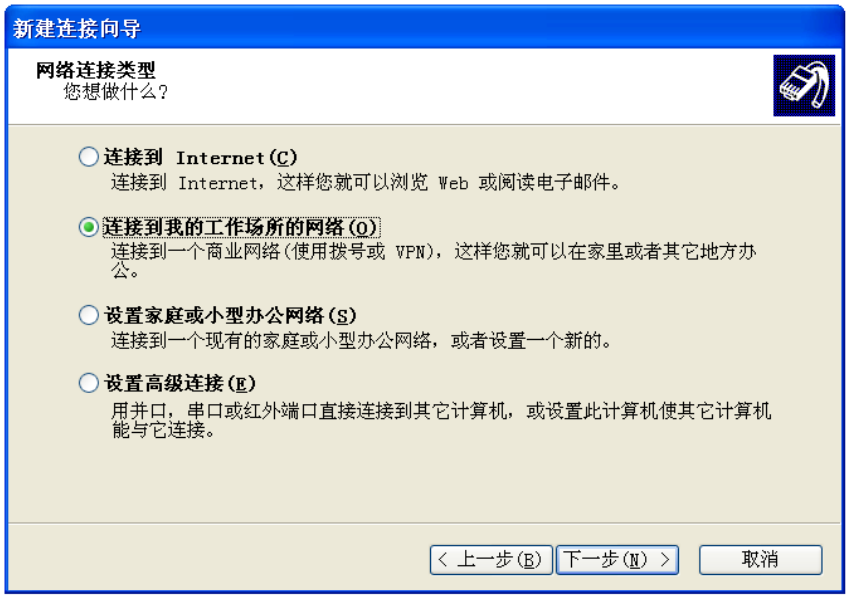


图 7-3 网络连接类型窗口

选择“连接到我的工作场所的网络”项，按“下一步”，出现网络连接窗口，如图 7-4 所示。

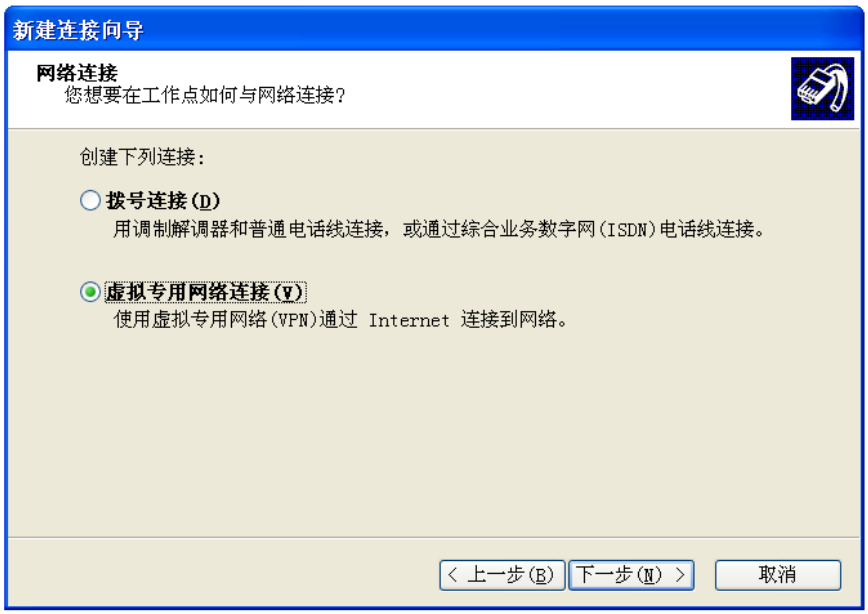


图 7-4 网络连接窗口

选择“虚拟专用网络连接”项，按“下一步”，出现连接名称窗口，如图 7-5 所示。

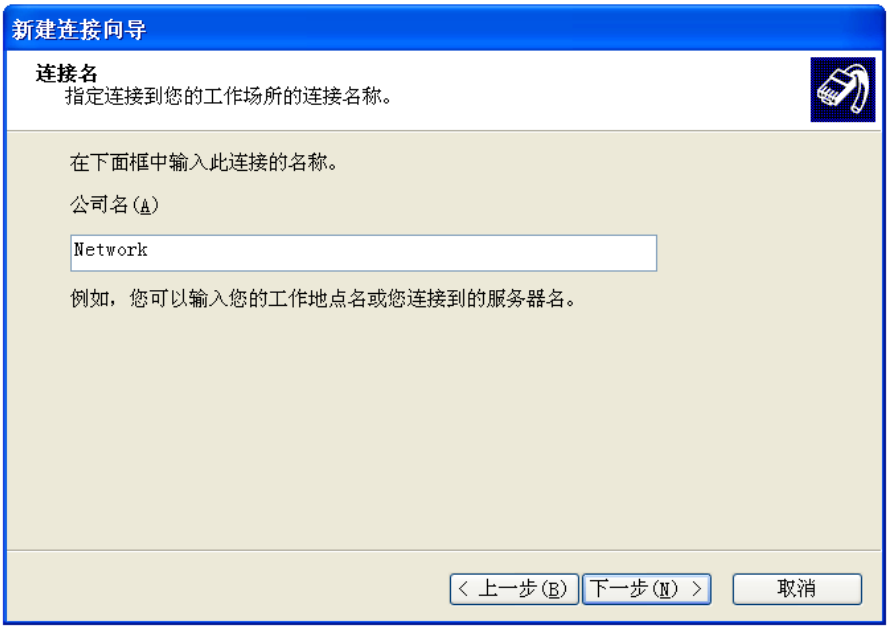


图 7-5 连接名称窗口

输入此连接的名称，例如：Network，按“下一步”，出现初始连接窗口，如图 7-6 所示。

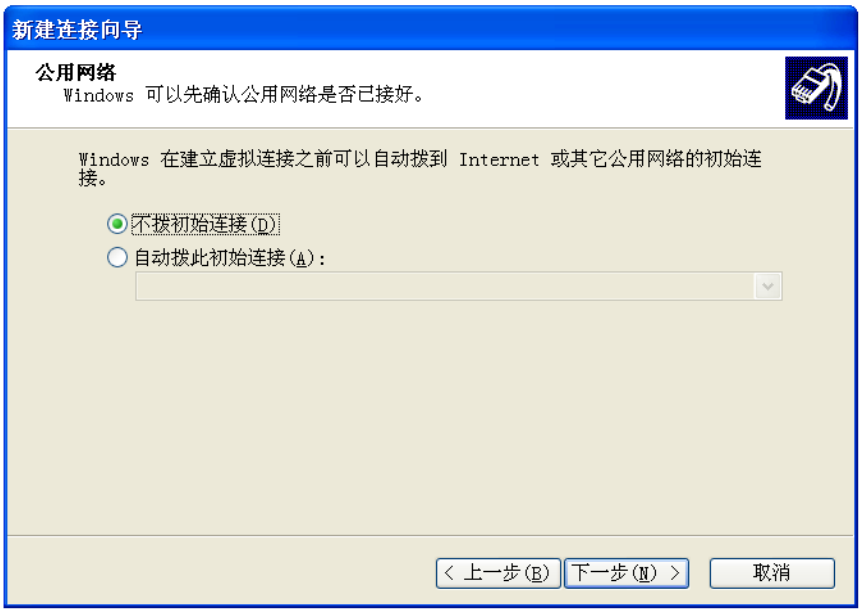


图 7-6 初始连接窗口

一般选择“不拨初始连接”项，按“下一步”，出现 VPN 服务器 IP 地址窗口，如图 7-7 所示。

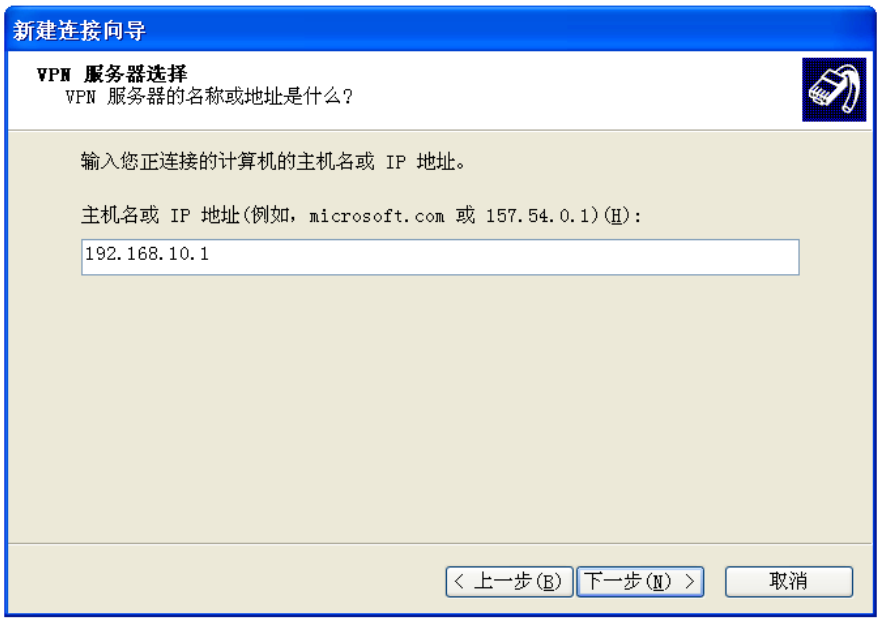


图 7-7 VPN 服务器 IP 地址窗口

输入管理员给出的 VPN 服务器 IP 地址，按“下一步”，出现完成窗口，如图 7-8 所示。

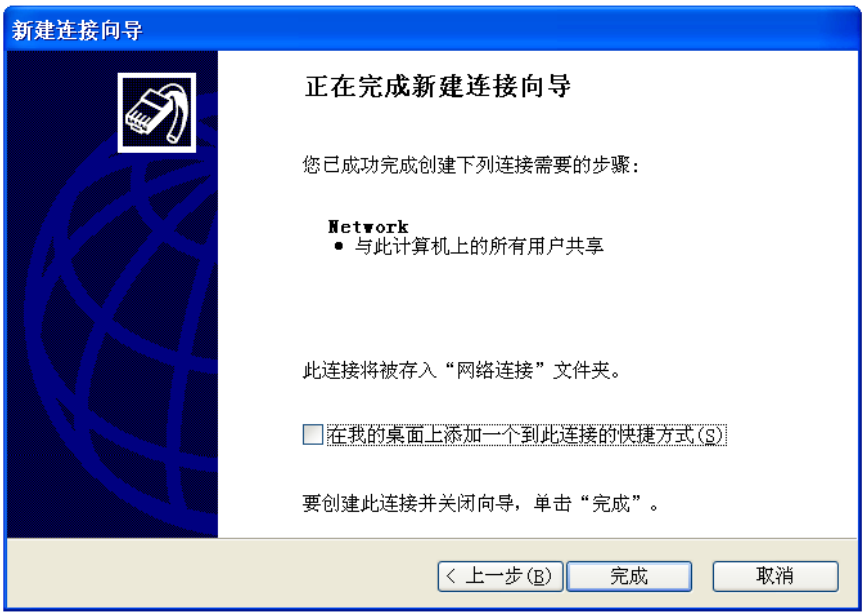


图 7-8 完成窗口

选择“完成”结束新建 PPTP VPN 连接设置。系统弹出连接对话框，如图 7-9 所示。

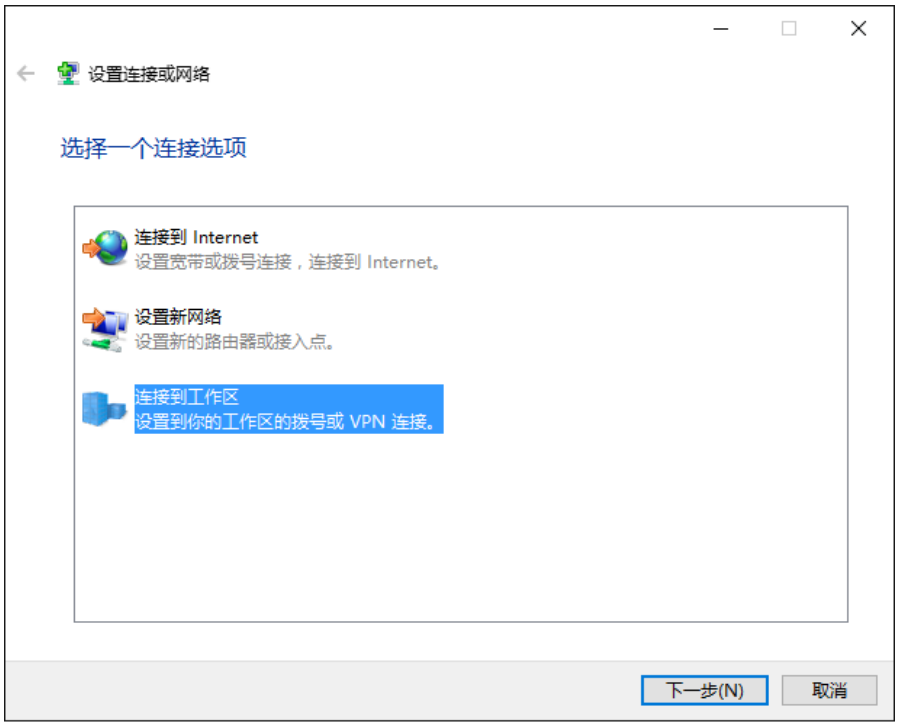
之后，在“网络连接”窗口中的“虚拟专用网络”列表中选择已建立的 PPTP VPN 连接，同样会出现此连接对话框。

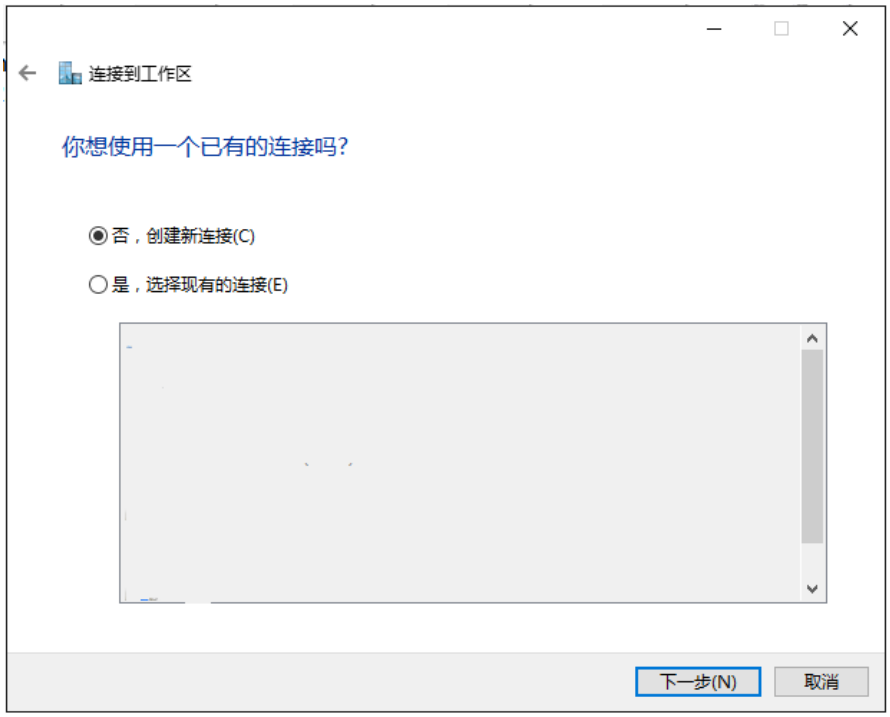
图 7-9 连接对话框

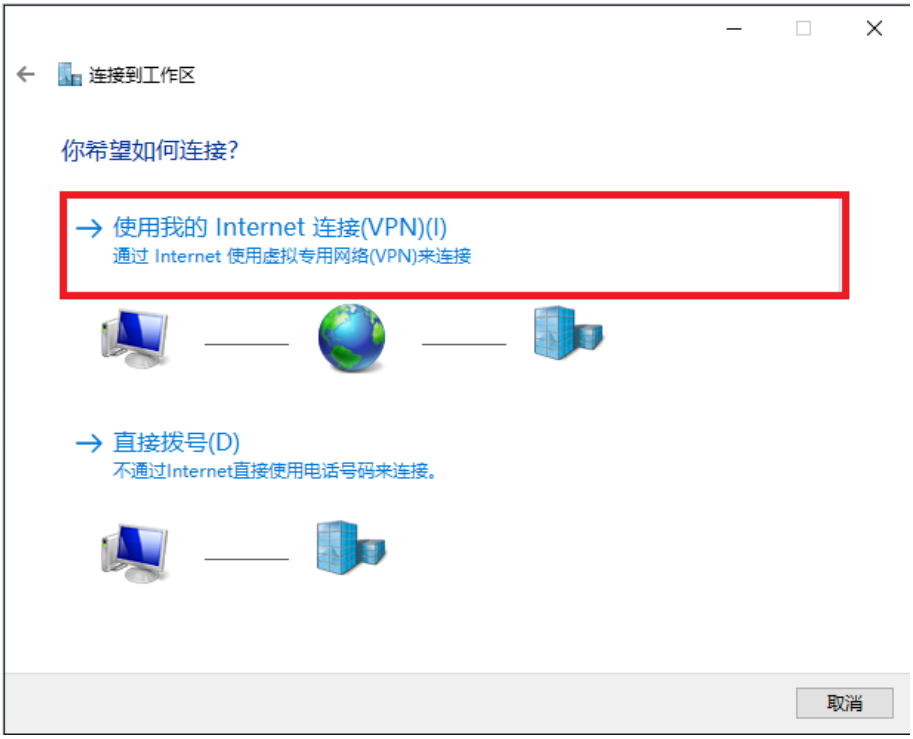
输入用户名和密码，按“连接”按钮登录 PPTP VPN 网络。

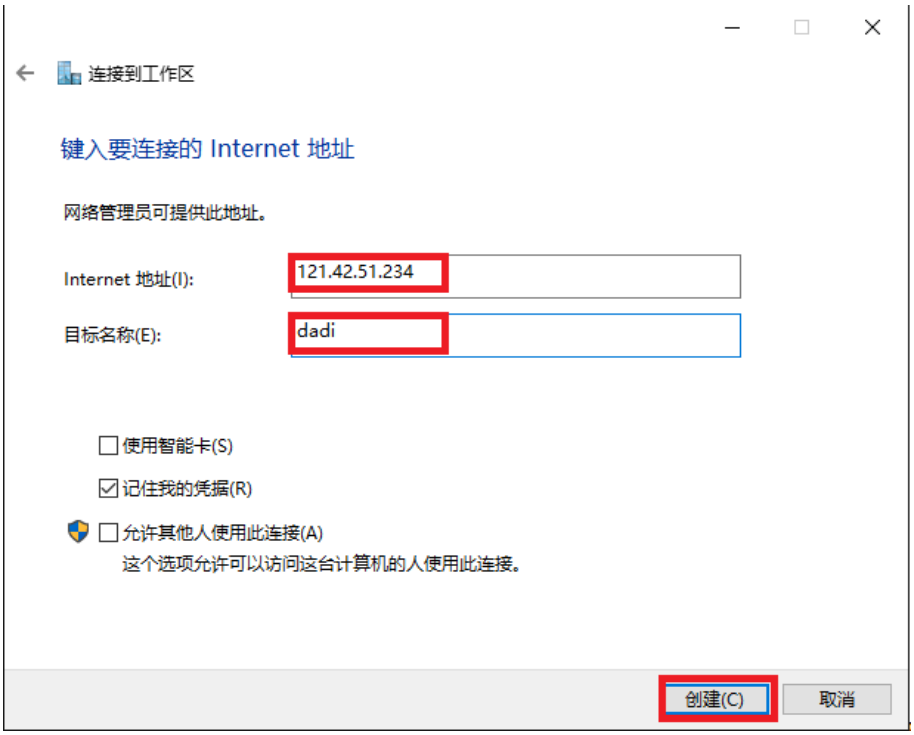
Windows 10 用户需要右键点击桌面右下角的“网络”图符，并选择“打开网

络和共享中心”，依次选择“设置新的连接或网络>连接到工作区>否，创建新连接>使用我的 Internet 连接”，输入“Internet 地址”、“目标名称”，并点击“创建”按钮；返回“网络和共享中心”界面，点击左边的“更改适配器设置”，在“网络连接”界面中，右键单击刚才创建的连接，并选择“属性”，切换到“安全”TAB，将“VPN 类型”改成“点对点隧道协议（PPTP）”，返回“网络连接”界面后，双击刚才创建的连接，进入到“网络和 INTERNET”界面，再选择刚才创建的连接，点击“连接”按钮，输入用户名和密码，具体如下组图 7-10 所示。

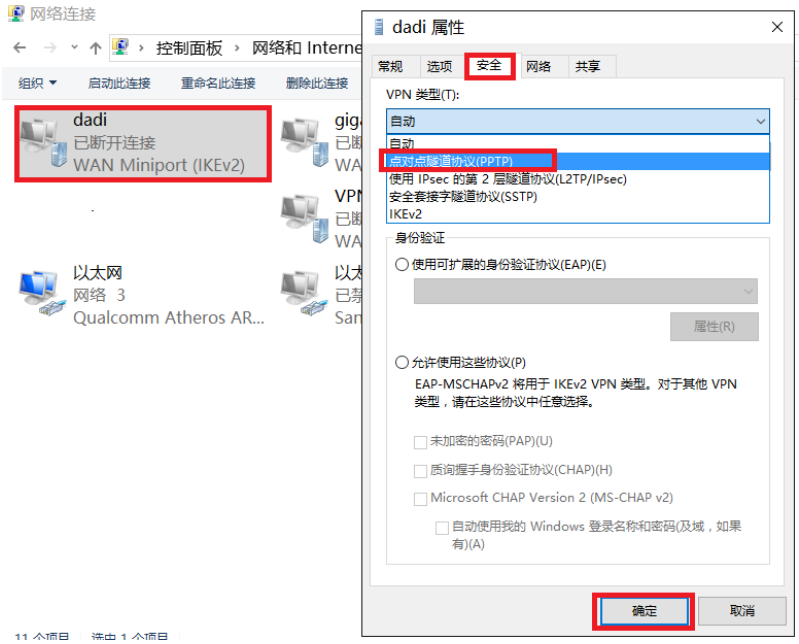

设置连接或网络
选择一个连接选项
连接到 Internet
设置宽带或拨号连接，连接到 Internet。
设置新网络
设置新的路由器或接入点。
连接到工作区
设置到你的工作区的拨号或 VPN 连接。
下一步(N)
取消


连接到工作区
你想使用一个已有的连接吗?
否，创建新连接(C)
是，选择现有的连接(E)
下一步(N)
取消


连接到工作区
你希望如何连接?
使用我的 Internet 连接(VPN)(I)
通过 Internet 使用虚拟专用网络(VPN)来连接
直接拨号(D)
不通过Internet直接使用电话号码来连接。
取消


连接到工作区
键入要连接的 Internet 地址
网络管理员可提供此地址。
Internet 地址(I):
121.42.51.234
目标名称(E):
dadi
使用智能卡(S)
记住我的凭据(R)
允许其他人使用此连接(A)
这个选项允许可以访问这台计算机的人使用此连接。
创建(C)
取消


网络和共享中心
控制面板 › 网络和 Internet › 网络和共享中心
搜索控制面板
控制面板主页
更改适配器设置
更改高级共享设置
查看基本网络信息并设置连接
查看活动网络
网络 3
公用网络
访问类型: Internet
连接: 以太网
更改网络设置
设置新的连接或网络
设置宽带、拨号或 VPN 连接；或设置路由器或接入点。
问题疑难解答
诊断并修复网络问题，或者获得疑难解答信息。
另请参阅
Internet 选项
Windows 防火墙
家庭组


网络连接
控制面板 › 网络和 Interne
组织
启动此连接
重命名此连接
删除此连接
dadi
已断开连接
WAN Miniport (IKEv2)
以太网
网络 3
Qualcomm Atheros AR...
dadi 属性
常规
选项
安全
网络
共享
VPN 类型(T):
自动
自动
点对点隧道协议(PPTP)
使用 IPsec 的第 2 层隧道协议(L2TP/IPsec)
安全套接字隧道协议(SSTP)
IKEv2
身份验证
使用可扩展的身份验证协议(EAP)(E)
属性(R)
允许使用这些协议(P)
EAP-MSCHAPv2 将用于 IKEv2 VPN 类型。对于其他 VPN 类型，请在这些协议中任意选择。
未加密的密码(PAP)(U)
质询握手身份验证协议(CHAP)(H)
Microsoft CHAP Version 2 (MS-CHAP v2)
自动使用我的 Windows 登录名称和密码(及域，如果有)(A)
确定
取消


添加 VPN 连接
VPN 提供商
Windows (内置)
连接名称
PPTP
服务器名称或地址
121.42.51.234
VPN 类型
点对点隧道协议(PPTP)
登录信息的类型
用户名和密码
用户名(可选)
p001
密码(可选)
记住我的登录信息
保存


设置
网络和 INTERNET
飞行模式
数据使用量
VPN
拨号
以太网
代理
VPN
添加 VPN 连接
dadi
连接
高级选项
删除

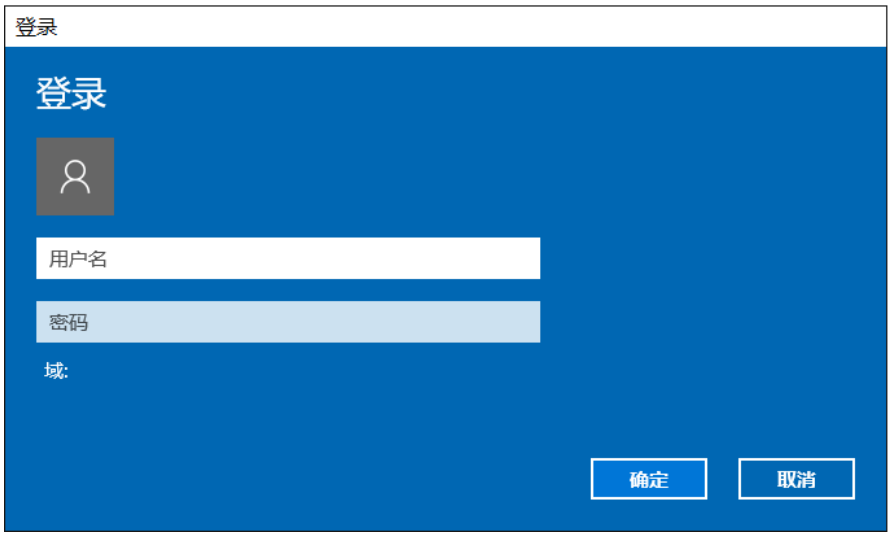
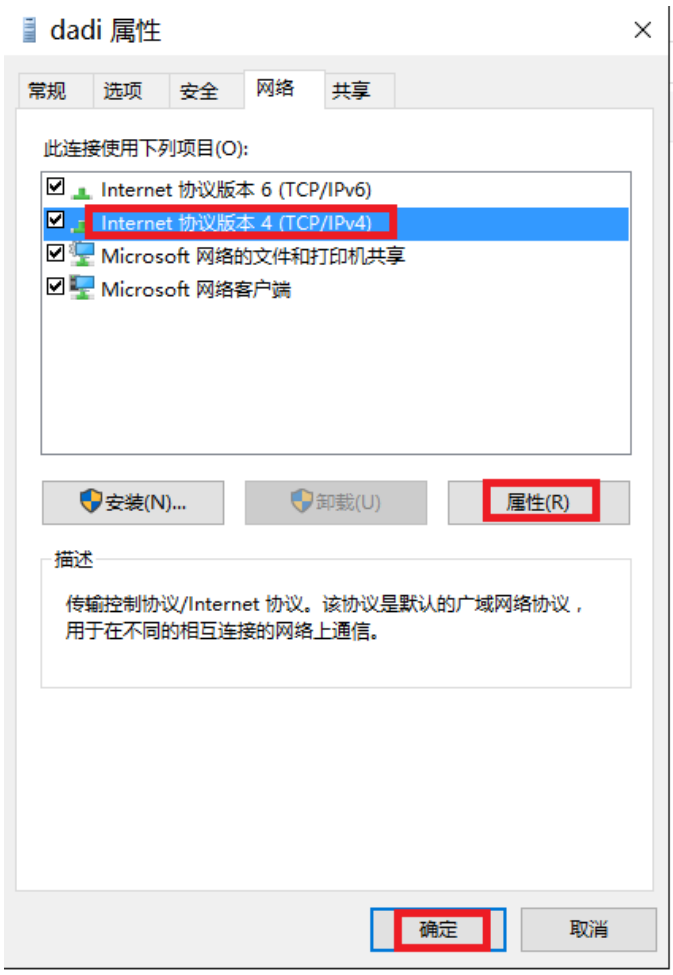


图 7-10 Windows10 系统下建立 PPTP 连接

成功登录后，可用 ipconfig /all、netstat -nr 等命令查看当前配置。

为了避免 DNS 泄露，可以将“接口跃点数”（Metric）由“自动跃点”改成“1”，如下组图 7-11 所示。

如果不想让 PPTP 连接成为缺省路由，可以切换到“网络”TAB，并修改“TCP/IPv4”的高级属性，将“在远程网络上使用默认网关”选项取消，如下组图 7-11 所示。


dadi 属性
常规
选项
安全
网络
共享
此连接使用下列项目(O):
Internet 协议版本 6 (TCP/IPv6)
Internet 协议版本 4 (TCP/IPv4)
Microsoft 网络的文件和打印机共享
Microsoft 网络客户端
安装(N)...
卸载(U)
属性(R)
描述
传输控制协议/Internet 协议。该协议是默认的广域网络协议，用于在不同的相互连接的网络上通信。
确定
取消


Internet 协议版本 4 (TCP/IPv4) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I):
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P):
备用 DNS 服务器(A):
高级(V)...
确定
取消

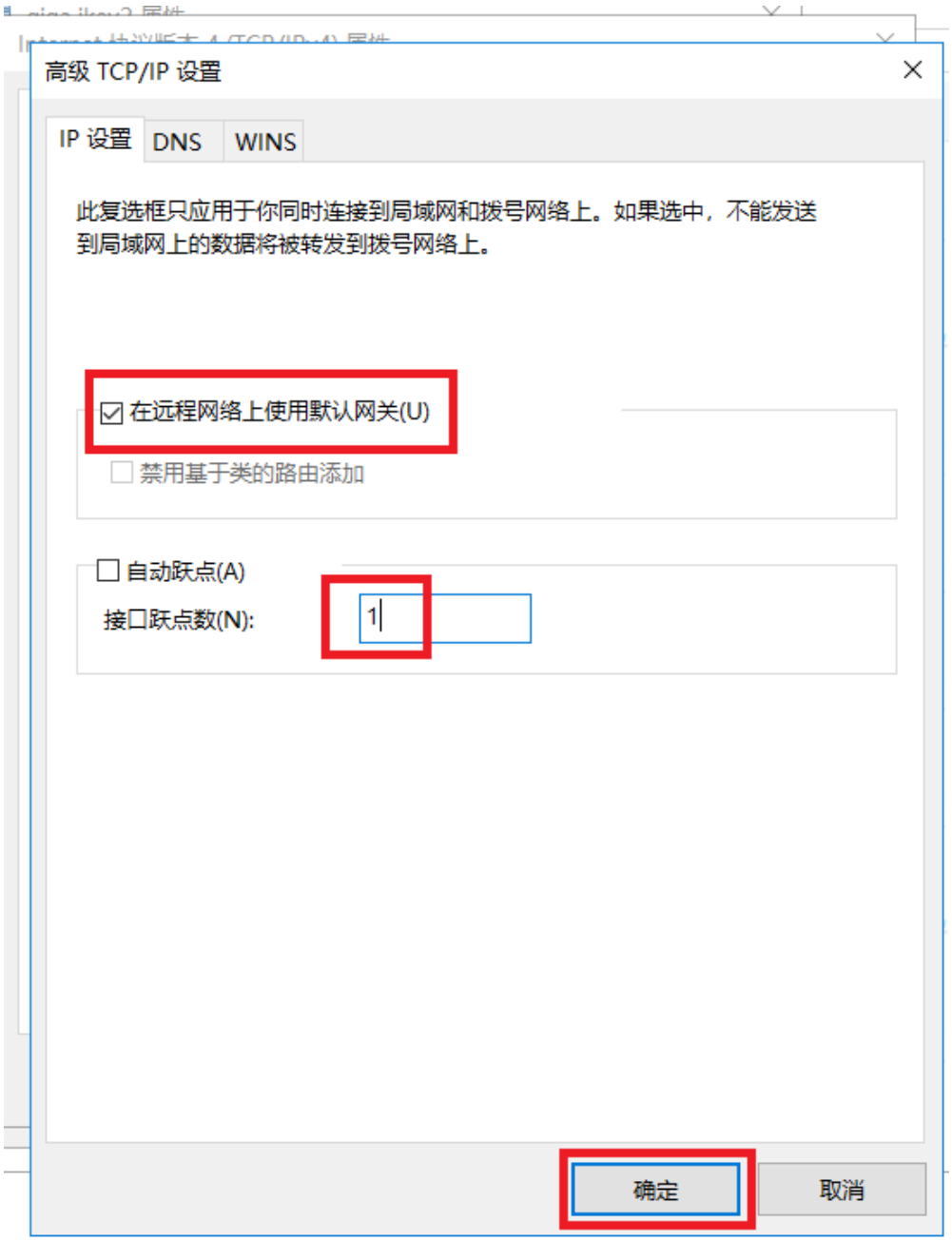
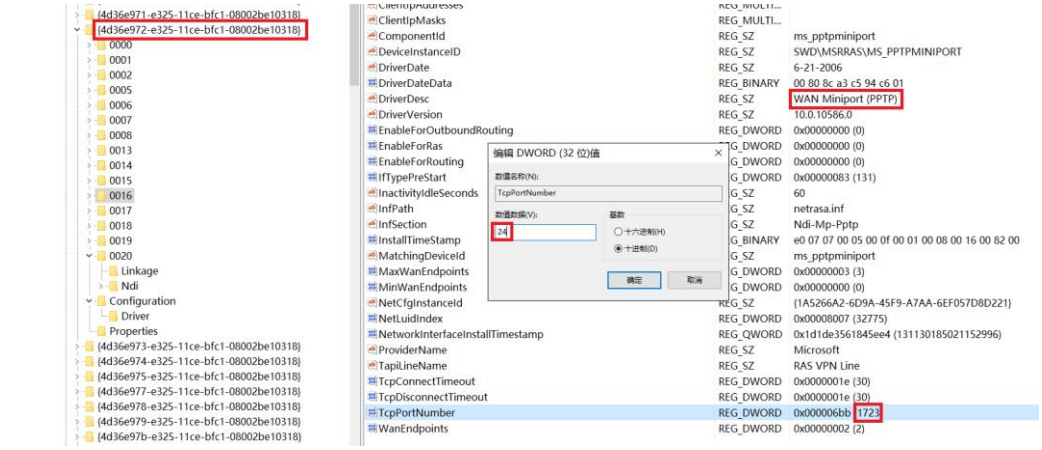


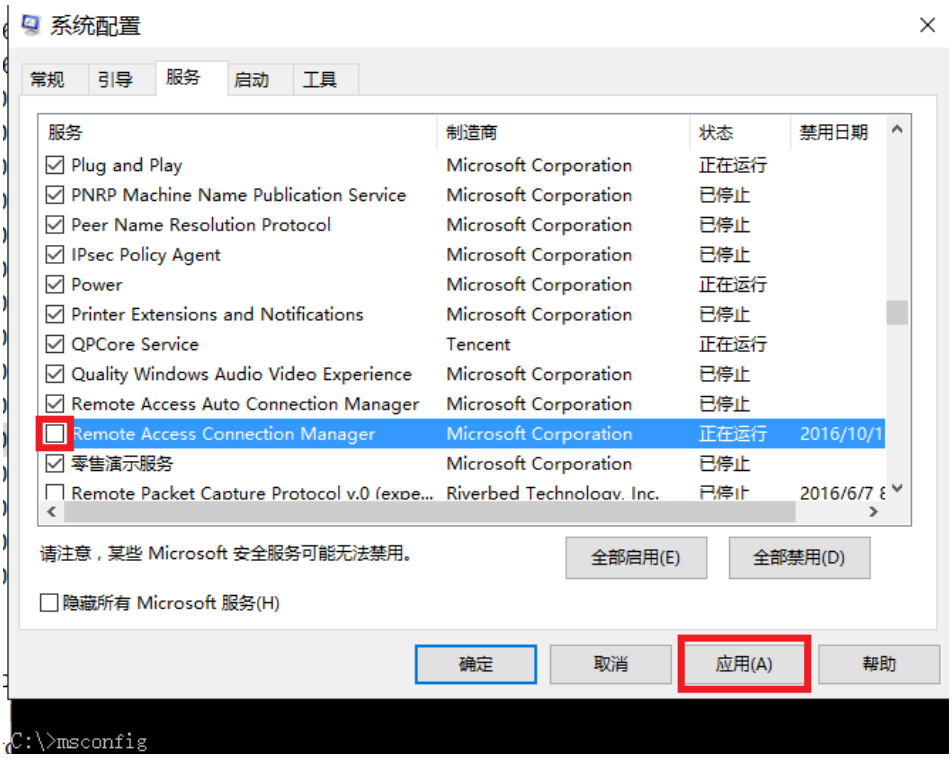
图 7-11 取消 PPTP 连接作为缺省路由

如果要修改 PPTP 的连接端口，可以运行“regedit”修改注册表，找到“DriverDesc”项内容是“WAN Minport (PPTP)”的分支，例如：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}]，将右边的“TcpPortNumber”项的十进制数值改成所需的端口值，例如：24，重启生效。

如果不想重启，可以运行程序“process hacker”，找到“svchost.exe”

进程，再找到“services”包含“RasMan”的，再按右键选择“Terminate”结束该进程。还可以运行 msconfig 命令，切换到“服务”TAB，将“Remote Access Connect Manager”服务取消，并应用，再打开系统服务窗口，停止再启动“Remote Access Connect Manager”服务，同样可以不重启 Windows，让 PPTP 端口改动生效，还要选择/恢复其“启动类型”为“自动”，重新发起 PPTP 连接进行验证，如下组图 7-12 所示。





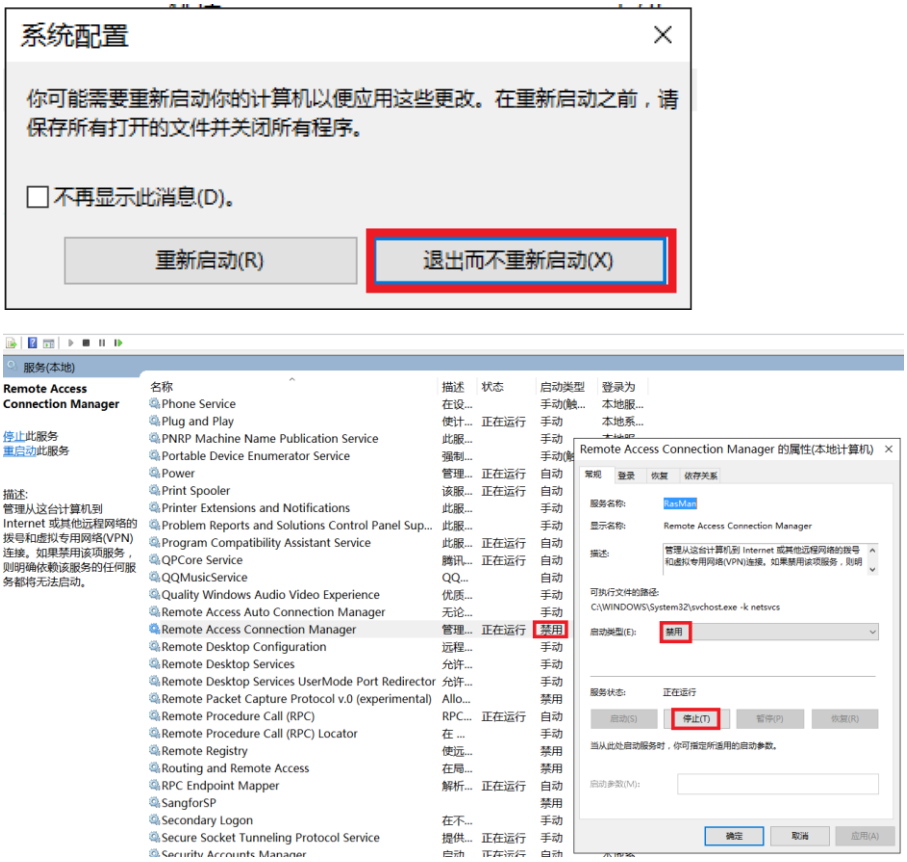


图 7-12 修改 PPTP 连接端口

修改客户端配置后，还要排除 NAT 的干扰，或者让沿途 NAT 设备开启对 24/TCP 端口的 PPTP NAT ALG 支持。

VPN 连接后，为了能让 VPN 虚拟网络（10.6.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“10.6.0.0/24”，参考图 5-5-6 所示。

7.2 安卓系统下设置 PPTP VPN

安卓系统 PPTP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/pptp/android_pptp.htm1

安卓系统下 PPTP VPN 具体设置过程描述如下：

1）点击桌面的“设置”图符，再点击“更多”菜单项，再点击“VPN”菜单项；

2）再点击左下角的“添加 VPN 网络”菜单项，输入名称、服务器地址栏的内容，选择类型“PPTP”，再点击“保存”按钮；

3）如果不想让 PPTP 连接成为缺省路由，就打开“显示高级选项”开关，在“转发路线”栏中填写“10.6.0.0/24”，相当于只是修改 DNS 服务器，其它流量还是走原来的 WIFI 或移动数据流量网络；

4）返回 VPN 界面后，点击刚才新建的 VPN，在对话框中输入用户名和密码。

具体设置过程详见下组图 7-13 所示。

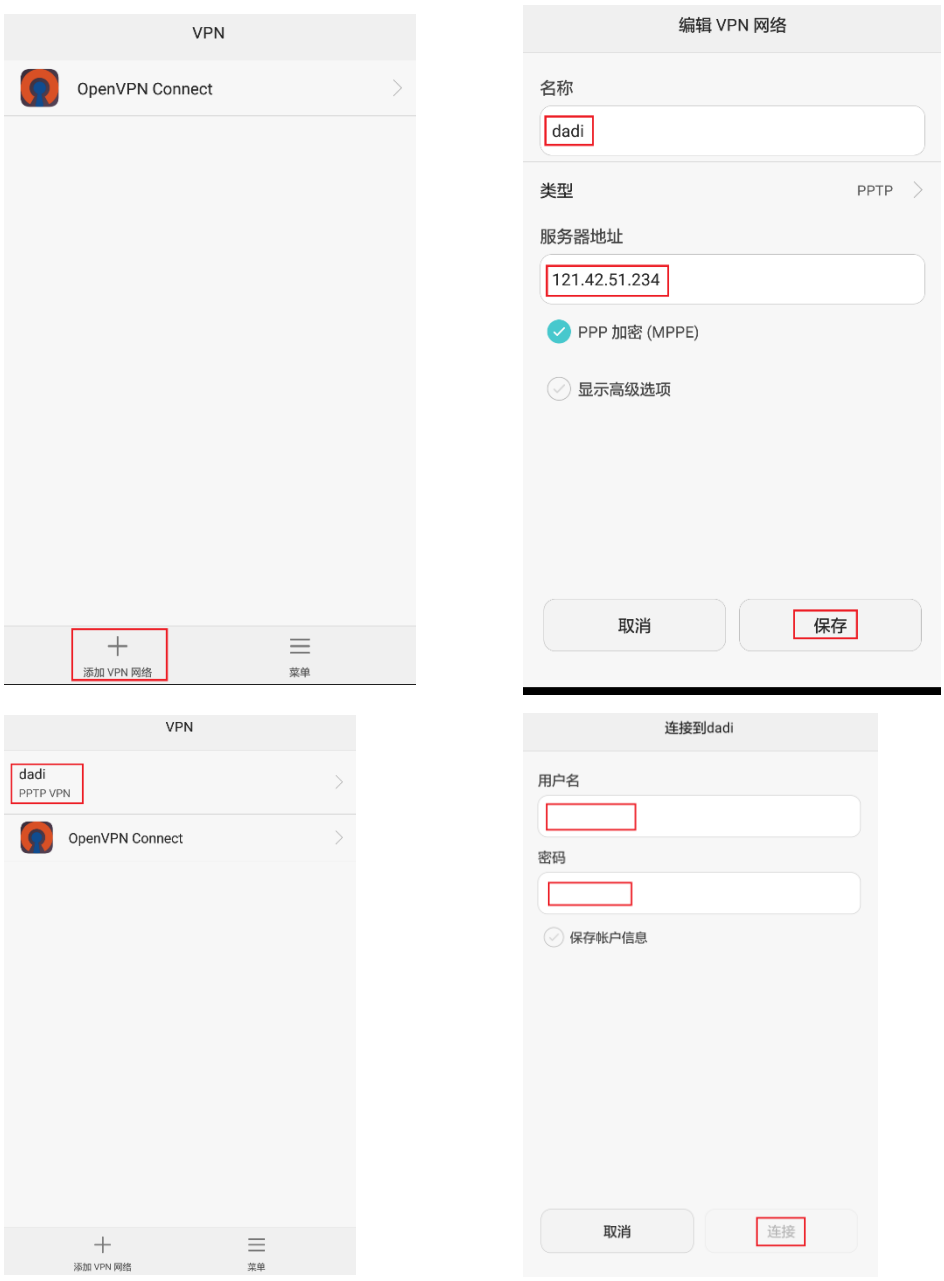


图 7-13 安卓系统下建立 PPTP 连接

为了在重新打开系统时 VPN 不中断，需要在“电池”设置中，启用“休眠时始终保持网络连接”选项。

7.3 iOS 系统下设置 PPTP VPN

iOS 系统 PPTP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/pptp/ios_pptp.html

注意：iOS 在 10.0 版本以后就没有 PPTP VPN 拨号连接了，只有 IKEV2 VPN、IPSEC VPN 和 L2TP VPN 拨号连接。

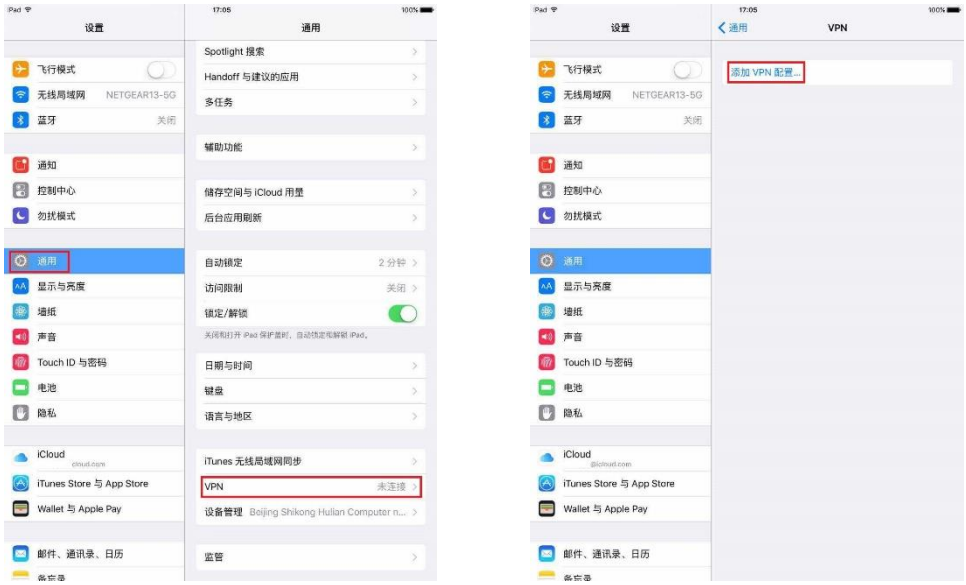
iOS 系统下设置 PPTP VPN 过程描述如下：

1）点击桌面的“设置”图符，再点击“通用”菜单项，再点击右边下方的“VPN”菜单项，如果已经有了 VPN 设置，则在左上方就有 VPN 菜单项；

2）再点击右边下方的“添加 VPN 配置…”菜单项，选择类型为“PPTP”，输入描述、服务器、账户、密码栏的内容，如果不想让 PPTP 连接成为缺省路由，就关闭“发送所有流量”选项，相当于只是修改 DNS 服务器，其它流量还是走原来的 WIFI 或移动数据流量网络，再点击右上角的“完成”按钮；

3）返回 VPN 界面后，勾选 VPN 连接，再点击“状态”栏“未连接”开关。

具体设置过程详见下组图 7-14 所示。



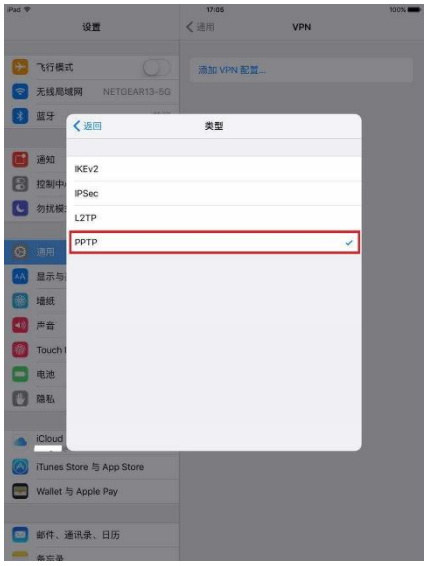


图 7-14 iOS 系统下新建 PPTP 连接

8 OpenVPN 客户端设置

8.1 Windows 系统下设置 OpenVPN 客户端

Windows 安装使用 OpenVPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/openvpn/windows_openvpn.html

注意：

1）为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”

2）OpenVPN 连接成功后，如果原来设置了系统代理，则浏览器仍然通过原来的代理进行连接。

3）如果 OpenVPN 客户端拨号成功，使用中突然不可用，可能是受到同一账号不能同时登陆的限制，需要再次登陆，最好能停止异地登陆，或修改密码再登陆。

OpenVPN Windows 客户端软件下载链接

官方：https://openvpn.net/community-downloads/ (选择 32 位或 64 位之一)

汉化：http://www.trustcomputing.com.cn/tools/dadivpn-2.0-client-install-x86_64.exe (全兼容)

1）安装软件

下载并安装 VPN 客户端软件，双击桌面的 VPN 程序图符，运行 VPN 客户端软件，此时会在 Windows 桌面的右下角任务栏中出现 VPN 程序图标，如图 8-1 所示。

图 8-1 任务栏中的 OpenVPN 程序图标

如果没有显示，则需要设置任务栏属性，右键单击右下角的时间和日期，选择最下面的“属性”项，在弹出来的窗口中点击“选择在任务栏上显示哪些图标”项，再将“xxxxVPN GUI for Windows”项设置为“开”，这样就可以在任务栏里长久显示图标，如图 8-2 所示。

图 8-2 选择在任务栏上显示的程序图符

2）修改 OpenVPN 网卡的跃点数/Metric 值

如果有多个 openvpn 网卡，则需要重命名 openvpn 网卡，例如：myopenvpn，再在客户端配置文件中加入"dev-node myopenvpn"。

如果日志中出现"CreateFile failed on TAP device", "All TAP-Windows adapters on this system are currently in use"的错误信息，则要删除所有的 TAP 网卡，再重装 VPN 客户端软件。

找到 OpenVPN 网卡，依次点击“Internet 协议版本 4（TCP/IPv4）>高级>接口跃点数”，缺省是“自动跃点”，修改为“1”，如图 8-3 所示。这样可以让用户在 OpenVPN 拨号连接后使用 OpenVPN 服务器分配的 DNS 服务器，避免可能出现的 DNS 泄露。

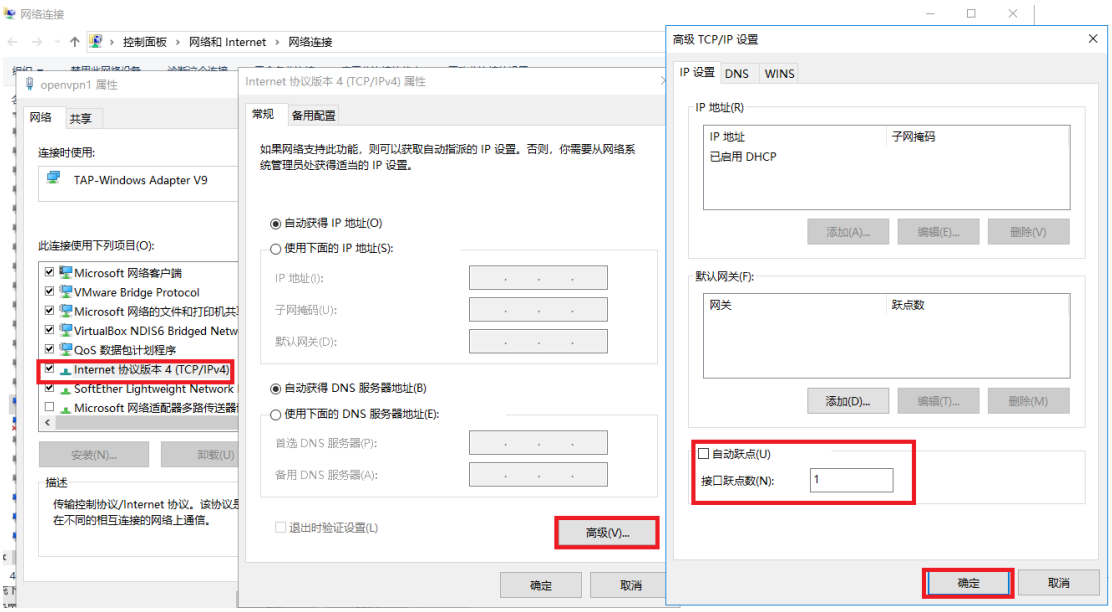


图 8-3 OpenVPN 网卡跃点数

3）修改配置文件

打开 VPN 客户端软件配置文件所在的目录，通常是“C:\Program Files\xxxxVPN\config”目录，编辑 ovpn 文件，设置好服务器 IP 及端口，协议，用户认证，代理服务器等参数，如有必要还可以将用户名和口令写到一个文件（由 auth-user-pass 参数指定）里，如图 8-4 所示。

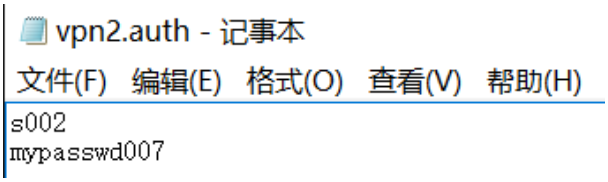


图 8-4 OpenVPN 客户端配置文件

4）连接服务器

右键点击任务栏上的 VPN 程序图标，在弹出的主菜单中选择“连接”项，就可以连接 VPN 服务器了，如图 8-5 所示。

图 8-5 连接 OpenVPN 服务器

OpenVPN 客户端软件允许同时连接多个服务器，只要各 VPN 虚拟 IP 地址池不一样就行。

5）修改防火墙规则

VPN 连接后，在 VPN 服务器允许的前提下，为了能让 VPN 虚拟网络（10.8.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“10.8.0.0/24”。参考图 5-5-6 所示。

注意，能连接的是监听在 OpenVPN 虚拟 IP 上的端口，而不是 0.0.0.0 上的端口，例如：10.8.0.6:139 这样的端口，可以用 CMD 命令 “netstat -nao | findstr 10.8.0.6”查看。

8.2 Android 系统下设置 OpenVPN 客户端

安卓系统安装使用 OpenVPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/openvpn/android_openvpn.html

OpenVPN 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=net.openvpn.openvpn

http://www.trustcomputing.com.cn/tools/ net.openvpn.openvpn_1.1.17.apk

1）安装软件

下载 OpenVPN Connect 客户端软件，安装后，点击桌面的 OpenVPN 程序图符，如图 8-6 所示，运行 OpenVPN Connect 客户端软件，如图 8-7 所示。

图 8-6 桌面上的 OpenVPN Connect 安卓客户端软件

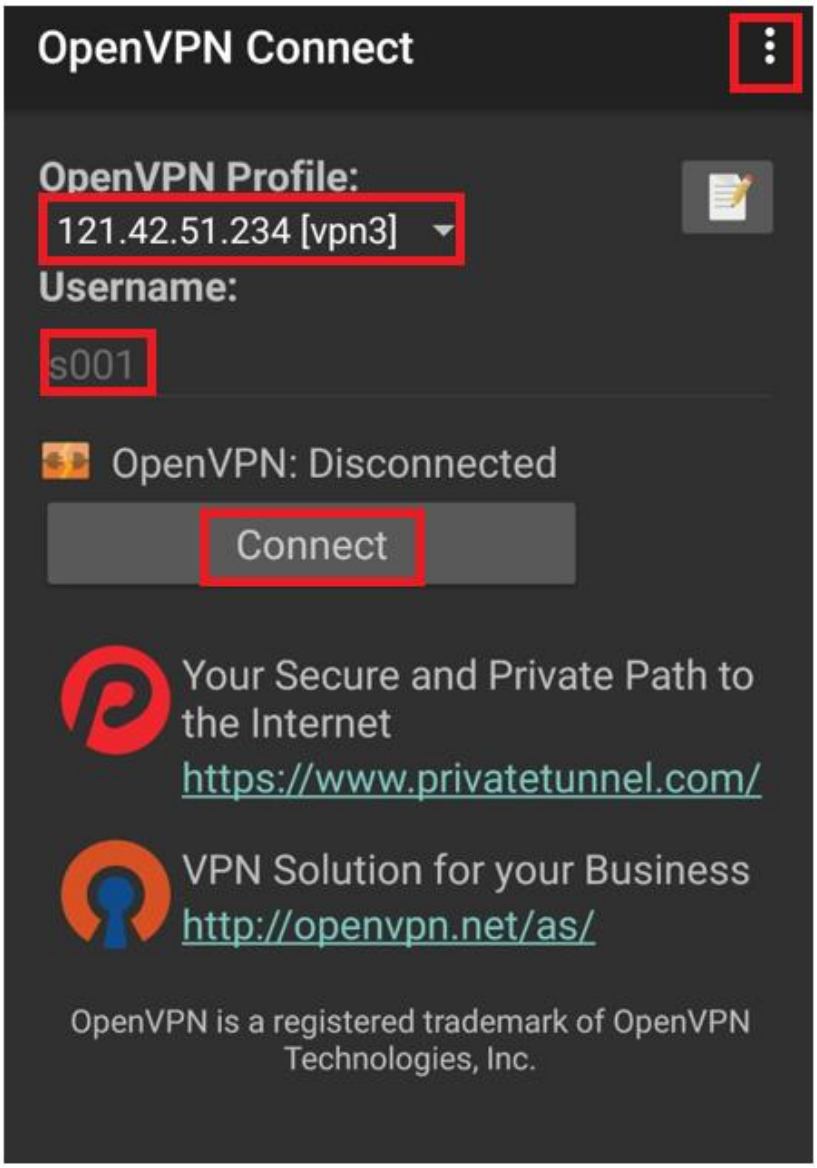


图 8-7 OpenVPN Connect 安卓客户端软件界面

2）上传配置文件

在 Windows 下打开浏览器，输入网址 https://wx.qq.com，出现一个二维码；用手机登录微信，再扫描这个二维码，进入 WEB 界面，再点击左边的“文件传输助手”项，再点击右下方的文件夹图符，在打开的文件框里选择事先修改好的 ovpn 等配置文件，上传至手机，如图 8-8 所示。

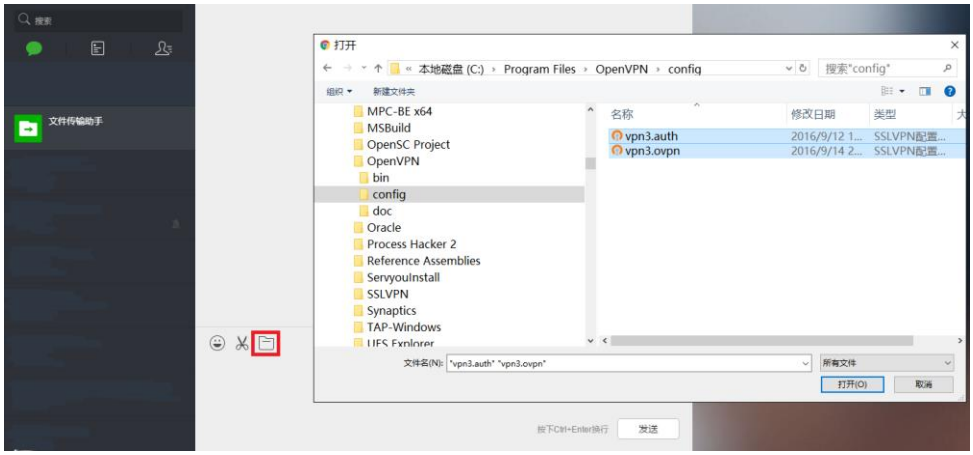


图 8-8 上传配置文件

再打开手机微信的“文件传输助手”，分别点击、打开刚才上传的文件，点击右上角图符，选择保存，即可将配置文件上传到手机。

3）打开配置文件

在手机的 OpenVPN Connect 客户端软件中，点击右上角的选项按钮，在弹出的菜单中选择“Import”项，继续选择“Import Profile from SD card”项，如图 8-9 所示。

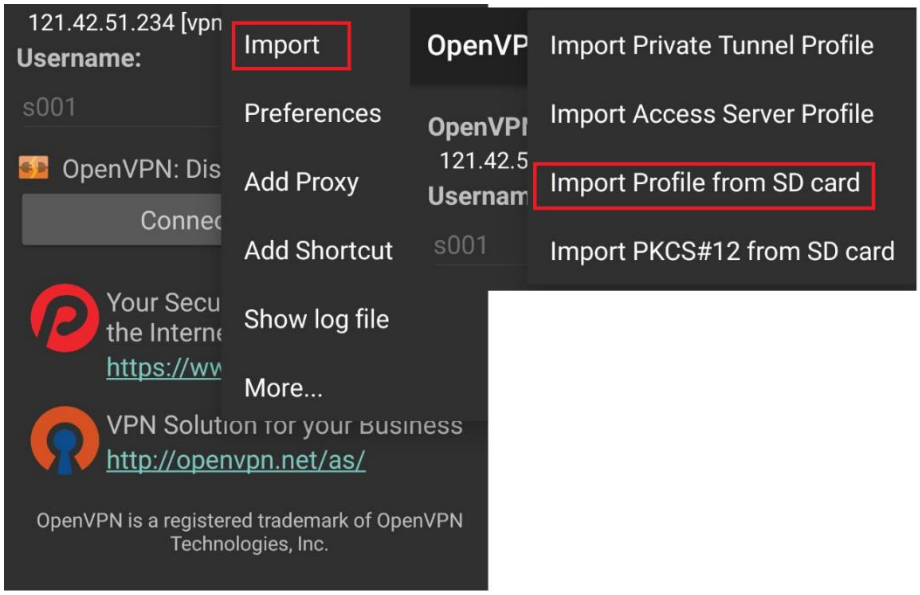


图 8-9 选择配置文件

在文件系统中，选择“/sdcard/Download/WeiXin”目录，并选择上传的 ovpn 文件，如图 8-10 所示。

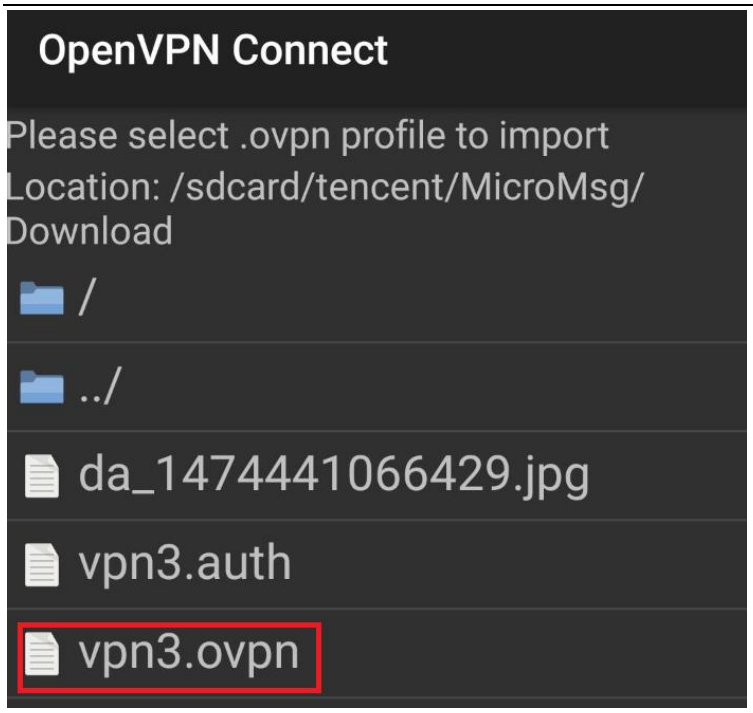


图 8-10 确定配置文件

4）连接服务器

返回 OpenVPN Connect 客户端软件主界面，点击“Connect”按钮，如果一切正常，就可以连接成功了，如图 8-11 所示。

图 8-11 OpenVPN Connect 客户端软件连接成功

为了在重新打开系统时 VPN 不中断，需要为了在重新打开系统时 VPN 不中断，需要：

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

安卓系统下 2.6+版本以上的 OpenVPN APP，需要特别设置才能和 2.3 版本的

服务器连接，主要是客户端配置文件中加入：

```
cipher BF-CBC
data-ciphers BF-CBC
data-ciphers-fallback BF-CBC
```

同时，OpenVPN APP 需要做兼容性设置：

1）配置文件选择兼容 2.3 版本（最后一项）（OpenSSL Legacy）

2）TLS 选择最低安全要求（第一项）

或者使用老版 OpenVPN APP，或者 OpenVPN Connect APP

8.3 iOS 系统下设置 OpenVPN 客户端

iOS 系统安装及使用 OpenVPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/openvpn/ios_openvpn.html

iOS 系统上传 OpenVPN 配置文件示例

http://www.trustcomputing.com.cn/help/cn/dadi/openvpn/ios_itunes.html

OpenVPN iOS 客户端软件下载链接（美区）

https://itunes.apple.com/us/app/openvpn-connect/id590379981

需要用美国的 Apple ID 登陆 iTunes Store 与 App Store，再下载 OpenVPN Connect 客户端 App。具体过程为：

1）在 iOS 设备上，点击“设置”界面中的“iTunes Store 与 App Store”项，再点击右边“Apple ID”输入框，如果已有账号则注销，再输入美国区的账号及密码，如图 8-12 所示，安装后，可以再切换回中国区账号；

2）在“App Store” 界面中查找“openvpn”，选择“OpenVPN Connect”App 下载并安装，如图 8-13 所示；

3）打开“OpenVPN Connect”App，当没有任何配置文件时，如图 8-14 所示；

4）用数据线连接 iOS 设备和 PC/MAC，再打开 PC/MAC 端的 iTunes 软件，点击上方的设备图标，点击左边的“设置-应用”项，在中间框中找到并点击“OpenVPN”项，在右边框中点击“添加文件…”按钮，在弹出的对话框中找到并选择 vpn.ovpn 以及 vpn.auth 两个文件，再点击“同步”按钮，如图 8-15 所示；

5）再在 iOS 设备上，打开“OpenVPN Connect”App，当有配置文件时，点击其右边的“+”号按钮，如图 8-16 所示；

6）当没有连接时，点击“Connection”图标进行连接，如图 8-17 所示；

7）当连接成功后，点击“Connection”图标断开连接，如图 8-18 所示；

同样也可以在“设置”界面中点击“VPN”项，再点击右边“OpenVPN”项进行连接和断开操作，如图 8-19 所示。

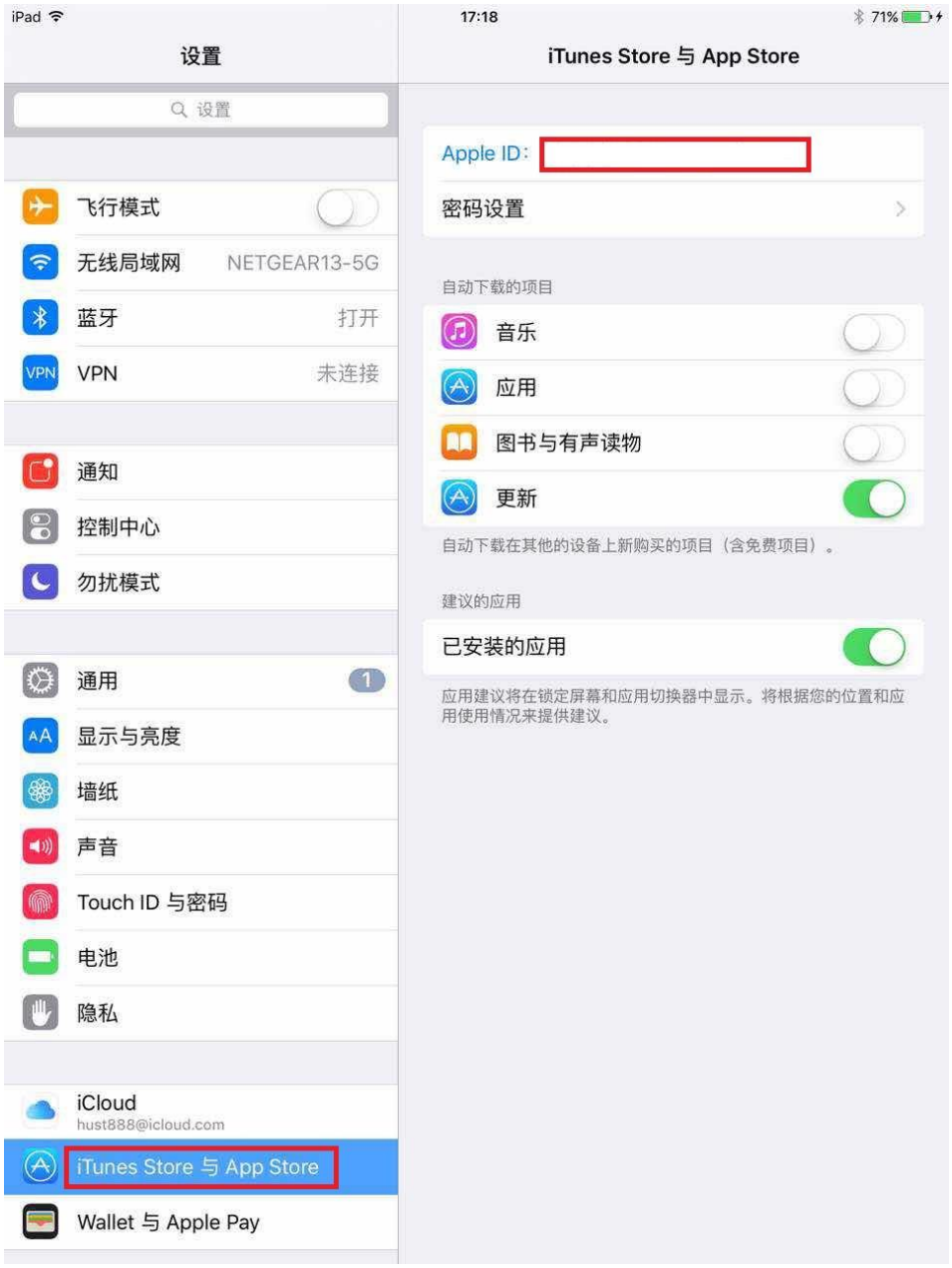


图 8-12 设置-切换 Apple ID

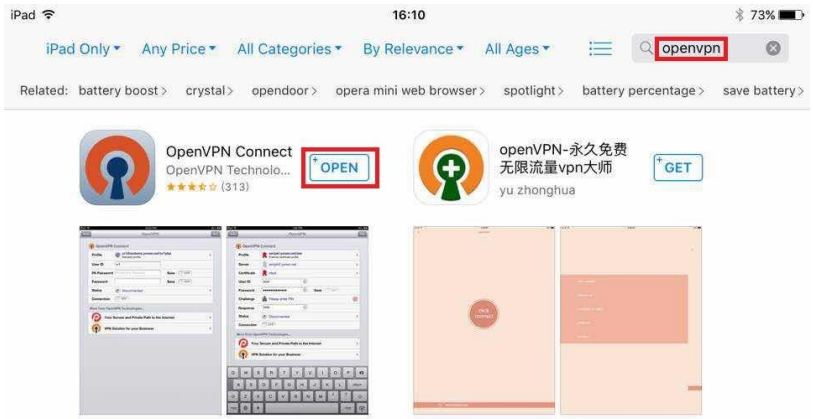


图 8-13 App Store 里查找并安装 OpenVPN Connect 客户端 App

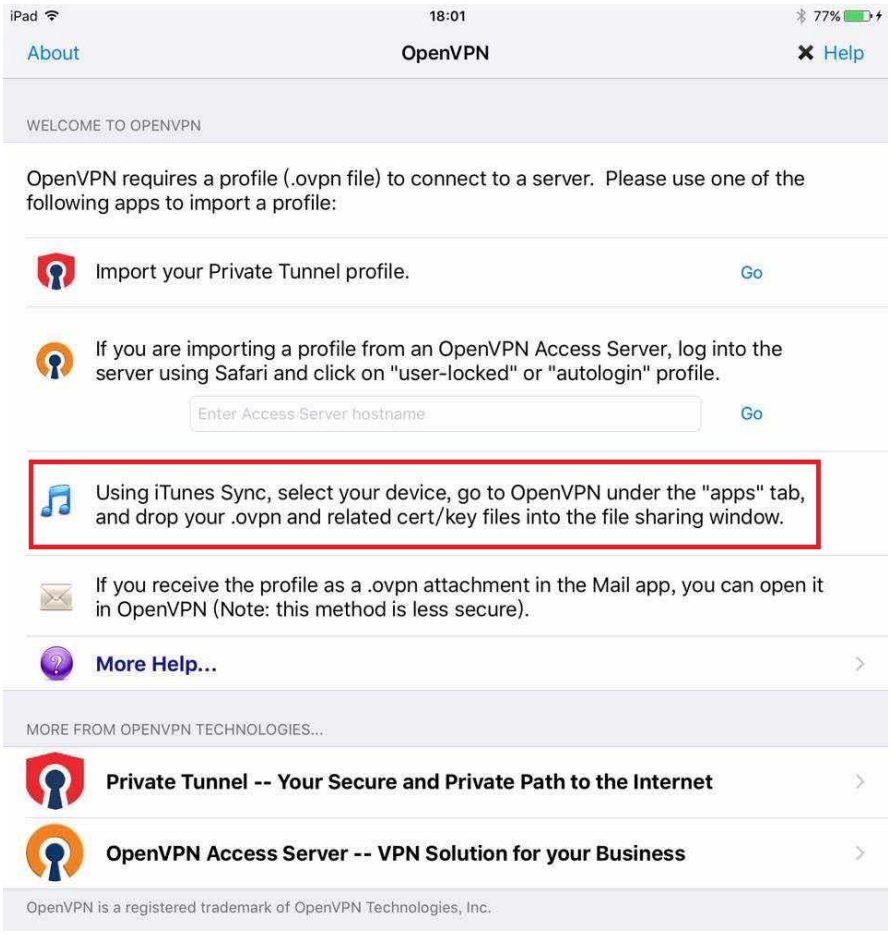


图 8-14 OpenVPN Connect 客户端 App 界面（无配置文件）

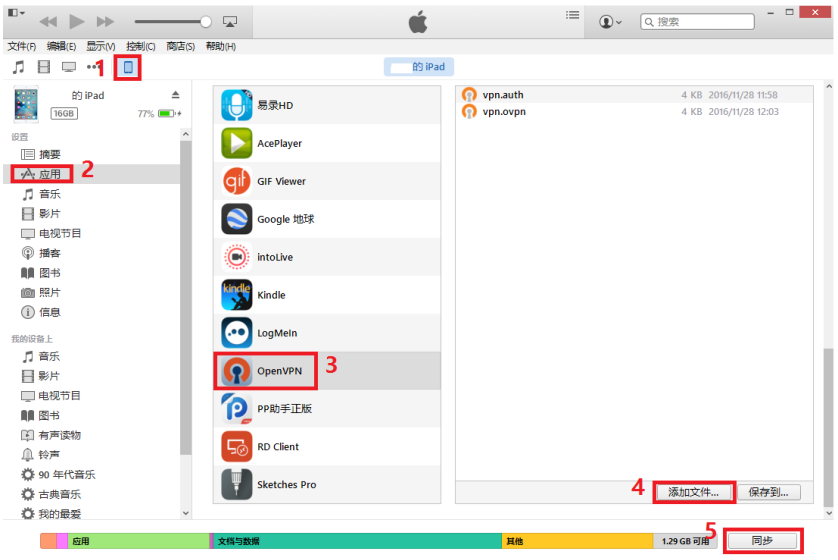


图 8-15 通过 PC/MAC 端的 iTunes 软件同步/上传 OpenVPN 配置文件

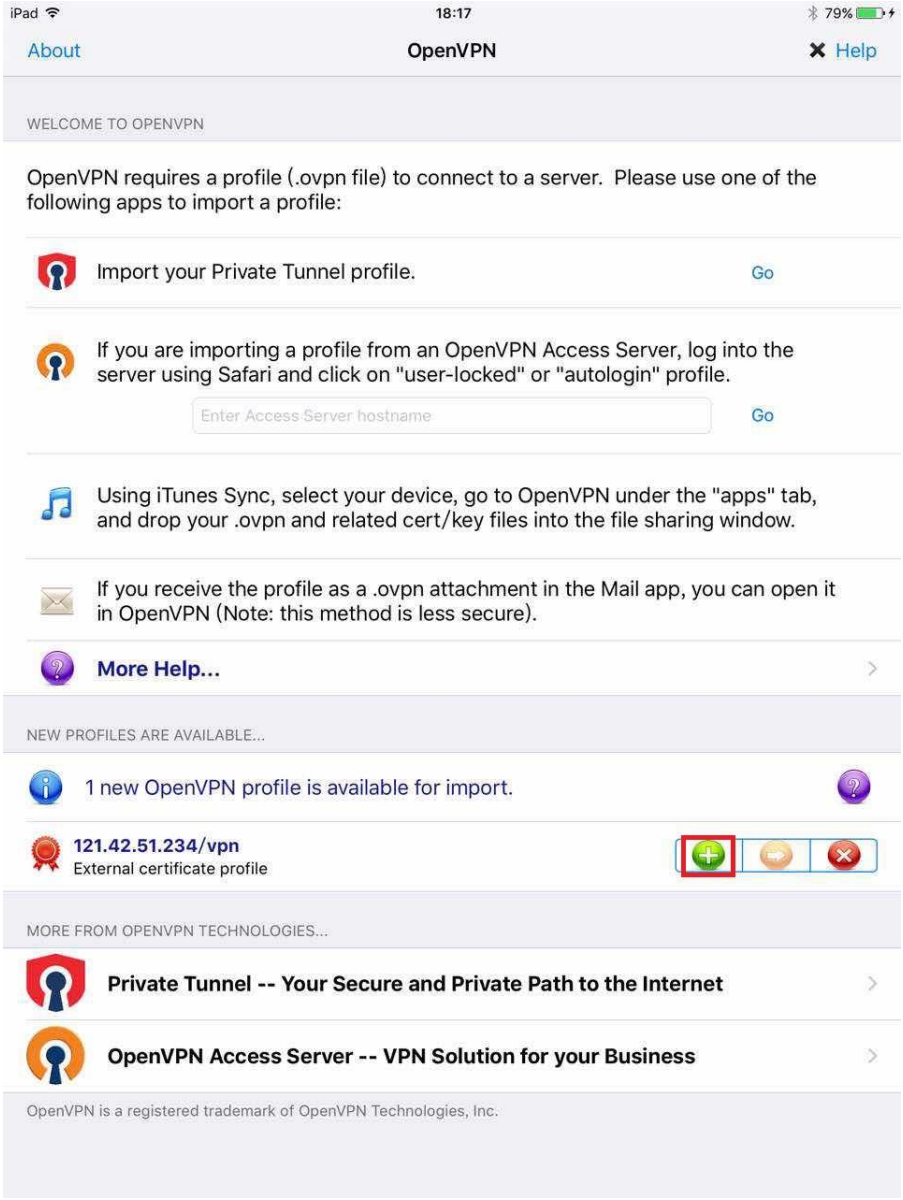


图 8-16 OpenVPN Connect 客户端 App 界面（有配置文件）

图 8-17 OpenVPN Connect 客户端 App 界面（未连接）

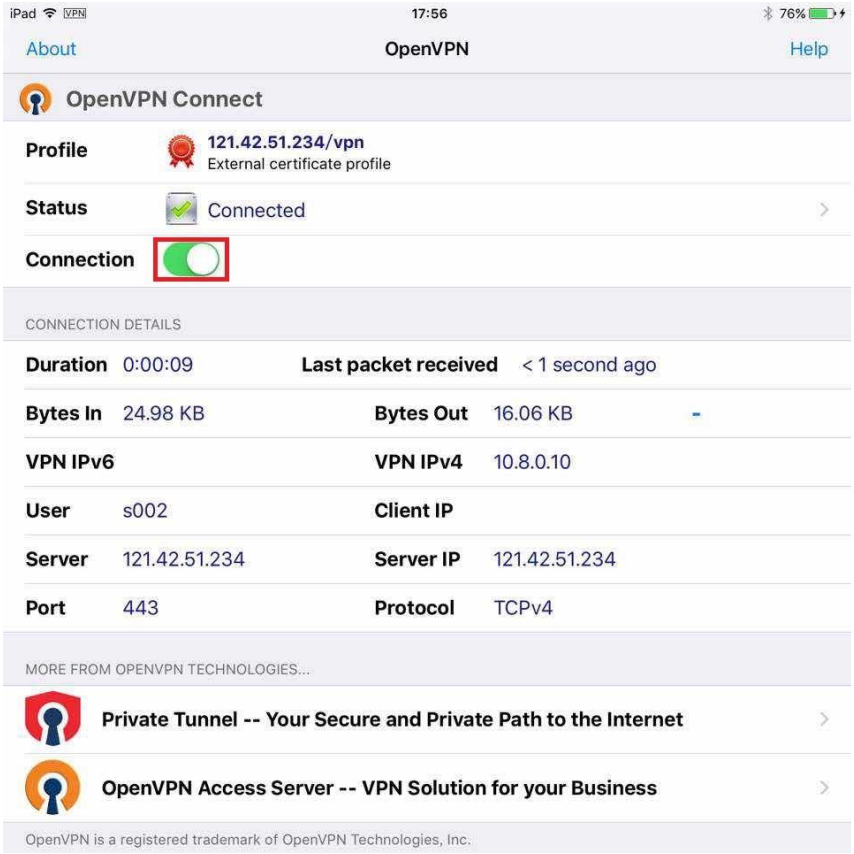


图 8-18 OpenVPN Connect 客户端 App 界面（已连接）

图 8-19 设置-VPN 界面

9 WireGuard VPN 客户端设置

WireGuard 用户的配置文件包括服务器的公钥和自己的私钥，口令只用于登录 WEB 用户门户以及 WEB、WEB 代理服务器认证和 VPN 客户端认证无关。

一旦客户端连接成功，用户自己可以先备份再在用户门户中将私钥清空，这样可以防止泄密。

如果 WireGuard VPN 客户端拨号成功，使用中突然不可用，可能是受到同一账号不能同时登陆的限制，需要再次登陆，或修改公钥、私钥后再登陆。

9.1 Windows 系统下设置 WireGuard VPN 客户端

Windows 安装使用 WireGuard VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/windows_wireguard.html

注意：

1）为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”；另外还需要修改电源属性，具体参考：http://trustcomputing.com.cn/bbs/viewthread.php?tid=1806

2）WireGuard VPN 连接成功后，如果 IE 设置了代理，则 IE 浏览器仍然通过该代理进行连接。

WireGuard VPN Windows 客户端软件下载链接

官方：https://download.wireguard.com/windows-client/wireguard-installer.exe

http://www.trustcomputing.com.cn/tools/wireguard-installer.exe

TunSafe：https://tunsafe.com/downloads/TunSafe-1.5-rc2.exe

http://www.trustcomputing.com.cn/tools/TunSafe-1.5-rc2.exe

1）安装软件

下载并安装 VPN 客户端软件，双击桌面的 VPN 程序图符，运行 VPN 客户

端软件，此时会在 Windows 桌面的右下角任务栏中出现 VPN 程序图标，如图 9-1 所示。

图 9-1 任务栏中的 WireGuard VPN 程序图标

如果没有显示，则需要设置任务栏属性，右键单击右下角的时间和日期，选择最下面的“属性”项，在弹出来的窗口中点击“选择在任务栏上显示哪些图标”项，再将“WireGuard: Fast, Modern, Secure VPN”项设置为“开”，这样就可以在任务栏里长久显示图标，如图 9-2 所示。

图 9-2 选择在任务栏上显示的程序图符

为了防止不必要的 DNS 污染，依次打开“控制面板\网络和 Internet\网络连接>[WireGuard 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>接口跃点数（Metric）”，将“自动跃点”改成“1”。

2）获取客户端配置文件

登录 WEB 用户门户，URL 是 https://_IP_/my，第一次登录时会强制修改密码，之后，在“用户>口令”页面，查看二维码，如图 9-3 所示，如果没有公钥、私钥和二维码，就点击“更新”按钮生成新的公钥、私钥和二维码，再点

击二维码图片下载 WireGuard VPN 客户端配置文件，文件名一般为 xxx_ip.conf，从 Windows 浏览器下载的文件里包含有用户名信息；如果直接扫描二维码，就没有用户名信息。

图 9-3 下载 WireGuard VPN 客户端配置文件

3）导入配置文件并连接

WireGuard 官方客户端导入配置文件并连接，如图 9-4-1 所示；Tunsafe 客户端导入配置文件并连接，如图 9-4-2 所示。

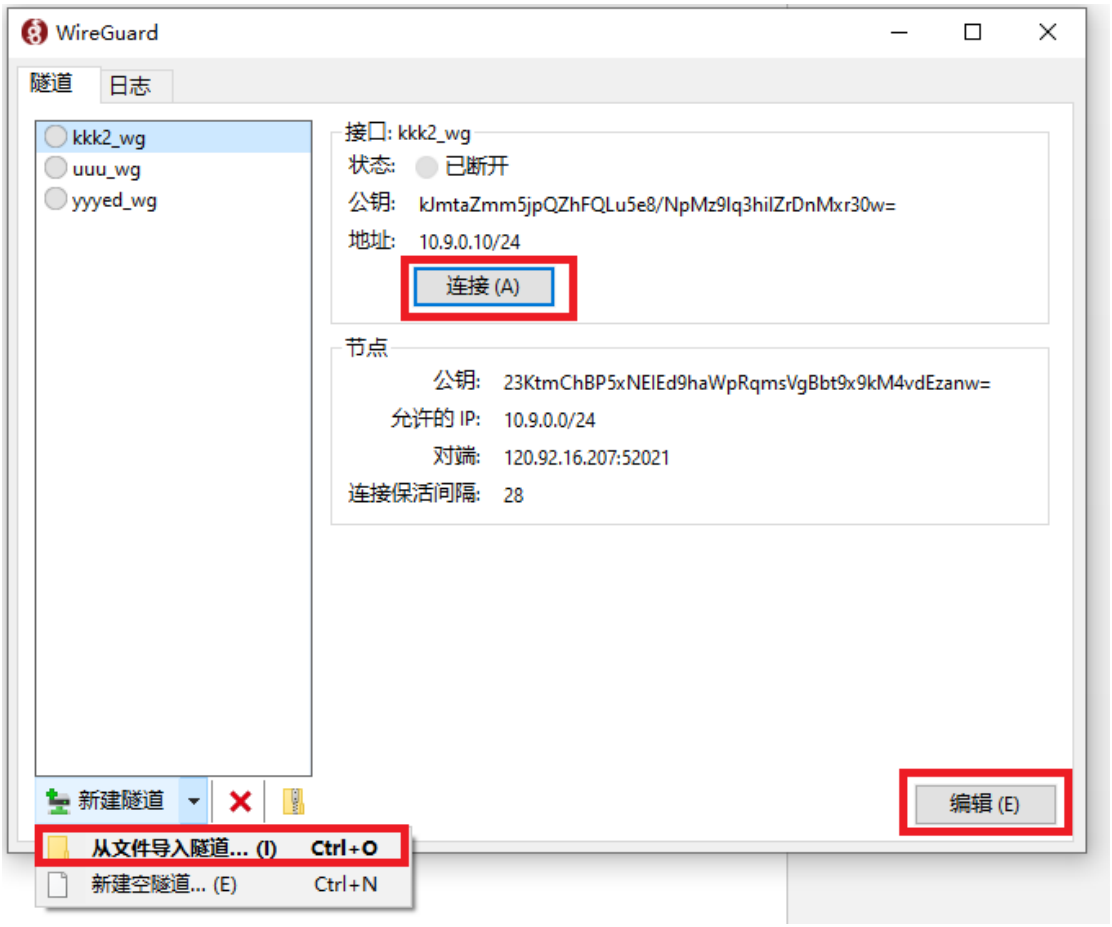


图 9-4-1 WireGuard 官方客户端界面

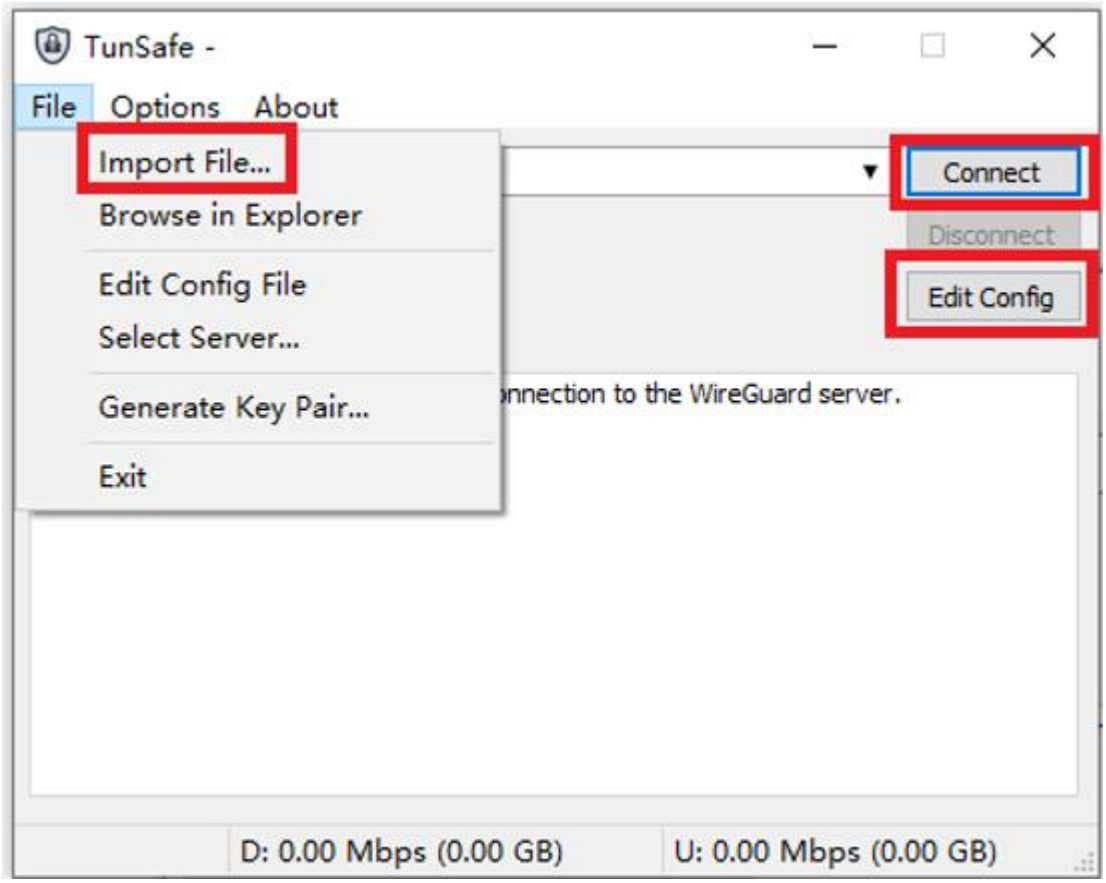
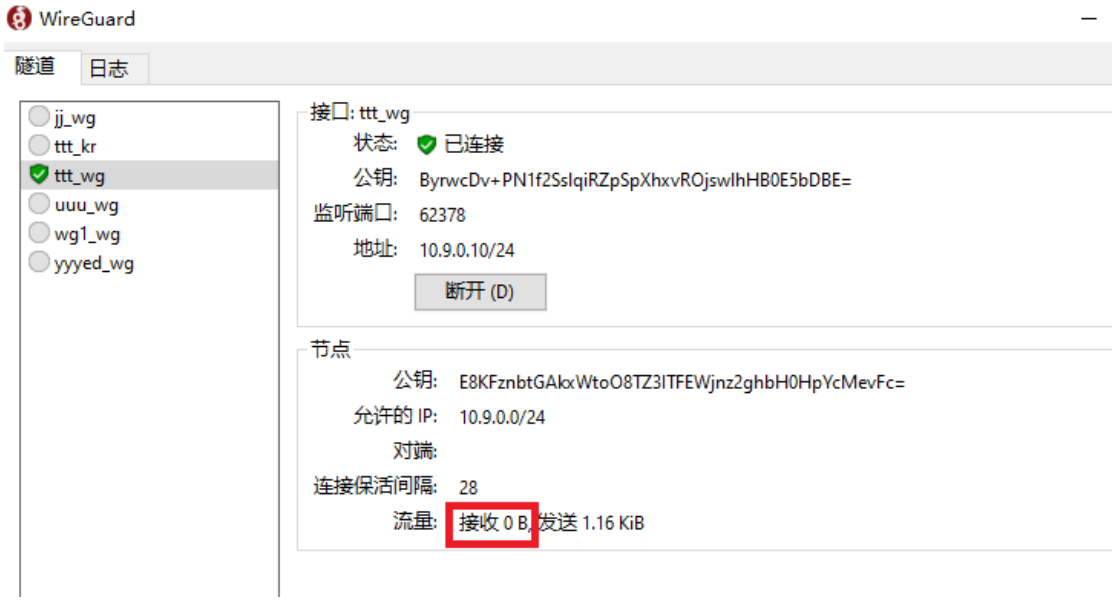


图 9-4-2 TunSafe 客户端界面

注意：

1、WireGuard 官方 Windows 客户端软件在目的地址是全部 IP 地址（0.0.0.0/0 或 0.0.0.0/1, 128.0.0.0/1）时，没有将 VPN 服务器的 IP 做原路由处理（netstat -nr 查看），仍然走 VPN 隧道，可能会导致 VPN 连通后异常(和 VPS 也有关)，可以换装 TunSafe 客户端；或者设置注册表“DangerousScriptExecution”，参考 http://www.trustcomputing.com.cn/tools/wgclient.reg



如果连接后，接收流量为 0，如上图所示，说明并没有正确连接，需要查看、修改配置文件，再连接

2、如果之前连接的 VPN 服务器突然无法再连接，之前下发的 VPN 路由不会自动撤销，可能会导致客户端网络中断，此时需要中断 VPN 连接

3、 WireGuard 官方 Windows 客户端软件不能使用 PreUp、PreDown 命令，但 TunSafe Windows 客户端软件可以通过“Options>Allow Pre/Post Commands”选项启用；或者设置注册表“DangerousScriptExecution”，参考 http://www.trustcomputing.com.cn/tools/wgclient.reg

4、为了能同时连接多个服务器（多云），可以分别使用官方 WireGuard VPN 客户端和 Tunsafe 客户端同时连接两个服务器，只要各 VPN 虚拟 IP 地址池不一样就行；或者设置注册表“MultipleSimultaneousTunnels”，参考 http://www.trustcomputing.com.cn/tools/wgclient.reg

4）编辑配置文件

以官方客户端为例说明，点击“编辑”按钮，弹出配置文件编辑对话框，如图 9-5 所示。

“[Interface]”大类下，“PrivateKey”是客户端私钥，“Address”是客户端虚拟 IP 地址，“DNS”是客户端 DNS 服务器，可用开头的#号取消。

注意：WireGuard VPN 客户端配置文件中的 DNS 服务器的值，缺省为“8.8.8.8”，需要手工添加/修改“DNS = ”值，保存文件后再重新连接才能生

效。如果填写 VPN 服务器的虚拟网卡 IP（缺省为 10.9.0.1）作为 DNS 服务器，保存文件后再重新连接，DNS 解析将 100%走 VPN 隧道，可以避免 ISP 的 DNS 污染，但也可能导致网速变慢；如果 VPN 连通后不能上网，可能是 DNS 服务器做了过滤，需要修改为没有过滤的 DNS 服务器

“[Peer]”大类下，“PublicKey”是服务器公钥，“AllowedIPs”是客户端 VPN 路由，即通过 VPN 隧道访问的目的地址，也是 VPN 连接后添加的路由项，可以根据需求缩小网段范围，例如，可以设置为和客户端虚拟 IP 所在的网段（缺省为 10.9.0.0/24），这样就不会影响现有的上网路由，只连接 VPN 虚拟服务器 IP 和其它 VPN 客户端 IP 的网络资源，“EndPoint”是服务器地址及端口（UDP 协议）。

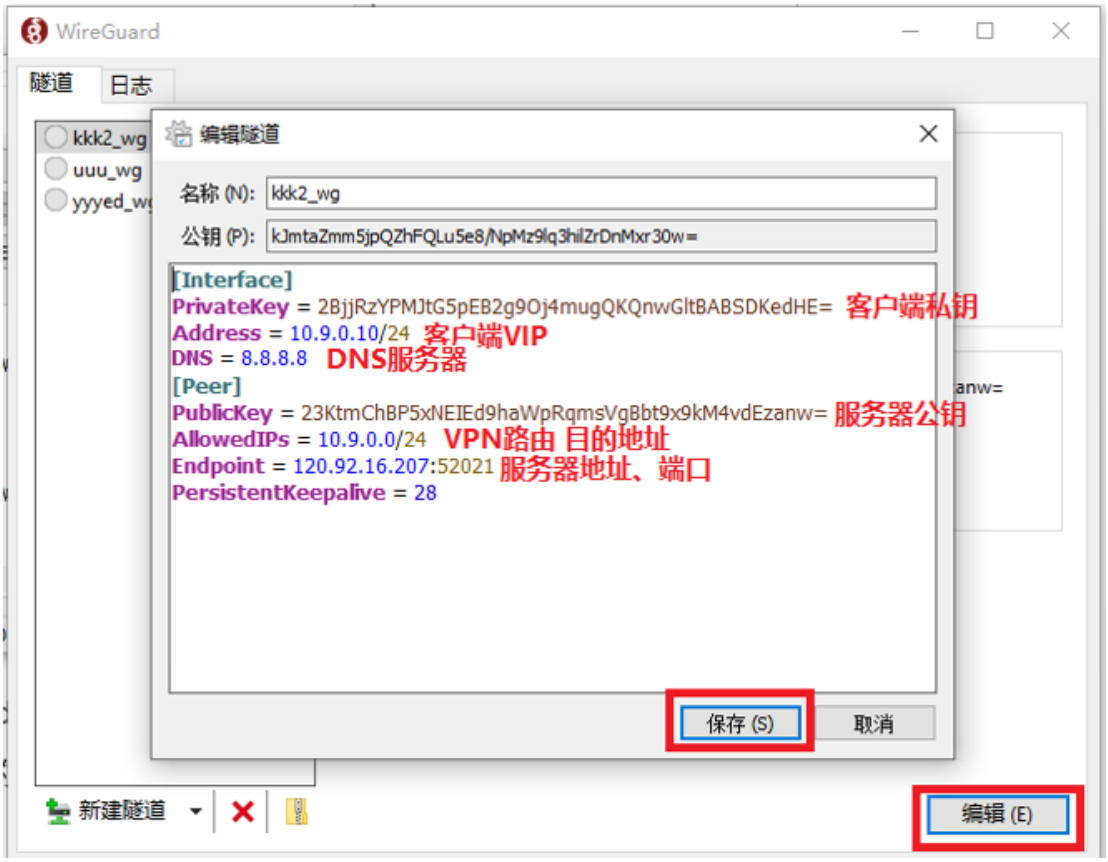


图 9-5 编辑配置文件

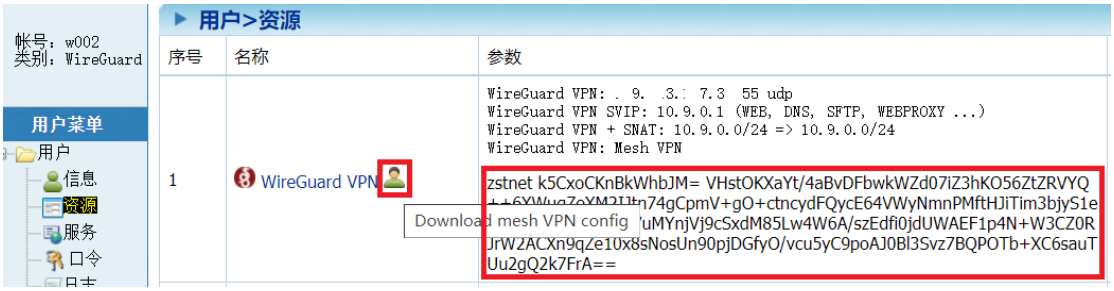
5）修改防火墙规则

VPN 连接后，在 VPN 服务器允许的前提下，为了能让 VPN 虚拟网络（缺省为 10.9.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP

地址”设置为“10.9.0.0/24”。参考图 5-5-6 所示。

注意：能连接的是监听在 WireGuard VPN 虚拟 IP 上的端口，而不是 0.0.0.0 上的端口，例如：10.9.0.10:139 这样的端口，可以用 CMD 命令 “netstat -nao | findstr 10.9.0.10”查看。

在 WEB 用户门户的“资源”页面中，可以查看当前账号的 Wireguard P2P VPN/Mesh VPN 连接信息，或者点击图符下载（事先需要备份并清空“WG 客户端私钥”的内容），文件名为“用户名_itself.bat”，此批处理文件不是给此用户使用的，是给其它用户添加此用户节点用的，双方分别在自己的 PC 上以管理员身份运行对方的 xxx_itself.bat 文件后，即构成 P2P VPN/Mesh VPN。



Windows 下，bat 批处理文件下载后，按右键“以管理员身份运行”。bat 批处理文件中用到的可执行文件 zstnet.exe 需要下载并拷贝到环境变量 PATH 中任意一个目录下（例如： c:\windows 等），下载地址是：

http://www.trustcomputing.com.cn/tools/zstnet.exe

Linux 下，bat 批处理文件下载后，需要执行命令“ sh xxx_meshvpn.bat”生效。Linux 下需要事先安装大地云控本系统，bat 批处理文件用到的可执行文件位于/usr/bin/zstnet，另外也有在线下载，下载地址是：

http://www.trustcomputing.com.cn/tools/zstnet

9.2 Android 系统下设置 WireGuard VPN 客户端

安卓系统安装使用 WireGuard VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/android_wireguard.html

WireGuard VPN 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=com.wireguard.android

https://apkcombo.com/zh/apk-downloader/?q=com.wireguard.android

https://play.google.com/store/apps/details?id=com.tunsafe.app

1）安装软件

下载 WireGuard VPN 客户端软件，安装后，点击桌面的 WireGuard VPN 程序图符，如图 9-6 所示，运行 WireGuard VPN 客户端软件，如图 9-7 所示。

图 9-6 桌面上的 WireGuard VPN 安卓客户端软件

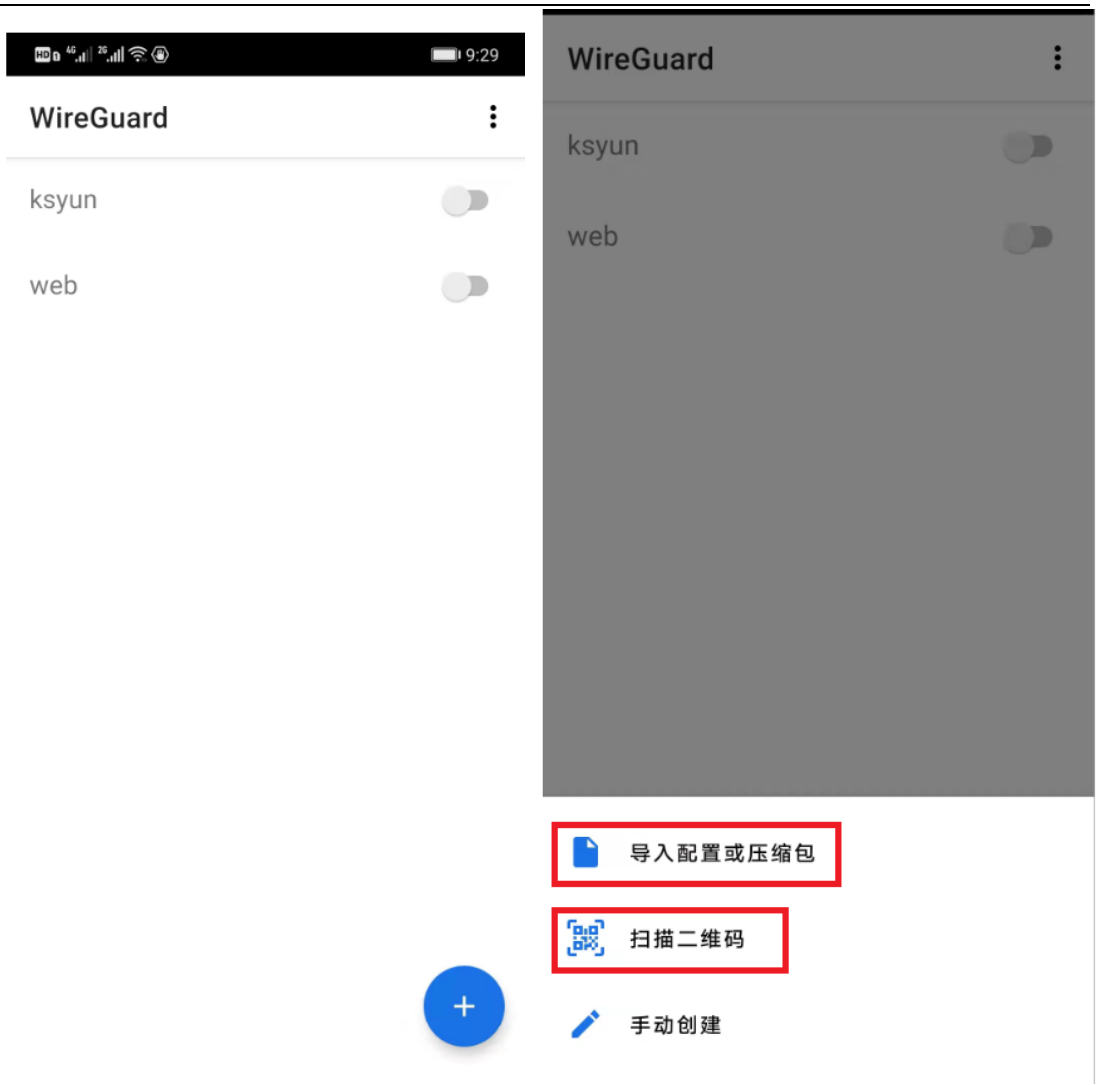


图 9-7 WireGuard VPN 安卓客户端软件界面

2）导入配置文件

A）扫描二维码导入配置文件

点击右下角+号按钮，选择“扫描二维码”，再登录 WEB 用户门户，在“用户>口令”页面下方有配置文件的二维码，扫描该二维码，在弹出的窗口中输入配置文件的名称，即可导入配置文件。

B）上传文件导入配置文件

使用手机 Chrome 浏览器（非系统自带浏览器）登录用户门户，在“用户>口令”页面点击下方的二维码下载配置文件，文件缺省保存至“/sdcard/Download”目录下。或者，在 Windows 下打开浏览器登录用户门户，在“用户>口令”页面点击下方的二维码下载配置文件，再修改配置文件，将#号开头的注释删掉，并保存文件，再输入网址 https://wx.qq.com，出现一个二维码；用手机登录微信，

再扫描这个二维码，进入 WEB 界面，再点击左边的“文件传输助手”项，再点击右下方的文件夹图符，在打开的文件框里选择事先修改好的 xxx_wg.conf 配置文件，上传至手机，如图 9-8 所示。

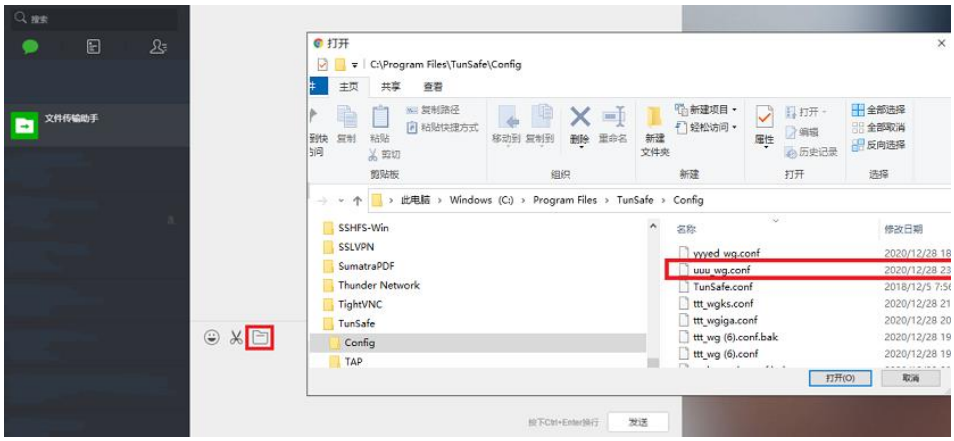


图 9-8 上传配置文件

再打开手机微信的“文件传输助手”，分别点击、打开刚才上传的文件，点击右上角  图符，选择保存，即可将配置文件上传到手机。

在手机的 WireGuard VPN 客户端软件中，点击右下角+号按钮，选择“导入配置或压缩包”，在弹出的窗口中点击左上角 ☰ 图符，继续选择手机空间项，如图 9-9 左边所示。

图 9-9 选择配置文件

在文件系统中，选择“/sdcard/Download/WeiXin”目录，并选择上传的 conf 文件，如图 9-9 右边所示，在弹出的窗口中输入配置文件的名称，即可导入配置文件。

3）连接服务器

返回 WireGuard VPN 客户端软件主界面，点击配置文件名称右边的开关按钮 ，如果一切正常，就可以连接成功了，如图 9-10 所示。

图 9-10 WireGuard VPN 客户端软件连接成功

注意：

1、WireGuard 官方客户端软件在目的地址是全部 IP 地址（0.0.0.0/0 或 0.0.0.0/1, 128.0.0.0/1）时，没有将 VPN 服务器的 IP 做原路由处理，仍然走 VPN 隧道，可能会导致 VPN 连通后异常，可以换装 TunSafe 客户端

2、为了在重新打开系统时 VPN 不中断，需要

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

9.3 iOS 系统下设置 WireGuard VPN 客户端

iOS 系统安装及使用 WireGuard VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/wireguard/ios_wiregua

rd.html

WireGuard VPN iOS 客户端软件下载链接（美区）

https://apps.apple.com/us/app/wireguard/id1441195209

https://itunes.apple.com/us/app/tunsafe-vpn/id1441020790

https://testflight.apple.com/join/63I19SDT

需要用美国的 Apple ID 登陆 iTunes Store 与 App Store，再下载 WireGuard VPN 客户端 App，具体过程为参见 8.3。

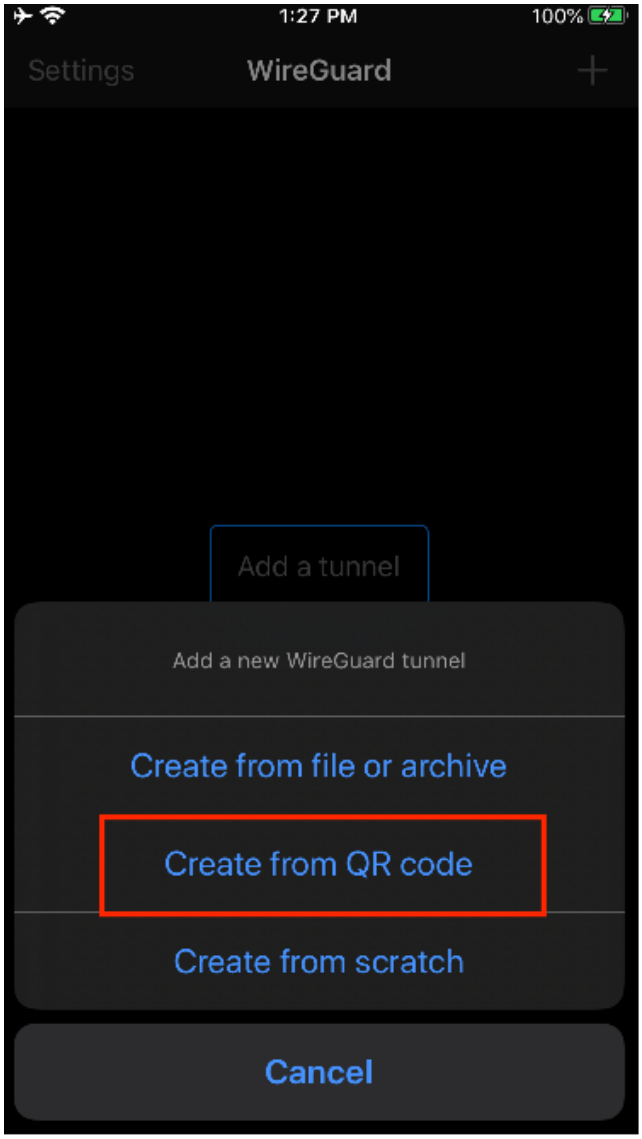


图 9-11 WireGuard VPN iOS 客户端

运行 WireGuard VPN 客户端 App，如图 9-11 所示，点击右下角+号按钮，选择扫描二维码，再登录 WEB 用户门户，在“用户>口令”页面下方有配置文件的二维码，扫描该二维码，在弹出的窗口中输入配置文件的名称，即可导入配置文件。

返回 WireGuard VPN 客户端 App 主界面，点击配置文件名称右边的开关按钮  ，如果一切正常，就可以连接成功了。之后可以在系统设置>VPN 里启用、停用设置好的 VPN，如图 9-12 所示。

图 9-12 设置-VPN 界面

10 SoftEther VPN 客户端设置

10.1 Windows 系统下设置 SoftEther VPN 客户端

Windows 安装使用 SoftEther VPN 示例

http://www.trustcomputing.com.cn/help/cn/dadi/softether/windows_softether.html

注意：

1）为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”

2）SoftEther VPN 连接成功后，如果原来设置了系统代理，则浏览器仍然通过原来的代理进行连接。

SoftEther VPN Windows 客户端软件下载链接

https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/releases/download/v4.29-9680-rtm/softether-vpnclient-v4.29-9680-rtm-2019.02.28-windows-x86_x64-intel.exe

目前，暂无安卓和 iOS 下的 SoftEther VPN 客户端 App，另外还有 Linux 和 MacOS 系统下的客户端软件。

下载并安装 SoftEther VPN 客户端软件，双击桌面的“SoftEther VPN Client 管理工具”程序图符，对应的文件是“"C:\Program Files\SoftEther VPN Client\vpncmgr_x64.exe"”，运行 SoftEther VPN 客户端软件，程序主界面如下图 10-1 所示。

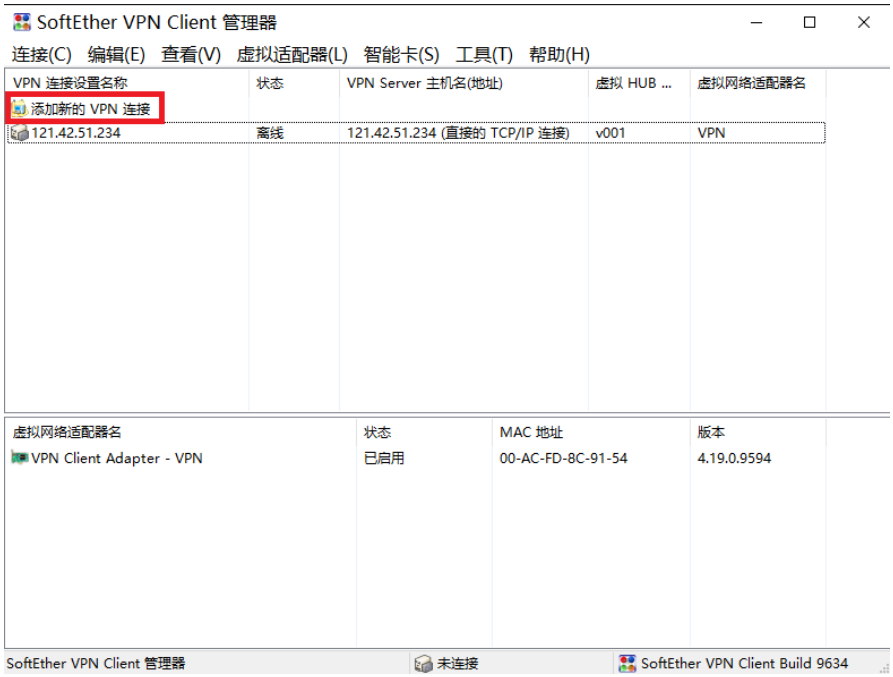


图 10-1 SoftEther VPN 软件主界面

双击“添加新的 VPN 连接”项，弹出“新的 VPN 连接设置属性”窗口，如下图 10-2 所示。

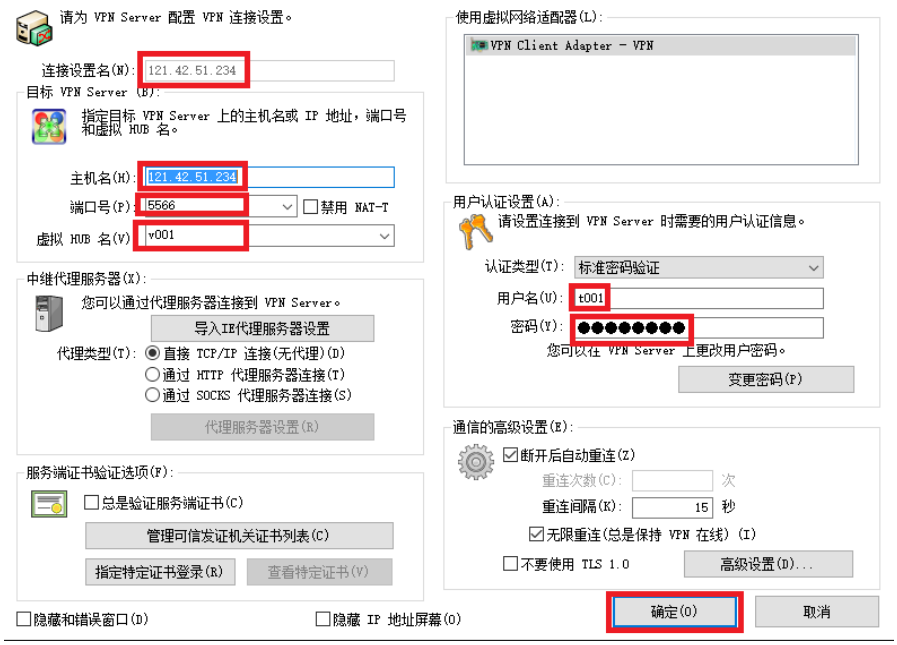


图 10-2 VPN 连接设置属性窗口

依次输入连接设置名、主机名、端口号、用户名、密码，其中端口号缺省为 5566，虚拟 HUB 名会根据主机名和端口号的内容自动查询并显示，最后点击“确定”按钮。

服务端口对应的协议缺省是“TCP/UDP”，如果客户端连接后出现带宽下降甚至不能用的情况，可能是 ISP 对 UDP 流量做了带宽 QoS 限制，此时需要把“端口号”后面的“禁用 NAT-T”选项启用，即禁用 UDP 协议。

返回主界面后，双击该 VPN 连接项，如果连接顺利、用户认证成功，就会显示分配的 IP 地址，如下图 10-3 所示，点击“关闭”按钮，返回主界面。

图 10-3 VPN 连接成功窗口

右键点击 VPN 连接项，弹出菜单，如下图 10-4 所示。

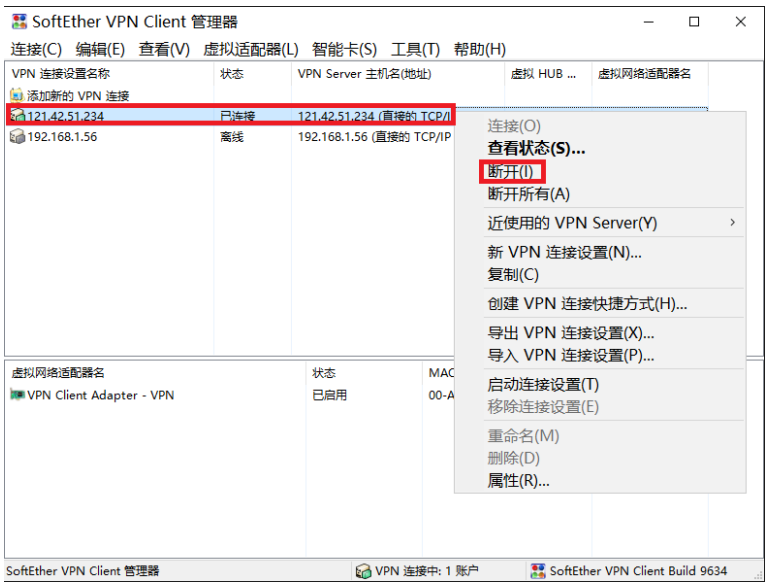


图 10-4 VPN 连接项的菜单

选择“断开”项，即可断开 VPN 连接。

为了防止不必要的 DNS 污染,需要修改 Windows 的 SoftEther VPN 网卡-“VPN Client Adapter - VPN”属性,“Internet 协议版本 4（TCP/IPv4)”>“高级设置”中的“接口跃点数”(Metric)，将“自动跃点”改成“1”。

VPN 连接后，为了能让 VPN 虚拟网络（192.168.30.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”,“作用域”的“本机 IP 地址”设置为“192.168.30.0/24”,参考图 5-5-6 所示。

11 L2TP VPN 客户端设置

11.1 Windows 系统下设置 L2TP VPN

Windows 系统下 使用预共享密钥的 L2TP VPN 设置示例
http://www.trustcomputing.com.cn/help/cn/dadi/l2tp/windows_l2tp1.html

Windows 系统下 使用证书的 L2TP VPN 设置示例
http://www.trustcomputing.com.cn/help/cn/dadi/l2tp/windows_l2tp2.html

注意：

1）Windows 内置的 L2TP VPN 连接成功后，浏览器的连接将忽视原有 IE 的代理设置，使用 Proxy SwitchyOmega 插件的 Chrome 浏览器不受影响，如果要设置代理，需要单独给每个 VPN 连接设置代理。L2TP VPN 无需修改网络的默认网关属性以及下载安装自签名 CA 证书。

2）可以通过安装特定的软件实现 Windows 内置的 VPN 拨号随机启动自动拨号，无需人工交互输入，适用于无人值守或普通用户无感知的情形。

具体操作步骤参考“**5.1.1 Windows10 内置的 IKEV2 VPN 设置**”节的“**1）建立 VPN 连接**”部分，主要的改变是图 5-3“添加 VPN 连接”窗口中，VPN 类型选择“使用预共享密钥的 L2TP/IPsec”项，或“使用证书的 L2TP/IPsec”项(可能无法连接)，如下图 11-1-1 所示。


VPN 连接
连接名称
aliyun l2tp
服务器名称或地址
121.42.51.234
VPN 类型
使用预共享密钥的 L2TP/IPsec
预共享密钥
myPSKkey
登录信息的类型
用户名和密码
用户名(可选)
t001
保存
取消

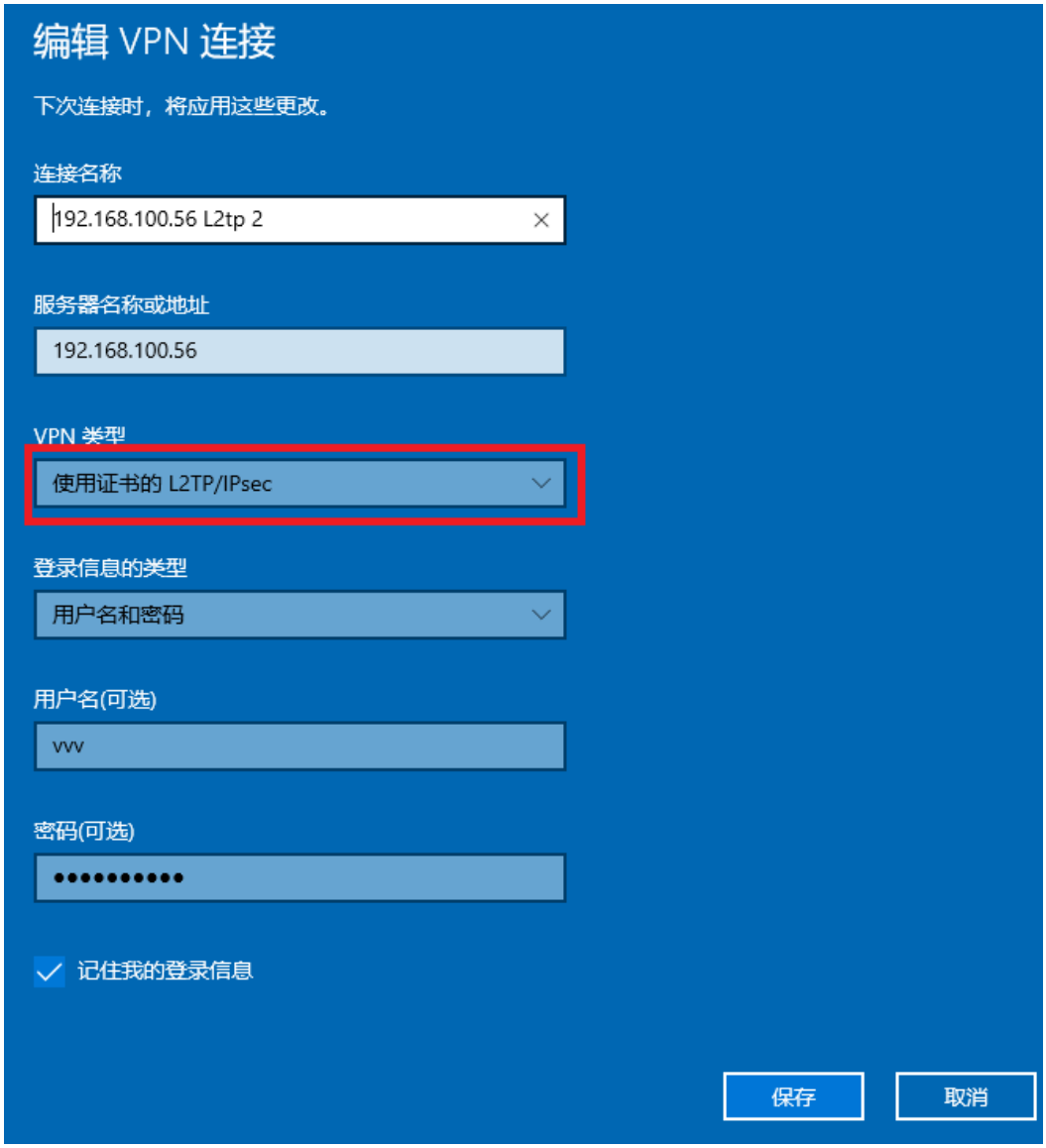


图 11-1-1 L2TP VPN 连接参数窗口

Windows 系统下设置 L2TP VPN 过程描述如下：

1）鼠标双击右下角“网络”图标，弹出 VPN 列表，点击任意项目，弹出“网络和 INTERNET”窗口；

2）点击最上面的“添加 VPN 连接”项目，出现“添加 VPN 连接”窗口。依次输入正确的内容，最后点击“保存”按钮，其中“服务器名称或地址”栏可以是 IP 或域名，VPN 类型选择“使用预共享密钥的 L2TP/IPsec”项，预共享密钥为“myPSKkey” ，不需要事先安装 CA 证书，或“使用证书的 L2TP/IPsec”项；

3）添加完成后，还需要修改多项设置：

a）修改网络连接属性，连接属性中“安全”TAB 中的“身份验证”框中，需要选择“允许使用这些协议”，再勾选“质询握手身份验证协议（CHAP）”项。如下图 11-1-2 所示。

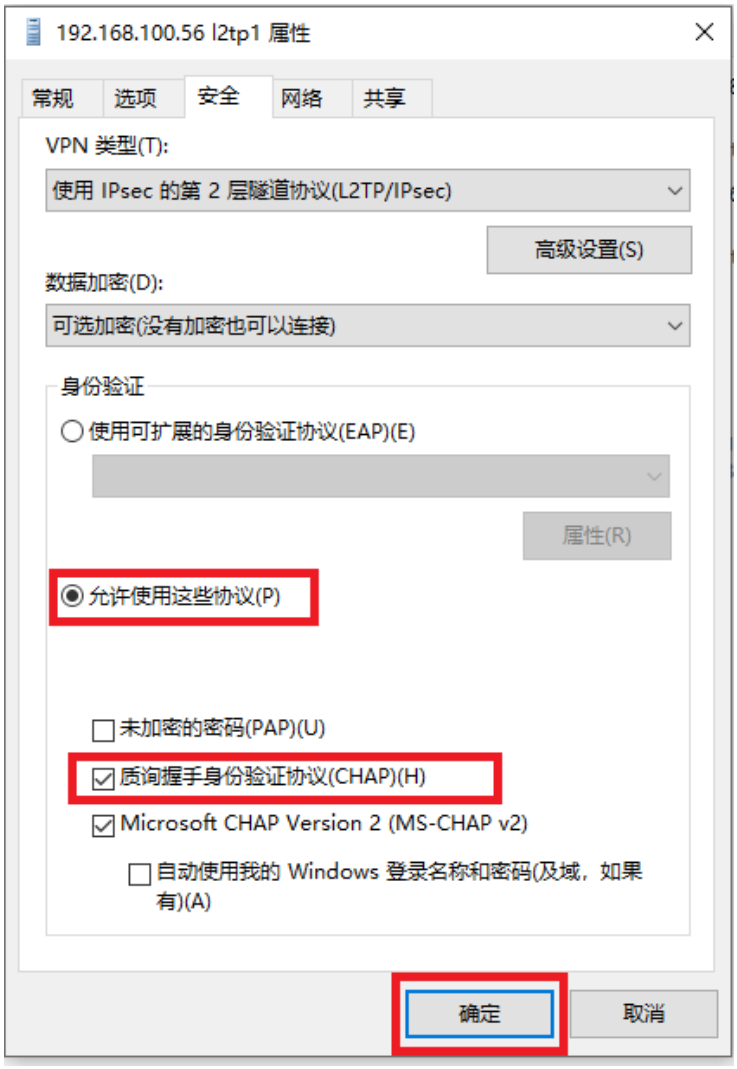


图 11-1-2 修改 L2TP 安全属性

b）修改 Windows 10 注册表，使得处于 NAT 的客户端也能连接，需要重启 Windows 才能生效。

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v
AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 0x2 /f
```

参考：https://superuser.com/questions/1298513/l2tp-ipsec-vpn-fails-to-connect-on-windows-10-works-fine-on-ios

c）如果 IKEv2/IPSEC 服务不存在或证书不对，可以使用 RAW L2TP（未加密，不安全），需要修改注册表，找到 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters，在“编辑”菜单上，单击“新建”->“DWORD 值”，在“名称”框中，键入“ProhibitIpSec”，在“数值数据”框中，键入“1”，然后单击“确定”，退出注册表编辑器，然后重新启动计算机，此时，选择预共享密钥或证书两种类型都行，实际上和 IKEv2（500、4500/UDP）无关的 RAW L2TP（1701/UDP）；反之，如果要使用“使用预共享密钥的 L2TP/IPsec”，就要删除“ProhibitIpSec”，再重新启动计算机

d）为了防止不必要的 DNS 污染，依次打开“控制面板\网络和 Internet\网络连接>[L2TP 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>接口跃点数（Metric）”，将“自动跃点”改成“1”。

e）VPN 连接后，为了能让 VPN 虚拟网络（10.7.0.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“10.7.0.0/24”，参考图 5-5-6 所示。

4）以上设置修改完成后，在 VPN 列表中找到新添加的连接名称，需要连接时可以点击该项，再点击下方的“连接”按钮，就可以连接 VPN 了。

11.2 安卓系统下设置 L2TP VPN

安卓系统 L2TP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/l2tp/android_l2tp.html

安卓系统下 L2TP VPN 具体设置过程描述如下：

1）点击桌面的“设置”图符，再点击“更多”菜单项，再点击“VPN”菜单项；

2）再点击左下角的“添加 VPN 网络”菜单项，输入名称、服务器地址栏的内容，类型选择“L2TP”项，也可以选择“L2TP/IPSec PSK”项，同时 IPSec 预共享密钥为“myPSKkey”，再点击“保存”按钮，如下图 11-2 所示；

3）如果不想让 L2TP 连接成为缺省路由，就打开“显示高级选项”开关，在“转发路线”栏中填写“10.7.0.0/24” ，相当于只是修改 DNS 服务器，其它流量还是走原来的 WIFI 或移动数据流量网络；

4)返回 VPN 界面后，点击刚才新建的 VPN，在对话框中输入用户名和密码。

图 11-2 安卓系统下 **L2TP VPN** 网络属性

其它示意图请参考“**7.2 安卓系统下设置 PPTP VPN**”的内容。

为了在重新打开系统时 VPN 不中断，需要在“电池”设置中，启用“休眠时始终保持网络连接”选项。华为、荣耀系列安卓、鸿蒙手机可能无法连接 L2TP

over IPSEC VPN。

11.3 iOS 系统下设置 L2TP VPN

iOS 系统 L2TP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/l2tp/ios_l2tp.html

iOS 系统下设置 L2TP VPN 过程描述如下：

1）点击桌面的“设置”图符，再点击“通用”菜单项，再点击右边下方的“VPN”菜单项，如果已经有了 VPN 设置，则在左上方就有 VPN 菜单项；

2）再点击右边下方的“添加 VPN 配置…”菜单项，选择类型为“L2TP”，输入描述、服务器、账户、密码栏的内容，密钥为“myPSKkey”，如果不想让 L2TP 连接成为缺省路由，就关闭“发送所有流量”选项，相当于只是修改 DNS 服务器，其它流量还是走原来的 WIFI 或移动数据流量网络；再点击右上角的“完成”按钮，详见下图 11-3 所示；

3）返回 VPN 界面后，勾选 VPN 连接，再点击“状态”栏“未连接”开关。

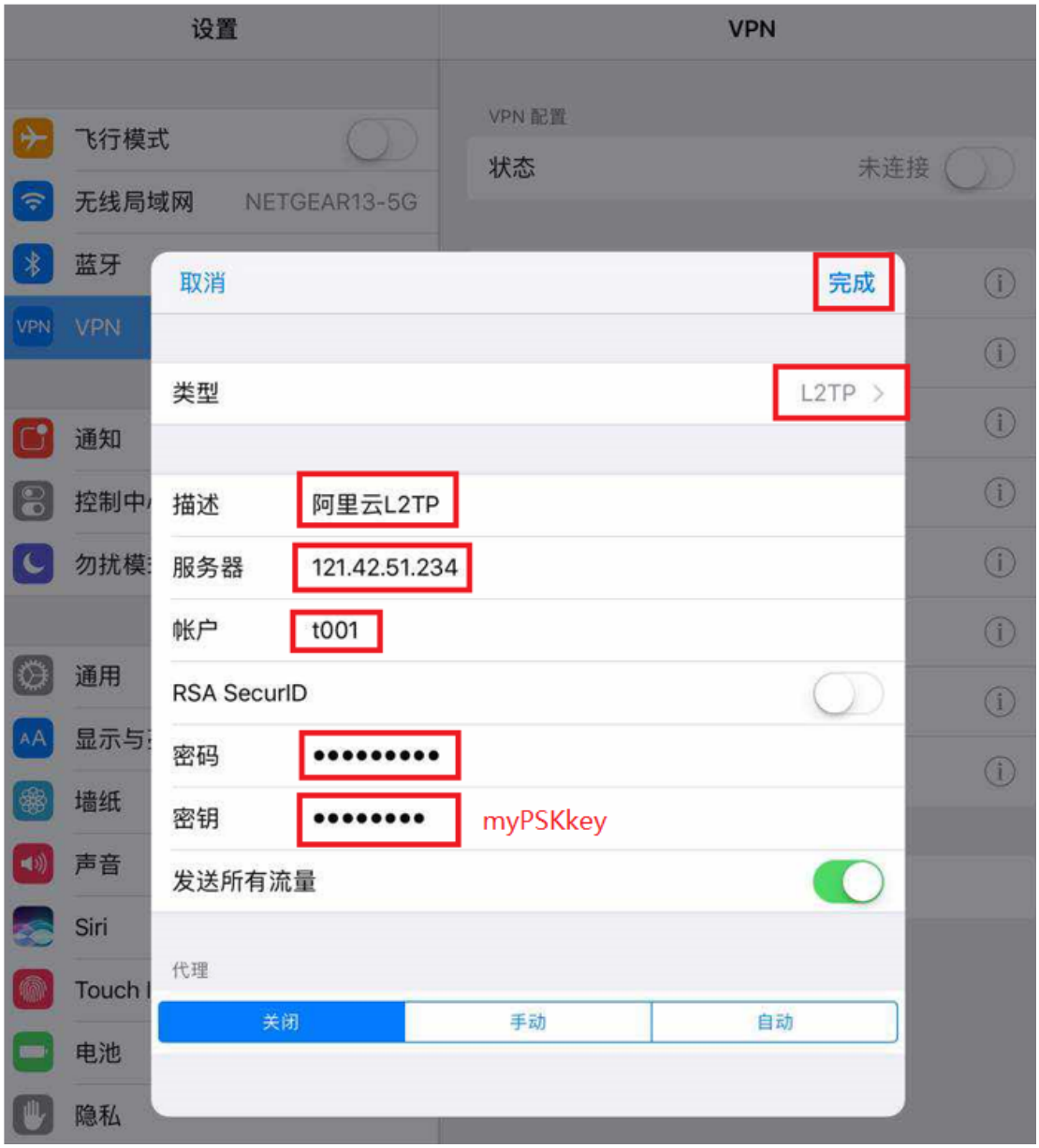


图 11-3 iOS 系统下 L2TP VPN 连接属性

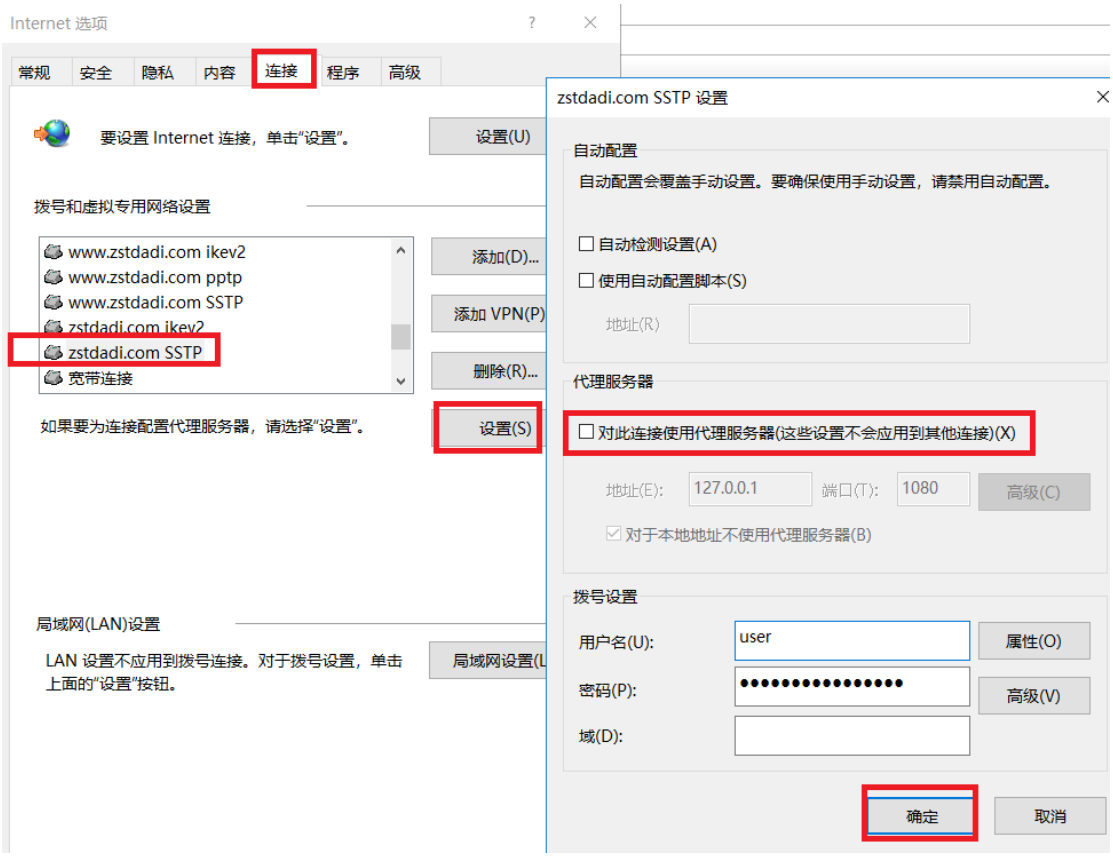
其它示意图请参考“**7.3 iOS 系统下设置 PPTP VPN**”的内容。

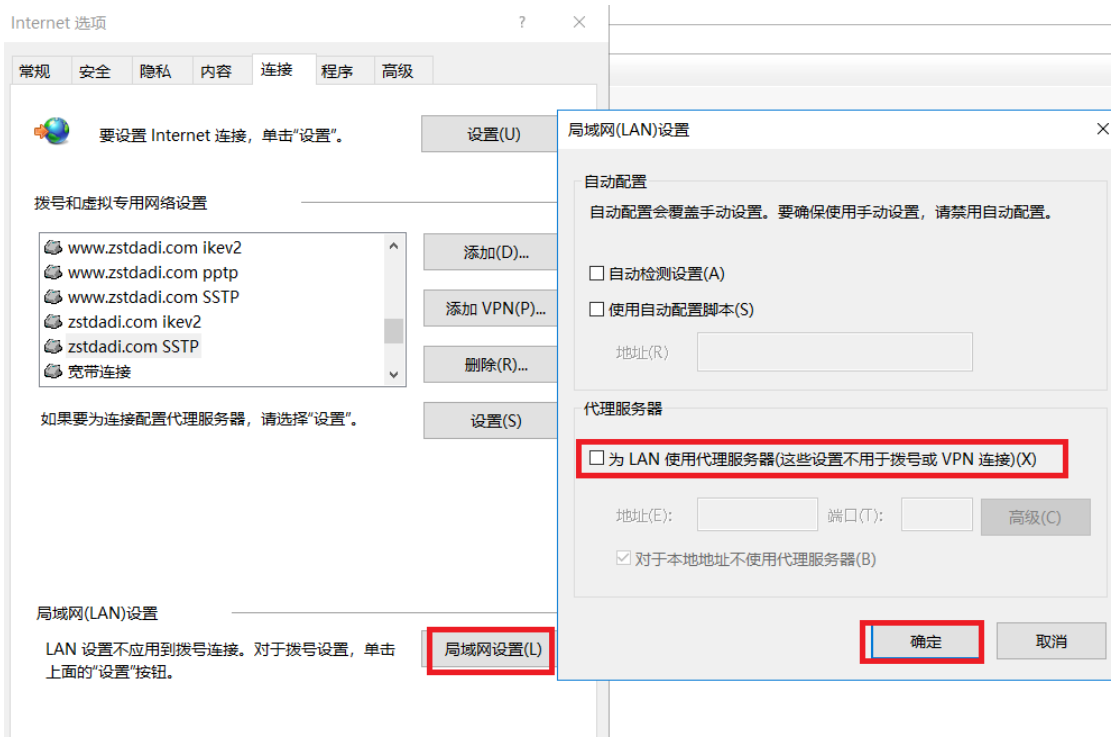
12 SSTP VPN 客户端设置

12.1 Windows 系统下设置 SSTP VPN

Windows 系统下 SSTP VPN 设置示例
http://www.trustcomputing.com.cn/help/cn/dadi/sstp/windows_sstp.html

Windows 内置的 SSTP VPN 客户端使用 TCP 协议，连接时，将首先通过现有 IE 的代理设置进行连接，如需直接连接，请停用现有 IE 的代理设置（4.1.1），
需要在以下两个设置界面中取消代理服务器，参见下图





为了避免 Windows 锁屏后，VPN 自动断开，需要修改物理网卡的“电源管理”属性，不勾选“允许计算机关闭此设备以节约电源”。

可以通过安装特定的软件实现 Windows 内置的 VPN 拨号随机启动自动拨号，无需人工交互输入，适用于无人值守或普通用户无感知的情形。

新建的 SSTP VPN 连接缺省使用 VPN 隧道作为连接后的默认网关，如需取消，即只使用 VPN 服务器虚拟网络上的服务，请依次打开“控制面板\网络和 Internet\网络连接>[SSTP 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>在远程网络上使用默认网关”并取消。

为了防止不必要的 DNS 污染，依次打开“控制面板\网络和 Internet\网络连接>[SSTP 连接]>属性>网络>Internet 协议版本 4（TCP/IPv4）>属性>高级>接口跃点数（Metric）”，将“自动跃点”改成“1”。

服务器地址不是真实域名时，SSTP VPN 客户端还需要下载安装验证 CA 证书并修改 hosts 文件。

Windows 系统下设置 SSTP VPN 分为两个步骤：下载安装自签名 CA 证书以及建立 VPN 连接。注意：当管理员为服务器地址申请了真实域名证书后，可不必再

下载安装自签名 CA 证书及修改 hosts 文件。

1）下载安装自签名 CA 证书

对于 SSTP VPN 需要在连接 VPN 前安装 VPN 服务器的 CA 证书（和 IKEV2 VPN 共一套 CA 证书，由 IKEV2 VPN 具体设置），具体操作步骤参考“**2.2.1 Windows 系统的证书导入**”。

CA 证书文件在线下载的 URL 类似“http://121.42.51.234/myca.crt”这样，证书安装到“本地计算机”“受信任的根证书颁发机构”项目中。

如果 VPN 拨号客户端出现“由本地系统终止网络连接/The network connection was aborted by the local system”的错误提示，可能是“服务器名称或地址”栏中的服务器 IP 或域名后面没有加端口号，应该是“121.42.51.234:5566”或“zstdadi.com:5566”这样。

2）建立 VPN 连接

具体操作步骤参考“**5.1.1 Windows10 内置的 IKEV2 VPN 设置**”节的“**1）建立 VPN 连接**”部分，主要的改变是图 5-3“添加 VPN 连接”窗口中，VPN 类型选择“安全套接字安全协议（SSTP）”项，再点击“保存”按钮，如下图 12-1 所示。

图 12-1 SSTP VPN 连接参数窗口

Windows 系统下设置 SSTP VPN 过程描述如下：

1）鼠标双击右下角“网络”图标，弹出 VPN 列表，点击任意项目，弹出“网络和 INTERNET”窗口；

2）点击最上面的“添加 VPN 连接”项目，出现“添加 VPN 连接”窗口。依次输入正确的内容，最后点击“保存”按钮，其中“服务器名称或地址”栏的内容可以是 IP 或域名加端口，中间以冒号:隔离，缺省端口是 5566，VPN 类型选择“安全套接字安全协议（SSTP）”项；

注意：

I、SSTP VPN 的“服务器名称或地址”需要和 VPN 服务器的服务器证书中的 CN 值保持一致（由 IKEV2 VPN 管理端决定），而 VPN 服务器的 CA 证书需要安装到客户端 Windows 系统中。

II、如果内容是域名（缺省是 zstdadi.com），且不是真实的域名，那么还要将域名解析成 IP，以管理员身份修改

“C:\Windows\System32\drivers\etc\hosts”文件，具体操作步骤参考“**2.2.5 编辑 hosts 文件**”，或者设置专门的 DNS 服务器做解析。

3）添加成功后，返回列表，在最后可以找到新添加的连接名称，需要连接时可以点击该项，再点击下方的“连接”按钮，就可以连接 VPN 了。如果设置正确但连接不成功，请取消 IE 浏览器里的代理服务器设置，具体见本章开头所述。

3）修改防火墙规则

VPN 连接后，为了能让 VPN 虚拟网络（192.168.30.0/24）内的其它终端能访问本机的虚拟 IP，可以设置防火墙策略，启用所有的防火墙，再在“高级设置”中添加“入站规则”，“作用域”的“本机 IP 地址”设置为“192.168.30.0/24”，参考图 5-5-6 所示。

12.2 安卓系统下设置 SSTP VPN

安卓系统 SSTP VPN 设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/sstp/android_sstp.html

SSTP VPN 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=it.colucciweb.sstpvpnclient

该 App 是收费下载的 App，具体设置过程略。

为了在重新打开系统时 VPN 不中断，需要：

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

13 SS 客户端设置

13.1 Windows 系统下设置 SS 客户端

Windows 安装使用 SS 客户端示例

http://www.trustcomputing.com.cn/help/cn/dadi/ss/windows_ss.html

注意：

SS 客户端连接成功后，会自动修改 IE 浏览器的代理设置，使用 Proxy SwitchyOmega 插件的 Chrome 浏览器不受影响。

可以使用 netch、ProxyCap 软件的进程模式，选择浏览器、游戏客户端的.exe 文件，使得浏览器、游戏客户端可以透明使用 socks 代理服务。

可以使用 V2rayN 软件，加入 SS、TJ 服务器。

SS Windows 客户端软件下载链接

https://github.com/shadowsocks/shadowsocks-windows/releases/download/4.1.6/Shadowsocks-4.1.6.zip

https://sourceforge.net/projects/sscap/

可以直接输入 ss://链接或扫描二维码快速建立服务器配置。

1）安装软件

下载并解压 SS 客户端软件，双击 Shadowsocks.exe 文件，运行 SS 客户端软件，此时会在 Windows 桌面的右下角任务栏中出现 SS 程序图标，如图 13-1 所示。

图 13-1 任务栏中的 SS 程序图标

2）新建 SS 连接

右键点击 SS 程序图标，弹出主菜单，选择“服务器”项，弹出子菜单，再选择“编辑服务器...”项，如下图 13-2 所示。

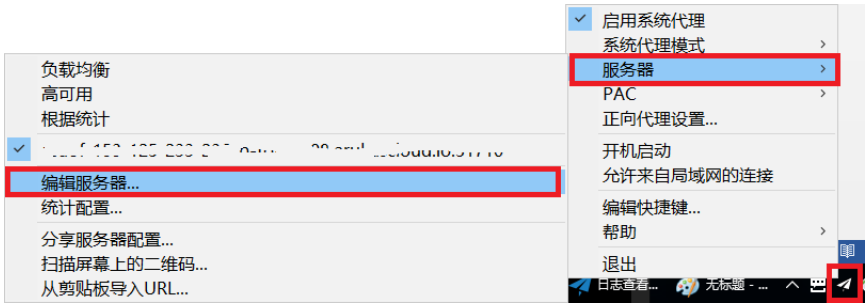


图 13-2 Windows 系统下新建 SS 连接

弹出“编辑服务器”窗口，如下图 13-3 所示。

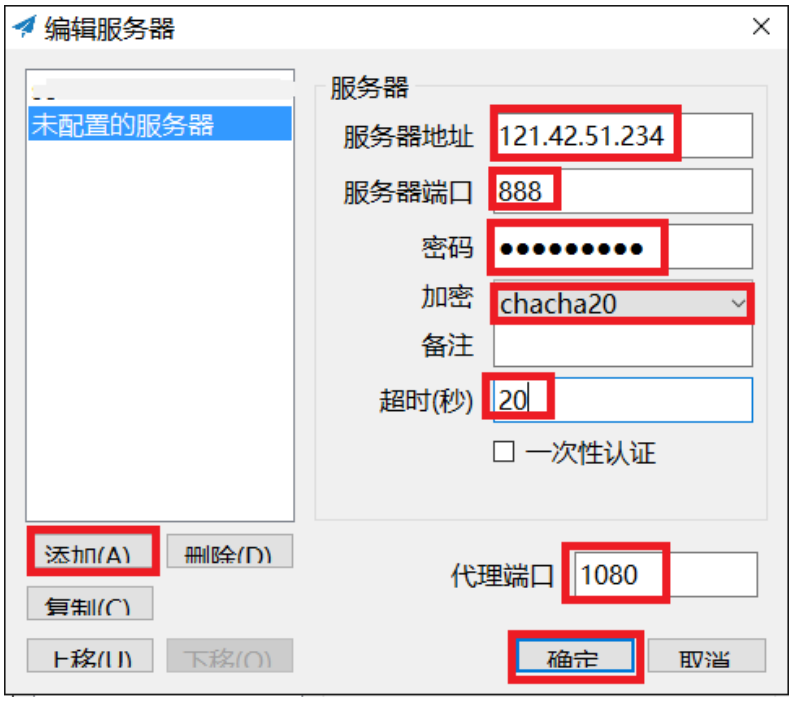


图 13-3 编辑服务器窗口

首先点击左下角的“添加”按钮，再在右边窗口中依次输入各项内容，最后点击“确定”按钮，这样就新建了一个 SS 连接，并马上进行连接。

还可以事先拷贝类似“ss://Y2hhY2hhMjA6UzUzV0NZT1FPW1BoQDExNy40OC4yMDguMTgyOjg4OA==”这样的 URL（不能加#号，SSR 客户端软件可以带#号），再选择“从剪贴板导入 URL…”选项，软件会自动解码，并显示类似图 13-3 这样的编辑服务器窗口，直接点击“确定”按钮即可新建。

另外，还需要在主菜单中设置“系统代理模式”项为“全局模式”，并勾选“启用系统代理”项，如下图 13-4 所示。

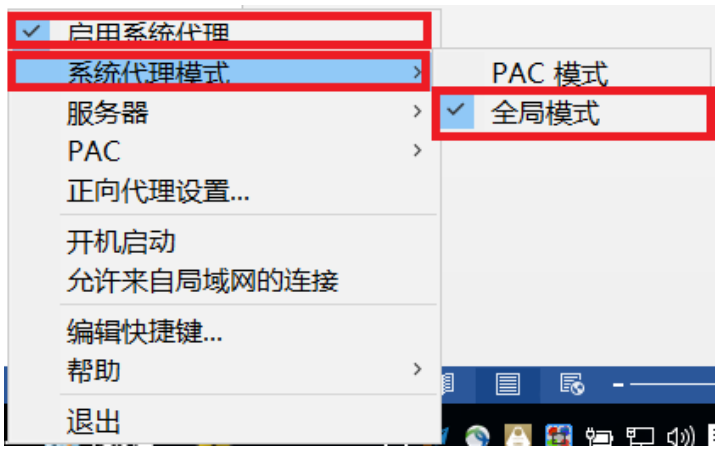


图 13-4 启动 SS 选项

当连接成功，任务栏的 SS 程序图标会变成深蓝色，当有数据传输时，SS 程序图标会出现一对上下箭头。

3）管理 SS 连接

右键点击任务栏上的 SS 程序图标，在弹出的主菜单中选择“帮助”项，弹出子菜单，勾选“详细记录日志”项，并选择“显示日志...”项，如下图 13-5 所示。

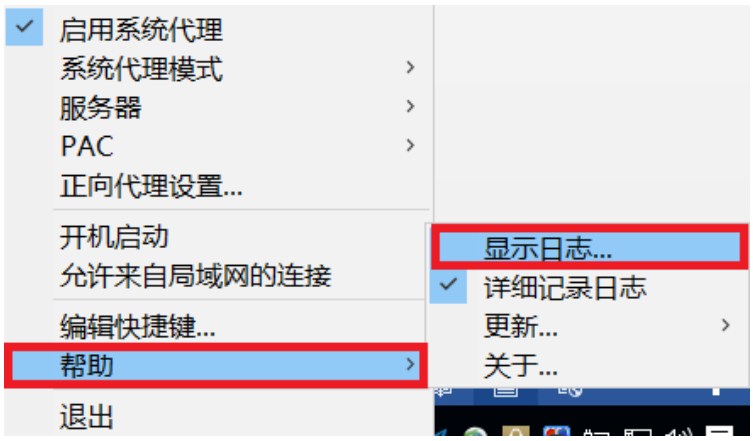


图 13-5 显示日志窗口

此时会弹出“日志查看器”窗口，如下图 13-6 所示。

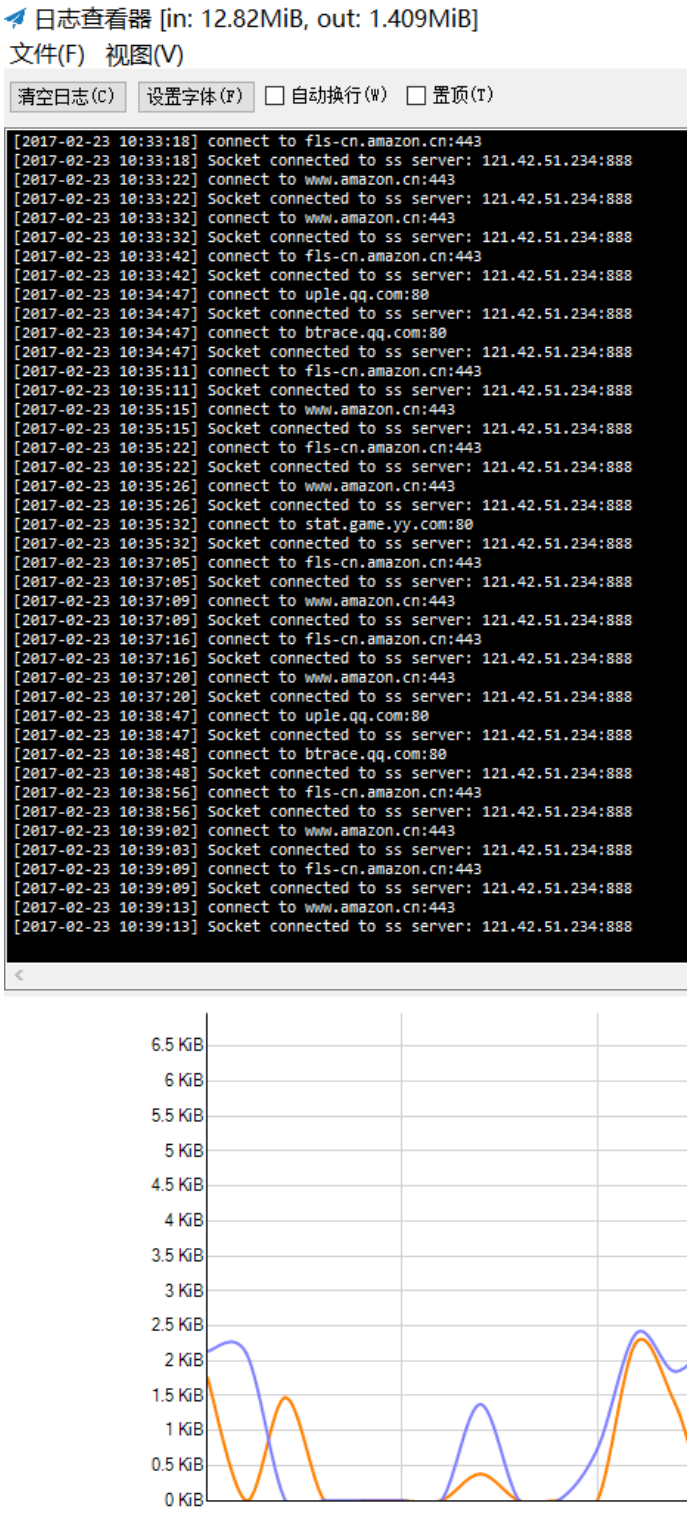
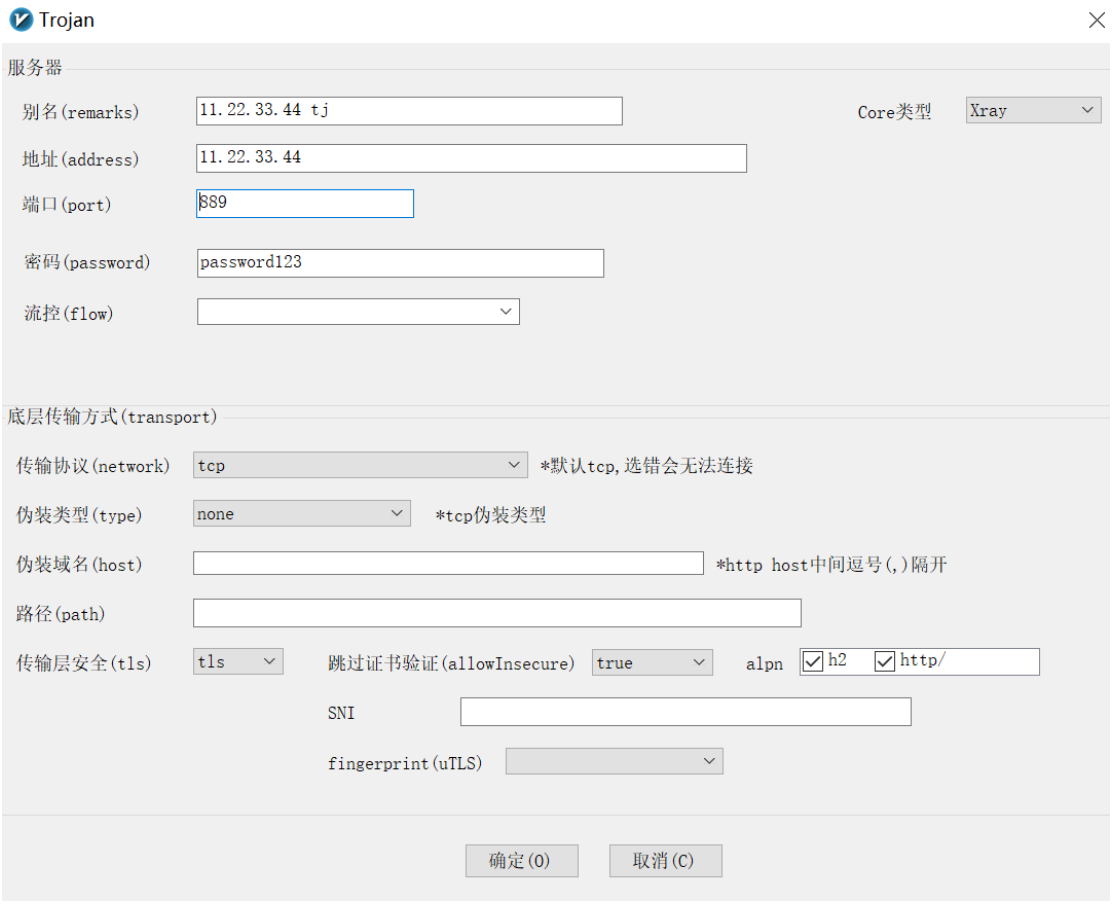


图 13-6 日志查看器窗口

当需要关闭 SS 代理功能时，可以右键点击任务栏上的 SS 程序图标，在弹出的主菜单中选择 “启用系统代理”项，使其不再处于勾选状态，此时任务栏的 SS 程序图标会变成浅灰色。

V2rayN 配置 TJ 的界面：



13.2 Android 系统下设置 SS 客户端

安卓系统安装使用 SS 示例

http://www.trustcomputing.com.cn/help/cn/dadi/ss/android_ss.html

SS 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=com.github.shadowsocks

1）安装软件

下载 SS 客户端软件，安装后，点击桌面的 SS 程序图符，如图 13-7 所示，运行 SS 客户端软件，如图 13-8 所示。

图 13-7 桌面上的 SS 安卓客户端软件

2）新建 SS 连接

图 13-8 SS 安卓客户端软件主界面

依次输入各项内容，其中“远程 DNS”的内容要根据是服务器在国内还是国外，使用不同的 DNS 服务器。

3）连接服务器

返回 SS 安卓客户端软件主界面，点击右上角的“纸飞机”按钮，如果一切正常，就可以连接成功了，如图 13-9 所示。

图 13-9 SS 安卓客户端软件连接成功

连接状态下，点击右上角的“纸飞机”按钮，可以关闭 SS 连接。

为了在重新打开系统时 VPN 不中断，需要：

1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

13.3 iOS 系统下设置 SS 客户端

iOS 系统安装及使用 SS 示例

http://www.trustcomputing.com.cn/help/cn/dadi/ss/ios_ss.html

SS iOS 客户端软件下载链接

https://apps.apple.com/us/app/wingy-http-s-socks5-proxy-utility/id1178584911

下载 SS iOS 客户端软件，安装后，点击桌面的 SS iOS 客户端程序图符，运行 SS iOS 客户端软件，如图 13-10 所示。

图 13-10 桌面上的 SS iOS 客户端软件图标

具体设置过程如图 13-11-1、2、3、4、5、6、7 所示。

图 13-11-1

图 13-11-2

图 13-11-3

图 13-11-4

图 13-11-5

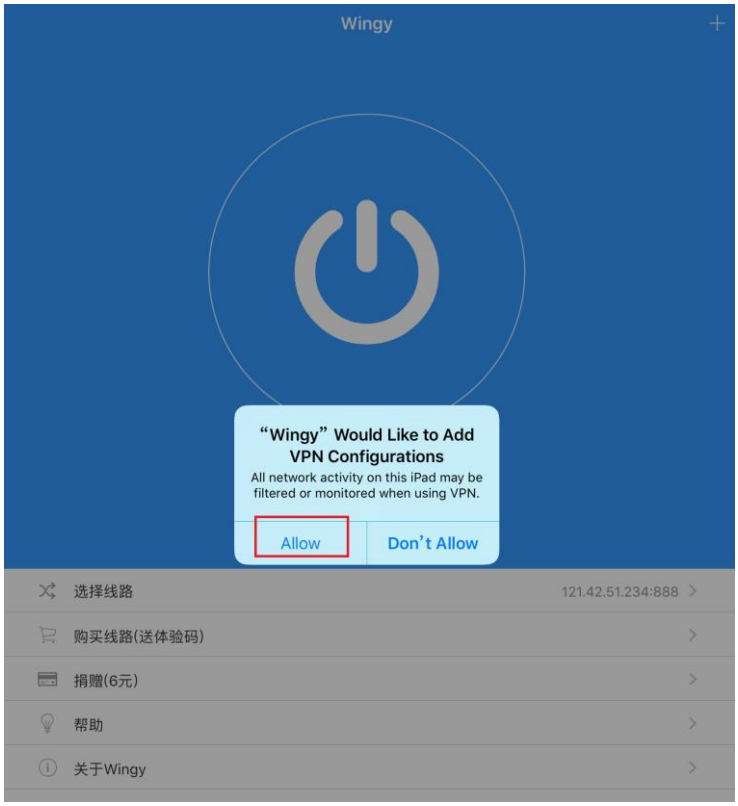


图 13-11-6

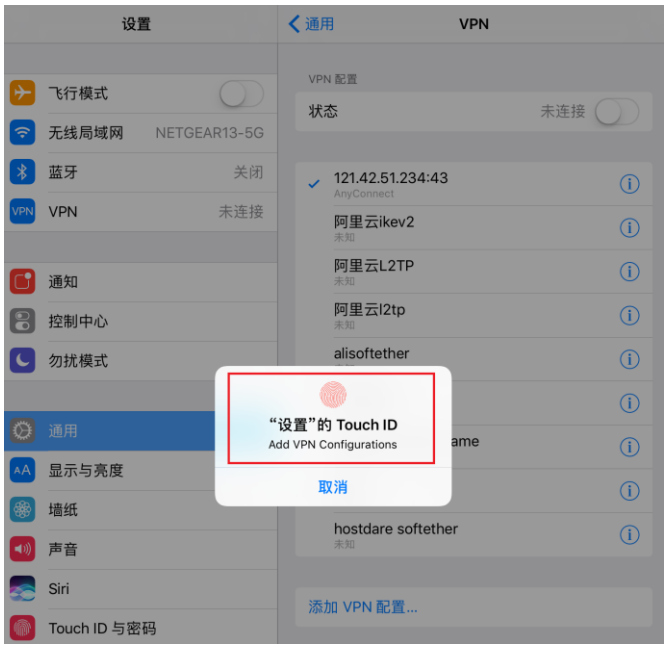


图 13-11-7

图 13-11-8

图 13-11 iOS 系统下 SS 客户端软件界面

iOS 系统下 SS 客户端软件具体设置过程描述如下：

1）点击下方的“选择线路”项，在新窗口中点击“新增线路”项，在“选择类型”窗口中选择“ShadowSocks（R）项”；

2）在“添加线路”窗口中输入服务器地址、端口、密码，选择代理模式为“全局代理”项，再选择“加密方式”，最后点击右上角“保存”按钮；

3）返回主界面，点击上方的“开关”按钮，第一次运行时，系统会弹出一个的警告窗口，点击左边的“Allow”按钮，在下一个窗口时用指纹验证通过；

4）连通后，点击主界面的“开关”按钮，退出 VPN 连接。由于 SS 并非传统意义上的 VPN，所以在 iOS 的“设置>VPN”界面中显示的服务器 IP 等信息不准

确，请忽略之。

13.4 通过 SS 客户端的 Socks 代理连接

当网络中已经有 SS 客户端运行时，其他程序可以通过连接其 Socks 代理间接使用 SS 服务器，例如：Windows 下可以启用 SS 客户端软件的“允许来自局域网的连接”选项，让无线局域网中的手机、平板等设备通过 Windows 下的 SS 客户端软件上网，如下图 13-12 所示。同时，Windows 还需要关闭 PC 防火墙或设置连接例外。

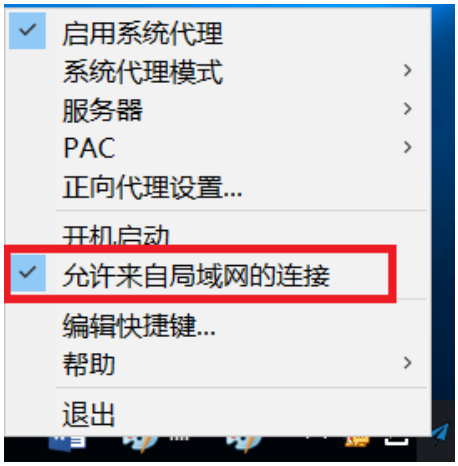


图 13-12 Windows SS 客户端软件允许来自局域网的连接

Windows 系统客户端设置 Socks 代理请参见“**4.1.2 Windows 系统设置 Socks 代理**”，安卓系统客户端设置 Socks 代理请参见“**4.2.2 安卓系统设置 Socks 代理**”，iOS 系统客户端设置 Socks 代理参见“**4.3.2 iOS 系统设置 Socks 代理**”。

14 SSH 客户端设置

本系统不提供基于 SSH 的 SHELL，只提供端口转发/端口代理、SFTP 等加密传输服务功能，OpenVZ 服务器系统没有 SFTP 服务。使用 SFTP 时，不能在根目录创建新文件，只能在二级子目录下创建新文件，可以编辑根目录下已有的文件，缺省磁盘空间是 10M。如果 10 分钟内累计三次输入错误的口令，则可能被系统屏蔽 10 小时。

14.1 Windows 系统下设置 SSH 客户端

Windows 系统下 SSH 客户端设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/ssh/windows_ssh.html

Windows 下有很多 SSH 端口转发/端口代理的软件，例如：Bitvise SSH Client (Tunnelier)、PuTTY（plink）等，SFTP 文件传输工具有 WinSCP、CuteFTP 等，基于 SSH/SFTP 的文件同步工具有 WinSCP 等，基于 SSH/SFTP 的文件系统工具有 nsoftware 的 Sftp Drive、RaiDrive、AirLiveDrive、WinFsp/SSHFS、WinSshFS，登陆 SFTP 服务器直接编辑文件的工具有 UltraEdit。

以下以 SecureCRT 软件为例，说明 SSH 客户端端口转发/端口代理的设置。

参考：https://www.vandyke.com/support/tips/socksproxy.html

1）点击左下角“快速新建”图标，弹出“快速新建”窗口，输入 SSH 服务器的 IP 地址或域名、端口以及 SSH 用户名，再点击“Connect”按钮，如图 14-1 所示；

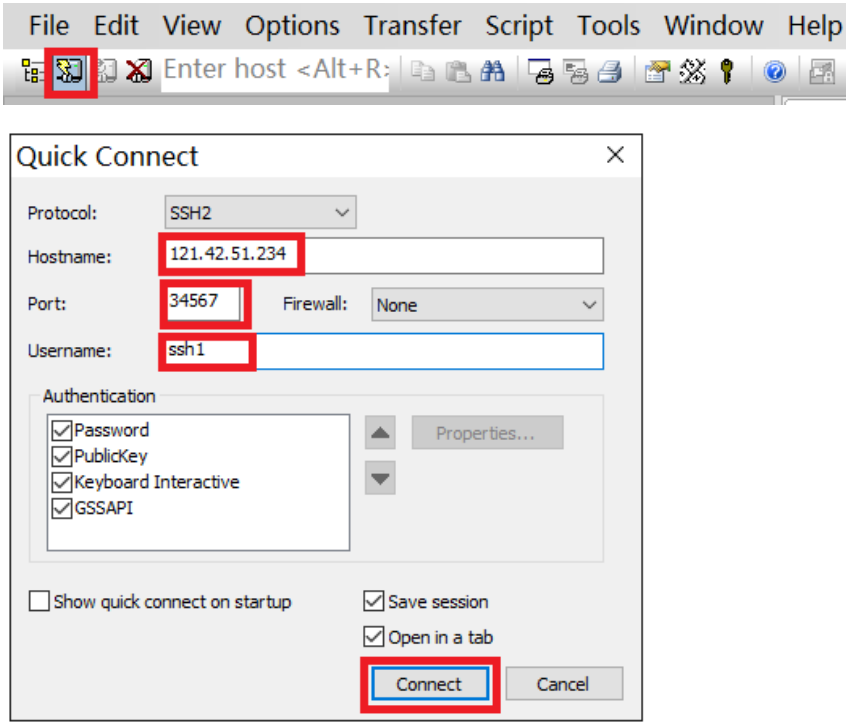


图 4-1 快速新建 SSH 连接窗口

2）在弹出的“输入 SSH 密码”窗口中输入密码，并勾选“Save password”选项，最后点击“OK”按钮，如图 14-2 所示；

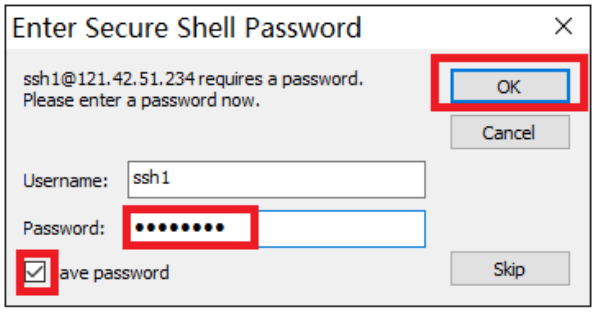
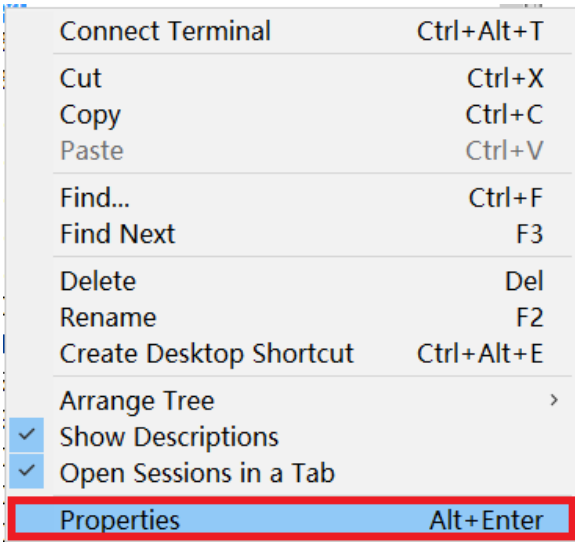


图 14-2 输入 SSH 密码窗口

3）首次连接一般不成功，需要继续修改。

在左边窗口中找到刚才新建的项目，在其上点击右键，在右键菜单中选择最后一项“Properties”。为确保 SSH 连接不中断，需要设置会话选项，点击左边的“Terminal”项 ，在其右侧的界面中，勾选“Auto reconnect”选项，以及“Send protocol NO-OP” 选项，并点击“OK”按钮，如图 14-3-1 所示；



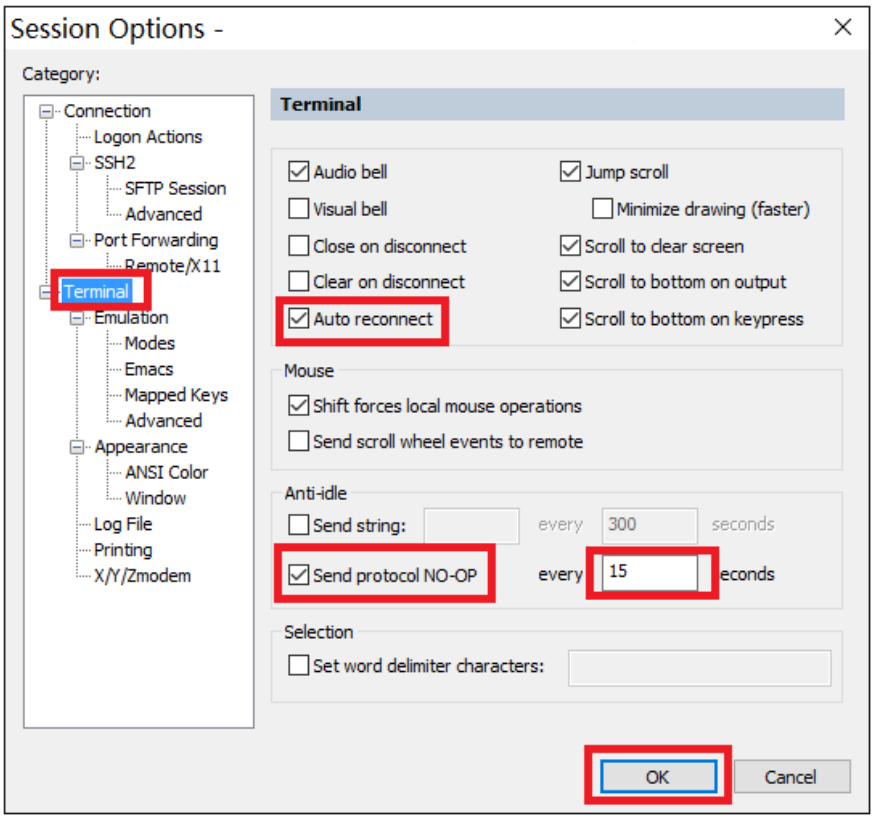


图 14-3-1 设置会话选项

4）在弹出的属性窗口中，点击“Port Forwarding”项，在其右侧的界面中，勾选“Do not request a shell”选项，并点击“Add”按钮，如图 14-3-2 所示；

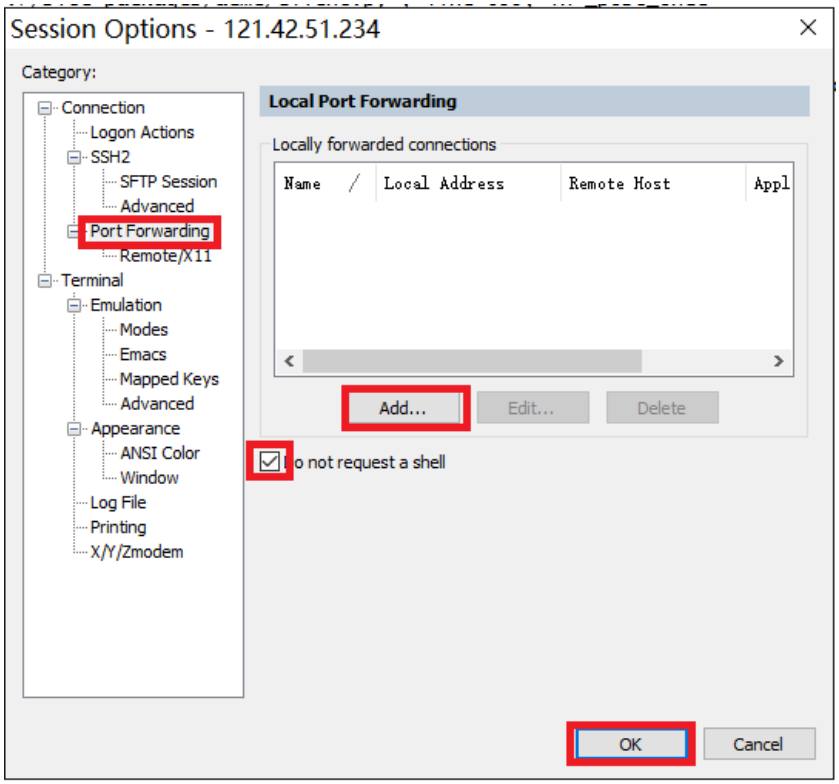


图 14-3-2 修改 SSH 连接属性

5）在弹出的本地端口映射窗口中，有两种设置方法：

（1）设置成 SOCKS 代理，如图 14-4-1 所示。

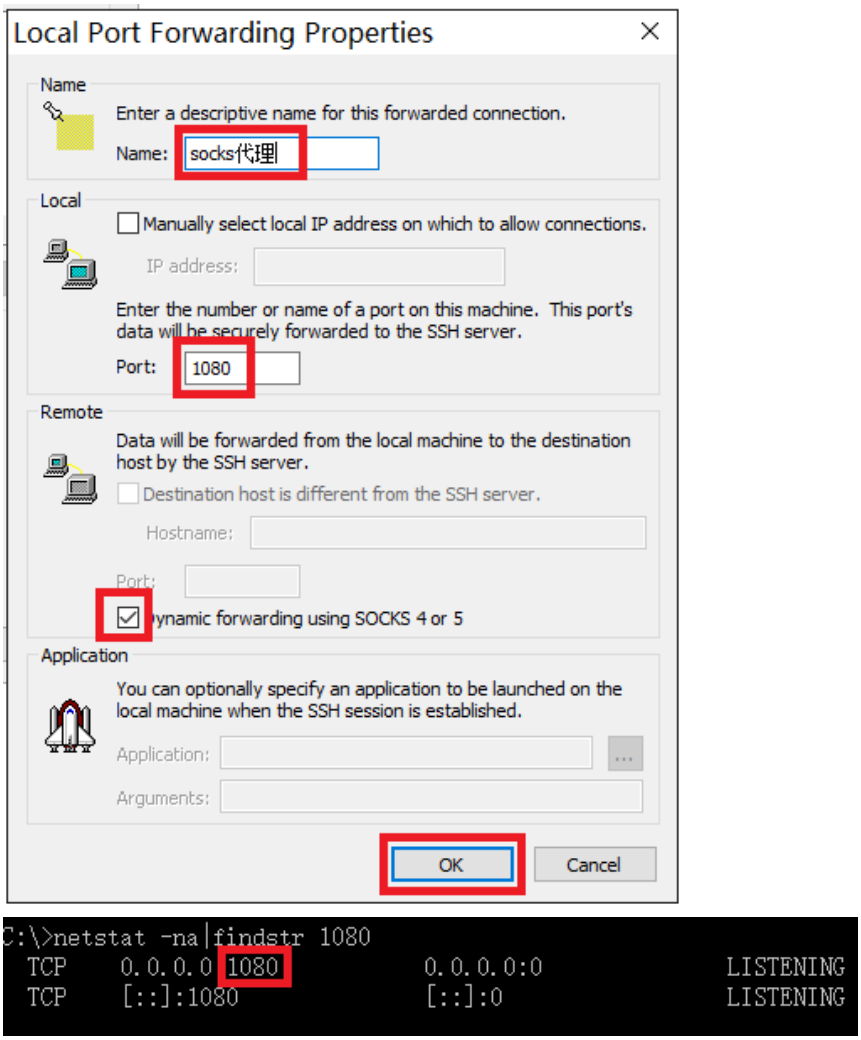
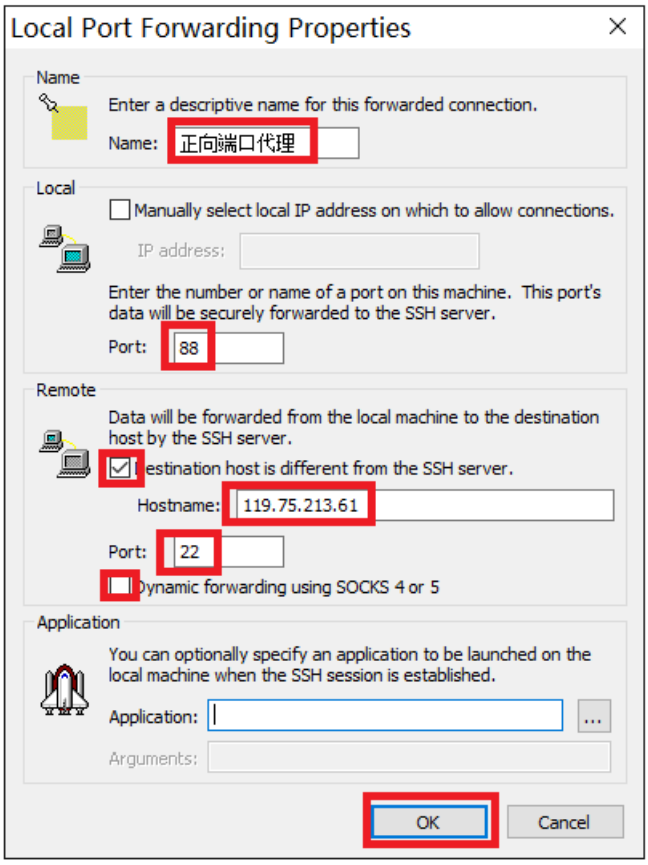


图 14-4-1 设置 SOCKS 动态代理

保存后，双击左边的项目，SSH 连接成功后，会在本地监听所设置的端口（netstat -nao|findstr 1080），其它软件可将该端口作为 SOCKS5 代理服务端口使用，SOCKS5 代理服务器 IP 是 127.0.0.1，具体使用参见 **4.1.2 Windows 系统设置 Socks 代理**

（2）设置成正向端口代理，如图 14-4-2 所示。



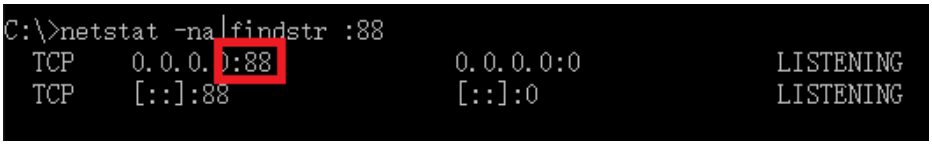


图 14-4-2 设置正向端口代理

保存后，双击左边的项目，SSH 连接成功后，会在本地监听所设置的端口（netstat -nao|findstr 88），当连接本地该端口时，将使得 SSH 服务器连接远端服务器及端口（本机连接 127.0.0.1:88 => 119.75.213.61:22）。

6）还可以设置成反向端口代理，或远程端口代理：

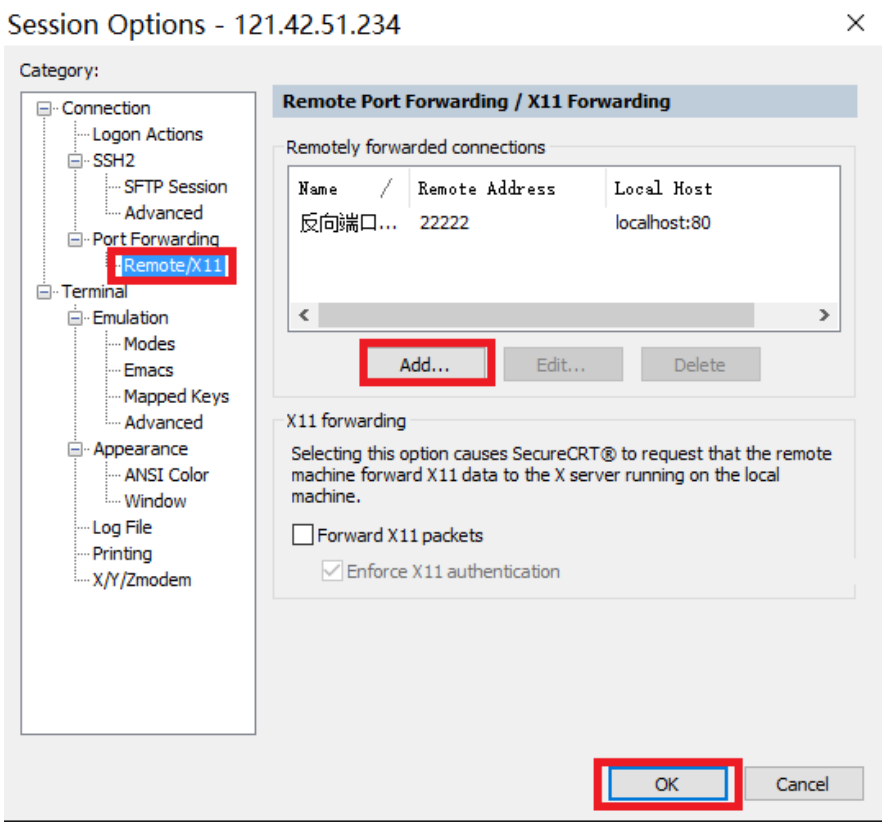


图 14-5-1 设置反向端口代理

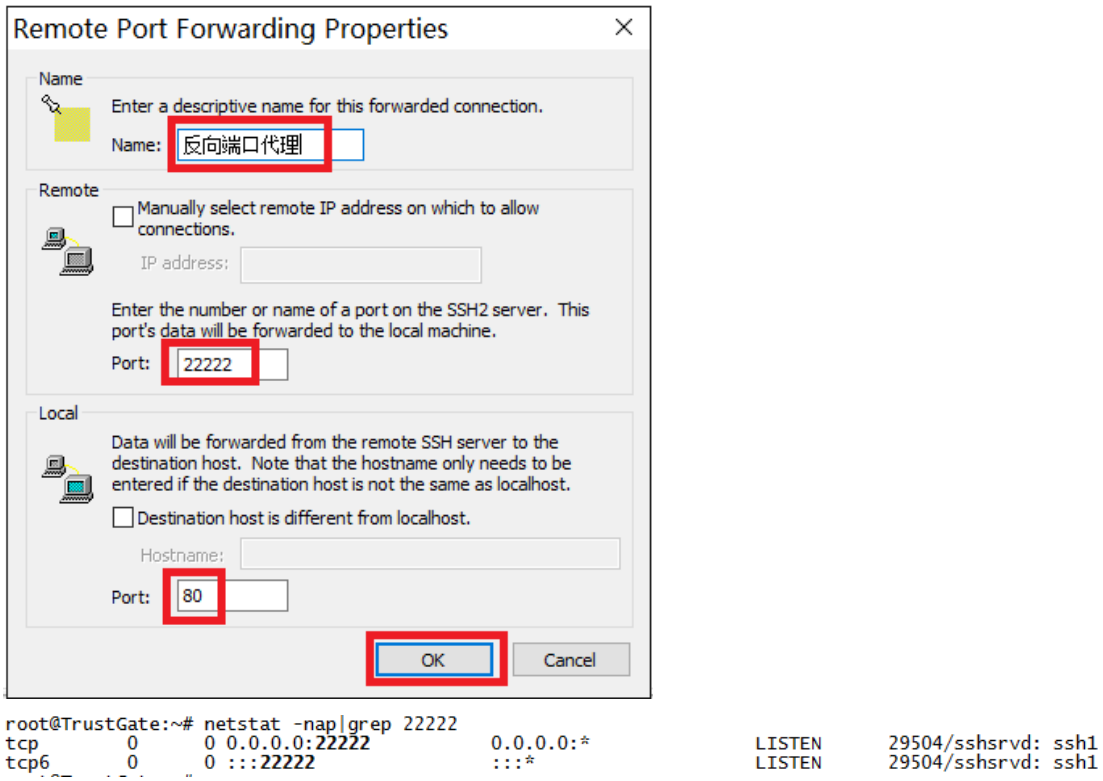


图 14-5-2 设置反向端口代理

在左边窗口中找到刚才新建的项目，在其上点击右键，在右键菜单中选择最后一项“Properties”。在弹出的属性窗口中，点击“Port Forwarding”项，清除其右侧界面中已有的内容，勾选“Do not request a shell”选项，再点击其下的“Remote/X11”子项，并点击“Add”按钮，如图 13-5-1 所示；填写远端端口（22222），必须大于 1024，缺省是 6001~7001，填写本地应用端口（80），缺省应用服务器是 127.0.0.1，如果应用服务器是其它 IP，则勾选“Destination host is different from localhost”项，并在“Hostname”栏中填写其它 IP，如图 14-2 所示。多个端口需要多次添加单个端口。

保存后，双击左边的项目，SSH 连接成功后，会在 SSH 服务器上监听所设置的端口（netstat -nap|grep 22222）。

之后根据 SSH 客户端软件/系统的不同有不同的限制，有的（SecureCRT）只能从 SSH 服务器上连接该端口（127.0.0.1:22222），进而连接到 SSH 客户端的本地端口（80），有的（Linux SSH 客户端）允许从任何地方连接该端口（远端连接 http:// 121.42.51.234:22222 => 本机 http:// 127.0.0.1:80）。SSH 客户端的主机防火墙不需要关闭，因为在 SSH 客户端 OS 看来，源 IP 是本地 127.0.0.1。

对于 SecureCRT 缺省只能从 SSH 服务器上连接反向端口代理端口，如果需要其它 IP 也能连接，需要手工修改 ini 配置文件，打开目录“C:\Users\userxxx\AppData\Roaming\VanDyke\Config\Sessions”，找到保存的 xxx.ini 文件，打开该文件，查找“Reverse Forward Filter”行，缺省是：

S:"Reverse Forward Filter"=allow,127.0.0.1,0 deny,0.0.0.0/0.0.0.0,0

改成 允许某个网段连接：

S:"Reverse Forward Filter"=allow,59.171.23.0/255.255.255.0,0

或 允许全部 IP 连接：

S:"Reverse Forward Filter"=allow,0.0.0.0/0.0.0.0,0

保存文件后，断开已有连接，再重新打开该连接，再测试。

如果连接不成功，可以查看 SSH 服务器所在 OS 的/var/log/messages 或 syslog 文件，如果出现“channel 2: open failed: administratively

prohibited: Rejecting remote forward request from 59.171.23.185:42456 to 127.0.0.1:8080 because the current filters do not allow 59.171.23.185:42456 to use the remote forward. [postauth]”的信息，则表明“Reverse Forward Filter”设置不成功，没有出现，则表明成功。

为了测试方便，可以运行 uTorrent 软件，打开“网页界面”功能，具体步骤是主菜单“选项”>“设置”，点击左边“高级>网页界面”，勾选右边“启用网页界面”，填写“用户”、“密码”、“备用监听端口”“8080”，在“只允许下列 IP 访问”中填写“127.0.0.1”，如图 14-5-3 所示。最后在浏览器地址栏中输入： http://47.110.70.85:6003/gui/ 这样的 URL 测试。

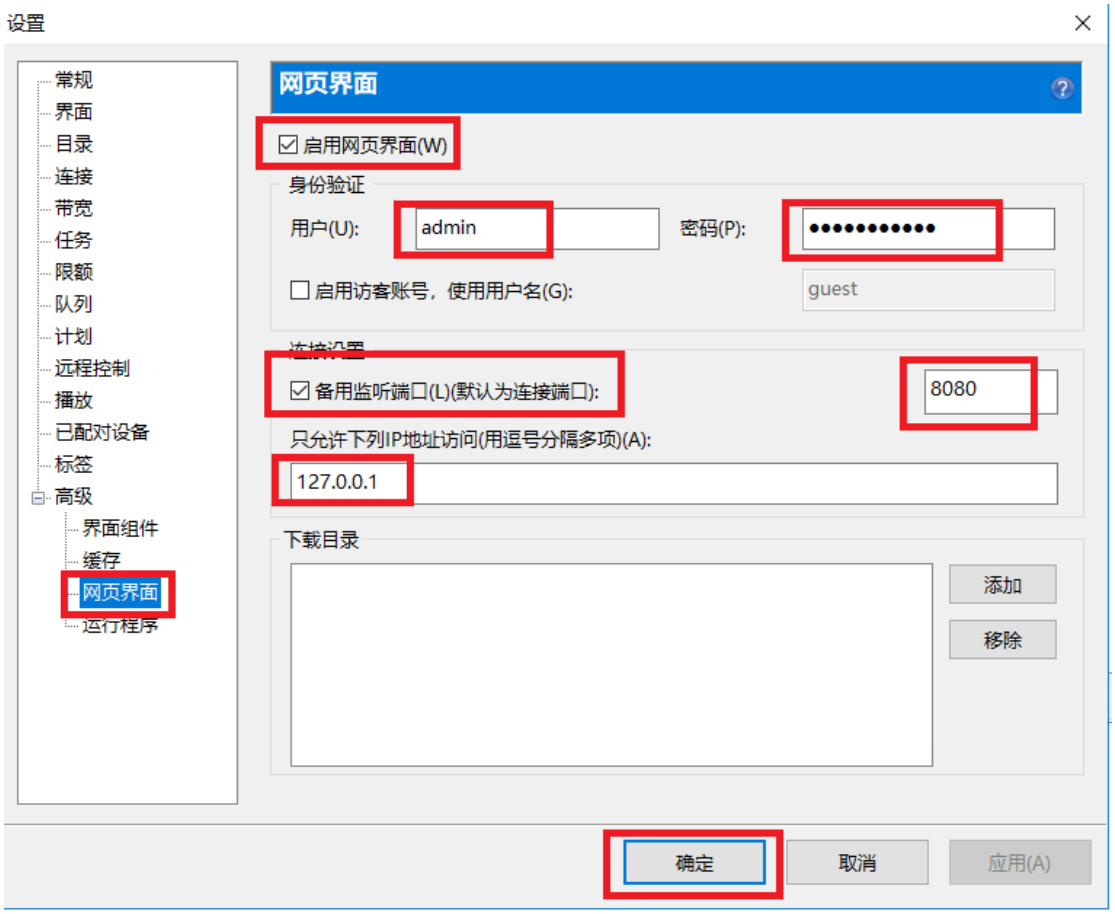
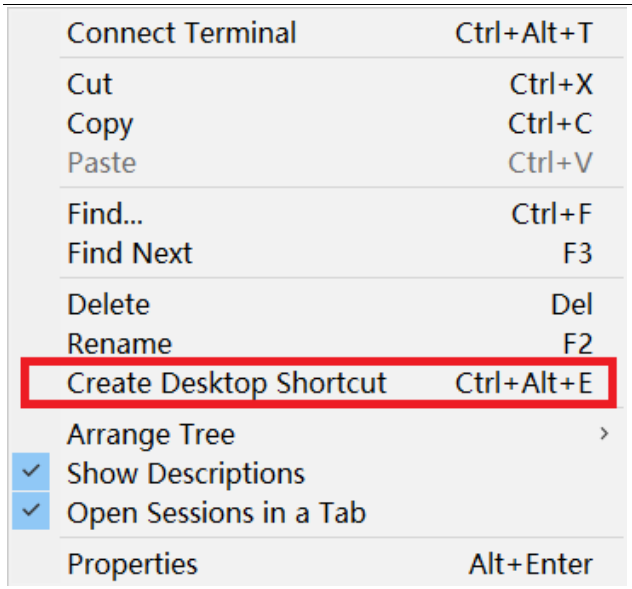


图 14-5-3 设置测试用的 utorrent 网页界面

也可以将本地 Socks 代理（127.0.0.1:8080）、远程桌面（127.0.0.1:3389）映射到外网做测试。

7）随机自启动设置：


Connect Terminal Ctrl+Alt+T
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Find... Ctrl+F
Find Next F3
Delete Del
Rename F2
Create Desktop Shortcut Ctrl+Alt+E
Arrange Tree
Show Descriptions
Open Sessions in a Tab
Properties Alt+Enter

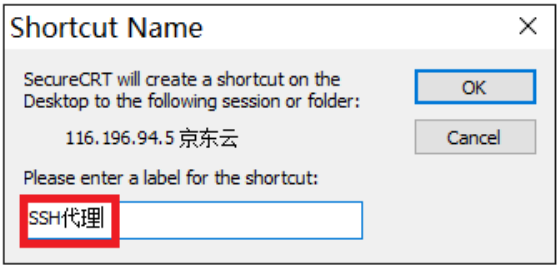

Shortcut Name
SecureCRT will create a shortcut on the Desktop to the following session or folder:
116.196.94.5 京东云
OK
Cancel
Please enter a label for the shortcut:
SSH代理

图 14-5-4 创建桌面快捷方式-设置随机自启动

在左边窗口中找到刚才新建的项目，在其上点击右键，在右键菜单中选择 “Create Desktop Shortcut”项，在弹出的窗口中输入名称，点击“确定”按钮后，在桌面找到该快捷方式，在其上点击右键，在右键菜单中选择 “属性”项，在弹出的窗口中将“运行方式”改成“最小化”，如图 14-5-4 所示。

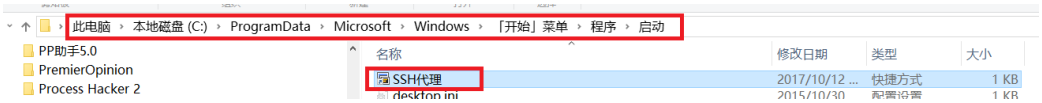


图 14-5-5 把桌面快捷方式放入“启动”程序组中-设置随机自启动

最后，在文件管理器中打开“启动”程序组目录，对于 Win10 是“C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp”目

录，将该快捷方式拖到此目录中完成操作，如图 14-5-5 所示。以后，用户 Windows 登陆后将自动最小化运行 SecureCRT，并启用该 SSH 代理。

另外，还可以使用 RaiDrive、AirLiveDrive、sshfs-win-manager 等软件通过 SSH 账号将远程磁盘资源安装为本地磁盘驱动器：

RaiDrive：https://www.raidrive.com/download

AirLiveDrive：https://www.airlivedrive.com/en/download/

WinFsp：https://github.com/billziss-gh/winfsp/releases

SSHFS：https://github.com/billziss-gh/sshfs-win/releases

sshfs-win-manager： https://github.com/evsar3/sshfs-win-manager/releases

14.2 安卓系统下设置 SSH 客户端

安卓系统 SSH 客户端设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/ssh/android_ssh.html

安卓系统下有很多 SSH 端口转发/端口代理的软件，例如：ConnectBot、JuiceSSH 等，SFTP 文件传输工具有 AndFTP、FTPCafe 等，基于 SFTP 的文件同步工具有 FolderSync 等。另外，还有基于 SSH 的系统代理程序，例如： Postern。

以下以 ConnectBot APP 程序为例，说明安卓系统下 SSH 客户端端口转发/端口代理的设置：

- ConnectBot 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=org.connectbot

- FolderSync lite 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=dk.tacit.android.foldersync.lite

- Postern 安卓客户端软件下载链接

https://play.google.com/store/apps/details?id=com.tunnelworkshop.postern

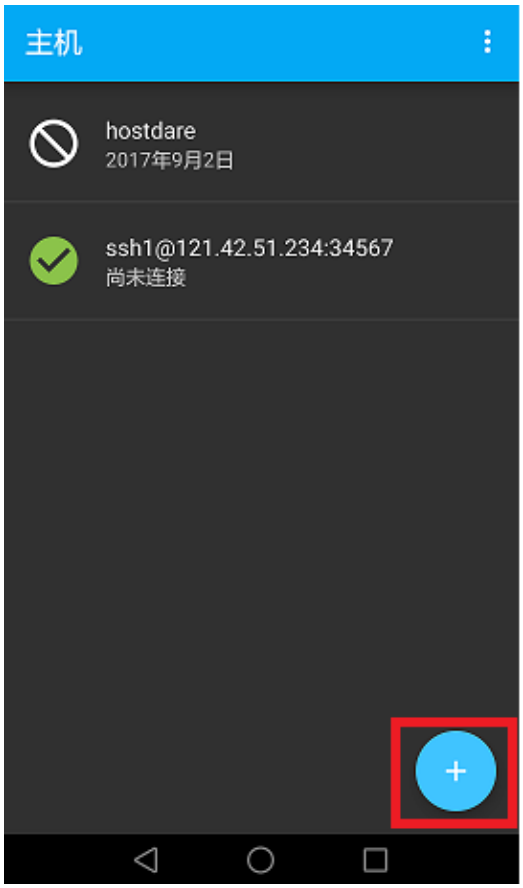


图 14-6-1 新建连接

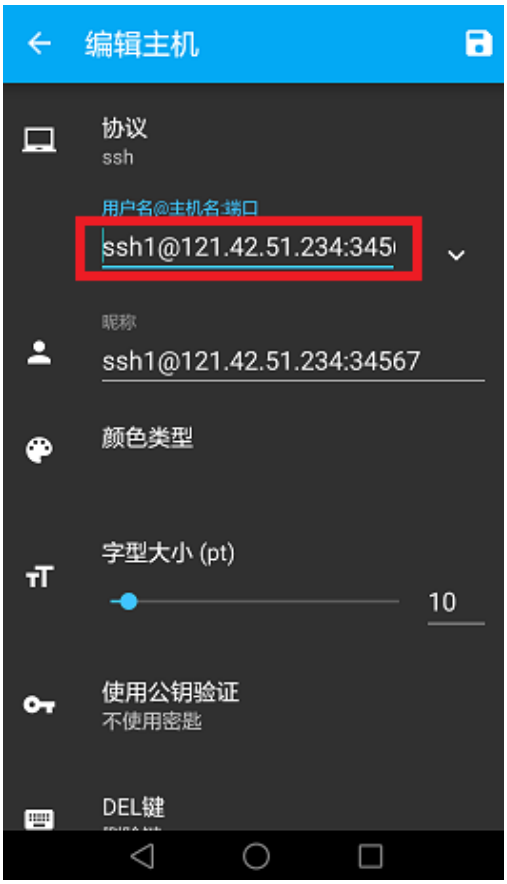


图 14-6-2 输入用户名主机名端口

图 14-6-3 禁用“开始 Shell 会话”

图 14-6-4 编辑端口转发

图 14-6-5 正向端口代理设置

图 14-6-6 反向端口代理设置

图 14-6-7 SOCKS 代理设置

图 14-6-8 输入密码登陆

图 14-6-9 X-plore 显示无线文件共享

图 14-6-10 X-plore 启用无线网络服务

1）点击主界面右下角的+号图符，开始新建 SSH 连接；

2）输入用户名、主机名、端口，类似 ssh1@121.42.51.234:34567 这样；

3）往下拉菜单，关闭“开始 Shell 会话”选项，并保存；

4）返回主界面后，右键点击刚才新建的项目，选择“编辑端口转发”；

5）正向端口代理设置，转发类型：本地，“源端口”必须大于 1024；SSH 连接建立后，在本机连接本机的“源端口”，进而使 SSH 服务器所在主机连接“目标端口”（本机连接 http://127.0.0.1:8866 => http://114.115.136.7:80）；

6）反向端口代理设置，转发类型：远端，“源端口”必须大于 1024；SSH 连接建立后，从任意地方连接 SSH 服务器所在主机的“源端口”，进而会连接到本机的“目标端口”（远端连接 http:// 121.42.51.234:33333 => 本机 http:// 127.0.0.1:80）；

7）SOCKS 代理设置，转发类型：动态套接字（SOCKS），“源端口”必须大于 1024；SSH 连接建立后，在本机连接本机的“源端口”作为 SOCKS 代理服务端口，进而连接任意目的地址，参考**“4.2.2 安卓系统设置 Socks 代理”**；

8）返回主界面后，右键点击刚才新建的项目，输入密码，建立 SSH 连接；

9）为了从外部连接进安卓系统，可以安装使用 X-plore、KSWEB 等 App 程序；对于 X-plore，首先要选择显示“无线文件共享”；

10）再启用“无线网络服务”，这样就可以通过 http://IP:1111 这样的 URL 连接到安卓系统，下载上传文件，再配合 ConnectBot 的反向端口代理，就可以从任意地方连接进安卓系统；

11）为了在重新打开系统时 SSH 不中断，需要：

（1）在“电池”设置中，启用“休眠时始终保持网络连接”选项；

（2）手机管家--应用启动管理--找到应用，不让它自动管理，选择允许后台运行；

（3）下拉手机顶部状态栏，找到应用，点击“ACQUIRE WAKELOCK”，即可看到 1 session(wake lock help)。此时，应用就可以保持后台运行，锁屏也不会关闭。

14.3 iOS 系统下设置 SSH 客户端

iOS 系统 SSH 客户端设置示例

http://www.trustcomputing.com.cn/help/cn/dadi/ssh/ios_ssh.html

iOS 系统下有很多 SSH 端口转发/端口代理的软件，例如：Termius（Port Forwarding 功能）、vSSH 等，SFTP 文件传输工具有 FTP Manager、File Manager 等，挂载 SFTP 目录的有 FileExplorer 、Documents by Readdle（可 SFTP 上传）等，基于 SFTP 的文件同步工具有 GoodSync、Transmit 等。

以下以 vSSH lite APP 程序为例，说明 iOS 系统下 SSH 客户端端口转发/端口代理的设置：

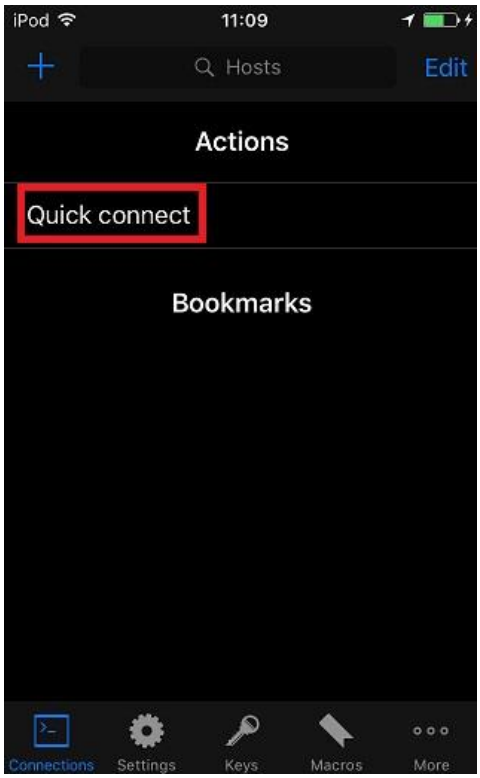


图 14-7-1 新建连接

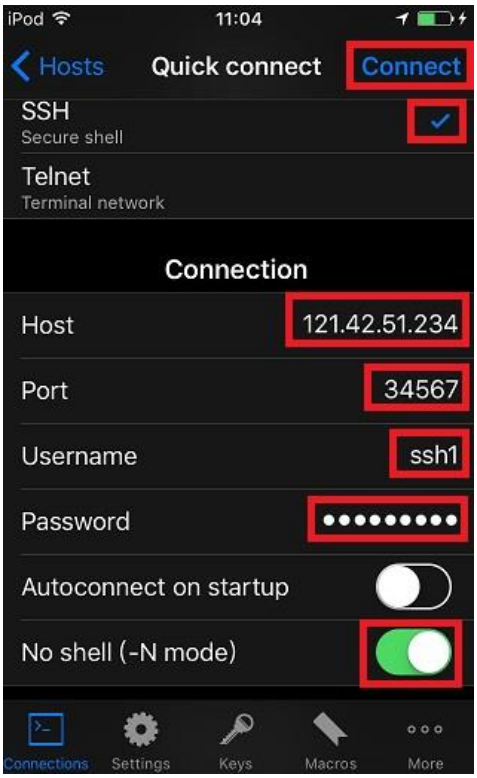


图 14-7-2 输入主机名端口用户名密码

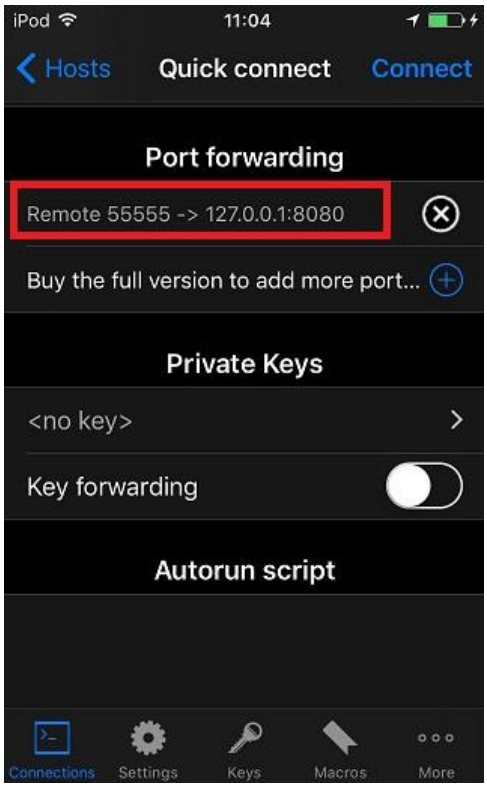


图 14-7-3 新建端口转发

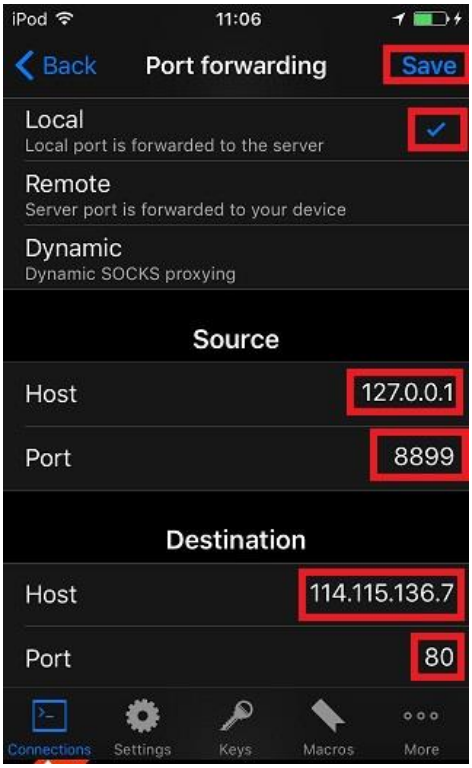


图 14-7-4 正向端口代理设置

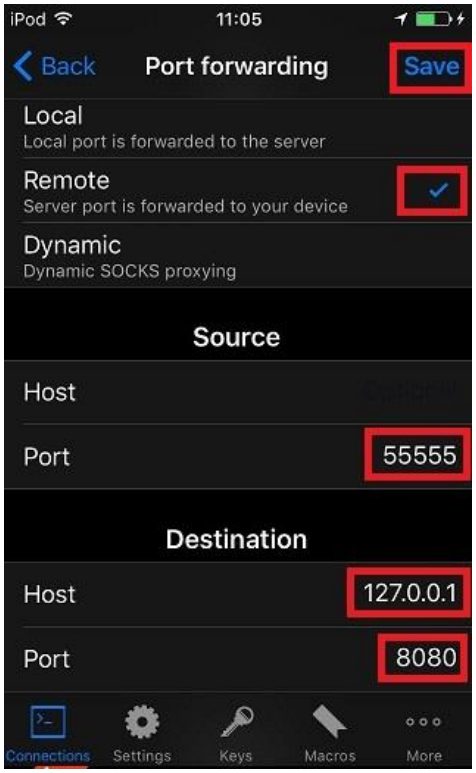


图 14-7-5 反向端口代理设置

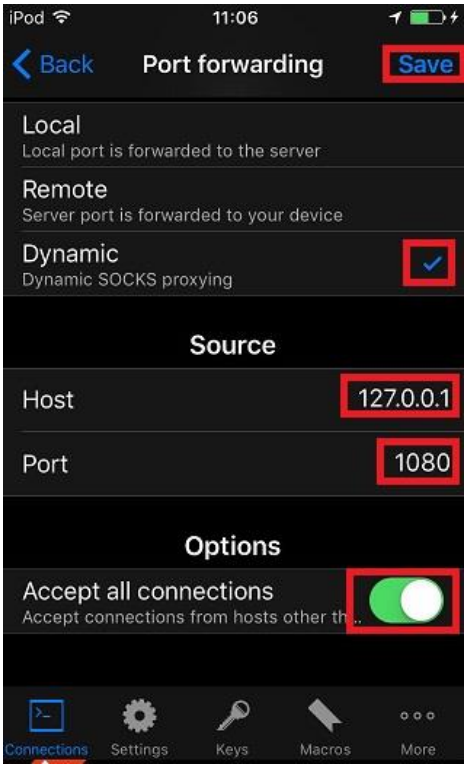


图 14-7-6 SOCKS 代理设置

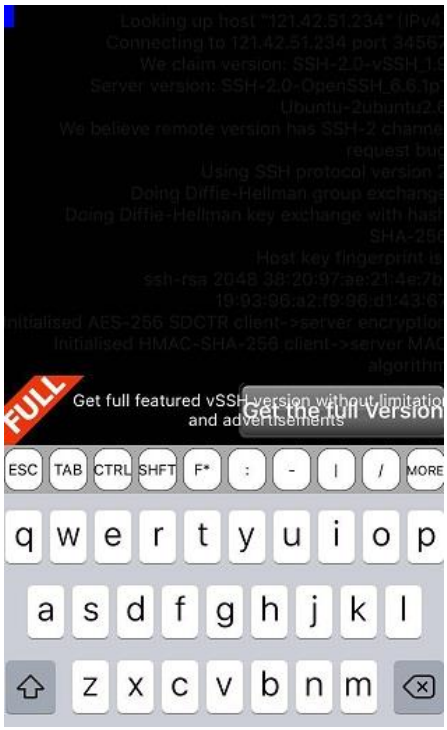


图 14-7-7 连接成功

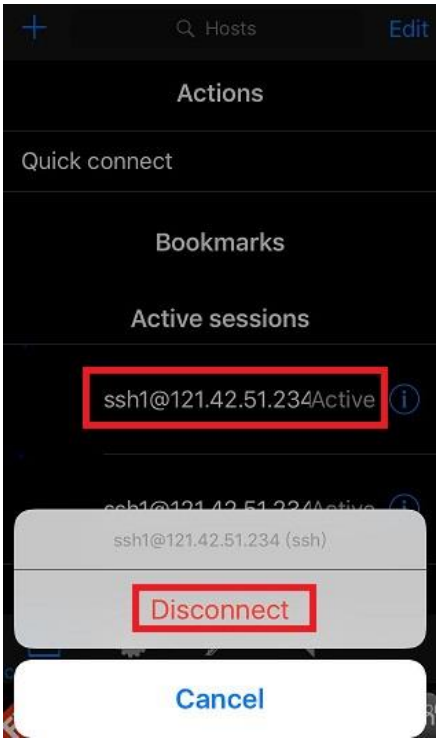


图 14-7-8 断开连接

图 14-7-9 AirDoc 中打开 WebSharing

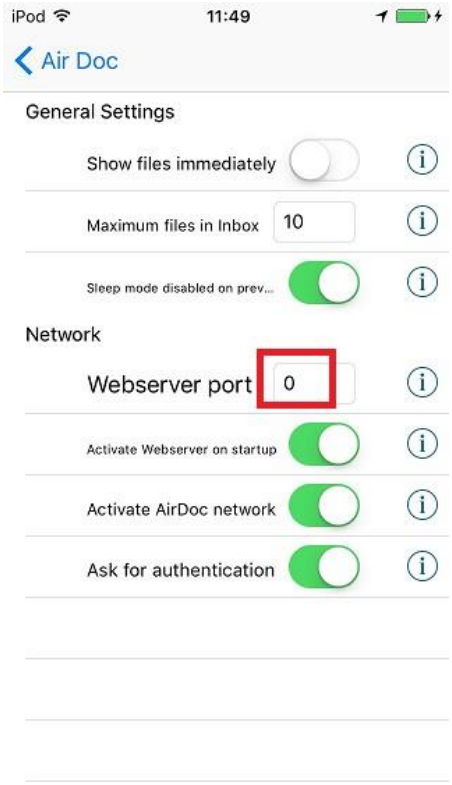


图 14-7-10 AirDoc 监听端口设置

1）点击主界面“Quick Connect”按钮，开始新建 SSH 连接；

2）输入主机名、端口、用户名、密码，启用“No shell”选项；

3）往下拉菜单，点击“Port forwarding”项右边的+号，新建端口转发；

4）正向端口代理设置，转发类型：Local（本地），“Source Port（源端口）”必须大于 1024，按右上角“Save”按钮保存；SSH 连接建立后，在本机连接本机的“Source Port（源端口）”，进而使 SSH 服务器所在主机连接“Destination Port（目标端口）”（本机连接 http://127.0.0.1:8899 => http://114.115.136.7:80）；

5）反向端口代理设置，转发类型：Remote（远端），“Source Port（源端口）”必须大于 1024，按右上角“Save”按钮保存；SSH 连接建立后，从任意地方连接 SSH 服务器所在主机的“Source Port（源端口）”，进而会连接到本机的“Destination Port（目标端口）”（远端连接 http:// 121.42.51.234:55555 => 本机 http:// 127.0.0.1:8080）；

6）SOCKS 代理设置，转发类型：Dynamic（SOCKS 代理），“Source Port（源端口）”必须大于 1024，按右上角“Save”按钮保存；SSH 连接建立后，在本机连接本机的“Source Port（源端口）”作为 SOCKS 代理服务端口，进而连接任意目的地址，参考“**3.3.2 iOS 系统设置 Socks 代理**”；

7）返回主界面后，点击刚才新建的项目，建立 SSH 连接；

8）返回主界面后，在“Active Sessions”栏目下，右键点击已经建立的 SSH 连接，选择“Disconnect”按钮断开；

9）为了从外部连接进安卓系统，可以安装使用 Air Doc、Hidisk 等 App 程序；对于 Air Doc，打开“Web Sharing”开关，这样就可以通过 http://IP:80 这样的 URL 连接到 iOS 系统，下载上传文件，再配合 vssh 的反向端口代理，就可以从任意地方连接进 iOS 系统；

10）对于 Air Doc，可以设置“Web Sharing”监听的端口，缺省是 80。

15 用户自服务门户

15.1 WEB 用户门户

WEB 用户门户使用示例

http://www.trustcomputing.com.cn/help/cn/dadi/user/userportal.html

注意：由于公众版本许可证的限制，只有 PPTP 用户才能够登录用户门户。

1、用户登录

WEB 用户门户的 URL 是“https://主机名/my”，登录账号、口令就是 WEB、WEB 代理、VPN、SSH 等具体服务的登录账号、口令。如果主机名是 IP 或没有 SSL 证书的域名，用户需要先下载安装 CA 证书，URL 是“http://外网 IP:HTTP 端口/myca.crt”，下载时需要输入用户名和（初始）密码，安装证书的“存储位置”是“本地计算机”，证书存储到“受信任的根证书颁发机构”，具体参见“导入 CA 证书（**2.2**）”。

首次登录强制修改口令，如图 15-1 所示；如果 10 分钟内累计三次输入错误的口令，则可能被系统屏蔽 10 分钟。退出登录需要关闭整个浏览器，或者通过 Chrome 浏览器的“打开新的无痕窗口”功能切换用户。

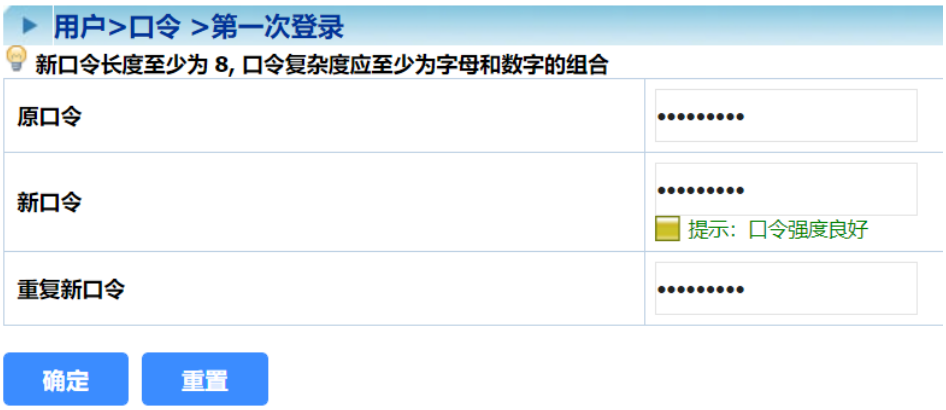


图 15-1 WEB 用户门户-首次登录强制修改口令

2、用户信息

在“信息”栏可以查看登录账号、用户姓名、用户组、用户状态、用户 URL、有效期、时间控制及状态、流量统计、绑定 VPN IP、WEB 登录 IP，如图 15-2 所示。用户 URL 是指 VPN 用户登录后，WEB 服务器提供的外网 URL，可以映射到 VPN 客户端虚拟 IP 的 WEB 服务器；或者是 SSH/SFTP 用户上传文件的根目录。

图 15-2 WEB 用户门户-用户信息

3、用户资源

“资源”栏可以查看用户可用资源，主要有 VPN/SSH 服务器、DNS 服务器、WEB 代理服务器、WEB 在线代理、WebDAV 服务、源 IP 显示、DDNS 在线更新、SFTP 在线客户端等，如图 15-3 所示，URL 有 http 和 https 两种，端口有标准端口和非标准端口两种，IP 有 IPV4 和 IPV6 两种。

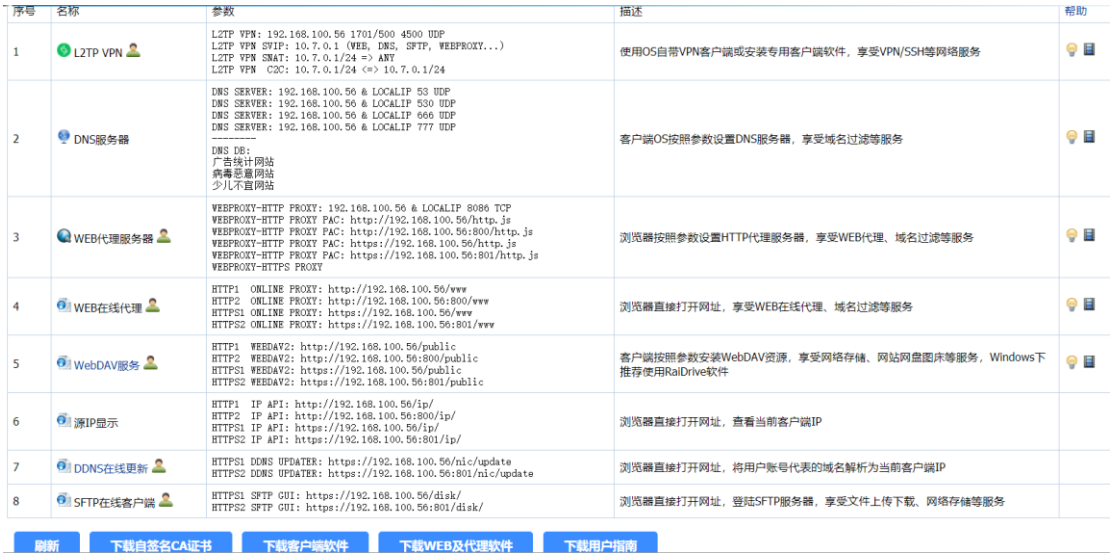


图 15-3 WEB 用户门户-用户资源

具体内容有：

1）“名称”列有图符的，表明需要用户认证；

2）非 SSH 用户，点击“WebDAV 服务”链接，可以下载用户通过 WebDAV 上传的文件形成的 URL；

3）非 SSH 用户且用户名是域名形式的，点击“DDNS 在线更新”链接，可以下载 DDNS 客户端配置文件；

4）PPTP 用户，同时显示可用的 Softether、SSTP 服务器信息，但 Softether、SSTP 的用户认证是另外的；

5）OpenVPN 用户，点击“OpenVPN”链接，可以下载 OpenVPN 客户端配置文件——vpn.ovpn，需要和 vpn.auth 文件一起放到 config 子目录里；点击图符，可以下载 OpenVPN 客户端安装软件；

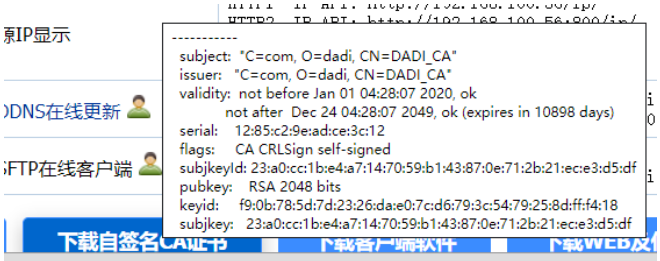
6）WireGuard VPN 用户，点击图符，可以下载 WireGuard VPN 客户端安装软件；点击“WireGuard VPN”链接，可以下载 WireGuard VPN 客户端配置文件——user_ip.conf，需要导入到 VPN 客户端软件里；点击图符，可以下载 WireGuard VPN 客户端 P2P VPN/Mesh VPN 配置文件，具体详见“9.1 Windows 系统下设置 WireGuard VPN 客户端”；

7）SSH 用户，点击“SSH/SFTP”链接，下载用户通过 SFTP 上传的文件形成的 URL；点击“SS”链接，下载 SS 客户端配置文件；同时显示可用的 Socks 代理信息，Socks 代理不需要用户认证；

8）“参数”列没有内容的，说明该服务停用；

9）点击“帮助”链接，下载本用户指南文件；点击“帮助”列图符，打开视频演示页面

10）鼠标移到下方“下载自签名 CA 证书”按钮上，显示当前系统（非客户端）自签名 CA 证书的有效期 validity 是否 ok，如下图所示



具体下载安装过程，参见“**导入 CA 证书（2.2）**”

具体资源显示的内容和客户端的设置详见文件《中神通大地云控客户端设置主图一览表》，下载链接是：

http://www.trustcomputing.com.cn/help/client_setup_list.docx

VPN 用户连接成功后获得的网络资源及前提条件，详见下表：

网络资源	虚拟网关的服务	虚拟内网的连接	SNAT 上外网
内容	VPN 用户以加密的形式连接虚拟网关即本系统的 DNS、WEB、WEBDAV、SSH/SFTP 服务器，HTTP、HTTPS、Socks 代理、WEB 在线代理、IPV6 网络连接；本系统的 DNS 及 HTTP、HTTPS 代理有细致的上网过滤功能	VPN 用户以加密的形式连接其它在线 VPN 用户的虚拟 IP 的网络服务	VPN 用户的虚拟 IP 网络通过本系统的外网 IP 上网，可同时分配本系统的 DNS 服务器作为客户端的 DNS 服务器，并做上网过滤。 即使停用 SNAT，也可以通过本系统虚拟网关的 HTTP、HTTPS 代理服务上网，不影响客户端路由
前提	本机的各网络服务可以设置为只对 VPN 虚拟网络开放，各 VPN 服务器可以停用 SNAT 上网功能	需要对方 PC 防火墙允许，OpenVPN 用户需要启用 C2C 功能	启用 SNAT 功能，下发给客户端可上网的路由，客户端 VPN 网卡设置 VPN 为默认路由

VPN 用户即使不拨号连接也可以作为认证用户使用 DDNS WEB 在线更新服务、WEB 在线代理、WebDAV 服务、HTTP/HTTPS 代理服务。

4、对外服务

VPN 用户连接成功后有三种对外服务，一是在 DDNS 域名解析基础上的客户端公网 IP 的对外服务，二是用户 URL，三是用户端口映射，只有用户端口映

射有用户设置项。**如果“用户 URL”内容是灰色显示，则表示用户当前没有在客户端处登录。**

“端口映射”用于 VPN 用户登陆并获得虚拟 IP 后，将外网 IP 及端口映射到该用户的虚拟 IP 端口上，虚拟 IP 可以是动态获得的（无用户 URL），也可以是绑定 IP（有用户 URL），从而达到内网穿透的效果，如果使用 OS（Windows、iOS、安卓）自带的 VPN 客户端，例如 IKEV2 VPN（参考**“5 IKE VPN 客户端设置”**）等，可以实现 0 客户端内网穿透；或者使用内核级 VPN——WireGuard VPN，比 DDNS、SSH 反向端口代理和普通的内网穿透都好。

端口映射设置界面

当“设置类型”为“管理员设置”时，只能由管理员做设置；当“设置类型”为“用户设置”时，管理员和用户都可以做设置，用户登录 WEB 用户门户后，在“对外服务”处进行设置，可以不中断当前 VPN 连接，可以通过查看“流量统计”获得当前端口映射设置及使用情况。用户只能设置 5 个单个的端口映射，管理员可以设置端口范围。举例说明：

（1）tcp 80

将外网 IP 的 TCP 80 端口映射到 VPN 客户端虚拟 IP 的 TCP 80 端口

（2）tcp 135:139

将外网 IP 的 TCP 135~139 端口范围一对一映射到 VPN 客户端虚拟 IP 的 TCP 135~139 端口。端口范围只能“系统管理员设置”

（3）tcp 1:65535

udp 1:65535

访问外网 IP 的 TCP、UDP 端口，将转发到 VPN 客户端虚拟 IP 相同的端口，但系统已有端口除外，相当于整机 IP 映射。端口范围只能“系统管理员设置”

（4）tcp 8080 80

将外网 IP 的 TCP 8080 端口映射到 VPN 客户端虚拟 IP 的 TCP 80 端口

（5）tcp 13389 3389 27.0.0.0/16,45.0.0.0/16

将外网 IP 的 TCP 13389 端口映射到 VPN 客户端虚拟 IP 的 TCP 3389 端口，且只允许 27.0.0.0/16 或 45.0.0.0/16 的源 IP 访问

VPN 用户连接成功后的对外服务的内容及前提条件，详见下表：

对外服务	**DDNS 解析**	**端口映射/内网穿透**	**用户 URL**
内容	本系统将 VPN 用户名解析为 VPN 用户连接时的公网 IP，A 或 AAAA 记录，在此基础上，客户端提供对外服务	将在线 VPN 用户的虚拟 IP 的端口服务映射到本系统外网 IP 的相应端口，达到内网穿透的效果；SSH 客户端的反向端口代理与此类似，但需要客户端设置；可以由客户端 PC 防火墙控制来源 IP	将在线 VPN 用户的虚拟 IP 的 80 端口 WEB 服务映射到本系统外网域名或 IP 的 http/https URL；WEB、SSH 用户上传的文件形成的 URL
服务器 IP	用户的公网 IP	本系统的外网 IP	本系统的外网 IP
前提	用户名必须是域名的形式，且属于自主管理 NS 域名；客户端设置对外访问的内容；客户端 PC 防火墙设置允许的来源 IP	需要先设置端口映射规则，分为管理员设置和用户设置两种权限；客户端设置对外访问的内容；客户端 PC 防火墙设置允许的来源 IP	管理员必须先设置“用户 URL”为“映射到用户文件”并绑定 IP；客户端 PC 防火墙设置允许的来源 IP

5、用户口令

“口令”栏可以修改用户的口令，由于登录账号、口令就是 WEB、WEB 代理、VPN、SSH 等具体服务的登录账号、口令，所以修改成功后将中断现有的 VPN/SSH 连接。WireGuard VPN 用户可以查看、下载、更新配置文件及二维码。

对于 IKEV2/IPSEC VPN、OCSERV/CISCO AnyConnect VPN、PPTP VPN、

L2TP VPN、OpenVPN、WireGuard VPN、SSH 用户有两种客户端认证方法：用户名密码认证和 TOTP 动态密码认证。

TOTP 动态密码认证的过程是：

1）管理员在 VPN/SSH 服务页面中设置“TOTP 动态密码认证”选项

2）管理员设置好系统时间

3）管理员新建 VPN/SSH 用户账号

4）用户在手机/平板/PC 中下载 TOTP APP 软件

可以自定义 time step 为 300 秒（缺省是 30 秒）的应用：

注意：请勿使用安卓版的 google 身份验证器/ google authenticator，因为 time step 固定为 30 秒

- Android:

1）Aegis（推荐，有指纹识别等保护措施）

https://github.com/beemdevelopment/Aegis

2）Freetop

https://github.com/helloworld1/FreeOTPPlus

https://github.com/freeotp/freeotp-android

注意：不能用安卓版的 google 身份验证器，因为其 time step 只能是 30 秒，不能是其他值

- Chrome:

https://authenticator.cc/

- iOS

1）google 身份验证器（和 android app 不同，可以扫描 time step 不是 30 秒的二维码）

https://apps.apple.com/cn/app/google-authenticator/id388497605

2）OTP Auth（带 Face ID, Touch ID 及系统锁屏密码，可备份恢复，可看到 time step 是 300，可显示 secret code 和二维码）

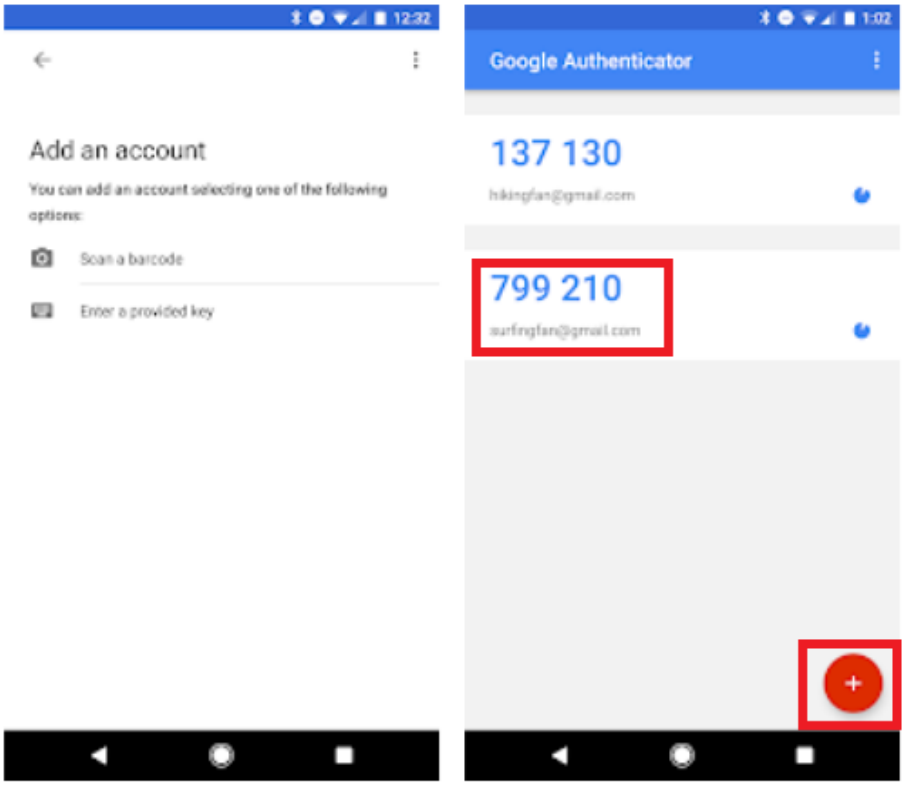
https://apps.apple.com/cn/app/otp-auth/id659877384

- Windows

Winauth 3.6.2

https://github.com/winauth/winauth/releases/tag/3.6.2

5）用户登录 WEB 用户门户，查看 TOTP 初始密码，扫描 TOTP 初始密码的二维码，在 APP 中添加认证项，接着查看验证码，在 WEB 门户中输入验证码，激活 TOTP 认证。注意：APP 每 5 分钟刷新验证码，系统时间和手机时间必须一致，否则无法激活



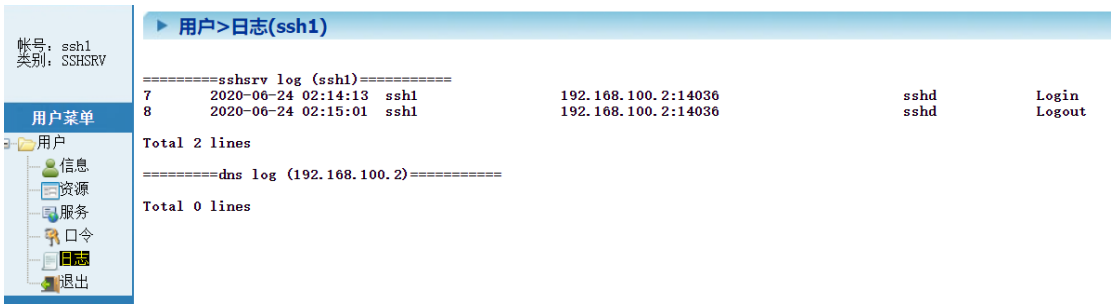
6）激活后，就可以使用 OpenVPN/SSH/SFTP 客户端登录，输入用户名以及 APP 显示的验证码，不需要登录 WEB 门户的密码（防止信息泄露）


```
root@TrustGate:/tmp# sftp -oPort=34567 ssh2@127.0.0.1
Verification code: 799 210
Connected to 127.0.0.1.
sftp>
```

7）激活后，WEB 用户门户中的 TOTP 初始密码及二维码不显示（防止信息泄露），可以再次输入 APP 显示的验证码，重新显示 TOTP 初始密码及二维码，方便在其它手机/平板/PC 中添加认证项

8）在 WEB 用户门户信息页面中查看“客户端认证方法”项，对于“TOTP 动态密码认证”，*号表示未激活，√号表示已经激活，？号表示 TOTP 初始密码错误

6、用户日志



登录用户可以查看本账号所属服务的日志，以及登录 IP 的 DNS 日志，都是当天的日志，最大 500 条。客户端 OS 网络设置中设置本系统 IP/域名为 DNS 服务器（**“1 DNS 服务器设置”**），就可以在此查看 DNS 日志。

参考：

安卓系统在 4G 移动数据流量及 WIFI 时设置（DOT 加密）DNS 服务器：http://trustcomputing.com.cn/bbs/viewthread.php?tid=1631

15.2 Console 用户终端

Console 用户终端使用示例

http://www.trustcomputing.com.cn/help/cn/dadi/user/modify_password.html

用户可以在本机 Console 口登录，或是用任意 SSH 客户端软件远程登录，查询信息或修改口令，其过程如下：

1）新建一个 SSH 连接，具体 IP 及端口请咨询服务提供商，用户名、密码是 console、zstdadi

```
Username: ssh1
Password:
----------
Connection:
192.168.1.2:55292 192.168.1.56:3456
Disk Quota: 8.9M/9.5M
----------
New password:
New password again:

Done.
```

图 15-3 修改用户密码

```
Username: ssh1
Password:
----------
Connection:
192.168.1.2:55304 192.168.1.56:3456
Disk Quota: 8.9M/9.5M
----------
New password:
Bye.
```

图 15-4 查询状态

2）用 console 账号登陆后，输入需要查询/修改的用户名及其当前密码，认证成功后，显示该用户当前活动的连接，SSH 用户还显示磁盘空间使用情况；接着输入新密码，再一次输入新密码，成功后显示 Done.，如图 15-3 所示，修改密码后，用户当前活动的连接全部停止。如果不输入新密码，直接回车，则相当于查询当前连接状态，如图 15-4 所示。

VPN、SS、SSH 的特性比较表

项目	协议端口	认证方式	事先安装 CA 证书	连通时通过系统代理	连通后通过系统代理	多用户	客户端	其它特性
IKEV2 VPN	500/UDP 4500/UDP ESP、AH	证书+用户名&密码	必须	否	否，需单独设置代理	是	Win10 OS 安卓 App iOS OS	MOBIKE 硬件加速性能好，适合移动终端
IPSEC VPN	500/UDP 4500/UDP ESP、AH	用户名&密码	否	否	否	是	Win10 App 安卓 OS iOS App	主要为了以前设备的兼容性
OCSERV VPN	TCP UDP	证书+用户名&密码	需要但非强制性	是	是	是	Win10 App 安卓 App iOS App	性能好，适合移动终端
PPTP VPN	1723/TCP GRE PPP	用户名&密码	否	否	否，需单独设置代理	是	Win10 OS 安卓 OS iOS App	无法 NAT 穿越，安全性不好，不支持 IPv6
L2TP VPN	1701/UDP 500/UDP 4500/UDP ESP PPP	用户名&密码	否	否	否，需单独设置代理	是	Win10 OS 安卓 OS iOS App	可以 NAT 穿越，支持 IPv6
OpenVPN	TCP UDP	证书+用户名	必须	否，但可通过	是	是	Win10 App 安卓 App	可下发路由，定制

		&密码		HTTP 代理，免流			iOS App	化程度高，断线重连，性能稍差
SoftEther VPN	TCP	用户名&密码	否	否，但可通过 Socks5、HTTP 代理	是	是	Win10 App Linux App MAC App	性能好，但不适合移动终端
SSTP VPN	TCP	证书+用户名&密码	必须	是	否，需单独设置代理	是	Win10 OS 安卓 App	性能好，但不适合移动终端
SS 服务器	TCP	用户名&密码	否	否，但可通过 Socks5、HTTP 代理	否，可另外设置代理	否	Win10 App 安卓 App iOS App	性能好，费电，不适合移动终端
SS/SSR 客户端代理	TCP	/	否	否	/	否	Win10 OS 安卓 OS iOS OS	通用方便，利用 netch 实现 4 层路由/每应用不同路由
SSH 客户端	TCP	用户名&密码	否	否	/	是	Win10 OS 安卓 OS iOS OS	通用方便，节电，适用于移动终端

注意：

1）Windows 下的 VPN 拨号如果有路由等问题，最好禁用所有无关的网卡，包括设备管理器中的网卡，再重新拨号

2）某些 ISP 对 UDP 协议做了出口 IP 分流，会导致与服务器连接的源 IP 不固定，此时只能换用别的 TCP 协议的程序或者换客户端的位置

参考文件：

《中神通大地云控客户端设置主图一览表》

http://www.trustcomputing.com.cn/help/client_setup_list.docx