

IPSEC 配置文档

V 1.1

客服部

深圳市磊科实业有限公司



版本控制

版本号	修改说明	修改人	修改时间
V1.1	初次撰写	Quhy	2013.04.8



目 录

第 1 章 IPSEC VPN 组网.....	1
1.1 组网拓扑图	1
1.2 适用范围	1
第 2 章 磊科 IPSEC VPN 配置.....	2
2.1 网对网模式	2
2.1.1 服务器模式	2
2.1.2 对等模式	4
2.1.3 IPSEC VPN 状态显示.....	5
2.2 点对网模式	6
2.2.1 服务器配置	6
2.2.2 XP 系统创建 VPN 拨号连接	6
2.2.3 Win7 系统创建 VPN 拨号连接.....	10



第1章 IPSEC VPN 组网

1.1 组网拓扑图

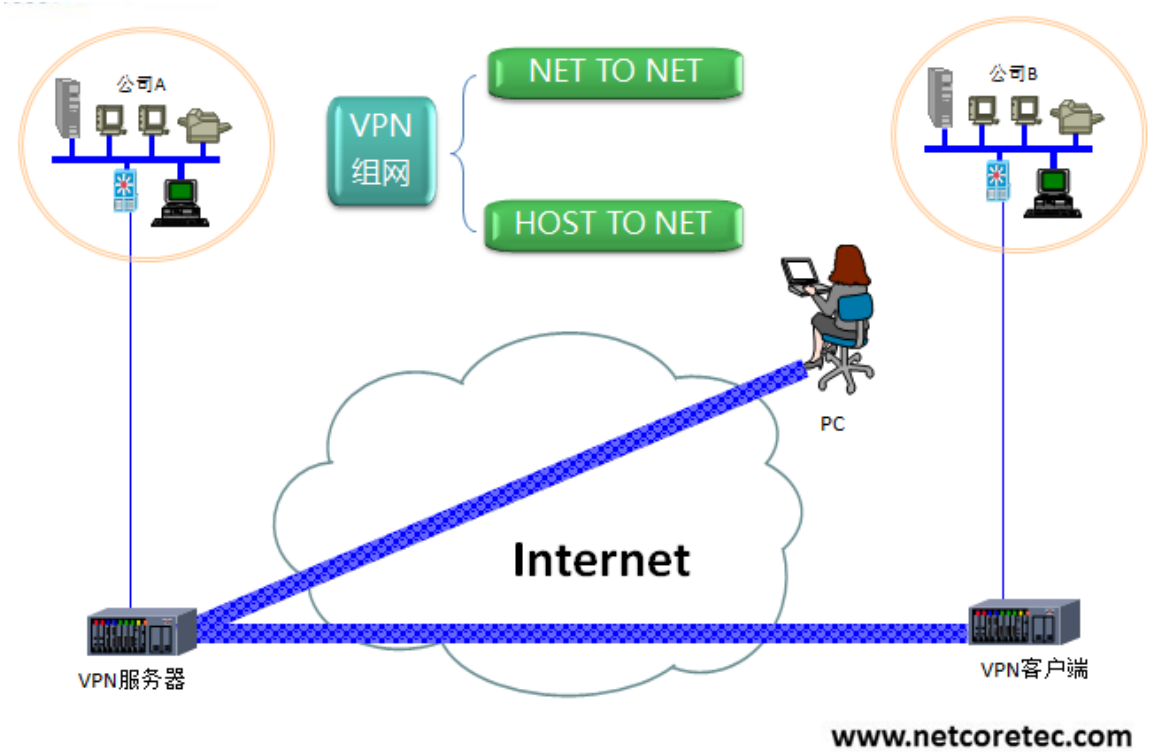


图 1

如上示意图，常见的 VPN 组网方式有两种：

- 1. 子网和子网通过 IPSEC VPN 互联，下文简称网对网模式
- 2. 主机和子网通过 IPSEC VPN 互联，下文简称点对网模式

1.2 适用范围

适用的产品型号包括但不限于：286、286E、288、289E、255V、256、256P、266、266E、268。



第2章 磊科 IPSEC VPN 配置

2.1 网对网模式

这种模式常用于总公司和分公司之间的 VPN 互联

该文档以 NR286 做对等模式(内网 192.168.1.0/24)、NR289-E(内网 192.168.10.0/24)做服务器模式演示。

2.1.1 服务器模式

一、进入配置界面，选择“VPN”--“IPSEC 设置”。



The screenshot shows the 'IPSec设置' (IPSec Settings) configuration page. The '状态' (Status) is set to '启用' (Enabled). The '名称' (Name) is 'admin'. The '认证模式' (Authentication Mode) is 'PSK'. The '密码' (Password) is masked with dots. The '模式' (Mode) is '服务器模式' (Server Mode). The '外出接口' (Outgoing Interface) is 'WAN1'. The '对端IP地址' (Peer IP Address) is '0.0.0.0'. The '本地子网1' (Local Subnet 1) is '192.168.10.1' with a mask of '255.255.255.0'. The '对端子网1' (Peer Subnet 1) is '192.168.1.1' with a mask of '255.255.255.0'. There are buttons for '内网IP' (Intranet IP) and '(可选)' (Optional).

图 2

状态：选择启用，IPSec 下方的配置才会生效。



名称：为该 IPSEC 服务器设置相应的名称，方便记忆。

认证模式：即 IPSEC 的加密方式。选择 PSK 模式则填写预共享密码，对等模式拨号时需要填入该密；选择 Rsa 则在右边 Rsa 密码设置里面点击生成。

模式：由于本端是服务器，故此处选择“服务器模式”。

外出接口：选择你连接 IPsec 的 WAN 口。

本地子网：填写本端路由器 LAN 口网段及子网掩码，此处为 192.168.10.1。

对端子网：填写对端路由器 LAN 口网段及子网掩码，此处为 192.168.1.1。

二、若有多个对等模式同时拨入本服务器，则需要选择“高级设置”，填入其他对等模式的内网 IP 网段。最多可以支持三个对等模式同时拨入，其他参数强烈建议保持默认。具体界面如下图所示：



高级设置

本地子网2：	<input type="text"/>	掩码：	<input type="text"/>	(可选)
本地子网3：	<input type="text"/>	掩码：	<input type="text"/>	(可选)
对端子网2：	<input type="text"/>	掩码：	<input type="text"/>	(可选)
对端子网3：	<input type="text"/>	掩码：	<input type="text"/>	(可选)
本地ID：	<input type="text"/>			(可选)
对端ID：	<input type="text"/>			(可选)
协商模式：	<input checked="" type="radio"/> 主动模式	<input type="radio"/> 侵略模式	(仅特殊情况使用)	
通道模式：	<input checked="" type="radio"/> 隧道模式	<input type="radio"/> 传输模式	(仅特殊情况使用)	
阶段一：	加密算法 <input type="text" value="自动"/>	认证算法 <input type="text" value="自动"/>	DH group <input type="text" value="自动"/>	
协议：	<input checked="" type="radio"/> ESP(支持加密)	<input type="radio"/> AH	(仅特殊情况使用)	
阶段二：	加密算法 <input type="text" value="自动"/>	认证算法 <input type="text" value="自动"/>	DH group <input type="text" value="自动"/>	
PFS：	<input checked="" type="radio"/> 开启	<input type="radio"/> 关闭		
DPD：	<input type="text" value="60"/>	秒		

图 3



由于本例中只有一个对等模式，故不需要设置“高级设置”。

2.1.2 对等模式

进入配置界面，选择“VPN”--“IPSEC 设置”



The screenshot shows the 'IPSec设置' (IPSec Settings) configuration page. The settings are as follows:

- 状态 (Status): 启用 (Enabled)
- 名称 (Name): admin
- 认证模式 (Authentication Mode): PSK (selected), RSA
- 密码 (Password): [Redacted]
- 模式 (Mode): 对等模式 (Peer Mode) (selected), 服务器模式 (Server Mode)
- 外出接口 (Outgoing Interface): WAN1
- 对端IP地址 (Peer IP Address): [Redacted] (可输入域名和IP地址, 0.0.0.0代表任意地址)
- 本地子网 (Local Subnet): 需要通过IPSec加密保护的源IP范围, 网对网时需要设置。
- 本地子网1 (Local Subnet 1): 192.168.1.1 掩码: 255.255.255.0 (可选) [内网IP]
- 对端子网 (Peer Subnet): 需要通过IPSec加密保护的目的地IP范围, 一般为对端设备内网网段。
- 对端子网1 (Peer Subnet 1): 192.168.10.1 掩码: 255.255.255.0 (可选)

图 4

认证模式：必须与服务器设置的认证模式一致。

密码：必须与服务器端密码一致。

模式：选择“对等模式”。

对端 IP 地址：填入服务器端 IP 地址。



2.1.3 IPSEC VPN 状态显示

一、在服务器端，点击“IPSEC 状态”，查看 IPSEC VPN 连接状态，如下图所示：



图 6

二、在对等模式端，点击“IPSEC 状态”，查看 IPSEC VPN 连接状态，如下图所示：



图 7

三、正常访问对端网段：

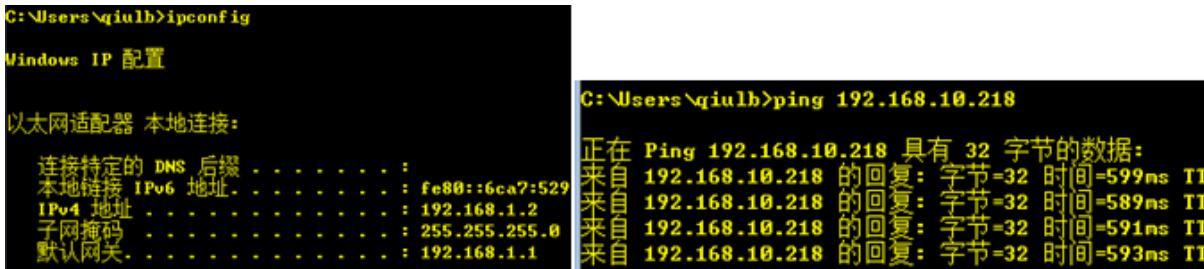


图 8



2.2 点对网模式

这种模式常用于员工出差在外和公司之间的安全互联。

该文档以 NR289-E(内网 192.168.10.0/24)做服务器演示。

2.2.1 服务器配置

请参考本文档 [2.1.1](#) 章节

2.2.2 XP 系统创建 VPN 拨号连接

第一步、打开网络连接：

如果桌面上没有“网上邻居”，依次点击“开始”菜单→“设置”→“控制面板”→“网络连接”；如果桌面上有“网上邻居”，直接用鼠标右键点击“网上邻居”，再点击“属性”；

第二步、创建 VPN 连接：



图 8



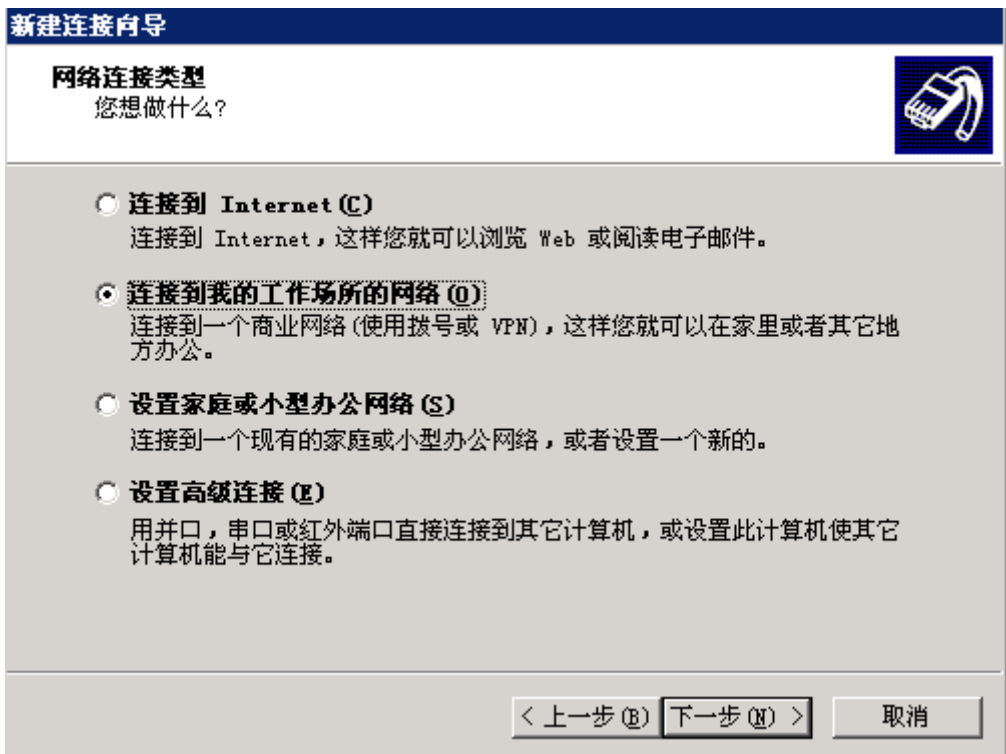


图 9

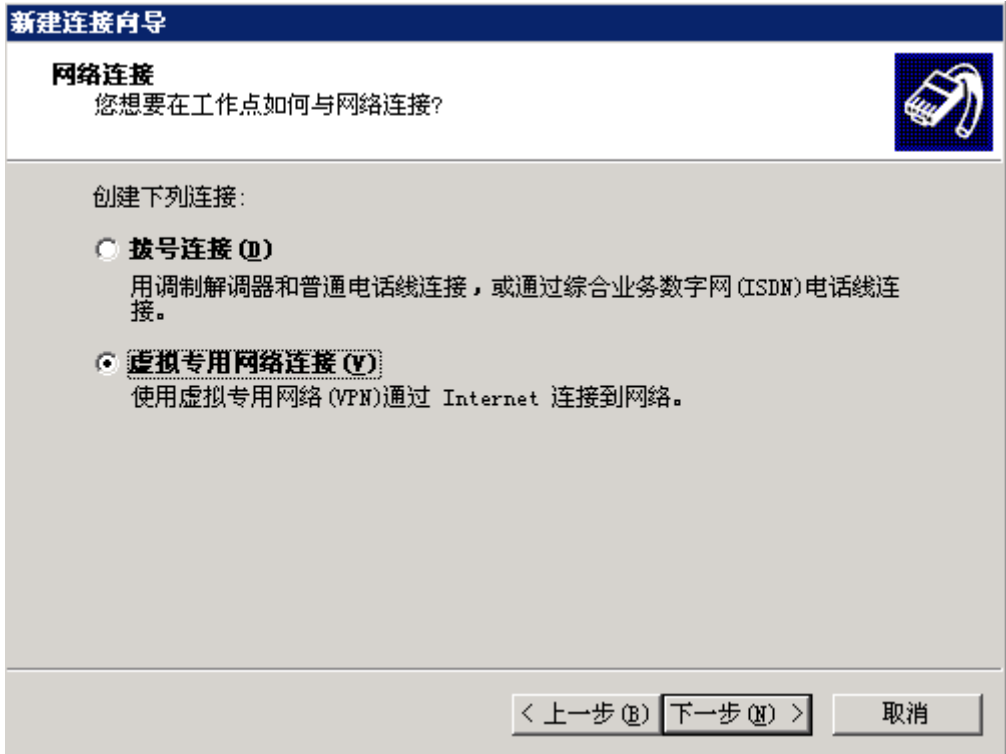


图 10



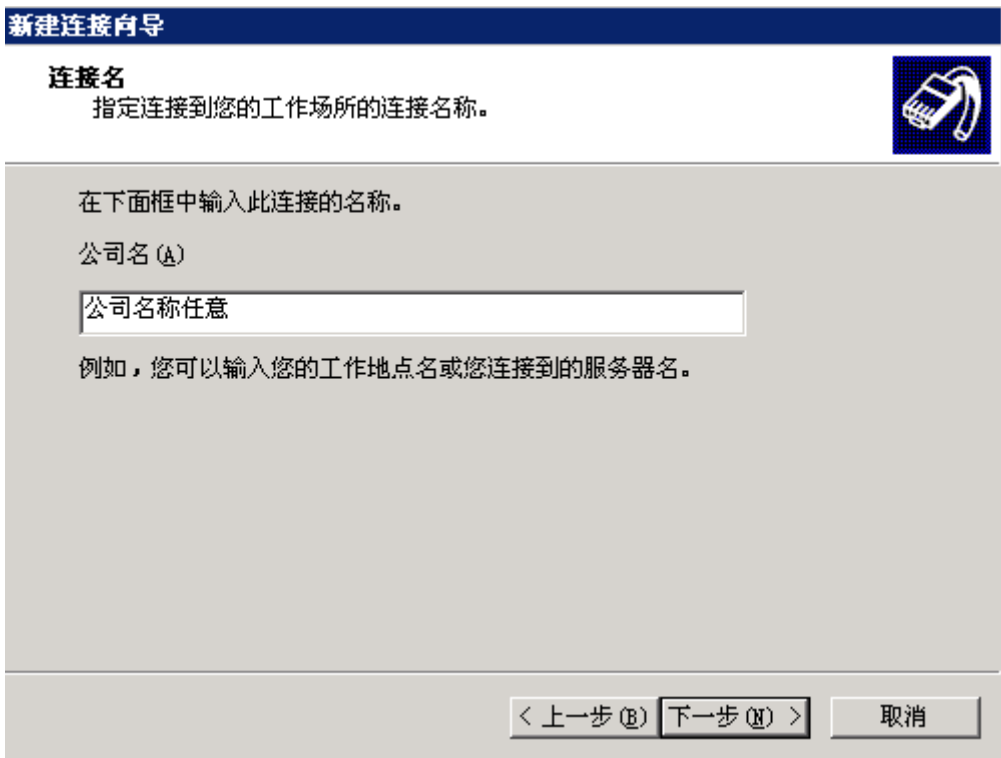


图 11

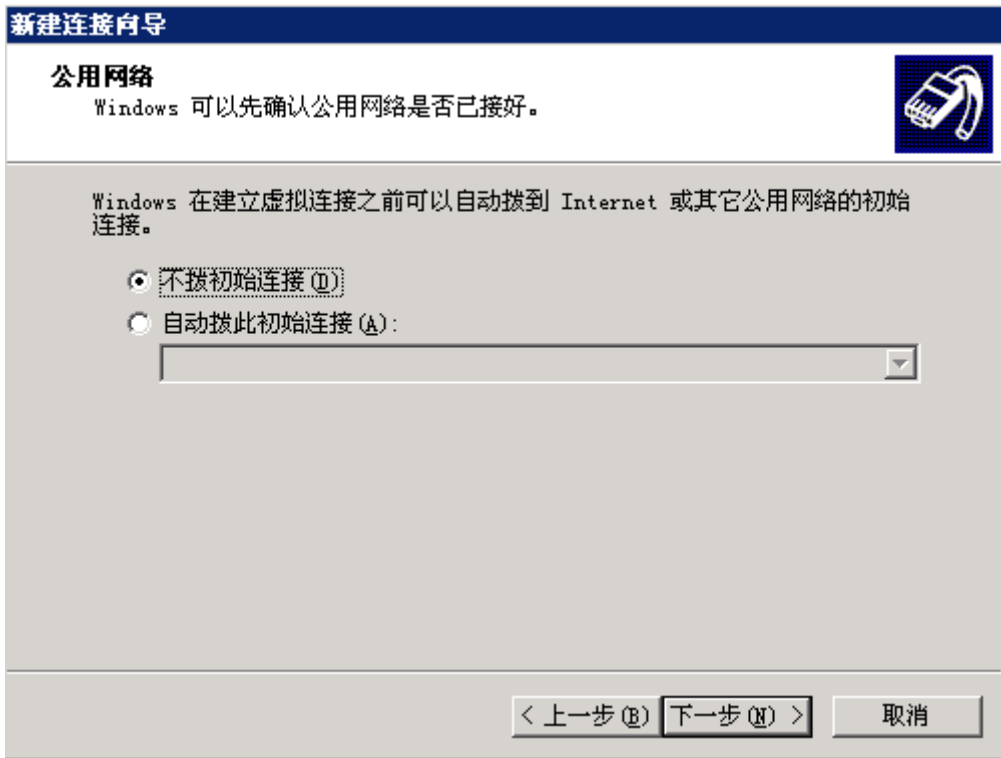


图 12



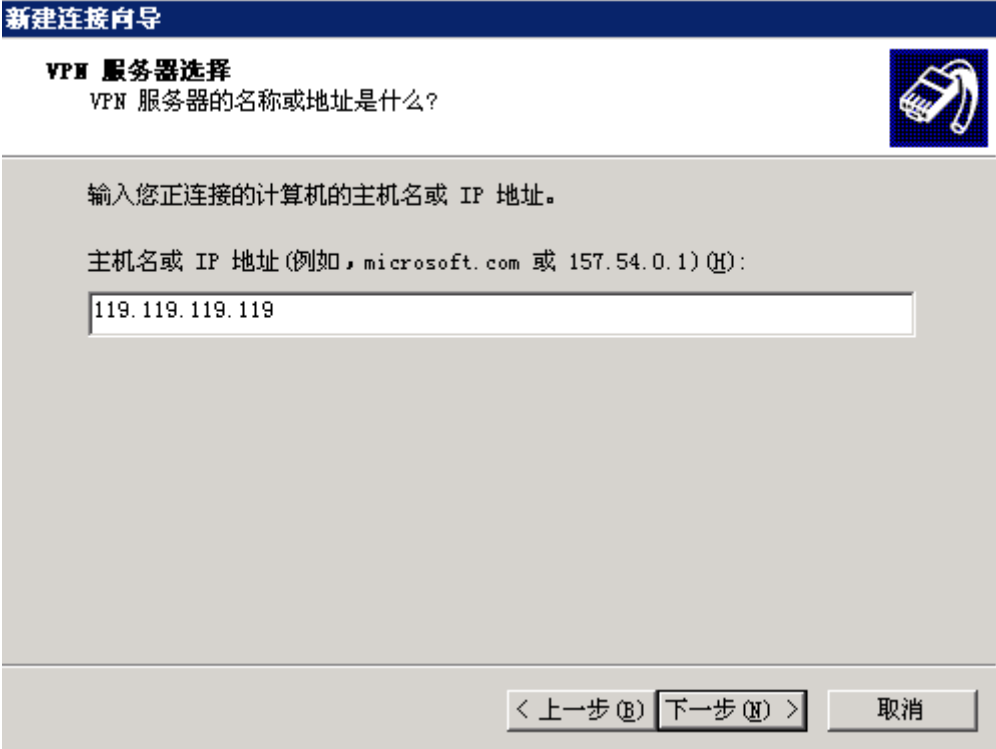


图 13

此处填写 VPN 服务器的公网 IP，继续点击下一步，即可完成新建连接

第三步、开始连接：双击 VPN 拨号连接（类似于宽带拨号连接），输入帐号和密码即可连接。

如果需要修改 VPN 服务器的 IP，右键点击属性修改



图 14

备注：电脑单机 VPN 拨号，如果连接不成功，可根据第三步步骤，选择“选项”，VPN 模式修改为“IPSEC”。若依旧拨号不成功，会有错误代码提示，根据对应代码可以到网上搜索连接失败的



原因及解决办法

2.2.3 Win7 系统创建 VPN 拨号连接

第一步、打开网络和共享中心：

如果桌面上没有“网络”图标，依次点击“开始”菜单→“控制面板”→“查看网络状态和任务”；如果桌面上有“网络”，直接用鼠标右键点击“网络”，再点击“属性”；

第二步、创建 VPN 连接：



图 15





图 16



图 17





图 18



图 19

点击创建，完成连接。

第三步、开始连接：双击 VPN 拨号连接（类似于宽带拨号连接），输入帐号和密码即可连接。如果需要修改 VPN 服务器的 IP，右键点击属性修改



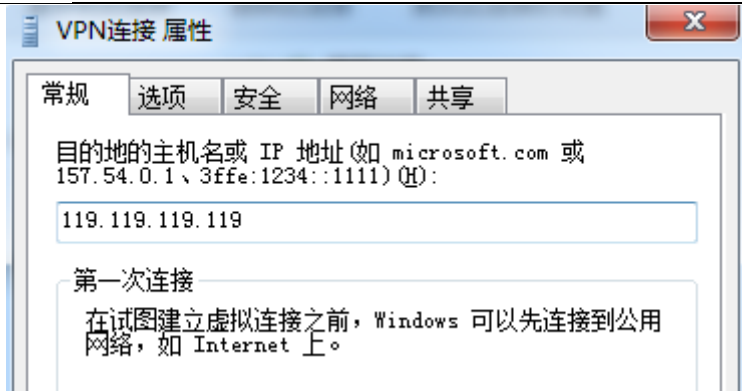


图 20

备注：电脑单机 VPN 拨号，如果连接不成功，可根据第三步步骤，选择“选项”，VPN 模式修改为“IPSEC”。电脑单机 VPN 拨号，如果连接不成功，会有错误代码提示，根据对应代码可以到网上搜索连接失败的原因及解决办法

