



# 4WAN VPN QoS安全路由器

具负载均衡，带宽管理，VPN与网络安全功能

简体中文使用手册

## 产品功能说明手册使用许可协议

《产品功能说明手册（以下称“手册”）使用许可协议》（以下称“协议”）是用户与侠诺科技股份有限公司（以下称“侠诺”）关于手册许可使用及相关方面的权利义务、以及免除或者限制侠诺责任的免责条款。直接或间接取得本手册档案以及享有相关服务的用户，都必须遵守此协议。

**重要须知：**侠诺在此提醒用户在下载、阅读手册前阅读本《协议》中各条款。请您审阅并选择接受或不接受本《协议》。除非您接受本《协议》条款，否则请您退回本手册及其相关服务。您的下载、阅读等使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。

### 【1】知识产权声明

手册内任何文字表述及其组合、图标、界面设计、印刷材料、或电子文件等均受我国著作权法和国际著作权条约以及其它知识产权法律法规的保护。当用户复制“手册”时，也必须复制并标示此知识产权声明。否则，侠诺视其为侵权行为，将适时予以依法追究。

### 【2】“手册”授权范围：

用户可以在配套使用的计算机上安装、使用、显示、阅读本“手册”。

### 【3】用户使用须知

用户在遵守法律及本协议的前提下可依本《协议》使用本“手册”。用户若是违反本《协议》，侠诺将中止其使用权力并立即销毁此“手册”的复本。本手册“纸质或电子档案”，仅限于为信息和非商业或个人之目的使用，并且不得在任何网络计算机上复制或公布，也不得在任何媒体上传播；及不得对任何“档案”作任何修改。为任何其它目的之使用，均被法律明确禁止，并可导致严重的民事及刑事处罚。违反者将在可能的最大程度上受到指控。

### 【4】法律责任与免责声明

**【4-1】**侠诺将全力检查文字及图片中的错误，但对于可能出现的疏漏，用户或相关人士因此而遭受的直接或间接的经济损失、数据损毁或其它连带的商业损失，侠诺及其经销商与供货商不承担任何责任。

**【4-2】**侠诺为了保障公司业务发展和调整的自主权，侠诺拥有随时自行修改或中断软件 / 手册授权而不需通知用户的权利，产品升级或技术规格如有变化，恕不另行通知，如有必要，修改或中断会以通告形式公布于侠

诺网站的相关版块。

**【4-3】**所有设置参数均为范例，仅供参考，您也可以对本手册提出意见或建议，我们会参考并在下一版本作出修正。

**【4-4】**本手册为解说同系列产品所有的功能设置方式，产品功能会按实际機種型号不同而有部份差异，因此部分功能可能不会出现在您所购买的产品上。

**【4-5】**侠诺保留此手册档案内容的修改权利，并且可能不会实时更新手册内容，欲进一步了解产品相关更新讯息，请至侠诺官方网站浏览。

**【4-6】**侠诺（和/或）其各供货商特此声明，对所有与该信息有关的保证和条件不负任何责任，该保证和条件包括关于适销性、符合特定用途、所有权和非侵权的所有默示保证和条件。所提到的真实公司和产品的名称可能是其各自所有者的商标，侠诺（和/或）其各供货商不提供其它公司之产品或软件等。在任何情况下，在由于使用或档案上的信息所引起的或与该使用或运行有关的诉讼中，侠诺和/或其各供货商就因丧失使用、数据或利润所导致的任何特别的、间接的或衍生性的损失或任何种类的损失，均不负任何责任，无论该诉讼是合同之诉、疏忽或其它侵权行为之诉。

## **【5】其它条款**

**【5-1】**本协议高于任何其它口头的说明或书面纪录，所定的任何条款的部分或全部无效者，不影响其它条款的效力。

**【5-2】**本协议的解释、效力及纠纷的解决，适用于台湾法律。若用户和侠诺之间发生任何纠纷或争议，首先应友好协商解决。若协商未果，用户在完全同意将纠纷或争议提交侠诺所在地法院管辖。中国则以「中国国际经济贸易仲裁委员会」为仲裁机构。

# 目 录

1. 简介.....	1
2. 安装 VPN QOS 安全路由器 .....	3
2.1. 硬件安装介绍.....	3
2.1.1. 面板灯号 .....	3
2.1.2. 硬件 Reset 按钮.....	3
2.2. 更换系统内建电池 .....	3
2.3. 将 VPN QOS 安全路由器安装于标准 19 吋机架上.....	4
2.4. 连接防火墙到您的网络上.....	5
3. 网络基本设定与管理 .....	8
3.1. 开始登录设定 VPN QOS 安全路由器 .....	8
3.2. 首页 .....	8
3.2.1. 系统信息 .....	9
3.2.2. 端口即时状态显示 .....	10
3.2.3. 基本项目配置状态显示 .....	12
3.2.4. 进阶项目配置状态显示 .....	13
3.2.5. 防火墙项目配置状态显示.....	14
3.2.6. VPN 配置状态显示 .....	14
3.2.7. 日志记录配置状态显示 .....	15
3.3. 基本配置项目设定 .....	16
3.3.1. 网络设定 .....	16
3.3.2. 多广域网设定.....	24
3.3.3. 网络品质服务 QoS .....	40
3.3.4. 管理密码设置.....	45
3.3.5. 系统时间设定.....	46
3.4. 进阶功能配置.....	48
3.4.1. DMZ 服务器地址配置 .....	48
3.4.2. 虚拟服务器 .....	49

---

3.4.3. UPnP 通讯协议 .....	53
3.4.4. 路由通讯协议.....	54
3.4.5. 一对一 NAT 对应 .....	57
3.4.6. 动态域名解析服务（DDNS） .....	58
3.4.7. 广域网接口 MAC 地址设定 .....	61
3.5. DHCP 发放 IP 服务器.....	62
3.5.1. DHCP 设定.....	62
3.5.2 DHCP 服务器状态.....	67
<b>4. 系统工具、端口以及安全的设定 .....</b>	<b>68</b>
4.1. 工具程序.....	68
4.1.1. SNMP 网络通讯管理协议.....	68
4.1.2. 自我检测功能.....	69
4.1.3. 重新启动.....	71
4.1.4. 恢复原出厂默认值 .....	72
4.1.5. 系统软件升级.....	73
4.1.6. 系统配置参数文件备份 .....	74
4.2. 网络硬件端口管理 .....	75
4.2.1. 端口配置.....	75
4.2.2. 网络端口状态即时显示 .....	77
4.3. 防火墙配置 .....	78
4.3.1. 基本设定.....	78
4.3.2. 网络访问存取规则 .....	81
4.3.3. 网页内容管制设定 .....	86
<b>5. 虚拟私有网络的连接（VPN） .....</b>	<b>89</b>
5.1. VPN 虚拟私有网络（VPN） .....	89
5.1.1. 目前所有的 VPN 状态显示（Summary） .....	89
5.1.2. 新增一条 VPN 信道（Add New Tunnel） .....	93
5.1.3. PPTP 设定.....	119
5.1.4. 封包穿透 VPN QOS 安全路由器功能（VPN Pass Through-VPN） .....	120
5.2. QVM VPN 功能设定 .....	122
5.2.1. QVM 中心服务器端设定 .....	123

---

---

5.2.2. QVM 中央控管 .....	124
5.2.3. QVM 客户端设定 .....	124
<b>6. 日志 .....</b>	<b>127</b>
6.1. 系统日志 .....	127
6.2. 系统状态实时监控 .....	131
6.3. 网络流量状态显示 .....	132
6.4. 特定 IP 及端口状态 .....	134
<b>7. 注销 .....</b>	<b>136</b>
<b>附录一：产品中有毒有害物质或元素表 .....</b>	<b>137</b>
<b>附录二：VPN Configuration Sample .....</b>	<b>138</b>
1. Sample VPN Environment 1: Gateway to Gateway .....	138
2. Sample VPN Environment 2: Gateway to Gateway .....	139
3. Sample VPN Environment 3: Client to Gateway (Tunnel) .....	140
4. Sample VPN Environment 4: Client to Gateway (GroupVPN) .....	141
<b>附录三：常见问题解决 .....</b>	<b>143</b>
(1) QQ 容易掉线问题 .....	143
(2) 挡基本 BT 下载方式 .....	144
(3) 冲击波及蠕虫病毒的防制 .....	145
(4) 阻止 QQLive 视频直播设定 .....	147
(5) ARP 病毒攻击防制 .....	150
<b>附录四：Qno 技术支持资讯 .....</b>	<b>158</b>

## 1. 简介

4 WAN VPN QoS 安全路由器适用于中大型企业、学校、机关单位等需要弹性多 WAN 宽带配置以及注重网络联机安全的机构，是一台高效能整合型新一代防火墙。

内建了 2-4 个 10/100 Base-T/TX 以太网(RJ45) 广域网端口使用。此四个广域网端口不仅可以支持高效能网络智能负载平衡模式，指定路由，并且还支持策略路由提供弹性灵活的网络需求设定，同时还支持 DHCP、固定 IP、PPPoE、桥接模式、VPN 透通、端口绑定、静态路由、动态路由、NAT、一对一 NAT、PAT、MAC Clone、支持动态域名解析。LAN 口方面内建了数个 10/100 Base-T/TX 以太网(RJ45)端口以及 1 个 DMZ 10/100 Base-T/TX 以太网(RJ45)端口。支持虚拟主机功能、微软 UPnP 功能、VLAN、多网域以及公网 IP 透通模式，内网使用公网 IP 地址运作无障碍。

配合新一代、多样化、高安全整合性的防火墙设备需求环境，内建超高速 Intel IXP425 533MHz 高效能四核心处理器，在高速处理架构下，发挥超高的网络效能。处理速度及带机量直逼中，大型企业用户专用的昂贵 VPN QOS 安全路由器设备；并获得企业界广泛的应用系统支持。

除了宽带市场适用的对外联机能力外，具备 VPN 虚拟网络联机功能，Qno 的 VPN 通过国际 VPNC 认证，且具备目前企业广泛应用的虚拟私有网络（VPN）硬件加速模式，提供完整 VPN 功能。

Qno 支持标准的 IPSec 协议，IPSec VPN 支持 DES、3DES、AES-128 加密，MD5、SH1 认证，IKE Pre-Share Key、或是手动设定的密钥交换。支持野蛮模式，断线后自动重新联机，以及网上邻居透通。支持群组式浮动 IP 客户端与总部进行虚拟私有网联机。

具备 PPTP 服务器功能，具备联机状态显示。每个 WAN 口可同时建立多种 DDNS 设定，可使用动态 IP 建立 VPN 联机。

支持 VPN 备援功能，断线可从另一个 WAN 自动建立 VPN 联机。每个 WAN 口可同时建立多种 DDNS 设定，可使用动态 IP 建立 VPN 联机。支持 VPN 备援功能，断线可从另一个 WAN 自动建立 VPN 联机。

VPN 方面独有 SmartLink IPSec VPN 设定，只需输入 VPN 服务器 IP、用户名、密码即可自动完成 IPSec VPN 建置，进入 VPN QOS 安全路由器领先同行独家的 QVM 功能，可设定客户端与 QVM 服务器进行虚拟私有网联机，让用户简易完成 VPN 配置，无需网管也能办到，让企业享有 VPN 的优点，而不必顾虑技术及管理上的困难。中央控制的功能，可以随时通过此功能远程登录到客户端进行中央控管，安全及保密性绝对符合 IPSec 精神。支持备援功能，断线可从另一个 WAN 自动建立联机，确保 VPN 服务永不断线。

VPN QOS 安全路由器内建进阶型防火墙功能，能够阻绝大多数的网络攻击行为，使用了 SPI 封包主动侦测检验技术，封包检验型防火墙主要运作在网络层，执行对每个连接的动态检验，也拥有应用程序的

警示功能，让封包检验型防火墙可以拒绝非标准的通讯协议所使用的连接，默认自动侦测并阻挡。VPN QOS 安全路由器亦同时支持使用网络地址转换 NAT 功能以及 Routing 路由模式，使网络环境架构更为弹性，易于规划管理。

通过网页内容管制设定，允许企业内部自定网络存取规则，管理页面内建可新增移除的过滤名单，可让用户选择应该禁止存取或记录监控哪些种类的网站，如此可对学校或企业的 Internet 管理有明确的作用，设置过滤设定并通过完整的 OS 管理核心进行管理。VPN QOS 安全路由器提供线上多样化的系统日志记录，支持线上管理设定工具，可清楚易懂的知道网络设定状态、并加强管理全部的网络安全存取规则、VPN、及其它服务等。

VPN QOS 安全路由器能充分保障各种分支机构办公室及各点间通讯的安全，避免日益趋多的商业机密窃取与攻击破坏等。专属的 OS 独立式作业平台，使用者无须具备专业级的网络知识即可安装使用。通过浏览器如:IE, Netscape...来设定与管理 VPN QOS 安全路由器。



## 2. 安装 VPN QOS 安全路由器

本章节主要介绍 VPN QOS 安全路由器的硬体安装过程以及可通过外观看到的信息参数。

### 2.1. 硬件安装介绍

#### 2.1.1. 面板灯号

LED	颜色	描述
电源-Power	绿灯	绿灯亮: 电源开启连接
自我测试-DIAG	橘灯	橘灯亮: 系统尚未完成开机自我检测功能。 橘灯熄灭: 系统已经正常完成开机自我检测功能
联机/动作-Link/ACT	绿灯	绿灯亮: 以太网网络联机正常 绿灯闪烁: 以太网网络端口正在传送/接收封包数据传输
速度-100M	橘灯	橘灯亮: 以太网网络联机在 100Mbps 的速度 橘灯熄灭: 以太网网络联机在 10Mbps 的速度
连接-Connect	绿灯	绿灯亮: 当 WAN 端联机并取得 IP 地址 绿灯熄灭: 当 WAN 端联机并未取得 IP 地址

#### 2.1.2. 硬件 Reset 按钮

动作	描述
按下 Reset 按钮 5 秒	热开机, 重新启动 VPN QOS 安全路由器 DIAG 灯号: 橘色灯号慢慢闪烁
按下 Reset 按钮 10 秒以上	恢复原出厂默认值(Factory Default) DIAG 灯号: 橘色灯号快闪

## 2.2. 更换系统内建电池

VPN QOS 安全路由器 内建有系统时间的电池。此电池使用寿命约为 1~2 年。当电池已经无法充电或是使用寿命结束后, VPN QOS 安全路由器将无法正确记录时间或是连接网际网络的同步 NTP 时间服务器, 您必须与系统厂商联系, 以便取得更换电池的技术。

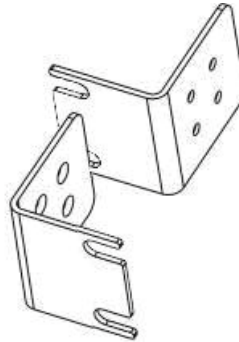
**注意！**

为了产品的正常运行，请勿自行更换电池，以免造成产品无法恢复的损坏！

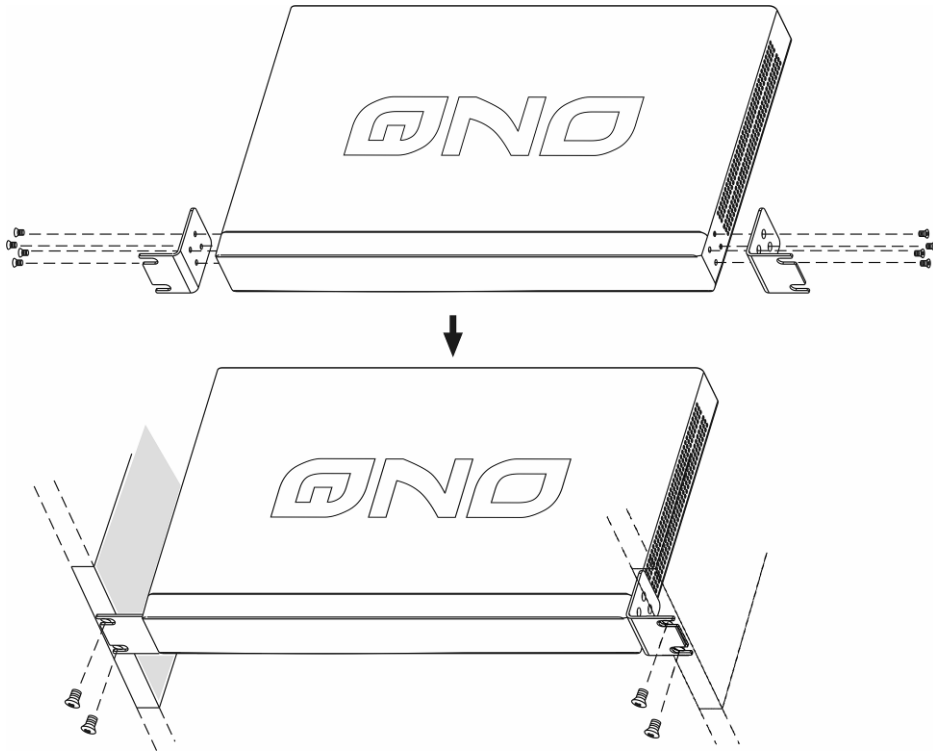
## 2.3. 将 VPN QOS 安全路由器安装于标准 19 吋机架上

建议您可以将 VPN QOS 安全路由器放置于桌上使用，或是您有机房专用 19 吋标准机架的话，可以将 VPN QOS 安全路由器安装于机架上，每一台 VPN QOS 安全路由器都有配备专用连接机架配件。当您安装 VPN QOS 安全路由器于机架上的时候，请注意不要将其它过重的物品堆栈或是放置于机器上，以免因重量过重无法承受而发生危险或是损伤机器本体。

每一台 VPN QOS 安全路由器都有配备专用连接机架配件，包含 2 只 L 型锁附架以及八颗专用螺丝，用来将 VPN QOS 安全路由器安装在机架上使用。



安装于您的 19 吋标准机架上的方法如下图所示：

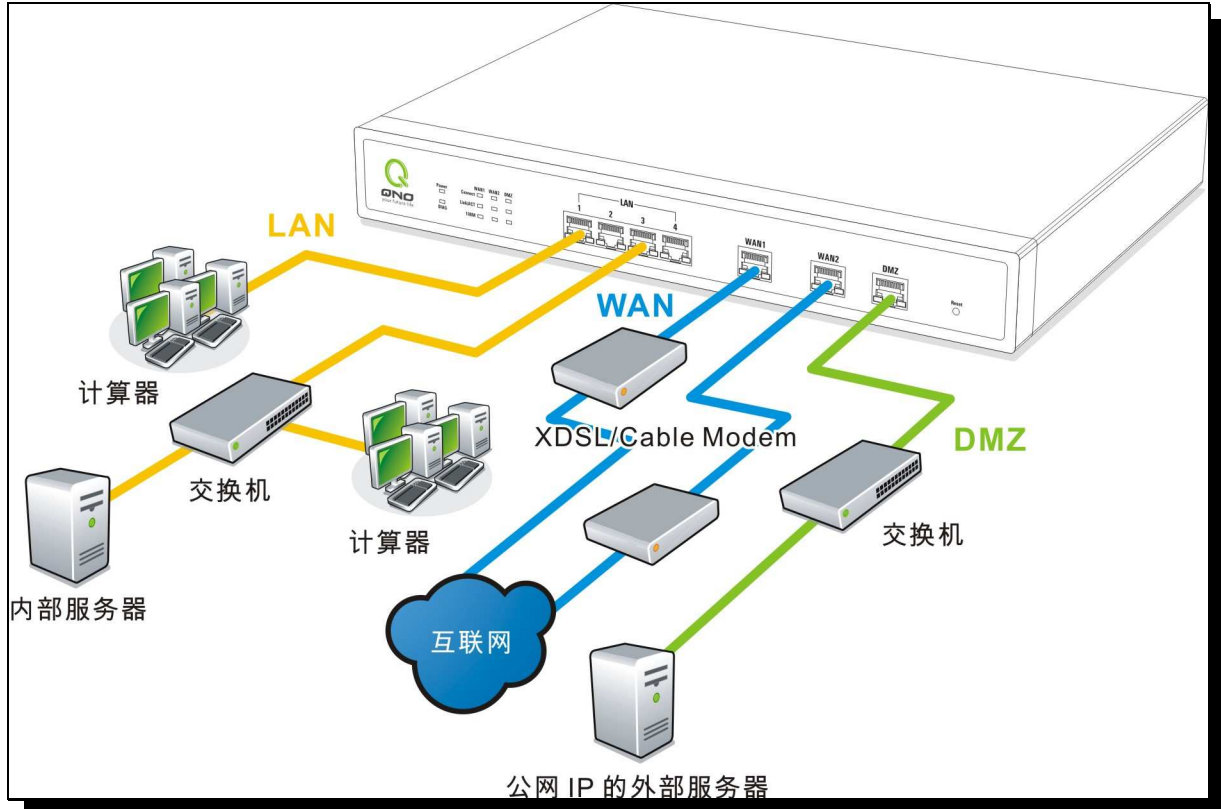


**注意！**

为了产品的稳定运行，无论您是如何放置防火墙，请不要阻塞产品两侧通风口的任何一侧，并保持通风口有 10 厘米以上的通风空间！

## 2.4. 连接防火墙到您的网络上

VPN QOS 安全路由器同时具备四个广域网接口以及硬件 DMZ 的端口口，因此您可以连接 VPN QOS 安全路由器到 Internet，并同时架设具公网 IP 地址的对外服务器。如下图所示：



### 广域网络联机：

连接 xDSL Modem 或光纤盒来连通互联网。或是连接交换机或外部 VPN QOS 安全路由器来连通您现有的网络。

### 局域网络联机：

连接交换机或计算机。

### DMZ 端口：

此端口可以连接具有外部合法 IP 地址的服务器，如网页 Web 服务器以及 E-mail 电子邮件服务器等。

我们做好了硬件的安装与连接后，下面我们就可以通过局域网中的一台电脑进入 VPN QOS 安全路由器的 **Web 管理页面** 对 VPN QOS 安全路由器进行 **设置与管理**，对网络有更高要求的企业可以通过进阶管



理达到用户特殊的需求，同时通过进阶工具的设置与防火墙的管理达到网络安全的要求。VPN QoS 安全路由器提供虚拟专用网络（VPN）的功能，用户可以通过 VPN QoS 安全路由器简单易学的功能建设公司与分支机构的方便可靠的 VPN 连接，VPN QoS 安全路由器的日志功能可以进一步方便我们查看 VPN QoS 安全路由器的工作情况来协助管理 VPN QoS 安全路由器以及网络。

### 3. 网络基本设定与管理

本章节介绍 VPN QOS 安全路由器的广域网络和局域网络的基本设置与管理, 同时通过进阶的设置功能对网络进行更深入的设置, 通过 DHCP 的设置对内部局域网络进行相关设定。

#### 3.1. 开始登录设定 VPN QOS 安全路由器



请输入**用户名**与**密码**于上方所示密码验证字段当中, 然后按下“确定”按钮。VPN QOS 安全路由器其默认的用户名与使用者密码皆为“**admin**”, 您可以更改此登录密码! 我们强烈建议您务必更改管理密码!

#### 3.2. 首页

此首页画面(Home)显示 VPN QOS 安全路由器系统所有参数以及状态显示信息, 此信息仅提供用户读取。若您想进一步查询该细部相关设定的话, 可以点击下面对应的超级链接按钮, 可以立即进入该信息选项设定画面当中进行设置管理。此画面也显示了两种语言版本(英文与简体中文)。请按下要显示语言版本的按钮, 此按钮也会自动改变成绿色显示出目前的版本画面。

### 3.2.1. 系统信息



The screenshot shows the 'System Information' page of a QNO router. It includes a sidebar with navigation options like 'Basic Configuration', 'Advanced Configuration', and 'System Tools'. The main content area displays system details and a table of port statuses.

**系统信息**

主机序列号 : Qnoz68C0000146359      当前 软件版本资讯 : 2.0.10RC3-Qno (Jul 28 2006 18:33:09)  
 中央处理器 : Intel IXP425-533      内存 : 64MB (512Mb)      闪存 : 16MB (128Mb)  
 主机工作时间 : 0 天 14 时 32 分 54 秒  
 目前正确时间 : Thu Aug 10 2006 09:13:40

**端口即时状态显示**

端口号	1	2	3	4	5	6	7	8
接口位置	局域网	局域网	局域网	局域网	局域网	局域网	局域网	局域网
状态	激活	激活	激活	激活	激活	激活	激活	激活

端口号	9	10	11	12	13	14	15	DMZ
接口位置	局域网	局域网	局域网	广域网4	广域网3	广域网2	广域网1	DMZ
状态	激活	联机	激活	激活	激活	激活	联机	激活

#### 主机序列号:

此为显示 VPN QOS 安全路由器的机器序号

#### 当前软件版本资讯:

此为显示 VPN QOS 安全路由器的目前使用的软件版本信息

#### 中央处理器 (CPU):

此为显示 VPN QOS 安全路由器使用的 CPU 型号为 Intel IXP425-533MHz

#### 内存 (DRAM):

此为显示 VPN QOS 安全路由器使用内存(DRAM)为 64MB (512Mbit)

#### 闪存 (Flash):

此为显示 VPN QOS 安全路由器使用闪存(Flash)为 16MB (128Mbit)

### 主机工作时间：

此为显示 VPN QOS 安全路由器目前已经开机的时间

### 目前正确时间：

此为显示 VPN QOS 安全路由器 目前正确时间，但是必须注意，您需要正确设定与远程 NTP 服务器的时间同步后才会正确显示。

## 3.2.2. 端口即时状态显示

**端口即时状态显示**

端口号	1	2	3	4	5	6	7	8
接口位置	局域网	局域网	局域网	局域网	局域网	局域网	局域网	局域网
状态	联机	激活	激活	激活	激活	激活	激活	激活
端口号	9	10	11	12	13	14	15	DMZ
接口位置	局域网	局域网	局域网	广域网4	广域网3	广域网2	广域网1	DMZ
状态	激活	激活	激活	激活	激活	激活	联机	激活

在此画面会显示系统各端口实时状态，包含每一个端口(联机/激活)。使用者可以按下此状态按钮，查看各端口更详细的数据显示。

于端口信息表，会显示目前该端口设定状态，如：网络连接，端口（开启或关闭），高低优先权(高或者一般)，连接速率（10Mbps 或者 100Mbps），工作模式（半双工或者全双工），以太网网络自动侦测(激活或关闭)。





**端口 2 信息**

**整体资讯项目:**

网路连接状态	10Base-T / 100Base-TX
接口位置	局域网
线路连线状态	激活
端口配置状态	端口激活
优先级设定	一般
网路连接速率	100 Mbps
半双/全双工模式	全双工
自动侦测模式	激活
VLAN	VLAN1

**端口流量即时显示:**

接收封包计算	3445
接收封包计算	773944
传送封包计算	3523
封包传送 Byte数	1391760
错误封包统计	0

刷新 关闭

于项目表格中(StatisticsTable), 将会显示此端口的接收 Receive/传送 Transmit 的封包数以及 Byte 数 /封包错误率等计算总数量。

### 3.2.3. 基本项目配置状态显示

**基本项目配置状态显示**

<u>局域网接口IP地址</u> :	192.168.1.1	
<u>广域网1接口IP地址</u> :	192.168.10.7	<input type="button" value="释放"/> <input type="button" value="更新"/>
<u>广域网2接口IP地址</u> :	0.0.0.0	<input type="button" value="释放"/> <input type="button" value="更新"/>
<u>广域网3接口IP地址</u> :	0.0.0.0	<input type="button" value="释放"/> <input type="button" value="更新"/>
<u>广域网4接口IP地址</u> :	0.0.0.0	<input type="button" value="释放"/> <input type="button" value="更新"/>
<u>DMZ IP地址</u> :	0.0.0.0	
<u>预设网关IP地址</u> (WAN1):	192.168.10.1	
(WAN2):	0.0.0.0	
(WAN3):	0.0.0.0	
(WAN4):	0.0.0.0	
<u>域名解析服务地址(DNS)</u> (WAN1):	202.96.128.86	202.96.134.133
(WAN2):		
(WAN3):		
(WAN4):		
<u>网络品质服务配置(QoS)</u> (WAN1   WAN2   3   4):	关闭	关闭   关闭   关闭

#### 局域网端口 IP 地址 (LAN IP) :

此为显示 VPN QOS 安全路由器的 LAN 端目前的 IP 地址设定信息，系统默认为 192.168.1.1，并且可以按下该超级链接直接进入该设定项目中。

#### 广域网 1~4 端口 IP 地址 (WAN1~4 IP) :

此为显示 VPN QOS 安全路由器的 WAN 1 端口目前的 IP 地址设定信息，并且可以按下该超级链接直接进入该设定项目中。当使用者选择自动取得 IP 地址时，他会显示二个按钮分别为释放与更新。使用者可以按下释放按钮去做释放 ISP 端所核发的 IP 地址，以及按下更新按钮去做更新 ISP 端所核发的 IP 地址。当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话，他会变为显示连接与中断联机。

#### DMZ IP 地址 (DMZ IP) :

此为显示 VPN QOS 安全路由器的 DMZ 目前的 IP 地址设定信息，并且可以按下该超级链接直接进入该设定项目中。

#### 默认网关 IP 地址:

此为显示 VPN QOS 安全路由器的默认网关 IP 地址设定信息，并且可以按下该超级链接直接进入该设定项目中

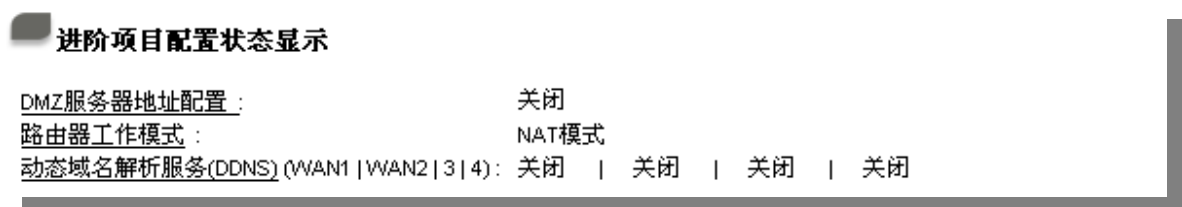
### 域名解析服务器 IP 地址（DNS）：

此为显示 VPN QOS 安全路由器的 DNS(Domain Name Server)的 IP 地址设定信息，并且可以按下该超级链接直接进入该设定项目中。

### 网络品质服务配置（QoS）：

此为显示 VPN QOS 安全路由器的 WAN 是否有使用 QoS，并且可以按下该超级链接直接进入该设定项目中。

## 3.2.4. 进阶项目配置状态显示



### DMZ 服务器地址配置（DMZ Host）：

此为显示 VPN QOS 安全路由器的 DMZ 功能选项是否激活，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为关闭。

### VPN QOS 安全路由器工作模式：

此为显示 VPN QOS 安全路由器的目前工作模式(可为 NAT Gateway 或是 Router 路由模式)，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为 NAT Gateway 模式。

### 动态域名解析服务（DDNS）：

此为显示 VPN QOS 安全路由器的 DDNS 动态 DNS 功能选项是否激活，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为关闭。

### 3.2.5. 防火墙项目配置状态显示

防火墙项目配置状态显示	
主动封包侦测过滤防火墙功能：	激活
防止DoS攻击功能：	激活
阻断广域端口的回应功能：	激活
远程管理功能：	关闭

#### 主动封包侦测防火墙功能:

此为显示 VPN QOS 安全路由器是否开启 SPI(Stateful Packet Inspection)主动封包侦测过滤防火墙功能选项是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为开启-On。

#### 防止 DoS 攻击功能:

此为显示 VPN QOS 安全路由器是否阻断来自 Internet 上的 DoS 攻击功能选项，是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为开启-On。

#### 阻断广域端口的回应功能:

此为显示 VPN QOS 安全路由器是否阻断来自 Internet 上的 ICMP-Ping 的响应功能选项，是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为开启-On。

#### 远程管理功能:

此为显示 VPN QOS 安全路由器的远程管理功能选项是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为关闭-Off。

### 3.2.6. VPN 配置状态显示

VPN配置状态显示	
VPN配置状态表：	
已经使用VPN隧道：	1
可用VPN隧道：	199
目前联机 sunny 使用者	0
目前联机 sunny1 使用者	0
PPTP服务器：	关闭

### VPN 配置状态:

此为显示 VPN QOS 安全路由器的 VPN 功能选项内容信息，并且可以按下该超级链接直接进入该设定项目中。

### 已经使用 VPN 隧道:

此为显示 VPN QOS 安全路由器的 VPN 功能目前已经设定的 Tunnel 数量。

### 可用 VPN 隧道:

此为显示 VPN QOS 安全路由器的 VPN 功能目前可使用的 Tunnel 数量。

### 如果配置了 GROUP VPN 将显示以下信息:

#### 目前联机 XXX (Group VPN 信道 1 的组名称) 使用者:

为显示 VPN QOS 安全路由器的 Group VPN 1 目前线上使用信道数量。

#### 目前联机 XXX (Group VPN 信道 2 的组名称) 使用者:

为显示 VPN QOS 安全路由器的 Group VPN 2 目前线上使用 Tunnel 数量。

若是 GroupVPN 为无设置的状态，显示没有 GroupVPN 被设定的信息。

### PPTP 服务器

显示 PPTP 服务器是否开启。

## 3.2.7. 日志记录配置状态显示

### Log 记录配置状态显示

邮件 无法传送,因为没有配置SMTP 服务器正确位置

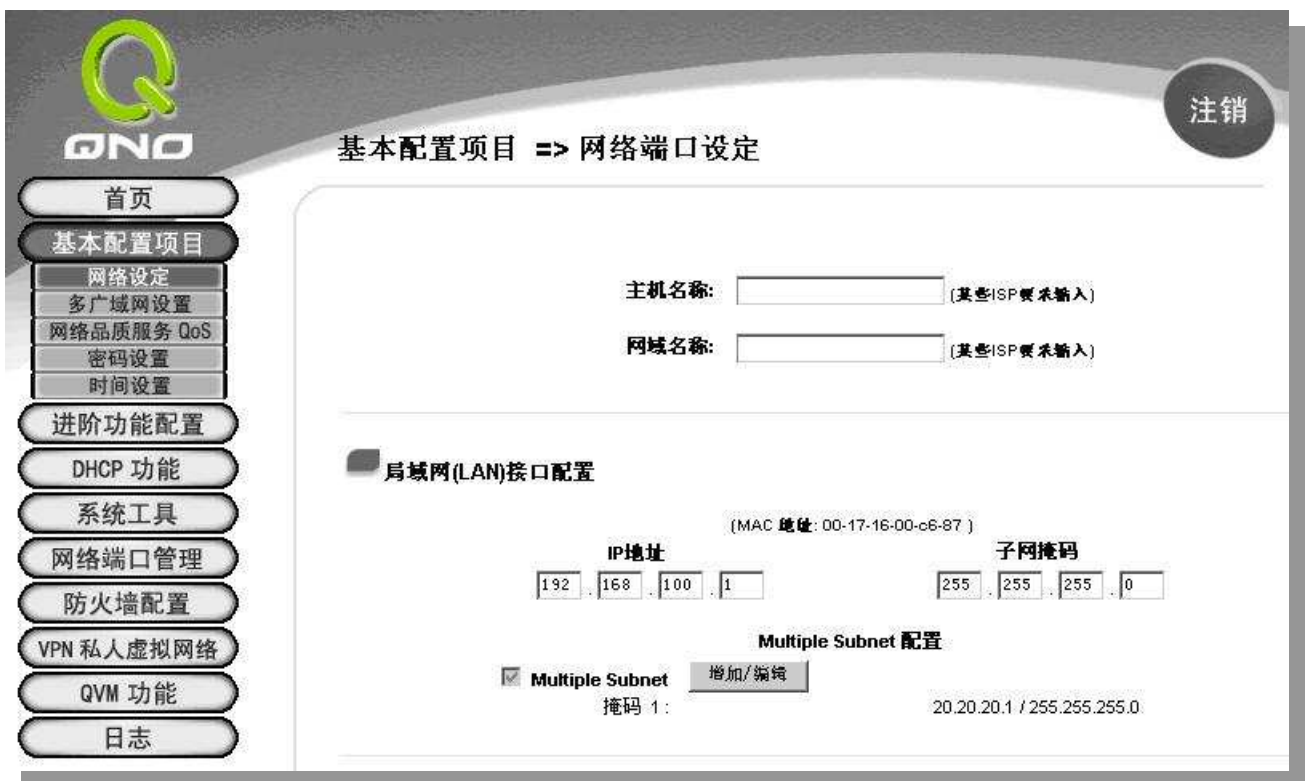
### E-Mail 的超级链接将会连到系统日志设定画面中:

1. 若您无设定电子邮件服务器于系统日志设定中，将显示您无设定电子邮件服务器所以无法发送系统日志电子邮件-“**邮件 无法传送,因为没有配置 SMTP 服务器正确位置。**”
2. 若您已经设定电子邮件服务器于系统日志设定中，但是日志尚未达到设定传送的条件时，它将显示电子邮件服务器已经设置-“**邮件 设定已经配置。**”
3. 若您已经设定电子邮件服务器于系统日志设定中，日志也已经传送出去时，它将显示电子邮件服务

器已经设置，并且已经发送-“邮件 设定已经配置并且已经发送。”

4. 若您已经设定电子邮件服务器于系统日志设定中，但是日志无法正确传出去时，它将显示电子邮件服务器已经设置，但是无法传出去，可能是设定有问题-“邮件 无法发送已经设置好邮件可能使用不正确的设定。”

### 3.3. 基本配置项目设定



此基本配置项目画面为 VPN QOS 安全路由器的基本设定内容。对大多数的用户来说，完成此项目的设定已经足够连接 Internet。当然有些情况下用户需要一些 ISP 所提供的进一步详细信息。其详细设定，请参考以下各节说明：

#### 3.3.1. 网络设定

##### 主机名称和网域名称：

可输入 VPN QOS 安全路由器的名称以及网域名称，于大多数的环境中不需做任何设定即可使用，国外有一些 ISP 可能需要用到！

主机名称:  (某些ISP要求输入)  
网域名称:  (某些ISP要求输入)

### 局域网(LAN)接口配置 (LAN Setting):

此为显示VPN QOS安全路由器的LAN端内部网络目前的IP地址设定信息,系统默认为192.168.1.1,子网掩码为255.255.255.0,可以依照您实际网络架构改动!

**局域网(LAN)接口配置**

(MAC 地址: 00-0e-a0-00-33-b8)

IP地址				子网掩码			
<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。


### Multiple-Subnet 配置:

此功能提供用户可以将不同于VPN QOS安全路由器网段的IP段填入到Multiple-Subnet后就可直接上网,也就是若原来内部环境已经有多组不同IP段组时,内部计算机不需做任何修改就可以上网,可以依照您实际网络架构改动!

**Multiple Subnet 配置**

Multiple Subnet

点击“增加/编辑”进入配置页面,如下图,填入相关IP地址段和子网掩码。



IP地址 :  .  .  .

子网掩码 :  .  .  .

增加到对应列表

删除所选择的掩码

确定 取消 离开

## WAN 口设置

### 连线类型配置

选择广域网个数 :  (预设值: 4)

接口位置	线路连线状态	配置
广域网1(WAN1)接口	自动取得 IP 地址 (线缆调制解调器使用者)	<a href="#">编辑</a>
广域网2(WAN2)接口	自动取得 IP 地址 (线缆调制解调器使用者)	<a href="#">编辑</a>
广域网3(WAN3)接口	自动取得 IP 地址 (线缆调制解调器使用者)	<a href="#">编辑</a>
广域网4(WAN4)接口	自动取得 IP 地址 (线缆调制解调器使用者)	<a href="#">编辑</a>

#### 选择广域网个数

请选择您要设定 WAN 端口的数目，默认值为 4，您可依照自己的需要加以更改

#### 接口位置

显示为第几个 WAN 端口

#### 线路连线状态

广域网络 Internet 联机形态设定:可以区分为五种:

- 自动取得 IP 地址 (Obtain an IP automatically)
- 固定 IP 地址联机 (Static IP)
- PPPoE 拨号联机 (Point-to-Point Protocol over Ethernet)
- PPTP 拨号联机 (Point-to-Point Tunneling Protocol)



- 通透桥接模式 (Transparent Bridge)

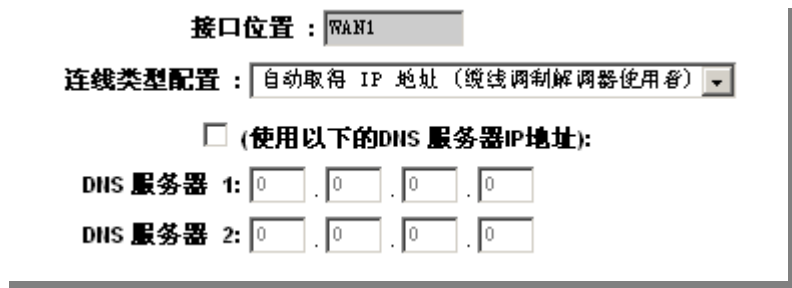
配置

显示进一步更改设定:点选 **编辑** 进入进一步设定画面

## 广域网络 Internet 联机形态设定

### 自动取得 IP 地址:

常用在 DHCP 自动取得 IP 联机形态上, 此为 VPN QOS 安全路由器系统默认的联机方式, 此联机方式为 DHCP Client 自动取得 IP 模式, 若您的联机为其它不同的方式, 请依照以下介绍并选取相关的设定。或是使用者自定 DNS 的 IP 地址, 与此选项勾选并自定填入 DNS 的 IP 地址。



**使用以下的 DNS 服务器 IP 地址:** 选择使用自定的 DNS 解析服务器的 IP 地址

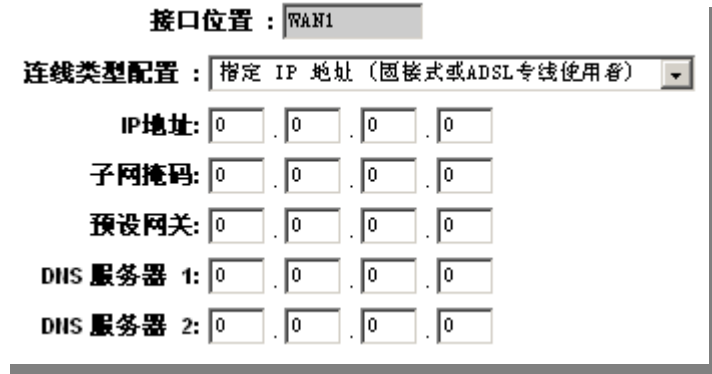
**DNS 服务器:** 输入您的 ISP 所规定的名称解析服务器 IP 地址, 最少填入一组, 最多可填二组

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 指定 IP 地址联机:

若您的 ISP 核发固定的 IP 地址给您(如 1 个 IP 或是 8 个 IP 等), 请您选择此种方式联机, 将 ISP 所核发的 IP 信息分别依照以下介绍填入相关设定参数中。

**请注意:** 有一些 ISP 虽会提供固定如一个 IP 地址给您, 但是有可能是使用如 DHCP 自动取得 IP 或是 PPPoE 拨接取得一个 IP 模式, 虽是每次都取得相同 IP 地址, 但联机模式您依然要选择正确的模式才可!



接口位置 : WAN1

连线类型配置 : 指定 IP 地址 (固接式或ADSL专线使用者)

IP地址: 0 . 0 . 0 . 0

子网掩码: 0 . 0 . 0 . 0

预设网关: 0 . 0 . 0 . 0

DNS 服务器 1: 0 . 0 . 0 . 0

DNS 服务器 2: 0 . 0 . 0 . 0

**IP 地址:** 输入您的 ISP 所核发的可使用固定 IP 地址

**子网掩码:** 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码, 如:

发放 8 个固定 IP 地址:255.255.255.248

发放 16 个固定 IP 地址:255.255.255.240

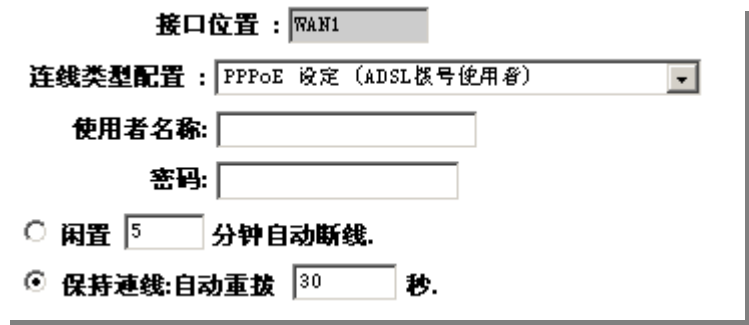
**默认网关:** 输入您的 ISP 所核发的默认网关, 若您是使用 ADSL 的话, 一般说来都是 ATU-R 的 IP 地址, 若是使用光纤接入请填写光纤转换器 IP

**DNS 服务器:** 输入您的 ISP 所规定的域名解析服务器 IP 地址, 最少填入一组, 最多可填二组。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### PPPoE 拨号联机:

此项为ADSL 计时制使用(适用于ADSL PPPoE), 填入 ISP 给予的使用者联机名称与密码并以 VPN QOS 安全路由器内建的 PPP Over-Ethernet 软件联机, 若是您的 PC 之前已经有安装由 ISP 所给予的 PPPoE 拨号软件的话, 请将其移除, 不需要再使用这些软件连接网络。



接口位置 : WAN1

连线类型配置 : PPPoE 设定 (ADSL拨号使用者)

使用者名称: [ ]

密码: [ ]

闲置 5 分钟自动断线.

保持连线:自动重拨 30 秒.

**使用者名称:** 输入您的 ISP 所核发的使用者名称。

**密码:** 输入您的 ISP 所核发的使用密码。

**闲置 ( ) 分钟断线:** 此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能, 当使用端若是有上网需求时, VPN QOS 安全路由器 会自动拨号联机, 当网络一段时间闲置无使用时, 则系统会自动离线(自动离线无封包传送时间默认为 5 分钟)。

**保持连线:** 此功能能够让您的 PPPoE 拨接连线能够保持联机, 且断线后会自动重拨, 并且可以依使用者使用方式自行设定重新拨接的时间, 默认为 30 秒。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### PPTP 拨号联机:

此项为 PPTP 计时制使用, 填入 ISP 给予的使用者联机名称与密码并以 VPN QOS 安全路由器内建的 PPTP 软件联机(多为欧洲国家使用)。



The screenshot shows a configuration window for PPTP. At the top, '接口位置' (Interface Location) is set to 'WAN1'. Below it, '连线类型配置' (Connection Type Configuration) is set to 'PPTP 设定 (ADSL 拨接 PPTP 使用者)'. There are four input fields for IP address, subnet mask, and default gateway, each with four digits. Below these are two text input fields for '使用者名称' (Username) and '密码' (Password). At the bottom, there are two radio button options: '闲置 5 分钟自动断线.' (Idle 5 minutes auto disconnect) and '保持连线:自动重拨 30 秒.' (Keep connection: auto redial 30 seconds). The second option is selected.

**IP 地址:** 此项为设定固定 IP 地址, 设定的 IP 可由您的 ISP 所提供的位置输入 (此 IP 地址各 ISP 都于装机后给予, 请咨询您的 ISP 给予相关信息)

**子网掩码:** 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码, 如:

发放 8 个固定 IP 地址:255.255.255.248

发放 16 个固定 IP 地址:255.255.255.240

**默认网关:** 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关, 若您是使用 ADSL 的话, 一般说来都是 ATU-R 的 IP 地址

**使用者名称:** 输入您的 ISP 所核发的使用者名称

**密码:** 输入您的 ISP 所核发的使用密码

**闲置（）分钟断线:** 此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，VPN QoS 安全路由器 会自动向默认的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线(自动离线无封包传送时间默认为 5 分钟)

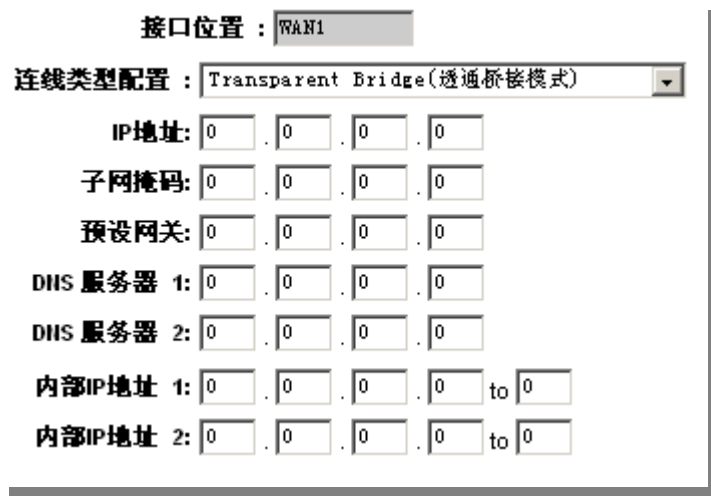
**保持连线:** 此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设定重新拨接的时间，默认为 30 秒

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 透明桥接模式:

当您内网的计算机 IP 已经都是公网 IP 而不希望将内网都改成私网 IP(例如 192.168.1.X)时，此功能可以让您不需改动原有架构，立即整合到既有网络中。选择广域网联机方式为透明桥接模式，这样您就可以保留内网计算机的 IP 设定为原本的公网 IP 仍然可以正常上网。

当您设定两个广域网时，广域网的联机模式选择此种透明桥接模式，还是可以做到负载均衡。



接口位置 : WAN1

连线类型配置 : Transparent Bridge(透明桥接模式)

IP地址: 0 . 0 . 0 . 0

子网掩码: 0 . 0 . 0 . 0

预设网关: 0 . 0 . 0 . 0

DNS 服务器 1: 0 . 0 . 0 . 0

DNS 服务器 2: 0 . 0 . 0 . 0

内部IP地址 1: 0 . 0 . 0 . 0 to 0

内部IP地址 2: 0 . 0 . 0 . 0 to 0

**IP 地址:** 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个

**子网掩码:** 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码，如:

发放 8 个固定 IP 地址:255.255.255.248

发放 16 个固定 IP 地址:255.255.255.240

**默认网关:** 输入您的 ISP 所核发的可使用固定 IP 地址的默认通讯闸，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址

**DNS 服务器:** 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少须填入一组，最多可填二组

**内部 IP 地址:** 输入您的 ISP 所核发的可使用固定 IP 范围。若是您的 ISP 分给您两个不连续的 IP 地址范围，您可以分别填入**内部 IP 地址 1** 以及**内部 IP 地址 2**

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 非军事区 (DMZ) 设定

于某些网络环境应用来说，您可能会需要用到独立的 DMZ 非军事管制区接口来置放您的对外服务的服务器，如 WEB 与 Mail 服务器等；VPN QOS 安全路由器 提供一组独立的 DMZ 接口来设定连接于合法 IP 地址的服务器。此 DMZ 接口为连接 Internet 与局域网络之间的沟通桥梁。

**DMZ 配置**

接口位置	IP地址	配置
DMZ	0.0.0.0	<a href="#">编辑</a>

- 接口位置:** 显示为 DMZ 端口。
- IP 地址:** 显示目前默认的固定 IP 地址。
- 配置** 显示进一步更改设定:点选[编辑](#)进入进一步设定画面。

此 DMZ 的设定可分为 Subnet 及 Range 两种:

#### Subnet: DMZ 与广域网络 WAN 位于不同的子网络 Subnet 中

比如 ISP 分配给你 16 个合法 IP:220.243.230.1-16 Mask 255.255.255.240 时，你必须将此 16 个 IP 再切两组变成 220.243.230.1-8 Mask 255.255.255.248 及另一组 220.243.230.9-16 Mask 255.255.255.248，然后 Router 及 Gateway 是在同一组，再将另一组设定在 DMZ 中。

接口位置 :

**Subnet**
                         
  **Range**(DMZ与广域网口IP地址相同子网掩码)

DMZ IP地址:  .  .  .

子网掩码:  .  .  .

- DMZ IP 地址:** 输入位在 DMZ 端口的 IP 地址。
- 子网掩码:** 输入位在 DMZ 端口的 IP 地址所对应的子网掩码。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### Range: DMZ 与广域网络 WAN 位于相同的子网络 Subnet

接口位置:

Subnet
  Range(DMZ与广域网口IP地址相同子网掩码)

接口位置:

IP地址范围:  .  .  .  to

IP 地址范围: 输入位在 DMZ 端口的 IP 范围

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.3.2. 多广域网设定



基本配置项目 => 多广域网设置

注销

模式

智慧型负载均衡      均衡模式:       速键数均衡       IP均衡  
 指定路由              未绑定端口均衡模式:       速键数均衡       IP均衡  
 策略路由              均衡模式:               速键数均衡       IP均衡

网通策略:              
 自订策略一:        
 自订策略二:     

接口配置

接口位置	模式	配置
广域网1	全自动	<a href="#">编辑</a>
广域网2	全自动	<a href="#">编辑</a>
广域网3	全自动	<a href="#">编辑</a>
广域网4	全自动	<a href="#">编辑</a>

### 3.3.2.1. 智能型负载均衡模式

当您选用智能负载均衡模式，VPN QoS 安全路由器将以联机数或是 IP 联机数为基础，并依据您广域网线路的带宽来自动分派联机，达到对外联机的负载均衡。线路的带宽是依据您所填入的带宽设定，例如当两条广域网都为上行 512Kbit/sec 时，其自动负载比例为 1:1，当一条线路的上行带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2:1，所以为了确保你的 VPN QoS 安全路由器达到实际线路负载能够均衡，请填入实际上行下载带宽 (请参考 3.3.2.3.带宽设定说明)。

- **联机数均衡：**当您选用联机数均衡模式，VPN QoS 安全路由器将以联机数为基础，并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。
- **IP 均衡：**当您选用 IP 负载均衡模式，VPN QoS 安全路由器将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。

#### 提示！

不论是联机数均衡或是 IP 负载均衡方式，搭配“通讯协议绑定”可以有更有弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

譬如您希望指定 IP 192.168.1.100 访问外网的时候走广域网 1，或内网所有 IP 去访问服务端 80 时都是经过广域网 2，或是内网所有 IP 去目的地 IP 211.1.1.1 访问时都要从广域网 1 去访问等等，都可以经由设定此“通讯协议绑定”功能来达到你的需求。

**请注意，**当使用智能负载均衡方式搭配“通讯协议绑定”功能时，除了您指定的服务会按照您的规则出去访问外网，其它未被指定的 IP 或服务端的访问还是按照 VPN QoS 安全路由器的机制做智能负载均衡。

关于如何设定“通讯协议绑定”功能，以及智能负载均衡方式搭配“通讯协议绑定”的范例，请参考 3.3.2.5. 通讯协议绑定设定说明。

### 3.3.2.2. 指定路由

这个模式让您对特定的内网 IP、特定要访问的应用服务端、或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端、或特定目的地 IP 使用。其它不在这些指定的内网 IP、特定要访问的应用服务端、或特定目的地 IP 都会从其它的广域网出去访问。对于没有被指定的广域网，您可以选择负载均衡模式以联机数作为负载均衡的基础，或是以 IP 联机数作为负载均衡的基础。

- **未绑定端口均衡模式：**若是有部分广网端口并没有被指定，例如广域网 3 与广域网 4 并没有

指定特定的 IP、服务端、或目的 IP 来使用，这些广域网端口(广域网 3 与 4)仍然会依据 VPN QOS 安全路由器的负载均衡机制来分派联机。均衡机制如下：

- **联机数均衡：**当您选用联机数均衡模式，VPN QOS 安全路由器将以联机数(session)为基础，并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。
- **IP 均衡：**当您选用 IP 负载均衡模式，VPN QOS 安全路由器将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。

**提示！**

此指定路由必须配合“通讯协议绑定”功能才能发挥作用。例如指定让内网去访问服务端 80 时都要从广域网 1 去访问，或内网去目的地 IP 211.1.1.1 访问时都要从广域网 1 去访问等等，必须要在“通讯协议绑定”功能中做设定。

**请注意**，当使用指定路由模式，以上述的例子来看，除了您指定的服务必须按照您的规则出去访问外网都走广域网 1 以外，其它未被指定的 IP 或服务端则经由 VPN QOS 安全路由器负载均衡的机制使用其它的广域网出去。

关于如何设定“通讯协议绑定”功能，以及指定路由模式搭配“通讯协议绑定”的范例，请参考 **3.3.2.5. 通讯协议绑定 设定说明**。

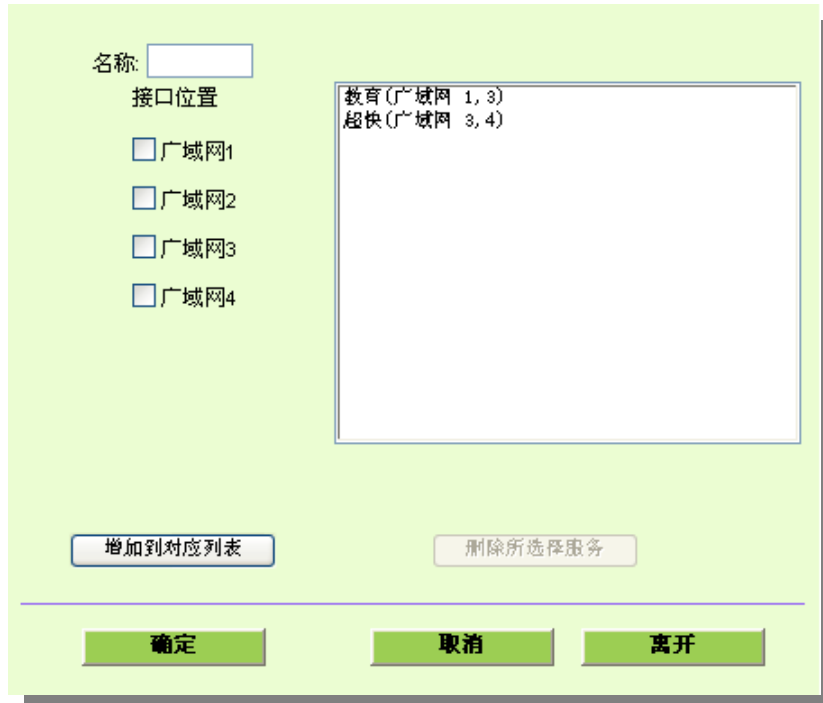
### 3.3.2.3. 策略路由

当您选用策略路由模式，VPN QOS 安全路由器会依照内建的策略(电信网通分流，用在中国大陆的环境)自动分派联机。您只需选择网通线路接入的广域网口(或广域网组合)，VPN QOS 安全路由器会自动将该走网通线路去外网访问的流量都从网通的广域网出去，对该走电信线路去外网访问的流量也都往电信的广域网出去，达到“电信走电信，网通走网通”的分流策略。

#### 广域网组合：

当您所接的网通线路不只一条，则需要做广域网的组合，以便将两个以上的广域网口合在一起做相同的策略分流。按下“广域网组合”会出现以下的对话框。





- 名称:** 在此自定的广域网组合名称，如 "教育" 等，用来辨识广域网群组
- 接口位置:** 在此勾选要设在此组合的广域网端口
- 增加到对应列表:** 增加到广域网组合列表
- 删除所选服务:** 删除所选择的广域网组合内容
- 确定:** 按下此按钮 "确定" 即会储存刚才所变动的修改设定内容参数
- 取消:** 按下此按钮 "取消" 即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效
- 离开:** 离开此功能设定画面

设定完成后，您就可以在网通策略的选择中选取您的网通接口的广域网组合。

#### 自定策略:

此外，您也可以自己建立分流策略。在"自定策略"中选择要指定的广域网口或广域网组合(例如广域网 1)，然后按下"更新网段"的按键，会出现汇入策略文件的对话框。策略文件是一个可编辑的文字文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，按下"汇入"，并在设定画面的最下方按下"确定"，VPN QOS 安全路由器就会将要往指定目的 IP 的流量从您指定的广域网(例如广域网 1)或广域网组合出去。

廣域組合設定

网通策略:

自訂策略一:

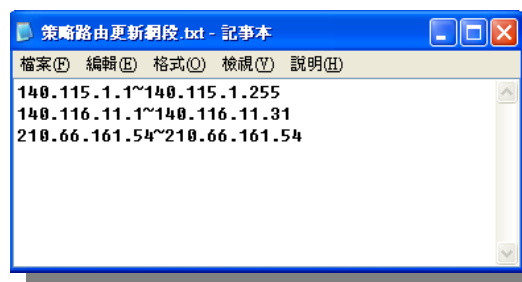
自訂策略二:

网通策略

自訂策略一

自訂策略二

策略文件的建立可以用纯文字编辑软件来撰写，例如使用 Windows 系统内建的“记事本”来建立。将您要指定的目的 IP 地址依下图的格式写入，例如您要指定的目的 IP 地址范围是从 140.115.1.1 到 140.115.1.255，则在“记事本”中输入 140.115.1.1~140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54~210.66.161.54。储存档案之后(扩展名为.txt)即可汇入自定义策略的更新网段。



**提示！**

网通策略与自定义策略可以同时存在，不过当某一个目的 IP 同时都在网通策略以及自定义策略中，会以网通策略为优先。也就是说要往该目的 IP 的流量会从网通策略的广域网(或广域网组合)出去外网。

### 3.3.2.4. 对 WAN 口的设定

在多广域网设置页面里的接口配置选择 WAN 口点击编辑进入 WAN 口设置页面进行相关配置。

**接口配置**

接口位置	模式	配置
广域网1	全自动	<a href="#">编辑</a>
广域网2	全自动	<a href="#">编辑</a>
广域网3	全自动	<a href="#">编辑</a>
广域网4	全自动	<a href="#">编辑</a>



The screenshot shows the '广域网设置' (WAN Settings) page. On the left is a navigation menu with options like '基本配置项目', '网络设定', '多广域网设置', etc. The main area is titled '基本配置项目 => 广域网设置'. It includes a '接口位置' dropdown, a text input for '填入ISP线路实际可供使用频宽', and fields for '上传频宽' (10000 Kbit/Sec) and '下载频宽' (10000 Kbit/Sec). Below these are settings for '线路侦测机制' (Line Detection Mechanism), including '重新发起测试次数' (5), '响应延迟时间' (30 秒), and '当线路连接失败时' (删除该线路). There are also checkboxes for '预设网关', 'ISP服务器', '远程服务器', and '使用DNS 服务器作域名解析'.

### 带宽设定

VPN QOS 安全路由器会依照你实际输入的上传带宽数据做为两条广域端口自动负载平衡的比例依据。例如当两条广域网都为上传 512Kbit/sec 时，其自动负载比例为 1: 1。当一条线路的上传带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2: 1。所以为了确保你的 VPN QOS 安全路由器达到实际线路负载能够均衡，请填入实际上下载带宽。另外，此字段也关系到 QoS 的设定，请参考 3.3.3.QoS 设定章节。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## 网络对外联机侦测

### 线路侦测机制：

网络对外服务侦测机制。若勾选此项设定，则会出现 **Retry Count**，**Retry Timeout** 等以下的讯息。当使用两条广域网做对外连接线路时一定将此 **NSD** 启用，以避免因为广域端口流量过大时造成 VPN QOS 安全路由器的误判将此线路判断为断线。

**重新发起测试次数：** 对外联机侦测重试次数，默认值为五次。若是于此设定次数当中，**Internet** 没有回应的话，就判断为对外线路中断！

**响应延迟时间：** 对外联机侦测逾时时间(秒)，默认值为 30 秒。于此设定秒数之后重新测试对外联机。

### 当线路连接失败时 **(1) 在系统日志中会产生错误讯息的信息：**

当侦测到与 **ISP** 连接失败时，系统就会在系统日志中将这项错误讯息记录下来，但依旧保持此线路不会移除，所以会有些原来使用此条线路上的 **User** 无法正常使用。

此选项适用在当某条广域网联机失败时，从这个广域网去访问的目的地址是无法从另一条线路去访问的时候，就可以用此选项。例如若是要访问 **10.0.0.1** 到 **10.254.254.254** 时一定要走广域网 1 去访问，而且广域网 2 是无法访问到此网段，那就可以使用此选项。因为若广域网 1 掉线后走广域网 2 也无法去访问到 **10.0.0.1** 到 **10.254.254.254**，就不需要在广域网 1 断线时将此线路移除。

### **(2) 移除有问题线路：**

当侦测到与 **ISP** 连接失败时，系统不会在系统日志中将这项错误讯息记录下来，原本使用此 **WAN** 端的封包传递会自动转换到另一条广域端口。等到原本断线的广域端口恢复后会自行重新连接，则封包传递会自动转换回来。

此选项适用在若某条广域网联机失败时，从这个广域网去访问的目的地址是可以从另一条线路去访问的时候，就要用此选项。如此可以让任何一条广域网断线的时候，另一条可以做备援，将流量转移到还在联机的广域网。

### 侦测以下可回应的服务器：

**默认网关：** 近端的默认通讯网关位置，如 **ADSL VPN QOS** 安全路由器的 **IP** 地址，此为 **Router** 自动填入，所以只需打勾选择是否启用。注意！有部分的 **ADSL** 线路的网关是不会响应侦测封包，或是当您使用光纤盒，或是运营商发给您的是固定的公网 **IP** 且网关就是在您网吧这端而不是在运营商那端时，此选项不要启动。

**ISP 服务器：** **ISP** 端的侦测位置，如 **ISP** 的 **DNS** 服务器 **IP** 地址等。在设定此 **IP** 地址时请确认此 **IP** 地址是可以且稳定快速的得到响应 (建议填入 **ISP** 端 **DNS** **IP**)。

**远程服务器：** 远程的网络节点侦测位置，此 Remote Host IP 地址最好也是可以且稳定快速的得到响应(建议填入 ISP 端 DNS IP)。

**使用 DNS 服务器做域名解析：** 网域名称端 DNS 的侦测位置(此字段只许填入网址如“www.hinet.net”，请勿填 IP 地址)。另外，两条 WAN 的此字段不可以填入相同的网址。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

**注意！**

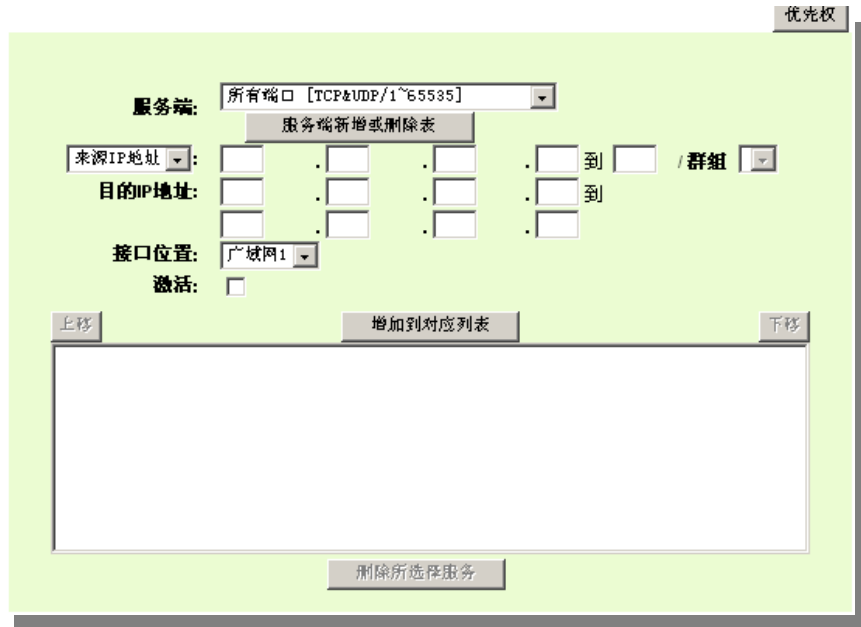
在“指定路由”的负载均衡模式下，第一个广域网口会保留给没有指定到其它广域网口(WAN2, WAN3, WAN4)的 IP 或应用服务端经由此广域网(WAN1)进出。因此建议您在此模式下将您的其中一条线路接在第一个广域网口。当您其它的广域网口(WAN2, WAN3, WAN4)断线时，而您在线路侦测机制下选择移除有问题线路，流量就会转移到第一个广域网口(WAN1)。此外，若是第一个广域网口(WAN1)断线，则流量会依次转移到其它广域网口，例如转移到 WAN2，若 WAN2 也断线则转移到 WAN3 等等。

### 3.3.2.5. 通讯协议绑定

使用者可将特定的 IP 或特定的应用服务端口经由您限定的 WAN 出去。其它没有做绑定的 IP 或服务还是会进行广域网的负载平衡。

**注意！**

在“指定路由”的负载均衡模式下，第一个广域网口(WAN1)是不能被指定的，保留给没有指定到其它广域网口(WAN2, WAN3, WAN4)的 IP 或应用服务端经由此广域网(WAN1)进出。也就是说第一个广域网口(WAN1)不能设置通讯协议绑定的规则，避免所有的广域网口都被指定有特定的内网 IP、应用服务端、目的地 IP，使其它的 IP 或应用服务端口没有广域网端口可以使用。



- 服务端:** 在此选择欲开启的绑定服务端口，从下拉式选单中可以选择默认列表(如 All-TCP&UDP 0~65535, WWW 为 80~80, FTP 为 21~21 等等), 默认的 Service 为 All 0~65535。
- 服务选单列表: 按下此按钮可以进入服务端口设定画面, 进行新增或删除选单中默认的服务端口。
- 来源 IP 地址:** 使用者可以指定特定的内部虚拟 IP 地址的封包经由特定的广域网端口出去。在此填上内部虚拟 IP 地址范围, 例如 192.168.1.100 到 150. 则 IP 地址 100 到 150 为绑定范围。如果使用者只需要设定特定的服务端口而不需指定特定的 IP 地址, 则在 IP 的字段皆填入 0。
- 目的 IP 地址:** 在此填上外部固定 IP 地址, 例如若有一目标地址 210.11.1.1, 要连接此地址的使用者限定只能从广域网端口 1 到达此目标地址, 则在此填上外部固定 IP 地址 210.11.1.1 to 210.11.1.1。如果用户要设定一个范围的目的地址, 则填入方式可以为 210.11.1.1 to 210.11.255.254, 则表示整组 210.11.x.x 的 Class B 网段都限制走某一条广域网, 若只需要设定特定的应用而不需指定特定的 IP 地址, 则在 IP 的字段皆填入 0.0.0.0。
- 接口:** 选择你所要绑定此条规则在哪个广域网端口
- 启用:** 启用此规则
- 增加到对应列表:** 增加此条规则到列表
- 删除所选服务:** 删除在服务列表里所选择的规则
- 上移 & 下移:** 由于每条规则执行的优先级为由列表的最上面那条往下执行, 也就是越后面设

定的规则会越后执行，所以你可以自行调整每条规则先后执行顺序。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

**注意！**

通讯绑定协议所设的规则在 VPN QOS 安全路由器执行时也有优先级的，在列表上最上方那条会先执行，然后依序往下。

**优先权：**

按下右上方的”优先权按钮，会出现以下的对话窗口。您可以选择以”优先权来显示排列的顺序，或是以”接口位置”来显示排列的顺序。按下”刷新”可以重新显示画面，按下”关闭”将结束这个对话窗口。

摘要						
<input checked="" type="radio"/> 优先权 <input type="radio"/> 接口位置						
优先权	接口位置	服务端	来源IP地址	目的IP地址	激活	配置
1	广域网2	所有端口[TCP&UDP/1~65535]	192.168.1.2~192.168.1.254	0.0.0.0~0.0.0.0	激活	<a href="#">编辑</a>
2	广域网2	HTTP[TCP/80~80]	192.168.5.0~192.168.5.0	0.0.0.0~0.0.0.0	激活	<a href="#">编辑</a>

**新增或删除管理服务端号**

若您欲开启的服务端口项目没有在表列中，您可以按下“服务新增或删除表”进入新增或删除管理服务端口号列表功能达成，如以下所述：



- 服务端口名称:** 在此自定义欲开启的服务端口名称加入列表中，如 BT 等
- 通讯协议:** 在此选择欲开启的服务端口的封包格式为 TCP 或 UDP
- 服务端口的位置范围:** 将你所需新增加的服务端口范围填入
- 增加到对应列表:** 增加到开启服务项目内容列表，最多可新增 100 组
- 删除所选服务端口列表:** 删除所选择的开启服务项目之一笔内容
- 确定:** 按下此按钮“Apply”即会储存刚才所变动的修改设定内容参数
- 取消:** 按下此按钮“Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效
- 离开:** 离开此功能设定画面

### 使用“智能型”负载均衡模式时其通讯协议绑定的设定方式:

智能负载均衡方式搭配“通讯协议绑定”可以有更有弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。



**范例一:若要指定内网 IP 192.168.1.100 去外网访问都走广域网 2,那通讯协议绑定设定方式?**

如以下范例所示,服务端选择”所有端口”,在来源 IP 地址填入 192.168.1.100 到 100,目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选择广域网 2,然后勾选激活。最后点击”新增”即可将此规则加入。

**通讯协议端口绑定**

**服务端:** 所有端口 [TCP&UDP/1~65535]

**来源IP地址:** 192 . 168 . 1 . 100 到 100

**目的IP地址:** 0 . 0 . 0 . 0 到

**接口位置:** 广域网2

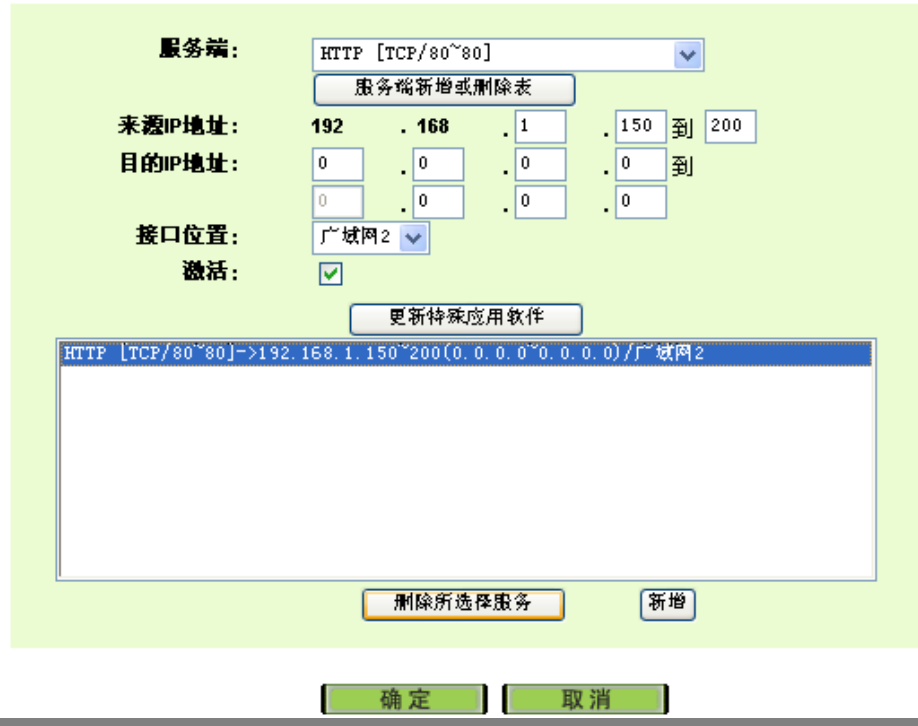
**激活:**

所有端口 [TCP&UDP/1~65535]->192.168.1.100~100(0.0.0.0~0.0.0.0)/广域网2

**范例二:若要指定内网 IP 192.168.1.150 到 200 去外网访问 80 端都走只能走广域网 2 去访问,那通讯协议绑定设定方式?**

如以下范例所示,服务端选择”HTTP[TCP/80~80]”,在来源 IP 地址填入 192.168.1.150 到 200,目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选择广域网 2,然后勾选激活。最后点击”新增”即可将此规则加入。

### 通讯协议端口绑定



服务端: HTTP [TCP/80~80]

来源IP地址: 192 . 168 . 1 . 150 到 200

目的IP地址: 0 . 0 . 0 . 0 到 0 . 0 . 0 . 0

接口位置: 广域网2

激活:

更新特殊应用软件

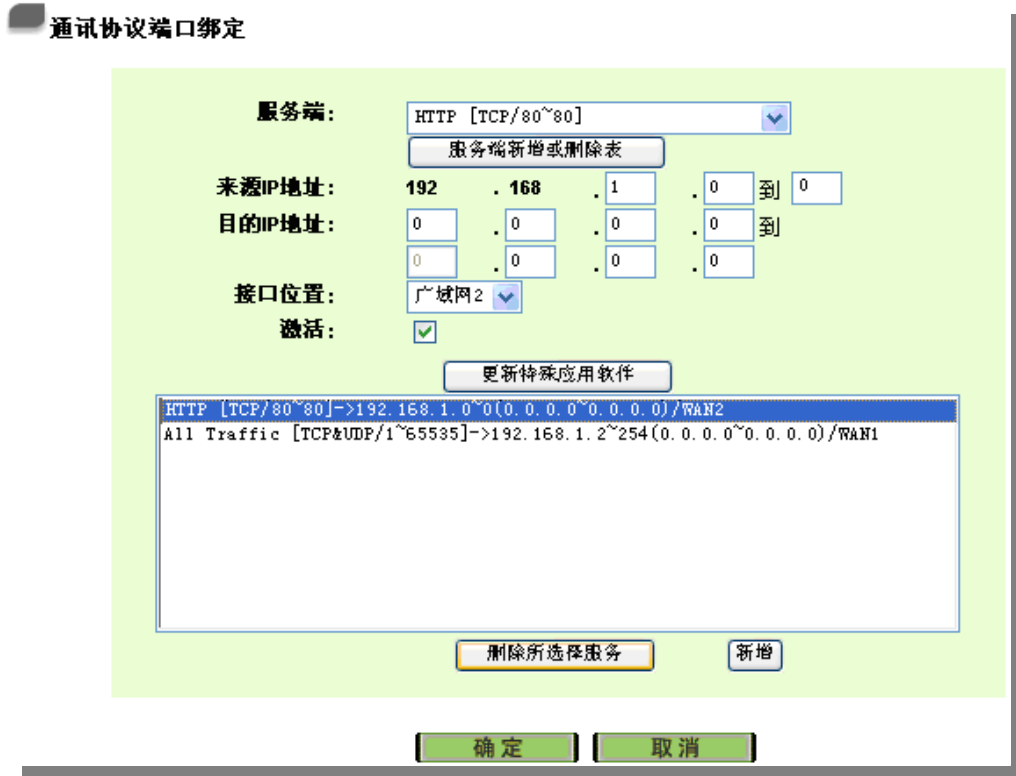
HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)/广域网2

删除所选服务 新增

确定 取消

**范例三：若要指定内网所有 IP 去外网访问 80 端都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设定方式？**

如以下范例所示，要设置两条规则，第一条规则服务端选择“HTTP[TCP/80~80]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选择广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。VPN QOS 安全路由器会将所有用 80 端去外网访问的流量都走广域网 2，但是不是用 80 端的流量根据 VPN QOS 安全路由器的自动负载均衡演算，还是有可能走广域网 2，因此还需要再设第二条规则，服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.2 到 254，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选择广域网 1，然后勾选激活。最后点击“新增”即可将此规则加入。这时 VPN QOS 安全路由器会将不是用 80 端去外网访问的流量都走广域网 1。



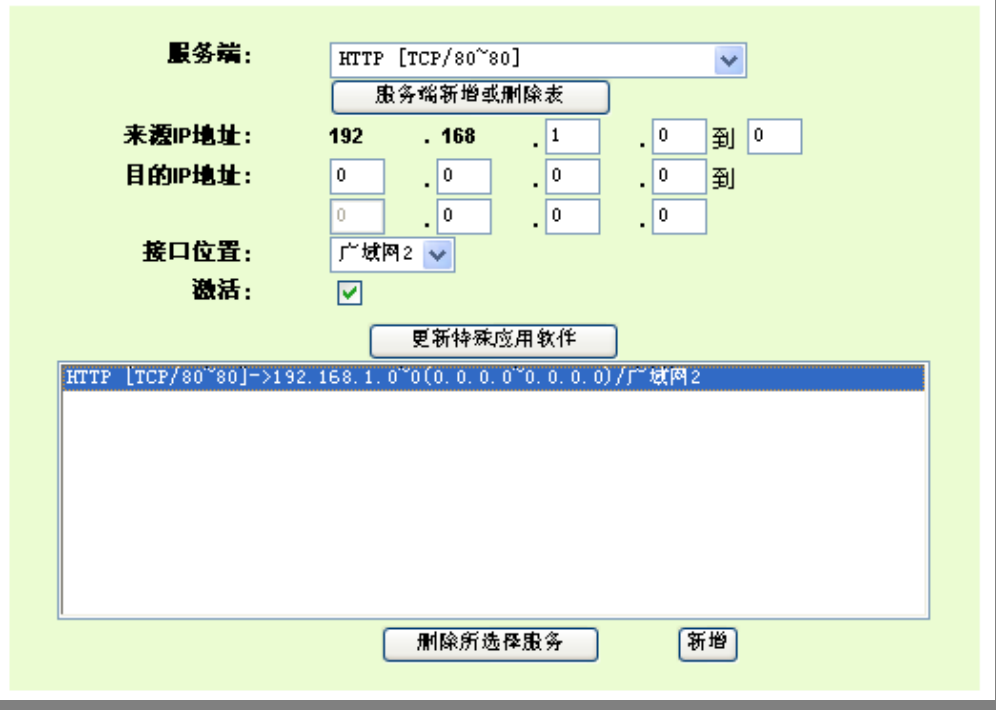
### 使用“指定路由”的负载均衡模式时其通讯协议绑定设定方式：

IP 群组-依使用者(IP Group)的模式让您对特定的内网 IP、特定要访问的应用服务端、或特定目的 IP 经由您指定的广域网端口对外网做访问。且一经指定后，该广域网端口也只能让这些指定的内网 IP、特定要访问的应用服务端、或特定目的地 IP 使用。其它不在这些指定的内网 IP、特定要访问的应用服务端、或特定目的地 IP 都会从另一条广域网出去访问。此模式必须配合“通讯协议绑定”功能才能发挥作用。

#### 范例一：若要指定内网所有 IP 去外网访问 80 端都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设定方式？

如以下范例所示设置规则，服务端选择“HTTP[TCP/80~80]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选择广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。此时广域网 2 只会有访问外网 80 端的流量，其余流量都只走广域网 1。

通讯协议端口绑定



服务端: HTTP [TCP/80~80]

来源IP地址: 192 . 168 . 1 . 0 到 0

目的IP地址: 0 . 0 . 0 . 0 到 0

接口位置: 广域网2

激活:

更新特殊应用软件

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)/广域网2

删除所选择服务 新增

范例二：若要指定内网所有 IP 去外网访问 IP 211.1.1.1 到 211.254.254.254 还有 60.1.1.1 到 60.254.254.254 整组 A 类段时都走走广域网 2 去访问，但去其余不是这几个目的地 IP 段时都走广域网 1 时，那通讯协议绑定设定方式？

如以下范例所示设置两条规则，第一条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 211.1.1.1 到 211.254.254.254。接口位置选择广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。第二条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 60.1.1.1 到 60.254.254.254。接口位置选择广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。此时，除了上述两条规则所涵盖的目的 IP，其余去外网访问的流量都只走广域网 1。

通讯协议端口绑定

**服务端:** 所有端口 [TCP&UDP/1~65535]

**来源IP地址:** 192 . 168 . 1 . 0 到 0

**目的IP地址:** 60 . 1 . 1 . 1 到 60 . 254 . 254 . 254

**接口位置:** 广域网2

**激活:**

所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)/广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)/广域网2

### 3.3.3. 网络品质服务 QoS



基本配置项目 => 网络品质服务配置

填入ISP线路实际可供使用频宽

接口位置	上传频宽 (Kbit/Sec)	下载频宽 (Kbit/Sec)
广域网1	10000	10000
广域网2	10000	10000
广域网3	10000	10000
广域网4	10000	10000

联机数管控

- 关闭
- 每一内网IP最大对外联机数限制不可超过
- 当单一个IP联机数到达 
  - 阻挡此 IP新联机  分钟
  - 封锁此IP所有联机  分钟

#### 带宽管理(QoS)

带宽管理 QoS 为 Quality of Service 缩写，其功能主要为限制某些服务及 IP 的带宽使用量，以满足特定应用程序或服务所需要的带宽或优先权，并让其余的使用者共享带宽，才能有比较稳定、可靠的数据传送服务。网络管理人员应该针对公司、小区、或是网吧的实际需求，对各种不同网络环境、应用程序或服务来进行带宽管理，才能充分且有效率的达到网络带宽使用。

#### 填入 ISP 线路实际可供使用频宽

填入ISP线路实际可供使用频宽

接口位置	上传频宽 (Kbit/Sec)	下载频宽 (Kbit/Sec)
广域网1	512	512
广域网2	512	512
广域网3	512	512
广域网4	512	512

WAN1 及 WAN2 的带宽数据请填写您所申请的宽带网络实际上传及下载带宽，QoS 的带宽控制会依照您所填入的带宽作为计算依据。例如说每个 IP 及服务端口可以保障使用的上传或下载的最小带宽会依照此 WAN1 及 WAN2 的实际带宽相加来换算实际可保障的大小。例如上传带宽若两条都为 512Kbit/Sec，那实际上传带宽就为 WAN1+WAN2=1024Kbit/Sec，所以若有 50 个 IP 在内部网络，若在保证每人最小可使用的上传带宽，则就把 1024Kbit/50=20Kbit，这样每人可以保证的最小带宽就可以填 20kbit/Sec，下载同此换算方式。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

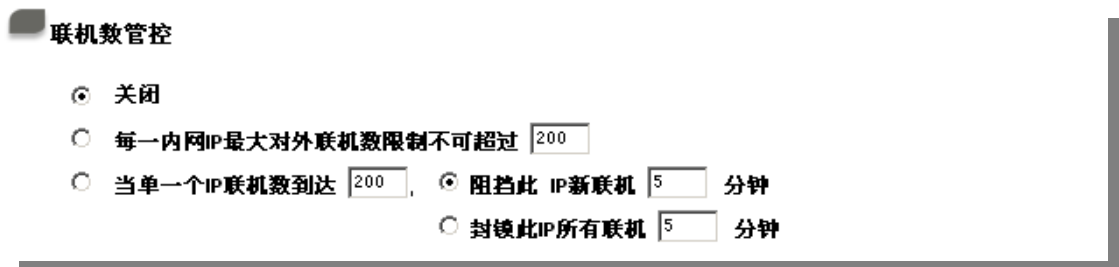
**注意！**

这里的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

### 联机数管控

联机数管控可以控制内网的计算机最多能同时建立的联机数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出联机数的软件提供了非常有效的管理。设置恰当的容许联机数可以有效控制 P2P 软件时所能产生的联机数，相对也使带宽使用量达到一定的限制。

另外，若内网有计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。



**关闭：** 不使用此联机数管控功能。

**每一内网 IP 最大对外联机数限制不可超过：** 此选项为限制每一台内网的计算机最大可建立的对外联机数，当用户计算机使用联机数到达此限制值时，要建立新的联机必须等到之前的联机结束后才能再建立。例如，当用户使用 BT 或 P2P 等下载时且联机数超过此设定值后，当用户又要再开其它服务时会无法使用，除非将使用中的 BT 或 P2P 软件关闭。

### 线路侦测机制

#### (当单一 IP 联机数达到设定值)

**阻挡此 IP 新联机**  分钟 此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户在 5 分钟之内将不能再增加新联机，就算旧联机已经结束，也必须等到设定时间过后才能再建立新的联机。

**封锁此 IP 所有联机**  分钟 此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户正在使用的所有联机都将被清除，且在 5 分钟之内将不能建立任何联机(不能上网)，必须等到设定时间过后才能再建立新的联机。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 网络品质服务配置(QoS)

VPN QoS 安全路由器让用户可以在特定的广域网络端口上，提供流量速度控制或者是服务优先权两种服务质量 QoS 的设定类型，以满足特定使用者的带宽需求。使用者在此只能够在这两种设定类型选择其中的一种作带宽服务质量 QoS。

VPN QoS 安全路由器带宽管理有两种方式可选择：一为流量控制，另一个为优先权控制。两种方式不可同时使用，网管人员可以依照内网需求做选择运用。

网管人员可依照您现有的带宽大小做每一个 IP 或一组 Range 做使用量限制或保障带宽。另外也可以针对服务端口去做带宽控制。若是内部有架设服务器的话，也可控制或保障其对外带宽。



**网络品质服务配置(QoS)**

状态:  带宽控制  优先权

接口位置:  广域网1  广域网2  广域网3  广域网4

服务端: SNMP [UDP/161~161] 服务端新增或删除表

IP地址: [0].[0].[0].[0] 到 [0].[0].[0].[0]

目的: 上传

最小带宽: [ ] Kbit/sec 最大带宽: [ ] Kbit/sec

带宽共享方式:  此范围IP地址共享此设定带宽.  
 此范围每一IP地址最大及最小可使用带宽.

激活:

上移 增加到对应列表 下移

删除所选择服务

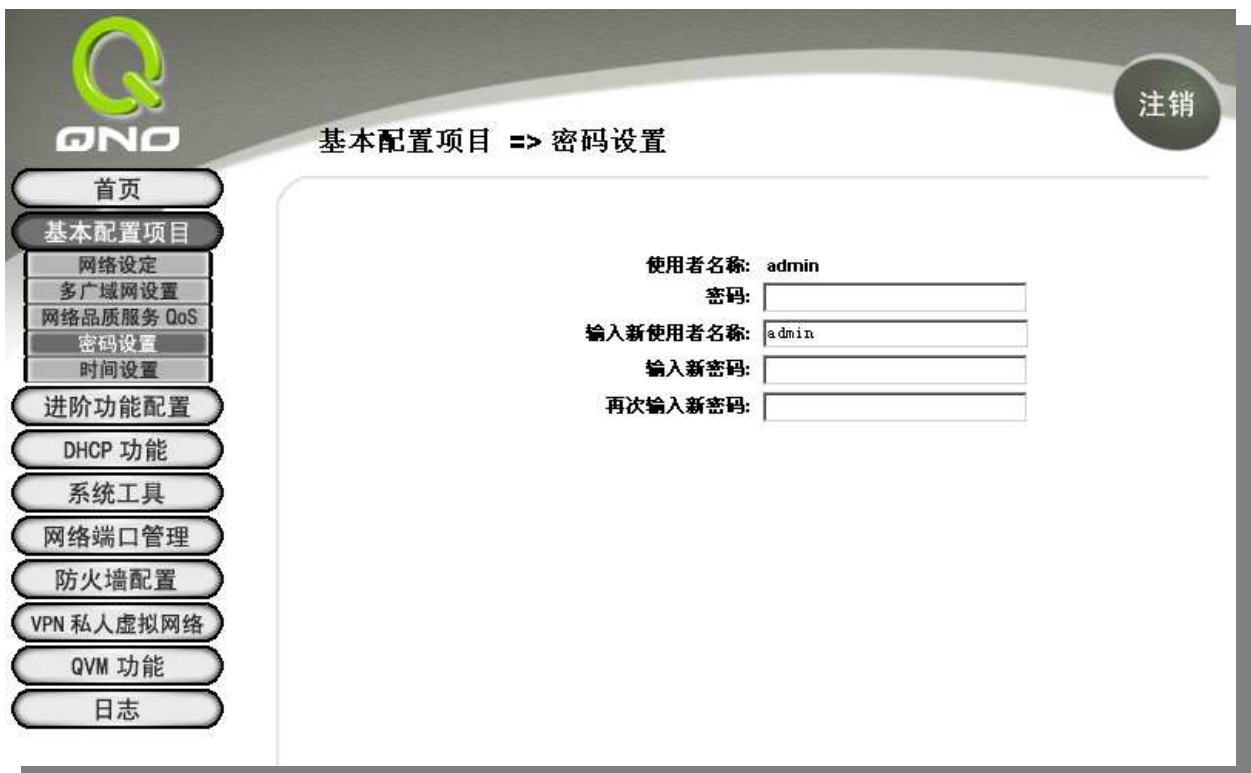
- 端口位置:** 勾选此条 QoS 设定要控制在哪条 WAN 执行，可单独或全部勾选
- 服务端:** 选择此条 QoS 所要设定的带宽控制为何，若您是要针对每个 IP 的所有服务的使用带宽，则将此选择在 All(TCP&UDP)1~65535。若您只要针对譬如 FTP 上传或下载，其余服务不限制，则选择 FTP Port21~21，可参考服务号码默认列表。
- IP 地址:** 此为选择你所要限制的使用者为何？若您只限制单一 IP，则直接将此 IP 填入，如：192.168.1.100 到 100，则此规则就是针对 192.168.1.100 此 IP 做控制。若是要限制一组 IP 范围，则填入如 192.168.1.100 ~ 150，这样此规则就是针对 192.168.1.100 到 150 做限制。若是此条带宽限制是针对所有人也就是接在 VPN QoS 安全路由器内网的所有 User 则可在 IP 的字段皆填入 0，也就是 192.168.1.0 到 0，这样就表示所有 IP 都受此规则限制。另外此 QoS 是可以控制到 Class B 的范围。
- 目的:**
- **上传:** 指对内网 IP 的上传带宽
  - **下载:** 指对内网 IP 的下载带宽
  - **虚拟服务器上传:** 若你有架设对外的 Server 网站在 VPN QoS 安全路由器内部，则此选项为控制外部访问此 Server 的带宽控制
  - **虚拟服务器下载:** 若你有架设网站在 VPN QoS 安全路由器内网，则此选项为控制外部对此服务上传数据时的带宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据更新时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。

- 最小带宽 & 最大带宽:** (Kbit/Sec)      最小带宽: 此为限制或保证此条规则的最小可使用带宽  
最大带宽: 此为限制此条规则的最大可使用带宽, 也就是最大不会超过此设定值
- 带宽共享方式:**
- 此范围 IP 地址共享此设定带宽:  
若选择此规则的话, 其表示所有 IP 或此 Service Port 共享这段 (最小到最大带宽)带宽范围。
  - 此范围每一 IP 地址最大或最小可使用带宽:  
若选择此规则的话, 其表示每一个 IP 或这一段服务端口都可以有此(最小到最大带宽)带宽范围, 例如若是针对每台计算机 (IP 地址)做的规则设定, 则每台计算机(IP 地址)都可以有这么大的带宽。
- 激活:**      启用此规则
- 增加到对应列表:**      增加此条规则到列表
- 上移 & 下移:**      由于 QoS 的每条规则执行的优先级为由列表的最下面那条往上执行, 也就是越后面设定的规则会优先执行, 所以你可以自行调整每条规则先后执行顺序。通常将要限制带宽的 Service Port 移至最下方如 BT, e-mule 等。然后将针对限制 IP 带宽的规则往上移。
- 删除所选服务:**      删除在服务列表里所选择的项目内容
- 显示开启表:**      可以显示出您所有在带宽控制 Rate Control 设定的规则, 并可直接按下“编辑”做修改

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.3.4. 管理密码设置

本功能设定多为 VPN QoS 安全路由器的进阶管理项目- 用户密码设定，本机使用密码出厂值为“admin”，您可当设定完成后修改此一存取密码，但是记得设定完成后按下“确定”。



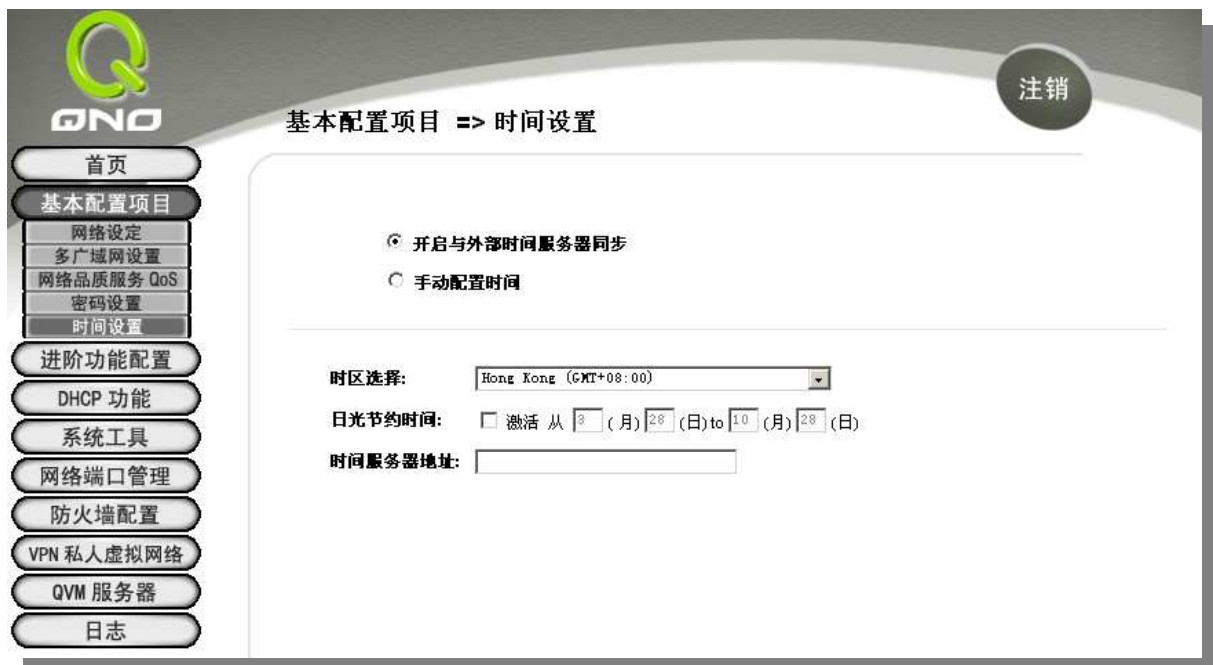
- 使用者名称:** 默认为 admin 。
- 密码:** 填写原本旧密码。
- 输入新使用者名称:** 输入使用者要建立的新用户的名称
- 输入新密码:** 填写所更改密码。
- 再次输入新密码:** 再填写确认一次更改密码。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.3.5. 系统时间设定

VPN QOS 安全路由器使用了正确的时间计算功能，您可以选择与 VPN QOS 安全路由器内建的外部时间同步服务器(NTP Server)或是自己设定正确时间参数，此项参数设置可以让您在看 VPN QOS 安全路由器的系统记录或是设置网络存取时间功能时，可以准确的知道事件所发生时间，以及关闭存取或是开放存取 Internet 资源的依据条件。

#### 设定自动与网络上的 NTP 服务器同步时间



请于**时区选择**选项选择您所在区域的时间参数以及日照时间，若是您所在的地区有实施**日光节约时间**，您可以输入实施的日期范围，VPN QOS 安全路由器会在此日期范围自动调整时间。若是您有专属使用的**时间服务器地址**的话，您可以输入此时间同步服务器的 IP 地址。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

手动输入日期时间参数:



基本配置项目 => 时间设置

开启与外部时间服务器同步

手动配置时间

18 时 5 分 20 秒

8 月 9 日 2006 年

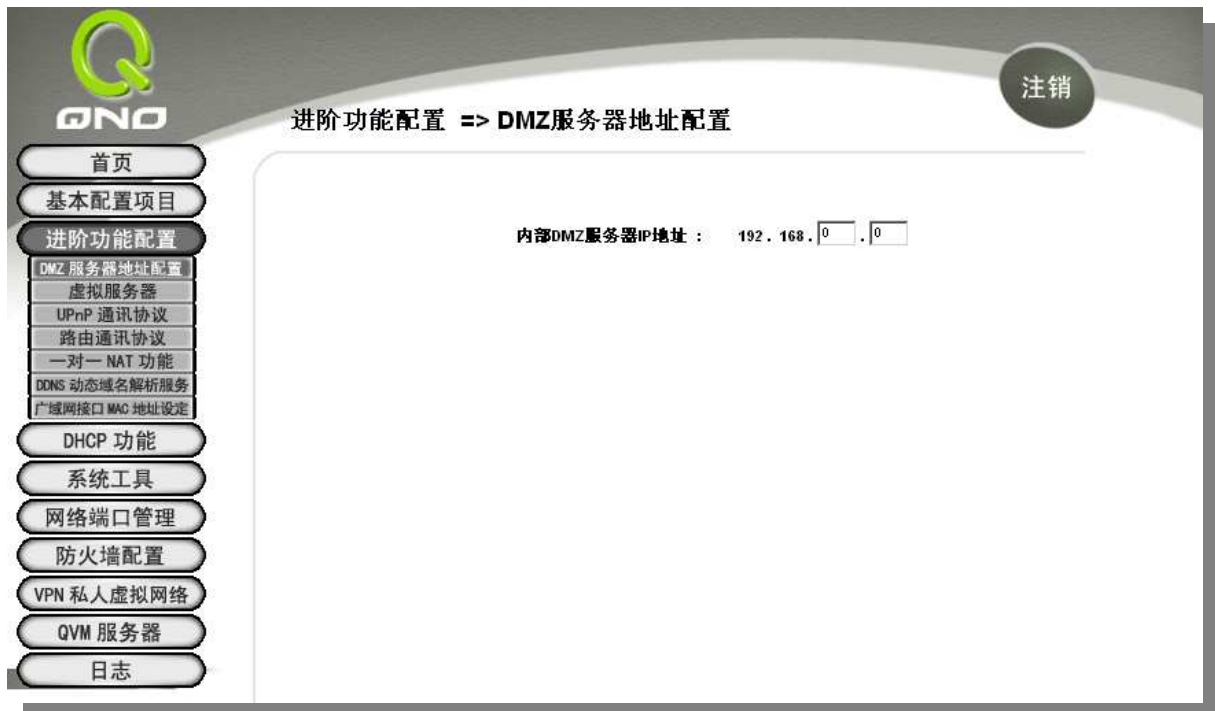
于此输入正确的时间。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## 3.4. 进阶功能配置

### 3.4.1. DMZ 服务器地址配置

当您使用 NAT 模式运作时，有时需要使用如“网络游戏”等任何不支持虚拟 IP 地址的各种应用程序时，可将 VPN QOS 安全路由器的 WAN 口的合法 IP 地址直接对应内部虚拟 IP 地址使用，设定如下填入下方的设定可用此功能达成！



于选择“DMZ 服务器”功能时，若您要取消此功能必须于后面设定虚拟 IP 地址地方填入“0”的参数，才会停止此功能使用。

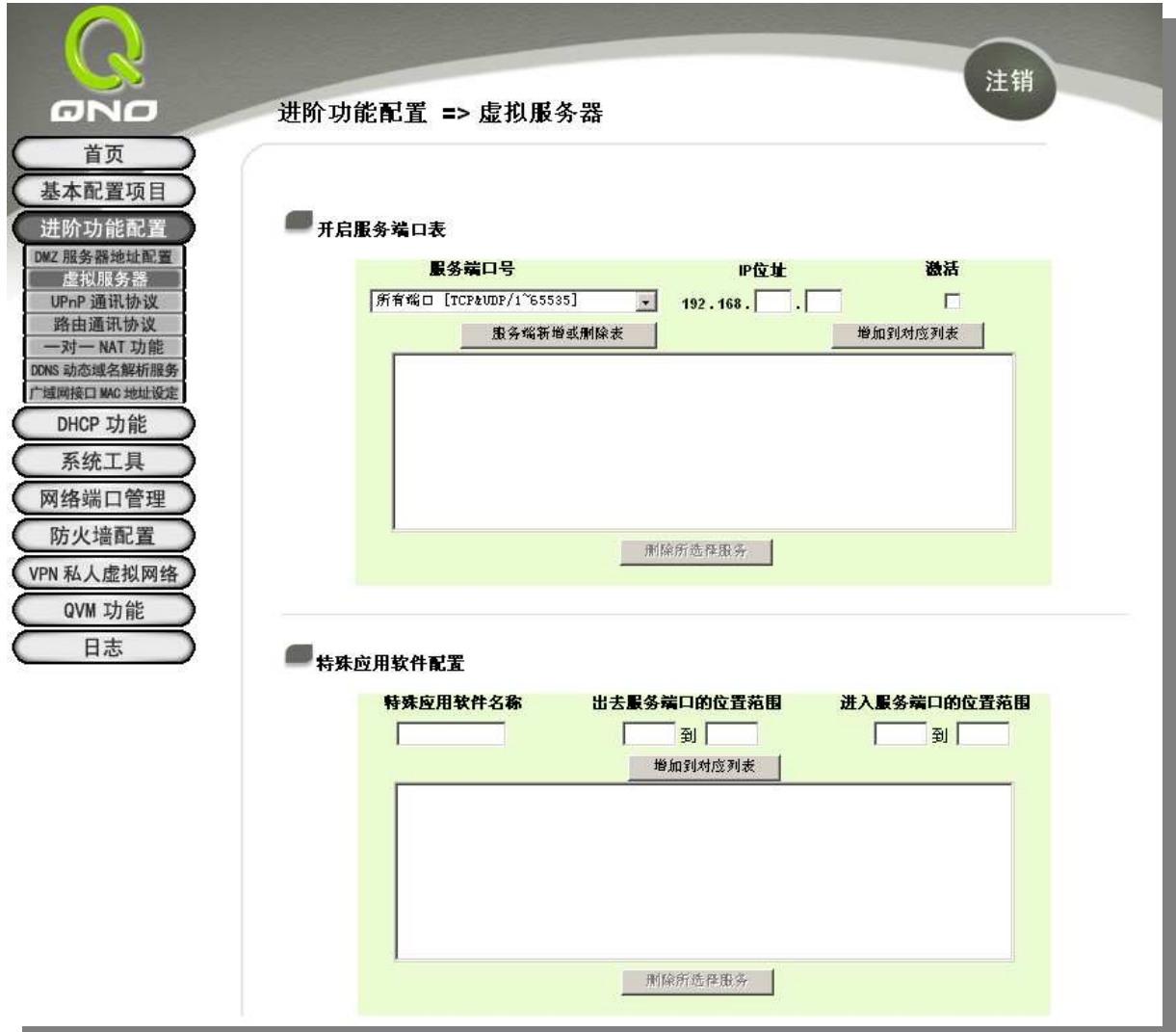
设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.4.2. 虚拟服务器

虚拟主机架设，若是网络中含有服务器功能（意指对外部的服务主机 WWW、FTP、Mail 等）可将此主机利用防火墙功能，将主机视为一虚拟的位置，可用 VPN QOS 安全路由器的外部合法 IP 地址（公网 IP 地址），经过端口的转换（如 WWW 服务端口为 80），直接存取内部服务器的服务。若于设定画面中，选项填入 WWW 服务器位置，如 192.168.1.50 且 port 是 80 的话，当 Internet 要存取这个网页时只要键入 VPN QOS 安全路由器的外部合法 IP 地址，如：<http://211.243.220.43>

此时，就会通过 VPN QOS 安全路由器的公网 IP 地址去转换到 192.168.1.50 的虚拟主机上的 Port 80 读取网页了。

其它的服务设定，如同上一般；只要将所用的服务器的 TCP 或 UDP 端口号码，以及虚拟主机的 IP 地址填入即可。



- 服务端口号:** 在此选择欲开启的虚拟主机的服务号码默认列表  
(如 All(TCP&UDP)0-65535), 如 WWW 为 80(80~80), FTP 为 21~21,  
可参考服务号码默认列表
- IP 地址:** 在此填上虚拟主机相对应的内部虚拟 IP 地址, 如 192.168.1.100
- 激活:** 开启此服务功能
- 服务端口新增或删除表:** 新增或删除管理服务端口号列表
- 增加对应列表:** 增加到开启服务项目内容

以上服务表列, 一些为较常使用的项目, 若您预开启的项目没有在表列中, 您可以使用**服务管理新增或删除端口表**功能, 如以下所述:



服务端口管理功能:



- 服务端口名称:** 在此自定选择欲开启的服务端口号名称加入列表中, 如 Edonky 等
- 通讯协议:** 选择此服务 Port 是 TCP 还是 UDP 封包
- 服务端口的位置范围:** 开启此服务功能在此填上欲开启的服务端口号的位置范围, 如 500~500 或是 2300~2310 等
- 增加到对应列表:** 增加到开启服务项目内容列表
- 删除所选服务端口列表:** 删除所选择的服务项目
- 确定:** 按下此按钮"Apply"即会储存刚才所变动的修改设定内容参数
- 取消:** 按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数, 但是必须于 Apply 储存动作之前才会有效
- 离开:** 离开此功能设定画面

## 特殊应用软件配置

**特殊应用软件配置**

特殊应用软件名称

出去服务端口的位置范围  到

进入服务端口的位置范围  到

增加到对应列表

删除所选服务

有一些特殊应用软件其进出 Internet 的端口号为非对称的，此时您必须使用此功能选项将一些特殊一用程序使用的端口号填入相关设定中，如以上画面所示：

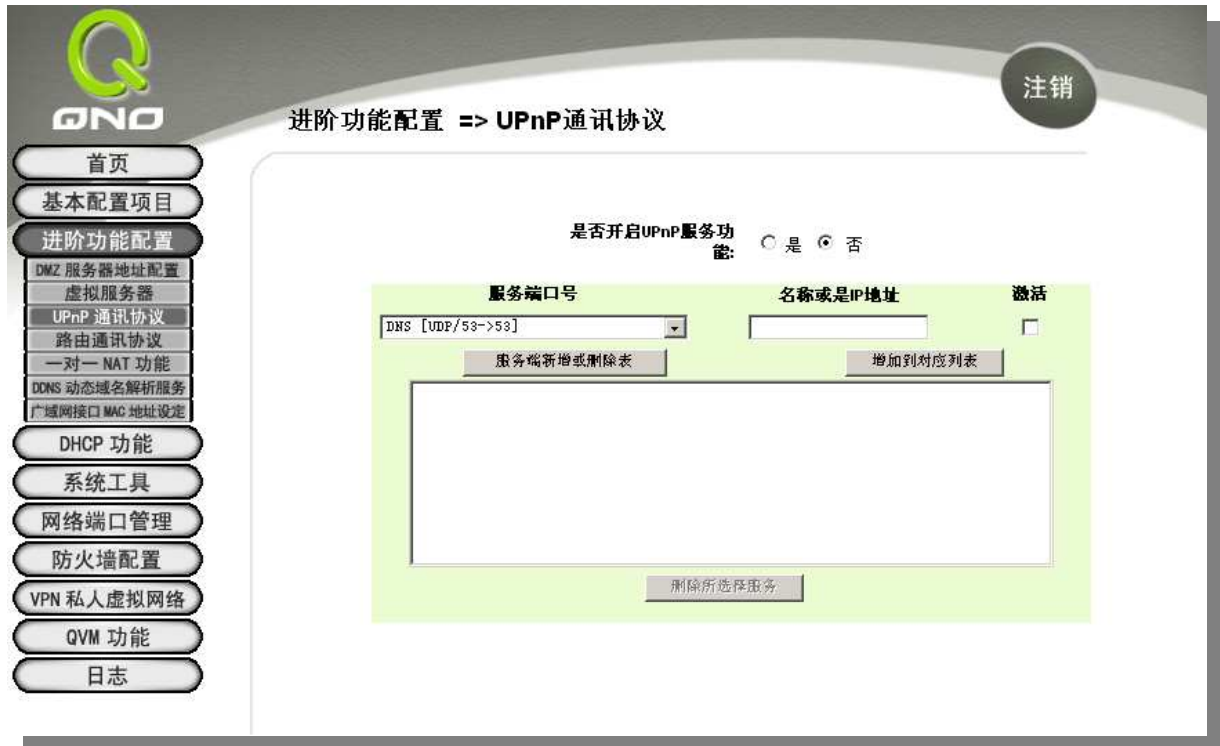
- 特殊应用软件名称：** 您可以自定此特殊应用软件名称，方便管理使用！
- 出去服务端口的位置范围：** 输入由 VPN QOS 安全路由器出 Internet 的使用端口编号。(如 9000~6600)。
- 进入服务端口的位置范围：** 输入由 Internet 进入的使用端口编号。(如 2004~2005)。
- 增加到对应列表：** 增加到开启服务项目内容列表。
- 删除所选服务目：** 删除所选择的服务项目。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

以下为一些常用的端号需设定到此功能项目中的列表：

Application	Outgoing Control	Incoming Data
Battle.net	6112	6112
DialPad	7175	51200, 51201, 51210
ICU II	2019	2000-2038, 2050-2051 2069, 2085, 3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000

### 3.4.3. UPnP 通讯协议



UPnP (Universal Plug and Play) 是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的虚拟主机计算机有支持 UpnP 机制的话(如 WindowsXP)，而您也必须相同设定您的计算机使用 UpnP 功能开启，以便与 VPN QOS 安全路由器协调搭配使用。

- 服务端口号：** 在此选择欲开启的 UPnP 的服务号码默认列表，如 WWW 为 80(80~80)，FTP 为 21~21，可参考服务号码默认列表！
- 名称或是 IP 地址：** 在此填上 UPnP 相对应的内部虚拟 IP 地址或名称，如 192.168.1.100
- 激活：** 开启此服务功能
- 服务端口增加或删除表：** 新增或删除管理服务端口列表
- 增加到对应列表：** 增加到开启服务项目内容
- 删除所选服务端口列表：** 删除所选择的服务项目
- 显示开启表：** 显示目前所开启设定的 UpnP 列表

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.4.4. 路由通讯协议

此节介绍 动态路由协议以及 静态路由的设定。



#### 动态路由通讯协议

RIP 是 Routing Information Protocol 的简称，在 IP 环境中存在 RIP I / RIP II，一般而言网络中大多只有一个 VPN QOS 安全路由器，所以绝大部分我们会只使用静态路由通讯，RIP 的使用时机是网络中有数个 VPN QOS 安全路由器时，此时不想每台 VPN QOS 安全路由器都去定义路径表，可自动选择 RIP 通讯协议，且自动将所有路径更新！

RIP 也是一个很非常简单的路由协议，是采用 Distance Vector 的方式，所谓 Distance Vector 是用以路由的个数来作为传送距离的判断，而不以实际联机的速率来作判断，所以在某些时候所选的路径是经过最少的路由，但是并不一定反应速度最快的路由。

### 动态路由通讯协议

选择路由器运作模式:  NAT模式  路由模式

动态路由通讯协议RIP功能:  激活  关闭

接收动态路由通讯协定功能:

传送动态路由通讯协定功能:

**选择 VPN QOS 安全路由器 运作模式:** 选择 VPN QOS 安全路由器运作模式为 NAT 模式或是路由模式。

**动态路由通讯协议 RIP 功能:** 选择按钮“激活”选择使用 RIP 动态路由通讯。

**接收动态路由通讯协议功能:** 可用上下选择按钮选择使用动态路由通讯 **None, RIPv1, RIPv2, Both RIPv1 and v2** 为传送动态路由通讯协议的“TX”功能。

**传送动态路由通讯协议功能:** 可用上下选择按钮选择使用动态路由通讯 **None, RIPv1, RIPv2-Broadcast, RIPv2-Multicast,** 为接收动态路由通讯协议的“RX”功能。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 静态路由通讯协议

如果在您的网络中有多个 VPN QOS 安全路由器与 IP 节点子网络，就必需设定 VPN QOS 安全路由器的静态路由功能，这些功能是让整个不同的网络节点能自动找寻所需路径，且能让不同网络节点能相户存取;使用图中的功能按钮“显示开启路由表”能知道最新的路径表。

**指定路由通讯协议**



- 目的地址和子网掩码:** 可填入欲绕径的远程网络 IP 节点与子网络节点位置，如另一个子网络节点为 192.168.2.0/255.255.255.0
- 默认网关:** 此网络节点欲绕径的默认网关位置。如 192.168.2.1
- 路由节点:** 此节点的 VPN QOS 安全路由器层数，如是在 VPN QOS 安全路由器下的二个 VPN QOS 安全路由器之一，此应填为 2，默认为 1 (最大为 15)
- 接口位置** 此网络节点的连接位置，是位于 WAN 端亦或是 LAN 端
- 增加/删除对应列表:** 增加/删除一个路由
- 显示开启路由表:** 显示目前最新的路径表

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 3.4.5. 一对一 NAT 对应

当您的 ISP 提供给您多个合法固定 IP (如 ADSL 固定 8 个或更多 IP 地址)时, 因 VPN QOS 安全路由器本身只有使用一个合法 IP 地址, 以及 ATU-R 也使用一个合法 IP 地址, 所以剩余的合法 IP 可将其直接对应到 VPN QOS 安全路由器内部的虚拟 IP 计算机!

#### 使用方法:

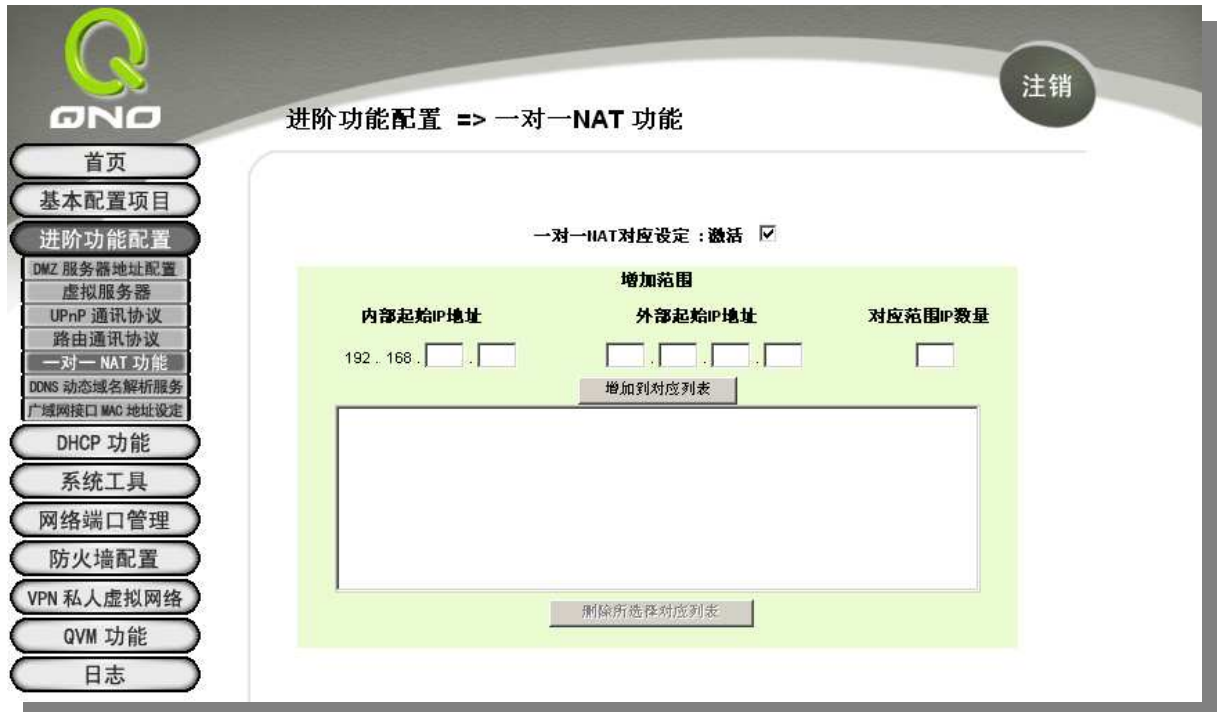
当您有使用如“网络游戏”等任何不支持虚拟 IP 地址的各种应用程序时, 可将外部的合法 IP 地址直接对应内部虚拟 IP 地址使用, 设定如下填入上方的设定中即可!

#### 范例:

如您有 5 个可用 IP 地址, 分别是 210.11.1.1~6, 而 210.11.1.1 已经给 VPN QOS 安全路由器的 WAN 合法 IP 使用于一般的 NAT 上, 另外还有其它四个合法 IP 可以分别设定到 Multi-DMZ 当中, 如下所述

210.11.1.4 → 192.168.1.3  
210.11.1.5 → 192.168.1.4  
210.11.1.6 → 192.168.1.5  
210.11.1.7 → 192.168.1.6

<b>注意!</b>
VPN QOS 安全路由器 WAN IP 地址不能被涵盖在一对一 NAT 的 IP 范围设定中。



- 一对一 NAT 功能:** 激活或关闭一对一 NAT 功能 (选择是否开启此功能)
- 内部起始 IP 地址:** 输入内网虚拟做一对一 NAT 的 IP 地址起始 IP 地址
- 外部起始 IP 地址:** 输入外网虚拟做一对一 NAT 的 IP 地址起始 IP 地址
- 对应范围 IP 数量:** 外部合法 IP 地址终止 IP 的数量(请勿含盖 WAN 在使用的 IP)
- 增加到对应列表:** 加入此设定到一对一 NAT 列表中
- 删除所选对应列表:** 删除所选择的一项一对一 NAT 列表

**注意!**

一对一的 NAT 模式将会改变防火墙运作的方式, 您若设定了此功能, LAN 端所对应公有网 IP 的服务器或计算机将会曝露到 Internet 上。若要阻绝 Internet 的使用者主动联机到一对一 NAT 的服务器或计算机, 请到 4.3.防火墙中设定适当的拒绝存取规则条件。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.4.6. 动态域名解析服务 (DDNS)

DDNS 支持 3322.org、DynDNS.org 以及 DtDNS.com 的动态网址转换功能, 其目的是为了使用户动态 IP 地址架设或是远程监控还有动态 IP 下需做 VPN 的联机为目的, 如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的合法 IP 地址都会随时间而改变, 当此使用者欲架设网站之类的服务, 但是因



IP 会随时变动，所以本设备提供了动态网址转换功能，此服务可向 [www.qno.cn/ddns](http://www.qno.cn/ddns)、[www.3322.org](http://www.3322.org)、[www.dyndns.org](http://www.dyndns.org) 或 [www.dtdns.com](http://www.dtdns.com) 提出申请，是完全免费的！



接口位置	状态	服务器名称	配置
广域网1	Dydns 关闭 3322 关闭 Dtdns 关闭 Gnodns 关闭	Dydns: --- 3322: --- Dtdns: --- Gnodns: ---	<a href="#">编辑</a>
广域网2	Dydns 关闭 3322 关闭 Dtdns 关闭 Gnodns 关闭	Dydns: --- 3322: --- Dtdns: --- Gnodns: ---	<a href="#">编辑</a>
广域网3	Dydns 关闭 3322 关闭 Dtdns 关闭 Gnodns 关闭	Dydns: --- 3322: --- Dtdns: --- Gnodns: ---	<a href="#">编辑</a>
广域网4	Dydns 关闭 3322 关闭 Dtdns 关闭 Gnodns 关闭	Dydns: --- 3322: --- Dtdns: --- Gnodns: ---	<a href="#">编辑</a>

请在设定栏的编辑按下该超级链接直接进入该设定项目中。



进阶功能配置 => DDNS动态域名解析服务

接口位置 : WAN1

DynDNS.org

使用者名称:

密码:

服务器名称:  .  .

内部IP地址:

状态: 没有更新

3322.org

使用者名称:

密码:

服务器名称:  .  .

内部IP地址:

状态: 没有更新

DtDNS.com

使用者名称:

密码:

服务器名称:  .  .

内部IP地址:

状态: 没有更新

返回上一页 确定 取消

接口位置:

显示使用者所选取的广域端口

- DynDNS.org
- 3322.org
- DtDNS.com

可以选择开启或关闭 DynDNS.org、3322.org 与 DtDNS.com 等三项 DDNS 动态网址转换服务功能，根据你的需要在其前面做“√”选。

使用者名称:

向 DDNS 所设定的名称

密码:

向 DDNS 所设定的密码

服务器名称

向 DDNS 所注册的网址，如：abc.dyndns.org 或 xyz.3322.org

内部 IP 地址

向 ISP 所取得的之动态合法 IP 地址

状态:

显示目前的 DDNS 所更新 IP 功能状态

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.4.7. 广域网接口 MAC 地址设定

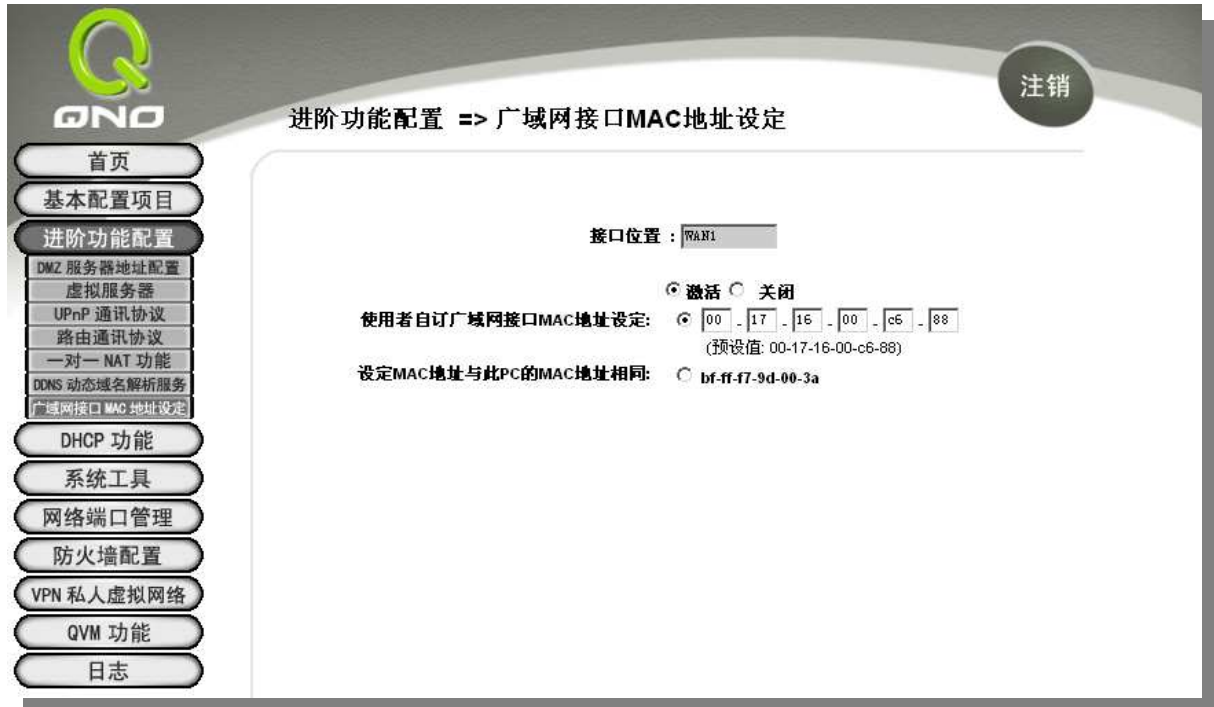
此多为使用于双向 Cable Modem 的用户，若有发生类似锁网卡的情况下，可使用此功能将原有网卡硬件地址(MAC Address:00-xx-xx-xx-xx-xx)填入此项目中以解除锁定问题！



进阶功能配置 => 广域网接口MAC地址设定

接口位置	MAC地址	配置
广域网1	00-17-16-00-c6-88	<a href="#">编辑</a>
广域网2	00-17-16-00-c6-89	<a href="#">编辑</a>
广域网3	00-17-16-00-c6-8a	<a href="#">编辑</a>
广域网4	00-17-16-00-c6-8b	<a href="#">编辑</a>

请在设定栏选择广域网端口点编辑，按下该超级链接直接进入该设定项目中。



- 接口位置: 使用者所选取的广域端口
- 激活  关闭 选择激活或关闭这项功能
- 使用者自订广域网接口 MAC 地址设定: 目前设备出厂默认的 MAC 位置
- 设定 MAC 地址与此 PC 的 MAC 地址相同: 目前连接此 PC 的 MAC 位置

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 3.5. DHCP 发放 IP 服务器

#### 3.5.1. DHCP 设定

因 VPN QOS 安全路由器本身就含有 DHCP 服务器，所以可以提供局域网络内的计算机自动取得 IP 的功能，（如同 NT 服务器中的 DHCP 服务，好处是每台 PC 不用去记录与设定其 IP 地址，当计算机开机后，就可从 VPN QOS 安全路由器自动取得，管理方便。

**激活 DHCP 服务功能:** 可选择开启 DHCP 服务器自动派发 IP 地址功能；若为激活选项，则所有 PC 都可使用自动取得 IP 地址，反之则无；每台 PC 必需去指定固定虚拟 IP 地址。



### 动态 IP

**租约时间:** 此设定为发给 PC 端 IP 地址的租约时间，默认为 1440 分钟(代表时间为一天)，您可以依照实际需求来设定，以分钟为单位。

**起始 IP 地址:** 此 IP 地址是 DHCP 服务自动派送 IP 的启使 IP，意指是从多少 IP 地址开始派送。系统默认从 192.168.1.100 的 IP 地址开始发放。

**终止 IP 地址:** 指是从多少 IP 地址停止派送。系统默认为从 149 的 IP 地址开始停止发放 IP，原厂设定值可供 50 台计算机自动取得 IP 地址，您可以是实际情况增减使用！

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

## 地址绑定功能

**IP 与 MAC 绑定**

显示新加入的IP地址

静态IP地址设定:  .  .  .

添入IP地址相对应MAC地址:  -  -  -  -  -

名称:

激活:

增加到对应列表

删除所选择对应项目

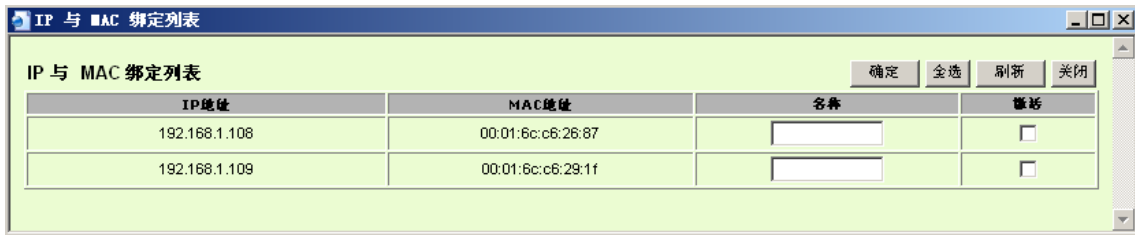
封锁在对应列表中IP地址错误的MAC地址

封锁不在对应列表中的MAC地址

- 静态 IP 地址设定:** 此字段有两种填入方式:
1. 若您只要限制 MAC Address 可以跟 DHCP 要 IP 而不一定是指定的那一个 IP, 请在此字段填 0.0.0.0, 不可为空白
  2. 若要求每次此台计算机都要分配到同一个 IP, 则将你所要求分配给此台计算机的 IP 地址输入。这样所要绑定服务器或 PC 端每次重启都会要到固定的同一个虚拟 IP
- 添入 IP 地址相应 MAC 地址:** 输入要绑定的服务器或 PC 端固定实体 MAC(网络卡上的地址)
- 名称:** 填入您所绑定此用户的名字或地址做辨识, 可输入 12 个字符, 中英文皆可以
- 激活:** 启用此组设定
- 增加到对应列表:** 加入或修正此设定到列表中
- 删除所选择对应项目:** 删除列表中所选择的绑定
- 新增:** 增加新的绑定
- 封锁在对应列表中 IP 地址错误的 MAC 地址:** 此选项打勾后, 只要不在列表中的 MAC Address 都无法上网
- 封锁不在对应列表中** 此选项打勾后, 只要是 User 自行更改计算机的 IP 或不是列表设定的

的 MAC 地址: IP 将无法上网

显示新加入的 IP 地址: 选者需要绑定的 IP/MAC, 命名好客户需要设定名称, 并做激活。



设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## DNS 服务器

### DNS域名解析

DNS域名解析地址1:  .  .  .

DNS域名解析地址2:  .  .  .

此设定为发给 PC 端 IP 地址的 DNS 域名服务器查询位置, 您可以直接输入此服务器的 IP 地址。

**DNS 域名解析地址 1:** 输入 DNS 网域服务器的 IP 地址, 默认值为 0

**DNS 域名解析地址 2:** 输入 DNS 网域服务器的 IP 地址, 默认值为 0

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## WINS 服务器

### WINS服务器

WINS服务器地址:  .  .  .

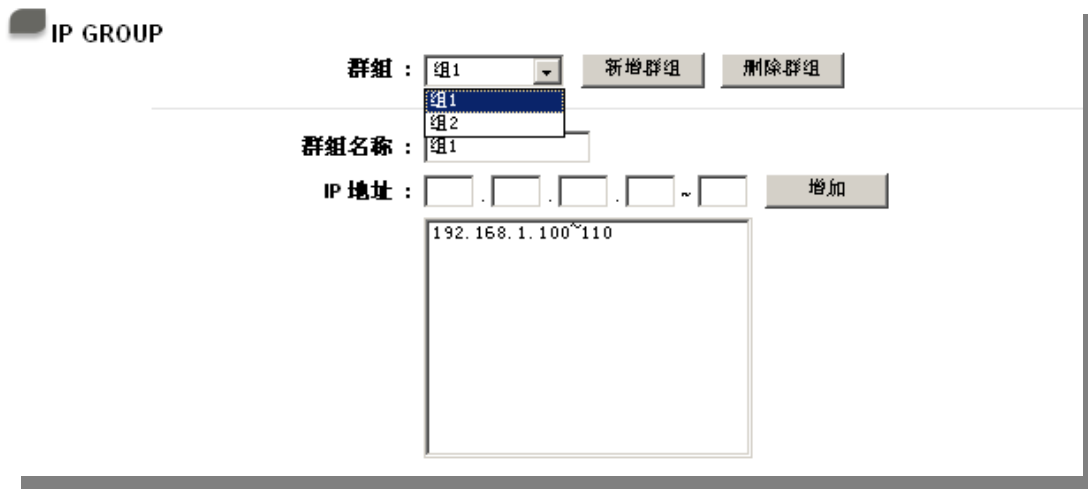
若您的网络上有解析如 Windows 的计算机名称服务器的话, 您可以直接输入此服务器的 IP 地址。

**WIN 服务器地址:** 输入 WIN 网域服务器的 IP 地址, 默认值为 0

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### IP 群组管理 (IP GROUP)

此方式的设定方便用户对网络内连续的 IP 做同样的操作。比如一个公司的同一部门分得了一段连续的 IP (192.168.1.100~192.168.1.110)，VPN QoS 安全路由器对这个部门做访问存取规则的设定，就把这个连续的 IP 地址绑在一起做相同的设定，相对于对每个 IP 进行设定节约了时间和操作过程中容易输入错误，方便用户设定省时省力。



IP GROUP

群组：组1 新增群组 删除群组

群组名称：组1

IP 地址：. . . ~ . 增加

192.168.1.100~110

- 群组：** 选择群组，对其做修改删除的操作
- 群组名称：** 输入群组的名称，如“市场部门、营销部门等”
- IP 地址：** 输入分配的 IP 地址范围
- 增加：** 增加新的条目

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。



### 3.5.2 DHCP 服务器状态



**DHCP功能 => DHCP服务器状态**

**状态**

DHCP服务器IP地址 : 192.168.1.1  
 已经使用的IP数量 : 1  
 发放固定IP数量 : 0  
 尚可使用的IP地址 : 49  
 配发DHCP IP地址总量 : 50

**DHCP服务器发放IP对应表**

主机名称	IP地址	MAC地址	目前租约时间	删除
PC-6	192.168.1.100	00:11:2f:57:52:32	Wed Aug 9 18:39:17 2006	

此状态表为显示 DHCP 服务器的目前使用状态与设定记录等，以便提供管理人员需要时做网络设定参考数据。以下针对其内容做介绍：

- DHCP 服务器 IP 地址：** 目前 DHCP 服务器的 IP 地址
- 已经使用 IP 数量：** 目前 DHCP 服务器已经发放动态 IP 的数量
- 发放固定 IP 数量：** 目前 DHCP 服务器已经发放固定 IP 的数量
- 尚可使用的 IP 地址：** 目前 DHCP 服务器可以发放的 IP 数量
- 配发 DHCP IP 地址总量：** 目前 DHCP 服务器所设定可发放的 IP 总数量
- 主机名称：** 目前此台计算机的计算机名称
- IP 地址：** 目前此台计算机所取得的 IP 地址
- MAC 地址：** 目前此台计算机的 MAC 网络实体位置
- 目前租约时间：** DHCP 目前核发 IP 地址的租约时间
- 删除：** 删除此笔核发 IP 记录

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## 4. 系统工具、端口以及安全的设定

本章节介绍 VPN QOS 安全路由器的一些工具的操作方法、端口的管理和网络安全的相关配置。通过设置方便用户对 VPN QOS 安全路由器及 VPN QOS 安全路由器端口的管理，来提高 VPN QOS 安全路由器的安全防护功能。

### 4.1. 工具程序

#### 4.1.1. SNMP 网络通讯管理协议

SNMP 为 Simple Network Management Protocol 的缩写，意指网络管理通讯协议，此为网络上重要的管理项目依据之一，透过此 SNMP 通讯协议，可以让已经具备有网络管理的程序(如 SNMP Tools-HP Open View)等做实时管理之通讯使用，VPN QOS 安全路由器支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前所有网络上的机器运作情况，以便随时掌握网络信息。



系统工具 => SNMP网络通讯协议

SNMP网络通讯协议 : 激活

系统名称: 4\_WAN\_QVM\_Router

联系方式:

系统地址:

Get Community Name: public

Set Community Name: private

Trap Community Name: public

Send SHIMP Trap to:

激活: 将 SNMP 功能开启，系统默认为开启此功能

<b>系统名称:</b>	设定机器的名称
<b>联系方式:</b>	设定机器的管理联系人员名称, 如 John
<b>系统地址:</b>	设定机器的目前所在位置, 如 Taipei
<b>Get Community Name:</b>	设定一组用户参数可以取得此机器的项目信息, 系统默认"公网"
<b>Set Community Name:</b>	设定一组用户参数可以设定此机器的项目信息, 系统默认"Private"
<b>Trap Community Name:</b>	设定一组用户参数可以传送 Trap 的信息
<b>Send SNMP Trap to:</b>	设定一组 IP 地址或是 Domain Name 名称的接收 Trap 讯号主机

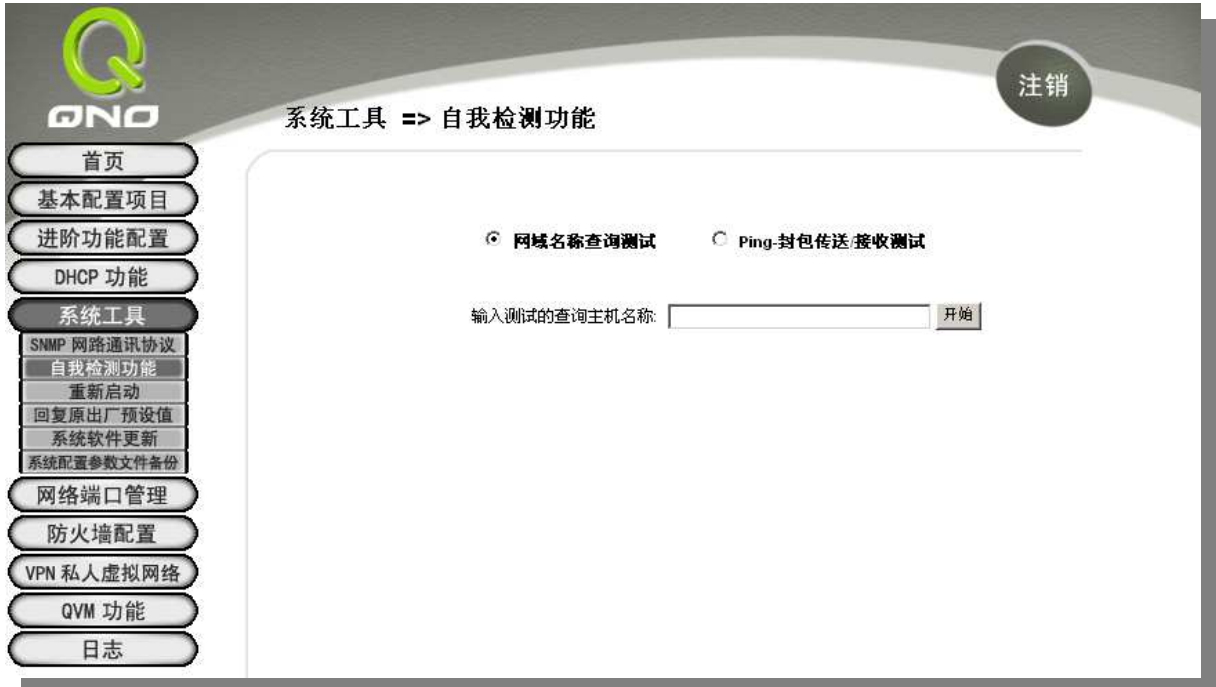
设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

#### 4.1.2. 自我检测功能

VPN QoS 安全路由器 提供简易的线上测试机制方便于除错时使用, 此除错机制包含**网域名称查询测试 DNS Lookup** 以及 **Ping 封包传送/接收测试** 二种。

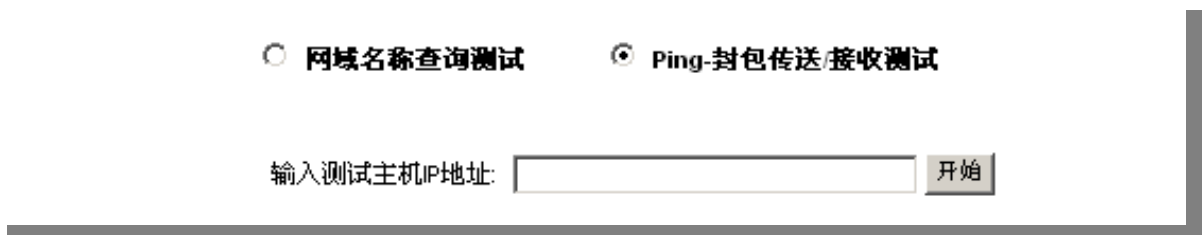
##### 网域名称查询测试

请于此测试画面输入您想查询的网域主机位置名称, 如www.abc.com 然后按下开始的按钮开始测试, 测试结果会显示于此画面上。



### Ping-封包传送/接收测试

此项目为主要提供用户了解对外联机的实际状况，可以利用此功能了解网络上的计算机是否存在！请于此测试画面输入您想测试的主机位置 IP，如 192.168.5.20 按下开始的按钮开始测试，测试结果会显示于此画面上。



### 4.1.3. 重新启动



通过此“立即重新激活”按钮重新启动 VPN QOS 安全路由器，重新启动后也会将此讯息传送到系统日志中。通过 VPN QOS 安全路由器面板上的“Reset”开关通过硬操作也可以重新启动，当按下 Reset 按钮 5 秒后当黄灯慢闪 5 次机器开始重新启动。

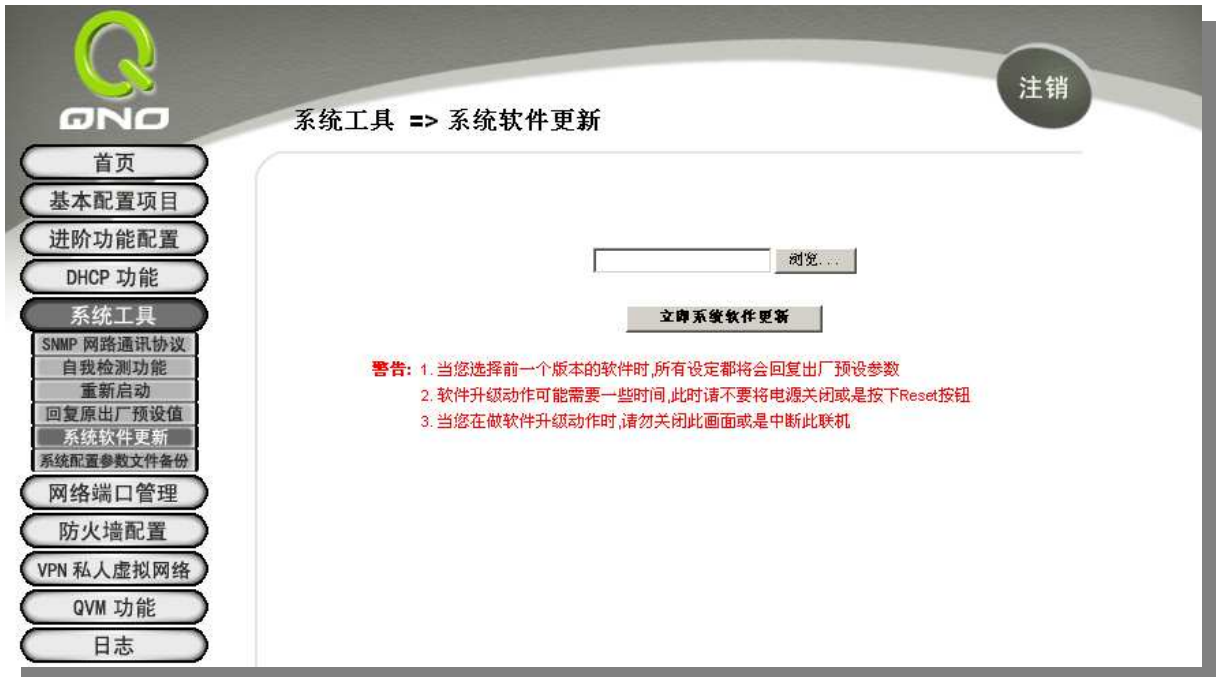
#### 4.1.4. 恢复原出厂默认值



若是选择“立即恢复原出厂值设定”，VPN QOS 安全路由器会将所有的设定清除，并重新开机，你还可以通过 VPN QOS 安全路由器面板上的“Reset”按钮通过硬操作恢复出厂值，当按下 Reset 按钮 10 秒以上后当黄灯慢闪后又出现快闪机器开始恢复出厂值。

**切记，使用此功能会将机器所有的资料清除！**

#### 4.1.5. 系统软件升级



此设定可以于 VPN QOS 安全路由器的 Web 设定画面中直接升级软件，并请您于升级前先确认软件版本信息，选择浏览至软件存放资料夹，选定该档案后，按下”立即系统软件更新”做升级。

**切记：当升级动作开始进行中时，请勿跳离此画面，否则升级会失败。**

#### 4.1.6. 系统配置参数文件备份



##### 配置文件设定档汇入:

此功能为将之前用户的所有设定参数值备份的内容导入机器中！ 并请您于升级前先确认软件版本信息，选择浏览至备份参数档案-"config.exp"存放资料夹选择该档案后，按下“汇入”按钮做设定档案导入。

##### 系统配置参数文件存储:

此功能为储存用户的所有设定参数值备份， 按下“存储”按钮，选择存放数据夹位置然后按下储存键将"config.exp"存入即可。



## 4.2. 网络硬件端口管理

于 VPN QOS 安全路由器 中，用户可以设定广域网端口数与每一个以太网端口连接速率，工作模式，高低优先权或是自动侦测等以太网端口的功能。

### 4.2.1. 端口配置



网络端口管理 => 端口配置

选择广域网个数：4 (预设值:4)

激活端口1为端口镜像

端口号	接口位置	关闭端口	优先权	网络端口连接速率	半双/全双工模式	自动侦测模式	VLAN
1	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
2	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
3	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
4	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
5	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
6	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
7	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
8	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
9	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
10	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
11	局域网	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	VLAN1
12	广域网4	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	
13	广域网3	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	
14	广域网2	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	
15	广域网1	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	
DMZ	DMZ	<input type="checkbox"/>	一般	10M 100M	半双 全双	激活	

#### 以太网端口设定

端口号: 显示每个端口的顺序

接口位置: 共有 LAN1~LAN 11、WAN1~WAN4 及 DMZ 等端口，这些端口会根据使用者所设定的广域网端口数而自动调整

- 关闭端口:** 此为设定以太网络的端口开启或是关闭的功能，若是打勾的话，则此以太网端口立即被关闭无法连接使用，默认为开启
- 优先权:** 此为设定此以太网络的端口封包传送高低优先权设定，若是此端口设定为高(High)的话，则最优先使用传送封包的权利，默认值为一般(Normal)
- 网络端口连接速率:** 此为设定此以太网络的端口网络硬件连接速率选项，您可以设定为 10Mbps 或是 100Mbps 连接速度
- 全双工/半双工:** 此为设定此以太网络的端口网络硬件连接速率工作模式选项，您可以设定为半双工或全双工模式运作
- 自动侦测模式:** 此为设定此以太网络的端口网络硬件连接速率自动侦测模式，若是勾选的话，自动侦测所有连接端口的信号与调整
- VLAN:** 此功能可以让网管人员在自己的局域网内将局域网端设定为 1 个或多个无法互通的不同网段，但都可以通过 VPN QOS 安全路由器上 Internet。  
在同一个网段内的成员(在同一个 VLAN 局域网内)可互相沟通并看得到对方，若不在同一个 VLAN 群组内的成员则无法得知其它成员的存在。  
使用者可为每一个 LAN 端选定为哪一个 VLAN 局域网群组，最多可设定为 13 个局域网群组。
- VLAN All:** 设置为 VLAN All 的端口即为 VLAN 的公共区域，可与其它所有的 VLAN 网络互通。当内网需要架设服务器让内网所有 VLAN 群组都可以访问此服务器，此时可以将某一局域网端设定为 VLAN All，将此服务器接入此 VLAN All 的端，这样就可以让所有不同 VLAN 群组的计算机都可以访问到此服务器。另外，网管所在端口也必须设置为 VLAN All，才可与整体网络联机，进行网络管理。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

## 4.2.2. 网络端口状态即时显示

用户可以于此项目中，选择所需要查看的以太网网络端口各项实时参数显示，如下图：



The screenshot shows the QNO web interface for network port management. The left sidebar contains navigation buttons: 首页, 基本配置项目, 进阶功能配置, DHCP 功能, 系统工具, 网络端口管理 (selected), 端口配置, 端口状态即时显示 (selected), 防火墙配置, VPN 私人虚拟网络, QVM 功能, and 日志. The main content area is titled "网络端口管理 => 端口状态即时显示" and includes a "注销" button. A dropdown menu shows "选择端口号 : 10".

**整体资讯项目**

网路连接状态	10Base-T / 100Base-TX
接口位置	局域网
线路连线状态	关闭
端口配置状态	端口激活
优先级设定	一般
网路连接速率	10 Mbps
半双/全双工模式	半双工
自动侦测模式	激活
VLAN	VLAN1

**端口流量即时显示**

接收封包计算	5401
封包接收 Byte数	679345
传送封包计算	6088
封包传送 Byte数	2117075
错误封包统计	0

于网络端口状态整体信息表格项目中，此部份会显示目前端口硬件设定项目，如：网络连接状态，接口位置，线路连线状态(激活/关闭)，端口配置状态(端口激活/关闭)，端口优先级设定 (高或一般)，网络连接速率(10Mbps 或 100Mbps)，双工模式(半双工或全双工)，自动侦测模式(激活/关闭)，VLAN 等。

网络端口流量实时显示信息表格项目中，将会显示目前此端口的封包数据，包含传送/接收封包计算/以及封包传送/接收 Byte 数计算与 错误封包统计等。您可以按下刷新按钮重新整理所有的实时信息显示。

## 4.3. 防火墙配置

### 4.3.1. 基本设定

VPN QOS 安全路由器默认防火墙功能为激活状态。如果用户关闭此防火墙选项功能的话，SPI，DoS，关闭对外封包响应等功能将会自动关闭，同时远程管理功能将会激活，而网络存取规则与内容服务过滤器也会关闭。



**防火墙功能:**

此为选择开启或关闭防火墙功能。

**SPI 封包主动侦测检验功能:**

此为封包主动侦测检验技术，防火墙主要运作在网络的层级，但是藉由执行对每个连接的动态检验，也拥有应用程序的警示功能。同时，封包检验型防火墙可以拒绝非标准的通讯协议所使用的连接。

**DoS 侦测功能:**

此为防止 DoS 攻击，如 SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing 等。

**关闭对外封包回应:** 若是选择**激活**的话, 则 VPN QOS 安全路由器 会关闭对外的 ICMP 与不正常联机的封包响应, 所以若是你从外部去 ping 这台 VPN QOS 安全路由器的 WAN IP 是无法 ping 通的, 默认值为开启拒绝对外响应的功能。

**远程配置管理功能:** 远程管理功能, 若您要透过远程 Internet 直接联机进入 VPN QOS 安全路由器的设定画面, 必需将此功能开启, 并于远程于浏览器网址填入 VPN QOS 安全路由器的外部合法 IP 地址(WAN IP), 并加上默认可修改的控制端口(默认为 80, 可更改)。

**允许 Multicast 封包穿透模式:** 网络上有许多影音串流媒体, 使用广播方式可以让客户端接收此类封包讯息格式。默认值为关闭这个功能。

**防止 ARP 病毒攻击:** 此功能为防止内网遭受 ARP 欺骗攻击而造成计算机无法上网, 此 ARP 病毒欺骗大多在网吧环境发生, 会让所有上网计算机一瞬间掉线或部份计算机无法上网。开启此功能可以避免此种病毒攻击。

**MTU:** MTU 为 Maximum Transmission Unit 的缩写, 一般默认值为 1,500。但是在不同的网络环境中, 可能会使用不同的数值, 尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU Size: 1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同, 一般使用默认 Auto 即可, 不需做任何调整。

**高级设定:**



**封包类型:** VPN QOS 安全路由器提供三种数据封包传输类型, 包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood,

TCP-SYN-Flood 封包是最常见的攻击方式, 利用 TCP 协议三次握手的方式制造大量伪造的 TCP 连接, 大量占用被攻击方资源而

造成网络线路拥塞或者不通。

**UDP-Flood**，一种基于 UDP 协议的攻击模式，利用 UDP 连接产生大量的联机数来达到占用网络资源进行攻击，造成网络运行不正常。

**ICMP-Flood**，一种基于 ICMP 协议的攻击模式，比如大量的 Ping 连接 VPN QoS 安全路由器占用带宽，造成带宽拥塞占用网络资源进行攻击，造成网络运行不正常。

**广域网络阈值设定：**

来自外部网络的攻击，所有封包阈值，当外部攻击的所有封包数据达到一个最大值（默认 15000pakets/Sec），单一封包阈值，当外部单一一个 IP 地址攻击的封包数据达到一个最大值（默认 2000pakets/Sec），当达到这些条件后，其“达到阈值则阻挡此 IP  分钟”（默认是 5 分钟），您可以根据需要调整您的阈值以及阻挡时间来达到对外部攻击的有效防护，建议其阈值从大到小来调节。

**网页内容管制功能：**

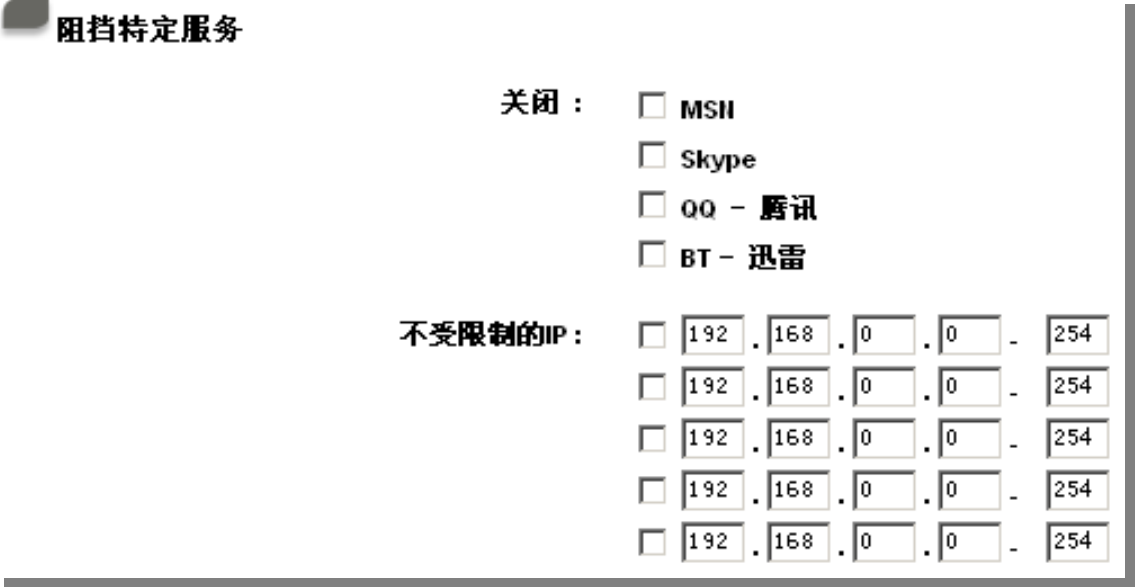
VPN QoS 安全路由器支持封锁下列几种的方式连接：Java，Cookies，Active X， HTTP 代理服务器存取。

**不需关闭 Java / ActiveX / Cookies 代理服务器存取于信任的主机：**

若启动这项功能，使用者可以将信任的网站或者 IP 地址加入可信任的网域中，则 VPN QoS 安全路由器就不会去阻挡可信任网域的网页中所带有的 Java/ActiveX/Cookies 等项目。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

## 阻挡特定服务



**阻挡特定服务**

关闭：  
 MSN  
 Skype  
 QQ - 腾讯  
 BT - 迅雷

不受限制的IP：  
 192 . 168 . 0 . 0 - 254  
 192 . 168 . 0 . 0 - 254  
 192 . 168 . 0 . 0 - 254  
 192 . 168 . 0 . 0 - 254  
 192 . 168 . 0 . 0 - 254

你可以在 **MSN/Skype/QQ-腾讯/BT-迅雷** 前面做“√”选，VPN QOS 安全路由器将阻挡你做“√”选的服务，但考虑到内网有特殊的 IP 地址需要此服务而不受限制，用户可以在下面做“√”选然后输入特定的 IP 地址或 IP 地址段开放以上做“√”选的特定服务。

### 4.3.2. 网络访问存取规则

用户可以设定 VPN QOS 安全路由器关闭或是允许任何的封包进出 Internet。您可以选择设定不同的网络存取限制，从内部到外部，从外部到内部。可以设定 IP 地址及通讯端口号不同的封包，过滤 Internet 存取规则条件。

网络存取规则依照 IP 地址，目的地 IP 地址，与 IP 通讯协议形态来管理所有的网络封包流量是否可以通过 VPN QOS 安全路由器的存取。

VPN QOS 安全路由器拥有简而易懂的网络存取规则条例工具。用户可自定的网络存取规则条例，可以选择关闭或是开启并保护所有对网际网络 Internet 的存取。以下就针对 VPN QOS 安全路由器的网络存取规则条例做一说明：

- All traffic from the LAN to the WAN is allowed - 从 LAN 端到 WAN 端的封包默认为可以通过
- All traffic from the WAN to the LAN is denied - 从 WAN 端到 LAN 端的封包默认为关闭

- All traffic from the LAN to the DMZ is allowed - 从 LAN 端到 DMZ 端的封包默认为可以通过
- All traffic from the DMZ to the LAN is denied - 从 DMZ 端到 LAN 端的封包默认为关闭
- All traffic from the WAN to the DMZ is allowed - 从 WAN 端到 DMZ 端的封包默认为开启
- All traffic from the DMZ to the WAN is allowed - 从 DMZ 端到 WAN 端的封包默认为开启

使用者可以自定义存取规则并且超越 VPN QOS 安全路由器的默认存取条件规则，但是以下的四种额外服务项目为永远开启，不受其它自定义规则所影响：

\* HTTP 的服务从 LAN 端到 VPN QOS 安全路由器 默认为开启的 (为了管理 VPN QOS 安全路由器使用)

\* DHCP 的服务从 LAN 端到 VPN QOS 安全路由器 默认为开启的 (为了从 VPN QOS 安全路由器自动取得 IP 地址使用)

\* DNS 的服务从 LAN 端到 VPN QOS 安全路由器 默认为开启的 (为了解析 DNS 服务使用)

\* Ping 的服务从 LAN 端到 VPN QOS 安全路由器 默认为开启的 (为了连通测试 VPN QOS 安全路由器使用)



QNO 防火墙配置 => 访问存取规则设定

跳到 1 / 1 页 每页显示的字段 20

优先权	激活	管制动作	服务端口	来源端口	来源位置	目的位置	管制时间	日	删除
	<input checked="" type="checkbox"/>	允许	所有端口 [1]	局域网	任何的	任何的	所有时间		
	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	广域网1	任何的	任何的	所有时间		
	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	广域网2	任何的	任何的	所有时间		
	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	广域网3	任何的	任何的	所有时间		
	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	广域网4	任何的	任何的	所有时间		
	<input checked="" type="checkbox"/>	关闭	所有端口 [1]	DMZ	任何的	192.168.2.0 ~ 192.168.2.255	所有时间		
	<input checked="" type="checkbox"/>	允许	所有端口 [1]	DMZ	任何的	任何的	所有时间		

增加新的管制规则 恢复原出厂预设值

除了默认规则以外，所有的网络存取规则都会显示如上图规则列表中，您可以依照或是自己选择高低优先权于每一个网络存取规则项目中。按下**编辑**按钮可以设定网络存取规则项目，以及按下**删除**可以删除网络存取规则项目。



按下**增加新的管制规则**新增新的网络存取规则按钮可以新增一项新的存取规则，或是按下 **恢复出厂默认值**可以恢复原有默认存取规则项目，以及删除所有的自定义规则内容回到出厂默认存取规则。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

## 增加新的管制规则



The screenshot shows the 'Access Control Rule Setting' page in the QNO firewall configuration interface. The page is titled '防火墙配置 => 访问存取规则设定'. On the left, there is a navigation menu with options like '首页', '基本配置项目', '进阶功能配置', 'DHCP 功能', '系统工具', '网络端口管理', '防火墙配置', '基本设定', '访问存取规则设定', '网页内容管制设定', 'VPN 私人虚拟网络', 'QVM 功能', and '日志'. The main content area is divided into two sections: '存取服务规则设定' and '时间管制设定'. The '存取服务规则设定' section includes fields for '管制动作' (Allow), '服务端口' (All ports), '日志' (Off), and '来源接口' (LAN). It also has input fields for '来源IP地址' and '目的IP地址'. The '时间管制设定' section includes a dropdown for '此存取规则' (All) and checkboxes for days of the week (每天, 周日, 周一, 周二, 周三, 周四, 周五, 周六).

## 服务管制内容

### 管制动作:

此为设定此规则的管制条例动作:

- 允许: 允许符合此管制条例行为的封包通过
- 禁止: 不允许符合此管制条例行为的封包通过

### 服务端口:

从下拉式选单中选择你所要允许或不允许的服务端口服务项目内容

### 服务端口新增或删除表:

- 若是您想要管制的服务端口内容没有存在于默认列表内的话，您可以按下右方的服务管理-**服务端口新增或删除表**来新增一个服务内容
- 于弹出窗口中输入一个服务名称-**Service Name** 以及通讯协议与端口- **Protocol & Prot**，按下新增-**Add**按钮即可新增一个管制服务项目内容

### 来源接口:

选择你所要允许或不允许的来源封包接口(如: LAN, WAN1, WAN2 或任何), 可以从下拉式选单中选择

- 来源 IP 地址:** 选择来源封包的 IP 范围(如任何的、单独、范围以及设定好的 IP 群组名称), 若是选择单独或是范围的话, 请输入此单一或是一区段范围的 IP 地址
- 目的 IP 地址:** 选择目的端封包的 IP 范围((如任何的, 单独或范围及设定好的 IP 群组名称), 若是选择单独或是范围的的话, 请输入此单一或是一区段范围的 IP 地址

### 时间管制设定

当选择为 **全部** 时, 表示此条规则 24 小时执行。若选择 **从** 时, 此管制条例会依据所设定的生效时间去执行此条规则, 如管制时间为周一到周五, 早上八点到下午六点, 您可以依照以下图例来管制。



- 存取规则:** 如果选择“**全部**”表示此管制规则 24 小时开启。如果“**从**”就激活特定时间设定如以下介绍
- .....到.....:** 此管制规则有时间限制, 设定方式为 24 小时制, 如 08: 00 ~ 18: 00 (早上 8 点到下午 6 点)
- 管制天数:** 勾选“**每天**”是表示每一天的这段时间都受控管, 若是只针对一星期特定星期几, 可以直接选择

设定修改完成请按下 **“确定”** 按钮储存网络设定变更或是按下 **“取消”** 按钮不做任何设定变更。

管制服务项目管理:



- 服务端名称:** 新增服务项目内容，可自定名称
- 通讯协议:** 新增服务项目通讯协议为 TCP 或是 UDP 封包格式
- 服务端口位置范围:** 设定开启此服务的端口位置范围，如 Port 从 9000~9002
- 增加到对应列表:** 增加此新增的服务项目内容到服务表列内
- 删除所选服务端口列表:** 选择删除服务项目内容从服务表列内
- 确定:** 按下此按钮"Apply"即会储存刚才所变动的修改设定内容参数
- 删除:** 按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效
- 离开:** 退出此服务表管理画面

### 4.3.3. 网页内容管制设定

VPN QOS 安全路由器的网页内容管制设定可支持两种模式的网页管制，一为开启网页内容管制功能封锁不允许访问的网址，另一个为开启只允许可以访问的网页管制允许访问的网站，此两种模式只能使用一种。

#### 封锁不允许访问的网址

此功能需将完整的网址如www.sex.com填入，即可封锁此网站。



#### 开启网页内容管制功能

选择打开启网页内容管制功能，默认为关闭。

**开启网页内容管制功能:** 网页管制内容项目

**新增:** 填写欲管制的网址，如 www.playboy.com

**增加到对应列表:** 按下“增加到对应表”按钮新增此一欲管制的网址

**删除所选择的过滤项目：** 可以使用鼠标点选一个或多个管制的网址，然后按下即可删除

### 网页字符串管制：

选择打勾开启网页字符串管制功能，默认为开启。例如：输入“sex”字符，那所有在网址里面有“sex”的网站都会被封锁。



- 新增：** 输入关键词
- 增加到对应列表：** 增加此新增的服务项目内容到服务表列内
- 删除所选择的内容：** 选择删除服务项目内容从服务表列内
- 确定：** 按下此按钮“确定”即会储存刚才所变动的修改设定内容参数
- 取消：** 按下此按钮“取消”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

### 时间管制设定

当选择为 **全部** 时，表示此条规则 24 小时执行。若选择 **从** 时，此管制条例会依据所设定的生效时间去执行此条规则，如管制时间为周一到周五，早上八点到下午六点，您可以依照以下图例来管制。

**时间管制设定**

此存取规则  :  :  到  :  (时间表示:24小时制)

每天  周日  周一  周二  周三  周四  周五  周六

- 存取规则:** 如果选择“全部”表示此管制规则 24 小时开启。如果“从”就激活特定时间设定如下介绍
- .....到.....:** 此管制规则有时间限制，设定方式为 24 小时制，如 08: 00 ~ 18: 00 (早上 8 点到下午 6 点)
- 管制天数:** 勾选“每天”是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

## 5. 虚拟私有网络的连接（VPN）

### 5.1. VPN 虚拟私有网络（VPN）

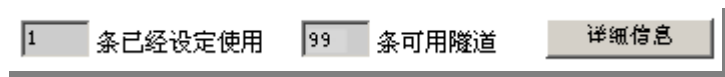


The screenshot shows the 'VPN 虚拟私有网络 => 目前VPN状态' page. On the left is a navigation menu with options like '首页', '基本配置项目', '进阶功能配置', 'DHCP 功能', '系统工具', '网络端口管理', '防火墙配置', 'VPN 私人虚拟网络', '目前 VPN 状态', '网关对网关设定', '客户端对网关设定', 'PPTP 设定', '封包穿透路由器功能', 'QVM 功能', and '日志'. The main content area is titled 'VPN虚拟私有网路 => 目前VPN状态' and includes a '注销' button in the top right. Below the title, there are statistics: '1 条已经设定使用' and '99 条可用隧道', with a '详细信息' button. The main section is '所有的VPN隧道状态', which includes a '新增一条隧道' button, a pagination control '跳到 1 / 1 页', and a table of VPN tunnels. The table has columns: No., Name, Status, Phase2 Enc/Auth/Grp, Local Group, Remote Group, Remote Gateway, Tunnel Test, and Config. One tunnel is listed with No. 1, Name 1, Status 联机, Phase2 Enc/Auth/Grp DES/MD5/1, Local Group 192.168.2.0/255.255.255.0, Remote Group 192.168.1.0/255.255.255.0, Remote Gateway 59.40.45.105, Tunnel Test 中断, and Config. Below the table are two summary boxes: '1 条隧道已经激活' and '1 条隧道已经设定'. At the bottom, there is a 'GroupVPN状态' section with a table of columns: Group Name, Connected Tunnels, Phase2 Enc/Auth/Grp, Local Group, Remote Client, Remote Client Status, Tunnel Test, and Config.

#### 5.1.1. 目前所有的 VPN 状态显示（Summary）

此 VPN 状态可以显示目前有关 VPN 方面的实时状态，包含：信道-Tunnel，设定参数以及 GroupVPN-VPN 群组状态等信息。

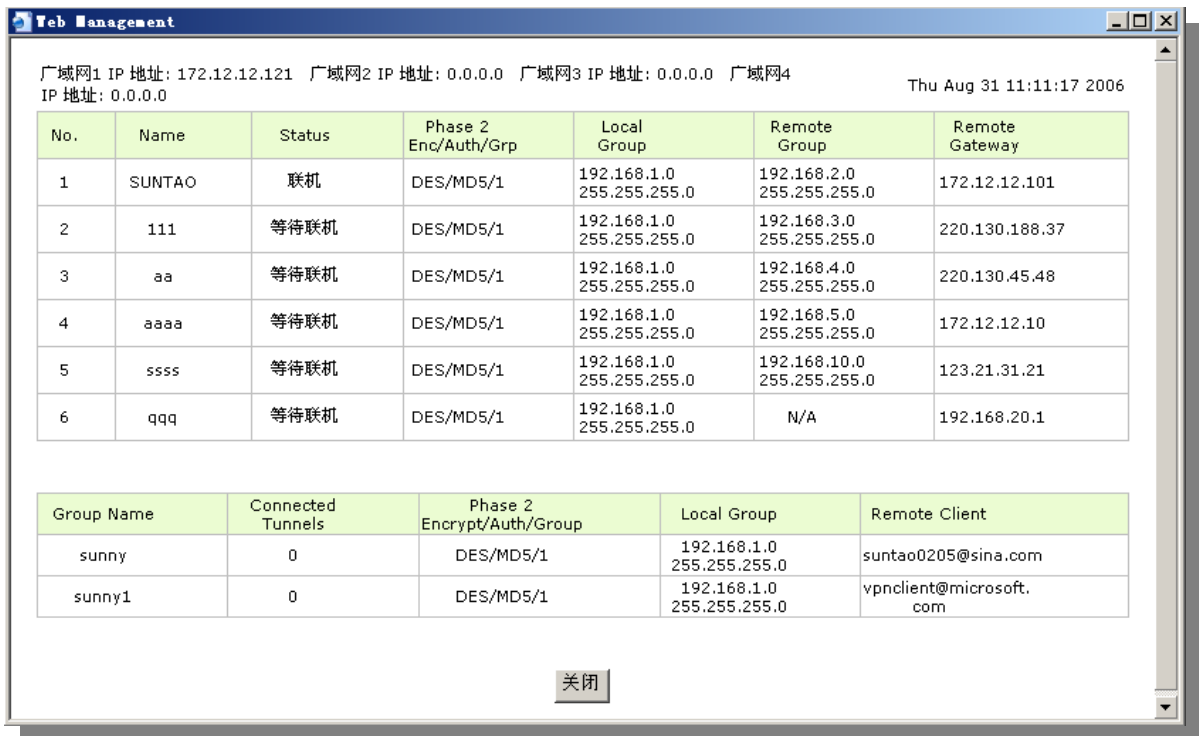
目前 VPN 状态（Summary）：



The summary statistics show: '1 条已经设定使用', '99 条可用隧道', and a '详细信息' button.

此为显示目前有多少 VPN 信道已经设定使用, 还剩下多少信道可以提供设定, VPN QOS 安全路由器 可同时支持共 200 组 IPSec VPN 信道(tunnels)。

**详细信息:** 按下此详细信息按钮可以显示如以下画面的目前所有 VPN 组态, 让用户清楚的管理所有 VPN 连接信息。



广域网1 IP 地址: 172.12.12.121 广域网2 IP 地址: 0.0.0.0 广域网3 IP 地址: 0.0.0.0 广域网4 IP 地址: 0.0.0.0 Thu Aug 31 11:11:17 2006

No.	Name	Status	Phase 2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway
1	SUNTAO	联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.2.0 255.255.255.0	172.12.12.101
2	111	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.3.0 255.255.255.0	220.130.188.37
3	aa	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.4.0 255.255.255.0	220.130.45.48
4	aaaa	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.5.0 255.255.255.0	172.12.12.10
5	ssss	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.10.0 255.255.255.0	123.21.31.21
6	qqq	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	N/A	192.168.20.1

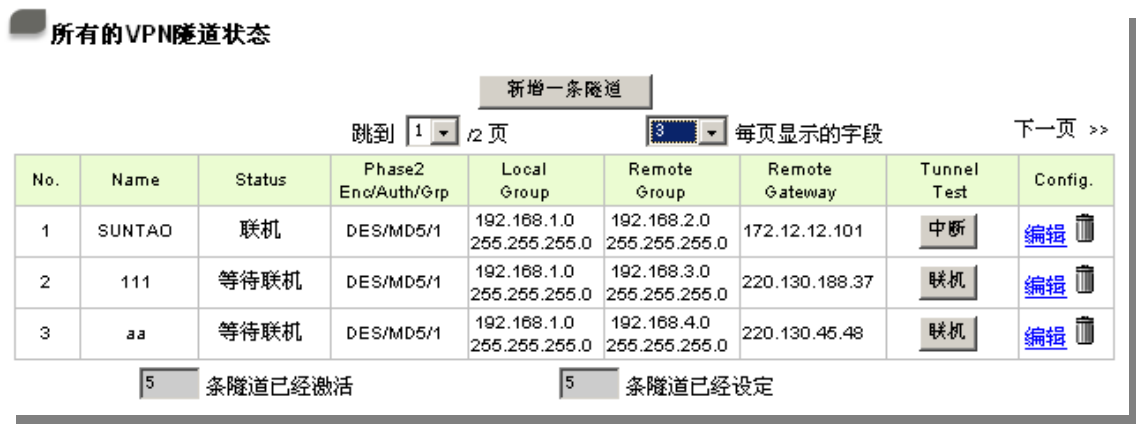
  

Group Name	Connected Tunnels	Phase 2 Encrypt/Auth/Group	Local Group	Remote Client
sunny	0	DES/MD5/1	192.168.1.0 255.255.255.0	suntao0205@sina.com
sunny1	0	DES/MD5/1	192.168.1.0 255.255.255.0	vpnclient@microsoft.com

关闭

### VPN 信道目前状态显示 (Tunnel Status) :

以下就针对“所有的 VPN 隧道状态” VPN 信道目前状态显示做完整解说:



**所有的VPN隧道状态**

新增一条隧道



跳到 1 /2 页 每页显示的字段 下一页 >>

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	SUNTAO	联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.2.0 255.255.255.0	172.12.12.101	中断	<a href="#">编辑</a>
2	111	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.3.0 255.255.255.0	220.130.188.37	联机	<a href="#">编辑</a>
3	aa	等待联机	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.4.0 255.255.255.0	220.130.45.48	联机	<a href="#">编辑</a>

5 条隧道已经激活      5 条隧道已经设定

上一页/下一页、跳到 您可以按下上一页( Previous page)与下一页(Next page)按钮跳到您想




<b>___ / ___ 页、每页显示的字 段</b>	监看的 VPN 信道画面上，或者您可以直接选择每一次所显示的页次，来监看您的所有 VPN 信道状态，如(3, 5, 10, 20, All)
<b>Tunnel No.</b>	当您设定 VPN QOS 安全路由器 内建之 VPN 功能时，请选择您要设定的信道编号，最多可支持 200 条 IPSec VPN 信道设定(VPN 网关对 VPN 网关的设定与客户端对 VPN 网关的设定)
<b>Status:</b>	于此状态显示已经联机成功- (Connected)，计算机名称解析失败- (Hostname Resolution Failed)，解析计算机名称 (Resolving Hostname) 以及等待联机- (Waiting for Connection) 等信息，若是用户选择手动-Manual 设定 IPSec 信道，则此状态会显示手动-Manual 设定与没有测试此项手动设定功能状态模式
<b>Name:</b>	目前联机 VPN 信道连接名称，如 XXX Office，建议您若是有一个以上的信道设定的话，务必将每一个信道名称都设为不同，以免混淆 <hr/> <b>注意:</b> 此信道名称若是您需要连接其它 VPN 设备(非 VPN QOS 安全路由器)时，有一些设备规定此信道名称要与主控端为相同名称并做验证，此信道才会顺利联机开启
<b>Phase2 Encrypt/Auth/Group:</b>	于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设定模式 若是您选择手动(Manual)设定 IPSec 的话，于此将不会显示 Phase 2 DH 群组
<b>Local Group:</b>	此为显示本地区域端的 VPN 联机安全群组设定
<b>Remote Group:</b>	此为显示远程的 VPN 联机安全群组设定
<b>Remote Gateway:</b>	此为设定为欲与远程 VPN 设备联机的 IP 地址，请设定为远程的 VPN VPN QOS 安全路由器的对外合法 IP 地址或是域名等
<b>Tunnel Test:</b>	可以按下“联机”按钮去验证此信道的状态，测试结果将会更新于此状态上，在联通的情况下显示“中断”，你可以点“中断”按钮中断 VPN 连接
<b>Config.:</b>	设定项目包含编辑(Edit)以及删除图标   若您按下编辑(Edit) 按钮，将会连接到此设定的项目当中，您可以修改其中的设定。若您选择按下垃圾桶图标的话  ，所有此信道的设定将会被删除
<b>___ 条信道已经激活、 ___ 条信道已经设定</b>	于此显示已有多少条信道已被激活开启以及有多少条信道已经被设定过

### 群组 VPN 状态显示 (GroupVPN Status) :

若您无选择并设定群组 VPN 模式(GroupVPNs)，此将不显示出会群组 VPN(GroupVPNs)状态。

### GroupVPN状态

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.
Group	0	DES/MD5/1	192.168.1.0 255.255.255.0	suntao@sina.com	<a href="#">详细信息</a>	N/A	<a href="#">编辑</a> 

- Group Name:** 目前设定联机 GroupVPNs 信道连接名称
- Connected Tunnels:** 于此显示已经联机的 VPNGroups 信道
- Phase2 Encrypt/Auth/Group:** 于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设定模式  
若是您选择手动(Manual)设定 IPsec 的话，于此将不会显示 Phase 2 DH 群组
- Local Group:** 此为显示本地区域端的群组 VPN 联机安全群组设定
- Remote Client:** 此为显示此 GroupVPN。远程的 VPN 联机安全群组设定
- Remote Client Status:** 若您按下更多信息列表(Detail List) 按钮，此将会显示更多有关信息，包含群组名称(Group Name)，IP 地址(IP 地址)以及联机时间信息等
- Tunnel Test:** 可以按下连接按钮-Connect 去验证此信道的状态，测试结果将会更新于此状态上
- Config:** 如下图所示，设定项目包含编辑(Edit)以及删除图标  若您按下编辑 (Edit) 按钮，将会连接到此设定的项目当中，您可以修改其中的设定。若您选择按下垃圾桶图标的话 ，所有此信道的设定将会被删除

### 5.1.2. 新增一条 VPN 信道（Add New Tunnel）

VPN QoS 安全路由器支持**网关对网关信道（Gateway to Gateway Tunnel）**或**客户端对网关信道（Client to Gateway Tunnel）**。

VPN 信道连接为 2 台 VPNVPN QoS 安全路由器分别通过网际网络 Internet 所组成，当您按下新增一条隧道的话，将会直接导引到 **VPN 网关对 VPN 网关** 的设定或**客户端对 VPN 网关** 的设定的页面上。

#### 网关对网关设定（Gateway to Gateway）：

当您按下新增“Add Now”的话，将会直接导引到 **VPN 网关对 VPN 网关** 的设定页面上。

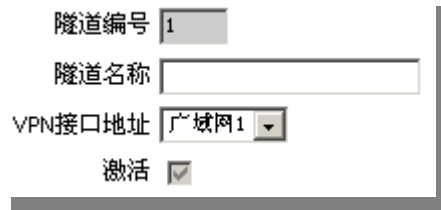


#### 客户端对网关(Client to Gateway):

当您按下新增“Add Now”的话，将会直接导引到**客户端对 VPN 网关** 的设定页面上。



### 5.1.2.1. 网关对网关的设定 (Gateway to Gateway-VPN)



隧道编号 1  
 隧道名称  
 VPN接口地址 广域网1  
 激活

透过以下的设定说明，使用者就可以在两台 VPN QOS 安全路由器之间建立一条 VPN 信道。

**隧道编号:** 当您设定 VPN QOS 安全路由器内建之 VPN 功能时,请选择您要设定的 Tunnel 信道编号

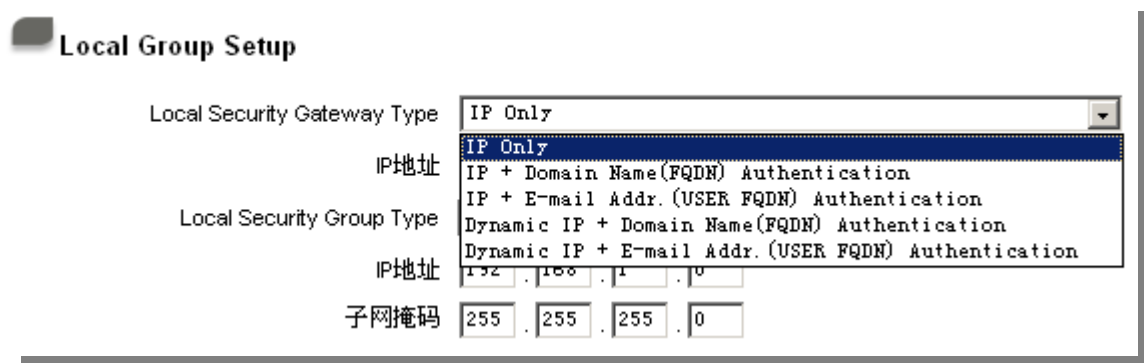
**VPN 接口地址:** 您可以选择哪一个接口位置做为此 VPN 信道的节点，一开始的默认 WAN 端共有四个 WAN1~4 可作为此 VPN 信道的使用

**隧道名称:** 设定此信道连接名称,如 XXX Office,建议您若是有一个以上的信道设定的话,务必将每一个信道名称都设为不同,以免混淆

**请注意:** 此信道名称若是您需要连接其它 VPN 设备(非 VPN QOS 安全路由器)时,有一些设备规定此信道名称要与主控端为相同名称并做验证,此信道才会顺利联机开启!。

**激活:** 勾选激活选项,将此 VPN 信道开启。此项目为默认为激活,当设定完成后,可以再选择是否激活信道设定

### 近端网关安全群组设定(Local Group Setup) :



**Local Group Setup**

Local Security Gateway Type IP Only  
 IP地址 IP Only  
 Local Security Group Type IP + Domain Name(FQDN) Authentication  
 IP + E-mail Addr. (USER FQDN) Authentication  
 Dynamic IP + Domain Name(FQDN) Authentication  
 Dynamic IP + E-mail Addr. (USER FQDN) Authentication  
 IP地址 192 . 168 . 1 . 0  
 子网掩码 255 . 255 . 255 . 0

此项目的近端网关安全群组设定( Local Security Gateway Type )类型必须与连接远程的网关安全



群组设定( Remote Security Gateway Type)类型相同。

### Local Security Gateway Type

区域端群组设定，有五种操作模式项目选择，分别为：

**IP Only**-只使用 IP 作为认证

**IP + Domain Name(FQDN) Authentication**，-IP+网域名称

**IP + E-mail Addr. (USER FQDN) Authentication**，-IP+电子邮件

**Dynamic IP + Domain Name(FQDN) Authentication**，-动态 IP 地址+网域名称

**Dynamic IP + E-mail Addr. (USER FQDN) Authentication**。 动态 IP 地址+电子邮件名称

此项目的近端网关安全群组设定( **Local Security Gateway Type** ) 类型必须与连接远程的远程网关安全群组设定( **Remote Security Gateway Type**)类型相同。

#### (1) IP Only:

若您选择 IP Only 类型的话，只有固定填入此 IP 地址可以存取此信道，然后 VPN QOS 安全路由器的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设定。

Local Security Gateway Type

IP地址

#### (2) IP + Domain Name(FQDN) Authentication:

若您选择 IP +网域名称类型的话，请输入您所验证的网域名称以及 IP 地址然后 VPN QOS 安全路由器的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设定。FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

Local Security Gateway Type

Domain Name

#### (3) IP + E-mail Addr. (USER FQDN) Authentication:

若您选择 IP 地址加上电子邮件类型的话，只有固定填入此 IP 地址以及电子邮件位置可以存取此信道，然后 VPN QOS 安全路由器的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设定。

Local Security Gateway Type

电邮地址  @

IP地址

#### (4) Dynamic IP + Domain Name(FQDN) Authentication:

若是您使用动态 IP 地址连接 VPN QOS 安全路由器时，您可以选择此类型连接 VPN，，当远程的 VPN 网关要求与 VPN QOS 安全路由器作为 VPN 联机时， VPN QOS 安全路由器 将会开始验证并

响应此 VPN 信道联机; 若您选择此类型连接 VPN, 请输入网域名称即可。

Local Security Gateway Type

Domain Name

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication:**

若是您使用动态 IP 地址连接 VPN QOS 安全路由器时, 您可以选择此类型连接 VPN, 使用者不必输入 IP 地址, 当远程的 VPN 网关要求与 VPN QOS 安全路由器作为 VPN 联机时, VPN QOS 安全路由器 将会开始验证并响应此 VPN 信道联机; 若您选择此类型连接 VPN, 请输入电子邮件认证到 E-Mail 位置空格字段中即可。

Local Security Gateway Type

电邮地址  @

**Local Security Group Type**

此为设定本地区域端的 VPN 联机安全群组设定, 以下有几个关于本地区域端设定的项目, 请您选择并设置适当参数:

**(1) IP 地址**

此项目为允许此 VPN 信道联机后, 只有输入此 IP 地址的本地端计算机可以联机。

Remote Security Gateway Type

IP地址   .  .  .

以 上的设定参考为: 当此 VPN 信道联机后, 于 192.168.1.0~255 的此网段的 IP 地址范围的计算机可以联机。

**(2) Subnet**

此项目为允许此 VPN 信道联机后, 每一台于此网段的本地端计算机都可以联机。

Remote Security Group Type

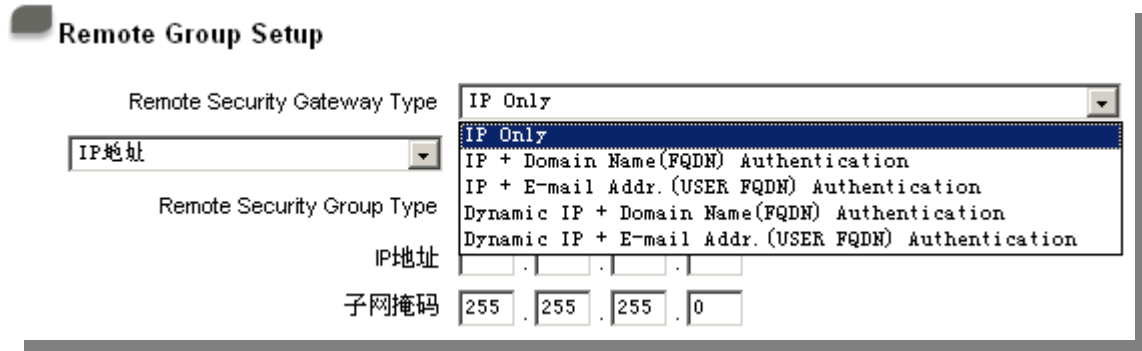
IP地址  .  .  .

子网掩码  .  .  .

以上的设定参考为: 当此 VPN 信道联机后, 只有 192.168.1.0, 子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机。



## 远程安全群组设定 (Remote Group Setup) :



The screenshot shows the 'Remote Group Setup' configuration page. It includes a dropdown for 'Remote Security Gateway Type' set to 'IP Only'. Below it is a dropdown for 'IP地址' (IP Address). The 'Remote Security Group Type' dropdown is open, showing options: 'IP Only', 'IP + Domain Name(FQDN) Authentication', 'IP + E-mail Addr. (USER FQDN) Authentication', 'Dynamic IP + Domain Name(FQDN) Authentication', and 'Dynamic IP + E-mail Addr. (USER FQDN) Authentication'. Below these are input fields for 'IP地址' and '子网掩码' (Subnet Mask) with values '255', '255', '255', and '0'.

此项目的远程网关安全群组设定( Remote Security Gateway Type)类型必须与连接远程的近端网关安全群组设定( Local Security Gateway Type)形态相同。

### Remote Security Gateway Type:

远程安全群组设定, 有五种操作模式项目选择, 分别为:

**IP Only**-只使用 IP 作为认证

**IP + Domain Name(FQDN) Authentication**, -IP+网域名称

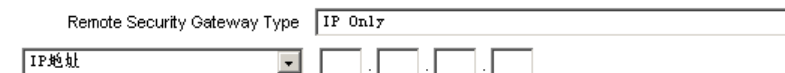
**IP + E-mail Addr. (USER FQDN) Authentication**, -IP+电子邮件

**Dynamic IP + Domain Name(FQDN) Authentication**, -动态 IP 地址+网域名称

**Dynamic IP + E-mail Addr. (USER FQDN) Authentication**. 动态 IP 地址+电子邮件名称

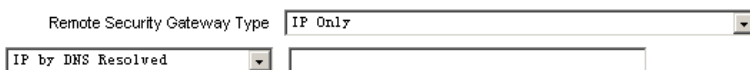
#### (1) IP Only:

若您选择 IP Only 类型的话, 只有固定填入此 IP 地址可以存取此信道,



The screenshot shows the 'Remote Security Gateway Type' dropdown set to 'IP Only'. Below it is a dropdown for 'IP地址' (IP Address) and four input fields for the IP address.

若是使用者不知道远程客户的 IP 地址, 则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。



The screenshot shows the 'Remote Security Gateway Type' dropdown set to 'IP Only'. Below it is a dropdown for 'IP by DNS Resolved' and an input field for the domain name.

#### (2) IP + Domain Name(FQDN) Authentication:

若您选择 IP+网域名称类型的话, 请输入 IP 地址以及您所验证的网域名称 FQDN 是指主机名称以及网域名称的结合, 使用者可以输入一个符合 FQDN 的网域名称即可。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

Remote Security Gateway Type

IP地址

若是使用者不知道远程的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。此网域名称必须存在 Internet 上可以查询的到。并且在设定完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址。

Remote Security Gateway Type

IP by DNS Resolved

Domain Name(FQDN)

### (3) IP + E-mail Addr. (USER FQDN) Authentication:

若您选择 IP 地址加上电子邮件类型的话，只有固定填入此 IP 地址以及电子邮件位置可以存取此信道，

Remote Security Gateway Type

IP地址

电邮地址(USER FQDN)  @

若是使用者不知道远程客户的 IP 地址，则可以透过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

Remote Security Gateway Type

IP by DNS Resolved

### (4) Dynamic IP + Domain Name(FQDN) Authentication:

若是您使用动态 IP 地址连接 VPN 时，您可以选择动态 IP 地址加上主机名称以及网域名称的结合。

Remote Security Gateway Type

Domain Name(FQDN)

### (5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication:

若是您使用动态 IP 地址连接 VPN QoS 安全路由器时，您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 VPN QoS 安全路由器作为 VPN 联机时，VPN QoS 安全路由器将会开始验证并响应此 VPN 信道联机；请输入电子邮件认证到 E-Mail 位置空格字段中。

Remote Security Gateway Type

电邮地址  @

### Remote Security Group Type:

此为设定本地区域端的 VPN 联机安全群组设定，以下有几个关于本地区域端设定的项目，请您选择并设置适当参数：

#### (1) IP 地址

此项目为允许此 VPN 信道联机后，只有输入此 IP 地址的本地端计算机可以联机。

Remote Security Group Type

IP地址  .  .  .

以上的设定参考为:当此 VPN 信道联机后，于 192.168.1.0~255 的此网段的 IP 地址范围的计算机可以联机。

#### (2)Subnet

此项目为允许此 VPN 信道联机后，每一台于此网段的本地端计算机都可以联机。

Remote Security Group Type

IP地址  .  .  .

子网掩码  .  .  .

以上的设定参考为:当此 VPN 信道联机后，只有 192.168.1.0，子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机

#### (3)IP Range

此项目为允许此 VPN 信道联机后，只有输入此 IP 地址范围的本地端计算机可以联机

Remote Security Group Type

IP地址范围  .  .  .  到

以上的设定参考为:当此 VPN 信道联机后，只有 192.168.1.0 到 192.168.1.254 的 IP 地址范围的计算机可以联机。

## IPSec Setup

若是任何加密机制存在的话，此两个 VPN 信道的加密机制必须要相同才可以将此信道连接，并于传输资料中加上标准的 IPSec 密钥，我们称为加密密钥 “key”。VPN QOS 安全路由器提供了以下二种加密管理模式 Key Management，分别为手动(Manual) 以及 IKE 自动加密模式- IKE with Preshared Key (automatic)，你可以通过下拉菜单选择需要的加密模式如下图所示。

**IPSec Setup**

Keying Mode: Manual

Incoming SPI: Manual  
IKE with Preshared key

Outgoing SPI:

Encryption: DES

Authentication: MD5

Encryption Key:

Authentication Key:

### Key Management:

此选项设定为当您设定此 VPN 信道使用何种加密模式以及验证模式后，必须设定一组交换密码，并注意此参数必须与远程的交换密码参数相同;设定的方式有自动 Auto (IKE)或是手动 Manual 设定二种，于设定时请您选择其中一种设定方式即可！

**IPSec Setup**

Keying Mode: IKE with Preshared key

Phase1 DH Group: Group1

Phase1 Encryption: DES

Phase1 Authentication: MD5

Phase1 SA Life Time: 28800 seconds

Perfect Forward Secrecy:

Phase2 DH Group: Group1

Phase2 Encryption: DES

Phase2 Authentication: MD5

Phase2 SA Life Time: 3600 seconds

Preshared Key:

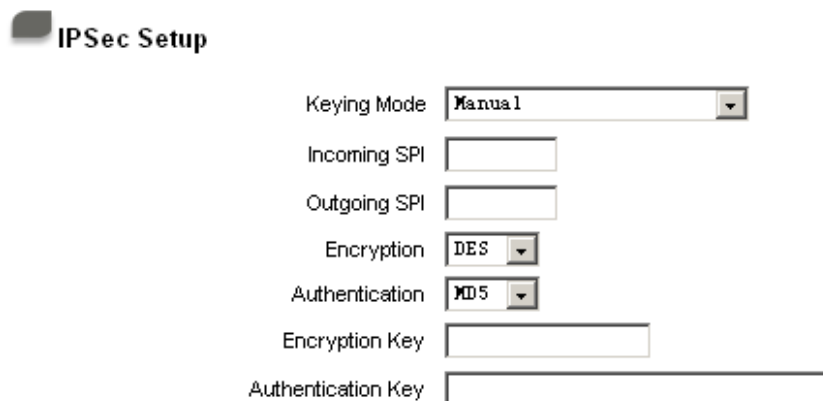
### IKE with Preshared Key (automatic):

透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将 PFS(Perfect Forward Secrecy)激活后，则会再第二阶段的 IKE 协调过程产生的第二把共同金钥做进一步加密与验证。当 PFS 激活后，透

过 brute force 来撬取金钥的骇客(hacker)无法在此短时间内，进一步得到第二把金钥。

- **PFS(Perfect Forward Secrecy):** 若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- **Phase1/Phase2 DH Group:** 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- **Phase1/Phase2 Encryption:** 此加密选项设定为设定此 VPN 信道使用何种加密模式，并注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安全码进行信息加密的标准，它支持 128 位、192 位和 256 位的密匙。
- **Phase1/Phase2 Authentication:** 此验证选项设定为设定此 VPN 信道使用何种验证模式，并注意设置此参数必须与远程的验证模式参数相同:“MD5”或“SHA1”。
- **Phase1 SA Lifetime:** 为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- **Phase2 SA Lifetime:** 为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- **Preshared Key:** 于 Auto (IKE) 选项中，您必须输入一组交换密码于 “Pre-shared Key” 的字段中，在此的范例设定为 test，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。

## Manual-手动方式



IPSec Setup

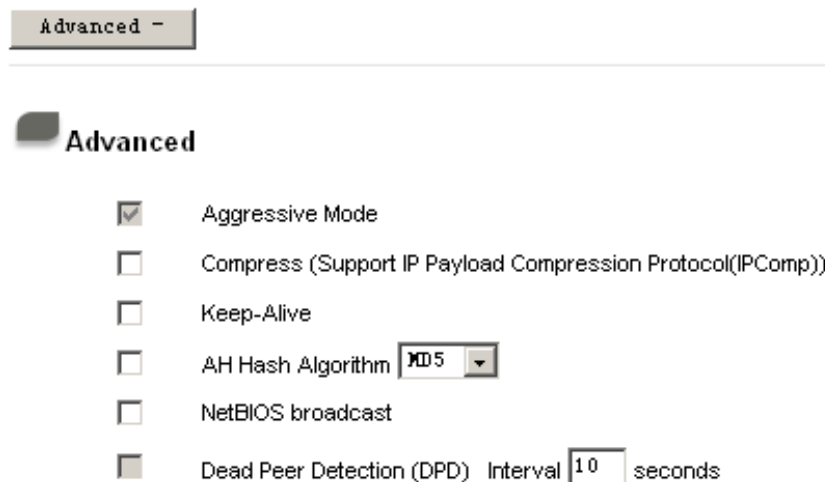
Keying Mode	Manual
Incoming SPI	<input type="text"/>
Outgoing SPI	<input type="text"/>
Encryption	DES
Authentication	MD5
Encryption Key	<input type="text"/>
Authentication Key	<input type="text"/>

若您选择手动模式 Manual 的话，此提供您自定加密密钥，而此密钥不需经过任何交换

(negotiation)。

- 于此分成加密密码“Encryption KEY”以及验证密码“Authentication KEY”二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。
- 另外还需要设定“Inbound SPI”的交换字符串以及“Outbound SPI” 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Inbound SPI 设定参数，您必须在远程的 VPN 设备的 Outbound SPI 设定相同字符串，而于本地端的 Outbound SPI 设定字符串，也必须与在远程的 VPN 设备的 Inbound SPI 设定相同字符串！

#### Advanced(进阶作业模式)-只供给使用自动交换密钥模式使用(IKE Preshared Key Only)



Advanced -

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS broadcast
- Dead Peer Detection (DPD) Interval 10 seconds

在 VPN QOS 安全路由器的进阶设定项目中，分别有 **Main Mode** 以及 **Aggressive**。模式，Main mode 是 VPN QOS 安全路由器的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- **Aggressive Mode:** 大多为远程的设备采用，如使用动态 IP 连接时，是为了加强其安全控管机制。
- **Compress:** 若选择此项目勾选，则连接的 VPN 信道中 VPN QOS 安全路由器 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- **Keep-Alive:** 若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- **AH Hash Algorithm:** AH (Authentication Header) 验证表头封包格式，可选择 MD5/DSHA-1。
- **NetBIOS Broadcast:** 若选择此项目勾选，则连接的 VPN 信道中会让 NetBIOS 广播封包通过。

有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 信道的流量就会加大！

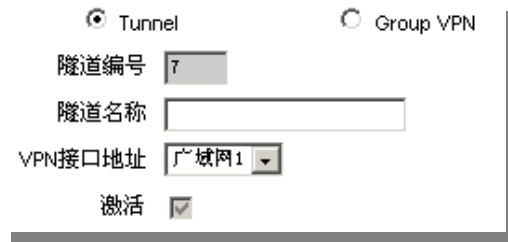
- **Dead Peer Detection(DPD):** 若选择此项目勾选，则连接的 VPN 信道中会定期的传送 HELLO/ACK 讯息封包来侦测是否 VPN 信道的两端仍有联机存在。当有一端断线则 VPN QoS 安全路由器会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息封包传递的时间，默认值为 10 秒。

### 5.1.2.2. 客户端对网关的设定 (Client to Gateway-VPN)

透过以下的设定说明, 管理人员就可以在客户端与 VPN QOS 安全路由器之间建立一条 VPN 信道。

用户可以选择这一条 VPN 信道在客户端是只供一个客户所使用(Tunnel)或者是由一群客户所使用(Group VPN)。若由一群客户所使用则可以节省个别设定远程的客户, 只需设定的一条信道供一组客户所使用, 以节省设定时的麻烦。

#### (1) 在 Tunnel 的情况:



**隧道编号:** 当您设定 VPN QOS 安全路由器内建之 VPN 功能时, 请选择您要设定的 Tunnel 信道编号。

**VPN 接口地址:** 您可以选择哪一个接口位置做为此 VPN 信道的节点, 一开始的默认 WAN 端共有四个 WAN1~4 可作为此 VPN 信道的使用。

**隧道名称:** 设定此信道连接名称, 如 XXX Office, 建议您若是有一个以上的信道设定的话, 务必将每一个信道名称都设为不同, 以免混淆

**请注意:** 此信道名称若是您需要连接其它 VPN 设备(非 VPN QOS 安全路由器)时, 有一些设备规定此信道名称要与主控端为相同名称并做验证, 此信道才会顺利联机开启!。

**激活:** 勾选**激活** 选项, 将此 VPN 信道开启。此项目为默认为激活 Enable, 当设定完成后可以再选择是否激活信道设定。



## Local Group Setup-近端服务端

此项目的近端网关安全群组设定( Local Security Gateway Type )类型必须与连接远程的网关安全群组设定( Remote Security Gateway Type)类型相同。

### Local Security Gateway Type:

区域端群组设定，有五种操作模式项目选择，分别为：

**IP Only**-只使用 IP 作为认证

**IP + Domain Name(FQDN) Authentication**， -IP+网域名称

**IP + E-mail Addr. (USER FQDN) Authentication**， -IP+电子邮件

**Dynamic IP + Domain Name(FQDN) Authentication**， -动态 IP 地址+网域名称

**Dynamic IP + E-mail Addr. (USER FQDN) Authentication**。 动态 IP 地址+电子邮件名称

#### (1) IP Only:

若您选择 IP Only 类型的话，FVR 9416 会依据你所选择的广域端口位置将其 IP 自动填入此项目空格内，您不需要在进行额外设定。

Local Security Gateway Type

IP地址

#### (2) IP + Domain Name(FQDN) Authentication:

若您选择 IP+网域名称类型的话，请输入您所验证的网域名称，VPN QOS 安全路由器的 WAN IP 地址，将会自动填入 IP 地址项目内，您不需要在进行额外设定。FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

Local Security Gateway Type

Domain Name

IP地址

#### (3) IP + E-mail Addr.(USER FQDN) Authentication:

若您选择 IP 地址加上电子邮件类型的话，只要将电子邮件位置填入，然后 VPN QOS 安全路由器的 WAN IP 地址，将会自动填入此项目空格内，您不需要在进行额外设定。

Local Security Gateway Type

电邮地址  @

IP地址

**(4) Dynamic IP + Domain Name(FQDN) Authentication:**

若是您使用动态 IP 地址连接 VPN QoS 安全路由器时，您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 VPN QoS 安全路由器作为 VPN 联机时，VPN QoS 安全路由器将会开始验证并响应此 VPN 信道联机；若您选择此类型连接 VPN，请输入网域名称即可

Local Security Gateway Type

Domain Name

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication:**

若是您使用动态 IP 地址连接 VPN QoS 安全路由器时，您可以选择此类型连接 VPN，使用者不必输入 IP 地址，当远程的 VPN 网关要求与 VPN QoS 安全路由器作为 VPN 联机时，VPN QoS 安全路由器将会开始验证并响应此 VPN 信道联机；请输入电子邮件认证到 E-Mail 位置空格字段中即可。

Local Security Gateway Type

电邮地址  @

**Local Security Group Type**

此为设定本地区域端的 VPN 联机安全群组设定，以下几个关于本地区域端设定的项目，请您选择并设置适当参数：

**(1)IP 地址(单一 IP 地址)**

此项目为允许此 VPN 信道联机后，只有输入此 IP 地址的本地端计算机可以联机。

Local Security Group Type

IP地址  .  .  .

以上的设定参考为:当此 VPN 信道联机后，于 192.168.1.0~255 的此网段的 IP 地址范围的计算机可以联机。

**(2)Subnet**

此项目为允许此 VPN 信道联机后，每一台于此网段的本地端计算机都可以联机。

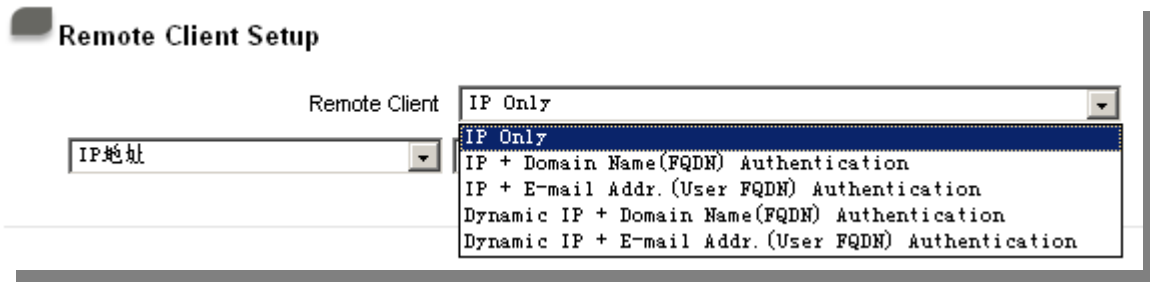
Local Security Group Type

IP地址  .  .  .

子网掩码  .  .  .

以上的设定参考为:当此 VPN 信道联机后，只有 192.168.1.0，子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机。

**Remote Client Setup-远程客户端设定:**



此项目的远程网关安全群组设定( Remote Security Gateway Type)类型必须与连接远程的近端网关安全群组设定( Local Security Gateway Type)类型相同。

**Remot Client:**

远程客户设定，有五种操作模式项目选择，分别为：

**IP Only-**只使用 IP 作为认证

**IP + Domain Name(FQDN) Authentication,** -IP+网域名称

**IP + E-mail Addr. (USER FQDN) Authentication,** -IP+电子邮件

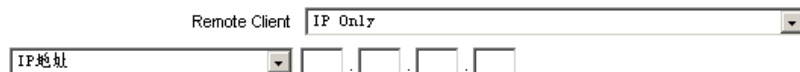
**Dynamic IP + Domain Name(FQDN) Authentication,** -动态 IP 地址+网域名称

**Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** 动态 IP 地址+电子邮件名称

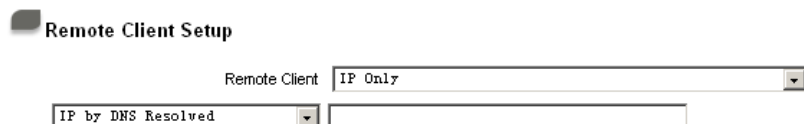
此项目的远程网关安全群组设定( Remote Security Gateway Type)类型必须与连接远程的近端网关安全群组设定( Local Security Gateway Type)类型相同。

**(1) IP Only:**

若您选择 IP Only 类型的话，只有固定填入此 IP 地址可以存取此信道。



若是使用者不知道远程客户的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。



**(2) IP+Domain Name(FQDN) Authentication:**

若您选择 IP+网域名称类型的话，请输入 IP 地址以及您所验证的网域

名称 FQDN 是指主机名称以及网域名称的结合，使用者可以输入一个符合 FQDN 的网域名称即可。此 IP 地址以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

Remote Client

IP地址

Domain Name(FQDN)

若是使用者不知道远程的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。此网域名称必须存在 Internet 上可以查询的到。并且在设定完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址。

Remote Client

IP by DNS Resolved

Domain Name(FQDN)

**(3) IP + E-mail Addr. (USER FQDN) Authentication:**

若您选择 IP 地址加上电子邮件类型的话，只有固定填入此 IP 地址以及电子邮件位置可以存取此信道。

Remote Client

IP地址

电邮地址(USER FQDN)  @

若是使用者不知道远程客户的 IP 地址，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP 地址。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

Remote Client

IP by DNS Resolved

电邮地址(USER FQDN)  @

**(4) Dynamic IP + Domain Name(FQDN) Authentication:**

若是您使用动态 IP 地址连接 VPN QOS 安全路由器时，您可以选择动态 IP 地址加上主机名称以及网域名称的结合。

Remote Client

Domain Name(FQDN)

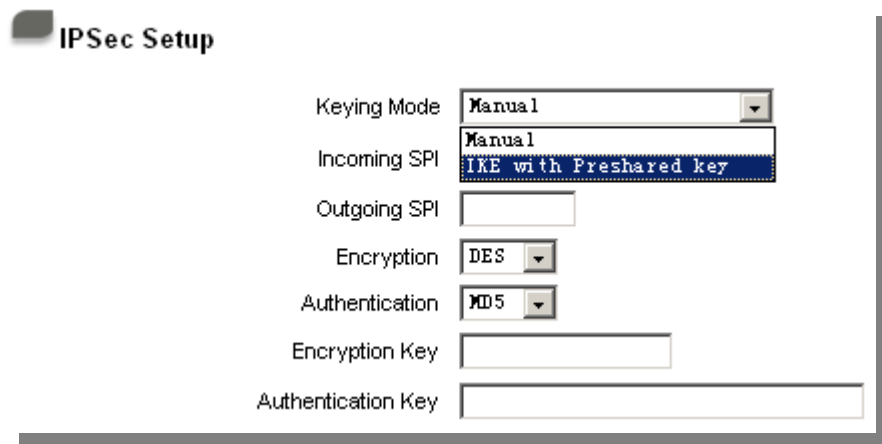
**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication:**

若是您使用动态 IP 地址连接 VPN QOS 安全路由器时，您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 VPN QOS 安全路由器作为 VPN 联机时，VPN QOS 安全路由器将会开始验证并响应此 VPN 信

道联机; 请输入电子邮件认证到 E-Mail 位置空格字段中。

Remote Client    
电邮地址(USER FQDN)  @

## IPSec Setup



**IPSec Setup**

Keying Mode    
Incoming SPI   
Outgoing SPI   
Encryption    
Authentication    
Encryption Key   
Authentication Key

若是任何加密机制存在的话, 此两个 VPN 信道的加密机制必须要相同才可以将此信道连接, 并于传输资料中加上标准的 IPSec 密钥, 于此我们称为加密密钥 “key”。VPN QOS 安全路由器提供了以下二种加密管理模式, 分别为手动(Manual) 以及 IKE 自动加密模式- IKE with Preshared Key (automatic) 如下图所示。

### Key Management:

此选项设定为当您设定此 VPN 信道使用何种加密模式以及验证模式后, 必须设定一组交换密码, 并注意此参数必须与远程的交换密码参数相同; 设定的方式有自动 Auto (IKE)或是手动 Manual 设定二种, 于设定时请您选择其中一种设定方式即可!

## IPSec Setup

Keying Mode	IKE with Preshared key
Phase1 DH Group	Group1
Phase1 Encryption	DES
Phase1 Authentication	MD5
Phase1 SA Life Time	28800 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DH Group	Group1
Phase2 Encryption	DES
Phase2 Authentication	MD5
Phase2 SA Life Time	3600 seconds
Preshared Key	

### IKE with Preshared Key (automatic):

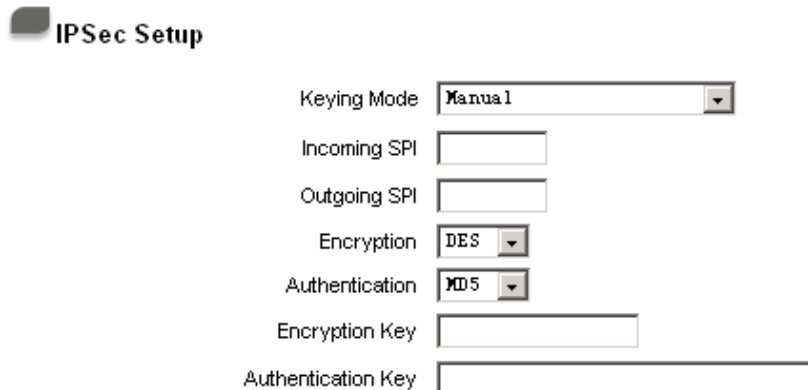
透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将 PFS(Perfect Forward Secrecy)激活后, 则会再第二阶段的 IKE 协调过程产生的第二把共同金钥做进一步加密与验证。当 PFS 激活后, 透过 brute force 来撷取金钥的骇客(hacker)无法在此短时间内, 进一步得到第二把金钥。

- **PFS(Perfect Forward Secrecy):** 若您将 PFS 选项勾选后, 记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- **Phase1/Phase2 DH Group:** 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- **Phase1/Phase2 Encryption:** 此加密选项设定为设定此 VPN 信道使用何种加密模式, 并注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安全码进行信息加密的标准, 它支持 128 位、192 位和 256 位的密匙。
- **Phase1/Phase2 Authentication:** 此验证选项设定为设定此 VPN 信道使用何种验证模式, 并注意设置此参数必须与远程的验证模式参数相同:“MD5”或“SHA1”。
- **Phase1 SA Lifetime:** 为此交换密码的有效时间, 系统默认值为 28800 秒(8 小时), 于此有效时间内的 VPN 联机, 系统会自动的将于有效时间后, 自动的生成其它的交换密码以确保安全。
- **Phase2 SA Lifetime:** 为此交换密码的有效时间, 系统默认值为 3600 秒(1 小时), 于此有效时间

内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

- **Preshared Key:** 于 Auto (IKE) 选项中，您必须输入一组交换密码于“Pre-shared Key”的字段中，在此的范例设定为 **test**，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。

### Manual-手动方式



**IPSec Setup**

Keying Mode	Manual
Incoming SPI	<input type="text"/>
Outgoing SPI	<input type="text"/>
Encryption	DES
Authentication	MD5
Encryption Key	<input type="text"/>
Authentication Key	<input type="text"/>

若您选择手动模式 **Manual** 的话，此提供您自定加密密钥，而此密钥不需经过任何交握 (negotiation)。

- 于此分成加密密码“**Encryption KEY**”以及验证密码“**Authentication KEY**”二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。
- 另外还需要设定“**Inbound SPI**”的交换字符串以及“**Outbound SPI**” 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 **Inbound SPI** 设定参数，您必须在远程的 VPN 设备的 **Outbound SPI** 设定相同字符串，而于本地端的 **Outbound SPI** 设定字符串，也必须与在远程的 VPN 设备的 **Inbound SPI** 设定相同字符串！

### Advanced(进阶作业模式)-只供给使用自动交换密钥模式使用(IKE Preshared Key Only)

Advanced -

---

**Advanced**

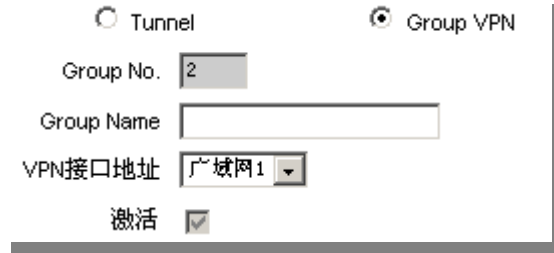
- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS broadcast
- Dead Peer Detection (DPD) Interval 10 seconds

在 VPN QOS 安全路由器的进阶设定项目中，分别有 **Main Mode** 以及 **Aggressive**。模式，Main mode 是 VPN QOS 安全路由器的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- **Aggressive Mode:** 大多为远程的设备采用，如使用动态 IP 连接时，是为了加强其安全控管机制。
- **Compress:** 若选择此项目勾选，则连接的 VPN 信道中 VPN QOS 安全路由器 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- **Keep-Alive:** 若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- **AH Hash Algorithm:** AH (Authentication Header) 验证表头封包格式，可选择 MD5/DSHA-1。
- **NetBIOS Broadcast:** 若选择此项目勾选，则连接的 VPN 信道中会让 NetBIOS 广播封包通过。，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 信道的流量就会加大！
- **Dead Peer Detection(DPD):** 若选择此项目勾选，则连接的 VPN 信道中会定期的传送 HELLO/ACK 讯息封包来侦测是否 VPN 信道的两端仍有联机存在。当有一端断线则 VPN QOS 安全路由器会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息封包传递的时间，默认值为 10 秒。



(2) 在 Group VPN 的情况:



**Group No.:** 最多可以设定两组 Group VPN。

**VPN 接口地址:** 您可以选择哪一个接口位置做为此 VPN 信道的节点, 一开始的默认 WAN 端共有四个 WAN1~4 可作为此 VPN 信道的使用。

**Group Name:** 设定此信道连接名称, 如 XXX Office, 建议您若是有一个以上的信道设定的话, 务必将每一个信道名称都设为不同, 以免混淆。

**请注意:** 此信道名称若是您需要连接其它 VPN 设备(非 VPN QoS 安全路由器)时, 有一些设备规定此信道名称要与主控端为相同名称并做验证, 此信道才会顺利联机开启!。

**激活:** 勾选**激活** 选项, 将此 VPN 信道开启。 此项目为默认为激活 Enable, 当设定完成后可以再选择是否激活信道设定。

**Local Group Setup-近端服务端设定:**

**Local Group Setup:** 此为设定本区域端端的 VPN 联机安全群组设定, 以下有几个关于本区域端端设定的项目, 请您选择并设置适当参数:

**Local Security Group Type:**

**(1) IP 地址**

此项目为允许此 VPN 信道联机后, 只有输入此 IP 地址的本地端计算机可以联机。

**Local Group Setup**

Local Security Group Type

IP地址  .  .  .

以上的设定参考为:当此 VPN 信道联机后, 于 192.168.1.0~255 的此网段的 IP 地址范围的计算机可以联机。

**(2) Subnet**

此项目为允许此 VPN 信道联机后, 每一台于此网段的本地端计算机都可以联机。

## Local Group Setup

Local Security Group Type

IP地址  .  .  .

子网掩码  .  .  .

以上的设定参考为:当此 VPN 信道联机后,只有 192.168.1.0,子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机。

## Remote Client Setup:远程客户端设定

### Remote Client Setup

Remote Client

Domain Name

#### Remote Client:

远程客户端设定,有三种操作模式项目选择,分别为:

**Domain Name(FQDN)**, -网域名称

**E-mail Address(USER FQDN)**, - 电子邮件名称

**Microsoft XP/2000 VPN Client**, - 微软 XP/2000 VPN 客户端

#### (1) Domain Name(FQDN):

若您选择网域名称类型的话,请输入您所验证的网域名称。FQDN 是指主机名称以及网域名称的结合,也必须存在于 Internet 上可以查询的到,如 vpn.Server.com。此网域名称必须与客户端的近端设定形态相同才可以正确连接。

Remote Client

Domain Name

#### (2) E-mail Addr. (USER FQDN):

若您选择电子邮件类型的话,只有固定填入此电子邮件位置可以存取此信道。

Remote Client

E-mail address  @

#### (3) Microsoft XP/2000 VPN Client:

若您选择微软 XP/2000 VPN 客户端形态的话，您不需要在进行额外设定。

Remote Client

## IPSec Setup

若是任何加密机制存在的话，此两个 VPN 信道的加密机制必须要相同才可以将此信道连接，并于传输资料中加上标准的 IPSec 密钥，于此我们称为加密密钥 “key”。VPN QOS 安全路由器提供了以下二种加密管理模式，分别为手动 (Manual) 以及 IKE 自动加密模式 - IKE with Preshared Key (automatic)。在选择 Group VPN 的情况之下或者是在远程网关安全形态 Remote Security Gateway Type 中使用动态位置 IP 时，Aggressive Mode 会自动激活，没有手动 Manual 模式。

## Key Management:

Keying Mode: IKE with Preshared key

Phase1 DH Group	<input type="text" value="Group1"/>
Phase1 Encryption	<input type="text" value="DES"/>
Phase1 Authentication	<input type="text" value="MD5"/>
Phase1 SA Life Time	<input type="text" value="28800"/>
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DH Group	<input type="text" value="Group1"/>
Phase2 Encryption	<input type="text" value="DES"/>
Phase2 Authentication	<input type="text" value="MD5"/>
Phase2 SA Life Time	<input type="text" value="3600"/>
Preshared Key	<input type="text"/>

- **PFS(Perfect Forward Secrecy):** 若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。
- **Phase1/Phase2 DH Group:** 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- **Phase1/Phase2 Encryption:** 此加密选项设定为设定此 VPN 信道使用何种加密模式，并注意设置此参数必须与远程的加密参数相同:DES:64-位加密模式、3DES:128-位加密模式、AES:用安

全码进行信息加密的标准，它支持 128 位、192 位和 256 位的密匙。

- **Phase1/Phase2 Authentication:** 此验证选项设定为设定此 VPN 信道使用何种验证模式，并注意设置此参数必须与远程的验证模式参数相同：“MD5”或“SHA1”。
- **Phase1 SA Lifetime:** 为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- **Phase2 SA Lifetime:** 为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。
- **Preshared Key:** 于 Auto (IKE) 选项中，您必须输入一组交换密码于 “Pre-shared Key” 的字段中，在此的范例设定为 test，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 30 个文字组合。

#### Advanced(进阶作业模式)-只供给使用自动交换密钥模式使用(IKE Preshared Key Only)

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS broadcast

在 VPN QOS 安全路由器的进阶设定项目中，分别有 **Main Mode** 以及 **Aggressive**。模式，Main mode 是 VPN QOS 安全路由器的默认 VPN 作业模式，而且与大多数的其它 VPN 设备使用连接方式为相同。

- **Aggressive Mode:** 大多为远程的设备采用，如使用动态 IP 连接时，为了加强其安全控管机制。在选择 Group VPN 时，Aggressive mode 会自动激活。
- **Compress:** 若选择此项目勾选，则连接的 VPN 信道中 VPN QOS 安全路由器支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- **Keep-Alive:** 若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 地址的远程使用。
- **AH Hash Algorithm:** AH (Authentication Header) 验证表头封包格式，可选择 MD5/SHA-1。

- **NetBIOS Broadcast:** 若选择此项目勾选，则连接的 VPN 信道中会让 NetBIOS 广播封包通过，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 信道的流量就会加大！

### 5.1.3. PPTP 设定

VPN QOS 安全路由器提供支持 Window XP/2000 的 PPTP 对我们 VPN QOS 安全路由器做点对点信道协议，让远程单机用户使用此种协议建立 VPN 联机。

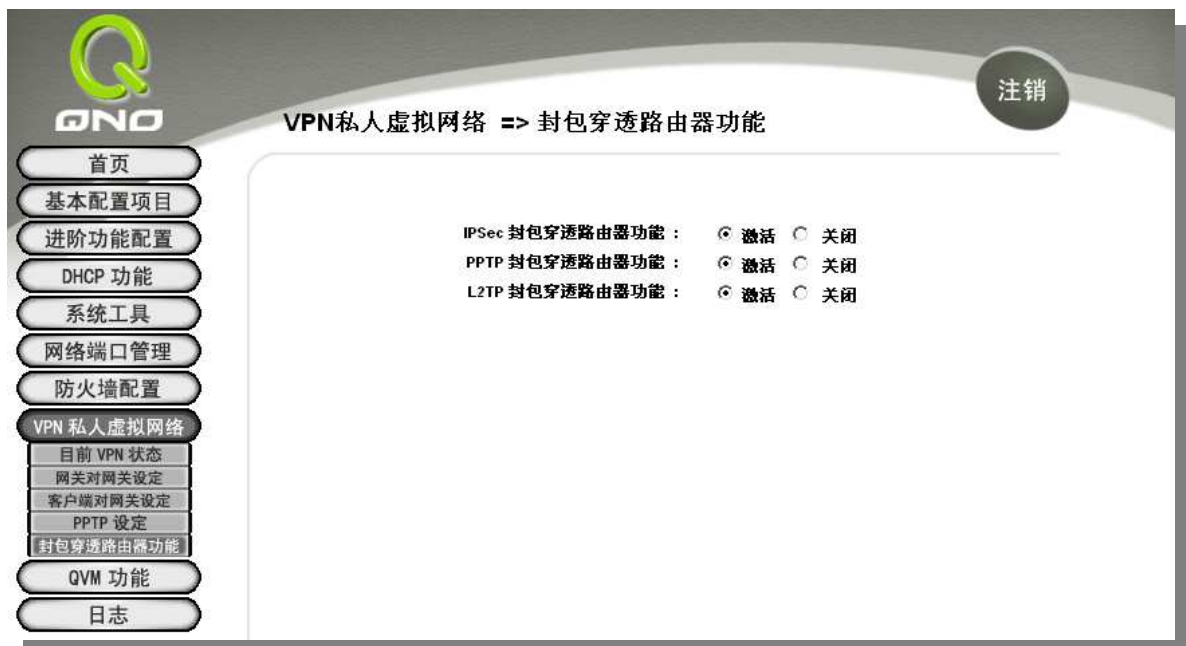


The screenshot shows the 'VPN私人虚拟网络 => PPTP 设定' (VPN Private Virtual Network => PPTP Settings) page. The interface includes a sidebar with navigation options like '首页', '基本配置项目', '进阶功能配置', 'DHCP 功能', '系统工具', '网络端口管理', '防火墙配置', 'VPN 私人虚拟网络', '目前 VPN 状态', '网关对网关设定', '客户端对网关设定', 'PPTP 设定', '封包穿透路由器功能', 'QVM 功能', and '日志'. The main content area has a '注销' (Logout) button in the top right. The configuration is divided into sections: '激活PPTP服务器' (checked), 'PPTP IP地址发放范围' (PPTP IP address distribution range) with '开始位置' (192.168.1.150) and '终止位置' (192.168.1.249), '新增使用者' (Add user) with '使用者已设定' (1 user set), and '所有的PPTP隧道状态' (All PPTP tunnel status) showing '0 条已经使用' (0 used) and '100 条可用隧道' (100 available tunnels). A table at the bottom shows columns for '使用者名称', '远程IP地址', and 'PPTP IP地址发放'.

- 激活 PPTP 服务:** 当使用者勾选后即可激活点对点隧道协议 PPTP 服务器
- PPTP IP 地址发放范围:** 请输入近端 PPTP IP 地址的范围,其目的是要给远程的使用者一个可进入近端网络的入口 IP。输入起始范围 Range Start:请在最后一栏输入数值。输入结束范围 Range End: 请在最后一栏输入数值
- 使用者名称:** 请输入远程使用者的名称
- 密码的输入与确认:** 输入使用者帐号密码及请再次确认输入远程使用者新的帐号密码
- 增加到对应列表:** 新增输入的帐号与密码
- 删除使用者:** 删除使用者
- 所有的 PPTP 隧道名称:** 显示出使用 PPTP 服务器信道的使用相关信息
- 使用者名称:** 联机建立后的远程使用者名称
- 远程 IP 地址:** 联机建立后的远程使用者的 IP 地址
- PPTP IP 地址发放:** 联机建立后,近端 PPTP 服务器的 IP 地址

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

#### 5.1.4. 封包穿透 VPN QOS 安全路由器功能 (VPN Pass Through-VPN)



IPSec 封包穿透 VPN QOS 安 若是选择**激活**的话,则允许 PC 端使用 VPN- IPSec 封包穿透 VPN

- 全路由器功能:** QOS 安全路由器以便与外部 VPN 设备联机
- PPTP 封包穿透 VPN QOS 安全路由器功能:** 若是选择**激活** 的话, 则允许 PC 端使用 VPN-PPTP 封包穿透 VPN QOS 安全路由器以便与外部 VPN 设备联机。
- L2TP 封包穿透 VPN QOS 安全路由器功能:** 若是选择**激活** 的话, 则允许 PC 端使用 VPN-L2TP 封包穿透 VPN QOS 安全路由器以便与外部 VPN 设备联机。

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

## 5.2. QVM VPN 功能设定

VPN QOS 安全路由器搭配 QVM 系列 VPN QOS 安全路由器提供了三大便利性功能：

1. **SmartLink IPSec VPN:** 简单建立 VPN，取代传统 VPN 建立的复杂缺点，只需要**服务器 IP、用户名及密码**就可以完成。
2. **中央控管功能:** 让所有外点或分公司的 VPN 联机状态清楚且可直接在 VPN QOS 安全路由器中控画面，远程进入外点客户端做设定。
3. **VPN 断线 中功能**



### 5.2.1. QVM 中心服务器端设定

选择 QVM 功能为服务器模式:



- 用户名称:** 需要跟远程客户端名称一致, 请输入远程客户端使用者的名称, 中英文皆可
- 密码:/再次输入密码:** 需要跟远程客户端密码一致, 请输入使用者密码及再次确认使用者密码
- IP 地址/子网掩码:** 此为 VPN QOS 安全路由器内部哪一个网段 IP 地址以及子网掩码, 需要跟远程客户端做 QVM 联机
- VPN Hub 功能:** 分点与总部连通后, 可以让分点之间实现互联互通, 不用再去各分点的设备之间建立通道, 方便管理, 更能节省资源。不同运营商电信网通线路可透过总部中央点进行转换, 让联机速度不延迟, 解决跨网 VPN 联机很卡的问题。同时还能结合侠诺专长的带宽管理功能, 让总部的网管人员可以控制不同分支持点间的互相联机, 达到更严密控管的功能。

- 激活:** 启用此帐号
- 添加到对应列表:** 新增输入的帐号与密码
- 删除所选择对应项目:** 删除所选择的使用者

设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

### 5.2.2. QVM 中央控管

用户可以通过点击远程用户的名称登录远程客户端 VPN QOS 安全路由器对远程网络进行相关设定。

**QVM服务器状态**

No.	用户名称	状态	接口位置	启动时间	结束时间	持续时间	控制
1	<a href="#">suntao</a>			---	---	---	请等候
2	<a href="#">Sunny</a>			---	---	---	请等候

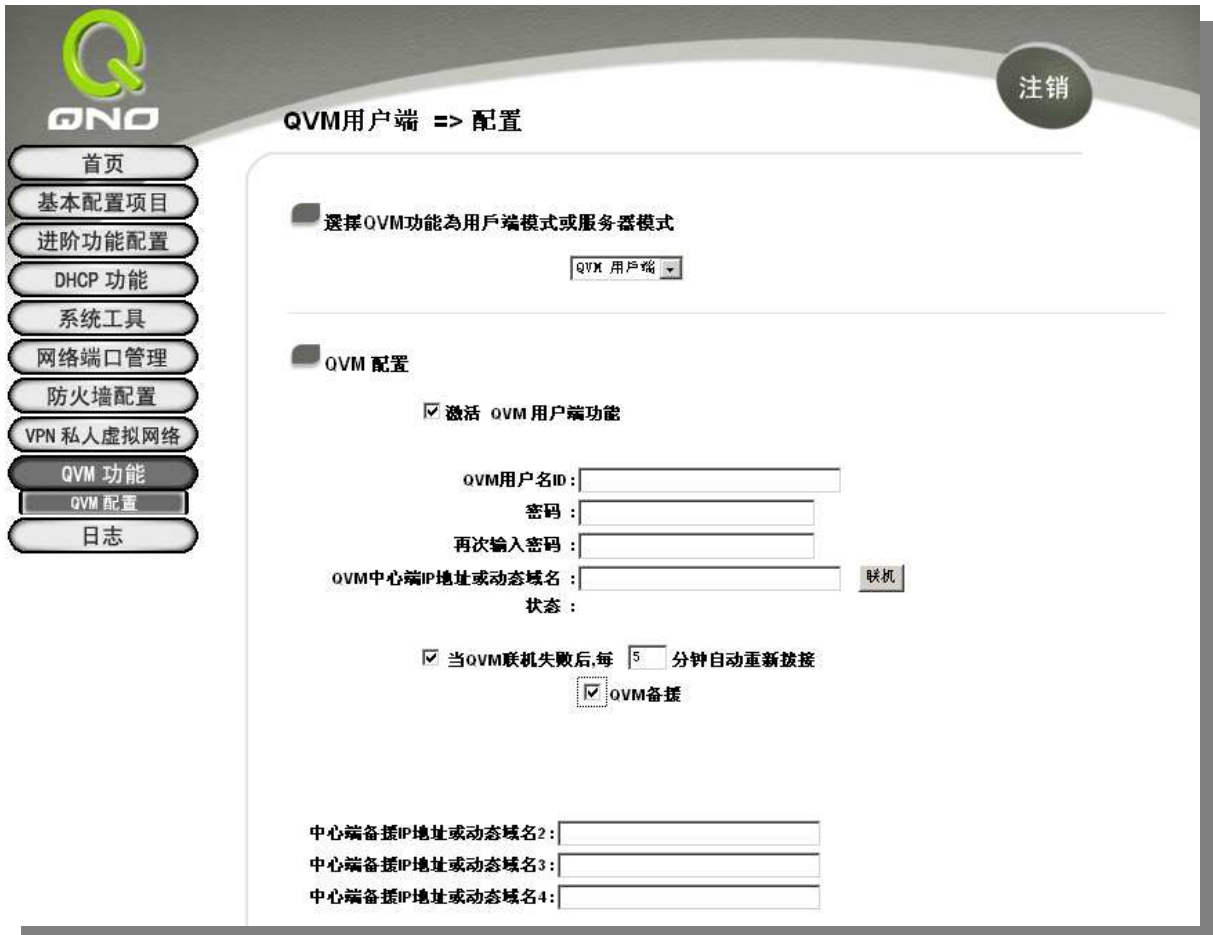
- 用户名称:** 此为用户的外点客户端如 QVM100、QVM330 或者 VPN QOS 安全路由器所显示的用户名称。绿色表示已经连通，蓝色表示等待联机，红色表示此条 QVM 关毕
- 状态:** 此为显示此条 QVM VPN 的联机状态。红色线表示断线，绿色线表示已经连通
- 接口位置:** 此为远程此条 QVM 现在经由 VPN QOS 安全路由器的哪一条 WAN 口进来做 QVM 联机
- 启动时间:** 表示此条 QVM 的起用时间
- 结束时间:** 表示此条 QVM 最后的结束时间
- 持续时间:** 表示此条 QVM 启用至结束的总时间
- 控制:** 表示现在此条 QVM 所处的状态：等待联机-**Waiting**，断开-**Disconnect** 将此条 QVM 断线并关毕-**Disable** 此功能，**激活**开启此条 QVM 至等待联机状态

### 5.2.3. QVM 用户端设定

**选择 QVM 功能为用户端模式:**

选择进行 VPN 连接的 VPN QOS 安全路由器为 **QVM 用户端**。勾选 **激活 QVM 用户端功能** 选项

的话，就开启此功能。



- QVM 用户名 ID:** 输入已在 QVM 服务端 QVM1000 中建立的对应用户 ID
- 密码:** 输入已在 QVM 服务端 QVM1000 中建立的对应密码
- 再次输入确认密码:** 再输入一次确认密码
- 中心端备援 IP 地址或动态域名:** 输入 QVM1000 中心端 IP 地址或是网域名
- 状态:** 在此字段可以看到 QVM 功能联机状态
- 当 QVM 联机失败后, 每 ( ) 分钟自动重新连接** 此功能为 QVM 联机断开后, 重新检测连接的间隔时间。时间范围为 1~60 分钟
- QVM 备援:** 若是勾选此选项, QVM 备援功能将被开启。您可以输入最多三个备援连接 IP 或是网域名
- 中心端备援 IP 地址或动态域名:** 输入对 VPN QOS 安全路由器中心端备援连接的 IP 或是网域名, 一旦断线可从中心服务端 VPN QOS 安全路由器的另一个 WAN



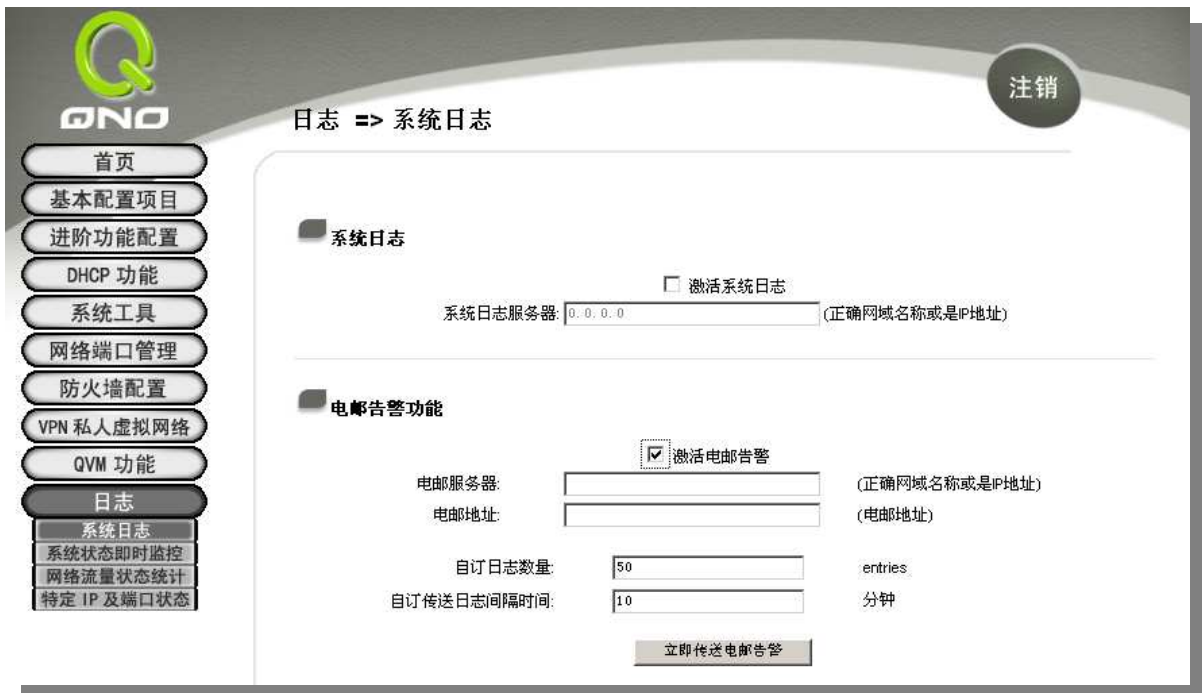
端口自动建立 VPN 联机，确保 VPN 服务永不断线，保证数据传输的安全

设定修改完成请按下 **“确定”** 按钮储存网络设定变更或是按下 **“取消”** 按钮不做任何设定变更。

## 6. 日志

通过对日志的管理和查找我们可以了解到 VPN QOS 安全路由器的相关工作情况更方便我们来设定操作 VPN QOS 安全路由器。

### 6.1. 系统日志



VPN QOS 安全路由器系统日志(System Log)提供三种功能项目，分别为- 系统日志 Syslog，电邮告警 E-mail 以及系统日志设定 Log Setting。

#### 系统日志

**激活系统日志:** 若是此选项勾选的话，系统日志功能将被开启。

**系统日志服务:** VPN QOS 安全路由器 提供了外部系统日志服务器收集系统信息功能。系统日志为一项工业标准通讯协议，于网络上动态撷取有关的系统信息。VPN QOS 安全路由器的系统日志提供了包含动作中的联机来源 IP 地址与目的地 IP 地址，服务编号以及类型，若要使用此功能，请输入系统日志服务器名称或是 IP 地

址于”系统日志服务器”的空格字段内。

设定修改完成请按下“确定”按钮储存网络设定变更或是按下“取消”按钮不做任何设定变更。

### 电邮告警 (E-mail)

- 激活电邮警告:** 若是此选项勾选的话，电子邮件告警将会被开启
- 电邮服务器:** 若您希望所有的日志电子邮件都可以寄出的话，请于此输入电子邮件服务器的名称或是 IP 地址，如：mail.abc.com
- 电邮地址:** 此为设定日志收件人电子邮件信箱，如：abc@mail.abc.com
- 自定义日志数量:** 自定义日志数量，系统默认为 50 个 entries。当到达此数量时，VPN QOS 安全路由器 将会自动传送-Mail 日志
- 自定义传送日志时间间隔:** 自定义传送日志间隔时间，系统默认为 10 分钟。当到达此时间时，VPN QOS 安全路由器 将会自动传送-Mail 此日志
- VPN QOS 安全路由器 将会自动判别当 entries 数量或是间隔时间哪一个参数先到达，就传送邮件日志讯息给用户
- 立即传送点邮告警:** 使用用户可以实时直接按下此按钮传送日志

### 系统日志设定

**系统日志配置**

**告警日志**

Syn Flooding       IP Spoofing       Win Nuke

Ping Of Death       登入认证错误

**一般日志**

系统错误信息       被阻挡的管制条例       允许通过的管制条例

系统配置变更       认证登入

### 选择需要告警的内容

VPN QOS 安全路由器 提供了包含以下的告警内容讯息，您只要打勾点选即可。Syn Flooding, IP

Spoofing, Win Nuke, Ping of Death / 登录人证 3 错误。

- Syn Flooding:** 即在短时间内传送大量的 syn packet, 造成系统记录联机的内存溢满。
- IP Spoofing:** 骇客通过封包监听程序来拦截网络上所传送资料, 并在读取后利用程序修改原发送端地址, 进入原目的端的系统内, 存取资源。
- Win Nuke:** 通过侵入或设陷阱的方式将木马程序送入对方服务器中。
- Ping of Death:** 通过传送来产生超过 IP 协议所能够允许的最大封包, 造成系统当机。
- 登录认证错误:** 当系统发现有企图进入 VPN QOS 安全路由器的入侵者时, 就会将讯息传到系统日志中。

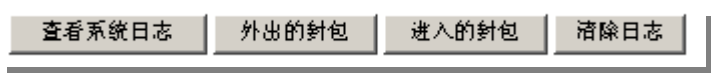
### 一般系统信息

VPN QOS 安全路由器 提供了包含以下的一般告警内容讯息, 您只要打勾点选即可。系统错误讯息, 被阻挡的管制条例, 允许通过的管制条例, 系统配置变更, 登录认证。

- 系统错误讯息:** 提供系统中各种错误讯息给系统日志。如:不正确的设定, 功能异常状况发生, system 重启, PPPoE 断线等等
- 被阻挡的管制条例:** 当远程使用者因为存取规则而无法进入系统, 此信息会传送到系统日志中
- 允许通过的管制条例:** 当远程使用者因为符合存取规则进入系统, 此信息会传送到系统日志中
- 系统配置变更:** 当系统的设定改变时, 此信息回传送到系统日志中
- 认证登录:** 每一个成功进入系统如:从远程进入或从LAN端Login进入此台VPN QOS安全路由器的信息都会传送到系统日志中

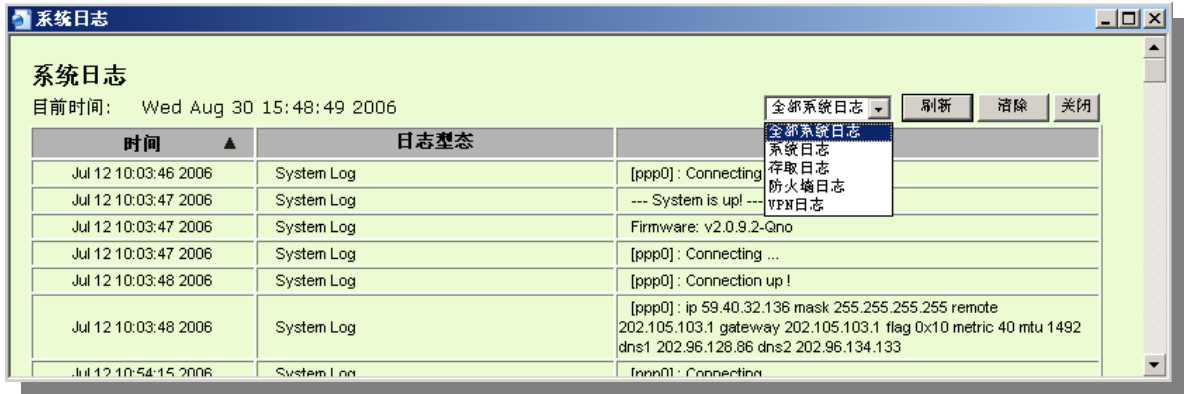
设定修改完成请按下“**确定**”按钮储存网络设定变更或是按下“**取消**”按钮不做任何设定变更。

以下有四个有关线上查询 Log 的按钮, 分别叙述如下:



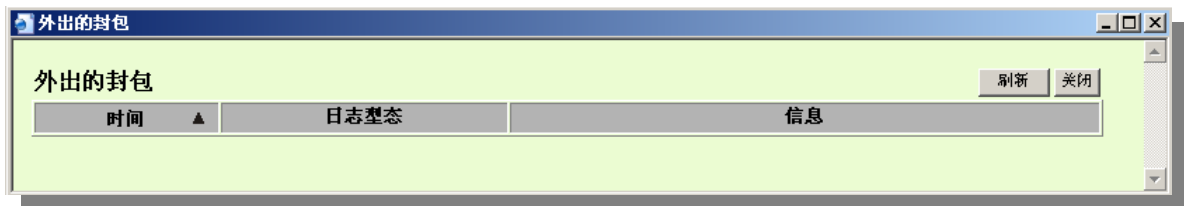
### 查看系统日志:

此为查看系统日志使用, 其信息内容分别可以于 VPN QOS 安全路由器线上读取, 包含全部系统日志, 系统日志, 存取日志, 防火墙日志以及 VPN 日志。如下图所示:



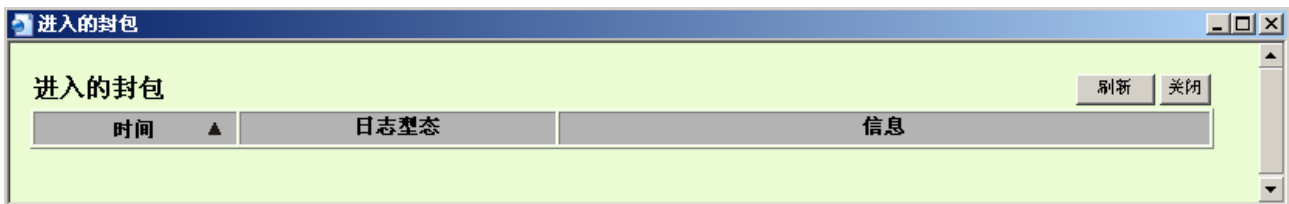
### 外出的封包:

查看内部 PC 出 Internet 的系统封包日志，此日志内涵内部网络地址(LAN IP)，目的地址以及所使用的通讯服务端口类型等信息。如下图所示:



### 进入的封包:

查看外部进入 VPN QOS 安全路由器的系统封包日志，此日志内含外部来源网络 IP 地址，目的地位置与通讯端口号等信息。如下图所示:



### 清除日志:

此按钮为清除所有目前 VPN QOS 安全路由器的日志相关信息。



## 6.2. 系统状态实时监控



日志 => 系统状态实时监控

注销

下一页 >>

接口位置	广域网1接口	广域网2接口	广域网3接口	广域网4接口
机器名称	ixp1	ixp2	ixp3	ixp4
目前端口连线状态	联机	关闭	关闭	关闭
IP地址	220.130.189.10	0.0.0.0	0.0.0.0	0.0.0.0
网络实体位置	00-17-16-00-c6-88	00-17-16-00-c6-89	00-17-16-00-c6-8a	00-17-16-00-c6-8b
子网掩码	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0
预设网关	220.130.189.254	0.0.0.0	0.0.0.0	0.0.0.0
域名解析服务器地址	168.95.1.1 0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
线路侦测机制	测试成功	测试失败	测试失败	测试失败
收到的封包数量	46386	0	0	0
传送的封包数量	41237	0	0	0
全部的封包数量	87623	0	0	0
统计收到的封包Byte数量	5186459	0	0	0
统计传送的封包Byte数量	18935612	0	0	0
统计全部的封包Byte数量	24122071	0	0	0
接收Bytes/秒	2286	0	0	0
传送Bytes/秒	1578	0	0	0
统计收到的错误封包统计	1	0	0	0
端口丢弃的封包统计	83	0	0	0
联机数	10	0	0	0
新联机数/秒	0	0	0	0
上传带宽使用率(%)	0	0	0	0
下载带宽使用率(%)	0	0	0	0

刷新

VPN QOS 安全路由器的系统状态实时监控管理功能可以提供系统目前运作信息，包含：接口位置，机器名称，目前 WAN 端联机状态，IP 地址，网络实体地址，子网掩码，默认网关，网域名称服务器，收到的封包数)，传送的封包数量，全部的封包数量统计，统计收到的封包 Byte 数量，统计传送的封包 Byte 数量，统计全部的封包 Byte 数量，接收 Bytes/秒，传送 Bytes/秒，统计收到的错误封包统计，端口丢弃的封包统计，联机数，新联机数/秒，上传带宽使用率(%)，下载带宽使用率(%)。

### 6.3. 网络流量状态显示

有六种信息会显示在流量统计的网页里，来提供网管对于流量有更好的管理与控制。



#### 对内流量来源位置 IP 地址:

在此图表中显示了来源端的 IP 地址，每秒有多少 byte 与百分比。



#### 对外流量来源位置 IP 地址:

在此图表中显示了来源端的 IP 地址，每秒有多少 byte 与百分比。

网络流量显示状态：

Source IP	bytes/sec	%
220.130.189.10	33	100

#### 对内流量 IP 服务端口号:

在此图表中显示了网络的协议的种类，目的端 IP 地址，每秒有多少 byte 与百分比。

网络流量显示状态：

Protocol	Dest. Port	bytes/sec	%
----------	------------	-----------	---

#### 对外流量 IP 服务端口号:

在此图表中显示了网络的协议的种类，目的端 IP 地址，每秒有多少 byte 与百分比。

网络流量显示状态：

Protocol	Dest. Port	bytes/sec	%
TCP	3376	4	50

#### 对内流量 IP 联机数:

在此图表中显示了来源端的 IP 地址，网络的协议的种类，来源端的端口，目的端 IP 地址，目的端的端口，每秒有多少 byte 与百分比。

网络流量显示状态：

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
-----------	----------	-------------	----------	------------	-----------	---

#### 对外流量 IP 联机数:

此图表中显示了来源端的 IP 地址，网络的协议的种类，来源端的端口，目的端 IP 地址，目的端的端口，每秒有多少 byte 与百分比。

网络流量显示状态：

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
-----------	----------	-------------	----------	------------	-----------	---

## 6.4. 特定 IP 及端口状态

VPN QOS 安全路由器提供网管人员可以针对某一 IP 或某一特定端口去查询此 IP 去访问过的目的地址，或是有哪些用户（来源 IP）使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走 Multi-WAN 而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做协议绑定来解决此登录问题，如在封特定端口软件的时候查询此特定端口软件服务器的 IP 地址可以用到此功能。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择端口做使用者查询。



日志 => 特定IP地址/端口状态

特定IP地址/端口状态： 端口：

来源IP地址	通讯协议	来源端口	接口位置(WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
218.18.57.111	TCP	3385	WAN1	220.130.189.10	80	0	0
218.18.57.111	TCP	3386	WAN1	220.130.189.10	80	0	0

### 特定 IP 状态:

直接在 IP 地址里填入您想要查询的 IP 地址,就可以显示出此 IP 对外联机的所有目的地 IP 及端口数。

特定IP地址/端口状态: IP地址:  .  .  .

来源IP地址	通讯协议	来源端口	接口位置(WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
192.168.1.100	TCP	1051	WAN1	207.46.0.80	1863	36	4
192.168.1.100	TCP	1674	WAN1	61.129.48.125	80	0	0
192.168.1.100	TCP	1688	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1689	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1690	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1691	WAN1	218.17.247.119	80	0	0
192.168.1.100	TCP	1696	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1697	WAN1	218.17.247.119	80	0	0
192.168.1.100	TCP	1711	WAN1	202.108.15.42	80	4	4
192.168.1.100	TCP	1712	WAN1	61.129.48.125	80	0	0
192.168.1.100	TCP	1717	WAN1	220.181.28.42	80	0	0

### 特定端口状态:

直接在端口字段里填入您想要查询的服务端口号,就可以显示出此端口现在有哪些 IP 正在使用。

特定IP地址/端口状态: 端口:

来源IP地址	通讯协议	来源端口	接口位置(WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
192.168.1.100	TCP	1688	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1689	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1690	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1691	WAN1	218.17.247.119	80	0	0
192.168.1.100	TCP	1696	WAN1	61.177.95.25	80	0	0
192.168.1.100	TCP	1712	WAN1	61.129.48.125	80	0	0
192.168.1.100	TCP	1737	WAN1	61.129.48.125	80	0	0

## 7. 注销



VPN QOS 安全路由器的网页画面右上方有一个**注销**的按钮，此按钮为终止管理 VPN QOS 安全路由器并注销此管理画面，若您下次想再进入 VPN QOS 安全路由器管理画面时，用户得重新打开 Web 浏览器输入 IP 地址确认后再输入管理验证使用名称与密码登录管理页面。

## 附录一：产品中有毒有害物质或元素表

部件名称	有毒有害物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯 醚(PBDE)
PCBA	X	O	O	O	O	O
<p>O：表示该有毒有害物质在部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。</p> <p>X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。</p> <p>1. 电阻内部导通部位为导电银糊剂(含有铅玻璃料)</p> <p>2. Diode 本体有采用含有铅玻璃料</p>						

## 附录二: VPN Configuration Sample

### 1. Sample VPN Environment 1: Gateway to Gateway



Firewall Setting: Firewall → General → Block WAN Request = Disable

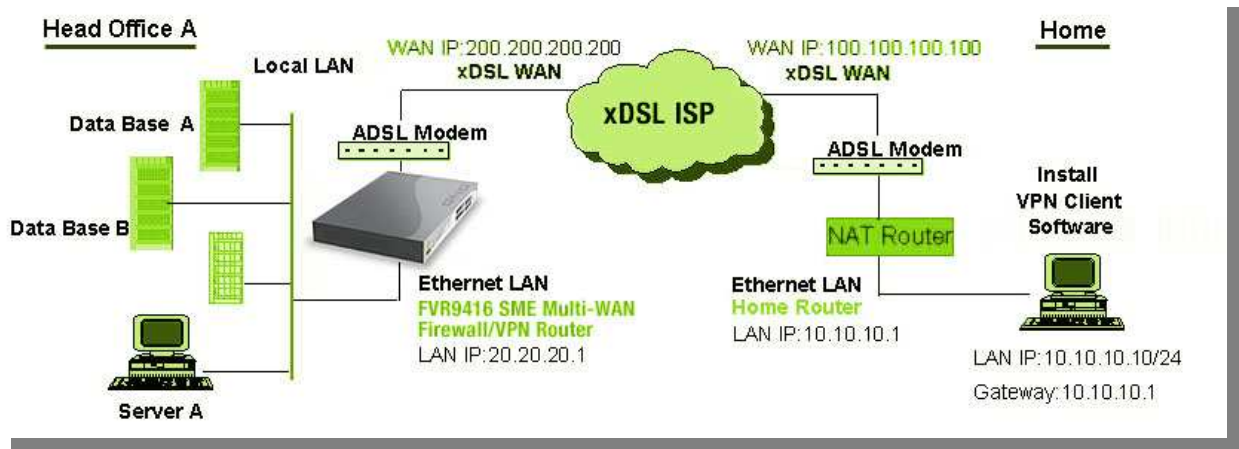
VPN Setting: VPN → Summary → Add New Tunnel → Gateway to Gateway

VPN QOS 安全路由器 VPN Configuration for	Head Office A	Head Office B
Tunnel Name	HOB	HOA
Interface	WAN1	WAN
激活	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type → IP 地址	20.20.20.0	10.10.10.0
Local Security Group Type → Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	IP	IP
Remote Security Gateway Type → IP 地址	100.100.100.100	200.200.200.200
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type → IP 地址	10.10.10.0	20.20.20.0
Remote Security Group Type → Subnet Mask	255.255.255.0	255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28, 800 Seconds	28, 800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1



Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key.	

## 2. Sample VPN Environment 2: Gateway to Gateway

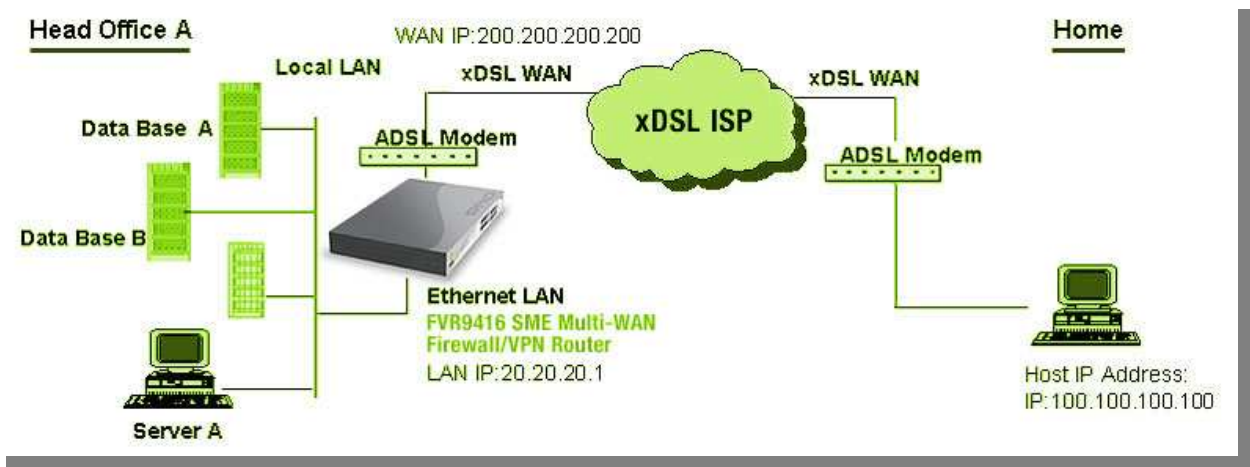


VPN Setting: VPN → Summary → Add New Tunnel → Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
激活	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type → IP 地址	20.20.20.0	10.10.10.10
Local Security Group Type → Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type → Domain Name	Company domain Name	
Local ID → Domain Name		Company domain Name
Remote Security Gateway Type → IP 地址	100.100.100.100	200.200.200.200
Remote Security Group Type	IP	Subnet
Remote Security Group Type → IP 地址	10.10.10.10	20.20.20.0
Remote Security Group Type → Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28, 800 Seconds	28, 800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1

Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

### 3. Sample VPN Environment 3: Client to Gateway (Tunnel)

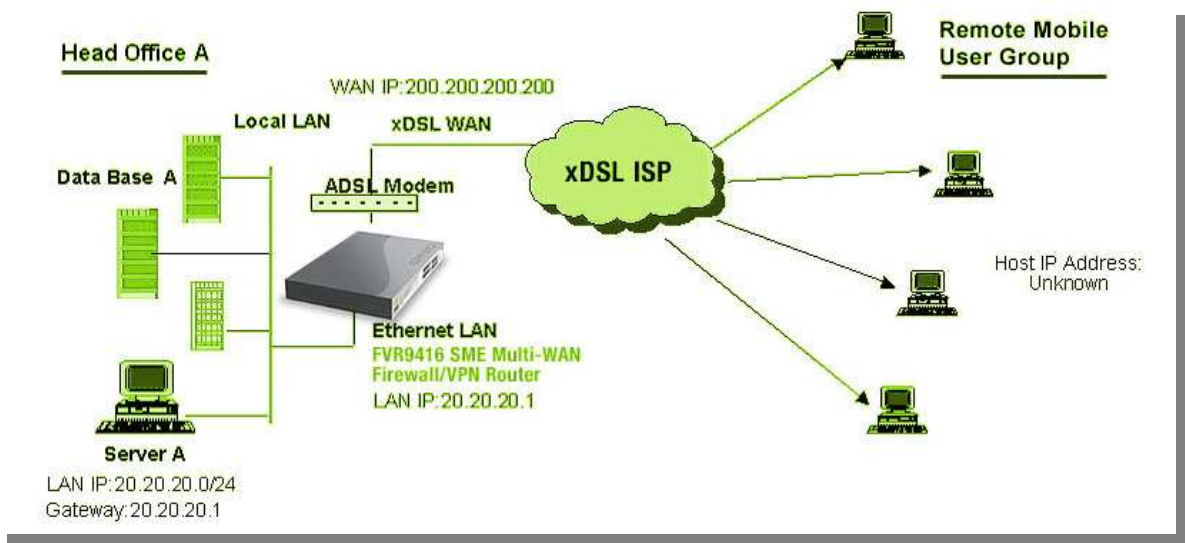


VPN Setting: VPN→Summary→Add New Tunnel→Client to Gateway→Tunnel

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
激活	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type→ IP 地址	20.20.20.0	100.100.100.100
Local Security Group Type→ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type→IP 地址		200.200.200.200
Remote Client	Email Address	
Remote Client→ Email Address	User Email Address	
Local ID→ Email Address		User Email Address
Remote Client→ IP 地址	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type→ IP 地址		20.20.20.0
Remote Security Group Type→ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28, 800 Seconds	28, 800 Seconds
Perfect Forward Secrecy	Checked	Checked

Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

#### 4. Sample VPN Environment 4: Client to Gateway (GroupVPN)



VPN Setting: VPN → Summary → Add New Tunnel → Client to Gateway → Group VPN

	Head Office A	HomeN (VPN Client SW)
Group Name/Tunnel Name	GroupVPN1	HOA
Interface	WAN1	WAN
激活	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type → IP 地址	20.20.20.0	Client IP 地址
Local Security Group Type → Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type → IP 地址		200.200.200.200
Remote Client	Domain Name	
Remote Client → Email Address	Company Domain Name	
Local ID → Email Address		Company Domain Name
Remote Security Group Type		Subnet
Remote Security Group Type → IP 地址		20.20.20.0
Remote Security Group Type → Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES



Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28, 800 Seconds	28, 800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	
Advanced	Aggressive Mode	

Note: All Clients can sign up into one Group VPN simultaneously

## 附录三：常见问题解决

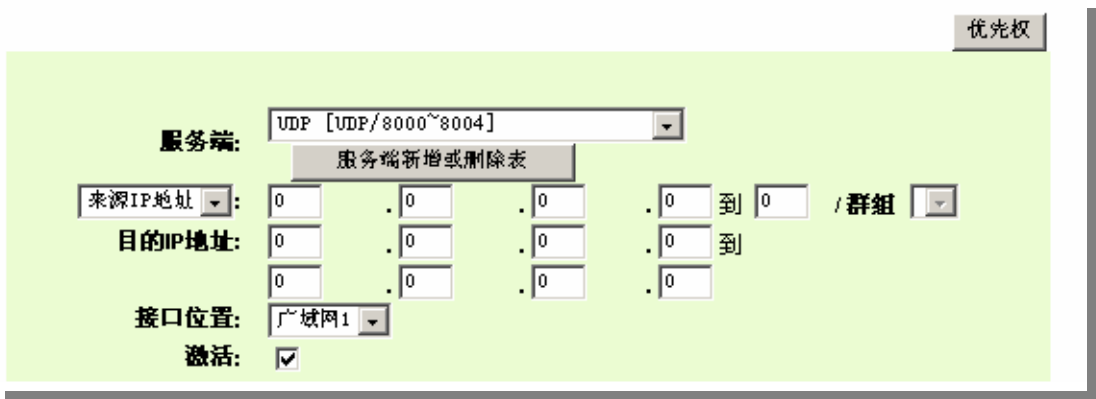
### 注意！

以下是几个常见问题的解决方法，如果有其它的问题出现可以在<http://www.qno.cn> 讨论区查找信息以及联系技术服务人员，具体方法可以参考附录五：Qno 技术支持资讯查找相关信息以及联系相关技术服务人员，以取得更详细的资料参考。

### (1) QQ 容易掉线问题

a). 检查 QQ 版本是否为 2006 版，经过 QQ 官方确认使用珊瑚版或是传美版掉线严重。

b). 2 条以上的线路，必须作协议绑定，让 QQ 走固定广域网，绑定 QQ(UDP8000~8004)走固定的广域网如下图协议绑定设置：



c). 保证带宽给 QQ 端口，依照网吧内部实际带宽评估 QoS 所需要设定的最小值与最大值，下图为 10M 光纤保证给 QQ 的方式，上下传都必须设定。

状态:  带宽控制  优先级

接口位置:  广域网1  广域网2  广域网3  广域网4

服务端: UDP [UDP/8000~8004] 服务端新增或删除表

IP地址: 0 . 0 . 0 . 0 到 0 . 0 . 0 . 0

群组:

目的: 上传

最小带宽: 200 Kbit/sec 最大带宽: 2000 Kbit/sec

带宽共享方式:  此范围IP地址共享此设定带宽.  
 此范围每一IP地址最大及最小可使用带宽.

激活:

## (2) 挡基本 BT 下载方式

若您想要封锁 BT 种子下载, 不让用户下载, 您可以直接在“防火墙配置”有一个“网页内容管制设定”选择“开启网页内容管制功能”后将激活网页字符串管制, 打入“.torrent”就可以防止用户下载种子。

## 防火墙配置 => 网页内容管制设定

- 开启网页内容管制功能  
 开启只允许可以访问的网页管制

- 激活域名过滤功能  
 激活网页字符串管制

### 网页字符串管制

字符串

新增:

更新字符串

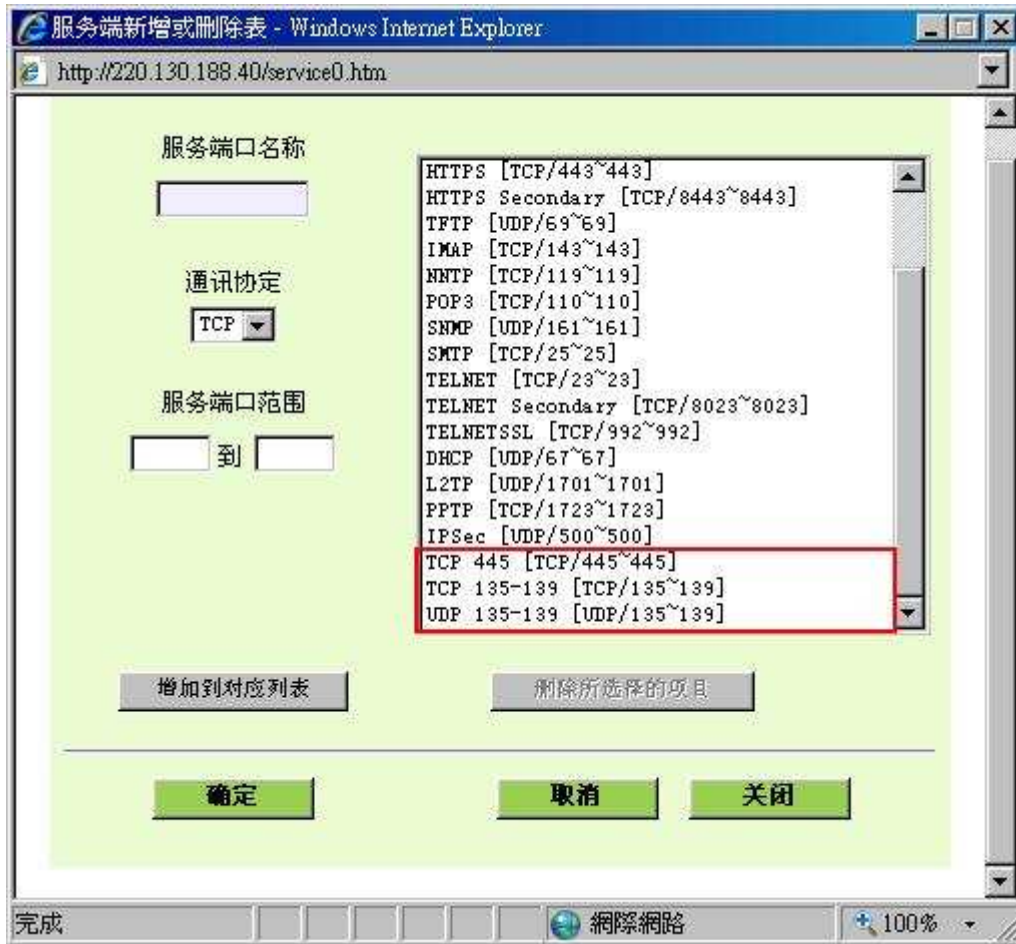
.torrent
----------

删除所选择的内容      新增

### (3) 冲击波及蠕虫病毒的防制

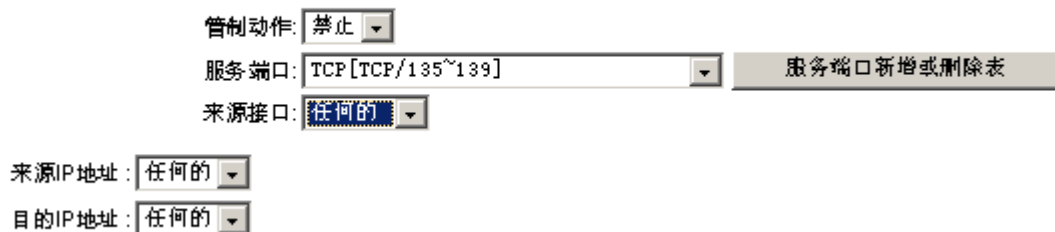
由于近来还是发生有许多用户内网中冲击波及蠕虫病毒造成内网访问 Internet 很慢及联机数 (Session) 大量增加造成 VPN QoS 安全路由器大量处理, 所以以下为指导您封锁这些病毒相应端口以达到防制目的。

- a. 增加此 TCP135-139, UDP135-139 还有 TCP445 端口:



b. 用防火墙里面的“存取规则”功能将设定好的此三组端口封锁:

### 存取服务规则设定



用同样的方法添加好 UDP [UDP135~139] 以及 TCP [445~445] 端口。

c. 将这三组的优先级至于最高:





#### (4) 阻止 QQLive 视频直播设定

QQLive 视频直播软件是一种流媒体点播软件，最近好多客户都在头痛一个同样的问题，当内网有多个用户使用 QQLive 视频直播软件，占用了比较大的带宽，造成 VPN QOS 安全路由器的负担过重，使得 VPN QOS 安全路由器反应迟钝或瘫痪，如果我们能够封锁 QQLive 的服务器登录过程就可以解决这样的问题，下面就这个问题来联系 Qno 产品的相关功能提出相关的解决方案，来如何配置 VPN QOS 安全路由器。

- a). 进入 VPN QOS 安全路由器 Web 管理页面，再进入“防火墙配置”的“访问存取规则设定”。

### 存取服务规则设定

管制动作:

服务器端口:

日志:

接口位置:

来源IP地址:

目的IP地址:

### 时间管制设定

管制时间为  :  :  到  :  :  (时间表示:24小时制)

每天  周日  周一  周二  周三  周四  周五  周六

b). 再点击“增加新的管制规则”，进入“访问存取规则设定”页面，在“存取服务规则设定”中的“管制动作”选项中选择“禁止”，再在“服务器端口”选择“所有端口[TCP&UDP/1~65535]”，选择“来源接口”为“任何的”，“来源 IP 地址”选择“任何的”（有相关需求的用户可以选择“单独”或“范围”阻止单个 IP 或者一段 IP 的 QQLive 的的登录），再在“目的 IP 地址”选择“单独”填入 QQLive 服务器的 IP 地址“121.14.75.115”（QQLive 服务器的 IP 地址不止一个，后面需要重复添加），最后在“时间管制设定”的“此存取规则”选择“全部”对上 QQLive 的登录时间进行设置（如有需要可以具体设置相关时间的设定），“确定”后进入下一步骤。

c). 重复以上的操作在只替换「目的 IP 地址」里分别填入以下 IP 地址：

121.14.75.115

60.28.234.117

60.28.235.119

222.28.155.17

可封锁的 QQ Live 版本：QQ Live 2008 (7.0.4017.0)

测试日期:2008-07-29

重复添加后可以看到相关 QQ Live 的服务器的连接被封锁，点击确认完成对阻止 QQ Live 视频直播设定

## (5) ARP 病毒攻击防制

### 1) . ARP 问题的提出以及相关知识

近期，国内多家网吧出现短时间内断线(全断或部分断)的现象，但会在很短的时间内会自动恢复。这是因为 MAC 地址冲突引起的，当带毒机器的 MAC 映射到主机或者 VPN QoS 安全路由器之类的 NAT 设备，那么全网断线，如果只映射到网内其它机器，则只有这部分机器出问题。多发于传奇游戏特别是私服务外挂等方面。此类情况就是网络受到了 ARP 病毒攻击的明显表现，其目的在于，该病毒破解游戏加密解密算法，通过截取局域网中的数据包，然后分析游戏通讯协议的方法截获用户的信息。运行这个病毒，就可以获得整个局域网中游戏玩家的详细信息，盗取用户帐号信息。下面我们谈谈如何防制这种攻击。

首先，我们了解下**什么是 ARP**，ARP “Address Resolution Protocol”（地址解析协议），局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

**ARP 协议的工作原理：**在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的，如表所示。

IP 址	MAC 地址
192.168.1.1	00-0f-3d-83-74-28
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	03-aa-01-75-c3-06
.....	.....

我们以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，主机 A 就会在网络上发送一个广播，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：“192.168.1.1 的 MAC 地址是什么？”网络上其它主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时它还更新了自己的 ARP 缓存表。

再者，我们先简单介绍一下什么是 ARP 病毒攻击，这种病毒是对内网的 PC 进行攻击，使内网 PC 机的 ARP 表混乱，在局域网中，通过 ARP 协议来完成 IP 地址转换为第二层物理地址（即 MAC 地址）的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的

ARP 通信量使网络阻塞。用伪造源 MAC 地址发送 ARP 响应包，对 ARP 高速缓存机制的攻击。这些情况主要出现在网吧用户，造成网吧部分机器或全部机器暂时掉线或者不可以上网，在重新启动后可以解决，但保持不了多久又会出现这样的问题，网吧管理员对每台机器使用 arp -a 命令来检查 ARP 表的时候发现 VPN QoS 安全路由器的 IP 和 MAC 被修改，这就是 ARP 病毒攻击的典型症状。

这种病毒的程序如 PWSteal.lemir 或其变种，属于木马程序/蠕虫类病毒，Windows 95/98/Me/NT/2000/XP/2003 将受到影响，病毒攻击的方式对影响网络连接畅通来看有两种，对 VPN QoS 安全路由器的 ARP 表的欺骗和对内网 PC 网关的欺骗，前者是先截获网关数据，再将一系列的错误的内网 MAC 信息不停的发送给 VPN QoS 安全路由器，造成 VPN QoS 安全路由器发出的也是错误的 MAC 地址，造成正常 PC 无法收到信息。后者 ARP 攻击是伪造网关。它先建立一个假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的 VPN QoS 安全路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

就这两种情况而言，如果对 ARP 病毒攻击进行防制的话我们必须得做 VPN QoS 安全路由器方面和客户端双方的设置才保证问题的最终解决。所以我们选择 VPN QoS 安全路由器的话最好看看 VPN QoS 安全路由器是否带有防制 ARP 病毒攻击的功能，Qno 产品正好提供了这样的功能，相比其它产品操作简单易学。

## 2) . ARP 的判断

如过网络中有一台或多台电脑受到或已经感染了 ARP 病毒，我们就必须学会判断并采取相应的解决方法处理类似问题的发生，下面来谈谈 Qno 技术工程师的 ARP 防制经验谈。

通过对 ARP 工作原理得知，如果系统 ARP 缓存表被修改不停的通知 VPN QoS 安全路由器一系列错误的内网 IP 或者干脆伪造一个假的网关进行欺骗的话，网络就肯定会出现大面积的掉线问题，这样的情况就是典型的 ARP 攻击，对遭受 ARP 攻击的判断，其方法很容易，你找到出现问题的电脑点开始运行进入系统的 DOS 操作。ping VPN QoS 安全路由器的 LAN IP 丢包情况。输入 ping 192.168.1.1 (网关 IP 地址)，如图。

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

内网 ping VPN QoS 安全路由器的 LAN IP 丢几个包，然后又连上，这很有可能是中了 ARP 攻击。为了进一步确认，我们可以通过查找 ARP 表来判断。输入 ARP -a 命令，显示如下图。

```
Interface: 192.168.1.72 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1          00-0f-3d-83-74-28    dynamic
192.168.1.43         00-13-d3-ef-b2-0c    dynamic
192.168.1.252        00-0f-3d-83-74-28    dynamic
C:\WINDOWS\System32>arp -a
```

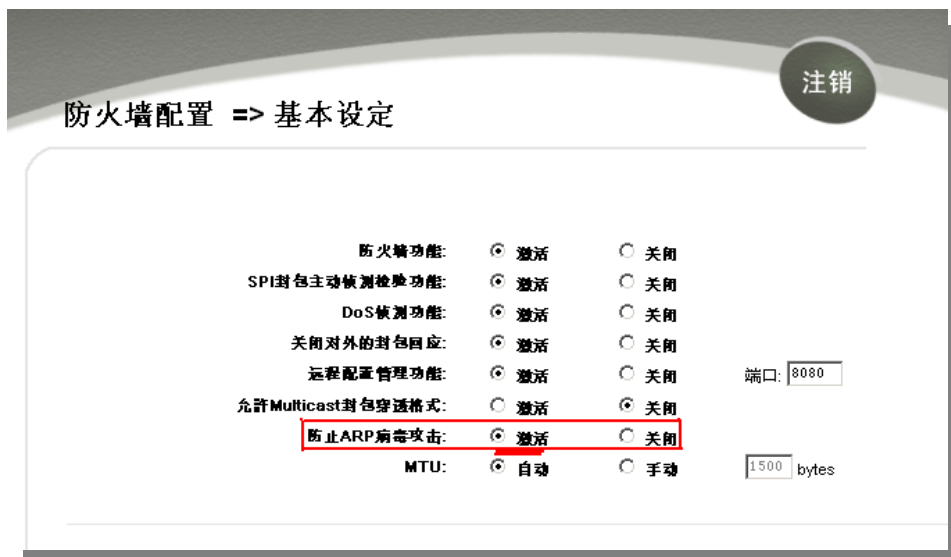
可以看出 192.168.1.1 地址和 192.168.252 地址的 IP 的 MAC 地址都是 00-0f-3d-83-74-28, 很显然, 这就是 ARP 欺骗造成的。

### 3) . ARP 的解决

我们现在已经理解了 ARP, ARP 欺骗攻击以及如何判断此类攻击, 下面的问题就是如何找到行之有效的防制办法来防止这类攻击对网络造成的危害。Qno 的一般处理办法分三个步骤来完成。

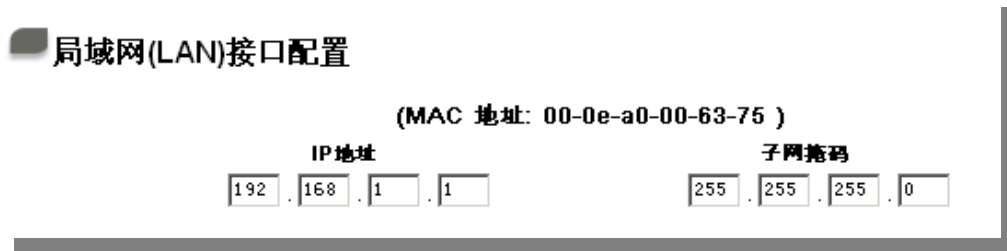
#### a)、激活防止 ARP 病毒攻击:

输入 VPN QOS 安全路由器 IP 地址登录 VPN QOS 安全路由器的 Web 管理页面, 进入“防火墙配置”的“基本页面”, 再在右边找到“防止 ARP 病毒攻击”在这一行的“激活”前面做点选, 再在页面最下点击“确认”, 如图。

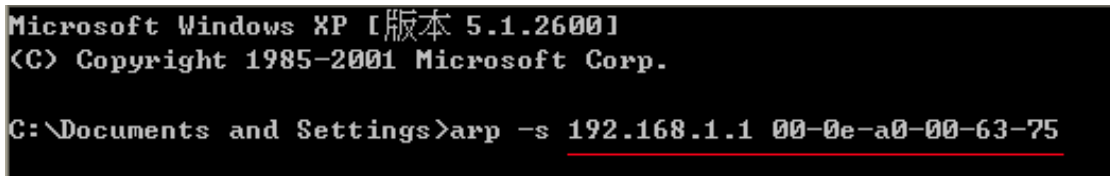


#### b)、对每台 pc 上绑定网关的 IP 和其 MAC 地址

进行这样的操作主要防止 ARP 欺骗网关 IP 和其 MAC 地址首先在 VPN QOS 安全路由器端查找网关 IP 与 MAC 地址，如图。



然后在每台 PC 机上开始/运行 cmd 进入 dos 操作,输入 `arp -s 192.168.1.1 00-0e-a0-00-63-75`. Enter 后完成 pc01 的绑定。如图 7



针对网络内的其它主机用同样的方法输入相应的主机 IP 以及 MAC 地址完成 IP 与 MAC 绑定。但是此动作，如果重起了电脑，作用就会消失，所以可以把此命令做成一个批处理文件，放在操作系统的启动里面，批处理文件可以这样写：

```
@echo off
```

```
arp -d
```

```
arp -sVPN QOS 安全路由器 LAN IP VPN QOS 安全路由器 LAN MAC
```

对于已经中了 arp 攻击的内网，要找到攻击源。方法：在 PC 上不了网或者 ping 丢包的时候，在 DOS 下打 `arp -a` 命令，看显示的网关的 MAC 地址是否和 VPN QOS 安全路由器真实的 MAC 相同。如果不是，则查找这个 MAC 地址所对应的 PC，这台 PC 就是攻击源。

其它的 VPN QOS 安全路由器用户的解决方案也是要在 VPN QOS 安全路由器和 PC 机端进行双向绑定 IP 地址与 MAC 地址来完成相应防制工作的，但在 VPN QOS 安全路由器端和 PC 端对 IP 地址与 MAC 地址的绑定比较复杂，需要查找每台 PC 机的 IP 地址与 MAC 加大了工作量，操作过程中还容易出错。

**c)、在 VPN QOS 安全路由器端绑定用户 IP/MAC 地址：**

进入“DHCP 功能”的“DHCP 配置”，在这个页面的右下可以看到一个“IP 与 MAC 绑定”你可以在此添加 IP 与 MAC 绑定，输入相关参数，在“激活”上点“√”选再“添加到对应列表”，重复操作添加内网里的其它 IP 与 MAC 的绑定，再点页面最下的“确定”。

**IP 与 MAC 绑定**

显示新加入的IP地址

**IP 与 MAC 绑定**

静态IP地址设定: 192 . 168 . 1 . 4

添入IP地址相对应MAC地址: 00 - 0E - 2E - 5B - 42 - 03

名称: PC01

激活:

增加到对应列表

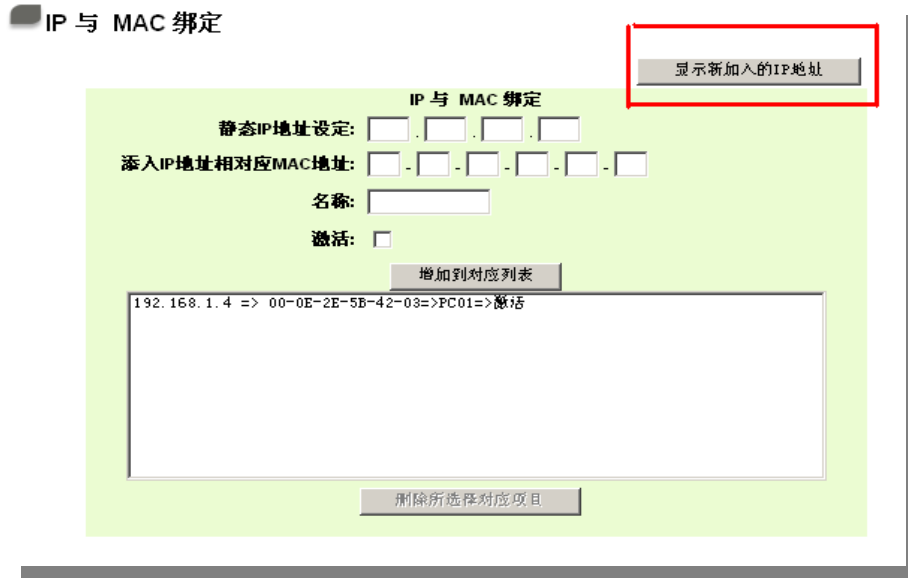
删除所选择对应项目

封锁在对应列表中IP地址错误的MAC地址

封锁不在对应列表中的MAC地址

当添加了对应列表之后，其对应的信息就会在下面的白色框里显示出来。不过建议不采用此方法，这样操作需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，操作会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

进入“DHCP 功能”的“DHCP 配置”找到 IP 与 MAC 绑定右边有一个“显示新加入的 IP 地址”点击进入。

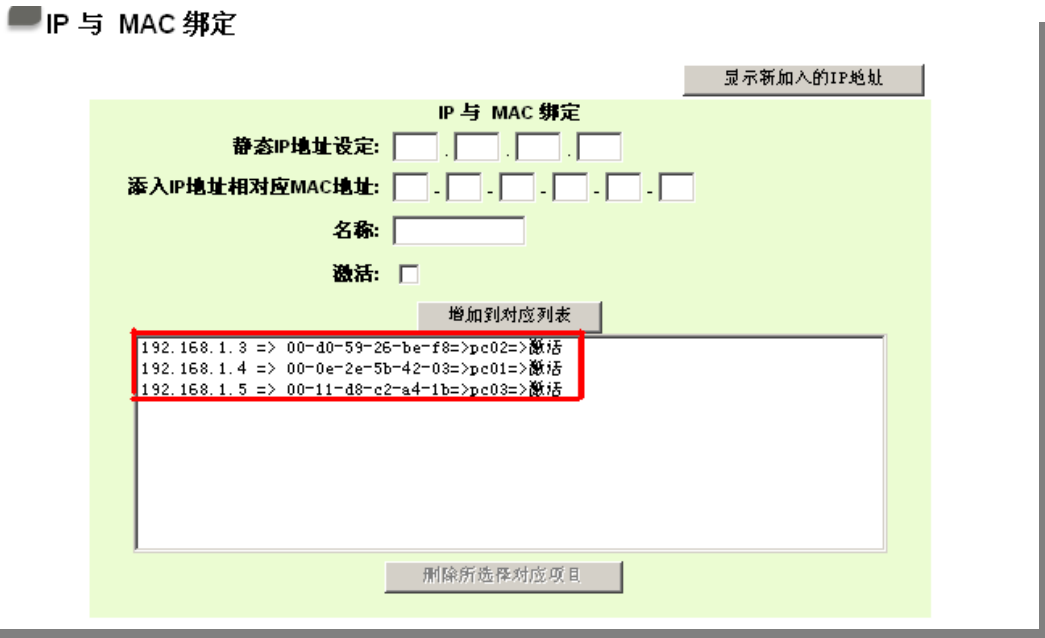


点击之后会弹出 IP 与 MAC 绑定列表对话框，此对话框里会显示网内未做绑定的 pc 的 IP 与 MAC 地址对应情况，输入计算机“名称”和“激活”上“√”选，再在右上角点确定。



此时你所绑定的选项就会出现在 IP 与 MAC 绑定列表框里，如图 5 再点击“确认/Apply”绑定完成。





但是我们单靠这样的操作基本可以解决问题，但 Qno 的技术工程师建议通过进一步通过一些手段来进一步控制 ARP 的攻击。

1、病毒源，对病毒源头的机器进行处理，杀毒或重新装系统。此操作比较重要，解决了 ARP 攻击的源头 PC 机的问题，可以保证内网免受攻击。

2、网吧管理员检查局域网病毒，安装杀毒软件（金山毒霸/瑞星，必须要更新病毒代码），对机器进行病毒扫描。

3、给系统安装补丁程序。通过 Windows Update 安装好系统补丁程序(关键更新、安全更新和 Service Pack)

4、给系统管理员帐户设置足够复杂的强密码，最好能是 12 位以上，字母+数字+符号的组合；也可以禁用/删除一些不使用的帐户

5、经常更新杀毒软件（病毒库），设置允许的可设置为每天定时自动更新。安装并使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版 Windows 用户不能正常安装补丁，不妨通过使用网络防火墙等其它方法来做到一定的防护

6、关闭一些不需要的服务，条件允许的可关闭一些没有必要的共享，也包括 C\$、D\$等管理共享。完全单机的用户也可直接关闭 Server 服务

7、不要随便点击打开 QQ、MSN 等聊天工具上发来的链接信息，不要随便打开或运行陌生、可疑文件和程序，如邮件中的陌生附件，外挂程序等。

#### 4) . 总结

ARP 攻击防制是一个任重而道远的过程，以上方法基本可以解决 ARP 病毒攻击对网络造成相关问题，而且客户采取类似的方法也收到了很大的效果，但还是提醒网落管理人员必须高度重视这个问题，而且不能大意马虎，我们可以采取以上建议随时警惕 ARP 攻击，以减少受到的危害，提高工作效率，降低经济损失。

## 附录四：Qno 技术支持资讯

更多有关侠诺产品技术资讯可以登录侠诺宽带讨论区，以及 FTP 服务器的相关实例，或者联系侠诺各经销商技术部门以及侠诺大陆技术中心联络。

### 网上讨论区及 FTP 服务器：

讨论区：<http://www.Qno.net.cn/forum>

FTP 服务器：[Qnoftp.3322.org](http://Qnoftp.3322.org)

### 各大经销商服务联系方式：

用户可以登录网站先上服务页面查询各大经销联系方法：

[http://www.qno.net.cn/tw/service\\_center.asp](http://www.qno.net.cn/tw/service_center.asp)

### 大陆技术中心：

电话：0755-88839400

电邮：[QnoFAE@qno.com.tw](mailto:QnoFAE@qno.com.tw)