



# 1WAN 4LAN VPN QoS Wireless Router

## VPN QoS 无线安全路由器

具负载均衡，带宽管理，网络安全等功能

简体中文使用手册

目錄

一、简介 .....	6
二、安全路由器设置操作流程 .....	8
2.1 系统性设置流程的需要 .....	8
2.2 设置流程表 .....	8
三、硬件安装 .....	10
3.1 安全路由器 LED 显示灯 .....	10
3.2 安全路由器的网络连接 .....	11
四、登录路由器 .....	12
五、确定设备规格、状态显示以及登录密码和时间的设置 .....	14
5.1 首页显示 .....	14
5.2 登录密码及时间的修改和设置 .....	18
六、广域网络连线设置 .....	21
6.1 网络设置 .....	21
6.2 多 WAN 设置 .....	35
6.3 3G/3.5G USB 上网卡的增益功能 .....	51
七、IPv6 设定方式 .....	58
7.1 设定 IPv6 网络 .....	58
7.2 设定局域网自动取得 IPv6 地址 .....	62
八、内部局域网络设置 .....	65
8.1 端口状态即时显示 .....	65
8.2 DHCP 发放 IP 服务器 .....	65
8.3 DHCP 状态显示 .....	67
8.4 IP 及 MAC 地址绑定 .....	70
九、Wireless 无线网络 .....	74
9.1 基本设定 .....	75
9.2 安全设定 .....	77
9.3 客户端联机清单 .....	85
9.4 無線流量統計 .....	86
十、QoS 带宽管理功能 .....	87
10.1 带宽设置(QoS) .....	87
10.2 会话数管理 .....	97
十一、防火墙设置 .....	99
11.1 基本设置 .....	99
11.2 访问规则设置 .....	102

11.3 网站内容过滤 .....	107
<b>十二、流行路由 .....</b>	<b>112</b>
12.1 上网行为管理 .....	112
12.2 L7 VIP 优先通道 .....	119
12.3 L7 QoS 带宽管理 .....	127
12.4 自定义应用程序 .....	133
<b>12.6 数据库更新 .....</b>	<b>136</b>
<b>十三、VPN 虚拟专用网设置 .....</b>	<b>140</b>
13.1 VPN 虚拟专用网 (VPN) .....	140
13.2 QVM VPN 功能设置 .....	168
<b>十四、其它进阶高级功能设置 .....</b>	<b>170</b>
14.1 DMZ/虚拟服务器 .....	170
14.2 UPnP 通讯协议 .....	173
14.3 路由通讯协议 .....	174
14.4 一对一 NAT 对应 .....	176
14.5 DDNS-动态域名解析 .....	178
14.6 广域网接口 MAC 地址设置 .....	182
<b>十五、工具程序功能设置 .....</b>	<b>183</b>
15.1 在线联机测试 .....	183
<b>15.2 系统软件更新 .....</b>	<b>184</b>
15.3 系统设置参数存储 .....	185
15.4 网络管理设置(SNMP) .....	186
15.5 系统恢复 .....	187
15.6 产品功能许可证密钥 (未来支持) .....	188
<b>十六、日志功能设置 .....</b>	<b>190</b>
16.1 系统日志 .....	190
16.2 系统状态实时监控 .....	194
16.3 流量统计 .....	195
16.4 特定 IP 及端口状态 .....	197
<b>附录一：常见问题解决 .....</b>	<b>199</b>
(1) QQ 容易掉线问题 .....	199
(2) 阻挡基本 BT 种子下载方式 .....	201
(3) 冲击波及蠕虫病毒的防制 .....	202
(4) 阻止 QQLive 视频直播设置 .....	204
<b>附录二：Qno 技术支持资讯 .....</b>	<b>206</b>

## 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”。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。

## 一、简介

IPSec VPN 防火墙 (以下称防火墙) 是因应高速网络的 VPN、防火墙需求, 所研发的一款全功能 VPN 防火墙。支持 IPSec、PPTP, 针对企业的分支部、第三方、行动外点、家庭办公等各式 VPN 运用环境, 提供全面性的解决方案。适用于各国多运营商及不同的带宽环境, 并提供硬件镜像端口、智能型带宽管理、多 WAN 负载均衡、线路备援、强效防火墙、虚拟路由等功能。

具备 1~2 个 10/100 Base-T/TX 以太网(RJ45) WAN 端端口, 并具有高效能线路负载平衡模式的功能, 达到对外联机的流量负载平衡。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。区域端内建 3~4 个 10/100 Base-T/TX 以太网(RJ45) LAN 端端口, Auto MDI/MDI-X 10/100Mbps 以太网网络交换器, 每个端口都可以连接额外的交换器以连接更多的上网设备, 加速企业网络效能, 带宽成长空间大。

强效的防火墙系统, 满足多数企业对防御外部网络攻击的市场需求。主动式封包检测功能, 经由对网络层联机的动态检测, 拒绝或阻挡非标准通信协议的联机要求。只需单向启动各式黑客攻击、蠕虫病毒、ARP 攻击防护功能, 即可简易完成配置, 有效防止内外网恶意攻击, 确保网络安全。防火墙系统除了 NAT 之外, 还具备有防止阻断服务攻击。功能完整的存取规则设定, 可让管理者选择应该禁止或开放存取的网络服务, 限制或禁止区域内用户的网络权限, 以避免占用网络资源或是不当使用而遭受潜在的危机。

独特的 QoS 带宽管理功能, 可以让管理者对有限的网络资源做合理而且有效的分配。功能强大但是设定简单, 用户可以直接在「动态智能 QoS」功能中, 简单完成平时的带宽限制, 弹性的「动态智能 QoS」不仅能在网络巅峰时期限制带宽, 还能在网络空闲时自动释放带宽, 达到带宽的最佳分配。如此之外, 也能够「QoS 带宽管理」依据 IP、服务、通讯端口做更细致的设定。简单的说, 就是在维持带宽秩序的前提下, 将带宽做最大的利用, 达到最佳的效果。

支持智能型、指定路由与策略路由等三种带宽负载均衡模式, 提供弹性灵活的网络联机需求设置, 来进行流量的负载均衡控制, 可保证所有线路畅通。策略路由设置简化无需导入 IP 地址列表, 自动判别对外网络封包, 并依据不同网络运营商分流, 确保跨网联机反应快速、通行无碍, 可汇聚不同运营商的线路带宽, 作负载均衡控制, 大大提升网络资源运用的灵活度。

网络地址转换(NAT) 除了可以做私网 IP 与公网 IP 转换, 让您只需要一个公网 IP 就可以让多人同时连上网络。区域内的 IP 地址支持 2 个 Class C 等级, DHCP 自动分配 IP, 以及简单勾选的 IP 与 MAC 地址绑定让网络环境架构具有弹性, 易于规划管理。

IPSec VPN 支援 DES、3DES、AES-128、AES192、AES256 加密, MD5、SH1 认证, IKE Pre-Share Key 设定的密钥交换。支持 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。另具备 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。

而 QVM 是 Qno 专为商用环境所研发的一 SmartLink IPSec VPN。企业总部的服务器端只需输入 VPN 服务器 IP、用户名、密码等三个参数，即可完成 IPSec VPN 配置。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。

此说明书用以说明每一个功能的设定方法与细节，若是您对于路由器如何连上网络的设定并不十分清楚，建议您先阅读“快速安装说明”，可以让您快速的将路由器连上网络，并在必要时取得技术人员的远程支持。您可上网 [www.qno.cn](http://www.qno.cn) 进行在线登录，以取得最新侠诺产品信息及应用实例，更加善用您的侠诺产品。

## 二、安全路由器设置操作流程

本章节介绍用户整体设置安全路由器操作流程，通过对安全路由器多 WAN 设置流程的了解可以很轻松的设置我们的网络，来有效的管理我们的网络，使安全路由器达到应有的功能，使安全路由器的效能达到最高。

### 2.1 系统性设置流程的需要

用户可以通过以下操作流程设置网络，能够使网络有效利用带宽，网络效能达到理想的效果，同时可以阻断一些攻击与预防一些安全隐患，通过流程设置更加方便用户的安装与操作，简化维护管理的难度，使得用户的网络设置一次到位。设置主要流程如下：

- 1、 硬件安装。
- 2、 登录设置窗口。
- 3、 确定设备规格及进行密码和时间设置。
- 4、 进行广域网联机的设置：进行内部联机的设置。
- 5、 进行局域网联机的设置：实体线路设置及 IP 地址设置
- 6、 进行 QoS 带宽管理设置：防止带宽占用情况。
- 7、 进行防火墙设置：预防攻击及不当存取网络资源。
- 8、 其它特别设置：开放服务器、UPnP、DDNS、MAC 克隆。
- 9、 管理维护的设置系统日志、SNMP、及设置参数备份注销设置窗口。
- 10、 VPN 虚拟专用网
- 11、 注销设置窗口

### 2.2 设置流程表

下表主要阐述每个设置流程相对应的安全路由器管理内容以及此设置所达到的目的，如需详细了解每步过程以及后面章节介绍所对应的内容，可参考（附录一、设置界面及使用手册章节对照）。

#	设置	内容	目的
1	硬件安装	构建用户需要的网络	根据用户实地网络的要求来安安全路由器硬件。
2	登录设置窗口	从计算器 Web 接入安全路由器设置窗口，了解系统信息	登录安全路由器的 Web 管理页面。



3	确定设备规格	确定产品软件版本以及路由工作情况	确定安全路由器规格，系统软件版本，以及安全路由器工作状态。
	进行密码及时间设置	设置时间及修改密码	安全的考虑修改登录密码。 设置安全路由器时间与广域网络同步。
4	进行广域网联机的设置	确定广域网线路设置、带宽调配、及协议绑定	连接广域网络，通过带宽的设置等能更好的利用带宽，优化数据转发能力。
5	进行局域网联机的设置	内部用户 IP 的分配群组及管理	应地区需求提供功能，弹性提供固定 IP/DHCP 自动 IP 地址分配，方便用户在不同网络环境的需要。
6	进行 QoS 带宽管理设置，防止带宽占用情况的发生	广域网端口、内部用户或应用流量及联机数的限制	确保网络重要信息不致延迟、确保网络重要应用服务联机顺畅；进一步针对现有的带宽进行管理运用，让有限的带宽资源发挥最大的效用。
7	进行防火墙设置，预防攻击及非法访问网络资源	攻击阻挡、访问规则及网页存取限制	当内网用户使用 BT、点点通影响其它人上网、员工上班时间不正当上网以及使用 MSN、QQ、影响工作效率；当网速因被黑客攻击而受影响或内网用户常被蠕虫及 ARP 软件所苦；网管可依据需求设置内外网络存取规则，以进一步管控员工个别上网行为。
8	其它特别设置：开放服务器、UPnP、DDNS、MAC 克隆	针对内部设置开放服务器、UPnP、路由模式、多广域网 IP、DDNS、Mac 克隆	高级管理设置完成对网络的更高一步要求，构建内部开放服务器，虚拟服务器，UPnP 通讯协议的设置，设置动态路由或者静态路由，一对一 NAT 设置，动态域名解析服务与 Mac 地址克隆。
9	管理维护的设置：系统日志、SNMP、及设置参数备份	安全路由器工作情况监测、系统参数的备份	网管可借此功能查看系统日志、即时监控系统状态及内外流量，确保内网运作无误。
10	VPN 虚拟专用网、QVM VPN 功能设置	针对 VPN 联机功能进行设置，包括 PPTP、QVM VPN	借由多种而简便的 VPN 设置，使各类的 VPN 虚拟专用网应用环境，能有效并顺利地运作
11	注销设置窗口	离开设置窗口	注销退出安全路由器 Web 管理页面。

下面我们就根据这个流程来设置完成我们的网络设置。

### 三、硬件安装

本章介绍产品的硬件接口以及实体安装。

#### 3.1 安全路由器 LED 显示灯

##### LED 灯号说明

LED	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。
WAM/LAN Link/Act	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/接收数据包数据传输
WLAN	绿灯	绿灯亮：无线网络工作中 绿灯闪烁：无线网络传送/接收数据包数据传输
WPS	绿灯	绿灯亮：WPS 模式工作中

##### 硬件恢复 (Reset) 按键

动作	意义
点击 Reset 按钮 5 秒	热开机，重新启动安全路由器 DIAG 灯号：橘色灯号慢慢闪烁
点击 Reset 按钮 10 秒以上	恢复原出厂默认值 DIAG 灯号：橘色灯号快闪

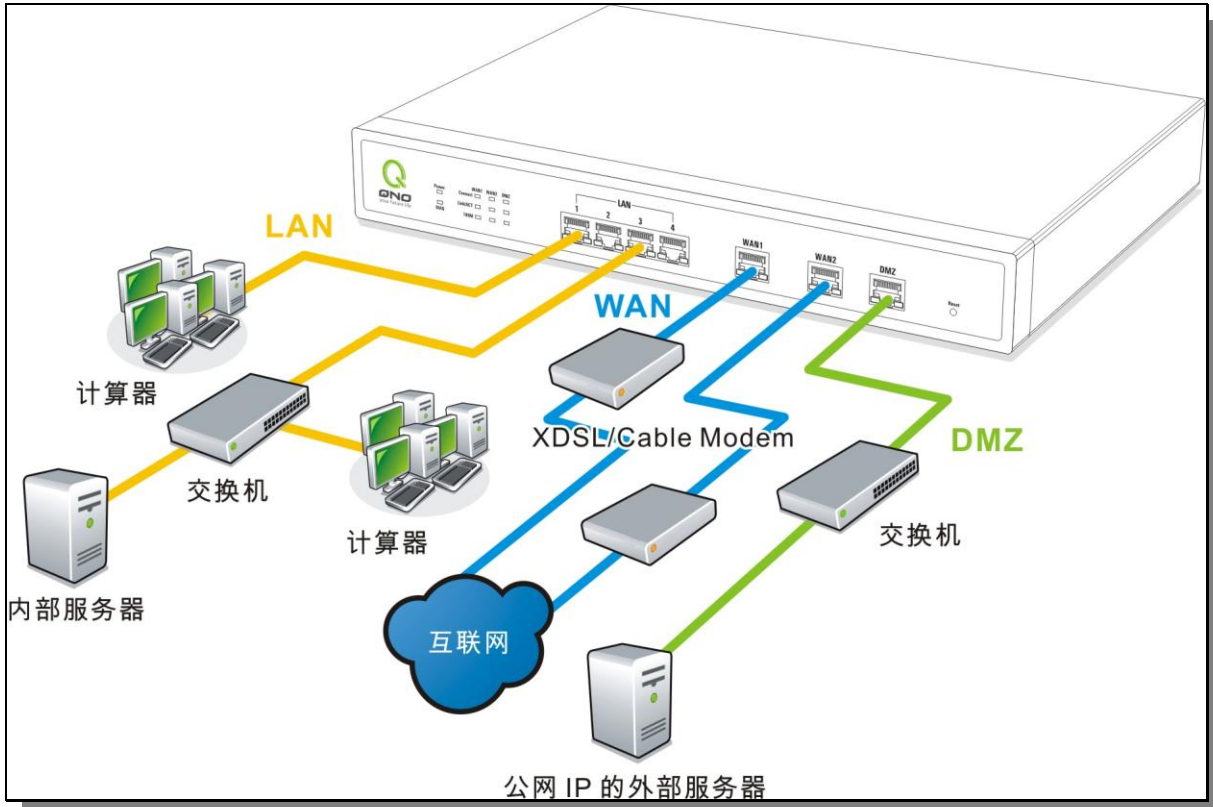
##### 系统内建电池

安全路由器内建有系统时间的电池，此电池的寿命约为 1~2 年，当电池已经无法充电或是使用寿命到达后，安全路由器将无法记录时间或是连接互联网同步 NTP 时间服务器。您必须与您的供应商联系，以便取得更换电池技术。

**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！

### 3.2 安全路由器的网络连接



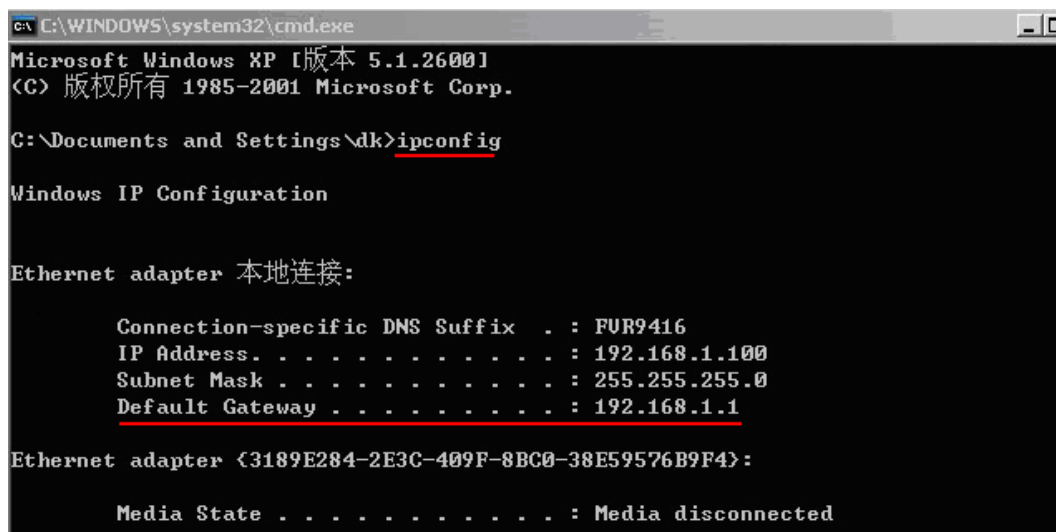
广域网络联机：连接 xDSL Modem 或光纤盒来连通互联网。或是连接交换机或外部路由器、防火墙来连通您现有的网络。

局域网络联机：连接交换机或计算机。若局域网端口有支持镜像功能，请在“端口管理”中做设置，设定完成即可直接将监控或过滤服务器接在此端口使用

#### 四、登录路由器

本章主要是在客户连接好路由器后，通过连接路由器的计算机登录路由器的 Web 管理页。

首先在连接到路由器 LAN 端的计算机（确定计算机是自动获得 IP 地址）上的 DOS 下查找路由器的 IP 地址，点开始→运行，输入 cmd 进入 DOS 操作，再输入 ipconfig→确认，查到默认网关（Default Gateway）地址如图，192.168.1.1。确认默认网关也就是路由器的默认 IP 地址。



```
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\dk>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : FUR9416
    IP Address. . . . .                : 192.168.1.100
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.1.1

Ethernet adapter {3189E284-2E3C-409F-8BC0-38E59576B9F4}:

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

#### 注意！

当“ipconfig”不能获得 IP 地址以及默认网关的情况，或者获得的 IP 地址为 0.0.0.0 以及 169.X.X.X 的情况，就是路由器并没有分配到 IP 地址，建议用户检查线路是否有问题，计算机网卡是否接好等。

然后开启网页浏览器 (如 IE)，在网址栏输入 192.168.1.1 (路由器的默认网关)，会出现以下的登录窗口：



路由器默认的使用者名称(User Name)与使用者密码(Password)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，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，将无法再登录至路由器的设定窗口，必须点击面板上的 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。

登录后，就会显示路由器的 Web 管理页面，在其页面的右上角选择路由器操作的语言模式，选中的图标将变成蓝色，这里选择“简体”中文版本)，如图。



## 五、确定设备规格、状态显示以及登录密码和时间的设置

本章介绍登录软件设置窗口后，进入首页可以了解到的设备规格以及设备工作状态信息，还有因安全考虑需要用户即时修改登录密码与系统时间设置。

### 5.1 首页显示

首页显示安全路由器目前系统所有参数以及状态显示信息。

#### 5.1.1 系统信息

##### ▶ 广域网状态

接口位置	广域网2	广域网1
IP地址	220.130.188.40	0.0.0.0
默认网关	220.130.188.33	0.0.0.0
DNS 服务器	168.95.1.1 0.0.0.0	0.0.0.0
会话数	3	0
下载带宽使用率(%)	0	0
上传带宽使用率(%)	0	0
动态域名服务	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dyndns 关闭 3322 关闭 Qnoddns 关闭
QoS带宽管理	0条规则	0条规则
手动连接	<input type="button" value="释放"/> <input type="button" value="更新"/>	<input type="button" value="释放"/> <input type="button" value="更新"/>

- IP 地址：** 此为显示安全路由器 WAN 端目前的 IP 地址信息。
- 默认网关：** 此为显示运营商分配给安全路由器 WAN 的网关 IP 地址信息。
- DNS 服务器：** 此为显示安全路由器的 DNS 的 IP 地址信息。
- 会话数：** 此为显示安全路由器每个 WAN 目前的会话数目。
- 下载带宽使用率：** 此为显示安全路由器每个 WAN 目前的下载带宽使用比例。
- 上传带宽使用率：** 此为显示安全路由器每个 WAN 目前的上传带宽使用比例。
- 动态域名服务：** 此为显示安全路由器的 DDNS 是否启动的状态信息。系统默认此功能为关闭。
- QoS 带宽管理：** 此为显示安全路由器的网络质量服务(QoS)是否开启。
- 手动连接：** 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。  
使用者可以点击释放按钮去做释放运营商所核发的 IP 地址，以及点击更新按钮去做更新运营商所核发的 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“连接”与“中断”。

### 5.1.2 硬件端口状态实时显示

#### ▶ 端口即时状态

端口号	1	2	3	
端口	局域网			
状态	连线	激活	激活	

端口号	Internet	Internet	USB	USB
端口	广域网1	广域网2	USB1	USB2
状态	连线	激活	激活	激活

此窗口会显示系统各端口目前实时状态：(连接-已经连接，激活-此端口处于开启状态，关闭-此端口处于关闭状态)。您可以点击此状态按钮，在弹出的窗口中查看各端口更详细的资料显示。如下图：

广域网1 信息

**摘要信息：**

网路连接状态	10Base-T / 100Base-TX
接口位置	广域网1
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
连接速率	100 Mbps
半双/全双工模式	全双工
自动翻转功能	激活

**流量实时状态：**

接收数据包统计	0
数据包接收Byte数量	107885800
传送数据包统计	0
数据包传送Byte数量	65509869
错误数据包统计	0

刷新
关闭

此表会显示目前该端口设置状态，如网路连接状态(10Base-T/100Base-TX)，接口位置(广域网/局域网)，线路连接状态(激活/关闭)，端口设置状态(端口激活/端口关闭)，优先级设置(高级/一般)，网络连接速率

(10Base-T/100Base-TX)，工作模式(半双工/全双工)，以太网自动翻转功能(激活/关闭)。于此项目表格中，会显示此端口的接收和传送的数据包以及数据包传送 Byte 数及数据包错误率等并计算总数量。

### 5.1.3 系统信息

#### ▶ 系统信息

局域网网关/子网掩码	10.10.10.1/255.255.255.0	序列号	
工作模式	NAT模式	软件版本	2.1.0.1-Qno (Jun 26 2008 20:38:08)
运作时间	7天 7时 10分 25秒	当前时间	Fri Jul 4 2008 18:21:06

**局域网网关地址：** 此为显示安全路由器本身的 LAN 端目前 IP 地址，系统默认为 192.168.1.1。

**工作模式：** 此为显示安全路由器的目前工作模式(可为 NAT 模式或是路由模式)。

系统默认此功能为 NAT 模式。

**运作时间：** 此为显示安全路由器目前已经开机的时间。

**主机序列号：** 此为显示安全路由器的产品序号。

**软件版本：** 此为显示安全路由器 目前使用的硬件版本。

**当前时间：** 此显示安全路由器 目前正确时间，但必须注意，您需要正确设置与远程 NTP 服务器的时间同步后才会正确显示。

### 5.1.4 防火墙状态

#### ▶ 防火墙状态

防火墙	状态
SPI数据包检测	激活
防止DoS攻击功能	激活
阻止广域网回应功能	关闭
防止ARP病毒攻击	关闭
远程管理功能	激活
访问规则设置	7条规则

**SPI 数据包检测：** 此为显示安全路由器的 SPI 主动数据包侦测过滤功能选项是否激活(激活/关闭)。

系统默认此功能为激活。



**防止 DoS 攻击功能：**此为显示安全路由器的阻断来自网络上的 DoS 攻击功能选项是否开启(激活/关闭)。

系统默认此功能为激活。

**阻止广域网回应功能：**此为显示安全路由器的阻断来自网络上的 ICMP-Ping 的响应功能选项是否激活

(激活/关闭)。系统默认此功能为激活。

**防止 ARP 病毒攻击：**此为显示安全路由器防止 ARP 攻击的功能选项是否激活(激活/关闭)。

系统默认此功能为关闭。

**远程管理功能：**此为显示安全路由器的远程管理功能选项是否启动(激活/关闭)。系统默认此功能为关闭。

**访问规则设置：**此为显示安全路由器的访问规则设置的数目。

### 5.1.5 VPN 虚拟专用网状态

#### ▶ VPN虚拟专用网状态

VPN配置	状态
已使用的隧道数目	0
可使用的隧道数目	150
PPTP服务器	关闭

**VPN 设置状态：**此为显示安全路由器的 VPN 功能选项内容信息。

**已使用的隧道数目：**此为显示安全路由器的 VPN 功能目前已经设置的隧道数量。

**可使用的隧道数目：**此为显示安全路由器的 VPN 功能目前可使用的隧道数量。

**PPTP 服务器：**显示 PPTP 服务器是否开启。

### 5.1.6 系统日志设置状态显示

#### ▶ 系统日志配置状态

发送到日志服务器	关闭
发送到电子邮箱	关闭

**发送到日志服务器：**此为显示您所设置安全路由器日志记录接收的服务器。

**发送到电子邮箱：**此为显示您所设置的 E-mail 地址，安全路由器的日志记录经由此 E-mail 传送出去。  
(未来支持)

**E-Mail 的链接将会连到系统日志设定窗口中：**

1. 若您没有设定电子邮件服务器于系统日志设定中，将显示“**邮件无法传送，因为没有配置 SMTP 服务器正确地址**”——表示您没设定电子邮件服务器所以无法发送系统日志电子邮件。
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，将显示“**邮件设定已经配置**”——表示您的电子邮件服务器已经设置，但是日志尚未达到设定传送的条件时。
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“**邮件设定已经配置并正常发送**”——表示您的电子邮件服务器已经设置，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送出去时，它将显示“**邮件不能发送，请使用正确的配置**”——电子邮件服务器已经设置，但是无法传送出去，可能是设定有问题。

## 5.2 登录密码及时间的修改和设置

### 5.2.1 密码设置

当您每次登录安全路由器的设置窗口时，必须输入密码。安全路由器的用户名和密码出厂值均为“admin”。考虑安全因素，我们强烈建议您务必在第一次登录并完成设置之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录安全路由器的设置窗口，必须点击安全路由器前面板上的 **Reset** 按键十秒以上，恢复到出厂值，所有设置值将需要重新设置。

#### 密码设置

用户名：	admin
密码：	<input type="password"/>
更改用户名：	admin
输入新密码：	<input type="password"/>
再次输入新密码：	<input type="password"/>

确定

取消

- 用户名： 出厂初始值默认为 admin。
- 密码： 填写原本旧密码（出厂初始值默认为“admin”）。
- 更改用户名： 输入新用户名，如 Qno。
- 输入新密码： 填写要更改的新密码。
- 再次输入新密码： 再次填写更改的新密码以确认。

- 确定：**                    点击此按钮“确定”存储刚才所修改设置的内容参数。
- 取消：**                    点击此按钮“取消”清除刚才所修改设置的内容参数，此操作必须于“确定” 存储动作之前才会有效。

### 5.2.2 系统时间设置

安全路由器可以设置时间，让您在查看安全路由器的系统纪录或设置网络存取的时间设置时，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网络资源的依据条件。您可以选择与安全路由器内建的外部时间服务器(NTP 服务器)取得时间同步，或自己设置正确时间参数。

与外部时间服务器同步：安全路由器有内建的网络时间服务器，会自动同步时间。

- 与外部时间服务器同步
- 手动配置时间

时区选择：	Hong Kong (GMT+08:00)
夏令时：	<input checked="" type="checkbox"/> 激活 从 3 月 28 日 到 10 月 28 日
外部时间服务器地址：	<input type="text"/>

- 时区选择：** 点开下拉菜单选择您所在地点的时区以正确显示当地时间。
- 夏令时：** 若是您所的地区有实施日光节约时间，可以输入实施的日期范围，安全路由器会在此日期范围自动调整时间。
- 外部时间服务器地址：** 若是您自己有偏爱使用的时间服务器，可以输入该服务器的地址。
- 确定：** 点击此按钮即会存储刚才所变动的修改设置内容参数。
- 取消：** 点击此按钮即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

手动设置时间：在这输入正确的时间：小时、分钟、秒、月份、日与年份。

<input type="radio"/> 与外部时间服务器同步												
<input checked="" type="radio"/> 手动配置时间												
<table border="0"> <tr> <td><input type="text" value="19"/></td> <td>时</td> <td><input type="text" value="7"/></td> <td>分钟</td> <td><input type="text" value="1"/></td> <td>秒</td> </tr> <tr> <td><input type="text" value="7"/></td> <td>月</td> <td><input type="text" value="4"/></td> <td>日</td> <td><input type="text" value="2008"/></td> <td>年</td> </tr> </table>	<input type="text" value="19"/>	时	<input type="text" value="7"/>	分钟	<input type="text" value="1"/>	秒	<input type="text" value="7"/>	月	<input type="text" value="4"/>	日	<input type="text" value="2008"/>	年
<input type="text" value="19"/>	时	<input type="text" value="7"/>	分钟	<input type="text" value="1"/>	秒							
<input type="text" value="7"/>	月	<input type="text" value="4"/>	日	<input type="text" value="2008"/>	年							
<input type="button" value="确定"/> <input type="button" value="取消"/>												

点击“确认”按钮即会存储刚才所修改的设置内容参数，点击此按钮“取消”即会清除刚才所修改的设置内容参数，此操作必须于确认存储动作之前才会有效。

## 六、广域网络连线设置

本章节讲述基本的广域网络设置，对大多数的用户来说，通过本章节完成基本的设置已经足够连接网络。网络的连接需要一些运营商所提供的进一步详细信息。其详细项目设置，请参考以下各节说明：

### 6.1 网络设置

<b>主机名称：</b>	<input type="text"/>	(某些 ISP 要求输入)
<b>网域名称：</b>	<input type="text"/>	(某些 ISP 要求输入)

---

**▶ 局域网(LAN)接口配置**

<b>MAC 地址设定</b> 00 - 17 - 16 - 99 - 45 - 20 (预设值:00-17-16-99-45-20)	
IP 地址 : 192 . 168 . 0 . 1	子网掩码 : 255 . 255 . 252 . 0
多重网段配置	关闭

---

**▶ 连线类型配置**

端口	线路连线类型	配置
广域网1界面	PPPoE 设定 (ADSL拨号使用者)	<a href="#">编辑</a>
广域网2界面	PPPoE 设定 (ADSL拨号使用者)	<a href="#">编辑</a>

---

**激活此选项会设定 DMZ 端口**

#### 6.1.1 主机名称及域名

<b>主机名称</b>	<input type="text" value="SMB"/>	(某些ISP要求输入)
<b>网域名称</b>	<input type="text" value="smb.com"/>	(某些ISP要求输入)

可输入安全路由器的名称（主机名称）以及网域名称，此设置在大多数环境中不需要做任何设置即可使用，除非特殊运营商需求！

### 6.1.2 局域网（LAN）接口设置

此为设置安全路由器的 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，您可以依照实际网络架构做变动。

**局域网(LAN)接口配置**

MAC 地址设定 00 . 17 . 16 . 99 . 45 . 20 (预设值:00-17-16-99-45-20)	
IP 地址 : 192 . 168 . 0 . 1	子网掩码 : 255 . 255 . 252 . 0
多重网段配置	关闭

[IP 整合管理](#)

#### IP 整合管理：

IP 整合管理的设置窗口可以设定局域网(LAN) IP、动态 IP(DHCP)发放范围。

Unified IP Management - Windows Internet Explorer  
http://61.222.81.94/ip\_management.htm

**区域网络(LAN)设定**

設備IP地址 192 . 168 . 1 . 1      子網路遮罩 255 . 255 . 255 . 0

多個子網設定  多個子網

區域網路IP位址 [ ][ ][ ][ ]  
子網路遮罩 [ ][ ][ ][ ]

[增加到對應表列](#)

[刪除選中的子網](#)

---

**動態IP**

啟用DHCP伺服器

	子網域1	子網域2
DHCP伺服器	<input checked="" type="checkbox"/> 啟用	<input type="checkbox"/> 啟用
起始IP位址	192 . 168 . 1 . 100	192 . 168 . 2 . 100
終止IP位址	192 . 168 . 1 . 149	192 . 168 . 2 . 149

完成      網際網路 | 受保護模式: 關閉      100%

### 区域网络(LAN)设定：

系统默认 LAN IP 为 192.168.1.1，子网掩码为 255.255.255.0，您可以依照实际网络架构做变动。

### Multiple-Subnet 多子网配置：

勾选“多个子网”，并填入您想要增加的子网 IP 地址以及子网掩码，即可增加新的子网在局域网。此功能是将不同于路由器局域网段的其他网段 IP 加入到路由器认可的局域网段中，这样局域网中的 PC 若是已经设定的 IP 所在的网段不同于路由器的局域网段也可以直接上网。举例来说，原来内部环境已经有多组不同的 IP 网段，例如 192.168.3.0，192.168.20.0，192.168.150.0 等等，将这些网段加入到子网中，则这些网段的内部计算机不需做任何修改就可以上网，这里可以依照您的实际网络架构运作。

### 动态 IP：

路由器有一组 Class C 的 DHCP 服务器，默认值是激活，可以提供局域网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，就可从路由器自动取得 IP 地址，管理方便。

**起始 IP 地址：** 系统默认从 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 192.168.1.149 的 IP 地址为最后发放 IP，也就是说可供 50 台计算机自动取得 IP 地址。

### 6.1.3 广域网络 WAN 及非军事区设置

#### 广域网网络连接型态设置：

#### 广域网线路配置

接口位置	连接类型	配置
广域网1	自动取得 IP 地址	<a href="#">编辑</a>
广域网2	指定 IP 地址	<a href="#">编辑</a>

**接口位置：** 广域网连线所在 WAN 接口位置。

**线路连接类型状态：** 此项显示该广域网口目前设置的联机状态。安全路由器提供五种联机状态设置：自动取得 IP 地址；固定 IP 地址；PPPoE 拨号联机；PPTP 拨号联机以及透明桥接模式。

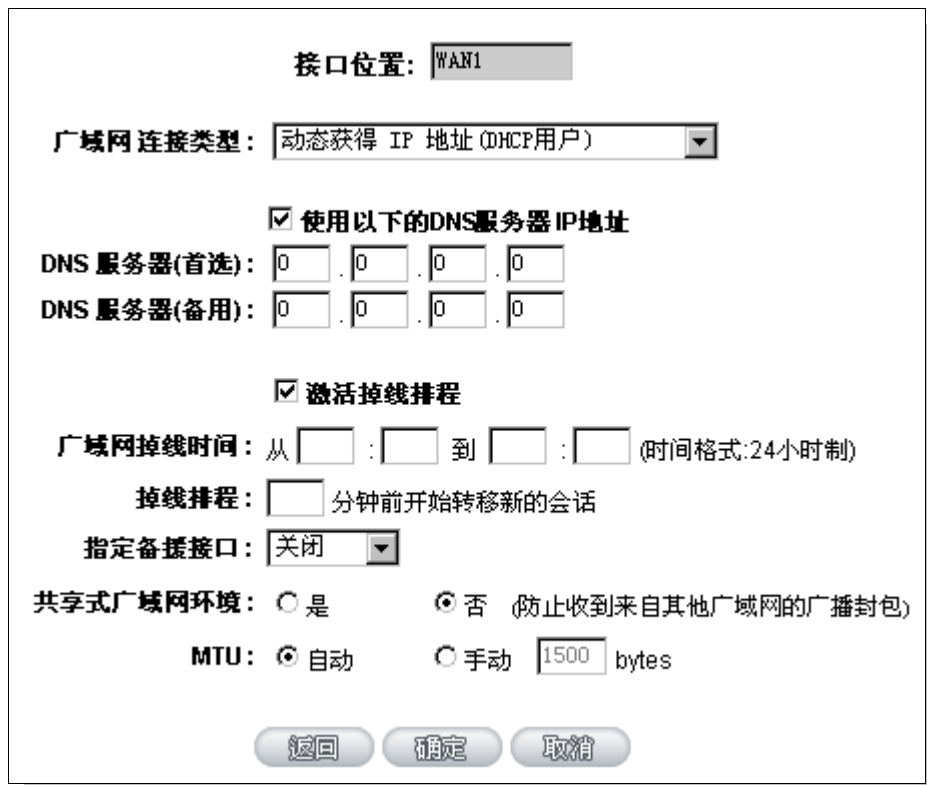
**配置：** 点击“编辑”按钮可以进入广域网联机状态的设置窗口。各类型的联机状态设置请参考以下的说明，并选择配合运营商所给您的联机状态来做设置。

#### 自动取得 IP 地址（动态获得 IP 地址/DHCP 用户）：

此为安全路由器系统默认的联机方式，此联机方式为 DHCP 客户端自动取得 IP 模式，多为应用于如线缆调制解

调器或是 DHCP 客户端联机状态等连接，若您的联机为其它不同的方式，请选取相关的设置并参考以下的介绍做设置。

在自动取得 IP 模式，您可以使用自定 DNS 的 IP 地址，勾选此选项并填入您要使用的 DNS 服务器 IP 地址。



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

**DNS 服务器：** 输入您的运营商所提供的动态域名解析服务器 IP 地址，最少填入一组，最多可填二组。

**广域网掉线排程：** 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

**广域网掉线时间：** 输入此广域网中断连接服务的规则时间。

**掉线排程：** 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

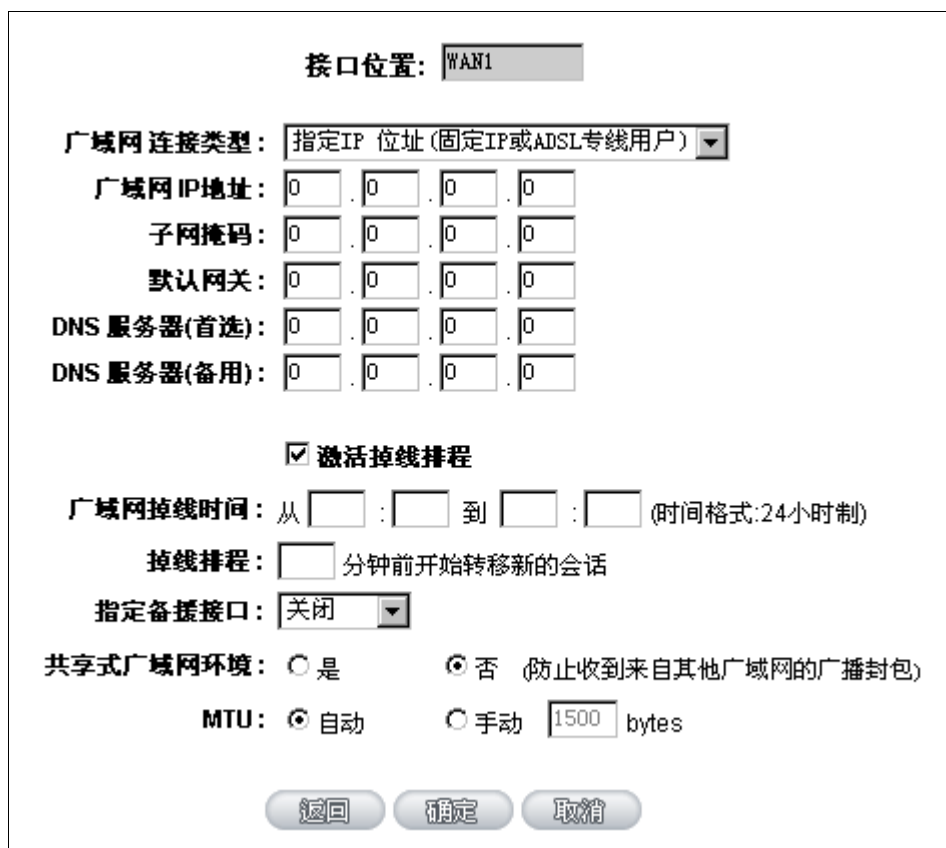


- 指定备援接口：** 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
- 共享式广域网环境：** 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏蔽掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
- MTU：** MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

**固定 IP 地址联机（指定 IP 地址）：**

若您的运营商有核发固定的 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，将运营商所核发的 IP 信息分别参照以下介绍填入相关设置参数中。



The screenshot shows a configuration window for WAN settings. At the top, the interface location is set to 'WAN1'. The connection type is '指定IP 位址 (固定IP或ADSL专线用户)'. Below this are input fields for WAN IP address, subnet mask, default gateway, and two DNS servers, all currently set to 0.0.0.0. There is a checked checkbox for '激活掉线排程' (Enable Disconnect Scheduling). The disconnect time is set from 0:00 to 0:00. The disconnect scheduling is set to start 0 minutes before the session transfer. The backup interface is set to '关闭'. The '共享式广域网环境' (Shared WAN Environment) is set to '否' (No). The MTU is set to '自动' (Auto) with a value of 1500 bytes. At the bottom, there are three buttons: '返回' (Back), '确定' (OK), and '取消' (Cancel).

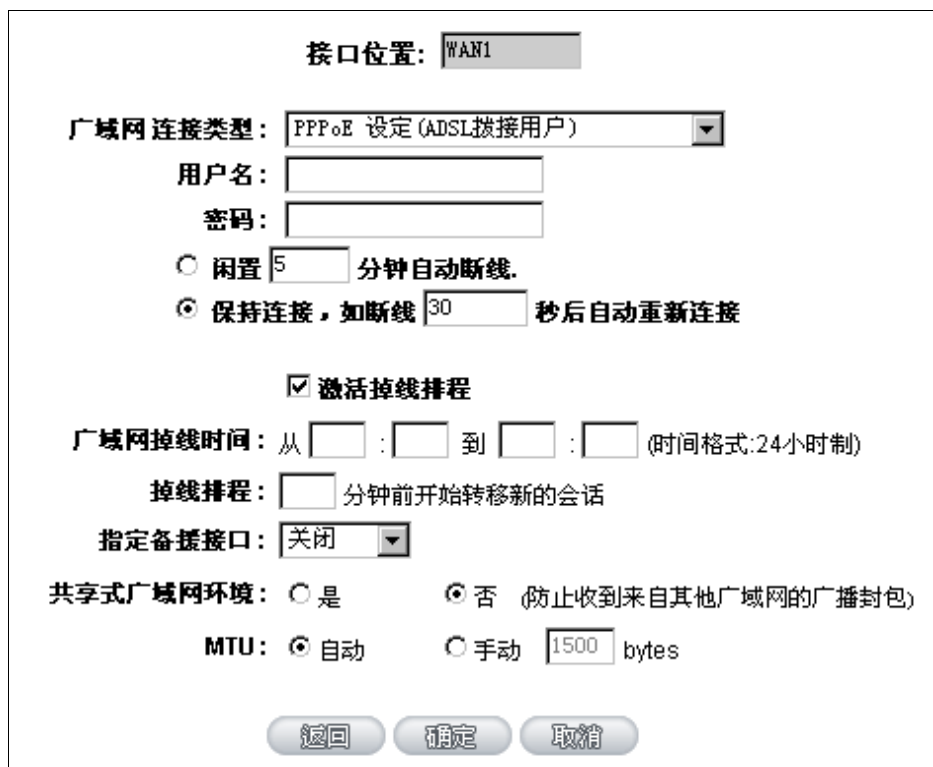
**广域网 IP 地址：** 输入您的运营商所核发的可使用固定 IP 地址的其中一个。

- 子网掩码：** 输入您的运营商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：** 输入您的运营商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 ADSL 数据机 (ATU-R) 的 IP 地址。
- DNS 服务器：** 输入您的运营商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。
- 广域网掉线排程：** 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
- 广域网掉线时间：** 输入此广域网中断连接服务的规则时间。
- 掉线排程：** 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
- 指定备援接口：** 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
- 共享式广域网环境：** 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏蔽掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
- MTU:** MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。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 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### PPPoE 拨号联机：

此项为 ADSL 虚拟拨号使用(适用于 ADSL PPPoE)，填入运营商给予的使用者联机名称与密码并以安全路由器内建的 PPP Over Ethernet 软件联机，若是您的 PC 之前已经有安装由运营商所给予的 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。



接口位置: WAN1

广域网连接类型: PPPoE 设定 (ADSL 拨接用户)

用户名:

密码:

闲置 5 分钟自动断线.

保持连接, 如断线 30 秒后自动重新连接

激活掉线排程

广域网掉线时间: 从  :  到  :  (时间格式:24小时制)

掉线排程:  分钟前开始转移新的会话

指定备援接口: 关闭

共享式广域网环境:  是  否 (防止收到来自其他广域网的广播封包)

MTU:  自动  手动 1500 bytes

返回 确定 取消

用户名： 输入您的运营商所核发的使用者名称。

密码： 输入您的运营商所核发的使用密码。

闲置( )分钟自动断线： 此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端是有上网需求时，安全路由器 会自动向默认的运营商自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。您可以自行输入所需要的无数据包传送自动离线等待时间，默认为 5 分钟。

保持连接： 此功能能够让您的 PPPoE 拨接连线能够断线自动重拨，您可以自行设置重新拨接的时间，默认值为 30 秒。

- 广域网掉线排程：** 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
- 广域网掉线时间：** 输入此广域网中断连接服务的规则时间。
- 掉线排程：** 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
- 指定备援接口：** 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
- 共享式广域网环境：** 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏蔽掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
- MTU:** MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。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 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### PPTP 拨号联机：

此项为 PPTP (Point to Point Tunneling Protocol) 计时制使用，填入运营商给予的使用者联机名称与密码并以安全路由器内建的 PPTP 软件联机。

**接口位置:**

**广域网 连接类型:**

**广域网 IP地址:**

**子网掩码:**

**默认网关:**

**用户名:**

**密码:**

闲置  分钟自动断线。

保持连接，如断线  秒后自动重新连接

激活掉线排程

**广域网掉线时间:** 从  :  到  :  (时间格式:24小时制)

**掉线排程:**  分钟前开始转移新的会话

**指定备援接口:**

**共享式广域网环境:**  是  否 (防止收到来自其他广域网的广播封包)

**MTU:**  自动  手动  bytes

- 广域网 IP 地址： 输入您的运营商所核发的可使用固定 IP 地址的其中一个。
- 子网掩码： 输入您的运营商所核发的可使用固定 IP 地址的子网掩码。
- 默认网关： 输入您的运营商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。
- 用户名： 输入您的运营商所核发的使用者名称。
- 密码： 输入您的运营商所核发的使用密码。
- 闲置( )分钟自动断线： 此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若有上网需求时，安全路由器 会自动向默认的运营商自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无数据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。


- 保持连接：** 此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设置重新拨接的时间，默认值为 30 秒。
- 广域网掉线排程：** 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
- 广域网掉线时间：** 输入此广域网中断连接服务的规则时间。
- 掉线排程：** 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
- 指定备援接口：** 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
- 共享式广域网环境：** 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏蔽掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
- MTU:** MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。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 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### 透通桥接模式 (Transparent Bridge) :

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更动原有架构, 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, 这样您可以保留内网计算机的 IP 设置为原本的公网 IP 仍然可以正常上网。

当您设置两个广域网时, 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。



The screenshot shows the WAN configuration interface for Transparent Bridge mode. The interface is titled '接口位置: WAN1'. The '广域网连接类型' (WAN Connection Type) is set to 'Transparent Bridge (透通桥接模式)'. Below this, there are input fields for '广域网 IP 地址' (WAN IP Address), '子网掩码' (Subnet Mask), '默认网关' (Default Gateway), 'DNS 服务器(首选)' (DNS Server (Preferred)), and 'DNS 服务器(备用)' (DNS Server (Backup)), all set to '0'. There are also two '公网 IP 地址范围' (Public IP Address Ranges) fields, both set to '0'. A checkbox for '激活掉线排程' (Enable Disconnect Scheduling) is checked. Below it, '广域网掉线时间' (WAN Disconnect Time) is set to '从 0 : 0 到 0 : 0 (时间格式:24小时制)'. '掉线排程' (Disconnect Scheduling) is set to '0' minutes before starting to transfer new sessions. '指定备援接口' (Specify Backup Interface) is set to '关闭' (Closed). '共享式广域网环境' (Shared WAN Environment) has '否' (No) selected, with a note '(防止收到来自其他广域网的广播封包)'. 'MTU' is set to '自动' (Automatic), with '1500 bytes' shown next to it. At the bottom, there are three buttons: '返回' (Back), '确定' (OK), and '取消' (Cancel).

- 广域网 IP 地址 : 输入您的运营商所核发的可使用固定 IP 地址的其中一个。
- 子网掩码 : 输入您的运营商所核发的可使用固定 IP 地址的子网掩码, 如:  
255.255.255.240
- 默认网关 : 输入您的运营商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。
- DNS 服务器 : 输入您的运营商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。
- 公网 IP 地址范围 : 输入您的运营商所核发的可使用固定 IP 范围。若是您的运营商分给您两个不连续的 IP 地址范围, 您可以分别填入。

- 广域网掉线排程：** 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
- 广域网掉线时间：** 输入此广域网中断连接服务的规则时间。
- 掉线排程：** 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
- 指定备援接口：** 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
- 共享式广域网环境：** 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏蔽掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
- MTU:** MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。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 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### 3G / 3.5G

点选“编辑”开始进行 3G/3.5G 网络连线的相关设定：

※路由器的 3G 功能默认为关闭，需先至 USB 设置页面选择其中一个模式以激活 3G 功能。

#### ◆ 连线类型配置

选择广域网个数： (预设值 2)

端口	线路连线类型	配置
广域网1界面	自动取得 IP 地址	编辑
广域网2界面	自动取得 IP 地址	编辑
USB1	3G / 3.5G	编辑
USB2	3G / 3.5G	编辑



端口:

线路连线类型: 3G / 3.5G

输入PIN CODE:

再次确认PIN CODE:

USB 连线状态: 無線上網卡已接上, 工作正常。

APN:

拨号号码:

使用者名称:

密码:

使用以下的 DNS 伺服器 IP 地址

DNS服务器(主要):  .  .  .

DNS服务器(次要):  .  .  .

MTU:  自动  手动  bytes

**PIN CODE 字段:**

输入PIN CODE:	<input type="text"/>
再次确认PIN CODE:	<input type="text"/>

若您的 SIM 卡有激活 PIN CODE 保护, 才会需到填入此字段。

若 PIN Code 不正确, 会影响 3G 无线上网卡无法使用。

### ※请注意:

※ISP 电信业者对于 PIN CODE 保护可能有错误次数门坎。若您输入错误的次数超过该门坎, 该张 SIM 卡将会被 ISP 电信业者锁卡, 而设定画面将出现[PUK] PIN Unlocked Key。

※因路由器产品不支持解锁。若有上述情形, 请联络您的 ISP 电信业者。

### 2. USB 连线状态:

\* 本例的 3G/3.5G USB 网卡没有激活 PIN CODE 保护机制, 故 USB 端口侦测到网卡之后, 就可以进行拨号动作。如下图所示, 3G/3.5G USB 网卡在成功完成拨号后, 系统显示: 无线上网卡已接上, 工作正常。

**USB 连线状态: 無線上網卡已接上, 工作正常。**

※该字段会依据 USB 端口不同的状态, 而出现不同的描述:

状态 1: 无线上网卡没有接上, 或是尚未能辨识为可用 3G Device.

状态 2：无线上网卡已接上，但是没有 SIM 卡，请插入 SIM 卡。

状态 3：无线上网卡已接上，但是需要使用者输入正确 PIN 码。

状态 4：无线上网卡已接上，但是因输入不正确次数过多，SIM 卡已死锁，需 PUK 解锁。

状态 5：无线上网卡已接上，工作正常。

**3. DNS 服务器：**选择使用自定的 DNS 服务器 IP 地址。

<input type="checkbox"/> 使用以下的 DNS 服务器 IP 地址			
DNS服务器(主要):	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
DNS服务器(次要):	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

**4. 其它字段：**以下字段请先参照您的 ISP 电信业者所提供的信息。

APN :	<input type="text"/>
拨号号码 :	<input type="text" value="*99#"/>
使用者名称 :	<input type="text"/>
密码 :	<input type="text"/>

**APN**： Access Point Network，一般多以“Internet”做为代码。

**拨号号码**：系统默认值为 WCDMA 系统的\*99#。

**使用者名称 / 密码**：视 ISP 电信业者是否要求输入。

## 6.2 多 WAN 设置

当用户的连线是采用多 WAN 的线路设计，管理人员可以进入网络连线设置的流量管理、与协议绑定栏目，对安全路由器的负载均衡模式等进行设置，使安全路由器达到最优数据转发是网络带宽效能达到最高。

### 模式

智能型负载均衡	均衡模式:	<input checked="" type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
指定路由	未绑定端口均衡模式:	<input type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
策略路由	均衡模式:	<input type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; background-color: #e0e0e0; margin: -1px -1px 1px -1px;">广域网组合设定</p> <p>联通策略 <input type="text" value="关闭"/> <span style="background-color: #4CAF50; color: white; padding: 2px 5px; margin-left: 10px;">更新网段</span></p> <p>自定义策略1 <input type="text" value="关闭"/></p> <p>自定义策略2 <input type="text" value="关闭"/></p> </div>			

### 端口

端口	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>

### 线路侦测机制

端口	广域网1
<input checked="" type="checkbox"/> 激活	
重新发起测试次数	<input type="text" value="5"/>
响应延迟时间	<input type="text" value="30"/> 秒
当线路连接失败时	<input type="text" value="移除该条线路"/>
<input checked="" type="checkbox"/> 当上传 或 <input type="text" value=""/> 下载流量超过 <input type="text" value="1"/> %，不进行线路侦测。	
<input checked="" type="checkbox"/> 预设网关 IP 地址	
<input checked="" type="checkbox"/> ISP 服务器	<input type="text" value="168.95.1.1"/>
<input checked="" type="checkbox"/> 远程服务器	<input type="text" value="168.95.192.1"/>
<input type="checkbox"/> 使用 DNS 服务器作域名解析	<input type="text"/>

## 6.2.1 负载均衡模式

### 模式

智能型负载均衡	均衡模式:	<input checked="" type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
指定路由	未绑定端口均衡模式:	<input type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
策略路由	均衡模式:	<input type="radio"/> 连机数均衡	<input type="radio"/> IP 均衡
<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; background-color: #e0e0e0; margin: -1px -1px 1px -1px;">广域网组合设定</p> <p>联通策略 <input type="button" value="关闭"/> <input type="button" value="更新网段"/></p> <p>自定义策略1 <input type="button" value="关闭"/></p> <p>自定义策略2 <input type="button" value="关闭"/></p> </div>			

#### 智能型负载均衡模式：

当您选用智能负载均衡模式，安全路由器将以会话数或是 IP 地址会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到对外会话的负载均衡。线路的带宽是依据您所填入的带宽设置(请参考下一小节设置说明)，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，所以为了确保您的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 (请参考下一段 QoS 节带宽管理设置说明)。

**依会话数均衡：**当您选用会话数均衡模式，安全路由器将以会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

**依 IP 地址均衡：**当您选用 IP 负载均衡模式，安全路由器将以会话的 IP 数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

#### 提示！

不论是会话数均衡或是 IP 负载均衡方式，搭配“通讯协议绑定”可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，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 去访问服务端口 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 访问时要从广域网 1 去访问等等，都可以经由设置此“通讯协议绑定”功能来达到您的需求。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，除了您指定的访问会按照您的规则出去访问外网，其它未被指定的 IP 或服务端口的访问还是按照安全路由器的机制做智能负载均衡。

关于如何设置“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 (6.2.3 节的通讯协议绑定设置说明)。

#### 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口、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口、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口、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，您可以选择他们的负载均衡模式是以会话数作为负载均衡的基础，还是以 IP 会话数作为负载均衡的基础。

**未绑定端口均衡模式：**若是有一部分广网端口并没有被指定，以 2WAN 的路由器产品为例，若广域网 2 没有指定特定的 IP、服务端口、或目的 IP 来使用，则广域网 2 仍然会依据安全路由器的负载均衡机制来分配会话。均衡机制如下：

**依会话数均衡：**当您选用会话数均衡模式，安全路由器将以会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

**依 IP 地址均衡：**当您选用 IP 负载均衡模式，安全路由器将以会话的 IP 数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

---

#### 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口 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”功能中做设置。要注意，当使用指定路由(Exclusive Mode)模式，以上述的例子来看，除了您指定的访问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 或服务端口则经由安全路由器负载均衡的机制使用其它的广域网出去。

关于如何设置“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（6.2.3 节的通讯协议绑定设置说明）。

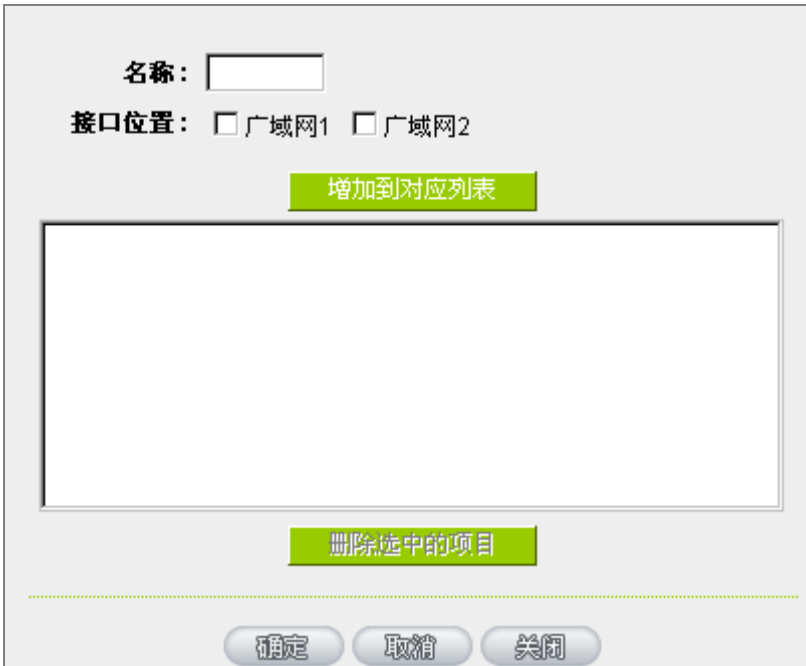
---

### 策略路由：

当您选用策略路由模式，安全路由器会依照内建的策略(电信、网通)自动分配会话。您只需选择网通线路接入的广域网口(或广域网组合)，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会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。

### 广域网组合设置：

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。点击“广域网组合设置”会弹出以下的对话框。



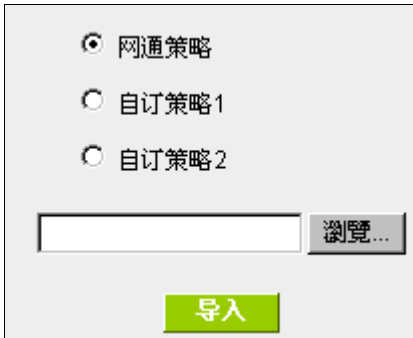
- 名称：**在此自定的广域网组合名称，如“教育”等，用来辨识广域网群组。
- 接口位置：**在此勾选要设在此组合的广域网口。
- 增加到对应列表：**增加到广域网组合列表。
- 删除选中的项目：**删除所选择的广域网组合内容。
- 确定：**点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。
- 取消：**点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。
- 关闭：**关闭并离开此功能设置窗口。

设置完成后，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)，然后点击“更新策略”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本文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，点击“汇入”，并在设置窗口的最下方点击“确定”，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。

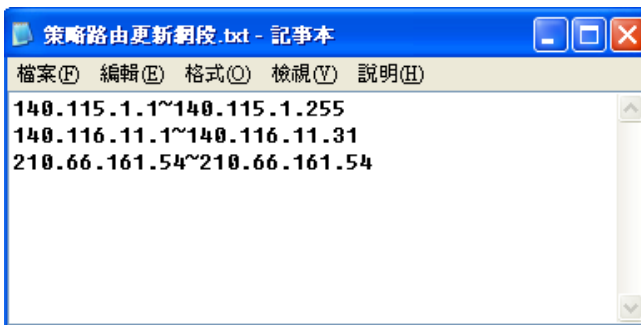


网通策略  
 自订策略 1  
 自订策略 2

浏览...

导入

策略文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序“记事本”来建立。将您要指定的目的 IP 地址按照下图的格式写入，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 格式。存储文件后(扩展名应该是.txt)即可汇入自定策略的更新网段。



提示！

网通策略与自定策略可以同时存在，但当某一个目的 IP 同时在网通策略以及自定策略中，则会以网通策略优先执行。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。

### 6.2.2 线路侦测机制

若勾选此项设置，则会显示出重新发起测试次数，响应延长时间等信息。当使用两条广域网做对外联结线路时一定将此 NSD 启用，以避免因为广域端口流量过大时造成 QoS 安全路由器的误判将此线路判断为断线。

#### 线路侦测机制

端口	广域网1 ▾
<input checked="" type="checkbox"/> 激活	
重新发起测试次数	5
响应延迟时间	30 秒
当线路连接失败时	移除该条线路 ▾
<input checked="" type="checkbox"/> 当上传 或 ▾ 下载流量超过 1 %，不进行线路侦测。	
<input checked="" type="checkbox"/> 预设网关 IP 地址	
<input checked="" type="checkbox"/> ISP 服务器	168.95.1.1
<input checked="" type="checkbox"/> 远程服务器	168.95.192.1
<input type="checkbox"/> 使用 DNS 服务器作域名解析	

**接口位置：** 选择您要设置线路侦测的广域网口。

**重新发起测试次数：** 对外会话侦测重试次数，默认值为五次。如果会话侦测重试次数超过设置次数，网络没有回应的话，则判断为对外线路中断！

**响应延迟时间：** 对外会话侦测逾时时间(秒)，默认值为 30 秒。于此设置秒数之后重新测试对外会话。



- 当线路连接失败时：** 线路连接失败时的处理方式，有两种：
- (1) 仅记录到日志：当侦测到与运营商连结失败时，系统就会在系统日志中将这项错误信息纪录下来，但保持此线路不会移除，所以会导致有些原来使用此条线路上的用户无法正常使用。
- 此选项适用在当某条广域网会话失败时，从这个广域网去访问的目的地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) 纪录到日志并移除该条线路：当侦测到与运营商连结失败时，系统不会在系统日志中将这项错误信息纪录下来，原本使用此 WAN 端的数据包传递会自动转换到另一条广域网端口。等到原本断线的广域网端口恢复后会自行重新连结，则数据包传递会自动转换回来。
- 此选项适用在当某条广域网会话失败时，从这个广域网去访问的目的地位置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，将流量转移到还在会话的广域网。
- 有流量时不进行侦测：** 当下载 或 / 与 上传流量超过带宽的百分之 ( ) 时，表示线路仍在会话运作，不必再一直送出 NSD 侦测要求数据包
- 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，此为路由自动填入，所以只须打勾选择是否启用。
- 
- 注意！**
- 有部分的 ADSL 线路的关是不会响应侦测数据包，或是当您是使用光纤盒，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，此选项不要动。
- 
- 运营商 服务器：** 运营商端的侦测位置，如运营商的 DNS 服务器 IP 地址等。在设置此 IP 地址时请确认此 IP 地址是可以且稳定快速的得到响应 (建议填入运营商端 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(建议填入运营商端 DNS IP)。
- DNS 服务器：** 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。
- 确定：** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。

**取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

---

**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的 IP 或应用服务端口(服务端口)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。

---

### 6.2.3 WAN 口协议绑定设置

#### 协议绑定

使用者可将特定的 IP 或特定的应用服务端口(服务端口)经由您限定的 WAN 出去。其它没有做绑定的 IP 或服务器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的 IP 或应用服务端口(服务端口)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，以避免所有的广域网口都被指定有特定的内网 IP、应用服务端口、目的地 IP，导致其它的 IP 或应用服务端口没有广域网口可以使用。

---

协议绑定



服务端口：所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

来源IP地址：10 . 10 . 10 . 0 到 0

目的IP地址：0 . 0 . 0 . 0 到 0 . 0 . 0 . 0

接口位置：广域网1

激活：

上移 增加到对应列表 下移

FTP [TCP/21~21]->10.10.10.0^0(0.0.0.0^0.0.0.0)广域网1

删除选中的项目

显示排序表 确定 取消

**服务端口：** 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)，默认的服务为 All 0~65535。

点击“服务端新增或删除表”按钮可以进入服务端口设置窗口，进行新增或删除选单中默认的服务端口。

**来源 IP 地址：** 您可以指定特定的内部虚拟 IP 地址的数据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置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 到 210.11.1.1。如果使用者要设置一个范围的目的地址位置，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，若只需要设置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。
- 删除选中的项目：** 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，也就是越后面设置的规则会越后执行，所以您可以自行调整每条规则先后执行顺序。
- 确定：** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
- 取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

**注意！**

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

**显示开启表：**

按下“显示开启表”，会出现以下的对话框。您可以选择以“优先级”来显示排列的顺序，或是以“接口位置”来显示排列的顺序。点击“刷新”可以重新显示窗口，点击“关闭”将结束这个对话框。

<input checked="" type="radio"/> 优先级 <input type="radio"/> 接口位置 <span>刷新</span> <span>关闭</span>						
优先级	接口位置	服务端口	来源IP地址	目的IP地址	激活	编辑
1	广域网1	FTP [TCP/21~21]	10.10.10.0~10.10.10.0	0.0.0.0~0.0.0.0	激活	编辑

**新增或删除管理服务端口号**

若您欲开启的服务端口项目没有在表列中，您可以点击“服务端口新增或删除表”按钮，新增或删除管理服务端口号列表，如以下所述：



服务名称:

通讯协议:

端口范围:  到

增加到对应列表

所有端口 [TCP&UDP/1~65535]  
DNS [UDP/53~53]  
FTP [TCP/21~21]  
HTTP [TCP/80~80]  
HTTP Secondary [TCP/8080~8080]  
HTTPS [TCP/443~443]  
HTTPS Secondary [TCP/8443~8443]  
TFTP [UDP/69~69]  
IMAP [TCP/143~143]  
NNTP [TCP/119~119]  
POP3 [TCP/110~110]  
SNMP [UDP/161~161]  
SMTP [TCP/25~25]  
TELNET [TCP/23~23]  
TELNET Secondary [TCP/8023~8023]  
TELNETSSL [TCP/992~992]  
DHCP [UDP/67~67]  
L2TP [UDP/1701~1701]

删除选中的项目

确定 取消 关闭

- 服务端口名称：** 在此自定义欲开启的服务端口号名称加入列表中，如 BT 等。
- 通讯协议：** 在此选择欲开启的服务端口号的数据包格式为 TCP 或 UDP。
- 服务端口的位置范围：** 填入您将新增加的服务端口范围。
- 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。
- 删除选中的项目：** 删除所选择的开启服务项目内容。
- 确定：** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
- 取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。
- 关闭：** 离开并关闭此功能设置窗口。

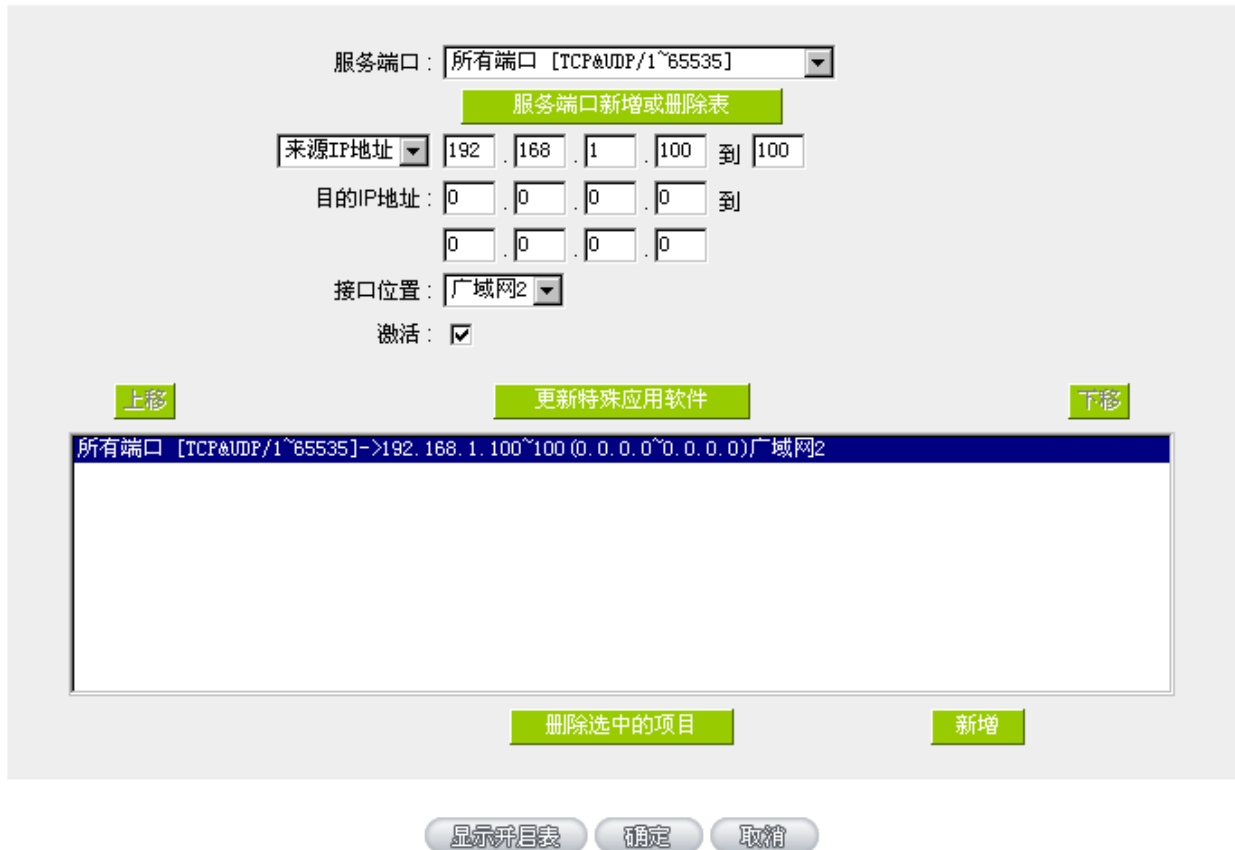
使用“智能型”负载均衡模式时其通讯协议绑定协议设置方式：

智能负载均衡方式搭配“通讯协议绑定”可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，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，那通讯协议绑定设置方式？**

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)。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。

协议绑定



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 0 . 0 . 0 . 0

接口位置: 广域网2

激活:

上移 更新特殊应用软件 下移

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
---

删除选中的项目 新增

显示并列表 确定 取消

**范例二:若要指定内网IP192.168.1.150到200去外网访问80端口都走只能走广域网2去访问,那通讯协议绑定怎样设置?**

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)。接口位置选则广域网2,然后勾选激活。最后点击“新增”即可将此规则加入。

协议绑定



服务端口： 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：

上移 更新特殊应用软件 下移

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

删除选中的项目 新增

显示列表 确定 取消

**范例三：若要指定内网所有 IP 去外网访问 80 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定是怎样设置？**

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)。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。QoS 安全路由器会将所有用 80 端口去外网访问的流量都走广域网 2，但是不是用 80 端口的流量根据路由器的自动负载平衡演算，还是有可能走广域网 2，因此还需要再设第二条规则。

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)。接口位置选则广域网 1，然后勾选激活。最后点击“新增”即可将此规则加入。这时 QoS 安全路由器会将不是用 80 端口去外网访问的流量都走广域网 1。

协议绑定

服务端口:

来源IP地址:  .  .  .  到

目的IP地址:  .  .  .  到

.  .  .

接口位置:

激活:

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

所有端口 [TCP&UDP/1~65535]->192.168.1.2~254 (0.0.0.0~0.0.0.0)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协议设置方式：

指定路由的模式让您对特定的内网 IP、特定要访问的应用服务端口或特定目的地 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口、或特定目的地 IP 使用。其它不在这些指定内的内网 IP、特定要访问的应用服务端口或特定目的地 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 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设置方式是怎样设置？**

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)。接口位置选则广域网 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 端口的流量，其余流量都只走广域网 1。



协议绑定



服务端口： 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 . 0 . 0 . 0

接口位置： 广域网2

激活：

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

**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，那通讯协议绑定设置方式如何设置？**

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。接口位置选则广域网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。接口位置选则广域网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。

协议绑定

服务端：

来源IP地址：  .  .  .  到  .  .  .

目的IP地址：  .  .  .  到  .  .  .

接口位置：

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

### 6.3 3G/3.5G USB 上网卡的增益功能

Qno 提供首创于业界的【智能型 USB 省电节能】模式，来达到节能的效果，并可延长 3G/3.5G USB 上网卡的寿命。系统执行方式为依据带宽流量使用率、时间及使用机制，而有以下四种模式：

- 1、高效运作模式
- 2、备援模式
- 3、自动化智能模式
- 4、时间排程模式



端口： USB1 ▾

#### ▶ 選擇模式

关闭

高效运作模式(始终连线)

备援模式

自动化智能模式       闲置时间  分

时间排程模式

#### ▶ USB激活触发条件

	该条线路侦测失败时，流量移转至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %
广域网2:	<input type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %

在每天  :  自动进行自我测试       将状态变化记录到日志中

确定

取消

在认识【智能型 USB 省电节能】模式之前，我们先了解 UI 上的其他基本字段。

端口： <input type="text" value="USB1"/>	选择要设定的 USB 端口
<input type="checkbox"/> 在每天 <input type="text" value="00"/> : <input type="text" value="00"/> 自动进行自我测试	USB 端口自我测试功能。 不管在任何模式，自我测试时间到达时，USB 端口都会令 3G/3.5G USB 上网卡拨号取得 IP，并将测试结果记录于日志中。测试完成之后 USB 端口会再切换为原本的设定模式。
<input checked="" type="checkbox"/> 将状态变化记录到日志中	勾选此字段以让您在本页更改过的设定，都记录于日志中。

注意事项：

- 1、路由器的 3G 功能默认为关闭，需先至此页选择其中一个模式以激活 3G 功能。
- 2、在任何模式下，只要进入 Power Saving State，则当每天 Auto Self Test 时间到达时，则自动切换至 Active State 连线并取得 IP，无论是否成功，皆需记录于 System Log，然后再将状态切回至 Power Saving State。
- 3、在各种状态切换的过程，依使用者设定，将切换状态记录于 System Log。
- 4、不管在任何模式下，当 WAN 全断时，USB 3G 一定要切换至 Active State，进行备援功能

### 6.3.1 高效运作模式(始终连线)

此模式允许 3G/3.5G USB 上网卡一直维持在连线状态。在这个模式电源功率消耗最大，系统将会持续侦测以确保 3G/3.5G USB 上网卡保持连线状态；在此模式时，USB 使用触发条件的各功能选项为关闭。

### 6.3.2 备援模式

此时 3G/3.5G USB 上网卡处于省电状态，提供低功率电力给 USB 接口。系统持续侦测有线网络状态及流量，以便于在有线网络断线时，随时可以唤醒 3G/3.5G USB 上网卡并提供连线服务；而当系统侦测到有线线路回复正常连线后，就会再将 3G/3.5G USB 转换为省电状态。

**选择模式**

关闭  
 高效运作模式(始终连线)  
 备援模式  
 自动化智能模式       闲置时间  分  
 时间排程模式             

**USB 激活触发条件**

	该条线路侦测失败时，流量移转至 USB	带宽超过门坎值时，将流量分流至 USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %

该条线路侦测失败时，流量移转至 USB：

#### 一、触发条件：

选择的有线线路全部侦测失败时。

您必须在此选择至少一个广域网口；当广域网为复选时，系统将会在选择的广域网全部都侦测失败时，再转移流量至 3G/3.5G USB 上网卡。

#### 二、回复条件：

当系统侦测到你选择的广域网全部都正常连线，此时系统会让 3G/3.5G USB 上网卡回复到省电状态，等待下一次需要协助分流的时机。

\*以本图为例，当用户一起勾选广域网 1 与网域网 2 时，当系统侦测到广域网 1 和 2 都同时失效时，会将 USB WAN 的 3G/3.5G USB 上网卡唤醒，来帮助有线线路备援；而在广域网 1 和 2 全部都正常连线后，3G/3.5G USB 上网卡也回复到省电状态。

### 6.3.3 自动化智能模式

在此模式，系统将持续侦测有线网络的带宽使用状况，当有线线路断线、或带宽使用超过设定门坎，系统会自动地唤起 3G/3.5G USB 上网卡，以帮助有线网络备援、或分担流量。

**▶ 選擇模式**

关闭  
 高效运作模式(始终连线)  
 备援模式  
 自动化智能模式  分  
 时间排程模式

**▶ USB激活触发条件**

	该条线路侦测失败时，流量移转至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 <input type="text" value="10000"/> kbits	<input type="checkbox"/> 低于带宽使用率 <input type="text" value="10"/> %

勾选自动化智能模式时，您会在旁边看到有闲置时间的设定。

自动化智能模式  分

若您有设定闲置时间，在 3G/3.5G USB 上网卡进入省电状态时，系统仍会对 USB 端口再供电一段时间(依据您设定的时间)。增加 USB 端口的供电时间，能够帮助您进一步争取 3G/3.5G USB 上网卡的拨号时间。

\*以上图为例。勾选闲置时间、并填入 10 分钟，代表在 3G/3.5G 回复省电状态时，系统仍会对 USB 端口再供电 10 分钟；在这 10 分钟中若又满足触发条件，3G/3.5G USB 上网卡将立即激活，并且还能够更立即的完成拨号动作，提供有线线路最实时的备援或分流。

若在这 10 分钟中没有发生触发条件，10 分钟后系统会安排 3G/3.5G USB 上网卡断电，以节省电力。

#### 一、触发条件：

触发条件 1：选择的有线线路全部侦测失败

触发条件 2：选择的有线线路，带宽全部都超过门坎值时

只要上述其中一个条件触发，系统就会让 3G/3.5G USB 上网卡协助备援或资料分流。

## 1\_选择的有线线路全部侦测失败时

	该条线路侦测失败时，流量转移至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %

同备援模式。您必须在此选择至少一个广域网口；当广域网为复选时，系统将会在选择的广域网全部都侦测失败时，再转移流量至 3G/3.5G USB 上网卡。

## 2\_选择的有线线路，带宽全部都超过门坎值时

在您已经选择好哪一些广域网需要 3G/3.5G USB 上网卡的备援协助后，系统会在右侧开放带宽门坎的设定字段(红框处)。

在这里，您除了可以决定广域网断线需要 3G/3.5G USB 上网卡备援之外，还可以更进一步决定，哪一些广域网在带宽使用超过多少时，也让 3G/3.5G USB 上网卡协助分流。

	该条线路侦测失败时，流量转移至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %



必须先勾选此字段，系统才会开放带宽门坎的设定字段。

### (1)设定激活门坎：

以下图为例，图中填入 10000 Kbits。代表当系统侦测到广域网 1 的带宽使用超过 10000 Kbits 时，会唤醒 3G/3.5G USB 上网卡协助资料分流。

	该条线路侦测失败时，流量转移至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input checked="" type="checkbox"/> 超过 10000 kbits	<input checked="" type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %

### (2)设定关闭门坎：

如果把每天带宽使用的情形做成一张折线图，我们会发现带宽的使用具有动态、经常变动的特性。所以当我们已经设定带宽门坎，让 3G/3.5G USB 上网卡帮助广域网做数据分流时，建议您也设定带宽门坎的下限，以降低系统控制 USB 端口的敏感度，减少 3G/3.5G USB 上网卡在短时间内太频繁的激活/关闭。

在 3G/3.5G USB 上网卡协助数据分流的期间，系统会持续注意广域网带宽使用状况，若带宽使用低于激活门坎值的\_\_%时，就可考虑将 3G/3.5G USB 上网卡回复至省电模式。

以下图做说明，当我们勾选并在字段中填入 10%后，图中的广域网 1 带宽使用少于 9000Kbit 时 (10000Kbits X 10%)，就可考虑将 3G/3.5G USB 上网卡回复至省电模式。

	该条线路侦测失败时，流量移转至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input checked="" type="checkbox"/> 超过 10000 kbits	<input checked="" type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %

## 二、回复条件：

只有在您所设定的触发条件都回复正常时，系统才会让 3G/3.5G USB 上网卡回复到省电状态。

以下以常见的设定方式来做说明：

举例 1：只有选择让 3G/3.5G USB 上网卡协助广域网备援

	该条线路侦测失败时，流量移转至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %

在广域网 1 和广域网 2 全部都回复到正常连线时，3G/3.5G USB 上网卡回复到省电状态。

举例 2：选择让 3G/3.5G USB 上网卡协助广域网备援、也同时设定了广域网 1 的带宽门坎

	该条线路侦测失败时，流量移转至USB	带宽超过门坎值时，将流量分流至USB	
广域网1:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input checked="" type="checkbox"/> 超过 10000 kbits	<input checked="" type="checkbox"/> 低于带宽使用率 10 %
广域网2:	<input checked="" type="checkbox"/> 激活侦测失败流量移转	<input type="checkbox"/> 超过 10000 kbits	<input type="checkbox"/> 低于带宽使用率 10 %

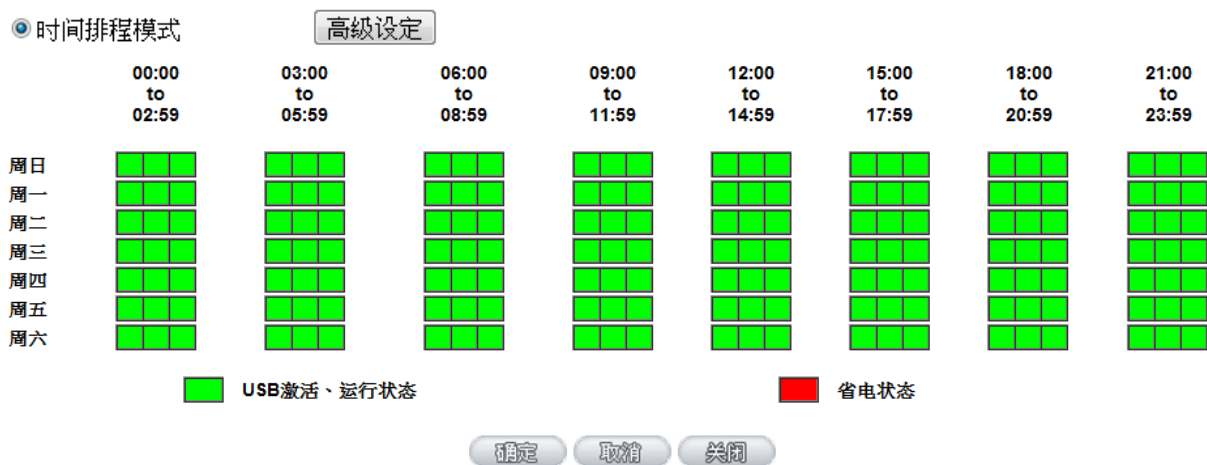
在广域网 1 和广域网 2 全部都正常连线 而且广域网 1 的带宽使用也少于 9000Kbit(10000Kbits X 10%)，这两个条件都需满足，系统就会安排 3G/3.5G USB 上网卡回复到省电状态。




### 6.3.4 时间排程模式


对于在网络使用率上有规律变化的环境，时间排程模式就是一个很好协助您做带宽规划的工具。例如一些私人企业就可以利用时间排程工具，在 XDSL 有线线路繁忙的特定时间，加入 3G/3.5G 的带宽帮助带宽扩充、数据分流。

勾选【时间排程模式】就可以在右侧看到【显示列表】按钮，点选按钮即可在时间排程窗口开始调整 USB 端口的时间排程。时间排程模式的最小单位为小时。



上图中为一间私人企业在规划 USB 1 端口的时间排程。网管希望在一般上班时间加入 3G/3.5G 的带宽来增加广域网带宽、帮助数据分流，所以您可以看到，他在周一到周五的 9:00~17:59 都是勾选为

 **USB 激活、运行状态**、而在上班时间以外，则是设定为  **省电状态**。

在  **省电状态** 中，系统仍然持续的侦测您的有线广域网线路，只要您的有线广域网侦测失败(断线)，也会立即唤醒 3G/3.5G USB 上网卡来协助备援，以保障网络的稳定性。

## 七、IPv6 设定方式

### 7.1 设定 IPv6 网络

IPv6 是新一代的网络协议，使用 128 位的地址，能提供更多的 IP 地址范围给用户使用。要设定 IPv6 网络，首先在首页选择网络联机设定，接着在右侧 IP 模式选择 Dual-Stack IP 启用设备的 IPv6 功能。



The screenshot shows the QNO router's web management interface. On the left is a navigation menu with options like '首页', '配置向导', '网络连线配置', '网络设置', '流量管理', '协议绑定', '流行路由', 'USB 设置', 'QoS 带宽管理', 'IP/DHCP 配置', '群组管理', '防火墙配置', '高级设置', '系统工具', '端口管理', 'VPN 虚拟私有网路', 'Smart Link VPN', and '无线网络'. The main content area is titled '网络设置' and includes a '网络联机配置' section with fields for '主机名称' (SMB) and '网络名称' (smb.com). Below this is the 'IP 模式' section, which contains a table for selecting IP modes for WAN and LAN.

模式	广域网	局域网
<input checked="" type="radio"/> IPv4 Only	IPv4	IPv4
<input type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

Below the table, there are tabs for 'IPv4' and 'IPv6'. The 'IPv6' tab is active, showing the '局域网(LAN)接口配置' section. This section includes a 'MAC 地址设定' field with a value of '00-17-16-05-40-64' and a note '(预设值 00-17-16-05-40-64)'. Below this is the 'IP 地址' field with '192.168.1.1' and the '子网掩码' field with '255.255.255.0'. A '多重网段配置' option is set to '关闭'. There is also an 'IP 整合管理' button.

The '连线类型配置' section is also visible, showing a dropdown for '选择广域网个数' set to '2' (预设值 2). Below this is a table for configuring WAN connections:

端口	线路连线类型	配置
广域网1界面	自动取得 IP 地址 (有线调制解调器使用者)	编辑

### 7.1.1 设定 IPv6 广域网

在首页选择网络连线配置，选择网络设置，接着在右侧 IP 模式底下点选 IPv6 的标签，接着就会出现广域网的 IPv6 设定项目。

IPv4

IPv6

**局域网(LAN)接口配置**

IPv6 地址 : fc00::1
前缀长度 : 7

IP 整合管理

---

**连线类型配置**

选择广域网个数 : 2 (预设值 2)

端口	线路连线类型	配置
广域网1界面	自动取得 IP 地址 (缆线调制解调器使用者)	<a href="#">编辑</a>
广域网2界面	自动取得 IP 地址 (缆线调制解调器使用者)	<a href="#">编辑</a>

确定
取消

点选对应广域网字段右侧的编辑，开始设定广域网的 IPv6 网络。广域网的 IPv6 网络支持以下几种类型：  
**自动取得 IP 地址：**

端口: 广域网1

广域网 线路连线类型: 自动取得 IP 地址(缆线调制解调器使用者)

使用以下的 DNS 服务器 IP 地址

DNS服务器(主要): ::

DNS服务器(次要): ::

MTU:  自动  手动 1500 bytes

---

Enable DHCP-PD:  2001:b010:7030:501:217:16ff:fe03:c1e4

LAN IPv6 Address: :: /64

返回
确定
取消

ISP 使用 DHCP 的方式派发 IPv6 地址，您可以选择手动设定 DNS 服务器地址，或是使用 ISP 派发过来的 DNS 服务器地址。

指定 IP 地址：

端口: 广域网1

广域网 线路连线类型: 指定 IP 地址(固接式或 ADSL 专线使用者) ▾

广域网 IP 地址: ::

前缀长度: 64

预设网关 IP 地址: ::

DNS 服务器(主要): ::

DNS 服务器(次要): ::

MTU:  自动  手动 1500 bytes

---

LAN IPv6 Address: :: /64

ISP 使用固定 IP 的方式设定 IPv6 地址，您需要输入广域网的 IP 地址、前缀长度、默认网关和 DNS 服务器等信息。

PPPoE 设定：

端口: 广域网1

广域网 线路连线类型: PPPoE 设定(ADSL 拨号使用者) ▾

使用者名称: 86352071@hinet.net

密码: ●●●●

闲置 5 分钟自动断线。

保持连线，如断线 30 秒后自动重新拨号

MTU:  自动  手动 1500 bytes

---

Enable DHCP-PD:  2001:b010:7030:501:217:16ff:fe03:c1e4

LAN IPv6 Address: :: /64

ISP 使用 PPPoE 方式连接 IPv6 网络，您需要在此输入 ISP 提供联机的用户名称以及密码。

Enable DHCP-PD (使用自动取得 IP 地址、PPPoE 设定时)：

如果您的 ISP 使用 DHCP-PD 配发局域网 IPv6 网络地址，您需要选取此项目来设定局域网。如果您的 ISP 没有支持这项功能，那么您需要取消这个选项，并且在底下 LAN IPv6 Address 输入您局域网的 IPv6 地址。

### 7.1.2 设定 IPv6 局域网

在首页选择网络连线配置，选择网络设置，接着在右侧 IP 模式下点选 IPv6 的标签，接着就会出现局域网的 IPv6 设定项目。

点击 IP 整合管理按钮，开启局域网的 IPv6 网络设定。

#### 局域网(LAN)接口配置

IPv6 地址 fc00::1	前缀长度 8
-----------------	--------

#### 动态 IP 服务

激活DHCP 服务功能

子网域1	
DHCP 服务功能	<input checked="" type="checkbox"/> 激活
起始 IP 地址	fc00::100
结束 IP 地址	fc00::17f

确定 取消

局域网 (LAN) 设定：

在此处输入路由器局域网的 IPv6 地址以及前缀长度。

动态 IP：

在此处输入路由器局域网 IPv6 的动态 IP 范围，或是取消使用 DHCP 服务器。

### 7.1.3 IPv6 地址转换

在只有 IPv4 的因特网环境的情况下，两个 IPv6 网络可以借由地址转换的方式互相联机。当您的设备启用 IPv6 功能 (设定为 Dual-Stack IP 模式) 此功能就会自动启用，您可以在首页选择网络连线配置选择 IPv6 地址转换，在右侧页面开启或是关闭这个功能。

#### IPv6 地址转换

6to4隧道  激活  关闭

确定 取消

## 7.2 设定局域网自动取得 IPv6 地址

局域网可以透过 DHCP 或是路由器广告 (Router Advertisement) 取得 IPv6 地址，并且借由 DNS Local Database 功能将 IPv6 地址对应为一主机名方便使用。

### 7.2.1 设定 IPv6 网络 DHCP 服务器

设定 IPv6 网络的 DHCP 服务器请在主画面选择 IP/DHCP 设定选择 DHCP 设定，右侧切换到 IPv6 的标签，确认后启用 DHCP 服务器有选取。

IPv4

IPv6

**激活 DHCP 服务功能**

---

**DHCP 动态 IP 服务**

租约到期时间  分

子网段：	子网段 1
DHCP 服务功能：	激活
起始 IP 地址：	fc00::100
结束 IP 地址：	fc00::17f

IP 整合管理

---

**域名解析服务(DNS)**

域名解析服务器(DNS)(主要) 1:	<input type="text" value="2001:b000:168::1"/>
域名解析服务器(DNS)(次要) 2:	<input type="text" value="2001:b000:168::2"/>

DHCP 动态 IP：在此项目中可以设定 IP 租用时间，默认为 1440 分 (一天)。

按下 IP 整合管理按钮可以修改 DHCP 配发的 IP 范围和修改局域网的 IPv6 网络设定，这部分的操作请参考第 **錯誤! 尚未定義書籤。页錯誤! 找不到参照来源。** 的内容。

DNS 网域服务：可以指定 DHCP 配发的设定 DNS 服务器地址，可以在此处填入 ISP 提供的服务器 IPv6 地址或是您内部架设的地址。

### 7.2.2 设定 DNS Local Database

DNS Local Database 的功能能让复杂的 IPv6 地址转变成容易记忆的主机名。要设定 IPv6 网络的 DNS Local Database 请在主画面选择 IP/DHCP 设定选择 DHCP 设定，右侧切换到 IPv6 的标签，在下方的 DNS Local Database 项目输入 Host Name 和 IP Address，最后按下新增到对应表列就可以完成设定。

#### ▶ DNS Local Database



主机名：

IP地址：

增加到对应列表

删除所选择服务

※请注意：使用 DNS Local Database 功能时需要将 DHCP 服务器的 DNS 网络服务设定为路由器的 IP 地址。设定方式请参考第 62 页的内容。

### 7.2.3 设定路由器广告

IPv6 网络除了使用 DHCP 服务器之外，还可以借由路由器广告的方式自动设定 IPv6 的地址。要设定路由器广告请在主画面选择 IP/DHCP 设定选择路由器广告，右侧设定画面和内容如下所示：

激活路由器广告

前缀	2001:b010:7030:501::/64
广告模式	Unsolicited Multicast
广告间隔	30 seconds
广告选项标志	<input checked="" type="checkbox"/> Managed <input checked="" type="checkbox"/> Other
路由器首选项	High
MTU	1500
路由器有效时间	3600 seconds

确定

取消

前缀：此处显示局域网透过路由器广告配发的 IPv6 前缀。

广告模式：Unsolicited Multicast 方式会对所有 IPv6 设备发送路由器广告。默认使用此种方式。若选择 Unicast Only 则路由器广告只会对已知的 IPv6 设备发送。

广告间隔：发送路由器广告的间隔时间。

广告选项标志：启用 Managed 表示局域网内有 DHCPv6 服务器可以取得 IP 信息；启用 Other 表示局域网内有 DHCPv6 服务器可以取得 IP 以外的信息 (ex. DNS Server)。

路由器首选项：设定发送的路由器广告等级。

MTU：设定网络的 MTU 值。

路由器有效时间：设定路由器广告内的路由器有效时间，超过此时间未收到此路由器的路由广告，则客户端会将此路由器的相关路由判定为无效 (过期) 而不使用。



## 八、内部局域网络设置

### 8.1 端口状态即时显示

此项功能可以让网络管理者查看每个实体端口的详细信息。

端口号：

#### 摘要信息

网络连接状态	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
连接速率	10 Mbps
半双/全双工模式	半双工
自动翻转功能	激活
VLAN	VLAN1

#### 流量实时状态

接收数据包统计	0
数据包接收Byte数量	3052672
传送数据包统计	0
数据包传送Byte数量	3204100
错误数据包统计	0

刷新

整体资讯项目：

网络连接状态（10Base-T / 100Base-TX），接口位置（局域网/广域网络），线路连线状态（激活/关闭），端口设置状态（端口激活/端口关闭），优先级设置（高级/一般），网络连接速率（10Mbps/100Mbps），半双/全双工模式（半双工/全双工），自动翻转功能（激活/关闭）。

端口流量实时状态：

即时显示安全路由器工作状态下的接收和传送数据包计算、数据包接收和传送 Byte 数以及错误数据包统计实际数值。

### 8.2 DHCP 发放 IP 服务器

安全路由器的 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 不用去记录与设置其 IP 地址，当计算机开机后，就可从安全路由器自动取得 IP 地址，管理方便。

IP/DHCP 配置	
▶ DHCP 配置	
DHCP 状态	
IP与MAC绑定	
IP 群组管理	

激活 DHCP服务器

### ▶ DHCP 用户使用IP范围

租约到期时间  分钟

起始IP地址: 10.10.	<input type="text" value="17"/>	.	<input type="text" value="100"/>
结束IP地址: 10.10.	<input type="text" value="17"/>	.	<input type="text" value="149"/>

### ▶ 域名解析服务(DNS)

DNS 服务器(首选) 1:	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>
DNS 服务器(备用) 2:	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>

### ▶ WINS服务器

WINS服务器地址:	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>	.	<input type="text" value="0"/>
------------	--------------------------------	---	--------------------------------	---	--------------------------------	---	--------------------------------

动态 IP 服务：

- 租约时间：** 此设置为发给 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 端会重新跟路由再申请一次。您可以依照实际需求来设置。
- 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置。
- 结束 IP 地址：** 系统默认为 192.168.1.149 的 IP 地址为最后发放 IP，也就是说可供 50 台计算机自动取得 IP 地址。

域名解析服务（DNS）地址：

此设置为发给 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 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 服务器地址。

**DNS 服务器 (首选) 1 :** 输入 DNS 网域服务器的 IP 位置。

**DNS 服务器 (备用) 2 :** 输入 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 服务器地址 :** 输入 WINS 网域服务器的 IP 位置。

**确定 :** 点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。

**取消 :** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### 8.3 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置纪录等，以便提供管理人员需要时做网络设置参考数据。

#### 状态

<b>DHCP服务器:</b>	10.10.10.1
<b>已使用的动态IP数量:</b>	0
<b>已发放的固定IP数量:</b>	0
<b>剩余可用的IP数量:</b>	50
<b>可发放的IP总量:</b>	50

#### DHCP 用户连接列表

主机名称	IP地址	MAC地址	租约到期时间	删除
------	------	-------	--------	----

刷新

- DHCP 服务器 IP 地址:** 目前 DHCP 服务器的 IP 地址。
- 已使用的动态 IP 数量:** 目前 DHCP 服务器已经发放动态 IP 的数量。
- 已发放的固定 IP 数量:** 目前 DHCP 服务器已经发放固定 IP 的数量。
- 剩余可用的 IP 地址:** 目前 DHCP 服务器可以还可发放的 IP 数量。
- 可发放的 IP 总量:** 目前 DHCP 服务器所设置可发放的 IP 总数量。
- 主机名称:** 目前此台计算机的名称。
- 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。
- 租约到期时间:** DHCP 目前核发 IP 地址的租约时间。
- 删除:** 删除此笔核发 IP 纪录。

## DNS 自订资料库

一般网络应用是将 DNS 服务器指向外部运营商的 DNS 服务器，或内部自行架设的 DNS 服务器，现在侠诺的安全路由器也提供类似「简易」的自订 DNS 服务，称为「DNS 自订资料库」，可以将网域名称与该名称所对应的 IP 地址做简单的设置。

### ▶ DNS 自订资料库



- 主机名称：** 输入需要做解析对应的网域名称。例如 `www.google.com`。
- IP 地址：** 输入上述网域名称所对应的 IP 地址。
- 加入到对应列表：** 将输入好的网域名称与 IP 对应，加入到下方对应列表当中。
- 删除点选的项目：** 删除所选的的对应项目。

#### ※请注意！

- (1) 「必须」要启用 DHCP 服务器服务，DNS 自订资料库服务才会启用。
- (2) 需要使用 DNS 自订资料库 需要将 DHCP 服务器的网域解析服务(DNS) IP 地址输入成防火墙 / 路由器设备的局域网网关 IP，以下图为例，局域网网关 IP 目前是 10.10.10.1。

### ▶ 局域网(LAN)接口配置

MAC地址：	00 . 17 . 41 . 51 . 88 . 45 (默认值: 08-3b-ba-8a-67-b9)
局域网网关：	10 . 10 . 10 . 1
子网掩码：	255 . 255 . 240 . 0

所以 DHCP 的 DNS IP 地址也要设定成 10.10.10.1 DNS 自订资料库的对应效果才会生效 (如下图)。

▶ 域名解析服务(DNS)

DNS 服务器(首选) 1:	10	10	10	1
DNS 服务器(备用) 2:	0	0	0	0

(3) 启用 DNS 自订资料库后，没有在资料库对应清单中的网域名称，还是会透过外网的运营商 DNS 服务器或是内网自行架设的 DNS 服务器进行解析。

测试 DNS 自订资料库是否生效：

假设设定 tw.yahoo.com 网域名称所对应的 IP 地址 10.10.10.199 如下图：

▶ DNS 自订资料库

主机名称:  (Ex: www.google.com)

IP地址:

```

erp.com => 10.10.10.2
jay => 10.10.10.222
www => 119.160.246.241
www.msn.com.tw => 59.124.180.50
tw.yahoo.com => 10.10.10.199
    
```

(1) 系统工具 => 自我诊断 => 域名解析测试

- 域名解析测试  Ping测试

测试域名(www.qno.cn):

(2) 输入网域名称 tw.yahoo.com 进行查询/解析

- 域名解析测试  Ping测试

测试域名(www.qno.cn):

(3) 解析出来的 IP 地址为 10.10.10.199，确认为 DNS 自订资料库所设定的对应 IP

- 域名解析测试  Ping测试

测试域名(www.qno.cn):

名称: tw.yahoo.com  
地址: 10.10.10.199

## 8.4 IP 及 MAC 地址绑定

在许多的大中型网吧及企业网络中，网管人员可以设置安全路由器所提供的 IP & MAC 绑定功能，达到用户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。另外通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。



### IP与MAC绑定

显示新加入的IP地址

静态IP地址:  .  .  .

所对应的MAC地址:  -  -  -  -  -

名称:

激活:

增加到对应列表

删除选中的项目

- 封锁绑定列表中IP地址与MAC地址不对应的用户
- 封锁未绑定或绑定列表中未激活的用户

您可以以两种方式来设置这个功能：

(一)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 分配的 IP 地址上网，未在此列表的计算机都无法取得 IP 上网；或是限制有在列表但是未激活绑定功能的计算机。当使用此功能时，切记要将静态 IP 地址填 0.0.0.0 不可以空白，另外将“封锁未绑定或绑定列表中未激活的用户”选项勾选才可以执行。如下图中范例所示：

▶ IP与MAC绑定



显示新加入的IP地址

静态IP地址： .  .  .

所对应的MAC地址： -  -  -  -  -

名称：

激活：

增加到对应列表

删除选中的项目

- 封锁绑定列表中IP地址与MAC地址不对应的用户
- 封锁未绑定或绑定列表中未激活的用户

显示列表 确定 取消

(二)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“封锁绑定列表中 IP 地址与 MAC 地址不对应的用户”功能启用，那么设置为固定 IP 的计算机或通过此功能已发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，则会无法上网。

IP与MAC绑定

显示新加入的IP地址

静态IP地址:  .  .  .

所对应的MAC地址:  -  -  -  -  -

名称:

激活:

增加到对应列表

删除选中的项目

- 封锁绑定列表中IP地址与MAC地址不对应的用户
- 封锁未绑定或绑定列表中未激活的用户

显示列表
确定
取消

**静态 IP 地址设置：**

此字段有两种填入方式：

1. 若您只要限制 MAC 地址可以跟 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。

**所对应的 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：**

启用此组设置。

**增加到对应列表：**

增加或修正此设置到列表中。

**删除选中的项目：**

删除列表中所选择的绑定。

**新增：**

当列表中有绑定规则后，右下角会出现此按钮，可点击增加新的绑定。

**封锁绑定列表中 IP 地址与 MAC 地址不对应的用户：** 此选项打勾后，只要是 User 自行更改计算机的 IP 或不是

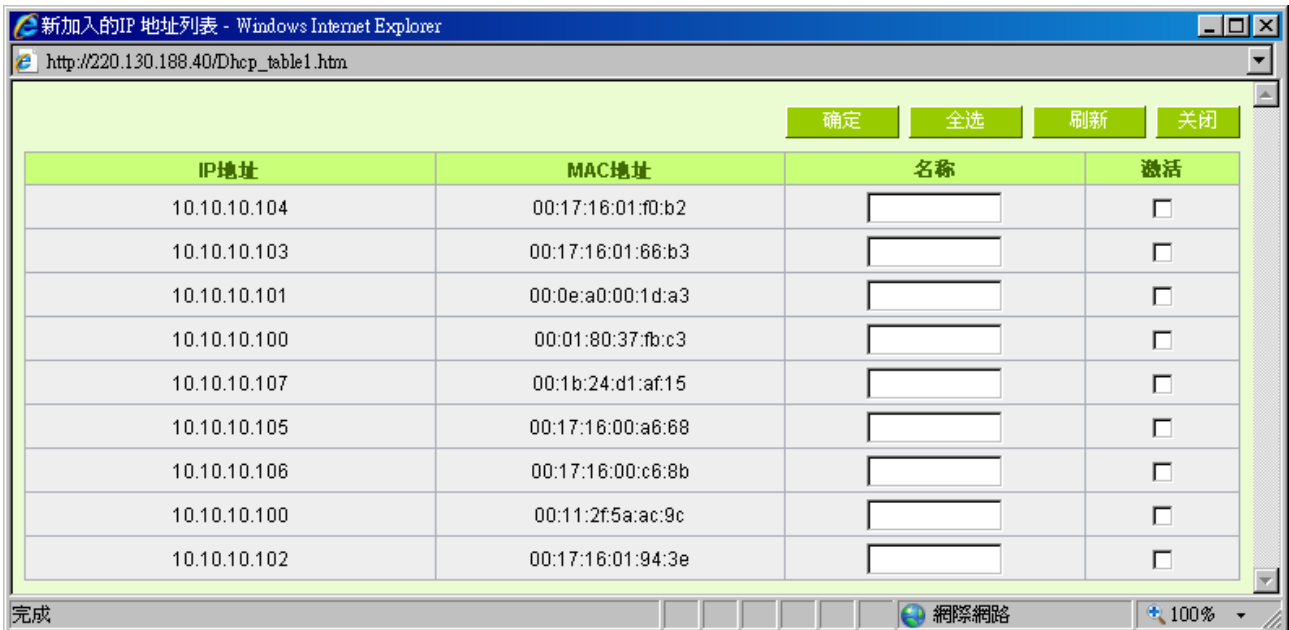


列表设置的 IP 将无法上网。

**封锁未绑定或绑定列表中未激活的用户:** 此选项打勾后,只要不在列表中或是在列表中未激活绑定功能的 MAC 地址都无法上网。

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 地址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 QoS 安全路由器且还未绑定的 MAC 地址,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,则表示此用户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。

## 九、Wireless 无线网络

Wireless 无线网络功能默认为开启，当路由器正常开机完成后，WLAN 灯亮，此时客户端设备即可在无线网络中找到 QNO\_AP\_1 的 SSID 来连接网络。若需更改设定可参考以下说明。



## 9.1 基本设定

### 无线网络

网络模式 :	11bgn Mixed Mode
国码 :	TW (Taiwan)
频道 :	频道 1
Wifi多媒体功能(WMM) :	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭 <span>进阶内容显示</span>
发射功率 :	100 (范围 1-100, 预设值 100)
频道带宽 :	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40

### SSID状态栏

编号	状态	SSID	广播 SSID	AP 隔离	安全性模式	访问过滤	客人网络	编辑
1	激活	QNO_AP_1	激活	关闭	关闭	关闭	关闭	Edit
2	关闭	QNO_AP_2	激活	关闭	关闭	关闭	关闭	Edit
3	关闭	QNO_AP_3	激活	关闭	关闭	关闭	关闭	Edit
4	关闭	QNO_AP_4	激活	关闭	关闭	关闭	关闭	Edit

确定

取消

激活无线网络	是否要激活无线网络功能。
网络模式	建议使用预设的「11bgn Mixed Mode」。其它另有「11bg Mixed Mode」、「11b Only」、「11g Only」、「11n Only」。
国码	选择你所在的国家。按照国际域名组织定义，TW，HK，CN 还需要加入“国家/地区代码”
频道	点下拉式选单选择这台装置使用的无线网络频道。请选择一个未被使用的频道，避免被其他的无线网络干扰。若不知道附近无线网络使用的频道，选择「自动」让系统自动选择可用的频道。
Rate (11bg Mixed Mode, 11b Only 或 11g Only)	选择使用的无线传输速率。默认为「自动」，设备会自动调整传输速率以达到最佳效果。
Wifi 多媒体功能(WMM)	是否要启用 Wifi 多媒体功能(WMM)功能。
Wifi 多媒体功能(WMM)	<p><b>自动省电模式(APSD)</b></p> <p>启用此功能，本装置将查询连上来的客户端无线网络卡是否启用省电功能，并据此传送带有省电标记的封包来调整。</p> <p><b>DLS功能</b></p>

进阶内容显示

	<p>Direct Link Setup(DLS) 连接至无线路由器的客户端必须同时支持此功能才可使用。</p> <p><b>基地台之WMM参数</b></p> <p>透过调整参数来控制WMM效果，建议以默认值为主。</p> <p><b>Wifi多媒体(WMM)</b></p> <table border="1" data-bbox="662 622 1422 698"> <tr> <td>自动省电模式(APSD) :</td> <td><input type="radio"/> 激活 <input checked="" type="radio"/> 关闭</td> </tr> <tr> <td>DLS功能 :</td> <td><input type="radio"/> 激活 <input checked="" type="radio"/> 关闭</td> </tr> </table> <p><b>基地台的WMM参数</b></p> <table border="1" data-bbox="662 763 1422 945"> <thead> <tr> <th></th> <th>仲裁帧间隙数</th> <th>最小竞争窗口</th> <th>最大竞争窗口</th> <th>传输机会</th> <th>存取指令</th> <th>回应策略</th> </tr> </thead> <tbody> <tr> <td>声音(最优先)</td> <td>1</td> <td>3</td> <td>7</td> <td>47</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>视频(最优先)</td> <td>1</td> <td>7</td> <td>15</td> <td>94</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>最佳性能(较优先)</td> <td>3</td> <td>15</td> <td>63</td> <td>0</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>后台运行(低优先)</td> <td>7</td> <td>15</td> <td>1023</td> <td>0</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="确定"/> <input type="button" value="取消"/> </p>	自动省电模式(APSD) :	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭	DLS功能 :	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭		仲裁帧间隙数	最小竞争窗口	最大竞争窗口	传输机会	存取指令	回应策略	声音(最优先)	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>	视频(最优先)	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>	最佳性能(较优先)	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>	后台运行(低优先)	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
自动省电模式(APSD) :	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭																																							
DLS功能 :	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭																																							
	仲裁帧间隙数	最小竞争窗口	最大竞争窗口	传输机会	存取指令	回应策略																																		
声音(最优先)	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>																																		
视频(最优先)	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>																																		
最佳性能(较优先)	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>																																		
后台运行(低优先)	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>																																		
发射功率	预设的发射功率为 100%，若想缩小无线网络的覆盖范围，输入较小的值，降低发射功率。																																							
频道带宽 (11n Only 或 11bgn Mixed Mode)	选择使用 20 MHz 或让装置自动选择 20 或 40MHz 的带宽。																																							
SSID 状态栏	显示系统已使用的各个 SSID 的状态，点选「编辑」按钮可进入设定页面。																																							

## 9.2 安全设定

### ④ 选择 SSID

编号：	1
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
SSID：	QNO_AP_1
BSSID：	00:17:16:05:40:60
广播 SSID：	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
AP隔离：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
客人网络：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭

### ④ 安全性模式

认证模式：	关闭
-------	----

### ④ WPS设定

WPS：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
------	--

### ④ WDS设定

WDS：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
------	--

### ④ 访问过滤

设定模式：	关闭
-------	----

新增MAC地址：  -  -  -  -  -

确定

取消

## 9.2.1 选择 SSID

### 选择 SSID

编号：	1
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
SSID：	QNO_AP_1
BSSID：	00:17:16:05:40:60
广播 SSID	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
AP 隔离：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
客人网络：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭

编号	这组 SSID 的编号。
状态	这组 SSID 是否有启用。
SSID	在无线网络中的名称。SSID 又称 ESSID 延伸无线网络标识符，是用来辨识及建立无线网络联机用的自定网络名称。同一个网络或子网的多个 AP 可以使用同一个名称。
BSSID	此 SSID 的 MAC 地址
广播 SSID	选择是否要在无线网络中显示此 SSID。若选择关闭则无线网络客户端或无线网络卡无法扫描到这台装置，而必须手动输入无线网络标识符以连到这台设备。
AP 隔离	启用这个功能后，则连接到这个 SSID 下的各个客户端彼此无法沟通。
客人网络	启用这个功能后，连接到这个 SSID 下的各客户端将无法连接到局域网络(有线)的客户端，只能联机到因特网。限定在第 2~4 个 SSID 设定此功能。

## 9.2.2 安全性模式

QNO 提供以下数种安全性模式，每种加密模式需要输入的密钥不同，AP 与无线网络卡/无线网络客户端的密钥要一致才能联机。

### 安全性模式

认证模式：	<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #e0e0e0; padding: 2px;">关闭</div> <div style="background-color: #0070c0; color: white; padding: 2px;">关闭</div> <div style="padding: 2px;">开启 WEP</div> <div style="padding: 2px;">共享 WEP</div> <div style="padding: 2px;">WEP 自动</div> <div style="padding: 2px;">WPA Enterprise</div> <div style="padding: 2px;">WPA Personal</div> <div style="padding: 2px;">WPA2 Enterprise</div> <div style="padding: 2px;">WPA2 Personal</div> <div style="padding: 2px;">WPA/WPA2 Personal Mixed Mode</div> <div style="padding: 2px;">WPA/WPA2 Enterprise Mixed Mode</div> <div style="padding: 2px;">802.1X</div> </div>
-------	---

## 1. WEP 认证模式

- 开启 WEP
- 共享 WEP
- WEP 自动

当选择「开启 WEP」或「共享 WEP」，所有无线网络客户端都要选择相同的模式才能连上本 AP 装置；若选择「WEP 自动」，无线网络客户端可任选一种认证模式，都可连上本 AP 装置。

### 🔹 WEP安全性设定

预设密钥：	<input type="text" value="密钥1"/>
WEP密钥1：	<input type="text"/> 密钥1 类型 <input type="text" value="64-bit (10 hex digits)"/>
WEP密钥2：	<input type="text"/> 密钥2 类型 <input type="text" value="64-bit (10 hex digits)"/>
WEP密钥3：	<input type="text"/> 密钥3 类型 <input type="text" value="64-bit (10 hex digits)"/>
WEP密钥4：	<input type="text"/> 密钥4 类型 <input type="text" value="64-bit (10 hex digits)"/>

预设密钥	选择 4 组中的其中一组做为加密密钥。
64-bit (10 hex digits)	请在 WEP 密钥字段输入刚好 10 个 16 进位值(0~9、a~f、A~F)做为加密密钥。
128-bit (26 hex digits)	请在 WEP 密钥字段输入刚好 26 个 16 进位值(0~9、a~f、A~F)做为加密密钥。
64-bit (5 ASCII)	请在 WEP 密钥字段输入刚好 5 个 ASCII 字母(英文字母、数字)做为加密密钥。
128-bit (13ASCII)	请在 WEP 密钥字段输入刚好 13 个 ASCII 字母(英文字母、数字)做为加密密钥。

## 2. WPA 认证模式

### (1) 采用 pre-shared key(PSK) 的 Personal 模式

个人及家庭用户，建议选择采用 pre-shared key 的 Personal 模式，如 WPA Personal、WPA2 Personal、WPA/WPA2 PersonalMixed mode。此种认证模式不须架设 RADIUS 认证服务器，只需路由器及无线网络客户两端都输入加密密钥来作加密。

- WPA Personal
- WPA2 Personal
- WPA/WPA2 PersonalMixed mode

### 🔹 Wireless安全设定

WPA算法：	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> 自动
通行码：	<input type="text"/>
密钥更新间隔：	<input type="text" value="0"/> 秒 (0~4194303)

WPA 算法	选择 TKIP、AES、自动。需注意只有选择 AES 算法才能达到 802.11n 的无线传输速率。若不清楚无线网络客户端会使用何种算法，选择「自动」以让系统自动切换。
通行码	输入 8~32 英文字符的通行码，只要 AP 装置与无线网络卡/客户端装置都设定为同一个通行码，无线网络就会连通并收到加密保护。
密钥更新间隔	WPA/WPA2-PSK 使用的算法会在固定时间重整密钥，可以调整重整的时间间隔。

## (2) Enterprise 模式

欲使用 WPA 或 WPA2 模式，需要架设 RADIUS 认证服务器作为认证用途。

- WPA Enterprise
- WPA2 Enterprise
- WPA/WPA2 Enterprise Mixed mode

### Wireless 安全设定

WPA算法：	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> 自动
密钥更新间隔：	0 秒 (0~4194303)
PMK快取：	10 分
预先认证：	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭

### RADIUS 服务器

IP 地址：	0 . 0 . 0 . 0
服务器套接字：	1812
共享密钥：	QNO
会话超时：	0 秒 (0 or 60~999999)

WPA 算法	选择 TKIP、AES、自动。需注意只有选择 AES 算法才能达到 802.11n 的无线传输速率。若不清楚无线网络客户端会使用何种算法，选择「自动」以让系统自动切换。
密钥更新间隔	WPA/WPA2-PSK 使用的算法会在固定时间重整密钥，可以调整重整的时间间隔。
PMK 快取 (WPA2 Enterprise)	当无线网络客户会在多个无线网络之间漫游时，此功能可让无线网络客户、与路由器暂存认证的信息，以便于增快更换无线网络覆盖范围时的认证程序。
预先认证 (WPA2 Enterprise)	预先认证允许无线网络客户在已经有连接一个无线网络时，就能预先和另一个无线网络预先认证，以加速更换无线网络的认证程序。
IP 地址	输入 RADIUS 认证服务器的 IP 地址。
服务器通讯端口	输入 RADIUS 认证服务器的通讯端口。
共享密钥	输入认证初期的共享密钥。
会话超时	输入一个联机最大的空闲时间；若闲置超过这个时间，会话会被停止。



### 3. 802.1X 认证模式

802.1X 模式，也需要架设 RADIUS 认证服务器作为认证用途。

#### 🔵 RADIUS 服务器

IP 地址：	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
服务器通讯端口：	<input type="text" value="1812"/>
共享密钥：	<input type="text" value="QNO"/>
会话超时：	<input type="text" value="0"/> 秒 (0 or 60~999999)

IP 地址	输入 RADIUS 认证服务器的 IP 地址。
服务器通讯端口	输入 RADIUS 认证服务器的通讯端口。
共享密钥	输入认证初期的共享密钥。
会话超时	输入一个联机最大的空闲时间；若闲置超过这个时间，会话会被停止。

## 9.2.3 WPS 设定

在 Wireless 安全设定为 WPA Personal、WPA2 Personal、WPA/WPA2 Personal Mixed Mode 时，可搭配设定 WPS 功能。当设备进入 WPS 等待模式时，会持续此模式等待 2 分钟，若超过 2 分钟都没有建立联机则会结束等待。

#### 🔵 WPS 设定

WPS：	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
本装置的个人标识符：	<input type="text" value="26988139"/> <input type="button" value="Generate"/>
WPS 模式：	<input checked="" type="radio"/> 个人标识号(PIN) <input type="text"/> <input type="radio"/> 按钮(PBC)

**连线**

#### 1. 使用个人标识符(PIN)设定 WPS

- (1) 点选「激活」WPS。
- (2) 将另一端无线网络客户设备的 PIN 码，填写入个人标识符(PIN)的字段中；同样地，无线网络客户设备也需填入本路由器的个人标识符(PIN)。
- (3) 填写完个人标识符(PIN)后，点选「连线」，此时两端设备开始连接 WPS、UI 会重新整理、WPS 灯号亮起。
- (4) 在无线网络客户设备确认 WPS 是否有连接成功。

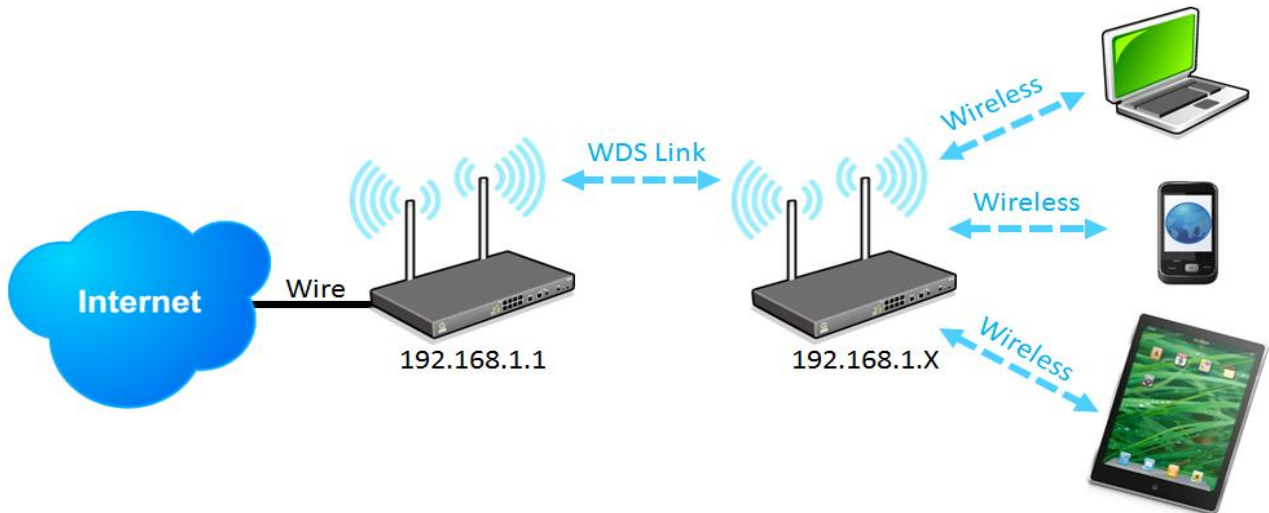
#### 2. 使用按钮(PBC)设定 WPS

- (1) 点选「激活」WPS。
- (2) 勾选按钮(PBC)，点选「连接」；或者是按压硬件上的 WPS 按钮约 5 秒钟，直至 WPS 灯号亮起。此时两端设备开始连接 WPS、UI 会重新整理。同样地，无线网络客户设备也需同样操作。

(3) 在无线网络客户设备确认 WPS 是否有连接成功。

## 9.2.4 WDS 设定

无线分布式系统(Wireless Distribution System, WDS)。系统将会透过 WDS 通讯转送网络封包给无线网络内其他 WDS 装置，以延伸无线网络覆盖范围。



1. 两台设备的 LAN IP 需设定为同一网段的不同 IP。例如图示的 192.168.1.1 与 192.168.1.X
2. 两台设备的以下设定都需一致：(红色箭头字段)

### (1) 基本设定

#### 无线网络

 网络模式：	11bgn Mixed Mode
国码：	TW (Taiwan)
 频道：	频道 1
Wifi多媒体功能(WMM)：	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
发射功率：	100 (范围 1-100, 预设值 100)
 频道带宽：	<input checked="" type="radio"/> 20 <input type="radio"/> 20/40

※在 WDS 模式下，「频道带宽」需选择 20。

### (2) 安全设定

#### 安全性模式

 认证模式：	关闭
---	----

填

3. 两台设备都需开启 WDS 模式。WDS 设定都互相填写对方的 MAC 地址。WDS 模式所支持的最大 AP 数量依各机种会有差异。

(1) 可在设定窗口中直接填写(如下图)

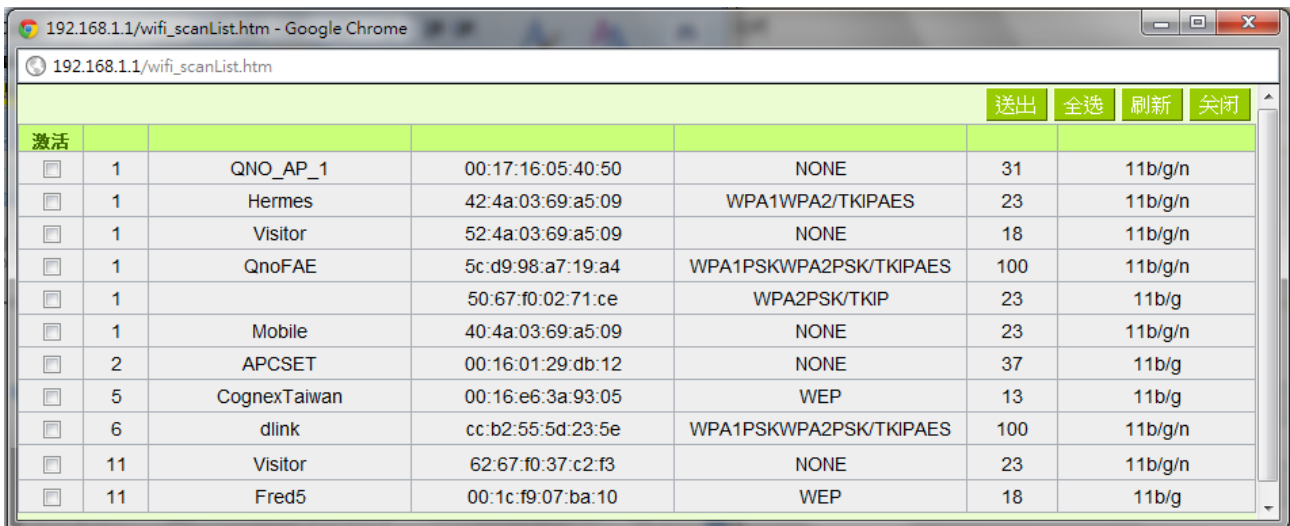
WDS設定

<b>WDS :</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
<b>AP MAC :</b>	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
<b>AP MAC :</b>	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
<b>AP MAC :</b>	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
<b>AP MAC :</b>	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>

检测实时保护

※ 若认证模式选择 WEP，则系统会自动安排 WEP 四组密钥依序对应此四组 AP MAC，填入时请注意顺序。

(2) 或是点选「检查实时扫描」，勾选已存在的 AP，然后点选「送出」按钮。



							送出	全选	刷新	关闭
激活										
<input type="checkbox"/>	1	QNO_AP_1	00:17:16:05:40:50	NONE	31	11b/g/n				
<input type="checkbox"/>	1	Hermes	42:4a:03:69:a5:09	WPA1WPA2/TKIPAES	23	11b/g/n				
<input type="checkbox"/>	1	Visitor	52:4a:03:69:a5:09	NONE	18	11b/g/n				
<input type="checkbox"/>	1	QnoFAE	5c:d9:98:a7:19:a4	WPA1PSKWPA2PSK/TKIPAES	100	11b/g/n				
<input type="checkbox"/>	1		50:67:f0:02:71:ce	WPA2PSK/TKIP	23	11b/g				
<input type="checkbox"/>	1	Mobile	40:4a:03:69:a5:09	NONE	23	11b/g/n				
<input type="checkbox"/>	2	APCSET	00:16:01:29:db:12	NONE	37	11b/g				
<input type="checkbox"/>	5	CognexTaiwan	00:16:e6:3a:93:05	WEP	13	11b/g				
<input type="checkbox"/>	6	dlink	cc:b2:55:5d:23:5e	WPA1PSKWPA2PSK/TKIPAES	100	11b/g/n				
<input type="checkbox"/>	11	Visitor	62:67:f0:37:c2:f3	NONE	23	11b/g/n				
<input type="checkbox"/>	11	Fred5	00:1c:f9:07:ba:10	WEP	18	11b/g				

### 9.2.5 访问过滤

存取原则包含「拒绝」与「允许」。「拒绝」原则将拒绝MAC地址列表上的无线网络客户端的连线；而「允许」原则的判断则是相反，只接受有在MAC地址列表上无线网络客户端的连线。

#### 访问过滤



设定模式	拒绝：被设定在 MAC 地址列表上的无线网络客户端将被系统拒绝连线。 允许：只有被设定在 MAC 地址列表上的无线网络客户端才会被系统允许连线。
增加 MAC 地址	地址：输入 MAC 地址以套用到存取原则。在无线网络卡/客户端的卷标及设定软件、接口上可以找到如同这种格式的值「00:11:22:33:44:55」，输入到这个字段。

## 9.3 客户端联机清单

显示目前有哪些已连接的无线网络客户

▶ 客户端联机列表

MAC 地址设定	DHCP IP	主机名称	SSID	Rate
D8:B3:77:1C:1D:0C	192.168.1.102	Android_356440043044963	QNO_AP_1	65
04:54:53:74:DF:1E	192.168.1.101	TINAmato-iPad	QNO_AP_1	65

刷新

MAC 地址	无线网络客户设备的 MAC 地址。
DHCP IP	系统分配给无线网络客户的 IP 地址。
主机名称	该台无线网络客户的设备名称。
SSID	无线网络客户所加入的 SSID。
Rate	信号强度指数(%)。

## 9.4 無線流量統計

▶ 传送统计

成功传送网络包：	470338
重传成功的网络包：	12228
重传失败的网络包：	14
成功接收CTS的RTS网络包：	0
接收CTS失败的网络包：	0

▶ 接收统计

成功接收的网络包：	3861403
接收含有CRC错误的网络包：	3337781

刷新

※单位皆为网络包数

成功传送的网络包	成功送出的网络包数量。
重送成功的网络包	经过重新尝试才成功送出的网络包数量。
重送失败的网络包	经过多次尝试仍然没有送出的网络包数量。
成功接收 CTS 的 RTS 网络包	成功接收 CTS 时的 RTS 网络包数量。
接收 CTS 失败的 RTS 网络包	接收 CTS 失败时的 RTS 网络包数量。
成功接收的网络包	封包接收的网络包数量。
接收含有 CRC 错误的网络包	接收到含有 CRC 错误的网络包数量。

## 十、QoS 带宽管理功能

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网吧、企业等的实际需求，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。

### 10.1 带宽设置(QoS)

#### ● 填入 ISP 线路实际可供使用带宽

端口	上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)
广域网1	10000	10000
广域网2	10000	10000
USB1	256	2048
USB2	256	2048

#### ● 网络品质服务配置(QoS)

端口： 广域网1  广域网2  USB1  USB2

服务端：

服务端新增或删除表

IP 地址： .  .  .  到

目的：

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

删除所选择的项目

激活 动态智能 QoS

### 10.1.1 带宽设置

#### ④ 填入 ISP 线路实际可供使用带宽

端口	上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)
广域网1	10000	10000
广域网2	10000	10000
USB1	256	2048
USB2	256	2048

WAN 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。例如每个 IP 及服务端口（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。

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。

### 10.1.2 QoS 设置

QoS 可以选择两种方式，无法同时使用，一为流量控制(带宽管理)，另一个为优先权控制，设置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 (带宽管理)- 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 或一个范围的 IP 的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)

端口： 广域网1  广域网2  USB1  USB2

服务端口：

IP 地址： .  .  .  到

目的：

最小带宽： Kbit/sec      最大带宽： Kbit/sec

频宽共享方式：  
 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：

**接口位置：** 勾选此条 QoS 设置要控制在哪条 WAN 执行，可单独或全部勾选。

**服务端口：** 选择此条 QoS 所要设置的带宽控制为哪个，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哪些?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 到 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 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 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(Server in LAN，上传)：若您有架设对外的 Server 网站在 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(Server in LAN，下载)：若您有架设网站在 QoS 安全路由器内网，则此选项为控制外部对此服务器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升级时，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。
- 保证带宽 & 最大可用带宽：**  
(Kbit/Sec)
- 保证带宽：此为限制或保证此条规则的最小可使用带宽。
  - 最大可用带宽：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置值。
- 请注意！这里填入的数值单位是 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。
- 管制时间：**
- 选择“所有时间”，此 QoS 设置在所有时间都有效果，如果选择“从\_\_：\_\_到\_\_：\_\_”填入时间段（24 小时计时制，例如 19：00 到 24：00），以及勾选“每天/周日/周一/周二/周三/周四/周五/周六”的某一天或者几天，其 QoS 设置只在所勾选设置的特定时间段内有效。
- 带宽分配方式：**
- 此范围每一 IP 地址独享此设置带宽：  
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保证带宽到最大可用带宽)带宽范围，例如若是针对每台计算机 (IP 地址)做的规则设置，则每台计算机(IP 地址)都可以有这么大的带宽。
  - 此范围所有 IP 地址共享此设置带宽：  
若选择此规则的话，其表示所有 IP 或此服务端口共享这段(保证带宽到最大可用带宽)带宽范围。
- 请注意！当您选择带宽的共享方式时，要留意实际应用的情况，以避免选择不恰当的方式而造成带宽太小无法正常使用网络。例如，内网多人使用 FTP 做文件下载，若是您希望 FTP 不会占用掉大部分的带宽，您就可以选择共享带宽，不论内网有多少人使用 FTP 做文件下载，总和所占用的带宽是固定的。
- 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，也就是越后面设置的规则会优先执行，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。

**删所选中的项目：** 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管理设置的规则，并可直接点击“编辑”做修改（见表后详解）。

**确定：** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。

**取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

**显示开启表：**

点击左下方的“显示开启表”按钮，会出现以下的对话窗口。您可以选择以“规则”来显示已设置的规则，或是以“接口位置”来显示已设置的规则。点击“刷新”可以重新显示窗口，点击“关闭”将结束这个对话窗口。可直接点击“编辑”做修改。

<input checked="" type="radio"/> 规则 <input type="radio"/> 接口位置 <span>刷新</span> <span>关闭</span>								
服务端口	IP地址	目的	保证带宽 (Kbit/sec)	最大可用带宽 (Kbit/sec)	带宽分配方式	激活	接口位置	编辑

**范例一：若希望内网去做 ftp 下载(Active Mode)，在每个广域网都只能共同使用 50kbit 下载带宽要如何设置？**

以 2WAN 路由器产品为例，接口位置勾选广域网 1、2，服务端选择“FTP[TCP /21~21]”，在 IP 地址填入局域网 IP 范围（例如 192.168.1.1 到 192.168.1.254），目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 50kbit/sec，表示 FTP 下载最多只能使用到 50kbit/sec 的带宽。带宽共享方式选择“此 IP 地址共享此设置带宽”，如此不管内网有多少人使用 FTP，不论哪个广域网接口，FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击“新增”即可将此规则加入。

接口位置： 广域网1  广域网2

服务端口：FTP [TCP/21~21]

IP地址：192 . 168 . 1 . 1 到 256

目的：下载

保证带宽：2 Kbit/sec 最大可用带宽：50 Kbit/sec

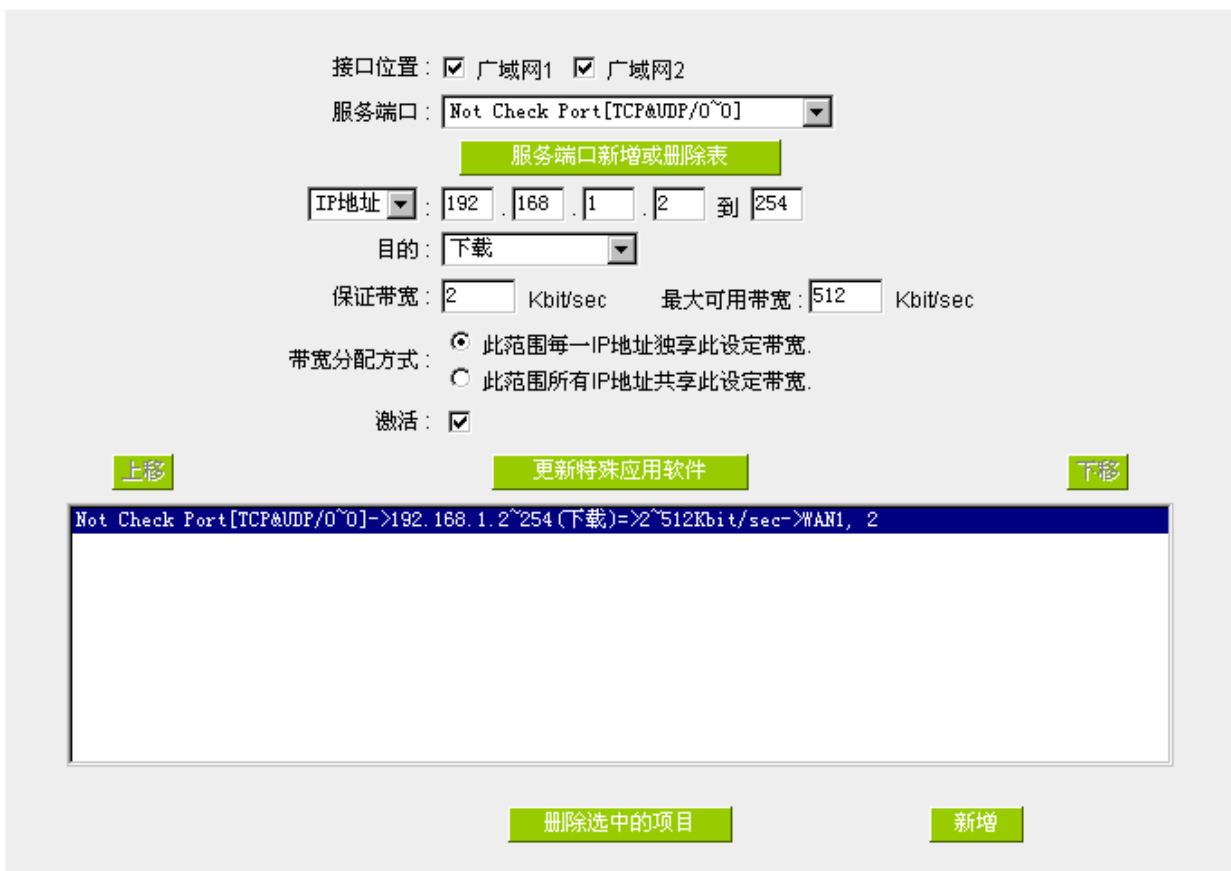
带宽分配方式：  
 此范围所有IP地址共享此设定带宽.  
 此范围每一IP地址独享此设定带宽.

激活：

FTP [TCP/21~21]-> 192.168.1.1~256(下载)=>2~50Kbit/sec->广域网1, 2
--

范例二：若希望内网所有 IP 每人，在每个广域网最大下载使用带宽只能有 512Kbit，需要 IP 一个一个设置吗？

不需要一个 IP 一个 IP 设置。以 2WAN 路由器产品为例，接口位置勾选广域网 1、2，服务端选择“No Check Port[TCP&UDP /0~0]”，在 IP 地址填入 192.168.1.2 到 254(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec 表示每个 IP 保证有 2kbit/sec 的带宽 最大带宽填入 512kbit/sec 表示每个 IP 最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择“此范围每一 IP 地址最大及最小可用带宽”，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选激活，最后点击“新增”即可将此规则加入。



接口位置： 广域网1  广域网2

服务端：

IP地址： .  .  .  到

目的：

保证带宽： Kbit/sec 最大可用带宽： Kbit/sec

带宽分配方式：  
 此范围每一IP地址独享此设定带宽。  
 此范围所有IP地址共享此设定带宽。

激活：

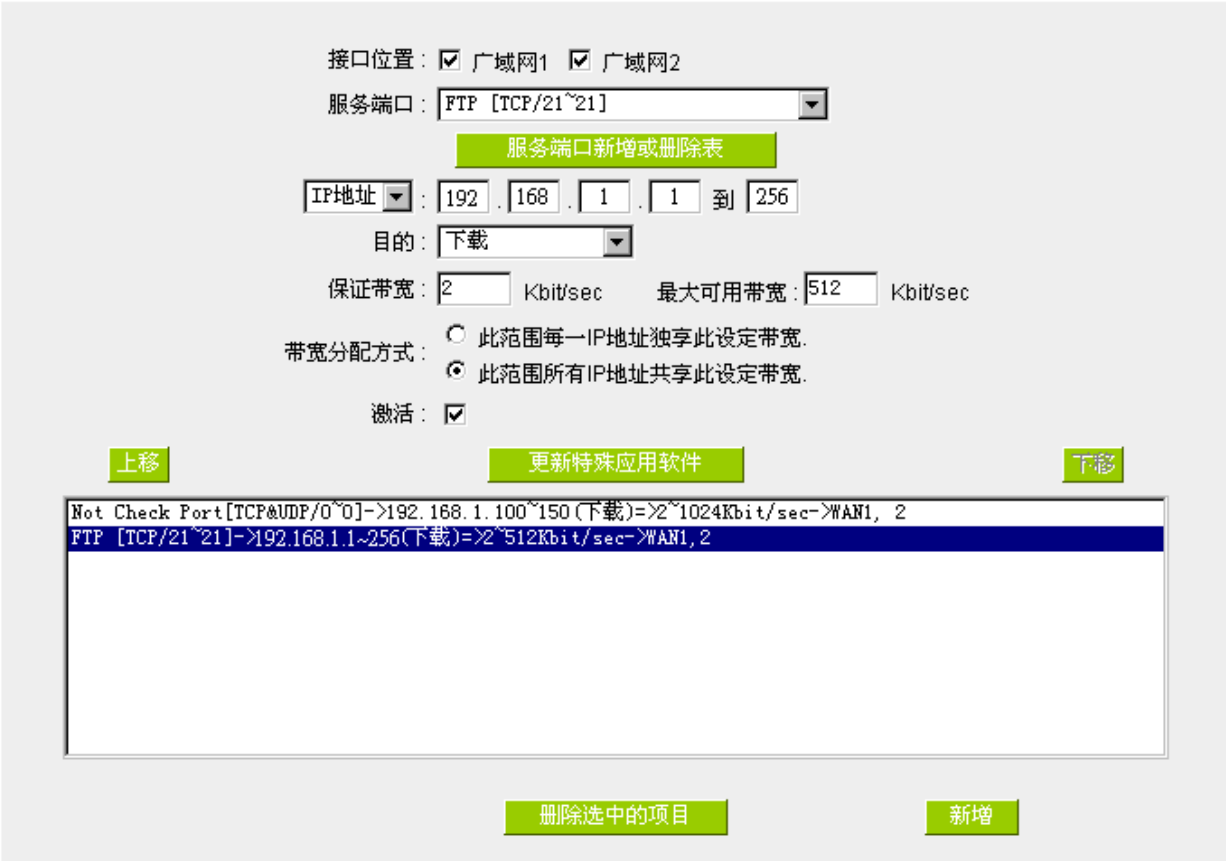
Not Check Port [TCP&UDP/0~0]->192.168.1.2~254 (下载)=>2~512Kbit/sec->WAN1, 2

范例三：若希望内网所有 IP 192.168.1.100-150 每人，在每个广域网最大下载使用带宽只能有 1M，但当使用 ftp 下载时(Active Mode)都只能共享 512Kbit 时要如何设置？

以 2WAN 路由器产品为例 第一条规则接口位置勾选广域网 1 2 服务端选择“No Check Port[TCP&UDP /0~0]”，在 IP 地址填入 192.168.1.100 到 150(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 1024kbit/sec，表示每个 IP 最多只能使用到 1M/sec 的带宽。带宽共享方式选择“此范围每一 IP 地址最大及最小可用带宽”，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选激活，最后点击“新增”即可将此规则加入。

第二条规则接口位置勾选广域网 1 2 服务端选择“FTP[TCP/21~21]”，填入局域网 IP 范围（例如 192.168.1.1 到 192.168.1.254），目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示 FTP 下载最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择“此 IP 地址共享此设置带宽”，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击“新增”即可将此规则加入。

请注意！QoS 带宽管理的执行顺序为由列表最下面那一条往上做执行动作，所以要将先执行的规则往最下面移。以这个范例来说，先执行 FTP 的共享带宽，在执行每个 IP 的保证以及最大可用带宽。因此若是内网有人使用 FTP 下载，就会先受到第一条规则的限制，最大只能用到 512kbit/sec。若是将规则反过来，将上述的第一条规则移到最下方来先执行，则每个 IP 最大可用到 1M 的带宽，此时用 FTP 下载也就可以用到 1M 的带宽，那么后执行的 FTP 带宽限制在 512kbit 就不会执行，也就没有意义了！



接口位置： 广域网1  广域网2

服务端：

IP地址： .  .  .  到

目的：

保证带宽： Kbit/sec    最大可用带宽： Kbit/sec

带宽分配方式：  
 此范围每一IP地址独享此设定带宽。  
 此范围所有IP地址共享此设定带宽。

激活：

Not Check Port[TCP&UDP/0~0]->192.168.1.100~150(下载)=>2~1024Kbit/sec->WAN1, 2
FTP [TCP/21~21]->192.168.1.1~256(下载)=>2~512Kbit/sec->WAN1, 2

### 10.1.3 Smart QoS

无需网管进行烦琐配置的智能型带宽管理 Smart QoS 功能，自动压抑占用带宽用户，来解决内网 QoS 管理的问题，简化网管的管理工作。

激活动态智能QoS

当任一广域网带宽使用率达到  %时, 激活智能QoS(此值为0表示永久激活)

内网IP在所有广域网最大容忍上传带宽:  Kbit/sec

内网IP在所有广域网最大容忍下载带宽:  Kbit/sec

当任一IP使用超过上述设定上传或下载带宽时, 此IP则使用下列指定带宽

上传带宽  
 (广域网1:  Kbit/sec 广域网2:  Kbit/sec  
 广域网3:  Kbit/sec 广域网4:  Kbit/sec)

下载带宽  
 (广域网1:  Kbit/sec 广域网2:  Kbit/sec  
 广域网3:  Kbit/sec 广域网4:  Kbit/sec)

激活二次惩罚

---

管制时间为  到  :  到  :  (时间格式:24小时制)

每天  周日  周一  周二  周三  周四  周五  周六

\*此为示意图，会因产品线不同，图形会有所差异

**激活动态智能 QoS:**

当任一广域网带宽使用率达到\_\_%时, 激活智能 QoS

内网 IP 在所有广域网最大容忍上传带宽 :

勾选激活动态智能 QoS。

当带宽使用率达到实际带宽的一个%比时，将激活智能 QoS 功能，您可输入需要的数值，系统预设是 60%。

当带宽使用率超过设定的启动百分比时，系统自动检查单一 PC IP 的上传下载使用带宽，若超过设定的值，将给予惩罚，请填入内网 IP 上传最大容许使用带宽。

由于 Smart QoS 进行带宽检查时，可能会消耗影响部分系统效能，所以假设不太需要管制上传带宽，您可以取消勾选此项目表示不检查上传带宽的使用状态。

**内网 IP 在所有广域网最大容忍下载带宽：**

当带宽使用率超过设定的启动百分比时，系统自动检查单一 PC IP 的上传下载使用带宽，若超过设定的值，将给予惩罚，请填入内网 IP 下载最大容许使用带宽。

**当任一 IP 使用超过上述设定上传或下载带宽时，此 IP 则使用下列指定带宽：**

由于 Smart QoS 进行带宽检查时，可能会消耗影响部分系统效能，所以假设不太需要管制下载带宽，您可以取消勾选此项目表示不检查下载带宽的使用状态。

当任一 IP 使用超过上述设定上传或下载带宽时，就实行惩罚措施，并以各个广域网络的上传 / 下载分别设定，惩罚后允许使用的带宽是多少

**激活二次性惩罚：**

点选勾选“激活二次性惩罚：”后，VPN 防火墙内部设置好二次惩罚条件，当内部网络上网用户上网过程中的上传与下载达到内部条件将执行二次惩罚。

**显示处罚列表：**

点选后，在弹出的对话框中将会显示处罚中的 IP，上行限制中，下载限制中以及二次惩罚信息。

**管制时间：**

选择“所有时间”，此 QoS 设定在所有时间都有效果，如果选择“从\_\_:\_\_到\_\_:\_\_”填入时间段（24 小时记时制，例如 19：00 到 24：00），以及勾选“每天/周日/周一/周二/周三/周四/周五/周六”的某一天或者几天，其 QoS 设定在所勾选设定的特定时间段内有效。



## 10.2 会话数管理

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

另外，若计算机中了类似冲击波的病毒而产生大量对外发会话请求时，也可以达到抑制作用。

### 会话数管制设定

#### ▶ 联机数设置

<input type="radio"/> 关闭	
<input type="radio"/> 每一内网 IP 最大对外联机数不可超过 <input type="text" value="300"/> 联机状态 (session)	
<input checked="" type="radio"/> 每一内网 IP 最大对外联机数不可超过 TCP <input type="text" value="1500"/> , UDP <input type="text" value="400"/> 联机状态 (session)	
<input type="radio"/> 当单一个 IP 联机数到达 <input type="text" value="200"/> 联机状态 (session)	<input type="radio"/> 阻挡此 IP 建立新连线达 <input type="text" value="5"/> 分钟
	<input type="radio"/> 封锁此 IP 所有连线达 <input type="text" value="5"/> 分钟

**关闭：** 不使用此会话数管控功能。

**每一内网 IP 最大对外联机数不可超过\_\_联机状态 (Session)** 此选项为限制每一台内网的计算机最大可建立的对外会话数，当用户计算机使用会话数到达此限制值时，要建立新的会话必须等到之前的会话结束后才能再建立。

例如，当用户使用 BT 或 P2P 等下载且会话数超过此设定值后，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。

**每一内网 IP 最大对外联机数不可超过 TCP\_\_UDP\_\_：** 除了以会话的总数量做限制之外，你也可选择针对 TCP/UDP 通讯协议类型，个别设定限制值，例如限制单一 TCP 会话数不可超过 150，UDP 会话数不可超过 50。

**若有 IP 对外会话数 在\_\_分钟内阻止此 IP 建立新会话** :此选项为当客户端计算机使用会话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会话，就算旧会话已经结束，也必须等到设定时间过后才能再建立新的会话。

**在\_\_分钟内封锁此 IP 所有会话** :此选项为当客户端计算机使用的会话数到达您的设定数值时，此用户正在使用的所有会话都将被清除，且在 5 分钟之内将不能建立任何会话 (不能上网)，必须等到设定时间过后才能再建立新的会话。

## 十一、防火墙设置

本章节介绍防火墙设置的选项，以及网络存取控制的设置，保证网络的安全性。

### 11.1 基本设置

从防火墙功能的一般设置选项当中，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。

<b>防火墙：</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
<b>SPI数据包检测：</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
<b>防止DoS攻击功能：</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭 <span style="background-color: #92d050; padding: 2px;">高级设定</span>
<b>阻止广域网回应功能：</b>	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
<b>远程管理功能：</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭 端口： <input type="text" value="80"/>
<b>允许Multicast组播穿透：</b>	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭
<b>防止ARP病毒攻击：</b>	<input type="radio"/> 激活 <input checked="" type="radio"/> 关闭 每秒主动发送 <input type="text" value="20"/> 笔ARP封包

- 防火墙功能：** 此为选择开启或关闭防火墙功能。默认激活。
- SPI 数据包检测：** 此为数据包主动侦测检验技术，防火墙主要运行在网络层，但是通过执行对每个连结的动态检验，也拥有应用程序的警示功能。同时，数据包检验型防火墙可以拒绝非标准的通讯协议所使用的连结。默认激活。
- 防止 DoS 攻击功能：** 此为保护 DoS 攻击，如 SYN Flooding，Smurf，LAND，Ping of Death，IP Spoofing 等。默认激活。
- 阻止广域网响应功能：** 若是选择激活的话，则 QoS 安全路由器会关闭对外的 ICMP 与不正常联机的数据包响应，所以若是您从外部去 ping 此台路由器的 WAN IP 是无法 ping 通的，默认值为开启拒绝对外响应的功能。
- 远程管理功能：** 远程管理功能，若您要通过远程网络 直接联机进 QoS 安全路由器的设置窗口，必需将此功能开启，并于远程于浏览器网址填路由器的外部合法 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 组播穿透：** 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数据包讯息格式。默认为关闭

**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。

**确定：** 点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。

**取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于“确定”存储动作之前才会有效。

**防止 DoS 攻击功能** 高级设定

数据包类型	广域网阈值设定	局域网阈值设定
<input checked="" type="checkbox"/> TCP_SYN_Flooding	所有数据包阈值 <input type="text" value="15000"/> Packets/sec	所有数据包阈值 <input type="text" value="15000"/> Packets/sec
	单一IP的数据包阈值 <input type="text" value="2000"/> Packets/sec	单一目的IP的数据包门限值 <input type="text" value="0"/> Packets/sec
	达到阈值便阻挡该IP <input type="text" value="5"/> 分钟	单一来源IP的数据包门限值 <input type="text" value="2000"/> Packets/sec
		达到阈值便阻挡该IP <input type="text" value="5"/> 分钟
<input checked="" type="checkbox"/> UDP_Flooding	所有数据包阈值 <input type="text" value="15000"/> Packets/sec	所有数据包阈值 <input type="text" value="15000"/> Packets/sec
	单一IP的数据包阈值 <input type="text" value="2000"/> Packets/sec	单一目的IP的数据包门限值 <input type="text" value="0"/> Packets/sec
	达到阈值便阻挡该IP <input type="text" value="5"/> 分钟	单一来源IP的数据包门限值 <input type="text" value="2000"/> Packets/sec
		达到阈值便阻挡该IP <input type="text" value="5"/> 分钟
<input checked="" type="checkbox"/> ICMP_Flooding	所有数据包阈值 <input type="text" value="200"/> Packets/sec	所有数据包阈值 <input type="text" value="200"/> Packets/sec
	单一IP的数据包阈值 <input type="text" value="50"/> Packets/sec	单一目的IP的数据包门限值 <input type="text" value="0"/> Packets/sec
	达到阈值便阻挡该IP <input type="text" value="5"/> 分钟	单一来源IP的数据包门限值 <input type="text" value="50"/> Packets/sec
		达到阈值便阻挡该IP <input type="text" value="5"/> 分钟
<input type="checkbox"/> 不受限制的来源IP地址	1. IP地址 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 到 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 2. IP地址 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 到 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
<input type="checkbox"/> 不受限制的目的地IP地址	1. <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 2. <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 3. <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 4. <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 5. <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	

**数据包类型：** QoS 安全路由器提供三种数据包传输类型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

**广域网限定值设置：**

防止来自外部网络的攻击。设置“所有数据包限定值”（即外部攻击的所有数据包数据），当其达到一个最大值（默认 15000pakets/Sec），QoS 安全路由器将只允许通过所设置最大值的数据包数。

当单一 IP 的数据包限定值（外部单一一个 IP 地址攻击的数据包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网  分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。这里您可以根据需要调整你的限定值以及阻挡时间来达到对外网攻击的有效防护，建议其限定值从大到小来调节，避免限定值过小影响正常网络的运行。

**局域网限定值设置：**

防止来自内部网络的攻击。同样，当所有数据包限定值（即外部攻击的所有数据包数据）达到一个最大值（默认 15000pakets/Sec），QoS 安全路由器将只允许通过所设置最大值的数据包数。

当单一数据包阈值（内部单一一个 IP 地址攻击的数据包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网  分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。您可以根据需要调整你的阈值以及阻挡时间来达到对内网攻击的有效防护，建议其阈值从大到小来调节，避免阈值过小影响正常网络的运行。

**不受限制的来源 IP 地址：**

输入不要被 DoS 防御设置限定值所限制的区域网来源 IP 地址或是范围

**不受限制的目的地 IP 地址：**

输入不要被 DoS 防御设置限定值所限制的目的 IP 地址

(从区域网发出的数据包)

**显示被阻挡的 IP：**



显示被 DoS 防御功能所阻挡的 IP 地址，以及该 IP 地址还剩余多少时间解除阻挡

## 11.2 访问规则设置

QoS 安全路由器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置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，例如可以设置数据包要管制的进出方向是从内部到外部还是从外部到内部，或是设置以使 IP 地址、目的地 IP 地址、IP 通讯协议状态等条件来做管制，管理者可以依照实际的需求调性设置。

### 11.2.1 默认管制规则

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网络的存取。以下就针对 QoS 安全路由器的网络存取规则条例做一说明：

QoS 安全路由器默认的网络存取规则条例：

- \*从 LAN 端到 WAN 端的所有数据包可以通过-All traffic from the LAN to the WAN is allowed
- \*从 WAN 端到 LAN 端的所有数据包不可以通过-All traffic from the WAN to the LAN is denied
- \*从 LAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the LAN to the DMZ is denied
- \*从 DMZ 端到 LAN 端的所有数据包不可以通过-All traffic from the DMZ to the LAN is denied
- \*从 WAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the WAN to the DMZ is denied
- \*从 DMZ 端到 WAN 端的所有数据包不可以通过-All traffic from the DMZ to the WAN is denied

管理者可以自定存取规则并且超越 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，不受其它自定规则所影响：

- \* HTTP 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了管理 QoS 安全路由器使用)。
- \* DHCP 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了从 QoS 安全路由器自动取得 IP 地址使用)。
- \* DNS 的服务从 LAN 端到 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 QoS 安全路由器 默认为开启的 (为了连通测试 QoS 安全路由器使用)。

跳到  / 2 页

每页显示  笔

[下一页 >>](#)

优先级	激活	管制动作	服务端口	接口位置	来源IP地址	目的IP地址	管制时间	日	编辑	删除
	<input checked="" type="checkbox"/>	允许	所有端口 [M]	局域网	任何的	任何的	所有时间			
	<input checked="" type="checkbox"/>	关闭	所有端口 [M]	广域网1	任何的	任何的	所有时间			
	<input checked="" type="checkbox"/>	关闭	所有端口 [M]	广域网2	任何的	任何的	所有时间			
	<input checked="" type="checkbox"/>	关闭	所有端口 [M]	广域网3	任何的	任何的	所有时间			
	<input checked="" type="checkbox"/>	关闭	所有端口 [M]	广域网4	任何的	任何的	所有时间			

添加新规则

恢复出厂默认值

\*此为示意图，会因产品线不同，图形会有所差异

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。QoS 安全路由器在做规则确认时是依照优先权 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置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：可以设置网络存取规则项目。
- 垃圾桶图像：可以删除网络存取规则项目。
- 添加新规则：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定义规则内容。

## 11.2.2 增加新的管制规则

### 访问规则设置

管制作动:	允许
服务端口:	所有端口 [TCP&UDP/1~65535] <span style="float: right;">服务端口新增或删除表</span>
日志:	关闭
接口位置:	局域网
来源IP地址:	单独 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
目的IP地址:	单独 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

### 生效时间

管制时间为	所有时间	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/> (时间格式:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日	<input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六

返回

确定

取消

- 管制作动:** 允许：允许符合此管制条例行为的数据包通过。  
关闭：不允许符合此管制条例行为的数据包通过。
- 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服务内容没有存在于默认列表内的话，您可以点击右方的服务端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以及通讯协议与端口，点击“新增”按钮即可新增一个管制服务项目内容。
- 日志:** 允许: 依据此规则发生的相关事件将在日志中记录。  
关闭: 依据此规则发生的相关事件不会在日志中记录。
- 接口位置:** 选择您所要允许或不允许的来源数据包接口(例如是从 LAN，WAN1，WAN2 还是任何的)，可以从下拉式选单中选择。
- 来源 IP 地址:** 选择来源数据包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。  
您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（“7.6 IP 群组管理”说明）。
- 目的 IP 地址:** 选择目的端数据包包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。
- 生效时间设置:** 您可以将此条规则依照您所需要的执行时间来做控管。例如您可以设置此



- 应用此存取规则:** 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。选择“所有时间”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，以及设置是每天还是某几天做管制。
- ...到... :** ...到... : 此管制规则有时间限制，设置方式为 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。
- 确定:** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
- 取消:** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

**范例 1 : 若要将病毒端口 TCP 135-139 封锁要如何设置?**

首先在服务端口新增部份加入 TCP 135-139 端口(请参考如何新增服务端口的章节)，然后进行以下的设置：

管制动作：禁止

服务端口：TCP135-139

来源接口：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

来源 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

目的 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

**访问规则设置**

管制动作:	禁止
服务端口:	TCP [TCP/135~139] <span style="float: right; background-color: #92d050; padding: 2px;">服务端口新增或删除表</span>
日志:	关闭
接口位置:	任何的
来源IP地址:	任何的
目的IP地址:	任何的

范例 2：若要禁止内网 IP 段 192.168.1.200 到 192.168.1.230 禁止访问 80 端口要如何设置？

管制动作：禁止

服务端口：TCP 80

来源界面：局域网(此意思为封锁由内网往外网的 80 端口)

来源 IP 地址：范围 192.168.1.200 到 192.168.1.230

目的 IP 地址：任何的(此意思为封锁由 192.168.1.200 到 192.168.1.230 内网往外网任何 80 端口)

### 访问规则设置

管制动作：	禁止
服务端口：	HTTP [TCP/80~80] <span style="float: right;">服务端口新增或删除表</span>
日志：	关闭
接口位置：	局域网
来源IP地址：	范围 192 . 168 . 1 . 200 到 192 . 168 . 1 . 230
目的IP地址：	任何的

### 11.3 网站内容过滤

网站内容过滤可支持两种模式的网页管制，一为封锁禁止访问的域名，另一个为允许访问的域名，此两种模式只能使用一种。

- 设定允许访问的域名
- 设定禁止访问的域名

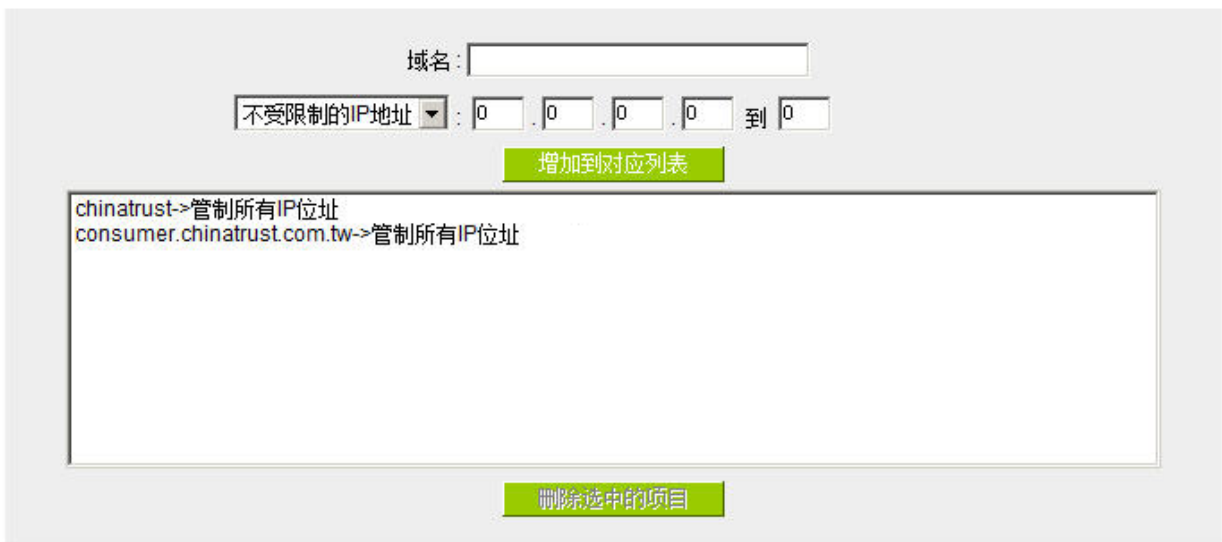
#### 11.3.1 设定 / 封锁禁止访问的域名

此功能需将完整的域名如 `www.sex.com` 填入，即可封锁此网站。

- 设定允许访问的域名
- 设定禁止访问的域名

#### 禁止访问的域名

激活



设定禁止访问/连接的域名:

设定那些是受管制禁止访问的域名。

激活管制/禁止访问的域名功能:

开启网页管制内容项目。

域名:

填写欲管制的网址，如 `www.playboy.com`。

不受限制的 IP 地址：

不受限制 IP 地址/IP 范围：

设定那些 IP/IP 范围可以不受限制访问上方所设定的网页。

其它不在不受限制的 IP 范围内，就会受到限制并且

无法访问上方所设定的网页。

**管制所有 IP 地址：**

表示所有 IP 地址皆会受到管制并且无法访问上方所设定的网页。

加入到对应列表：

点选“增加到对应表”按钮新增此一欲管制的网址。

删除点选的项目：

可以使用鼠标点选一个或多个管制的网址，然后点选即可删除。

**网页内容过滤(关键词)：**

- 设定允许访问的域名
- 设定禁止访问的域名

**禁止访问的域名**

激活

**网页内容过滤(关键字)**

激活



关键字： (仅支持英文关键字)

不受限制的IP地址： .  .  .  到

chinatrust->管制所有IP位址

**激活网页内容过滤(关键词)功能：** 当此项功能激活后，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。

**关键词（仅支持英文关键词）：** 输入关键词。(目前只支持英文关键词，不支持中文或其它语言)

**不受限制的 IP 地址：**

**不受限制 IP 地址/IP 范围：**

设定那些 IP/IP 范围可以不受限制访问含有上方设定关键词的

网页。其它不在不受限制的 IP 范围内，就会受到限制并且无法访问含有上方设定关键词的网页。

**管制所有 IP 地址：**

表示所有 IP 地址皆会受到管制并且无法访问含有上方设定关键词的网页。

**加入到对应列表：**

增加此新增的服务项目内容到服务表列内。

**删除选中的项目：**

选择删除服务项目内容从服务表列内。

**生效时间设定：**

当选择为“所有时间”时，表示此条规则每天并且 24 小时皆会生效，随时进行管制检查；选择为“从”时，可以在单一天中设定三个时段，以及选择那几天（或是每天）在此三个时段规则生效并进行管制检查。

**生效时间**

管制时间为 <input type="text" value="所有时间"/>	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (时间格式:24小时制)
	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (时间格式:24小时制)
	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (时间格式:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input checked="" type="checkbox"/> 周一 <input checked="" type="checkbox"/> 周二 <input checked="" type="checkbox"/> 周三 <input checked="" type="checkbox"/> 周四 <input checked="" type="checkbox"/> 周五 <input type="checkbox"/> 周六

※请注意！所设定的三个时间区段不能重复！

**11.3.2 允许访问的域名**

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。

- 设定允许访问的域名
- 设定禁止访问的域名

▶ 允许访问的域名

激活

域名:

www.baidu.com  
www.google.com  
tw.yahoo.com

▶ 生效时间

管制时间为 <span style="border: 1px solid black; padding: 2px;">所有时间</span>		: <input type="text"/>	到 <input type="text"/>	(时间格式:24小时制)
		: <input type="text"/>	到 <input type="text"/>	(时间格式:24小时制)
		: <input type="text"/>	到 <input type="text"/>	(时间格式:24小时制)
<input type="checkbox"/> 每天 <input type="checkbox"/> 周日 <input checked="" type="checkbox"/> 周一 <input checked="" type="checkbox"/> 周二 <input checked="" type="checkbox"/> 周三 <input checked="" type="checkbox"/> 周四 <input checked="" type="checkbox"/> 周五 <input type="checkbox"/> 周六				

▶ 不受限制的IP地址

IP地址 ▼:  .  .  .  到

**激活允许访问的域名功能：**

选择打勾开启允许网址管制功能，预设为关闭。  
激活此功能后，只有加到允许访问网页清单的网站才能够进行访问，其它未加入清单的网站会被封锁无法访问。

**域名：**

填写欲管制的允许网址，如 www.google.com。

**时间排程设定：** 当选择为“所有时间”时，表示此条规则每天并且 24 小时皆会生效，随时进行管制检查；选择为“从”时，可以在单一天中设定三个时段，以及选择那几天（或是每天）在此三个时段规则生效并进行管制检查。

**※请注意！所设定的三个时间区段不能重复！**

**時間排程設定**

管制時間為 <input type="text" value="所有時間"/>	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (24小時制)
	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (24小時制)
	<input type="text" value=""/> : <input type="text" value=""/> 到 <input type="text" value=""/> : <input type="text" value=""/> (24小時制)
<input type="checkbox"/> 每天	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat

**不受限制的 IP 地址：** **不受限制 IP 地址/IP 范围：**  
 设定那些 IP/IP 范围可以不受限制可以访问所有的网站。  
 其它不在不受限制的 IP 范围内，就会受到限制并且只能访问上方所设定的网页。

## 十二、流行路由

### 12.1 上网行为管理



#### (1) 规则列表：

Outbound L7 filter
Inbound L7 filter

▶ 模式

Block Application ▼

---

▶ L7 Block Application

跳到 1 /页      5 每页显示笔数

优先权	激活	名称	管制时间	例外的来源 IP	编辑	删除
1 ▼	<input checked="" type="checkbox"/>	人人網	所有时间	---	编辑	删除
2 ▼	<input checked="" type="checkbox"/>	P2P	所有时间	---	编辑	删除
3 ▼	<input checked="" type="checkbox"/>	skype	所有时间	---	编辑	删除

[加入新的管制规则](#)

#### (2) 加入新的规则：点选 [加入新的管制规则](#)



增加 规则

规则名称：

分类	项目		分类 ▲	封锁项目 ▲	删除
Im即时通信		>>>>			
P2P软件					
在线游戏					
网页控制物件					
网页档案下载					
炒股软件					
社群网站					
视频网站					
影音播放软件					
博客					

自定义应用程序

时间管制设定

管制时间为 <span style="border: 1px solid black; padding: 2px;">所有时间</span> ▼		: : 到 : : (时间表示:24小时制)	
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日	<input type="checkbox"/> 周一	<input type="checkbox"/> 周二
	<input type="checkbox"/> 周三	<input type="checkbox"/> 周四	<input type="checkbox"/> 周五
	<input type="checkbox"/> 周六		

此设定将套用该应用程序的所有规则

- 不受限制的 QQ 号码
- 例外的来源 IP

以下为规则设定步骤，并以一个企业的例子辅助说明：

**步骤一：为此规则命名**

规则的名称会显示在功能规则列表，网管可以管制对象或用途来命名，来达到注册的效果。

规则名称：

**步骤二：选取套用的应用程序**




※图标为说明之用，实际的应用程序支持列表请参考官网说明。

(1) 选取[分类]后，在[项目] 选单会出现对应的应用程序列表。

提示：

- 在想要的应用程序上单击，即可选取该应用程序，也可复选。
- 在同一个应用程序上点击第二次则是取消。
- 或是直接点击[全选]，则选取所有应用程序，再点击不要的项目即可取消勾选。
- 可以跨分类选取。

(2) 点选  将已选取好的应用程序指到右侧选单中，如此即完成选取。

分类 ▲	封锁项目 ▲	删除
Im即时通信	MSN	
Im即时通信	QQ/TM	
Im即时通信	Skype(Voice)	
Im即时通信	Yahoo!Messenger	

**步骤三：确认是否配置生效时间，让规则只在设定的时间内生效。**

预设对所有时间都生效。若您需要设定生效时间可以在以下更改设定。

**▶ 时间管制设定**

管制时间为 <b>所有时间</b> ▼	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/> (时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六

**步骤四：设定例外对象(IP 或 QQ 号)**

**▶ 此设定将套用该应用程序的所有规则**

- 不受限制的 QQ 号码
- 例外的来源 IP

- 在例外对象设定这里可以设定 IP、或例外 QQ 号(若您有选择封锁 QQ 才需要设定例外 QQ 号)。
- 注意，例外对象的设定会套用该应用程序的所有规则。

例如在上网行为管理原本就已经有 1 条 google talk 的规则，但没有设定例外 IP；此规则也选择了 google talk 并设定了例外 IP 192.168.1.100，则代表 IP 192.168.1.100 在使用 google talk 时都可正常使用（不管是套用在原本的规则、或是后来新增的规则）。

**步骤五：点选  以储存规则**

若您在内网架设服务器，并且已经使用【虚拟服务器】、【DMZ 主机】功能来指向内部服务器所在主机和端口号，则搭配 Inbound L7 Filter 功能，能够进一步规范只有指定的应用程序流量才允许进入，提高服务器的安全层级。

**(1) 规则列表：**



**例外外部客户**



不受 Inbound L7 Filter 管制的外部用户。例如某企业北京总公司的 ERP 服务器，除了北京总公司内部员工之外、只有天津、石家庄两个分公司在使用。则可将天津、石家庄两个分公司的 IP 范围加到例外外部客户，当系统辨识到进入的流量是来自天津、石家庄两个分公司时，则会直接允许通过，不会再进入 Filter 流程中，以加快服务速度。

例外外部客户除了可以指定 IP 范围之外，也可选用【群组管理】中设定的目的地 IP 群组。

**(2) 加入新的规则：** 点选 



### 步骤一：为此规则命名

规则的名称会显示在功能规则列表，网管可以管制对象或用途来命名，来达到注册的效果。

规则名称：

### 步骤二：选取套用的服务器

选取已设定的[虚拟服务器]、[DMZ 主机]规则。

#### ▶ 选择内部服务器



### 步骤三：选取套用的应用程序

#### ▶ 选择应用程序

- 此服务器不需被L7管制
- 选择允许项目



※图标为说明之用，实际的应用程序支持列表请参考官网说明。


(1) 此服务器不需被 L7 管制：

启用此选项后，此规则选定的服务器规则不会套用 Inbound L7 Filter，则外面进来的相关流量会直接允许。

(2) 选取[分类]后，在[项目] 选单会出现对应的应用程序列表。

提示：

- 在想要的应用程序上单击，即可选取该应用程序，也可复选。
- 在同一个应用程序上点击第二次则是取消。
- 或是直接点击[全选]，则选取所有应用程序，再点击不要的项目即可取消勾选。
- 可以跨分类选取。

(3) 点选  将已选取好的应用程序指到右侧选单中，如此即完成选取。

#### 步骤四：是否增加外部用户 IP 做为过滤条件

##### 增加外部用户IP作为过滤条件

进入的流量除了必须为指定的应用程序流量之外，则还需符合指定的外部 IP 范围。

例如某企业台北总公司的 ERP 服务器，除了北京总公司内部员工之外、只有天津、石家庄两个分公司在使用。则可指定进入流量必须为 ERP 流量、且还要来自天津、石家庄分公司 IP 范围才予以通过。若应用程序不符合、或外部 IP 范围不符合，则进入流量会被封锁。

步骤五：点选  以储存规则

## 12.2 L7 VIP 优先通道



(1) 规则列表：

### 规则列表

跳到 1 / 页

5 每页显示笔数

No.	激活	名称	端口	VIP 应用程序	IP范围/群组	管制时间	编辑	删除
1	<input checked="" type="checkbox"/>	董事長室	广域网1,2	所有应用程序	192.168.1.100~110	所有时间	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
2	<input checked="" type="checkbox"/>	VoIP	广域网1,2	Skype(Voice)	任何IP	所有时间	<input type="button" value="编辑"/>	<input type="button" value="删除"/>

(2) 加入新的规则：点选 **加入新的管制规则**

基本设定

规则名称：	<input type="text"/>
界面：	<input type="checkbox"/> 广域网1 <input type="checkbox"/> 广域网2 <input type="checkbox"/> 广域网3 <input type="checkbox"/> 广域网4 <input type="checkbox"/> 广域网5 <input type="checkbox"/> USB1 <input type="checkbox"/> USB2

设定VIP应用程序或对象

- VIP应用程序
- VIP来源IP范围/群组

时间管制设定

管制时间为	所有时间 ▾	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/>	(时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日	<input type="checkbox"/> 周一	<input type="checkbox"/> 周二
	<input type="checkbox"/> 周三	<input type="checkbox"/> 周四	<input type="checkbox"/> 周五
	<input type="checkbox"/> 周六		

步骤一：基本设定

基本设定

规则名称：	<input type="text"/>
界面：	<input type="checkbox"/> 广域网1 <input type="checkbox"/> 广域网2 <input type="checkbox"/> 广域网3 <input type="checkbox"/> 广域网4 <input type="checkbox"/> 广域网5 <input type="checkbox"/> USB1 <input type="checkbox"/> USB2

规则的名称会显示在功能规则列表，网管可以管制对象或用途来命名，来达到注记的效果。

并选取此规则在哪一条广域网上为VIP。例如设定董事长室只有流量走在广域网1、2时为VIP、而流量走在其它广域网上则没有VIP权限。

提示：

如果您希望流量只走在有VIP效果的广域网上，可以搭配 [L7 线路绑定] 功能来达成。



## 步骤二：设定 VIP 应用程序或对象

### 设定VIP应用程序或对象

- VIP应用程序**
- VIP来源IP范围/群组**

单独设定应用程序为 VIP。例如选择[webpage]，则代表当系统辨识到任何 IP 在使用 webpage 时，带宽的使用层级都是 VIP。

单独设定 IP 为 VIP。例如选择[总经理室] IP 群组，则代表总经理室不管使用任何上网行为的带宽使用层级都是 VIP。

同时设定应用程序与 IP。例如设定[Webpage]与[总经理室]，意即总经理室只有在使用 webpage 时，带宽的使用层级为 VIP、但是使用其它的网络行为则没有 VIP 效果。



步骤三：确认是否配置生效时间，让规则只在设定的时间内生效。

预设为所有时间都生效。若您需要设定生效时间可以在以下更改设定。

#### 时间管制设定

管制时间为 <span>所有时间</span> ▾	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/> (时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六

步骤四：点选  以储存规则



(1) 规则列表：

#### 规则列表

跳到 1 ▾ / 页 5 ▾ 每页显示笔数

优先权	激活	名称	端口	IP范围/群组	管制时间	编辑	删除
<span>1</span> ▾	<input checked="" type="checkbox"/>	網頁	广域网2	任何的	所有时间	<input type="button" value="编辑"/>	
<span>2</span> ▾	<input checked="" type="checkbox"/>	P2P	广域网1	任何的	所有时间	<input type="button" value="编辑"/>	

(2) 加入新的规则：点选 

选择应用程序

规则名称:

分类	项目	分类 ▲	项目 ▲	删除
P2P软件				
影音播放软件				
其它分类				

**自定义应用程序**

设置

绑定界面:	广域网1 ▼ <input type="checkbox"/> 当绑定的线路断线时, 将流量转导到其它可用线路
来源IP范围/群组:	任何的 ▼

时间管制设定

管制时间为 所有时间 ▼	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/> (时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六

下列叙述以一个小区的设置当做说明：

该小区申请了二条带宽各不同的 XDSL，需要将易占用带宽的应用程序、和一般网页浏览行为各自绑定到不同的广域网，来避免应用程序互相争抢带宽。

步骤一：为此规则命名

规则的名称会显示在功能规则列表，网管可以管制对象或用途来命名，来达到注记的效果。

规则名称:

步骤二：选取套用的应用程序



※图标为说明之用，实际的应用程序支持列表请参考官网说明。

(1) 选取[分类]后，在[项目] 选单会出现对应的应用程序列表。

提示：

- 在想要的应用程序上单击，即可选取该应用程序，也可复选。
- 在同一个应用程序上点击第二次则是取消。
- 或是直接点击[全选]，则选取全部应用程序，再点击不要的项目即可取消勾选。
- 可以跨分类选取。

(2) 点选 >>>> 将已选取好的应用程序指到右侧选单中，如此即完成选取。

步骤三：设定绑定规则相关参数

🔹 设置

绑定界面:	广域网1 ▾
	<input type="checkbox"/> 当绑定的线路断线时，将流量转导到其它可用线路
来源IP范围/群组:	任何的 ▾

绑定界面	设定此应用程序、或 IP 的流量，要绑定在哪一条广域网线路上。
当绑定的线路断线时，将流量转导到其它可用线路	若有勾选此选项，则当系统侦测绑定的广域网断线时，会将流量转至其它有联机的线路。
来源 IP 范围/群组	此规则是否将套用的范围缩小至某 IP( 或 IP 群组)范围。

步骤四：确认是否配置生效时间，让规则只在设定的时间内生效。

预设为所有时间都生效。若您需要设定生效时间可以在以下更改设定。

🔹 时间管制设定

管制时间为 所有时间 ▾	□ : □ 到 □ : □ (时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六

步骤五：点选  以储存规则

以此范例而言，网管还会再另外设置一条规则来将一般网页浏览绑定到另一个广域网。因设置方式相同故不再说明。

### 12.3 L7 QoS 带宽管理

**流行路由**

▶ **L7 QoS带宽管理**

**(1) 规则列表：**

▶ 填入 ISP 线路实际可供使用带宽

端口	上传带宽 (Kbit/sec)	剩余保证 上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)	剩余保证 下载带宽 (Kbit/sec)
广域网1	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
广域网2	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
广域网3	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
广域网4	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
广域网5	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
USB1	<input type="text" value="256"/>	<input type="text" value="256"/>	<input type="text" value="2048"/>	<input type="text" value="2048"/>
USB2	<input type="text" value="256"/>	<input type="text" value="256"/>	<input type="text" value="2048"/>	<input type="text" value="2048"/>

▶ 规则列表

跳到  /页

每页显示笔数

优先级	激活	名称	端口	IP范围/群组	上传/下载	管制带宽	管制时间	编辑	删除
<input type="text" value="1"/>	<input type="checkbox"/>	P2P	广域网1, 广域网2	192.168.1.100~150	下载频宽	500~1000Kbit	所有时间	<input type="button" value="编辑"/>	<input type="button" value="删除"/>
<input type="text" value="2"/>	<input type="checkbox"/>	網頁	广域网1, 广域网2	192.168.1.100~150	下载频宽	1000~1000Kbit	所有时间	<input type="button" value="编辑"/>	<input type="button" value="删除"/>

**ISP 线路可供使用带宽值：**此表和一般 QoS 功能联动。

**填入 ISP 线路实际可供使用带宽**

端口	上传带宽 (Kbit/sec)	剩余保证 上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)	剩余保证 下载带宽 (Kbit/sec)
广域网1	10000	10000	10000	10000
广域网2	10000	10000	10000	10000
广域网3	10000	10000	10000	10000
广域网4	10000	10000	10000	10000
广域网5	10000	10000	10000	10000
USB1	256	256	2048	2048
USB2	256	256	2048	2048

WAN 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。输入完成请按  以储存设定。

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。计算 QoS 规则设定所使用的带宽，为 最小带宽×设定的 IP 数。例如 192.168.1.101~110 范围，每个 IP 的最小带宽设定 500kbit/sec，则此规则总共使用 500kbit/sec × 10(个 IP) = 5000kbit/sec  
 剩余保证带宽 = 原本填入的带宽 - QoS 规则(L7 QoS 和一般 QoS)设定的带宽。当系统计算规则设定的带宽已经超过原本填写的广域网带宽时，就会以红色负值显示。

**显示QoS列表**

：此表显示已设定的 QoS 规则，L7 QoS 和一般 QoS 都会列在表上。当 L7 QoS 和一般 QoS 规则设定的范围有重复时，以 L7 QoS 的优先权为高。



QoS 类型	应用程序/服务端口	IP 地址	上传/下载	最小带宽 (Kbit/sec)	最大带宽 (Kbit/sec)	带宽共享 方式	激活	接口配置(WAN)
L7 QoS	Web Page	192.168.1.100~192.168.1.150	下载	1000	1000	单一频宽	激活	广域网1,2,
L7 QoS	比特彗星/EMule/PP点点通	192.168.1.100~192.168.1.150	下载	500	1000	单一频宽	激活	广域网1,2,
QoS	All Traffic [ALL/1~65535]	192.168.1.100~192.168.1.110	下载	2000	5000	共享频宽	激活	广域网1,2,

**(2) 加入新的规则：**点选



新增阻挡规则

规则名称：

分类	项目	分类 ▲	封锁项目 ▲	删除
P2P软件				
影音播放软件				
其它分类				

自定义应用程序

网络品质服务配置(QoS)

端口：	<input type="checkbox"/> 广域网1 <input type="checkbox"/> 广域网2 <input type="checkbox"/> 广域网3 <input type="checkbox"/> 广域网4 <input type="checkbox"/> 广域网5 <input type="checkbox"/> USB1 <input type="checkbox"/> USB2
来源IP范围/群组：	范围 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 到 <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
管制带宽：	最小带宽： <input type="text"/> 0 Kbit/sec   最大带宽： <input type="text"/> 0 Kbit/sec
上传/下载：	下载带宽 <input type="text"/>
频宽共享方式：	<input type="radio"/> 此范围IP地址共享此设定带宽。 <input checked="" type="radio"/> 此范围每一 IP 地址最大及最小可使用带宽。

时间管制设定

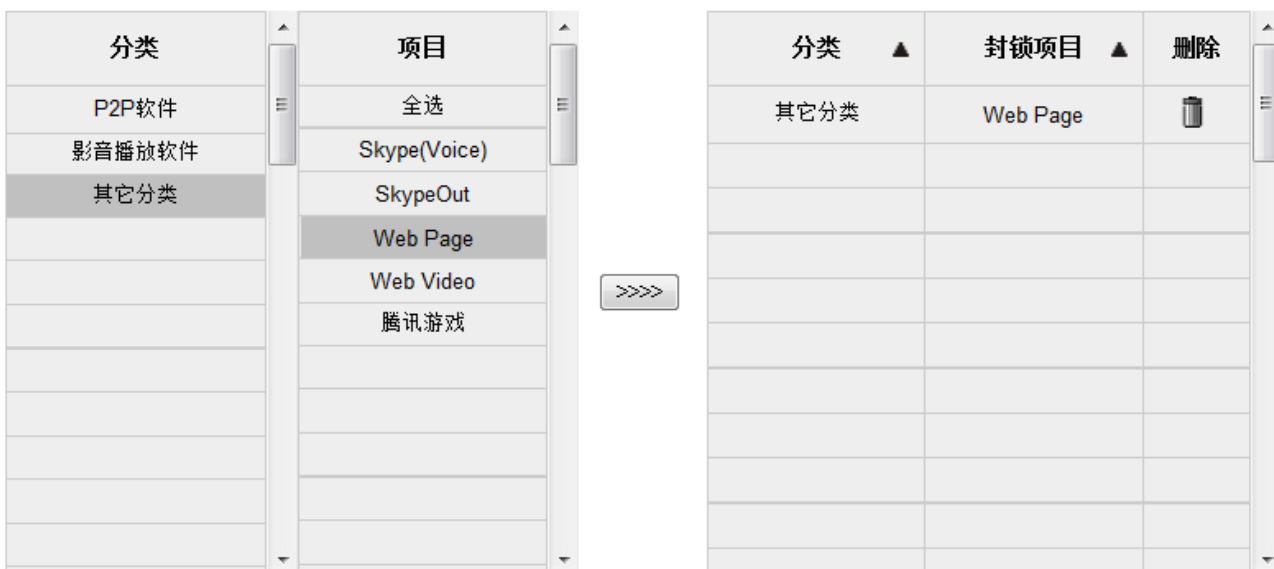
管制时间为 <input type="text"/> 所有时间 <input type="text"/>	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/> (时间表示:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日 <input type="checkbox"/> 周一 <input type="checkbox"/> 周二 <input type="checkbox"/> 周三 <input type="checkbox"/> 周四 <input type="checkbox"/> 周五 <input type="checkbox"/> 周六
<input type="button" value="确定"/> <input type="button" value="取消"/>	

步骤一：为此规则命名

规则的名称会显示在功能规则列表，网管可以管制对象或用途来命名，来达到注册的效果。

规则名称：

**步骤二：选取套用的应用程序**



自定义应用程序

※图标为说明之用，实际的应用程序支持列表请参考官网说明。

(1) 选取[分类]后，在[项目] 选单会出现对应的应用程序列表。


提示：

在想要的应用程序上单击，即可选取该应用程序，也可复选。

在同一个应用程序上点击第二次则是取消。

或是直接点击[全选]，则选取所有应用程序，再点击不要的项目即可取消勾选。

可以跨分类选取。

点选  将已选取好的应用程序指到右侧选单中，如此即完成选取。

步骤三：设定 QoS 相关参数

网络品质服务配置(QoS)

端口：	<input checked="" type="checkbox"/> 广域网1 <input checked="" type="checkbox"/> 广域网2 <input type="checkbox"/> 广域网3 <input type="checkbox"/> 广域网4 <input type="checkbox"/> 广域网5 <input type="checkbox"/> USB1 <input type="checkbox"/> USB2
来源IP范围/群组：	范围   192   .   168   .   1   .   100   到   150
管制带宽：	最小带宽：1000 Kbit/sec   最大带宽：1000 Kbit/sec
上传/下载：	下载带宽
带宽共享方式：	<input type="radio"/> 此范围IP地址共享此设定带宽。 <input checked="" type="radio"/> 此范围每一 IP 地址最大及最小可使用带宽。

界面	勾选此条 QoS 设定要控制在哪条 WAN 执行，可单独或全部勾选。
来源 IP 范围/群组	此为选择您所要限制的使用者为哪些？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 到 149，这样此规则就是针对 192.168.1.100 到 149 做限制。
上传/下载	上传：指对内网 IP 的上传带宽。 下载：指对内网 IP 的下载带宽。
带宽分享方式	<p><b>所有 IP 范围分享总带宽：</b> 若选择此规则的话，其表示所有 IP 或此服务端口共享这段(最小带宽到最大带宽)带宽范围。</p> <p><b>指定每一 IP 之可用带宽：</b> 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(Mini 到 Max.Rtae)带宽范围，例如若是针对每台计算机 (IP 地址)做的规则设定，则每台电脑(IP 地址)都可以有这么大的带宽。</p> <p><b>※注意：</b> 当您选择带宽的共享方式时，要留意实际应用的情况，以避免选择不恰当的方式而造成带宽太小无法正常使用网络。例如，内网多人使用 FTP 做档案下载，若是您希望 FTP 不会占用掉大部分的带宽，您就可以选择共享带宽，不论内网有多少人使用 FTP 做档案下载，总和所占用的带宽是固定的。</p>

步骤四：确认是否配置生效时间，让规则只在设定的时间内生效。

预设为所有时间都生效。若您需要设定生效时间可以在以下更改设定。

▶ **时间管制设定**

管制时间为	所有时间 ▾	<input type="text"/> : <input type="text"/> 到 <input type="text"/> : <input type="text"/>	(时间表示:24小时制)												
<input type="checkbox"/>	每天	<input type="checkbox"/>	周日 <input type="checkbox"/>	<input type="checkbox"/>	周一 <input type="checkbox"/>	<input type="checkbox"/>	周二 <input type="checkbox"/>	<input type="checkbox"/>	周三 <input type="checkbox"/>	<input type="checkbox"/>	周四 <input type="checkbox"/>	<input type="checkbox"/>	周五 <input type="checkbox"/>	<input type="checkbox"/>	周六

步骤五：点选  以储存规则

## 12.4 自定义应用程序

在设置流行路由规则时，除了直接选用 qno 支持的应用程序之外，也可以透过 [自定义应用程序] 功能，利用 URL、目的 IP 或端口号来增加应用程序。

您可以在应用程序状态表上、或是流行路由各功能的 APP List 列表上找到[自定义应用程序] 功能。

### ※应用程序状态

流行路由

- ▶ 应用程序状态
- 上网行为管理
- L7 VIP优先通道
- L7 线路绑定
- L7 QoS带宽管理
- 资料库更新

● 应用程序状态

自定义应用程序

跳到 1 /页      10 每页显示笔数      下一页>>

分类 ▲	应用程序 ▲	上网行为管理		L7 VIP优先通道	L7 线路绑定	L7 QoS带宽管理
		对外	对内			
其它分类	Skype(Voice)	---	---	2	---	---
其它分类	Web Page	---	---	---	2	1

加入新的管制规则

※图标为说明之用，实际的功能、与应用程序支持列表请参考官网说明。

### ※流行路由各功能的 APP List

#### ● 增加 规则

规则名称：

分类 ▲	项目 ▲
Im即时通信	
P2P软件	
在线游戏	
网页控制物件	
网页档案下载	
炒股软件	
社群网站	
视频网站	
影音播放软件	
博客	

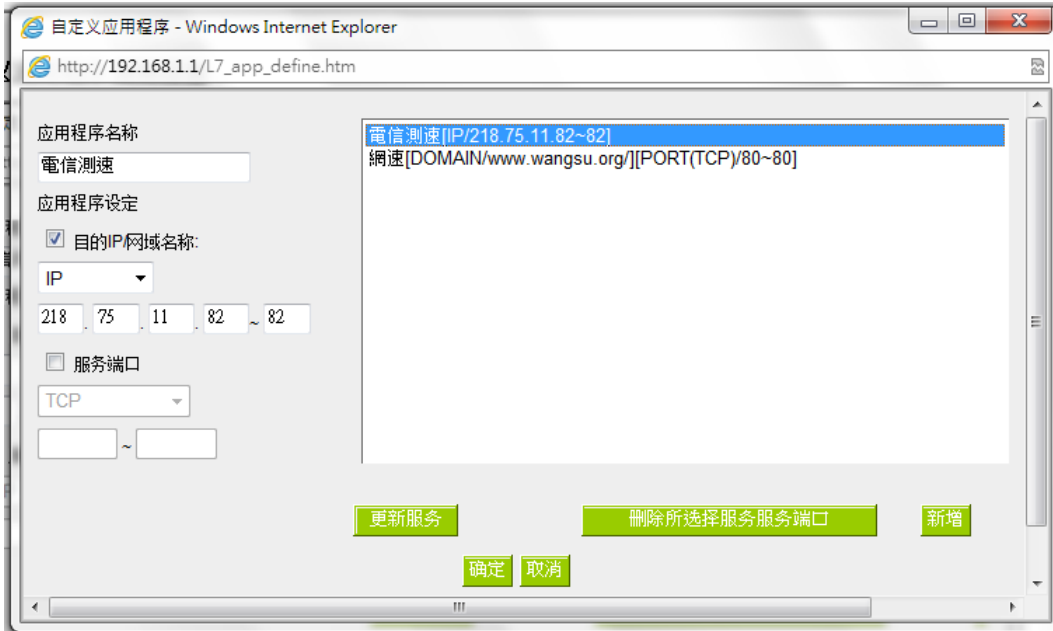
>>>>

分类 ▲	封锁项目 ▲	删除 ▲

自定义应用程序

※图标为说明之用，实际的功能、与应用程序支持列表请参考官网说明。

### 自定义应用程序 规则添加



**步骤一：命名这个应用程序的名称。**

**步骤二：利用 URL、目的 IP 或服务端口，来定义此应用程序。**可定义参数有以下：

目的 IP 地址	若为单一 IP，则直接将此 IP 填入，如 100.100.100.105，则填入 100.100.100.105 到 105。 若是要限制一组 IP 范围，则填入如 100.100.100.105 到 200。
目的 IP 群组	套用在 [群组管理] 功能建立的目的 IP 群组。
域名	以域名来定义自定义应用程序，例如 http://speed.hinet.net 则输入 speed.hinet.net 即可。
服务端口	可选用 TCP、UDP 或是套用在 [群组管理] 功能建立的服务端口群组。

**步骤三：**点击 **增加到對應表列** 加到右侧清单中，即完成此设定。

**步骤四：**规则添加完成后，可以在 APP List 的 [自定义应用程序] 分类中找到自定义的项目。并可套用至各流行路由的功能中。



### 12.5 应用程序状态

**流行路由**

应用程序状态

在应用程序状态表，提供网管可以一次看到哪些应用程序已经建立规则。在哪个功能已建立规则、以及在该功能的规则编号。

应用程序状态

自定义应用程序

1 2 跳到 1 /页 3 10 每页显示笔数 4 下一页>>

分类 ▲	应用程序 ▲	上网行为管理		L7 VIP优先通道	L7 线路绑定	L7 QoS带宽管理
		对外	对内			
其它分类	Skype(Voice)	--	--	2	--	--
其它分类	Web Page	--	--	--	2	1
影音播放软件	酷狗音乐	--	--	5 1	--	--
影音播放软件	PPS网络电视	--	--	1	--	--
影音播放软件	QQ音乐/QQLive	--	--	1	--	--
影音播放软件	千千静听	--	--	1	--	--
社群网站	Google+	3	--	--	--	--
社群网站	Facebook	3	--	--	--	--
社群网站	QQ农场	3	--	--	--	--
社群网站	QQ校友	3	--	--	--	--

加入新的管制规则

※图标为说明之用，实际的应用程序支持列表请参考官网说明。

1	分类/应用程序排序	依据应用程序的分类、或是应用程序名称做排序。
2	跳到 1 /页	直接跳到其它页次。
3	10 每页显示笔数	定义每一页显示的应用程序行数。
4	下一页>>	前往下一页。
5	规则编号	显示该应用程序在这个功能所建立的规则、以及编号 点击后会进入该规则的编辑页面。

## 12.6 数据库更新



数据库更新功能，网管在此页面即可得知服务器端是否有最新版本更新、并可设定数据库更新的时间与检查频率。

### 状态检查

### 尚未检查到新版本

版本号：V1.0.0.0  
档案大小：0KB

[立即下载](#)

上次检测：[立即检查](#)

### 高级设置

版本管理	前次版本： V0.0.0.0 <a href="#">退回前版</a> 当前版本： V1.0.0.0 已下载版本： -- <a href="#">立即更新</a>
状态检查	<input type="radio"/> 每隔 <input type="text" value="24"/> 小时检查一次更新 <input checked="" type="radio"/> 禁用
自动更新	<input checked="" type="radio"/> 禁用自动更新 <input type="radio"/> 自动更新 <input type="radio"/> 自定更新排程 <input type="text" value="23"/> : 00(24小时制) <input checked="" type="checkbox"/> 周一 <input checked="" type="checkbox"/> 周二 <input checked="" type="checkbox"/> 周三 <input checked="" type="checkbox"/> 周四 <input checked="" type="checkbox"/> 周五 <input checked="" type="checkbox"/> 周六 <input checked="" type="checkbox"/> 周日
服务器设置	<input checked="" type="radio"/> 默认服务器(建议选项) <input type="radio"/> 备援服务器 IP/域名： <input type="text"/> 服务端口： <input type="text" value="443"/>

[确定](#) [取消](#)



状态检查：

状态检查

**1 尚未检查到新版本**  
 版本号：V1.0.0.0  
 档案大小：0KB

**2 立即下载**

**3 上次检测：Mon Dec 19 2011 15:23:25 立即检查**

1	状态检查选单	当您的路由器与数据库服务器连接后，若有检查到新版本可供下载时，则会在此显示提示语、最新版本的版本号、与该版本的档案大小。
2	立即下载	点击后会立即下载此版本。若您在下载后没有立即更新的话，则版本会保留在系统中，您可在【版本管理】的已下载版本处，手动更新。
3	上次检查	路由器最近一次检查服务器端版本的时间印。手动点击 <b>立即检查</b> 则会立即再检查一次。检查时间的频率可在【进阶设定】中调整。

版本管理：

**版本管理**

前次版本： V0.0.0.0 **退回前版**

当前版本： V1.0.0.0

已下载版本： -- **立即更新**

前次版本	系统前一个使用的数据库版本。
当前版本	系统当前使用的数据库版本。
已下载版本	您在状态检查使用【立即下载】所下载的版本。可在此处点击 <b>立即更新</b> 立即手动更新。

状态检查：

<b>状态检查</b>	<input type="radio"/> 每隔 <input type="text" value="24"/> 小时检查一次更新 <input checked="" type="radio"/> 禁用
-------------	--

每隔__小时检查一次更新	调整检查服务器端版本的间隔频率。
不检查	系统不主动检查更新，网管仍然可透过 <b>立即检查</b> 来手动确认是否有更新版本、或者在此调整检查频率。

(高级设定)自动更新：

<b>自动更新</b>	<input checked="" type="radio"/> 禁用自动更新 <input type="radio"/> 自动更新 <input type="radio"/> 自定更新排程 <input type="text" value="23"/> : 00(24小时制) <input checked="" type="checkbox"/> 周一 <input checked="" type="checkbox"/> 周二 <input checked="" type="checkbox"/> 周三 <input checked="" type="checkbox"/> 周四 <input checked="" type="checkbox"/> 周五 <input checked="" type="checkbox"/> 周六 <input checked="" type="checkbox"/> 周日
-------------	---

关闭自动更新	系统不主动更新数据库。但网管仍然可点击 <b>立即下载</b> ，手动来更新数据库。
自动更新	当系统检查到有新版本时，主动下载并更新版本。
自定更新排程__ : 00 (24 小时制)	当系统检查到有新版本时，会在网管指定的时间自动下载与更新版本。

服务器设定：请勿自行更动设定

<b>服务器设置</b>	<p><input checked="" type="radio"/> 默认服务器(建议选项)</p> <p><input type="radio"/> 备援服务器</p> <p>IP/域名：<input type="text"/></p> <p>服务端口：<input type="text" value="443"/></p>
--------------	---

预设服务器	系统默认连接的服务器设定。
被援服务器	填入备援服务器的 IP 或域名，与使用的服务端口号。

### 十三、VPN 虚拟专用网设置

#### 13.1 VPN 虚拟专用网 (VPN)

**VPN 虚拟私有网路**

- ▶ 目前 VPN 状态
- 网关对网关设定
- 客户端对网关设定
- PPTP 设定
- 封包穿透路由功能

PPTP隧道数:  条已经设定使用       条可用隧道  
 QnoKey隧道数:  条已经设定使用       条可用隧道  
 IPSec VPN隧道数:  条已经设定使用       条可用隧道

[高级设定](#)  
[详细信息](#)

#### VPN 隧道状态

条隧道已经激活并连线       条隧道已经设定

跳到  / 1页      每页显示  笔

No.	帐户	状态	Phase2 Encrypt/Auth/DH	本地群组	远程群组	远程网关	连接控制	配置
1	to suzhou	联机	DES/MD5/1	10.10.10.0 255.255.255.0	192.168.8.0 255.255.255.0	1@1 58.210.239.22	<input type="button" value="中断"/>	<a href="#">编辑</a> 
2	shenzhen	联机	DES/MD5/1	10.10.10.50	172.16.16.16	shenzhenqno 58.60.77.47	<input type="button" value="中断"/>	<a href="#">编辑</a> 
3	ryan	等待联机	DES/MD5/1	0.0.0.0 0.0.0.0	61.222.81.0 255.255.255.0	58.61.113.31	<input type="button" value="联机"/>	<a href="#">编辑</a> 

[新增一条隧道](#)

#### VPN 群组隧道状态

群组名称	已联机隧道	Phase2 Encrypt/Auth/DH	本地群组	远程客户端	客户端状态	连接控制	配置
------	-------	------------------------	------	-------	-------	------	----

\*此为示意图，会因产品线不同，图形会有所差异

### 11.1.1. 新增一条 VPN 隧道

QoS 安全路由器支持网关对网关隧道、或客户端对网关隧道。

VPN 隧道连接为 2 台路由器，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 网关的设置或客户端对 VPN 网关的设置页面上。

#### 网关对网关设置 (Gateway to Gateway) :

当您按下新增“新增”的话，将会直接导引到 VPN 网关对 VPN 网关的设置页面上。



#### 客户端对网关(Client to Gateway):

当您按下“新增”的话，将会直接导引到客户端对 VPN 网关的设置页面上。



### 13.1.2.1. 网关对网关的设置

隧道编号:	<input type="text" value="1"/>
隧道名称:	<input type="text" value="sdfsdf"/>
接口位置:	<input type="text" value="广域网2"/>
激活:	<input checked="" type="checkbox"/>

透过以下的设置说明，使用者就可以在两台 QoS 安全路由器之间建立一条 VPN 隧道。

**隧道编号:** 当您设置路由器内建之 VPN 功能时，请选择您要设置的 Tunnel 隧道编号

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

请注意: 此隧道名称若是您需要连接其它 VPN 设备(非侠诺的路由器)时，有一些设备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！

**VPN 接口地址:** 您可以选择哪一个接口位置做为此 VPN 隧道的节点

**激活:** 勾选激活选项，将此 VPN 隧道开启。此项目为默认为激活，当设置完成后，可以再选择是否激活隧道设置

本机用户群组设置(Local Group Setup) :

#### 本地用户群组配置

本地网关身份类型:	<input type="text" value="仅用IP"/>
IP地址:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
本地安全组类型:	<input type="text" value="子网"/>
IP地址:	<input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="0"/>
子网掩码:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

**本地网关身分类型：**

本机网关认证类型，有五种操作模式项目选择，分别为：

仅用 IP

IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail (USER FQDN) 认证

此项目的本机网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

**(1) 仅用 IP:**

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，然后 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置。

<b>本地网关身份类型:</b>	仅用IP
<b>IP地址:</b>	220 . 130 . 188 . 40

**(2) IP + Domain Name(FQDN) 认证:**

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 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置。

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 安全网关设置类型相同才可以正确连接。

<b>本地网关身份类型:</b>	IP + Domain Name (FQDN) 认证
<b>IP地址:</b>	220 . 130 . 188 . 40
<b>域名:</b>	

**(3) IP + E-mail (USER FQDN) 认证:**

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隧道，然后 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置。

本地网关身份类型:	IP + E-mail (User FQDN) 认证
IP地址:	220 . 130 . 188 . 40
电子邮件:	<input type="text"/> @ <input type="text"/>

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入网域名称即可。

本地网关身份类型:	动态IP + Domain Name (FQDN) 认证
域名:	<input type="text"/>

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器 将会开始验证并响应此 VPN 隧道联机; 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。

本地网关身份类型:	动态IP + E-mail (User FQDN) 认证
电子邮件:	<input type="text"/> @ <input type="text"/>

本地安全组类型：

此为设置本地区域端的 VPN 联机存取类型，以下有几个关于本地区域端设置的项目，请您选择并设置适当参数:

(1) IP 地址

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

本地安全组类型:	IP地址
IP地址:	192 . 168 . 1 . 0

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0 的此 IP 地址的计算机可以联机。



(2) 子网域

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。

本地安全组类型:	子网
IP地址:	192 . 168 . 1 . 0
子网掩码:	255 . 255 . 255 . 0

以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.1.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机。

(3) IP 地址范围

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

本地安全组类型:	IP地址范围
IP地址范围:	192 . 168 . 1 . 0 到 254

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.1.0~254 的此网段的 IP 地址范围的计算机可以联机。

远程用户群组设置 (Remote Group Setup) :

④ 远程用户群组配置

远程网关身份类型:	仅用IP
IP地址	121 . 30 . 131 . 143
远程安全组类型:	子网
IP地址:	192 . 168 . 2 . 0
子网掩码:	255 . 255 . 255 . 0

此项目的远程的网关身分类型( Remote Security Gateway Type)必须与连接远程的近端本地网关身分类型( Local Security Gateway Type)相同。

**远程的网关身分类型:** 远程的网关认证类型，有五种操作模式项目选择，分别为：  
仅用 IP

IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail (USER FQDN) 认证

(1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，

<b>远程网关身份类型:</b>	仅用IP
IP地址	121 . 30 . 131 . 143

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，并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	仅用IP
IP by DNS Resolved	

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址，并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	仅用IP
IP by Multiple DNS Resolved	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

(2) IP + Domain Name(FQDN) 认证:

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 安全网关设置类型相同才可以正确连接。

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
IP地址	121 . 30 . 131 . 143
<b>域名:</b>	<input type="text"/>

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。并且在设置完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
IP by DNS Resolved	<input type="text"/>
<b>域名:</b>	<input type="text"/>

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
IP by Multiple DNS Resolved	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>
<b>域名:</b>	<input type="text"/>

### (3) IP + E-mail(USER FQDN) 认证:

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隧道，

<b>远程网关身份类型:</b>	IP + E-mail (User FQDN) 认证
IP地址	<input type="text" value="121"/> . <input type="text" value="30"/> . <input type="text" value="131"/> . <input type="text" value="143"/>
<b>电子邮件:</b>	<input type="text"/> @ <input type="text"/>

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。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	IP + E-mail (User FQDN) 认证
IP by DNS Resolved	<input type="text"/>
<b>电子邮件:</b>	<input type="text"/> @ <input type="text"/>

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

远程网关身份类型:	IP + E-mail (User FQDN) 认证
IP by Multiple DNS Resolved	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>
电子邮件:	<input type="text"/> @ <input type="text"/>

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 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。

远程网关身份类型:	动态IP + Domain Name (FQDN) 认证
域名:	<input type="text"/>

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器将会开始验证并响应此 VPN 隧道联机；请输入电子邮件认证到 E-Mail 位置空格字段中。

远程网关身份类型:	动态IP + E-mail (User FQDN) 认证
电子邮件:	<input type="text"/> @ <input type="text"/>

**远程安全组类型:**

此为设置远程端的 VPN 联机存取类型，以下有几个关于远程端设置的项目，请您选择并设置适当参数:

**(1) IP 地址**

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

<b>远程安全组类型:</b>	IP地址
<b>IP地址:</b>	192 . 168 . 2 . 1

以上的设置参考为:当此 VPN 隧道联机后，于 192.168.2.1 的此 IP 地址范围的计算机可以联机。

**(2)子网域**

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。

<b>远程安全组类型:</b>	子网
<b>IP地址:</b>	192 . 168 . 2 . 0
<b>子网掩码:</b>	255 . 255 . 255 . 0

以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.2.0，子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机

**(3)IP 地址范围**

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

<b>远程安全组类型:</b>	IP地址范围
<b>IP地址范围:</b>	192 . 168 . 2 . 1 到 254

以上的设置参考为:当此 VPN 隧道联机后，只有 192.168.2.1 到 192.168.2.254 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 隧道的加密机制必须要相同才可以将此隧道连接，并于传输资料中加上标准的 IPSec 密钥，我们称为加密密钥 “key”。 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 配置

密钥管理协定:	使用IKE协定 ▾
阶段1 DH协议群组:	群组1 ▾
阶段1 加密演算法:	DES ▾
阶段1 认证演算法:	MD5 ▾
阶段1 SA有效时间:	28800 秒
完全顺向密钥(PFS)	<input checked="" type="checkbox"/>
阶段2 DH协议群组:	群组1 ▾
阶段2 加密演算法:	DES ▾
阶段2 认证演算法:	MD5 ▾
阶段2 SA有效时间:	3600 秒
共用密钥:	test

高级设定 +

密钥管理协议:

此选项设置为当您设置此 VPN 隧道使用何种加密模式以及验证模式后，必须设置一组交换密码，并注意此参数必须与远程的交换密码参数相同;设置的方式有自动 Auto (IKE)或是手动 Manual 设置二种，于设置时请您选择其中一种设置方式即可！

▶ IPsec 配置

密钥管理协定:	使用IKE协定 ▾
阶段1 DH协议群组:	群组1 ▾
阶段1 加密演算法:	DES ▾
阶段1 认证演算法:	MD5 ▾
阶段1 SA有效时间:	28800 秒
完全顺向密钥(PFS)	<input checked="" type="checkbox"/>
阶段2 DH协议群组:	群组1 ▾
阶段2 加密演算法:	DES ▾
阶段2 认证演算法:	MD5 ▾
阶段2 SA有效时间:	3600 秒
共用密钥:	test

高级设定 +

### 使用 IKE 协定:

透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将完全顺向密钥 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。

- 完全顺向密钥(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。
- 阶段 1/阶段 2 DH 协议群组:于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- 阶段 1/阶段 2 加密算法:此加密选项设置为设置此 VPN 隧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。
- 阶段 1/阶段 2 认证算法:此验证选项设置为设置此 VPN 隧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”。
- 阶段 1 SA 有效时间: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。
- 阶段 2 SA 有效时间: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。
- 共享密钥: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,在此的范例设置为 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。

高级设置-只供给使用 IKE 协议使用

### 高级设定

- 野蛮模式
- 使用 IP Header 压缩协定
- 保持连接
- AH 哈希算法 MD5
- 允许 NetBIOS 广播封包通过
- 允许掉线侦测封包穿越 NAT
- 掉线侦测功能(DPD) 每隔 10 秒进行侦测
- 心跳, 远程服务器 0.0.0.0  
每隔 30 秒进行侦测, 重新发起测试次数 5 次

在 QoS 安全路由器的进阶设置项目中, 分别有 Main 以及 Aggressive (野蛮模式) 模式, Main mode 是 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。

- 野蛮模式 (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。
- 使用 IP Header 压缩协议: 若选择此项目勾选, 则连接的 VPN 隧道中 QoS 安全路由器 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- 持续保持联机: 若选择此项目勾选, 则连接的 VPN 隧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 哈希算法: AH (Authentication Header) 验证表头数据包格式, 可选择 MD5/DSHA-1。
- 允许 NetBIOS 广播数据包通过: 若选择此项目勾选, 则连接的 VPN 隧道中会让 NetBIOS 广播数据包通过, 有助于微软的网络邻居等连接容易, 但是相对的占用此 VPN 隧道的流量就会加大!
- 允许穿越 NAT: 允许 VPN 可以穿透位于 QoS 安全路由器前方的 NAT 机制
- 掉线侦测功能(DPD): 若选择此项目勾选, 则连接的 VPN 隧道中会定期的传送 HELLO/ACK 讯息数据包来侦测是否 VPN 隧道的两端仍有联机存在。当有一端断线则 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 讯息数据包传递的时间, 默认值为 10 秒。
- 心跳: VPN Tunnel 心跳监测功能。

若勾选此项设定, 系统会定期传送 ICMP 给在 VPN 通道远程的服务器主机, 远程服务器收到封包之后也会以封包响应。若侦测次数已超过您所设定的值, 而 VPN 远程服务器都没有响应的话, 系统会判定此 VPN 通道为断线。若您为主动建立 VPN 通道的一方, 系统将自动再一次地重建 VPN 通道; 而若您为被



动的一方，系统会等待对方再度建立 VPN 通道。

- 远程服务器：** 远程的网络节点侦测位置，此服务器地址最好是可以且稳定快速的得到响应(建议可以填入 VPN remote Sever LAN IP，请误填无法响应 ICMP 的服务器地址)。
- 时间间隔：** 对外联机侦测逾时时间(秒)，默认值为 30 秒。于 VPN 建立后，每隔 30 秒丢 ICMP 侦测与服务器联机状态。
- 重新侦测次数：** 联机侦测重试次数，默认值为五次。如果联机侦测重试次数超过设定次数，远程服务器没有响应的话，则判断 VPN 线路中断！

※心跳和 DPD 功能，皆能够保障 VPN 通道更稳定的联机质量。不同的是，心跳功能不需考虑远程的 VPN 设备是否具备标准 IPSec 协议，皆能完成 VPN 通道监测，以确定 VPN 通道联机存在、并且流量畅通。

### 13.1.2.2. 客户端对网关的设置

透过以下的设置说明，管理人员就可以在客户端与 QoS 安全路由器之间建立一条 VPN 隧道。

用户可以选择这一条 VPN 隧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置远程的客户，只需设置的一条隧道供一组客户所使用，以节省设置时的麻烦。

在隧道模式 (Tunnel) 的情况:

隧道编号:	<input type="text" value="2"/>
隧道名称:	<input type="text"/>
接口位置:	<input type="text" value="广域网1"/>
激活:	<input checked="" type="checkbox"/>

**隧道编号:** 当您设置 QoS 安全路由器内建之 VPN 功能时，请选择您要设置的 Tunnel 隧道编号。

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

请注意: 此隧道名称若是您需要连接其它 VPN 设备时，有一些设备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！。

**VPN 接口地址:** 您可以选择哪一个接口位置做为此 VPN 隧道的节点

**激活:** 勾选激活 选项，将此 VPN 隧道开启。 此项目为默认为激活，当设置完成后可以再选择是否激活隧道设置。

### 本机用户群组设置(Local Group Setup)

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

本地网关身分类型： 本机网关认证类型，有五种操作模式项目选择，分别为：

仅用 IP

IP + Domain Name(FQDN) 认证

IP + E-mail (USER FQDN) 认证

动态 IP + Domain Name(FQDN) 认证

动态 IP + E-mail(USER FQDN) 认证

此项目的本地网关身分类型( Local Security Gateway Type )必须与连接远程的网关身分类型( Remote Security Gateway Type)相同。

#### (1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，然后 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置。

本地网关身份类型:	仅用IP
IP地址:	0 . 0 . 0 . 0

#### (2) IP + Domain Name(FQDN) 认证:

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 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置。 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 安全网关设置类型相同才可以正确连接。

本地网关身份类型:	IP + Domain Name (FQDN) 认证
IP地址:	0 . 0 . 0 . 0
域名:	

(3) IP + E-mail(USER FQDN) 认证:

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隧道，然后 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置。

本地网关身份类型:	IP + E-mail (User FQDN) 认证
IP地址:	0 . 0 . 0 . 0
电子邮件:	<input type="text"/> @ <input type="text"/>

(4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器 将会开始验证并响应此 VPN 隧道联机; 若您选择此类型连接 VPN，请输入网域名称即可。

本地网关身份类型:	动态IP + Domain Name (FQDN) 认证
域名:	<input type="text"/>

(5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器 将会开始验证并响应此 VPN 隧道联机; 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。

本地网关身份类型:	动态IP + E-mail (User FQDN) 认证
电子邮件:	<input type="text"/> @ <input type="text"/>

本地安全组类型：

此为设置本地区域端的 VPN 联机存取类型，以下有几个关于本地区域端设置的项目，请您选择并设置适当参数:

(1)IP 地址

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

本地安全组类型:	IP地址
IP地址:	192 . 168 . 1 . 0

以上的设置参考为:当此 VPN 隧道联机后,于 192.168.1.0 的此 IP 地址的计算机可以联机。

### (2)子网域

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。

本地安全组类型:	子网
IP地址:	192 . 168 . 1 . 0
子网掩码:	255 . 255 . 255 . 0

以上的设置参考为:当此 VPN 隧道联机后,只有 192.168.1.0,子网掩码为 255.255.255.0 的此网段计算机可以与远程 VPN 联机。

### (3)IP 地址范围

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

本地安全组类型:	IP地址范围
IP地址范围:	192 . 168 . 1 . 0 到 254

以上的设置参考为:当此 VPN 隧道联机后,于 192.168.1.0~254 的此网段的 IP 地址范围的计算机可以联机。

远程用户群组设置 (Remote Group Setup) :

**远程用户群组配置**

<b>远程网关身份类型:</b>	仅用IP
<b>IP地址</b>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

此项目的远程的网关身分类型( Remote Security Gateway Type)必须与连接远程的近端本地网关身分类型( Local Security Gateway Type)相同。

远程的网关认证类型: 远程的网关认证类型，有五种操作模式项目选择，分别为:

- 仅用 IP
- IP + Domain Name(FQDN) 认证
- IP + E-mail (USER FQDN) 认证
- 动态 IP + Domain Name(FQDN) 认证
- 动态 IP + E-mail (USER FQDN) 认证

(1) 仅用 IP:

若您选择仅用 IP 类型的话，只有固定填入此 IP 地址可以存取此隧道，

<b>远程网关身份类型:</b>	仅用IP
<b>IP地址</b>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

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，并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	仅用IP
<b>IP by DNS Resolved</b>	<input type="text"/>

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址，并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	仅用IP
<b>IP by Multiple DNS Resolved</b>	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

(2) IP + Domain Name(FQDN) 认证:

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 安全网关设置类型相同才可以正确连接。

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
<b>IP地址</b>	<input type="text" value="121"/> <input type="text" value="30"/> <input type="text" value="131"/> <input type="text" value="143"/>
<b>域名:</b>	<input type="text"/>

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。并且在设置完成后在 Summary 的远程网关下面自动显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
<b>IP by DNS Resolved</b>	<input type="text"/>
<b>域名:</b>	<input type="text"/>

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

<b>远程网关身份类型:</b>	IP + Domain Name (FQDN) 认证
<b>IP by Multiple DNS Resolved</b>	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>
<b>域名:</b>	<input type="text"/>

(3) IP + E-mail (USER FQDN) 认证:

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隧道，

远程网关身份类型:	IP + E-mail (User FQDN) 认证
IP地址	<input type="text"/>
电子邮件:	<input type="text"/> @ <input type="text"/>

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。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

远程网关身份类型:	IP + E-mail (User FQDN) 认证
IP by DNS Resolved	<input type="text"/>
电子邮件:	<input type="text"/> @ <input type="text"/>

或者也可以通过 Multiple DNS Resolved 来将 DNS 转成 IP 地址。并且在设置完成后在 Summary 的远程网关下面显示出相对应的 IP 地址。

远程网关身份类型:	IP + E-mail (User FQDN) 认证
IP by Multiple DNS Resolved	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>
电子邮件:	<input type="text"/> @ <input type="text"/>

#### (4) 动态 IP + Domain Name(FQDN) 认证:

若是您使用动态 IP 地址连接 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。

远程网关身份类型:	动态IP + Domain Name (FQDN) 认证
域名:	<input type="text"/>

#### (5) 动态 IP + E-mail (USER FQDN) 认证:

若是您使用动态 IP 地址连接 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 QoS 安全路由器作为 VPN 联机时，QoS 安全路由器将会开始验证并响应此 VPN 隧道联机；请输入电子邮件认证到 E-Mail 位置空格字段中。



远程网关身份类型:	动态IP + E-mail (User FQDN) 认证
电子邮件:	<input type="text"/> @ <input type="text"/>

## IPSec Setup

### IPSec 配置

密钥管理协定:	使用IKE协定
阶段1 DH协议群组:	群组1
阶段1 加密演算法:	DES
阶段1 认证演算法:	MD5
阶段1 SA有效时间:	28800 秒
完全顺向密钥(PFS)	<input checked="" type="checkbox"/>
阶段2 DH协议群组:	群组1
阶段2 加密演算法:	DES
阶段2 认证演算法:	MD5
阶段2 SA有效时间:	3600 秒
共用密钥:	<input type="text"/>

高级设定 +

若是任何加密机制存在的话，此两个 VPN 隧道的加密机制必须要相同才可以将此隧道连接，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”。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。

密钥管理协议:

此选项设置为当您设置此 VPN 隧道使用何种加密模式以及验证模式后，必须设置一组交换密码，并注意此参数必须与远程的交换密码参数相同;设置的方式有自动 Auto (IKE)或是手动 Manual 设置二种，于设置时请您选择其中一种设置方式即可！

IPSec 配置

密钥管理协定:	使用IKE协定
阶段1 DH协议群组:	群组1
阶段1 加密演算法:	DES
阶段1 认证演算法:	MD5
阶段1 SA有效时间:	28800 秒
完全顺向密钥(PFS)	<input checked="" type="checkbox"/>
阶段2 DH协议群组:	群组1
阶段2 加密演算法:	DES
阶段2 认证演算法:	MD5
阶段2 SA有效时间:	3600 秒
共用密钥:	

高级设定 +

使用 IKE 协定:

透过 IKE 产生共享的金钥来加密与验证远程的使用者。若将完全顺向密钥 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。

- 完全顺向密钥(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。
- 阶段 1/阶段 2 DH 协议群组: 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。
- 阶段 1/阶段 2 加密算法: 此加密选项设置为设置此 VPN 隧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。
- 阶段 1/阶段 2 认证算法: 此验证选项设置为设置此 VPN 隧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”。
- 阶段 1 SA 有效时间: 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。
- 阶段 2 SA 有效时间: 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。

- 共享密钥：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，在此的范例设置为 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)

### ▶ 高级设定

- 野蛮模式
- 使用IP Header压缩协定
- 保持连接
- AH哈希算法 MD5
- 允许NetBIOS广播封包通过
- 允许掉线侦测封包穿越NAT
- 掉线侦测功能(DPD) 每隔 10 秒进行侦测
- 心跳, 远程服务器 0.0.0.0  
每隔 30 秒进行侦测,重新发起测试次数 5 次

在 QoS 安全路由器的进阶设置项目中，分别有 Main 以及 Aggressive 模式，Main mode 是 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。

- 野蛮模式 (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。
- 使用 IP Header 压缩协定：若选择此项目勾选，则连接的 VPN 隧道中 QoS 安全路由器 支持 IP 表头形态的压缩(IP Payload compression Protocol)。
- 持续保持联机：若选择此项目勾选，则连接的 VPN 隧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 哈希算法：AH (Authentication Header) 验证表头数据包格式，可选择 MD5/DSHA-1。
- 允许 NetBIOS 广播数据包通过：若选择此项目勾选，则连接的 VPN 隧道中会让 NetBIOS 广播数据包通过，有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 隧道的流量就会加大！
- 允许穿越 NAT：允许 VPN 可以穿透位于 QoS 安全路由器前方的 NAT 机制
- 掉线侦测功能(DPD)：若选择此项目勾选，则连接的 VPN 隧道中会定期的传送 HELLO/ACK 讯息数据

包来侦测是否 VPN 隧道的两端仍有联机存在。当有一端断线则 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 讯息数据包传递的时间，默认值为 10 秒。

- 心跳：VPN Tunnel 心跳监测功能。

若勾选此项设定，系统会定期传送 ICMP 给在 VPN 通道远程的服务器主机，远程服务器收到封包之后也会以封包响应。若侦测次数已超过您所设定的值，而 VPN 远程服务器都没有响应的话，系统会判定此 VPN 通道为断线。若您为主动建立 VPN 通道的一方，系统将自动再一次地重建 VPN 通道；而若您为被动的一方，系统会等待对方再度建立 VPN 通道。

**远程服务器：** 远程的网络节点侦测位置，此服务器地址最好是可以且稳定快速的得到响应(建议可以填入 VPN remote Sever LAN IP，请误填无法响应 ICMP 的服务器地址)。

**时间间隔：** 对外联机侦测逾时时间(秒)，默认值为 30 秒。于 VPN 建立后，每隔 30 秒丢 ICMP 侦测与服务器联机状态。

**重新侦测次数：** 联机侦测重试次数，默认值为五次。如果联机侦测重试次数超过设定次数，远程服务器没有响应的话，则判断 VPN 线路中断！

※心跳和 DPD 功能，皆能够保障 VPN 通道更稳定的联机质量。不同的是，心跳功能不需考虑远程的 VPN 设备是否具备标准 IPSec 协议，皆能完成 VPN 通道监测，以确定 VPN 通道联机存在、并且流量畅通。

### 13.1.2 PPTP 设置

提供支持 Window XP/2000/Vista 的 PPTP 对 Qno 防火墙/路由器做点对点隧道协议，让远程单机用户使用此种协议建立 VPN 联机。

激活 PPTP 服务器

PPTP隧道数:  条已经设定使用  条可用隧道 高级设定

---

**PPTP 用户使用IP范围**

起始IP地址: 10.10.	<input type="text" value="10"/>	.	<input type="text" value="200"/>
结束IP地址: 10.10.	<input type="text" value="10"/>	.	<input type="text" value="230"/>

---

**远程用户配置**

用户名:

密码:

再次输入密码:

IP地址:  随机分配  指定IP地址: 10.10..

增加到对应列表

```
1=>10.10.10.204
ryan=>10.10.10.200
test=>10.10.10.201
tony=>10.10.10.202
2=>10.10.10.203
suro=>10.10.10.221
```

删除选中的项目

确定
取消

**激活 PPTP 服务器:**

当勾选后即可以后用点对点隧道协议 PPTP 服务器。

**PPTP 用户使用 IP 范围:**

请输入本地 PPTP IP 地址的范围，其目的是要给远程的使用者一个可进入本地网络的入口 IP。

起始 IP 地址:请在最后两栏输入数值。

结束 IP 地址:请在最后两栏数入数值。

**远程用户配置：**

- 用户名：** 请输入远程使用者的名称。
- 密码的输入与确认：** 输入远程使用者账号密码，及请再次确认远程使用者的账号密码。
- IP 地址：** (1)随机分配：在 PPTP 用户使用 IP 范围之内，随机分配某个 IP 给成功联机的远程用户。  
(2)指定 ip 地址：指定每一个远程用户成功联机时，在 PPTP 用户使用 IP 范围之内被分配到固定的某一个 IP 地址。
- ※请注意！**  
目前 PPTP 用户 IP 在设定时，不是全部随机分配，就是全部都要指定固定的 IP，「无法」设定成某些用户是随机分配，某些用户是指定固定 IP。
- 加入到对应列表：** 将上述设定新增至下方列表之中。

所有的 PPTP 通道状态：显示所有连接成功的用户，包括使用者名称、远程 IP 地址和 PPTP 发放的地址

**▶ PPTP 用户连接列表**

用户名	远程用户的IP地址	本地对映的IP地址
test001	60.248.180.226	192.168.1.151

刷新

### 13.1.3 数据包穿透 QoS 安全路由器功能 (VPN Pass Through)



<b>IPSec 数据包穿透:</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
	<input checked="" type="radio"/> 固定来源端口 <input type="radio"/> 变更来源端口
<b>PPTP 数据包穿透:</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭
<b>L2TP 数据包穿透:</b>	<input checked="" type="radio"/> 激活 <input type="radio"/> 关闭

**IPSec 数据包穿透 QoS 安全路由器功能:**

固定来源端口(未来支持)

或

变更来源端口:(未来支持)

若是选择激活 的话,则允许 PC 端使用 VPN-IPSec 数据包穿透 QoS 安全路由器以便与外部 VPN 设备联机

在 VPN 联机是以 Cisco VPN Server 与 Cisco VPN Client 的状况下才有需要用的此选项,因为 VPN Server 不接受先后两笔用同一个 IP 地址以及同一个 Source Port 的第二笔联机,所以第二笔联机需要变更 Source Port,此时就需要选择 Change Source Port 将原来以 UDP 500 的 Source Port 改成另外随机的 Source Port 联机,选择 Fixed 代表不变更 Source Port 仍以 UDP 500 联机

**PPTP 数据包穿透 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 数据包穿透 QoS 安全路由器以便与外部 VPN 设备联机。

**L2TP 数据包穿透 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 数据包穿透 QoS 安全路由器以便与外部 VPN 设备联机。

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

### 13.2 QVM VPN 功能设置

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 QoS 安全路由器中控画面，远程进入外点客户端做设置。
3. VPN 断线备份机制：让运营商断线困扰造成外点或分公司资料无法对总公司传送问题顺利解决。

#### QVM 用户端设置

选择 QVM 功能为用户端模式：

选择进行 VPN 连接的 QoS 安全路由器为 QVM 用户端。

#### QVM 配置模式

QVM 用户端

#### QVM 用户端设置

帐户：  
 密码：  
 再次输入密码：  
 QVM VPN： 连接  
(IP地址或动态域名)  
 状态：掉线

保持连接，如断线  分钟后自动重新连接  
 QVM 备援隧道

QVM 备援隧道1： (IP地址或动态域名)  
 QVM 备援隧道2： (IP地址或动态域名)  
 QVM 备援隧道3： (IP地址或动态域名)

#### 高级设置

更改QVM用户端服务端口：

**QVM 用户帐户名称：** 输入已在 QVM 服务端中建立的对应用户名称

**密码：** 输入已在 QVM 服务端中建立的对应用户密码

**再次输入确认密码：** 再输入一次确认密码



<b>QVM VPN (中心端 IP 地址或动态域名):</b>	输入 QVM VPN 服务端 IP 地址或是网域名
<b>状态:</b>	在此字段可以看到 QVM 功能联机状态
<b>保持连接, 如断线( )分钟后自动重新连接</b>	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
<b>QVM 备援隧道:</b>	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, 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

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

## 十四、其它进阶高级功能设置

本章介绍 QoS 安全路由器进阶功能的设置，如果内网需要设置服务器提供 Web/FTP 服务等，可以通过虚拟服务器的连接设置完成，同时应部分用户需要提供静态路由以及动态路由协议的设置，一对一 NAT 功能的设置解决实体 IP 与虚拟 IP 对应，以及设置动态域名解析服务满足用户获得运营商的动态公网 IP 情况下需要建设 Web/FTP 服务器等要求。

### 14.1 DMZ/虚拟服务器

#### DMZ 服务主机

内部DMZ服务器 IP 地址 192.168.1.0

#### 虚拟服务器

服务端口	IP 地址	端口	激活
All Traffic [TCP&UDP/1 ~65535]	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	任何的	<input type="checkbox"/>
<a href="#">服务端新增或删除表</a>	<a href="#">增加到对应列表</a>		
<a href="#">删除所选择服务</a>			

[显示开列表](#) [确定](#) [取消](#)

#### 14.1.1 DMZ 设置

当您将在 QoS 安全路由器内部的某台 PC 的虚拟 IP 填入到此 DMZ 选项时，QoS 安全路由器 WAN 端的合法 IP 地址会直接对应给这台 PC 使用，也就是说从 WAN 端进来的数据包，若是不属于内部的任何一台 PC，都会传送到这台 PC 上。

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

点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。点击“取消”即会清除刚才所变动的修改设置内容参数，此操作必须在确认存储动作之前才会有效。

### 14.1.2 虚拟服务器设置

若是您需在内网需架设服务器（意指对外部的服务主机 WEB、FTP、Mail 等），这个功能可将服务器主机视为一个虚拟位置，利用 Qno 防火墙/路由器的外部合法 IP 地址，经过通讯端口的转换，（如 WWW 为 80 端口），直接存取到内部虚拟 IP 的服务器的服务。

例如在设定窗口中，选项填入服务器位置，如 192.168.1.2 且端口是 80 的话，当外部网络要进来存取这个网页时只要键入：

http://220.130.188.45 (假设此为 Qno 防火墙 / 路由器的外部合法 IP 地址)

此时，就会通过此公网 IP 地址去转换到 192.168.1.2 的虚拟主机上的 80 端口读取网页了。

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

#### 虚拟服务器



The screenshot shows a configuration window for Virtual Servers. It has four main input areas: 'Service Port' with a dropdown menu showing 'All Traffic [TCP&UDP/1~65535]', 'IP Address' with four empty text boxes, 'Port' with a dropdown menu showing '任何的', and 'Enable' with an unchecked checkbox. Below the 'Service Port' and 'IP Address' fields are green buttons labeled '服务端新增或删除表' and '增加到对应列表' respectively. A large empty rectangular box is in the center. At the bottom of this box is a green button labeled '删除所选择服务'. Below the main configuration area are three buttons: '显示开列表', '确定', and '取消'.

**服务端口：** 在此选择欲开启的虚拟服务器的通讯端口号码预设列表，如 WWW 为 80(80~80)，FTP 为 21~21，可参考服务号码预设列表！

**服务端口设定：** 若您所需要的通讯端口没有在列表里面，可以利用此功能新增或删除管理通讯端口号列表。

**内部 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 192.168.8.100。

**接口位置：** 设定内部服务器通讯端口转换所对应的广域网界面是哪一个，您可以设定外部用户只能从某一个广域网界面（某一个合法 IP）进来存取服务器的服务。

**启用：** 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口号列表。
- 加入到对应列表：** 增加到开启服务项目内容。

### 新增或删除通讯端口号

若您欲开启的服务埠项目没有在表列中，您可以点击“服务埠新增或删除表”新增或删除管理服务埠号列表，如下图所示：



The screenshot shows a web interface for managing service ports. On the left, there are input fields for 'Service Port Name', a dropdown for 'Protocol' (currently set to TCP), and 'Service Port Range' (with '到' between two boxes). On the right, a scrollable list contains various services with their protocols and port ranges: All Traffic [TCP&UDP/1~65535], DNS [UDP/53~53], FTP [TCP/21~21], HTTP [TCP/80~80], HTTP Secondary [TCP/8080~8080], HTTPS [TCP/443~443], HTTPS Secondary [TCP/8443~8443], TFTP [UDP/69~69], IMAP [TCP/143~143], NNTP [TCP/119~119], POP3 [TCP/110~110], SNMP [UDP/161~161], SMTP [TCP/25~25], TELNET [TCP/23~23], and TELNET Secondary [TCP/8023~8023]. At the bottom, there are buttons: '增加到对应列表' (Add to List), '删除所选服务服务端口' (Remove Selected Service Port), '确定' (Confirm), '取消' (Cancel), and '退出' (Exit).

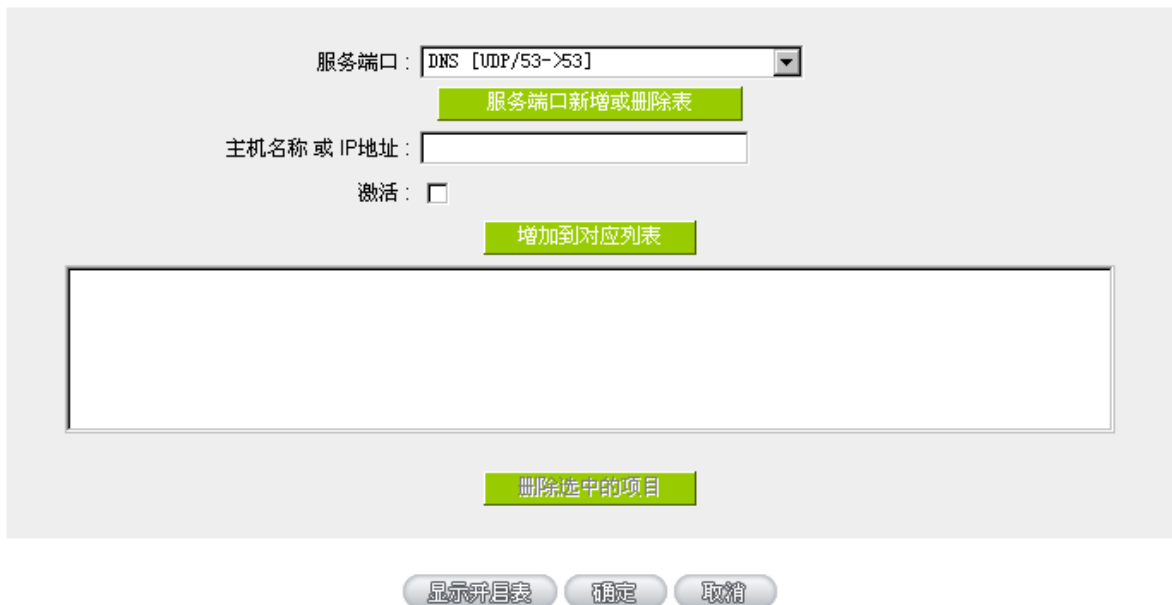
- 服务端口名称：** 在此自定义开启的服务埠名称加入列表中，如 BT 等。
- 通讯协议：** 在此选择欲开启的服务埠号的封包格式为 TCP 或 UDP。
- 服务埠范围：** 将您所需新增的服务埠范围填入。
- 增加到对应列表：** 增加到开启服务项目内容列表，最多可新增 100 组。
- 删除选择服务服务端口：** 删除所选择的开启服务项目之一笔内容。
- 确定：** 点击此按钮“确认”即会储存刚才所变动的修改设定内容参数。
- 取消：** 点击此按钮“取消”即会清除刚才所变动的修改设定内容参数，此操作必须于确认储存动作之前才会有效。
- 退出：** 离开此功能设定窗口。

## 14.2 UPnP 通讯协议

UPnP (Universal Plug and Play) 是微软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 Windows XP)而且您的计算机 UpnP 功能有开启,您可以将 VPN 防火墙的 UPnP 功能启动,可以从您的计算机上开启或关闭 UPnP Forwarding 的选项。

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。

### ▶ UPnP手动映射



- |                    |   |
|--------------------|---|
| <b>服务端口：</b>       | 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! |
| <b>主机名称或IP地址：</b>  | 在此填上UPnP相对应的内部虚拟IP地址或名称,如192.168.1.100。                     |
| <b>激活：</b>         | 开启此服务功能。  |
| <b>服务端口增加或删除表：</b> | 新增或删除管理服务端口号列表。   |
| <b>增加到对应列表：</b>    | 增加到开启服务项目内容。  |
| <b>删除所选中的项目：</b>   | 删除所选择的开启服务项目之一笔内容。  |
| <b>显示开启表：</b>      | 显示目前所开启设置的UPnP Forwarding列表。                                |
| <b>确定：</b>         | 点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。                                |
| <b>取消：</b>         | 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数,此操作必须于确认存储动作之前才会有效。             |

### 14.3 路由通讯协议

静态路由是以手动设置路由表的方式来达成数据包路由。在此 QoS 安全路由器的应用可分为两种方式，一是在内网中连结不同网段或路由器，一是在 Multi-WAN 的环境中让路由器知道去那个目的地时就要走那条 WAN。例如常常会遇到路由器不同的 WAN 申请不同运营商的线路，为了避免有些服务像是邮件服务器，或游戏服务器是架设在不同一运营商环境而且运营商之间无法彼此互通，此时去邮件服务器或是去游戏服务器就应该走不同的 WAN，而避免绕远路。这个用意跟协议绑定是有相似的做法。

#### ▶ 静态路由



The image shows a web-based configuration interface for static routing. It includes the following fields and controls:

- 目的IP地址: [ ] . [ ] . [ ] . [ ]
- 子网掩码: [ ] . [ ] . [ ] . [ ]
- 网关: [ ] . [ ] . [ ] . [ ]
- 路由节点数: [ ]
- 接口位置: 局域网 (dropdown menu)
- 增加到对应列表 (green button)
- 删除选中的项目 (green button)
- 显示开启表 (button)
- 确定 (button)
- 取消 (button)

**目的 IP 地址和子网掩码：** 填入目的地的远程网络 IP 节点与子网络节点地址。

**默认网关：** 从此网络节点到目的远程网络欲绕径的默认网关器地址。

**路由节点数：** 从此网络节点到目的远程网络所经过 QoS 安全路由器层数，如是在 QoS 安全路由器下的二个 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，是位于广域端口 WAN 端亦或是局域端口 LAN 端。

**增加到对应列表：** 增加此路径规则到列表中。

**删除所选中的项目：** 删除在表中所选择的路径表。

**显示开启表：** 显示目前最新的路径表。



#### 14.4 一对一 NAT 对应

当您的运营商线路为固定制(如 ADSL 固定 IP)时，通常运营商会给您多个合法 IP 地址。QoS 安全路由器提供您可将除了路由器本身 WAN 端口以及光纤盒或 ATU-R(网关) 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路由器内部的计算机使用，也就是这些计算机在内网虽为虚拟 IP，但当做了一对一 NAT 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 QoS 安全路由器的 WAN1 使用，另外还有其它四个合法 IP 可以分别设置到 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！

QoS 安全路由器 WAN IP 地址不能被涵盖在一对一 NAT 的 IP 范围设置中。

---



激活一对一 NAT 功能

内部起始IP地址:  .  .  .

外部起始IP地址:  .  .  .

对应范围的IP数量:

- 激活一对一 NAT 功能:** 选择是否开启此一对一 NAT 功能 “激活”开启 “禁止”关闭。
- 内部起始 IP 地址:** 虚拟 IP 地址起始 IP 地址。
- 外部起始 IP 地址:** 外部合法 IP 地址起始 IP。
- 对应范围的 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:** 加入此设置到一对一 NAT 列表中。
- 删除选中的项目:** 删除所选择的一对一 NAT 规则。
- 确定:** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
- 取消:** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于“确定”存储动作之前才会有效。

**注意！**

一对一的 NAT 模式将会改变防火墙运作的方式，您若设置了此功能，LAN 端所对应公网 IP 的服务服务器或计算机将会暴露在互联网上。若要阻绝网络的使用者主动联机到一对一 NAT 的服务服务器或计算机，请到防火墙的存取规则中设置适当的拒绝存取规则条件。

## 14.5 DDNS-动态域名解析

此路由器的“DDNS”功能可以支持 QnoDDNS.org.cn、DynDNS.org、3322.org（支持 DDNS 种类依机种不同而相异）的动态域名解析功能，其目的是为了使用动态 IP 地址(也就是无法有固定 IP 的环境)来架设虚拟服务器、建立企业使用、及远程监控时查询现在的路由器 IP。如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的 WAN IP 地址都会随运营商端要求而改变，当此时使用者申请了 DDNS 后，如“qno.QnoDDNS.org.cn”，将其设置在 DDNS 设置中，则在远程只要去 Ping QnoDDNS.org.cn 则可以知道现在 QoS 安全路由器的实际 IP。且若是内部有架设网站之类的服务，网络使用者只要在网址打上 qno.QnoDDNS.org.cn 就可以直接进入到您内部架设的 WEB。在设置此功能之前，请向 [www.qno.cn/ddns](http://www.qno.cn/ddns)、[www.dyndns.org](http://www.dyndns.org) 或是 [www.3322.org](http://www.3322.org) 提出申请，此服务是完全免费的！

另外，为了解决 DDNS 服务器可能会发生不稳定的情况，现在 QoS 安全路由器每个 WAN 都可同时对此二家 DDNS 做动态 IP 升级。

### 🔹 动态域名服务

接口位置	动态域名	状态	配置
广域网1	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns 关闭 3322 关闭 Dtdns 关闭 Qnoddns 关闭	<a href="#">编辑</a>
广域网2	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns 关闭 3322 关闭 Dtdns 关闭 Qnoddns 关闭	<a href="#">编辑</a>

\*此为示意图，会因产品线不同，图形会有所差异

选择您要设置的广域网端口，比如“广域网 1”，点击“编辑”进入广域网 1 的 DDNS 设置窗口，对要设置的 WAN 口的 DDNS 方式进行勾选。

接口位置:

DynDNS.org

用户名:	<input type="text"/>	<input type="button" value="注册"/>
密码:	<input type="text"/> (密码不能含有字符串'password')	
动态域名:	<input type="text"/> . <input type="text"/> . <input type="text"/>	
广域网 IP地址:	0.0.0.0	
状态:	DDNS功能关闭或是没有联机	

3322.org

用户名:	<input type="text"/>	<input type="button" value="注册"/>
密码:	<input type="text"/> (密码不能含有字符串'password')	
动态域名:	<input type="text"/> . <input type="text"/> . <input type="text"/>	
广域网 IP地址:	0.0.0.0	
状态:	DDNS功能关闭或是没有联机	

QnoDDNS.org.cn

\*此为示意图，会因产品线不同，图形会有所差异

- 接口位置** 显示使用者所选取的广域端口
- DDNS 动态域名解析服务：** 可以选择 QnoDDNS.org.cn、以及 3322.org(可以同时使用)。(支持 DDNS 种类依机种不同而相异)
- 用户名称：** 向 DDNS 服务提供者所申请的使用者名称。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。
- 动态域名：** 动态网址名称：向 DDNS 所注册的网址，如 abc.QnoDDNS.org.cn 或者 abc.dyndns.org。
- 广域网 IP 地址：** 目前此条 WAN 所取得的运营商之动态合法 IP 地址，当 QoS 安全路由器得到运营商端给的合法 IP 地址后会自动显示于此。
- 状态：** 显示目前 QoS 安全路由器对 DDNS 的更新状态。
- 确定：** 点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。
- 取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

### 注册 QnoDDNS 侠诺动态域名

1. 请先至 Qno 侠诺网站，进行产品注册：<http://www.qno.cn>
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 设置。
  - 4 Wan 系列产品最多申请 4 个 DDNS 设置。
  - 8 Wan 系列产品(含以上)最多申请 4 个 DDNS 设置。



:: 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快诺科技动态域名服务，代表您同意[快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:

尚可申请 4 组DDNS

已输入0个字

第1组 用户名称:  域名:

已输入0个字

第2组 用户名称:  域名:

已输入0个字

第3组 用户名称:  域名:

已输入0个字

第4组 用户名称:  域名:

## 14.6 广域网接口 MAC 地址设置

有些运营商会要求提供一固定 MAC 地址(网卡物理地址)做为运营商分配 IP 给您的认证使用,此大多适用于 Cable Mode 的用户。若有此需求的话,可使用此功能将提供给运营商的网卡物理地址(MAC 地址:00-xx-xx-xx-xx-xx)填入此项目中, QoS 安全路由器就会以此 MAC 地址作为跟运营商请求 IP 时的认证!

### ▶ 广域网MAC地址设置

接口位置	MAC地址	配置
广域网1	00-17-16-01-35-d0	<a href="#">编辑</a>
广域网2	00-17-16-01-35-d1	<a href="#">编辑</a>

选择您要设置的广域网端口,比如“广域网 1”,点击“编辑”进入广域网 1 的端口 MAC 地址设置窗口,使用者可以自行输入提供给运营商的网卡物理地址 MAC,点击此按钮“确认”即会存储刚才所变动的修改设置内容参数,点击此按钮“取消”即会清除刚才所变动的修改设置内容参数,此操作必须于确认存储动作之前才会有效。

目前设备出厂默认的 MAC 位置为 WAN 端的 MAC 地址。

接口位置: WAN1

使用者自定义广域网接口MAC地址 :	<input checked="" type="radio"/> <span style="border: 1px solid black; padding: 2px;">00</span> <span style="border: 1px solid black; padding: 2px;">-17</span> <span style="border: 1px solid black; padding: 2px;">-16</span> <span style="border: 1px solid black; padding: 2px;">-01</span> <span style="border: 1px solid black; padding: 2px;">-35</span> <span style="border: 1px solid black; padding: 2px;">-d0</span> (默认值: 00-17-16-01-35-d0)
设定与此PC的MAC地址相同 :	<input type="radio"/> bf-ff-f7-95-00-43


## 十五、工具程序功能设置

此章节介绍用来管理路由器以及测试网络联机的工具。

考虑安全的因素，建议修改密码。关于登录密码与路由器时间的设置已经在第五章 5.2 节已经介绍，在此就不做重复介绍了。

### 15.1 在线联机测试

路由器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 DNS 查询以及 Ping 二种。



The screenshot shows the 'Ping测试' (Ping Test) interface. At the top, there are two radio buttons: '域名解析测试' (DNS Resolution Test) and 'Ping测试' (Ping Test), with 'Ping测试' selected. Below the buttons, there is a text input field containing '10.10.10.100' and a '开始' (Start) button. The results are displayed as follows:

状态:	测试成功
封包:	4/4 传输, 4/4 接收, 0% 遗失
循环次数:	最小值 = 1 ms
	最大值 = 56 ms
	平均值 = 15 ms

### 域名解析测试

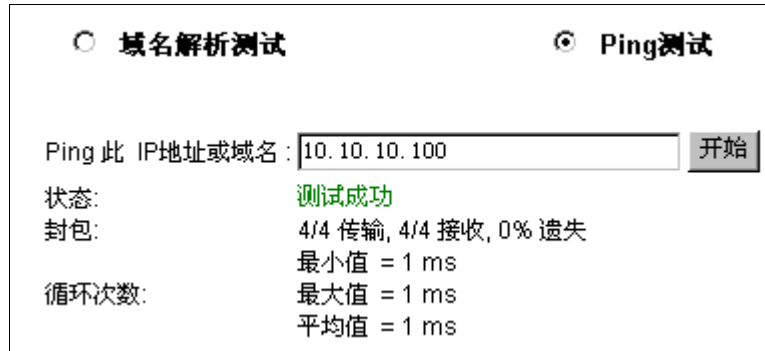
请于此测试窗口输入您想查询的网域主机位置名称，如 `www.abc.com` 然后点击开始的按钮开始测试。测试结果会显示于此窗口上。



The screenshot shows the '域名解析测试' (DNS Resolution Test) interface. At the top, there are two radio buttons: '域名解析测试' (DNS Resolution Test) and 'Ping测试' (Ping Test), with '域名解析测试' selected. Below the buttons, there is a text input field containing 'www.google.com' and a '开始' (Start) button. The results are displayed as follows:

测试域名(www.qno.cn):	www.google.com
名称:	www.google.com
地址:	72.14.235.99

## Ping-数据包传送/接收测试



域名解析测试       Ping测试

Ping 此 IP地址或域名 :

状态:                    测试成功

封包:                    4/4 传输, 4/4 接收, 0% 遗失

                             最小值 = 1 ms

循环次数:                最大值 = 1 ms

                             平均值 = 1 ms

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

请于此测试窗口输入您想测试的主机位置 IP，如 168.95.1.1 点击开始的按钮开始测试，测试结果会显示在窗口上。

## 15.2 系统软件更新

此功能可以让 QoS 安全路由器在 Web 设置窗口中直接做软件升级。请您于升级前先确认软件版本信息。点击“浏览”按钮，选择软件存放文件夹，并于选择欲升级的软件后，点击立即系统软件更新做升级。

注意！

执行软件升级前，请详细阅读窗口中的注意事项。

正在做软件升级当中时，请勿离开此升级窗口，否则会造成 QoS 安全路由器升级失败。

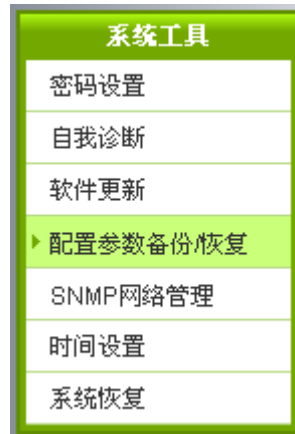
## 软件更新



- 警告：**
1. 当您选择前一个版本的软件时，所有的设定都将回复到出厂预设值
  2. 软件升级需要一点时间，此时切勿拔除电源或按下Rest按钮
  3. 当您在作软件升级时，请勿关闭此画面或中断此联机



### 15.3 系统设置参数存储



#### 从指定的配置文件恢复



#### 备份目前的配置



#### 从指定的设置文件恢复：

此功能将之前所存储在计算机的备份设置参数内容回存到 QoS 安全路由器中！选择“浏览”至备份参数文件“config.exp”存放数据夹，选择该文件后，点击“导入”按钮做设置文件导入。

#### 备份目前的设置：

此功能为存储网管人员在 QoS 安全路由器的设置参数备份到计算机中，通常做路由器版本升级前，请务必将您现在的路由器设置文件用此功能存储在计算机中！点击存储按钮，选择至备份参数文件“config.exp”存放数据夹位置，点击存储即可。

## 15.4 网络管理设置(SNMP)

SNMP 为 Simple Network Management Protocol 的缩写，指网络管理通讯协议。此为互联网上使用的一个管理工具。通过此 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)等网管程序做实时管理之通讯使用。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 QoS 安全路由器上的机器运作情况，以便随时掌握网络信息。

### SNMP网络管理

激活

系统名称:	<input type="text" value="4_WAN_QVM_Router"/>
联系方式:	<input type="text"/>
系统地址:	<input type="text"/>
Get Community Name:	<input type="text" value="public"/>
Set Community Name:	<input type="text" value="private"/>
Trap Community Name:	<input type="text" value="public"/>
Send SNMP Trap to:	<input type="text"/>

确定

取消

\*此为示意图，会因产品线不同，图形会有所差异

- 激活：** 将 SNMP 功能开启或关闭。系统默认为开启此功能。
- 系统名称：** 设置机器的名称，如 Firewall。
- 联系方式：** 设置机器的管理联系人员名称。
- 系统地址：** 设置机器的目前所在位置。
- Get Community Name：** 设置一组管理者参数可以取得此机器的项目信息，系统默认“Public”。
- Set Community Name：** 设置一组管理者参数可以设置此机器的项目信息，系统默认“Private”。
- Trap Community Name：** 设置一组管理者参数可以传送 Trap 的信息。
- Send SNMP Trap 到：** 设置一组 IP 地址或是域名名称的接收 Trap 讯号主机。
- 确定：** 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
- 取消：** 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

## 15.5 系统恢复

您可以于此工具中选择 QoS 安全路由器系统重新开机功能，请点击“系统重新启动”的“立即重新激活”按钮即可重新开机启动。

### ▶ 重新启动

立即重新启动

### ▶ 恢复原出厂设置

立即恢复原出厂设置

### 系统重新启动

如图，如果点击系统启动下的“立即重新激活”，会弹出提示对话框提示是否重新启动 QoS 安全路由器，确定 QoS 安全路由器就做重新启动操作。

### ▶ 重新启动

立即重新启动

### ▶ 恢复原出厂设置



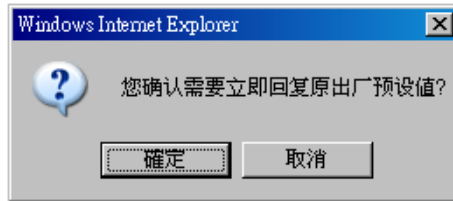
### 恢复原出厂默认值

若是选择重新恢复“立即重新激活”，会弹出提示对话框提示是否恢复出厂值，确定后 QoS 安全路由器将做恢复出厂值操作。

▶ 重新启动

立即重新启动

▶ 恢复原出厂设置



我们建议在做版本升级前请先将 QoS 安全路由器现在的设置值存储在计算机当中，等做完版本升级后，使用此功能将机器做出厂值设置以确保机器升级后的稳定运行，然后再将刚才存在计算机的设置直存回 QoS 安全路由器(如何存储路由器的设置数据、及升级完成后如何存回路由器，请参考 13.3 系统设置参数存储说明)。

### 15.6 产品功能许可证密钥 (未来支持)

Qno 侠诺系列防火墙 / 路由器产品，会有一些功能的「启用」或是「正式版」(非试用版)，会需要申请与购买许可证密钥才能够进行使用。例如 QnoSniff (侠诺神捕)、Inbound Load Balance (对内负载均衡) 等。

▶ 许可证密钥

当前时间： 2010-11-01 时间服务器地址

许可证密钥内容：  -  -  -  -

功能名称	试用版	正式版	注册时间	状态与信息
QnoSniff	√			剩余: 3 天 3 时
Router Trial				
QnoSoftKey				

**当前时间：** 在输入正式版许可证密钥 (License Key) 时，系统自动检查目前的时间是否正确，并且密钥是否仍然在有效的时间内，所以强烈建议您在试用与输入正式版密钥时，先检查并更新至目前最新且正确的时间，以避免在使用功能时产生问题。

**许可证密钥内容：** 输入您所申请与购买的正式版产品密钥内容，一般是数十个英文与数字的组合，输入之后按下「提交」，系统会检查该把产品密钥是否合法正确，如果是

- 功能名称：**合法正确即可开始使用该功能正式版，下方该功能的正式版栏位也会打勾。显示加值的功能列表，若出厂默认值在试用版栏位没有「试用」按钮，表示该功能无法进行试用，或是该类功能是属于如 QnoSoftKey 之类的支持隧道数量。
- 试用版 / 正式版：**可以进行试用的功能项目在出厂默认值时，会在试用版的栏位中显示「试用」按钮，按下按钮后就可以试用该功能一段时间。
- 注册时间：**正式版栏位在您申请并且成功输入密钥、认证成功后，会在该栏位打勾表示该功能项目已经成为正式版，不用受到试用版天数的限制。
- 状态与信息：**显示目前试用版剩余的试用天数，或是 QnoSoftKey 等目前系统所支持的隧道数量。
- 刷新：**重新更新目前系统功能的状态与时间。

## 十六、日志功能设置

日志功能纪录 QoS 安全路由器的运行数据，并以可读的方式呈现再设置窗口上提供给您作为参考。您可以依据需求检视这些信息。

### 16.1 系统日志

QoS 安全路由器的日志记录提供三种设置：系统日志，电子邮件通知，以及选择日志的类别。

#### 发送到日志服务器

激活

主机名称：	<input type="text" value="0.0.0.0"/>	(正确网域名称或IP地址)
-------	--------------------------------------	---------------

#### 发送到电子邮箱

激活

电邮服务器：	<input type="text"/>	(正确网域名称或IP地址)
电子邮件：	<input type="text"/>	
发送数量：	<input type="text" value="50"/>	笔
发送间隔时间：	<input type="text" value="10"/>	分钟

立即发送到电子邮箱

#### 系统日志配置

告警日志		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> 登入认证错误	

一般日志		
<input checked="" type="checkbox"/> 系统错误信息	<input type="checkbox"/> 被阻挡的管制条例	<input type="checkbox"/> 允许通过的管制条例
<input checked="" type="checkbox"/> 系统配置变更	<input checked="" type="checkbox"/> 认证登入	

查看系统日志

出去NAT记录

进入NAT记录

清除日志

## 系统日志

- 激活传送到日志服务器:** 若是勾选此选项的话，传送系统日志功能将被开启。
- 系统日志服务器主机名称:** 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。  
QoS 安全路由器的系统日志 提供了包含动作中的联机来源位置与目的位置，服务编号以及状态。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。

## 电邮告警功能(未来支持)

- 激活传送到电子邮箱:** 若是勾选此选项的话，电子邮件告警将会被开启。
- 电邮服务器:** 请输入电子邮件服务器的名称或是 IP 地址，如 mail.abc.com。请注意，您必须有权限经由所填入的电子邮件服务器寄送日志电子邮件，否则此日志电子邮件将无法被寄出。
- 电邮地址:** 此为设置日志收件人电子邮件信箱，例如 abc@mail.abc.com
- 传送日志数量:** 自定日志数量，系统默认为 50 条。当到达此数量时，QoS 安全路由器将会自动 Mail 传送日志。
- 传送区隔时间:** 自定传送日志间隔时间，系统默认为 10 分钟。当到达此时间时，QoS 安全路由器将会自动 Mail 传送此日志。  
QoS 安全路由器将会自动判别当数量或是间隔时间哪一个参数先到达，就 Mail 传送日志信息给管理者。
- 立即传送到电子邮箱:** 使用管理者可以直接按此按钮传送日志。

## 系统日志设置

### ▶ 系统日志配置

告警日志		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> 登入认证错误	

一般日志		
<input checked="" type="checkbox"/> 系统错误信息	<input type="checkbox"/> 被阻挡的管制条例	<input type="checkbox"/> 允许通过的管制条例
<input checked="" type="checkbox"/> 系统配置变更	<input checked="" type="checkbox"/> 认证登入	

查看系统日志	出去NAT记录	进入NAT记录	清除日志
--------	---------	---------	------

QoS 安全路由器 提供了包含以下的告警内容信息，您只要打勾点选即可包含在日志信息中。

- Syn Flooding :** 即在短时间内传送大量的 syn 数据包，造成系统记录联机的内存溢满。
- IP Spoofing :** 通过数据包监听程序来拦截网络上所传送数据，并在读取后藉由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数据包，造成系统宕机。
- 登录认证错误 :** 当系统发现有企图登录 QoS 安全路由器的入侵者时，就会将信息传到系统日志中。

### 一般系统日志信息

QoS 安全路由器 提供了包含以下的一般性内容信息，您只要打勾点选即可。系统错误信息，被阻挡的管制条例，允许通过的管制条例，认证登录，系统设置变更。

- 系统错误信息 :** 提供系统中各种错误给系统日志。例如：不正确的设置或是功能异常状况发生。
- 被阻挡的管制条例 :** 当有用户试图进行存取规则中不允许的规则时，此信息会传送到系统日志中。
- 允许通过的管制条例 :** 当用户进行存取规则所允许的规则时，此信息会传送到系统日志中。
- 系统设置变更 :** 当系统的设置值改变时，此信息回传送到系统日志中。
- 认证登录 :** 每一个成功登录系统的 IP 地址都会传送并记录到系统日志中。

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：

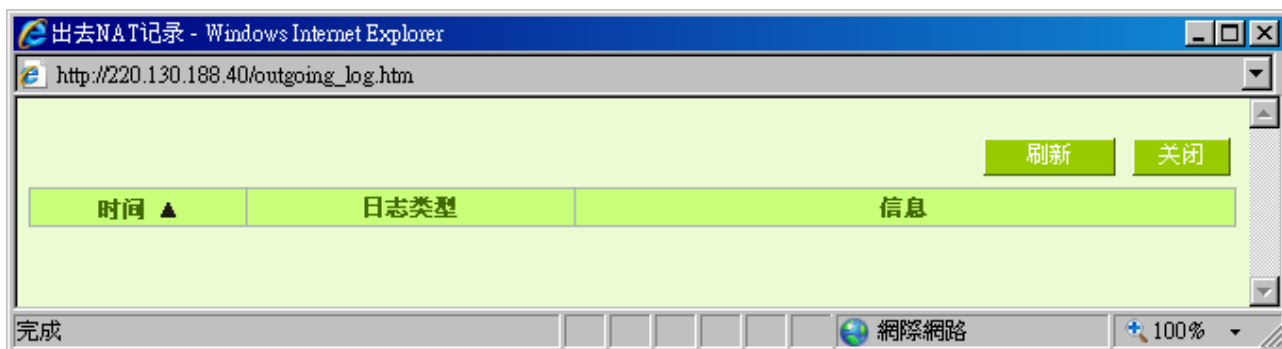
此为查看系统日志使用，其信息内容可以从下拉式选单中分类读取，包含全部日志，系统日志，防火墙日志。选择“刷新”按钮可以刷新日志显示窗口，“清除”按钮可以清除所有日志记录。如下图所示：





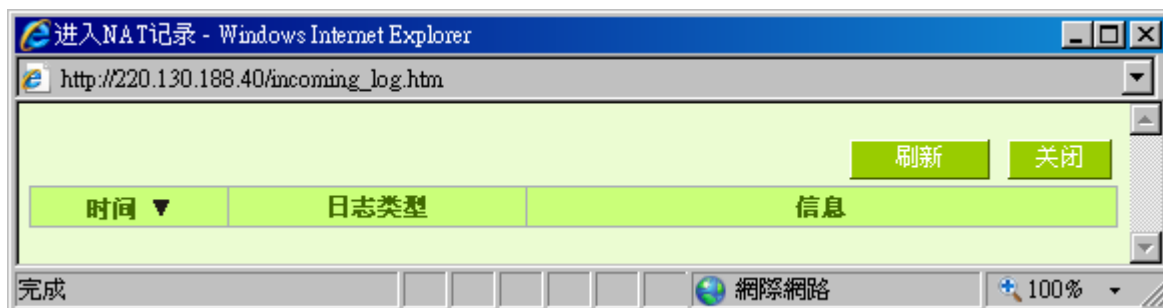
### 出去 NAT 记录：

查看内部 PC 出互联网的的系统数据包日志，此日志包含内部网络地址，目的地地址以及所使用的通讯服务端口号、类型等信息。



### 进入 NAT 记录：

查看外部进入 QoS 安全路由器的系统数据包日志，此日志内含外部来源网络地址，目的地地址与通讯端口号等信息。



### 清除日志：

此按钮为清除所有目前 QoS 安全路由器的日志相关信息。

## 16.2 系统状态实时监控

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的运行信息，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(MAC 地址)，子网掩码，默认网关，域名解析服务器(DNS)，网络侦测，收到的数据包数量，传送的数据包数量，全部的进出数据包数量统计，收到的数据包 Byte 流量统计，传送的数据包 Byte 流量统计，全部进出的数据包 Byte 流量统计，收到的错误数据包统计以及端口丢弃的数据包统计，会话数，新联机数，上传带宽使用率，下载带宽使用率等信息。

### ▶ 系统状态

端口：	广域网1接口	广域网2接口	局域网
机器名称：	eth1	eth2	eth0
目前端口连线状态：	联机	激活	---
IP 地址：	192.168.3.108	0.0.0.0	192.168.1.1
MAC 地址设定：	00-17-16-03-26-CE	00-17-16-03-26-CF	00-17-16-03-26-CD
子网掩码：	255.255.255.0	0.0.0.0	255.255.255.0
预设网关 IP 地址：	192.168.3.1	0.0.0.0	---
域名解析服务地址：	192.168.3.10	0.0.0.0	---
线路侦测机制：	测试成功	测试失败	---
收到的网络包数量：	1758	0	2972
传送的网络包数量：	1085	0	3877
全部的网络包数量：	2843	0	6849
收到的网络包 Byte 数量：	261279	0	423041
传送的网络包 Byte 数量：	155810	0	2456424
全部的网络包 Byte 数量：	417089	0	2879465
接收 Bytes/秒：	300	0	2156
传送 Bytes/秒：	0	0	30789
收到的错误网络包统计：	0	0	0
端口丢弃的网络包统计：	0	0	0
联机状态 (session)：	0	0	---
新联机数/秒：	0	0	---
上传带宽使用率：	0	0	---
下载带宽使用率：	0	0	---

### 16.3 流量统计

QoS 安全路由器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。

**流量统计**

激活

网络流量统计方式： 依下载流量的会话 ▾

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

刷新

依上传流量的 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。

网络流量统计方式： 依上传流量的IP地址 ▾

来源IP地址	bytes/sec	%
10.10.10.100	1395	100

刷新

依下载流量的 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。

网络流量统计方式： 依下载流量的IP地址 ▾

来源IP地址	bytes/sec	%
10.10.10.100	8737	100

刷新

依上传流量的端口：

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。

网络流量统计方式：

通讯协议	目的端口	bytes/sec	%
TCP	443	2862	98
UDP	8000	30	1
TCP	1863	4	0

依下载流量的端口：

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。

网络流量统计方式：

通讯协议	目的端口	bytes/sec	%
TCP	2082	160	50
TCP	443	70	22
TCP	2083	52	16
TCP	1863	29	9

依上传流量的会话：

在此图表中显示了从广域网络进来的(Dest. IP)地址所联机的局域网络的 IP(Source IP)位置所使用的服务端口 (Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式：

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
10.10.10.100	TCP	3802	59.124.180.50	443	30	68
10.10.10.100	UDP	4000	58.251.60.87	8000	5	12
10.10.10.100	TCP	3803	59.124.180.50	443	4	9

依下载流量的会话：

在此图表中显示了从局域网络的 IP(Source IP)地址对外联机的目的地位置(Dest. IP)IP 及所使用的服务端口 (Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式： 依下载流量的会话

目的IP地址	通讯协议	目的端口	来源IP地址	来源端口	bytes/sec	%
10.10.10.100	TCP	3979	65.55.15.244	80	72	37
10.10.10.100	TCP	3964	122.116.228.7	443	39	20
10.10.10.100	TCP	3980	207.46.26.26	1863	36	19
10.10.10.100	UDP	1056	168.95.1.1	53	29	15
10.10.10.100	TCP	3328	207.46.107.46	1863	12	6

刷新

#### 16.4 特定 IP 及端口状态

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 端口而必须走单一个 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。

**IP/端口流量监控**

激活

查询方式依 IP地址 IP地址： .  .  .  查询

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
--------	------	------	------	--------	------	-------------------	-------------------

刷新

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端口号。

查询方式依  IP地址:  .  .  .

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
10.10.10.100	TCP	3328	WAN2	207.46.107.46	1863	0	0
10.10.10.100	TCP	3351	WAN2	59.124.180.50	443	4	22
10.10.10.100	TCP	3352	WAN2	59.124.180.50	443	18	4
10.10.10.100	UDP	4000	WAN2	58.251.60.87	8000	70	39
10.10.10.100	TCP	3802	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3803	WAN2	59.124.180.50	443	0	0
10.10.10.100	UDP	6001	WAN2	58.251.62.71	8000	0	0
10.10.10.100	TCP	3964	WAN2	122.116.228.7	443	40	25
10.10.10.100	TCP	3977	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3978	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3980	WAN2	207.46.26.26	1863	4	20
10.10.10.100	UDP	1056	WAN2	168.95.1.1	53	0	0
10.10.10.100	TCP	3981	WAN2	208.50.79.27	80	0	0
10.10.10.100	UDP	6007	WAN2	210.22.23.177	8000	0	0

刷新

特定端口状态：

直接在端口里填入您想要查询的端口号，就可以显示出此端口现在有哪些 IP 正在使用。

查询方式依  服务端:

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
60.248.180.226	TCP	2110	WAN2	220.130.188.40	80	471	885
60.248.180.226	TCP	2111	WAN2	220.130.188.40	80	52	57
60.248.180.226	TCP	2112	WAN2	220.130.188.40	80	99	873
60.248.180.226	TCP	2113	WAN2	220.130.188.40	80	52	57
60.248.180.226	TCP	2114	WAN2	220.130.188.40	80	0	0

刷新

## 附录一：常见问题解决

### (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)走固定的广域网参照下图协议绑定设置：

#### 协议绑定



服务端：QQ [UDP/8000~8004]

来源IP地址：0 . 0 . 0 . 0 到 0 . 0 . 0 . 0

目的IP地址：0 . 0 . 0 . 0 到 0 . 0 . 0 . 0

接口位置：广域网1

激活：

QQ [UDP/8000~8004] -> 0.0.0.0~0 (0.0.0.0~0.0.0.0) 广域网1

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

### QoS带宽管理

控制类型： 带宽控制  优先级

接口位置： 广域网1  广域网2

服务端口：

IP地址： .  .  .  到

目的：

保证带宽： Kbit/sec 最大可用带宽： Kbit/sec

带宽分配方式： 此范围每一IP地址独享此设定带宽。  
 此范围所有IP地址共享此设定带宽。

激活：

QQ [UDP/8000~8004]->0.0.0.0~0 (上传)=>200~2000Kbit/sec->WAN1, 2
---



(2) 阻挡基本 BT 种子下载方式

若您想要封锁 BT 种子，不让用户下载，您可以直接在 "防火墙设置" => "内容过滤" 选择 "设定禁止访问的域名" 后将 "网页内容过滤(关键字)" 打入 ".torrent" 这样就可以防止用户下载种子。

- 设定允许访问的域名
- 设定禁止访问的域名

禁止访问的域名

激活

网页内容过滤(关键字)

激活



关键字:  (仅支持英文关键字)

管制所有IP地址:  .  .  .  到

(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局域网中冲击波及蠕虫病毒造成局域网访问互联网很慢及联机数(Session)大量增加造成 QoS 安全路由器大量处理，以下将指导您封锁此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:



服务名称:

通讯协议:

端口范围:  到

增加到对应列表

HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]
PPTP [TCP/1723~1723]
IPSec [UDP/500~500]
TCP [TCP/135~139]
UDP [UDP/135~139]
TCP [TCP/445~445]

删除选中的项目

确定 取消 关闭

b.用防火墙里面的“存取规则”功能将设置好的此三组端口封锁:

访问规则设置

管制动作:	禁止
服务端口:	TCP [TCP/135~139] <span>服务端口新增或删除表</span>
日志:	激活
接口位置:	任何的
来源IP地址:	任何的
目的IP地址:	任何的

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:

跳到  / 2 页      每页显示  笔      [下一页 >>](#)

优先级	激活	管制动作	服务端口	接口位置	来源IP地址	目的IP地址	管制时间	日	编辑	删除
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	关闭	TCP [445]	*	任何的	任何的	所有时间		<input type="button" value="编辑"/>	<input type="button" value="删除"/>
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	关闭	UDP [135]	*	任何的	任何的	所有时间		<input type="button" value="编辑"/>	<input type="button" value="删除"/>
<input type="text" value="3"/>	<input checked="" type="checkbox"/>	关闭	TCP [135]	*	任何的	任何的	所有时间		<input type="button" value="编辑"/>	<input type="button" value="删除"/>
	<input checked="" type="checkbox"/>	允许	所有端口 [门]	局域网	任何的	任何的	所有时间			
	<input checked="" type="checkbox"/>	关闭	所有端口 [门]	广域网1	任何的	任何的	所有时间			

#### (4) 阻止 QQLive 视频直播设置

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，当局域网有多用户同时使用 QQLive 视频直播软件，占用了比较大的带宽，造成 QoS 安全路由器的负担过重，使得 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，下面就这个问题来结合 Qno 产品的相关功能提出相关的解决方案，来进行 QoS 安全路由器设置。

a). 进入路由器 Web 管理页面，再进入“防火墙设置”的“访问存取规则设置”。

#### 1 访问规则设置

管制作动:	禁止
服务器端口:	所有端口 [TCP&UDP/1~65535] <span style="float: right;">服务器端口新增或删除表</span>
日志:	关闭
接口位置:	任何的
来源IP地址:	任何的
目的IP地址:	单独 58 . 60 . 11 . 145

#### 2 生效时间

管制时间为	所有时间	:	:	到	:	:	(时间格式:24小时制)
<input type="checkbox"/> 每天	<input type="checkbox"/> 周日	<input type="checkbox"/> 周一	<input type="checkbox"/> 周二	<input type="checkbox"/> 周三	<input type="checkbox"/> 周四	<input type="checkbox"/> 周五	<input type="checkbox"/> 周六

b). 再点击“增加新的管制规则”，进入“访问存取规则设置”页面，在“存取服务规则设置”中的“管制作动”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“时间管制设置”的“此存取规则选择”所有时间，“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 QQLive 的服务器的连接被封锁，点击确认完成对阻止 QQLive 视频直播设置，此方案是在 QQLive3.1 的版本下测试并完成阻挡的。

## 附录二：Qno 技术支持资讯

更多有关侠诺产品技术资讯，除了可以登录侠诺宽带讨论区、参照 FTP 服务器的相关实例；或是进一步联系侠诺各经销商技术部门、或侠诺大陆技术中心取得相关协助。

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](http://www.Qno.cn/web/where_buy.asp)

技术中心：

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