your future life

2 WAN 3 LAN VPN Firewall

Load Balance, Bandwidth Management, VPN, and Network Security

English User's Manual

Product Manual Using Permit Agreement

[Product Manual (hereafter the "Manual") Using Permit Agreement] hereafter the "Agreement" is the using permit of the Manual, and the relevant rights and obligations between the users and Qno Technology Inc (hereafter "Qno"), and is the exclusion to remit or limit the liability of Qno. The users who obtain the file of this manual directly or indirectly, and users who use the relevant services, must obey this Agreement.

Important Notice: Qno would like to remind the users to read the clauses of the "Agreement" before downloading and reading this Manual. Unless you accept the clauses of this "Agreement", please return this Manual and relevant services. The downloading or reading of this Manual is regarded as accepting this "Agreement" and the restriction of clauses in this "Agreement".

【1】Statement of Intellectual Property

Any text and corresponding combination, diagram, interface design, printing materials or electronic file are protected by copyright of our country, clauses of international copyright and other regulations of intellectual property. When the user copies the "Manual", this statement of intellectual property must also be copied and indicated. Otherwise, Qno regards it as tort and relevant duty will be prosecuted as well.

【2】Scope of Authority of "Manual"

The user may install, use, display and read this "Manual on the complete set of computer.

【3】User Notice

If users obey the law and this Agreement, they may use this "Manual" in accordance with "Agreement". If the users violate the "Agreement", Qno will terminate the using authority and destroy the copy of this "Manual". The "hardcopy or softcopy" of this Manual is restricted using for information, non-commercial and personal purpose. Besides, it is not allowed to copy or announce on any network computer. Furthermore, it is not allowed to disseminate on any media. It is not allowed to modify any part of the "file". Using for other purposes is prohibited by law and it may cause serious civil and criminal punishment. The transgressor will receive the accusation possibly.

【4】Legal Liability and Exclusion

【4-1】Qno will check the mistake of the texts and diagrams with all strength. However, Qno, distributors, and resellers do not bear any liability for direct or indirect economic loss, data loss or other corresponding commercial loss to the user or relevant personnel due to the possible omission.

【4-2】In order to protect the autonomy of the business development and adjustment of Qno, Qno reserves the right to adjust or terminate the software / Manual any time without informing the users. There will be no further notice regarding the product upgrade or change of technical specification. If it is necessary, the change or termination will be announced in the relevant block of the Qno website.

【4-3】All the set parameters are examples and they are for reference only. You may also purpose your opinion or suggestion. We will take it as reference and they may be amended in the next version.

【4-4】This Manual explains the configuration of all functions for the products of the same series. The actual functions of the product may vary with the model. Therefore, some functions may not be found on the product you purchased.

【4-5】Qno reserves the right to change the file content of this Manual and the Manual content may not be updated instantly. To know more about the updated information of the product, please visit Qno official website.

【4-6】Qno (and / or) distributors hereby declares that no liability will be born for any guarantee and condition of the corresponding information. The guarantee and condition include tacit

Content

I. Introduction

2 WAN 3 LAN VPN Firewall (referred as VPN Firewall hereby) is a small business, local branch, and government and school department level router that high efficiently integrates full function VPN firewall with well worth it's value. This VPN Firewall has two WAN ports and also provides high proformance dual-line Intelligent Load Balancing which supports exteral connections of WAN prot. Besides, Internet connection capacity is satisfied with the spec. of most bandwidth marketing. Moreover, the second WAN port can be a configurable hardware DMZ port. In addition, VPN Firewall has 3 10/100 Bazs-T/TX Ethernet (RJ45) Switch ports, each of which can connect extra switches to connect more Internet devices.

To fulfill the requirement for self defense of most enterprise against from the Internet network attack, our VPN Firewall has firewall system embedded. In addition to include NAT, it has DoS (Denial of Service), and SPI (Stateful Packet Inspection). Also it could use the default setting to automatically detect the Internet network attack.

And, Qno is a supporter of the IPSec Protocol. IPSec VPN provides DES(56bit), 3DES(168bit), MD5 & SHA certification. VPN Firewall also has unique QVM VPN- SmartLink IPSec VPN. Just input VPN server IP, user name, and password, and IPSec VPN will be automatically set up. Through VPN Firewall exclusive QVM function, users can set up QVM to work as a server, and have it accept other QVM series products from client ports.

VPN Firewall also has unique QVM VPN- SmartLink IPSec VPN. Just input VPN server IP, user name, and password, and IPSec VPN will be automatically set up. Through VPN Firewall exclusive QVM function, users can set up QVM to work as a server, and have it accept other QVM series products from client ports. QVM offers easy VPN allocation for users; users can do it even without a network administrator. VPN Firewall enables enterprises to benefit from VPN without being troubled with technical and network management problems. The central control function enables the host to log in remote client computers at any time. Security and secrecy are guaranteed to meet the IPSec standard, so as to ensure the continuity of VPN service.

NAT (Network Address Translation) can do Private IP and Public IP exchange, which you can only need one Public IP but many people could go to the Internet at the same time. Besides, it includes virtual NAT application function, which makes the network environment more flexible and easier to manage.

Through web- based UI, VPN Firewall enables enterprises to have their own network access rules . To control web access, users can build and edit filter lists. It also enables users to ban or monitor websites according to their needs. By the filter setting and complete OS management, school and business internet management will be clearly improved. VPN Firewall offers various on-line SysLog records. It supports on-line management setup tools; it makes setting up networks easy to understand. It also reinforces the management of network access rules, VPN, and all other network services.

II. Hardware Installation

In this chapter we are going to introduce hardware interface as well as physical installation.

2.1 VPN Firewall LED Signal

LED Signal Description

LED	Color	Description
Power	Green	Green LED on: Power ON
DIAG	Amber	Amber LED on: System self-test is running. Amber LED off: System self-test is completed successfully.
Link/Act （Green light at the right of the port）	Green	Green LED on: Ethernet connection is fine. Green LED blinking: Packets are transmitting through Ethernet port.
100M- Speed （Amber light at the left of the port）	Amber	Green LED on: Ethernet is running at 100Mbps. Green LED off: Ethernet is running at 10Mbps.
Connect	Green	Green LED on: WAN is connected and gets the IP address.

Reset

Action	Description
Press Reset Button For 5 Secs	Warm Start DIAG indicator: Amber LED flashing slowly.
Press Reset Button Over 10 Secs	Factory Default DIAG indicator: Amber LED flashing quickly.

System Built-in Battery

A system timing battery is built into VPN Firewall. The lifespan of the battery is about 1~2 years. If the battery life is over or it can not be charged, VPN Firewall will not be able to record time correctly, nor synchronize with internet NTP time server. Please contact your system supplier for information on how to replace the battery.

Attention!

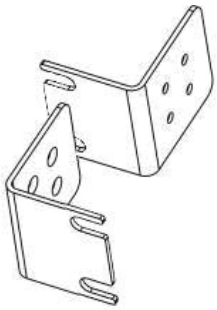
Do not replace the battery yourself; otherwise irreparable damage to the product may be caused.

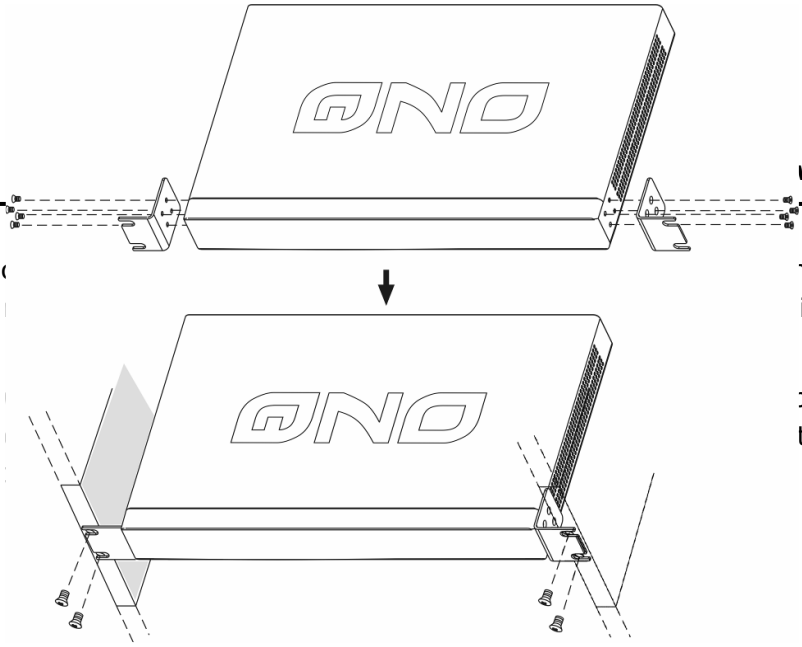
Installing VPN Firewall on a Standard 19” Rack

wall

We suggest to either pla ned
brac ing
may

brac the
figu

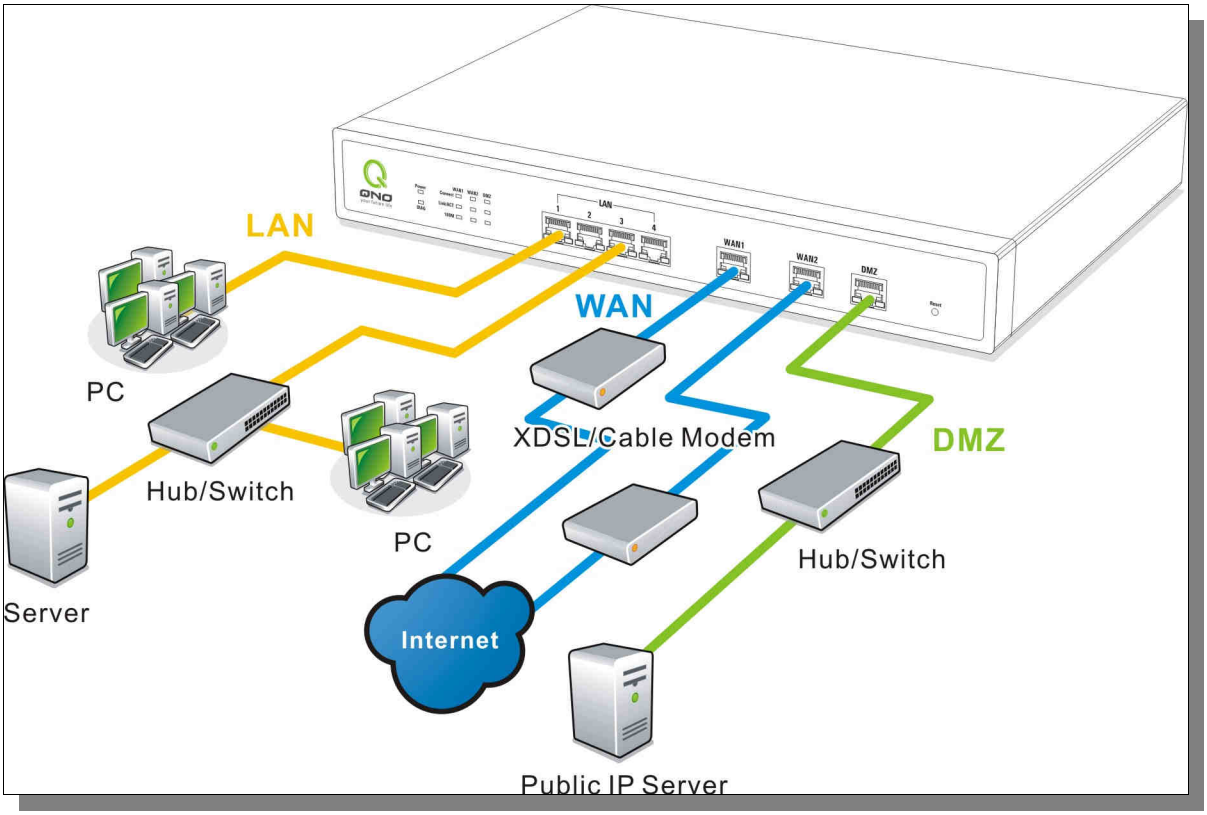




Attention!

In order for the device to run smoothly, wherever users install it, be sure not to obstruct the vent on each side of the device. Keep at least 10cm space in front of both the vents for air convection.

2.2 VPN Firewall Network Connection



WAN connection : A WAN port can be connected with xDSL Modem, Fiber Modem, Switching Hub, or through an external router to connect to the Internet.

LAN Connection: The LAN port can be connected to a Switching Hub or directly to a PC.

Users can use servers for monitoring or filtering through the port after "Physical Port Mangement" configuration is done.

DMZ : The DMZ port can be connected to servers that have legal IP addresses, such as Web servers, mail servers, etc.

III. Quick Configuration

In this chapter we are going to introduce software setting interface, explaining the message of home page as well as basic connection setting.

3.1 Login and Set Up

VPN Firewall default username and password are both "admin". Users can change the login password in the setting later.

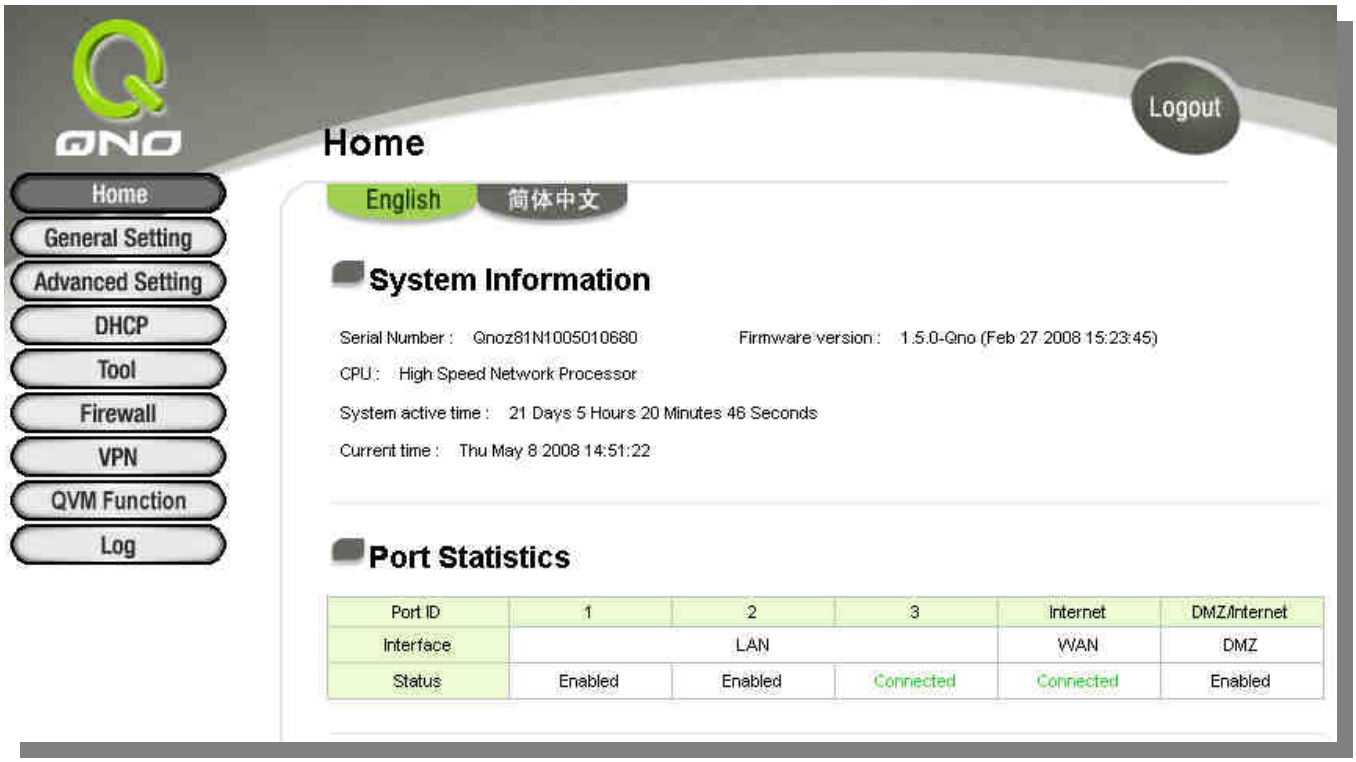
Attention!

For security, we strongly suggest that users must change password after login. Please keep the password safe, or you can not login to VPN Firewall. Press Reset button for more than 10 sec, all the setting will return to default.

3.2 Home Page

In the Home page, all the device parameters and status are listed for users' reference. For detailed settings, click each parameter or status hyperlink below: the relevant set-up tab will be loaded for users to choose their management options.

3.2.1 System Information



Serial No.

This number is the device serial number.

Firmware version

Information about the device present software version.

CPU (Central Processing Unit)

Indicates the device CPU model No.: Intel IXP425-533MHz

System active time:

Indicates how long the device has been running.

Current Time:

Indicates the device present time, but you have to pay attention to set the synchronous time with that of the romote NTP server, and then the time will be shown correctly.

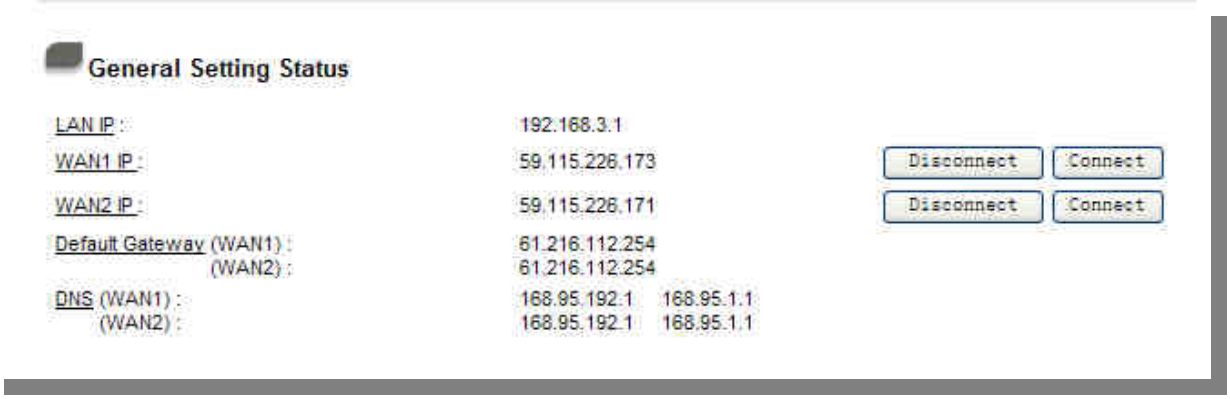
3.2.2 Port Statistics

Port Statistics

Port ID	1	2	3	Internet	DMZ/Internet
Interface	LAN			WAN	DMZ
Status	Enabled	Enabled	Connected	Connected	Enabled

The current port setting status information will be shown in the Port Status Table. Examples: Network connection, port (on or off), priority (high or normal), connection speed (10Mbps or 100Mbps), duplex status (half-duplex or full duplex), and auto negotiation (Enabled or Disabled).

3.2.3 General Setting Status



LAN IP:

Indicates the LAN port current IP configuration. The default IP is 192.168.1.1. Click the hyperlink to enter and manage the configuration.

WAN 1 IP:

Indicates the WAN1 current IP configuration. Click the hyperlink to enter and manage the configuration. When "Obtain an IP automatically" is selected, two buttons (Release and Renew) will appear on the right of the page. Click "Release" to release the IP that is issued by the ISP, and click "Renew" to refresh the IP that is issued by the ISP. If a WAN connection, such as PPPoE or PPTP, is selected, "Disconnect" and "Connect" will appear on the page.

WAN 2/DMZ IP:

Indicates the WAN2 or DMZ current IP configuration. Click the hyperlink to enter and manage the configuration.

Default Gateway:

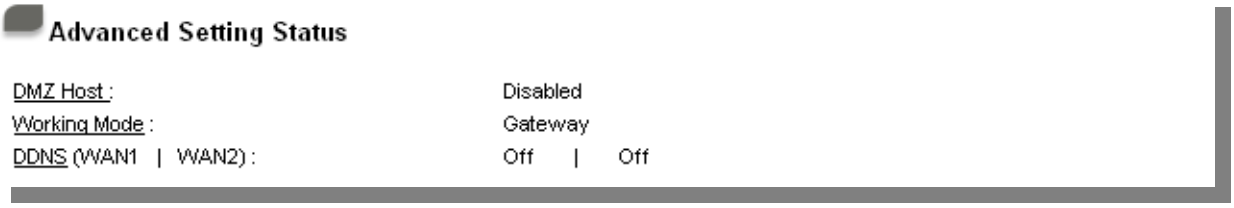
Indicates the current Gateway IP configuration. Click the hyperlink to enter and manage the configuration.

DNS:

Indicates the current DNS IP configuration. Click the hyperlink to enter and manage the

configuration.

3.2.4 Advanced Setting Status



DMZ Host:

Indicates if DMZ is activated. Click the hyperlink to enter and manage the configuration. The default configuration is "Disabled".

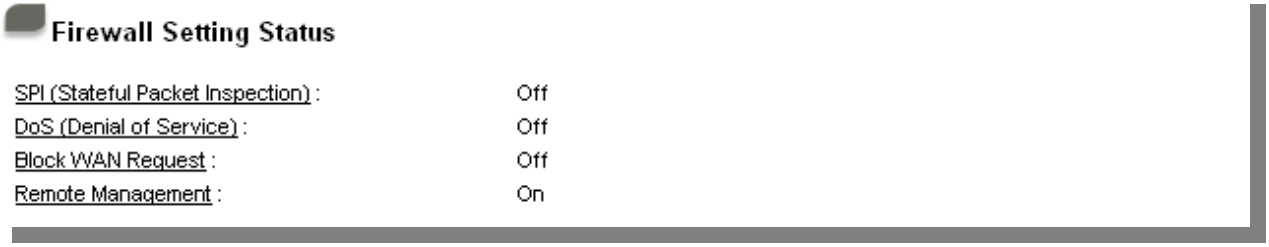
Working Mode:

Indicates the the device current operation mode (either Gateway mode or Router mode). Click the hyperlink to enter and manage the configuration. The default operation mode is Gateway mode.

DDNS (Dynamic Domain Name Service):

Indicates if Dynamic Domain Name is activated. Click the hyperlink to enter and manage the configuration. The default configuration is "Off".

3.2.5 Firewall Setting Status



SPI (Stateful Packet Inspection):

Indicates whether SPI (Stateful Packet Inspection) is on or off. Click the hyperlink to enter and manage the configuration. The default configuration is "Off".

DoS (Denial of Service):

Indicates if DoS attack prevention is activated. Click the hyperlink to enter and manage the configuration. The default configuration is "Off".

Block WAN Request:

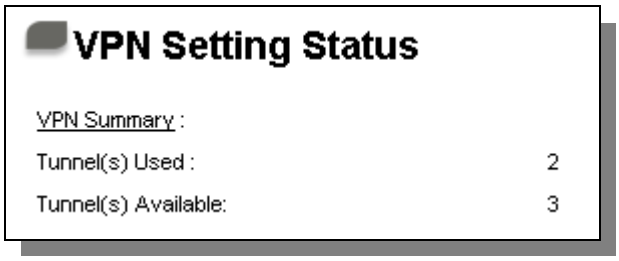
Indicates that denying the connection from Internet is activated. Click the hyperlink to

enter and manage the configuration. The default configuration is "Off".

Remote Management:

Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is "Off".

3.2.6 VPN Setting Status



VPN Summary:

Indicates VPN configuration status. Click the hyperlink to enter and manage the configuration.

Tunnel(s) Used:

Indicates number of tunnels that have been configured in VPN (Virtual Private Network).

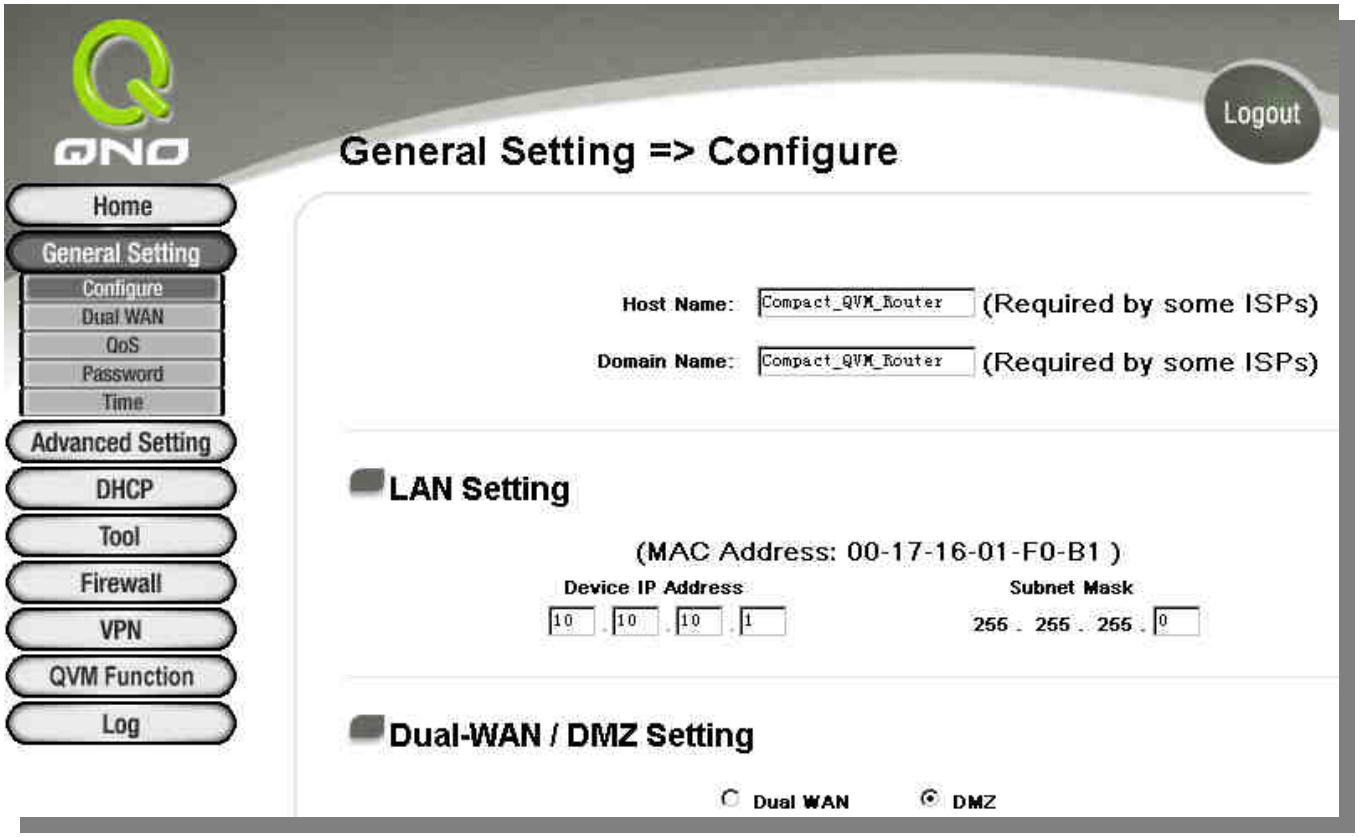
Tunnel(s) Available:

Indicates number of tunnels that are available for VPN (Virtual Private Network).

3.3 General Setting

General Setting provides basic VPN firewall Internet connection setting. For most users, it's enough to go to Internet after making basic setting without doing any changes. However, to connect Internet still needs some ISPs to provide advanced detail information. Therefore, please refer to the following explaination of the detail setting.

3.3.1 Configure



Host Name and Domain Name

Device name and domain name can be input in the two boxes. Though this configuration is not necessary in most environments, some ISPs in some countries may require it.

LAN Setting

This is configuration information for the device current LAN IP address. The default configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. Now it can support to the IP Class C network and also it can be changed according to the actual network structure.

Dual-WAN / DMZ Setting

It provides a configurable WAN 2 or DMZ port. First, choose this port as the second WAN port or define it as DMZ mode, and then keep doing the following setting.

DMZ Setting

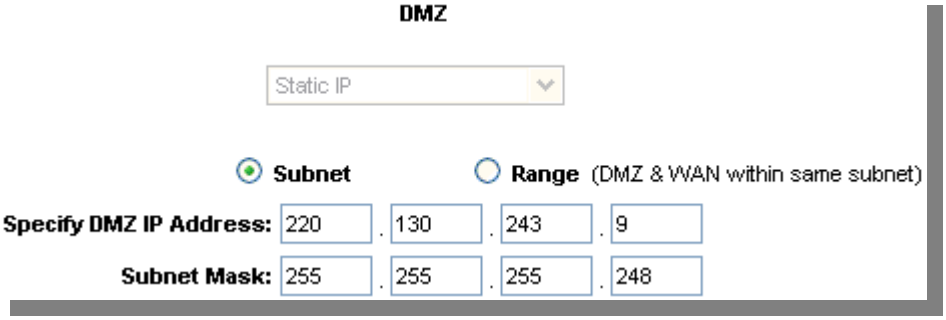
For some network environments, an independent DMZ port may be required to set up externally connected servers such as WEB and Mail servers. Therefore, the device supports a set of independent DMZ ports for users to set up connections for servers with real IPs. The

DMZ ports act as bridges between the Internet and LANs.

Subnet :

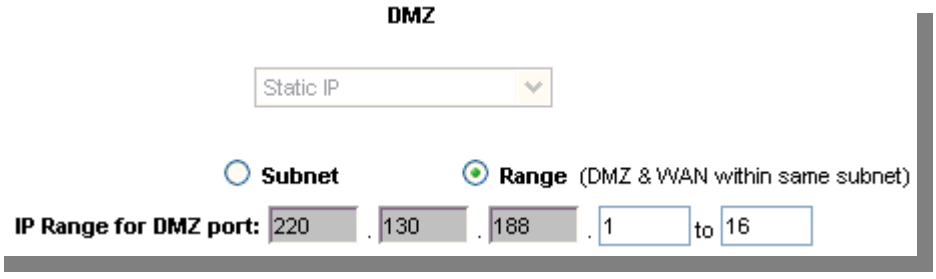
The DMZ and WAN located in different Subnets

For example: If the ISP issued 16 real IP addresses: 220.243.230.1-16 with Mask 255.255.255.240, users have to separate the 16 IP addresses into two groups: 220.243.230.1-8 with Mask 255.255.255.248, and 220.243.230.9-16 with Mask 255.255.255.248 and then set the device and the gateway in the same group with the other group in the DMZ.



Range :

DMZ and WAN within same Subnet



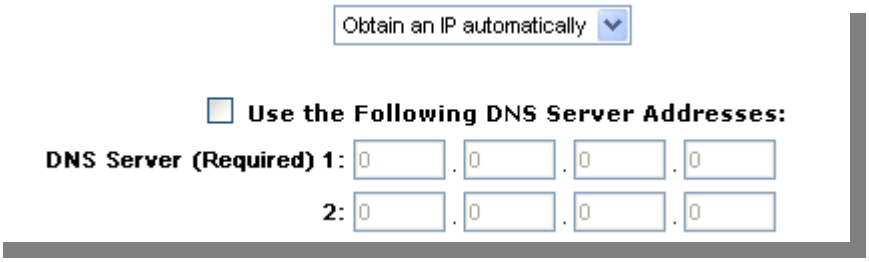
IP Range for DMZ port: Put IP range in DMZ port.

After the changes are completed, click **"Apply"** to save the configuration, or click **"Cancel"** to leave without making any changes.

WAN Connection Type

Obtain an IP automatically

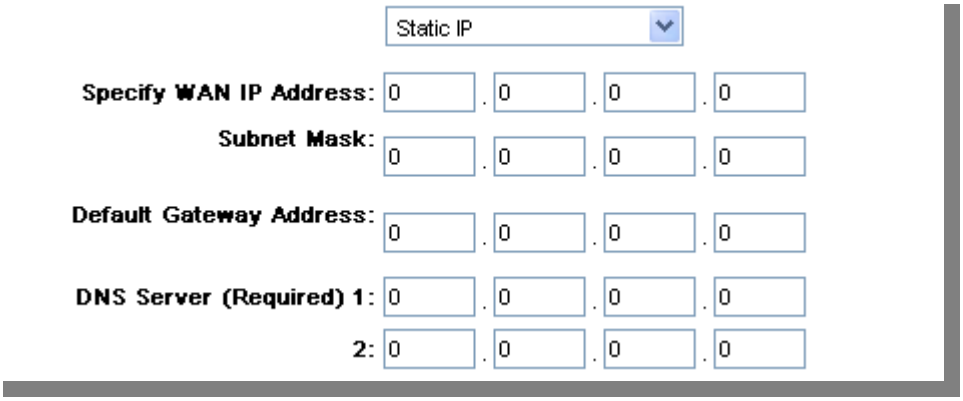
This mode is often used in the connection mode to obtain an automatic DHCP IP. This is the device system default connection mode. It is a connection mode in which DHCP clients obtain an IP address automatically, which is often applied in Cable Modem or DHCP Client connection mode, etc. If having a different connection mode, please refer to the following introduction for selection of appropriate configurations. Users can also set up their own DNS IP address (Use the Following DNS Server Address). Check the options and input the user-defined DNS IP addresses.



Static IP

If ISP issue a static IP (such as one IP or eight IPs, etc.), please select this connection mode and follow the steps below to input the IP numbers issued by ISP into the relevant boxes.

Attention: Even if ISP offers a static IP address, it might be an automatic mode to obtain a DHCP IP or to obtain a PPPoE dial-up IP. Although the IP address obtained will be the same each time, users still must select the correct connecting mode!



Specify WAN IP address: Input the available static IP address issued by ISP.

Subnet Mask: Input the subnet mask of the static IP address issued by ISP, such as:

Issued eight static IP addresses: 255.255.255.248

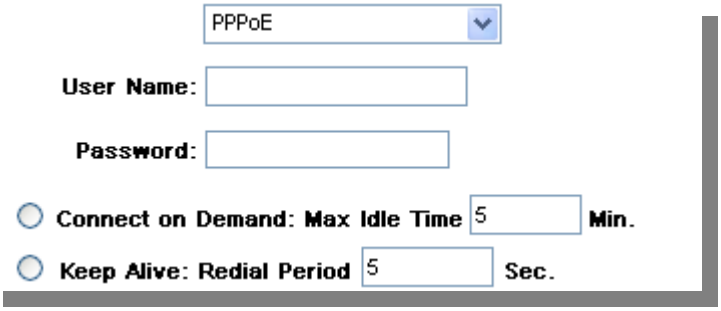
Issued 16 static IP addresses: 255.255.255.240

Default Gateway Address: Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.

Domain Name Server (DNS) : Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.

Point-to-Point Protocol over Ethernet

This option is for an ADSL virtual dial-up connection (suitable for ADSL PPPoE). Input the user connection name and password issued by ISP. Then use the PPP Over-Ethernet software built into the device to connect with the Internet. If the PC has been installed with the PPPoE dialing software provided by ISP, remove it. This software will no longer be used for network connection.



User Name: Input the user name issued by ISP.

Password Input the password issued by ISP.

Connect on Demand: This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break-off resulting from no packet transmissions is five minutes).

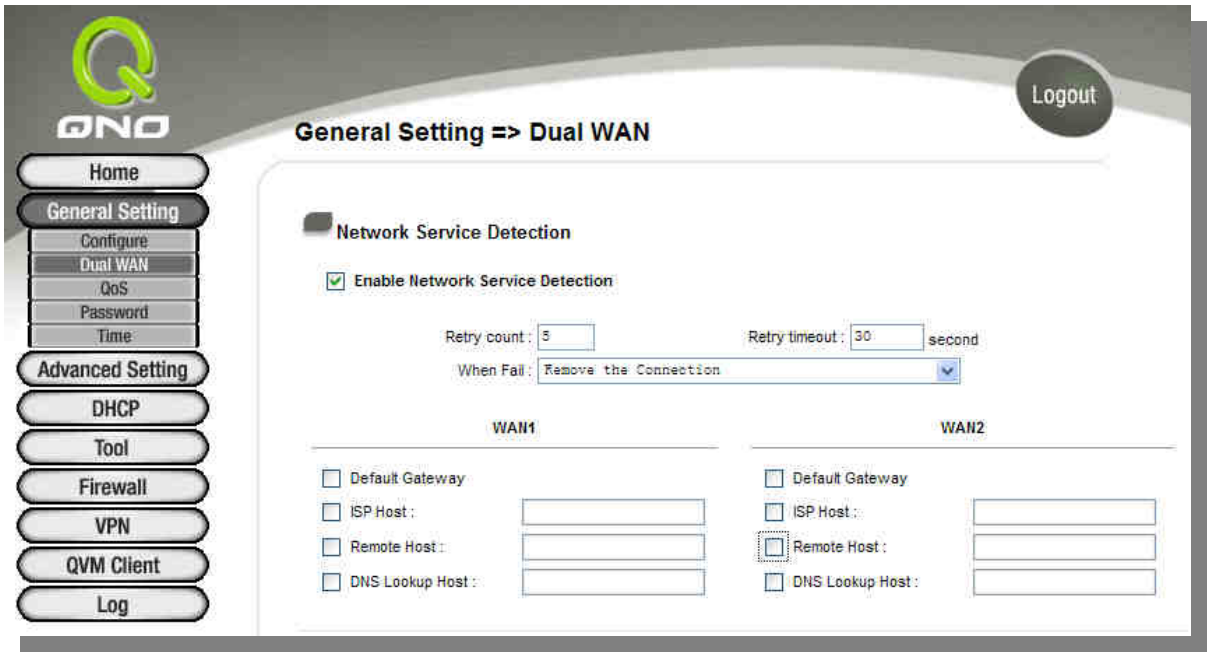
Keep Alive: This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is interrupted. It also enables a user to set up a time for redialing. The default is 30 seconds.

After the changes are completed, click **"Apply"** to save the configuration, or click **"Cancel"** to leave without making any change.

3.3.2 Dual WAN

If you have chosen the second WAN, then you can employment this setting.

Network Service Detection

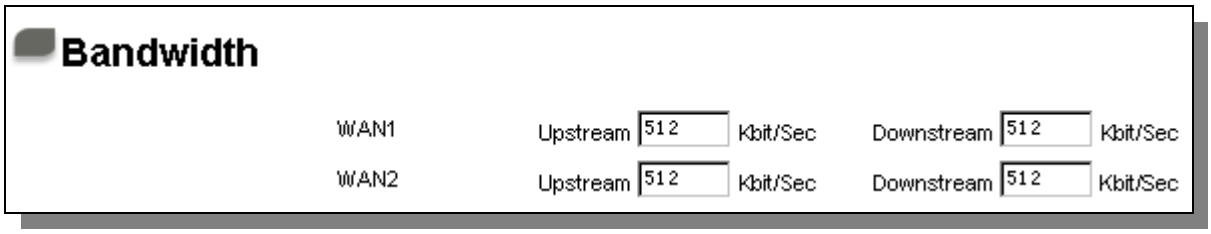


Network Service Detection System: This is a detection system for network external services. If this option is selected, information such "**Retry Count**" or "**Retry Timeout**" will be displayed. If two WANs are used for external connection, be sure to activate the NSD system, so as to avoid any unwanted break caused by the device misjudgment of the overload traffic for the WAN.	
Retry Count:	This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured "Retry Times", it will be judged as "External Connection Interrupted".
Retry Timeout:	Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.
When Fail:	(1) Generate the Error Condition in the System Log: If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections. This option is suitable under the condition that one of the WAN

	connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination. For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 is not to support these destinations, users should select this option. When the WAN1 connection is interrupted, packets for 10.0.0.1~10.254.254.254 cannot be transmitted through WAN 2, and there is no need to remove the connection when WAN 1 is interrupted. (2) Remove the Connection: If an ISP connection failure is detected, no error message will be recorded in the System Log. The packet transmitted through this WAN will be shifted to the other WAN automatically, and be shifted back again when the connection for the original WAN is repaired and reconnected. This option is suitable when one of the WAN connections fails and the traffic going through this WAN to the destination IP should go through the other WAN to reach the destination. In this way, when any of the WAN connections is broken, other WANs can serve as a backup; traffic can be shifted to a WAN that is still connected.
Detecting Feedback Servers:	
Default Gateway:	The local default communication gateway location, such as the IP address of an ADSL router, will be input automatically by the device. Therefore, users just need to check the option if this function is needed. Attention! Some gateways of an ADSL network will not affect packet detection. If users have an optical fiber box, or the IP issued by ISP is a public IP and the gateway is located at the port of the net café rather than at the IP provider's port, do not activate this option.
ISP Server:	This is the detected location for the ISP port, such as the DNS IP address of ISP. When configuring an IP address for this function, make sure this IP is capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port)

Remote Server:	This is the detected location for the remote Network Segment. This Remote Host IP should better be capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port).
Use DNS server for Domain Name Service:	This is the detect location for DNS. (Only a web address such as www.hinet.net is acceptable here. Do not input an IP address.) In addition, do not input the same web address in this box for two different WANs.
Apply:	After the changes are completed, click **"Apply"** to save the network configuration modification.
Cancel:	Click **"Cancel"** to leave without making any change, but only it works before you click apply button.

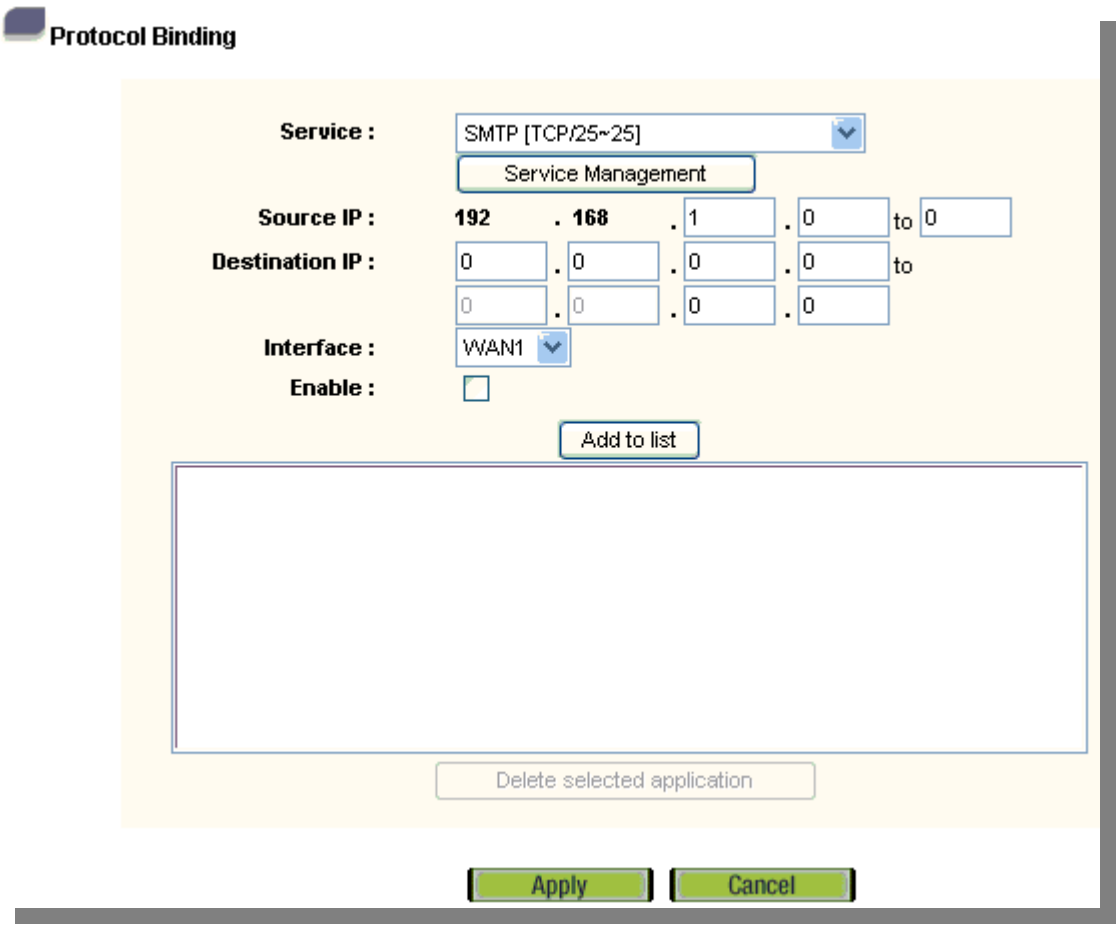
Bandwidth



Automatic load balance ratio will be made according to the upstream bandwidth users input for the two WAN ports. For instance, if the upstream bandwidth for both WANs is 512Kbit/sec, the automatic balance ratio will be 1:1. If one WAN upstream bandwidth is 1024Kbit/sec while the other is 512Kbit/sec, the automatic balance ratio will be 2:1. Therefore, to ensure the load can be really balanced, please input the actual upstream and downstream bandwidth. In addition, the data users input will also affect the QoS configuration. Please refer to **QoS Configuration.**

Protocol Binding

Users can define specific IP addresses or specific application service ports to go through a user-assigned WAN for external connections. For any other unassigned IP addresses and services, WAN load balancing will still be carried out.

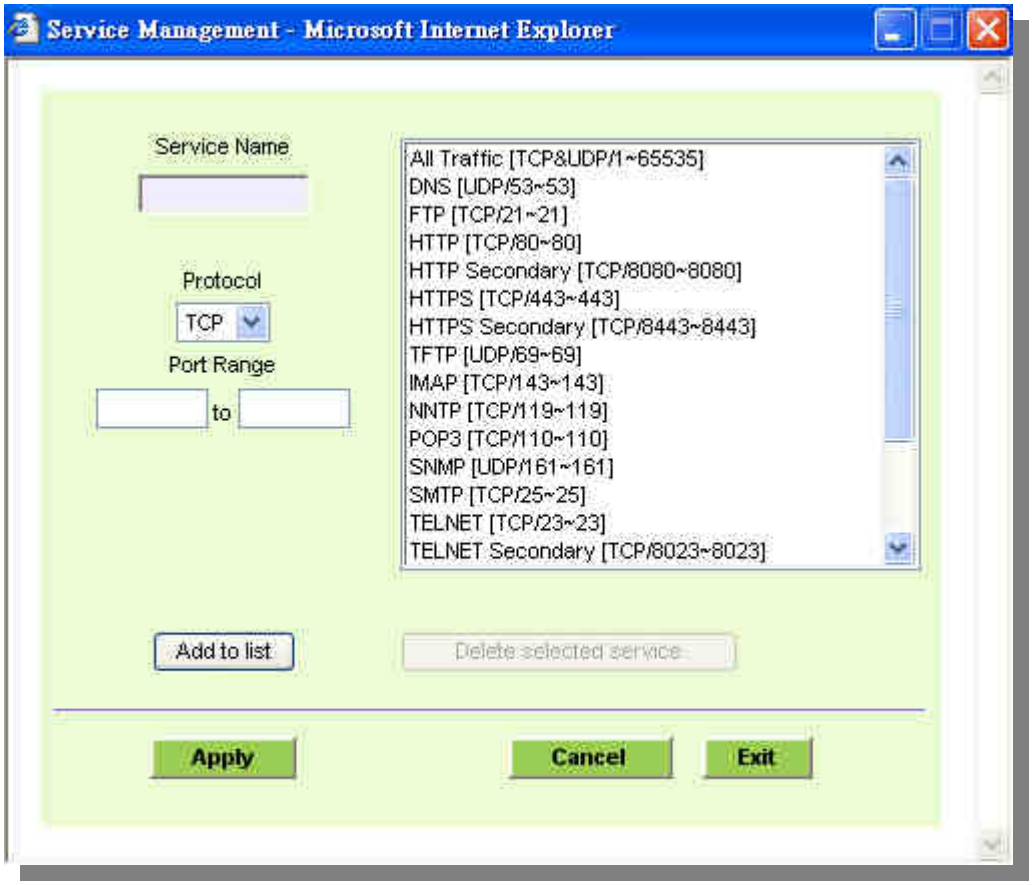


Service:	This is to select the Binding Service Port to be activated. The default (such as ALL-TCP&UDP 0~65535, WWW 80~80, FTP 21 to 21, etc.) can be selected from the pull-down option list. The default Service is All 0~65535. Option List for Service Management: Click the button to enter the Service Port configuration page to add or remove default Service Ports on the option list.
Source IP:	Users can assign packets of specific Intranet virtual IP to go through a specific WAN port for external connection. In the boxes here, input the Intranet virtual IP address range; for example, if 192.168.1.100~150 is input, the binding range will be 100~150. If only specific Service Ports need to be designated, while specific IP designation is not necessary, input "0" in the IP boxes.
Destination IP:	In the boxes, input an external static IP address. For example, if connections to destination IP address 210.11.1.1 are to be

	restricted to WAN1, the external static IP address 210.1.1.1 ~ 210.1.1.1 should be input. If a range of destinations is to be assigned, input the range such as 210.11.1.1 ~ 210.11.255.254. This means the Class B Network Segment of 210.11.x.x will be restricted to a specific WAN. If only specific Service Ports need to be designated, while a specific IP destination assignment is not required, input "0" into the IP boxes.
Interface:	Select the WAN for which users want to set up the binding rule.
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Delete selected application:	To remove the rules selected from the Service List.
Apply:	Click **"Apply"** to save the modification.
Cancel:	Click **"Cancel"** to leave without making any change, but only it works before you click apply button.

Add or Remove Service Ports

If the Service Port users want to activate is not in the list, users can click "Add or Remove Service Ports from "Service Management" to arrange the list, as described in the following:

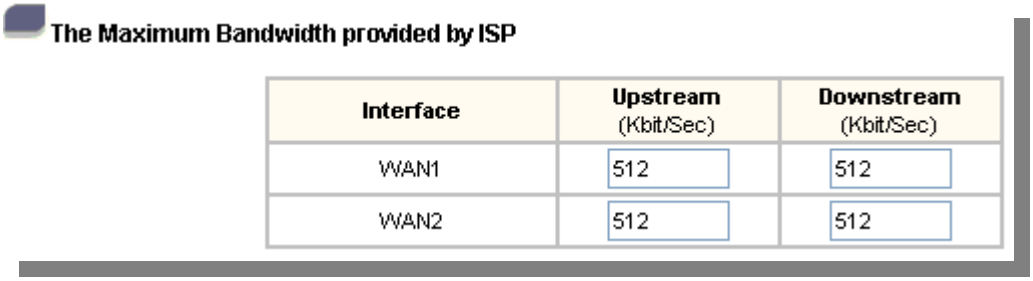


Service Name:	In this box, input the name of the Service Port which users want to activate, such as BT, etc.
Protocol:	This option list is for selecting a packet format such as TCP or UDP for the Service Ports users want to activate.
Port range:	In the boxes, input the range of Service Ports users want to add.
Add To List:	Click the button to add the configuration into the Services List. Users can add up to 100 services into the list.
Delete selected service:	To remove the selected activated Services.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.
Exit:	To quit this configuration window.

3.3.3 QoS

QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IPs to save bandwidth or provide priority to specific applications or services, and also to enable other users to share bandwidth, as well as to ensure stable and reliable network transmission. To maximize the bandwidth efficiency, network administrators should take account of the practical requirements of a company, a community, a building, or a café etc, and modify bandwidth management according to the network environment, application processes or services.

QoS Setting

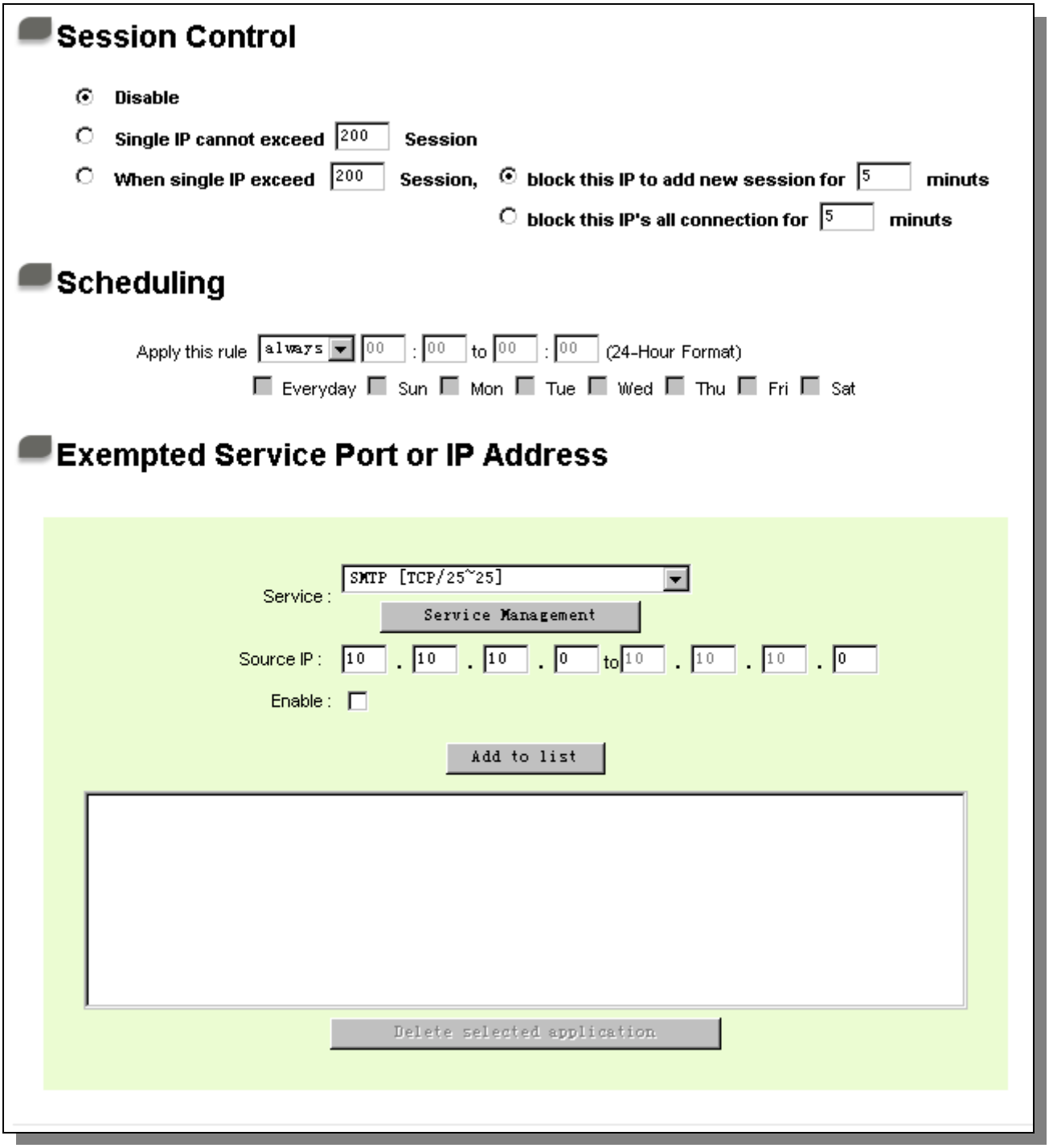


In the boxes for WAN1 and WAN2 bandwidth, input the upstream and downstream bandwidth which users applied for from bandwidth supplier. The bandwidth QoS will make calculations according to the data users input. In other words, it will guarantee a minimum rate of upstream and downstream for each IP and Service Port based on the total actual bandwidth of WAN1 and WAN2. For example, if the upstream bandwidths of both WAN1 and WAN2 are 512Kbit/Sec, the total upstream bandwidth will be: WAN1 + WAN2 = 1024Kbit/Sec. Therefore, if there are 50 IPs in the Intranet, the minimum guaranteed upstream bandwidth for each IP would be 1024Kbit/50=20Kbit/Sec. Thus, 20Kbit/Sec can be input for "Mini. Rate" Downstream bandwidth can be calculated in the same way.

Session Control

Session management controls the acceptable maximum simultaneous connections of Intranet PCs. This function is very useful for managing connection quantity when P2P software such as BT, Thunder, or emule is used in the Intranet causing large numbers of connections. Setting up proper limitations on connections can effectively control the connections created by P2P software. It will also have a limiting effect on bandwidth usage.

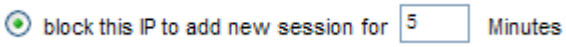
In addition, if any Intranet PC is attacked by a virus like Worm.Blaster and sends a huge number of connection requests, session control will restrict that as well.



Disable: To disable Session Control function.

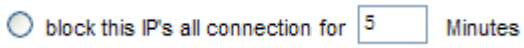
Single IP cannot exceed ___ Session This option enables the restriction of maximum external connections to each Intranet PC. When the number of external connections reaches the limit, to allow new connections to be built, some of the existing connections must be closed. For example, when BT or P2P is being used to download information and the connections exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.

Network Service Detection:



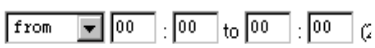
(When single IP exceed limit)

If this function is selected, when the user's port connection reach the limit, this user will not be able to make a new connection for five minutes. Even if the previous connection has been closed, new connections cannot be made until the setting time ends.



If this function is selected, when the user's port connections reach the limit, all the lines that this user is connected with will be removed, and the user will not be able to connect with the Internet for five minutes. New connections cannot be made until the delay time ends.

Scheduling



If "**Always**" is selected, the rule will be executed around the clock. If "**From**…" is selected, the rule will be executed according to the configured time range. For example, if the time control is from Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.

Days Management:

If "**Everyday**" is selected, the rule will be activated for the control time range every day. Users can choose to activate the rule during certain days of the week.

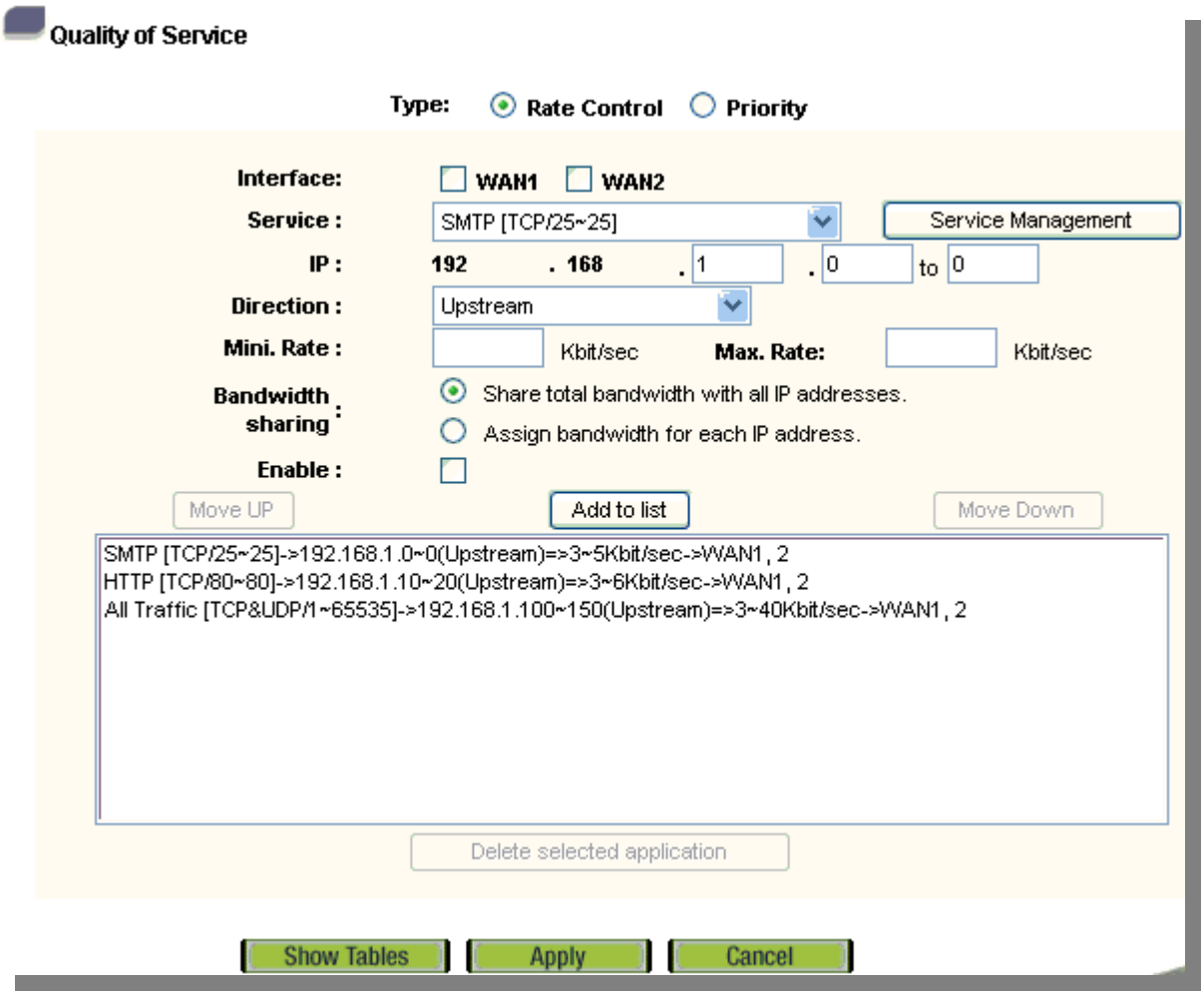
Exempted Port or IP Service:	The important services or IPs in a company or business can be configured to be free of the Connection Restriction Rule.
Service:	To select a Service Port to be free of the connection rule.
Service Management:	To add or remove a Service Port.
Source IP/Group:	To add IP addresses/Groups that are free from restriction.
Enable:	To activate the added rule.
Add To List:	To add the rule into the list.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

QoS Configuration

There are two options for bandwidth management: one is Rate Control, the other is Priority Control. The two kinds of management cannot be used at the same time. Network administrators must choose one or the other based on the Intranet needs.

Rate Control :

The network administrator can set up bandwidth or usage limitations for each IP or IP range according to the actual bandwidth. The network administrator can also set bandwidth control for certain Service Ports. A guarantee bandwidth control for external connections can also be configured if there is an internal server.



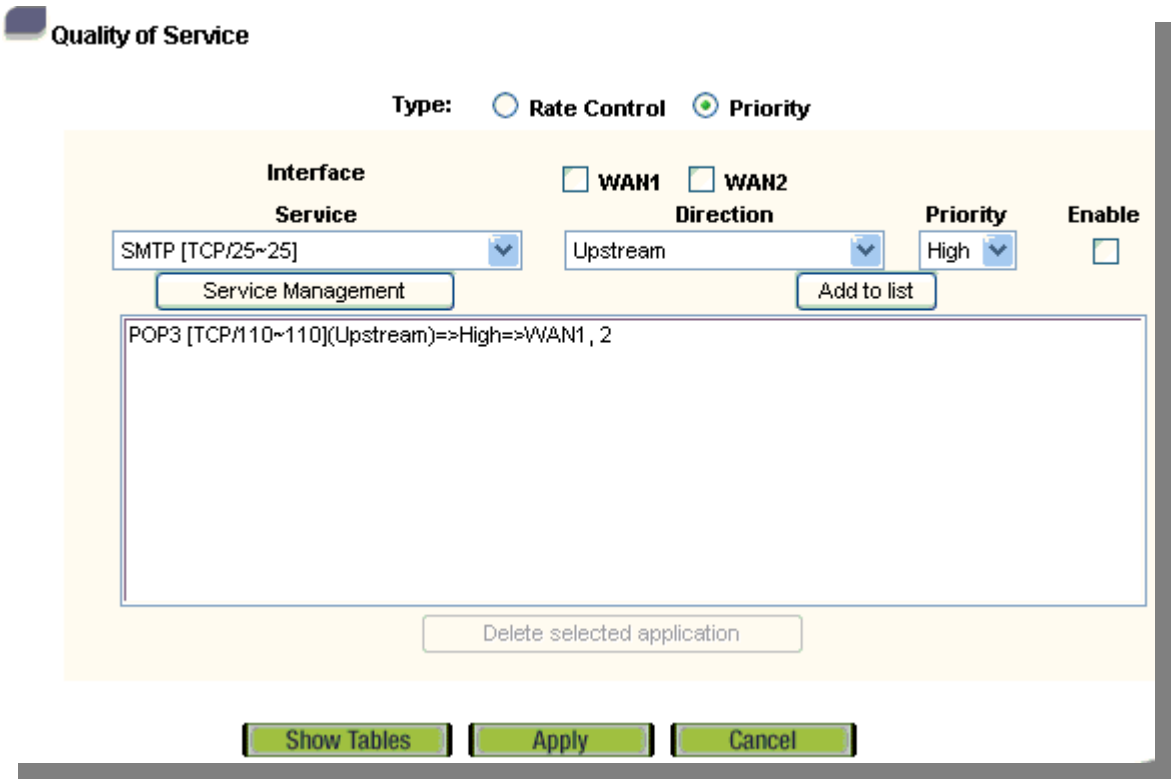
Interface:	To select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service:	To select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select "All (TCP&UDP) 1~65535". If only FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
IP:	This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 150". The rule will control IPs from 192.168.1.100 to 150. If all

	Intranet users that connect with the device are to be controlled, input "0" in the boxes of IP address. This means all Intranet IPs will be restricted. QoS can also control the range of Class B.
Direction:	**Upstream:** Means the upload bandwidth for Intranet IP. **Downstream:** Means the download bandwidth for Intranet IP. **Server in LAN, Upstream:** If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server. **Server in LAN, Downstream:** If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.
Min. & Max. Rate: (Kbit/Sec)	The minimum bandwidth: The rule is to guarantee minimum available bandwidth. The maximum bandwidth: This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule. **Attention!** The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.
Bandwidth Sharing:	Sharing total bandwidth with all IP addresses: If this option is selected, all IPs or Service Ports will share the bandwidth range (from minimum to maximum bandwidth). Assign bandwidth for each IP address: If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum.). For example: If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth. **Attention:** If "Share-Bandwidth" is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small. For example, if users do not want an FTP to occupy too

	much bandwidth, users can select the "Share-Bandwidth Mode", so that no matter how much users use FTPs to download information, the total occupied bandwidth is fixed.
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Move up & Move Down:	The QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. Usually the service ports which need to be restricted, such as BT, e-mule etc., will be moved to the bottom of the list. The rules for certain IPs would then be moved upward.
Delete selected application:	To remove the rules selected from the Service List.
Show Table:	This will display all the Rate Control Rules users made for the bandwidth. Click "Edit" to modify.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

Priority Control :

The Router will distribute the bandwidth as 60% (the highest) and 10% (the lowest). If you set the service port 80 as "High" priority, the router will give 60% bandwidth to the port 80. In the other hand, if you give the port 21 as "Low" priority, the device will only give it 10% bandwidth. The remained 30% bandwidth will be shared by the other service.

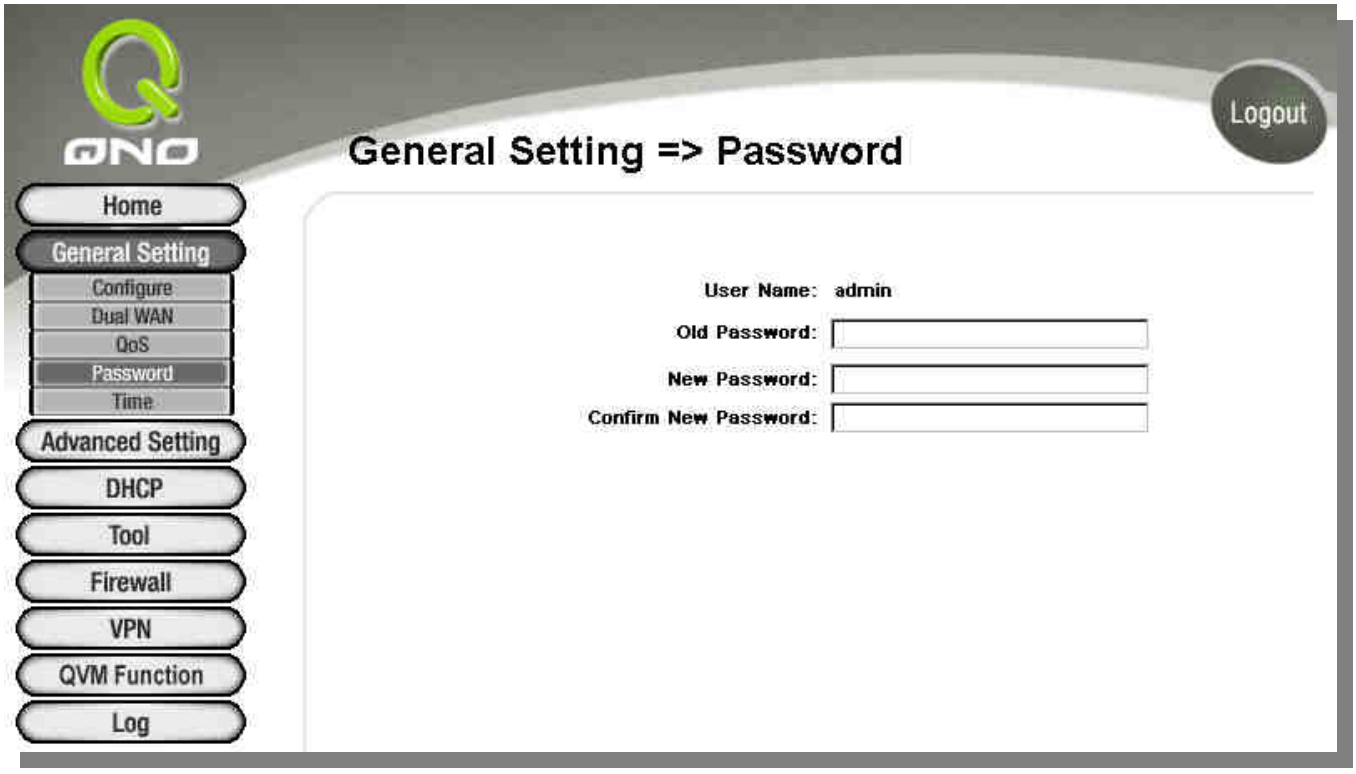


Interface :	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service Port :	Select what bandwidth control is to be configured in the QoS rule. If FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
Direction :	Upstream: Means the upload bandwidth for Intranet IP. Downstream: Means the download bandwidth for Intranet IP. Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server. Server in LAN, Downstream: If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.

Priority :	High: 60% guaranteed bandwidth to the service Low: Only 10% bandwidth offered to the service
Enabled :	Activate the rule.
Add to list :	Add this rule to the list.
Delete Selected items :	Remove the rules selected from the Service List.
Show Table :	This will display all the Priority Rules users made for the bandwidth. Click "Edit" to modify.
Apply :	Click **"Apply"** to save the configuration
Cancel :	Click **"Cancel"** to leave without making any change.

3.3.4 Password

This is an advanced management tool for the device. The default password of the host is "admin". Users can change the password after configuration has been completed. Remember to click "**Apply**" when the configuration data has been completed.



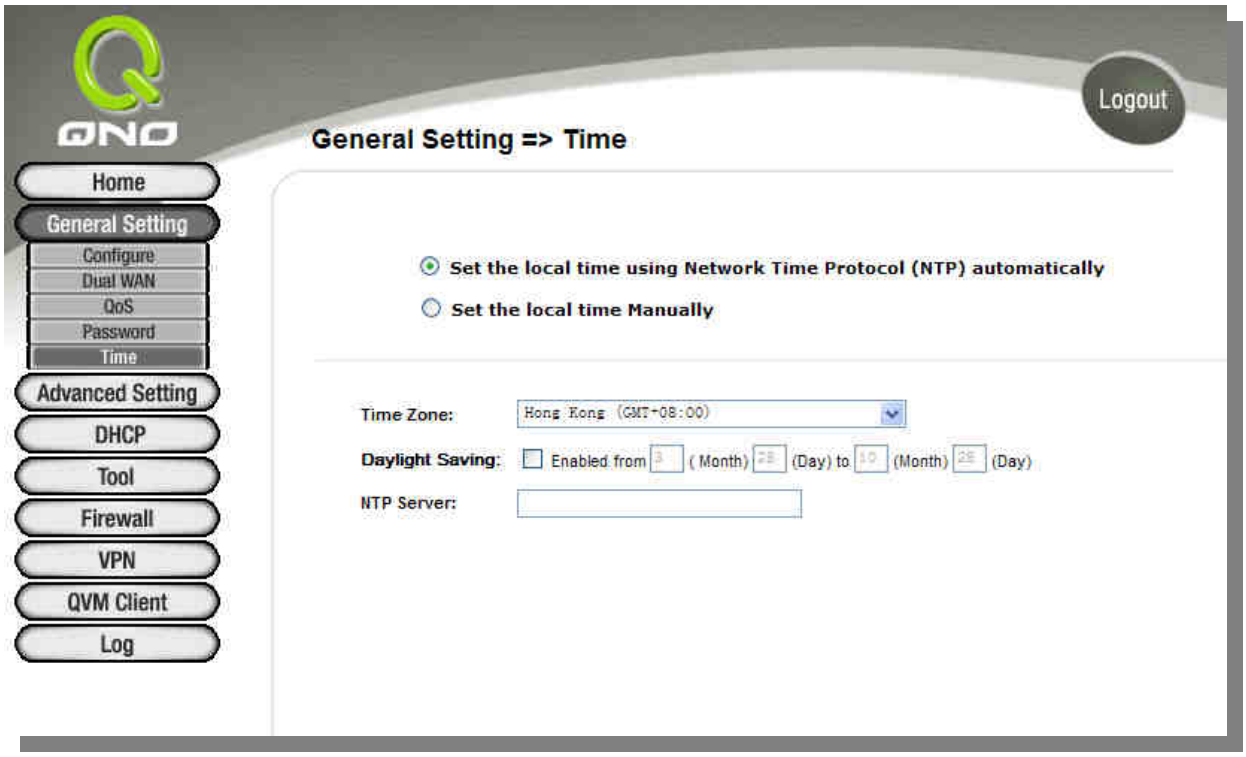
User Name:	The default is "admin".
Old Password:	Input the original password.
New User Name:	Input the new user name.
New Password:	Input the changed password.
Confirm New Password:	Input the new password again for verification.

3.3.5 Time

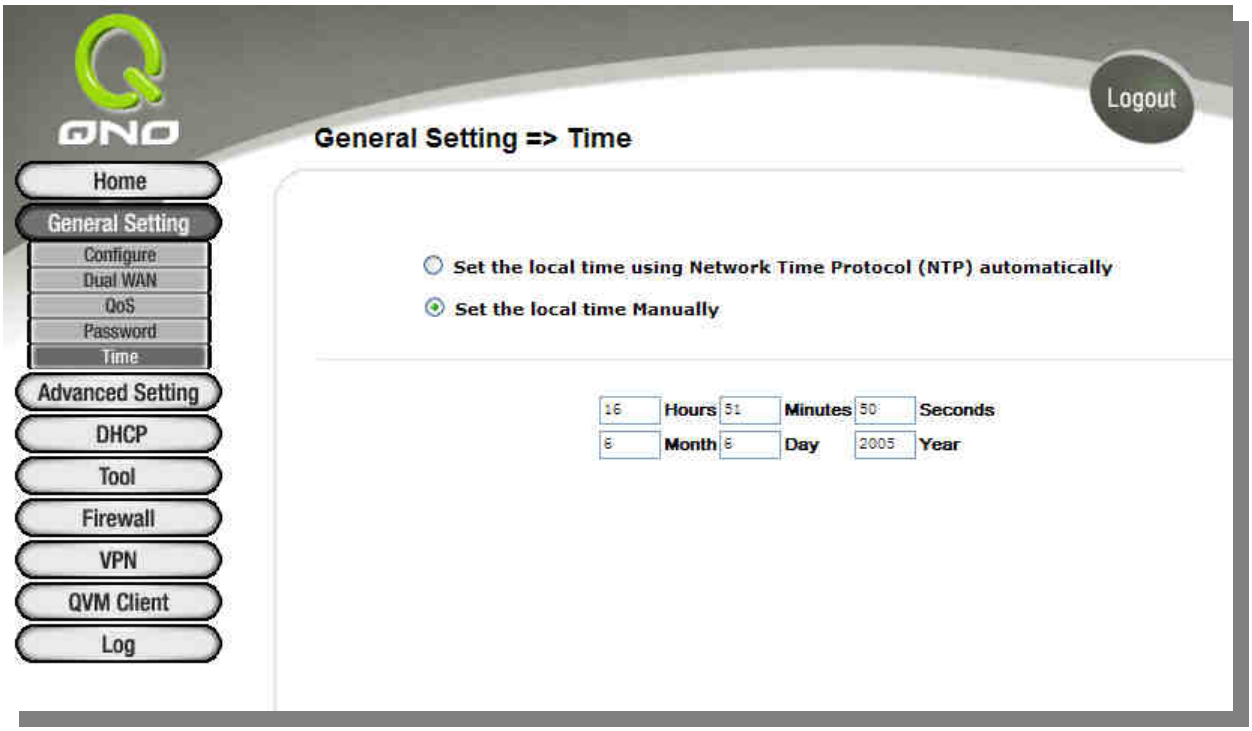
A function to calculate the correct time is available with the device. Users can either select the embedded NTP Server synchronization function or set up a time reference. This function enables users to know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources.

Configuring Automatic Synchronize With NTP Function

Select the time zone from the "**Time Zone"** pull-down option list. If there is **Daylight Saving Time** in the area, input it. The device will adjust the time for the Daylight Saving period automatically. If users have their own "**Time Server Address**", input the Server's IP address.



Input Date and Time Manually



Input the correct date and time in the boxes.

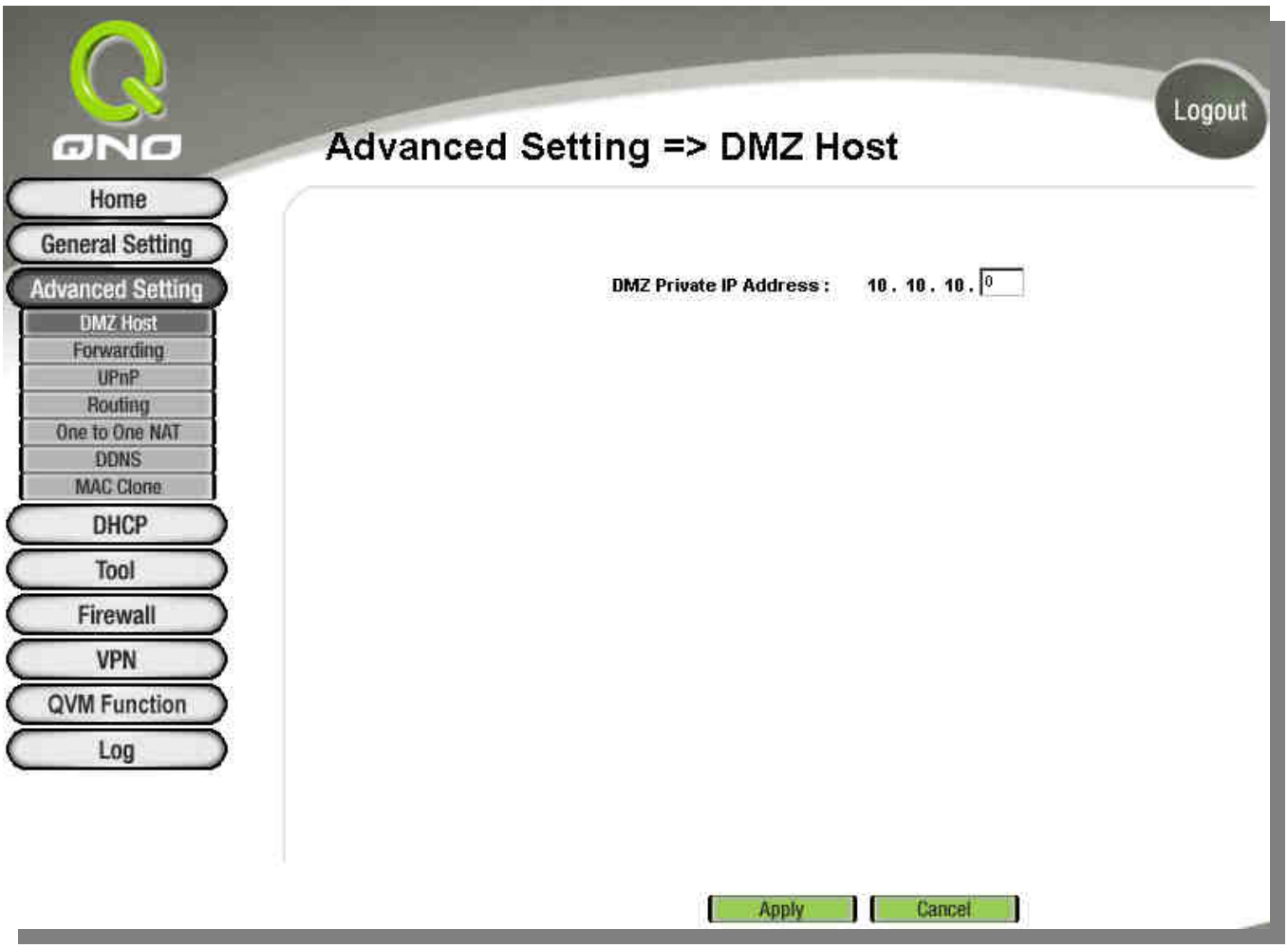
After the changes are completed, click **"Apply"** to save the configuration, or click **"Cancel"** to leave without making any changes.

IV. Advanced Configuration

This chapter introduces the VPN Firewall advanced configuration, including opening the link of virtual server, routing setting, physical IP corresponding to virtual IP as well as setting dynamic DNS, etc.

4.1 DMZ Host-(Demilitarized Zone)

When the NAT mode is activated, sometimes users may need to use applications that do not support virtual IP addresses such as network games. We recommend that users map the device actual WAN IPs directly to the Intranet virtual IPs, as follows:



If the "**DMZ Host**" function is selected, to cancel this function, users must input "0" in the following "DMZ Private IP". This function will then be closed.

After the changes are completed, click **"Apply"** to save the network configuration

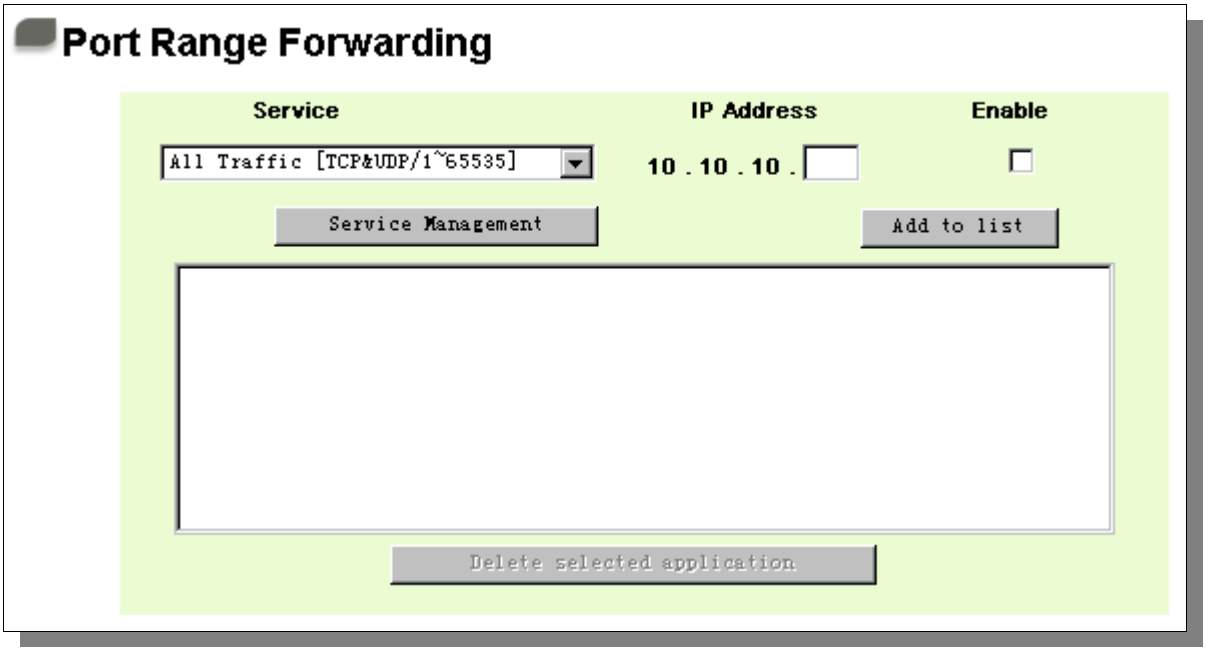
modification, or click **"Cancel"** to leave without making any changes.

4.2 Forwarding

Setting up a Port Forwarding Virtual Host: If the server function (which means the server for an external service such as WWW, FTP, Mail, etc) is contained in the network, we recommend that users use the firewall function to set up the host as a virtual host, and then convert the actual IPs (the Internet IPs) with Port 80 (the service port of WWW is Port 80) to access the internal server directly. In the configuration page, if a web server address such as 192.168.1.2 and the Port 80 have been set up in the configuration, this web page will be accessible from the Internet by keying in the device actual IP address such as: http://220.130.188.45 (This is VPN Firewall legal IP address).

At this moment, the device actual IP will be converted into "192.168.1.2" by Port 80 to access the web page.

In the same way, to set up other services, please input the server TCP or UDP port number and the virtual host IP addresses.



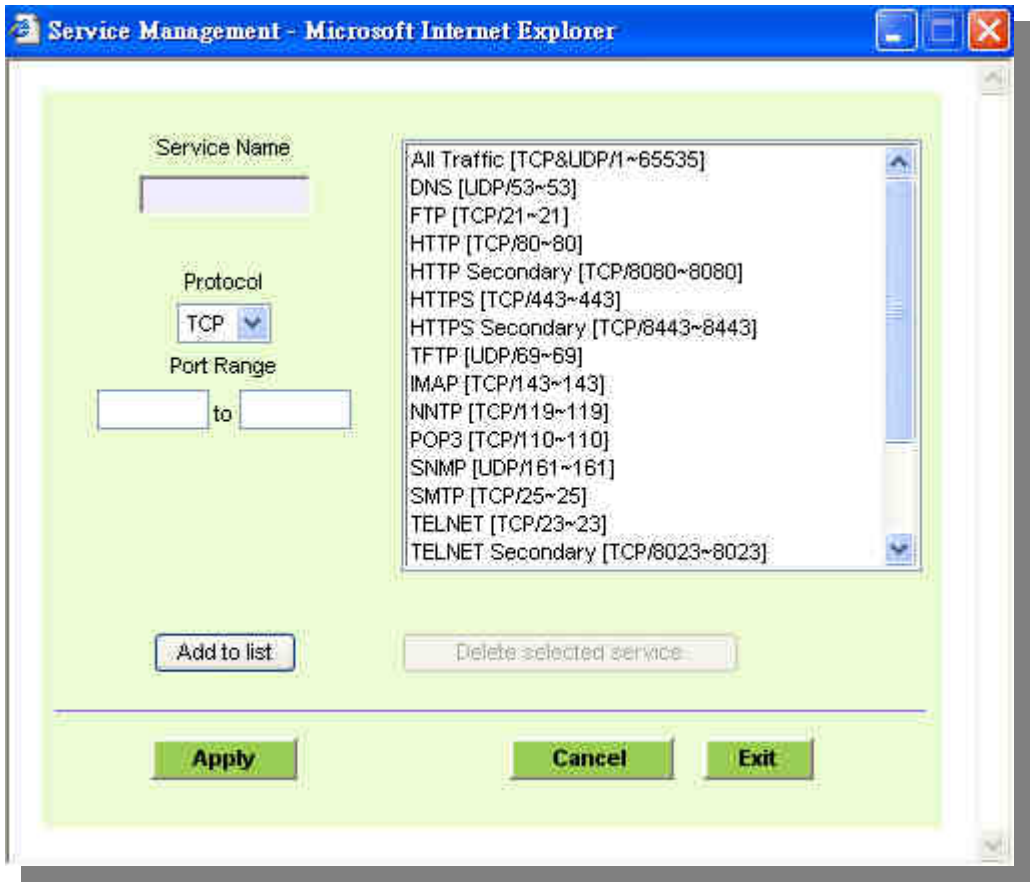
Service: To select from this option the default list of service ports of the virtual host that users want to activate.

Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and

	21~21 for FTP. Please refer to the list of default service ports.
Internal IP Address:	Input the virtual host IP addresses.
Enable:	To activate this function.
Service Management:	Add or remove service ports from the list of service ports.
Add to list:	Add to the active service content.

Add or Remove Service Ports

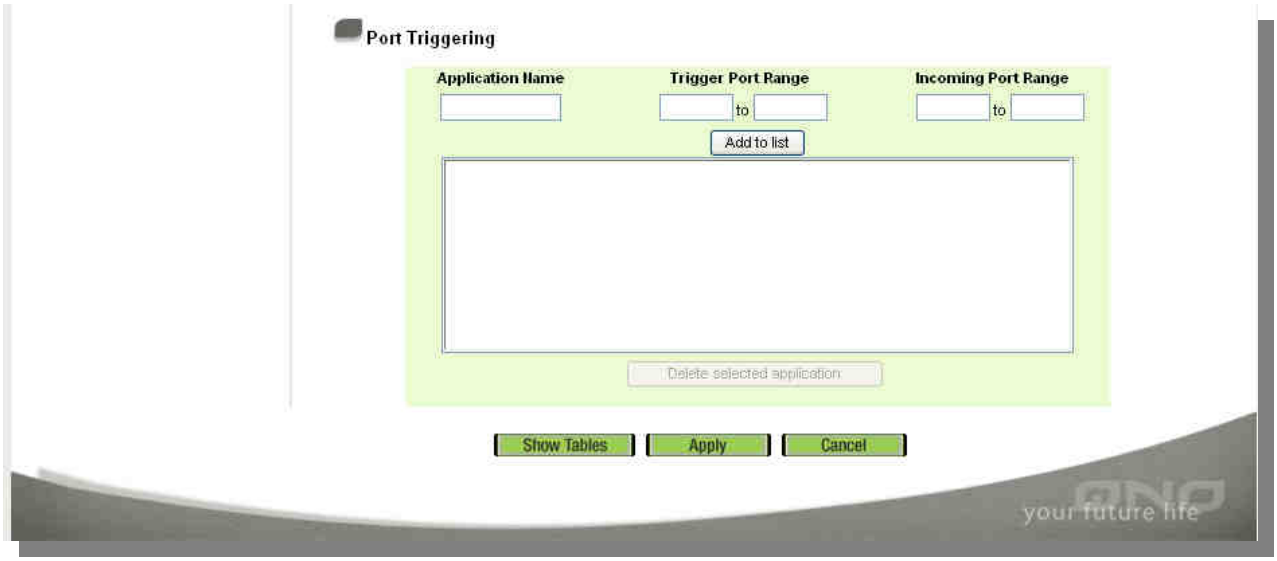
The services in the list mentioned above are frequently used services. If the service users want to activate is not in the list, we recommend that users use "Service Management" to add or remove ports, as follows:



Service Name:	In this box, input the name of the Service Port which users want to activate, such as BT, etc.
Protocol:	This option list is for selecting a packet format such as TCP or UDP for the Service Ports users want to activate.
Port range:	In the boxes, input the range of Service Ports users want to add.
Add To List:	Click the button to add the configuration into the Services List. Users can add up to 100 services into the list.
Delete selected service:	To remove the selected activated Services.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.
Exit:	To quit this configuration window.

Port Triggering :

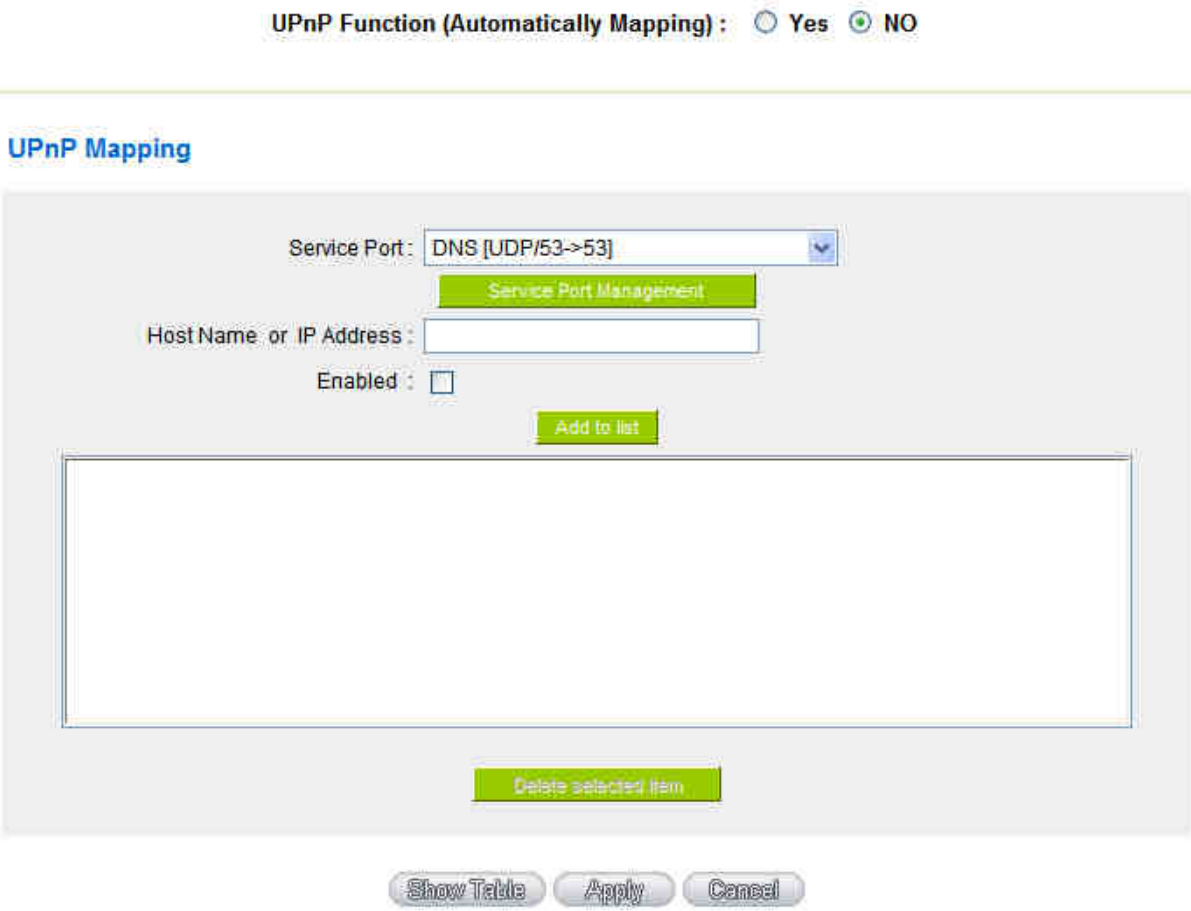
For some special application software, the Internet accessing port numbers are unsymmetrical. Therefore, the port numbers for this special software must be input in the "Port Triggering", as in the above fig.



Application Name:	Users can define names for special application software. This is to make management simple.
Trigger Port Range:	Input the port numbers for data going from the device to the Internet. (Such as 9000~6600).
Incoming Port Range:	Input the port numbers for data coming in from the Internet to the device. (Such as 2004~2005).
Add to list:	Add the service to the active service list.
Delete selected application:	To remove selected services.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

4.3 UPnP- (Universal Plug and Play)

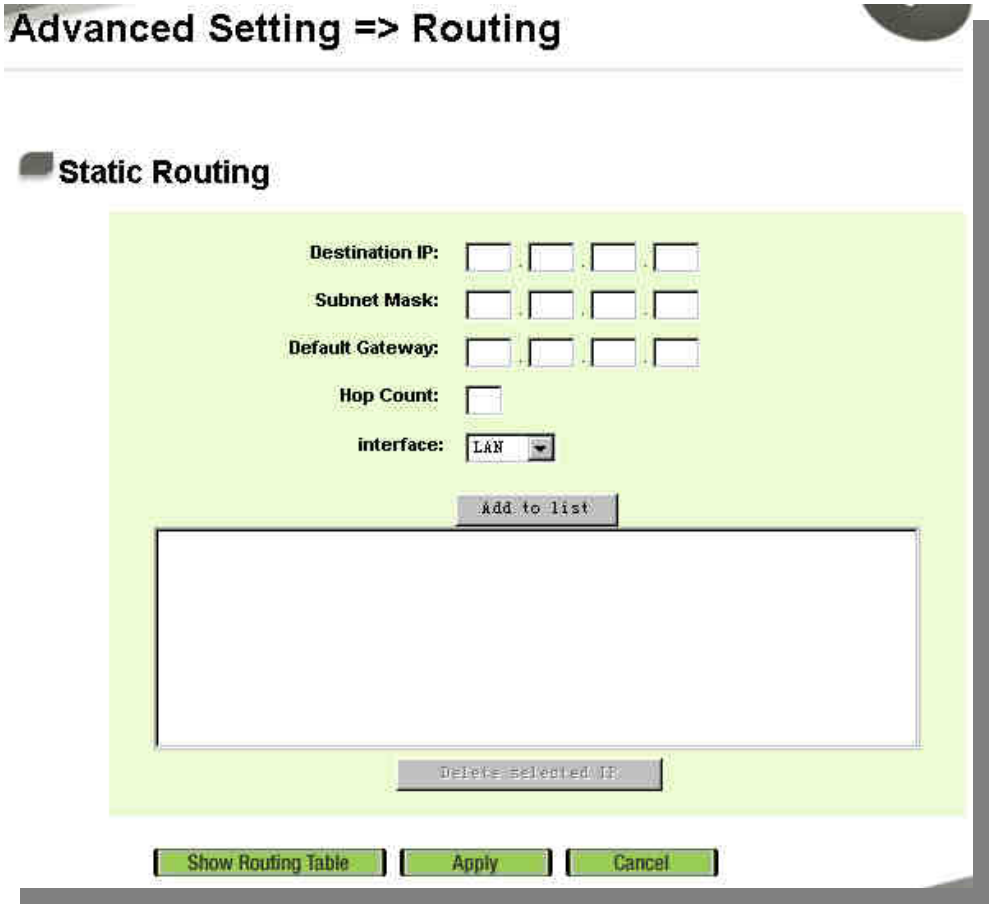
UPnP (Universal Plug and Play) is a protocol set by Microsoft. If the virtual host supports UPnP system (such as Windows XP), users could also activate the PC UPnP function to work with the device.



Service Port :	Select the UPnP service number default list here; for example, WWW is 80~80, FTP is 21~21. Please refer to the default service number list.
Host Name or IP Address :	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.
Enabled :	Activate this function.
Service Port Management :	Add or remove service ports from the management list.
Add to List :	Add to active service content.
Delete Selected Item :	Remove selected services.
Show Table :	This is a list which displays the current active UPnP functions.
Apply :	Click "Apply" to save the network configuration modification.
Cancel :	Click "Cancel" to leave without making any change.

4.4 Routing

When there are more than one router and IP subnets, the routing mode for the device should be configured as static routing. Static routing enables different network nodes to seek necessary paths automatically. It also enables different network nodes to access each other. Click the button "**Show Routing Table**" (as in the figure) to display the current routing list.



Destination IP / Subnet Mask :	Input the remote network IP locations and subnet that is to be routed. For example, the IP/subnet is 192.168.2.0/255.255.255.0.
Default Gateway :	The default gateway location of the network node which is to be routed.
Hop Count :	This is the router layer count for the IP. If there are two routers under the device, users should input "2" for the router layer; the default is "1". (Max. is 15.)

Interface :	This is to select "WAN port" or "LAN port" for network connection location.
Add to list / Delete selected IP :	Add the routing rule into the list or remove the selected routing rule from the list.
Show Running Table :	Show current routing table.

4.5 One-to-One NAT

As both the device and ATU-R need only one actual IP, if ISP issued more than one actual IP (such as eight ADSL static IP addresses or more), users can map the remaining real IP addresses to the intranet PC virtual IP addresses. These PCs use private IP addresses in the Intranet, but after having One to One NAT mapping, these PCs will have their own public IP addresses.

For example, if there are more than 2 web servers requiring public IP addresses, administrators can map several public IP addresses directly to internal private IP addresses.

Example : Users have five available IP addresses - 210.11.1.1~5, one of which, 210.11.1.1, has been configured as a real IP for WAN, and is used in NAT. Users can respectively configure the other four real IP addresses for Multi-DMZ, as follows:

210.11.1.2→ 192.168.1.3

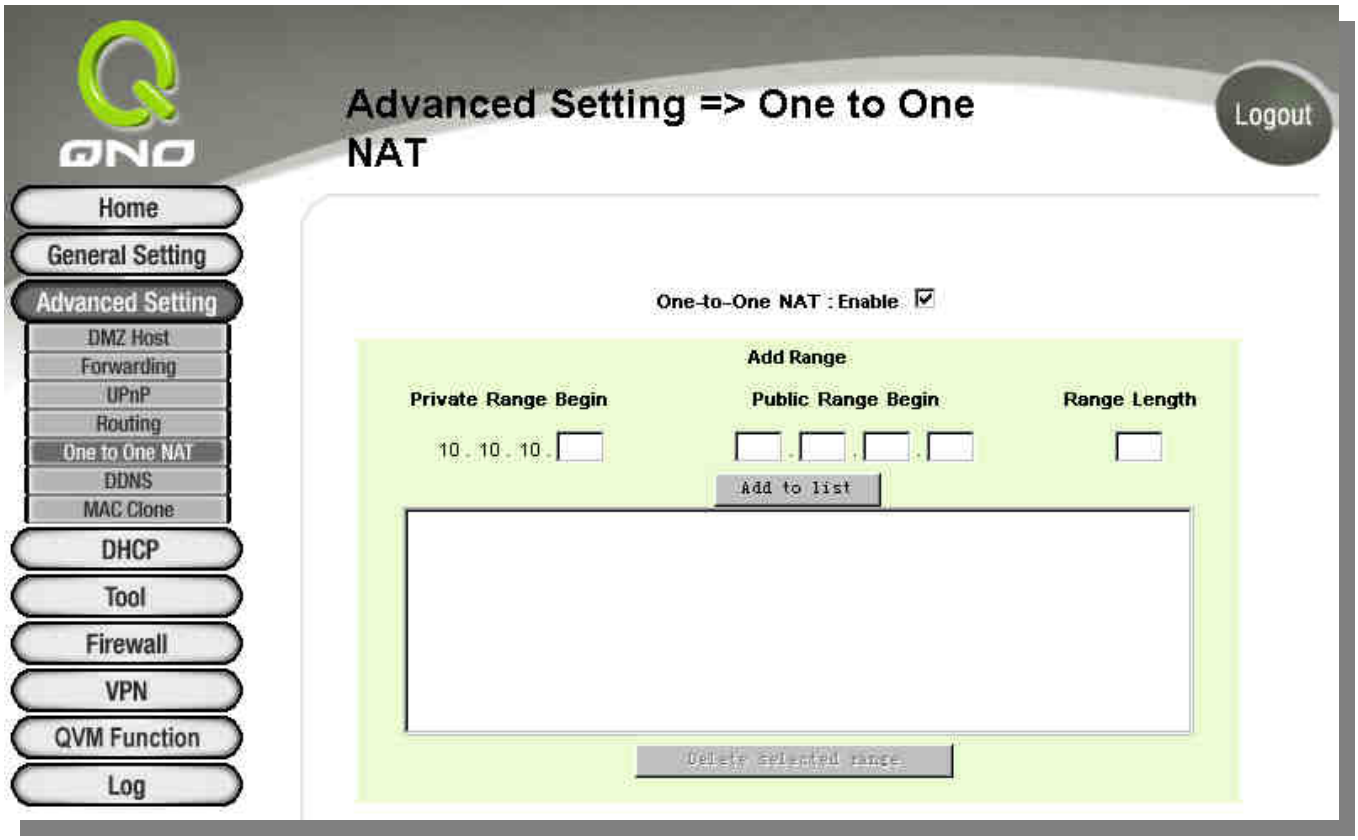
210.11.1.3→ 192.168.1.4

210.11.1.4→ 192.168.1.5

210.11.1.5→ 192.168.1.6

Attention !

The device WAN IP address can not be contained in the One-to-One NAT IP configuration.



One to One NAT :	To enable or close the One-to-One NAT function. (Check to "Enable" or "Close" the function).
Private IP Range Begin :	Input the Private IP address for the Intranet One-to-One NAT function.
Public IP Range Begin :	Input the Public IP address for the Internet One-to-One NAT function.
Range Length :	The numbers of final IP addresses of actual Internet IP addresses. (Please do not include IP addresses in use by WANs.)
Add to List :	Add this configuration to the One-to-One NAT list.
Delete Sleeted Item :	Remove a selected One-to-One NAT list.
Apply :	Click **"Apply"** to save the network configuration modification.
Cancel :	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

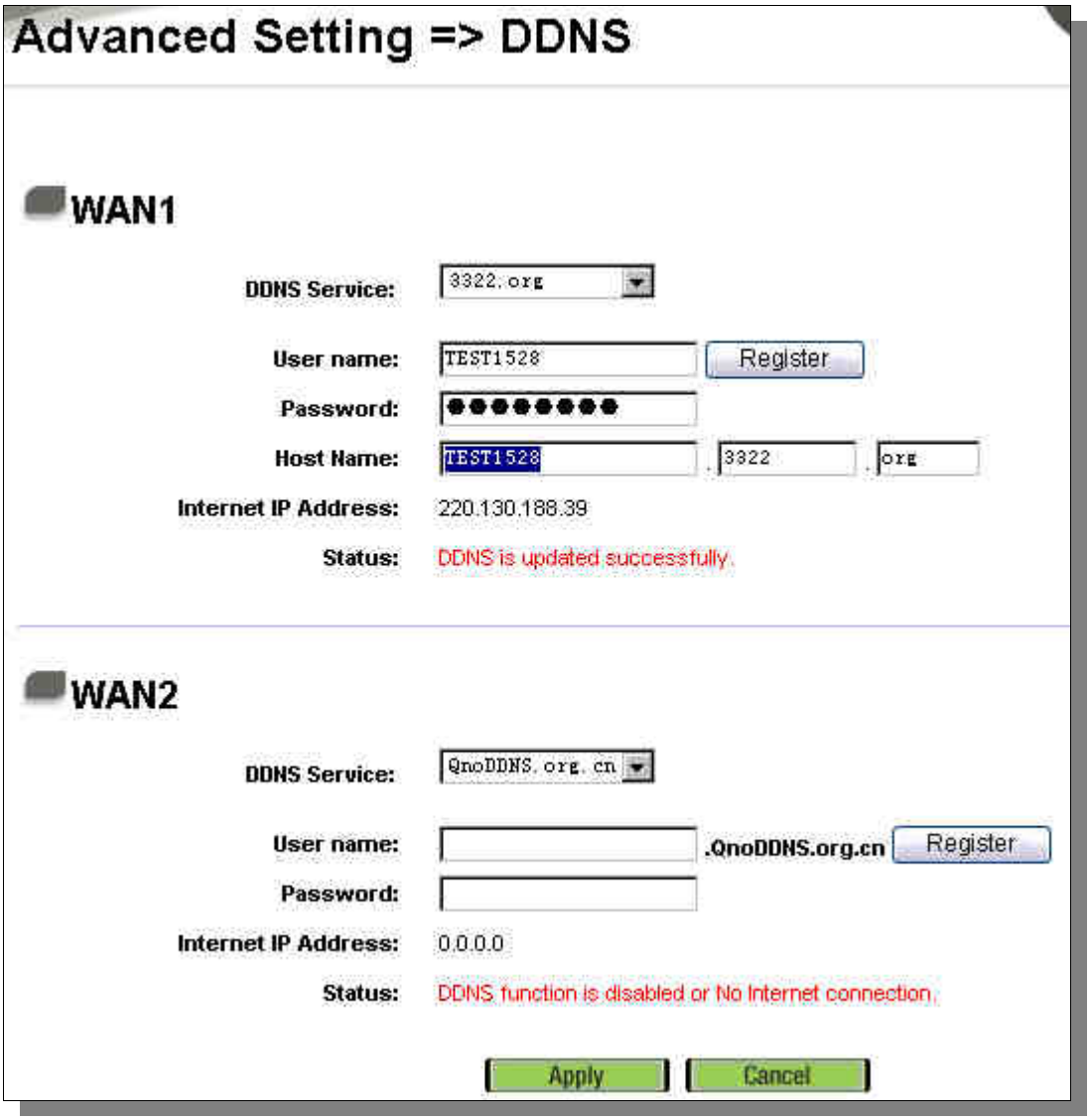
Attention: One-to-One NAT mode will change the firewall working mode. If this function

has been set up, the Internet IP server or PC which is mapped with a LAN port will be exposed on the Internet. To prevent Internet users from actively connecting with the One-on-One NAT server or PC, please set up a proper denial rule for access, as described Firewall.

4.6 DDNS- Dynamic Domain Name Service

DDNS supports the dynamic web address transfer for QnoDDNS.org.cn, 3322.org, DynDNS.org and DtDNS.com. This is for VPN connections to a website that is built with dynamic IP addresses, and for dynamic IP remote control. For example, the actual IP address of an ADSL PPPoE time-based system or the actual IP of a cable modem will be changed from time to time. To overcome this problem for users who want to build services such as a website, it offers the function of dynamic web address transfer. This service can be applied from www.qno.cn/ddns, www.3322.org, www.dyndns.org, or www.dtdns.com, and these are free.

Also, in order to solve the issue that DDNS server is not stable, the device can update the dynamic IP address with different services at the same time.

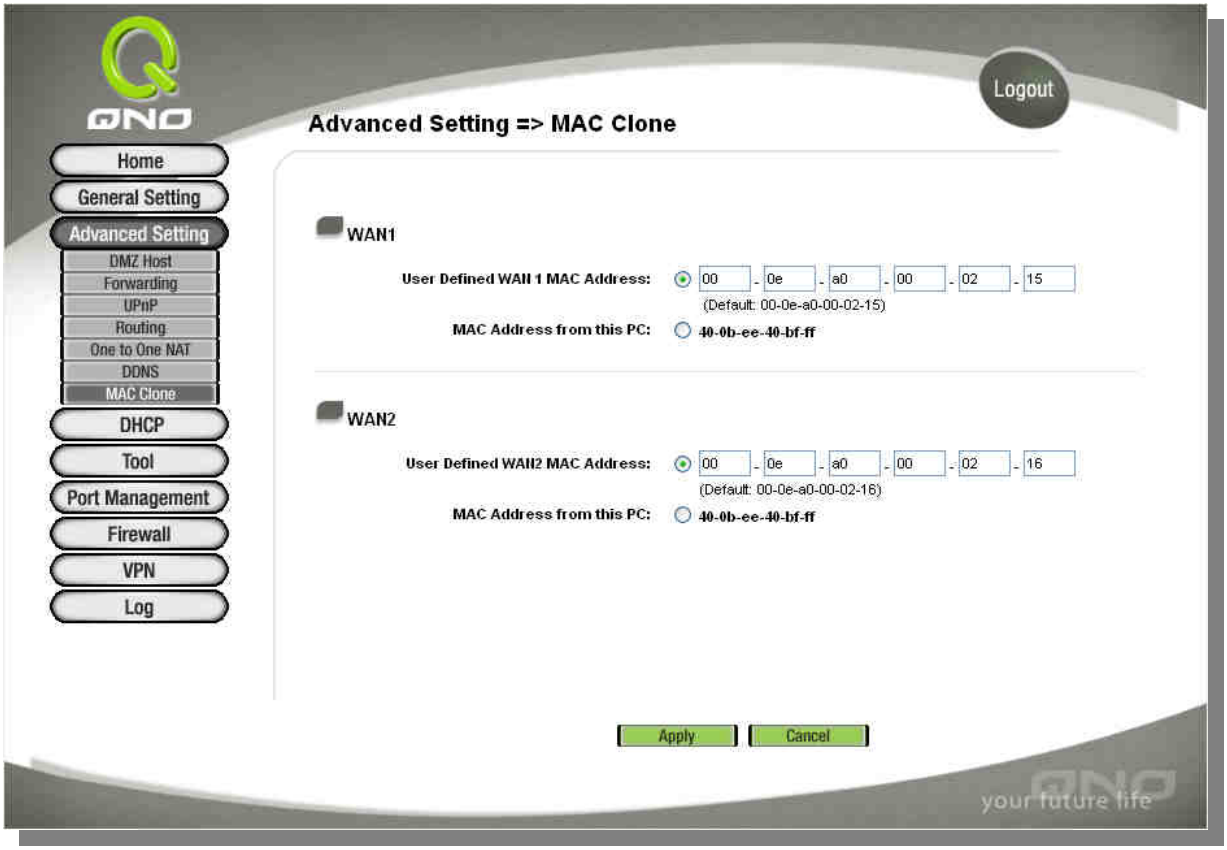


DDNS	Check either of the boxes before DynDNS.org, 3322.org, DtDNS.com and QnoDDNS.org.cn to select one of the four DDNS website address transfer functions.
User name	The name which is set up for DDNS. Input a complete website address such as abc.qnoddns.org.cn as a user name for QnoDDNS.
Password	The password which is set up for DDNS.
Host Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.

Internet IP Address	Input the actual dynamic IP address issued by the ISP.
Status	An indication of the status of the current IP function refreshed by DDNS.
Apply	After the changes are completed, click "Apply" to save the network configuration modification.
Cancel	Click the "Cancel" button to cancel the modification. This only works before "Apply" is clicked.

4.7 MAC Clone

Some ISP will request for a fixed MAC address (network card physical address) for distributing IP address, which is mostly suitable for cable mode users. Users can input the network card physical address (MAC address: 00-xx-xx-xx-xx-xx) here. The device will adopt this MAC address when requesting IP address from ISP.



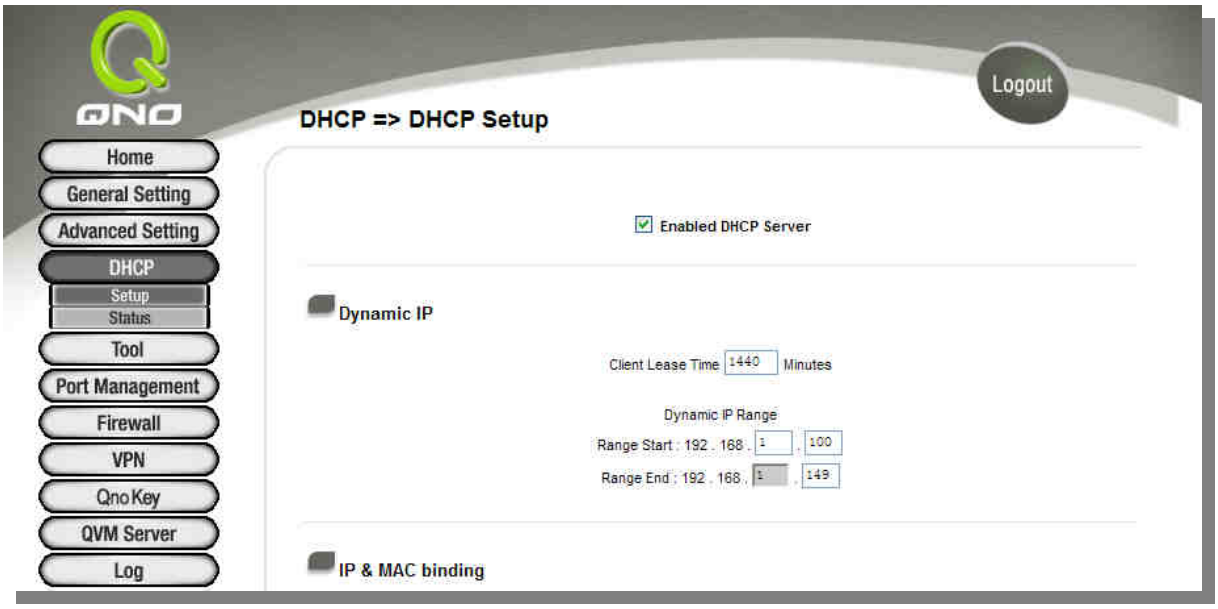
User Defined WAN MAC Address:	The default MAC location of the current equipment.
MAC Address from connected device:	Current address of MAC that is connected with this PC.
Apply	After the changes are completed, click **"Apply"** to save the network configuration modification.
Cancel	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

4.8 DHCP IP Issuing Server

With an embedded DHCP server, it supports automatic IP acquisition for LAN computers. (This function is similar to the DHCP service in NT servers. It benefits users by freeing them from the inconvenience of recording and configuring IP addresses for each PC respectively. When a computer is turned on, it will acquire an IP address from the device automatically. This function is to make management easier.)

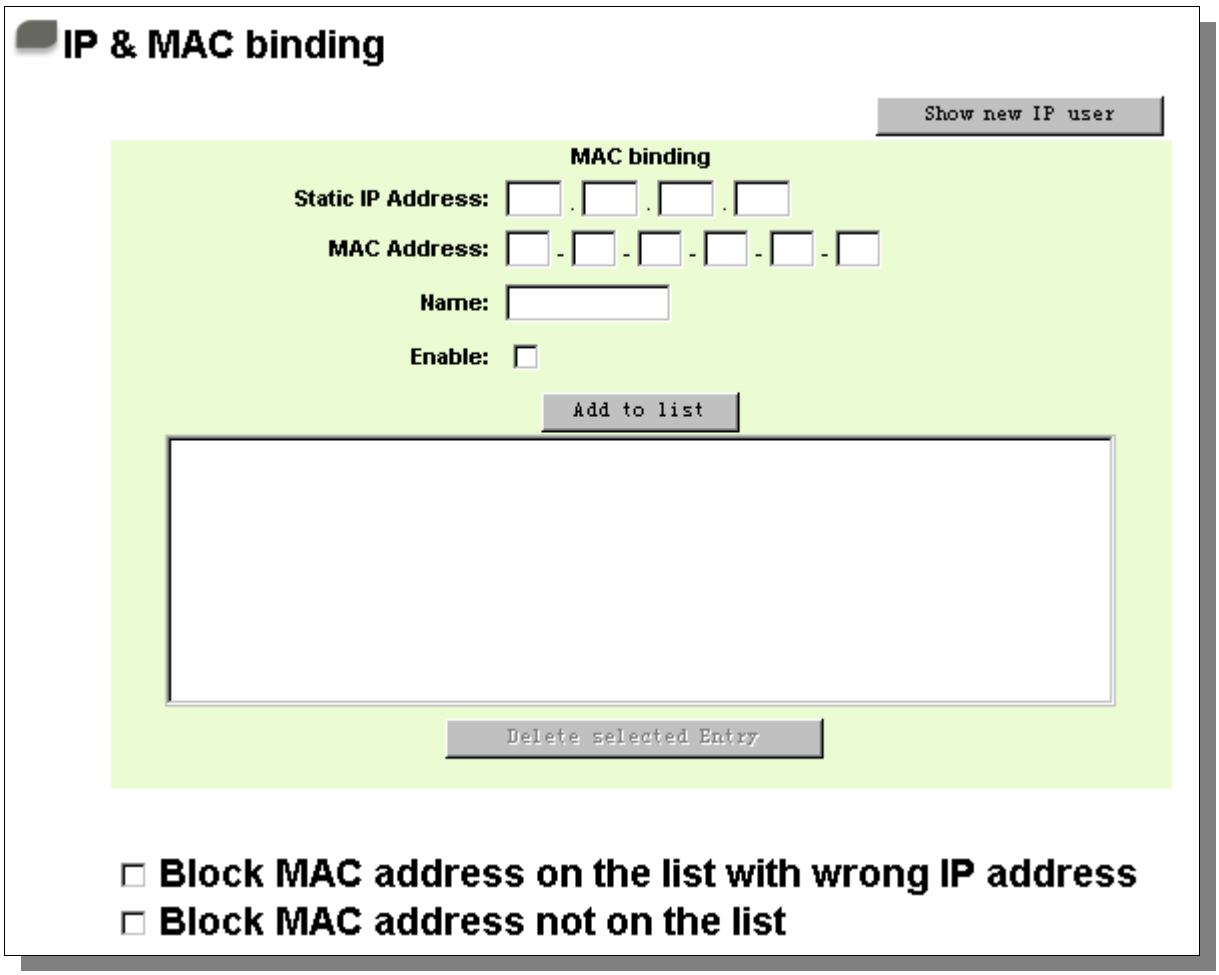
[VPN Firewall offers a class C DHCP server with default setting to on. It can provide the computer to get the IP address automatically in the LAN (Like the DHCP service in the NT Server). It benefits the computer do not need to record and setup its IP address. When the PC started, it would get the IP address automatically from the VPN Firewall, and it is easier to management.]

4.8.1 Dynamic IP



Client Lease Time:	This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Users can change it according to their needs. The time unit is minute.
Range Start:	This is an initial IP automatically leased by DHCP. It means DHCP will start the lease from this IP. The default initial IP is 192.168.1.100.
Range End:	This means DHCP will terminate the lease at this IP address. The default terminal IP address is 149. Though the default supports automatic IP acquisition for 50 computers, users can increase or reduce the number according to their needs.

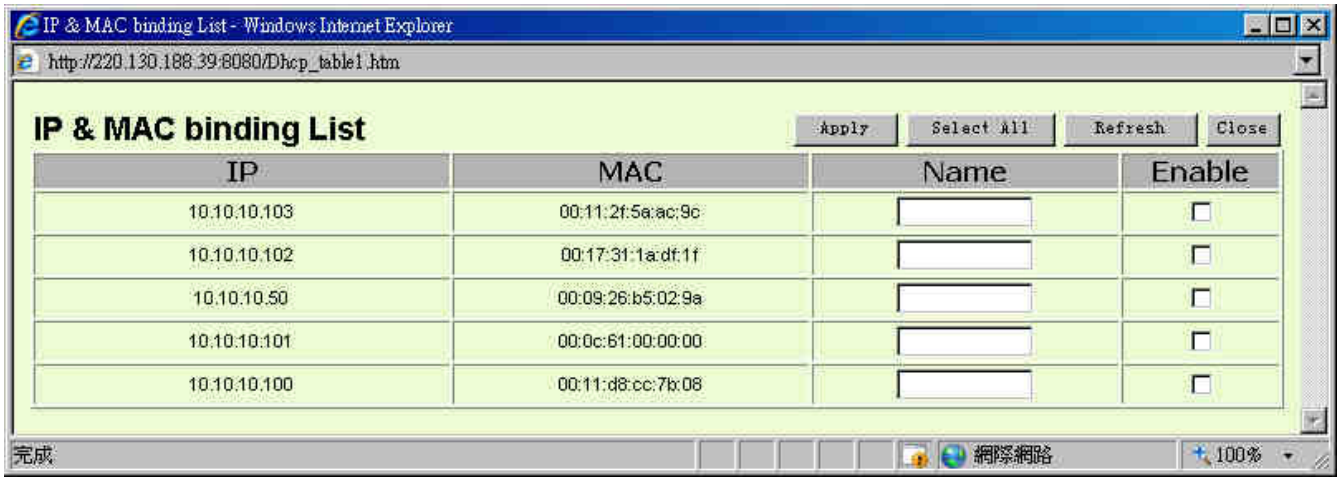
4.8.2 IP & MAC Binding



Static IP:	There are two ways to input static IP: . If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a static IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty. . If users want DHCP to assign a static IP for a PC every single time, users should input the IP address users want to assign to this computer in the boxes. The server or PC which is to be bound will then acquire a static virtual IP whenever it restarts.
MAC Address:	Input the static real MAC (the address on the network card) for the server or PC which is to be bound.
Name:	For distinguishing clients, input the name or address of the

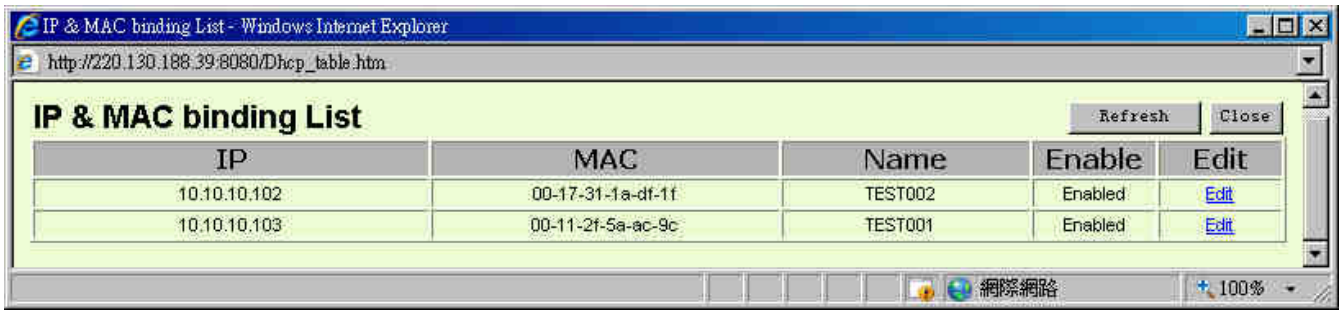
	client that is to be bound. The maximum acceptable characters are 12. Either Chinese or English can be accepted.
Enabled:	To activate this configuration.
Add To List:	To add the configuration or modification to the list.
Delete Selected Items:	To remove the selected binding from the list.
Add:	To add new binding.
Block MAC address on the list with wrong IP address:	When this option is activated, MAC addresses which are not included in the list will not be able to connect with the Internet.
Block MAC address not on the list:	When this option is checked, user-modified IP or IP which is not configured in the list will not be able to connect with the Internet.

Show New IP User



After the changes are completed, click **"Apply"** to save the network configuration modification, or click **"Cancel"** to leave without making any change.

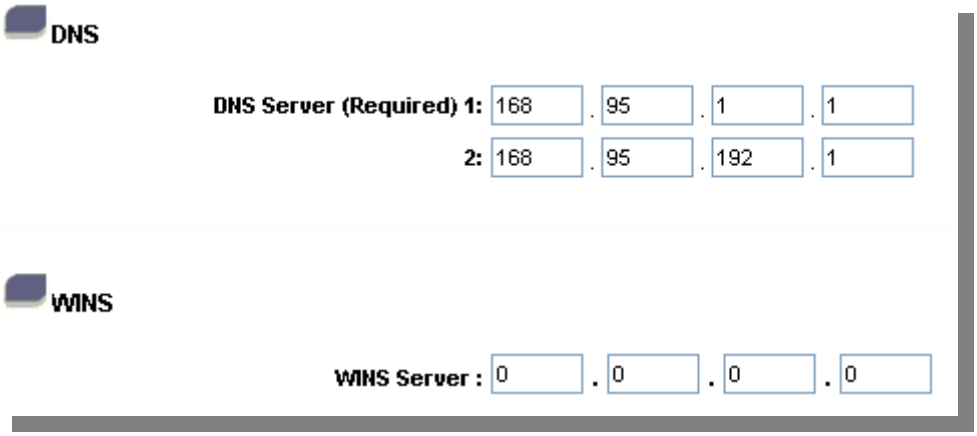
Show Tables



Click "Edit" to set binding rule

4.8.3 DNS & WINS Server

This is for checking the DNS from which an IP address has been leased to a PC port. If you have specific DNS Server, input the IP address of this server directly. As an IP address has been leased to a PC port, it also gets designated DNS Server address.



DNS Server 1 :	Input the IP address of the DNS server.
DNS Server 2 :	Input the IP address of the DNS server.

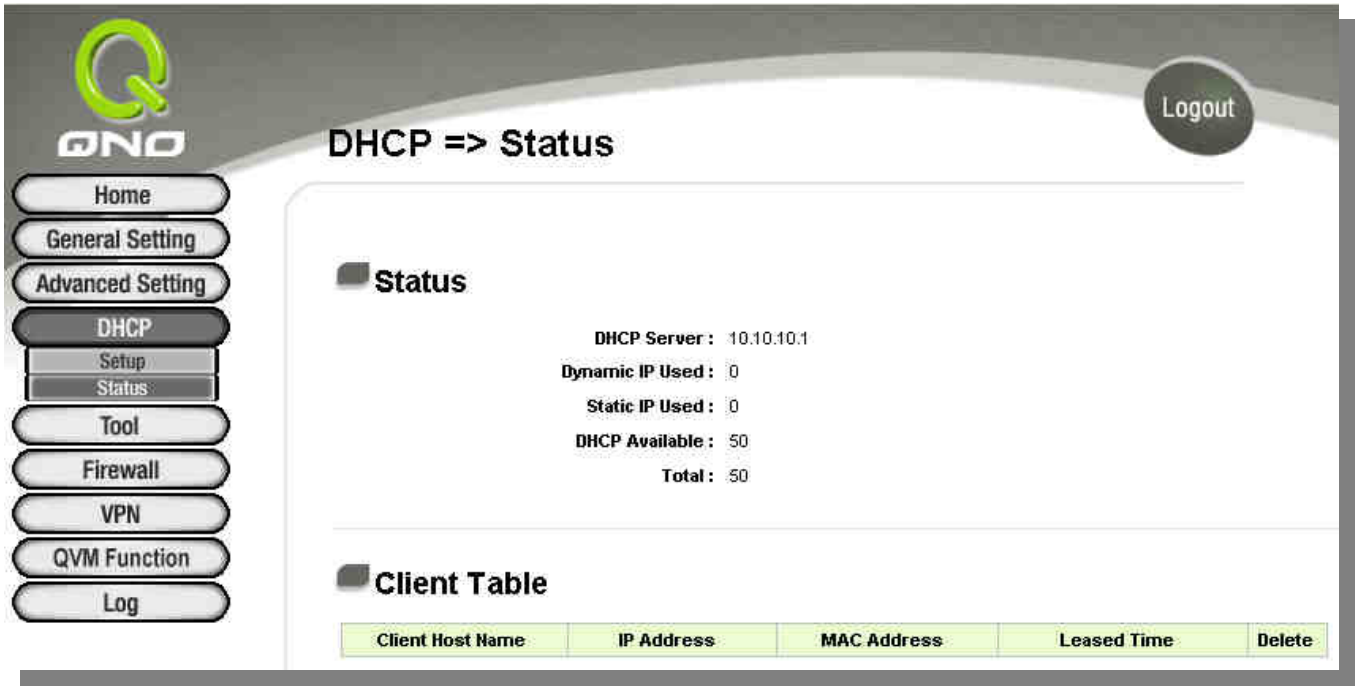
WINS Server :

If there is a WIN server in the network, users can input the IP address of that server directly.

WINS Server :	Input the IP address of WINS.
Apply :	Click **"Apply"** to save the network configuration modification.
Cancel :	Click **"Cancel"** to leave without making any changes.

4.8.4 DHCP Status

This is an indication list of the current status and setup record of the DHCP server. The indications are for the administrator's reference when a network modification is needed.



DHCP Server : This is the current DHCP IP.

Dynamic IP Used : The amount of dynamic IP leased by DHCP.

Static IP Used : The amount of static IP assigned by DHCP.

IP Available : The amount of IP still available in the DHCP server.

Total IP : The total IP which the DHCP server is configured to lease.

Host Name : The name of the current computer.

IP Address : The IP address acquired by the current computer.

MAC Address : The actual MAC network location of the current computer.

Client Lease Time : The lease time of the IP released by DHCP.

Delete : Remove a record of an IP lease.

V. Tool Configuration

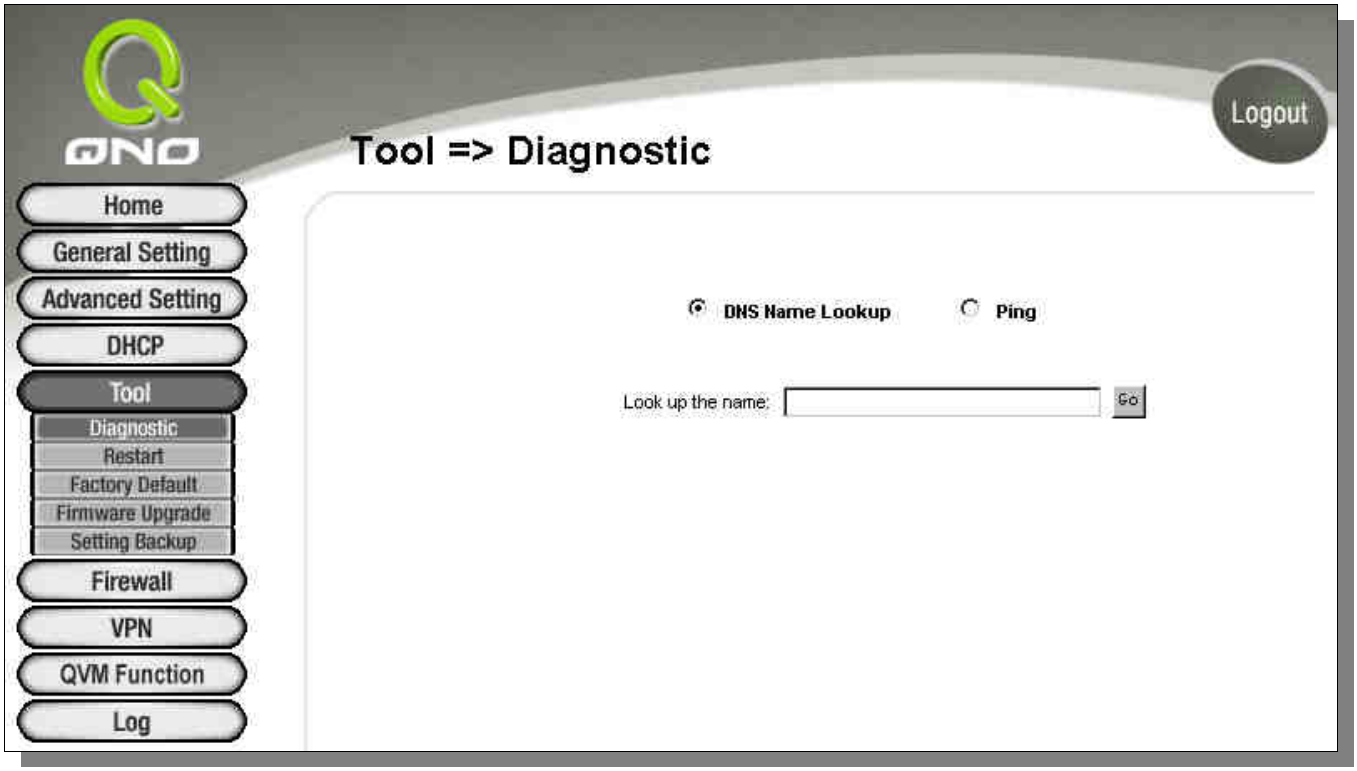
This chapter introduces the management tool for controlling the device and testing network connection.

5.1 Diagnostic

The device provides a simple online network diagnostic tool to help users troubleshoot network-related problems. This tool includes **DNS Name Lookup** (Domain Name Inquiry Test) and **Ping (Packet Delivery/Reception Test)**.

DNS Name Lookup

On this test screen, please enter the host name of the network users want to test. For example, users may enter www.abc.com and press "Go" to start the test. The result will be displayed on this page.



This item informs users of the status quo of the outbound session and allows the user to know the existence of computers online.

On this test screen, please enter the host IP that users want to test such as 192.168.5.20. Press "Go" to start the test. The result will be displayed on this screen.

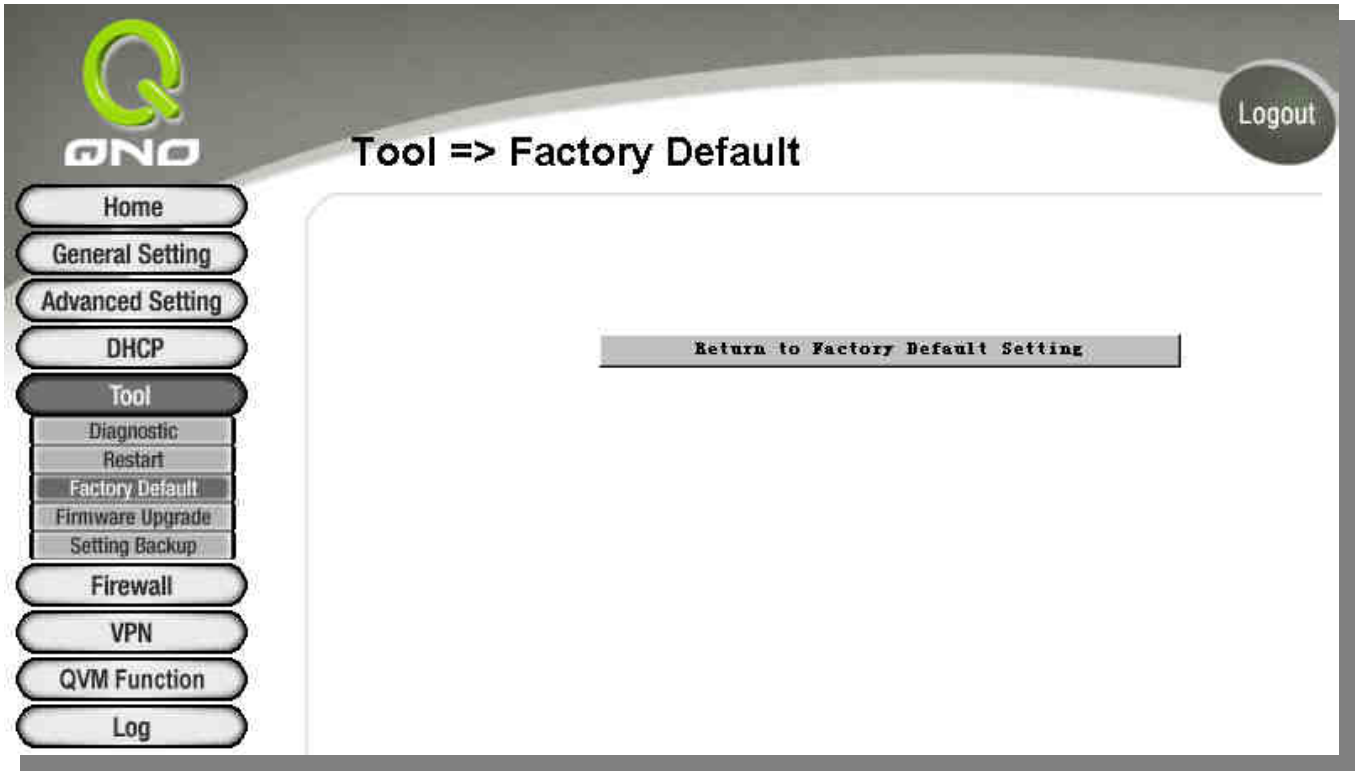
5.2 Restart

As the figure below, if clicking "Restart Router" button, the dialog block will pop out, confirming if users would like to restart the device.

5.3 Return to Factory Default Setting

Select "**Return to Factory Default Setting**" to reset all the settings and restart the device. Alternatively, users may press "**Reset**" button on the device to manually restore the default value and clear all settings including port configures, password setting and etc. **Press "Reset" and hold for more than 10 seconds.** The flicker of the yellow light indicates the default value is being restored.

Please note that this feature resets all the data on the device!



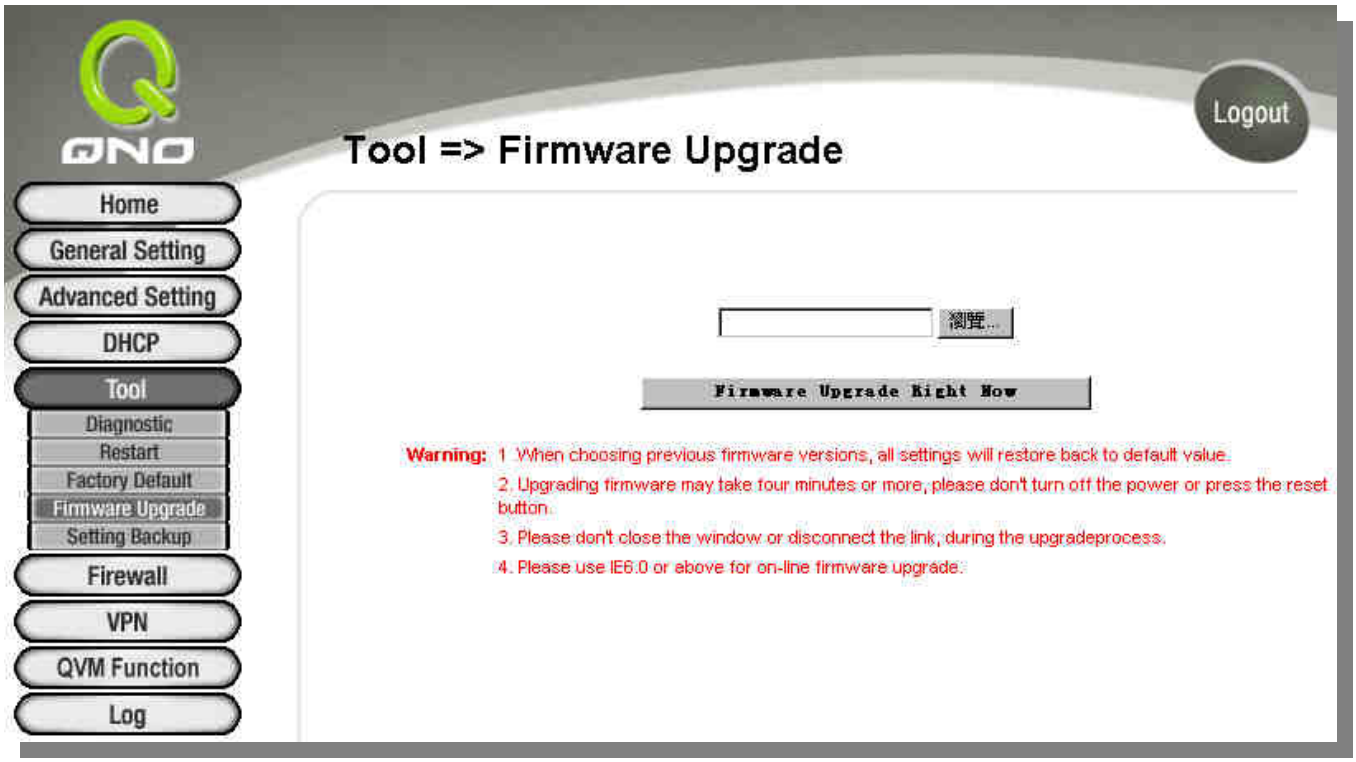
5.4 Firmware Upgrade

Users may directly upgrade the device firmware on the Firmware Upgrade page. Please confirm all information about the software version in advance. Select and browse the software file, click **"Firmware Upgrade Right Now"** to complete the upgrade of the designated file.

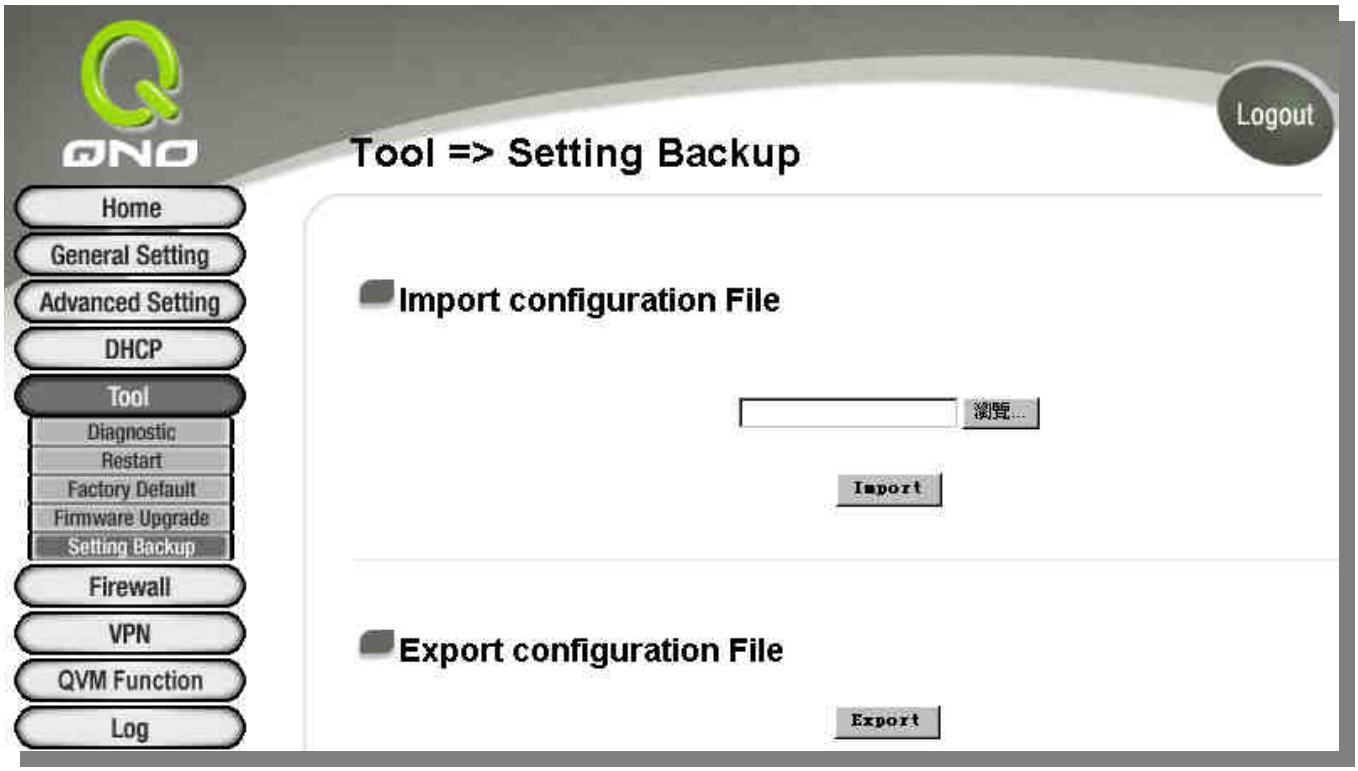
Note !

Please read the warning before firmware upgrade.

Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.



5.5 Setting Backup



Import configuration file

This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to import the file.

Export Configuration File

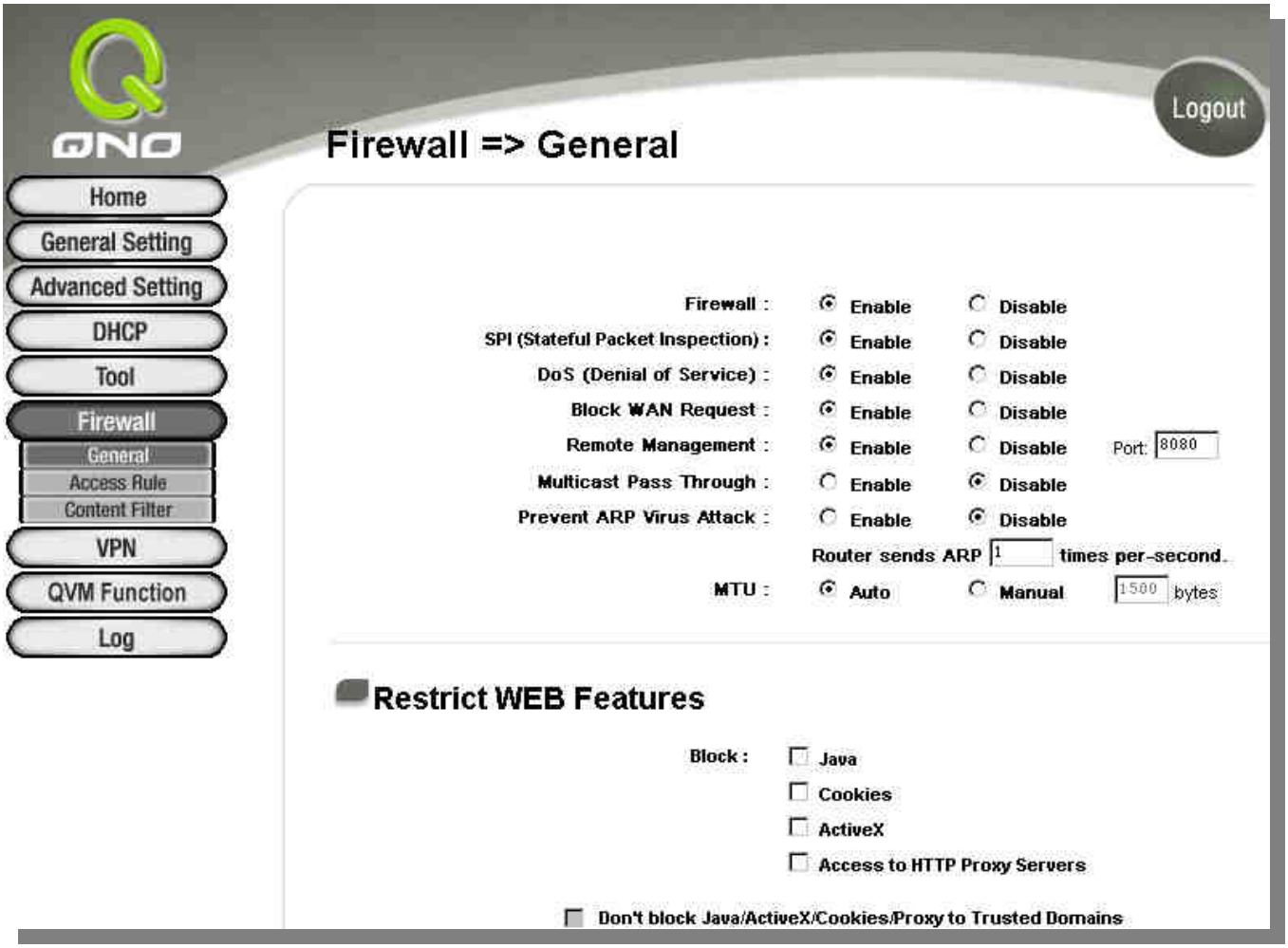
This feature allows users to backup all parameter settings. Click "**Export**" and select the location to save the "config.exp" file.

VI. Firewall Configuration

This chapter introduces the option of firewall setting as well as the setting of network access and control.

6.1 General Settings

The firewall is enabled by default. If the firewall is set as disabled, features such as SPI, DoS, and outbound packet responses will be turned off automatically. Meanwhile, the remote management feature will be activated. The network access rules and content filter will be turned off.



Firewall:

SPI (Stateful Packet Inspection):

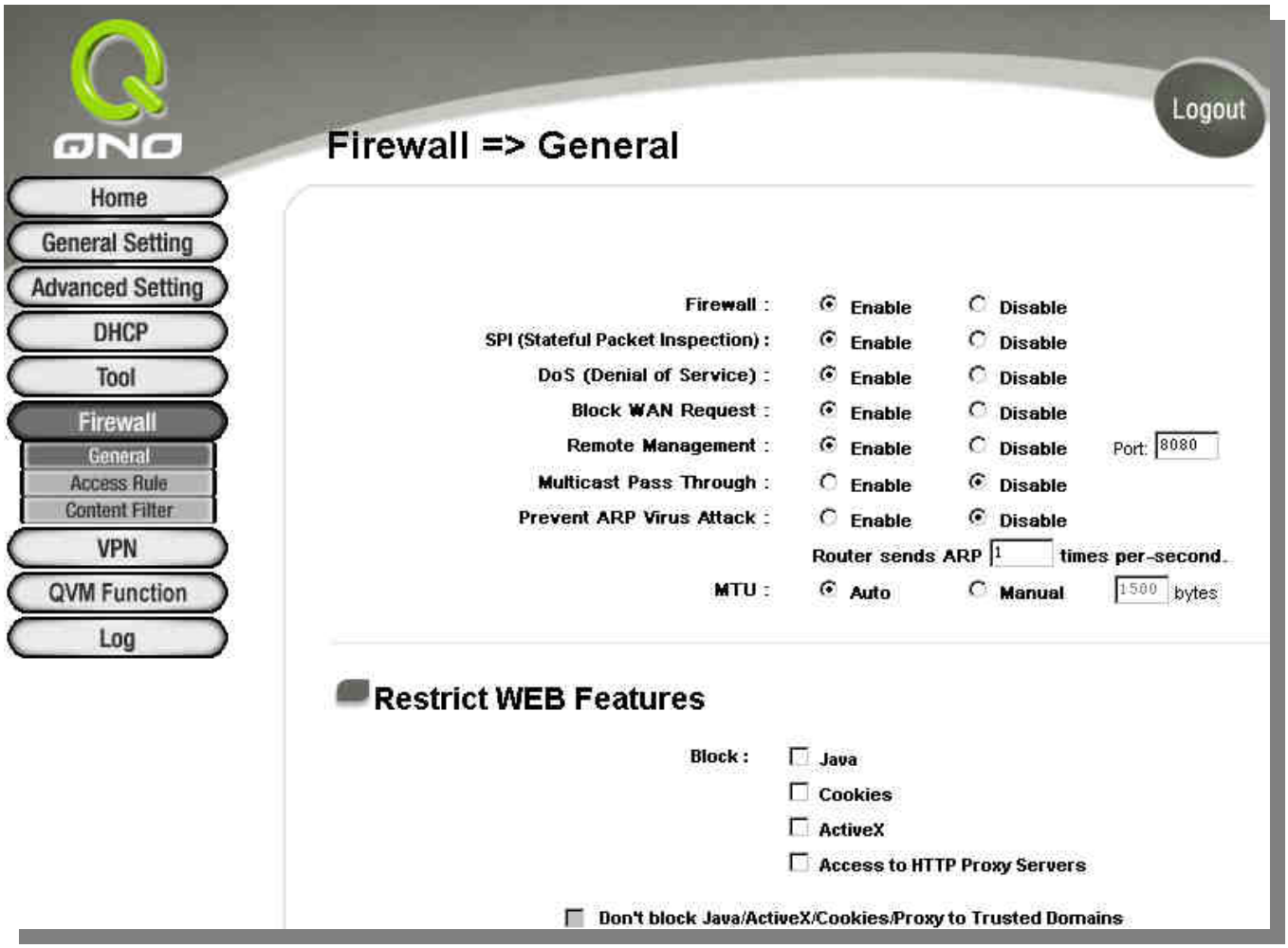
This feature allows users to turn on/off the firewall. This enables the packet automatic authentication detection technology. The Firewall operates mainly at

	the network layer. By executing the dynamic authentication for each connection, it will also perform an alarming function for application procedure. Meanwhile, the packet authentication firewall may decline the connections which use non-standard communication protocol.
DoS (Denial of Service):	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and so on.
Block WAN Request:	If set as Enabled, then it will shut down outbound ICMP and abnormal packet responses in connection. If users try to ping the WAN IP from the external, this will not work because the default value is set as activated in order to decline the outbound responses.
Remote Management:	To enter the device web- based UI by connecting to the remote Internet, this feature must be activated. In the field of remote browser IP, a valid external IP address (WAN IP) for the device should be filled in and the modifiable default control port should be adjusted (the default is set to 80, modifiable)
Multicast Pass Through:	There are many audio and visual streaming media on the network. Broadcasting may allow the client end to receive this type of packet message format. This feature is off by default.
Prevent ARP Virus Attack:	This feature is designed to prevent the intranet from being attacked by ARP spoofing, causing the connection failure of the PC. This ARP virus cheat mostly occurs in Internet cafes. When attacked, all the online computers disconnect immediately or some computers fail to go online. Activating this feature may prevent the attack by this type of virus.
Router sends ARP ____ times per second:	Prevent ARP attack by broadcast packet issued on the intranet
MTU:	MTU is an acronym for Maximum Transmission Unit. The default value is 1500.But in different network environments, different values can be applied. ADSL

PPPoE is the most common condition. (ADSL PPPoE MTU Size: 1492).But the MTU Size of many users of Servers and ADSL PPPoE are identical. Generally, the default value of Auto is good enough and further settings are not necessary.

Apply: After the changes are completed, click "**Apply**" to save the network configuration modification.

Delete : Click the "**Cancel**" button to cancel the modification. This only works before "**Apply**" is clicked.



6.2 Access Rule

Users may turn on/off the setting to permit or forbid any packet to access internet. Users may select to set different network access rules: from internal to external or from external to

internal. Users may set different packets for IP address and communication port numbers to filter Internet access rules.

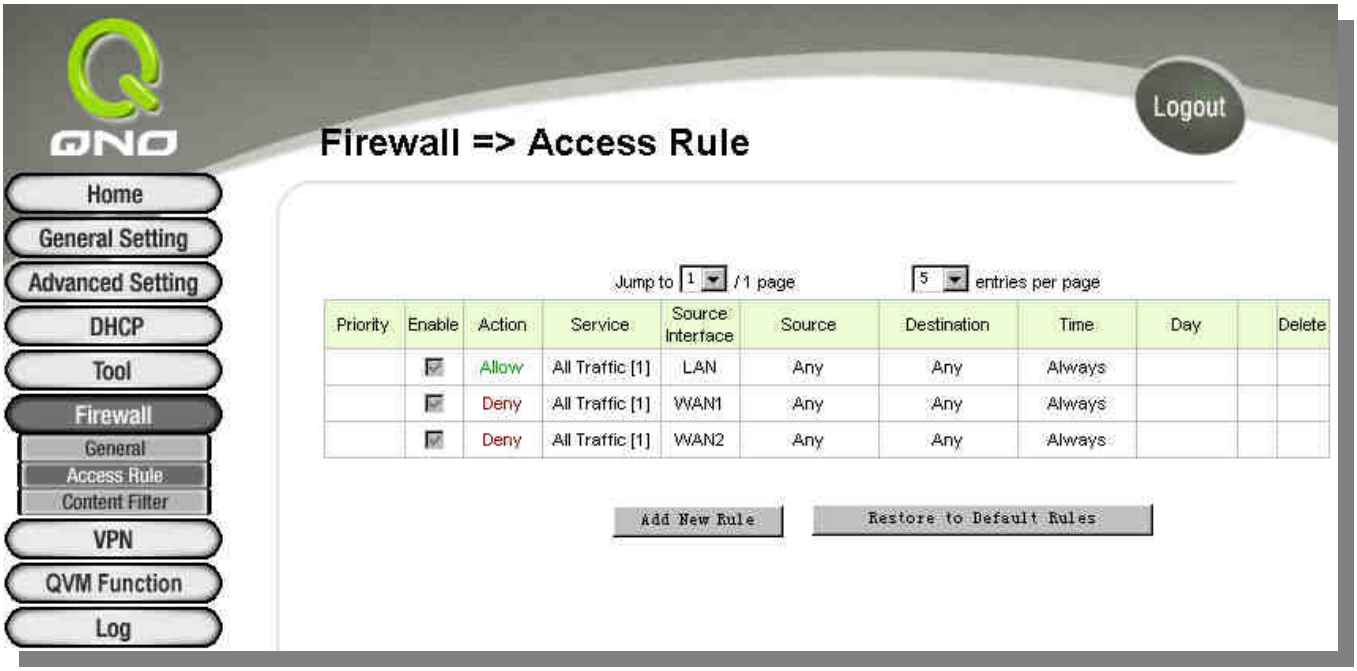
Network access rule follows IP address, destination IP address, and IP communications protocol status to manage the network packet traffic and make sure whether their access is allowed by the firewall.

The device has a user-friendly network access regulatory tool. Users may define network access rules. They can select to enable/ disable the network so as to protect all internet access. The following describes the internet access rules:

* All traffic from the LAN to the WAN is allowed - by default.
* All traffic from the WAN to the LAN is denied - by default.
* All traffic from the LAN to the DMZ is allowed - by default.
* All traffic from the DMZ to the LAN is denied - by default.
* All traffic from the WAN to the DMZ is allowed - by default.
* All traffic from the DMZ to the WAN is allowed - by default.

Users may define access rules and do more than the default rules. However, the following four extra service items are always on and are not affected by other user-defined settings.

* HTTP Service (from LAN to Device) is on by default (for management)
* DHCP Service (from LAN to Device) is set to on by default (for the automatic IP retrieval)
* DNS Service (from LAN to Device) is on by default (for DNS service analysis)
* Ping Service (from LAN to Device) is on by default (for connection and test)

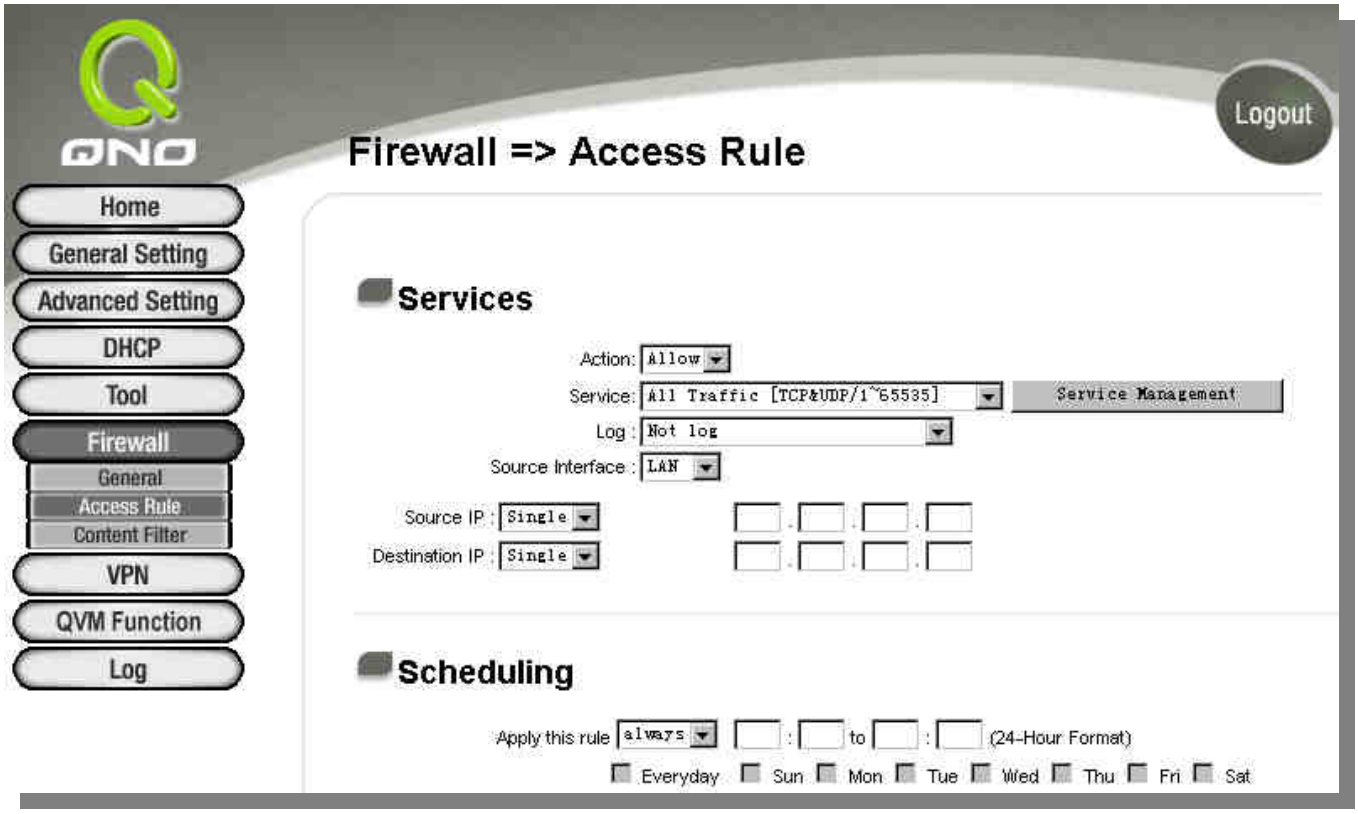

Logout
Firewall => Access Rule
Home
General Setting
Advanced Setting
DHCP
Tool
Firewall
General
Access Rule
Content Filter
VPN
QVM Function
Log
Jump to 1 /1 page
5 entries per page
Priority
Enable
Action
Service
Source Interface
Source
Destination
Time
Day
Delete
Allow
All Traffic [1]
LAN
Any
Any
Always
Deny
All Traffic [1]
WAN1
Any
Any
Always
Deny
All Traffic [1]
WAN2
Any
Any
Always
Add New Rule
Restore to Default Rules

In addition to the default rules, all the network access rules will be displayed as illustrated above. Users may follow or self- define the priority of each network access rule. Click on **Edit** to define the network access rule item and press **Delete** to remove the item.

Press **Add New Rule** to create a new network access rule. Or press **Return to Default Rules** to restore all settings to the default values and delete all the self-defined settings.

After modification, press **"Apply"** button to save the network settings or press **"Cancel"** to keep the settings unchanged.

6.2.1 Add a new Rule



Action : Allow: Permits the pass of packets compliant with this control rule

Deny: Prevents the pass of packets not compliant with this control rule

Service Port : From the drop-down menu, select the service that users grant or do not give permission.

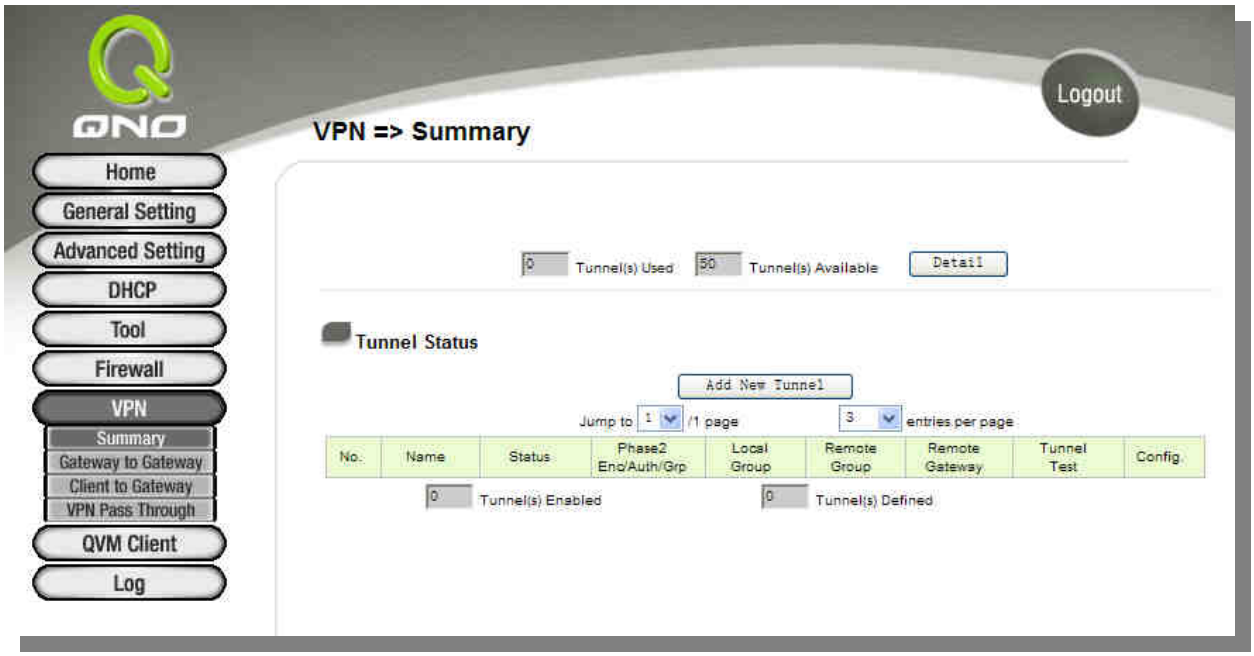
Service Port If the service that users wish to manage does not exist in the

Management :	drop-down menu, press – Service Management to add the new service. From the pop-up window, enter a service name and communications protocol and port, and then click the "Add to list" button to add the new service.
Log :	No Log： There will be no log record. Create Log when matched： Event will be recorded in the log.
Interface :	Select the source port whether users are permitted or not (for example: LAN, WAN1, WAN2 or Any). Select from the drop-down menu.
Source IP :	Select the source IP range (for example: Any, Single, Range, or preset IP group name). If Single or Range is selected, please enter a single IP address or an IP address within a session.
Dest. IP :	Select the destination IP range (such as Any, Single, Range, or preset IP group name) If Single or Range is selected; please enter a single IP address or an IP address within a session.
Scheduling :	Select **"Always"** to apply the rule on a round-the-clock basis. Select **"from",** and the operation will run according to the defined time.
Apply this rule :	Select "**Always**" to apply the rule on a round-the-clock basis. If "**From**" is selected, the activation time is introduced as below
... to ... :	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)
Day Control :	"**Everyday**" means this period of time will be under control everyday. If users only certain days of a week should be under control, users may select the desired days directly.
Apply :	Click **"Apply"** to save the configuration.
Delete :	Click the "**Cancel**" button to cancel the modification. This only works before "**Apply**" is clicked.

VII. VPN Configuration

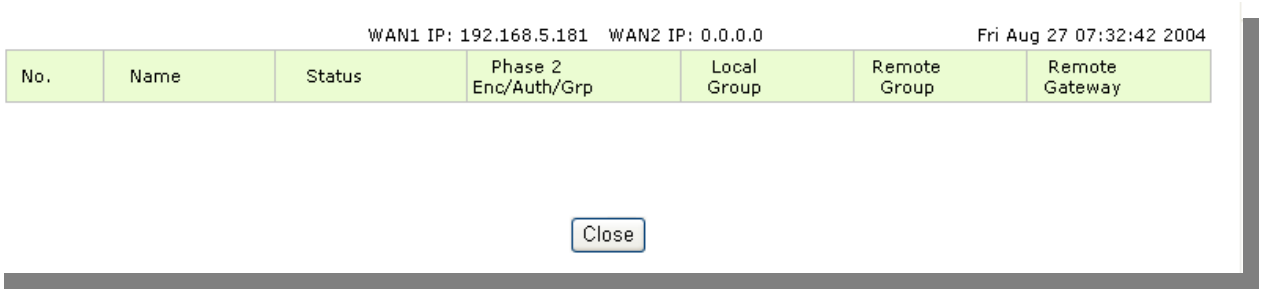
7.1 Display All VPN Summary

This VPN Summary displays the real-time data with regard to VPN status. These data include: all tunnel numbers (PPTP, IPSec + QnoKey and IPSec VPN), setting parameters and Group VPN and so forth.

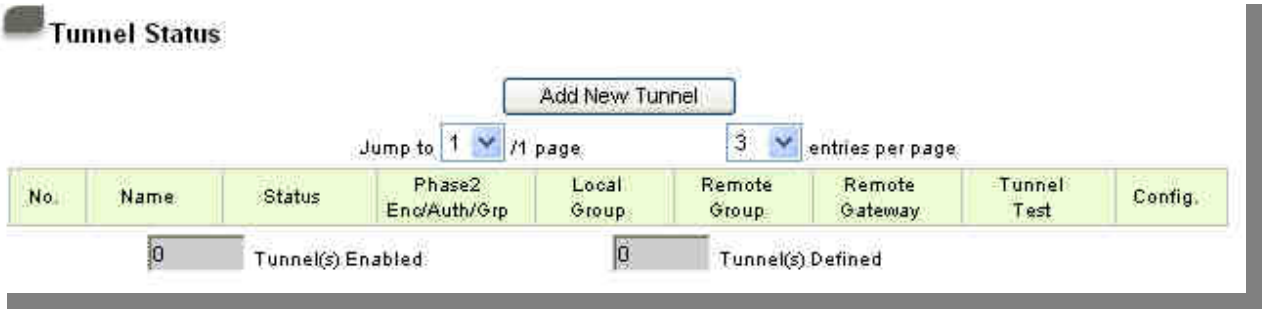


Summary：

Detail： Push this button to display the following information with regard to all current VPN configurations to facilitate VPN connection management.



Tunnel Status :



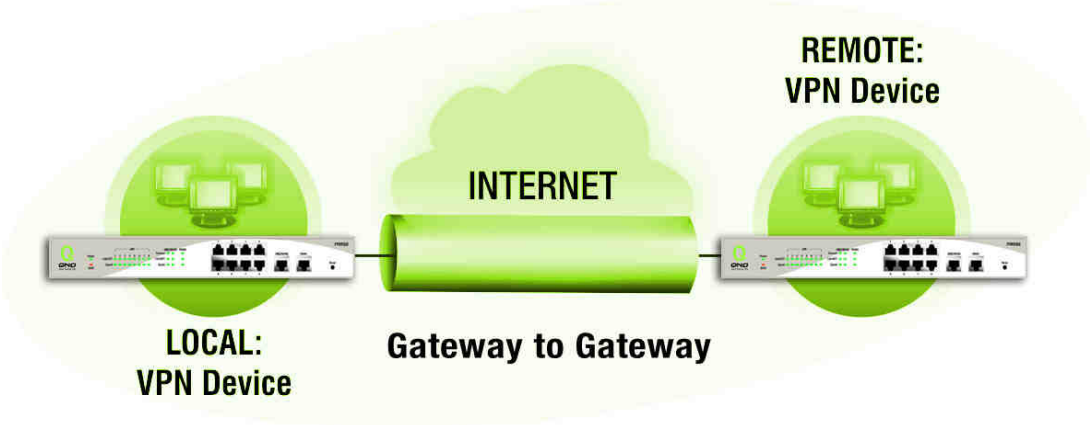
Add New Tunnel :

The device supports **Gateway to Gateway tunnel or Client to Gateway tunnel.**

The VPN tunnel connections are done by 2 VPN devices via the Internet. When a new tunnel is added, the setting page for **Gateway to Gateway** or **Client to Gateway** will be displayed.

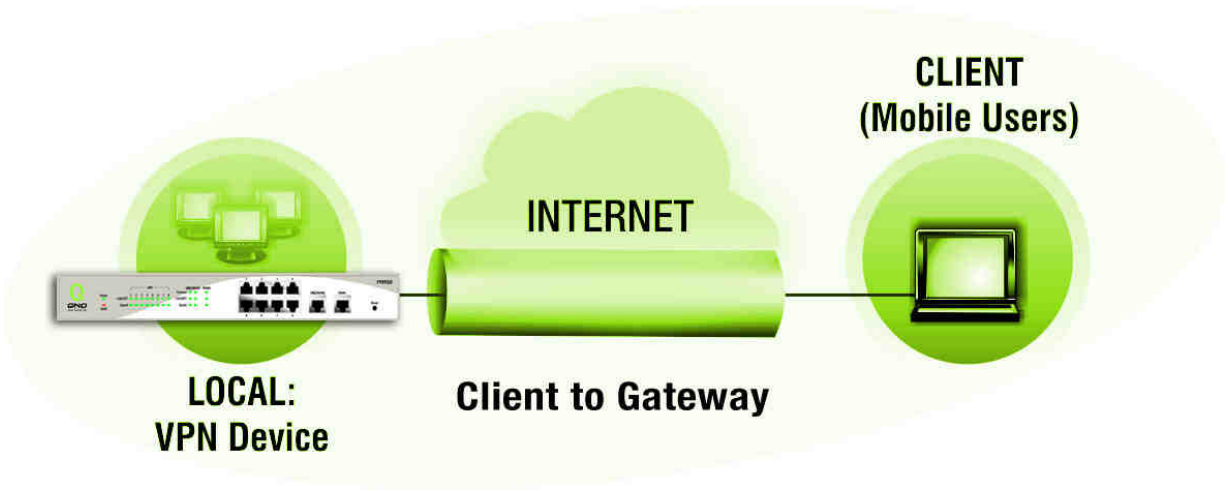
Gateway to Gateway :

Click **"Add"** to enter the setting page of **Gateway to Gateway**.



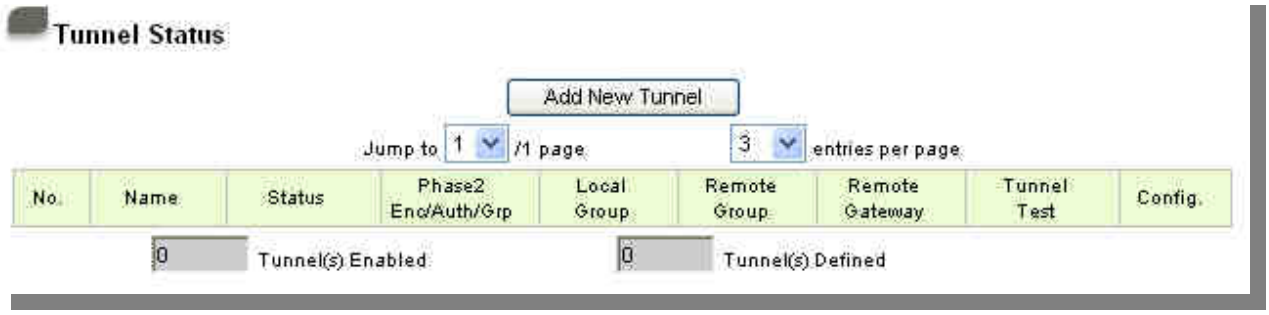
Client to Gateway :

Click **"Add"** to enter the setting page of **Client to Gateway**.



VPN Tunnel Status :

The following describes VPN Tunnel Status, the current status of VPN tunnel in detail :



Previous Page/Next Page, Jump to __/__ Page, __ Entries Per Page :	Click Previous page or Next page to view the desired VPN tunnel page. Or users can select the page number directly to view all VPN tunnel statuses, such as 3, 5, 10, 20 or All.
Tunnel No :	To set the embedded VPN feature, please select the tunnel number. It supports up to 300 IPSec VPN tunnel Setting

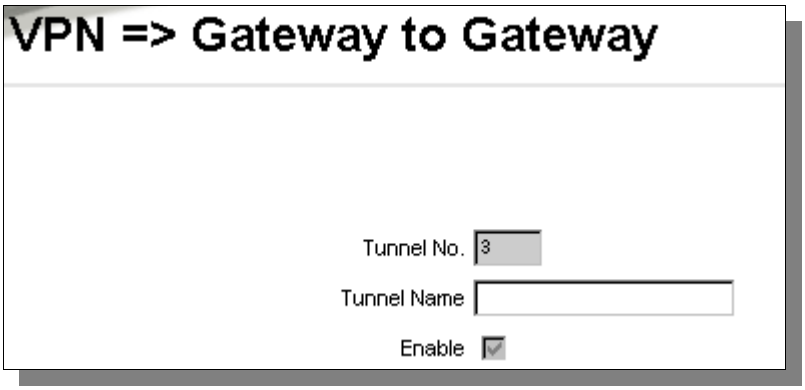
Status :	(gateway to gateway as well as client to gateway). Successful connection is indicated as-(Connected). Failing hostname resolution is indicated as - (Hostname Resolution Failed). Resolving hostname is indicated as -(Resolving Hostname) Waiting to be connected is indicated as - (Waiting for Connection). If users select Manual setting for IPSec setup, the status message will display as "Manual" and there is no Tunnel test function available for this manual setting.
Account ID :	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion should users have more than one tunnel settings. **Note:** If this tunnel is to be connected to other VPN device (not QVM750), some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.
Phase2 Encrypt/Auth/Group :	Displays settings such as encryption (DES/3DES), authentication (MD5/SHA1) and Group (1/2/5). If users select Manual setting for IPSec, Phase 2 DH group will not display.
Local Group :	Displays the setting for VPN connection secure group of the local end.
Remote Group :	Displays the setting for remote VPN connection secure group.
Remote Gateway :	Set the IP address to connect the remote VPN device. Please set the VPN device with a valid IP address or domain name.
Control :	Click **"Connect"** to verify the tunnel status. The test result will be updated. To disconnect, click **"Disconnect"** to stop the VPN connection.
Config. :	Setting items include Edit and Delete icon.  Click on **Edit** to enter the setting items and users may change the settings. Click on the trash bin icon  and all the tunnel settings will be deleted.

7.2 Gateway to Gateway VPN

In this session, we are going to introduce Gateway to Gateway VPN setting.

7.2.1 Tunnel Setup

The following instructions will guide users to set a VPN tunnel between two devices.



Tunnel No.: To set the embedded VPN feature, please select the Tunnel number. This device supports up to 5 VPN tunnel settings.

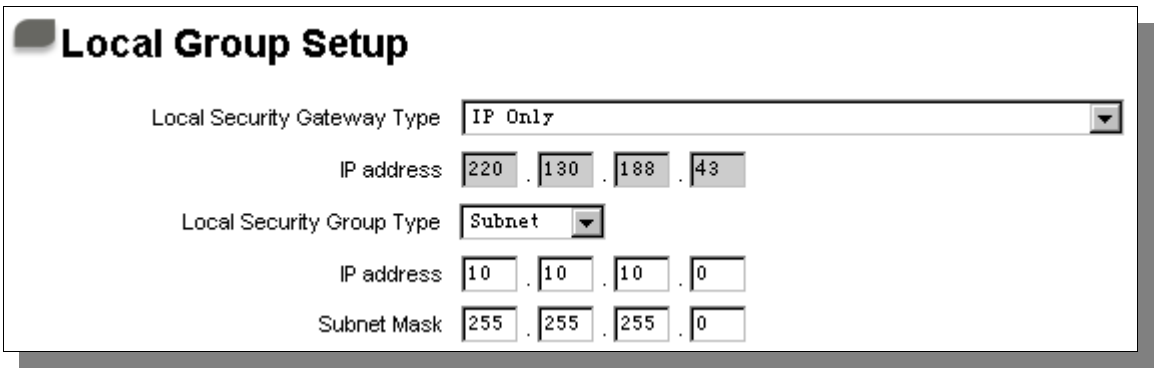
Tunnel Name: Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion should users have more than one tunnel settings.

Note: If this tunnel is to be connected to any other VPN device (not VPN firewall), some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.

Enabled: Click to "**Enable**" the VPN tunnel. This option is set to enable by default. Afterwards, users may select to enable this tunnel feature.

Local Group Setup:

This Local Security Gateway Type must be identical with that of the remote type (Remote Security Gateway Type).



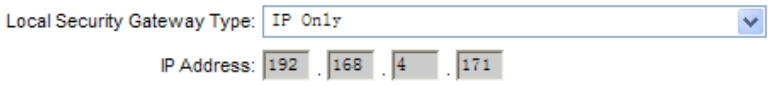
Local Security This local gateway authentication type comes with five

Gateway Type

operation modes, which are:
IP only - Authentication by the use of IP only
IP + Domain Name (FQDN) Authentication, -IP + Domain name
IP + E-mail Addr. (USER FQDN) Authentication,-IP + Email address
Dynamic IP + Domain Name (FQDN) Authentication, -Dynamic IP address + Domain name
Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name

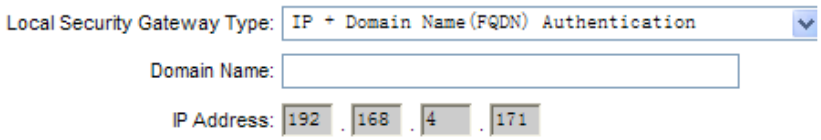
(1) IP only:

If users decide to use **IP only**, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.



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

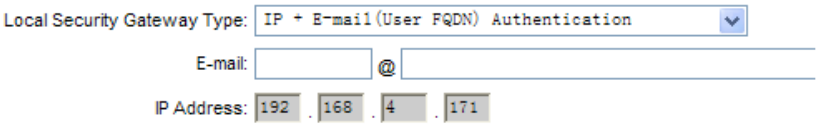
If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.



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

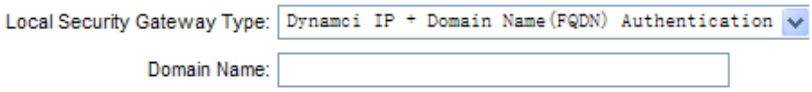
If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users

don't need to do further settings.



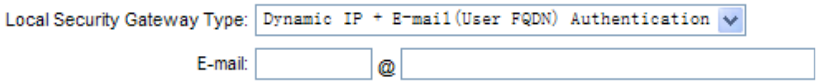
(4) Dynamic IP + Domain Name(FQDN) Authentication:

If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.



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

If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; If users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.

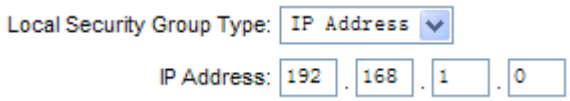


Local Security Group Type	This option allows users to set the local VPN connection access type. The following offers a few items for local

settings. Please select and set appropriate parameters:

1. **IP address**

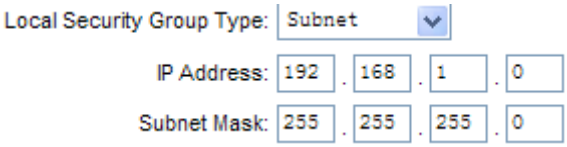
   This option allows the only IP address which is entered to build the VPN tunnel.



Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

2. Subnet

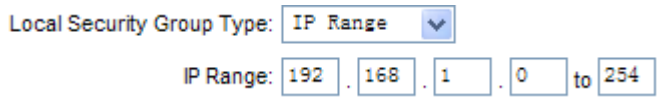
This option allows local computers in this subnet can be connected to the VPN tunnel.



Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

3. IP Range

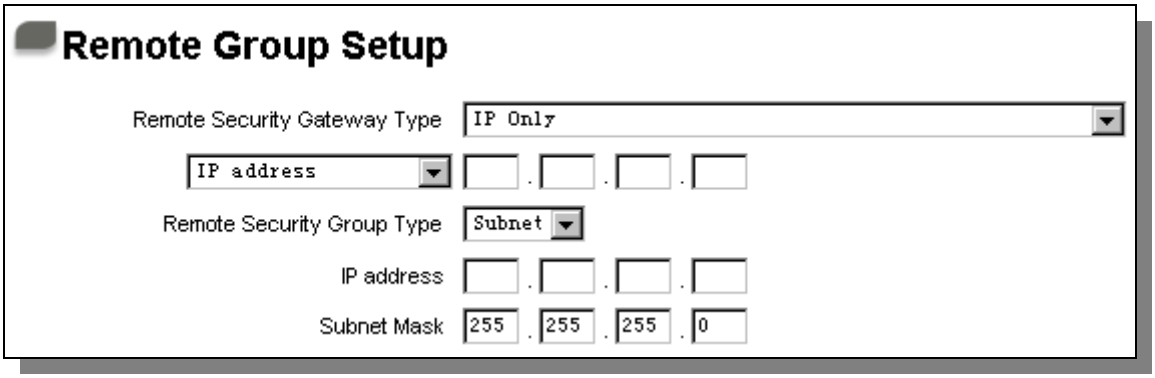
This option allows connection only when IP address range which is entered after the VPN tunnel is connected.



Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 ~254 can establish connection.

Remote Group Setup

This remote gateway authentication type (Remote Security Gateway Type) must be identical to the remotely-connected local security gateway authentication type (Local Security Gateway.

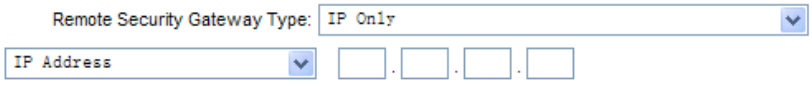


Remote Security Gateway Type:

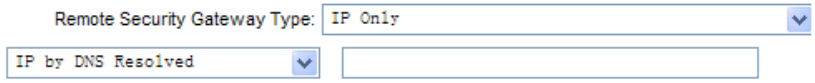
This remote gateway authentication type comes with five operation modes, which are:
IP only-Authentication by use of IP only
IP + Domain Name(FQDN) Authentication, -IP + Domain name
IP + E-mail Addr. (USER FQDN) Authentication, -IP + Email address
Dynamic IP + Domain Name (FQDN) Authentication, -Dynamic IP address + Domain name
Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name

(1) IP only:

If users select the IP Only type, entering this IP allows users to gain access to this tunnel.

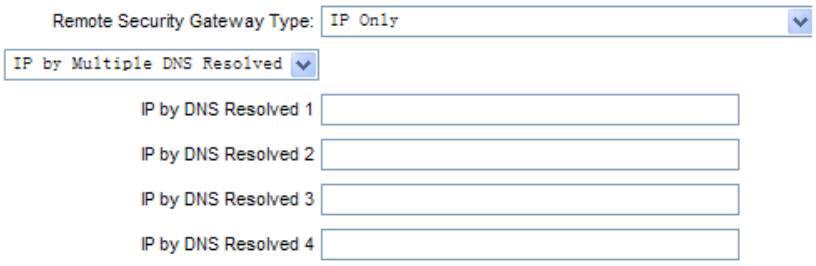


If the IP address of the remote client is unknown, choose IP by DNS Resolved, allowing DNS to transcode IP address. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.



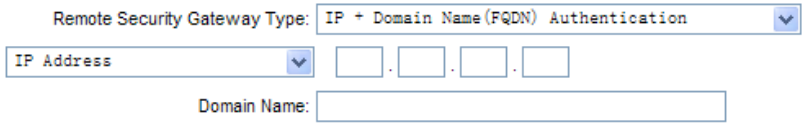
Or users can choose IP by Multiple DNS Resolved, and IP

address can be transcoded through DNS. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

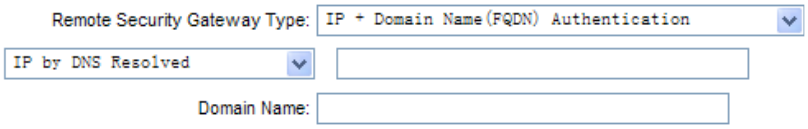


(2) IP + Domain Name(FQDN) Authentication:

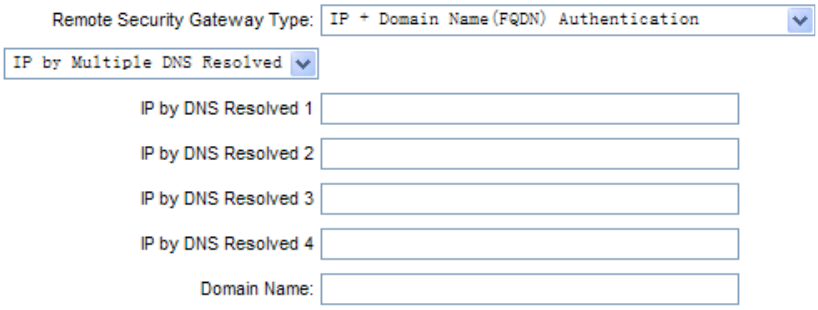
If users select IP + domain name, please enter IP address and the domain name to be verified. FQDN refers to the combination of host name and domain name. Users may enter any name that corresponds to the domain name of FQDN. This IP address and domain name must be identical to those of the remote VPN security gateway setting type to establish successful connection.



If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to transcode the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

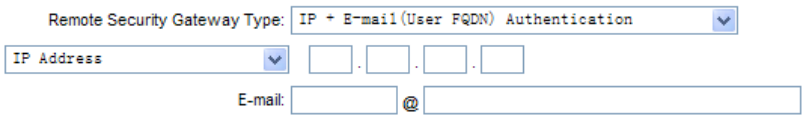


Or users can choose IP by Multiple DNS Resolved, and IP address can be transcoded through DNS. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

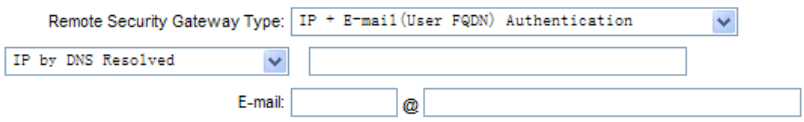


(3) IP + E-mail Addr. (USER FQDN) Authentication:

If users select IP address and E-mail type, entering the IP address and the E-mail allows users to gain access to this tunnel.

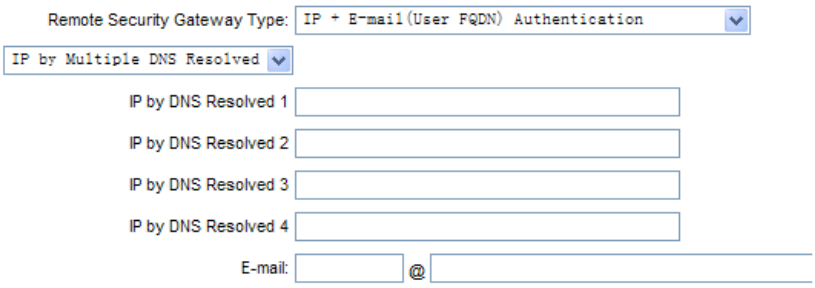


If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to transcode the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.



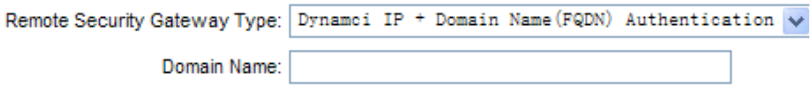
Or users can choose IP by Multiple DNS Resolved, and IP

address can be transcoded through DNS. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.



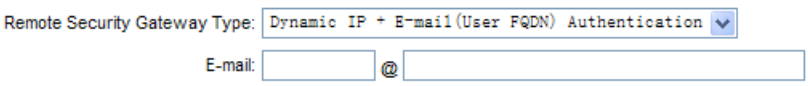
(4) Dynamic IP + Domain Name(FQDN) Authentication:

If users use dynamic IP address to connect with the device, users may select the combination of the dynamic IP address, host name and domain name.



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

If users use dynamic IP address to connect with the device, users may select this type to link to VPN. When the remote VPN gateway requires connection to facilitate VPN connection, the device will start authentication and respond to the VPN tunnel connection; Please enter the E-Mail to the empty space.

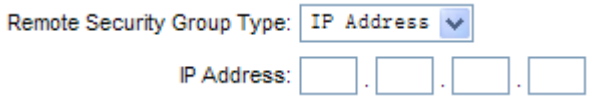


Remote Security Group Type:

This option allows users to set the remote VPN connection access type. The following offers a few items for remote settings. Please select and set appropriate parameters:

(1) **IP address**

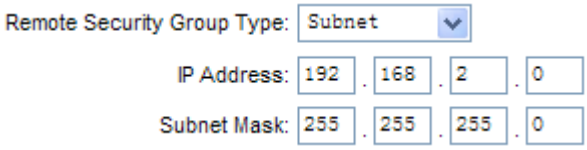
This option allows the only IP address which is entered to build the VPN tunnel.



Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.2.1 can establish connection.

(2) **Subnet**

This option allows local computers in this subnet can be connected to the VPN tunnel.



Reference: When this VPN tunnel is connected, only computers with the session of 192.168.2.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

7.2.2 IPSec Setup

If there is any encryption mechanism, the encryption mechanism of these two VPN tunnels must be identical in order to create connection. And the transmission data must be encrypted with IPSec key, which is known as the encryption "key". The device provides the following two encrypted Key Management. They are Manual and IKE automatic encryption mode- IKE with Preshared Key (automatic). By using the drop down menu, select the desired encryption mode as illustrated below.

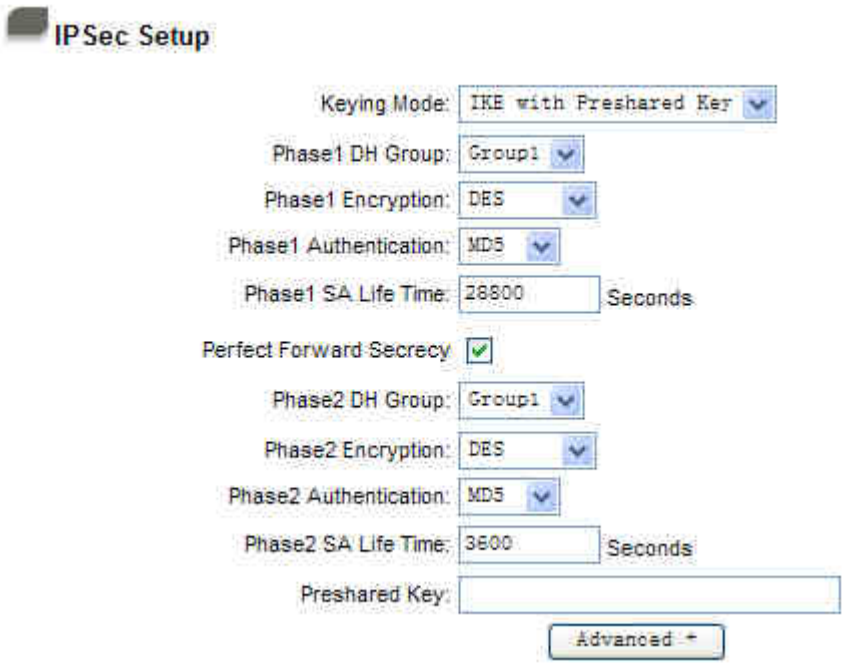
Key Mode：

When users set this VPN tunnel to use any encryption and authentication mode, users must set the parameter of this exchange password with that of the remote. Setting methods include Auto (IKE) or Manual. To do the settings, select any one from the two options.

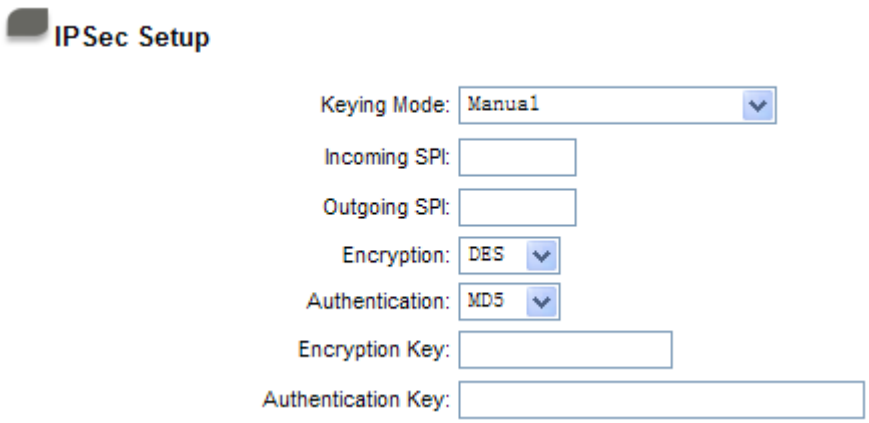
IKE with Preshared Key :

Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the key will not be able to get the Phase 2 key in such a short period of time.

- **Perfect Forward Secrecy:** When users tick the PFS option, don't forget to activate the PFS function of the VPN device and the VPN Client as well.
- **Phase 1/ Phase 2 DH Group:** This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
- **Phase 1/ Phase 2 Encryption:** This option allows users to set this VPN tunnel to use any encryption mode. Note that this parameter must be identical to that of the remote encryption parameter: DES: 64-bit encryption mode, 3DES: 128-bit encryption mode, AES: the standard of using security code to encrypt information. It supports 128-bit, 192-bit and 256-bit encryption keys.
- **Phase 1/Phase 2 Authentication:** This authentication option allows users to set this VPN tunnel to use any authentication mode. Note that this parameter must be identical to that of the remote authentication mode: "MD5" or "SHA1".
- **Phase 1 SA Life Time:** The life time for this exchange code is set to 28800 seconds (or 8hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Phase2 SA Life Time:** The life time for this exchange code is set to 3600 seconds (or 1hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Preshared Key :** For the Auto (IKE) option, enter a password of any digit or characters in the text of "Pre-shared Key" (the example here is set as test), and the system will automatically transcode what users entered as exchange password and authentication mechanism during the VPN tunnel connection. This exchange password can be made up of up to 30 characters.



Manual Mode



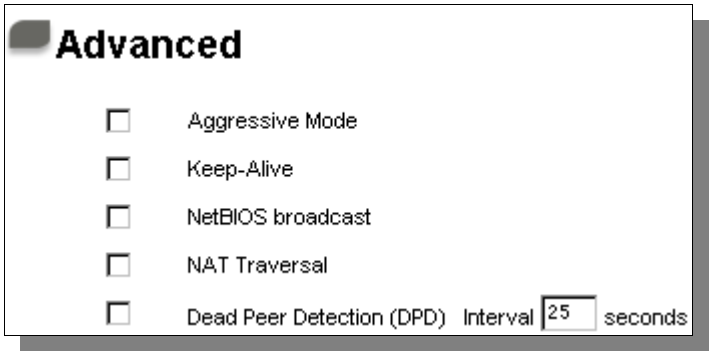
If the Manual mode is selected, users need to set encryption key manually without negotiation.

- It is divided into two types: "Encryption KEY" and "Authentication KEY". Users may enter an exchange password made up of either digits or characters. The systems will automatically transcode what users entered into the exchange password and authentication mechanism during the VPN tunnel connection. This exchange password can be made up of digits and characters up to 23.
- Moreover, the exchange strings for "Incoming SPI" and "Outgoing SPI" must be

identical to those of the connected VPN device. For the Incoming SPI parameters, users must set it the same with the Outgoing SPI string of the remote VPN device. And the Outgoing SPI string must be the same with the coming SPI string of the remote VPN device.

7.2.3 VPN Advanced

IKE Preshared Key Only



Aggressive Mode :	This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
Compress :	If this option is selected, in the connected VPN tunnel, the device supports IP Payload Compression Protocol.
Keep-Alive :	If this option is selected, VPN tunnel will keep this VPN connection. This is mostly used to connect the remote node of the branch office and headquarter or used for the remote dynamic IP address.
NetBIOS Broadcast :	If this option is selected, the connected VPN tunnel allows the passage of NetBIOS broadcast packet. This facilitates the easy connection with other Microsoft network; however, the traffic using this VPN tunnel will increase.
NAT Traversal :	It will let VPN related packs transcend the front NAT rules without any limits.
Dead Peer Detection(DPD):	If this option is selected, the connected VPN tunnel will regularly transmit HELLO/ACK message packet to detect whether there is connection between the two ends of the VPN tunnel. If one end is

	disconnected, the device will disconnect the tunnel automatically and then create new connection. Users can define the transmission time for each DPD message packet, and the default value is 10 seconds.

7.3 Client to Gateway & Group VPN

The following describes how an administrator builds a VPN tunnel between devices.

Users can set this VPN tunnel to be used by one client or by a group of clients (Group VPN) at the client end. If it is used by a group of clients, the individual setting for remote clients can be reduced. Only one tunnel will be set and used by a group of clients, which allows easy setting.

The following introduces Group Mode VPN setting.

Group No. : Two Group VPN settings at most.

Group Name : Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion.

Note: If this tunnel is to be connected to other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.

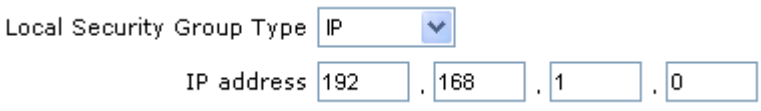
Interface : From the pull-down list, users can select the Interface for this VPN tunnel.

Enabled : Click to **Enabled** the VPN tunnel. This option is set to Enabled by default. After the set up, users may select to activate this tunnel feature.

Local user group configuration: This option allows users to set the local VPN user group type. The following are a few items for local settings. Please select and set appropriate parameters:

(1) IP address

This option allows the only IP address which is entered to build the VPN tunnel.

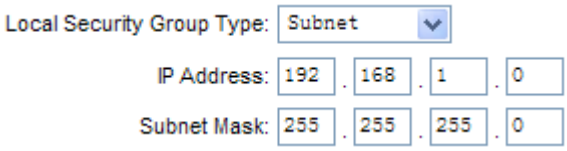


Reference: When this VPN channel is connected, computers

with the IP address of 192.168.1.0 can establish connection.

(2) Subnet

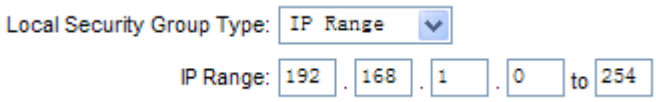
This option allows remote computers in this IP session can be connected when the VPN tunnel is connected.



Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

(3) IP Address Range

This option allows connection only when IP address range which is entered after the VPN tunnel is connected.



Reference: When this VPN channel is connected, computers with the IP address range between 192.168.2.1 and 192.168.1.254 can establish connection.

Remote Client configuration:

This setting offers three operation modes, which are:

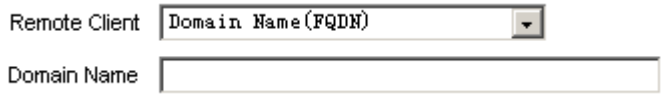
Domain Name (FQDN), - Domain Name

E-mail Address (USER FQDN), - Email Address

Microsoft XP/2000 VPN Client, - Microsoft XP/2000 VPN Client end

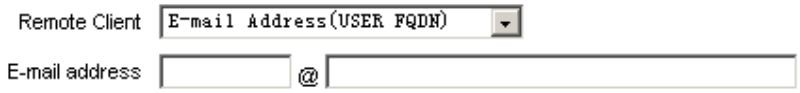
(1) Domain Name(FQDN), - Domain Name

If users select Domain Name type, please enter the domain name to be authenticated. FQDN refers to the combination of host name and domain name that are available on the Internet (i.e. vpn.Server.com).The domain name must be identical to the status setting of the client end to establish successful connection.



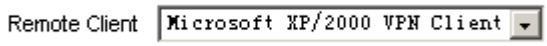
(2) E-mail Addr. (USER FQDN): E-mail address

If users select this option, only filling in the E-mail address allows access to this tunnel.



(3) Microsoft XP/2000 VPN Client, - Microsoft XP/2000 VPN Client end

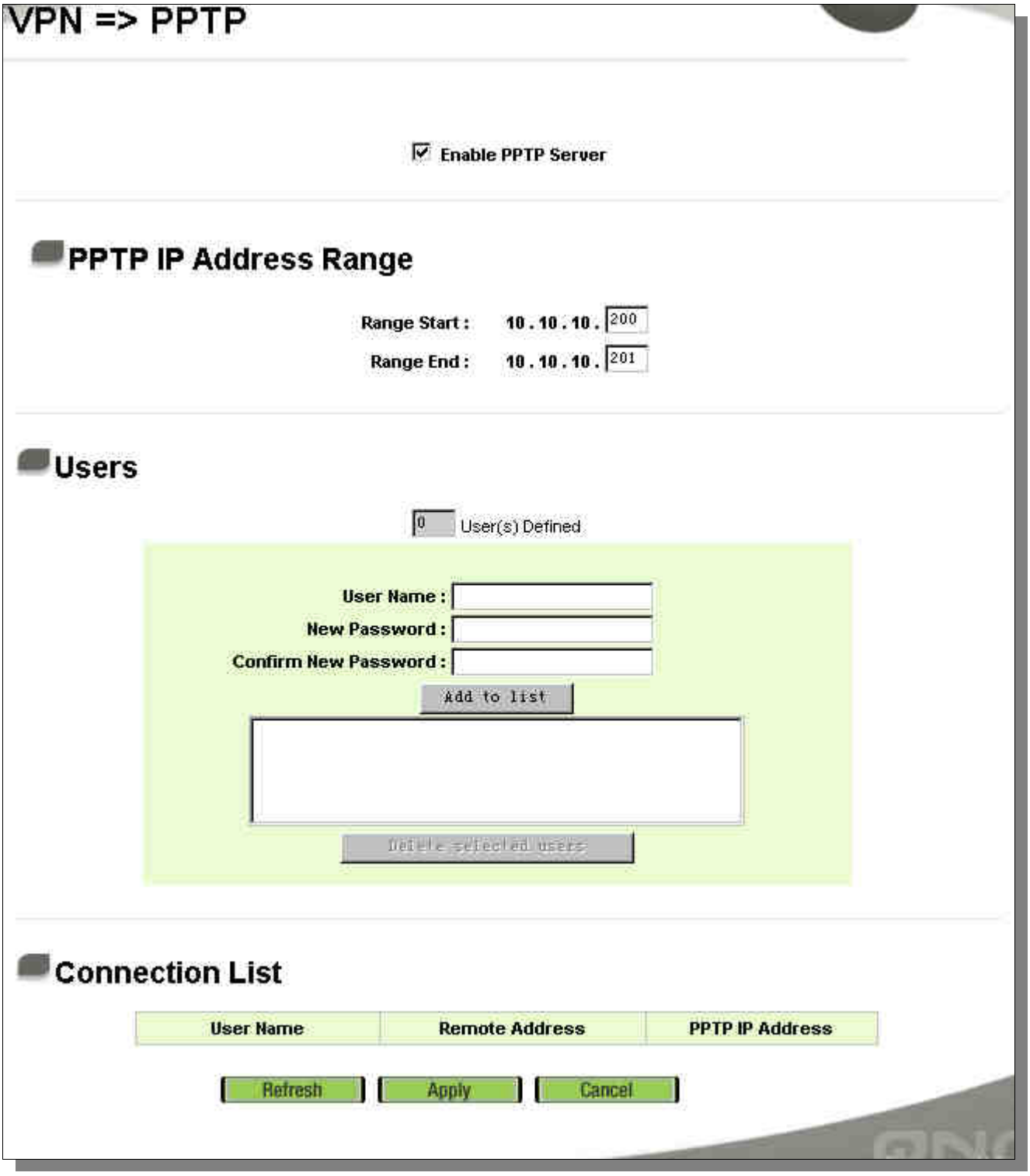
If users select XP/2000 VPN Client end status, users don't need to do extra settings.



As far the details of setting please refer to 7.2 IPSec Setup.

7.4 PPTP Setting

It supports the PPTP of Window XP/ 2000 to create point-to-point tunnel protocol for single- device users to create VPN connection.



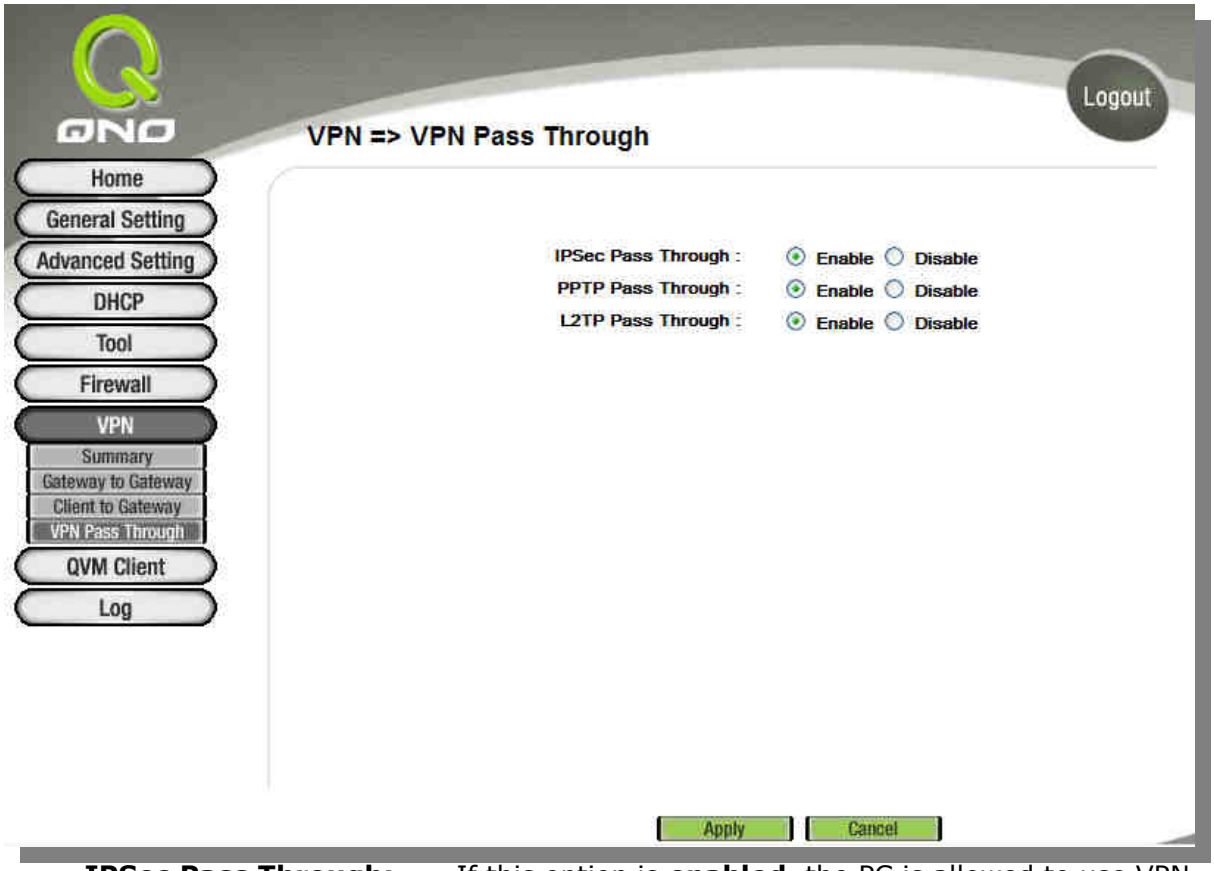
Enable PPTP Service: When this option is selected, the point-to-point tunnel protocol PPTP server can be enabled.

PPTP IP Address Please enter PPTP IP address range so as to provide the remote users with an entrance IP into the local network.

Range:	Enter Range Start: Enter the value into the last field. Enter Range End: Enter the value into the last field.
User Name:	Please enter the name of the remote user.
Password: **Confirm Password:**	Enter the password and confirm again by entering the new password.
Add to List:	Add a new account and password.
Delete Selected Item:	Delete Selected Item.
Client Table:	Displays relevant information with regard to the use of PPTP Server tunnel
User Name:	Remote user name after connection is established.
Remote Client IP:	Remote IP address after connection is established.
PPTP IP Address :	The local PPTP server IP address after connection is established.

7.5 VPN Pass Through

VPN Pass Through setting allows or rejects other VPN devices of Local network or VPN PC clients and remote VPN devices to set VPN tunnel.



IPSec Pass Through: If this option is **enabled**, the PC is allowed to use VPN-IPSec packet to pass in order to connect to external VPN device.

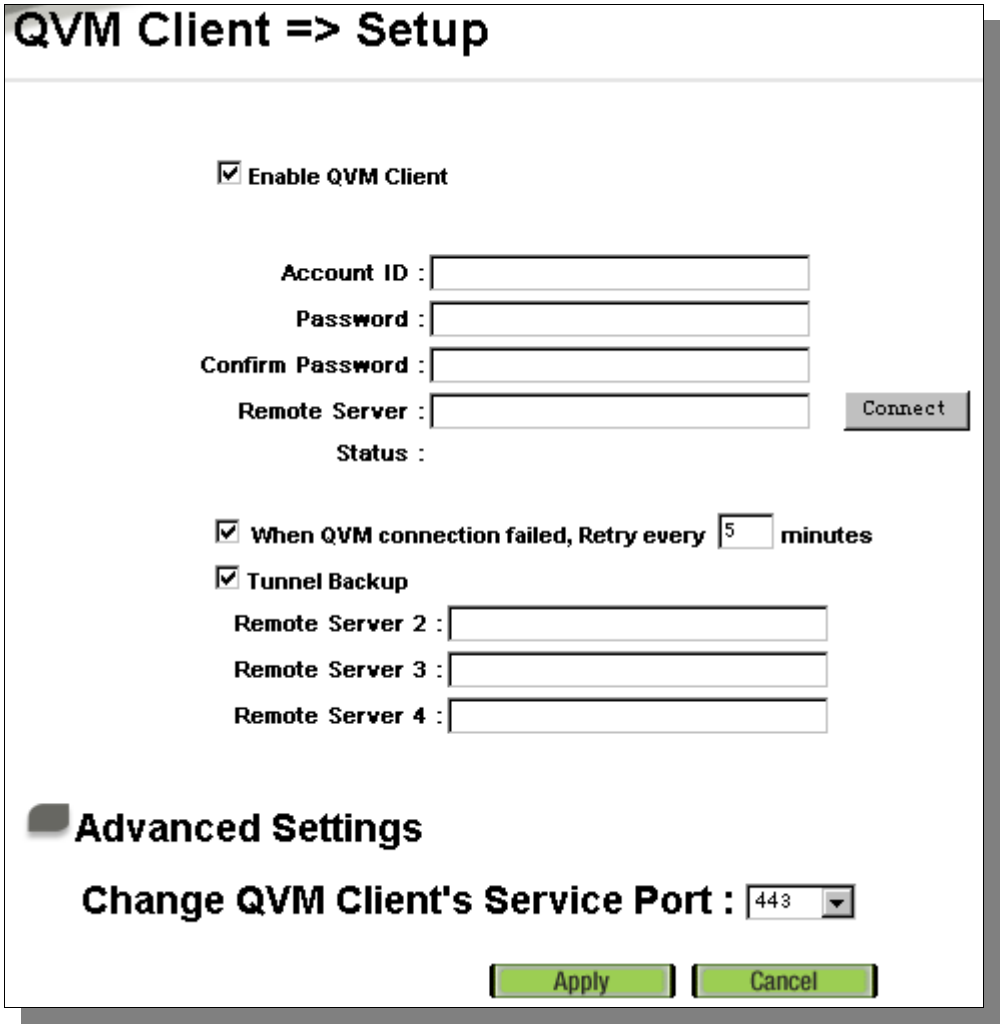
PPTP Pass Through: If this option is **enabled**, the PC is allowed to use VPN-PPTP packet to pass in order to connect with external VPN device.

L2TP Pass Through: If this option is **enabled**, the PC end is allowed to use VPN- L2TP packet to pass in order to connect with external VPN device.

VIII. QVM VPN Function Setup

The QVM-series device provides three major convenient functions:

1. **Smart Link IPSec VPN:** Easy VPN setup replaces the conventional complicated VPN setup process by entering **Server IP, User Name,** and **Password**.
2. **Central Control Feature:** Displays a clear VPN connection status of all remote ends and branches. Its central control screen allows setup from remote into external client ends.
3. **VPN Disconnection Backup:** Solves data transmission problem arising from failed ISP connection with remote ends or the branches.



Enable QVM	Enable this account.

Client：	
Account ID：	Must be identical to that of the remote client end such as QVM100, QVM330 or QVM660. Please enter the remote client user name in either English or Chinese.
Password：	Must be identical to that of the remote client end such as QVM100,
Confirm Password：	Please enter the password and confirm again.
Remote Server：	Input the IP address or Domain name of QVM Server.
Status：	Displays the QVM VPN connection status. Red means disconnection and green means connection.
When QVM connection failed， Retry every ( ) minutes	This function is to set re- connect duration if QVM contention drops. The range is 1~60 mins.
Tunnel Backup：	You can input at most 3 backup IP addresses or domain names for backup. Once the connection is dropped, the function will be automatically enabled to backup the VPN connection and ensure data transition security.
Remote Server 2/3/4：	Input the IP address or Domain Name of QVM back-up central server .

After modification, push "Apply" button to save the network setting or push "Cancel" to keep the settings unchanged.

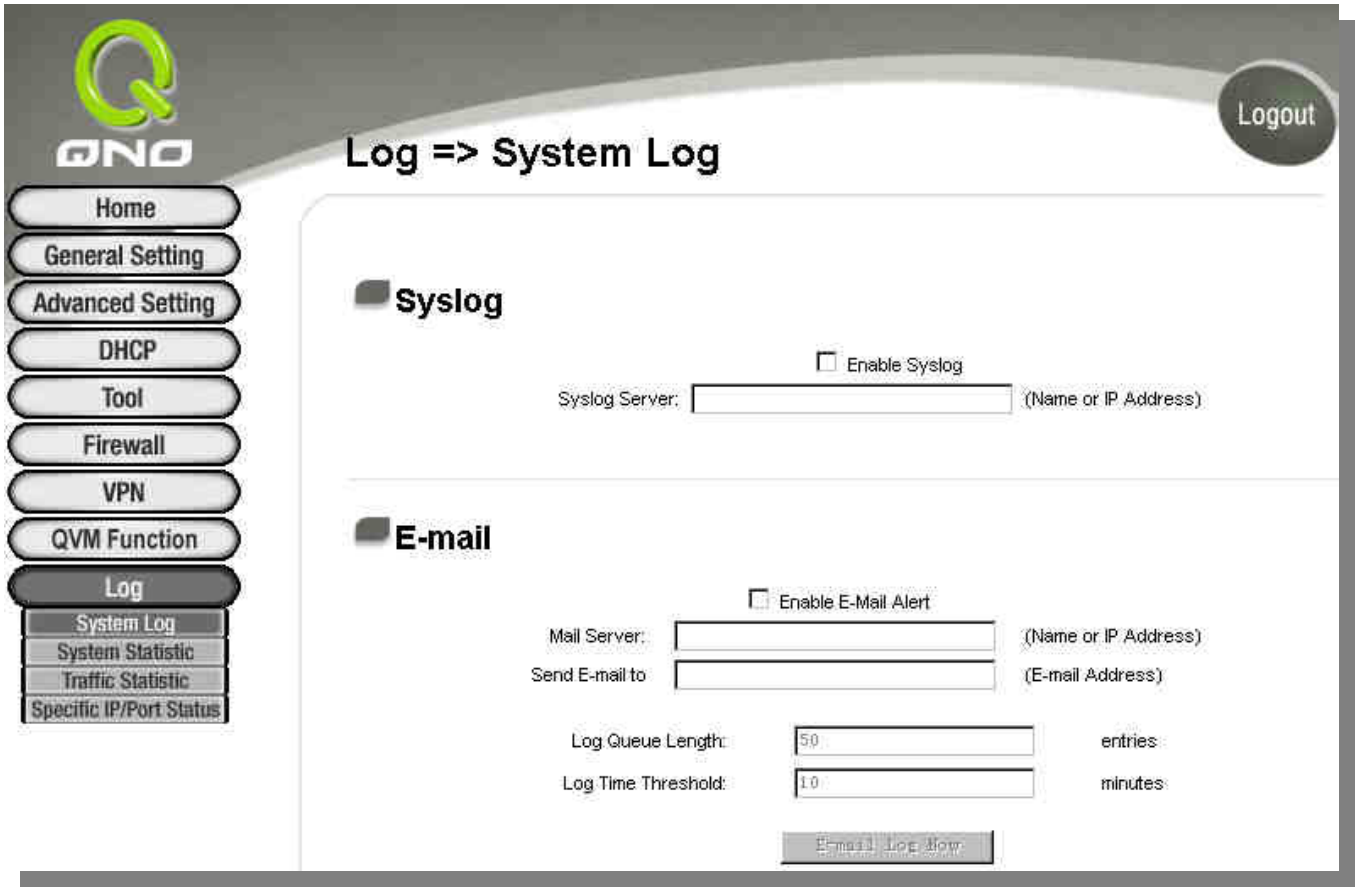
QVM Advanced Settings

IX. Log Configuration

From the log management and look up, we can see the relevant operation status, which is convenient for us to facilitate the setup and operation.

9.1 System Log

Its system log offers three options: system log, E-mail alert and log setting.



Syslog:

Enabled: If this option is selected, the System Log feature will be enabled.

SysLog Server: The device provides external system log servers with log collection feature. System log is an industrial standard communications protocol. It is designed to dynamically capture related system message from the network. The system log provides the source and the destination IP addresses during the connection, service number

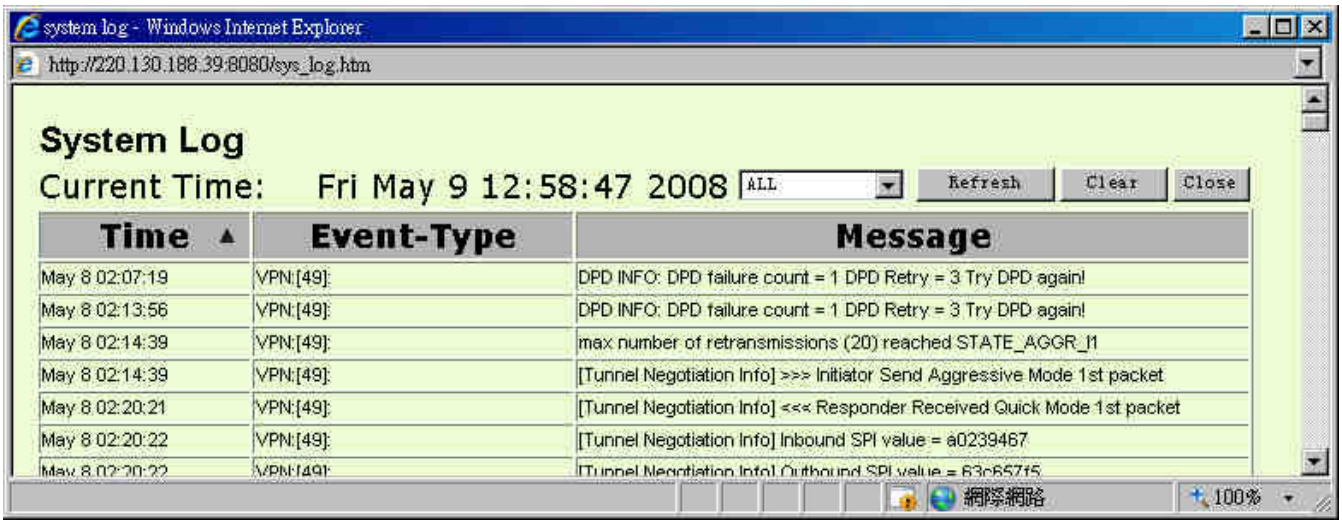
and type. To apply this feature, enter the system log server name or the IP address into the empty "system log server" field.

E-mail :

Enabled:	If this option is selected, E-mail Warning will be enabled.
Mail Server:	If users wish to send out all the logs, please enter the E-mail server name or the IP address, for instance:mail.abc.com
E-mail:	This is set as system log recipient email address such asabc@mail.abc.com
Log Queue Length:	Set the number of Log entries, and the default entry number is 50. When this defined number is reached, it will automatically send out the log mail.
Log Time Threshold:	Set the interval of sending the log, and the default is set to 10 minutes. Reaching this defined number, it will automatically send out the Mail log. The device will detect which parameter (either entries or intervals) reaches the threshold first and send the log message of that parameter to the user.
E-mail Log Now:	Users may send out the log right away by pressing this button.

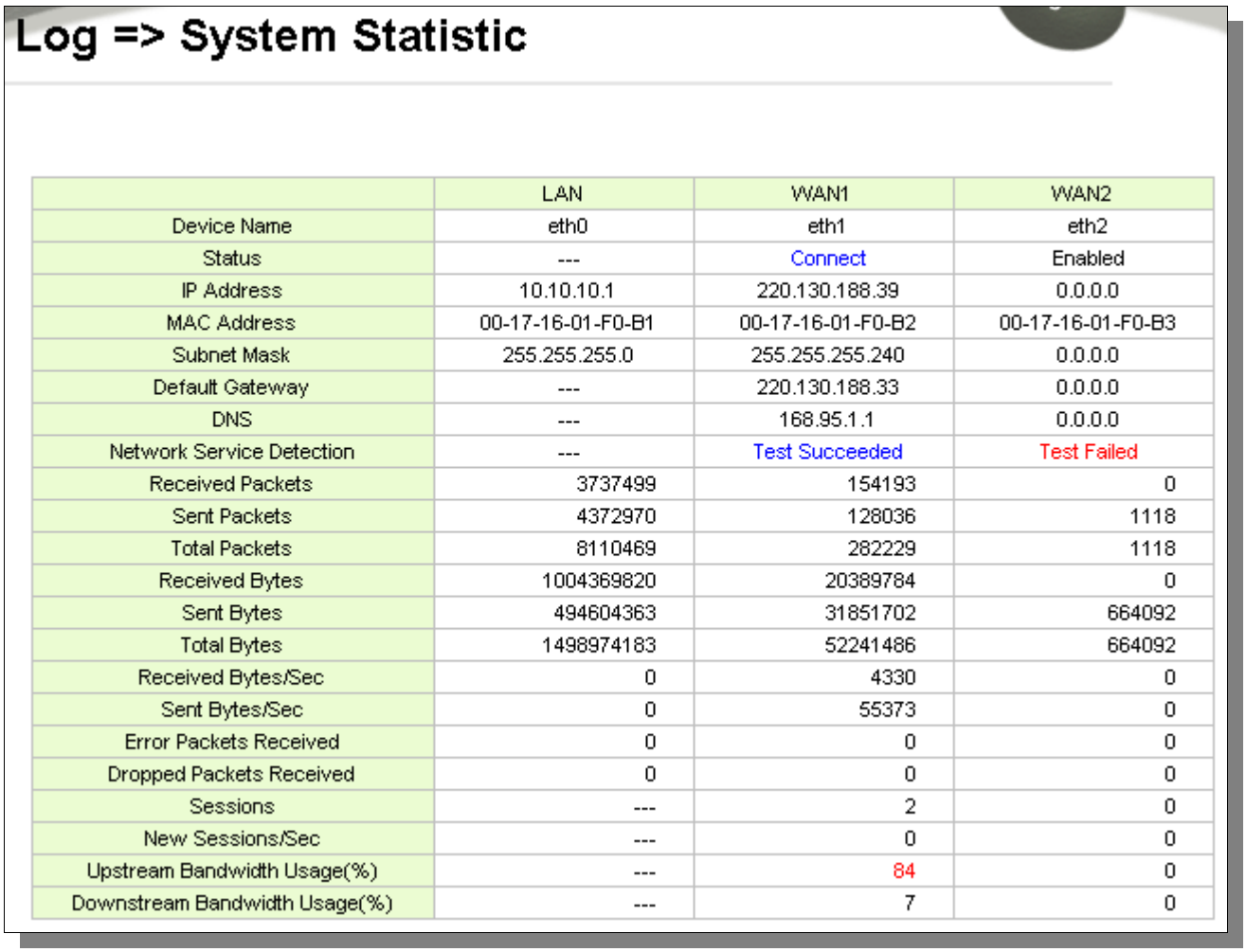
Clink "**View System Log**", and then you can review the related list of system log:

This option allows users to view system log. The message content can be read online via the device. They include **All Log, System Log, Access Log, Firewall Log** and **VPN log**, which is illustrated as below.



9.2 System Statistics

The device has the real-time surveillance management feature that provides system current operation information such as port location, device name, current WAN link status, IP address, MAC address, subnet mask, default gateway, DNS, number of received/ sent/ total packets , number of received/ sent/ total Bytes, Received and Sent Bytes/Sec., total number of error packets received, total number of the packets dropped, number of session, number of the new Session/Sec., and upstream as well as downstream broadband usage (%).

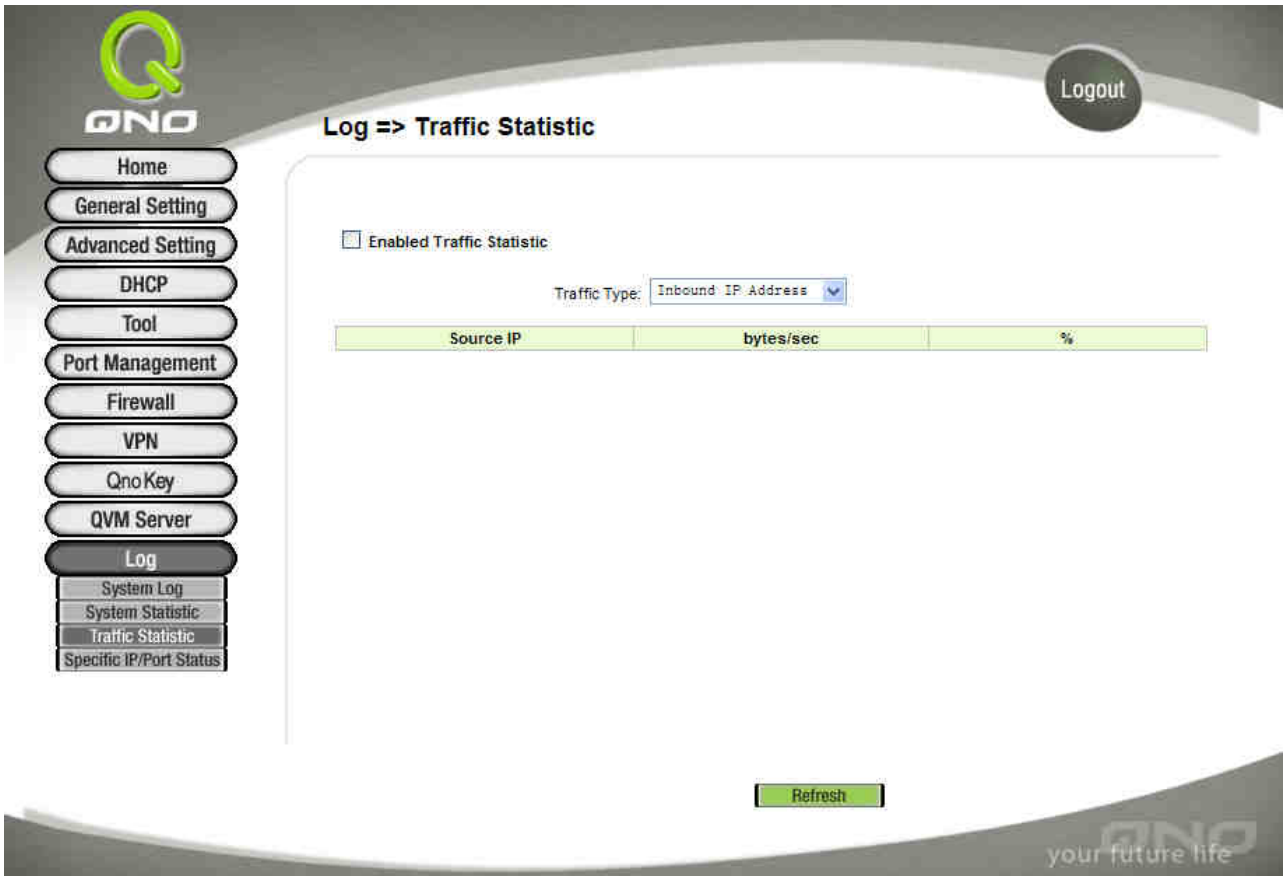


Log => System Statistic

	LAN	WAN1	WAN2
Device Name	eth0	eth1	eth2
Status	---	Connect	Enabled
IP Address	10.10.10.1	220.130.188.39	0.0.0.0
MAC Address	00-17-16-01-F0-B1	00-17-16-01-F0-B2	00-17-16-01-F0-B3
Subnet Mask	255.255.255.0	255.255.255.240	0.0.0.0
Default Gateway	---	220.130.188.33	0.0.0.0
DNS	---	168.95.1.1	0.0.0.0
Network Service Detection	---	Test Succeeded	Test Failed
Received Packets	3737499	154193	0
Sent Packets	4372970	128036	1118
Total Packets	8110469	282229	1118
Received Bytes	1004369820	20389784	0
Sent Bytes	494604363	31851702	664092
Total Bytes	1498974183	52241486	664092
Received Bytes/Sec	0	4330	0
Sent Bytes/Sec	0	55373	0
Error Packets Received	0	0	0
Dropped Packets Received	0	0	0
Sessions	---	2	0
New Sessions/Sec	---	0	0
Upstream Bandwidth Usage(%)	---	84	0
Downstream Bandwidth Usage(%)	---	7	0

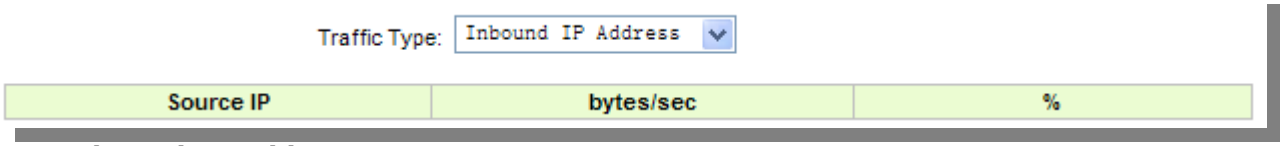
9.3 Traffic Statistic

Six messages will be displayed on the **Traffic Statistic** page to provide better traffic management and control.



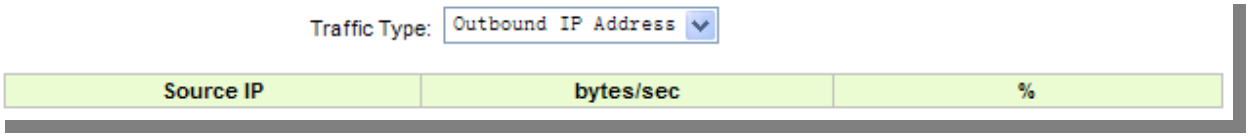
Inbound IP Address

The figure displays the source IP address, bytes per second and percentage.



Outbound IP Address

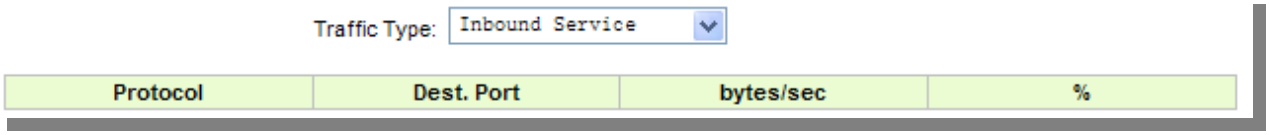
The figure displays the source IP address, bytes per second and percentage.



Inbound Service

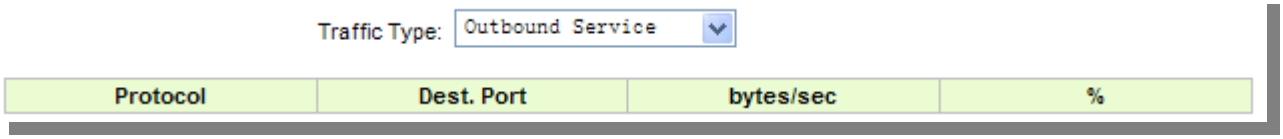
The figure displays the network protocol type, destination IP address, bytes per second

and percentage.



Outbound Service Ports

The figure displays the network protocol type, destination IP address, bytes per second and percentage.



Inbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

Outbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

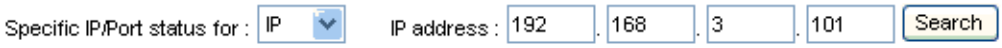
9.4 Specific IP/ Port Status

The device allows administrators to inquire a specific IP (or from a specific port) about the addresses that this IP had visited, or the users (source IP) who used this service port. This facilitates the identification of websites that needs authentication but allows single WAN port rather than Multi-WAN. Administrators may find out the destination IP for protocol binding to solve this login problem. For example, when certain port software is denied, inquiring about the IP address of this specific software server port may apply this feature. Moreover, to find out

BT or P2P software; users may select this feature to inquire users from the port.

Specific IP Status

Enter the IP address that users want to inquire, and then the entire destination IP connected to remote devices as well as the number of ports will be displayed.



Source IP	Protocol	Source Port	Interface(WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.3.101	TCP	4522	WAN1	24.147.69.61	44677	60	29
192.168.3.101	UDP	16086	WAN1	219.134.169.251	9533	3	3
192.168.3.101	TCP	4926	WAN1	24.232.220.43	40638	9	4
192.168.3.101	TCP	4927	WAN1	81.98.30.81	2048	9	4
192.168.3.101	UDP	16086	WAN1	24.15.195.99	47466	0	0
192.168.3.101	UDP	16086	WAN1	24.232.220.43	40638	5	5
192.168.3.101	UDP	16086	WAN1	211.162.238.218	32523	0	0
192.168.3.101	UDP	16086	WAN1	81.98.30.81	2048	5	5
192.168.3.101	TCP	4945	WAN1	211.162.238.218	32523	0	0
192.168.3.101	TCP	4946	WAN1	24.15.195.99	47466	0	0
192.168.3.101	UDP	16086	WAN1	211.31.56.225	8764	0	0
192.168.3.101	UDP	16086	WAN1	210.6.20.120	55870	6	15
192.168.3.101	UDP	16086	WAN1	220.15.76.4	25576	0	0
192.168.3.101	UDP	16086	WAN1	219.212.48.36	62510	0	0
192.168.3.101	UDP	16086	WAN1	211.21.137.7	81	0	0
192.168.3.101	UDP	16086	WAN1	221.216.138.191	14372	0	0
192.168.3.101	UDP	16086	WAN1	163.25.149.159	30416	0	0
192.168.3.101	UDP	16086	WAN1	81.111.168.144	9749	4	6
192.168.3.101	UDP	16086	WAN1	220.210.225.129	18569	7	15
192.168.3.101	UDP	16086	WAN1	24.253.72.162	43076	0	0
192.168.3.101	TCP	3637	WAN1	220.130.115.248	80	0	0

Specific Port Status

Enter the service port number in the field and IP that are currently used by this port will be displayed.

Specific IP/Port status for : Port Port: 80 Search

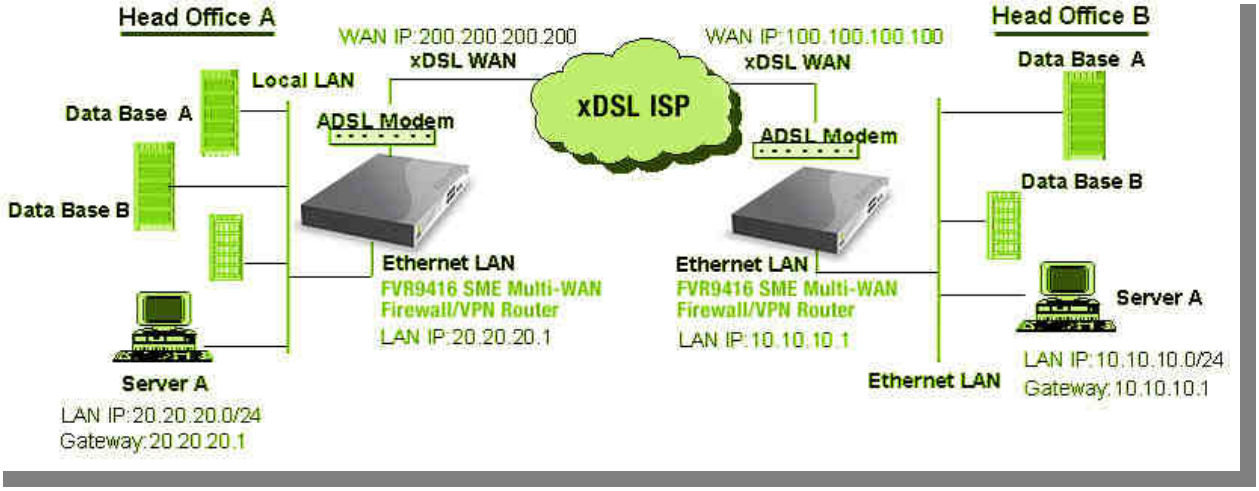
Source IP	Protocol	Source Port	Interface(WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.3.101	TCP	3853	WAN1	220.130.115.248	80	28	60

X. Logout

Click the "**Logout**" button, which is to terminate VPN Firewall management meanwile it also terminates the management user interface. If you want to go into this user interface, please repeat the same steps and input administrator's ID and password.

Appendix I: VPN setting Sample

VPN Environment Sample 1： Gateway to Gateway



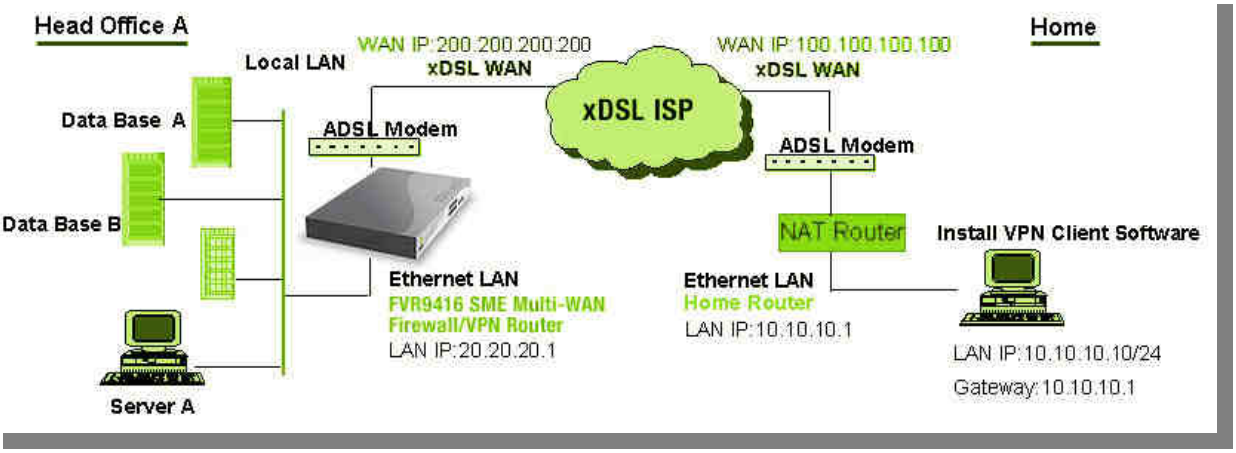
Firewall Setting： Firewall➔General➔Block WAN Request = Disable

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

QVM100 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	255.255.255.0	255.255.255.0

Mask		
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Both sides should use the same key.	

VPN Environment Sample 2： Gateway to Gateway

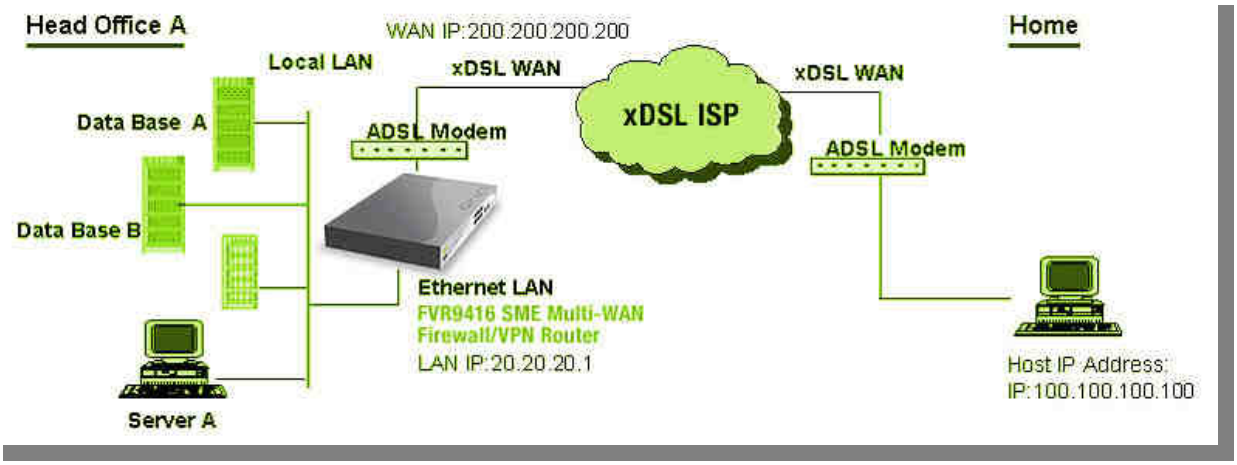


VPN Setting： VPN➔Summary➔Add New Tunnel➔Gateway to Gateway

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	10.10.10.10

Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.0
Remote Security Gateway Type	Domain Name	IP
Remote Security Gateway Type➔ Domain Name	Company domain Name	
Local ID➔ Domain Name		Company domain Name
Remote Security Gateway Type➔ IP Address	100.100.100.100	200.200.200.200
Remote Security Group Type	IP	Subnet
Remote Security Group Type➔ IP Address	10.10.10.10	20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

VPN Environment Sample 3： Client to Gateway (Tunnel)



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

	Head Office A	Home1 (VPN Client SW)
Tunnel Name	Home1	HOA
Interface	WAN1	WAN
Enable	Checked	Checked
Local Security Group Type	Subnet	IP
Local Security Group Type➔ IP Address	20.20.20.0	100.100.100.100
Local Security Group Type➔ Subnet Mask	255.255.255.0	255.255.255.255
Remote Security Gateway Type		IP
Remote Security Gateway Type➔IP Address		200.200.200.200
Remote Client	Email Address	
Remote Client➔ Email Address	User Email Address	
Local ID➔ Email Address		User Email Address
Remote Client➔ IP Address	100.100.100.100	
Remote Security Group Type		Subnet
Remote Security Group Type➔ IP Address		20.20.20.0
Remote Security Group Type➔ Subnet Mask		255.255.255.0
Keying Mode	IKE with preshared key	IKE with preshared key
Phase 1 DH Group	Group 1	Group 1
Phase 1 Encryption	DES	DES
Phase 1 Authentication	MD5	MD5
Phase 1 SA Life Time	28，800 Seconds	28，800 Seconds
Perfect Forward Secrecy	Checked	Checked
Phase 2 DH Group	Group 1	Group 1
Phase 2 Encryption	DES	DES
Phase 2 Authentication	MD5	MD5
Phase 2 SA Life Time	3600 Seconds	3600 Seconds
Preshared Key	Your tunnel password	

Appendix II：Qno Technical Support Information

For more information about the Qno's product and technology, please log onto the Qno's bandwidth forum, refer to the examples of the FTP server, or contact the technical department of Qno's dealers as well as the Qno's Mainland technical center.

Qno Official Website

http：//www.Qno.com.tw

Dealer Contact

Users may log on to the service webpage to check the contacts of dealers.

http：//www.qno.com.tw/web/where_buy.asp

Taiwan Support Center：

E- mail：QnoFAE@qno.com.tw