**Adroid、Iphone、Windows10通过ipsec over l2tp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，l2tp over ipsec是目前最好的选择

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tt，把test选入该组。





## 设置l2tp

该步骤在命令行下完成：

define vpn l2tp

 set eip 10.1.1.10

 set sip 10.1.1.1

 set status enable

 set usrgrp "tt"

end

sip用来指定分配给客户端的起始IP，eip用来指定分配给客户端的最大IP。

## 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
* 加密算法要有3DES-SHA1 (为Windows)AES256—MD5(为Android和iPhone)
* 不要设置为接口模式
* DH要有2(为Android和iphone)， 14(为windows10)

图形界面配置如下：



## 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
* 启用传输模式(命令行下设置)
* 密钥周期要设置成“两者都有”

图形界面如下：



命令行设置如下：

define vpn ipsec phase2

 edit "phase2"

 set encapsulation transport-mode （设置为传输模式）

 set keylife-type both

 set pfs disable

 set phase1name "phase1"

 set proposal 3des-sha1 aes256-md5

 set keylifekbs 4608000

 set keylifeseconds 3600

 next

end

## 防火墙策略配置

防火墙策略分为两条：

* IPSec策略，源地址是内网地址，目标地址是all
* L2tp客户端访问内网的策略，源地址是分配的客户端IP，目标地址是内网地址命令行配置。

IPsec策略如下：



策略是从内向外建立的，也就是port2到port1，源地址是内网地址(192.168.100.0/24)，目标地址all, 选择VPN通道为l2tpvp。

允许客户端访问内网的策略如下：



策略是从外到内，也就是port1到port2, 源地址是分配给客户端的ip地址，在本案例中是10.1.1.0/24。

# 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“l2tp/IPSec 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，就可以拨号成功。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l2tp over ipsec客户端。在“设置>通用”，如下图。



在“通用>VPN”设置中，新建一个l2tp，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

在“控制面板>网络和共享中心”选择“设置新的连接或网络”。



在“设置连接网络”中，选择“连接到工作区”



在连接工作区中选择“使用我的Internet连接”。



在下图中输入VPN的IP地址，然后选择“创建”



创建连接后，在网络连接处，选择该链接，右键菜单中选择属性，如下图所示



如下图所示，在属性的安全页，VPN类型选择为“L2TP/IPsec”，选择“允许使用这些协议”，如下图所示。



点击高级设置，设置“使用预共享密钥做身份认证”，输入IPsec的共享密钥，如下图所示。



如果要连接vpn，则在网络连接处选择该vpn，右键菜单中选择连接。



然后输入用户名密码，即可连接成功。我们通过ipconfig和route print查看分配的IP和生成的路由。