Windows主机LTP VPN典型配置

巫继雨 2009-01-04 发表

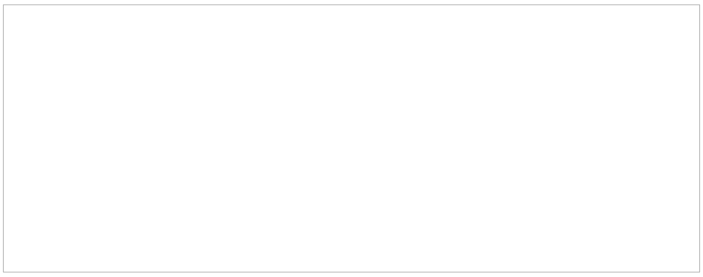
Windows主机L2TP VPN典型配置

一、 组网需求

Windows自身可以作为PPTP/L2TP/IPSec三种VPN的接入客户端，而无需专门的VPN拨号软件(例如iNode)。其中，比较典型的应用是Windows的L2TP VPN，因此本文档将说明在Windows平台上如何配置L2TP VPN接入。

PC1作为L2TP客户端，拨入SecPath V100-A VPN设备。

二、 组网图



如图所示，使用SecPath V100-A作为L2TP的LNS，客户端软件是Windows自带的拨号软件。

三、 配置步骤

1. SecPath V100-A配置

```
[VPN]dis cur
#
 sysname VPN
#
 l2tp enable                                    //使能L2TP功能
#
 insulate
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
radius scheme system
 server-type huawei
#
domain system
 ip pool 1 192.168.1.2 192.168.1.3          //在相应域下配置地址池，默认域为system
#
local-user h3c                                 //配置L2TP接入用户
 password simple h3c
 service-type ppp
#
interface Virtual-Template1                    //配置拨入虚模板
 ppp authentication-mode pap
 ip address 192.168.1.1 255.255.255.0
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 202.38.1.1 255.255.255.0
#
interface Encrypt1/0
#
interface NULL0
#
interface LoopBack1                            //配置Loopback地址，用于测试
 ip address 3.3.3.3 255.255.255.255
#
l2tp-group 1                                   //配置L2TP组
```

```
 undo tunnel authentication
allow l2tp virtual-template 1
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

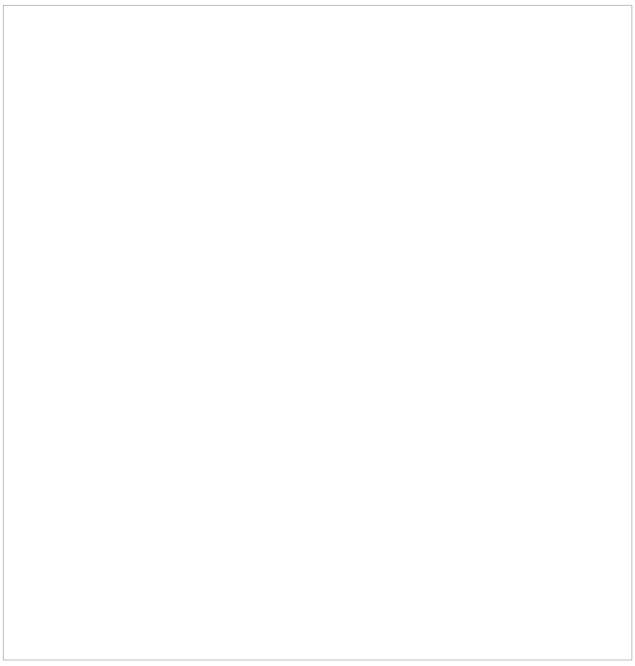
2. Windows L2TP配置

2.1 禁用证书方式的IPSEC

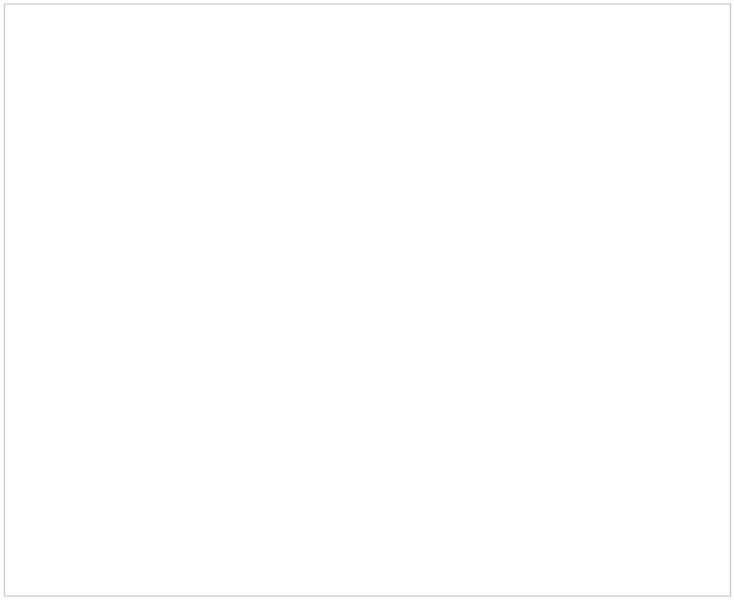
Windows的L2TP功能缺省启动IPSEC，即缺省为L2TP+IPSec VPN，并且IPSec的验证方式为证书方式，应当在注册表中禁用证书方式的IPSec。
方法如下：
在Windows的开始à运行里面输入regedit，找到如下位置
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
加入如下注册项：
Value Name: ProhibitIPSec
Data Type: REG_DWORD
Value: 1
【注意】：注册表修改完成后需要重启Windows。

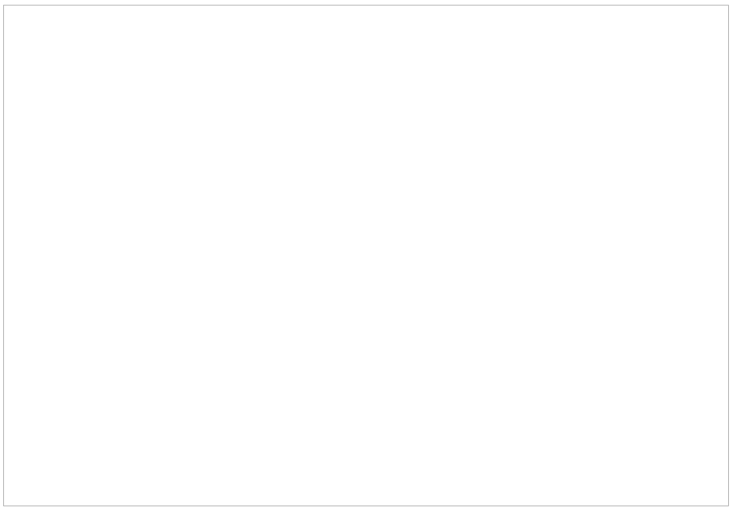
2.2 创建L2TP连接

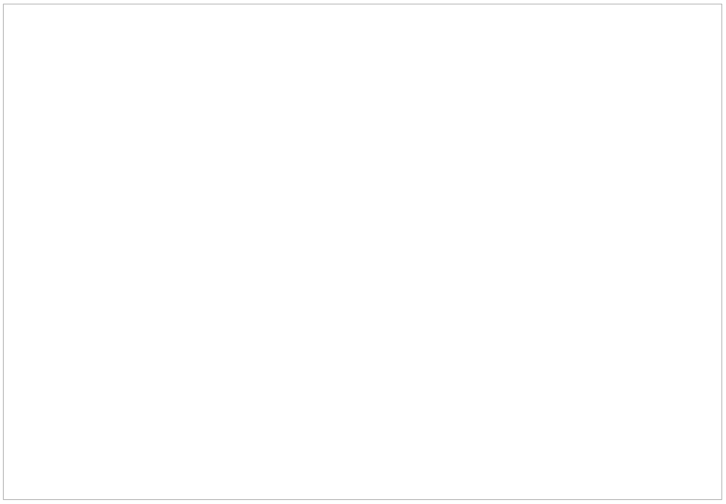
按下面图形依次进行
【说明】：XP和2000/2003 Server的配置略有不同，没有列在下面的步骤按缺省操作即可，下面操作步骤在Windows 2003系统上完成。

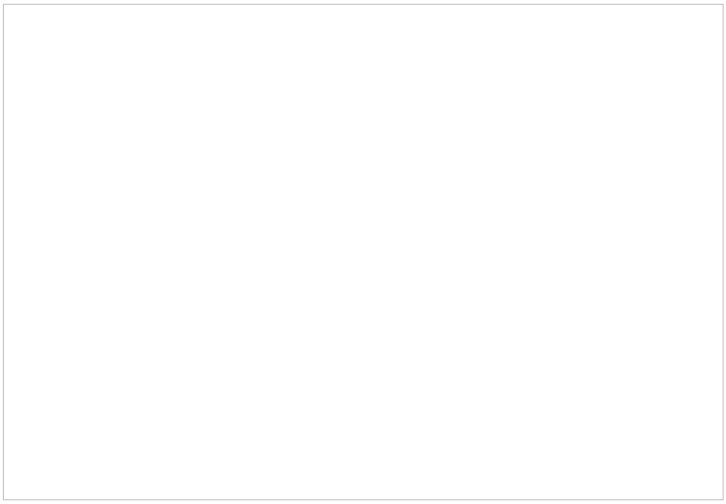


PC1配置IP地址202.38.1.2。（本举例中PC1并未指定网关，这是为了拨号后测试通过VPN ping Loopback地址，实际组网以用户环境为主，一般来讲需配置网关）。

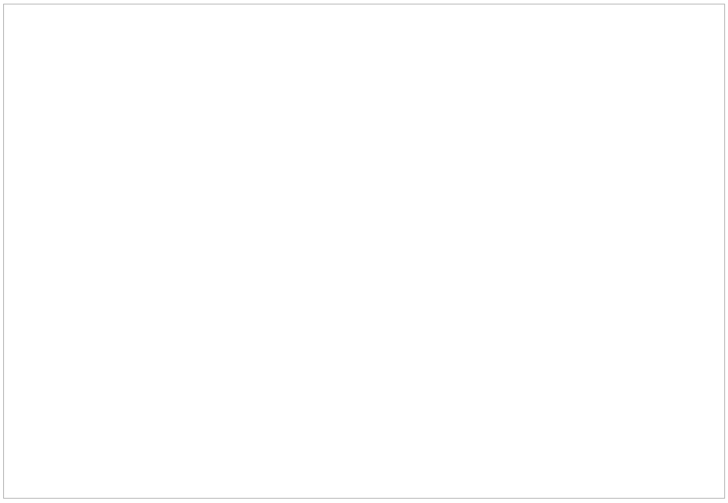


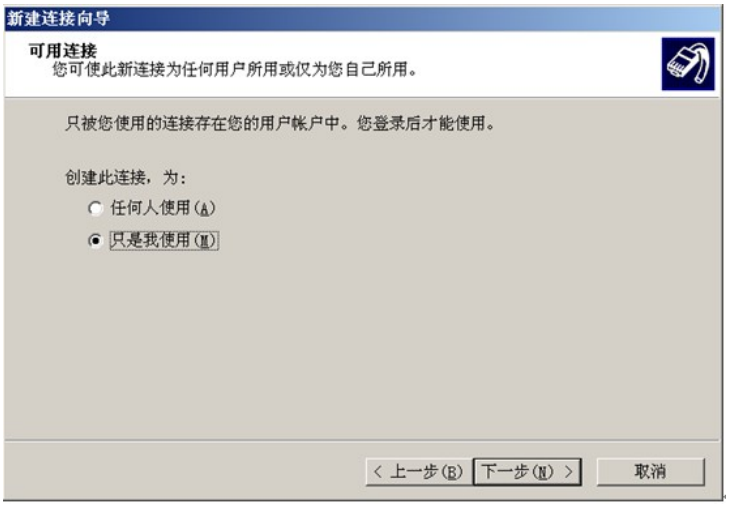


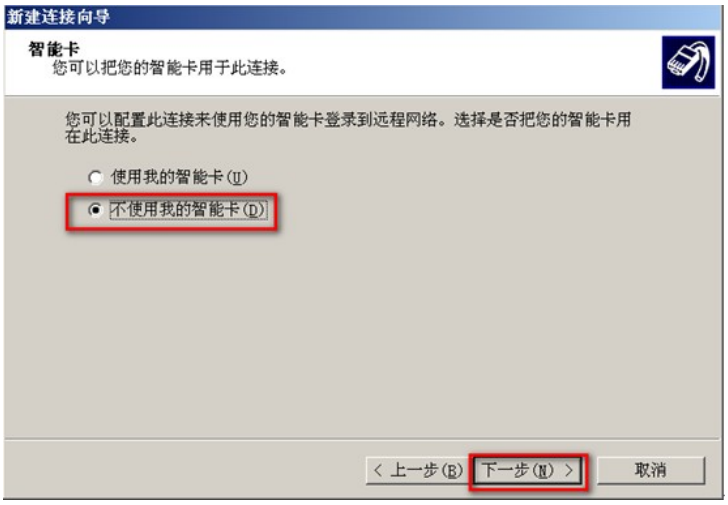


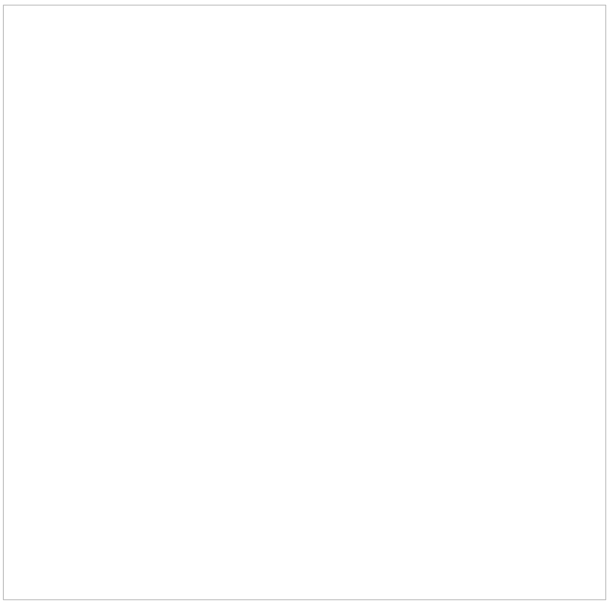


此地址为SecPath V100-A的外网口地址，即接受L2TP拨入的公网地址。

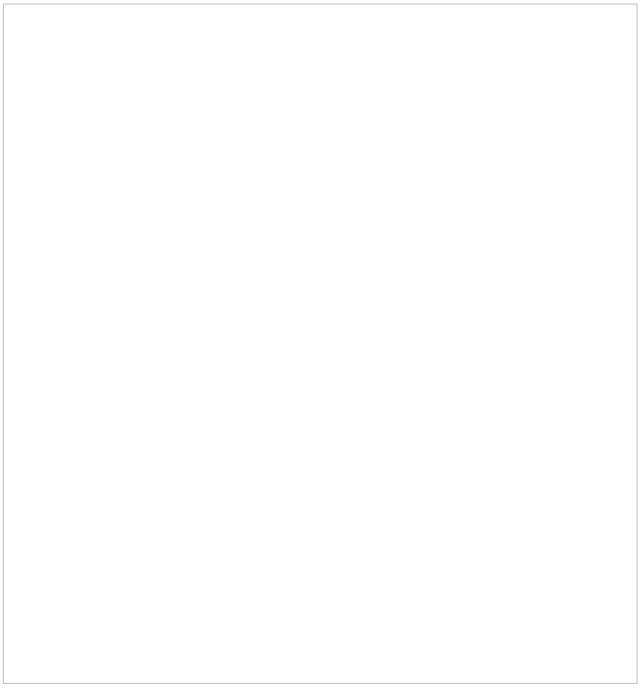



新建连接向导
可用连接
您可使此新连接为任何用户所用或仅为您自己所用。
只被您使用的连接存在您的用户帐户中。您登录后才能使用。
创建此连接，为：
任何人使用(A)
只是我使用(M)
< 上一步(B)
下一步(N) >
取消

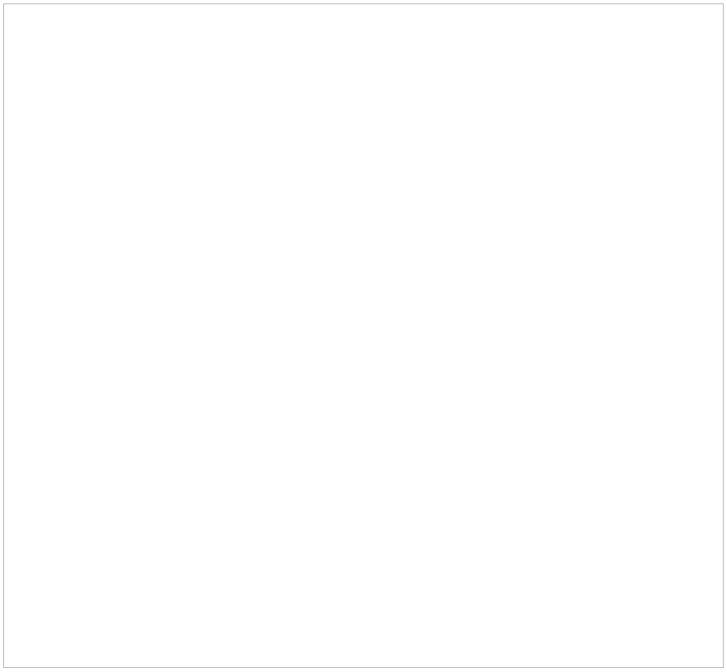

新建连接向导
智能卡
您可以把您的智能卡用于此连接。
您可以配置此连接来使用您的智能卡登录到远程网络。选择是否把您的智能卡用在此连接。
使用我的智能卡(U)
不使用我的智能卡(D)
< 上一步(B)
下一步(N) >
取消



点击“属性”。

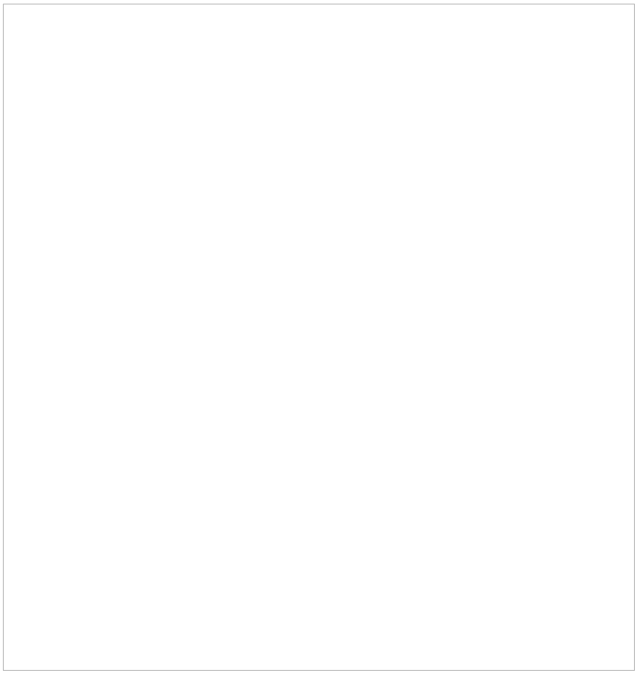


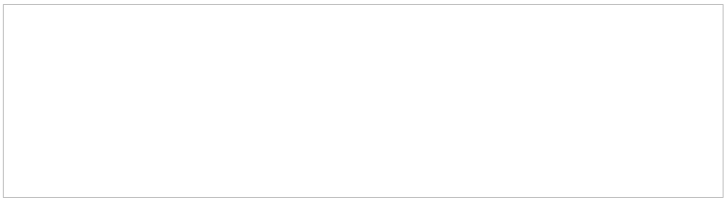
选择安全a高级（自定义设置），点击设置按钮。



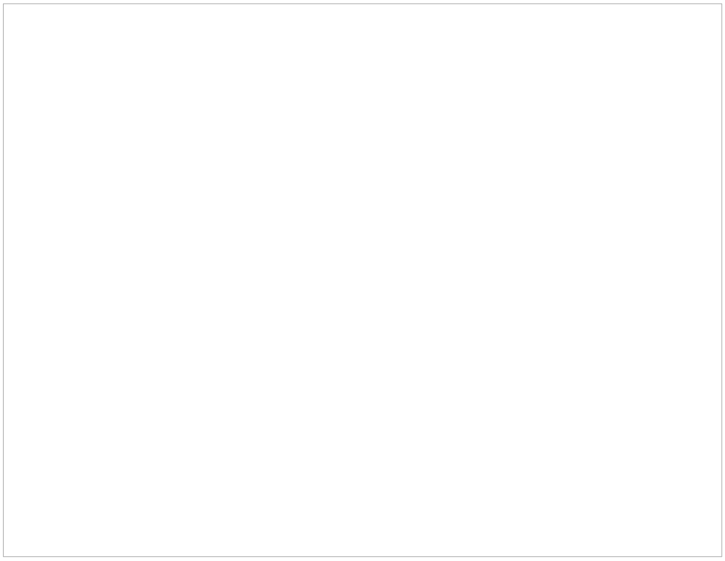
选择认证方式，建议除最后一项外全部勾选。
【说明】：Windows默认的认证方式为MS-CHAP，可以兼容我司的CHAP认证方式。但如果在虚模板里面配置的ppp authentication-mode不是chap，则必须在上面勾选相应协议。

四、 测试结果





拨号成功后，L2TP虚拟网卡获得地址192.168.1.4。



Ping内网地址3.3.3.3，可以ping通。

五、　故障排查

1，错误800：不能建立VPN连接

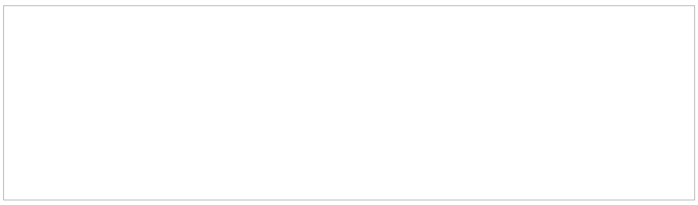
原因分析：此错误表示Windows无法和VPN设备建立连接。

解决方法：首先通过ping VPN地址来确定路径是否可达。如果可以ping通网关，但还是提示800错误，请确认是否已经修改注册表(禁用IPSec，见2.1部分)，注意修改注册表后必须重启windows主机。

2，错误781：连接需要证书

原因分析：未禁用证书方式的IPSec
解决方法：修改注册表，禁用证书方式的IPSec（见2.1部分）。

3， 错误741：本地计算机不支持所要求的数据加密类型



原因分析：客户端所配置的认证协议不包含VPN的认证协议，例如VPN配置了PAP验证，但客户端还是默认的MS-CHAP认证。
解决方法：在VPN连接的“安全à高级(自定义设置)”部分可以更改(见2.2最后部分)。