Air Live®
Powered by OvisLink Corp.

RS-3000

Office UTM Gateway

User's Manual

www.airlive.com

Copyright

Trademarks

FCC Interference Statement

The **RS-3000** has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility,
EN 55022/A1/A2, EN 61000-3-2, EN 61000-3-3/A1, EN 55024/A1/A2, Class B.

The specification is subject to change without notice.

Table of Contents

Chapter 1 Introduction

Congratulations on your purchase of this outstanding RS-3000 Office UTM Gateway. This product is specifically designed for the office that has the higher security request. It provides an advanced security protection to internal clients or servers from threats, such as virus, spam and hacker attack. It can also manage user's access right for IM and P2P, to save precious bandwidth from being exhausting. With all-in-one security device, user can fully utilize the budget to construct the security environment and does not need to purchase the further device.

Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Functions and Features

Mail Security

- **Anti-Virus for Inbound E-mail filter**
  Integrated with Clam AV virus engine can filter the attached virus of incoming mail.
- **Regularly or manually updated virus pattern**
  The virus pattern can be auto updated regularly (every 10 minutes), or manually updated. And the license is free.
- **Anti-Spam for Inbound E-mail filter**
  Built-in with Bayesian, fingerprint, verifying sender account, and checking sender IP in RBL system work to filter spam mail automatically.
- **Mail Training system**
  Update system with the error judged type of mail, to improve the accurate rate of Anti-Spam.

Network Security

- **IDP (Intrusion Detection Prevention)**
  The IDP system provides the function to detect and stop the hacker software's attack from Internet. It filters the malicious packets based on the embedded signature database; user can select to update the database by regularly or manually.
- **Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS**
  RS-3000 Anti-Virus not only can filter mail, it also supports to scan HTTP, FTP, P2P, IM and NetBIOS packets.
- **Detect and block the anomaly flow IP**
  Anomaly flow packets usually spread out to the network as abnormal type, and administrator can configure the function to drop them.

- **IPSec and PPTP VPN**

  VPN (Virtual Private Network) uses to secure the data transferring with encrypted and private channel, IPSec provides high level of data encrypted, and PPTP provides easily configuration.

- **VPN Trunk**

  VPN trunk function allows user to create two VPN tunnels simultaneously, and offers VPN fail-over feature.

- **IM / P2P Blocking**

  Currently IM and P2P can be managed separately the access right. IM types include MSN, Yahoo Messenger, ICQ, QQ, Google Talk, Gadu-Gadu and Skype, and P2P types include eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, VNN Client, PPLive, Ultra-Surf, PPStream, GoGoBox, Tor, UUSee, QQLive/QQGame, QQDownload, Ares, Hamachi, TeamViewer, and GLWorld.

- **Content Blocking**

  Four types of Internet services can be managed the access right: **URL**, **Scripts** (Popup, ActiveX, Java, Cookie), **Download** and **Upload**.

- **User Authentication**

  User must pass the authenticated for the Internet accessed right. The account database can be the local database, RADIUS and POP3 server.

- **QoS**

  Divided the bandwidth per service or IP address, to guarantee a certain bandwidth for the specific service server to be accessed.

- **Personal QoS**

  Just a simple setting to unify the bandwidth of all internal clients.

Advanced functions

- **Multiple WANs Load Balance**

  Supports Round-Robin, By Traffic/Session/Packet Load Balance types to fit the different kinds of request and environment

- **Load Balance by Source IP / Destination IP**

  WAN path will be defined based on the first access packets from Source IP or Destination IP. The function can avoid the disconnection due to the specific server only accepts a single IP per each client, such as banking system, and Internet on-line Game Server.

- **Multiple Subnet**

  Multiple LAN subnets are allowable to be configured simultaneously, but only the subnet of LAN port supports the DHCP server function.

- **DMZ Transparent**

  The function uses to simulate WAN port real IP to DMZ device.

1.2 Front Panel

Figure 1-1 Front Panel

LED	Color	Status	Description
POWER	Green	On	Power on the device
Status	Green	On	Device is ready to use
		Blinking	Device is at the booting process
WAN 1/2	Green	Blinking	Packets is sending/receiving
	Orange	On	Cable speed is 100 Mbps
LAN	Green	Blinking	Packets is sending/receiving
	Orange	On	Cable speed is 100 Mbps
DMZ	Green	Blinking	Packets is sending/receiving
	Orange	On	Cable speed is 100 Mbps

Port	Description
WAN 1/2	Use this port to connect to a router, DSL modem, or Cable modem
LAN	Use this port to connect to the LAN network of the office
DMZ	Connection to the Internet (FTP, SNMP, HTTP, DNS)
Console Port	9-pin serial port connector for checking setting and restore to the factory setting

1.3 Packing List

- RS-3000 Office UTM Gateway
- Installation CD-ROM
- Quick Installation Guide
- CAT-5 UTP Fast Ethernet cable
- CAT-5 UTP Fast Ethernet cross-over cable
- RS-232 cable
- Power code
- Accessories

Chapter 2 Network Settings and Software Installation

To use this product correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000/XP).

2.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.1.1, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to the example:

1. Configure IP as 192.168.1.2, subnet mask as 255.255.255.0 and gateway as 192.168.1.1, or more easier,
2. Configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows platforms. First, execute the **ping** command

ping 192.168.1.1

If the following messages appear:

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

A communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

   Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

   Tip: If the IP address of this product is 192.168.1.1, the IP address of your computer must be 192.168.1.X and default gateway must be 192.168.1.1.

2.2 Example for configure RS-3000 Web UI

STEP 1:

1. Connect the Admin's PC and the LAN port of the Security Gateway.
2. Open an Internet web browser and type the default IP address of the Security Gateway as **192.168.1.1** in the address bar.
3. A pop-up screen will appear and prompt for a username and password. Enter the default login username (**admin**) and password (**airlive**) of Administrator.

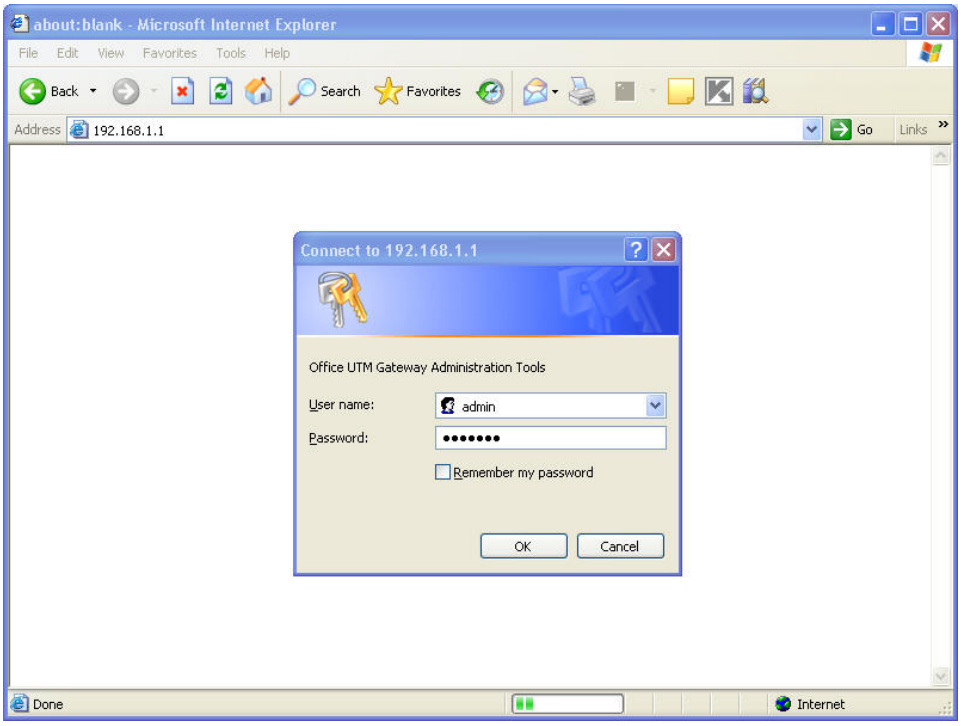


Figure 2-1 Login page

STEP 2:

After entering the username and password, the Security Gateway WEB UI screen will display. Select the **Interface** tab on the left menu and a sub-function list will be displayed.

◊ Click on **WAN** from the sub-function list, enter proper the network setup information

◊ Click **Modify** to modify WAN1/2 settings (i.e. WAN1 Interface)

WAN1 interface	IP Address	60.250.158.66
	NetMask	255.255.255.0
	Default Gateway	60.250.158.254
	DNS Server1	168.95.1.1

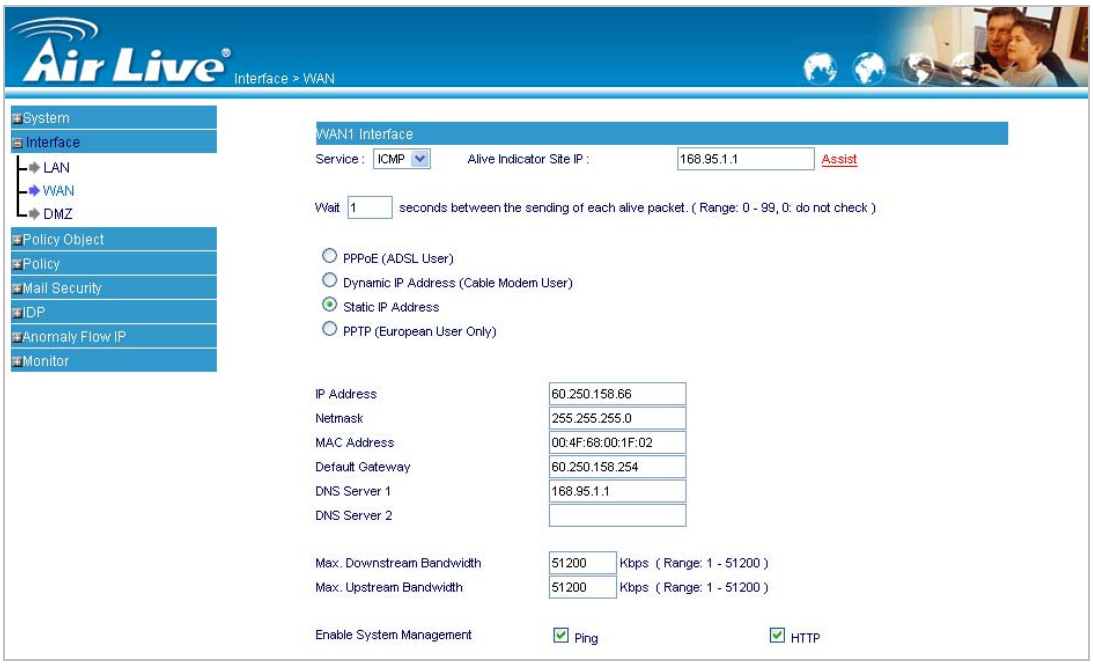


Figure 2-2 WAN interface setting page

STEP 3:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** from the sub-function list.

STEP 4:

Click on **New Entry** button.

STEP 5:

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

Source Address – select **Inside_Any**

Destination Address – select **Outside_Any**

Service - select **ANY**

Action - select **Permit ALL**

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

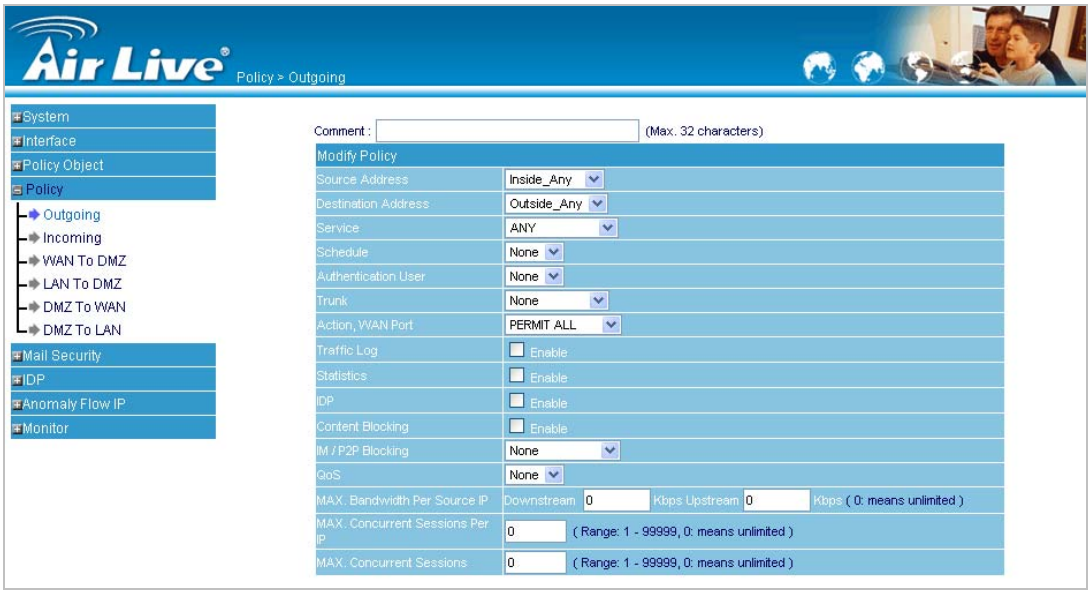


Figure 2-3 Policy setting page

STEP 6:

The configuration is successful when the screen below is displayed. Make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Security Gateway's LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately.

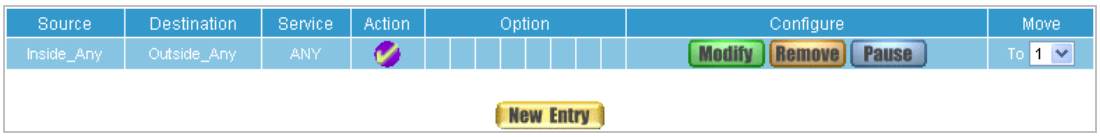


Figure 2-4 Complete Policy setting page

Chapter 3 Administration

"System" is the managing of settings such as the privileges of packets that pass through the RS-3000 and monitoring controls. The System Administrators can manage, monitor, and configure RS-3000 settings. But all configurations are "read-only" for all users other than the System Administrator; those users are not able to change any setting of the RS-3000.

3.1 Admin

Administrator Name:

- The username of Administrators and Sub Administrator for the RS-3000. The **admin** user name cannot be removed; and the sub-admin user can be removed or modified.


The default Account: **admin**; Password: **airlive**

Privilege:

- The privileges of Administrators (Admin or Sub Admin). The username of the main Administrator is **Administrator** with **reading / writing** privilege. Administrator also can change the system setting, log system status, and to increase or delete sub-administrator. Sub-Admin may be created by the **Admin** by clicking **New Sub Admin.** Sub Admin have **only** read and monitor privilege and cannot change any system setting value.

Configure:

- Click **Modify** to change the "Sub-Administrator's" password or click **Remove** to delete a "Sub Administrator."

Adding a new Sub Administrator

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

STEP 2 . In the **Add New Sub Administrator** WebUI (Figure 3-1) and enter the following setting:

- Sub Admin Name: sub_admin
- Password: 12345
- Confirm Password: 12345

STEP 3 . Click **OK** to add the user or click **Cancel** to cancel it.

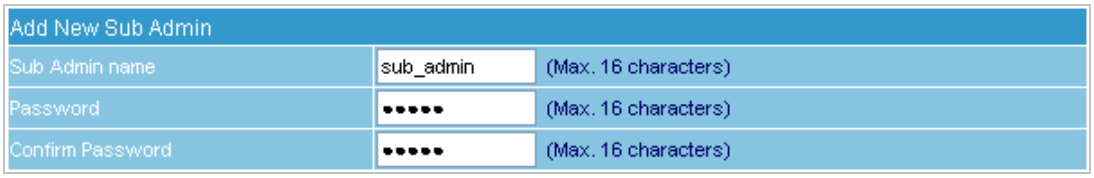


Figure 3-1 Add New Sub Admin

Modify the Administrator's Password

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

STEP 2 . The **Modify Administrator Password** WebUI will appear. Enter the following information:

- **Password:** admin
- **New Password:** 52364
- **Confirm Password:** 52364 (Figure 3-2)

STEP 3 . Click **OK** to confirm password change.

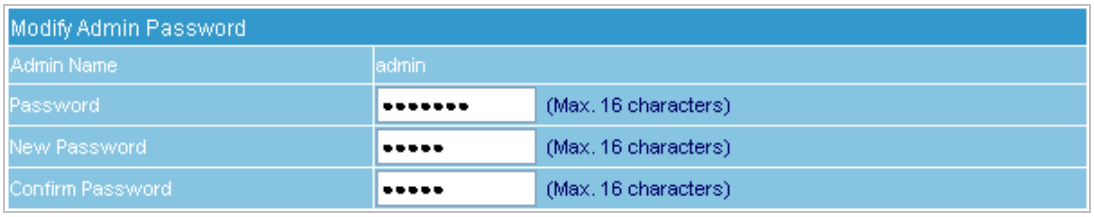


Figure 3-2 Modify Admin Password

3.2 Permitted IP

Add Permitted IPs

STEP 1 . Add the following setting in **Permitted IPs** of **Administration**: (Figure 3-3)

- **Name:** Enter master
- **IP Address:** Enter 163.173.56.11
- **Netmask:** Enter 255.255.255.255
- **Service:** Select Ping and HTTP
- Click **OK**
- Complete add new permitted IPs (Figure 3-4)

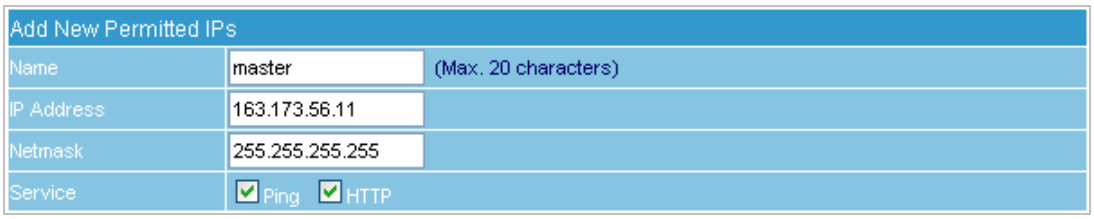


Figure 3-3 Setting Permitted IPs WebUI

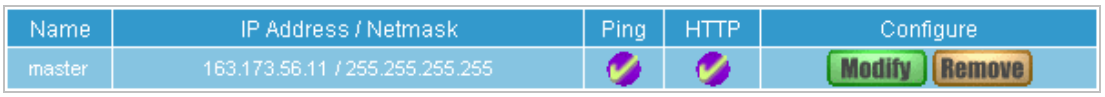


Figure 3-4 Complete Add New Permitted Ips

To make Permitted IPs be effective, it must cancel the **Ping** and **WebUI** selection in the WebUI of RS-3000 that Administrator enter. (LAN, WAN, or DMZ Interface)

Before canceling the **WebUI** selection of Interface, must set up the Permitted IPs first, otherwise, it would cause the situation of cannot enter WebUI by appointed Interface.

3.3 Logout

STEP 1 . Click **Logout** in **System** to protect the system while Administrator is away. (Figure 3-5)

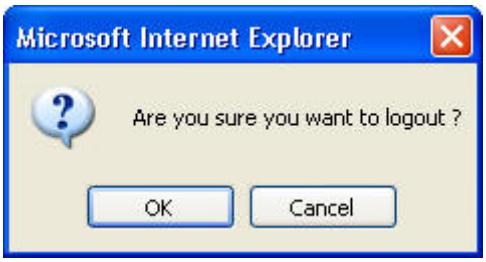


Figure 3-5 Confirm Logout WebUI

STEP 2 . Click **OK** and the logout message will appear in WebUI. (Figure 3-6)

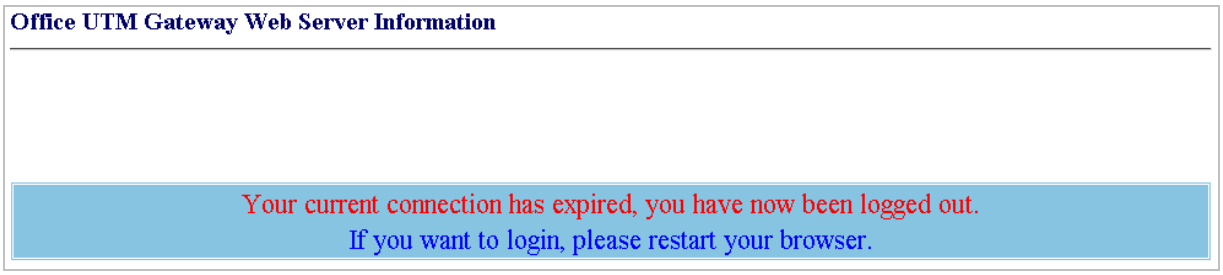


Figure 3-6 Logout WebUI Message

3.4 Software Update

STEP 1 **.** Select **Software Update** in **System**, and follow the steps below:

- To obtain the version number from **Version Number** and obtain the latest version from Internet. And save the latest version in the hardware of the PC, which manage the RS-3000
- Click **Browse** and choose the latest software version file.
- Click **OK** and the system will update automatically. (Figure 3-7)

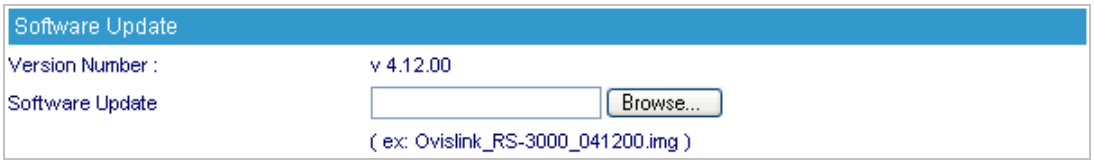


Figure 3-7 Software Update

It takes 3 minutes to update software. The system will reboot after update. During the updating time, please don't turn off the PC or leave the WebUI. It may cause some unexpected mistakes. (Strong suggests updating the software from LAN to avoid unexpected mistakes.)

Chapter 4 Configure

The Configure is according to the basic setting of the RS-3000. In this chapter the definition is Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Hosts Table, SNMP and Language settings.

4.1 Setting

AirLive RS-3000 Configuration:

- The Administrator can import or export the system settings. Click **OK** to import the file into the RS-3000 or click **Cancel** to cancel importing. You also can revive to default value here.
- Select **Reset Factory Setting** will reset RS-3000 as factory default setting.

Email Settings:

- Select **Enable E-mail Alert Notification** under E-mail Settings. This function will enable the RS-3000 to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur. (It can be set from Anomaly Flow IP Setting to detect Hacker Attacks)

Web Management (WAN Interface):

- The System Manager can change the port number used by HTTP port anytime. (Remote WebUI management)

After HTTP port has changed, if the administrator wants to enter WebUI from WAN, will have to change the port number of browser. (For example: http://61.62.108.172:8080)

MTU Setting:

- It provides the Administrator to modify the networking package length anytime. Its default value is 1500 Bytes.

Link Speed / Duplex Mode:

- By this function can set the transmission speed and mode of WAN Port when connecting other device.

Dynamic Routing (RIPv2):

- Select to enable the function of AirLive RS-3000 LAN, WAN1, WAN2 or DMZ Port to send/receive RIPv2 packets, and communication between Internal Router or External Router, to update Dynamic Routing.

SIP protocol pass-through:

- Select to enable the function of RS-3000 of passing SIP protocol. It is also possible that the SIP protocol can pass through RS-3000 without enabling this function depends on the SIP device's type you have.

Administration Packet Logging:

- After enable this function; the RS-3000 will record packet which source IP or destination address is RS-3000. And record in Traffic Log for System Manager to inquire about.

System Reboot:

- Once this function is enabled, the **Office UTM Gateway** will be rebooted.

System Settings- Exporting

STEP 1 . In System Setting WebUI, click on 

button next to Export System Settings to Client.

STEP 2 . When the **File Download** pop-up window appears, choose the destination place where to save the exported file and click on **Save**. The setting value of RS-3000 will copy to the appointed site instantly. (Figure 4-1)

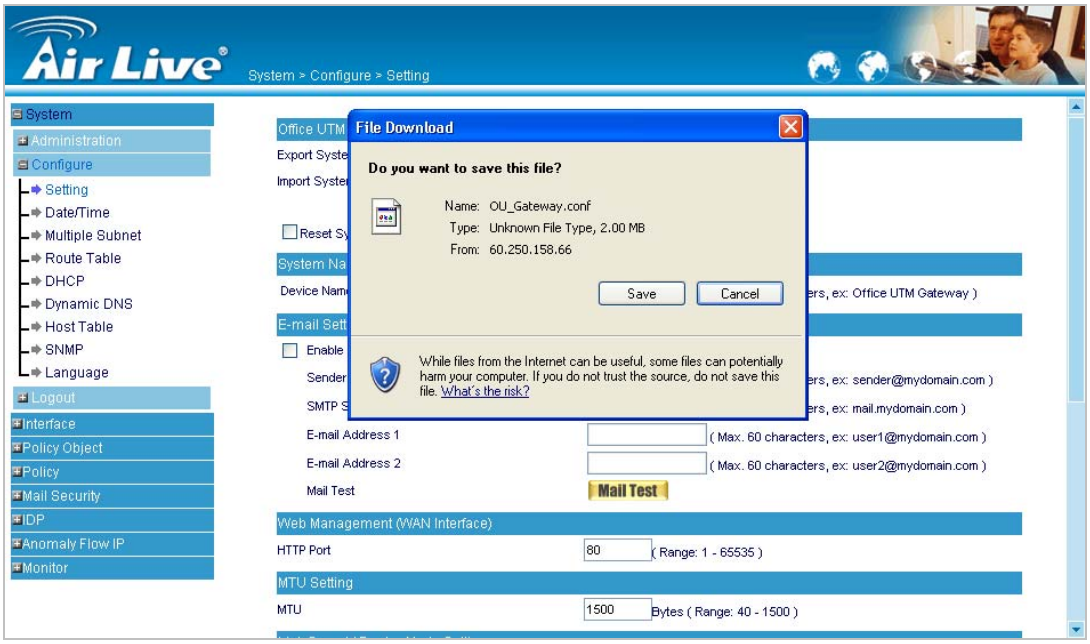


Figure 4-1 Select the Destination Place to Save the Exported File

System Settings- Importing

STEP 1 . In **System Setting** WebUI, click on the **Browse** button next to **Import System Settings from Client**. When the Choose File pop-up window appears, select the file to which contains the saved RS-3000 Settings, then click **OK**. (Figure 4-2)

STEP 2 . Click **OK** to import the file into the RS-3000 (Figure 4-3)

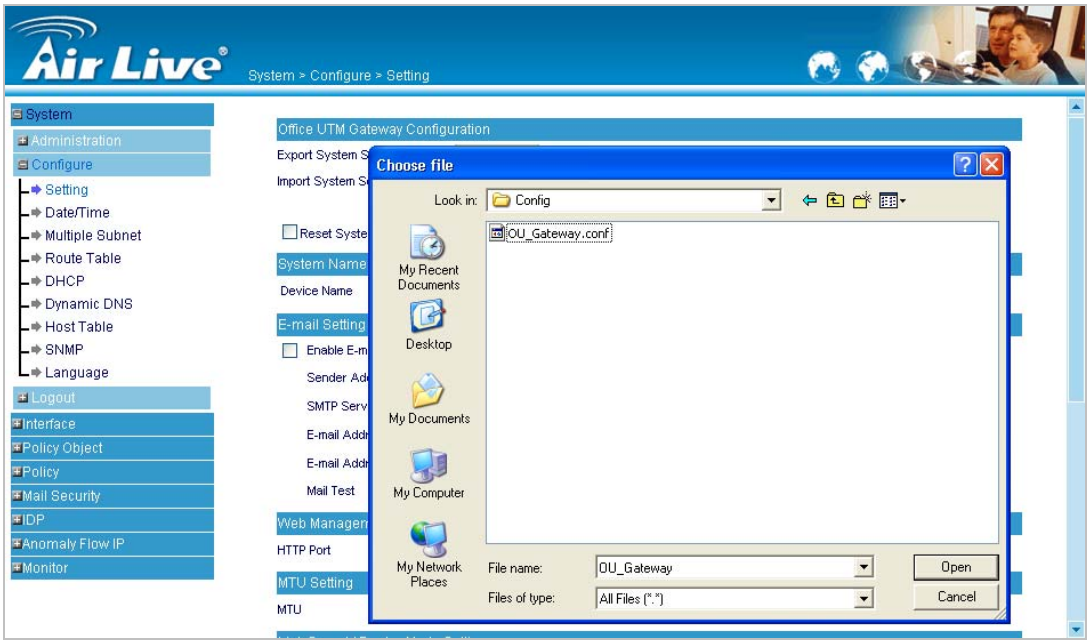


Figure 4-2 Enter the File Name and Destination of the Imported File

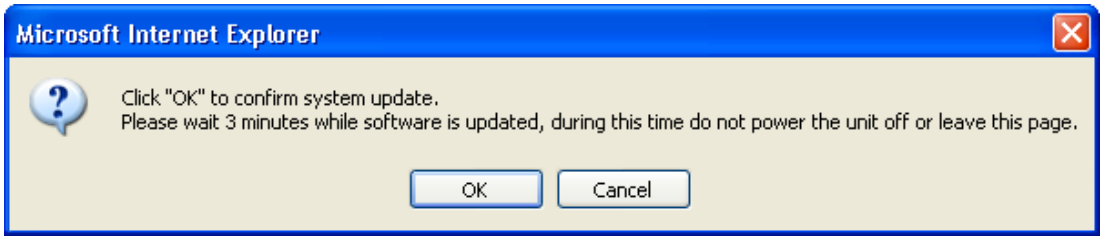


Figure 4-3 Upload the Setting File WebUI

Restoring Factory Default Settings

STEP 1 . Select **Reset Factory Settings** in RS-3000 **Configuration** WebUI

STEP 2 . Click **OK** at the bottom-right of the page to restore the factory settings. (Figure 4-4)

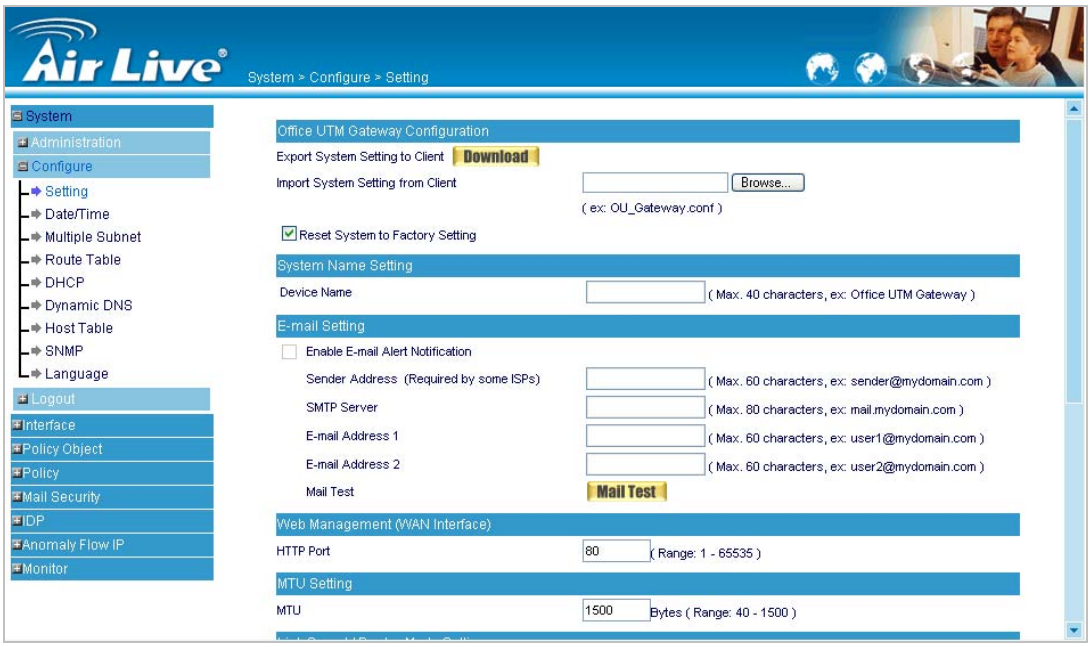


Figure 4-4 Reset Factory Settings

Enabling E-mail Alert Notification

STEP 1 . Select **Enable E-mail Alert Notification** under E-Mail Settings.

STEP 2 . **Device Name:** Enter the Device Name or use the default value.

STEP 3 . **Sender Address:** Enter the Sender Address. (Required by some ISPs.)

STEP 4 . **SMTP Server IP:** Enter SMTP server's IP address

STEP 5 . **E-Mail Address 1:** Enter the e-mail address of the first user to be notified.

STEP 6 . **E-Mail Address 2:** Enter the e-mail address of the second user to be notified. (Optional)

STEP 7 . Click **OK** on the bottom-right of the screen to enable E-mail Alert Notification. (Figure 4-5)

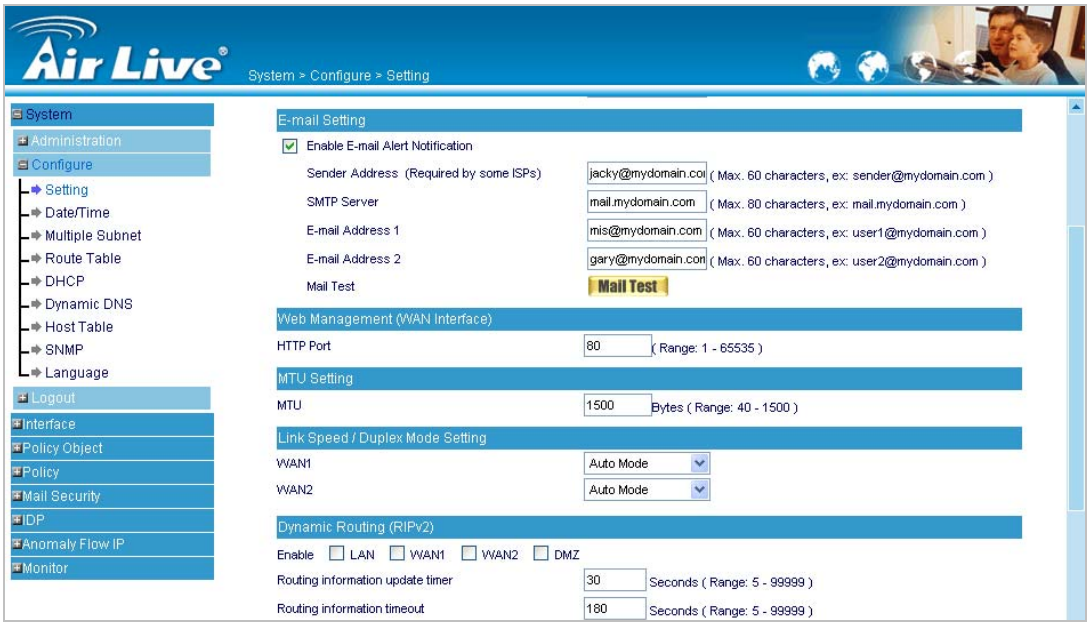


Figure 4-5 Enable E-mail Alert Notification

Click on **Mail Test** to test if E-mail Address 1 and E-mail Address 2 can receive the Alert Notification correctly.

Reboot RS-3000

STEP 1．Reboot RS-3000：Click **Reboot** button next to **Reboot RS-3000 Appliance.**

STEP 2．A confirmation pop-up page will appear.

STEP 3．Follow the confirmation pop-up page; click **OK** to restart RS-3000. (Figure 4-6)

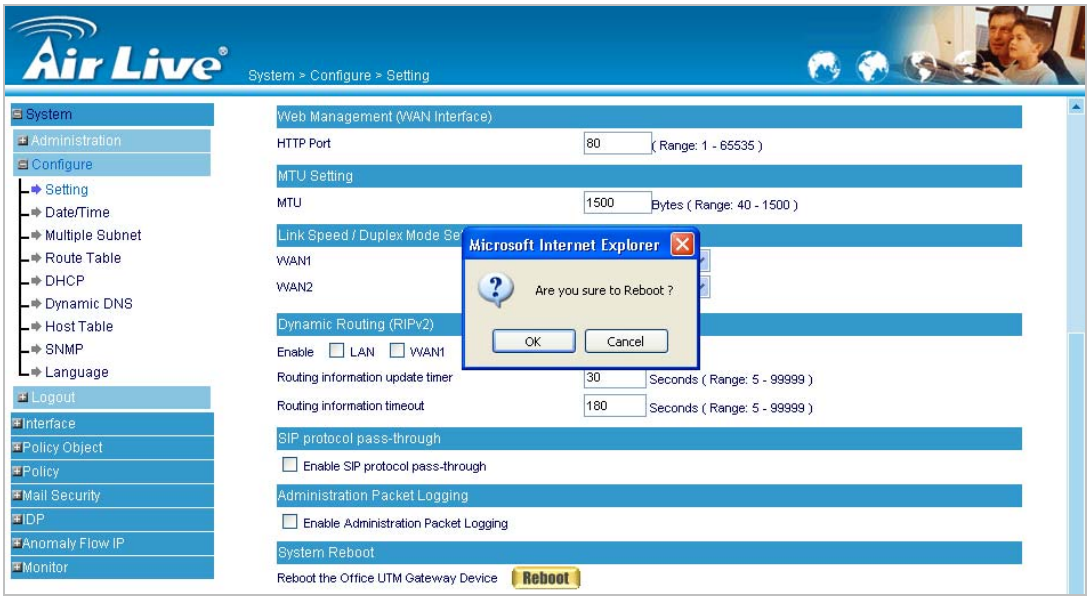


Figure 4-6 Reboot RS-3000

4.2 Date/Time

Synchronize system clock:

- Synchronizing the RS-3000 with the System Clock. The administrator can configure the RS-3000's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

STEP 1． Select **Enable synchronize with an Internet time Server** (Figure 4-7)

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

STEP 3． If necessary, select **Enable daylight saving time setting**

STEP 4． Enter the **Server IP / Name** with which you want to synchronize.

STEP 5． Set the interval time to synchronize with outside servers.

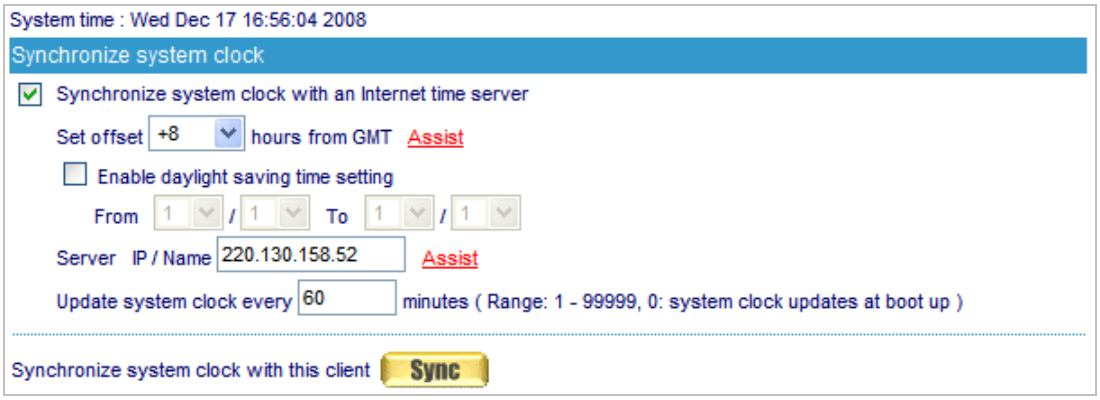


Figure 4-7 System Time Setting

Click on the **Sync** button and then the RS-3000's date and time will be synchronized to the Administrator's PC

The value of **Set Offset From GMT** and **Server IP / Name** can be looking for from **Assist**.

4.3 Multiple Subnet

Connect to the Internet through Multiple Subnet NAT or Routing Mode by the IP address that set by the LAN user's network card.

Alias IP of Interface / Netmask:

- The Multiple Subnet range

WAN Interface IP:

- The IP address that Multiple Subnet corresponds to WAN.

Forwarding Mode:

- To display the mode that Multiple Subnet use. (NAT mode or Routing Mode)

Preparation

RS-3000 WAN1 (60.250.158.66) connect to the ISP Router (60.250.158.254) and the subnet that provided by ISP is 162.172.50.0/24
To connect to Internet, WAN2 IP (211.22.22.22) connects with ATUR.

Adding Multiple Subnet

Add the following settings in **Multiple Subnet** of **System** function**:**

- Click on **New Entry**
- **Alias IP of LAN Interface：** Enter 162.172.50.1
- **Netmask：**Enter 255.255.255.0
- **WAN1:** Choose **Routing** in **Forwarding Mode**, and press **Assist** to select Interface IP 60.250.158.66.
- **WAN2：**Enter Interface IP 211.22.22.22, and choose **NAT** in **Forwarding Mode**
- Click **OK**
- Complete Adding Multiple Subnet (Figure 4-8)

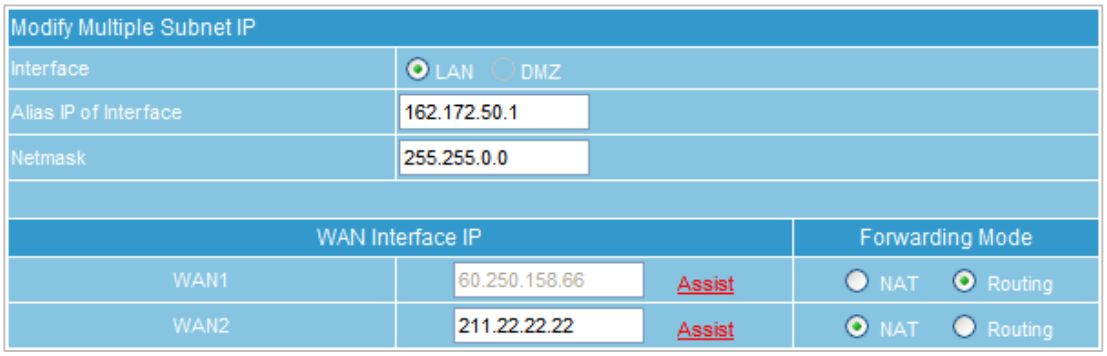


Figure 4-8 Add Multiple Subnet WebUI

WAN1 and **WAN2** Interface can use **Assist** to enter the data.

After setting, there will be two subnets in LAN: 192.168.1.0/24 (default LAN subnet) and 162.172.50.0/24. So if LAN IP is:

192.168.1.x: it must use NAT Mode to access to the Internet. (In Policy it only can setup to access to Internet by WAN2. If by WAN1 Routing mode, then it cannot access to Internet by its virtual IP)

162.172.50.x: it uses Routing mode through WAN1 (The Internet Server can see your IP 162.172.50.x directly). And uses NAT mode through WAN2 (The Internet Server can see your IP as WAN2 IP)

NAT Mode:

- It allows Internal Network to set **multiple subnet** address and connect with the Internet through different WAN IP Addresses. For example：The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into **Service**, **Sales**, **Procurement**, and **Accounting** department, the company can distinguish each department by different subnet for the purpose of managing conveniently. The settings are as the following：

  1. R&D department subnet：192.168.1.1/24 (LAN) ←→ 168.85.88.253 (WAN)
  2. Service department subnet：192.168.2.1/24 (LAN) ←→ 168.85.88.252 (WAN)
  3. Sales department subnet：192.168.3.1/24 (LAN) ←→ 168.85.88.251 (WAN)
  4. Procurement department subnet：192.168.4.1/24 (LAN) ←→ 168.85.88.250 (WAN)
  5. Accounting department subnet：192.168.5.1/24 (LAN) ←→ 168.85.88.249 (WAN)

The first department (R&D department) had set while setting interface IP; the other four ones have to be added in Multiple Subnet. After completing the settings, each department uses the different WAN IP Address to connect to the Internet. The settings of each department are as following:

	Service	Sales	Procurement	Accounting
IP Address	192.168.2.2~254	192.168.3.2~254	192.168.4.2~254	192.168.5.2~254
Subnet Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.2.1	192.168.3.1	192.168.4.1	192.168.5.1

Routing Mode:

- It is the same as NAT mode approximately but does not have to correspond to the real WAN IP address, which let internal PC to access to Internet by its own IP. (External user also can use the IP to connect with the Internet)

4.4 Route Table

STEP 1 **.** Enter the following settings in **Route Table** in **System** function:

- 【Destination IP】: Enter 192.168.10.1
- 【Netmask】: Enter 255.255.255.0。
- 【Gateway】: Enter 192.168.1.252
- 【Interface】: Select LAN
- Click **OK** (Figure 4-9)

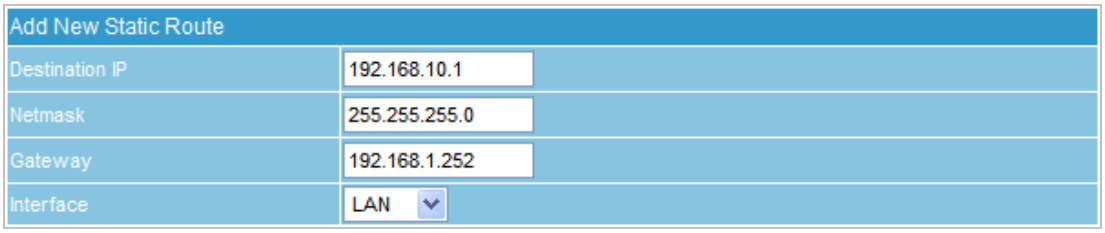


Figure 4-9 Add New Static Route1

STEP 2 **.** Enter the following settings in **Route Table** in **System** function:

- 【Destination IP】: Enter 192.168.20.1
- 【Netmask】: Enter 255.255.255.0
- 【Gateway】: Enter 192.168.1.252
- 【Interface】: Select LAN
- Click **OK** (Figure 4-10)

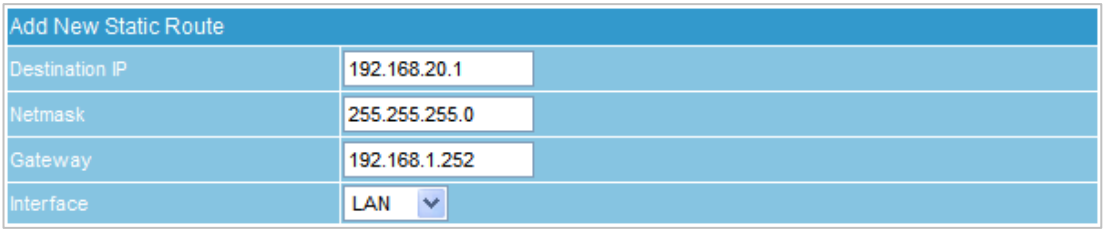


Figure 4-10 Add New Static Route2

STEP 3 **.** Enter the following setting in **Route Table** in **System** function:

- 【Destination IP】: Enter 10.10.10.0
- 【Netmask】: Enter 255.255.255.0
- 【Gateway】: Enter 192.168.1.252
- 【Interface】: Select LAN
- Click **OK** (Figure 4-11)

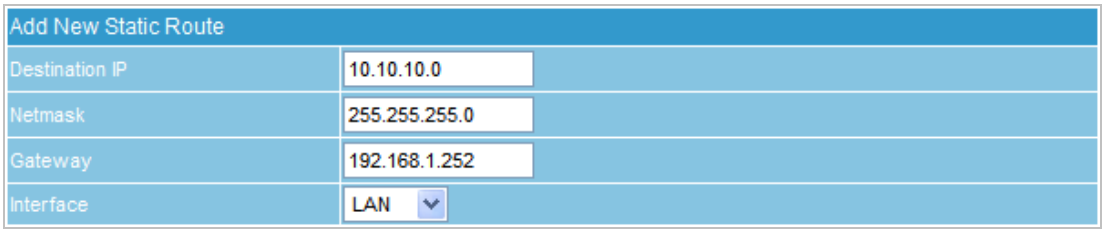


Figure 4-11 Add New Static Route3

STEP 4 . Adding successful. At this time the computer of 192.168.10.1/24, 192.168.20.1/24 and 192.168.1.1/24 can connect with each other and connect to Internet by NAT.

4.5 DHCP

Subnet: The domain name of LAN

NetMask: The LAN Netmask

Gateway: The default Gateway IP address of LAN

Broadcast IP: The Broadcast IP of LAN

STEP 1． Select **DHCP** in **System** and enter the following settings:

- **Domain Name**：Enter the Domain Name
- **DNS Server 1:** Enter the distributed IP address of DNS Server1.
- **DNS Server 2:** Enter the distributed IP address of DNS Server2.
- **WINS Server 1:** Enter the distributed IP address of WINS Server1.
- **WINS Server 2:** Enter the distributed IP address of WINS Server2.
- **LAN Interface:**
  - **Client IP Address Range 1:**

    Enter the starting and the ending IP address dynamically assigning to DHCP clients. The default value is 192.168.1.2 to 192.168.1.254 (it must be in the same subnet)
  - **Client IP Address Range 2:**

    Enter the starting and the ending IP address dynamically assigning to DHCP clients. But it must be within the same subnet as **Client IP Address Range 1** and the range cannot be repeated.

- **DMZ Interface:** the same as LAN Interface. (DMZ works only if to enable DMZ Interface)
- **Leased Time:** Enter the leased time for Dynamic IP. The default time is 24 hours.
- Click **OK** and DHCP setting is completed. (Figure 4-12)

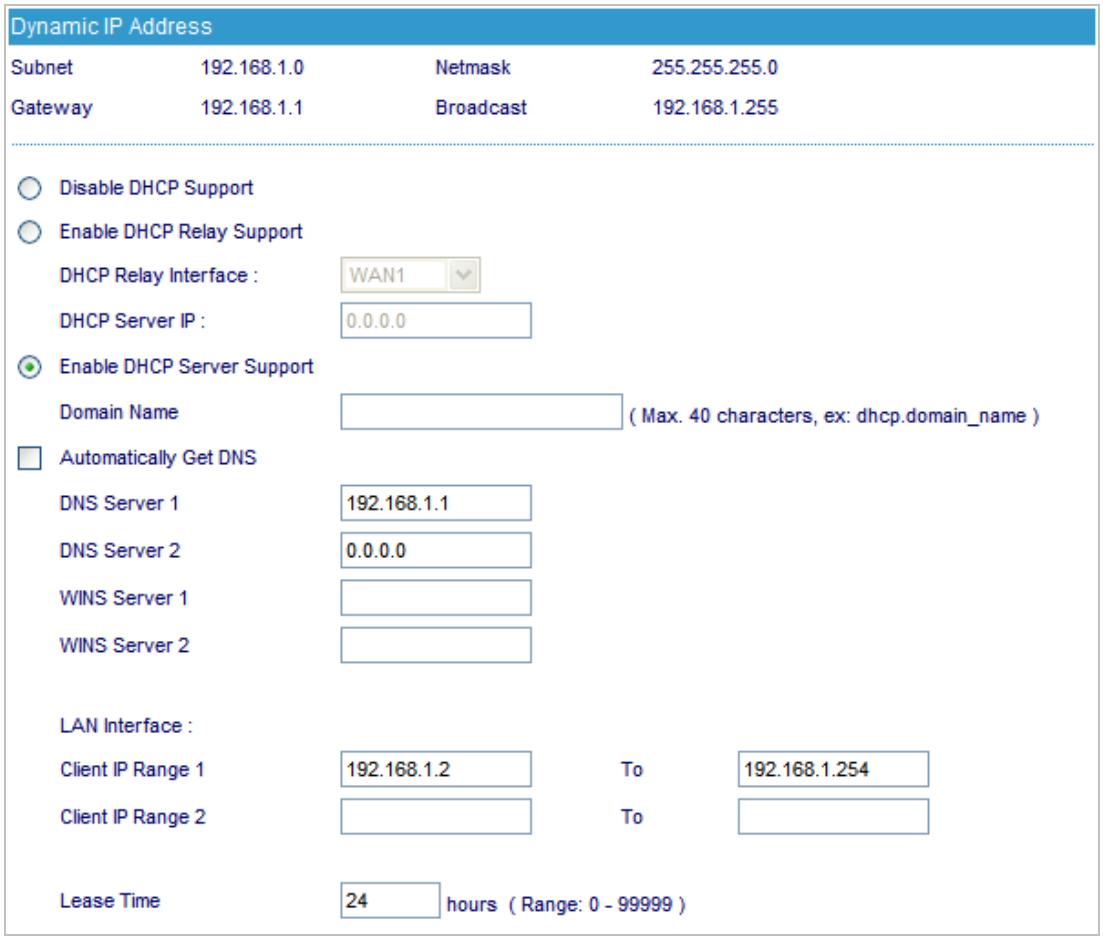


Figure 4-12 DHCP WebUI

When selecting **Automatically Get DNS**, the DNS Server will be locked as LAN Interface IP. (Using Occasion: When the system Administrator starts Authentication, the users' first DNS Server must be the same as LAN Interface IP in order to enter Authentication WebUI)

4.6 Dynamic DNS

STEP 1 **.** Select **Dynamic DNS** in **System** function (Figure 4-13). Click **New Entry** button

- **Service providers**：Select service providers.
- **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.
- **Domain name**：Enter Your host domain name
- Click **OK** to add Dynamic DNS. (Figure 4-14)

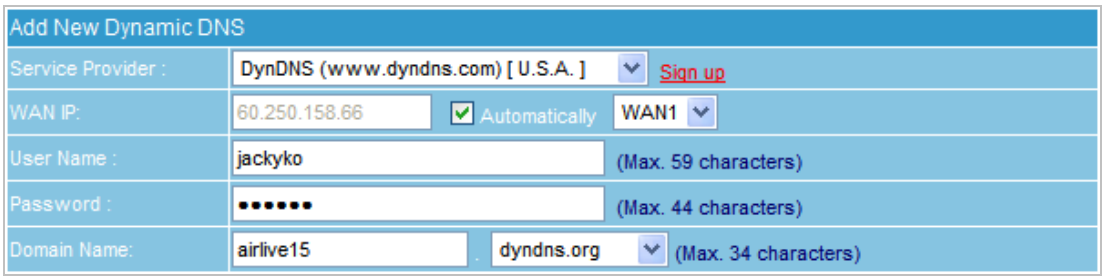


Figure 4-13 DDNS WebUI

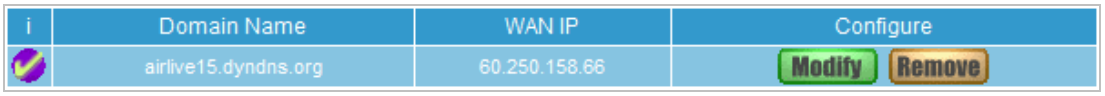


Figure 4-14 Complete DDNS Setting

Chart				
Meaning	Update successfully	Incorrect username or password	Connecting to server	Unknown error

If System Administrator had not registered a DDNS account, click on **Sign up** then can enter the website of the provider.

If you do not select **Automatically fill in the WAN IP** and then you can enter a specific IP in **WAN IP**. DDNS corresponds to that specific IP address.

4.7 Host Table

Host Name:

It can be set by System Manager, to allow internal user accessing the information provided by the host of the domain.

Virtual IP Address:

The virtual IP address is corresponding to the Host. It must be LAN or DMZ IP address.

STEP 1. Select **Host Table** in **Settings** function and click on **New Entry**

- **Host Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address is corresponding to the Host.
- Click **OK** to add Host Table. (Figure 4-15)

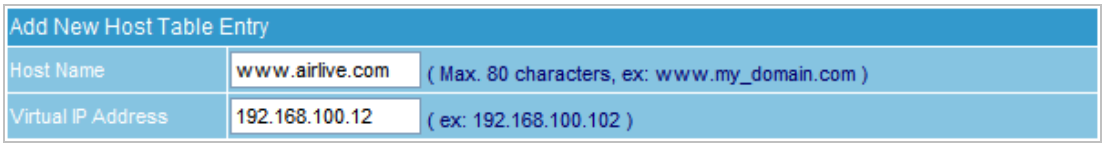


Figure 4-15 Add New Host Table

To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of RS-3000. That is, the default gateway.

4.8 SNMP

STEP 1. Select **SNMP** in **Settings** function, click **Enable SNMP Agent** and type in the following information:

- **Device Name:** The default setting is “Office UTM Gateway”, and user can change it.
- **Device Location:** The default setting is “Taipei, Taiwan”, and user can change it.
- **Community:** The default setting is “public”, and user can change it.
- **Contact Person:** The default setting is “root@public”, and user can change it.
- **Description:** The default setting is “Office UTM gateway Appliance”, and user can change it.
- Click **OK**.
- The SNMP Agent setting is done. So administrator can install SNMP management software on PC and monitor RS-3000 via SNMP Agent. (Figure 4-16)

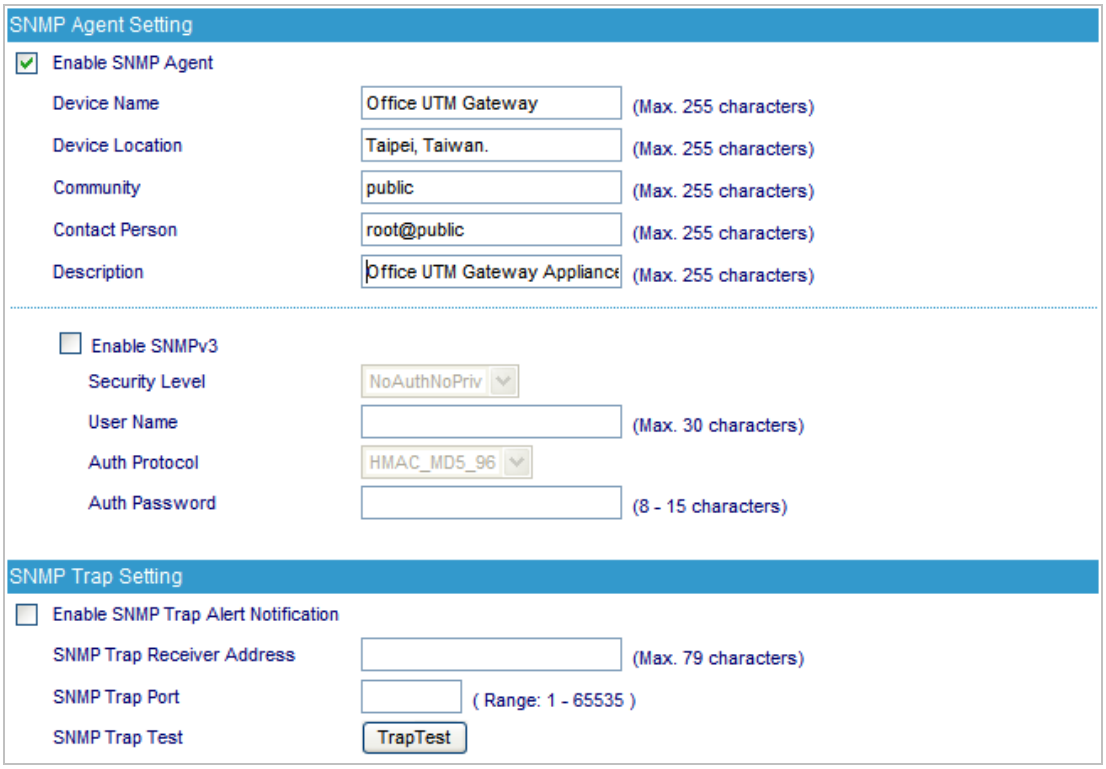


Figure 4-16 SNMP Agent setting

STEP 2. Select **SNMP** in **Settings** function, click **Enable SNMP Trap Alert Notification** and type in the following information:

- **SNMP Trap Receiver Address:** Input SNMP Trap Receiver site of IP address
- **SNMP Trap Port:** Input the port number.
- Click **OK**.
- **SNMP Trap** setting is done. So administrator can receive alert message from PC installed with SNMP management software, via RS-3000 SNMP Trap function. (System will transfer the alert messages to specific IP address, when RS-3000 is attacked by hacker, or connect/disconnect status of line. (Figure 4-17)

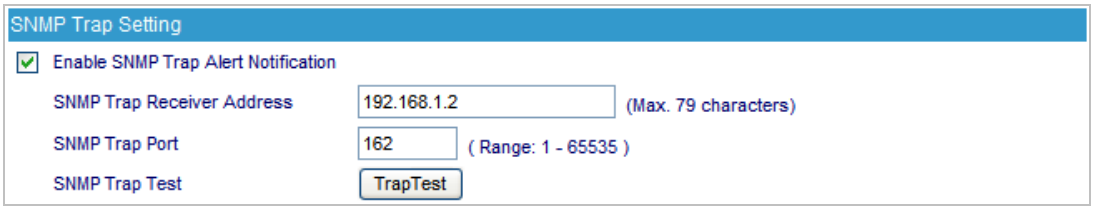


Figure 4-17 SNMP Trap setting

4.9 Language

Select the Language version (**English Version**/ **Traditional Chinese Version** or **Simplified Chinese Version**) and click **OK**. (Figure 4-18)

Figure 4-18 Language Setting WebUI

Chapter 5 Interface

In this section, the Administrator can set up the IP addresses for the office network.

The Administrator may configure the IP addresses of the LAN network, the WAN 1/2 network, and the DMZ network.

The Netmask and gateway IP addresses are also configured in this section.

Define the required fields of Interface

LAN: Using the LAN **Interface**, the Administrator can set up the LAN network of RS-3000.

Ping: Select this function to allow the LAN users to ping the Interface IP Address.

HTTP: Select to enable the user to enter the WebUI of RS-3000 from Interface IP.

WAN: The System Administrator can set up the WAN network of RS-3000.

Balance Mode:

- **Auto:** The RS-3000 will adjust the WAN 1/2 utility rate automatically according to the downstream/upstream of WAN. (For users who are using various download bandwidth)
- **Round-Robin:** The RS-3000 distributes the WAN 1/2 download bandwidth 1:1, in other words, it selects the agent by order. (For users who are using same download bandwidths)
- **By Traffic:** The RS-3000 distributes the WAN 1/2 download bandwidth by accumulative traffic.
- **By Session:** The RS-3000 distributes the WAN 1/2 download bandwidth by saturated connections.
- **By Packet:** The RS-3000 distributes the WAN 1/2 download bandwidth by accumulated packets and saturated connection.
- **By Source IP:** The RS-3000 distributes the WAN 1/2 connection by source IP address, once the connection is built up, all the packets from the same source IP will pass through the same WAN interface.
- **By Destination IP:** The RS-3000 will allocate the WAN connection corresponding to the destination IP, once the connection is built up, all the packets to the same destination IP will pass through the same WAN interface. The connection will be re-assigned with WAN interface when the connections are stopped.

Connect Mode:

- Display the current connection mode:
  - PPPoE (ADSL user)
  - Dynamic IP Address (Cable Modem User)
  - Static IP Address
  - PPTP (European User Only)

Saturated Connections:

- Set the number for saturation whenever session numbers reach it, the RS-3000 switches to the next agent on the list.

Priority:

- Set priority of WAN for Internet Access.

Connection Test:

- The function works to identify WAN port's connection status. The testing ways are as following:
  - **ICMP**：User can define the IP address and RS-3000 will ping the address to verify WAN port's connection status.
  - **DNS**：Another way to verify the connection status by checking the DNS server and Domain Name configured by user.

Upstream/Downstream Bandwidth:

- The System Administrator can set up the correct Bandwidth of WAN network Interface here.

Auto Disconnect:

- The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter "0" means the PPPoE connection will not disconnect at all.

DMZ:

- The Administrator uses the DMZ Interface to set up the DMZ network.
- The DMZ includes:
  - **NAT Mode**：In this mode, the DMZ is an independent virtual subnet. This virtual subnet can be set by the Administrator but cannot be the same as LAN Interface.
  - **Transparent Mode:** In this mode, the DMZ and WAN Interface are in the same subnet.

5.1 LAN

Modify LAN Interface Settings

STEP 1 **.** Select **LAN** in **Interface** and enter the following setting:

- Enter the new **IP Address** and **Netmask**
- Select **Ping** and **HTTP**
- Click **OK** (Figure 5-1)

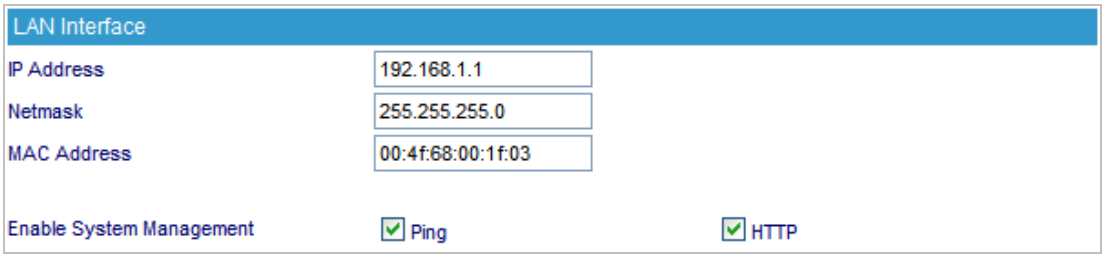


Figure 5-1 Setting LAN Interface WebUI

The default LAN IP Address is 192.168.1.1. After the Administrator setting the new LAN IP Address on the computer , he/she have to restart the System to make the new IP address effective. (when the computer obtain IP by DHCP)

Do not cancel WebUI selection before not setting Permitted IPs yet. It will cause the Administrator cannot be allowed to enter the RS-3000 WebUI from LAN.

5.2 WAN

Setting WAN Interface Address

STEP 1 **.** Select **WAN** in **Interface** and click **Modify** in **WAN1 Interface.**

The setting of WAN2 Interface is almost the same as WAN1. The difference is that WAN2 has a selection of **Disable**. The System Administrator can close WAN2 Interface by this selection. (Figure 5-2)

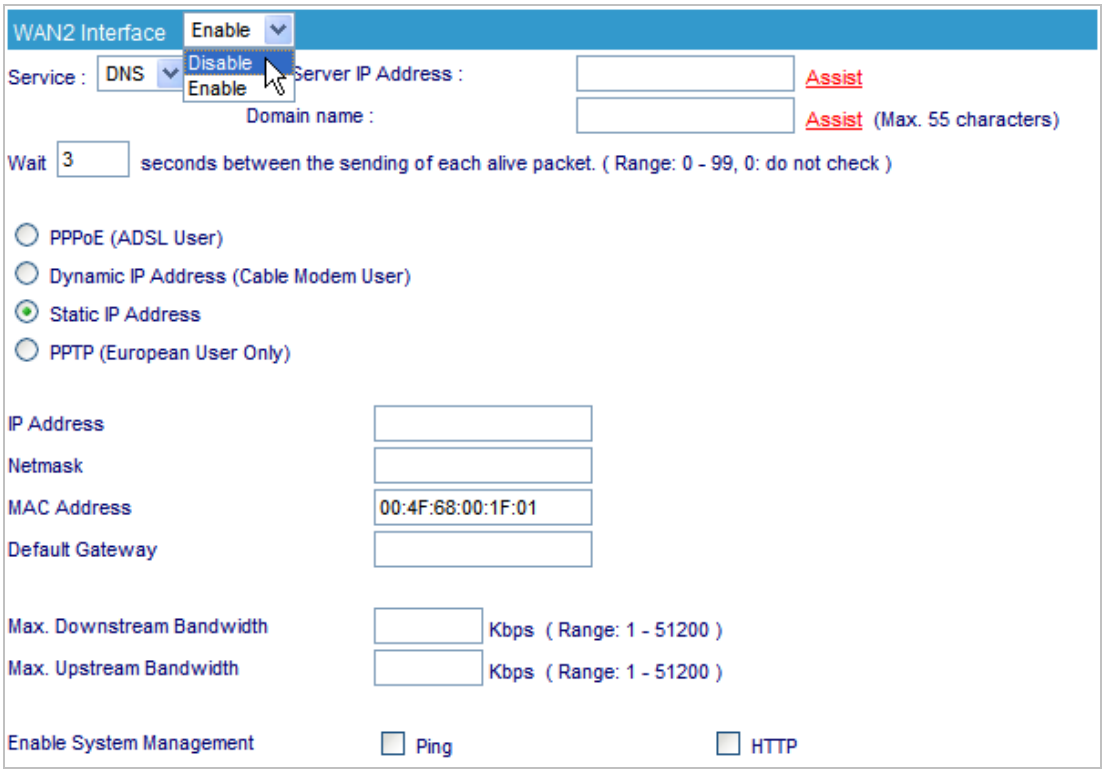


Figure 5-2 Disable WAN2 Interface

STEP 2 . Setting the Connection Service (ICMP or DNS way)：

- **ICMP**：Enter an Alive Indicator Site IP (can select from **Assist**) (Figure 5-3)
- **DNS**：Enter two different DNS Server IP Address and Domain Name (can select from **Assist**) (Figure 5-4)
- Setting time of seconds between sending alive packet.

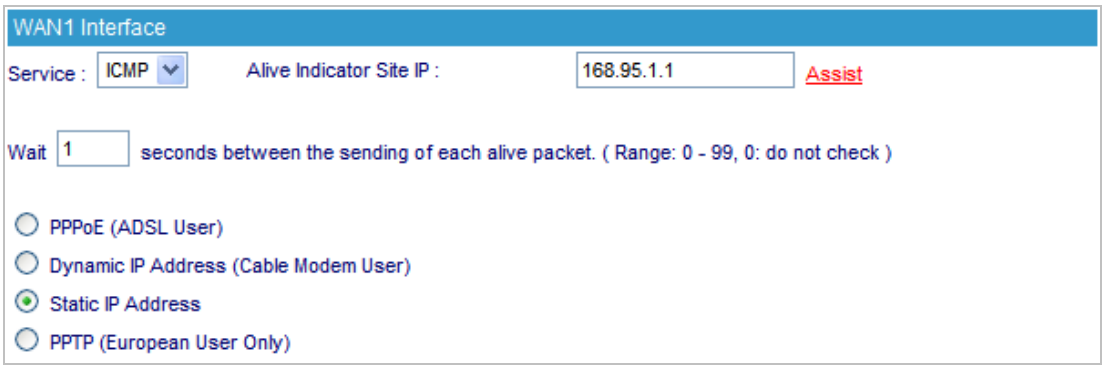


Figure 5-3 ICMP Connection

Figure 5-4 DNS Service

Connection test is used for RS-3000 to detect if the WAN can connect or not. So the **Alive Indicator Site IP**, **DNS Server IP Address**, or **Domain Name** must be able to use permanently. Or it will cause judgmental mistakes of the device.

STEP 3 . Select the Connecting way:

- **PPPoE (ADSL User)** (Figure 5-5):

1. Select **PPPoE**
2. Enter **User Name** as an account
3. Enter **Password** as the password
4. Select **Dynamic** or **Fixed** in **IP Address provided by ISP**.
   If you select Fixed, please enter IP Address, Netmask, and Default Gateway.
5. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth**. (According to the flow that user apply)
6. Select **Ping** and **HTTP**
7. Click **OK** (Figure 5-6)

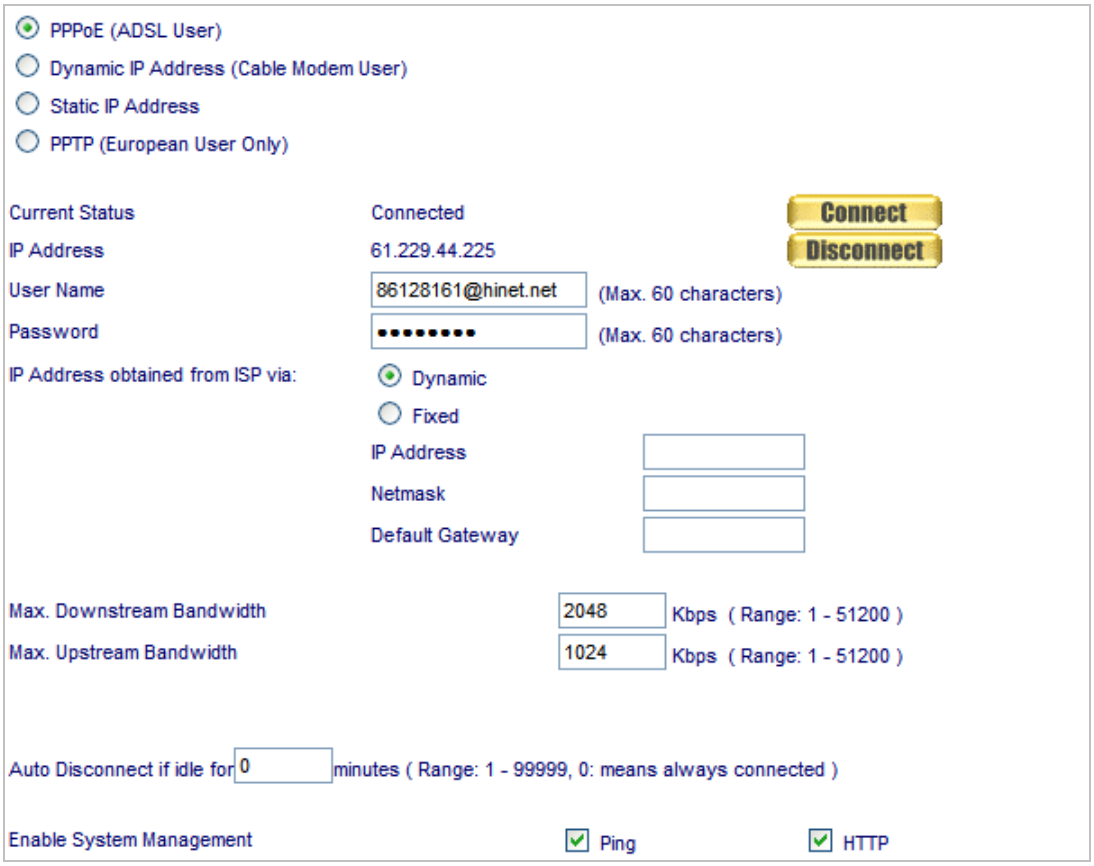


Figure 5-5 PPPoE Connection

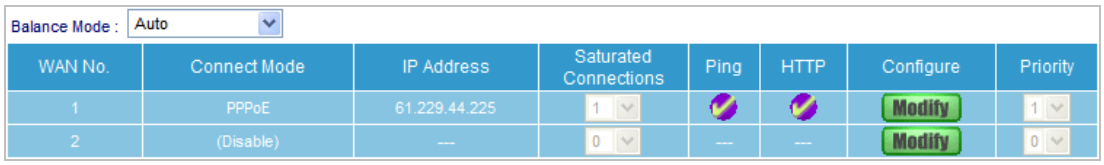


Figure 5-6 Complete PPPoE Connection Setting

You can set up **Auto Disconnect if idle**, in order to disconnect the PPPoE when the idle time is up, and save the network expense.

- **Dynamic IP Address (Cable Modem User)** (Figure 5-7)**:**

1. Select **Dynamic IP Address (Cable Modem User)**
2. Click **Renew** in the right side of IP Address and then can obtain IP automatically.
3. If the MAC Address is required for ISP then click on **Clone MAC Address** to obtain MAC IP automatically.
4. **Hostname:** Enter the hostname provided by ISP.
5. **Domain Name:** Enter the domain name provided by ISP.
6. **User Name** and **Password** are the IP distribution method according to Authentication way of DHCP + protocol
7. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow applied by user)
8. Select **Ping** and **HTTP**
9. Click **OK** (Figure 5-8)

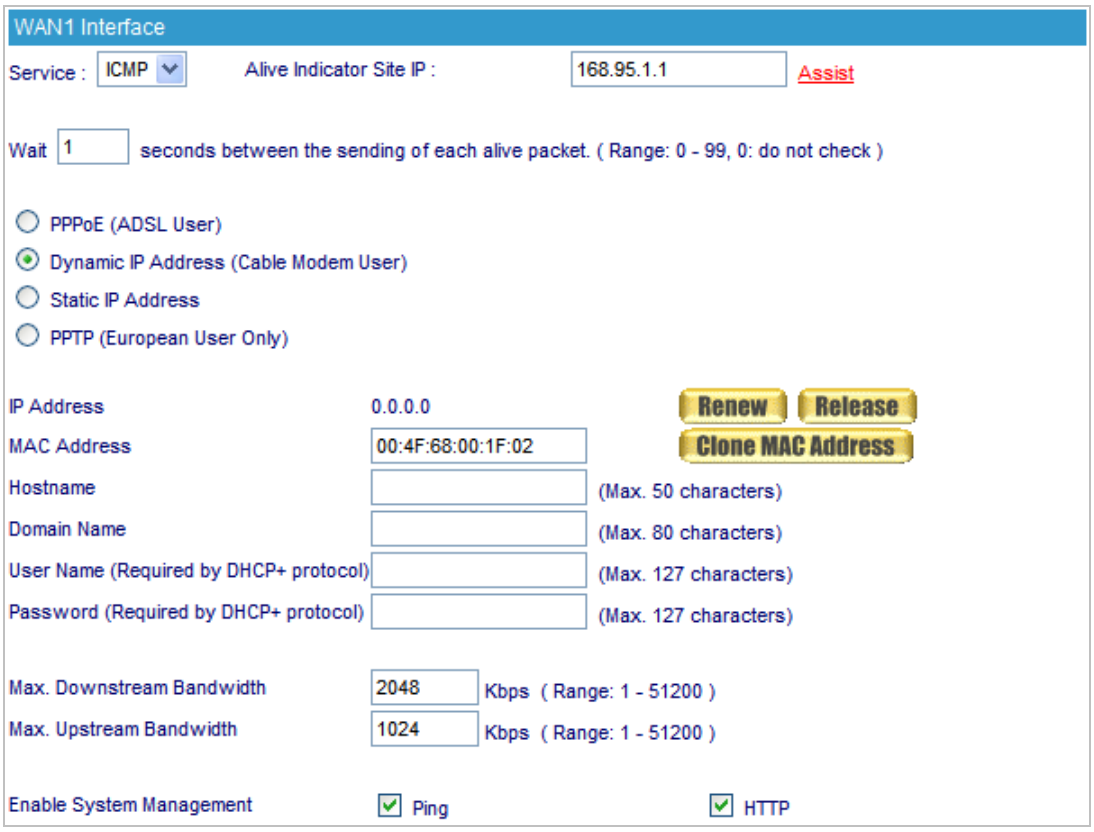


Figure 5-7 Dynamic IP Address Connection

Figure 5-8 Complete Dynamic IP Connection Setting

- **Static IP Address** (Figure 5-9)
  1. Select **Static IP Address**
  2. Enter **IP Address**, **Netmask**, and **Default Gateway** that provided by ISP
  3. Enter **DNS Server1** and **DNS Server2**

In WAN2, the connecting of Static IP Address does not need to set DNS Server

  4. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow applied by user)
  5. Select **Ping** and **HTTP**
  6. Click **OK** (Figure 5-10)

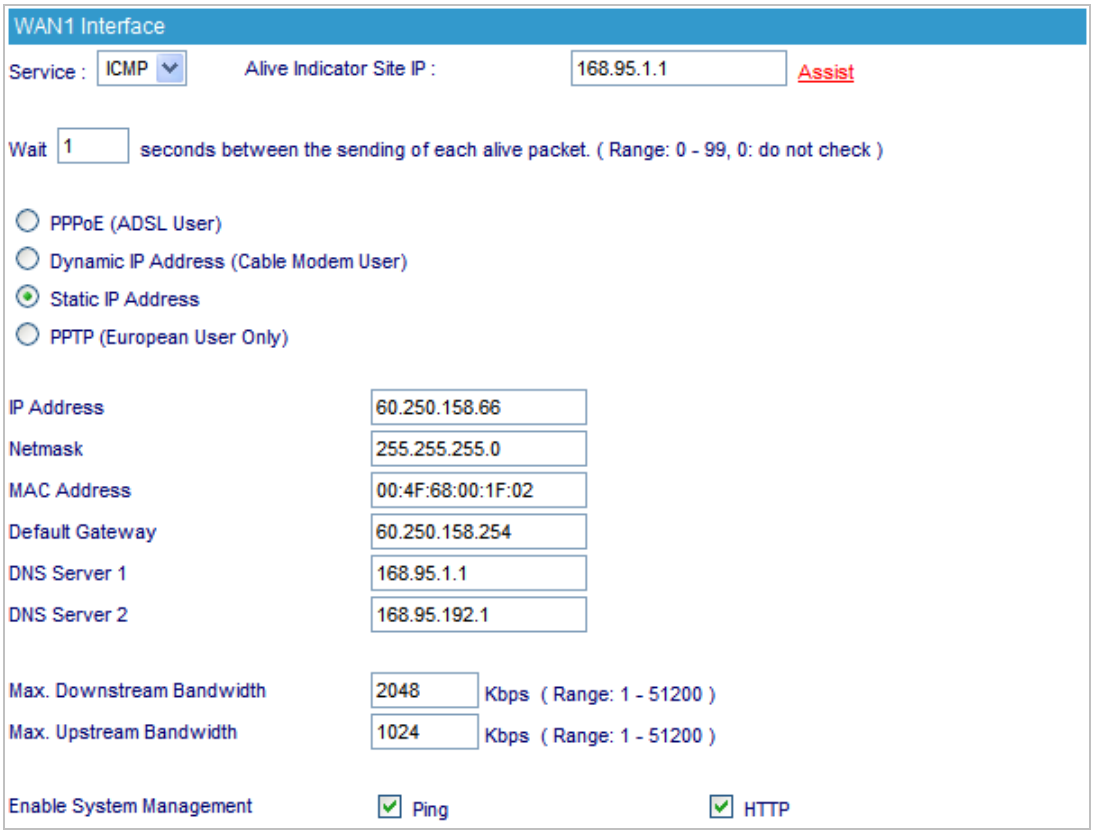


Figure 5-9 Static IP Address Connection

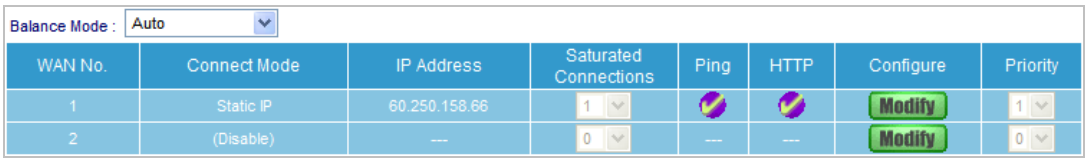


Figure 5-10 Complete Static IP Address Connection Setting

When selecting **Ping** and **WebUI** on **WAN** network Interface, users will be able to ping the RS-3000 and enter the WebUI WAN network. It may influence network security. The suggestion is to **Cancel Ping** and **WebUI** after all the settings have finished. And if the System Administrator needs to enter UI from WAN, he/she can use **Permitted IPs** to enter.

- **PPTP (European User Only)** (Figure 5-11)**:**
  1. Select **PPTP (European User Only)**
  2. Enter **User Name** as an account.
  3. Enter **Password** as the password.
  4. If the MAC Address is required for ISP then click on **Clone MAC Address** to obtain MAC IP automatically.
  5. Select **Obtain an IP address automatically** or **Use the following IP address** provided by ISP.
  6. **Hostname:** Enter the hostname provided by ISP.
  7. **Domain Name:** Enter the domain name provided by ISP.
  8. If user selects **Use the following IP address**, please enter IP Address, Netmask, and Default Gateway.
  9. Enter PPTP server IP address as the **PPTP Gateway** provided by ISP.
  10. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow applied by user)
  11. Select **BEZEQ-ISRAEL (Israel User Only)**
  12. Select **Ping** and **HTTP**
  13. Click **OK** (Figure 5-12)


You can choose **Service-On-Demand** for WAN Interface to connect automatically when disconnect; or to set up **Auto Disconnect if idle** (not recommend)

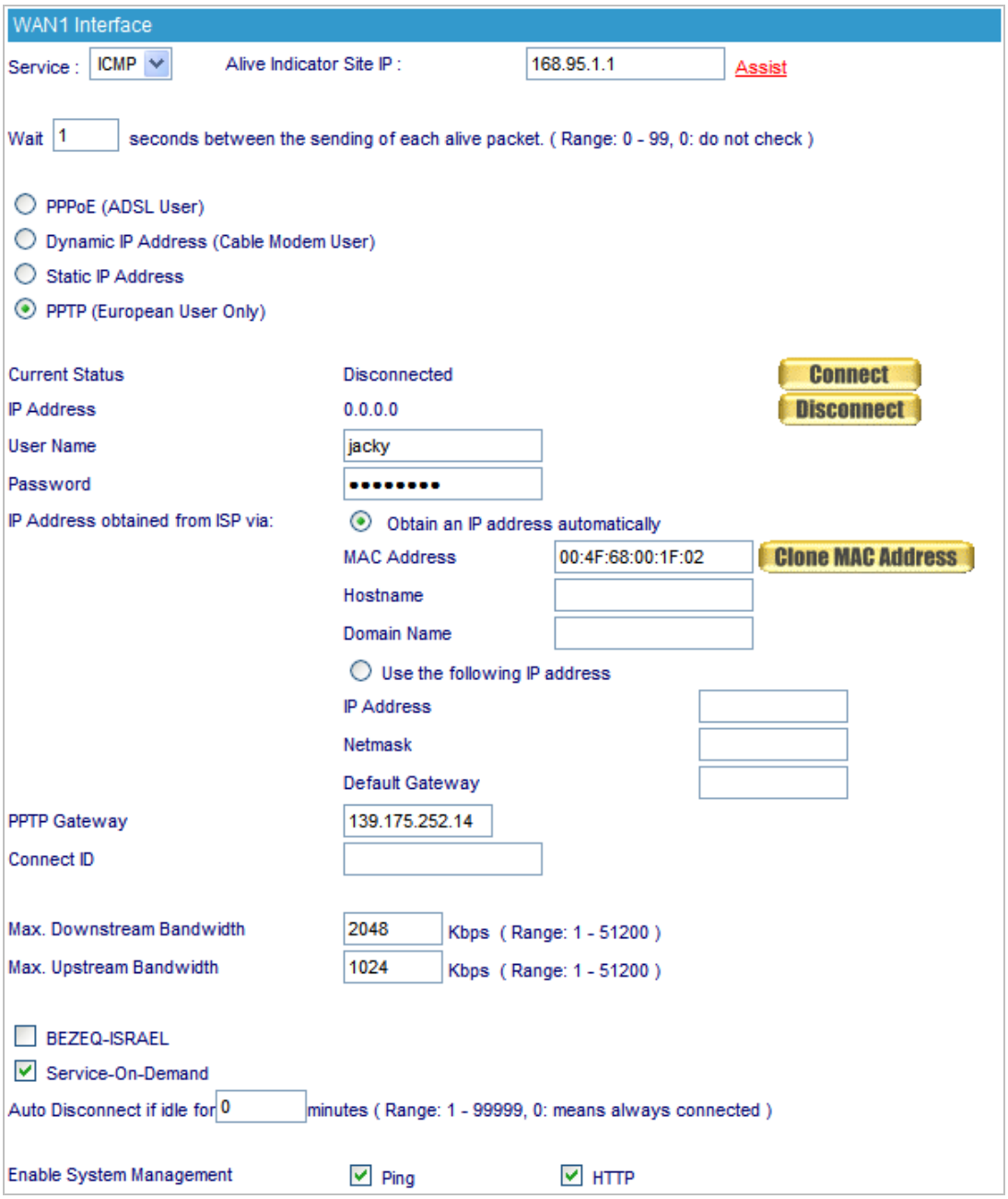


Figure 5-11 PPTP Connection

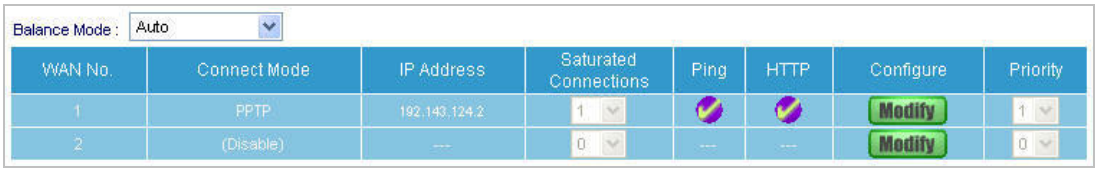


Figure 5-12 Complete PPTP Connection Setting

5.3 DMZ

Setting DMZ Interface Address (NAT Mode)

STEP 1 . Click **DMZ** Interface

STEP 2 . Select NAT Mode in DMZ Interface

- Select **NAT** in **DMZ Interface**
- Enter **IP Address** and **Netmask**

STEP 3 . Select **Ping** and **HTTP**

STEP 4 . Click **OK** (Figure 5-13)

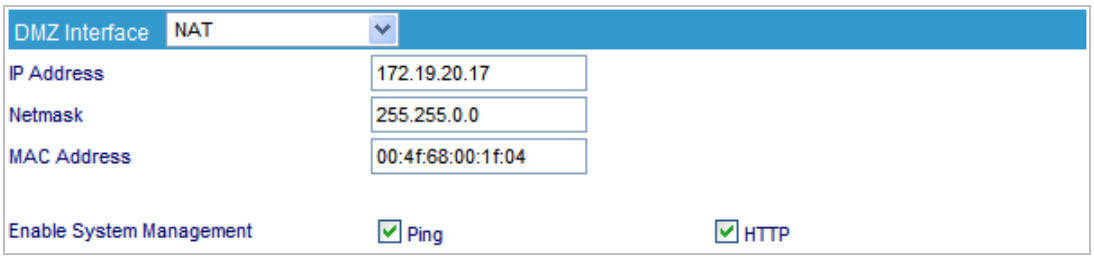


Figure 5-13 Setting DMZ Interface Address (NAT Mode) WebUI

Setting DMZ Interface Address (Transparent Mode)

STEP 1 . Select **DMZ** Interface

STEP 2 . Select Transparent Mode in DMZ Interface

- Select **DMZ_Transparent** in **DMZ Interface**

STEP 3 . Select **Ping** and **HTTP**

STEP 4 . Click **OK** (Figure 5-14)

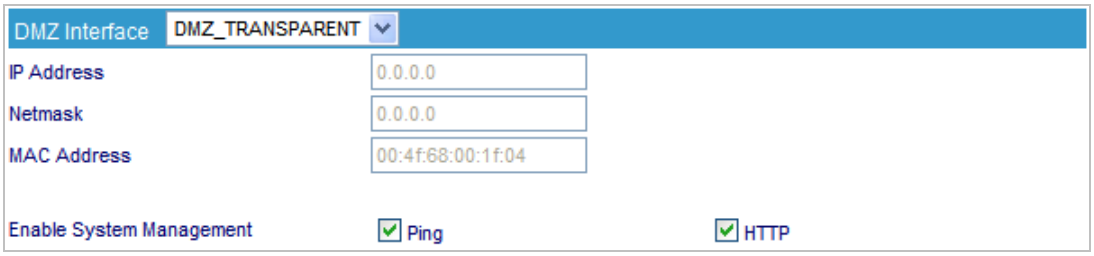


Figure 5-14 Setting DMZ Interface Address (Transparent Mode) WebUI

In WAN, the connecting way must be **Static IP Address** and can choose **Transparent Mode** in **DMZ.**

Chapter 6 Address

The RS-3000 allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN network, WAN network group, DMZ and DMZ group.

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address or DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN Group or the WAN 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 setup 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.

Define the required fields of Address

Name:

- The System Administrator set up a name as IP Address that is easily recognized.

IP Address:

- It can be a PC's IP Address or several IP Address of Subnet. Different network area can be: Internal IP Address, External IP Address, and DMZ IP Address.

Netmask:

- When correspond to a specific IP, it should be set as: 255.255.255.255.
- When correspond to several IP of a specific Domain. Take 192.168.100.1 (C Class subnet) as an example, it should be set as: 255.255.255.0.

MAC Address:

- Correspond a specific PC's MAC Address to its IP; it can prevent users changing IP and accessing to the net service through policy without authorizing.

Get Static IP address from DHCP Server:

- When enable this function and then the IP obtain from DHCP Server automatically under LAN or DMZ will be distributed to the IP that correspond to the MAC Address.

6.1 LAN

Under DHCP situation, assign the specific IP to static users and restrict them to access FTP net service only through policy

STEP 1 **.** Select **LAN** in **Address** and enter the following settings:

- Click **New Entry** button (Figure 6-1)
- **Name:** Enter Jacky
- **IP Address:** Enter 192.168.3.2
- **Netmask:** Enter 255.255.255.255
- **MAC Address :** Enter the user's MAC Address (00:18:F3:F5:D3:54)
- Select **Get static IP address from DHCP Server**
- Click **OK** (Figure 6-2)

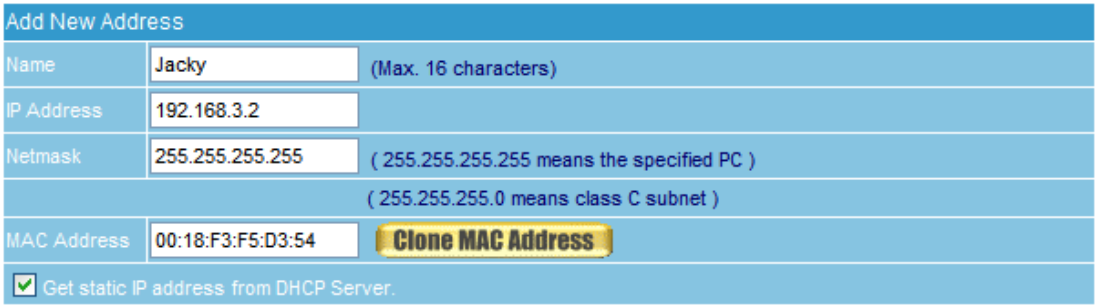


Figure 6-1 Setting LAN Address Book WebUI

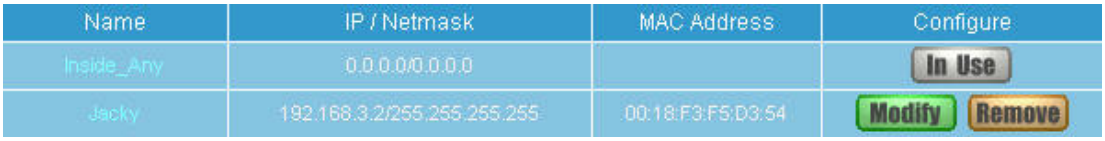


Figure 6-2 Complete the Setting of LAN

STEP 2 . Adding the following setting in **Outgoing Policy**: (Figure 6-3)

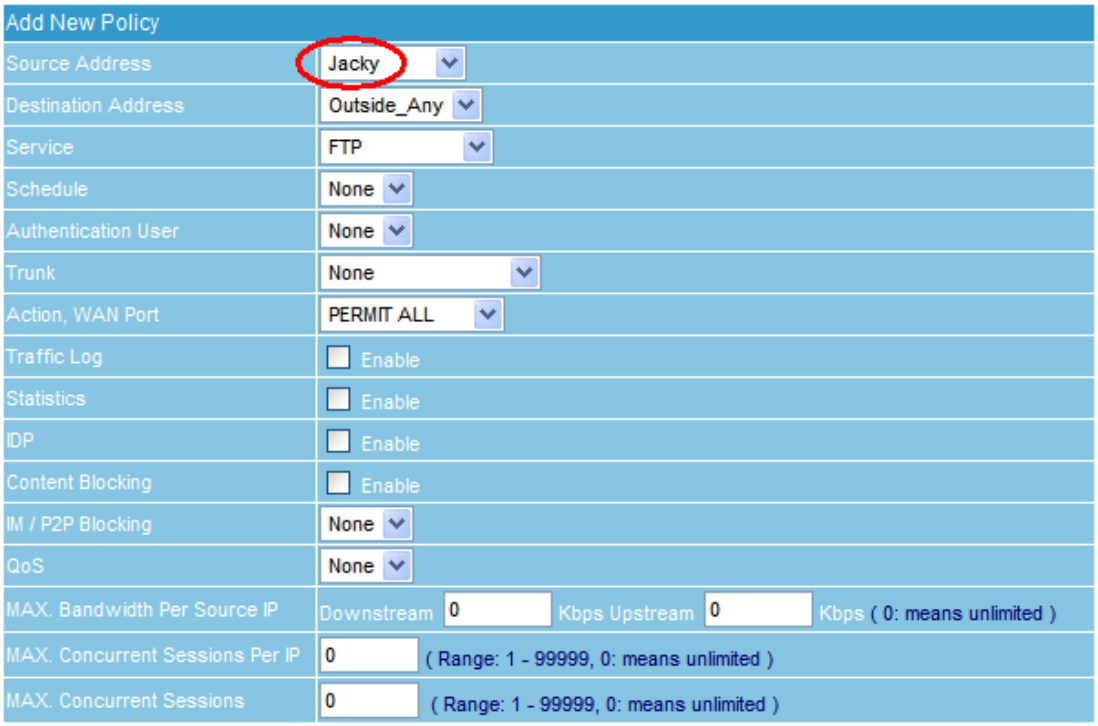


Figure 6-3 Add a Policy of Restricting the Specific IP to Access to Internet

STEP 3 . Complete assigning the specific IP to static users in **Outgoing Policy** and restrict them to access FTP net service only through policy: (Figure 6-4)

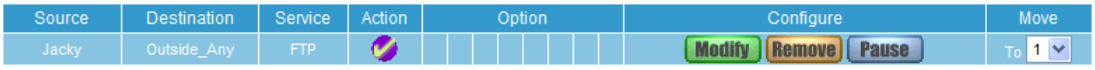


Figure 6-4 Complete the Policy of Restricting the Specific IP to Access to Internet

When the System Administrator setting the **Address** Book, he/she can choose the way of clicking on Clone MAC Address to make the RS-3000 to fill out the user's MAC Address automatically.

In **LAN** of **Address** function, the RS-3000 will default an **Inside Any** address represents the whole LAN network automatically. Others like **WAN, DMZ** also have the **Outside Any** and **DMZ Any** default address setting to represent the whole subnet.

The setting mode of **WAN** and **DMZ** of **Address** are the same as **LAN**; the only difference is **WAN** cannot set up MAC Address.

6.2 LAN Group

Setup a policy that only allows partial users to connect with specific IP (External Specific IP)

STEP 1 . Setting several LAN network Address. (Figure 6-5)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Jacky	192.168.1.2/255.255.255.255	00:18:F3:F5:D3:54	In Use
John	192.168.1.4/255.255.255.255		Modify Remove
James	192.168.1.5/255.255.255.255		Modify Remove
Evelyn	192.168.1.7/255.255.255.255	00:D0:59:59:79:2D	Modify Remove
Michael	192.168.1.8/255.255.255.255		Modify Remove

Figure 6-5 Setting Several LAN Network Address

STEP 2. Enter the following settings in **LAN Group** of **Address**:

- Click **New Entry** (Figure 6-6)
- Enter the **Name** of the group
- Select the users in the **Available Address** column and click **Add**
- Click **OK** (Figure 6-7)

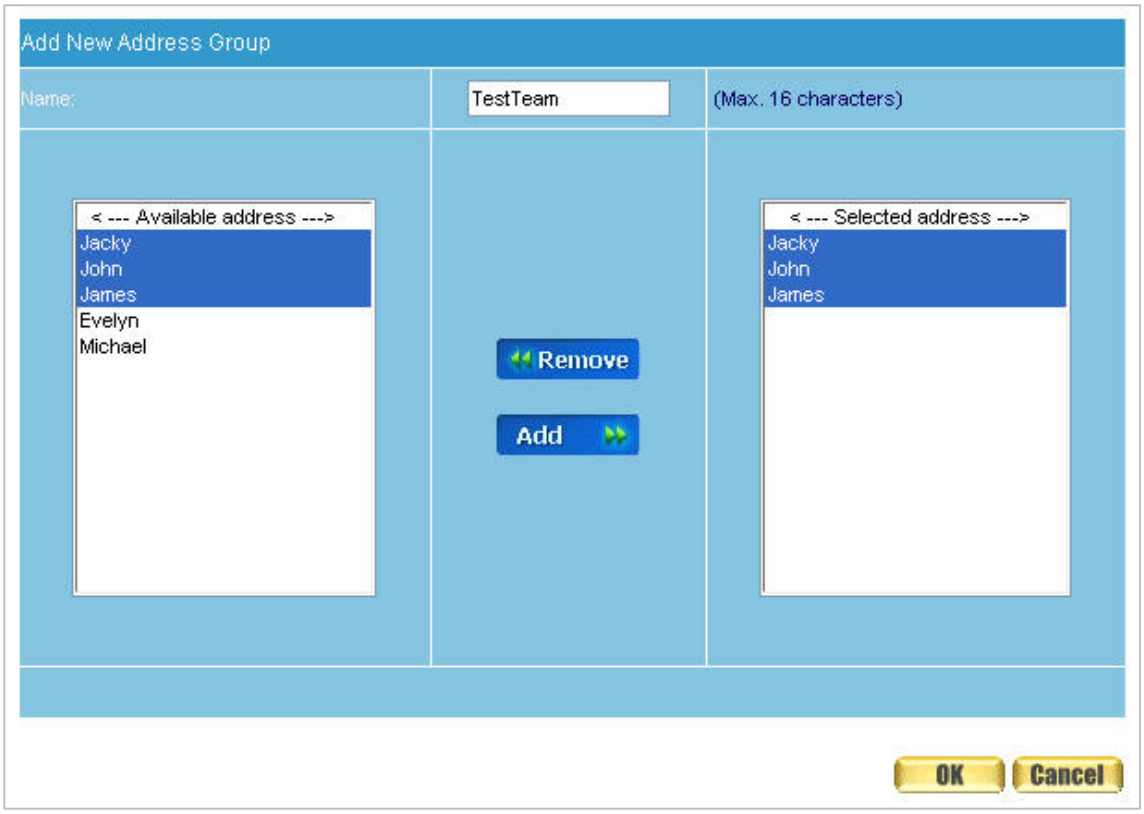


Figure 6-6 Add New LAN Address Group

Figure 6-7 Complete Adding LAN Address Group

The setting mode of **WAN Group** and **DMZ Group** of **Address** are the same as **LAN Group**.

STEP 3 **.** Enter the following settings in **WAN** of **Address** function:

- Click **New Entry** (Figure 6-8)
- Enter the following data (**Name, IP Address, Netmask**)
- Click **OK** (Figure 6-9)

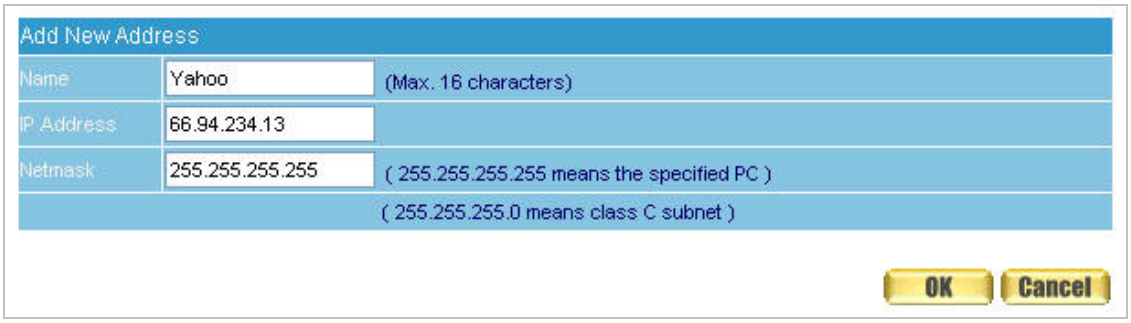


Figure 6-8 Add New WAN Address

Figure 6-9 Complete the Setting of WAN Address

STEP 4 . To exercise STEP1~3 in **Policy** (Figure 6-10, 6-11)

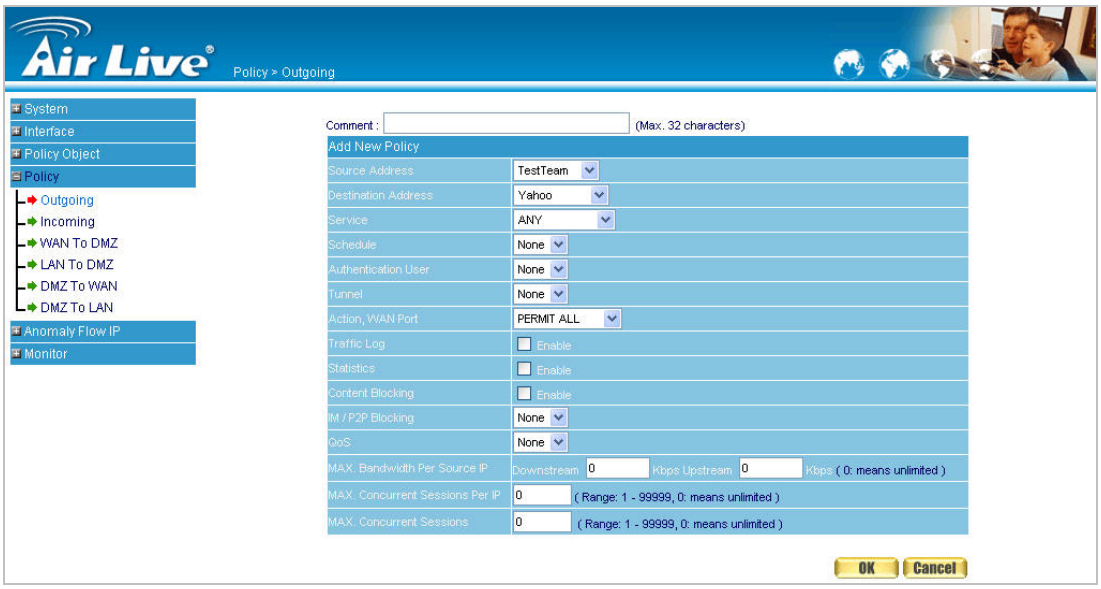


Figure 6-10 To Exercise Address Setting in Policy

Figure 6-11 Complete the Policy Setting

The **Address** function really take effect only if use with **Policy**.

Chapter 7 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), SMTP (25), POP3 (110), etc. The RS-3000 includes 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 65535

In this chapter, 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.

 How to 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.

7.1 Pre-defined

Define the required fields of Service

Pre-defined WebUI's Chart and Illustration:

Chart	Illustration
ANY	Any Service
TCP	TCP Service, For example：AFPoverTCP, AOL, BGP, FTP, FINGER, HTTP, HTTPS, IMAP, SMTP, POP3, GOPHER, InterLocator, IRC, L2TP, LDAP, NetMeeting, NNTP, PPTP, Real-Media, RLOGIN, SSH, TCP-ANY, TELNET, VDO-Live, WAIS, WINFRAME, X-WINDOWS, MSN, …etc.
UDP	UDP Service, For example：IKE, DNS, NFS, NTP, PC-Anywhere, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP,…etc.
ICMP	ICMP Service, Foe example：PING, TRACEROUTE…etc.

Define the required fields of Service

New Service Name:

- The System Manager can name the custom service.

Protocol:

- The protocol type to be used in connection for device, such as TCP and UDP mode

Client Port:

- The port number of network card of clients. (The range is 0 ~ 65535, suggest to use the default range)

Server Port:

- The port number of custom service

7.2 Custom

Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)

STEP 1 **.** Set **LAN** and **LAN Group** in **Address** function as follows: (Figure 7-1, 7-2)

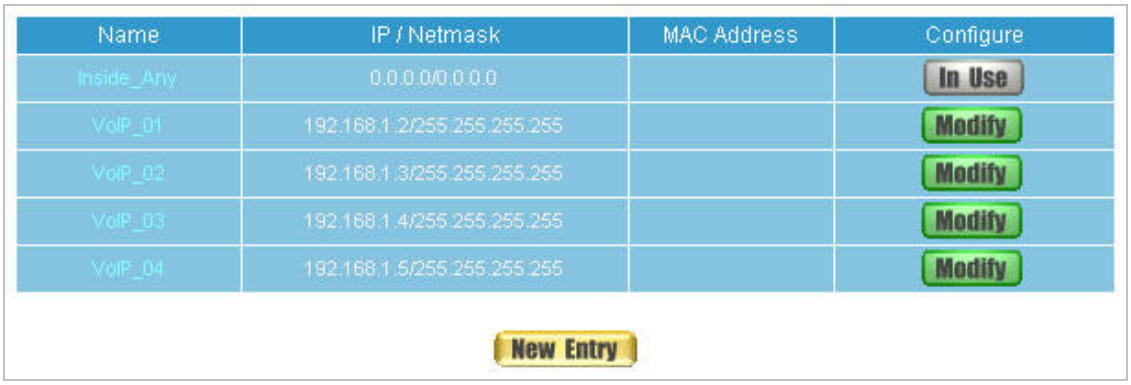


Figure 7-1 Setting LAN Address Book WebUI

Figure 7-2 Setting LAN Group Address Book WebUI

STEP 2 **.** Enter the following setting in **Custom** of **Service** function:

- Click **New Entry** (Figure 7-3)
- **Service Name**: Enter the preset name VoIP
- Protocol#1 select **TCP,** need not to change the **Client Port,** and set the **Server Port** as: 1720:1720
- Protocol#2 select **TCP**, need not to change the **Client Port,** and set the **Server Port** as: 15328:15333
- Protocol#3 select **UDP**, need not to change the **Client Port,** and set the **Server Port** as: 15328:15333
- Click **OK** (Figure 7-4)

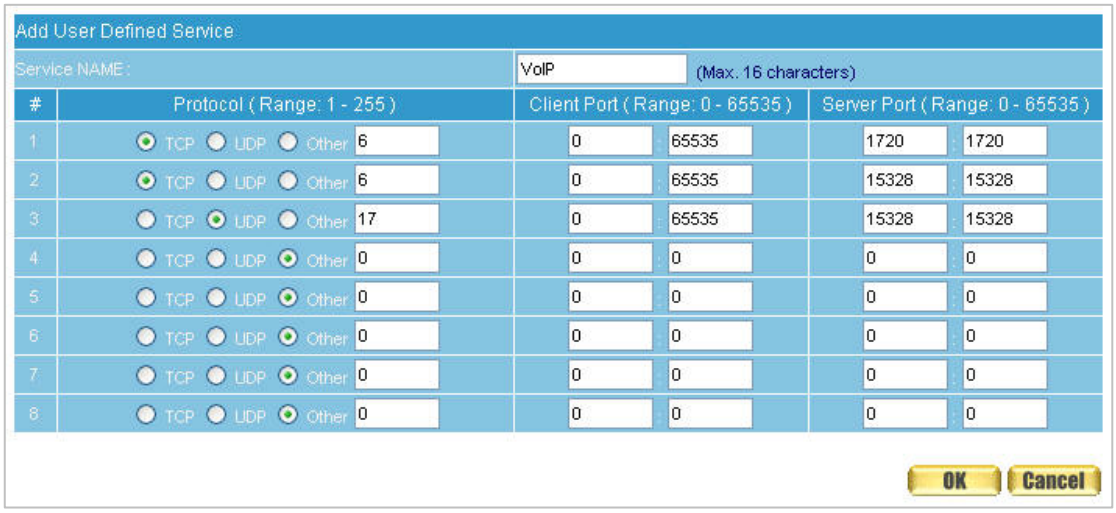


Figure 7-3 Add User Define Service

Figure 7-4 Complete the Setting of User Define Service of VoIP

Under general circumstances, the range of port number of client is 0-65535. Change the client range in **Custom** of is not suggested.

If the port numbers that enter in the two spaces are different port number, then enable the port number under the range between the two different port numbers (for example: 15328:15333). And if the port number that enters in the two spaces are the same port number, then enable the port number as one (for example: 1720:1720).

STEP 3 . Compare **Service** to **Virtual Server.** (Figure 7-5)

Figure 7-5 Compare Service to Virtual Server

STEP 4 . Compare **Virtual Server** to **Incoming Policy**. (Figure 7-6)

Figure 7-6 Complete the Policy for External VoIP to Connect with Internal VoIP

STEP 5 . In **Outgoing Policy**, complete the setting of internal users using VoIP to connect with external network VoIP: (Figure 7-7)

Figure 7-7 Complete the Policy for Internal VoIP to Connect with External VoIP

Service must cooperate with **Policy** and **Virtual Server** that the function can take effect.

7.3 Group

Setting service group and restrict the specific users only can access to service resource that provided by this group through policy (Group: HTTP, POP3, SMTP, DNS)

STEP 1 **.** Enter the following setting in **Group** of **Service**:

- Click **New Entry** (Figure 7-8)
- **Name:** Enter Main_Service
- Select HTTP, POP3, SMTP, DNS in **Available Service** and click **Add**
- Click **OK** (Figure 7-9)

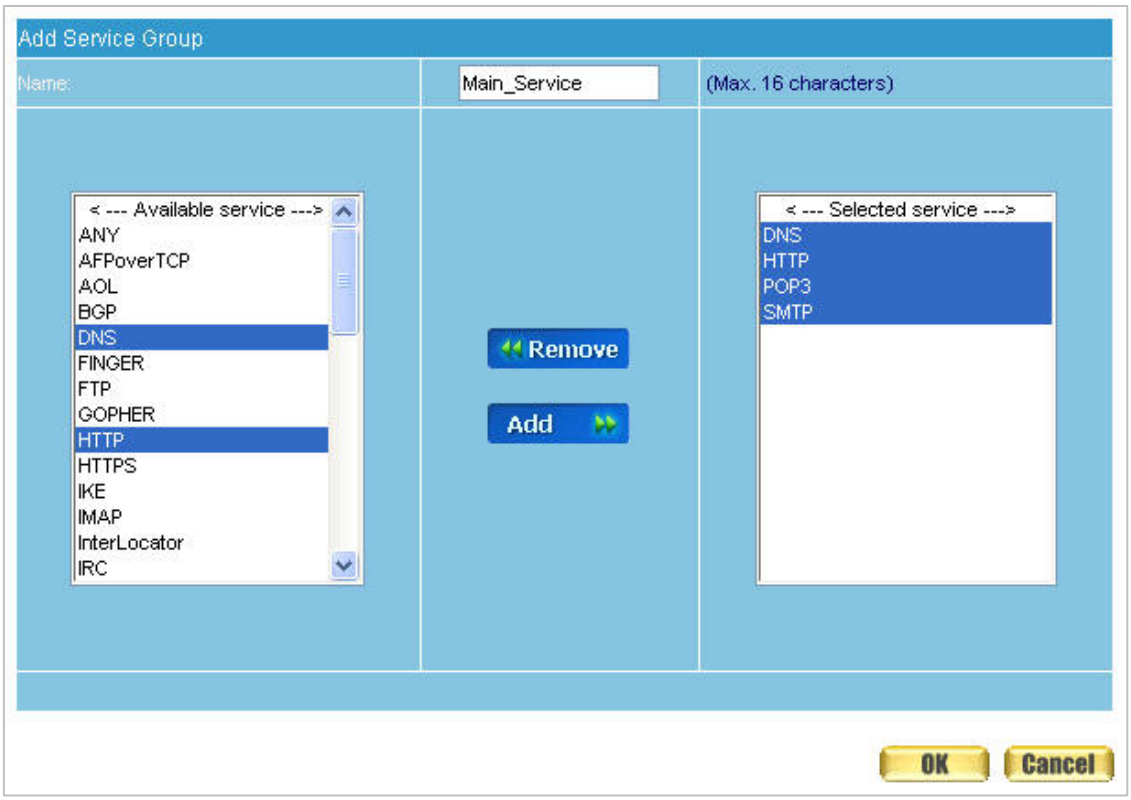


Figure 7-8 Add Service Group

Figure 7-9 Complete the setting of Adding Service Group

If you want to remove the service you choose from **Selected Service**, choose the service you want to delete and click **Remove**.

STEP 2 **.** In **LAN Group** of **Address** function, set up an **Address Group** that can include the service of access to Internet. (Figure 7-10)

Figure 7-10 Setting Address Book Group

STEP 3 **.** Compare **Service Group** to **Outgoing Policy.** (Figure 7-11)

Figure 7-11 Setting Policy

Chapter 8 Schedule

In this chapter, the RS-3000 provides the Administrator to configure a schedule for policy to take effect and allow the policies to be used at those designated times. And then the Administrator can set the start time and stop time or VPN connection in Policy or VPN. By using the Schedule function, the Administrator can save a lot of management time and make the network system most effective.

 How to use the Schedule?

The system Administrator can use schedule to set up the device to carry out the connection of Policy or VPN during several different time division automatically.

To configure the valid time periods for LAN users to access to Internet in a day

STEP 1 **.** Enter the following in **Schedule**:

- Click **New Entry** (Figure 8-1)
- Enter **Schedule Name**
- Set up the working time of Schedule for each day
- Click **OK** (Figure 8-2)

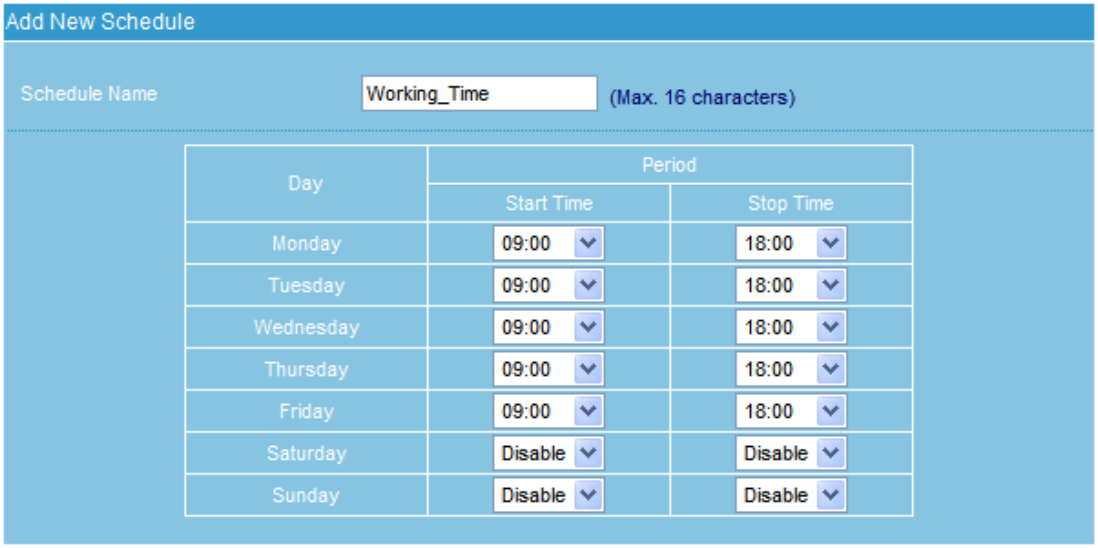


Figure 8-1 Setting Schedule WebUI

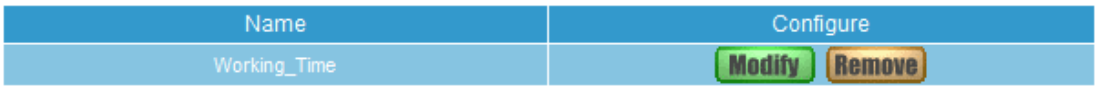


Figure 8-2 Complete the Setting of Schedule

STEP 2 **.** Compare **Schedule** with **Outgoing Policy** (Figure 8-3)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)

Figure 8-3 Complete the Setting of Comparing Schedule with Policy

The Schedule must compare with **Policy**.

Chapter 9 QoS

By configuring the QoS, you can control the OutBound and InBound Upstream/Downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth.

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

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

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

The RS-3000 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The RS-3000 also makes it convenient for the administrator to make the Bandwidth to reach the best utility. (Figure 9-1, 9-2)

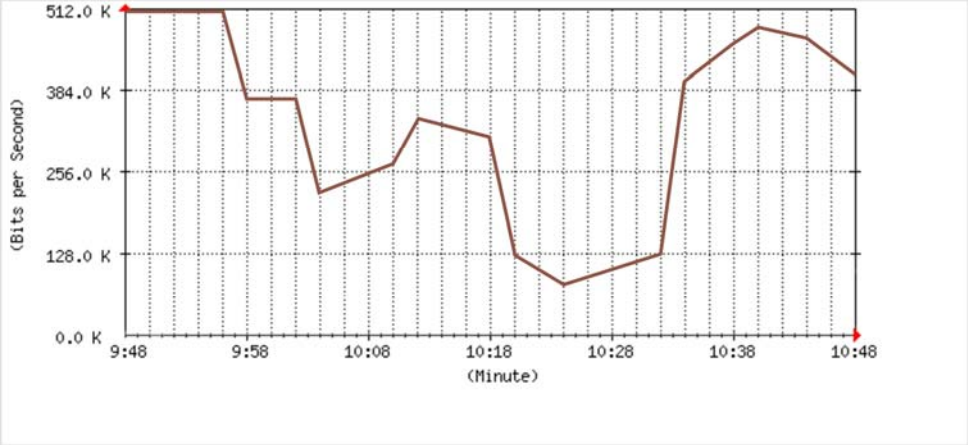


Figure 9-1 the Flow Before Using QoS

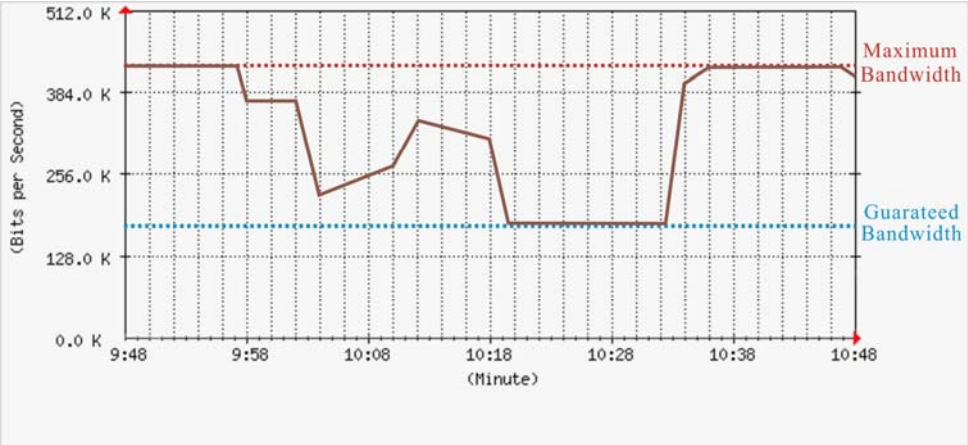


Figure 9-2 the Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

Define the required fields of QoS

WAN:

- Display WAN1 and WAN2

Downstream Bandwidth:

- To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you applied from ISP

Upstream Bandwidth:

- To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you applied from ISP

Priority:

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

Guaranteed Bandwidth:

- The basic bandwidth of QoS. The connection that uses the IPSec Autokey of VPN or Policy will preserve the basic bandwidth.

Maximum Bandwidth:

- The maximum bandwidth of QoS. The connection that uses the IPSec Autokey of VPN or Policy, which bandwidth will not exceed the amount you set.

Setting a policy that can restrict the user's downstream and upstream bandwidth

STEP 1 . Enter the following settings in **QoS**:

- Click **New Entry** (Figure9-3)
- **Name:** The name of the QoS you want to configure.
- Enter the bandwidth in WAN1, WAN2
- Select **QoS Priority**
- Click **OK** (Figure9-4)

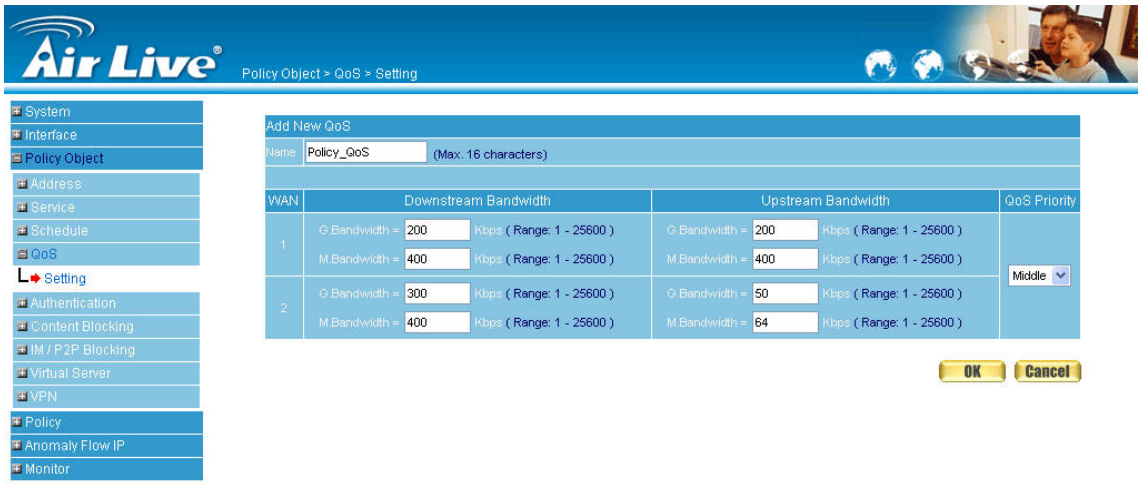


Figure9-3 QoS WebUI Setting

Figure9-4 Complete the QoS Setting

STEP 2 . Use the QoS that set by STEP1 in **Outgoing Policy.** (Figure9-5, 9-6)

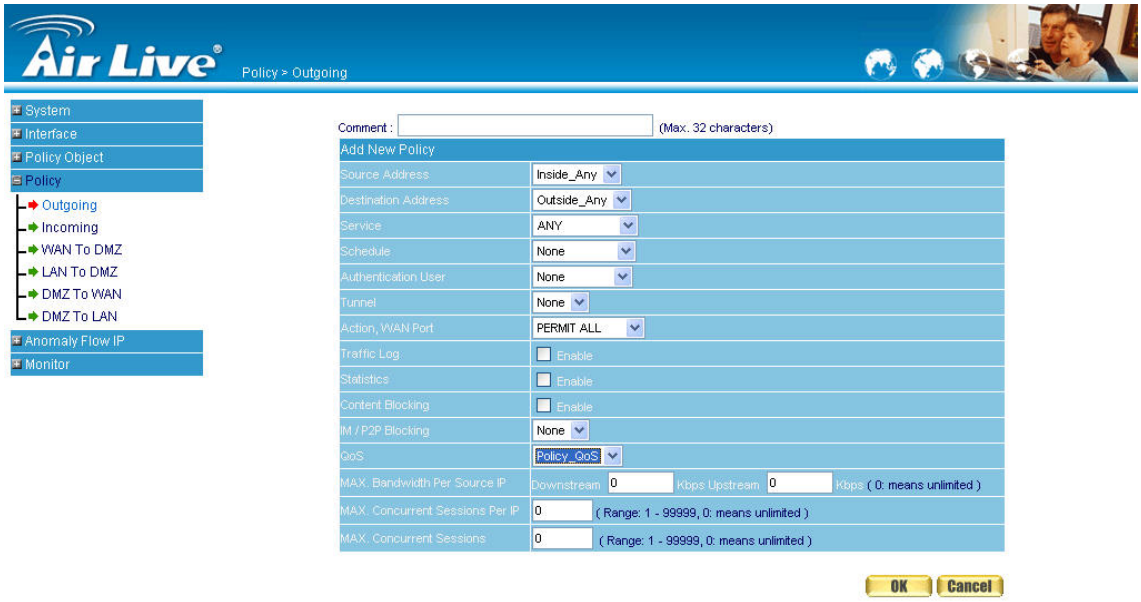


Figure9-5 Setting the QoS in Policy

Figure9-6 Complete Policy Setting

When the administrator are setting QoS, the bandwidth range that can be set is the value that system administrator set in the **WAN** of **Interface**. So when the System Administrator sets the downstream and upstream bandwidth in **WAN** of **Interface**, he/she must set up precisely.

Chapter 10 Authentication

By configuring the Authentication, you can control the user's connection authority. The user has to pass the authentication to access to Internet.

The RS-3000 configures the authentication of LAN's user by setting account and password to identify the privilege.

Define the required fields of Authentication

Authentication Management

- Provide the Administrator the port number and valid time to setup RS-3000 authentication. (Have to setup the Authentication first)
  - **Authentication Port:** The port number to allow internal users to connect to the authentication page. The port number is allowed to be changed.
  - **Re-Login if Idle:** The function works to force internal user to login again when the idle time is exceeded after passing the authentication. The default value is 30 minutes.
  - **Re-Login after user login successfully:** The function works to permit user to re-login within a period of time. The default value is 0, means unlimited.
  - **URL to redirect when authentication succeed:** The function works to redirect the homepage to the specific website, after the user had passes Authentication. The default value is blank.
  - **Messages to display when user login:** It will display the login message in the authentication WebUI. (Support HTML) The default value is blank (display no message in authentication WebUI)

- Add the following setting in this function: (Figure10-1)

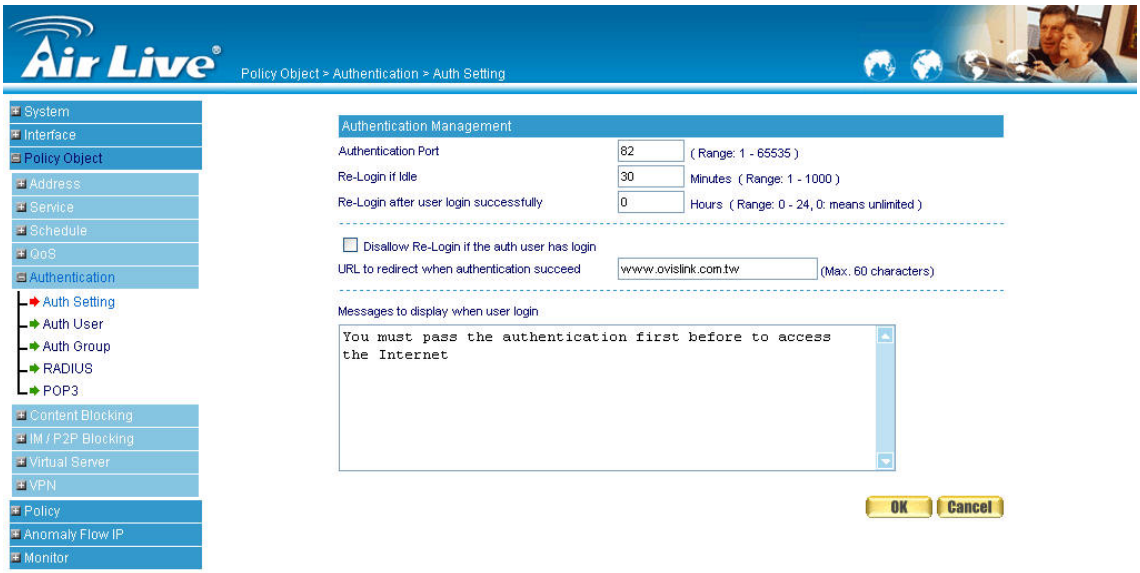


Figure10-1 Authentication Setting WebUI

- When the user connect to external network by Authentication, the following page will be displayed: (Figure10-2)

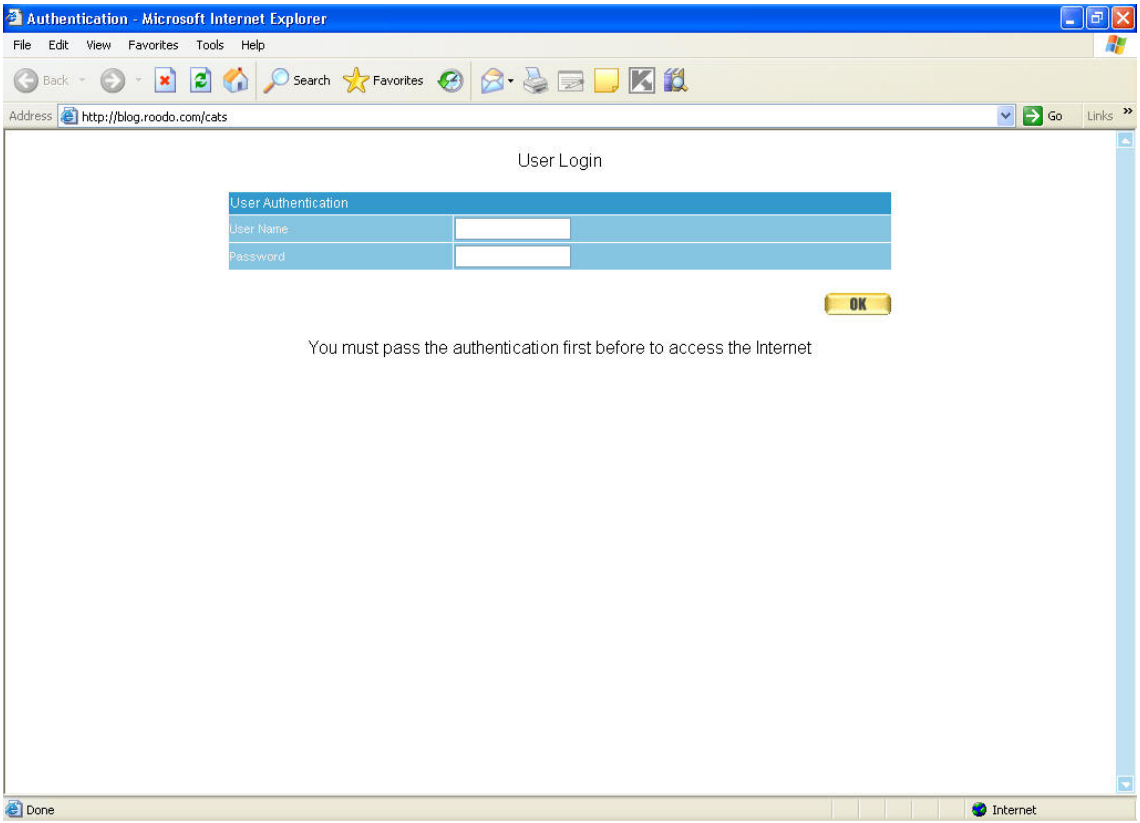


Figure10-2 Authentication Login WebUI

- It will connect to the appointed website after passing Authentication: (Figure10-3)

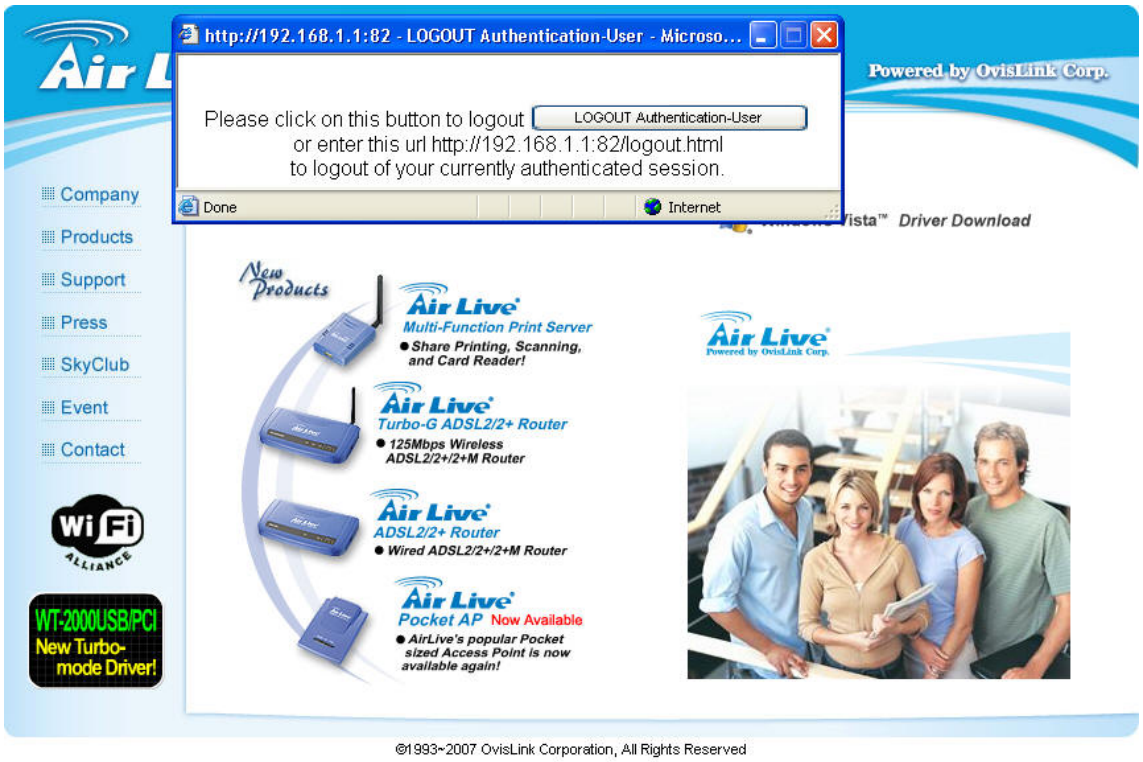


Figure10-3 Connecting to the Appointed Website After Authentication

If user asks for authentication positively, he/she can enter the LAN IP with the Authentication port number. And then the Authentication WebUI will be displayed.

Authentication-User Name:

- The user account for Authentication you want to set.

Password:

- The password when setting up Authentication.

Confirm Password:

- Enter the password that correspond to Password

Configure specific users to connect with external network only when they pass the authentication of policy.（Adopt the built-in Auth User and Auth Group, RADIUS, or POP3 Function）

STEP 1 . Setup several **Auth User** in **Authentication**. (Figire10-4)

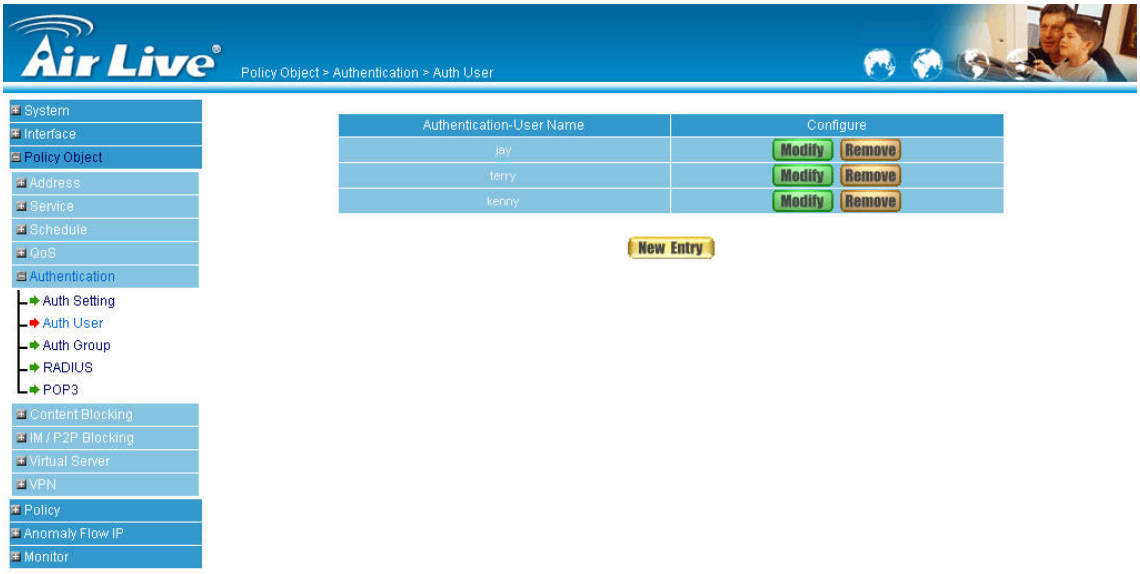


Figure10-4 Setting Several Auth Users WebUI

To use Authentication, the DNS Server of the user's network card must be the same as the LAN Interface Address of RS-3000.

STEP 2 . Add **Auth User Group** Setting in **Authentication** function and enter the following settings:

- Click **New Entry**
- **Name:** Enter Product_dept
- Select the Auth User you want and **Add** to Selected Auth User
- Click **OK**
- Complete the setting of Auth User Group (Figure10-5)

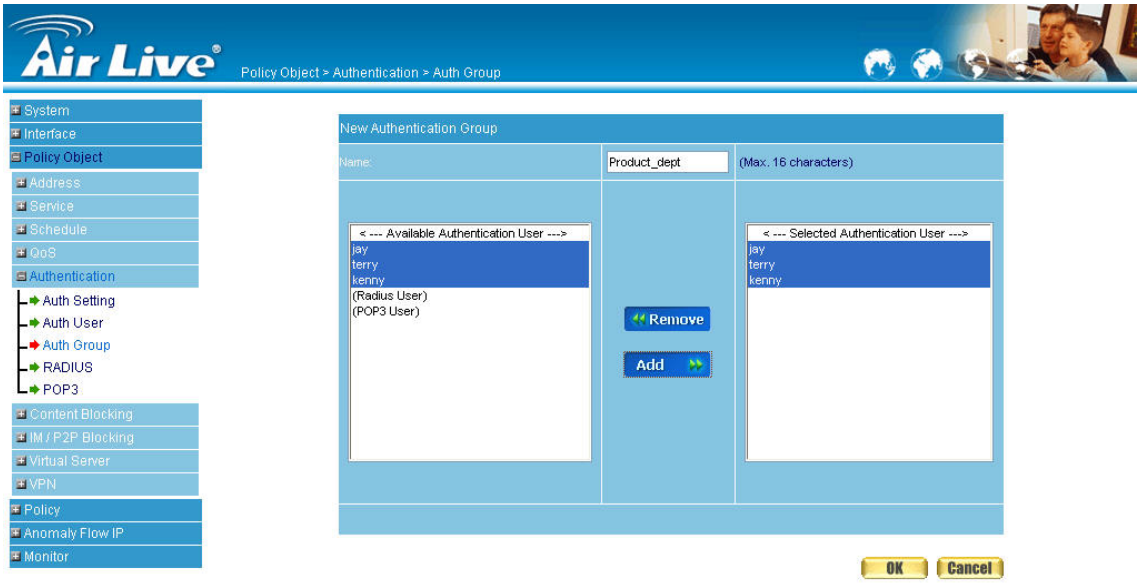


Figure10-5 Setting Auth Group WebUI

STEP 3 . User also can select to authenticate user with RADIUS server. Just need to enter the Server IP, Port number, password, and enable the function.

- Enable **RADIUS Server Authentication**
- Enter **RADIUS Server IP**
- Enter **RADIUS Server Port**
- Enter password in **Shared Secret**
- Complete the setting of **RADIUS Server** (Figure10-6)

Figure10-6 Setting RADIUS WebUI

STEP 4 . The third method of Authentication is to check the account with POP3 Server.

- Enable **POP3 Server Authentication**
- Enter **POP3 Server IP**
- Enter **POP3 Server Port**
- Complete the setting of **POP3 Server** (Figure10-7)

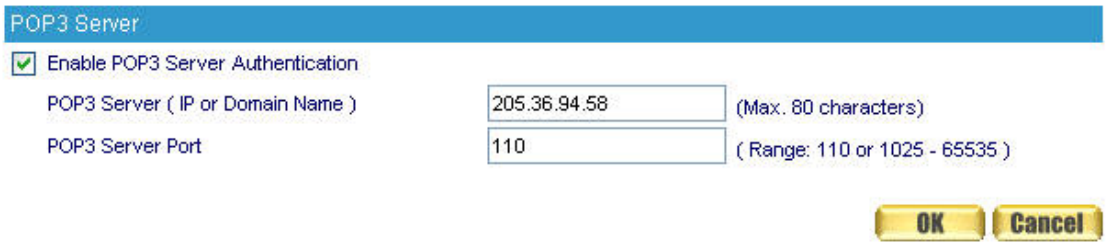


Figure10-7 Setting POP3 WebUI

STEP 5 . Add a policy in **Outgoing Policy** and input the Address and Authentication of STEP 2 (Figure10-8, 10-9)

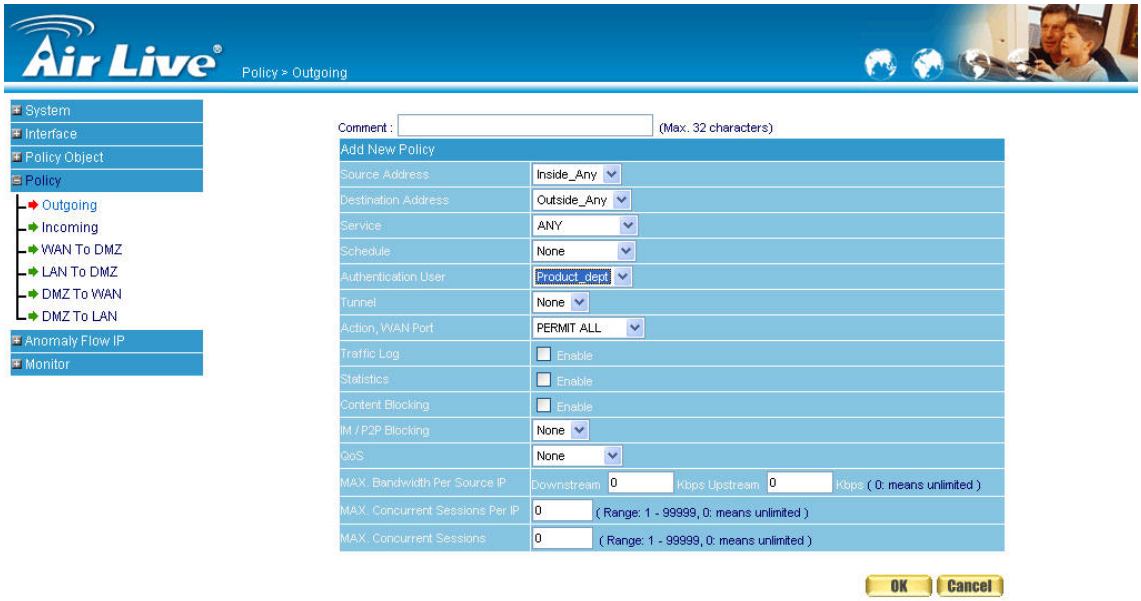


Figure10-8 Auth-User Policy Setting

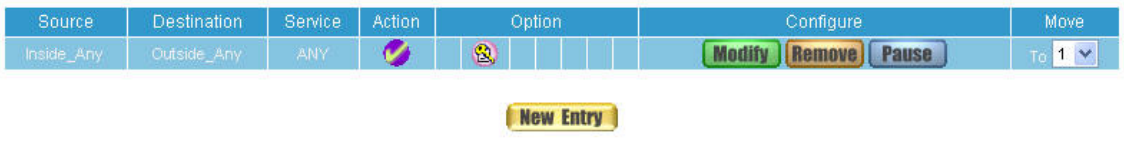


Figure10-9 Complete the Policy Setting of Auth-User

STEP 6 **.** When user is going to access to Internet through browser, the authentication UI will appear in Browser. After entering the correct user name and password, click **OK** to access to Internet. (Figure10-10)

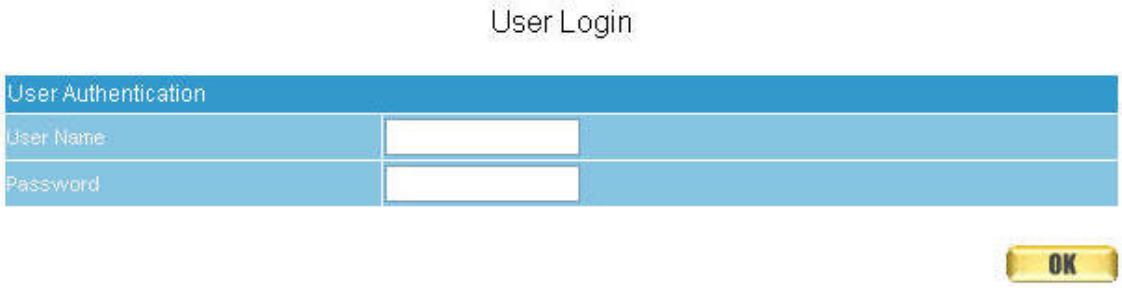


Figure10-10 Access to Internet through Authentication WebUI

STEP 7.If the user does not need to access to Internet anymore and is going to logout, he/she can click **LOGOUT Auth-User** to logout the system. Or enter the Logout Authentication WebUI (http:// LAN Interface: Authentication port number/ logout.html) to logout (Figure10-11)

Figure10-11 Logout Auth-User WebUI

Chapter 11　Content Blocking

Content Filtering includes「URL」,「Script」,「Download」,「Upload」.

【URL Blocking】： The administrator can set up to “Allow” or “Restrict” entering the specific website by complete domain name, key words, and meta-character (～and＊).

【Script Blocking】： To restrict the access authority of Popup, ActiveX, Java, or Cookie.

【Download Blocking】： To restrict the authority of download specific sub-name file, audio, and some common video by http protocol directly.

【Upload Blocking】： To restrict the authority of upload specific sub-name file, or restrict all types of the files.

Define the required fields of Content Blocking

URL String:

- The domain name that restricts to enter or only allow entering.

Popup Blocking:

- Prevent the pop-up WebUI appearing

ActiveX Blocking:

- Prevent ActiveX packets

Java Blocking:

- Prevent Java packets

Cookie Blocking:

- Prevent Cookies packets

Audio and Video Types:

- Prevent users to transfer sounds and video file by http

Extension Blocking:

- Prevent users to deliver specific sub-name file by http

All Type:

- Prevent users to send the Audio, Video types, and sub-name file…etc. by http protocol.

11.1 URL

Restrict the Internal Users only can access to some specific Website

※URL Blocking:

Symbol: **～ means open up**; *** means meta-character**

Restrict to block specific website: Type the 「complete domain name」 or 「key word」of the website you want to restrict in **URL String**. For example: www.kcg.gov.tw or gov.

Restrict to access specific website:

1. Type the symbol "~" in front of the 「complete domain name」or「key word」that represents to access the specific website only. For example: ~www.kcg.gov.tw or ~gov.
2. After setting up the website you want to access, user needs to input an order to **forbid all** in the last URL String; just type in ***** in URL String.

Warning! The order to forbid all must be placed at the last. If you want to open a new website, you must delete the order of forbidding all and then input the new domain name. At last, re-type in the "forbid all" order again.

STEP 1． Enter the following in **URL** of **Content Filtering** function:

- Click **New Entry**
- **URL String:** Enter ~yahoo, and click **OK**
- Click **New Entry**
- **URL String:** Enter ~google, and click **OK**
- Click **New Entry**
- **URL String**: Enter ***,** and click **OK**
- Complete setting a URL Blocking policy (Figure11-1)

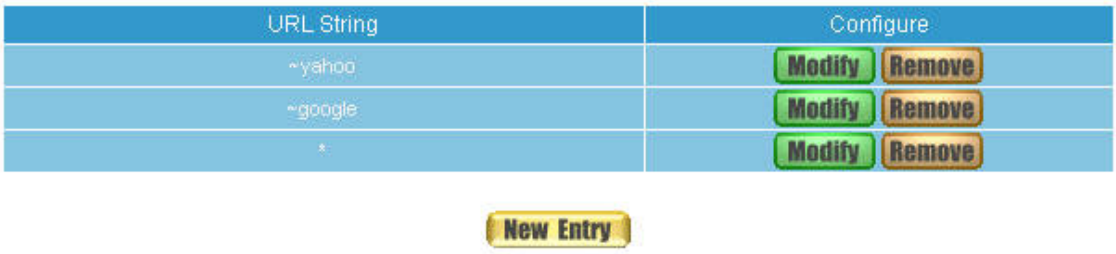


Figure11-1 Content Filtering Table

STEP 2． Add a **Outgoing Policy** and use in **Content Blocking** function: (Figure11-2)

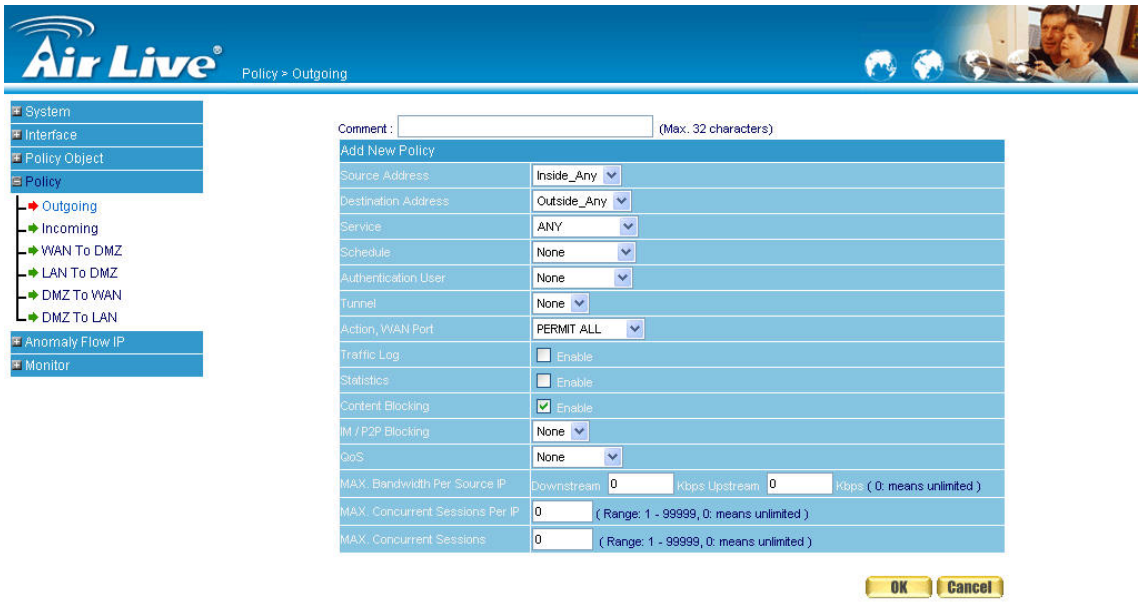


Figure11-2 URL Blocking Policy Setting

STEP 3． Complete the policy of permitting the internal users only can access to some specific website in **Outgoing Policy** function: (Figure11-3)

Figure11-3 Complete Policy Settings

Afterwards the users only can browse the website that includes “yahoo” and “google” in domain name by the above policy.

11.2 Script

Restrict the Internal Users to access to Script file of Website

STEP 1 . Select the following data in **Script** of **Content Blocking** function:

- Select **Popup** Blocking
- Select **ActiveX** Blocking
- Select **Java** Blocking
- Select **Cookie** Blocking
- Click **OK**
- Complete the setting of Script Blocking (Figure11-4)

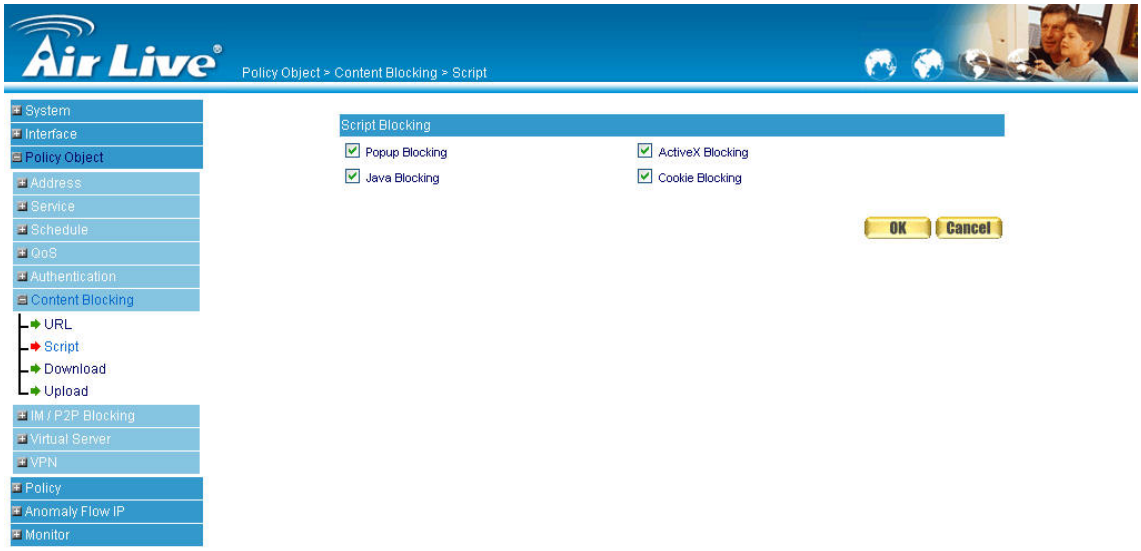


Figure11-4 Script Blocking WebUI

STEP 2 . Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure11-5)

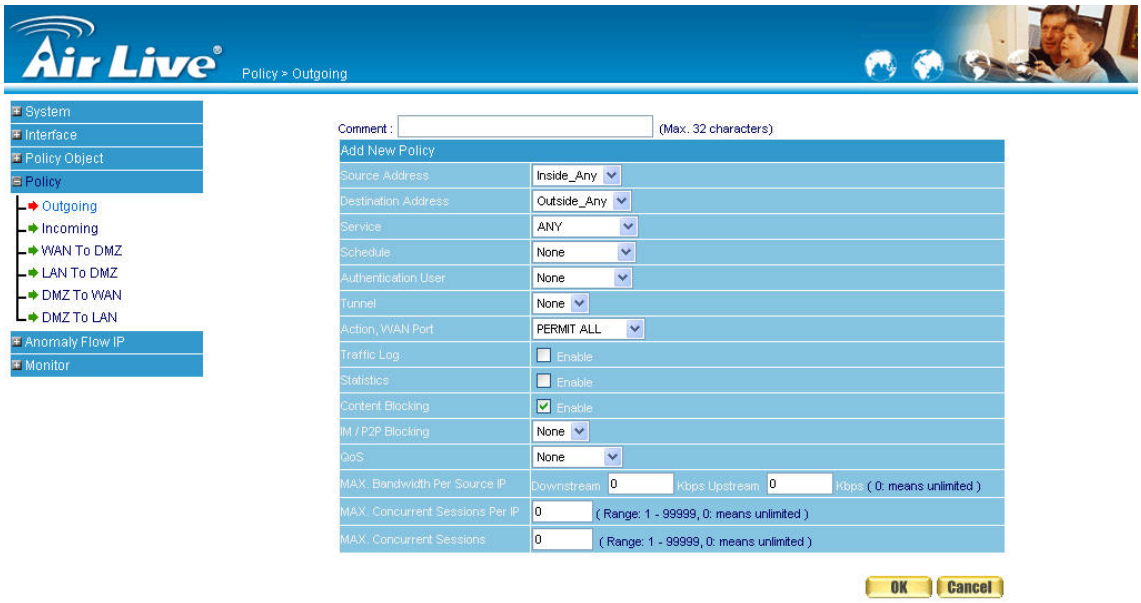


Figure11-5 New Policy of Script Blocking Setting

STEP 3 . Complete the policy of restricting the internal users to access to Script file of Website in **Outgoing Policy**: (Figure11-6)

Figure11-6 Complete Script Blocking Policy Setting

The users may not use the specific function (like JAVA, cookie…etc.) to browse the website through this policy. It can forbid the user browsing stock exchange website…etc.

11.3 Download

Restrict the Internal Users to download video, audio and some specific sub-name file from http or ftp protocol directly

STEP 1． Enter the following settings in **Download** of **Content Blocking** function**:**

- Select **All Types Blocking**
- Click **OK**
- Complete the setting of Download Blocking. (Figure11-7)

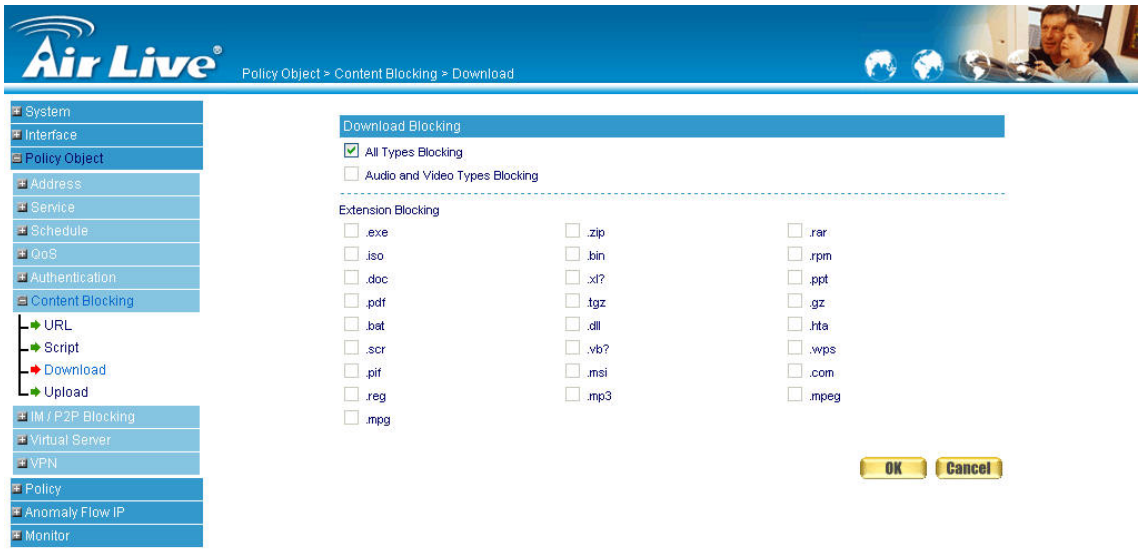


Figure11-7 Download Blocking WebUI

STEP 2． Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure11-8)

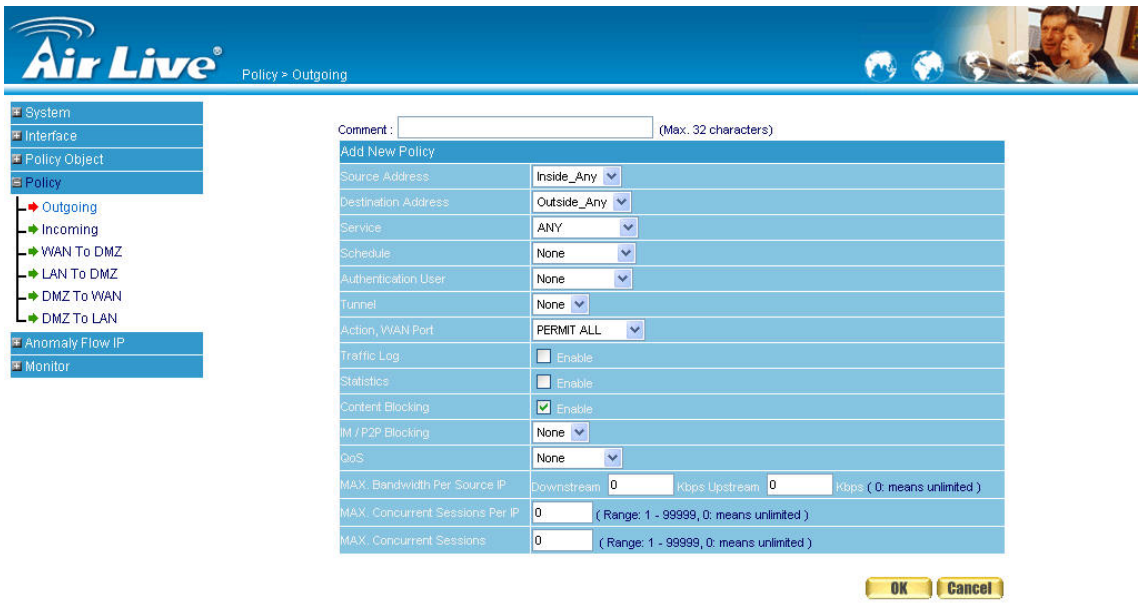


Figure11-8 Add New Download Blocking Policy Setting

STEP 3 **.** Complete the **Outgoing Policy** of restricting the internal users to download video, audio, and some specific sub-name file by http protocol directly: (Figure11-9)

Figure11-9 Complete Download Blocking Policy Setting

11.4 Upload

Restrict the Internal Users to upload some specific sub-name file from http or ftp protocol directly

STEP 1 . Enter the following settings in **Upload** of **Content Blocking** function**:**

- Select **All Types Blocking**
- Click **OK**
- Complete the setting of Upload Blocking. (Figure11-10)

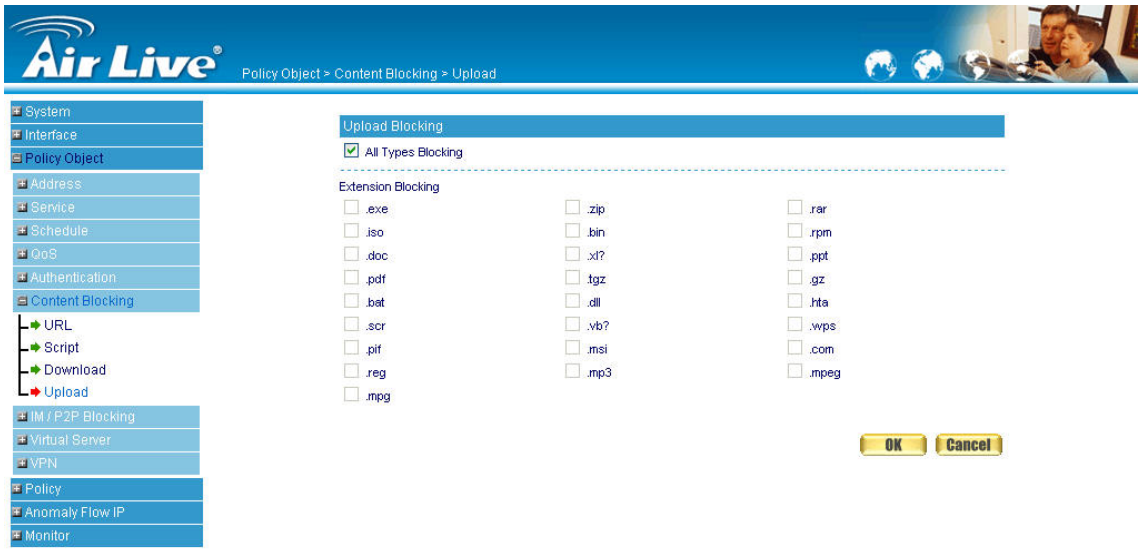


Figure11-10 Upload Blocking WebUI

STEP 2 . Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure11-11)

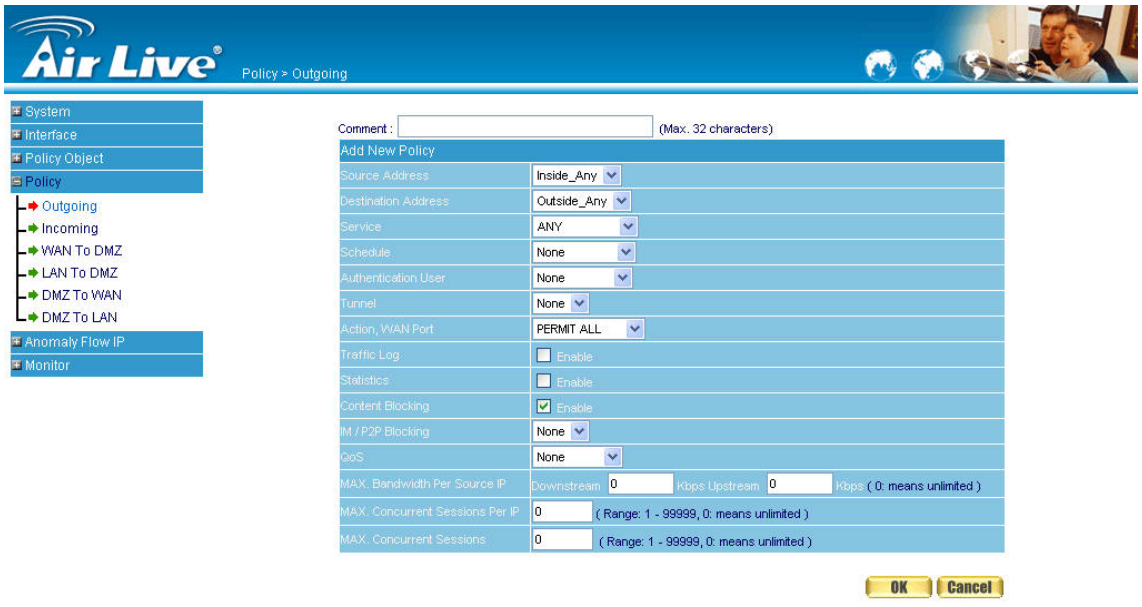


Figure11-11 Add New Upload Blocking Policy Setting

STEP 3 **.** Complete the **Outgoing Policy** of restricting the internal users to upload some specific sub-name file by http protocol directly: (Figure11-12)

Figure11-12 Complete Upload Blocking Policy Setting

Chapter 12 Application Blocking

RS-3000 Application Blocking offers the system to block the connection of applications, such as **IM**, **P2P**, **Video/Audio Application**, **Webmail**, **Game Application**, **Tunnel Application**, and **Remote Control Application**.

【Application Signature Definition】: System will automatically check new signature per every one hour, or user can also click "**Update NOW**" button to check new signature. (Figure 12-1)

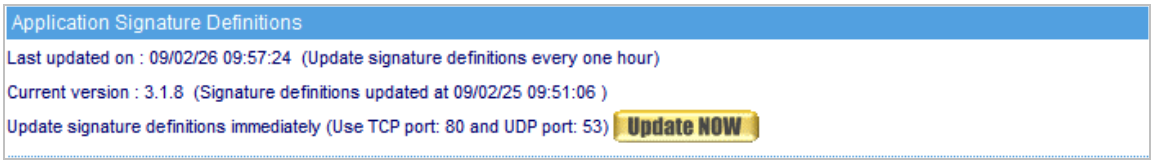


Figure 12-1 Application Signature Definition WebUI

【Instant Message Login】: Restrict the authority to login MSN, Yahoo Messenger, ICQ/AIM, QQ/TM2008, Skype, Google Talk, Gadu-Gadu, Rediff, WebIM, and AllSoft. (Figure 12-2)

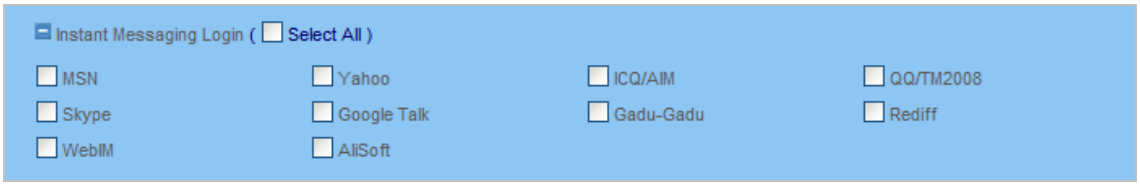


Figure 12-2 Instant Message Login WebUI

【Instant Message File Transfer】: Restrict the authority to transfer file from MSN, Yahoo Messenger, ICQ/AIM, QQ, Skype, Google Talk, and Gadu-Gadu. (Figure 12-3)

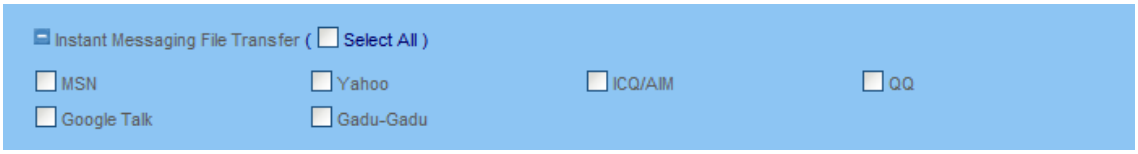


Figure 12-3 Instant Message File Transfer WebUI

Due to the hardware limitation, it is not possible to block all kinds of application in the world, so we just choose to block some popular application. If you require RS-3000 to block a specific application please contact with AirLive Support Team. We will evaluate the application and try to improve it.

【Peer-to-Peer Application】： Restrict the authority to send files connection by using eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, GoGoBox, QQDownload, Ares, Shareaza, BearShare, Morpheus, Limewire, and KaZaa. (Figure 12-4)

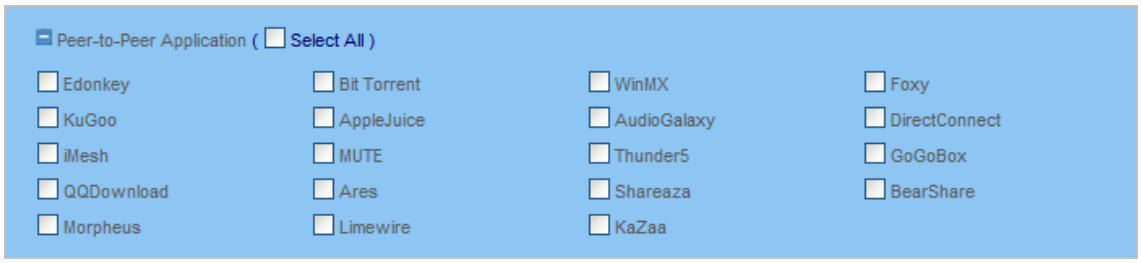


Figure 12-4 Peer-to-Peer Application WebUI

【Video / Audio Application】： Restrict the authority to watch video or listen audio from Internet by using PPLive, PPStream, UUSee, QQLive, ezPeer, and qvodplayer. (Figure 12-5)

Figure 12-5 Video / Audio Application WebUI

【Webmail】： Restrict the authority to access web mail service, such as Gmail, Hotmail, Yahoo, Hinet, PChome, URL, Yam, Seednet, 163/126/Yeah, Tom, Sina, Sohu, and QQ/Foxmail. (Figure 12-6)

Figure 12-6 Webmail WebUI

【Game Application】： Restrict the authority to access Internet Game such as GLWorld and QQGame. (Figure 12-7)

Figure 12-7 Game Application WebUI

【Tunnel Application】：Restrict the authority to access Internet via tunnel application such as VNN Client, Ultra-Surf, Tor, and Hamachi. (Figure 12-8)

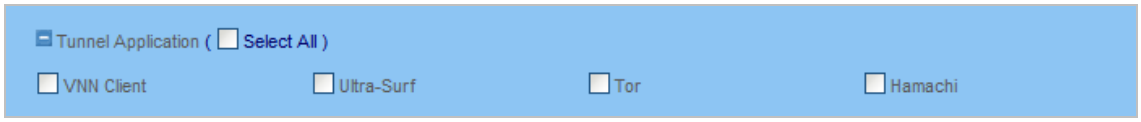


Figure 12-8 Tunnel Application WebUI

【Remote Control Application】：Restrict the authority to access remote control application such as TeamViewer, VNC, and RemoteDestop. (Figure 12-9)

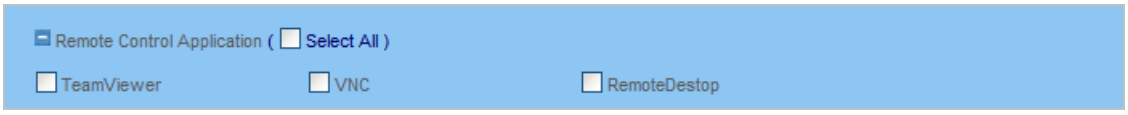


Figure 12-9 Tunnel Application WebUI

- **Configuration Example**

■ GroupA users are not allowed to use MSN, Yahoo, and Skype.

■ GroupB users are allowed to use MSN, but they can not transfer file by MSN.

■ GroupC users are not allowed to use MSN, Yahoo, Skype, eDnokey, Bit Torrent.

STEP 1 **. Policy Object → Address → LAN:** Enter the name and IP address of LAN users.

STEP 2 **. Policy Object → Address → LAN Group:** Allocate the users to the dedicated group, and create GroupA, GroupB, GroupC. (Figure 12-10)

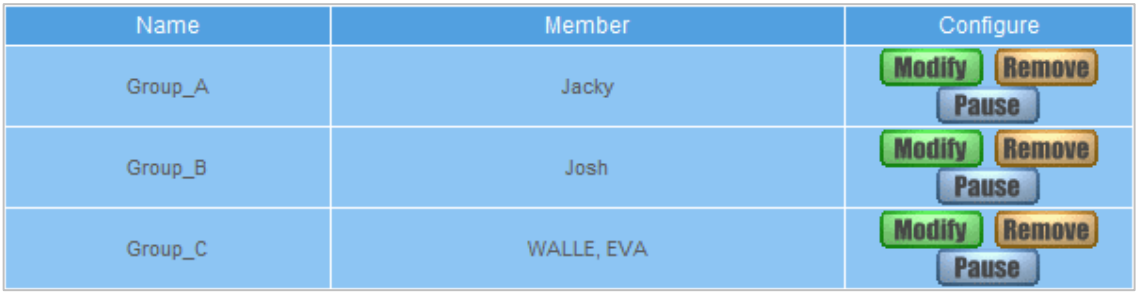


Figure 12-10 Create Groups

STEP 3 **. Policy Object → Application Blocking → Setting:** Create first Application Blocking rule for GroupA to block MSN, Yahoo and Skype. (Figure 12-11)

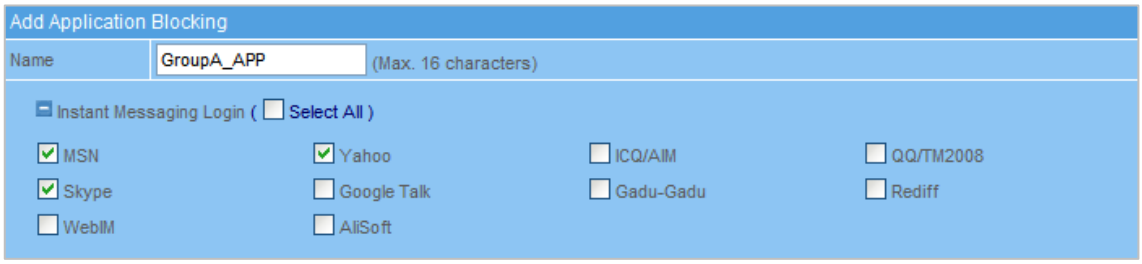


Figure 12-11 Create first Application Groups

STEP 4 **. Policy Object → Application Blocking → Setting:** Create Second Application Blocking rule for GroupB. So the user in GroupB can access MSN, but can not send files using MSN. (Figure 12-12)

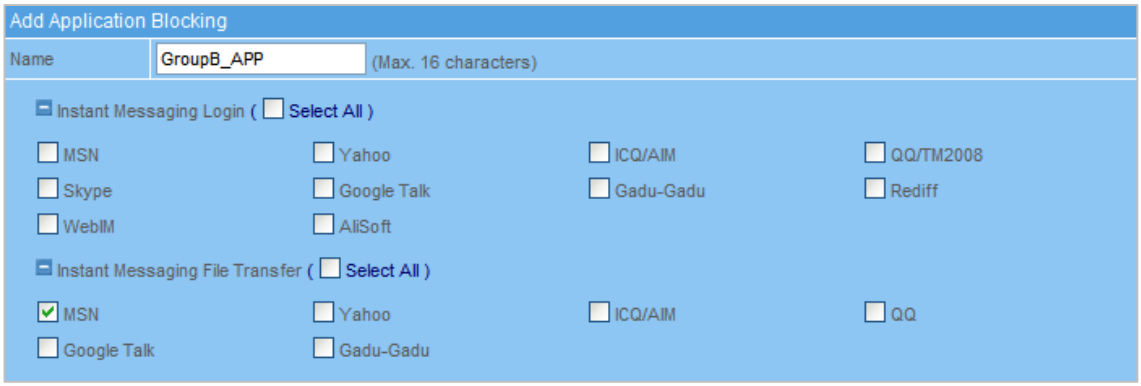


Figure 12-12 Create Second Application Groups

STEP 5 **. Policy Object → Application Blocking → Setting:** Create Second Application Blocking rule for GroupC to block MSN, Yahoo, Skype, eDonkey, and Bit Torrent. (Figure 12-13)

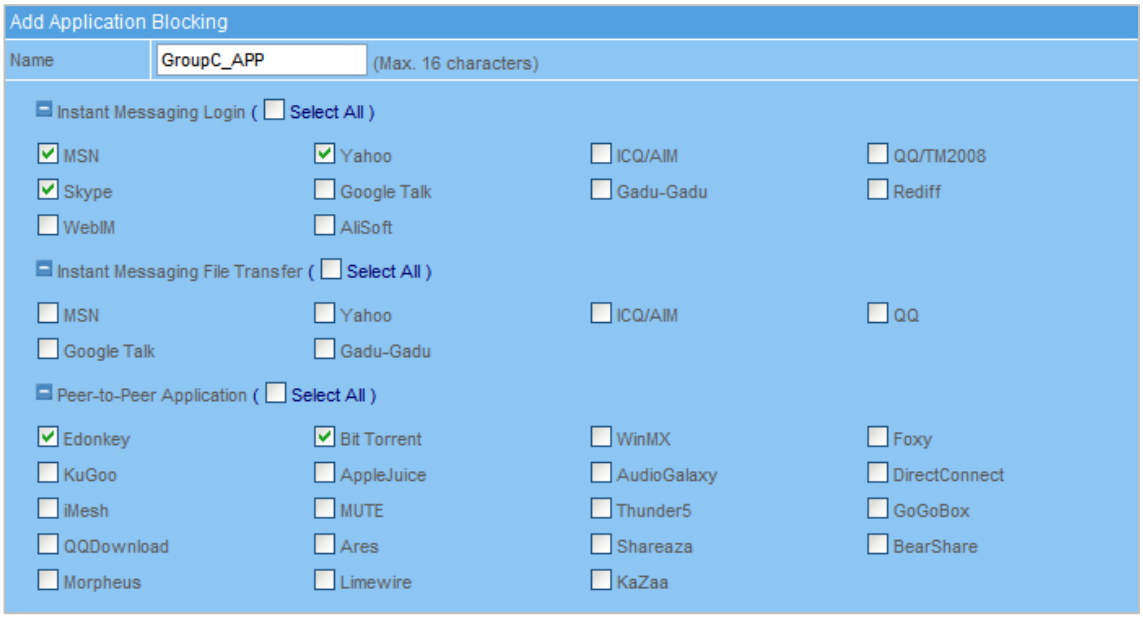


Figure 12-13 Create Second Application Groups

STEP 6 . **Policy → Outgoing:** Create three Outgoing Policy rules and assign the group with its Application Blocking setting. (Figure 12-14)

Source	Destination	Service	Action	Option	Configure	Move
Group_A	Outside_Any	ANY			Modify Remove Pause	To 1
Group_B	Outside_Any	ANY			Modify Remove Pause	To 2
Group_C	Outside_Any	ANY			Modify Remove Pause	To 3

Figure 12-14 Create Policy rules with groups and enable Application Blocking

P2P Transfer will occupy large bandwidth so that it may influence other users. And P2P Transfer can change the service port free so it is invalid to restrict P2P Transfer by **Service**. Therefore, the system manager must use **Application Blocking** to restrict users to use P2P Transfer efficiently.

Chapter 13 Virtual Server

The real IP address provided from ISP is always not enough for all the users when the system manager applies the network connection from ISP. 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 RS-3000's NAT (Network Address Translation) function. If a server that provides service to WAN network is located in LAN networks, external users cannot directly connect to the server by using the server's private IP address.

The RS-3000's Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the RS-3000's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the RS-3000 translates the Virtual Server's IP address into the private IP address in the LAN network.

Virtual Server owns another feature know as one-to-many mapping. This is when one real server IP address on the WAN interface can be mapped into four LAN network servers provide the same service 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 session. Therefore, it can reduce the loading of a single server and lower the crash risk. And can improve the work efficiency.

In this chapter, we will have detailed introduction and instruction of **Mapped IP** and **Server 1/2/3/4**:

Mapped IP: Because the Intranet is transferring the private IP by NAT Mode (Network Address Translation). And if the server is in LAN, its IP Address is belonging to Private IP Address. Then the external users cannot connect to its private IP Address directly. The user must connect to the RS-3000's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the RS-3000. It is a one-to-one mapping. That is, to map all the service of one WAN Real IP Address to one LAN Private IP Address.

Server 1/2/3/4: Its function resembles Mapped IP's. But the Virtual Server maps one to many. That is, to map a Real IP Address to 1~4 LAN Private IP Address and provide the service item in Service.

Define the required fields of Virtual Server

WAN IP：

- WAN IP Address (Real IP Address)

Map to Virtual IP：

- Map the WAN Real IP Address into the LAN Private IP Address

Virtual Server Real IP：

- The WAN IP address which mapped by the Virtual Server.

Service name (Port Number)：

- The service name that provided by the Virtual Server.

External Service Port：

- The WAN Service Port that provided by the virtual server. If the service you choose only have one port and then you can change the port number here. (If change the port number to 8080 and then when the external users going to browse the Website; he/she must change the port number first to enter the Website.)

Server Virtual IP：

- The virtual IP which mapped by the Virtual Server.

13.1 Mapped IP

Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy

STEP 1 . Setting a server that provide several services in LAN, and set up the network card's IP as 192.168.1.100. DNS is External DNS Server.

STEP 2 . Enter the following setting in **LAN** of **Address** function: (Figure13-1)

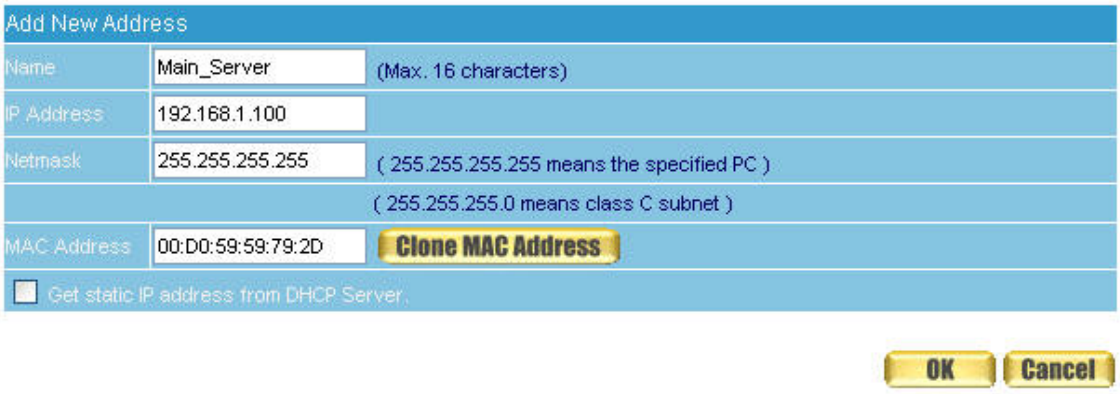


Figure13-1 Mapped IP Settings of Server in Address

STEP 3 . Enter the following data in **Mapped IP** of **Virtual Server** function:

- Click **New Entry**
- **WAN IP:** Enter 61.11.11.12 (click **Assist** for assistance)
- **Map to Virtual IP:** Enter 192.168.1.100
- Click **OK**
- Complete the setting of adding new mapped IP (Figure13-2)

Figure13-2 Mapped IP Setting WebUI

STEP 4 . Group the services (DNS, FTP, HTTP, POP3, SMTP…) that provided and used by server in **Service** function. And add a new service group for server to send mails at the same time. (Figure13-3)

Figure13-3 Service Setting

STEP 5 . Add a policy that includes settings of STEP3, 4 in **Incoming Policy.** (Figure13-4)

Figure13-4 Complete the Incoming Policy

STEP 6 . Add a policy that includes STEP2, 4 in **Outgoing Policy**. It makes the server to send e-mail to external mail server by mail service. (Figure13-5)

Figure13-5 Complete the Outgoing Policy

STEP 7 . Complete the setting of providing several services by mapped IP.

Strong suggests **not** to choose **ANY** when setting Mapped IP and choosing service. Otherwise the Mapped IP will be exposed to Internet easily and may be attacked by Hacker.

13.2 Virtual Server 1/2/3/4

Make several servers that provide a single service, to provide service through policy by Virtual Server (Take Web service for example)

STEP 1 . Setting several servers that provide Web service in LAN network, which IP Address is **192.168.1.101**, **192.168.1.102**, **192.168.1.103**, and **192.168.1.104**

STEP 2 . Enter the following data in **Server 1** of **Virtual Server** function:

- Click the button next to **Virtual Server Real IP** ("**click here to configure**") in **Server1**
- **Virtual Server Real IP:** Enter 211.22.22.23 (click **Assist** for assistance)
- Click **OK** (Figure13-6)

Figure13-6 Virtual Server Real IP Setting

- Click **New Entry**
- **Service:** Select HTTP (80)
- **External Service Port:** Change to 8080
- **Load Balance Server1:** Enter 192.168.1.101
- **Load Balance Server2:** Enter 192.168.1.102
- **Load Balance Server3:** Enter 192.168.1.103
- **Load Balance Server4:** Enter 192.168.1.104
- Click **OK** and complete the setting of Virtual Server (Figure13-7)

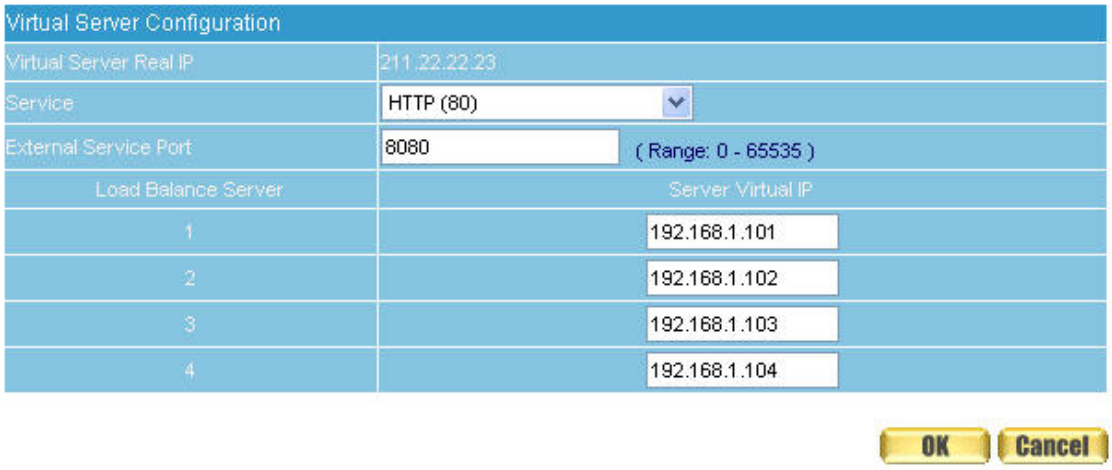


Figure13-7 Virtual Server Configuration WebUI

STEP 3 . Add a new policy in **Incoming Policy**, which includes the virtual server, set by STEP2. (Figure13-8)

Figure13-8 Complete Virtual Server Policy Setting

In this example, the external users must change its port number to 8080 before entering the Website that set by the Web server.

STEP 4 . Complete the setting of providing a single service by virtual server.

The external user use VoIP to connect with VoIP of LAN (VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)

STEP 1． Set up VoIP in LAN network, and its IP is 192.168.1.100

STEP 2． Enter the following setting in **LAN** of **Address** function: (Figure13-9)

Figure13-9 Setting LAN Address WebUI

STEP 3． Add new VoIP service group in **Custom** of **Service** function. (Figure13-10)

Figure13-10 Add Custom Service

STEP 4． Enter the following setting in **Server1** of **Virtual Server** function:

- Click the button next to **Virtual Server Real IP** (“**click here to configure**”) in **Server1**
- **Virtual Server Real IP:** Enter 61.11.11.12 (click **Assist** for assistance) (Use WAN)
- Click **OK** (Figure13-11)

Figure13-11 Virtual Server Real IP Setting WebUI

- Click **New Entry**
- **Service:** Select (Custom Service) VoIP_Service
- **External Service Port:** From-Service (Custom)
- **Load Balance Server1:** Enter 192.168.1.100
- Click **OK**
- Complete the setting of Virtual Server (Figure13-12)

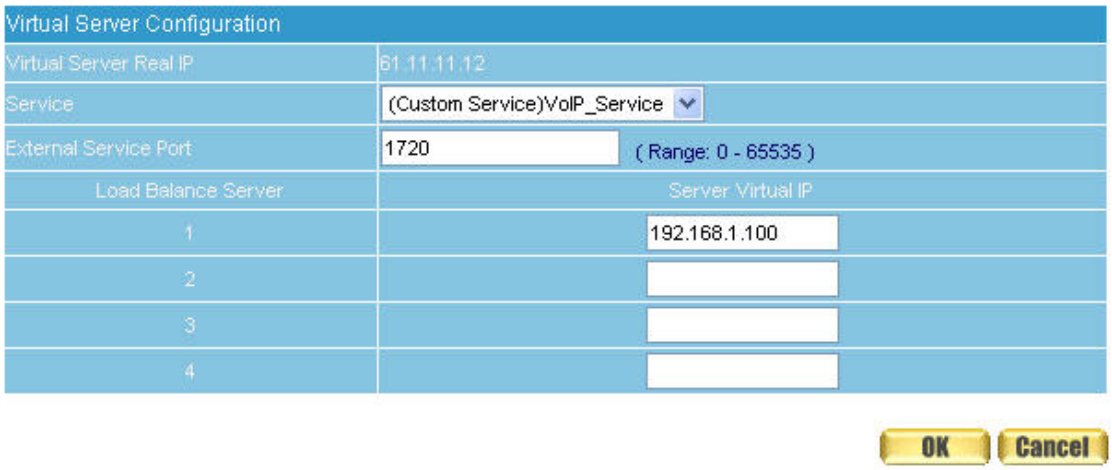


Figure13-12 Virtual Server Configuration WebUI

When the custom service only has one port number, then the external network port of **Virtual Server** is changeable; On the contrary, if the custom service has more than one port network number, then the external network port of **Virtual Server** cannot be changed.

STEP 5 . Add a new **Incoming Policy,** which includes the virtual server that set by STEP4: (Figure13-13)

Figure13-13 Complete the Policy includes Virtual Server Setting

STEP 6 . Enter the following setting of the internal users using VoIP to connect with external network VoIP in **Outgoing Policy**: (Figure13-14)

Figure13-14 Complete the Policy Setting of VoIP Connection

STEP 7 . Complete the setting of the external/internal user using specific service to communicate with each other by Virtual Server.

Make several servers that provide several same services, to provide service through policy by Virtual Server. (Take POP3, SMTP, and DNS Group for example)

STEP 1 . Setting several servers that provide several services in LAN network. Its network card's IP is 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104 and the DNS setting is External DNS server.

STEP 2 . Enter the following in **LAN** and **LAN Group** of **Address** function: (Figure13-15, 13-16)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Server_01	192.168.1.101/255.255.255.255		Modify Remove
Server_02	192.168.1.102/255.255.255.255		Modify Remove
Server_03	192.168.1.103/255.255.255.255		Modify Remove
Server_04	192.168.1.104/255.255.255.255		Modify Remove

New Entry

Figure13-15 Mapped IP Setting of Virtual Server in Address

Name	Member	Configure
Server_Group	Server_01, Server_02, Server_03...	Modify Remove Pause

New Entry

Figure13-16 Group Setting of Virtual Server in Address

STEP 3 . Group the service of server in **Custom** of **Service**. Add a Service Group for server to send e-mail at the same time. (Figure13-17)

Figure13-17 Add New Service Group

STEP 4 . Enter the following data in **Server1** of **Virtual Server**:

- Click the button next to **Virtual Server Real IP** ("**click here to configure**") in **Server1**
- **Virtual Server Real IP:** Enter 211.22.22.23 (click **Assist** for assistance)
- Click **OK** (Figure13-18)

Figure13-18Virtual Server Real IP Setting

- Click **New Entry**
- **Service:** Select (Group Service) Mail_Service
- **External Service Port:** From-Service (Group)
- Enter the server IP in Load Balance Server
- Click **OK**
- Complete the setting of Virtual Server (Figure13-19)

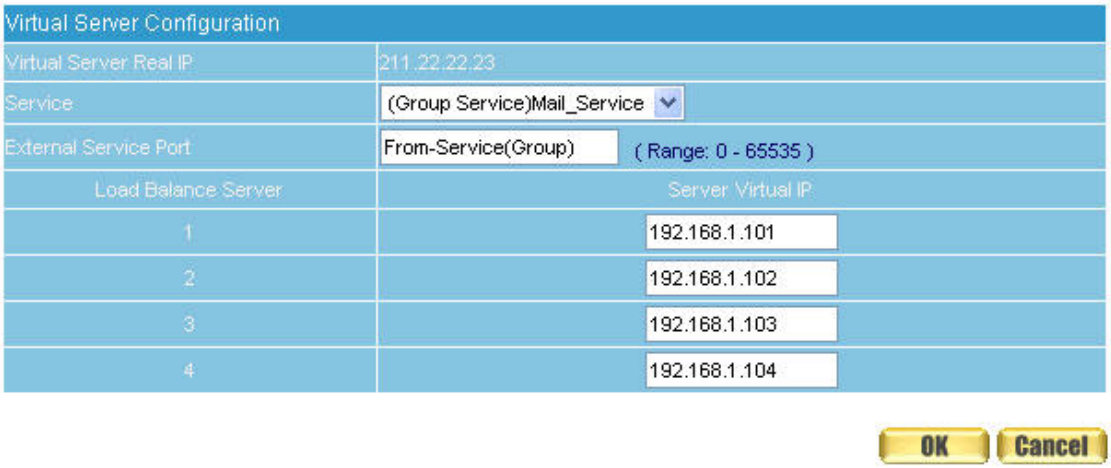


Figure13-19 Virtual Server Configuration WebUI

STEP 5 . Add a new **Incoming Policy,** which includes the virtual server that set by STEP 4: (Figure13-20)

Figure13-20 Complete Incoming Policy Setting

STEP 6 . Add a new policy that includes the settings of STEP2, 3 in **Outgoing Policy.** It makes server can send e-mail to external mail server by mail service. (Figure13-21)

Figure13-21 Complete Outgoing Policy Setting

STEP 7 . Complete the setting of providing several services by Virtual Server.

Chapter 14 VPN

The RS-3000 adopts VPN to set up safe and private network service. And combine the remote Authentication system in order to integrate the remote network and PC of the enterprise. Also provide the enterprise and remote users a safe encryption way to have best efficiency and encryption when delivering data. Therefore, it can save lots of problem for manager.

【IPSec Autokey】： The system manager can create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. Also set up IPSec Lifetime and Preshared Key of the RS-3000.

【PPTP Server】： The System Manager can set up VPN-PPTP Server functions in this chapter.

【PPTP Client】： The System Manager can set up VPN-PPTP Client functions in this chapter

How to use VPN?

To set up a Virtual Private Network (VPN), you need to configure an Access Policy include IPSec Autokey, PPTP Server, or PPTP Client settings of Tunnel to make a VPN connection.

14.1 IPSec Autokey

Define the required fields of VPN:

Preshare Key:

- The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.

ISAKMP (Internet Security Association Key Management Protocol):

- An extensible protocol-encoding scheme that complies to the Internet Key Exchange (IKE) framework for establishment of Security Associations (SAs).

Main Mode:

- This is another first phase of the Oakley protocol in establishing a security association, but instead of using three packets like in aggressive mode, it uses six packets.

Aggressive mode:

- This is the first phase of the Oakley protocol in establishing a security association using three data packets.

AH (Authentication Header):

- One of the IPSec standards that allows for data integrity of data packets.

ESP (Encapsulating Security Payload):

- One of the IPSec standards that provides for the confidentiality of data packets.

DES (Data Encryption Standard):

- The Data Encryption Standard developed by IBM in 1977 is a 64-bit block encryption block cipher using a 56-bit key.

Triple-DES (3DES):

- The DES function performed three times with either two or three cryptographic keys.

AES (Advanced Encryption Standard):

- An encryption algorithm yet to be decided that will be used to replace the aging DES encryption algorithm and that the NIST hopes will last for the next 20 to 30 years.

NULL Algorithm:

- It is a fast and convenient connecting mode to make sure its privacy and authentication without encryption. NULL Algorithm doesn't provide any other safety services but a way to substitute ESP Encryption.

SHA-1 (Secure Hash Algorithm-1):

- A message-digest hash algorithm that takes a message less than 264 bits and produces a 160-bit digest.

MD5:

- MD5 is a common message digests algorithm that produces a 128-bit message digest from an arbitrary length input, developed by Ron Rivest.

GRE/IPSec:

- The device Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology.

Define the required fields of IPSec Function

- To display the VPN connection status via icon。

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

Name:

- The VPN name to identify the IPSec Autokey definition. The name must be the only one and cannot be repeated.

Gateway IP:

- The WAN interface IP address of the remote Gateway.

IPSec Algorithm:

- To display the Algorithm way.

Configure:

- Click **Modify** to change the argument of IPSec; click **Remove** to remote the setting. (Figure14-1)

Figure14-1 IPSec Autokey WebUI

14.2 PPTP Server

Define the required fields of PPTP Server Function

PPTP Server:

- To select Enable or Disable

Client IP Range:

- Setting the IP addresses range for PPTP Client connection

- To display the VPN connection status via icon。

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

User Name:

- Displays the PPTP Client user's name when connecting to PPTP Server.

Client IP:

- Displays the PPTP Client's IP address when connecting to PPTP Server.

Uptime:

- Displays the connection time between PPTP Server and Client.

Configure:

- Click **Modify** to modify the PPTP Server Settings or click **Remove** to remove the setting (Figure14-2)

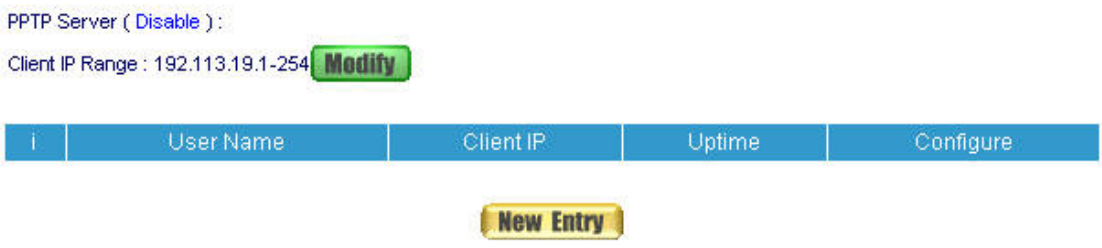


Figure14-2 PPTP Server WebUI

14.3 PPTP Client

Define the required fields of PPTP Client Function

- To display the VPN connection status via icon

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

User Name:

- Ddisplays the PPTP Client user's name when connecting to PPTP Server.

Server IP or Domain Name:

- Displays the PPTP Server IP addresses or Domain Name when connecting to PPTP Server.

Encryption:

- Displays PPTP Client and PPTP Server transmission, whether opens the encryption authentication mechanism.

Uptime:

- Displays the connection time between PPTP Server and Client.

Configure:

- Click **Modify** to change the argument of PPTP Client; click **Remove** to remote the setting. (Figure14-3)

Figure14-3 PPTP Client WebUI

14.4 Trunk

Define the required fields of Tunnel Function

- To display the VPN connection status via icon。

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

Name:

- The VPN name to identify the VPN tunnel definition. The name must be the only one and cannot be repeated.

Source Subnet:

- Displays the Source Subnet.

Destination Subnet:

- Displays the Destination Subnet.

Tunnel:

- Displays the Virtual Private Network's (IPSec Autokey, PPTP Server, PPTP Client) settings of Tunnel function.

Configure:

- Click **Modify** to change the argument of VPN Tunnel; click **Remove** to remote the setting.(Figure14-4)

Figure14-4 VPN Tunnel Web UI

Setting IPSec VPN connection between two RS-3000

Preparation

Company A **WAN IP: 61.11.11.11, LAN IP: 192.168.10.X**

Company B **WAN IP: 211.22.22.22, LAN IP: 192.168.20.X**

This example takes two RS-3000s as work platform. Suppose Company A 192.168.10.100 create a VPN connection with Company B 192.168.20.100 for downloading the sharing file.

The Default Gateway of Company A is the LAN IP of the RS-3000 192.168.10.1. Follow the steps below:

STEP 1 **.** Enter the default IP of Gateway of Company A's RS-3000 with 192.168.10.1, and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure14-5)

Figure14-5 IPSec Autokey WebUI

STEP 2 **.** In the list of **IPSec Autokey**, fill in Name with **VPN_A.** (Figure14-6)

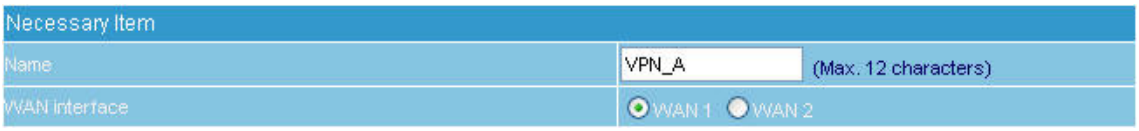


Figure14-6 IPSec Autokey Name Setting

STEP 3 **.** Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.(Figure14-7)

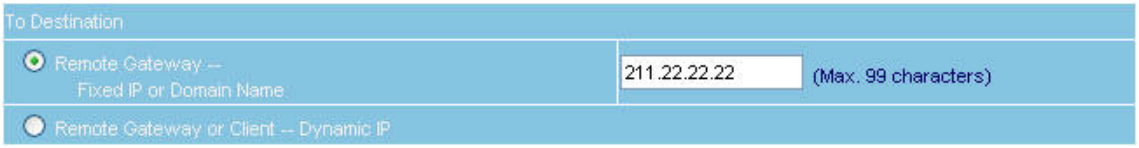


Figure14-7 IPSec To Destination Setting

STEP 4.Select **Preshare** in **Authentication Method** and enter the **Preshared Key** (Figure14-8)

Figure14-8 IPSec Authentication Method Setting

STEP 5 . Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Please select ENC Algorithm (**3DES/DES/AES**), AUTH Algorithm (**MD5/SHA1**), and Group (**GROUP1, 2, 5**). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for Group. (Figure14-9)

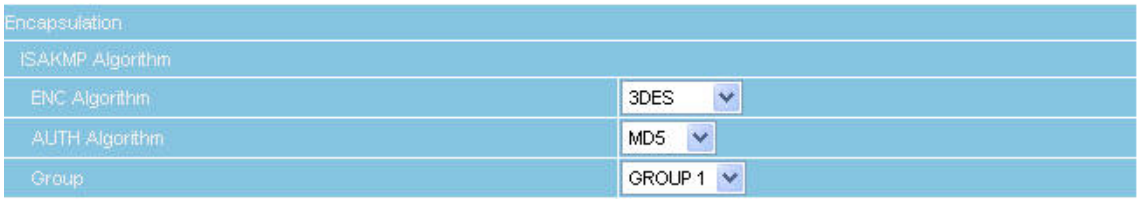


Figure14-9 IPSec Encapsulation Setting

STEP 6 . You can choose Data Encryption + Authentication or Authentication Only to communicate in **IPSec Algorithm** list:

ENC Algorithm: **3DES/DES/AES/NULL**

AUTH Algorithm: **MD5/SHA1**

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission (Figure14-10)

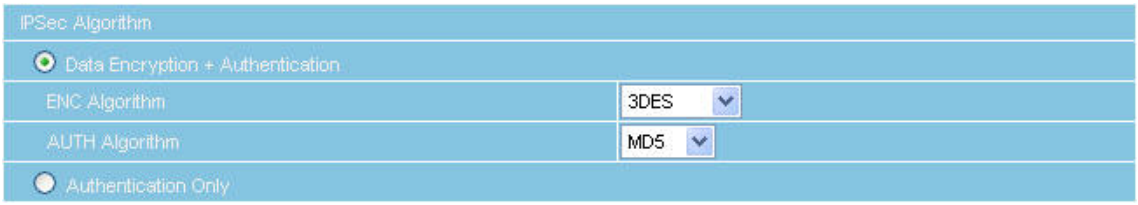


Figure14-10 IPSec Algorithm Setting

STEP 7 . Select GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**. (Figure14-11)

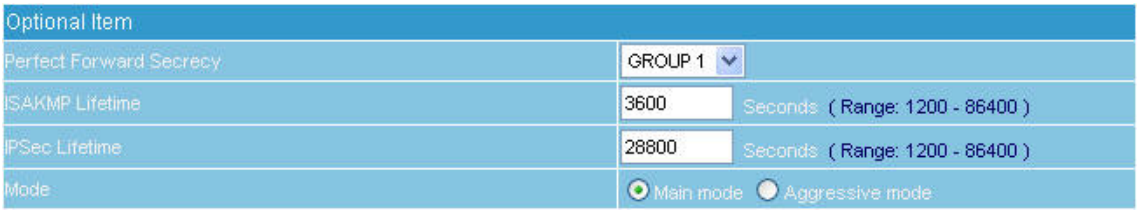


Figure14-11 IPSec Perfect Forward Secrecy Setting

STEP 8.Complete the IPSec Autokey setting. (Figure14-12)

Figure14-12 Complete Company A IPSec Autokey Setting

STEP 9 . Enter the following setting in **Trunk** of **VPN** function**:** (Figure14-13)

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select VPN_A.
- Enter 192.168.20.1 (the Default Gateway of Company B) as the **Keep alive IP**
- Select **Show remote Network Neighborhood** and Click **OK**. (Figure14-14)

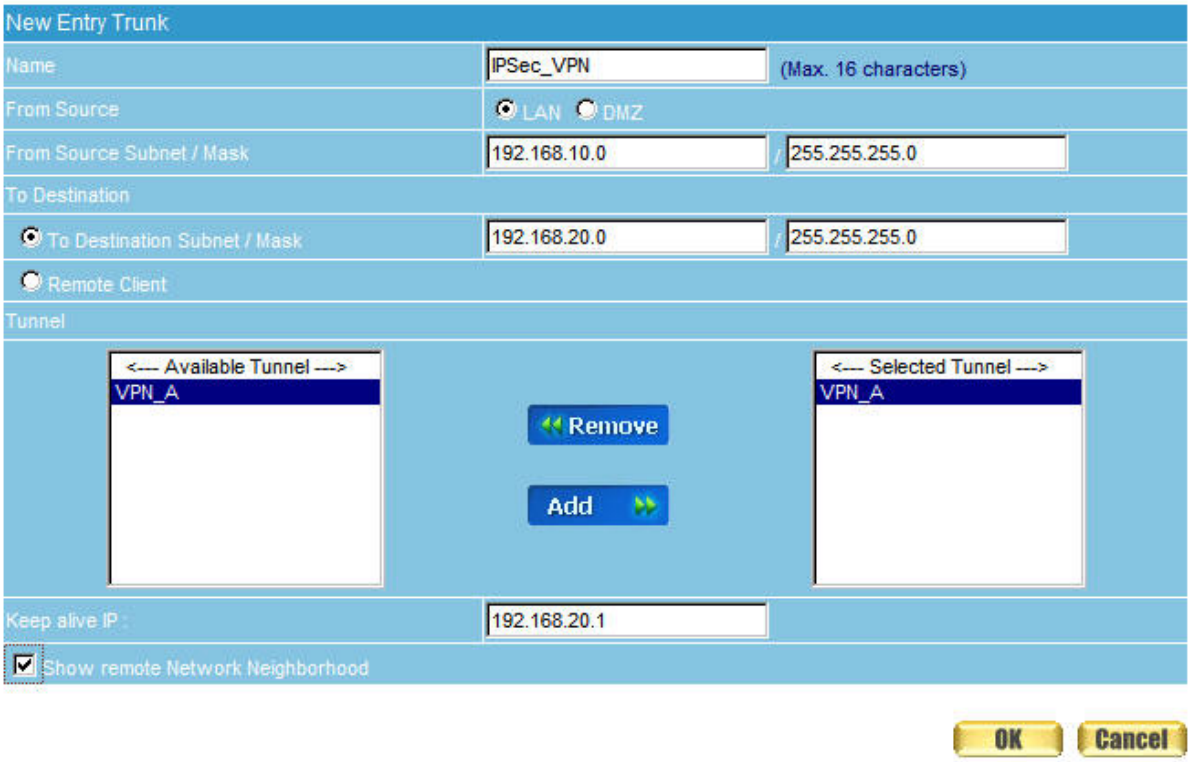


Figure14-13 New Entry Tunnel Setting

Figure14-14 Complete New Entry Tunnel Setting

STEP 10 **.** Enter the following setting in **Outgoing Policy:**(Figure14-15)

- **Trunk:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure14-16)

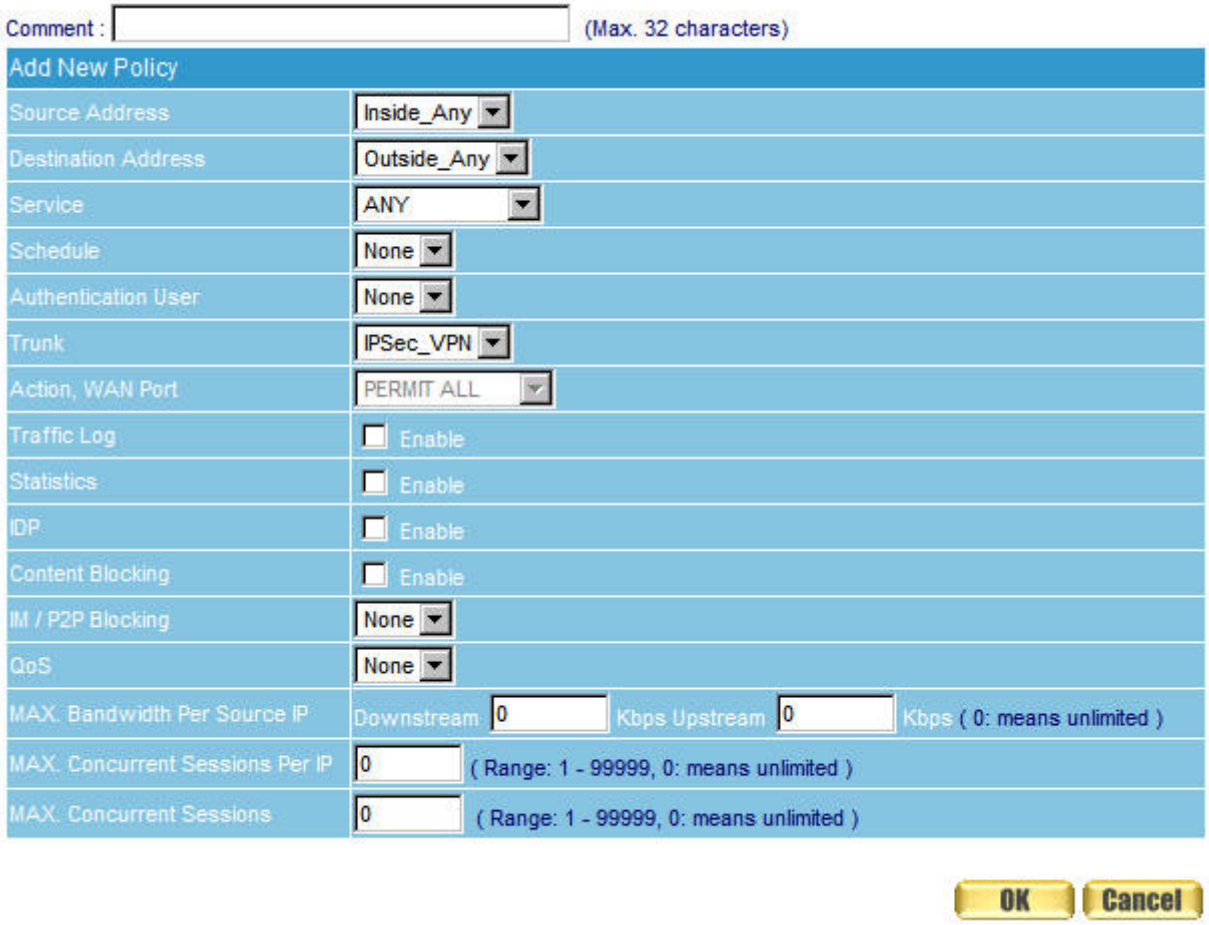


Figure14-15 Setting the VPN Tunnel Outgoing Policy

Figure14-16 Complete the VPN Tunnel Outgoing Policy Setting

STEP 11 **.** Enter the following setting in **Incoming Policy:** (Figure14-17)

- **Trunk:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure14-18)

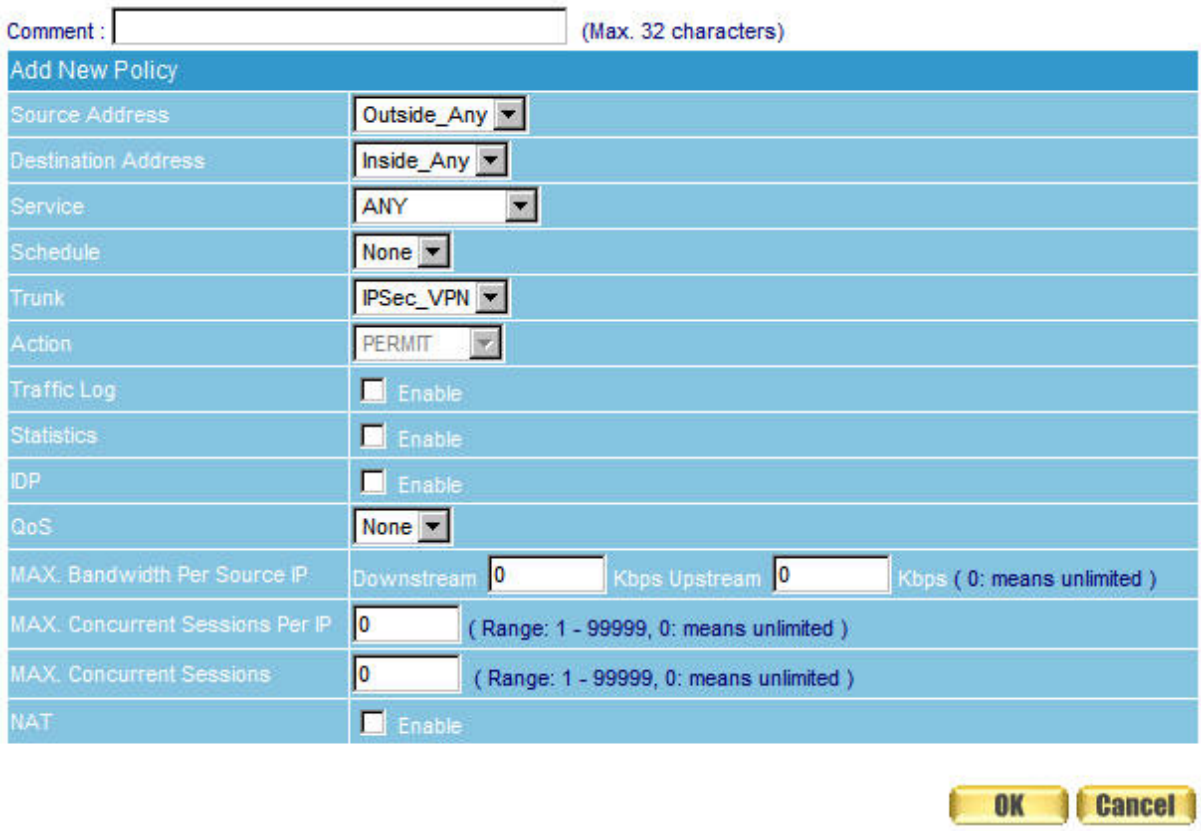


Figure14-17 Setting the VPN Tunnel Incoming Policy

Figure14-18 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the RS-3000 192.168.20.1. Follow the steps below:

STEP 1. Enter the default IP of Gateway of Company B's RS-3000, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure14-19)

Figure14-19 IPSec Autokey Web UI

STEP 2. In the list of **IPSec Autokey**, fill in Name with **VPN_B**. (Figure14-20)

Figure14-20 IPSec Autokey Name Setting

STEP 3. Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.(Figure14-21)

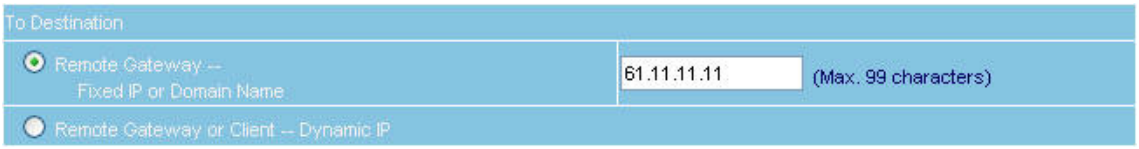


Figure14-21 IPSec To Destination Setting

STEP 4. Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure14-22)

Figure14-22 IPSec Authentication Method Setting

STEP 5. Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Please select ENC Algorithm (**3DES/DES/AES**), AUTH Algorithm (**MD5/SHA1**),

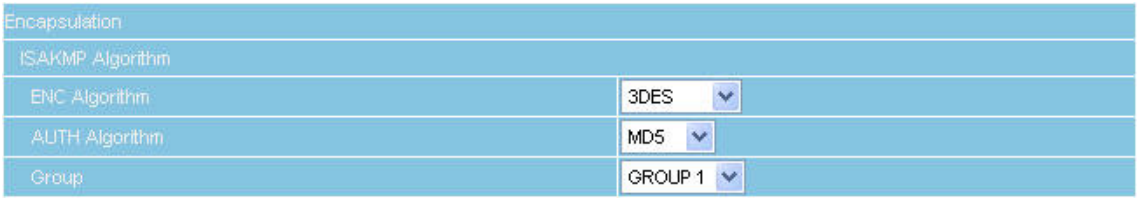


Figure14-23 IPSec Encapsulation Setting

STEP 6. You can choose Data Encryption + Authentication or Authentication Only to communicate in **IPSec Algorithm** list:

ENC Algorithm: **3DES/DES/AES/NULL**

AUTH Algorithm: **MD5/SHA1**

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission. (Figure14-24)

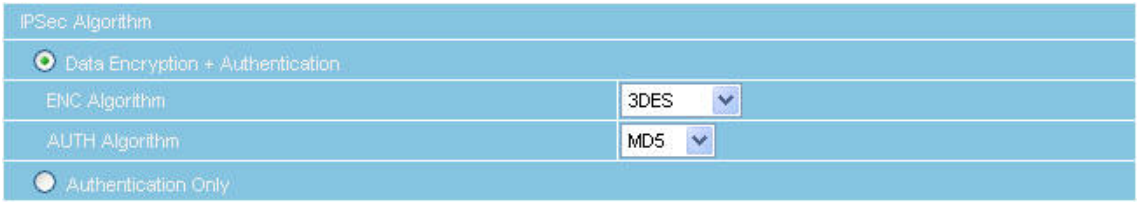


Figure14-24 IPSec Algorithm Setting

STEP 7. After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**. (Figure14-25)

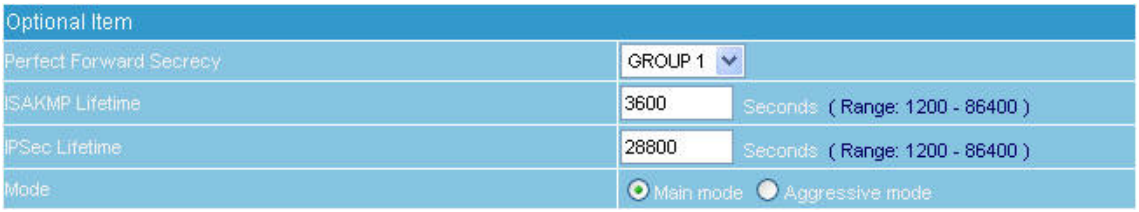


Figure14-25 IPSec Perfect Forward Secrecy Setting

STEP 8. Complete the IPSec Autokey setting. (Figure14-26)

Figure14-26 Complete Company B IPSec Autokey Setting

STEP 9. Enter the following setting in **Trunk** of **VPN** function**:** (Figure14-27)

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select VPN_B.
- Enter 192.168.10.1 (the Default Gateway of Company A) as the **Keep alive IP**
- Select **Show remote Network Neighborhood**.
- Click **OK**. (Figure14-28)

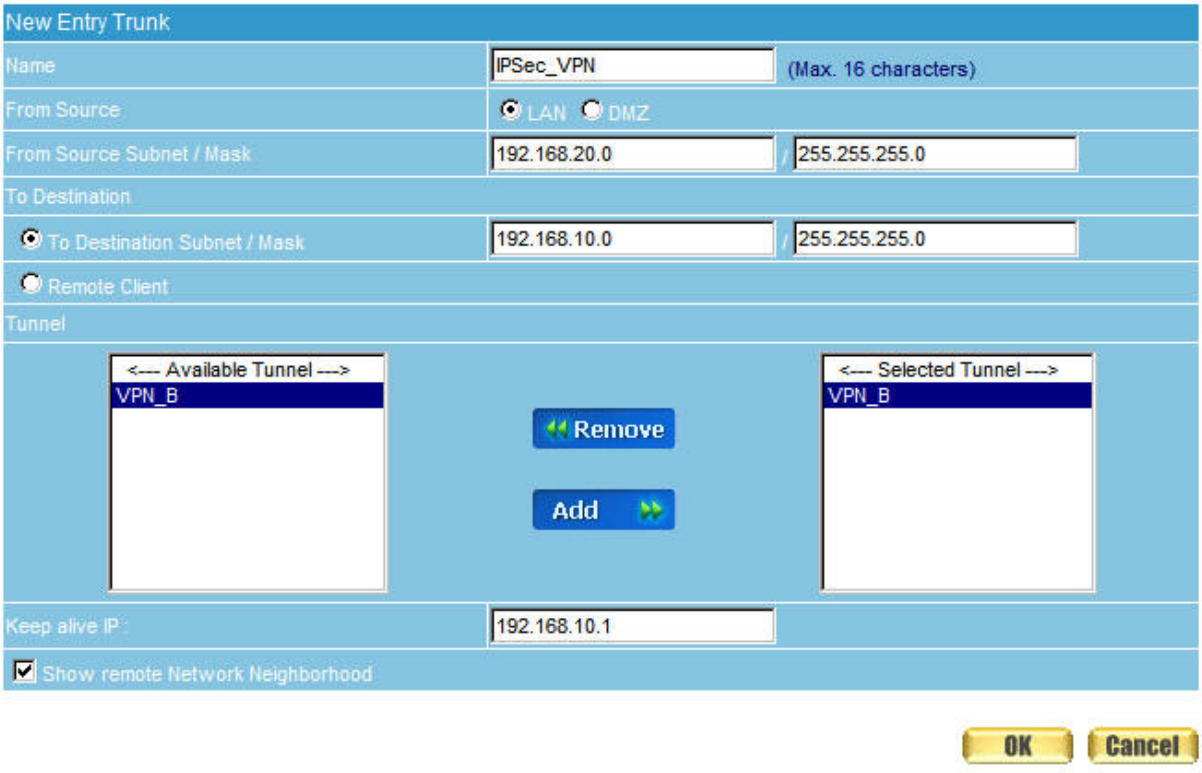


Figure14-27 New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN	192.168.20.0	192.168.10.0	VPN_B	Modify Remove Pause

New Entry

Figure14-28 Complete New Entry Tunnel Setting

STEP 10. Enter the following setting in **Outgoing Policy:** (Figure14-29)

- **Trunk:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure14-30)

Comment : (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	IPSec_VPN
Action, WAN Port	PERMIT ALL
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)

OK Cancel

Figure14-29 Setting the VPN Tunnel Outgoing Policy

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1

New Entry

Figure14-30 Complete the VPN Tunnel Outgoing Policy Setting

STEP 11. Enter the following setting in **Incoming Policy:** (Figure14-31)

- **Trunk:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure14-32)

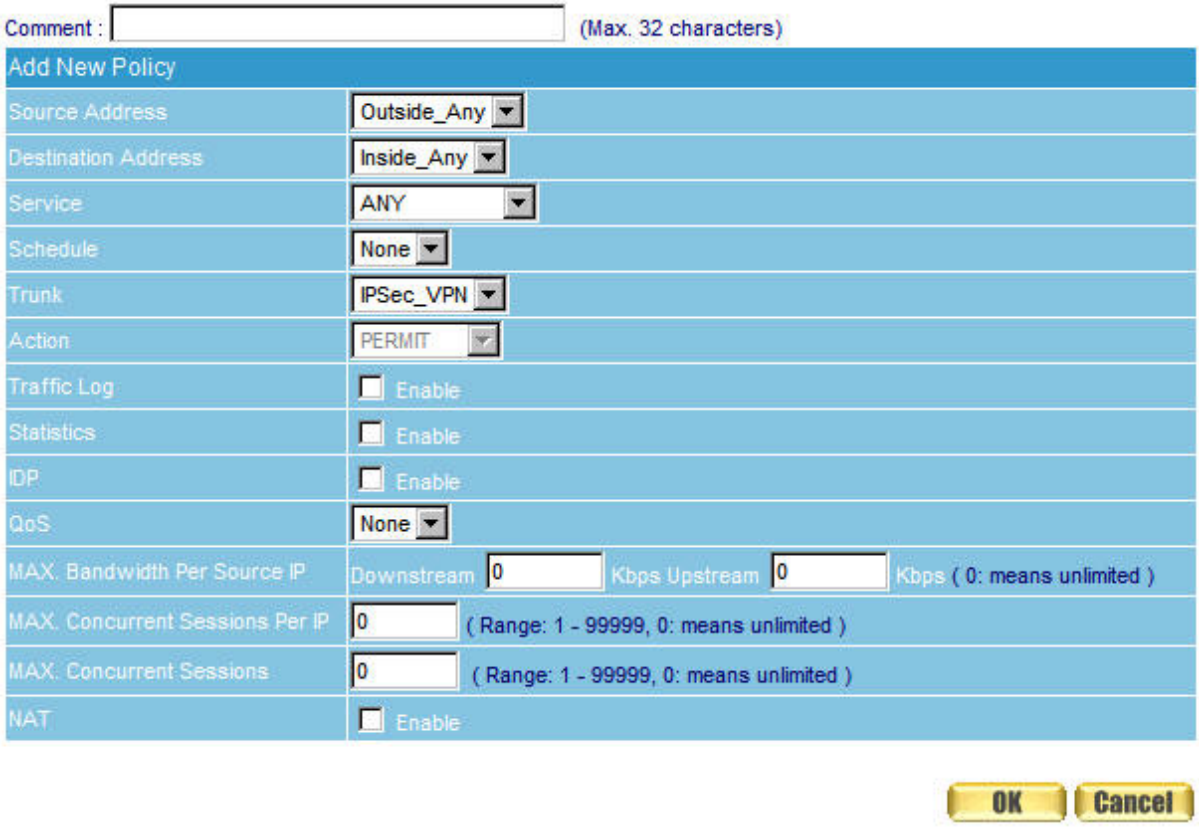


Figure14-31 Setting the VPN Tunnel Incoming Policy

Figure14-32 Complete the VPN Tunnel Incoming Policy Setting

STEP 12. **Complete IPSec VPN Connection.**

Setting PPTP VPN connection between two RS-3000s

Preparation

Company A **WAN IP: 61.11.11.11**
LAN IP: 192.168.10.X
Company B **WAN IP: 211.22.22.22**
LAN IP: 192.168.20.X

This example takes two RS-3000s as flattop. Suppose Company B 192.168.20.100 is going to have VPN connection with Company A 192.168.10.100 and download the resource.

The Default Gateway of Company A is the LAN IP of the RS-3000 192.168.10.1. Follow the steps below:

STEP 1. Enter **PPTP Server** of **VPN** function in the RS-3000 of Company A. Select **Modify** and enable PPTP Server:

- **Client IP Range**: Keep the setting with original, ex. 192.44.75.1-254.
- Enter **DNS Server** or **WINS Server** IP if necessary.
- Idle Time: Enter 0. (Figure14-33)

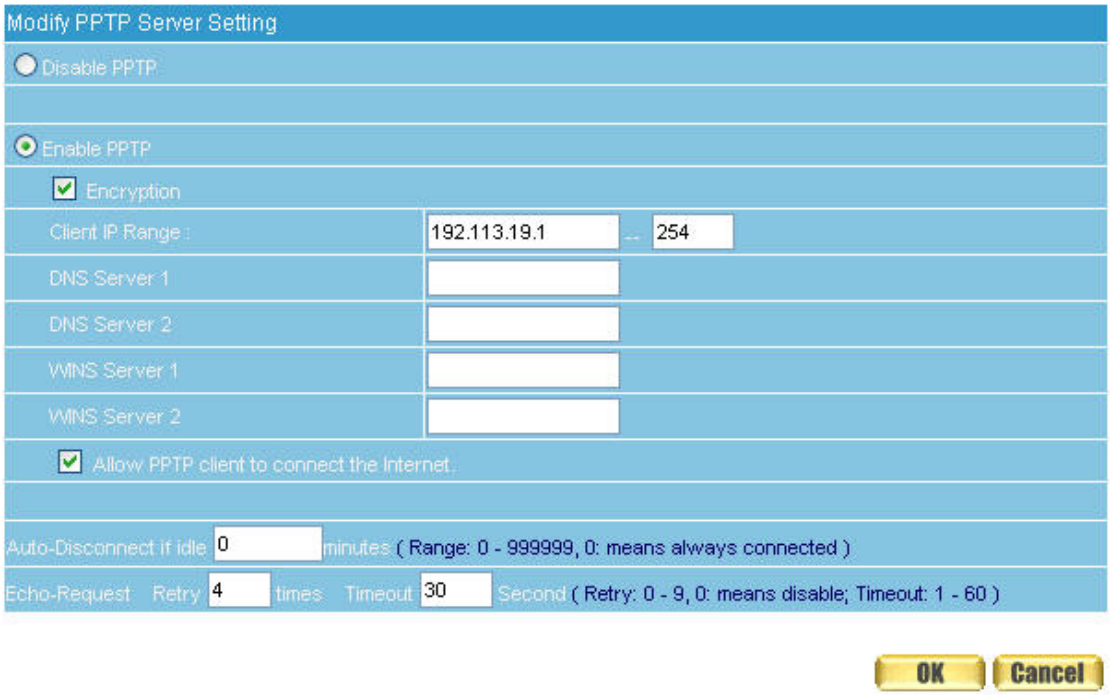


Figure14-33 Enable PPTP VPN Server Settings

Client IP Range: the setting can not be the same as LAN IP subnet, or the PPTP function will not be workable.

Idle Time: the setting time that the VPN Connection will auto-disconnect under unused situation. (Unit: minute)

STEP 2. Add the following settings in **PPTP Server** of **VPN** function in the RS-3000 of Company A:

- Select **New Entry**. (Figure14-34)
- **User Name**: Enter PPTP_Connection.
- **Password**: Enter 123456789.
- **Client IP assigned by**: Select **IP Range**.
- Click **OK**. (Figure14-35)

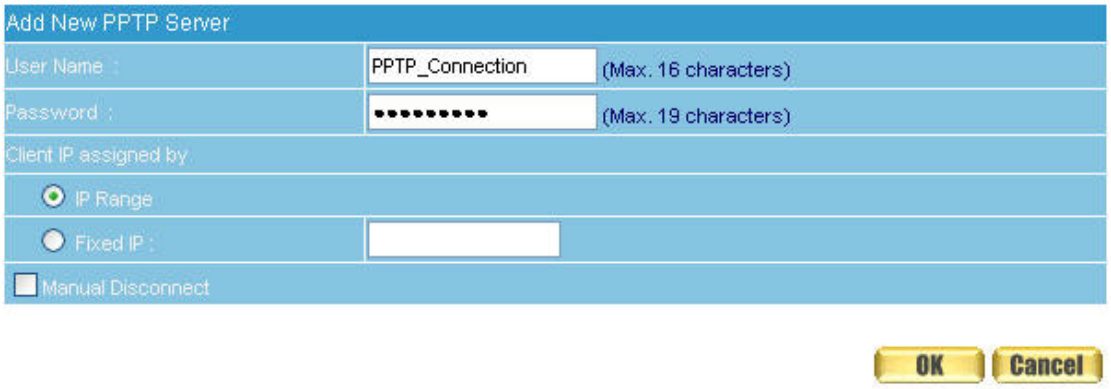


Figure 14-34 PPTP VPN Server Setting

Figure 14-35 Complete PPTP VPN Server Setting

STEP 3. Enter the following setting in **Trunk** of **VPN** function**:** (Figure14-36)

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP_Server_PPTP_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**. (Figure14-37)

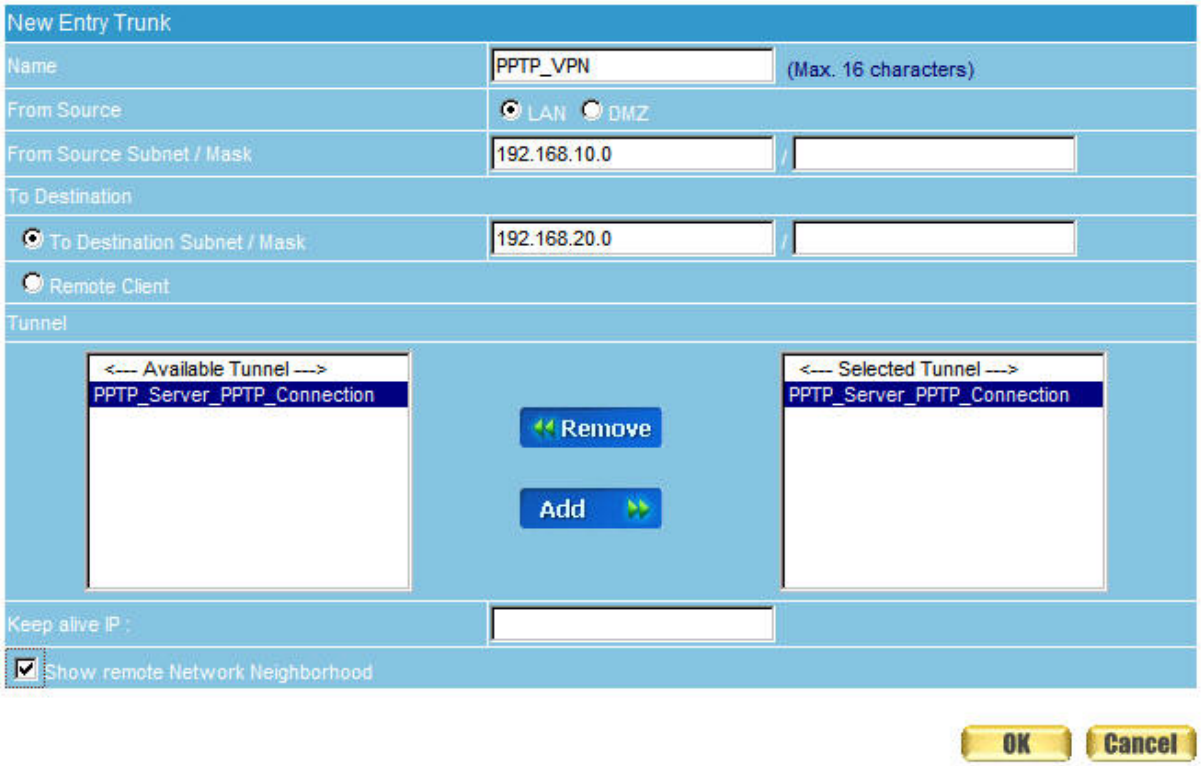


Figure14-36 New Entry Tunnel Setting

Figure14-37 Complete New Entry Tunnel Setting

STEP 4. Enter the following setting in **Outgoing Policy:** (Figure14-38)

- **Trunk:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure14-39)

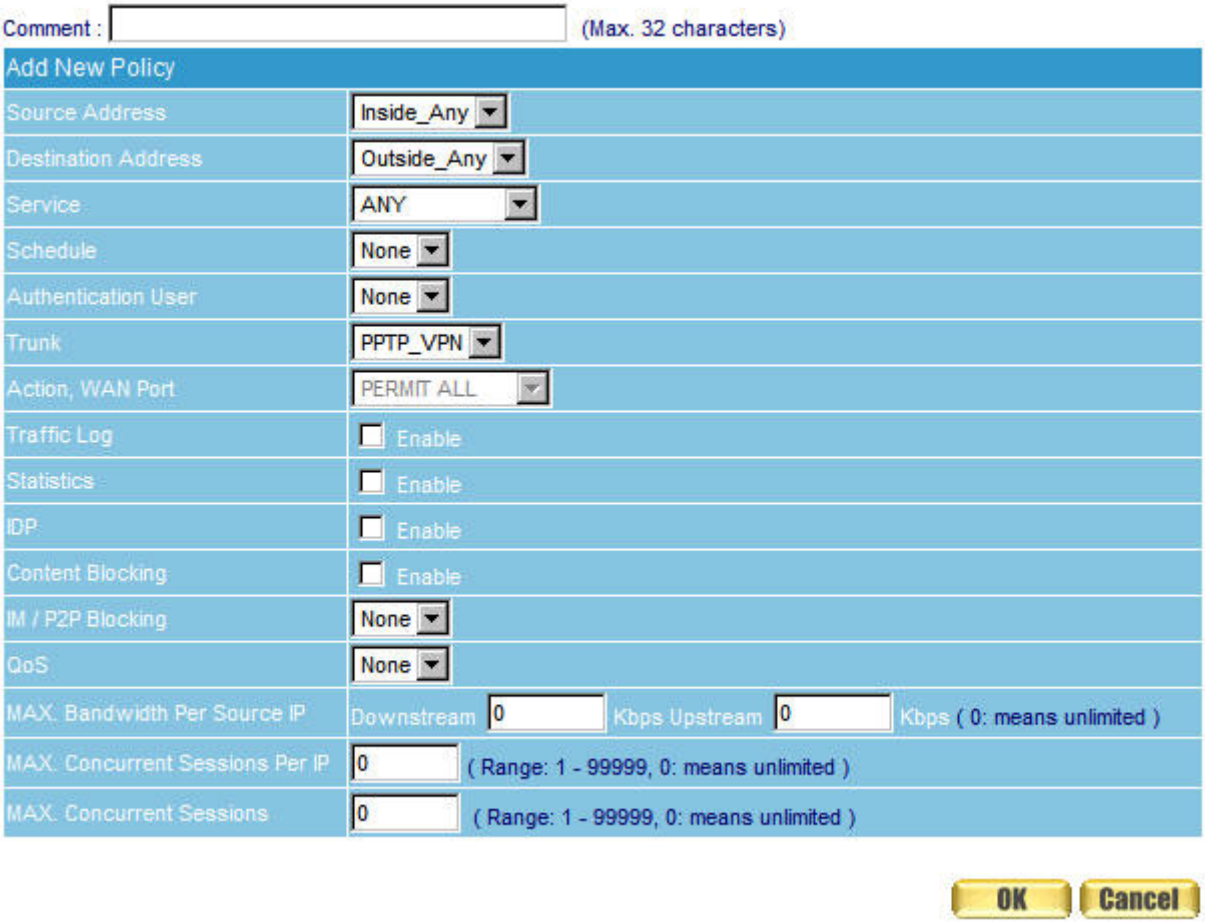


Figure14-38 Setting the VPN Tunnel Outgoing Policy

Figure14-39 Complete the VPN Tunnel Outgoing Policy Setting

STEP 5. Enter the following setting in **Incoming Policy:** (Figure14-40)

- **Trunk:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure14-41)

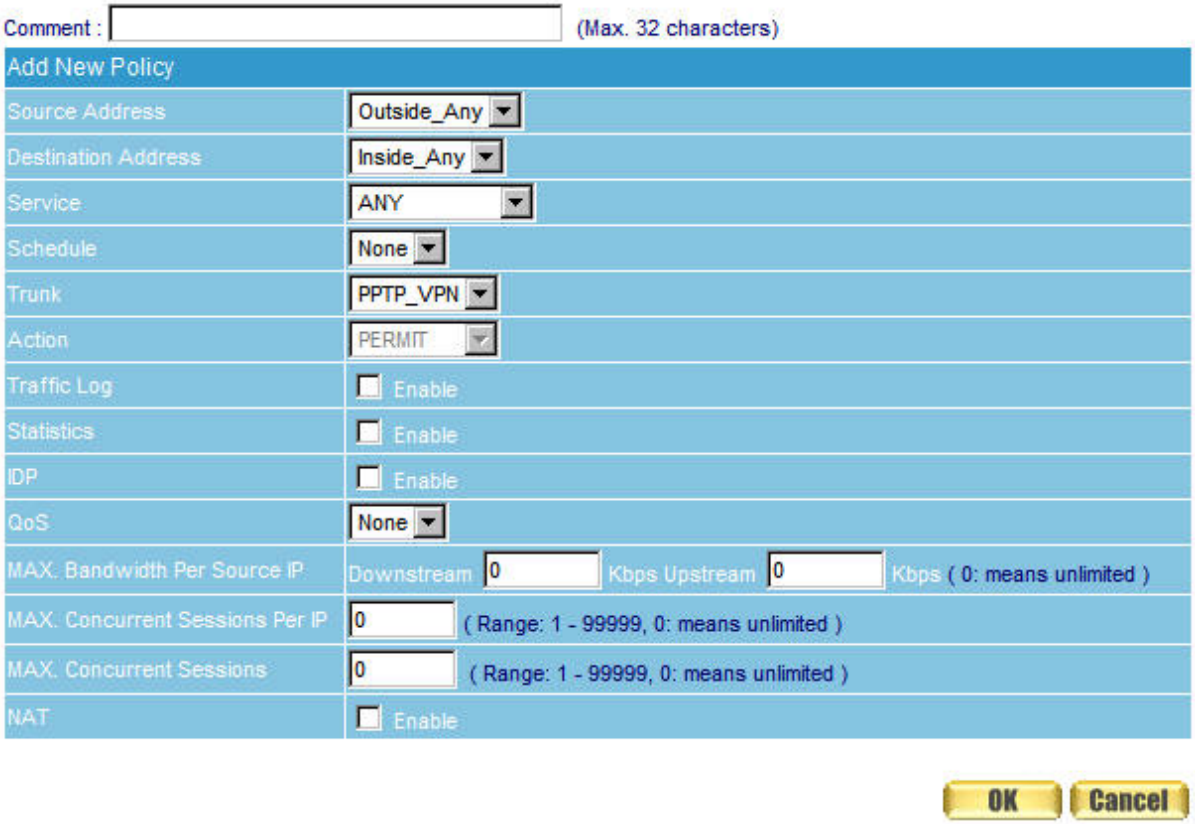


Figure14-40 Setting the VPN Tunnel Incoming Policy

Figure14-41 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the RS-3000 192.168.20.1. Follow the steps below:

STEP 1. Add the following settings in **PPTP Client** of **VPN** function in the RS-3000 of Company B:

- Click **New Entry** Button. (Figure14-42)
- **User Name**: Enter PPTP_Connection.
- **Password**: Enter123456789.
- **Server IP or Domain Name**: Enter 61.11.11.11.
- Select **Encryption**.
- Click **OK**. (Figure14-43)

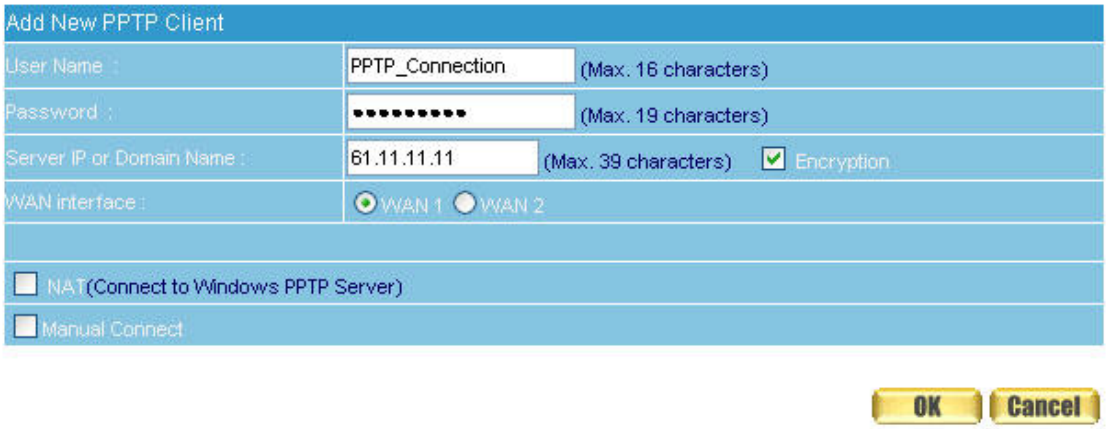


Figure 14-42 PPTP VPN Client Setting

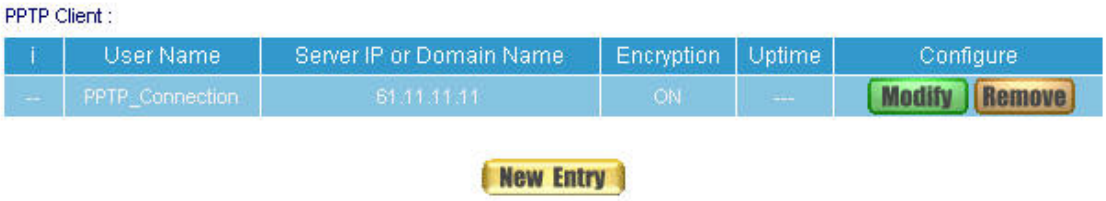


Figure 14-43 Complete PPTP VPN Client Setting

STEP 2. Enter the following setting in **Tunnel** of **VPN** function**:** (Figure14-44)

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP_Client_PPTP_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**. (Figure14-45)

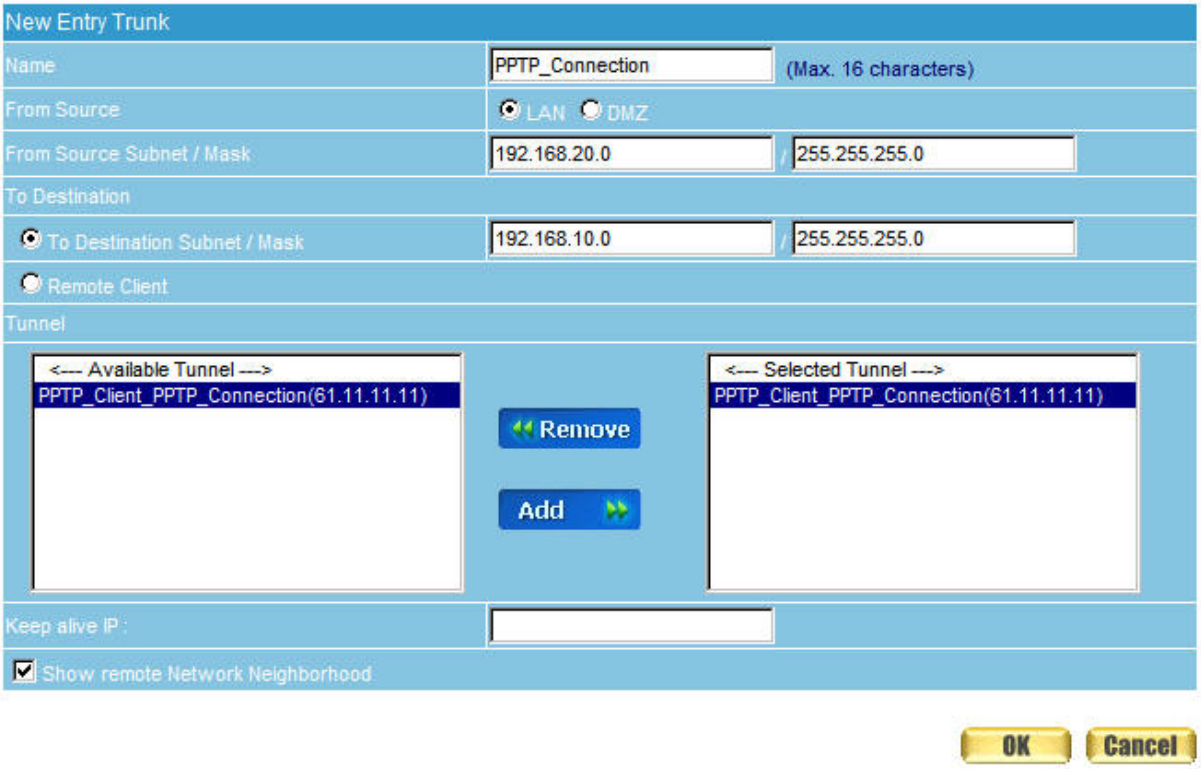


Figure14-44 New Entry Tunnel Setting

Figure14-45 Complete New Entry Tunnel Setting

STEP 3. Enter the following setting in **Outgoing Policy:** (Figure14-46)

- **Trunk:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure14-47)

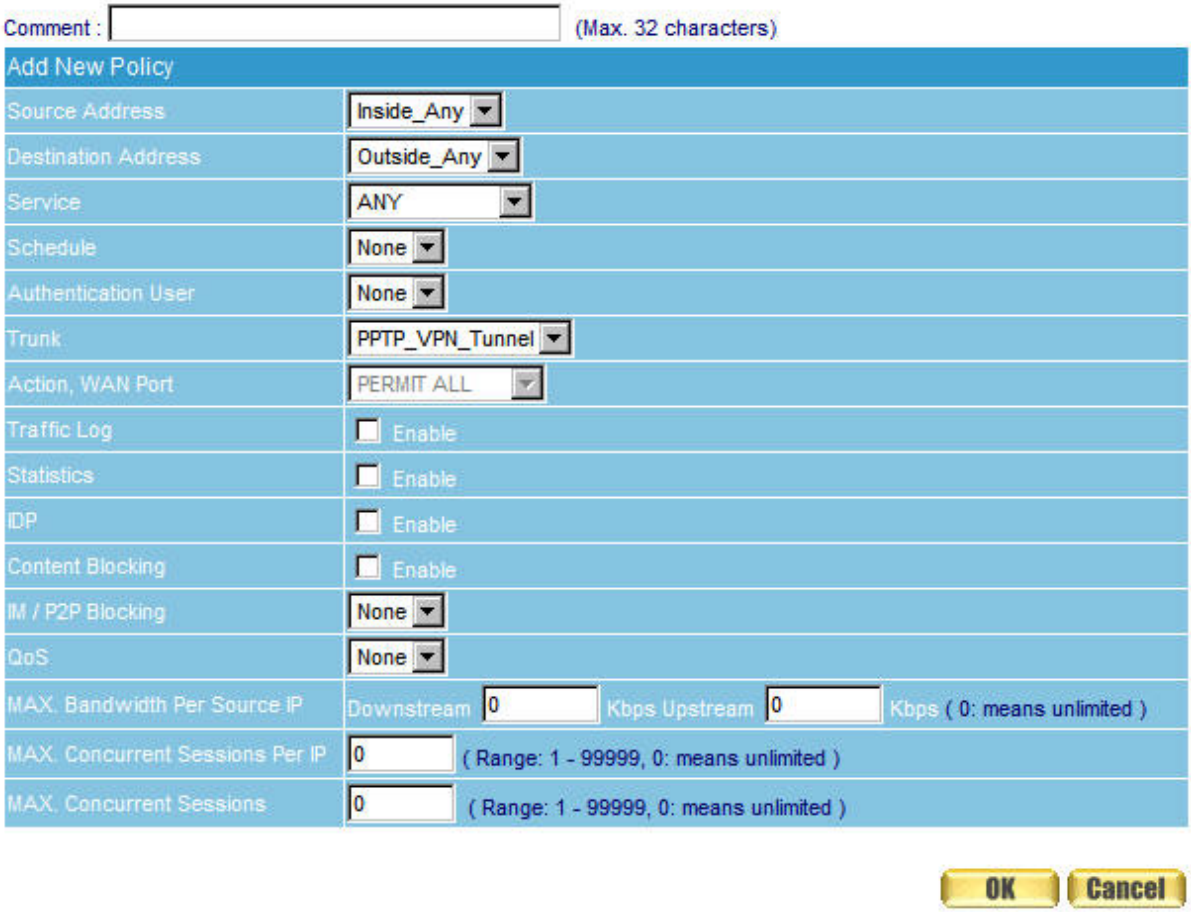


Figure14-46 Setting the VPN Tunnel Outgoing Policy

Figure14-47 Complete the VPN Tunnel Outgoing Policy Setting

STEP 4. Enter the following setting in **Incoming Policy:** (Figure14-48)

- **Trunk:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure14-49)

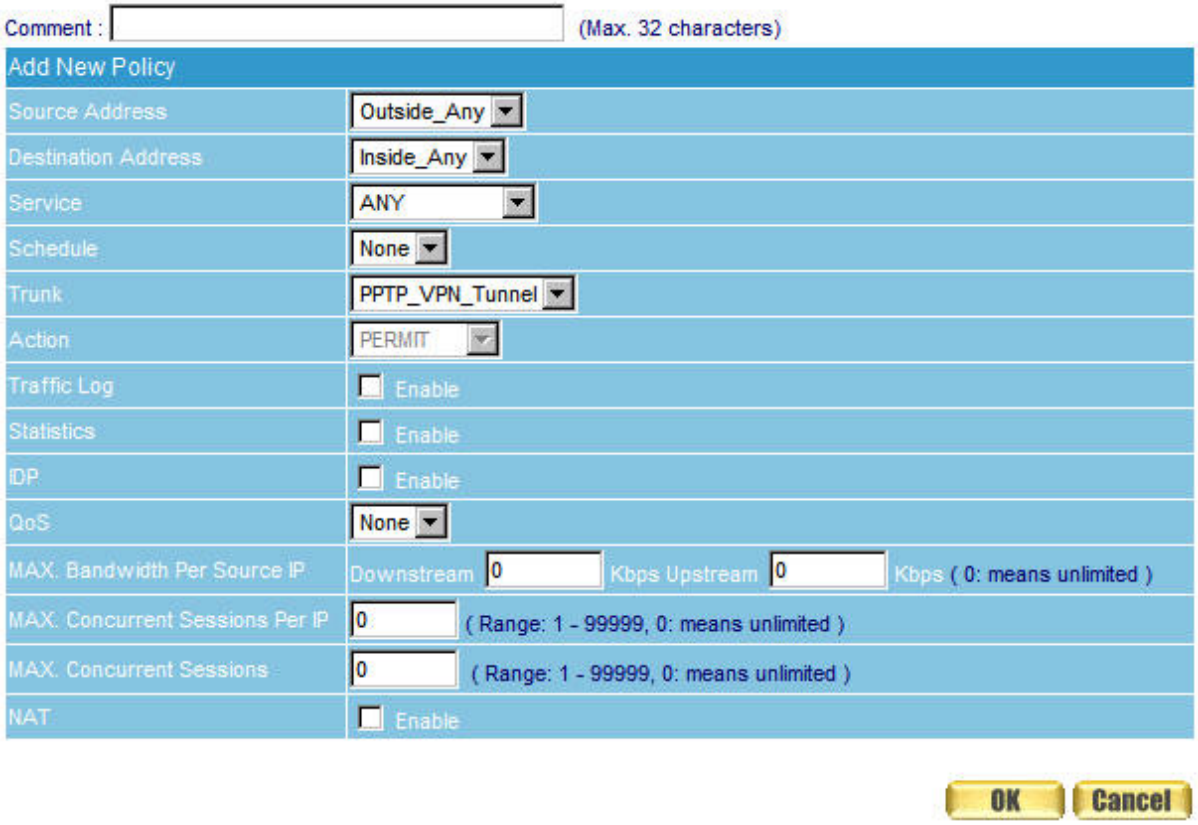


Figure14-48 Setting the VPN Tunnel Incoming Policy

Figure14-49 Complete the VPN Tunnel Incoming Policy Setting

STEP 5. **Complete PPTP VPN Connection**.

Chapter 15 Policy

Every packet has to be detected if it corresponds with Policy or not when it passes the RS-3000. When the conditions correspond with certain policy, it will pass the RS-3000 by the setting of Policy without being detected by other policy. But if the packet cannot correspond with any Policy, the packet will be intercepted.

The parameter of the policy includes Source Address, Destination Address, Service, Schedule, Authentication User, Tunnel, Action-WAN Port, Traffic Log, Statistics, Content Blocking, IM/P2P Blocking, QoS, MAX. Bandwidth Per Source IP, MAX. Concurrent Sessions Per IP and MAX. Concurrent Sessions. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the RS-3000.

 **How to use Policy?**

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

(1) **Outgoing:** The source IP is in LAN network; the destination is in WAN network. The system manager can set all the policy rules of Outgoing packets in this function

(2) **Incoming:** The source IP is in WAN network; the destination is in LAN network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of Incoming packets in this function

(3) **WAN to DMZ:** The source IP is in WAN network; the destination is in DMZ network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of WAN to DMZ packets in this function

(4) **LAN to DMZ:** The source IP is in LAN network; the destination is in DMZ network. The system manager can set all the policy rules of LAN to DMZ packets in this function

(5) **DMZ to LAN:** The source IP is in DMZ network; the destination is in LAN network. The system manager can set all the policy rules of DMZ to LAN packets in this function

(6) **DMZ to WAN:** The source IP is in DMZ network; the destination is in WAN network. The system manager can set all the policy rules of DMZ to WAN packets in this function

 All the packets that go through RS-3000 must pass the policy permission. Therefore, the LAN, WAN, and DMZ network have to set the applicable policy when establish network connection.

Define the required fields of Policy

Source and Destination:

- Source IP and Destination IP is according to the RS-3000's point of view. The active side is the source; passive side is destination.

Service:

- It is the service item that controlled by Policy. The user can choose default value or the custom services that the system manager set in **Service** function.

Action, WAN Port:

- Control actions to permit or reject packets that delivered between LAN network and WAN network when pass through RS-3000 (See the chart and illustration below)

Chart	Name	Illustration
	Permit all WAN network Interface	Allow the packets that correspond with policy to be transferred by WAN1/2 Port
	Permit WAN1	Allow the packets that correspond with policy to be transferred by WAN1 Port
	Permit WAN2	Allow the packets that correspond with policy to be transferred by WAN2 Port
	DENY	Reject the packets that correspond with policy to be transferred by WAN Port
	Permit VPN	Allow the VPN packets that correspond with policy to be transferred

Option:

- To display if every function of Policy is enabled or not. If the function is enabled and then the chart of the function will appear (See the chart and illustration below)

Chart	Name	Illustration
	Schedule	Enable the policy to automatically execute the function in a certain time
	Authentication User	Enable Authentication User
	Traffic Log	Enable traffic log
	Statistics	Enable traffic statistics
	IDP	Enable IDP
	Content Blocking	Enable Content Blocking
	IM / P2P Blocking	Enable IM / P2P Blocking
	QoS	Enable QoS

Schedule:

- Setting the policy to automatically execute the function in a certain time

Authentication User:

- The user have to pass the authentication to connect by Policy

Trunk:

- Select the specific VPN setting to allow the packets passing through.

Traffic Log:

- Record all the packets that go through policy.

Statistics:

- Chart of the traffic that go through policy

IDP:

- Select to enable IDP feature in Policy

Content Blocking:

- To restrict the packets that passes through the policy

IM / P2P Blocking:

- To restrict the packets passing via IM or P2P

QoS:

- Setting the Guarantee Bandwidth and Maximum Bandwidth of the Policy (the bandwidth is shared by the users who correspond to the Policy)

MAX. Bandwidth Per Source IP:

- Set the maximum bandwidth that permitted by policy. And if the IP bandwidth exceed the setting value, the surplus connection cannot be set successfully.

MAX. Concurrent Sessions Per IP:

- Set the concurrent sessions that permitted by policy. And if the IP sessions exceed the setting value, the surplus connection cannot be set successfully.

MAX. Concurrent Sessions:

- Set the concurrent sessions that permitted by policy. And if the whole Policy sessions exceed the setting value, the surplus connection cannot be set successfully.

Move:

- Every packet that passes the RS-3000 is detected from the front policy to the last one. So it can modify the priority of the policy from the selection.

Set up the policy that can monitor the internal users. (Take Logging, Statistics, and Alarm Threshold for example)

STEP 1 . Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- Select **Traffic Log**
- Select **Statistics**
- Click **OK** (Figure15-1)

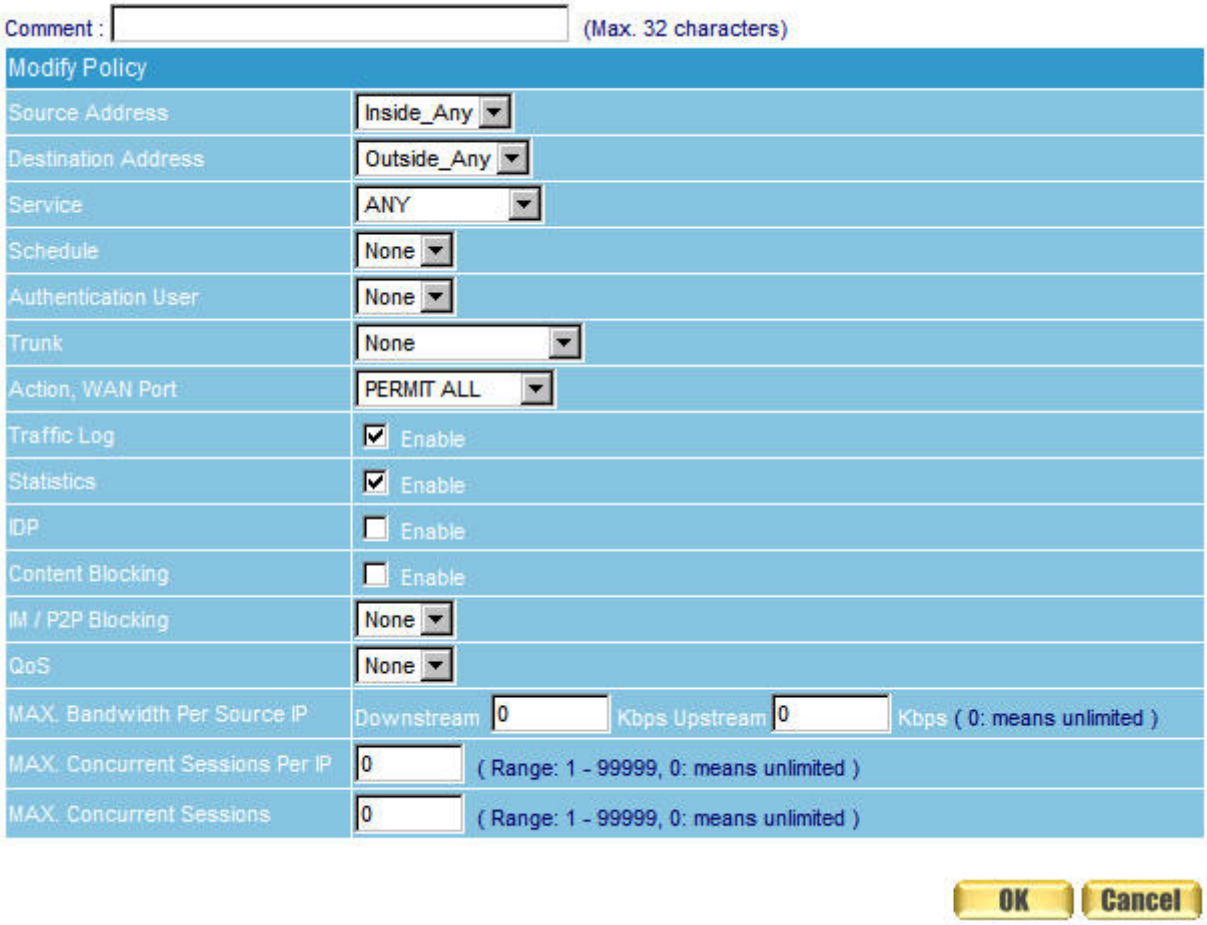


Figure15-1 Setting the different Policies

STEP 2 . Complete the setting of Logging, Statistics, and Alarm Threshold in **Outgoing Policy**: (Figure15-2)

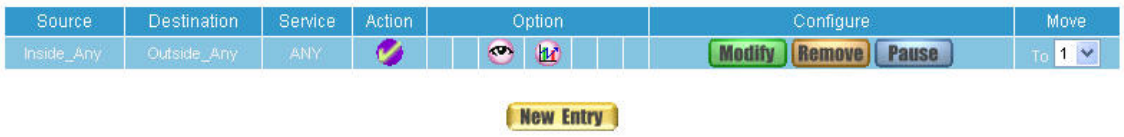


Figure15-2 Complete Policy Setting

STEP 3 . Obtain the information in **Traffic** of **Log** function if you want to monitor all the packets of the RS-3000. (Figure15-3)

Figure15-3 Traffic Log Monitor WebUI

STEP 4 . To display the traffic record that through Policy to access to Internet in **Policy Statistics** of **Statistics** function. (Figure15-4)

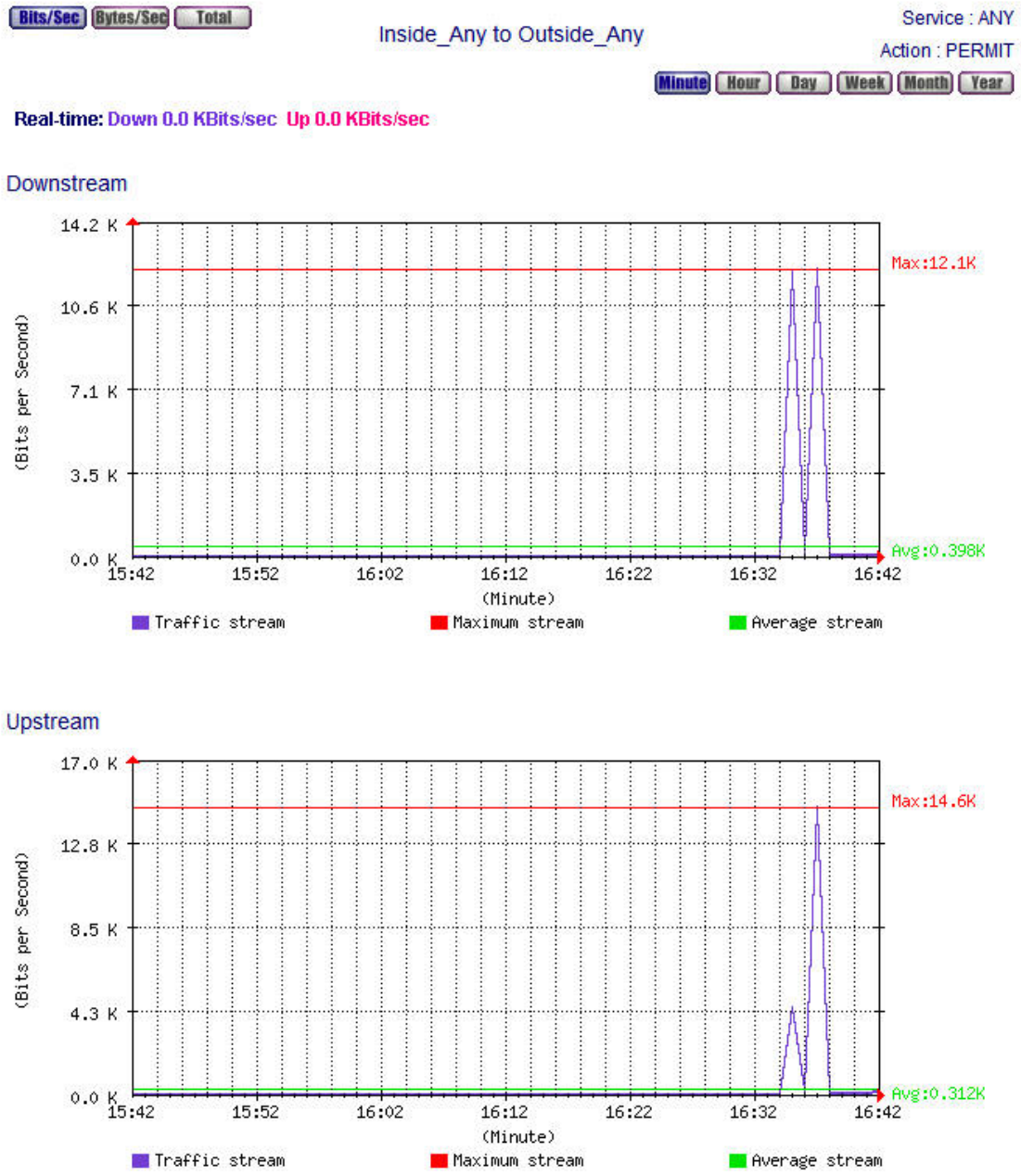


Figure15-4 Statistics WebUI

Forbid the users to access to specific network. (Take specific WAN IP, Content Blocking and IM/P2P Blocking for example)

STEP 1 . Enter the following setting in **URL Blocking, Script Blocking,** and **Download Blocking** in **Content Blocking** function, and **IM/P2P Blocking** Function: (Figure15-5, 15-6, 15-7, 15-8)

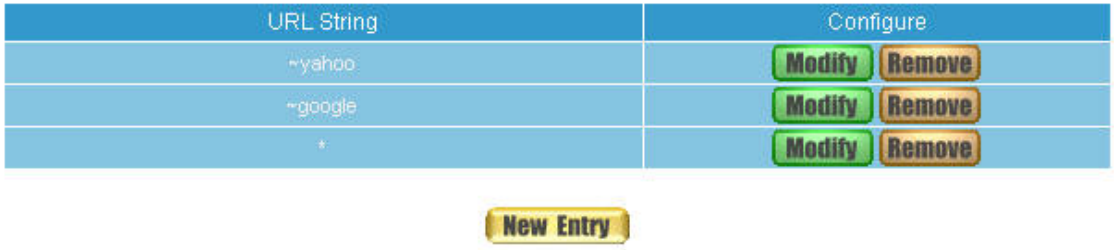


Figure15-5 URL Blocking Setting

Figure15-6 Script Blocking Setting

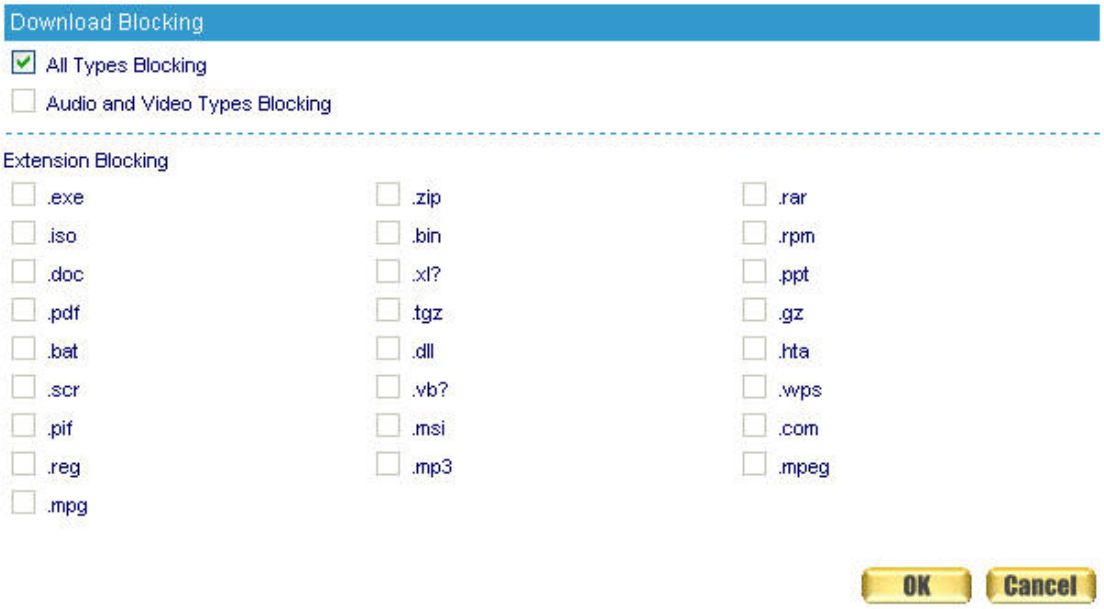


Figure15-7 Download Blocking Setting

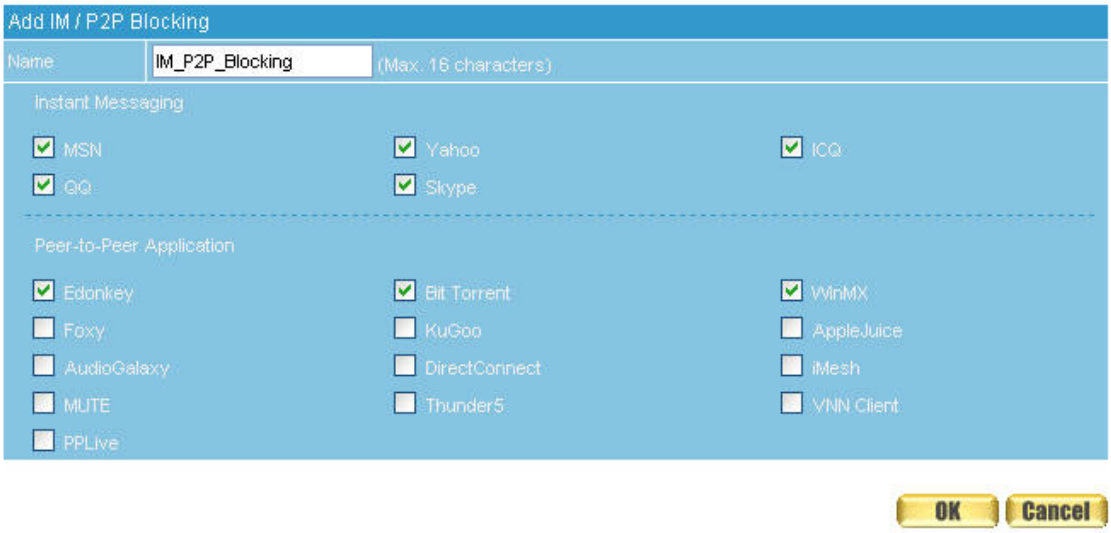


Figure15-8 IM / P2P Blocking Setting

URL Blocking can restrict the Internal Users only can access to some specific Website.

Script Blocking can restrict the Internal Users to access to Script file of Website. (Java, Cookies…, etc.)

Download Blocking can restrict the Internal Users to access to video, audio, and some specific sub-name file by http protocol directly.

IM/P2P Blocking can restrict the Internal Users to send message, files, audio, and video by instant messaging (Ex: MSN, Yahoo Messenger, QQ, ICQ and Skype), and to access to the file on Internet by P2P (eDonkey, BT).

STEP 2 **.** Enter as following in **WAN** and **WAN Group** of **Address** function: (Figure15-9, 15-10)

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
Remote_Server1	61.11.11.11/255.255.255.255	Modify Remove
Remote_Server2	211.22.22.22/255.255.255.255	Modify Remove

New Entry

Figure15-9 Setting the WAN IP that going to block

Name	Member	Configure
WAN_Group	Remote_Server1, Remote_Server2	Modify Remove Pause

New Entry

Figure15-10 WAN Address Group

The Administrator can group the custom address in **Address**. It is more convenient when setting policy rule.

STEP 3 . Enter the following setting in **Outgoing Policy:**

- Click **New Entry**
- **Destination Address:** Select WAN_Group that set by **STEP 2**. (Blocking by IP)
- **Action, WAN Port:** Select **Deny**
- Select to enable **Content Blocking**
- Select to enable **IM/P2P Blocking**
- Click **OK** (Figure15-11)

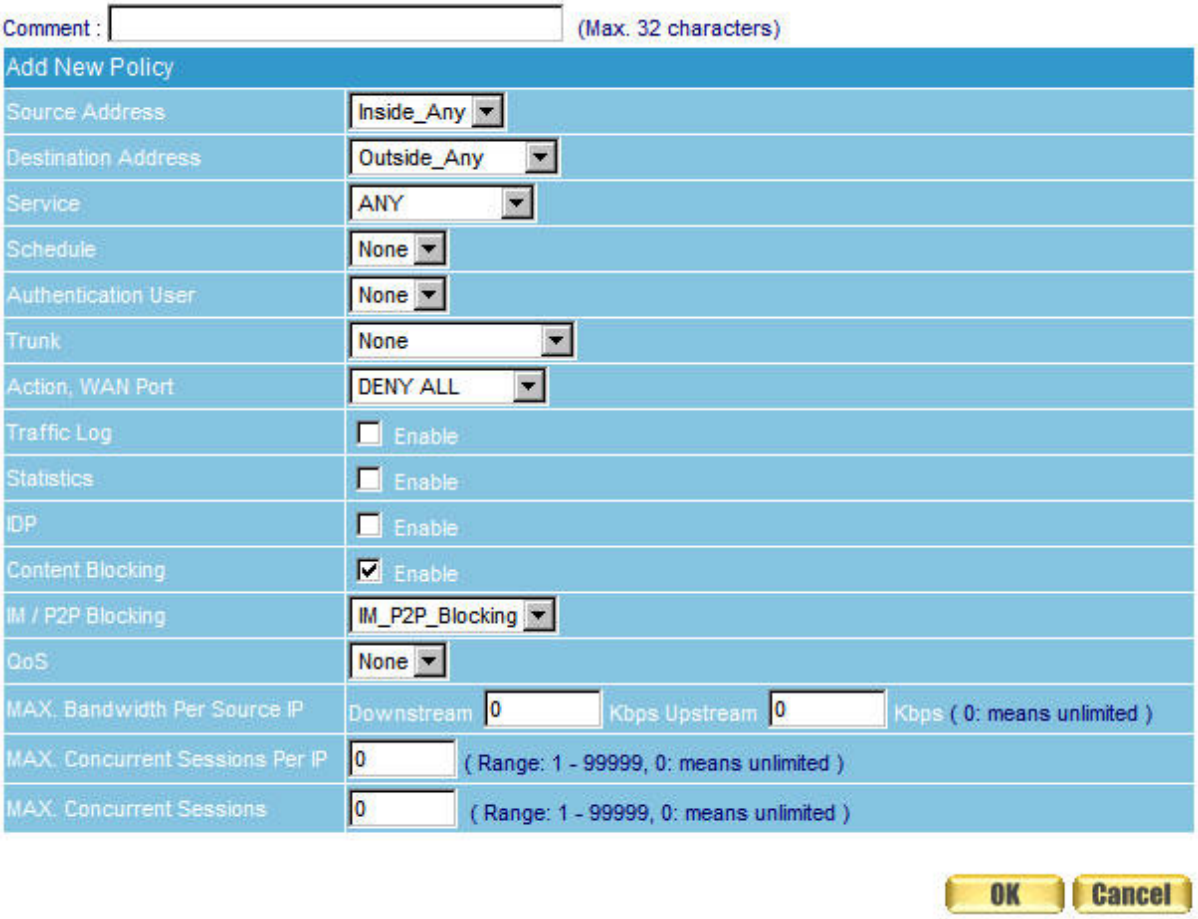


Figure15-11 Setting Blocking Policy

STEP 4 . Complete the setting of forbidding the users to access to specific network. (Figure15-12)

Figure15-12 Complete Policy Setting

Deny in Policy can block the packets that correspond to the policy rule. The System Administrator can put the policy rule in the front to prevent the user connecting with specific IP.

Only allow the users who pass Authentication to access to Internet in particular time

STEP 1 . Enter the following in **Schedule** function: (Figure15-13)

Figure15-13 Add New Schedule

STEP 2 . Enter the following in **Auth User** and **Auth User Group** in **Authentication** function**:** (Figure15-14)

Figure15-14 Setting Auth User Group

The Administrator can use group function the **Authentication** and **Service**. It is more convenient when setting policy.

STEP 3 . Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- **Authentication User:** Select laboratory
- **Schedule:** Select Working_Time
- Click **OK** (Figure15-15)

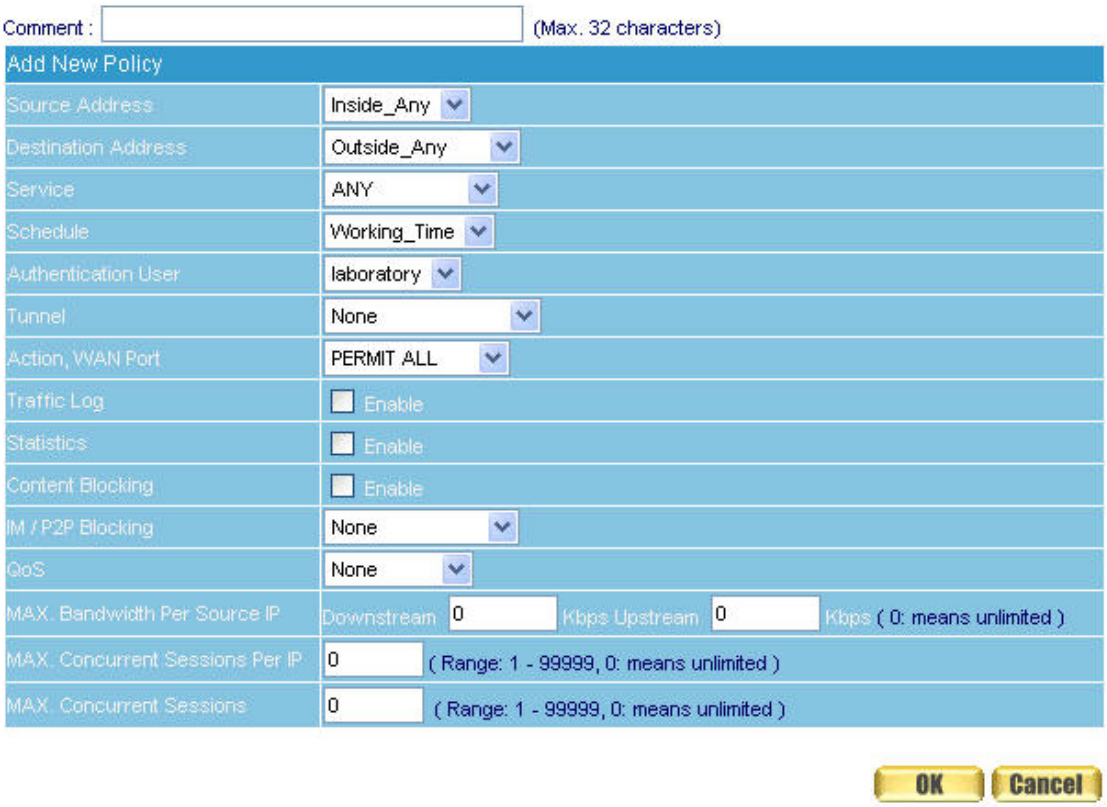


Figure15-15 Setting a Policy of Authentication and Schedule

STEP 4 . Complete the policy rule of only allows the users who pass authentication to access to Internet in particular time. (Figure15-16)

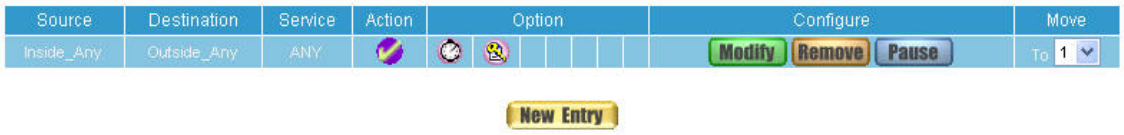


Figure15-16 Complete Policy Setting

The external user controls the internal PC through remote control software (Take pcAnywhere for example)

STEP 1 . Set up a Internal PC controlled by external user, and Internal PC's IP Address is 192.168.1.2

STEP 2 . Enter the following setting in **Virtual Server1** of **Virtual Server** function**:** (Figure15-17)

Figure15-17 Setting Virtual Server

STEP 3 . Enter the following in **Incoming Policy**:

- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select PC-Anywhere (5631-5632)
- Click **OK** (Figure15-18)

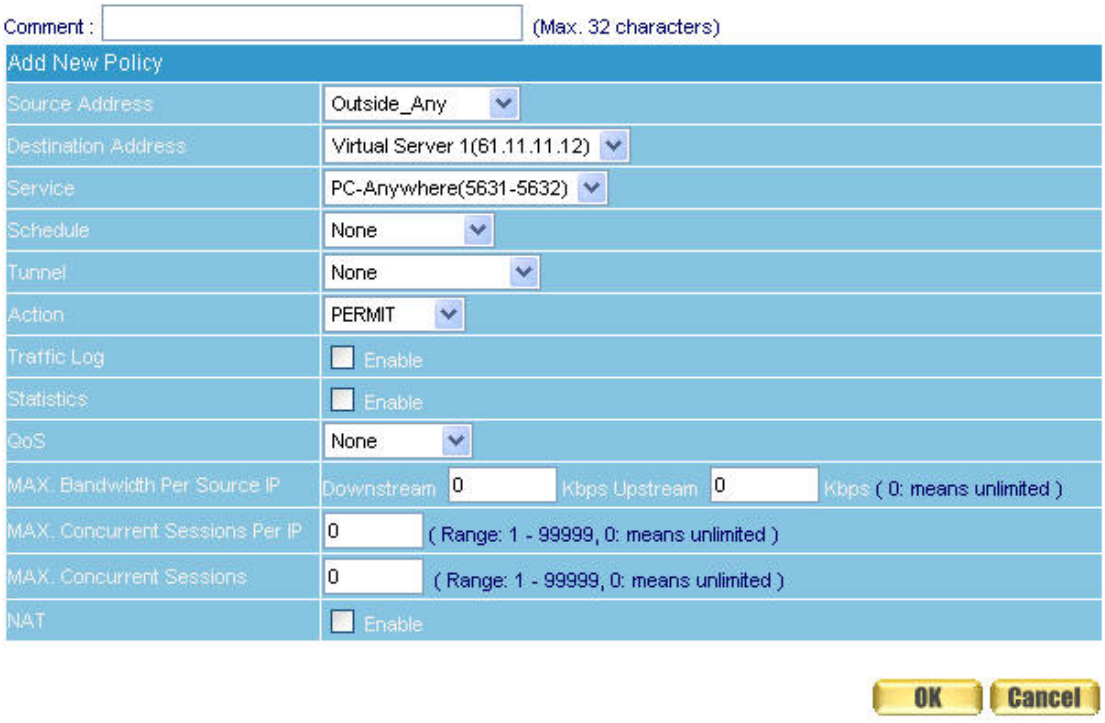


Figure15-18 Setting the External User Control the Internal PC Policy

STEP 4 . Complete the policy for the external user to control the internal PC through remote control software. (Figure15-19)

Figure15-19 Complete Policy Setting

Set a FTP Server under DMZ NAT Mode and restrict the download bandwidth and the MAX. Concurrent Sessions.

STEP 1 . Set a FTP Server under **DMZ**, which IP is 192.168.3.2 (The DMZ Interface Address is 192.168.3.1/24)

STEP 2 . Enter the following setting in **Virtual Server1** of **Virtual Server** function**:** (Figure15-20)

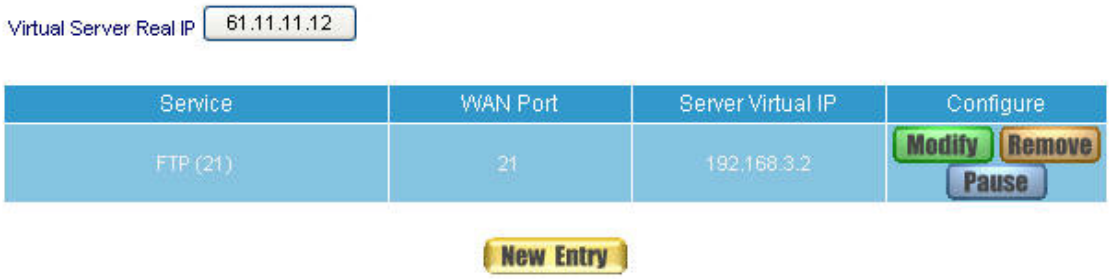


Figure15-20 Setting up Virtual Server Corresponds to FTP Server

When using the function of **Incoming** or **WAN to DMZ** in **Policy**, strong suggests that cannot select **ANY** in **Service**. It may be attacked by Hacker easily.

STEP 3 . Enter the following in **QoS:** (Figure15-21)

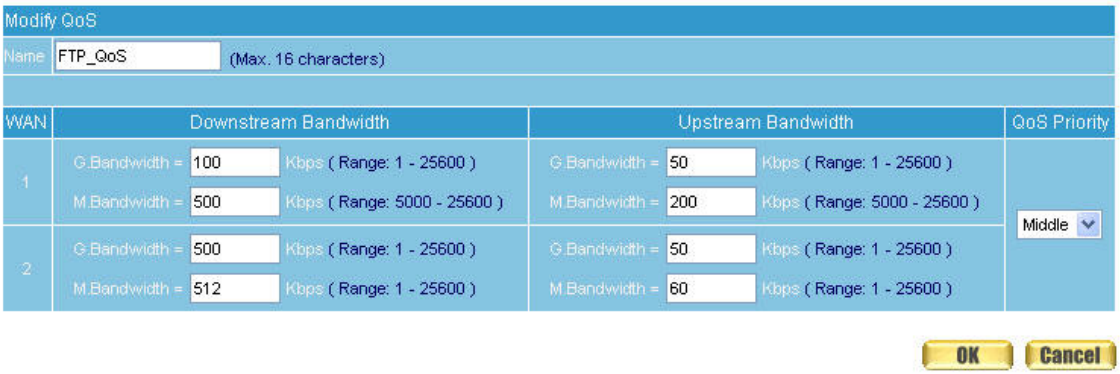


Figure15-21 QoS Setting

STEP 4 . Enter the following in **WAN to DMZ Policy:**

- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select FTP (21)
- **QoS:** Select FTP_QoS
- **MAX. Concurrent Sessions:** Enter 100
- Click **OK** (Figure15-22)

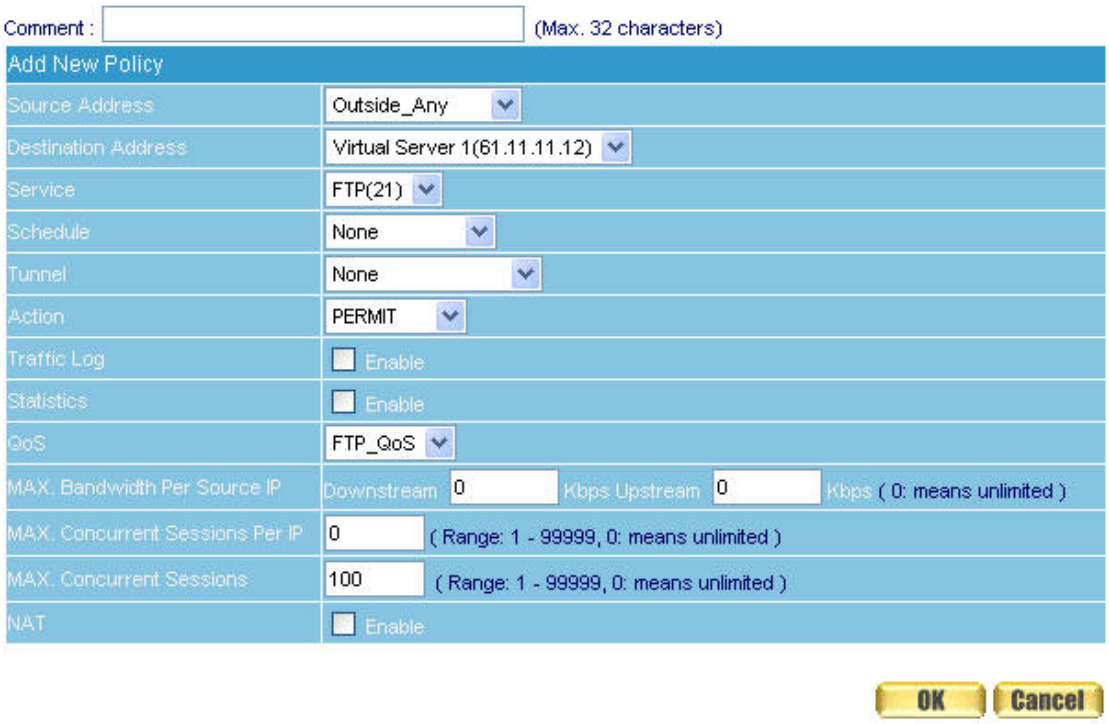


Figure15-22 Add New Policy

STEP 5 . Complete the policy of restricting the external users to access to internal network server (which may occupy the resource of network) (Figure15-23)

Figure15-23 Complete the Policy Setting

Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode

STEP 1 . Set a Mail Server in **DMZ** and set its network card's IP Address as 61.11.11.12. The DNS setting is external DNS Server.

STEP 2 . Add the following setting in **DMZ** of **Address** function**:** (Figure15-24)

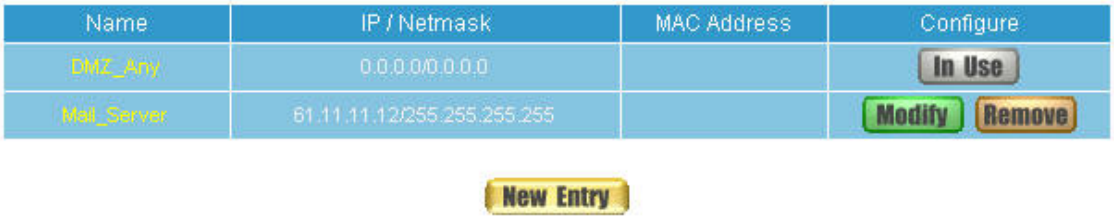


Figure15-24 Specify Mail Server's IP

STEP 3 . Add the following setting in **Group** of **Service** function: (Figure15-25)

Figure15-25 Setting up a Service Group that has POP3, SMTP, and DNS

STEP 4 . Enter the following setting in **WAN to DMZ Policy**:

- Click **New Entry**
- **Destination Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK** (Figure15-26)

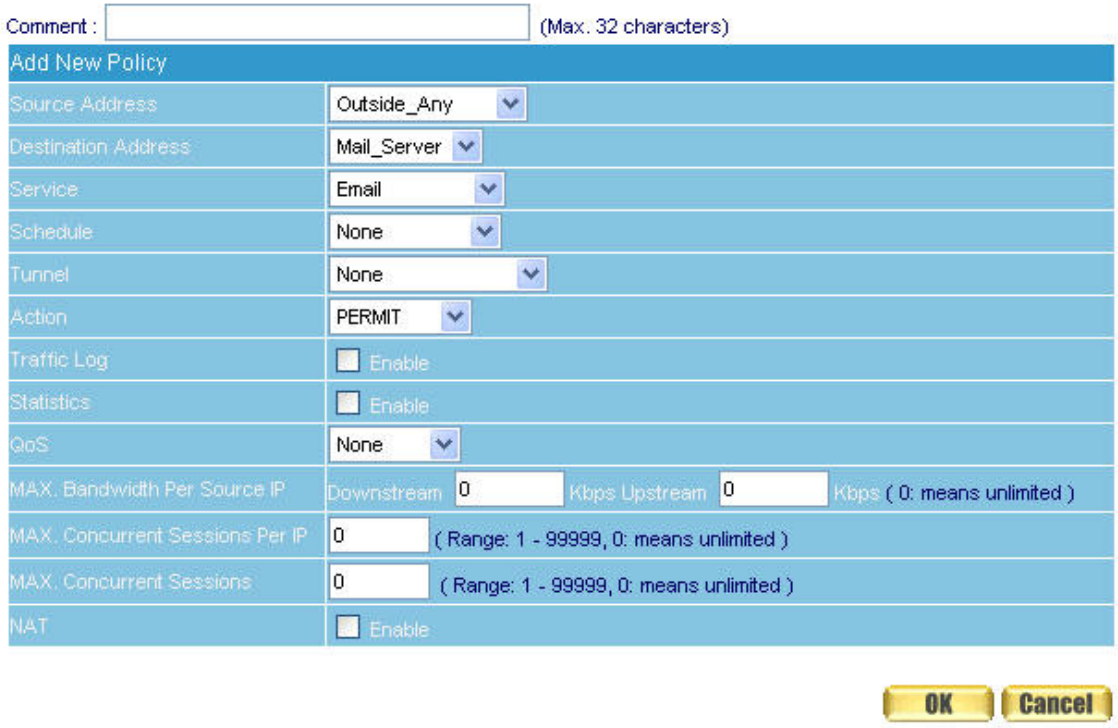


Figure15-26 Setting a Policy to access Mail Service by WAN to DMZ

STEP 5 . Complete the policy to access mail service by **WAN to DMZ**. (Figure15-27)

Figure15-27 Complete the Policy to access Mail Service by WAN to DMZ

STEP 6 . Add the following setting in **LAN to DMZ Policy**:

- Click **New Entry**
- **Destination Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK** (Figure15-28)

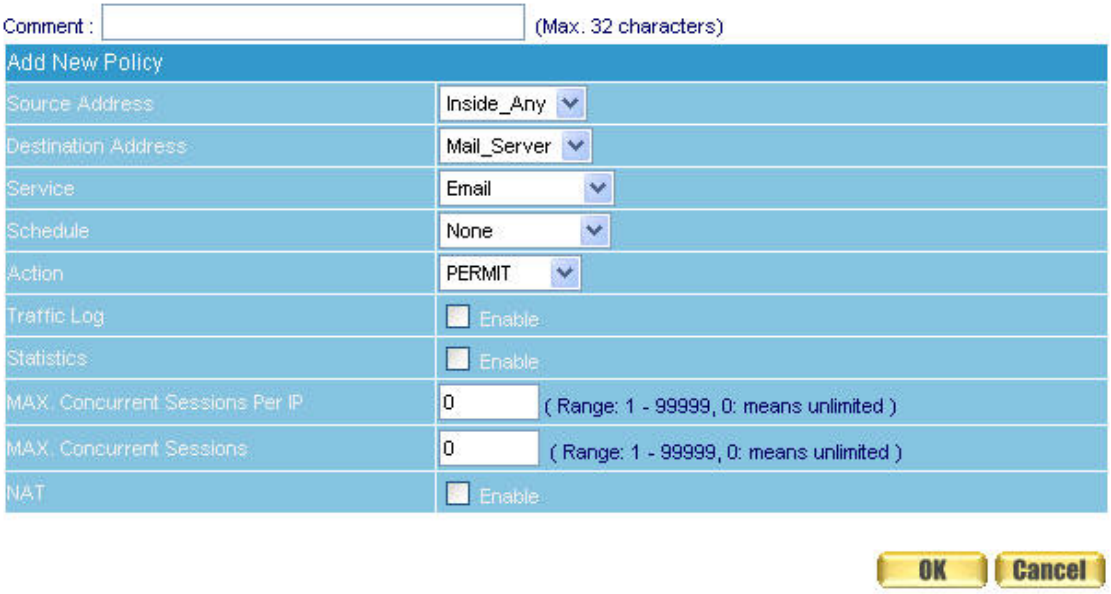


Figure15-28 Setting a Policy to access Mail Service by LAN to DMZ

STEP 7 . Complete the policy to access mail service by **LAN to DMZ** (Figure15-29)

Figure15-29 Complete the Policy to access Mail Service by LAN to DMZ

STEP 8 . Add the following setting in **DMZ to WAN Policy**:

- Click **New Entry**
- **Source Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK** (Figure15-30)

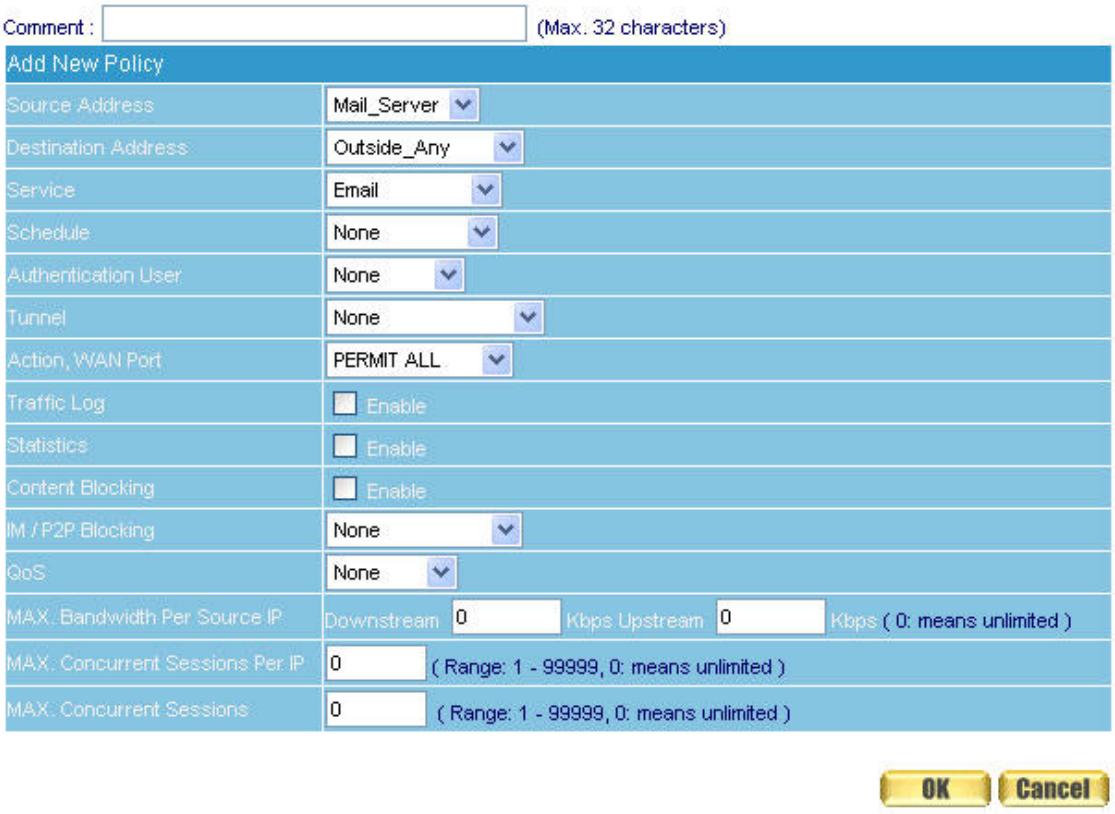


Figure15-30 Setting the Policy of Mail Service by DMZ to WAN

STEP 9 . Complete the policy access to mail service by **DMZ to WAN**. (Figure15-31)

Figure15-31 Complete the Policy access to Mail Service by DMZ to WAN

Chapter 16 Mail Security

According to the Mail Security Configure function, it means the dealing standard towards mail of RS-3000. In this chapter, it is defined as Setting and Mail Relay.

After scanning the mails that sent to Internal Mail Server by **Anti-Spam** and **Anti-Virus** functions of RS-3000, then to setup the relevant setting in **Mail Relay** function.

Define the required fields of Setting:

Scanned Mail Setting:

- It can setup to deal with the size of mail in order to judge if to scan the mail or not.

Unscanned Mail Setting:

- According to the unscanned mail, it can add an unscanned message in the mail subject.
  - For example, add the following setting in this function:
    1. The scanned mail size is less than 200Kbytes
    2. Add the message to the subject line --Unscanned--
    3. Click OK (Figure16-1)

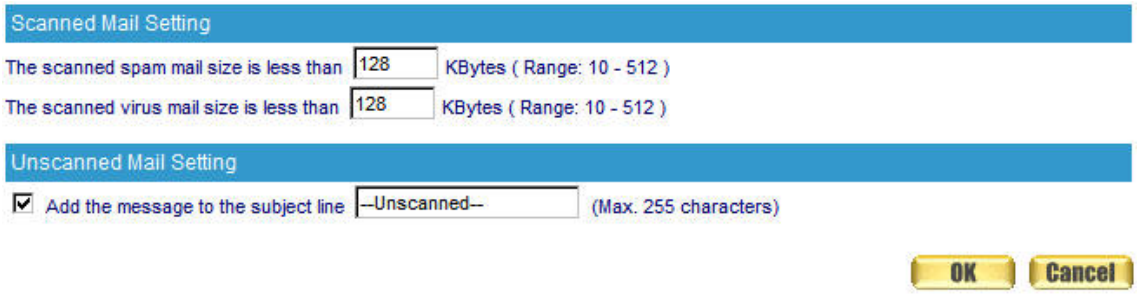


Figure16-1 Scanned Mail Setting

◆ When receive unscanned mail, it will add the tag in front of the e-mail subject. (Figure16-2)

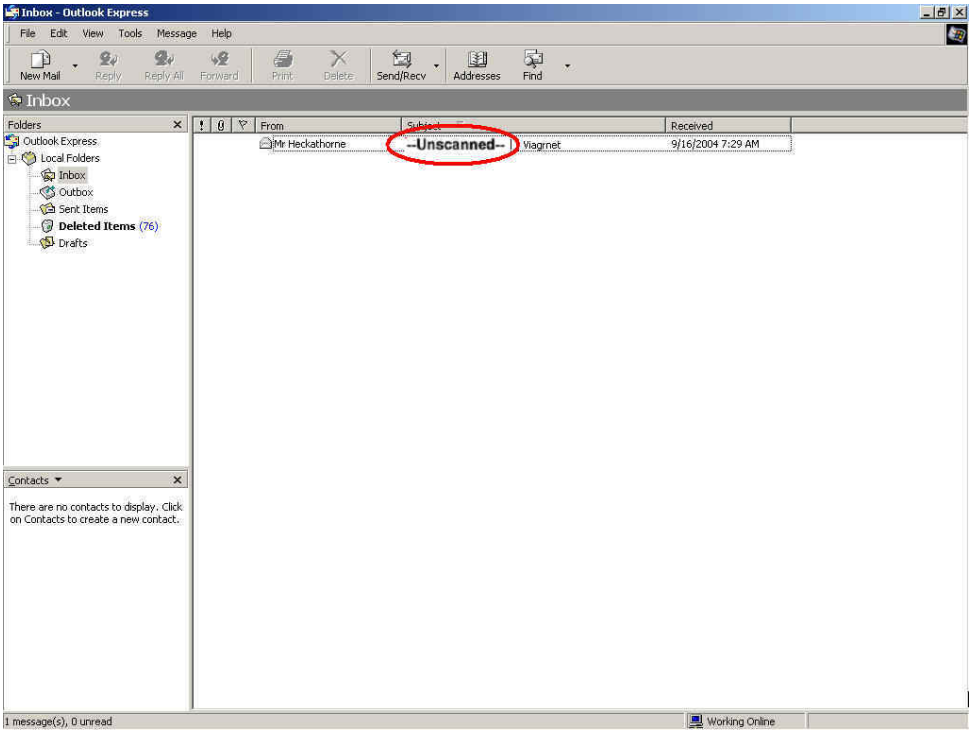


Figure16-2 The Unscanned Mail Subject WebUI

To setup RS-3000 as Gateway (Mail Server is in DMZ, Transparent Mode)

Preparation

WAN Port IP: 61.11.11.11

Mail Server IP: 61.11.11.12

Map the DNS Domain Name that apply from ISP (broadband.com.tw) to DNS Server IP (setup MX record is Mail Server IP)

When external sender to send mail to the recipient account in broadband.com.tw, add the following Mail Relay setting:

STEP 1． Add the following setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to
- **Mail Relay** setting is complete. The mails from external and its destination mail server have to be in the domain name setting, that can be received by RS-3000 and be sent to the appointed mail server after filtering. (Figure16-3)

Figure16-3 Mail Relay Setting WebUI

To setup RS-3000 between the original Gateway and Mail Server (Mail Server is in DMZ, Transparent Mode)

Preparation

The Original Gateway's LAN Subnet: 172.16.1.0/16

WAN Port IP: 61.11.11.11

RS-3000's WAN Port IP: 172.16.1.12

Mail Server IP: 172.16.1.13

Map the DNS Domain Name (broadband.com.tw) to DNS Server IP (setup MX record is Mail Server IP) When LAN (172.16.1.0/16) user use the sender account of broadband.com.tw mail server to send mail to the recipient account in external mail server, have to add the following mail relay setting

STEP 1． Add the first setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to (Figure16-4)

Figure16-4 The First Mail Relay Setting WebUI

STEP 2． Add the second setting in **Mail Relay** function of **Configure**:

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting (Figure16-5)

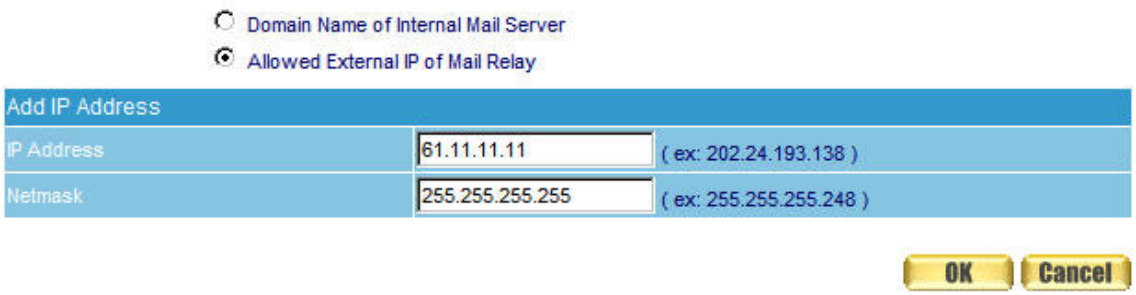


Figure16-5 The Second Mail Relay Setting WebUI

The Headquarters setup RS-3000 as Gateway (Mail Server is in DMZ, Transparent Mode) to make the Branch Company's employees can send mails via Headquarters' Mail Server

Preparation

WAN Port IP of RS-3000: 61.11.11.11

Mail Server IP: 61.11.11.12

WAN Port IP of the Branch Company's Firewall: 211.22.22.22

Map the DNS Domain Name (broadband.com.tw) to DNS Server IP (setup MX record is Mail Server IP) When the branch company's users send mail to the external mail server's recipient account by mail server's sender account of broadband.com.tw, add the following Mail Relay setting:

STEP 1 . Add the first setting in **Mail Relay** function of **Configure**:

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to (Figure16-6)

Figure16-6 The First Mail Relay Setting WebUI

STEP 2 . Add the second setting in **Mail Relay** function of **Configure**:

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting (Figure16-7)

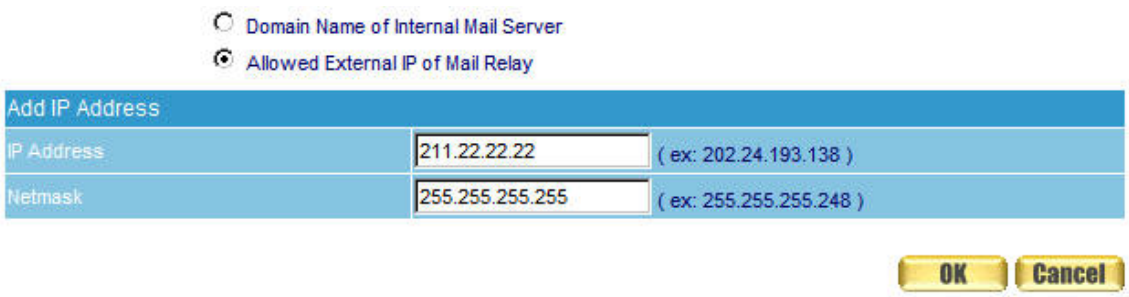


Figure16-7 The Second Mail Relay Setting WebUI

Chapter 17 Anti-Spam

RS-3000 can filter the e-mails that are going to send to the mail server of enterprise. In order to make sure the e-mail account that communicates with outside won't receive a mass advertisement or Spam mail, meanwhile, it can reduce the burden of mail server. Also can prevent the users to pick up the message he/she needs from a mass of useless mails; or delete the needed mail mistakenly while deleting mails. It will raise the work efficiency of the employees and will not lose the important information of enterprise.

In this chapter, we will have the detailed illustration about **Anti-Spam:**

17.1 Setting

Define the required fields of Setting:

Spam Setting:

- It can choose the inspection way of the mails, where the mail server is placed in Internal (LAN or DMZ) or External (WAN)
- It can inspect all of the mails that are sent to the enterprise. Also can add score tag or message to the subject line of Spam mail while it exceeds the standard. After filtering if the mails still don't reach the standard, it will only add score tag to the subject of the spam mail.
- It also can check sender address in blacklist of anti-spam website to determine if it is spam mail or not

Action of Spam Mail:

- The mail that considered as spam mail can be coped with **Delete mail**, **Deliver to the recipient**, **Forward to** another mail account
  - After setup the relevant settings in **Mail Relay** function of **Configure**, add the following settings in this function:
    1. The Mail Server is placed in **Internal (LAN or DMZ)**
    2. **The threshold score**: Enter 5
    3. **Add the message to the subject line**: Enter ---spam---
    4. Select **Add score tag to the subject line**
    5. Select **Deliver to the recipient**
    6. Click **OK** (Figure17-1)

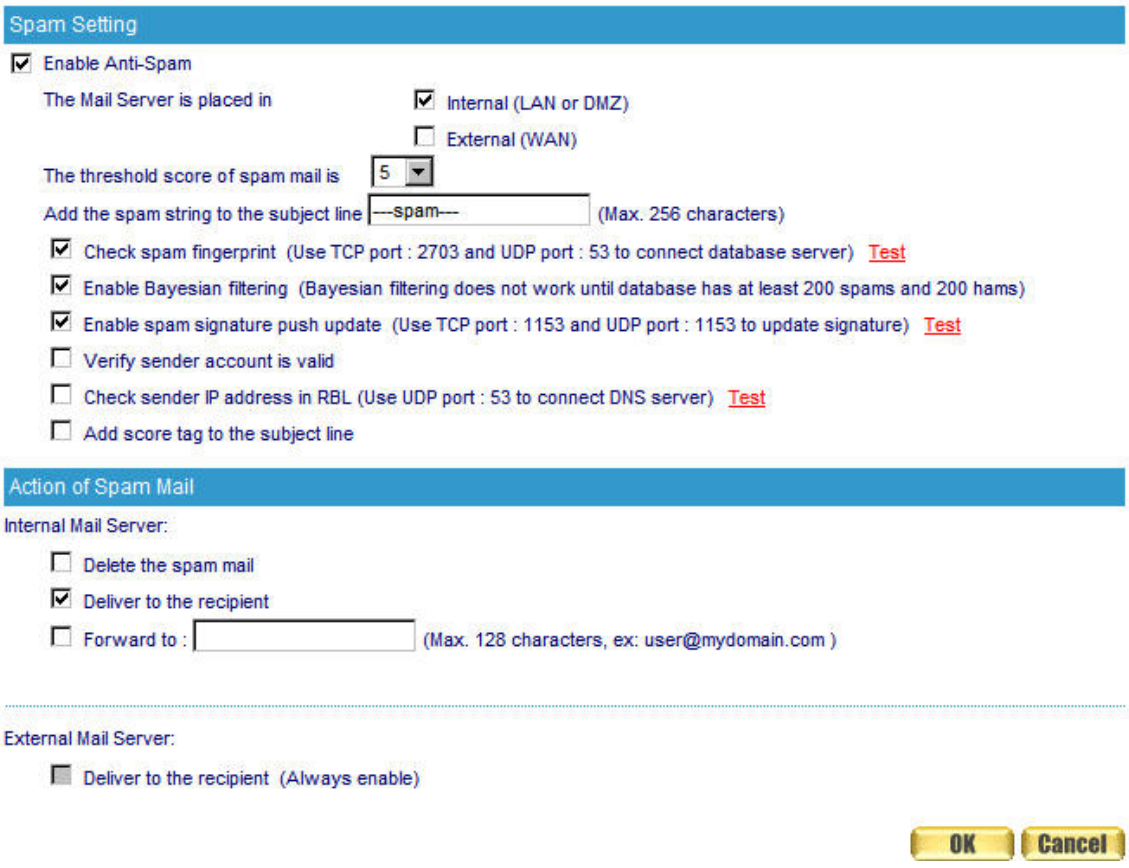


Figure17-1 Anti-Spam Setting WebUI

- When receive Spam mail, it will add **score tag** and **message** in front of the subject of the E-mail. (Figure17-2)

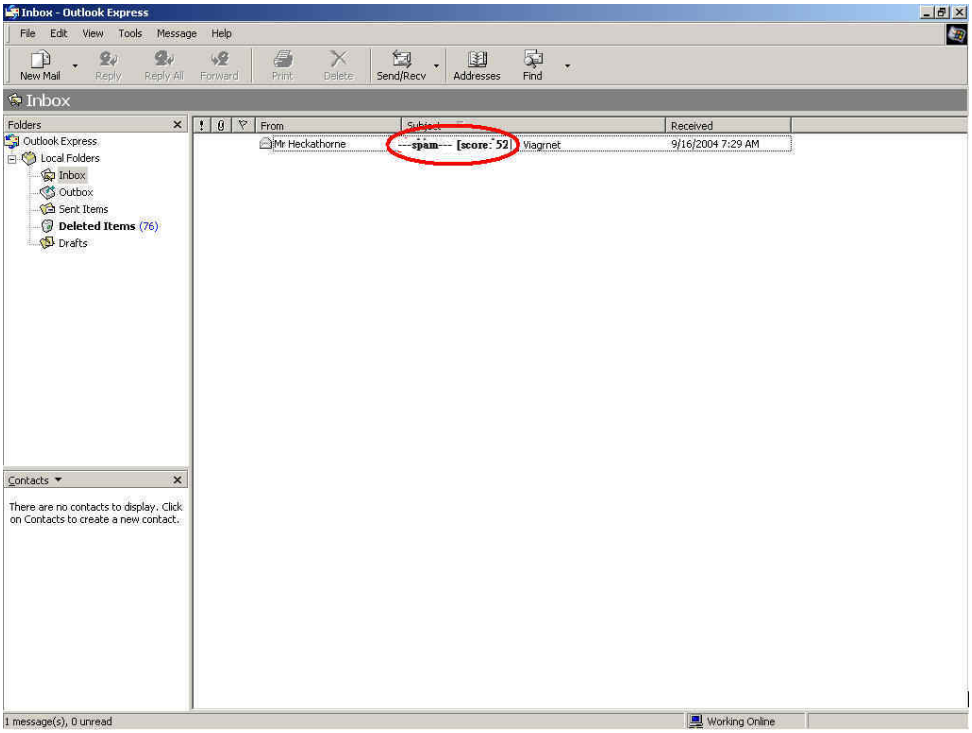


Figure17-2 the subject of the mail that considered as spam mail WebUI

- When receive Ham mail, it will only add **score tag** in front of the e-mail's subject (Figure17-3)

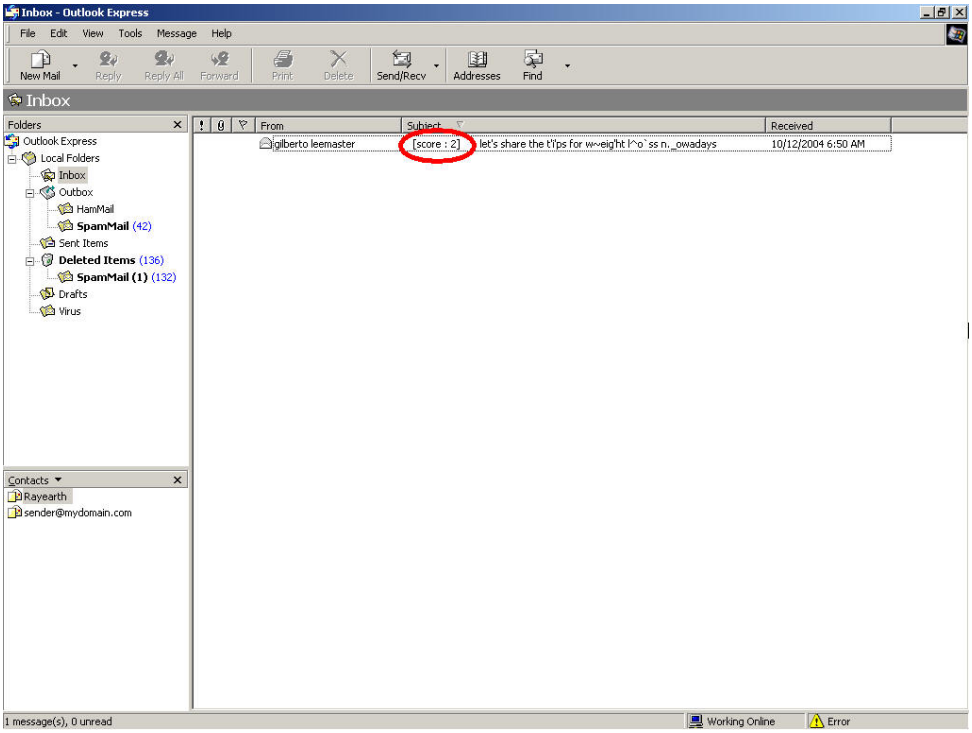


Figure17-3 the subject of the mail that considered as Spam mail WebUI

17.2 Rule

Define the required fields of Rule

Rule Name:

- The name of the custom spam mail determination rule

Comment:

- To explain the meaning of the custom rule

Combination:

- Add: It must be fit in with all of the custom rule mails that would be considered as spam mail or ham mail.
- Or: Only be fit in with one of the custom rule mails that would be considered as spam mail or ham mail.

Classification:

- When setting as **Spam**, it will classify the mails that correspond to the rule as spam mail.
- When setting as **Ham (Non-Spam)**, it will classify the mails that correspond to the rule as ham mail.

Action:

- Only when **Classification** is set as **Spam** that will enable this function. Because only spam mail needs to be handled.
- You can choose to Delete mail, Deliver to the recipient, or Forward to another mail account

Auto-Training:

- When **Classification** is set as **Spam** and enable this function, and then the mails that correspond to this rule will be trained to identify as spam mail according to the setting time in Training function
- When **Classification** is set as **Ham (Non-Spam)** and enable this function, and then the mails correspond to this rule will be trained to identify as ham (non-spam) mail according to the setting time in Training function

Item:

- To judge if it is spam mail or not according to the Header, Body, Size of the mail.
- The Header items to detect the mail are: Received, Envelope-To, Form, To, Cc, Bcc, Subject, Sender, Reply-To, Errors-To, Message-ID, and Date.

Condition:

- When **Item** is set as **Header** and **Body**, the available conditions are: Contains, Does Not Contain, Is Equal To, Is Not Equal To, Starts With, Ends With, Exist and Does Not Exist.
- When **Item** is set as **Size**, the available conditions are: More Than, Is Equal To, Is Not Equal To and Less Than.

Pattern:

- Enter the relevant value in **Item** and **Condition** field. For example: **From** Item and use **Contains** Condition, and enter josh as a characteristics. Afterward when the sender and receiver's mail account has josh inside and then it will be considered as spam mail or ham mail.

17.3 Whitelist

Define the required fields of Whitelist

Whitelist:

- To determine the mail comes from specific mail address that can send to the recipient without being restricted.

Direction:

- **【From】**：To judge the sending address of the mail
- **【To】**：To judge the receiving address of the mail

17.4 Blacklist

Define the required fields of Blacklist

Blacklist:

- To determine the mail comes from specific mail address that cannot be sent to the recipient.

17.5 Training

Define the required fields of Training

Training Database:

- The System Manager can Import or Export Training Database here.

Spam Mail for Training:

- The System Manager can import the file which is not determined as spam mail here. To raise the judgment rate of spam mail after the RS-3000 learning the file.

Ham Mail for Training:

- The System Manager can import the file which is determined as spam mail here. To raise the judgment rate of ham mail after the RS-3000 learning the file

Training time:

- The System Manager can set the training time for RS-3000 to learn the import file each day here.

17.6 Spam Mail

Define the required fields of Spam Mail

Top Total Spam:

- To show the top chart that represent the spam mail that recipient receive and send

 In **Top Total Spam** report, you can choose to display the scanned mails that sent to **Internal Mail Server** or received from **External Mail Server.**

 In **Top Total Spam** report, it can sort the mail according to Recipient, Total Spam and Scanned Mail.

Advance Instruction:

When talking to Mail Server, it is the medium of sending or receiving all the e-mail in Internet. The indicative way of the e-mail is: acoount@server.name. In front of the @ means the account; behinds the @ mean the Master's name.

When you send e-mail to josh@yahoo.com.tw, your sending software will go to DNS Server to find the mail Master name, mapped IP, and MX record first. If there is a mapped MX record and then the e-mail will be delivered to the MX Master first, and then be delivered to the destination (yahoo.com.tw) by MX Master (means the Master of yahoo.co.tw). If it maps to several MX records, and then the e-mail will be deliver to the first priority Master. And if there is no MX record, the e-mail will deliver to your mail master only after searching for mapped IP. And then your mail master can deliver it to the mail master of yahoo.com.tw. The master of yahoo.com.tw will deliver the mail to every recipient according to the account in front of the @.

The flow of delivering e-mail:

The three key element of sending e-mail are: MUA, MTA, MDA

- **MUA (Mail User Agent):** The PC of client cannot send mail directly. It must deliver mail by MUA. No matter to send or to receive the mail, the Client user still has to use mail system by MUA that provided by operation system. For example: Outlook Express in Windows is MUA. The main function of MUA is to receive or send e-mail from mail master and provide the function for users to browse and edit mail
- **MTA (Mail Transfer Agent):** When the user sending or receiving mails, they are both completed by MTA. Basically, its functions are as below:

1. To receive the mail that sent by external master: when receiving the mails from external; only if the recipient exists in MTA internal account then this mail will be received by MTA.
2. To send mail for user: Only if the user has the authority to use MTA, and then the mail can be sent by MTA.
3. To let user to receive his/her own mail: The user can take the mails to his/her own PC from mail master.

 Generally the Mail Server we refer to is talking about MTA.

- **MDA (Mail Delivery Agent):** To let the mail that received by MTA be put in the Mailbox according to its destination. Or by MTA to send the mail to the next MTA.

To introduce the delivery procedure of the mail by two Send and Receive way:

If the user wants to send the mail, the steps can be divided as follows:

- Use MUA to send mail to MTA: Enter the following setting while the user write e-mail by MUA:

    1. The e-mail address and the mail server of the sender (To receive the MTA that sent by MTA from the sender)
    2. The e-mail address and the mail server of the recipient (To receive the MTA that sent from the external master)

After the user writing e-mail by MUA, and use the sending function of MUA, it will deliver the mail to the MTA you appoint to.

- When MTA receive the mail from itself, it will hand over to MDA to deliver the mail to the mailbox of the user's account: In the received mail, if the destination is Mail Server it means MTA itself. Meanwhile, MTA will transfer the mail to MDA and put the mail in the recipient's mailbox.
- MTA will transfer the mail again; if the recipient of the mail is not the internal account, then the mail will be transferred again. This function is called Relay
- Remote MTA receive the mail that sent by local MTA: Remote MTA will receive the mail that sent by local MTA and transfer the mail to its MDA. Meanwhile, the mail will be saved in remote MTA and applied for the user to download.

And the action of user to receive mail is as follows:

The PC that used by remote user will connect to his/her MTA directly, to ask MTA to check if its mailbox has mails or not. After MTA check by MDA, it will transfer the mail to the user's MUA. Meanwhile, according to MUA setting, MTA will choose to delete the Mailbox or to preserve it. (For the next time when user receive the mail again, the preserved mail will be downloaded again)

The protocol of send/receive e-mail is as follows:

1. Sending e-mail: It is a function of the process of sending the mail from MUA to MTA, and transfer mail from MTA to the next MTA. At present, most of the mail server uses SMTP Protocol (Simple Mail Transfer Protocol), and the Port Number is 25.

2. Receiving e-mail: MUA connect to MTA user's Mailbox by POP (Post Office Protocol) in order to read or download the mail in user's mailbox. At present, common POP Protocol is POP3 (Post Office Protocol version 3), and the Port Number is 110.

 Generally, a MTA that provides sending/receiving mail function needs two protocols at least. They are SMTP and POP3. And as long as your MUA and MTA support SMPT and POP3, then they can connect with each other.

 After MTA analyzing the received mail and if the recipient is not in the master account, then MTA will transfer the mail to the next MTA. This function is called Relay.

 If anyone can deliver the mail by one of the mail server, we called this **Open Relay** mail server. To avoid this question, most of the mail server's default value will not open up Relay function. It only will open up Relay function according to **Localhost.** Therefore, MTA can receive the mail that indicative of the recipient is the internal account of MTA mail server. So there is no problem in receiving the mail. However it causes some problems because MTA only setup some standard IP and Subnet to open their Relay function. So in the range of this setting, the Client can send/receive mail very free. As for the mail from the IP source without standard will be blocked completely. In this case, there comes **Simple Mail Transfer Protocol** to solve the problem.

 Simple Mail Transfer Protocol is when MUA send mail to MTA; the master will ask to detect the account and password of MUA sender. And then MTA can provide the Relay function after authentication without setup Relay function according to some trusting domain or IP. By Authentication, MTA will analyze the relevant authentication information of the sender. After passing the authentication that will accept mail and send the mail, otherwise; MTA will not receive the mail.

To detect if the mail from External Mail Server is spam mail or not

STEP 1． In **LAN Address** to permit a PC receiving the mail from external mail server. Its network card is set as 192.168.139.12, and the DNS setting is DNS server.

STEP 2． In **LAN** of **Address** function, add the following settings: (Figure17-4)

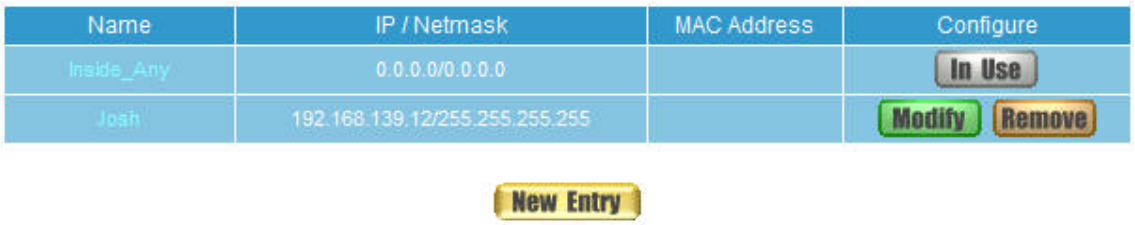


Figure17-4 Mapped IP of Internal User's PC in Address Book

STEP 3． Add the following setting in **Group** of **Service**. (Figure17-5)

Figure14-5 Service Group that includes POP3, SMTP, or DNS

STEP 4． Add the following setting in **Outgoing Policy**: (Figure17-6)

Figure17-6 Outgoing Policy Setting

STEP 5.Add the following setting in **Setting** of **Anti-Spam** function: (Figure17-7)

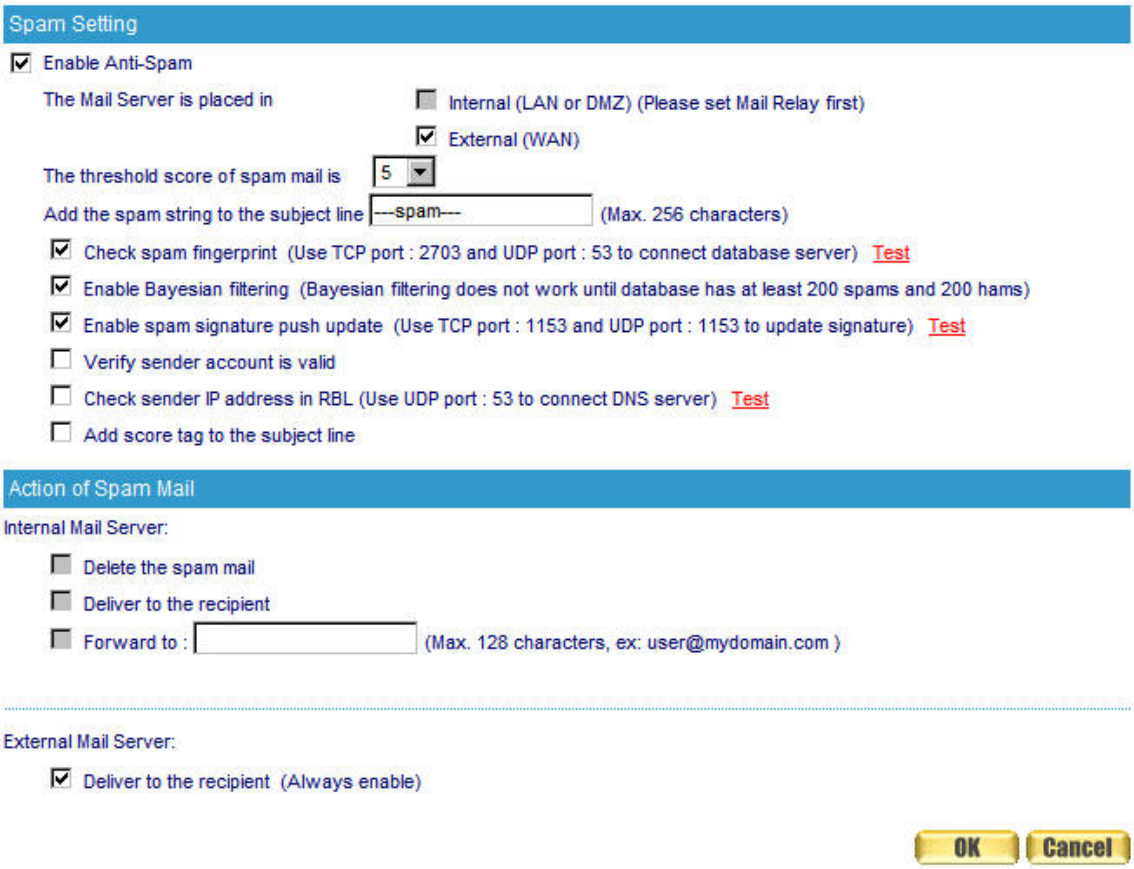


Figure17-7 Action of Spam Mail and Spam Setting

Anti-Spam function is enabled in default status. So the System Manager does not need to set up the additional setting and then the RS-3000 will filter the spam mail according to the mails that sent to the internal mail server or received from external mail server. (Figure17-8)

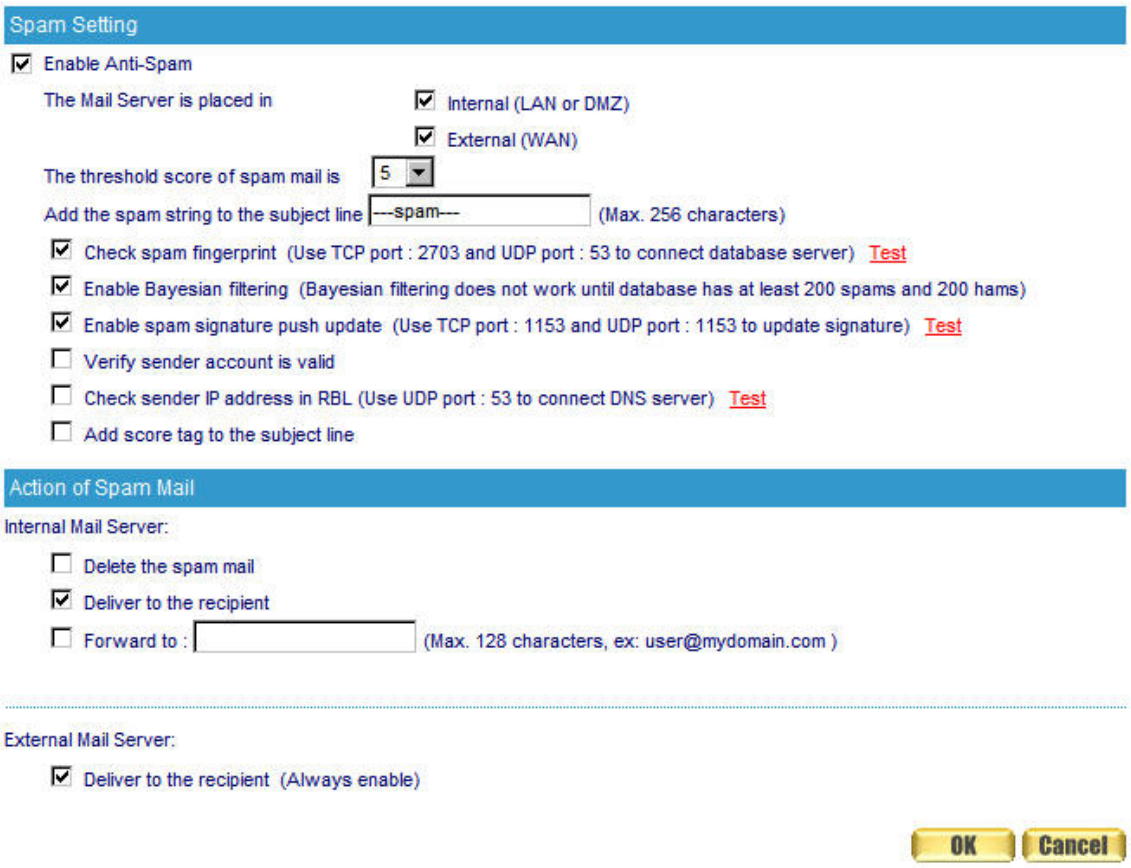


Figure17-8 Default Value of Spam Setting

When only filter the mail that internal users received from external server:

1. In **Action of Spam Mail**, no matter choose **Delete mail, Deliver to the recipient,** or **Forward to,** it will add the message on the subject line of spam mail and send it to the recipient.
2. Also can use **Rule, Whitelist, Blacklist** or **Training** function to filter the spam mail.

STEP 6 . When the internal users are receiving the mail from external mail account (js1720@ms21.pchome.com.tw), the RS-3000 will filter the mail at the same time and the chart will be in the **Spam Mail** in **Anti-Spam** function. (At this time, choose **External** to see the mail account chart) (Figure17-9)

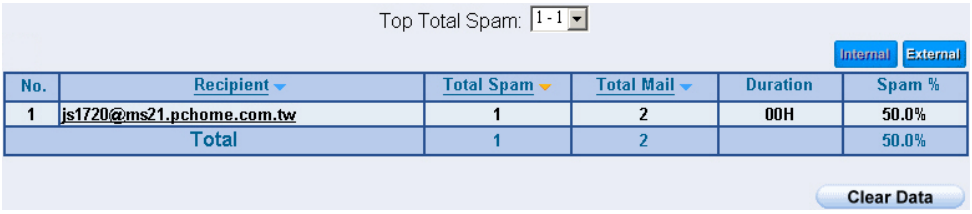


Figure17-9 Report Function Chart

To setup the relevant settings in **Mail Relay** function of **Configure**, so that can choose to display the scanned mails that sent to Internal Mail Server.

Take RS-3000 as Gateway and use Whitelist and Blacklist to filter the mail. (Mail Server is in DMZ and use Transparent Mode)

STEP 1． Set up a mail server in **DMZ** and set its network card IP as 61.11.11.12. The DNS setting is external DNS server, and the Master name is broadband.com.tw

STEP 2． Enter the following setting in **DMZ** of **Address** function: (Figure17-10)

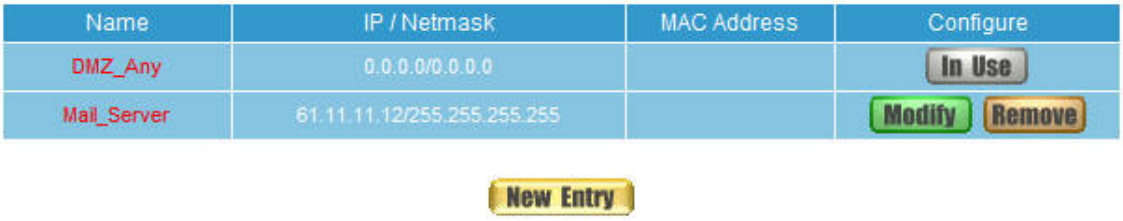


Figure17-10 Mapped Name Setting in Address of Mail Server

STEP 3.Enter the following setting in **Group** in **Service** function: (Figure17-11)

Figure17-11 Setting Service Group that include POP3, SMTP or DNS

STEP 4.Enter the following setting in **WAN to DMZ Policy**: (Figure17-12)

Figure17-12 WAN to DMZ Policy Setting

STEP 5.Enter the following setting in **DMZ to WAN Policy**: (Figure17-13)

Figure17-13 DMZ to WAN Policy Setting

STEP 6 . Enter the following setting in **Mail Relay** function of **Setting**: (Figure17-14)

Figure17-14 Mail Relay Setting of External Mail to Internal Mail Server

Mail Relay function makes the mails that sent to DMZ's mail server could be relayed to its mapped mail server by RS-3000

STEP 7 . Enter the following setting in **Setting** function of **Anti-Spam**: (Figure17-15)

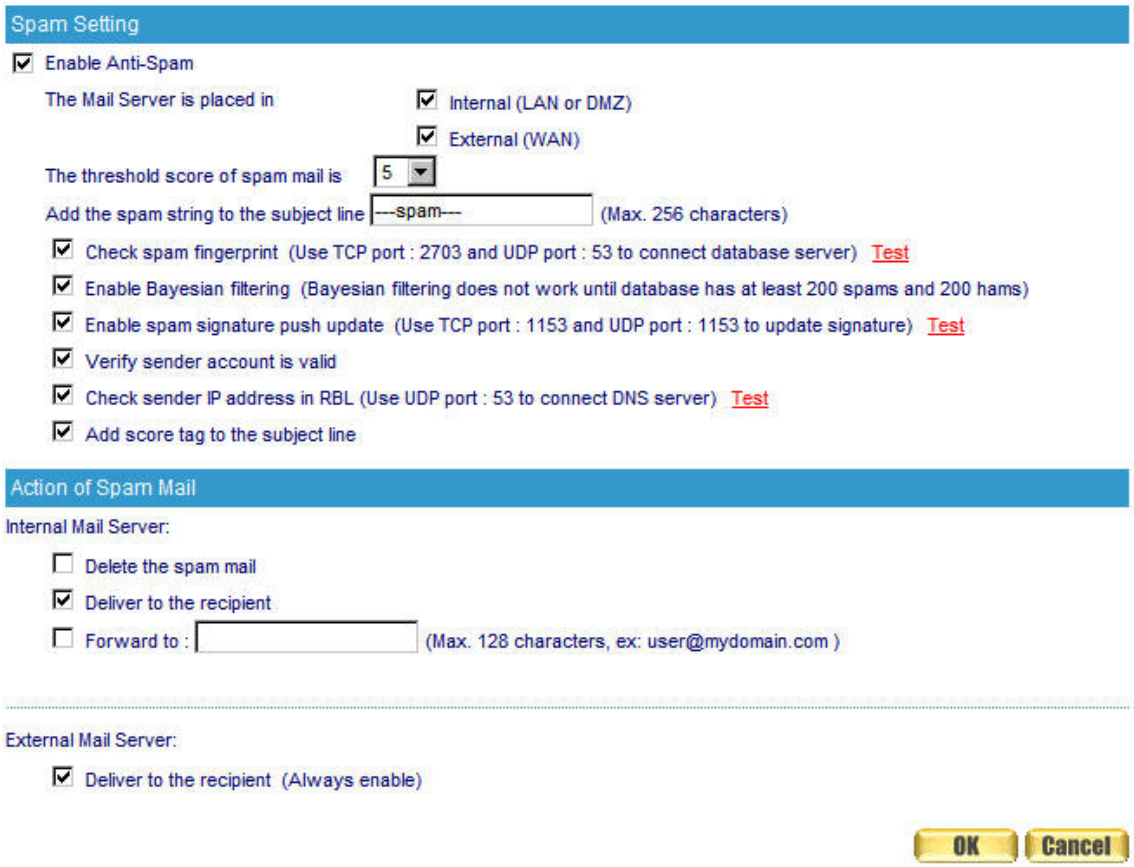


Figure17-15 Spam Setting and Action of Spam Mail

When select **Delete mail** in **Action of Spam Mail**, and then the other functions (**Deliver to the recipient**, or **Forward to**) cannot be selected. So when RS-3000 had scanned spam mail, it will delete it directly. But still can check the relevant chart in **Spam Mail** function.

Action of Spam Mail here is according to the filter standard of **Blacklist** to take action about spam mail.

STEP 8 . Enter the following setting in **Whitelist** of **Anti-Spam** function:

- Click **New Entry**
- **Whitelist:** Enter share2k01@yahoo.com.tw
- **Direction:** Select From
- Enable **Auto-Training**
- Click **OK** (Figure17-16)
- Enter **New Entry** again
- **Whitelist:** Enter josh@broadband.com.tw
- **Direction:** Select To
- Enable **Auto-Training**
- Click **OK** (Figure17-17)
- Complete setting (Figure17-18)

Figure17-16 Add Whitelist Setting 1

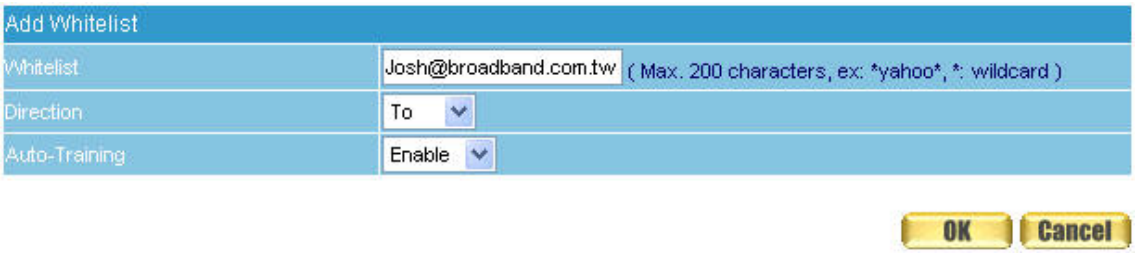


Figure17-17 Add Whitelist Setting 2

Figure17-18 Complete Whitelist Setting

When enable **Auto-Training** function, the mail that correspond to **Whitelist** setting will be trained as Ham Mail automatically according to the time setting in **Training** function.

STEP 9.Enter the following setting in **Blacklist** of **Anti-Spam** function:

- Enter **New Entry**
- **Blacklist:** Enter *yahoo*
- **Direction:** Select From
- Enable **Auto-Training**
- Click **OK** (Figure17-19)
- Complete the Setting (Figure17-20)

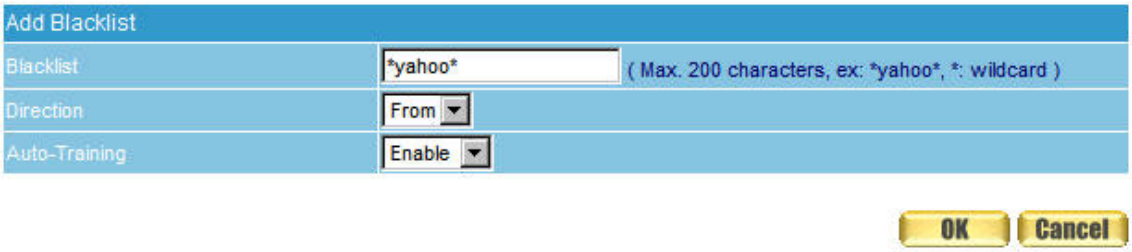


Figure17-19 Add Blacklist Setting

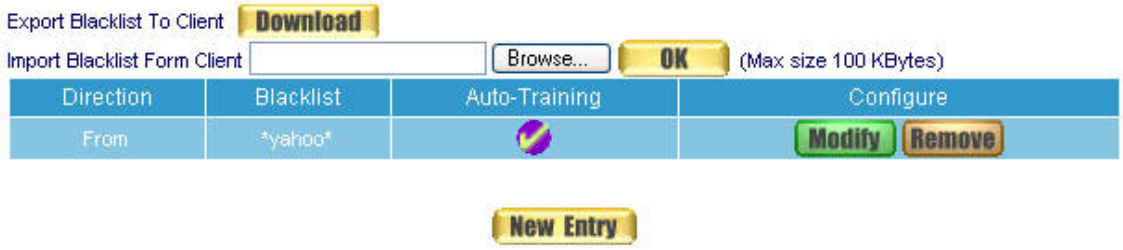


Figure17-20 Complete Blacklist Setting

When enable **Auto-Training** function, the mail that correspond to **Blacklist** setting will be trained as Spam Mail automatically according to the time setting in **Training** function.

The address of **Whitelist** and **Blacklist** can be set as complete mail address (For example: josh@broadband.com.tw) or the word string that make up of【*】(For example: *yahoo* means the e-mail account that includes “yahoo” inside)

The privilege of **Whitelist** is greater than **Blacklist**. So when RS-3000 is filtering the spam mail, it will adopt the standard of **Whitelist** first and then adopt **Blacklist** next.

STEP 10.When the external yahoo mail account send mail to the recipient account of mail server of broadband.com.tw in RS-3000; josh@broadband.com.tw and steve@broadband.com.tw

- If the sender account is share2k01@yahoo.com.tw, then these two recipient accounts both will receive the mail that sent by this sender account.
- If it comes from other yahoo sender account (share2k003@yahoo.com.tw), and then there will only be josh@broadband.com.tw can receive the mail that sent from this sender account; the mail that sent to steve@broadband.com.tw will be considered as spam mail.
- After RS-3000 had filtered the mail above, it will bring the chart as follows in the **Spam Mail** function of **Anti-Spam**. (Figure17-21)

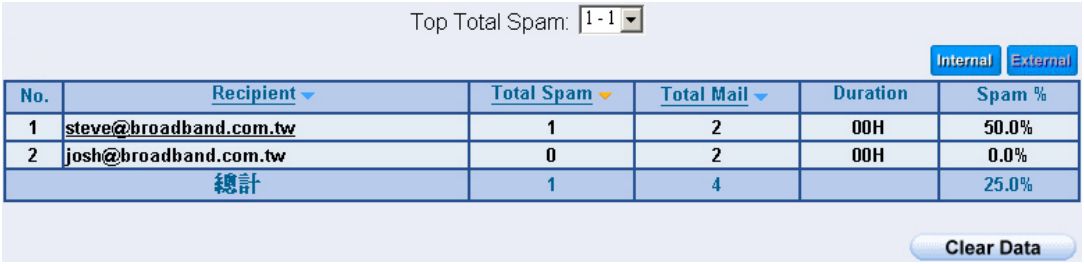


Figure17-21 Chart of Report Function

When clicking on **Remove** button in **Total Spam Mail,** the record of the chart will be deleted and the record cannot be checked in **Spam Mail** function.

Place RS-3000 between the original Gateway and Mail Server to set up the Rule to filter the mail. (Mail Server is in DMZ, Transparent Mode)

The LAN Subnet of enterprise's original Gateway: 172.16.1.0/16

The WAN IP of RS-3000: 172.16.1.12

STEP 1 . Setup a Mail Server in **DMZ** and its network card IP is 172.16.1.13. The DNS setting is external DNS Server. Its host name is broadband.com.tw

STEP 2 . Enter the following setting in **DMZ Address**: (Figure17-22)

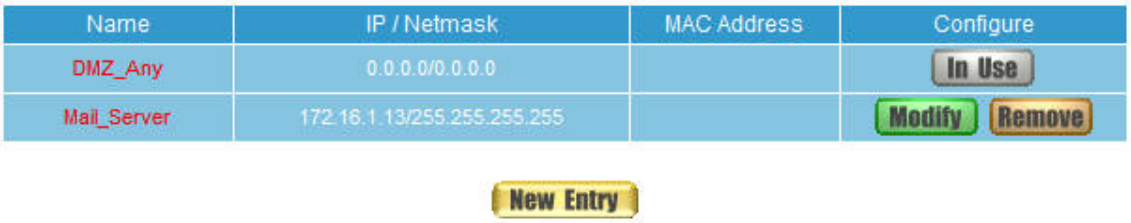


Figure17-22 Mapped IP Setting of Mail Server in Address Book

STEP 3 . Enter the following setting in **Service Group**. (Figure17-23)

Figure17-23 Setting Service Group includes POP3, SMTP or DNS

STEP 4 **.** Enter the following setting in **WAN to DMZ Policy:** (Figure17-24)

Figure17-24 WAN to DMZ Policy Setting

STEP 5.Enter the following setting in **DMZ to WAN Policy:** (Figure17-25)

Figure17-25 DMZ to WAN Policy Setting

STEP 6 **.** Add the following setting in **Mail Relay** in **Configure**: (Figure17-26)

Figure17-26 Mail Relay Setting of External Mail to Internal Mail Server

STEP 7 . Enter the following setting in **Rule** of **Anti-Spam** function:

- Enter **New Entry**
- **Rule Name:** Enter HamMail
- **Comments:** Enter Ham Mail
- **Combination:** Select Or
- **Classification:** Select Ham (Non-Spam)
- Enable **Auto-Training**
- In the first field **Item**: Select From; **Condition**: Select Contains; **Pattern**: share2k01
- Click **Next Row**
- In the second **Item** field: Select To; **Condition**: Select Contains; **Pattern:** josh (Figure17-27)
- Press **OK** (Figure17-28)

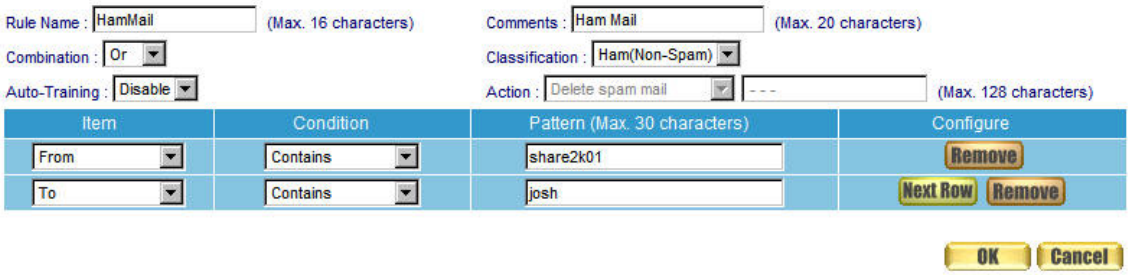


Figure17-27 The First Rule Item Setting

Figure17-28 Complete First Rule Setting

In **Rule** Setting, when **Classification** select as Ham (Non-Spam), the **Action** function is disabled. Because the mail that considered as Ham mail will send to the recipient directly.

STEP 8 . Enter the following setting in **Rule** of **Anti-Spam** function:

- Enter **New Entry**
- **Rule Name:** Enter SpamMail
- **Comments:** Enter Spam Mail
- **Combination:** Select And
- **Classification:** Select Spam
- **Action:** Select Deliver to the recipient
- Enable **Auto-Training**
- **Item**: Select From; **Condition**: Select Contains; **Pattern**: yahoo (Figure17-29)
- Press **OK** (Figure17-30)

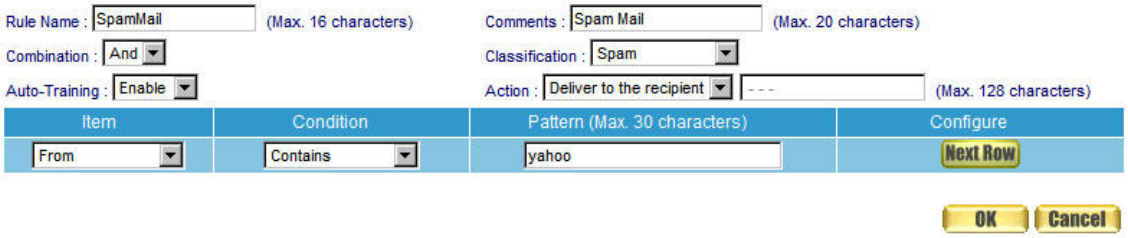


Figure17-29 The Second Rule Setting

Figure17-30 Complete the Second Rule Setting

In **Rule** Setting, when the **Classification** select as **Spam**, then the **Action** only can select **Delete the spam mail, Forward to,** or **Deliver to the recipient.**

The privilege of **Rule** is greater than **Whitelist** and **Blacklist**. And in **Rule** function, the former rule has the greater privilege. So when the RS-3000 is filtering the spam mail, it will take **Rule** as filter standard first and then is **Whitelist**; **Blacklist** is the last one be taken.

Select one of the mails in **Outlook Express**. Press the right key of the mouse and select **Content**, and select **Details** in the pop-up page. It will show all of the headers for the message to be taken as the reference value of **Condition** and **Item** of the **Rule**.

STEP 9.When the external yahoo mail account send mail to the recipient account of mail server of broadband.com.tw in RS-3000; josh@broadband.com.tw and steve@broadband.com.tw

- If the sender account is share2k01@yahoo.com.tw, then these two recipient accounts both will receive the mail that sent by this sender account.
- If it comes from other yahoo sender account (share2k003@yahoo.com.tw), and then there will only be josh@broadband.com.tw can receive the mail that sent from this sender account; the mail that sent to steve@broadband.com.tw will be considered as spam mail.
- After RS-3000 had filtered the mail above, it will bring the chart as follows in the **Spam Mail** function of **Anti-Spam**. (Figure17-31)

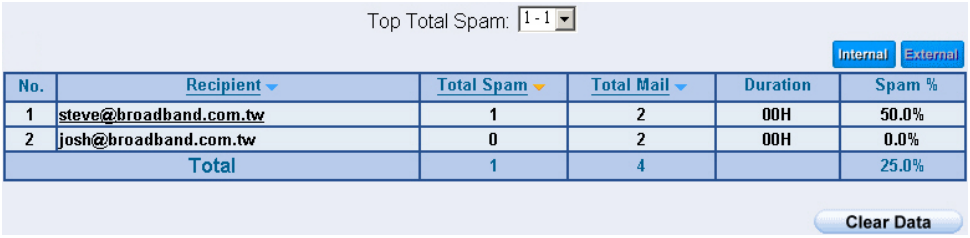


Figure17-31 Chart of Report Function

Use Training function of the RS-3000 to make the mail be determined as Spam mail or Ham mail after Training. (Take Outlook Express for example)

To make the spam mail that had not detected as spam mail be considered as spam mail after training.

STEP 1.Create a new folder SpamMail in **Outlook Express**:

- Press the right key of the mouse and select **New Folder**. (Figure17-32)
- In **Create Folder** WebUI and enter the Folder's Name as SpamMail, and then click on OK. (Figure17-33)

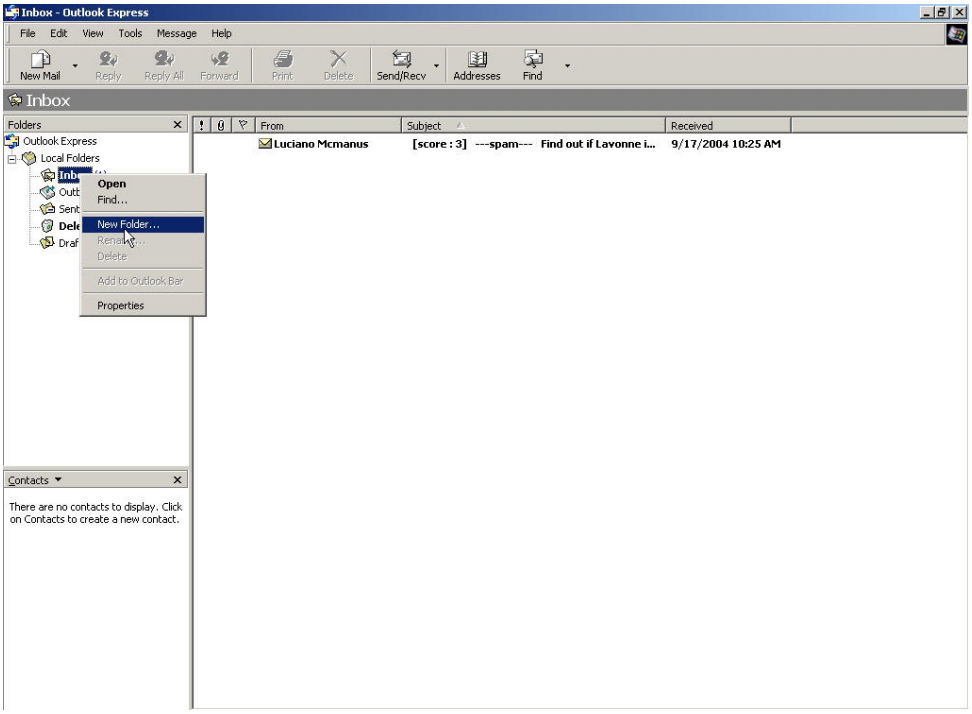


Figure17-32 Select New Folder Function WebUI

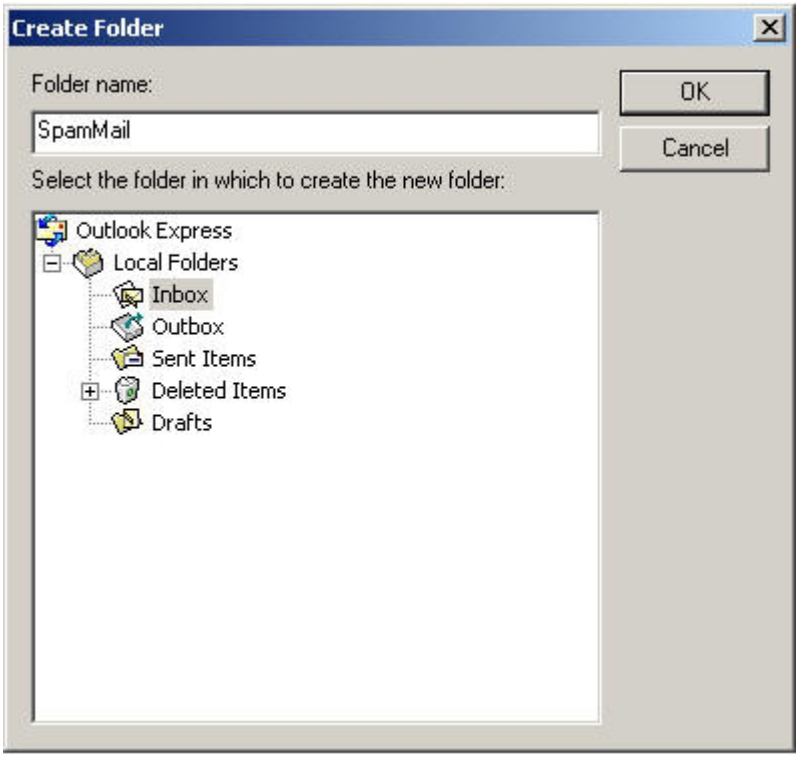


Figure17-33 Create Folder WebUI

STEP 2.In **Inbox-Outlook Express**, move spam mail to **SpamMail** Folder:

- In Inbox, select all of the spam mails that do not judge correctly and press the right key of the mouse and move to the folder. (Figure17-34)
- In **Move** WebUI, select **SpamMail** Folder and click **OK** (Figure17-35)

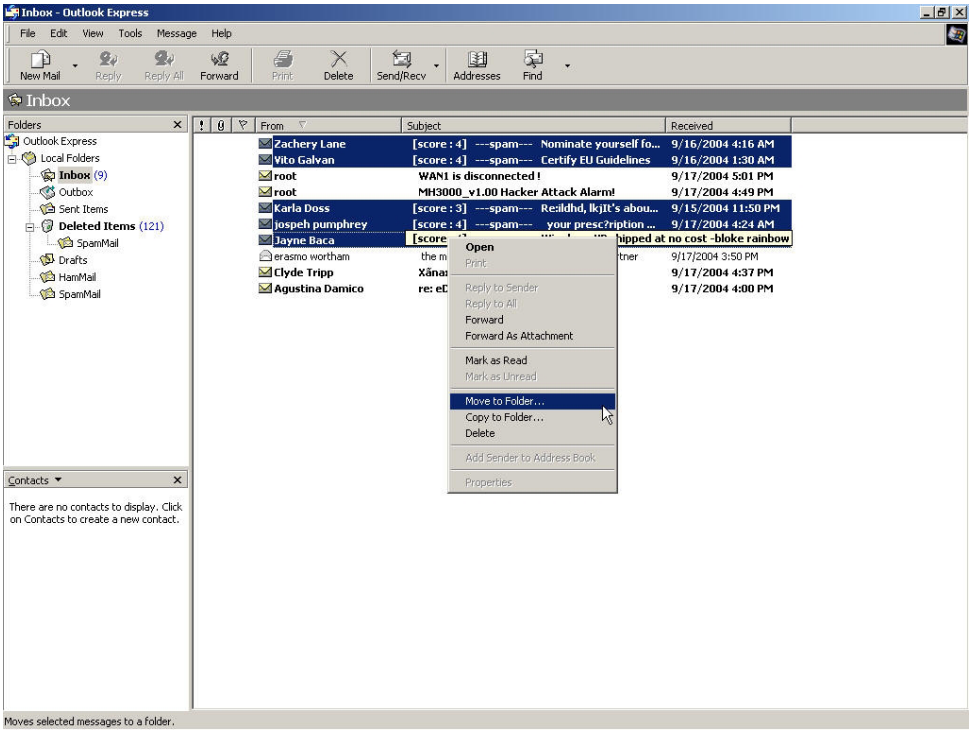


Figure17-34 Move Spam Mail WebUI

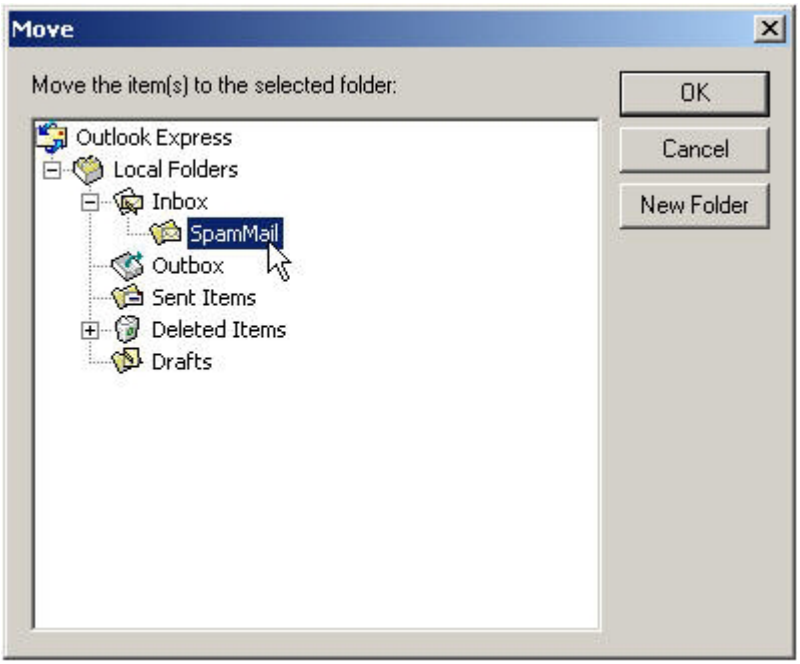


Figure17-35 Select Folder for Spam Mail to move to

STEP 3 . Compress the SpamMail Folder in **Outlook Express** to shorten the data and upload to RS-3000 for training:

- Select **SpamMail** Folder (Figure17-36)
- Select **Compact** function in selection of the folder (Figure17-37)

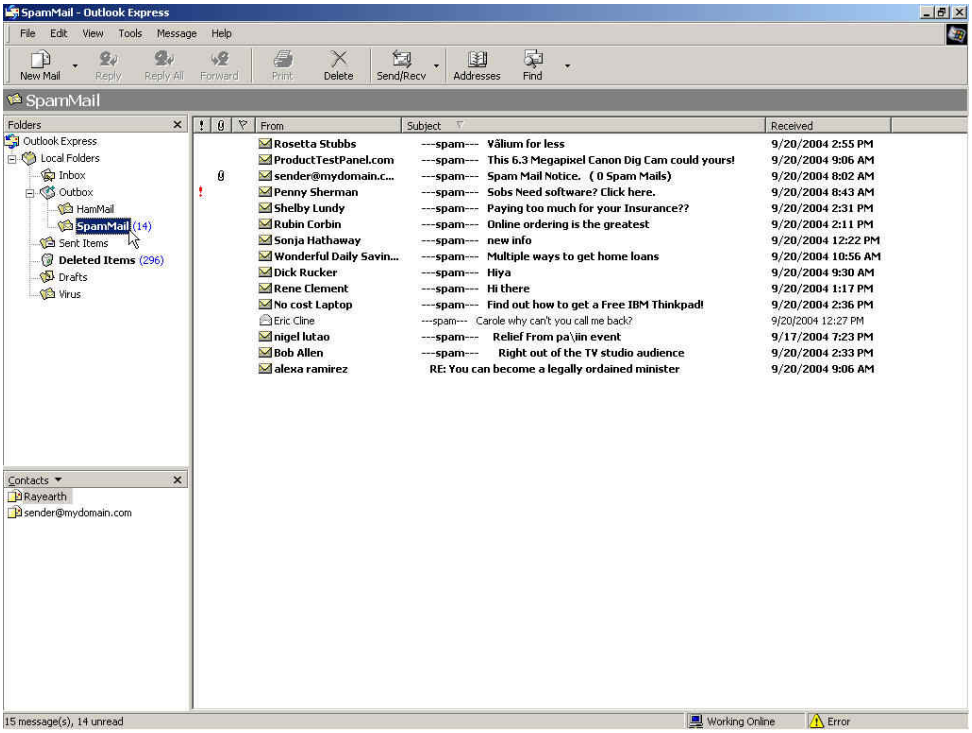


Figure17-36 Select SpamMail Folder

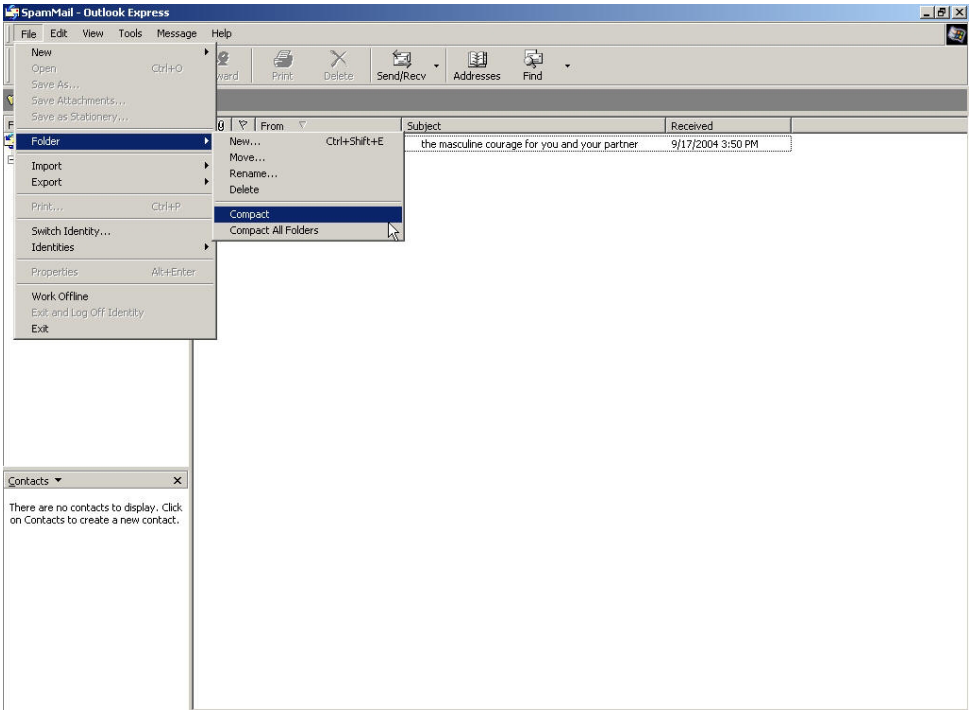


Figure17-37 Compact SpamMail Folder

STEP 4 . To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to RS-3000:

- Press the right key of the mouse in SpamMail file and select **Properties** function. (Figure17-38)
- Copy the file address in **SpamMail Properties** WebUI. (Figure17-39)

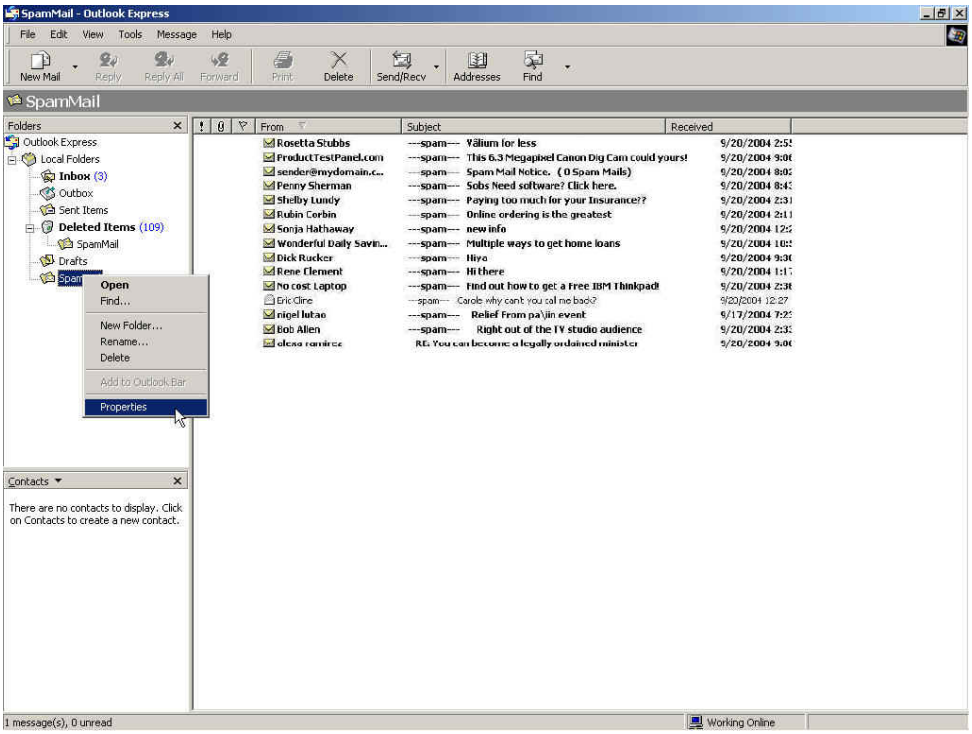


Figure17-38 Select SpamMail File Properties Function

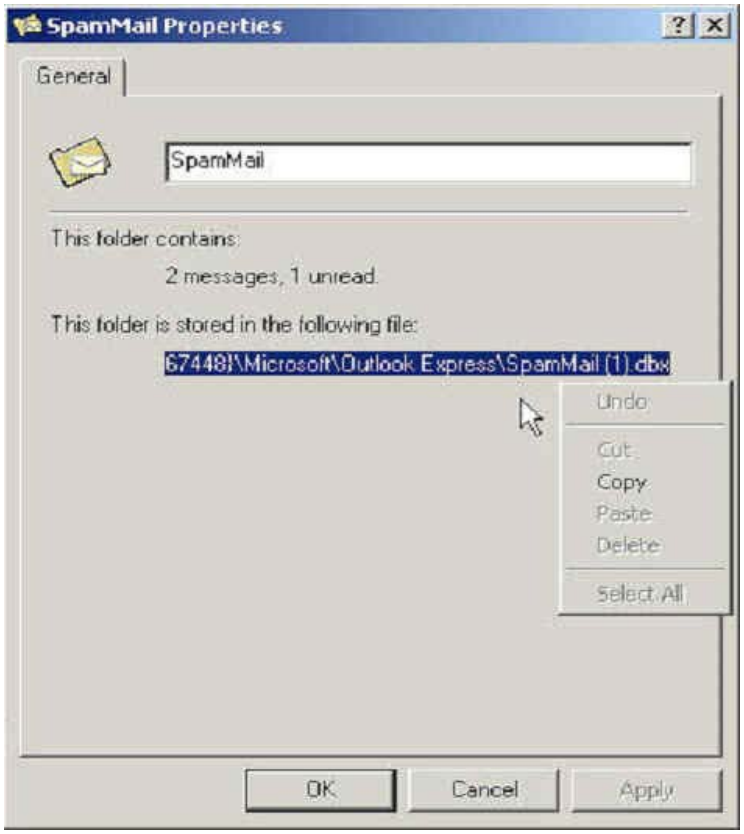


Figure17-39 Copy the File Address that SpamMail File Store

STEP 5 . Paste the route of copied from SpamMail file to the **Spam Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to deliver this file to RS-3000 instantly and to learn the uploaded mail file as spam mail in the appointed time. (Figure17-40)

Figure17-40 Paste the File Address that SpamMail File Save to make RS-3000 to be Trained

The training file that uploads to RS-3000 can be any data file and not restricted in its sub-name, but the file must be ACS11 form.

When the training file of RS-3000 is Microsoft Office Outlook exporting file [.pst], it has to close Microsoft Office Outlook first to start Importing

STEP 6 . Remove all of the mails in **SpamMail** File in **Outlook Express** so that new mails can be compressed and upload to RS-3000 to training directly next time.

- Select all of the mails in **SpamMail** File and press the right key of the mouse to select **Delete** function. (Figure17-41)
- Make sure that all of the mails in SpamMail file had been deleted completely. (Figure17-42)

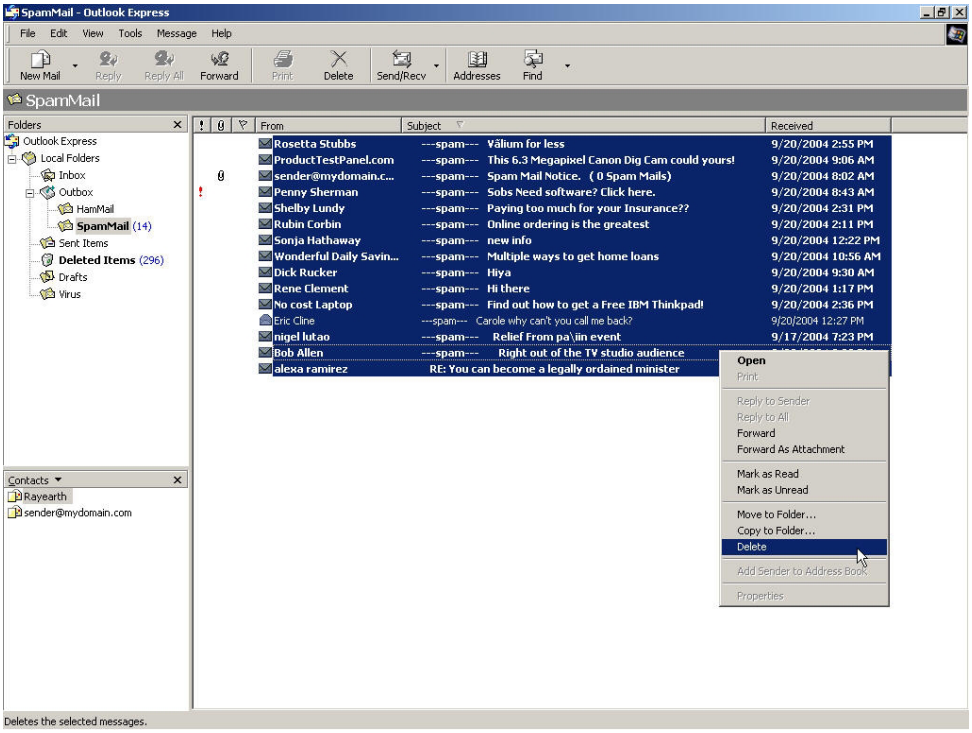


Figure17-41 Delete all of the mails in SpamMail File

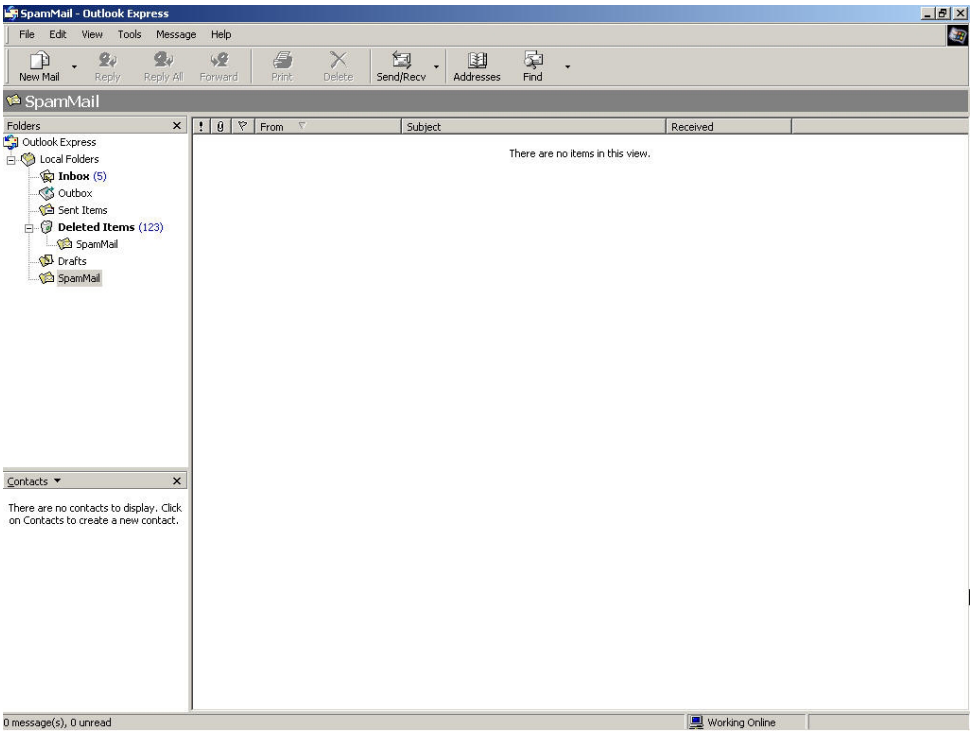


Figure17-42 Confirm that All of the Mail in SpamMail File had been Deleted

To make the mail that is judged as spam mail can be received by recipient after training.

STEP 1 **.** Add a new **HamMail** folder in **Outlook Express**:

- Press the right key of the mouse in **Local Folders** and select **New Folder**. (Figure17-43)
- Enter HamMail in **Folder Name** in **Create Folder** WebUI and click **OK**. (Figure17-44)

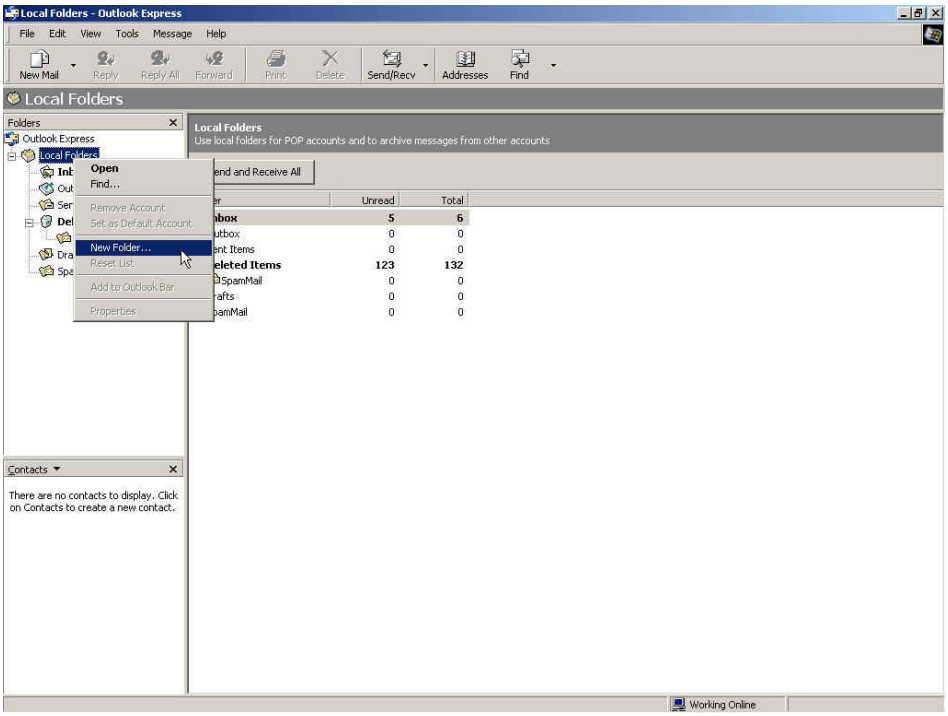


Figure17-43 Select Create New Folder Function WebUI

Figure17-44 Create Folder Function WebUI

STEP 2 . In **Inbox-Outlook Express**, move spam mail to HamMail Folder:

- In Inbox, select the spam mail that all of the recipients need and press the right key of the mouse on the mail and choose **Move to Folder** function. (Figure17-45)
- Select HamMail folder in **Move** WebUI and click **OK.** (Figure17-46)

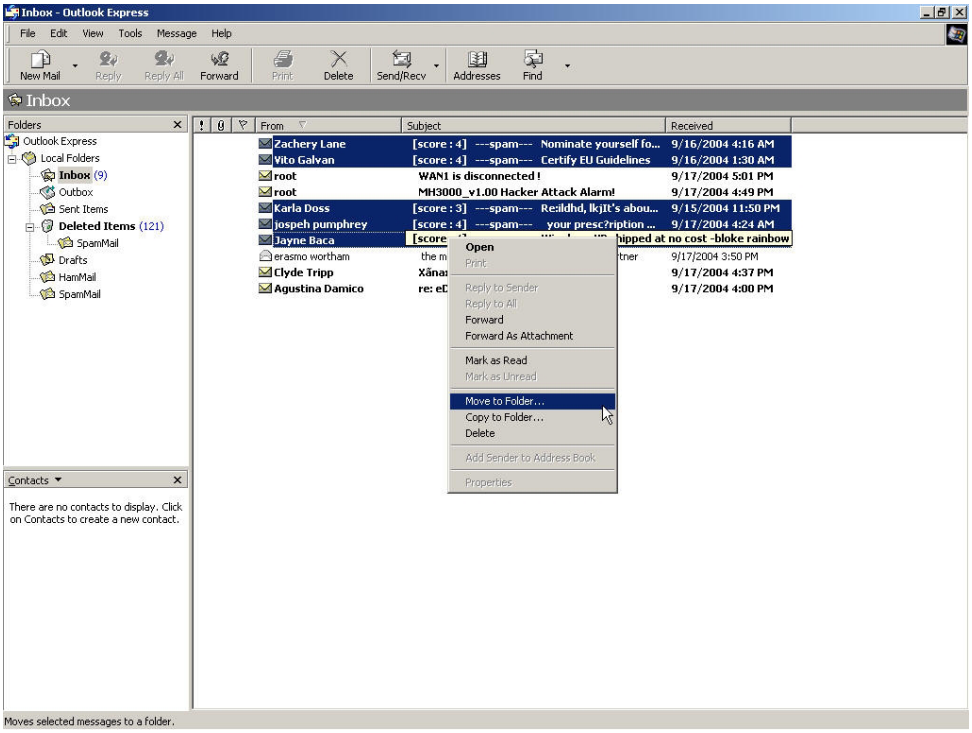


Figure17-45 Move the Needed Spam Mail WebUI

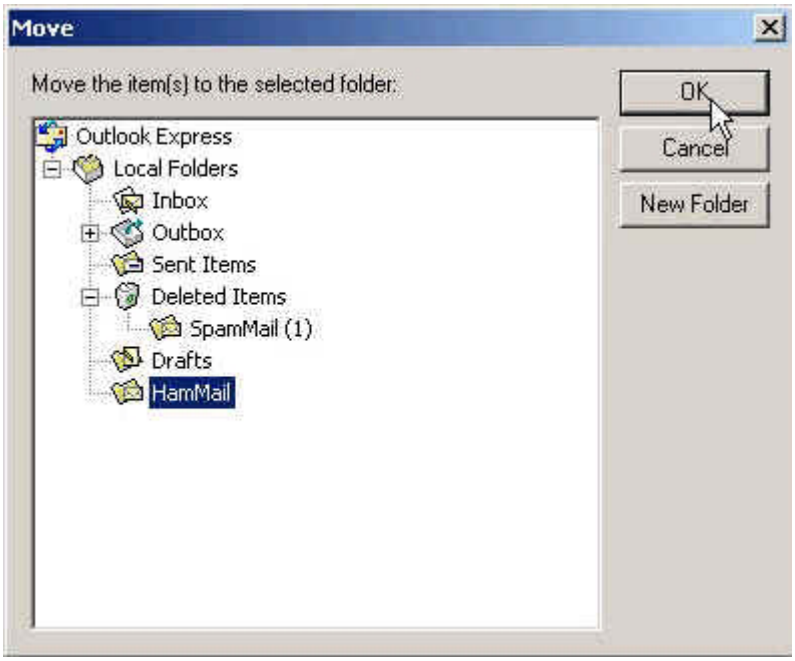


Figure17-46 Select the Folder for Needed Spam Mail to Move to

STEP 3 . Compact the HamMail folder in **Outlook Express** to shorten the data and upload to RS-3000 for training:

- Select HamMail File (Figure17-47)
- Select **Compact** function in selection of File (Figure17-48)

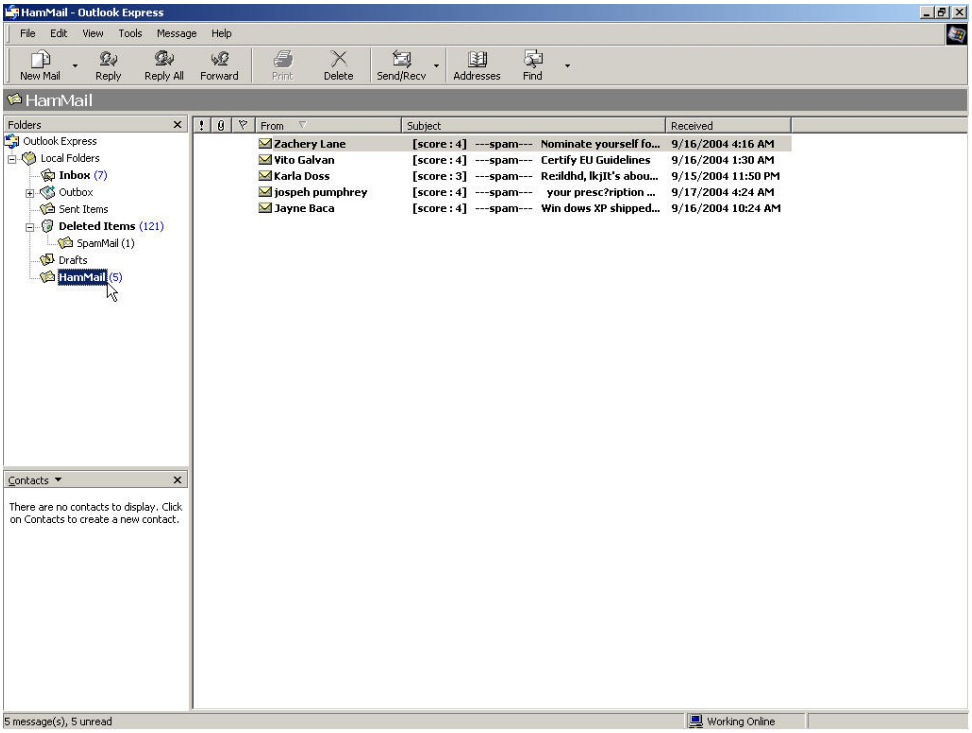


Figure17-47 Select HamMail File

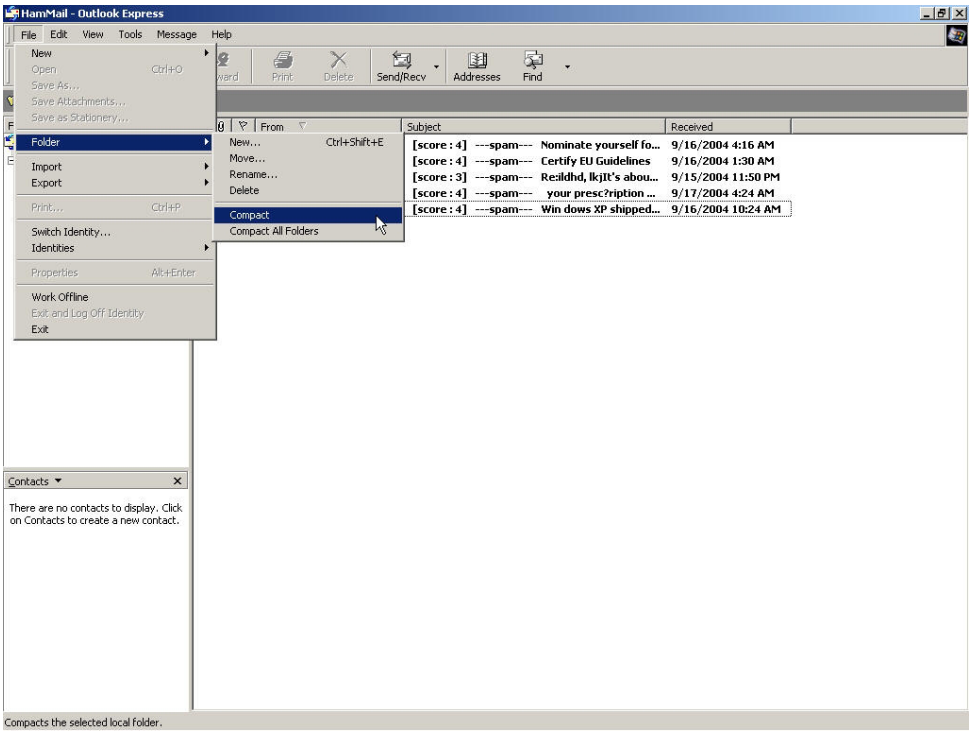


Figure17-48 Compact HamMail File

STEP 4 . To copy the route of HamMail Folder in **Outlook Express** to convenient to upload the training to RS-3000:

- Press the right key of the mouse in HamMail file and select **Properties** function. (Figure17-49)
- Copy the file address in HamMail **Properties** WebUI. (Figure17-50)

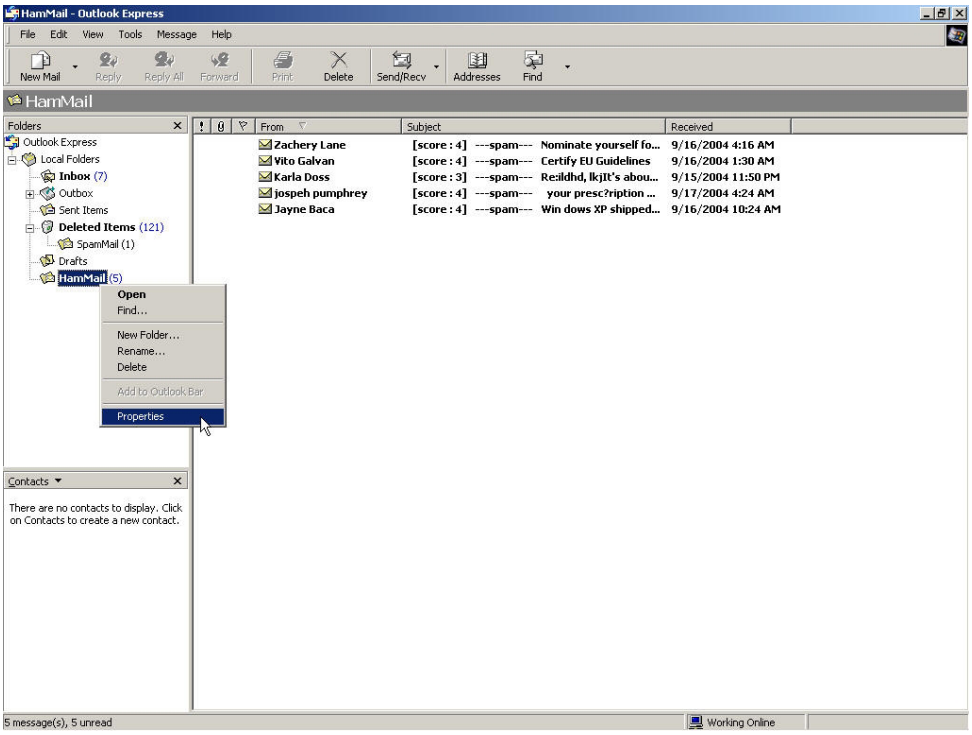


Figure17-49 Select Properties of HamMail File WebUI

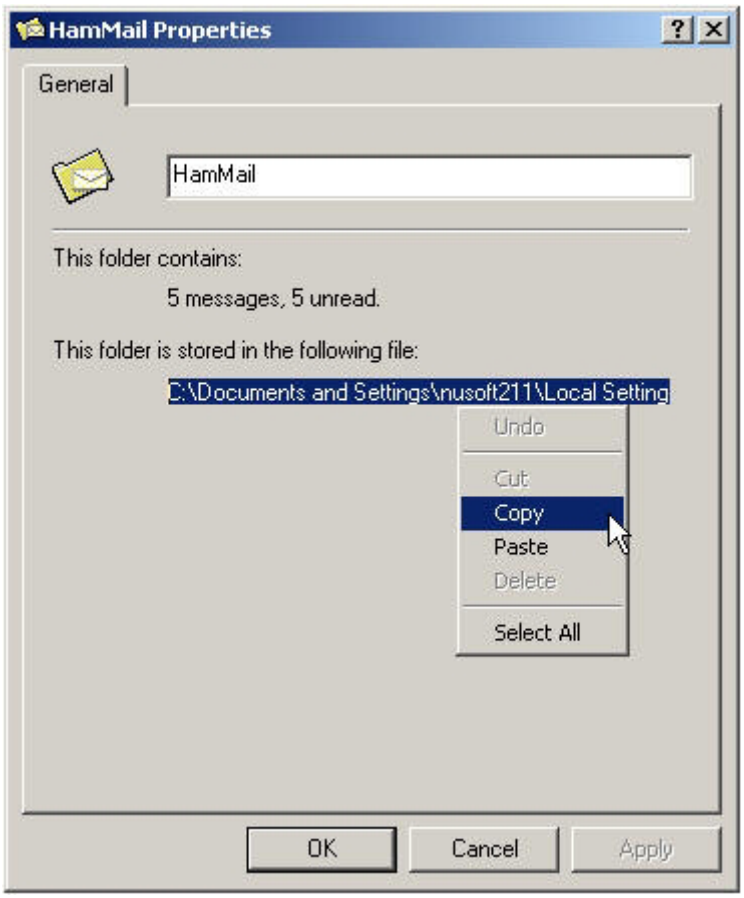


Figure17-50 Copy the File Address that HamMail File Store

STEP 5. Paste the route of copied HamMail file to the **Ham Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to transfer this file to the RS-3000 instantly and to learn the uploaded mail file as ham mail in the appointed time. (Figure17-51)

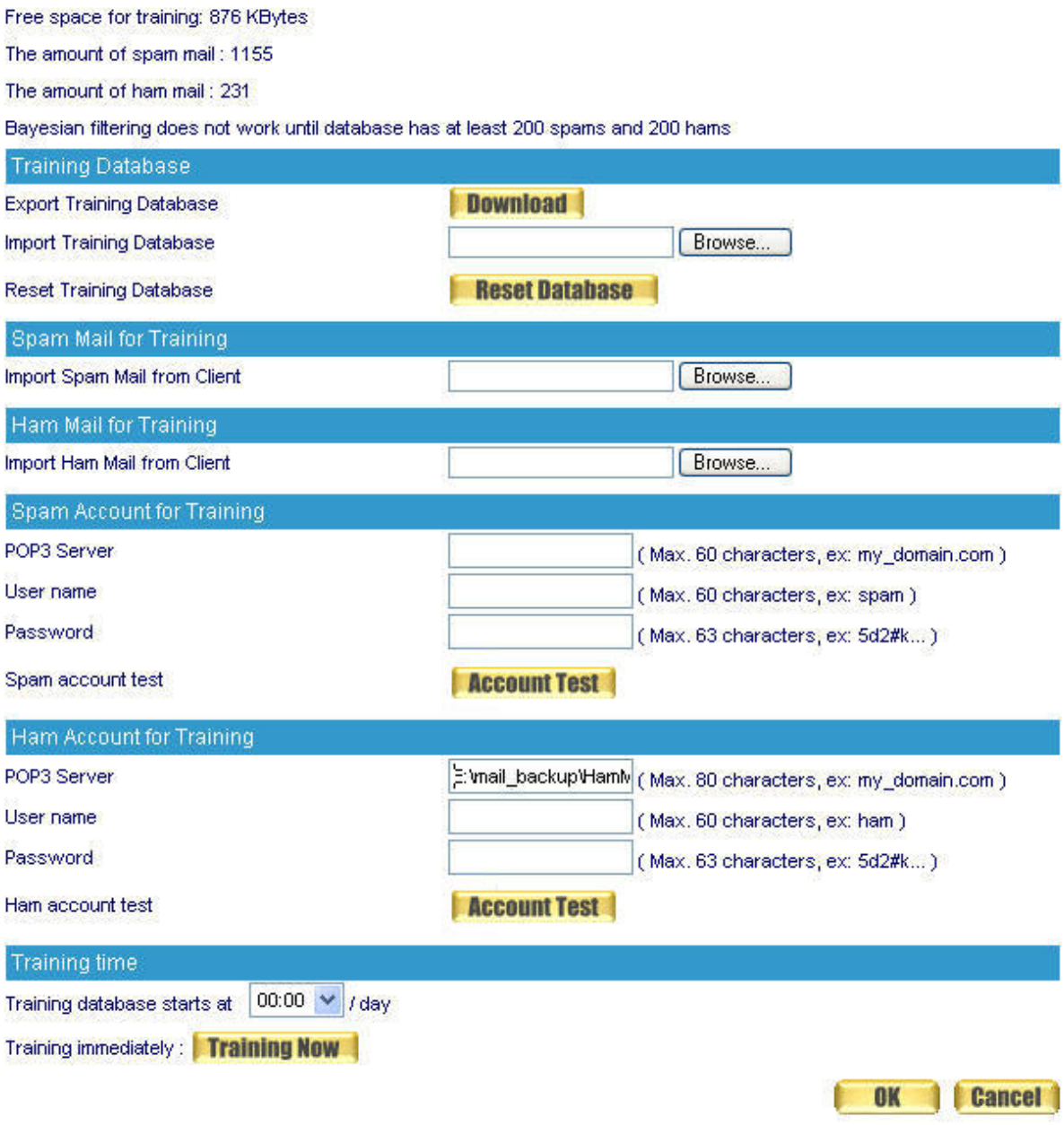


Figure17-51 Paste the File Address that HamMail File Save to make RS-3000 to be trained

STEP 6 . Remove all of the mails in **HamMail** File in **Outlook Express** so that new mails can be compressed and upload to RS-3000 to training directly next time.

- Select all of the mails in **HamMail** and press the right key of the mouse to select **Delete** function. (Figure17-52)
- Make sure that all of the mails in HamMail file had been deleted completely.

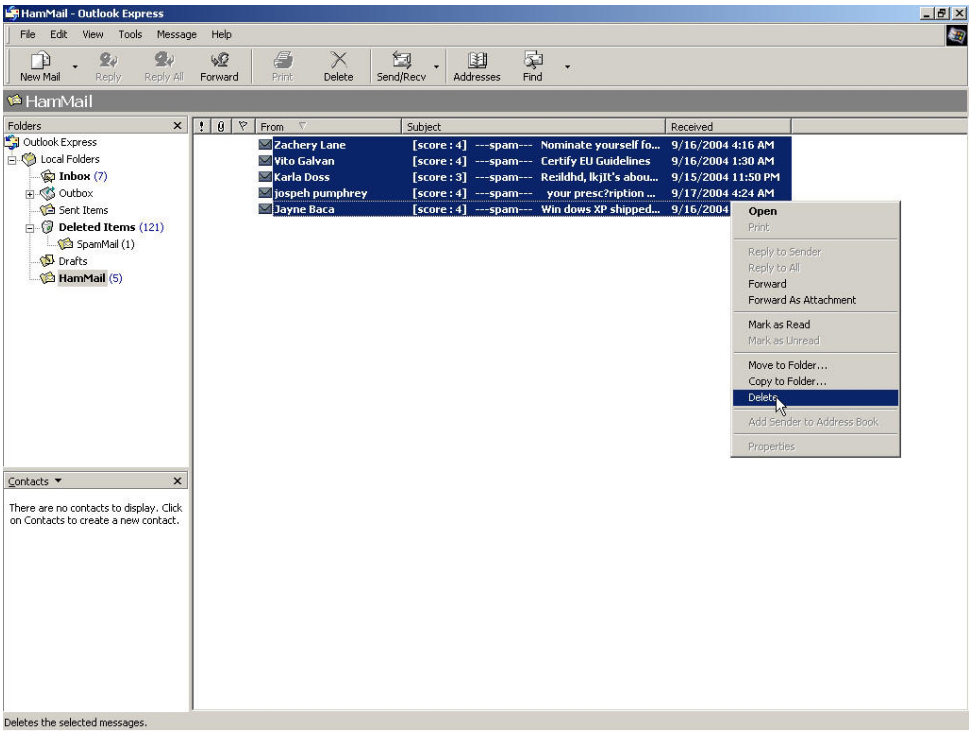


Figure17-52 Delete All of Mails in HamMail File

Chapter 18 Anti-Virus

RS-3000 can scan the mail that sent to Internal Mail Server and prevent the e-mail account of enterprise to receive mails include virus so that it will cause the internal PC be attacked by virus and lose the important message of enterprise.

In this chapter, we will have the detailed illustration about **Anti-Virus:**

Define the required fields of Setting:

Anti-Virus Settings:

- It can detect the virus according to the mails that sent to internal mail server or receive from external mail server.
- It will add warning message in front of the subject of the mail that had been detected have virus. If after scanning and do not discover virus then it will not add any message in the subject field.
- It can set up the time to update virus definitions for each day. Or update virus definitions immediately (Synchronize). It will show the update time and version at the same time.

Action of Infected Mail:

- The mail that had been detected have virus can choose to Delete mail, Deliver to the recipient, or Forward to another mail account

  - After setup the relevant settings in **Mail Relay** function of **Configure**, add the following settings in this function:

    1. **Virus Scanner:** Select Clam
    2. **The Mail Server is placed in** Internal (LAN or DMZ)
    3. **Add the message to the subject line** ---virus---
    4. Select **Remove virus mail and the attached file**
    5. Select **Deliver to the recipient**
    6. Click **OK** (Figure18-1)

Figure18-1 Anti-Virus Settings WebUI

◆ Add the message ---virus---in the subject line of infected mail (Figure18-2)

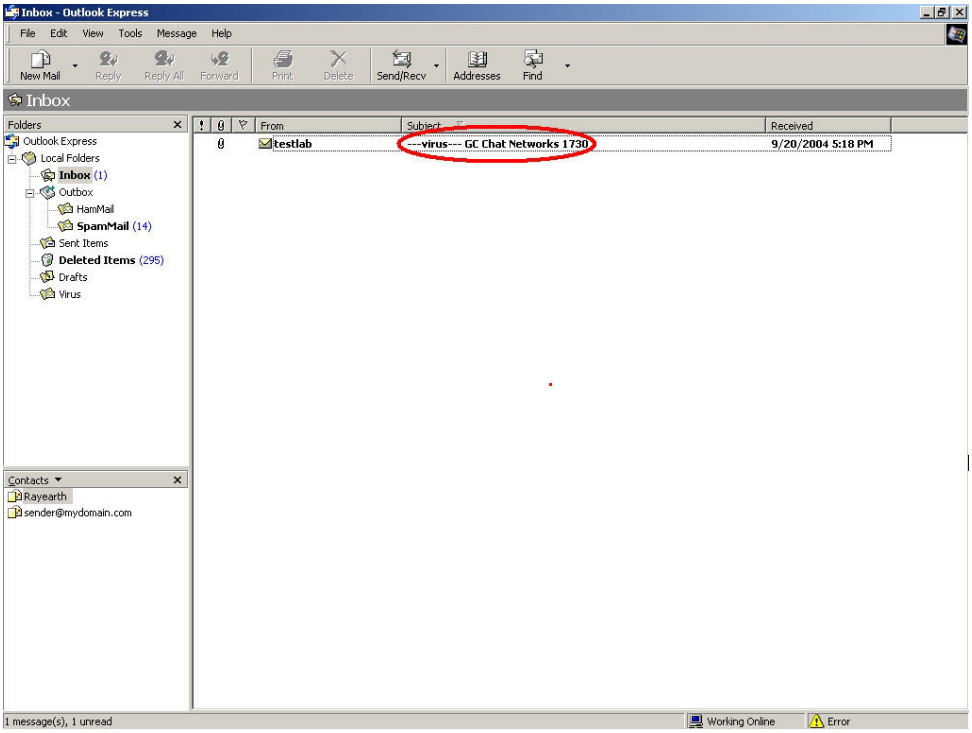


Figure18-2 The Subject of Infected Mail WebUI

When select Disable in **Virus Scanner,** it will stop the virus detection function to e-mail.

Define the required fields of Virus Mail:

Top Total Virus:

- To show the top chart that represent the virus mail that the recipient receives and the sender sent

 In **Top Total Virus** Report, it can choose to display the scanned mail that sent to **Internal** Mail Server or received from **External** Mail Server

 In **Top Total Virus**, it can sort the mail according to Recipient and Sender, Total Virus and Scanned Mail.

To detect if the mail that received from external Mail Server have virus or not

STEP 1． In **LAN Address** to permit a PC receiving the mail from external mail server. Its network card is set as 192.168.139.12, and the DNS setting is DNS server.

STEP 2． In **LAN** of **Address** function, add the following settings: (Figure18-3)

Figure18-3 Mapped IP of Internal User's PC in Address Book

STEP 3． Add the following setting in **Group** of **Service**. (Figure18-4)

Figure18-4 Service Group that includes POP3, SMTP, or DNS

STEP 4． Add the following setting in **Outgoing Policy**: (Figure18-5)

Figure18-5 Outgoing Policy Setting

STEP 5.Add the following setting in **Setting** of **Anti-Virus** function: (Figure18-6)

- **Virus Scanner:** Select Clam
- **The Mail Server is placed in** External (WAN)
- **Add the message to the subject line:** ---virus---
- Select **Deliver a notification mail instead of the original virus mail**

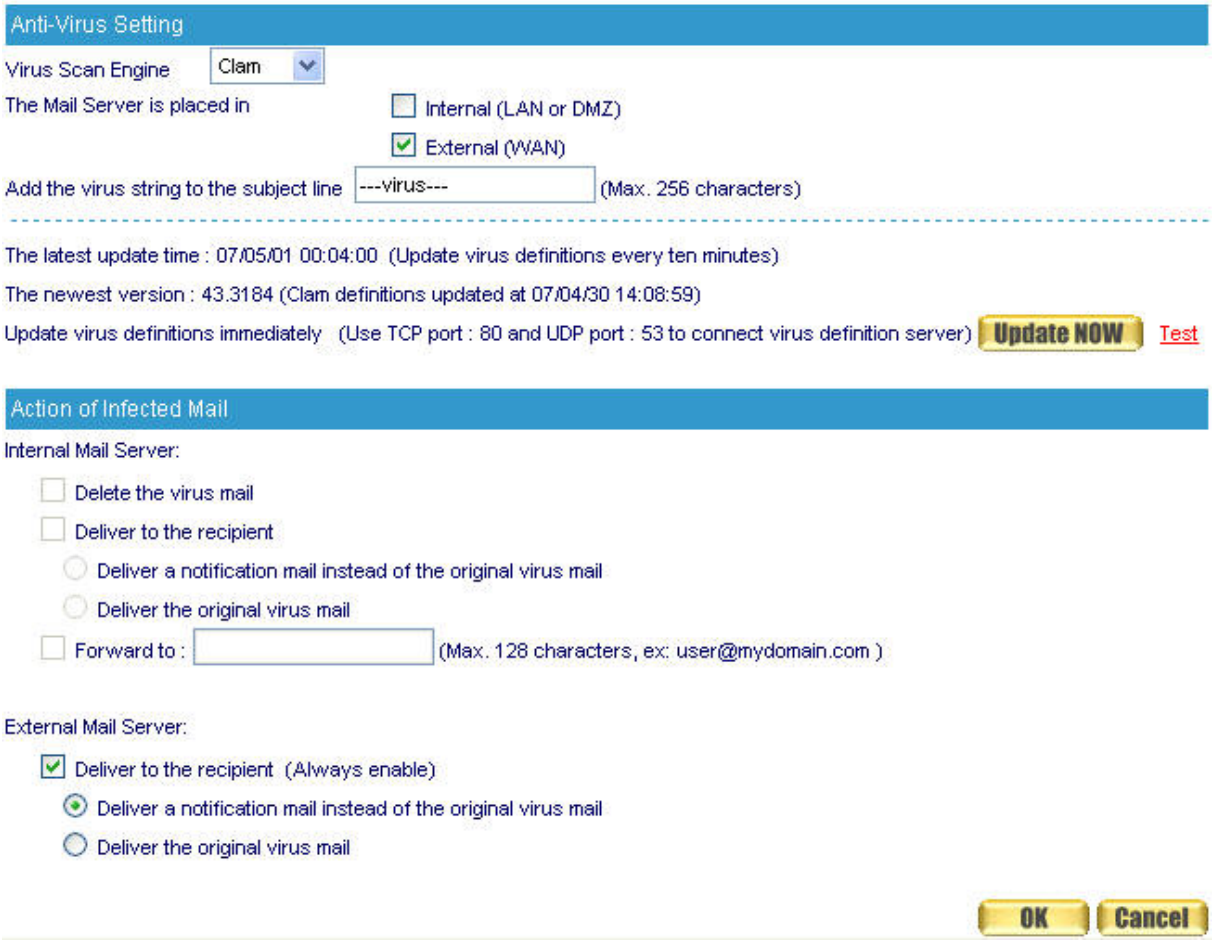


Figure18-6 Action of Infected Mail and Anti-Virus Settings

Anti-Virus function is enabled in default status. So the System Manager does not need to set up the additional setting and then the RS-3000 will scan the mails automatically, which sent to the internal mail server or received from external mail server.

STEP 6.When the internal users are receiving the mail from external mail account (js1720@ms21.pchome.com.tw), the RS-3000 will scan the mail at the same time and the chart will be in the **Virus Mail** in **Anti-Virus** function. (At this time, choose **External** to see the mail account chart) (Figure18-7)

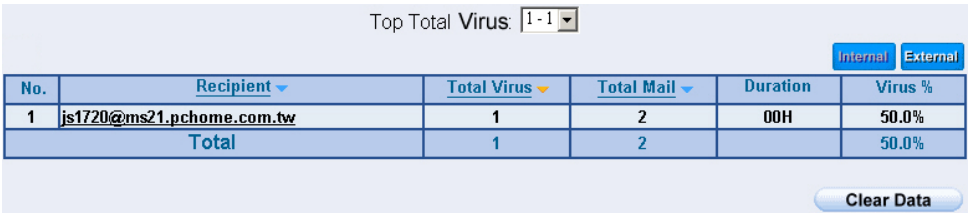


Figure18-7 Report Function Chart

To setup the relevant settings in **Mail Relay** function of **Configure**, so that can choose to display the scanned mail that sent to Internal Mail Server.

To detect the mail that send to Internal Mail Server have virus or not. (Mail Server is in LAN, NAT Mode)

WAN IP of RS-3000: 61.11.11.12

LAN Subnet of RS-3000: 192.168.2.0/24

STEP 1． Set up a mail server in **LAN** and set its network card IP as 192.168.2.12. The DNS setting is external DNS server, and the Master name is broadband.com.tw

STEP 2． Enter the following setting in **LAN** of **Address** function: (Figure18-8)

Figure18-8 Mapped IP Setting in Address of Mail Server

STEP 3． Enter the following setting in **Group** in **Service** function: (Figure18-9)

Figure18-9 Setting Service Group that include POP3, SMTP or DNS

STEP 4． Enter the following setting in **Server1** in **Virtual Server** function: (Figure18-10)

Figure18-10 Virtual Server Setting WebUI

STEP 5 . Enter the following setting in **Incoming Policy**: (Figure18-11)

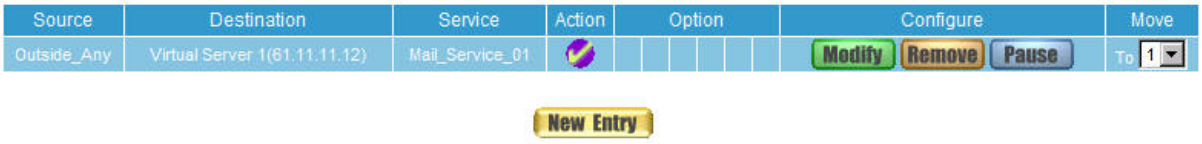


Figure18-11 Incoming Policy Setting

STEP 6 . Enter the following setting in **Outgoing Policy**: (Figure18-12)

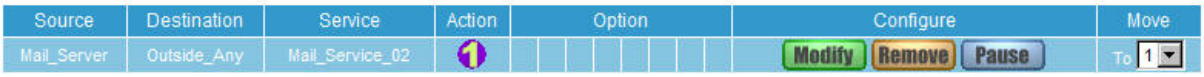


Figure18-12 Outgoing Policy Setting

STEP 7 . Enter the following setting in **Mail Relay** function of **Configure**: (Figure18-13)

Figure18-13 Mail Relay Setting of External Mail to Internal Mail Server

Mail Relay function makes the mails that sent to LAN's mail server could be relayed to its mapped mail server by RS-3000.

STEP 8.Add the following setting in **Setting** of **Anti-Virus** function:

- **Virus Scanner:** Select Clam
- **The Mail Server is placed in** Internal (LAN or DMZ)
- **Add the message to the subject line**: ---virus---
- **Action of Infected Mail:** Select **Deliver to the recipient** (Figure18-14)

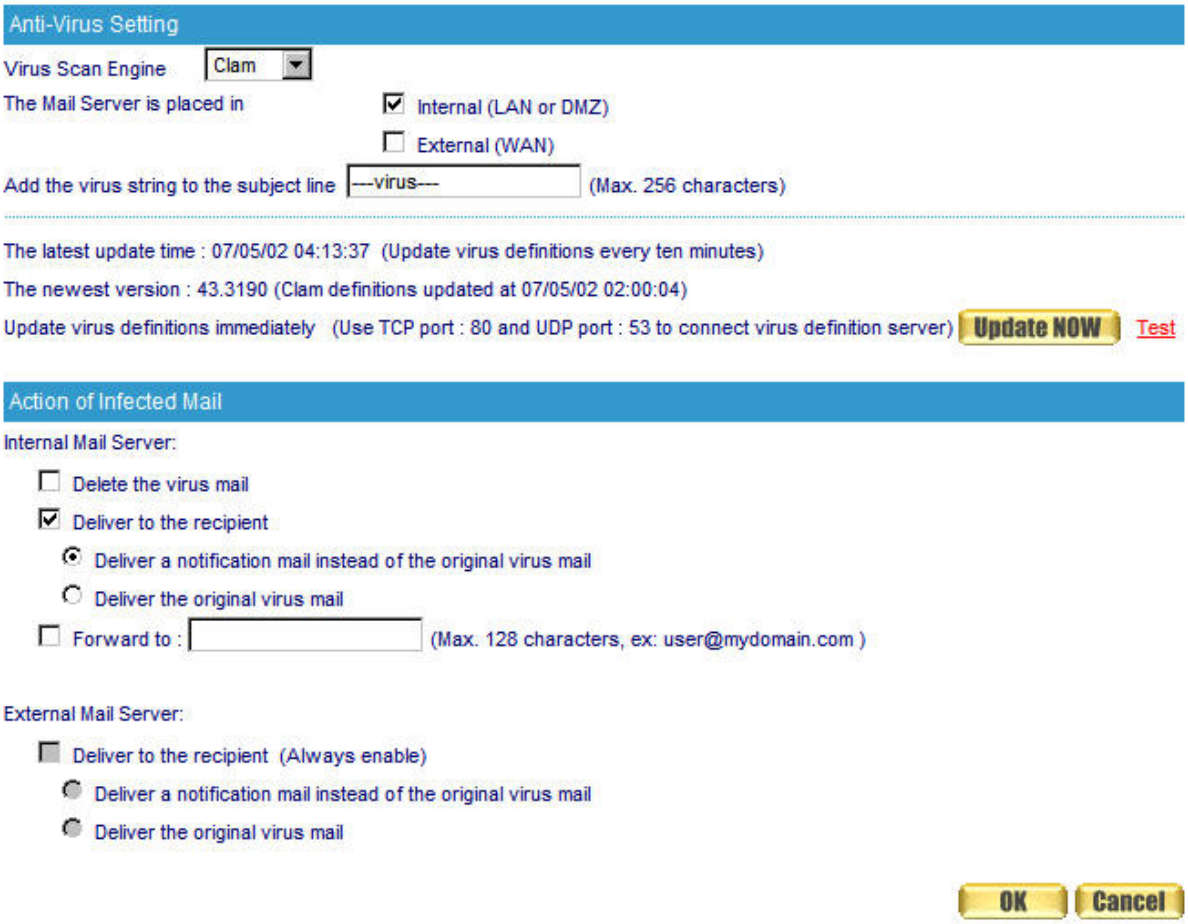


Figure18-14 Infected Mail Definition and Action of Infected Mail

When select **Delete mail** in **Action of Infected Mail**, and then the other functions (**Deliver to the recipient**, or **Forward to**) cannot be selected. So when RS-3000 had scanned mail that have virus, it will delete it directly. But still can check the relevant chart in **Virus Mail** function.

STEP 9.When the external yahoo mail account sends mail to the recipient account of mail server of broadband.com.tw in RS-3000; josh@broadband.com.tw

- If the mails are from the sender account, share2k01@yahoo.com.tw, which include virus in the attached file.
- If it comes from other yahoo sender account share2k003@yahoo.com.tw, which attached file is safe includes no virus.
- After RS-3000 had scanned the mails above, it will bring the chart as follows in the **Virus Mail** function of **Anti-Virus**. (Figure18-15)

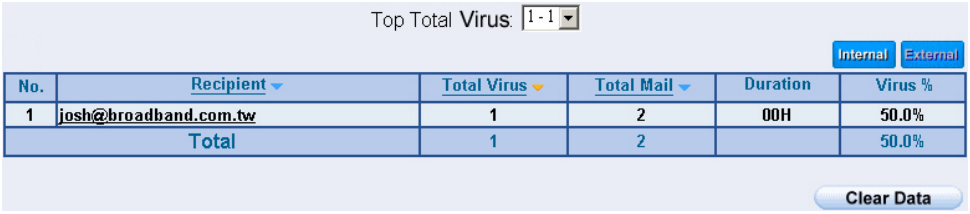


Figure18-15 Report Chart

When clicking on **Remove** button in **Total Virus Mail,** the record of the chart will be deleted and the record cannot be checked in **Virus Mail** function.

Chapter 19 IDP

The RS-3000 can detect the anomaly flow packets and notice the MIS engineer to handle the situation, in order to prevent any suspicious program to invade the destination PC. In other words, the RS-3000 can provide the instant network security protection as detects any internal or external attacks, to enhance the enterprises network stability.

19.1 Setting

- The RS-3000 can update signature definitions every 30 minutes or the MIS engineer can select to use manual update. It also shows the latest update time and version.
- The MIS engineer can enable anti-virus to the compact or non-encryption files.
- Virus engine：The default setting is free to use Clam engine.

 The MIS engineer can click Test, in order to make sure the RS-3000 can connect to the signature definition server normally.

Set default action of all signatures:

- The internet attack risks included High, Medium and Low. The MIS engineer can select the action of Pass, Drop, and Log to the default signatures.
  - In **IDP → Configure → Setting**, to add the following settings：
    1. Select **Enable Anti-Virus**.
    2. **High Risk:** Select Drop, and Log.
    3. **Medium Risk:** Select Drop, and Log.
    4. **Low Risk:** Select Pass, and Log.
    5. Click **OK**. (Figure19-1)
    6. Select enable **IDP** in Policy.

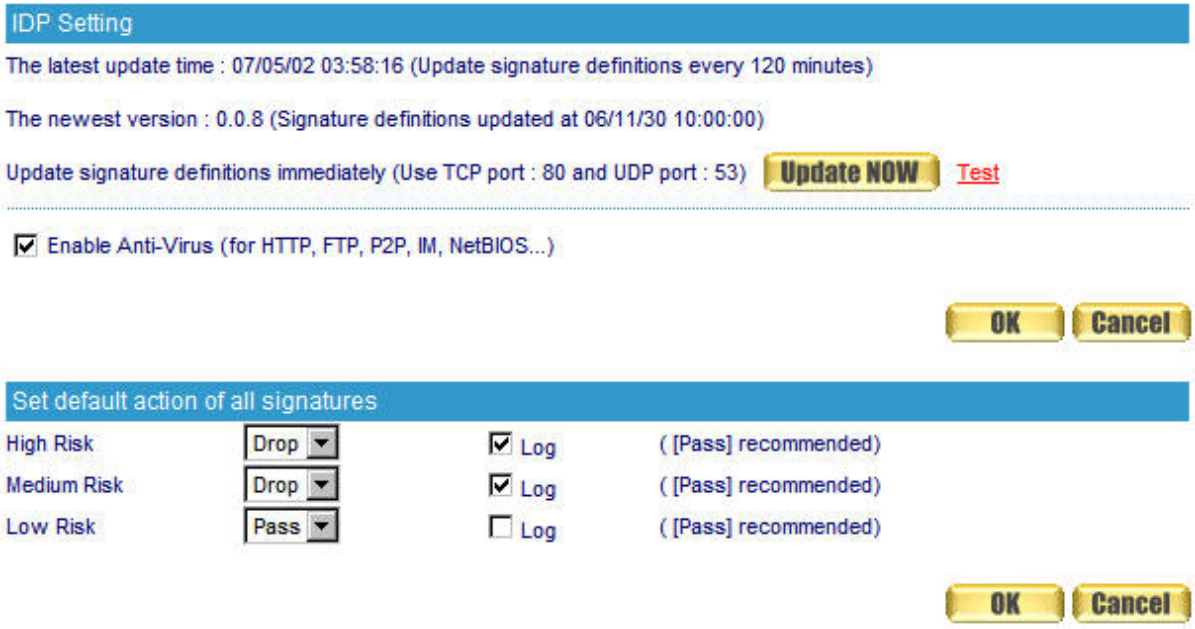


Figure19-1 The IDP setting

  - When the RS-3000 detected the attack types corresponded to the signature, then it will save the **Log** results in **IDP → IDP Report**.

19.2 Signature

The RS-3000 can provide the correspond comparison rules included **Anomaly**, **Pre-defined** and **Custom** according to different attack types.

The **Anomaly** can detect and prevent the anomaly flow and packets via the signature updating. The **Pre-defined** can also detect and prevent the intrusion through the signature updating. Both the anomaly and pre-defined signatures can not be deleted or modified. The **Custom** can detect the other internet attacks, anomaly flow packets except the original **Anomaly** and **Pre-defined** detection according to the user demand.

Anomaly:

- It includes the syn flood, udp flood, icmp flood, syn fin, tcp no flag, fin no ack, tcp land, larg icmp, ip record route, ip strict src record route, ip loose src record route, invalid url, winnuke, bad ip protocol, portscan and http inspect, such Anomaly detection signatures. (Figure 19-2)
- User can enable the anomaly packets signature to detect, depends on the user demand.
- User can manage the specific anomaly flow packets.
- User can modify the action of pass, drop and log.
- The RS-3000 can display all the anomaly detection signature attribute of Name, Enable, Risk, Action, and Log.

Name	Enable	Risk	Action	Log	Configure
syn flood					Modify
udp flood					Modify
icmp flood					Modify
syn fin					Modify
tcp no flag					Modify
fin no ack					Modify
tcp land					Modify
large icmp					Modify
ip record route					Modify
ip strict src record route					Modify
ip loose src record route					Modify
invalid url					Modify
winnuke					Modify
bad ip protocol					Modify
portscan					Modify
http inspect					Modify

Figure19-2 The anomaly signature setting

Pre-defined:

- Pre-defined signature contains 5 general classifications, includes Backdoor, DDoS, Dos, Exploit, NetBIOS and Spyware. Each type also includes its attack signatures, and user can select to enable the specific signature defense system based on the request. (Figure 19-3)
- User can modify the signature action of pass, drop, and log in each type.
- The RS-3000 can display all the attack signature attribute of Name, Risk, Action and Log.

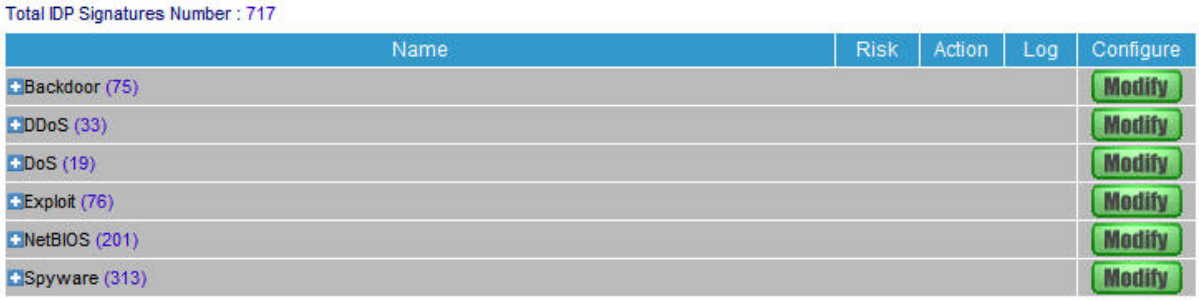


Figure19-3 The Pre-defined setting

Custom:

- Except Anomaly and Pre-defined settings, the RS-3000 also provides a feature to allow user modifying the custom signature, in order to block the specific intruder system.
  - **Name:** The MIS engineer can define the signature name.
  - **Protocol:** The detection and prevention protocol setting includes TCP, UDP, ICMP and IP.
  - **Source Port:** To set the attack PC port.（Range: 0 ~ 65535）
  - **Destination Port:** To set the attacked (victim) PC port.（Range: 0 ~ 65535 ）
  - **Risk:** To define the threats of attack packets.
  - **Action:** The action of attack packets.
  - **Content:** To set the attack packets content.

To detect the anomaly flow and packets with the custom and predefined settings, in order to detect and prevent the intrusion.

STEP 1 **.** In **Configure → Setting**, add the following settings: (Figure 19-4)

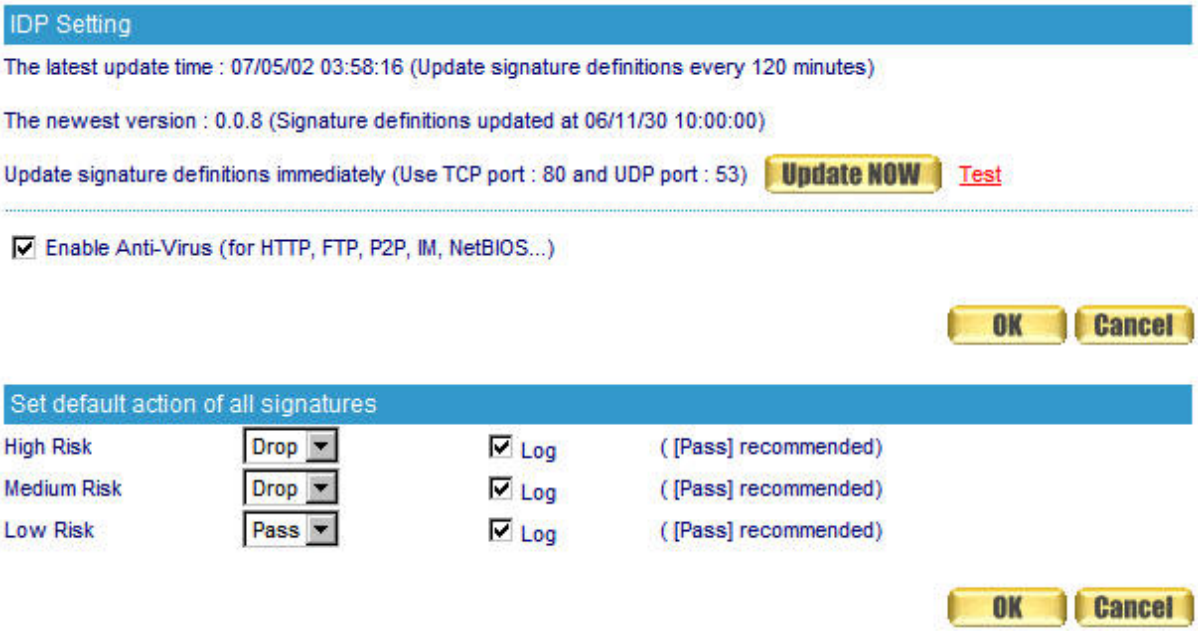


Figure19-4 The IDP configure setting

STEP 2 **.** In **Signature → Anomaly**, add the following settings: (Figure 19-5)

Figure19-5 The Anomaly setting

STEP 3 . In **Signature → Custom**, add the following setting:

- Click **New Entry**. (Figure 19-6)
- **Name**, enter Software_Crack_Website.
- **Protocol**, select TCP.
- **Source Port**, enter 0:65535.
- **Destination Port**, enter 80:80.
- **Risk**, select High.
- **Action**, select Drop and Log.
- **Content**, enter cracks.
- Click **OK** to complete the setting. (Figure 19-7)

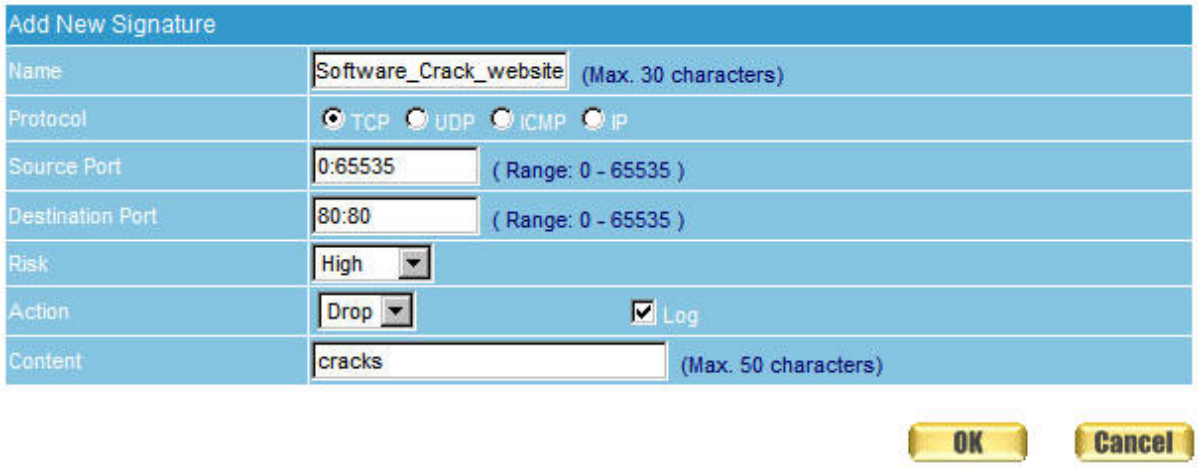


Figure19-6 The custom setting

Figure19-7 Complete the custom setting

STEP 4 **.** In **Policy → Outgoing** , add the new policy and enable **IDP**: (Figure 19-8, 19-9)

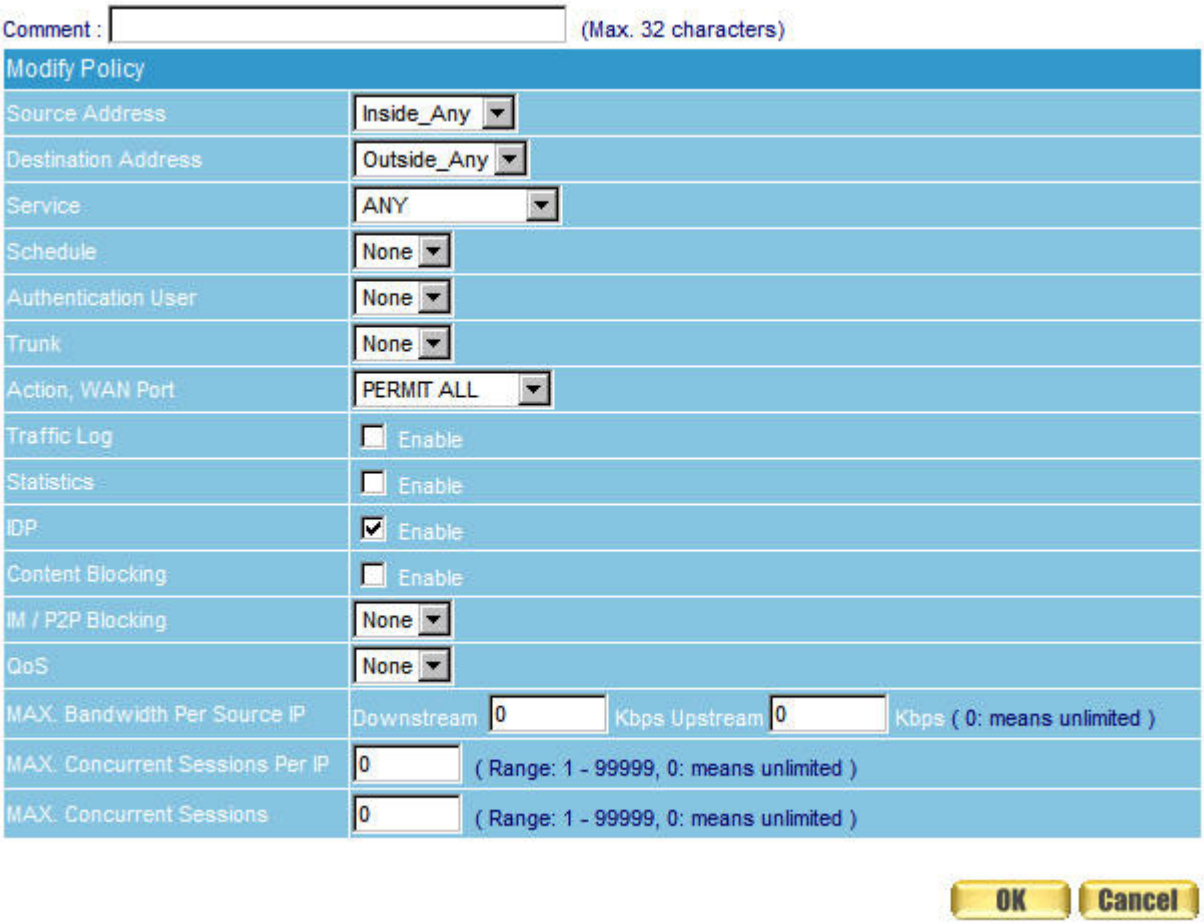


Figure19-8 The IDP setting in Policy

Figure19-9 Complete the IDP setting in Policy

19.3 IDP Report

The RS-3000 can display the IDP record by statistics and log, so the enterprises can easily know the whole network status.

STEP 1． In **IDP Report → Log**, it shows the IDP status in RS-3000.

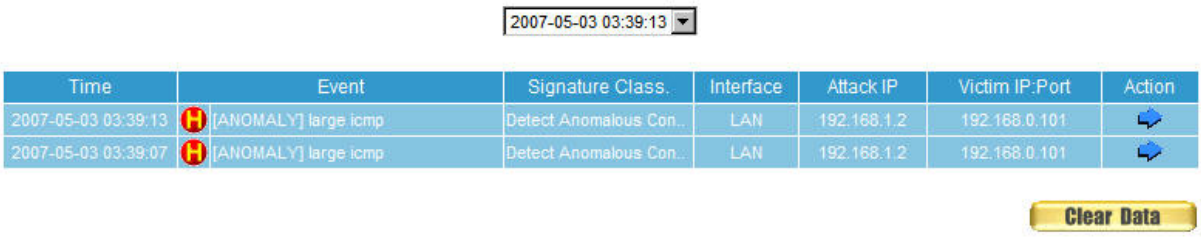


Figure19-9 The IDP log

The icon description in Log:

1. Action:

Icon		
Description	Pass	Drop

2. Risk:

Icon			
Description	High Risk	Medium Risk	Low Risk

Chapter 20 Anomaly Flow IP

When the RS-3000 had detected attacks from hackers and internal PC who are sending large DDoS attacks. The Anomaly Flow IP will start on blocking these packets to maintain the whole network.

In this chapter, we will have the detailed illustration about Anomaly Flow IP:

Define the required fields of Virus-infected IP

The threshold sessions of virus-infected (per source IP)

- When the session number (per source IP) has exceeded the limitation of anomaly flow sessions per source IP, RS-3000 will take this kind of IP to be anomaly flow IP and make some actions. For example, block the anomaly flow IP or send the notification.

Anomaly Flow IP Blocking

- RS-3000 can block the sessions of virus-infected IP.

Notification

- RS-3000 can notice the user and system administrator by e-mail or NetBIOS notification as any anomaly flow occurred.

 After System Manager enable **Anomaly Flow IP**, if the RS-3000 has detected any abnormal situation, the alarm message will appear in **Virus-infected IP**. And if the system manager starts the **E-mail Alert Notification** in **Settings**, the device will send e-mail to alarm the system manager automatically.

RS-3000 Alarm and to prevent the computer which being attacked to send DDoS packets to LAN network

STEP 2． Select **Anomaly Flow IP** setting and enter as the following:

- Enter **The threshold sessions of anomaly flow (per Source IP)** (the default value is 100 Sessions/Sec)
- Select **Enable Anomaly Flow IP Blocking** and enter the **Blocking Time** (the default time is 600 seconds)
- Select **Enable E-Mail Alert Notification**
- Select **Enable NetBIOS Alert Notification**
- **IP Address of Administrator:** Enter 192.168.1.10
- Click **OK**
- Anomaly Flow IP Setting is completed. (Figure20-1)

Figure20-1 Anomaly Flow IP Setting

After complete the Internal Alert Settings, if the device had detected the internal computer sending large DDoS attack packets and then the alarm message will appear in the **Virus-infected IP** or send NetBIOS Alert notification to the infected PC Administrator's PC

If the Administrator starts the **E-Mail Alert Notification** in **Setting**, the RS-3000 will send e-mail to Administrator automatically.

Chapter 21 Log

Log records all connections that pass through the RS-3000's control policies. The information is classified as Traffic Log, Event Log, and Connection Log.

Traffic Log's parameters are setup when setting up 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 Log record the contents of System Configurations changes made by the Administrator such as the time of change, settings that change, the IP address used to log in…etc.

Connection Log records all of the connections of RS-3000. When the connection occurs some problem, the Administrator can trace back the problem from the information.

Application Blocking Log records the contents of Application Blocking result when RS-3000 is configured to block Application connections.

Content Blocking Log records the contents of Content Blocking result when RS-3000 is enabled Content Blocking function.

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.

To detect the information and Protocol port that users use to access Internet or Intranet by RS-3000

STEP 1． Add new policy in **DMZ to WAN** of **Policy** and select **Enable Logging**: (Figure21-1)

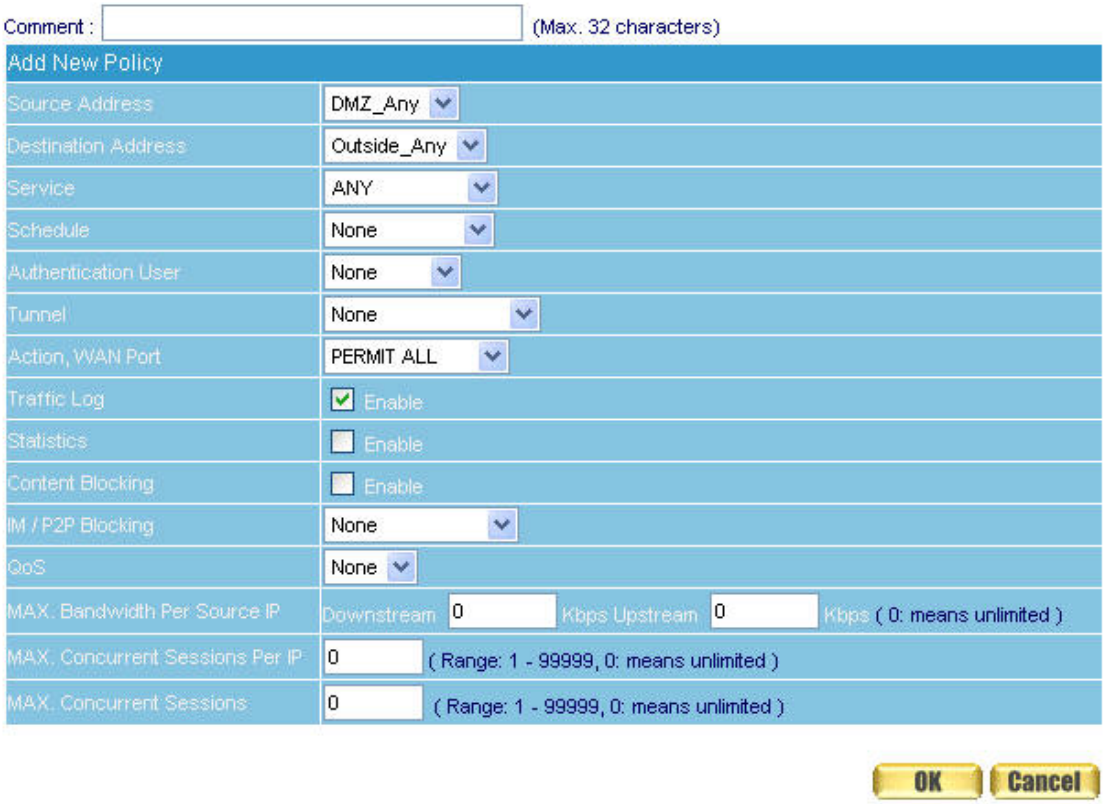


Figure21-1 Logging Policy Setting

STEP 2． Complete the Logging Setting in **DMZ to WAN Policy**: (Figrue21-2)

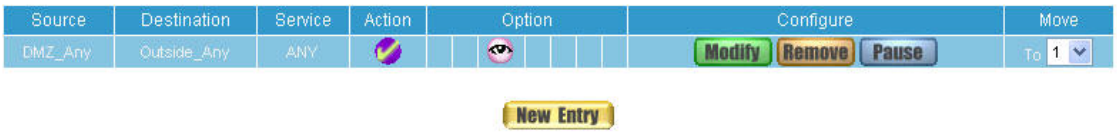


Figure21-2 Complete the Logging Setting of DMZ to WAN

STEP 3 **.** Click **Traffic Log**. It will show up the packets records that pass this policy. (Figure21-3)

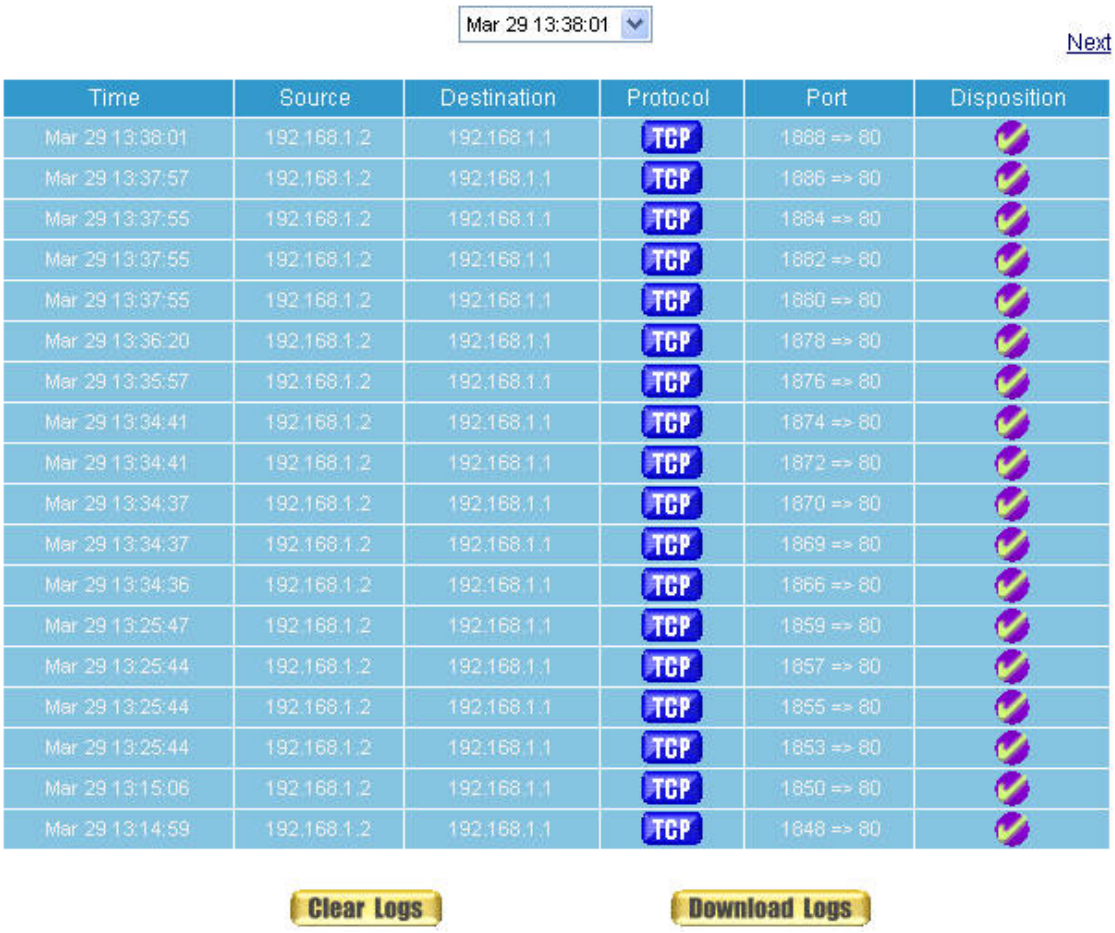


Figure21-3 Traffic Log WebUI

STEP 4 **.** Click on a specific IP of **Source IP** or **Destination IP** in Figure20-3, it will prompt out a WebUI about Protocol and Port of the IP. (Figure21-4)

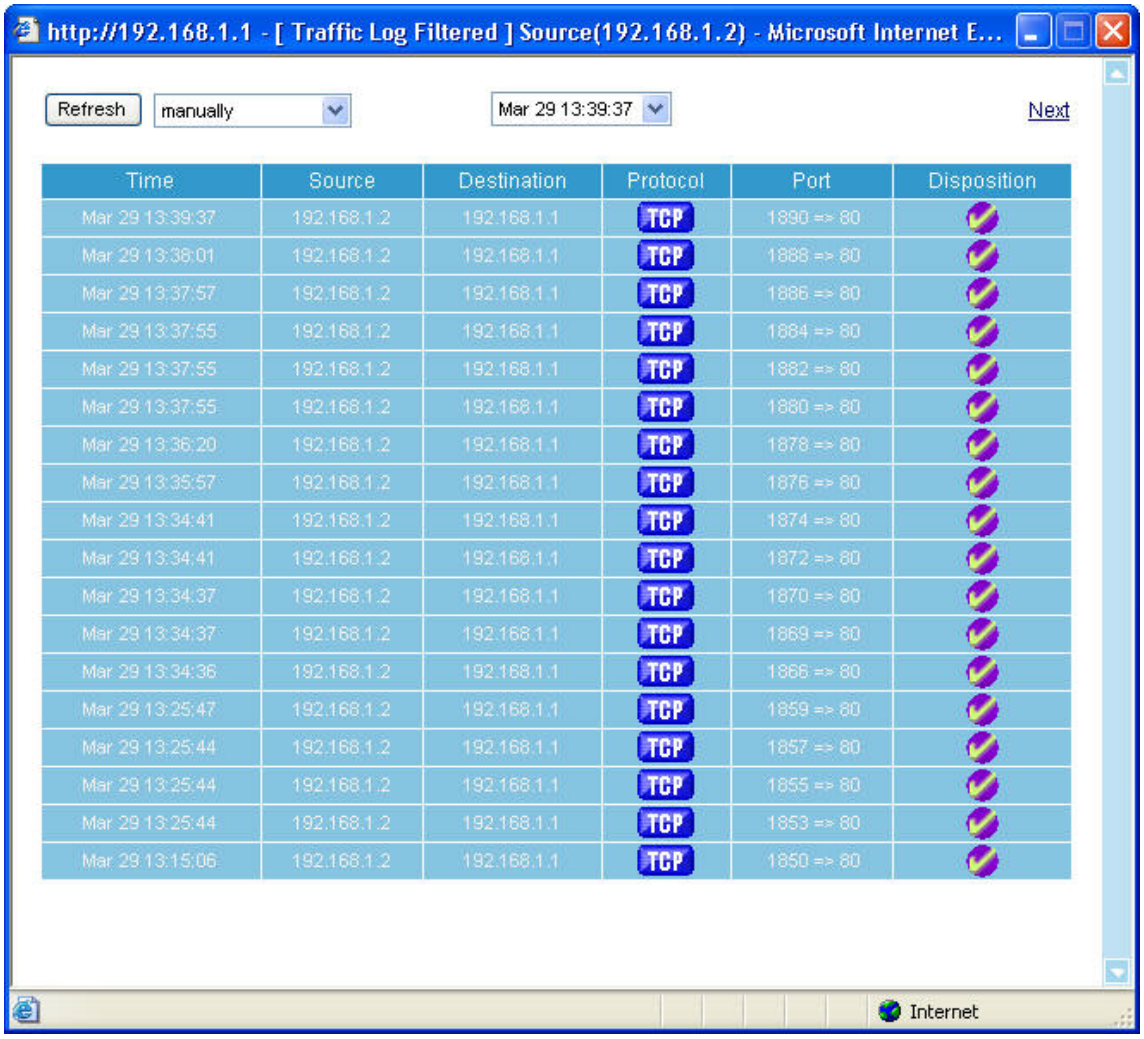


Figure21-4 The WebUI of detecting the Traffic Log by IP Address

STEP 5.Click on **Download Logs**, RS-3000 will pop up a notepad file with the log recorded. User can choose the place to save in PC instantly. (Figure21-5)

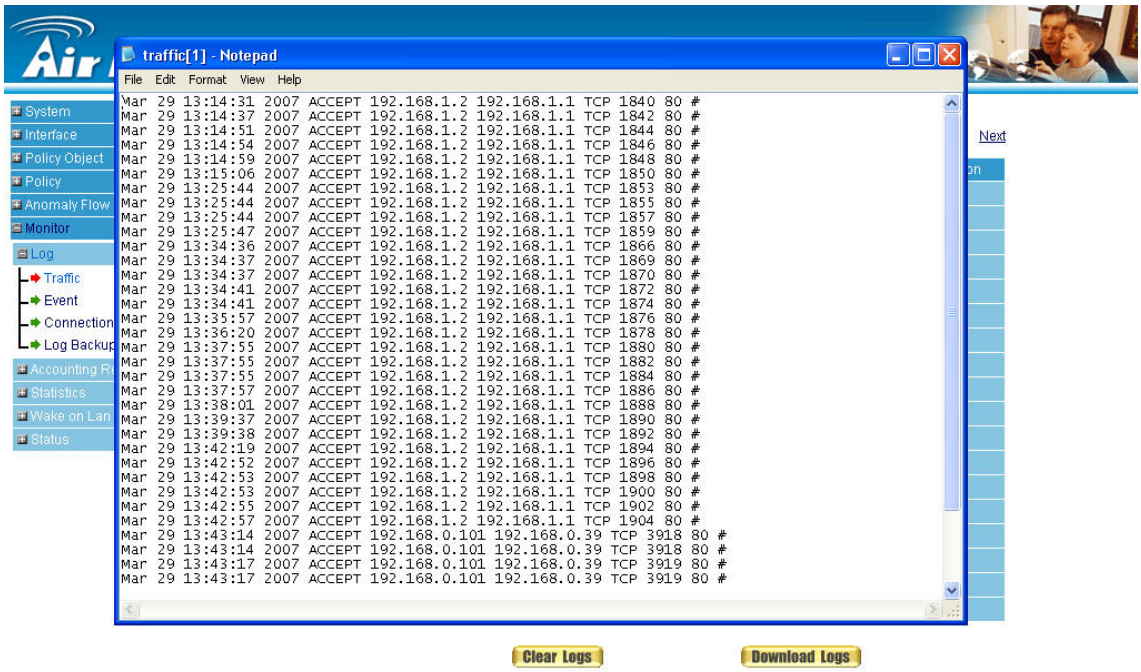


Figure21-5 Download Traffic Log Records WebUI

To record the detailed management events (such as Interface and event description of RS-3000) of the Administrator

STEP 1 . Click **Event** log of **LOG**. The management event records of the administrator will show up (Figure21-6)

Figure21-6 Event Log WebUI

STEP 2 . Click on **Download Logs**, RS-3000 will pop up a notepad file with the log recorded. User can choose the place to save in PC instantly. (Figure21-7)

Figure21-7 Download Event Log Records WebUI

To Detect Event Description of WAN Connection

STEP 1 . Click **Connection** in **LOG**. It can show up WAN Connection records of the RS-3000. (Figure21-8)

Back Mar 29 13:47:19 Next

Time	Connection Log
Mar 29 13:47:19	listening for IKE messages
Mar 29 13:47:19	forgetting secrets
Mar 29 13:47:20	"VPN_A" #24: initiating Main Mode
Mar 29 13:47:31	"VPN_A" #24: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Mar 29 13:48:46	"VPN_A": deleting connection
Mar 29 13:48:48	added connection description "VPN_A"
Mar 29 13:48:49	listening for IKE messages
Mar 29 13:48:49	forgetting secrets
Mar 29 13:48:51	"VPN_A" #25: initiating Main Mode
Mar 29 13:49:01	"VPN_A" #25: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Mar 29 13:50:19	"VPN_A": deleting connection
Mar 29 13:50:20	added connection description "VPN_A"
Mar 29 13:50:22	listening for IKE messages
Mar 29 13:50:22	forgetting secrets
Mar 29 13:50:23	"VPN_A" #26: initiating Main Mode
Mar 29 13:50:34	"VPN_A" #26: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Mar 29 13:51:46	"VPN_A": deleting connection
Mar 29 13:51:47	added connection description "VPN_A"

Figure21-8 Connection records WebUI

STEP 2． Click on **Download Logs**, RS-3000 will pop up a notepad file with the log recorded. User can choose the place to save in PC instantly. (Figure21-9)

Figure21-9 Download Connection Log Records WebUI

If the content of notepad file is not in order, user can read the file with WordPad or MS Word, Excel program, the logs will be displayed with good order.

To save or receive the records that sent by the RS-3000

STEP 1 . Enter **Setting** in **System**, select **Enable E-mail Alert Notification** function and set up the settings. (Figrue21-10)

Figure21-10 E-mail Setting WebUI

STEP 2.Enter **Log Backup** in **Log**, select **Enable Log Mail Support** and click **OK** (Figure21-11)

Figure21-11 Log Mail Configuration WebUI

After **Enable Log Mail Support,** every time when **LOG** is up to 300Kbytes and it will accumulate the log records instantly. And the device will e-mail to the Administrator and clear logs automatically.

STEP 3 **.** Enter **Log Backup** in **Log,** enter the following settings in **Syslog Settings**:

- Select **Enable Syslog Messages**
- Enter the IP in **Syslog Host IP Address** that can receive Syslog
- Enter the receive port in **Syslog Host Port**
- Click **OK**
- Complete the setting (Figure21-12)

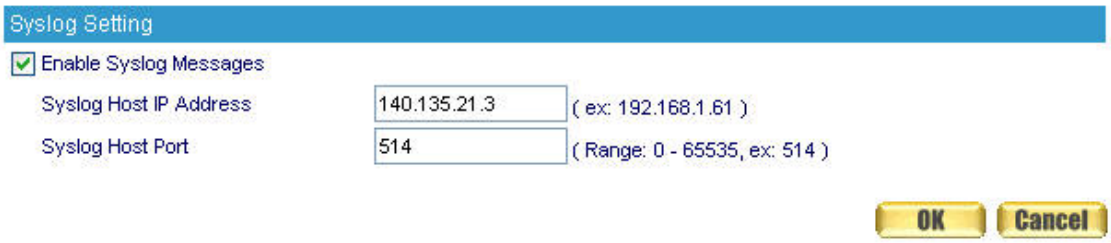


Figure21-12 Syslog Messages Setting WebUI

Chapter 22 Accounting Report

Administrator can use this Accounting Report to inquire the

LAN IP users and WAN IP users, and to gather the statistics of **Downstream/Upstream**, **First packet/Last packet/Duration** and the **Service** for the entire user's IPs that pass the RS-3000.

Define the required fields of Accounting Report

Accounting Report Setting:

- By accounting report function can record the sending information about Intranet and the external PC via RS-3000.

Accounting Report can be divided into two parts: **Outbound Accounting Report** and **Inbound Accounting Report**

Outbound Accounting Report

It is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication network services

Source IP：

- The IP address used by LAN users who use RS-3000

Destination IP：

- The IP address used by WAN service server which uses RS-3000.

Service：

- The communication service which listed in the menu when LAN users use RS-3000 to connect to WAN service server.

Inbound Accounting Report

It is the statistics of downstream / upstream for all kinds of communication services; the Inbound Accounting report will be shown if Internet user connects to LAN Service Server via RS-3000.

Source IP：

- The IP address used by WAN users who use RS-3000

Destination IP：

- The IP address used by LAN service server who use RS-3000

Service：

- The communication service which listed in the menu when WAN users use RS-3000 to connect to LAN Service server.

Outbound

STEP 1 **.** Select to enable the items for Outbound Accounting Report in **Setting** of **Accounting Report** function. (Figure22-1)

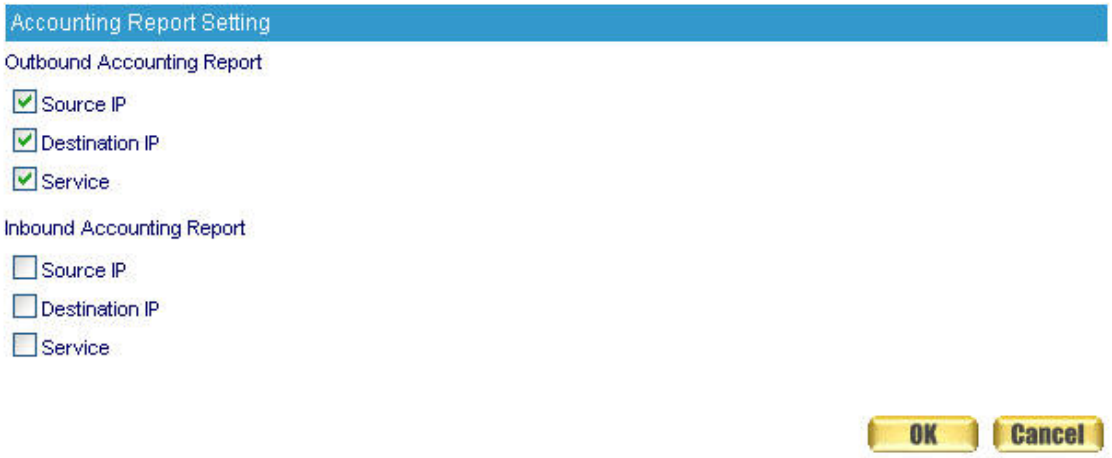


Figure22-1 Accounting Report Setting

STEP 2 **.** Enter **Outbound** in **Accounting Report** and select **Source IP** to inquire the statistics of Send/Receive packets, **Downstream / Upstream, First packet /Last packet/Duration** from the LAN or DMZ user's IP that pass the RS-3000. (Figure22-2)

- **TOP:** Select the data you want to review; it presents 10 results in one page.
- **Source IP**：To display the report sorted by Source IP, the LAN users who access WAN service server via RS-3000.
- **Downstream**：The percentage of downstream and the value of each WAN service server which passes through RS-3000 to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who passes through RS-3000 to WAN service server.
- **First Packet**：When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time between the first packet and the last packet.
- **Total Traffic**：The RS-3000 will record and display the amount of Downstream and Upstream packets passing from LAN user to WAN Server.

- **Reset Counter**：Click Reset Counter button to refresh Accounting Report.

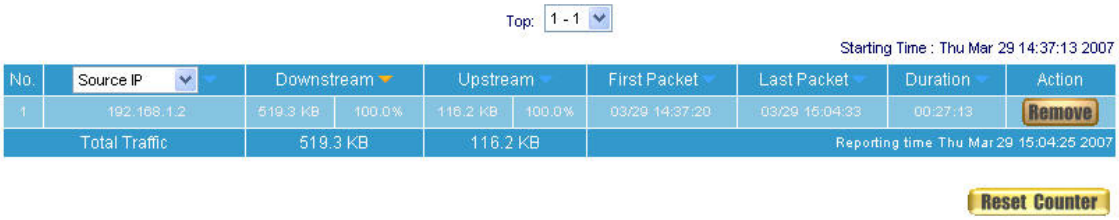


Figure22-2 Outbound Source IP Statistics Report

STEP 3 **.** Enter **Outbound** in **Accounting Report** and select **Destination IP** to inquire the statistics of Send/Receive packets, **Downstream/Upstream, First packet/Last packet/Duration** from the WAN Server to pass the RS-3000. (Figure22-3)

- **TOP**：Select the data you want to view; it presents 10 results in one page.
- **Destination IP**：To display the report sorted by Destination IP, the IP address used by WAN service server connecting to RS-3000.
- **Downstream**：The percentage of downstream and the value of each WAN service server which passes through RS-3000 to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who passes through RS-3000 to WAN service server.
- **First Packet**：When the first packet is sent from WAN service server to LAN users, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time between the first packet and the last packet.
- **Total Traffic**：The RS-3000 will record and display the amount of Downstream and Upstream packets passing from WAN Server to LAN user.
- **Reset Counter**：Click Reset Counter button to refresh Accounting Report.

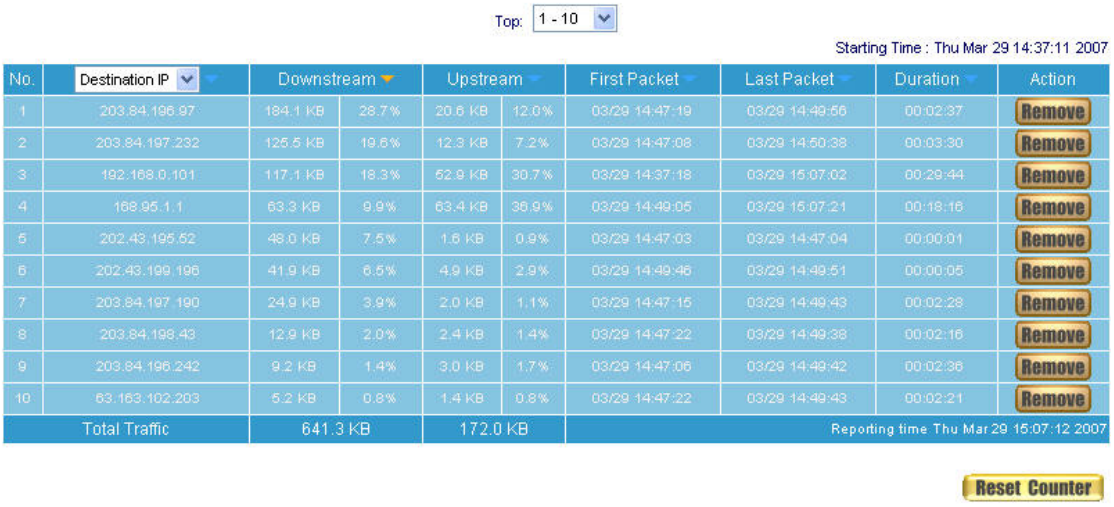


Figure22-3 Outbound Destination IP Statistics Report

STEP 4 . Enter **Outbound** in **Accounting Report** and select **Top Services** to inquire the statistics webpage of **Send/Receive packets, Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the RS-3000. (Figure22-4)

- **TOP**：Select the data you want to view. It presents 10 results in one page.
-  ：According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart. (Figure22-5)
- **Service**：To display the report sorted by Port, which LAN users use the RS-3000 to connect to WAN service server.
- **Downstream**：The percentage of downstream and the value of each WAN service server who passes through RS-3000 and connects to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who passes through RS-3000 to WAN service server.
- **First Packet**：When the first packet is sent to the WAN Service Server, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet is sent from the WAN Service Server, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The RS-3000 will record and display the amount of Downstream and Upstream packets passing from LAN users to WAN service server.
- **Reset Counter**：Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 10

Starting Time : Thu Mar 29 15:38:16 2007

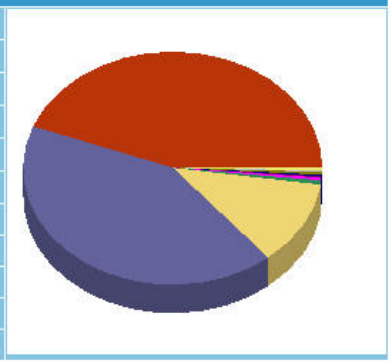
No.	Service	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	HTTPS [443]	96.2 KB	56.3%	29.4 KB	68.4%	03/29 15:38:22	03/29 15:39:26	00:01:04	Remove
2	HTTP [80]	74.1 KB	43.3%	12.3 KB	28.6%	03/29 15:36:17	03/29 15:39:26	00:03:09	Remove
3	MICROSOFT-DS [445]	368.0 B	0.2%	518.0 B	1.2%	03/29 15:38:22	03/29 15:40:01	00:01:39	Remove
4	RTSP [554]	150.0 B	0.1%	126.0 B	0.3%	03/29 15:39:50	03/29 15:40:01	00:00:11	Remove
5	UNKNOW [4254]	91.0 B	0.1%	137.0 B	0.3%	03/29 15:39:50	03/29 15:40:01	00:00:11	Remove
6	UNKNOW [20366]	0.0 B	0.0%	63.0 B	0.1%	03/29 15:40:00	03/29 15:40:00	00:00:00	Remove
7	UNKNOW [4713]	0.0 B	0.0%	63.0 B	0.1%	03/29 15:39:54	03/29 15:39:54	00:00:00	Remove
8	UNKNOW [4242]	0.0 B	0.0%	96.0 B	0.2%	03/29 15:39:39	03/29 15:39:41	00:00:02	Remove
9	UNKNOW [54007]	0.0 B	0.0%	125.0 B	0.3%	03/29 15:39:50	03/29 15:39:59	00:00:09	Remove
10	UNKNOW [6100]	0.0 B	0.0%	63.0 B	0.1%	03/29 15:39:53	03/29 15:39:53	00:00:00	Remove
Total Traffic		170.8 KB		43.0 KB		Reporting time Thu Mar 29 15:40:03 2007			

Reset Counter

Figure22-4 Outbound Services Statistics Report

Service Distribution

No.	Downstream	
1	HTTPS [443]	100.4 KBytes (44.2%)
2	HTTP [80]	95.2 KBytes (41.9%)
3	MICROSOFT-DS [445]	26.4 KBytes (11.6%)
4	UNKNOW [4672]	1.1 KBytes (0.5%)
5	UNKNOW [4254]	721.0 Bytes (0.3%)
6	UNKNOW [4713]	622.0 Bytes (0.3%)
7	RTSP [554]	592.0 Bytes (0.3%)
8	UNKNOW [4256]	479.0 Bytes (0.2%)
9	UNKNOW [3320]	360.0 Bytes (0.2%)
10	UNKNOW [4675]	278.0 Bytes (0.1%)
	OTHER	962.0 Bytes (0.4%)



No.	Upstream	
1	HTTPS [443]	30.2 KBytes (56.4%)
2	HTTP [80]	15.7 KBytes (29.4%)
3	MICROSOFT-DS [445]	2.0 KBytes (3.7%)
4	UNKNOW [4672]	1.3 KBytes (2.5%)
5	UNKNOW [4254]	374.0 Bytes (0.7%)
6	UNKNOW [4713]	363.0 Bytes (0.7%)
7	UNKNOW [6100]	252.0 Bytes (0.5%)
8	RTSP [554]	168.0 Bytes (0.3%)
9	UNKNOW [4256]	168.0 Bytes (0.3%)
10	TRACEROUTE [33434]	128.0 Bytes (0.2%)
	OTHER	2.9 KBytes (5.4%)

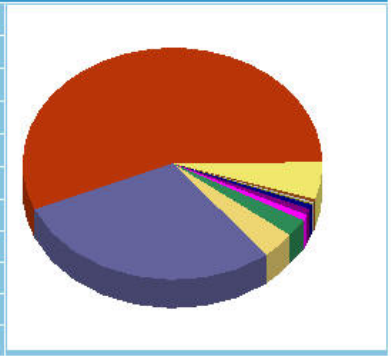


Figure22-5 The Pizza chart of Accounting report published base on Service

 Press  to return to **List Table** of **Accounting Report** window.

 Accounting Report function will occupy lots of hardware resource, so users must take care to choose the necessary items, in order to avoid slowing down the total performance.

Inbound

STEP 1 . Select to enable the items for Inbound Accounting Report in **Setting** of **Accounting Report** function. (Figure22-6)

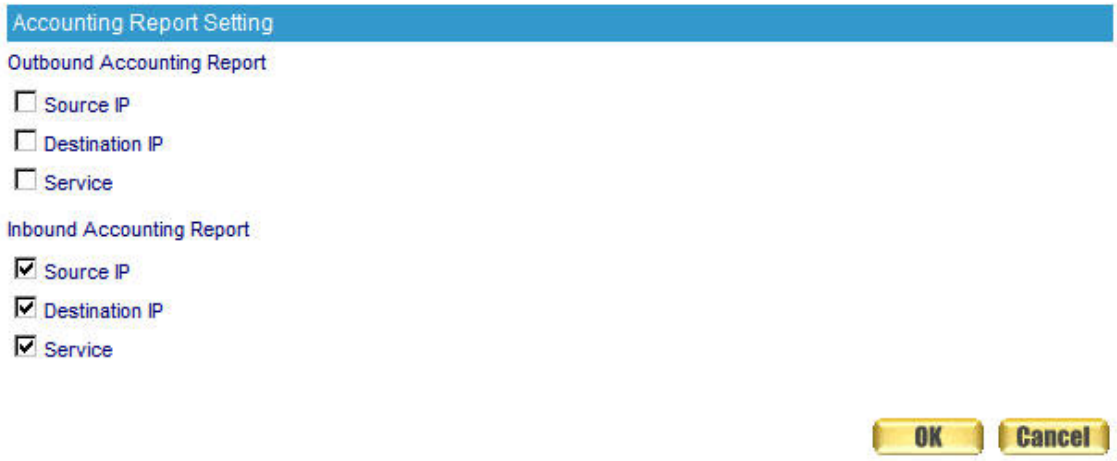


Figure22-6 Accounting Report Setting

STEP 2 . Enter **Inbound** in **Accounting Report** and select **Top Users** to inquire the statistics of **Send/Receive packets**, **Downstream/Upstream, First packet / Last packet / Duration** from the WAN user to pass the RS-3000. (Figure22-7)

- **TOP**：Select the data you want to view. It presents 10 pages in one page.
- **Source IP**：To display the report sorted by Source IP, the IP address used by WAN user connecting to RS-3000.
- **Downstream**：The percentage of Downstream and the value of each WAN user which passes through RS-3000 to LAN service server.
- **Upstream**：The percentage of Upstream and the value of each LAN service server which passes through RS-3000 to WAN users.
- **First Packet**：When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The RS-3000 will record and display the amount of Downstream and Upstream packets passing from WAN users to LAN service server.
- **Reset Counter**：Click the Reset Counter button to refresh the Accounting Report.

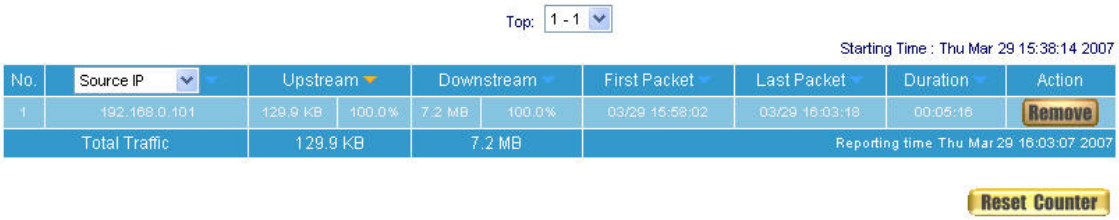


Figure22-7 Inbound Top Users Statistics Report

STEP 3 . Enter **Inbound** in **Accounting Report** and select **Top Sites** to inquire the statistics website of **Send / Receive packets**, **Downstream / Upstream, First packet / Last packet / Duration** from the WAN user to pass the RS-3000. (Figure22-8)

- **TOP**：Select the data you want to view. It presents 10 pages in one page.
- **Destination IP**：To display the report sorted by Destination IP, the IP address used by LAN service server passing through RS-3000 to WAN users.
- **Downstream**：The percentage of Downstream and the value of each WAN user who passes through RS-3000 to LAN service server.
- **Upstream**：The percentage of Upstream and the value of each LAN service server who passes through RS-3000 to WAN users.
- **First Packet**：When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The RS-3000 will record the sum of time and show the percentage of each WAN user's upstream / downstream to LAN service server.
- **Reset Counter**：Click the Reset Counter button to refresh the Accounting Report.

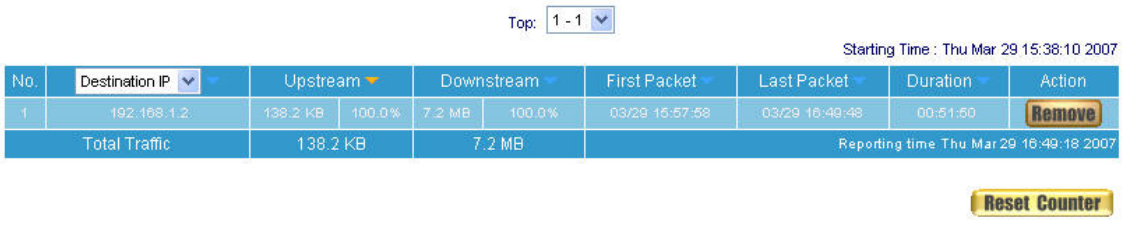


Figure 22-8 Outbound Destination IP Statistics Report

STEP 4 . Enter **Inbound** in **Accounting Report** and select **Top Services** to inquire the statistics website of Send/Receive packets, **Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the RS-3000. (Figure22-9)

- **TOP**：Select the data you want to view. It presents 10 results in one page.
-  ：According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart. (Figure22-10)
- **Service**：The report of Communication Service when WAN users use the RS-3000 to connect to LAN service server.
- **Downstream**：The percentage of downstream and the value of each WAN user who uses RS-3000 to LAN service server.
- **Upstream**：The percentage of upstream and the value of each LAN service server who uses RS-3000 to WAN user.
- **First Packet**：When the first packet is sent to the LAN Service Server, the sent time will be recorded by the RS-3000.
- **Last Packet**：When the last packet is sent from the LAN Service Server, the sent time will be recorded by the RS-3000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The RS-3000 will record the sum of time and show the percentage of each Communication Service's upstream / downstream to LAN service server.
- **Reset Counter**：Click the Reset Counter button to refresh the Accounting Report.

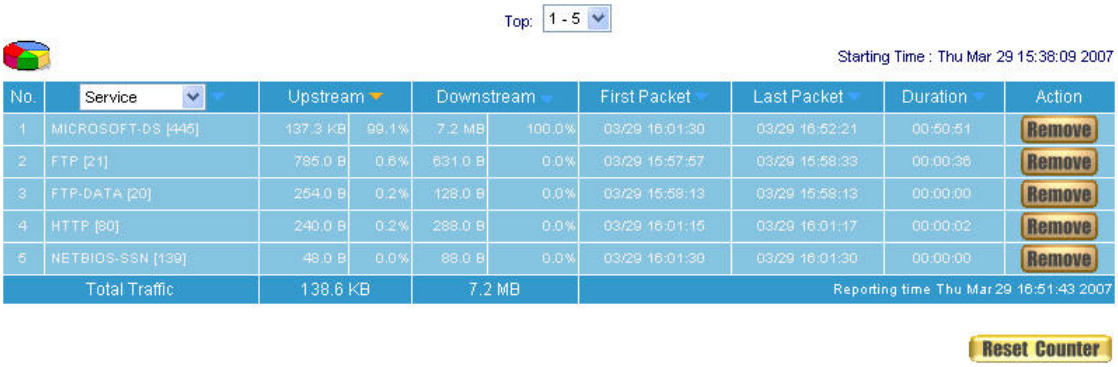
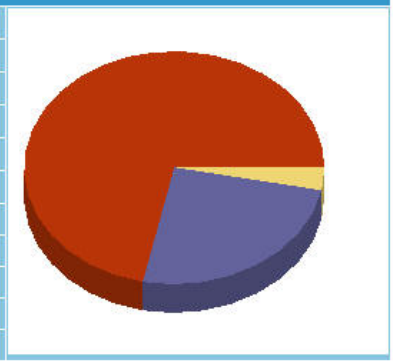


Figure22-9 Inbound Services Statistics Report

Service Distribution

No.	Downstream	
1	MICROSOFT-DS [445]	139.0 KBytes (71.6%)
2	FTP-DATA [20]	49.1 KBytes (25.3%)
3	FTP [21]	5.9 KBytes (3.0%)
4	HTTP [80]	240.0 Bytes (0.1%)
5	NETBIOS-SSN [139]	48.0 Bytes (0.0%)
	OTHER	0.0 Bytes (0.0%)



No.	Upstream	
1	MICROSOFT-DS [445]	7.2 MBytes (71.7%)
2	FTP-DATA [20]	2.8 MBytes (28.2%)
3	FTP [21]	4.1 KBytes (0.0%)
4	HTTP [80]	288.0 Bytes (0.0%)
5	NETBIOS-SSN [139]	88.0 Bytes (0.0%)
	OTHER	0.0 Bytes (0.0%)

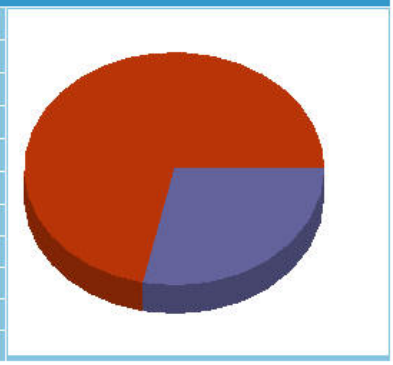


Figure22-10 The Pizza chart of Inbound Accounting report published base on Service

Accounting Report function will occupy lots of hardware resource, so users must take care to choose the necessary items, in order to avoid slowing down the total performance.

Chapter 23 Statistic

WAN Statistics:

The statistics of Downstream / Upstream packets
and Downstream/Upstream traffic record that pass WAN Interface

Policy Statistics:

The statistics of Downstream / Upstream packets and Downstream / Upstream traffic record that pass Policy

In this chapter, the Administrator can inquire the RS-3000 for statistics of packets and data that passes across the RS-3000. The statistics provides the Administrator with information about network traffics and network loads.

Define the required fields of Statistics:

Statistics Chart:

- **Y-Coordinate**：Network Traffic（Kbytes/Sec）
- **X-Coordinate**：Time（Hour/Minute）

Source IP, Destination IP, Service, and Action:

- These fields record the original data of Policy. From the information above, the Administrator can know which Policy is the Policy Statistics belonged to.

Time:

- To detect the statistics by minutes, hours, days, months, or years.

Bits/sec, Bytes/sec, Utilization, Total:

- The unit that used by Y-Coordinate, which the Administrator can change the unit of the Statistics Chart here.
  - **Utilization**：The percentage of the traffic of the Max. Bandwidth that System Manager set in Interface function.
  - **Total:** To consider the accumulative total traffic during a unit time as Y-Coordinate

WAN Statistics

STEP 1 **.** Enter **WAN** in **Statistics** function, it will display all the statistics of Downstream/Upstream packets and Downstream/Upstream record that pass **WAN** Interface. (Figure23-1)

WAN	Time
WAN 1	Minute Hour Day Week Month Year
WAN 2	Minute Hour Day Week Month Year
All WAN Interface	Minute Hour Day Week Month Year

Figure23-1 WAN Statistics function

- **Time:** To detect the statistics by minutes, hours, days, week, months, or years.

WAN Statistics is the additional function of **WAN** Interface. When enable **WAN** Interface, it will enable **WAN Statistics** too.

STEP 2 **.** In the Statistics window, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics figure every minute; click **Hour** to check the Statistics figure every hour; click **Day** to check the Statistics figure every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

STEP 3 . Statistics Chart (Figure23-2)

- **Y-Coordinate**：Network Traffic（Kbytes/Sec）
- **X-Coordinate**：Time（Hour/Minute）

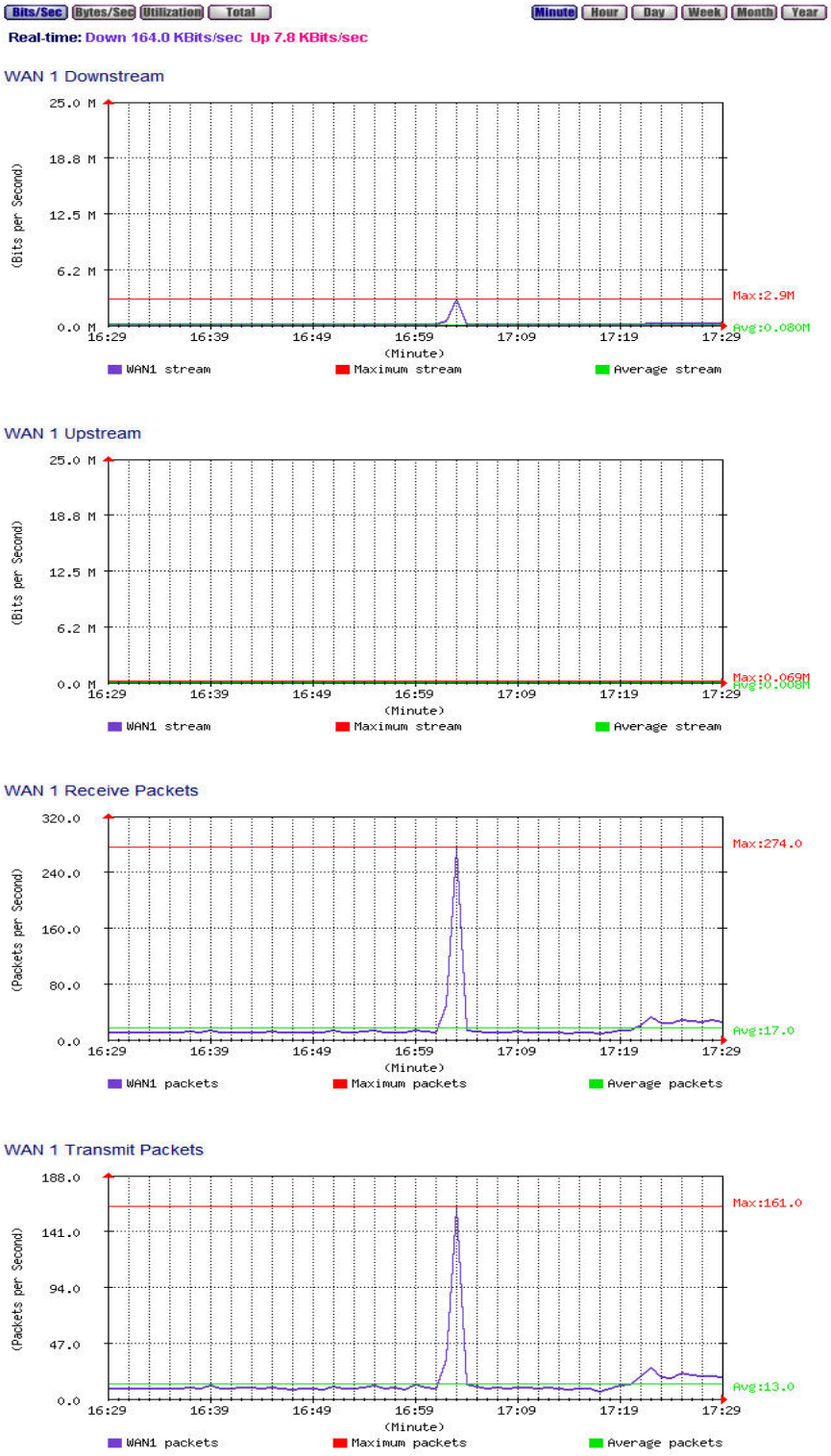


Figure23-2 To Detect WAN Statistics

Policy Statistics

STEP 1 . If you had select **Statistics** in **Policy**, it will start to record the chart of that policy in **Policy Statistics**. (Figure23-3)

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY		Minute Hour Day Week Month Year
Outside_Any	192.168.0.39	FTP(21)		Minute Hour Day Week Month Year

Figure23-3 Policy Statistics Function

If you are going to use **Policy Statistics** function, the System Manager has to enable the **Statistics** in **Policy** first.

STEP 2 . In the **Statistics** WebUI, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics chart every minute; click **Hour** to check the Statistics chart every hour; click **Day** to check the Statistics chart every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

STEP 3 . Statistics Chart (Figure23-4)

- **Y-Coordinate**：Network Traffic（Kbytes/Sec）
- **X-Coordinate**：Time（Hour/Minute/Day）

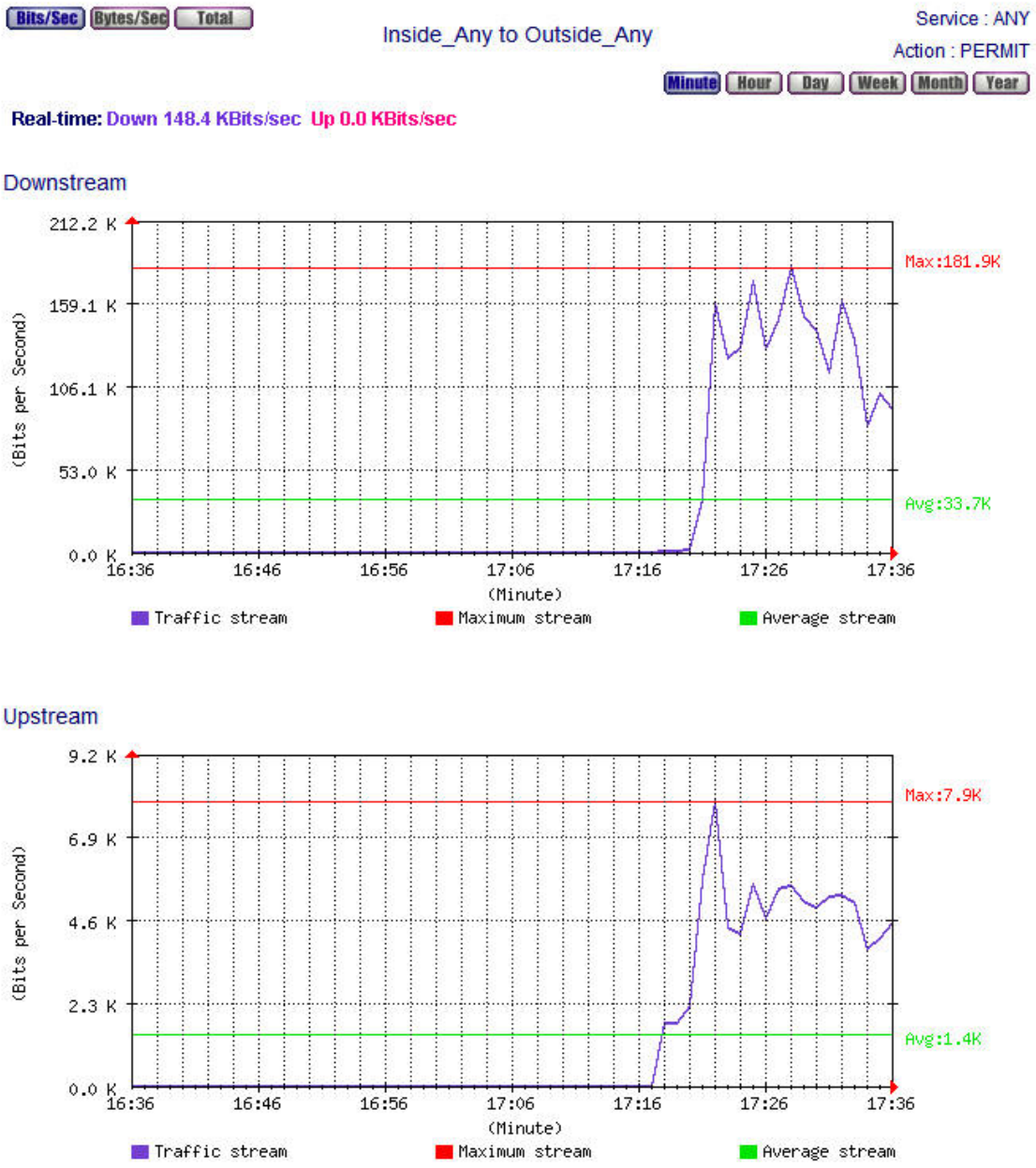


Figure23-4 To Detect Policy Statistics

Chapter 24 Diagnostic

User can realize RS-3000 WAN connecting status by using **Ping** or **Traceroute** tool.

24.1 Ping

STEP 1． In **Diagnostic → Ping** function, user can configure RS-3000 to ping specific IP address, and confirm RS-3000 WAN connecting status. (Figure24-1)

- Type in available Internet IP address or domain name
- Choose the Ping **Packets size** (32 Bytes by default)
- Type in the **Count** value (the default setting is 4)
- Type in the "**Wait Time**" (the default setting is 1 second)
- Choose the source interface to send out the Ping packets
- Press "OK" to ping the IP address or domain name (Figure24-2)

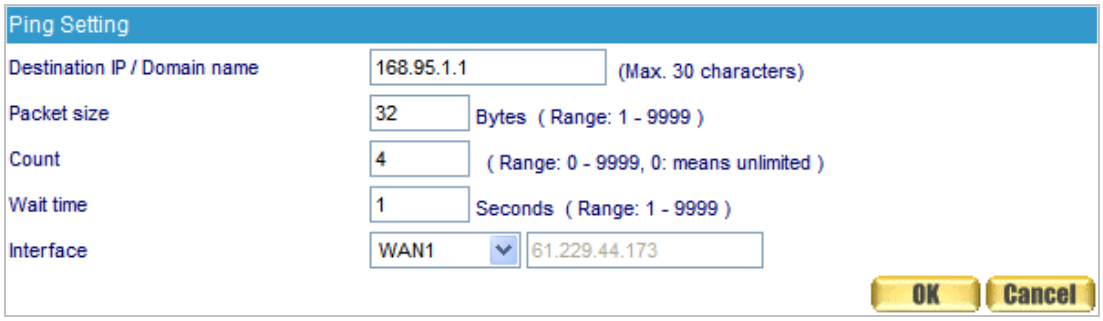


Figure 24-1 Ping Diagnostic

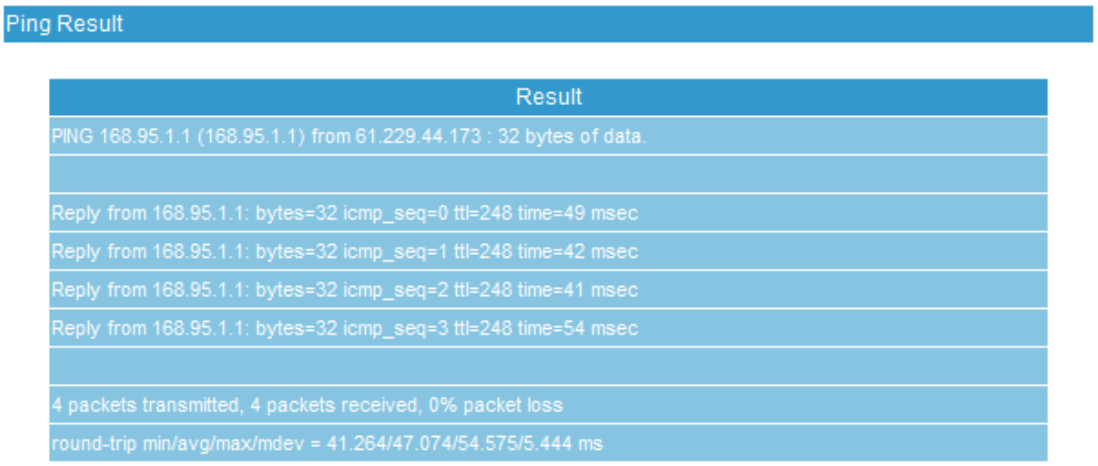


Figure 24-2 Ping Result

If **Interface** is selected "**VPN**", it must be typed in with RS-3000 LAN IP address, and type in remote VPN site of LAN IP address in **Destination IP / Domain name**. (Figure 24-3)

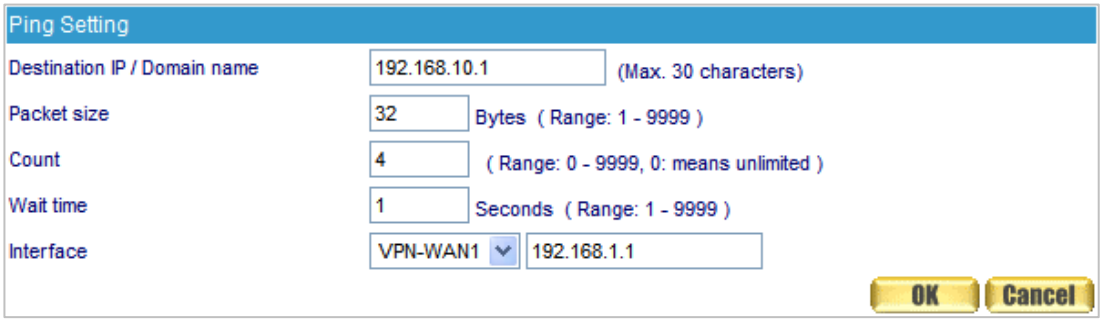


Figure 24-3 Ping configuration via VPN

24.2 Traceroute

STEP 1 . In **Diagnostic → Traceroute** function, user can configure RS-3000 to trace specific IP address or domain name, and confirm RS-3000 WAN connecting status. (Figure24-4)

- Type in available Internet IP address or domain name
- Choose the Ping **Packets size** (40 Bytes by default)
- Type in the **Max Time-to-Live** value (30 Hops by default)
- Type in the "**Wait Time**" (the default setting is 2 seconds)
- Choose the source interface to send out the Ping packets
- Press "OK" to ping the IP address or domain name (Figure24-5)

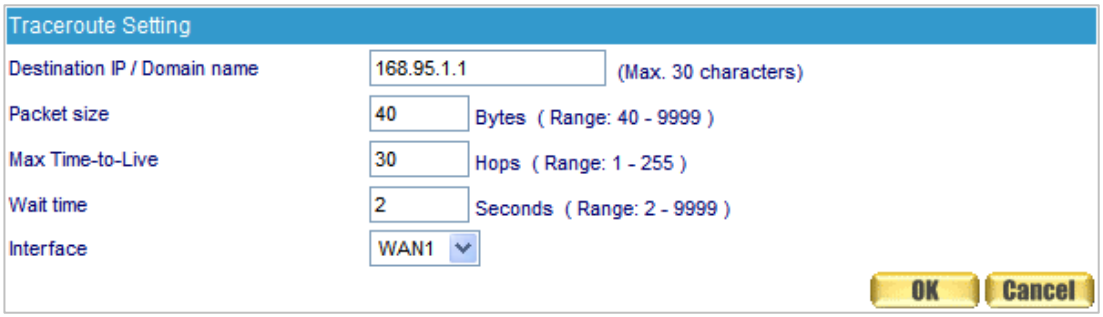


Figure 24-4 Traceroute Diagnostic

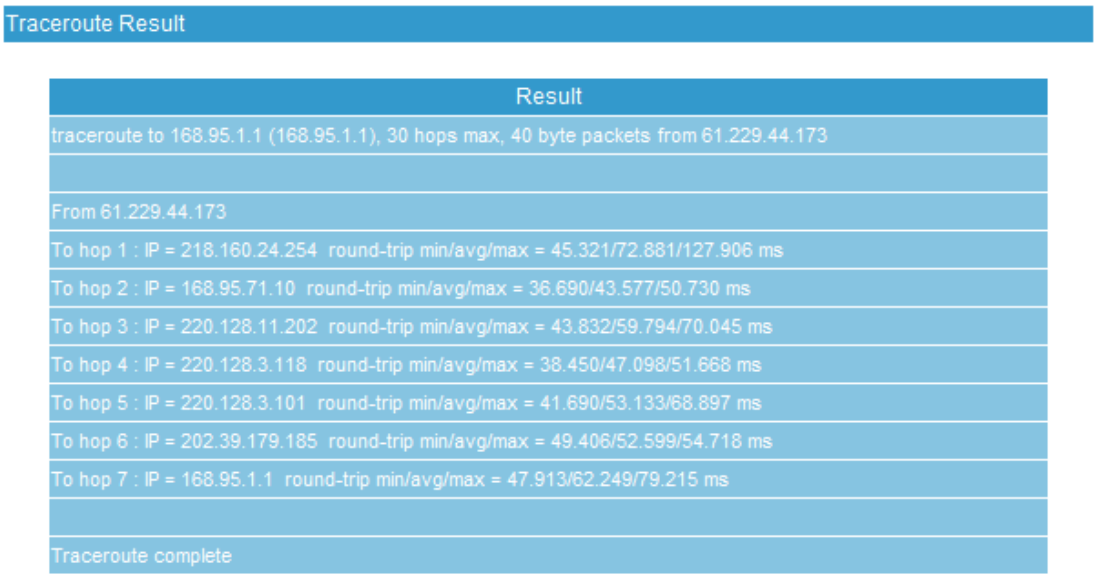


Figure 24-5 Traceroute result

Chapter 25 Wake on Lan

Wake on Lan (WOL) function works to power on the computer remotely. The computer's network card must also support WOL function, when it receive the waked up packets and the computer will auto boot up.

Normally the broadcast packets are not allowed to transfer within Internet, but user can login RS-3000 remotely and enable Wake on Lan function to boot up the LAN computer.

To configure Wake on Lan function in RS-3000

STEP 1. Select **Setting** in **Wake on Lan**, and enter MAC Address to specify the computer who needs to be booted up remotely. User can press **Assist** to obtain the MAC Address from the table list. (Figure25-1)

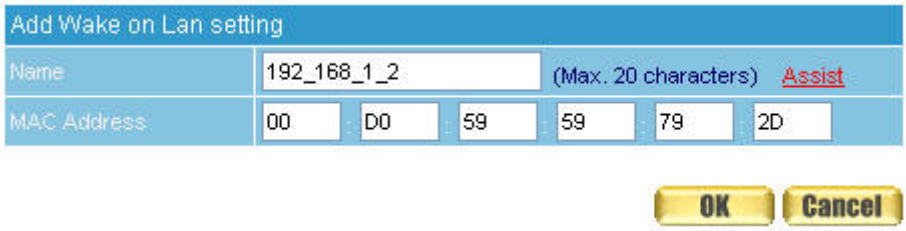


Figure 25-1 Wake on Lan Setting

STEP 2. User only needs to press **Wake Up** button to boot up the specific LAN computer. (Figure 25-2)

Figure 25-2 Complete Wake on Lan Setting

Chapter 26 Status

The users can know the connection status in Status. For example: LAN IP, WAN IP, Subnet Netmask, Default Gateway, DNS Server Connection,
and its IP…etc.

- **Interface:** Display all of the current Interface status of the RS-3000
- **Authentication:** The Authentication information of RS-3000
- **ARP Table:** Record all the ARP that connect to the RS-3000
- **DHCP Clients:** Display the table of DHCP clients that are connected to the RS-3000.

Interface

STEP 1． Enter **Interface** in **Status** function; it will list the setting for each Interface: (Figure 26-1)

- **Forwarding Mode:** The connection mode of the Interface
- **WAN Connection:** To display the connection status of WAN
- **Max. Downstream / Upstream Kbps:** To display the Maximum Downstream/Upstream Bandwidth of that WAN (set from **Interface**)
- **Downstream Alloca.:** The distribution percentage of Downstream according to WAN traffic
- **Upstream Alloca.:** The distribution percentage of Upstream according to WAN traffic
- **PPPoE Con. Time:** The last time of the RS-3000 to be enabled
- **MAC Address:** The MAC Address of the Interface
- **IP Address/ Netmask:** The IP Address and its Netmask of the Interface
- **Default Gateway:** To display the Gateway of WAN
- **DNS1/2:** The DNS1/2 Server Address provided by ISP
- **Rx/Tx Pkts, Error Pkts:** To display the received/sending packets and error packets of the Interface
- **Ping, HTTP:** To display whether the users can Ping to the RS-3000 from the Interface or not; or enter its WebUI

Active Sessions Number : 22 System Uptime : 0 Day 0 Hour 18 Min 17 Sec

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Dynamic IP	Static IP	---
WAN Connection	---			---
Max. Downstream / Upstream	---	25600 / 25600 Kbps	25600 / 25600 Kbps	---
Downstream Alloca.	---	75%	24%	---
Upstream Alloca.	---	73%	26%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:4f:68:00:0a:ab	00:4f:68:00:0a:aa	00:4f:68:00:0a:a9	00:4f:68:00:0a:ac
IP Address	192.168.1.1	192.168.0.30	61.11.11.12	0.0.0.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	---	192.168.0.254	61.11.11.11	---
DNS1	---	168.95.192.1	168.95.192.1	---
DNS2	---	168.95.1.1	168.95.1.1	---
Rx Pkts, Error Pkts	580, 0	246, 0	245, 0	0, 0
Tx Pkts, Error Pkts	546, 0	102, 0	45, 0	0, 0
Ping			---	---
HTTP			---	---

Figure 26-1 Interface Status

Authentication

STEP 1. Enter **Authentication** in **Status** function; it will display the record of login status: (Figure 26-2)

- **IP Address:** The authentication user IP
- **Auth-User Name:** The account of the auth-user to login
- **Login Time:** The login time of the user (Year/Month/Day Hour/Minute/Second)

Figure 26-2 Authentication Status WebUI

ARP Table

STEP 1 . Enter **ARP Table** in **Status** function; it will display a table about IP Address, MAC Address, and the Interface information which is connecting to the RS-3000: (Figure26-3)

- **Anti-ARP virus software:** Works to rewrite LAN ARP table as default
- **IP Address:** The IP Address of the network
- **MAC Address:** The identified number of the network card
- **Interface:** The Interface of the computer

Figure 26-3 ARP Table WebUI

DHCP Clients

STEP 1.In **DHCP Clients** of **Status** function, it will display the table of DHCP Clients that are connected to the RS-3000: (Figure26-4)

- **IP Address:** The dynamic IP that provided by DHCP Server
- **MAC Address:** The IP that corresponds to the dynamic IP
- **Leased Time:** The valid time of the dynamic IP (Start/End) (Year/Month/Day/Hour/Minute/Second)

IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.2	00:d0:59:59:79:2d	2007/3/30 16:36:37	2007/3/31 16:36:37

Figure 26-4 DHCP Clients WebUI

Chapter 27 Specification

Hardware			
CPU			Intel IXP 425, 533MHz
DRAM			128 MB
Flash ROM			16MB (Flash)
Console port	RS232 Serial Port		○
LAN port (Switch Hub)	Shield RJ-45 Ethernet UTP port		1 (10/100)
	Modify the MAC address		○
WAN port	Shield RJ-45 Ethernet UTP port		2 (10/100)
	Support xDSL/Cable/Leased Line Service		○
	Modify the MAC address		○
DMZ port	Shield RJ-45 Ethernet UTP port		1 (10/100)
	Modify the MAC address		○
Dimensions	W x D x H (cm)		44x23.7x4.3
Size			Rack Mount
Weight	Kgs		2.75
Power			100~250 VAC / 80W
Performance			
Throughput	WAN-LAN / Zone 1-Zone 2 / Port 1-Port 2		100 Mbps
	VPN	DES Encryption	18 Mbps
		3DES Encryption	16 Mbps
	Anti-Virus	HTTP	12Mbps
		FTP	20Mbps
	IDP		10 Mbps
Max Concurrent Sessions			110,000
New Sessions / Second			10,000
Email Capacity Per Day (Mail Size 1098 bytes)			120,000
Corporation Size			SMB (clients 50~80)
Unlimited User			○
Mail Security Function			
Scanned Mail Settings	The allowed size of scanned mail		10-512 (KBytes)
	Add the message to the subject line of unscanned mail		○

Mail Relay	Max entry		50
	Internal Mail Server		○
	Allowed External IP		○
Anti-Spam	Setting	Inbound Scanning for Internal Mail Server	○ (LAN & DMZ)
		Inbound Scanning for External Mail Server	○
		Score Tag	○
		Spam Fingerprint	○
		Bayesian Filtering	○
		Check sender address in RBL	○
		Check sender account	○
		Spam signature	○
	Action of Spam Mail	Delete spam mail	○
		Deliver to the recipient	○
		Forward mail	○
	Global Rule	Max entry	100
		Auto-Training	○
	Whitelist	Export & Import Whitelist	○
		Max entry	128
		Auto-Training	○
	Blacklist	Export & Import Blacklist	○
		Max entry	128
		Auto-Training	○
	Spam Training	Export & Import Training Database	○
		Spam Mail for Training	○
		Ham Mail for Training	○
		Spam Account for Training	○
		Ham Account for Training	○
Mail Anti-Virus	Anti-Virus Setting	Virus Scanner	Clam
		Auto Update Virus Definitions	10 min
		Inbound Scanning for Internal Mail Server	○ (LAN & DMZ)
		Inbound Scanning for External Mail Server	○
	Action of Infected Mail	Delete infected mail	○
		Deliver a notification mail instead of the original virus mail	○

		Deliver the original virus mail	○
		Forward mail	○
Security Function			
Anti-Virus	Policy	HTTP	○
		FTP	○
	P2P, IM, NetBIOS… (IDP)		○
IDP	Auto Update IDP Definitions		30 min
	Anomaly		○
	Total IDP Signatures Number (2006/01/18)		716
	Custom (Max entry)		256
	IDP Log	Log	○
	Blaster Alarm	Enable Blaster Blocking	○
		E-Mail / NetBIOS Alert Notification	○/○
	Un-detected IP		○
Static ARP			○
Management			
Web Based UI	Traditional Chinese , Simplified Chinese and English Web UI		○
Web Management	HTTP		○
Firmware Upgrade	From LAN & WAN (Web UI)		○
Sub-Administrator	Max entry		10
Remote management	Remote Monitor		○
	Web Management (Port Number) can be changeable		○
	Permitted IPs（Max entry）		32
	Web UI Logout		○
	MTU changeable for WAN		○
Interface Statistics			○
Traffic Statistics	WAN / Policy		○
Multiple Subnet (NAT)	Routing / NAT (Max entry)		○ / ○ (16)
Configuration	Route Table（Max entry）		10
	Dynamic Routing (RIPv2)		○
	Host Table（Max entry）		20

	DDNS（Max entry）		16
	Save configuration to files		○
	Load configuration from files		○
	Load Default (Factory Reset)		○
Protocols Supported	DHCP Client / Server		○ (LAN)
	DHCP Server assign dynamic IP		Up to 512
	DHCP Server assign static IP (MAC+IP)		○
	NTP (Network Time Protocol)		○
Wake on Lan			○
Bandwidth Manager Function			
QoS	Guaranteed Bandwidth		○
	Priority-bandwidth utilization		○
	QoS（Max entry）		100
	Max. Bandwidth (MB)		50
	Personal QoS		○
Accounting Report	Ranking by IP / Port		○
Authentication	Authentication User（Max entry）		200
	Authentication Group（Max entry）		50
	RADIUS		○
	POP3		○
	Authentication Status	URL to redirect	○
		Messages to display	○
		Disable re-login	○
Inbound / Outbound Function			
Load-balancing	OutBound	Auto(AI) Mode,By Session,By Packet, Round-Robin,Auto Backup, By Secure IP, By Destination IP	○
WAN Port connection status	ICMP		○
	DNS		○
Firewall Function			
Deployment	NAT		○
	Transparent Mode (Enable / Disable)		○
Address Book	Internal	Max entry	200
	Internal Group（Max entry）		20
	External（Max entry）		100

	External Group	China Telecom & CNC	○
		Max entry	20
	DMZ	Max entry	100
	DMZ Group（Max entry）		20
Service Book	Custom（Max entry）		20
	Group（Max entry）		20
Schedule（Max entry）			20
Virtual Server	Mapped IP（Max entry）		16
	Multiple Virtual Servers		4
	Virtual Server Service Name （Max entry）		16
	Multi-Servers Load Balancing		4
Policy Control	SPI (Stateful Packet Inspection)		○
	MAC Address Filtering		○
	Assign WAN Link by Source IP		○
	Assign WAN Link by Destination IP		○
	Assign WAN Link by Port		○
	Packet Filtering by Source IP		○
	Packet Filtering by Destination IP		○
	Packet Filtering by Port		○
	Access control by group		○
	Time-Schedule Management		○
	Max. Concurrent Sessions		○
	Incoming NAT mode & External To DMZ NAT mode		○
	Outgoing（Max entry）		200
	Incoming（Max entry）		50
	LAN To DMZ（Max entry）		20
	WAN To DMZ（Max entry）		50
	DMZ To LAN（Max entry）		20
	DMZ To WAN（Max entry）		20
	Tips		○
Content Filtering	URL Blocking（Max entry）		300
	Script Blocking (Java / ActiveX / Cookie / Popup)		○
	Download Blocking	All Types Block	○
		Audio and Video Types Block	○
		Extensions Block (exe, zip, rar, iso, bin, rpm, doc, xl?, ppt, pdf, tgz, gz, bat, com, dll, hta, scr, vb?, wps, pif, com, msi, reg, mp3, mpeg, mpg)	○

	Upload Blocking	All Types Block	○
		Extensions Block (exe,zip,rar,iso,bin,rpm,doc,xl?,ppt,pdf,tgz,gz,bat,com,dll,hta,scr,vb?,wps,pif,com,msi,reg,mp3,mpeg,mpg)	○
IM / P2P Blocking	Auto Update Definitions		30 min
	P2P Blocking	eDonkey	○
		BT	○
		WinMX	○
		Foxy	○
		KuGoo	○
		AppleJuice	○
		AudioGalaxy	○
		DirectConnect	○
		iMesh	○
		MUTE	○
		Thunder5	○
		VNN Client	○
	IM Blocking	MSN Messenger	○
		Yahoo Messenger	○
		ICQ	○
		QQ	○
		Skype VoIP	○
		Google Talk	○
		Gadu-Gadu	○
	IM / P2P Rule		○
Drop Intruding Packets			○
Log	Traffic Log / Event Log / Connection Log		○/○/○
	Log Backup	Syslog Settings	○
		E-mail alert when WAN link failure	○
H/W Watch-Dog	Auto rebooting when detecting system fails		○
VPN Function			
One-Step IPSec			○
IPSec Autokey	IPSec Dead Peer Detection		○
	Show remote Network Neighborhood		○
	IKE, SHA-1, MD5 Authentication		○
	Auto Key management via IKE/ISAKMP		○

Allow to Configure / Connection Tunnels	IPSec（Max entry）	200 / 100
	PPTP Server（Max entry）	32 / 32
	PPTP Client（Max entry）	16 / 16
Stateful Packet Inspection		○
Supports Windows VPN Client		○
VPN Hub		○
VPN Trunk（Max entry）		50

Chapter 28 Network Glossary

The network glossary contains explanation or information about common terms used in networking products. Some of information in this glossary might be outdated, please use with caution.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

100Base-TX

Also known as 802.3u. The IEEE standard defines how to transmit Fast Ethernet 100Mbps data using Cat.5 UTP/STP cable. The 100Base-TX standard is backward compatible with the 10Mbps 10-BaseT standard.

WAN

Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area.

LAN

Local Area Network. It is a computer network covering a small physical area or small group of buildings.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device.

PPPoE

Point-to-Point over Ethernet. PPPoE relies on two widely accepted standards; PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as single DSL line, wireless device or cable modem.

Transparent

Transparent mode works to transfer real IP address from WAN interface to the device that connects to DMZ port. So the DMZ device can also get real IP address and offer the service with Internet users.

NAT

Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

DHCP

Dynamic Host Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as router.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection or Internet servers.

DDNS

Dynamic Domain Name System. An Algorithm that allows the use of dynamic IP address for hosting Internet Server. DDNS service provides each user account with a domain name. Router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, switch or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

IP Address

IP (Internet Protocol) is a layrer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

MAC

Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC

address can connect with the network.

TCP

A layre-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

UDP

User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

QoS (Bandwidth Management)

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function. For switch's bandwidth management, please see "Rate Control".

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. RADIUS typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Wake on Lan

Wake on Lan (WOL) function works to power on the computer remotely. The computer’s network card must also support WOL function, when it receive the waked up packets and the computer will auto boot up.

VPN

Virtual Private Network. A type of technology designed to increase the security of information over the Internet. VPN creates a private encrypted tunnel from the end user’s computer, through the local wireless network, through the Internet, all the way to the corporate network.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec

supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preshare Key

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

ISAKMP (Internet Security Association Key Management Protocol)

An extensible protocol-encoding scheme that complies to the Internet Key Exchange (IKE) framework for establishment of Security Associations (SAs).

AH (Authentication Header)

One of the IPSec standards that allows for data integrity of data packets.

ESP (Encapsulating Security Payload)

One of the IPSec standards that provides for the confidentiality of data packets.

DES (Data Encryption Standard)

The Data Encryption Standard developed by IBM in 1977 is a 64-bit block encryption block cipher using a 56-bit key.

Triple-DES (3DES)

The DES function performed three times with either two or three cryptographic keys.

AES (Advanced Encryption Standard)

An encryption algorithm yet to be decided that will be used to replace the aging DES encryption algorithm and that the NIST hopes will last for the next 20 to 30 years.

NULL Algorithm

It is a fast and convenient connecting mode to make sure its privacy and authentication without

encryption. NULL Algorithm doesn’t provide any other safety services but a way to substitute ESP Encryption.

SHA-1 (Secure Hash Algorithm-1)

A message-digest hash algorithm that takes a message less than 264 bits and produces a 160-bit digest.

MD5

MD5 is a common message digests algorithm that produces a 128-bit message digest from an arbitrary length input, developed by Ron Rivest.

Main Mode

This is another first phase of the Oakley protocol in establishing a security association, but instead of using three packets like in aggressive mode, it uses six packets.

Aggressive mode

This is the first phase of the Oakley protocol in establishing a security association using three data packets.

GRE/IPSec

The device Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology.

Sasser

Sasser is a computer worm that affects computers running vulnerable versions of the Microsoft operating systems Windows XP and Windows 2000. Sasser spreads by exploiting the system through a vulnerable network port (as do certain other worms). Thus it is particularly virulent in that it can spread without user intervention, but it is also easily stopped by a properly configured firewall or by downloading system updates from Windows Update.

MSBlaster

The Blaster Worm (also known as Lovsan or Lovesan) was a computer worm that spread on computers running the Microsoft operating systems: Windows XP and Windows 2000.

Code Red

The **Code Red worm** was a computer worm observed on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS web server.

Nimda

Nimda is a computer worm, and is also a file infector. It quickly spread, eclipsing the economic damage caused by past outbreaks such as Code Red. Multiple propagation vectors allowed Nimda to become the Internet's most widespread virus/worm within 22 minutes.

SYN Flood

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system.

ICMP Flood

A smurf attack is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.

UDP Flood

A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.
Using UDP for denial-of-service attacks is not as straightforward as with the Transmission Control Protocol (TCP). However, a UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host.

Ping of Death

It is 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.

IP Spoofing

Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the firewall system and invade the network.

Port Scan

Hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.

Tear Drop

The Tear Drop attacks 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 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.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.