L2TP IPSec 朱尘炀 2016-01-08 发表

客户处需要实现windows10自带的客户端和我司V5版本防火墙的L2TP over IPSEC的对接,如标题。

简易拓扑如下:

- 1、FW直连公网,有固定的公网IP地址
- 2、PC连接网络,可以正常访问公网,即可以访问到防火墙的公网地址



一、Windows10终端配置步骤

提示:win10的L2TP和PPTP方式相比,前面的创建步骤相同,仅在属性设置(<u>第8步</u>)上有所不同, 若需要将已有的pptp方式的VPN连接更换为L2TP,则可直接修改VPN的属性。

1.点击桌面右下角任务栏中的<u>网络图</u>标,然后点击"打开网络和共享中心"。也可以通过控制面板中的网络和Internet进入网络和共享中心。





2. 在网络和共享中心里, 点击"设置新的连接或网络";

网络和共享中心			100	>
	面板 > 网络和 Internet > 网络和共享中心	5 v	搜索控制面板	\$
控制面板主页	查看基本网络信息并设置连接			
更改适配器设置	查看活动网络			
更改高级共享设置	网络 公用网络	访问类型 连接:	: Internet Ethernet0	
	更改网络设置		1	
	设置宽带、拨号或 VPN 连接;或设	置路由器或接入点。		
	诊断并修复网络问题,或者获得疑难	解答信息。		
中洋关闭				
力呵参问 Internet 洗顶				
Windows 防火墙				
the second purchase				

3. 选中"连接到工作区",点击"下一步";

	-			×
4	🔮 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)	I II	消

4. 点击"使用我的Internet连接 (VPN)";

← 🖬 连接到工作区	5000)		×
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。			
🔍 — 🦫			
		Ę	以消

5. 在Internet地址处栏填写VPN服务器地址(本例中地址118.119.250.10),服务器地址可于后台查看 。"目标名称"可随意填写主要用于标识或区别线路。点击创建;

÷	🖕 连接到工作区			_		×
	键入要连接的 Inter	net 地址				
	网络管理员可提供此地址					
	Internet 地址(I):	jp6.yunfv.com				
	目标名称(E):	XingYunVPN				
	□ 使用智能卡(S)					
	☑记住我的凭据(R)					
	允许其他人使用此 这么选项会达可以	连接(A)	心在这			
	这个边现几件可以		utix.			
				创建(C)) 取	消
				创建(C)) 取	消

6. 此时已成功创建VPN连接,但不建议立即连接,我们还需要设置一下VPN的协议(PPTP或L2TP)

, 点击网络与共享中心面板左上角的"更改适配器设置";

→ ~ ↑	面板 > 网络和 Internet > 网络和共享中心	5 ~	搜索控制面板	
控制面板主页	查看基本网络信息并设置连接			
更改活配器设置	查看活动网络			
更改高级共享设置	网络	访问类型	: Internet	
	公用网络	连接:	Ethernet0	
	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;或诊	设置路由器或接入点		
	设置宽带、拨号或 VPN 连接;或3	2置路由器或接入点		
	设置宽带、拨号或 VPN 连接;或纷 问题疑准解答 诊断并修复网络问题,或者获得疑别	2置路由器或接入点 推解答信息。		
	设置宽带、拨号或 VPN 连接;或说 问题疑准解答 诊断并修复网络问题,或者获得疑》	2置路由器或接入点 推解答信息。		
	设置宽带、拨号或 VPN 连接;或说 问题疑准解答 诊断并修复网络问题,或者获得疑	2置路由器或接入点 推解答信息。		
	设置宽带、拨号或 VPN 连接;或说 问题疑准解答 诊断并修复网络问题,或者获得疑知	20世路由器或接入点 性解答信息。		
	设置宽带、拨号或 VPN 连接;或必	2置路由器或接入点 推解答信息。		
日志会问	设置宽带、拨号或 VPN 连接;或说 问题疑准解答 诊断并修复网络问题,或者获得疑》	2置路由器或接入点 推解答信息。		
叧请参阅 Internet 洗项	设置宽带、拨号或 VPN 连接;或说 问题疑准解答 诊断并修复网络问题,或者获得疑	2置路由赣或接入点 推解答信息。		
叧请参阅 Internet 选项 Windows 防火墻	设置宽带、拨号或 VPN 连接;或说 同题疑准解答 诊断并修复网络问题,或者获得疑	2000年前日期 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997年1月19日 1997 1997 1997 1997 1997 1997 1997 1		

7. 右击刚创建的VPN连接,选择属性,更改设置;



2 个项目	洗中 1 个项目		
L I XH	201111241		

8.1.在属性对话框中选择安全选项卡, VPN类型选择"使用IPSec...(L2TP/IPSEC)", 然后点击"高级设置";

8.2.在高级属性对话框中,设置预共享密钥为123456,然后点击确定,保存设置。

ZingYunVPN 屬性 ×	高级属性)
常规 选项 安全 网络 共享	L2TP	
VPN 类型(T): 使用 IPsec 的第 2 层隙道协议(L2TP/IPsec) ~	●使用预共事約密钥作身份验证(P)	
数据加密(D): 需要加密(如果服务器拒绝将新开连接) ~ ~	 ● 將证书用于身份验证(C) >> 验证服务器证书的'名称'和'用法 熰性(V) 	
身份验证 〇 使用可扩展的身份验证协议(EAP)(E)		
■性(R) ■性(R)	确定	取消
□ 未加高的密码(PAP)(U) □ 质词提手导份验证协议(CHAP)(H)		
☑ Microsoft CHAP Version 2 (MS-CHAP v2) □ 自动使用我的 Windows 登录名称印密码(反域,如果 有)(A)		
補定 取消	E C	

9. 右击启动VPN连接,即可看到Win8右侧出现的连接按钮;



	查找设置
数据使用量 VPN 拨号	VPN + 添加 VPN 连接 変 XingYunVPN
代理	達接 高級选项 删除 相关设置 更改活配器选项 更改高級共享设置 内络和共享中心 Internet 选项 Windows 防火増

登录			
受录 へ			
XingYunVPN			
	·		
域:			
		确定	取消
二、防火墙配置			
[LSSH-F1000-S-AI]disp cu			
#			
version 5.20, Release 3733			
#			
sysname LSSH-F1000-S-AI			
#			
l2tp enable			

```
#
```

undo voice vlan mac-address 00e0-bb00-0000

#

ike local-name Isshvpn

interzone policy default by-priority

#

domain default enable system

#

telnet server enable

#

undo alg dns undo alg rtsp undo alg h323 undo alg sip

undo alg sqlnet undo alg pptp

undo alg ils undo alg nbt

undo alg msn

undo alg qq undo alg tftp

undo alg sccp

```
undo alg gtp
```

session synchronization enable

#

password-recovery enable #

#

#

vlan 2

domain system access-limit disable state active idle-cut disable

vlan 1

```
self-service-url disable
ip pool 1 192.168.10.2 192.168.10.254
#
pki domain default
 crl check disable
#
ike proposal 10
#
ike peer 10
exchange-mode aggressive
pre-shared-key cipher $c$3$CiguB8zu1FETb+Od7ZqwSYuwCm+N3VV/0YE=
id-type name
local-name lsshvpn
nat traversal
#
ipsec transform-set 10
encapsulation-mode tunnel
transform esp
esp authentication-algorithm sha1
esp encryption-algorithm aes-cbc-128
#
ipsec policy-template fbvpn 10
ike-peer 10
transform-set 10
#
ipsec policy lsshvpn 10 isakmp template fbvpn
#
user-group system
group-attribute allow-guest
#
local-user admin
password cipher $c$3$E3w4cYdrrdDQwSMwk5w/sehiHHC+bRMsdk1SSVnGJg==
authorization-attribute level 3
service-type telnet
service-type web
#
l2tp-group 1
undo tunnel authentication
allow l2tp virtual-template 1
tunnel password cipher $c$3$t/cKMaQQhpYPfcRpo1oHUWAcLd0hsJ4ywx8=
tunnel name Issh
#
interface Virtual-Template1
ppp authentication-mode chap
remote address pool 1
ip address 192.168.10.1 255.255.255.0
#
interface NULL0
#
interface Vlan-interface2
ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet0/0
port link-mode route
ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/1
port link-mode route
ip address 118.119.250.10 255.255.255.0
ipsec policy Isshvpn
#
interface GigabitEthernet0/4
port link-mode route
```

```
#
```

interface GigabitEthernet0/5 port link-mode route # interface GigabitEthernet0/6 port link-mode route # interface GigabitEthernet0/7 port link-mode route # interface GigabitEthernet0/8 port link-mode route # interface GigabitEthernet0/9 port link-mode route # interface GigabitEthernet0/10 port link-mode route # interface GigabitEthernet0/11 port link-mode route # interface GigabitEthernet0/2 port link-mode bridge port access vlan 2 # interface GigabitEthernet0/3 port link-mode bridge port access vlan 2 # vd Root id 1 # zone name Management id 0 priority 100 import interface GigabitEthernet0/0 zone name Local id 1 priority 100 zone name Trust id 2 priority 85 zone name DMZ id 3 priority 50 zone name Untrust id 4 priority 5 import interface GigabitEthernet0/1 switchto vd Root zone name Management id 0 ip virtual-reassembly zone name Local id 1 ip virtual-reassembly zone name Trust id 2 ip virtual-reassembly zone name DMZ id 3 ip virtual-reassembly zone name Untrust id 4 ip virtual-reassembly interzone source Local destination Trust rule 0 permit source-ip any_address destination-ip any_address service any_service rule enable interzone source Trust destination Trust rule 0 permit source-ip any_address destination-ip any_address

service any service rule enable interzone source Trust destination Untrust rule 0 permit source-ip any_address destination-ip any_address service any_service rule enable interzone source Untrust destination Trust rule 0 permit source-ip any_address destination-ip any_address service any_service rule enable # ip route-static 0.0.0.0 0.0.0.0 118.119.250.1 ip route-static 10.0.0.0 255.255.224.0 192.168.1.1 ip route-static 192.168.0.0 255.255.0.0 192.168.1.1 # load xml-configuration # load tr069-configuration # user-interface con 0 user-interface vty 0 4 authentication-mode scheme # return

1、目前win7、win8、win10、iphone、Android上的L2TP连接,只要终端上提示必须输入预共享秘钥,实际上都是L2TP over IPSEC,当然windows也支持直接使用L2TP和设备进行对接 2、iphone和Android上的配置很简单,不做介绍了,只需要手机能正常上网,在VPN设置中填写用户 名密码以及预共享秘钥即可

3、防火墙的配置信息可以参照附件