**Adroid、Iphone、Windows10通过ipsec与防火墙建立通道**

鉴于手机比较普遍。如何通过手机来防火墙建立VPN通道，经过测试，ipsec客户端可以实现通道分割，而且不需要安装客户端软件，比较便捷。

实验拓扑如下：



# 防火墙配置

## 设置用户和用户组

先建用户test, 然后建用户组t，把test选入该组。





## 设置通道分割的地址段对象

我们需要先定义一个地址对象，该地址对象用于通道分割，意思就是vpn客户端所访问的内网地址段。该地址段可以比较宽泛一些。

地址对象是在“防火墙/地址/地址”中定义的，如下图所示。



## IPSec阶段1

配置阶段1，可以在图形界面下完成，注意是以下几条：

* 模式选择连接用户
* 主模式
* DH要有2(为Android和iphone)
* 启用xauth认证，选择用户组t

图形界面配置如下：



命令行下指定分配的地址段和通道分割的地址段：

define vpn ipsec phase1-interface

 edit "dialup"

 set mode-cfg enable

 set default-gw 10.1.1.254

 set ipv4-start-ip 10.1.1.1 ------指定分配的起始地址

 set ipv4-end-ip 10.1.1.25 ------指定分配的终止地址

 set ipv4-dns-server1 4.2.2.1 ------指定分配的DNS地址

 set ipv4-split-include "net" ------指定通道分割地址段

 next

end

## IPSec阶段2

配置阶段2，有以下注意事项：

* 加密算法要有AES256+MD5
* 关闭PFS
* 密钥周期要设置成“两者都有”

图形界面如下：



## 设置路由

我们需要将分配的地址段设置路由给vpn虚拟接口上。如下图所示，在静态路由中指定vpn虚拟接口路由，目标地址段是分配给vpn客户端的。



## 防火墙策略配置

添加策略允许vpn客户端访问内网。源接口设置为vpn虚拟接口，目标接口为要访问的网段，如下图所示。



# Android客户端

## VPN设置

Android上已经具备VPN功能，所以在“设置>更多>VPN”直接开启即可：



如上图所示，设置类型为“IPSec xauth PSK”指定服务器地址和IPsec预共享密钥，然后保存。

## VPN拨号

在Android上选择连接VPN，会提示输入用户和密码。在本例中输入前面已经定义好的“test”和相应的密码即可。在防火墙的“VPN>IPsec>监控器”中可以看到拨号用户。



# iphone客户端

iphone也具有ipsec客户端。在“设置>通用”，如下图。



在“通用>VPN”设置中，新建一个ipsec，如下图所示



输入内容：

* 服务器， 指定防火墙IP
* 账户和密码，输入test和它的密码
* 密钥，输入ipsec的共享密钥

IPhone拨号成功后，在防火墙上也可以看到该用户。

# Windows10客户端

Windows 需要安装ipsec客户端软件。下载地方如下所示。

<https://www.shrew.net/download>

## 客户端安装

安装Shrew VPN客户端，需要注意要选择安装标准版本，如安装为默认的专业版本，则只有15天的试用期。如下图所示：



## 客户端配置

安装完成后，打开Shrew软件，进行配置。点击Add按钮，新建客户端VPN连接。

* General标签配置



Hostname处填写防火墙vpn网关地址。”Auto configuration” 选择Ike config pull，对应的是vpn网关的mode-config。当Adapter Mode下有三个选项，在这里选择自动分配，如上图所示。

* Name Resolution标签配置

选择“enable DNS”和“Obtain Automatically”，设置为自动获得IP。



* Authentication标签配置

在Authentication Method中选择Mutual PSK



在Credentials中填写预共享密钥：



* Phase 1标签配置



 对阶段1 VPN协商参数进行配置，此配置需要与防火墙阶段1配置匹配，设置为”main”和“group 2”。

* Phase 2标签配置



 对阶段2 VPN协商参数进行配置，此配置需要与防火墙阶段2配置匹配。

配置完成后，点击save。接着可以进行VPN拨号连接：



连接成功后，客户端会显示如下信息：



在防火墙上VPN->IPSec->监视器中，可以看到隧道成功建立。



此时，VPN拨号客户端IP为客户端PC网卡配置的IP地址。

shrew vpn client可以备份配置。所以配置一份后，其他用户导入该配置即可。



# ubuntu客户端

VPN客户端ubuntu 16.04下安装方法。Shrew Soft VPN客户端图形界面要求使用Qt 4.x。所以，作为依赖，你需要安装其开发文件。

1.安装依赖包：

$ Yum -y install gcc gcc-c++ flex libedit libedit-devel bison openssl openssl-devel qt qt-devel

2.安装cmake和lib包

$ sudo apt-get install cmake libqt4-core libqt4-dev libqt4-gui libedit-dev libssl-dev checkinstall flex bison

3.下载ike即为shrew软件解压并安装。

$ wget <https://www.shrew.net/download/ike/ike-2.2.1-release.tbz2>

$ tar xvfvj ike-2.2.1-release.tbz2

$ cd ike

$ cmake -DCMAKE\_INSTALL\_PREFIX=/usr -DQTGUI=YES -DETCDIR=/etc -DNATT=YES

$ sudo apt install ike

4.启动

**$ qikea**

1. 接下来的配置就和windows客户端一样。请按照windows客户端界面设置方法进行配置。

这部分内容参照：

**<https://stackoverflow.com/questions/13175823/how-can-i-install-shrew-soft-vpn-client-under-ubuntu-12-10>**

# MAC客户端

苹果笔记本电脑自带Cisco vpn client。打开“系统偏好设置”中的“网络”。点击”+”来添加接口，设置接口为vpn，类型为cisco ipsec，如下图所示。

****

设置服务器IP地址，也就是vpn网关地址，然后设置xauth用户名和密码，如下所示。

****

点开鉴定设置，设置共享密钥，如下图所示。

****

设置完毕后，点击连接，就可以建立起vpn。