# 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

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。

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。

|  |
| --- |
| Windows10下使用IKEV2 VPN示例  http://www.trustcomputing.com.cn/help/cn/dadi/ikev2/windows\_ikev2.html |

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



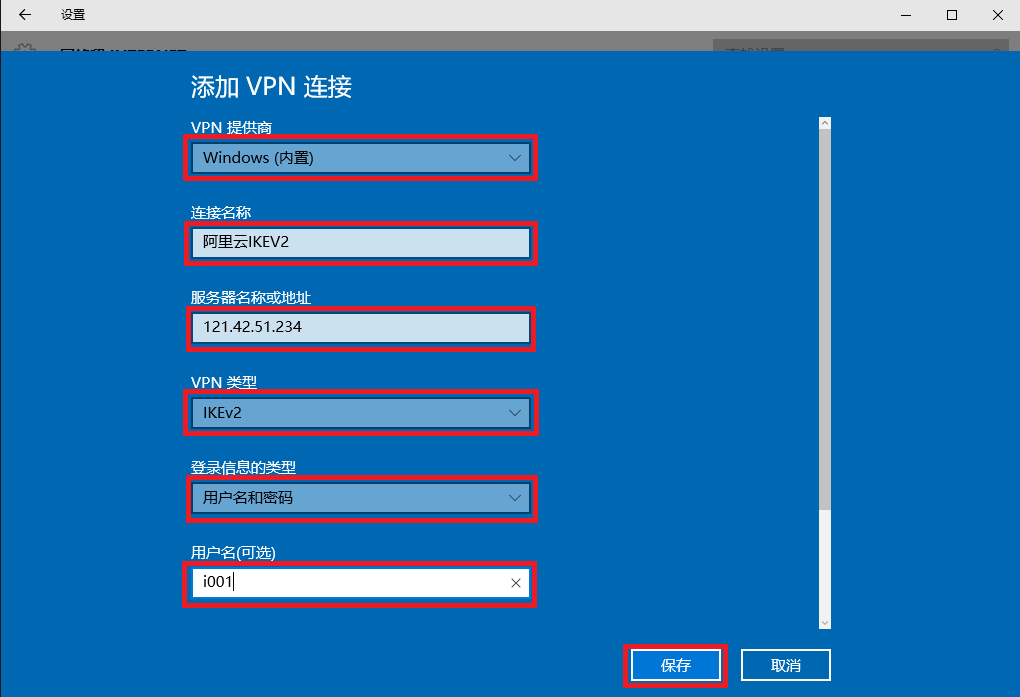
**图5-2**“网络和INTERNET”窗口

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

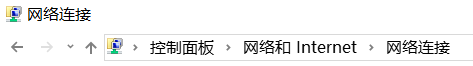
添加成功后，返回列表，在末尾找到新添加的连接名称，需要连接时可以点击该项，再点击下方的“连接”按钮，就可以连接VPN了，如下图5-4所示。



**图5-4** 连接VPN

**2）修改网络的默认网关属性**

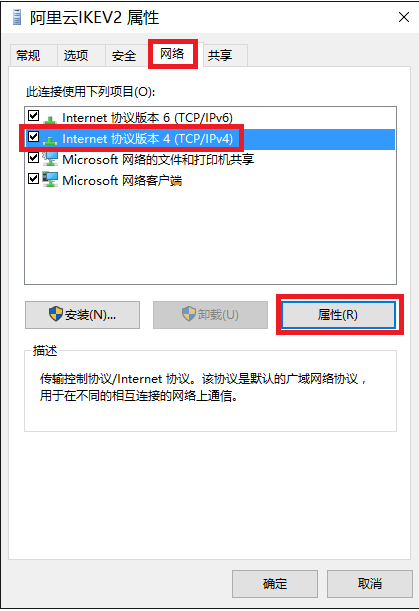
VPN连通后，只能访问10.32.0.1，为了能访问10.32.0.0/24网络及其它公网IP，需要使VPN连接成为缺省路由，即需要对该VPN连接的网络属性进行修改。具体过程如下图5-5-1、2、3、4、5所示。



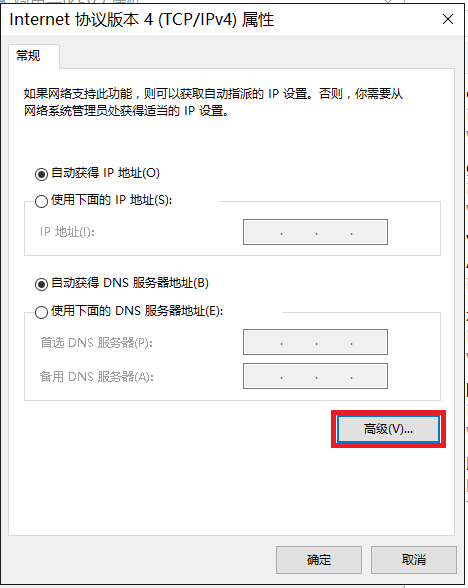
**图5-5-1** 修改VPN连接的默认网关的网络属性1



**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



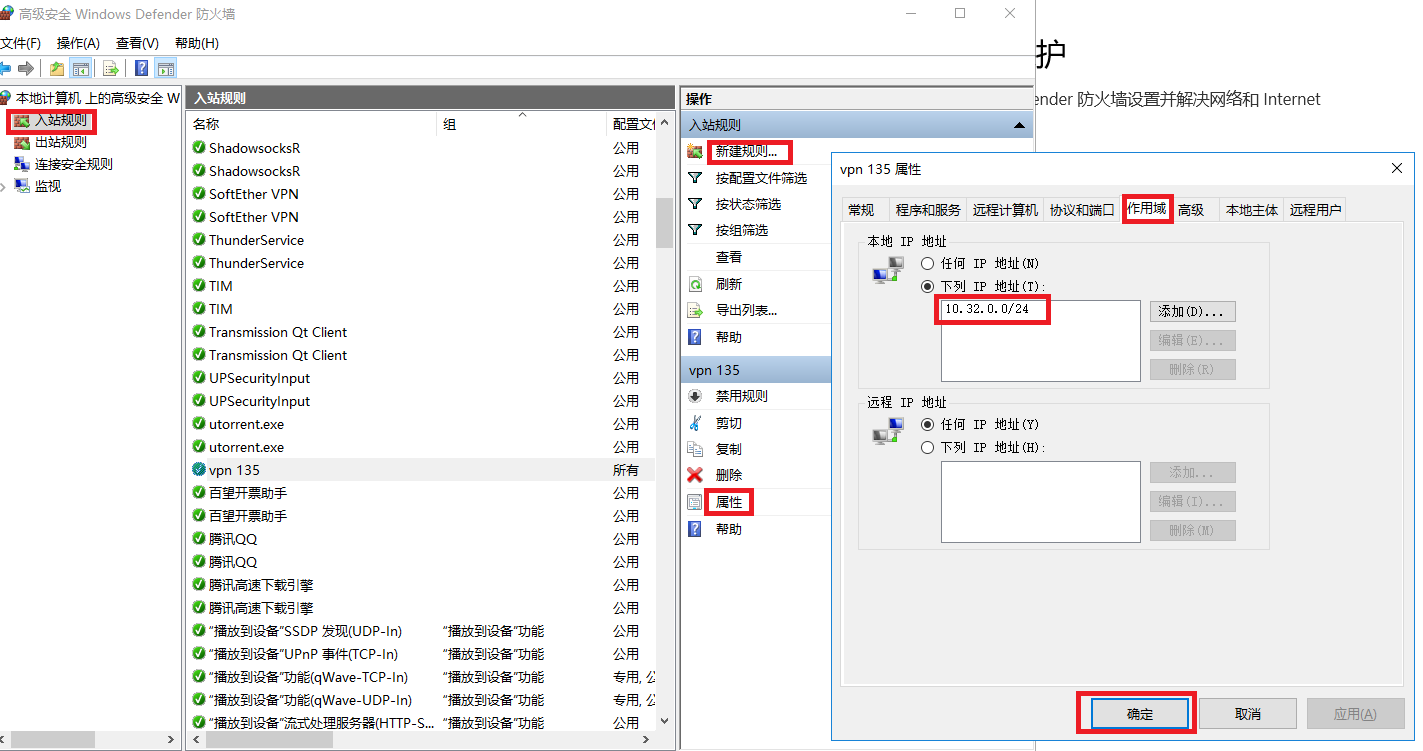
**图5-5-5** 修改VPN连接的默认网关的网络属性5

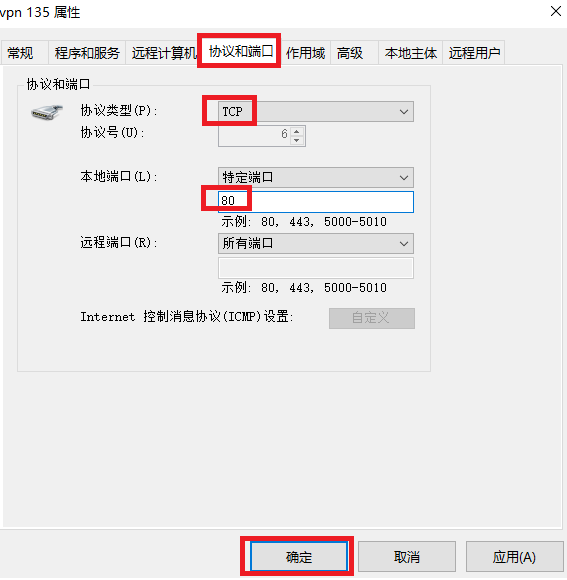
打开网络连接控制面板，找到VPN连接，按右键，选择“属性”项，弹出属性窗口，切换到“网络”TAB，选择“Internet协议版本4（TCP/IPv4）”项，点击下方的“属性”按钮，在弹出的窗口中点击“高级”按钮，在弹出的窗口中勾选“在远程网络上使用默认网关”项，再一路点击“确定”按钮，保存配置。

**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

**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。

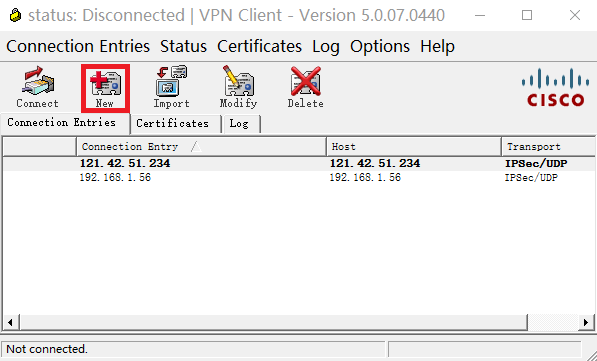
5.1.2 CISCO VPN Client安装及使用

**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 |

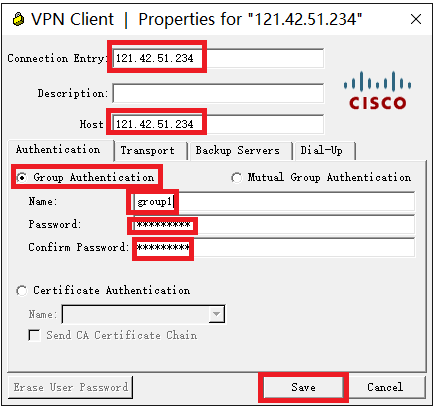
下载并安装CISCO VPN Client软件，对于Win10系统还需要安装补丁，依次运行WinFix.exe、DNEUpdatex64.msi、CiscoVPNClientFixx64.exe，具体过程参考http://cisco.techygeekshome.info/windows-10。

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

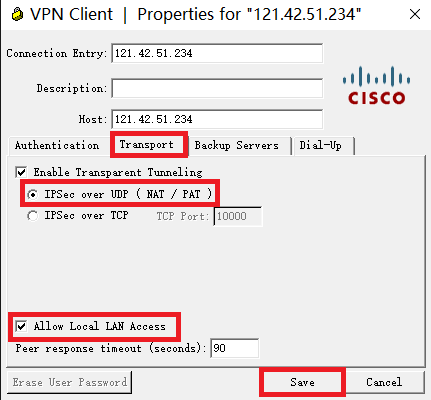
点击“New”按钮新建一个VPN连接，弹出参数窗口，如下图5-8所示。

****

**图5-8** CISCO VPN Client软件参数窗口1

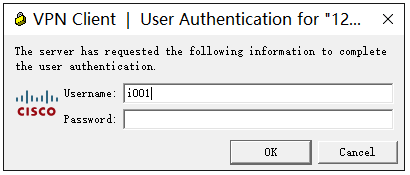
依次填写各栏目，最后点击“Save”按钮。其中Name栏填写“group1”，Password栏填写“myPSKkey”。

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

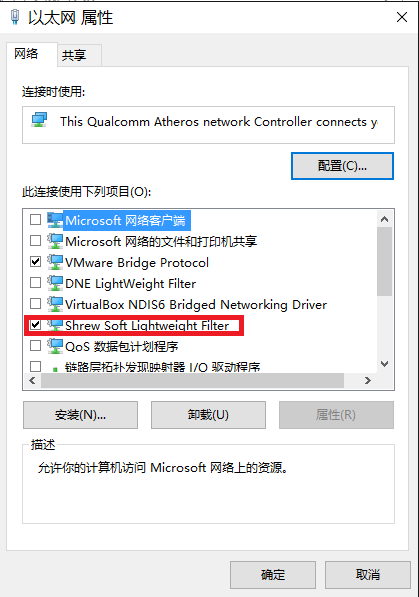
输入正确的用户名和密码，连接成功后主窗口关闭，需要到右下角任务栏图标中找到图标，右键点击图标弹出菜单项，点击“Disconnect”中断连接。

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 |

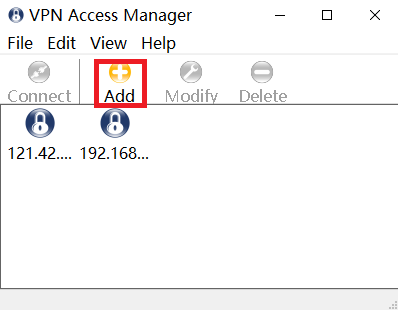
下载并安装ShrewSoft VPN软件，相比CISCO VPN Client软件，其在Win8/Win10系统下不需要另外安装补丁也可以运行，是免费软件。

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。



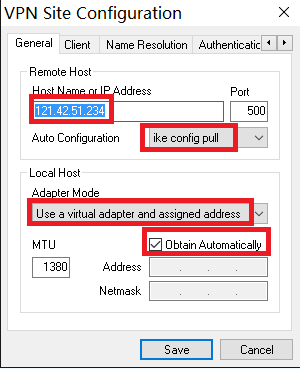
**图5-11** 物理网卡与ShrewSoft VPN有关的属性

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。

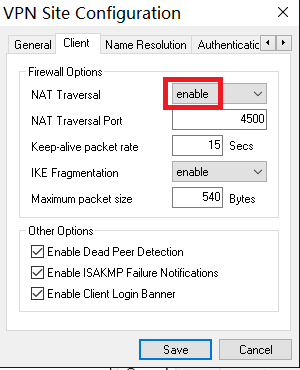


**图5-12** ShrewSoft VPN软件主窗口

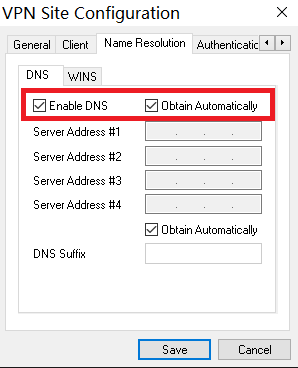
填写各个参数窗口的设置，如下图5-13-1、2、3、4、5、6、7、8、9所示。



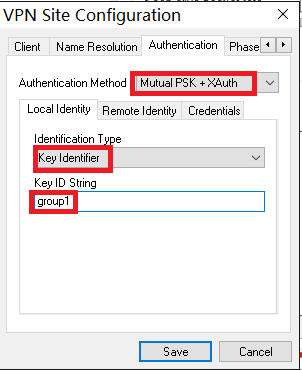
**图5-13-1** ShrewSoft VPN软件参数窗口1



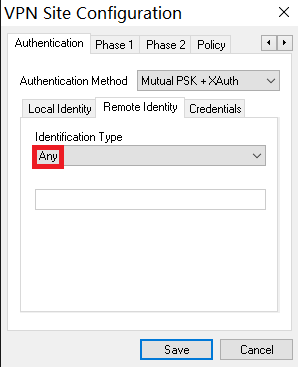
**图5-13-2** ShrewSoft VPN软件参数窗口2



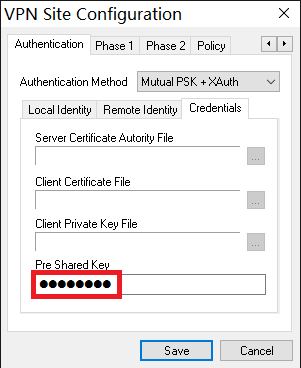
**图5-13-3** ShrewSoft VPN软件参数窗口3



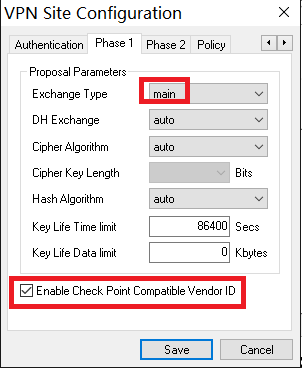
**图5-13-4** ShrewSoft VPN软件参数窗口4



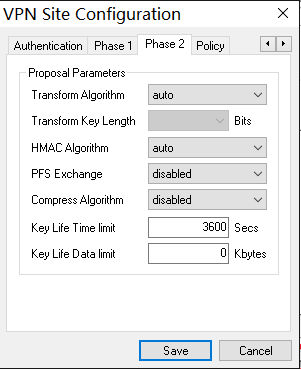
**图5-13-5** ShrewSoft VPN软件参数窗口5



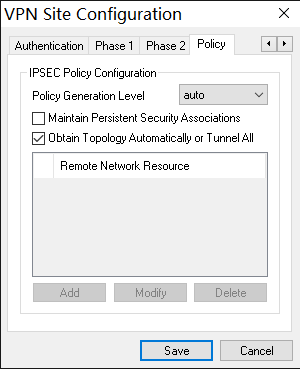
**图5-13-6** ShrewSoft VPN软件参数窗口6



**图5-13-7** ShrewSoft VPN软件参数窗口7



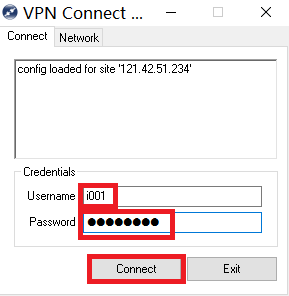
**图5-13-8** ShrewSoft VPN软件参数窗口8



**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，而且部分手机/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。

**1、下载安装自签名CA证书**

对于IKEV2 VPN（第三方APP）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”，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”；

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** |

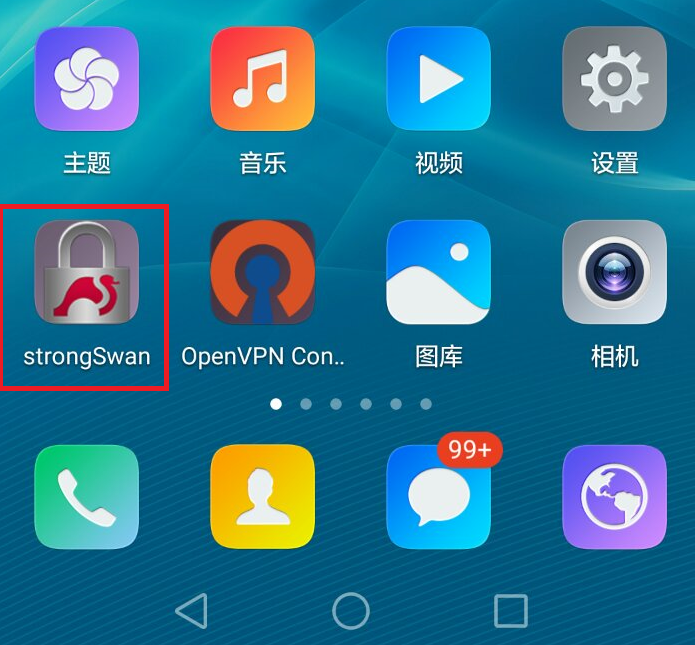
**图5-15** 安卓系统自带的IPSEC VPN设置

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  http://www.trustcomputing.com.cn/tools/org.strongswan.android\_1.8.1.apk |

strongSwan VPN client软件是安卓系统下的专门的IKEV2 VPN客户端软件。

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）通过浏览器下载安装自签名CA证书，URL类似“http://121.42.51.234/ikev2.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。

## 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”，输入“描述”、“服务器”、“远程ID”、“用户名”、“密码”，其中，“服务器”、“远程ID”均为VPN服务器的IP或域名，再点击右上角的“完成”按钮；

3）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。

|  |  |
| --- | --- |
| iOS 1 | iOS%202 |
|  |  |
| iOS%205 |  |

**图5-18** iOS系统下新建IKEV2 VPN连接