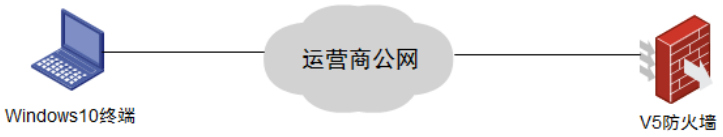
Windows10和V5版本的防火墙对接L2TP over IPSEC配置案例

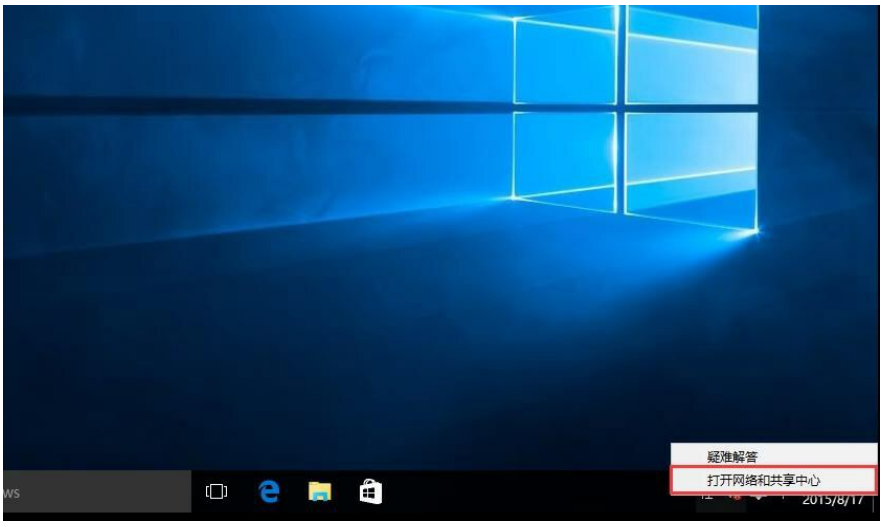
L2TP IPSec 朱尘扬 2016-01-08 发表

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。

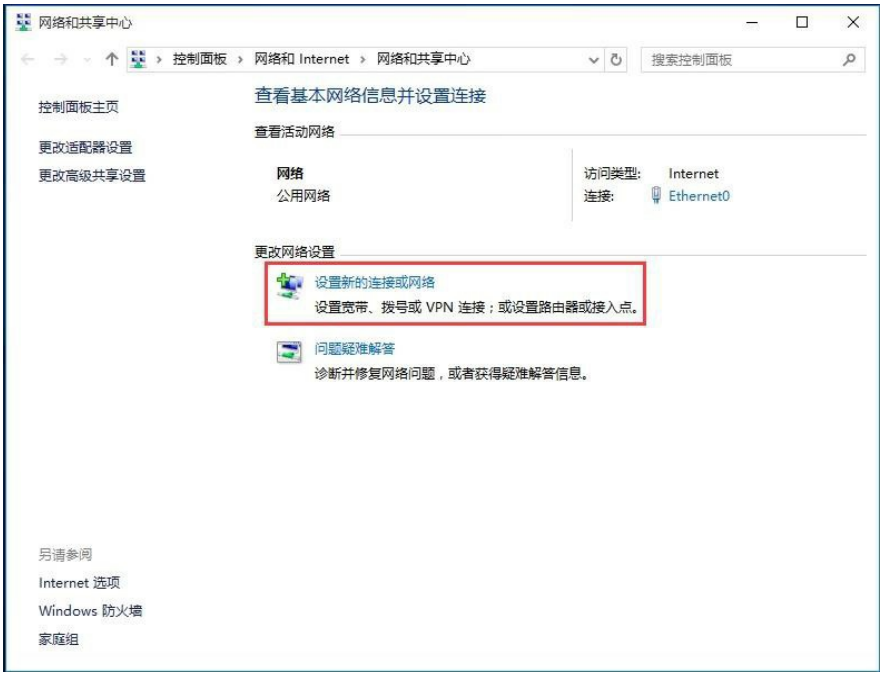
简易拓扑如下：
1、FW直连公网，有固定的公网IP地址
2、PC连接网络，可以正常访问公网，即可以访问到防火墙的公网地址



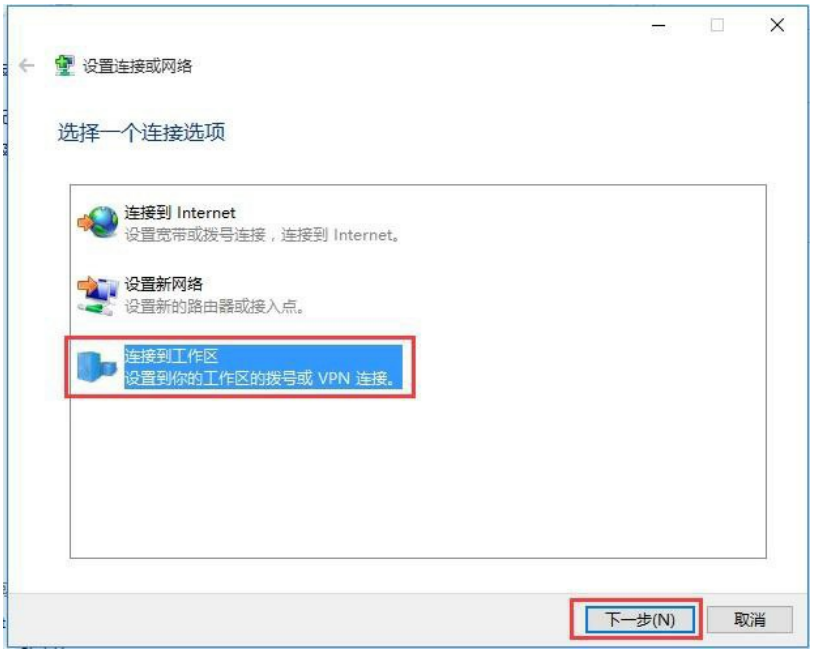
一、Windows10终端配置步骤
提示：win10的L2TP和PPTP方式相比，前面的创建步骤相同，仅在属性设置（第8步）上有所不同，若需要将已有的pptp方式的VPN连接更换为L2TP，则可直接修改VPN的属性。
1.点击桌面右下角任务栏中的网络图标，然后点击“打开网络和共享中心”。也可以通过控制面板中的网络和Internet进入网络和共享中心。



2. 在网络和共享中心里，点击“设置新的连接或网络”；

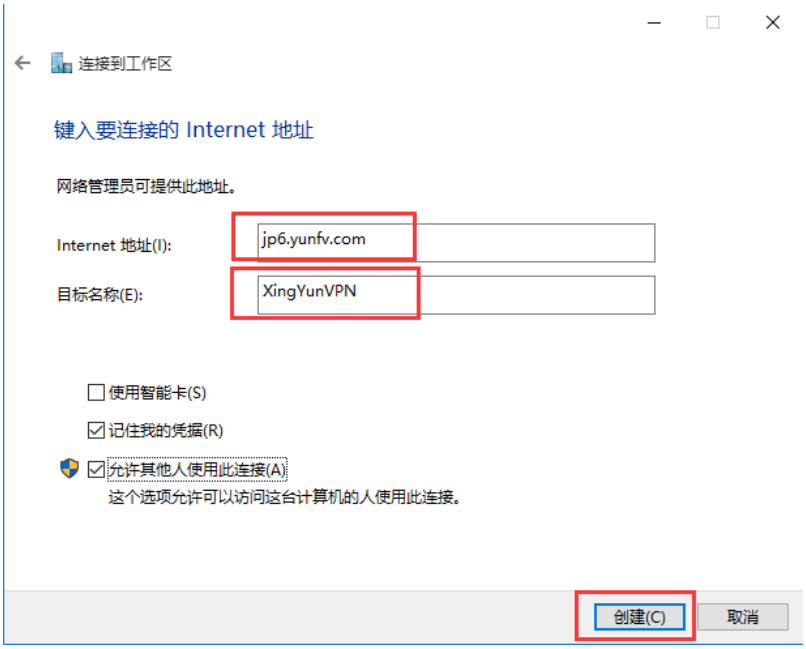


3. 选中“连接到工作区”，点击“下一步”；



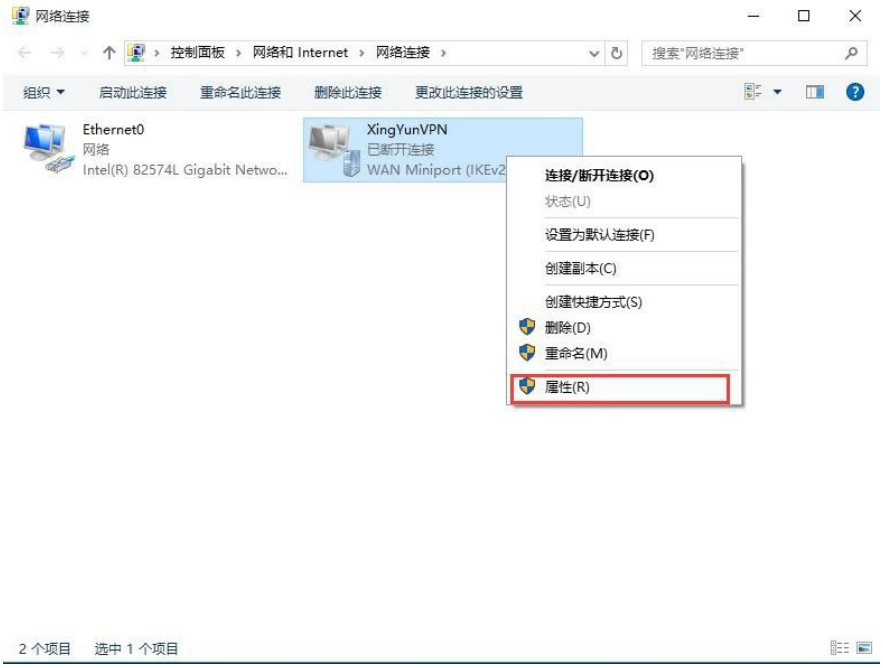
4. 点击“使用我的Internet连接（VPN）”；

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；



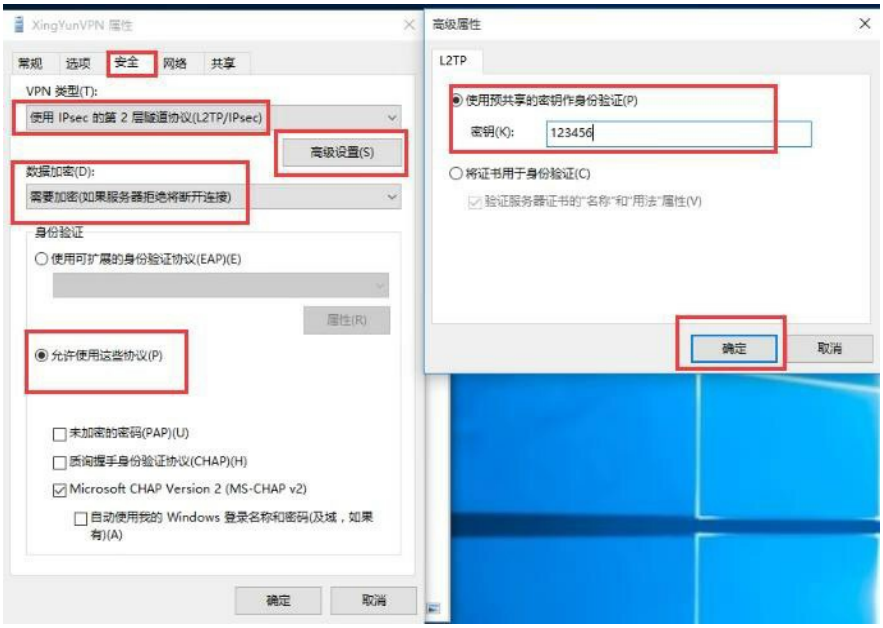
6. 此时已成功创建VPN连接，但不建议立即连接，我们还需要设置一下VPN的协议（PPTP或L2TP），点击网络与共享中心面板左上角的“更改适配器设置”；

7. 右击刚创建的VPN连接，选择属性，更改设置；

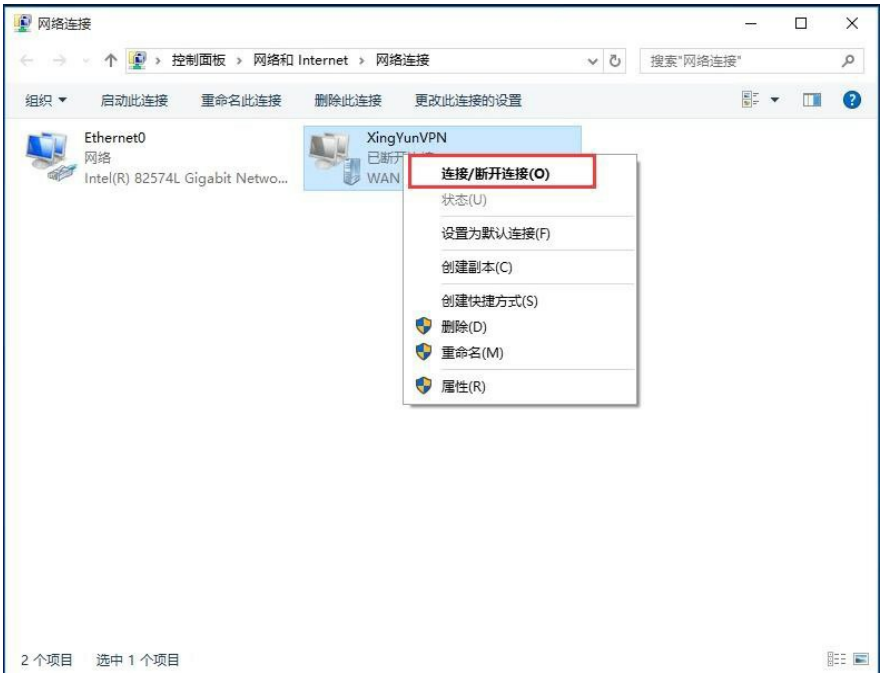


8.1.在属性对话框中选择安全选项卡，VPN类型选择“使用IPSec...(L2TP/IPSEC)”，然后点击“高级设置”；

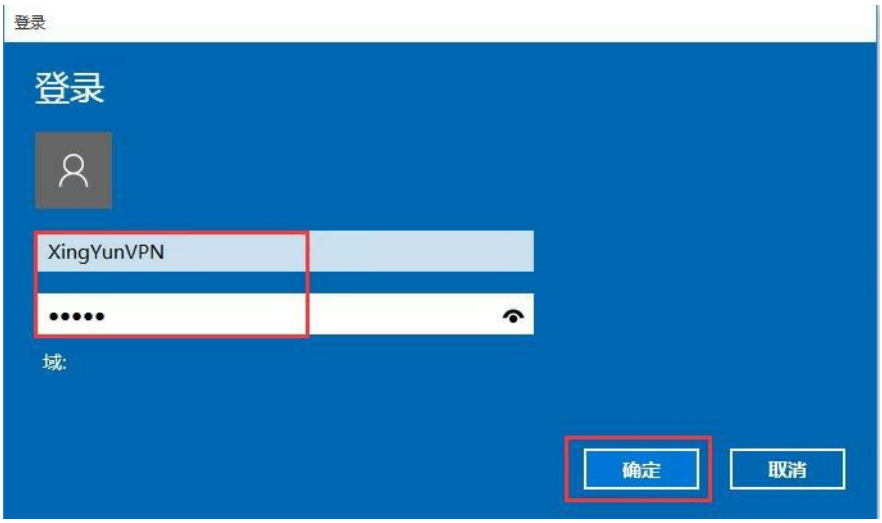
8.2.在高级属性对话框中，设置预共享密钥为123456，然后点击确定，保存设置。



9. 右击启动VPN连接，即可看到Win8右侧出现的连接按钮；



10.点击连接，输入VPN账号（本案例中为lsshvpn）及VPN密码，点击确认进行连接即可。



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 lsshvpn
#
 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 1
#
vlan 2
#
domain system
 access-limit disable
 state active
 idle-cut disable
```

```
 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 lssh
#
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 lsshvpn
#
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