

# **Multi-Homing Dual WAN Firewall Router**

## **User's Manual**

# Contents

<b>System</b>	<b>5</b>
Admin	7
Setting	12
Date/Time	19
Multiple NAT	20
Hack Alert	25
Route Table	27
DHCP	31
DNS Proxy	33
Dynamic DNS	37
Logout	41
Software Update	42
<b>Interface</b>	<b>43</b>
LAN	44
WAN	45
<b>Address</b>	<b>51</b>
LAN	52
LAN Group	56
WAN	59
WAN Group	63
<b>Service</b>	<b>67</b>
Pre-defined	68
Custom	69

Group	<b>73</b>
<b>Schedule Policy</b>	<b>77</b>
	<b>81</b>
Outgoing	<b>82</b>
Incoming	<b>89</b>
<b>VPN</b>	<b>93</b>
Autokey IKE	<b>94</b>
PPTP Server	<b>98</b>
PPTP Client	<b>103</b>
<b>Content filtering</b>	<b>107</b>
URL Blocking	<b>108</b>
General Blocking	<b>112</b>
<b>Virtual Server</b>	<b>113</b>
Mapped IP	<b>114</b>
Virtual Server	<b>118</b>
<b>LOG</b>	<b>125</b>
Traffic Log	<b>126</b>
Event Log	<b>129</b>
Log Backup	<b>132</b>
<b>Alarm</b>	<b>135</b>
Traffic Alarm	<b>136</b>
Event Alarm	<b>139</b>
<b>Statistics</b>	<b>143</b>
WAN Statistics	<b>144</b>
Policy Statistics	<b>145</b>
<b>Status</b>	<b>147</b>

Interface Status	<b>148</b>
ARP Table	<b>149</b>
DHCP Clients	<b>150</b>
<b>Setup Examples</b>	<b>151</b>

# System

The device Multi-Homing Administration and monitoring control 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 settings into local files;
- (3) Set up alerts for Hackers invasion.

## What is System?

"System" is the managing of settings such as the privileges of packets that pass through the Multi-Homing and monitoring controls. Administrators may manage, monitor, and configure Multi-Homing 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.

The eleven sub functions under **System** are **Admini**, **Setting**, **Date/Time**, **Multiple NAT**, **Hack Alert**, **Route Table**, **DHCP**, **DNS Proxy**, **Dynamic DNS**, **Logout** and **Software Update**.

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

**Setting:** The Administrator may use this function to backup Multi-Homing 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 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 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.

**Software Update:** 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.

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

**Multiple NAT** Multiple NAT allows local port to set multiple subnetworks and connect with the internet through different WAN 1 IP Addresses.

**Hack Alert** When abnormal conditions occur, the Multi-Homing will send an e-mail alert 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.

**DNS Proxy** The device's Administrator may use the DNS Proxy function to make the 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router act as a DNS Server for the LAN and WAN 1/2 network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing's IP address. For example, let's say an organization has their mail server (i.e., mail.dfl300.com) in the WAN 1/2 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 1/2 DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.dfl300.com), they would have to go out to the Internet, then come back through the Multi-Homing 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 WAN 1/2 network and they are bounded to real IP addresses. To avoid this, set up DNS Proxy so all the LAN network computers will use the device as a DNS server, which acts as the DNS Proxy.

**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

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

**Software Update** The administrator can update the device's software with the latest version..

# Admin

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

The screenshot shows the Mikrotik WinBox Admin interface. The left-hand menu is expanded to show the 'Admin' option. The main content area displays a table of administrators with the following data:

Admin Name	Privilege	Configure
admin	Read/Write	Modify

Below the table, there is a button labeled 'New Sub-Admin'.

## Settings of the Administration table

**Administrator Name:** The username of Administrators for the Multi-Homing. 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.”



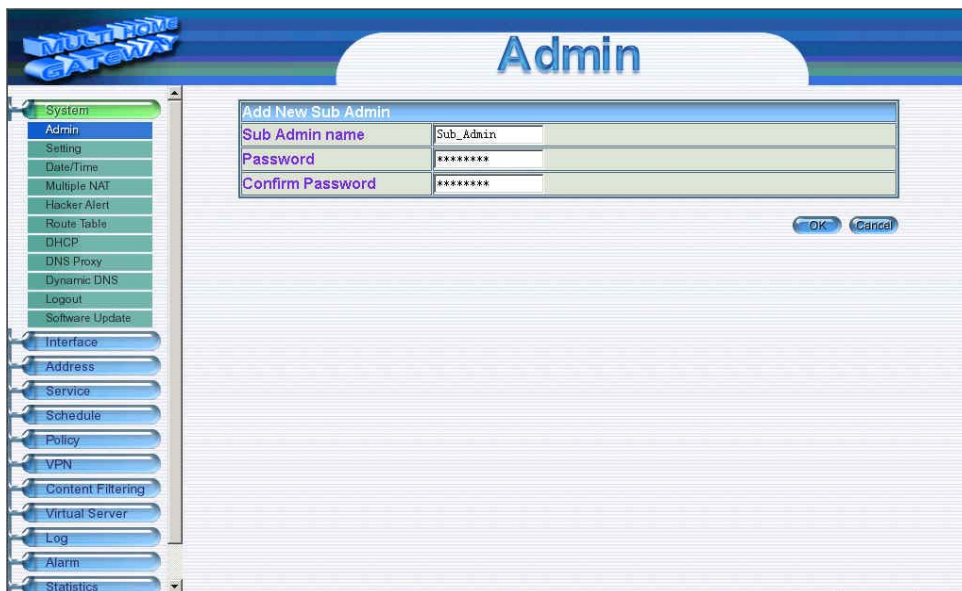
## Adding a new Sub Administrator

**Step 1.** In the **Admin** window, click the **New Sub Admin** button to create a new **Sub Administrator**.

**Step 2.** 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 3.** Click **OK** to add the user or click **Cancel** to cancel the addition.



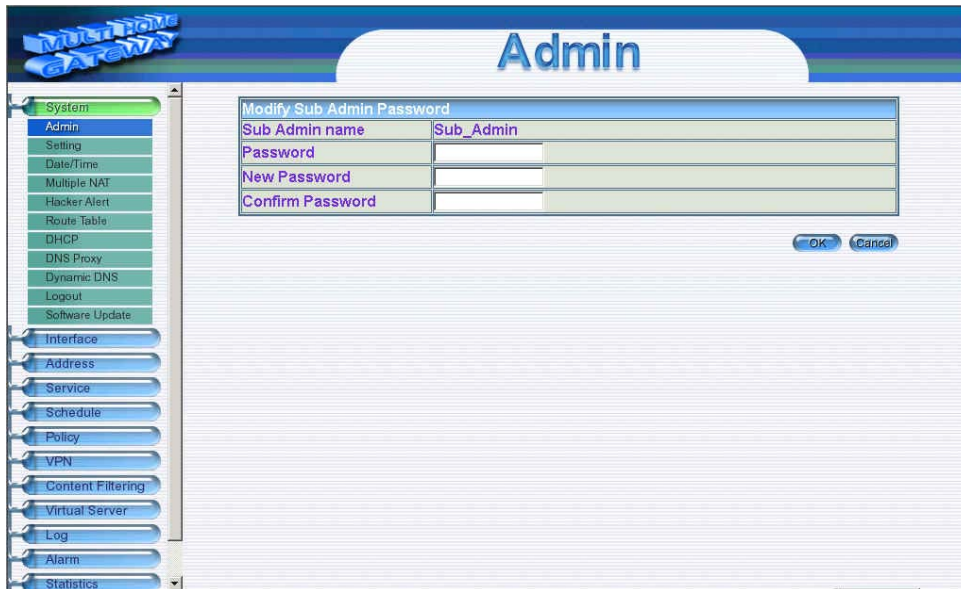
## Changing the Sub-Administrator's Password

**Step 1.** In the **Admin** window, locate the **Administrator** name you want to edit, and click on **Modify** in the **Configure** field.

**Step 2.** 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 3.** Click **OK** to confirm password change or click **Cancel** to cancel it.

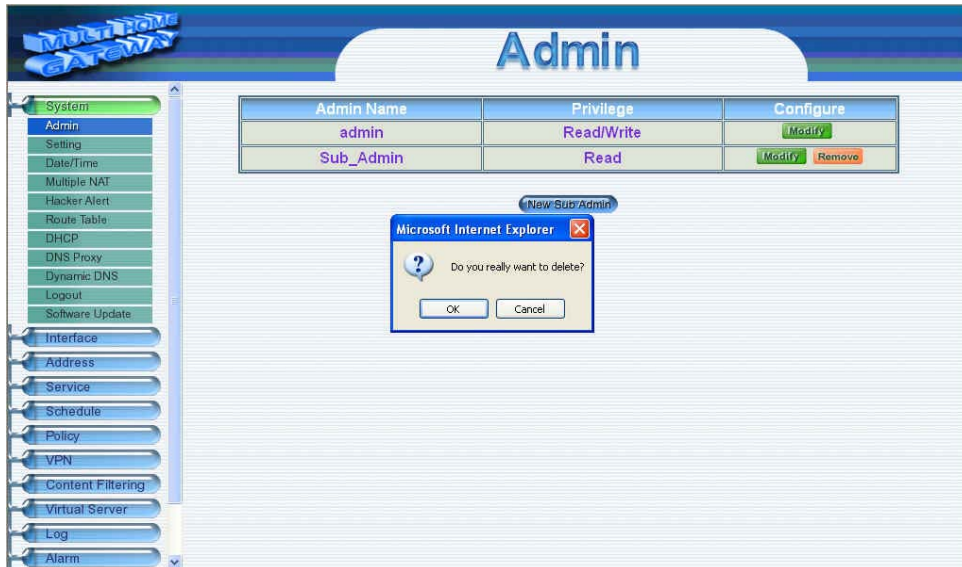


## Removing a Sub Administrator

**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.

**Step 3.** Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

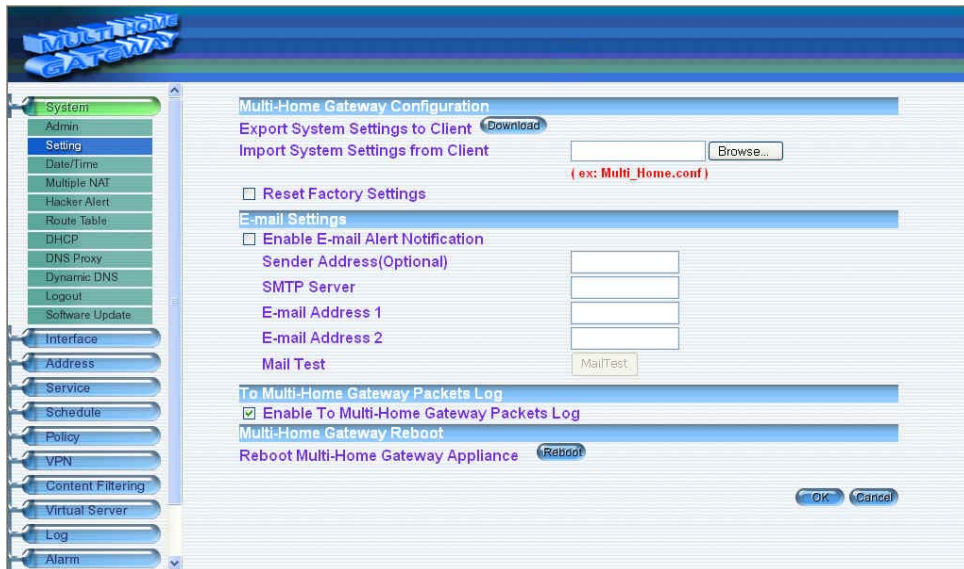


# Settings

The Administrator may use this function to backup Multi-Homing 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 back to default factory settings.

## Entering the Settings window

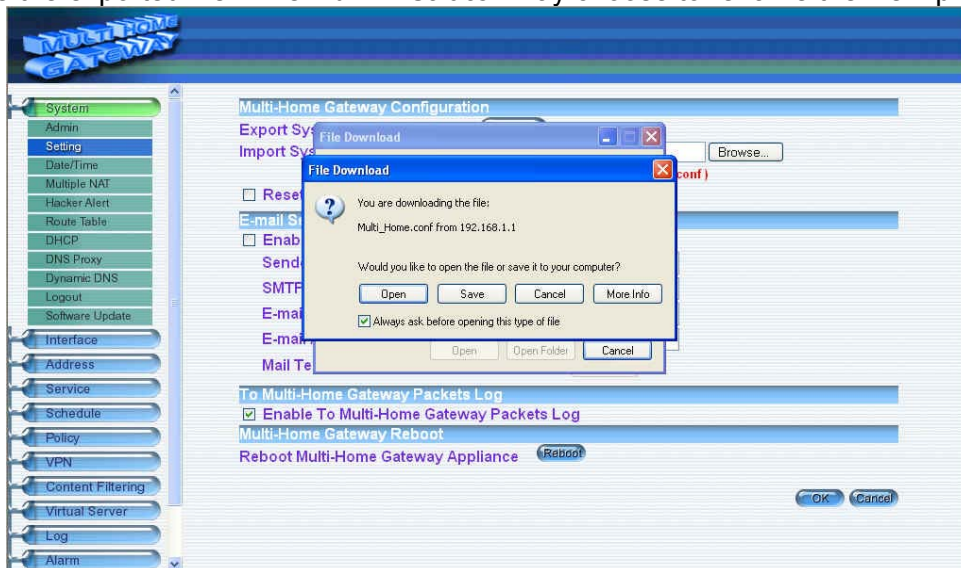
Click **Setting** in the **System** menu to enter the **Settings** window. The **Multi-Homing Configuration** settings will be shown on the screen.



## Exporting Multi-Homing Dual WAN Firewall Router settings

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

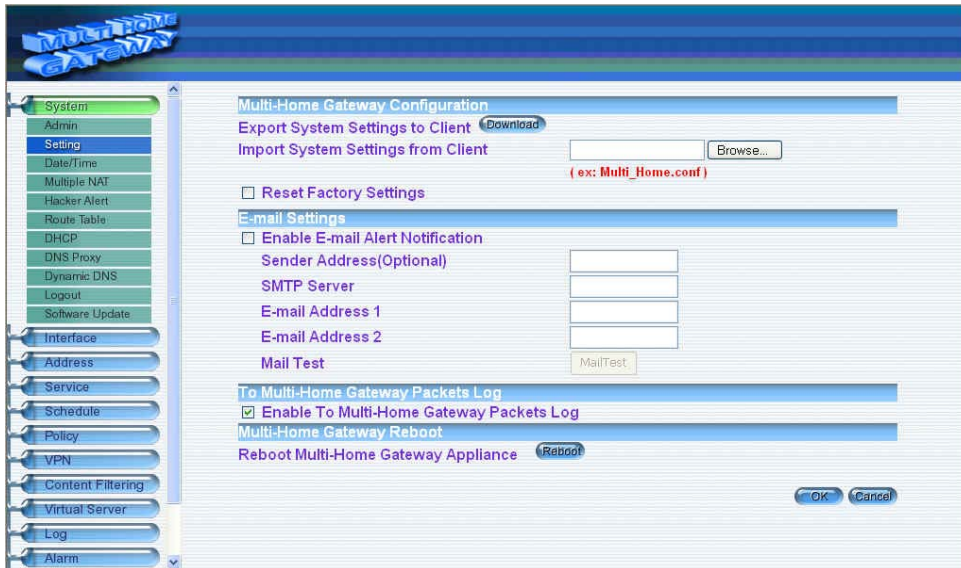
**Step 2.** When the **File Download** pop-up window appears, choose the destination place in which to save the exported file. The **Administrator** may choose to rename the file if preferred.



## Importing Multi-Homing settings

**Step 1.** Under **Multi-Homing Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file to which contains the saved Multi-Homing Settings, then click **OK**.

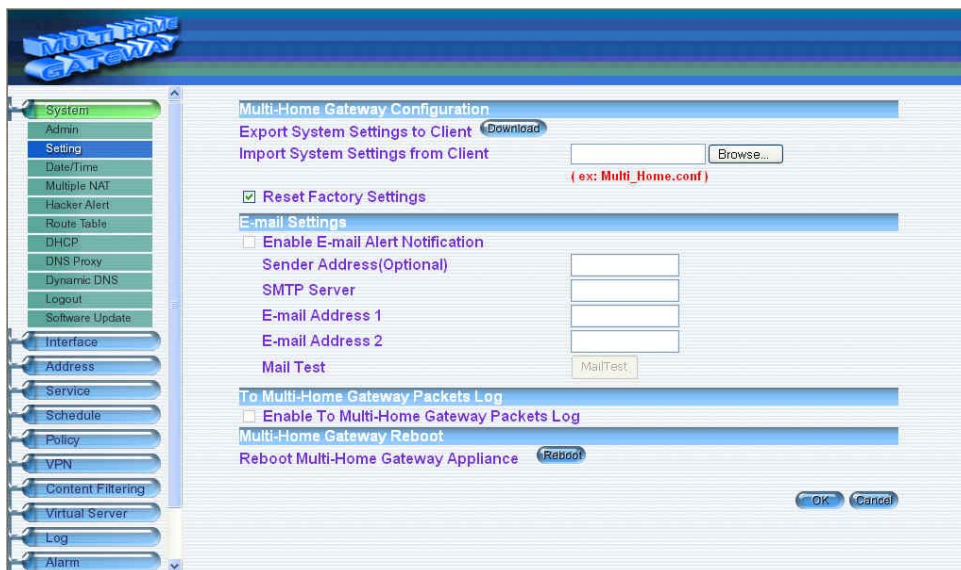
**Step 2.** Click **OK** to import the file into the **Multi-Homing** or click **Cancel** to cancel importing.



## Restoring Factory Default Settings

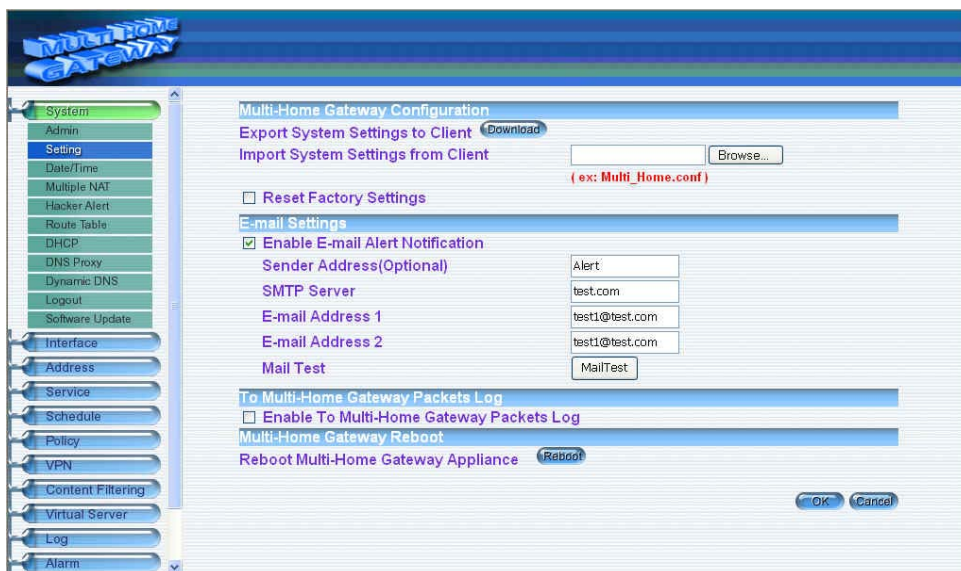
**Step 1.** Select **Reset Factory Settings** under **Multi-Home Configuration**.

**Step 2.** Click **OK** at the bottom-right of the screen to restore the factory settings.



## Enabling E-mail Alert Notification

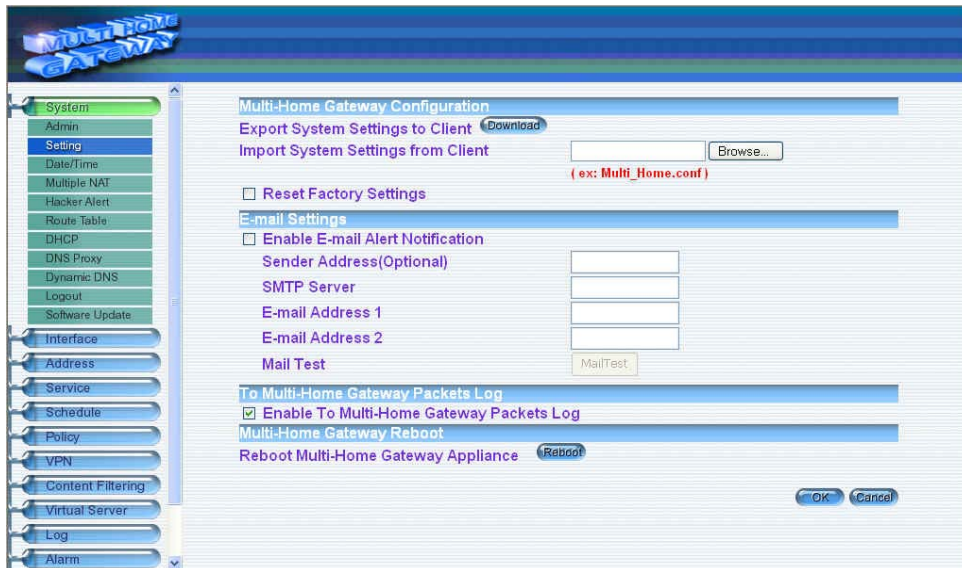
- Step 1.** Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Multi-Homing to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.
- Step 2. SMTP Server IP:** Enter SMTP server's 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)
- Step 5.** Click **OK** on the bottom-right of the screen to enable E-mail alert notification.





## To-Multi-Homing Packets Log

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



## Multi-Homing Reboot

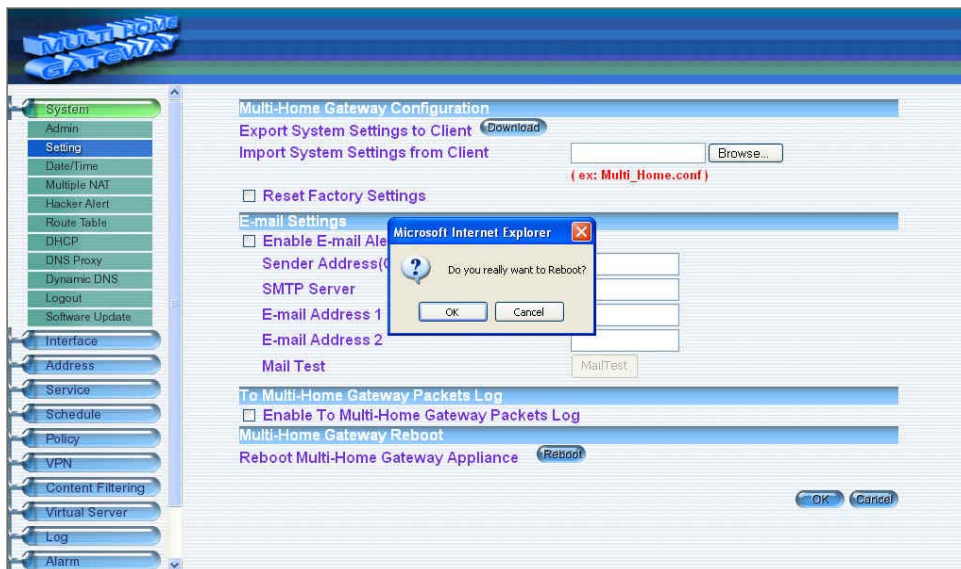
Select this option to the device's **Multi-Homing Reboot**. Once this function is enabled, the Multi-Homing will be reboot.

**Step 1.** Click **Setting** in the **Administration** menu to enter the settings window.

**Step 2.** Reboot Multi-Homing: Click **Reboot**.

**Step 3.** A confirmation pop-up box will appear.

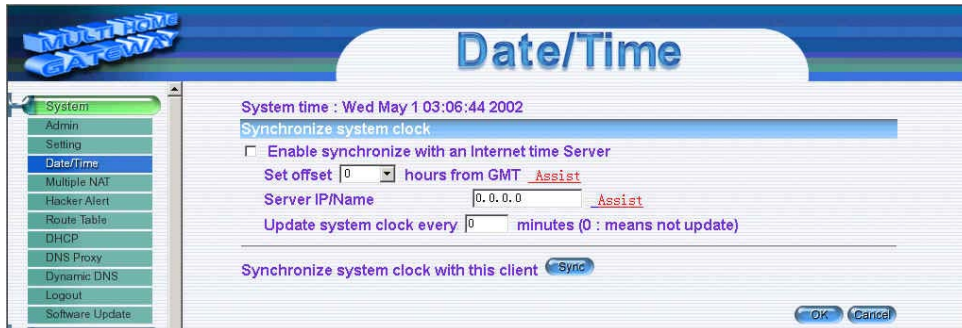
**Step 4.** Follow the confirmation pop-up box, click **OK** to restart Multi-Homing or click **Cancel** to discard changes.



## Date/Time

### Synchronizing the Multi-Homing with the System Clock

Select this option to synchronize this device's System clock with the client computer's clock. This will allow the logs to be time stamped correctly according to the computer clock time.



**Step 1.** Click **System** →Date/Time.

**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  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.

**Step 5. Synchronize system clock with this client:** You can synchronize this Homing Gateway with this client computer by clicking the **Sync** button .

**Step 6.** Click the **OK** button below to change the setting or click **Cancel** to discard changes.

## Multiple NAT

Multiple NAT allows local port to set multiple subnetworks 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 subnetworks for the purpose of convenient management. The settings are as the following :

- 1.R&D department subnetwork : 192.168.1.11/24(Internal)  $\leftrightarrow$  168.85.88.253(WAN 1)
2. Service department subnetwork : 192.168.2.11/24(Internal)  $\leftrightarrow$  168.85.88.252(WAN 1)
- 3.Sales department subnetwork : 192.168.3.11/24(Internal)  $\leftrightarrow$  168.85.88.251(WAN 1)
- 4.Procurement department subnetwork 192.168.4.11/24(Internal)  $\leftrightarrow$  168.85.88.250(WAN 1)
- 5.Accounting department subnetwork 192.168.5.11/24(Internal)  $\leftrightarrow$  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 NAT , after completing the settings, each department use the different WAN IP Address to connect to the internet. The settings of each department are as the following

Service IP Address : 192.168.2.1

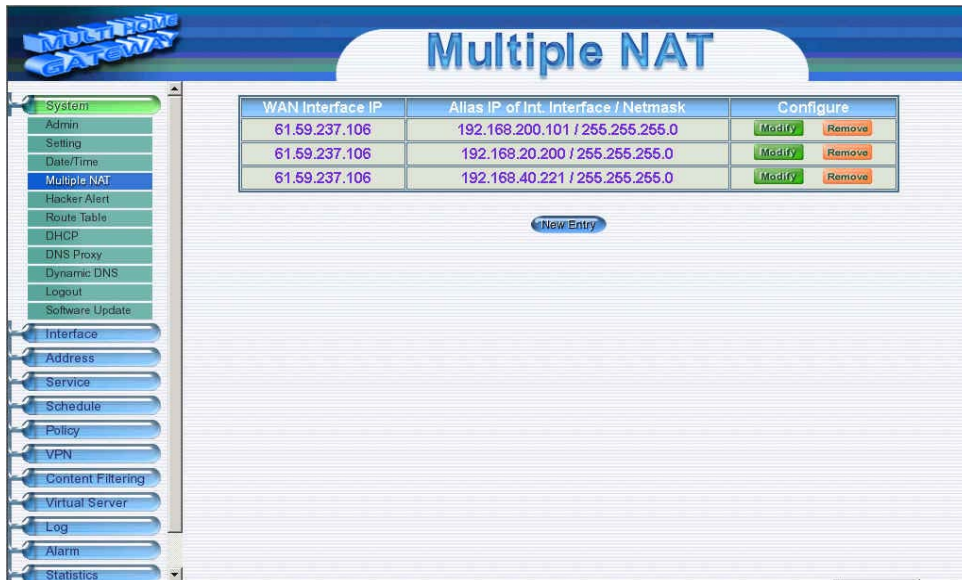
Subnet Mask : 255.255.255.0

Default Gateway : 192.168.2.11

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

## Multiple NAT settings

Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.



### Multiple NAT

- **Global port interface IP Address** : Global port IP Address.
- **Local port interface IP Address** : Local port IP Address and subnet Mask.
- **Modify** : Modify the settings of Multiple NAT. Click **Modify** to modify the parameters of Multiple NAT or click **Delete** to delete settings.

## Add Multiple NAT

**Step 1.** Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.

**Step 2.** Click the **Add** button below to add Multiple NAT.

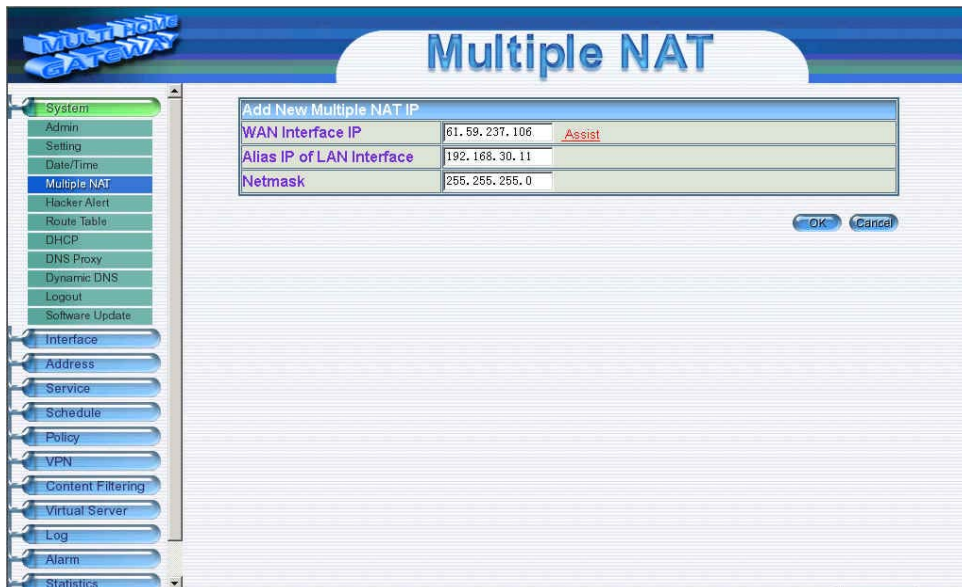
**Step 3.** Enter the IP Address in the website name column of the new window.

1.1 Global port interface IP Address : Select Global port IP Address.

3.2 Local port interface IP Address : Enter Local port IP Address.

3.3 Subnet Mask : Enter Local port subnet Mask.

**Step 4.** Click **OK** to add Multiple NAT or click **Cancel** to discard changes.



The screenshot shows a web-based configuration interface for 'Multiple NAT'. On the left is a vertical menu with categories: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, and Statistics. The 'Multiple NAT' option is selected under the 'System' category. The main area is titled 'Multiple NAT' and contains a form titled 'Add New Multiple NAT IP'. The form has three rows of input fields:

Add New Multiple NAT IP		
WAN Interface IP	61.59.237.106	<a href="#">Assist</a>
Alias IP of LAN Interface	192.168.30.11	
Netmask	255.255.255.0	

At the bottom right of the form are 'OK' and 'Cancel' buttons.

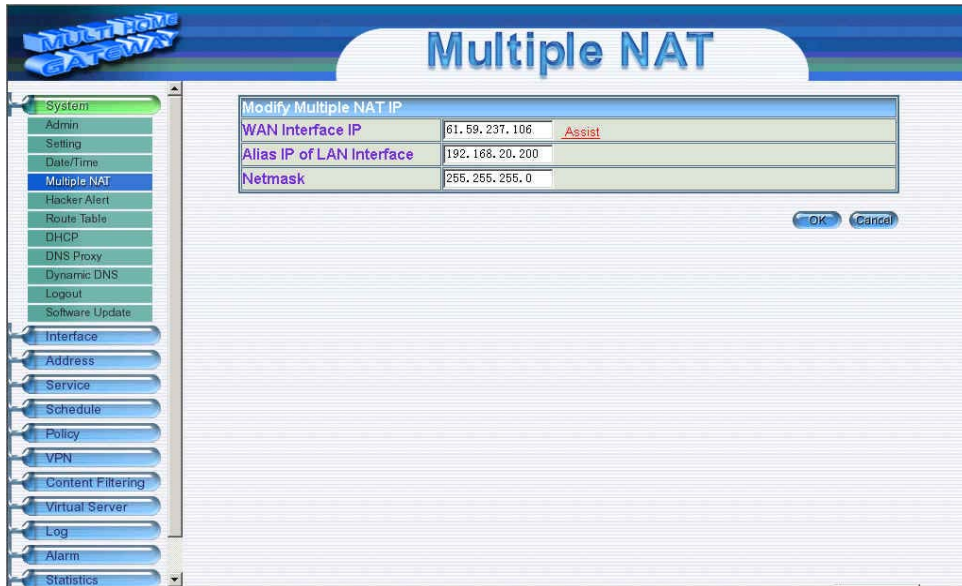
## Modify Multiple NAT

**Step 1.** Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.

**Step 2.** Find the IP Address you want to modify and click **Modify**

**Step 3.** Enter the new IP Address in **Modify Multiple NAT** window.

**Step 4.** Click the **OK** button below to change the setting or click **Cancel** to discard changes.

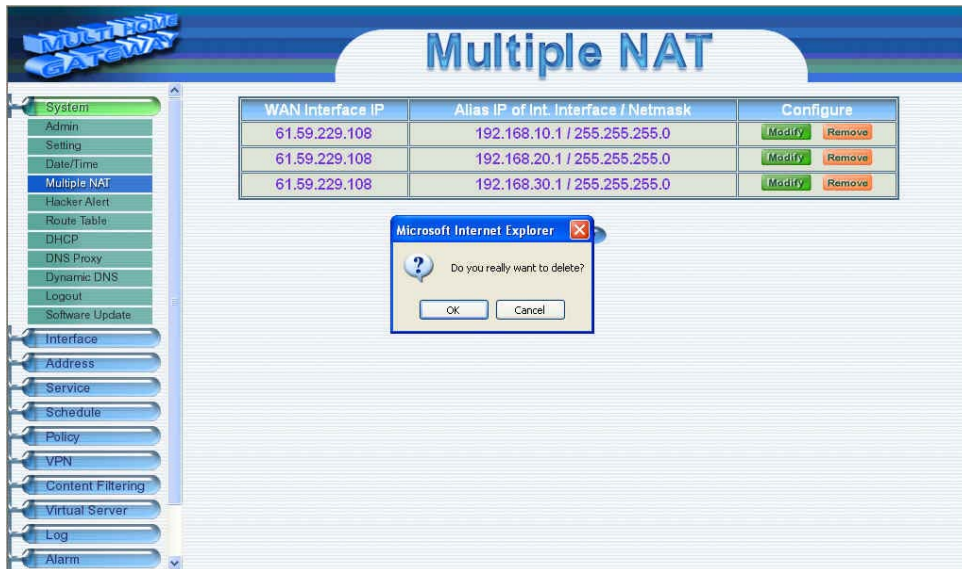


# Delete Multiple NAT

**Step 1.** Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.

**Step 2.** Find the IP Address you want to delete and click **Delete**.

**Step 3.** A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.





## Hacker Alert

The Administrator can enable the device's auto detect functions in this section. When abnormal conditions occur, the Multi-Homing 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 allow to enter the network/Multi-Homing. 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 theLAN networks or to the Multi-Homing, 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. 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. 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 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. 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.

## Route Table

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

### Entering the Route Table screen

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.

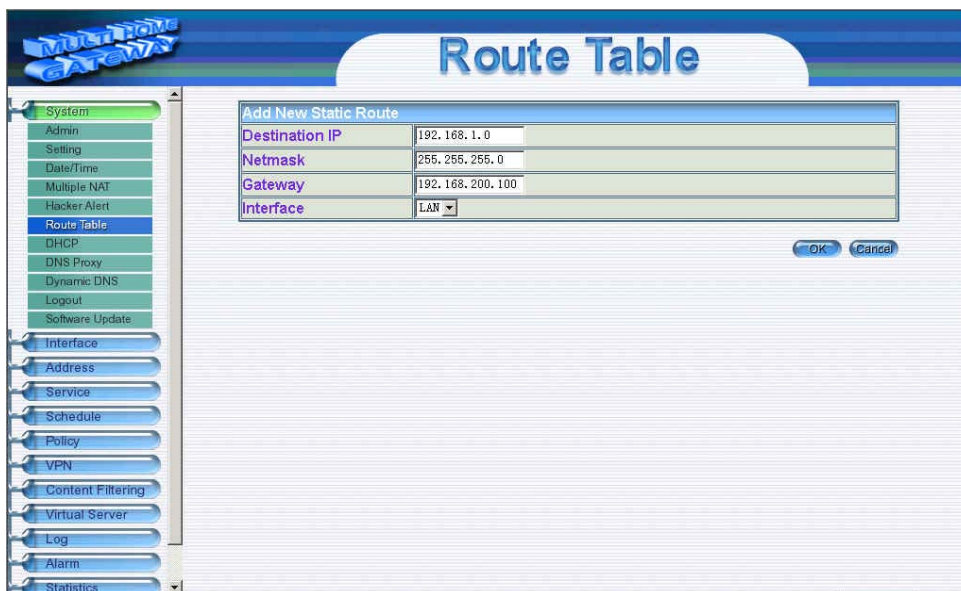
## Adding a new Static Route

**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 (Internal, WAN 1 or WAN 2).

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



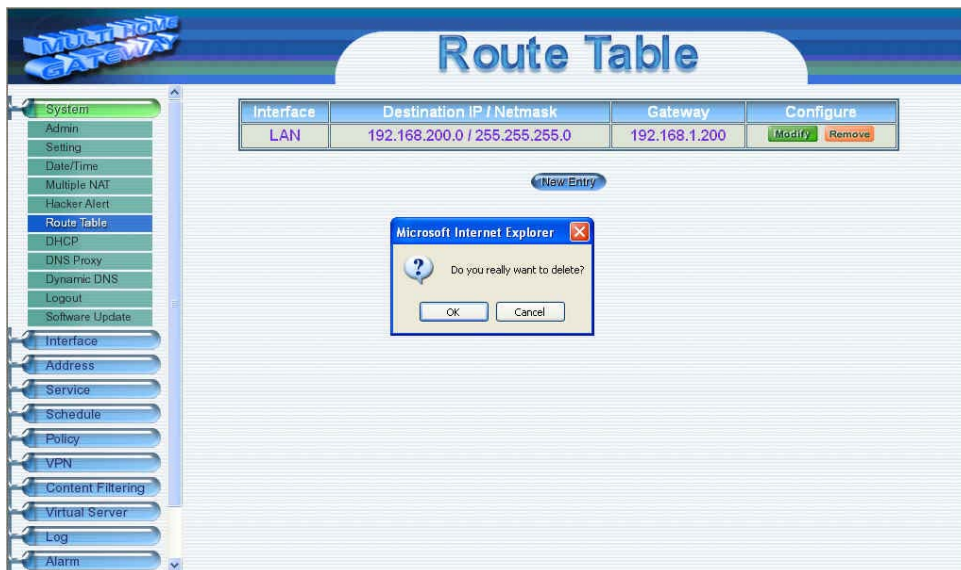
## Modifying a Static Route:

- 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.



## DHCP

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

### Entering the DHCP window

**Step 1.** 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.

**DHCP**

**Dynamic IP Address**

Subnet	192.168.200.0	Netmask	255.255.255.0
Gateway	192.168.200.1	Broadcast	192.168.200.255

Enable DHCP Support

Domain Name

Domain Name Server

Client IP Range 1  To

Client IP Range 2  To

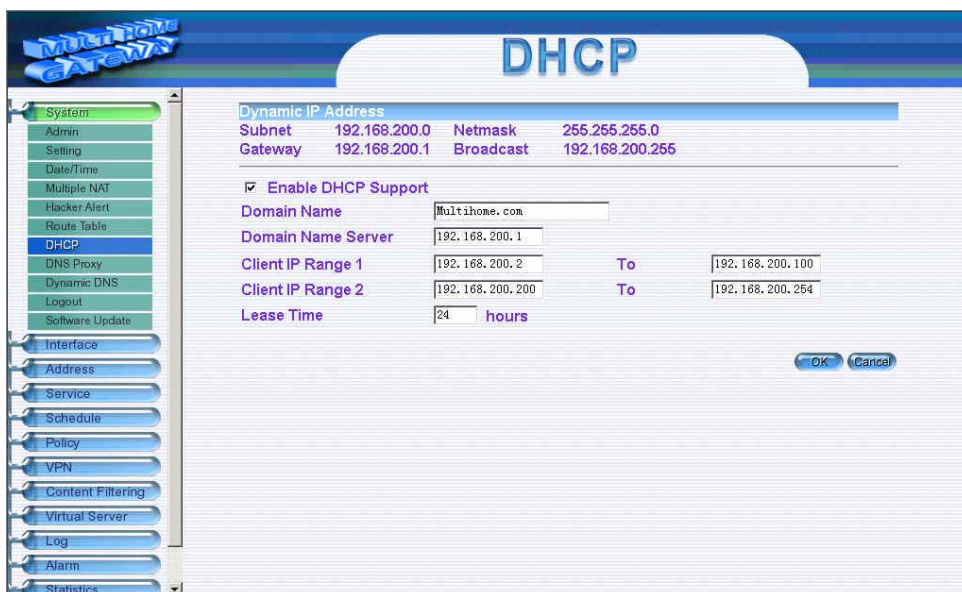
Lease Time  hours

### 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**.
- Step 2. Domain Name:** The Administrator may enter the name of the LAN network domain if preferred.
- Step 3. Domain Name Server:** Enter in the IP address of the DNS Server to be assigned to the LAN network.
- Step 4. Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients.
- Step 5. Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)
- Step 6.** Click **OK** to enable DHCP support.



The screenshot shows a web-based configuration interface for DHCP. The title bar reads "DHCP". On the left is a vertical menu with various system settings, with "DHCP" highlighted. The main content area is titled "Dynamic IP Address" and contains the following configuration fields:

Dynamic IP Address			
Subnet	192.168.200.0	Netmask	255.255.255.0
Gateway	192.168.200.1	Broadcast	192.168.200.255

Below this table, there is a checkbox labeled "Enable DHCP Support" which is checked. The following fields are present:

- Domain Name: Multihome.com
- Domain Name Server: 192.168.200.1
- Client IP Range 1: 192.168.200.2 To 192.168.200.100
- Client IP Range 2: 192.168.200.200 To 192.168.200.254
- Lease Time: 24 hours

At the bottom right of the configuration area, there are "OK" and "Cancel" buttons.



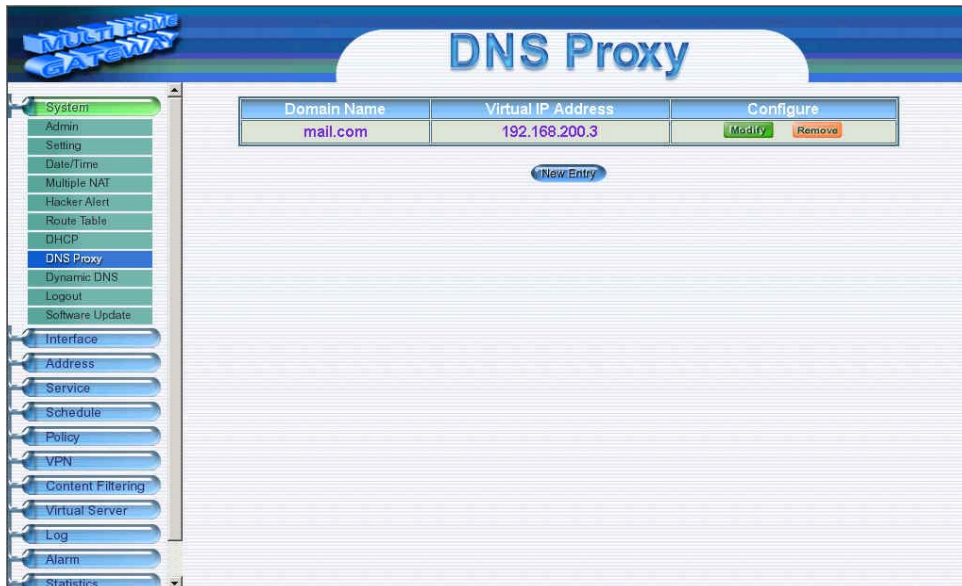
## DNS-Proxy

The device's Administrator may use the DNS Proxy function to make the 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router act as a DNS Server for the LAN and WAN 1/2 network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing's IP address. For example, let's say an organization has their mail server (i.e., mail.dfl300.com) in the WAN 1/2 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 1/2 DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.dfl300.com), they would have to go out to the Internet, then come back through the Multi-Homing 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 WAN 1/2 network and they are bounded to real IP addresses. To avoid this, set up DNS Proxy so all the LAN network computers will use the device 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.***

### Entering the DNS Proxy window

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**:

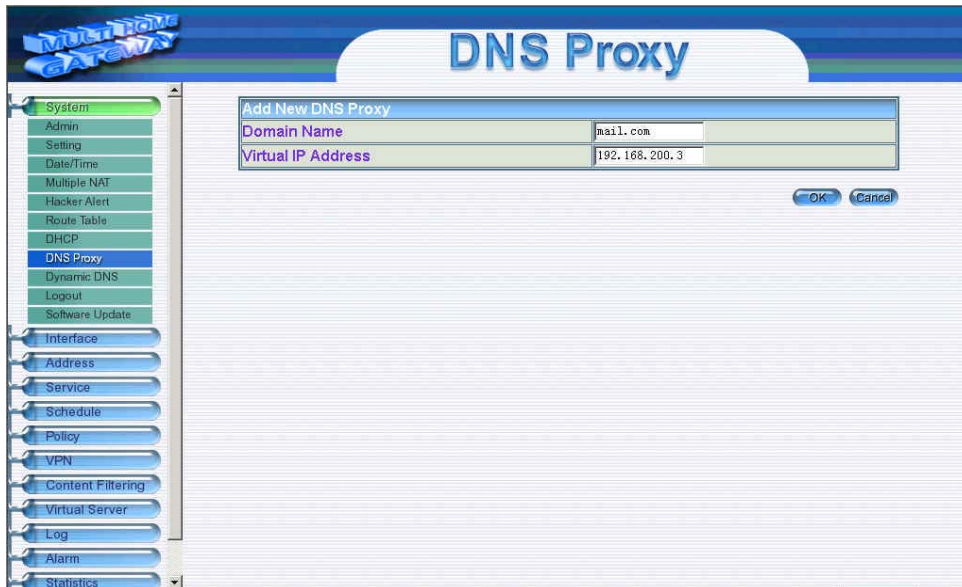
- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to DNS Proxy
- **Configure:** modify or remove each DNS Proxy policy

## Adding a new DNS Proxy

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

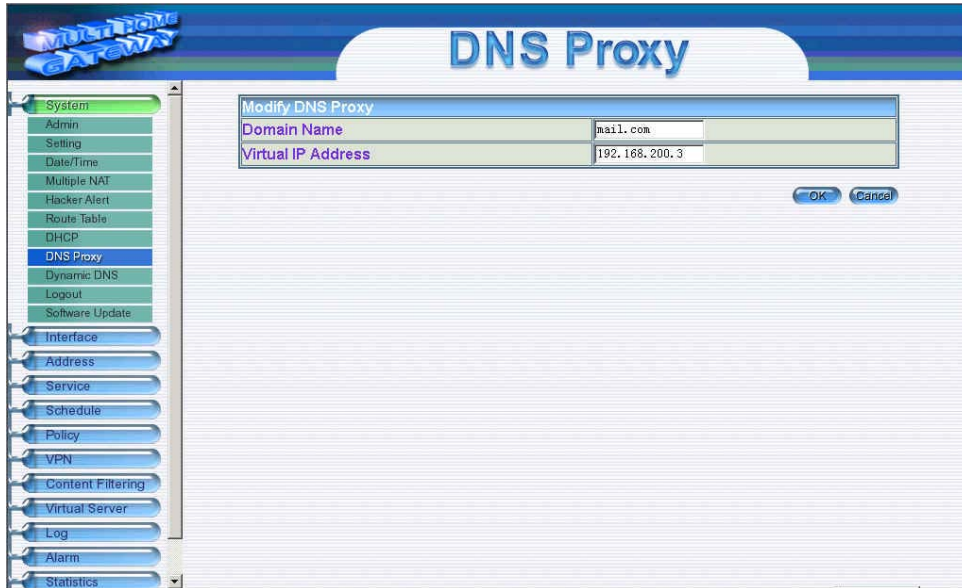
**Step 2:** Fill in the appropriate settings for the domain name and virtual IP address.

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



## Modifying a DNS Proxy

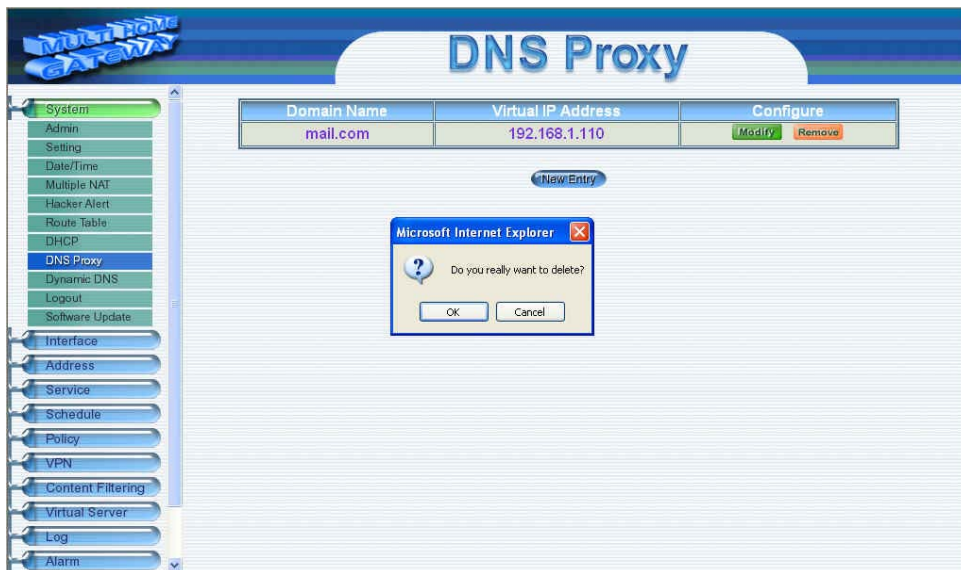
- Step 1:** In the DNS Proxy window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.
- Step 2:** Make the necessary changes needed.
- Step 3:** Click **OK** to save changes or click on **Cancel** to cancel modifications.



## 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**.







## 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.

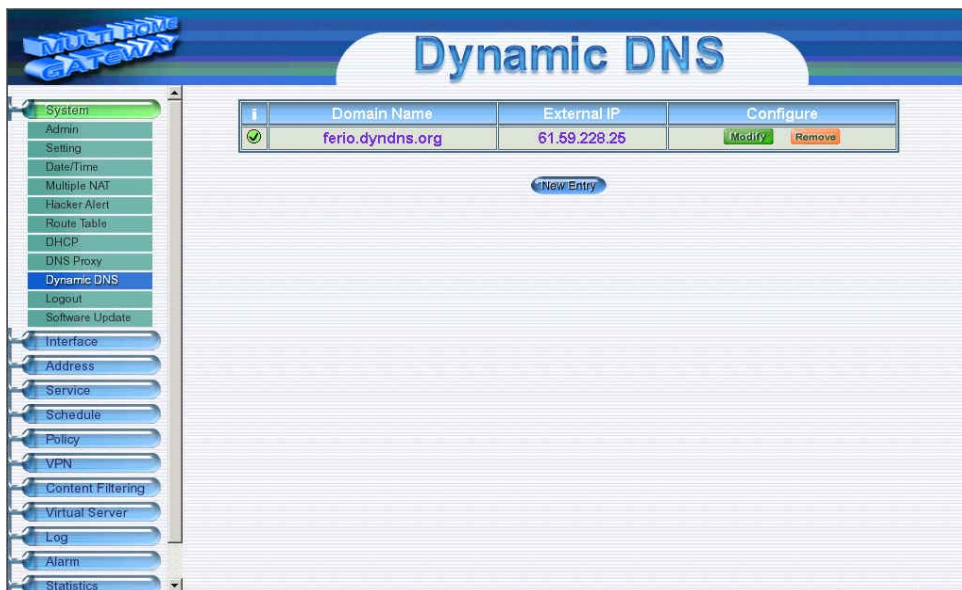
1. The nouns in Dynamic DNS window :

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

2. How to use dynamic DNS :

The Multi-Homing provides 3 service providers, users have to register first to use this function. For the usage regulations, see the providers' websites.

**How to register** : First, 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.



## Dynamic DNS settings

**Step 1:** Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

**Step 2:** Click **Add** button.

**Step 3:** 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 1/2 IP** : Check to automatically fill in the WAN 1/2 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.

**Step 4:** Click **OK** to add dynamic DNS or click **Cancel** to discard changes.

The screenshot shows the 'Dynamic DNS' configuration window in Mikrotik WinBox. The window title is 'Dynamic DNS' and the main title is 'Add New Dynamic DNS'. The form contains the following fields:

Service Provider :	DynDNS (www.dyndns.org) [ U. S. A. ]	<a href="#">Sign up</a>
External IP :	61.59.228.25	<input checked="" type="checkbox"/> Automatically WAN1
User Name :	ferio	
Password :	*****	
Domain Name :	ferio . dyndns.org	

At the bottom right of the form, there are two buttons: 'OK' and 'Cancel'.

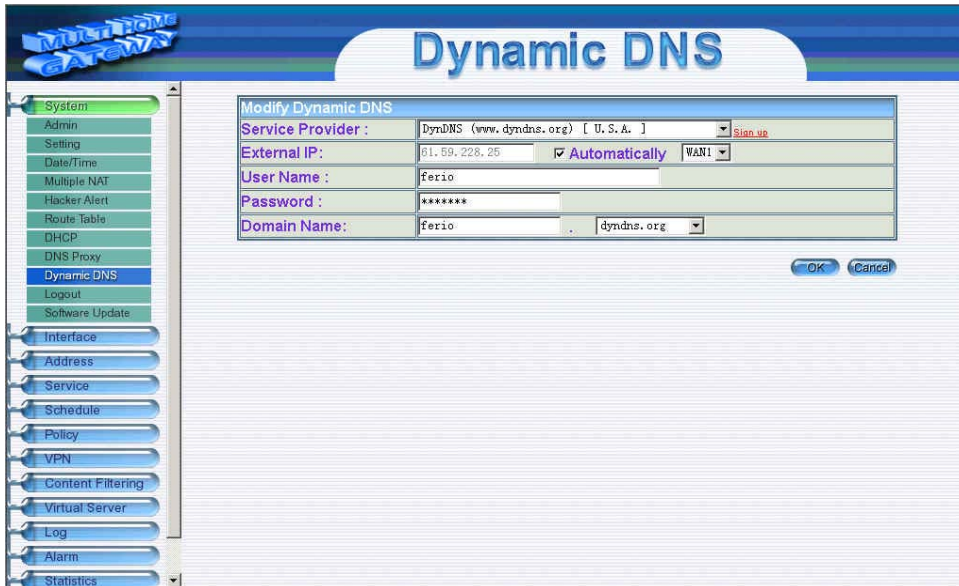
## Modify dynamic DNS

**Step 1:** Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

**Step 2:** Find the item you want to change and click **Modify**.

**Step 3:** Enter the new information in the Modify Dynamic DNS window.

**Step 4:** Click **OK** to change the settings or click **Cancel** to discard changes.



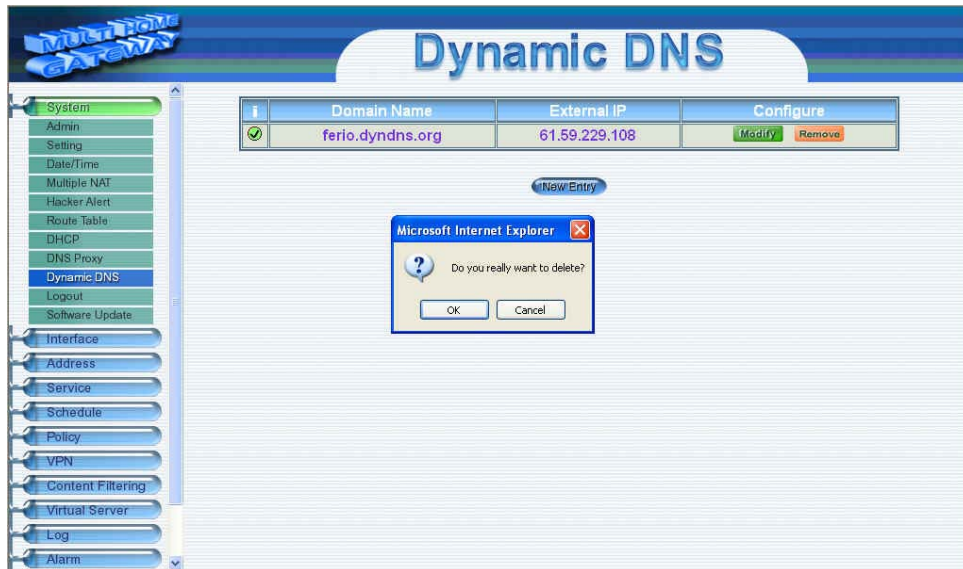
The screenshot shows the Mikrotik WinBox interface. On the left is a navigation menu with the following items: System (highlighted), Admin, Setting, Date/Time, Multiple NAT, Hacker Alert, Route Table, DHCP, DNS Proxy, Dynamic DNS (highlighted), Logout, Software Update, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, and Statistics. The main window is titled "Dynamic DNS" and contains a "Modify Dynamic DNS" form. The form fields are: Service Provider (DynDNS (www.dyndns.org) [ U. S. A. ] with a "Sign up" link), External IP (61.59.228.25 with "Automatically" checked and "WAN1" selected), User Name (ferio), Password (\*\*\*\*\*), and Domain Name (ferio . dyndns.org). At the bottom right of the form are "OK" and "Cancel" buttons.

## Delete Dynamic DNS

**Step 1:** Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

**Step 2:** Find the item you want to change and click **Delete**.

**Step 3:** A confirmation pop-up box will appear, click **OK** to delete the settings or click **Cancel** to discard changes.



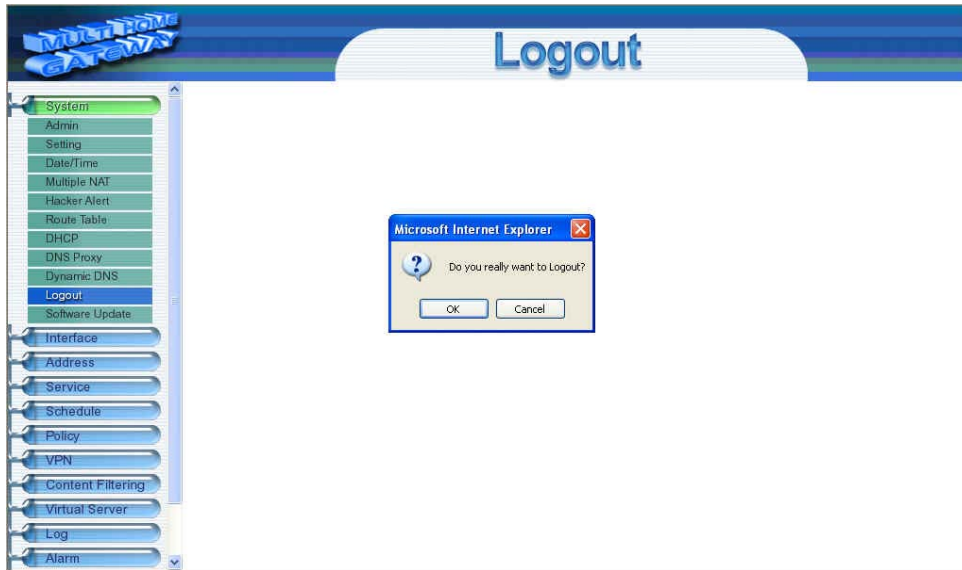


## Logout

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

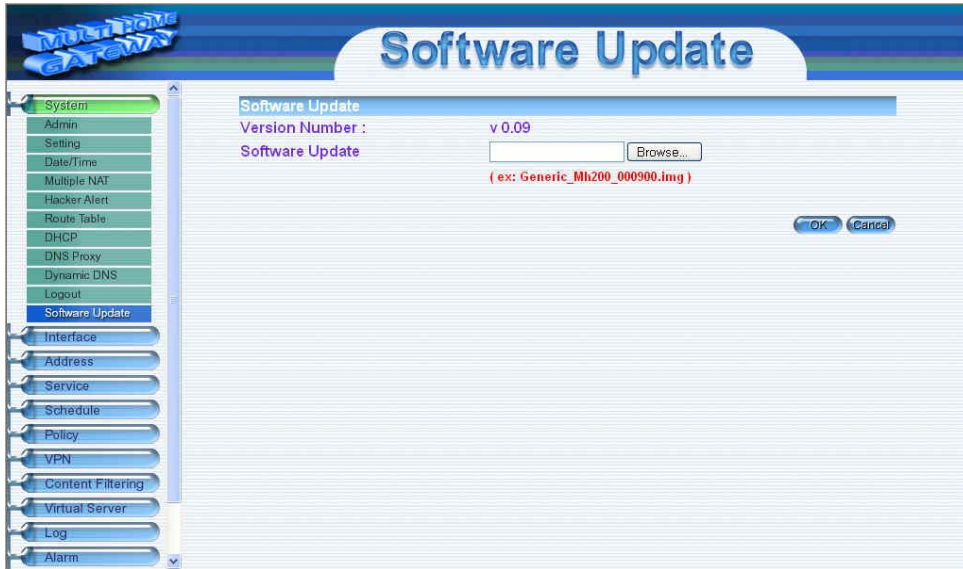
**Step 1.** Click Logout the Multi-Homing.

**Step 2.** Click OK to logout or click Cancel to discard the change.



# Software Update

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



# 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 network, and the WAN 2 network. The netmask and gateway IP addresses are also configured in this section.

## 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

### Internal Interface

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'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 and restart the System to make the new IP address effective. For example, if the Multi-Homing'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.

**NetMask:** This is the netmask 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. *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.

## 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.

The screenshot displays the WAN configuration page. On the left, a vertical menu lists various system settings, with 'Interface' and 'WAN' highlighted. The main content area features a 'Balance Mode' dropdown set to 'Auto'. Below this is a table with the following data:

WAN No.	Connect Mode	IP Address	Saturated Connections	Enable	Configure	Priority
1	Dynamic IP	192.168.1.79	1	P W	Modify	1
2	Dynamic IP	---	1	P W	Modify	2

#### Balance Mode :

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

**WAN No:** Set the WAN 1/2 order.

**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 switches to the next agent on the list. This function is only applicable for **By Session** mode.

**Enable:** 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 Interface

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

**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.

**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. This will allow people from the Internet to be able to ping the Multi-Homing. *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.

**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:

**IP Address:** The dynamic IP address obtained by the Multi-Homing 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.

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

**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.

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

The screenshot shows the 'WAN1 Interface' configuration page. On the left is a navigation menu with options: System, Interface, LAN, WAN, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'WAN' option is selected. The main content area is titled 'WAN1 Interface' and contains the following fields and controls:

- Alive Indicator Site IP or URL :  [Assist](#)
- Wait  seconds between sending each packet. (0 : means not checking)
- Service selection:
  - PPPoE (ADSL User)
  - Dynamic IP Address (Cable Modem User)
  - Static IP Address
- IP Address:  [Renew](#)
- MAC Address:  [Release](#)
- Hostname:
- Domain Name:
- Downstream Max Bandwidth:  Kbps
- Upstream Max Bandwidth:  Kbps
- Enable:
- Ping:
- WebUI:

At the bottom right, there are 'OK' and 'Cancel' buttons.

## WAN 2 Interface

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

**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.

**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 2 network to ping the IP Address of the Multi-Homing. This will allow people from the Internet to be able to ping the Multi-Homing. *If set to enable, the device will respond to echo request packets from the WAN 2 network.*

**WebUI:** Select this to allow the device WEBUI to be accessed from the WAN 2 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.

**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:

**IP Address:** The dynamic IP address obtained by the Multi-Homing from the ISP will be displayed here. This is the IP address of the WAN 2 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.

**Ping:** Select this to allow the WAN 2 network to ping the IP Address of the Multi-Homing. This will allow people from the Internet to be able to ping the Multi-Homing. *If set to enable, the device will respond to echo request packets from the WAN 2 network.*

**WebUI:** Select this to allow the device WEBUI to be accessed from the WAN 2 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.



**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 2 port of the device.

**Netmask:** This will be the Netmask of the WAN 2 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.

**Ping:** Select this to allow the WAN 2 network to ping the IP Address of the Multi-Homing. This will allow people from the Internet to be able to ping the Multi-Homing. *If set to enable, the device will respond to echo request packets from the WAN 2 network.*

**WebUI:** Select this to allow the device WEBUI to be accessed from the WAN 2 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.

The screenshot shows a web-based configuration interface for a WAN2 interface. The interface is titled "WAN" and has a sidebar with various configuration options. The main content area is titled "WAN2 Interface" and is currently set to "Enable". The "Alive Indicator Site IP or URL" is set to "168.95.1.1" with an "Assist" button. The "Wait" time is set to "1" seconds between sending each packet. The "Service" is set to "Dynamic IP Address (Cable Modem User)". The "IP Address" is set to "0.0.0.0" with "Renew" and "Release" buttons. The "MAC Address" is set to "00e09895dc3b" with a "Release" button. The "Hostname" and "Domain Name" fields are empty. The "Downstream Max Bandwidth" is set to "512" Kbps and the "Upstream Max Bandwidth" is set to "64" Kbps. The "Enable" checkbox is checked, and the "Ping" and "WebUI" checkboxes are also checked. The interface has "OK" and "Cancel" buttons at the bottom right.



# Address

The 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN 1/2 network, WAN 1/2 group.

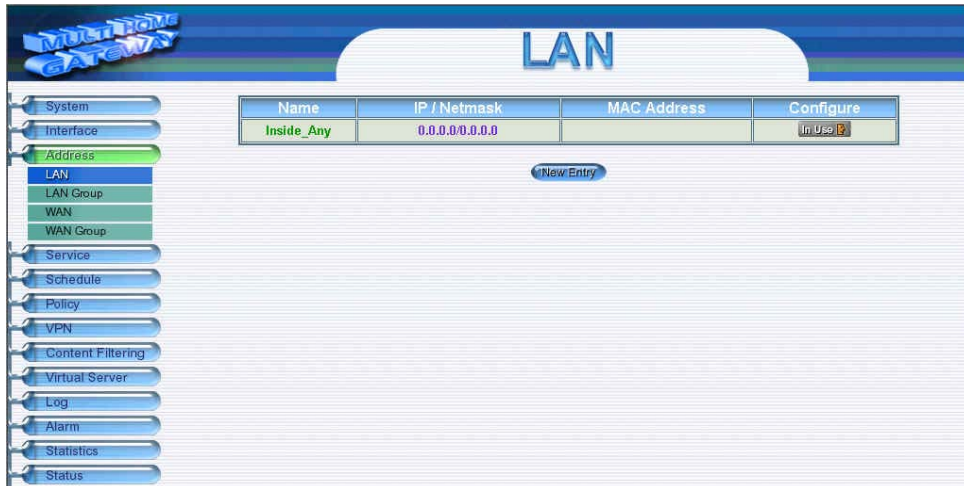
## What is the Address Table?

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, WAN1/2 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 1/2 Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies. 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.

# 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.

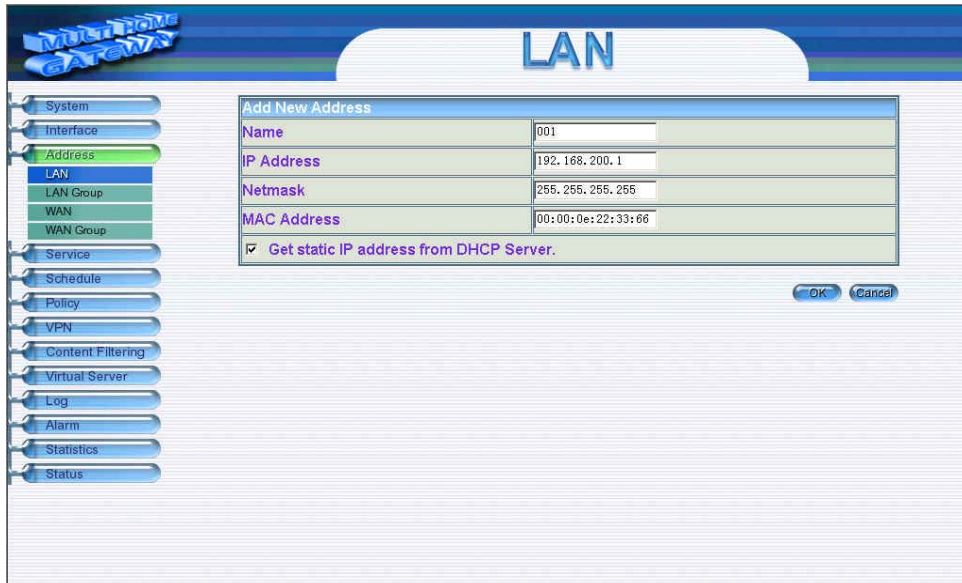


## Adding a new LAN Address

**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.



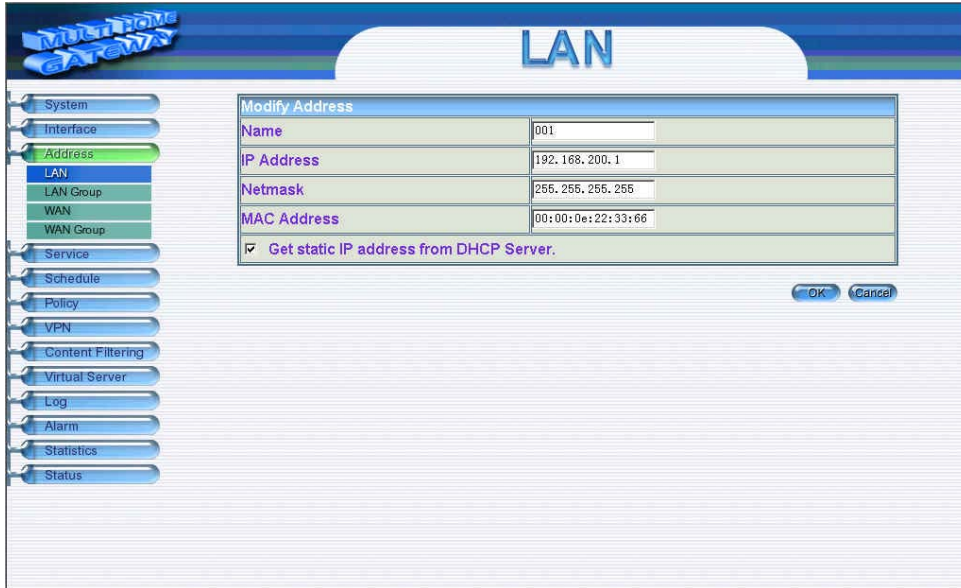
The screenshot displays the LAN configuration interface. On the left is a vertical navigation menu with buttons for System, Interface, Address, LAN, LAN Group, WAN, WAN Group, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'LAN' button is highlighted. The main area is titled 'LAN' and contains a dialog box titled 'Add New Address'. The dialog box has the following fields and values:

Add New Address	
Name	001
IP Address	192.168.200.1
Netmask	255.255.255.255
MAC Address	00:00:0e:22:33:66
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.	

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

## 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 **Cancel** to discard changes.



The screenshot displays the LAN configuration interface. On the left is a vertical menu with options: System, Interface, Address, LAN, LAN Group, WAN, WAN Group, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'LAN' option is selected. The main area is titled 'LAN' and contains a 'Modify Address' dialog box. The dialog box has the following fields and values:

Modify Address	
Name	001
IP Address	192.168.200.1
Netmask	255.255.255.255
MAC Address	00:00:0e:22:33:66
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.	

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

## Removing an 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.



# LAN Group

## Entering the LAN Group window

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

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.



## Adding an LAN Group

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

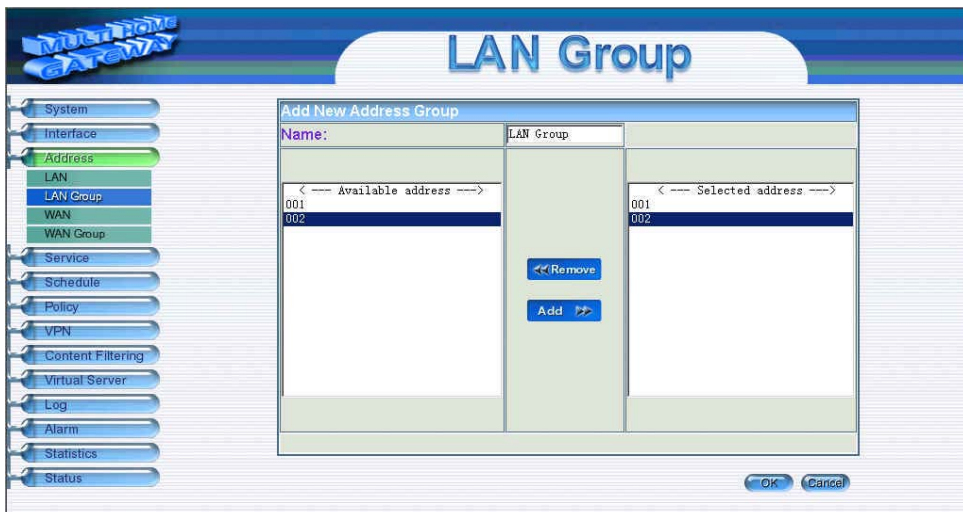
**Step 2.** In the **Add New Address Group** window:

- **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.

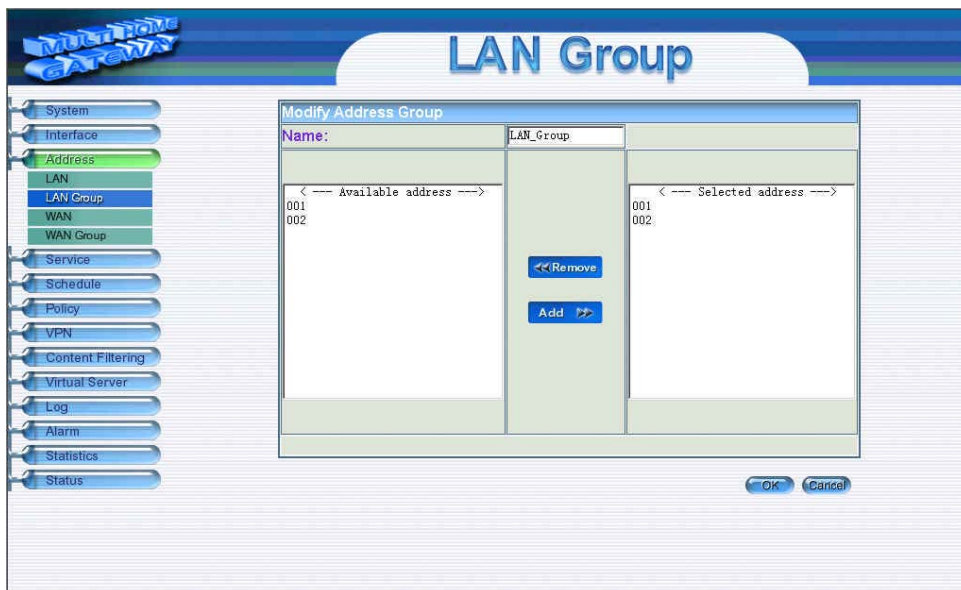
**Step 5.** Click **OK** to add the new group or click **Cancel** to discard changes.





## Modifying an 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.
- Step 5.** Click **OK** to save changes or click **Cancel** to discard changes.



## Removing an 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.



# WAN

## Entering the WAN window

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.

The screenshot shows a web-based configuration interface for WAN settings. On the left is a vertical navigation menu with buttons for System, Interface, Address, LAN, LAN Group, WAN, WAN Group, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'Address' menu is expanded, and 'WAN' is selected. The main content area is titled 'WAN' and contains a table with the following data:

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use

Below the table is a 'New Entry' button.

## 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.



# WAN Group

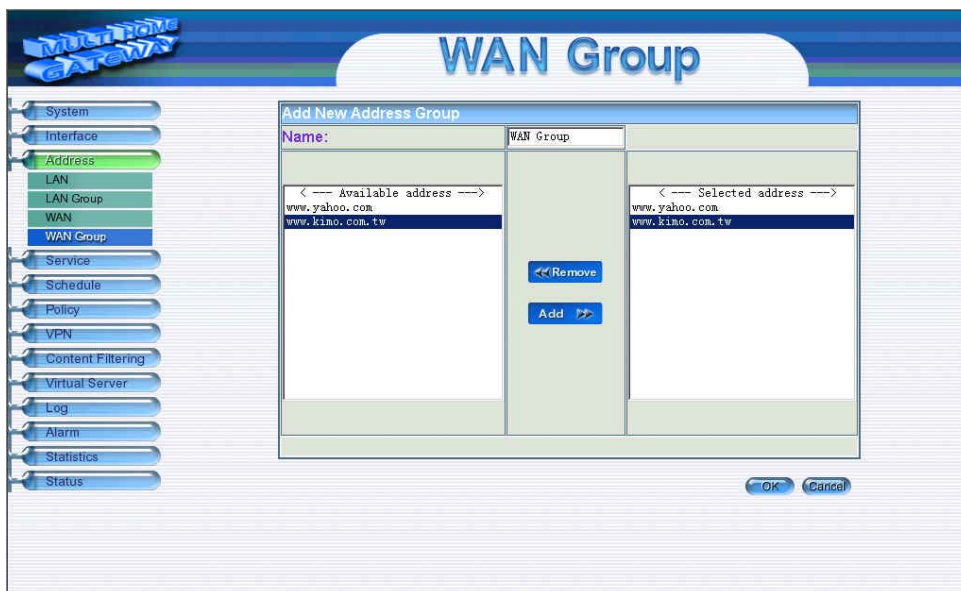
## Entering the WAN Group window

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.



## 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.
- 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 add the new group or click **Cancel** to discard changes.





## Editing an 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 an 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.



# 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 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router 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.

# Pre-defined

## Entering a Pre-defined window

Click **Service** on the menu bar on the left side of the window. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.

Protocol	Service Name	Count
ANY	ANY (Any)	
TCP	IMAP	(143)
TCP	POP3	(110)
TCP	TELNET	(23)
TCP	AFFoverTCP	(548)
TCP	InterLocator	(389)
TCP	PPTP	(1723)
UDP	IFIP	(69)
TCP	AOL	(5190-5194)
TCP	IRC	(6660-6669)
TCP	Real-Media	(7070)
ICMP	Traceroute	(3,11)
TCP	BCP	(179)
TCP	L2TP	(1701)
UDP	RIP	(520)
UDP	UDP-ANY	(Any)
UDP	DNS	(53)
TCP	LDAP	(389)
TCP	RLOGIN	(513)
UDP	URCP	(540)
TCP	FINGER	(79)
TCP	NetMeeting	(1503&1702)
TCP	SMTP	(25)
TCP	VDO-Live	(7000-7010)
TCP	FTP	(20-21)
UDP	NFS	(111)
UDP	SNMP	(161)
TCP	WAIS	(210)
TCP	GOPHER	(70)
TCP	NNTP	(119)
TCP	SSH	(22)
TCP	WINFRAME	(1494)
TCP	HTTP	(80)
UDP	NTP	(123)
UDP	SYSLOG	(514)
TCP	X-Windows	(6000-6063)
TCP	HTTPS	(443)
UDP	PC-Anywhere	(5631-5632)
UDP	TALK	(517-518)
TCP	MSN	(1863)
UDP	IKE	(500)
ICMP	PING	(Any)
TCP	TCP-ANY	(Any)

# Custom

## Entering the Custom window

Click **Service** on the menu bar on the left side of the window. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	4661:4665	4661:4665	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

## Adding a new Service

**Step 1** In the **Custom** window, click the **New Entry** button and a new service table appears.



**Step 2** 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 3** Click **OK** to add new services, or click **Cancel** to cancel.

## Modifying Custom Services

**Step 1.** In the **Custom** table, locate the name of the service to be modified. Click its corresponding **Modify** option in the **Configure** field.

**Step 2.** A table showing the current settings of the selected service appears on the screen

**Step 3.** Enter the new values.

**Step 4.** Click **OK** to accept editing; or click **Cancel**.

**Modify User Define Service**

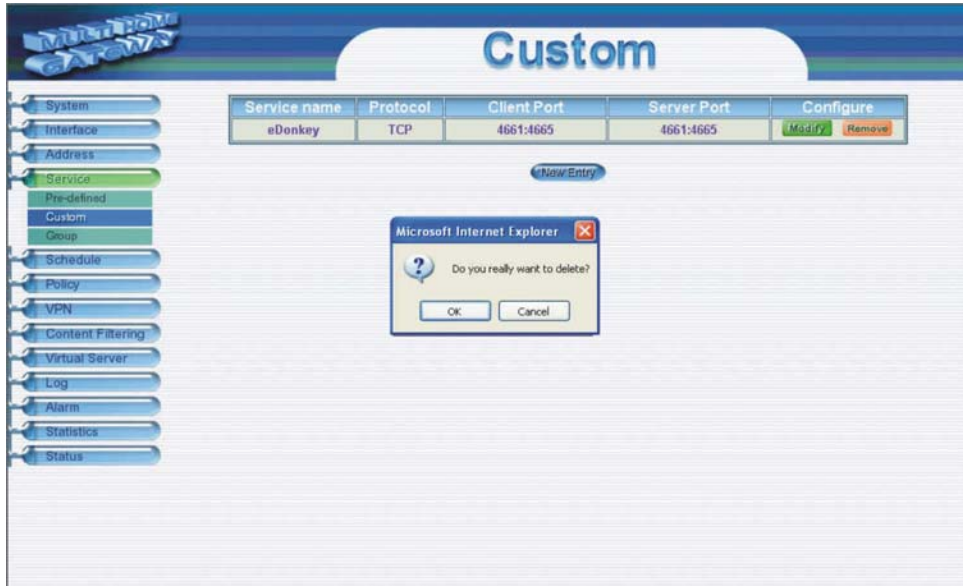
Service NAME : sDonkey

#	Protocol	Client Port	Server Port
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	4661 : 4665	4661 : 4665
2	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other	4661 : 4665	4661 : 4665
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
4	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
5	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
6	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
7	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
8	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0

OK Cancel

## Removing Custom Services

- Step 1.** In the **Custom** window, locate the service to be removed. 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.





# Group

## Accessing the Group window

Click **Service** in the menu bar on the left hand side of the window. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.

The screenshot shows a web-based configuration interface. On the left is a vertical menu with items: System, Interface, Address, Service (highlighted in green), Pre-defined, Custom, Group (highlighted in blue), Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The main area is titled "Group" and contains a table with the following data:

Group name	Service	Configure
Service_Group	AFPOverTCP,AOL,BGP...	<a href="#">Modify</a> <a href="#">Remove</a>

Below the table is a "New Entry" button.

## Adding Service Groups

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

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

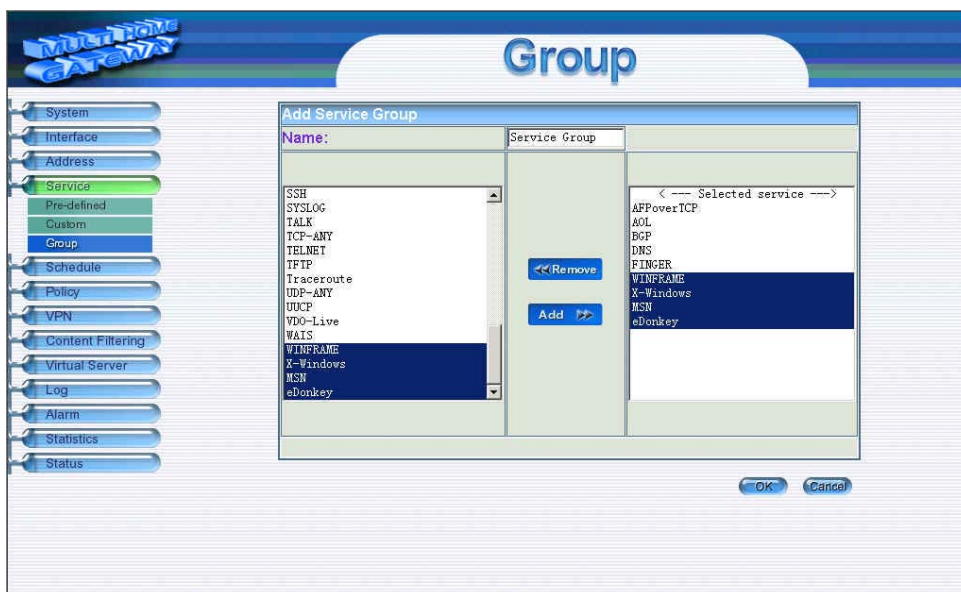
- **Available Services:** list all the available services.
- **Selected Services:** list services to be assigned to the new group.

**Step 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 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.

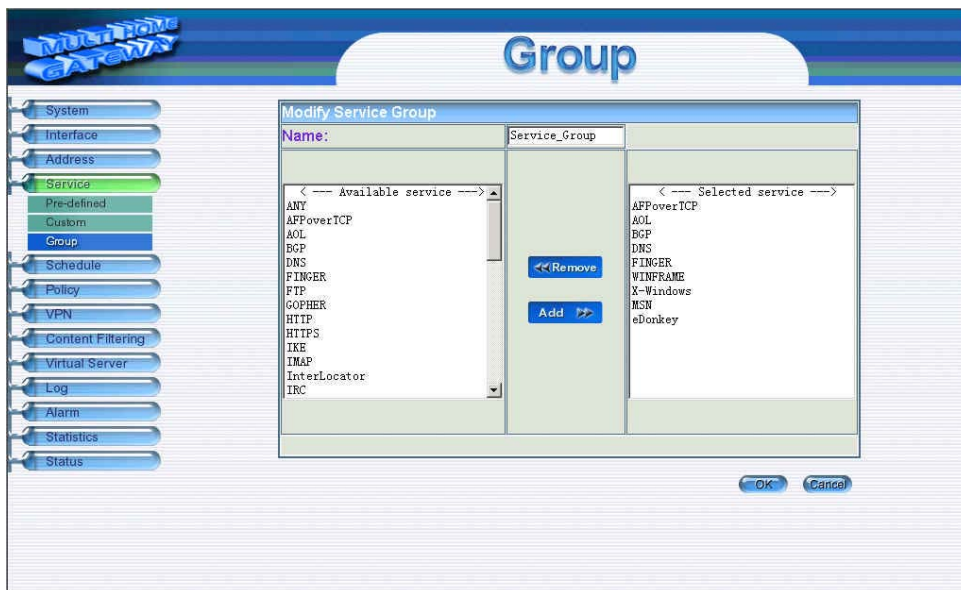
**Step 5. To remove services:** Select services desired to be removed in the **Available Services**, and then click the **<<Remove** button to remove them from the group.

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



## Modifying Service Groups

- Step 1.** In the **Group** window, locate the service group to be edited. Click its corresponding **Modify** option in the **Configure** field.
- Step 2.** 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 3.** **Add new services:** Select services in the **Available Services** list, and then click the **Add>>** button to add them to the group.
- Step 4.** **Remove services:** Select services to be removed in the **Selected Services** list, and then click the **<<Remove** button to remove these services from the group.
- Step 5.** Click **OK** to save editing changes.



## Removing Service Groups

- Step 1.** In the **Group** window, locate the service 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.

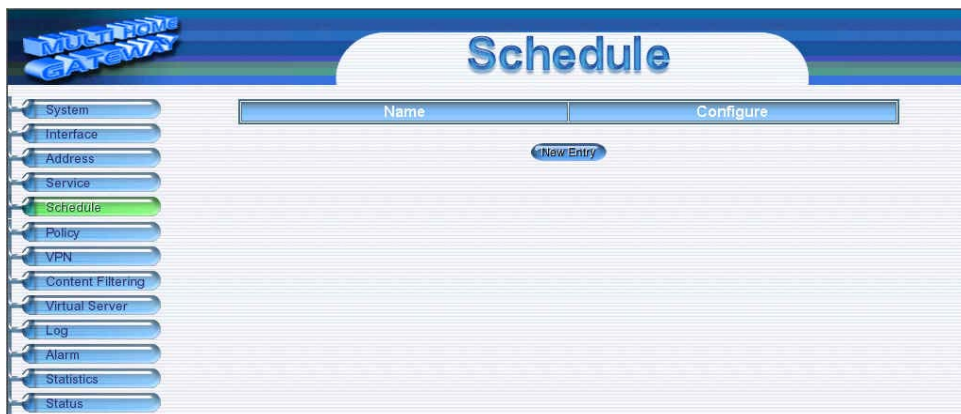


# Schedule

The 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Multi-Homing policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Multi-Homing policies therefore will likely not be permitted to pass through the Multi-Homing. 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 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 to work Monday-Friday, 8AM-5PM only. During the non-work hours, the Multi-Homing will not allow Internet access.

## Accessing the Schedule window

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.

### Step 2:

**Schedule Name:** Fill in a name for the new schedule.

**Period 1:** Configure the start and stop time for the days of the week that the schedule will be active.

**Step 3:** Click Ok to save the new schedule or click Cancel to cancel adding the new schedule.

Week Day	Period	
	Start Time	Stop Time
Monday	All day	All day
Tuesday	00:00	03:30
Wednesday	All day	All day
Thursday	Disable	Disable
Friday	All day	All day
Saturday	All day	All day
Sunday	Disable	Disable

## 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.

**Step 2:** Make needed changes.

**Step 3:** Click **OK** to save changes.

**Schedule**

Modify Schedule

Schedule Name: test

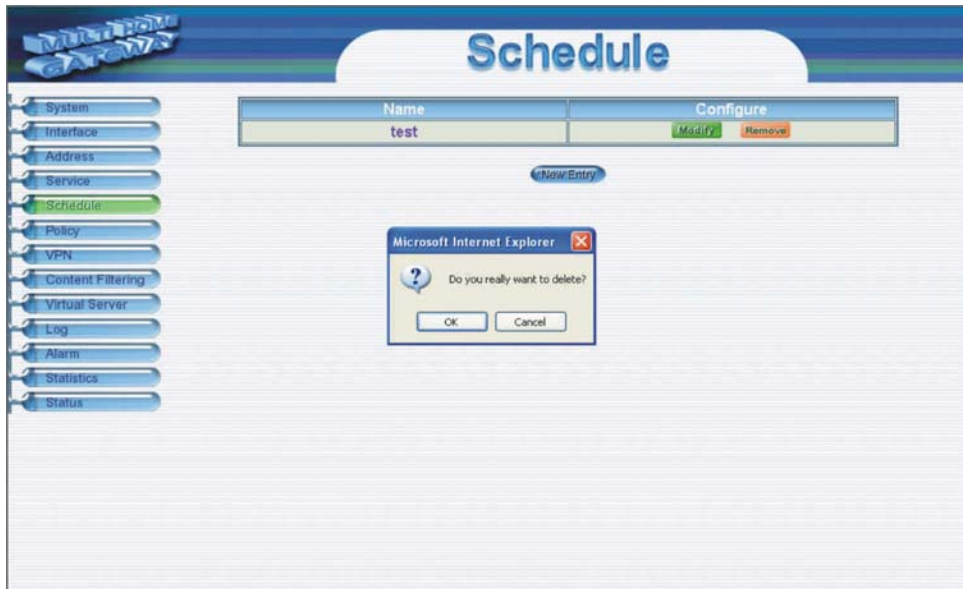
Week Day	Period	
	Start Time	Stop Time
Monday	All day	All day
Tuesday	00:00	03:30
Wednesday	All day	All day
Thursday	Disable	Disable
Friday	All day	All day
Saturday	All day	All day
Sunday	Disable	Disable

OK Cancel

## 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.





# 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.

## 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.

## 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:

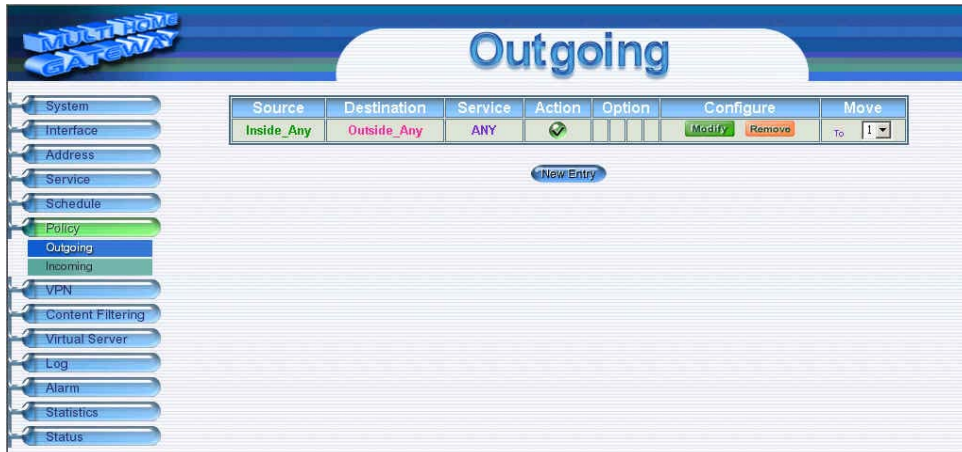
- Step 1.** In **Address**, set names and addresses of source networks and destination networks.
- Step 2.** In **Service**, set services.
- Step 3.** In **Virtual Server**, set names and addresses of mapped IP or virtual server (only applied to **Incoming policies**).
- Step 4.** Set control policies in **Policy**

## 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 reject/deny packets from LAN networks to WAN 1/2 network travelling through the Multi-Homing.
- **Option:** specify the monitoring functions on packets from LAN networks to WAN 1/2 networks travelling through the Multi-Homing.
- **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.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT, ALL
Logging	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec

### Step 2:

**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 network 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.

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

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

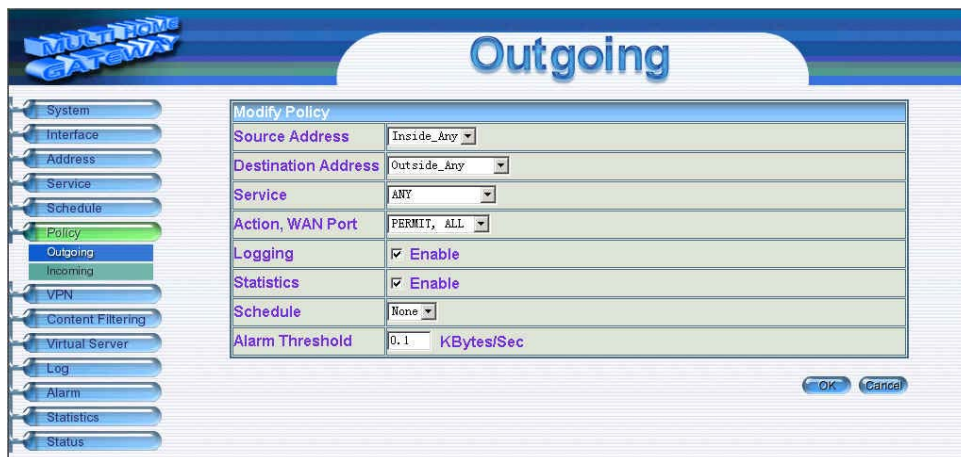
## Modifying an Outgoing policy

**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 1 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.



The screenshot shows a network management interface with a sidebar on the left containing menu items: System, Interface, Address, Service, Schedule, Policy, Outgoing, Incoming, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'Outgoing' menu item is highlighted. The main area displays the 'Outgoing' policy configuration window, which includes a 'Modify Policy' dialog box. The dialog box contains the following fields and values:

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT, ALL
Logging	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.1 KBytes/Sec

At the bottom right of the dialog box, there are two buttons: 'OK' and 'Cancel'.

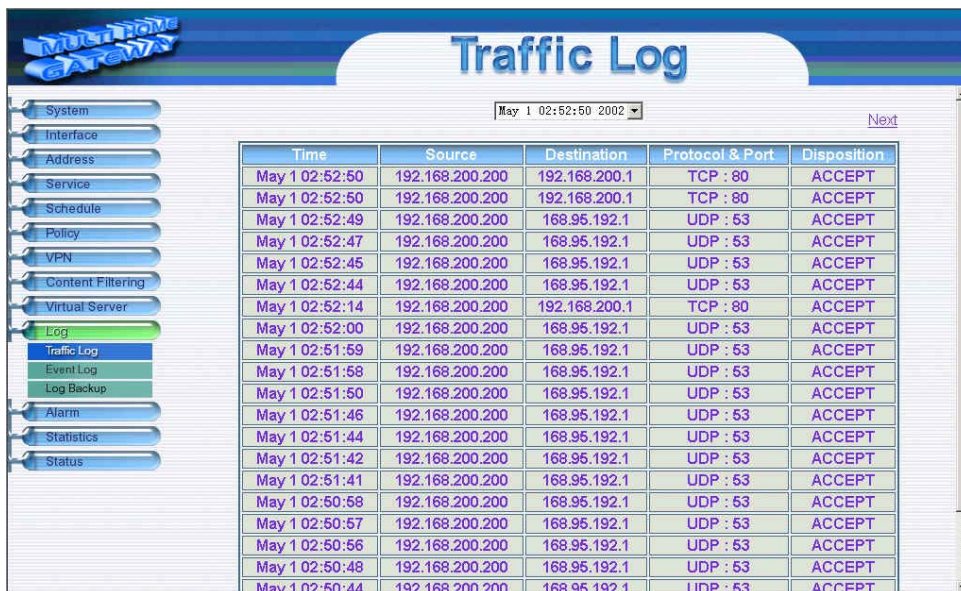
## Removing the Outgoing Policy

- 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 DUAL WAN FIREWALL ROUTER will log the traffic and event passing through the Multi-Homing. The Administrator can click **Log** on the left menu bar to get the flow and event logs of the specified policy.



The screenshot displays the 'Traffic Log' window. On the left is a vertical menu with options: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log (highlighted in green), Traffic Log (highlighted in blue), Event Log, Log Backup, Alarm, Statistics, and Status. The main area shows a table of traffic logs for May 1, 2002, at 02:52:50. The table has five columns: Time, Source, Destination, Protocol & Port, and Disposition. The data shows multiple entries of traffic from 192.168.200.200 to 192.168.200.1 (TCP:80) and 168.95.192.1 (UDP:53), all with a disposition of 'ACCEPT'. A 'Next' link is visible in the top right corner of the table area.

Time	Source	Destination	Protocol & Port	Disposition
May 1 02:52:50	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 02:52:50	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 02:52:49	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:52:47	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:52:45	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:52:44	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:52:14	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 02:52:00	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:59	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:58	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:50	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:46	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:44	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:42	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:51:41	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:50:58	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:50:57	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:50:56	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:50:48	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT
May 1 02:50:44	192.168.200.200	168.95.192.1	UDP : 53	ACCEPT

**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 DUAL WAN FIREWALL ROUTER will log the traffic alarms and event alarms passing through the Multi-Homing. The Administrator can click **Alarm** on the left menu to get the logs of flow and event alarms of the specified policy.

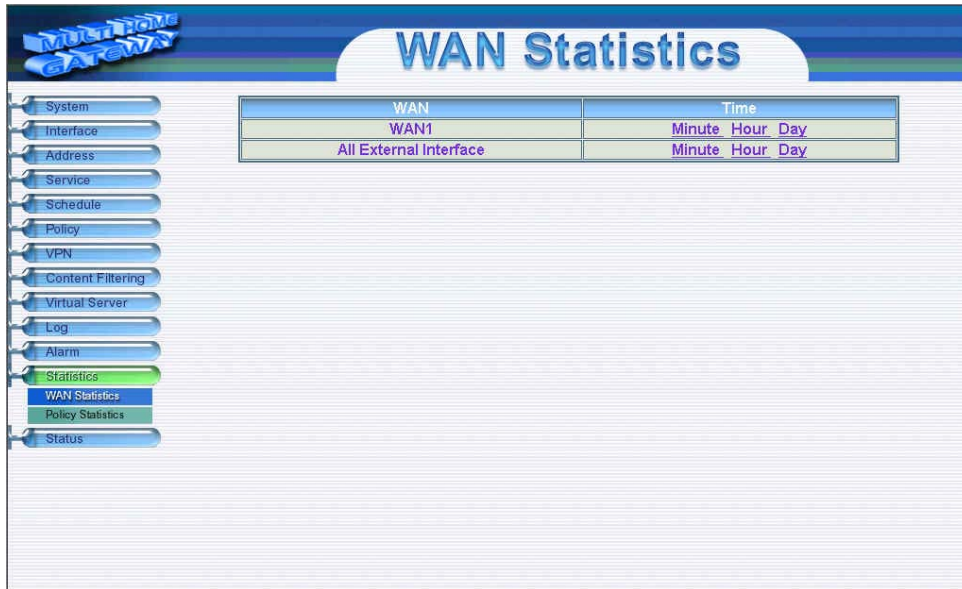
**Traffic Alarm**

Time	Source	Destination	Service	Traffic
May 1 19:00~19:15	Inside_Any	Outside_Any	ANY	0.858K/Sec
May 1 18:45~19:00	Inside_Any	Outside_Any	ANY	0.513K/Sec
May 1 18:30~18:45	Inside_Any	Outside_Any	ANY	4.515K/Sec
May 1 04:00~04:15	Inside_Any	Outside_Any	ANY	0.681K/Sec
May 1 03:45~04:00	Inside_Any	Outside_Any	ANY	1.415K/Sec
May 1 03:15~03:30	Inside_Any	Outside_Any	ANY	0.761K/Sec

Clear Logs      Download Logs

**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 DUAL WAN FIREWALL ROUTER will display the flow statistics passing through the Multi-Homing.



The screenshot displays the 'WAN Statistics' page in a 'MULTI-HOMING GATEWAY' interface. On the left is a navigation menu with items: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, WAN Statistics, Policy Statistics, and Status. The 'Statistics' item is highlighted in green, and 'WAN Statistics' is highlighted in blue. The main content area features a table with the following structure:

WAN	Time
WAN1	Minute Hour Day
All External Interface	Minute Hour Day

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

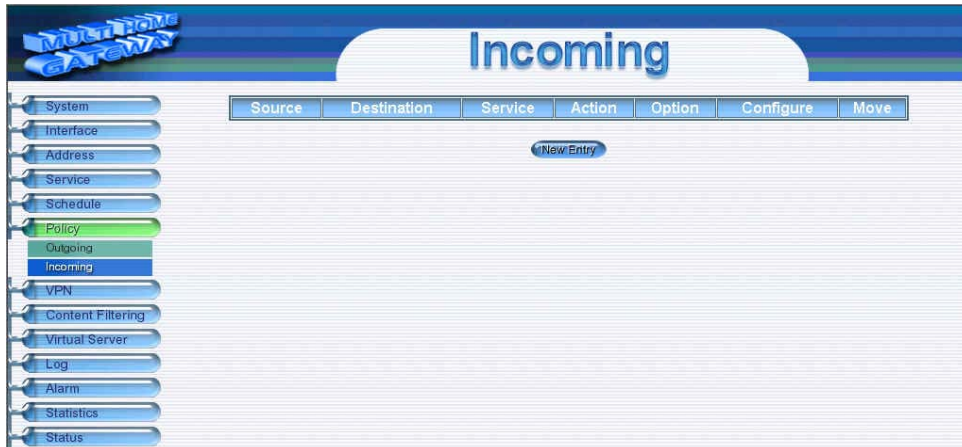


## Incoming

This chapter 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.



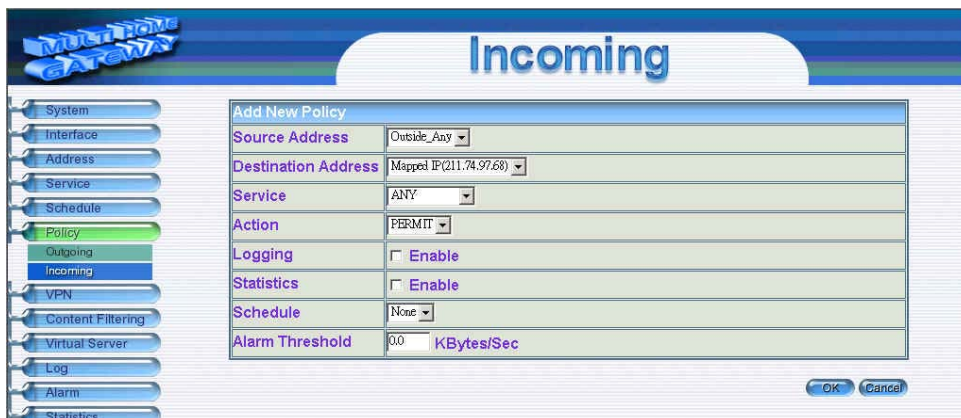
**Step 2:** The fields of the **Incoming** window are:

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

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

## Adding an Incoming Policy

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



Add New Policy	
Source Address	Outside_Any
Destination Address	Mapped IP(211.74.97.68)
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec

### Step 2:

**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.

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

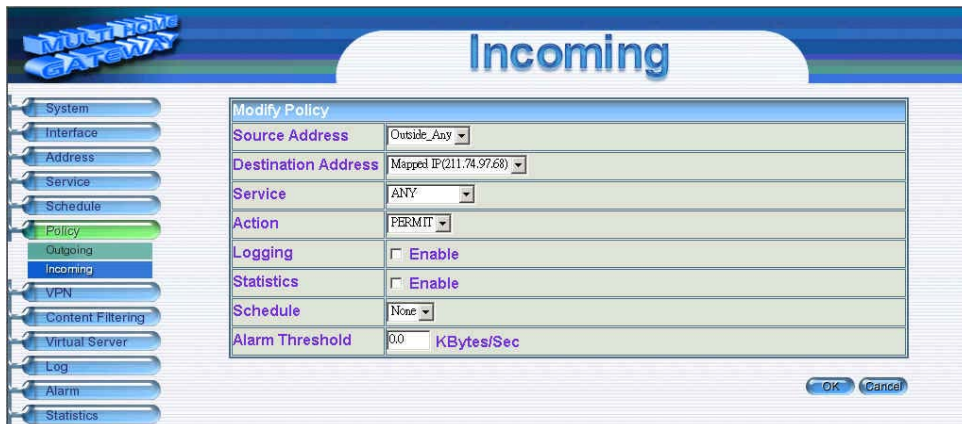
**Step 3:** Click **OK** to add new policy or click **Cancel** to cancel adding new incoming policy.

## 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.



The screenshot displays the 'Incoming' configuration window. On the left is a vertical menu with options: System, Interface, Address, Service, Schedule, Policy, Outgoing, Incoming, VPN, Content Filtering, Virtual Server, Log, Alarm, and Statistics. The 'Incoming' option is selected. The main area is titled 'Incoming' and contains a 'Modify Policy' dialog box. The dialog box has the following fields:

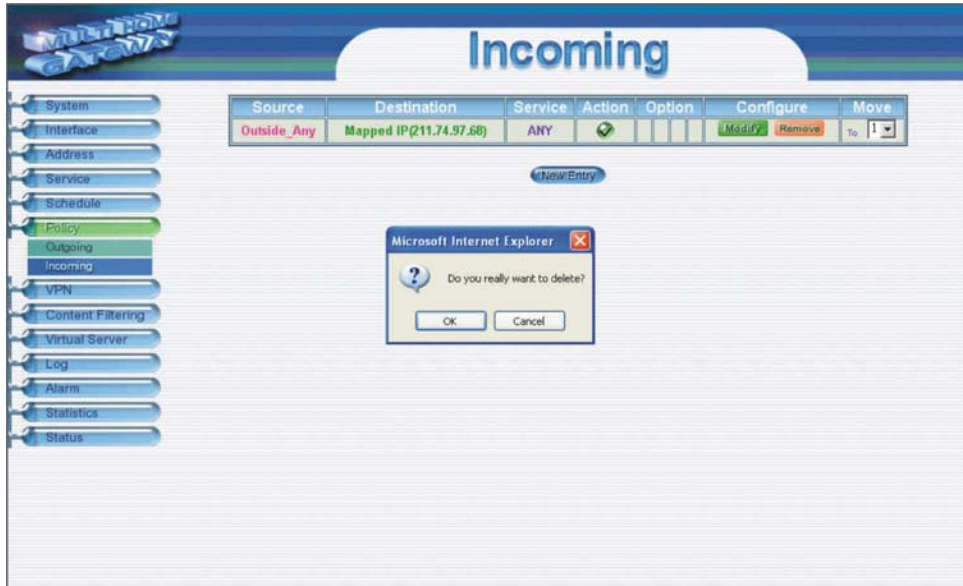
Modify Policy	
Source Address	Outside_Any
Destination Address	Mapped IP(211.74.97.68)
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	00 KBytes/Sec

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

## 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.



# VPN

The 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router's VPN (Virtual Private Network) is set by the System Administrator. The System Administrator can add, modify or remove VPN settings.

## What is VPN?

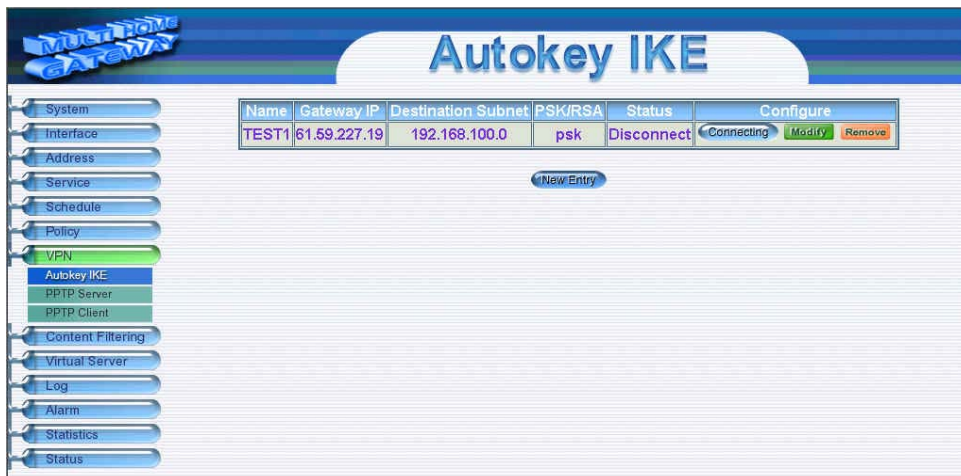
To set up a **Virtual Private Network** (VPN), you *don't need* to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet, Destination Gateway, Destination Subnet, Authentication Method, Preshare key, Encapsulation and IPSec lifetime. The Multi-Homings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

## Autokey IKE

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



The fields in the Autokey IKE 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.
- **Destination Subnet:** Destination network subnet.
- **PSK/RSA:** The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.
- **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.

The screenshot shows the 'Autokey IKE' configuration window. The left sidebar has 'Autokey IKE' selected. The main window is titled 'VPN Auto Keyed Tunnel' and contains the following configuration fields:

- Name: TEST1
- Use interface:  WAN1  WAN2
- Subnet / Mask: 192.168.200.0 / 255.255.255.0
- To Destination:
  - Remote Gateway -- Fixed IP
  - Subnet / Mask: 61.59.227.19 / 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: 123456
- Encapsulation:
  - Data Encryption + Authentication
  - Authentication Only
- Perfect Forward Secrecy
- IPsec Lifetime: 28800 Seconds
- Schedule: None

Buttons: OK, Cancel

### Step 2:

- **Preshare Key:** The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.
- **ESP/AH:** The IP level security headers, AH and ESP, were originally proposed by the Networking Group focused on IP security mechanisms, IPsec. The term IPsec is used loosely here to refer to packets, keys, and routes that are associated with these headers. The IP Authentication Header (AH) is used to provide authentication. The IP Encapsulating Security Header (ESP) is used to provide confidentiality to IP datagrams.
- **ESP-Encryption Algorithm:** The device auto-selects 56 bit DES-CBC or 168-bit Triple DES-CBC encryption algorithm. The default algorithm is 168-bit Triple DES-CBC.
- **ESP-Authentication Method:** The device auto-selects MD5 or SHA-1 authentication algorithm. The default algorithm is MD5.
- **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.

## Modifying an Autokey IKE

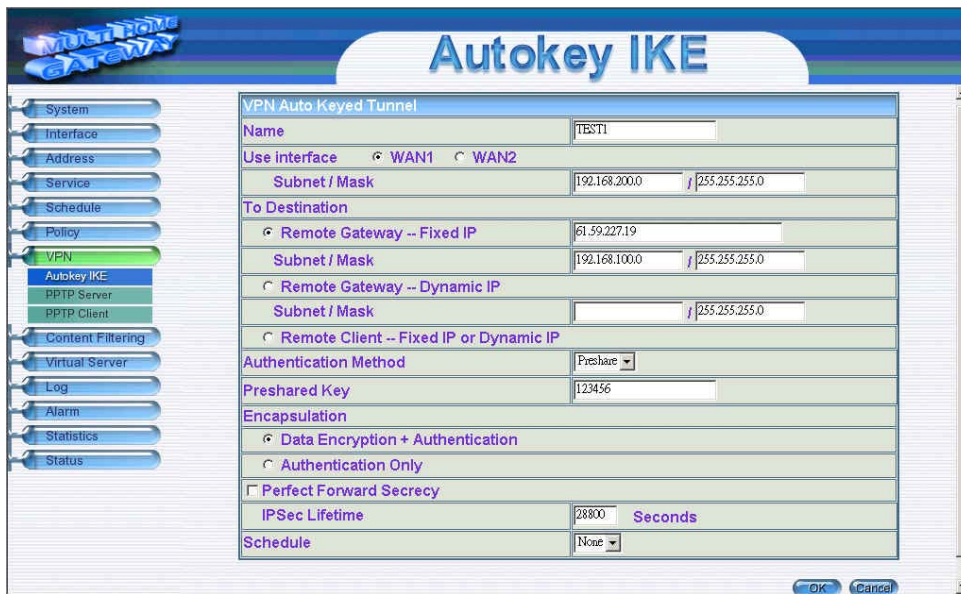
**Step 1:** In the Autokey IKE window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

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

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

### Connecting the VPN connection:

Once all the policy is created with the correct settings, click on the **Connect** option in the **Configure** field. The **Status** field will change to indicate Connecting. If the remote Multi-Homing is set up correctly with the VPN active, the VPN connection will be made between the two Multi-Homings and the Status field will change to Connect.



The screenshot shows the 'Autokey IKE' configuration window. On the left is a navigation menu with options: System, Interface, Address, Service, Schedule, Policy, VPN, Autokey IKE (highlighted), PPTP Server, PPTP Client, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The main area is titled 'VPN Auto Keyed Tunnel' and contains the following fields:

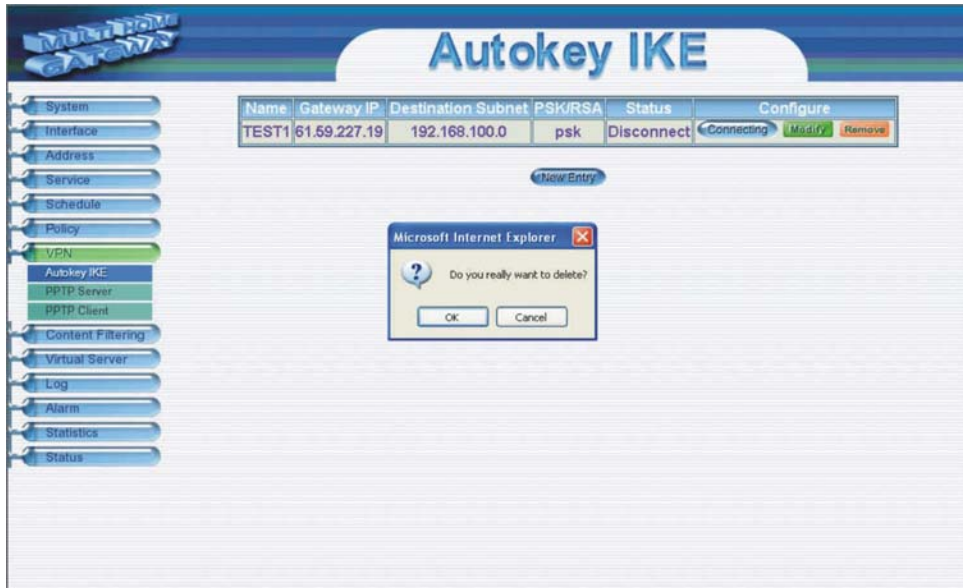
Name	TEST1
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.200.0 / 255.255.255.0
To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	61.59.227.19
Subnet / Mask	192.168.100.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	
Authentication Method	Preshare
Preshared Key	123456
Encapsulation	
<input checked="" type="radio"/> Data Encryption + Authentication	
<input type="radio"/> Authentication Only	
<input type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Schedule	None

At the bottom right, there are 'OK' and 'Cancel' buttons.



## Removing Autokey IKE

- Step 1.** Locate the name of the Autokey IKE desired to be removed and click its corresponding Delete option in the Configure field.
- Step 2.** In the Remove confirmation pop-up box, click **OK** to remove the Autokey IKE or click **Cancel** to cancel deleting.



# PPTP Server

## Entering the PPTP Server window

**Step 1.** Select VPN→PPTP Server.

PPTP Server ( Enable, Encryption:OFF ) :

Client IP Range : 192.132.35.1-254 [Modify](#)

User Name	Client IP	Uptime	Status	Configure
test	0.0.0.0	---	Disconnect	<a href="#">Modify</a> <a href="#">Remove</a>

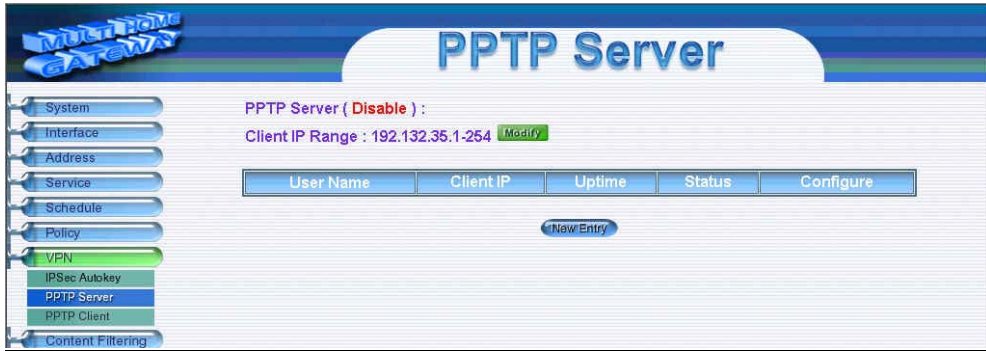
[New Entry](#)

- **PPTP Server** : Click **Modify** to select Enable or Disable.
- **Client IP Range**: **192.26.145.1-254** : 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.

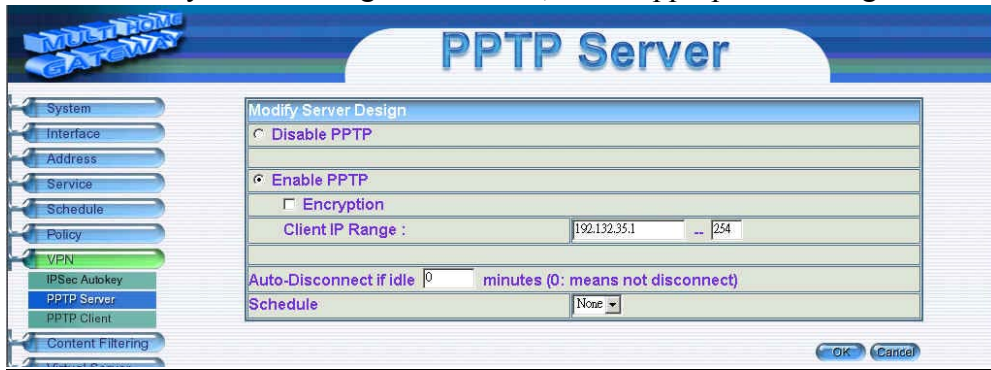
# Modifying PPTP Server Design

**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.



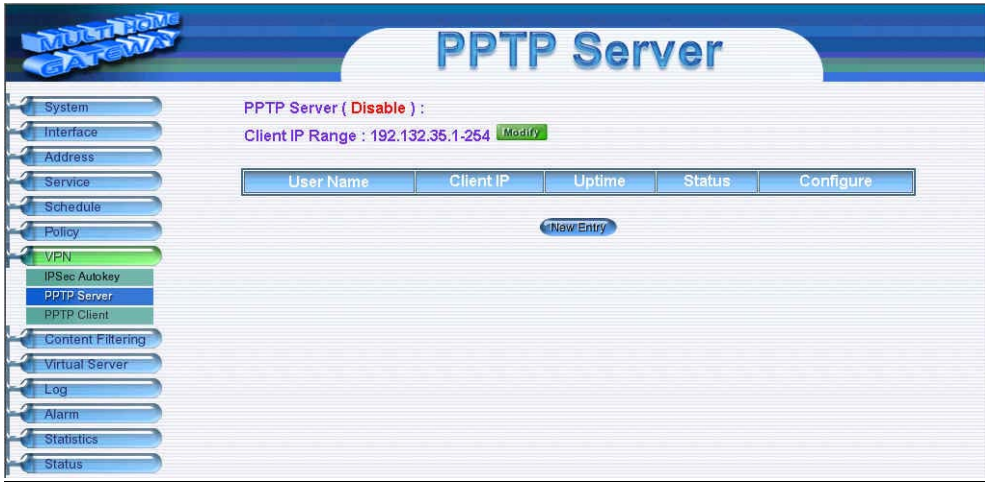
### Modify Server Design

- **Disable PPTP** : Check to disable PPTP Server.
- **Enable PPTP** : Check to enable PPTP Server.
  1. Encryption: the default is set to disabled.
  2. Client IP Range : Enter the IP range allocated for PPTP Client to 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

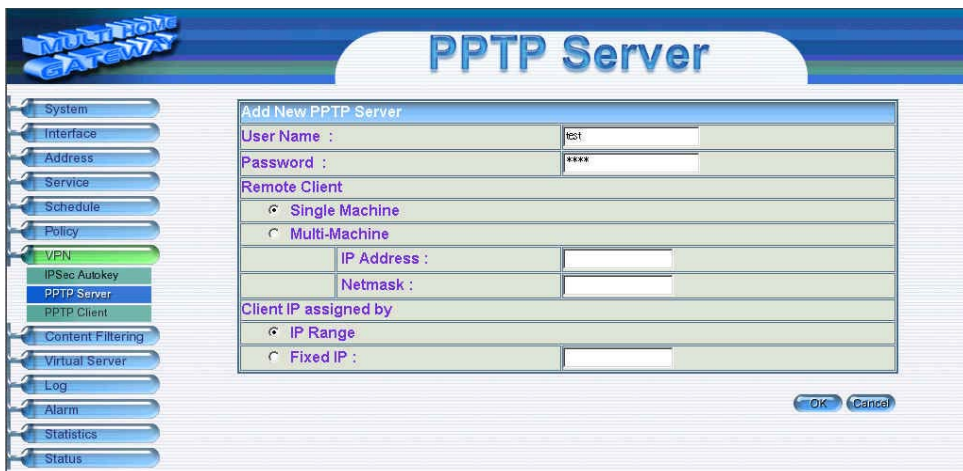
# Adding PPTP Server

**Step 1.** Select VPN→PPTP Server. Click NewEntry.



**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 Sub net 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.



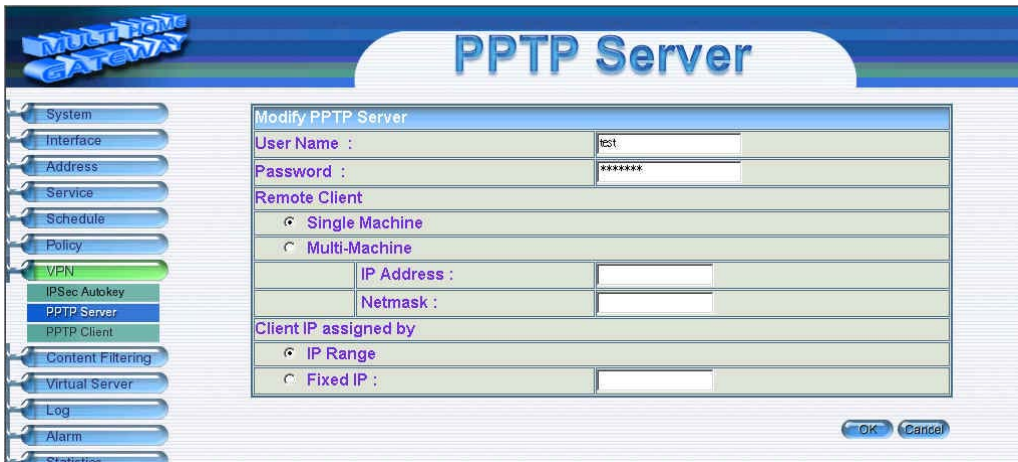
**Step 3.** Click **OK** to save modifications or click **Cancel** to cancel modifications

## 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.



The screenshot shows a web-based configuration interface for a PPTP Server. On the left is a vertical navigation menu with buttons for System, Interface, Address, Service, Schedule, Policy, VPN, IPSec Autokey, PPTP Server, PPTP Client, Content Filtering, Virtual Server, Log, Alarm, and Statistics. The 'PPTP Server' button is highlighted in blue. The main content area is titled 'PPTP Server' and contains a 'Modify PPTP Server' form. The form has the following fields and options:

- User Name :** A text input field containing 'test'.
- Password :** A text input field containing '\*\*\*\*\*'.
- Remote Client:** A section with two radio button options:
  - Single Machine
  - Multi-Machine
- IP Address :** A text input field.
- Netmask :** A text input field.
- Client IP assigned by:** A section with two radio button options:
  - IP Range
  - Fixed IP : [text input field]

At the bottom right of the form are two buttons: 'OK' and 'Cancel'.

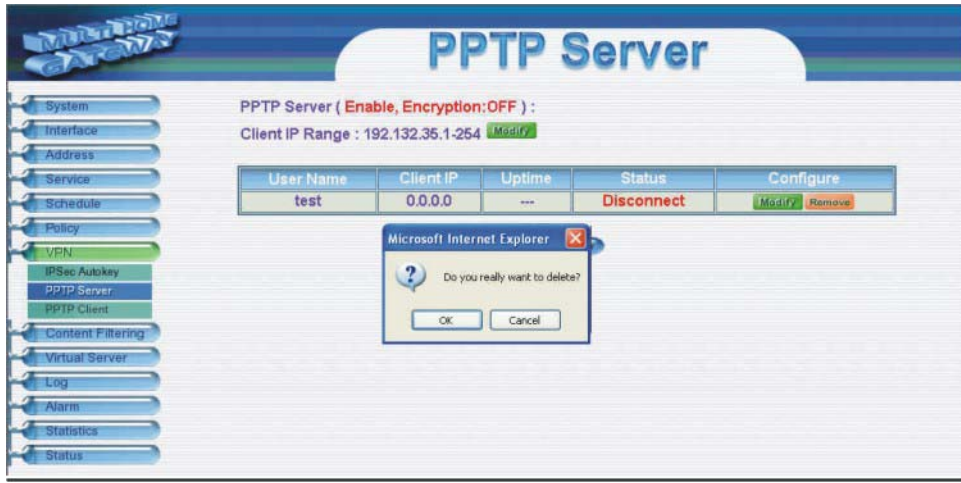
**Step 4.** Click **OK** to save modifications or click **Cancel** to cancel modifications

## Removing PPTP Server

**Step 1.** Select VPN→PPTP Server.

**Step 2.** In the **【PPTP Server】** window, find the PPTP server that you want to modify. Click **【Configure】** and click **【remove】** .

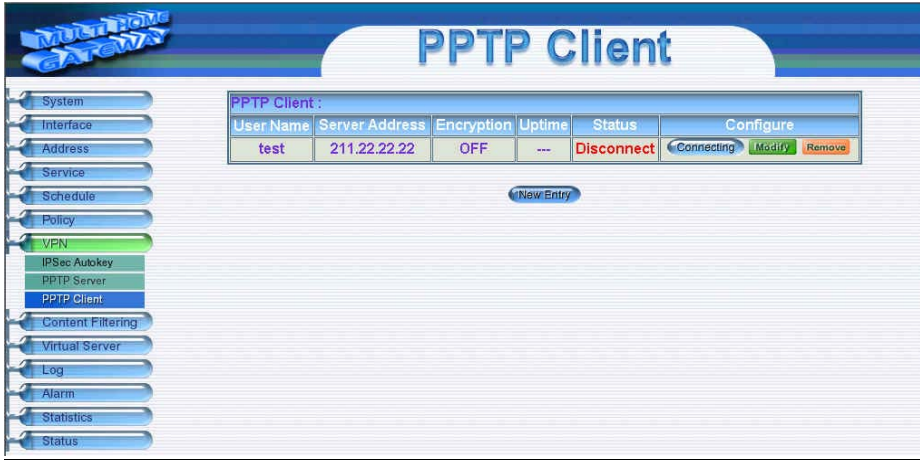
**Step 3.** Click **OK** to remove the PPTP server or click **Cancel** to exit without removal.



# PPTP Client

## Entering the PPTP Client window

**Step 1.** Select VPN→PPTP Client.



- **Server Address** : Display the PPTP Server IP addresses..
- **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.

## Adding a PPTP Client

### Step 1. Select VPN→PPTP Client.

- 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.
  - 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 Sub net mask.

The screenshot shows a web-based configuration interface for a PPTP Client. The main window is titled "PPTP Client" and contains a form titled "Add New PPTP Client". The form has the following fields and options:

- User Name :** A text input field containing "test".
- Password :** A text input field with masked characters "\*\*\*\*".
- Server Address :** A text input field containing "211.22.22.22" and a checkbox for "Encryption".
- Remote Server:** Radio buttons for "Single Machine" (selected) and "Multi-Machine".
- IP Address :** A text input field.
- Netmask :** A text input field.
- Auto-Connect when sending packet through the link:** A checkbox that is currently unchecked.
- Auto-Disconnect if idle:** A text input field containing "0" followed by "minutes (0: means not disconnect)".
- Schedule:** A dropdown menu currently set to "None".

At the bottom right of the form are "OK" and "Cancel" buttons. On the left side of the interface is a sidebar menu with various configuration options, including "VPN" which is highlighted in green.

- **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 4. Click **OK** to save modifications or click **Cancel** to cancel modifications.

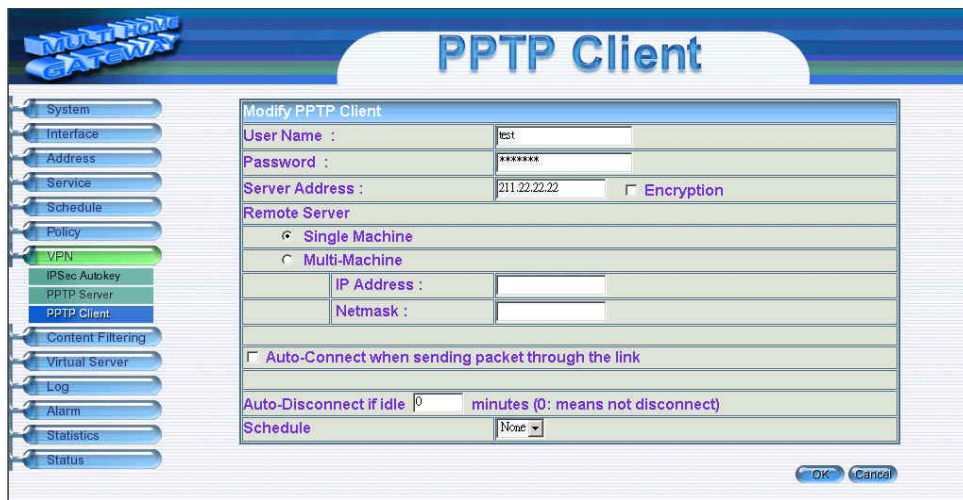


## Modifying PPTP Client

**Step 1.** Select VPN→PPTP Client.

**Step 2.** In the 【PPTP Client】 window, find the PPTP server that you want to modify. Click 【Configure】 and click 【Modify】 .

**Step 3.** Enter appropriate settings.



The screenshot shows the 'PPTP Client' configuration window. On the left is a navigation menu with items: System, Interface, Address, Service, Schedule, Policy, VPN, IPsec Autokey, PPTP Server, PPTP Client, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'PPTP Client' item is selected. The main area displays the 'Modify PPTP Client' dialog box with the following fields and options:

- User Name : test
- Password : \*\*\*\*\*
- Server Address : 211.22.22.22  Encryption
- Remote Server
  - Single Machine
  - Multi-Machine
- IP Address : [empty field]
- Netmask : [empty field]
- Auto-Connect when sending packet through the link
- Auto-Disconnect if idle 0 minutes (0: means not disconnect)
- Schedule None

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

**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. Click **【Configure】** and click **【remove】** .

**Step 3.** Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.



# Content filtering

Content filtering includes URL Blocking and general filtering. Content Filtering includes 「**URL Blocking**」 and 「**General Blocking**」 .

- (一) **URL Blocking** : The device manager can use a complete domain name, key word, “~” or “\*” to make rules for specific websites.
- (二) **General Blocking** : To let Popup 、 ActiveX 、 Java 、 Cookie in or keep them out.

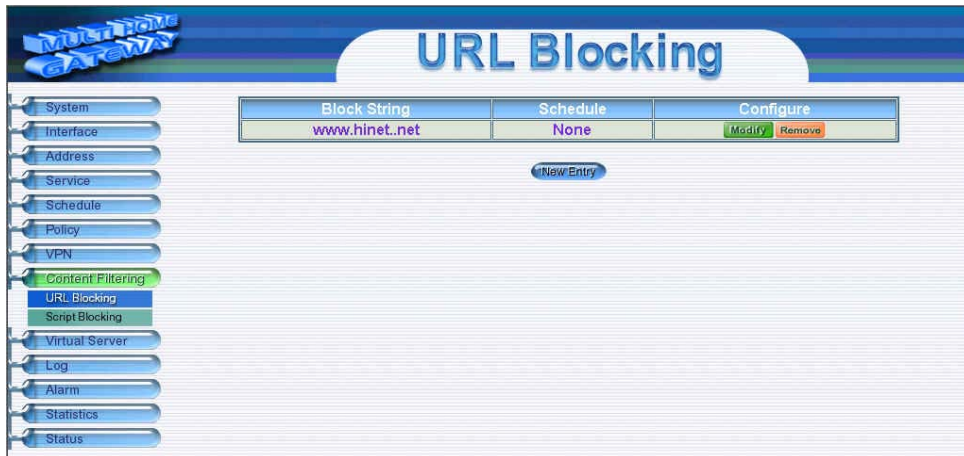
## URL Blocking

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

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

Click on **New Entry**.

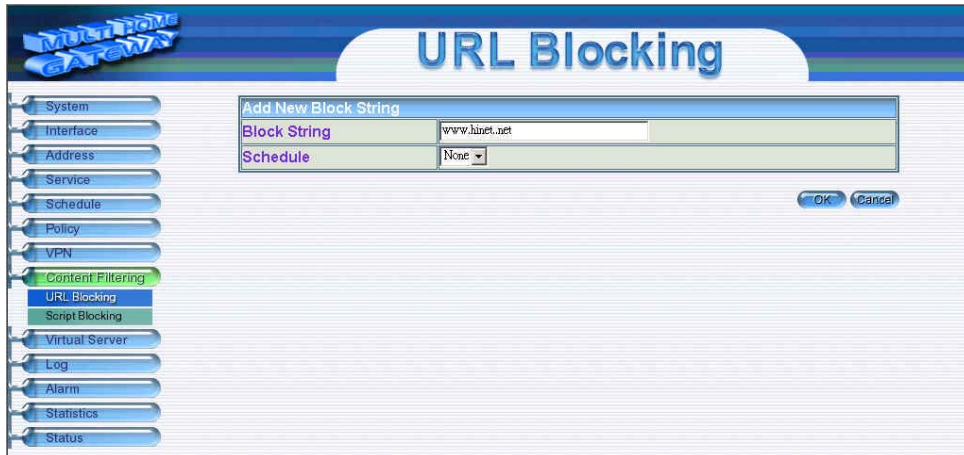


## Adding a URL Blocking policy

**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.



The screenshot shows a web-based configuration interface for a network device. The main title is "URL Blocking". On the left, there is a vertical menu with various configuration options: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, URL Blocking (highlighted in blue), Script Blocking, Virtual Server, Log, Alarm, Statistics, and Status. The "Add New Block String" dialog box is open, showing a form with the following fields:

Add New Block String	
Block String	<input type="text" value="www.linnet.net"/>
Schedule	<input type="text" value="None"/>

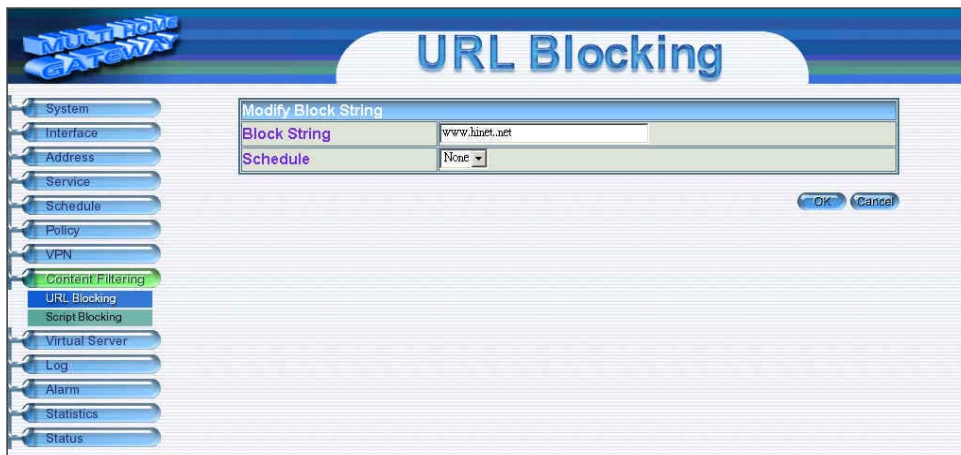
At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

## 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 cancel modifications.



## Removing a URL Blocking policy

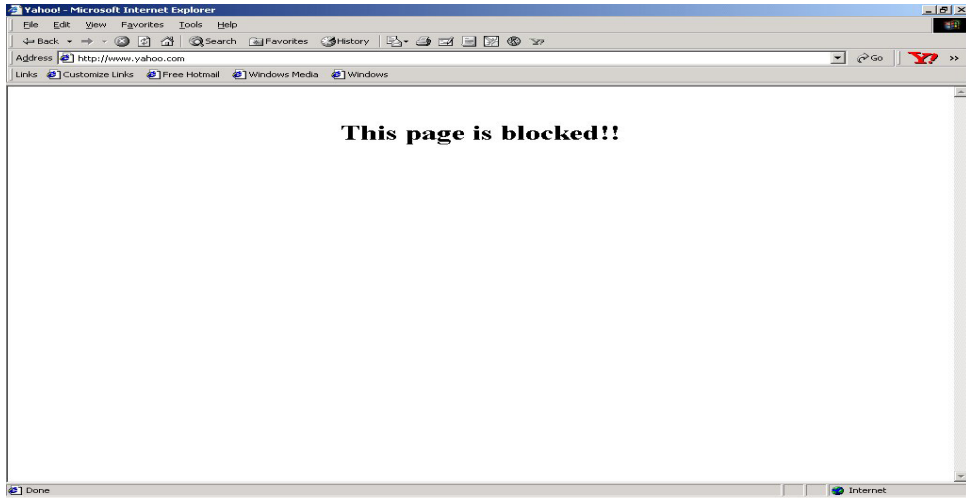
**Step 1:** In the **URL Blocking** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

**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.



## General Blocking

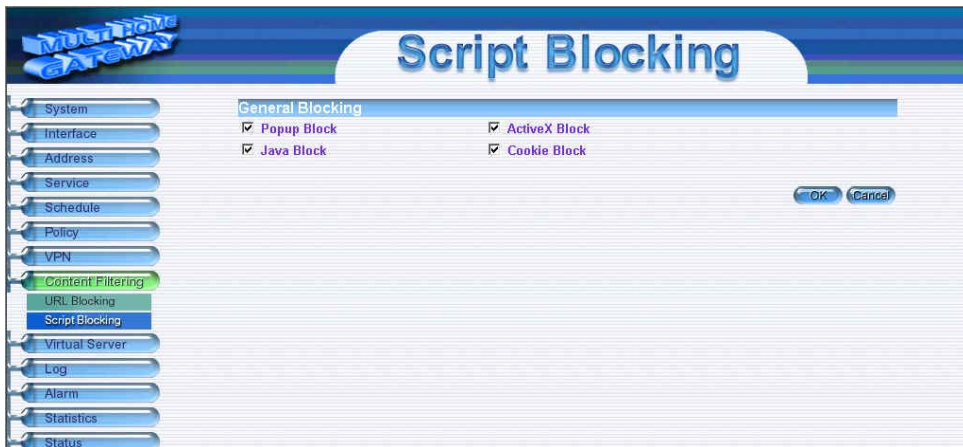
To let Popup、ActiveX、Java、Cookie in or keep them out.

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

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

- Popup filtering : Prevent the pop-up boxes 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 will spontaneously work.*



# Virtual Server

The 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router separates an enterprise's Intranet and Internet into LAN networks and WAN 1/2 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's NAT (Network Address Translation) function. If a server which provides service to the WAN 1/2 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 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router's Virtual Server can solve this problem. A virtual server has set the real IP address of the Multi-Homing's WAN 1/2 network interface to be the Virtual Server IP. Through the virtual server feature, the Multi-Homing 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 know as one-to-many mapping. This is when one virtual server IP address on the WAN 1/2 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 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 still exists 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 1/2 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.

## 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 1/2 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 1/2 IP address is mapped to one private LAN IP address.

### Entering the Mapped IP window

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

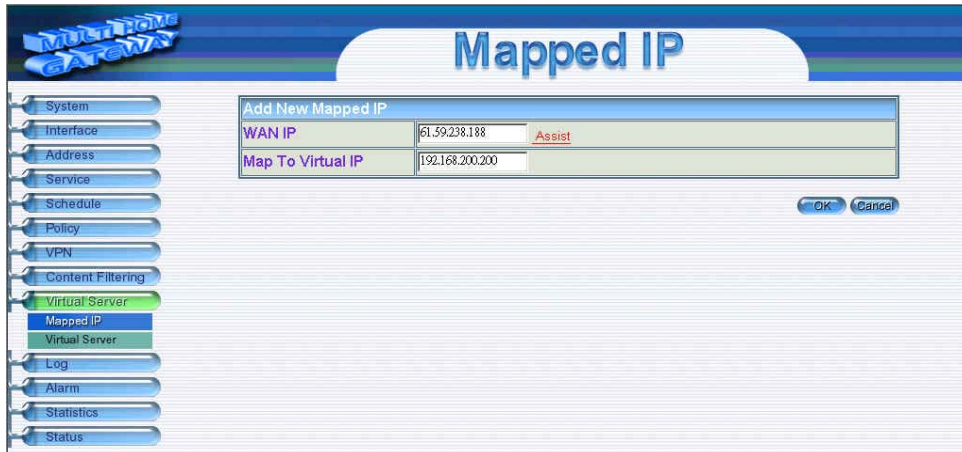


## Adding a new IP Mapping

**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 1/2 public IP address to be mapped.
- Internal IP: enter the LAN private IP address will be mapped 1-to-1 to the WAN 1/2 IP address.

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

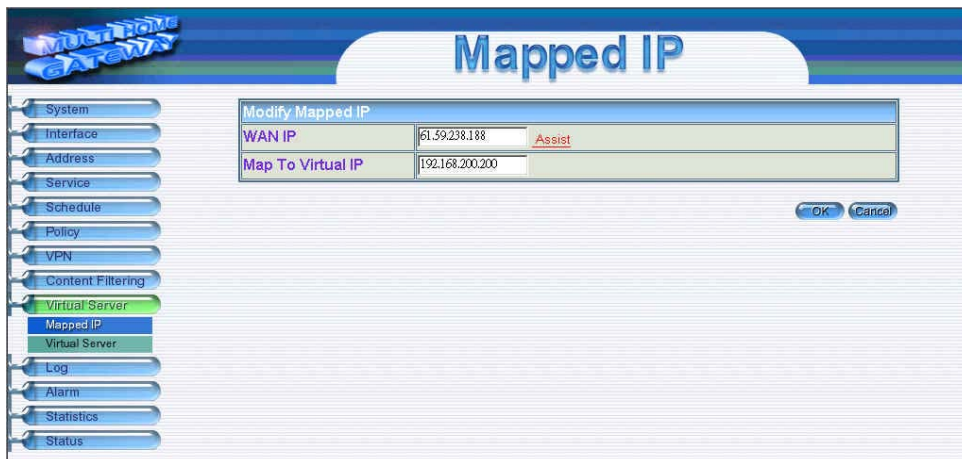


## Modifying a Mapped IP

**Step 1.** In the **Mapped IP** table, locate the Mapped IP desired 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.

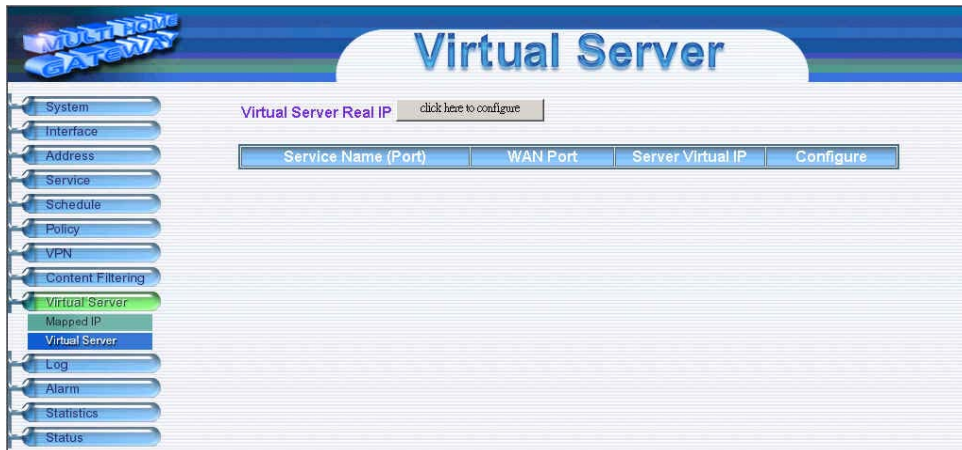


## Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN 1/2 interface to private IP addresses of the LAN network. This is done to provide services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds an WAN 1/2 IP to an LAN IP, virtual server binds WAN 1/2 IP ports to LAN IP ports.

### 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:

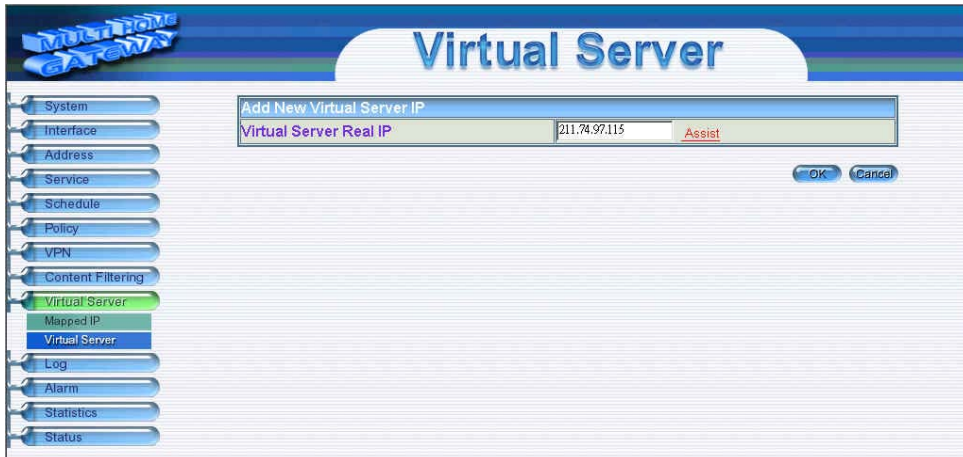


**Step 2.** Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the WAN 1 network.

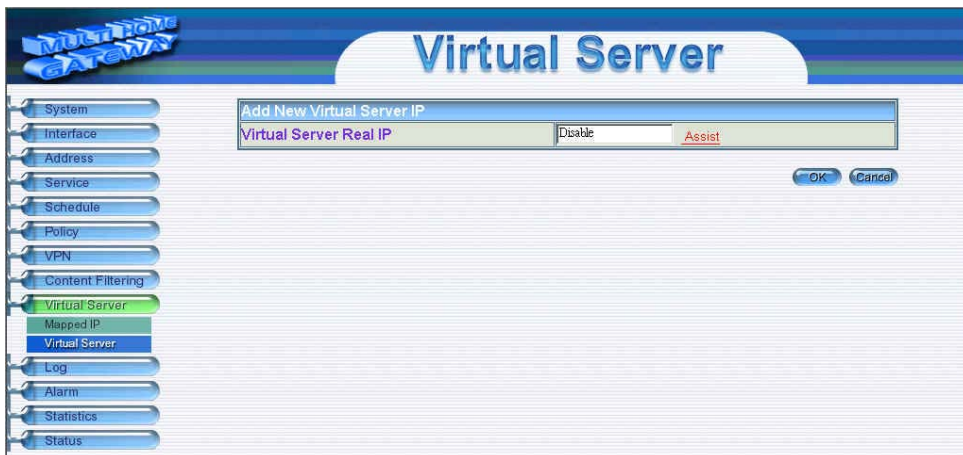
**Step 3.** Select an IP address from the drop-down list of available WAN 1/2 network IP addresses.

**Note:** *If the drop-down list contains only (Disable), there is no available IP addresses of WAN 1/2 network of the System and no Virtual Server can be added.*

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

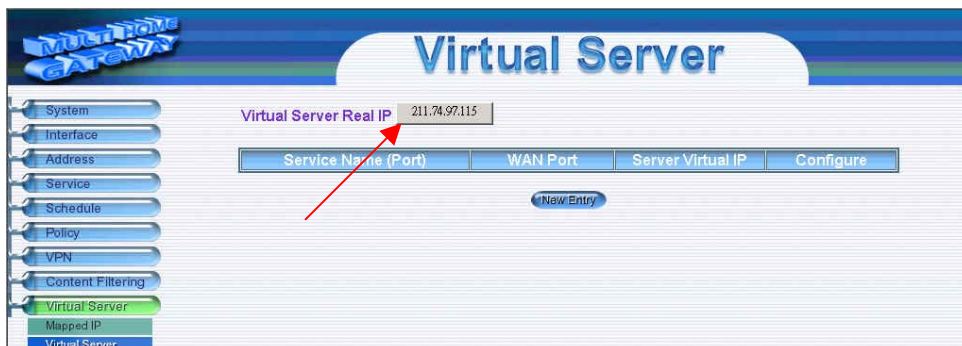


When **Disable** appears in the drop-down list, no Virtual Server can be added.



## Modifying a Virtual Server IP Address

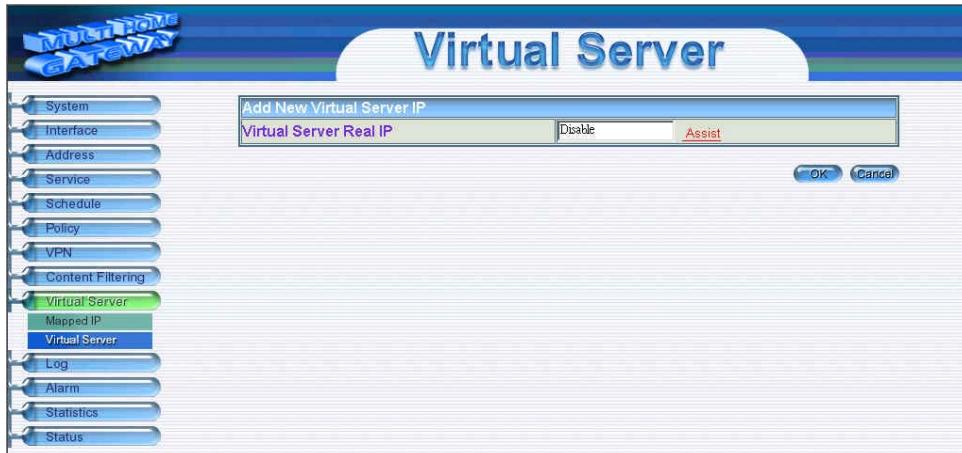
- Step 1.** Click the virtual server to be modified Virtual Server under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.
- Step 2.** Click on the Virtual Server's IP Address button at the top of the screen.
- Step 3.** Choose a new IP address from the drop-down list.
- Step 4.** Click **OK** to save new IP address or click **Cancel** to cancel modification.





## 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.** Select Disable in the drop-down list in.
- 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 IP:** displays the WAN 1/2 IP address assigned to the Virtual Server
- **External Service Port:** select the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Service:** select the service from the pull down list that will be provided by 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.*

**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.

Load Balance Server	Server Virtual IP
1	192.168.1.223
2	192.168.1.224
3	
4	

## 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 cancel modification.

Load Balance Server	Server Virtual IP	
1	192.168.1.223	
2	192.168.1.224	
3		
4		

**Note:** A virtual server cannot be modified or removed if it has been assigned to the destination address of any Incoming policies.

## 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.



# Log

The 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router 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 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router.

## What is Log?

Log records all connections that pass through the Multi-Homing'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.

## Traffic Log

The Administrator queries the Multi-Homing for information, such as source address, destination address, start time, and Protocol port, of all connections.

### Entering the Traffic Log window

Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.



The screenshot shows the 'Traffic Log' window with a sidebar menu on the left and a table of logs. The sidebar menu includes options like System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Traffic Log (highlighted), Event Log, Log Backup, Alarm, Statistics, and Status. The table displays connection details for May 1, 2019, at 19:59:40.

Time	Source	Destination	Protocol & Port	Disposition
May 1 19:59:40	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:59:32	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:58:46	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:58:17	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:57:42	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:54:55	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:54:55	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:52:53	192.168.1.106	255.255.255.255	UDP : 67	ACCEPT
May 1 19:52:45	192.168.1.106	255.255.255.255	UDP : 67	ACCEPT
May 1 19:52:37	192.168.1.106	255.255.255.255	UDP : 67	ACCEPT
May 1 19:52:29	192.168.1.106	255.255.255.255	UDP : 67	ACCEPT
May 1 19:52:23	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:52:18	192.168.1.200	192.168.1.170	TCP : 80	ACCEPT
May 1 19:50:14	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 19:50:13	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 19:46:37	211.74.216.238	61.59.238.188	ICMP : 8	ACCEPT
May 1 19:28:35	192.168.200.200	192.168.200.1	TCP : 80	ACCEPT
May 1 19:28:05	209.73.225.7	192.168.200.200	TCP : 1681	ACCEPT
May 1 19:28:05	192.168.200.200	209.73.225.7	TCP : 80	ACCEPT
May 1 19:28:05	192.168.200.200	209.73.225.7	TCP : 80	ACCEPT

### Traffic Log Table

The table in the Traffic Log window displays current System statuses:

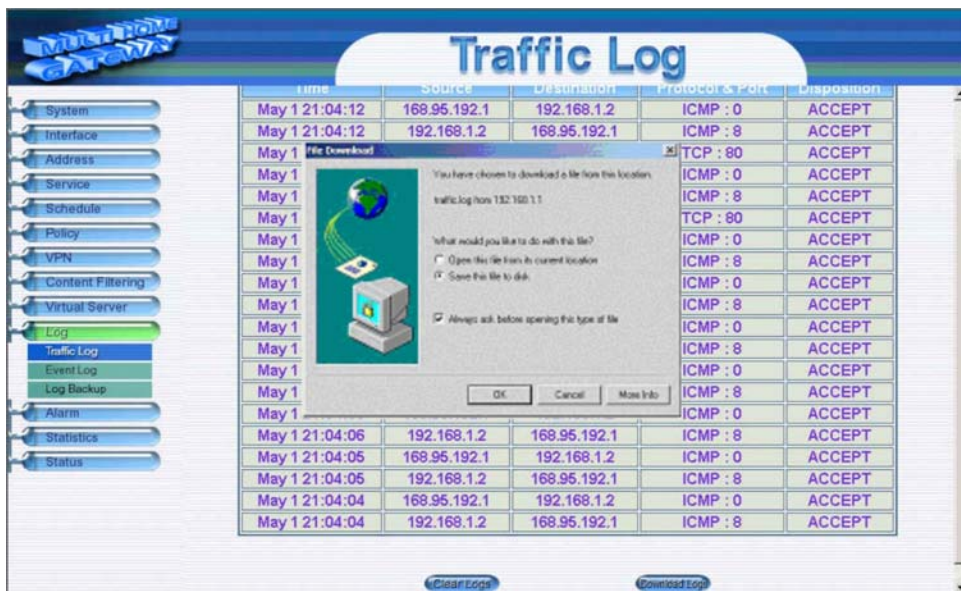
- **Time:** The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol & Port:** Protocol type and Port number of the specific connection.
- **Disposition:** 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.

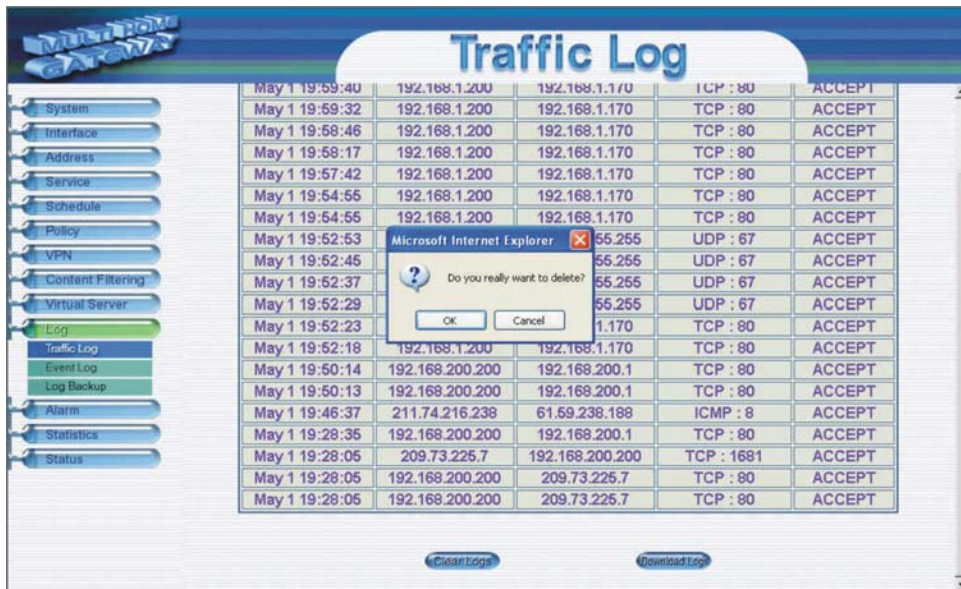


## Clearing the Traffic Logs

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.





## Event Log

When the 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router 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

Click the **Event Log** option under the **Log** menu and the Event Log window will appear.

Time	Event
May 1 19:59:38	admin Remove [Virtual Server 1] from 192.168.1.200
May 1 19:59:32	admin Remove [FTP] (Virtual Server 1) from 192.168.1.200
May 1 19:57:42	admin Add [FTP] (Virtual Server 1) from 192.168.1.200
May 1 19:52:23	user admin [Login success] from 192.168.1.200
May 1 19:50:30	admin Modify [LAN Interface] from 192.168.200.200
May 1 19:50:13	user admin [Login success] from 192.168.200.200
May 1 19:28:38	admin Add [Virtual Server 1] from 192.168.200.200
May 1 19:28:35	user admin [Login success] from 192.168.200.200
May 1 19:23:06	admin Remove [Virtual Server 1] from 192.168.200.200
May 1 19:22:59	admin Add [Virtual Server 1] from 192.168.200.200

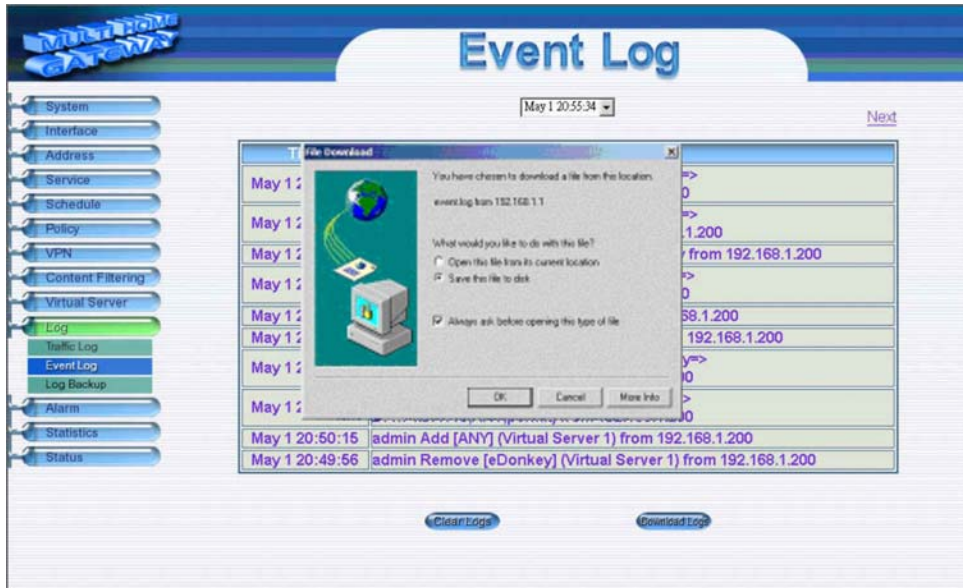
The table in the Event Log window displays the time and description of the events.

- **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.

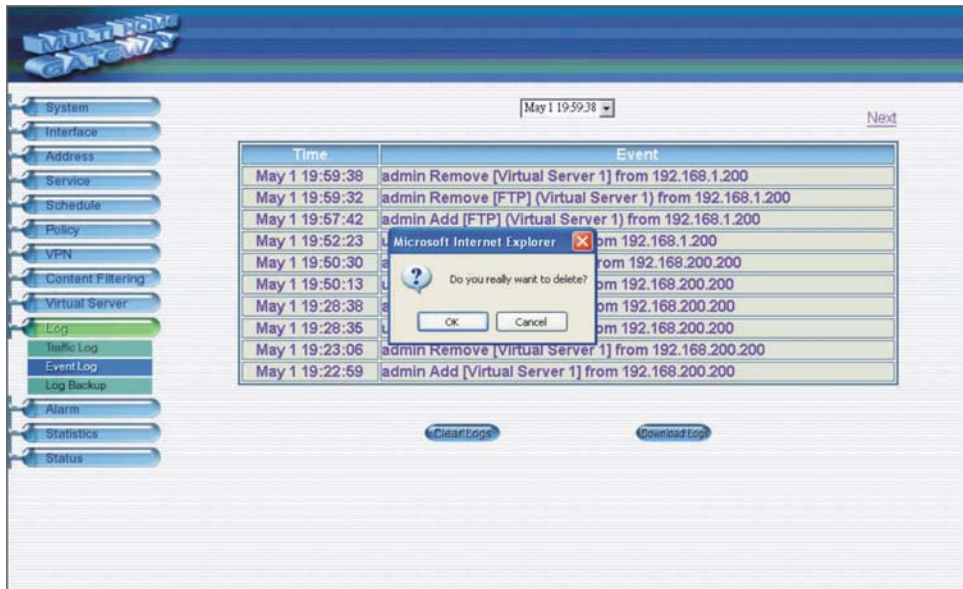


## Clearing the Event Logs

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.

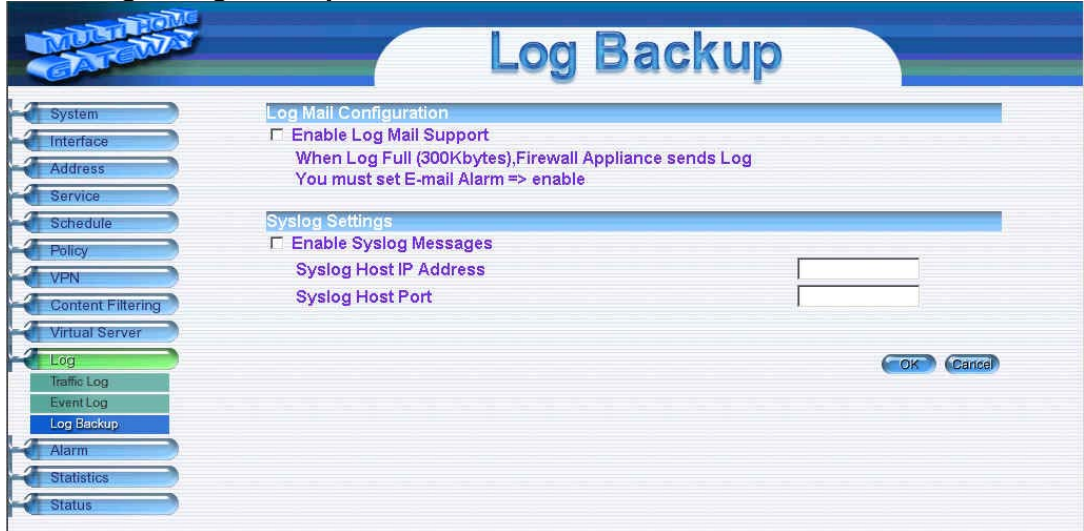
**Step 2.** In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.



# Log Backup

The Log Backup

**Step 1.** Click **Log** → **Log Backup**.



**Step 2.**

- **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 enable E-mail Alarm in Administrator.*
- **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.

## 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 3.** Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.
- Step 4.** Click **OK**.

**Log Backup**

**Log Mail Configuration**

**Enable Log Mail Support**  
When Log Full (300Kbytes), Firewall Appliance sends Log  
You must set E-mail Alarm => enable

**Syslog Settings**

**Enable Syslog Messages**

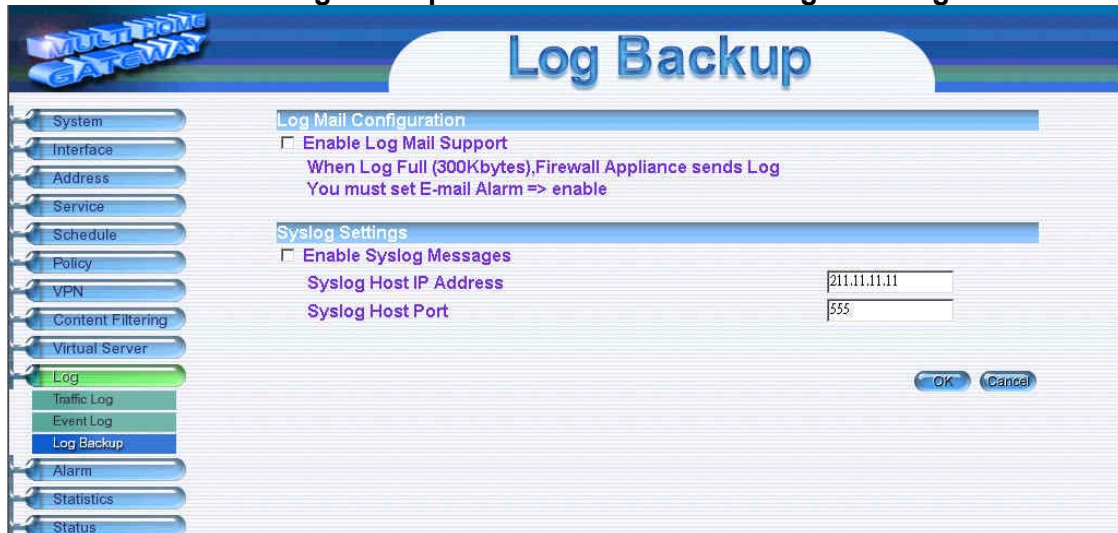
Syslog Host IP Address: 211.11.11.11

Syslog Host Port: 555

OK Cancel

## 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**.



The screenshot shows the 'Log Backup' configuration page. On the left is a navigation menu with items: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log (highlighted), Traffic Log, Event Log, Log Backup, Alarm, Statistics, and Status. The main content area is titled 'Log Backup' and contains two sections:

- Log Mail Configuration**
  - Enable Log Mail Support**  
When Log Full (300Kbytes), Firewall Appliance sends Log  
You must set E-mail Alarm => enable
- Syslog Settings**
  - Enable Syslog Messages**
  - Syslog Host IP Address:
  - Syslog Host Port:

At the bottom right of the configuration area are 'OK' and 'Cancel' buttons.

# Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the Multi-Homing has logged.

Multi-Homing 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.

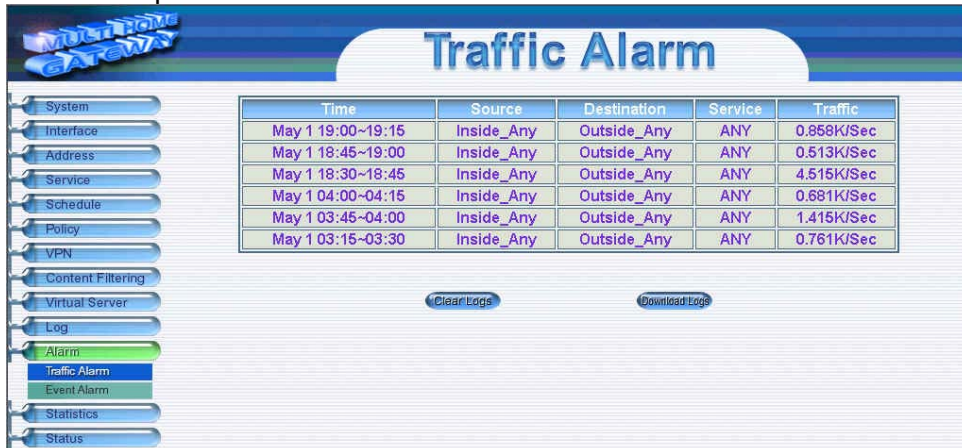
## **Event alarm:**

When Multi-Homing 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.

# Traffic Alarm

## Entering the Traffic Alarm window

Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.



The screenshot shows the 'Traffic Alarm' window with a sidebar menu on the left and a table of logs in the center. The sidebar menu includes options like System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Traffic Alarm (highlighted), Event Alarm, Statistics, and Status. The table displays traffic logs with columns for Time, Source, Destination, Service, and Traffic.

Time	Source	Destination	Service	Traffic
May 1 19:00~19:15	Inside_Any	Outside_Any	ANY	0.858K/Sec
May 1 18:45~19:00	Inside_Any	Outside_Any	ANY	0.513K/Sec
May 1 18:30~18:45	Inside_Any	Outside_Any	ANY	4.515K/Sec
May 1 04:00~04:15	Inside_Any	Outside_Any	ANY	0.681K/Sec
May 1 03:45~04:00	Inside_Any	Outside_Any	ANY	1.415K/Sec
May 1 03:15~03:30	Inside_Any	Outside_Any	ANY	0.761K/Sec

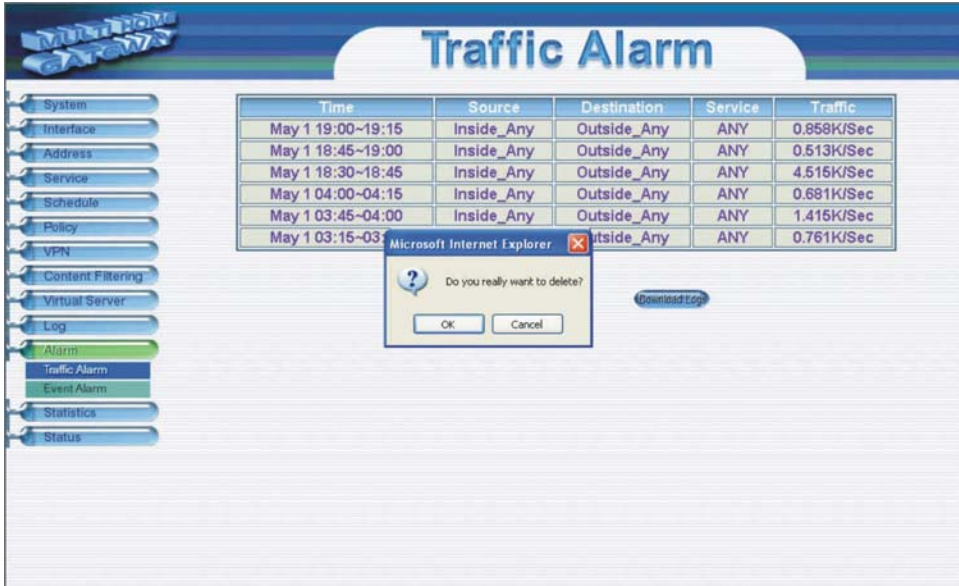
The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- **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.



## 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.



The screenshot displays the 'Traffic Alarm' window. On the left is a navigation pane with buttons for System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Traffic Alarm, Event Alarm, Statistics, and Status. The 'Traffic Alarm' button is highlighted. The main area contains a table with the following data:

Time	Source	Destination	Service	Traffic
May 1 19:00~19:15	Inside_Any	Outside_Any	ANY	0.859K/Sec
May 1 18:45~19:00	Inside_Any	Outside_Any	ANY	0.513K/Sec
May 1 18:30~18:45	Inside_Any	Outside_Any	ANY	4.516K/Sec
May 1 04:00~04:15	Inside_Any	Outside_Any	ANY	0.681K/Sec
May 1 03:45~04:00	Inside_Any	Outside_Any	ANY	1.416K/Sec
May 1 03:15~03:30	Inside_Any	Outside_Any	ANY	0.761K/Sec

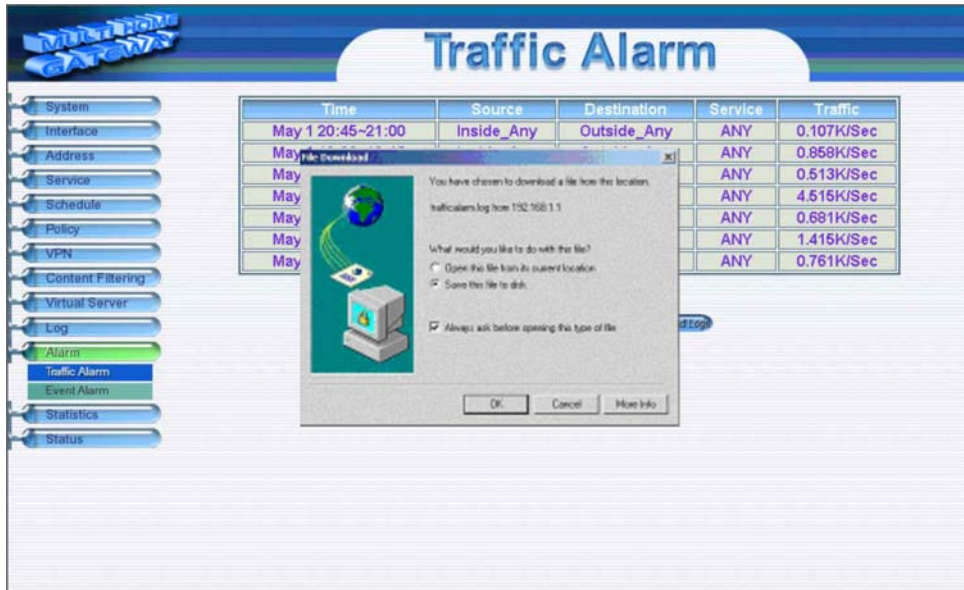
A 'Microsoft Internet Explorer' dialog box is overlaid on the table, asking 'Do you really want to delete?' with 'OK' and 'Cancel' buttons. A 'Download Log' button is visible to the right of the dialog box.

## 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.

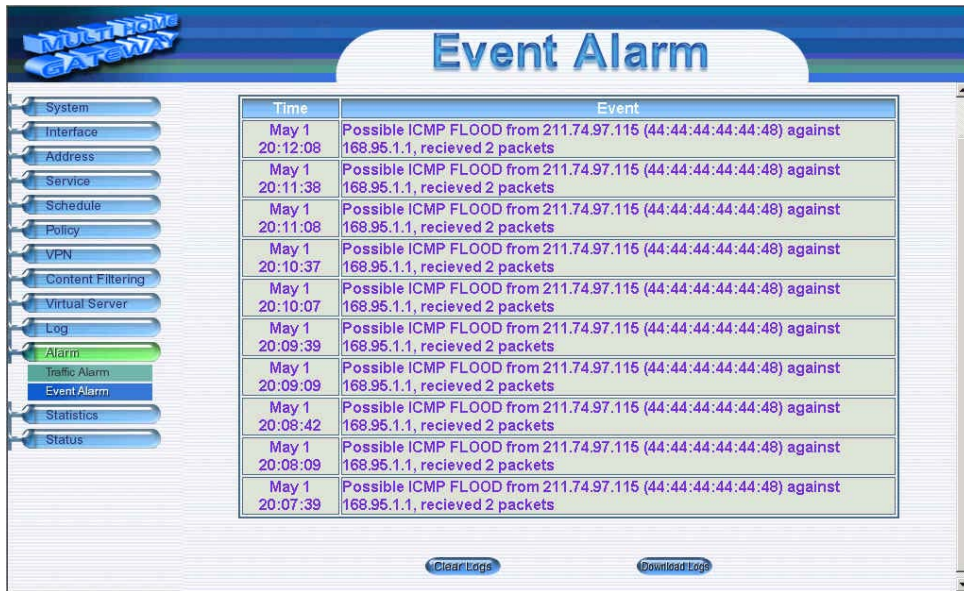
**Step 2.** Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.



# Event Alarm

## Entering the Event Alarm window

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.

## 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**.



The screenshot shows the 'Event Alarm' window with a table of events. A confirmation dialog box is overlaid on the table, asking 'Do you really want to delete?'. The dialog box has 'OK' and 'Cancel' buttons. The table contains the following data:

Time	Event
May 1 20:12:08	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:11:38	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:11:08	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:10:37	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:10:07	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:09:39	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:09:09	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:08:42	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:08:09	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets
May 1 20:07:39	Possible ICMP FLOOD from 211.74.97.115 (44:44:44:44:48) against 168.95.1.1, recieved 2 packets

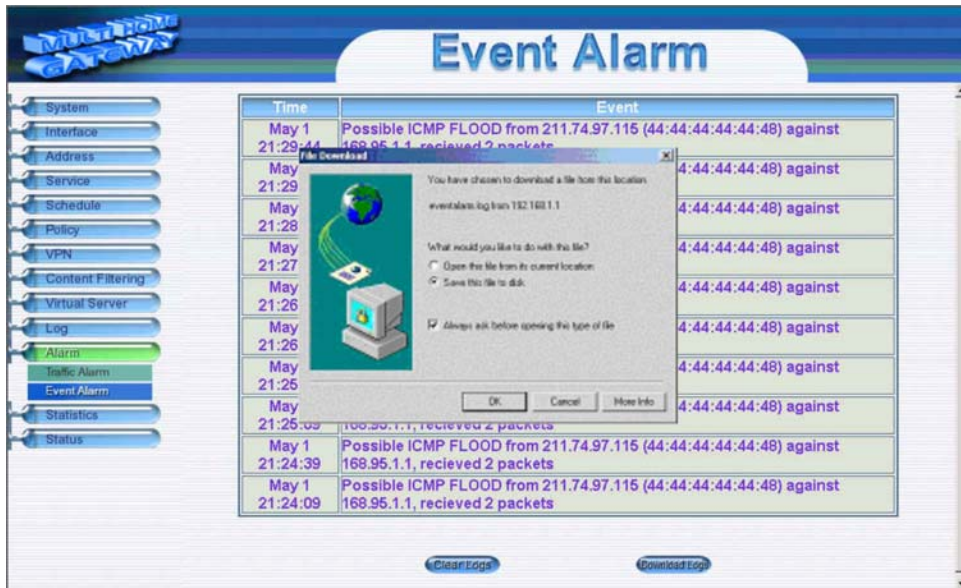
At the bottom of the window, there are two buttons: 'Clear Logs' and 'Download Log'.

## 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.





# Statistics

In this chapter, the Administrator queries the 10/100M 2 WAN /4 LAN Multi-Homing Dual WAN Firewall Router for statistics of packets and data which passes across the Multi-Homing. 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 by control policies setup by the Administrator.

## **How to use Statistics**

The Administrator can get the current network condition from statistics, and use the information provided by statistics as a basis to manage networks.

# WAN Statistics

WAN	Time
WAN1	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a>
All External Interface	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a>

## Entering the Statistics window by Time

The Statistics window displays the statistics of network connections (downstream and upstream as well) by minute, hour, or day.

**All External Interface** : Displays statistics of WAN 1/2 network connections (downstream and upstream as well) in a total amount by minute, hour or day.



# Policy Statistics

## Entering the Statistics window

**Step 1.** 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

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	PERMIT	Minute Hour Day



# Status

In this section, the device displays the status information about the Multi-Homing. 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.

# 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 Interface, and the WAN 2 Interface.

The screenshot displays the 'Interface Status' window. On the left is a vertical menu with items: System, Interface, Address, Service, Schedule, Policy, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, Status (highlighted), Interface Status, ARP Table, and DHCP Clients. The main content area shows 'Active Sessions Number : 7' and 'System Uptime 0 Day 17 Hour 34 Min 10 Sec'. Below this is a table with columns for LAN, WAN1 (PPPoE), and WAN2 (PPPoE). The table lists various interface parameters and their values for each interface.

	LAN	WAN1 (PPPoE)	WAN2 (PPPoE)
Forwarding Mode	NAT	---	---
Current Status	---	Connecting	Connecting
Connection Time	---	1: 33: 10	1: 33: 40
MAC Address	44:44:44:44:44:47	44:44:44:44:44:48	44:44:44:44:44:49
IP Address	192.168.1.170	211.74.97.115	61.59.238.188
Netmask	255.255.255.0	255.255.255.255	255.255.255.255
Default Gateway	---	211.74.97.1	61.59.238.1
MTU	1504	1492	1492
Rx Pkts, Error Pkts	18929, 0	8067, 0	7427, 0
Tx Pkts, Error Pkts	18497, 0	5943, 0	6374, 0
Ping	Enable	Enable	Enable
WebUI	Enable	Enable	Enable

# 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, and WAN 2 network that replies to an ARP packet, the device will list them in this ARP table.



IP Address	MAC Address	Interface
192.168.1.200	00:48:54:5C:A9:4F	LAN

**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, WAN 2)

# 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's DHCP server function.

IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.3	00:48:54:5c:7c:3f	2002/5/1 20:7:2	2002/5/2 20:7:2

**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.

# Setup Examples

**Example 1:** Allow the LAN network to be able to access the Internet

**Example 2:** The LAN network can only access Yahoo.com website

**Example 3:** Outside users can access the LAN FTP server through Virtual Servers

**Example 4:** Install a server inside the LAN network and have the Internet (WAN 1) users access the server through IP Mapping-----

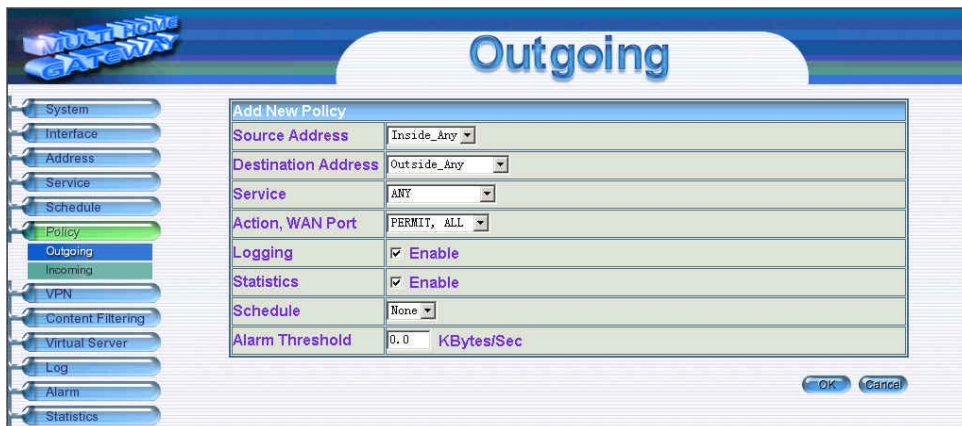
*Please see the explanation of the examples below:*

**Example 1:** Allow the LAN network to be able to access the Internet

**Step 1** Enter the Outgoing window under the Policy menu.

**Step 2** Click the New Entry button on the bottom of the screen.

**Step 3** In the Add New Policy window, enter each parameter, then click OK.



**Step 4** When the following screen appears, the setup is completed.



**Example 2:** The LAN network can only access Yahoo.com website.

Step 1. Enter the WAN window under the Address menu.

Step 2. Click the New Entry button.

Step 3. In the Add New Address window, enter relating parameters.

Add New Address	
Name	www.yahoo.com
IP Address	61.222.254.137
Netmask	255.255.255.255

Step 4. Click **OK** to end the address table setup.

Step 5. Go to the Outgoing window under the Policy menu.

Step 6. Click the New Entry button.

Step 7. In the Add New Policy window, enter corresponding parameters. Click **OK**.

Add New Policy	
Source Address	Inside_Any
Destination Address	www.yahoo.com
Service	ANY
Action, WAN Port	PERMIT, ALL
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec

Step 8. When the following screen appears, the setup is completed.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To: 1
Inside_Any	www.yahoo.com	ANY	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To: 2



**Example 3:** Outside users can access the LAN FTP server through Virtual Servers

- Step 1. Enter Virtual Server under the Virtual Server menu.
- Step 2. Click the 'click here to configure' button.
- Step 3. Select an WAN 1/2 IP address, then click OK.
- Step 4. Click the New Service button on the bottom of the screen.
- Step 5. Add the FTP service pointing to the LAN server IP address.  
Click OK.

The screenshot shows a 'Virtual Server Configuration' dialog box. It has a title bar and several fields. The 'Virtual Server Real IP' is set to 61.59.238.123. The 'Service Name (Port)' is 'FTP (21)'. The 'External Service Port' is '21'. Below these fields is a table with two columns: 'Load Balance Server' and 'Server Virtual IP'. The table has four rows, with the first two rows containing the values 1 and 2 in the first column, and 192.168.1.200 and 192.168.1.224 in the second column. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Load Balance Server	Server Virtual IP
1	192.168.1.200
2	192.168.1.224
3	
4	

Step 6. A new Virtual Service should appear.

The screenshot shows a table of Virtual Servers. The 'Virtual Server Real IP' is 61.59.238.123. The table has four columns: 'Service Name (Port)', 'WAN Port', 'Server Virtual IP', and 'Configure'. The first row contains 'FTP (21)', '21', and two IP addresses: 192.168.1.200 and 192.168.1.224. The 'Configure' column has 'Modify' and 'Remove' buttons. Below the table is a 'New Entry' button.

Service Name (Port)	WAN Port	Server Virtual IP	Configure
FTP (21)	21	192.168.1.200 192.168.1.224	Modify Remove

Step 7. Go to the Incoming window under the Policy menu, then click on the New Entry button.

The screenshot shows the 'Incoming' window in the Policy menu. The window has a title bar and a navigation pane on the left with buttons for System, Interface, Address, Service, Schedule, and Policy. The main area has a table with columns: Source, Destination, Service, Action, Option, Configure, and Move. Below the table is a 'New Entry' button.

Source	Destination	Service	Action	Option	Configure	Move
--------	-------------	---------	--------	--------	-----------	------

Step 8. In the Add New Policy window, set each parameter, then click OK.

The screenshot shows a web-based configuration interface for a network device. On the left is a vertical navigation menu with buttons for System, Interface, Address, Service, Schedule, Policy, Outgoing, Incoming, VPN, Content Filtering, Virtual Server, Log, Alarm, Statistics, and Status. The 'Incoming' button is highlighted. The main area is titled 'Incoming' and contains a 'Add New Policy' form. The form fields are as follows:

Add New Policy	
Source Address	Outside_Any
Destination Address	Virtual Server 1 (61.59.238.123)
Service	FTP
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec

At the bottom right of the form are two buttons: 'OK' and 'Cancel'.

Step 9. An Incoming FTP policy should now be created.

**Example 4:** Install a server inside the LAN network and have the Internet (WAN 1) users access the server through IP Mapping

Step 1. Enter the Mapped IP window under the Virtual Server menu.

Step 2. Click the New Entry button.

Step 3. In the Add New IP Mapping window, enter each parameter, and then click OK.

Add New Mapped IP	
WAN IP	61.59.238.188 <a href="#">Assist</a>
Map To Virtual IP	192.168.1.201

Step 4. When the following screen appears, the IP Mapping setup is completed.

WAN IP	Map To Virtual IP	Configure
61.59.238.188	192.168.1.201	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Step 5. Go to the Incoming window under the Policy menu.

Step 6. Click the New Entry button.

Step 7. In the Add New Policy window, set each parameter, then click OK.

Add New Policy	
Source Address	Outside_Any
Destination Address	Mapped IP(61.59.238.188)
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec

Step 8. Open all the services. (ANY)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mapped IP(61.59.238.188)	ANY				To 1

Step 9. The setup is completed.