QVM1000 中文使用手册

软件版本 :V 2.0.1

Table of Contents

1. Introduction 概述

QVM1000 是一台符合中大型企业，网吧及社区等级的 Multi-WAN 旗舰型机种，高效能整合新一代设计的防火墙多 WAN 口路由器。 除了具备绝大多数宽带市场适用的对外联机能力外，还内建了 10/100Mbps QoS 及 VLAN 交换器，以满足多数企业、网吧对防火墙的市场需求。QVM1000 除了提供硬件 DMZ 端口为防火墙的标准配备外，还提供最高八个 WAN Ports 使用。此八个 WAN Ports 不仅可以支持高效能网络自动负载平衡模式(Intelligent Balancer by auto mode)，亦可针对特定使用者的 IP 群组，以提供分级服务 classes of service (CoS) (IP Group by Users)，并且还支持 IP Balance Mode 提供弹性灵活的网络需求设定。

配合新一代、多样化、高安全整合性的防火墙设备需求环境，内建超高速 Intel IXP 425 整合型 RISC CPU，在频率 533Mhz 的高速处理架构下加上 128M 的高内存容量，发挥超高的网络效能。处理速度及带机量直逼中，大型企业用户专用的昂贵防火墙设备；并获得企业界广泛的应用系统支持，其防火墙效能可达 200Mbps 以上。且具备目前企业广泛应用的虚拟私有网络（VPN）硬件加速模式，包含 IPSec DES/3DES 等 VPN 加密，同时可以处理 200 条的 VPN 联机，以 3DES 方式工作性能可达 90Mbps 以上，不论是功能，实用还是安全性等，都超越目前大型昂贵设备的性能。

QVM1000 IPSec VPN 适用于各办公室， 事业伙伴及远程使用者一个安全便利的网络加密方式。 包括 168 bit Data Encryption Standard (3DES)， 56 bit Data Encryption Standard (DES)， 以及 AH/ESP 方式。VPN 功能提供了各分支点间或大多数远程使用者采 VPN 方式，将资料自动加密解密的通讯方式，支持 Gateway To Gateway ，Client To Gateway 与 Group VPNs 等模式

配合 Qno 领先同行独家的 QVM 功能，搭配 QVM330 的应用，实现了简单易懂的设定 VPN，且提供了中央控制的功能，可以随时通过 VPN 进行远程登入，并对远程的 QVM330 进行控管，且安全及保密性绝对符合 IPSec 精神。

QVM1000 内建进阶型防火墙功能，能够阻绝大多数的网络攻击行为， 使用了 SPI 封包主动侦测检验技术 (Stateful Packet Inspection)，封包检验型防火墙主要运作在网络层，执行对每个连接的动态检验，也拥有应用程序的警示功能，让封包检验型防火墙可以拒绝非标准的通讯协议所使用的连结， 预设自动侦测并阻挡。QVM1000 亦同时支持使用网络地址转换 Network Address Translation (NAT)功能以及 Routing 路由模式，使网络环境架构更为弹性，易于规划管理。

Content Filtering 内容过滤功能允许企业内部自订网络存取规则，管理页面内建可新增移除的过滤名单，可让管理者选择应该禁止存取或记录监控哪些种类的网站， 如此可对学校或企业的 Internet 管理有明确的作用，设置过滤设定并通过完整的 OS 管理核心。 QVM1000 提供线上多样化的日志(SysLog)纪录，支持线上管理设定工具，可清楚易懂的知道网络设定状态、并加强管理全部的网络安全存取规则、VPN、及其它服务等。

QVM1000 能充分保障各种分支机构办公室及各点间通讯的安全， 避免日益趋多的商业机密窃取与攻击破坏等。专属的 OS 独立式作业平台， 使用者无须具备专业级的网络知识即可安装使用。 通过浏览器如:IE，Netscape..来设定与管理 QVM1000 防火墙路由器。

2. Main features:主要产品功能

Product Features

网络联机:

- One IP address to access the Internet over your entire network
- WAN: DHCP client， static IP， PPPoE，PPTP
- DMZ: DHCP client， static IP， PPPoE
- LAN: DHCP auto-assignment， Mac-assignment DHCP static IP， Static IP。

Multi-WAN 多线网络连结:

- 全自动型的负载平衡模式 Intelligent Balancer (Auto Mode)
- 网络服务侦测-NSD for Intelligent Balancer
- 特定使用者的 IP 群组，以提供分级服务 classes of service (CoS) (IP Group by Users)
- 以 IP 来平均分派给每一个 WAN 的 IP Balance Mode
- 协议绑定 Protocol Binding
- 服务质量 QoS

TCP/IP 通讯协议:

- DHCP Client/Server
- IP & MAC Binding
- PPPoE
- NAT with popular ALG support
- NAT with port forwarding
- NAT with port triggers
- DNS 转送功能-DNS Relay
- ARP
- ICMP
- FTP/TFTP
- 密码保护-Password protected configuration or management sessions for web access
- 全自动型的负载平衡模式 Intelligent Balancer (Auto Mode)
- 特定使用者的 IP 群组，以提供分级服务 classes of service (CoS)
- 以端口为基础的带宽政策 Port-based QoS

- 时间服务器通讯协议 NTP Time Server

路由通讯协议:

- 支持动态路由 RIP 1， RIP 2 compatible， 静态路由 Static routing
- 支持网关模式 Gateway/路由模式 Routing Mode Support

路由器管理功能:

- 网页模式管理与规则设定-Comprehensive web based management and policy setting
- 支持网络管理通讯协议 SNMP v1/v2c
- 线上动态实时系统日志 Monitoring， Logging， 系统告警功能 Alarms of system activities
- 具备由 Web 方式的软件升级备份(Fault-tolerance Web upgrade new software)
- 具备双份的可置换软件储存空间备份(Dual Firmware Backup or Restore)
- Supports filter capability (Service and IP)
- 支持系统日志以及电子邮件自动告警功能(Support Syslog & E-Mail Alert。)

防火墙功能:

- 防火墙主动封包检测技术-Stateful Packet Inspection Firewall
- IP 位置过滤功能-IP filtering; allows you to configure IP address filters
- 端口位置过滤功能-Port filtering; allows you to configure TCP/UDP port filters
- 支持硬件式的 DMZ 独立端口-Support Hardware DMZ to protect your network
- 阻断式攻击-Denial of Service (DoS) prevention Dos attack prevention
- 网页内容过滤机制-Inappropriate URL command line filter
- 可设定网络存取时间控制-Set Internet accessing time schedule
- 网络攻击模式侦测-Syn Flooding/IP Spoofing/Win Nuke/Ping Of Death

VPN 虚拟私有网络功能:

- 支持高速 3DES VPN 联机效能速率可达 90Mbps-IPSec VPN 3DES Throughput 90Mbps UP。
- 支持 VPN 联机信道数 200 条-Support up to 200 VPN tunnels
- 支持 2 组群组 VPN 功能-Up to 2 Group VPNs support
- 简单易懂的 VPN 设定与管理接口-Friendly VPN Tunnel Management
- 支持 IKE 功能-IKE : Pre-Shared keys
- 支持 IPSec 标准的 DES/3DES 加密-IPSec Encryption DES/3DES
- 支持以 IPSec 为标准的 MD5/SHA1 验证-IPSec Authentication MD5/SHA1
- 支持 PMTU 的密钥管理-Support PMTU Key management: IKE
- 支持网域名称转换 IP 位置 DNS Resolve

- 支持 PPTP 协议建立 VPN 信道
- 支持 VPN 透通功能-VPN Pass-through

QVM:

- Qno VPN 中央控管功能，其搭配 QVM330，可以达到 VPN 简单快速的 IPSec 信道连接，更可以直接透过中央控制接口透过 VPN 信道直接连接进入 QVM330 做控制。
- 简单的 User Name(用户名称)及 Password(密码)，就可以将 VPN 信道连接成功
- 搭配 QVM 系列可以确保 VPN 信道断线后可迅速连接成功
- 搭配 QVM 系列可以支持 VPN 备份，确保中心端或客户端 VPN 服务永不断线

其它功能:

- 虚拟主机 Virtual Server –Port Forwarding。
- 特殊应用软件 Port-Triggering Support
- 支持内建软件式非军事管制区 DMZ 功能-Support Software DMZ。
- 支持国际标准即插即用功能-UPnP Support
- 支持一对一的网络位置对应功能-One to One NAT Support。
- 动态 DNS 支持-DDNS Support
- 可变更的 WAN 网络实体位置-MAC Clone Change Support
- 线上对外线路测试功能-Diagnostic with DNS Lookup & Ping。
- 路由器参数设定备份和储存-Setting Backup with Import & Export。

封包传输效能:

- 防火墙效能-Firewall: 200Mbps
- VPN 虚拟私有网络效能-3DES 168bit VPN: Up to 90Mbps。

硬件规格:

- 中央处理器 CPU: Intel IXP425- 533MHz RISC
- 内存 SDRAM : 128Mbyte
- 闪存 Flash Memory: 16Mbyte

网络支持通讯规格:

- IEEE 802.3 10Base-T

- IEEE 802.3u 100Base-TX

网络硬件接口规格:

- 广域网络 WAN 2~8: 10/100Base-T/TX RJ-45 ports
- DMZ: One 10/100Base-T/TX RJ-45 port
- 局域网络-LAN 1~11: 11 Port 10/100Base-T/TX RJ-45 ports
- 一个硬件重置按钮可回复出厂默认值-One reset button for factory default setting

LED显示:

- 系统-电源与自我检测功能 System: Power， DIAG
- 速度 Speed， 联机/动作 Link/Activity， 广域网络 WAN，连结 Connect

操作环境:

- 工作温度 Operating Temperature: 0^0 ~ 45^0C (32^0 ~ 113^0F)
- 储存温度 Storage Temperature: -20^0 ~ 60^0C (-4^0 ~ 140^0F)
- 湿度 Humidity: 0 ~ 90% non-condensing

安规验证:

- EMI/EMC: FCC Class A， CE Mark

外型尺寸:

- 19″ (L) x 9″ (W) x 1。75″ (H) Inch

电源供应:

- Internal: AC100~240V /50~60Hz

安装方式:

- Desktop
- 19″ Rack- Mount Tools Kit

3. How To Install QVM1000-如何安装

Hardware –硬件安装介绍

QVM1000 前面板:

LED Status-面板灯号

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

Reset Button-硬件 Reset 按钮

Action	Description
按下 Reset 按钮 5 秒	热开机，重新激活 QVM1000 DIAG 灯号: 橘色灯号慢慢闪烁
按下 Reset 按钮 10 秒以上	回复原出厂默认值(Factory Default) DIAG 灯号: 橘色灯号快闪。

Replacing a Lithium Battery-更换系统内建电池

QVM1000 防火墙路由器内建有系统时间的电池。 此电池使用寿命约为 1~2 年。 当电池已经无法充电或是使用寿命结束后， QVM1000 将无法正确纪录时间或是连接网际网络的同步 NTP 时间服务器，您必须与系统厂商联系，以便取得更换电池的

技术。

Note: 请勿自行拆解机器，若您需要更换电池的话，请与我们联系！

Setting up the Chassis-将 QVM1000 安装于标准 19”机架上

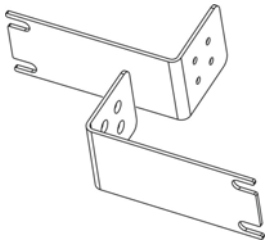
您可以将 QVM1000 放置于桌上使用，或是您有机房专用 19 吋标准机架的话，可以将 QVM1000 安装于机架上，每一台 QVM1000 都有配备专用连接机架配件。

Setting the Chassis on a desktop or other flat， secure surface

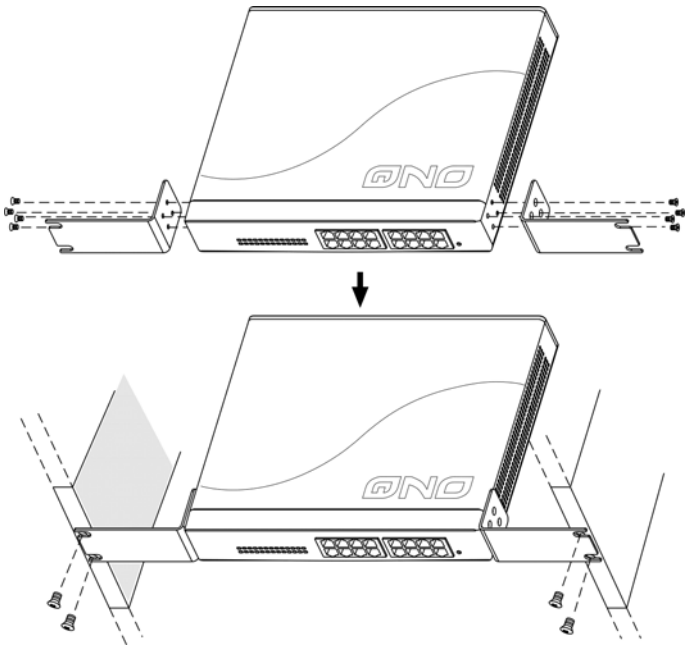
若您需要安装 QVM1000 于机架上的话，请不要将其它过重的物品堆叠或是放置于机器上，以免因承受重量过重而发生危险或是损伤机器。

Rack-Mounting the Chassis

每一台 QVM1000 都有配备专用连接机架配件，包含 2 只 brackets 以及八颗专用螺丝提供与 QVM1000 连接安装使用。

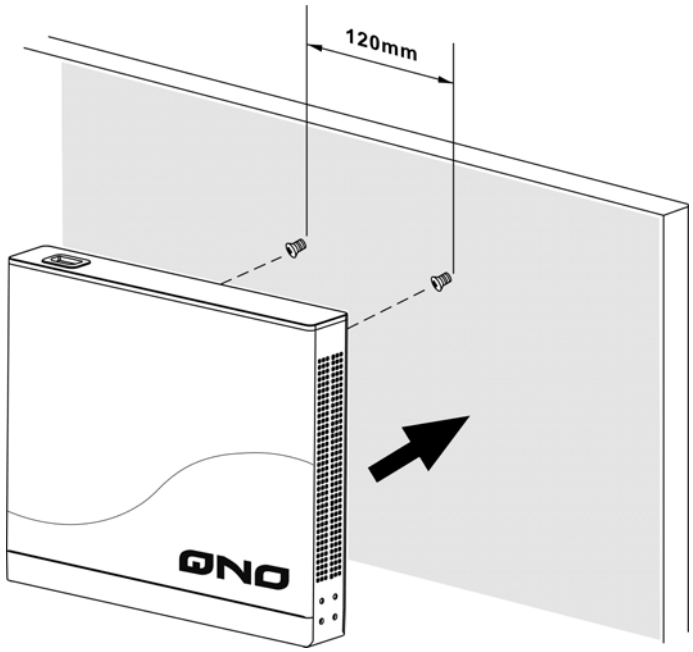


当您安装锁定 QVM1000 所提供的机架专属配件后，您可以直接安装于您的标准机架上，如下图所示:



Wall-Mounting the Chassis-将 QVM1000 设备安装在墙上

于 QVM1000 机器底部有二个十字孔位，您可以使用一般螺丝先旋转锁进墙壁上，确认牢固后，再将 QVM1000 的底部二个十字孔位准确的挂在此二颗螺丝上即可完成安装，如下图所示:



Connecting the QVM1000 to your Network-连接路由器到您的网络上

QVM1000 防火墙路由器到您的网络上，连接模式有分为二种:

设定广域网络联机(**WAN** connection): WAN 端口可以连接如 xDSL Modem， Switch HUB，光纤盒或是外部路由器。

设定局域网络联机(**LAN** connection): LAN 埠口可以连接如 Switch HUB 或是直接与 PC 联机。

设定 **DMZ** 埠口: 此端口口可以连接如外部合法 IP 位置的服务器， 如网页 (Web) 以及电子邮件服务器(Mail servers)等。

接下来请连接 QVM1000 背部电源线，然后会看到 QVM1000 的面板 Power 灯号亮起，以及一小段时间做自我开机测试即可开始使用并进行设置工作！

4。 How To Manage QVM1000

Login-开始登入设定 QVM1000

请输入使用者名称(User Name)与密码(Password)于上方所示密码验证字段当中， 然后按下”确定”按钮。

QVM1000 防火墙路由器其预设的使用者名称(User Name)与使用者密码(Password)皆为’admin' ，您可以更改此登入密码！我们强烈建议您务必更改管理密码！！

Home-设定首页

此首页画面(Home)显示 QVM1000 防火墙路由器系统所有参数以及状态显示信息，此信息仅提供管理者读取。若您想进一部查询该细部相关设定的话，可以按点击下面的超级链接按钮，并可以快速立即进入该选项设定当中。 此画面也显示了两种语言版本(英文与简体中文)。请按下要显示语言版本的按钮，此按钮也会自动改变成绿色显示出目前的版本画面。

System Information

Serial Number:(机器序号)

此为显示 QVM1000 的机器序号。

Firmware version:(软件版本信息)

此为显示 QVM1000 的目前使用的软件版本信息。

CPU:

此为显示 QVM1000 使用的 CPU 型号为 Intel IXP425-533Mhz。

DRAM:

此为显示 QVM1000 使用内存(DRAM)为 128MB。

Flash:

此为显示 QVM1000 使用闪存(Flash)为 16MB。

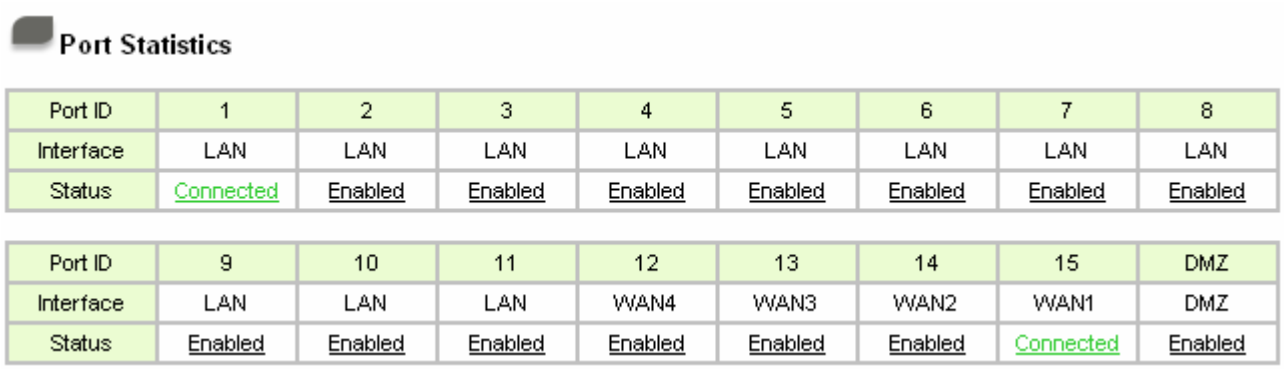
System active time:

此为显示 QVM1000 目前已经开机的时间。

Current time:

此为显示 QVM1000 目前正确时间，但是必须注意，您需要正确设定与远程 NTP 服务器的时间同步后才会正确显示。

Port Statistics(硬件各端口-Port 状态实时显示)

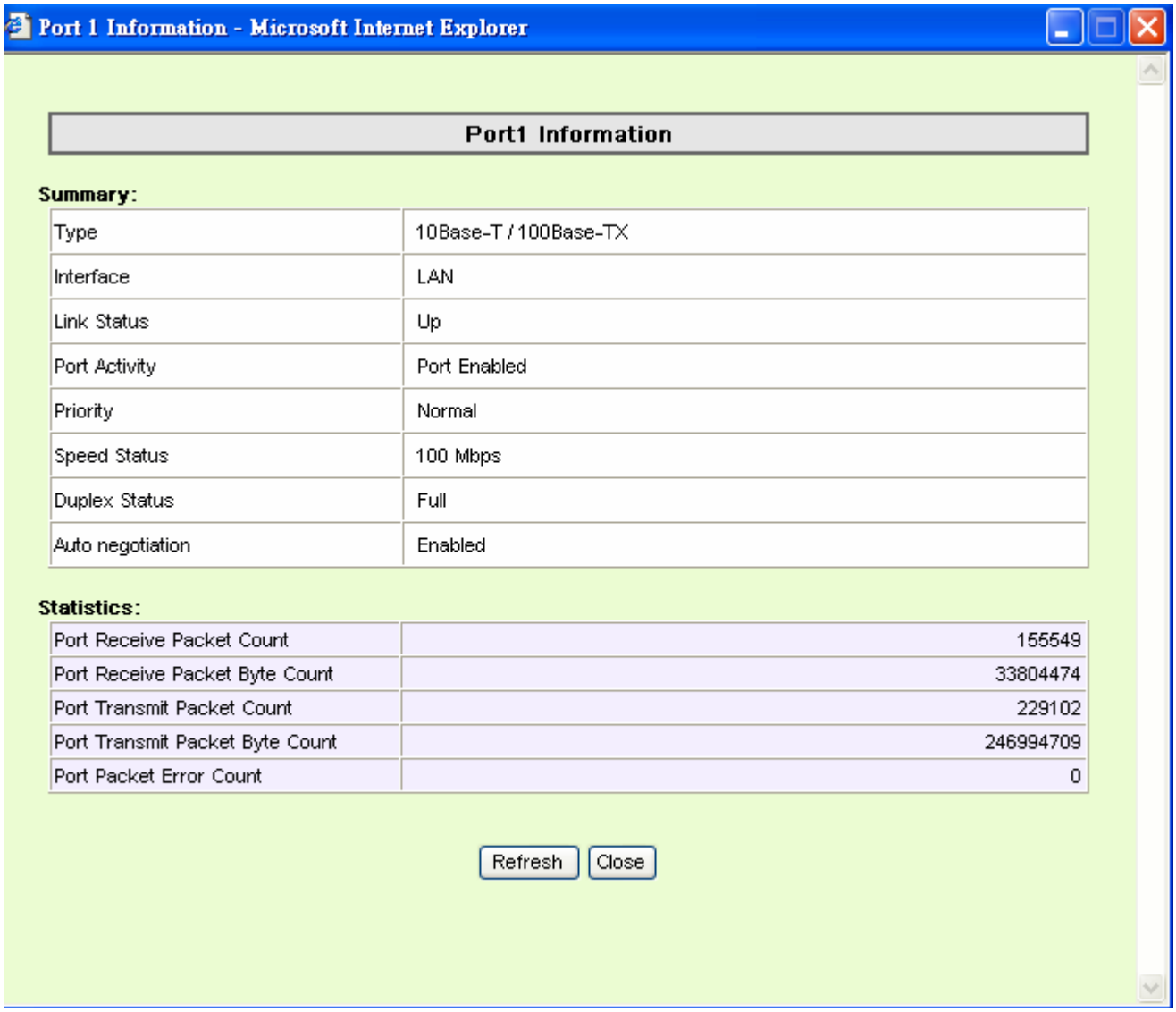


Port Statistics

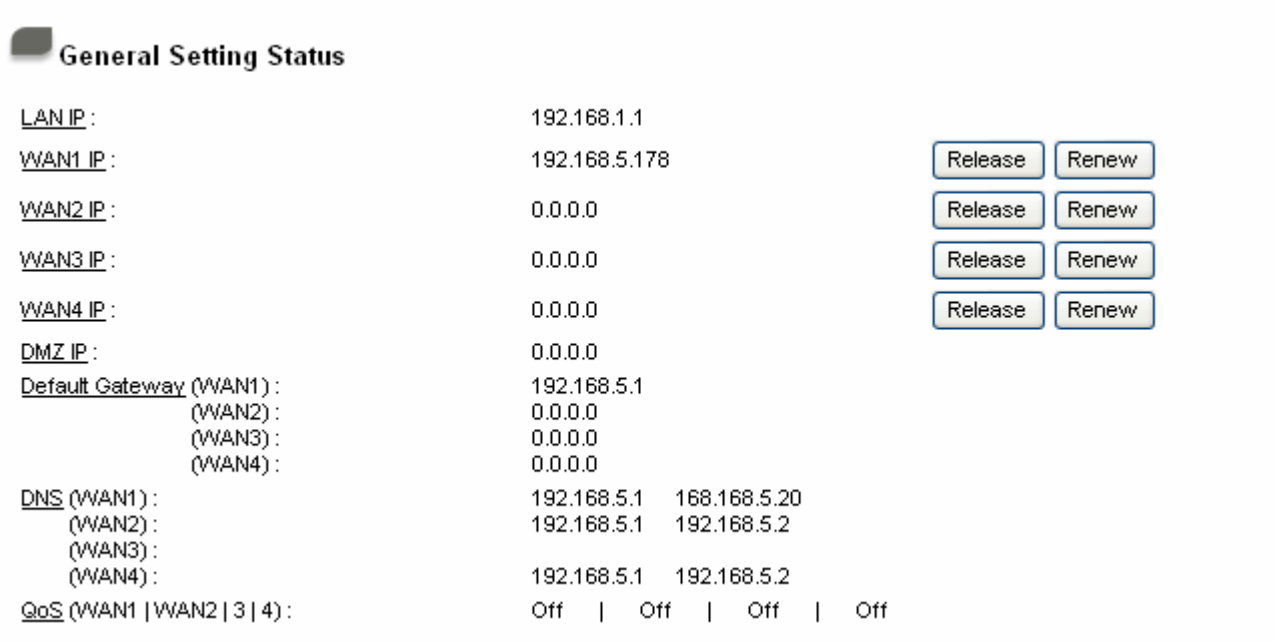
Port ID	1	2	3	4	5	6	7	8
Interface	LAN	LAN	LAN	LAN	LAN	LAN	LAN	LAN
Status	Connected	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Port ID	9	10	11	12	13	14	15	DMZ
Interface	LAN	LAN	LAN	WAN4	WAN3	WAN2	WAN1	DMZ
Status	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Connected	Enabled

在此画面会显示系统各端口(Port)实时状态，包含每一个 Port (Connected-已经连接， Enabled-开启，Disabled-关闭) 。 使用者可以按下此状态按钮，查看各端口更详细的数据显示。 于 **summary** table 总表，会显示目前该端口设定状态，如：网络连接 Link (up or down)， 端口 Port 开启或关闭 Disable(on or off)，高低优先权 Priority (高 High or 一般 Normal)， 连接速率 Speed Status(10Mbps or 100Mbps)， 工作模式 Duplex Status(半双工 half or 全双工 full)， 以太网络自动侦测 Auto negotiation(Enabled or Disabled)。 于此项目表格中(**statistics** table)， 将会显示此端口的接收 receive/传送 transmit 的封包数以及 Byte 数/封包错误率等并计算总数量。


Port 1 Information - Microsoft Internet Explorer
Port1 Information
Summary:
Type
10Base-T / 100Base-TX
Interface
LAN
Link Status
Up
Port Activity
Port Enabled
Priority
Normal
Speed Status
100 Mbps
Duplex Status
Full
Auto negotiation
Enabled
Statistics:
Port Receive Packet Count
155549
Port Receive Packet Byte Count
33804474
Port Transmit Packet Count
229102
Port Transmit Packet Byte Count
246994709
Port Packet Error Count
0
Refresh
Close

General Setting Status(一般设定状态显示)



LAN IP: 此为显示路由器的 LAN 端目前的 IP 位置设定信息，系统预设为 192.168.1.1，并且可以按下该超级链接直接进入该设定项目中。

WAN1~4 IP: 此为显示路由器的 WAN 1 端目前的 IP 位置设定信息，并且可以按下该超级链接直接进入该设定项目中。当使用者选择自动取得 IP 位置时(**Obtain an IP automatically)，** 他会显示二个按钮分别为释放 **-release** 与更新-**renew**。 使用者可以按下释放- **release** 按钮去做释放 ISP 端所核发的 IP 位置，以及按下更新- **renew** 按钮去做更新 ISP 端所核发的 IP 位置。 当选择 WAN 端联机使用如 **PPPoE** 或是 **PPTP** 的话，他会变为显示 连接-Connect 与中断联机-Disconnect。

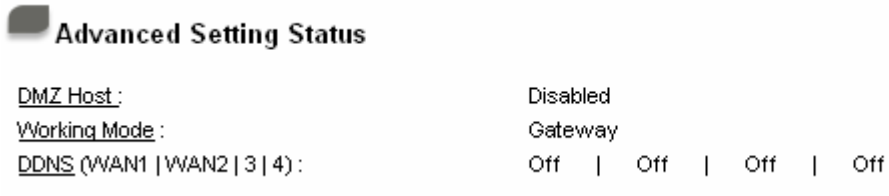
DMZ IP: 此为显示路由器的 DMZ 目前的 IP 位置设定信息，并且可以按下该超级链接直接进入该设定项目中。

Default Gateway: 此为显示路由器的预设网关 IP 位置设定信息，并且可以按下该超级链接直接进入该设定项目中

DNS: 此为显示路由器的 DNS(Domain Name Server)的 IP 位置设定信息，并且可以按下该超级链接直接进入该设定项目中。

QoS: 此为显示路由器的 WAN1~4 是否有使用 QoS，并且可以按下该超级链接直接进入该设定项目中。

Advanced Setting Status(进阶设定状态显示)

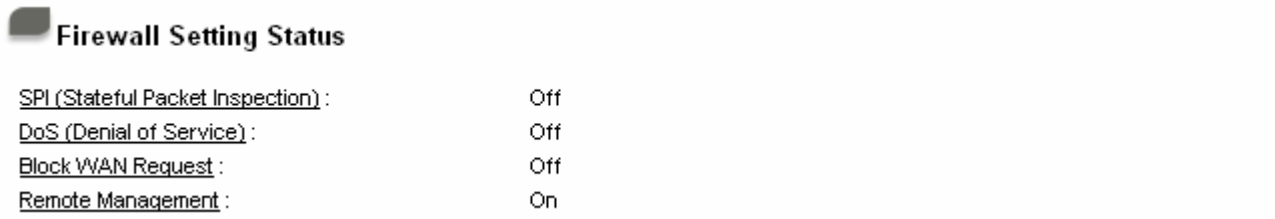


DMZ Host: 此为显示路由器的 DMZ 功能选项是否激活，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭。

Working Mode: 此为显示路由器的目前工作模式(可为 NAT Gateway 或是 Router 路由模式)，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为 NAT Gateway 模式。

DDNS: 此为显示路由器的 DDNS 动态 DNS 功能选项是否激活，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭。

Firewall Setting Status(防火墙设定状态显示)



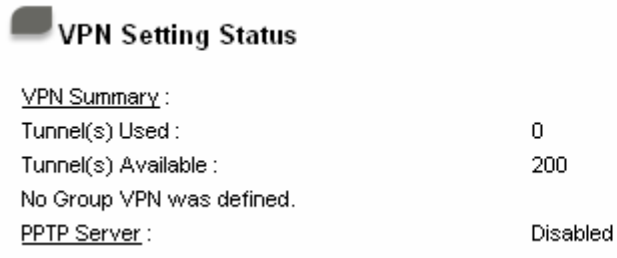
SPI (Stateful Packet Inspection): 此为显示路由器是否开启 SPI(Stateful Packet Inspection)主动封包侦测过滤防火墙功能选项是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭-Off。

DoS (Deny of Service): 此为显示路由器是否阻断来自 Internet 上的 DoS 攻击功能选项，是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭-Off。

Block WAN Request: 此为显示路由器是否阻断来自 Internet 上的 ICMP-Ping 的响应功能选项，是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭-Off。

Remote Management: 此为显示路由器的远程管理功能选项是否激活(开启-On/关闭-Off)，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭-Off。

VPN Setting Status(VPN 设定状态显示)



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

Tunnel(s) Used: 此为显示路由器的 VPN 功能目前已经设定的 Tunnel 数量。

Tunnel(s) Available: 此为显示路由器的 VPN 功能目前可使用的 Tunnel 数量。

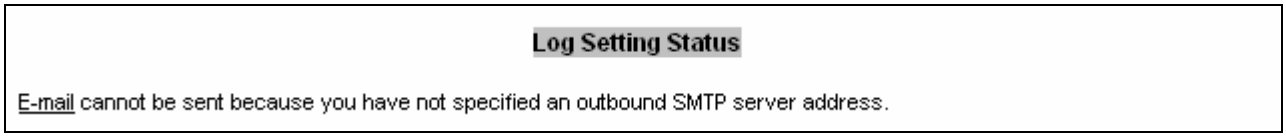
Current Connected (The Group Name of GroupVPN1) users: 为显示路由器的 VPN 1 目前线上使用 Tunnel

数量。

Current Connected (The Group Name of GroupVPN2) users: 为显示路由器的 VPN 2 目前线上使用 Tunnel 数量。

若是 GroupVPN 为无设置的状态，会显示“No Group VPN was defined。”没有 GroupVPN 被设定的信息。

Log Setting Status: (系统日志设定状态显示)



E-Mail 的超级链接将会连到系统日志设定画面中:

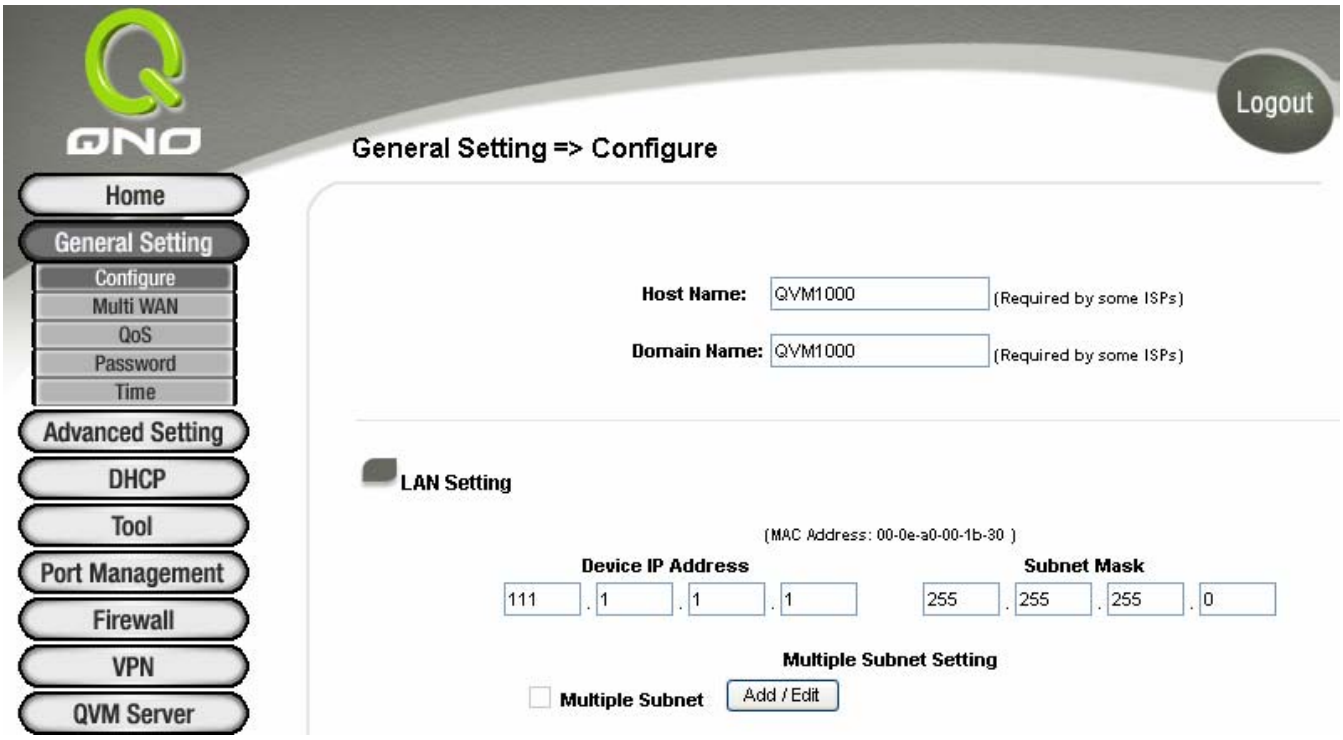
1.若您无设定电子邮件服务器(Mail Server)于系统日志设定中(Log page)， 将显示您无设定电子邮件服务器所以无法发送系统日志电子邮件-“E-mail cannot be sent because you have not specified an outbound SMTP server address。”

2.若您已经设定电子邮件服务器(Mail Server)于系统日志设定中(Log page)， 但是 Log 尚未达到设定传送的条件时，它将显示电子邮件服务器已经设置-“E-mail settings have been configured。”

3.若您已经设定电子邮件服务器(Mail Server)于系统日志设定中(Log page)， Log 也已经传送出去时，它将显示电子邮件服务器已经设置，并且已经发送- “E-mail settings have been configured and sent out normally。”

4.若您已经设定电子邮件服务器(Mail Server)于系统日志设定中(Log page)， 但是 Log 无法正确传送出去时，它将显示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-“E-mail cannot be sent out，probably use incorrect settings。”

General Setting: 一般项目设定



此一般项目设定-General Setting 画面为 QVM1000 防火墙路由器为基本的设定内容。 对大多数的用户来说，此预设的项目已经足够连接网际网络而不需做任何变更。 当然有些情况下使用者需要一些 ISP 所提供的进一步详细信息。其详细设定，请参考以下各节说明:

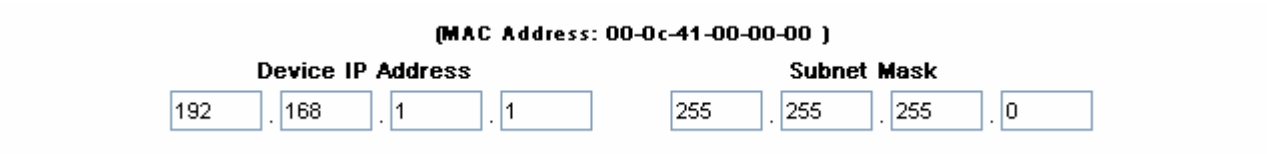
Configure-设定

Configure

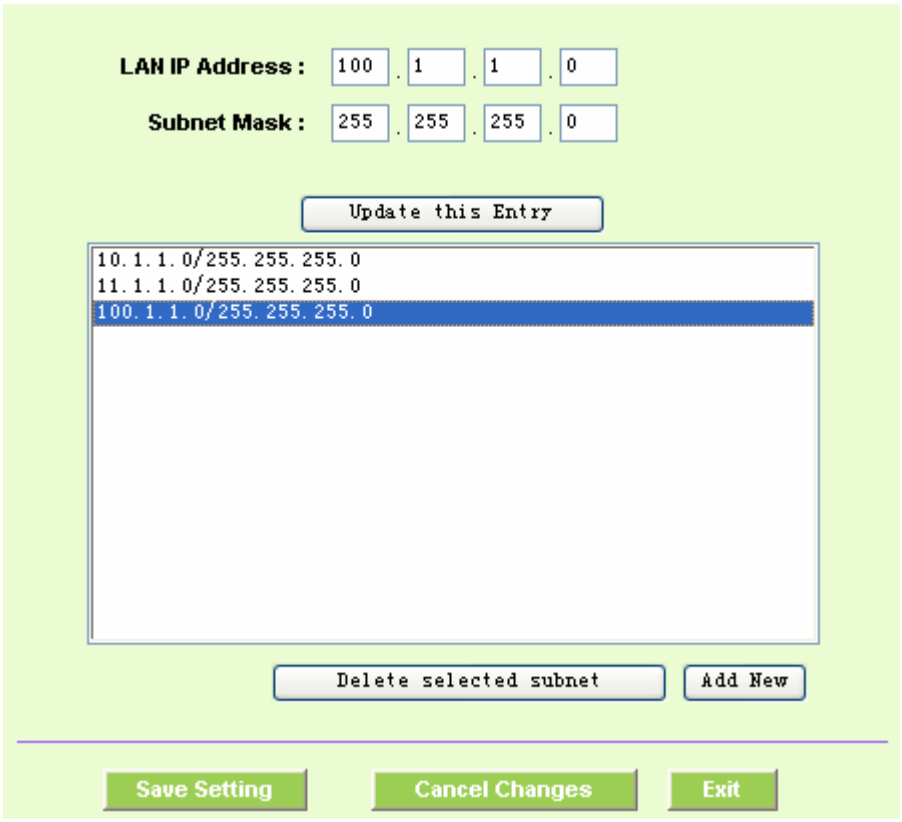
Host Name & **Domain Name**: 可输入路由器的名称-Host name 以及网域名称-Domain Name，于大多数的环境中不需做任何设定即可使用，国外有一些 ISP 可能需要用到！

LAN Setting

此为显示路由器的 LAN 端内部网络目前的 IP 位置设定信息，系统预设为 192.168.1.1，子网掩码为 255.255.255.0，可以依照您实际网络架构更动！

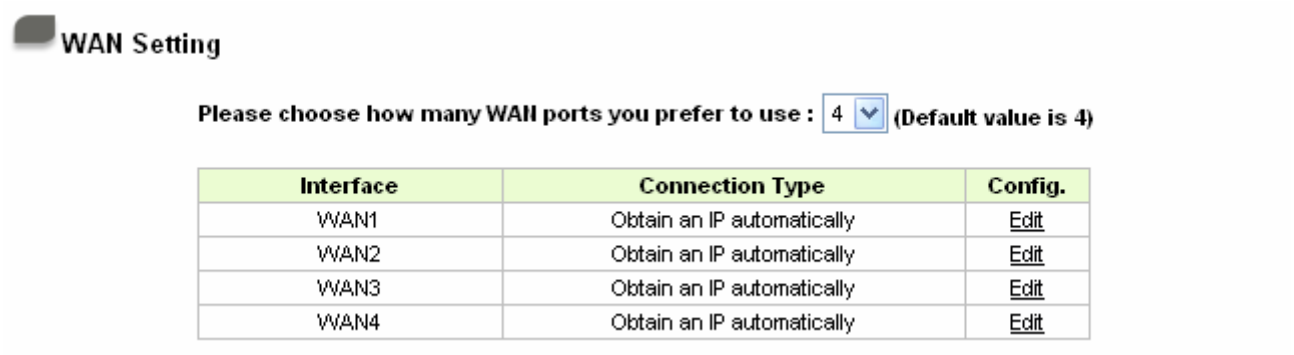


Multiple-Subnet Setting



此功能提供 User 可以将不同于路由器网段的 IP 群组填入到 Multiple-Subnet 后就可直接上网，也就是若原来内部环境已经有多组不同 IP 群组时，内部计算机不需做任何修改就可以上网，可以依照您实际网络架构更动！

WAN Setting

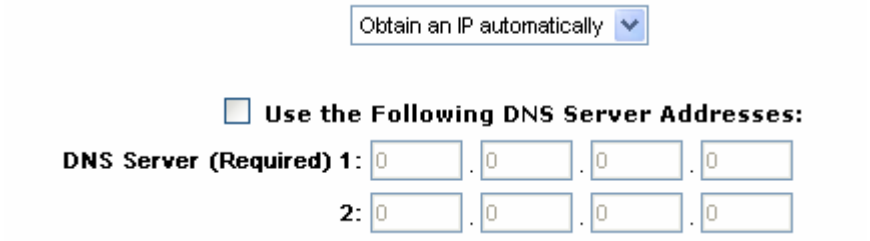


Please choose how many WAN ports you prefer to use	请选择您要设定 WAN 端口的数目，默认值为 4。您可以依照自己的需要加以更改。
Interface:	显示为第几个 WAN 端口
Connection Type	广域网络 Internet 联机型态设定:可以区分为四种。 Obtain an IP automatically:自动取得 IP 位置; Static IP: 固定 IP 位置联机; PPPoE (Point-to-Point Protocol over Ethernet):PPPoE 拨号联机; PPTP (Point-to-Point Tunneling Protocol): PPTP 拨号联机
Config。:	显示进一步更改设定:点选 Edit 进入近一步设定画面。

WAN Connection Type:广域网络 Internet 联机型态设定

Obtain an IP automatically:自动取得 IP 位置(常用在缆线调制解调器 Cable Modem 或是 DHCP 自动取得 IP 联机型态上)

此为路由器系统预设的联机方式，此联机方式为 DHCP Client 自动取得 IP 模式，多为应用于如 Cable Modem 等连接，若您的联机为其它不同的方式，请依照以下介绍并选取相关的设定。或是使用者自订 DNS 的 IP 位置(Use the Following DNS Server Address)，与此选项勾选并自订填入 DNS 的 IP 位置。

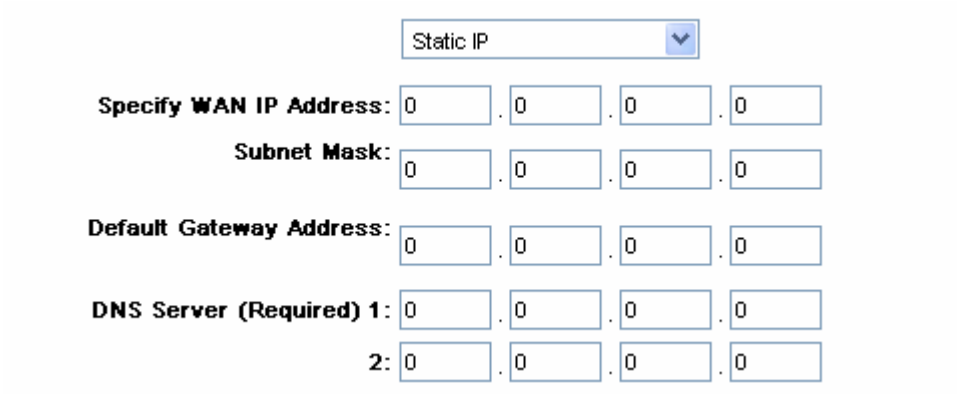


Use the Following DNS Server Address:	选择使用自订的 DNS 解析服务器的 IP 位置。
Domain Name Server (DNS): 解析服务器	输入您的 ISP 所规定的名称解析服务器 IP 位置，最少填入一组，最多可填二组。

Static IP: 固定 IP 位置联机

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

Notes:请注意，有一些 ISP 虽会提供固定如一个 IP 位置给您，但是有可能是使用如 DHCP 自动取得 IP 或是 PPPoE 拨接取得一个固定 IP 模式，虽是每次都取得相同 IP 位置，但联机模式您依然要选择相关之模式才可！

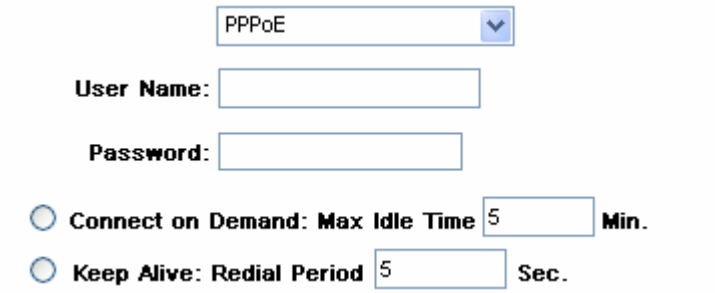


Specify WAN IP Address:	输入您的 ISP 所核发的可使用固定 IP 位置
Subnet Mask:	输入您的 ISP 所核发的可使用固定 IP 位置的子网掩码，如: 发放 8 个固定 IP 位置:255.255.255.248 发放 16 个固定 IP 位置:255.255.255.240
Default Gateway IP Address:	输入您的 ISP 所核发的预设网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 位置，若是使用光纤接入请填光纤转换器 IP。
Domain Name Server (DNS):	输入您的 ISP 所规定的域名解析服务器 IP 位置，最少填入一组，最多可填二组。

PPPoE (Point-to-Point Protocol over Ethernet):PPPoE 拨号联机

此项为 ADSL 计时制使用(适用于 ADSL PPPoE)，填入 ISP 给予的使用者联机名称与密码并以路由器内建的

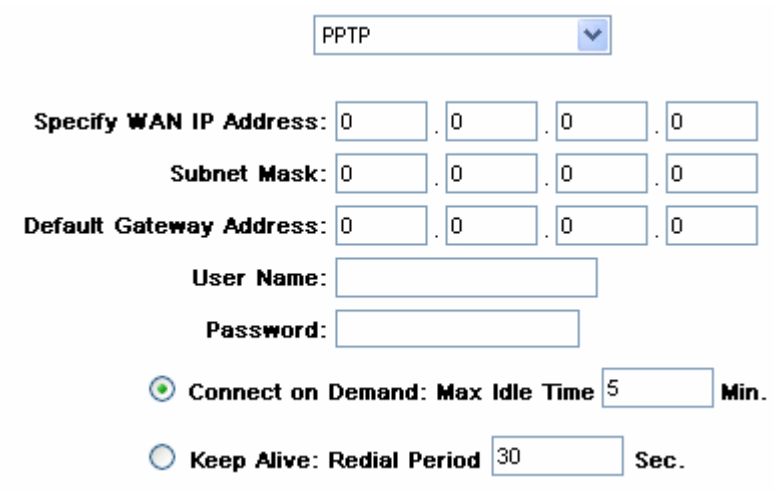
PPP Over –Ethernet 软件联机，若是您的 PC 之前已经有安装由 ISP 所给予的 PPPoE 拨号软件的话，请将其移除，不需要再使用这些软件连接网络。



User Name:	输入您的 ISP 所核发的使用者名称
Password:	输入您的 ISP 所核发的使用密码
Connect-on-demand:	此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，QVM1000 会自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线(自动离线无封包传送时间预设为 5 分钟)。
Keep Alive:	此功能能够让您的 PPPoE 拨接连线能够保持联线，且断线后会自动重拨，并且可以依使用者使用方式自行设定重新拨接的时间，预设为 30 秒。

PPTP (Point-to-Point Tunneling Protocol): PPTP 拨号联机

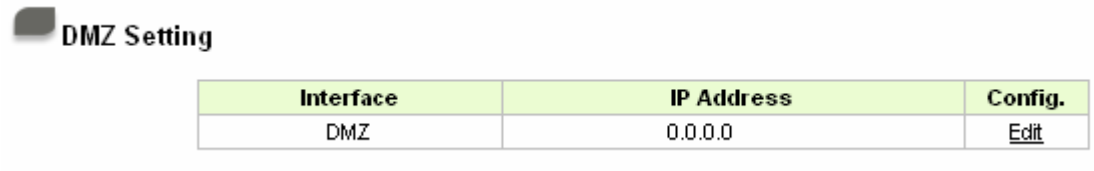
此项为 PPTP (Point to Point Tunneling Protocol) 计时制使用，填入 ISP 给予的使用者联机名称与密码并以 QVM1000 内建的 PPTP 软件联机，(多为欧洲国家使用)



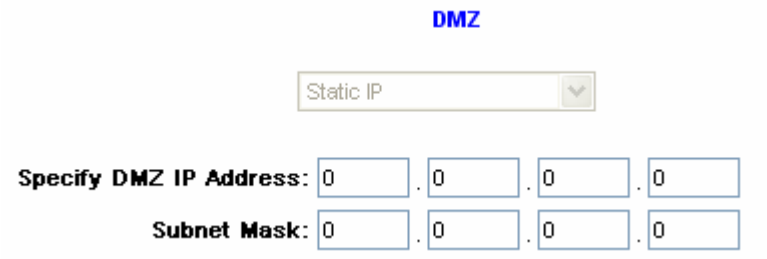
Specify WAN IP Address:	此项为设定固定 IP Address，设定的 IP 可由您的 ISP 所提供的位置输入（此 IP 位置各 ISP 都于装机后给予，请询问您的 ISP 给予相关信息）
Subnet Mask:	如上将 ISP 的子网掩码地址资料填入
Default Gateway Address:	输入您的 ISP 所核发的可使用固定 IP 位置的预设网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 位置。
User Name:	输入您的 ISP 所核发的使用者名称
Password:	输入您的 ISP 所核发的使用密码
Connect-on-demand:	此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，QVM1000 会自动向预设的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线(自动离线无封包传送时间预设为 5 分钟)。
Keep Alive:	此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设定重新拨接的时间，预设为 30 秒。

DMZ Setting

于某些网络环境应用来说，您可能会需要用到独立的 DMZ 非军事管制区接口来置放您的对外服务器，如 WEB 与 Mail 服务器等; QVM1000 提供一组独立的 DMZ 接口来设定连接合法 IP 位置的服务器。此 DMZ 接口为连接 Internet 与局域网络之间的沟通桥梁。



Interface:	显示为 DMZ 埠口
IP Address:	显示目前预设的固定 IP 位置。
Config。	显示进一步更改设定:点选 Edit 进入近一步设定画面。



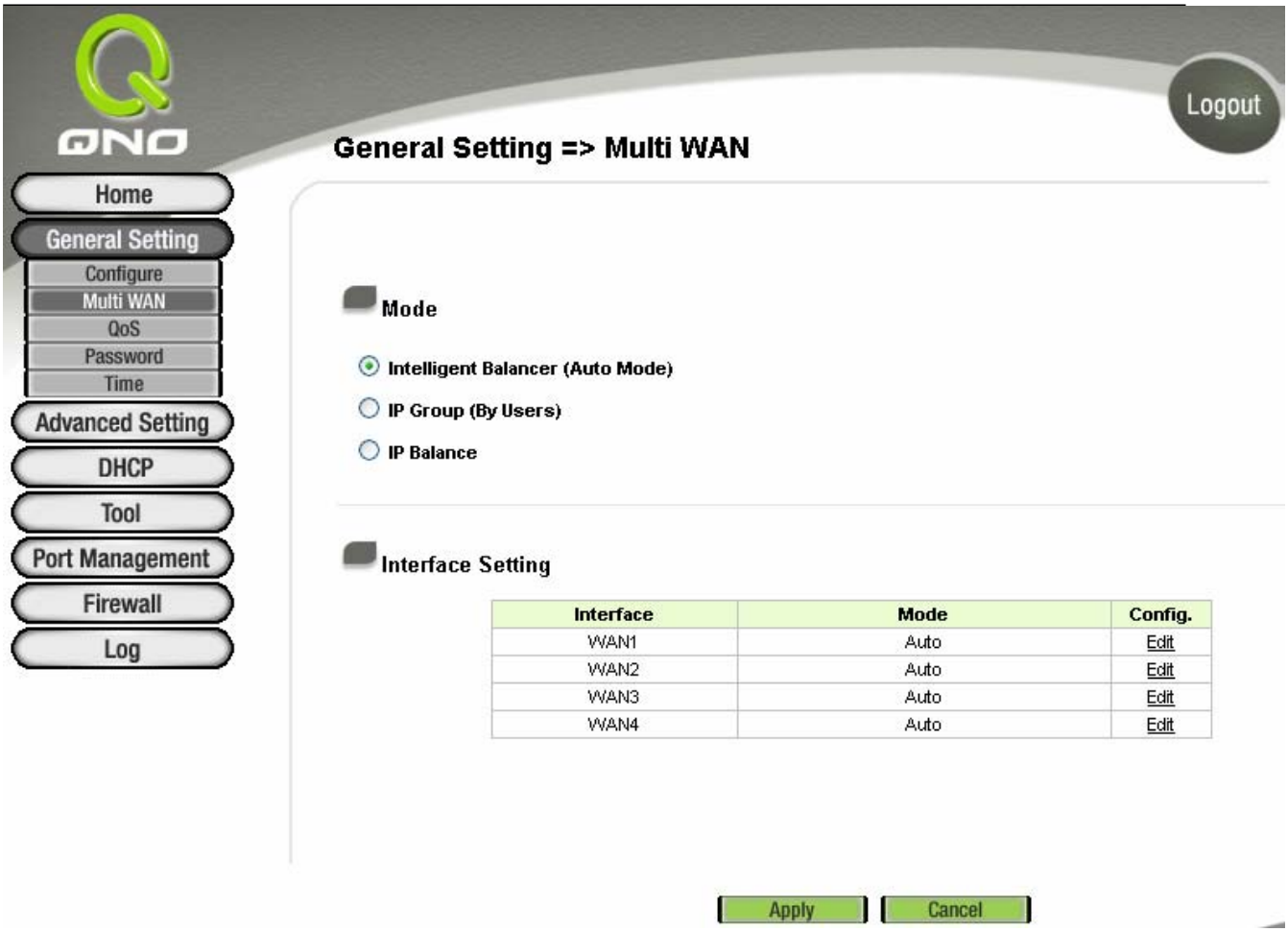
Specify DMZ IP Address: 请输入 DMZ 接口的 IP 位置信息以及子网掩码。

Multi WAN-多 WAN Port 设定

于多 WAN 的运作模式当中，提供了使用者三种模式选择，分别为 **–全自动型的负载平衡模式 Intelligent Banancer(Auto Mode)**以及 **特定使用者的 IP 群体模式 IP Group (By Users)还有 IP 负载均衡 IP Balance。**

全自动型的负载平衡模式 Intelligent Banancer(Auto Mode)的情况下

系统会自动整合 WAN1 到 WAN4 四条线路最大带宽做最佳的负载平衡。



Mode:

全自动型的负载平衡模式: Intelligent Balancer (Auto Mode)

此模式主要是让路由器自行做每一条 WAN 的频宽自动负载均衡

IP 负载均衡（IP Balance）:

此为最传统的负载均衡，若选择此方式，则路由器会依照内网计算机上网的顺序依次分配一条 WAN 使用。

Interface Setting 可选择所需要进一步设定的接口。

Interface 显示出广域网络端口的数目。

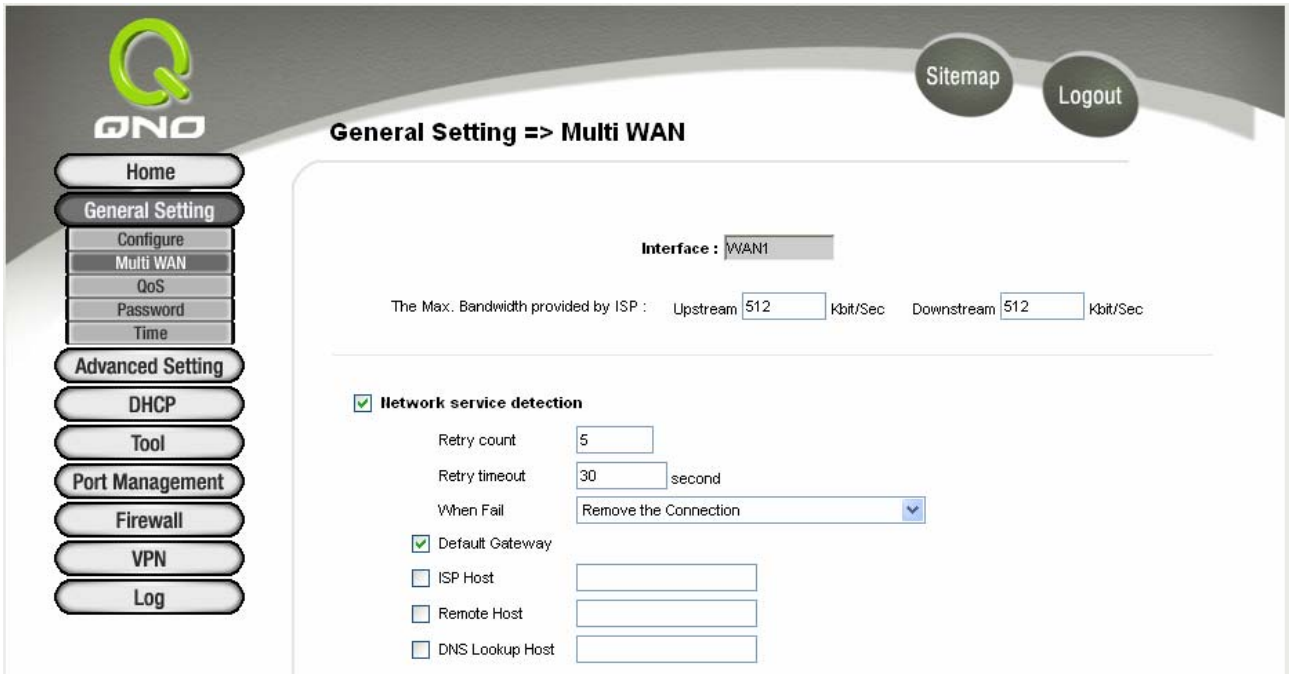
Mode 在选择完 Auto 后，其显示的结果在**全自动型的负载平衡模式** Intelligent Balancer (Auto Mode)的情况之下，会自动显示出自动分配带宽。

Config。 可经由点选 Edit 进行进一步的设定。

Apply 按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。。

Cancel 按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Multi-WAN Config setting



Interface: 显示现在所要设定的广域网络端口。

The Max。 Bandwidth provided by ISP: 需填入此条广域端口实际支持的上传(Upstream)及下载(Downstream)的实际 ISP 带宽。其范围介于 0~100Mbits 之间

Network Services Detection: 网络对外服务侦测机制。若勾选此项设定，则会出现 Retry Count，Retry Timeout..等以下的讯息。

Retry Count: 对外联机侦测重试次数，默认值为五次。若是于此测试次数当中，Internet 没有响应的话，路由器会判断此条广域端口对外线路中断！

Retry Timeout: 对外联机侦测逾时时间(秒)，默认值为 30 秒。若是于此秒数当中，你所设定的针测点没有响应的话， 路由器会判断此条广域网对外线路中断。

When Fail

(1)Generate the Error Condition in the System Log:在系统日志中会产生错误讯息的信息: 当侦测到与 ISP 连结失败时，系统就会在系统日志中将这项错误讯息纪录下来，但**依旧保持此线路不会移除**，所以会有些原来在此条线路上的 User 无法正常使用。

(2)Remove the Connection 移除有问题线路: 当侦测到与 ISP 连结失败时，系统不会在系统日志中将这项错误讯息纪录下来。原本在此 WAN 端的封包传递会自动转换到另一条广域端口。等到原本断线的广域端口恢复后会自行重新连结，则封包传递会自动转换回来。

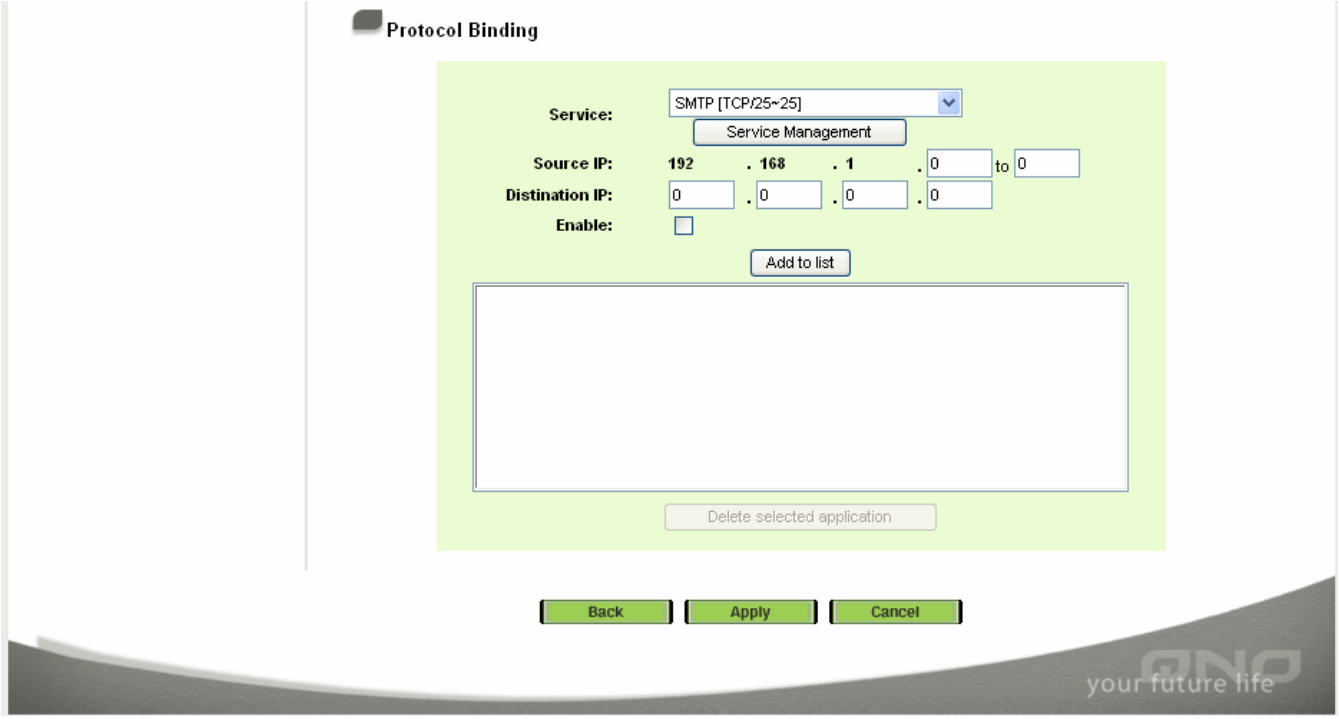
Default Gateway: 预设网关位置，如 ADSL 或缆线调制解调器及光纤转换器的 IP 位置

ISP Host: 将此字段填入 ISP 端的 DNS 解析服务器，填入前请确定此 DNS 是会做响应。 ISP 端的侦测位置，如 ISP 的 DNS IP 位置等，在设定此 IP 地址时请确认此 IP 地址是可以且稳定快速的得到响应。 (建议填入

ISP 端 DNS IP)

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

DNS Lookup Host: 网域名称端 DNS 的侦测位置网域名称端 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**。



Protocol Binding-协议绑定

它提供使用者可将特定的 IP 或特定的应用服务端口（Service port）经由您限定的 WAN 出去。

Service: 在此选择欲开启的绑定服务端口 Service Port
预设列表(如 All(TCP&UDP)0-65535)，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表！预设的 Service 为 SMTP。

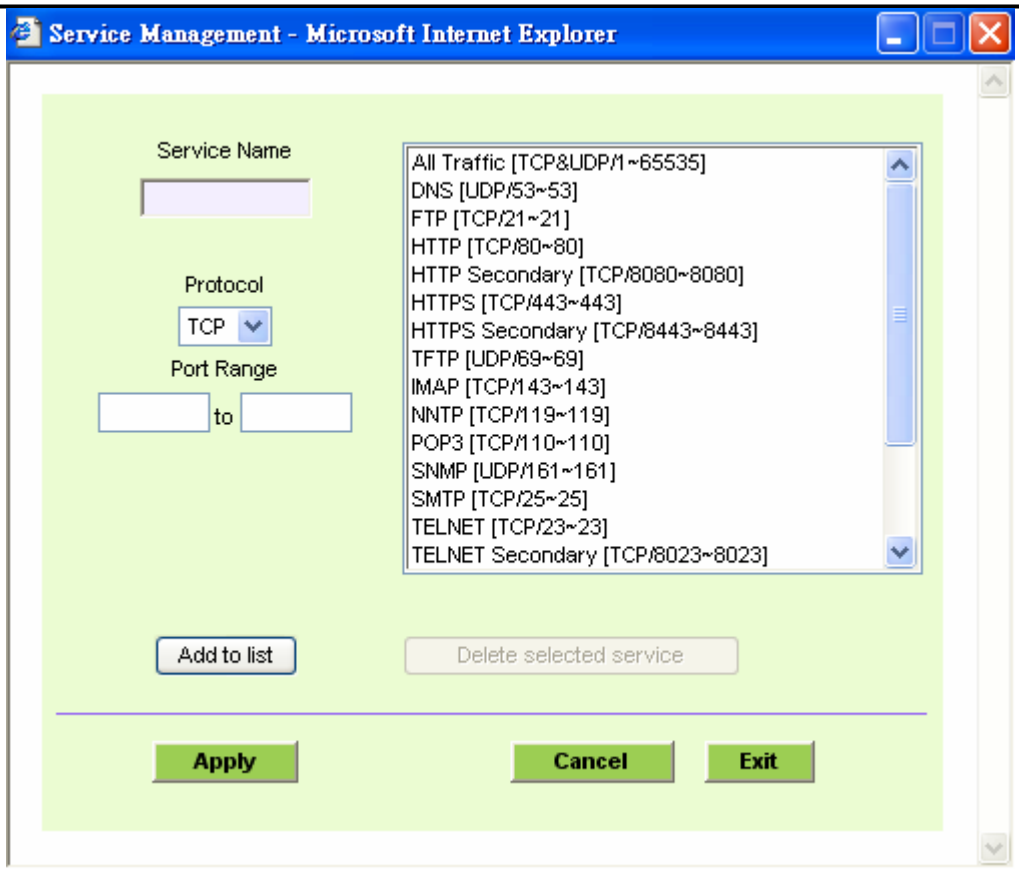
Source IP: 使用者可以绑定特定的内部虚拟 IP 位置的封包经由特定的广域端口出去。在此填上的内部虚拟 IP 位置范围，例如 192.168.1.100 到 150。则 IP 地址 100 到 150 为绑定范围， 如果使用者只需要设定特定的 Service Port 而不需设定特定的 IP 的话， 则在 IP 的字段皆填入 0，另外此 Source IP 是可以控制到 Class B 的范围。

Destination IP: 在此填上的外部固定 IP 位置，例如若有一目标地址 210.11.1.1 使用者限定只能从广域端口 1 到达此目标地址。则在此填上的外部固定 IP 位置 210.11.1.1 to 210.11.1.1。如果使用者要设定一个范围的目

	的地为置，则填入方式可以为 210.11.1.1 to 210.11.255.254，则表示整组 210.11.x.x 的 Class B 网段都限制走某一条广域网，若只需要设定特定的应用而不需设定特定的 IP 的话，则在 IP 的字段皆填入 0.0.0.0。
Enable:	开启此条服务功能
Add to list:	新增此条管理服务至列表
Delete selected application:	从列表上删除此条管理服务
Back:	按下此按钮”Back”即会回到上一页
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

以上服务表列的 Service port，为一些较常使用的项目，若您预开启的项目没有在表列中，您可以使用 **Services Management:** 新增管理服务端口号列表功能达成，如以下所述:

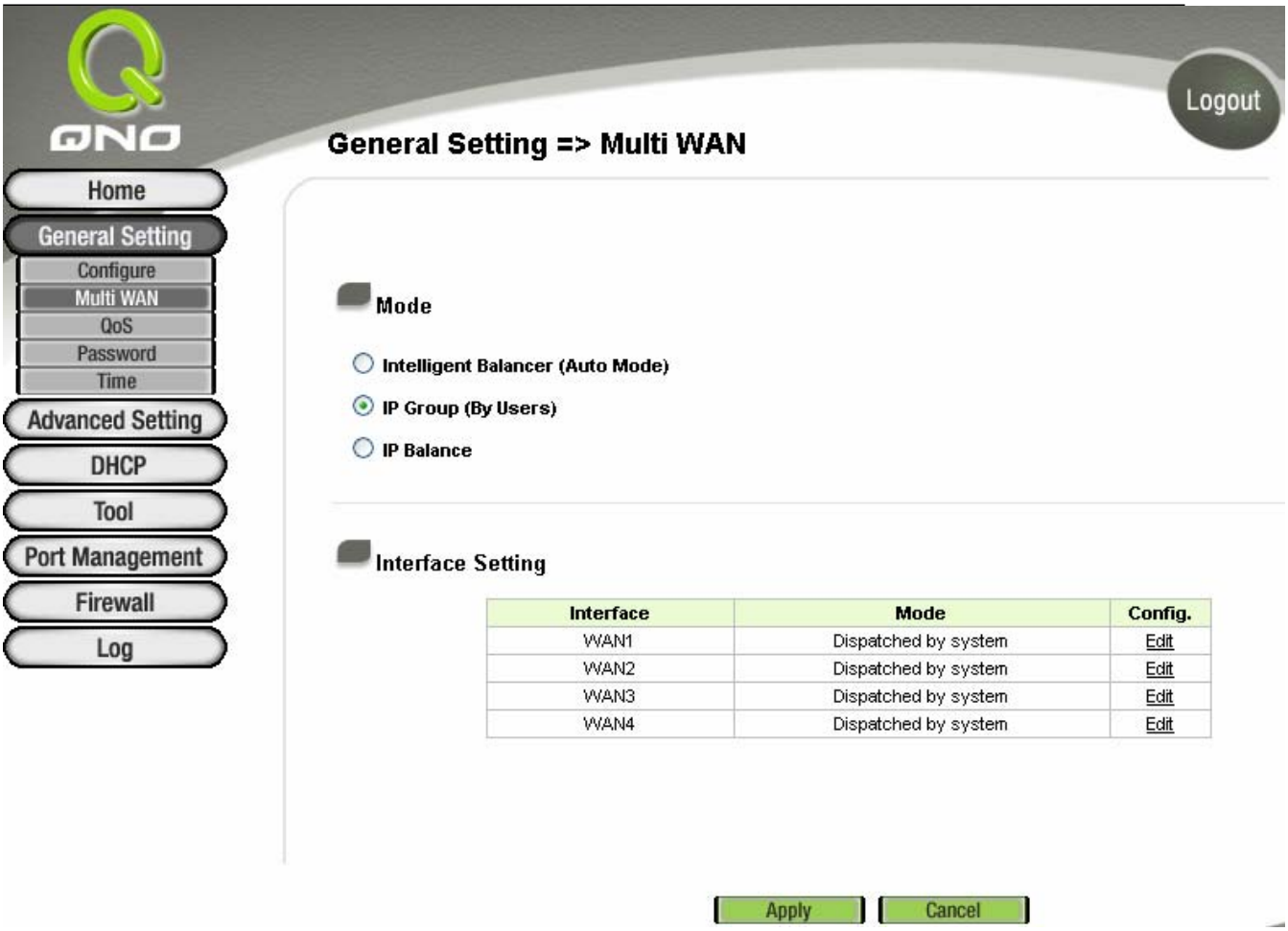
Services Name:	在此自订选择欲开启的服务埠号名称加入列表中，如 Edonky 等
Protocol:	选择所需管理的 Service port 为 TCP or UDP 封包。
Port Range:	在此填上欲开启的服务端口号的位置范围，如 TCP/500~500 或是 UDP/2300~2310 等。
Add to List:	增加到开启服务项目内容列表，最多可新增 30 组。
Delete Selected Services:	删除所选择的服务项目。
Apply	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效。
Exit:	离开此功能设定画面。



使用者的 IP 群组模式 IP Group (By Users)

管理者可设定"使用者的 IP 群组"， 以提供分级服务或指定某些 IP 或 Service Port 只能用那一条 WAN 进出，且一经选择指定后此条 WAN 也**只能**提供给这几个 IP 或 Service Port 使用。管理者可将特定的 WAN 限定给"特定使用者的 IP 群组"使用，不用与其它非"特定使用者的 IP 群组"使用者分享带宽，可享有较优的分级服务。若特定的 IP 使用者仅选择特定的服务时，则其它的服务会经由其余的广域网络端口传送。

广域端口 WAN 1 预设是保留做为非 IP 群体使用，也就是所有未设定在 WAN2-WAN4 的 IP 或 Service Port 都会自动经由此端口进出，**广域端口** WAN2~4 则作为特定使用者使用。



Mode: **特定使用者的 IP 群体模式 IP Group (By Users) :**

此模式主要是将某一条 WAN 2 到 WAN 4 指定给某些 IP 或 Service Port 单独使用，当此 WAN 被设定后，只有设定的 IP 或 Service Port 可以使用此条 WAN，另外，WAN1 是无法做指定的，以避免 WAN2-4 都被设定后，其余未被绑定的 IP 或 Service Port 有一条 WAN 可使用。

Interface Setting: 选择要进一步设定的接口。

Interface: 显示出广域网络端口的数目，默认值为四个。

Mode: 在预设的情况下，WAN1 是给非指定到 WAN2 到 WAN4 的 IP 及 Service Port 所使用。WAN2~4 可以加以设定，若没有设定会显示出由系统自行分配 Dispatched by system，也就是会跟 WAN1 由 Router 自己做 Load Balance。

Config。 可经由点选 Edit 进行进一步的设定。

Apply 按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。。

Cancel 按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Interface: 显示为第几个 WAN 埠口。在预设的情况 WAN2~4 是可以做为**特定使用者的 IP 群体模式 IP Group (By Users)**

The Max。 Bandwidth provided by ISP:: 需手动填入此条广域端口所能支持的上传(Upstream)及下载(Downstream)的网络流量。其范围介于 0~100Mbits 之间

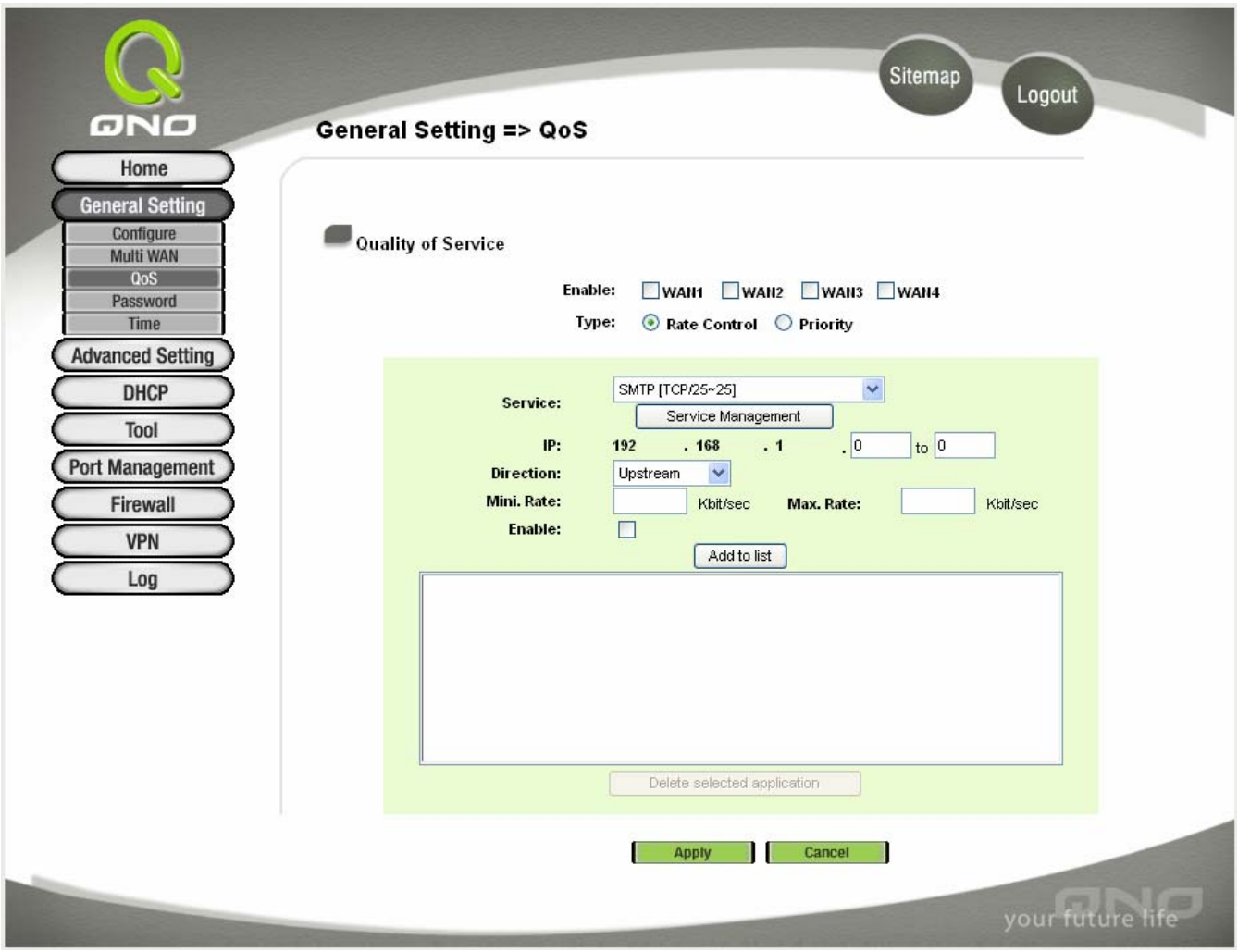
Network Service detection **在全自动型的负载平衡模式 Intelligent Banancer(Auto Mode)已经有详细介绍过。使用者可以回到全自动型的负载平衡模式中观看。**

QoS

QVM1000 让使用者可以在特定的广域网络端口上，提供流量速度控制（Rate Control）或者是服务优先性（Priority）两种服务质量 QoS 的设定类型，以满足特定使用者的带宽需求。使用者在此只能够在这两种设定类型选择其中的一种作带宽服务质量 QoS。

在 Rate Control 的情况下

QVM1000 可以针对特定的广域端口(WAN1-WAN4)提供针对设定 IP 或设定 Service port 的上下传带宽控制服务，以保障宽带需求，用来传送重要的信息封包。

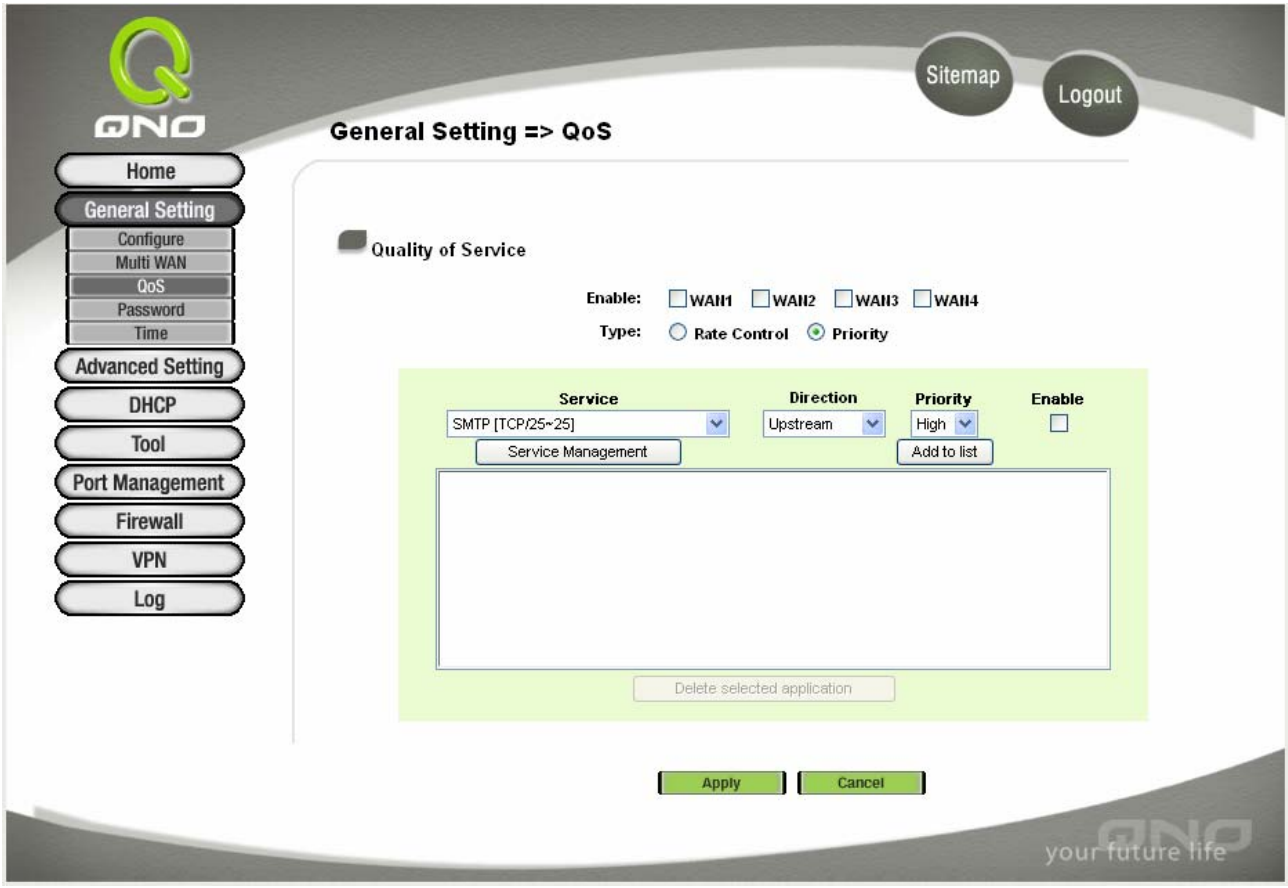


Enable:	激活选择要执行此 QoS 限制的广域网端口
Type:	点选流量速度控制 Rate Control
Services:	在此选择限定的服务端口 Service Port:(如 All(TCP&UDP)0-65535)，如 WWW 为 80(80~80)，FTP 为 21~21，可参考服务号码预设列表！。预设的 Service 为 SMTP。

Services Management:	新增或删除管理服务端口号列表
Direction:	选择上传 uplink 或下载 down link 的限制服务
Minimum Rate (Min。Rate):	在此填入保证或最低的带宽。例如:填入 15，系统自动会保证这项服务至少有 15 Kbps 的带宽保证
Maximum Rate (Max。Rate):	在此填入最高的带宽。例如:填入 700，系统自动会保证这项服务不会超过 700 Kbps 的带宽
Enable:	开启此服务功能
Add to List:	增加到开启服务项目内容列表。
Delete Selected Services:	删除所选择的服务项目。
Apply	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

在服务优先性 Priority 的情况下

QVM1000 可以针对特定的广域端口。保证在提供特定的服务时，可以区分成高，低的优先级，来传送重要的信息封包，其默认值为高优先级。

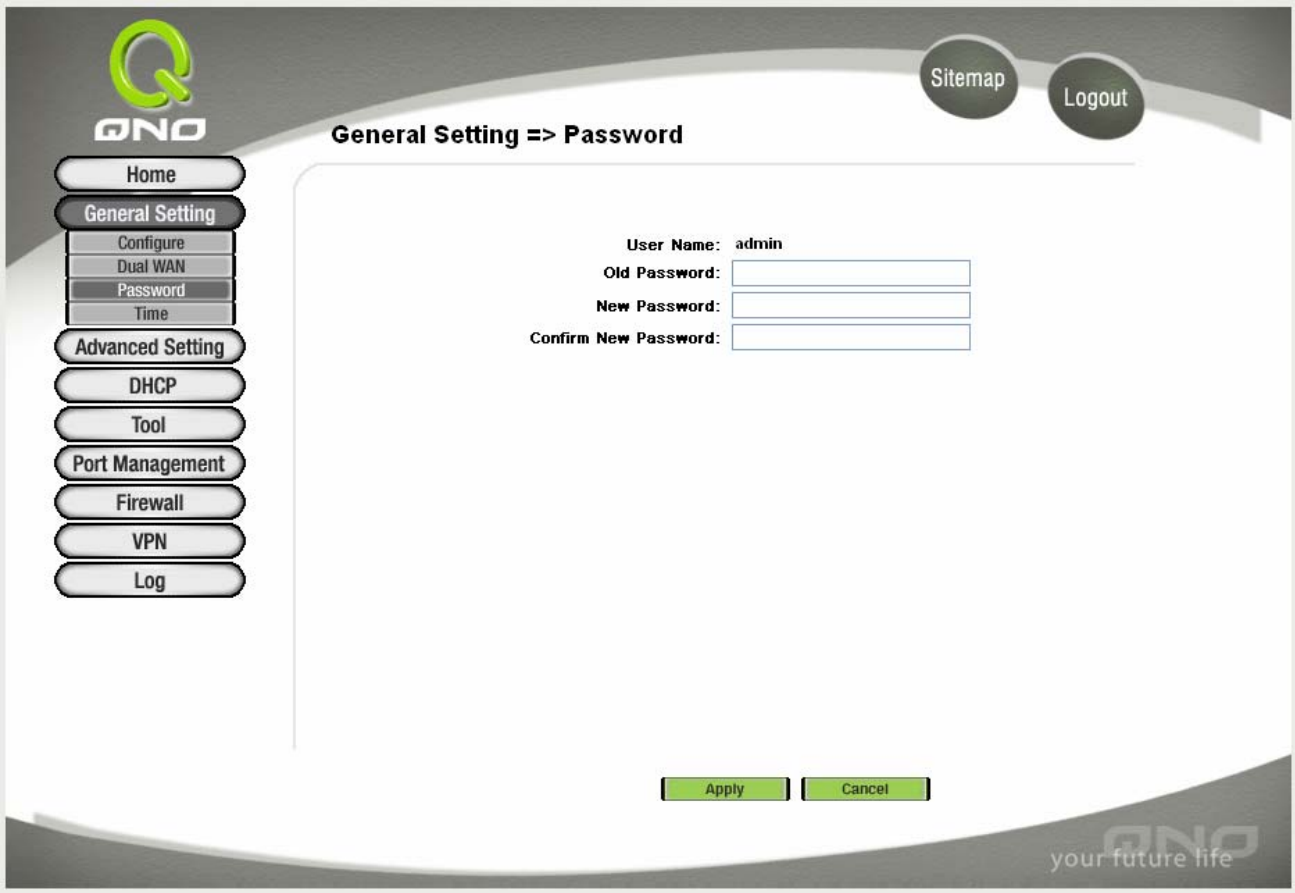


Enable:	激活选择要执行此 QoS 的广域网络端口
Type:	点选**服务优先性 Priority**
Services:	在此选择欲开启的虚拟主机的服务号码预设列表(如 All(TCP&UDP)0-65535)，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表!。
Services Management:	新增或删除管理服务端口号列表
Direction:	选择上传 uplink 或下载 down link。
Priority:	在选择服务的优先级时，使用者可以选择高优先级 High(60%) 与低优先级 Low(10%) 两种。其余部份则为中优先级(30%)。在列表中高优先级的全部服务会均分系统 60%的带宽。低优先级的全部服务会均分系统 10%的带宽。其余中优先级的全部服务则均分 30%的带宽。
Add to List:	增加到开启服务项目内容列表。
Enable:	开启此服务功能。
Delete Selected application:	删除所选择的服务项目。
Apply	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。

Cancel	按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Password

本功能设定多为 QVM1000 的进阶管理项目- 管理者密码设定，本机使用密码出厂值为“admin”，您可当设定完成后修改此一存取密码，但是记得设定完成后 Apply。



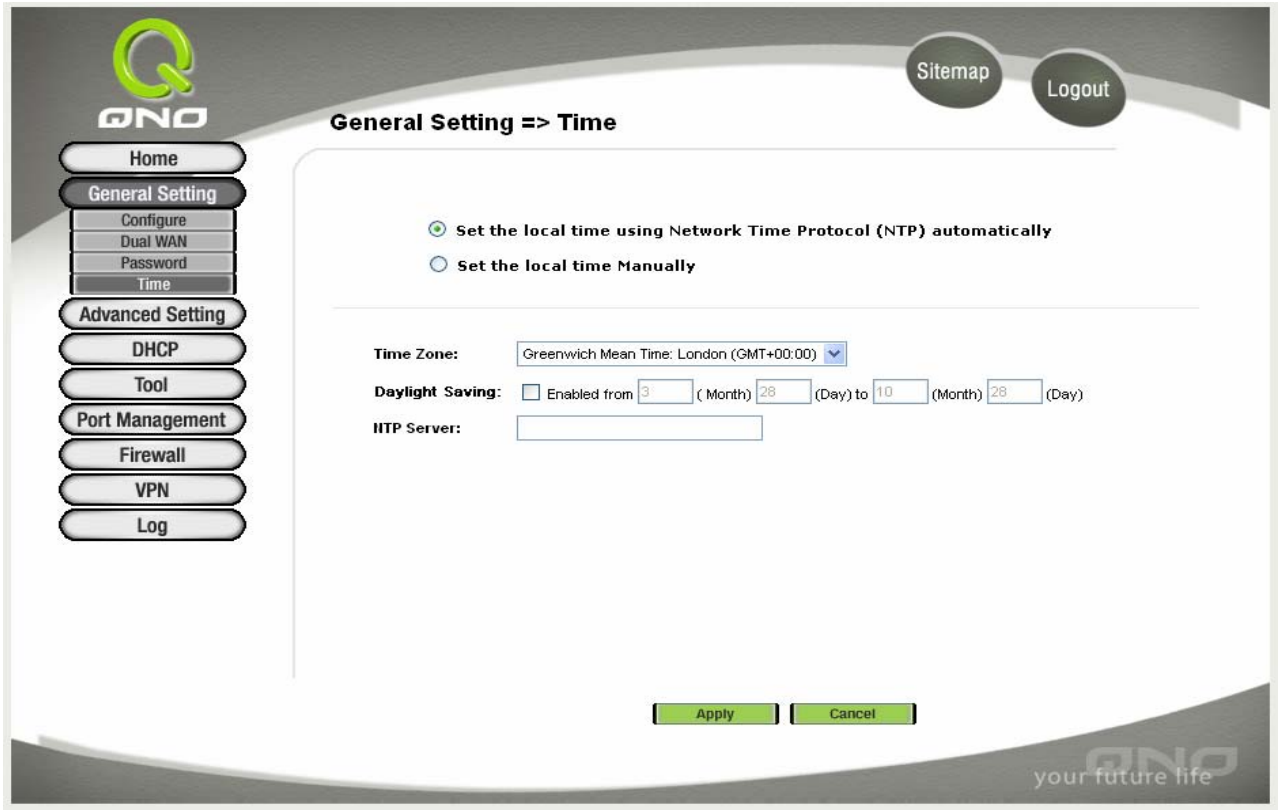
User Name:	预设为 admin
Old Password:	填写原本旧密码
New Password:	填写所更改密码
Confirm New Password:	再填写确认一次更改密码
Apply	按下此按钮"Apply"即会储存刚才所变动的修改设定内容参数。。
Cancel	按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Time-系统时间设定

QVM1000 使用了正确的时间计算功能，您可以选择与 QVM1000 内建的外部时间同步服务器(NTP Server)或是自己设定正确时间参数，此项参数设置可以让您在看 QVM1000 的系统纪录或是设置网络存取时间功能时，可以准确的知道事件所发生时间，以及关闭存取或是开放存取 Internet 资源的依据条件。

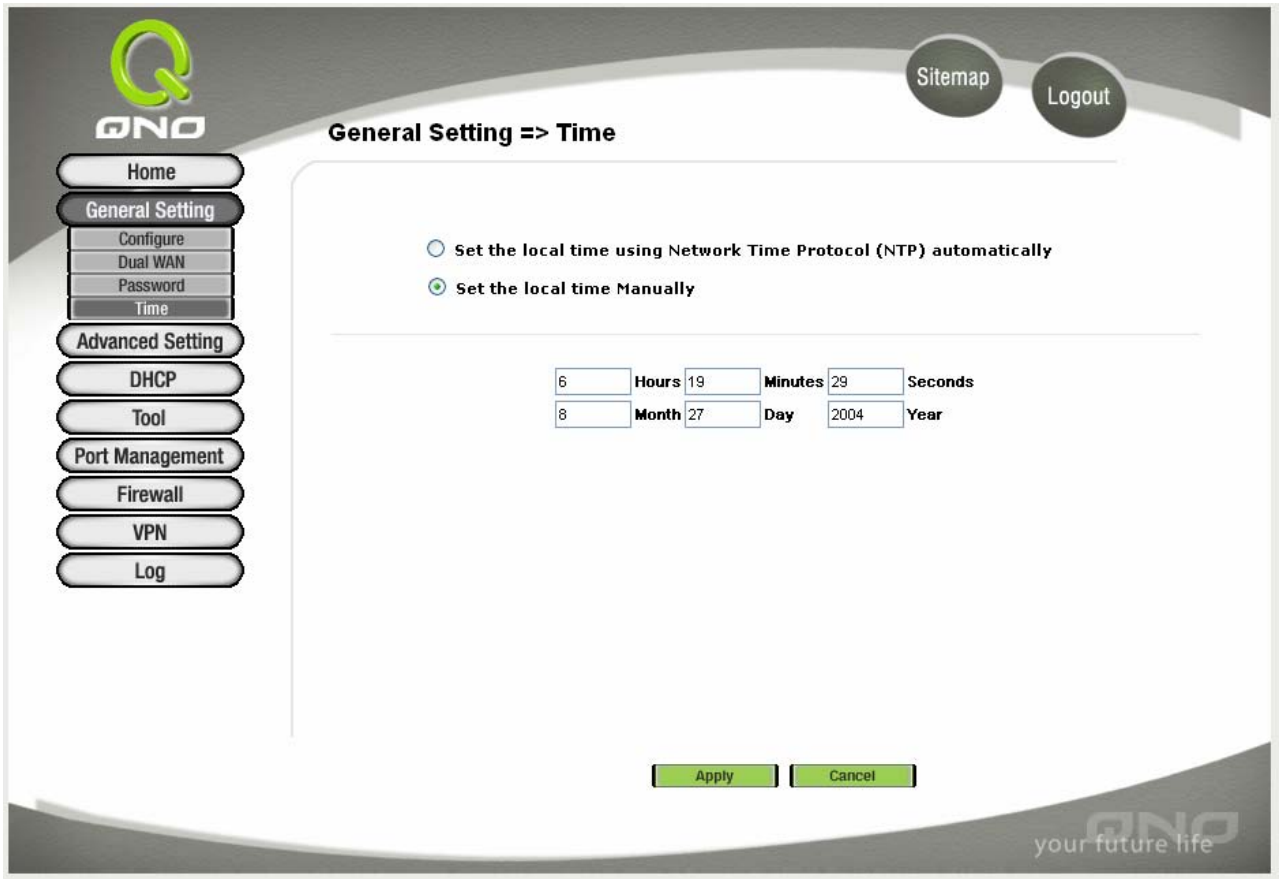
Automatically:设定自动与网络上的 NTP 服务器同步时间

请于 Time Zone 选项选择您所在区域的时间参数以及日照时间，或是您有专属使用的时间同步服务器(NTP Server)的话，您可以输入此时间同步服务器的 IP 位置。



Manually:手动输入日期时间参数

于此输入正确的小时(Hours)， 分钟(Minutes)， 秒(Seconds)， 月份(Month)， 日(Day) 与年(Year)。

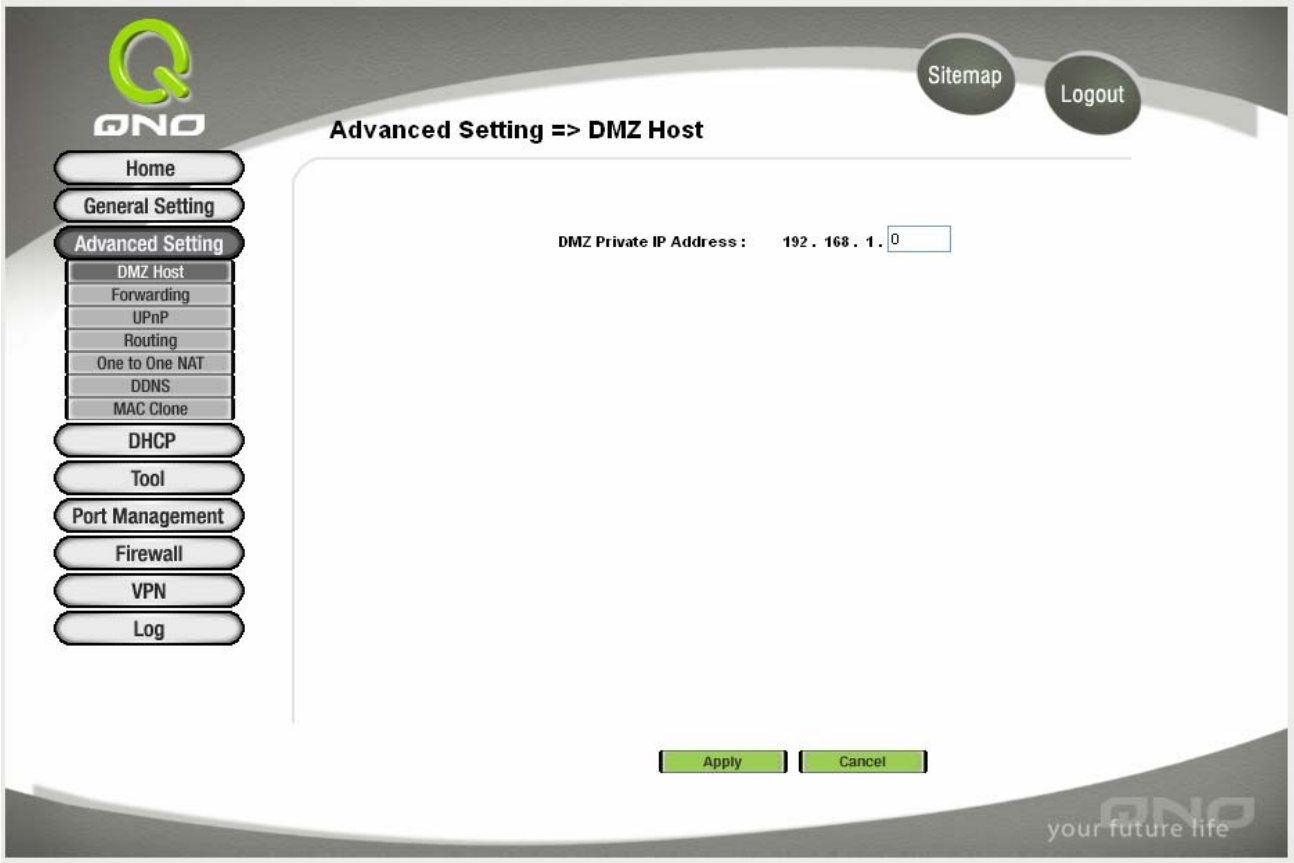


按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。 按下”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效。

Advanced Setting

DMZ Host-(Demilitarized Zone)

当您使用 NAT 模式运作时，有时需要使用如“网络游戏”等任何不支持虚拟 IP 位置的各种应用程序时，可将 QVM1000 的 WAN Port 的合法 IP 位置直接对应内部虚拟 IP 位置使用，设定如下填入下方的设定可用此功能达成！



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

按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。 按下”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效。

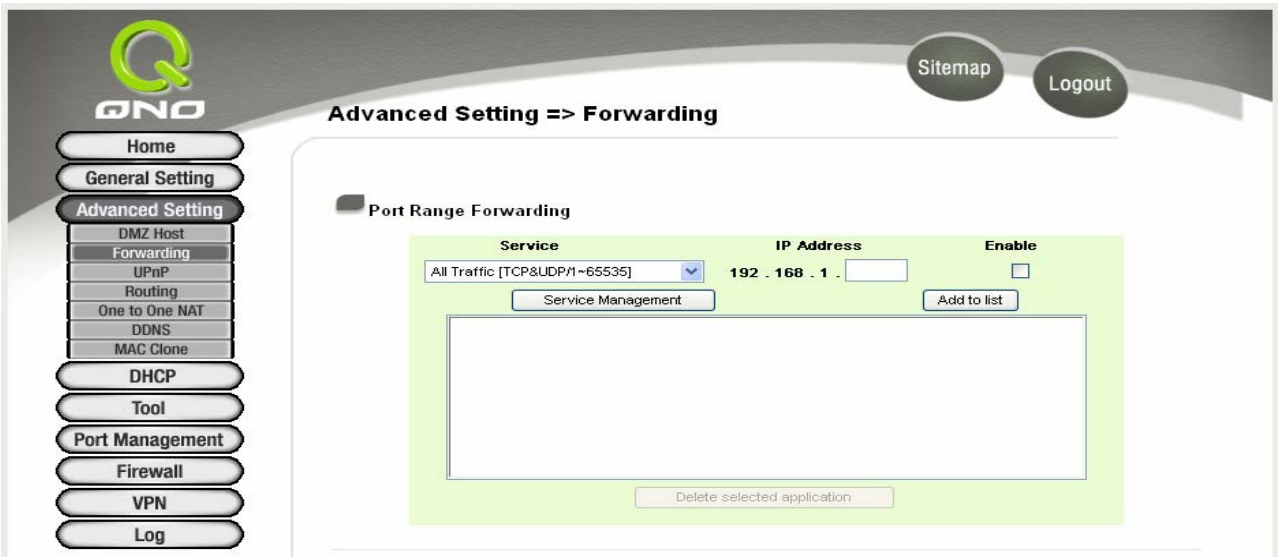
Forwarding

Port forwarding 虚拟主机架设，若是网络中含有服务器功能（意指对外部的服务主机 WWW，FTP．Mail 等）可将此主机利用防火墙功能，将主机视为一虚拟的位置，可用 QVM1000 的外部合法 IP 位置<Public IP>，经过 port 的转换（如 WWW 为 port 80），直接存取内部服务器的服务。若于设定画面中，选项填入ＷＷＷ服务器位置，如 192.168.1.50 且 port 是 80 的话，当 Internet 要存取这个网页时只要键入：

http://211.243.220.43(此为 QVM1000 的外部合法 IP 地址)

此时，就会通过 QVM1000 的 Public IP 位置去转换到 192.168.1.50 的虚拟主机上的 Port 80 读取网页了。

其它的服务设定，如同上一般；只要将所用的 Server 的 UDP Port 号码，以及虚拟主机的 IP 位置填入即可。



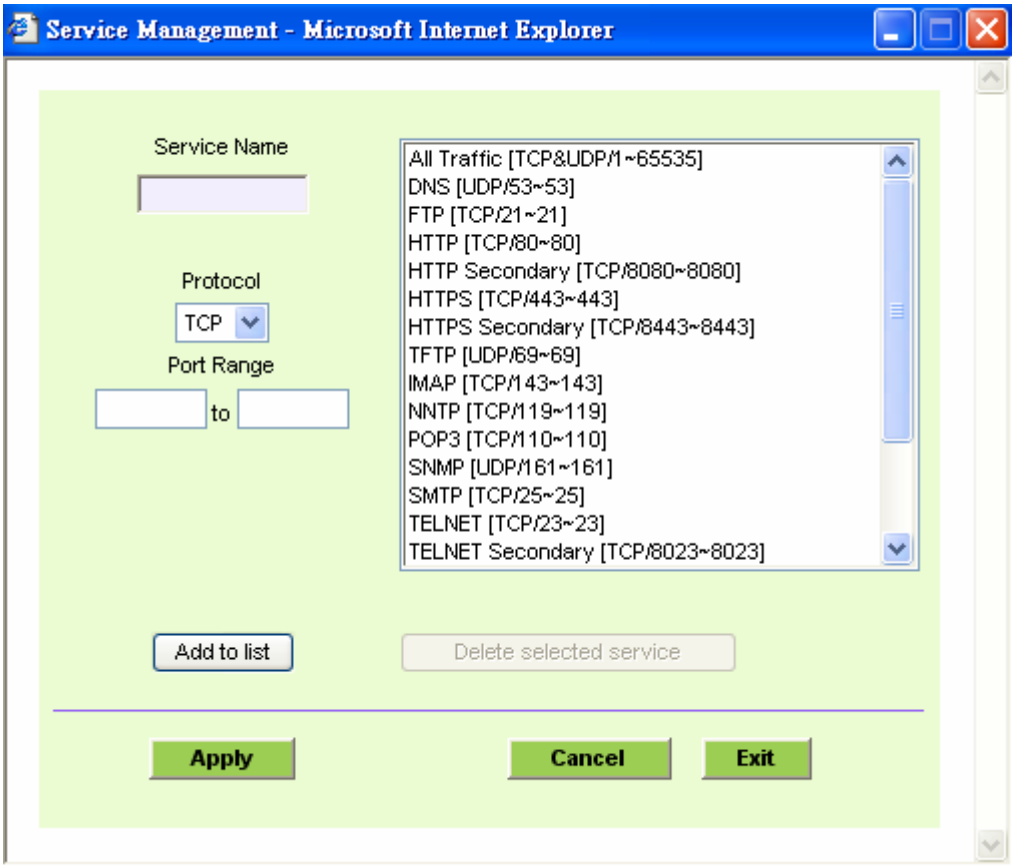
Services:	在此选择欲开启的虚拟主机的服务号码预设列表(如 All(TCP&UDP)0-65535)，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表。
IP Address:	在此填上虚拟主机相对应的内部虚拟 IP 位置，如 192.168.1.100
Enable:	开启此服务功能
Services Management:	新增或删除管理服务端口号列表
Add to List:	增加到开启服务项目内容

以上服务表列，一些为较常使用的项目，若您预开启的项目没有在表列中，您可以使用 **Services Management** 新增或删除管理服务端口号列表功能，如以下所述:

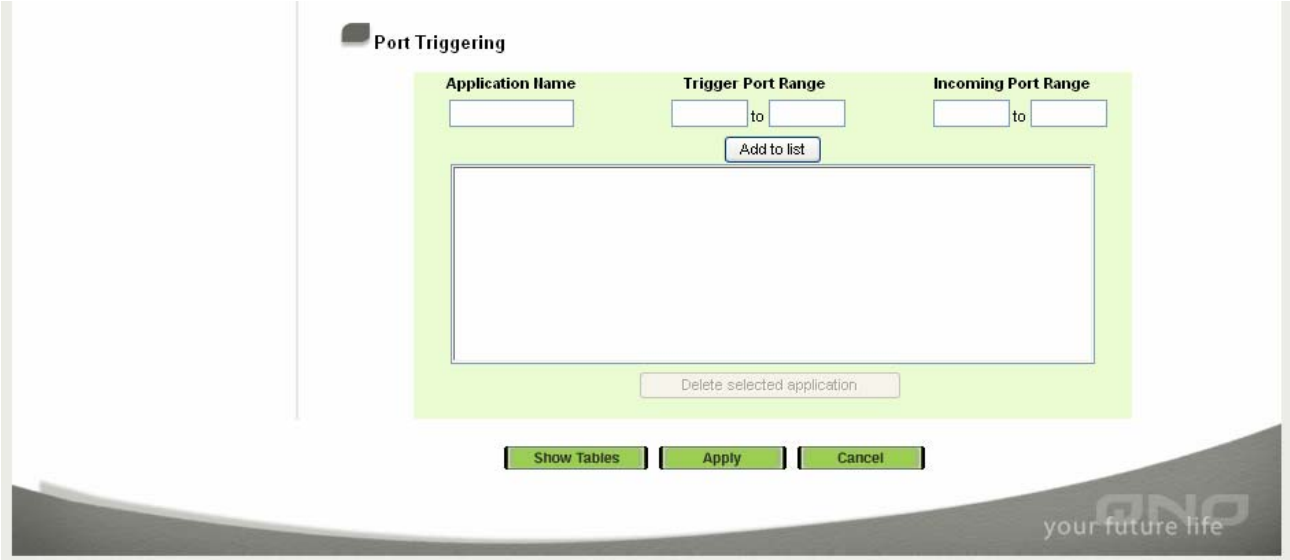
***Port Range Forwarding:*端口映射管理功能**

Services Name:	在此自订选择欲开启的服务端口号名称加入列表中，如 Edonky 等
Protocol:	选择此服务 Port 是 TCP 还是 UDP 封包。
Port Range:	开启此服务功能在此填上欲开启的服务端口号的位置范围，如 500~500 或是 2300~2310 等。
Add to List:	增加到开启服务项目内容列表。

Delete Selected Services:	删除所选择的服务项目。
Apply	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效
Exit:	离开此功能设定画面



Port Triggering



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

Application name: 您可以自订此特殊应用软件名称，方便管理使用！

Trigger Port Range: 输入由 QVM1000 出 Internet 的使用埠口(Port Number)编号。(如 9000~10000)

Incoming Port Range: 输入由 Internet 进入的使用埠口(Port Number)编号。 (如 2004~2005)

Add to List: 增加到开启服务项目内容列表。

Delete Selected Application: 删除所选择的服务项目。

Show Tables: 按下此按钮即会显示 Table 上的所有设定项目内容参数。

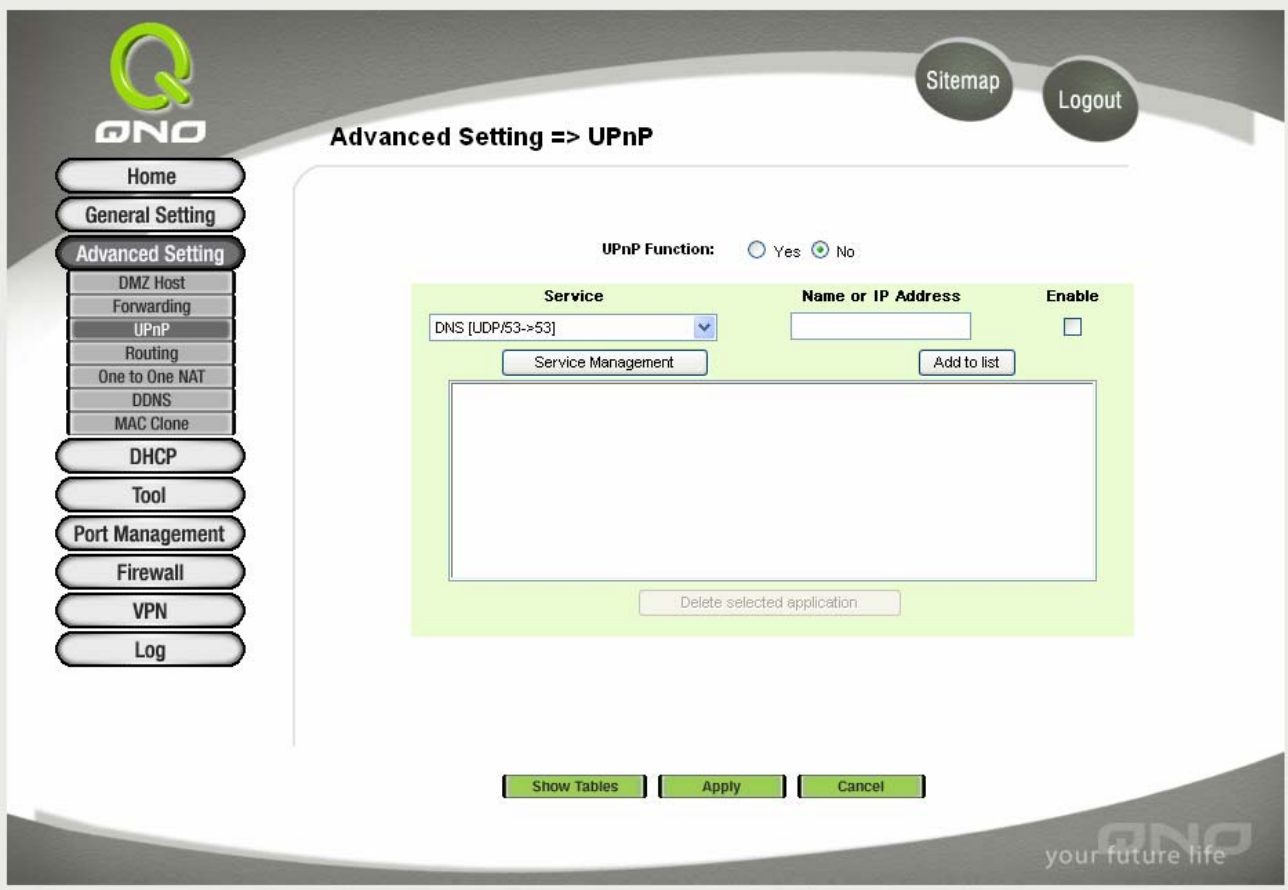
Apply: 按下此按钮"Apply"即会储存刚才所变动的修改设定内容参数。。

Cancel 按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

以下为一些常用的埠号需设定到此功能项目中的列表:

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

UPnP



UPnP (Universal Plug and Play) 是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的虚拟主机计算机有支持 UpnP 机制的话(如 WindowsXP)，而您也必须相同设定您的计算机使用 UpnP 功能开启，以便与 QVM1000 路由器协调搭配使用。

Services:	在此选择欲开启的 UPnP 的服务号码预设列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表!。
IP Address:	在此填上 UPnP 相对应的内部虚拟 IP 位置或名称，如 192。168。1。100
Enable:	开启此服务功能
Services Management:	新增或删除管理服务埠号列表
Add to List:	增加到开启服务项目内容
Delete Selected Services:	删除所选择的服务项目。
Show Tables:	显示目前所开启设定的 UpnP 列表
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。

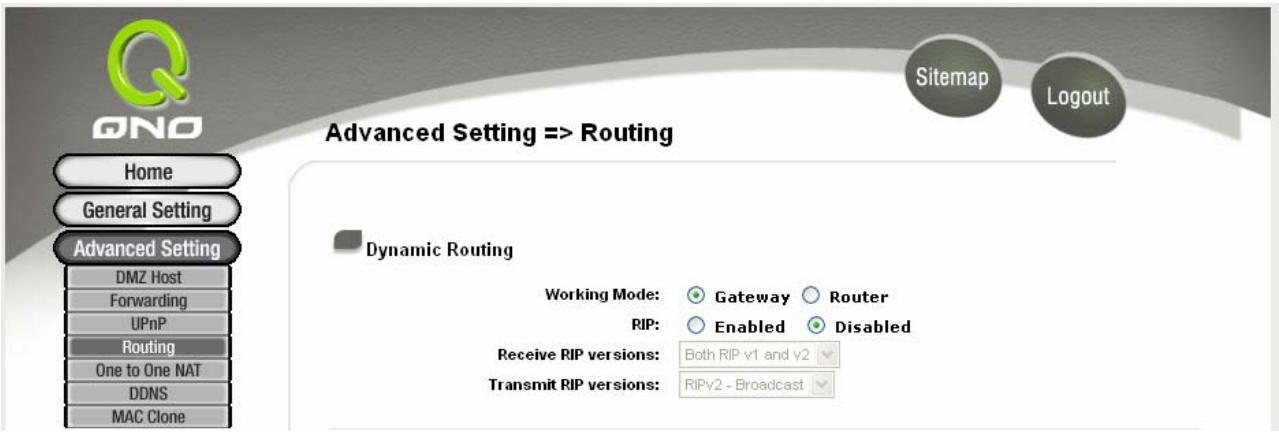
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Routing-路由通讯协议

***Dynamic Routing*-动态路由通讯协议**

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

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



Working Mode:	选择路由器运作模式为”Gateway”模式(NAT)或是一般路由(LAN to LAN Routing)模式。
RIP:	选择按钮”Enable”选择使用 RIP 动态路由通讯
Transmit RIP Version:	可于上下选择按钮选择使用动态路由通讯 **None， RIPv1， RIPv2， Both RIPv1 and v2** 为传送动态路由通讯协议的 **“TX”** 功能
Receive RIP Version:	可于上下选择按钮选择使用动态路由通讯 **None， RIPv1， RIPv2-Broadcast， RIPv2-Multicast，** 为接收动态路由通讯协议的 **“RX”** 功能
Show Routing Table:	可使用图中的功能按钮 “Show Routing Table “ 了解最新的路径表
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。

Cancel:	按下此按钮"Cancel"即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

***Static Routing*-静态路由通讯协议**

如果在您的网络中有多个路由器与 IP 节点子网络，就必需设定 QVM1000 的静态路由功能(Static Routing)，这些功能是让整个不同的网络节点能自动找寻所需路径，且能让不同网络节点能相户存取;使用图中的功能按纽 "Show Routing Table " 能知道最新的路径表

Select Route entry:	可选择静态路由表格，QVM1000 共支持了多达 30 组路由表
Delete this entry	删除一个路由表
Destination IP and Subnet Mask:	可填入欲绕径的远程网络 IP 节点与子网络节点位置，如另一个子网络节点为 192.168.2.0/255.255.255.0
Default Gateway:	此网络节点欲绕径的预设网关位置。 如 192.168.2.1
Hop Count:	此节点的路由器层数，如是在 QVM1000 下的二个路由器之一，此应填为 2，预设为 1。(最大为 15)
Interface	此网络节点的连接位置，是位于 WAN 端亦或是 LAN 端。
Delete Selected IP:	删除一个路径表
Show Routing Table:	显示目前最新的路径表

。

One-to-One NAT-- 一对一 NAT 对应

当您的 ISP 提供给你多个合法固定 IP (如 ADSL 固定 8 个或更多 IP 位置)时，因 QVM1000 本身只有使用一个合法 IP 位置，以及 ATU-R 也使用一个合法 IP 位置，所以剩余的合法 IP 可将其直接对应到 QVM1000 内部的虚拟 IP 计算机！

使用方法:

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

范例: 如您有 5 个可用 IP 位置，分别是 210.11.1.1~6，而 210.11.1.1 已经给 QVM1000 的 WAN 合法 IP 使用于一般的 NAT 上，另外还有其它四个合法 IP 可以分别设定到 Multi-DMZ 当中，如下所述

210.11.1.4→ 192.168.1.3

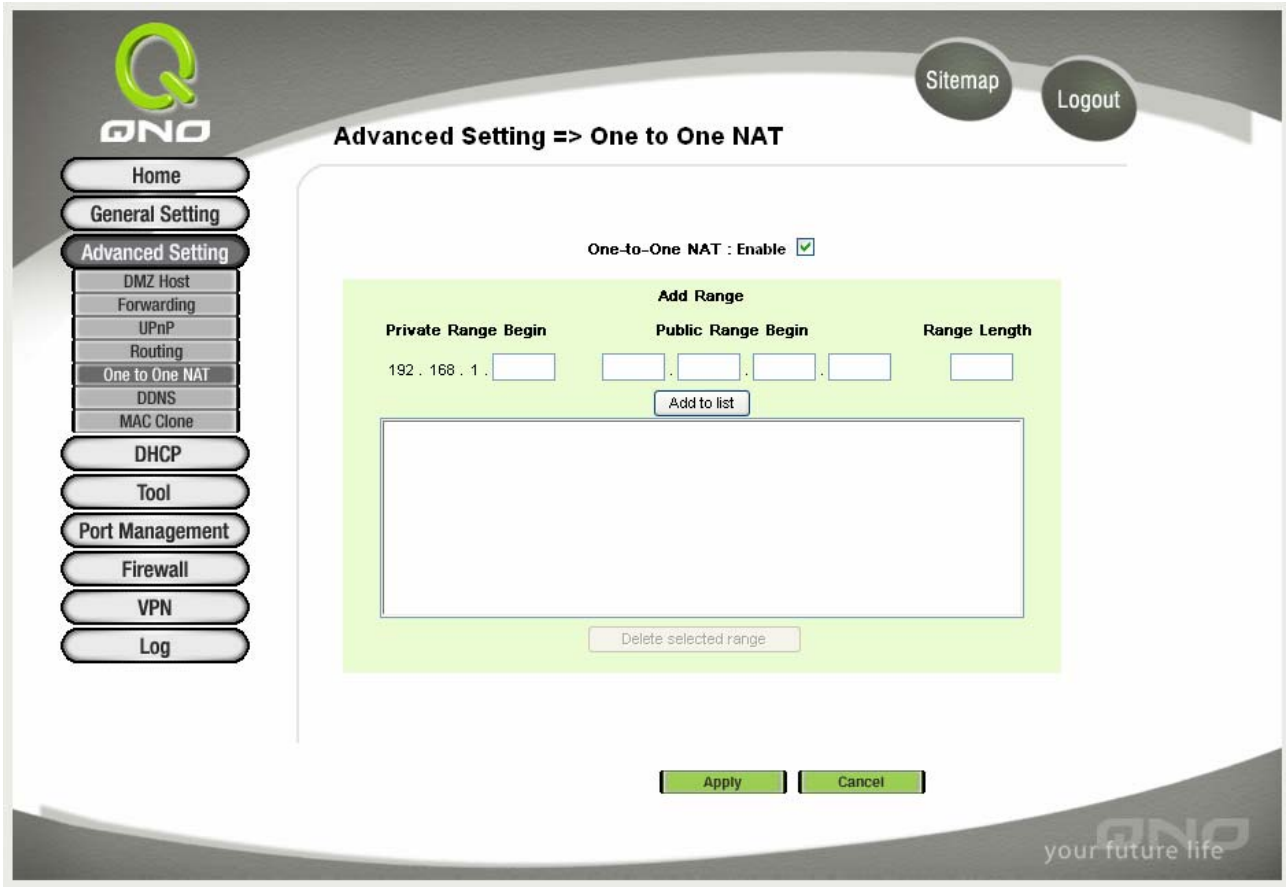
210.11.1.5→ 192.168.1.4

210.11.1.6→ 192.168.1.5

210.11.1.7→ 192.168.1.6

。

Note: QVM1000 广域网络 IP 位置(WAN IP -NAT Public) **不行纳入此 one to one 的范围设定中。**

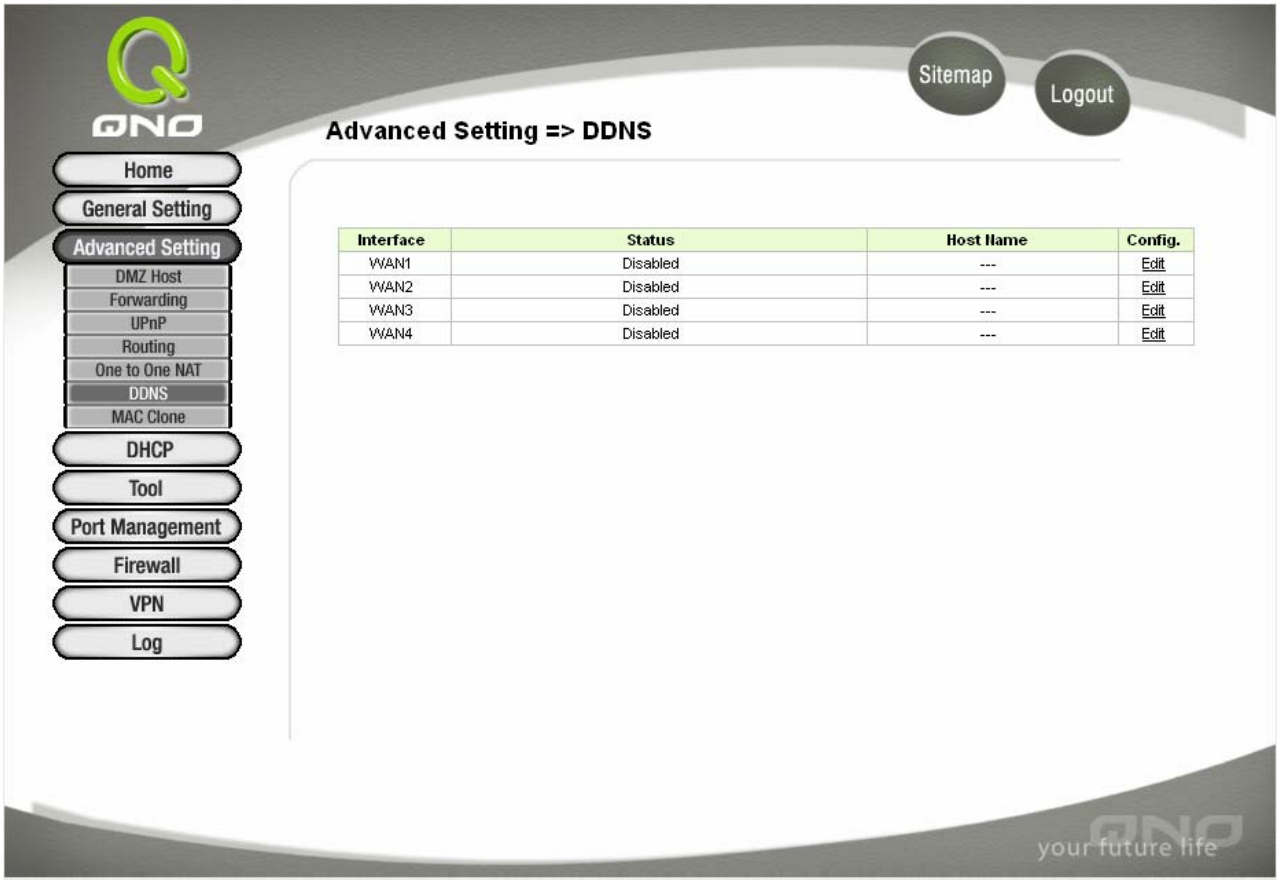


One-to-One NAT:	激活或关闭一对一 NAT 功能“**Enable”**开启 **Disable** 关闭 (选择是否开启此功能)
Private Range Begin:	虚拟 IP 位置起始 IP 位置
Public Range Begin:	外部合法 IP 位置起始 IP
Range Length:	外部合法 IP 位置终止 IP 的数量(请勿含盖 WAN 在使用的 IP)
Add to List:	加入此设定到一对一 NAT 列表中
Delete selected range:	删除所选择的一项一对一 NAT 列表
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

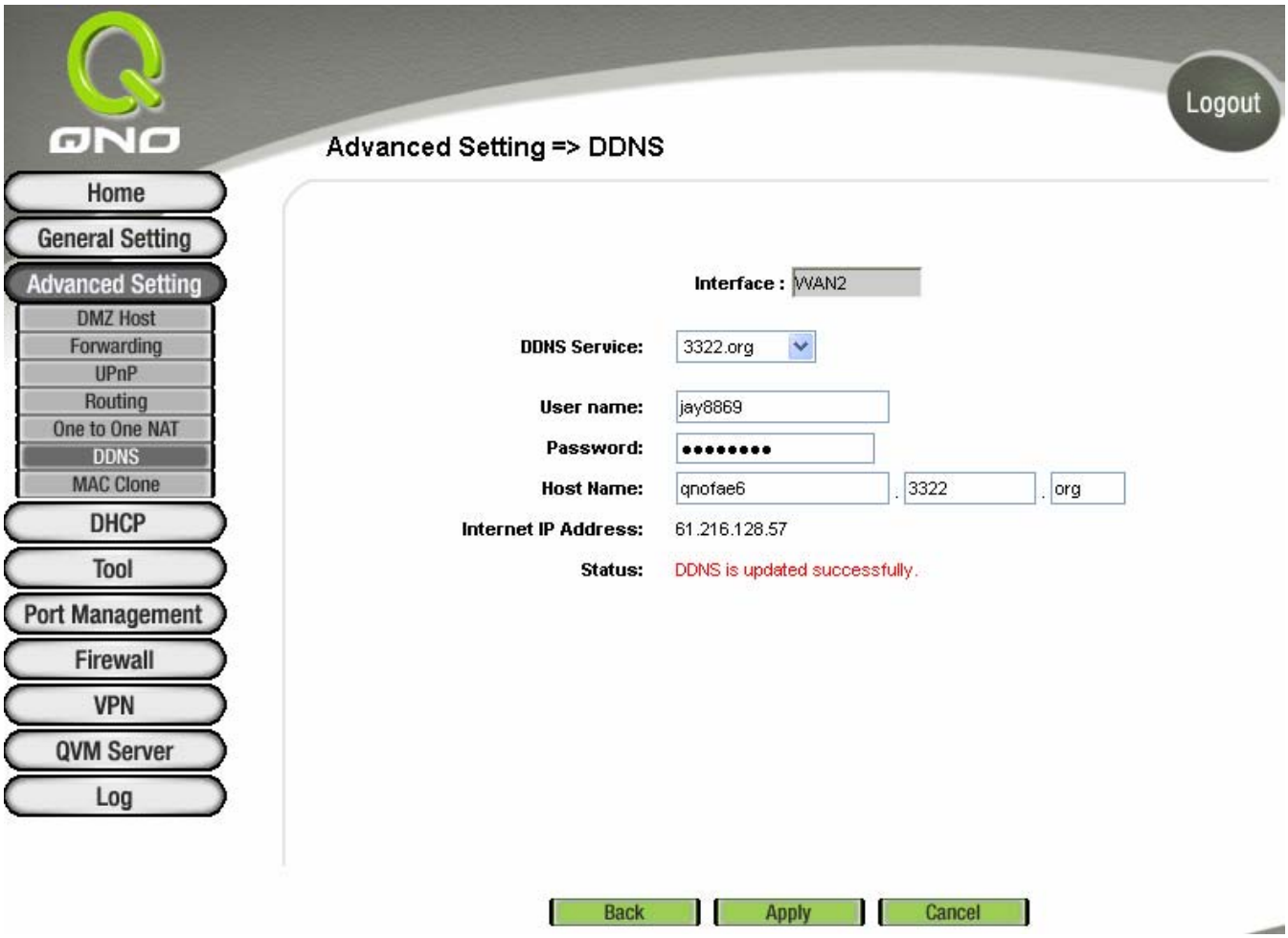
Note: 一对一的 NAT 模式(One-to-One NAT)将会改变防火墙运作的方式。您若设定了此功能， LAN 端所设定的机器或 PC 将会曝露到 Internet 上（在路由器防火墙外）， 除非到防火墙的 Access Rule 中加入拒绝存取规则项目条件，才可以阻断由 Internet 进到 LAN 端设定一对一 NAT 的机器或 PC。 您可以按下新增一个一对一 NAT 位置项目(**Add to List)** 按钮或是选择删除一个一对一 NAT 位置(**Delete selected range)**。

DDNS-动态域名解析服务

“DDNS”目前支持 Dyndns.org 与 3322.org 的动态网址转换功能，其目的是为了让使用动态 IP 位置架站或是远程监控还有动态 IP 下需做 VPN 的联机为目的，如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的合法 IP 地址都会随时间而改变，当此使用者欲架设网站之类的服务，但是因 IP 会随时变动， 所以本设备提供了动态网址转换功能，此服务可向 www.dyndns.org 或是 www.3322.org 提出申请，是完全免费的!!



请在设定栏(Config。) 的编辑(Edit) 按下该超级链接直接进入该设定项目中。

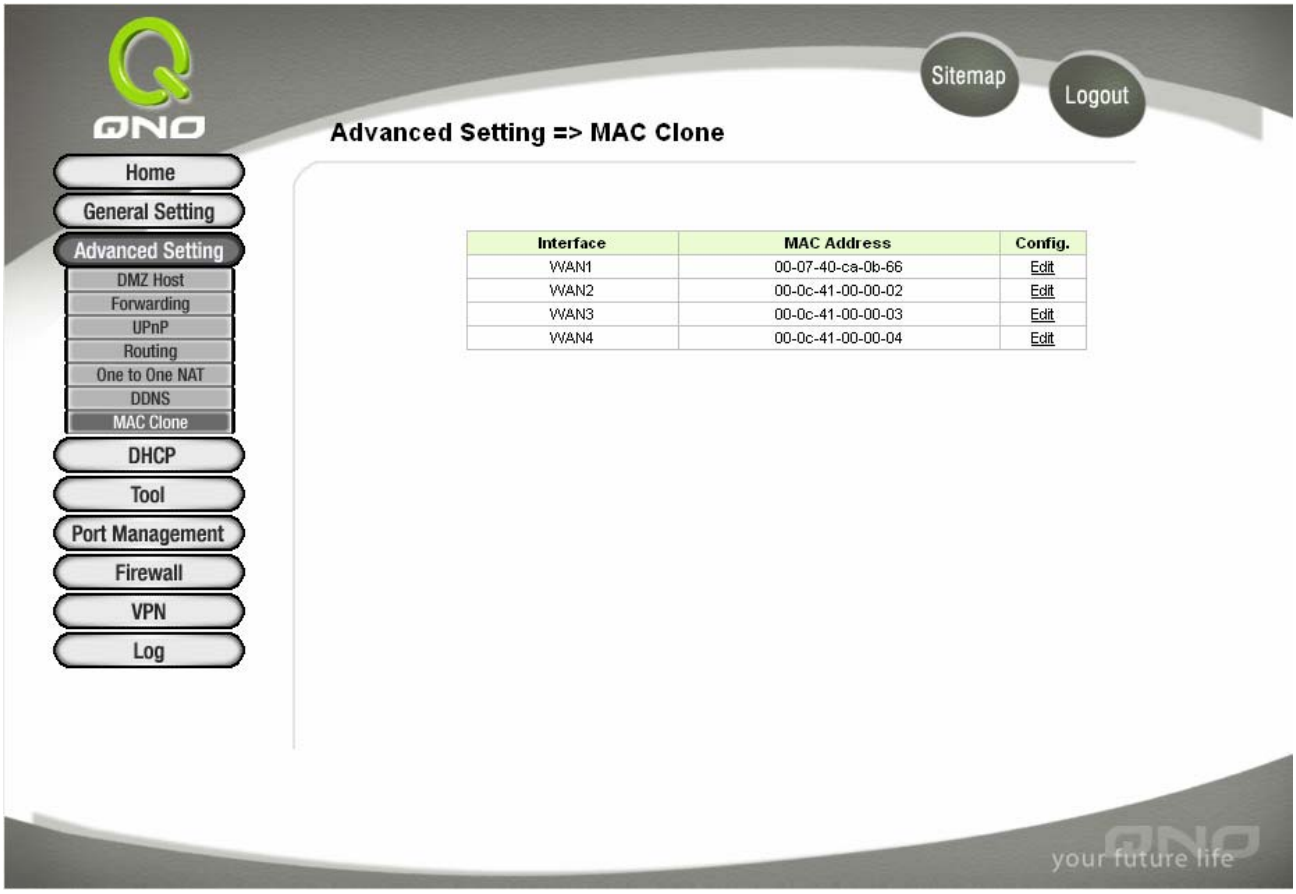


Interface:	使用者所选取的广域端口
DDNS Service:	DDNS 动态网址转换功能可以选择 **Disable** 关闭，DDNS.org 与 3322.org 等三项。
Username:	使用者名称:向 DDNS 所设定的名称
Password:	使用者密码:向 DDNS 所设定的密码
Host Name:	动态网址名称:向 DDNS 所注册的网址，如 abc.dyndns.org or xyz.3322.org 等。
Internet IP Address	目前向 ISP 所取得的之动态合法 IP 位置
Status:	目前 DDNS 的状态:显示目前的 DDNS 所更新 IP 功能状态
Back:	按下此按钮”Back”即会回到前一个画面。
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但

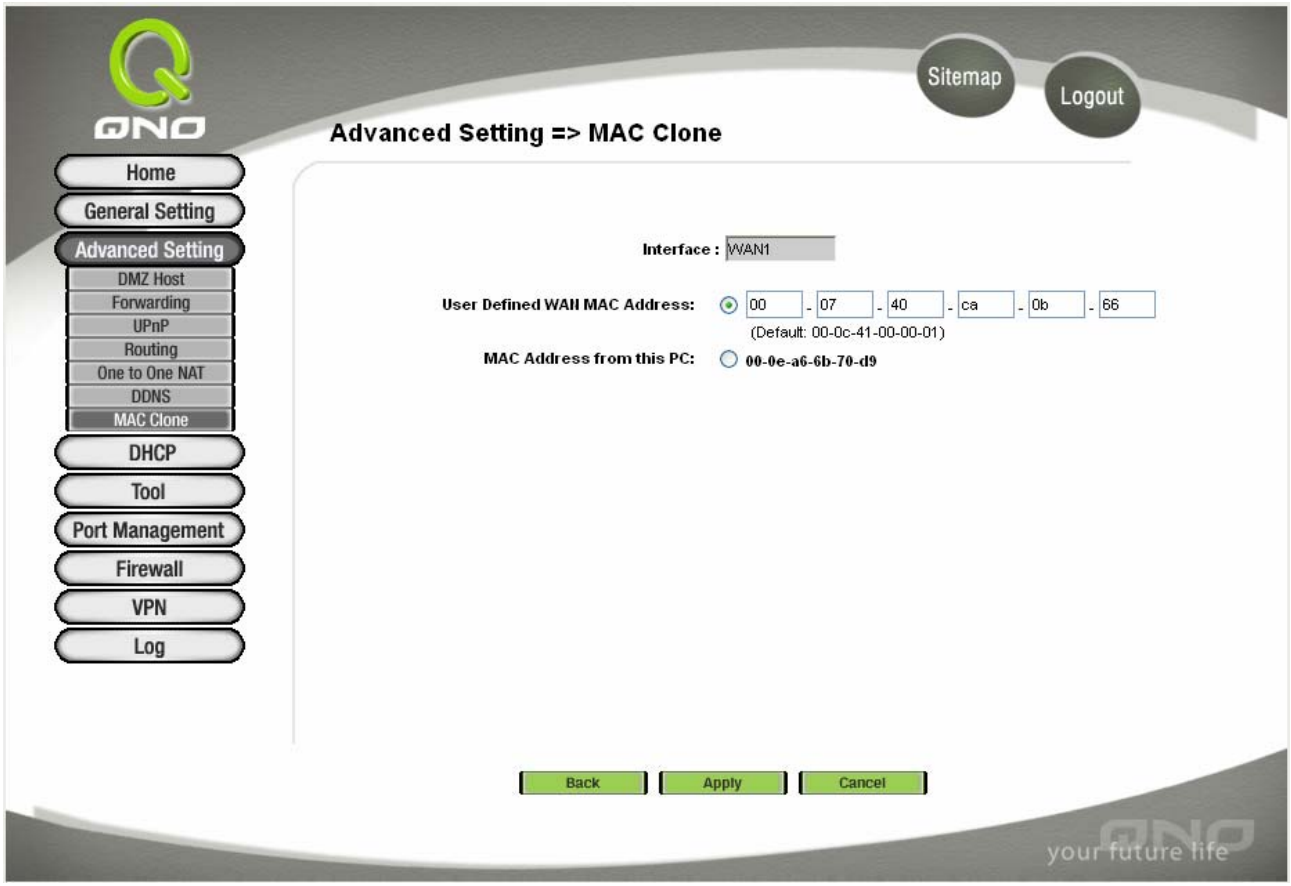
是必须于 Apply 储存动作之前才会有效

MAC Clone-变换硬件 MAC 位置

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



请在设定栏（Config） 的编辑（Edit） 按下该超级链接直接进入该设定项目中。



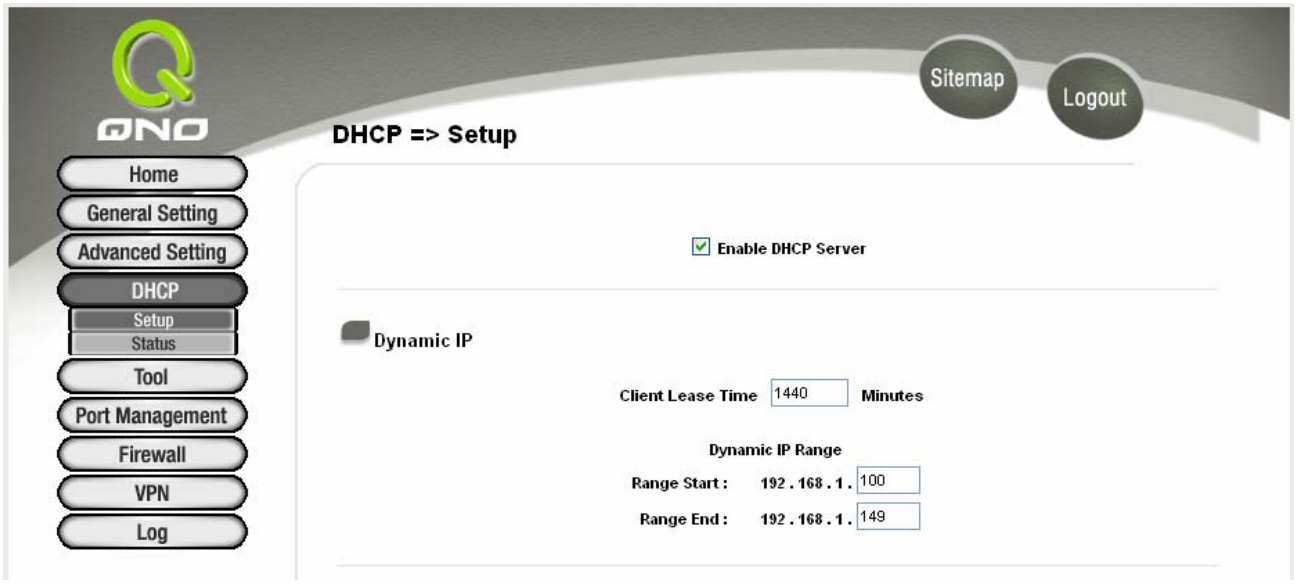
Interface:	使用者所选取的广域端口
User Defined WAN1 MAC Address:	目前设备出厂预设的 MAC 位置。
MAC Address From this PC:	目前连接此 PC 的 MAC 位置。
Back:	按下此按钮”Back”即会回到前一个画面。
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

DHCP-DHCP 发放 IP 服务器

Setup-设定

因 QVM1000 本身就含有 DHCP 服务器，所以可以提供局域网络内的计算机自动取得 IP 的功能，（如同 NT 服务器中的 DHCP 服务，好处是每台 PC 不用去记录与设定其 IP 位置，当计算机开机后，就可从 QVM1000 自动取得，管理方便。。

Enable DHCP Server: 可选择开启 DHCP 服务器自动派发 IP 位置功能;若为 Enable 选项，则所有 PC 都可使用自动取得 IP 位置，反之则无；每台 PC 必需去指定固定虚拟 IP 位置



***Dynamic IP*-动态 IP**

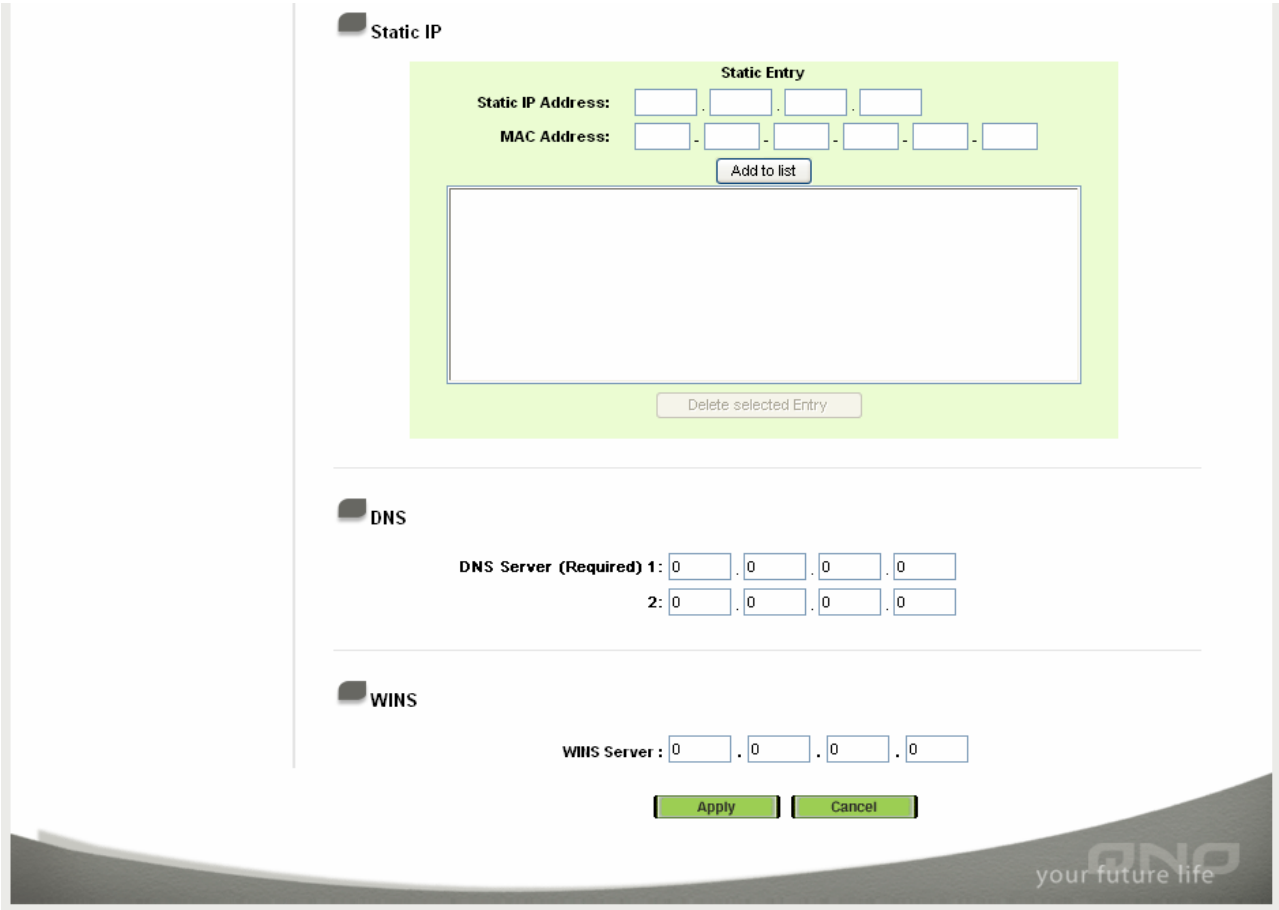
Client Lease Time: 此设定为发给 PC 端 IP 位置的租约时间，预设为 1440 分钟(代表时间为一天)，您可以依照实际需求来设定，以分钟为单位。

Range Start: 此 IP 位置是 DHCP Server 自动派送 IP 的启使 IP，意指是从多少 IP 地址开始派送。系统预设为从 192.168.1.100 的 IP 位置开始发放。

Range End: 意指是从多少 IP 地址停止派送。系统预设为从 149 的 IP 位置开始停止发放 IP，原厂设定值可供 50 台计算机自动取得 IP 地址，您可以是实际情况增减使用！

***Static IP*- IP 地址绑定功能(IP by MAC)**

Static IP address	输入 PC 端固定虚拟 IP 位置
MAC:	输入 PC 端网络卡固定硬件 MAC 位置
Add to List:	加入此设定到 Static IP 列表中
Delete selected Entry:	删除所选择的 Static IP 列表
Add New	新增固定虚拟 IP 位置



DNS Server

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

DNS Server (Required)1	输入 DNS 网域服务器的 IP 位置。默认值为 0。
2	输入 DNS 网域服务器的 IP 位置。默认值为 0。

WINS

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

WIN Server	输入 WIN 网域服务器的 IP 位置。默认值为 0。
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Cancel:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Status-状态显示

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

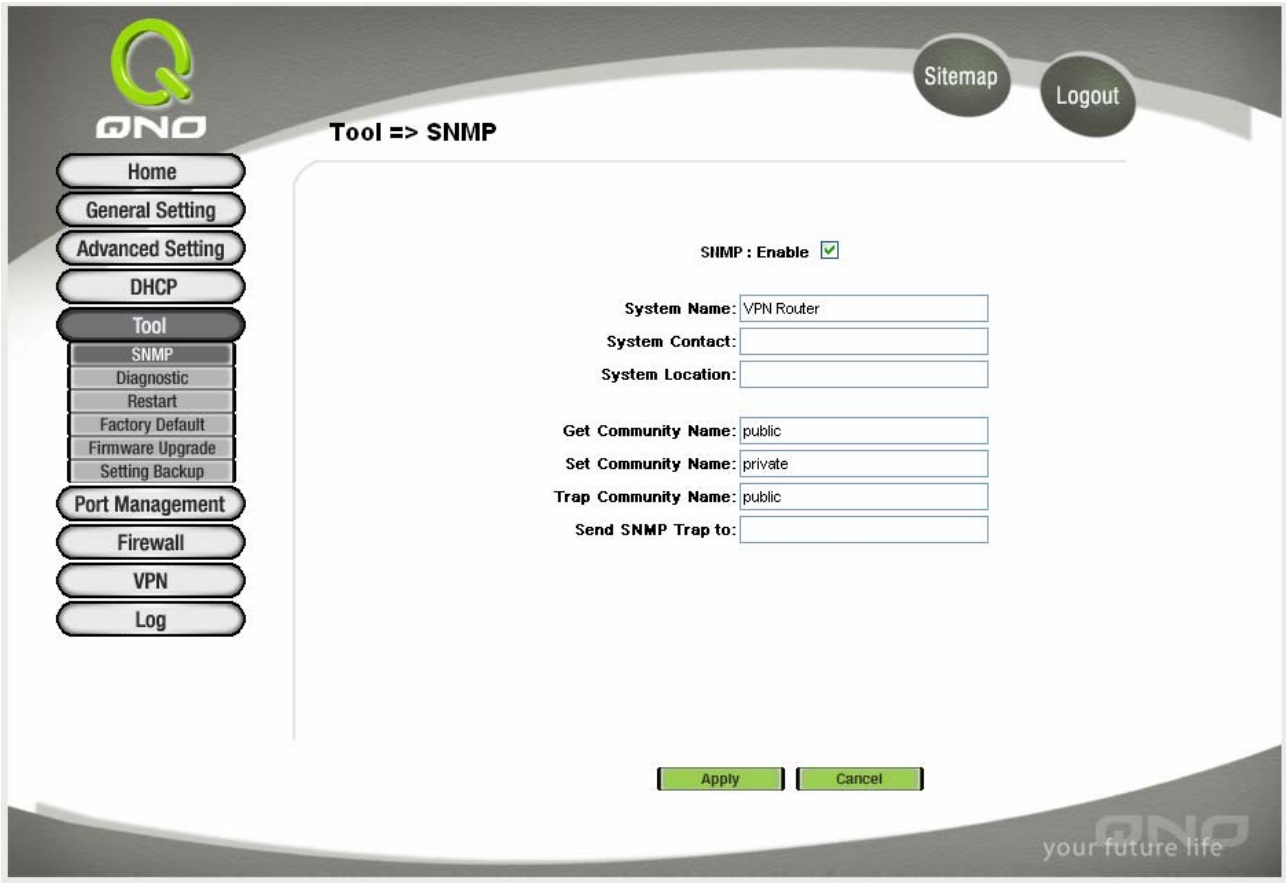
DHCP Server:	目前 DHCP 服务器的 IP 位置
Dynamic IP Used:	目前 DHCP 服务器已经发放动态 IP 的数量
Static IP Used:	目前 DHCP 服务器已经发放固定 IP 的数量

DHCP Available:	目前 DHCP 服务器可以发放的 IP 数量
Total:	目前 DHCP 服务器所设定可发放的 IP 总数量
Client Host Name:	目前此台计算机的计算机名称
IP Address:	目前此台计算机所取得的 IP 位置
MAC Address:	目前此台计算机的 MAC 网络实体位置
Leased Time:	DHCP 目前核发 IP 位置的租约时间
Delete:	删除此笔核发 IP 纪录

Tool-工具程序

SNMP-网络通讯管理协议

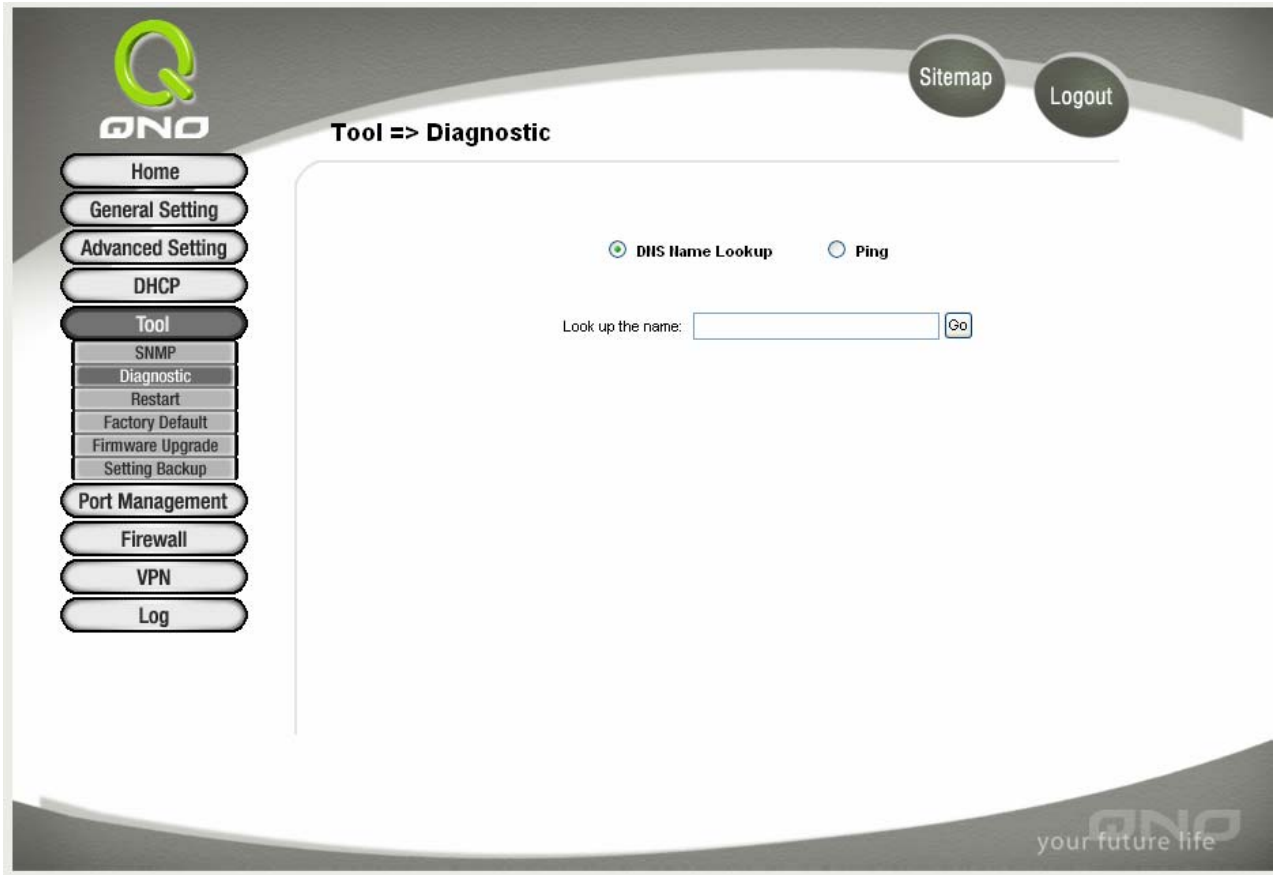
SNMP 为 Simple Network Management Protocol 的缩写，意指网络管理通讯协议，此为网络上重要的管理项目依据之一，透过此 SNMP 通讯协议，可以让已经具备有网络管理的程序(如 SNMP Tools-HP Open View)等网管程序做实时管理之通讯使用， QVM1000 支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前所有网络上的机器运作情况，以便随时掌握网络信息。



Enable SNMP:	将 SNMP 功能开启，系统预设为开启此功能。
System Name:	设定机器的名称，如 QVM1000
System Contact:	设定机器的管理联系人员名称，如 John
System Location:	设定机器的目前所在位置，如 Taipei
Get Community Name:	设定一组管理者参数可以取得此机器的项目信息，系统预设"Public"
Set Community Name:	设定一组管理者参数可以设定此机器的项目信息，系统预设"Private"
Trap Community Name:	设定一组管理者参数可以传送 Trap 的信息
Send SNMP Trap to:	设定一组 IP 位置或是 Domain Name 名称的接收 Trap 讯号主机
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Delete:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Diagnostic-线上联机除错测试

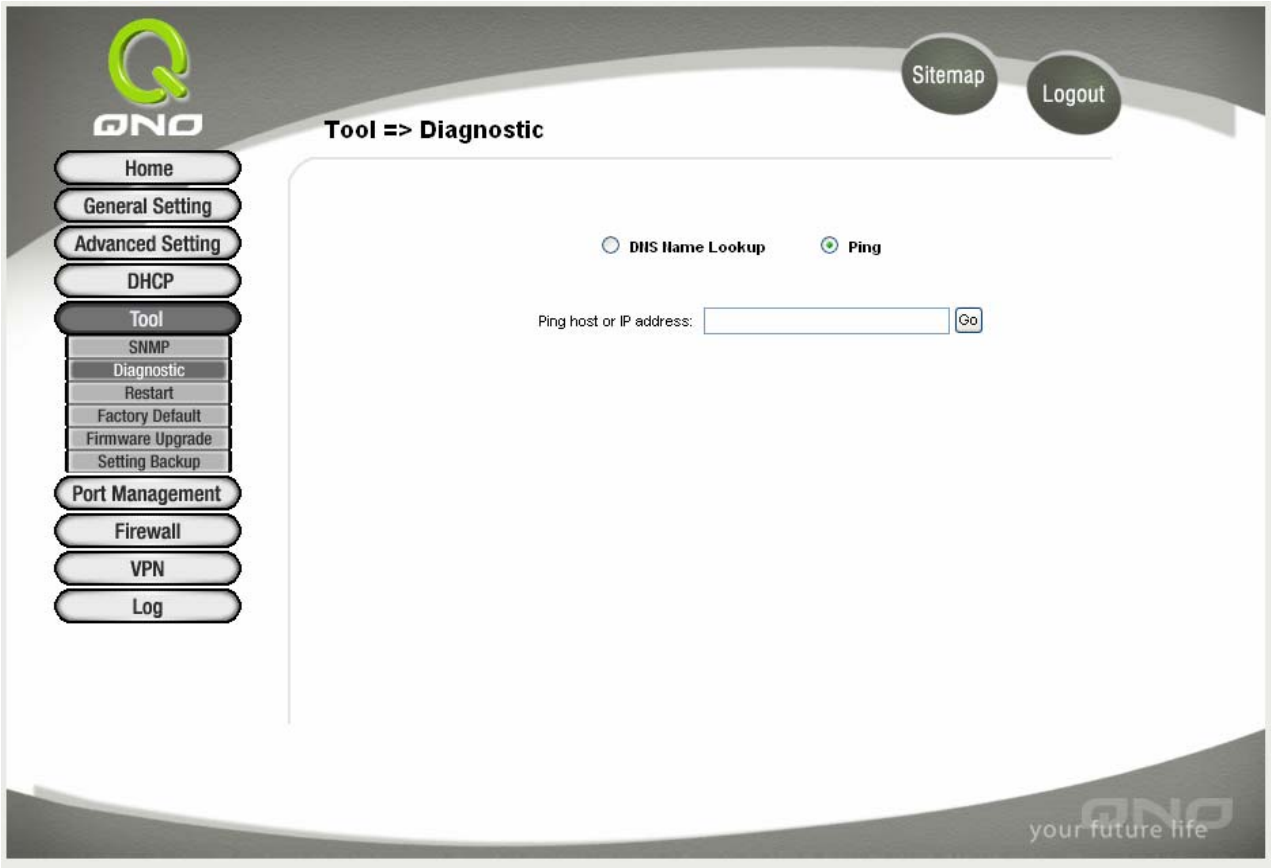
QVM1000 提供简易的线上测试机制方便于除错时使用，此除错机制包含 DNS Lookup 以及 Ping 二种。



DNS Name Lookup-网域名称查询测试

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

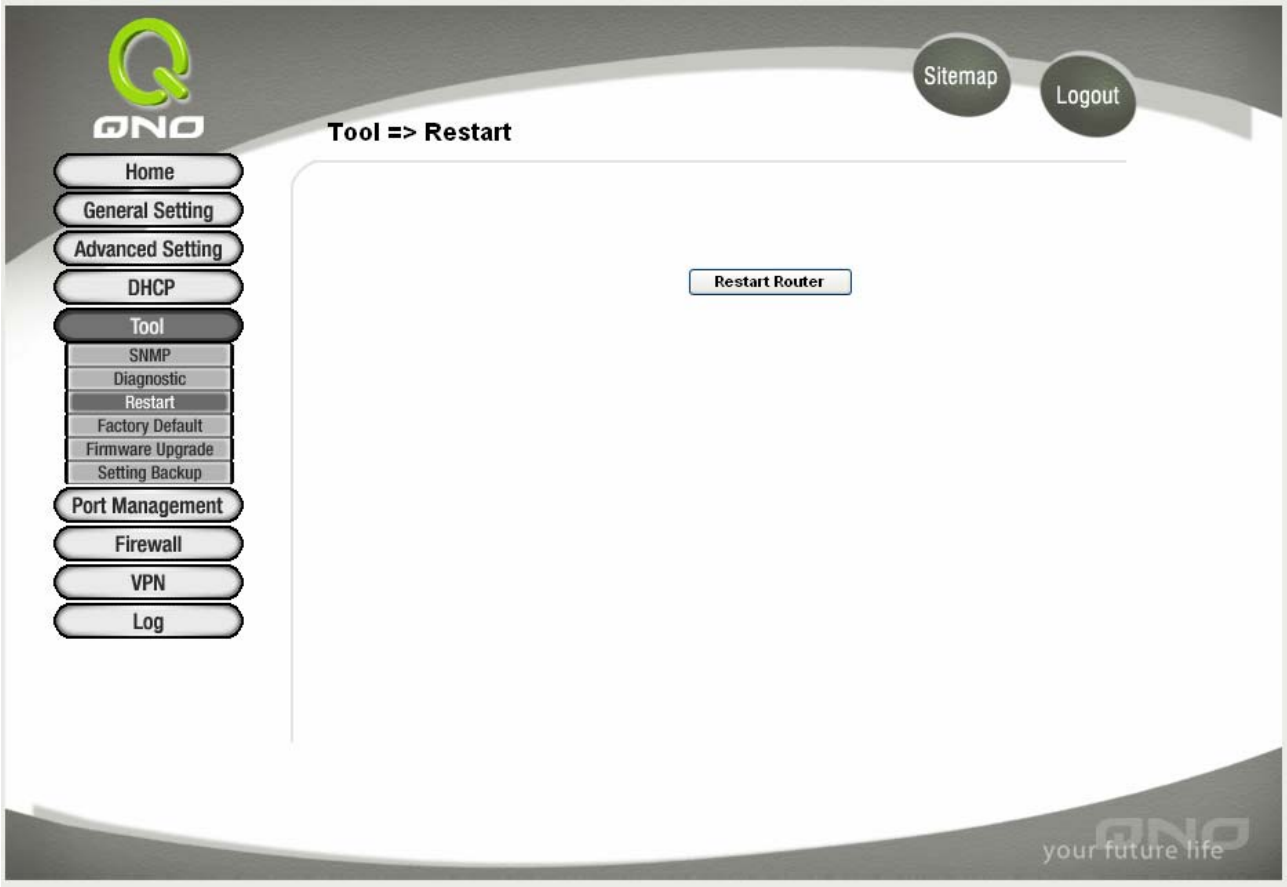
Ping-封包传送/接收测试



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

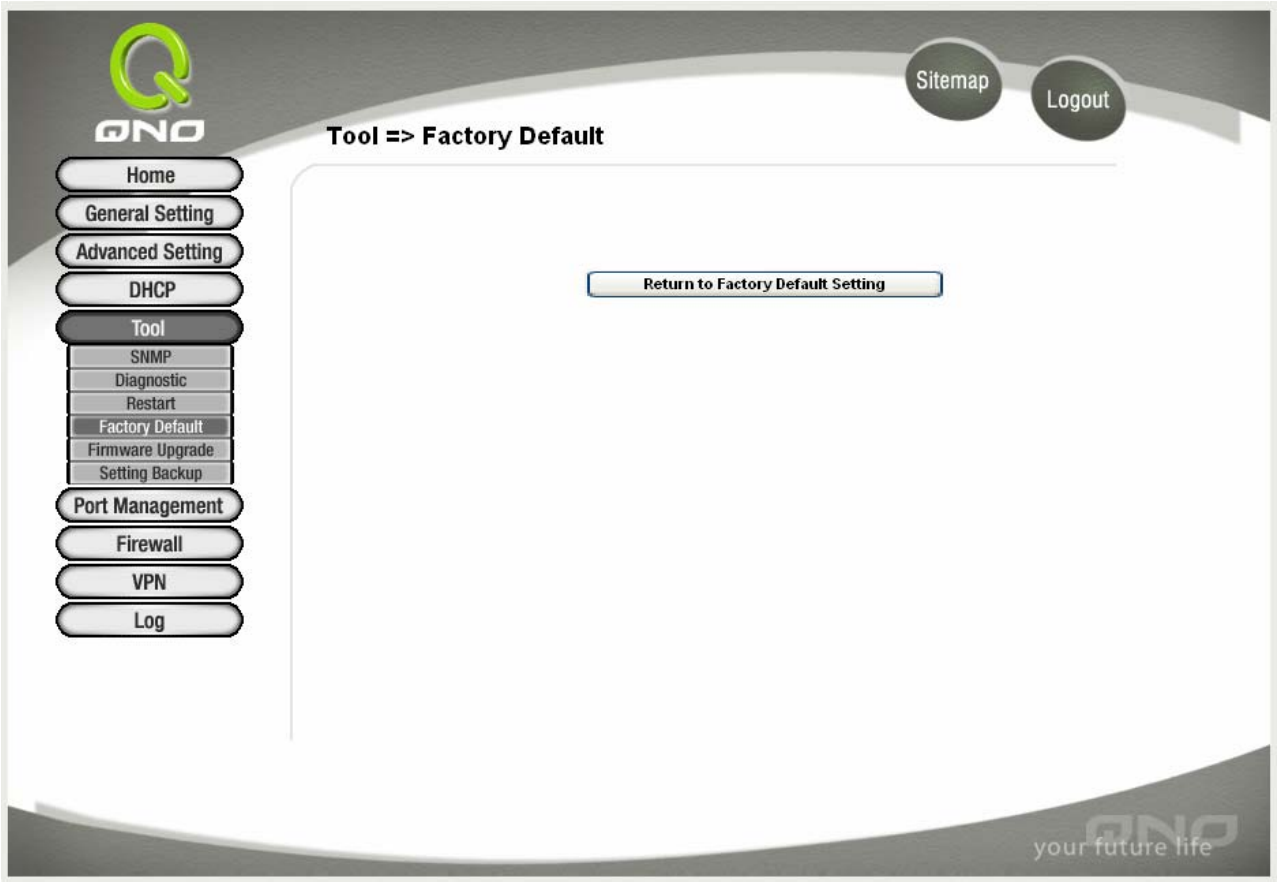
请于此测试画面输入您想测试的主机位置 IP，如 192.168.5.20 按下 Go 的按钮开始测试，测试结果会显示于此画面上。

Restart-重新激活



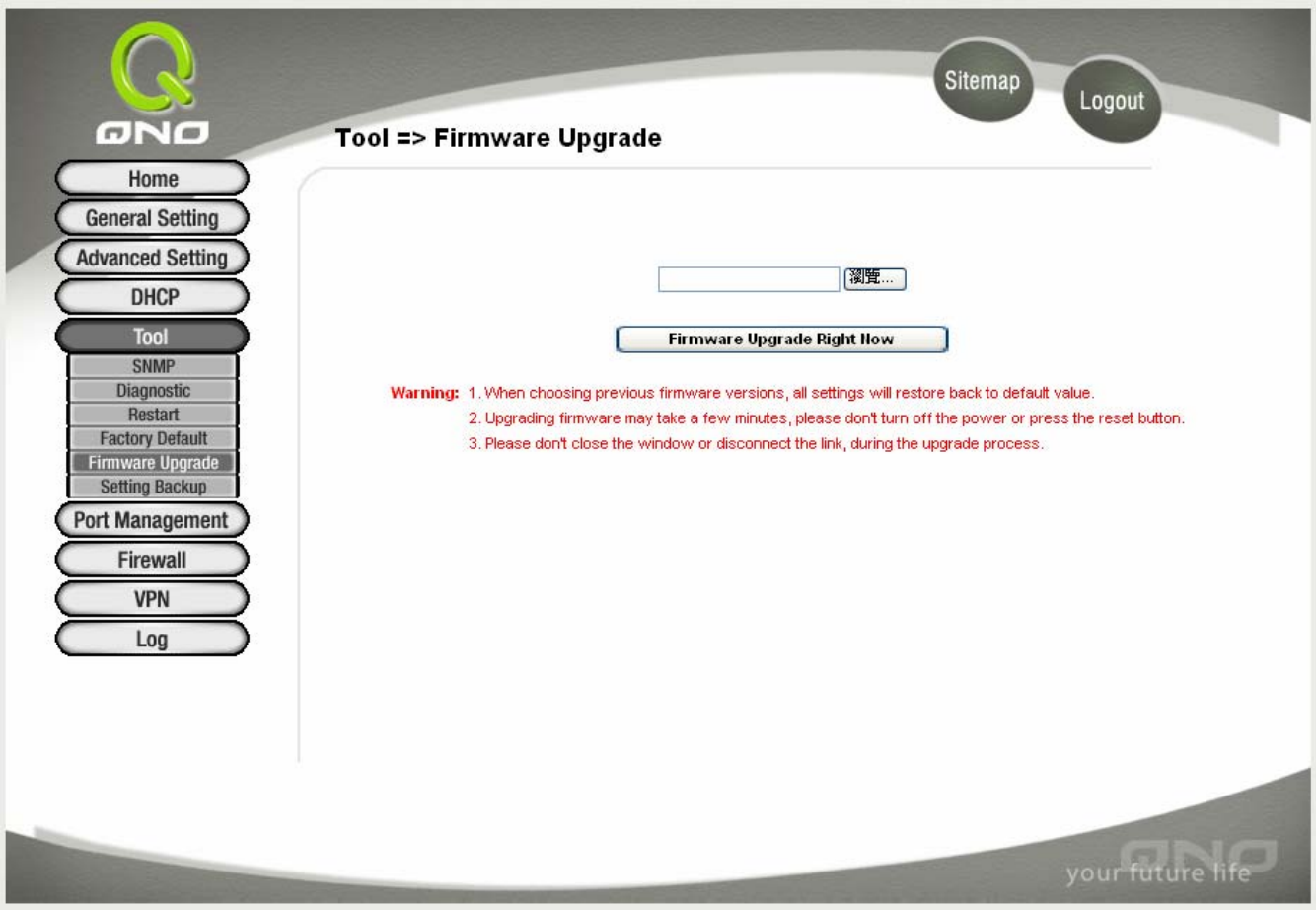
通过此"Restart"按钮来重新激活 QVM1000，重新激活后也会将此讯息传送到系统日志中。选择后，请按下 **Restart Router** 按钮即可重新开机激活。

Factory Default-回复原出厂默认值



若是选择**“Return Factory Default Setting”**， QVM1000 会将所有的 QVM1000 上面的设定清除，并重新开机。切记，使用此功能会将机器所有的资料清除！

Firmware Upgrade-系统软件升级

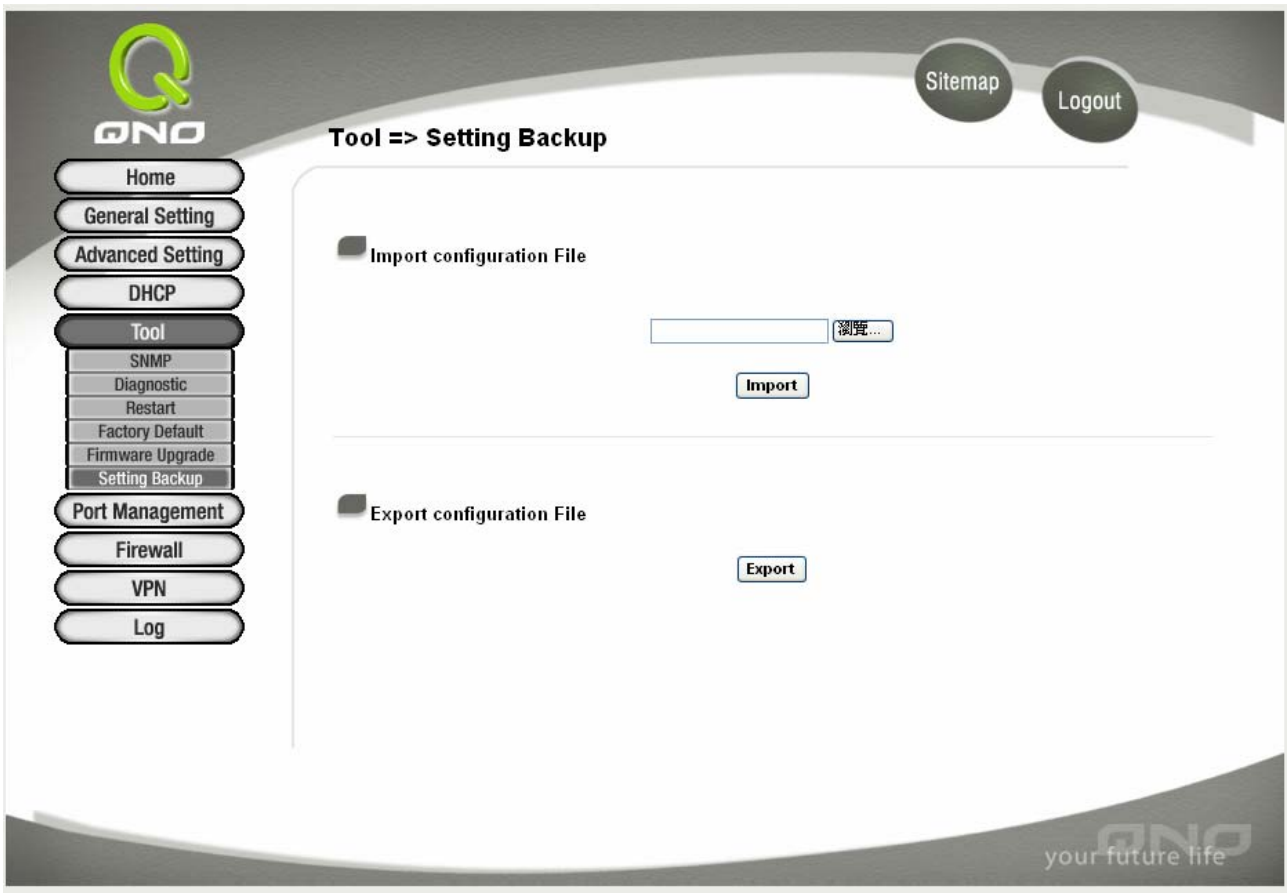


Firmware Upgrade

此设定可以于 QVM1000 的 Web 设定画面中直接升级软件，并请您于升级前先确认软件版本信息，选择浏览至软件-Firmware 存放资料夹，选定该档案后，按下 **Firmware Upgrade Right Now** 做升级。

切记:当升级动作开始进行中时，请勿跳离此画面，否则升级会失败。

Setting Backup-系统设定参数储存



Import Configuration File:

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

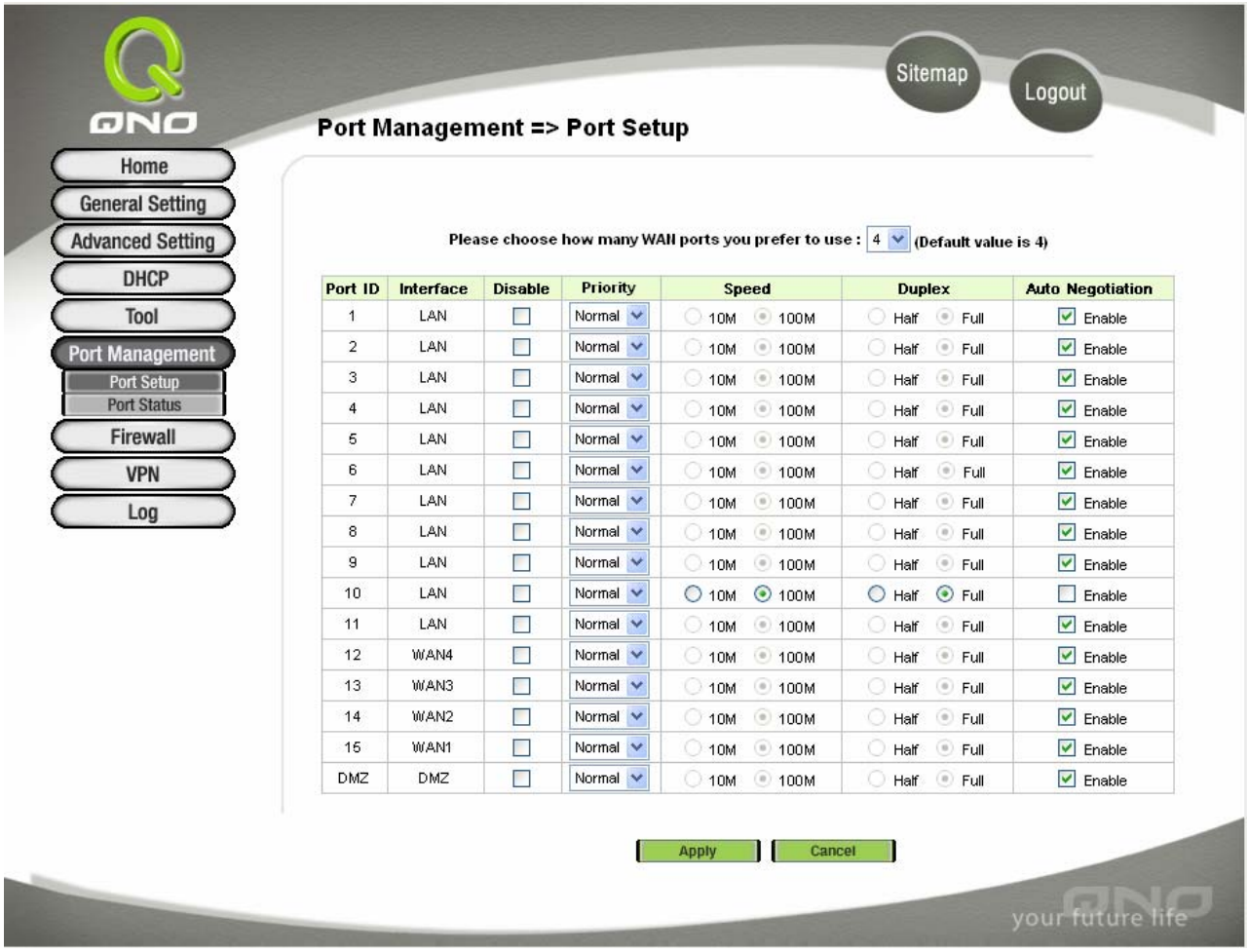
Export Configuration File:

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

Port Management-网络硬件端口管理

于 QVM1000 中，使用管理者可以设定广域端口数与每一个以太网络端口连接速率(Speed)，工作模式(Half &Full)，高低优先权(Priority)或是自动侦测(Auto-negotiation)等以太网络端口的功能。

Port Setup-网络端口设定



***Basic Per Port Config*。-以太网络端口设定**

Port ID: 显示每个端口的顺序。

Interface: 共有 LAN1~LAN 11， WAN1~WAN4， and DMZ 等埠口 。这些端口会根据使用者所设定的广域端口数而自动调整。

Port Disable: 此为设定以太网络的端口开启或是关闭的功能，若是打勾的话，则此以太网络端口立即被关闭无法连接使用。预设为开启

Priority: 此为设定此以太网络的端口封包传送高低优先权设定，若是此 Port

	设定为 High 的话，则最优先使用传送封包的权利，默认值为-Normal 优先级为一般
Speed:	此为设定此以太网络的端口网络硬件连接速率选项，您可以设定为 10Mbps 或是 100Mbps 连接速度。
Duplex:	此为设定此以太网络的端口网络硬件连接速率工作模式选项，您可以设定为 Half –半双工模式或是 Full-全双工模式运作。
Auto-negotiation:	此为设定此以太网络的端口网络硬件连接速率自动侦测模式，若是勾选的话，自动侦测所有连接端口的信号与调整。

按下 **Apply** 按钮可以储存设定或是按下 **Cancel** 按钮可以取消设定更改。

Port Status-网络端口状态实时显示

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

于网络端口状态-Port Status 整体信息**(Summary)** 表格项目中， 此部份会显示目前端口硬件设定项目如网络连接型态(Type)， 线路联机状态(Link Status)， 端口使用状态(Port Activity 开-on 或关-off)， 端口优先权设

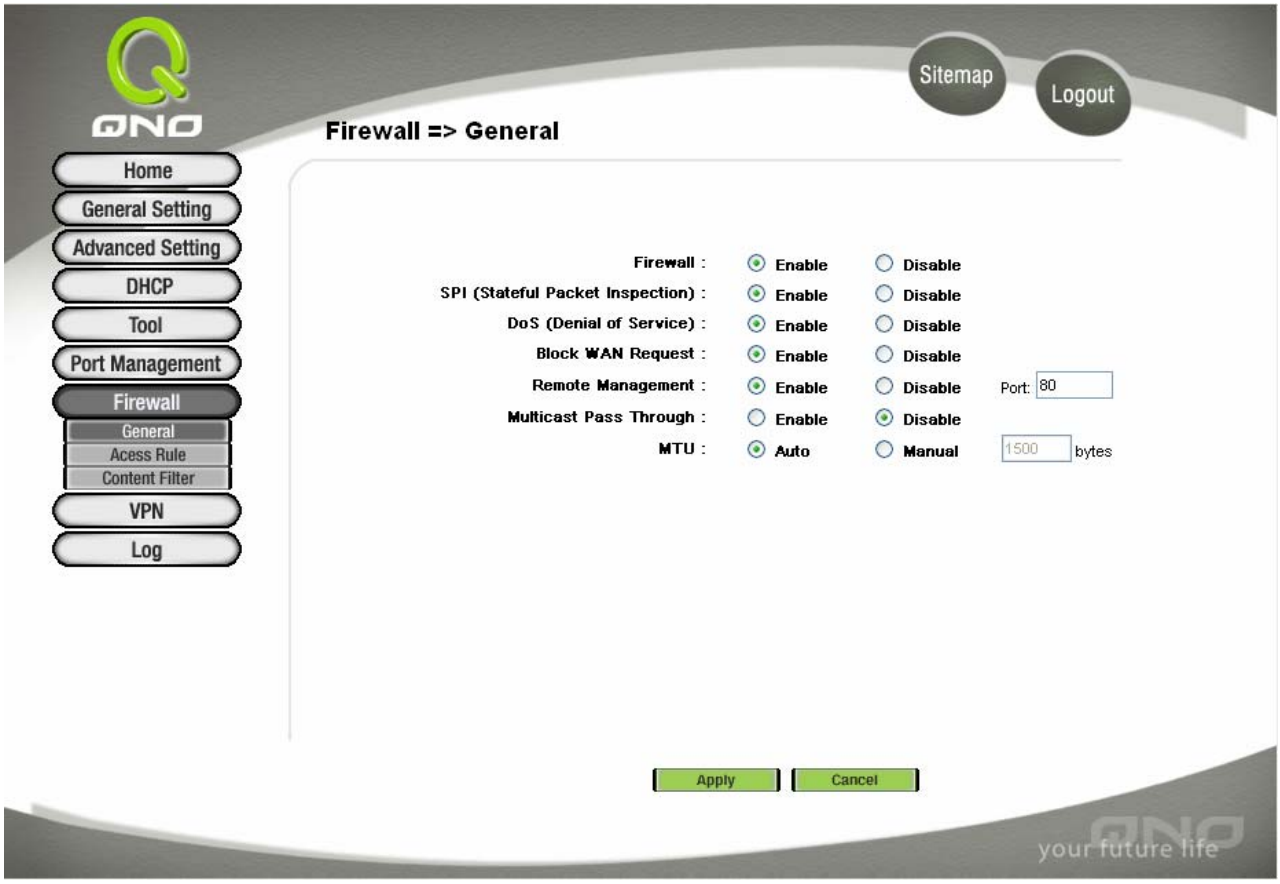
定(Priority- (高-High 或一般-Normal)，网络连接速率(Speed Status-10Mbps 或100Mbps)，双工模式(Duplex Status-半双工 half 或全双工-full)，自动侦测模式(Auto negotiation)。

网络端口实时显示**(statistics)** 信息表格项目中， 将会显示目前此端口的封包数据，包含传送/接收封包计算(receive/transmit packet count)/以及封包传送/接收 Byte 数计算(packet byte count)与 错误封包统计(Port Packet Error Count) 等。 您可以按下 **Refresh** 按钮重新整理所有的实时信息显示。

Firewall-防火墙设定

General-一般

QVM1000 预设防火墙功能为激活状态。 如果管理者关闭此防火墙选项功能的话(Firewall Disable)， SPI，DoS， Block WAN Request 等功能将会自动关闭(disabled)， 远程管理功能(Remote Management) 将会开启(enabled)，而网络存取规则(Access Rules) 与内容服务过滤器(Content Filter)也会关闭(disabled)。



Firewall:	开启或关闭防火墙功能
SPI:	此为封包主动侦测检验技术(Stateful Packet Inspection)，防火墙主要运作在网络层，所以执行对每个连接的动态检验，并拥有应用程序的警示功能，让封包检验型防火墙可以拒绝非标准的通讯协议所使用的连接。
DoS:	此为保护 DoS 攻击，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。
Block WAN Request:	若是选择 **Enable** 的话，则 QVM1000 会关闭对外的 ICMP 与不正常联机的封包响应，默认值为开启。(若您是使用 Cable 联机的话，此选项请开启)，当 **Enable** 此功能时，远程将无法 **ping** 到此台路由器， 当 **Disable** 此功能时，远程 **ping** 此台路由器广域端口 IP 地址时会得到响应。
Remote Management:	远程管理功能，若您要通过远程 Internet 直接联机进入路由器的设定画面，必需将此功能开启，并于远程使用 IE 于网址填入 QVM1000 的广域端口 IP 位置(WAN Port IP)，并加上预设可修改的控制埠口(预设为 80，可更改为其它端口)，如 http://210.11.11.1:8080 or http://210.11.11.1:8081
Multicast Pass Through:	网络上有许多影音串流媒体，使用广播方式可以让您的 Client 端接收此类封包讯息格式。
MTU:	MTU 为 Maximum Transmission Unit 的缩写， 一般预设的 default 为 1，500。 但是在不同的网络环境中， 应该是有不同的数值。 尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU Size:1492); 不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 有所相关，一般预设 **Auto** 即可，不需做任何调整

Access Rules-网络存取规则

管理者可以设定 QVM1000 路由器关闭(deny)或是允许(allow)任何的封包进出 Internet。 您可以选择设定不同的网络存取限制，从内部到外部(Inside-LAN to Outside-WAN)，从外部到内部(Outside-WAN to Inside-LAN)。设定 IP 位置及通讯端口号 (Port Number)不同的封包，过滤于 Internet 存取规则条件。

网络存取规则依照 IP address(IP 位置)， Destination IP address(目地端 IP 位置)， 与 IP protocol type(IP 通讯协议型态) 来管理所有的网络封包流量是否可以通过 QVM1000 防火墙的存取。

QVM1000 拥有简而易懂的网络存取规则条例工具。 管理者可自订的网络存取规则条例， 可以选择关闭或是开启并保护所有对网际网络 Internet 的存取。以下就针对 QVM1000 的网络存取规则条例做一说明:

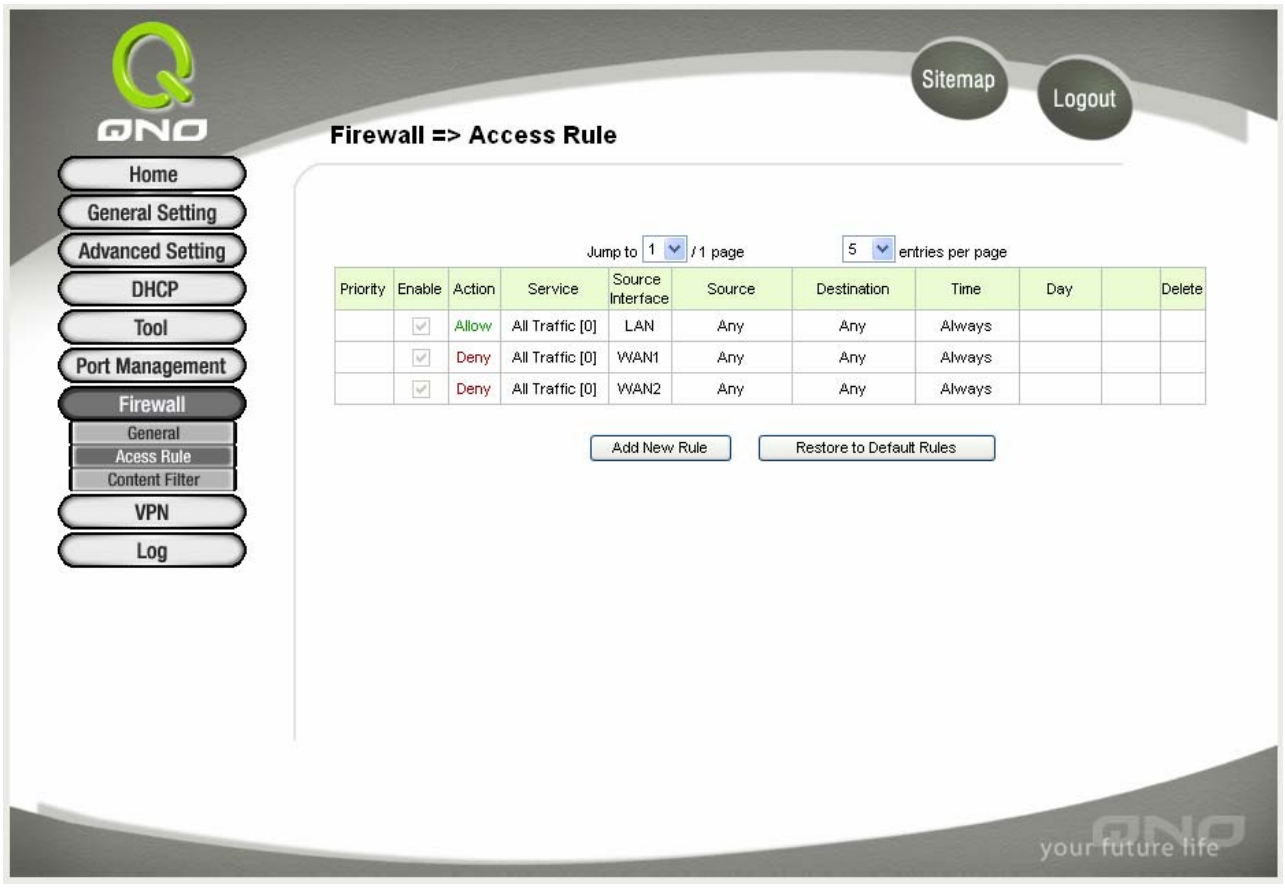
以下为 QVM1000 预设的网络存取规则条例:

* All traffic from the LAN to the WAN is allowed-从 LAN 端到 WAN 端的封包预设为可以通过

* All traffic from the WAN to the LAN is denied。- 从 WAN 端到 LAN 端的封包预设为关闭
* All traffic from the LAN to the DMZ is allowed。- 从 LAN 端到 DMZ 端的封包预设为可以通过
* All traffic from the DMZ to the LAN is denied-从 DMZ 端到 LAN 端的封包预设为关闭。
* All traffic from the WAN to the DMZ is allowed-从 WAN 端到 DMZ 端的封包预设为开启。
* All traffic from the DMZ to the WAN is allowed-从 DMZ 端到 WAN 端的封包预设为开启。

使用者可以自定存取规则并且超越 QVM1000 的预设存取条件规则， 但是以下的四种额外服务项目为永远开启，不受其它自订规则所影响:

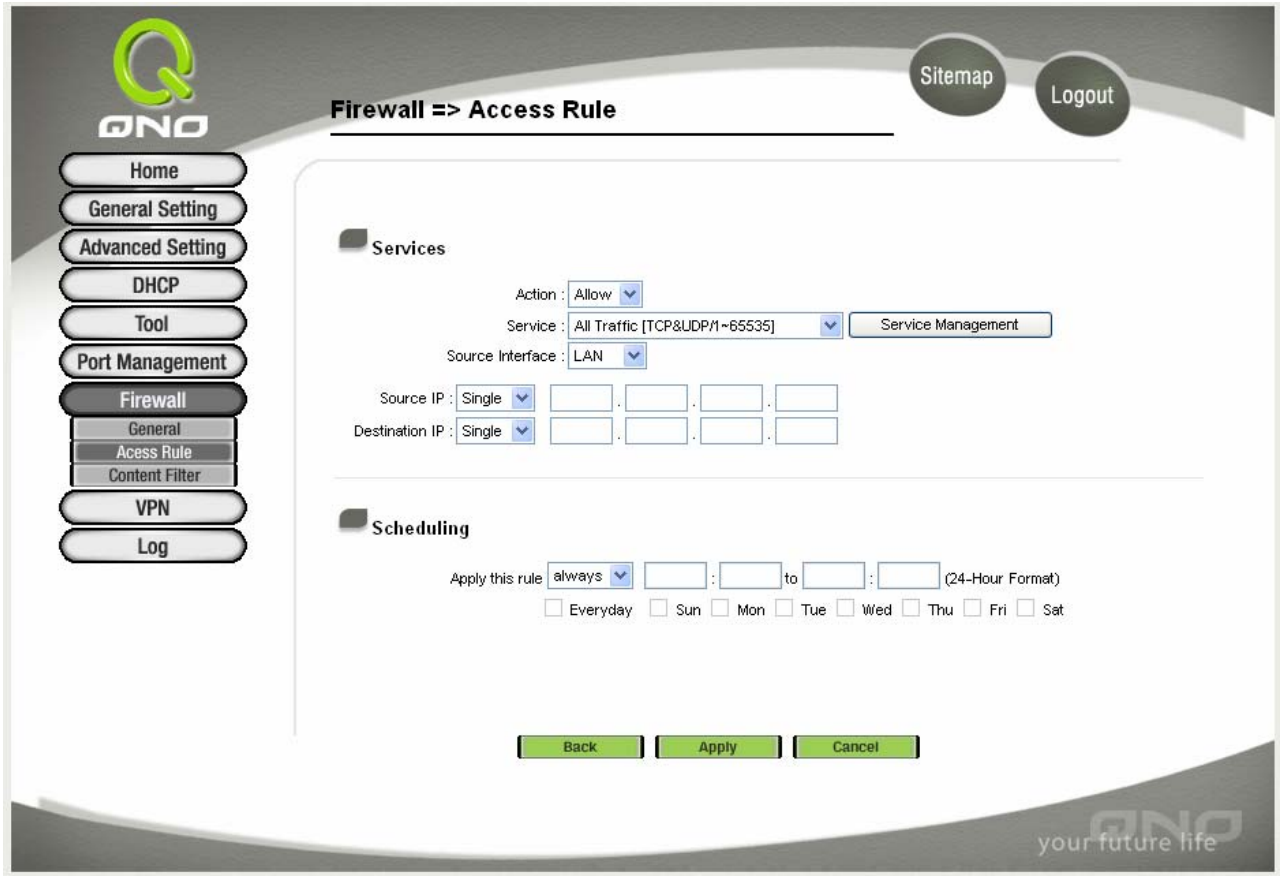
* HTTP 的服务从 LAN 端到 QVM1000 预设为开启的。(为了管理 QVM1000 使用)
* DHCP 的服务从 LAN 端到 QVM1000 预设为开启的。 (为了从 QVM1000 自动取得 IP 位置使用)
* DNS 的服务从 LAN 端到 QVM1000 预设为开启的。 (为了解析 DNS 服务使用)
* Ping 的服务从 LAN 端到 QVM1000 预设为开启的。(为了连通测试 QVM1000 使用)



除了预设规则以外， 所有的网络存取规则都会显示于此规则列表中，您可以依照或是自己选择高低优先权 (**Priority)** 于每一个网络存取规则项目中。 按下 Edit 按钮可以设定网络存取规则项目， 以及按下 Trash Can icon 可以删除网络存取规则项目。

按下 **Add New Rule** 新增新的网络存取规则按钮可以新增一项新的存取规则， 或是按下 **Restore to Default Rules** 可以回复原有预设存取规则项目， 以及删除所有的自订规则内容回到出厂预设存取规则。

Add a new Rule-增加新的管制规则

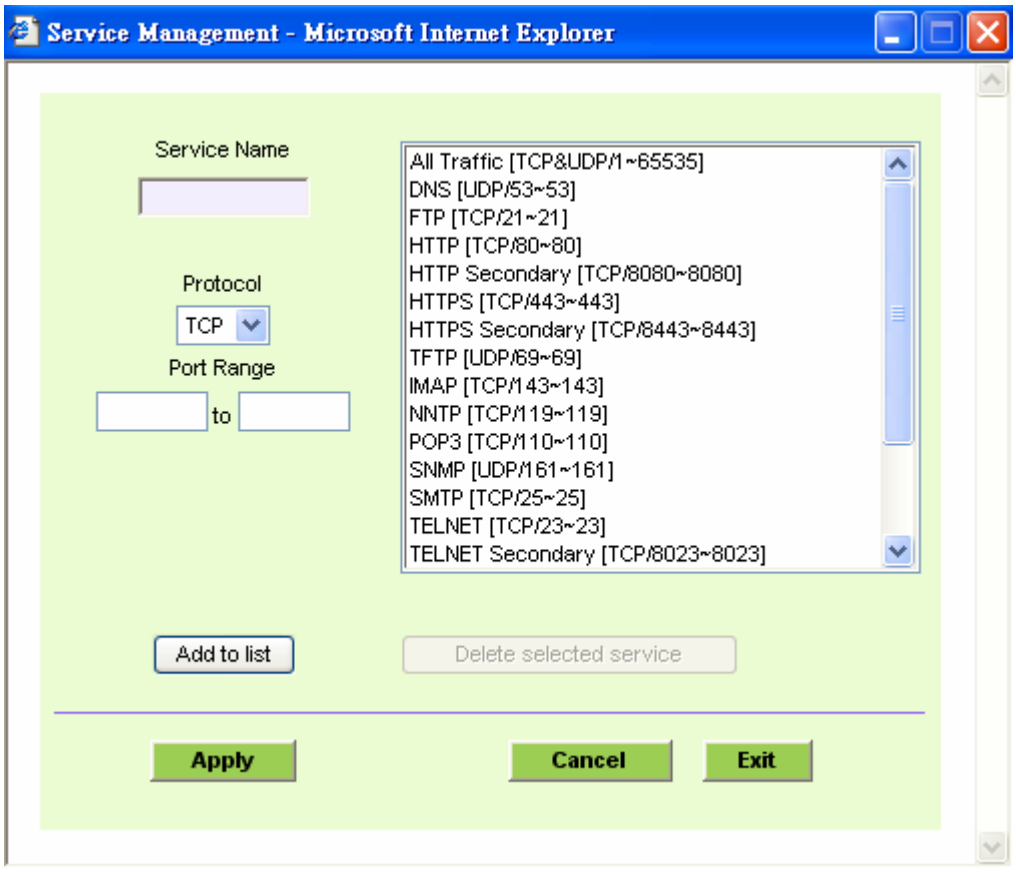


Services-服务管制内容

Action:	此为设定 QVM1000 的管制条例动作: **Allow:**允许此管制条例通过 **Deny:**关闭此管制条例
Service:	选择服务项目内容，可以上下做选单的选择。
Service Management:	若是您想要管制的服务内容没有存在于预设列表内的话，您可以按下右方的 **Service Management** –服务管理 新增一个服务内容，输入一个服务名称-Service Name 以及通讯协议与端口- Protocol & Port ，以及按下 Add-新增按钮即可新增一个管制服务项目内容。
Log:	使用者可以选择是否要将此管制条例存入 Log。若是符合此件的话，将此 Log 存入或是不需要 Log 的信息

Source Interface:	选择来源的封包位置接口(如 LAN， WAN1~WAN4， Any)项目内容，可以上下做选单的选择。
Source IP:	选择来源封包的 IP 位置(如 **Any**， **Single** or **Range**)，若是选择 Single 或是 Range 的话，请输入此单一或是一区段范围的 IP 位置。
Destination IP:	选择目的端封包的 IP 位置(如 **Any**， **Single** or **Range**)，若是选择 Single 或是 Range 的话，请输入此单一或是一区段范围的 IP 位置。
Scheduling:	是否需要将此管制条例安排于特定的管制时间设定
Apply this rule (time parameter):	可选择 **Always**(预设)-都关闭或开启，或是选择 **From** 每周那一天及从几点到几点做管制

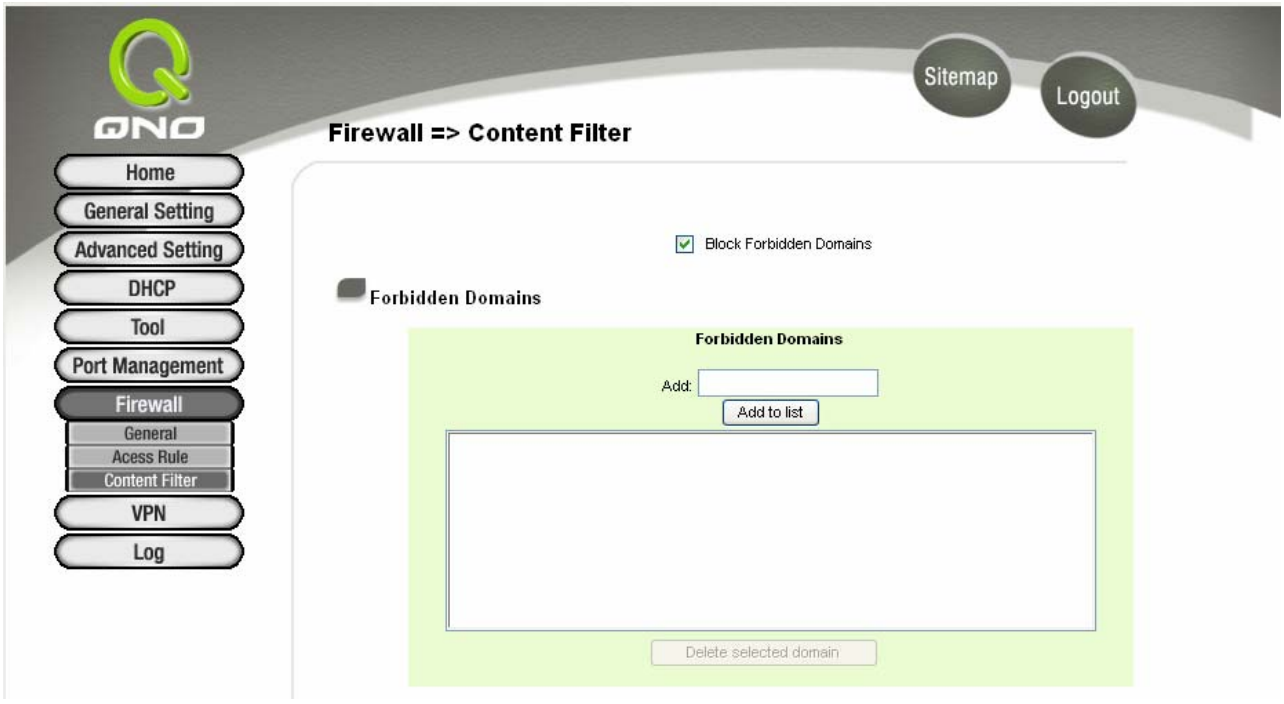
Services Management:管制服务项目管理



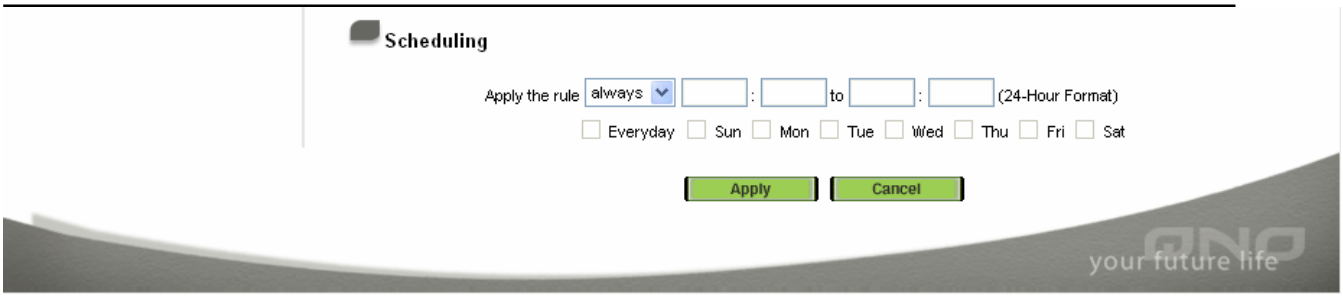
Services Name:	新增服务项目内容，可自订名称。
Protocol:	新增服务项目通讯协议为 TCP 或是 UDP 封包格式。
Port Range:	设定开启此服务的端口位置范围，如 Port 从 9000~9002。

Add to List:	增加此新增的服务项目内容到服务表列内
Delete Selected Services:	选择删除服务项目内容从服务表列内
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。
Delete:	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效
Exit:	退出此服务表管理画面

Content Filter-网页内容管制



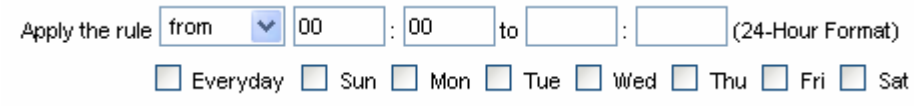
Block Forbidden Domains:	选择打勾开启网页内容管制功能，预设为关闭
Forbidden Domains:	网页管制内容项目。
Add:	填写欲管制的网页内容，如 www.playboy.com
Add to List:	按下 Add 按钮新增此一欲管制的网页内容。
Delete Selected Domain:	可以使用鼠标点选一个或多个管制的网页内容，然后按下即可删除



Scheduling-管制时间

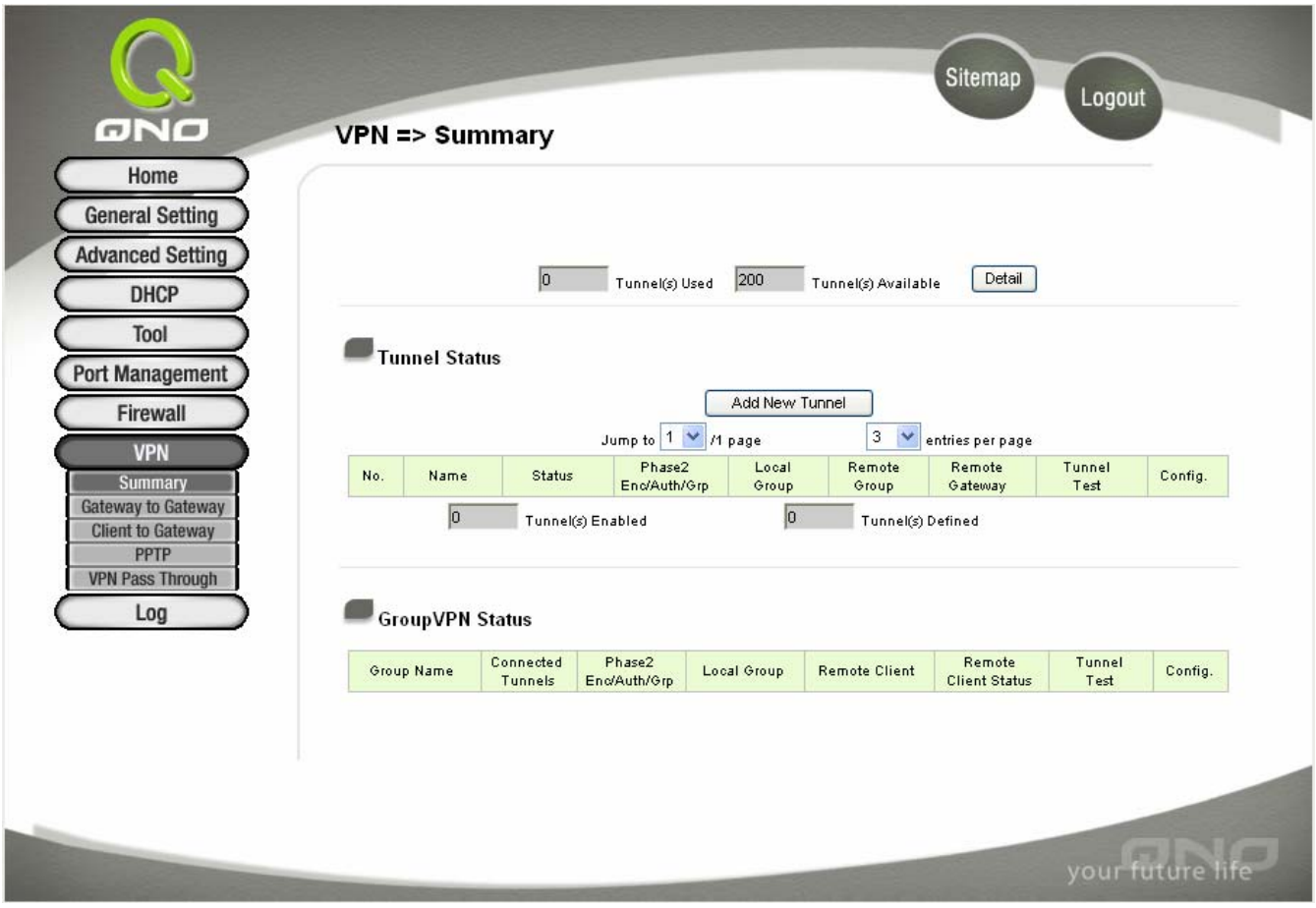
此日期与时间项目功能为管制该条例所生效的实际时间才进行管制，如管制时间为周一到周五，早上八点到下午六点，您可以依照以下说明适当的管制您所需要的时间参数设定。

Apply this rule:



Apply this rule):	选择打勾开启网页内容管制功能，预设为关闭
Time parameter:	**Always:** 此管制规则持续开启
	From:从何时到何时
	…to…: 此管制规则有时间限制内容，设定为 24 小时制，如 08:00 to 18:00 (早上 8 点到下午 6 点)。
Day:	勾选 Every Day 每一天，或是依照实际的需要时间做管制

VPN-虚拟私有网络



Summary-目前所有的 VPN 状态显示

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

Summary:

此为显示目前有多少VPN信道已经设定使用，还剩下多少信道可以提供设定，QVM1000 可同时支持共200 组 VPN 信道(tunnels)。

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

WAN1 IP: 192.168.5.140 WAN2 IP: 0.0.0.0 WAN3 IP: 0.0.0.0 WAN4 IP: 0.0.0.0 Wed Sep 1 06:01:03 2004

No.	Name	Status	Phase 2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway

Close

Tunnel Status: VPN 信道目前状态显示

Tunnel Status

Add New Tunnel

Jump to 1 /1 page 3 entries per page

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.

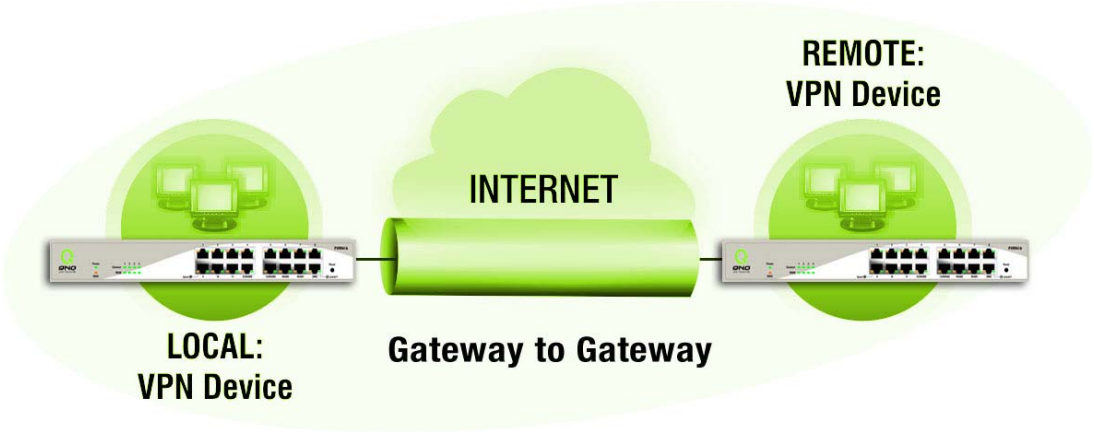
0 Tunnel(s) Enabled 0 Tunnel(s) Defined

Add New Tunnel: 新增一条 VPN 信道设定

QVM1000 可以支持包含 **Gateway to Gateway Tunnel 或是 Client to Gateway Tunnel**

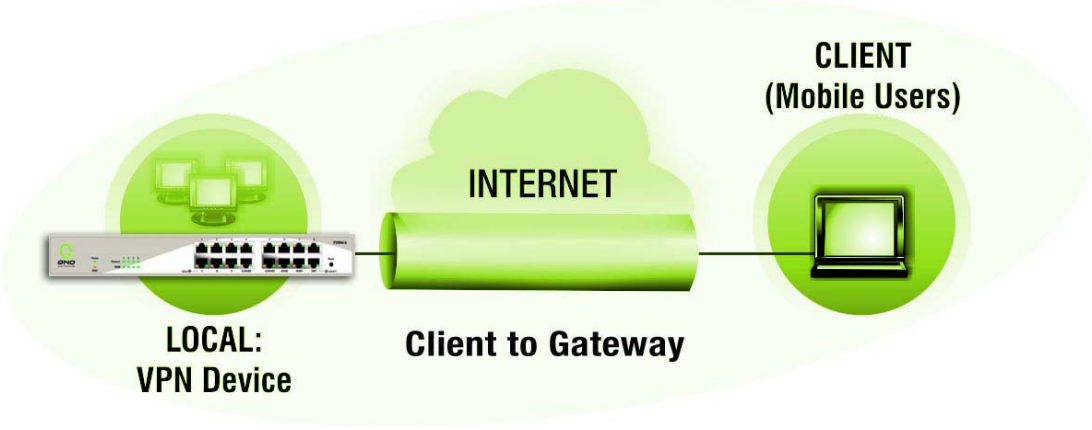
Gateway to Gateway:

以下的 VPN 网络连接为运作于 Gateway to Gateway 模式环境，VPN 信道连接为 2 台 VPN 路由器分别通过网际网络 Internet 所组成，当您按下新增“Add Now” 的话， 将会直接导引到 **Gateway to Gateway** 的设定页面上。



Client to Gateway:

以下的 VPN 网络连接为运作于 Client to Gateway 模式环境，VPN 信道连接为一台 PC 以及一台 VPN 路由器分别通过网际网络 Internet 所组成，当您按下新增“Add Now” 的话，将会直接导引到 **Client to Gateway** 的设定页面上。



以下就针对"**Tunnel Status"** VPN 信道目前状态显示做完整解说:

Page: Previous page，Next page， Jump to page / 200 pages and entries per page	您可以按下上一页(Previous page)与下一页(Next page)按钮跳到您想监看的VPN信道画面上,或者您可以直接选择每一次所显示的页次，来监看您的所有 VPN 信道状态，如(3， 5， 10， 20， All)。
Tunnel No	当您设定 QVM1000 内建之 VPN 功能时，请选择您要设定的 Tunnel 信道编号，最多可支持 200 条 VPN 信道设定(Gateway To Gateway 或 Client To Gateway
Status:	于此状态显示已经联机成功-Connected，计算机联机名称-Hostname Resolution Failed， Resolving Hostname 以及等待联机-Waiting for Connection 等信息，若是管理者选择手动-Manual 设定 IPSec 信道，则此状态会显示手动-Manual 设定与没有测试此项手动设定功能状态模式
Name:	目前联机 VPN 信道连接名称，如 XXX Office，建议您若是有一个以上的信道设定的话，务必将每一个信道名称都设为不同，以免混淆
	Note: 此信道名称若是您需要连接其它 VPN 设备(非 QVM1000)时，有一些设备规定此信道名称要与主控端为相同名称并做验证，此信道才会顺利联机开启。
Phase2 Encrypt/Auth/Group:	于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设定模式。 若是您选择手动(Manual)设定 IPSec 的话，于此将不会显示 Phase 2 DH 群组
Local Group:	此为显示本地区域端的 VPN 联机安全群组设定
Remote Group:	此为显示远程的 VPN 联机安全群组设定
Remote Gateway:	此为设定为欲与远程 VPN 设备联机的 IP 位置，请设定为远程的 VPN 路由器的对外合法 IP 位置或是 Domain Name 等
Tunnel Test:	可以按下连接按钮-Connect 去验证此信道的状态，测试结果将会更新于此状态上。
Configure:	设定项目包含编辑-Edit 以及删除图标

若您按下编辑按钮- Edit ， 将会连接到此设定的项目当中，您可以修改其中的设定。 若您选择按下垃圾桶图标的话 ，所有此信道的设定将会被删除。

Tunnel(s) Enable and Tunnel(s) Defined: 于此显示此信道是否开启 (Tunnel(s) Enable)以及此信道是否已经设定过(Tunnel(s) Defined)。

GroupVPN Status: 群组 VPN 状态显示

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

Group ID Name: 目前设定联机 GroupVPNs 信道连接名称。

Connected Tunnels: 于此显示已经联机的 VPNGroups 信道。

Phase2 Encrypt/Auth/Group: 于此显示加密(DES/3DES)以及验证(MD5/SHA1)以及群组 Group (1/2/5)等设定模式。
若是您选择手动(Manual)设定 IPSec 的话，于此将不会显示 Phase 2 DH 群组

Local Group: 此为显示本地区域端的群组 VPN 联机安全群组设定

Remote Client: 此为显示此 GroupVPN。远程的 VPN 联机安全群组设定

Remote Clients Status: 若您按下更多信息列表(Detail List) 按钮， 此将会显示更多有关信息，包含群组名称(Group Name)，IP 位置(IP Address)以及联机时间信息等。

Tunnel Test: 可以按下连接按钮-Connect 去验证此信道的状态，测试结果将会更新于此状态上。

Config: 如下图所示，设定项目包含编辑-Edit 以及删除图标

若您按下编辑按钮- Edit ， 将会连接到此设定的项目当中，您可以修改其中的设定。 若您选择按下垃圾桶图标的话 ，所有此信道的设定将会被删除。

。

Add New Tunnel-新增一条 VPN 信道

Gateway to Gateway-VPN 网关对网关的设定

透过以下的设定说明，使用者就可以在两台 QVM1000 之间建立一条 VPN 信道。

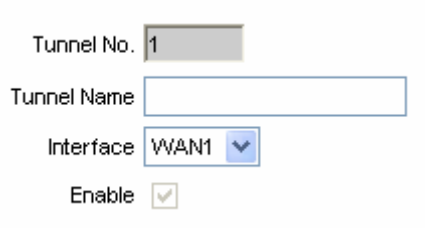
Tunnel No。: 当您设定 QVM1000 内建之 VPN 功能时，请选择您要设定的 Tunnel 信道编号，QVM1000 可支持最高 200 条 VPN 信道设定

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

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

> **Note:** 此信道名称若是您需要连接其它 VPN 设备(非 QVM1000)时，有一些设备规定此信道名称要与主控端为相同名称并做验证，此信道才会顺利联机开启！。

Enable: 勾选 Enable 选项，将此 VPN 信道开启。此项目为预设为激活 Eanble，当设定完成后，可以再选择是否激活信道设定。

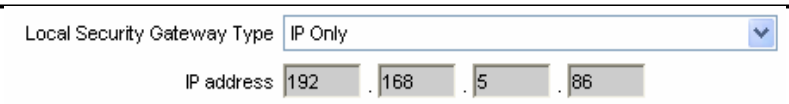


Local Group Setup: 此项目的近端网关安全群组设定**(Local Security Gateway Type)**类型必须与连接远程的网关安全群组设定**(Remote Security Gateway Type)**类型相同。

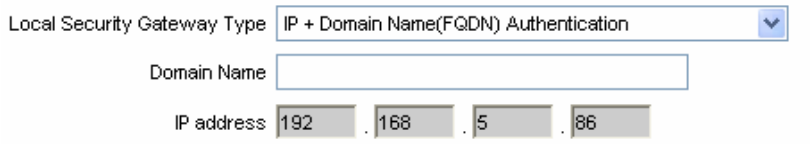
Local Security Gateway Type: 区域端群组设定，有五种操作模式项目选择，分别为:
IP Only-只使用 IP 作为认证
IP + Domain Name(FQDN) Authentication，-IP+网域名称
IP + E-mail Addr。(USER FQDN) Authentication，-IP+电子邮件
Dynamic IP + Domain Name(FQDN) Authentication，-动态 IP 位置+网域名称
Dynamic IP + E-mail Addr。(USER FQDN) Authentication。 动态 IP 位置+电子邮件名称

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

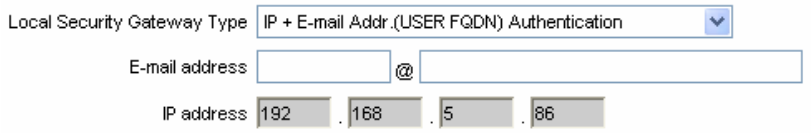
(1) IP Only: 若您选择 IP Only 类型的话， 只有固定填入此 IP 位置可以存取此信道，然后 QVM1000 的 WAN IP 位置，将会自动填入此项目空格内，您不需要在进行额外设定。



(2) IP + Domain Name(FQDN) Authentication:若您选择 IP +网域名称类型的话,请输入您所验证的网域名称以及 IP 位置然后 QVM1000 的 WAN IP 位置，将会自动填入此项目空格内，您不需要在进行额外设定。 FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com。此 IP 位置以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

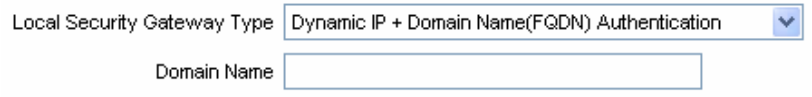


(3) IP + E-mail Addr。(USER FQDN) Authentication: 若您选择 IP 位置加上电子邮件类型的话， 只有固定填入此 IP 位置以及电子邮件位置可以存取此信道，然后 QVM1000 的 WAN IP 位置，将会自动填入此项目空格内，您不需要在进行额外设定

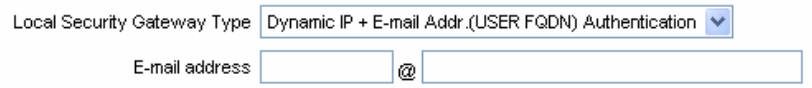


(4) Dynamic IP + Domain Name(FQDN) Authentication:

若是您使用动态 IP 位置连接 QVM1000 时， 您可以选择此类型连接 VPN， ，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时， QVM1000 将会开始验证并响应此 VPN 信道联机; 若您选择此类型连接 VPN，请输入网域名称即可



(5) Dynamic IP + E-mail Addr。(USER FQDN) Authentication: 若是您使用动态 IP 位置连接 QVM1000 时， 您可以选择此类型连接 VPN，使用者不必输入 IP 位置，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时， QVM1000 将会开始验证并响应此 VPN 信道联机; 若您选择此类型连接 VPN，请输入电子邮件认证到 E-Mail 位置空格字段中即可



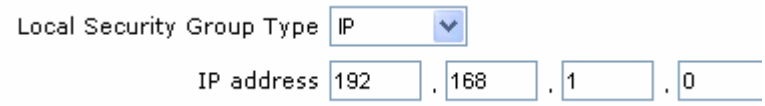
Local Security Group Type

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

(1) **IP Address**

此项目为允许此 VPN 信道联机后，只有输入此 IP 位置的本地端

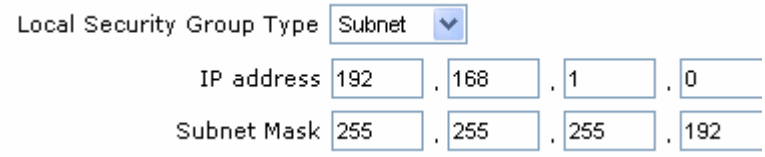
计算机可以联机。



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

(2) **Subnet**

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



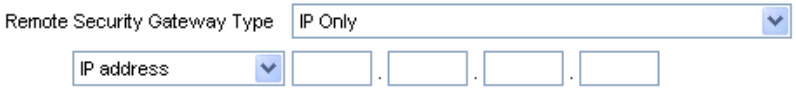
以上的设定参考为:当此 VPN 信道联机后，只有 192.168.1.0，子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机

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

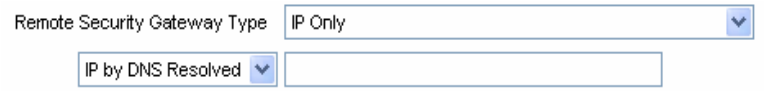
Remote Security Gateway Type:

远程安全群组设定，有五种操作模式项目选择，分别为:
IP Only-只使用 IP 作为认证
IP + Domain Name(FQDN) Authentication，-IP+网域名称
IP + E-mail Addr。(USER FQDN) Authentication，-IP+电子邮件
Dynamic IP + Domain Name(FQDN) Authentication，-动态 IP 位置+网域名称
Dynamic IP + E-mail Addr。(USER FQDN) Authentication。 动态 IP 位置+电子邮件名称

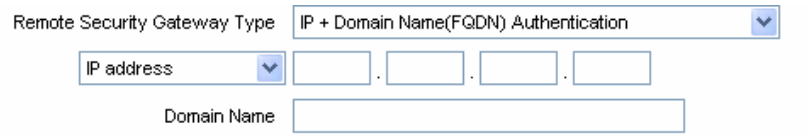
(1) IP Only: 若您选择 IP Only 类型的话， 只有固定填入此 IP 位置可以存取此信道，



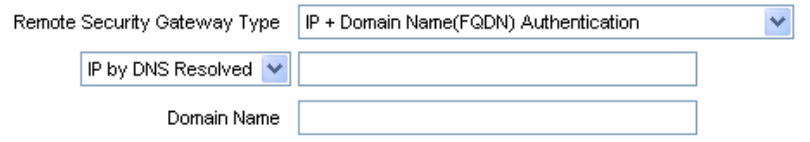
若是使用者不知道远程客户的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP address。



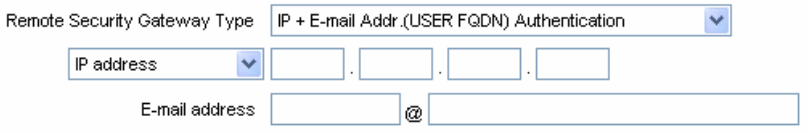
(2) IP + Domain Name(FQDN) Authentication:若您选择 IP +网域名称类型的话，请输入 IP 位置以及您所验证的网域名称 FQDN 是指主机名称以及网域名称的结合，使用者可以输入一个符合 FQDN 的网域名称即可。此 IP 位置以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。



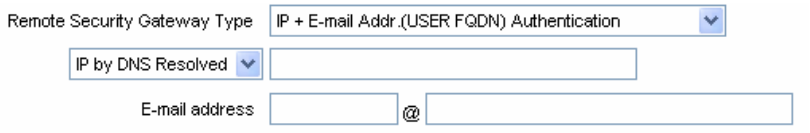
若是使用者不知道远程的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。此网域名称必须存在 Internet 上可以查询的到。并且在设定完成后在 Summary 的远程网关下面自动显示出相对应的 IP address。



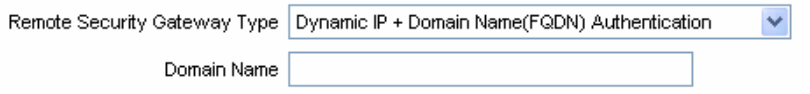
(3) IP + E-mail Addr。(USER FQDN) Authentication: 若您选择 IP 位置加上电子邮件类型的话，只有固定填入此 IP 位置以及电子邮件位置可以存取此信道，



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

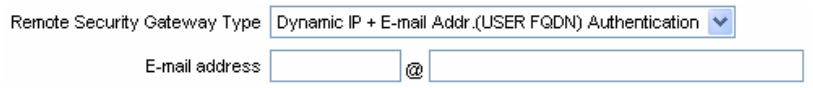


(4) Dynamic IP + Domain Name(FQDN) Authentication: 若是您使用动态 IP 位置连接 QVM1000 时，您可以选择动态 IP 位置加上主机名称以及网域名称的结合



(5) Dynamic IP + E-mail Addr。(USER FQDN) Authentication: 若是您使用动态 IP 位置连接 QVM1000 时，您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时，QVM1000 将会开始验证并响应此 VPN 信道联机; 请输入电子邮

件认证到 E-Mail 位置空格字段中

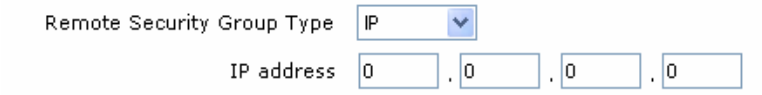


Remote Security Group Type:

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

(1) IP Address

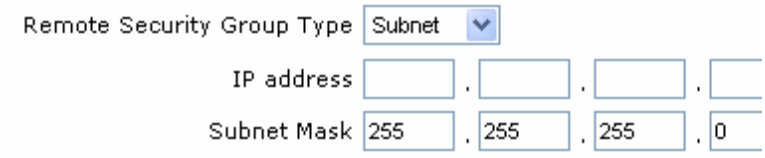
此项目为允许此 VPN 信道联机后，只有输入此 IP 位置的本地端计算机可以联机。



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

(2)Subnet

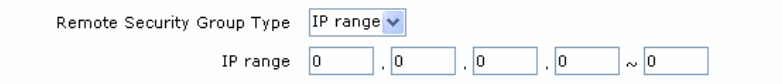
此项目为允许此 VPN 信道联机后，每一台于此网段的本地端计算机都可以联机。。



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

(3)IP Range

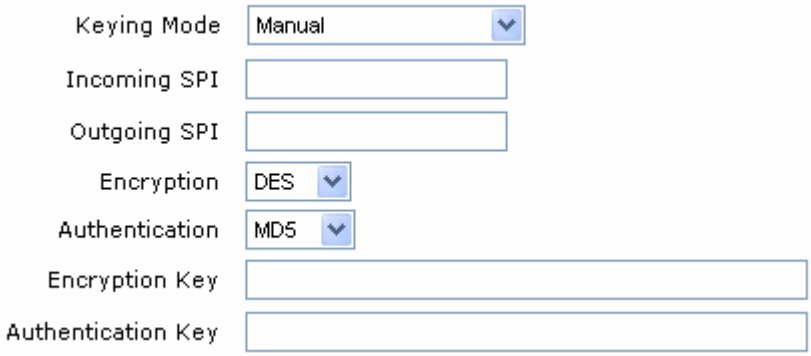
此项目为允许此 VPN 信道联机后，只有输入此 IP 位置范围的本地端计算机可以联机



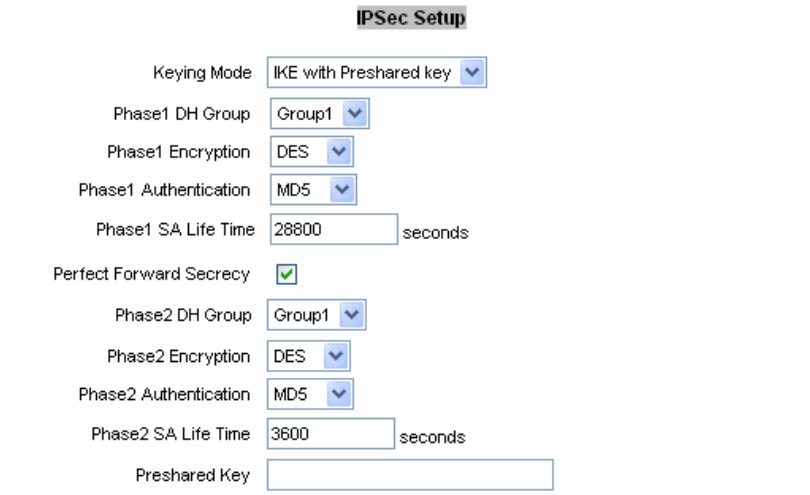
以上的设定参考为:当此 VPN 信道联机后，只有 192.168.1.0 到 192.168.1.254 的 IP 位置范围的计算机可以联机

IPSec Setup

若是任何加密机制存在的话， 此两个 VPN 信道的加密机制必须要相同才可以将此信道连接，并于传输资料中加上标准的 IPSec 密钥，我们称为加密密钥 “key” 。 QVM1000 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)**如下图所示。



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



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

PFS:若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。

Phase1/Phase2 DH Group:

于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。

Phase1/Phase2 Encryption:
此加密选项设定为设定此 VPN 信道使用何种加密模式，并请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。

Phase1/Phase2 Authentication:

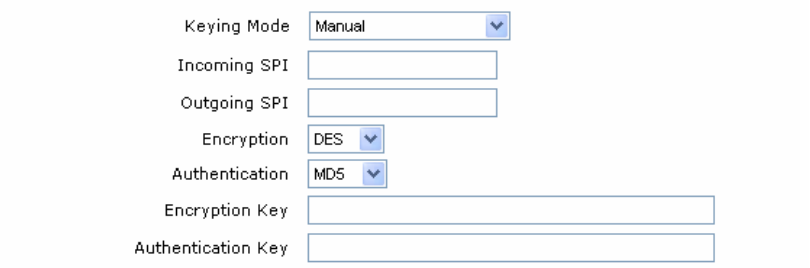
此验证选项设定为设定此 VPN 信道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:
“**MD5”/“SHA”**。

Phase1 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。

Phase2 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

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

Manual-手动方式



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

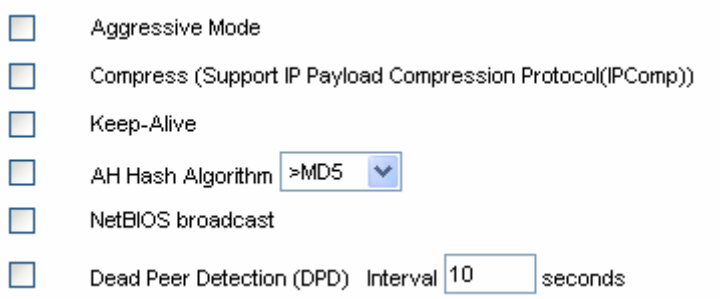
Manual 为手动方式设定交换密码，于此分成加密密码“**Encryption KEY**”以及验证密码“**Authentication KEY**”二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。

另外还需要设定“**Inbound SPI”**的交换字符串以及“**Outbound SPI”** 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Inbound SPI 设定参数，您必须在远程的 VPN 设备的 Outbound SPI 设定相同字符串，而于本地端的 Outbound SPI 设定字符串，也必须与在远程的 VPN 设备的 Inbound SPI 设定相同字符串！

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

Advanced settings are only for IKE with Preshared Key mode of IPSec。

Advance Mode:(进阶作业模式)



在 QVM1000 的进阶设定项目中，分别有主要模式 **Main Mode** 以及进阶模式 **Aggressive Mode**， Main mode 是 QVM1000 的预设 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;另外 Aggressive mode 大多为远程的设备采用，如使用动态 IP 连接时，为了加强其安全控管机制，。

Compress:
若选择此项目勾选，则连接的 VPN 信道中 QVM1000 支持 IP 表头型态的压缩(IP Payload compression Protocol)。

Keep-Alive:
若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 位置的远程使用。

AH Hash Algorithm:
AH (Authentication Header) 验证表头封包格式，可选择 MD5/DSHA-1

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

Dead Peer Detection(DPD):

若选择此项目勾选，则连接的 VPN 信道中会定期的传送 HELLO/ACK 讯息封包来侦测是否 VPN 信道的两端仍有联机存在。当有一端断线则 QVM1000 会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息封包传递的时间，默认值为 10 秒。

Client to Gateway-VPN 客户端对网关的设定

透过以下的设定说明，管理人员就可以在客户端与 QVM1000 之间建立一条 VPN 信道。

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

在 Tunnel 的情况:

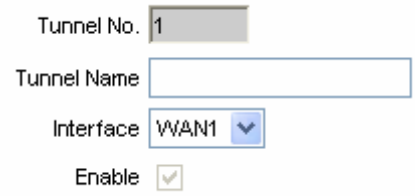
Tunnel No。: 当您设定 QVM1000 内建之 VPN 功能时，请选择您要设定的 Tunnel 信道编号，QVM1000 可支持最高 200VPN 信道设定。

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

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

> **Note:** 此信道名称若是您需要连接其它 VPN 设备(非 QVM1000)时，有一些设备规定此信道名称要与主控端为相同名称并做验证，此信道才会顺利联机开启！。

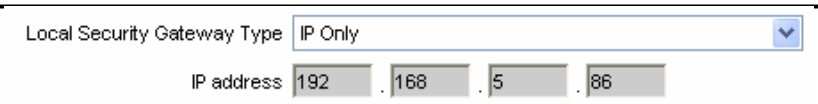
Enable: 勾选 Enable 选项，将此 VPN 信道开启。此项目为预设为激活 Eanble，当设定完成后可以再选择是否激活信道设定。



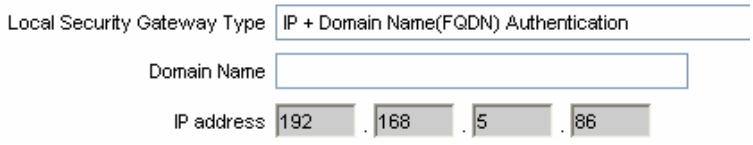
Local Group Setup: 此项目的近端网关安全群组设定**(Local Security Gateway Type)**型态必须与连接远程的网关安全群组设定**(Remote Security Gateway Type)**型态相同。

Local Security Gateway Type: 区域端群组设定，有五种操作模式项目选择，分别为:
IP Only-只使用 IP 作为认证
IP + Domain Name(FQDN) Authentication，-IP+网域名称
IP + E-mail Addr。(USER FQDN) Authentication，-IP+电子邮件
Dynamic IP + Domain Name(FQDN) Authentication，-动态 IP 位置+网域名称
Dynamic IP + E-mail Addr。(USER FQDN) Authentication。 动态 IP 位置+电子邮件名称

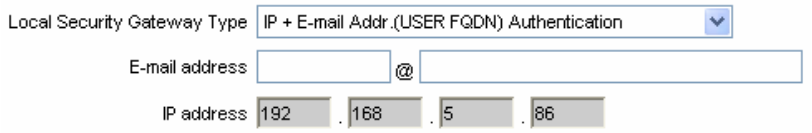
(1) IP Only: 若您选择 IP Only 类型的话，FVR 9416 会依据你所选择的广域端口位置将其 IP 自动填入此项目空格内，您不需要在进行额外设定。



(2) IP + Domain Name(FQDN) Authentication: 若您选择 IP+网域名称类型的话，请输入您所验证的网域名称，QVM1000 的 WAN IP 位置，将会自动填入 IP Address 项目内，您不需要在进行额外设定。 FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn。server。com。此 IP 位置以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。

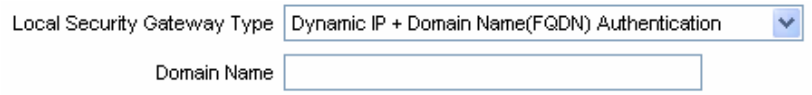


(3) IP + E-mail Addr 。(USER FQDN) Authentication: 若您选择 IP 位置加上电子邮件类型的话，只要将电子邮件位置填入，然后 QVM1000 的 WAN IP 位置，将会自动填入此项目空格内，您不需要在进行额外设定

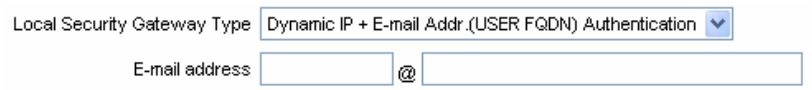


(4) Dynamic IP + Domain Name(FQDN) Authentication:

若是您使用动态 IP 位置连接 QVM1000 时，您可以选择此类型连接 VPN，，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时，QVM1000 将会开始验证并响应此 VPN 信道联机; 若您选择此类型连接 VPN，请输入网域名称即可



(5) Dynamic IP + E-mail Addr。(USER FQDN) Authentication: 若是您使用动态 IP 位置连接 QVM1000 时，您可以选择此类型连接 VPN，使用者不必输入 IP 位置，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时，QVM1000 将会开始验证并响应此 VPN 信道联机;请输入电子邮件认证到 E-Mail 位置空格字段中即可

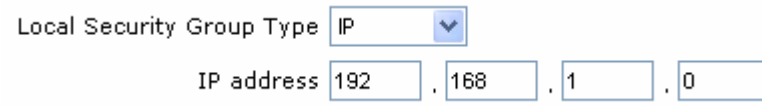


Local Security Group Type

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

(1)IP Address(单一 IP 地址)
此项目为允许此 VPN 信道联机后，只有输入此 IP 位置的本地端计算

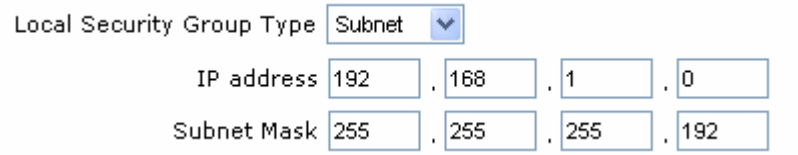
机可以联机。



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

(2)Subnet

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



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

Remote Client Setup 远程客户端设定 ：

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

Remot Client: 远程客户设定，有五种操作模式项目选择，分别为:

IP Only-只使用 IP 作为认证

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

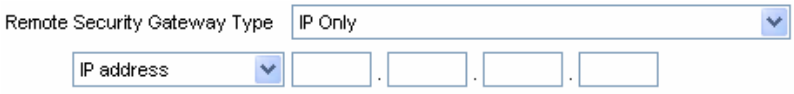
IP + E-mail Addr。(USER FQDN) Authentication，-IP+电子邮件

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

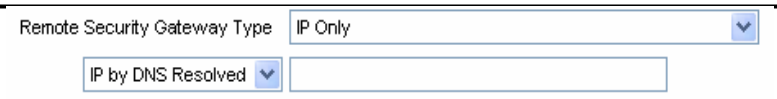
Dynamic IP + E-mail Addr。(USER FQDN) Authentication。 动态 IP 位置+电子邮件名称

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

(1) IP Only: 若您选择 IP Only 类型的话，只有固定填入此 IP 位置可以存取此信道，

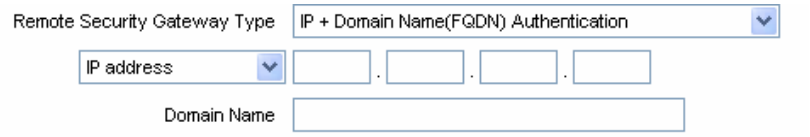


若是使用者不知道远程客户的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP address。

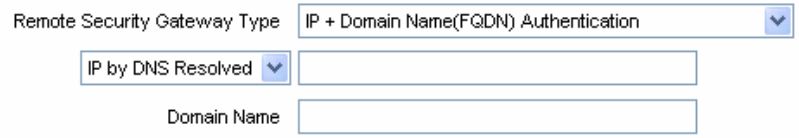


(3) **IP+Domain Name(FQDN) Authentication**:

若您选择 IP+网域名称类型的话，请输入 IP 位置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 位置以及网域名称必须与远程的 VPN 安全网关设定类型相同才可以正确连接。



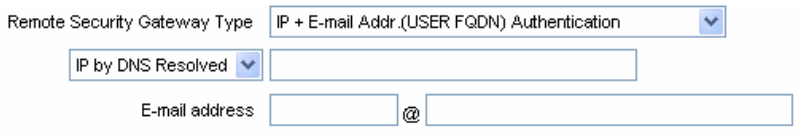
若是使用者不知道远程的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。此网域名称必须存在 Internet 上可以查询的到。并且在设定完成后在 Summary 的远程网关下面自动显示出相对应的 IP address。



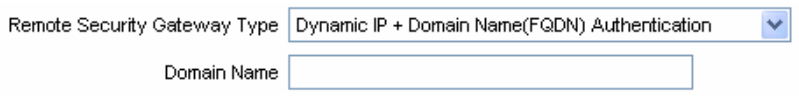
(4) **IP + E-mail Addr。(USER FQDN) Authentication**: 若您选择 IP 位置加上电子邮件类型的话， 只有固定填入此 IP 位置以及电子邮件位置可以存取此信道

(5)

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

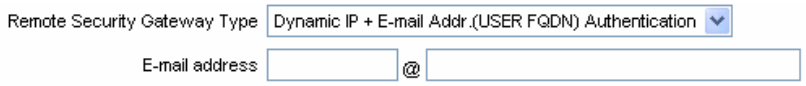


(4) **Dynamic IP + Domain Name(FQDN) Authentication:** 若是您使用动态 IP 位置连接 QVM1000 时，您可以选择动态 IP 位置加上主机名称以及网域名称的结合



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

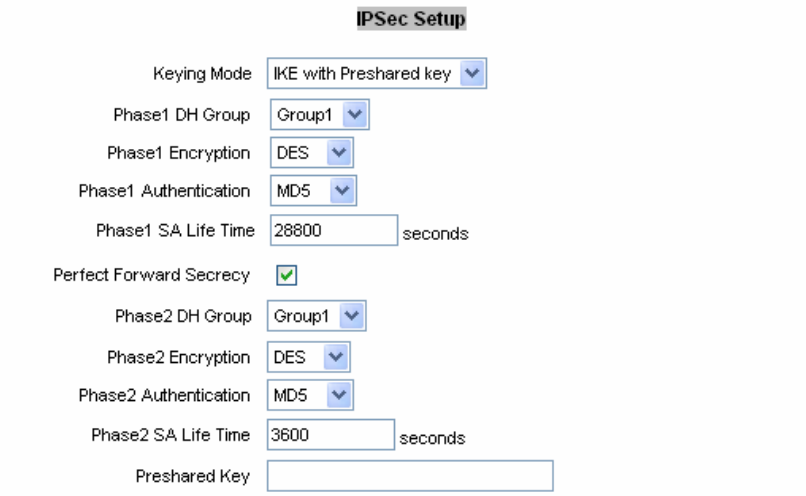
是您使用动态 IP 位置连接 QVM1000 时，您可以选择此类型连接 VPN，当远程的 VPN 网关要求与 QVM1000 作为 VPN 联机时，QVM1000 将会开始验证并响应此 VPN 信道联机; 请输入电子邮件认证到 E-Mail 位置空格字段中



IPSec Setup

若是任何加密机制存在的话， 此两个 VPN 信道的加密机制必须要相同才可以将此信道连接，并于传输资料中加上标准的 IPSec 密钥，于此我们称为加密密钥 “key” 。 QVM1000 提供了以下二种加密管理模式，分别为手动(**Manual**) 以及 IKE 自动加密模式- **IKE with Preshared Key (automatic)**如下图所示。

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



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

PFS:若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。

Phase1/Phase2 DH Group:

于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是

Group2/Group5。

Phase1/Phase2 Encryption:
此加密选项设定为设定此 VPN 信道使用何种加密模式，并请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。

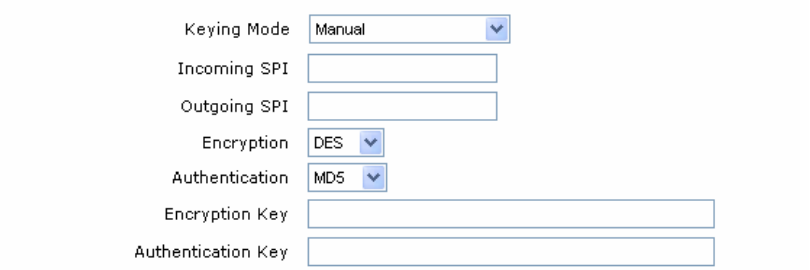
Phase1/Phase2 Authentication:
此验证选项设定为设定此 VPN 信道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:
“**MD5”/“SHA”**。

Phase1 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。

Phase2 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

Preshared Key:于 **Auto (IKE)，** 选项中，您必须输入一组交换密码于 **“Pre-shared Key”** 的字段中，在此的范例设定为 **test**，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。

Manual-手动方式



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

Manual 为手动方式设定交换密码，于此分成加密密码“**Encryption KEY**”以及验证密码“**Authentication KEY**”二种，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 个文字组合。

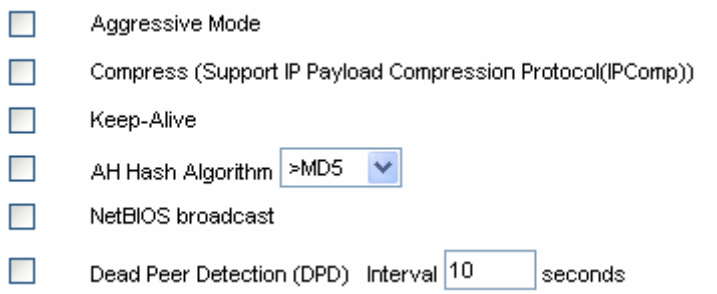
另外还需要设定“**Inbound SPI”**的交换字符串以及“**Outbound SPI”** 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Inbound SPI 设定参数，您必须在远程的 VPN 设备的 Outbound SPI

设定相同字符串，而于本地端的 Outbound SPI 设定字符串，也必须与在远程的 VPN 设备的 Inbound SPI 设定相同字符串！

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

Advanced settings are only for IKE with Preshared Key mode of IPSec。

Advance Mode:(进阶作业模式)



在 QVM1000 的进阶设定项目中，分别有主要模式 **Main Mode** 以及 进阶模式 **Aggressive Mode**， Main mode 是 QVM1000 的预设 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;另外 Aggressive mode 大多为远程的设备采用，如使用动态 IP 连接时，为了加强其安全控管机制，。

Compress:
若选择此项目勾选，则连接的 VPN 信道中 QVM1000 支持 IP 表头型态的压缩(IP Payload compression Protocol)。

Keep-Alive:
若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 位置的远程使用。

AH Hash Algorithm:
AH (Authentication Header) 验证表头封包格式，可选择 MD5/DSHA-1

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

Dead Peer Detection(DPD):

若选择此项目勾选，则连接的 VPN 信道中会定期的传送 HELLO/ACK 讯息封包来侦测是否 VPN 信道的两端仍有联机存在。当有一端断线则 QVM1000 会自动断线，然后再建立新联机。使用者可以选择每一次 DPD 讯息封包传递的时间，默认值为 10 秒。

在 Group VPN 的情况:

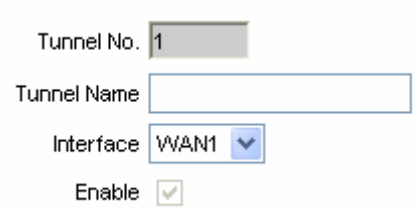
Group No。: 最多可以设定两组 Group VPN。

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

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

Note: 此信道名称若是您需要连接其它 VPN 设备(非 QVM1000)时，有一些设备规定此信道名称要与主控端为相同名称并做验证，此信道才会顺利联机开启！。

Enable: 勾选 Enable 选项，将此 VPN 信道开启。此项目为预设为激活 Eanble，当设定完成后可以再选择是否激活信道设定。

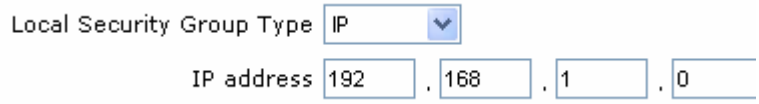


Local Group Setup: 此为设定本地区域端的 VPN 联机安全群组设定，以下有几个关于本地区域端设定的项目，请您选择并设置适当参数:

Local Security Group Type:

(1)IP Address

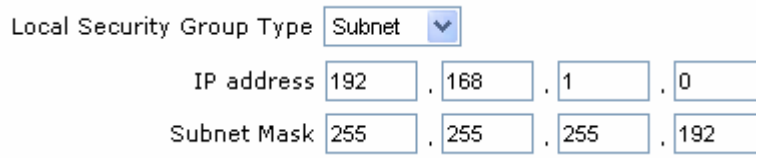
此项目为允许此 VPN 信道联机后，只有输入此 IP 位置的本地端计算机可以联机。



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

(2)Subnet

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



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

***Remote Client Setup**:远程客户端设定*

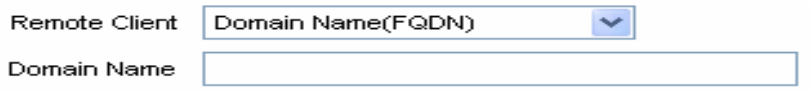
Remote Client: *远程客户端设定*，有三种操作模式项目选择，分别为:

Domain Name(FQDN)，-网域名称

E-mail Address(USER FQDN)，- 电子邮件名称
Microsoft XP/2000 VPN Client，- 微软 XP/2000 VPN 客户端

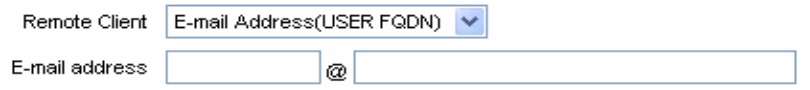
(1) Domain Name(FQDN):

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



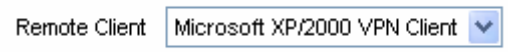
(2) E-mail Addr。(USER FQDN):

若您选择电子邮件类型的话， 只有固定填入此电子邮件位置可以存取此信道



(3) Microsoft XP/2000 VPN Client:

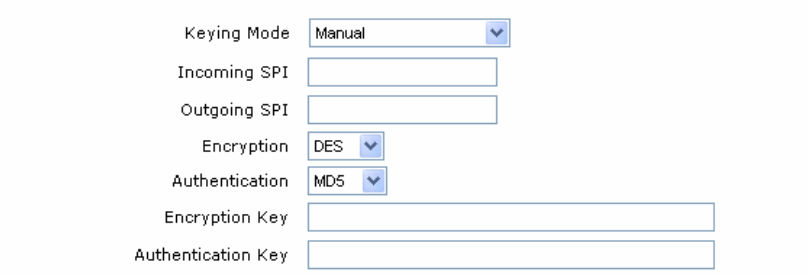
若您选择微软 XP/2000 VPN 客户端型态的话，您不需要在进行额外设定。

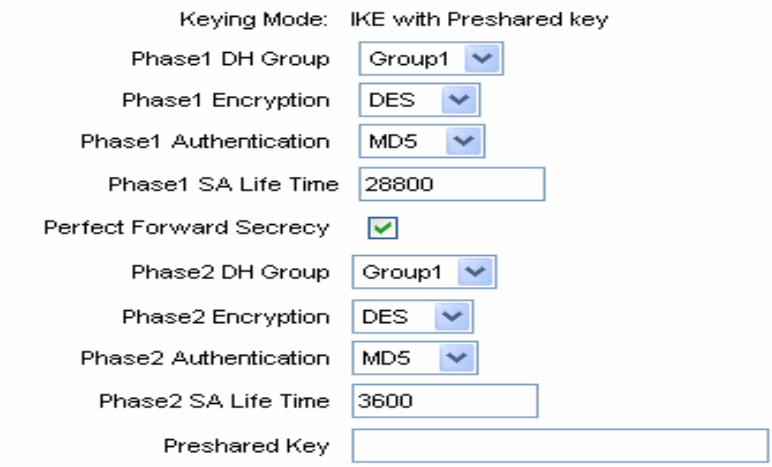


IPSec Setup

若是任何加密机制存在的话， 此两个 VPN 信道的加密机制必须要相同才可以将此信道连接，并于传输资料中加上标准的 IPSec 密钥，于此我们称为加密密钥 “key” 。 QVM1000 提供了以下二种加密管理模式，分别为手动(**Manual**) 以及 IKE 自动加密模式- **IKE with Preshared Key (automatic)**。在选择 Group VPN 的情况之下或者是在远程网关安全型态 Remote Security Gateway Type 中使用动态位置 IP 时，Aggressive mode 会自动激活，没有手动 Manual 模式 。

Key Management:





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

PFS:若您将 PFS 选项勾选后，记得另外的远程 VPN 设备或是 VPN Client 也要将 PFS 功能开启。

Phase1/Phase2 DH Group:

于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5。

Phase1/Phase2 Encryption:
此加密选项设定为设定此 VPN 信道使用何种加密模式，并请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。

Phase1/Phase2 Authentication:
此验证选项设定为设定此 VPN 信道使用何种验证模式，并请注意设置此参数必须与远程的验证模式参数相同:
“**MD5**”/“**SHA**”。
Phase1 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 28800 秒(8 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全。

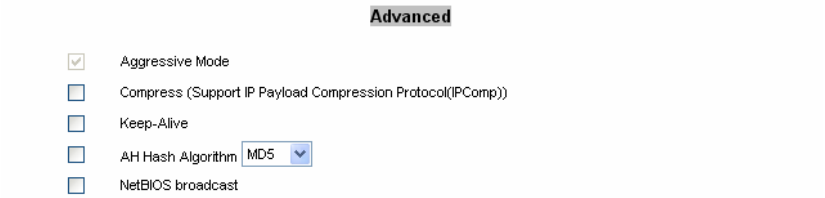
Phase2 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 3600 秒(1 小时)，于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

Preshared Key:于 **Auto (IKE)，** 选项中，您必须输入一组交换密码于 **“Pre-shared Key”** 的字段中，在此的范例设定为 **test**，您可以输入数字或是文字的交换密码，系统将会自动的将您输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制;此数字或是文字的交换密码最高可输入 23 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 Preshareed Key Only)**

Advanced settings are only for IKE with Preshared Key mode of IPSec。

Advance Mode:(进阶作业模式)



在 QVM1000 的进阶设定项目中，分别有 **Main** Mode 以及 **Aggressive**。模式， Main mode 是 QVM1000 的预设 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;另外 Aggressive mode 大多为远程的设备采用，如使用动态 IP 连接时，为了加强其安全控管机制。在选择 Group VPN 时，Aggressive mode 会自动激活。

Compress:
若选择此项目勾选，则连接的 VPN 信道中 QVM1000 支持 IP 表头型态的压缩(IP Payload compression Protocol)。

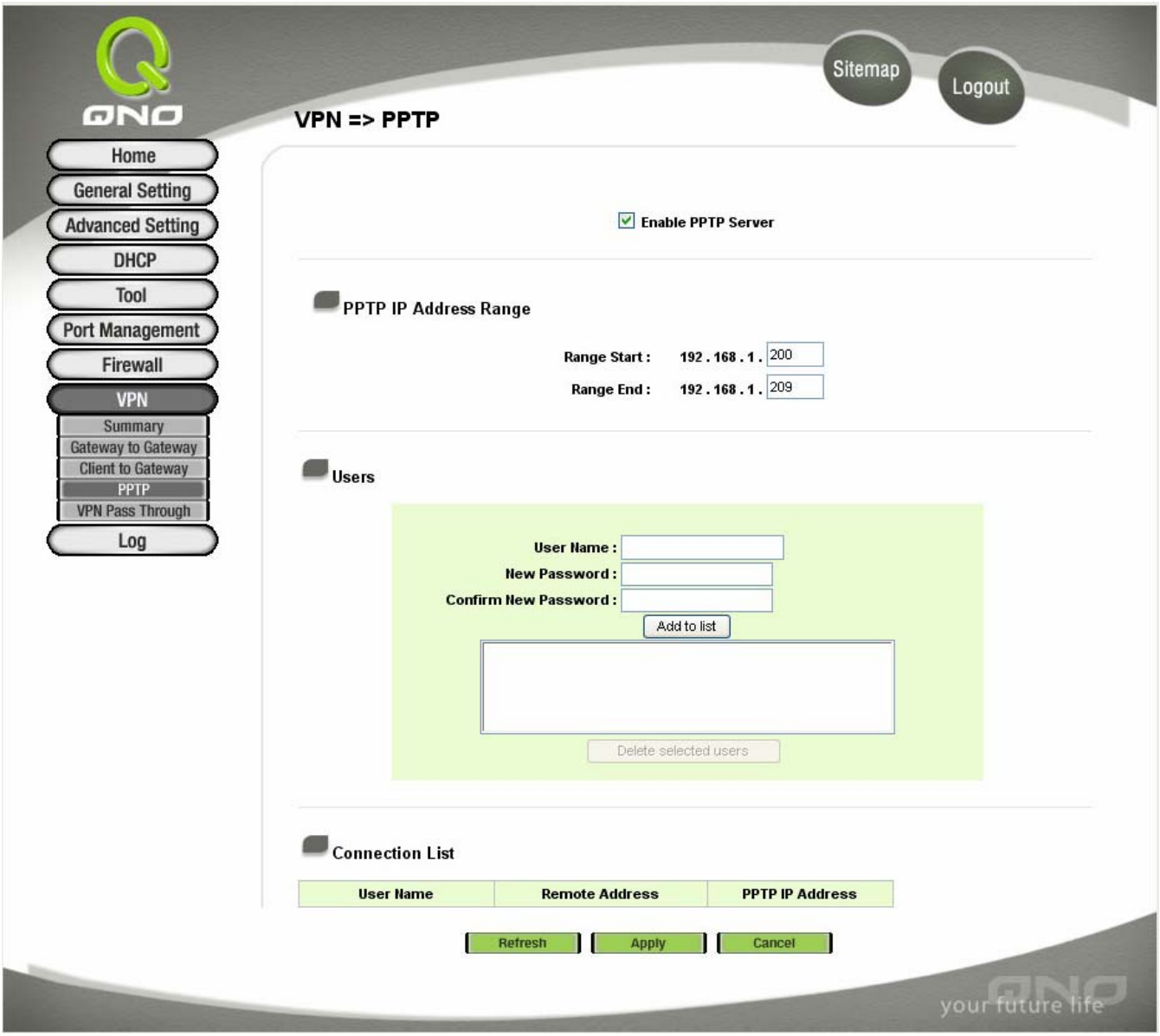
Keep-Alive:
若选择此项目勾选，则连接的 VPN 信道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 位置的远程使用。

AH Hash Algorithm:
AH (Authentication Header) 验证表头封包格式，可选择 MD5/DSHA-1

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

PPTP

QVM1000 提供支持 Window XP/2000 的 PPTP 对我们 QVM1000 做点对点信道协议，让远程使用此种协议建立 VPN 联机。



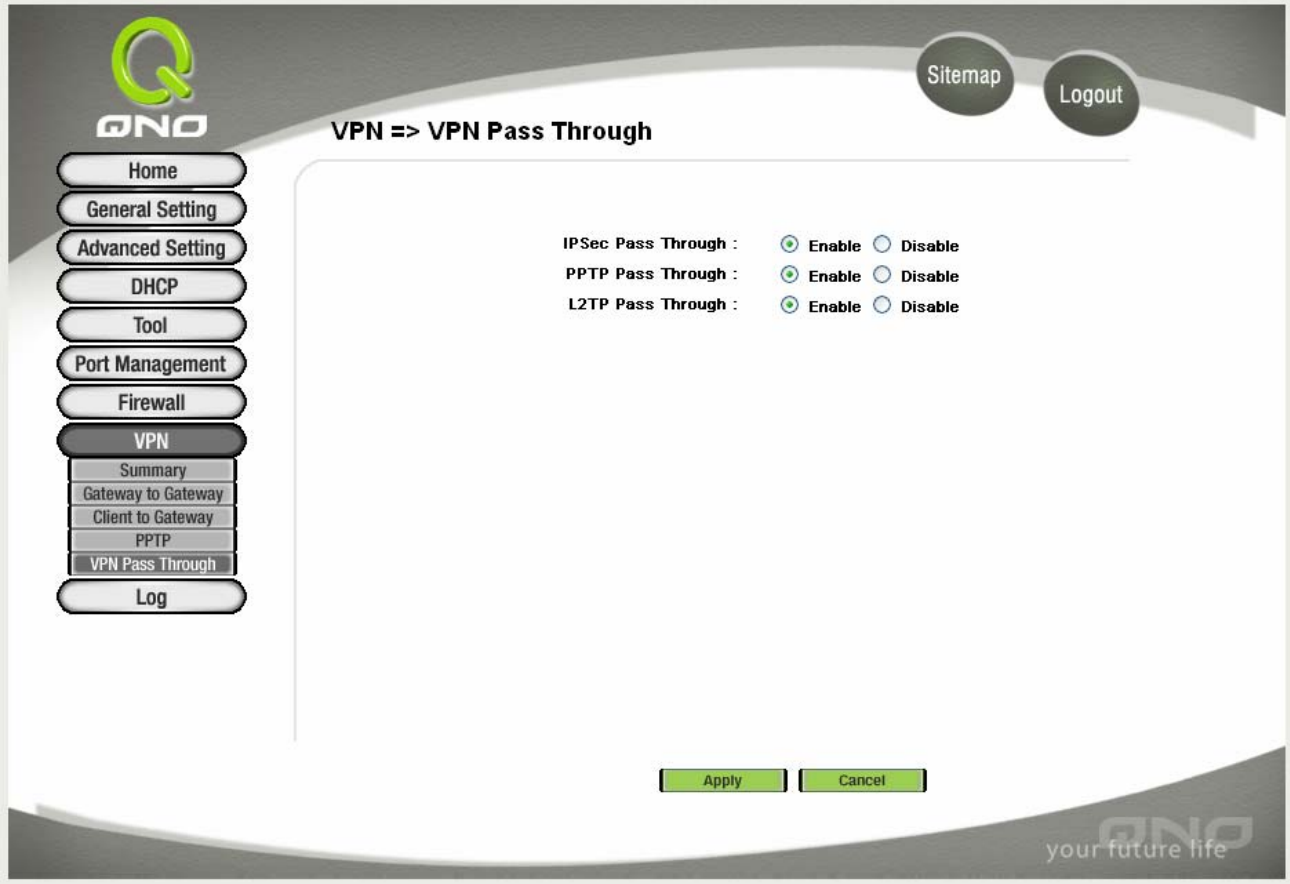
Enable PPTP Server: 当使用者勾选后即可以激活点对点隧道协议 PPTP 服务器。

PPTP IP Address Range: 请输入近端 PPTP IP 地址的范围，其目的是要给远程的使用者一个可进入近端网络的入口 IP。输入起始范围 Range Start:请在最后一栏输入数值。输入结束范围 Range End: 请在最后一栏数入数值。

User Name: 请输入远程使用者的名称

New Password and Confirm New Password:	输入使用者帐号密码及请再次确认输入远程使用者新的帐号密码
Add to list:	新增输入的帐号与密码
Delete selected User:	删除使用者
Connection List:	显示出使用 PPTP 服务器信道的使用相关信息。
User Name:	联机建立后的远程使用者名称
Remote Address:	联机建立后的远程使用者的 IP 位置
PPTP IP Address:	联机建立后，近端 PPTP 服务器的 IP 位置
Back:	按下此按钮”Back”即会回到上一页
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。。
Cancel	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

VPN Pass Through-VPN 透通:封包穿透路由器功能



IPSec Pass Through: 若是选择 **Enable** 的话，则允许 PC 端使用 VPN- IPSec 封包穿透 QVM1000 以便与外部 VPN 设备联机

PPTP Pass Through: 若是选择 **Enable** 的话，则允许 PC 端使用 VPN-PPTP 封包穿透 QVM1000 以便与外部 VPN 设备联机

L2TP Pass Through: 若是选择 **Enable** 的话，则允许 PC 端使用 VPN-L2TP 封包穿透 QVM1000 以便与外部 VPN 设备联机

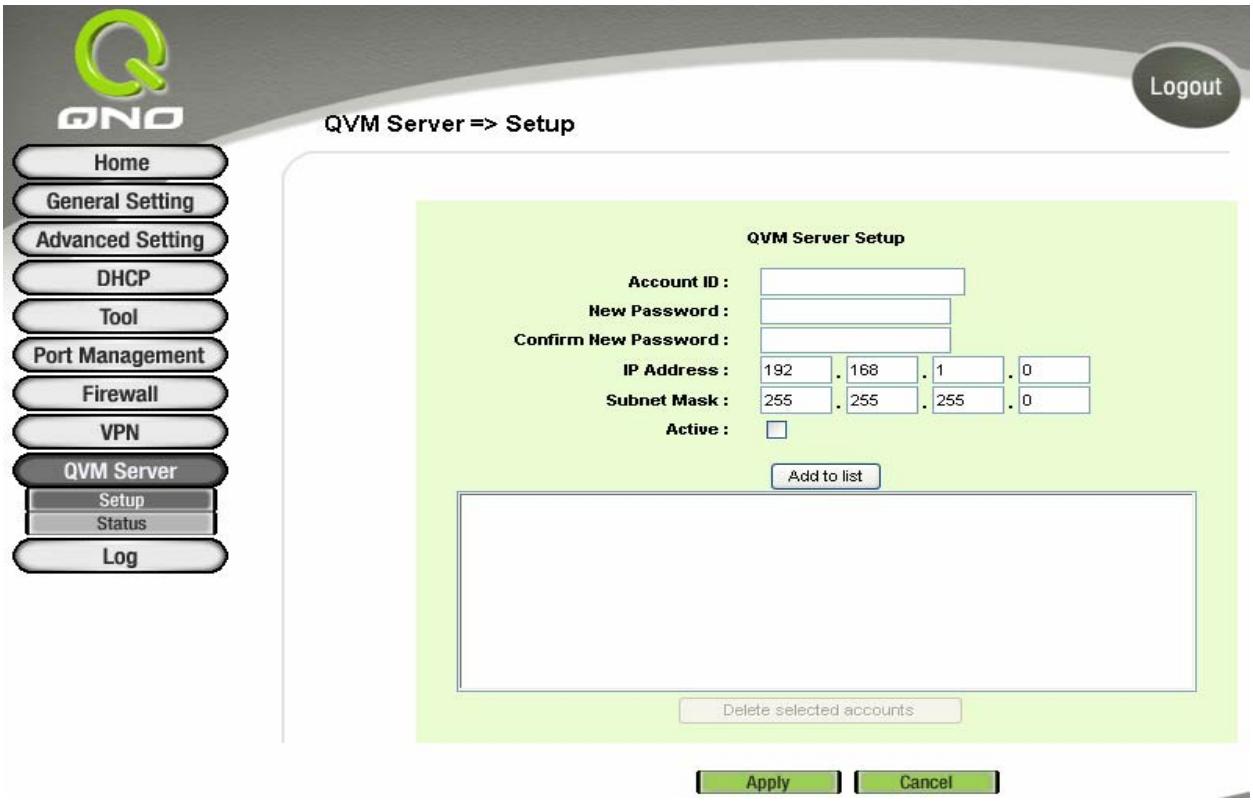
QVM Server-QVM VPN 功能设定

QVM1000 搭配 QVM330 提供了，三大便利性功能:

1.简单建立 VPN，取代传统 VPN 建立的复杂缺点，只需要 User Name 及 Password 就可以完成。

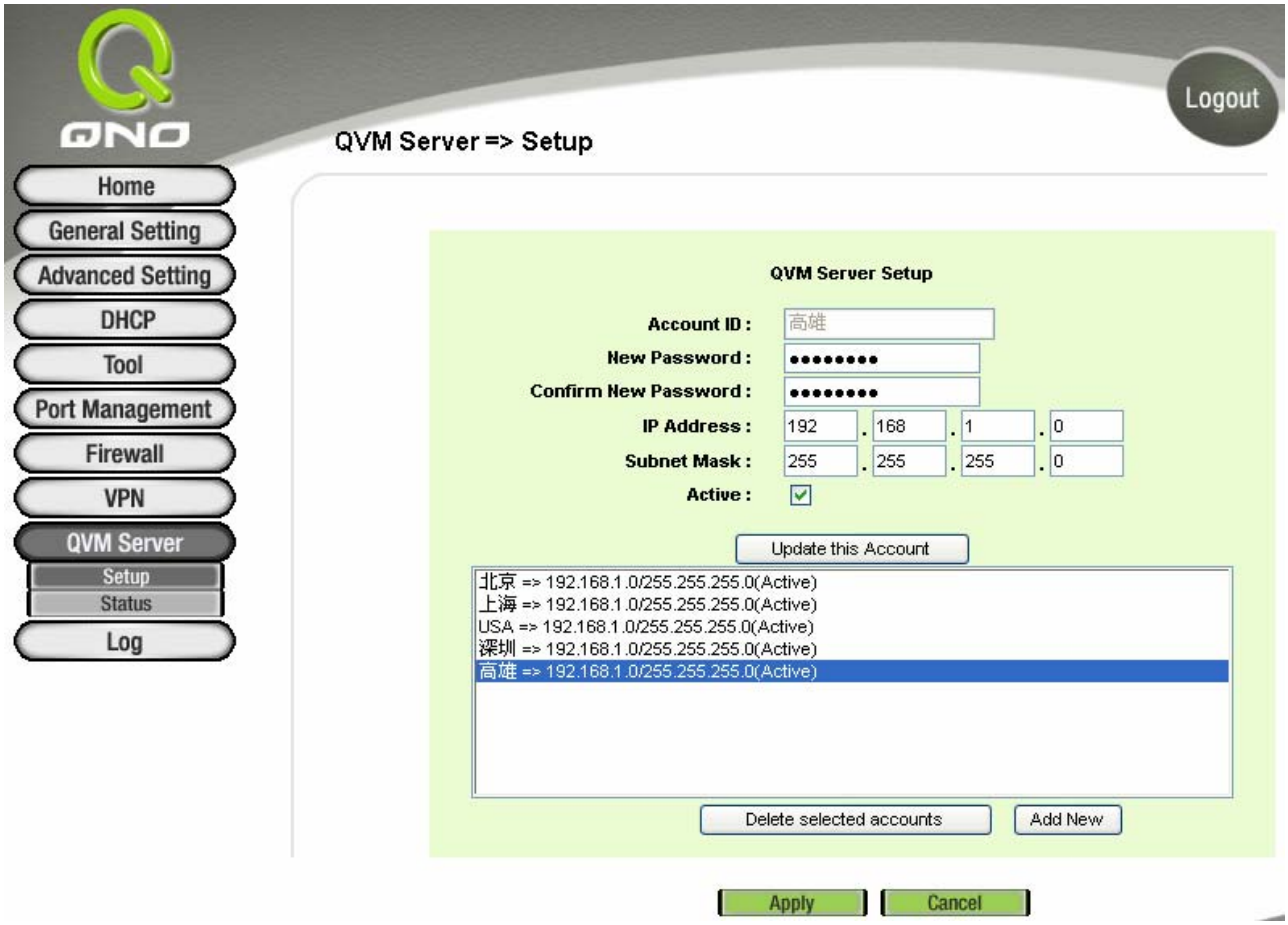
2.中央控管功能，让所有外点或分公司的 VPN 联机状态清楚且可直接在 QVM1000 中控画面，进入外点 QVM330 做设定

3。VPN 断线备芬机制，让 ISP 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。

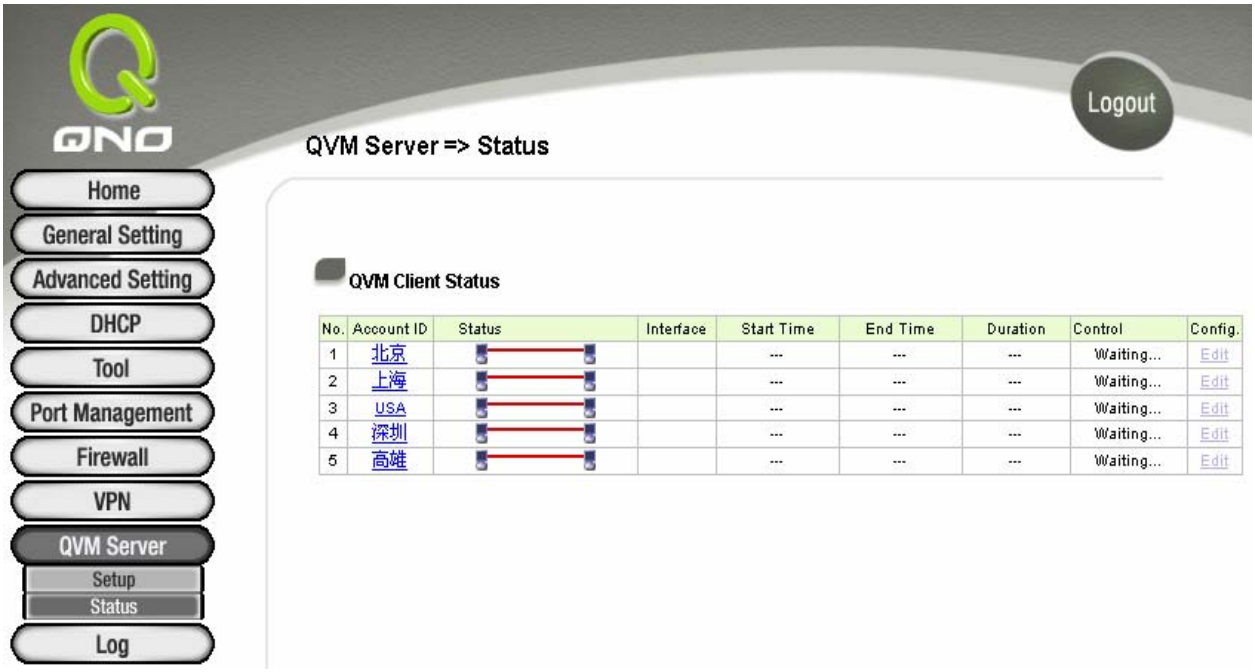


Account ID:	请输入远程 QVM330 使用者的名称:中英文皆可，需要跟远程 QVM330 一致
New Password and Confirm New Password:	输入使用者帐号密码及再次确认使用者帐号密码，需要跟远程 QVM330 一致
IP Address and Subnet Mask:	此为 QVM1000 内部哪一个网段要跟远程 QVM330 做 QVM 联机
Active:	启用此帐号。
Add to list:	新增输入的帐号与密码
Delete selected Account:	删除所选择的使用者
Apply:	按下此按钮”Apply”即会储存刚才所变动的修改设定内容参数。。
Cancel	按下此按钮”Cancel”即会清除刚才所变动的修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

QVM1000 设定完成画面



QVM Status-中央控管



Account ID: 此为您的外点 QVM330 所显示的 Account ID:绿色表示已经连通，蓝色表示等待联机，红色表示此条 QVM 关毕。

Status: 此为显示此条 QVM VPN 的联机状态，红色表示断线，绿色表示已经连通。

Interface: 此为远程此条 QVM 现在经由哪一条 QVM1000 的 WAN 进来做 QVM 联机

Start Time: 表示此条 QVM 的起用时间。

End Time: 表示此条 QVM 最后的结束时间。

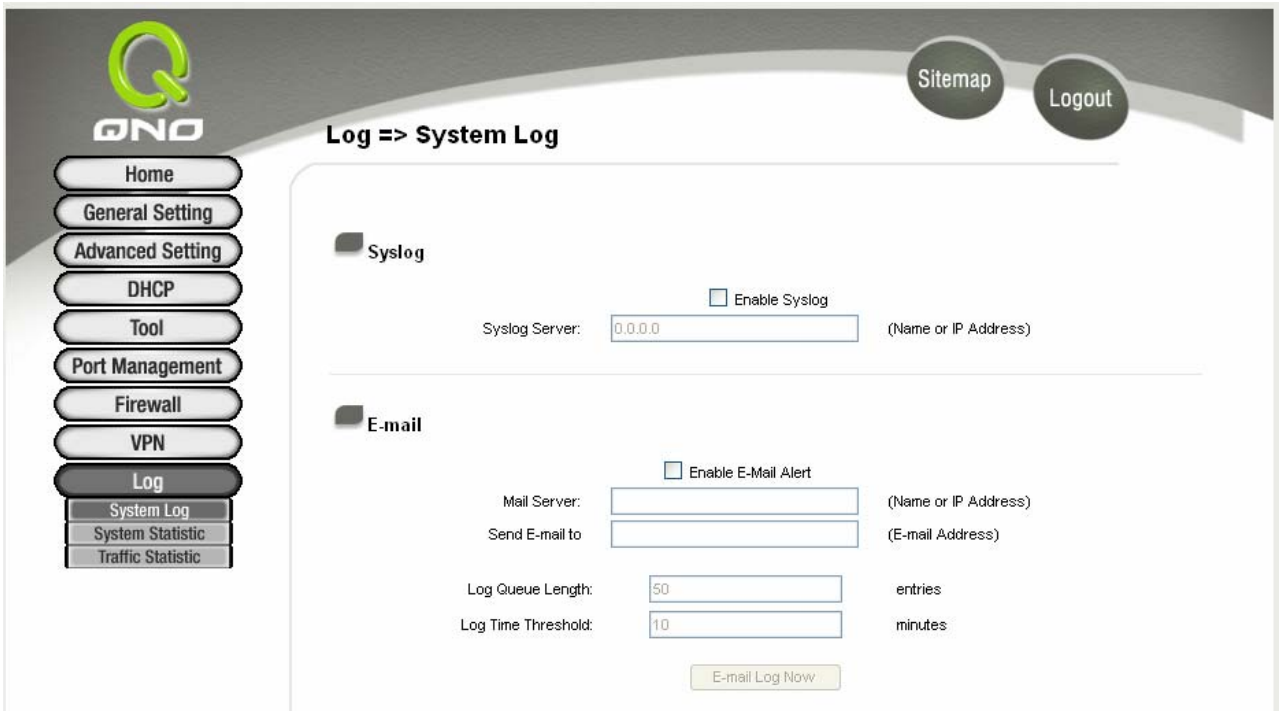
Duration: 表示此条 QVM 启用至结束的总时间。

Control: 表示现在此条 QVM 所处于的状态:Waiting 等待联机，Disconnect 将此条 QVM 断线并 Disable 关毕此功能，Enable 开启此条 QVM 至等待联机状态

Config。 按下此按钮”Edit”即可以连结到此条 QVM 的设定直接修改设定内容参数，但是必须于 Apply 储存动作之前才会有效

Log-日志

System Log-系统日志



QVM1000 系统日志(System Log)提供三种功能项目，分别为- **Syslog， E-mail** and **Log Setting**。

Syslog-系统日志

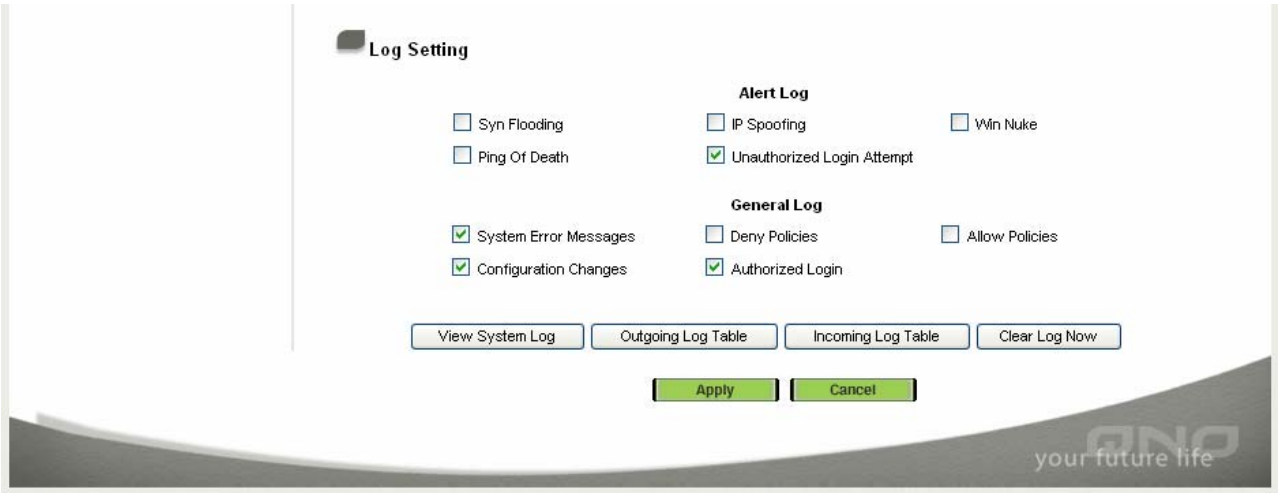
Enable Syslog: 若是此选项勾选的话， Syslog 功能将被开启

Syslog Server: QVM1000 提供了外部 Syslog 服务器收集系统信息功能。 Syslog 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。 QVM1000 的 Syslog 提供了包含动作中的联机来源位置(source IP Address)与目地(destination IP Address)位置， 服务编号(Port Number)以及类型(IP service)，若要使用此功能，请输入 Syslog 服务器名称或是 IP 位置于" **Syslog Server"** 的空格字段内。

E-mail-电子邮件

Enable E-Mail Alert:	若是此选项勾选的话， 电子邮件告警(E-Mail Alert)将会被开启
Mail Server	若您希望所有的 Log 电子邮件都可以寄出的话，请于此输入电子邮件服务器的名称或是 IP 位置，如 mail.abc.com
Send E-mail To:	此为设定 Log 收件人电子邮件信箱，如 abc@mail.abc.com
Log Queue Length (entries):	自订 Log entries 数量，系统预设为 50 个 entries。 当到达此数量时，QVM1000 将会自动 Mail 传送 Log。
Log Time Threshold (minutes):	自订传送 Log 间隔时间，系统预设为 10 分钟。 当到达此时间时，QVM1000 将会自动 Mail 传送此 Log。 QVM1000 将会自动判别当 entries 数量或是间隔时间哪一个参数先到达，就 Mail 传送 Log 讯息给管理者。
E-mail Log Now:	使用管理者可以实时直接按下此钮传送 Log。

Log Setting-系统日志设定



Alert Log-选择需要告警的内容

QVM1000 提供了包含以下的告警内容讯息，您只要打勾点选即可。Syn Flooding， IP Spoofing， Win Nuke，Ping of Death / Unauthorized Login Attempt。

Syn Flooding:	即在短时间内传送大量的 syn packet，造成系统记录联机的内存溢满。
IP Spoofing:	骇客通过封包监听程序来拦截网络上所传送资料，并在读取后利用程序修改原发送端地址(source IP address)， 进入原目的端的系统内，

	存取资源。
Win Nuke:	通过侵入或设陷阱的方式将木马程序送入对方服务器中。
Ping of Death:	通过传送来产生超过 IP 协议所能够允许的最大封包，造成系统当机。
Unauthorized Login Attempt:	当系统发现有企图进入QVM1000的入侵者时，就会将讯息传到系统日志中。

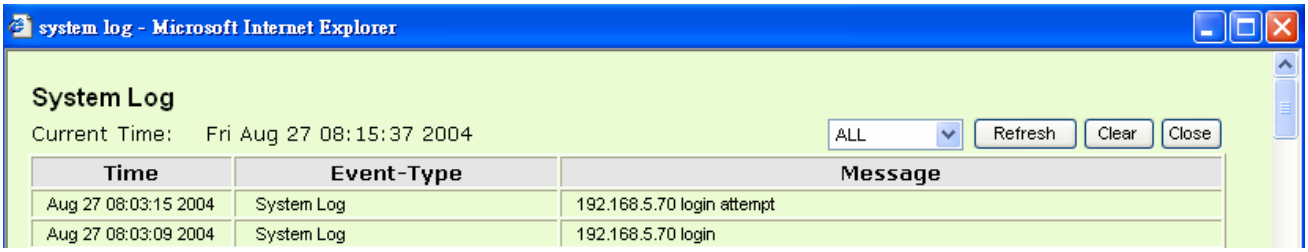
General Log-一般系统日志信息

QVM1000 提供了包含以下的一般告警内容讯息，您只要打勾点选即可。 系统错误讯息(System Error Messages)， 封锁的规则(Deny Policies)， 允许的规则(Allow Policies)， 网页过滤信息(Content Filtering)，Data Inspection， 登入设备(Authorized Login)， 设定变更(Configuration Changes)。

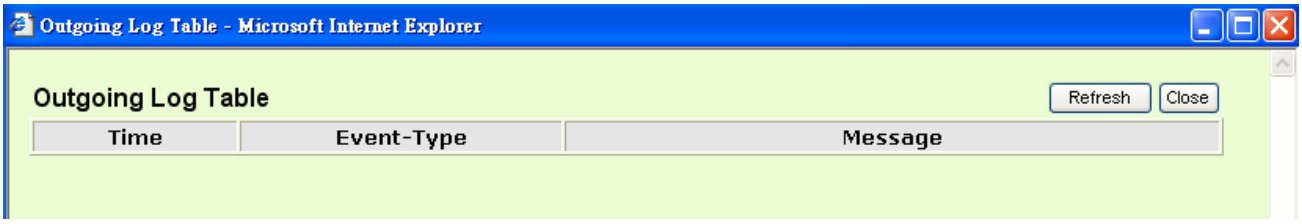
System Error Message:	提供系统中各种错误讯息给系统日志。如:不正确的设定，功能异常状况发生，system 重启，PPPoE 断线等等…。
Deny Policies:	当远程使用者因为Access Rule 而无法进入系统，此信息会传送到系统日志中。
Allow Policies:	当远程使用者因为符合Access Rule 进入系统，此信息会传送到系统日志中。
Configuration Changes	当系统的设定改变时，此信息回传送到系统日志中。
Authorized Login	每一个成功进入系统如:从远程进入或从LAN端Login进入此台路由器的信息都会传送到系统日志中。

以下有四个有关线上查询 Log 的按钮，分别叙述如下:

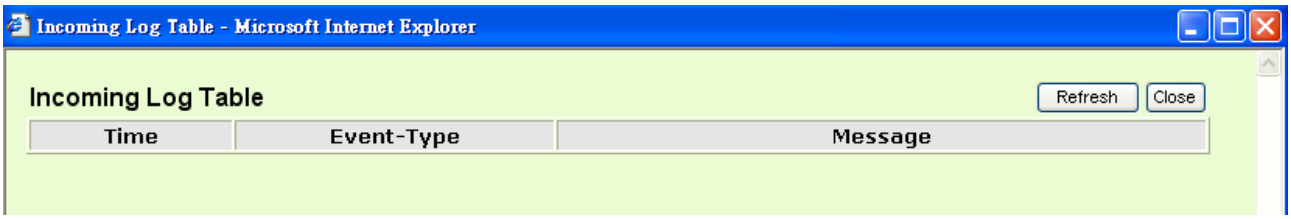
View System Log: 此为查看系统日志使用，其信息内容分别可以于 QVM1000 线上读取，包含全部讯息读取**-ALL， 系统日志-System Log， Access Log， Firewall Log 以及 VPN Log**。如下图所示:



Outgoing Log Table: 查看内部 PC 出 Internet 的系统封包日志，此日志内涵内部网络位置(LAN IP)， 目的地位置(Destination URL/IP) 以及所使用的通讯服务端口(Port Number)类型(Type)等信息。 如下图所示:

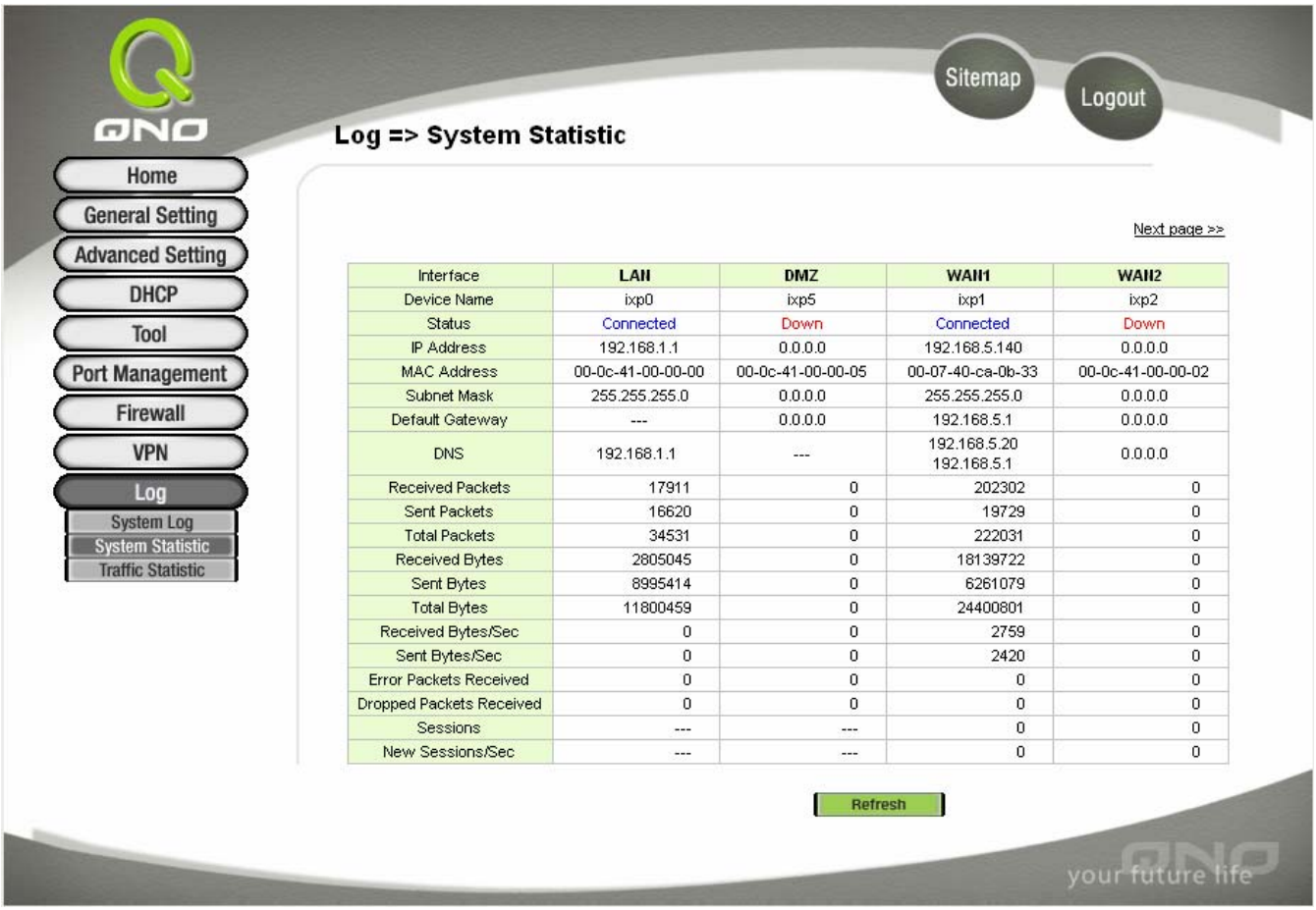


Incoming Log Table: 查看外部进入 QVM1000 防火墙的系统封包日志，此日志内含外部来源网络位置(Source IP Address)， 目的地位置与通讯端口号(Destination Port Number)等信息。 如下图所示:



Clear Log Now: 此按钮为清除所有目前 QVM1000 的 Log 相关信息。

System Statistics-系统状态实时监控



Interface	LAN	DMZ	WAN1	WAN2
Device Name	ixp0	ixp5	ixp1	ixp2
Status	Connected	Down	Connected	Down
IP Address	192.168.1.1	0.0.0.0	192.168.5.140	0.0.0.0
MAC Address	00-0c-41-00-00-00	00-0c-41-00-00-05	00-07-40-ca-0b-33	00-0c-41-00-00-02
Subnet Mask	255.255.255.0	0.0.0.0	255.255.255.0	0.0.0.0
Default Gateway	---	0.0.0.0	192.168.5.1	0.0.0.0
DNS	192.168.1.1	---	192.168.5.20 192.168.5.1	0.0.0.0
Received Packets	17911	0	202302	0
Sent Packets	16620	0	19729	0
Total Packets	34531	0	222031	0
Received Bytes	2805045	0	18139722	0
Sent Bytes	8995414	0	6261079	0
Total Bytes	11800459	0	24400801	0
Received Bytes/Sec	0	0	2759	0
Sent Bytes/Sec	0	0	2420	0
Error Packets Received	0	0	0	0
Dropped Packets Received	0	0	0	0
Sessions	---	---	0	0
New Sessions/Sec	---	---	0	0

QVM1000 的 System Statistics 管理功能可以提供系统目前运作信息，包含：Device Name(机器名称)，Status(目前 WAN 端联机状态)， IP Address(IP 位置)， MAC Address(网络硬件地址)， Subnet Mask(子网掩码)， Default Gateway(预设网关)， DNS(网域名称服务器)，Received Packets(收到的封包数量)， Sent Packets(传送的封包数量)， Total Packets(全部的封包数量统计)， Received Bytes(收到的封包 Byte 数量统计)， Sent Bytes(传送的封包 Byte 数量统计)， Total Bytes(全部的封包 Byte 数量统计)， Error Packets Received(收到的错误封包统计)以及 Dropped Packets Received(LAN， WAN1 ~ WAN4 丢弃的封包统计)，Session(联线数)， New Session/Sec(每秒新的联线数)等信息。

Traffic Statistic:

有六种信息会显示在流量统计的网页里，来提供管理对于流量有更好的管理与控制。

Inbound IP Source Address:对内流量来源位置 IP 位置

在此图表中显示了来源端的 IP 地址， 每秒有多少 byte 与百分比。

Traffic Type : Inbound IP Source Address

Source IP	bytes/sec	%
192.168.1.100	4	100

Outbound IP Source Address: 对外流量来源位置 IP 位置

在此图表中显示了来源端的 IP 地址， 每秒有多少 byte 与百分比。

Traffic Type : Outbound IP Source Address

Source IP	bytes/sec	%
192.168.5.173	422	99
192.168.1.100	4	0

Inbound IP Service:对内流量 IP 服务端口号

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

Traffic Type : Inbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	http(80)	1270	99
TCP	1863	4	0

Outbound IP Service: 对外流量 IP 服务端口号

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

Traffic Type : Outbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	1161	216	67
TCP	http(80)	102	32

Inbound IP session: 对内流量 IP 联机数

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

Traffic Type : Inbound IP Session

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	3563	66.35.229.141	80	57	100

Outbound IP Session:对外流量 IP 联机数

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

Traffic Type : Outbound IP Session

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

Logout

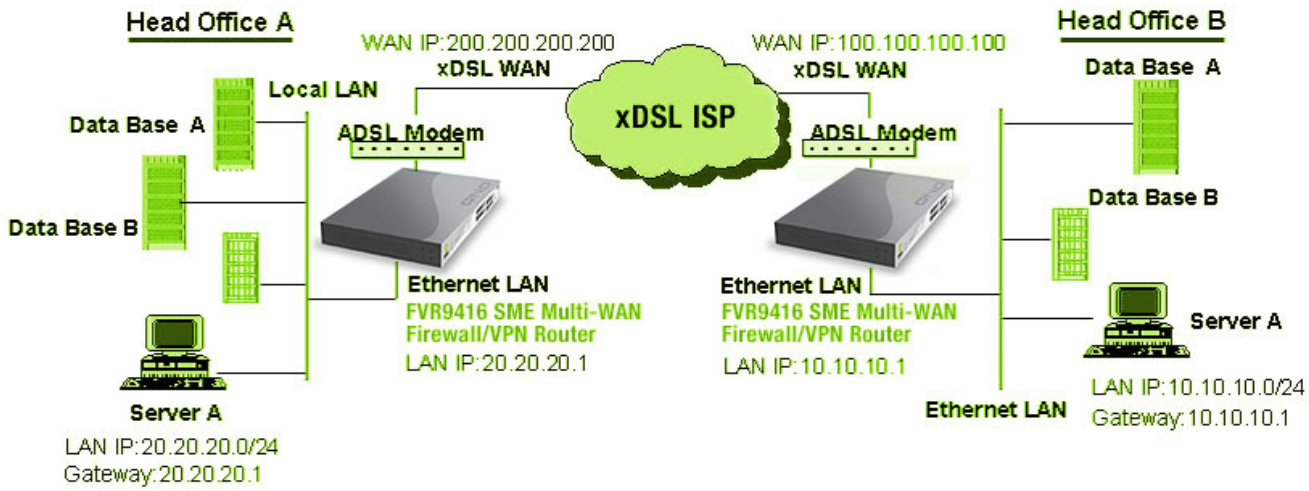
QVM1000 的网页画面右下方有一个 **Logout** 的按钮，此按钮为终止管理 QVM1000 并注销此管理画面，若您下次想再进入 QVM1000 管理画面时，您必须再输入管理验证使用名称与密码。

5。 Troubleshooting

6。 FAQ

7。 Appendix A: VPN Configuration Sample

Sample VPN Environment 1: Gateway to Gateway



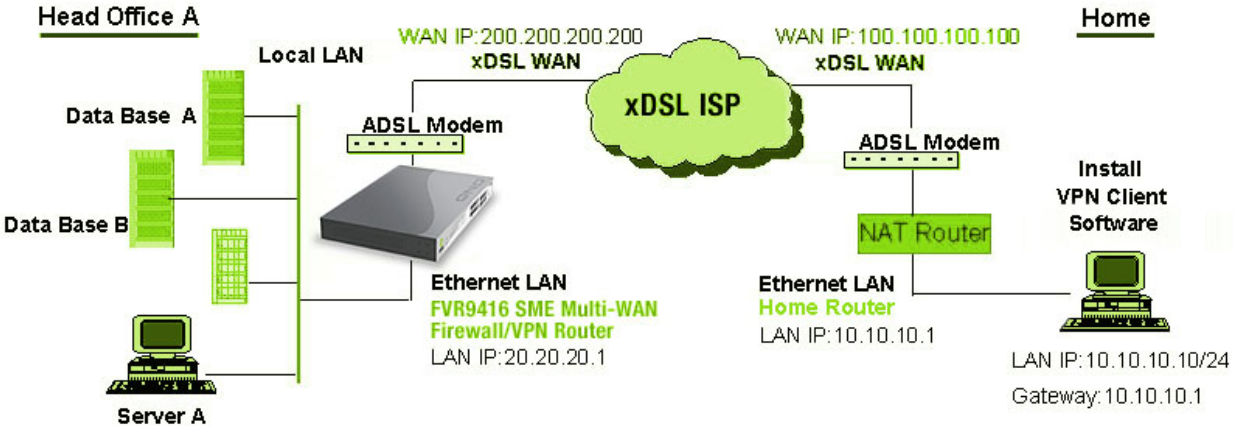
Firewall Setting: Firewall➔General➔Block WAN Request = Disable

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

QVM1000 VPN Configuration for	Head Office A	Head Office B
Tunnel Name	HOB	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	Subnet
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.0

Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	IP	IP
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	Subnet	Subnet
Remote Security Group Type➔ IP Address	10.10.10.0	20.20.20.0
Remote Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key。	

Sample VPN Environment 2: Gateway to Gateway

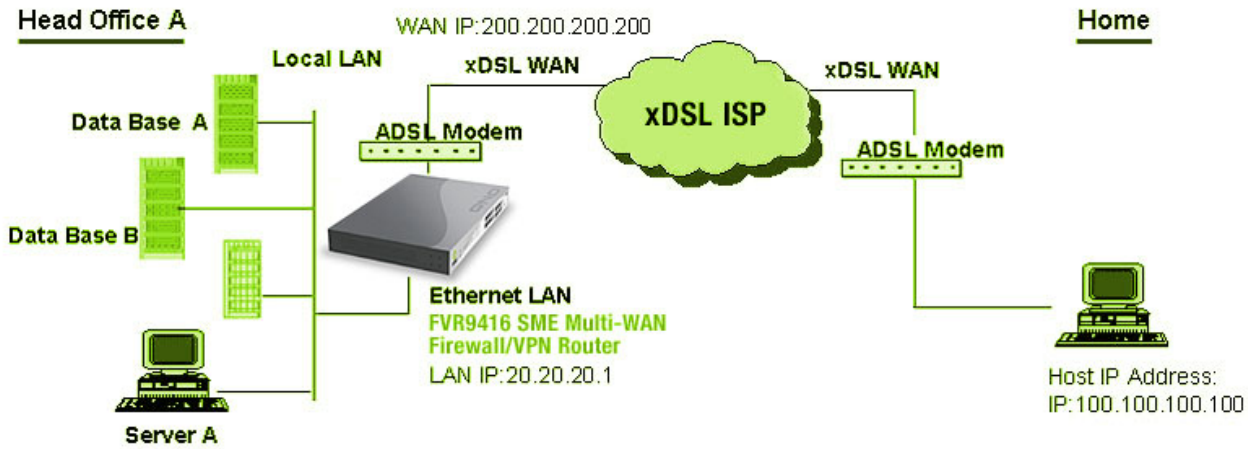


VPN Setting: VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.10
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type➔ Domain Name	Company domain Name	
Local ID➔ Domain Name		Company domain Name
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200

Remote Security Group Type	IP	Subnet
Remote Security Group Type➔ IP Address	10.10.10.10	20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 3: Client to Gateway (Tunnel)

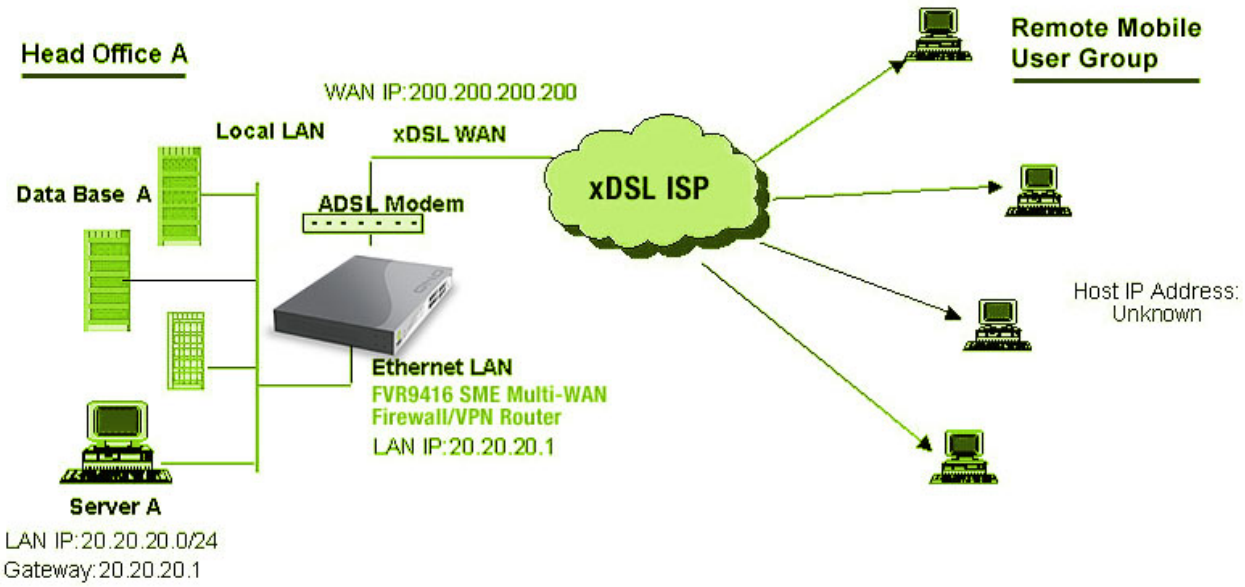


VPN Setting: VPN➔Summary➔Add New Tunnel➔Client to Gateway➔Tunnel

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	100.100.100.100
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200
Remote Client	Email Address	
Remote Client➔ Email Address	User Email Address	
Local ID➔ Email Address		User Email Address
Remote Client➔ IP Address	100.100.100.100	
Remote Security Group Type		Subnet

Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Sample VPN Environment 4: Client to Gateway (GroupVPN)



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

	Head Office A	HomeN (VPN Client SW)
Group Name/Tunnel Name	GroupVPN1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	Client IP Address
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200

Remote Client	Domain Name	
Remote Client➔ Email Address	Company Domain Name	
Local ID➔ Email Address		Company Domain Name
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	
Advanced	Aggressive Mode	

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