东软·VPN安全网关

VPN Security Gateway

用户手册

东软集团有限公司

关于本手册

版权声明

信息更新

本文档仅用于为最终用户提供信息，并且随时可由东软更改或撤回。

免责条款

根据适用法律的许可范围，东软按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，东软都不会对最终用户或任何第三方因根据说明文档使用VPN安全网关造成的任何直接或间接损失或损坏负责，即使东软明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

阅读对象

本文的读者对象为企业IT决策人员、东软VPN安全网关的使用用户、东软的合作伙伴等具有一定网络安全知识的有关人员。

目 录

1. 导读

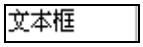
1-1 界面风格

NEUSOFT　VPN 系列产品的 WEB 管理界面遵循浏览器的习惯用法，如下图所示：

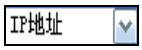
 单选框：选中代表只选择此项。

 复选框：选中代表此选项所述功能被选中。

命令按键：单击则执行该按钮的动作。



文本框： 输入相关参数。



下拉列表： 通过下拉列表可以找到可选择的项。

1-2 基本约定

◆ 表示基本参数，描述参数基本涵义。如果界面中该参数后有“*”表示该参数为必填项。

● 表示按钮，描述操作动作。

✧ 表示说明，提出重点注意事项。

1-3 出厂配置

本路由器默认出厂配置如下表所示，管理员可以根据自己需求对相应参数进行修改，也可以通过超级终端连接 NEUSOFT　VPN 后，使用“mode clear”命令恢复默认配置。

admin 密码	neusoft
enable 密码	neusoft
超时时间	300 秒
默认 lan 口地址	192.168.0.1
默认 func 网口地址	1.1.1.1

1-4 技术规格

- 基于 IPSec 国际标准协议
- 完善的路由功能
- NAT 地址转换技术保护内部网络
- 内置 DHCP 服务器
- 内置 DNS 转发
- 目录服务器
- 高性能防火墙
- 内置 PPPOE
- SSH 终端控制
- SSL/PPTP、WebSSL/WebTSSL 远程登陆

1-5 指示灯含义

指示灯	描述
Lan	局域网指示灯，该灯闪烁表明与局域网有数据通讯。
Wan	广域网指示灯，该灯闪烁表明与广域网有数据通讯。
Func	网络指示灯，根据配置可能会是局域网或广域网指示灯。
System	系统指示灯，在有系统读写动作发生时将闪烁。
Power	电源指示灯，该灯亮表明设备电源已接通。

1-6 硬件接口

接口性质	功能描述
Power	电源接口。
Lan 口	局域网口。
Wan 口	广域网口。
Function 口	功能口，根据配置需求可以配置成 WAN1 口或 LAN 口。
Console 口	可通过 Console 线连接到客户机，进行配置。
Com 口	根据需要连接，可连接 DB-9Console 或 Modem。
Dmz 口	非军事化安全区域

1-7 环境参数

- 输入电压：220V
- 使用温度环境：0~40℃，使用环境湿度：10~85%（相对，非凝结）

2. 安装前的准备

2-1 注意事项

基于 NEUSOFT VPN 产品的广泛应用及其在数据通信网络中担当的重要作用，在安装和使用过程中，特提出如下安全建议：

- 请将安全网关放置在远离潮湿或远离热源的地方。
- 请确认安全网关已经正确接地。
- 请在安装维护过程中佩戴防静电手腕，并确保防静电手腕与皮肤良好接触。
- 请不要带电插拔配置口(console)、备份口(COM)的电缆。
- 建议用户使用 UPS(uninterrupted power supply，不间断电源)

2-2 辅助设施

在配置本产品之前，您需要配备一台电脑。

若采用 Web 方式配置需直接通过单机连入设备 LAN 口或 FUNC 口。若习惯使用 Console 方式配置，则需要该电脑装有超级终端软件，同时具有至少一个 9 针的 Com 接口。如果您运行的是 Microsoft 公司的 Windows95、Windows98 或 Windows2000 系统，需要检查其是否安装了“超级终端”程序。

3. NEUSOFT VPN 安装

3-1 硬件连接方法

第一步：打开 NEUSOFT VPN 包装，取出设备、电源线、网线、配置线。

第二步：确认电源开关为“OFF”状态，用电源线将 POWER 口接上电源。

第三步：用 RJ45 直通线将路由器设备的 LAN 口连接到本地局域网（Swich 或 Hub）中。

第四步：将公网网线连接到 VPN 的 WAN 口上。确认 NEUSOFT VPN 的 WAN 口同 ADSL Modem，DDN 或者 Cable Modem 的连接方式。由于各种设备之间区别较大，因此我们建议用户首先使用级联线，如果发生问题，可以再用正常网线试验（注意请将 ADSL Modem 设置成桥接模式或者恢复成出厂默认配置，同时将 ADSL Modem 断电重启）。

第五步：如果用 Console 方式配置 VPN，就用 RS232-RJ45 配置线将 VPN 的 Console 口与控制终端（电脑的 Com 口）互联。

以上连接完成，硬件安装即完成。打开设备电源，设备启动后，可以看到电源指示灯亮。若用 Console 方式配置，在电脑中启动超级终端应用程序，配置好终端参数，会看到有关 NEUSOFT VPN 的启动信息和登陆提示。

3-2 安装后的检查

在 NEUSOFT VPN 系列产品安装过程中，加电前均要进行安装检查，检查事项如下：

- ◆ 请检查 NEUSOFT VPN 产品周围是否留有足够的散热空间，机柜是否稳固。
- ◆ 检查电源线所接电源与要求的电源是否一致。
- ◆ 检查 NEUSOFT VPN 与配置终端等其它设备的连接关系是否正确。
- ◆ 两根 RJ45 的网线中一根是直通线，一根是交叉线。同类设备相连用交叉线，不同类设备用直通线。
- ✧ NEUSOFT VPN 产品安装完毕后的检查非常重要，因为安装的牢固与否、接地良好与否、电源匹配与否，将直接关系到产品的正常使用。

4. NEUSOFT VPN 快速配置指南

4-1 网络配置

首先设置 PC 机的 IP 地址、子网掩码。NEUSOFT VPN 默认的 Lan 口 IP 地址是 192.168.0.1，Function 口默认 IP 地址为 1.1.1.1。配置之前，必须确保用户的电脑与 NEUSOFT VPN 设备在同一个网段。如果用 Lan 口登陆，则可将 PC 机的 IP 地址设为：192.168.0.×（但不能是 192.168.0.1），子网掩码为：255.255.255.0；如果用 Function 口登陆，则可将 PC 机的 IP 地址设为：1.1.1.×，子网掩码同样为 255.255.255.0。

4-2 Web 管理登陆

在浏览器里输入下列地址：http://192.168.0.1:8080（Lan 口连接）或 http://1.1.1.1:8080（Function 口连接），进入连接到 VPN 设备。

输入用户名、密码（NEUSOFT 默认用户名/密码为 admin/neusoft ）用户名和密码均为小写，点击“登陆”，语言可以选择“中文”或“英文”。进入主界面。

4-3 三种广域网接入配置

进入登陆页面后，管理员就可以开始配置网络信息了，根据上网方式的不同，可自由选择“PPPoE 客户端(ADSL)”、“固定 IP（专线）”或“DHCP（有线通）”三种接入类型。

4-3-1 PPPoE 客户端(ADSL)配置

单击左边菜单中的“快速配置”，进入快速配置向导页面。如下图（图 4－1）：

图 4－1 快速配置

选中“PPPoE（ADSL）类型”，点击“下一步”进入，填写 ADSL 帐号/密码信息。如下图（图 4－4）：

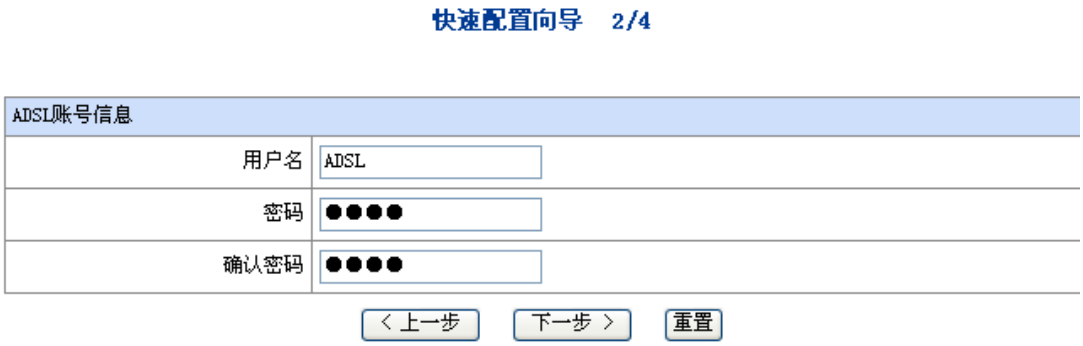


图 4－4 ADSL 配置 1

点击“下一步”，进入 LICENSE 设置。如下图（图 4－2）：

图 4－2 ADSL 配置 2

- VPN 组名：东软公司提供的 8 位字母开头的字母字符串名称。
- 节点名：东软公司提供的不超过 7 位字母开头字符串节点名称。
- LICENSE：东软公司提供的 16 位随机字符串。
- NAT-T：东软产品支持 NAT-T 功能，当路由器放在局域网内也能通过这一功能与另一端的 VPN 路由器建立 VPN 隧道，在用户网络环境较为复杂或者没有专门的公网线路给 VPN 设备单独使用的情况下，该功能将发挥作用。用户可以根据自己的网络环境来选择是否开启这一功能。但如果 VPN 设备不在局域网环境中，请不要选取此选项。

点击“下一步”，进入局域网 IP 设定。如下图（图 4－3）：

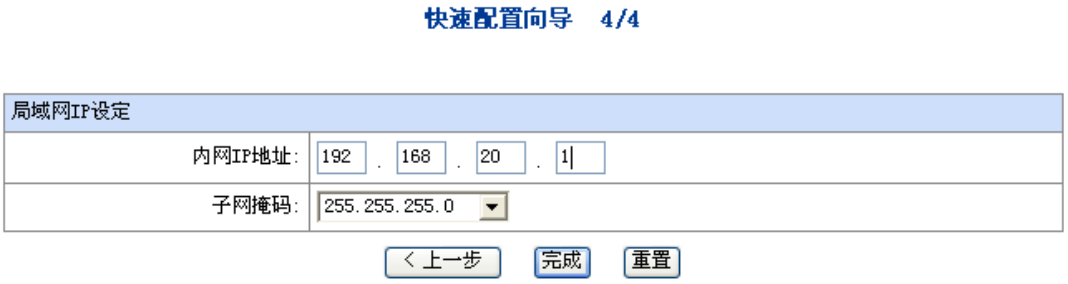


图 4－3 ADSL 配置 3

- ◆ 内网 IP 地址：VPN 设备的 Lan 口 IP。
- ◆ 子网掩码：子网掩码提供多种可选，用户根据情况自行选择。
- ● 上一步：返回上一步操作。
- ● 完成：结束 ADSL 方式配置，配置参数生效。
- ● 重置：恢复到修改前的配置参数。
- ✧ 说明：

  各个 VPN 节点必须在不同的网段，建议管理员在安装前对需要建立 VPN 连接的各 LAN 作整体 IP 地址规划。

  完成以上简单配置操作后，NEUSOFT VPN 即可以正常工作了。如果需要实现更多高级功能，请参考 NEUSOFT VPN 产品详细配置手册。

4-3-2 固定 IP 地址(专线)配置

大部分公网接入方式多为光纤用户，运营商会提供一个或多个固定的公网 IP 地址，单击左边菜单中的“快速配置”，进入快速配置向导页面,选中“固定 IP 地址(专线)”，进入固定 IP 地址配置。如下图（图 4－4）：

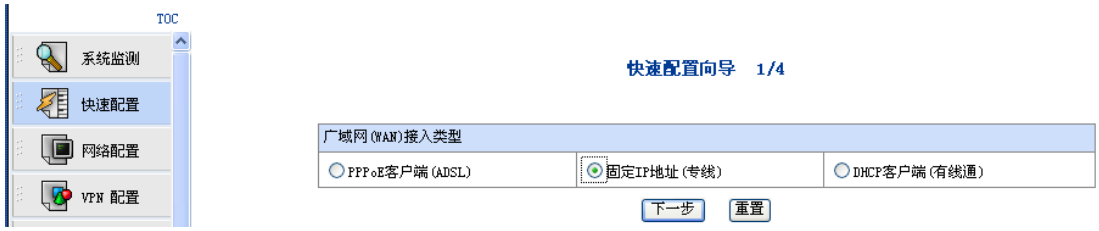


图 4－4 固定 IP 地址（专线）配置 1

点击“下一步”进入“固定 IP 地址(专线)”界面。如下图（图 4－8）：

图 4－8 固定 IP 地址（专线）配置 2

- 本地 IP 地址：VPN 设备的 Wan 口 IP。
- 网关 IP 地址：由运营商提供的网关地址。
- 子网掩码：子网掩码提供多种可选，用户根据运营商提供的线路申请确认单选择相应的子网掩码。

点击“下一步”，进入“LICENSE 设置”界面。如下图（图 4－9）：

图 4－9 固定 IP 地址（专线）配置 3

- VPN 组名：东软公司提供的 8 位字母开头的字母字符串名称。
- 节点名：东软公司提供的不超过 7 位字母开头字符串节点名称。
- LICENSE：东软公司提供的 16 位随机字符串。
- NAT-T：东软产品支持 NAT-T 功能，当路由器放在局域网内也能通过这一功能与另一端的 VPN 路由器建立 VPN 隧道，在用户网络环境较为复杂或者没有专门的公网线路给 VPN 设备单独使用的情况下，该功能将发挥作用。用户可以根据自己的网络环境来选择是否开启这一功能。但如果 VPN 设备不在局域网环境中，请不要选取此选项。

点击“下一步”，进入局域网 IP 配置界面。如下图（图 4－10）：

图 4—10 固定 IP 地址（专线）配置 4

- ◆ 内网 IP 地址：VPN 设备的 Lan 口 IP。
- ◆ 子网掩码：子网掩码提供多种可选，用户根据情况自行选择。
- ● 上一步：返回上一步操作。
- ● 完成：结束固定 IP 方式配置，配置参数生效。
- ● 重置：恢复到修改前的配置参数。

完成以上简单配置操作后，NEUSOFT VPN 即可以正常工作了。如果需要实现更多高级功能，请参考 NEUSOFT VPN 详细配置手册。

4-3-3 DHCP 客户端(有线通)配置

单击左边菜单中的“快速配置”，进入快速配置向导 1/4 界面。如下图（图 4—11）：

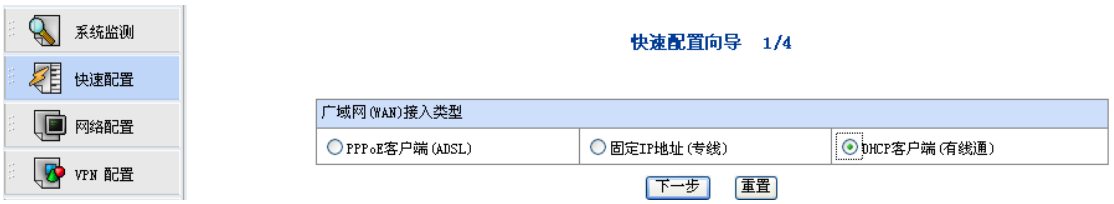


图 4—11 DHCP 客户端（有线通）配置 1

选中“DHCP 客户端（有线通），进入 DHCP 快速配置向导 2/4 界面。如下图（图 4—12）：

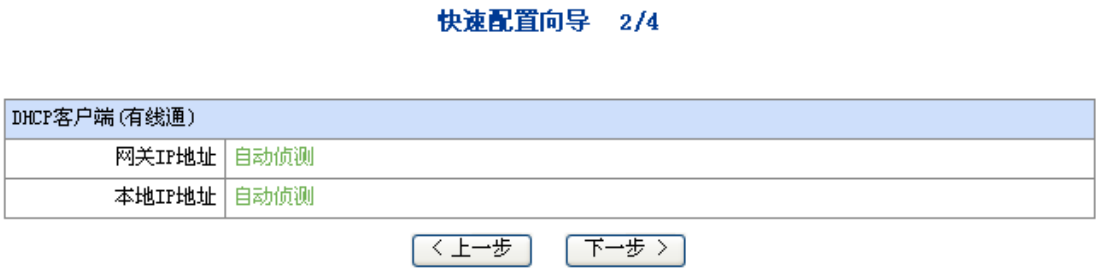


图 4—12 DHCP 客户端（有线通）配置 2

这里网关地址和本地 IP 地址均可自动侦测获得，单击“下一步”，进入 LICENSE 设

定。如下图（图 4－13）：

图 4－13 DHCP 客户端（有线通）配置 3

- VPN 组名：东软公司提供的 8 位字母开头的字母字符串名称。
- 节点名：东软公司提供的不超过 7 位字母开头字符串节点名称。
- LICENSE：东软公司提供的 16 位随机字符串。
- NAT-T：东软产品支持 NAT-T 功能，当路由器放在局域网内也能通过这一功能与另一端的 VPN 路由器建立 VPN 隧道，在用户网络环境较为复杂或者没有专门的公网线路给 VPN 设备单独使用的情况下，该功能将发挥作用。您可以根据自己的网络环境来选择是否开启这一功能。但如果 VPN 设备不在局域网环境中，请不要选取此选项。

点击“下一步”，进入局域网 IP 配置。如下图（图 4－14）：

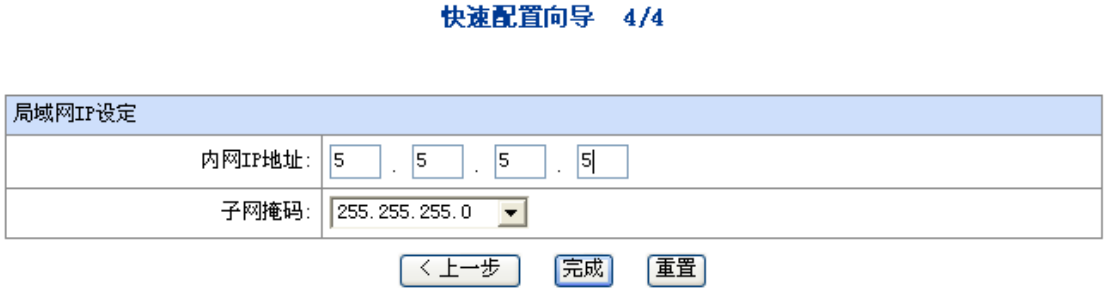


图 4－14 DHCP 客户端（有线通）配置 4

- 上一步：返回上一步操作。
- 完成： 结束 DHCP 客户端方式配置，配置参数生效。
- 重置： 恢复到修改前的配置参数。

完成以上简单配置操作后，NEUSOFT VPN 即可以正常工作了。如果需要实现更多高级功能，请参考 NEUSOFT VPN 详细配置手册。

4-4 验证配置

完成上述三种广域网接入方式中任意一种配置操作后，可通过“系统监测”模块中“网络信息”和“VPN”子模块来查看当前配置是否生效。

4-4-1 网络信息验证

在“网络信息”子模块中可对当前设备的公网口、局域网口、功能口及 DNS 的相关信息一目了然。如下图（图 4－15)：

图 4－15 网络信息

4-4-2 VPN 信息验证

在“VPN”模块中，可以看到本地 VPN 网段信息，以及对端公网地址、VPN 网段和各自加密的协议认证信息。通过此信息列表，可以一目了然的看到与本设备搭建的 VPN 隧道连接的各节点状态。如下图（图 4－16）：

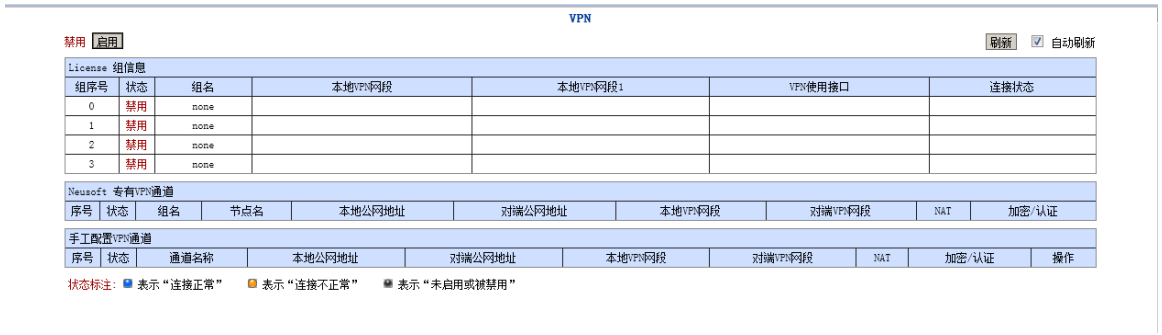


图 4－16 VPN 信息

4-5 移动用户 SSL/PPTP 配置

NEUSOFT VPN 支持“SSL”方式和“PPTP、l2tp”方式接入，主要用于移动用户连接NEUSOFT VPN时需要的用户名和密码，以及是否分配给移动用户虚拟的IP地址信息。

4-5-1 SSL 用户配置

单击左边菜单“VPN”配置，选择“SSLVPN 配置”子模块，进入“用户管理”界面。如下图（图 4－17）：

图 4－17 SSL 设置

第一步：添加 SSL 用户名和密码，其中“引号”、“逗号”、“空格”、“\”、“-”、“|”、“%”、“*” 这八个符号不允许在用户名和密码中出现，用户名严格区分大小写。

第二步：点击“提交”，添加的用户即可采用移动客户端拨号方式连接到内部局域网。

如果您需要实现更多移动用户功能，请参考 NEUSOFT VPN 产品详细配置手册。

4-5-2 PPTP/L2TP 用户配置

单击左边菜单“VPN”配置，选择“PPTP/L2TP”子模块，进入“PPTP 配置/L2TP 配置”界面。如下图（图 4－18）：

图 4－18 PPTP 设置

第一步：选择模式，可分为“池模式”和“固定模式”，在两种模式只能选择一种，切换模式后，用户列表信息将清空，建议谨慎使用。

第二步：添加 PPTP/L2TP 用户名和密码，其中“引号”、“逗号”、“空格”、“\”、“-”、“|”、“%”、“*”这八个符号不允许在用户名和密码中出现，用户名严格区分大小写。如

果选择“固定模式”，则需要填写指定 IP 地址，池模式则不用，增强认证选择“密码验证”。

第三步：点击“提交”，以上基本操作配置完成后，在 PPTP 用户列表中可以看到添加的用户信息。添加的用户即可采用移动客户端拨号方式连接到内部局域网。

注：在 pptp 用户列表的用户名，在拨 pptp 或 l2tp 都是通用的。

4-5-3 客户端 SSL/PPTP/l2TP 登陆

登陆东软客户端，通过虚拟拨号连接到 NEUSOFT VPN 设备上，从而接入内部局域网。SSL 用户与 PPTP 用户连接方式一致，这里例举 SSL 用户连接方法，详细方法如下：

第一步：双击运行下载到本机的移动客户端，会自动生成一个移动客户端快捷方式图标，并弹出客户端对话框，在路由器地址栏填写需要连接的路由器地址，输入 SSL 用户名和密码后，点击“登陆”，在屏幕右下角出现“开始设置虚拟 IP”界面。如下图（图 4－19）：

图 4－19 客户端运行

第二步：用户登陆成功后，在屏幕右下角出现 VPN 客户端状态框，双击屏幕右下角移动客户端小图标，可以看见 VPN 连接状态。点击“断开”，您可以断开 VPN 连接。如下图（图 4－20）：

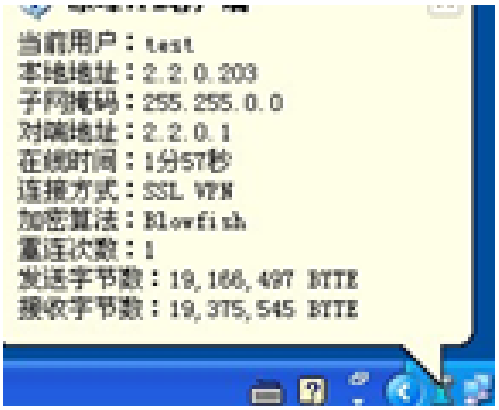


图 4－20 客户端登陆成功

第三步：打开本机“开始—运行”菜单，输入“cmd”,进入命令行界面，在命令行界面输入“ipconfig”可以看到本机已经获取到一个虚拟局域网 IP 地址 2.2.0.*，此时移动用户可以访问局域网内部资源信息。如下图（图 4－21）：

```
^C
C:\Documents and Settings\iceflow>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.2.0.202
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.0.1

Ethernet adapter 本地连接 2:

        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter 本地连接 4:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 2.2.0.203
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

图 4－21 命令行验证

第四步：选择“SSL 配置”，点击“查看状态”，可以看到 SSL 用户连接状态信息。如下图（图 4－22）：

图 4－22 查看状态

4-6 WebSSL 用户配置与登陆

WebSSL 用户登陆需要最基本的四个操作过程，分别为用户组创建、WebSSL 基本配置、WebSSL 站点资源发布。

4-6-1 WebSSL 用户配置

Webssl 配置

“webssl 配置”默认状态禁用的，需要启用才可使用。如下图（图 4－25）：

图 4－25 用户组管理配置

WebSSL 配置

第一步：基本配置

WebSSL 配置除包含 WebSSL 所有配置外，还需要进行 WebSSL 池地址设置，如下图（图 4－26）：

图 4－26 WebSSL 池地址设置

第二步：添加站点资源

站点资源添加，如下图（图 4－27）：

图 4－27 WebTSSL 资源发布

第三步：用户管理

单击“用户管理”，选择组名，创建 WebSSL 用户名，密码和增强认证方式（默认为密码认证），点击“提交”即可。如下图（图 4－28）：

图 4－28－1 WebSSL 用户创建

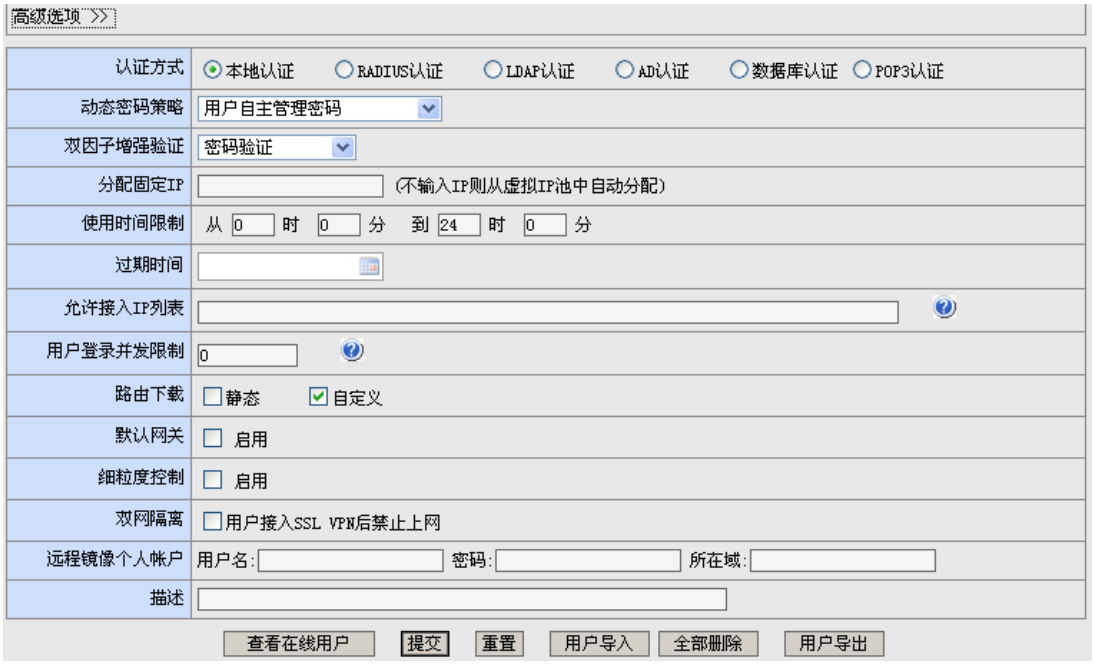


图 4－28－2 WebSSL 高级选项

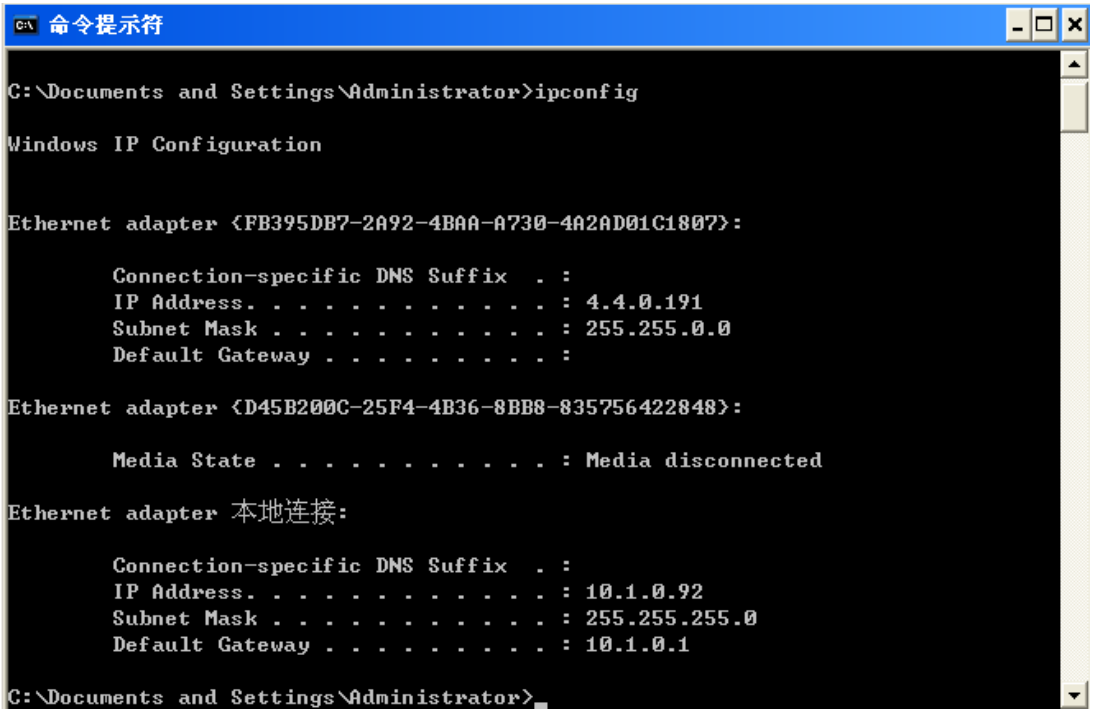
图 4－28－3 WebSSL 用户列表

4-6-2 WebSSL 用户登陆

用户通过 WebSSL 方式登陆后，如下图（图 4－29）：

图 4－29 WebSSL 用户登陆

注：首次登陆成功后，点击“控件”安装 webssl 插件，如需要卸载插件直接点击“卸载”，即可。如上图（图 4-30）：



登录成功之后可以再本地的计算机开始--运行-输入：ipconfig 可以看到获得的虚拟地址。如上图（图 4-31）：

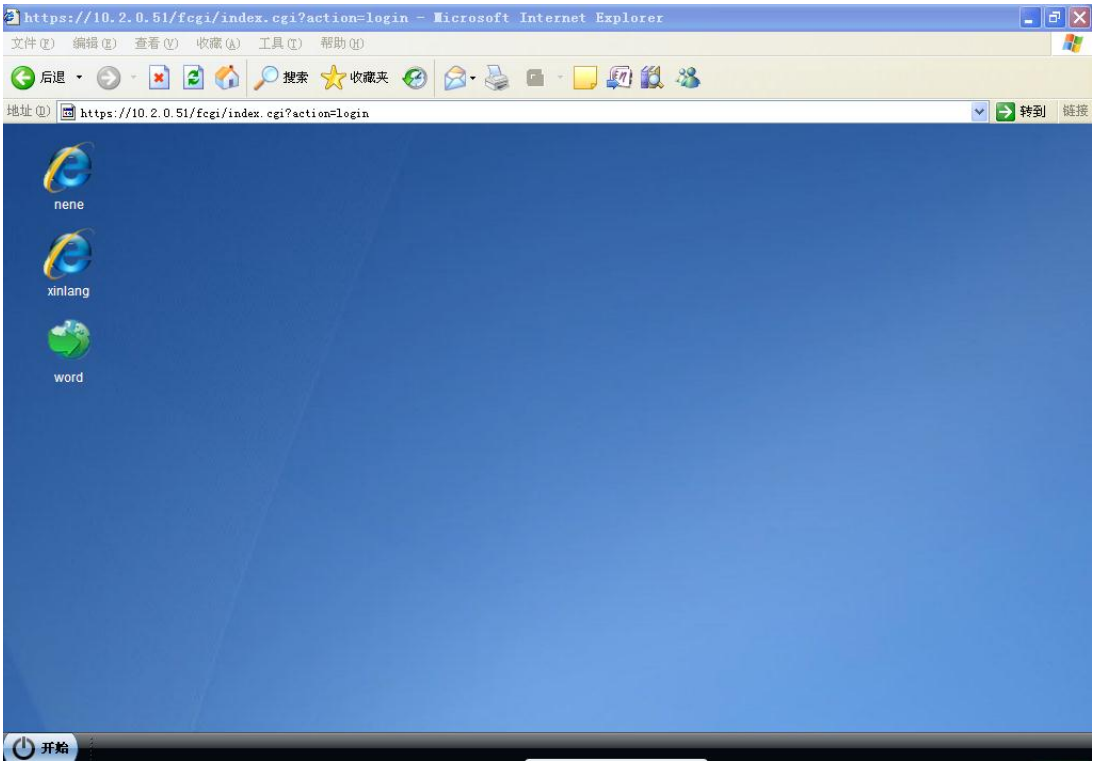


图 4－32 WebSSL 虚拟通道状态

虚拟通道建立成功后，WebSSL 用户即可访问发布的站点资源，WebSSL 用户修改密码、NEUSOFT　VPN Web 详细配置

4-7 网络配置

网络配置请参照快速配置指南 4.1 章节。

4-8 设备配置登录界面

在 IE 浏览器里输入下列地址：http://192.168.0.1:8080（LAN 口连接）或 http://1.1.1.1:8080（Function 口连接），进入连接到 VPN 路由器；

输入用户名、密码（NEUSOFT 默认用户名/密码为 admin/neusoft ）用户名和密码均为小写，点击“登陆”，进入“系统监测”界面。

4-9 系统监测

在“系统监测”模块中，包括以下子模块：“基本信息”、“网络信息”、“VPN”、“移动用户”、“手工 ssl 通道”“流量监控”、“日志”。

4-9-1 基本信息

“基本信息”模块中显示了设备当前时间、启动时间、序列号、软件版本以及当前设备工作中系统的各项资源的消耗情况，包括 CPU 的负载、内存、并发会话连接数等。网络信息

在“网络信息”子模块中管理员可对当前设备的公网口、局域网口、功能口及 DNS 的相关信息一目了然。如下图（图 4－35）：

图 4－3 5 网络信息

4-9-2 VPN

在此模块中，管理员可以看到本地 VPN 网段信息，以及对端公网地址、VPN 网段和各自加密的协议认证信息。通过此信息列表，管理员可以一目了然的看到与本设备搭建的 VPN 隧道连接的各节点状态。如下图（图 4－36）：

图 4－36 VPN 通道信息

4-9-3 移动用户

在“移动用户”子模块中，管理员可以查看以 PPTP 方式拨入的在线用户使用情况，还可以查看以 SSL 拨入和 PPTP 用户登陆时间和隧道类型，并可对其进行断开操作。如下图（图 4－37）：

图 4－37 移动用户信息

4-9-4 流量监控

“流量监控”子模块中包含了“接口流量”和“单机流量”，“接口流量”的主要功能是为了监控路由器各物理接口和逻辑接口出入双向的数据流量。在此模块中，管理员可以

监测到本设备各网口及 VPN 的接收数量、接受速率、发送数量和发送速率等。如下图（图 4－38）：

图 4－38 接口流量

选择“单机流量”，可以对多个网段进行流量监控，如下图（图 4－39）：

图 4－39 单机流量

4-9-5 日志

“日志”体现了本产品的安全管理功能，它记录了系统发生的所有事件，管理员可以根据它来检查错误发生的原因，记录攻击时攻击者留下的“罪证”。管理员可以选择“系统”、“VPN”、“移动用户”、“访问”、“告警”、“错误”、“调试”或“防火墙”来查看相关信息，可以将日志下载到本地保存，也可对本地显示的日志进行清空处理。还可以通过关键字进行搜索。如下图（图 4－40）：

图 4－40 日志

4-10 网络配置

本模块包括以下子配置模块:“公网配置”、“局域网配置”、“功能口配置”、“NAT 配置”、“静态路由配置”、“动态路由配置”、“策略路由配置”、“VRRP 配置”、“公网监测配置”，在前面快速配置完成之后，管理员在日常使用之中可以通过本模块对网络配置进行更详细的调整。

4-10-1 公网配置

单击左边菜单栏中的“网络配置”，进入“公网配置”子模块。

- 状态：系统状态信息，分为“启用”和“禁用”两种。
- 广域网接口:在广域网接口类型中,有 WAN 口和 WAN1 口两种接入方式可供选择(根据产品型号不同可选择的接入方式也不同)。
- 广域网接入类型：在广域网接入类型选项中包括 PPPOE 客户端（ADSL）、固定 IP 地址（专线）、DHCP 客户端（有线通）三种模式。
- PPPOE 客户端（ADSL）：选择“PPPOE 客户端（ADSL）”，填写 ADSL 帐号信息，并自由选择“MTU”为自动或手动，若“MTU”选为“手工”，可自行填写其大小值。用户可以启用公网监测功能来帮助判断公网口的连接状态。填写如下图（图 4－41）：

图 4－41 公网配置 1

- 提交：所做的配置提交成功后即可生效。
- 重置：恢复到修改前的配置参数。

✧ 说明：

最大传输单元（MTU）：网络上传送的最大数据包长度，大部分网络设备的 MTU 缺省值为 1500 字节（MTU 单位为字节），VPN 拨号连接时将自动与对方设备协商，除非特别应用，建议不要修改。

◆ 固定 IP 地址（专线）：选定“固定 IP 地址（专线）”填写固定 IP 相关信息，并可在 WAN 口上绑定多个 IP 地址，还可对绑定 IP 进行增减操作，并可自由选择“MTU”为自动或手动，配置多公网线路时，用户可以启用公网监测功能来帮助判断公网口的连接状态。

◆ DHCP 客户端（有线通）：若是 DHCP 客户端操作，仅选择“MTU”为自动或手动，若“MTU”选为“手工”，可自行填其大小值。管理员可以启用公网监测功能来帮助判断公网口的连接状态。

4-10-2 局域网配置

选择左边菜单栏中的“网络配置”，进入“局域网配置”子模块，填写局域网 IP 详细信息，。

◆ 状态：显示当前局域网状态信息，可分为“启用”和“禁用”两种。

- 内网 IP 地址：设定局域网 IP 地址，一般为设备 LAN 口 IP。
- 子网掩码：子网掩码提供多种可选，用户根据情况自行选择。
- 序号：在 LAN 口上可绑定 99 个逻辑网段。
- 局域网 IP 地址：支持绑定多个局域网 IP 地址。

如下图（图 4－42）：

图 4－42 局域网配置

- 绑定局域网 IP 列表：通过浏览“绑定局域网 IP 列表”信息来确定内网哪些 IP 地址被绑定，避免重复设置该 IP 地址的情况发生，还可对绑定的局域网 IP 地址进行删除。
- 提交：所做的配置提交成功后即可生效。
- 重置：恢复到修改前的配置参数。

4-10-3 功能口配置

在“功能口配置”子模块中，根据需要可将功能口作为“局域网口”、“公网口”、“检测口”或“DMZ”口，进行相应配置。

- 选择为局域网口

局域网口 IP 地址：VPN 设备的 LAN 口 IP

子网掩码：子网掩码提供多种可选，用户根据情况自行选择。

如下图（图 4－43）：

图 4－43 功能口配置

- ◆ 若作为公网口，详细参数可在“网络配置”栏目中的“公网配置”里选择“广域网接口”进行 WAN1 口设置。
- ◆ 若作为监测口或 DMZ 口，即设置相应类型口的 IP 地址，并均可重置。
- ✧ 说明：

  DMZ（非军事化区）：DMZ 的安全性介于外部网络和内部网络之间，用来部署对外提供服务的主机，DMZ 内通常放置一些不含机密信息的公用服务器，比如 Web、Mail、FTP 等。这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等。即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。

4-10-4 NAT 配置

在默认情况下，NEUSOFT VPN 设备会自动使用动态 NAT 方式对内部地址进行转换从而访问公网。

基本配置

- ◆ 启用：选择此功能后即处于路由模式。
- ◆ 关闭：选择此功能后即处于透明模式。
- ● 提交：提交后所做配置即可生效。
- ● 重置：用于对所有 NAT 规则的清空及重新设定，建议慎重使用。

如下图（图 4－44）：

图 4－44NAT 基本配置

源地址转换（SNAT）

“SNAT”是源地址转换，作用在于将 IP 数据包的源地址转换成另外一个地址，并且保存修改前后的映射关系，根据需要进行还原操作。即出去的时候改变源地址，回来的时候改变目标地址。

- 编辑方式：分“追加”、“插入”、“修改”三种操作方式，如果要添加 NAT 规则，就必须选择其中之一。
- 源地址：有“IP 地址”、“地址网段”、“地址范围”、“MAC 地址”和“所有”5 个选项，用户可以根据自己的实际需求来选择。
- 目标地址：可根据“IP 地址”、“地址网段”、“地址范围”和“所有”来选择。
- 协议类型：分为“TCP”、“UDP”、“BOTH”和“ALL”四种，默认为 TCP 协议。
- 源端口列表：源地址的一些应用程序的端口或者所有。
- 目标端口列表：目标地址的应用程序的端口或者所有。
- 出口：可以选择“LAN”、“FUNC”、“VPN”、“WAN”和“WAN1”口来作为出口选择。
- 转换源地址为：将 IP 数据包的源地址转换成另外一个地址.
- 删除：在 SNAT 规则列表中，可对单条规则列表进行“删除”操作。
- 提交：提交后所做的 SNAT 规则即可生效。
- 重置：用于对所有 SNAT 规则的清空及重新设定，建议慎重使用。

如下图（图 4－45）：

图 4－45 源地址转换

目标地址转换（DNAT）

“DNAT”是对数据包的目标地址进行转换，保存修改前后的映射关系，并且根据需要进行还原操作。即进来的时候改变目的地址，出去的时候改变源地址。

- 编辑方式：分“追加”、“插入”、“修改”三种操作方式，如果要添加 NAT 规则，必须选择其中之一。
- 源地址：有“IP 地址”、“地址网段”、“地址范围”、“MAC 地址”和“所有”5 个选项，管理员可以根据自己的实际需求来选择。
- 目标地址：可根据“IP 地址”、“地址网段”、“地址范围”和“所有”来选择。
- 协议类型：分为“TCP”、“UDP”、“BOTH”和“ALL”四种，默认为 TCP 协议。
- 源端口列表：源地址的一些应用程序的端口或者所有。
- 目标端口列表：目标地址的应用程序的端口或者所有。
- 出口：可以选择“LAN”、“FUNC”、“VPN”、“WAN”和“WAN1”口来作为出口选择。
- 转换源地址为：将 IP 数据包的源地址转换成另外一个地址.
- 删除：在 DNAT 规则列表中，可对单条规则列表进行“删除”操作。
- 提交：提交后所做的 DNAT 规则即可生效。
- 重置：用于对所有 DNAT 规则的清空及重新设定，建议慎重使用。

如图（图 4－46）：

图 4－46 目标地址转换

4-10-5 静态路由配置

“静态路由”是在路由器中设置固定的路由表，除非网络用户干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反应，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。通过添加静态路由设置，对经过路由器的 IP 包进行管理。

- 目标地址：可选择固定 IP 和某一网段。
- 网关：到达目标路由器的下一跳地址。
- 跳跃数：拨号成功后，表示该线路的路由跳数，从源到目的的路径中每一跳被赋予以一个跳数值，此值通常为 1；跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，NEUSOFT VPN 会采用跳数值最小的那条路由。跳跃数越低，优先级别越高。
- 删除：在静态路由列表中，显示所有添加的静态路由信息，当不需要设置静态路由时可将其删除。

如下图（图 4－47）：

图 4－47 静态路由配置

- 查看路由：可对设备现有全部路由配置进行查看。
- 提交：提交后所做配置即可生效。
- 重置：该模块所有信息将被清空，需重新配置，建议慎重使用。

4-10-6 动态路由配置

动态路由是将两台路由器之间内网发布出来。通过相互连接的路由器之间交换彼此信息，而这些路由信息是在一定时间间隙里不断更新，以适应不断变化的网络，以随时获得最优的寻路效果。

- RIP 功能：默认是禁用的，需要手工启用。
- 版本：RIP1 或 RIP2
- 生效网段：指的是内网网段。
- 生效接口：这里指的是的 wan，根据公网线插在哪个口就选哪个口。
- 邻居路由器：就是对端路由器
- 路由转发：就是直连网段的跳数。最大 15 跳
- 默认接收管理距离：120s
- 更新间隔时间为：30s

如下图（图 4－48）：

图 4－48　RIP 配置界面

- 接口列表—新建
- 状态：默认是禁用，如需使用勾选即可。
- 接口：根据相应的接线，选择相应的接口。

如下图（图 4－49）：

图 4-49　RIP 接口配置

4-10-7 策略路由配置

“策略路由”是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的 IP 地址决定，而是综合考虑多种因素决定。在此模块中，分“基本配置”和“地址组管理”两个子模块。

基本配置

- ◆ 默认路由方向：可选择“LOCAL”、“WAN”、“WAN1”或“VPN”方向。
- ◆ 编辑方式：分“追加”、“插入”、“修改”三种操作方式，如果要添加策略路由规则，就必须选择其中之一。
- ◆ 源地址：有“IP 地址”、“地址网段”、“地址范围”、“MAC 地址”和“所有”5 个选项，用户可以根据自己的实际需求来选择。
- ◆ 目标地址：可以选择“IP 地址”、“地址网段”、“地址范围”、“地址组”和“所有”。
- ◆ 协议类型：分为“TCP”、“UDP”、“BOTH”和“ALL”四种，默认为 TCP 协议。
- ◆ 源端口列表：源地址的一些应用程序的端口或者“ALL”。
  目标端口列表：目标地址的应用程序的端口或者“ALL”。
- ◆ 方向：可选择“主路由表”、“WAN”、“WAN1”或“自定义”作为路由出口方向。
- ◆ 删除：在策略路由规则列表中，用户可以查看到所有添加的策略路由信息，还可以对策略路由进行“删除”。
- ● 提交：点击提交后，所做配置即可生效。
- ● 重置：可对所有策略路由清空并要求重新配置，建议慎重使用。
- ✧ 说明：

  1、如果将默认路由方向设定为 WAN 或者 WAN1。为了保证 VPN 的正常使用，需要手工添加 VPN 路由策略，即添加目的地址为 VPN 网段的数据，选择方向 主路由。

  2、主路由表： 本地路由表，包含所有的路由信息。

  VPN： VPN 路由表，包含 IPSec VPN，移动用户 VPN 路由信息。

  WAN： WAN 路由表，仅仅包含 WAN 口路由信息。

  WAN1： WAN1 路由表， 仅仅包含 WAN1 口路由信息。

  3、当有多线路分流、备份的时候，可以根据 IP、端口分类，选择不同的出口(WAN 或 WAN1)，以到达分流目的。如下图（图 4－50）：

图 4－50 策略路由基本配置

地址组管理

当用户采用不同的公网线路接入时，可以在此模块中对不同的接入方式进行统一的地址组管理。默认是“未设定”状态，点击“编辑”，可以对其进行设置。如下图（4－51）：

图 4－51 地址组管理

- 编辑：选择“编辑”后，弹出地址组管理的对话框，管理员可以自定义组名称，对组进行注释，在地址选项中可以添加“IP 地址”、“地址网段”和“地址范围”，还可以

将编辑好的地址一次性导入，减少用户的工作量。所做的设置必须提交才能生效。管理员可以对某个地址进行“修改”或“删除”操作。也可以选择“全部删除”。具体配置如图（图 4－52）：

图 4－52 地址组管理配置

4-10-8 VRRP 配置

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议。当 master 路由器出现故障时，会由 backup 路由器代替所有工作，内网用户网关指向虚拟地址。

- Vrid：范围 1-255 之间
- 虚拟地址：两台路由器配置同一个虚拟地址
- 接口选择：建议使用 func 口。
- 优先级：默认为 100.
- 抢占模式：指的是优先级的高低。

如下图（图 4－53）：

图 4-53　VRRP 配置界面

4-10-9 公网监测

“公网监测”主要是用来帮助判断公网口的连接状态。例如各地常用的可以 ping 通的 DNS 服务器 DOMAIN(53)端口，或者邮件服务器的 SMTP(25)和 POP3(110)端口。每个公网可以选择三个不同的监测点，任意一个连通就表示公网连接正常。请选择不同区域或者不同网络运营商内的监测点，以保证监测的准确性。

- WAN 口监测点：需要将“监测启用”勾选上。填写好“监测点的相关信息，使用的协议和端口号。在填写监测地址时，各公网口不能配置相同的公网监测点。
- 提交：点击提交后，所做配置即可生效。
- 重置：对所有修改清空并要求重新配置，建议慎重使用。

如下图（图 4－54）：

图 4－54 公网监测配置

4-11 VPN 配置

本模块包括以下子配置模块:“NEUSOFT 专有 VPN 配置”、“手工 ipsec 通道配置”,“SSL VPN 配置”,“手工 ssl 通道”,“统一身份认证”,“pptp/l2tp”,“许可管理”。

4-11-1 NEUSOFT 专有 VPN 配置

“NEUSOFT 专有 VPN 通道”是指在 NEUSOFT 设备间通过东软独有的目录服务协议建立的 VPN 通道，故称“专有”。单击左边菜单中的“VPN 配置”，进入“NEUSOFT 专有 VPN 配置”子模块。

- License 选择：支持 License Group0 和 License Group1 两个不同的通道组，最多可配置四个 VPN 组。根据 NEUSOFT VPN 产品型号不同，License 组支持通道也不同。
- License 功能：如果用户需要配置 VPN 通道，就需要启用该功能。
- VPN 组名：东软公司提供的以字母开头的 8 位字母数字串。严格区分大小写，VPN 组名不能重名。不支持特别字符。不支持空格。
- 节点名：东软公司提供的不超过 7 位的字母开头的字母数字串。不同组内节点名可以重名。严格区分大小写。不支持空格
- LICENSE：东软公司提供的 16 位的随机字符串。

- VPN 网段：这里需要填写对端的 VPN 网段地址，选择“启用”。
- VPN 网段 1：不同于前一网段的另一网段，可能是通过 Function 口连接的另一网段，也可能是通过其它路由设备、防火墙或三层交换设备相连的另一网段，三层设备后的这些网段需要加静态路由，另外三层设备本身也需要添加静态路由或默认路由，来实现对 VPN 对端的访问。如下图（图 4－55）：

图 4－55 NEUSOFT 专有 VPN 配置

- VPN 绑定端口设置：选择指定的公网口来建立 NEUSOFT 专有 VPN 隧道。
- 对端检测功能（DPD）：自动检查 VPN 隧道连接状态。
- IPSec：在建立 ipsec 通道时必须勾选启用，否则通道建立不成功。
- 查看状态：点击“查看状态”，可见 NEUSOFT 专有配置通道各 VPN 节点状态，如下图（图 4－56）：

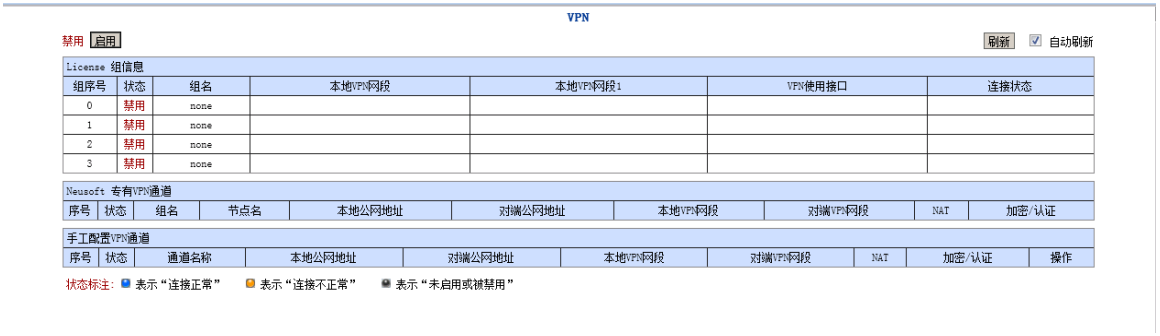


图 4－56 查看 VPN 节点状态

- 提交：所做配置提交后即可生效。
- 重置：对所有修改清空并要求重新配置，建议慎重使用。
- 说明：

此处显示各节点信息，可判断隧道目前是否正常。其中：
蓝灯表示现在正连通，正常；
黄灯表示曾登陆过但现为离线状态；
黑灯表示从未登陆过。

4-11-2 手工 IPSEC 通道配置

NEUSOFT VPN 系列产品同时还支持与其他 VPN 设备建立隧道连接。如要与 NEUSOFT 之间建立 VPN 通道，就要手工配置二者之间的通道，故称“手工 VPN 通道配置”。点击进入“手工 VPN 通道配置”子模块，对手工配置的通道信息进行设置。

- 选择通道：NEUSOFT 支持 50 条 VPN 通道，用户可以自行选择。
- 通道名称：用户可以自定义通道的名称。
- 本地地址：用户可以选择“指定 IP”、“WAN”或者“WAN1”口。
- 本地网关：本地公网口的网关地址。
- 本地 VPN 网段：本地的 VPN 网段范围。
- 对端地址：对端地址可以是“IP 地址”、“域名”、“NEUSOFT 认证”或“任意”。如果选择任意，对端地址为任意的 VPN 连接只能设置一个。
- 对端 VPN 网段：可以选择“指定网段”或者“任意”，如本地要跟多个远程的 ADSL 接入 VPN 设备建立手工 VPN，可选择任意，这样就无需配置多条 VPN 连接，只要满足其他参数协商的 VPN 设备均可与本端建立 VPN 隧道。
- 数据加密算法：支持“AES-128”、“AES-256”、“3DES-128”、“SERPENT-256”、“BLIWFISH-468”、“TWOFISH-256”、“CAST”、“NULL”算法，建议用户选择安全性等级高和速度较快的 AES－128 算法。
- 传输认证算法：支持“MD5”、“SHA1”、“SHA2-256”、“SHA2-512”四种算法，建议用户选择速度较快的 MD5 算法。
- 数据压缩：选择数据压缩类型，管理员可以根据实际传输速度来选择“开启”或者“关闭”该功能，必须将本地和对端设置成相同才有效。如对端不是 NEUSOFT 的设备，建议该项设置成关闭。
- PFS(完美向前保护)：管理员可以选择“开启”会话密钥 PFS，或者“关闭”，必须将本地和对端的设置成相同才有效。如对端不是 NEUSOFT 的设备，建议对端事先参考一下相关的配置手册，查看在与其他厂商的设备互联时是否支持 PFS。
- 预共享密钥：在通信双方中必须就共享的密钥达成一致，信息在传输前使用共享密钥加密，接收端使用同样的密钥解密，如果接收方能够解密，即可被通过认证。必须将本地和对端的密钥设置成相同才有效。
- 密钥生命周期：通过预共享密钥认证后，通信双方将使用 IKE 动态协商密钥，在密钥的一个生命周期中将使用同一密钥加解密数据，因此两端必须设置相同的值，密钥生命周期完结后将重新生成新的密钥，这时 VPN 隧道会重连一次，使用新的密钥，生

命周期的长短决定了 VPN 的安全性和 VPN 重新连接的次数，用户可以根据自己对安全性的要求和使用的需要确定合理的生命周期，最大为 86400 秒。如下图（图 4－57）：

图 4－57 手工 VPN 通道配置

- 查看状态：点击“查看状态”，可见 NEUSOFT 手工配置通道各 VPN 节点状态，如上图（图 6－23）所示。
- 提交：所做配置提交后即可生效。
- 重置：对所有配置信息清空并要求重新配置，建议慎重使用。

◆ 说明：

NEUSOFT 认证根据组名/用户名从 NEUSOFT 服务商直接获取 IP，避免了域名系统的延迟和不稳定性。（此功能需要对端 VPN 路由器也是采用 NEUSOFT 系列）。

4-11-3 SSLVPN 配置

- 基本配置

◆ SSL 用户上限：显示 SSL 用户同时登陆在线最大上限值。

◆ SSL 当前使用数：显示当前 SSL 用户使用数（包含分配池 IP 地址数和固定模式用户数）

◆ 服务端 IP/掩码：定义客户端拨号获取的地址池，格式为服务端 IP/掩码，如默认为 3.3.0.1/16，代表服务端 IP 为 3.3.0.1,掩码为 255.255.0.0

◆ 分配 DNS 服务器：根据是否需要解析内网的域名服务器来设置，可以为空（默认为空）

◆ 本地认证端口：自定义认证端口，默认 81，包含 TCP&UDP 两种协议端口

◆ 本地数据端口：自定义数据端口，默认 82，优先选择协议默认为 UDP

◆ 客户端监测：间隔时间指客户端向服务端发送的检测包间隔时间，超时时间指超过指定时间后客户端主动发起重连，保持默认即可

- 服务端监测：间隔时间指服务端向客户端发送的检测包间隔时间，超时时间指超过指定时间后服务端主动发起重连，保持默认即可
- 传输加速：传输加速再针对较大文件传输时有效，保持默认即可
- 强制重连：针对无人值守移动用户可选，服务端主动强制重连（默认不勾选）
- 用户锁定：密码输入安全性保护（默认参数即可）
- 用户描述自定义 1&2：匹配用户管理中新建用户时的说明（默认不勾选）
- 默认认证方式：可选多种认证方式（默认本地认证）
- 默认双因子增强验证：登录用户的安全性验证方式（默认密码认证）
- 默认路由下载：移动用户连通后，可选自动下载的路由来源（默认都不勾选）
- 默认网关：移动用户连通后，指定 VPN 为默认网关，所有数据都经设备转发（默认不勾选）
- 默认细粒度控制：结合访问的资源，可根据用户组来区别访问权限，非对应组发布资源均访问受限（默认不勾选）
- 默认双网隔离：移动用户连通后，只能访问内网资源，不能上网（默认不勾选）
- 自定义路由定义：勾选了路由下载中的自定义路由，在此栏中填写下载的地址，可拉伸（默认为空）
- 自定义主机列表：移动用户连通后，可自动下载自定义的主机对应列表，即可修改 hosts 文件中信息，可拉伸（默认为空）如下图（图 4－58）：

图 4-58　SSLVPN 配置界面

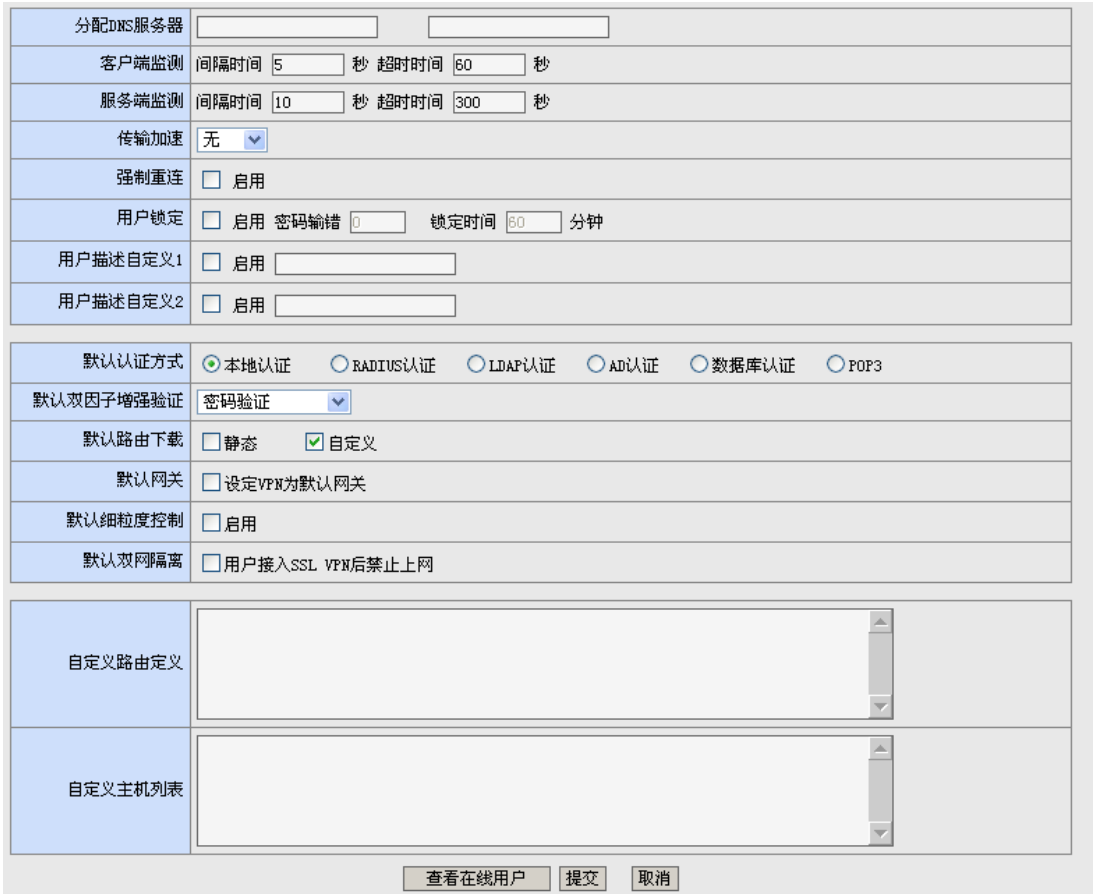


图 4-58-1　SSLVPN 高级选项

- Webssl 配置

需要使用 WEBSSL 方式的用户配置，使用 WEBSSL 需要开启 SSL VPN 和 WEBSSL 两个功能：

- HTTPS 登录端口：设置 HTTPS 登录方式使用的端口，默认 443
- HTTP(80)自动跳转：勾选使用 HTTP 方式自动跳转至 HTTPS 登录页面
- 会话超时时间：设置无会话超时断开时间，0 表示永不超时
- 通道状态：勾选关闭登录页面隧道不断开
- 客户端缓存控制：勾选用户关闭登录页面自动清除浏览器缓存

如下图（图 4－59）：

图 4-59　webssl 配置界面

- 用户组管理

“用户组管理”模块主要针对 NEUSOFT 系列 VPN 产品来进行管理。用户组管理中的用户组用于对资源按组进行分类，然后根据用户组来划分权限。

- ◆ 组名：管理员可以设置组名对所有的用户进行集中管理。
- ◆ 注释：对组名进行注释，方便用户管理。
- ◆ 默认组：可以将组设为默认组，默认组一旦确定后是不能被删除的，可以修改其他组为默认组。在添加用户时，如果不给用户定义组的话，一般都属于默认组的成员。当用户通过“RADIUS”、“LDAP”、“第三方认证方式”登录的时候都是属于默认组的成员。
- 修改：可以对单个组进行修改操作。
- 删除：可以对单个组进行删除操作。
- 提交：所做配置提交后即可生效。
- 重置：对所有配置信息清空并要求重新配置，建议慎重使用。

如下图（图 4－60）：

图 4－60 用户组管理配置

组配置—关联资源

选择“关联资源”子模块，管理员可以将组与发布的资源关联起来，严格控制组内用户访问资源权限，对当前资源可进行全选、多选或单选，点击“保存”，配置即生效。如下图（图 4－61）：

图 4－61 用户组管理—关联资源配置

组配置—关联用户

选择“关联用户”子模块，管理员可将用户与组关联起来，对当前用户可进行全选、多选或单选，点击“保存”，配置即生效。如下图（图 4－62）：

图 4－62 用户组管理—关联用户配置

- **用户管理**
- SSL 用户上限：显示 SSL 用户同时登陆在线最大上限值。
- 用户组：添加用户时可以选择不同的组，进行管理。
- 默认认证方式：支持本地认证、RADIUS 认证、LDAP 认证、AD 域认证、统一身份平台认证、数据库认证多种认证方法，默认为本地认证。
- 动态密码策略：四种方式选择，自主管理可让用户自己更改管理密码；不能更改只能由管理员设置；用户下次登录时必须改密码；定期强制修改
- 默认增强认证：支持多种增强认证，可以根据用户需求来选择“密码验证”、“ISK”认证、“硬件特征码”认证或“ISK+硬件特征码认证方式，系统默认采用认证“密码验证”。
- 分配固定 IP：可设置用户获取固定 IP，不能被包含在用户组地址池中使用时间限制。
- 使用时间限制：设置一天中可使用时间范围
- 过期时间：设置账号使用有效期
- 公网 IP 限制：设置用户登录公网 IP，绑定公网 IP 和用户账号，可设置多个
- 用户登录并发限制：设置账号同时使用并发数，0 不限制
- 默认路由下载：移动用户连通后，可选自动下载的路由来源（默认都不勾选）
- 默认网关：移动用户连通后，指定 VPN 为默认网关，所有数据都经设备转发（默认不勾选）
- 默认细粒度控制：结合访问的资源，可根据用户组来区别访问权限，非对应组发布资源均访问受限（默认不勾选）
- 默认双网隔离：移动用户连通后，只能访问内网资源，不能上网（默认不勾选）
- 远程镜像个人帐户：可设置远程镜像资源主机个人账户的用户名密码，可省去每次登录输入密码的过程

- 描述：对用户账号进行描述
- 用户导入：可将保存好的用户导入列表
- 用户导出：可将用户列表中的用户导出
- 用户列表－显示新建的用户账号信息

如下图（图 4－63）：

图 4-63 添加用户配置

图 4-63-1 查看用户列表

- 资源配置
- 组名&描述：自定义资源组的名称和描述
- 设置为默认资源组：可以将当前在建资源组定义为默认组

- 用户组列表：设置当前资源组关联的用户组，可多选
- 删除&修改：对已有资源组删除、修改操作

如下图（图 4－64）：

图 4-64　资源组配置

- 资源配置
- 协议类型：自定义资源的类型，如 Http、Ftp、远程镜像等
- 所属主站点：设置当前资源隶属于某资源
- 站点名称：定义当前资源名称，桌面显示名称
- 目标地址：定义资源指向的服务器 IP 地址或域名
- 目标端口列表：定义资源使用的端口号，默认选择协议自动匹配
- 路径：配置远程桌面打开时要引用的应用程序全路径
- 远程镜像属性：当资源为远程镜像时，可设置远程桌面的用户名密码所属域，实现自动登录，可以设置共享串口、打印机、智能卡、登录时全屏显示
- 资源组列表：设置当前资源隶属于哪些资源组中，未选中的资源组中不会显示本资源
- 客户端显示：“在开始菜单显示”设置 webssl 应用界面的开始选项中是否显示本资源；“显示为桌面快捷方式”设置该资源是否显示在 webssl 桌面
- 描述&删除&修改：对资源进行描述、删除、修改等操作

如下图（图 4－65）：

图 4-65 资源发布界面

- Isk 认证管理
- SSL 用户选择 ISK 双因子增强认证方式后，登陆 NEUSOFT VPN 后直接上传其 ISK 的硬件信息，无需手动操作，管理员可对认证的用户信息进行删减操作 如下图（图 4－66）：

图 4-66 isk 认证管理

- 硬件特征码
- SSL 用户选择硬件特征码双因子增强认证方式后，登陆 NEUSOFT VPN 后直接上传硬件信息，无需手动操作，管理员可对认证的用户信息进行删减操作
- 手工绑定：输入用户名然后使用工具提取硬件特征码复制、粘贴即可。工具上面的网址。如下图（图 4－67）：

图 4-67　硬件特征码管理

➢ 页面订制

- NEUSOFT VPN 支持客户页面定制，可根据客户需求提供友好美观的登陆界面
- 窗口标题：web 界面窗口标题，位于浏览器左上角，可自定义编辑显示内容（默认为空）
- 系统标题：web 界面登录框标题，如图“测试案例”处（默认为空）
- 联系电话：此处可自定义内容，如“网管电话：010-56550505”（默认为空）
- 联系 Email：此处可自定义内容，如“值班时间：周一至周五”（默认为空）
- 客户信息：此处可自定义内容，如“地址：上海市中山北路 838 号 2F”（默认为空）
- 效果如下图，显示在页面底端：
- 首页欢迎图片：1000 X 110 像素的 .jpg 文件，位于页面顶端
- 客户图标图片：58 X 54 像素的 .jpg 文件，位于登录窗口左上角
- 配置完成后提交直接生效，刷新 web 界面即可

4-11-4 SSL VPN 手工 SSL 通道配置

- 新增：新建 SSL 通道配置
- 启用：勾选启用此隧道，配置好后的通道信息可通过对“ √ ”符号点击实现禁用启用
- 通道序号：设置此通道的序号，新建支持自动排序
- 目的地址：服务端 IP 或域名
- 认证协议：认证采用的协议，与服务端认证端口协议保持一致即可，默认 UDP
- 认证端口：认证采用的端口，与服务端认证端口保持一致即可，默认 81
- 用户名&密码：填写服务端给予的用户名/密码

如下图（图 4－70）：

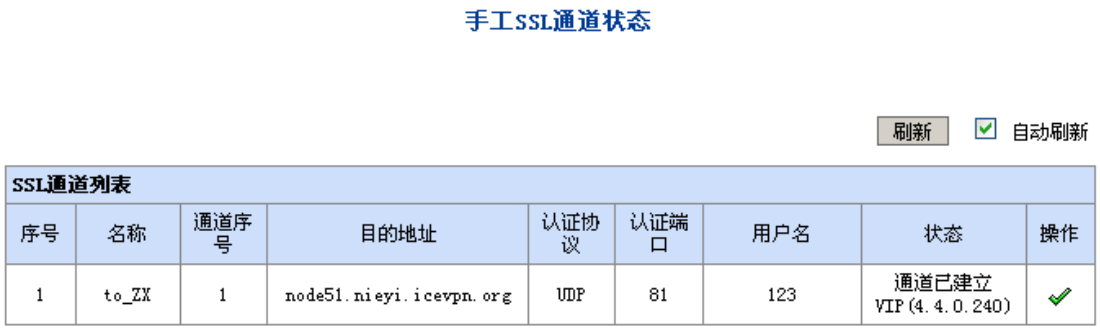


图 4—70 手工 SSL 通道

如下图（图 4－71）：

中心服务端：

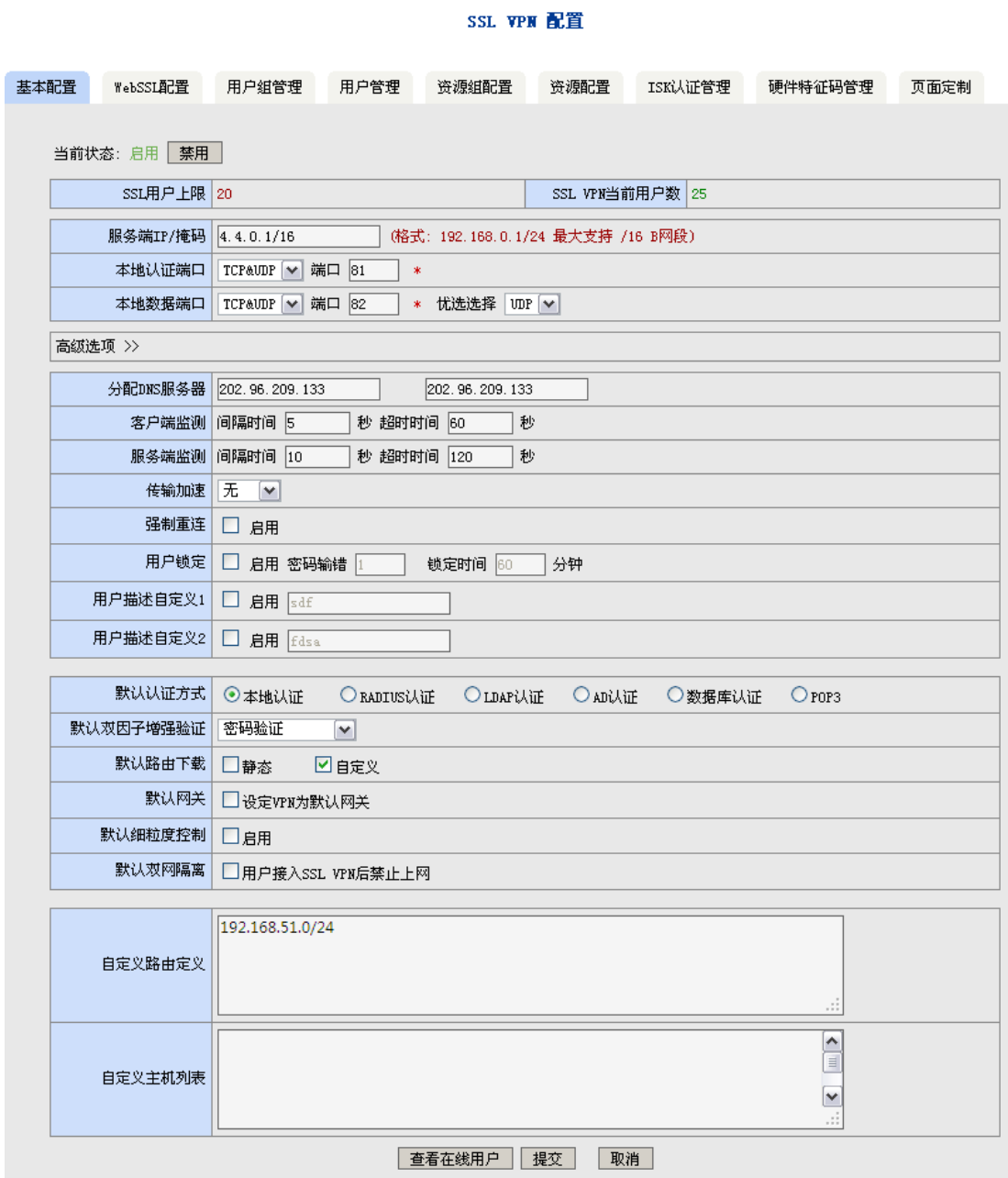

SSL VPN 配置
基本配置
WebSSL配置
用户組管理
用户管理
资源組配置
资源配置
ISK认证管理
硬件特征码管理
页面定制
当前状态：启用
禁用
SSL用户上限
20
SSL VPN当前用户数
25
服务端IP/掩码
4.4.0.1/16
(格式：192.168.0.1/24 最大支持 /16 B网段)
本地认证端口
TCP&UDP
端口
81
本地数据端口
TCP&UDP
端口
82
优选选择
UDP
高级选项 >>
分配DNS服务器
202.96.209.133
202.96.209.133
客户端监测
间隔时间
5
秒 超时时间
60
秒
服务端监测
间隔时间
10
秒 超时时间
120
秒
传输加速
无
强制重连
启用
用户锁定
启用 密码输错
1
锁定时间
60
分钟
用户描述自定义1
启用
sdf
用户描述自定义2
启用
fdsa
默认认证方式
本地认证
RADIUS认证
LDAP认证
AD认证
数据库认证
POP3
默认双因子增强验证
密码验证
默认路由下载
静态
自定义
默认网关
设定VPN为默认网关
默认细粒度控制
启用
默认双网隔离
用户接入SSL VPN后禁止上网
自定义路由定义
192.168.51.0/24
自定义主机列表
查看在线用户
提交
取消

图 4—71　中心服务配置

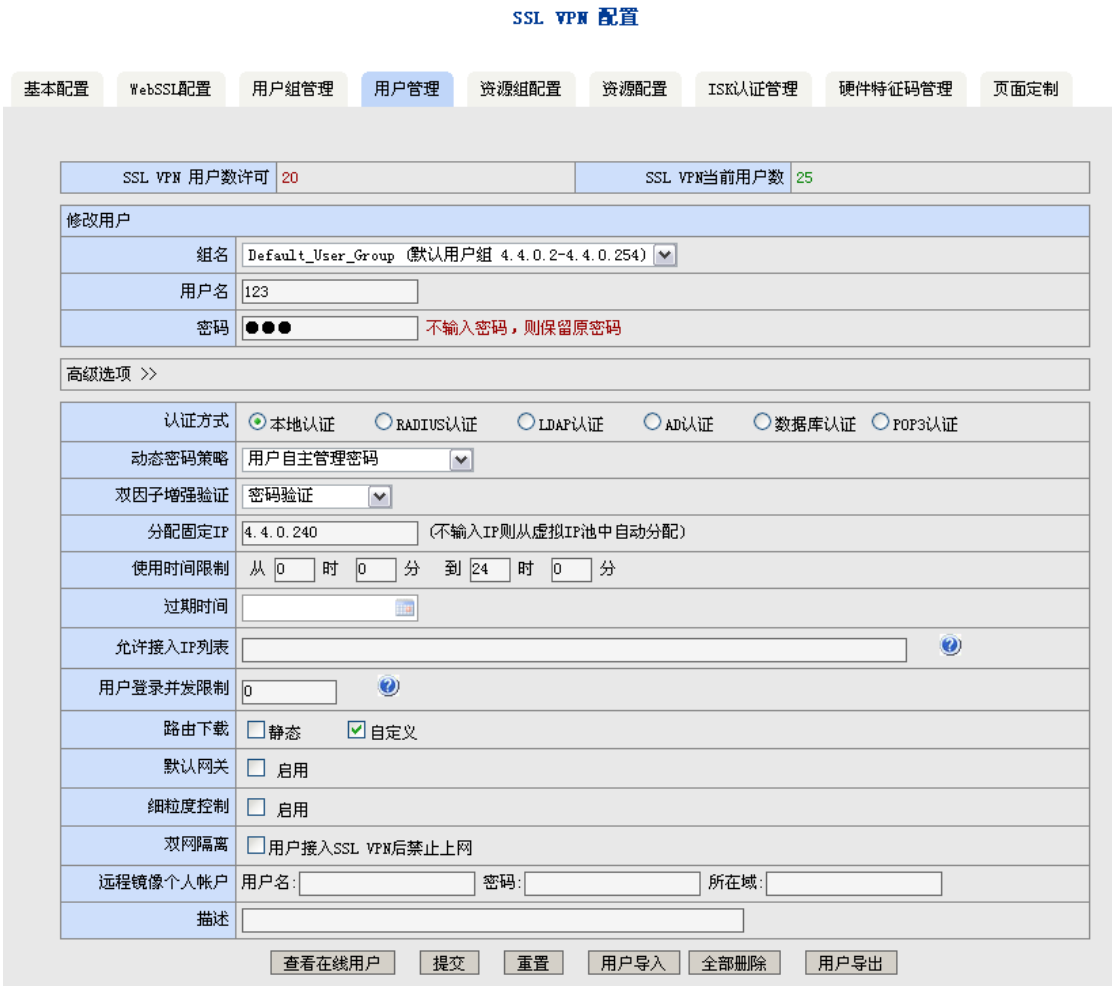


图 4—72　用户管理配置

新建用户名：123　分配固定 ip

图 4—73　手工 SSL 通道配置

客户端设置

4-11-5 统一身份认证

- RADIUS 认证
- NEUSOFT　VPN 支持 RADIUS 外部认证方式，该模块属增值模块，仅针对高端产品开放，管理员可根据实际网络环境进行如下配置，首先配置 RADIUS 服务器地址 如下图（图 4—74）：

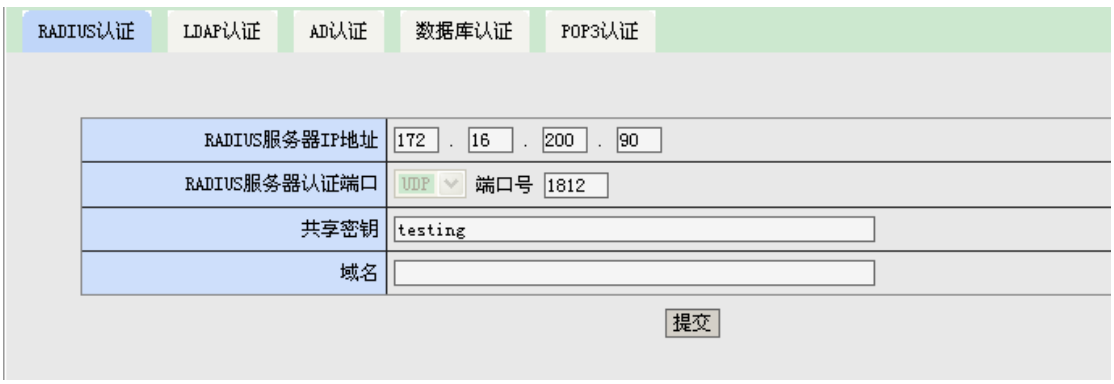


图 4—74 RADIUS 配置

- Ssl 客户端用户认证选择 radius 认证 如下图（图 4－75）：

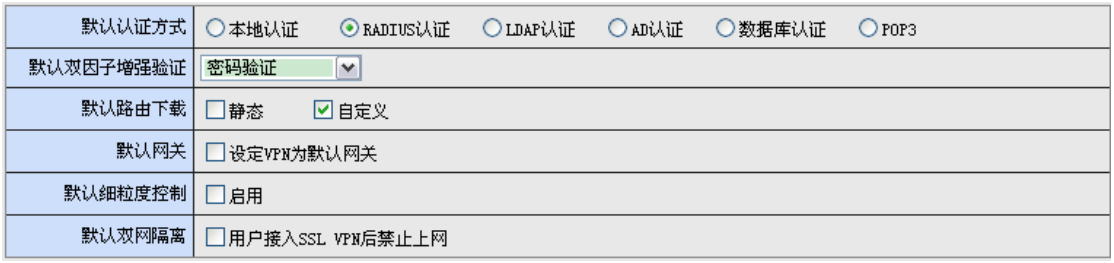


图 4－75　新建用户时选择 RADIUS 认证

- LDAP 认证
- LDAP 服务器地址：填入 LDAP 服务器地址
- LDAP 服务器端口：填入 LDAP 服务器端口号，默认为 389
- LDAP 版本：选择 LDAP 版本，默认为 LDZPv3
- 起始搜索 DN：目录树的根，就是基准 DN，如 NEUSOFT .cn 格式为 dc=NEUSOFT ,dc=cn
- LDAP 访问用户名：LDAP 管理员账户，如 Manager，根目录为 NEUSOFT .cn，填写格式为 cn=Manager,dc=NEUSOFT ,dc=cn(若能匿名访问,此项可置空)
- LDAP 访问用户密码：账户密码(若能匿名访问,此项可置空)
- 验证用户名属性：用户名属性字段设置，默认为 uid
- 验证密码属性：验证密码属性字段设置，默认为 userPassword
- 密码加密算法：可选加密算法，明文或标准 SSHA　如下图（图 4－76）：

图 4－76　LDAP 配置

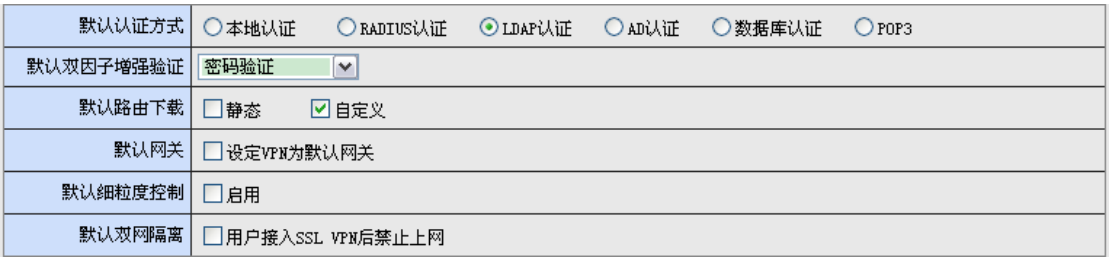


图 4—77 新建用户时选择 LDAP 认证

- Ssl 客户端用户认证选择 LDAP 认证
- AD 认证
- AD 服务器地址：填写域服务器 IP（默认为空）
- AD 服务器端口：AD 域服务器使用的端口（默认为 TCP3268）
- 活动目录基础 DN：例如 AD 域名为 NEUSOFT .cn，用户组在 users 中，填写格式是：CN=Users,DC=NEUSOFT ,DC=cn,若用户不在 user 组中可对应更改去除 CN=Users 项，表示所有用户组
- AD 访问用户名：AD 域管理员用户名，例如以默认管理员 Administartor，格式是：CN=Administrator,CN =Users,DC=NEUSOFT ,DC=cn;（默认为空）
- AD 访问用户密码：对应域管理员用户密码（默认为空）如下图（图 4—78）：

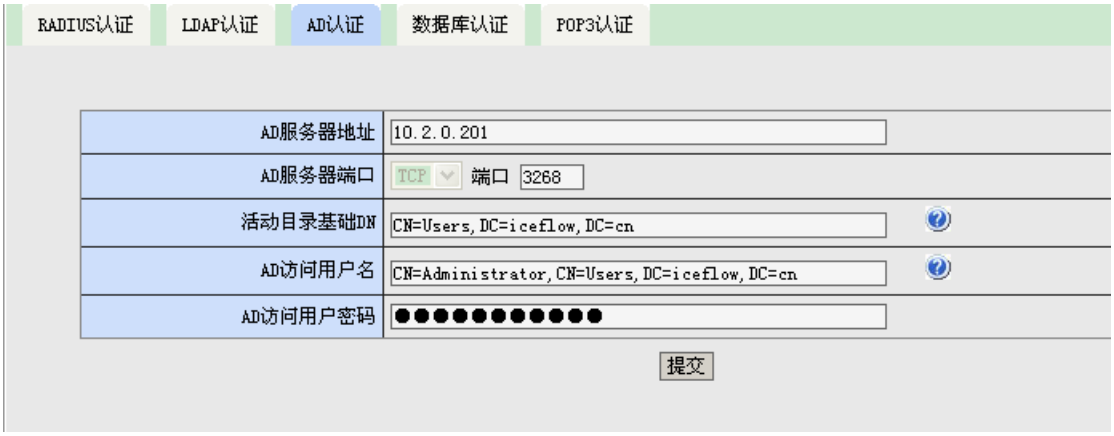


图 4—78 AD 认证

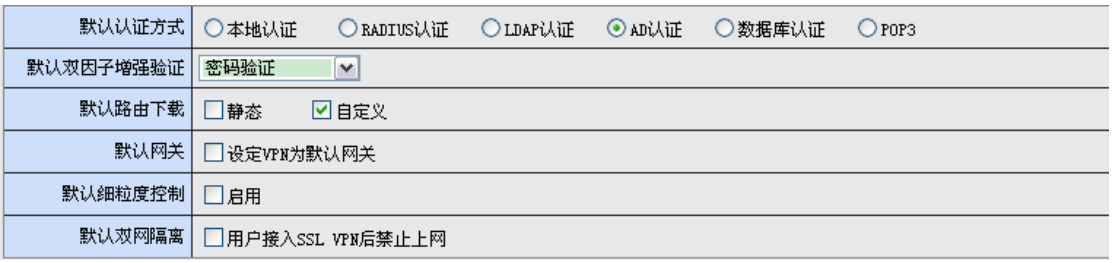


图 4—79 新建 AD 时选择此认证

- Ssl 客户端用户认证选择 AD 认证
- 数据库认证
- 数据库认证服务器 IP 地址：填写服务器 IP（默认为空）
- 数据库类型：默认支持 MySQL，可定制 Oracle
- 数据库名称：填写数据库名称
- 数据库访问用户名：填写数据库管理员用户名
- 数据库访问密码：填写数据库管理员密码
- 用户验证表名：填写数据库用户表名
- 用户名验证字段：填写用户名验证字段
- 密码验证字段：填写密码验证字段
- 密码加密算法：选择加密算法，明文或 MD5 如下图（图 4－80）：

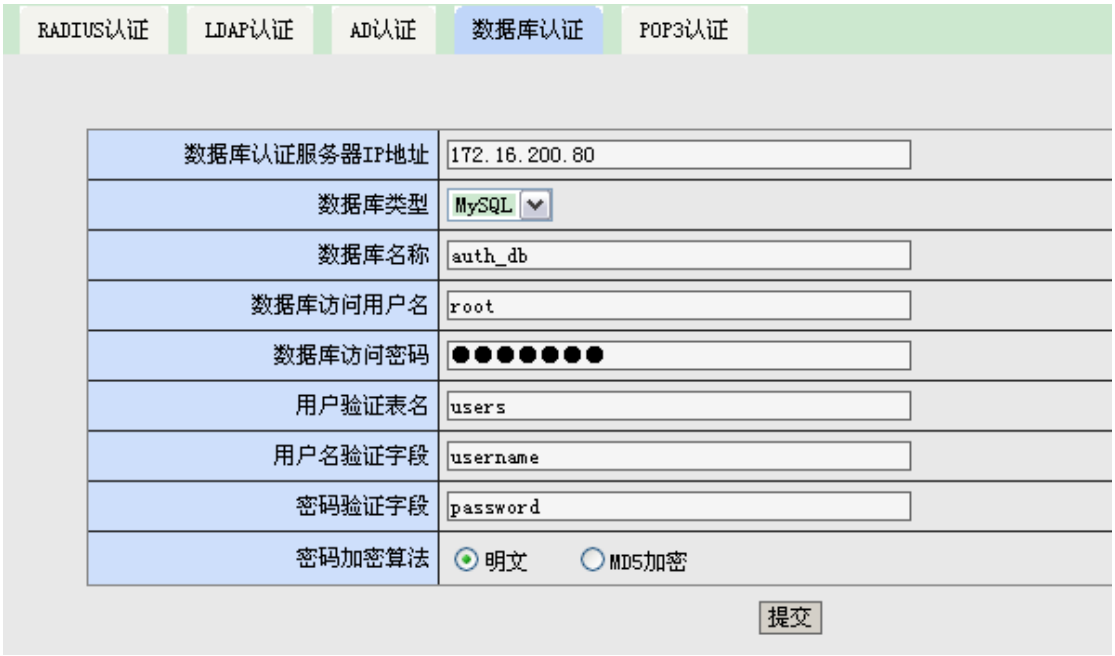


图 4—80 数据库认证

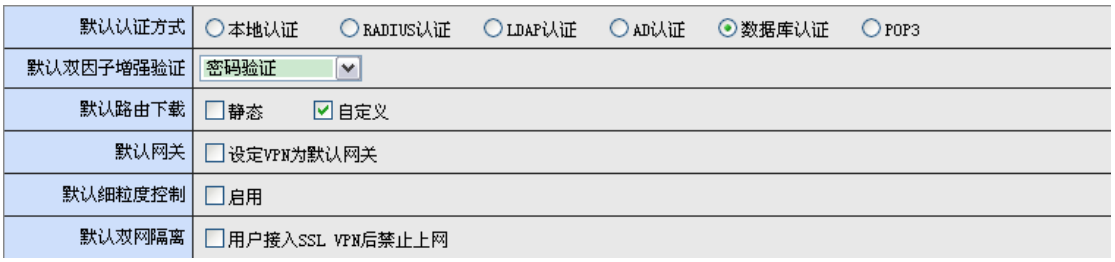


图 4—81 用户选择数据库认证

- Ssl 客户端用户认证选择数据库认证

- POP3 认证
- POP3 服务器地址：邮箱服务器地址(默认为空)
- 邮箱域名：邮箱域名，如 163.com，若填写用户名不需在加后缀，若空用户名要打全。(默认为空)
- POP3 服务器端口：（默认为 110） 如下图（图 4－82）：

图 4—82 POP3 认证

- Ssl 客户端用户认证选择 POP3 认证

4-11-6 PPTP/L2TP

PPTP 和 SSL 接入只是移动用户接入 VPN 网络时所采用的两种不同协议。PPTP 配置方法和 SSL 方法相同，只是在配置模式和安全协议上有些区别，下面仅对不同的地方进行描述。

- 模式：池模式、固定模式（PPTP 模式改变后，用户列表将清空!）
- 分配 IP 地址：池模式的地址池（需要跟局域网的 IP 地址段相同，但不能跟局域网 IP 地址冲突）固定模式的 IP 地址分配是在建用户的时候分配的
- 分配 DNS：为 PPTP 登录用户分配的 DNS（默认为空）
- 安全协议：PPTP 用户登录使用的安全协议，有 PAP、CHAP、CHAPv2 三种（默认为 CHAPv2）

- 用户名：PPTP 用户登录的名称（默认为空）
- 密码：PPTP 用户登录的密码（默认为空）
- 描述：为此 PPTP 用户添加描述（默认为空）如下图（图 4－83）：

图 4—83 PPTP 配置界面

L2TP 是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如 PPTP 要求网络为 IP 网络，L2TP 要求面向数据包的点对点连接；PPTP 使用单一隧道，L2TP 使用多隧道；L2TP 提供包头压缩、隧道验证，而 PPTP 不支持

- L2TP 功能：是否启用 L2TP 功能（默认未启用）
- 服务端 IP：可填写为内网 IP（默认为空）
- 地址池范围：为 L2TP 用户分配的 IP 地址池，跟 PPTP 地址池相同的要求，需要跟局域网的 IP 地址段相同，但不能跟局域网 IP 地址冲突（默认为空）
- 分配子网掩码：为拨号用户分配的子网掩码（默认为空）
- 非配 DNS：为 L2TP 拨号用户分配的 DNS（默认为空，可为空）
- IPSec 预共享密钥：主要是为手机平台的拨号用户设置，自定义（长度最长 16 位，不可为空）
- 查看在线用户：点击“查看在线用户”，可以在弹出的页面中看到已连接的用户，点击“断开”，可在设备上将该用户断开连接 如下图（图 4－84）：

图 4—84 L2TP 配置界面

4-11-7 许可管理

由厂商提供的移动用户拨入数量的管理文件，能方便的升级用户许可数。

如下图（图 4－85）：

图 4—85 许可管理

- 移动用户总许可数：由厂商提供的移动用户许可总数量。
- SSL/PPTP 许可数：用户可以根据具体需求自行修改 SSL/PPTP 的许可数，但不能超过总的移动用户许可数。
- ISK 许可数：由厂商提供给移动用户通过 ISK 认证方式的许可总数量。
- 硬件特征码许可数：由厂商提供的移动用户通过硬件特征码认证方式的许可总数量。
- WebSSL 许可数：由厂商提供的 WebSSL 方式登陆的许可总数量。
- 许可证管理：用户可以将许可文件提取到本机，选择“浏览”，“提交”成功后，文件中的许可数与用户可使用的许可数为一致。

4-12 防火墙配置（VPN 高级功能）

本模块包括“规则列表”、“访问控制”、“端口映射控制”、“包转发控制”、“透明模式”、“过滤控制”、“IP—MAC 绑定”、“攻击防范”八大子模块，其中“透明模式”、“过滤控制”、“IP-MAC 绑定”、“攻击防范”属增值模块，仅对高端产品开放。

4-12-1 规则列表

点击“规则列表”，显示防火墙所有规则配置信息。如下图（图 4－86）：

图 4－86 规则列表

4-12-2 访问控制

在“访问控制”中通过添加新的管理规则来设置对 VPN 设备的访问许可。

远程访问控制策略

如下图（图 4－87）：

图 4－87 访问控制

- LAN 口：管理员可以选择“接受”或“拒绝”来控制远程用户对 LAN 口的访问，默认为“接受”状态。
- FUNC 口：管理员可以选择“接受”或“拒绝”来控制远程用户对 FUNC 口的访问，默认为“接受”状态。
- VPN（IPSEC）：管理员可以选择“接受”或“拒绝”来控制 VPN 用户对本设备的访问。
- 默认规则：管理员可以选择“接受”或“拒绝”来控制公网用户对本设备的访问，默认为“接受”状态。

Web 远程访问

- 接受：勾选该选项后，公网用户可以通过远程来访问 Web 界面，对本机进行配置管理，管理员可以对管理端口进行修改。
- 拒绝：选择该选项后，不能通过远程来对 Web 页面进行管理，默认是“关闭”状态。
- HTTPS 访问：勾选该选项后，
- 设置“Web 公网远程访问控制”的目的在于给本机一个可从外网访问的途径，在需要远程调试的时候可以接受。如果用户的配置已经完成，建议关闭此选项以隐常本设备，避免受到攻击，它不会影响 VPN 隧道通讯。

SSH 远程访问

- 接受：选择该选项后，可以通过终端工具 SSH 来远程登陆管理和配置 NEUSOFT

VPN。默认为“接受”状态，管理员可以通过动态改变 SSH 登陆端口来避免遭受攻击。

- 拒绝：选择该选项后，不能通过 SSH 来访问 NEUSOFT VPN。

公网远程 PING

通过“允许”或“拒绝”来控制外网对 NEUSOFT VPN Ping 命令的使用。

添加访问规则

管理员可以添加新的访问规则来允许或拒绝公网 IP 对 NEUSOFT VPN 设备的访问。如下图（图 4－88）：

图 4－88 访问控制

- 地址：允许添加具体 IP 或者一个网段
- 操作：对添加的地址规则进行“接受”或者“拒绝”访问控制。若选择“接受”（默认是“关闭”的），这样可以通过外网访问本机。
- 访问控制列表：显示所有添加的访问规则列表信息，管理员可以对不需要的规则进行“删除”操作。
- 提交：所做配置提交即可生效。
- 重置：对所有配置信息清空并要求重新配置，建议慎重使用。

4-12-3 端口映射控制

管理员可以通过端口映射控制方法，将局域网上的应用（WEB，SMTP，POP3 等等）拓展到公网上，方便外网用户访问。具体配置如下图（图 4－90）：

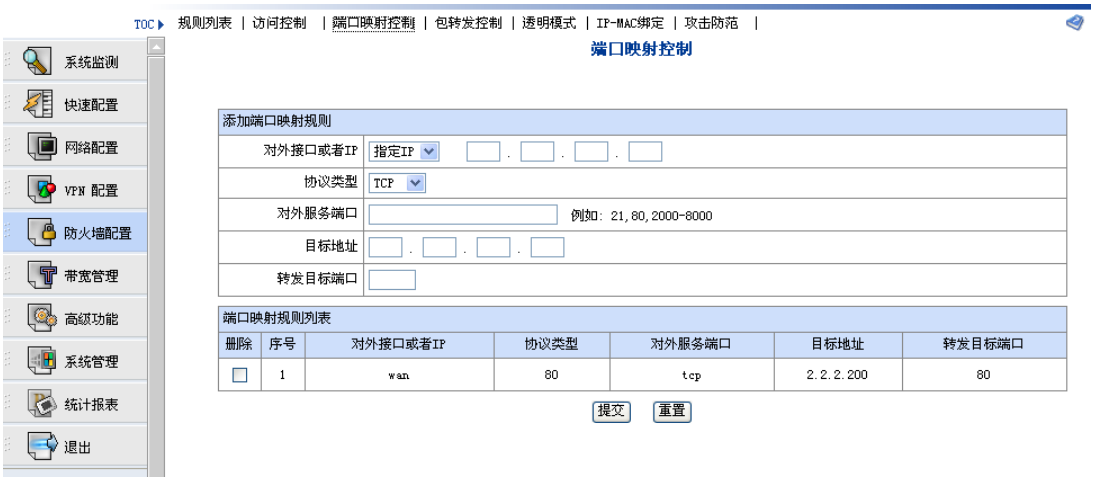


图 4－90 端口映射控制

添加端口映射规则

- 对外接口或 IP：可以指定对外接口为“WAN”口和“WAN1”口，或者指定为“固定的 IP 地址”。
- 协议类型：可以根据具体的应用来选择协议类型为“TCP”、“UDP”、“BOTH”和“ALL”。
- 对外服务端口：根据应用来选择对外服务的具体端口号。
- 转发目标地址：局域网中具体应用服务器地址。
- 转发目标端口：局域网中应用服务端口号。

端口映射规则列表

- 删除：在列表中可以看到添加后的规则列表信息，管理员选择“删除”选项将某条规则删除。

说明：

为了安全起见，建议将对外公布的应用服务器放到 DMZ 区域，可将 FUNC 口功能设为 DMZ 区域。

4-12-4 包转发控制

包转发控制包括“基本配置”、“地址组管理”、“应用组管理”三个子模块。

基本配置

在此模块中，管理员可以通过源地址、目标地址及其协议类型，并选择源端口号及目标端口号来进行接受或丢弃操作。也可以在此处设置上公网、转发 ICMP ping 包是否开启，默认包转发策略为接收或丢弃。具体操作如下图（图 4－91）：

图 4－91 基本配置

- 上公网控制：管理员可以选择“接受”或“丢弃”上公网控制，默为“接受”状态。
- 转发 ICMP 控制：管理员可以选择“接受”或“丢弃”转发 ICMP 控制。默认为“接受”状态。
- 转发默认策略：管理员可以选择“接受”或“丢弃”默认包转发策略。默认为“接受”状态。
- P2P、QQ、MSN：管理员可以通过该选项的设置，来控制局域网内用户 P2P 软件和即时聊天工具的使用。默认为“允许”状态。
- 时间计划：管理员通过选择“开启”或“关闭”对时间计划的控制，默认情况下是“关闭”状态。如果选择“开启”后，对应的有个时间计划选项，时间可设置为“永远”、“每周”和“每天”。对相应时间段做了限制后，选择“启用”后即可生效。

包转发规则控制

管理员可以通过该模块的配置，来控制局域网内用户对网络的访问。

具体配置如下图（图 4－92）：

图 4－92 包转发控制

- 编辑方式：添加包转发规则时，包括“追加”、“插入”、“修改”三个选项，可以选择“追加”一条规则，或者“插入”另外一条规则，或者选择“修改”其中的某条规则。

但必须在三种方式中选择其中的一种进行编辑。

- 源地址：可以选择“IP 地址”、“地址网段”、或“地址范围”，或者精确到某个固定的“MAC 地址”、“地址组”和“所有”来进行选择。
- 目标地址：可以选择“IP 地址”、“地址网段”、或“地址范围”，或者选择“地址组”、“应用组”和“所有”。
- 协议类型：协议类型包括“TCP”、“UDP”、“BOTH”、“ICMP”和“ALL”，管理员可以根据实际应用来选择协议类型。
- 源端口列表：根据具体的应用来选择相应的端口。
- 目标端口列表：根据具体的应用来选择相应端口号。
- 操作：对于创建的规则进行“接受”或“丢弃”操作。

包转发列表

- 删除：在此列表中可以可以看到添加的包转发规则的详细信息。可以对相应的规则进行“删除”操作。
- 操作：在包转发规则列表中，对所选规则点击“操作”按钮，该规则将被丢弃。
- 启用：在包转发规则列表中，对所选规则点击“启用”按钮，该规则将被禁用。

✧ 说明：

规则匹配是顺序执行的，当匹配后它就进行相应的操作（接受或者丢弃），其后的规则不会在产生效果。如果当所有的规则都不能匹配的时候，它就按照转发默认规则来操作。

地址组管理

当用户采用不同的公网线路接入时，可以在此模块中对不同的接入方式进行统一的地址组管理。默认是“未设定”状态，点击“编辑”，可以对其进行设置。如下图（图 4—93）：

图 4—93 地址组管理

- 编辑：选择“编辑”后，弹出地址组管理的对话框。

- ◆ 组名称：用户可以自定义组名称。
- ◆ 组注释：对组进行详细注释。
- ◆ 启用：选择该选项框启用地址组功能。
- ● 提交：提交后设置的组名称即可生效。
- ● 重置：对所有配置信息清空并要求重新配置。
- ◆ 地址：用户选择“IP 地址”、“地址网段”和“地址范围”。
- ◆ 注释：对“IP 地址”、“地址网段”和“地址范围”进行详细的描述。
- ● 地址导入：可以将编辑好的地址文本一次性导入，减少用户的工作量。文本格式只支持“.txt”。
- ● 全部删除：将添加在地址列表中的用户全部删除。
- ● 修改：可以对单个地址进行“修改”操作。
- ● 删除：可以对单个地址进行“删除”操作。

具体配置如图（图 4—94）：

图 4—94 地址组管理

应用组管理

为了更好的控制局域网内的稳定性和安全性，管理内部用户的上网行为，在此模块中用户可以对一些应用资源进行统一的管理。默认情况下是“未设定”，点击“编辑”可以对其进行设置。如下图（4—95）：

图 4—95 应用组管理 1

- 编辑：选择“编辑”后，弹出“应用组管理的对话框”。管理员可以对应用组进行编辑管理。
  - 组名称：用户可以自定义组名称。
  - 组注释：对组进行详细注释。
  - 启用：选择该选项框启用应用组功能。
- 提交：提交后设置的组名称即可生效。
- 重置：对所有配置信息清空并要求重新配置。
  - 目标地址：在“目标地址”选项中，可以填写“IP 地址”、“地址网段”和“地址范围”。
  - 协议类型：协议类型支持“TCP”、“UDP”、“BOTH”、“ICMP”和“ALL”。
  - 源端口列表：用户根据具体的应用来填写相应的端口。
  - 目标端口列表：用户根据具体的应用来填写相应的端口。
  - 注释：对添加的目标地址进行具体的描述。
- 提交：提交后对目标地址作的设置即可生效。
- 重置：对所有配置信息清空并要求重新配置。
- 地址导入：支持大量用户地址导入，减少用户操作。
- 全部删除：可以对地址列表中的用户全部删除。
- 修改：可以对添加的单个地址进行修改操作。
- 删除：对单个地址进行删除操作。

详细配置如图（4—96）：

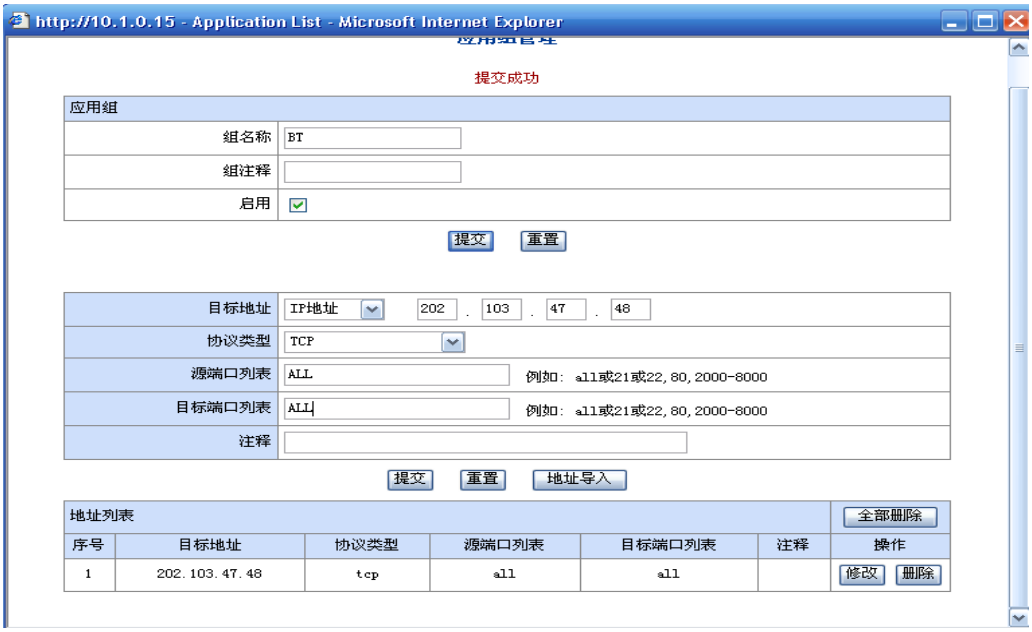


图 4—96 应用组管理 2

4-12-5 IP—MAC 绑定

为了防止内部人员进行非法 IP 盗用(例如盗用权限更高人员的 IP 地址，以获得权限外的信息)，可以将内部网络的 IP 地址与 MAC 地址绑定，盗用者即使修改了 IP 地址，也因 MAC 地址不匹配而盗用失败，并且可以根据 MAC 地址的唯一性查出使用该 MAC 地址的网卡，从而查出非法盗用者。

基本配置

在“基本配置”子模块中，管理员可以启用 IP-MAC 功能，不在绑定列表中的 IP-MAC 地址将被封锁。如下图（图 4—98）：

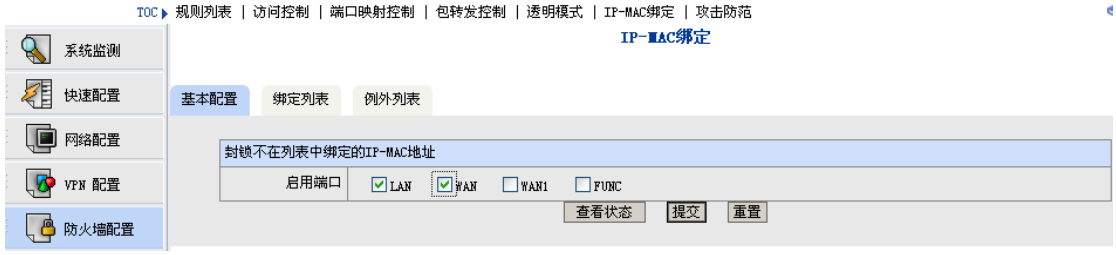


图 4—98 透明模式

◆ 启用端口：管理员可以选择需要进行“IP-MAC 绑定”的网口。根据产品型号不同，开放的端口也不同。

- 查看状态：点击“查看状态”可以看到所有 IP-MAC 状态和接口信息。还可以对单个处于动态状态的 IP 地址进行绑定操作。
- 提交：提交后，所做配置即可生效。
- 重置：恢复到修改前的状态。

绑定列表

管理员可以在此模块中进行具体的 IP-MAC 地址绑定，如下图（图 4—99）：

图 4—99 绑定列表

- IP 地址：具体的 IP 地址。
- MAC 地址：与 IP 地址相对应的 MAC 地址，该地址具有唯一性。管理员可以点击“手工扫描”来自动显示该 IP 对应的 MAC 地址和计算机名。
- 启用 IP-MAC 绑定：勾选该选项后，所设定的 IP 将启用 IP-MAC 绑定功能。
- 启用 DHCP 静态绑定：勾选该选项后，通过 DHCP 分配的 IP 地址将启用静态绑定。
- 查看状态：点击该选项，可以查看到所有的 IP—MAC 绑定的详细信息。
- 提交：提交后所做配置即可生效。
- 重置：恢复到修改前的配置参数。
- 搜索：在 IP-MAC 绑定规则信息繁多的情况下，可以输入包含需要查询的用户信息关键字进行搜索，搜索出包含该关键字的所有信息结果会在列表中显示。
- 导出：可以将绑定规则列表内的信息导出另存。
- 文件导入：管理员可以将预先编辑好的 IP-MAC 信息一次性导入，支持导入文本格式为“.txt”。
- 扫描导入：管理员可以通过网关扫描来自动扫描出当前设定的网段 IP 地址。
- 全部删除：对列表内的信息全部删除。
- IP-MAC 绑定全部启用：启用所有 IP-MAC 绑定规则，启用后绑定规则即可生效。

- IP-MAC 绑定全部禁用：禁用所有 IP-MAC 绑定规则。
- 修改：对单个 IP-MAC 规则进行修改操作。如果此时为“禁用”状态，点击“修改”后会显示为“启用”状态。

例外列表

对于一些临时性访问或用做测试的网段地址，不需要进行 IP-MAC 绑定即可将其添加到例外列表中。添加在例外列表中的 IP 地址将不受 IP-MAC 绑定检测。如下图（图 4—100）：

图 4—100 例外列表

- 源地址：源地址的添加可以是“IP 地址”、“地址网段”、“地址范围”和“MAC 地址”。
- 说明：对源地址详细的描述。
- 查看状态：点击该选项，可以查看到所有 IP—MAC 绑定的详细信息。
- 提交：提交后所做配置即可生效。
- 重置：恢复到修改前的配置参数。
- 搜索：在 IP-MAC 绑定规则信息繁多的情况下，可以输入包含需要查询的用户信息关键字进行搜索，搜索出包含该关键字的所有信息结果会在列表中显示。
- 删除：勾选该选项后，点击“提交”即可对单条 IP-MAC 绑定规则进行删除操作。

4-12-6 攻击防范

NEUSOFT VPN 将常见的十几种攻击防范分为“非法报文攻击”和“统计型报文攻击”两大类。（该模块为增值模块，仅对 F 系列产品开放。）

非法报文攻击

在“非法报文攻击”模块中，用户可以根据需要对相关攻击防范进行“开启”操作。还可以对单项进行“记录日志”操作。记录的日志信息可以在防火墙日志里查看到。非法报文攻击默认为“开启”状态。如下图（图 4—101）所示：

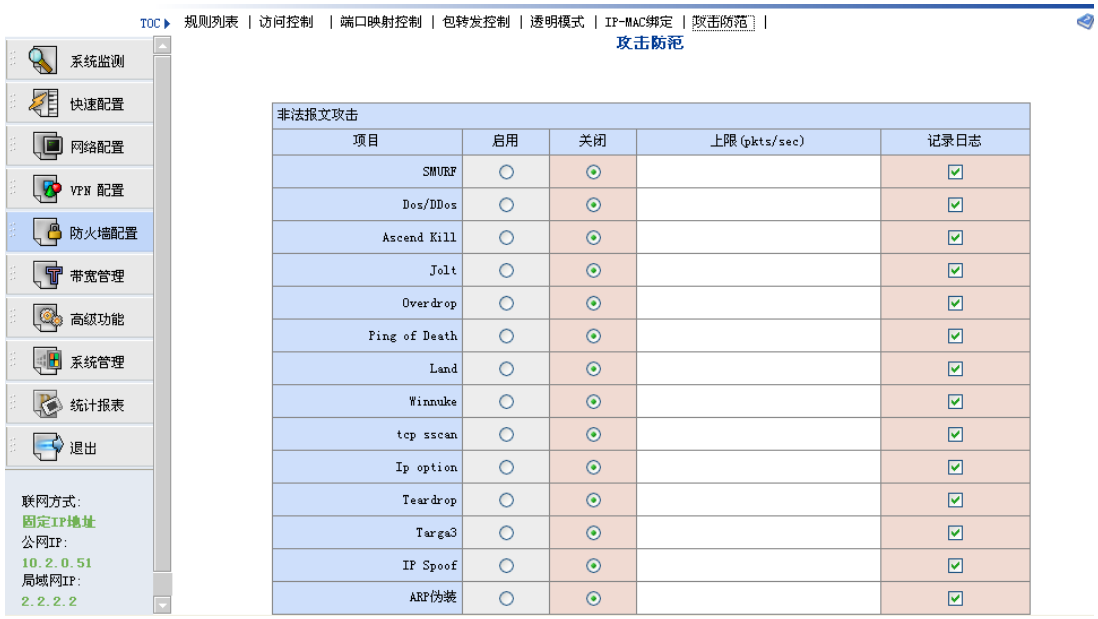


图 4－101 非法报文攻击

统计型报文攻击

管理员可以根据需要对相关攻击进行“开启”操作，也可以根据具体应用来设置上限值，或者是否进行“日志记录”，若将所有攻击防范全部打开，将占用部分系统资源，建议根据实际需要作部分开启。下列选项默认为“关闭”状态，如下图（图 4—102）：

图 4—102 统计型报文攻击

4-13 带宽管理

在“带宽管理”模块中，包括“基本设置”、“组策略管理”、“规则管理”和“限定列表”。本模块功能主要定义一些相应组策略，添加明细的规则列表，通过设定限定列表来更好的优化网络数据包流量。

4-13-1 基本配置

在“基本配置”中设置公网口的总带宽，管理员可以对 WAN 或 WAN1 口进行“启用”或“禁用”操作，对实际物理网口进行总带宽限制。如图（4－103）：

图 4－103 基本设置

4-13-2 规则管理

在“规则管理”模块中，添加明细的策略规则，添加的明细规则优先于组策略规则生效。如下图（图 4－104）：

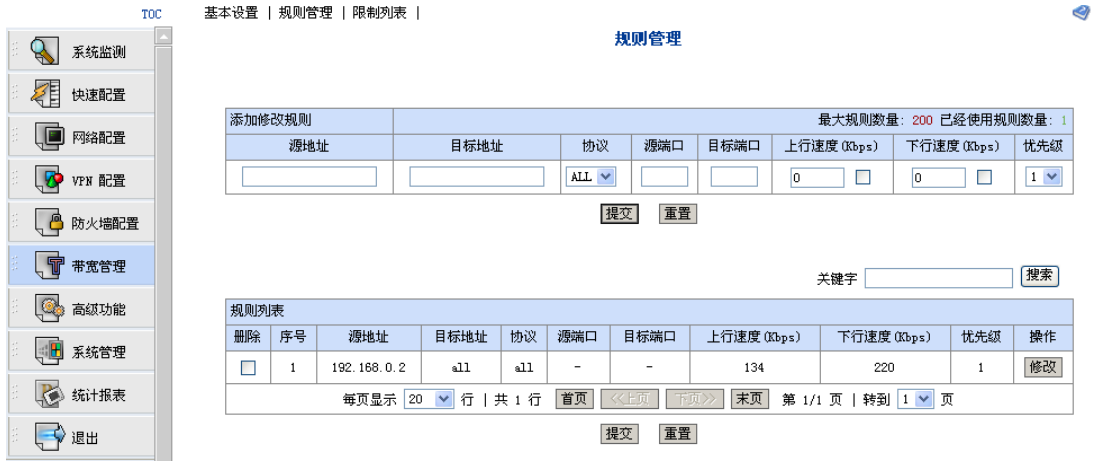


图 4－104 规则管理

- 源地址：可以输入“IP 地址”、“地址网段”和“地址范围”。
- 目标地址：输入“IP 地址”、“地址网段”和“所有”。目的地址若输入 0.0.0.0/0 则表示所有目的地址。
- 协议类型：协议类型支持“TCP”、“UDP”、和“ALL”。
- 源/目标端口列表：用户根据具体的应用来填写端口号。
- 上行/下行速度：设定上行和下行的带宽速度。
- 限定：选择该选项后，用户不能超越限定的速率。

- ◆ 优先级：数值越小，优先级越高，如果优先级别相同，则按顺序匹配生效。
- ◆ 搜索：为了更加方便快捷查询到相关规则，管理员可以在该选项中输入需要查询的关键字进行搜索。
- ◆ 删除：在规则列表中可以看到所有添加的规则列表信息，管理员可以点击“删除”来进行相关的操作。
- ◆ 修改：管理员可以点击“修改”来对单条规则进行修改操作。
- ● 提交：提交成功后，所做配置即可生效。
- ● 重置：恢复到修改前的配置参数。

4-13-3 限定列表

在此子模块中，管理员可以对内网需要进行带宽限制的单机进行管理，更好的优化网络数据包流量。该规则在所有带宽策略中最先生效。详细配置如下图（图 4－105）：

图 4－105 限定列表

- ◆ 内网地址：内网中具体的地址，可以为 IP 地址、地址网段和地址范围。
- ◆ 说明：管理员自定义描述。
- ◆ 搜索：为了更加方便快捷查询到相关规则，管理员可以在该选项中输入需要查询的关键字进行搜索。
- ◆ 删除：在限制列表中可以看到所有添加的限制列表信息，可以选择“删除”来进行相关的操作。
- ● 提交：提交成功后，所做配置即可生效。
- ● 重置：恢复到修改前的配置参数。

4-14 高级功能

本模块包括以下子配置模块：“DHCP 配置”、“DNS 转发配置”、“广播包转发”、“集群模块”。

4-14-1 DHCP 配置

为了便于统一管理，可以通过 NEUSOFT VPN 系统内置的 DHCP 功能，使客户端动态获得 IP 地址。在“DHCP 配置”模块中，包括“基本配置”和“静态绑定列表”子模块。

基本配置

NEUSOFT VPN 支持 LAN 口和 FUNC 口同时启用 DHCP 服务。如下图（图 4－106）：

图 4－106 DHCP 配置-基本配置

- 状态：该功能在出厂时默认为“禁用”状态。需要开启该功能时“启用”即可。
- 域名：如果有指定的域名可以填写在文本框内，该选项可以为空。
- LAN 口作用域网段：定义 LAN 口作用域网段，地址网段必须和 LAN 为同一网段。
- LAN 口地址范围：分配给内网通过 LAN 口进行访问的地址范围。
- LAN 口分配网关：分配给内网通过 LAN 口进行访问的网关地址
- FUNC 口作用域网段：定义 FUNC 口作用域网段，地址网段必须和 FUNC 口同一网段。

- ◆ FUNC 口地址范围：分配给内网通过 FUNC 口进行访问的地址范围。
- ◆ FUNC 口分配网关：分配给内网通过 FUNC 口进行访问的默认网关。
- ◆ 租约期限：管理员自行设置租约天数。
- ◆ 分配 DNS：管理员可以自行分配 DNS 地址，DNS 服务器最多可设置 3 个。
- ● 提交：提交后 DHCP 基本配置生效。
- ● 重置：恢复到修改前的配置参数。

静态绑定列表

在“静态绑定列表”中，管理员可以为特殊地址进行静态绑定服务，从而使通过 DHCP 获得的 IP 地址不变。如下图（图 4－107）：

图 4－107 DHCP 配置-静态绑定列表

- ◆ IP 地址：可以为指定 PC 分配固定的 IP 地址。
- ◆ MAC 地址：点击“手工扫描”，系统将自动扫描出当前输入 IP 的实际 MAC 地址和计算机名。MAC 地址的填写也可以通过手工输入来进行填写。
- ◆ 启用 IP-MAC 绑定：勾选该选项后，当前 IP 地址和 MAC 地址进行绑定。
- ◆ 启用 DHCP 静态绑定：勾选该选项后，DHCP 静态绑定生效。
- ◆ 用户名：对绑定 IP 地址进行名称描述。
- ● 提交：提交后所做配置即可生效。
- ● 重置：恢复到修改前的配置参数。
- ● 搜索：管理员可输入关键字进行搜索。
- ◆ 修改：对单个静态 DHCP 规则进行修改操作。如果此时为“禁用”状态，点击修改后会显示为“启用”状态。
- ◆ 删除：对单个的静态 DHCP 规则进行删除操作。

4-14-2 DNS 转发配置

在此子模块中，通过“启用”该功能模块，NEUSOFT VPN 设备会将 DNS 查询请求转发到此处设置的 DNS 服务器上。如下图（图 4－108）：

图 4－108 DNS 转发配置

4-14-3 集群模块

NEUSOFT VPN 集群技术支持在多线路或者多设备的情况下，对外提供更稳定、更可靠、更快速的的 VPN 解决方案，在线路出现问题或设备宕机的情况下能自动将 VPN 数据流和上网数据流切换到正常的线路上或转到另一台设备上，从而实现线路备份、设备备份、快速分流等功能。该功能模块为增值功能，仅在高端设备上开放。

状态

在“状态”子模块中，显示当前集群配置信息。默认情况下是“禁用”状态。如下图（图 4—109）：

图 4—109 状态显示

集群配置

NEUSOFT 3000 以上系列支持单机双线路备份、双机双线路备份以及双机单线路备份功能，根据具体的业务情况可对设备进行集群配置。如下图（图 4－110）：

图 4－110 集群配置

4-15 系统管理

本模块包括以下子配置模块：“启动列表”、“修改密码”、“时间设置”、“备份配置”、“恢复配置”、“日志管理”、“超时设置”，“系统升级”、“系统重启”。

启动列表

“启动列表”子模块中，显示了设备默认状态下开机启动的服务选项，启动项目包括“TC”、“SSH”、“WEB”、“VPN”、“SSL”、“PPTP”、“DHCP”、“DNS”、“CLUSTER”。如下图（图 4－111）：

图 4－111 启动列表

4-15-1 权限管理

NEUSOFT VPN 系统支持三种管理员角色权限，其中“guset”、“user”、“admin”为系统默认角色，管理员可以另外新建不同角色管理权限的登陆用户。如下图（图 4－112）：

图 4－112 权限管理

- ◆ 用户名：创建新用户名。
- ◆ 使用权限：为新建用户赋予不同权限，权限包括“普通查看”、“完全查看”、“编辑”三种。
- ◆ 描述：对新建用户的描述。
- ◆ 密码：设置密码及确认输入密码。
- ● 提交：点击“提交”，创建新用户即生效。
- ● 取消：取消当前操作。
- ● 状态：在状态栏中，系统默认的“guest”角色和“user”角色默认是“禁用”状态，点击“×”将启用该角色权限。点击“√”则禁用该角色权限。
- ● 修改：点击“修改”，可以对选中角色进行编辑操作。

4-15-2 群组管理

“群组管理”模块中只有“主机管理”模块，下面只对“主机管理”进行说明。

主机管理

“主机管理”模块用于统一管理内网所有主机，如下图（图 4－113）：

图 4—113 主机管理

4-15-3 SNMP 配置

网络管理软件要求管理代理定期收集重要的设备信息，这些信息将用于确定网络设备和网络整体运行状态是否正常。管理器应该定期查询管理代理收集到的设备运转状态、配置及性能等方面的信息。

- 状态：默认是禁用的，需要启用
- 版本可以选择：v1 或 v2
- 只读团体名：public
- 可写团体名：private
- 位置或联系人可以随意填。如下图（图 4—114）：

图 4—114 SNMP 配置

4-15-4 时间设置

在此模块中可设置系统时间。如下图（图 4－115）：

图 4－115 时间设置

4-15-5 备份设置

在设置完毕所有的参数后，管理员可以使用此功能将设置的配置文件进行备份，便于以后恢复。如下图（图 4－116）：

图 4－116 备份配置

- ◆ 立即备份：开始备份配置文件，备份后的文件自动添加在备份日志列表中。
- ◆ 删除：选择此选项，管理员可以对配置文件进行“删除”操作。
- ● 下载：点击“下载”，可以将当前配置文件打开浏览或作为一个文件保存在需要的位置。
- ● 提交：点击“提交”后系统会自动收集已经配置过的信息。
- ● 重置：恢复到修改前的配置参数。
- ✧ 说明：最多可以在 VPN 路由器上保留 5 种配置，请下载到本地进行备份。根据设备型号不同，同型号的不同版本间的配置文件不能通用。

4-15-6 恢复设置

备份了配置文件后，在需要时可通过导入备份文件将系统恢复到备份时设置。

如下图（图 4－117）

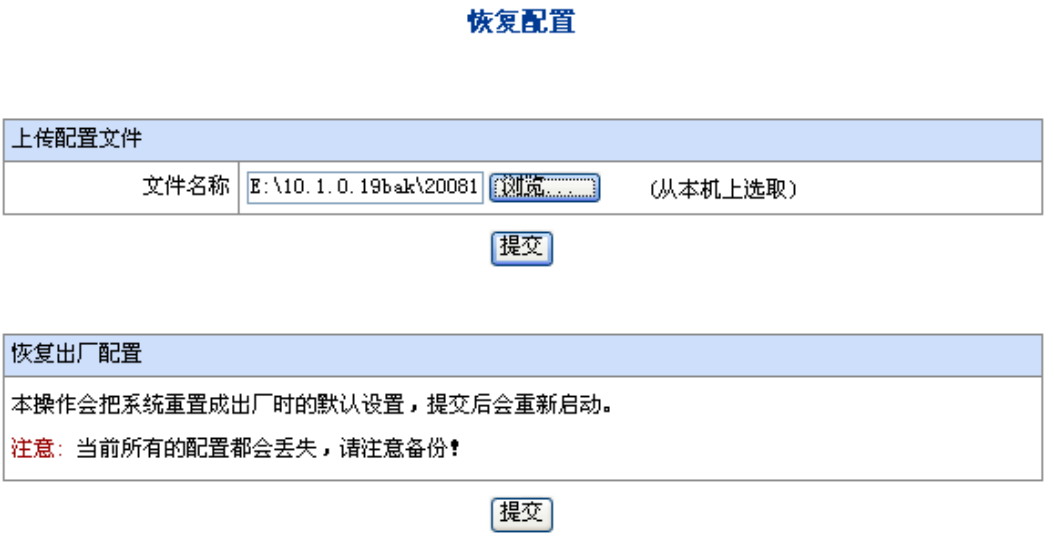


图 4－117 恢复配置

◆ 文件名称：输入备份后的配置名称。

● 提交：提交后所做操作即可生效。

✧ 说明：

恢复配置会恢复为出厂时原始设置，当前的配置会被全部清除，系统内网 IP 也变成 192.168.0.1，请谨慎使用。

4-15-7 日志管理

“日志管理”主要用来记录整个系统的运行情况及用户操作行为。完整的日志管理能够帮助用户及时了解和监控系统的工作情况，并实时记录系统的异常信息。日志信息来源于系统中所有的运行模块，日志系统完成信息的收集、管理、下载、存储、告警和显示。

如下图（图 4－118）：

图 4－118 日志管理

- ◆ 日志保存方式：管理员可将日志下载到“本地”或“远程管理”。选择远程保存方式需要“东软 VPN 监控中心”支持。
- ◆ 日志最大行数：管理员用户可自行修改最大行数，最小为 100 行。当日志文件超过指定行数，将生成当前日志备份文件，再清空日志。
- ◆ 日志等级：日志等级分为“调试”、“信息”、“警告”、“错误”和“严重”五种级别。
- ◆ 自动告警提示：勾选该选项后，当有新的告警日志时，系统会自动弹出告警对话框提醒用户查看。
- ◆ 日志磁盘：在此选项中可以很清楚查看到总的容量、已经使用的容量、空闲容量和使用率。当日志空间超过 80%显示黄色，超过 90%显示红色。
- ◆ 日志类型：日志包括“系统”、“VPN”、“移动用户”、“防火墙”、“访问”、“告警”、“错误”和“调试”八种类型。对于每一种类型都可以选择“启用”功能，查看各日志类型的使用空间和当前的行数。
- ● 下载：选择“下载”可以将日志信息下载到本地保存或查看。
- ● 压缩备份：选择“压缩备份”，将生成当前日志备份文件，再清空日志信息至历史日志。
- ● 历史日志：历史日志记载了所有备份的日志文件，点击“历史日志”可以查看历史日志详细列表。在列表中，可以将日志下载到本地保存，或者对日志进行“清空”处理。
- ● 提交：所做的配置提交即可生效。
- ● 重置：选择此选项对日志信息进行重新配置。

4-15-8 超时设置

此模块可设置管理员在设定时间内无操作后，系统自动退出，防止其他非授权用户进入系统修改配置。如下图（图 4－119）：

图 4－119 超时设置

4-15-9 系统重启

点击重启。本操作将会使系统热启动。

4-16 统计报表

统计报表是 VPN 设备访问历史记录。主要是记录 SSL VPN 用户登录信息统计，查询，SSL VPN 用户在线时长统计查询，VPN 资源访问统计查询。

这些记录对于管理员来说是很有用的，通过查询来统计某个用户的登录次数，在线时长，访问了哪些资源，是如何退出等。

4-16-1 概述

- 今日 SSL VPN 用户登录：是对今日 SSL VPN 用户登录次数的排名（前十），点击“更多”可以查看今日所有用户登录统计的详细信息，转到统计页面的时候还可以查看每个用户的详细登录信息列表（这里的登录包含登录成功和登录失败）如下图（图 4－120）：

图 4—120 统计报表概述

4-16-2 SSL VPN 用户登录

- 查询条件：
- 用户（最长 48 位）
- 组名（最长 48 位）
- 时间范围（自定义时间和预定义时间）
- 查询条件可相互组合来查询（如果全部默认的话，是今天的所有用户统计信息）
- 统计结果：是查询出来的用户排名，按登录次数排名。点击登录次数可以重排名。有最后一次登录时间和最后一次登录 IP 记录。
- 点击用户名或者登录次数，会有该用户的详细统计信息。统计结果有记录时间，用户，组名，登录类型，登录 IP，分配 IP，客户端版本，登录行为，认证方式，增强认证记录。
- 每页显示有 20，30，50，100，200 选择。
- 点击导出可以将查询出的用户统计信息导出到本地。如下图（图 4－121）：

图 4—121　SSLVPN 用户登录

- 查询条件：
- 用户（最长 48 位）
- 组名（最长 48 位）
- 登录类型（客户端，webssl）
- 登录 IP（用户登录使用的本地 IP）
- 分配 IP（客户端登录后获得的 IP）
- 客户端版（客户端登录后获得的 IP 所使用的客户端版本）
- 登录行为（登录成功，登录失败，用户主动退出，超时提出，管理员断开）
- 认证方式（本地认证，AD，Radius，LDAP，数据库）
- 双因子增强认证，（精确是全部匹配，模糊是只需匹配其中一项，密码认证，ISK，硬件特征码）
- 时间范围（自定义时间和预定义时间）
- 查询条件可相互组合来查询（如果全部默认的话，是今天的所有用户统计信息，要选用模糊查询）
- 统计结果：有记录时间，用户，组名，登录类型，登录 IP，分配 IP，客户端版本，登录行为，认证方式，增强认证记录。点击记录时间可以重排名。
- 每页显示有 20，30，50，100，200 选择。
- 点击导出可以将查询出的用户统计信息导出到本地。如下图（图 4－122）：

图 4-122 用户查询

4-16-3 SSL VPN 用户在线时长

今日 SSL VPN 用户在线时长：是对今日 SSL VPN 用户在线时长的排名（前十），点击“更多”可以查看今日所有用户在线时长的详细统计信息，转到统计页面后，还可以点击用户名来查看每次登录的在线时长

- 查询条件：
- 用户（最长 48 位）
- 组名（最长 48 位）
- 时间范围（自定义时间和预定义时间）
- 查询条件可相互组合来查询（如果全部默认的话，是今天的所有用户统计信息）
- 统计结果：是查询出来的用户排名，按在线时长排名。点击在线时长可以重排名。
- 点击用户名或者登录次数，会有该用户的详细统计信息。统计结果有登录时间，用户，组名，登录类型，登录 IP，分配 IP，客户端版本，退出时间，在线时长。
- 每页显示有 20，30，50，100，200 选择。
- 点击导出可以将查询出的用户统计信息导出到本地。如下图（图 4－123）：

图 4—123 用户在线时长

4-16-4 SSL VPN 资源访问

今日 SSL VPN 资源访问：是对今日访问的资源次数的排名（前十），点击“更多”可以查看今日所有资源访问记录，点击资源名称还可以查看访问资源的用户

- 查询条件：
- 用户（最长 48 位）
- 组名（最长 48 位）
- 时间范围（自定义时间和预定义时间）
- 查询条件可相互组合来查询（如果全部默认的话，是今天的所有用户统计信息）
- 统计结果：是查询出来的资源排名，按访问次数排名。点击资源访问次数可以重排名。
- 点击资源名称，会有该资源的详细统计信息。统计结果有时间，用户，组名，登录类型，登录 IP，分配 IP 资源名称。
- 每页显示有 20，30，50，100，200 选择。
- 点击导出可以将查询出的资源访问统计信息导出到本地。如下图（图 4－124）：

图 4—124 资源访问量

- 查询条件：
  用户（最长 48 位）
  组名（最长 48 位）
  登录类型（客户端，webssl）
  登录 IP（用户登录使用的本地 IP）
  分配 IP（客户端登录后获得的 IP）
  客户端版（客户端登录后获得的 IP 所使用的客户端版本）
  查询条件可相互组合来查询（如果全部默认的话，是今天的所有用户统计信息）
- 统计结果：有时间，用户，组名，登录类型，登录 IP，分配 IP，客户端版本，退出时间，在线时长。点击时间可以重排名
  每页显示有 20，30，50，100，200 选择。
  点击导出可以将查询出的资源访问统计信息导出到本地。如下图（图 4－125）：

图 4—125 资源查询

4-17 退出

点击配置页面左侧“退出”，将弹出提示对话框“您是否确认现在退出？”，选择“确定”，退出 NEUSOFT VPN 配置页面。

5. NEUSOFT VPN Console 口配置

第一次安装使用 NEUSOFT VPN 产品时，可以通过配置口（Console）进行配置。

5-1 配置电脑（超级终端）

将 NEUSOFT VPN 设备 Console 口和一台 PC 机的 Com 口用 RS232-RJ45 配置线连接起来。

第一步：启动计算机，打开开始——程序——附件——通讯——超级终端。打开超级终端软件。

若按照上列目录没有找到该软件，用户可以按照“我的电脑\控制面板\删除添加程序”路径来打开“安装删除程序|属性”窗口，选择“Windows 安装程序”选项，在“组件”列表框中找到“通讯”，双击，弹出“通讯”窗口如下图所示（图 5－1）：

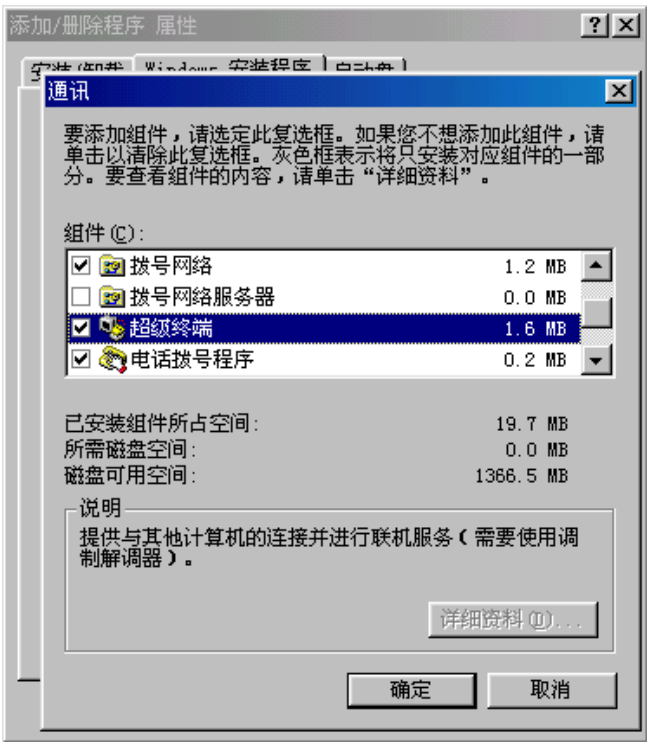


图 5－1 通讯窗口

勾选“超级终端”前面的方框，选择“确定”按钮。再选择“安装删除程序|属性”窗口中“确定”按钮，此时将 Windows 安装光盘放入光驱，安装完成超级终端。

打开超级终端软件后，新建一连接，任意输入一个“名称”，如“admin”，如下图（图

5－2）：

图 5－2 连接描述

第二步：点击“确定”进入下一步，出现如下窗口（图 5－3）：

图 5－3 连接窗口

✧ 如果把 NEUSOFT S 系列 VPN 通过串口线连接在计算机的串口 1 上，这里就选择“直接连接到串口 1”，确定，弹出“COM 1 属性”窗口，如果 Console 线连在电脑的 Com3 口上，在超级终端中就需要选择 Com3 口。

第三步：“确定”进入下一步，在窗口中点击“还原为默认值（R）”，如下图（图 5－4）：

图 5—4 属性

点击“确定”即进入超级终端命令行进行配置了。

5-2 基本配置

首次登陆 NEUSOFT VPN 设备，主要有三个步骤：

第一步：公网连接配置（ADSL，Cable Modem，FTTB+LAN，DDN）；

第二步：输入使用 VPN 网络的许可证（License）；

第三步：配置本地网络。

NEUSOFT VPN 在第一次启动时，会自动要求用户输入必要的相关信息。用户按步骤输入正确的信息后，系统就能正常运行。

用户名: admin 密码: neusoft (出厂默认值，均为小写)

在用户第一次登录时系统会提示用户需要修改默认密码，用户可以在此时修改密码，也可选择稍后再修改。

第一步：公网连接配置

输入用户名和密码登陆后，进入网络配置界面，如下图（图 5—6）：

- 输入 2 选择“ ddn ”模式
- 进入“ddn”配置选择。选择“yes”，输入给定的“IP”，“Netmask”和“Gateway IP

“，选择”no“，略过 ddn 配置。进入控制界面后，在特权模式内，输入“# config ddn ”也可以配置。

图 5—6 DDN 配置 1

第二步：进入“License 设置”，选择“yes”,输入厂商提供的组名、节点名、License 信息，选择“no”，略过 License 配置，进入控制界面后，在特权模式下，输入“#config license”也可以进行配置。如下图（图 5—7）：

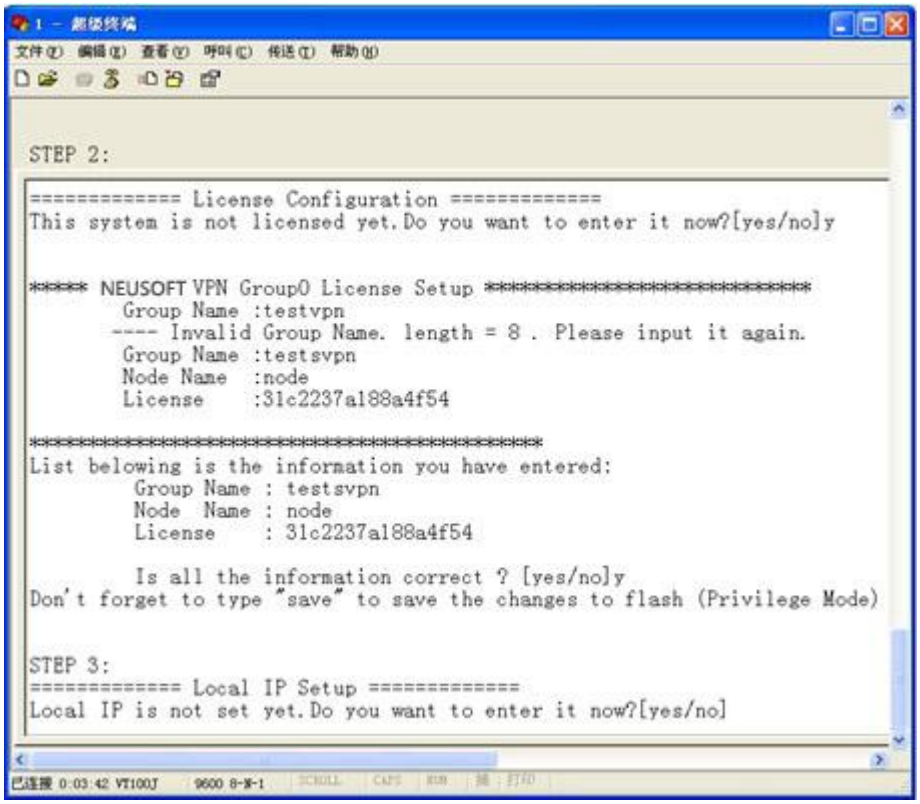


图 5—7 DDN 配置 2

第三步：进入“Local IP”配置选择。选择“yes”，输入分配好地局域网 IP，选择“no”，略过 Local IP 配置，进入控制界面后，在特权模式内，输入“#config lan”也可以进行配置。

经过这三步操作，完成对 NEUSOFT VPN 初始化配置。进入“NEUSOFT >>”提示符界面。可以使用“show wan”、“show lan”、“show vpn”查看系统运行状况

6. Windows Vista 系统下移动用户使用方法

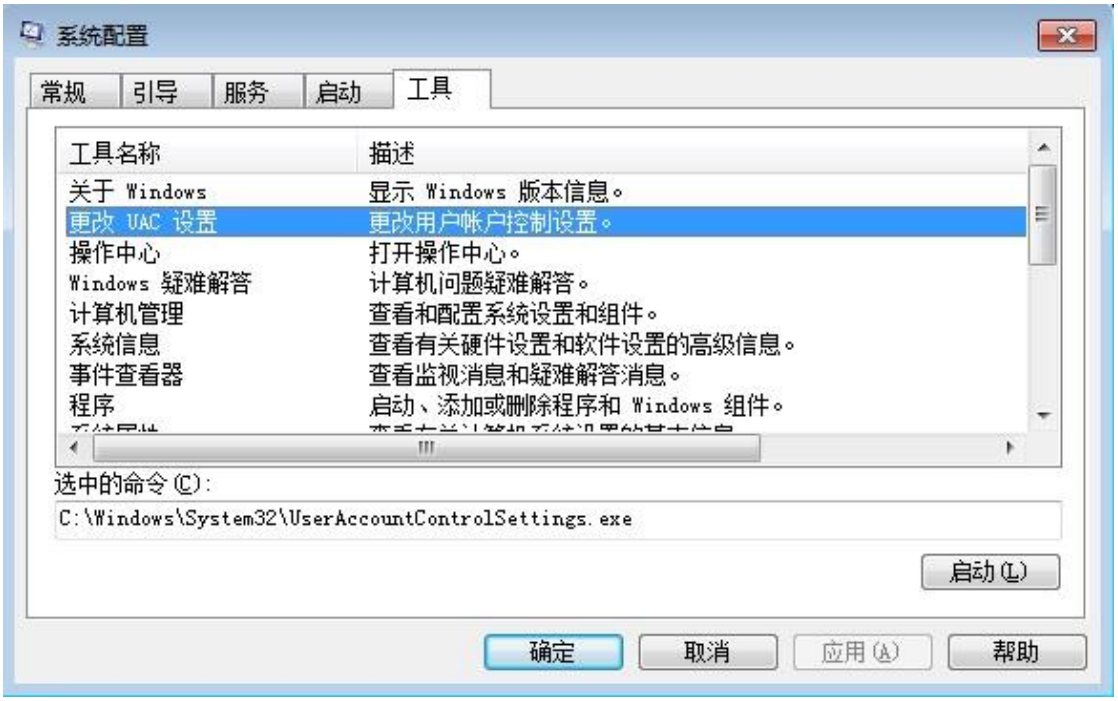
在 Windows Vista 中大幅度改进了网络功能。其中包含的新功能使网络更易于设置和使用。并增强了可管理性、安全性和可靠性。下面详细讲解用户在 Windows Vista 系统下怎样建立 NEUSOFT VPN 拨号连接。

6-1-1 Vista 系统下 SSL/PPTP 用户登陆方法

第一步：右键单击“VPNClient1.6.0.1 发行版”程序图标，选择“以管理员身份运行”，如下图（图 6—1）：

图 6—1 以管理员身份运行

打开电脑开始菜单中的运行输入 msconfig 后，点开工具中的更改 UAC 将 UAC 值设为最低（如图 6-2）


系统配置
常规
引导
服务
启动
工具
工具名称
描述
关于 Windows
显示 Windows 版本信息。
更改 UAC 设置
更改用户帐户控制设置。
操作中心
打开操作中心。
Windows 疑难解答
计算机问题疑难解答。
计算机管理
查看和配置系统设置和组件。
系统信息
查看有关硬件设置和软件设置的高级信息。
事件查看器
查看监视消息和疑难解答消息。
程序
启动、添加或删除程序和 Windows 组件。
选中的命令(C):
C:\Windows\System32\UserAccountControlSettings.exe
启动(L)
确定
取消
应用(A)
帮助

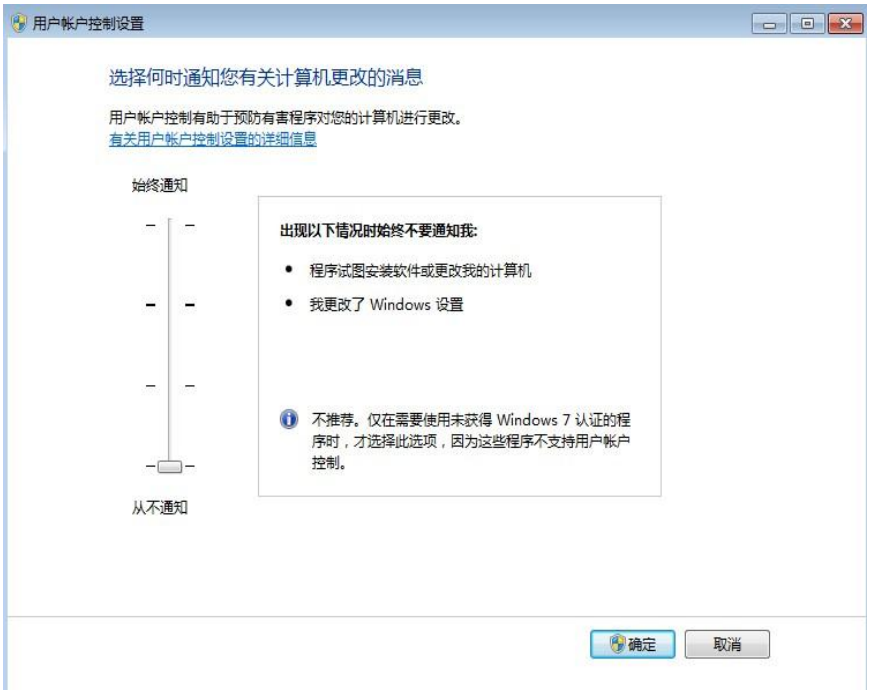

用户帐户控制设置
选择何时通知您有关计算机更改的消息
用户帐户控制有助于预防有害程序对您的计算机进行更改。
有关用户帐户控制设置的详细信息
始终通知
从不通知
出现以下情况时始终不要通知我:
程序试图安装软件或更改我的计算机
我更改了 Windows 设置
不推荐。仅在需要使用未获得 Windows 7 认证的程序时，才选择此选项，因为这些程序不支持用户帐户控制。
确定
取消

图 6－2 关闭 UAC 功能

第二步：选择“是”，重启电脑，双击客户端图标快捷方式，输入用户名和密码，点击登陆，将弹出如下对话框，如下图（图 6—3）：

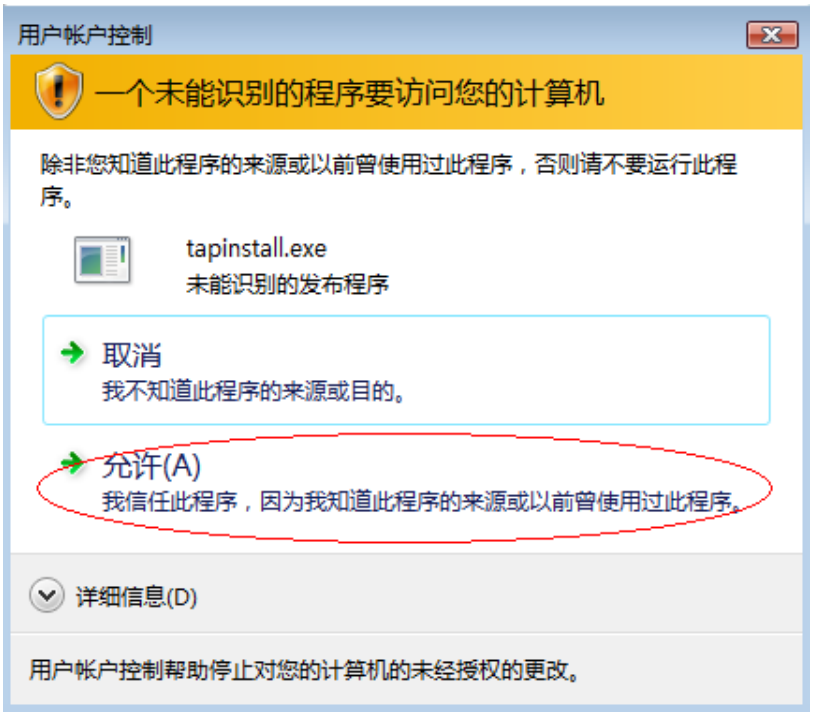


图 6—3 用户控制

选择“允许”后，开始建立隧道连接，同时会弹出 Windows 安全对话框，选择“始终安装此驱动程序软件”，如下图（图 6—4）：

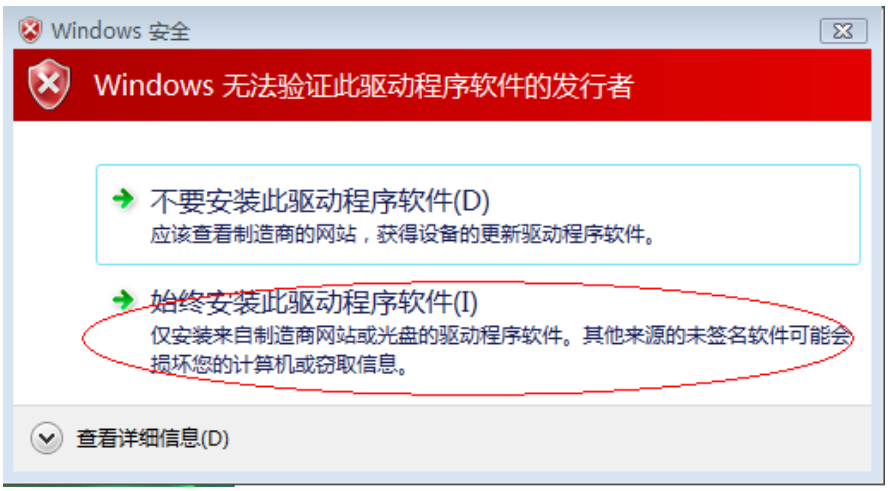


图 6—4 Windows 警告对话框

第三步：客户端隧道建立成功，右键单击右下角客户端图标，查看连接状态。此时，用户即可访问内网资源。

6-1-2 Vista 系统下 WebSSL 用户登陆方法

第一步：右键单击桌面“Internet”浏览器，选择“以管理员身份运行”，如下图（图 6—5）：

图 6－5 WebSSL 登陆 1

第二步：弹出是否允许 IE 浏览器运行，选择“允许”，如下图（图 6—6）：

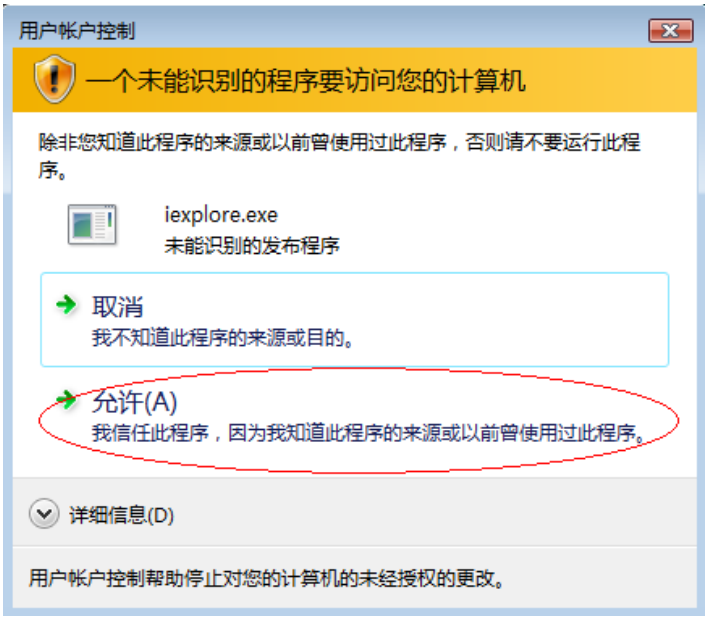


图 6－6WebSSL 登陆 2

第三步：将进入 WebSSL 登陆界面，请参照 WebSSL 用户登陆方法，这里不再进行描述。

7. FAQ 常见问题解答

7-1 硬件故障

7-1-1 NEUSOFT 设备状态是否正常

- POWER 灯是否长亮；
- 网口灯是否亮（正常状态下，网口 link 灯长亮，有数据时 active 灯闪烁）；
- 各网口长 ping 没有丢包，延时没有抖动；
- 设备前面板上的 WAN 口、LAN 口、FUNC 口指示灯有数据时是否闪烁；
- 设备重启时前面板上的 SYSTEM 灯是否闪烁；
- 是否可以通过 CONSOLE 登录 NEUSOFT 。

7-2 移动用户拨号常见问题

7-2-1 PPTP 拨号常见错误号

- 800：NEUSOFT 上 PPTP 服务没有开启，拨号时输入的域名错误；
- 756：已经拨了一个 vpn 连接；
- 691：用户名、密码错误，8 里面的域不要选，而且必须保持空白；
- 619：局域网上拨号，网关设备（防火墙、路由器、MODEM）不支持 PPTP 穿越，可以在网关设备上打开 PPTP 穿越或打开 TCP 1723 端口和 GRE 协议；GPRS 用户不支持 pptp 拨号，可以改用 ssl 拨号解决；
- 651：连接数用满；

7-2-2 SSL 拨号常见问题

- 建议安装客户端软件时，将单机上的杀毒软件和个人防火墙暂停，否则可能导致软件中某些文件安装路径不正确，从而无法拨号。
- SSL 客户端要获取的池地址或固定 IP 地址，必须和 NEUSOFT 服务器端的 LAN 口 IP 同一网段，第一次设置 SSL 用户后必须重新重启设备启用 bro 接口，本地不能与拨号端网段冲突，否则会停留在初始化连接处或拨号成功一分钟后自动重拨。
- 客户端认证端口与服务器端认证端口不一致，无法拨号。

7-2-3 WebSSL 常见问题

- WebSSL 用户登陆后不能访问资源，有可能插件没有正常安装，请卸载插件后重新安装。