your future life

2WAN / 3LAN VPN QoS 安全路由器

具负载平衡，带宽管理，VPN 与网络安全功能

简体中文使用手册

www.Qno.cn

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，产品功能会按实际机种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

2WAN / 3LAN VPN QoS 安全路由器 ，是一台为小型企业、地区分公司、以及政府学校部门单位等而设计，符合经济实惠且高效能整合的全功能 VPN QOS 安全路由器。具备两个广域网端口，并具有高效能双线路负载平衡模式的功能，以支持 WAN 端的对外联机负载平衡。WAN 端的对外联机能力满足绝大多数宽带市场都适用的规格。第二个广域网端口可选择性作为可设定的硬件 DMZ 端口。内建三个局域网 LAN 端口，每个端口都可以连接额外的交换机以接入更多的上网设备。

VPN QOS 安全路由器产品内建防火墙系统，以满足多数企业对防御外部网络攻击的市场需求。防火墙系统除了 NAT 模式外，还具备防止阻断服务攻击(DoS)，以及封包主动侦测检验技术(SPI)，可以默认自动侦测并阻挡外部网络攻击。

除了宽带接入适用的对外联机能力外，还具备目前企业广泛应用的 VPN 虚拟私有网络硬件加速模式。提供完整 VPN 功能，可同时建立数个 IPSec VPN 隧道联机，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(Aggressive Mode)，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。

VPN QOS 安全路由器产品同时内建有侠诺科技独特的 SmartLink 快速建立 VPN 加密隧道的 QVM 客户端功能，可以与具有 QVM 服务器功能的其它 QVM 系列 VPN QOS 安全路由器快速建立 VPN 联机。

网络地址转换 NAT 除了可以做私网与公网的 IP 转换，让您只需要一个公网 IP 就可以让多人同时连上互联网。此外，包含虚拟服务器等 NAT 应用功能，让网络环境架构具有弹性，易于规划管理。局域网内的 IP 地址支持 Class C 等级。操作系统支持多任务模式，并占用较少内存。

VPN QOS 安全路由器产品具有进阶的存取规则的设定，可让管理者选择应该禁止或开放存取的网络服务，以避免占用网络资源，或是不当使用而遭受潜在的危机。

除了上述的功能之外，VPN QOS 安全路由器产品还具备同级产品所没有的带宽流量与优先权管理，可以让管理者对有限的网络资源做合理而且有效的分配，达成最有效率的运用。这些管理工具容易理解与设定，可让网络管理者对 Internet 存取资源管理有明确的策略。同时，透过在线多样化的日志记录，管理者可以清楚的知道网络活动状况，以此来调整设定，达到更安全且更有效率的网络使用。

2、硬件安装

本章介绍产品的硬件接口以及实体安装。

2.1 VPN QOS 安全路由器 LED 显示灯

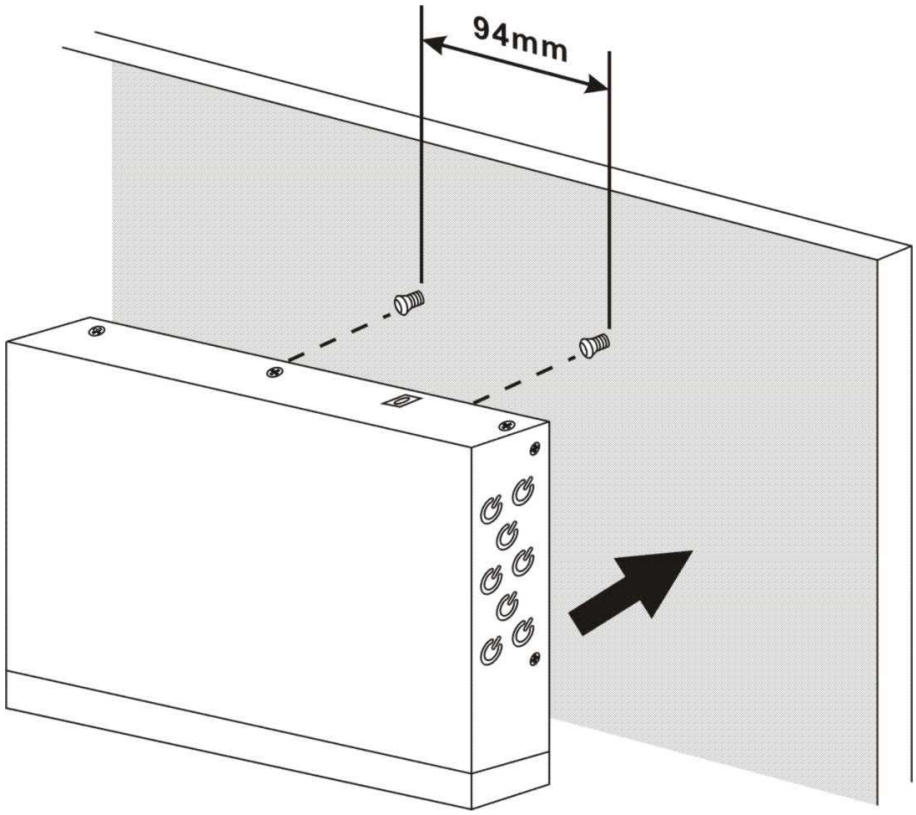
LED Status-面板灯号

LED 灯号	颜色	意义
Power-电源	绿灯	绿灯亮: 电源开启连接
DIAG-自我测试	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
Link/ACT-联机/动作	绿灯	绿灯亮: 以太网络联机正常 绿灯闪烁: 以太网络端口正在传送/接收封包数据传输
100M-速度	绿灯	绿灯亮: 以太网络联机在 100Mbps 的速度 绿灯熄灭: 以太网络联机在 10Mbps 的速度
WAN-广域网络	绿灯	绿灯亮: 指定为广域网络端口 绿灯熄灭: 指定为局域网络端口
Connect-连接	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

硬件恢复 (Reset) 按键

动作	描述
按下 Reset 按钮 5 秒	热开机，重新启动机器 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 DIAG 灯号: 橘色灯号快闪

将 VPN QOS 安全路由器产品安装在墙上

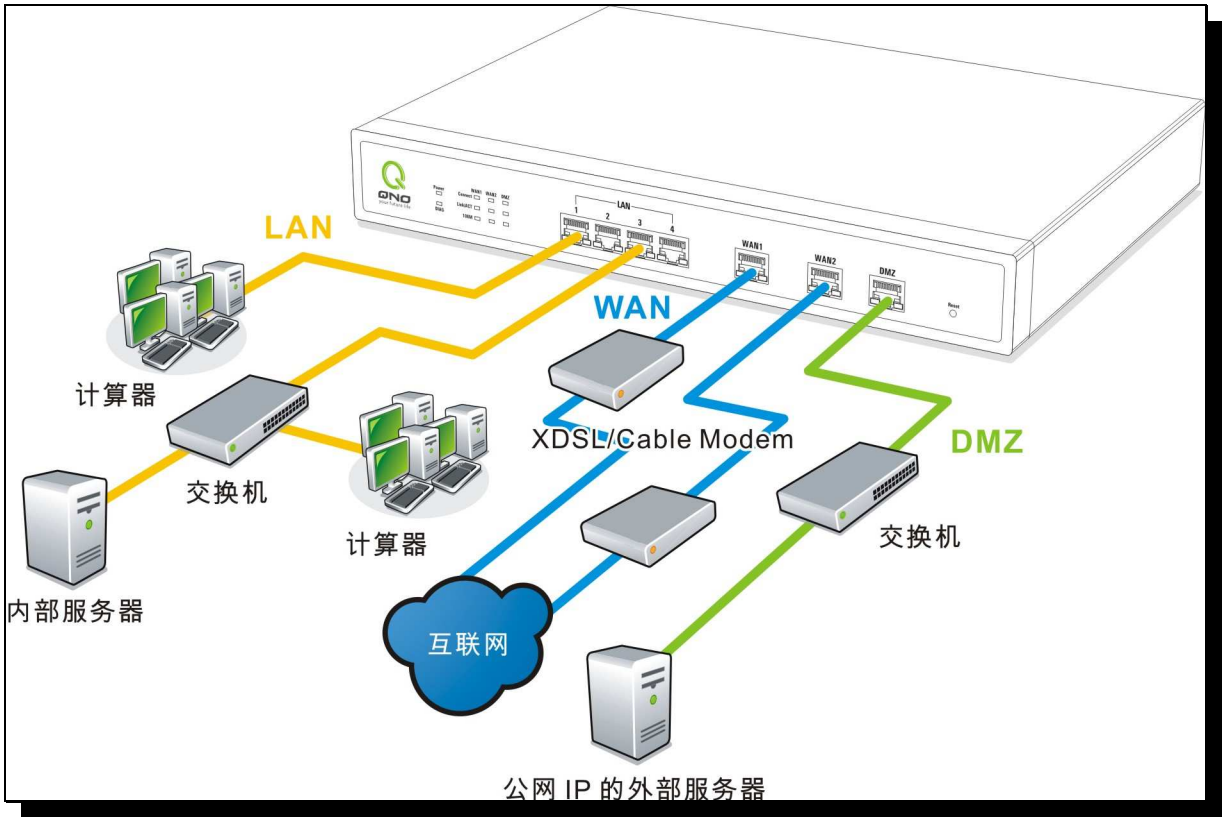


于 VPN QOS 安全路由器机器底部有两个十字孔位，壁挂孔圆心间距为 94mm，您可以使用一般螺丝先旋转锁进墙壁上，确认牢固后，再将产品底部两个十字孔位准确的挂在此二颗螺丝上即可完成安装。

注意：螺丝钉高度请勿突出壁挂孔防静电盖，以避免发生产品损害。

2.2 连接 VPN QOS 安全路由器产品到您的网络上

VPN QOS 安全路由器产品设计了一个可选择作为 WAN2 或是 DMZ 的广域网接口 (此功能是经由软件设定，在下一章节的基本设定中会说明)，各端口的使用拓墣范例如下图：



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。

3、快速连网设定

本章介绍登录软件设定画面，说明首页的显示讯息，以及基本连网设定。

3.1 登录到软件设定画面

在连接到VPN QOS安全路由器LAN端的计算机上开启网页浏览器(如IE)，在网址栏输入192.168.1.1 (VPN QOS 安全路由器的默认网关)，会出现以下的登录画面：

默认的使用户名与密码皆为 “admin”，您可以于稍后设定时更改此登录密码。

注意！

为了安全起见，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至 VPN QOS 安全路由器的设定画面，必须按下面板上的 Reset 按键十秒以上，恢复到出厂值，其所有配置将需要重新设定。

3.2 首页显示

首页显示 VPN QOS 安全路由器目前系统所有参数以及状态显示信息。若您想进一部查询该细部相关设定的话，可以按下各细部选项的超级链接按钮，即可快速立即进入该选项设定当中。

3.2.1 系统讯息

主机器序列号： 显示产品序号

软件版本信息： 显示目前使用的韧体版本

中央处理器（CPU）： 显示使用的 CPU

主机工作时间： 显示目前已经开机的时间

目前正确时间： 显示目前正确时间。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

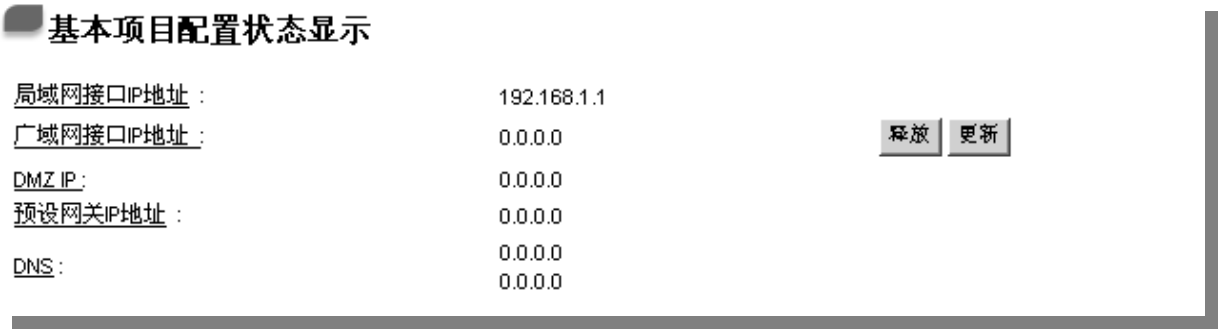
3.2.2 硬件端口-状态实时显示

端口即时状态显示

端口号	1	2	3	Internet	DMZ/Internet
接口位置	局域网			广域网	DMZ
状态	激活	联机	激活	激活	激活

在此画面会显示系统各端口目前实时状态显示 (**联机**-已经连接，**激活**-开启，**关闭**-未开启)。

3.2.3 一般设定状态显示



局域网接口 IP 地址：显示 LAN 端目前 IP 地址，系统默认为 192.168.1.1，可以按下该超级链接直接进入该设定项目中做修改。

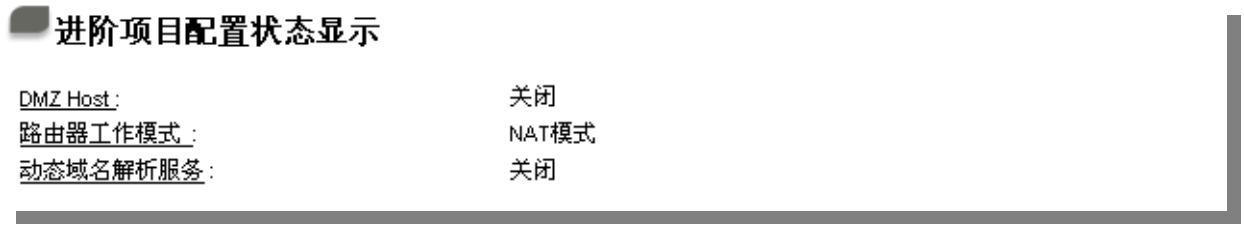
广域网 1 接口 IP 地址(WAN1)：显示 WAN1 端目前的 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。当使用者选择自动取得 IP 地址时，画面上会显示二个按钮分别为**释放**与**更新**。使用者可以按下**释放**按钮去做释放 ISP 端所核发的 IP 地址，以及按下**更新**按钮去做更新 ISP 端所核发的 IP 地址。当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话，它会变为显示**联机**与**中断联机**。

广域网 2 接口 IP 地址(WAN2/DMZ)：显示 WAN2 端或是 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：显示 ISP 分配给 WAN1 及 WAN2 的网关 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。

DNS 域名解析服务地址：显示 DNS 的 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。防火墙防火墙

3.2.4 进阶设定状态显示

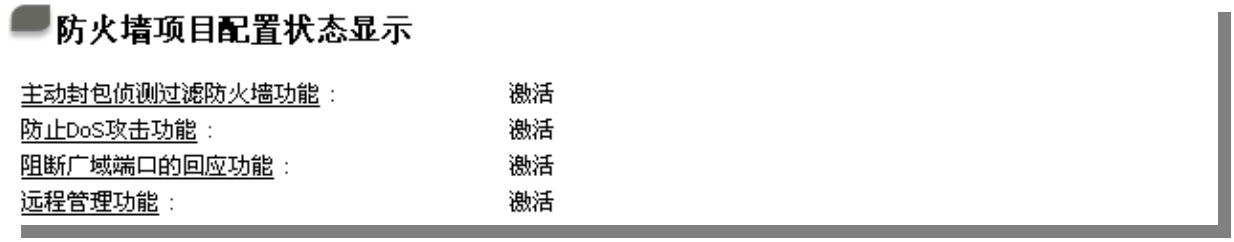


DMZ Host：显示 DMZ 功能选项是否启动，并且可以按下该超级链接直接进入该设定项目中。系统默认此功能为关闭。

VPN QOS 安全路由器工作模式：显示目前工作模式(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)：显示动态 DNS 功能选项是否启动，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 防火墙设定状态显示



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

防止 DoS 攻击功能：此为显示 VPN QOS 安全路由器的阻断来自 Internet 上的 DoS 攻击功能选项是否开启。可以按下该超级链接直接进入该设定项目中。系统默认此功能为激活。

阻断广域端口回应：此为显示 VPN QOS 安全路由器的阻断来自 Internet 上的 ICMP-Ping 的响应功能选项是否开启。可以按下该超级链接直接进入该设定项目中。系统默认此功能为激活。

远程配置管理功能：此为显示 VPN QOS 安全路由器的远程管理功能选项是否启动。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。

3.2.6 VPN 设定状态显示

VPN 状态配置表：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。

3.2.7 日志记录配置状态显示

显示电邮告警功能是否设置。

3.3 基本连网设定

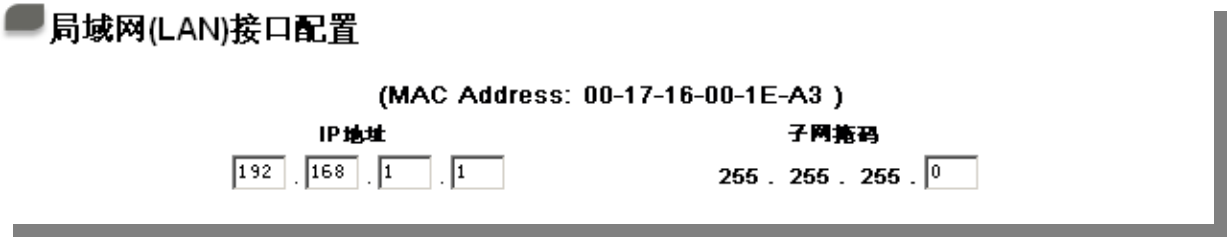
基本连网设定提供基本的网络连接设定内容，对大多数的用户来说，完成基本的设定已经足够连接 Internet 而不需做任何变更。Internet 的连接需要一些 ISP 所提供的进一步详细信息，其详细细部设定，请参考以下各节说明：

3.3.1 基本设定

主机名称及网域名称：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，除非特殊 ISP 需求！

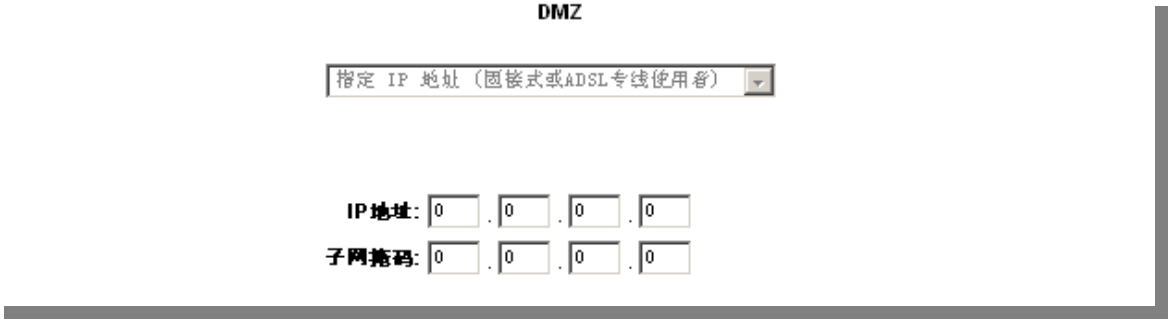
设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

局域网设定：此为设定 VPN QOS 安全路由器的 LAN 端内部网络的 IP 地址，系统默认为 192.168.1.1，子网掩码为 255.255.255.0，VPN QOS 安全路由器局域网 IP 地址可支持 Class C 等级，您可以依照实际网络架构做改动！



第二条 WAN 及非军事区设定：VPN QOS 安全路由器提供可以选择为广域网 WAN2 或是 DMZ 的接口。请先选择要设定为第二条 WAN 或是定义其使用模式为 DMZ 非军事管制区形态，再继续以下的设定。

非军事区(DMZ)：对于某些网络环境应用来说，可能会需要用到独立的 DMZ 非军事管制区接口来置放对外服务器，如 WWW 网页服务器与 Mail 电子邮件服务器等等。VPN QOS 安全路由器提供一个 DMZ 接口来设定连接有合法 IP 地址的服务器，此 DMZ 接口为从 Internet 或从局域网络存取服务器内容的沟通桥梁。



IP 地址： 输入 DMZ 服务器的 IP 地址

子网掩码： 输入 DMZ 服务器的子网掩码

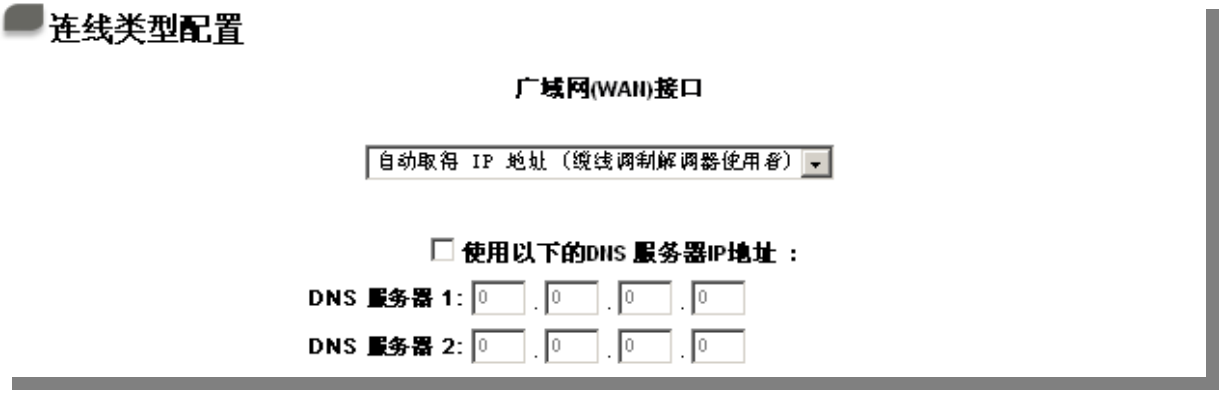
设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

广域网络 Internet 联机形态设定：

自动取得 IP 地址：

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，多为应用于如 Cable Modem 或是 DHCP Client 联机形态等连接，若您的联机为其它不同的方式，请选取相关的设定并依照以下的介绍做设定.

在自动取得 IP 模式，您可以使用自订 DNS 的 IP 地址，于此选项勾选并填入您要使用的 DNS IP 地址。



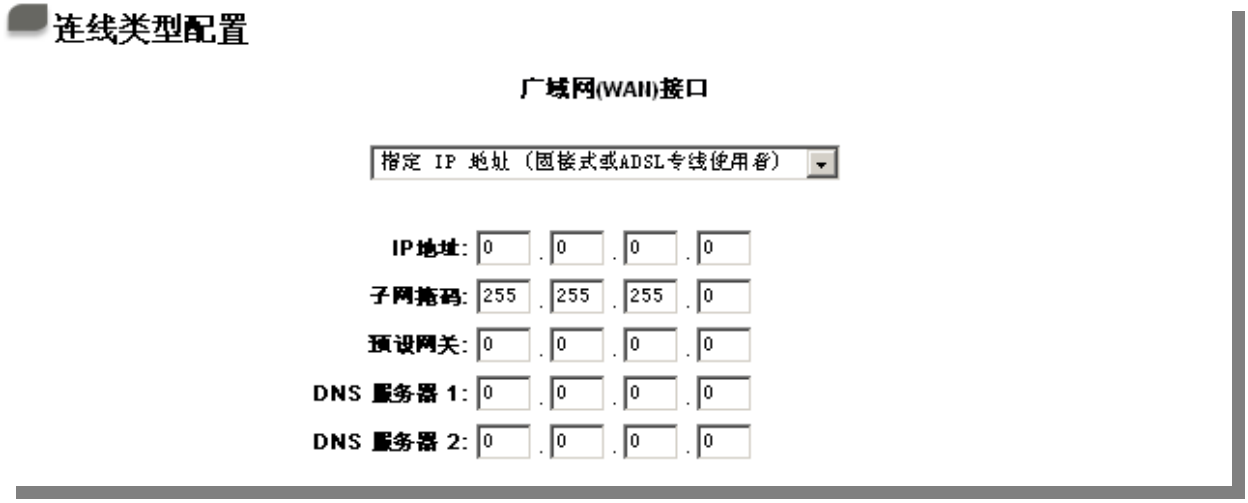
使用以下的 DNS 服务器 IP 地址： 选择使用自订的 DNS 服务器 IP 地址。

DNS 服务器： 输入您的 ISP 所提供的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

固定 IP 地址联机：

若您的 ISP 有核发固定的 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。



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

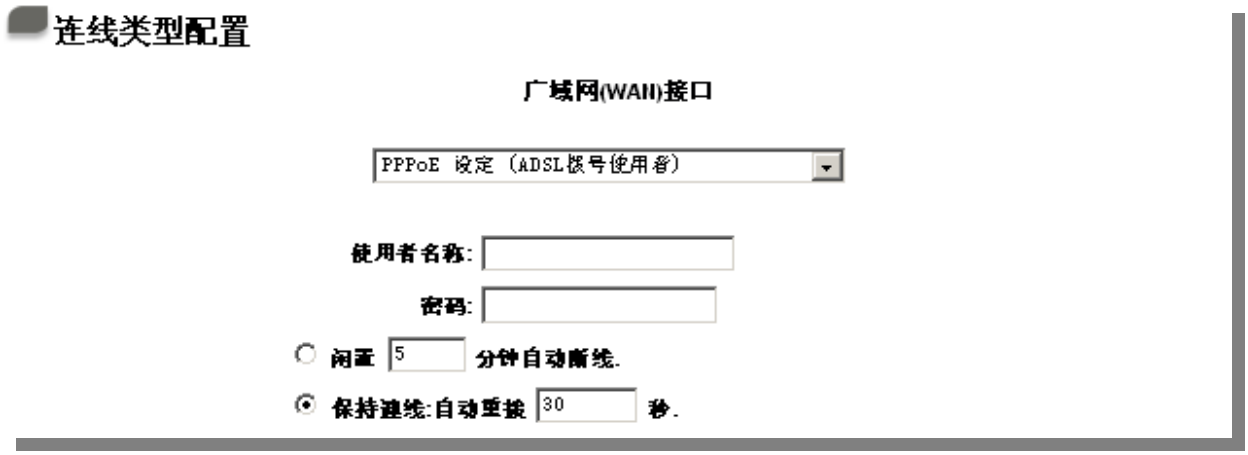
默认网关： 输入您的 ISP 所核发的可使用固定 IP 地址的默认通讯闸，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

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

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

PPPoE 拨号联机：

此项为 ADSL 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 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，不需要再使用此个别连接网络。



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。无封包传送的自动离线时间默认为 5 分钟，您可以自行输入所需要的自动离线等待时间。

保持连线： 此功能能够让您的 PPPoE 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，默认值为 30 秒。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

3.3.2 双 WAN 设定

如果您在“**基本配置项目**”中双广域网/DMZ 模式中选择了双广域网，才可以进行此选项设定。

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。

(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。

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 路由器的 IP 地址，此为 VPN QOS 安全路由器自动填入，所以只需打勾选择是否启用。
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，此远程服务器 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。

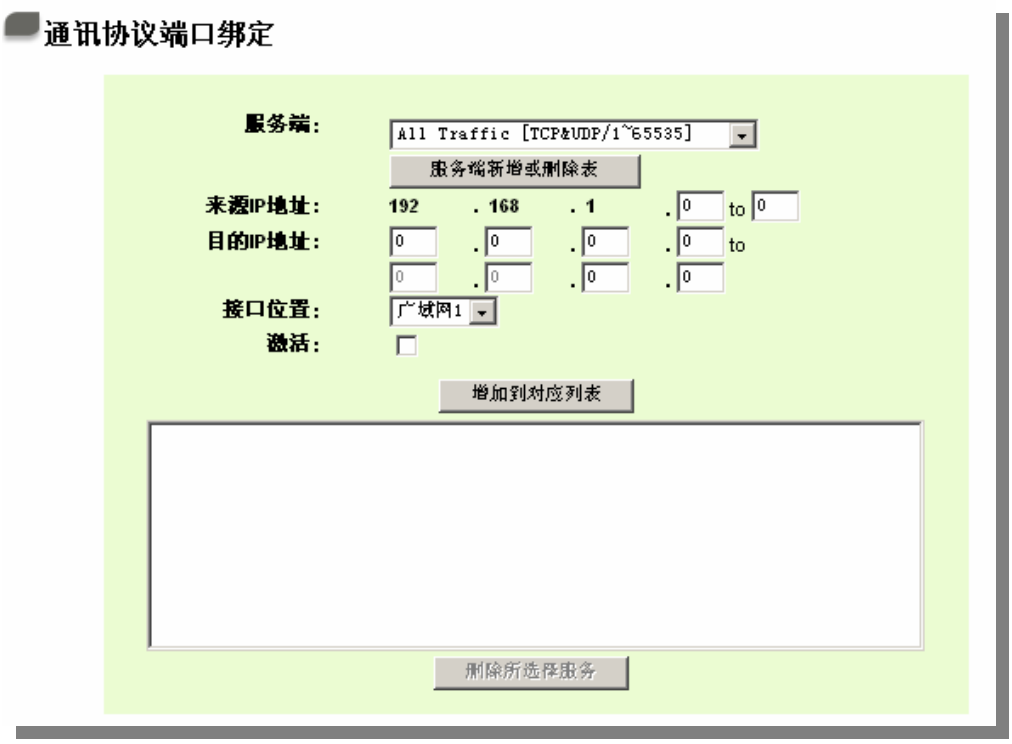
设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

带宽设定

VPN QOS 安全路由器产品会依照您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。所以为了确保您的 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 QoS 设定章节说明。

3.3.3 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 或服务端口还是会进行广域网的负载平衡。



服务端： 在此选择欲开启的绑定服务端口(Service Port)，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。

服务端口管理选单列表：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端口出去。在此填上内部虚拟 IP 地址范围，例如 192.168.1.100~150.则 IP 地址 100~150 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 到 210.11.1.1。如果使用者要设定一个范围的目的地位置，则填入方式可以为 210.11.1.1 到 210.11.255.254，则表示整组 210.11.x.x 的 Class C 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。

接口位置： 选择您所要绑定此条规则在哪一个 WAN 端口。

激活： 启用此规则。

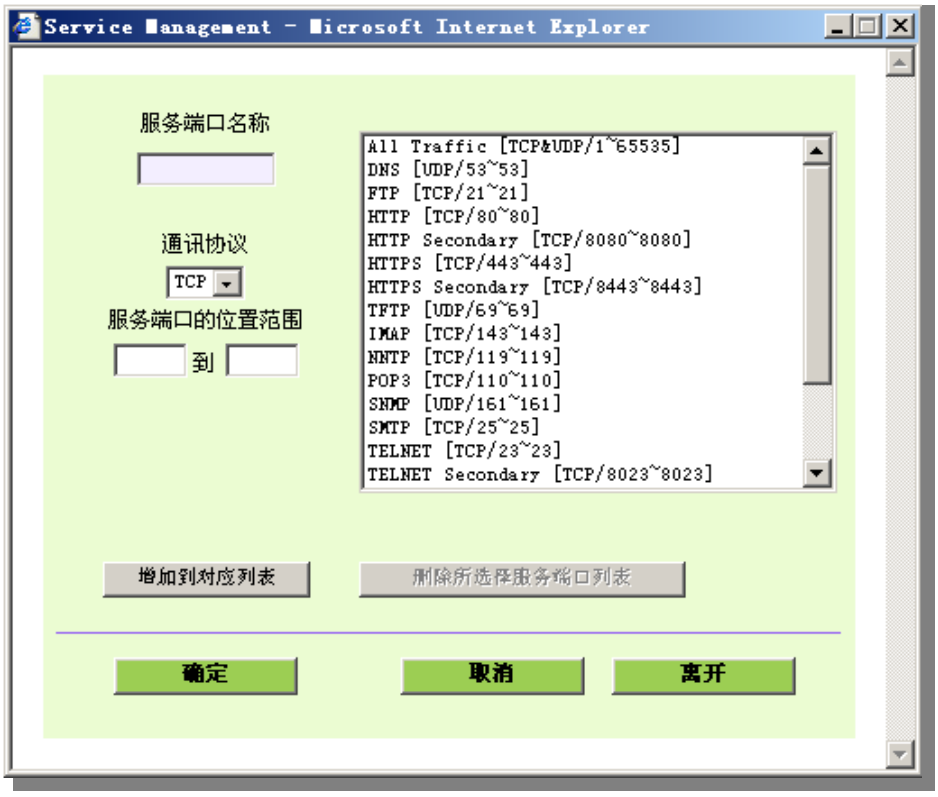
增加到对应列表： 增加此条规则到列表。

删除所选服务： 删除在服务列表里所选择的规则。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

新增或删除管理服务端口

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



服务端口名称： 在此自订欲开启的服务端号名称加入列表中，如 BT 等。

通讯协议：	在此选择欲开启的服务端号的封包格式为 TCP 或 UDP。
服务端口的位置范围：	将您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”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，但是必须于确定储存动作之前才会有效。
离开：	离开此功能设定画面。

3.3.4 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。

带宽设定

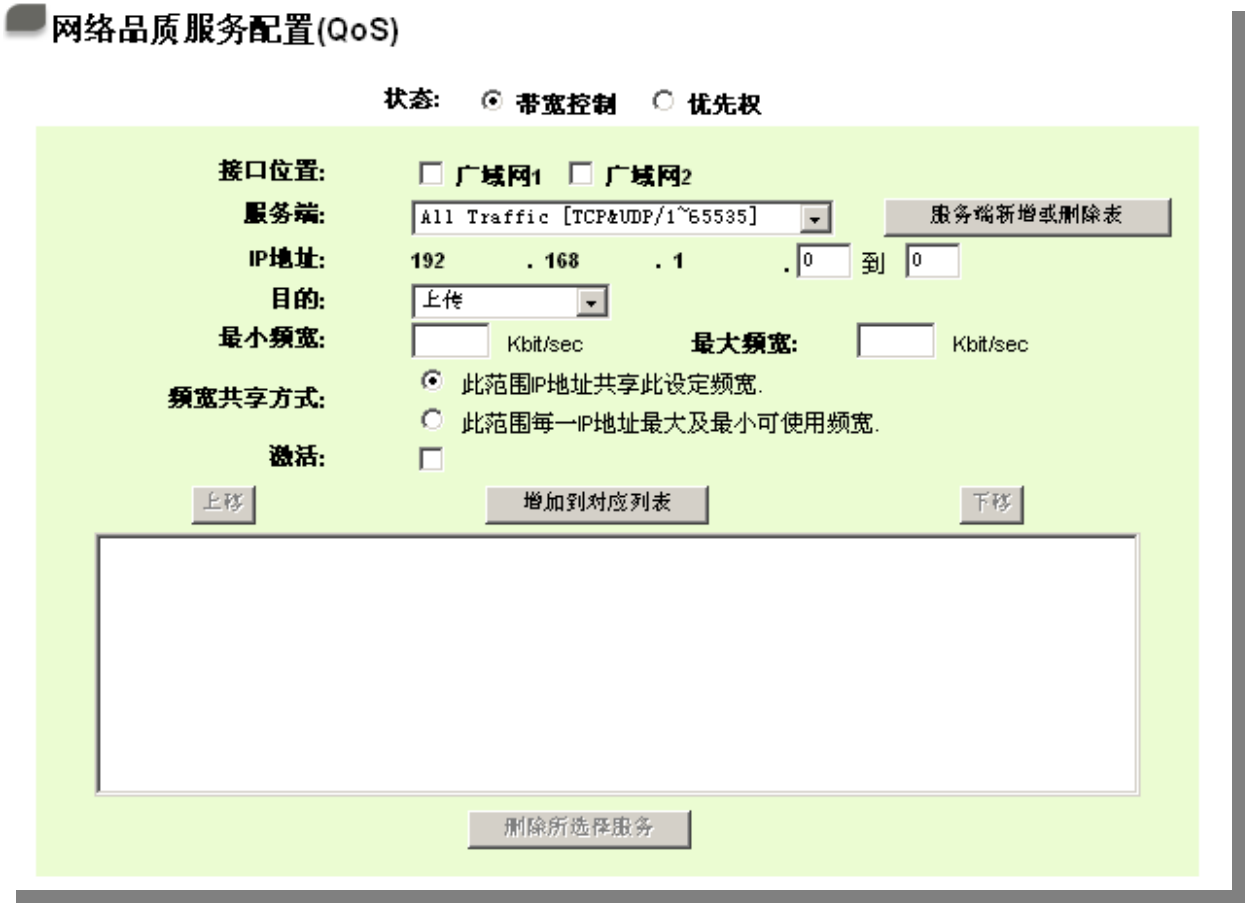
WAN1 及 WAN2 的带宽数据请填入您所申请的宽带网络实际上传及下载带宽，QoS 的带宽控制会依照您所填入的带宽作为计算依据。例如说每个 IP 及服务端口可以保障使用的上传或下载的最小带宽会依照此 WAN1 及 WAN2 的实际带宽相加来换算实际可保障的大小。例如上传带宽若两条都为 512Kbit/Sec，那实际上传带宽就为 WAN1+WAN2=1024Kbit/Sec，所以若有 50 个 IP 在内部网络，若要保证每人最小可使用的上传带宽，则就把 1024Kbit/50=20Kbit，这样每人可以保证的最小带宽就可以填 20kbit/Sec，下载同此换算方式。**注意：**这里的数值单位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

QoS 设定

QoS 可以选择两种方式，无法同时使用，一为流量控制(Rate Control)，另一个为优先权控制(Priority Control)，设定人员可以依照自己内网需求做两种模式灵活运用。

带宽控制-依使用量做管理：

网管人员可依照您现有的带宽大小做每一个 IP 或一段 IP 做使用量限制或保障带宽。另外也可以针对服务端口(Service Port)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。



接口位置： 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： 此为选择您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：192.168.1.100~100，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 192.168.1.100~150 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 192.168.1.0~0，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 C 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：若您有架设对外的服务器网站在 VPN QOS 安全路由器内部，则此选项为控制外部访问此服务器的带宽控制

虚拟服务器下载：若您有架设网站在 VPN QOS 安全路由器产品内网，则此选项为控制外部对此 Server 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 共享这段带宽范围。

此范围每一 IP 地址有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，所以您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服务端口移至最下方如 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设定的规则，并可直接按下**编辑**做修改。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

优先权-依优先级做管理：

优先级顾名思义就是可以将您选定想要的服务做先后顺序的调配，也就是可以直接选择服务端口将其优先级做一分配。

VPN QOS 安全路由器产品会将带宽做 60%(最高)，10%(最低) 的带宽分配，也就是若您将 Port 80 选择为**高级**，那么只要遇到 Port 80 的封包就会给予 60%的带宽出去，若您将 FTP Port 21 设定为**最低**，那当有人使用 Port 21 时，只会给它 10%的带宽使用，其余未做分配的应用服务就使用 30%带宽。

接口位置： 勾选此条优先权的设定要控制在哪条 WAN 执行。

服务端： 在此选择此条优先权所要设定的服务端口为何，要针对譬如 FTP 上传或下载，则选择 FTP Port21~21，可参考服务号码默认列表。

目的： 上传：指针对此服务端口的上传做优先权控制。
下载：指针对此服务端口的下载做优先权控制。

优先权： 高级：此为保证 60%的带宽给此服务端口使用。
低级：此为只给 10%的带宽给此服务端口使用。

激活： 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： 删除所选择在服务列表里的项目内容。

显示开启服务： 可以显示出您所有在优先权设定的规则，并可直接按下**编辑**做修改。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

3.3.5 密码设定

当您每次登录至 VPN QOS 安全路由器产品的设定画面时，必须输入密码。密码出厂值为“**admin**”。为了安全起见，我们强烈建议您务必在第一次登录并完成设定之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至 VPN QOS 安全路由器的设定画面，必须恢复到出厂值。

使用者名称： 默认为 admin 。

密码： 填写原本旧密码。

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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

3.3.6 系统时间设定

VPN QOS 安全路由器产品可以设定时间，让您在看系统记录或是设置网络存取的时间设定时，可以了解事件发生的正确时间，以及作为关闭存取或是开放存取 Internet 资源的依据条件。您可以选择与 VPN QOS 安全路由器产品内建的外部时间服务器取得时间同步，或是自己设定正确时间参数。

设定自动与网络上的 NTP 服务器同步时间：VPN QOS 安全路由器产品内建网络时间服务器，会自动同步时间。

设手动输入日期时间参数：与此输入正确的时间。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4、进阶功能设定

本章介绍 VPN QOS 安全路由器进阶功能的设定，包括开启虚拟服务器的连接，路由设定，实体 IP 与虚拟 IP 对应，以及设置动态域名解析等功能。

4.1 DMZ 服务器地址配置

当您将 VPN QOS 安全路由器产品内部的某台 PC 的虚拟 IP 填入到此 DMZ 选项时，VPN QOS 安全路由器 WAN1 及 WAN2 的合法 IP 地址会直接对应给此台 PC 使用，也就是说从 WAN 端进来的封包，若是不属于内部的任何一台 PC，都会传送到这台 PC 上。

于使用 “DMZ Host” 功能后，若您要取消此功能必须于在设定虚拟 IP 地址地方填入“0” 的参数，才会停止此功能使用。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4.2 虚拟服务器设定

若是您在内网需架设服务器（意指对外部的服务主机 WEB，FTP，Mail 等），这个功能可将虚拟服务器主机视为一虚拟的位置，利用外部合法 IP 地址，经过服务端口的转换，（如 WWW 为 Port 80），直接存取到内部虚拟 IP 的服务器的服务。例如在设定画面中，选项填入服务器位置，如 192.168.1.2 且端口是 80 的话，当 Internet 外部要进来存取这个网页时只要键入：

如：http://220.130.188.45 (假设此为 VPN QOS 安全路由器产品外部合法 IP 地址)

此时，就会透过 VPN QOS 安全路由器产品的公网 IP 地址去转换到 192.168.1.2 的虚拟主机上的 Port

80 读取网页了。

其它种类的服务器设定，都如以上设定；只要将所用的服务的服务端口以及虚拟主机的 IP 地址填入即可！

服务端口号： 在此选择欲开启的虚拟服务器的服务端口号。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！

IP 地址： 在此填上虚拟服务器所要相对应的内部虚拟 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： 若您所需要的服务端口没有在列表里面，可以利用此功能新增或删除管理服务端号列表。

增加对应列表： 增加到开启服务项目内容。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

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 **服务端口新增或删除表** 新增或删除管理服务端口号列表功能达到，如以下所述：

服务端口名称： 在此自订欲开启的服务端号名称加入列表中，如 BT 等。

通讯协议： 在此选择欲开启的服务端号的封包格式为 TCP 或 UDP。

服务端口的位置范围： 将您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”确定”即会储存刚才所变动的修改设定内容参数。

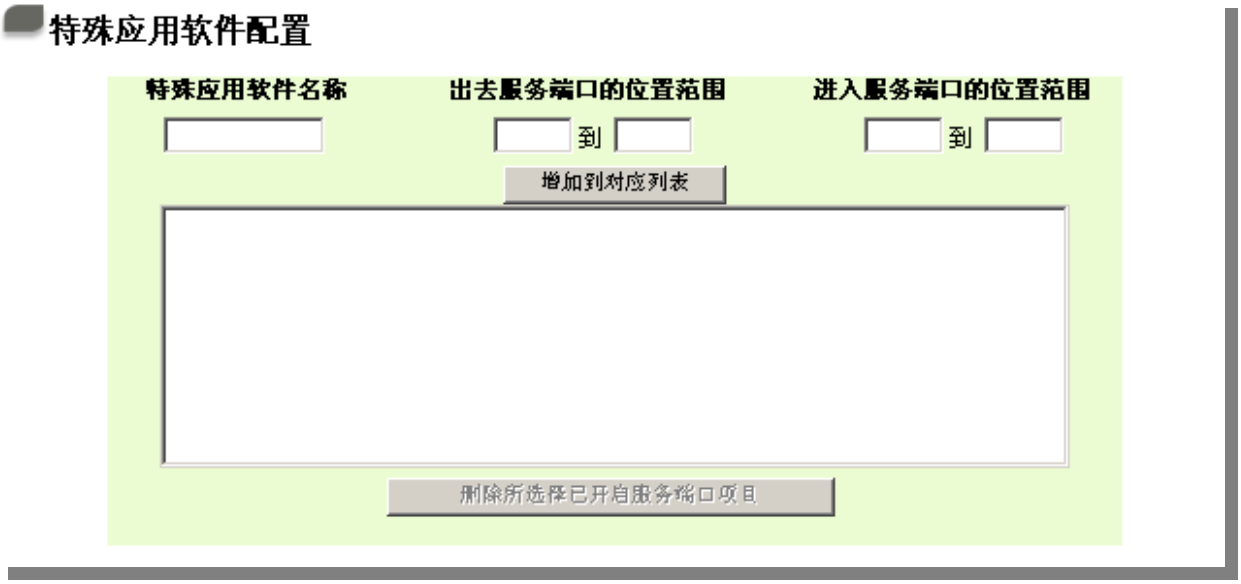
取消： 按下此按钮”取消”即会清除刚才所变动的修改设定内容参数，但是必须于

确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 (Port Triggering)：

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



特殊应用软件名称： 您可以自订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： 输入使用端口编号(如 9000~10000)

进入服务端口的位置范围： 输入使用端口编号. (如 2004~2005)

增加到对应列表： 增加到开启服务项目内容列表

删除所选已开启服务端口项目： 删除所选择的开启服务项目之一笔内容

显示开启表： 按下此按钮即会显示 Table 上的所有设定项目内容参数

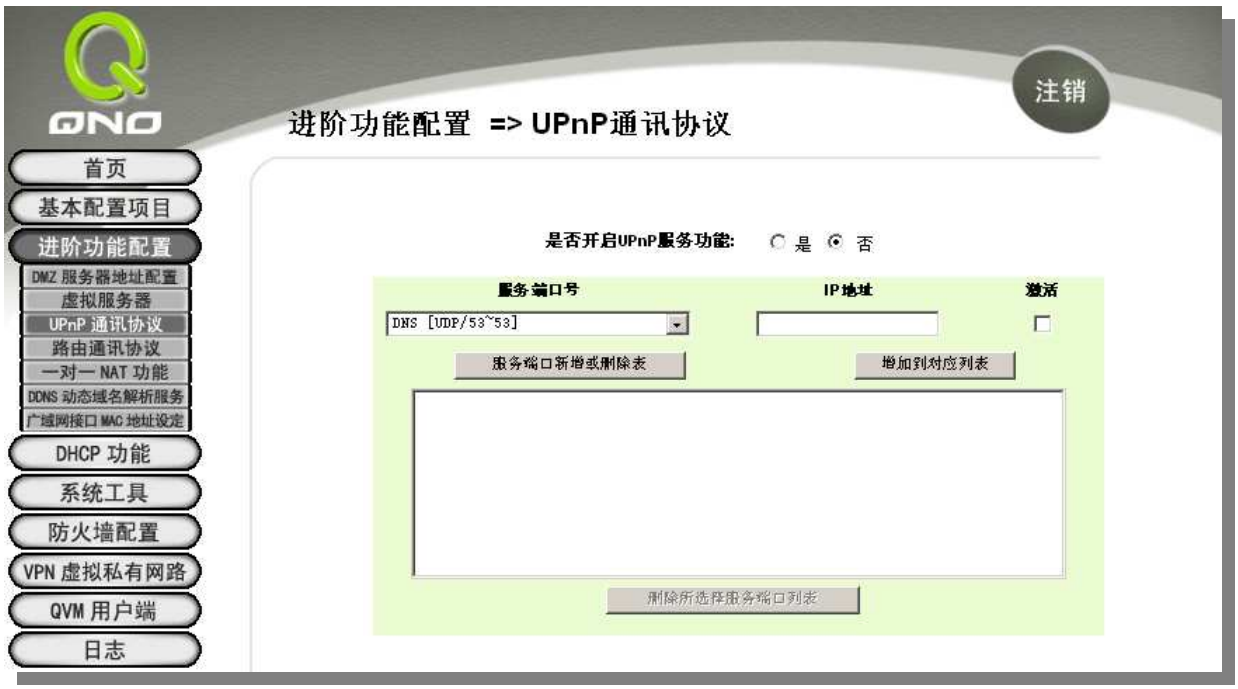
设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取**

消按钮，将不做任何设定变更。

4.3 UPnP- Universal Plug and Play

UPnP (Universal Plug and Play) 是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的计算机有支持 UPnP 机制的话(如 WindowsXP) 而且您的计算机 UPnP 功能有开启，您可以将 VPN QOS 安全路由器产品的 UPnP 功能启动。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在内网设置虚拟服务器，您可以在前章节介绍的 Forwarding 功能设置，或是在此 UPnP Forwarding 中设置。不过请不要重复输入造成冲突。



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

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号列表

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： 删除所选择的开启服务项目之一笔内容

显示开启表： 显示目前所开启设定的 UpnP 服务列表

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4.4 一对一 NAT 对应

当您的 ISP 线路为固定制时，通常 ISP 会给您多个合法 IP 地址。VPN QOS 安全路由器产品提供您可将除了 VPN QOS 安全路由器产品本身广域网端口以及光纤盒或 ATU-R(Gateway) 各使用一个合法 IP 地址后，所剩的合法 IP 地址可以直接对应到内部的计算机使用，也就是这些计算机在内网虽为虚拟 IP，但当做了 One to One 对应后，这些对应到的计算机去外部访问时都是有自己的合法 IP。

例如，当您公司内部环境需有两台或两台以上的 WEB 服务器时，由于需要两个或两个以上的合法 IP 地址，所以可以利用此功能达到将外部多个合法 IP 地址直接对应到内部多个虚拟服务器 IP 地址使用！

范例：如您有 5 个合法 IP 地址，分别是 210.11.1.1~6，而 210.11.1.1 已经给 WAN1 使用，另外还有其它四个合法 IP 可以分别设定到 One to One NAT 当中，如下所述：

210.11.1.2 → 192.168.1.3

210.11.1.3 → 192.168.1.4

210.11.1.4 → 192.168.1.5

210.11.1.5 → 192.168.1.6

注意！

VPN QOS 安全路由器 WAN IP 地址不能被涵盖在 One to One NAT 的 IP 范围设定中。

一对一 NAT 功能: 选择是否开启此一对一 NAT 功能开启 /关闭

内部范围 IP 地址: 虚拟 IP 地址起始 IP 地址

外部范围 IP 地址: 外部合法 IP 地址起始 IP

对应 IP 数量: 填入您同时要有多少个外部合法 IP 地址需要对应

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: 删除所选择的一对一 NAT 规则

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

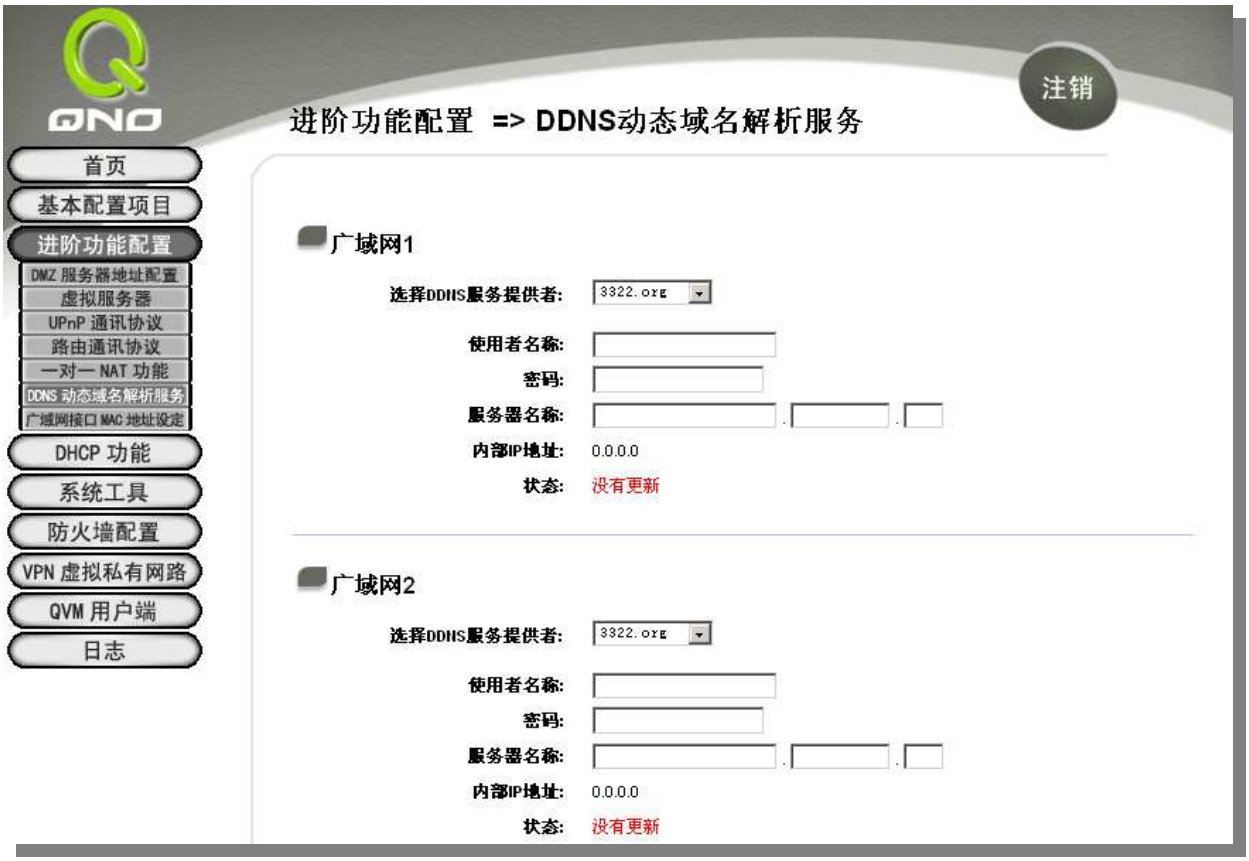
注意！

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，局域网端所对应公网 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，请到防火墙的"存取规则设定"中设定适当的拒绝存取规则条件。

4.5 DDNS-动态域名解析

“DDNS”功能可以支持 QnoDDNS.org.cn、Dyndns.org 与 3322.org 的动态域名解析功能，其目的是为了让使用动态 IP 地址(也就是无法有固定 IP 的环境)来架设虚拟服务器、建立企业 VPN 使用、及远程监控时查询现在的 Router IP。如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的 WAN IP 地址都会随 ISP 端要求而改变，当此时使用者申请了 DDNS 后，如”abc.qnoddns.org.cn”，将其设定在 DDNS 设定中，则在远程只要去 Ping abc.qnoddns.org.cn 则可以知道现在 VPN QOS 安全路由器产品的实际 IP。且若是内部有架设网站之类的服务，Internet 使用者只要在网址打上 abc.qnoddns.org.cn 就可以直接进入到您内部架设的 WEB。在设定此功能之前，请向 www.qno.cn/ddns、www.dyndns.org 或是 www.3322.org 提出申请，是完全免费的！

另外，为了解决 DDNS 服务器可能会发生不稳定的情况，现在 VPN QOS 安全路由器产品每个 WAN 都可同时对 DDNS 服务做动态 IP 更新。



DDNS 动态域名解析服务： 可以选择 QnoDDNS.org.cn、Dyndns.org、以及 3322.org (可同时使

用)

使用者名称： 向 DDNS 所设定的名称

●QnoDDN 使用者名称要填入完整的网址，如：abc.qnoddns.org.cn

密码： 向 DDNS 服务提供者所申请的密码

服务器名称： 动态网址名称： 向 DDNS 所注册的网址，如：abc.dyndns.org 或 xyz.3322.org

内部地址： 目前此条 WAN 所取得的 ISP 之动态合法 IP 地址，当 VPN QOS 安全路由器得到 ISP 端给的合法 IP 位置后会自动显示于此

状态： 显示目前 VPN QOS 安全路由器对 DDNS 的更新状态

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

注册 QnoDDNS 侠诺动态域名(Qno Dynamic DNS Service)

1. 请先至 Qno 侠诺网站，进行产品注册：http://www.qno.cn/web/register.asp
2. 依据产品注册使用的电邮以及产品序列号，登入 QnoDDNS 侠诺动态域名服务系统；请确认电邮可以确实收信，以利注册域名后，可收到系统寄出的启用 QnoDDNS 服务密码。

3. 域名申请规则：

- 域名最少需为 4 个字，最多 63 个字
- 域名只能由 a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母
- 域名不得有特殊符号(例如："."；"-"；"_"等等)
- 2 Wan 系列产品最多申请 2 个 DDNS 设定
- 4 Wan 系列产品最多申请 4 个 DDNS 设定
- 8 Wan 系列产品(含以上)最多申请 4 个 DDNS 设定


登 出
QnoDDNS
侠 诺 动 态 域 名
Qno Dynamic DNS Service
:: 用户数据 ::
姓名
Email
序列号
型号
Wan数量
:: 申请规则 ::
1. 如果您申请Qno侠诺科技动态域名服务，代表您同意侠诺科技动态域名服务条款。
2. "用户名称"最少需要4个字，最多63个字(4-63个字)。
3. "用户名称"只能由a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。
4. "用户名称"不得有特殊符号(例如："."；"-"；"_"等等)。(范例)
5. 2 Wan系列产品最多申请2个DDNS设定。
6. 4 Wan系列产品最多申请4个DDNS设定。
7. 8 Wan系列产品(含以上)最多申请4个DDNS设定。
:: Host Name 测试 ::
已输入0个字
测试
用户名称：
域名：
qnoddns.org.cn
发送
重设
尚可申请 4 组DDNS
已输入0个字
第1组
用户名称：
域名：
qnoddns.org.cn
申请
已输入0个字
第2组
用户名称：
域名：
qnoddns.org.cn
申请
已输入0个字
第3组
用户名称：
域名：
qnoddns.org.cn
申请
已输入0个字
第4组
用户名称：
域名：
qnoddns.org.cn
申请

4.6 广域网接口 MAC 地址设定

有些 ISP 会要求提供一固定 MAC 地址(网卡地址)做为 ISP 端分配 IP 给您的认证使用，此大多使用于 Cable Mode 的用户。若有此需求的话，可使用此功能将提供给 ISP 的网卡地址(MAC Address：00-xx-xx-xx-xx-xx) 填入此项目中，VPN QOS 安全路由器产品就会以此 MAC Address 做为跟 ISP 请求 IP 时的认证！**请注意**：VPN QOS 安全路由器产品只有 WAN1 才能进行此功能的设定。

使用者自订广域网接口 MAC 地址设定： 使用者可以自行输入提供给 ISP 的网卡地址，目前设备出厂默认的 MAC 位置为 WAN 端的 MAC 地址。

设定 MAC 地址与此 PC 的 MAC 地址相同： 目前这台 PC 的 MAC 地址。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4.7 DHCP 发放 IP 服务器

VPN QOS 安全路由器产品有一组 Class C 的 DHCP 服务器，默认值是启动，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，就可自动取得 IP 地址，管理方便。

4.7.1 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)，当租约时间到后，PC 端会重新跟 Router 再申请一次。您可以依照实际需求来设定。

起始 IP 地址： 系统默认为从 192.168.1.100 的 IP 地址开始发放。您可以依照实际需求来设定。

终止 IP 地址： 系统默认为 192.168.1.149 IP 地址为最后发放 IP，也就是说出厂设定值可供 50 台计算机自动取得 IP 地址。您可以依照实际需求来设定。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4.7.2 IP 及 MAC 地址绑定

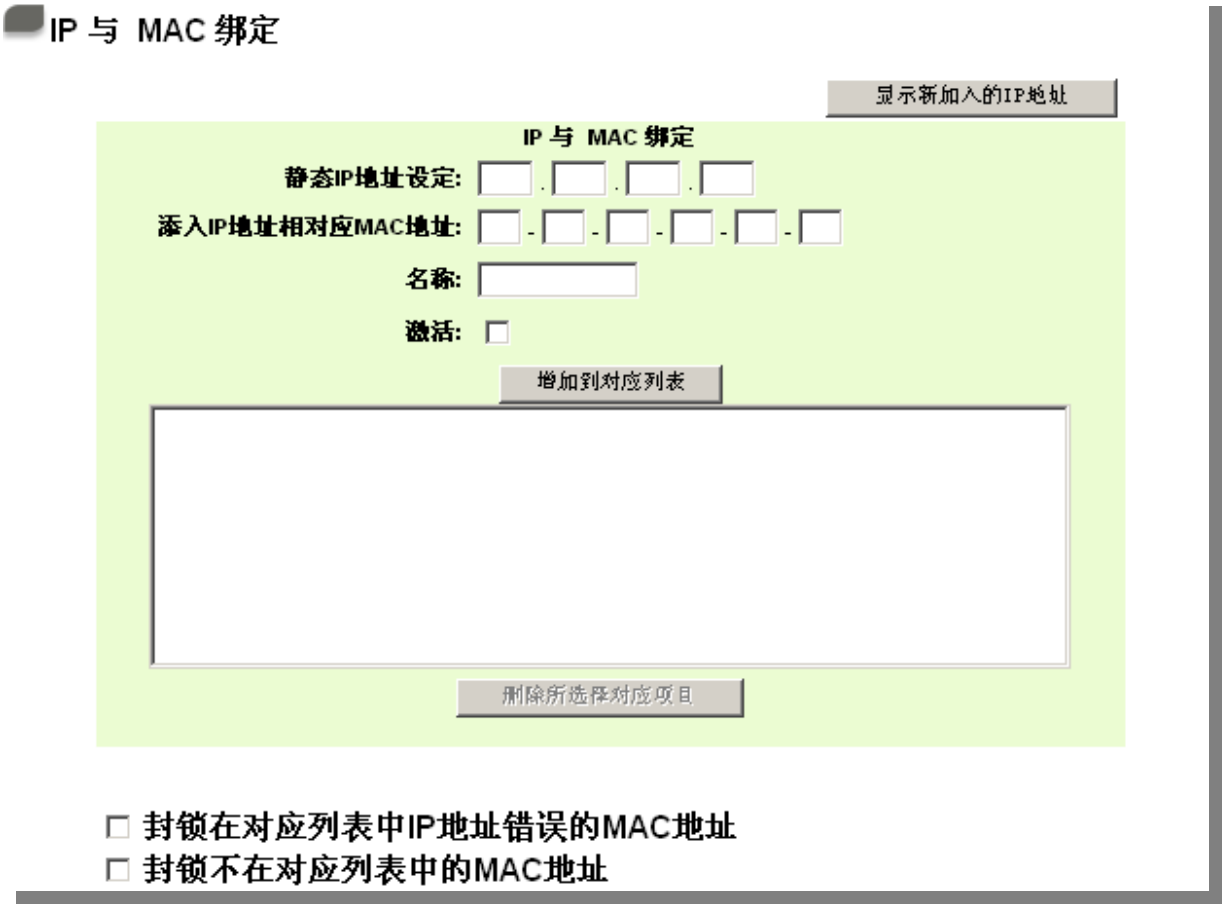
在许多的企业及小区网络中，网管人员可以设定 VPN QOS 安全路由器产品所提供的 IP & MAC 绑定功能，达到 User 不能自行添加计算机来使用对外网络或是私自擅改 IP 上网影响他人。另外透过此功能也可以将每台计算机或服务器的 MAC 地址绑定，达到计算机或服务器每次开机或重新要 IP 时，都分配给它相同的一组 IP 地址。

您可以以下两种方式来设定这个功能：

限定可以使用网络的 MAC 地址

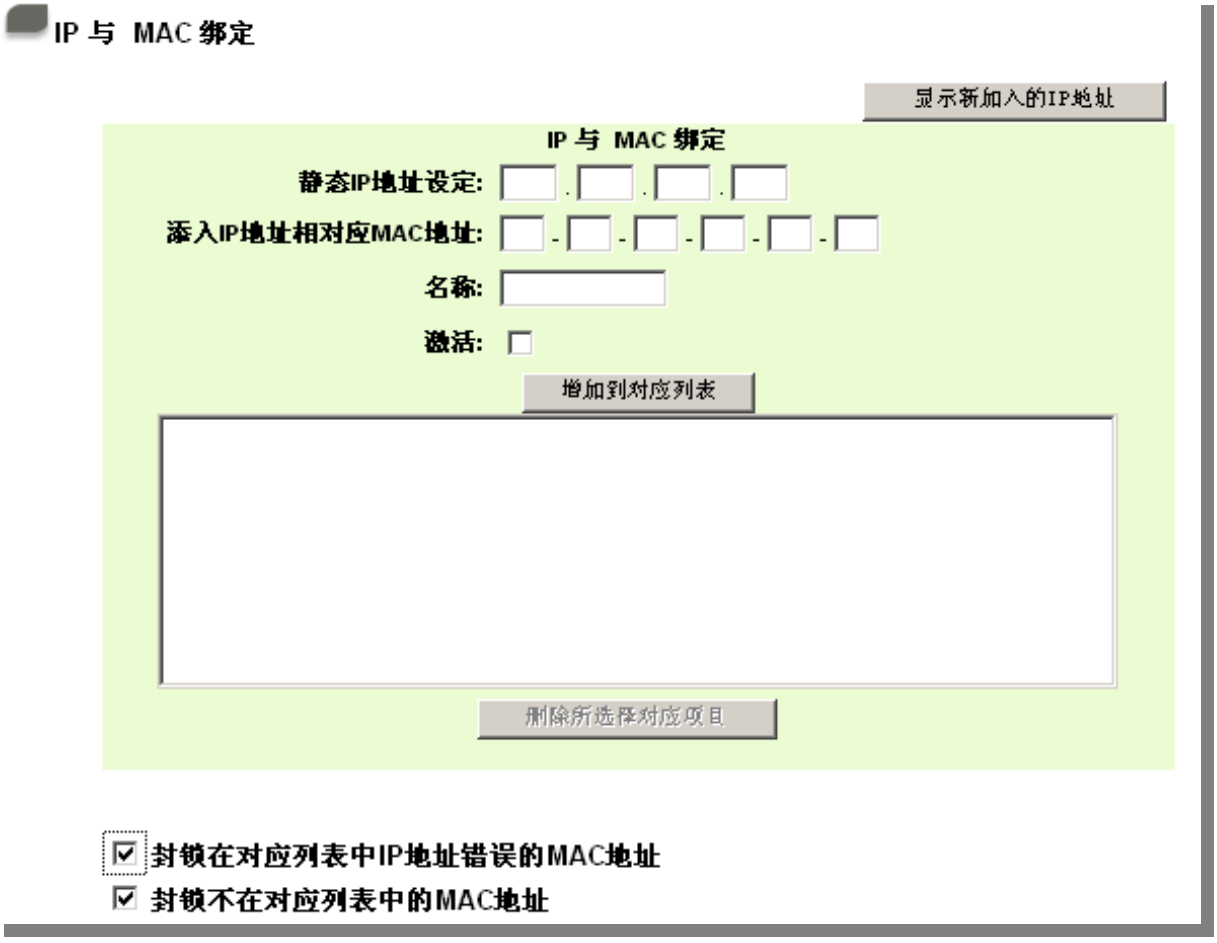
此功能主要目的是限制只有在列表里面的 MAC 地址才可以得到 DHCP 分派的 IP 地址上网，未在此列表的计算机都无法取得 IP 上网。

当使用此功能时，切记要将固定 IP 地址填 0.0.0.0 不可以空白，另外将 **封锁不在对应列表中的 MAC 地址** 选项打勾才可以执行。如下图中范例所示：



IP 及 MAC 地址绑定

此功能主要目的是让指定的 MAC 地址计算机在每次开机都会要到同一个指定 IP。此外，若将 **封锁在对应列表中 IP 地址错误的 MAC 地址** 功能启用，则设定为固定 IP 或以此功能发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，会无法上网。



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，则将您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。

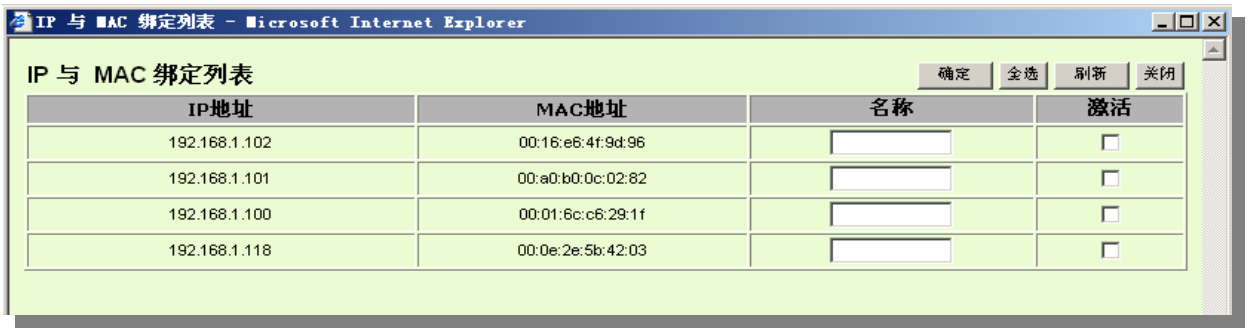
封锁在对应列表中 IP 地址错误的 MAC 地址: 此选项打勾后，只要是用户自行更改计算机的 IP 或不是列表设定的 IP 将无法上网。

封锁不在对应列表中的 MAC 地址: 此选项打勾后，只要不在列表中的 MAC Address 都无法上网。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

显示出还未做绑定或新加入的 IP 及其 MAC 地址：

此功能的主要目的是为了减少网管人员需一一查询每台计算机的 MAC 地址后才能进行绑定，因为会非常耗时且困难。再者，将 MAC Address 手动填入列表也很容易出错。所以只需要查询此表格，就可以看到所有进出 VPN QOS 安全路由器产品且还未绑定的 MAC Address，然后直接在此表格做绑定动作即可.另外，若您发现此表格出现已经绑定的某组 MAC 又出现在此表格，则表示此 User 试图修改不是您指定的 IP 上网。



名称: 可以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。

激活 勾选您所要绑定的目标。

确定: 将您所选定好的目标绑定到 IP & MAC 绑定列表。

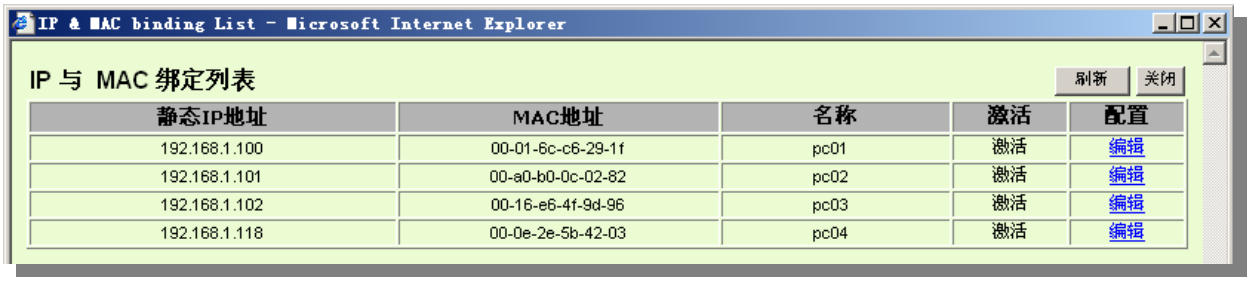
全选 选择所有在此列表中的目标做绑定。

刷新: 更新此列表。

关闭: 关闭此列表。

显示表格

此功能可以列出所有现在已经设定好的 IP/MAC 绑定的状态，并且可以选择 **编辑** 做修改。



4.7.3 DNS 与 WINS 服务器设定

域名解析服务地址：

此设定为发给 PC 端 IP 地址的 DNS 网域服务器查询地址，若您有特定使用的 DNS 网域服务器，可以直接输入此服务器的 IP 地址，则 PC 端从 DHCP 取得 IP 地址时，也会一并取得指定的 DNS 网域服务器地址。

DNS 域名解析地址 1： 输入第一个 DNS 网域服务器的 IP 位置。

DNS 域名解析地址 2： 输入第二个 DNS 网域服务器的 IP 位置。

WINS 服务器：

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

WINS 服务器： 输入 WINS 网域服务器的 IP 位置。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

4.7.4 DHCP 状态显示

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。

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 服务器可以还可发放的 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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

5、系统工具功能设定

此章节介绍用来管理 VPN QOS 安全路由器以及测试网络联机的工具。

5.1 在线联机测试

VPN QOS 安全路由器产品提供简易的在线测试机制，方便于测试线路质量时使用。 此包含网域名称查询测试以及 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。测试结果会显示于画面上。

Ping-封包传送/接收测试

此项目为主要提供管理者了解对外联机的实际状况，可以藉由此功能了解网络上的计算机是否存在！

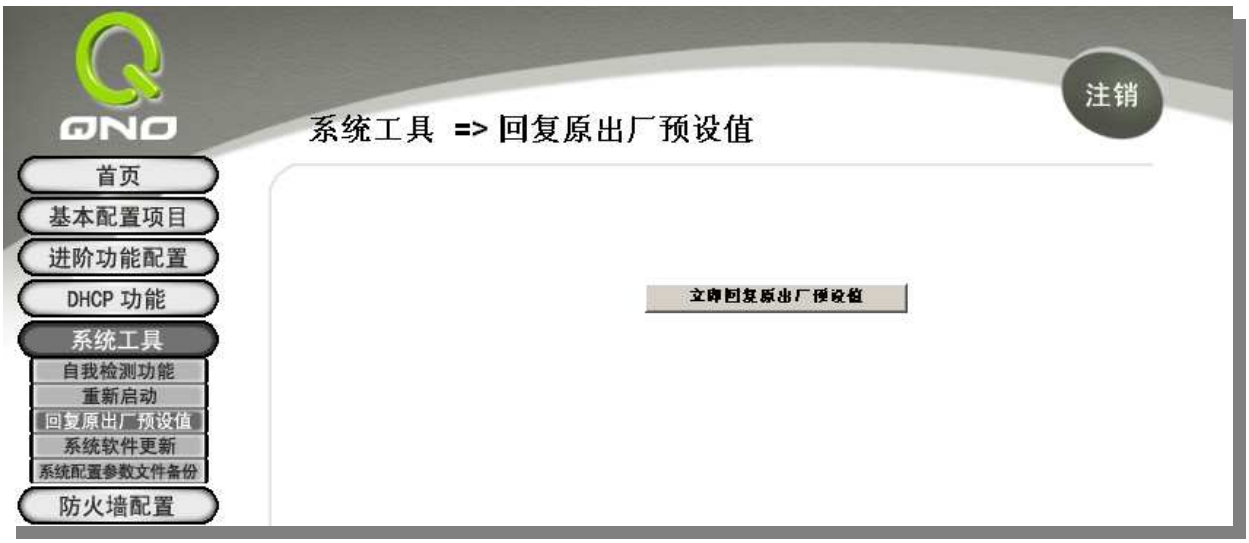
请于此测试画面输入您想测试的主机位置 IP，如 192.168.5.20 按下 **开始** 的按钮开始测试，测试结果会显示于画面上。

5.2 重新启动

您可以于此工具中选择系统重新开机功能，请按下 **立即重新激活** 按钮即可重新开机启动。

5.3 恢复原出厂默认值

若是选择 **立即恢复原出厂默认值**，VPN QOS 安全路由器产品会将所有的设定清除，并重新开机。我们建议在做版本升级前请先将 VPN QOS 安全路由器现在的设定值存储到计算机，等做完版本升级后，使用此功能将机器做出厂值设定以确保机器升级后的稳定性，然后再将刚才存在计算机的设定值存回 (如何储存设定数据及升级完成后如何存回，请参考“系统配置参数文件备份”说明)。

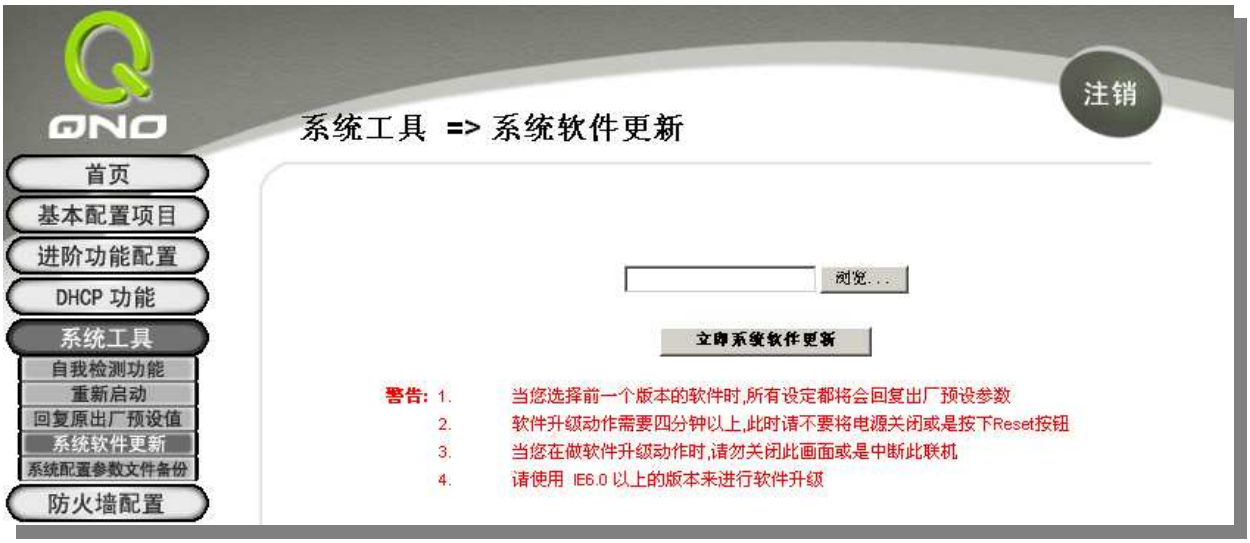


5.4 系统软件更新

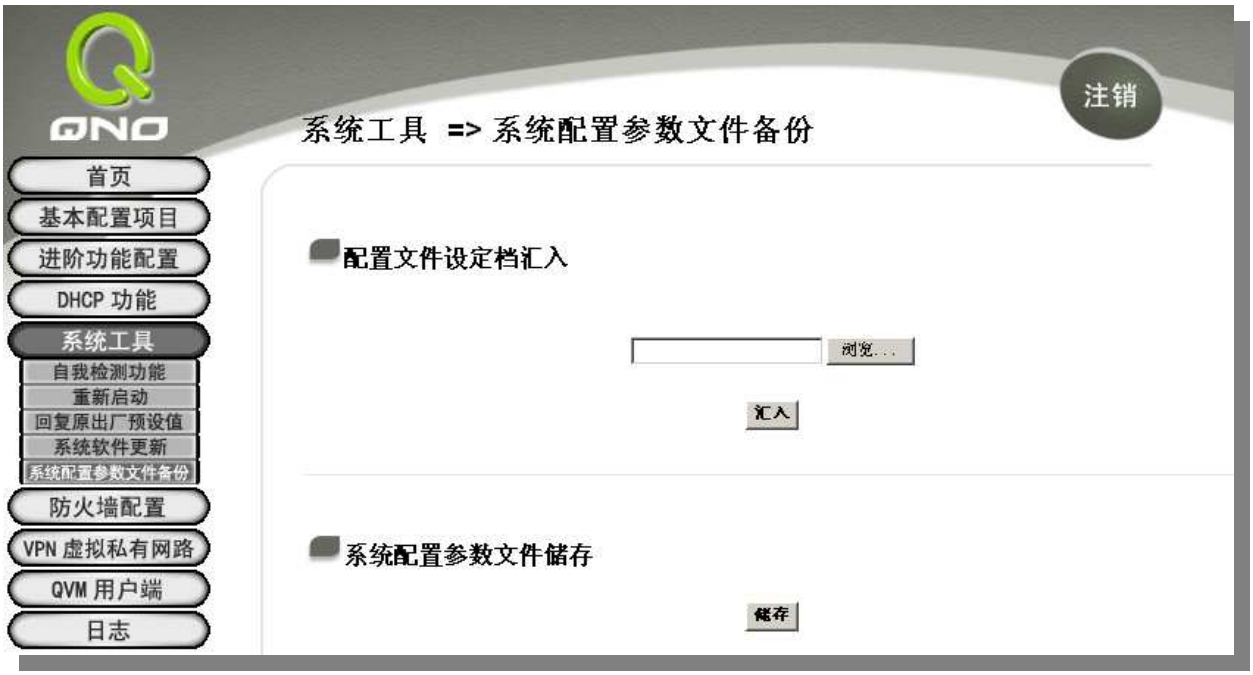
此功能可以让 VPN QOS 安全路由器产品在 Web 设定画面中直接做软件升级。请您于升级前先确认软件版本信息。按下 **浏览** 按钮，选择软件存放数据夹，并于选择欲升级的软件后，按下 **立即系统软件更新** 做升级。

注意！

执行软件(Firmware)升级前，请详细阅读画面中的注意事项。 正在做软件(Firmware)升级当中时，请勿离开此升级画面，否则会造成升级失败。



5.5 系统配置参数文件备份



汇入配置文件：

此功能为将之前所储存在计算机的备份设定参数内容回存到 VPN QOS 安全路由器产品中！选择 **浏览** 至备份参数档案 "config.exp" 存放数据夹，选择该档案后，按下 **汇入** 按钮做设定档案汇入。

储存系统配置参数文件：

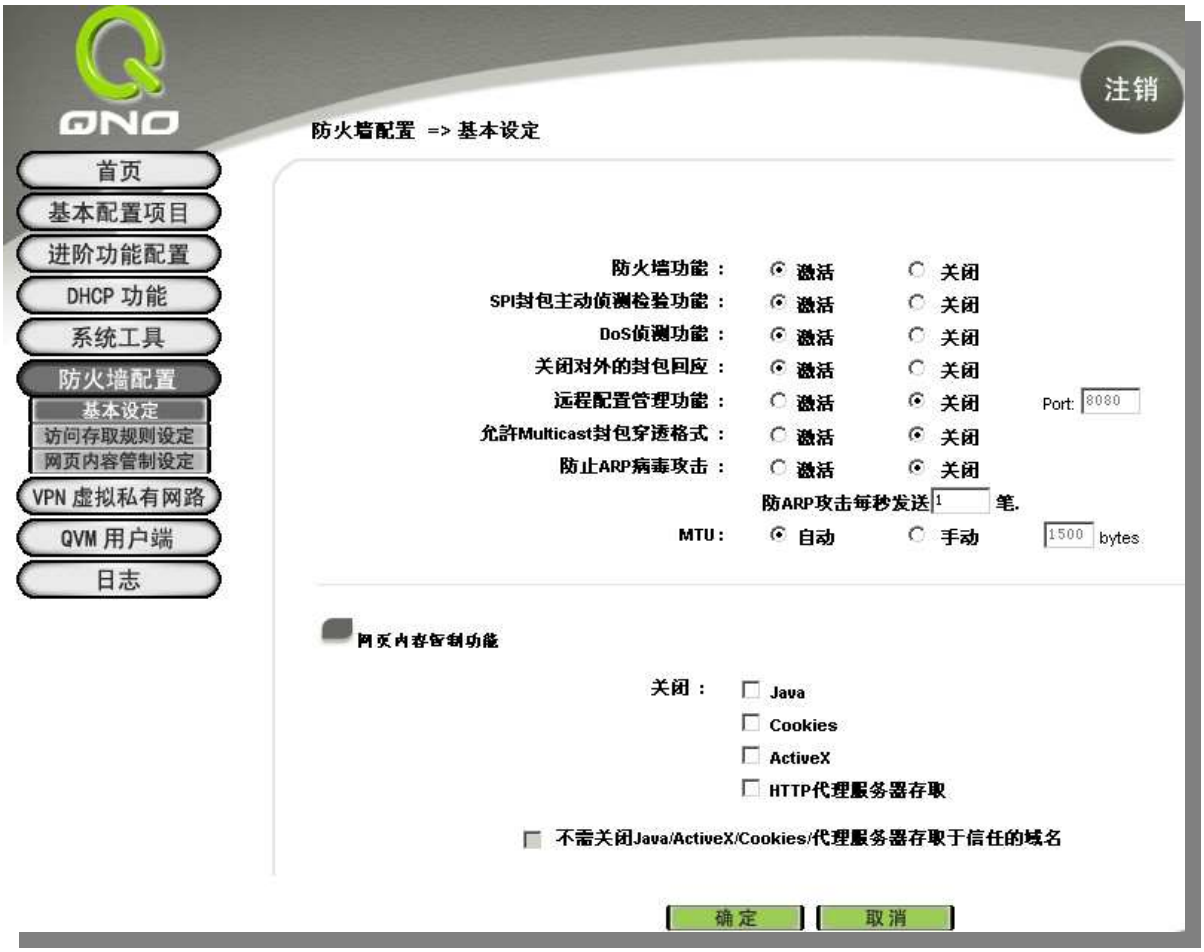
此功能为储存网管人员在 VPN QOS 安全路由器产品的设定参数备份到计算机中，通常做 VPN QOS 安全路由器版本升级前，请务必将您现在的设定文件用此功能储存在计算机中！选择至备份参数档案 -"config.exp" 存放数据夹位置，按下 **储存** 按钮即可。

6、防火墙功能设定

本章节介绍防火墙设定的选项，以及网络存取控制的设定。

6.1 防火墙一般设定

从防火墙功能的一般设定选项当中，您可以控制开启或是关闭这些选项功能。出厂默认值是将防火墙开启，并关闭不必要的响应。



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: 此为保护 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，则会关闭对外的 ICMP 与不正常联机的封包响应，所以若是您从外部去 ping 此台机器的 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机器的外部合法 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 Client 端接收此类封包讯息格式。默认值为关闭这个功能。

MTU: MTU 为 Maximum Transmission Unit 的缩写，一般默认为 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 相关，一般使用默认 Auto 即可，不需做任何调整。

网页内容管制功能： 支持封锁下列几种的方式连接：Java，Cookies，Active X， Access to HTTP Proxy Servers。

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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

6.2 网络存取规则

VPN QOS 安全路由器产品设计有简而易懂的网络存取规则条例工具，管理者可以用来对不同的使用者设定不同的存取规则条件，来管理使用者对网络的存取权限。存取规则可以依据不同的条件来过滤，例如可以设定封包要管制的进出方向是从内部到外部、还是从外部到内部，或是设定以使用者的 IP 地址、目地端 IP 地址、IP 通讯协议形态等条件来做管制，管理者可以依照实际的需求调性设置。

管理者定订的网络存取规则条例，可以选择关闭或是允许来调整使用者对 Internet 的存取。以下就针对网络存取规则条例做一说明：

VPN QOS 安全路由器产品默认的网络存取规则条例：

- All traffic from the LAN to the WAN is allowed- 从 LAN 端到 WAN 端的所有封包可以通过
- All traffic from the WAN to the LAN is denied.- 从 WAN 端到 LAN 端的所有封包不可以通过
- All traffic from the LAN to the DMZ is denied.- 从 LAN 端到 DMZ 端的所有封包不可以通过
- All traffic from the DMZ to the LAN is denied- 从 DMZ 端到 LAN 端的所有封包不可以通过
- All traffic from the WAN to the DMZ is denied- 从 WAN 端到 DMZ 端的所有封包不可以通过
- All traffic from the DMZ to the WAN is denied- 从 DMZ 端到 WAN 端的所有封包不可以通过

管理者可以自定存取规则并且超越默认的存取条件规则，但是以下的四种额外服务项目为永远开启，不受其它自订规则所影响：

- HTTP 的服务从 LAN 端到 VPN QOS 安全路由器产品默认为开启的 (为了管理机器使用)。
- DHCP 的服务从 LAN 端到 VPN QOS 安全路由器产品默认为开启的 (为了从机器自动取得 IP 地址使用)。
- DNS 的服务从 LAN 端到 VPN QOS 安全路由器产品默认为开启的 (为了解析 DNS 服务使用)。
- Ping 的服务从 LAN 端到 VPN QOS 安全路由器产品默认为开启的 (为了连通测试机器使用)。

除了默认规则以外，所有的网络存取规则都会显示于此规则列表中，您可以自己选择高低优先权于每一个网络存取规则项目中。在做规则确认时是依照优先权利 1-2-3.....依序做规则判断，所以优先权是让您在做存取规则的设定规划中必须要考虑的，以避免您想开启或关闭的功能失效。

编辑： 可以设定网络存取规则项目。

垃圾桶图像： 可以删除网络存取规则项目。

新增规则： 新增新的网络存取规则按钮可以新增一项新的存取规则。

恢复到出厂默认值： 可以恢复到出厂原有默认存取规则项目并删除所有的自订规则内容。

增加新的管制规则

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。
关闭：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您所要允许或不允许的服务端口项目。

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

来源接口: 选择您所要允许或不允许的来源封包接口(例如是从 LAN，WAN1，WAN2 或是任何)，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，单一，或范围)，若是选择单一或是范围的话，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，单一，或范围)，若是选择单一或是范围的话，请输入此单一或是一区段范围的 IP 地址。

时间管制设定: 您可以将此条规则依照您所需要的执行时间来做控管。例如您可以设定此

规则每天上午 8：00 开始执行下午 17：00 结束，或 24 小时都执行管制。

应用此存取规则: 可选择全部表示都 24 小时都执行此规则(默认)，或是可以选择从几点到几点，以及设定是每天还是某几天做管制。

到: …到….： 此管制规则有时间限制，设定方式为 24 小时制，如 08：00 到 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，可以直接做个别选择。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

6.3 网页内容管制

VPN QOS 安全路由器产品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: 选择打勾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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

网页字符串管制:

只要输入如 “sex”的字符，那所有在网址里面有 “sex”的网站都会被封锁。

网页字符串管制: 当此项功能启动后，当输入网站地址有存在 “sex”关键词时，则会将所有有“sex”的网页封锁。

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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

允许访问的网站

此功能的目的是设定只能去访问的网址，在有些公司或学校中，会只允许员工或学生只能去哪些网站，

就可以用此功能来达成。

允许网页配置: 选择打勾开启允许网址管制功能，默认为关闭。

新增: 填写欲管制的允许网址，如 www.playboy.com。

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: 可以使用鼠标点选一个或多个管制的允许网址，然后按下即可删除。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

管制内容排程时间

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。

全部: 表示此管制规则 24 小时开启。

…到…: …到….: 此管制规则有时间限制，设定方式为 24 小时制，如 08：00 到 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，可以直接选择星期。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

7、虚拟私有网络功能设定 (VPN)

本章节介绍 VPN 虚拟私有网络的设定方式，附录三将介绍三种 VPN 环境的案例及其设定方式，提供作为范例参考。

7.1 VPN 状态显示

此 VPN 状态可以显示目前有关 VPN 方面的实时状态包含隧道-Tunnel，设定参数等信息.

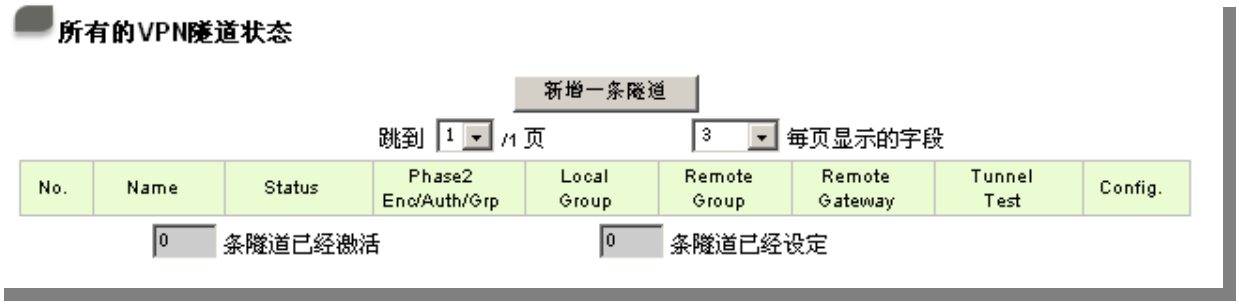
Summary：

此为显示目前有多少 VPN 隧道已经设定使用及还剩下多少隧道可以提供设定。

详细讯息： 按下此 Detail 按钮可以显示如以下画面的目前所有 VPN 组态，让管理者清楚的管理所

有 VPN 连接信息。

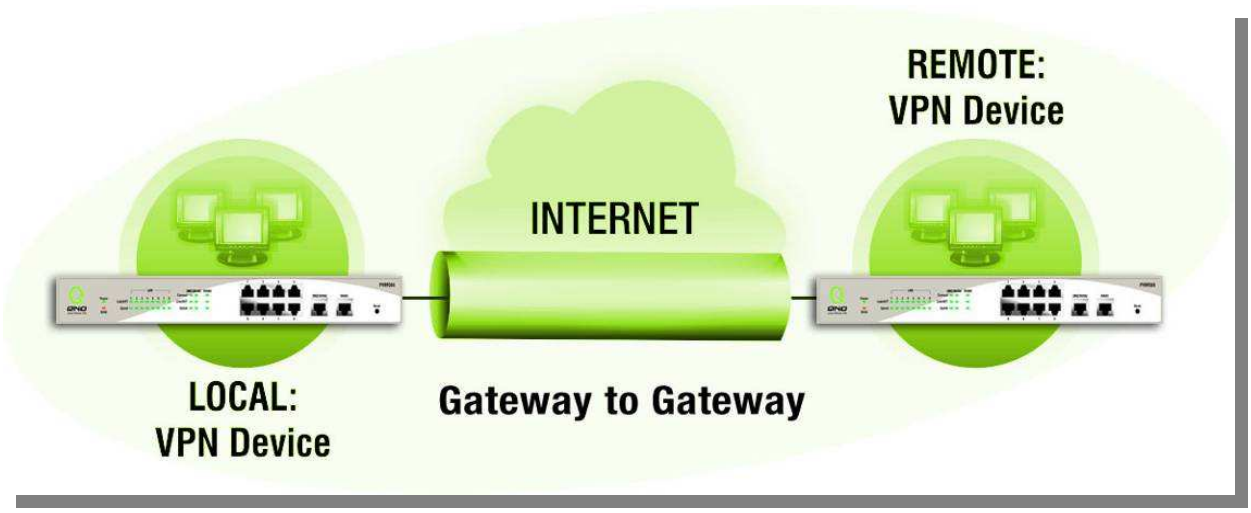
VPN 隧道目前状态显示



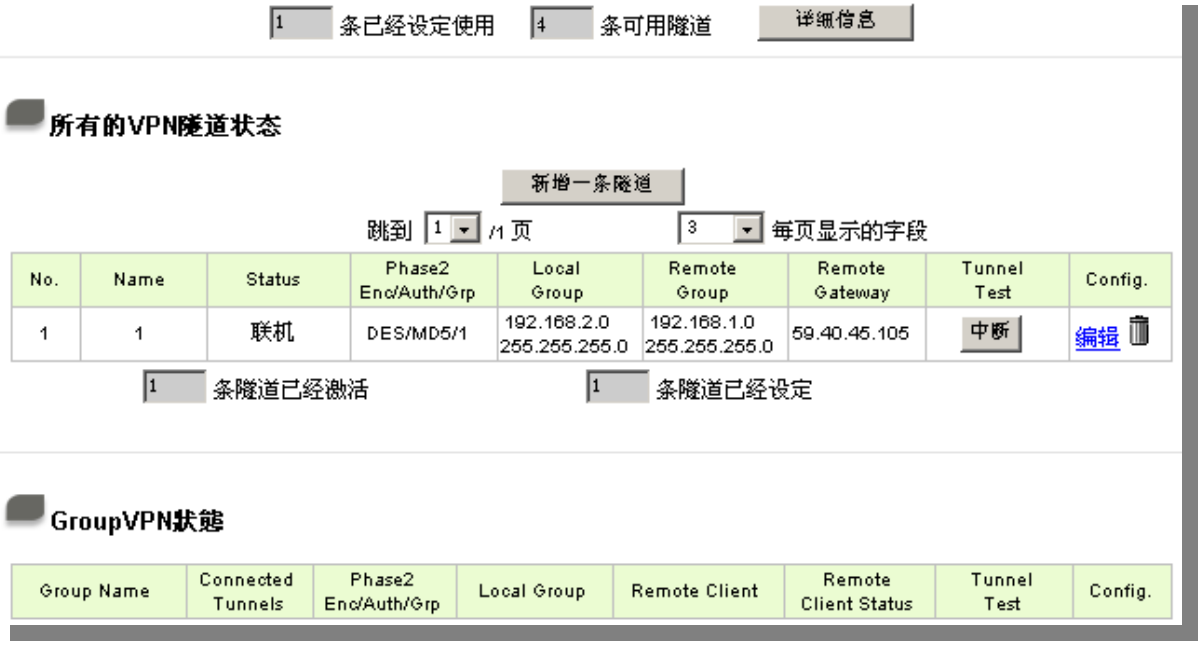
新增一条新的 VPN 隧道：按下此按钮可以新增一条新的 VPN 隧道设定。VPN QOS 安全路由器产品提供网关对网关(Gateway to Gateway) 隧道的设定模式。

网关对网关模式 (Gateway to Gateway)：

以下图例为运作于网关对网关(Gateway to Gateway) 模式的 VPN 网络连接环境。VPN 隧道连接为 2 台 VPN QOS 安全路由器分别透过 Internet 所组成。当您按下 “新增” 的话，将会直接导引到网关对网关(Gateway to Gateway) 的设定页面上。



以下针对 VPN 隧道显示讯息做完整解说：



Page：Previous page，Next page，Jump to page / 100 pages，and entries per page

您可以按**上一页**与**下一页**按钮跳到您想监看的 VPN 隧道画面上，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 隧道状态，如(3，5，10，20，All)。

Tunnel No：	显示您设定之 VPN 功能时所选择的 Tunnel 隧道编号。
Status：	于此状态显示现在联机状态为 “联机中” 或是 “等待联机” 等信息。 若是管理者选择手动-设定 IPSec 隧道，则此状态会显示手动。
Name：	目前联机 VPN 隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设定的话，务必将每一个隧道名称都设为不同，以免混淆。 **请注意**:若是您需要连接其它 VPN 设备(非 VPN QOS 安全路由器产品)，有些会规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启!
Phase2 Encrypt/Auth/Group：	显示此条 VPN 的加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设定模式。若是您选择手动设定 IPSec 的话，于此将不会显示 Phase 2 DH 群组。
Local Group：	显示本地局域网内部做 VPN 联机的群组范围。
Remote Group：	显示远程的 VPN 设备的局域网的联机群组范围。
Remote Gateway：	此为远程 VPN 设备的 IP 地址，也就是远程的 VPN QOS 安全路由器之对外的合法 IP 地址或是 Domain Name 等。
Tunnel Test：	可以按下连接按钮 去验证此隧道的状态，测试结果将会更新于此状态上。
Configure：	设定项目包含编辑以及删除图示 若您按下编辑按钮，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示的话，所有此隧道的设定将会被删除。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

7.2 网关器对网关器的 VPN 设定

此节介绍网关器对网关器的 VPN 设定方式。

7.2.1 隧道设定

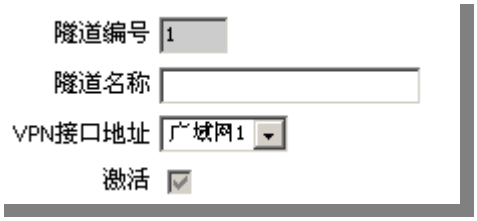
隧道编号: 当您设定内建之 VPN 功能时，此设定的 Tunnel 隧道编号会自动加 1 表示现在的隧道号码，VPN QOS 安全路由器产品可支持最高 5 条 IPSec VPN 隧道。

VPN 接口地址: 您可以选择哪一个广域网端口为此 VPN 隧道的节点，当您有设定为双线负载平衡模式时，您可以选择 WAN1 或是 WAN2 作为此 VPN 隧道的使用。

隧道名称: 设定此隧道连接名称，如 XXX Office，建议您若是有一个以上的隧道设定的话，务必将每一个隧道名称都设为不同，以免混。

请注意：若是您需要连接其它 VPN 设备(非 VPN QOS 安全路由器产品)，有些会规定此隧道名称要与主控端为相同名称并做验证，此隧道才会顺利联机开启!

激活: 勾选**激活**将此 VPN 隧道开启。此项目默认为启动，当设定完成后，可以选择是否启动隧道设定。

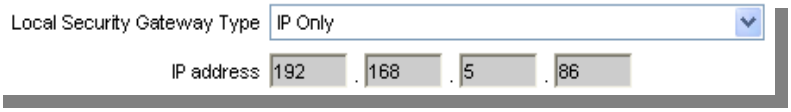


近端安全群组设定(Local Group Setup)：

您在近端网关安全群组设定(Local Security Gateway Type)形态必须与 VPN 隧道远程的 “远程网关安全群组设定(Remote Security Gateway Type)” 形态设定相同，才能成功的连接。

Local Security Gateway Type： 此为本地端的 VPN 隧道结止点，IP Only-只使用广域网 IP 作为认证。

IP Only：VPN QOS 安全路由器产品的 WAN IP 地址，会自动填入此项目空格内，您不需要再进行额外设定。

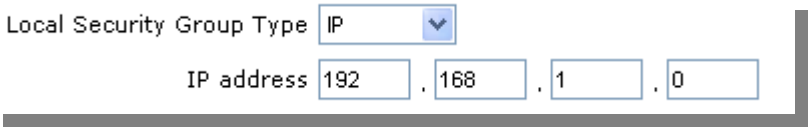


Local Security Group Type

此为设定本地区域端可以使用 VPN 联机的安全群组。请您选择适当的设置：

(1) IP Address：

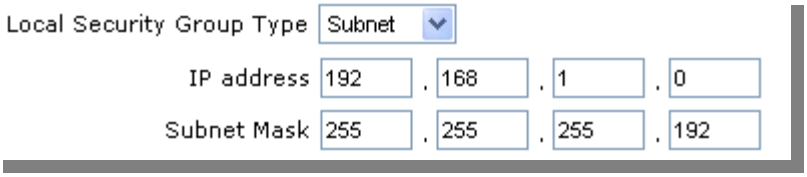
此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的本地端计算机可以联机。



注意：若是您填入 IP 地址的最后一位数为 0，表示整个网段都可以使用此 VPN 联机。例如图中所示的设定为： 当此 VPN 隧道联机后，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 隧道联机后，每一台于此网段的本地端计算机都可以联机。



以上的设定参考为： 当此 VPN 隧道联机后，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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

远程安全群组设定(Remote Group Setup)：

您在远程网关安全群组设定(Remote Security Gateway Type)形态必须与 VPN 隧道远程的 “近端网关安全群组设定(Local Security Gateway Type)” 形态设定相同，才能成功的连接。

Remote 远程安全群组设定，IP Only-只使用 IP 作为认证

Security Gateway Type：

IP Only：

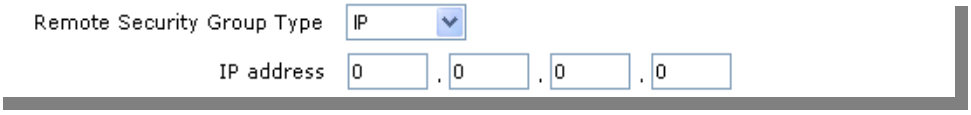
请填入对方 VPN 网关器的 WAN IP 地址.

Remote Security Group Type：

此为设定远程局域网可以使用 VPN 联机的安全群组，以下有几个关于远程区域设定的项目，请您选择适当设置：

(1) IP Address：

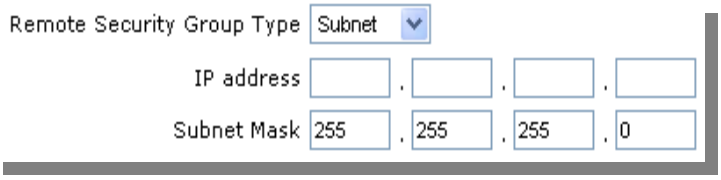
此项目为允许此 VPN 隧道联机后，只有输入此 IP 地址的远程计算机可以联机。



注意：若是您填入 IP 地址的最后一位数为 0，表示整个网段都可以使用此 VPN 联机。例如输入 192.168.2.0 则表示当此 VPN 隧道联机后，于 192.168.2.0~255 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 隧道联机后，每一台于此网段的远程计算机都可以联机..



例如输入 192.168.2.0 且 Subnet Mask 为 255.255.255.192 则表示当此 VPN 隧道联机后，只有 192.168.2.0，子网掩码为 255.255.255.192 的此网段计算机可以使用 VPN 联机。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

7.2.2 加密机制设定(IPSec Setup)

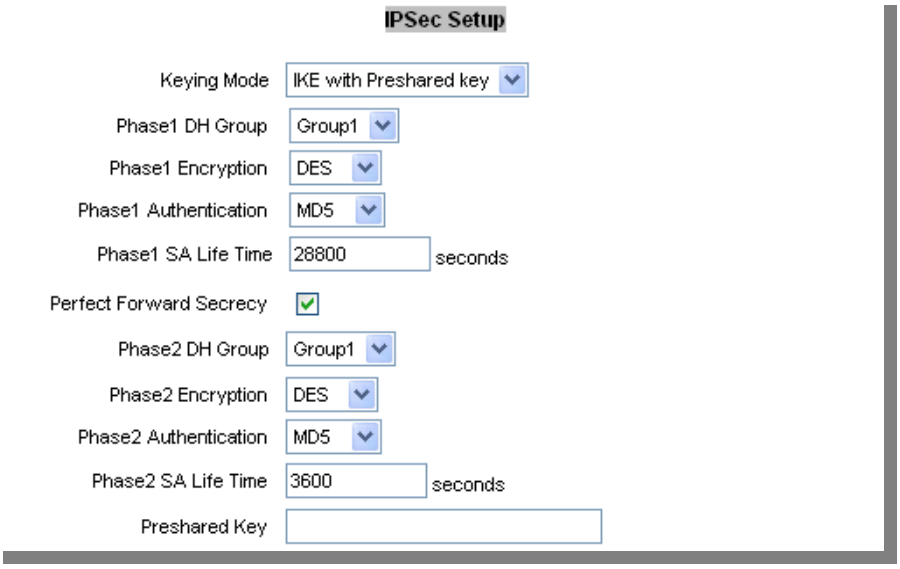
VPN 隧道可以用来安全的传输数据，其原理是在传送数据之前要将数据以密钥加密，在以封包经过 Internet 传送，收到封包后再解密还原数据。VPN 隧道的两端加密机制必须要相同才可以将此隧道建立起来，数据的收送才会正确。以下介绍密钥以及加密机制的设定。

Key Mode：

此选项为当您设定此 VPN 隧道是使用何种加密模式以及验证模式，然后，必须设定一组交换密码。请注意此参数必须与远程的交换密码参数相同。VPN QOS 安全路由器产品提供了以下二种密钥管理模式，分别为手动以及 IKE 自动加密模式。请您选择其中一种设定方式即可。

自动加密模式 IKE with Preshared Key：

透过 IKE 产生共享的金钥来加密数据与验证远程的使用者。若将 PFS(Perfect Forward Secrecy)启动后，则会在第二阶段(phase 2)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 启动后，透过 brute force 来撷取金钥的黑客(hacker)无法在此短时间内进一步得到第二把金钥，可以提高安全性。注意，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。



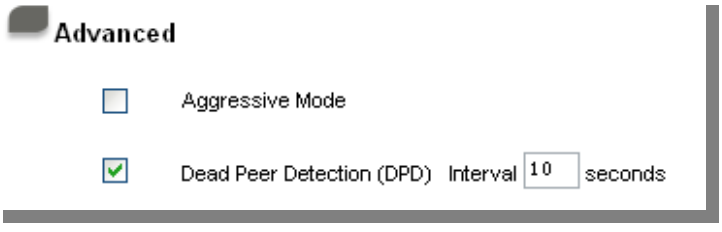
Phase1/Phase2 DH Group： 于此选项可以选择采用 Diffie-Hellman 蜜要交换群组方式： Group1 或是 Group2/Group5.

Phase1/Phase2 Encryption：	此项目为设定此 VPN 隧道使用何种加密模式。您可以选择 DES： 64-位加密模式，或是 3DES： 128-位加密模式。请注意此参数设置必须与远程的 VPN 设备设定的加密参数相同。
Phase1/Phase2 Authentication：	此验证选项设定为设定此 VPN 隧道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同： “MD5”/“SHA”.
Phase1 SA Lifetime	此为设定第一阶段所使用的密钥的有效时间，系统默认值为 28800 秒(8 小时)。于此有效时间内，此 VPN 联机会使用同一个密钥。于有效时间到期后，系统会自动的生成及更换其它的交换密码以确保安全。
Phase2 SA Lifetime	此为设定第二阶段所使用的密钥的有效时间，系统默认值为 3600 秒(1 小时)。于此有效时间内，此 VPN 联机会使用同一个密钥。于有效时间到期后，系统会自动的生成及更换其它的交换密码以确保安全。
Preshared Key：	于此项目中，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 隧道连接时的交换密钥与验证机制。此字段可以填入数字或是文字，最高可输入 23 个数字文字组合。注意，在此输入的数字文字组合，必须与远程 VPN 设备的“Pre-shared Key”字段中的相同。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

7.2.3 VPN 进阶设定(Advanced)

只有使用自动交换密钥模式(IKE Preshareed Key Only)才有此选项。



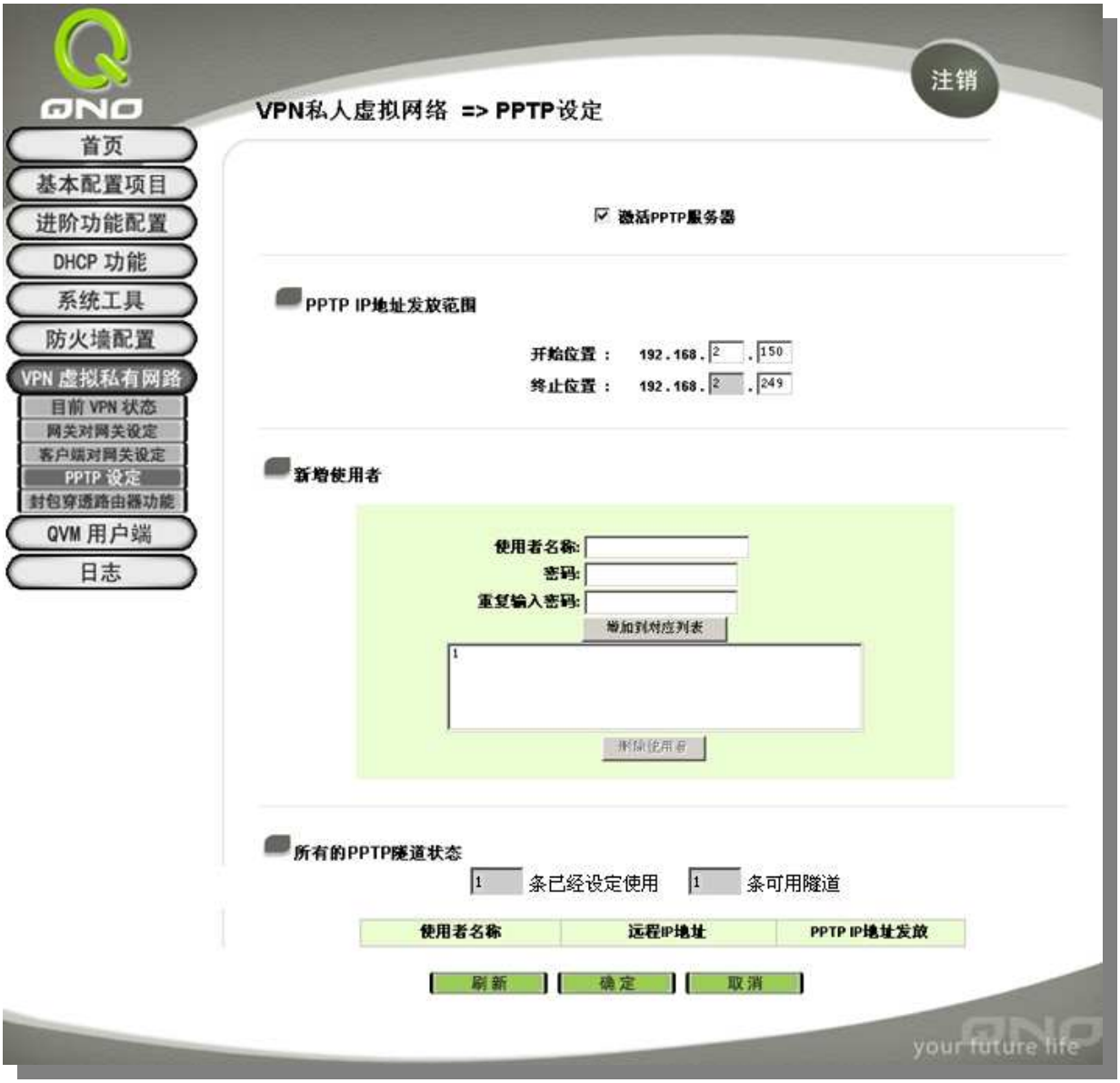
Aggressive Mode： VPN 功能默认为主要模式(Main Mode)，而且与大多数的其它 VPN 设备使用连接方式为相同。若是与 VPN QOS 安全路由器产品做 VPN 连接的远程的 VPN 设备使用 Aggressive Mode， 您可以将此选项勾选。

Dead Peer Detection(DPD)： 若选择此项目勾选，则连接中的 VPN 隧道会定期的传送 HELLO/ACK 讯息封包来侦测 VPN 隧道的两端是否仍有联机存在。当有一端断线则 VPN QOS 安全路由器产品会自动断线，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。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

7.3 PPTP 设定

VPN QOS 安全路由器产品提供支持 WindowsXP/2000 的 PPTP 连接，与 QVM 系列产品做点对点隧道协议，让远程单机用户使用此种协议建立 VPN 联机。



激活 PPTP 服务: 当使用者勾选后即可以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:请在最后一栏输入数值。输入结束范围: 请在最后一栏数入数值

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 服务器隧道的使用相关信息。VPN QOS 安全路由器产品支持 2 条 PPTP 隧道
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。

7.4 VPN 透通(VPN Pass Through)

VPN 透通设定可以允许或拒绝区域网内的其它 VPN 设备或是以 PC 上的 VPN 用户软件与远程的 VPN 设备建立 VPN 隧道。

IPSec 封包穿透：	若是选择 Enable 的话，则允许区域网内的其它 VPN 设备或是 PC 端使用 VPN-IPSec 封包穿透 VPN QOS 安全路由器产品，以便与外部 VPN 设备联机。

PPTP 封包穿透： 若是选择 Enable 的话，则允许区域网内的其它 VPN 设备或 PC 端使用 VPN-PPTP 封包穿透 VPN QOS 安全路由器产品，以便与外部 VPN 设备联机。

L2TP 封包穿透： 若是选择 Enable 的话，则允许区域网内的其它 VPN 设备或 PC 端使用 VPN-L2TP 封包穿透 VPN QOS 安全路由器产品，以便与外部 VPN 设备联机。

设定完成请按下**确定**按钮储存网络设定变更。若是不想进行变更，请在按下**确定**储存动作之前按下**取消**按钮，将不做任何设定变更。

8、QVM 超快速 VPN 设定

此一功能为 QVM 系列产品独特功能，特别为简化虚拟私有网络 IPSec VPN 的复杂配置以及管理方便所设计，符合中大型机构对高性价比以及高整合度负载均衡 VPN QOS 安全路由器的需求。当 VPN QOS 安全路由器产品和其它 QVM 系列产品配合使用时，您的 VPN 将享有以下特点：

SmartLink 设定：将原本 IPSec 复杂的设定，简化为三个参数，仍保有 IPSec 的安全性，减轻网管人员的配置负担。

远程管理功能：网管人员可于 VPN 服务器端即可监控各个分支点的联机及内部相关配置，安全及带宽管理都可实时完成。VPN QOS 安全路由器产品只提供客户端功能，未提供服务器功能；远程管理功能只适用于具有服务器功能的产品。

VPN 线路备援：QVM 系列产品于中心端及分支机构均提供 VPN 线路备援功能，大幅降低 VPN 断线风险。

在您设定 VPN QOS 安全路由器产品的 QVM 客户端功能时，请确定在 QVM 服务器中建立对应的用户名以及密码，此 QVM 隧道才能连接成功。

激活 QVM 用户端功能： 若是勾选此选项的话，QVM 功能将被开启。

QVM 用户名 ID： 输入已在 QVM 服务器中建立的对应用户 ID。

密码： 输入已在 QVM 服务器中建立的对应密码。

再次输入新密码： 再输入一次确认密码。

中心端 IP 地址或动态域名： 输入中心端 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（）分钟自动重新拨接： 此功能为 QVM 联机断开后，重新检测连接的每间隔时间。出入范围为 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。

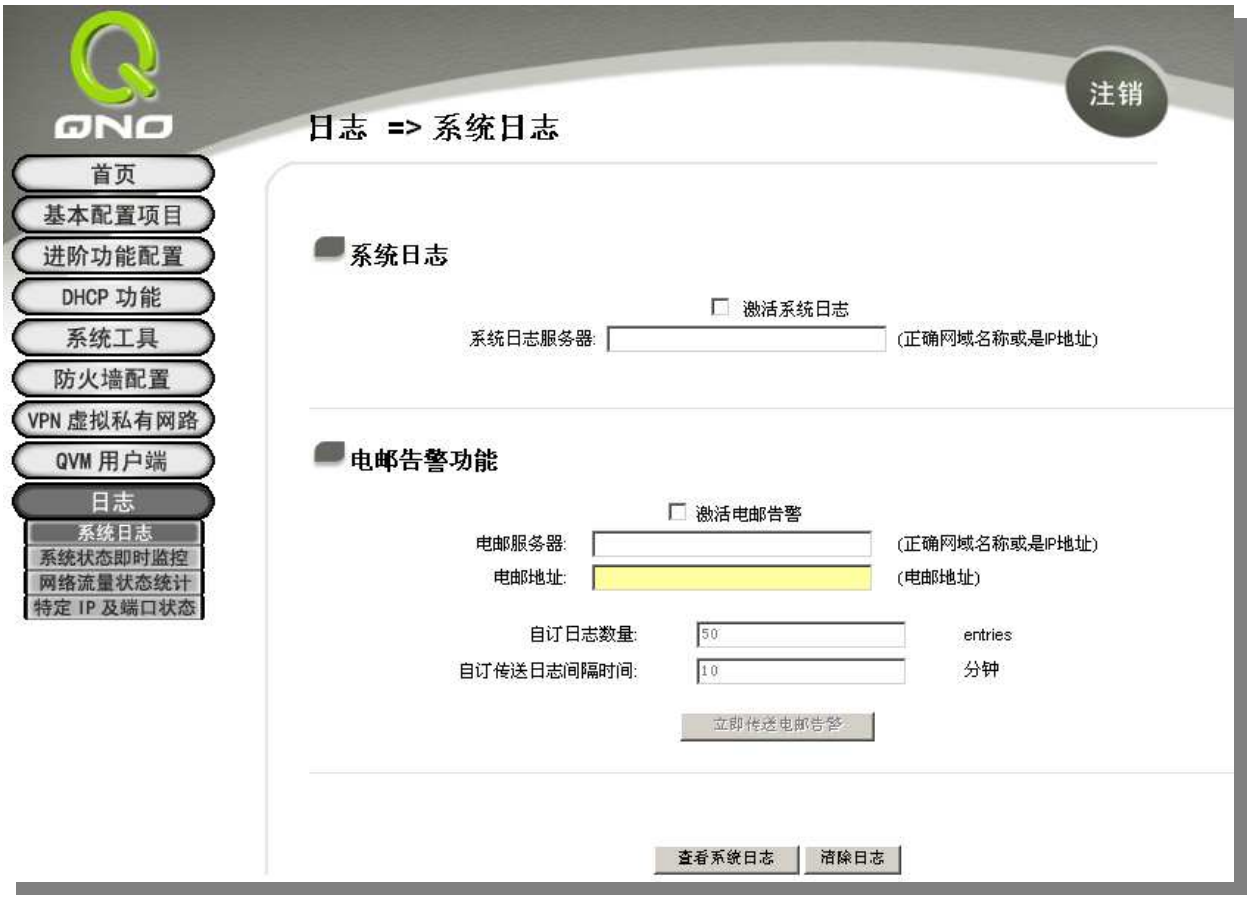
中心端备援 IP 地址或动态域名：	输入对中心端备援连接的 IP 或是网域名。

9、日志功能设定

日志(Log)功能记录 VPN QOS 安全路由器的运行数据，并以可读的方式呈现再设定画面上提供给您作为参考。您可以依据需求检视这些信息。

9.1 系统日志

VPN QOS 安全路由器产品的日志记录提供三种设定：系统日志， 电子邮件通知，以及选择日志的类别。



系统日志

激活系统日志: 若是勾选此选项的话，系统日志功能将被开启。

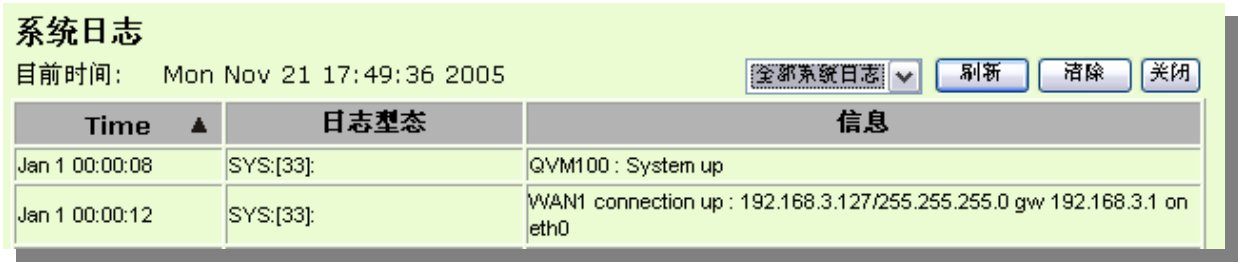
系统日志服务器: VPN QOS 安全路由器产品提供了外部系统日志服务器收集系统信息功能。系

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。系统日志提供了包含动作中的联机来源 IP 地址与目地 IP 地址，服务编号以及形态。输入您要接收系统日志的服务器名称或是 IP 地址于“系统日志服务器”的空格字段内。

以下有四个有关查询日志的按钮，分别叙述如下：

查看系统日志：

此为查看系统日志使用，其信息内容可以从下拉式选单中分类读取，包含所有讯息-ALL， 系统日志，防火墙日志，VPN 日志。选择”刷新”按钮可以刷新日志显示画面，”清除”按钮可以清除所有日志记录。如下图所示：



清除日志信息：

此按钮为清除所有目前的日志相关信息。

9.2 系统状态实时监控

VPN QOS 安全路由器产品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，包含局域或广域端口名称，目前端口联机状态，IP 地址，网络实体位置，子网掩码，默认网关，DNS 域名解析服务器，网络侦测，收到的封包数量，传送的封包数量，全部的进出封包数量统计，收到的封包 Byte 流量统计，传送的封包 Byte 流量统计，全部进出的封包 Byte 流量统计，收到的错误封包统计以及端口丢弃的封包统计等信息。

	局域网接口	广域网1接口	广域网2接口
机器名称	eth1	eth0	eth2
目前端口连线状态	---	联机	激活
IP地址	192.168.1.1	192.168.3.127	0.0.0.0
网络实体位置	00-0E-A0-00-69-AB	00-0E-A0-00-69-AC	00-0E-A0-00-69-AD
子网掩码	255.255.255.0	255.255.255.0	0.0.0.0
预设网关	---	192.168.3.1	0.0.0.0
域名解析服务地址	---	192.168.3.10 192.168.3.2	0.0.0.0
收到的封包数量	42455	10461	0
传送的封包数量	47318	6084	0
全部的封包数量	89774	16545	0
统计收到的封包Byte数量	3164808	9517281	0
统计传送的封包Byte数量	62620823	362419	0
统计全部的封包Byte数量	65787859	9879700	0
统计收到的错误封包统计	0	0	0
端口丢弃的封包统计	0	0	0

9.3 流量统计

VPN QOS 安全路由器产品提供六种显示流量统计的信息，来提供管理者对于流量有更好的管理与控制。

来源IP地址	bytes/sec	%
192.168.1.100	2685	100

对内流量内网 IP 地址：

在此图表中显示了从外进入内网流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。

网络流量显示状态：对内流量来源位置IP位置

来源IP地址	bytes/sec	%
192.168.1.100	4	100

对外流量内网 IP 地址：

在此图表中显示了从内网出去流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。

网络流量显示状态：对外流量来源位置IP位置

来源IP地址	bytes/sec	%
192.168.1.100	100	76
192.168.9.108	31	23

对内流量 IP 服务端口号：

在此图表中显示了以网络的服务端口来分类进入内网使用流量统计(每秒)byte 与百分比。

网络流量显示状态：对内流量IP服务端口号

通讯协议	目的端口	bytes/sec	%
TCP	http(80)	4	100

对外流量 IP 服务端口号：

在此图表中显示了以网络的服务端口来分类从内网出去的使用流量统计(每秒)byte 与百分比。

网络流量显示状态：对外流量IP服务端口号

通讯协议	目的端口	bytes/sec	%
TCP	http(80)	905	97
UDP	dns(53)	18	2

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：对内流量IP联机数

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
192.168.1.100	TCP	1678	202.108.15.42	80	51	76
192.168.1.100	TCP	1672	202.108.9.30	80	4	5

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：对外流量IP联机数

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%

9.4 特定 IP 及端口状态

VPN QOS 安全路由器产品提供网管人员可以针对某一 IP 或某一特定 Port 去查询此 IP 去访问的目的地址，或是有哪些人使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走多 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。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择 Port 做使用者查询。

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及服务端口。

特定IP地址/端口状態 : IP地址 IP地址 : 192 . 168 . 1 . 100 开始

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 Port 里填入您想要查询的服务端口，就可以显示出此服务端口现在有哪些 IP 正在使用。

特定IP地址/端口状態：端口 端口：80 开始

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

10、注销

VPN QOS 安全路由器产品的网页画面右上方有一个注销的按钮，此按钮为终止管理并结束此管理画面。若您下次想再进入管理画面时，您必须重复进入管理画面的步骤，并再输入管理者使用名称与密码。

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

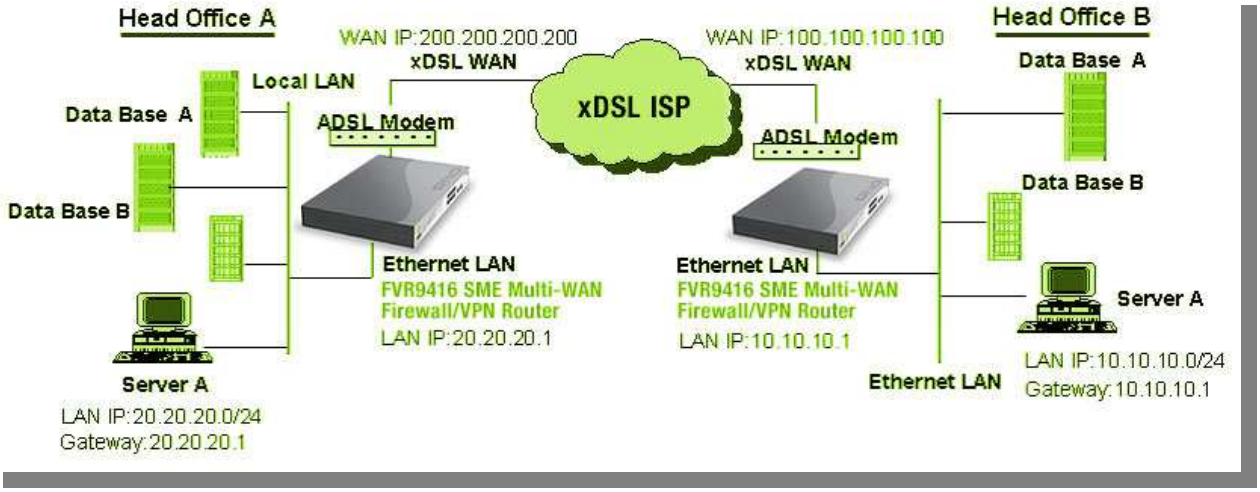
O：表示该有毒有害物质在部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。

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。

1. 电阻内部导通部位为导电银糊剂(含有铅玻璃料)
2. Diode 本体有采用含有铅玻璃料

附录二：虚拟私有网络设定范例

VPN Environment Sample 1： Gateway to Gateway



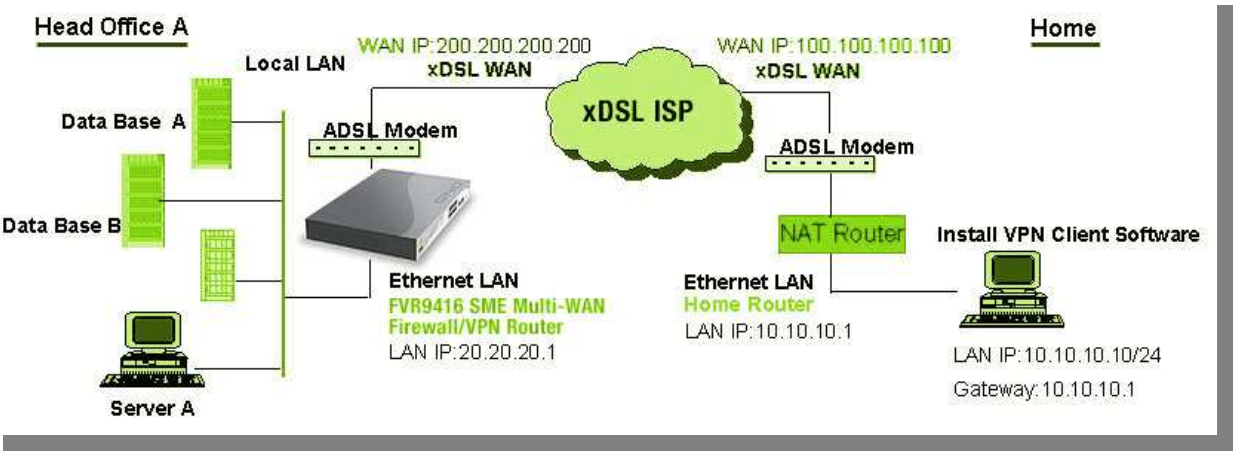
Firewall Setting： Firewall➔General➔Block WAN Request = Disable

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
Enable	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type➔ IP Address	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 Address	100.100.100.100	200.200.200.200
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type➔ IP Address	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.	

VPN Environment Sample 2： Gateway to Gateway

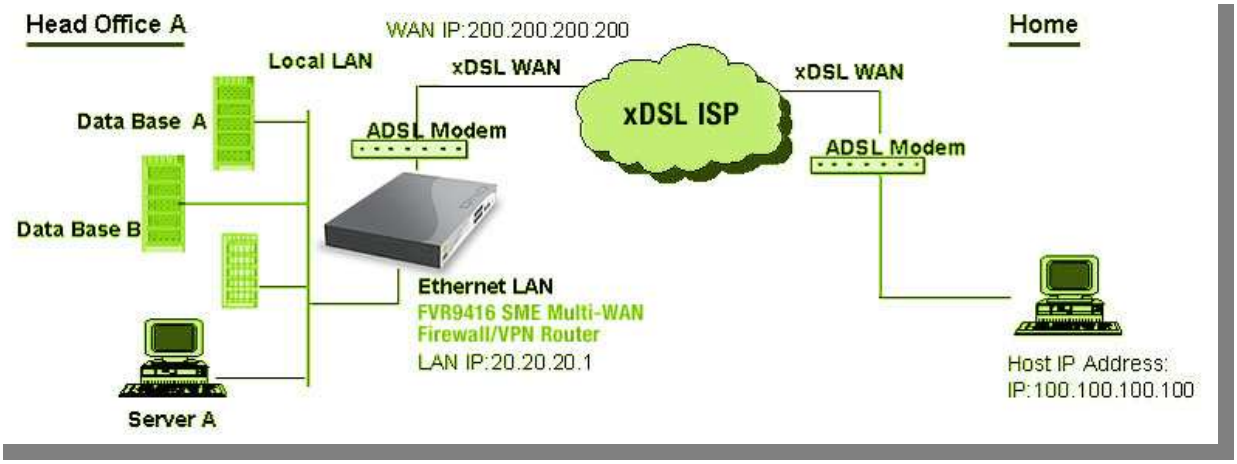


VPN Setting： VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	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 Address	100.100.100.100	200.200.200.200
Remote Security Group Type	IP	Subnet
Remote Security Group Type➔ IP Address	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	

VPN Environment Sample 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
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	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 Address		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 Address	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		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	

附录三：常见问题解决

注意！

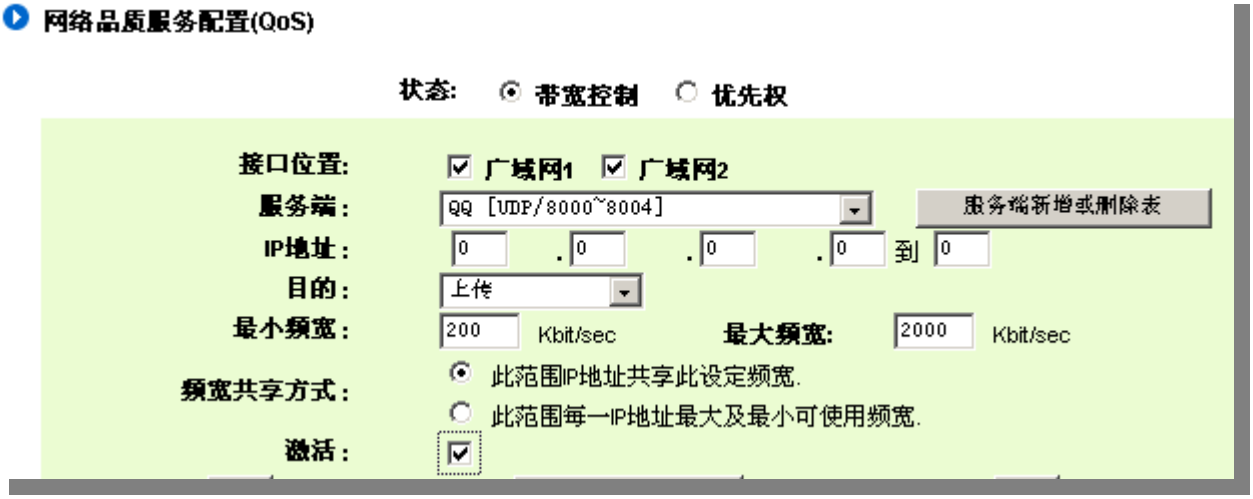
以下是几个常见问题的解决方法，如果有其它的问题出现可以在 http://www.qno.cn 讨论区查找信息以及联系技术服务人员，具体方法可以参考附录五：Qno 技术支持资讯查找相关信息以及联系相关技术服务人员，以取得更详细的资料参考。

（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。



（2） 挡基本 BT 下载方式

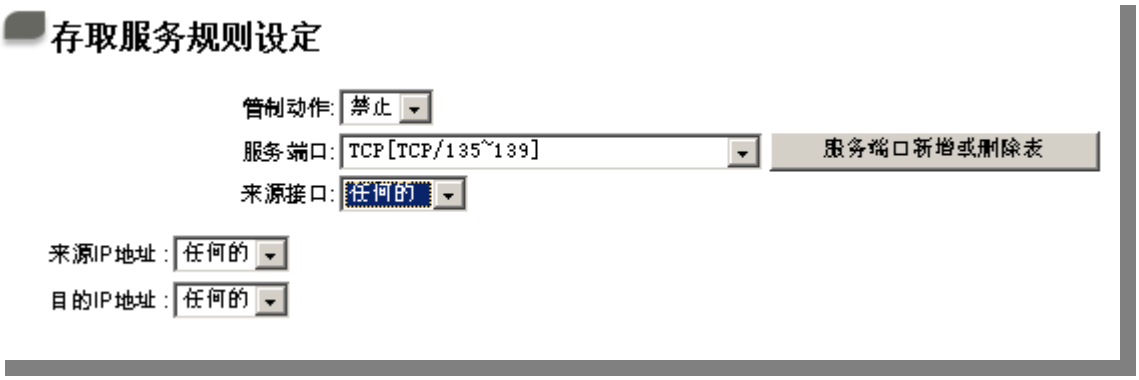
若您想要封锁 BT 种子，不让用户下载，您可以直接在“防火墙配置”有一个“网页内容管制设定”选择“开启网页内容管制功能”后将激活网页字符串管制，打入“.torrent”就可以防止用户下载种子。

（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:



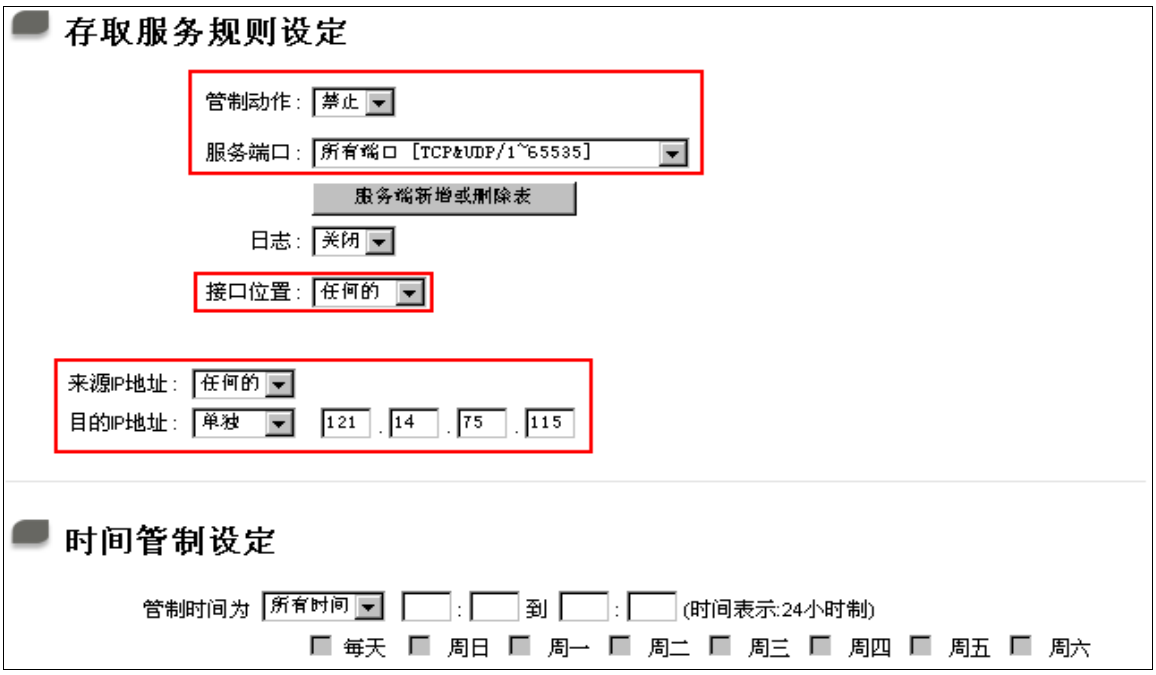
用同样的方法添加好 UDP[UDP135~139]以及 TCP[445~445]端口。

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”。



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。

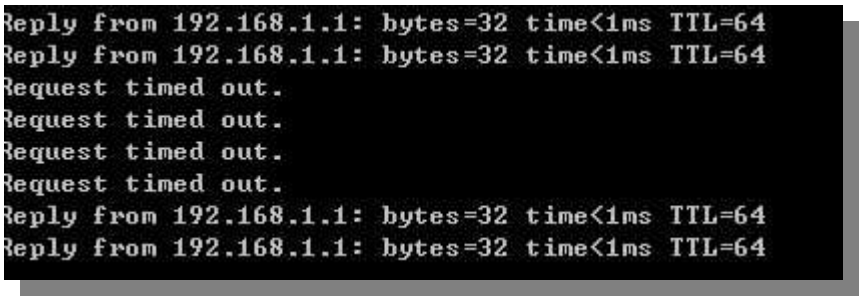
这种病毒的程序如 PWSteal.lemir 或其变种，属于木马程序/蠕虫类病毒，Windows 95/98/Me/NT/2000/XP/2003 将受到影响，病毒攻击的方式对影响网络连接畅通来看有两种，对 VPN QOS 安全路由器的 ARP 表的欺骗和对内网 PC 网关的欺骗，前者是先截获网关数据，再将一系列的错误的内网 MAC 信息不停的发送给 VPN QOS 安全路由器，造成 VPN QOS 安全路由器发出的也是错误的 MAC 地址，造成正常 PC 无法收到信息。后者 ARP 攻击是伪造网关。它先建立一个假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的 VPN QOS 安全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

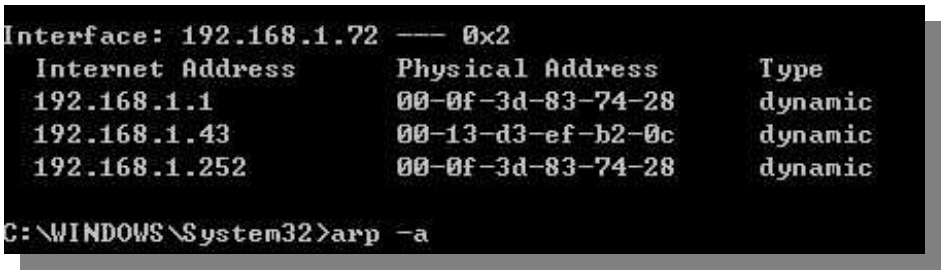
2）. ARP 的判断

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，您找到出现问题的电脑点开始运行进入系统的 DOS 操作。pingVPN 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。



内网 pingVPN 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。



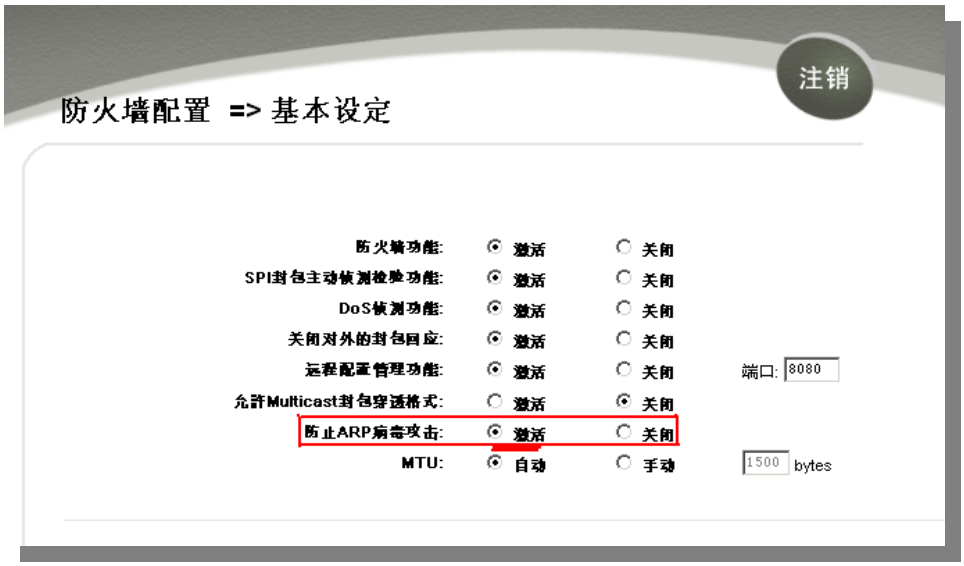
可以看出 192.168.1.1 地址和 192.168.252 地址的 IP 的 MAC 地址都是 00-0f-3d-83-74-28，很显然，这就是 ARP 欺骗造成的。

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。

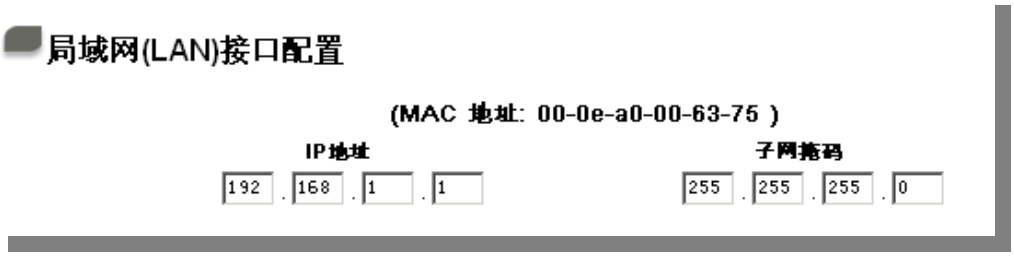
a)、激活防止 ARP 病毒攻击：

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。

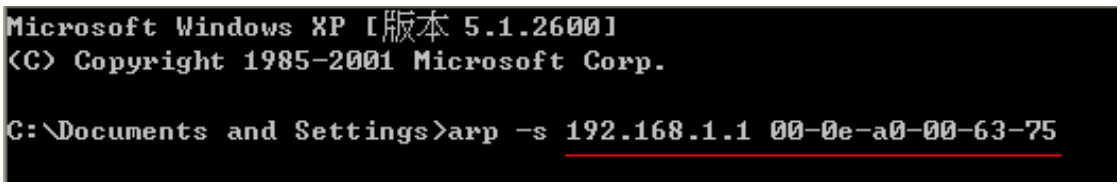


b)、对每台 pc 上绑定网关的 IP 和其 MAC 地址

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 0-0e-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

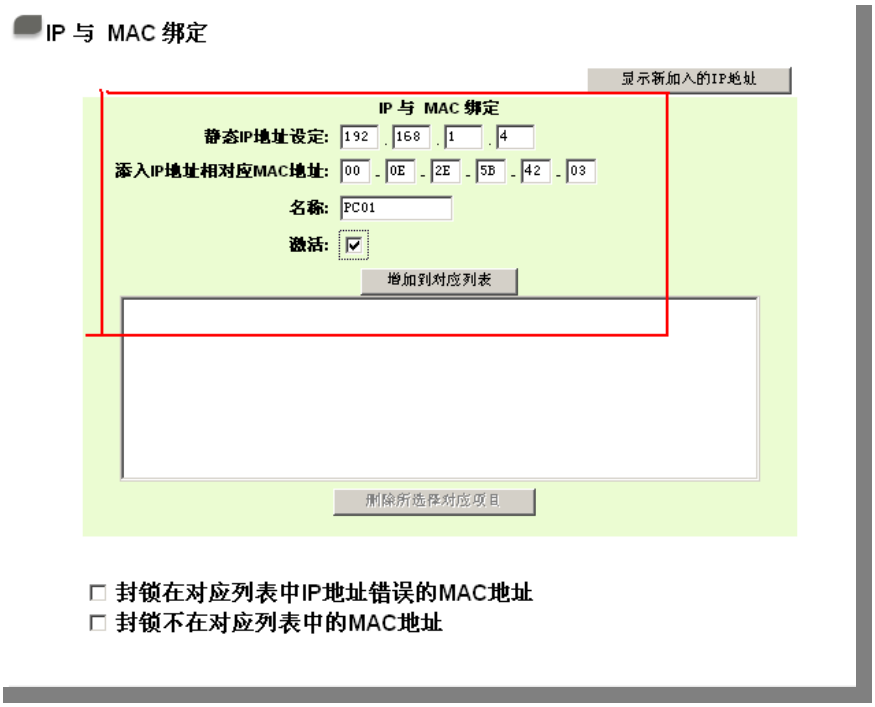
arp -sVPN QOS 安全路由器 LAN IP　VPN QOS 安全路由器 LAN MAC

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。

其它的路由器用户的解决方案也是要在路由器和 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：

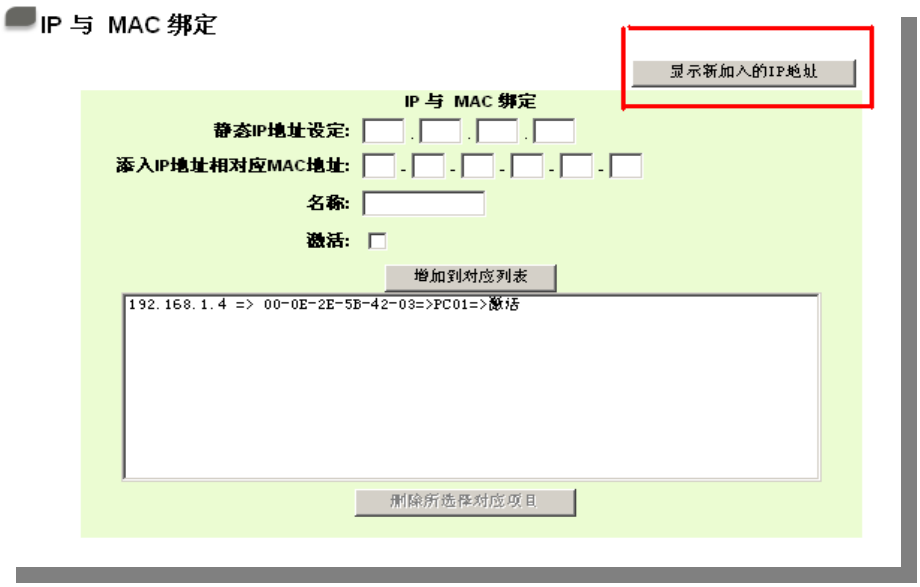
进入“DHCP 功能”的“DHCP 配置”，在这个页面的右下可以看到一个“IP 与 MAC 绑定”您可以在此添加 IP 与 MAC 绑定，输入相关参数，在“激活”上点“ √ ”选再“添加到对应列表”，重复操作添加内网里的其它 IP 与 MAC 的绑定，再点页面最下的“确定”。



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

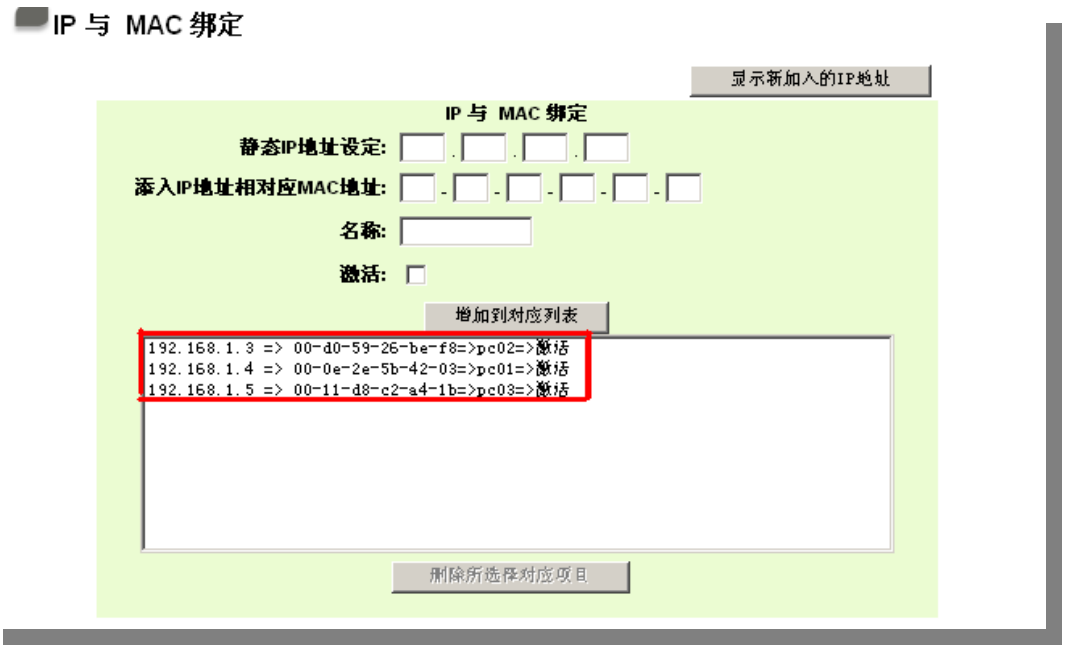
样操作需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，操作会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

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。

此时您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.cn/forum

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.cn/web/where_buy.asp

技术中心：

电邮：QnoFAE@qno.com.tw