# ICG2000D/ICG3000F系列路由器L2TP over IPSec VPN配置方法

L2TP VPN IPSec VPN 史晓虎 2019-08-21 发表

## 组网及说明

**1 配置需求或说明**

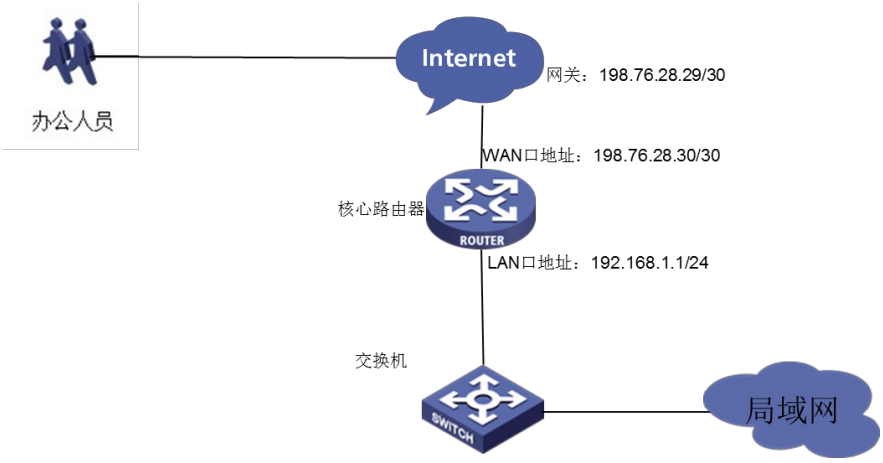
**1.1 适用产品系列**

本案例适用于如ICG2000D、ICG3000F系列的路由器。

**1.2 配置需求及实现的效果**

路由器采用固定IP地址的方式部署在公司互联网出口，运营商提供的IP地址为198.76.28.30/30，内网地址为192.168.1.1/24。外网用户为了访问公司的内网资源，出于安全考虑采用l2tp over ipsec的方式拨入公司内网进行访问。

**2 组网图**




## 配置步骤

**3 配置步骤**

**3.1 配置路由器基本上网**

#路由器基本上网配置省略，具体设置步骤请参考“2.2.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830-WiNet系列路由器基本上网（静态IP）WEB配置（V7）”案例

**3.2 配置路由器**

#开启L2TP功能

system-view

[H3C]l2tp enable

#创建地址池

[H3C]ip pool 1 192.168.10.2 192.168.10.200

#创建一个虚模板，指定地址池

[H3C]interface Virtual-Template1

[H3C-Virtual-Template1] ppp authentication-mode chap domain system

[H3C-Virtual-Template1]remote address pool 1

[H3C-Virtual-Template1]ip address 192.168.10.1 24

[H3C-Virtual-Template1]quit

#创建l2tp组

[H3C]l2tp-group 1 mode lns

[H3C-l2tp1] allow l2tp virtual-template 1

[H3C-l2tp1]undo tunnel authentication

[H3C-l2tp1]quit

#创建本地用户

[H3C]local-user 123 class network

[H3C-luser-network-123]password simple 123456

[H3C-luser-network-123]service-type ppp

[H3C-luser-network-123]quit

#创建多个ike安全提议，采用不同的加密算法和验证算法

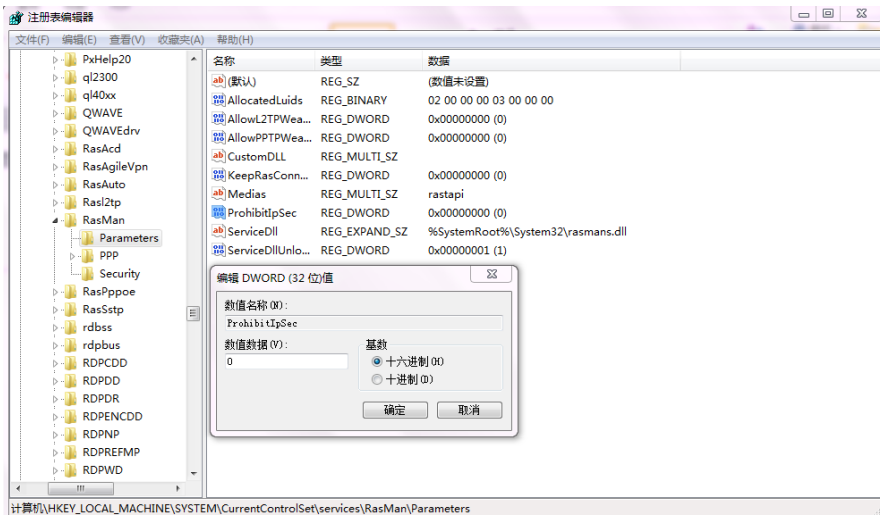
[H3C]ike proposal 1

[H3C-ike-proposal-1]encryption-algorithm aes-cbc-128
[H3C-ike-proposal-1]authentication-algorithm md5
[H3C-ike-proposal-1]dh group2
[H3C]ike proposal 2
[H3C-ike-proposal-2]encryption-algorithm 3des-cbc
[H3C-ike-proposal-2]authentication-algorithm md5
[H3C-ike-proposal-2]dh group2
[H3C]ike proposal 3
[H3C-ike-proposal-3]encryption-algorithm 3des-cbc
[H3C-ike-proposal-3]dh group2
[H3C]ike proposal 4
[H3C-ike-proposal-4]encryption-algorithm aes-cbc-256
[H3C-ike-proposal-4]dh group2
[H3C]ike proposal 5
[H3C-ike-proposal-5]dh group2
[H3C]ike proposal 6
[H3C-ike-proposal-6]encryption-algorithm aes-cbc-192
[H3C-ike-proposal-6]dh group2
#配置ike keychain，配置对端地址为0.0.0.0，预共享密钥为123456
[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address 0.0.0.0 0 key simple 123456
#配置ike profile，引用ike keychain和ike安全提议，本端公网地址为198.76.28.30
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]exchange-mode aggressive
[H3C-ike-profile-1]local-identity address 198.76.28.30
[H3C-ike-profile-1]match remote identity address 0.0.0.0 0.0.0.0
[H3C-ike-profile-1]proposal 1 2 3 4 5 6
#配置多个ipsec安全提议，采用不同的验证算法和加密算法
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]encapsulation-mode transport
[H3C-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128
[H3C-ipsec-transform-set-1]esp authentication-algorithm sha1
[H3C]ipsec transform-set 2
[H3C-ipsec-transform-set-2]encapsulation-mode transport
[H3C-ipsec-transform-set-2]esp encryption-algorithm aes-cbc-256
[H3C-ipsec-transform-set-2]esp authentication-algorithm sha1
[H3C]ipsec transform-set 3
[H3C-ipsec-transform-set-3]encapsulation-mode transport
[H3C-ipsec-transform-set-3]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-3]esp authentication-algorithm sha1
[H3C]ipsec transform-set 4
[H3C-ipsec-transform-set-4]encapsulation-mode transport
[H3C-ipsec-transform-set-4]esp encryption-algorithm des-cbc
[H3C-ipsec-transform-set-4]esp authentication-algorithm sha1
[H3C]ipsec transform-set 5
[H3C-ipsec-transform-set-5]encapsulation-mode transport
[H3C-ipsec-transform-set-5]esp encryption-algorithm aes-cbc-192
[H3C-ipsec-transform-set-5]esp authentication-algorithm sha1
[H3C]ipsec transform-set 6
[H3C-ipsec-transform-set-6]encapsulation-mode transport
#配置一个名字为1，序号为1的安全策略模板，引用ike profile和ipsec安全提议
[H3C]ipsec policy-template 1 1
[H3C-ipsec-policy-template-1-1]
[H3C-ipsec-policy-template-1-1]transform-set 1 2 3 4 5 6
[H3C-ipsec-policy-template-1-1]ike-profile 1
#引用ipsec安全策略模板，创建ipsec安全策略
[H3C]ipsec policy 1 1 isakmp template 1
#在公网口调用ipsec安全策略
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]ipsec apply policy 1

### 3.3 手机侧配置

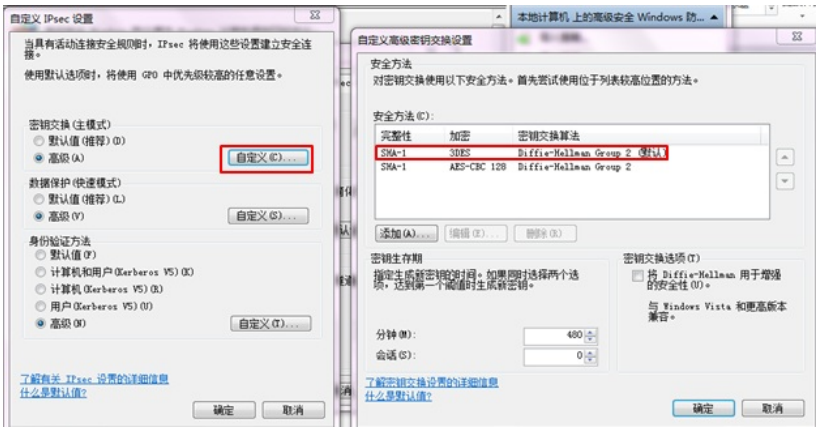

**3.4 Windown7电脑侧配置**

1．在命令行模式下执行regedit命令，弹出“注册表编辑器”对话框。在左侧注册表项目中逐级找到：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters，单击Parameters参数，然后双击ProhibitIpSec，把值改为0.

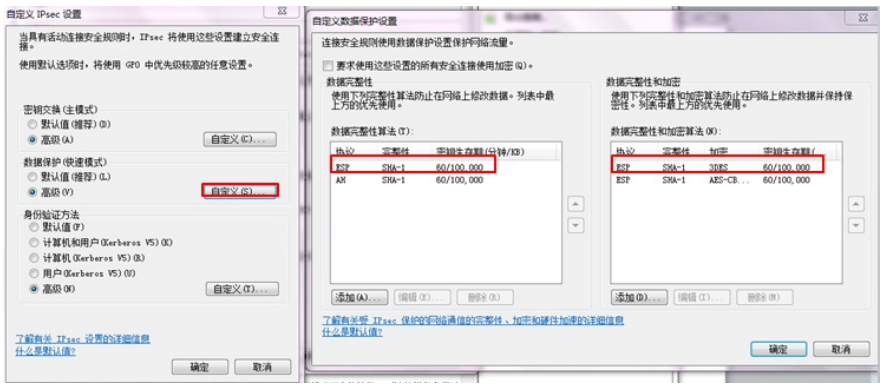



2．打开控制面板/系统与安全/windows防火墙高级设置/属性/IPSec设置，如图

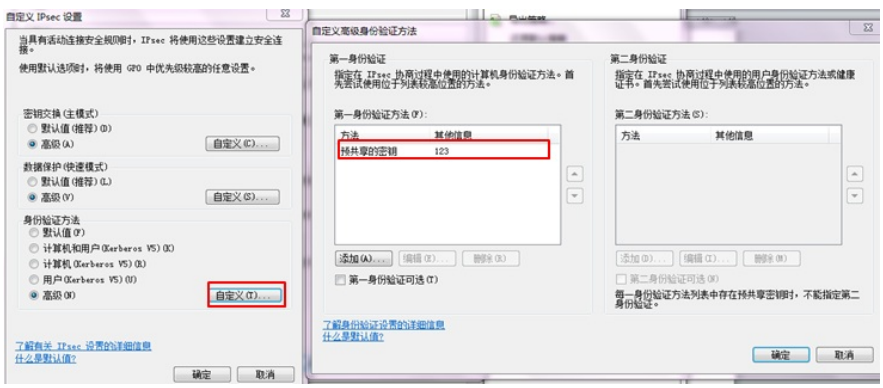

#选择SHA-1，3DES，Group2




选择加密参数

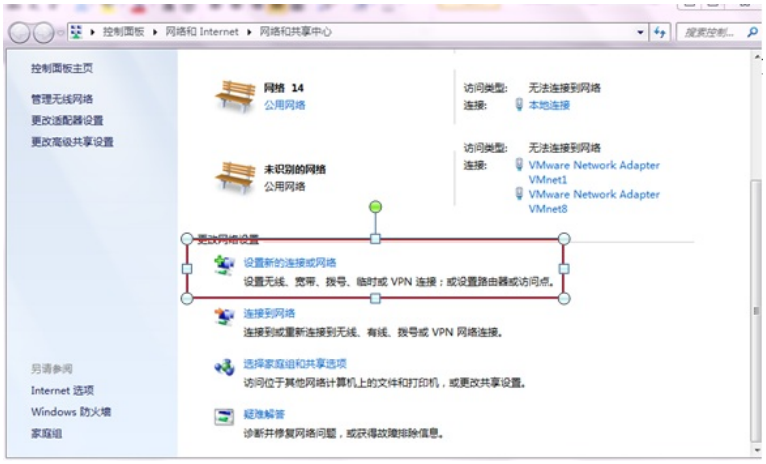



选择预共享密钥，数值需要与IKE 配置中的数值相同，然后确定，应用



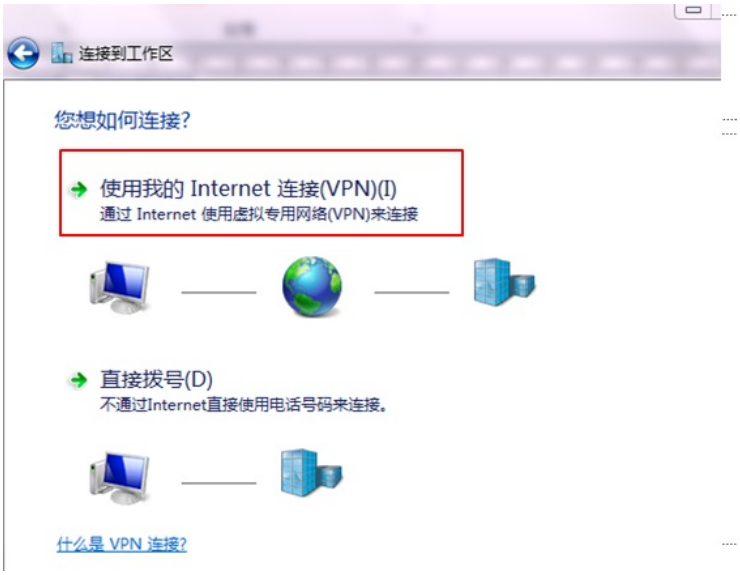
配置好终端之后一定要重新启动电脑

3．打开window7自带客户端设置连接，选择新建连接

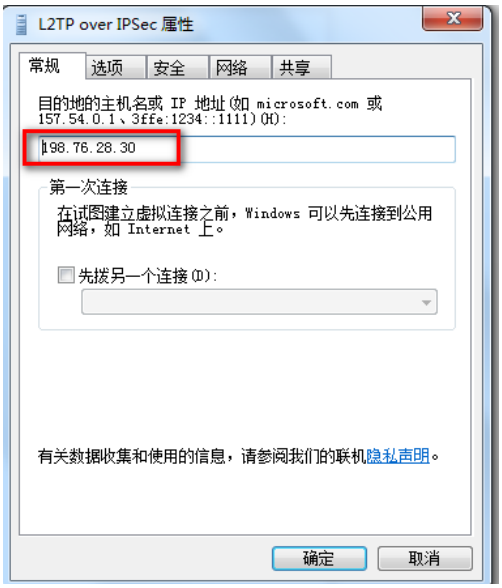


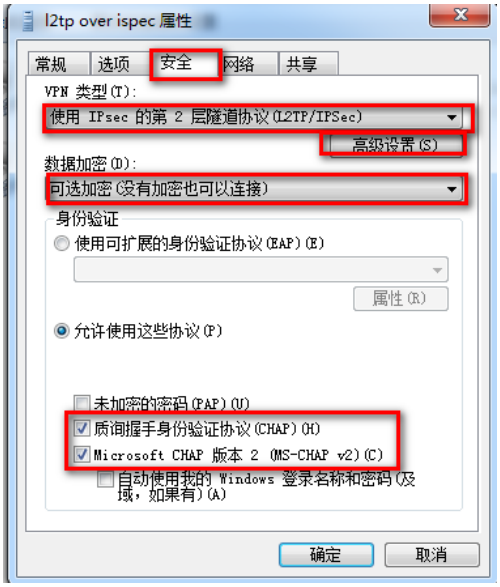

选择连接到工作区


选择设置Internet连接

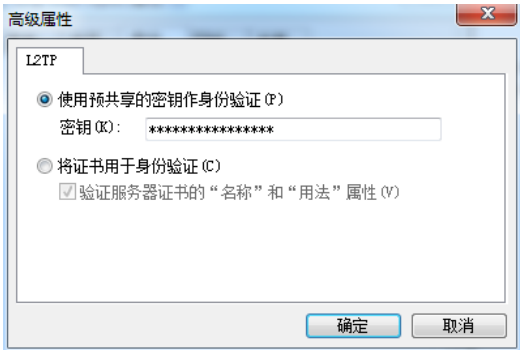



右击VPN连接点属性




使用密钥：也就是ike的共享密钥： 如果选证书可以拨号成功只是触发不了ipsec，填上错误的密码拨号不成功（即使写l2tp的隧道密码也不行）。




连接 L2TP over IPSec
用户名(U):
123
密码(P):
域(M):
为下面用户保存用户名和密码(S):
只是我(M)
任何使用此计算机的人(A)
连接(C)
取消
属性(O)
帮助(H)

## 配置关键点