Multi-Homing Security Gateway

MH-2000, MH-4000

User s Manual

Copyright

Copyright (C) 2004 PLANET Technology Corp. All rights reserved.
The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.
No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.
PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.
Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.
If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

This is a class B device, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology.
This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Customer Service

For information on customer service and support for the Multi-Homing Security Gateway, please refer to the following Website URL:

http://www.planet.com.tw

Before contacting customer service, please take a moment to gather the following information:

- Multi-Homing Security Gateway serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User's Manual for PLANET Multi-Homing Security Gateway

Model: MH-2000, MH-4000

Rev: 2.0 (July, 2004)

Part No. EM-MHv2

Table of Contents

CHAPTER 1: INTRODUCTION 1

1.1 FEATURES 1
1.2 PACKAGE CONTENTS 2
1.3 MULTI-HOMING SECURITY GATEWAY FRONT VIEW 3
1.4 MULTI-HOMING SECURITY GATEWAY REAR PANEL 3
1.5 SPECIFICATION 5

CHAPTER 2: HARDWARE INSTALLATION 6

2.1 INSTALLATION REQUIREMENTS 6
2.2 OPERATION MODE 6
2.2.1 Transparent Mode Connection Example 6
2.2.2 NAT Mode Connecting Example 7

CHAPTER 3: GETTING STARTED 9

3.1 WEB CONFIGURATION 9
3.2 CONFIGURE WAN 1 INTERFACE 10
3.3 CONFIGURE WAN 2 INTERFACE 12
3.4 CONFIGURE DMZ INTERFACE 12
3.5 CONFIGURE POLICY 12

CHAPTER 4: WEB CONFIGURATION 14

4.1 SYSTEM 15
4.1.1 Admin 17
4.1.2 Settings 20
4.1.3 Date/Time 27
4.1.4 Multiple Subnet 28
4.1.5 Hacker Alert 36
4.1.6 Blaster Alert (MH-4000 only) 38
4.1.7 Route Table 39
4.1.8 DHCP 43
4.1.9 Dynamic DNS 45
4.1.10 DNS Proxy 49
4.1.11 SNMP (MH-4000 only) 51
4.1.12 Permitted IPs 52
4.1.13 Language 55
4.1.14 Logout 56
4.1.15 Software Update 57

4.2 INTERFACE 59
4.2.1 LAN *59*
4.2.2 WAN *60*
4.2.3 DMZ *65*
4.3 ADDRESS 67
4.3.1 LAN *67*
4.3.2 LAN Group *71*
4.3.3 WAN *75*
4.3.4 WAN Group *79*
4.3.5 DMZ *83*
4.3.6 DMZ Group *87*
4.4 SERVICE 91
4.4.1 Pre-defined *91*
4.4.2 Custom *92*
4.4.3 Group *95*
4.5 SCHEDULE 99
4.6 QOS (MH-4000 ONLY) 102
4.7 AUTHENTICATION (MH-4000 ONLY) 106
4.7.1 Auth User *106*
4.7.2 Auth User Group *111*
4.7.3 Radius Server *115*
4.8 CONTENT FILTERING 117
4.8.1 URL Blocking *117*
4.8.2 General Blocking *120*
4.8.3 P2P Blocking (MH-4000 only) *121*
4.8.4 IM Blocking (MH-4000 only) *122*
4.8.5 Download Blocking (MH-4000 only) *122*
4.9 VIRTUAL SERVER 123
4.9.1 Mapped IP *124*
4.9.2 Virtual Server *128*
4.10 POLICY 137
4.10.1 Outgoing *137*
4.10.2 Incoming *144*
4.10.3 WAN To DMZ & LAN To DMZ *148*
4.10.4 DMZ To WAN & DMZ To LAN *153*
4.11 VPN 158
4.11.1 IPSec Autokey *158*
4.11.2 PPTP Server *216*
4.11.3 PPTP Client *220*

4.12 INBOUND BALANCE (MH-4000 ONLY) 225
4.13 LOG 250
4.13.1 Traffic Log *250*
4.13.2 Event Log *253*
4.13.3 Connection Log *256*
4.13.4 Log Backup *259*
4.14 ALARM 262
4.14.1 Traffic Alarm *262*
4.14.2 Event Alarm *264*
4.15 ACCOUNTING REPORT (MH-4000 ONLY) 266
4.15.1 Outbound Accounting Report *266*
4.15.2 Inbound Accounting Report *271*
4.16 STATISTICS 274
4.16.1 Interface Statistics *274*
4.16.2 Policy Statistics *276*
4.17 STATUS 279
4.17.1 Interface Status *279*
4.17.2 System Info (MH-4000 only) *279*
4.17.3 Auth Status (MH-4000 only) *280*
4.17.4 ARP Table *281*
4.17.5 DHCP Clients *282*

Chapter 1: Introduction

As Internet become essential for your business, the only way to prevent your Internet connection from failure is to have more than one connection. PLANET's Multi-Homing Security Gateways reduce the risk of potential shutdown if one of the Internet connections should fail. In addition, they allow you to perform load-balancing by distributing the traffic through two WAN connections. With embedded DNS server of MH-4000, Connections from Internet are given the IP address of two WAN ports to balance the traffic over the links.

Not only a multi-homing device, PLANET's Multi-Homing Security Gateways provide a complete security solution in a box. The policy-based firewall, Intrusion detection and prevention, content filtering function and VPN connectivity with 3DES and AES encryption make it a perfect product for your network security. No more complex connection and settings for integrating different security products on the network is required.

Bandwidth management function is also supported on MH-4000 to offers network administrators an easy yet powerful means to allocate network resources based on business priorities, and to shape and control bandwidth usage.

1.1 Features

- **WAN Backup:** The MH-2000 and MH-4000 can monitor the each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including "Auto", "Round-Robin", "By Traffic", "By Session" and "By Packet". User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- **Inbound Load Balancing with Embedded DNS Server:** In order to direct traffic to hosted servers through two links and provide inbound loading balancing, the MH-4000 provides a built-in DNS server for the hosted servers.
- **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including SYN attack, ICMP flood, UDP flood, Ping of Death, etc. The access control function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- **VPN Connectivity:** The security gateway support PPTP and IPSec VPN. With DES, 3DES and AES encryption and SHA-1 / MD5 authentication, the network traffic over public Internet is secured.
- **Content Filtering:** The security gateway can block network connection based on URLs or keywords. The Pop-up, Java Applet, cookies and Active X packets can also be blocking by user configuration.
- **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname.
- **Multiple NAT:** Multiple NAT allows local port to set multiple subnetworks and connect with the Internet through different WAN IP Addresses.
- **Server Load Balancing:** Up to 4 group virtual servers are supported for server load balancing
- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **Web based GUI:** supports web based GUI for configuration and management. It also supports multiple language including English, Traditional Chinese and Simplified Chinese.
- **Bandwidth Management (MH-4000 only):** Network packets can be classified based on IP address, IP subnet and TCP/UDP port number and give guarantee and burst bandwidth with three levels of priority.
- **User Authentication (MH-4000 only):** Web-based authentication allows users to be authenticated by web browser. User database can be configured on the devices or through external RADIUS server.

1.2 Package Contents

The following items should be included:

MH-2000

- Multi-Homing Security Gateway
- User's Manual CD-ROM
- This Quick Installation Guide
- Power Adapter

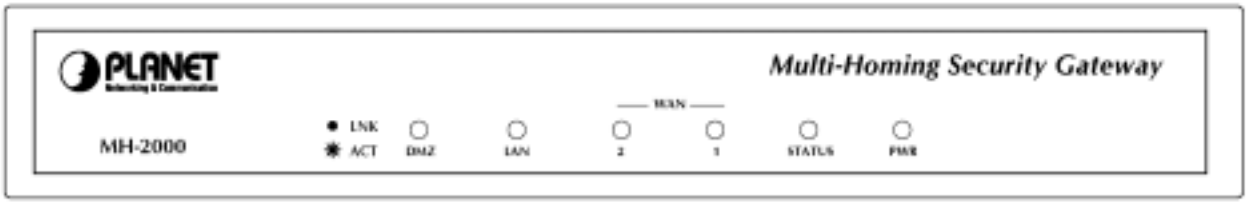
MH-4000

- Multi-Homing Security Gateway
- User's Manual CD-ROM
- This Quick Installation Guide
- Power Cord
- Rack-mounting kit
- RS-232 console cable

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

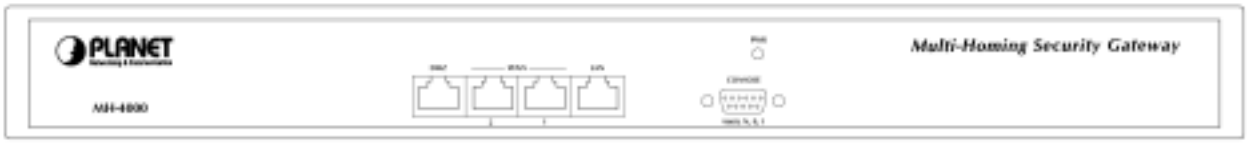
1.3 Multi-Homing Security Gateway Front View

MH-2000 Front Panel



LED	Description
PWR	Power is supplied to this device.
STATUS	Blinks to indicate this devise is being turned on and booting. After one minute, this LED indicator will stop blinking, it means this device is now ready to use.
WAN1, WAN2, LAN, DMZ	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port

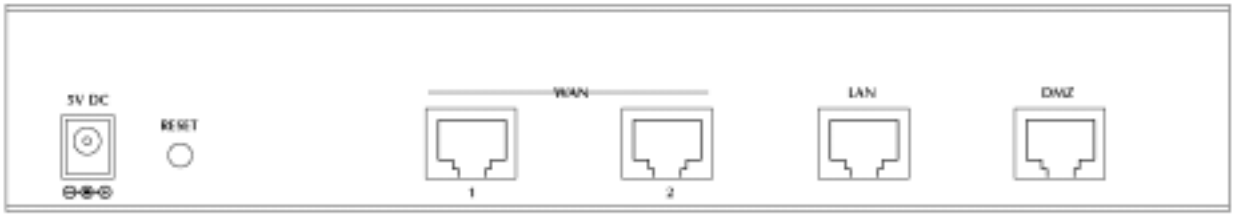
MH-4000 Front Panel



LED	Description	
PWR	Power is supplied to this device.	
WAN1, WAN2, LAN, DMZ	Green	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
	Orange	Steady on indicates the port is connected at 100Mbps speed

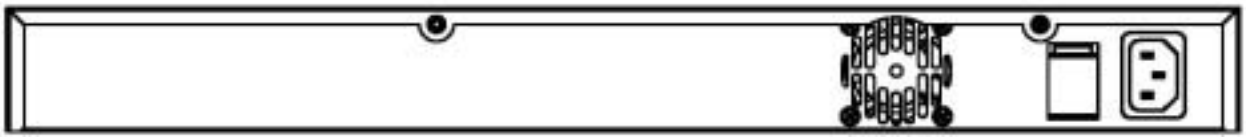
1.4 Multi-Homing Security Gateway Rear Panel

MH-2000 Rear Panel



Port or button	Description
RESET	Press this button to restore to factory default settings.
WAN 1, WAN2	Connect to your xDSL/Cable modem or other Internet connection devices
LAN	Connect to your local PC, switch or other local network device
DMZ	Connect to your server or other network device

MH-4000 Rear Panel



1.5 Specification

Product		Multi-homing Security Gateway	
Model		MH-2000	MH-4000
Hardware			
Ethernet	LAN	1 x 10/100Mbps RJ-45	
	WAN	2 x 10/100Mbps RJ-45	
	DMZ	1 x 10/100Mbps RJ-45	
LED		POWER, STATUS, 10/100 and LNK/ACT for each LAN and WAN port	
Power		5VDC, 2.4A	100~240 VAC, 50~60Hz
Operating Environment		Temperature: 0~50°C Relative Humidity: 10%~90%	
Dimension W x D x H, mm		220 x 149 x 37	431 x 254 x 44
Regulatory		FCC, CE Mark	
Software			
Management		Web	Web, SNMP
Network Connection		Transparent mode (WAN to DMZ), NAT, Multi-NAT, Static Route	
Outbound Load Balancing		Policy-based routing Load-balancing by Round-Robin, traffic, session and packet	
Inbound Load Balancing			Built-in DNS for inbound
Firewall		Policy-based firewall rule with schedule NAT/ NAPT SPI firewall Prevention of SYN attack, ICMP Flood, UDP flood, Ping of Death, Tear Drop, IP Spoofing, IP route, Port Scan and Land attack	
VPN Tunnels		200	1000
VPN Functions		PPTP, IPSec DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN	
Bandwidth Management		-	Policy-based bandwidth management Guarantee and maximum bandwidth with 3 priority levels Classify traffics based on IP, IP subnet, TCP/UDP port
Content Filtering		URL blocking Blocks Popup, Java Applet, cookies and Active X	
User authentication		-	Built-in user database with up to 500 entries Support RADIUS authentication
Log and Alarm		Log and alarm for event and traffic Log can be saved from web, sent by e-mail or sent to syslog server	
Statistics		Traffic statistic for interface (WAN 1/2) and policies Graphic display Record up to 30 day	
Others		Dynamic DNS NTP support DHCP server Mapping IP (DMZ) Server load balancing	

Chapter 2: Hardware Installation

2.1 Installation Requirements

Before installing the Multi-Homing Security Gateway, make sure your network meets the following requirements.

- Mechanical Requirements

The Multi-Homing Security Gateway is to be installed between your Internet connection and local area network. The Multi-Homing Security Gateway can be placed on the table or rack. Locate the unit near the power outlet.

- Electrical Requirements

The Multi-Homing Security Gateway is a power-required device, it means, the Multi-Homing Security Gateway will not work until it is powered. If your networked PCs will need to transmit data all the time, please consider use an UPS (Uninterrupted Power Supply) for your Multi-Homing Security Gateway. It will prevent you from network data loss. In some area, installing a surge suppression device may also help to protect your Multi-Homing Security Gateway from being damaged by unregulated surge or current to the Multi-Homing Security Gateway.

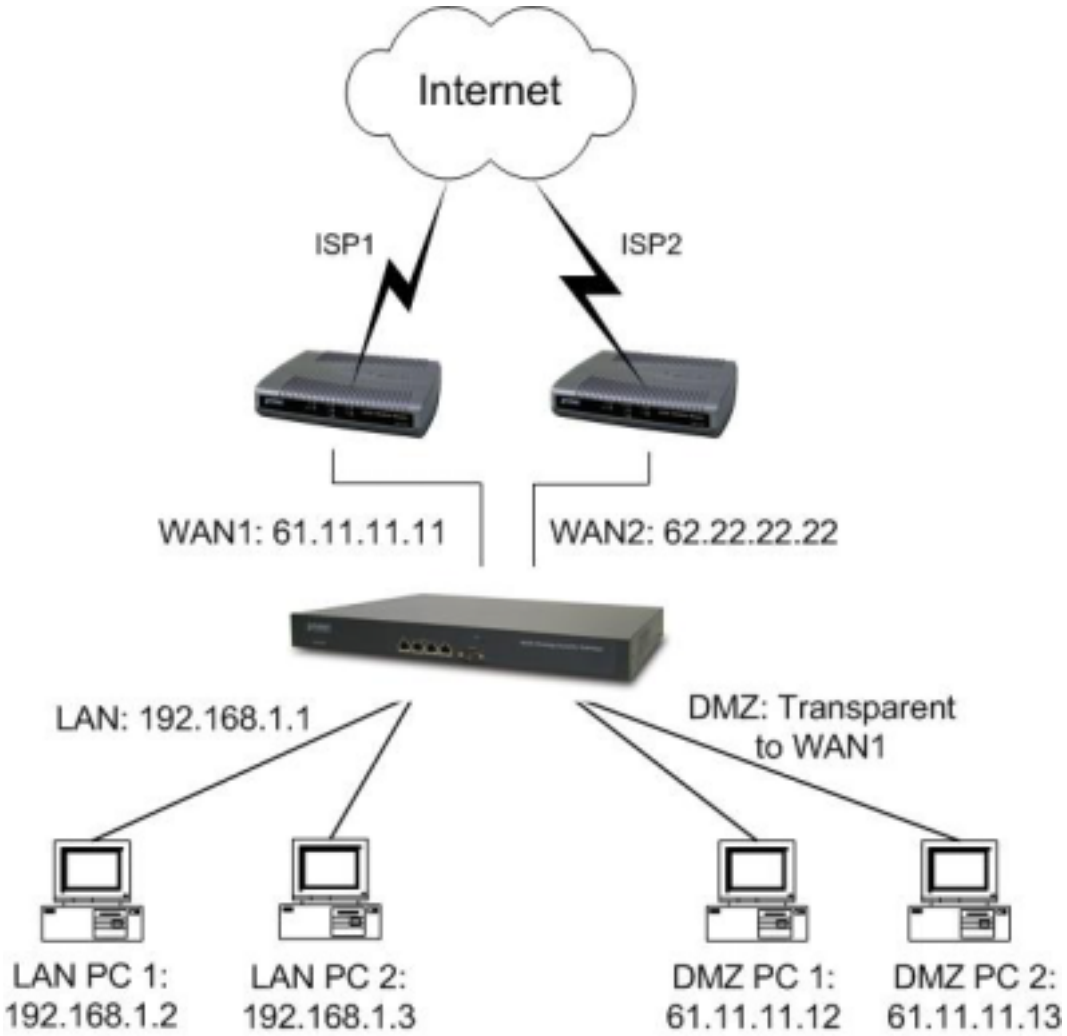
- Network Requirements

In order for Multi-Homing Security Gateway to secure your network traffic, the traffic must pass through Multi-Homing Security Gateway at a useful point in a network. In most situations, the Multi-Homing Security Gateway should be placed behind the Internet connection device.

2.2 Operation Mode

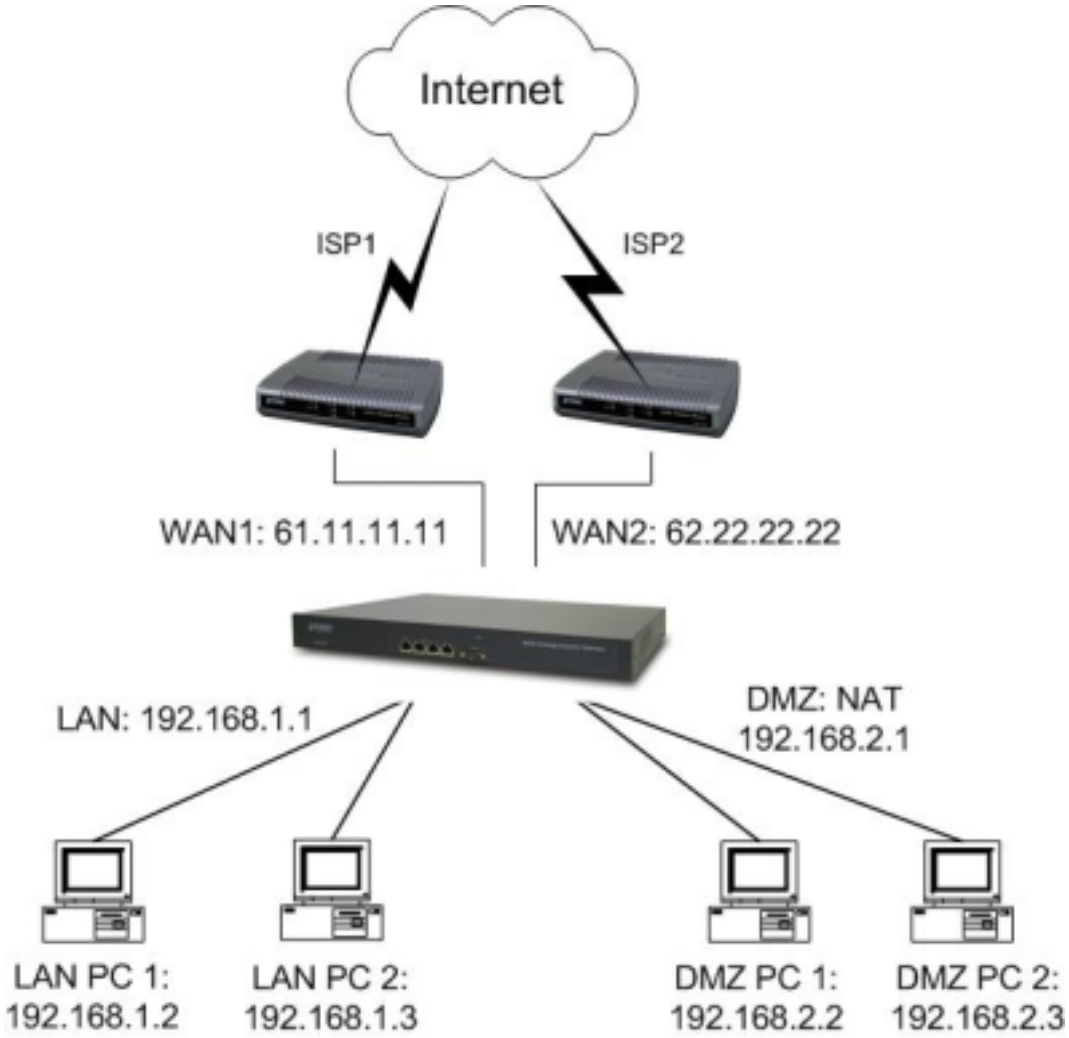
MH-2000/-4000 DMZ port supports three operation modes, Disable, NAT and Transparent. In Disable mode, the DMZ port is not active. In transparent mode, MH-2000/-4000 works as proxy with forward DMZ packet to WAN and forward WAN packet to DMZ. The DMZ and WAN side IP addresses are in the same subnet. In NAT mode, DMZ side user will share one public IP address of WAN port to make Internet connection. Please find the following two pictures for example.

2.2.1 Transparent Mode Connection Example



The WAN1 and DMZ side IP addresses are on the same subnet. This application is suitable if you have a subnet of IP addresses and you do not want to change any IP configuration on the subnet.

2.2.2 NAT Mode Connecting Example



DMZ and WAN1 IP addresses are on the different subnet. This provides higher security level then transparent mode.

Chapter 3: Getting Started

3.1 Web Configuration

STEP 1:

Connect both the Administrator's PC and the LAN port of the Multi-Homing Security Gateway to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Multi-Homing Security Gateway has an embedded web server used for management and configuration. Use a web browser to display the configurations of the Multi-Homing Security Gateway (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of the Multi-Homing Security Gateway is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2– 192.168.1.254

If the company's LAN IP Address is not subnet of 192.168.1.0, (i.e. LAN IP Address is 172.16.0.1), then the Administrator must change his/her PC IP address to be within the same range of the LAN subnet (i.e. 172.16.0.2). Reboot the PC if necessary.

By default, the Multi-Homing Security Gateway is shipped with its DHCP Server function enabled. This means the client computers on the LAN network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the Multi-Homing Security Gateway.

The following table is a list of private IP addresses. These addresses may not be used as a WAN IP address.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

STEP 2:

Once the Administrator PC has an IP address on the same network as the Multi-Homing Security Gateway, open up an Internet web browser and type in http://192.168.1.1 in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required to connect to the Multi-Homing Security Gateway. Enter the default login username and password of Administrator (see below).

Username: admin
Password: admin
Click OK.

3.2 Configure WAN 1 interface

After entering the username and password, the Multi-Homing Security Gateway WEB UI screen will display. Select the **Interface** tab on the left menu then click on WAN below it.
Click on Modify button of WAN NO. 1. The following page is shown.

Alive Indicator Site IP: This feature is used to ping an address for detecting WAN connection status.
Service: ICMP You can select an IP address by **Assist**, or type an IP address manually.
Service: DNS You can select a DNS IP and Domain name by **Assist**, or type the related data manually.

PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect.
Username: Enter the PPPoE username provided by the ISP.
Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Service-On-Demand:

The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

MAC Address: This is the MAC Address of the device. Some ISPs require specified MAC address. If the required MAC address is your PC's, click **Clone MAC Address**.

Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: You can specify your own domain name or leave it blank.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN 1 port of the device.

Netmask: This will be the Netmask of the WAN 1 network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP Address of the DNS server.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

For PPTP (European User Only): This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.

PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.

Connect ID: This is the ID given by ISP. This is optional.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.

Service-On-Demand:

The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

NOTE: This function is not supported on MH-4000.

Ping: Select this to allow the WAN network to ping the IP Address of the Multi-Homing Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

WebUI: Select this to allow the device WEBUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

3.3 Configure WAN 2 interface

If you want to connect WAN 2 to another ISP connection, click **Modify** button of **WAN No. 2** then repeat above procedures to setup.

3.4 Configure DMZ interface

Depends on your network requirement, you can disable the DMZ port, make DMZ port transparent to WAN 1 or enable NAT function on it.
To configure the DMZ port, select the **Interface** tab on the left menu, then click on DMZ, the following page is shown.

Please refer to section 3 for select the mode you need and configure relative IP parameters.

3.5 Configure Policy

STEP 1:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** (LAN to WAN) from the sub-function list.

STEP 2:

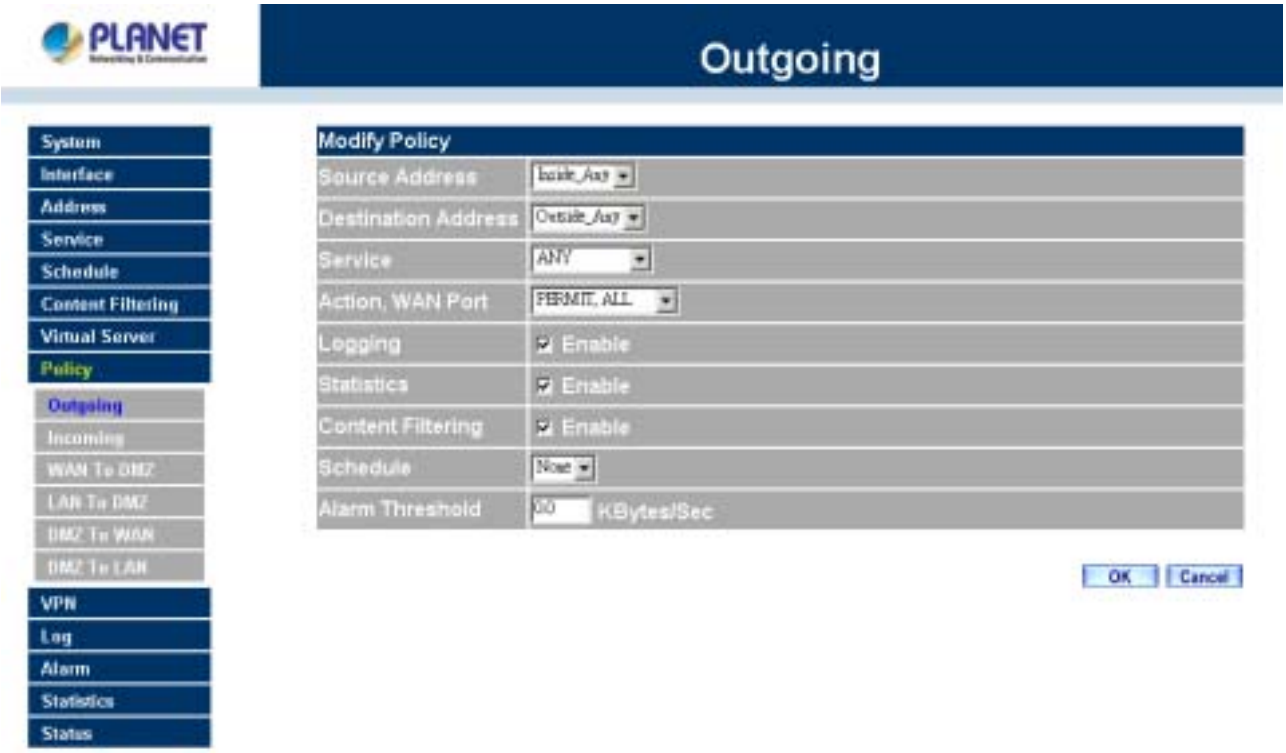
Click on **New Entry** button.

STEP 3:

When the **New Entry** option appears, enter the following configuration:

Source Address – select **Inside_Any**
Destination Address – select **Outside_Any**
Service - select **ANY**
Action - select **Permit, ALL**

Click on **OK** to apply the changes.



STEP 4:

The configuration is successful when the screen below is displayed.

Please make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Multi-Homing Security Gateway's LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately. If a Multi-Homing Security Gateway filter function is required, please refer to the Policy section in chapter 4.

Chapter 4: Web Configuration

The functions of MH-2000 and MH-4000 have some differences. MH-4000 support more functions then MH-2000. Please find the following table for a list of their functions comparison.

Menu items	MH-2000	MH-4000
System		
Admin	V	V
Setting	V	V
Date/Time	V	V
Multiple Subnet	V	V
Hacker Alert	V	V
Blaster Alert	N/A	V
Route Table	V	V
DHCP	V	V
DNS Proxy	V	V
SNMP	N/A	V
Dynamic DNS	V	V
Language	V	V
Permitted IP	V	V
Logout	V	V
Software Update	V	V
Interface	V	V
LAN	V	V
WAN	V	V
DMZ	V	V
Address	V	V
LAN	V	V
LAN Group	V	V
WAN	V	V
WAN Group	V	V
DMZ	V	V
DMZ Group	V	V
Service	V	V
Pre-defined	V	V
Custom	V	V
Group	V	V
Schedule	V	V
QoS	N/A	V
Authentication	N/A	V
Auth User	N/A	V
Auth User Group	N/A	V
RADIUS	N/A	V
Content Filter	V	V
URL Blocking	V	V
Script Blocking	V	V
P2P Blocking	N/A	V
IM Blocking	N/A	V
Download Blocking	N/A	V
Virtual Server	V	V
Mapped IP	V	V
Virtual Server1	V	V
Virtual Server2	V	V
Virtual Server3	V	V

Virtual Server4	V	V
Policy	V	V
Outgoing	V	V
Incoming	V	V
WAN to DMZ	V	V
LAN to DMZ	V	V
DMZ to WAN	V	V
DMZ to LAN	V	V
VPN	V	V
IPSec Autokey	V	V
PPTP Server	V	V
PPTP Client	V	V
Inbound Balance	N/A	V
Log	V	V
Traffic Log	V	V
Event Log	V	V
Connection Log	V	V
Log Backup	V	V
Alarm	V	V
Traffic Alarm	V	V
Event Alarm	V	V
Accounting Report	N/A	V
Outbound	N/A	V
Inbound	N/A	V
Statistics	V	V
Interface Statistics	V	V
Policy Statistics	V	V
Status	V	V
Interface Status	V	V
System Info.	N/A	V
Auth. Status	N/A	V
ARP Table	V	V
DHCP Clients	V	V

4.1 System

The Multi-Homing Security Gateway Administration and monitoring configuration is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

1. Add and change the sub Administrator's names and passwords;
2. Back up all Multi-Homing Security Gateway settings into local files;
3. Set up alerts for Hackers invasion.

"System" is the managing of settings such as the privileges of packets that pass through the Multi-Homing Security Gateway and monitoring controls. Administrators may manage, monitor, and configure Multi-Homing Security Gateway settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the Multi-Homing Security Gateway.

Admin: has control of user access to the Multi-Homing Security Gateway. He/she can add/remove users and change passwords.

Setting: The Administrator may use this function to backup Multi-Homing Security Gateway configurations and export (save) them to an **Administrator** computer or anywhere on the network; or restore a configuration file to the device; or restore the Multi-Homing Security Gateway back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the Multi-Homing Security Gateway has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP (Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.

Date/Time: This function enables the Multi-Homing Security Gateway to be synchronized either with an Internet Server time or with the client computer's clock.

Multiple Subnet: This function allows local port to set multiple subnet works and connect with the internet through different WAN 1 IP Addresses.

Hacker Alert: When abnormal conditions occur, the Multi-Homing Security Gateway will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Blaster Alert (MH-4000 only): This function is to protect your network from blaster worm. When abnormal network access on RPC port occur, the Multi-Homing Security Gateway will block the access on specified time, send an e-mail alert or SNMP trap to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Route Table: Use this function to enable the Administrator to add static routes for the networks when the dynamic route is not efficient enough.

DHCP: Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Dynamic DNS: The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP

DNS-Proxy: The Multi-Homing Security Gateway Administrator may use the DNS Proxy function to make the Multi-Homing Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then come back through the Multi-Homing Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one. This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up DNS Proxy so all the LAN network computers will

use the Multi-Homing Security Gateway as a DNS server, which acts as the DNS Proxy.

SNMP (MH-4000 only): Provide the System Administrator enabling SNMP Trap Alert Notification for sending email to the setting SNMP Trap receiver IP address when the network is disconnected/ connected and being attacked by hackers or when emergency conditions occur.

Permitted IP: Enables the Administrator to authorize specific internal/external IP address(es) for Managing Gateway.

Language: Both Chinese and English are supported in the Multi-Homing Security Gateway.

Logout: Administrator logs out the Multi-Homing Security Gateway. This function protects your system while you are away.

Software Update: The administrator can update the device's software with the latest version. Administrators may visit distributor's web site to download the latest firmware. Administrators may update the device firmware to optimize its performance and keep up with the latest fixes for intruding attacks.

4.1.1 Admin

On the left hand menu, click on **Setup**, and then select **Admin** below it. The current list of Administrator(s) shows up.

Settings of the Administration table

<u>Administrator Name:</u> The username of Administrators for the Multi-Homing Security Gateway. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)

The username of the main Administrator is **Administrator** with **read / write** privilege.

Sub Admins may be created by the **Admin** by clicking **New Sub Admin.** Sub Admins have **read only** privilege.

Configure: Click **Modify** to change the "Sub Administrator's" password and click **Remove** to delete a "Sub Administrator."

Changing the Main/Sub-Administrator s Password

Step 1. The **Modify Administrator Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.

Adding a new Sub Administrator

Step 1. In the **Add New Sub Administrator** window:

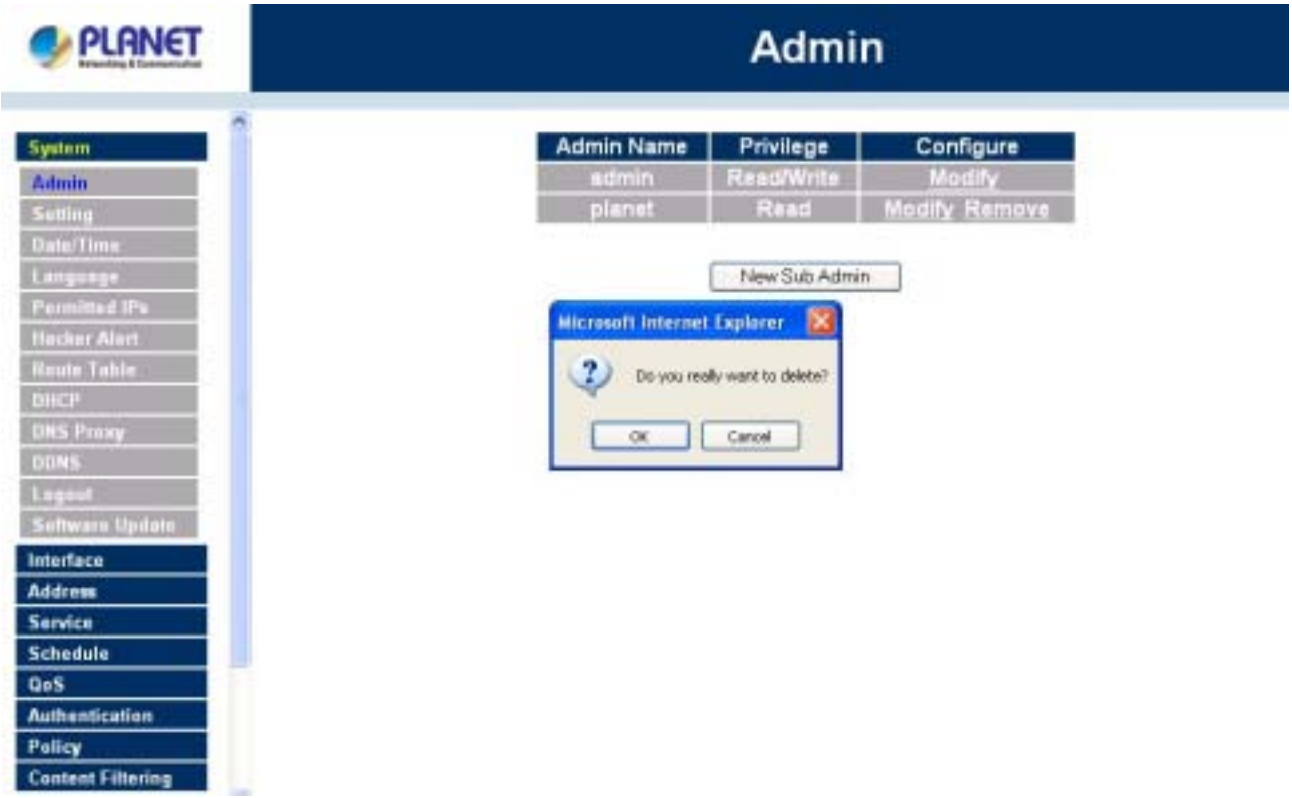
- **Sub Admin Name:** enter the username of new **Sub Admin.**
- **Password:** enter a password for the new **Sub Admin.**
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.

Removing a Sub Administrator

Step 1. In the Administration table, locate the Administrator name you want to edit, and click on the **Remove** option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

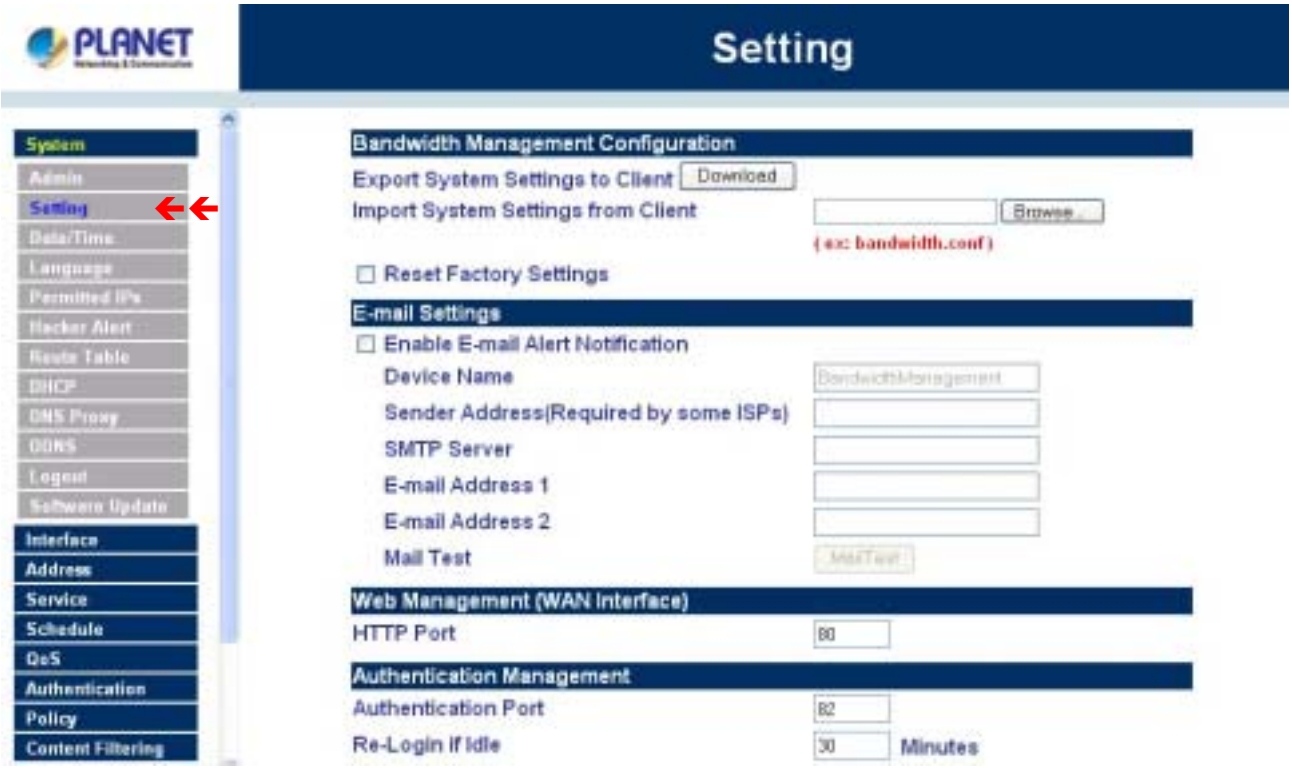


4.1.2 Settings

The Administrator may use this function to backup Multi-Homing Security Gateway configurations and export (save) them to an **Administrator** computer or anywhere on the network; or restore a configuration file to the device; or restore the Multi-Homing Security Gateway back to default factory settings.

Entering the Settings window

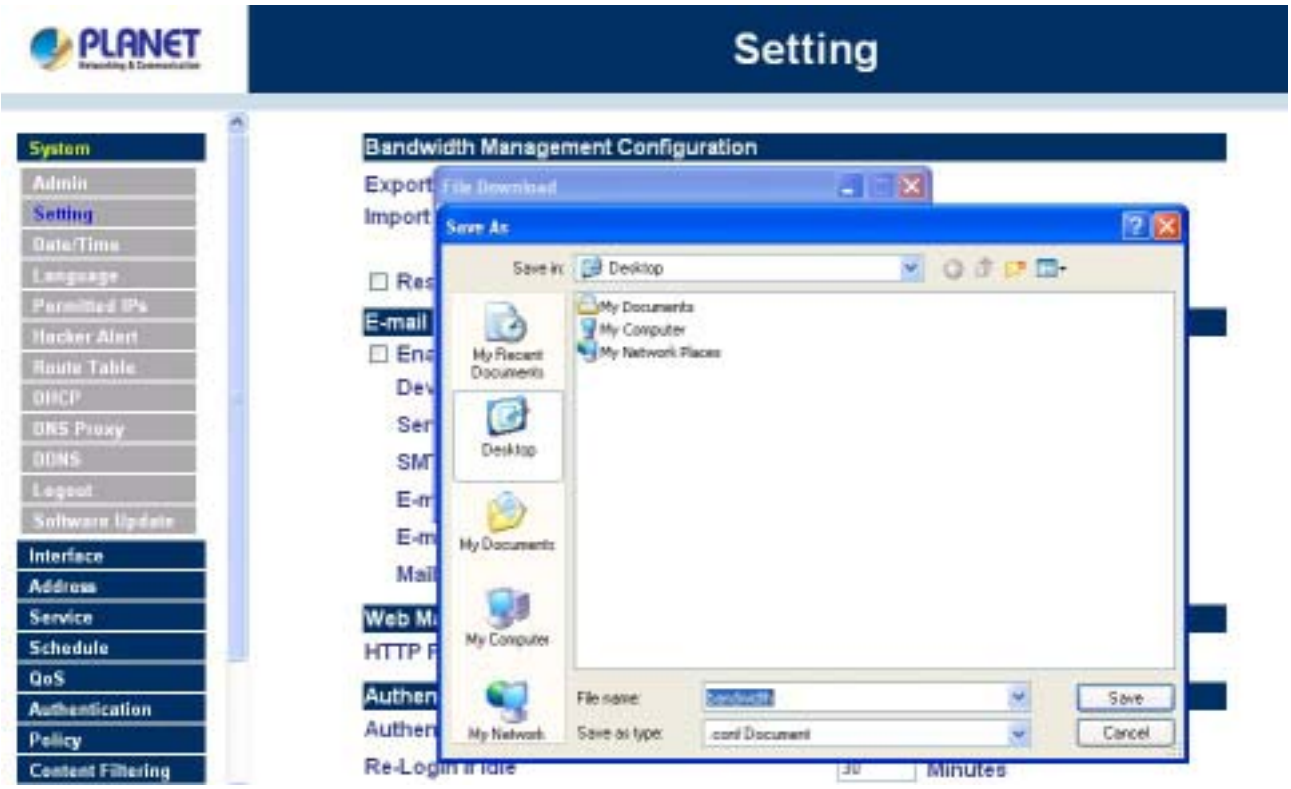
Click **Setting** in the **System** menu to enter the **Settings** window. The **Multi-Homing Security Gateway Configuration** settings will be shown on the screen.



Exporting Multi-Homing Security Gateway settings

Step 1. Under **Configuration**, click on the **Download** button next to **Export System Settings to Client**.

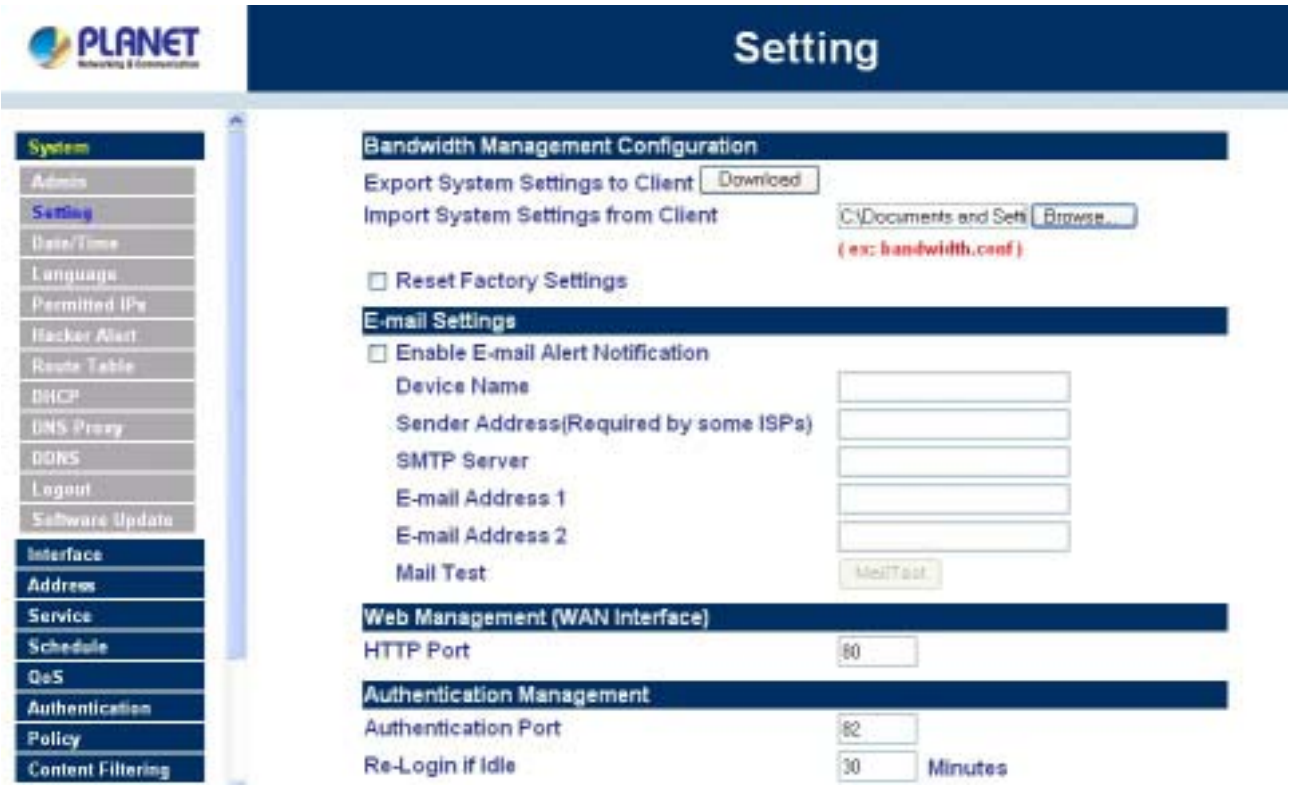
Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.



Importing Multi-Homing Security Gateway settings

Under **Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file which contains the saved Multi-Homing Security Gateway Settings, then click **OK**.

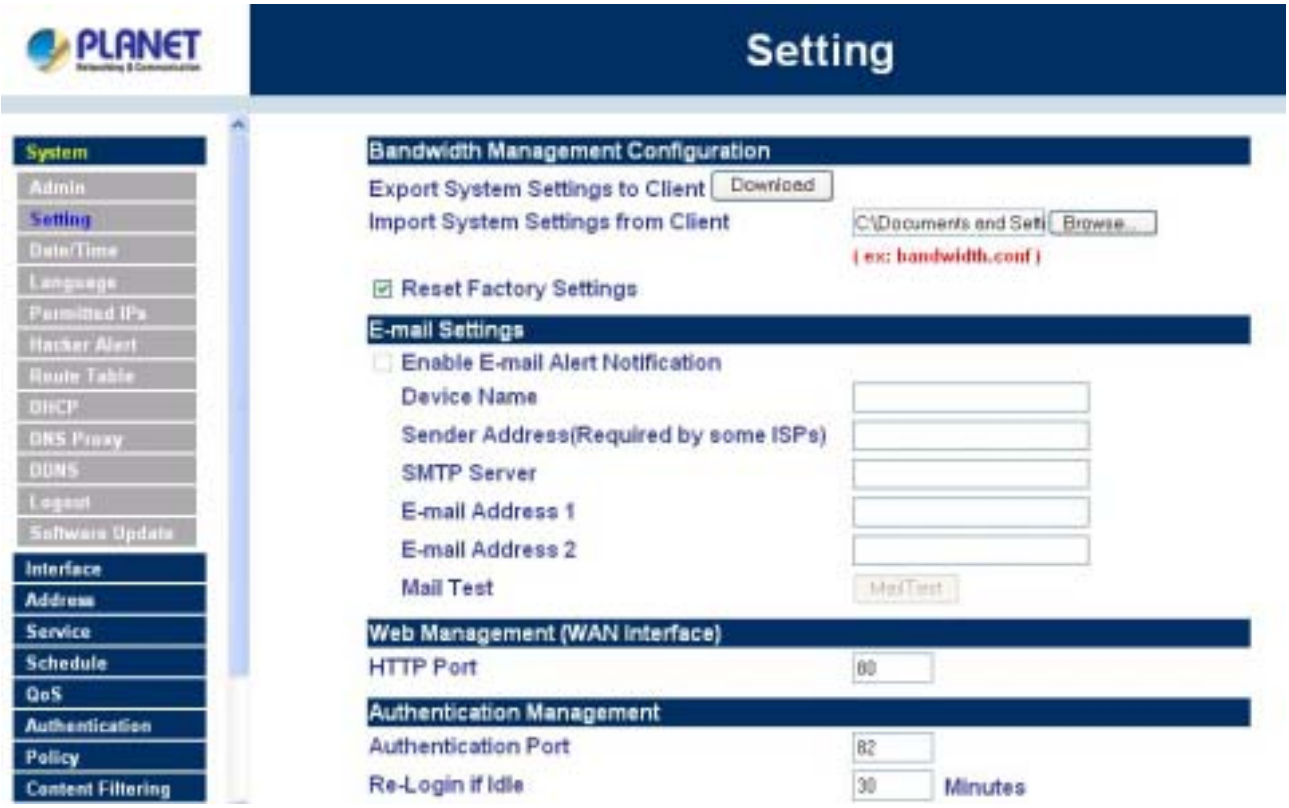
Click **OK** to import the file into the **Multi-Homing Security Gateway** or click **Cancel** to cancel importing.



Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Configuration**.

Click **OK** at the bottom-right of the screen to restore the factory settings.



Enabling E-mail Alert Notification

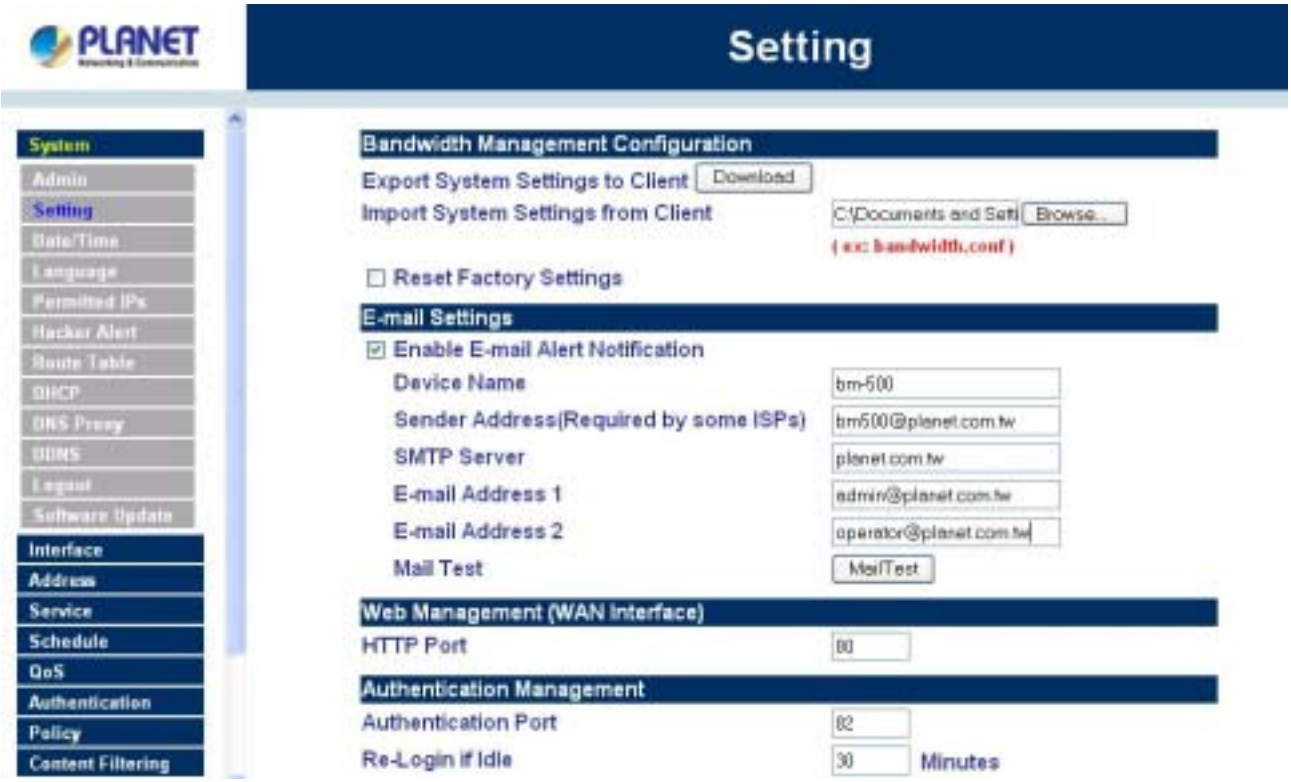
Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Multi-Homing Security Gateway to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Click **OK** on the bottom-right of the screen to enable E-mail alert notification.



Web Management (WAN Interface) (Remote UI Management)

The administrator can change the port number used by HTTP port1 anytime. (Remote UI Management)

Step 1. **Set Web Management (WAN Interface).** The administrator can change the port number used by HTTP port anytime.

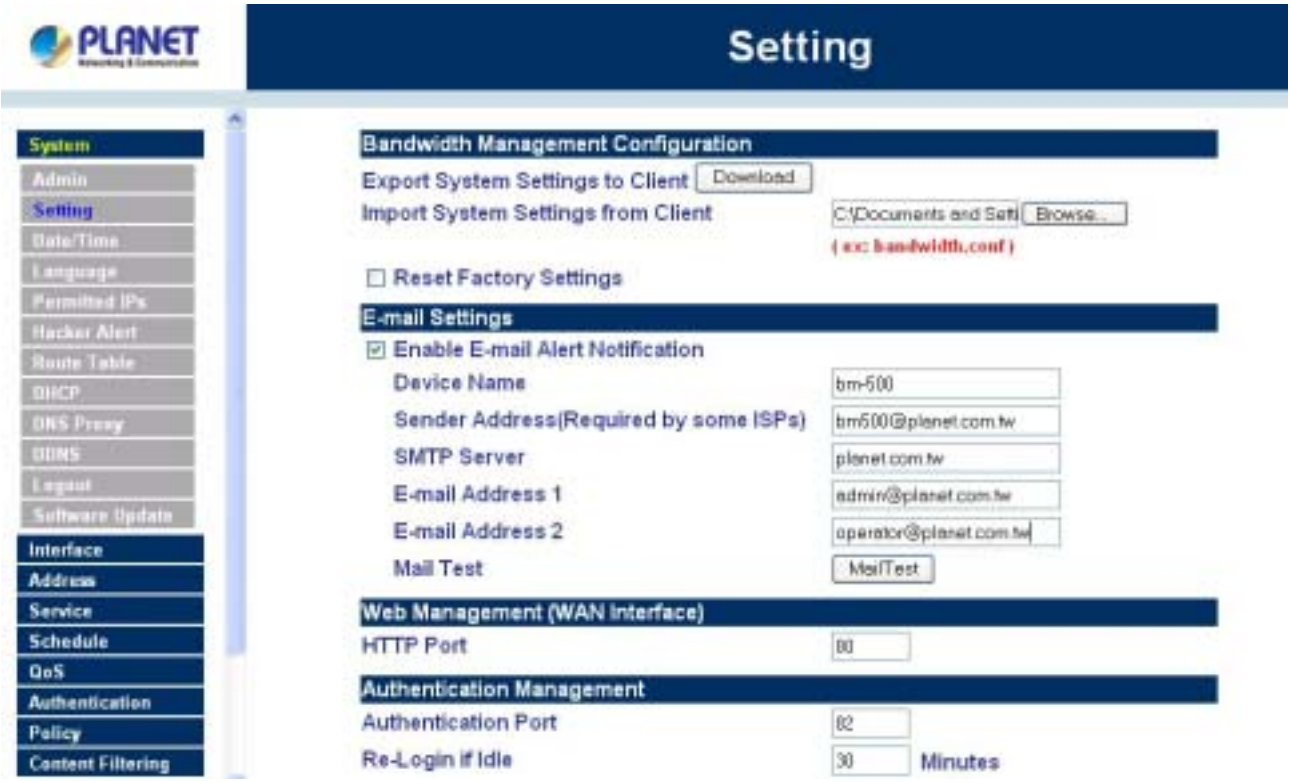
Authentication

The administrator can specify the port number and authentication time of authentication management system for LAN user to access WAN network. (Needs to setup authentication table in advance. This option is only available on MH-4000)

Authentication functions:

Authentication Port: The port number used for user login page. When user want to access WAN network and the authentication (Policy -> Outgoing) is enabled, the user has to send http request with this port number. The Multi-Homing Security Gateway will send a User Login page for user to input user name and password. For example, if the gateway IP address is 192.168.1.1 and authentication port is 82, user have to open a web browser and input http://192.168.1.1:82 on the address file to have the user login page.

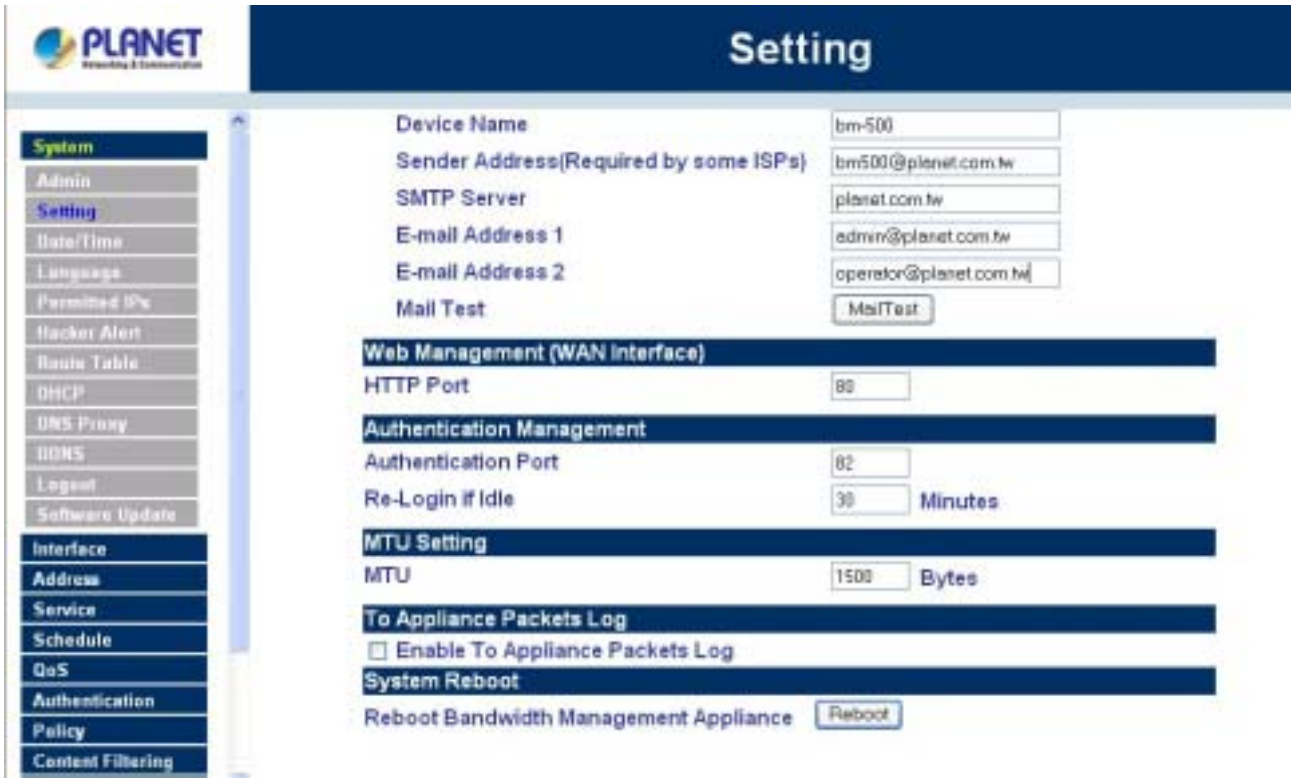
Re-Login if Idle: When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "System"-> "Setting" page.



MTU (set networking packet length)

The administrator can modify the networking packet length.

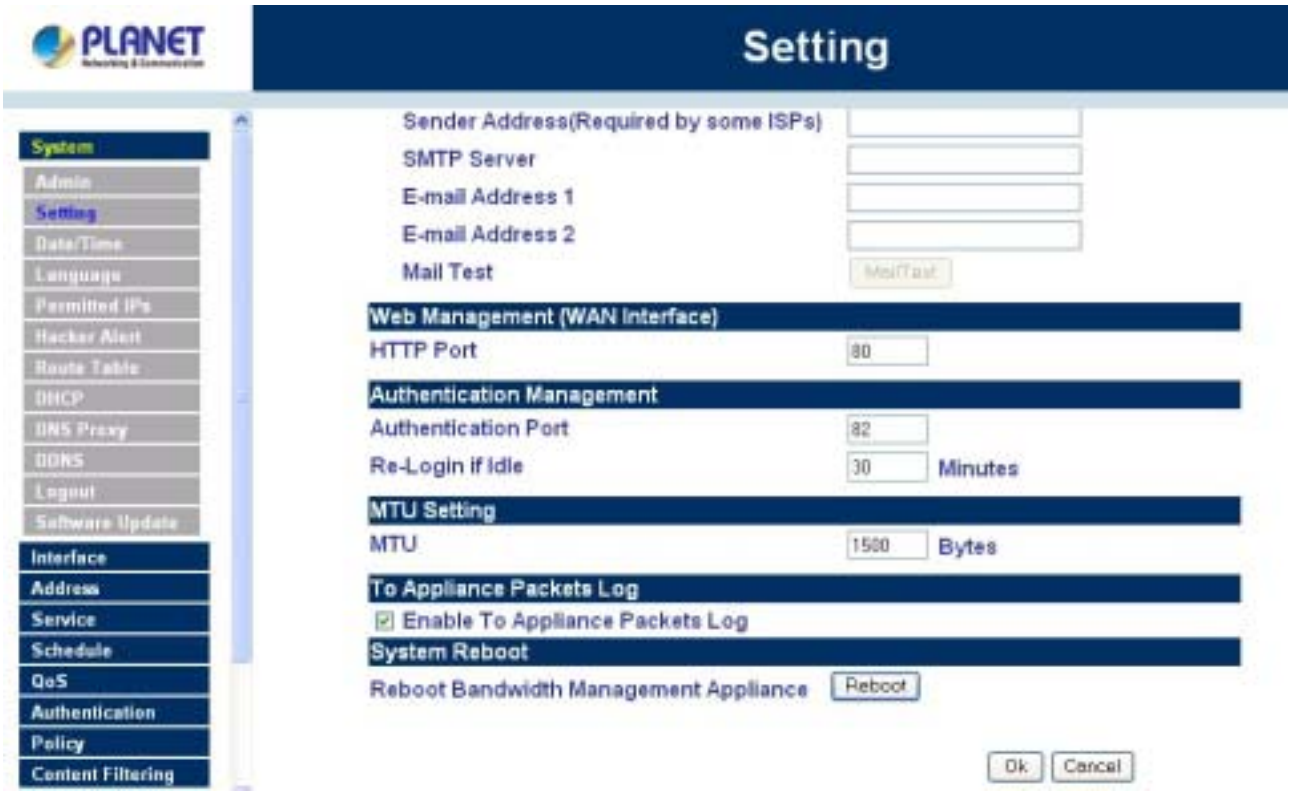
Step 1. **MTU Setting.** Modify the networking packet length.



To-Appliance Packets Log

Once this function is enabled, every packet to this appliance will be recorded for the administrator to trace.

Step 1. Select this option to the device's **To-Appliance Packets Log.** Once this function is enabled, every packet to this appliance will be recorded for system administrator to trace.

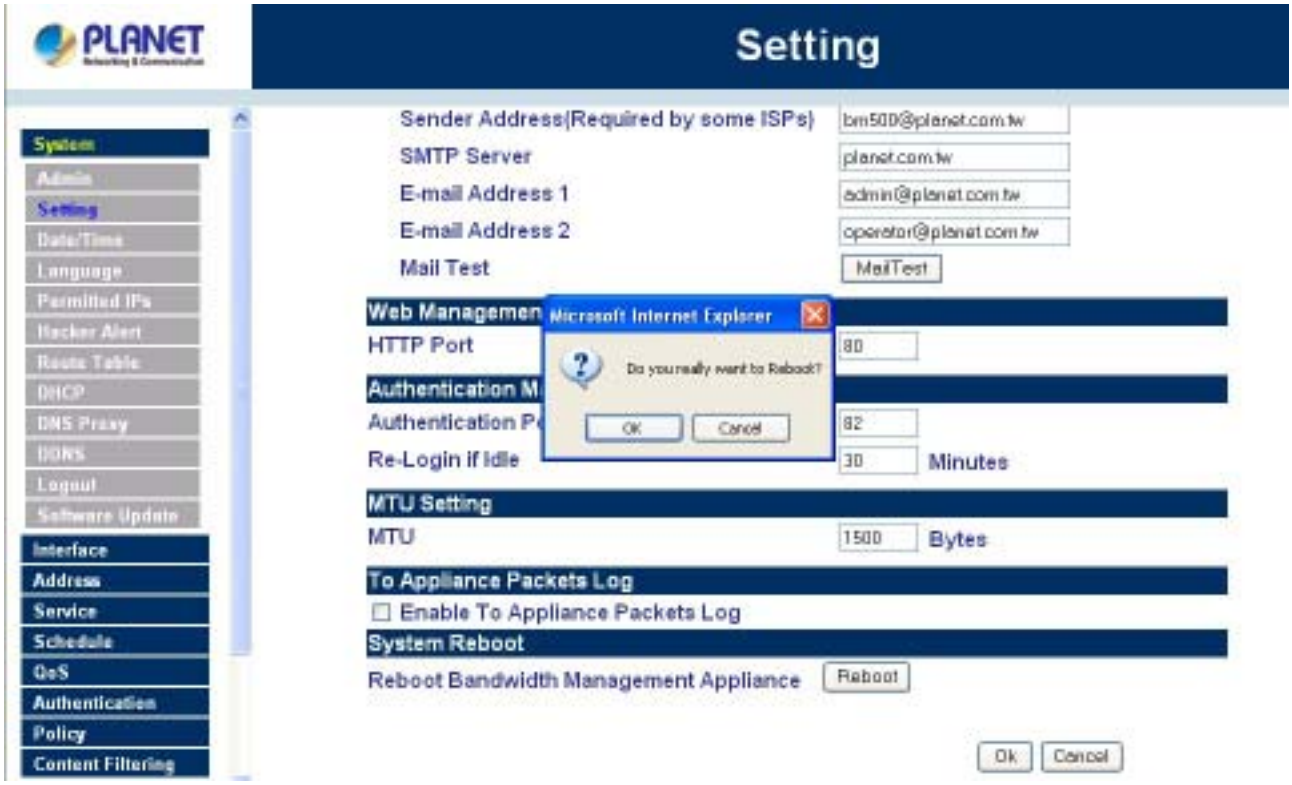


System Reboot

Once this function is enabled, the Multi-Homing Security Gateway will be rebooted**.**

Reboot Appliance: Click **Reboot.**

A confirmation pop-up box will appear. Follow the confirmation pop-up box, click **OK** to restart Multi-Homing Security Gateway or click **Cancel** to discard changes



4.1.3 Date/Time

Synchronizing the Multi-Homing Security Gateway with the System Clock

Administrator can configure the Multi-Homing Security Gateway's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

Follow these steps to sync to an Internet Time Server

Step 1. Enable synchronization by checking the box.

Step 2. Click the down arrow to select the offset time from GMT.

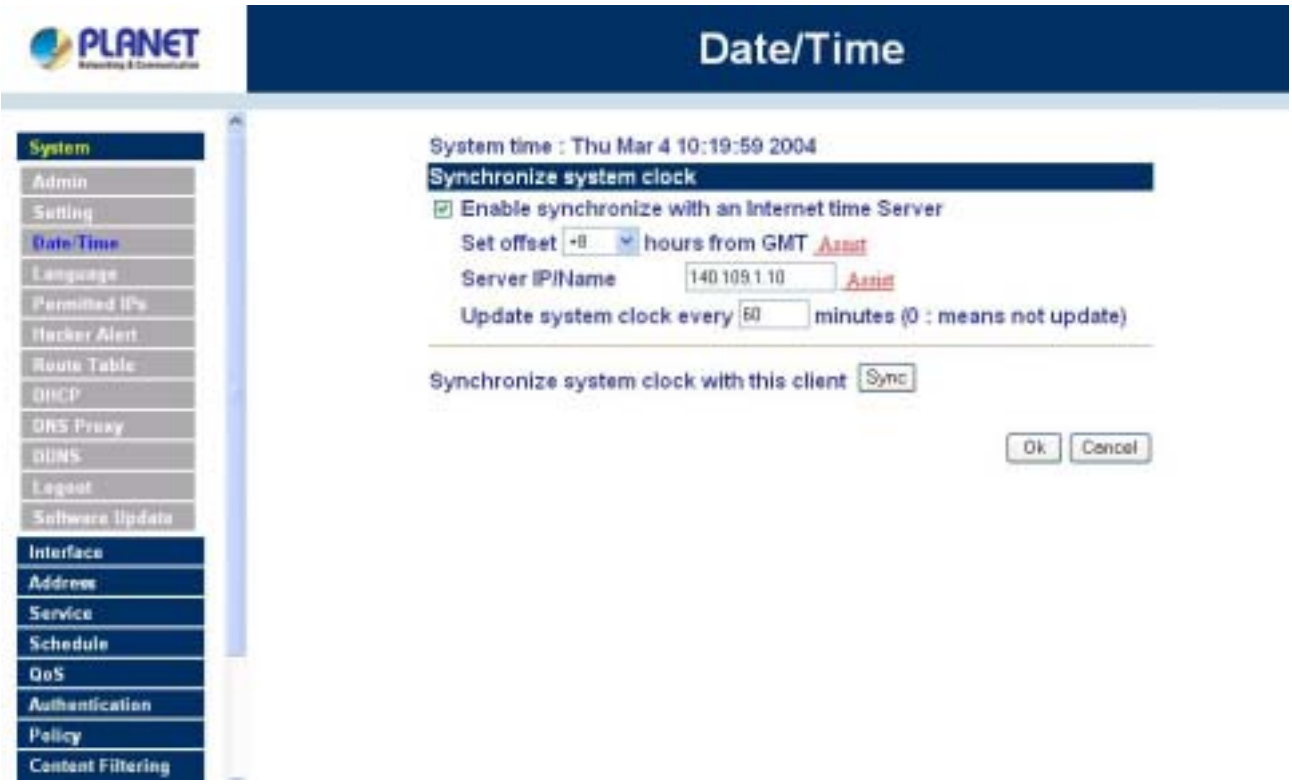
Step 3. Enter the Server IP Address or Server name with which you want to synchronize.

Step 4. **Update system clock every 5 minutes** You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer s clock.

Step 1. Click on the **Sync** button.

Click **OK** to apply the setting or click **Cancel** to discard changes.



4.1.4 Multiple Subnet

NAT mode

Multiple Subnet allows local port to set multiple subnet works and connect with the internet through different WAN 1 IP Addresses.

For instance: The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet works for the purpose of convenient management. The settings are as the following:

1. R&D department sub-network: 192.168.1.11/24(LAN) ←→ 168.85.88.253(WAN 1)
2. Service department sub-network: 192.168.2.11/24(LAN) ←→ 168.85.88.252(WAN 1)
3. Sales department sub-network: 192.168.3.11/24(LAN) ←→ 168.85.88.251(WAN 1)
4. Procurement department sub-network: 192.168.4.11/24(LAN) ←→ 168.85.88.250(WAN 1)
5. Accounting department sub-network: 192.168.5.11/24(LAN) ←→ 168.85.88.249(WAN 1)

The first department(R&D department) was set while setting interface IP, the other four ones have to be added in Multiple Subnet, after completing the settings, each department use the different WAN IP Address to

connect to the internet. The settings of LAN computers on service department are as the following

Service IP Address: 192.168.2.1

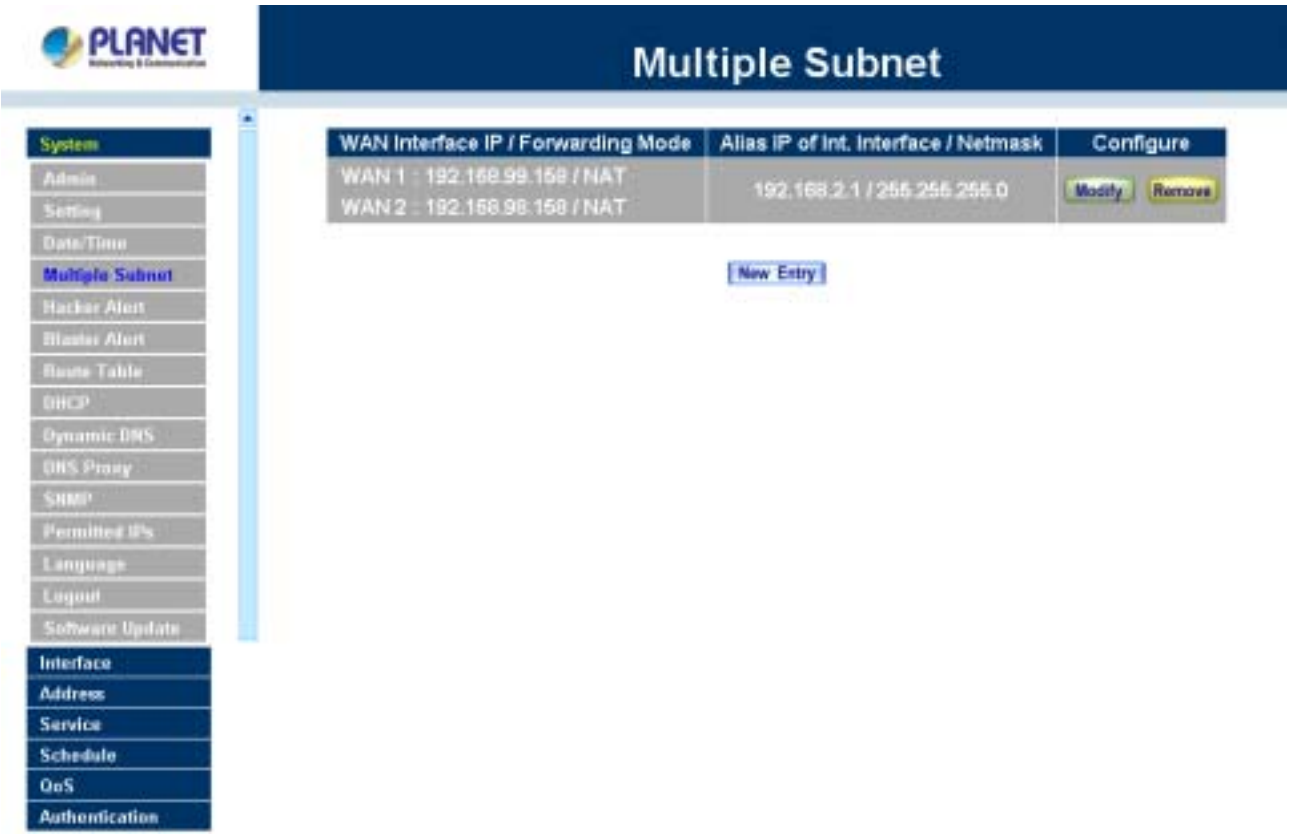
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.11

The other departments are also set by groups, this is the function of Multiple Subnet.

Multiple Subnet settings

Click Multiple Subnet in the System menu to enter Multiple Subnet window.



Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP Address and Forwarding Mode.

Alias IP of Int. Interface / Netmask: Local port IP Address and subnet Mask.

Configure: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click Delete to delete settings.

Add a Multiple Subnet NAT Mode.

Step 1: Click the **New Entry** button below to add Multiple Subnet.

Step 2: Enter the IP Address in the website name column of the new window.

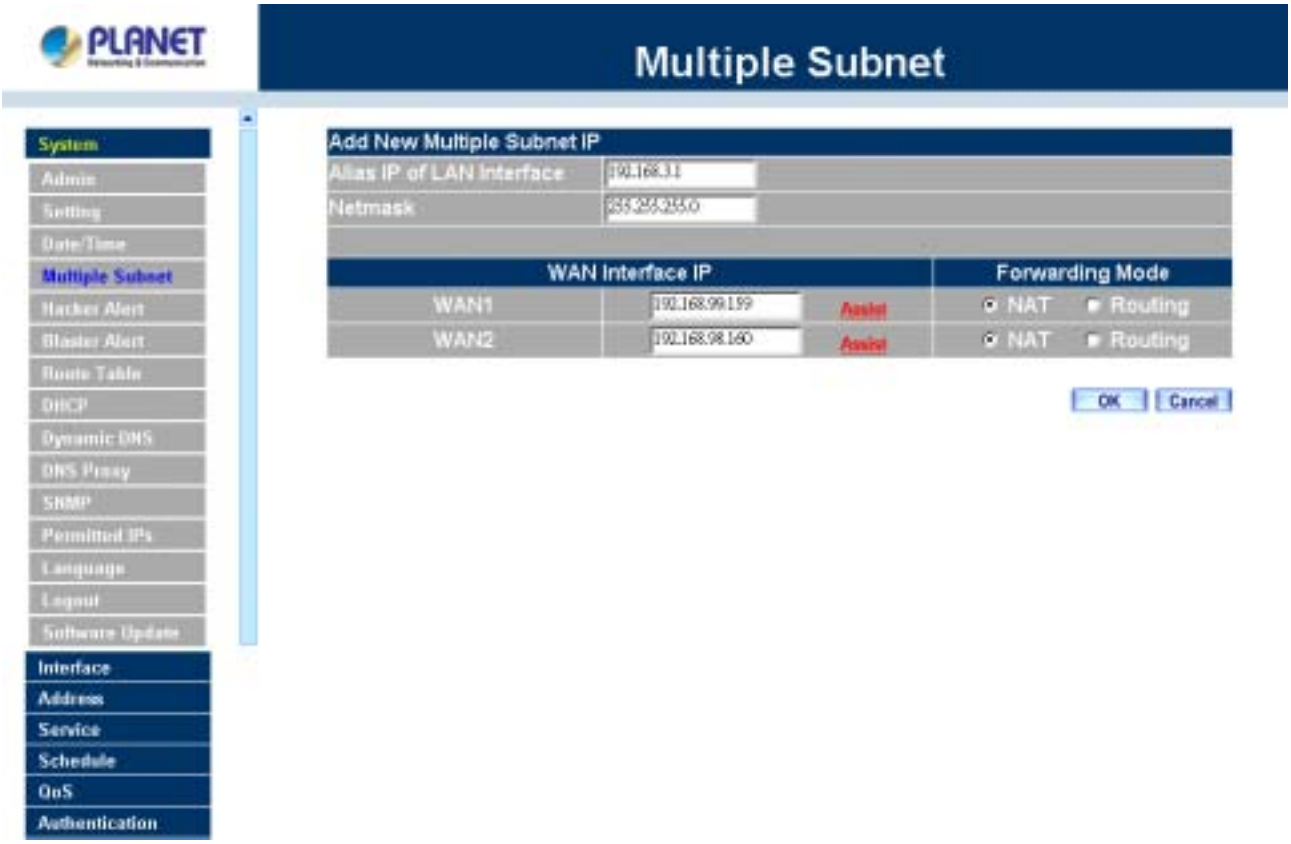
Alias IP of LAN Interface: Enter Local port IP Address.

Netmask: Enter Local port subnet Mask.

WAN Interface IP: Add WAN 1 or WAN 2 IP.

Forwarding Mode: Click the NAT button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.

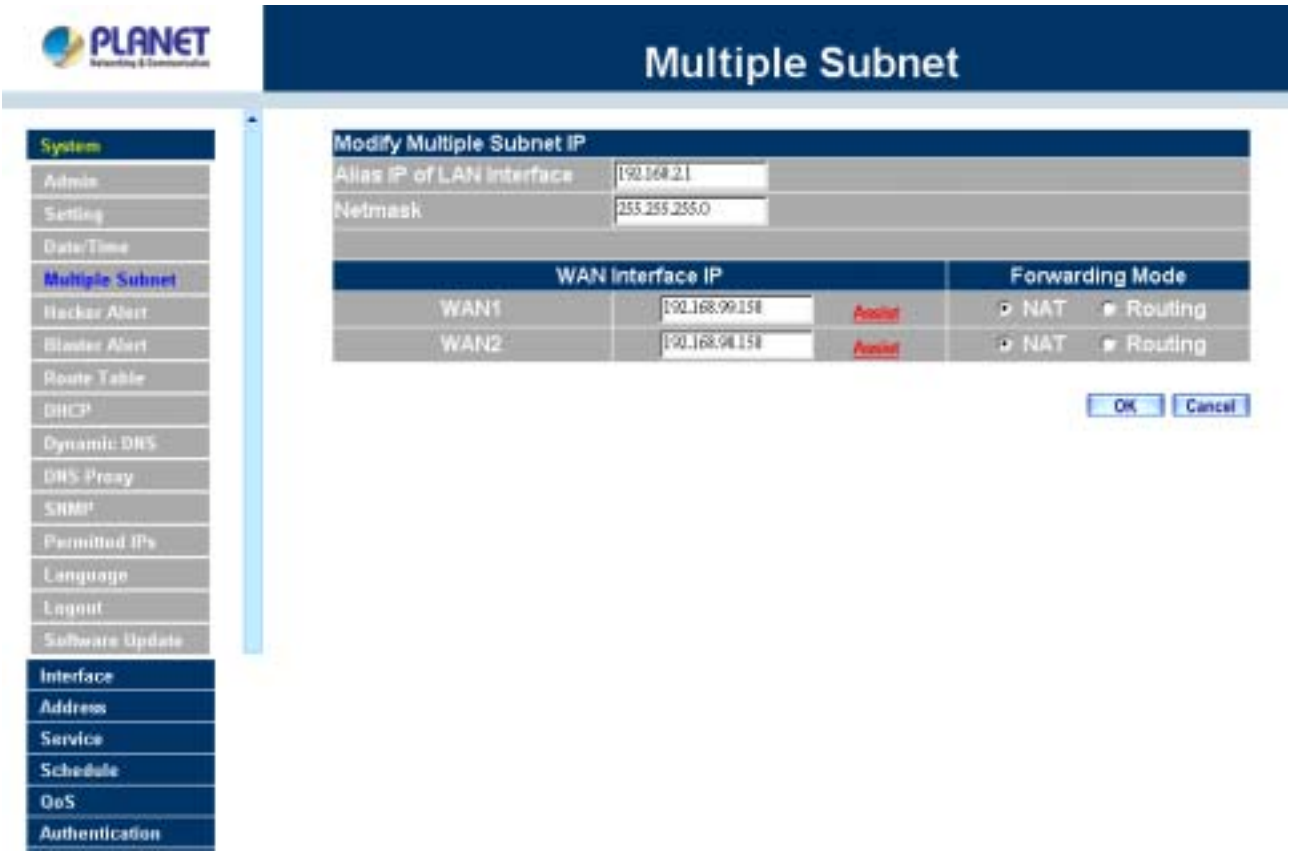


Modify a Multiple Subnet

Step 1: Find the IP Address you Want to modify and click Modify.

Step 2: Enter the new IP Address in Modify Multiple Subnet window.

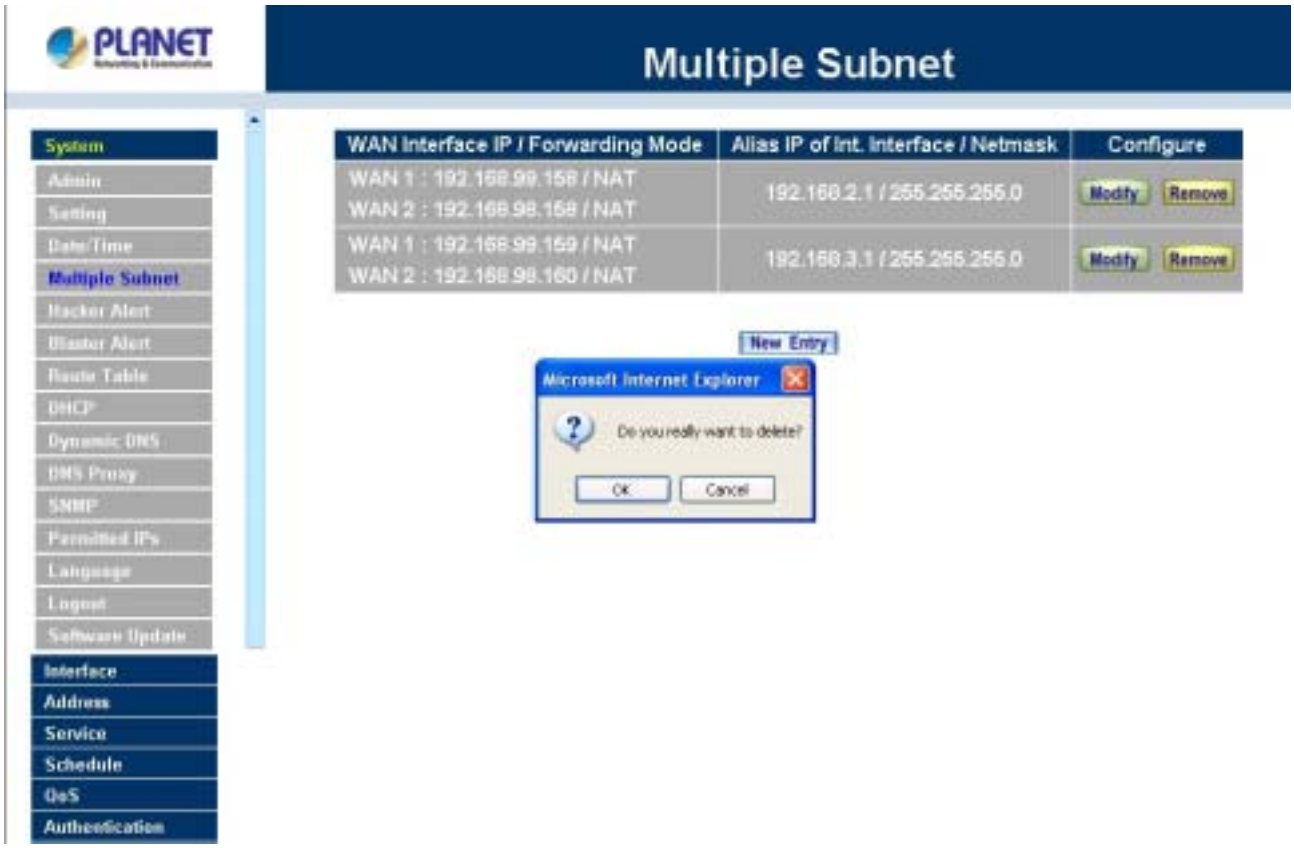
Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



Removing a Multiple Subnet

Step 1: Find the IP Address you want to delete and click Delete.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



Routing Mode

Multiple Subnet allows local port to set Multiple Subnet Routing Mode and connect with the internet through different WAN IP Addresses.

For example, the leased line of a company applies several real IP Addresses 168.85.88.0/24 and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. The company can distinguish each department by different sub-network for the purpose of convenient management.

The settings are as the following:

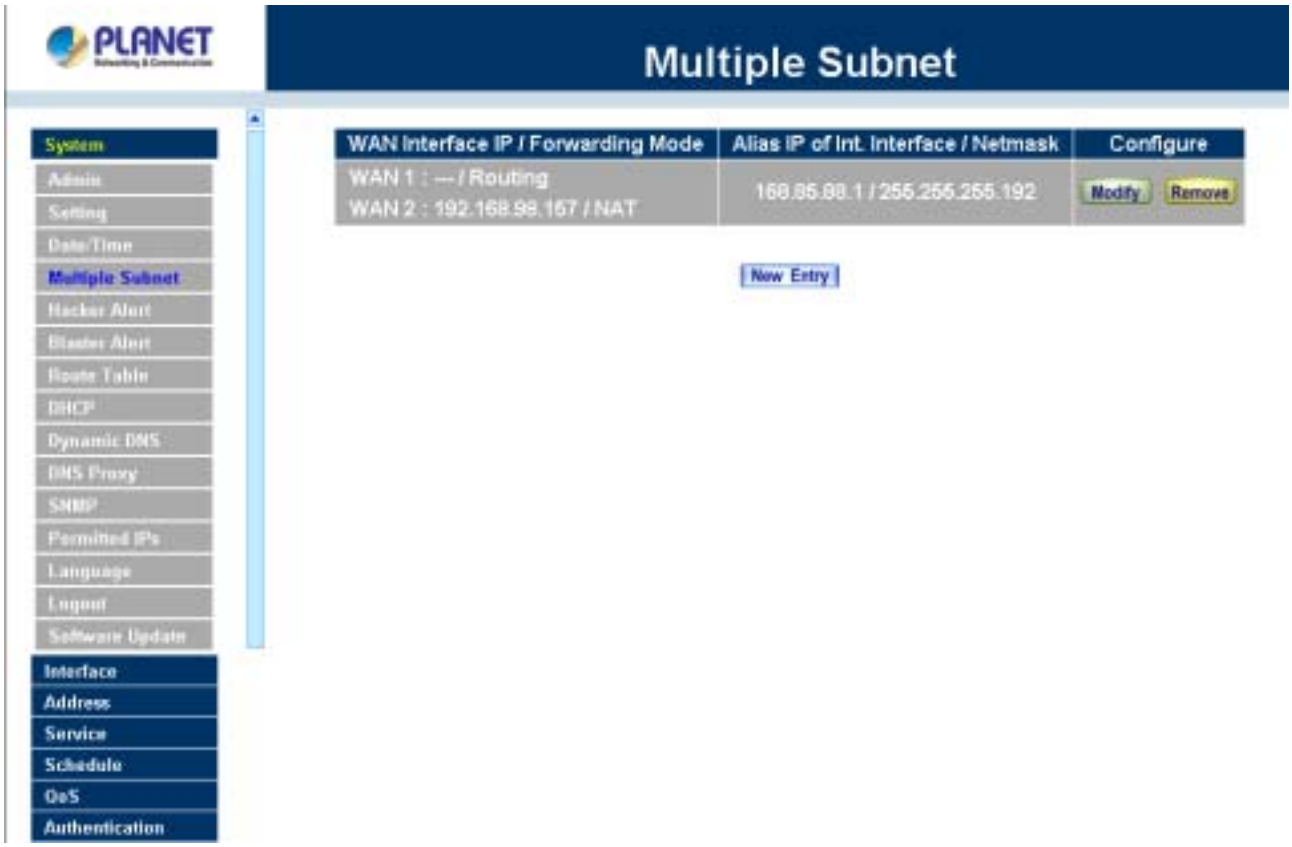
R&D: Alias IP of LAN interface - 168.85.88.1, Netmask: 255.255.255.192

Sales: Alias IP of LAN interface - 168.85.88.65, Netmask: 255.255.255.192

Procurement: Alias IP of LAN interface - 168.85.88.129, Netmask: 255.255.255.192

Accounting: Alias IP of LAN interface - 168.85.88.193, Netmask: 255.255.255.192

Click System Configuration on the left side menu bar, then click Multiple Subnet below it. Enter Multiple Subnet window.



Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP Address and Forwarding Mode which is NAT Mode or Routing Mode.

Alias IP of Int. Interface / Subnet Mask: Local port IP Address and subnet Mask.

Modify: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click **Remove** to delete settings.

Adding a Multiple Subnet Routing Mode

Step 1: Click the Add button below to add Multiple Subnet.

Step 2: Enter the IP Address in Add Multiple Subnet window.

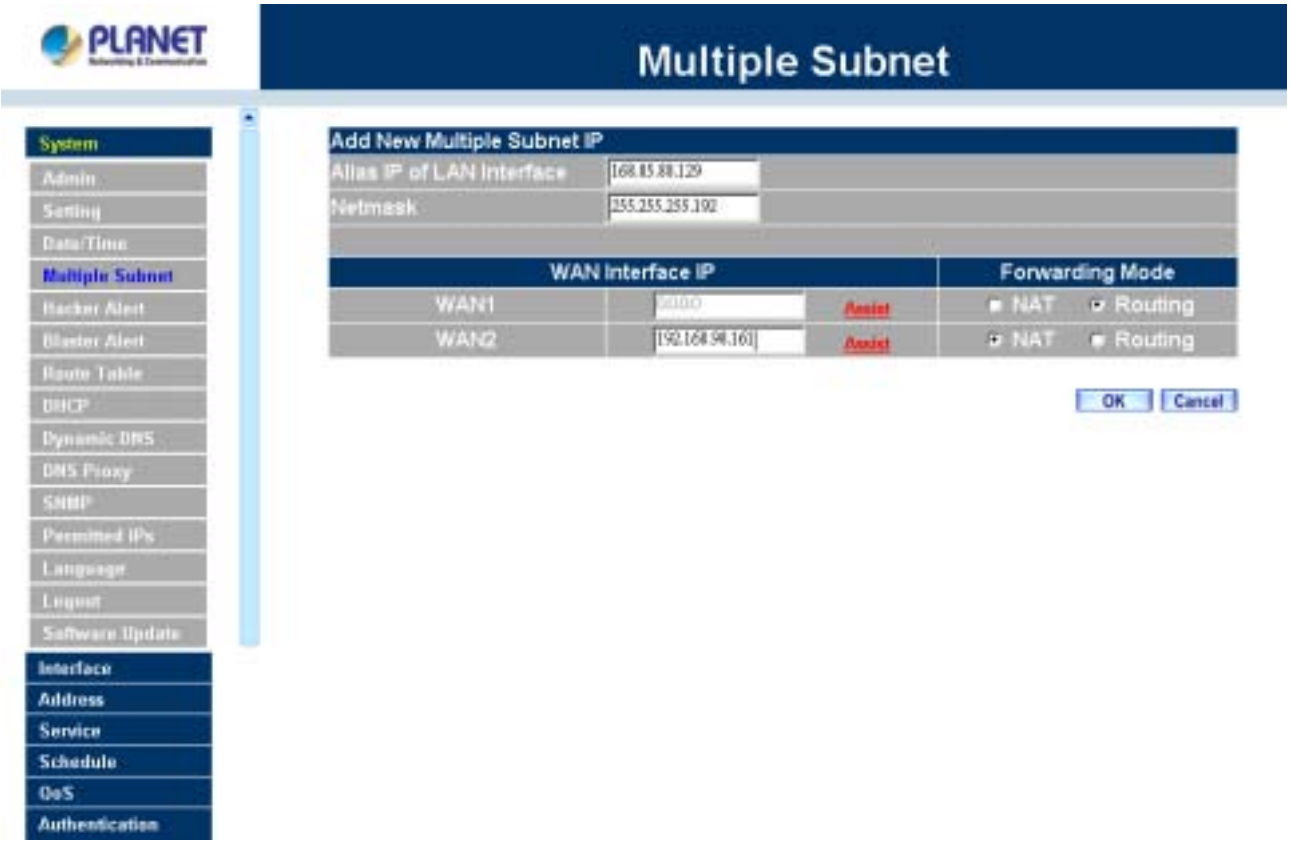
Alias IP of LAN Interface: Enter Local port IP Address.

Netmask: Enter Local port subnet Mask.

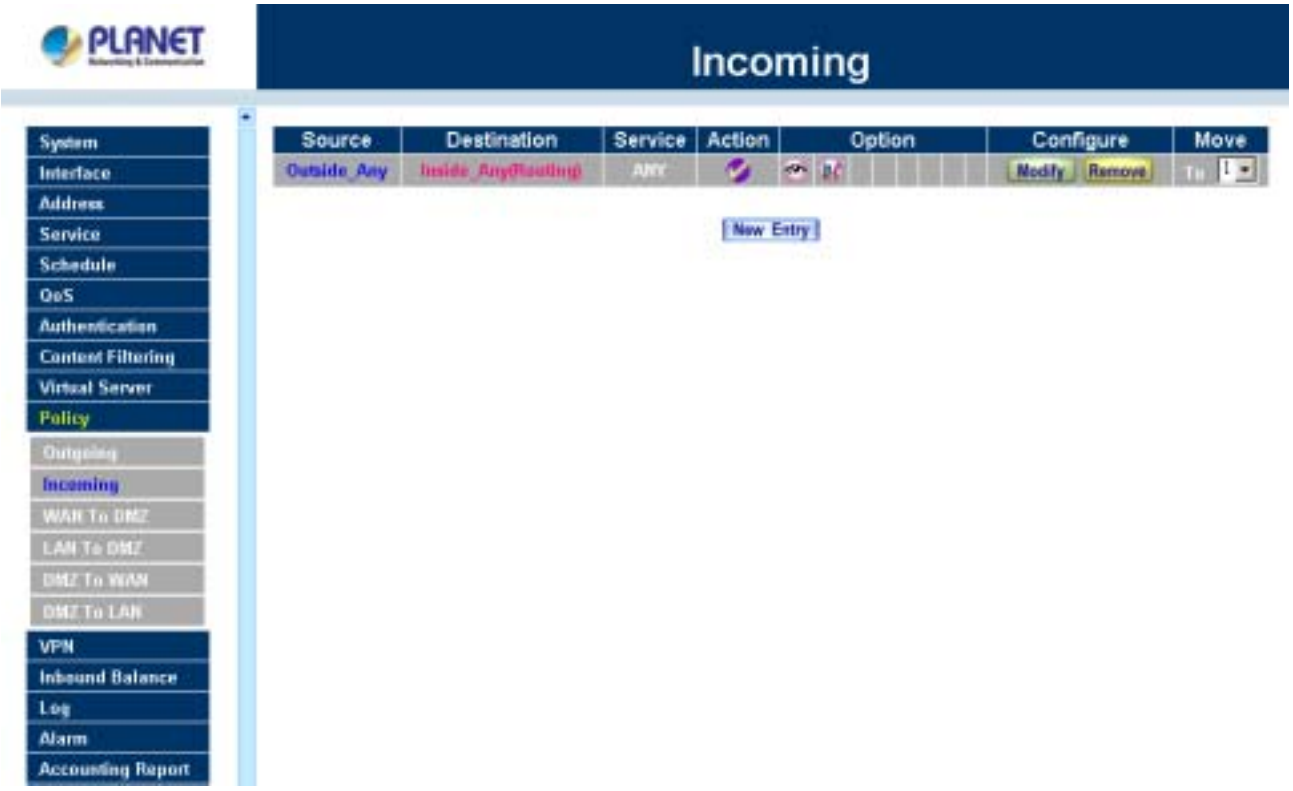
WAN Interface IP: Add WAN1 or WAN2 IP

Forwarding Mode: Click the Routing button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.



Step 4: Adding a new WAN to LAN Policy. In the Incoming window, click the New Entry button.

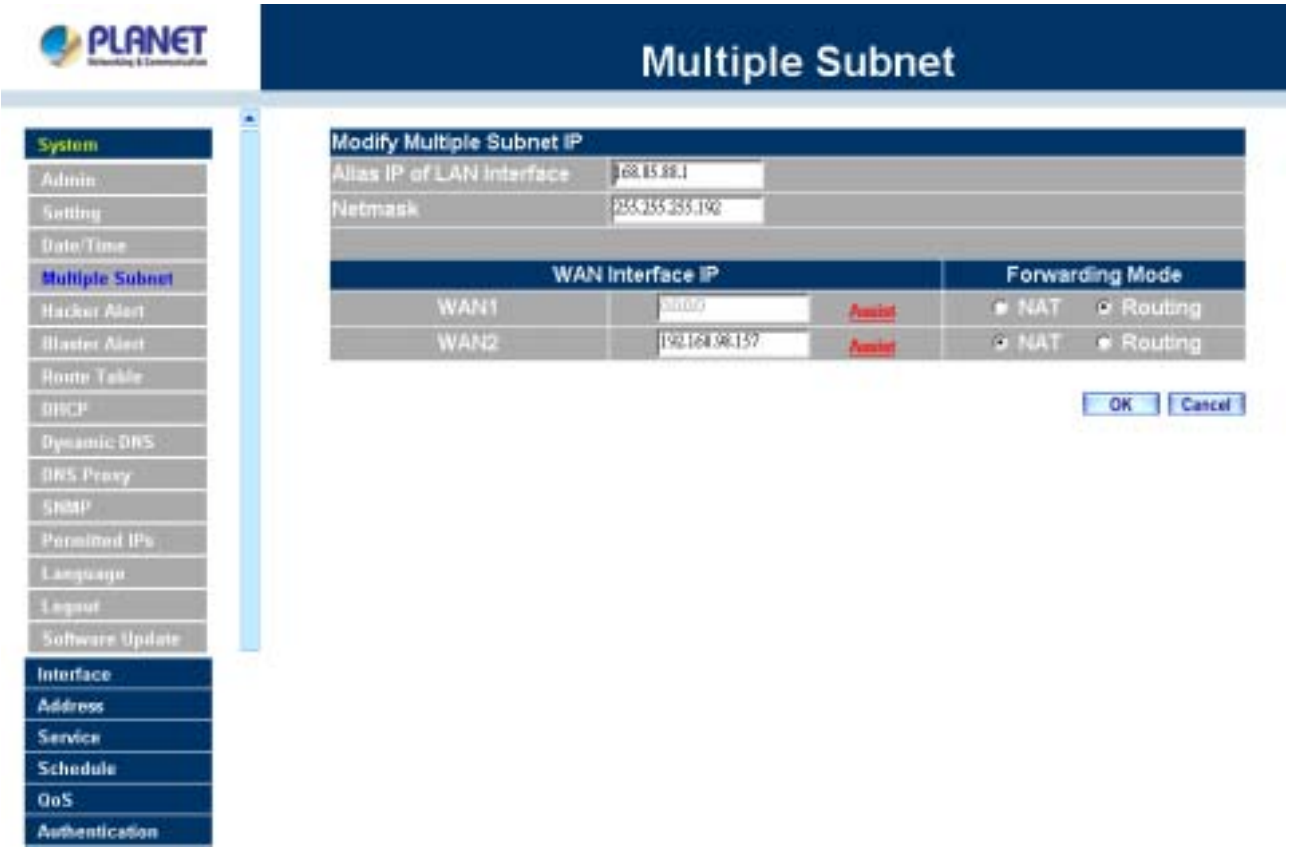


Modify a Multiple Subnet Routing Mode

Step 1: Find the IP Address you want to modify in Multiple Subnet menu, then click Modify button, on the right side of the service providers, click OK.

Step 2: Enter the new IP Address in Modify Multiple Subnet window.

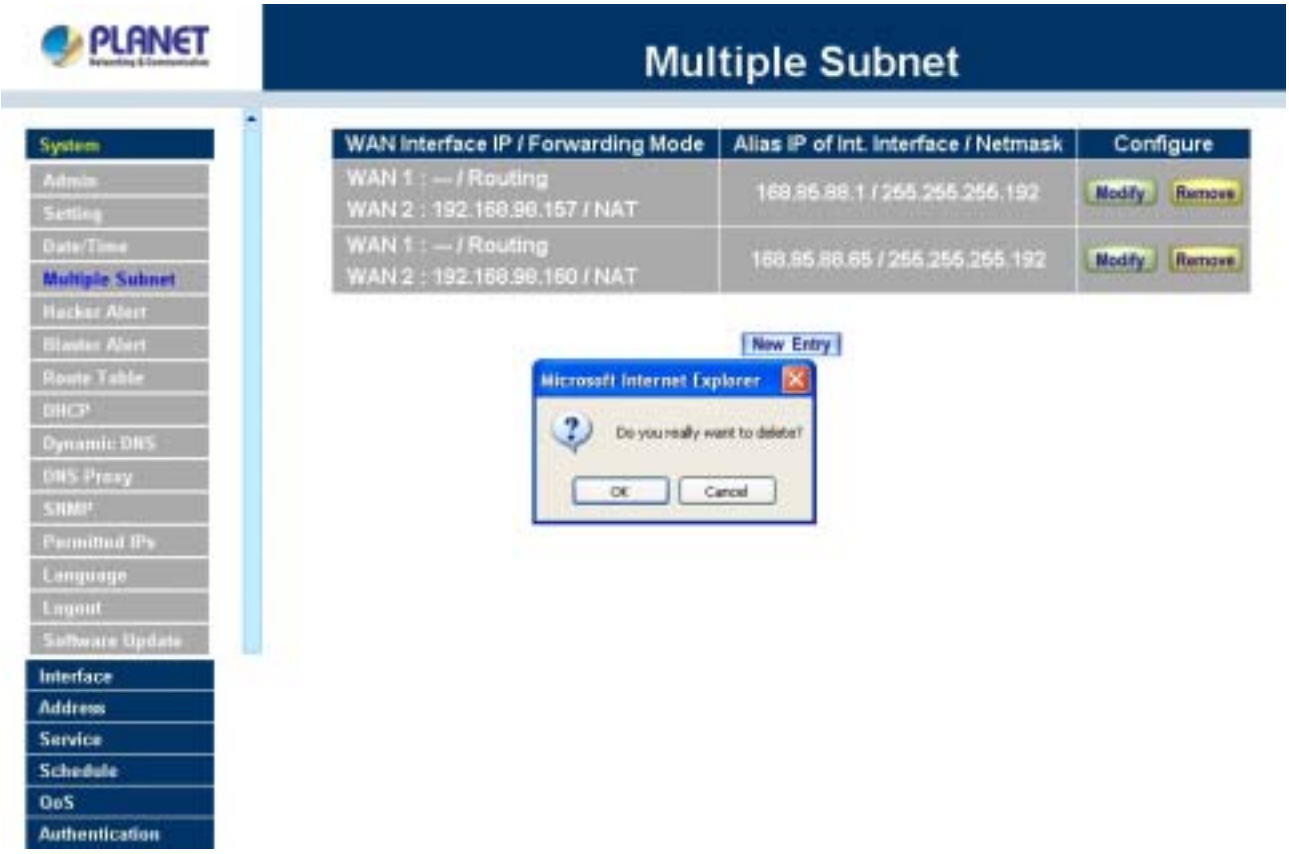
Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



Removing a Multiple Subnet Routing Mode

Step 1: Find the IP Address you want to delete in Multiple Subnet menu, then click Delete button, on the right side of the service providers, click OK.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



4.1.5 Hacker Alert

The Administrator can enable the device's auto detect functions for hacker attacking this section. When abnormal conditions occur, the Multi-Homing Security Gateway will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Auto Detect functions

- **Detect SYN Attack**: Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will prevent valid users from connecting to the servers. After enabling this function, the System Administrator can enter the number of SYN packets per second that is allowed to enter the network/Multi-Homing Security Gateway. Once the SYN packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default SYN flood threshold is set to 200 Pkts/Sec .

- **Detect ICMP Flood**: Select this option to detect ICMP flood attacks. When hackers continuously send PING packets to all the machines of the LAN networks or to the Multi-Homing Security Gateway, your network is experiencing an ICMP flood attack. This can cause traffic congestion on the network and slows the network down. After enabling this function, the System Administrator can enter the number of ICMP packets per second that is allowed to enter the network/Multi-Homing Security Gateway. Once the ICMP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default ICMP flood threshold is set to 1000 Pkts/Sec.

- **Detect UDP Flood**: Select this option to detect UDP flood attacks. A UDP flood attack is similar to an ICMP flood attack. After enabling this function, the System Administrator can

enter the number of UDP packets per second that is allow to enter the network/Multi-Homing Security Gateway. Once the UDP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default UDP flood threshold is set to 1000 Pkts/Sec .

- **Detect Ping of Death Attack**: Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.
- **Detect Tear Drop Attack**: Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.
- **Detect IP Spoofing Attack**: Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the Multi-Homing Security Gateway System and invade the network.
- **Filter IP Source Route Option**: Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade LAN networks and send LAN networks' data back to them.
- **Detect Port Scan Attack**: Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.
- **Detect Land Attack**: Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when SYN on the TCP header is marked.
  Enable this function to detect such abnormal packets.
- **Default Packet Deny**: Denies all packets from passing the Multi-Homing Security Gateway. A packet can pass only when there is a policy that allows it to pass.

After enabling the needed detect functions, click OK to activate the changes.

4.1.6 Blaster Alert (MH-4000 only)

The Administrator can enable the device's auto detect functions for blaster worm attacking the local network. When abnormal conditions occur, the Multi-Homing Security Gateway will send an e-mail alert and/or SNMP

trap to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

NOTE: This function is not supported on MH-2000.

Blaster Alerts Settings

- **Enable Blaster Blocking**: Select this option to enable the blaster blocking function. ONice the blaster worm is detected, it will block the TCP port 135 for user-drefined blocking time.
- **Enable E-mail Alert Notification:** When Blaster worm is detected, send alert e-mail to administrator by using e-mail address defined on System -> Setting.
- **Enalbe SNMP Trap Alert Notification:** When Blaster worm is detected, send SNMP trap to user-defined SNMP trap receiver IP address defined on System -> SNMP.

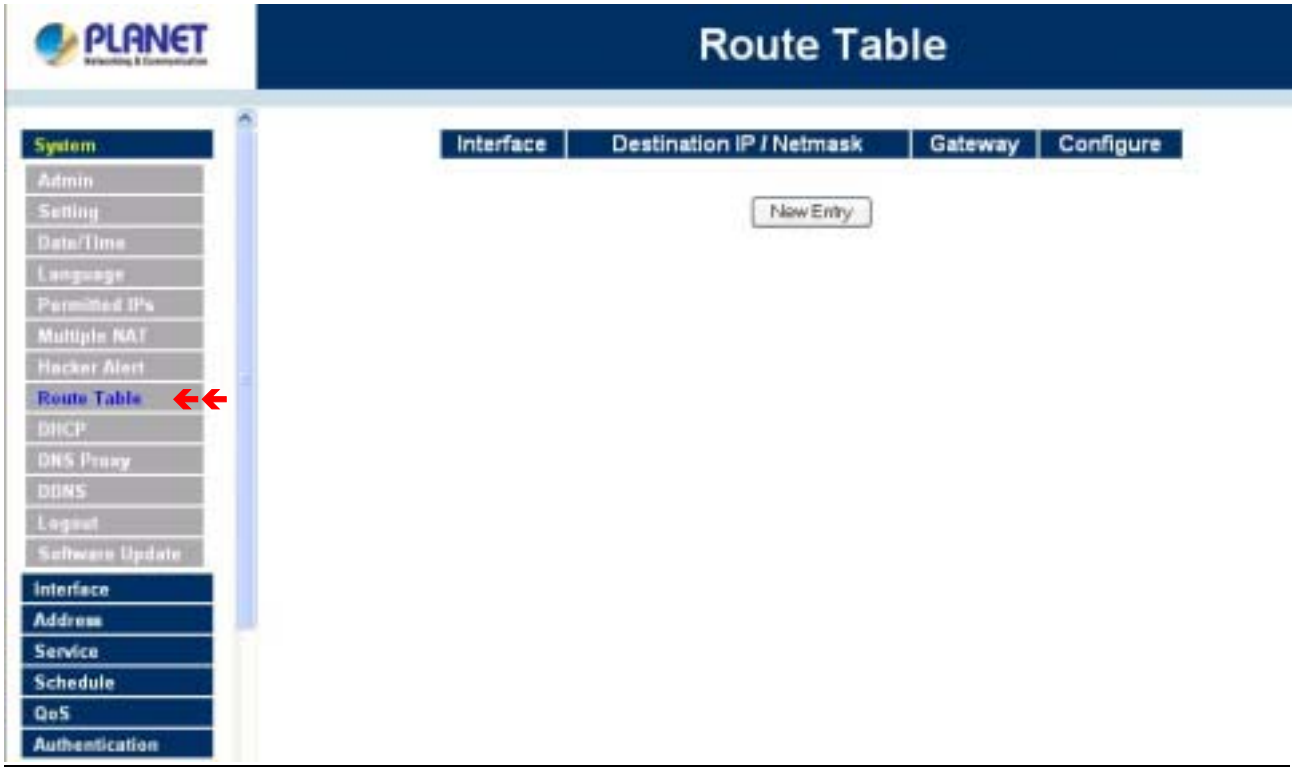
After enabling the needed options, click OK to activate the changes.

4.1.7 Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen

Step 1. Click **System** on the left side menu bar, then click **Route Table** below it. The Route Table window appears, in which current route settings are shown.



Route Table functions

- **Interface:** Destination network, LAN or WAN 1 networks.
- **Destination IP:** IP address of destination network.
- **NetMask:** Netmask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

Adding a new Static Route

Step 1. In the Route Table window, click the **New Entry** button.

Step 2. In the Add New Static Route window, enter new static route information.

Step 3. In the Interface field's pull-down menu, choose the network to connect (LAN, WAN1, WAN2, DMZ).

Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.

Modifying a Static Route:

Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the Configure field.

Step 2. In the **Modify Static Route** window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

Removing a Static Route

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

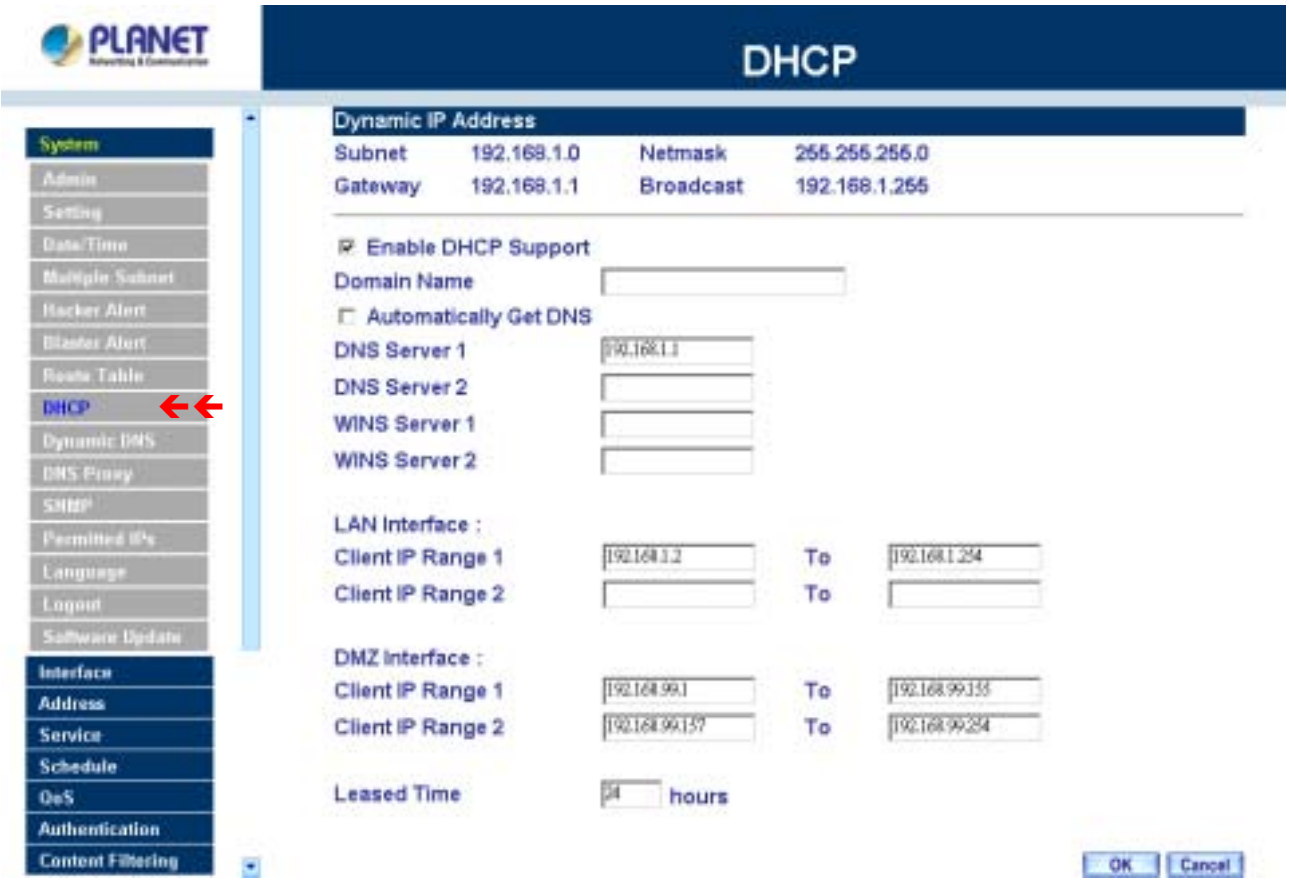
Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.

4.1.8 DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Entering the DHCP window

Click **System** on the left hand side menu bar, then click **DHCP** below it. The DHCP window appears in which current DHCP settings are shown on the screen.



Dynamic IP Address functions

- **Subnet:** LAN network's subnet
- **NetMask:** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

Enabling DHCP Support

Step 1. In the Dynamic IP Address window, click **Enable DHCP Support**.

Domain Name: The Administrator may enter the name of the LAN network domain if preferred.

Automatically Get DNS: Check this box to automatically detect DNS server.

DNS Server 1 : Enter the distributed IP address of DNS Server 1.

DNS Server 2 : Enter the distributed IP address of DNS Server 2.

WINS Server 1 : Enter the distributed IP address of WINS Server 1.

WINS Server 2 : Enter the distributed IP address of WINS Server 2.

LAN interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

DMZ interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

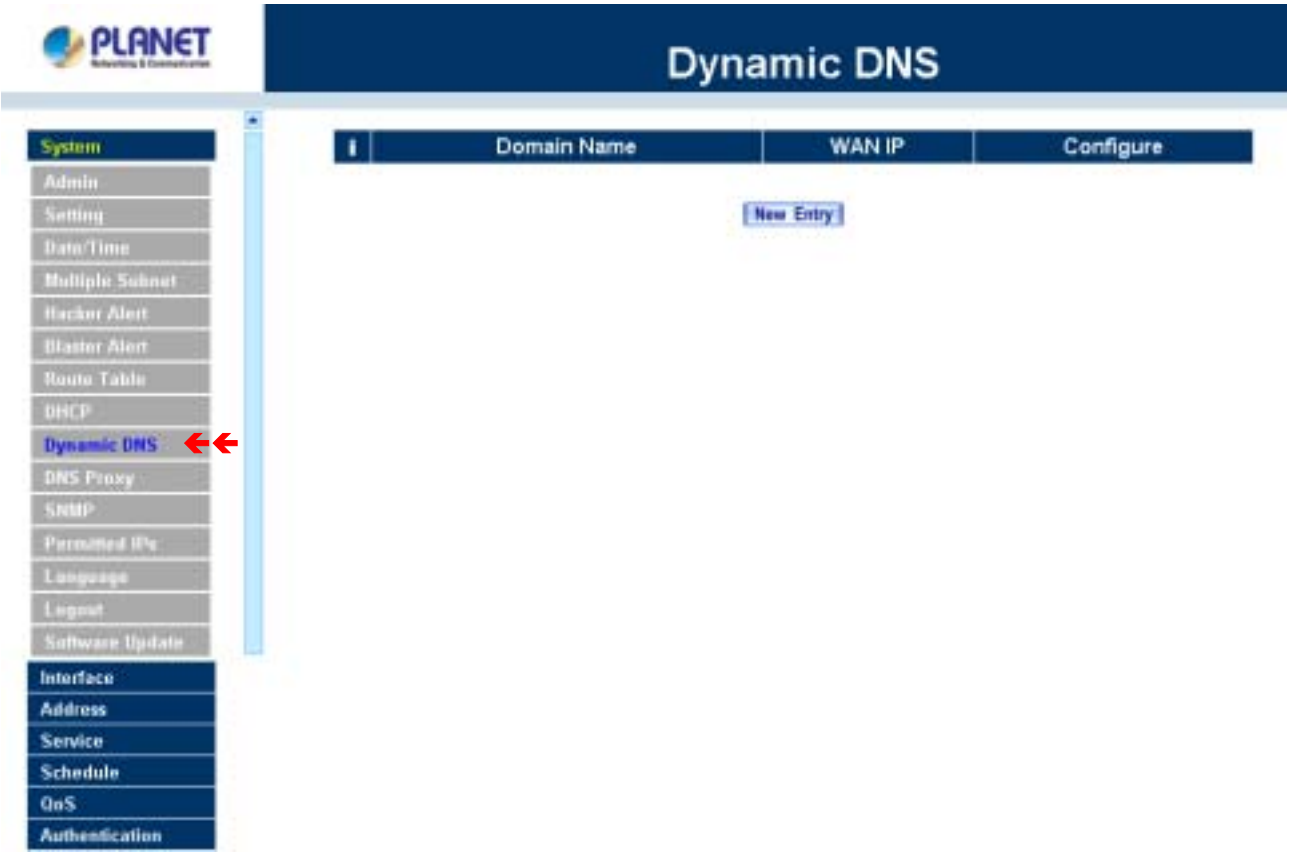
Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Leased Time: Enter the leased time for DHCP.

Step 2. Click **OK** to enable DHCP support.

4.1.9 Dynamic DNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.



Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

The icons in Dynamic DNS window:

!: Update Status, Connecting; Update succeed; Update fail; Unidentified error.

Domain name: Enter the password provided by ISP.

WAN IP Address: IP Address of the WAN port.

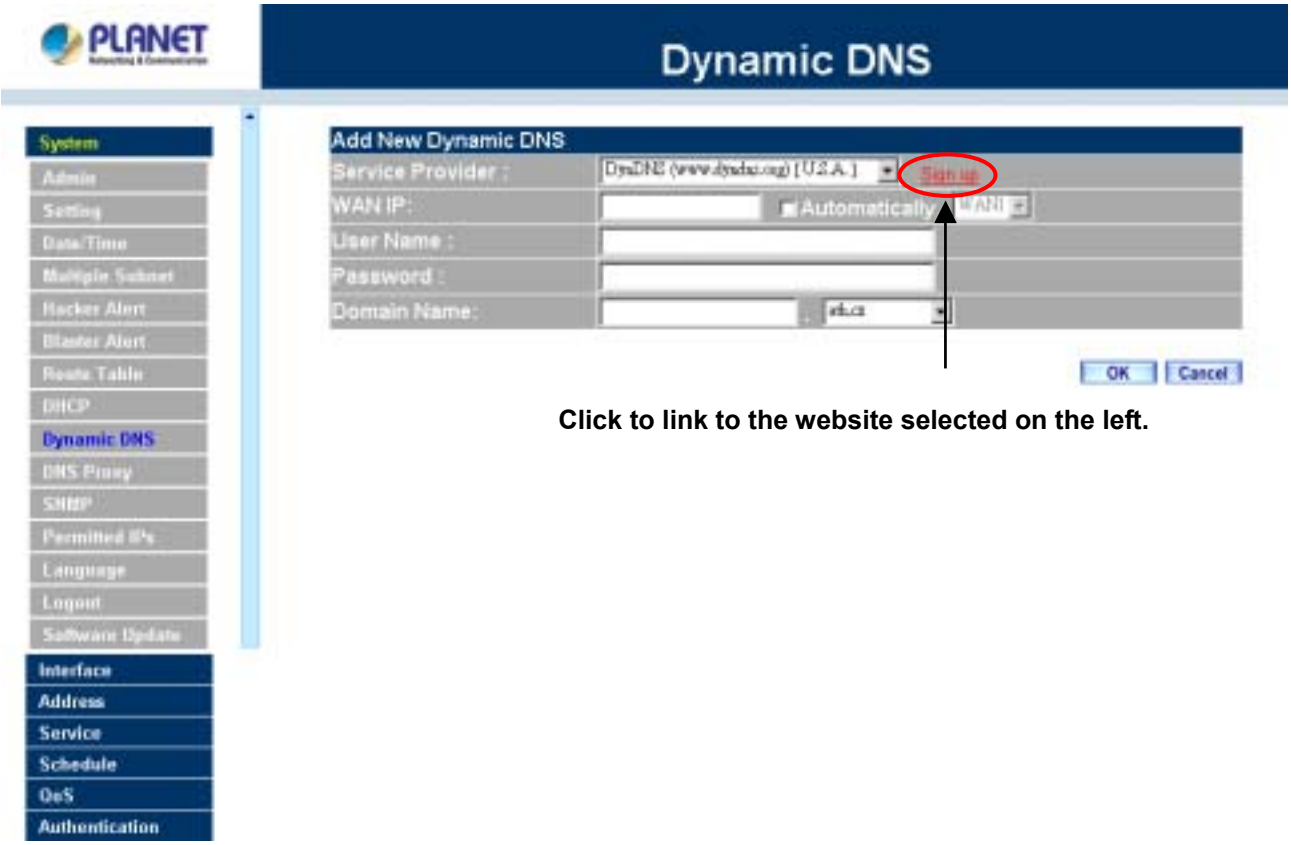
Configure: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

How to use dynamic DNS:

The Multi-Homing Security Gateway provides many service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

How to register:

Firstly, Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window, then click **Add** button, on the right side of the service providers, click **Register**, the service providers' website will appear, please refer to the website for the way of registration.



Click to link to the website selected on the left.

Add Dynamic DNS settings

Step 1. Click **Add** button.

Step 2. Click the information in the column of the new window.

Service providers: Select service providers.

Register: to the service providers' website.

WAN IP Address: IP Address of the WAN port.

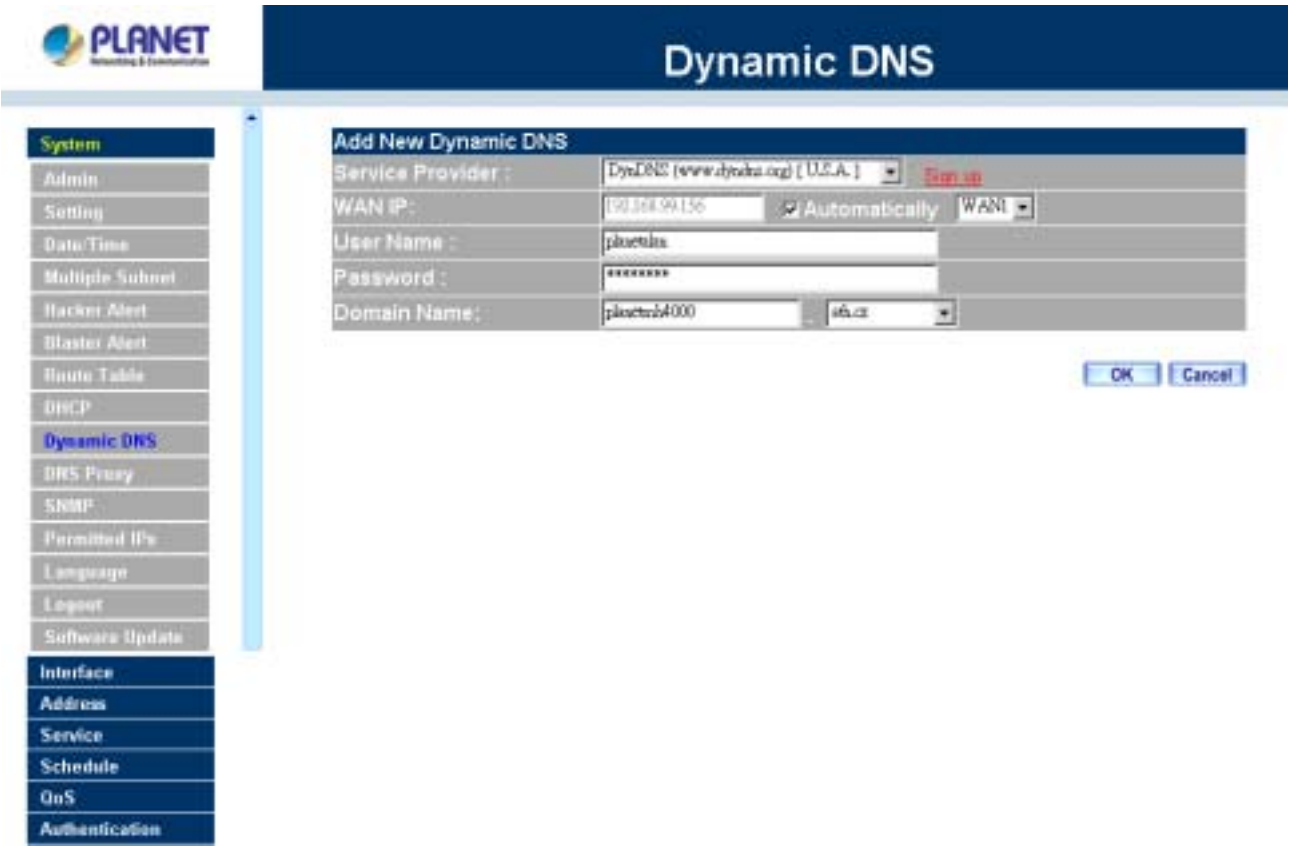
☐ **automatically fill in the WAN IP**: Check to automatically fill in the WAN IP.。

User Name: Enter the registered user name.

Password: Enter the password provided by ISP(Internet Service Provider).

Domain name: Your host domain name provided by ISP.

Click **OK** to add dynamic DNS or click **Cancel** to discard changes.

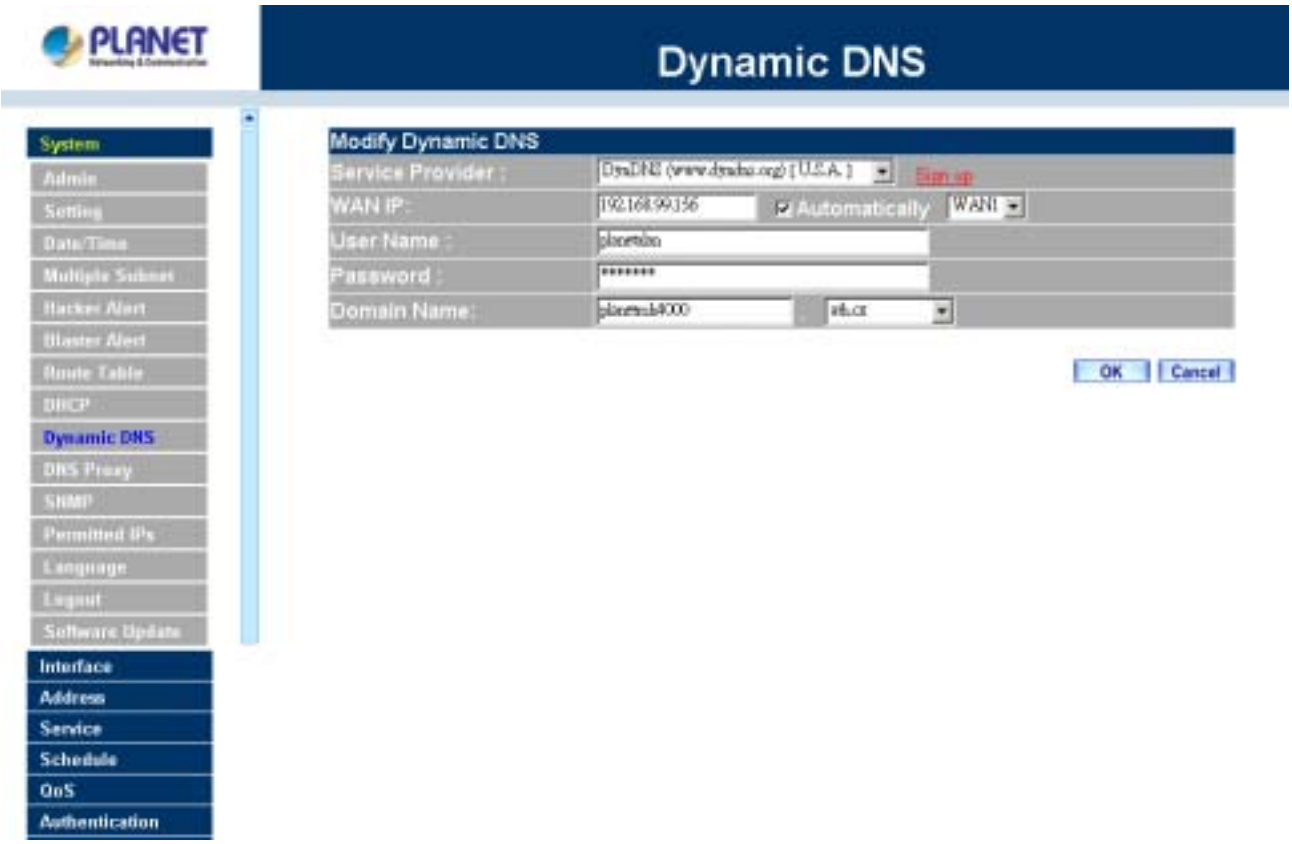


Modify dynamic DNS

Step 1. Find the item you want to change and click **Modify**.

Step 2. Enter the new information in the Modify Dynamic DNS window.

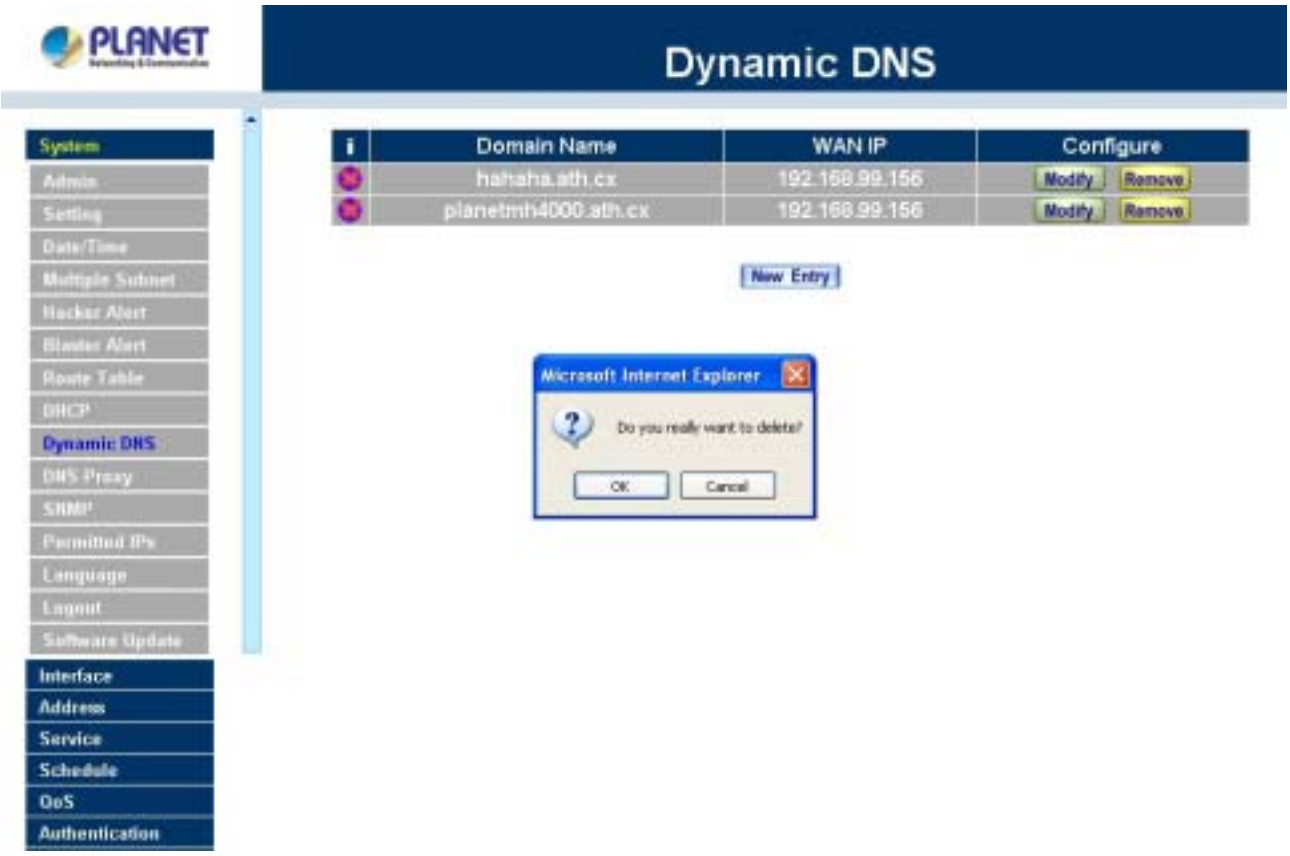
Click **OK** to change the settings or click **Cancel** to discard changes.。



Remove Dynamic DNS

Step 1. Find the item you want to change and click **Remove**.

Step 2. A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.



4.1.10 DNS Proxy

The Multi-Homing Security Gateway's Administrator may use the DNS Proxy function to make the Multi-Homing Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then come back through the Multi-Homing Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one.

This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up DNS Proxy so all the LAN network computers will use the Multi-Homing Security Gateway as a DNS server, which acts as the DNS Proxy.

If you want to use the DNS Proxy function of the device, the end user s main DNS server IP address should be the same IP Address as the device.

Click on **System** in the menu bar, then click on **DNS Proxy** below it. The DNS Proxy window will appear.

Below is the information needed for setting up the **DNS Proxy**:

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to DNS Proxy
- **Configure:** modify or remove each DNS Proxy policy

Adding a new DNS Proxy

Step 1: Click on the **New Entry** button and the **Add New DNS Proxy** window will appear.

Step 2: Fill in the appropriate settings for the domain name and virtual IP address.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

Modifying a DNS Proxy

Step 1: In the DNS Proxy window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

Removing a DNS Proxy

Step 1: In the **DNS Proxy** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the DNS Proxy or click **Cancel**.

4.1.11 SNMP (MH-4000 only)

The administrator could send the information to SNMP by enabling **SNMP Agent.**

NOTE: This function is not supported on MH-2000.

Step 1: Enable SNMP Agent.

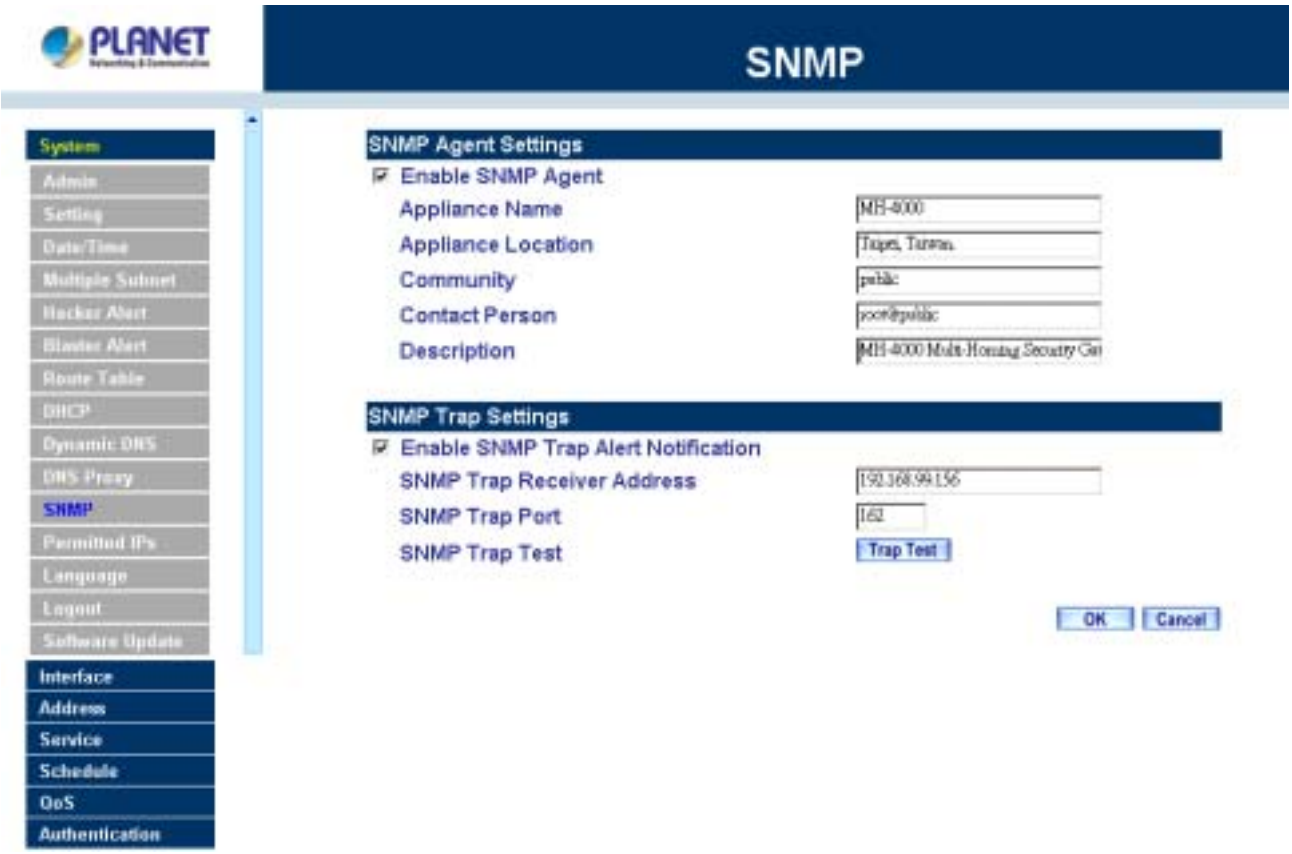
Step 2: Enter Appliance Name.

Step 3: Enter Appliance Location.

Step 4: Enter Community.

Step 5: Enter Contact Person.

Step 6: Enter Description or not.



SNMP Trap Settings

Allow the System Administrator to enable SNMP Trap Alert Notification for sending trap message to the set SNMP Trap receiver IP address when the network is disconnected/ connecting and being attacked by hackers or when emergency conditions occur.

Step 1: Enable SNMP Trap Alert Notification.

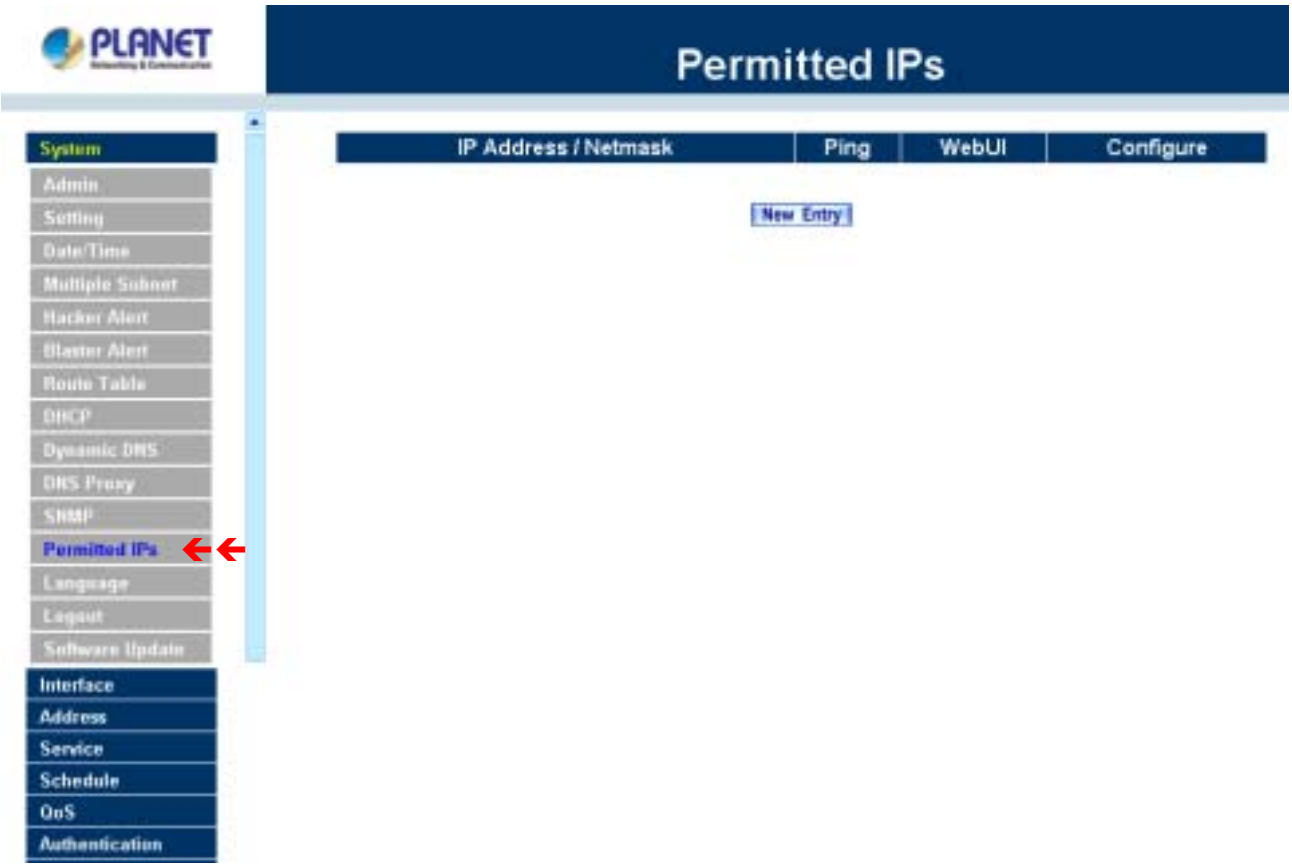
Step 2: SNMP Trap Receiver Address : Set the SNMP Trap Receiver Address.

Step 3: SNMP Trap Port : Set the SNMP Trap Receiver Port.

Step 4: SNMP Trap Test : Click the [Trap Test] button to test if you can receive the SNMP Trap Alert Notification.

4.1.12 Permitted IPs

Only the authorized IP address is permitted to manage the Multi-Homing Security Gateway.



Add Permitted IP Address

Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **IP address**: Enter the LAN IP address or WAN IP address.
- **Netmask**: Enter the netmask of LAN/WAN.
- **Ping**: Select this to allow the external network to ping the IP Address of the Firewall.
- **WebUI**: Check this item, Web User can use HTTP to connect to the Setting window of

Multi-Homing Security Gateway.

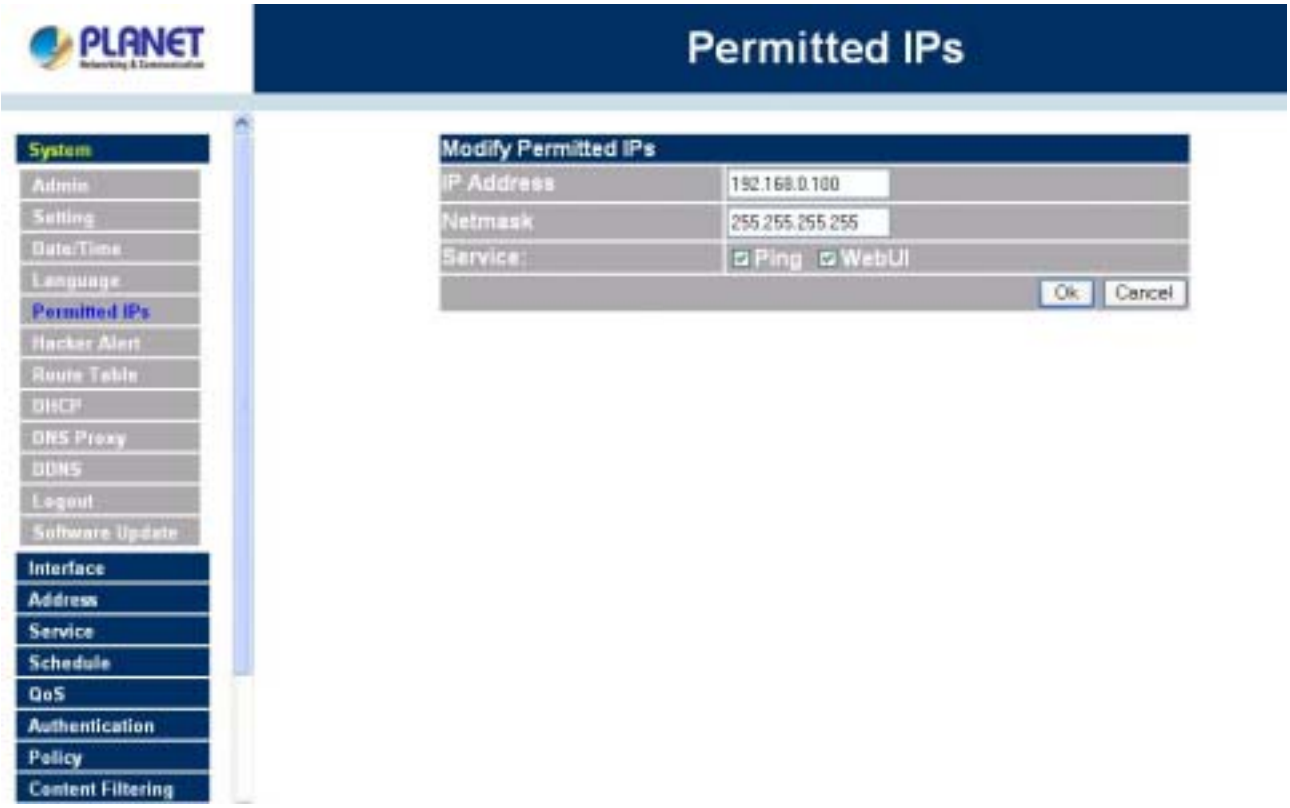
Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.

Modify Permitted IP Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IP**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.

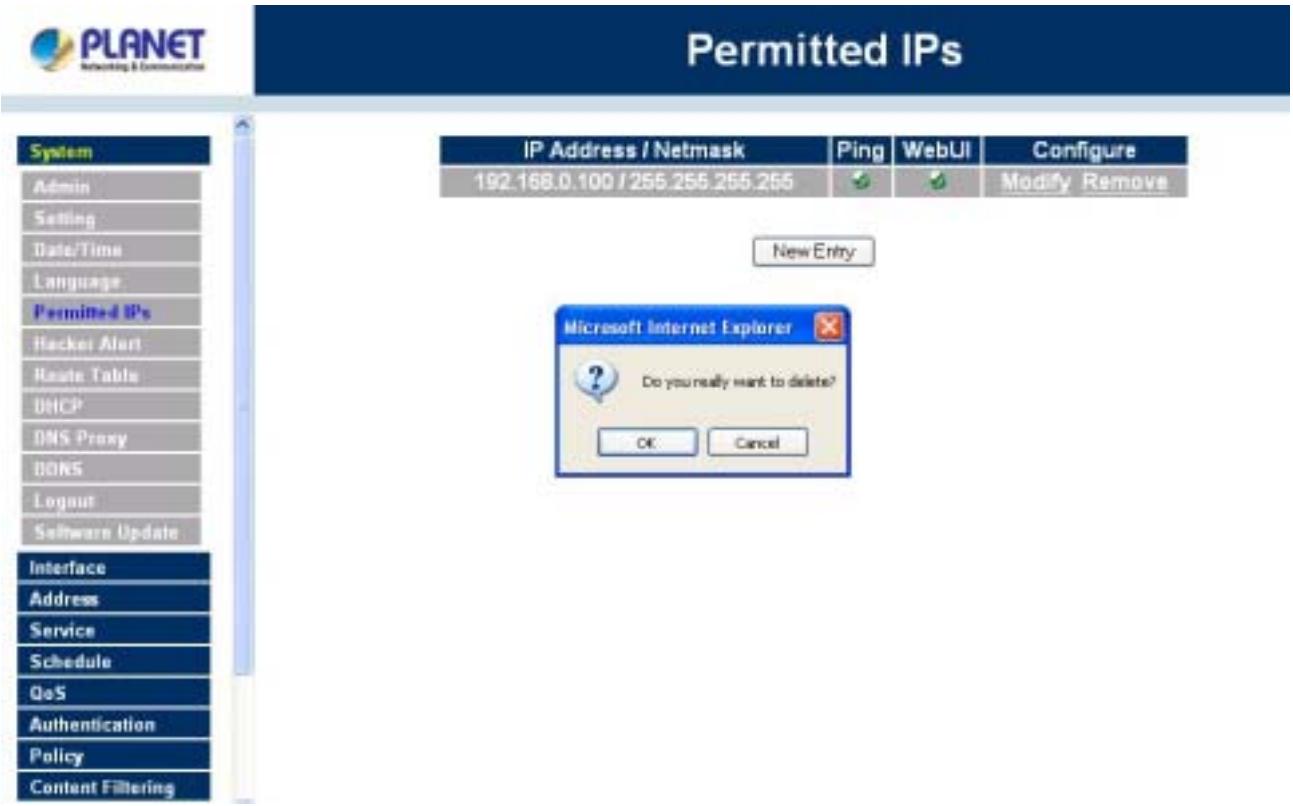


Remove Permitted IP addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In **Remove Permitted IP**, enter new IP address.

Step 3. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.



4.1.13 Language

Administrator can configure the Multi-Homing Security Gateway to select the Language version

Step 1. Select the Language version (**English Version, Traditional Chinese Version** or **Simplified Chinese Version**).

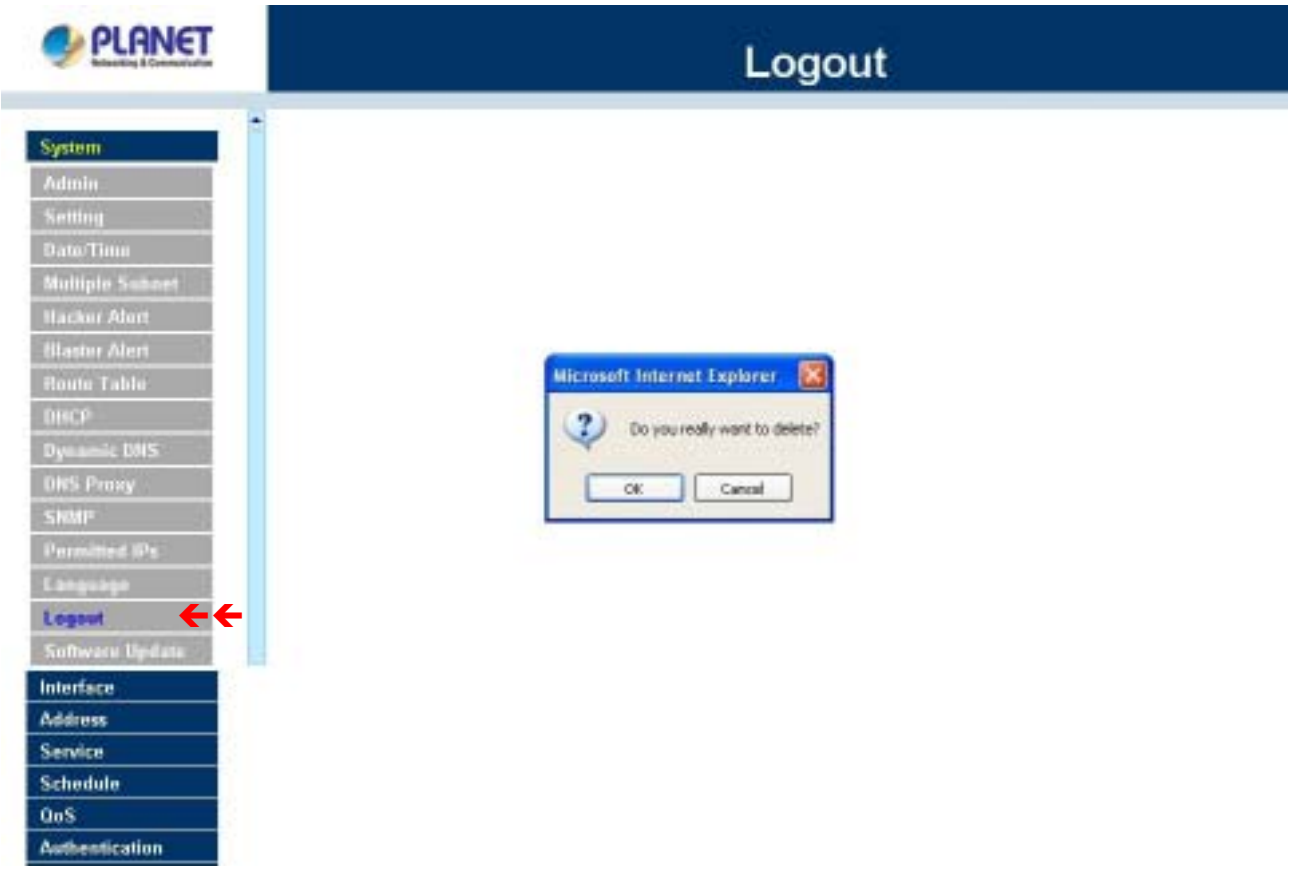
Step 2. Click **[OK]** to set the Language version or click **Cancel** to discard changes.

4.1.14 Logout

Step 1. Select this option to the device's **Logout** the Multi-Homing Security Gateway. This function protects your system while you are away.

Step 2. Click Logout the Multi-Homing Security Gateway.

Step 3. Click **OK** to logout or click **Cancel** to discard the change.



4.1.15 Software Update

Under **Software Update**, the admin may update the device's software with a newer software.

You may acquire the current version number of software in **Version Number**. Administrators may visit distributor's web site to download the latest version and save it in server's hard disc.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.

NOTE: It takes three minutes to update the software. The system will restart automatically after updating the software.

4.2 Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the LAN network, the WAN 1/2 network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

4.2.1 LAN

Entering the Interface menu:

Click on **Interface** in the left menu bar. Then click on **LAN** below it. The current settings of the interface addresses will appear on the screen.

Configuring the Interface Settings

Using the LAN **Interface**, the Administrator sets up the LAN network. The LAN network will use a private IP scheme. The private IP network will not be routable on the Internet.

IP Address: The private IP address of the Multi-Homing Security Gateway's LAN network is the IP address of the LAN port of the device. The default IP address is 192.168.1.1. If the new LAN IP Address is not 192.168.1.1, the Administrator needs to set the IP Address on the computer to be on the same subnet as the Multi-Homing Security Gateway and restart the System to make the new IP address effective. For example, if the Multi-Homing Security Gateway's new LAN IP Address is 172.16.0.1, then enter the new LAN IP Address 172.16.0.1 in the URL field of browser to connect to Multi-Homing Security Gateway.

NetMask: This is the subnet mask of the LAN network. The default netmask of the device is 255.255.255.0.

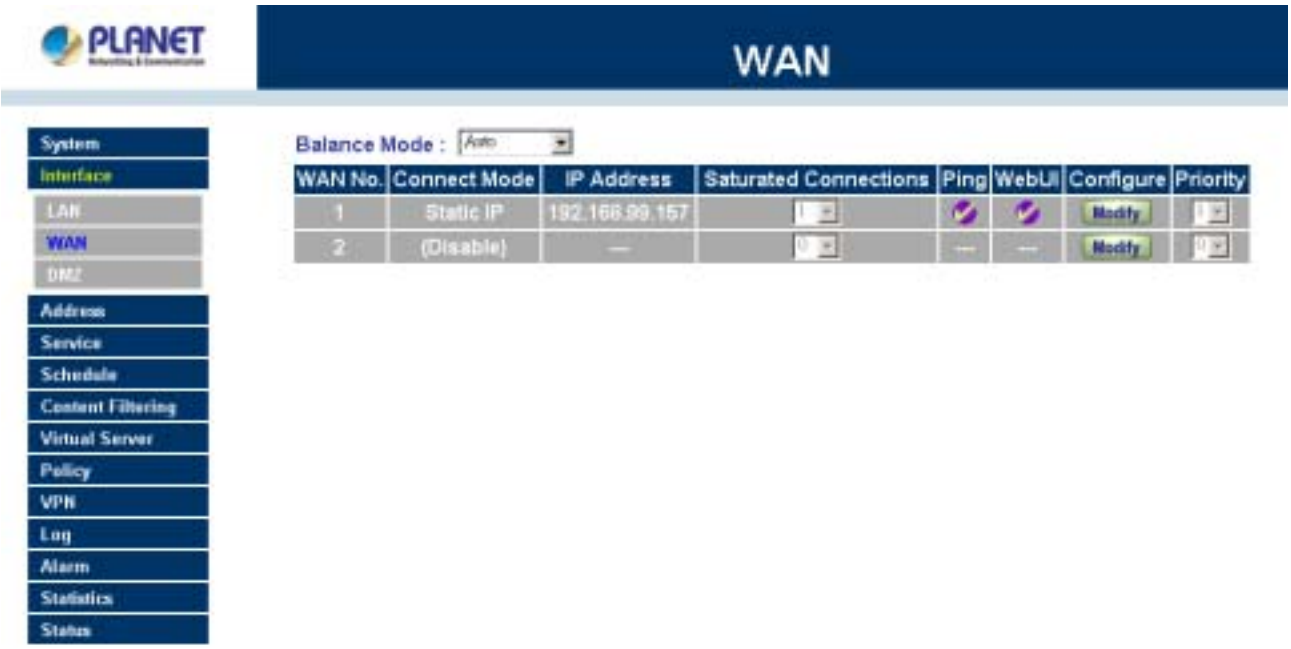
Ping: Select this to allow the LAN network to ping the IP Address of the Multi-Homing Security Gateway. If set to enable, the device will respond to ping packets from the LAN network.

WebUI: Select this to allow the device WEBUI to be accessed from the LAN network.

4.2.2 WAN

Entering the Interface menu

Click on **Interface** in the left menu bar. Then click on **WAN** below it. The current settings of the interface addresses will appear on the screen.



Balance Mode:

Auto: The Multi-Homing Security Gateway distributes the WAN 1/2 download by proportion automatically according to the WAN download bandwidth. (For users who are using various download bandwidth.)

Round-Robin: The Multi-Homing Security Gateway distributes the WAN 1/2 download bandwidth 1:1, in other words, it selects the agent by order. (For users who are using same download bandwidths.)

By Traffic: The Multi-Homing Security Gateway distributes the WAN 1/2 download bandwidth by traffic. (For users who are connected to the Internet via a fixed WAN IP address.

By Session: The Multi-Homing Security Gateway distributes the WAN 1/2 download bandwidth by session. (For users who are connected to the Internet via a fixed WAN IP address.

By Packet: The Multi-Homing Security Gateway distributes the WAN 1/2 download bandwidth by packet and saturated connection. (For users who are connected to the Internet via a fixed WAN IP address.

WAN No: WAN port 1 or 2.

Connect Mode: Display the current connection mode: PPPoE, Dynamic IP Address (Cable Modem User) or Static IP Address.

IP Address: Display the current WAN IP Address.

Saturated Connections: Set the number for saturation whenever session numbers reach it, the Multi-Homing Security Gateway switches to the next WAN port on the list. This function is only applicable for **By Session** mode.

Ping / WebUI: Display Ping/WebUI functions of WAN 1/2 to show if they are enabled or disabled.

Configure: Click **Modify** to modify WAN 1/2 settings.

Priority: Set priority of WAN 1/2 for Internet Access.

WAN 1/2 Interface

Using the WAN 1/2 **Interface**, the Administrator can sets up the **WAN 1/2** network. These IP Addresses are real public IP Addresses, and are routable on the Internet.

Alive Indicator Site IP: This feature is used to ping an address for detecting WAN connection status.

Service: ICMP You can select an IP address by Assist, or type an IP address manually.

Service: DNS You can select a DNS IP and Domain name by Assist, or type the related data manually.

For PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect, such as ADSL users.

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP Address of the PPPoE connection

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Service-On-Demand:

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway.

If set to enable, the device will respond to echo request packets from the WAN 1/2 network.

WebUI: Select this to allow the device WebUI to be accessed from the WAN 1 network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

<u>For Dynamic IP Address (Cable Modem User):</u> This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by the Multi-Homing Security Gateway from the ISP will be displayed here. This is the IP address of the WAN 1 (WAN) port of the device.

MAC Address: This is the MAC Address of the device.

Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: You can specify your own domain name or leave it blank.

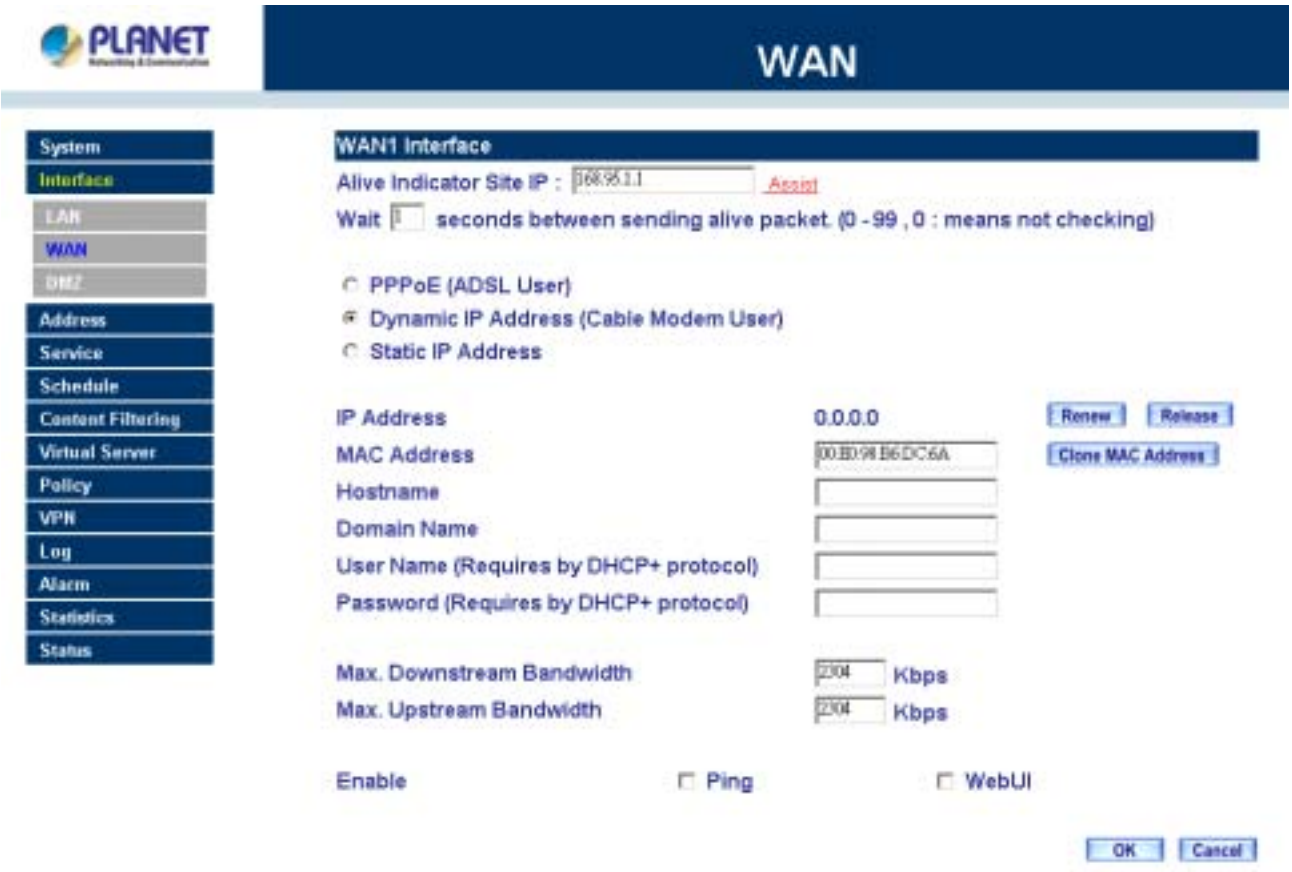
User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the WAN 1 network.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

WebUI: Select this to allow the device WEBUI to be accessed from the WAN 1 network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



<u>For Static IP Address:</u> This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN 1 port of the device.

Netmask: This will be the subnet mask of the WAN 1 network. (i.e. 255.255.255.0)

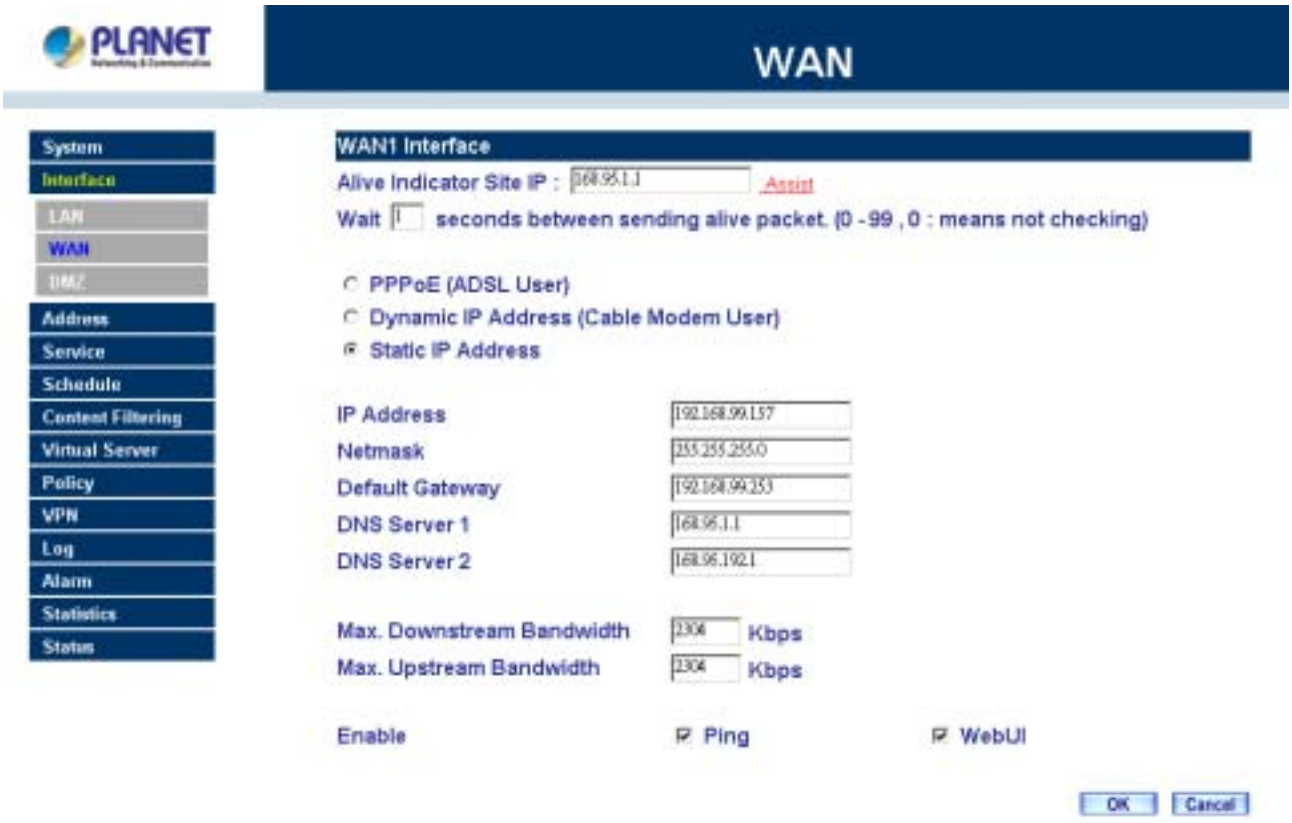
Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP Address of the DNS server.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the WAN 1 network.

WebUI: Select this to allow the device WebUI to be accessed from the WAN 1 network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



<u>For PPTP (European User Only):</u> This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.

PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.

Connect ID: This is the ID given by ISP. This is optional.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.

Service-On-Demand:

The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway.This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the WAN 1 network.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

WebUI: Select this to allow the device WEBUI to be accessed from the WAN 1 network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

NOTE: This function is not supported on MH-4000.

4.2.3 DMZ

The Administrator uses the **DMZ Interface** to set up the DMZ network. The DMZ network consists of server computers such as FTP, SMTP, and HTTP (web). These server computers are put in the DMZ network so they can be isolated from the LAN (LAN) network traffic. Broadcast messages from the LAN network will not cross over to the DMZ network to cause congestions and slow down these servers. This allows the server computers to work efficiently without any slowdowns.

DMZ Interface: Display DMZ NAT Mode /DMZ TRANSPARENT Mode functions of DMZ to show if they are enabled or disabled.

IP Address: The private IP address of the Multi-Homing Security Gateway's DMZ interface. This will be the IP address of the DMZ port. If it is in NAT mode, the IP address the Administrator chooses will be a private IP address and cannot use the same network as the WAN or LAN network.

NetMask: This will be the subnet mask of the DMZ network.

Ping: Select this to allow the DMZ network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the DMZ network.

WebUI: Select this to allow the device WebUI to be accessed from the DMZ network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

4.3 Address

The Multi-Homing Security Gateway allows the Administrator to set addresses of the LAN network, LAN network group, WAN network, WAN group, DMZ network and DMZ group. These settings are to be used for policy editing.

What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address and DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN **Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.

How to use Address Table

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

4.3.1 LAN

Entering the LAN window

Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.

Definition

Name: Name of LAN network address.

IP: IP address of LAN network

Netmask: subnet mask of LAN network.

MAC Address: MAC address corresponded with LAN IP address.

Configure: You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN network. Click **Remove** to delete the settings.

In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

Adding a new LAN Address

Step 1. In the LAN window**,** click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.

Step 3. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.

If you want to enable **Get Static IP address from DHCP Server** function, enter the MAC Address then check the **Get Static IP address from DHCP Server**.

Modifying an LAN Address

Step 1. In the LAN window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.

Step 2. In the **Modify Address** window, fill in the new addresses.

Step 3. Click **OK** to save changes or click **Cance**l to discard changes.

Removing a LAN Address

Step 1. In the LAN window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

4.3.2 LAN Group

Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

Step 1. Click LAN **Group** under the **Address** menu to enter the LAN Group window. The current setting information for the LAN network group appears on the screen.

Definitions (LAN group):

Name: Name of the LAN group.

Member: Members of the group.

Configure: Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click **Remove** to delete the group.

In the **LAN Group** window, if one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group. You have to delete the Group in **Policy** window, and then you are allowed to configure the LAN Group.

Adding a LAN Group

Step 1. In the LAN **Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

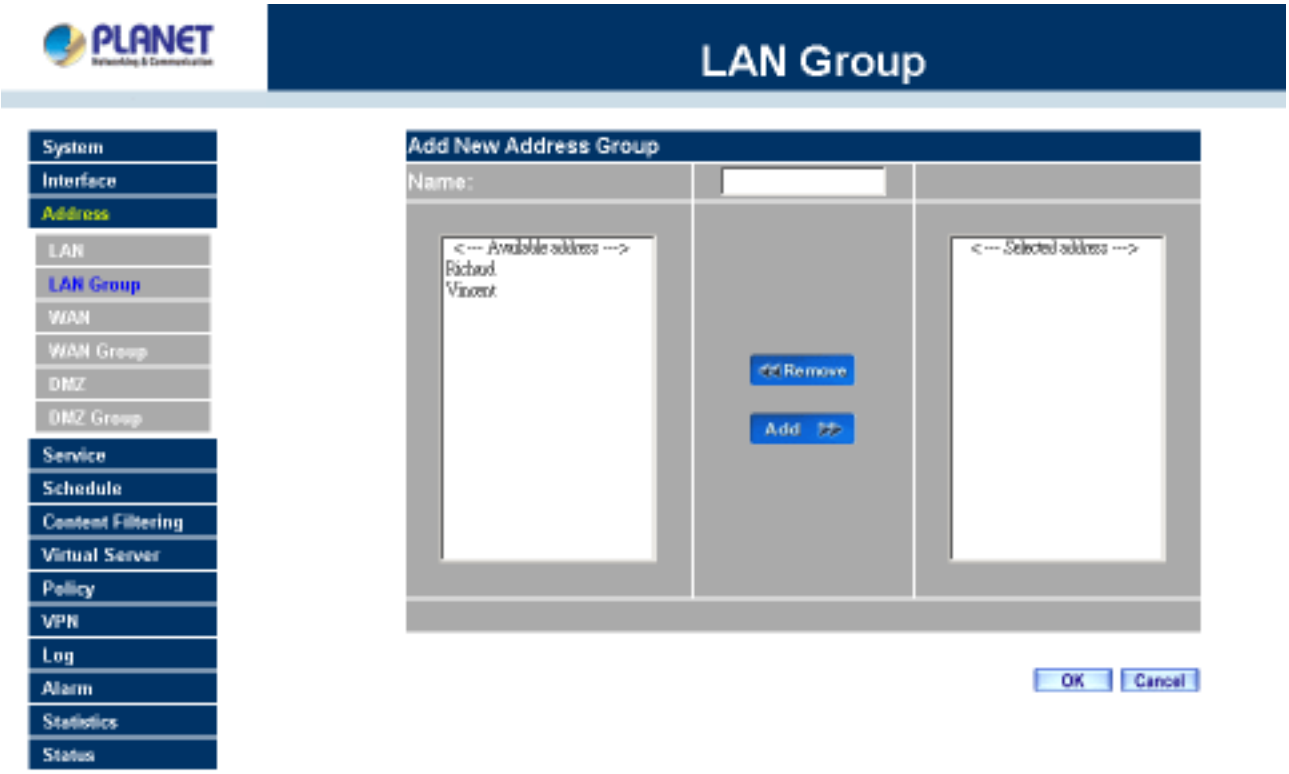
Step 2. In the Add New Address Group window:

- **Available Address:** list the names of all the members of the LAN network.
- **Selected Address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available Address list, and click the **Add>>** button to add them to the Selected Address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click Cancel to discard changes.



Modifying a LAN Group

Step 1. In the LAN **Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

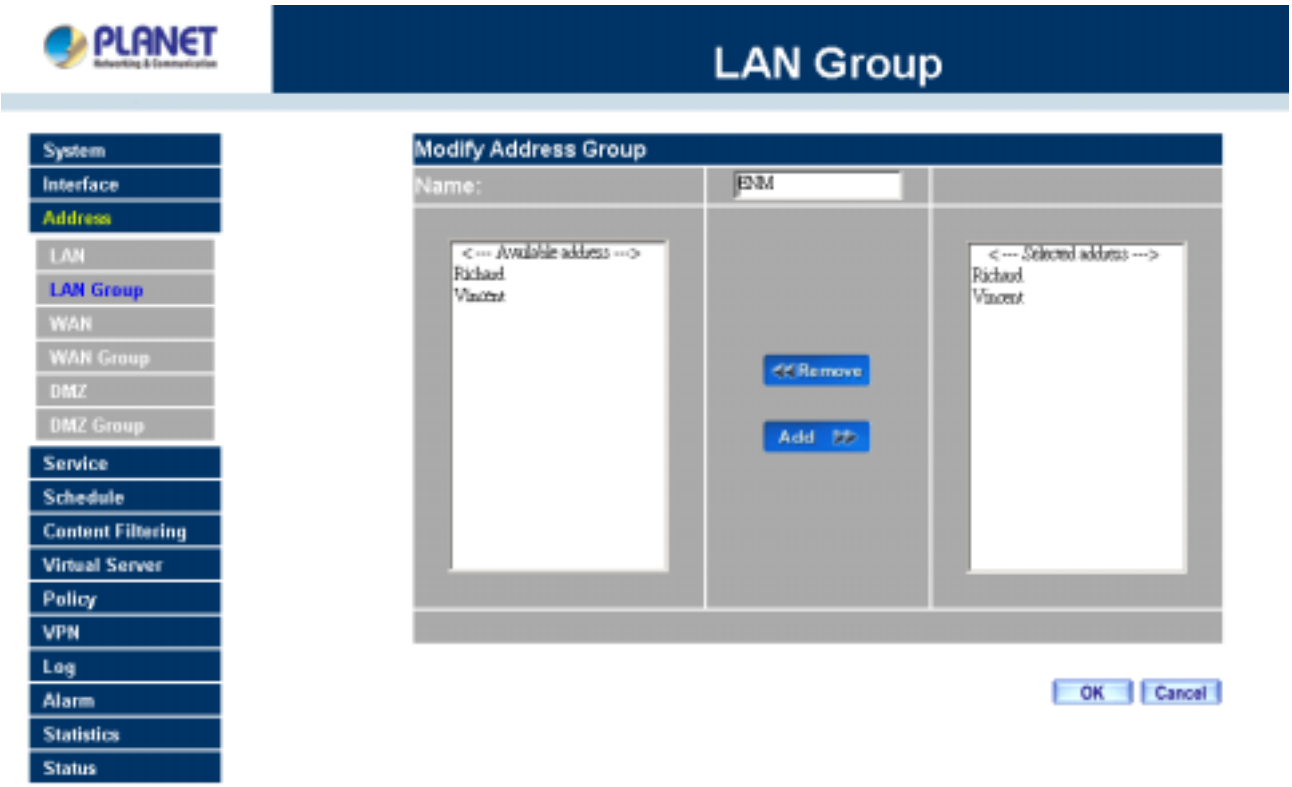
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list names of all members of the LAN network.
- **Selected Address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names in the **Selected Address** list, and click the **<<Remove** button to remove these members from the **Selected Address** list.

Click **OK** to save changes or click **Cancel** to discard changes.



Removing a LAN Group

Step 1. In the LAN **Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

4.3.3 WAN

Entering the WAN window

Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.

Definitions

Name: Name of WAN network address.

IP/Netmask: IP address/Netmask of WAN network.

Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network. Click **Remove** to delete the setting of WAN network.

NOTE: In the WAN Network window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.

Adding a new WAN Address

Step 1. In the WAN window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.

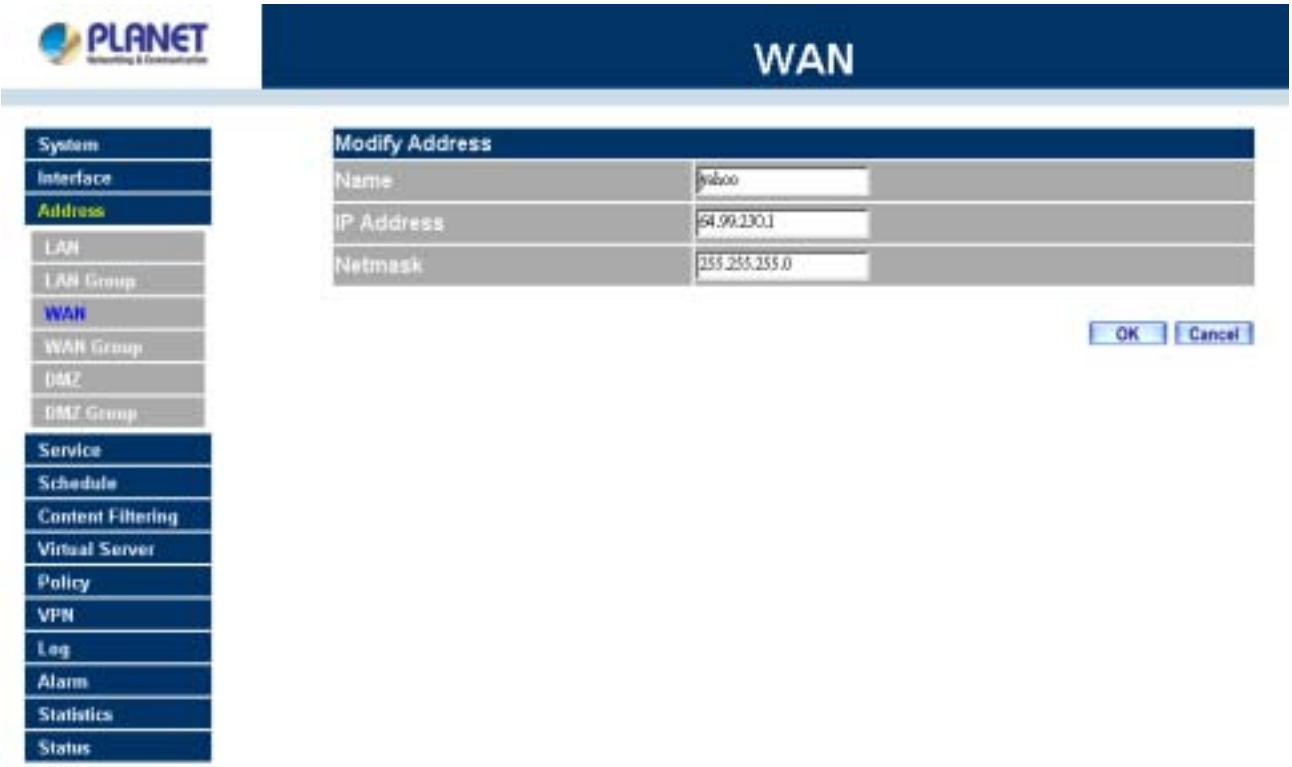
Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.

Modifying an WAN Address

Step 1. In the WAN table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.



Removing an WAN Address

Step 1. In the WAN table, locate the name of the network to be removed and click the **Remove** option in its corresponding Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

4.3.4 WAN Group

Entering the WAN Group window

Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current settings for the WAN network group(s) will appear on the screen.

Definitions:

Name: Name of the WAN group.

Member: Members of the group.

Configure: Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group Click Remove to delete the selected group.

NOTE: In the **WAN Group** window, if one of the members has been added to the **Policy**, "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the **Policy** window to remove the setting, and then you can configure.

Adding an WAN Group

Step 1. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 2. In the **Add New Address Group** window the following fields will appear:

- **Name:** enter the name of the new group.
- **Available Address:** List the names of all the members of the WAN network.
- **Selected Address:** List the names to assign to the new group.
- **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.
- **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.

Modifying a WAN Group

Step 1. In the **WAN Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.

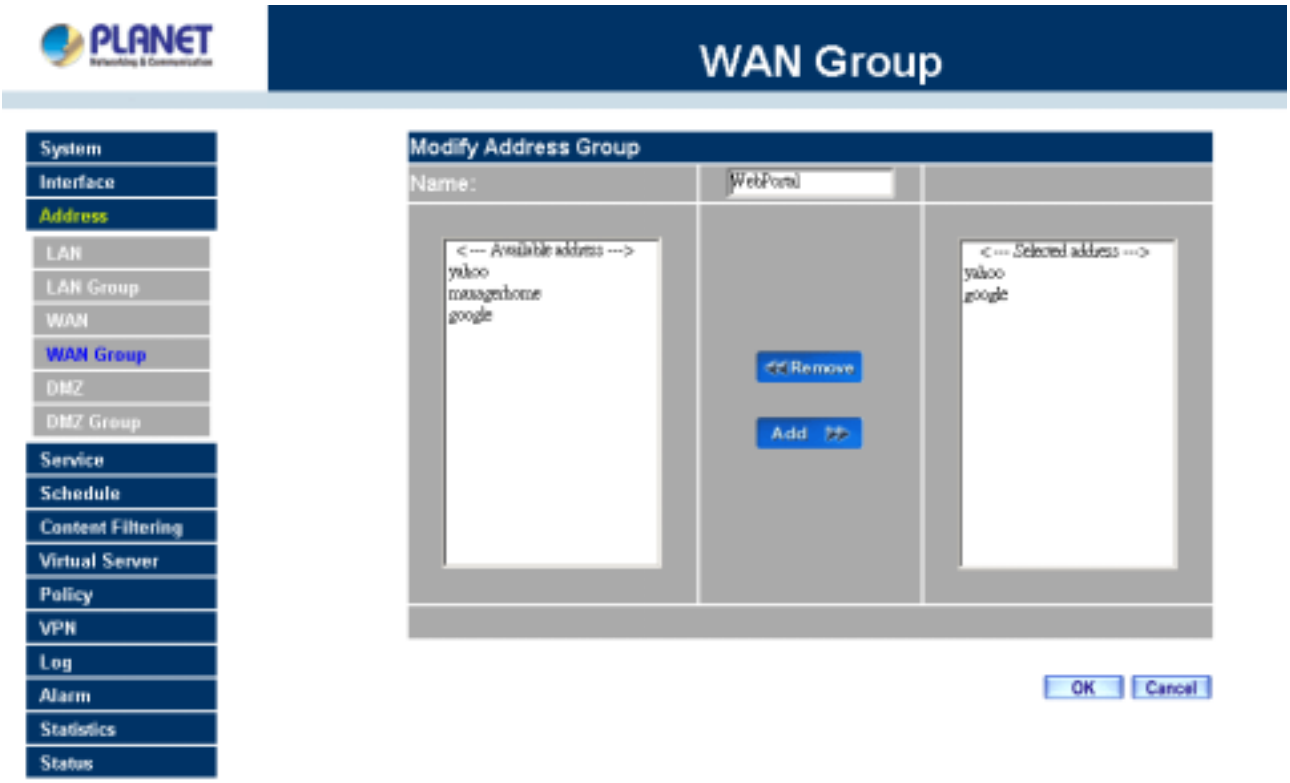
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list the names of all the members of the WAN network.
- **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.



Removing a WAN Group

Step 1. In the **WAN Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

4.3.5 DMZ

Entering the DMZ window:

Click **DMZ** under the **Address** menu to enter the **DMZ** window. The current setting information such as the name of the LAN network, IP, and Netmask addresses will show on the screen.

Adding a new DMZ Address:

Step 1. In the DMZ window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new DMZ address.

Step 3. Click **OK** to add the specified DMZ or click **Cancel** to discard changes.

PLANET
DMZ
System
Interface
Address
LAN
LAN Group
WAN
WAN Group
DMZ
DMZ Group
Service
Schedule
Content Filtering
Virtual Server
Policy
VPN
Log
Alarm
Statistics
Status
Add New Address
Name
IP Address
Netmask
MAC Address
Clone MAC Address
Get static IP address from DHCP Server.
OK
Cancel

Modifying a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** on save the changes or click **Cancel** to discard changes.

Removing a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

4.3.6 DMZ Group

Entering the DMZ Group window

Click **DMZ Group** under the **Address** menu to enter the **DMZ** window. The current settings information for the DMZ group appears on the screen.

Adding a DMZ Group:

Step 1. In the DMZ Group window, click the **New Entry** button.

Step 2. In the **Add New Address** Group window:

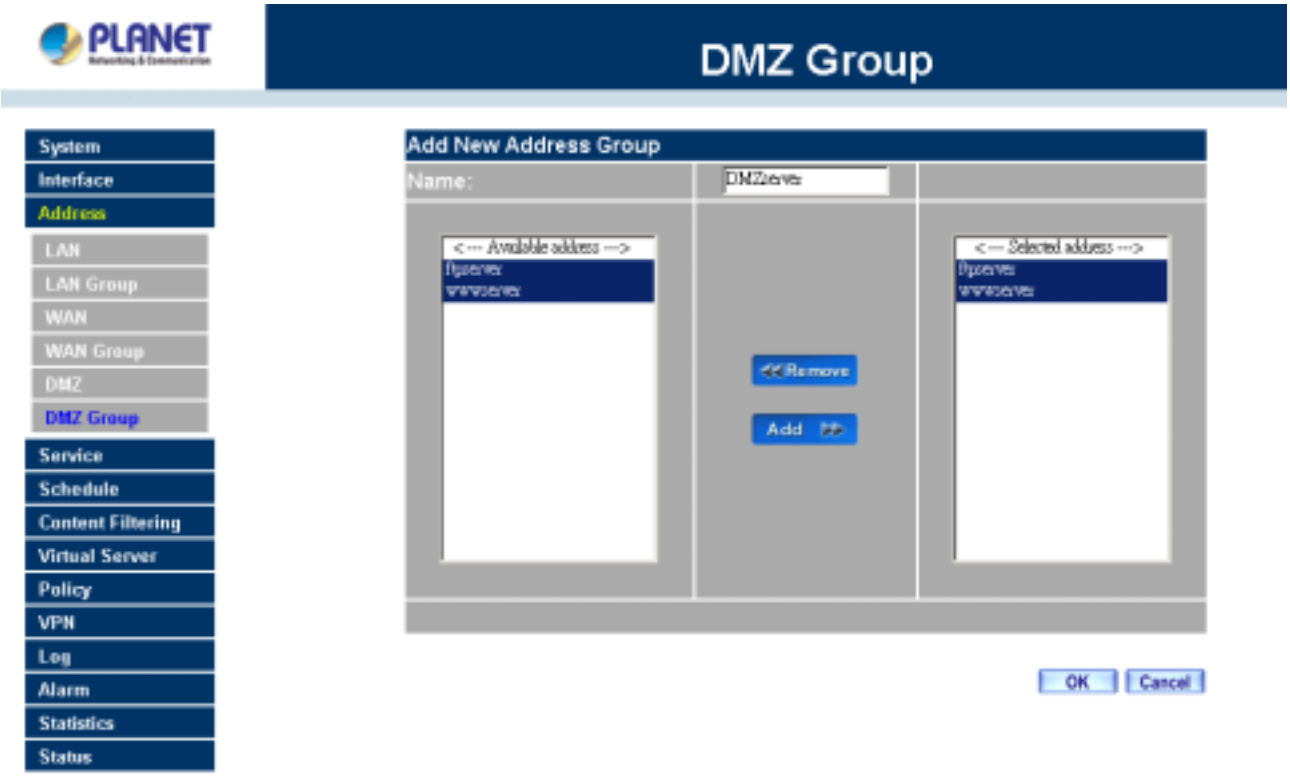
- **Available Address:** list names of all members of the DMZ.
- **Selected Address:** list names to assign to a new group.

Step 3. Name: enter a name for the new group.

Step 4. **Add members:** Select the names to be added from the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 5. **Remove members:** Select names to be removed from the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 6. Click **OK** to add the new group or click **Cancel** to discard changes.



Modifying a DMZ Group:

Step 1. In the **DMZ** Group window, locate the **DMZ** group to be modified and click its corresponding **Modify** button in the **Configure** field.

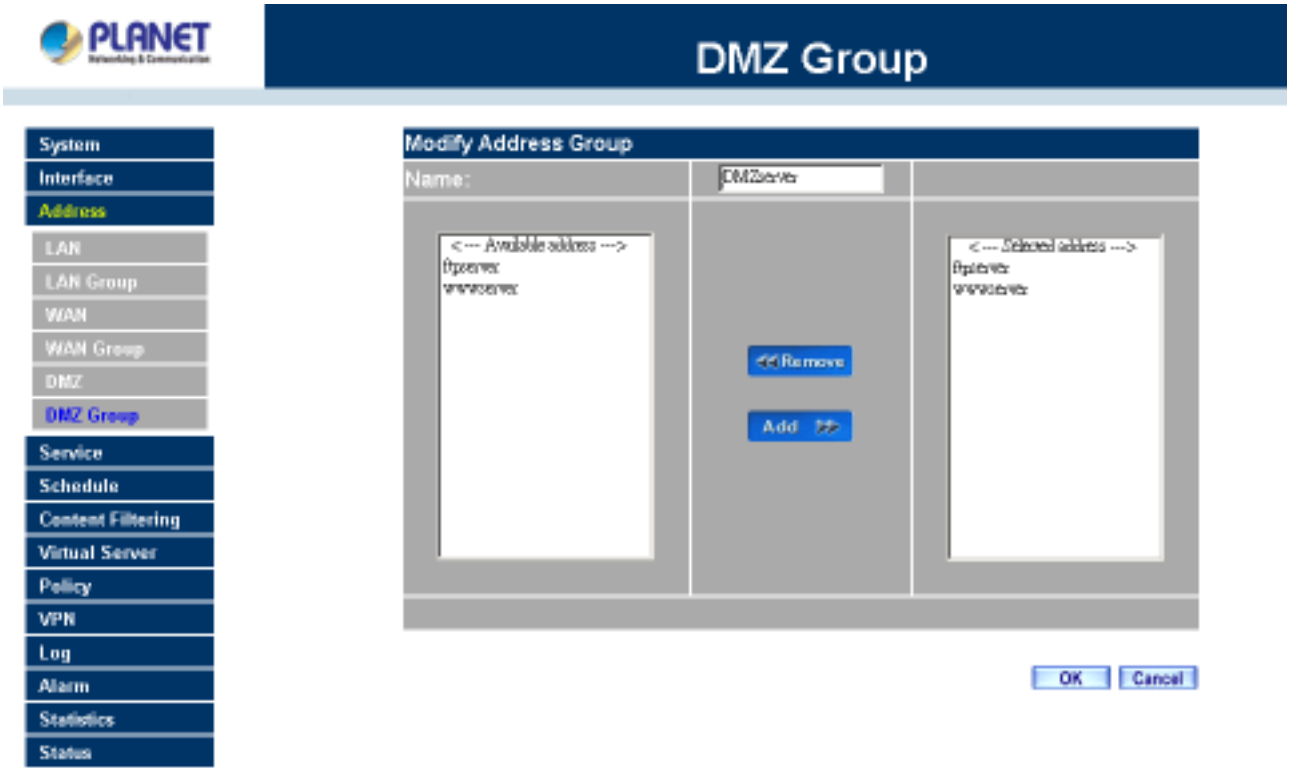
Step 2. A window displaying information about the selected group appears:

- **Available Address:** list the names of all the members of the DMZ.
- **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select names to be added from the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names to be removed from the **Selected Address** list, and click the **<<Remove** button to remove them from **Selected Address** list.

Step 5. Click **OK** to save changes or click Cancel to cancel editing.



Removing a DMZ Group:

Step 1. In the **DMZ Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group.

4.4 Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined**, **Custom**, and **Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. The Multi-Homing Security Gateway defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

How do I use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

4.4.1 Pre-defined

Entering a Pre-defined window

Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.

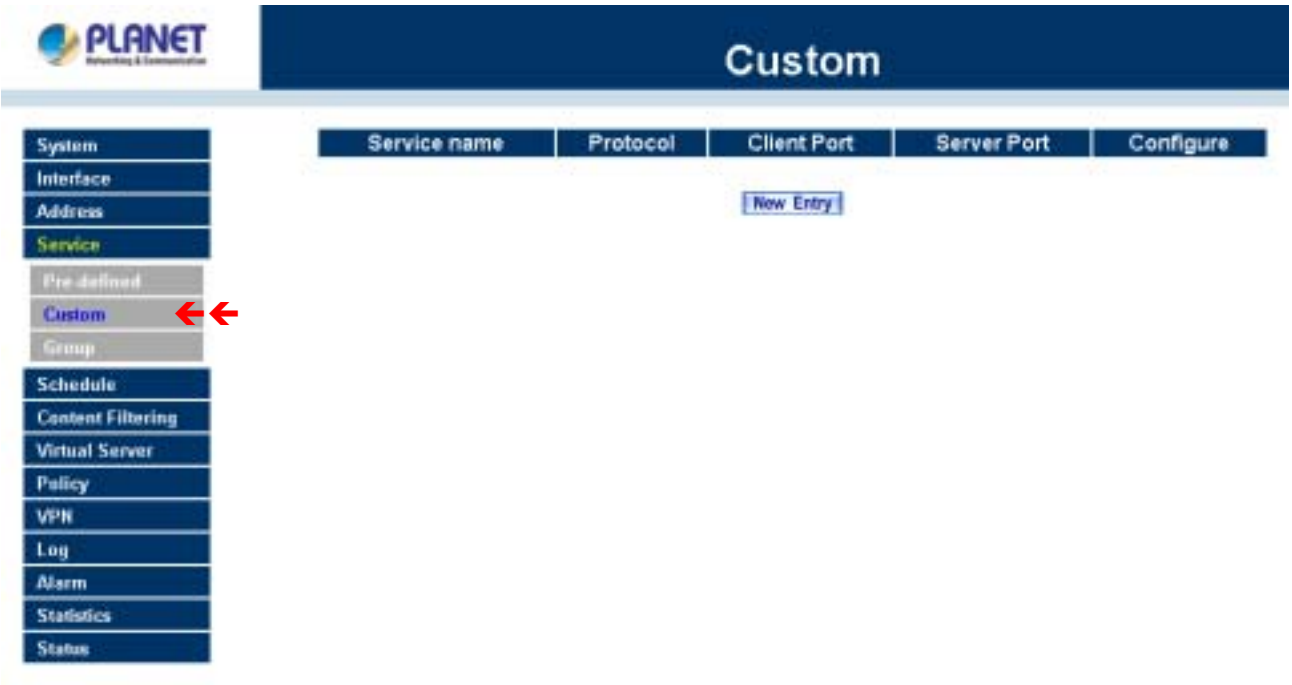
Icons and Descriptions

Figur	Description
TCP	TCP services, i.g. FTP, FINGER, HTTP, HTTPS, IMAP, SMTP, POP3, ANY, AOL, BGP, GOPHER, InterLocator, IRC, L2TP, LDAP, NetMeeting, NNTP, PPTP, Real Media, RLOGIN, SSH, TCP ANY, TELNET, VDO Live, WAIS, WINFRAME, X-WINDOWS, etc.
UDP	UDP services, i.g. IKE, DNS, NTP, IRC, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUC, etc.
ICMP	ICMP services, i.g. PING, TRACEROUTE, etc.

4.4.2 Custom

Entering the Custom window

Step 1. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.



Definitions:

Service name: The defined service name.

Protocol: Network protocol used in the basic setting. Such as TCP、UDP or others.

Client port: The range of Client port in defined service. If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

Service port: The range of Service port in defined service.

If the number of ports entered in the two fields of Service port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Service port is identical, it means that the entered port number is opened.

Configure: Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.

NOTE: In the **Custom** window, if one of the services has been added to **Policy** or **Group**, "**In Use**" message will appear in the **Configure** column. In this case you are not allowed to modify or remove the settings. Go to the **Policy** or **Group** window to delete the setting, and then you can configure the settings.

Adding a new Service

In the **Custom** window, click the **New Entry** button and a new service table appears.

In the new service table:

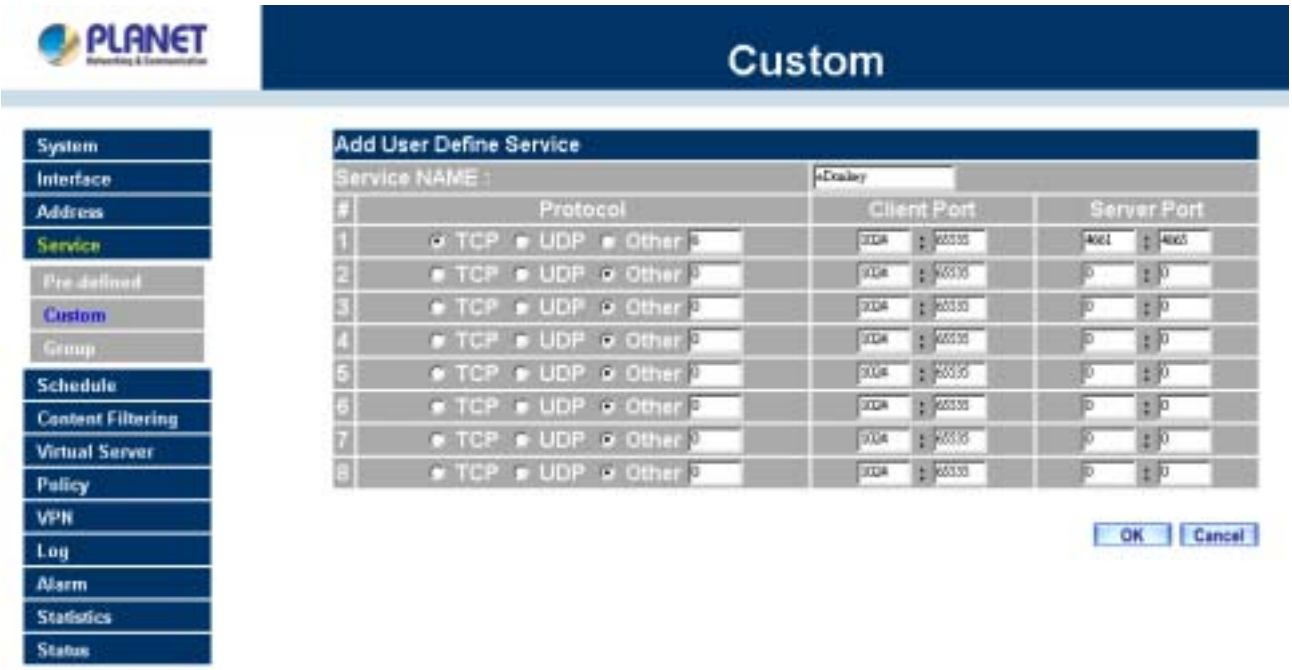
- New Service Name: This will be the name referencing the new service.

- Protocol: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- Client Port: enter the range of port number of new clients.
- Server Port: enter the range of port number of new servers.

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

Step 1. Click **OK** to add new services, or click **Cancel** to cancel.

Step 2. Click **OK** to accept editing; or click **Cancel**.



Modifying Custom Services

Step 1. A table showing the current settings of the selected service appears on the screen

Step 2. Enter the new values.

Step 3. Click **OK** to accept editing; or click **Cancel**.

Removing Custom Services

Step 1. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.

4.4.3 Group

Accessing the Group window

Step 1. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.

Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

Configure: Configure the settings of Group. Click **Modify** to change the parameters of the Group. Click Remove to delete the Group.

NOTE: In the **Group** window, if one of the Service Groups has been added to **Policy**. "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the Policy window, remove the Service group first, and then you are allowed to configure the setting.

Adding Service Groups

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

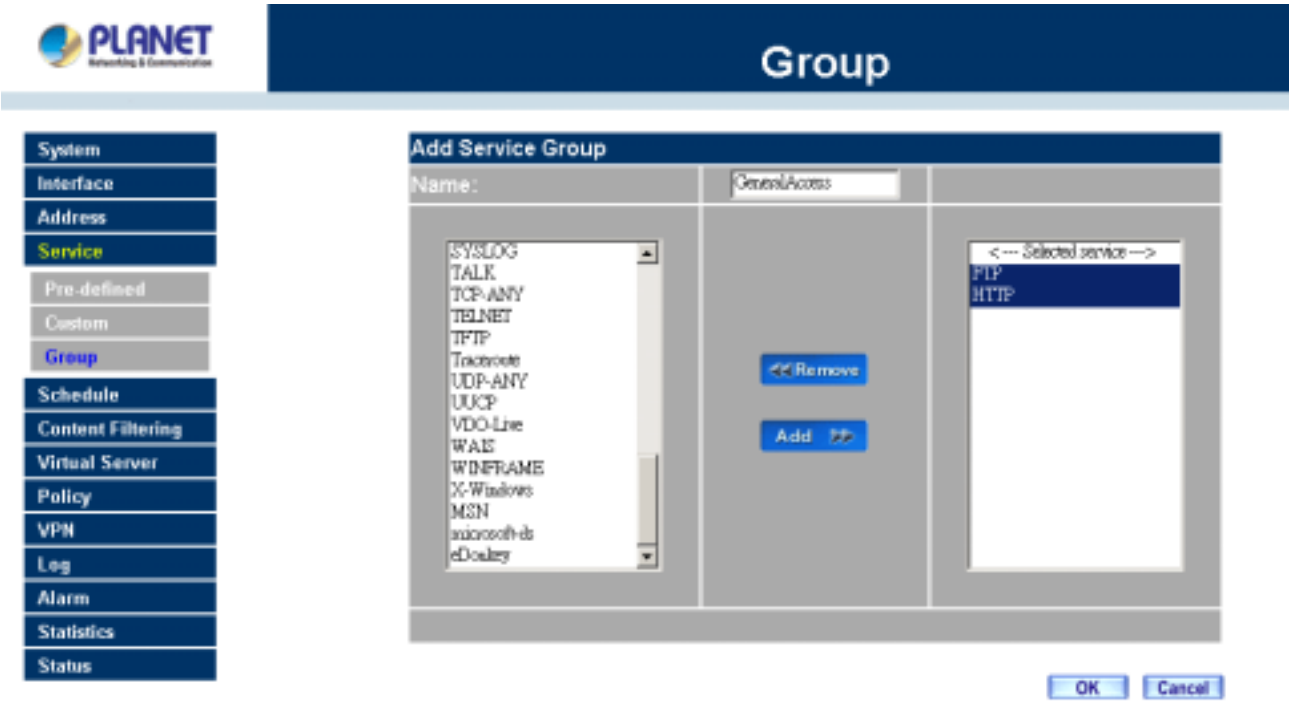
- **Available Services:** list all the available services.
- **Selected Services:** list services to be assigned to the new group.

Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available Services** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Available Services**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.



Modifying Service Groups

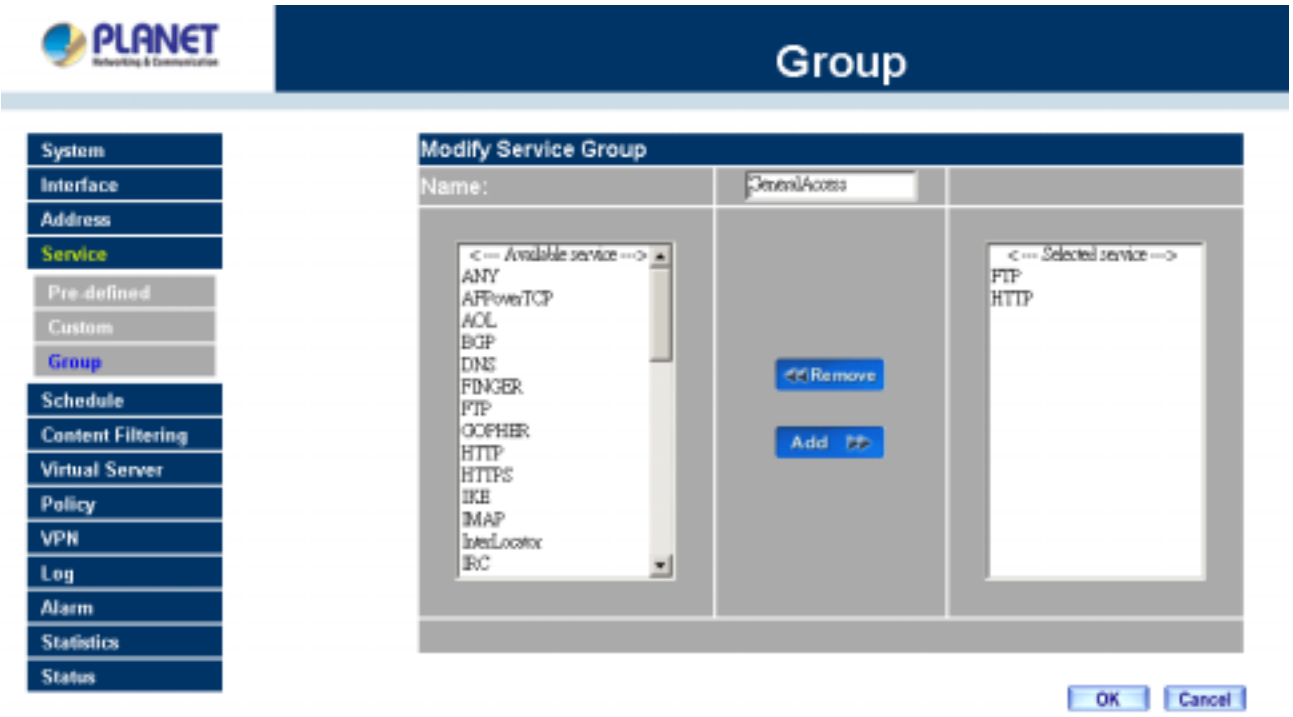
Step 1. In the Mod (modify) group window the following fields are displayed:

- **Available Services:** lists all the available services.
- **Selected Services:** list services that have been assigned to the selected group.

Step 2. **Add new services:** Select services in the **Available Services** list, and then click the **Add>>** button to add them to the group.

Step 3. **Remove services:** Select services to be removed in the **Selected Services** list, and then click the **<<Remove** button to remove theses services from the group.

Step 4. Click **OK** to save editing changes.



Removing Service Groups

In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.

4.5 Schedule

The Multi-Homing Security Gateway allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Multi-Homing Security Gateway policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Multi-Homing Security Gateway policies therefore will likely not be permitted to pass through the Multi-Homing Security Gateway. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Multi-Homing Security Gateway to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Multi-Homing Security Gateway to work Monday-Friday, 8AM - 5PM only. During the non-work hours, the Multi-Homing Security Gateway will not allow Internet access.

Accessing the Schedule window

Step 1. Click on **Schedule** on the menu bar and the schedule window will appear displaying the active schedules.

The following items are displayed in this window:

Name: the name assigned to the schedule

Comment: a short comment describing the schedule

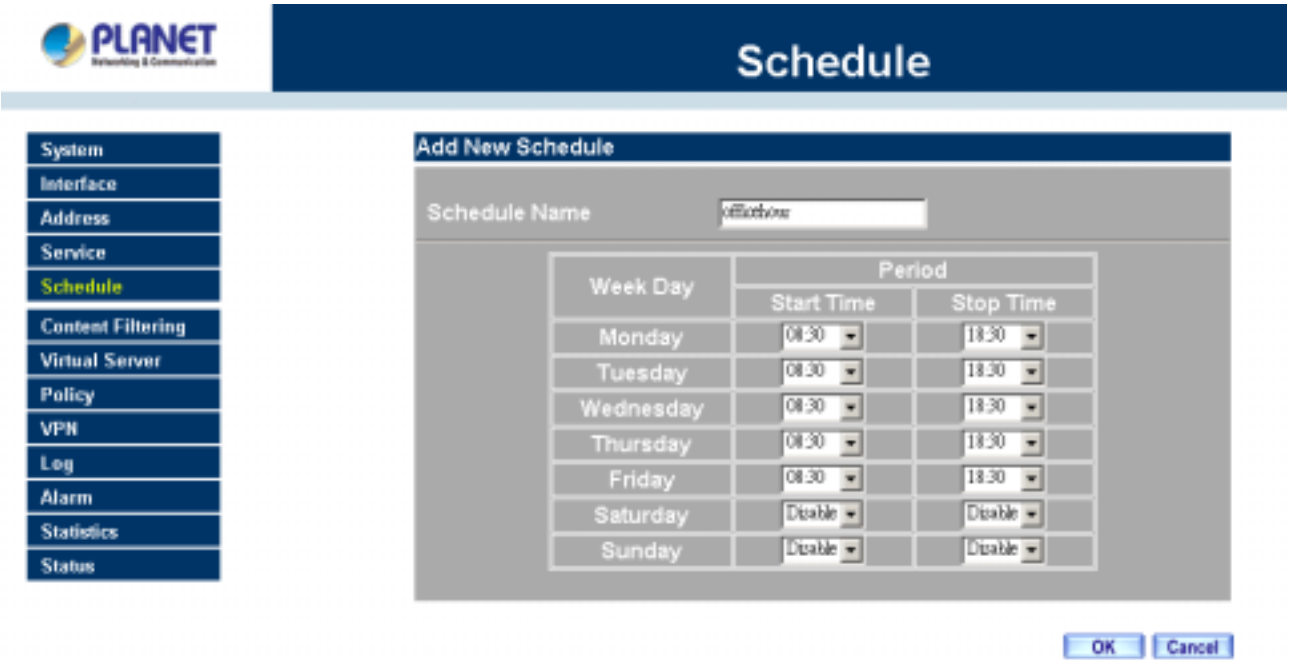
Configure: modify or remove

Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

- **Schedule Name:** Fill in a name for the new schedule.
- **Period:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click Cancel to cancel adding the new schedule.

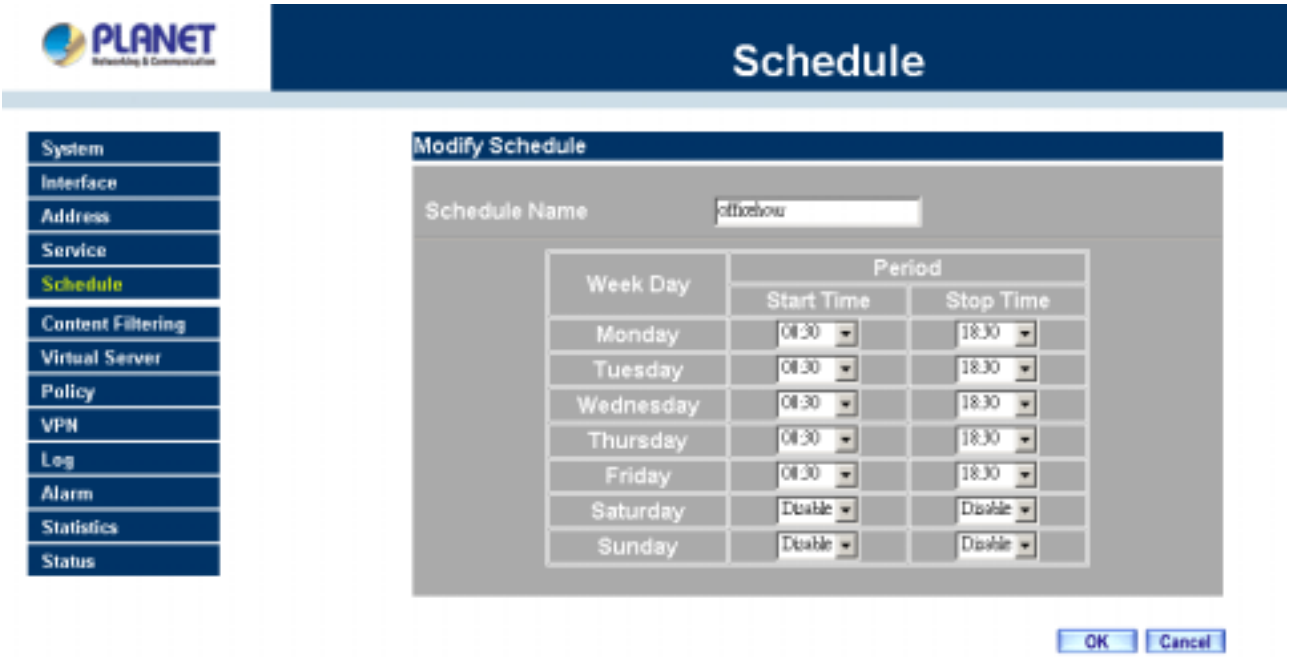


NOTE: In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

Modifying a Schedule

Step 1. In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field. Make needed changes.

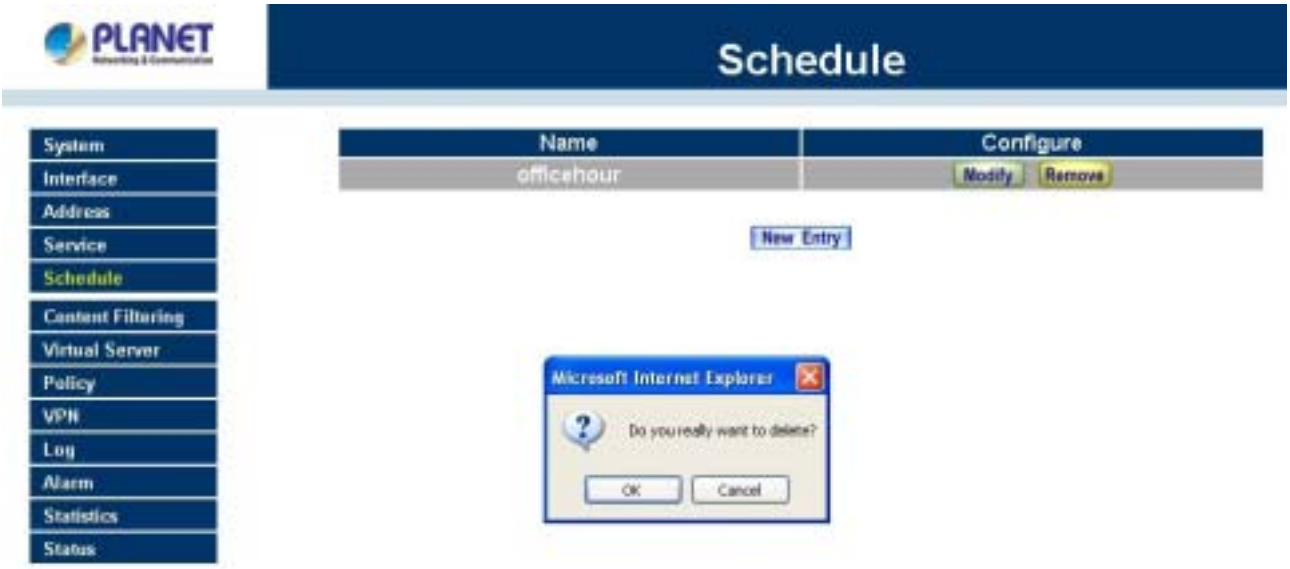
Step 2. Click **OK** to save changes.



Removing a Schedule

Step 1. In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the schedule.



4.6 QoS (MH-4000 only)

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth.

The administrator can configure the bandwidth according to the WAN bandwidth.

Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

The Multi-Homing Security Gateway configures the bandwidth by different QoS , and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The Multi-Homing Security Gateway also makes it convenient for the administrator to use the Multi-Homing Security Gateway with the best Utility.

NOTE: This function is not supported on MH-2000.

Configuration of QoS

Click QoS in the menu bar on the left hand side.

Definitions:

Name: The name of the QoS you want to configure.

WAN: Display WAN 1 or WAN 2.

Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

Add New QoS

Step 1. Click QoS in the menu bar on the left hand side.

Step 2. Click the **New Entry** button to add new QoS.

Definition

Name: The name of the QoS you want to configure.

Downstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Click the **OK** button to add new QoS.

Modify QoS

Step 1. Click QoS in the menu bar on the left hand side.

Click the Modify button to modify QoS.

Definition:

Name: The name of the QoS you want to configure.

Downstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Click the **OK** button to modify QoS.

Delete QoS

Step 1. In the QoS window, find the QoS you want to change, and click **Delete** in the Configure column.

Step 2. In the Delete QoS window, click **OK** to delete the QoS or click Cancel to discard the change.

PLANET
QoS
System
Interface
Address
Service
Schedule
QoS
Authentication
Content Filtering
Virtual Server
Policy
VPN
Inbound Balance
Log
Alarm
Accounting Report
Statistics
Status
Name
WAN
Downstream Bandwidth
Upstream Bandwidth
Priority
Configure
ICF
1
G.Bandwidth = 400Kbps
M.Bandwidth = 420Kbps
G.Bandwidth = 400 Kbps
M.Bandwidth = 420 Kbps
High
Modify
2
G.Bandwidth = 400Kbps
M.Bandwidth = 420Kbps
G.Bandwidth = 400 Kbps
M.Bandwidth = 420 Kbps
Remove
New Entry
Microsoft Internet Explorer
Do you really want to delete?
OK
Cancel

4.7 Authentication (MH-4000 only)

By configuring the Authentication, you can control the user's access right time of LAN to WAN. The administrator can configure the authentication according to the authentication account and password. The Multi-Homing Security Gateway configures the authentication of LAN's user by setting account and password to identify the privilege.

NOTE: This function is not supported on MH-2000.

4.7.1 Auth User

Configuration of Authentication

Click **Authentication** in the menu bar on the left hand side and click **Auth User**.

Definitions:

Name：The name of the Authentication you want to configure.

Configure: modify settings or remove users.

Adding a new Auth User

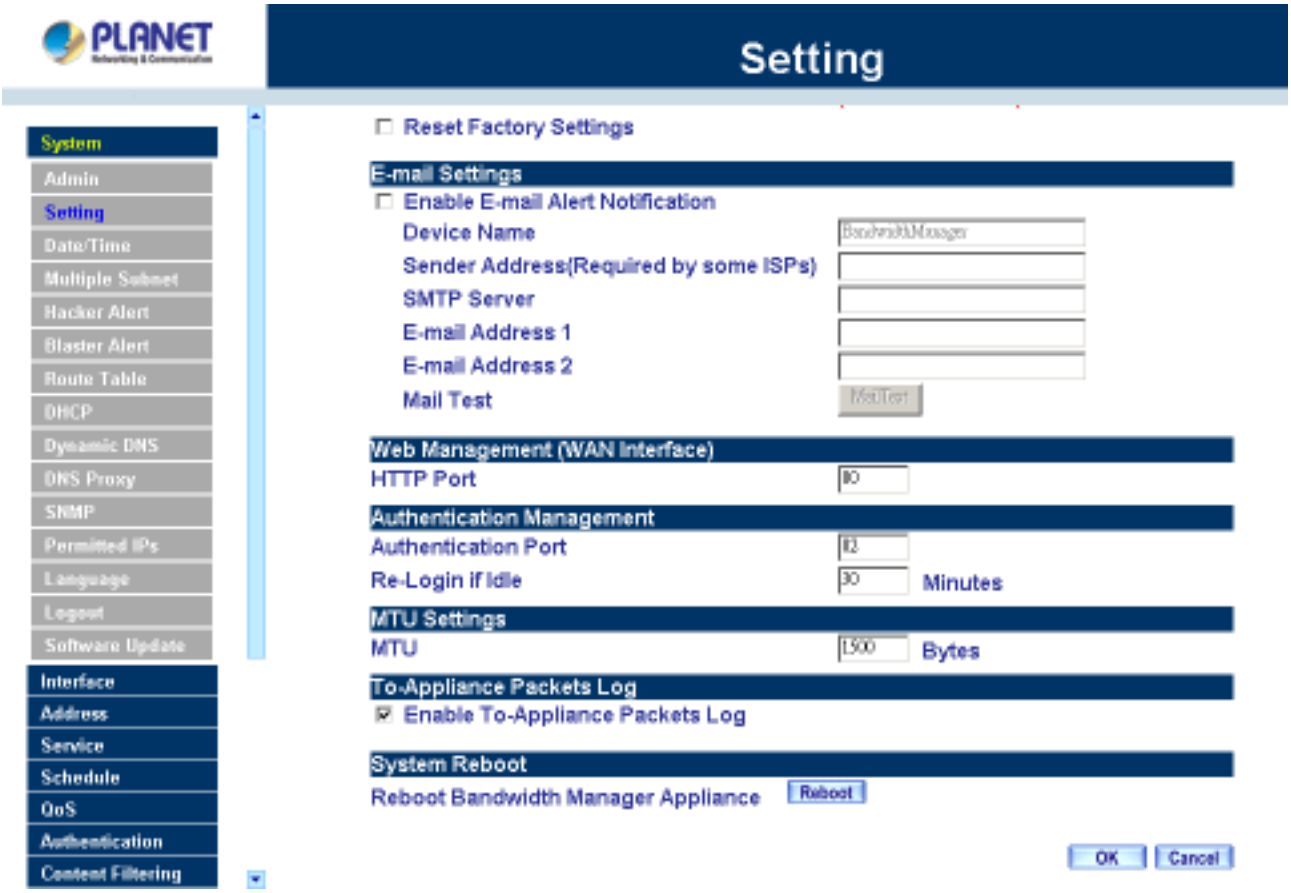
Step 1. In the **Authentication** window, click the **New User** button to create a new **Auth User.**

Step 2. In the **Auth-User** window:

- **Auth-User Name:** enter the username of new **Authentication.**
- **Password:** enter a password for the new **Authentication.**
- **Confirm Password:** enter the password again.

Step 3. Click **OK** to add the user or click **Cancel** to cancel the addition.

NOTE*:* When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "System"-> "Setting" page.

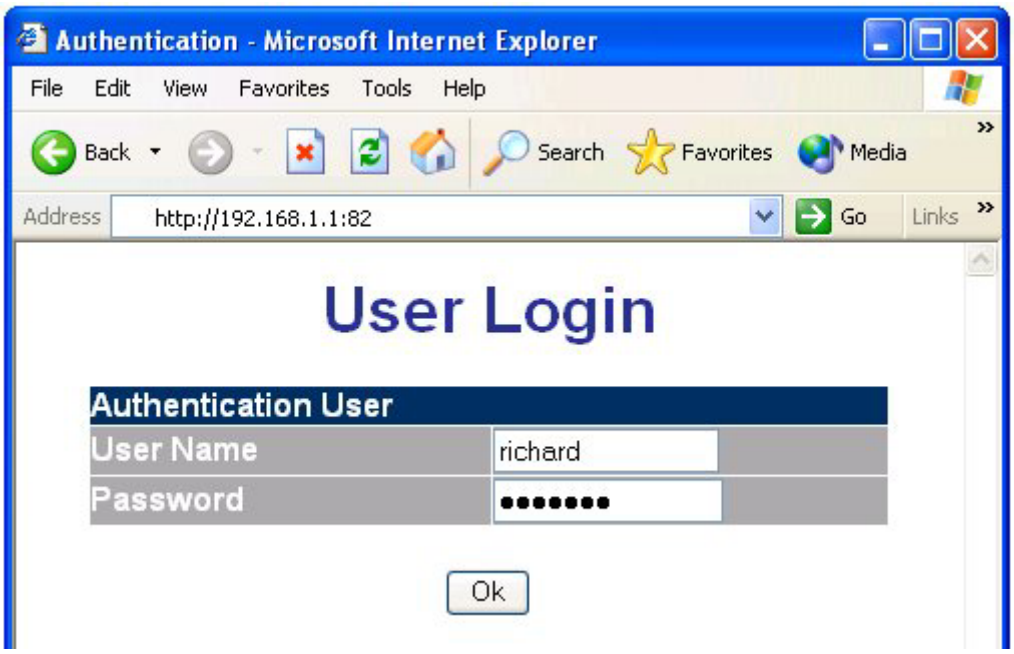


In the form of controlling the [Outgoing] Policy, enable the Authentication-User Function.

When the user's idle time exceed the "Re-Login If Idle" time and the user wan to connect to WAN, the authentication web page will be shown again or user need to manually input the login page. Once user enters the correct user name and password, he can access the WAN resource again.

User Login Page Definitions:

- **User Name**: The name of the Authentication you want to configure.
- **Password**: The input carries on the authentication the password



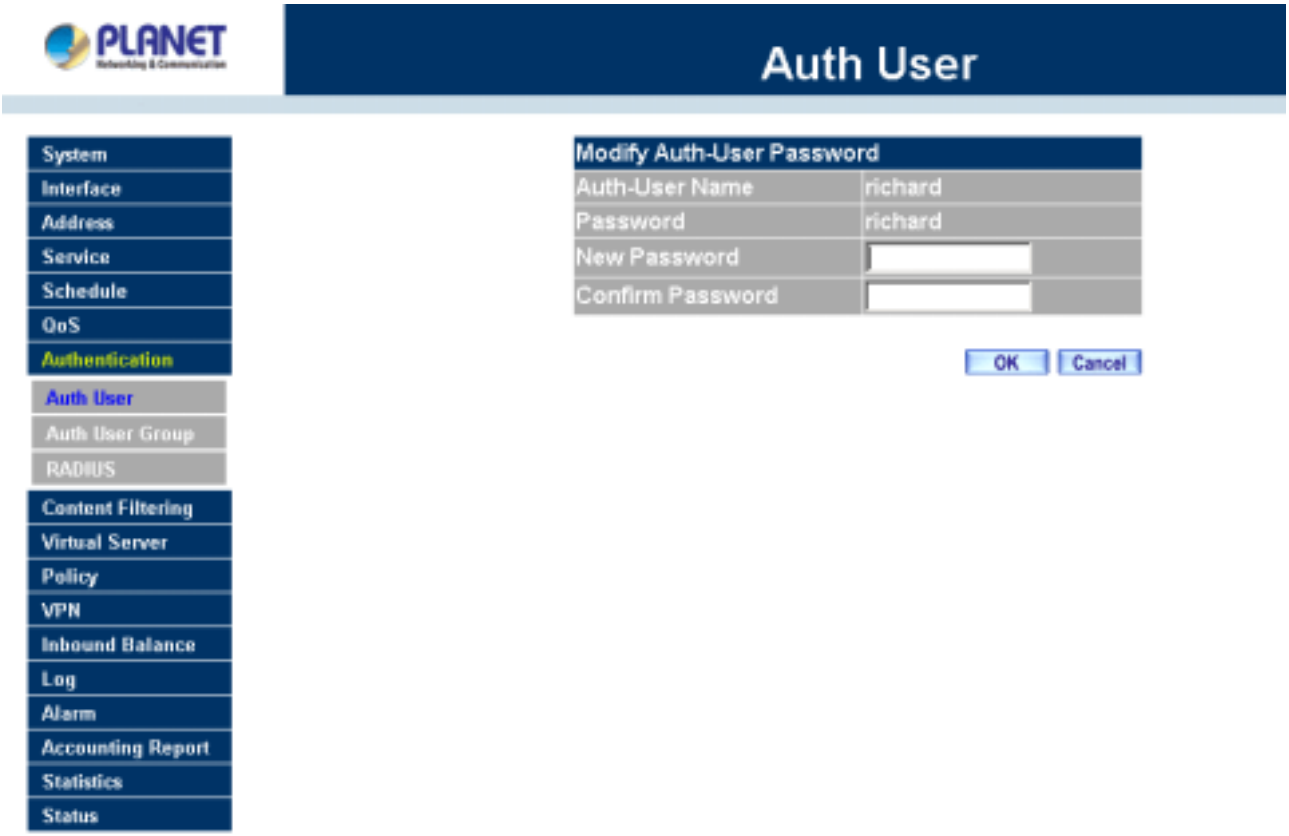
Modifying the Authentication User

Step 1. In the **Authentication** window, locate the **Auth-User** name you want to edit, and click on **Modify** in the **Configure** field.

Step 2. The **Modify Auth-User Password** window will appear. Enter in the required information:

- **Auth-User:** show original authentication user.
- **Password:** show original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 3. Click **OK** to confirm authentication user change or click **Cancel** to cancel it.



Removing a Authentication User

Step 1. In the Authentication table, locate the Auth-User name you WAN t to edit, and click on the Remove option in the Configure field.

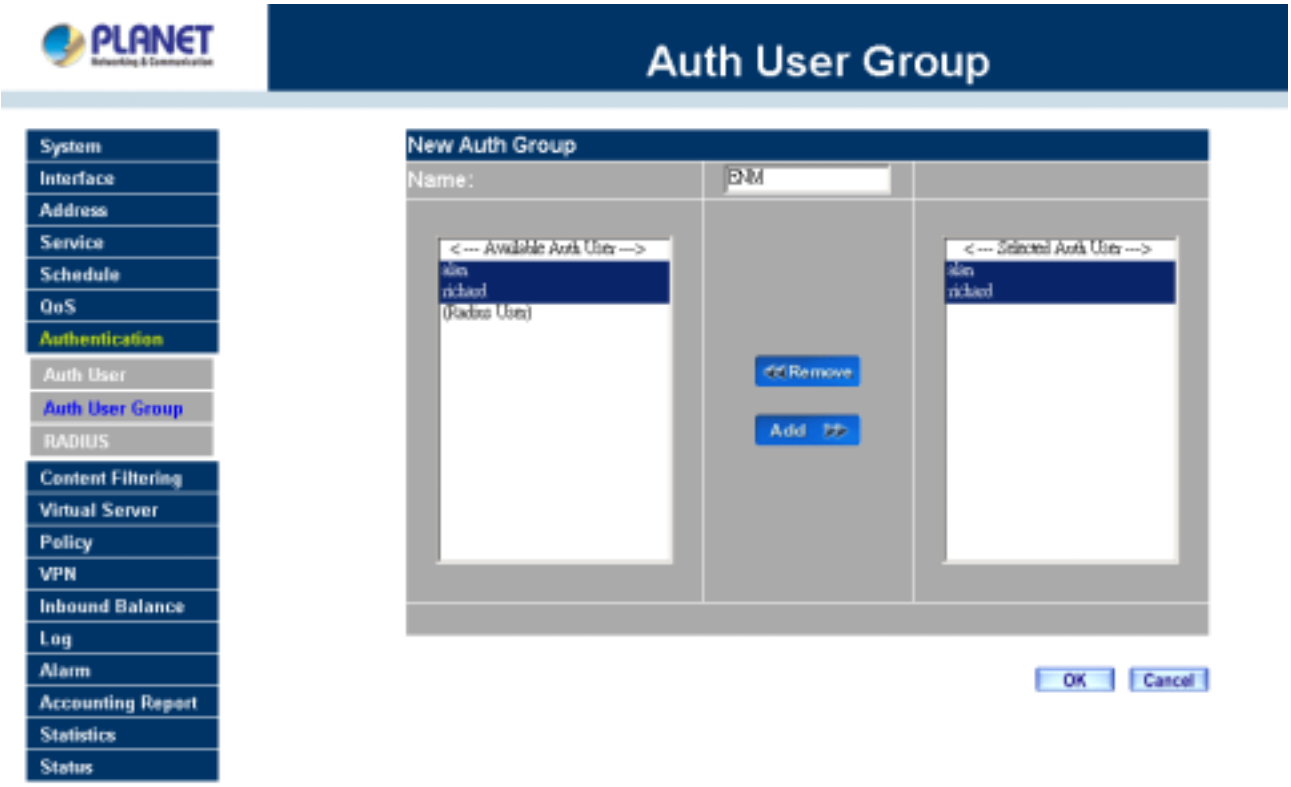
Step 2. The Remove confirmation pop-up box will appear.

Step 3. Click **OK** to remove that Authentication User or click **Cancel** to cancel.

4.7.2 Auth User Group

Accessing the Auth User Group window

Click **Authentication** in the menu bar on the left hand side of the window. Click **Auth User Group** under it. A window will appear with a table displaying current Auth User Group settings by the Administrator.



Adding Auth User Group

Step 1. In the Auth User Group window, click the **New Entry** button.

In the Auth User Group window, the following fields will appear:

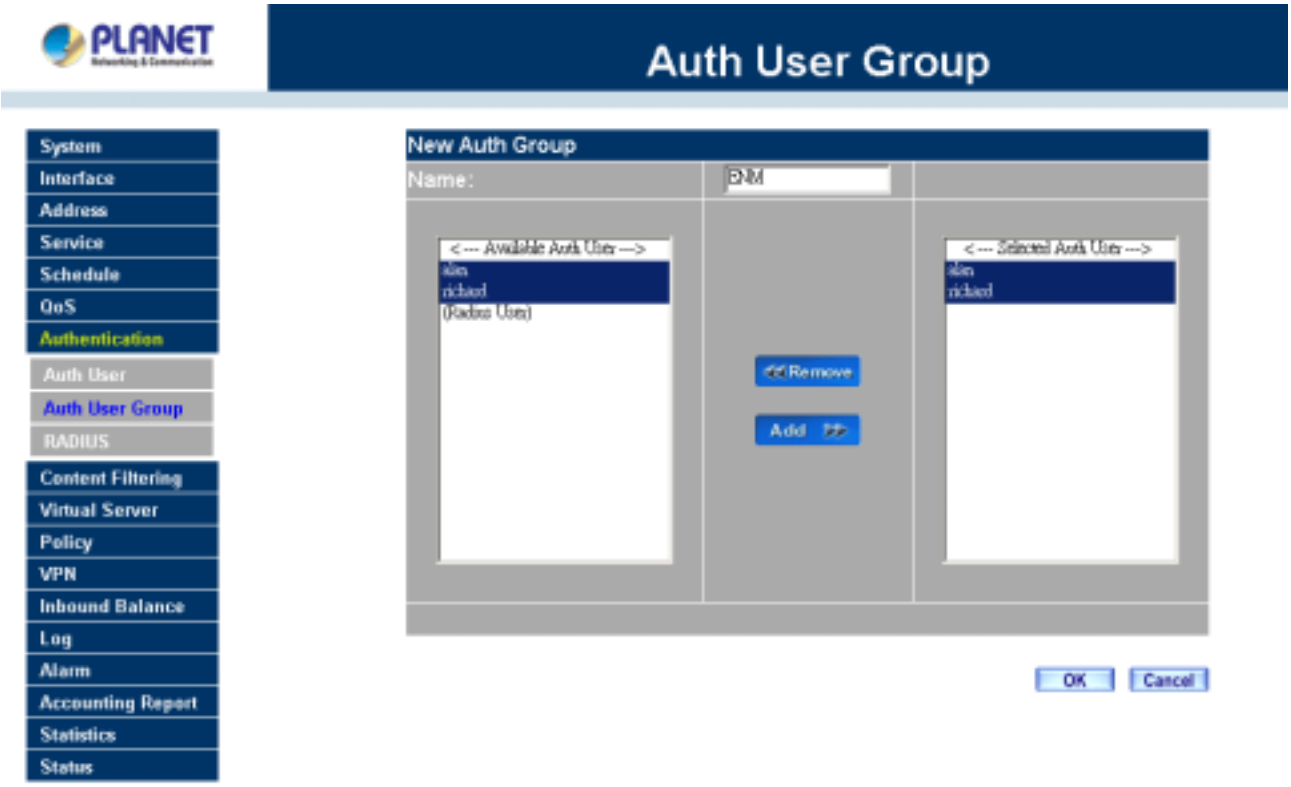
- **Name:** Enter the new Auth User group name.
- **Available auth user:** List all the available Auth User.
- **Selected auth user:** List Auth User to be assigned to the new group.

Step 2. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new Auth User:** Select the Auth User desired to be added in the **Available auth user** list, and then click the **Add>>** button to add them to the group.

Step 5. **To remove Auth User:** Select Auth User desired to be removed in the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.



Modifying Auth User Group

Step 1. In the Auth User Group window, locate the Auth User Group to be edited. Click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Modify Auth group** window the following fields are displayed::

- **Name:** Enter the new Auth User group name .
- **Available auth user:** List all the available Auth User.
- **Selected auth user:** List Auth User to be assigned to the new group.

Step 3. **To add new Auth User:** Select the Auth User desired to be added in the **Available auth user** list, and then click the **Add>>** button to add them to the group.

Step 4. **To remove Auth User:** Select Auth User desired to be removed in the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.

Step 5. Click **OK** to modify the Group.

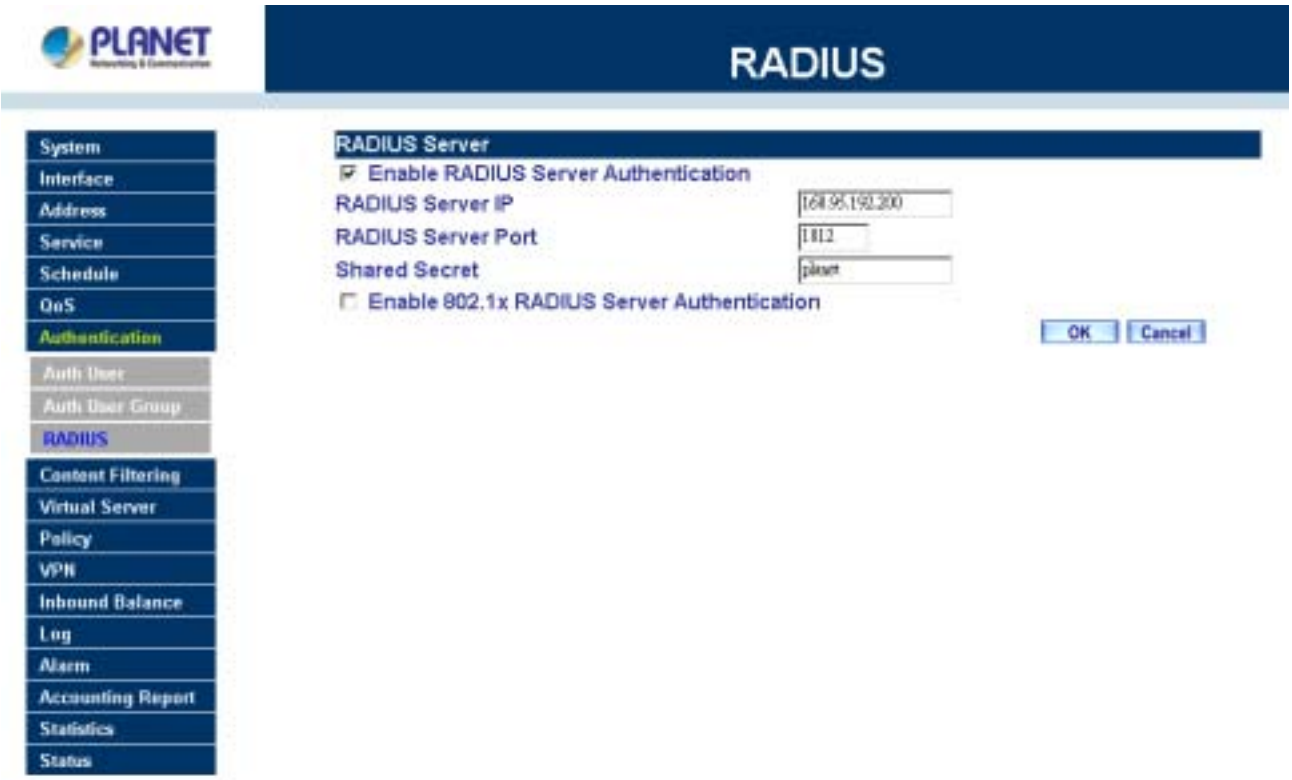
Removing Auth User Group

Step 1. In the **Auth User Group** window, locate the Auth User Group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.

4.7.3 Radius Server

Click **Authentication** on the left side menu bar, then click **Radius Server** below it. The following window is shown.



Definition

- **Enable RADIUS Server**: Enable RADIUS Server Authentication.
- **RADIUS Server IP**: Enter RADIUS Server IP address.
- **RADIUS Server Port**: Enter RADIUS Server Port. The default port is 1812.
- **Shared Secret**: The Password for the Multi-Homing Security Gateway to access RADIUS Server.
- **Enable 802.1x RADIUS Server Authentication**: The Multi-Homing Security Gateway enable 802.1x RADIUS Server Authentication.

4.8 Content filtering

Content Filtering includes "**URL Blocking**" and "**General Blocking**". MH-4000 also includes "**P2P Blocking** , **IM Blocking** and **Download Blocking** .

URL Blocking: The administrator can use a complete domain name or key word to make rules for specific websites.

General Blocking: To let Popup、ActiveX、Java、Cookie in or keep them out.

P2P Blocking: Block P2P program, include "eDonkey" and "Bit Torrent ".

IM Blocking: Block Internet Message program, include "MSN", "Yahoo Messenger" and "ICQ".

Download Blocking: Block download connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

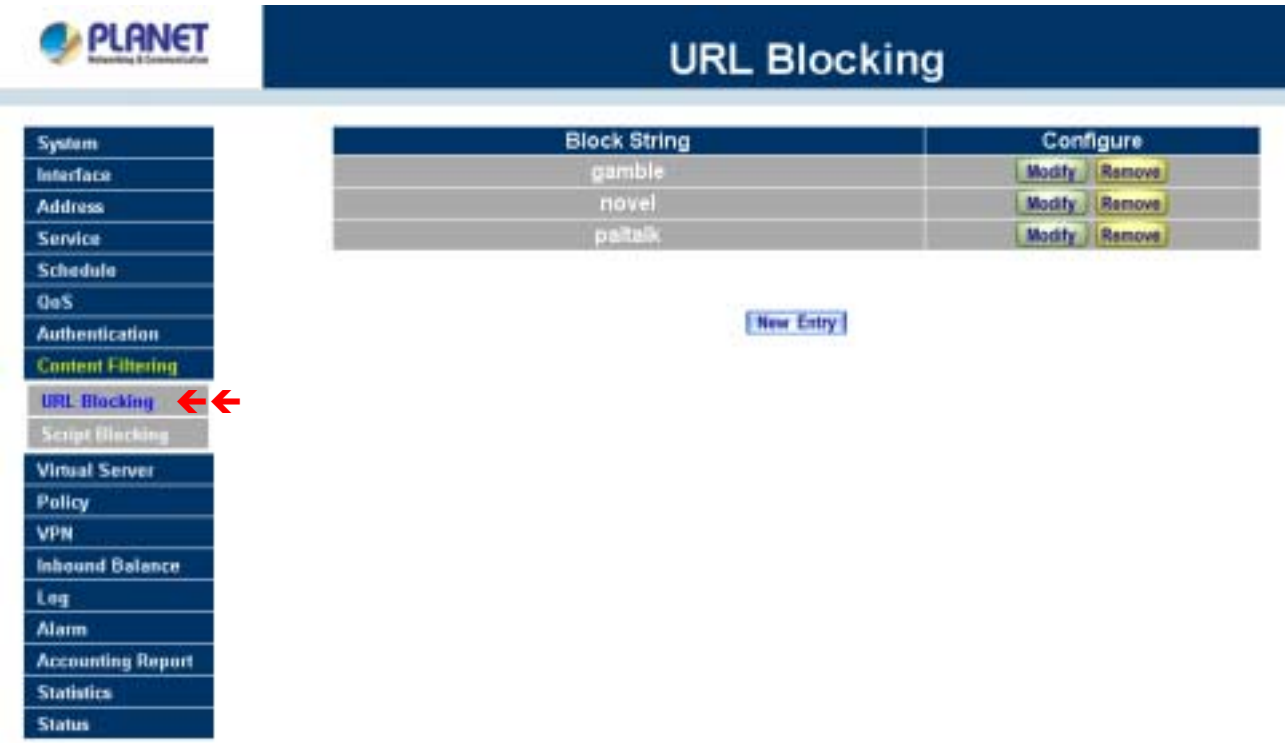
4.8.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from an LAN network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window

Step 1. Click on **URL Blocking** under the **Configuration** menu bar.

Step 2. Click on **New Entry.**



Definition:

Block String: The domain name that is blocked to enter by Multi-Homing Security Gateway.

Configuration: To change the settings of URL Blocking, click **Modify** to change the parameters; click **Delete** to delete the settings.

Adding a URL Blocking policy

Step 1. After clicking **New Entry**, the **Add New Block String** window will appear.

Step 2. Enter the URL of the website to be blocked.

Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.

Modifying a URL Blocking Policy

Step 1. In the **URL Blocking** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2. Make the necessary changes needed.

Step 3. Click on **OK** to save changes or click on **Cancel** to discard changes.

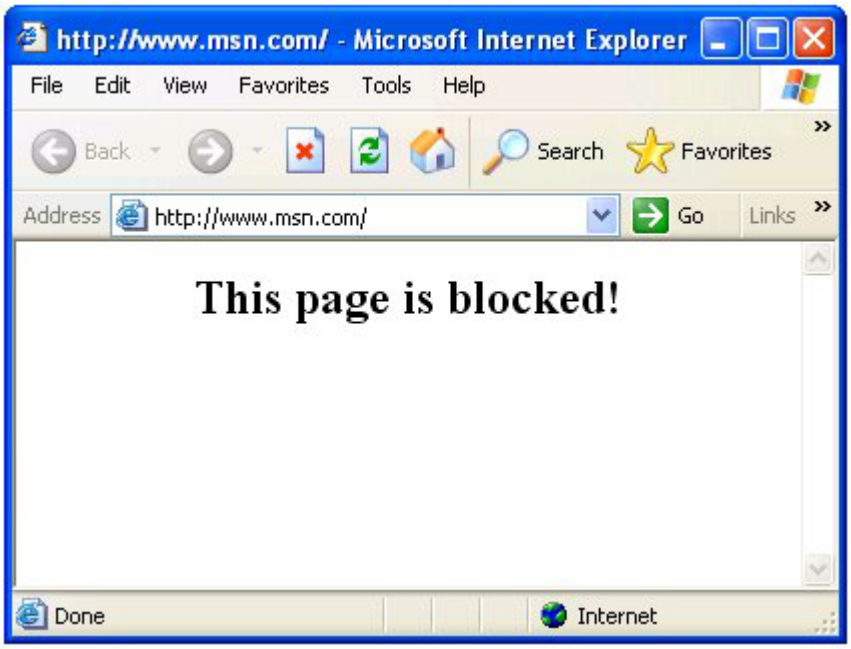
Removing a URL Blocking policy

Step 1. In the **URL Blocking** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the policy or click on **Cancel** to discard changes.

Blocked URL site:

When a user from the LAN network tries to access a blocked URL, the error below will appear.



4.8.2 General Blocking

To let Popup, ActiveX, Java, or Cookies in or keep them out.

Step 1: Click **Content Filtering** in the menu.

Step 2: **General Blocking** detective functions.

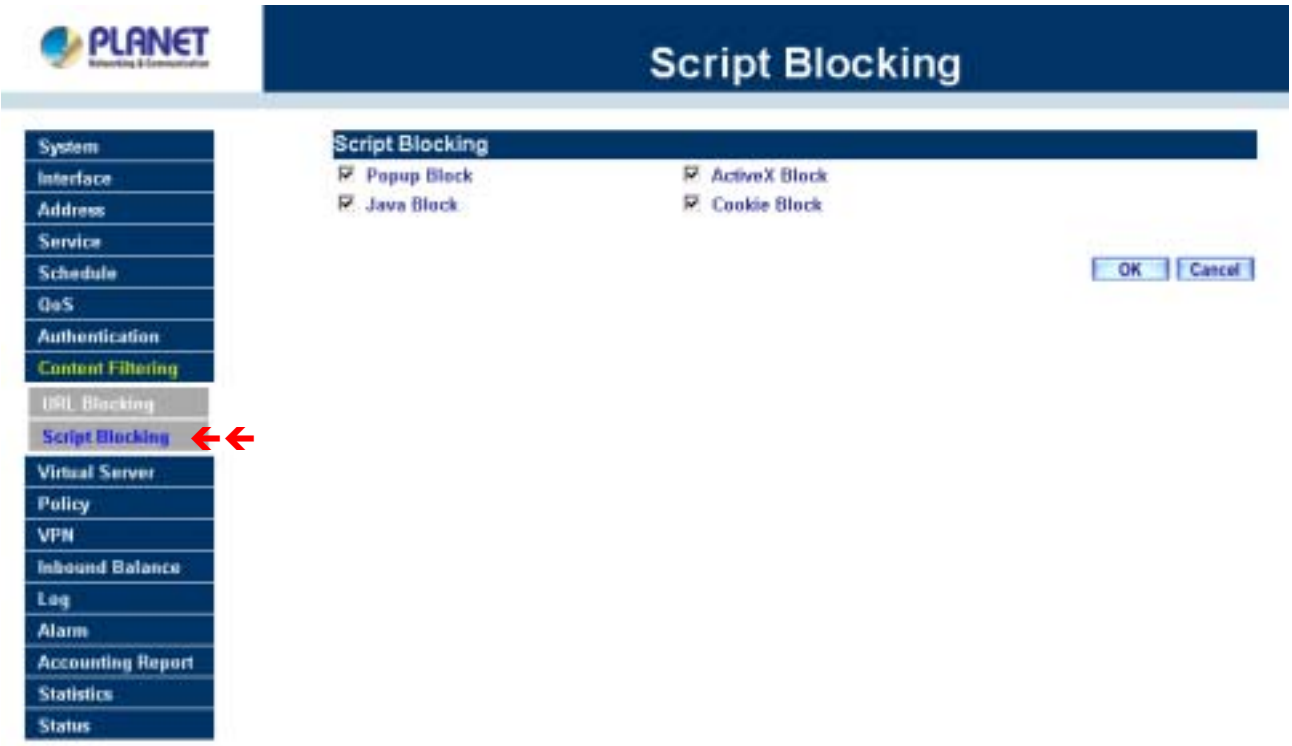
Popup filtering: Prevent pop-up boxes from appearing.

ActiveX filtering: Prevent ActiveX packets.

Java filtering: Prevent Java packets.

Cookie filtering: Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.



When the system detects the setting, the Multi-Homing Security Gateway will spontaneously work**.**

4.8.3 P2P Blocking (MH-4000 only)

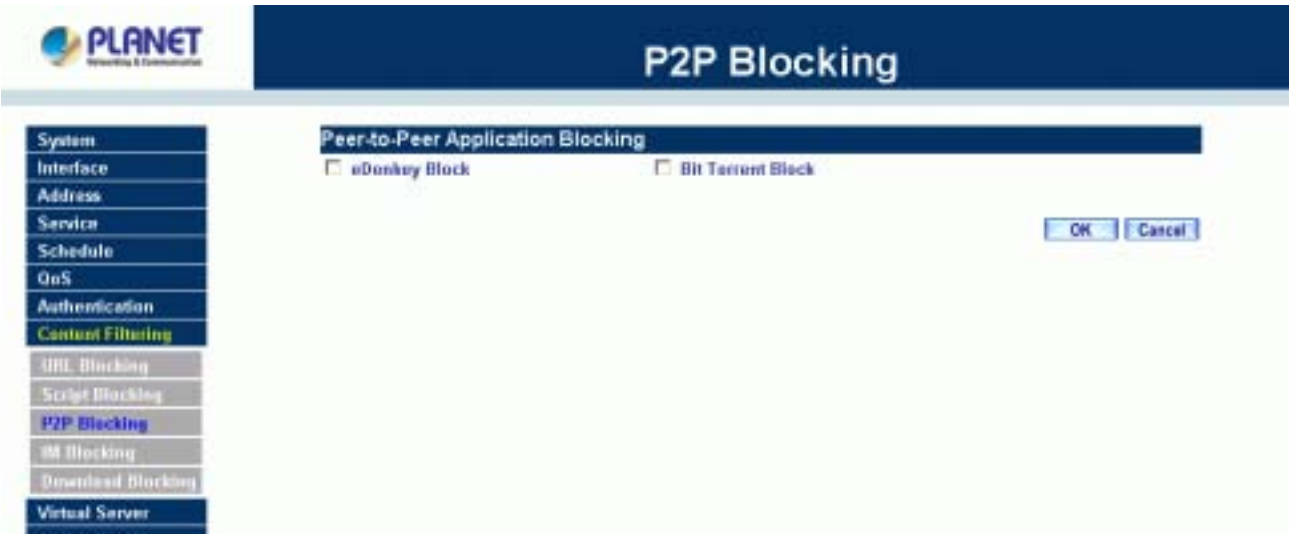
Step 1: Click **Content Filtering** in the menu.

Step 2: Select **P2P Blocking** and configure the setting.

eDonkey Block: Prevent eDonkey connection built up.

Bit Torrent Block: Prevent Bit Torrent connection built up.

Step 3: After selecting each function, click the **OK** button below.



4.8.4 IM Blocking (MH-4000 only)

Step 1: Click **Content Filtering** in the menu.

Step 2: Select **IM Blocking** and configure the setting.

MSN Messenger Blocking: To select to block MSN Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

Yahoo Messenger Blocking: To select to block Yahoo Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

ICQ Blocking: Only to select to block ICQ **login**.

Step 3: After selecting each function, click the **OK** button below.

4.8.5 Download Blocking (MH-4000 only)

Step 1: Click **Content Filtering** in the menu.

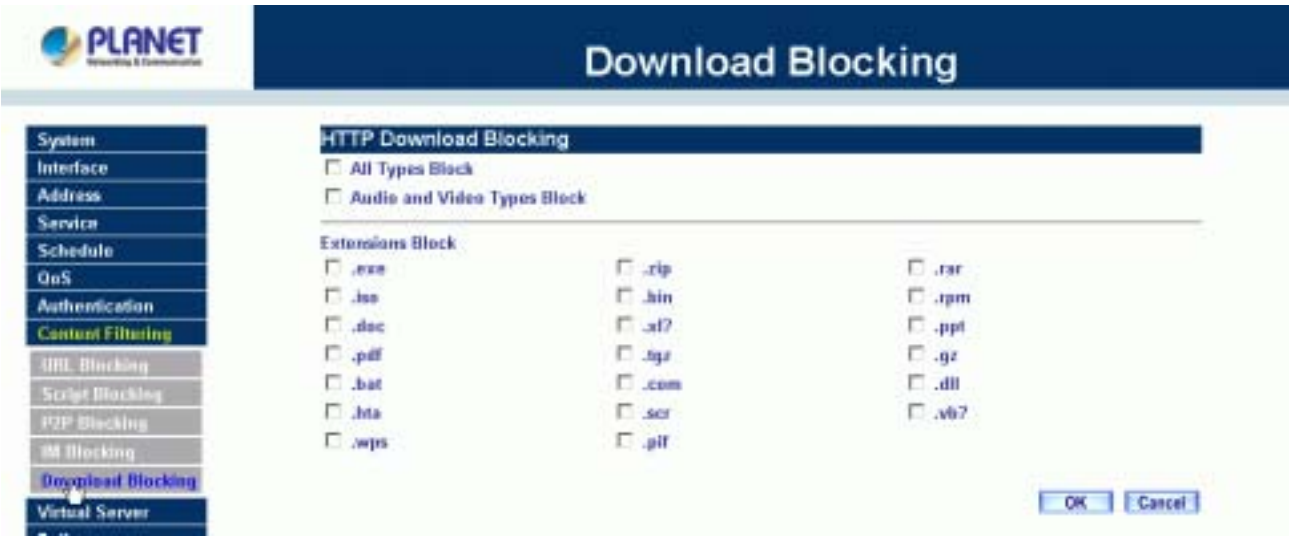
Step 2: Select **Download Blocking** and configure the setting.

All Types Block: To block all types of the files downloading from web page.

Audio and Video Types block: To block audio and video downloading from web page..

Extensions Block: To block specific extensions name of the files from web page.

Step 3: After selecting each function, click the **OK** button below.



4.9 Virtual Server

The Multi-Homing Security Gateway separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through Multi-Homing Security Gateway's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

The Multi-Homing Security Gateway's Virtual Server can solve this problem. A virtual server has set the real IP address of the Multi-Homing Security Gateway's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Multi-Homing Security Gateway translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping (also called DMZ, De-Militarization Zone) scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which is opposite to NAT), but there are still some differences:

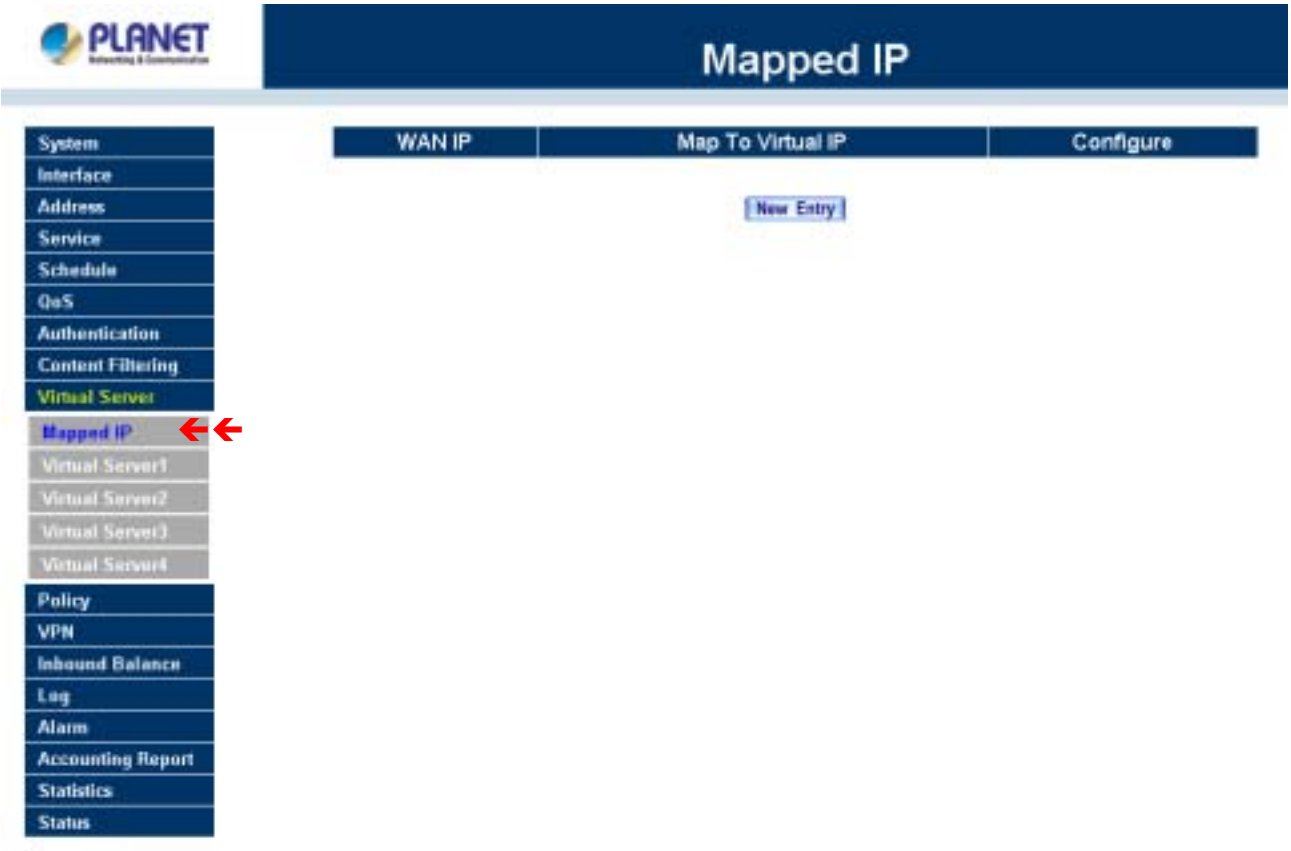
- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

4.9.1 Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real WAN IP address is mapped to one private LAN IP address.

Entering the Mapped IP window

Step 1. Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.



Definition:

WAN IP: WAN IP Address.

Map to Virtual IP: The IP address which WAN maps to the virtual network in the server.

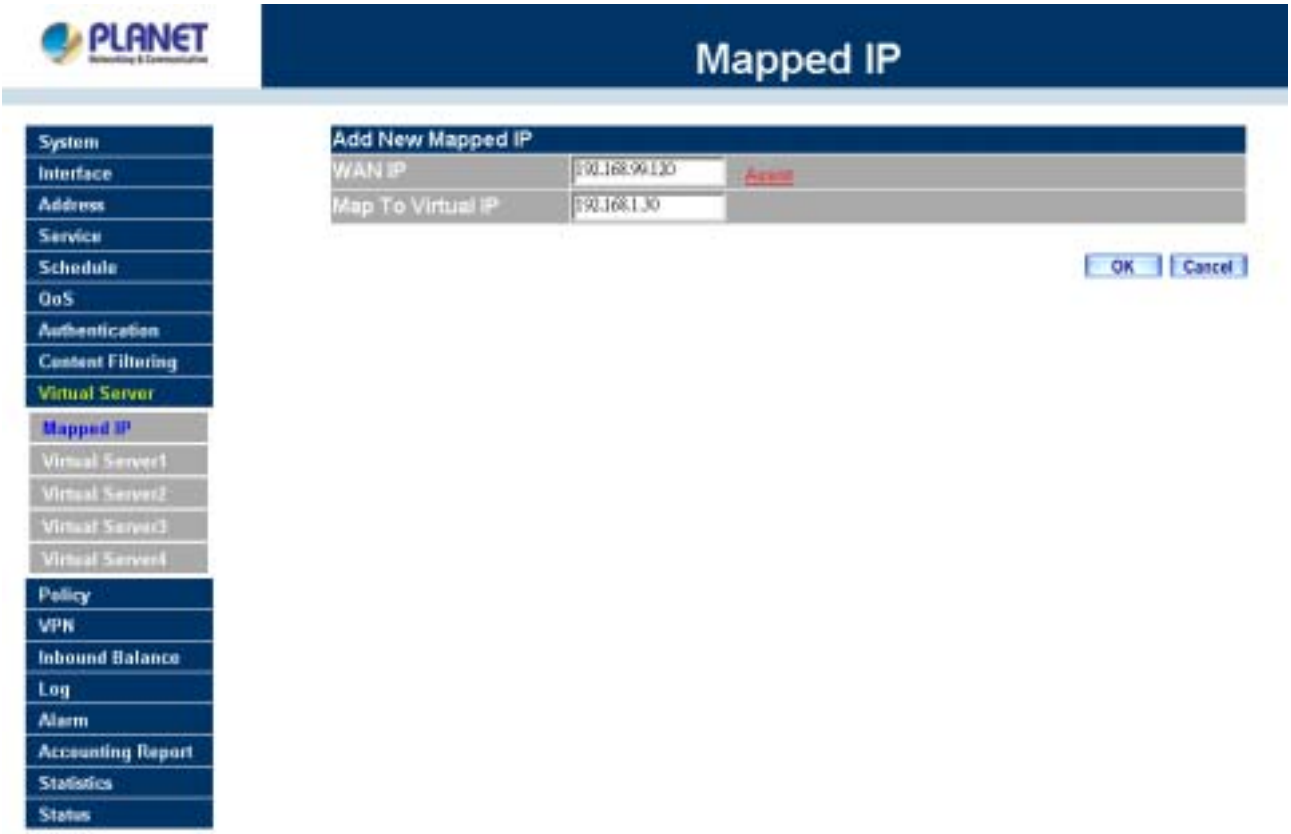
Configure: To change the setting, click Configure to modify the parameters; click delete to delete the setting.

Adding a new IP Mapping

Step 1. In the **Mapped IP** window, click the New Entry button. The Add New Mapped IP window will appear.

- **WAN IP**: select the WAN public IP address to be mapped.
- **Internal IP**: enter the LAN private IP address will be mapped 1-to-1 to the WAN IP address.

Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.

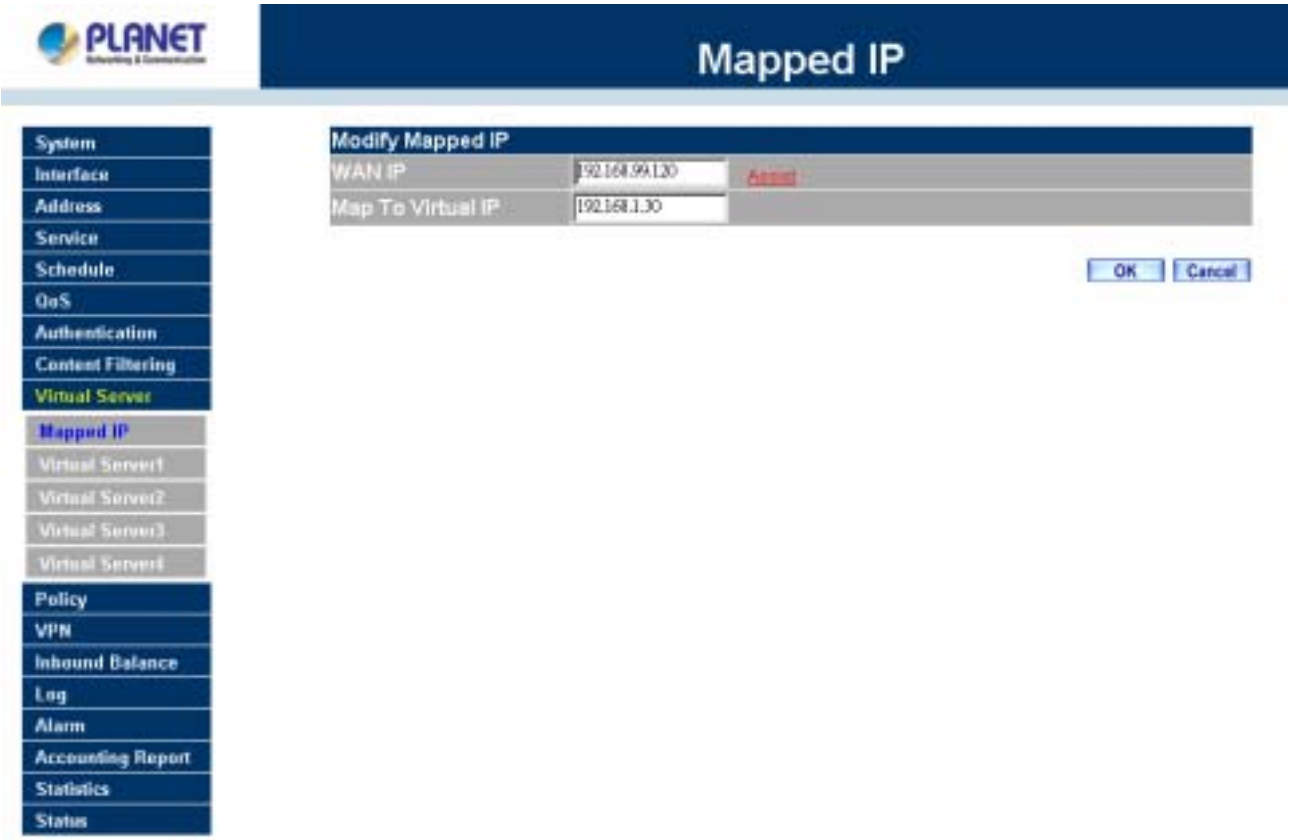


Modifying a Mapped IP

Step 1. In the **Mapped IP** table, locate the Mapped IP you want it to be modified and click its corresponding Modify option in the Configure field.

Step 2. Enter settings in the Modify Mapped IP window.

Step 3. Click **OK** to save change or click **Cancel** to cancel.



NOTE: A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.

Removing a Mapped IP

Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up window, click **OK** to remove the Mapped IP or click **Cancel** to cancel.

4.9.2 Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds a WAN IP to a LAN IP, virtual server binds WAN IP ports to LAN IP ports.

Definition:

Virtual Server IP: The WAN IP address configured by the virtual server. Click "**Click here to configure**" button to add new virtual server address.

Service name: The service names that provided by the virtual server.

WAN Port: The TCP/UDP ports that present the service items provided by the virtual server.

Server Virtual IP: The virtual IP which mapped by the virtual server.

Configure: To change the service configuration, click **Configure** to change the parameters; click **Delete** to delete the configuration.

This virtual server provides four real IP addresses, which means you can setup four virtual servers at most （Setup under the Virtual Server sub-selections Virtual Server 1/2/3/4 in the menu bar on the left hand side.）

The administrator can select Virtual Server1/2/3/4 under Virtual Server selection in the menu bar on the left hand side, click **Server Virtual IP** to add or change the virtual server IP address; click **Click here to configure** to add or change the virtual server service configuration.

Adding a Virtual Server

Step 1. Click an available virtual server from **Virtual Server** in the **Virtual Server** menu bar to enter the virtual server configuration window. In the following, Virtual Server is assumed to be the chosen option:

Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and

asks for an IP address from the WAN network.

Step 3. Select an IP address from the drop-down list of available WAN network IP addresses.

Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.

Modifying a Virtual Server IP Address

Step 1. Click the virtual server to be modified Virtual Server under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.

Step 2. Click on the Virtual Server's IP Address button at the top of the screen.

Step 3. Choose a new IP address from the drop-down list.

Step 4. Click **OK** to save new IP address or click **Cancel** to discard changes.

Removing a Virtual Server

Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.

Step 2. Click the Virtual Server's IP Address button at the top of the screen.

Step 3. Delete the IP address.

Step 4. Click **OK** to remove the virtual server.

Setting the Virtual Server s services

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

Step 2. In the Virtual Server Configurations window:

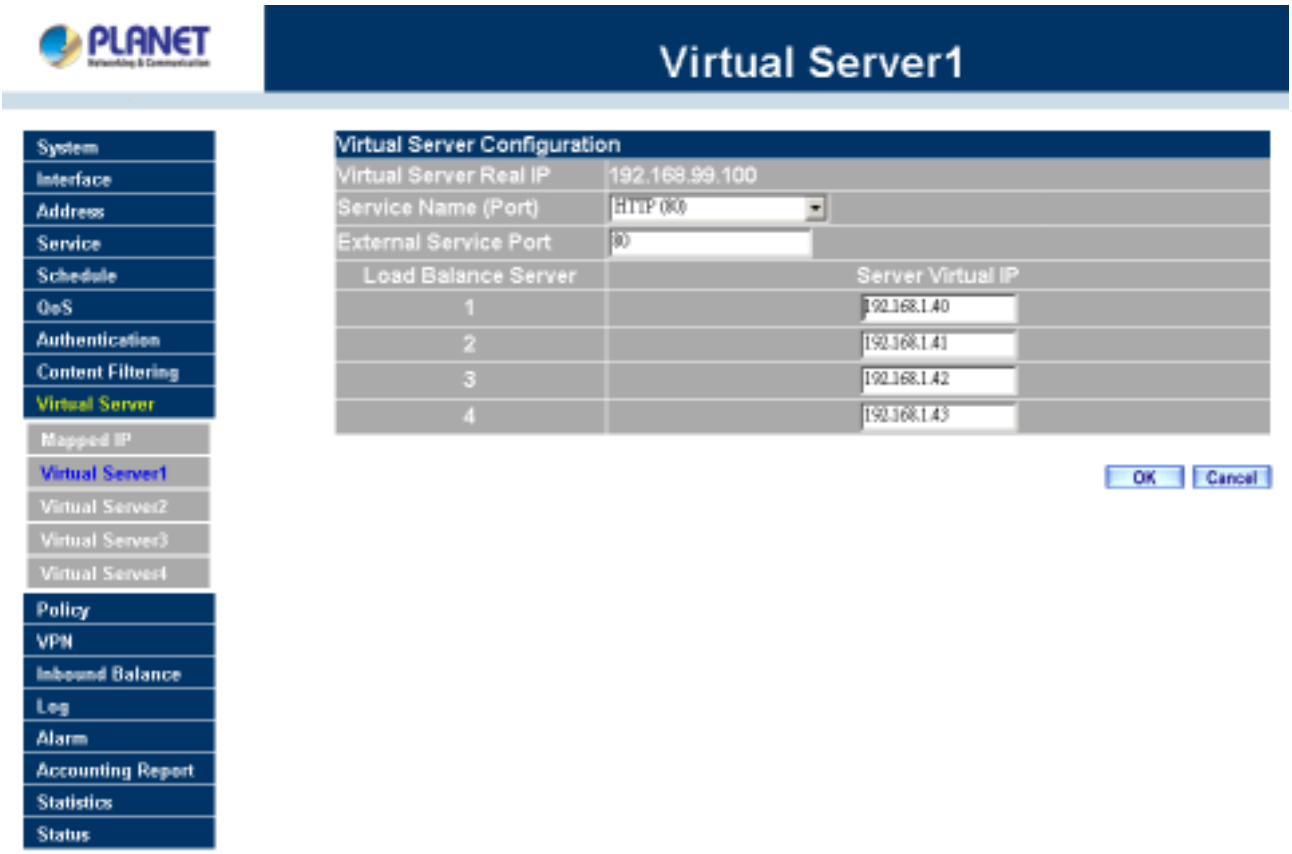
- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- **Service Name (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Step 3. Enter the IP address of the LAN network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

NOTE: The services in the drop-down list are all defined in the Pre-defined and Custom section of the

Service menu.

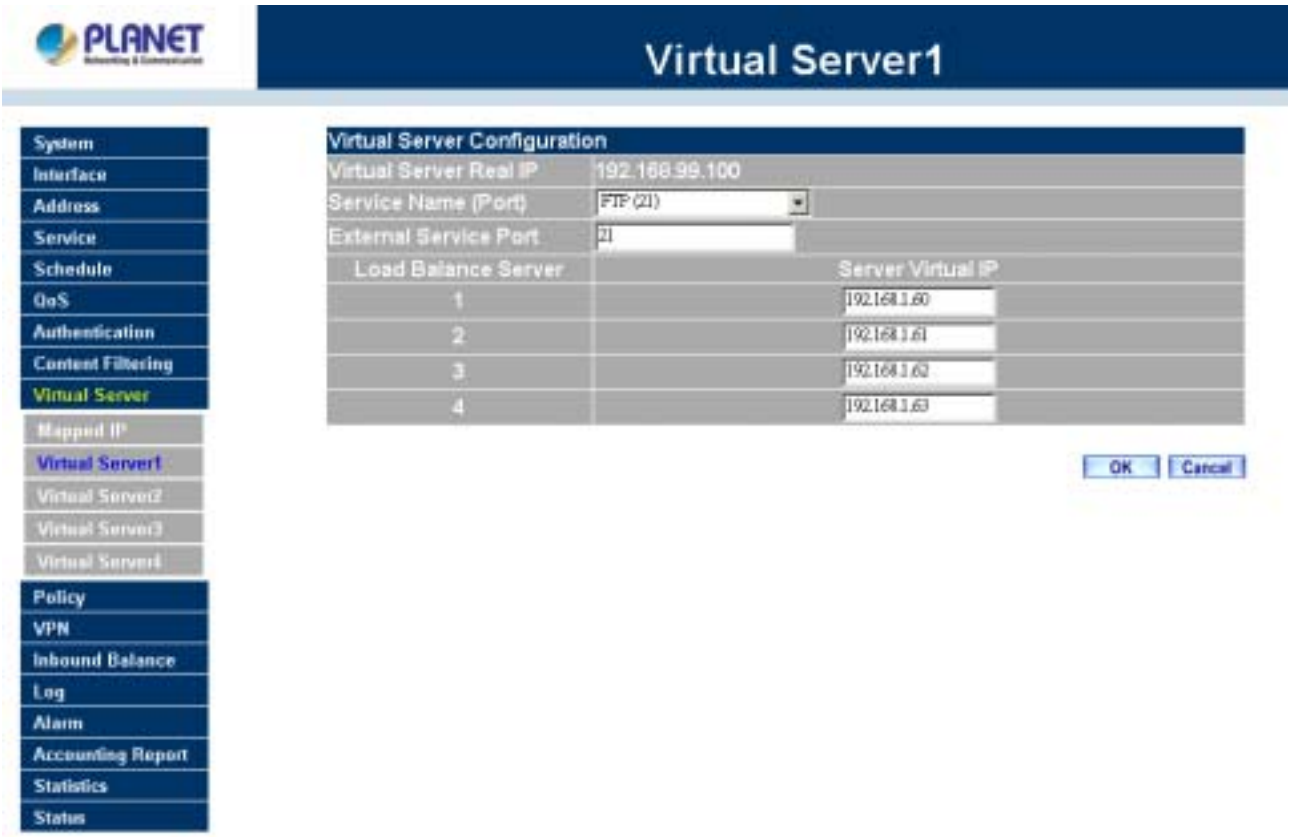


Adding New Virtual Server Service Configuration

Step 1. Select Virtual Server in the menu bar on the left hand side, and then select Virtual Server 1/2/3/4 sub-selections.

Step 2. In Virtual Server 1/2/3/4 Window, click "**New Entry**" button.

Step 3. Enter the parameters in the Virtual Server Configuration column.



- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- **Service Name (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.

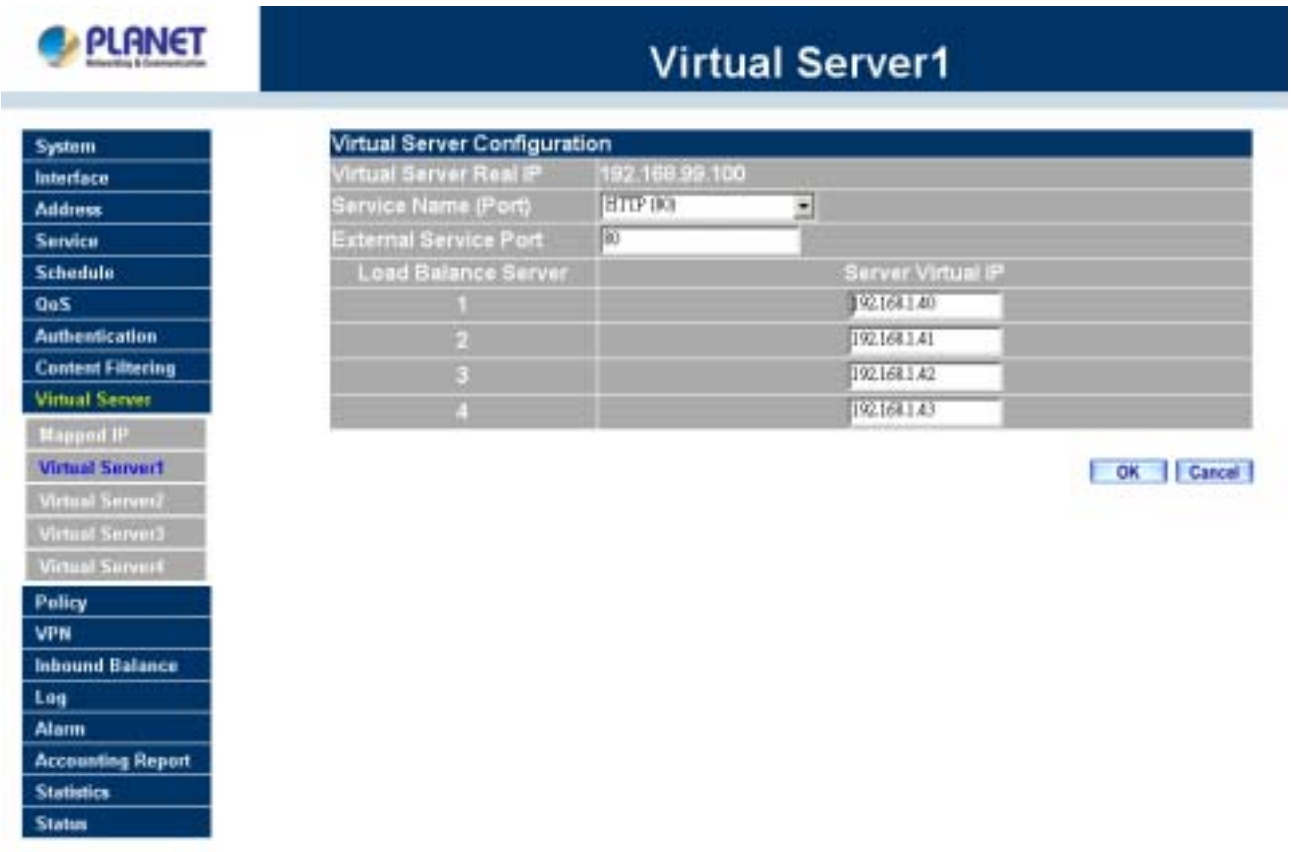
Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.

Modifying the Virtual Server configurations

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. In the Virtual Server Configuration window, enter the new settings.

Step 3. Click **OK** to save modifications or click **Cancel** to discard changes.



Click **OK** to execute the change of the virtual server, or click **Cancel** to discard changes.

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server, you have to remove this configuration of Policy, and then you can execute the modification or configuration.

Removing the Virtual Server service

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the service or click **Cancel** to cancel removing.

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server unless you have already removed this configuration of Policy.

4.10 Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Multi-Homing Security Gateway.

What is Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

(1)Outgoing: a client is in the LAN networks while a server is in the WAN 1/2 networks.

(2) Incoming, a client is in the WAN 1/2 networks, while a server is in the LAN networks.

(3) To DMZ: a client is either in the LAN networks or in the WAN networks while, server is in DMZ.

(4) From DMZ, a client is in DMZ while server is either in the LAN networks or in the WAN networks.

How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

Policy Directions:

Step 1. In **Address**, set names and addresses of source networks and destination networks.

Step 2. In **Service**, set services.

Step 3. In **Virtual Server**, set names and addresses of mapped IP or virtual server (only applied to **Incoming policies**).

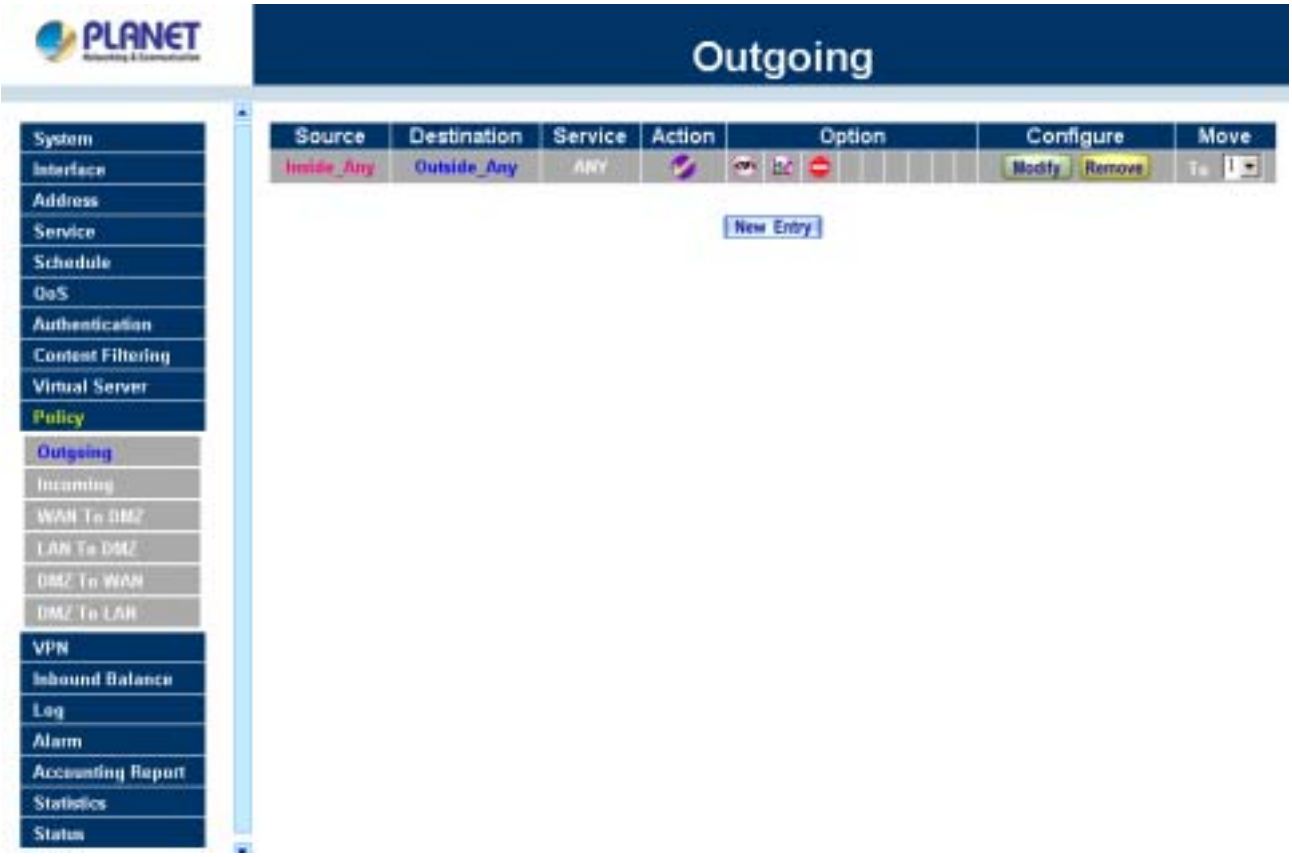
Step 4. Set control policies in **Policy.**

4.10.1 Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN 1/2 network.

Entering the Outgoing window:

Click **Policy** on the left hand side menu bar, then click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.

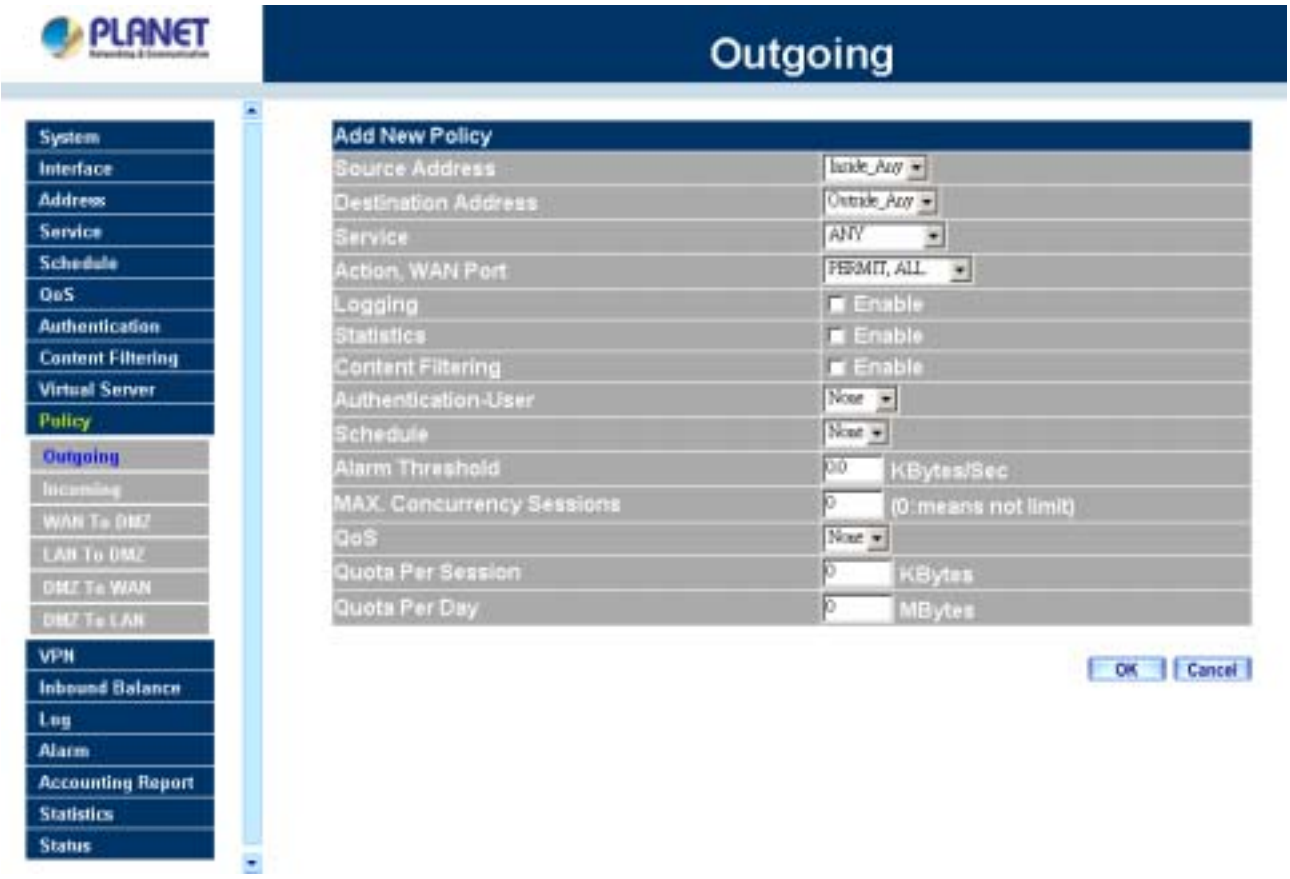


The fields in the Outgoing window are:

- **Source:** source network addresses that are specified in the LAN section of **Address** menu, or all the LAN network addresses.
- **Destination:** destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- **Service:** specify services provided by WAN network servers.
- Action: control actions to permit or deny packets from LAN networks to WAN 1/2 network travelling through the Multi-Homing Security Gateway.
- **Option:** specify the monitoring functions on packets from LAN networks to WAN 1/2 networks travelling through the Multi-Homing Security Gateway.
- **Configure:** modify settings.
- **Move:** this sets the priority of the policies, number 1 being the highest priority.

Adding a new Outgoing Policy

Step 1: Click on the New Entry button and the Add New Policy window will appear.



Step 2: Configure all the parameters.

Source Address: Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

Destination Address: Select the name of the WAN 1/2 network from the drop down list. The drop down list contains the names of all WAN 1/2 networks defined in the WAN 1/2 section of the **Address** window. To create a new destination address, please go to the WAN 1/2 section under the **Address** menu.

Service: Specified services provided by WAN 1/2 net work servers. These are services/application that are allowed to pass from the LAN network to the WAN 1/2 network. Choose ANY for all services.

Action: Select Permit, Permit WAN 1, Permit WAN 2 or Deny from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Authentication-User: Select the item listed in the Authentication-User to enable the policy to automatically execute the function in a certain time and range.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Quota Per Session: The maximum throughput quota(in Kbytes/Sec) per session.

Quota Per Day: The maximum throughput quota(in Kbytes/Sec) per day.

Step 3: Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

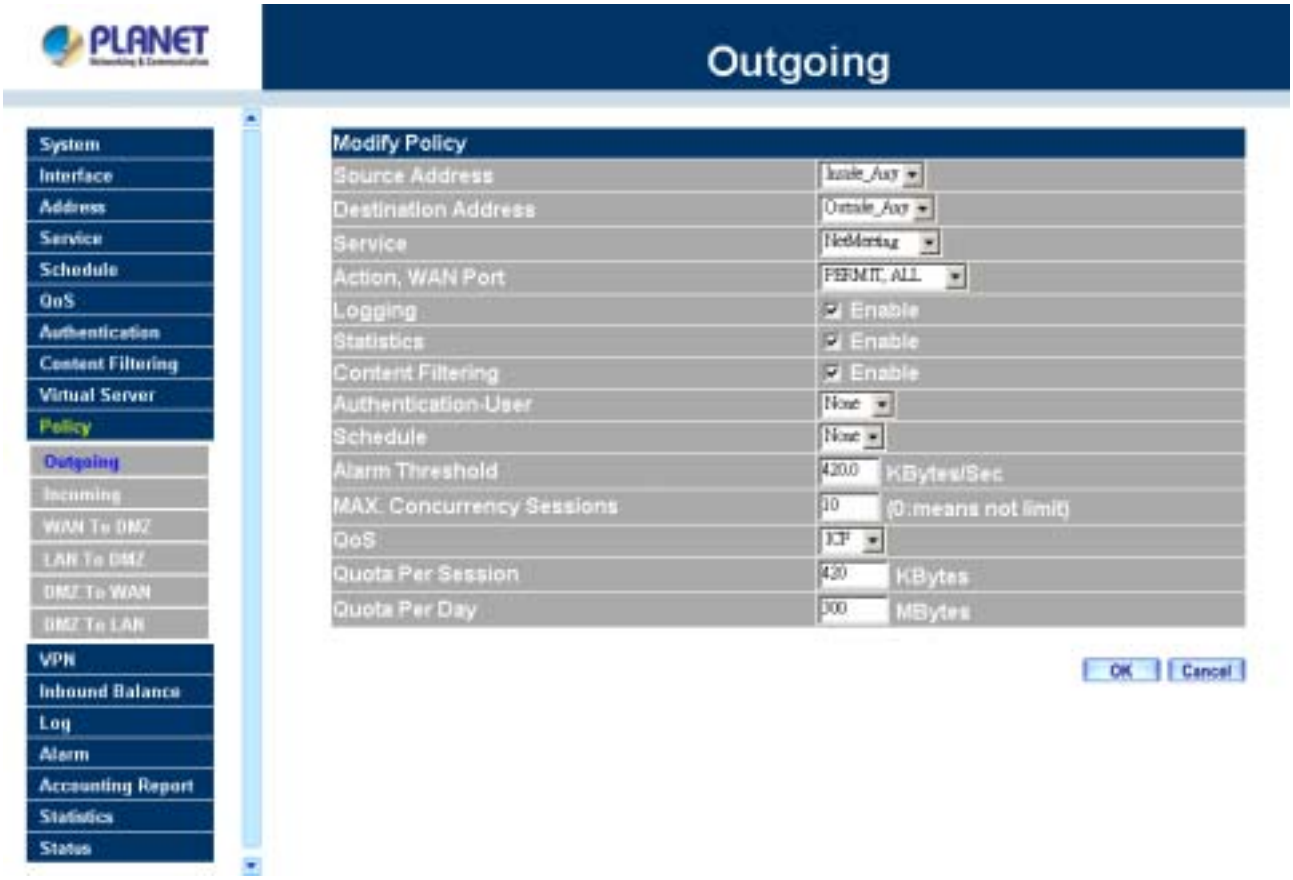
Modifying an Outgoing policy

Step 1: In the **Outgoing** policy section, locate the name of the policy desired to be modified and click its corresponding Modify option under the Configure field.

Step 2: In the **Modify Policy** window, fill in new settings.

NOTE: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→ [Pre-defined], [Custom] or Group under **Service**).

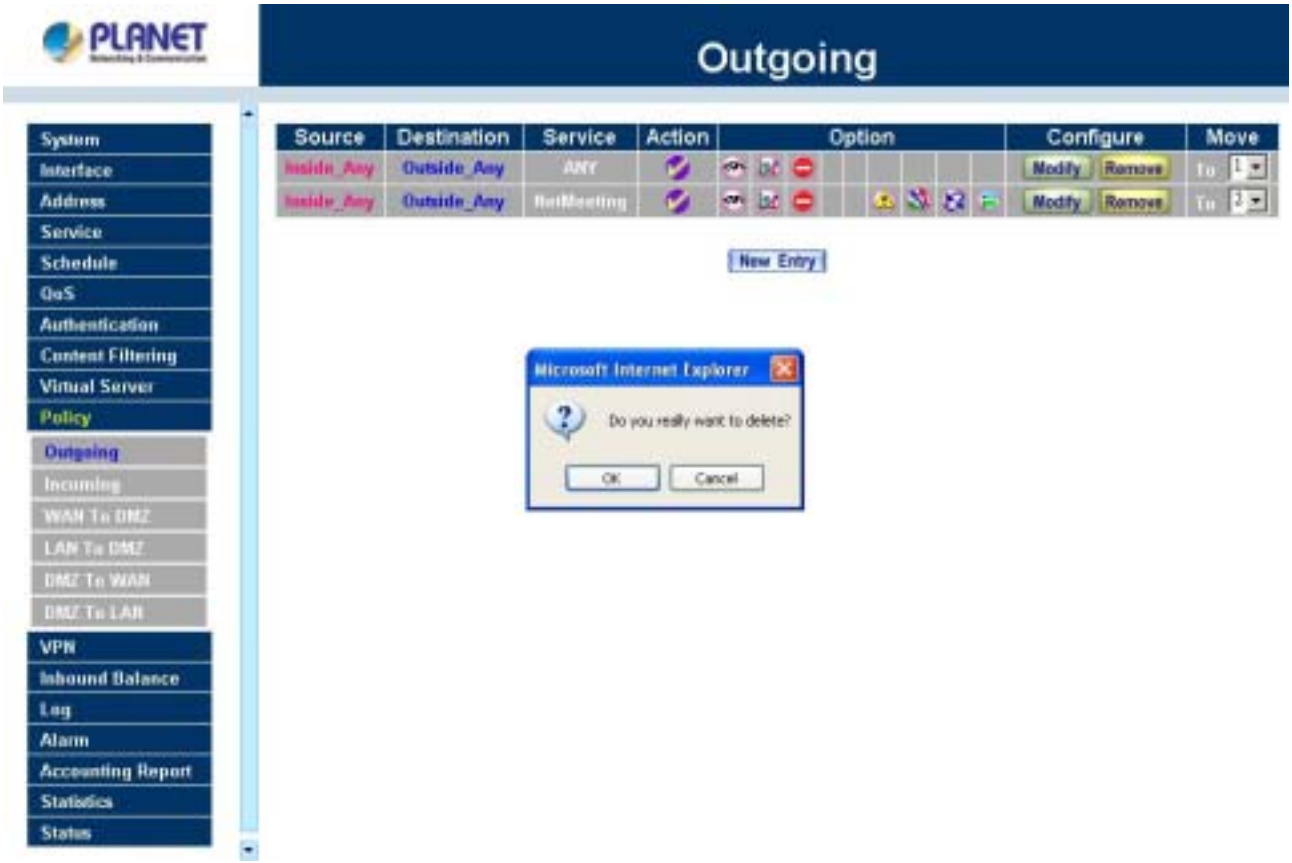
Step 3: Click **OK** to do confirm modification or click **Cancel** to cancel it.



Removing the Outgoing Policy

Step 1. In the **Outgoing** policy section, locate the name of the policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.



Enabled Monitoring function:

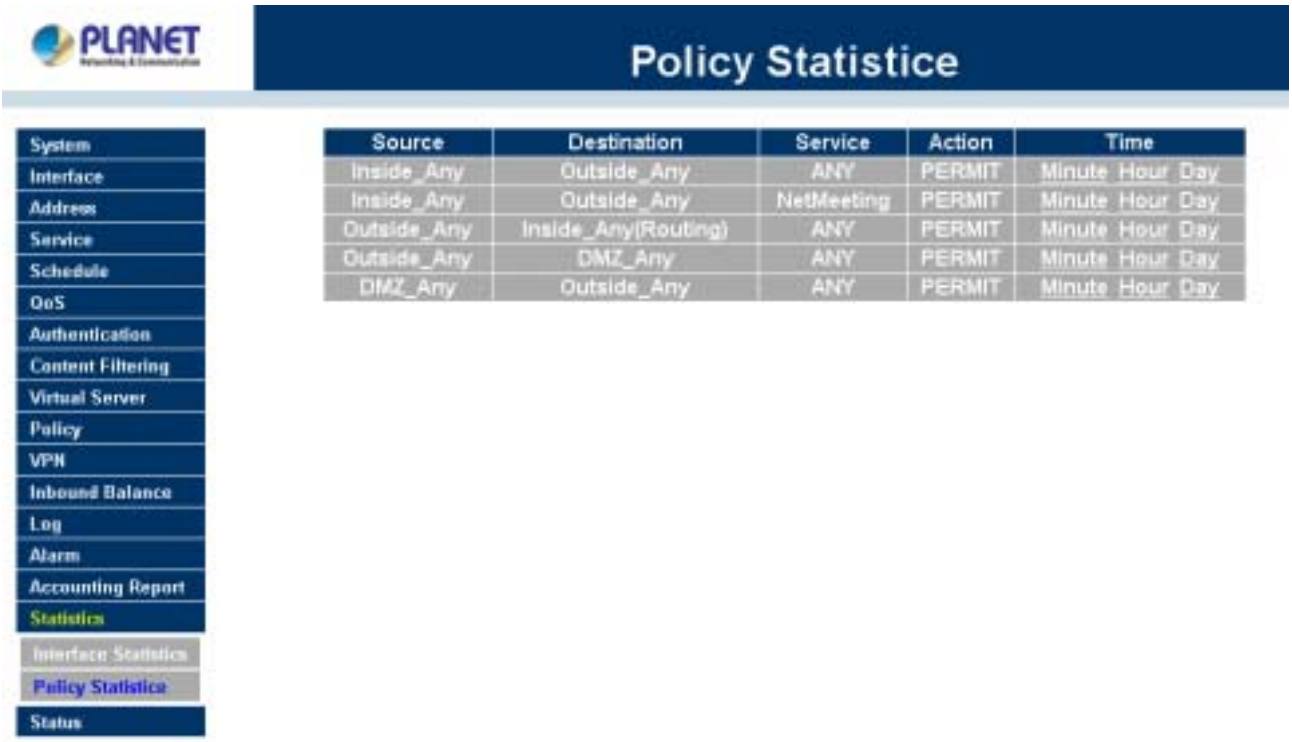
Log: If Logging is enabled in the outgoing policy, the Multi-Homing Security Gateway will log the traffic and event passing through the Multi-Homing Security Gateway. The Administrator can click **Log** on the left menu bar to get the traffic and event logs of the specified policy.

NOTE: System Administrator can back up and clear logs in this window. Check **the chapter entitled Log** to get details about the log and ways to back up and clear logs.

Alarm: If Logging is enabled in the outgoing policy, the Multi-Homing Security Gateway will log the traffic alarms and event alarms passing through the Multi-Homing Security Gateway. The Administrator can click **Alarm** on the left menu to get the logs of flow and event alarms of the specified policy.

NOTE: The Administrator can also get information on alarm logs from the Alarm window. Please refer to the section entitled "**Alarm** for more information.

Statistics: If statistics is enabled in the outgoing policy, the Multi-Homing Security Gateway will display the flow statistics passing through the Multi-Homing Security Gateway.



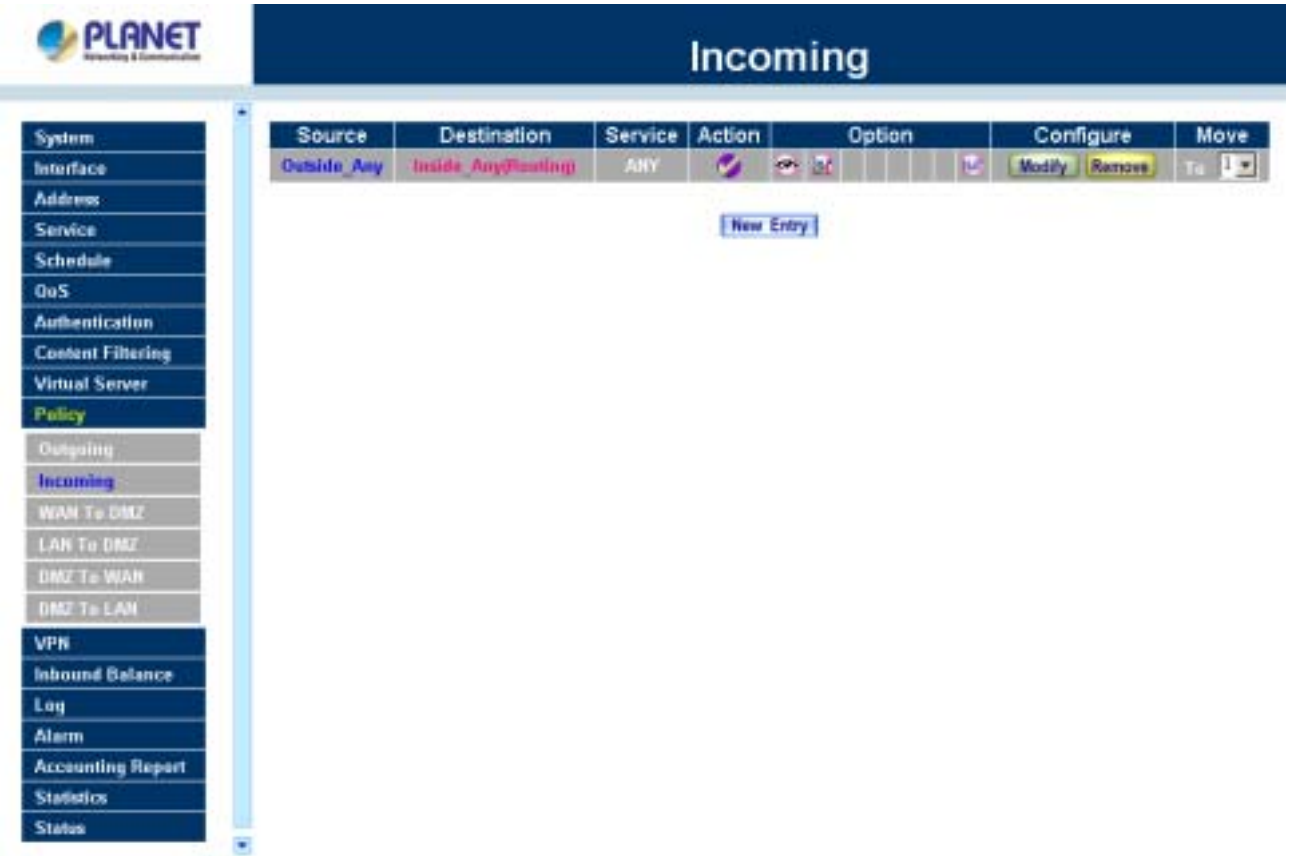
NOTE: The Administrator can also get flow statistics in **Statistics**. Please refer to **Statistics** in Chapter 11 for more details.

4.10.2 Incoming

This section describes steps to create policies for packets and services from the WAN 1/2 network to the LAN network including Mapped IP and Virtual Server.

Enter Incoming window

Step 1: Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the WAN 1/2 network to assigned Mapped IP or Virtual Server.



Step 2: The fields of the **Incoming** window are:

- **Source:** source networks which are specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.
- **Destination:** destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.
- **Service:** services supported by Virtual Servers (or Mapped IP).

■ **Action:** control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.

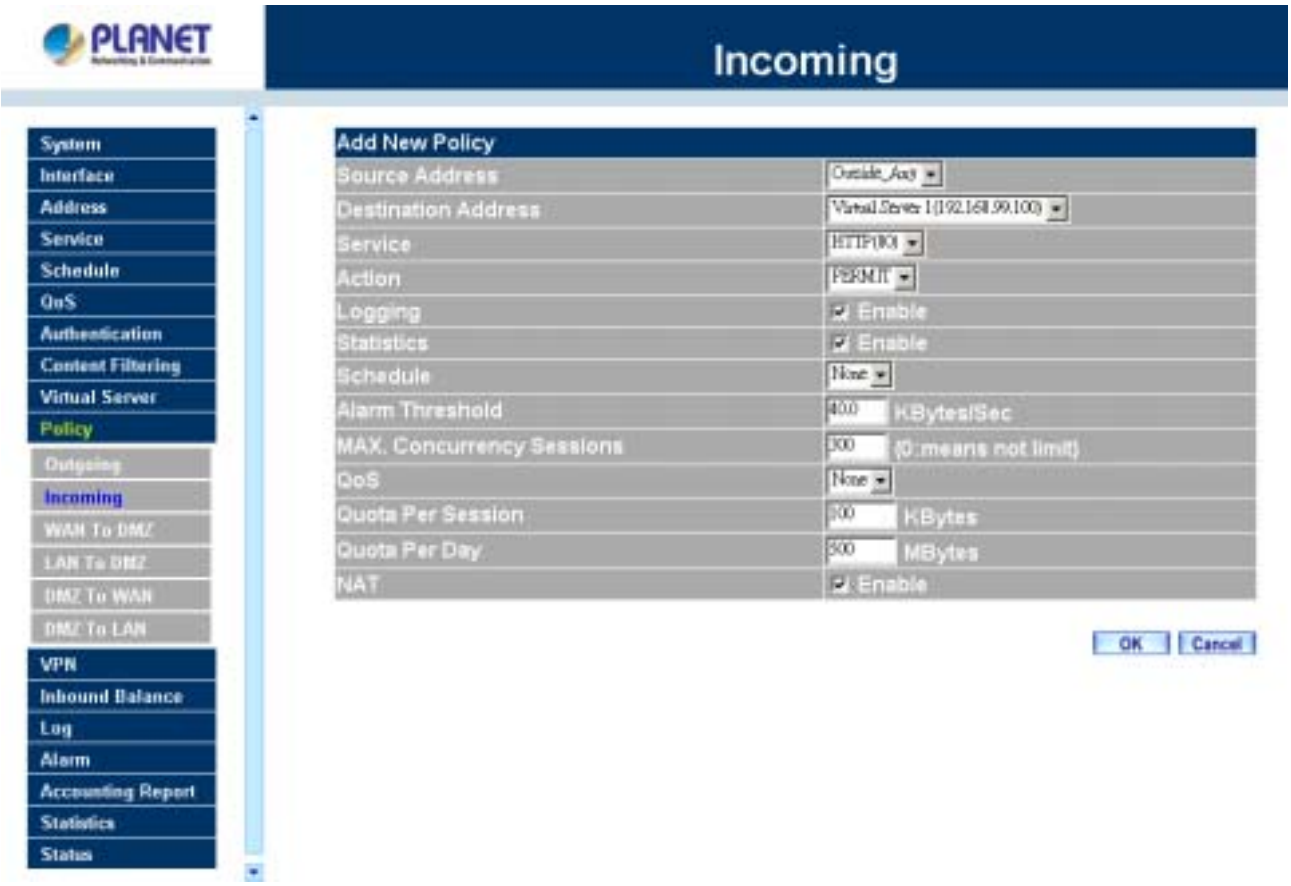
■ **Option:** specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Multi-Homing Security Gateway.

■ **Configure:** modify settings or remove incoming policy.

■ **Move:** this sets the sequence of the policies, number 1 being the first policy to proceed.

Adding an Incoming Policy

Step 1: Under **Incoming** of the **Policy** menu, click the New Entry button.



Step 2: Configure the parameters.

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the Address menu. To create a new source address, please go to the LAN section under the Address menu.

Destination Address: Select names of the LAN networks from the drop down list. The drop down list contains the names of IP mapping addresses specified in the **Mapped IP** or the **Virtual Server** sections of **Virtual Server** menu. To create a new destination address, please go to the **Virtual Server** menu.

Service: Specified services provided by LAN network servers. These are services / application that are allowed to pass from the network to the LAN network. Choose ANY for all services.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling between the specified WAN network and Virtual Server/Mapped IP.

Logging: select Enable to enable flow monitoring.

Statistics: select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Quota Per Session: The maximum throughput quota (in Kbytes/Sec) per session.

Quota Per Day: The maximum throughput quota (in Kbytes/Sec) per day.

NAT: Select all WAN networks source address will used NAT mode to a server is in the LAN networks.

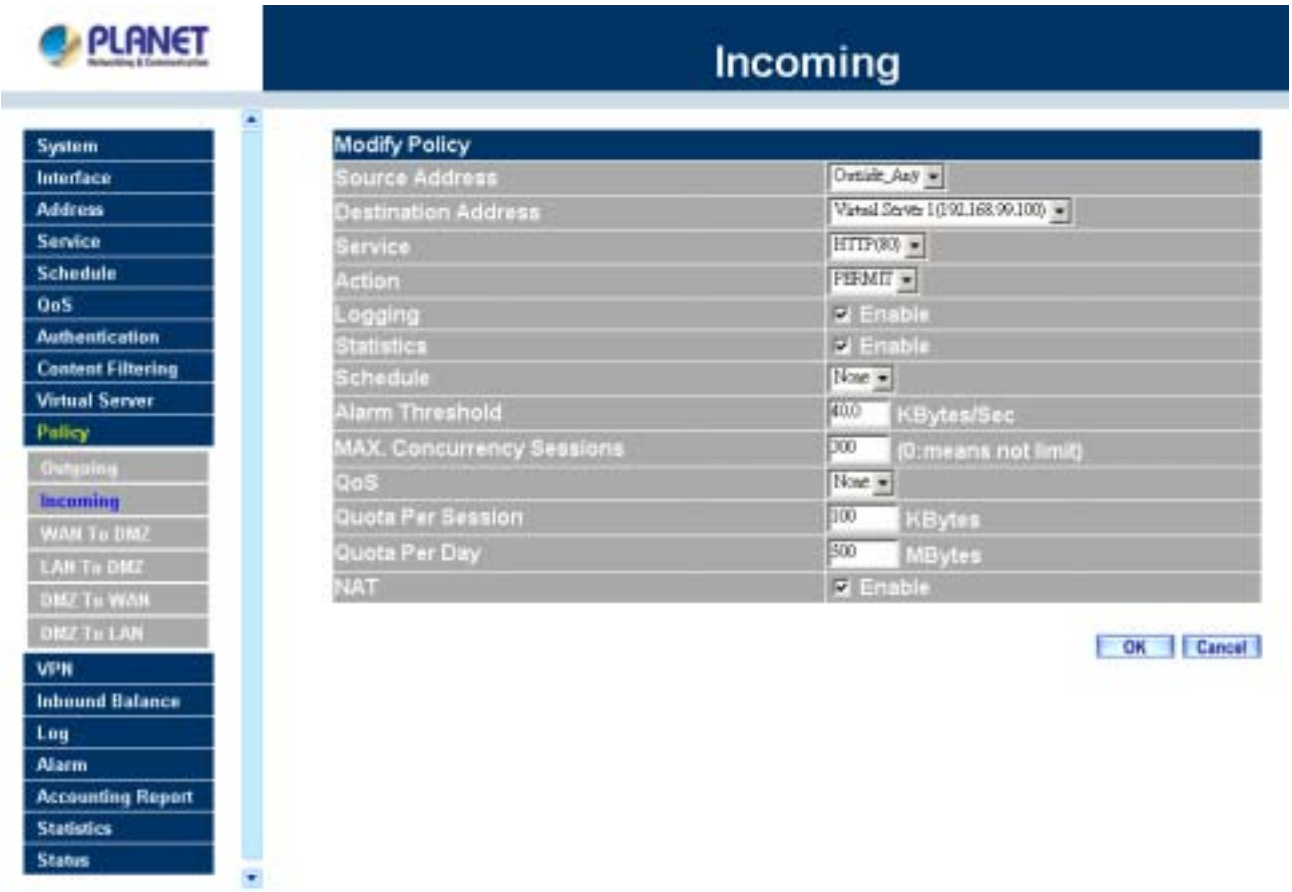
Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding new incoming policy.

Modifying Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

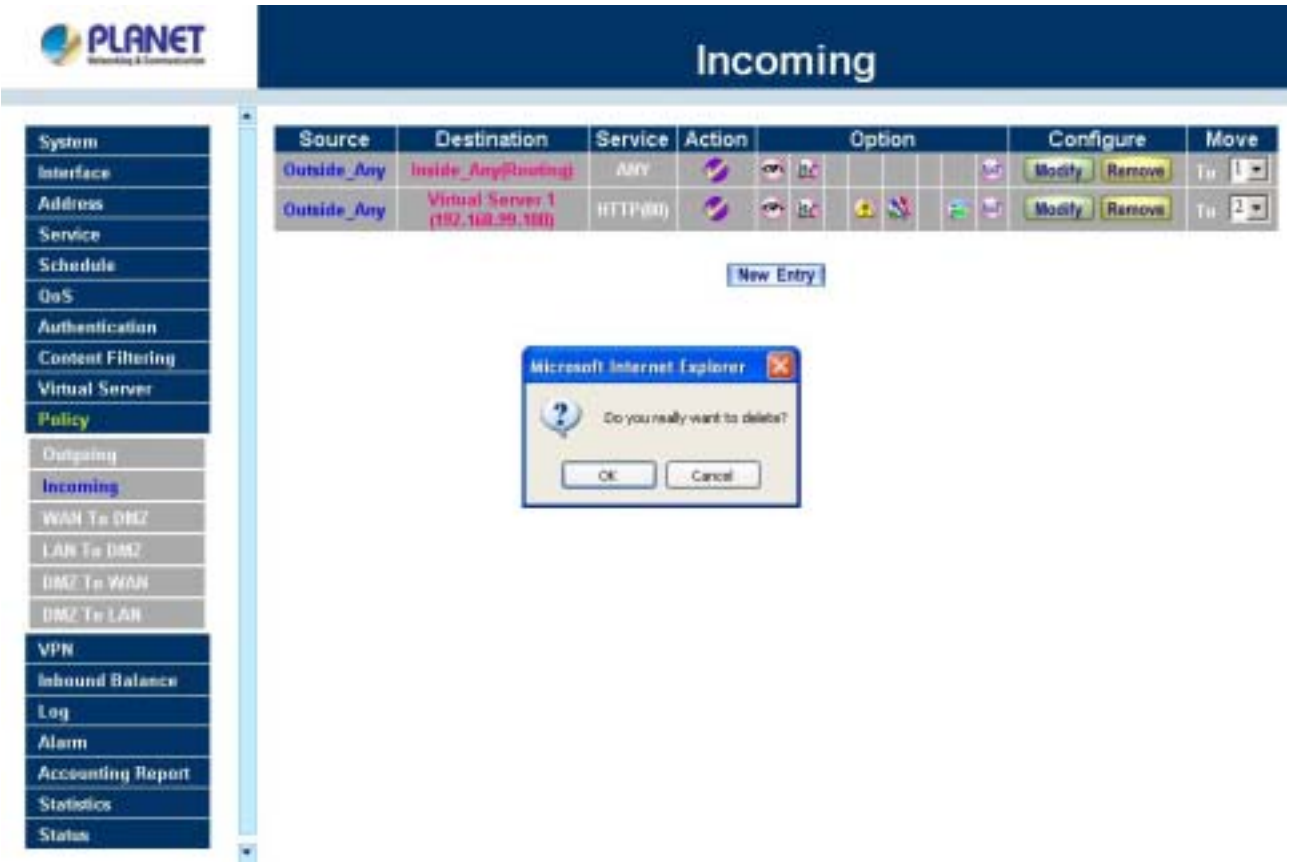
Step 3: Click **OK** to save modifications or click **Cancel** to cancel modifications.



Removing an Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be removed and click its corresponding [**Remove**] in the Configure field.

Step 2: In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.

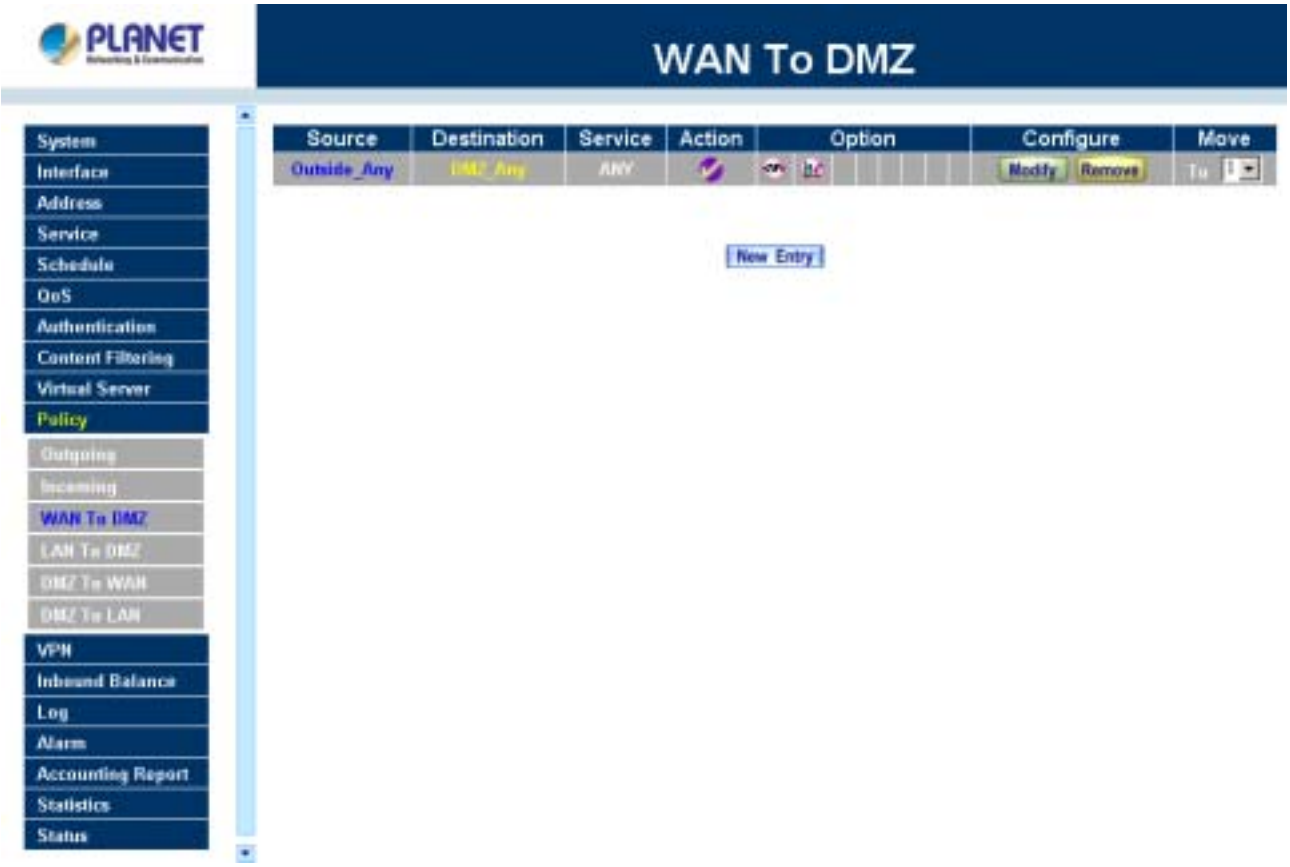


4.10.3 WAN To DMZ & LAN To DMZ

This section describes steps to create policies for packets and services from the WAN networks to the DMZ networks. Please follow the same procedures for LAN networks to DMZ networks.

Enter [WAN To DMZ] or [LAN To DMZ] window:

Click **WAN To DMZ** under **Policy** menu to enter the **WAN To DMZ** window. The WAN To DMZ table will show up displaying currently defined policies.



The fields in WAN To DMZ window:

Source: source networks, which are addresses specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.

Destination: destination networks, which are addresses specified in **DMZ** section of the **Address** menu and **Mapped IP** addresses of the **Virtual Server** menu.

Service: services supported by servers in DMZ network.

Action: control actions, to permit or deny packets from WAN networks to DMZ travelling through the Multi-Homing Security Gateway.

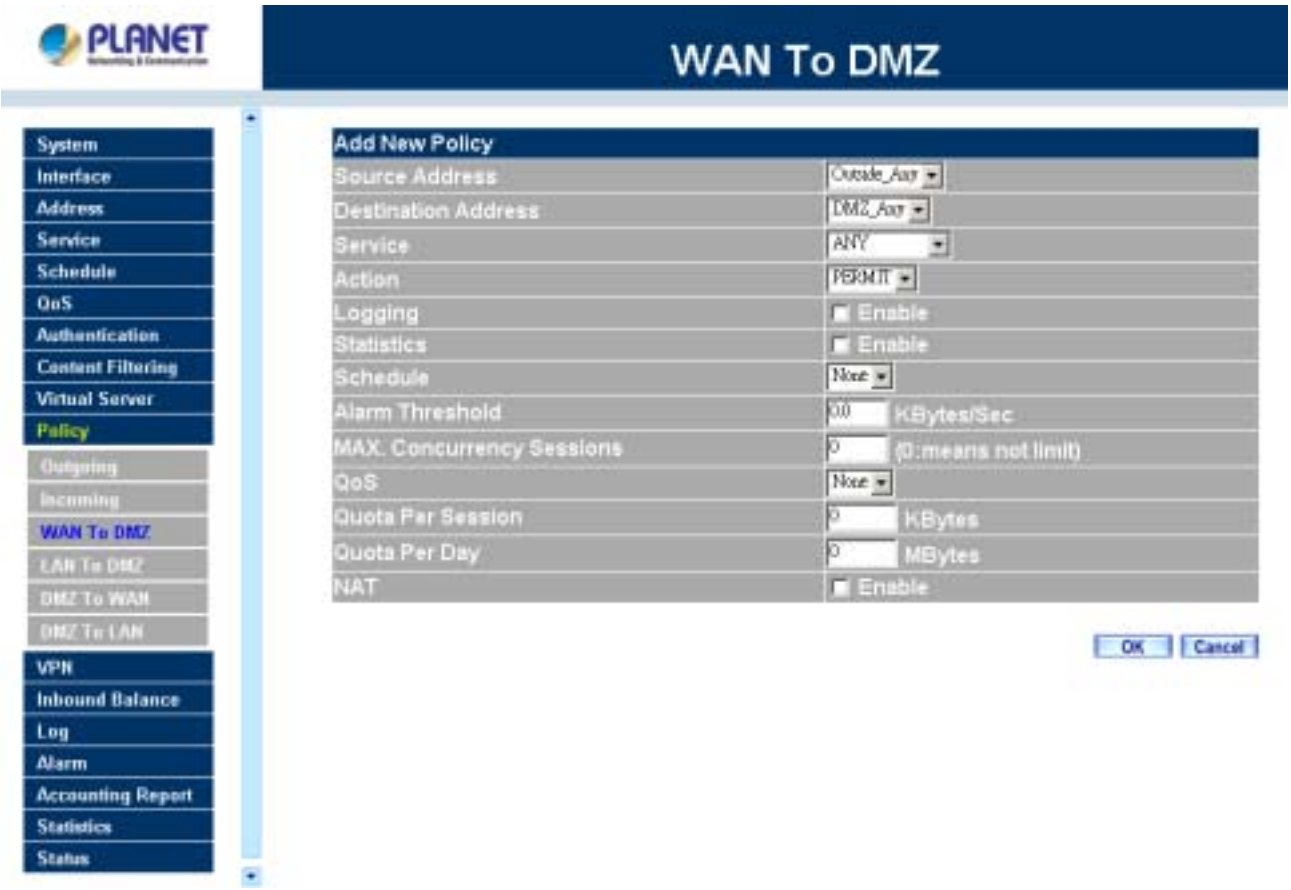
Option: specify the monitoring functions of packets from WAN network to DMZ network travelling through Multi-Homing Security Gateway.

Configure: modify settings or remove policies.

Move: this sets the priority of the policies, number 1 being the highest priority.

Adding a new WAN To DMZ Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Step 2: Configure the parameters.

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the **WAN** section of the **Address** menu. To create a new source address, please go to the **LAN** section under the **Address** menu.

Destination Address: Select the name of the DMZ network from the drop down list. The drop down list contains the names of the DMZ network created in the **Address** menu. It will also contain Mapped IP addresses from the **Virtual Server** menu that were created for the DMZ network. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to the sections entitled **Address** and **Virtual Server** for details)

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the WAN network to the DMZ network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu. (Please refer to the section entitled **Services** for details)

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling from the specified WAN network to the DMZ network.

Logging: select Enable to enable flow monitoring.

Statistics: select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be send if a flow rate exceeds the specified value.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Quota Per Session: The maximum throughput quota (in Kbytes/Sec) per session.

Quota Per Day: The maximum throughput quota (in Kbytes/Sec) per day.

NAT: Select all WAN networks source address will used NAT mode to a server is in the DMZ networks.

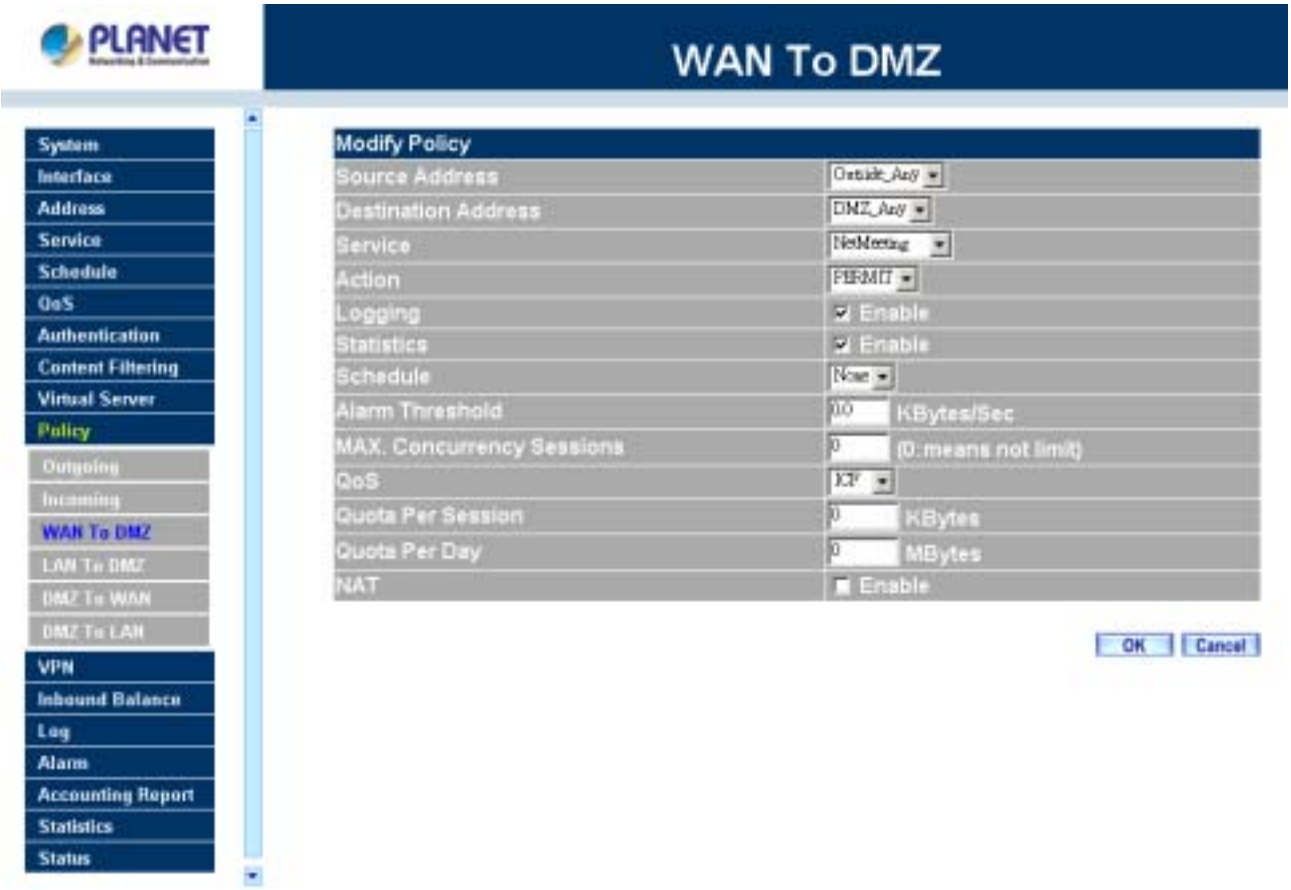
Step 3: Click **OK**.

Modifying an WAN To DMZ policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be modified and click its corresponding **Modify** option in the **Configure** field.

Step 2: In the **Modify Policy** window, fill in new settings.

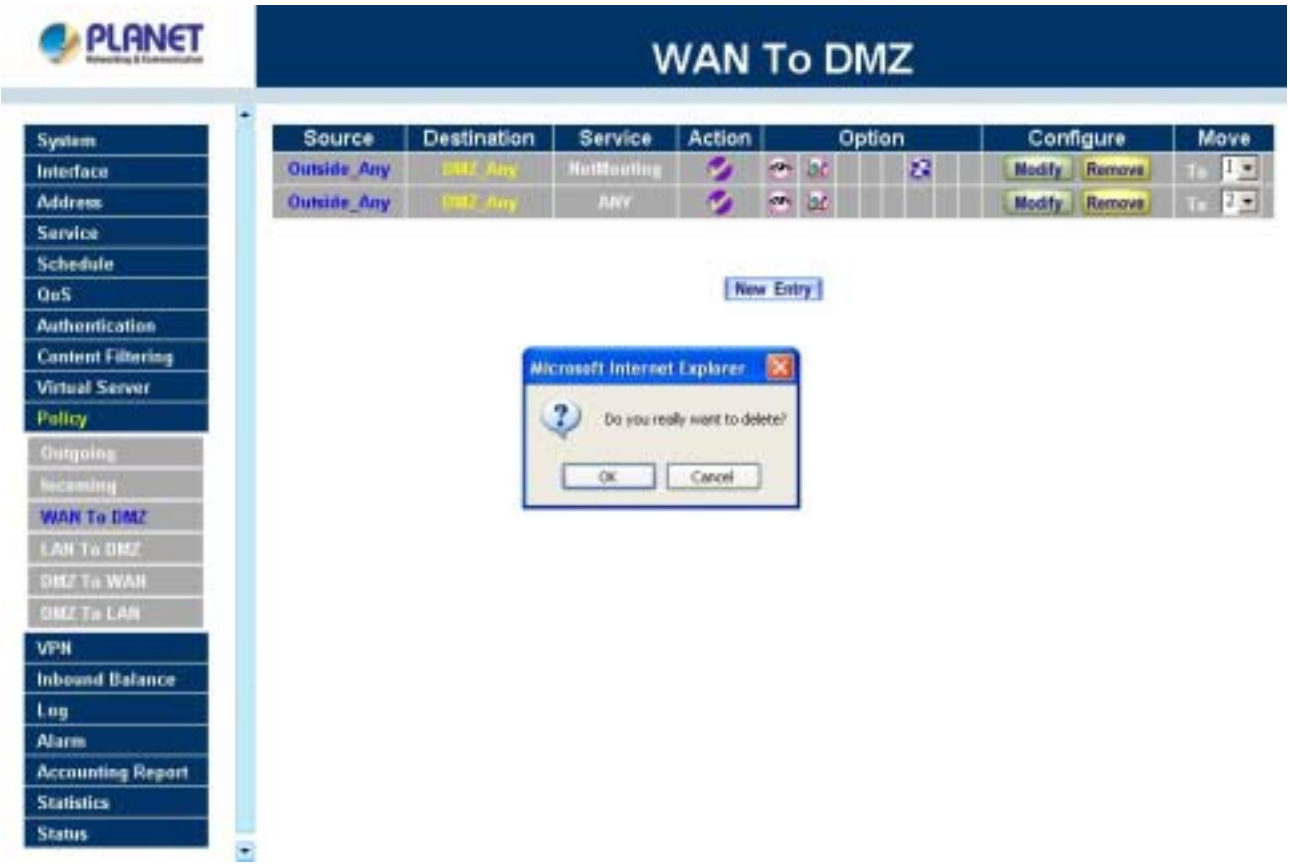
Step 3: Click **OK** to do save modifications.



Removing a WAN To DMZ Policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2: In the **Remove** confirmation pop-up box, click **OK** to remove the policy.



4.10.4 DMZ To WAN & DMZ To LAN

This section describes steps to create policies for packets and services from DMZ networks to WAN networks. Please follow the same procedures for DMZ networks to LAN networks.

Entering the DMZ To WAN window:

Click **DMZ To WAN** under **Policy** menu and the **DMZ To WAN** table appears displaying currently defined **DMZ To WAN** policies.

The fields in the DMZ To WAN window are:

Source: source network addresses which are specified in the **DMZ** section of the **Address** window.

Destination: destination networks, which is the WAN network address

Service: services supported by Servers of WAN networks.

Action: control actions, to permit or deny packets from the DMZ network to WAN networks travelling through the Multi-Homing Security Gateway.

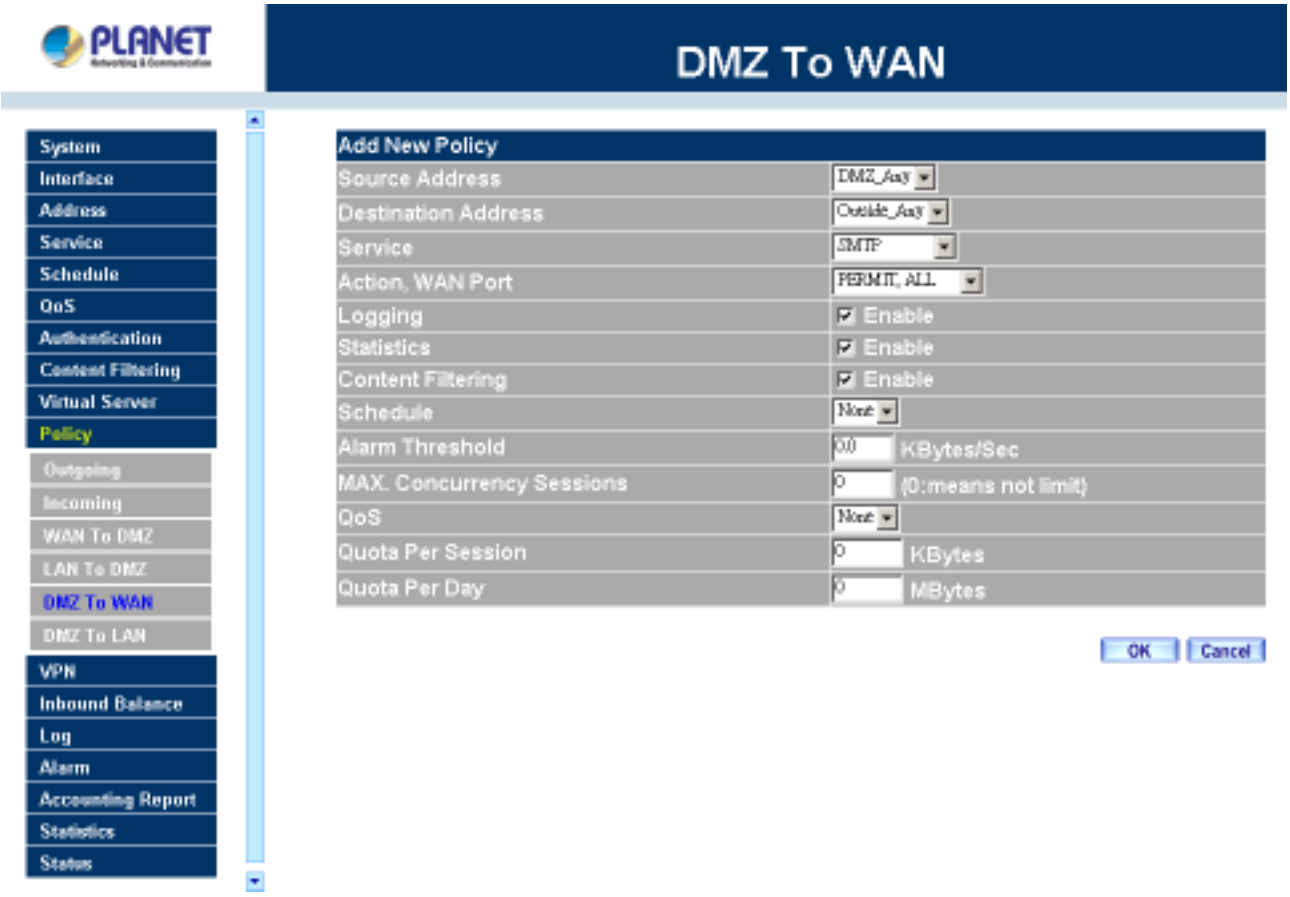
Option: specify the monitoring functions on packets from the DMZ network to WAN networks travelling through the Multi-Homing Security Gateway.

Configure: modify settings or remove policies

Move: this sets the sequence of the policies, number 1 being the first policy to proceed.

Adding a DMZ To WAN Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Step 2: Configure the parameters.

Source Address: Select the name of the DMZ network from the drop down list. The drop down list will contain names of DMZ networks defined in **DMZ** section of the **Address** menu. To add a new source address, please go to the **DMZ** section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list lists names of addresses defined in **WAN** section of the **Address** menu. To add a new destination address, please go to **WAN** section of the **Address** menu.

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the DMZ network to the WAN network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling from the specified DMZ network to the WAN network.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Quota Per Session: The maximum throughput quota(in Kbytes/Sec) per session.

Quota Per Day: The maximum throughput quota(in Kbytes/Sec) per day.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding.

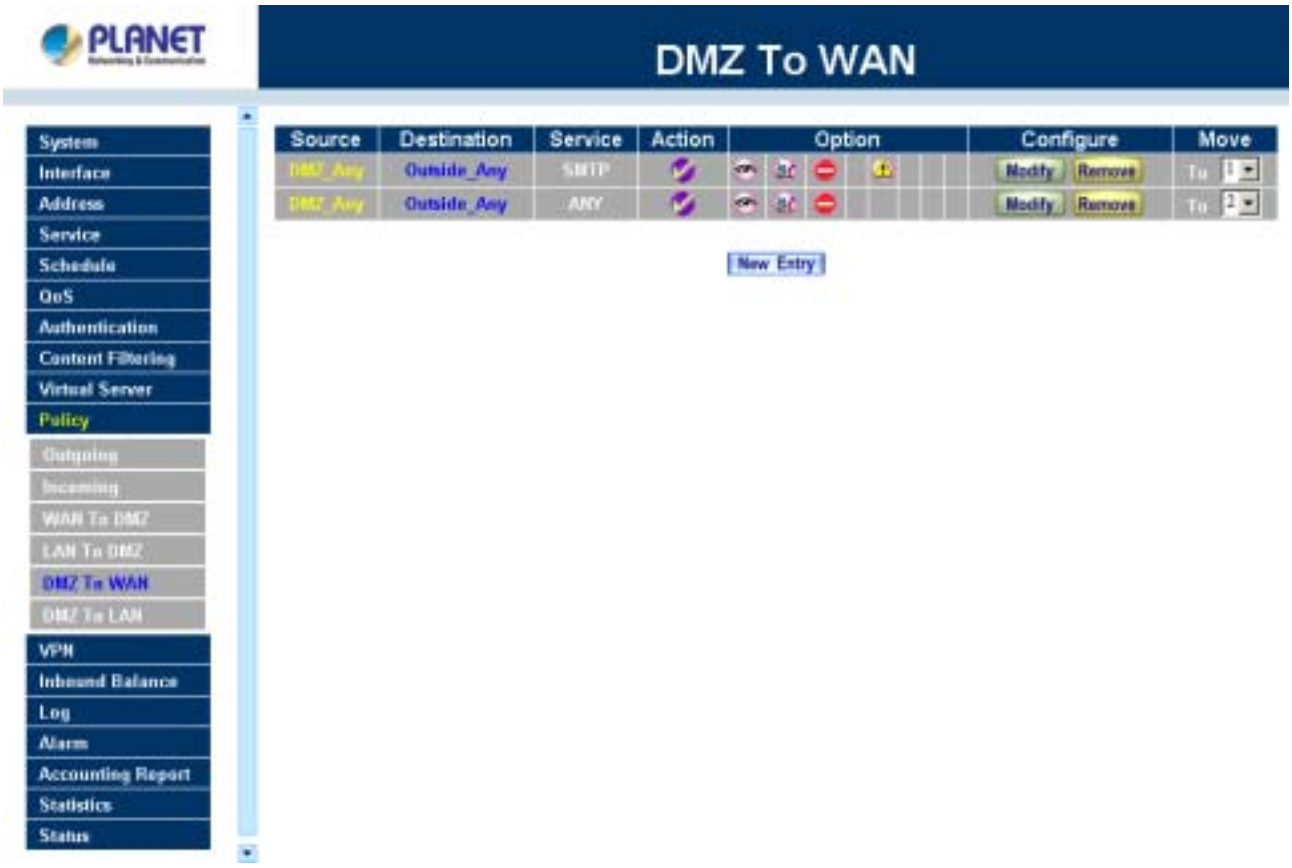
Modifying a DMZ To WAN policy:

Step 1: In the DMZ To WAN window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

NOTE: To change or add selections in the drop-down list, go to the section where the selections are setup. (Source Address → DMZ of Address; Destination Address →WAN, Service →Pre-defined Service, Custom or Group under Service.)

Step 3: Click OK to save modifications or click Cancel to cancel modifications.



Removing a DMZ To WAN Policy:

Step 1. In the **DMZ To WAN** window, locate the name of policy desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the **Remove confirmation** dialogue box, click **OK.**

4.11 VPN

The Multi-Homing Security Gateway's VPN (Virtual Private Network) is set by the System Administrator. The System Administrator can add, modify or remove VPN settings.

What is VPN?

To set up a **Virtual Private Network** (VPN), you don't need to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet, Destination Gateway, Destination Subnet, Authentication Method, Preshare key, Encapsulation and IPSec lifetime. The Multi-Homing Security Gateway Gateways on both ends must use the same **Preshare** key and **IPSec** lifetime to make a **VPN** connection.

4.11.1 IPSec Autokey

This chapter describes steps to create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. For example, with two Multi-Homing Security Gateway Gateway devices, IKE allows new keys to be generated after a set amount of time has passed or a certain threshold of traffic has been exchanged.

Accessing the Autokey IKE window

Click **IPSec Autokey** under the VPN menu to enter the **IPSec Autokey** window. The **IPSec Autokey** table displays current configured VPNs.

The fields in the IPSec Autokey window are:

■ **Name:** The VPN name to identify the VPN tunnel definition. The name must be different for the two sites creating the tunnel.

■ **Gateway IP:** The WAN 1 interface IP address of the remote Multi-Homing Security Gateway Gateway.

■ **Destination Subnet:** Destination network subnet.

■ **Algorithm:** The display the Algorithm way.

■ **Status:** Connect/Disconnect or Connecting/Disconnecting.

■ **Configure:** Connect, Disconnect, Modify and Delete.

Adding the Autokey IKE

Step 1. Click the **New Entry** button and the **VPN Auto Keyed Tunnel** window will appear.

Step 2: Configure the paremeters.

■ **Preshare Key:** The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.

Encapsulation

ISAKMP Algorithm

■**ENC Algorithm:** ESP Encryption Algorithm. ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. The available encryption algorithms including: 56 bit DES-CBC, 168-bit Triple DES-CBC, AES 128-bit, AES 192-bit and AES 256-bit encryption algorithm. The default algorithm 56 bit DES-CBC.

■**AUTH Method:** Authentication Method. Selects MD5(128-bit hash) or SHA-1(160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.

■ **Group:** Selects Group 1(768-bit modulus), Group 2(1024-bit modulus) or Group 5(1536-bit modulus). The larger the modulus, the more secure the generated key is. However, the larger the modulus, the longer the key generation process takes. Both side of VPN tunnels must aggree to use the same group. The default algorithm is Group 1.

IPSec Algorithm: Select Data Encryption + Authentication or Authentication Only.

Data Encryption + Authentication

■ **Encryption Algorithm:** Selects 56 bit DES-CBC, 168-bit Triple DES-CBC, AES or NULL encryption algorithm. The default algorithm is 56 bit DES-CBC.

■ **Authentication Algorithm:** Selects MD5(128-bit hash) or SHA-1(160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.

Authentication Only

Perfect Forward Secrecy

■**IPSec Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 28800 seconds (eight hours). Selection of small values could lead to frequent re-keying, which could affect performance.

■ **Keep alive IP:** Check to allow Remote Client computer IP Address connected to keep alive.

■ **Aggressive mode:** Select Aggressive mode algorithm.

■ **GRE/IPSec:** Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology.

■ **Schedule:** Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time.

■ **QoS:** Select the item listed in the QoS to enable the policy to automatically execute the function in a certain range.

■ **Authentication-User:** Select the item listed in the Authentication-User to enable the policy to automatically execute the function in a certain time and range.

■ **Show remote Network Neighborhood:** Select the remote Network Neighborhood enable to show.

There are 5 examples of VPN setting.

Example 1. Create a VPN connection between two Multi-Homing Security Gateways.

Example 2. Create a VPN connection between the Multi-Homing Security Gateway and Windows XP Professional VPN Client.

Example 3. Create a VPN connection between two Multi-Homing Security Gateways using Aggressive mode Algorithm (3DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Example 4. Create a VPN connection between two Multi-Homing Security Gateways using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

Example 5. Create a VPN connection between Multi-Homing Security Gateway and PLANET VRT-401 VPN Router.

Example 1. Create a VPN connection between two Multi-Homing Security Gateways.

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be LAN. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel			
Name		VPN_A	
From Source	◉ LAN	○ DMZ	
Use interface	◉ WAN1	○ WAN2	
Subnet / Mask		192.168.10.0	/ 255.255.255.0

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected,

company B's subnet IP and mask.

To Destination	
Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.20.0 / 255.255.255.0
Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
Remote Client -- Fixed IP or Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Authentication Only	

Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.20.100

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

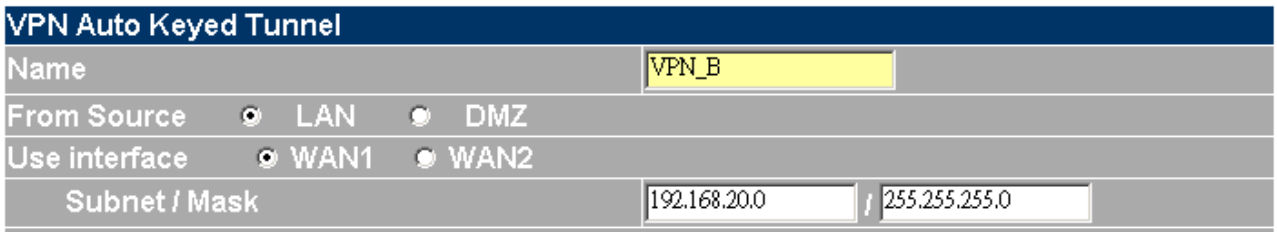
Schedule	None

Step 9. Click OK to finish the setting of Company A.

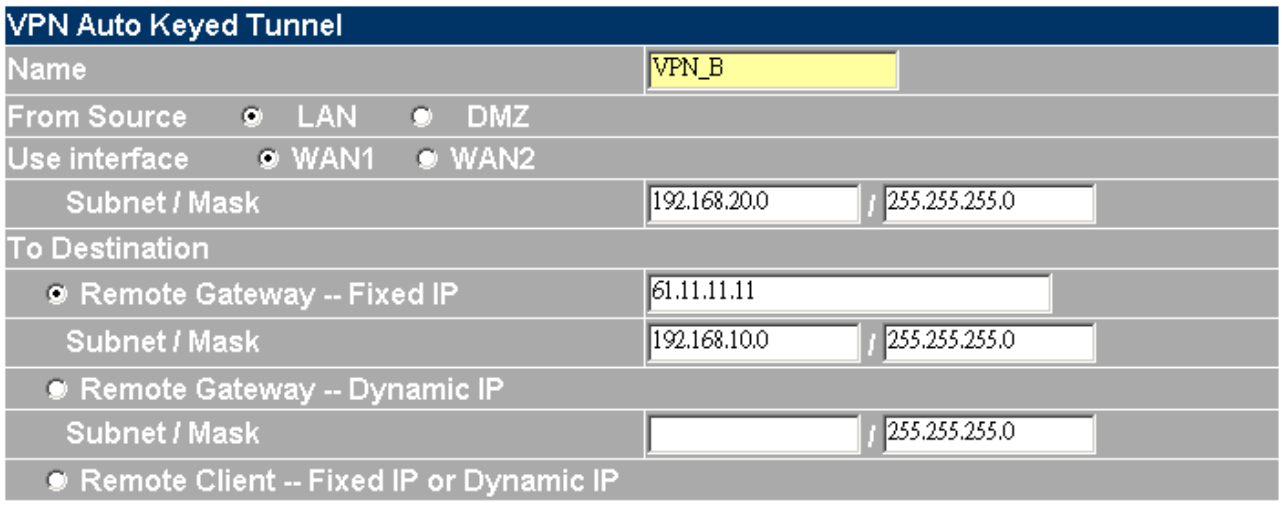
The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's Multi-Homing Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.



Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.



Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group to connect.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
◉ Authentication Only	

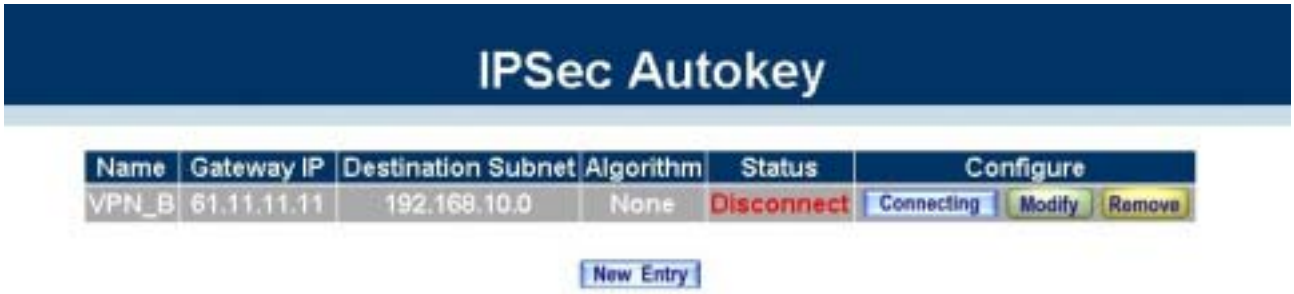
Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.10.100

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule . Refer to the corresponding section for details.

Schedule	None

Step 9. Click OK to finish the setting of Company B.



Example 2. Create a VPN connection between the Multi-Homing Security Gateway and Windows XP Professional VPN Client.

Preparation Task:
Company A External IP is 61.11.11.11, Internal IP is 192.168.10.X
Remote User External IP is 211.22.22.22

Remote user with an external IP wants to create a VPN connection with company A and connect to 192.168.10.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel	
Name	VPN_A
From Source	◉ LAN ○ DMZ
Use interface	◉ WAN1 ○ WAN2
Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 3. In to Destination table, choose Remote Client – Fixed IP or Dynamic IP.

To Destination	
○ Remote Gateway -- Fixed IP	
Subnet / Mask	/ 255.255.255.0
○ Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
◉ Remote Client -- Fixed IP or Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation, ISAKMP Algorithm, choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
◉ Authentication Only	

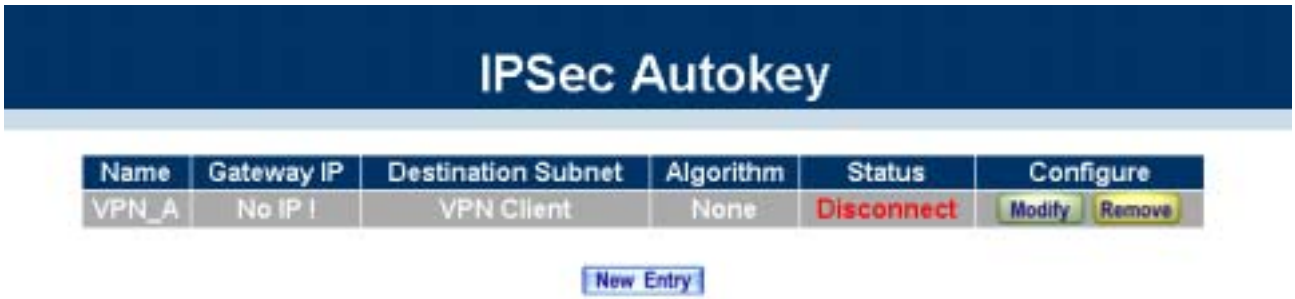
Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	211.22.22.22

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

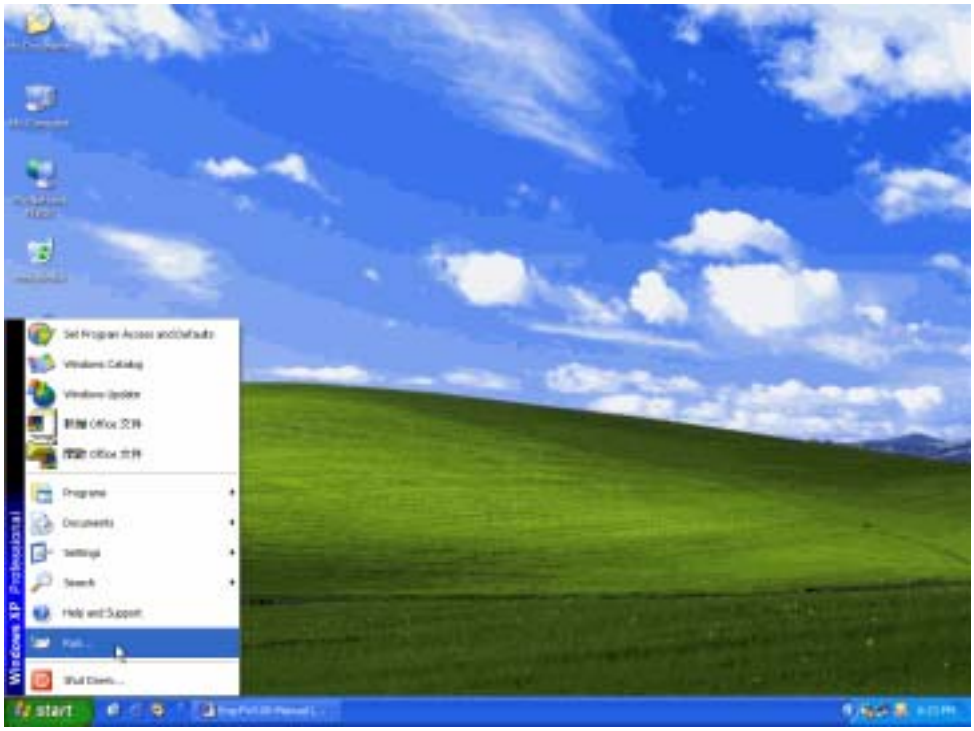
Schedule	None

Step 9. Click OK to finish the setting of Company A.



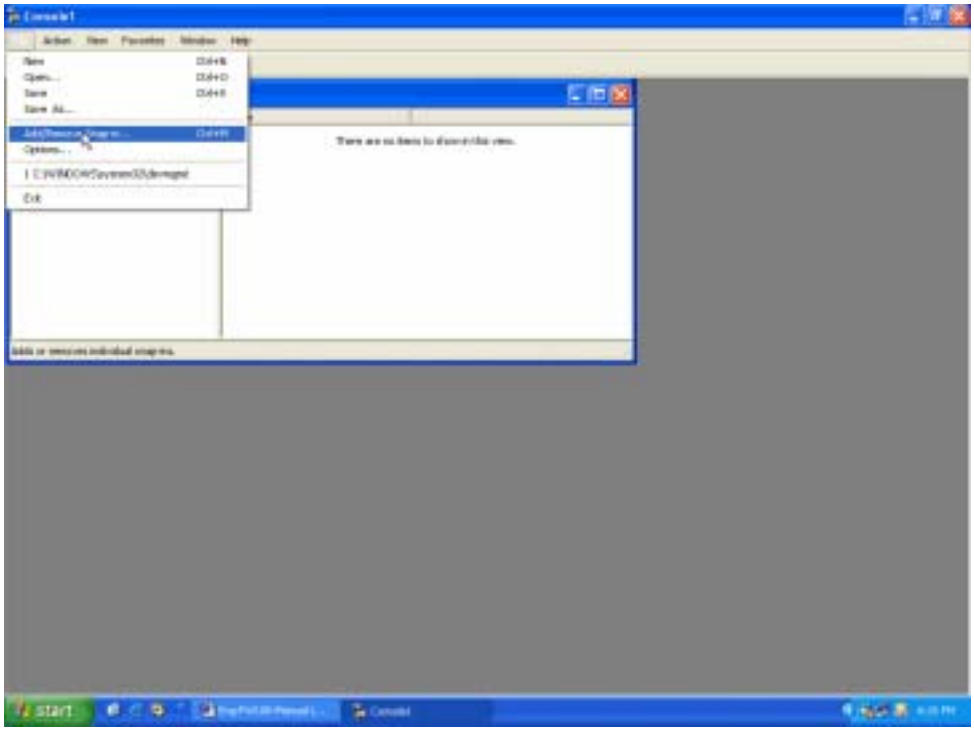
The IP of remote user is 211.22.22.22. The settings of remote user are as the following.

Step 1. Enter Windows XP, click Start and click Execute function.

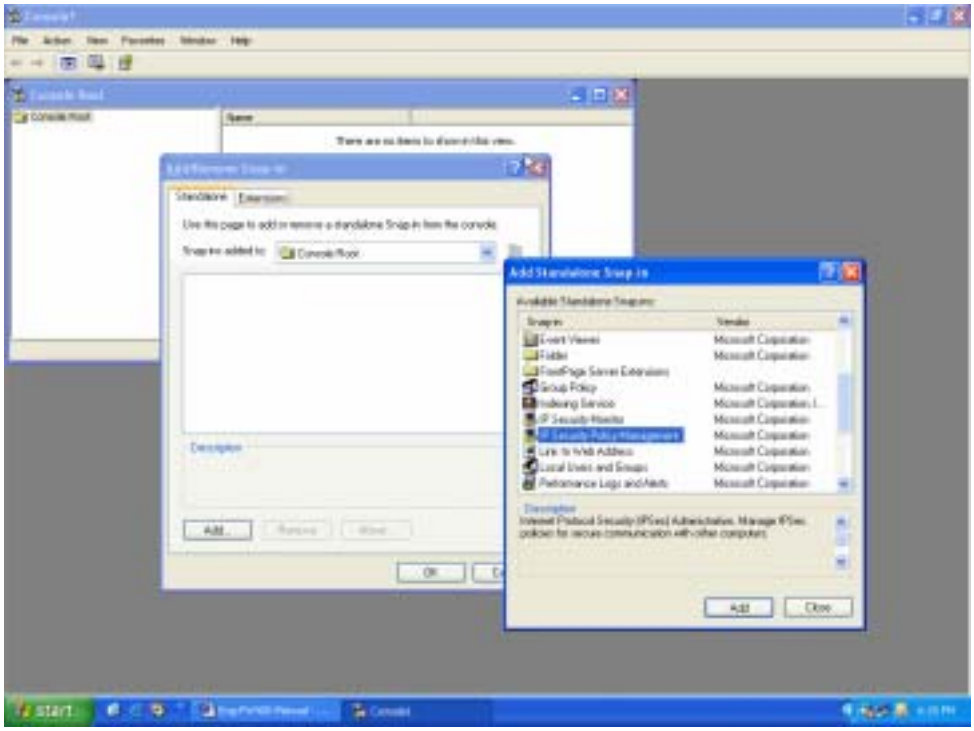


Step 2. In the Execute window, enter the command, MMC in Open.

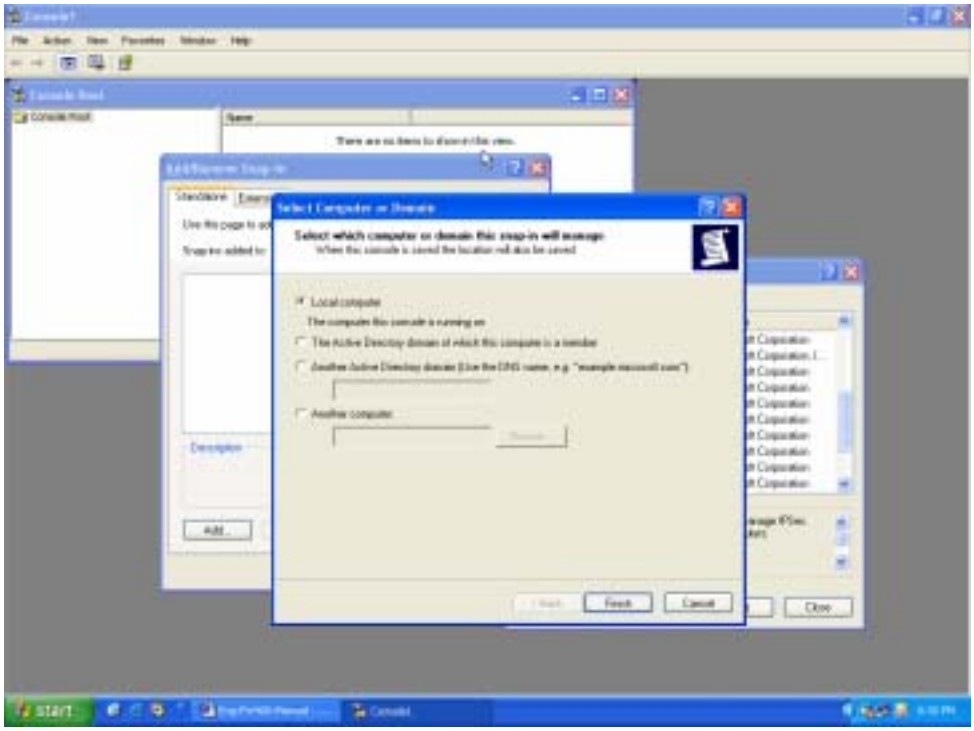
Step 3. Enter the Console window, click Console(C) option and click Add/Remove Embedded Management Option.



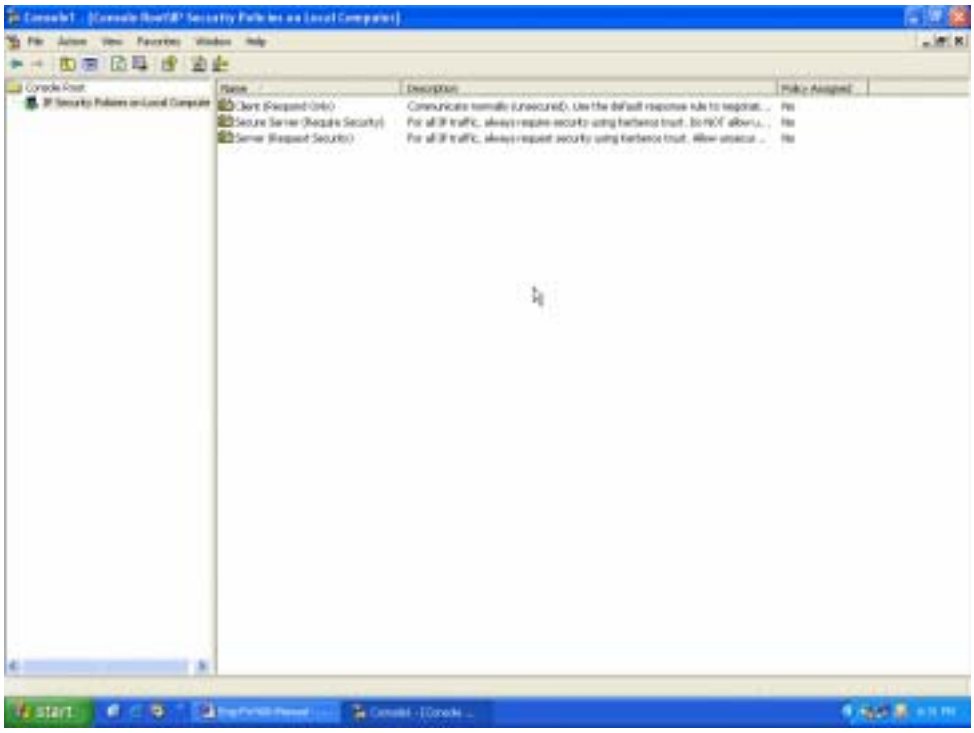
Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.



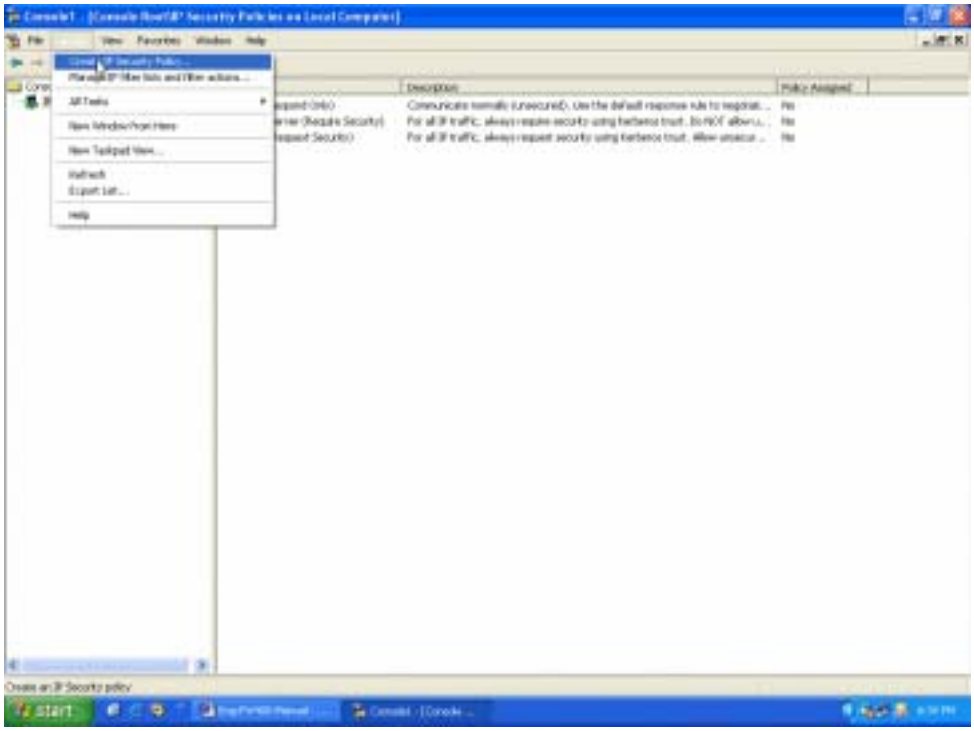
Step 5. Choose Local Machine (L) for finishing the setting of Add.



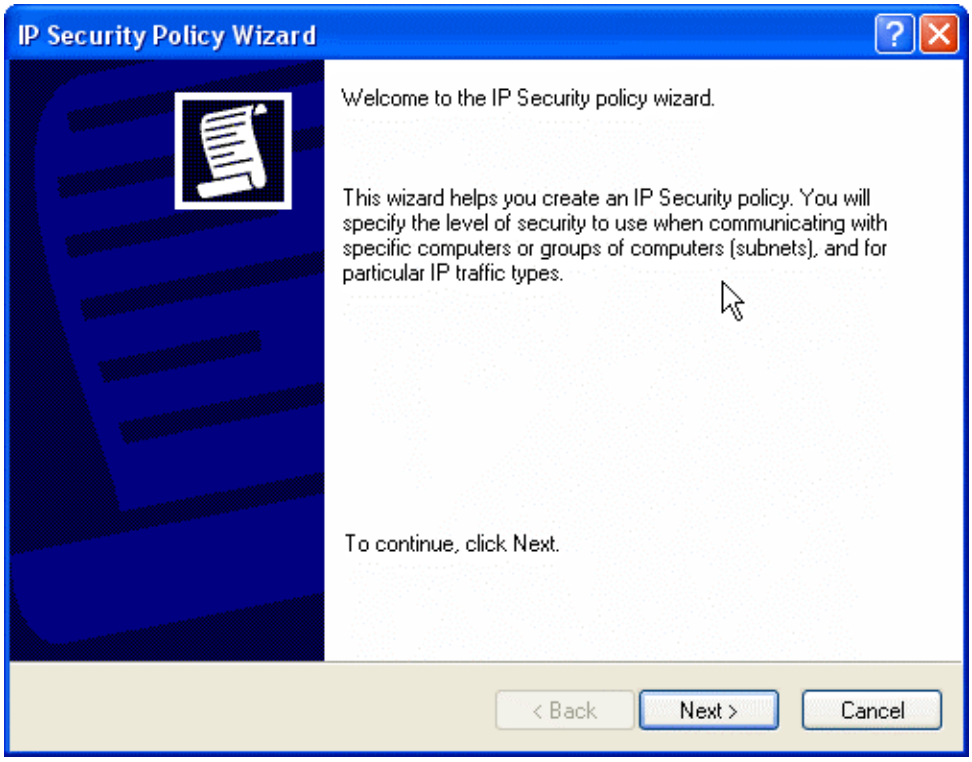
Step 6. Finish the setting of Add.



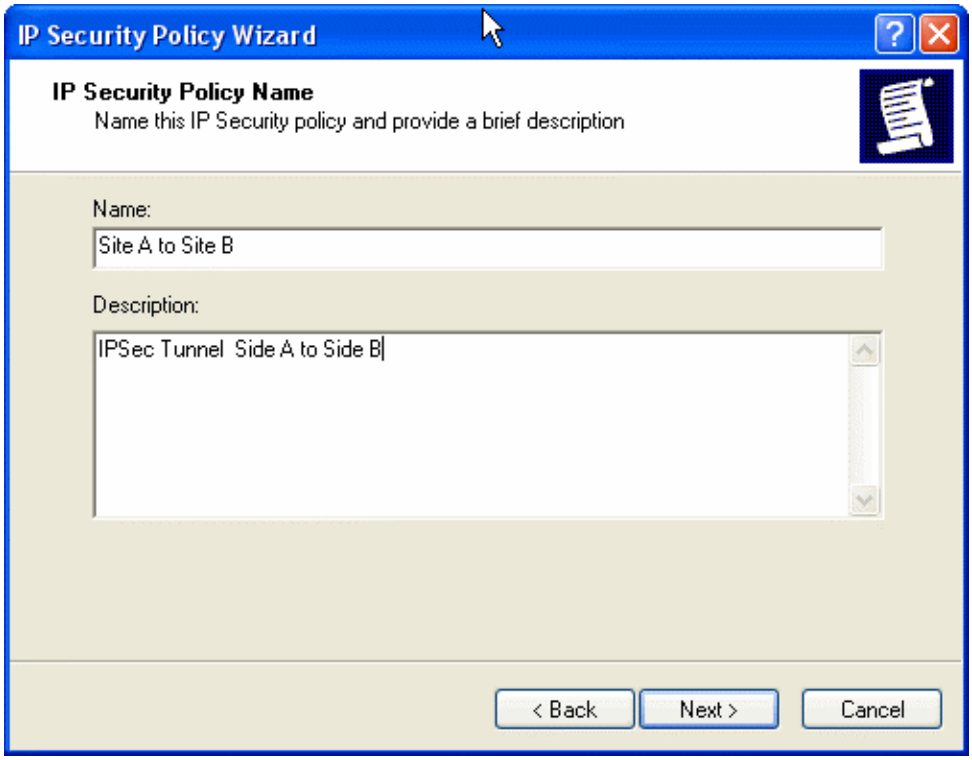
Step 7. Click the right button of mouse in IP Security Policies on Local Machine and choose Create IP Security Policy(C) option.



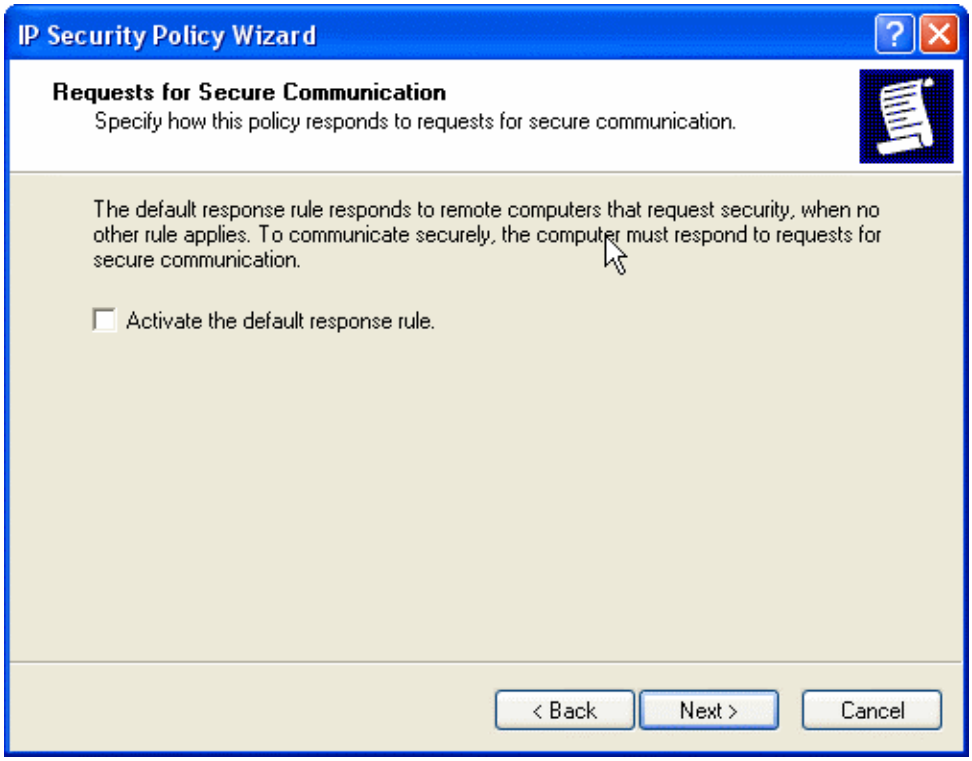
Step 8. Click Next.



Step 9. Enter the Name of this VPN and optionally give it a brief description.

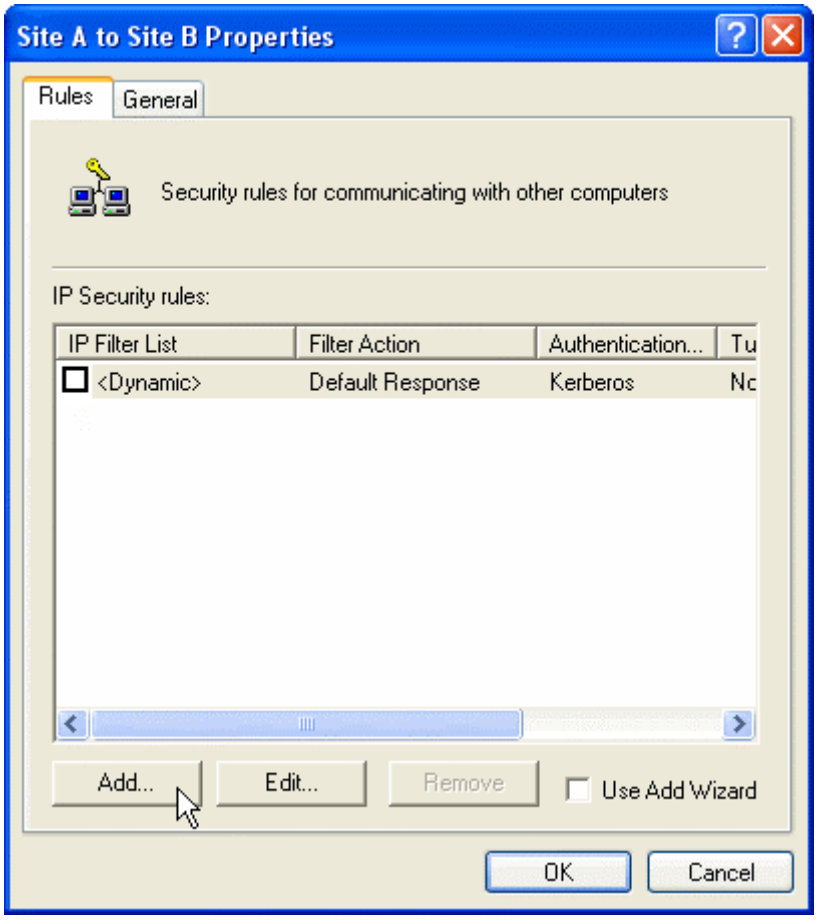


Step 10. Disable **Activate the default response rule**. And click Next.

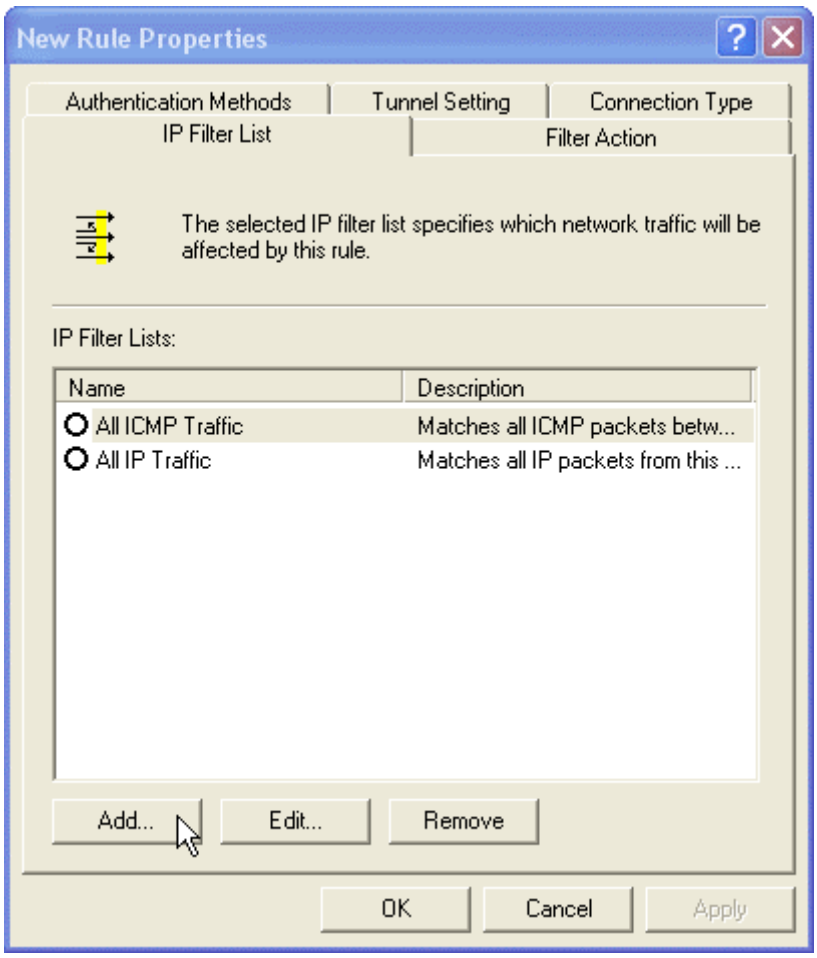


Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.

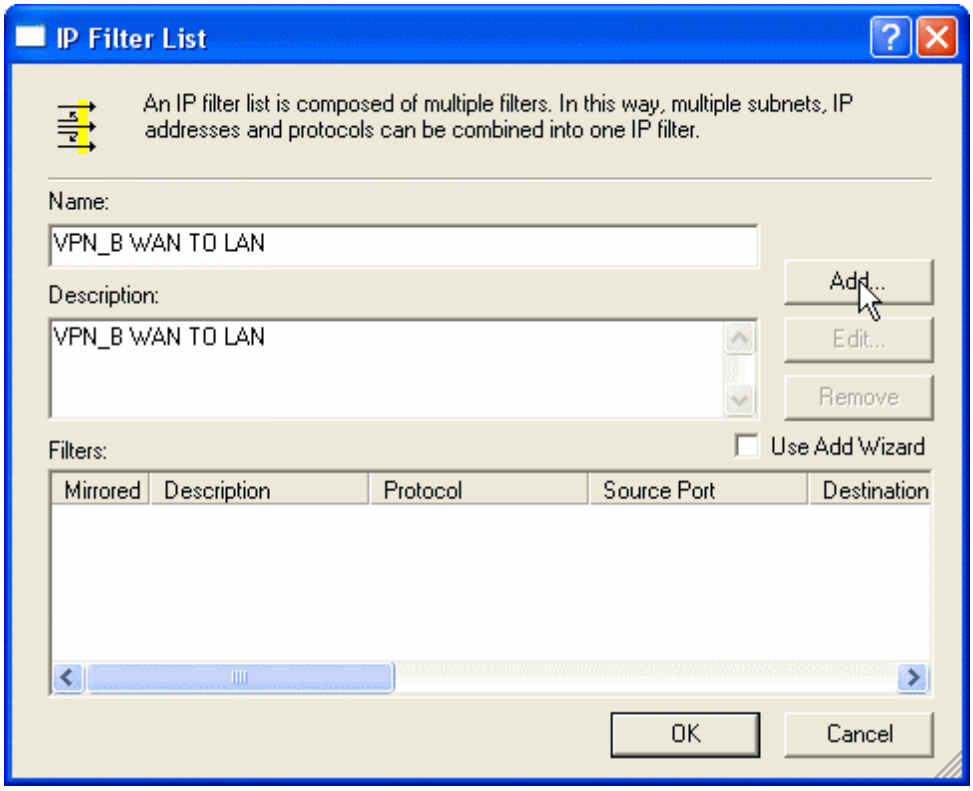
Step 12. In VPN_B window, click Add and please don't click Use Add Wizard.



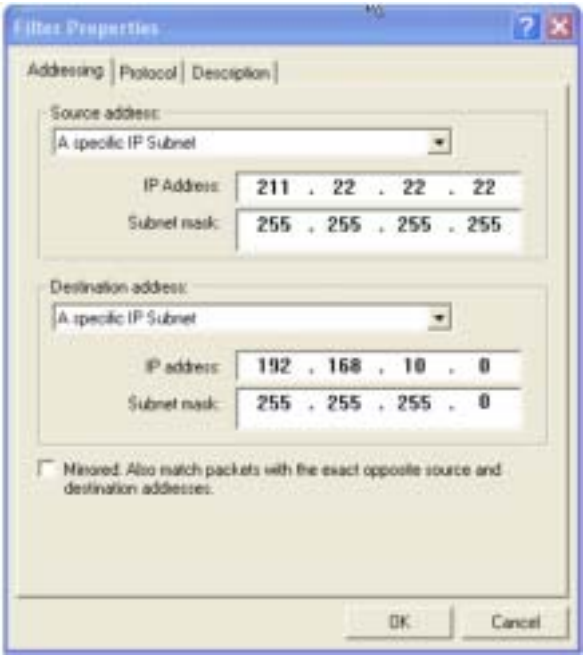
Step 13. In IP Filter List tab, click Add.



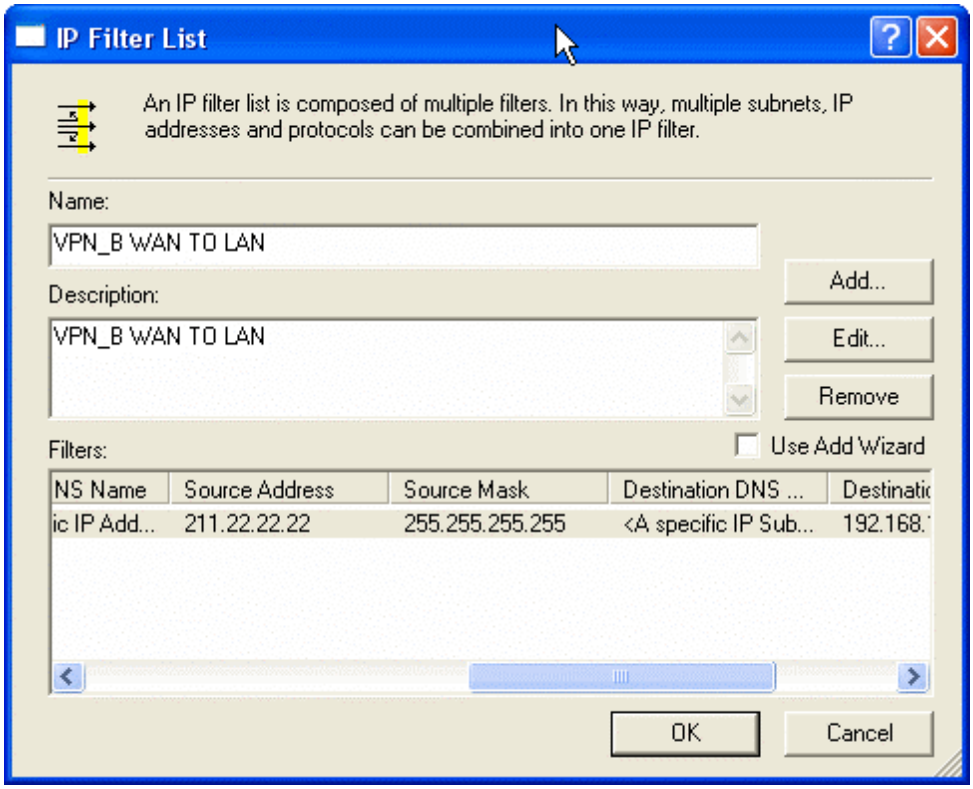
Step 14. In IP Filter List window, please don't choose Use Add Wizard and change Name to VPN_B WAN TO LAN. Click Add.



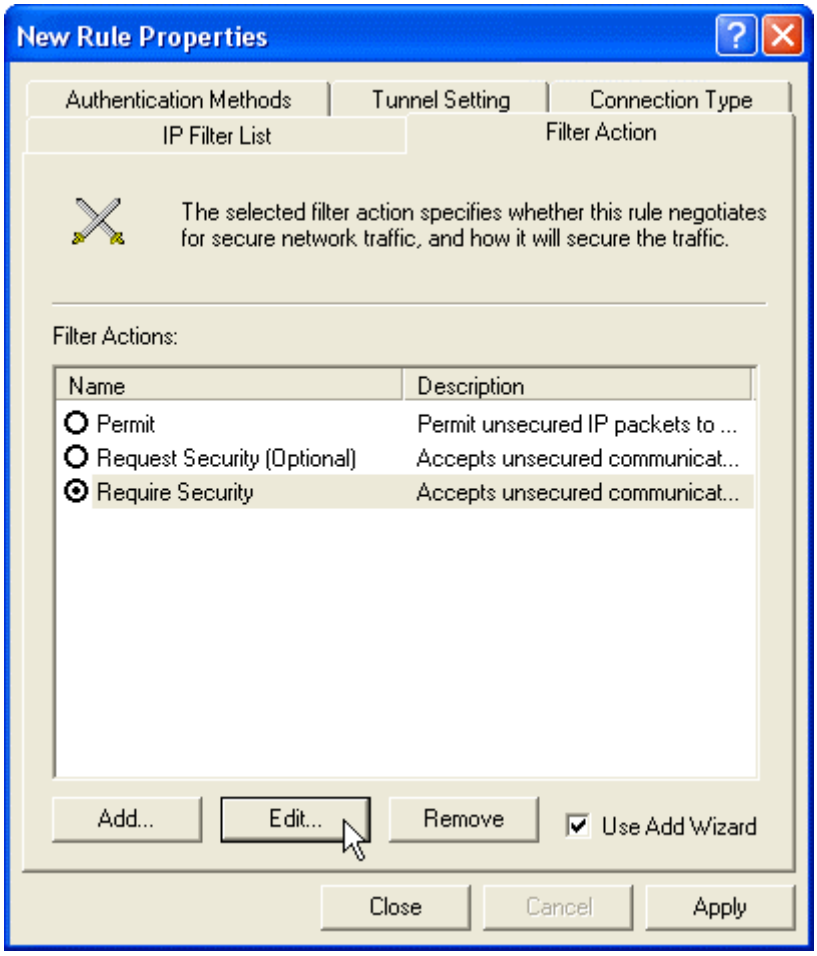
Step 15. In Filter Properties window, in Source address, click down the arrow to select the specific IP Subnet and fill remote user's IP Address, 211.22.22.22 and Subnet mask, 255.255.255.255. In Destination address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0. Please disable Mirrored. Also match packets with the exact opposite source and destination addresses.



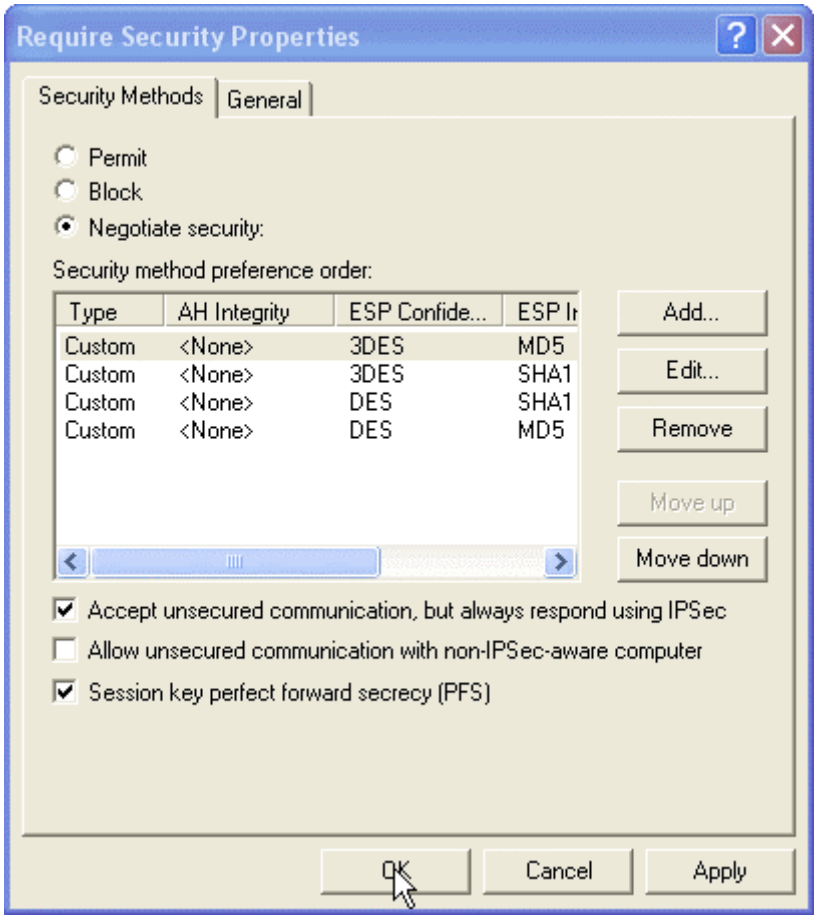
Step 16. Finish the setting and close IP Filter List window.



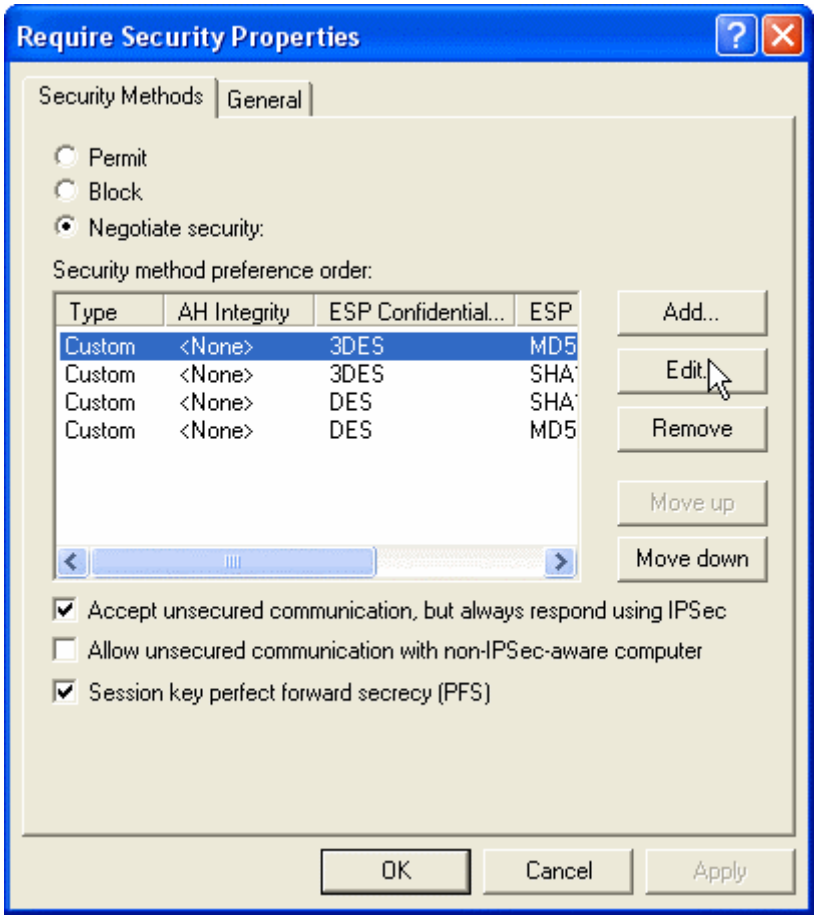
Step 17. Click Filter Action tab and choose Require Security. Click Edit.



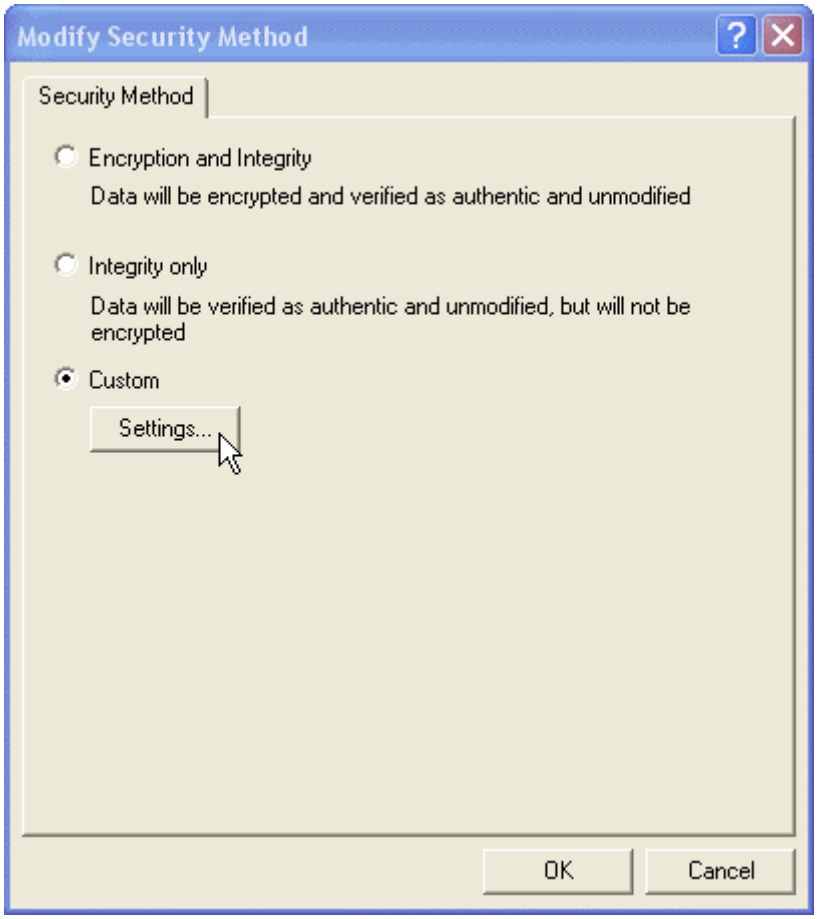
Step 18. In Security Methods tab, choose accept unsecured communication, but always respond using IPSec.



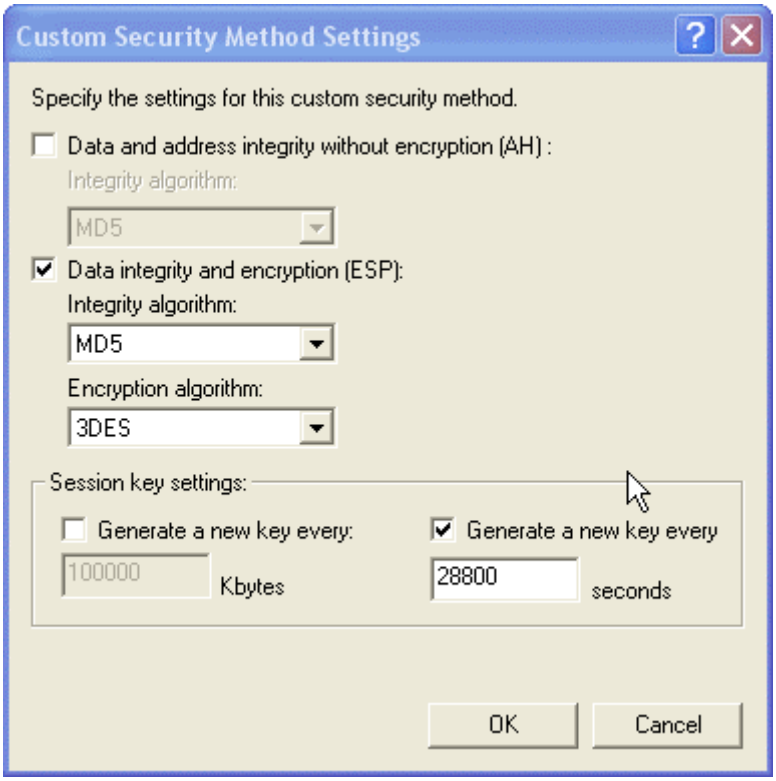
Step 19. Click Edit in Custom/ None/ 3DES/ MD5.



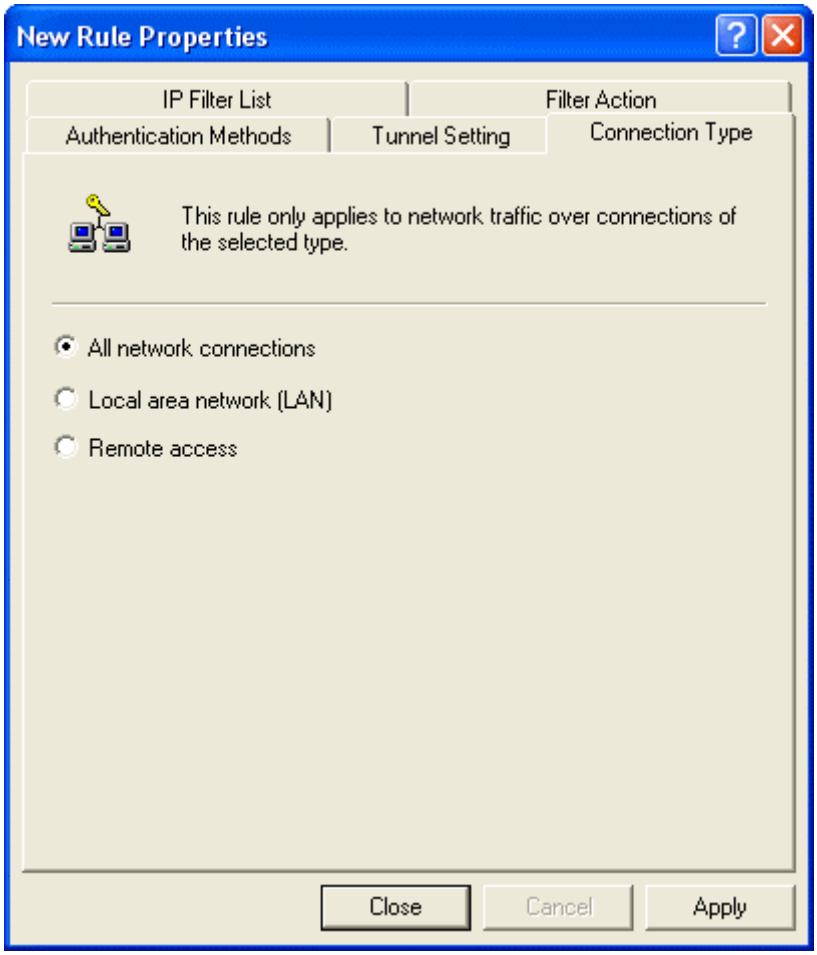
Step 20. Click Custom(For professional user) and click Edit.



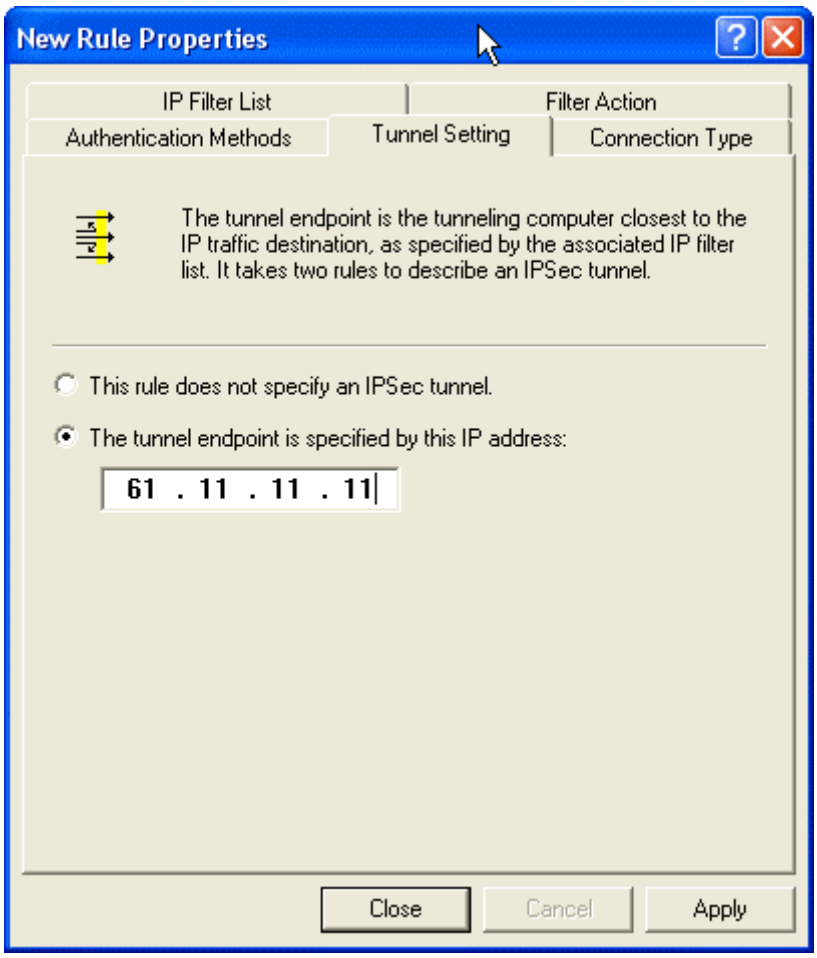
Step 21. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



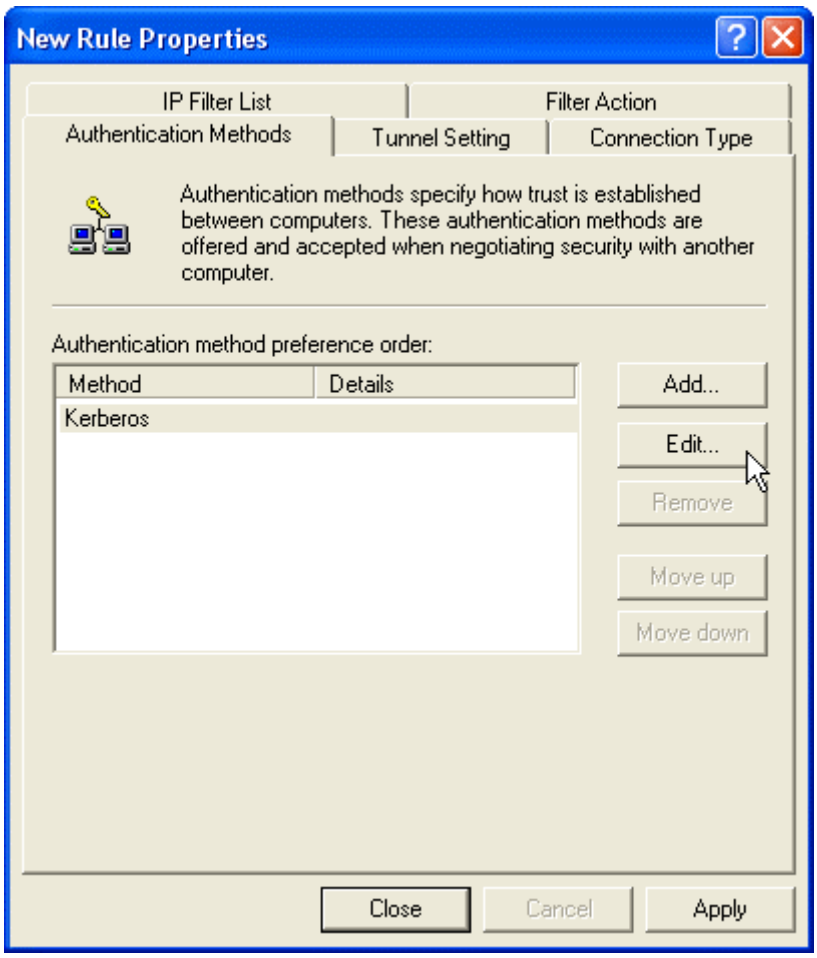
Step 22. Click Connection Type tab and click all network connections.



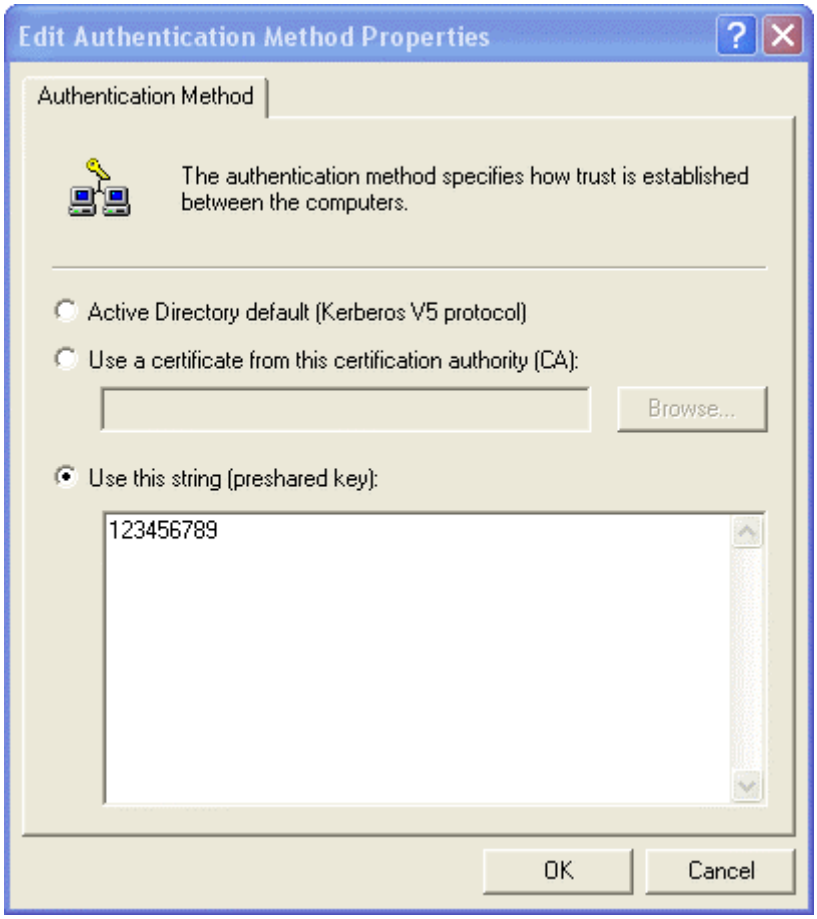
Step 23. Click Tunnel Setting tab, and click The tunnel endpoint is specified by the IP Address. Enter the WAN IP of Company A, 61.11.11.11.



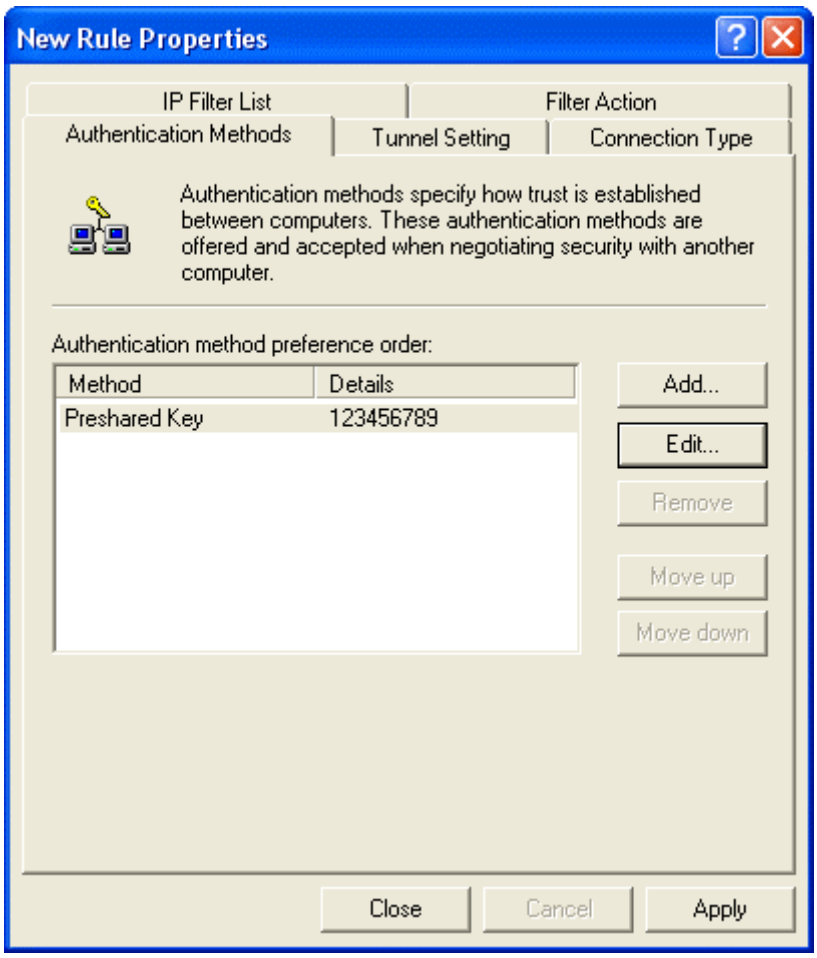
Step 24. Click Authentication Methods and click Edit.



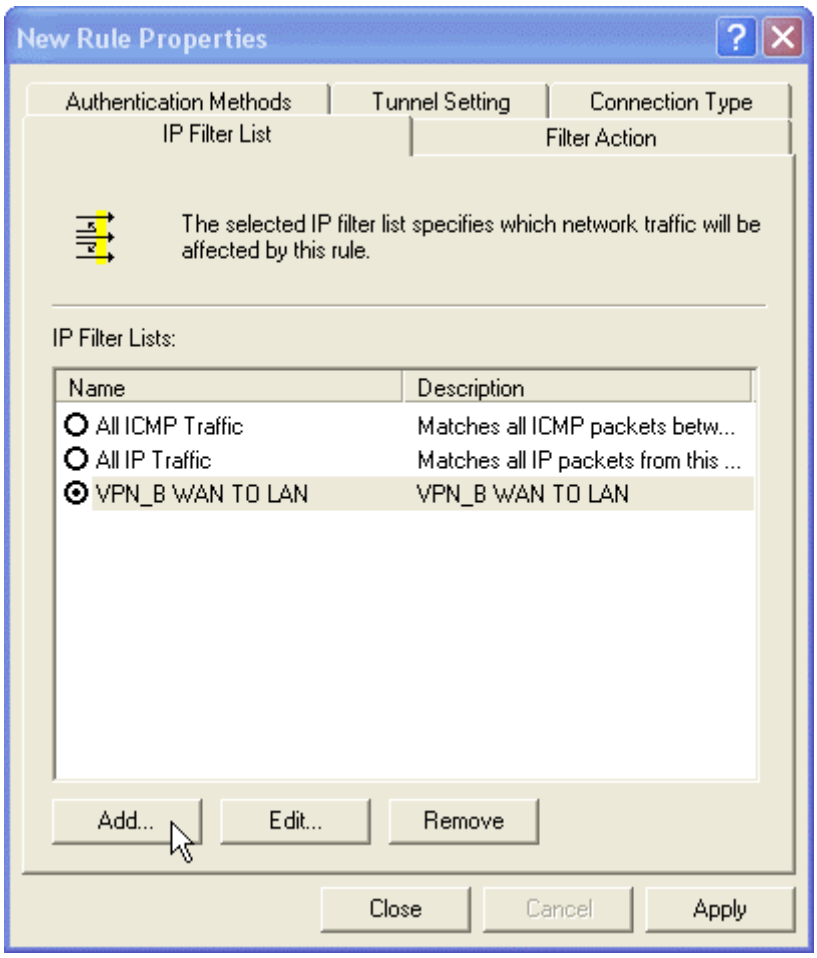
Step 25. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



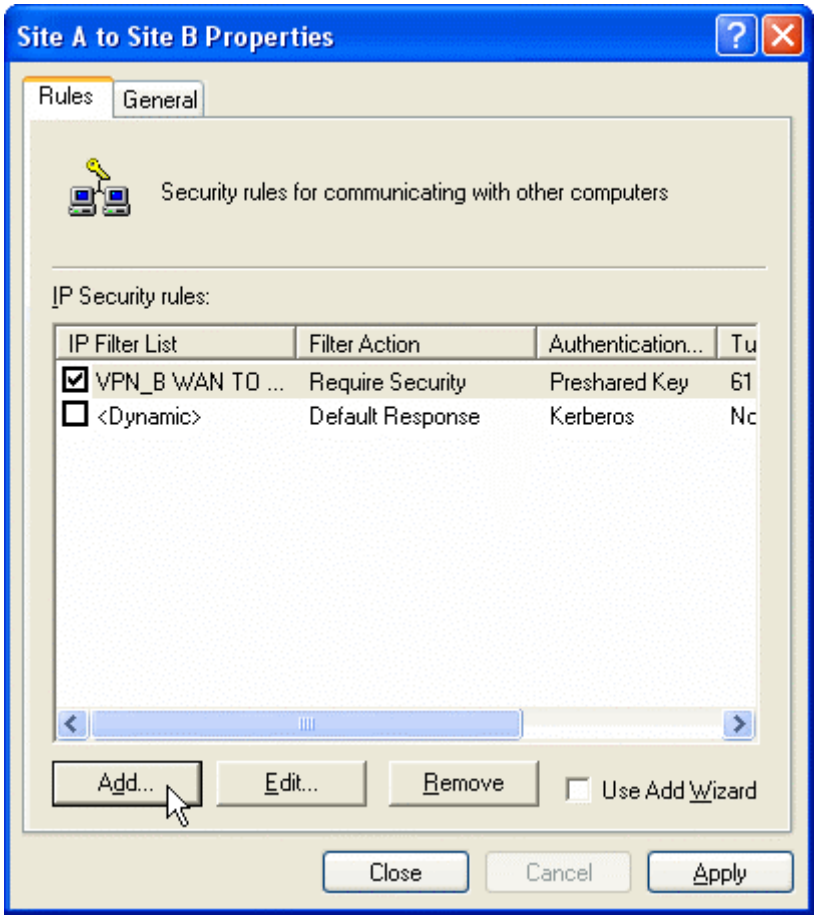
Step 26. Finish the setting, and close the window.



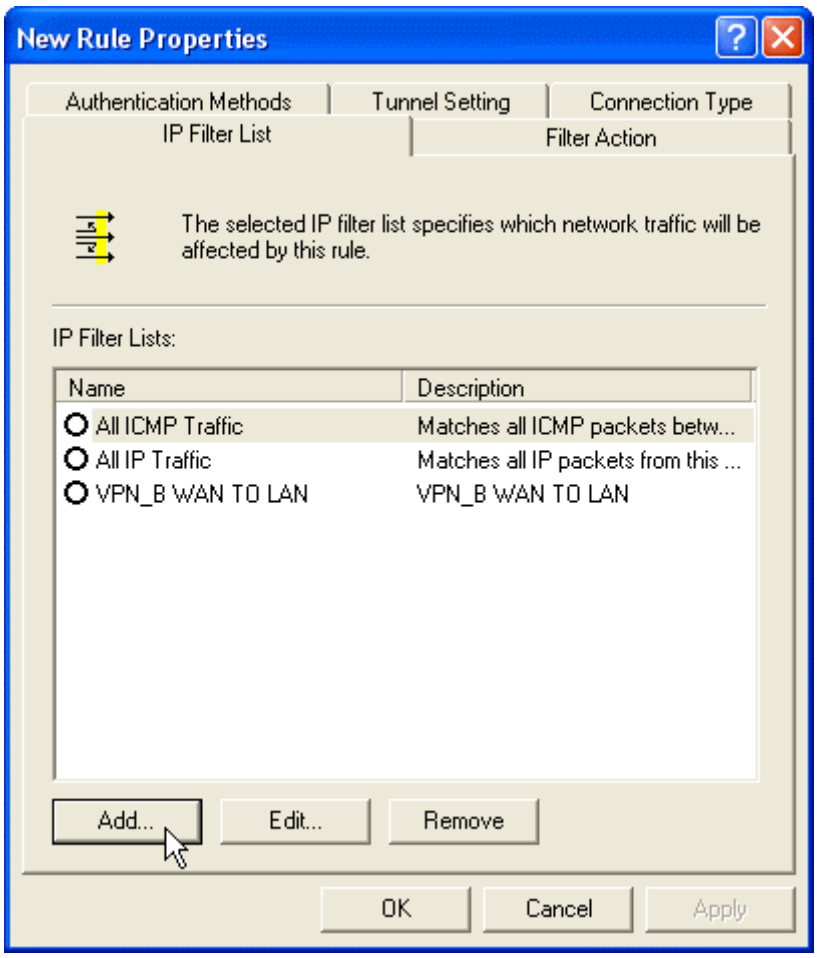
Step 27. Finish the Policy setting of VPN_B WAN TO LAN.



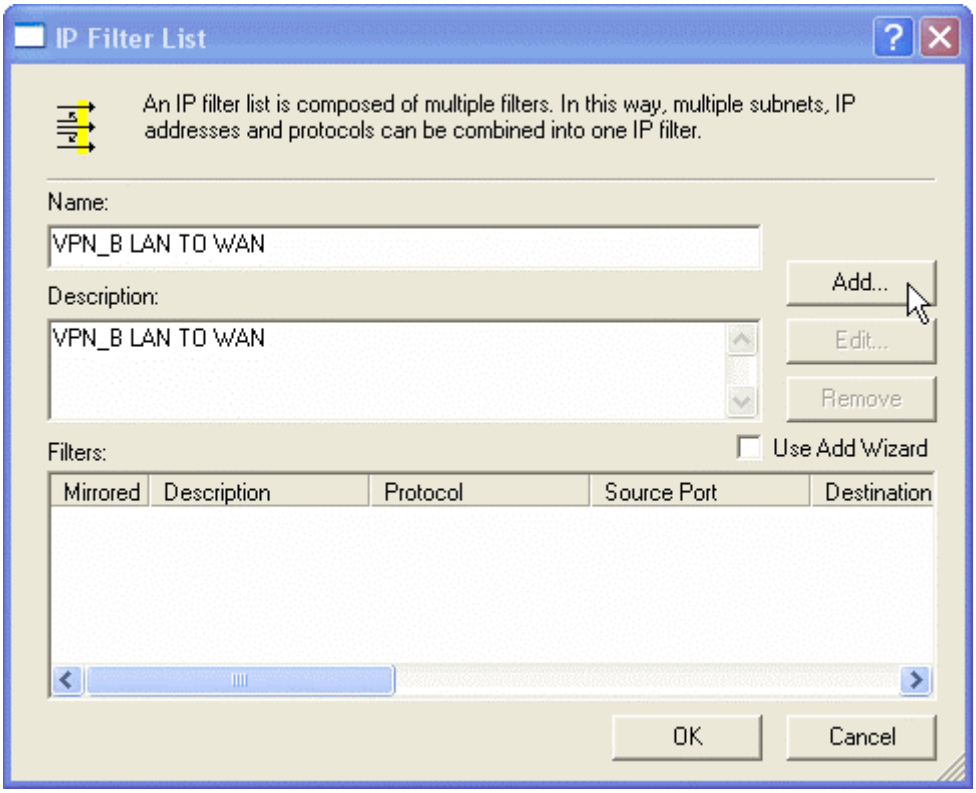
Step 28. Enter VPN_B window again and click Add to add second IP Security Policy. Please don't enable Use Add Wizard.



Step 29. In New Rule Properties, click Add.



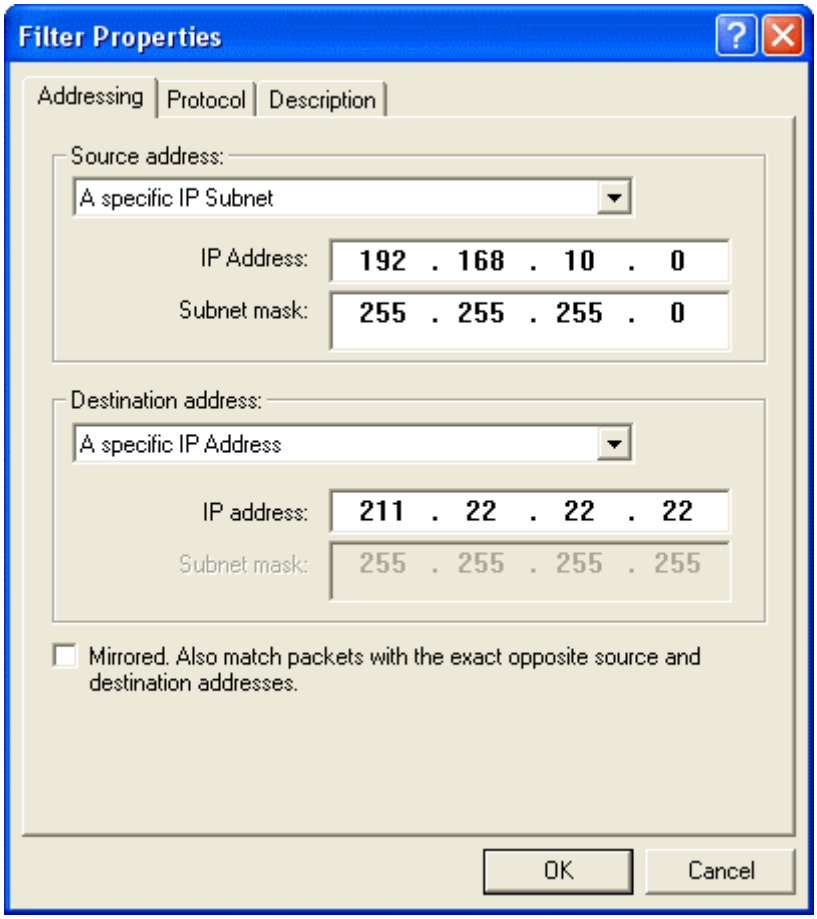
Step 30. In IP Filter List window, please disable Use Add Wizard, and change Name to VPN_B LAN TO WAN. Click Add.



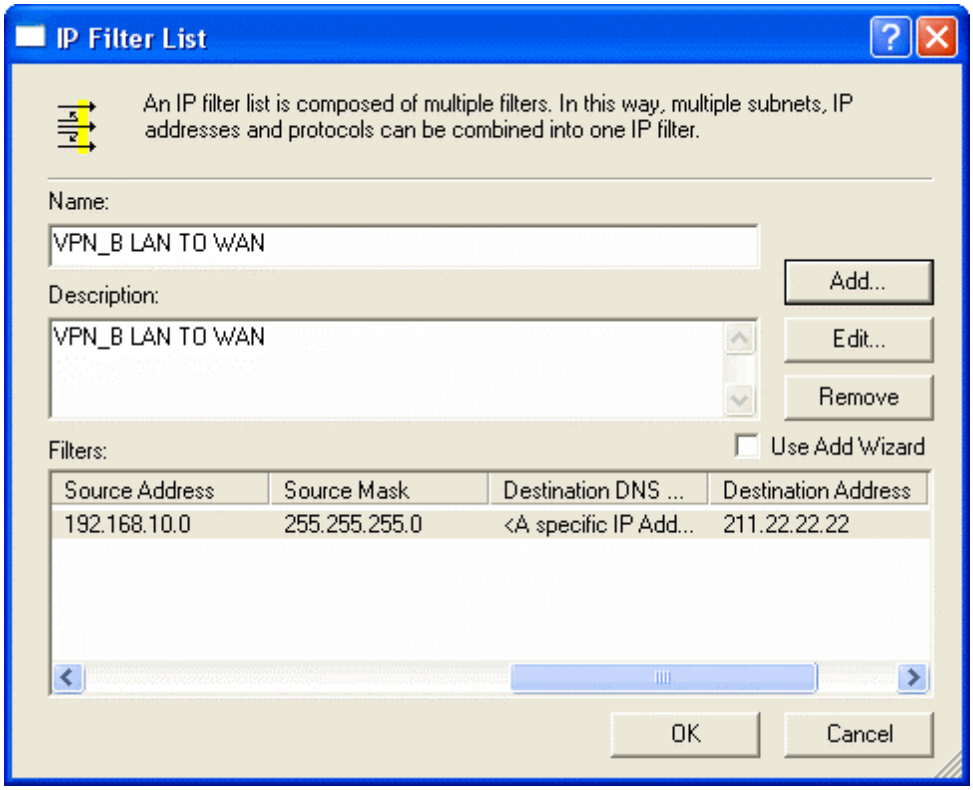
Step 31. In Filter Properties window,

in Source address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.

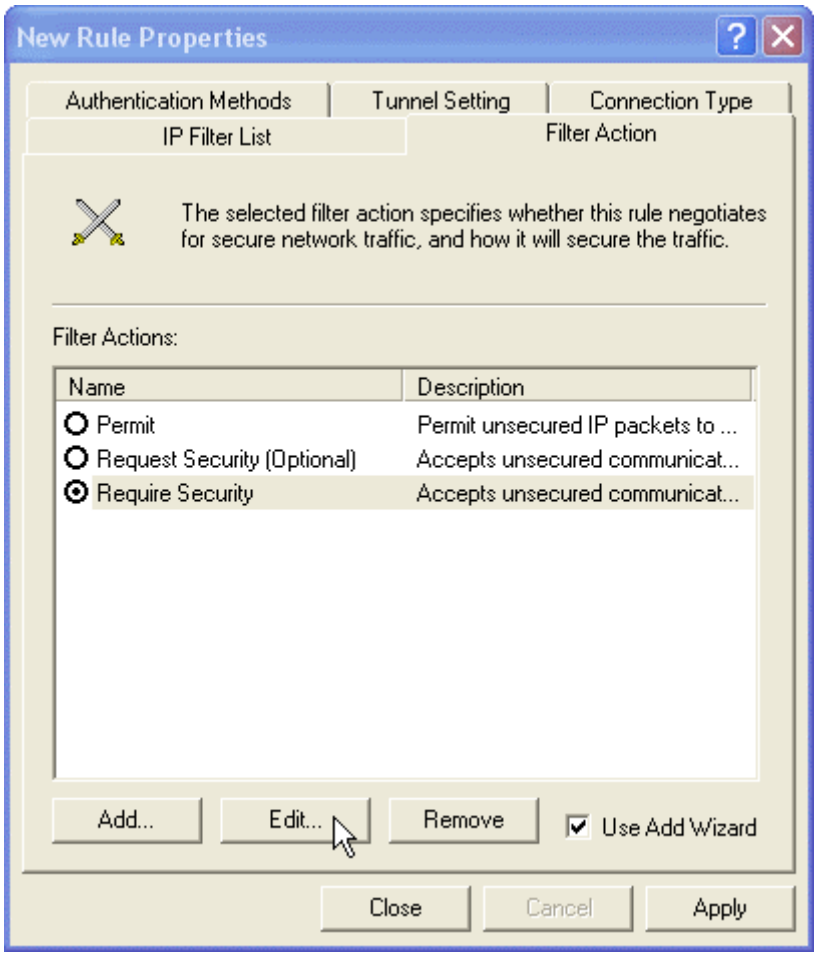
In Destination address click down the arrow to select the specific IP Subnet and fill remote user's IP Address, 211.22.22.22 and Subnet mask, 255.255.255.255., Please disable Mirrored. Also match packets with the exact opposite source and destination addresses.



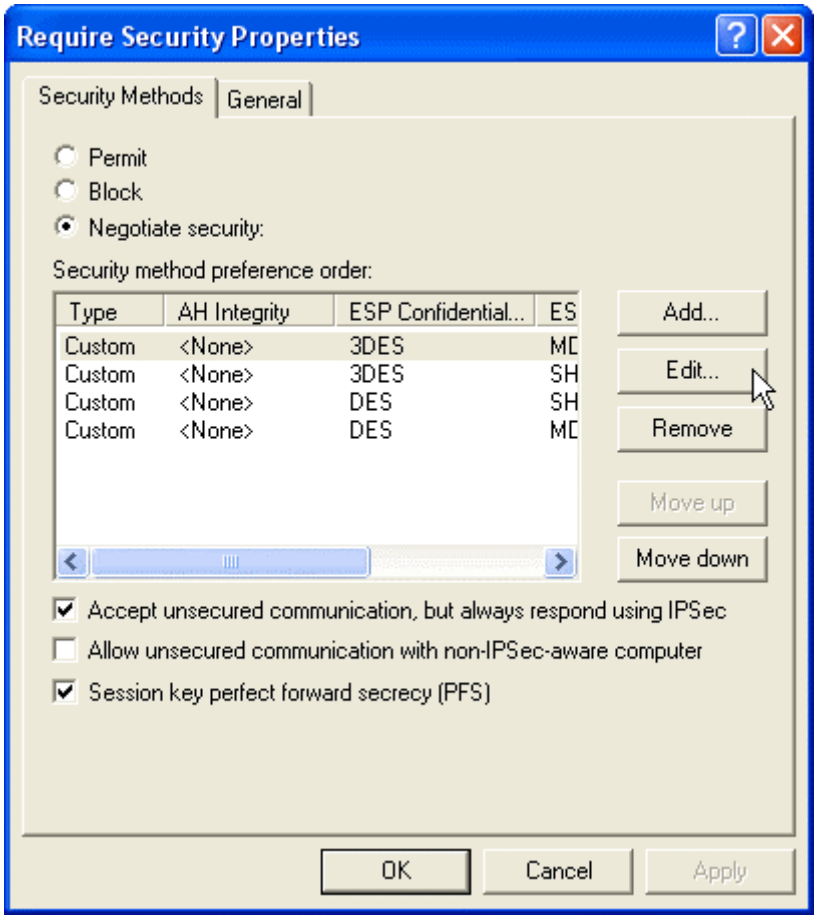
Step 32. Finish the setting and close IP Filter List window.



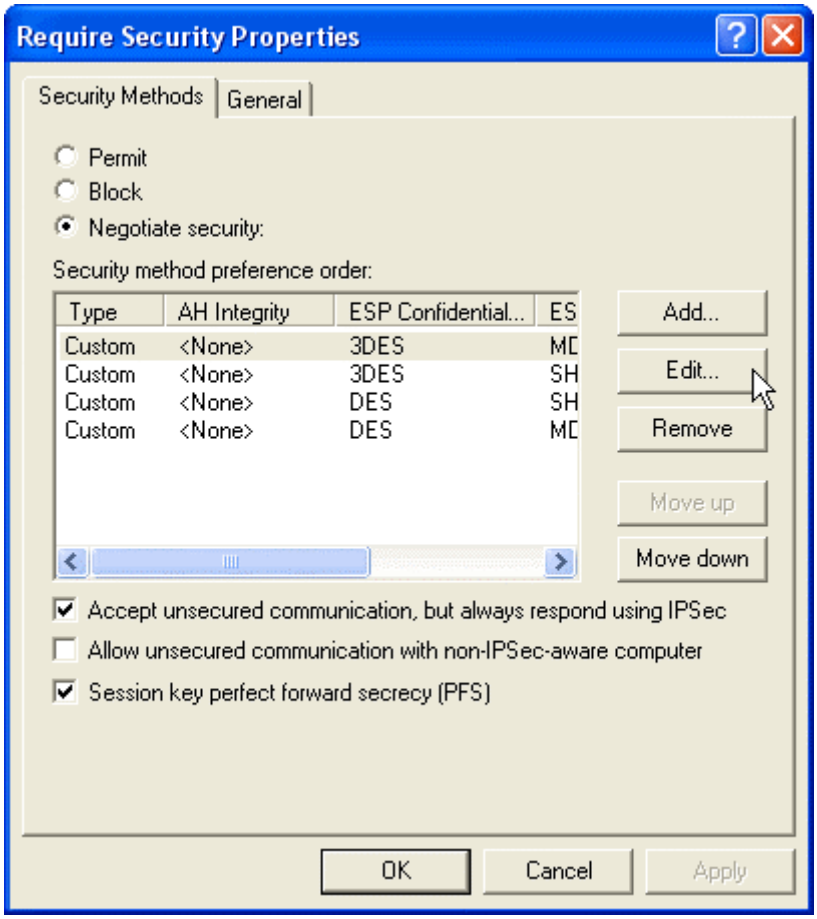
Step 33. Click Filter Action tab and choose Require Security. Click Edit.



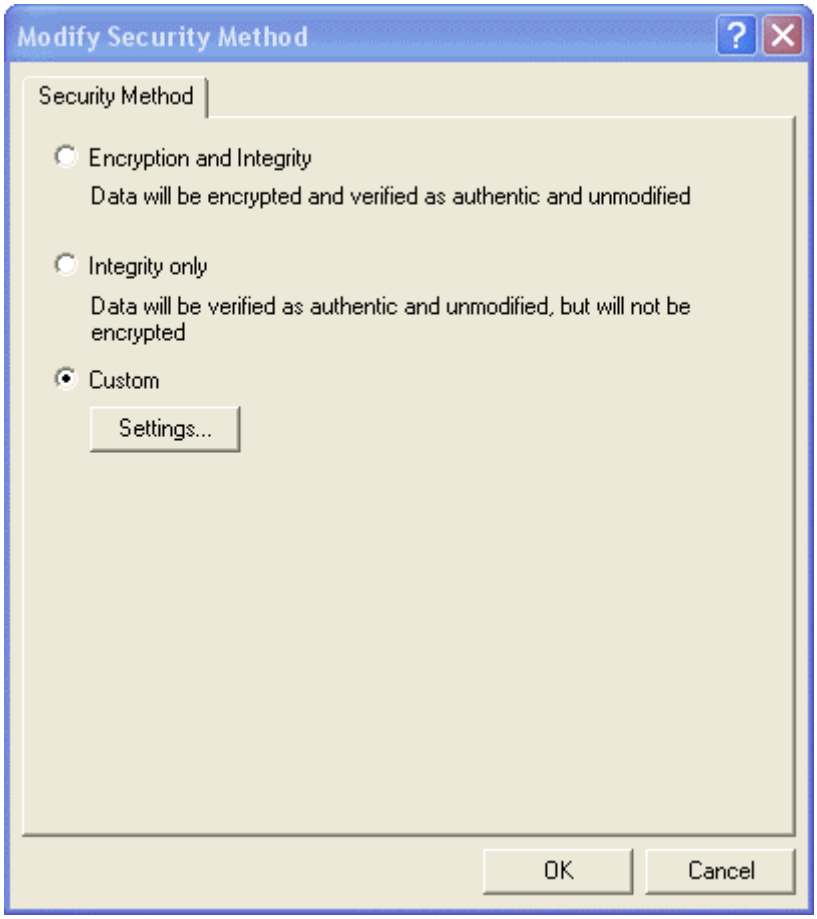
Step 34. In Security Methods tab, choose accept unsecured communication, but always respond using IPSec.



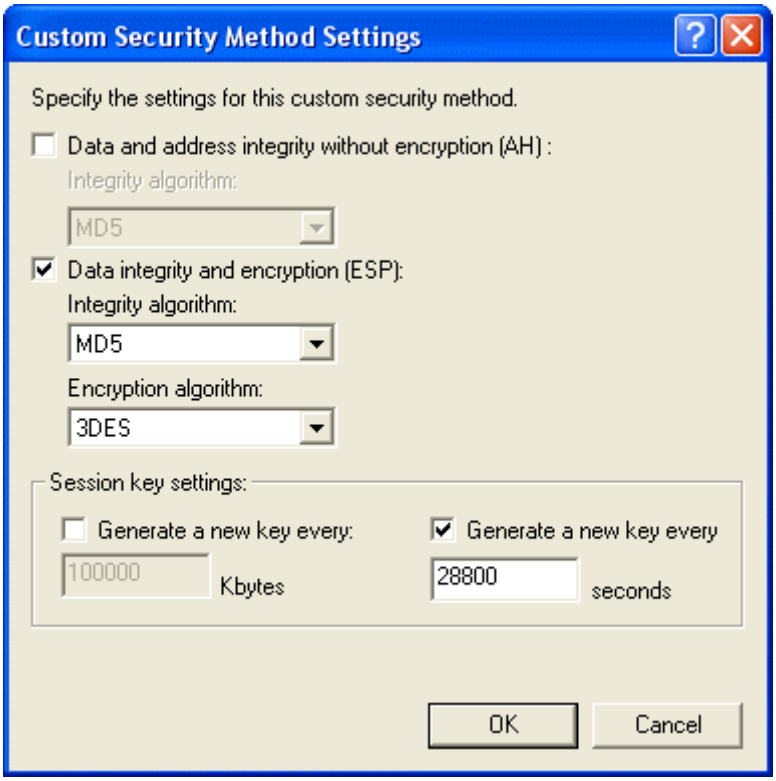
Step 35. Click Edit in Custom/ None/ 3DES/ MD5.



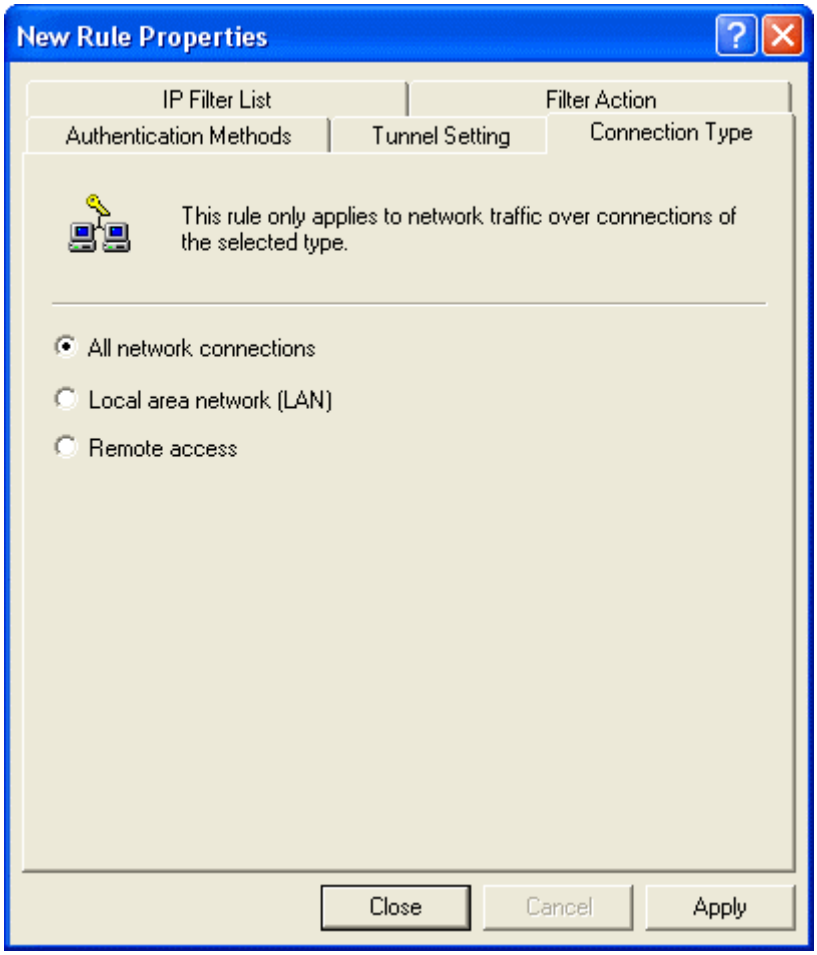
Step 36. Click Custom (For professional user) and click Edit.



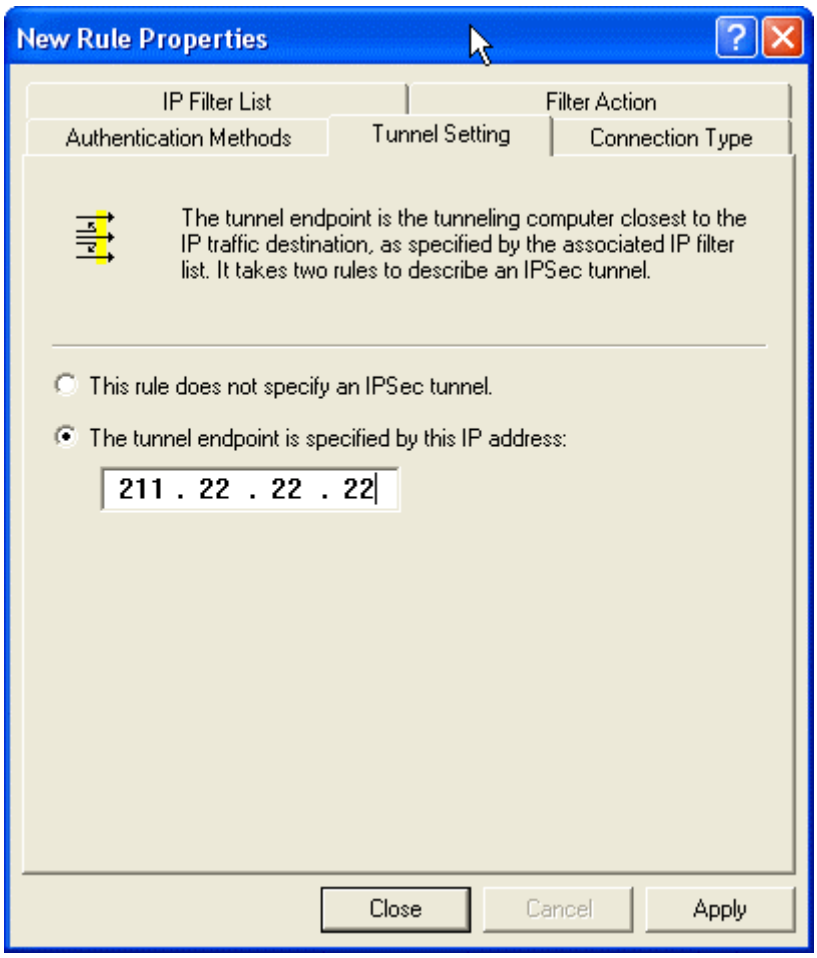
Step 37. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



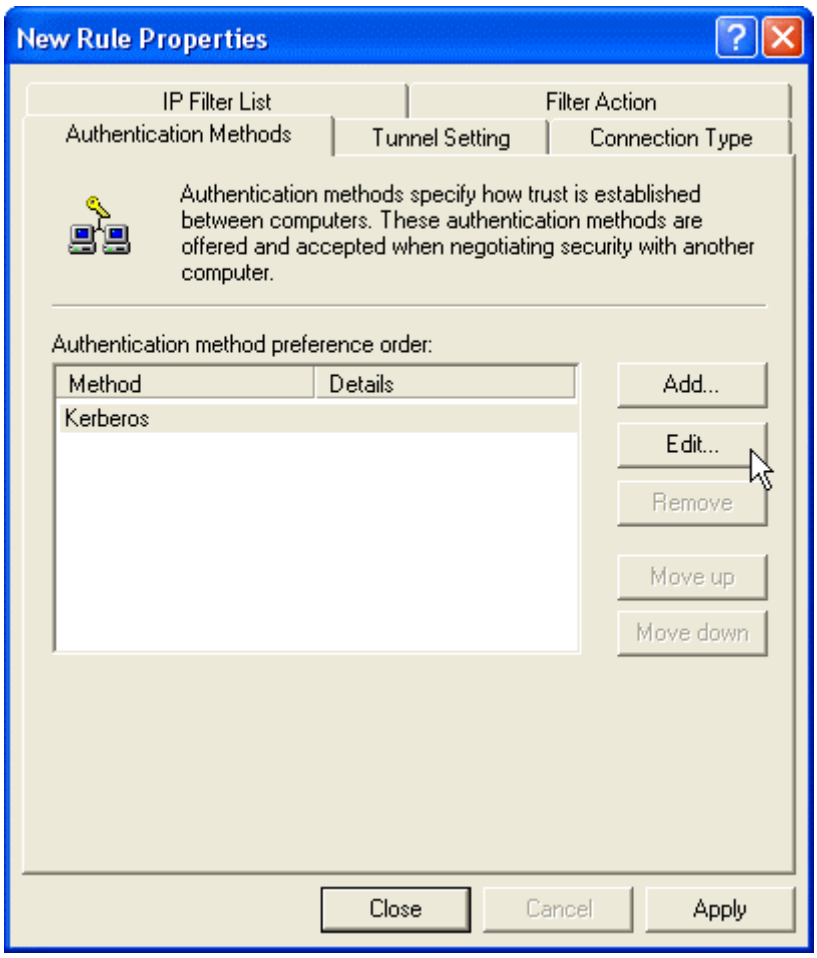
Step 38. Click Connection Type tab and click all network connections.



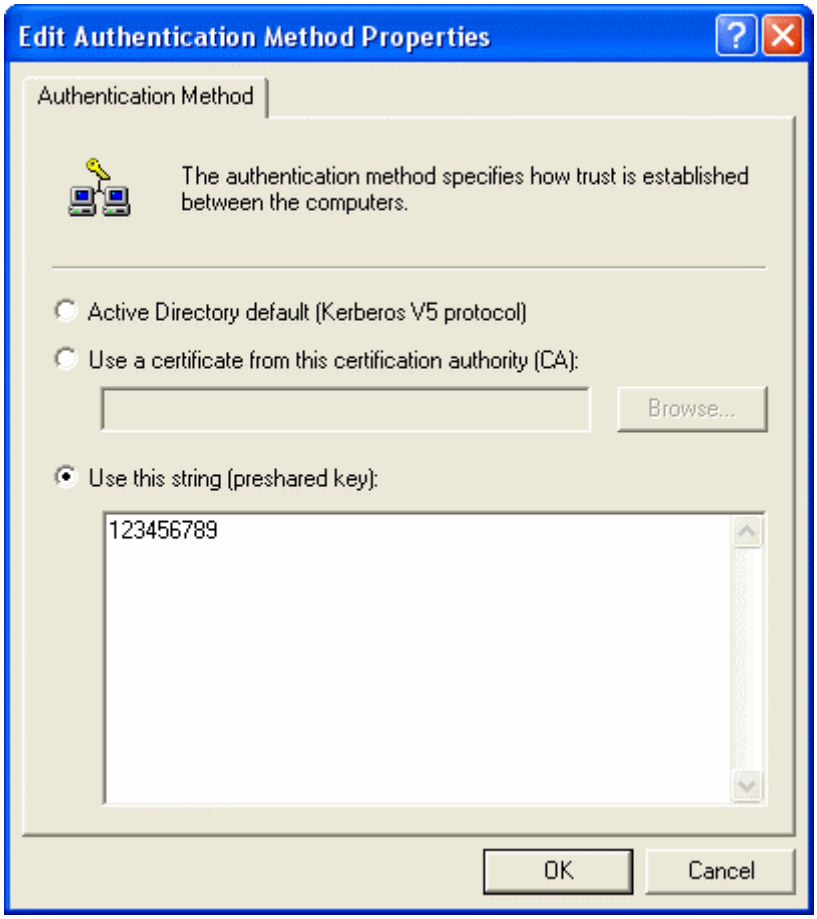
Step 39. Click Tunnel Setting tab, and click The tunnel endpoint is specified by the IP Address. Enter the WAN IP of remote user, 211.22.22.22.



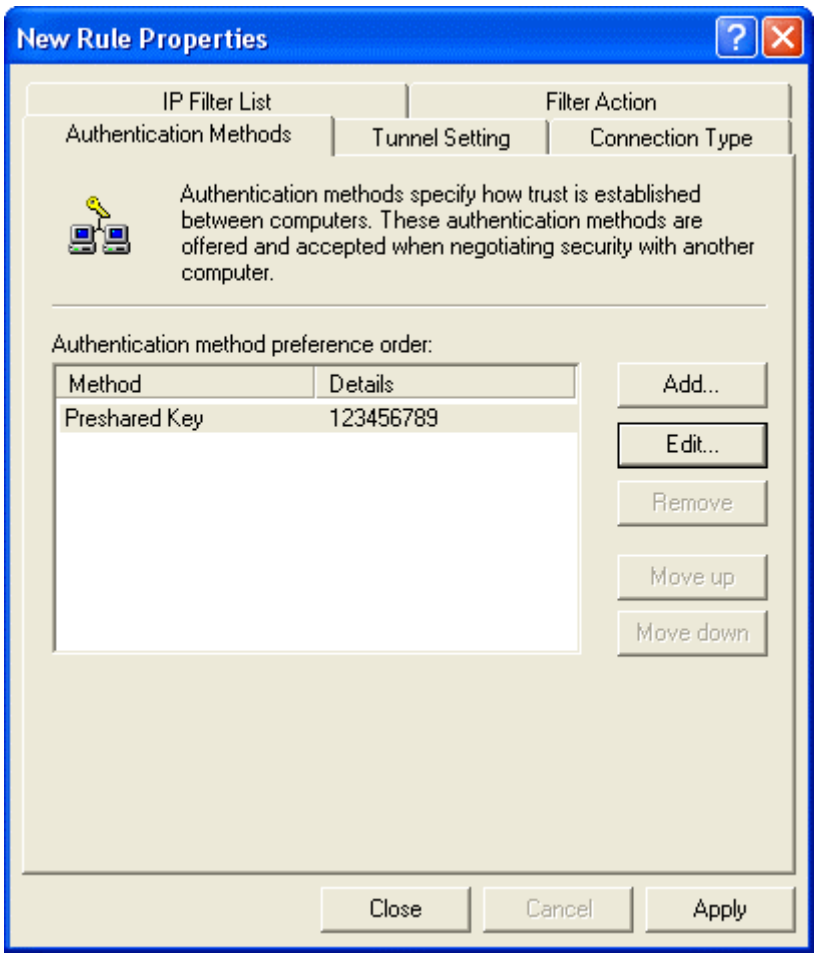
Step 40. Click Authentication Methods and click Edit.



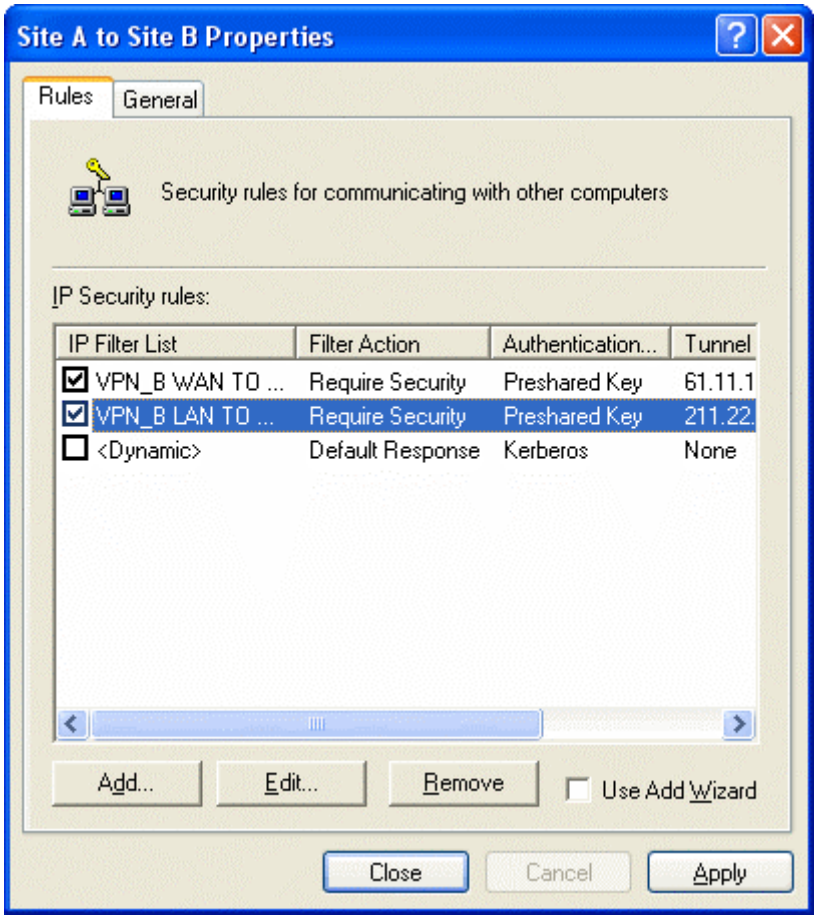
Step 41. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



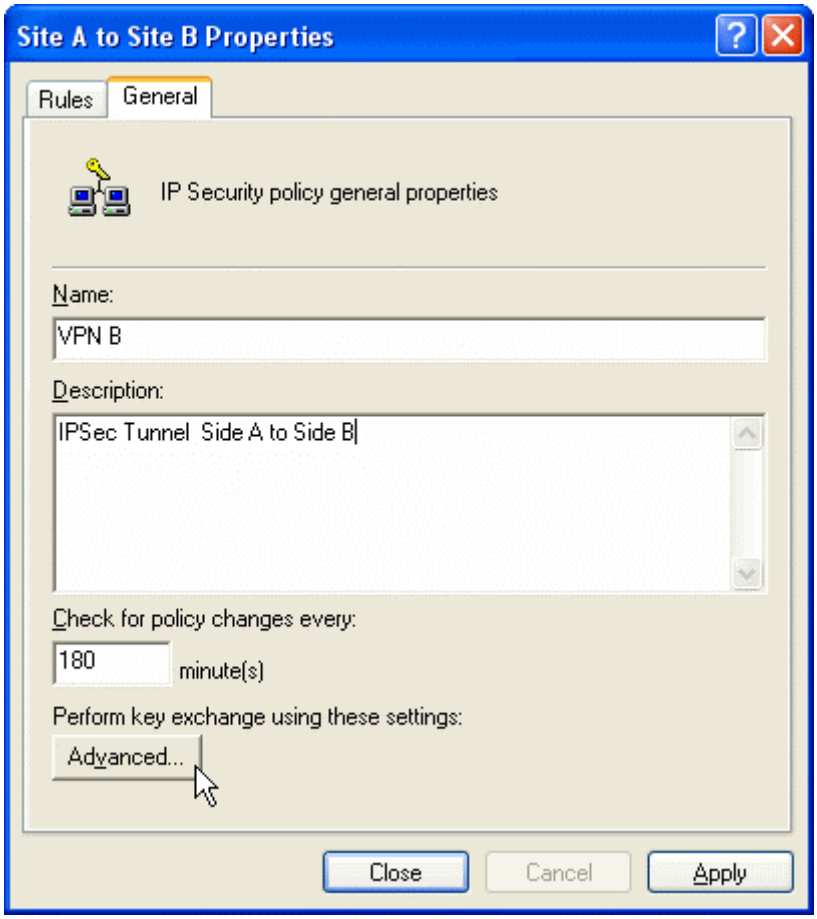
Step 42. Finish the setting, and close the window.



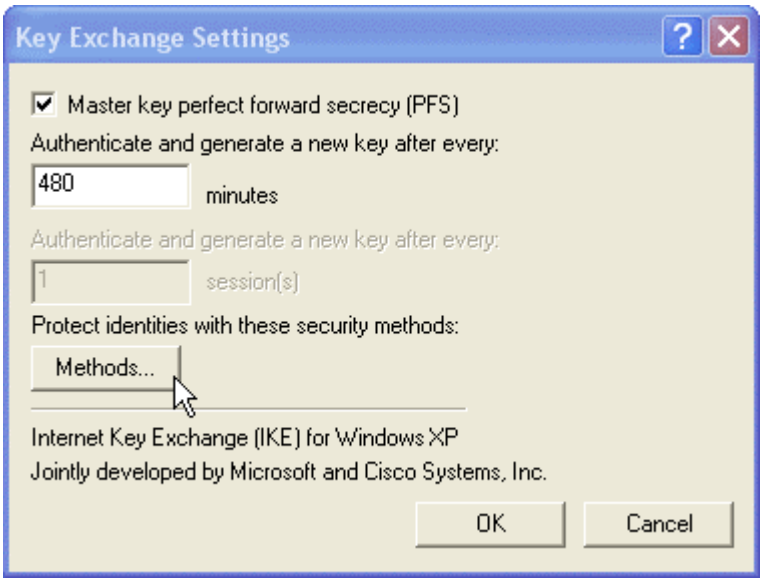
Step 43. Finish the Policy setting of VPN_B LAN TO WAN.



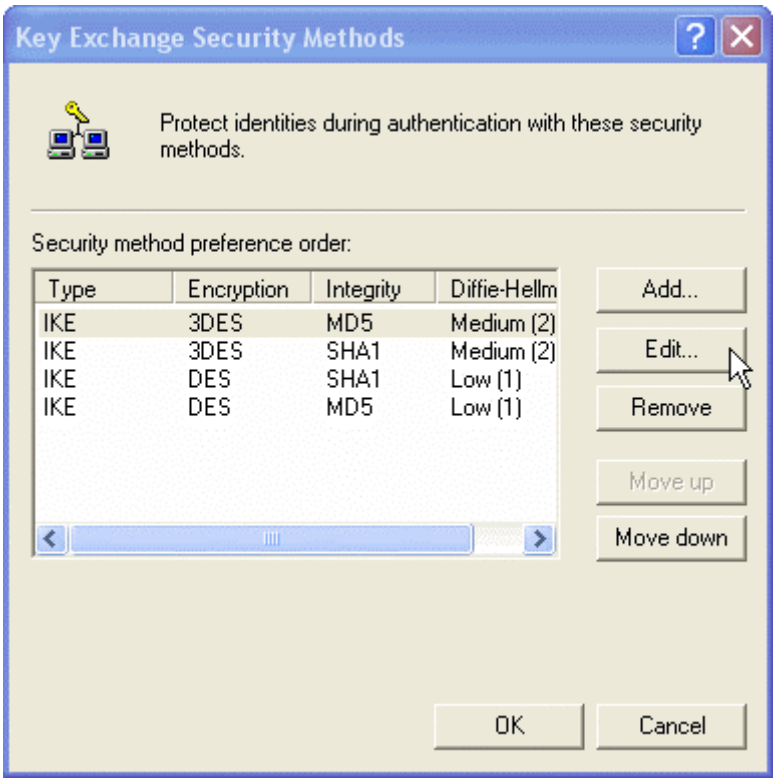
Step 44. In VPN_B window, click General tab. And click Advanced for Key Exchange using these settings.



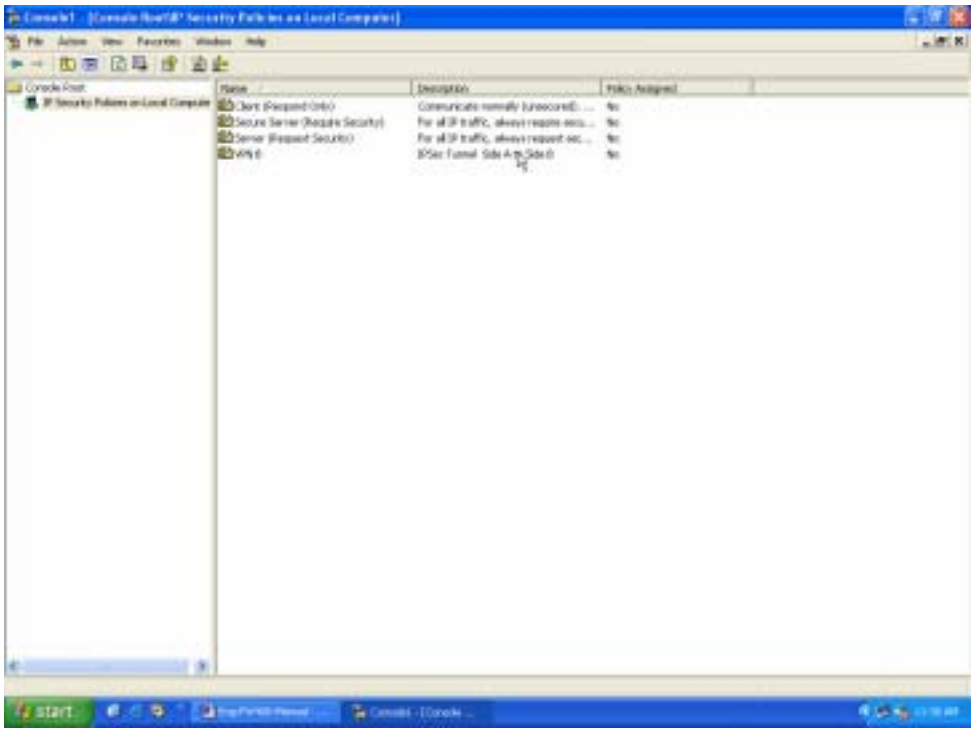
Step 45. Click Master key Perfect Forward Secrecy.



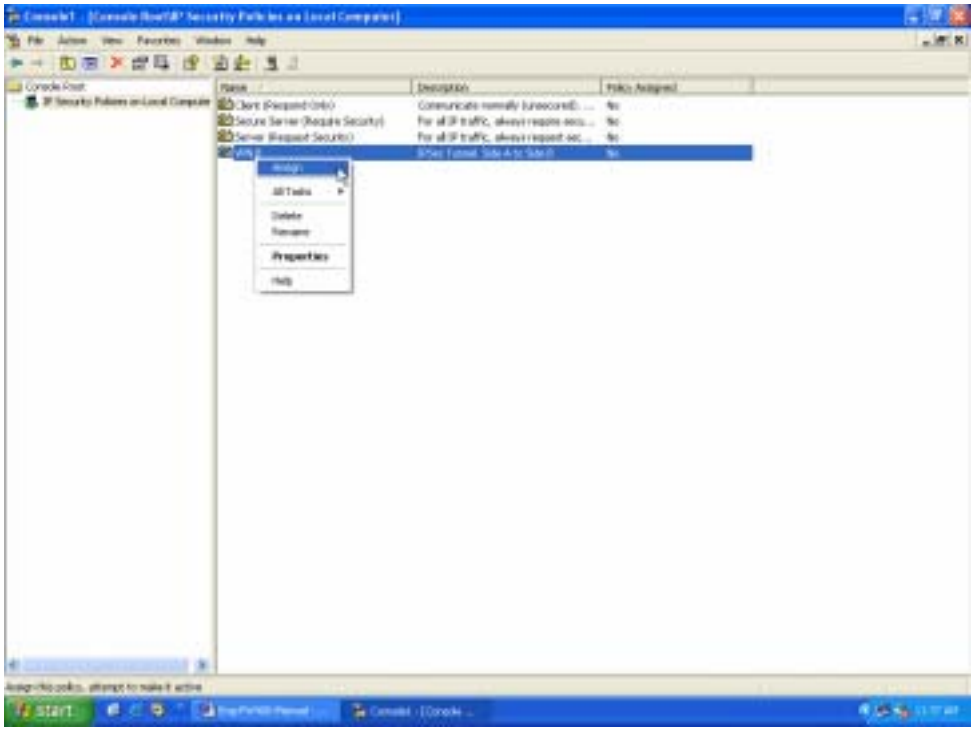
Step 46. Move IKE/ 3DES/ MD5/ up to the highest order. Finish all settings.



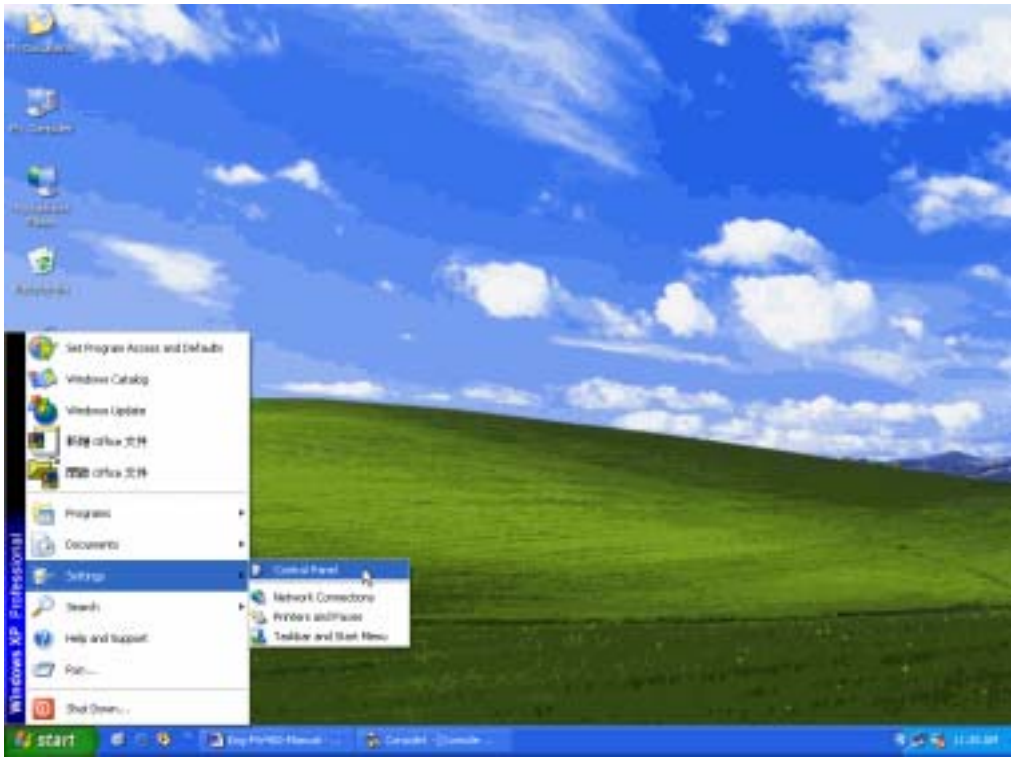
Step 47. Finish the settings of remote user's Windows XP VPN.



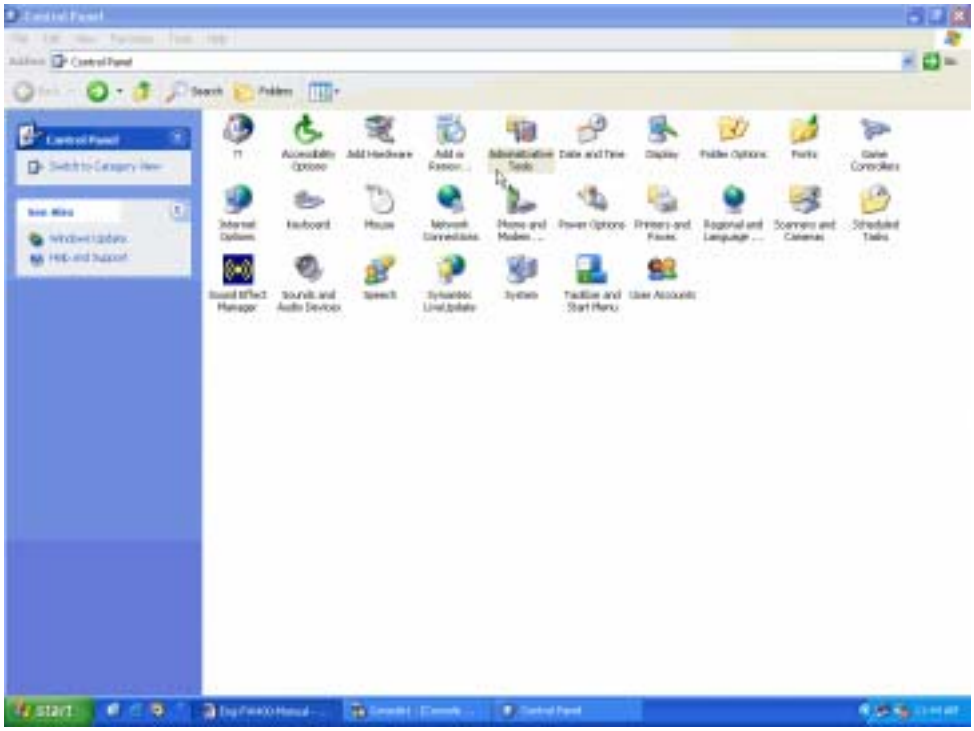
Step 48. Click the right button of mouse in VPN_B and enable Assign.



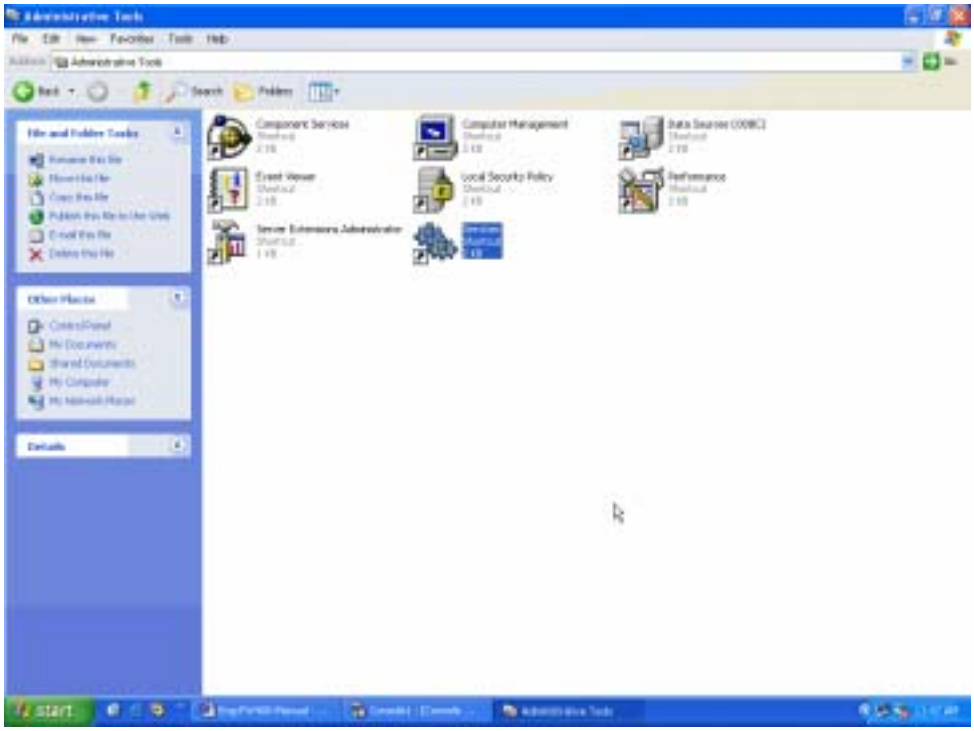
Step 49. To restart IPSec by Start→Settings→Control Panel



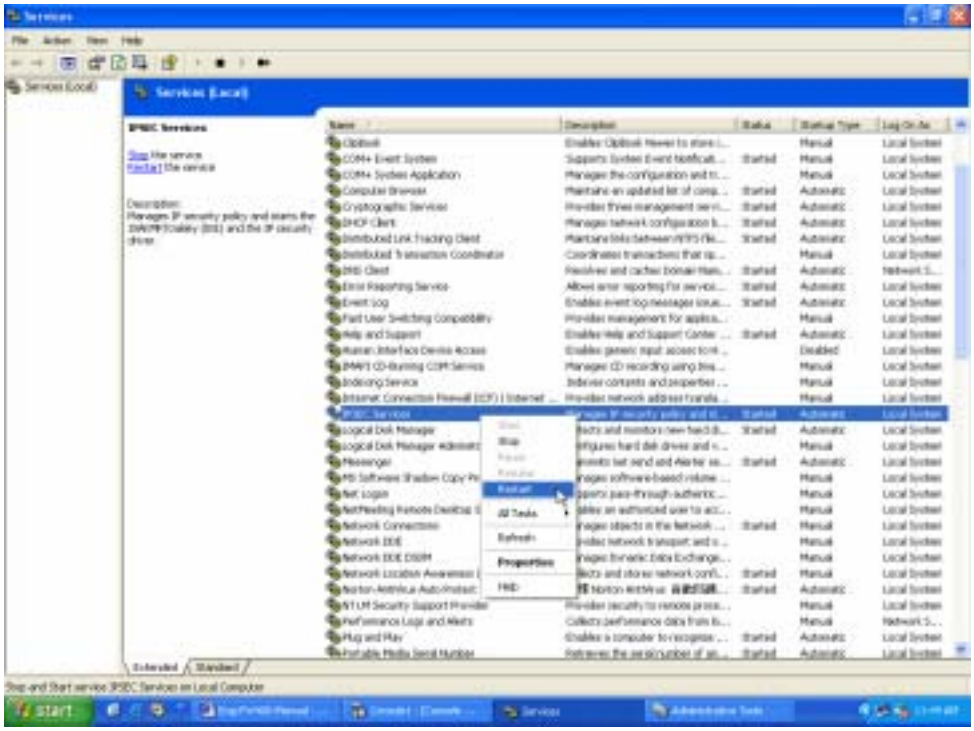
Step 50. Enter Control Panel and click Administrative Tools.



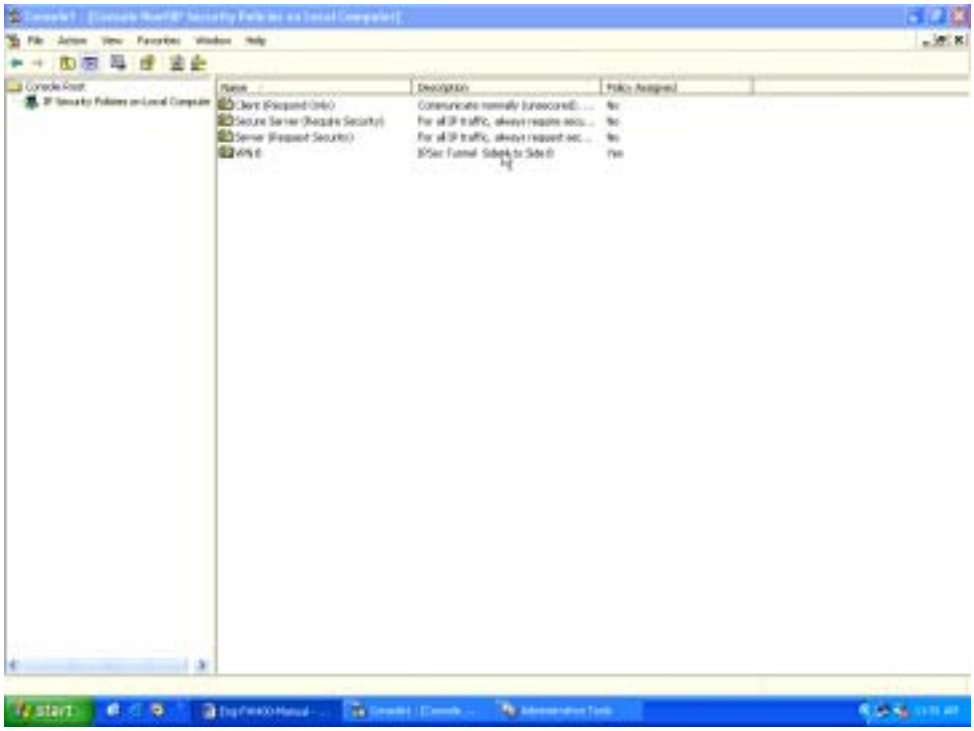
Step 51. After entering Administrative Tools, click Services.



Step 52. After entering Service, click IPSec Services, Restart the Service.



Step 53. Finish all settings.



Example 3. Create a VPN connection between two Multi-Homing Security Gateways using Aggressive mode Algorithm (3 DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel	
Name	VPN_A
From Source ◉ LAN ○ DMZ	
Use interface ◉ WAN1 ○ WAN2	
Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

To Destination	
◉ Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.20.0 / 255.255.255.0
○ Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
○ Remote Client -- Fixed IP or Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Multi-Homing Security Gateway will

automatically choose 3DES for ENC Algorithm, MD5 for AUTH Algorithm and select Group 2 to connect. Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123A and @abcd123.

☑ Aggressive mode	
My ID	@abc123
Peer ID	11.11.11.11

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.20.100

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None

Step 9. Click OK to finish the setting of Company A.

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's Multi-Homing Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel	
Name	VPN_B
From Source ◉ LAN ○ DMZ	
Use interface ◉ WAN1 ○ WAN2	
Subnet / Mask	192.168.20.0 / 255.255.255.0

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination	
◉ Remote Gateway -- Fixed IP	61.11.11.11
Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
○ Remote Client -- Fixed IP or Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Multi-Homing Security Gateway will automatically choose 3DES for ENC Algorithm, MD5 for AUTH Algorithm and select Group 2 to connect. Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123A and @abcd123.

☑ Aggressive mode	
My ID	11.11.11.11
Peer ID	@abc123

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
◉ Authentication Only	

Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.10.100

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None

Step 9. Click OK to finish the setting of Company B.

Example 4. Create a VPN connection between two Multi-Homing Security Gateway using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file by GRE/ IPSec Algorithm.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel		
Name	VPN_A	
From Source	◉ LAN ○ DMZ	
Use interface	◉ WAN1 ○ WAN2	
Subnet / Mask	192.168.10.0	/ 255.255.255.0

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

To Destination		
◉ Remote Gateway -- Fixed IP	211.22.22.22	
Subnet / Mask	192.168.20.0	/ 255.255.255.0
○ Remote Gateway -- Dynamic IP		
Subnet / Mask		/ 255.255.255.0

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation / ISAKMP Algorithm, choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. Choose GRE/ IPSec and enter GRE Source IP, 192.168.50.100 and GRE Remote IP, 192.168.50.200.

NOTE: The Source IP and Remote IP should be in the same C Class.

☑ GRE/IPSec	
GRE Local IP	192.168.50.100
GRE Remote IP	192.168.50.200

Step 7. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

IPSec Algorithm	
◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 8. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	

Step 9. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None

Step 10. Click OK to finish the setting of Company A.

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's Multi-Homing Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel	
Name	VPN_B
From Source ◉ LAN ○ DMZ	
Use interface ◉ WAN1 ○ WAN2	
Subnet / Mask	192.168.20.0 / 255.255.255.0

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination	
◉ Remote Gateway -- Fixed IP	61.11.11.11
Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
○ Remote Client -- Fixed IP or Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method	Preshare
Preshared Key	123456789

Step 5. In Encapsulation -> ISAKMP Algorithm, choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Step 6. Choose GRE/ IPSec and enter GRE Source IP, 192.168.50.200 and GRE Remote IP, 192.168.50.100.

Note. The Source IP and Remote IP should be in the same C Class.

☑ GRE/IPSec	
GRE Local IP	192.168.50.200
GRE Remote IP	192.168.50.100

Step 7. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

◉ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

Step 8. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime.

☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	

Step 9. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None

Step 10. Click OK to finish the setting of Company B.

Example 5. Create a VPN connection between Multi-Homing Security Gateway and PLANET VRT-401 VPN Router.

Preparation Task:

Company A External IP is 172.19.50.29

Internal IP is 192.168.120.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.2.X

To Allow Company A, 192.168.120.100 create a VPN connection with company B, 192.168.2.100 for downloading the sharing file.

Step 1: Configure the Mutli-Homing Secruity Gateway as the following:

VPN Auto Keyed Tunnel	
Name	mh
From Source ◉ LAN ○ DMZ	
Use interface ◉ WAN1 ○ WAN2	
Subnet / Mask	192.168.120.0 / 255.255.255.0
To Destination	
◉ Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.2.0 / 255.255.255.0
○ Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
○ Remote Client -- Fixed IP or Dynamic IP	
Authentication Method	Preshare
Preshared Key	123
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2
IPSec Algorithm	
○ Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
◉ Authentication Only	
☑ Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	
☑ Aggressive mode	
My ID	
Peer ID	
☐ GRE/IPSec	
GRE Local IP	
GRE Remote IP	
Schedule	None
QoS	None
Authentication-User	None
☐ Show remote Network Neighborhood	

OK Cancel

Step 2: Configure VRT-401 VPN policy as the following:

VPN Policy Definition

Policy ☑ Enable
Policy Name: vv

Remote VPN endpoint ○ Dynamic IP
◉ Fixed IP: 172 . 19 . 50 . 29
○ Domain Name:

Local IP addresses
Type: Subnet address IP address: 192 . 168 . 2 . 0 ~ 0
Subnet Mask: 255 . 255 . 255 . 0

Remote IP addresses
Type: Subnet address IP address: 192 . 168 . 120 . 0 ~ 0
Subnet Mask: 255 . 255 . 255 . 0

☐ **AH Authentication** Algorithm: SHA-1
☑ **ESP Encryption** Algorithm: 3DES
☑ **ESP Authentication** Algorithm: SHA-1
○ **Manual Key Exchange**
◉ **IKE (Internet Key Exchange)**

Direction: Both Directions
Local Identity: ◉ IP address
○ Name:
Remote Identity: ◉ IP address
○ Name:
Authentication: ○ RSA Signature (requires certificate)
◉ Pre-shared Key
123
Authentication Algorithm: SHA-1
Encryption: 3DES
Exchange Mode: Aggressive Mode
IKE SA Life Time: 3660 (secs)
☐ IKE Keep Alive Ping IP Address: 0 . 0 . 0 . 0
IPSec SA Life Time: 28000 (secs)
DH Group: Group 2 (1024 Bit)
IKE PFS: Group 2 (1024 Bit)
IPSec PFS: Group 2 (1024 Bit)

Save Cancel

Back Help

4.11.2 PPTP Server

This function allow the remote client dialup to your local network and access local resources by PPTP (Point to Point Tunnel Protocol) client software.

Entering the PPTP Server window

Step 1. Select **VPN→PPTP Server**.

- **PPTP Server**：Click **Modify** to select Enable or Disable.
- **Client IP Range**: Display the IP addresses range for PPTP Client connection.
- **User Name**：Displays the PPTP Client user's name for authentication.
- **Client IP**：Displays the PPTP Client's IP address for authentication.
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Status**：Displays current connection status between PPTP Server and PPTP client.
- **Configure**：Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Modifying PPTP Server Design

Step 1. Select **VPN→PPTP Server**.

Step 2. Click **Modify** after the Client IP Range.

Step 3. In the **Modify** Server Design Window, enter appropriate settings.

- **Disable PPTP**：Check to disable PPTP Server.
- **Enable PPTP**：Check to enable PPTP Server.

  Encyption: the default is set to disabled.

  Client IP Range: Enter the IP range allocated for PPTP Clients when they connect to the PPTP server.
- **Auto-Disconnect if idle** ☐ **minutes**: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Schedule**：Click the down arrow to select the schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Adding PPTP Server

Step 1. Select **VPN→PPTP Server**. Click **New Entry.**

Step 2. Enter appropriate settings in the following window.

- User name: Specify the PPTP client. This should be unique.
- Password: Specify the PPTP client password.
- Remote Client:

  ☐ Single Machine: Check to connect to single computer.

  ☐ Multi-Machine: Check to allow multiple computers connected to the PPTP server.

  IP Address: Enter the PPTP Client IP address.

  Netmask: Enter the PPTP Client subnet mask.

- Client IP assigned by:
  1. IP Range: check to enable auto-allocating IP for PPTP client to connect.
  2. Fixed IP: check and enter a fixed IP for PPTP client to connect.

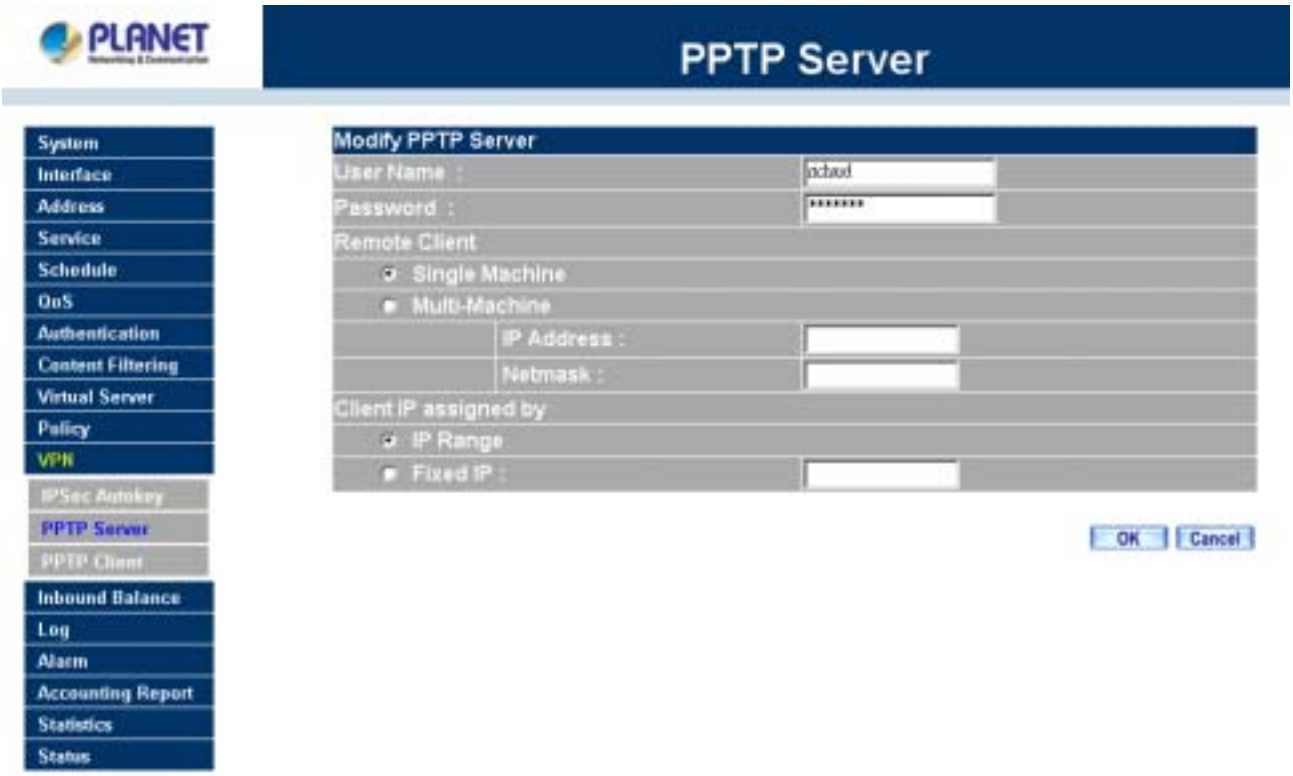
Step 3. Click **OK** to save modifications or click **Cancel** to cancel modifications.

Modifying PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you want to modify. Click **Configure** and click **Modify**.

Step 3. Enter appropriate settings.



Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you WAN t to modify. Click **Configure** and click **Remove**.

Step 3. Click **OK** to remove the PPTP server or click **Cancel** to exit without removing.

4.11.3 PPTP Client

This function allows the Multi-Homing Security Gateway dial-up to remote PPTP server and access the network resources on remote network.

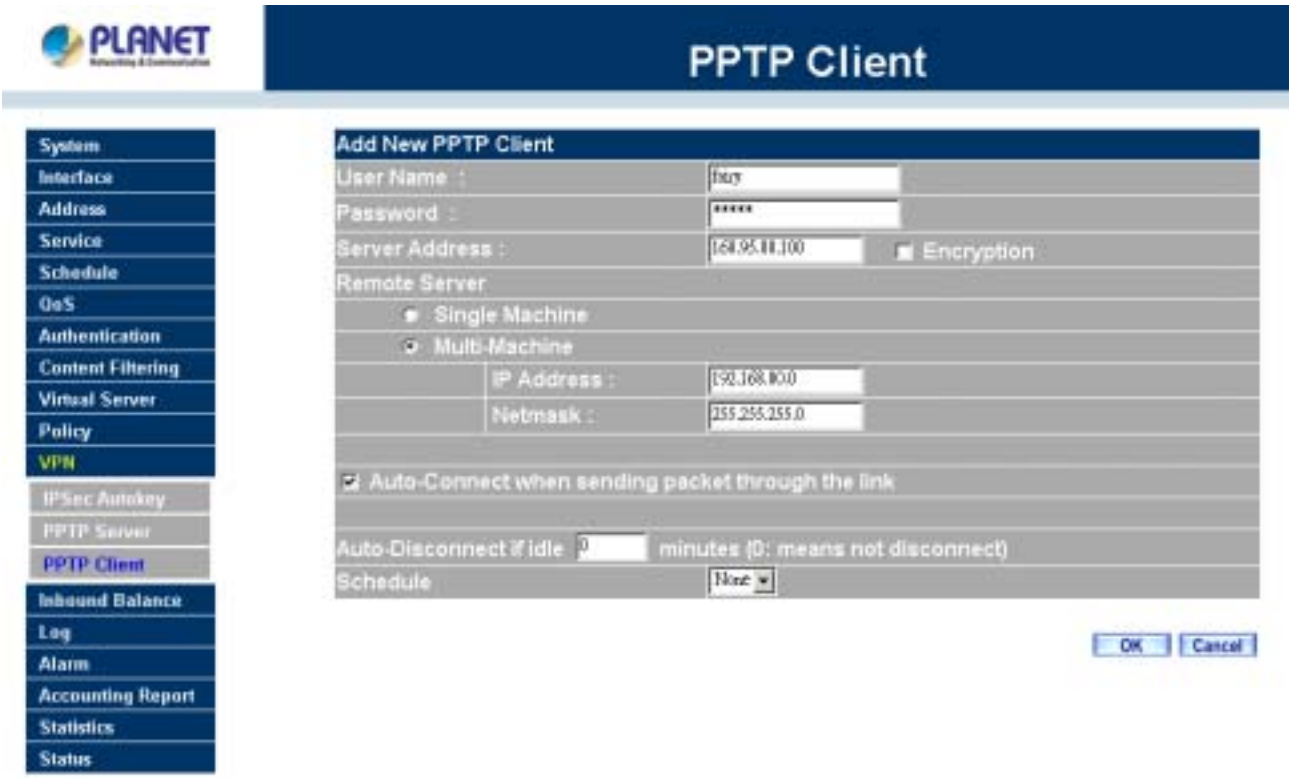
Entering the PPTP Client window

Step 1. Select **VPN→PPTP Client**.

- **Server Address**s：Display the PPTP Server IP addresses..
- **User Name**：Displays the PPTP Client user's name for authentication.
- **Server IP**：Displays the PPTP Server's IP address for authentication.。
- **Encryption**：Displays the PPTP Client Encryption ON or OFF
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Status**：Displays current connection status between PPTP Server and PPTP client.
- **Configure**：Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Adding a PPTP Client

Step 1. Select **VPN→PPTP Client**.



Step 2. Configure the parameters.

- **User name:** Specify the PPTP client. This should be unique.
- **Password:** Specify the PPTP client password.
- **Server Address:** Enter the PPTP Server's IP address.
- **Encryption:** Enable or Disabled the Encryption.
- **Remote Server:**

  ☐ **Single Machine:** Check to connect to single computer.

  ☐ **Multi-Machine:** Check to allow connecting to multiple computers on remote site.

  IP Address：Enter the PPTP Client IP address.

  Netmask: Enter the PPTP Client subnet mask.
- **Auto-Connect when sending packet through the link**: Check to enable the auto-connection whenever there's packet to transmit over the connection.
- **Auto-Disconnect if idle □ minutes**: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Schedule**：Click the down arrow to select the schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

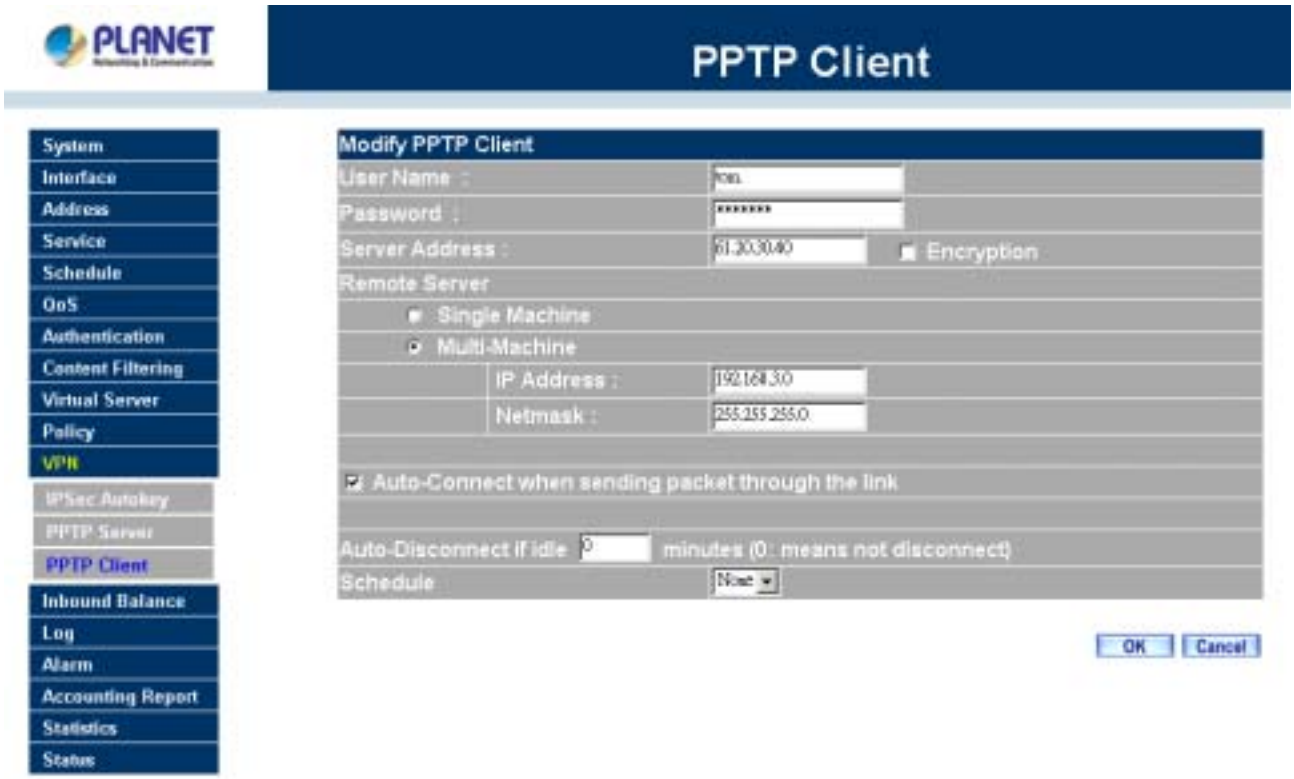
Step 3. Click **OK** to save modifications or click **Cancel** to cancel modifications.

Modifying PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the **PPTP Client** window, find the PPTP server that you want to modify and click **Modify**.

Step 3. Enter appropriate settings.



Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the **PPTP Client** window, find the PPTP client that you want to modify and click **Remove**.

Step 3. Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.

PLANET
PPTP Client
System
Interface
Address
Service
Schedule
QoS
Authentication
Content Filtering
Virtual Server
Policy
VPN
IPSec Autokey
PPTP Server
PPTP Client
Inbound Balance
Log
Alarm
Accounting Report
Statistics
Status
PPTP Client :
User Name
Server Address
Encryption
Uptime
Status
Configure
tom
61.20.30.40
OFF

Disconnect
Connecting
Modify
Remove
fairy
168.95.89.100
OFF

Disconnect
Connecting
Modify
Remove
New Entry
Microsoft Internet Explorer
Do you really want to delete?
OK
Cancel

4.12 Inbound Balance (MH-4000 only)

The Multi-Homing Security Gateway provides the function of Inbound Load Balance to the enterprise's website. When customers visit the website and the internet is disconnected, customers still can connect to the website via the other lines instead of missing the chance of business.

NOTE: This function is not supported on MH-2000.

This chapter describes the detail introduction of Inbound Load Balance and steps to setup Inbound Load Balance.

Pre-requirement

1. Register the Domain Name, for example, planet.com.tw. You need to visit the Network Information Center in local (i.e., the origination in Taiwan and China is TWNIC (Taiwan Network Information Center) and CNNIC (China Network Information Center) respectively) to register the domain name.
2. Suppose the IP Address which is registered as below,
   61.11.11.11 ~ 61.11.11.15
   211.22.22.22~ 211.22.22.26
3. Setup the Primary Domain Name Server:
   Host Name：dns1.planet.com.tw
   IP Address：61.11.11.11
   Setup the Secondary Domain Name Server:
   Host Name：dns2.planet.com.tw
   IP Address：211.22.22.22

Enter the Inbound Load Balance configuration page

Click on **Inbound Balance** on the menu, the following page is shown.

Domain Name: The IP Address isn't suitable for users to memorize and manage. So there's the Domain to map it. The format of Domain is xx.xx.xx.xx i.e., ftp.planet.com.tw or www.planet.com.tw. It's more convenient to use the meaningful words as Domain instead of the meaningless IP number. There are two parts of the address of website, host name and domain name. If the user would like to browse the website of Yahoo, he may encounter the Yahoo via entering www.yahoo.com in the browser. As a matter of fact, the Address of Yahoo is 66.218.71.84. The Multi-Homing Security Gateway provide the DNS Server to deal with the process of mapping the Domain Name (Yahoo) and IP(66.218.71.84).

Enable: Enable or Disable of the domain.

Configure: Click **Modify** to make further configuration and **Remove** to delete the domain.

New Entry: Click **New Entry** to add new domain.

Add New Domain

Click the New Entry button on Inbound Balance page to add new domain. The following page is shown.

Domain Name: The domain name you applied from your local network information centre.

Enable DNS Zone: Enable the configuration of domain name.

Name: The service name before the Domain Name. For example, www, ftp, mail, etc.

Type: A for Address, CNAME for Canonical NAME and MX for Mail eXchanger.

Address: The IP Address of this server.

Backup: The server whether enable the function of backup or not and the System Administrator could chose WAN 1/2.

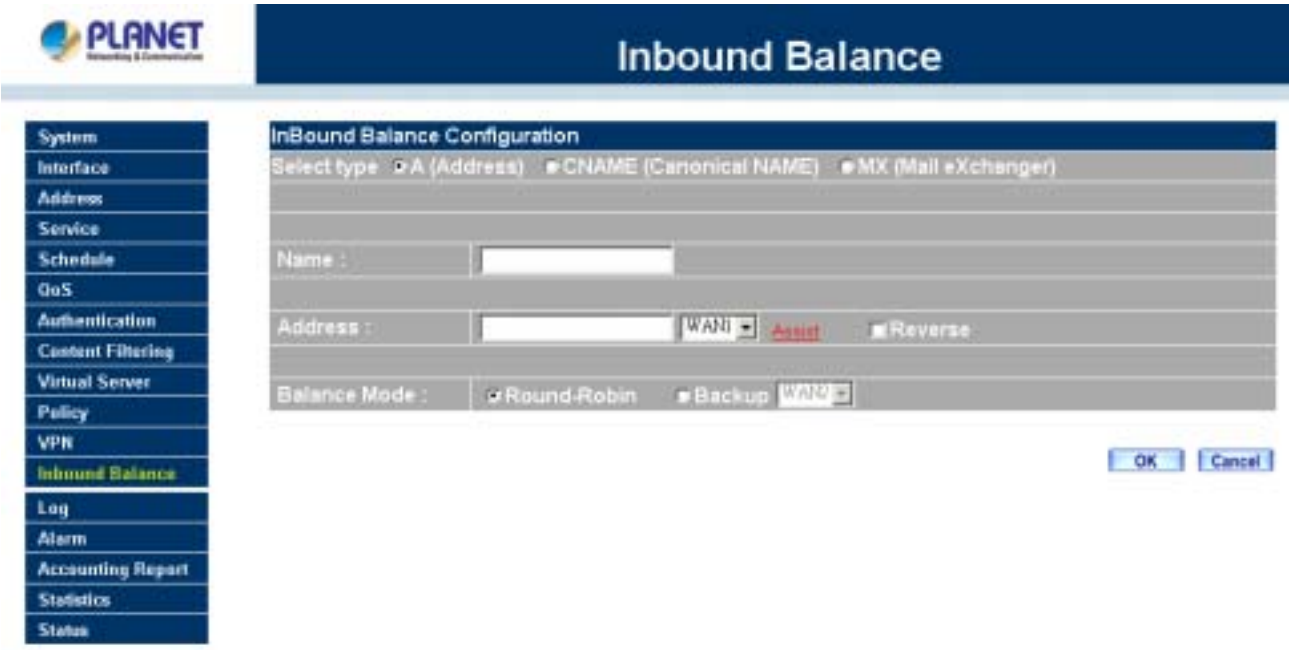
Weight: The Multi-Homing Security Gateway would distribute the DNS inquiry WAN ports via the weight number. Each number stands for the round-robin distribution.

Priority: Adjust the priority of each WAN IP address.

Click **OK** to create the domain and click **New Entry** to add host DNS name.

Add New Host DNS name

On the domain configuration page, click **New Entry** to add host DNS name. The following page is shown.



Select type: There are 3 selectable types as below.

1. A (Address):

Set up the mapping of Domain Name and IP Address. For example, address record the mapping relation of Domain Name and IP Address.

Domain Name	Type	IP Address
host1.planet.com.tw	A	61.11.11.12
host2.planet.com.tw	A	61.11.11.13
host2.planet.com.tw	A	211.22.22.23

"A" stands for Address, and each record provides each Domain Name map into each IP Address. Because the host2 server has 2 IP Address, there are 2 records in the data file of DNS. The DNS request can return not only one IP Address for each Domain Name, and it may sort the DNS request result via *address-sorting* or *round-robin*.

2. CNAME

CNAME stands for the record of alias. The mechanism can provide Record A to have more than one name(Alias) for querying. For example the 2nd record provide the Alias of server map into it's formal name, host5.planet.com.tw.

Domain Name	Type	IP Address
Host5.planet.com.tw	A	61.11.11.14
Host23.planet.com.tw	CNAME	Host5.planet.com.tw

The alias name, host23.planet.com.tw may map into the formal name, host5.planet.com.tw. So when user ping host23.planet.com.tw, it'll get the IP Address, 61.11.11.14.

3. MX

"MX" stands for Mail Exchange Server. This mechanism would inquire about the mail server. The advantage is that the System Administrator may change the mail server via updating the DNS

Record here. And the remote mail server doesn't need to care to communicate with which mail server. For example, this mechanism is provided for the service of Internet Email for special DNS record.

Domain Name	Type	IP Address
host25.planet.com.tw	A	211.22.22.24
mail.planet.com.tw	MX	host25.planet.com.tw

Enter the command in DOS, nslookup-type-MX mail.planet.com.tw*(nslookup is the command of DNS uery -type is the type of DNS Record and mail.planet.com.tw is the uerying DNS Name)* , the result show the Mail Exchange Server(host25.planet.com.tw) which is mapping into the mail.planet.com.tw and the IP Address(211.22.22.24) of the server (host25.planet.com.tw).

If the engineer of Customer Service Center may send an E-Mail to the customer, support@planet.com.tw . The engineer may send the mail via test.com.tw as SMTP Server. And the server(test.com.tw) could decide how to send the mail to the server(mail.planet.com.tw) via DNS Request. The server will send E-mail via the destination server of host3.planet.com.tw. (Via SMTP Protocol)

Name: Enter the service name before the Domain Name, it can be defined by user.

Address: The IP address of WAN port for remote user to connect to local server.

Reverse: Use IP Address to reverse the Domain Name. There're 2 mechanisms for DNS Mapping, Reverse and Forward. Here's an example of Forward. By entering www.planet.com.tw, the DNS Server may convert the Domain Name into 203.70.249.1. The opposite method is Reverse.

Balance Mode: The are two balance mode-

Round-Robin: According to specific weight and priority to distribute the load sharing from WAN to LAN.

Backup: After selecting the backup mode, if the defined WAN port of Multi-Homing Security Gateway encounters disconnection, the device will return this IP address for future DNS inquiry.

Click **OK** to confirm the configuration and **Cancel** to discard.

Advanced Introduction

Announcement the domain name is managed by which DNS Server. All the records about that domain name could be queried in this primary DNS Server, for example, the domain name or IP Address of website, or the alias name or IP Address of mail server. So the DNS Server should be searched via the Internet actually and the DNS record should be accurate.

According to the International usage and enhance the reliability and security, the DNS system must point to 2 DNS Servers.

Example:

Suppose we would like to setup a DNS Server applied as below situation:

1. Register a domain name, planet.com.tw.
2. The IP Address of Primary DNS Server is 61.11.11.11, and the host name is main.planet.com.tw.
   The IP Address of Secondary DNS Server is 211.22.22.22, and the host name is main.planet.com.tw.
3. Connect to the Internet via Leased line or ADSL(Fixed IP).
4. Address Resolution for the following servers:
   www.planet.com.tw (192.168.1.100) Web Server
   mail.planet.com.tw (192.168.1.101) E-Mail Server

At first, we have to register 2 leased line/ADSL line for fixed IP.

Suppose the IP range provided by the ISP is below,

61.11.11.11 ~ 61.11.11.15

211.22.22.22~ 211.22.22.26

Visit the Network Information Center in local (i.e., the origination in Taiwan and China is TWNIC (Taiwan Network Information Center) and CNNIC (China Network Information Center) respectively) and register the domain name.

The Primary DNS Server:

Host Name：dns1.planet.com.tw

IP Address：61.11.11.11

The Secondary DNS Server:

Host Name：dns2.planet.com.tw

IP Address：211.22.22.22

NOTE: The domain name which is register to the local Network Information Center should map to Fixed IP absolutely.

The System Administrator may configure the below data in the function of InBound Balance of the Multi-Homing Security Gateway:

Name	Type	Address	Reverse	Weight	Priority
main.planet.com.tw	A	61.11.11.11	O	1	1
main.planet.com.tw	A	211.22.22.22	O	1	2

So, the 1st DNS Server(main.planet.com.tw) and 2nd DNS Server(main.planet.com.tw) should both record the above data. The mechanism of backup is that the 2nd DNS Server can run automatically to replace the 1st DNS Server which can't run well for uncertain reasons.

From the above table, the System Administrator could enter the command in DOS, nslookup, to test the Forward/Reverse Address Resolution.

C:\>nslookup main.planet.com.tw

…

Address Name: main. planet.com.tw

Address: 61.11.11.11----------> **Test whether if the domain name map to IP or not accurately.**

Enter the command in DOS, nslookup, to test if the backup function of 2nd DNS Server is enabled automatically or not when the 1st DNS Server is disconnected or can't run well.

C:\>nslookup main.planet.com.tw

…

Address Name: main.planet.com.tw

Address: 211.22.22.22 ----------> **Test whether if the function of backup is enabled automatically and smoothly or not. (Forward)**

C:\>nslookup 61.11.11.11

…

Address Name: main.planet.com.tw

Address: 61.11.11.11 ----------> **Test whether the domain name map to IP accurately or not. (Reverse)**

C:\>nslookup 211.22.22.22

…

Address Name: main.planet.com.tw

Address: 211.22.22.22 ----------> **Test whether if the function of backup is enabled automatically and smoothly or not. (Reverse)**

The System Administrator may configure the below data in the function of Inbound Balance of the Multi-Homing Security Gateway:

Name	Type	Address	Weight	Priority
web.planet.com.tw	A	61.11.11.11	1	1
web.planet.com.tw	A	211.22.22.22	2	2
www.planet.com.tw	CNAME	web.planet.com.tw	--	--

From the above table, the System Administrator could enter the command in DOS, nslookup, to test the Forward/Reverse Address Resolution.

C:\>nslookup

…

> server 61.11.11.11 ----------> **Change to your own DNS Server**

Default Server：main.planet.com.tw

Address: 61.11.11.11

> www.planet.com.tw ----------> **Test if the web server could map to the IP Address accurately. (Forward)**

Server: main.planet.com.tw

Address: 61.11.11.11

Name: web.planet.com.tw ----------> **The server s alias(www.planet.com.tw) map to the formal domain name(web.planet.com.tw).**

Addresses: 61.11.11.11 ----------> **Test the result is accurate.**

Aliases: www.planet.com.tw ---------> **The alias of web server(web.planet.com.tw).**

So the DNS Server records the mapping relation with domain name and IP Address.

In the above table, we can learn the conclusion below.

When users query the DNS name of www.planet.com.tw, the sequence of entering the website is as below.

The first user enter the server of 61.11.11.11

The second user enter the server of 211.22.22.22

The third user enter the server of 211.22.22.22

The fourth user enter the server of 61.11.11.11

The fifth user enter the server of 211.22.22.22

The sixth user enter the server of 211.22.22.22

……

The Multi-Homing Security Gateway would distribute the load sharing to different WAN ports sequentially via round-robin and weight repeatedly. That's the mechanism of Inbound Load Balance via round-robin and weight for conquering the over-loading problem of WAN link in most of enterprises.

In the MX Record of the following table, the less number of priority has much higher priority. Suppose there is an user would like to send an e-mail to support@mail.planet.com.tw, the user may send the mail via test.com.tw as SMTP Server. And the server(test.com.tw) could decide how the server(test.com.tw) to send the mail via DNS Request.

At first, the System Administrator can learn the 2 MX Records from querying mail.planet.com.tw below.

Name	Type	Address	Reverse	Weight	Priority
mail.planet.com.tw	MX	smtp1.planet.com.tw	X	--	1

mail.planet.com.tw	MX	smtp2.planet.com.tw	X	--	2

Because the number of priority, 1, has the highest priority, the Multi-Homing Security Gateway would use the server, smtp1.planet.com.tw, to send e-mail(via SMTP Protocol) by default. If the 1st server can't run well, it will send the e-mail to the server with second priority automatically.

Inbound Load Balance Examples

The following provide 4 examples for testing the Inbound Load Balance feature.

Example 1	Setup【WEB Server】and Type is 【A】 for 【Back up】in Inbound Load Balance.
Example 2	Setup【WEB Server】and Type is 【A】 for 【Round-Robin】in Inbound Load Balance.
Example 3	Setup【WEB Server】and Type is 【CNAME】 for 【Round-Robin】in Inbound Load Balance.
Example 4	Setup【MAIL Server】for 【Round-Robin】in Inbound Load Balance.

Preparation

The domain name of DNS Server should map into Fixed IP.

Enter the WAN window under the Interface menu.

In WAN 1 and WAN 2 window respectively, enter relating parameter below:

WAN 1 IP: 61.11.11.11

WAN 2 IP: 211.22.22.22

Have the DNS's domain name (broadband.com.tw) provided by ISP registered in Network Information Center.

Primary DNS Server

Host Name：dns1.broadband.com.tw

IP Address：61.11.11.11

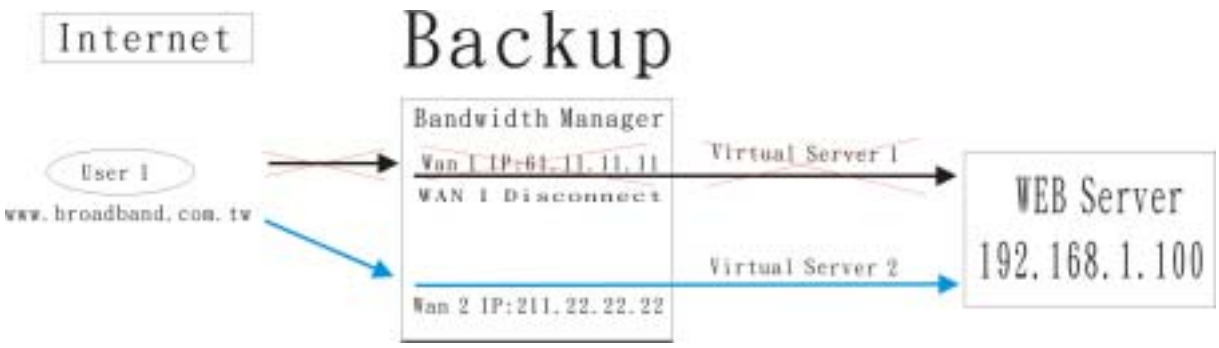
Secondary DNS Server

Host Name：dns2.broadband.com.tw

IP Address：211.22.22.22

Example 1: Setup【WEB Server】and Type is 【A】 for 【Back up】in Inbound Load Balance.

【Backup】: For providing stable and reliable connection service quality, the Multi-Homing Security Gateway provide this mechanism in setup of Inbound Load Balance. Below is the detail setup description for this function:

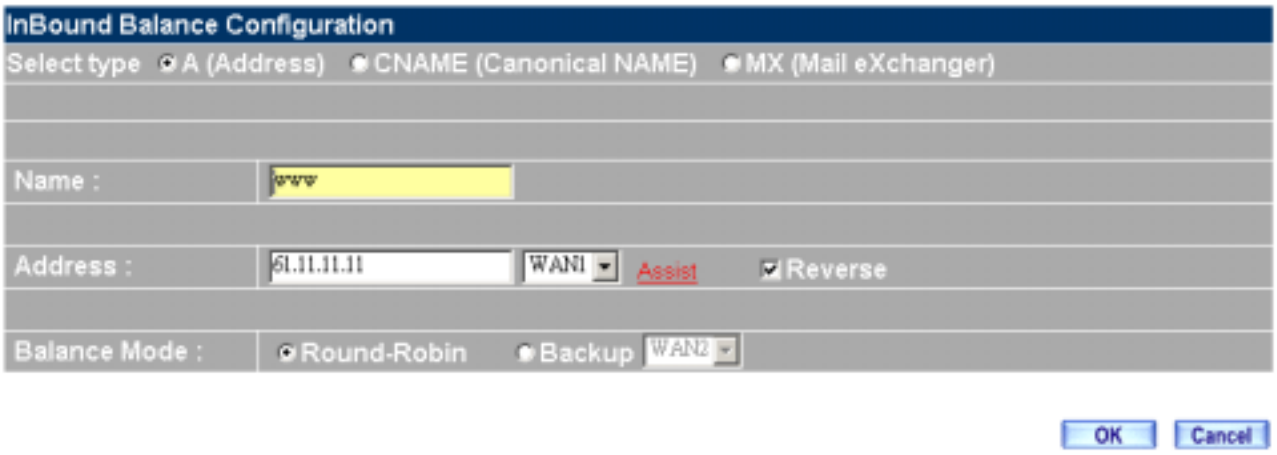


Step 1. Enter the window of Inbound Balance.

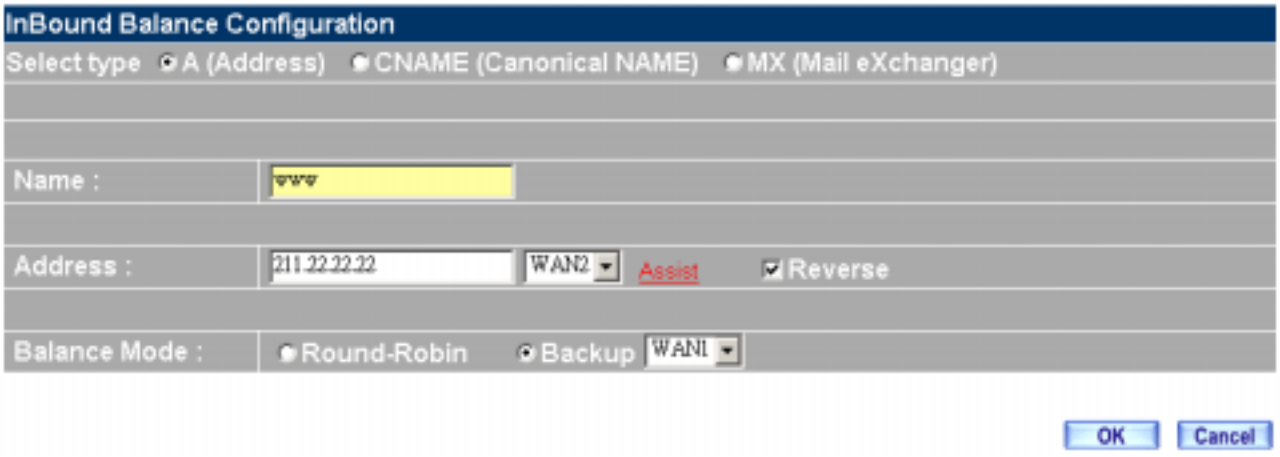
Step 2. Enter the DNS domain name(broadband.com.tw) registered by ISP in the field of【Domain Name】and enable【Enable the Zone】.

Step 3. Enter the window of 【InBound Balance Configuration】and select 【A】for the 【Select Type】.

Step 4. Add the 1st entry, and enter the【www】 in the field of 【Name】. And after selecting 【WAN 1】from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 61.11.11.11. And select【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.



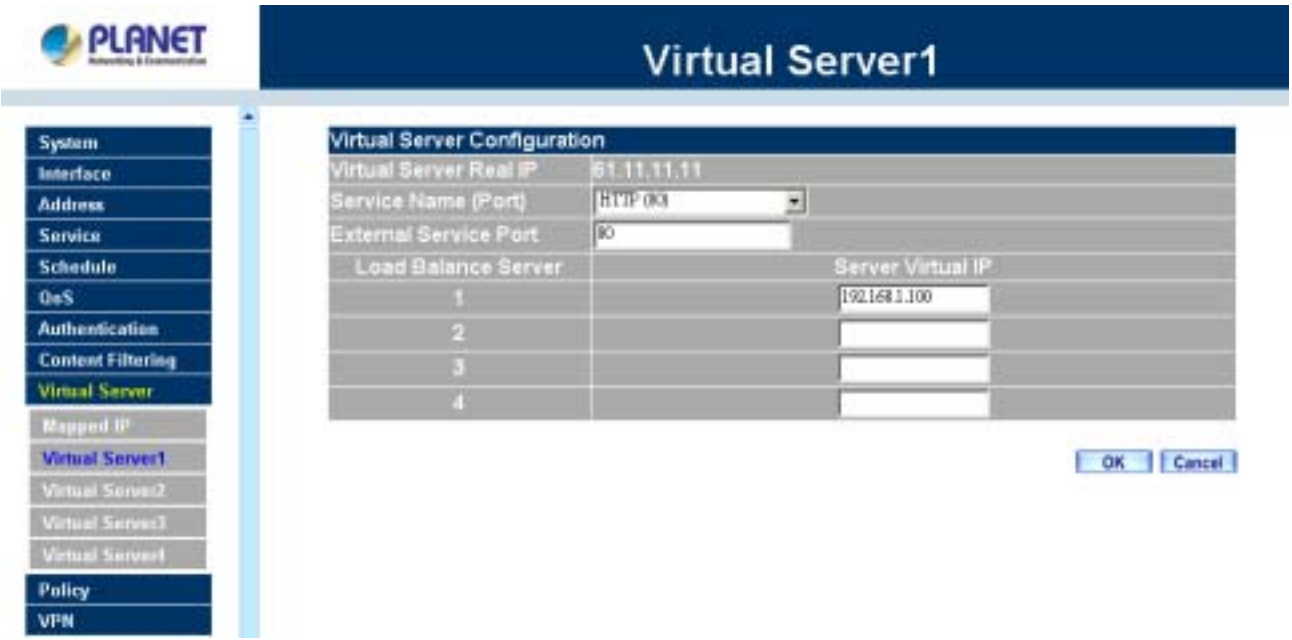
Step 5. Add the 2nd entry, and enter the【www】in the field of 【Name】. And after selecting 【WAN 2】from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 211.22.22.22. And select【Backup】in 【Balance Mode】. After the setup is completed, please click on【OK】.



Step 6. The setup is completed below.

Step 7. Enter the setup window of 【Virtual Server 1】in the menu.

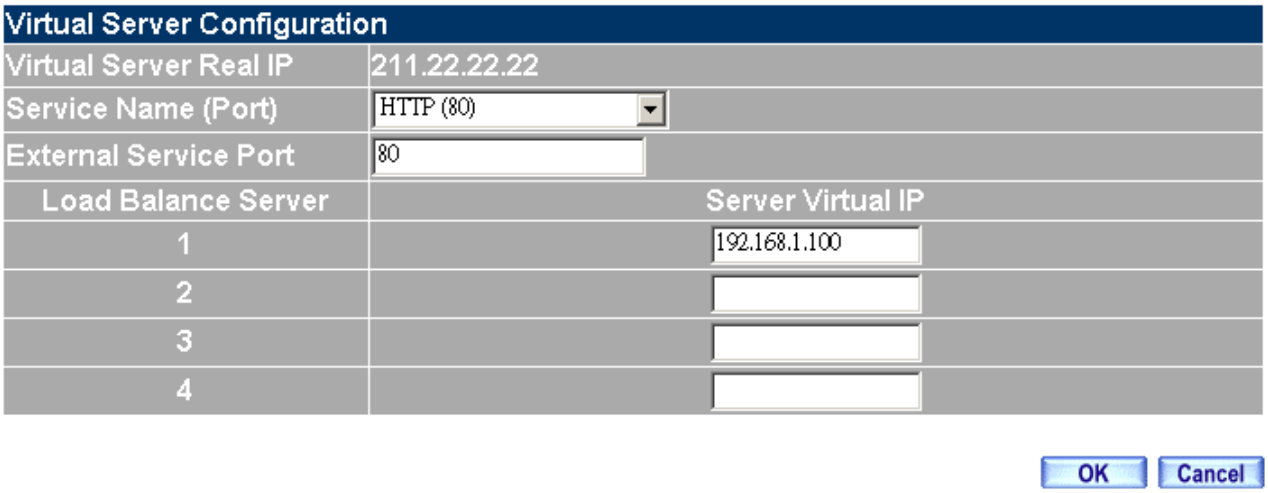
Step 8. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 1, 61.11.11.11】. And click the 【Add】 button. Enter the relating parameters and click on 【OK】.



Step 9. Add new policy of **Incoming** in 【Policy】for Virtual Server 1.

Step 10. Enter the setup window of 【Virtual Server 2】.

Step 11. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 2, 211.22.22.22】. And click the 【Add】 button. Enter the relating parameters and click on 【OK】.



Step 12. Add new policy of **Incoming** in 【Policy】for Virtual Server 2.

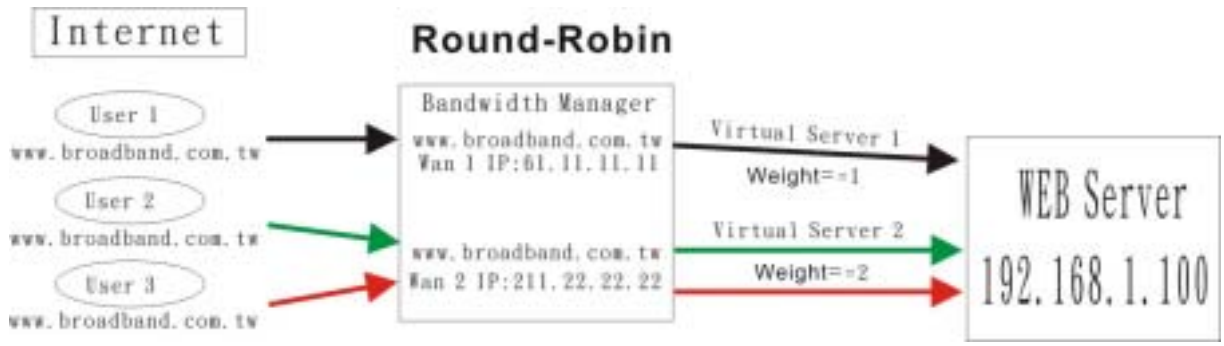
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	HTTP(80)			Modify Remove	To 1
Outside_Any	Virtual Server 2 (211.22.22.22)	HTTP(80)			Modify Remove	To 2

Step 13. The setup is completed.

If WAN 1 is disconnected and WAN 2 can start for backup automatically, so the WEB Server could provide the stable and reliable service for users.

Example 2: Setup【WEB Server】and Type is 【A】 for 【Round-Robin】in Inbound Load Balance.

【Round-Robin】: For providing stable and reliable connection service quality, the Multi-Homing Security Gateway provide this mechanism according to specific weight and priority in setup of Inbound Load Balance. Below is the detail setup description for this function:

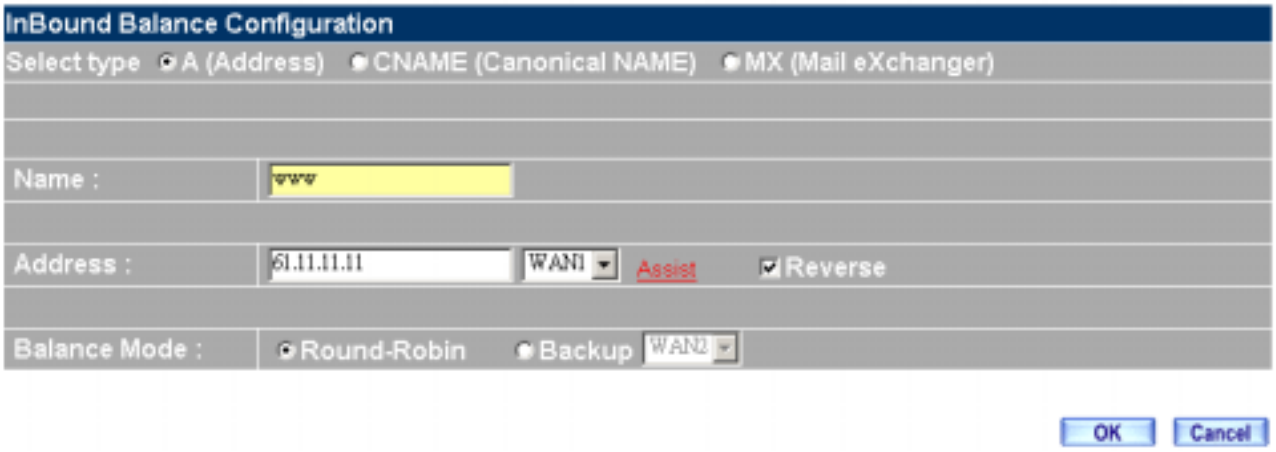


Step 1. Enter the window of Inbound Balance.

Step 2. Enter the DNS domain name(broadband.com.tw) registered by ISP in the field of【Domain Name】and enable【Enable the Zone】.

Step 3. Enter the window of 【Inbound Balance Configuration】and select 【A】for the 【Select Type】.

Step 4. Add the 1st entry, and enter the【www】 in the field of 【Name】. And after selecting 【WAN 1】 from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 61.11.11.11. And select【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.



Step 5. Set 【weight】 to be 1(first priority), and the setup is completed below.

Step 6. Enter the setup window of 【Virtual Server 1】in the menu.

Step 7. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 1, 61.11.11.11】. And click the 【Add】 button. Enter the relating parameters and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 8. Add new policy of **Incoming** in 【Policy】of Virtual Server 1.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	HTTP(80)			Modify Remove	To 1

Step 9. Add the 2nd entry, and enter the【www】in the field of 【Name】. And after selecting 【WAN 2】from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 211.22.22.22. And select【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.

InBound Balance Configuration	
Select type	A (Address) CNAME (Canonical NAME) MX (Mail eXchanger)
Name :	www
Address :	211.22.22.22 WAN2 Assist Reverse
Balance Mode :	Round-Robin Backup WAN1

OK Cancel

Step 10. Set 【weight】to be 2(second priority), and the setup is completed below.

Domain Name : broadband.com.tw OK Enable DNS zone

Name	Type	Address	Backup	Weight	Priority	Configure
www	A	61.11.11.11(WAN1)	--	1	1	Modify Remove
www	A	211.22.22.22(WAN2)	--	2	2	Modify Remove

Step 11. Enter the setup window of 【Virtual Server 2】.

Step 12. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 2, 211.22.22.22】. And click the 【Add】 button. Enter the relating parameters and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 13. Add new policy of **Incoming** in 【Policy】of Virtual Server 2.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	HTTP(80)			Modify Remove	To 1
Outside_Any	Virtual Server 2 (211.22.22.22)	HTTP(80)			Modify Remove	To 2

Step 14. The setup is completed.

Name	Type	Address	Weight	Priority
www.broadband.com.tw	A	61.11.11.11	1	1
www.broadband.com.tw	A	211.22.22.22	2	2

When users want to connect www.planet.com.tw, the sequence of entering the website is below.

The first user enter the server of 61.11.11.11

The second user enter the server of 211.22.22.22

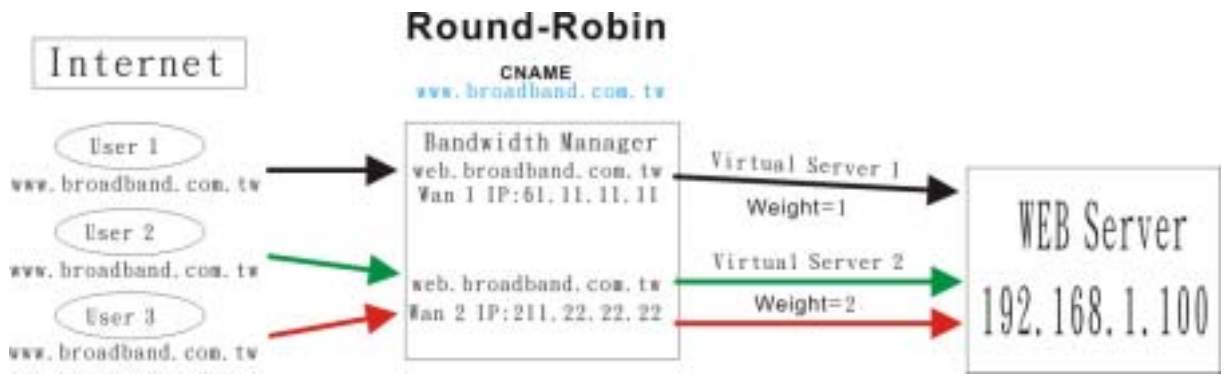
The third user enter the server of 211.22.22.22

The fourth user enter the server of 61.11.11.11

The fifth user enter the server of 211.22.22.22

The sixth user enter the server of 211.22.22.22

Example 3: Setup【WEB Server】and Type is 【CNAME】 for 【Round-Robin】in Inbound Load Balance.



【Round-Robin】: For providing stable and reliable connection service quality, the Multi-Homing Security Gateway provide this mechanism according to specific weight and priority in setup of Inbound Load Balance. Below is the detail setup description for this function:

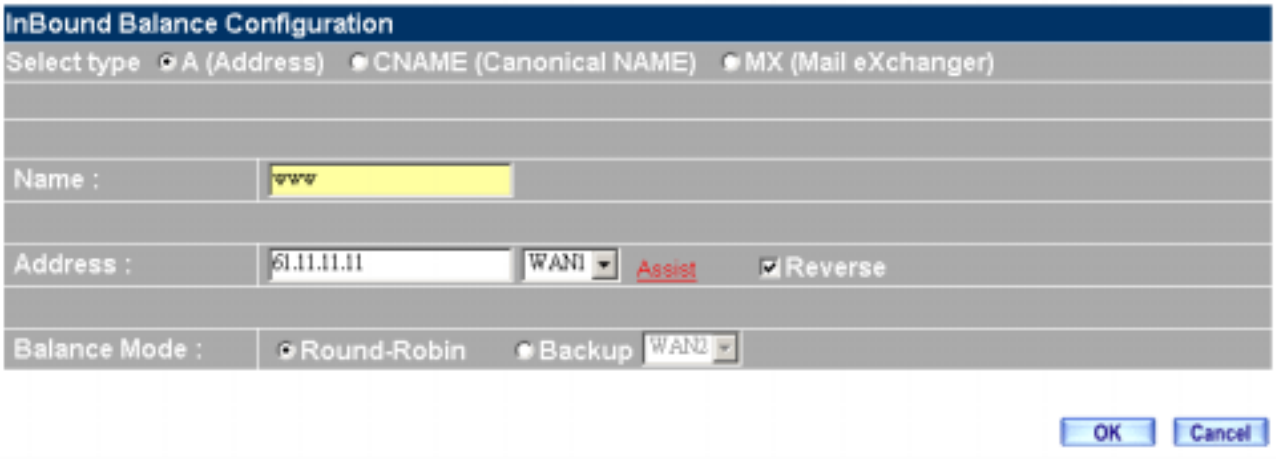
Step 1. Enter the window of Inbound Balance.

Step 2. Enter the DNS domain name(broadband.com.tw) registered by ISP in the field of【Domain Name】and enable【Enable the Zone】

Step 3. Enter the window of 【Inbound Balance Configuration】and select 【A】for the 【Select Type】.

Step 4. Add the 2nd entry, and enter the【www】 in the field of 【Name】.

Step 5. And after selecting 【WAN 1】 from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 61.11.11.11. And select【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.

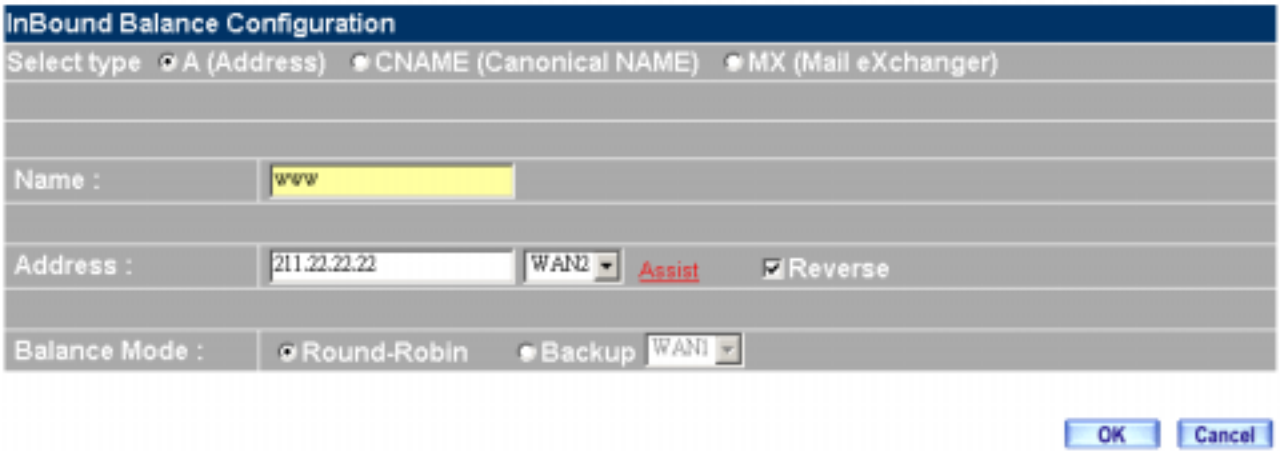


Step 6. Set 【weight】 to be 1(first priority), and the setup is completed below.

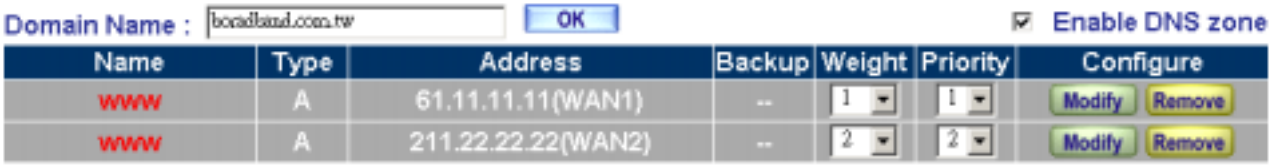
Step 7. Enter the window of 【InBound Balance Configuration】and select 【A】for the 【Select Type】.

Step 8. Add the 1st entry, and enter the【www】 in the field of 【Name】.

Step 9. Select 【WAN 2】 from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 211.22.22.22. And select【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.



Step 10. Set 【weight】 to be 2(second priority), and the setup is completed below.



Step 11. Enter the window of 【Inbound Balance Configuration】and select 【CNAME】for the 【Select Type】.

Step 12. The 【Alias Name】 is web.

The 【Real Name】 is www.broadband.com.tw.

InBound Balance Configuration	
Select type	A (Address) CNAME (Canonical NAME) MX (Mail eXchanger)
Alias Name :	web
Real Name :	www.broadband.com.tw

OK Cancel

Step 13. The setup is completed.

Domain Name : broadband.com.tw OK Enable DNS zone

Name	Type	Address	Backup	Weight	Priority	Configure
www	A	61.11.11.11(WAN1)	--	1	1	Modify Remove
www	A	211.22.22.22(WAN2)	--	2	2	Modify Remove
web	CNAME	www.broadband.com.tw	--	--	--	Modify Remove

Step 14. Enter the setup window of 【Virtual Server 1】in the menu.

Step 15. Enter the window of【Add Virtual Server IP】and enter the virtual server IP【WAN 1, 61.11.11.11】. And click the 【Add】 button. Enter the relating parameters and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 16. Add new policy of **Incoming** in 【Policy】of Virtual Server 1.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	HTTP(80)			Modify Remove	To 1

Step 17. Enter the setup window of 【Virtual Server 2】.

Step 18. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 2, 211.22.22.22】. And click the 【Add】 button. Enter the relating parameters according to the service

provided by this server (ex., HTTP 80) and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 19. Add new policy of WAN to LAN in 【Policy】of Virtual Server 2.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	HTTP(80)			Modify Remove	To 1
Outside_Any	Virtual Server 2 (211.22.22.22)	HTTP(80)			Modify Remove	To 2

The setup is completed.

Name	Type	Address	Weight	Priority
www.broadband.com.tw	A	61.11.11.11	1	1
www.broadband.com.tw	A	211.22.22.22	2	1
web.broadband.com.tw	CNAME	www.broadband.com.tw	--	--

When users encounter web.broadband.com.tw (Alias Server), the connection service maps into www.broadband.com.tw (Real Server) and the sequence of entering the website is below.

The first user enter the server of 61.11.11.11

The second user enter the server of 211.22.22.22

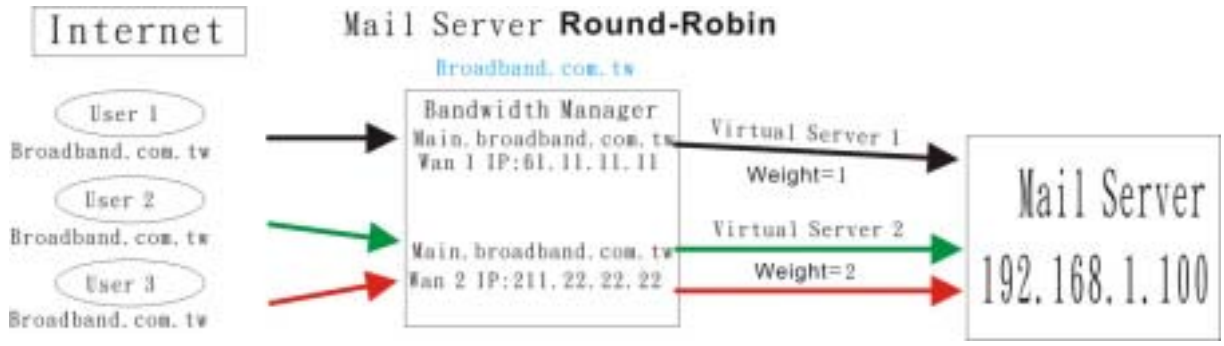
The third user enter the server of 211.22.22.22

The fourth user enter the server of 61.11.11.11

The fifth user enter the server of 211.22.22.22

The sixth user enter the server of 211.22.22.22

Example 4: Setup 【MAIL Server】 for 【Round-Robin】in Inbound Load Balance.



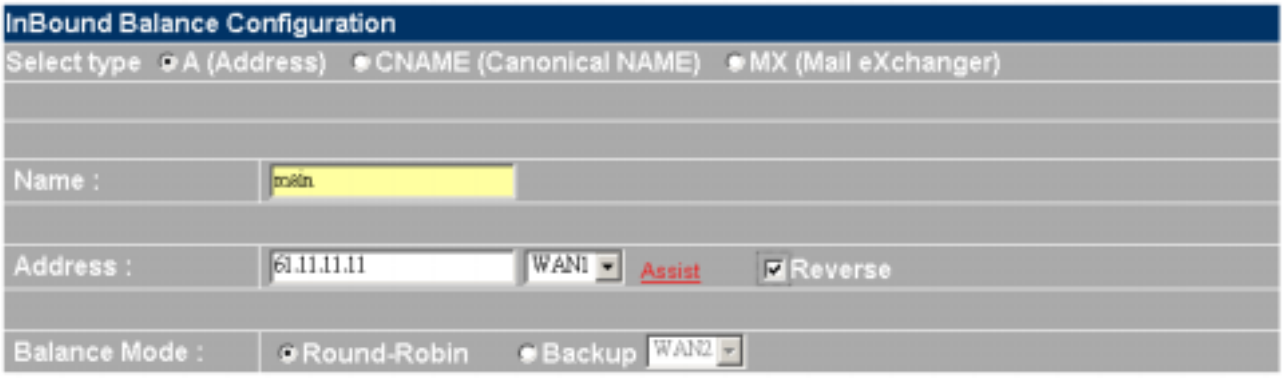
For setup Mail Server, below is the detail setup description for this function:

Step 1. Enter the window of Inbound Balance.

Step 2. Enter the DNS domain name(broadband.com.tw) registered by ISP in the field of【Domain Name】and enable【Enable the Zone】.

Step 3. Enter the window of 【Inbound Balance Configuration】and select 【A】for the 【Select Type】.

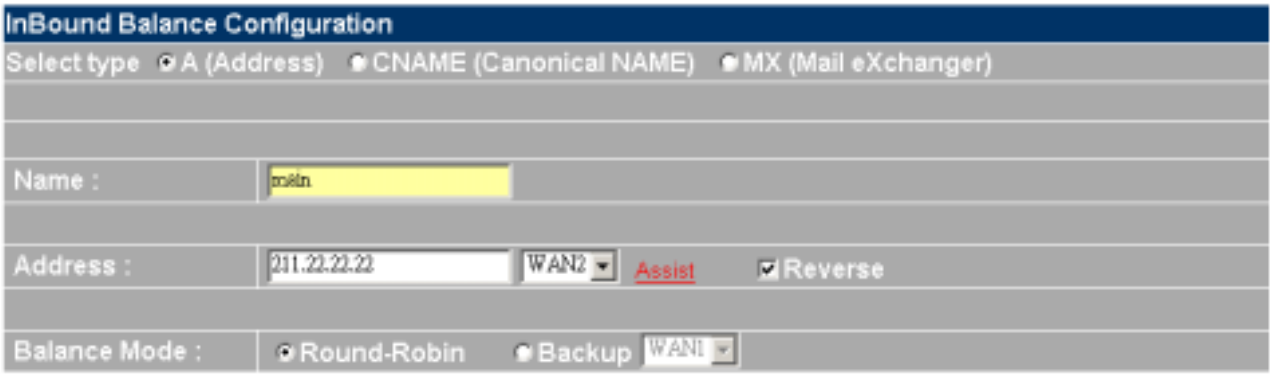
Step 4. Add the 1st entry, and enter the【main】 in the field of 【Name】. Selecting 【WAN 1】 from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 61.11.11.11. And select 【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.



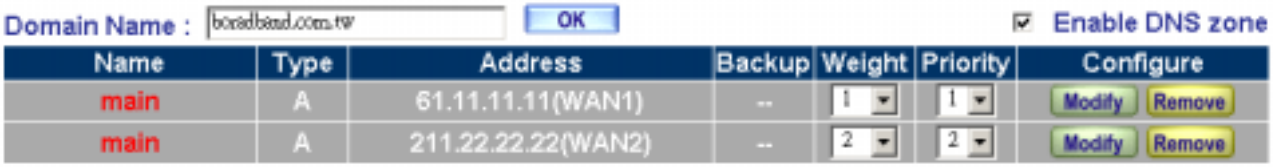
Step 5. Set 【weight】to be 1(first priority), and the setup is completed below.

Step 6. Enter the window of 【Inbound Balance Configuration】and select 【A】for the 【Select Type】.

Step 7. Add the 2nd entry, and enter the【main】 in the field of 【Name】. Select 【WAN 2】 from the drop down list in the right side of 【Address】, click on the 【Assist】 to select 211.22.22.22. And select 【Round-Robin】in 【Balance Mode】. After the setup is completed, please click on 【OK】.

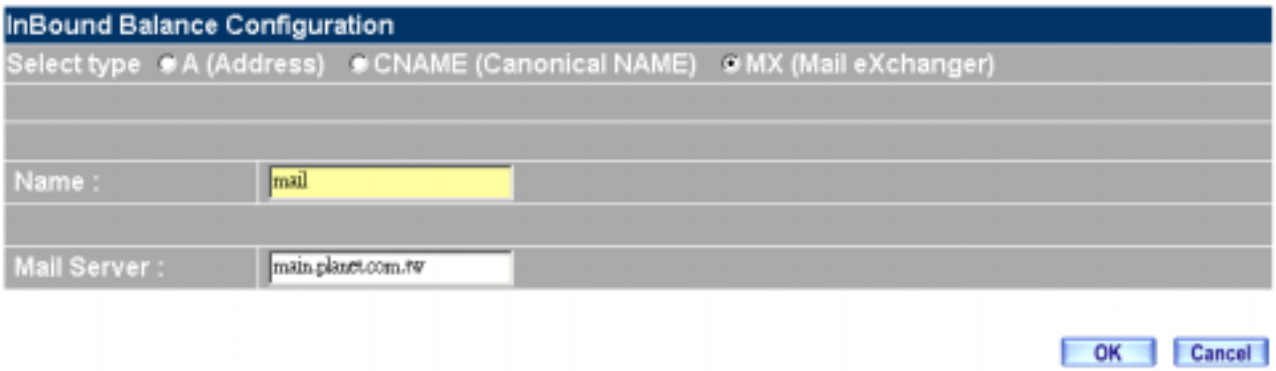


Step 8. Set 【weight】 to be 2(second priority), and the setup is completed below.



Step 9. Enter the window of 【Inbound Balance Configuration】and select 【MX】for the【Select Type】. The【Name】is mail

the【Real Name】is main.broadband.com.tw.



Step 10. The setup is completed.

Domain Name : broadband.com.tw OK ☑ Enable DNS zone

Name	Type	Address	Backup	Weight	Priority	Configure
main	A	61.11.11.11(WAN1)	--	1	1	Modify Remove
main	A	211.22.22.22(WAN2)	--	2	2	Modify Remove
mail	MX	main.planet.com.tw	--	--	1	Modify Remove

Step 11. Enter the setup window of 【Virtual Server 1】in the menu.

Step 12. Enter the window of【Add Virtual Server IP】and enter the virtual server IP【WAN 1, 61.11.11.11】. And click the 【Add】 button. Enter the relating parameters according the service provided by this server (ex. POP3 110) and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service Name (Port)	POP3 (110)
External Service Port	110
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 13. Enter the window of【Add Virtual Server IP】and enter the virtual server IP【WAN 1, 61.11.11.11】. And click the 【Add】 button. Enter the relating parameters according the service provided by this server (ex., SMTP 25) and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service Name (Port)	SMTP (25)
External Service Port	25
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 14. Add new policy of **Incoming** in 【Policy】for Virtual Server 1.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	POP3(110)			Modify Remove	To 1
Outside_Any	Virtual Server 1 (61.11.11.11)	SMTP(25)			Modify Remove	To 2

New Entry

Step 15. Enter the setup window of 【Virtual Server 2】.

Step 16. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 2, 211.22.22.22】. And click the 【Add】 button. Enter the relating parameters according to the service provided by this server (ex. POP3 110) and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service Name (Port)	POP3 (110)
External Service Port	110
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 17. Enter the window of 【Add Virtual Server IP】 and enter the virtual server IP【WAN 2, 211.22.22.22】. And click the 【Add】 button. Enter the relating parameters according to the service provided by this server (ex. SMTP 25) and click on 【OK】.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service Name (Port)	SMTP (25)
External Service Port	25
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Step 18. Add new policy of Incoming in 【Policy】for Virtual Server 2.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.11)	POP3(110)			Modify Remove	To 1
Outside_Any	Virtual Server 1 (61.11.11.11)	SMTP(25)			Modify Remove	To 2
Outside_Any	Virtual Server 2 (211.22.22.22)	POP3(110)			Modify Remove	To 3
Outside_Any	Virtual Server 2 (211.22.22.22)	SMTP(25)			Modify Remove	To 4

Step 19. The setup is completed.

Name	Type	Address	Weight	Priority
main.broadband.com.tw	A	61.11.11.11	1	1
main.broadband.com.tw	A	211.22.22.22	2	2
mail.broadband.com.tw.	MX	main.broadband.com.tw	--	--

When users encounter mail.broadband.com.tw (Alias Server), the connection service maps into main.broadband.com.tw (Real Server) and the sequence of entering the website is below.

The first user enter the server of 61.11.11.11

The second user enter the server of 211.22.22.22

The third user enter the server of 211.22.22.22

The fourth user enter the server of 61.11.11.11

The fifth user enter the server of 211.22.22.22

The sixth user enter the server of 211.22.22.22

4.13 Log

The Multi-Homing Security Gateway supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the Multi-Homing Security Gateway.

What is Log?

Log records all connections that pass through the Multi-Homing Security Gateway's control policies. Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.

How to use the Log

The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

4.13.1 Traffic Log

The Administrator queries the Multi-Homing Security Gateway for information, such as source address, destination address, start time, and Protocol port of all connections.

Entering the Traffic Log window

Step 1. Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

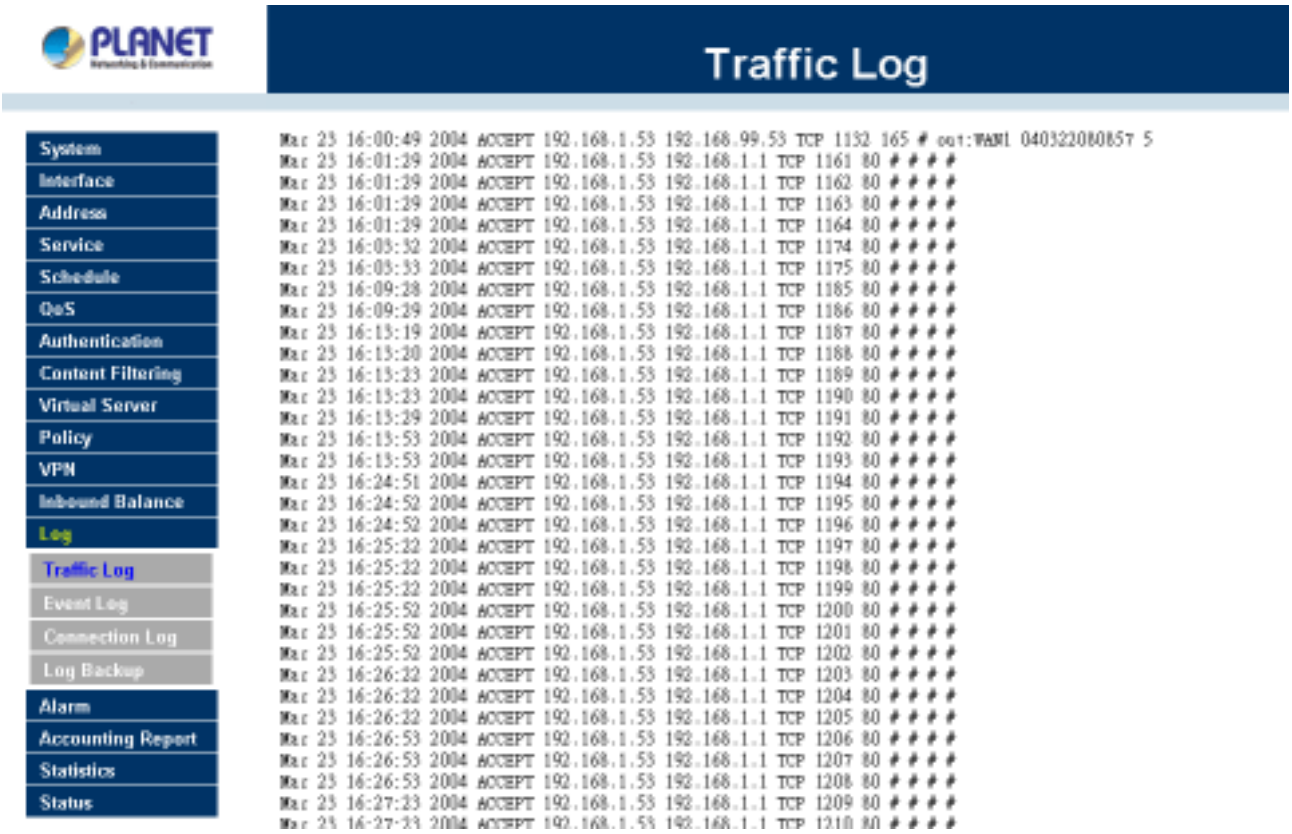
- **Time**: The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol:** Protocol type of the specific connection.
- **Port:** Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

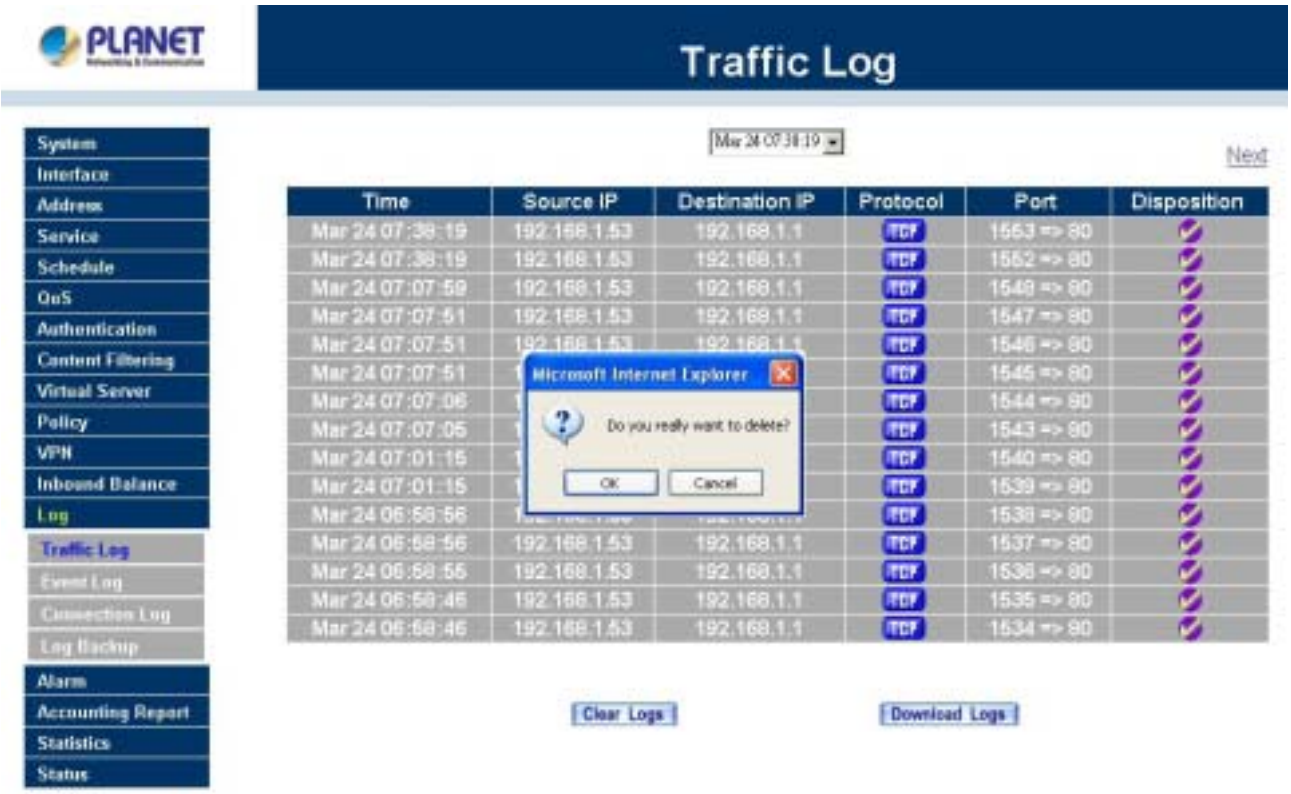


Clearing the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.



4.13.2 Event Log

When the Multi-Homing Security Gateway WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.

Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

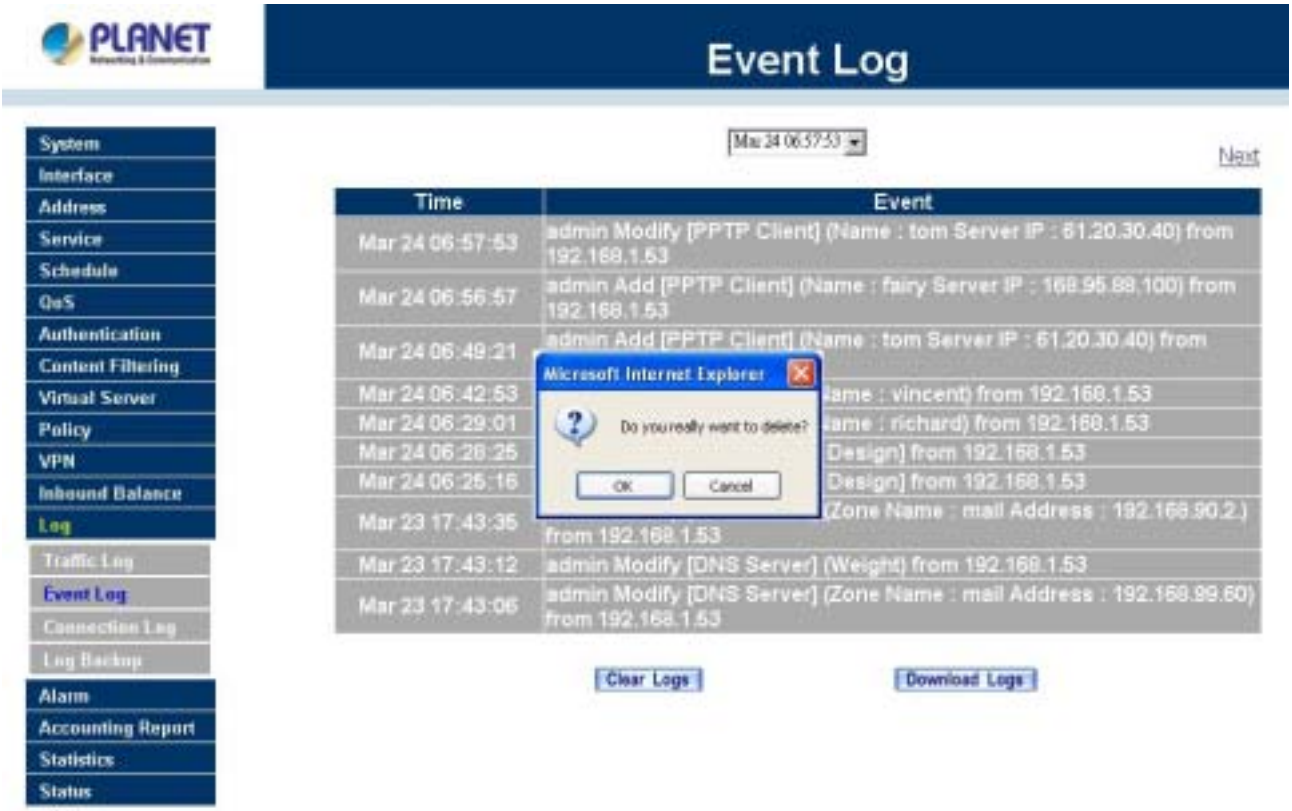
Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

Clearing the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

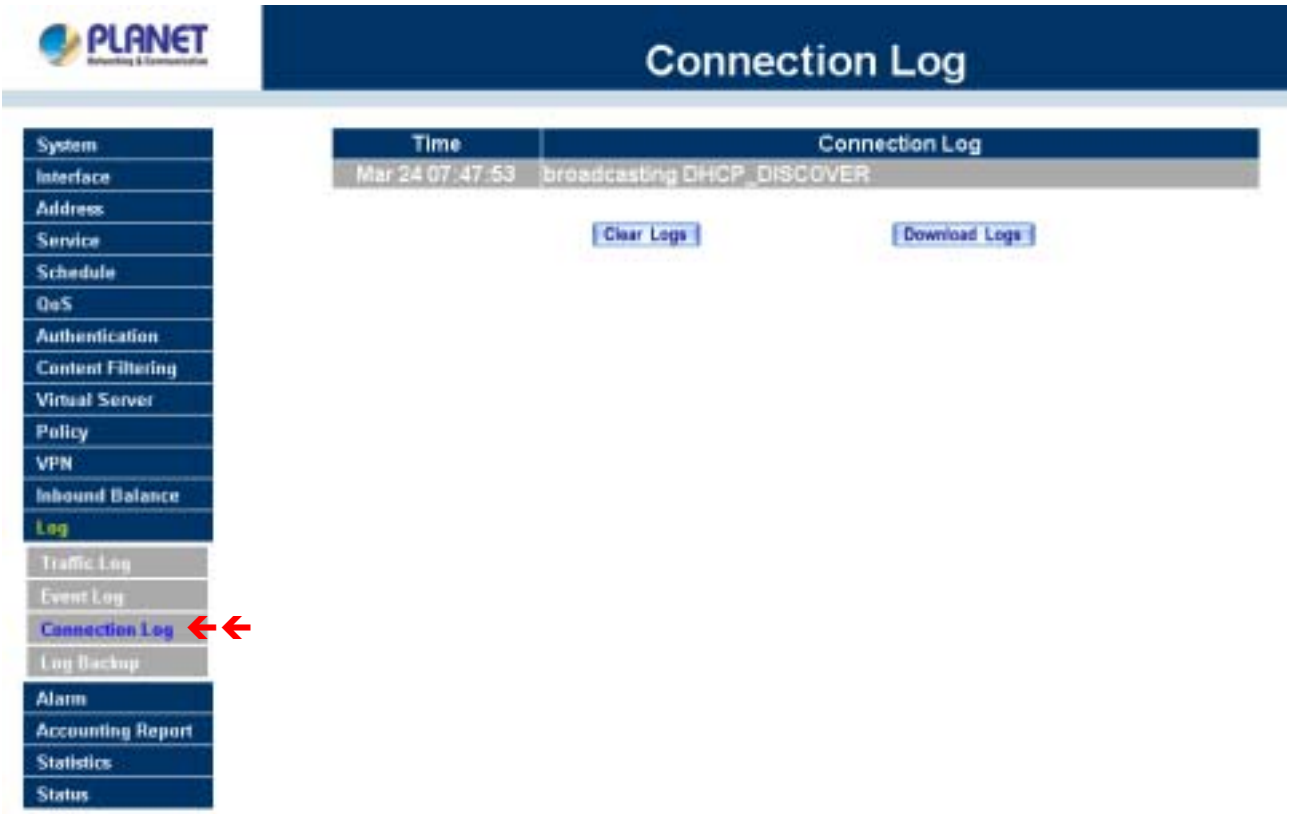
Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.



4.13.3 Connection Log

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.



Definition:

Time: The start and end time of connection.

Connection Log: Event description during connection.

Download Logs

Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.

Step 2. In Connection Log window, click the **Download Logs** button.

Step 3. In the Download Logs window, save the logs to the specified location.

Clear Logs

Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.

Step 2. In Connection Log window, click the **Clear Logs** button.

Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.

4.13.4 Log Backup

Click **Log →Log Backup**.

Log Mail Configuration: When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

NOTE: Before enabling this function, you have to configure E-mail Settings in System -> Settings.

Syslog Settings: If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

NOTE: To restart Connection Log, click the **Refresh** button on the right hand side in Log window.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.

Step 2. Go to **LOG →Log Backup.** Check to enable **Log Mail Support.** Click **OK.**

System Settings/Enable Syslog Message

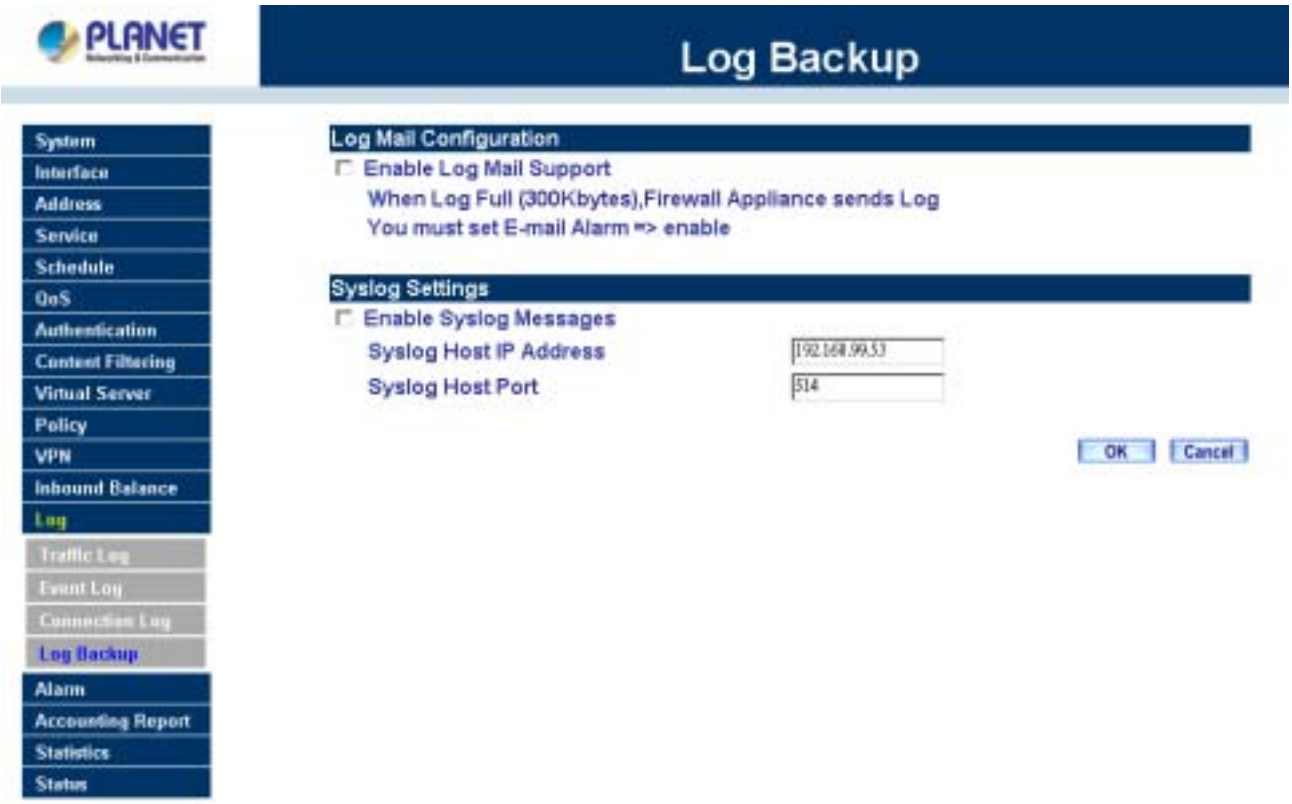
Step 1. Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.

Step 2. Click **OK**.

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG →Log Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG →Log Backup**. Uncheck to disable Settings Message. Click **OK**.



4.14 Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the Multi-Homing Security Gateway has logged.
Multi-Homing Security Gateway has two alarms: **Traffic Alarm** and **Event Alarm**.

Traffic alarm:

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Event alarm:

When Multi-Homing Security Gateway detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

4.14.1 Traffic Alarm

How to apply Traffic Alarm

The administrator can use Traffic Alarm to track the Source Address, Destination Address, network service and the status of network. The administrator can save Traffic Logs and Event Logs for a pre-determined time and then delete them to keep the newest log.
In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Entering the Traffic Alarm window

Step 1. Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.

Step 2. The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- **Time:** The start and stop time of the specific connection.
- **Source:** Name of the source network of the specific connection.
- **Destination:** Name of the destination network of the specific connection.
- **Service:** Service of the specific connection.
- **Traffic:** Traffic (in Kbytes/Sec) of the specific connection.

Downloading the Traffic Alarm Logs

The Administrator can back up traffic alarm logs regularly and download it to a file on the computer.

Step 1. In the Traffic Alarm window, click the **Download Logs** button on the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.

Clearing the Traffic Alarm Logs

Step 1. In the Traffic Alarm window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel.

4.14.2 Event Alarm

When Multi-Homing Security Gateway detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

Entering the Event Alarm window

Step 1. Click the **Event Alarm** option below the **Alarm** menu to enter the Event Alarm window.

The table in Event Alarm window displays current traffic alarm logs for connections.

- **Time:** log time.
- **Event:** event descriptions.

Downloading the Event Alarm Logs

The Administrator can back up event alarm logs regularly by downloading it to a file on the computer.

Step 1. In the Event Alarm window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the event alarm logs into specific directory on the hard drive.

Clearing Event Alarm Logs

The Administrator may clear on-line logs to keep the most updated logs on the screen.

Step 1. In the Event Alarm window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK**.

4.15 Accounting Report (MH-4000 only)

Accounting Report can be divided into two parts, one is Outbound Accounting Report, and the other is Inbound Accounting Report.

NOTE: This function is not supported on MH-2000.

Outbound Accounting Report is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication services.

Source IP: the IP address used by LAN users who use Multi-Homing Security Gateway

Destination IP: The IP address used by WAN service server which uses Multi-Homing Security Gateway.

Service: The communication service which listed in the pull-down menu when LAN users use Multi-Homing Security Gateway to connect to WAN service server.

Inbound Accounting Report is the statistics of downstream/upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN user uses Multi-Homing Security Gateway to connect to LAN Service Server.

Source IP: the IP address used by WAN users who use Multi-Homing Security Gateway

Destination IP: the IP address used by LAN service server who use Multi-Homing Security Gateway

Service: The communication service which listed in the pull-down menu when WAN users use Multi-Homing Security Gateway to connect to LAN Service server..

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service of all the user's IP that passes the Multi-Homing Security Gateway.

4.15.1 Outbound Accounting Report

Click the **Accounting Report** function, and then select **Outbound**. There are three options for outbound acounting report: Top Users (source IP), Top Sites(Destination IP) and Top Services(Service).

Outbound source IP Accounting Report

Click **Top Users** icon on the page to show the source IP accounting report. If this option is already selected, it does not change when you click it.

When LAN users use Multi-Homing Security Gateway to connect to WAN service server, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

TOP Users: Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

Source IP: The IP address used by LAN users who use Multi-Homing Security Gateway to connect to WAN service server.

Downstream: The percentage of downstream and the value of each WAN service server which uses Multi-Homing Security Gateway to LAN user.

Upstream: The percentage of upstream and the value of each LAN user who uses Multi-Homing Security Gateway to WAN service server

First Packet: When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the Multi-Homing Security Gateway.

Last Packet: When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the Multi-Homing Security Gateway.

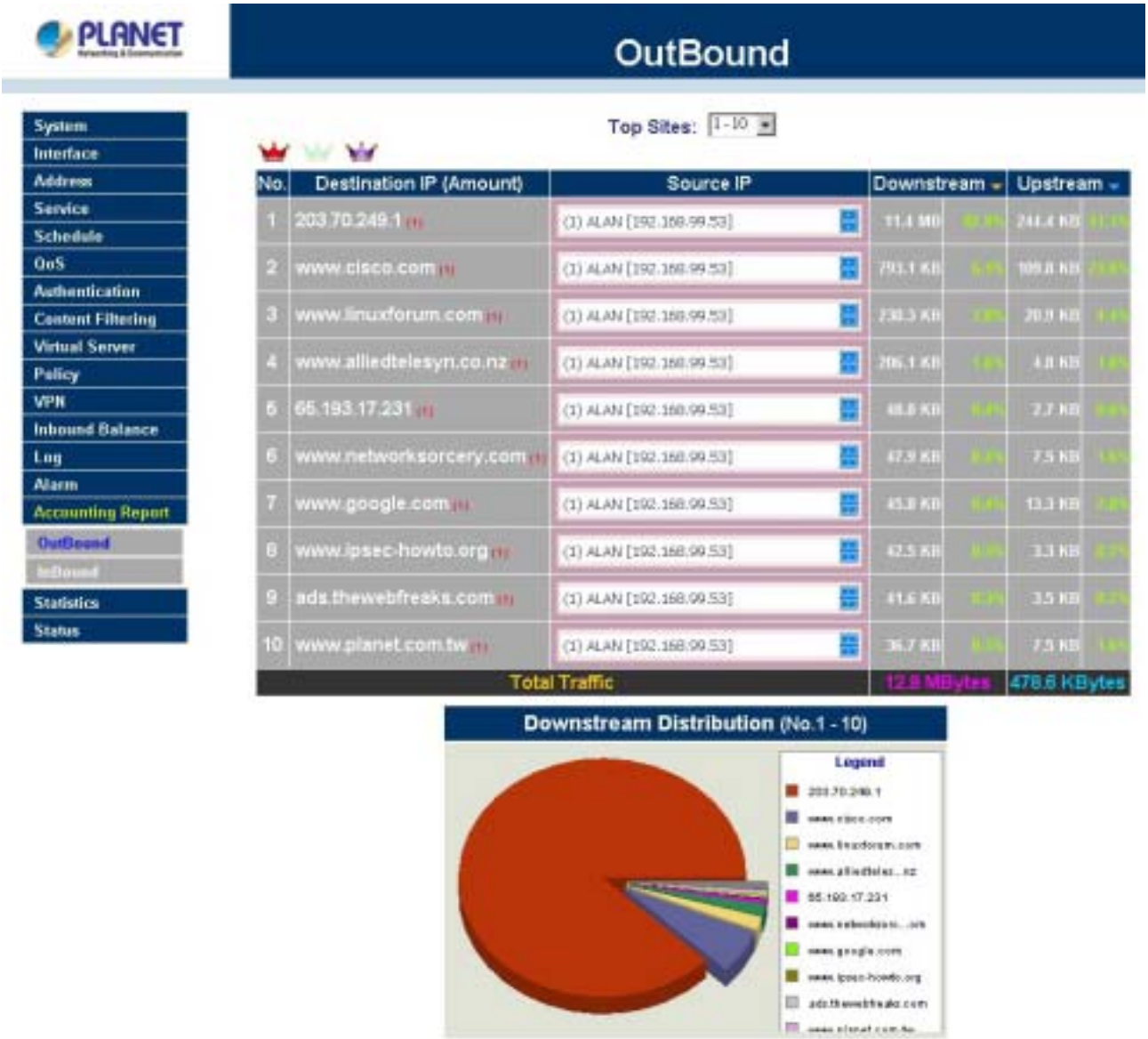
Duration: The period of time which starts from the first packet to the last packet to be recorded.

Total Traffic: The Multi-Homing Security Gateway will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.

Reset Counter: Click **Reset Counter** button to refresh Accounting Report.

Outbound Destination IP Accounting Report

Click **Top Sites** icon on the page to show the Destination IP accounting report. If this option is already selected, it does not change when you click it.



When LAN user connect to WAN service server through Multi-Homing Security Gateway, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Destination IP will be recorded.

Definition:

Top Sites: Select the data you want to view, it presents 10 results in one page.

Destination IP: The IP address used by WAN service server which uses Multi-Homing Security Gateway.

Downstream: The percentage of downstream and the value of each WAN service server which uses Multi-Homing Security Gateway to LAN user.

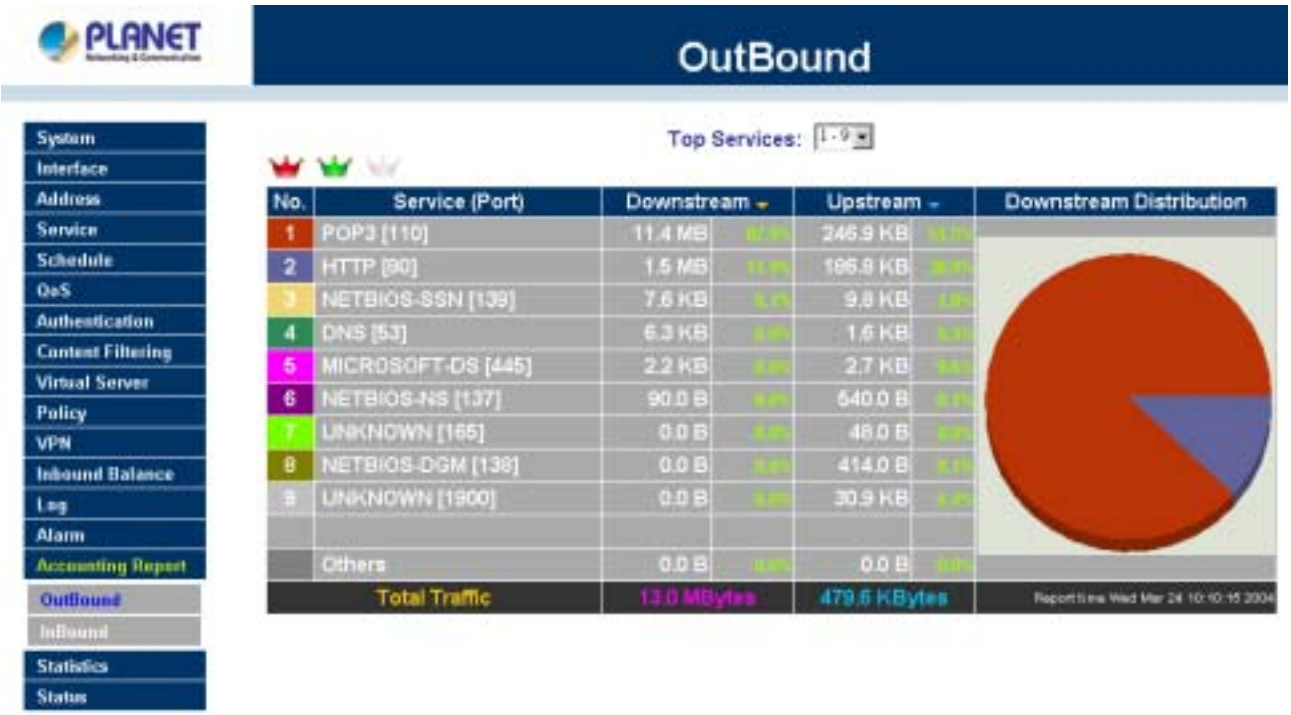
Upstream: The percentage of upstream and the value of each LAN user who uses Multi-Homing Security Gateway to WAN service server.

Total Traffic: The Multi-Homing Security Gateway will record the sum of time and show the percentage of each WAN service server's upstream / downstream to LAN user.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

Outbound Service Accounting Report

Click **Top Services** icon on the page to show the outbound service accounting report. If this option is already selected, it does not change when you click it.



When LAN users use Multi-Homing Security Gateway to connect to WAN Service Server, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Communication Service will be recorded.

Definitions:

Top Services: Select the data you want to view. It presents 10 results in one page.

Service: The report of Communication Service when LAN users use the Multi-Homing Security Gateway to connect to WAN service server.

Downstream: The percentage of downstream and the value of each WAN service server who uses Multi-Homing Security Gateway to connect to LAN user.

Upstream: The percentage of upstream and the value of each LAN user who uses Multi-Homing Security Gateway to WAN service server.

Duration: The period of time starts from the first packet to the last packet to be recorded.

Total Traffic: The Multi-Homing Security Gateway will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.15.2 Inbound Accounting Report

Click the **Accounting Report** function, and then select **Inbound**. There are three options for outbound acounting report: Top Users (source IP), Top Sites(Destination IP) and Top Services(Service).

Inbound Source IP Accounting Report

Click **Top Users** icon on the page to show the inbound source IP accounting report. If this option is already selected, it does not change when you click it.

When WAN users use Multi-Homing Security Gateway to connect to LAN service server, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

TOP Users: Select the data you want to view. It presents 10 pages in one page.

Select from the Pull-down menu

Source IP: The IP address used by WAN users who use Multi-Homing Security Gateway.

Downstream: The percentage of Downstream and the value of each WAN user who uses Multi-Homing Security Gateway to LAN service server.

Upstream: The percentage of Upstream and the value of each LAN service server who uses Multi-Homing Security Gateway to WAN users.

Total Traffic: The Multi-Homing Security Gateway will record the sum of time and show the percentage of each WAN user's upstream/downstream to LAN service server.

Inbound Destination IP Accounting Report

Click **Top Sites** icon on the page to show the inbound Destination IP accounting report. If this option is already selected, it does not change when you click it.

When WAN users use Multi-Homing Security Gateway to connect to LAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Top Site: Select the data you want to view. It presents 10 pages in one page.

Destination IP: The IP address used by WAN users who uses Multi-Homing Security Gateway.

Downstream: The percentage of Downstream and the value of each WAN user who uses Multi-Homing Security Gateway to LAN service server.

Upstream: The percentage of Upstream and the value of each LAN service server who uses Multi-Homing Security Gateway to WAN users.

Total Traffic: The Multi-Homing Security Gateway will record the sum of time and show the percentage of each WAN user's upstream/downstream to LAN service server.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

Inbound Service Accounting Report

Click **Top Services** icon on the page to show the inbound service accounting report. If this option is already selected, it does not change when you click it.

When WAN users use Multi-Homing Security Gateway to connect to LAN Service Server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Top Services: Select the data you want to view. It presents 10 results in one page.

Service: The report of Communication Service when WAN users use the Multi-Homing Security Gateway to connect to LAN service server.

Downstream: The percentage of downstream and the value of each WAN user who uses Multi-Homing Security Gateway to LAN service server.

Upstream: The percentage of upstream and the value of each LAN service server who uses Multi-Homing Security Gateway to WAN user.

Total Traffic: The Multi-Homing Security Gateway will record the sum of time and show the percentage of each Communication Service's upstream / downstream to LAN service server..

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.16 Statistics

In this chapter, the Administrator queries the Multi-Homing Security Gateway for statistics of packets and data which passes across the Multi-Homing Security Gateway. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the Multi-Homing Security Gateway by control policies setup by the Administrator.

How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to mange networks.

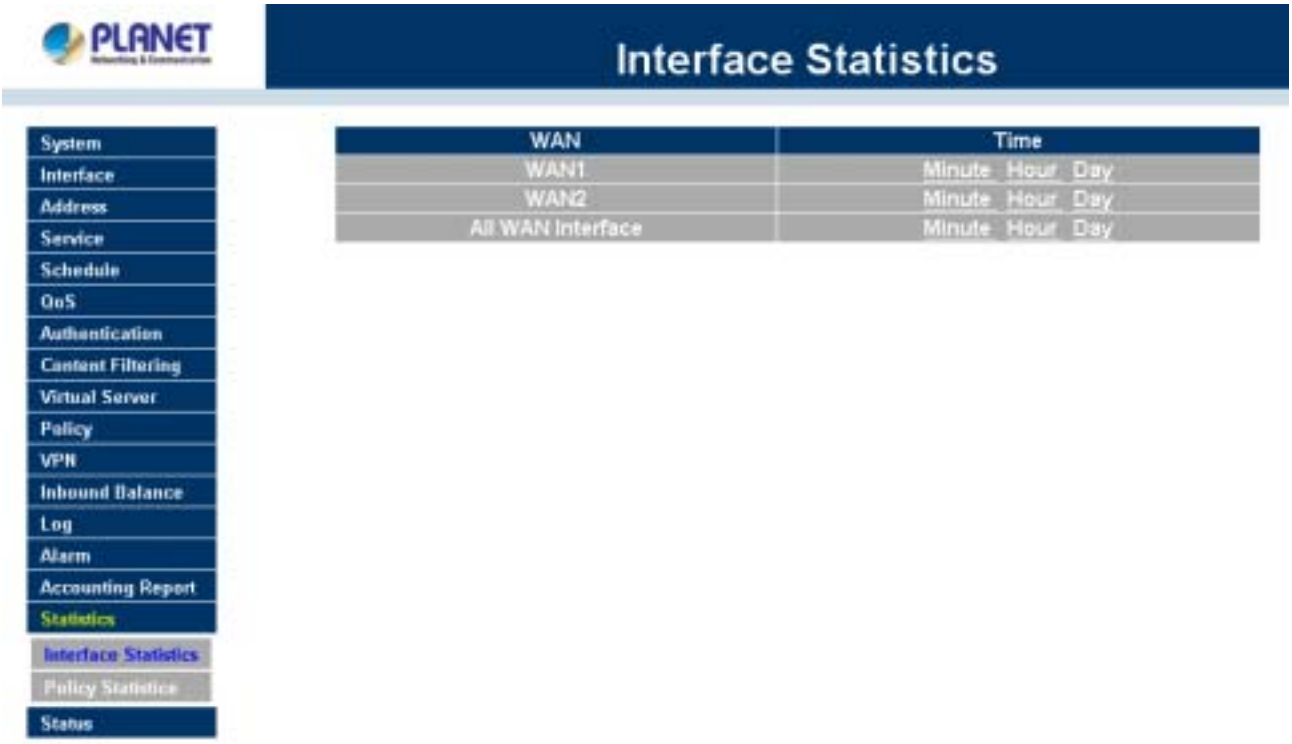
How to apply WAN Statistics

The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics. In this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

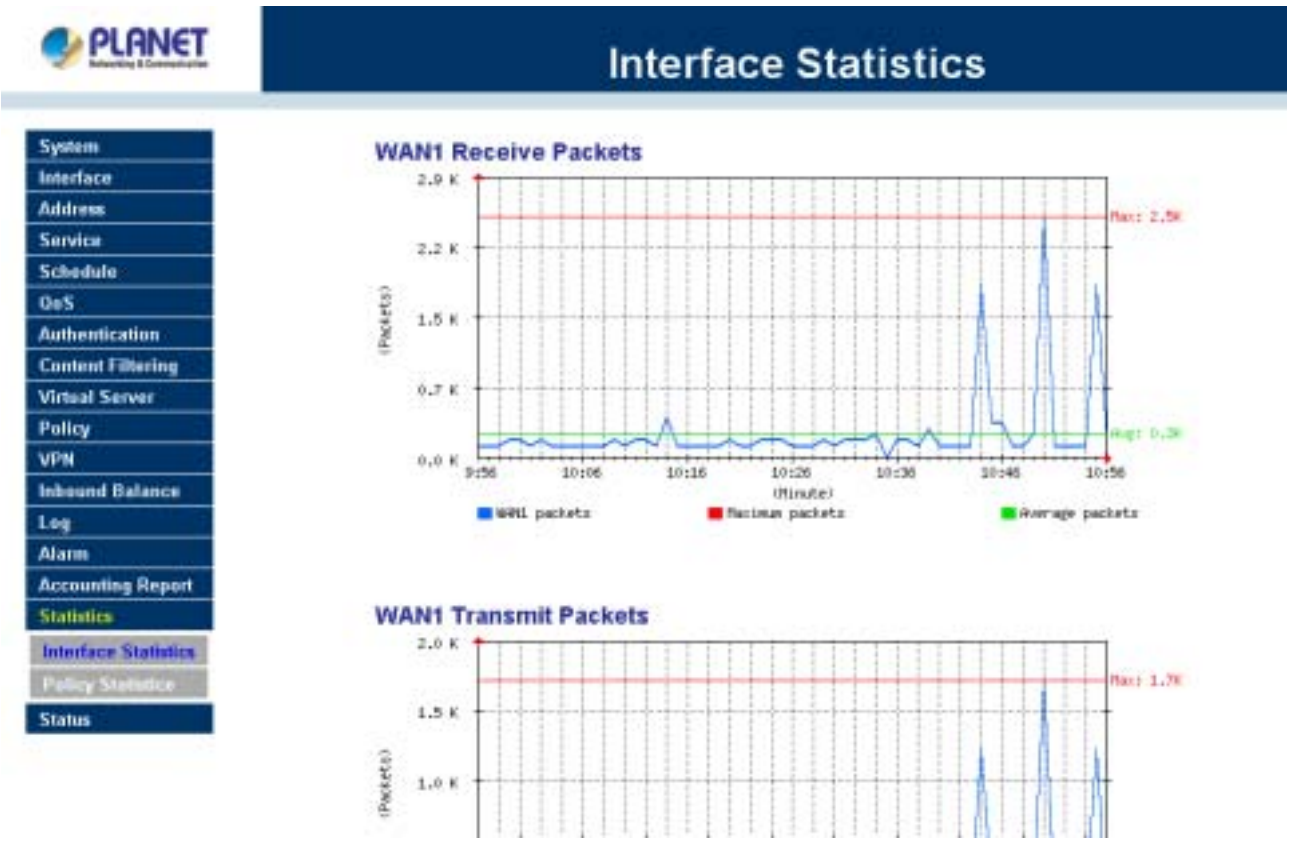
The administrator needs to go to the Policy to set the network IP of the statistics. By the WAN statistics you can obtain the status of the network.

4.16.1 Interface Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select Interface Statistics.



Step 2. The Interface Statistics will be displayed. It displays statistics of WAN 1/2 network connections (downstream and upstream as well) in a total amount by minute (60 minutes), hour (24 hours) and day (30 days). Select the WAN port you want to show and select the time units (minute, hour or day) of the graph.



Y-Coordinate: Four options are available: Total, Bits/sec, Bytes/sec and Utilization.

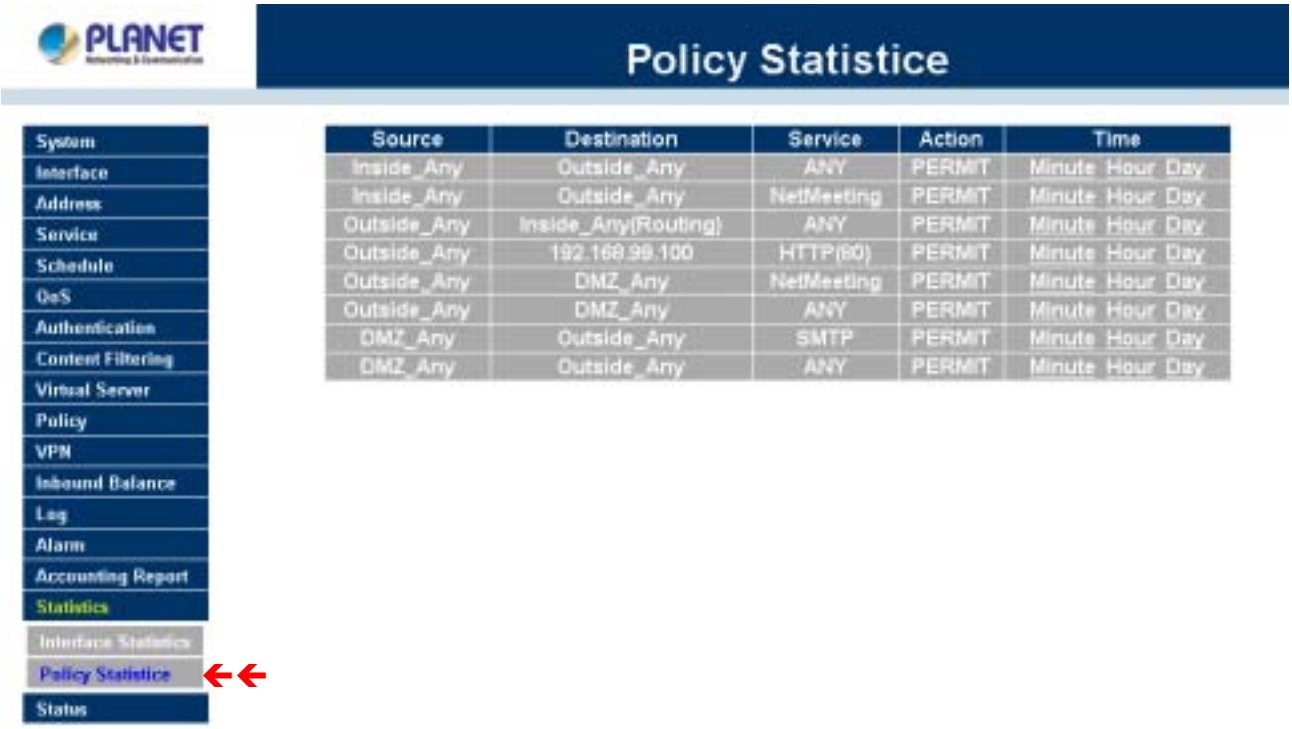
X-Coordinate: Time（Hour/Minute/Day）.

4.16.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, or days



NOTE: To use Statistics, the administrator needs to go to Policy to enable Statistics function.

Entering the Policy Statistics

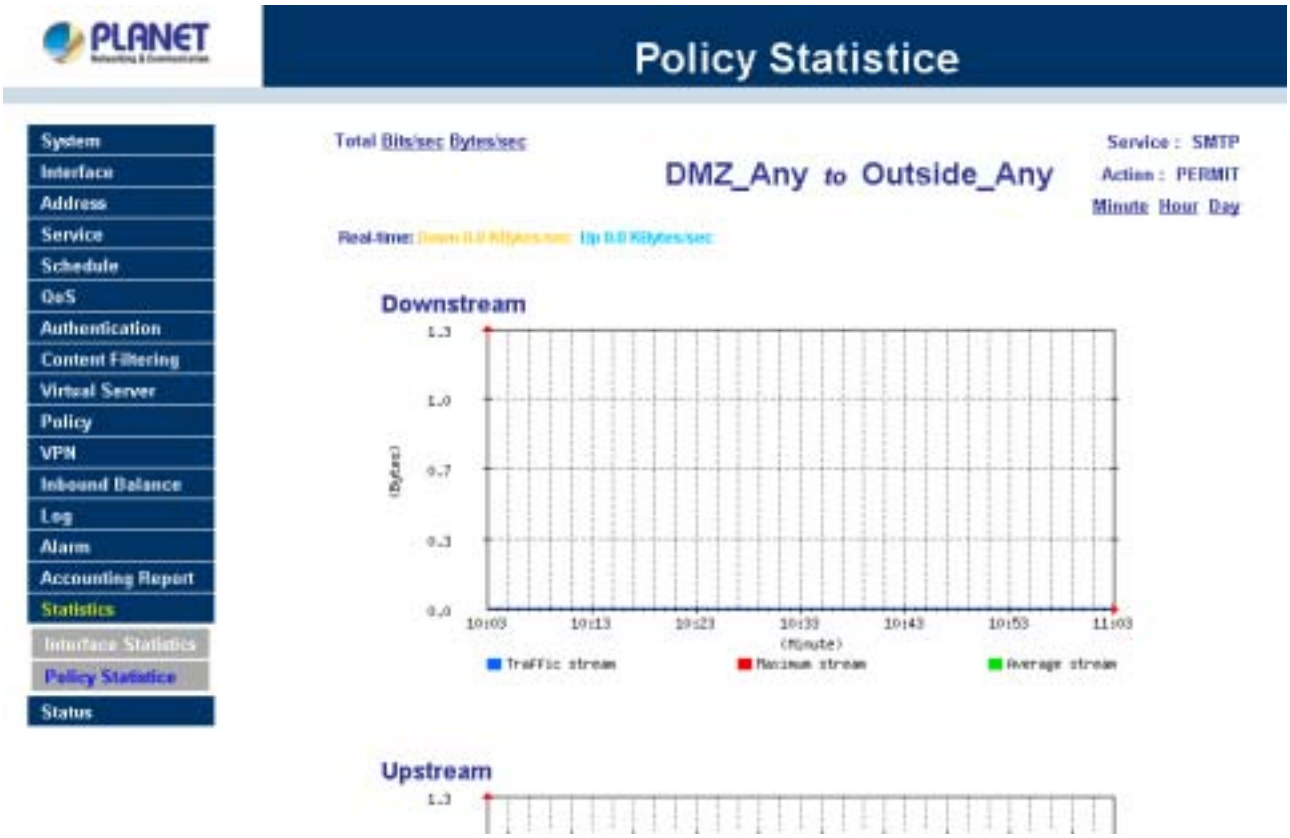
Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **Policy Statistics**.

Step 2. In Statistics window, find the policy you want to view

Step 3. In the Statistics window, click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate: There are three options: Total, Kbit/sec, Kbytes/sec.

X-Coordinate: Time (Hour/Minute/Day).


PLANET
Policy Statistice
System
Interface
Address
Service
Schedule
QoS
Authentication
Content Filtering
Virtual Server
Policy
VPN
Inbound Balance
Log
Alarm
Accounting Report
Statistics
Interface Statistics
Policy Statistice
Status
Total Bits/sec Bytes/sec
DMZ_Any to Outside_Any
Service : SMTP
Action : PERMIT
Minute Hour Day
Real-time:
Downstream
1.3
1.0
0.7
0.3
0.0
(Bytes)
10:03
10:13
10:23
10:33
10:43
10:53
11:03
(Minute)
Traffic stream
Maximum stream
Average stream
Upstream
1.3

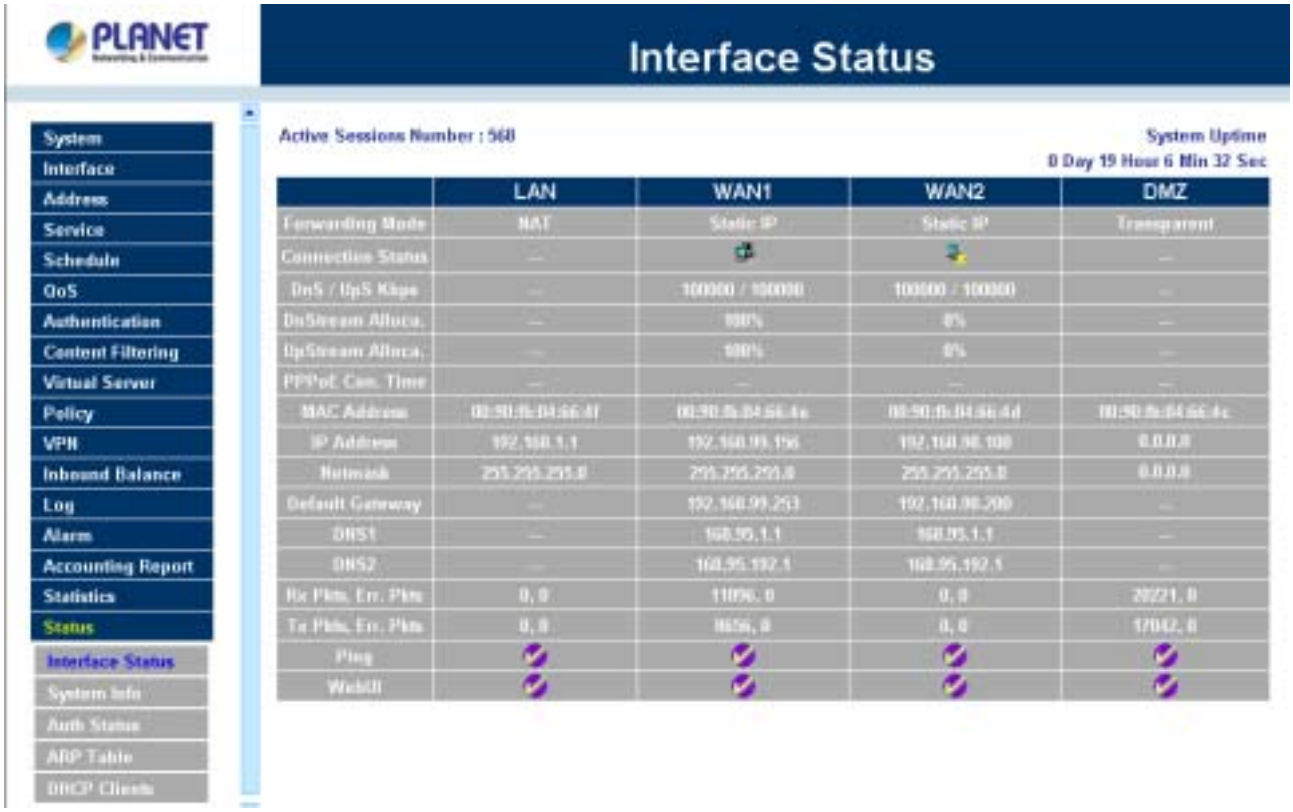
4.17 Status

In this section, the device displays the status information about the Multi-Homing Security Gateway. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Multi-Homing Security Gateway.

4.17.1 Interface Status

Entering the Interface Status window

Click on **Status** in the menu bar, then click **Interface Status** below it. A window will appear providing information from the Configuration menu. **Interface Status** will list the settings for **LAN Interface**, **WAN 1/2 Interface**, and the **DMZ Interface**.

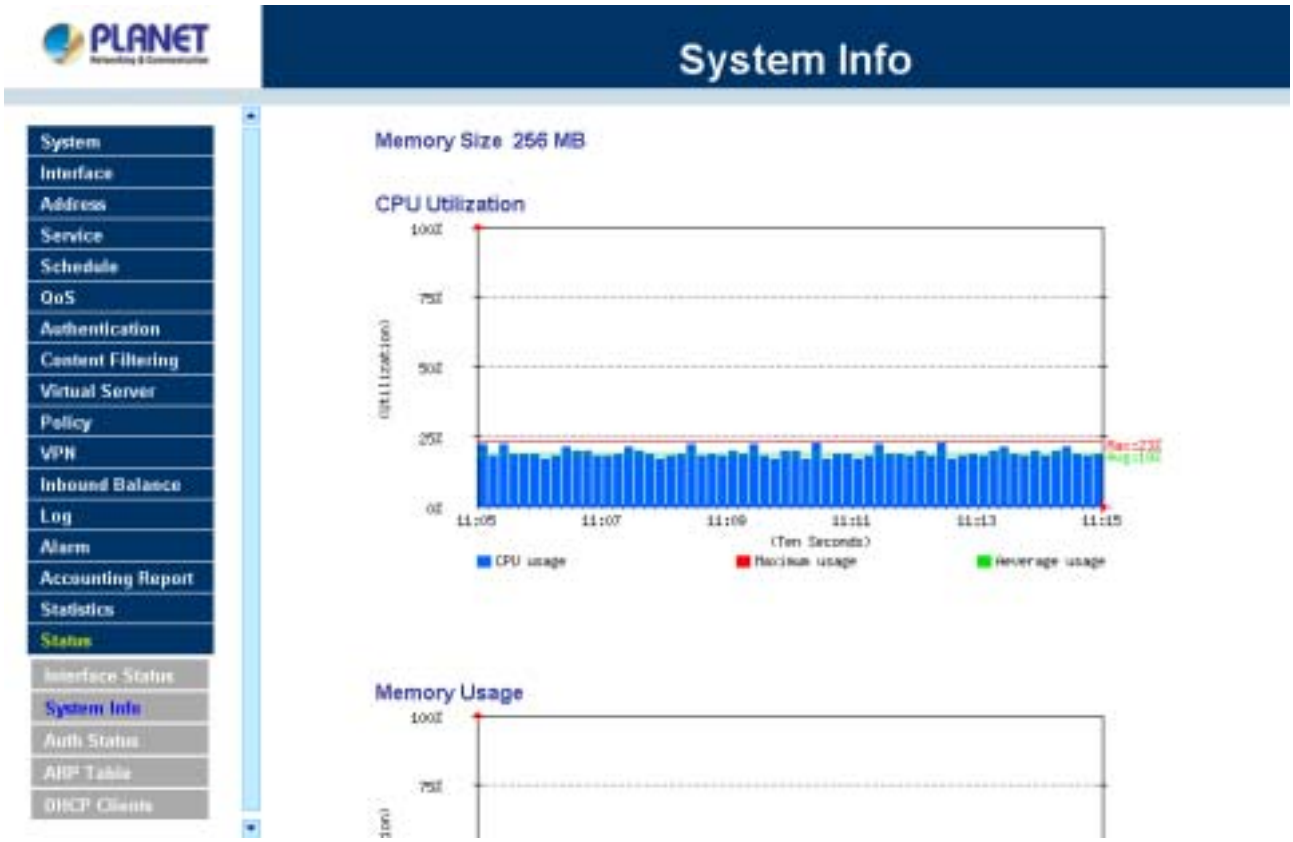


4.17.2 System Info (MH-4000 only)

NOTE: This function is not supported on MH-2000.

Entering the System Info window

Click on **Status** in the menu bar, then click **System Info** below it. A window will appear displaying a table with CPU Utilization / Memory Usage and Ram Disk Usage, the device will list them in this System Info.

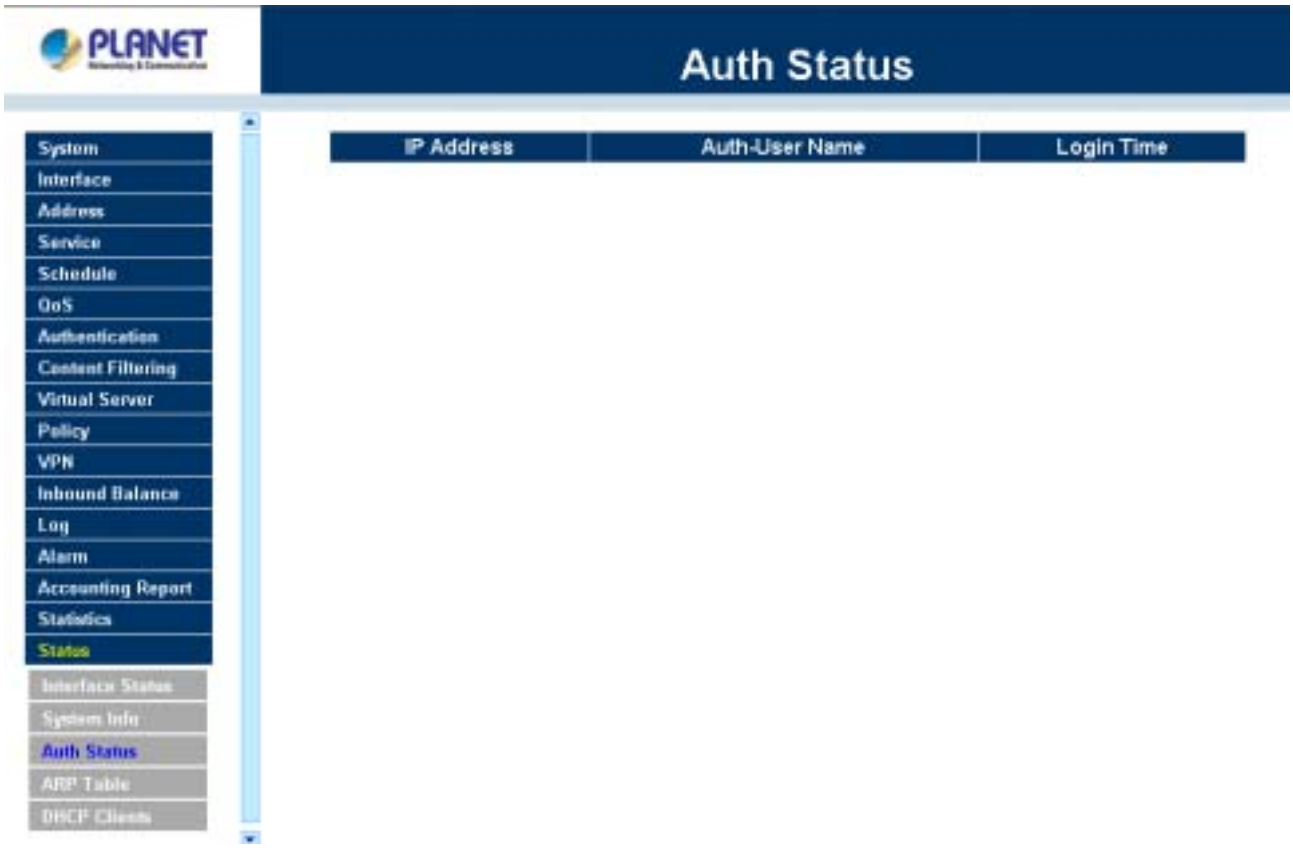


4.17.3 Auth Status (MH-4000 only)

NOTE: This function is not supported on MH-2000.

Entering the Auth Status window

Click on **Status** in the menu bar, then click Auth Status below it. A window will appear providing information from the Auth User menu. Auth Status will list the settings for Auth User login status.



IP Address: The IP address of the host computer.

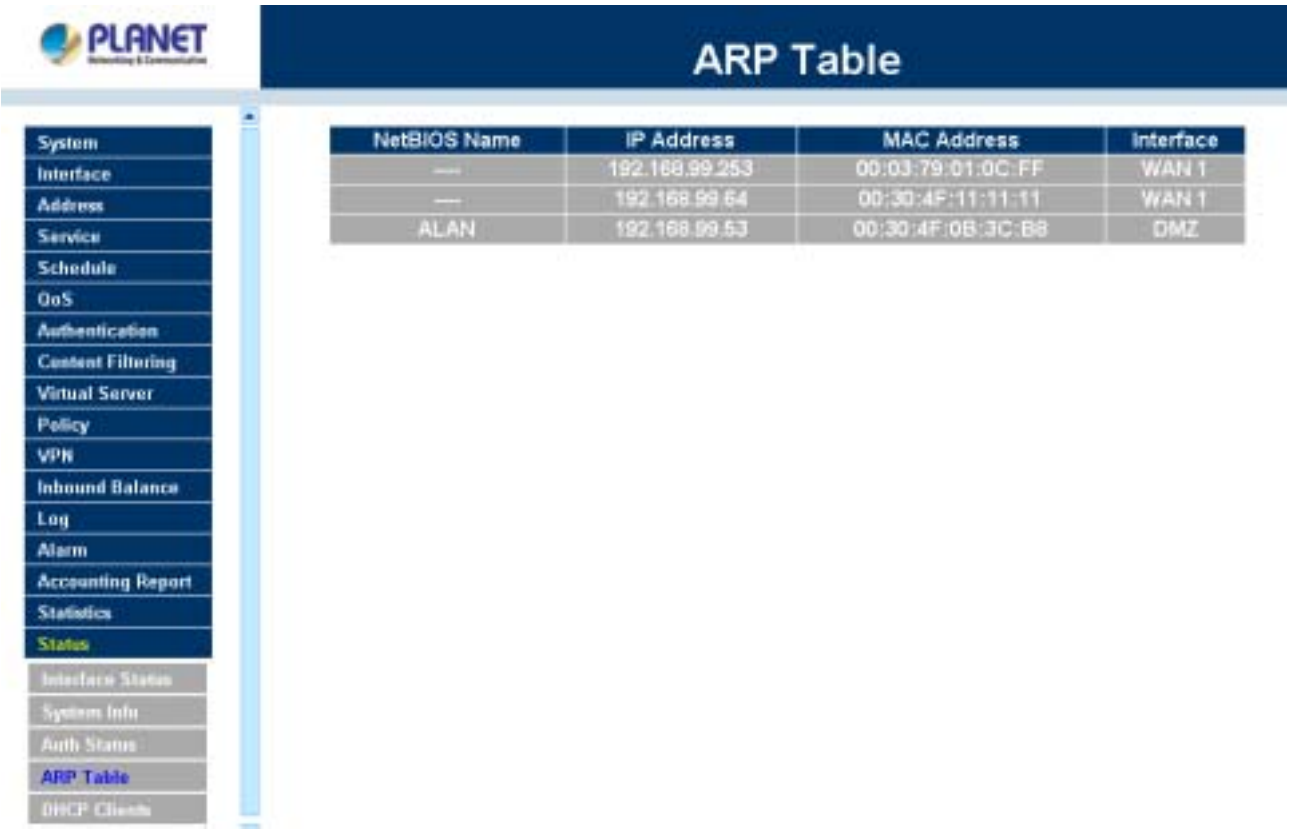
Auth-User Name: The Auth User Name of that host computer.

Login time: The Auth User login in time.

4.17.4 ARP Table

Entering the ARP Table window

Click on **Status** in the menu bar, then click **ARP Table** below it. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN 1/2, and DMZ network that replies to an ARP packet, the device will list them in this ARP table.



IP Address: The IP address of the host computer

MAC Address: The MAC address of that host computer

Interface: The port that the host computer is connected to (LAN, WAN 1/2, DMZ)

4.17.5 DHCP Clients

Entering the DHCP Clients window

Click on **Status** in the menu bar, then click on **DHCP Clients** below it. A window will appear displaying the table of DHCP clients that are connected to the device. The table will list host computers on the LAN network that obtain its IP address from the Multi-Homing Security Gateway's DHCP server function.

IP Address: the IP address of the LAN host computer

MAC Address: MAC address of the LAN host computer

Leased Time: The Start and End time of the DHCP lease for the LAN host computer.