ALL7000

Load balancing Router with DMZ

User's Manual

Table of Contents

Chapter 1

Administration

“System” is the managing of settings such as the privileges of packets that pass through the ALL7000 and monitoring controls. The System Administrators can manage, monitor, and configure ALL7000 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 ALL7000.

Define the required fields of Administrator

Administrator Name:

- The username of Administrators and Sub Administrator for the ALL7000. The **admin** user name cannot be removed; and the sub-admin user can be removed or configure.

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

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 1-1) 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.

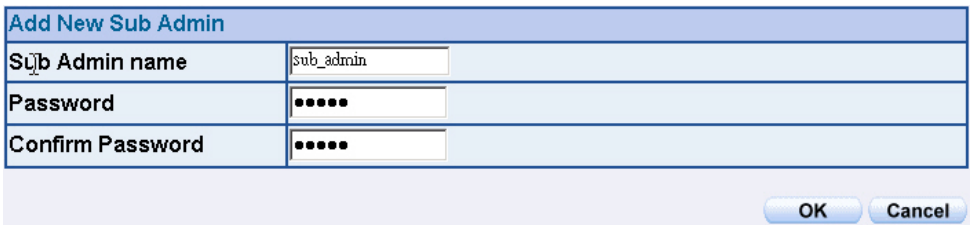


Figure1-1 Add New Sub Admin

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 (Figure1-2)

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

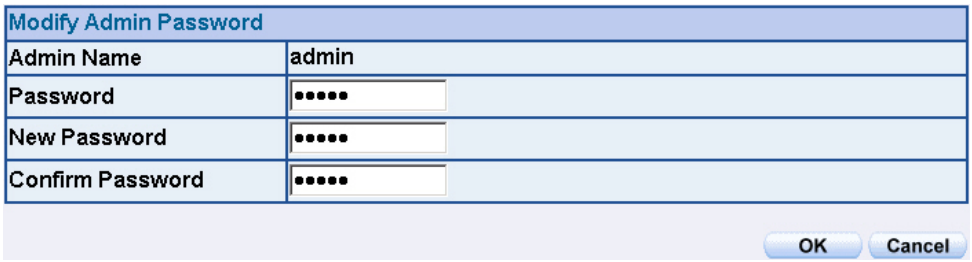


Figure1-2 Modify Admin Password

Add Permitted IPs

STEP 1 . Add the following setting in **Permitted IPs** of **Administration**: (Figure1-3)

- **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 (Figure1-4)

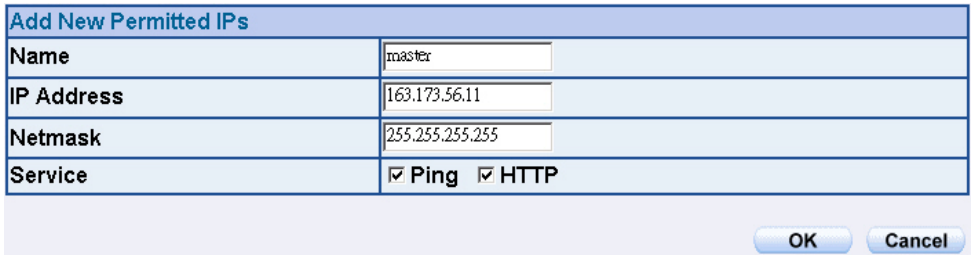


Figure1-3 Setting Permitted IPs WebUI

Figure1-4 Complete Add New Permitted IPs

To make Permitted IPs be effective, it must cancel the **Ping** and **WebUI** selection in the WebUI of ALL7000 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.

Logout

STEP 1． Click **Logout** in **System** to protect the system while Administrator are away. (Figure1-5)

Figure1-5 Confirm Logout WebUI

STEP 2． Click **OK** and the logout message will appear in WebUI. (Figure1-6)

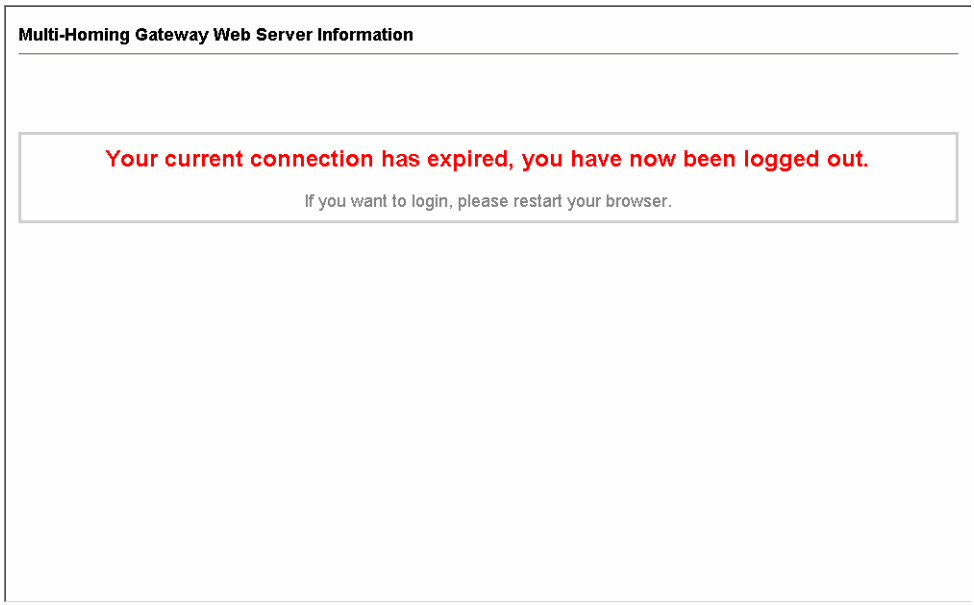


Figure1-6 Logout WebUI Message

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 ALL7000
- Click **Browse** and choose the latest software version file.
- Click **OK** and the system will update automatically. (Figure1-7)

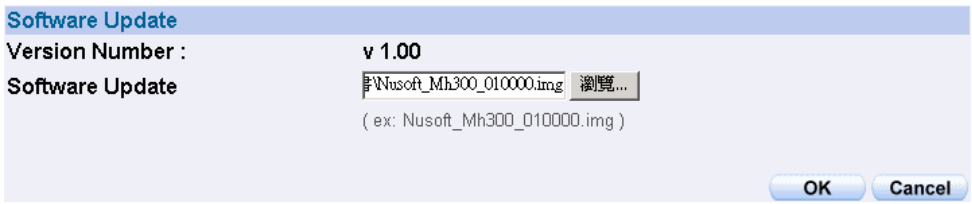


Figure1-7 Software Update

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 2

Configure

The Configure is according to the basic setting of the ALL7000. In this chapter the definition is Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Hosts Table, and Language settings.

Define the required fields of Settings

ALL7000 Configuration:

- The Administrator can import or export the system settings. Click **OK** to import the file into the ALL7000 or click **Cancel** to cancel importing. You also can revive to default value here.

Email Settings:

- Select **Enable E-mail Alert Notification** under E-mail Settings. This function will enable the ALL7000 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 Settings-Hacker Alert in System 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 want 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.

Administration Packet Logging:

- After enable this function; the ALL7000 will record packet which source IP or destination address is ALL7000. And record in Traffic Log for System Manager to inquire about.

Define the required fields of Time Settings

Synchronize Time/Date:

- Synchronizing the ALL7000 with the System Clock. The administrator can configure the ALL7000's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

GMT:

- International Standard Time (Greenwich Mean Time)

Define the required fields of Multiple Subnet

Forwarding Mode:

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

WAN Interface Address:

- The IP address that Multiple Subnet corresponds to WAN.

LAN Interface Address/Subnet Netmask:

- The Multiple Subnet range

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 R&D department, service, sales department, procurement department, 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)

Define the required fields of 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

Define the required fields of DDNS

Domain Name:

- The domain name that provided by DDNS

WAN IP Address:

- The WAN IP Address, which the domain name corresponds to.

Define the required fields of Host Table

Domain Name:

- It can be set by System Manager. To let the internal user to access to the information that provided by the host by this domain name

Virtual IP Address:

- The virtual IP address respective to Host Table. It must be LAN or DMZ IP address.

System Settings- Exporting

STEP 1． In System Setting WebUI, click on Download 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 ALL7000 will copy to the appointed site instantly. (Figure2-1)

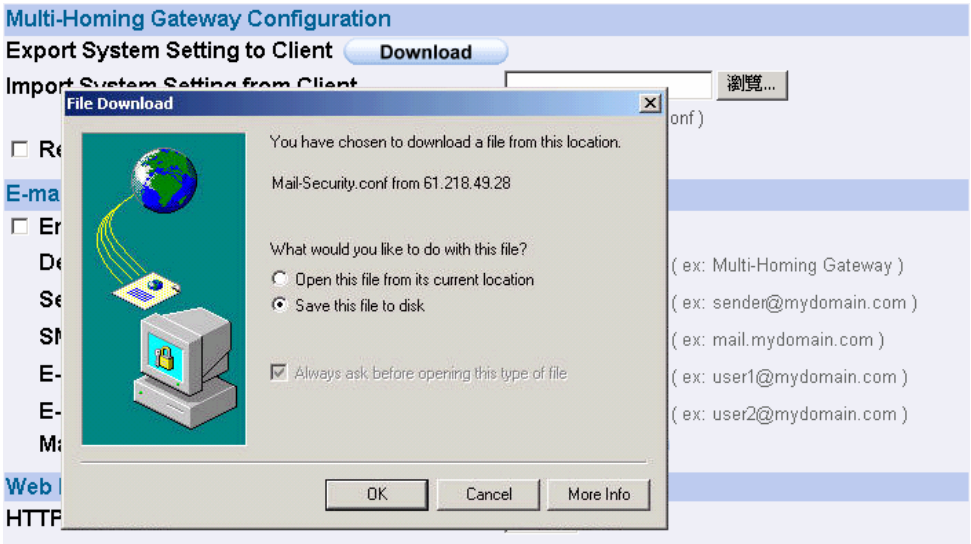


Figure2-1 Select the Destination Place to Save the Exported File

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 ALL7000 Settings, then click **OK**. (Figure2-2)

STEP 2． Click **OK** to import the file into the ALL7000 (Figure2-3)

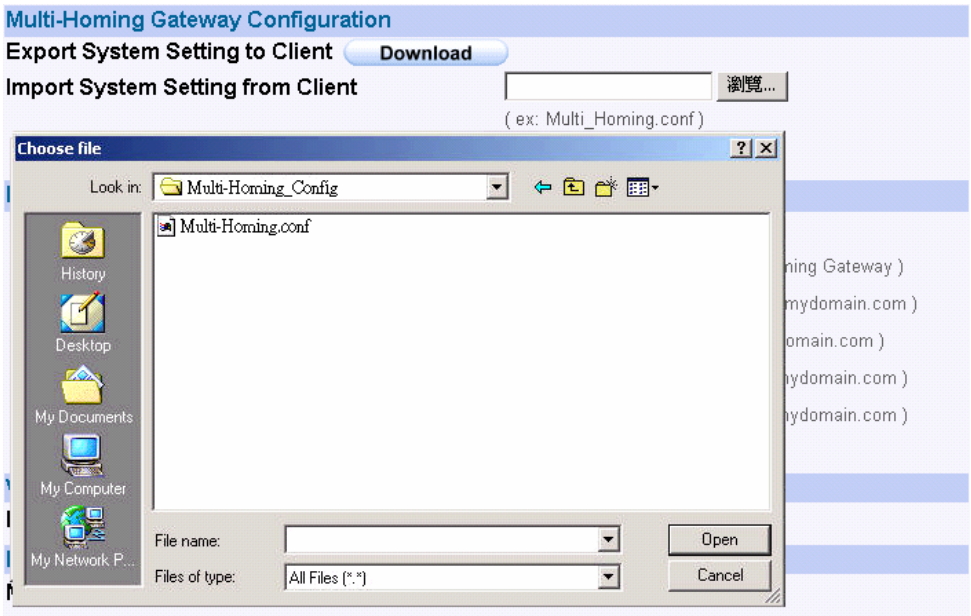


Figure 2-2 Enter the File Name and Destination of the Imported File

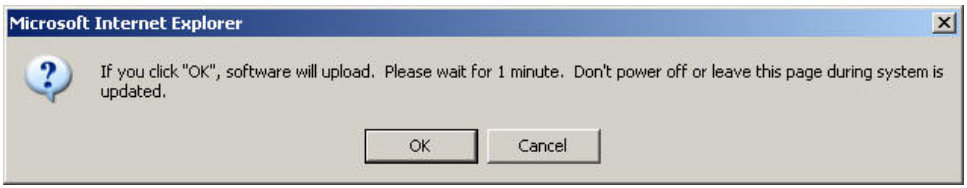


Figure 2-3 Upload the Setting File WebUI

Restoring Factory Default Settings

STEP 1．Select **Reset Factory Settings** in ALL7000 **Configuration** WebUI

STEP 2．Click **OK** at the bottom-right of the page to restore the factory settings. (Figure2-4)

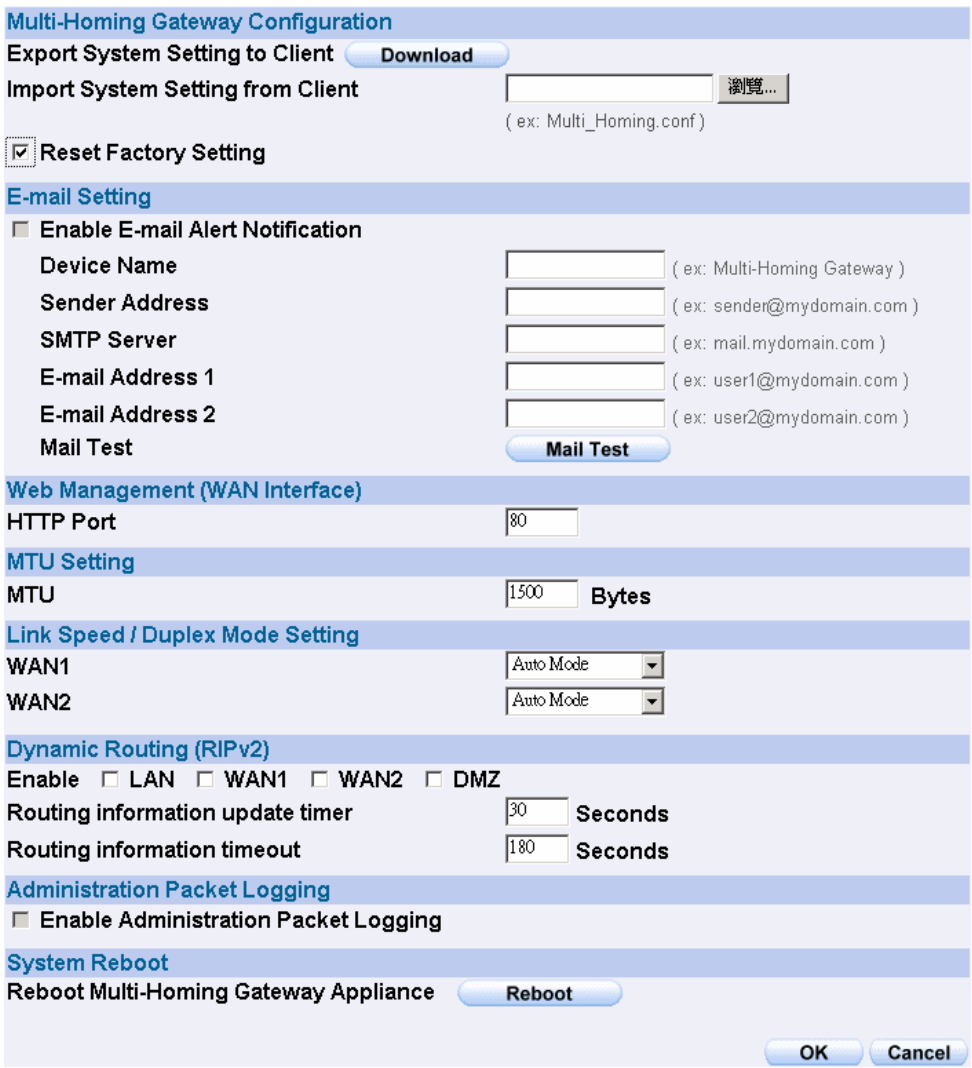


Figure2-4 Reset Factory Settings

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. (Figure2-5)

Figure2-5 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 ALL7000

STEP 1．Reboot ALL7000：Click **Reboot** button next to **Reboot ALL7000 Appliance.**

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

STEP 3．Follow the confirmation pop-up page; click **OK** to restart ALL7000. (Figure2-6)

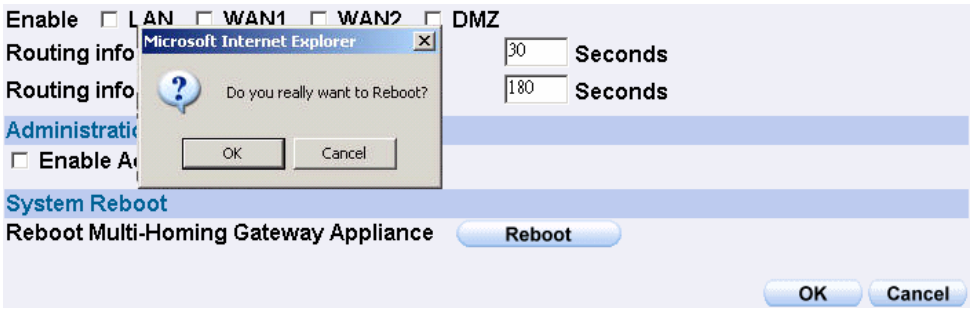


Figure2-6 Reboot ALL7000

Date/Time Settings

STEP 1．Select **Enable synchronize with an Internet time Server** (Figure2-7)

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

STEP 3．Enter the **Server IP / Name** with which you want to synchronize.

STEP 4．Set the interval time to synchronize with outside servers.

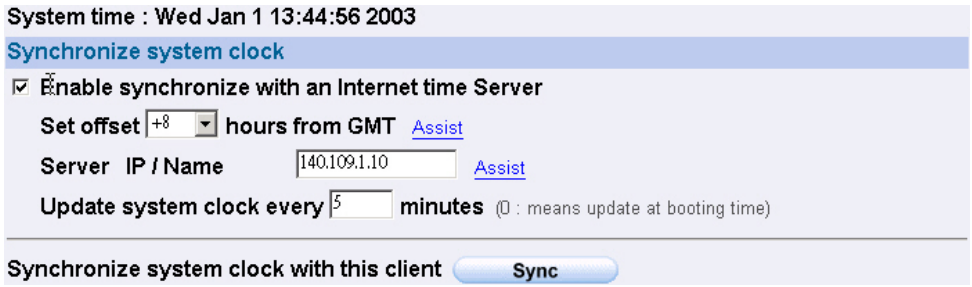


Figure2-7 System Time Setting

Click on the **Sync** button and then the ALL7000'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**.

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

Preparation

ALL7000 WAN1 (10.10.10.1) connect to the ISP Router (10.10.10.2) 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:** Enter Interface IP 10.10.10.1, and choose **Routing** in **Forwarding Mode**
- **WAN2**：Enter Interface IP 211.22.22.22, and choose **NAT** in **Forwarding Mode**
- Click **OK**
- Complete Adding Multiple Subnet (Figure2-8)

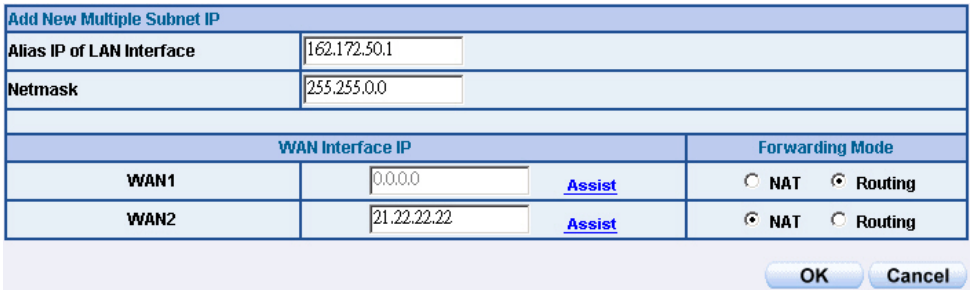


Figure 2-8 Add Multiple Subnet WebUI

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

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

˙192.168.1.xx, 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.xx, it uses Routing mode through WAN1 (The Internet Server can see your IP 162.172.50.xx directly). And uses NAT mode through WAN2 (The Internet Server can see your IP as WAN2 IP)(Figure2-9)

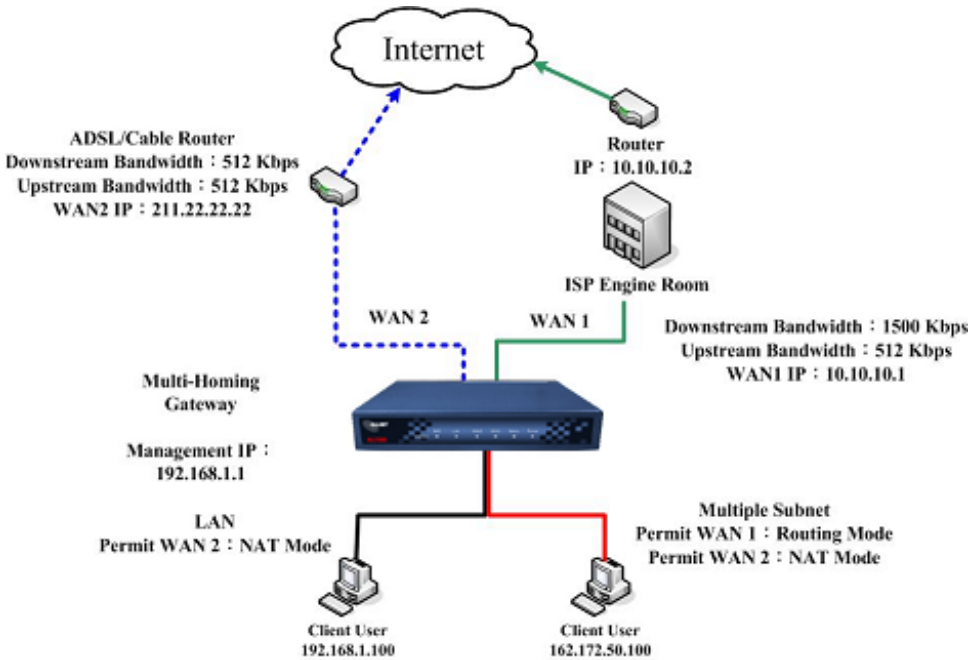


Figure 2-9 Multiple Subnet Network

- The ALL7000's Interface Status:
  WAN1 IP： 10.10.10.1
  WAN2 IP：211.22.22.22
  LAN Port IP：192.168.1.1
  LAN Port Multiple Subnet：162.172.50.1

Route Table

To connect two different subnet router with the ALL7000 and makes them to connect to Internet through ALL7000

Preparation

Company A: WAN1 (61.11.11.11) connects with ATUR to Internet

WAN2 (211.22.22.22) connects with ATUR to Internet

LAN subnet: 192.168.1.1/24

The Router1 which connect with LAN (10.10.10.1, support RIPv2) its LAN subnet is 192.168.10.1/24

Company B: Router2 (10.10.10.2, support RIPv2), its LAN subnet is 192.168.20.1/24

Company A ‘s Router1 (10.10.10.1) connect directly with Company B ‘s Router2 (10.10.10.2).

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 2-10)

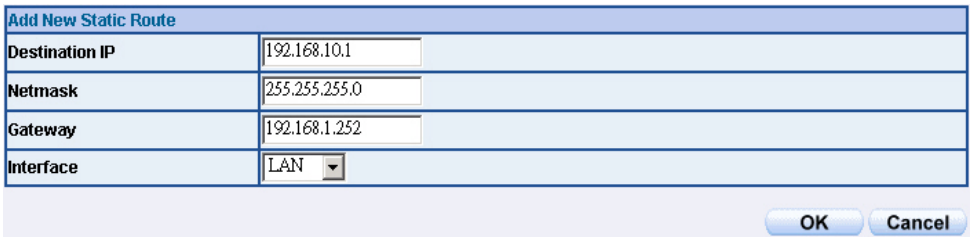


Figure2-10 Add New Static Route1

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 2-11)

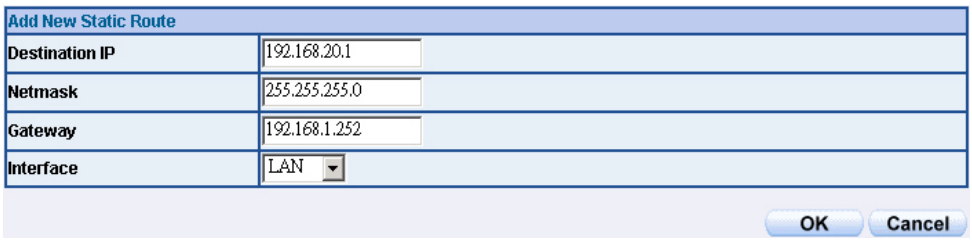


Figure2-11 Add New Static Route2

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 2-12)

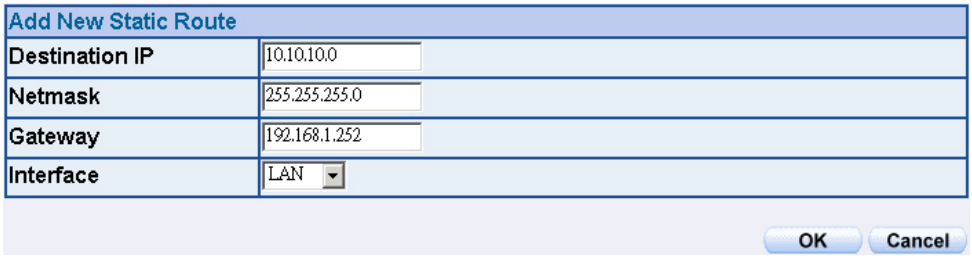


Figure2-12 Add New Static Route3

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 (Figure 2-13)

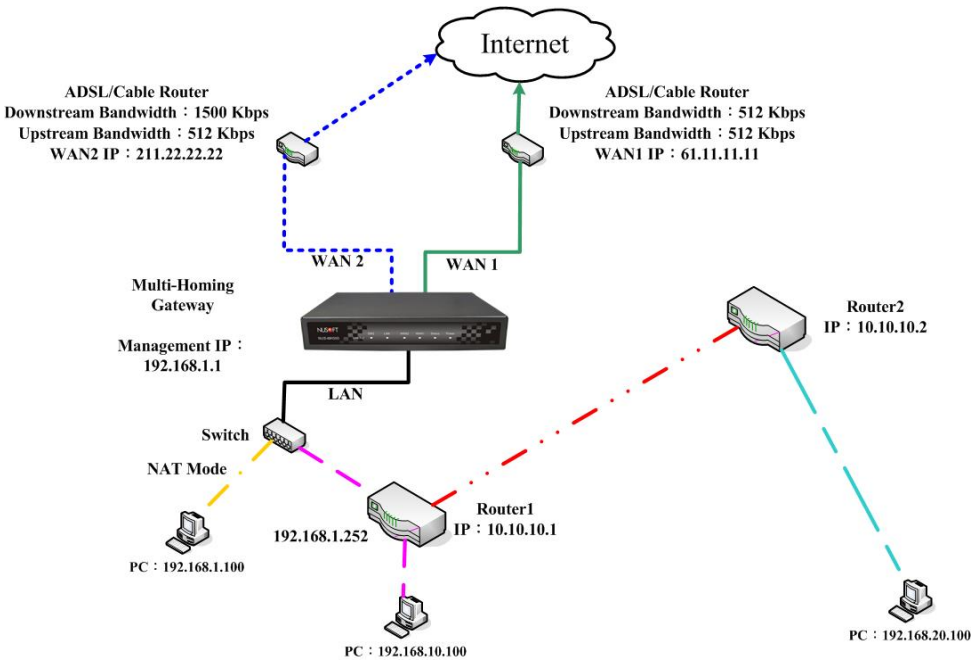


Figure 2-13 Route Table Setting

DHCP

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 in 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. (Figure2-14)

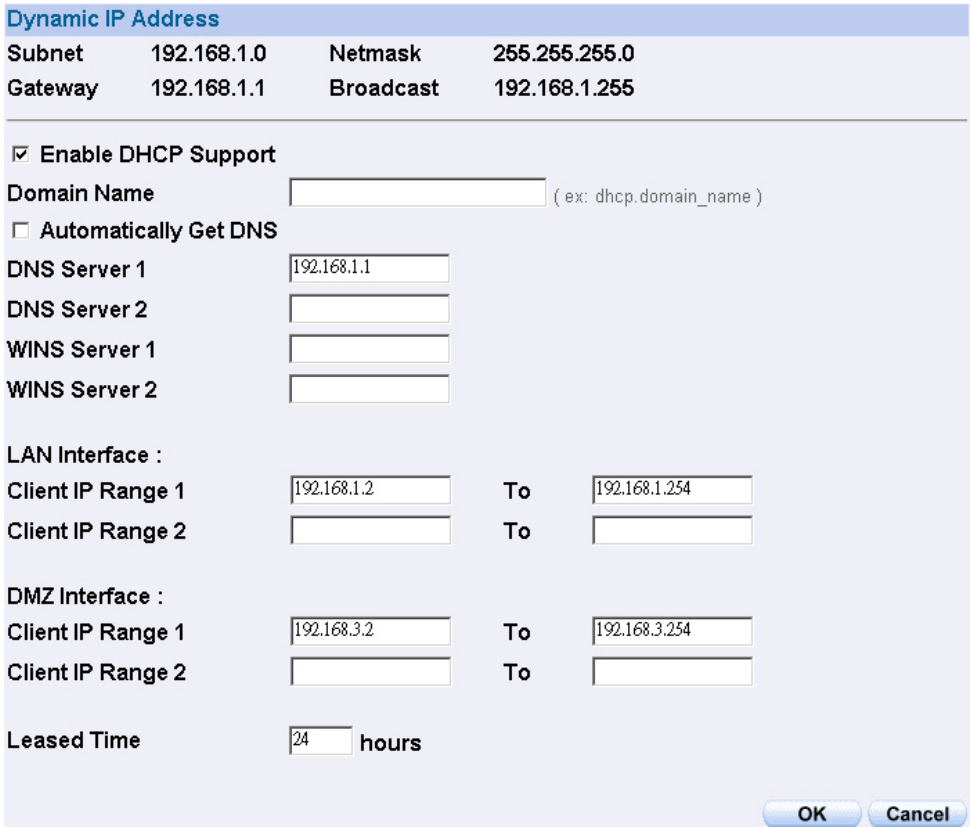


Figure 2-14 DHCP WebUI

When selecting **Automatically Get DNS**, the DNS Server will lock it 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)

Dynamic DNS Settings

STEP 1． Select **Dynamic DNS** in **System** function (Figure2-15). 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. (Figure2-16)

Figure2-15 DDNS WebUI

Figure 2-16 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**. Let DDNS to correspond to that specific IP address.

Host Table

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

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to Host Table
- Click **OK** to add Host Table. (Figure2-17)

Figure2-17 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 ALL7000. That is, the default gateway.

Language

Select the Language version (**English Version**/ **Traditional Chinese Version** or **Simplified Chinese Version**) and click **OK**. (Figure2-18)

Figure2-18 Language Setting WebUI

Chapter 3

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 ALL7000.

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 ALL7000 from Interface IP.

WAN:

- The System Administrator can set up the WAN network of ALL7000.

Balance Mode:

- **Auto:** The ALL7000 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 ALL7000 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 ALL7000 distributes the WAN 1/2 download bandwidth by accumulative traffic.
- **By Session:** The ALL7000 distributes the WAN 1/2 download bandwidth by saturated connections.
- **By Packet:** The ALL7000 distributes the WAN 1/2 download bandwidth by accumulated packets and saturated connection.

Connect Mode:

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

Saturated Connections:

- Set the number for saturation whenever session numbers reach it, the ALL7000 switches to the next agent on the list.

Priority:

- Set priority of WAN for Internet Access.

Connection Test:

- To test if the WAN network can connect to Internet or not. The testing ways are as following:
  - **ICMP**：To test if the connection is successful or not by the Ping IP you set.
  - **DNS**：To test if the connection is successful or not by checking Domain Name.

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 the amount of idle time before disconnection in the field. Enter “0” if you do not want the PPPoE connection to 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.

We set up four Interface Address examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	**LAN**	Modify LAN Interface Settings	**41**
Ex2	**WAN**	Setting WAN Interface Address	**42**
Ex3	**DMZ**	Setting DMZ Interface Address (NAT Mode)	**50**
Ex4	**DMZ**	Setting DMZ Interface Address (Transparent Mode)	**51**

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** (Figure3-1)

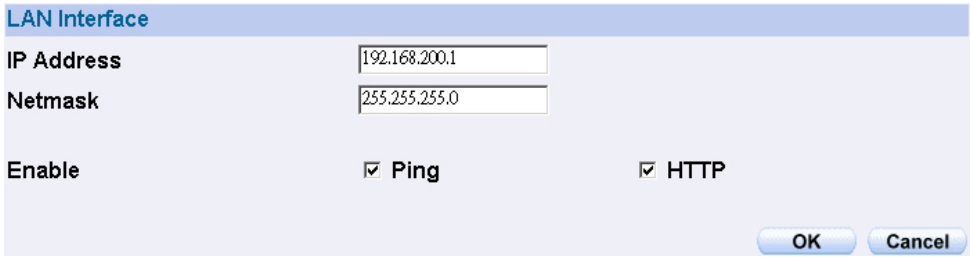


Figure3-1 Setting LAN Interface WebUI

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 ALL7000's WebUI from LAN.

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. (Figure3-2)

Figure3-2 Disable WAN2 Interface

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

- **ICMP**：Enter an Alive Indicator Site IP (can select from **Assist**) (Figure3-3)
- **DNS**：Enter DNS Server IP Address and Domain Name (can select from **Assist**) (Figure3-4)
- Setting time of seconds between sending alive packet.

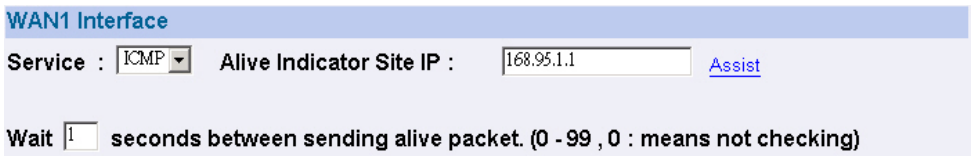


Figure3-3 ICMP Connection

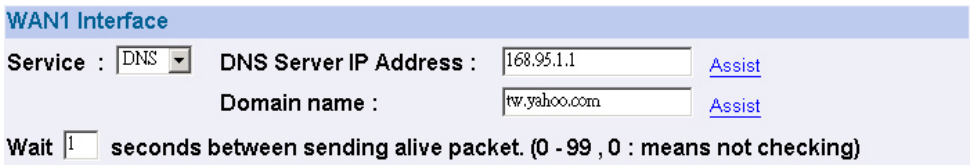


Figure 3-4 DNS Service

Connection test is used for ALL7000 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)** (Figure3-5):

  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** (Figure3-6)

Figure3-5 PPPoE Connection

Balance Mode : Auto

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	PPPoE	61.228.184.87	1	✔	✔	Modify	1
2	(Disable)	---	0	---	---	Modify	0

Figure3-6 Complete PPPoE Connection Setting

If the connection is PPPoE, you can choose **Service-On-Demand** for WAN Interface to connect automatically when disconnect; or to set up **Auto Disconnect if idle** (not recommend)

■ **Dynamic IP Address (Cable Modem User)** (Figure3-7)**:**

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 (like ISP in China)
7. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow that user apply)
8. Select **Ping** and **HTTP**
9. Click **OK** (Figure3-8)

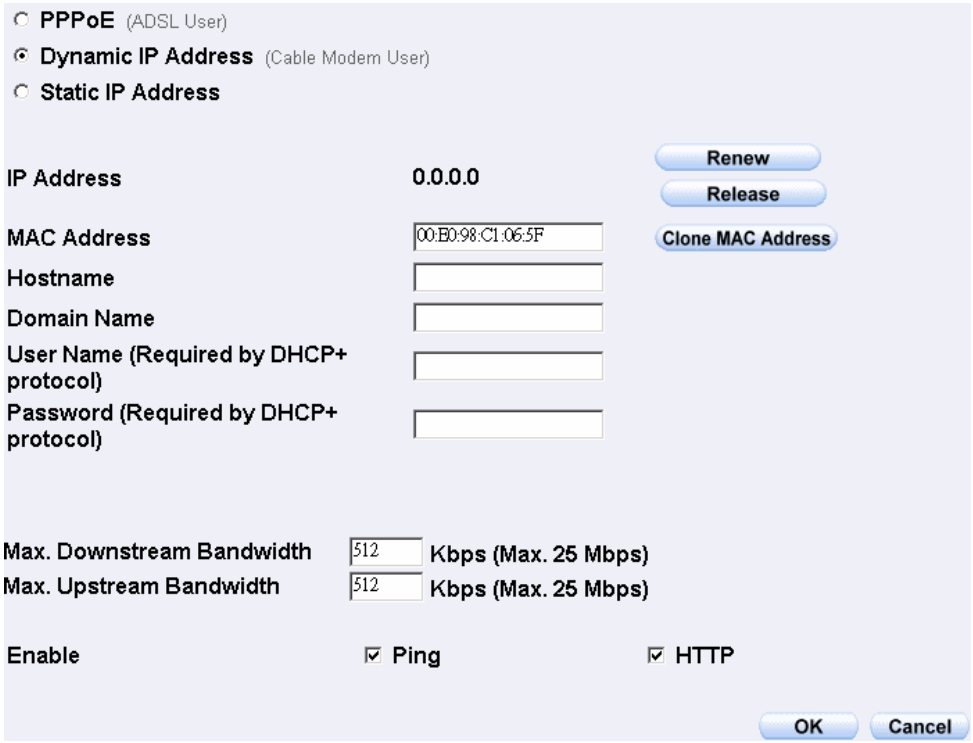


Figure3-7 Dynamic IP Address Connection

Balance Mode : Auto

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Dynamic IP	233.61.56.87	1	✔	✔	Modify	1
2	(Disable)	---	0	---	---	Modify	0

Figure3-8 Complete Dynamic IP Connection Setting

■ **Static IP Address** (Figure3-9)

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 that user apply)
5. Select **Ping** and **HTTP**
6. Click **OK** (Figure3-10)

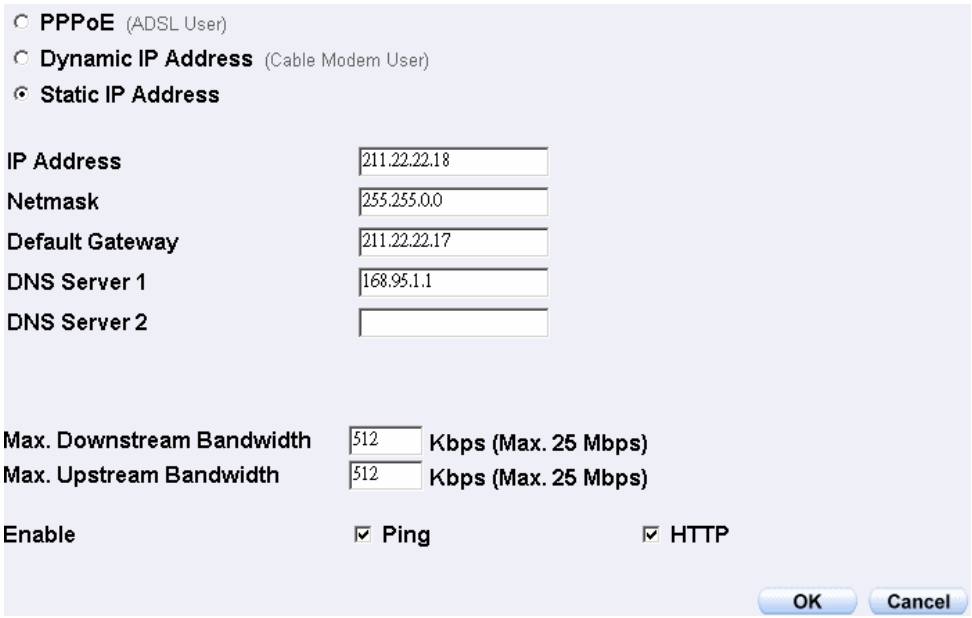


Figure3-9 Static IP Address Connection

Balance Mode : Auto

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Static IP	211.22.22.18	1	✓	✓	Modify	1
2	(Disable)	---	0	---	---	Modify	0

Figure3-10 Complete Static IP Address Connection Setting

When selecting **Ping** and **WebUI** on **WAN** network Interface, users will be able to ping the ALL7000 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.

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** (Figure3-11)

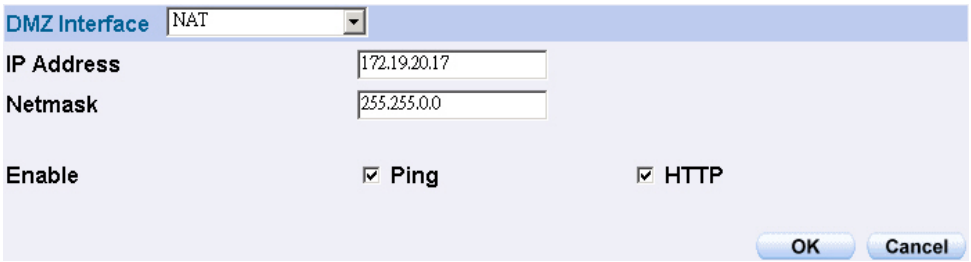


Figure3-11 Setting DMZ Interface Address (NAT Mode) WebUI

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 1．Select **Ping** and **HTTP**

STEP 2．Click **OK** (Figure3-12)

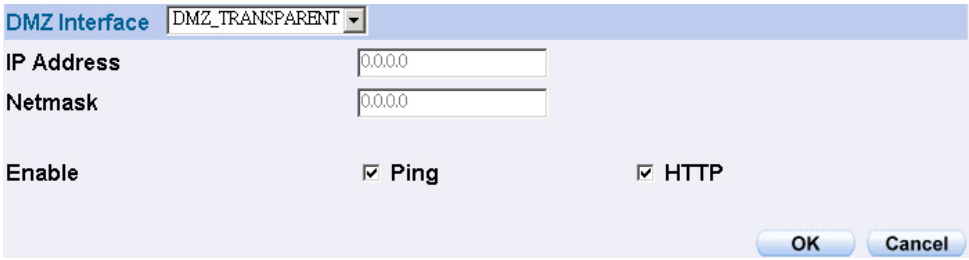


Figure 3-12 Setting DMZ Interface Address (Transparent Mode) WebUI

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

Chapter 4

Address

The ALL7000 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.

We set up two Address examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	**LAN**	Under DHCP circumstances, assign the specific IP to static users and restrict them to access FTP net service only through policy.	**55**
Ex2	**LAN Group WAN**	Set up a policy that only allows partial users to connect with specific IP (External Specific IP)	**58**

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 (Figure4-1)
- **Name:** Enter Rayearth
- **IP Address:** Enter 192.168.3.2
- **Netmask:** Enter 255.255.255.255
- **MAC Address :** Enter the user's MAC Address （00:B0:18:25:F5:89）
- Select **Get static IP address from DHCP Server**
- Click **OK** (Figure4-2)

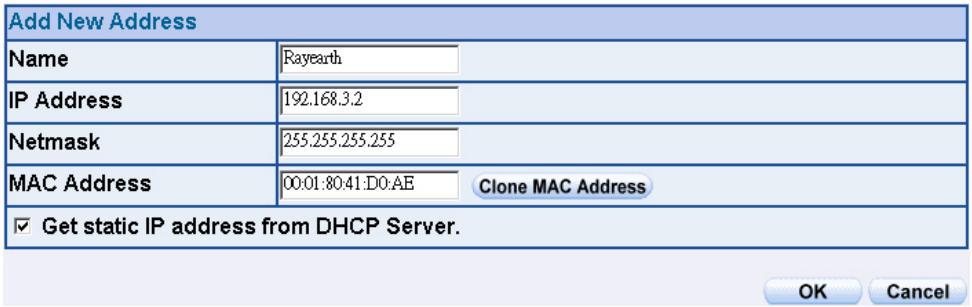


Figure 4-1 Setting LAN Address Book WebUI

Figure4-2 Complete the Setting of LAN

STEP 2．Adding the following setting in **Outgoing Policy**: (Figure4-3)

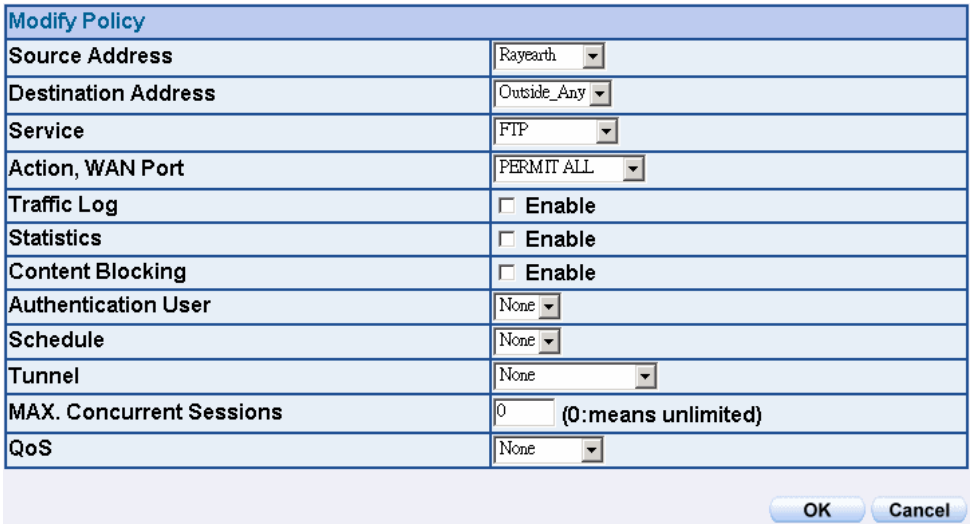


Figure 4-3 Add a Policy of Restricting the Specific IP to Access to Internet

STEP 3．Complete assigning the specific IP to static users in **Outgoing Policy** and restrict them to access FTP net service only through policy: (Figure4-4)

Figure 4-4 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 ALL7000 to fill out the user's MAC Address automatically.

 In **LAN** of **Address** function, the ALL7000 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.

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

STEP 1 . Setting several LAN network Address. (Figure4-5)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.1.2/255.255.255.255	00:E0:18:25:F5:89	In Use
Josh	192.168.1.4/255.255.255.255		Modify Remove
SinSan	192.168.1.5/255.255.255.255	00:E0:18:25:F5:88	Modify Remove
Daniel	192.168.1.7/255.255.255.255	00:E0:18:25:87:1A	Modify Remove
Luke	192.168.1.8/255.255.255.255		Modify Remove

Figure4-5 Setting Several LAN Network Address

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

- Click **New Entry** (Figure 4-6)
- Enter the **Name** of the group
- Select the users in the **Available Address** column and click **Add**
- Click **OK** (Figure 4-7)

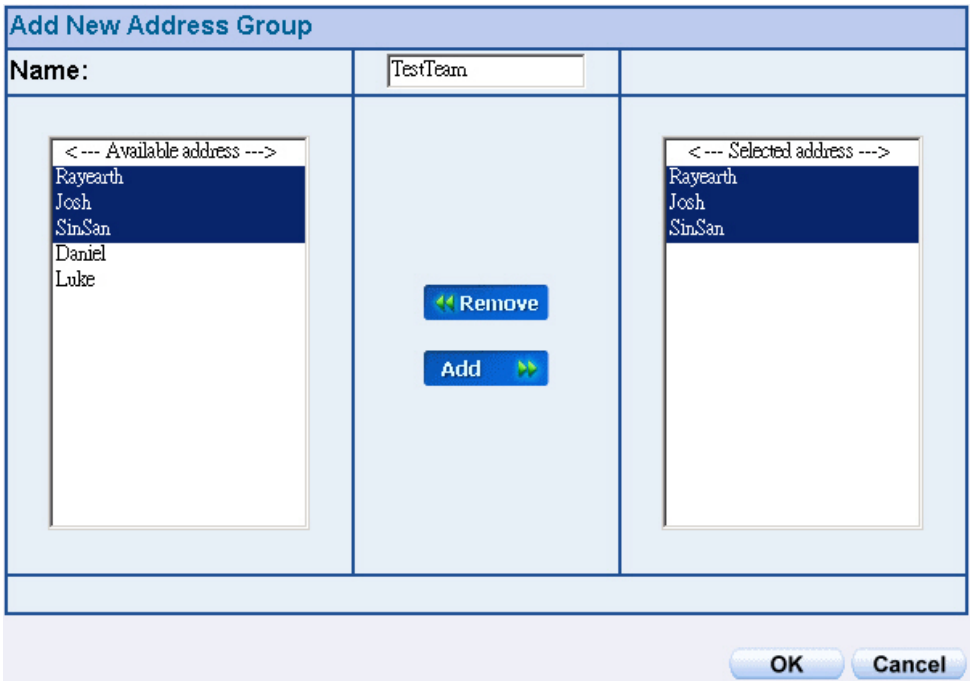


Figure4-6 Add New LAN Address Group

Figure4-7 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** (Figure4-8)
- Enter the following data (**Name, IP Address, Netmask**)
- Click **OK** (Figure4-9)

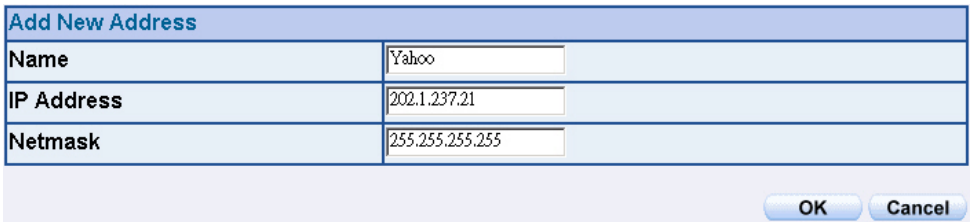


Figure4-8 Add New WAN Address

Figure4-9 Complete the Setting of WAN Address

STEP 4．To exercise STEP1~3 in **Policy** (Figre4-10, 4-11)

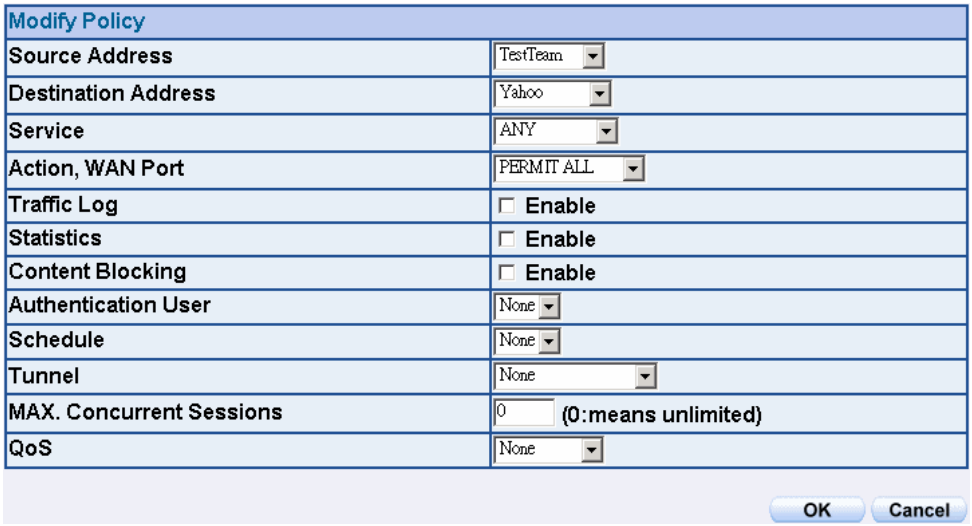


Figure4-10 To Exercise Address Setting in Policy

Figure4-11 Complete the Policy Setting

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

Chapter 5

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 ALL7000 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.

Define the required fields of Service

Pre-defined WebUI's Chart and Illustration:

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

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 1024~65535, suggest to use the default range)

Server Port:

- The port number of custom service

We set up two Service examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	**Custom**	Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15325-15333, UDP 15325-15333)	**65**
Ex2	**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)	**69**

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: (Figure5-1, 5-2)

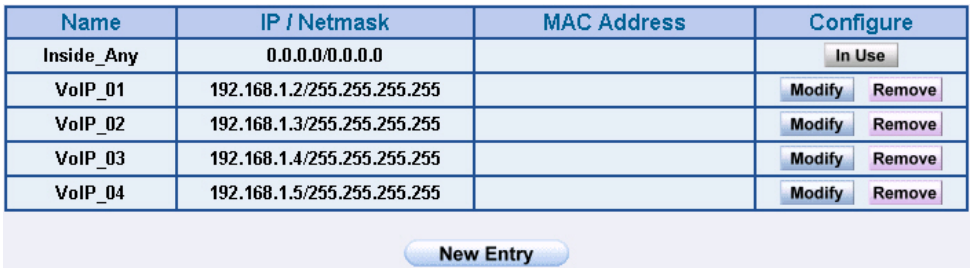


Figure5-1 Setting LAN Address Book WebUI

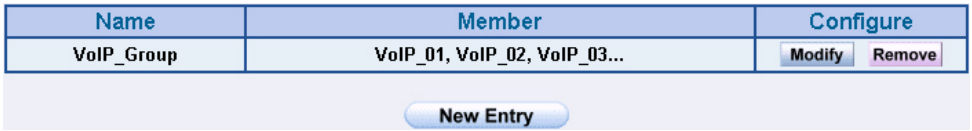


Figure5-2 Setting LAN Group Address Book WebUI

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

- Click **New Entry** (Figure5-3)
- **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** (Figure5-4)

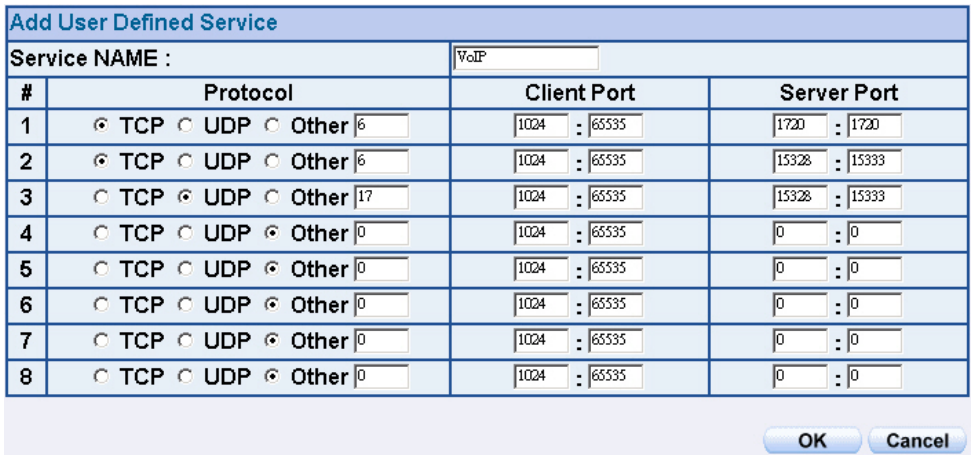


Figure5-3 Add User Define Service

Figure5-4 Complete the Setting of User Define Service of VoIP

 Under general circumstances, the range of port number of client is 1024-65535. 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 enter in the two space are the same port number, then enable the port number as one (for example: 1720:1720).

STEP 3．Compare **Service** to **Virtual Server.** (Figure5-5)

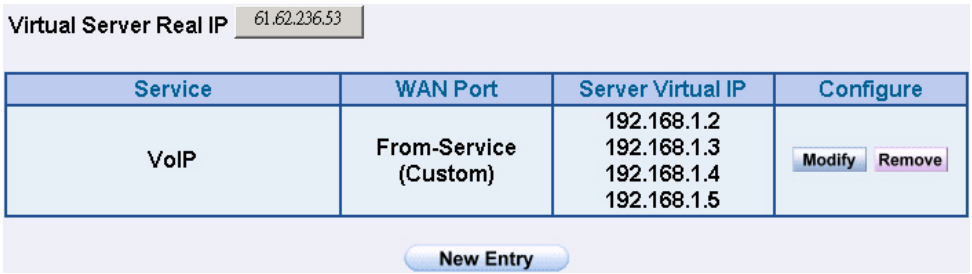


Figure5-5 Compare Service to Virtual Server

STEP 4．Compare **Virtual Server** to **Incoming Policy**. (Figure5-6)

Figure5-6 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: (Figure5-7)

Figure5-7 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

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 5-8)
- **Name:** Enter Main_Service
- Select HTTP, POP3, SMTP, DNS in **Available Service** and click **Add**
- Click **OK** (Figure 5-9)

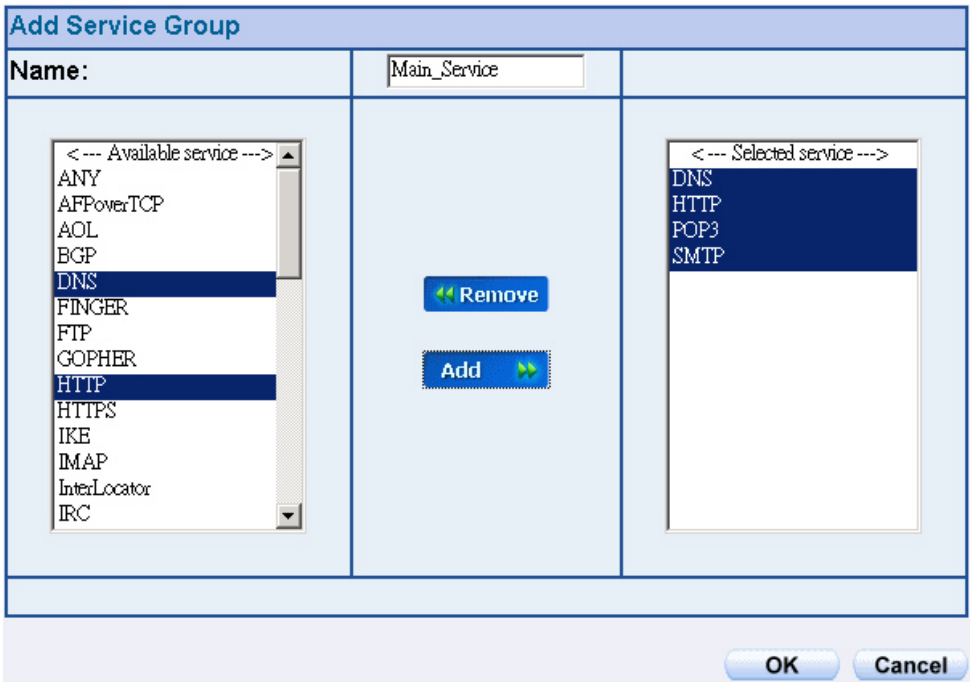


Figure5-8 Add Service Group

Figure5-9 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, Setting an **Address Group** that can include the service of access to Internet. (Figure5-10)

Figure5-10 Setting Address Book Group

STEP 3．Compare **Service Group** to **Outgoing Policy.** (Figure5-11)

Figure5-11 Setting Policy

Chapter 6

Schedule

In this chapter, the ALL7000 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** (Figure6-1)
- Enter **Schedule Name**
- Set up the working time of Schedule for each day
- Click **OK** (Figure6-2)

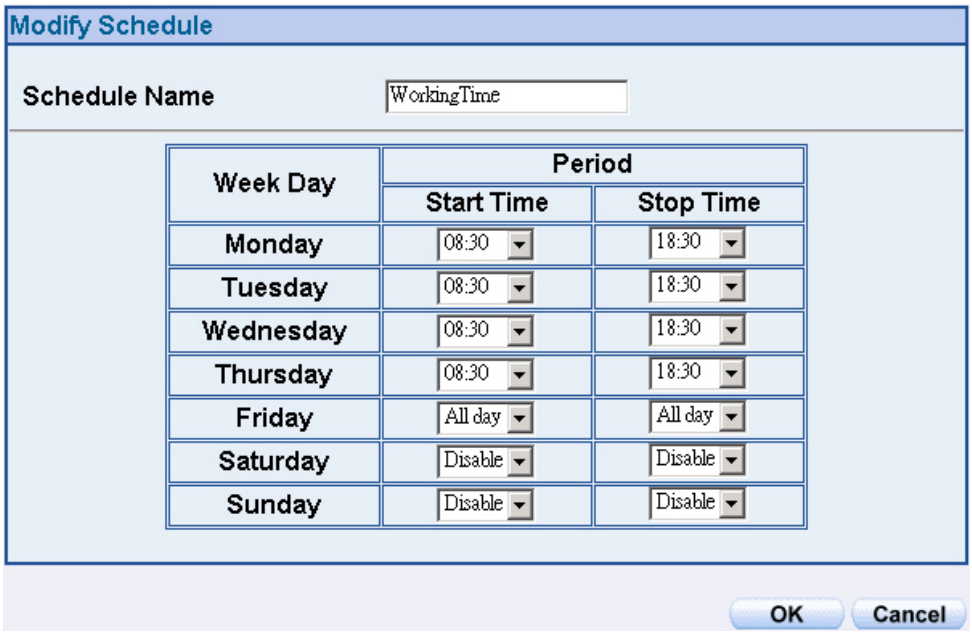


Figure6-1 Setting Schedule WebUI

Figure6-2 Complete the Setting of Schedule

STEP 2．Compare **Schedule** with **Outgoing Policy** (Figure6-3)

Figure6-3 Complete the Setting of Comparing Schedule with Policy

The Schedule must compare with **Policy** .

Chapter 7

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 ALL7000 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The ALL7000 also makes it convenient for the administrator to make the Bandwidth to reach the best utility. (Figure7-1, 7-2)

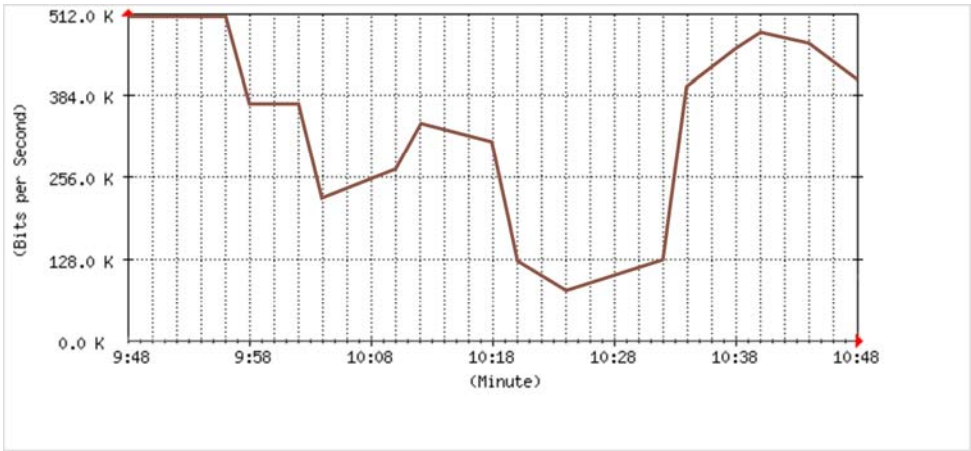


Figure7-1 the Flow Before Using QoS

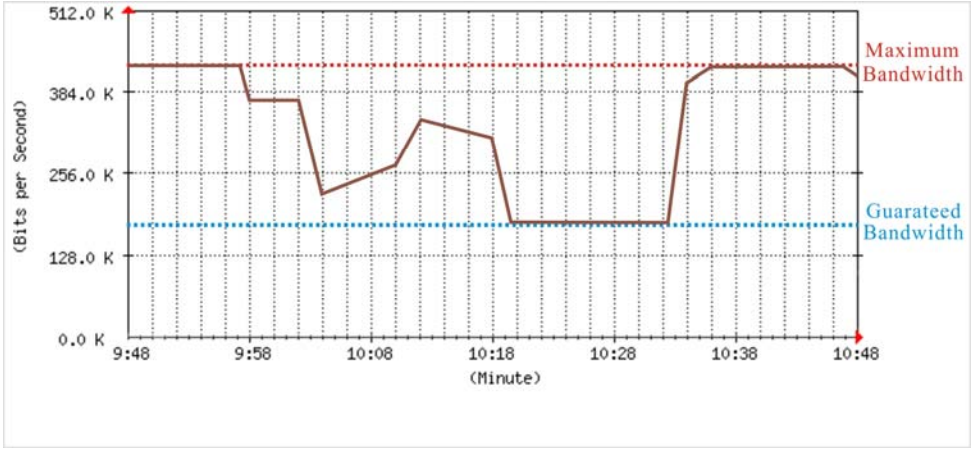


Figure7-2 the Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

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 apply from ISP

Upstream Bandwidth:

- To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply 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.

We set up two QoS examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	**QoS**	Setting a policy that can restrict the user's downstream and upstream bandwidth.	**79**

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

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

- Click **New Entry** (Figure7-3)
- **Name:** The name of the QoS you want to configure.
- Enter the bandwidth in WAN1, WAN2
- Select **QoS Priority**
- Click **OK** (Figure7-4)

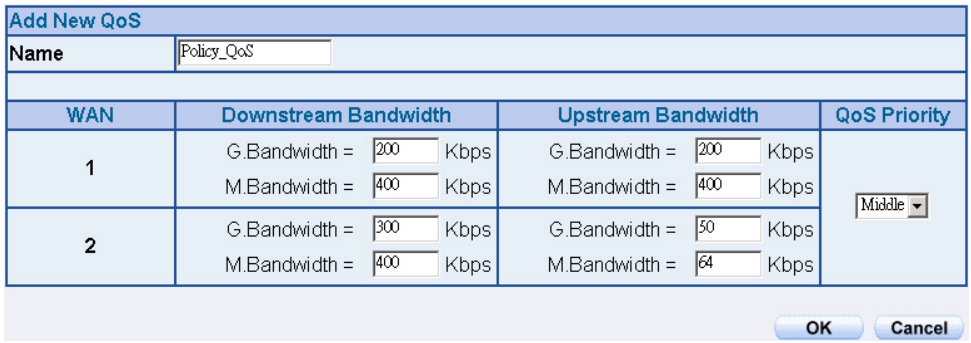


Figure7-3 QoS WebUI Setting

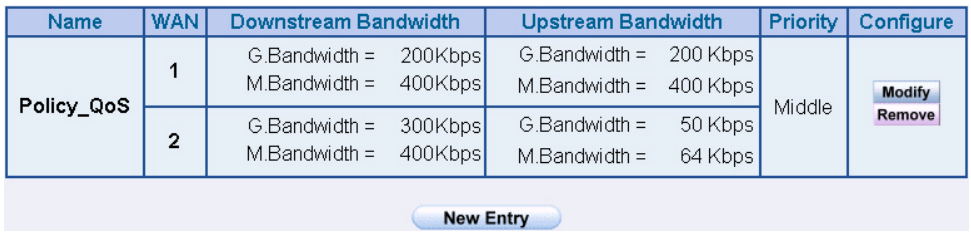


Figure7-4 Complete the QoS Setting

STEP 2． Use the QoS that set by STEP1 in **Outgoing Policy.** (Figure7-5, 7-6)

Schedule	WorkingTime
Tunnel	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Policy_QoS

Figure7-5 Setting the QoS in Policy

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

New Entry

Figure7-6 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 8

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 ALL7000 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 ALL7000 authentication. (Have to setup the Authentication first)
  - **Authentication Port:** The internal user have to pass the authentication to access to the Internet when enable ALL7000.
  - **Re-Login if Idle:** When the internal user access to Internet, can setup the idle time after passing authentication. If idle time exceeds the time you setup, the authentication will be invalid. The default value is 30 minutes.
  - **URL to redirect when authentication succeed:** The user who had passes Authentication have to connect to the specific website. (It will connect to the website directly which the user want to login) 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: (Figure8-1)

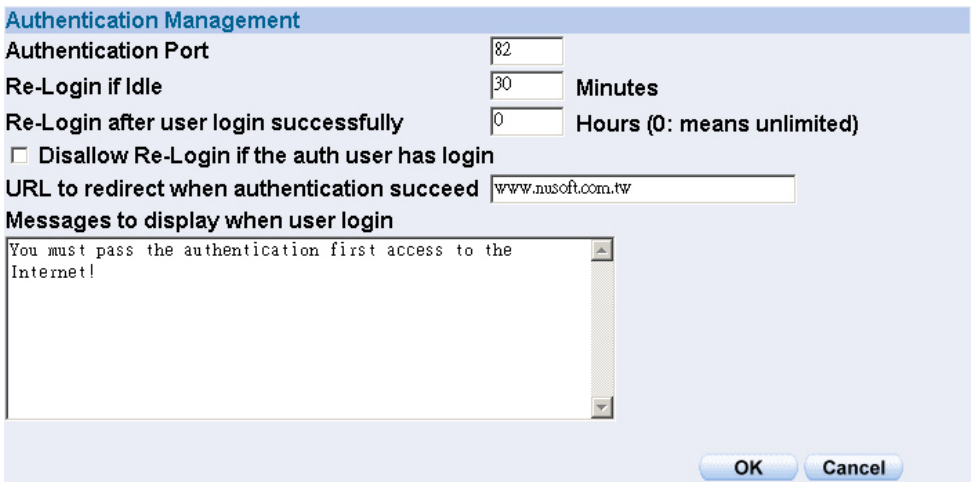


Figure8-1 Authentication Setting WebUI

- When the user connect to external network by Authentication, the following page will be displayed: (Figure8-2)

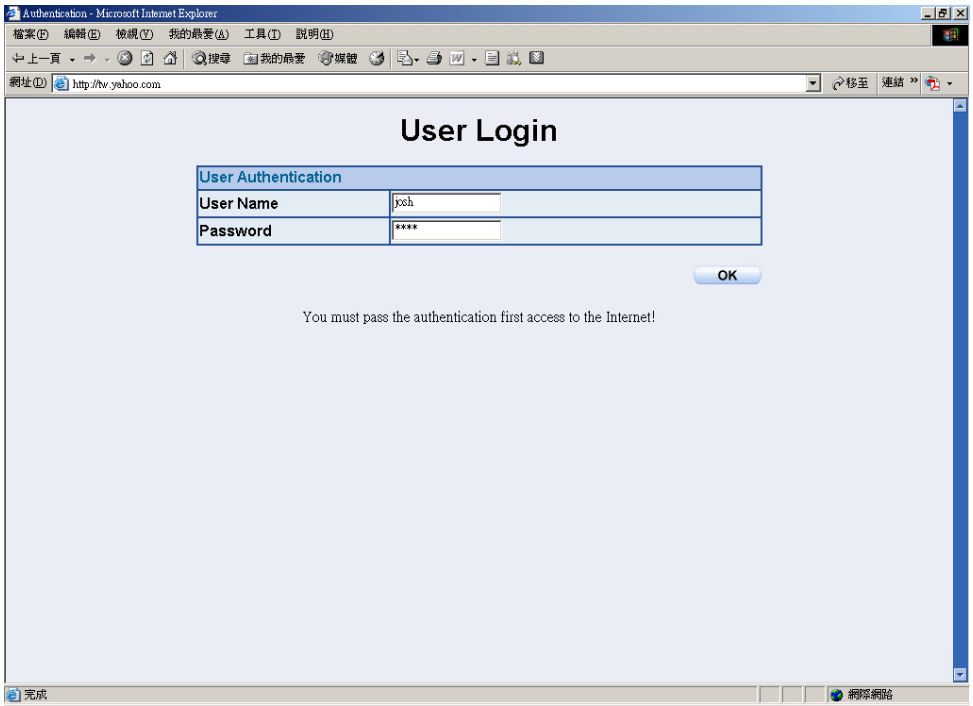


Figure8-2 Authentication Login WebUI

- It will connect to the appointed website after passing Authentication: (Figure8-3)

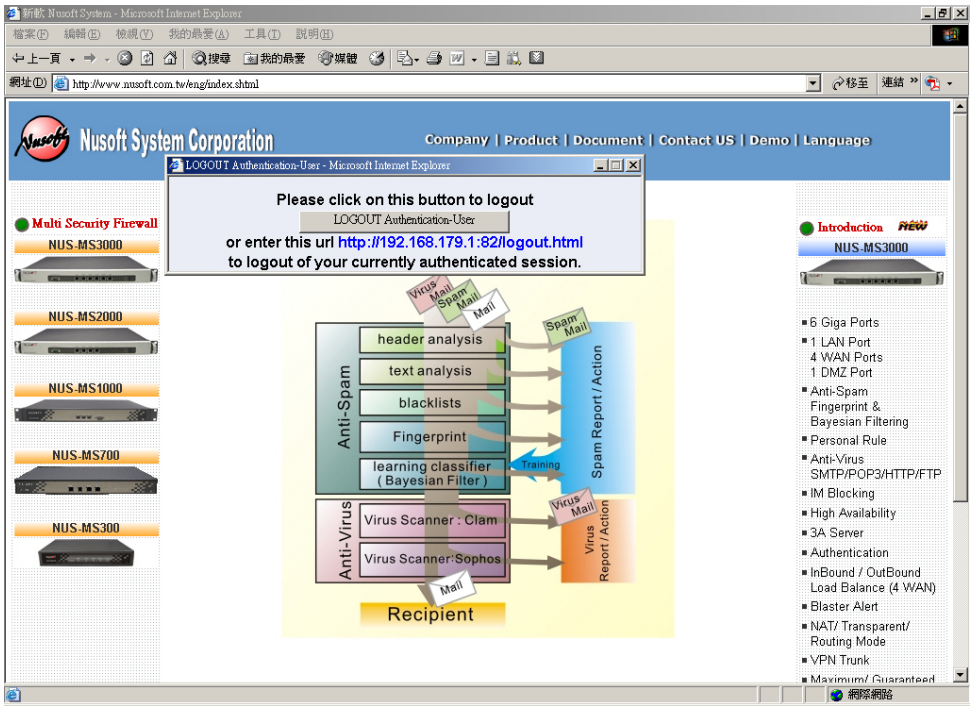


Figure8-3 Connecting to the Appointed Website After Authentication

If the user ask for authentication positively, can enter the LAN IP by the Authentication port number. And then the Authentication WebUI will be displayed.

Auth-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

We set up four Authentication examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	**Auth User Auth Group**	Setting specific users to connect with external network only before passing the authentication of policy. （Adopt the built-in Auth User and Auth Group Function）	**87**

Setting specific users to connect with external network only before passing the authentication of policy.
（Adopt the built-in Auth User and Auth Group Function）

STEP 1．Setup several **Auth User** in **Authentication**. (Figire8-4)

Figure8-4 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 ALL7000.

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

- Click **New Entry**
- **Name:** Enter laboratory
- Select the Auth User you want and **Add** to Selected Auth User
- Click **OK**
- Complete the setting of Auth User Group (Figure8-5)

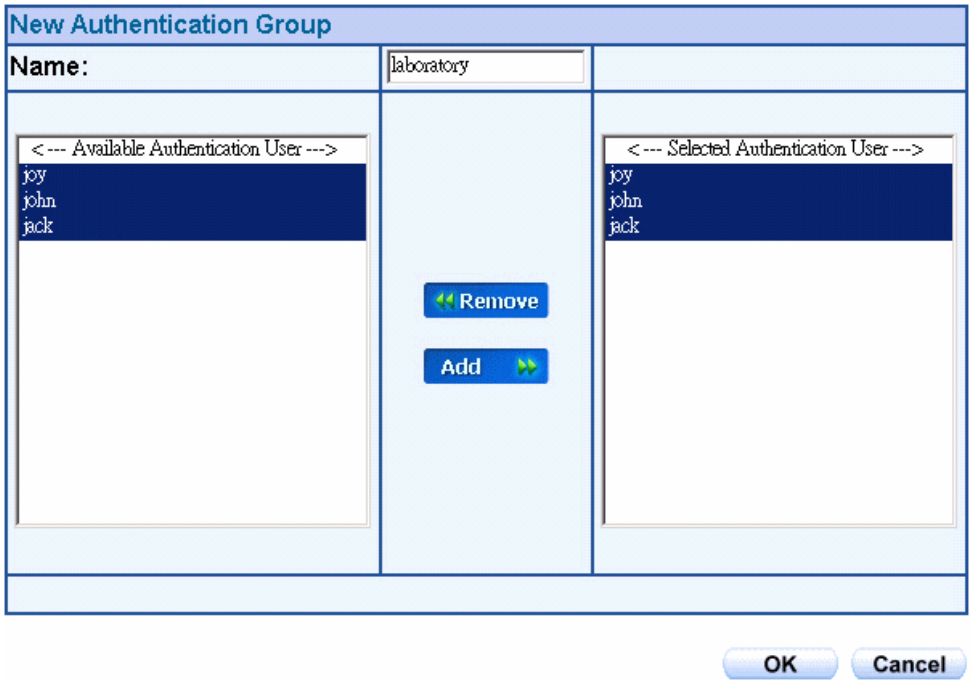


Figure8-5 Setting Auth Group WebUI

STEP 3 . Add a policy in **Outgoing Policy** and input the Address and Authentication of STEP 2 (Figure8-6, 8-7)

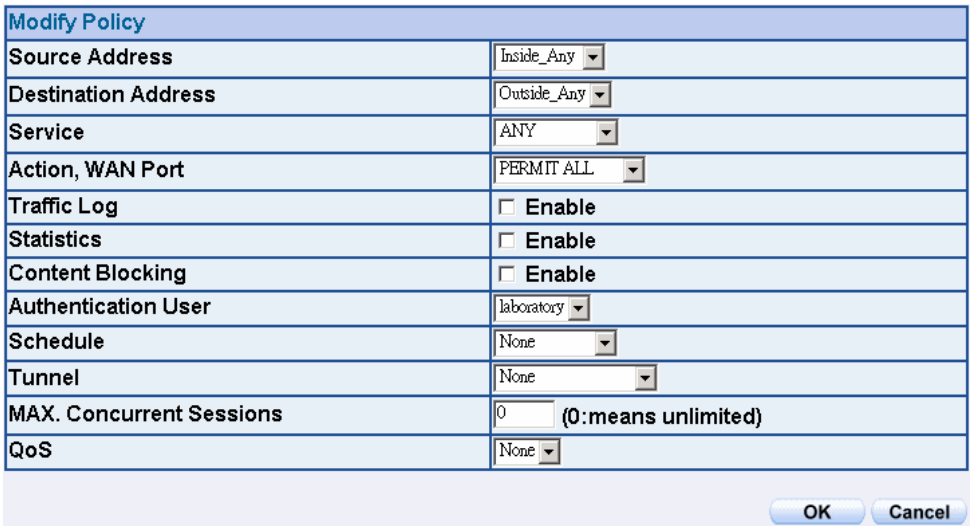


Figure8-6 Auth-User Policy Setting

Figure8-7 Complete the Policy Setting of Auth-User

STEP 4 . 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. (Figure8-8)

STEP 5 . 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 (Figure8-9)

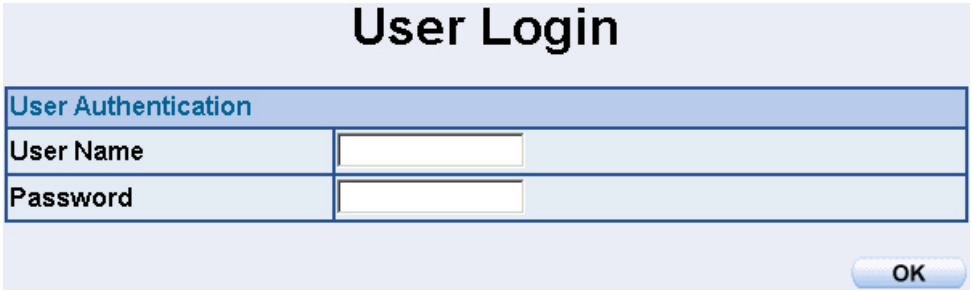


Figure8-8 Access to Internet through Authentication WebUI

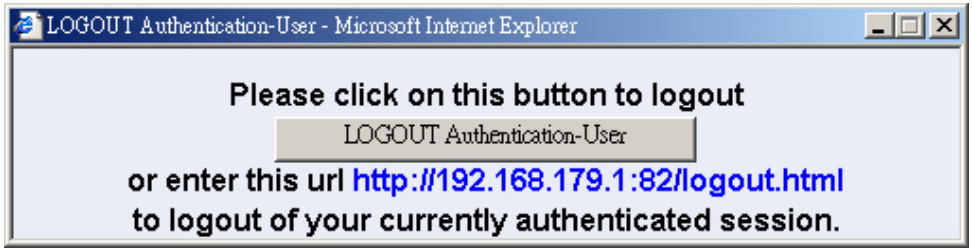


Figure8-9 Logout Auth-User WebUI

Chapter 9

Content Filtering

Content Filtering includes「URL」,「Script」,「P2P」,「IM」,「Download」.

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

【Script Blocking】： The access authority of Popup, ActiveX, Java, Cookies

【P2P Blocking】： The authority of sending files by eDonkey, eMule, Bit Torrent

【IM Blocking】： To restrict the authority of receiving video, file and message from MSN Messenger, Yahoo Messenger, ICQ, QQ.

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

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

Cookies Blocking:

- Prevent Cookies packets

eDonkey Blocking:

- Prevent users to deliver files by eDonkey and eMule

BitTorrent Blocking:

- Prevent users to deliver files by BitTorrent

WinMX:

- Prevent users to deliver files by WinMX

IM Blocking:

- Prevent users to login MSN Messenger, Yahoo Messenger, ICQ, QQ, and Skype

Audio and Video Types:

- Prevent users to transfer sounds and video file by http

Sub-name file 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.

We set up five Content Blocking examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	**URL Blocking**	Restrict the Internal Users only can access to some specific Website	**95**
Ex2	**Script Blocking**	Restrict the Internal Users to access to Script file of Website.	**98**
Ex3	**P2P Blocking**	Restrict the Internal Users to access to the file on Internet by P2P.	**100**
Ex4	**IM Blocking**	Restrict the Internal Users to send message, files, video and audio by Instant Messaging.	**102**
Ex5	**Download Blocking**	Restrict the Internal Users to access to video, audio, and some specific sub-name file from http or ftp protocol directly.	**104**

Restrict the Internal Users only can access to some specific Website

※URL Blocking:

Symbol: ～ means open up; ＊ means metacharacter

Restrict not to enter specific website: Enter 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.

Only open specific website to enter:

1. Add the website you want to open up in URL String. While adding, you must enter the symbol “~” in front of the 「complete domain name」 or 「key word」 that represents to open these website to enter”. For example: ~www.kcg.gov.tw or ~gov.
2. After setting up the website you want to open up, enter an order to “forbid all” in the last URL String; means only enter ＊ in URL String.

 **Warning!** The order to forbid all must be placed at last forever. If you want to open a new website, you must delete the order of forbidding all and then enter the new domain name. At last, re-enter 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 (Figure9-1)

Figure9-1 Content Filtering Table

STEP 2 . Add a **Outgoing Policy** and use in **Content Blocking** function: (Figure9-2)

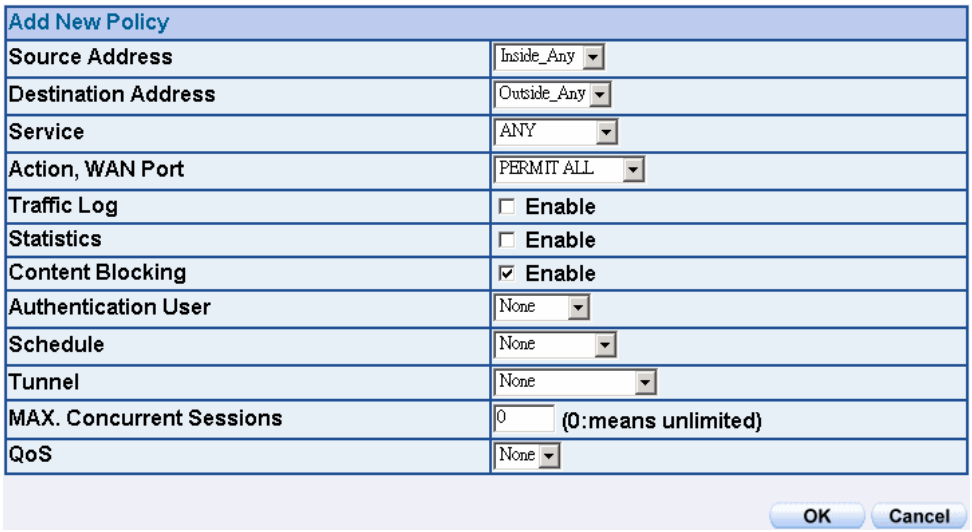


Figure9-2 URL Blocking Policy Setting

STEP 3 . Complete the policy of permitting the internal users only can access to some specific website in **Outgoing Policy** function: (Figure9-3)

Figure9-3 Complete Policy Settings

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

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 **Cookies** Blocking
- Click **OK**
- Complete the setting of Script Blocking (Figure9-4)

Figure9-4 Script Blocking WebUI

STEP 2． Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure9-5)

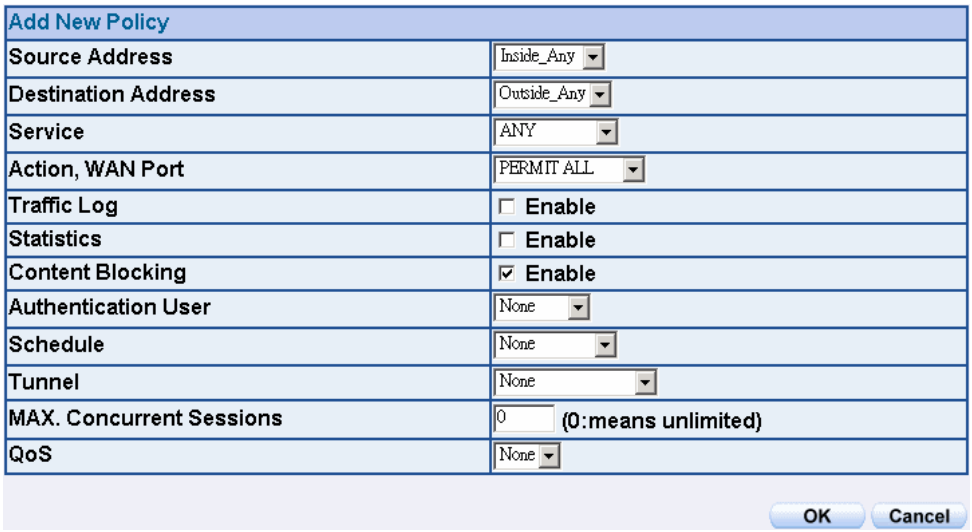


Figure9-5 New Policy of Script Blocking Setting

STEP 3． Complete the policy of restricting the internal users to access to Script file of Website in **Outgoing Policy**: (Figure9-6)

Figure9-6 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.

Restrict the Internal Users to access to the file on Internet by P2P

STEP 1 . Select the following data in **P2P** of **Content Blocking** function**:**

- Select **eDonkey Blocking**
- Select **BitTorrent Blocking**
- Select **WinMX Blocking**
- Click **OK**
- Complete the setting of P2P Blocking (Figure9-7)

Figure9-7 P2P Blocking WebUI

STEP 2． Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure9-8)

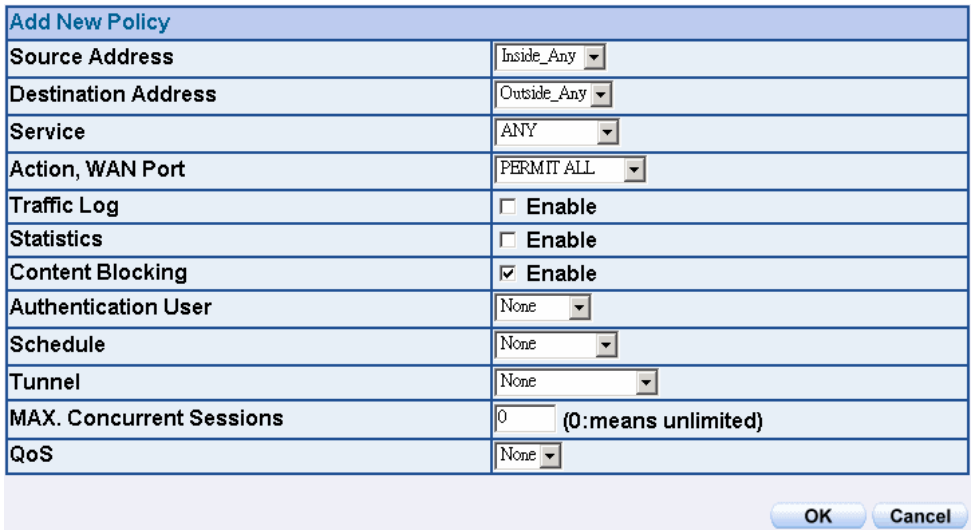


Figure9-8 Add New Policy of P2P Blocking

STEP 3． Complete the policy of restricting the internal users to access to the file on Internet by P2P in **Outgoing Policy**: (Figure9-9)

Figure9-9 Complete P2P Blocking Policy Setting

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 **P2P Blocking** in **Content Blocking** to restrict users to use P2P Transfer efficiently.

Restrict the Internal Users to send message, files, video and audio by Instant Messaging

STEP 1．Enter as following in **IM Blocking** of **Content Blocking** function:

- Select **MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger** and **Skype.**
- Click **OK**
- Complete the setting of IM Blocking. (Figure9-10)

Figure9-10 IM Blocking WebUI

STEP 2． Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figire9-11)

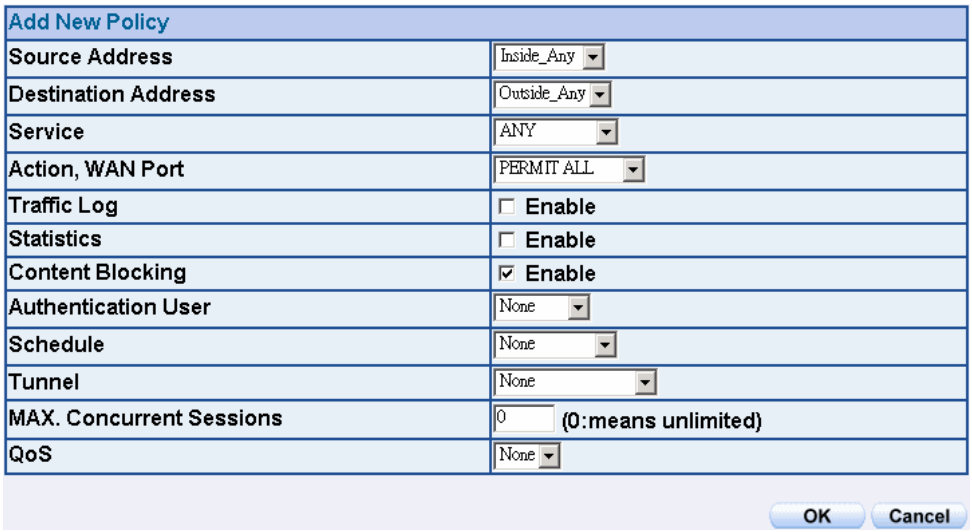


Figure9-11 Add New IM Blocking Policy

STEP 3． Complete the policy of restricting the internal users to send message, files, audio, and video by instant messaging in **Outgoing Policy:** (Figure9-12)

Figure9-12 Complete IM Blocking Policy Setting

Restrict the Internal Users to access to 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. (Figure9-13)

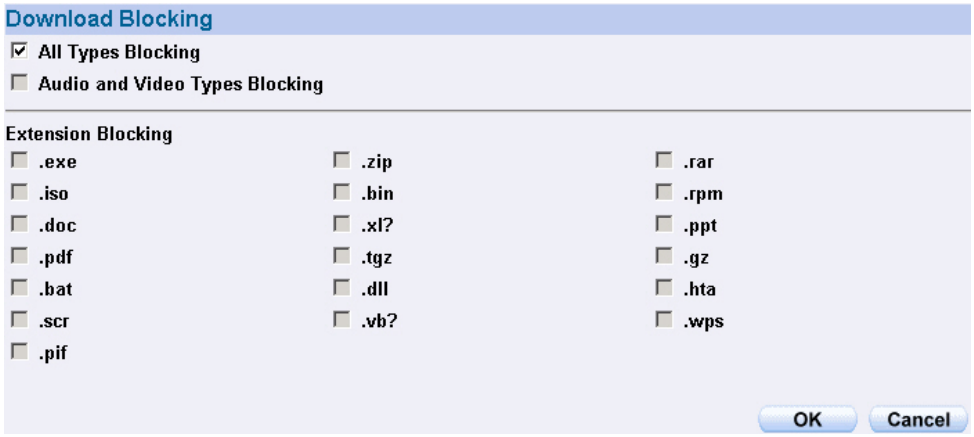


Figure9-13 Download Blocking WebUI

STEP 2 . Add a new **Outgoing Policy** and use in **Content Blocking** function: (Figure9-14)

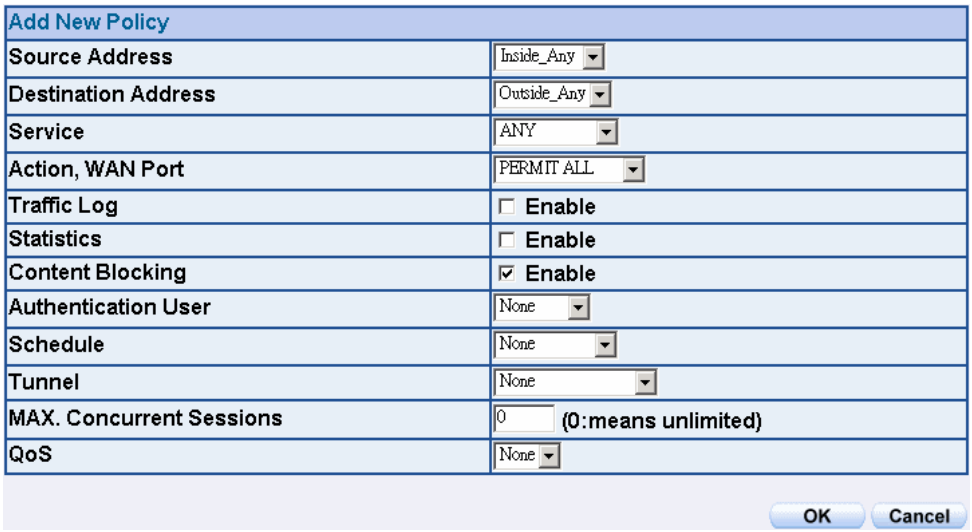


Figure9-14 Add New Download Blocking Policy Setting

STEP 3 . Complete the **Outgoing Policy** of restricting the internal users to access to video, audio, and some specific sub-name file by http protocol directly: (Figure9-15)

Figure9-15 Complete Download Blocking Policy Setting

Chapter 10

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 ALL7000'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 ALL7000's Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the ALL7000's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the ALL7000 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 ALL7000's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the ALL7000. 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.

We set up four Virtual Server examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	**Mapped IP**	Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy.	**110**
Ex2	**Virtual Server**	Make several servers that provide a single service, to provide service through policy by Virtual Server. (Take Web service for example)	**113**
Ex3	**Virtual Server**	The external user use VoIP to connect with VoIP of LAN. (VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)	**116**
Ex4	**Virtual Server**	Make several servers that provide several same services, to provide service through policy by Virtual Server. (Take HTTP, POP3, SMTP, and DNS Group for example)	**120**

Preparation

Apply for two ADSL that have static IP
(WAN1 static IP is 61.11.11.10~ 61.11.11.14)
(WAN2 static IP is 211.22.22.18~ 211.22.22.30)

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: (Figure10-1)

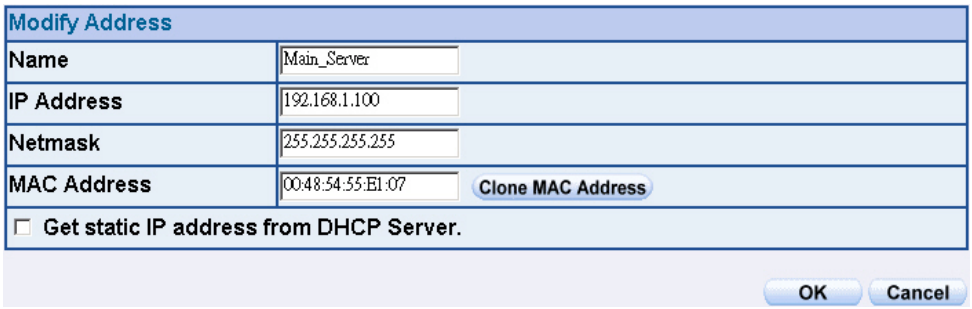


Figure10-1 Mapped IP Settings of Server in Address

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 (Figure10-2)

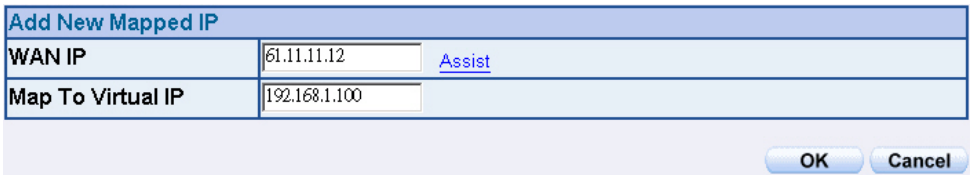


Figure10-2 Mapped IP Setting WebUI

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. (Figure10-3)

Figure10-3 Service Setting

STEP 5 . Add a policy that includes settings of STEP3, 4 in **Incoming Policy.** (Figure10-4)

Figure10-4 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. (Figure10-5)

Figure10-5 Complete the Outgoing Policy

STEP 7 . Complete the setting of providing several services by mapped IP. (Figure10-6)

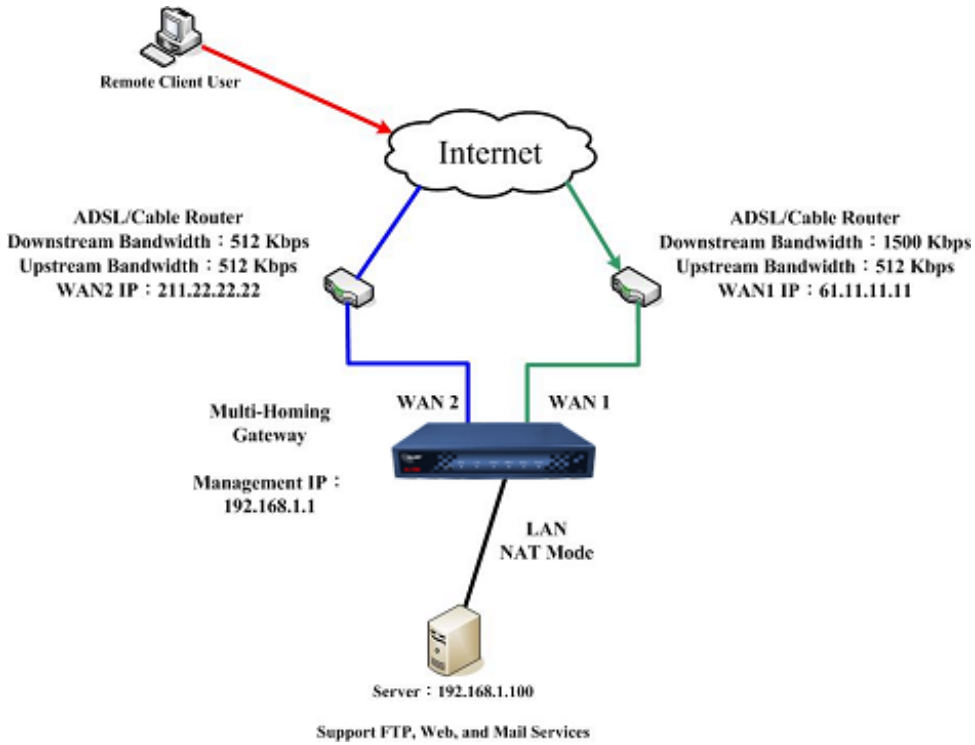


Figure10-6 A Single Server that Provides Several Services by Mapped IP

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.

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 **Server 1**
- **Virtual Server Real IP:** Enter 211.22.22.23 (click **Assist** for assistance)
- Click **OK** (Figure10-7)

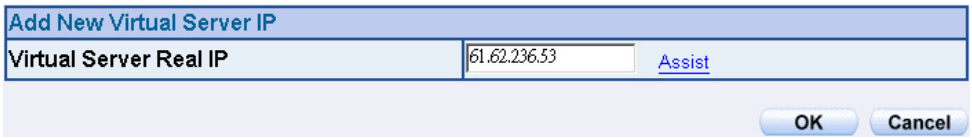


Figure10-7 Virtual Server Real IP Setting

- 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**
- Complete the setting of Virtual Server (Figure10-8)

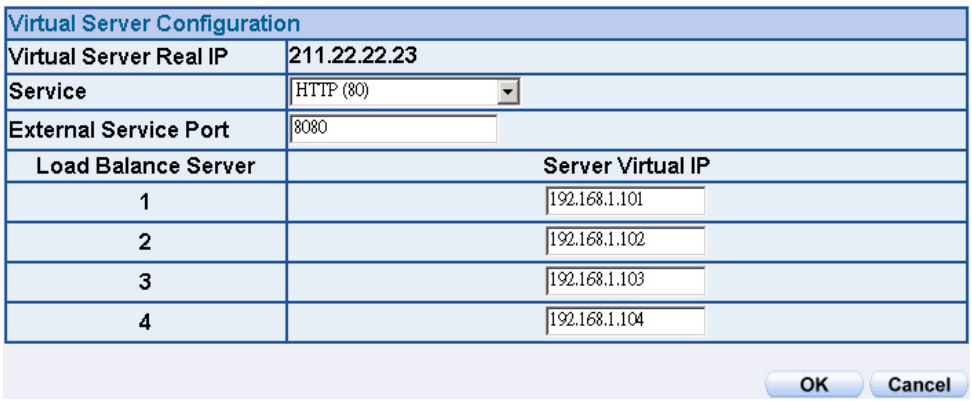


Figure10-8 Virtual Server Configuration WebUI

STEP 3． Add a new policy in **Incoming Policy**, which includes the virtual server, set by STEP2. (Figure10-9)

Figure10-9 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. (Figure10-10)

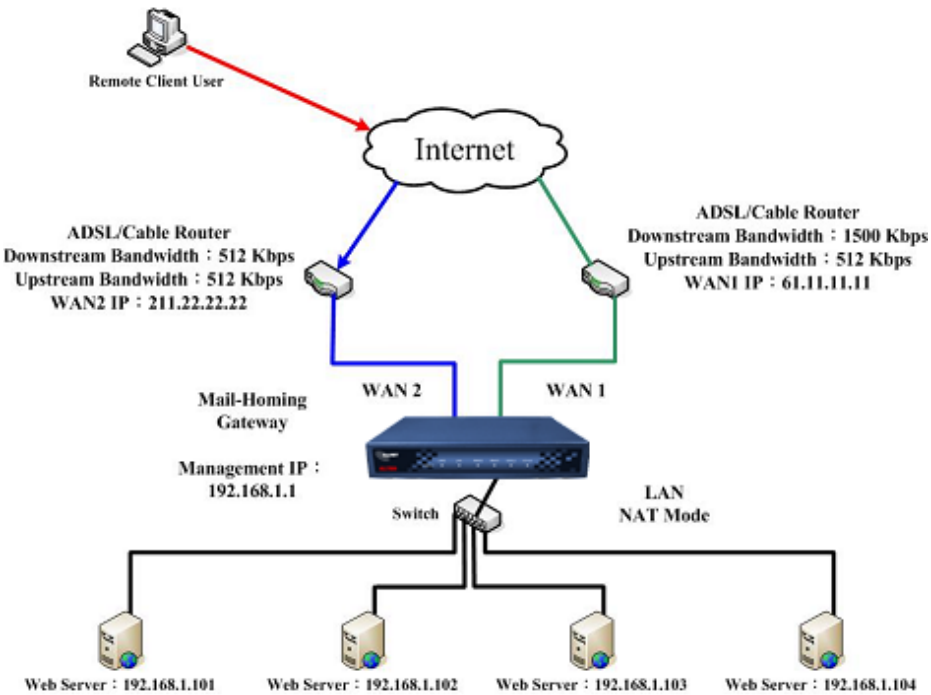


Figure10-10 Several Servers Provide a Single Service by Virtual Server

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: (Figure10-11)

Figure10-11 Setting LAN Address WebUI

STEP 3 . Add new VoIP service group in **Custom** of **Service** function. (Figure10-12)

Figure10-12 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** (Figure10-13)

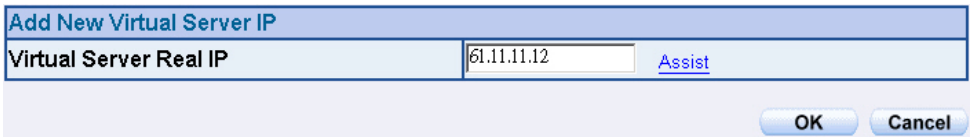


Figure10-13 Virtual Server Real IP Setting WebUI

- 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 (Figure10-14)

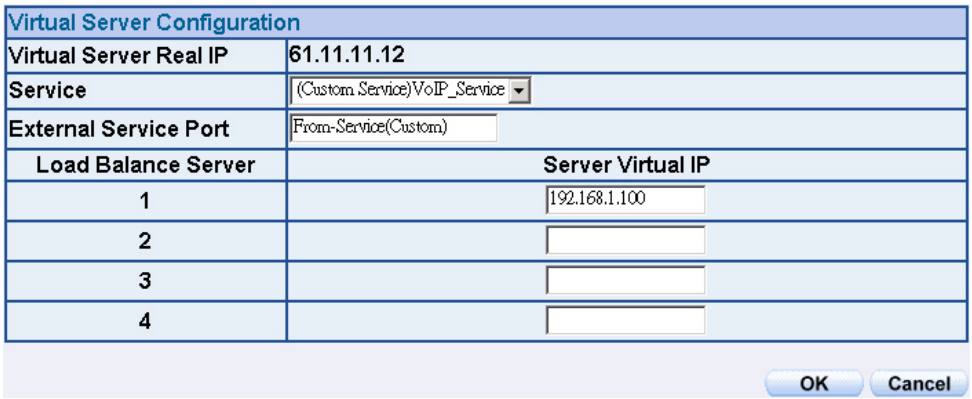


Figure10-14 Virtual Server Configuration WebUI

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: (Figure10-15)

Figure10-15 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**: (Figure10-16)

Figure10-16 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. (Figure10-17)

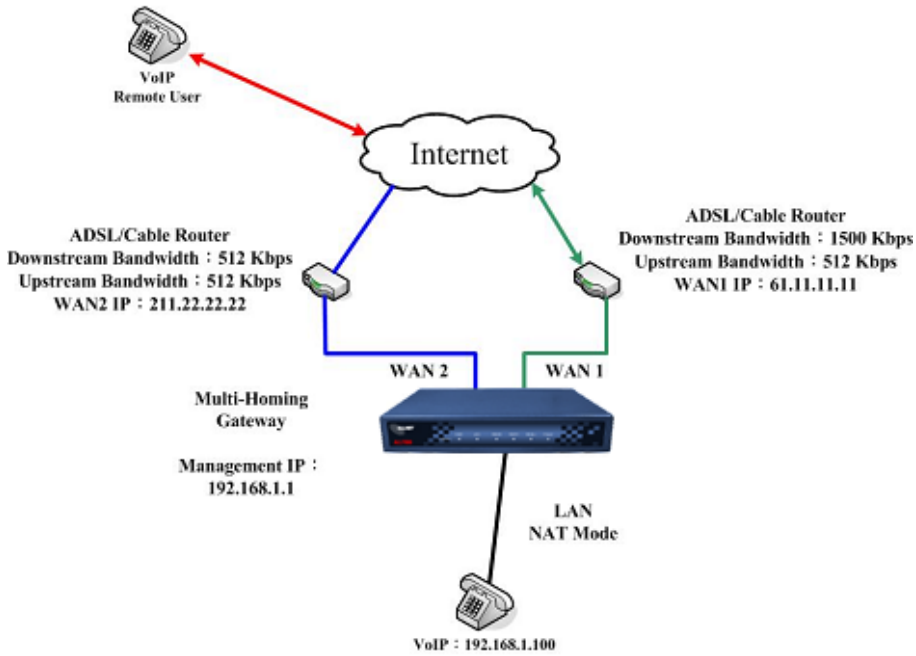
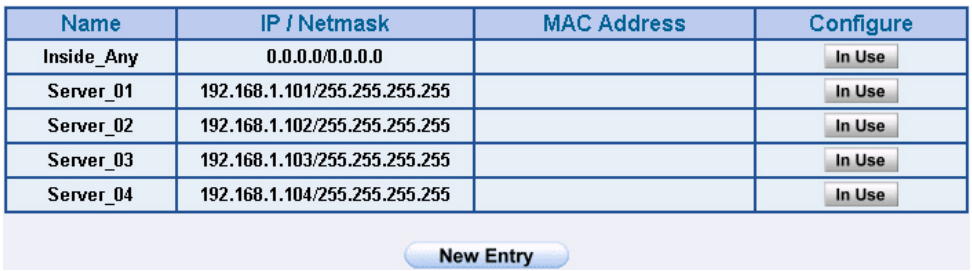


Figure10-17 Complete the Setting of the External/Internal User using specific service to communicate with each other by Virtual Server

Make several servers that provide several same services, to provide service through policy by Virtual Server. (Take HTTP, 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: (Figure10-18, 10-19)



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		In Use
Server_02	192.168.1.102/255.255.255.255		In Use
Server_03	192.168.1.103/255.255.255.255		In Use
Server_04	192.168.1.104/255.255.255.255		In Use

New Entry

Figure10-18 Mapped IP Setting of Virtual Server in Address

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

New Entry

Figure10-19 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. (Figure10-20)

Figure10-20 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** (Figure10-21)

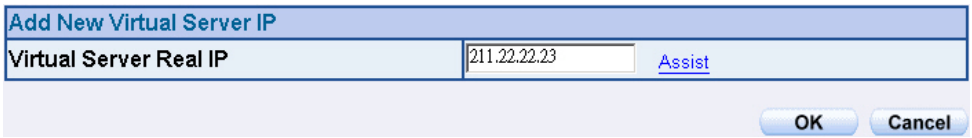


Figure10-21 Virtual Server Real IP Setting

- Click **New Entry**
- **Service:** Select (Group Service) Main_Service
- **External Service Port:** From-Service (Group)
- Enter the server IP in Load Balance Server
- Click **OK**
- Complete the setting of Virtual Server (Figure10-22)

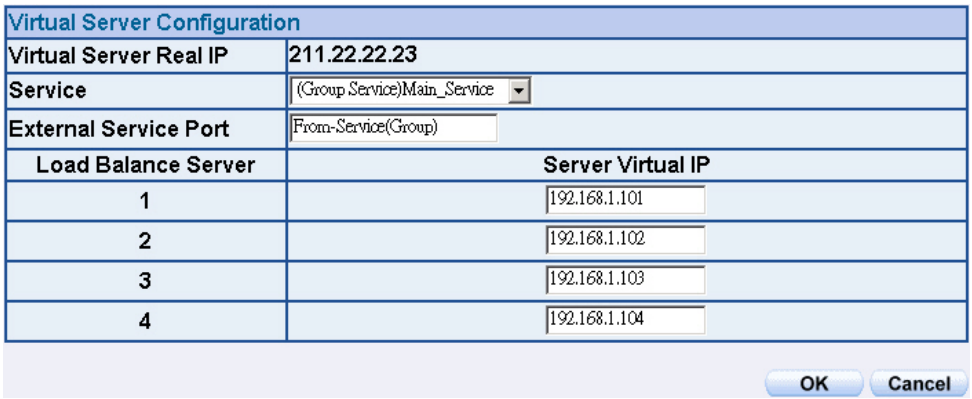


Figure10-22 Virtual Server Configuration WebUI

STEP 5． Add a new **Incoming Policy,** which includes the virtual server that set by STEP 3: (Figure10-23)

Figure10-23 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. (Figure10-24)

Figure10-24 Complete Outgoing Policy Setting

STEP 7 . Complete the setting of providing several services by Virtual Server. (Figure10-25)

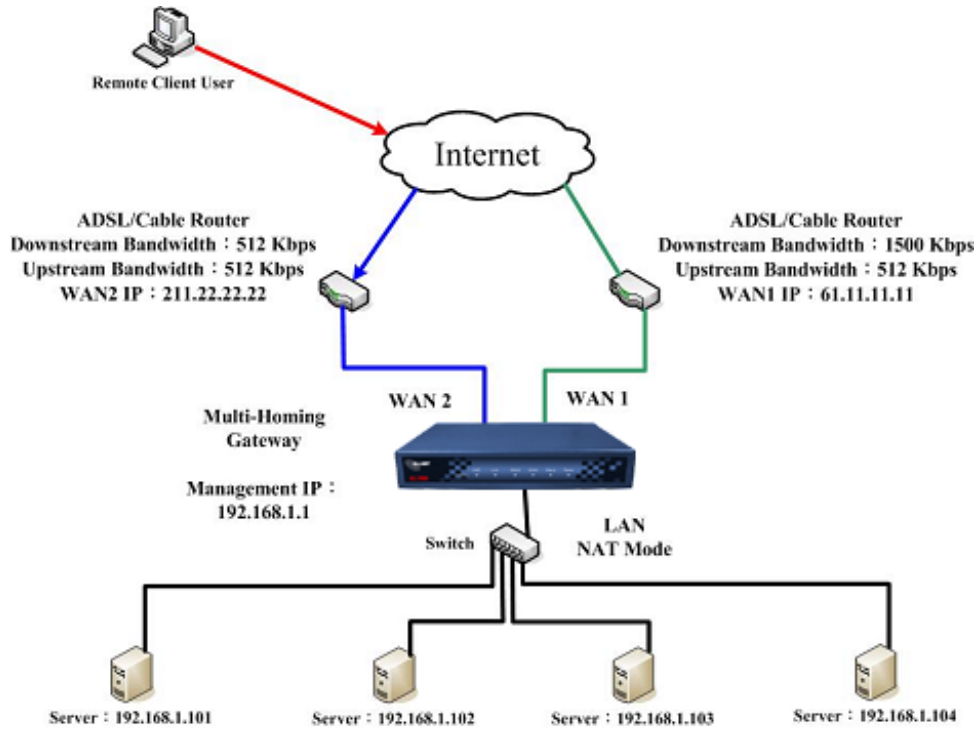


Figure10-25 Complete the Setting of Providing Several Services by Several Virtual Server

Chapter 11

VPN

The ALL7000 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 ALL7000.

【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.

Define the required fields of VPN:

RSA:

- A public-key cryptosystem for encryption and authentication.

Preshared 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

i:

- 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. (Figure11-1)

Figure11-1 IPSec Autokey WebUI

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

i:

- To display the VPN connection status via icon ◦

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

User Name:

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

Client IP:

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

Uptime:

- Display the connection time between PPTP Server and Client.

Configure:

- Click **Modify** to modify the PPTP Server Settings or click **Remove** to remove the setting (Figure11-2)

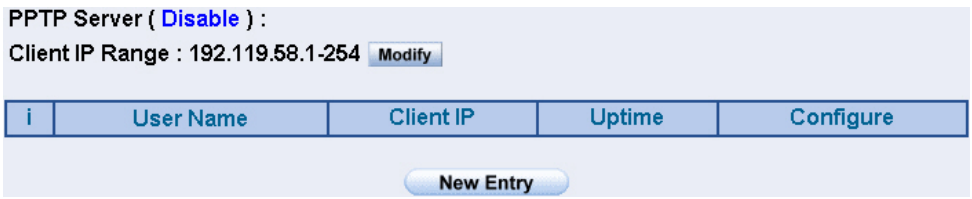


Figure11-2 PPTP Server WebUI

Define the required fields of PPTP Client Function

i:

- 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.

Server IP or Domain Name:

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

Encryption:

- Display 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. (Figure11-3)

Figure11-3 PPTP Client WebUI

Define the required fields of Tunnel Function

i:

- 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.

IPSec / PPTP:

- 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.(Figure11-4)

Figure11-4 VPN Tunnel Web UI

We set up two VPN examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	**IPSec Autokey**	Setting IPSec VPN connection between two ALL7000	**133**
Ex2	**PPTP**	Setting PPTP VPN connection between two ALL7000	**146**

Setting IPSec VPN connection between two ALL7000

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 ALL7000 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 ALL7000 192.168.10.1. Follow the steps below:

STEP 1 . Enter the default IP of Gateway of Company A's ALL7000, 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure11-5)

Figure11-5 IPSec Autokey WebUI

STEP 2 . In the list of **IPSec Autokey**, fill in Name with **VPN_A.** (Figure11-6)

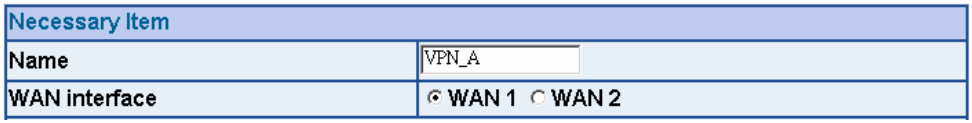


Figure11-6 IPSec Autokey Name Setting

STEP 3．Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.(Figure11-7)

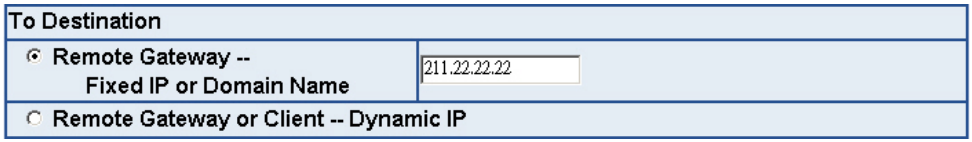


Figure11-7 IPSec To Destination Setting

STEP 4．Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-8)

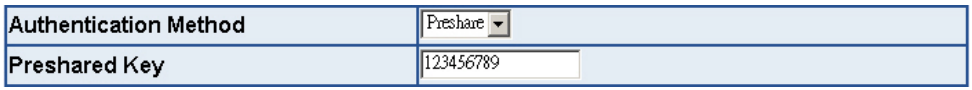


Figure11-8 IPSec Authentication Method Setting

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. (Figure11-9)

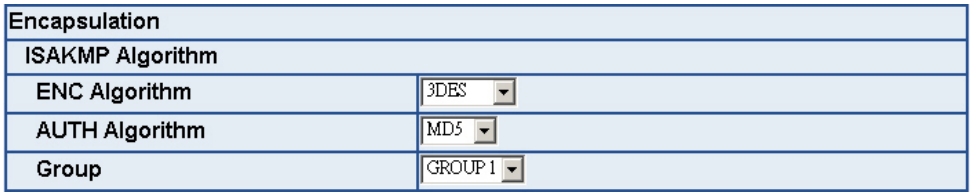


Figure11-9 IPSec Encapsulation Setting

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 (Figure11-10)

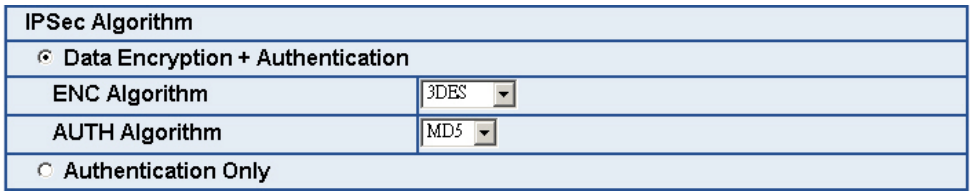


Figure11-10 IPSec Algorithm Setting

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**. (Figure11-11)

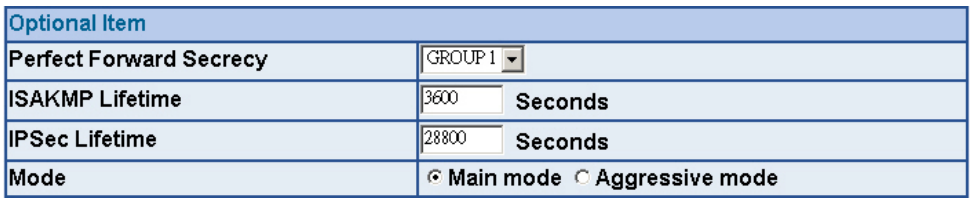


Figure11-11 IPSec Perfect Forward Secrecy Setting

STEP 8． Complete the IPSec Autokey setting. (Figure11-12)

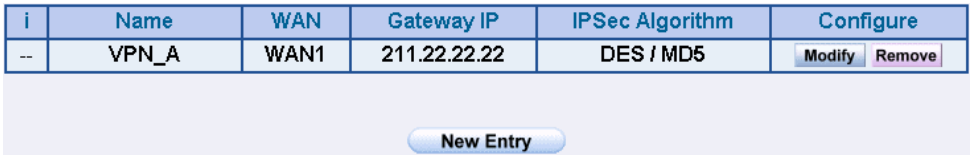


Figure11-12 Complete Company A IPSec Autokey Setting

STEP 9． Enter the following setting in **Tunnel** of **VPN** function**:** (Figure11-13)

- 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.
- Select **Show remote Network Neighborhood**.
- Click **OK**. (Figure11-14)

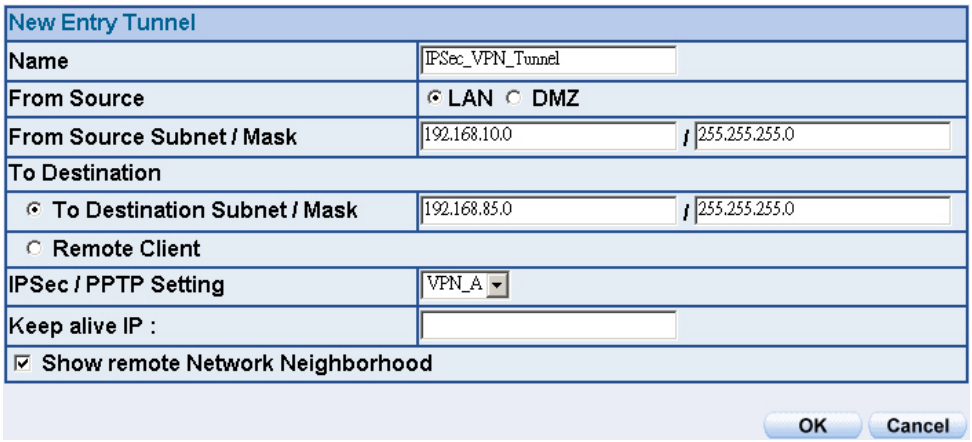


Figure11-13 New Entry Tunnel Setting

Figure11-14 Complete New Entry Tunnel Setting

STEP 10．Enter the following setting in **Outgoing Policy:**(Figure11-15)

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure11-16)

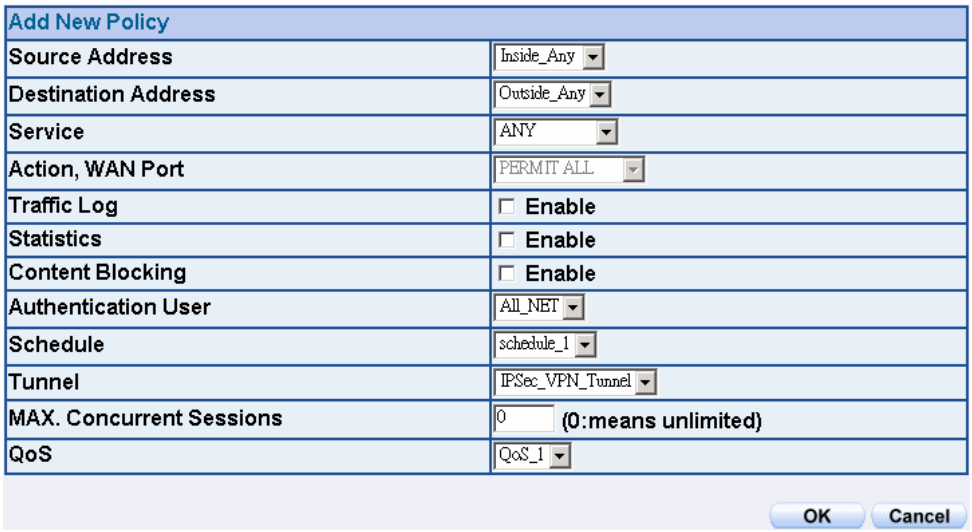


Figure11-15 Setting the VPN Tunnel Outgoing Policy

Figure11-16 Complete the VPN Tunnel Outgoing Policy Setting

STEP 11．Enter the following setting in **Incoming Policy:** (Figure11-17)

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure11-18)

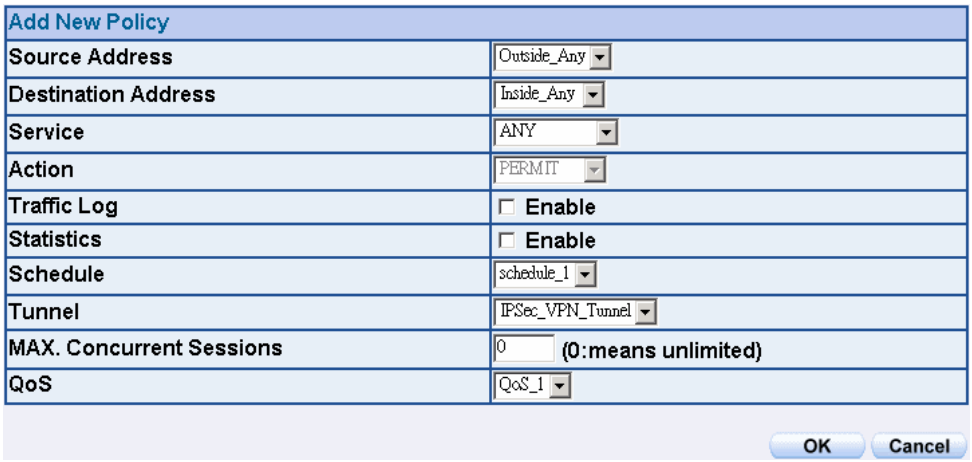


Figure11-17 Setting the VPN Tunnel Incoming Policy

Figure11-18 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the ALL7000 192.168.20.1. Follow the steps below:

STEP 1. Enter the following setting in **Multiple Subnet** of **System Configure** function**:** (Figure11-19)

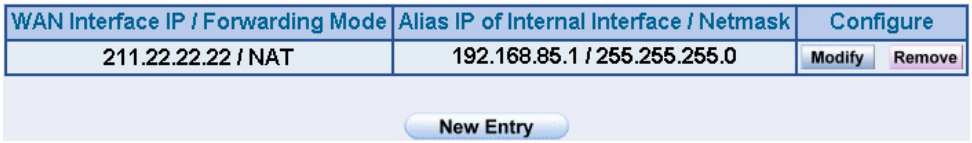


Figure11-19 Multiple Subnet Setting

STEP 2. Enter the default IP of Gateway of Company B's ALL7000, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure11-20)

Figure11-20 IPSec Autokey Web UI

STEP 3. In the list of **IPSec Autokey**, fill in Name with **VPN_B**. (Figure11-21)

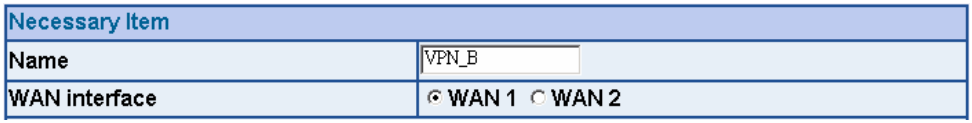


Figure11-21 IPSec Autokey Name Setting

STEP 4. Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.(Figure11-22)

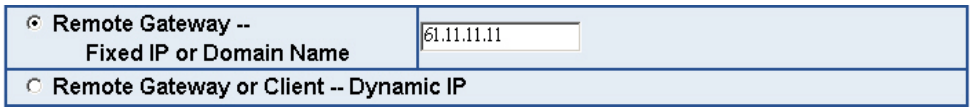


Figure11-22 IPSec To Destination Setting

STEP 5. Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-23)

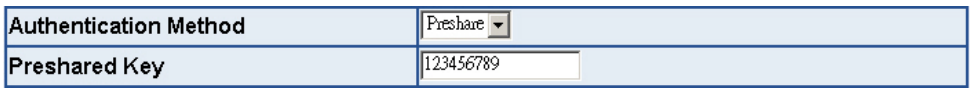


Figure11-23 IPSec Authentication Method Setting

STEP 6. 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. (Figure11-24)

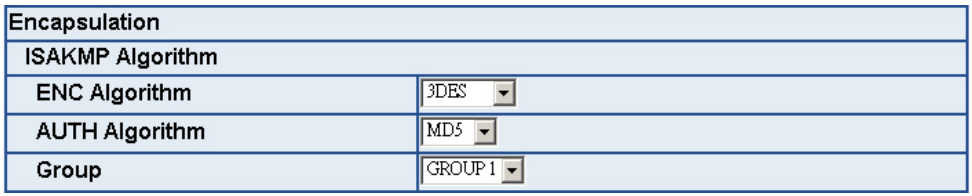


Figure11-24 IPSec Encapsulation Setting

STEP 7. 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. (Figure11-25)

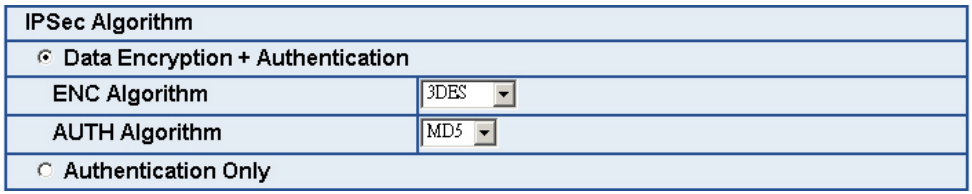


Figure11-25 IPSec Algorithm Setting

STEP 8. 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**. (Figure11-26)

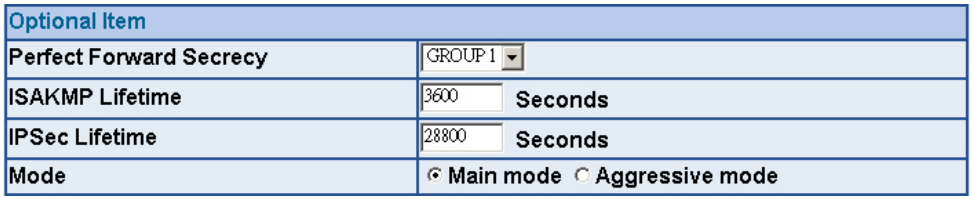


Figure11-26 IPSec Perfect Forward Secrecy Setting

STEP 9. Complete the IPSec Autokey setting. (Figure11-27)

Figure11-27 Complete Company B IPSec Autokey Setting

STEP 10. Enter the following setting in **Tunnel** of **VPN** function**:** (Figure11-28)

- 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.
- Select **Show remote Network Neighborhood**.
- Click **OK**. (Figure11-29)

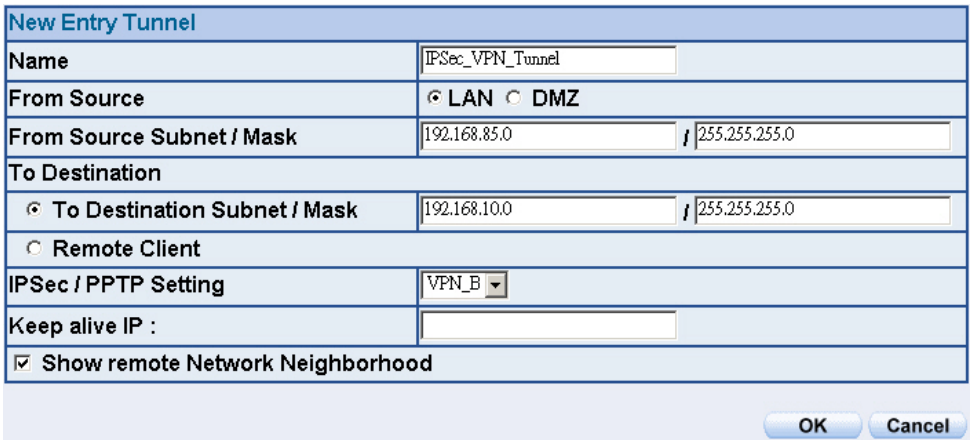


Figure11-28 New Entry Tunnel Setting

Figure11-29 Complete New Entry Tunnel Setting

STEP 11. Enter the following setting in **Outgoing Policy:** (Figure11-30)

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure11-31)

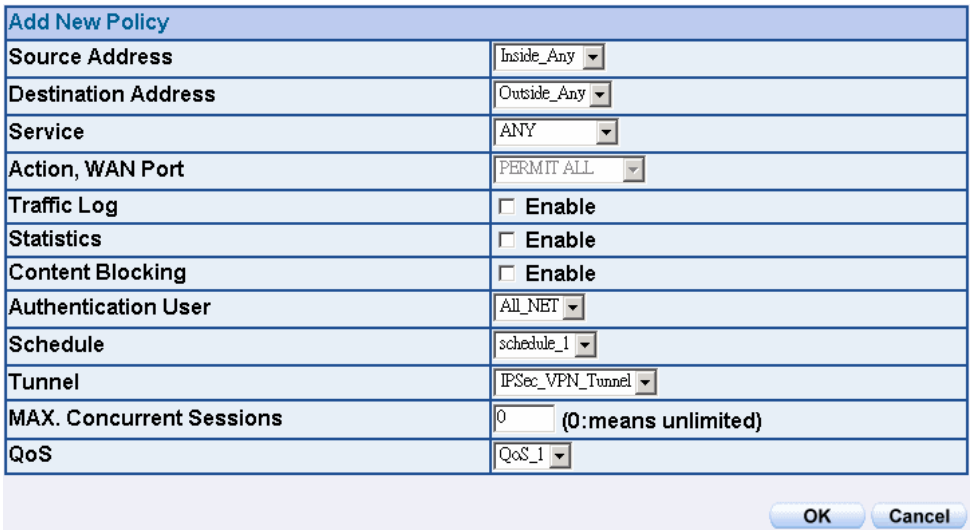


Figure11-30 Setting the VPN Tunnel Outgoing Policy

Figure11-31 Complete the VPN Tunnel Outgoing Policy Setting

STEP 12. Enter the following setting in **Incoming Policy:** (Figure11-32)

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**.(Figure11-33)

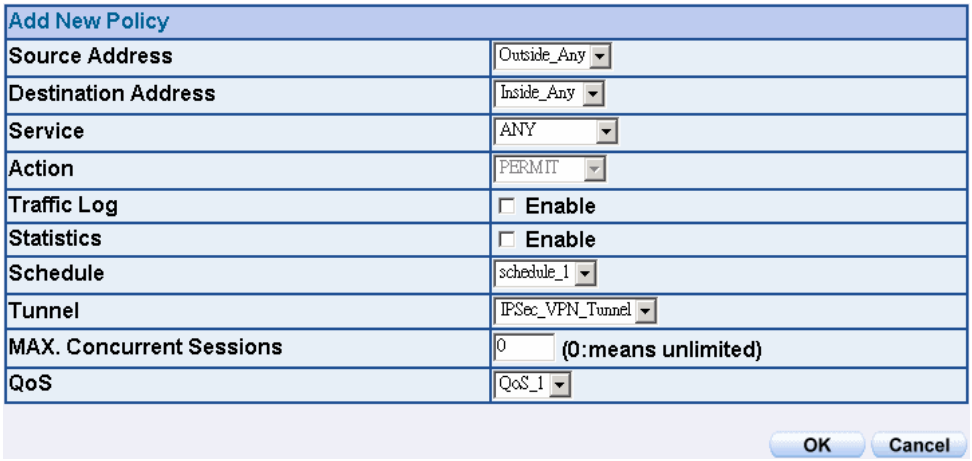


Figure11-32 Setting the VPN Tunnel Incoming Policy

Figure11-33 Complete the VPN Tunnel Incoming Policy Setting

STEP 13. Complete IPSec VPN Connection. (Figure11-34)

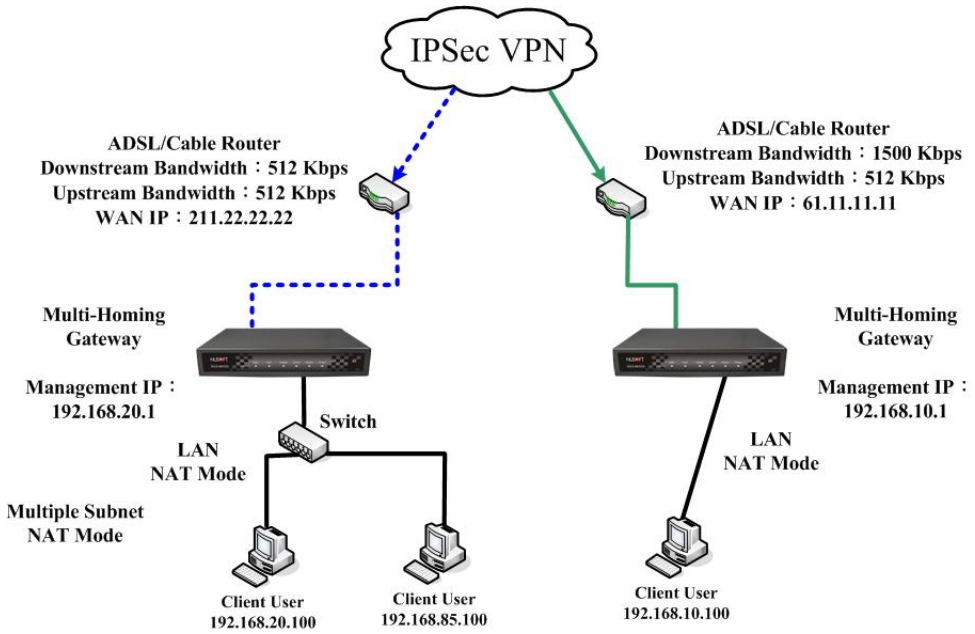


Figure 11-34 IPSec VPN Connection Deployment

Setting PPTP VPN connection between two ALL7000

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 ALL7000 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 ALL7000 192.168.10.1. Follow the steps below:

STEP 1. Enter **PPTP Server** of **VPN** function in the ALL7000 of Company A.

Select **Modify** and enable PPTP Server:

- Select **Encryption**.
- **Client IP Range**: Enter 192.44.75.1-254.
- Idle Time: Enter 0. (Figure11-35)

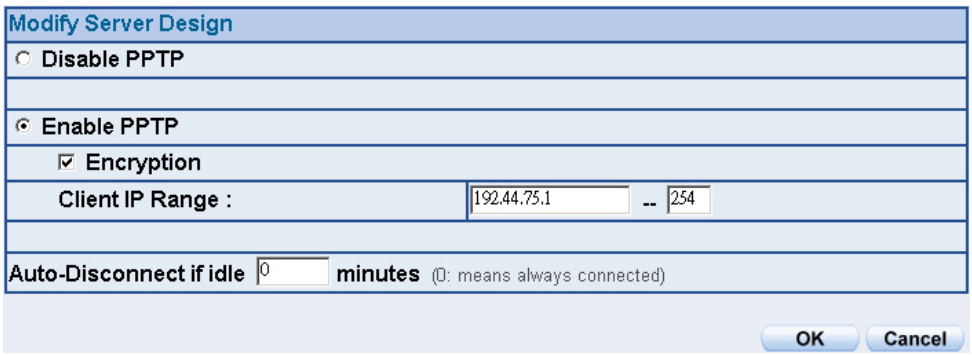


Figure11-35 Enable PPTP VPN Server Settings

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 ALL7000 of Company A:

- Select **New Entry**. (Figure11-36)
- **User Name**: Enter PPTP_Connection.
- **Password**: Enter 123456789.
- **Client IP assigned by**: Select **IP Range**.
- Click **OK**. (Figure11-37)

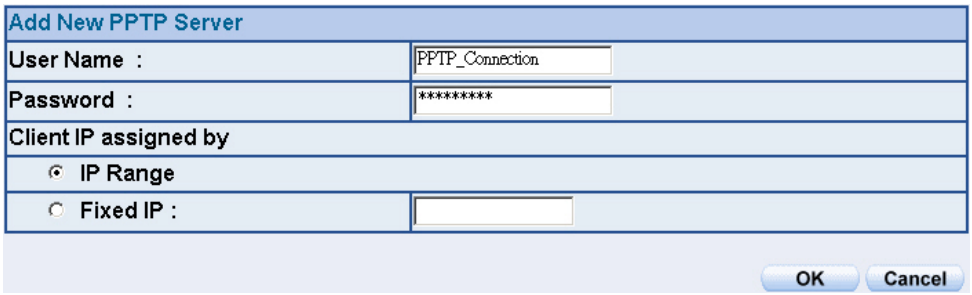


Figure 11-36 PPTP VPN Server Setting

Figure 11-37 Complete PPTP VPN Server Setting

STEP 3. Enter the following setting in **Tunnel** of **VPN** function**:** (Figure11-38)

- 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**. (Figure11-39)

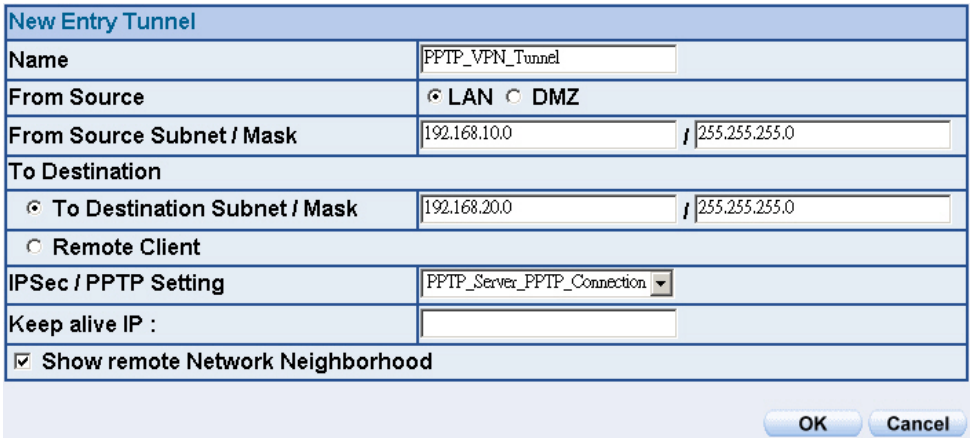


Figure11-38 New Entry Tunnel Setting

Figure11-39 Complete New Entry Tunnel Setting

STEP 4. Enter the following setting in **Outgoing Policy:** (Figure11-40)

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure11-41)

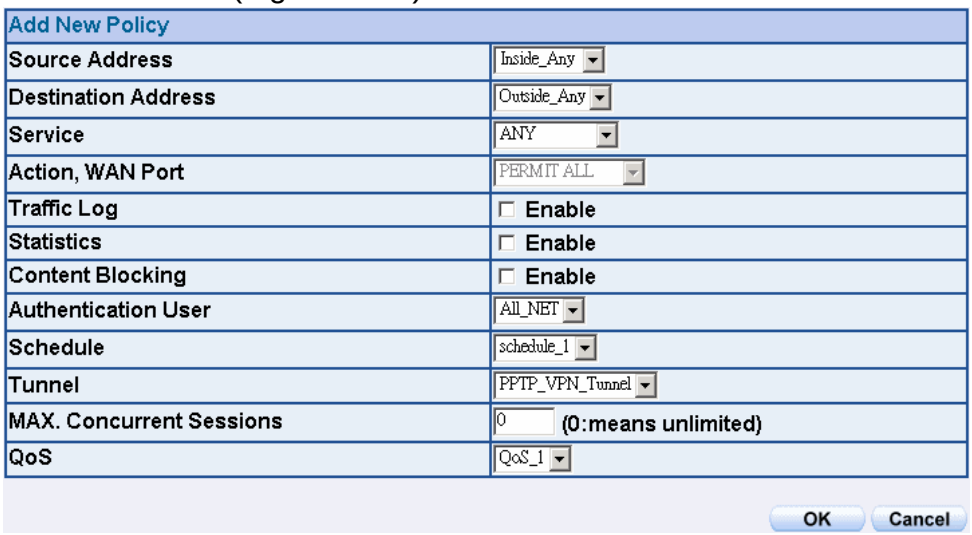


Figure11-40 Setting the VPN Tunnel Outgoing Policy

Figure11-41 Complete the VPN Tunnel Outgoing Policy Setting

STEP 5. Enter the following setting in **Incoming Policy:** (Figure11-42)

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure11-43)

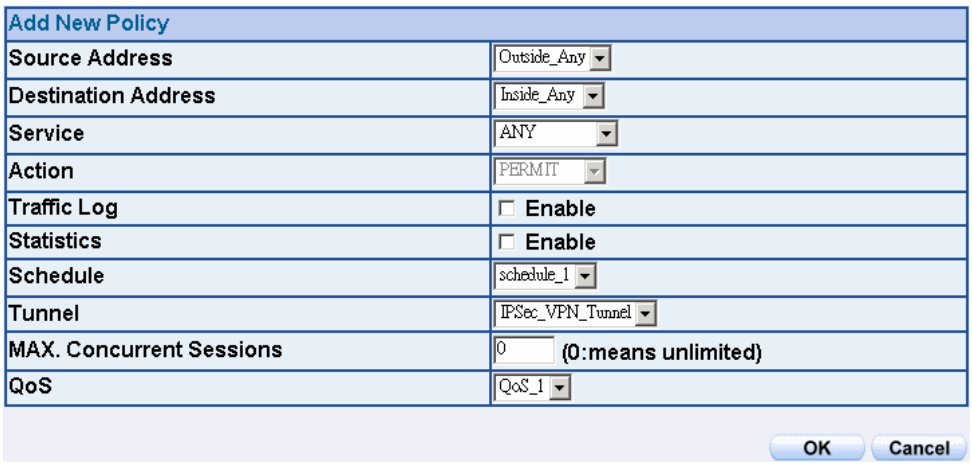


Figure11-42 Setting the VPN Tunnel Incoming Policy

Figure11-43 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the ALL7000 192.168.20.1. Follow the steps below:

STEP 1. Add the following settings in **PPTP Client** of **VPN** function in the ALL7000 of Company B:

- Click **New Entry** Button. (Figure11-44)
- **User Name**: Enter PPTP_Connection.
- **Password**: Enter123456789.
- **Server IP or Domain Name**: Enter 61.11.11.11.
- Select **Encryption**.
- Click **OK**. (Figure11-45)

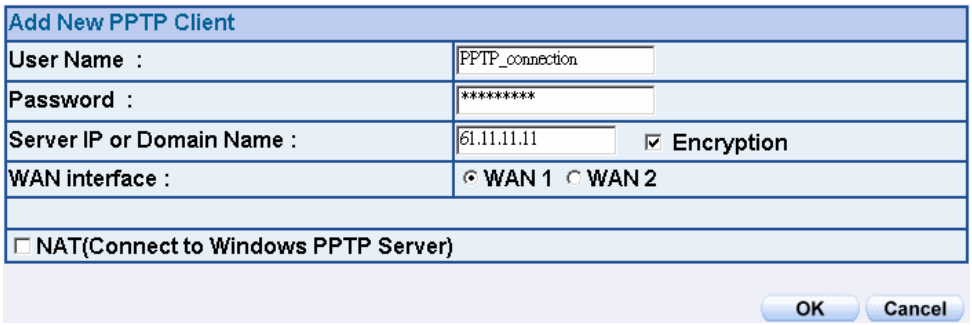


Figure 11-44 PPTP VPN Client Setting

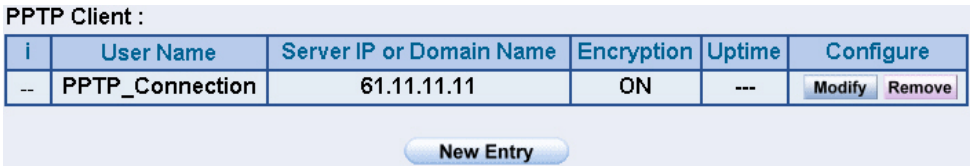


Figure 11-45 Complete PPTP VPN Client Setting

STEP 2. Enter the following setting in **Tunnel** of **VPN** function**:** (Figure11-46)

- 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**. (Figure11-47)

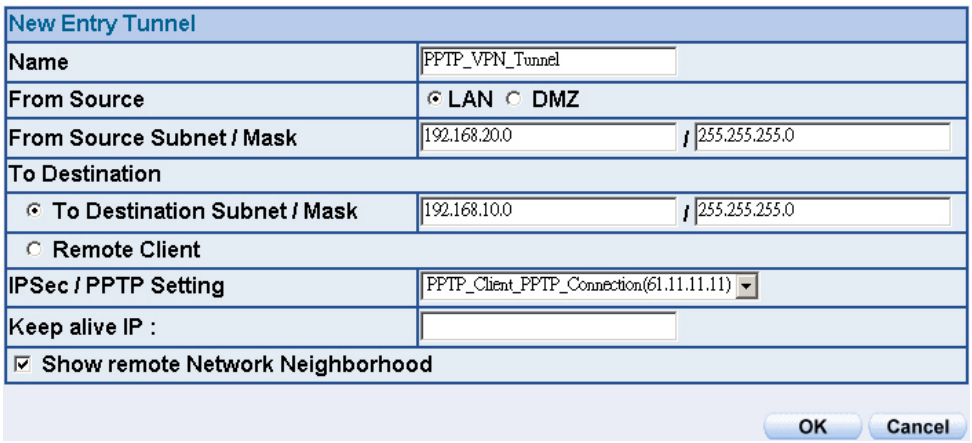


Figure11-46 New Entry Tunnel Setting

Figure11-47 Complete New Entry Tunnel Setting

STEP 3. Enter the following setting in **Outgoing Policy:** (Figure11-48)

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure11-49)

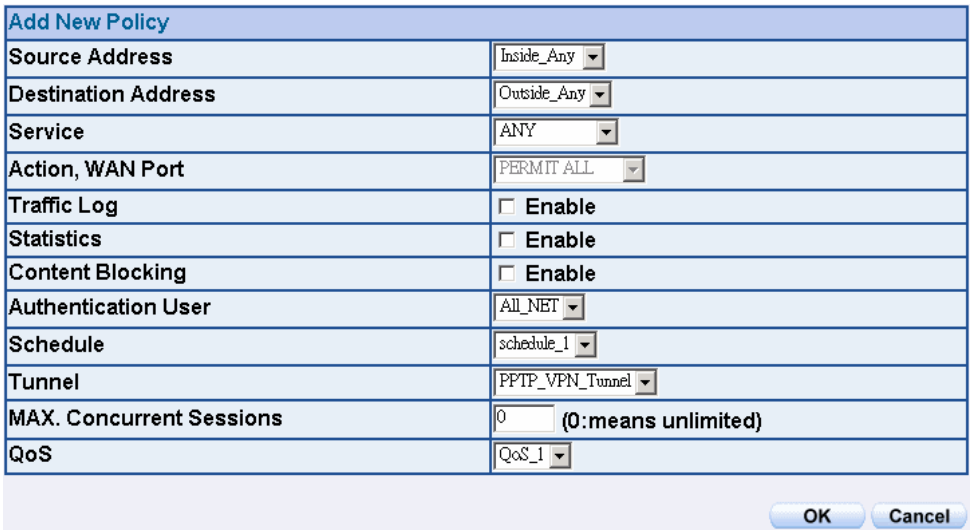


Figure11-48 Setting the VPN Tunnel Outgoing Policy

Figure11-49 Complete the VPN Tunnel Outgoing Policy Setting

STEP 4. Enter the following setting in **Incoming Policy:** (Figure11-50)

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**.(Figure11-51)

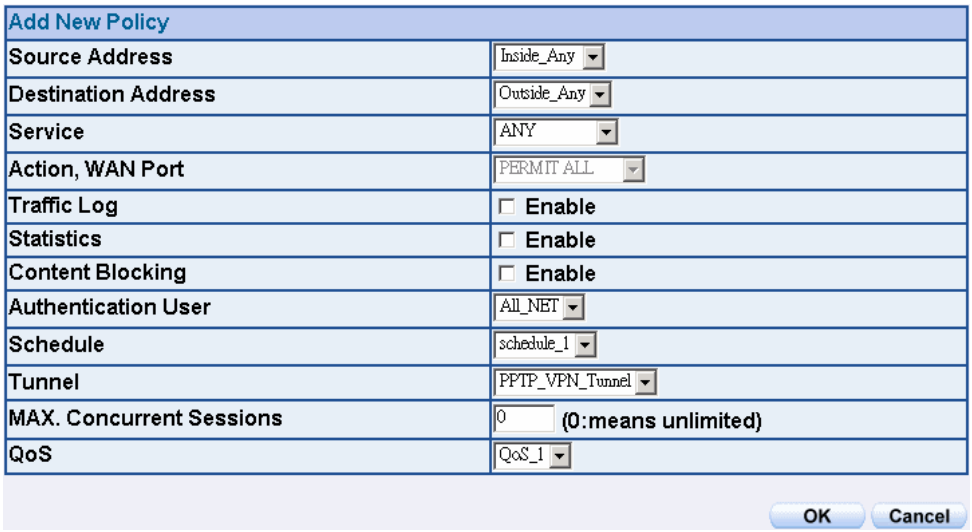


Figure11-50 Setting the VPN Tunnel Incoming Policy

Figure11-51 Complete the VPN Tunnel Incoming Policy Setting

STEP 5. Complete PPTP VPN Connection. (Figure11-52)

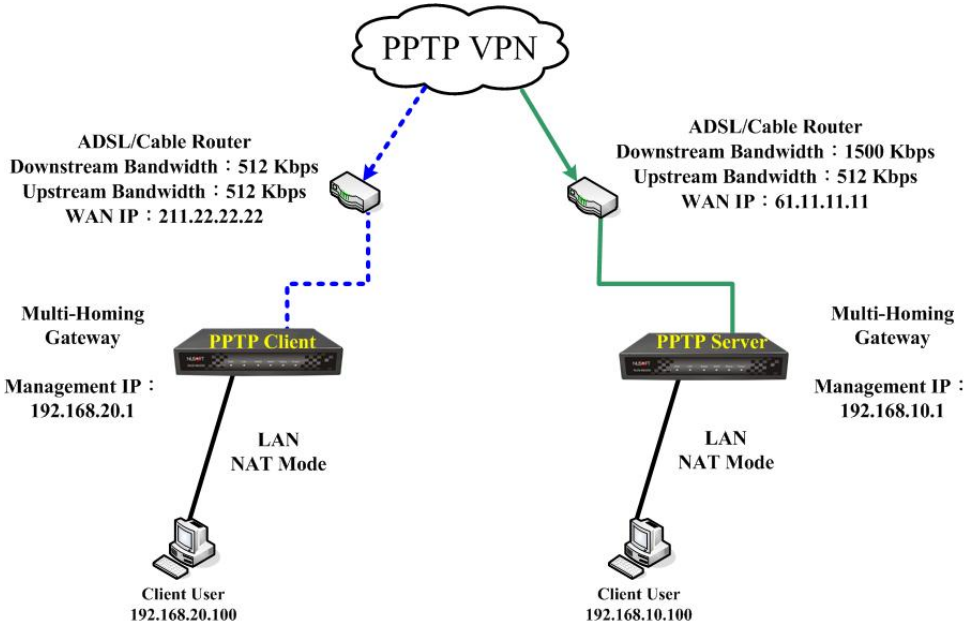


Figure 11-52 PPTP VPN Connection Deployment

Chapter 12

Policy

Every packet has to be detected if it corresponds with Policy or not when it passes the ALL7000. When the conditions correspond with certain policy, it will pass the ALL7000 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, Action, WAN Port, Traffic Log, Statistics, Content Blocking, Anti-Virus, Authentication User, Schedule, Alarm Threshold, Trunk, Max. Concurrent Sessions, and QoS. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the ALL7000.

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 alarm. 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 ALL7000 must pass the policy permission (except VPN). 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 ALL7000'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 ALL7000 (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

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
	Traffic Log	Enable traffic log
	Statistics	Enable traffic statistics
	Authentication User	Enable Authentication User
	Schedule	Enable the policy to automatically execute the function in a certain time
	Content Blocking	Enable Content Blocking
	QoS	Enable QoS

Traffic Log:

- Record all the packets that go through policy.

Statistics:

- Chart of the traffic that go through policy

Content Blocking:

- To restrict the packets that passes through the policy

Authentication-User:

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

Schedule:

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

MAX. Concurrent Sessions:

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

QoS:

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

Move:

- Every packet that passes the ALL7000 is detected from the front policy to the last one. So it can modify the priority of the policy from the selection.

We set up six Policy examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	**Outgoing**	Set up the policy that can monitor the internal users. (Take Logging, Statistics, Alarm Threshold for example)	**163**
Ex2	**Outgoing**	Forbid the users to access to specific network. (Take specific WAN IP and Content Blocking for example)	**166**
Ex3	**Outgoing**	Only allow the users who pass Authentication to access to Internet in particular time.	**171**
Ex4	**Incoming**	The external user control the internal PC through remote control software (Take pcAnywhere for example)	**173**
Ex5	**WAN to DMZ**	Under DMZ NAT Mode, set a FTP Server and restrict the download bandwidth from external and MAX. Concurrent Sessions.	**175**
Ex6	**WAN to DMZ** **DMZ to WAN** **LAN to DMZ**	Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode	**177**

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 **Logging**
- Select **Statistics**
- Click **OK** (Figure12-1)

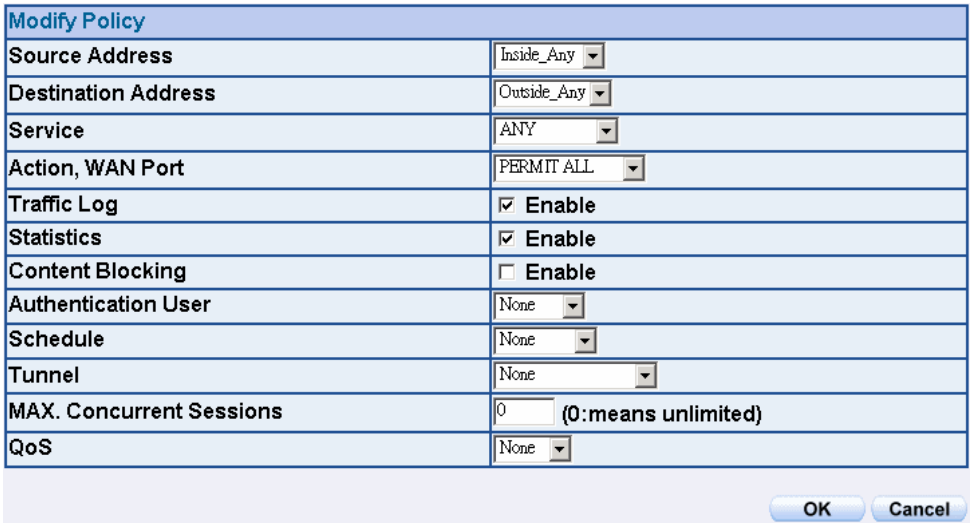


Figure12-1 Setting the different Policies

STEP 2 . Complete the setting of Logging, Statistics, and Alarm Threshold in **Outgoing Policy**: (Figure12-2)

Figure12-2 Complete Policy Setting

STEP 3 . Obtain the information in **Traffic** of **Log** function if you want to monitor all the packets of the ALL7000. (Figure12-3)

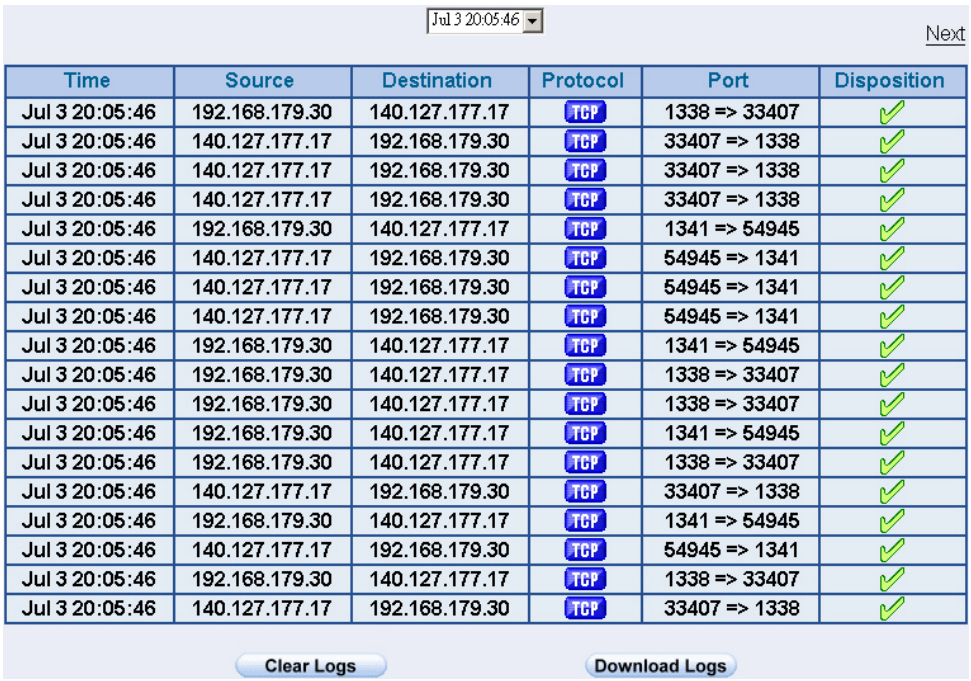


Figure12-3 Traffic Log Monitor WebUI

STEP 4． To display the traffic record that through Policy to access to Internet in **Policy Statistics** of **Statistics** function. (Figure12-4)

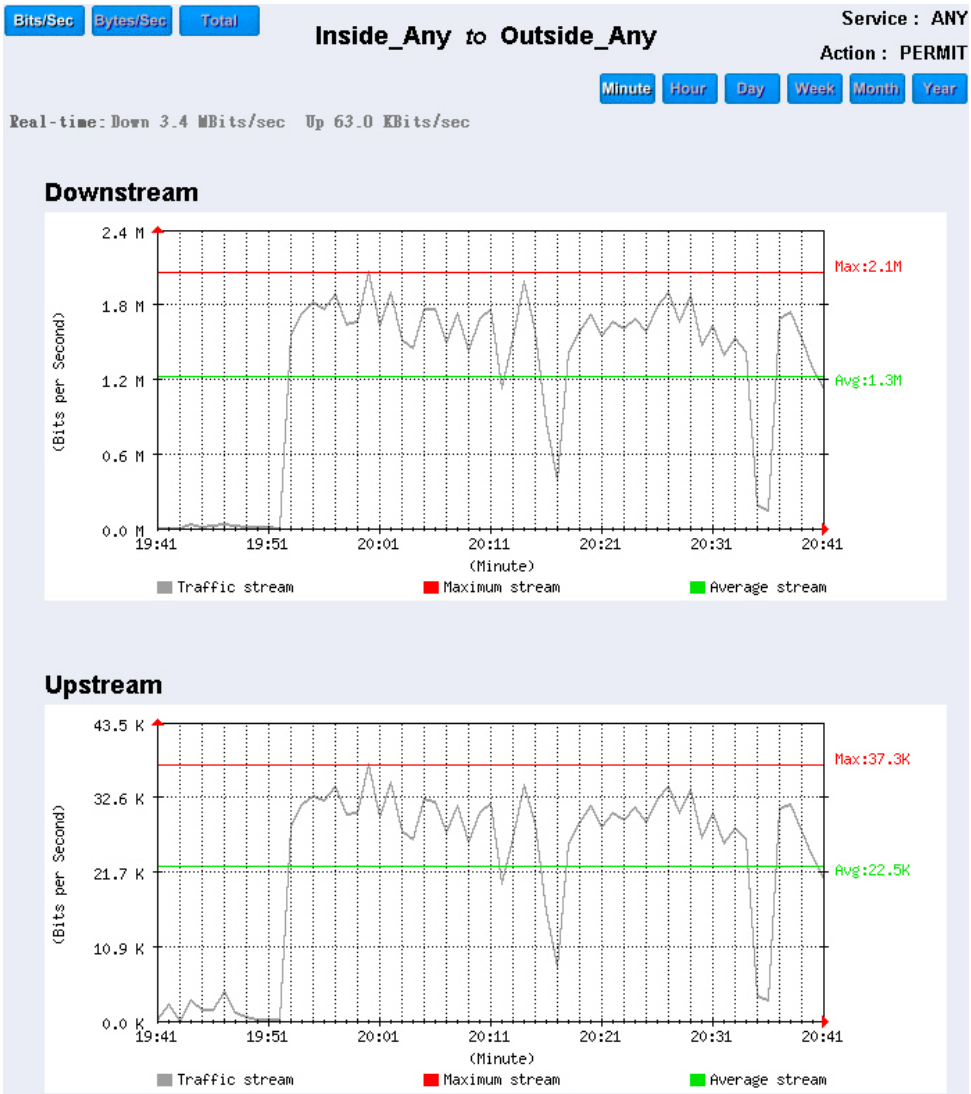


Figure12-4 Statistics WebUI

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

STEP 1 . Enter the following setting in **URL Blocking, Script Blocking, P2P Blocking, IM Blocking,** and **Download Blocking** in **Content Blocking** function: (Figure12-5, 12-6, 12-7, 12-8, 12-9)

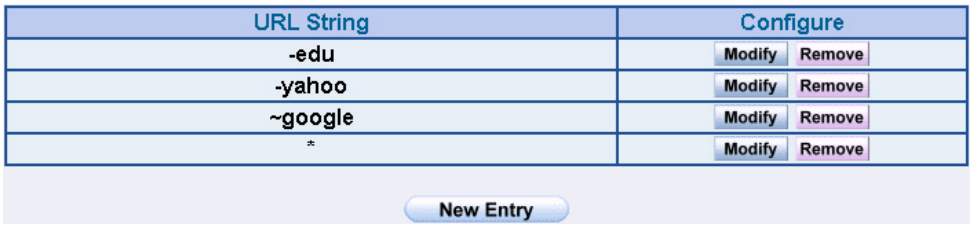


Figure12-5 URL Blocking Setting

Figure12-6 Script Blocking Setting

Figure12-7 P2P Blocking Setting

Figure12-8 IM Blocking Setting

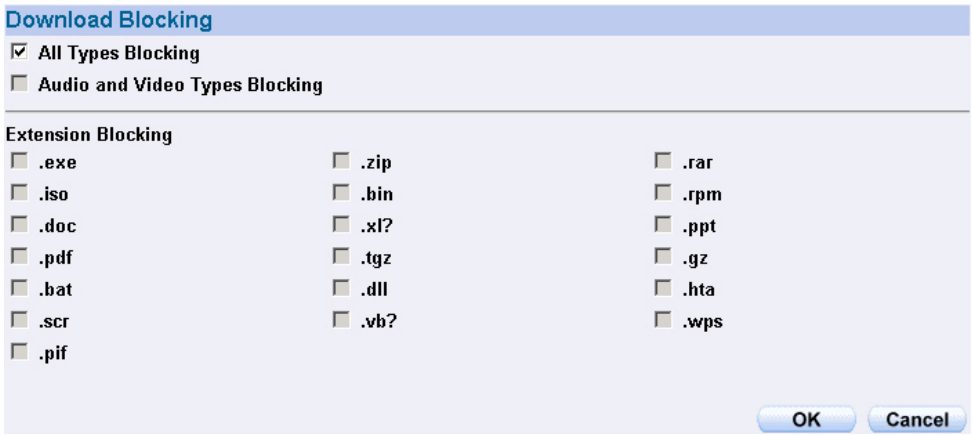


Figure12-9 Download Blocking Setting

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

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

3. P2P Blocking can restrict the Internal Users to access to the file on Internet by P2P. (eDonkey, BT)

4. IM Blocking can restrict the Internal Users to send message, files, audio, and video by instant messaging. (Ex: MSN Messenger, Yahoo Messenger, QQ, ICQ and Skype)

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

STEP 2． Enter as following in **WAN** and **WAN Group** of **Address** function: (Figure12-10, 12-11)

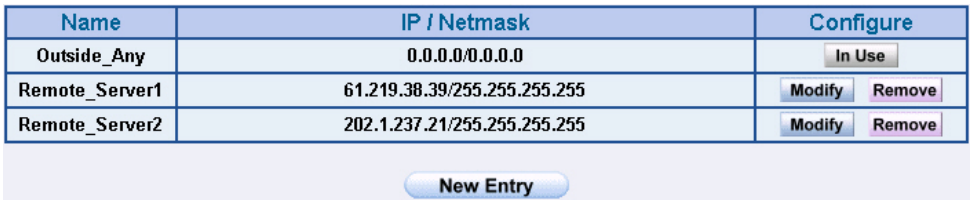


Figure12-10 Setting the WAN IP that going to block

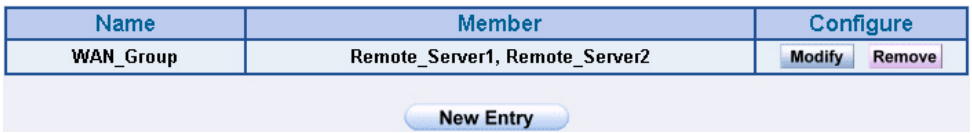


Figure12-11 WAN Address Group

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**
- Click **OK** (Figure12-12)

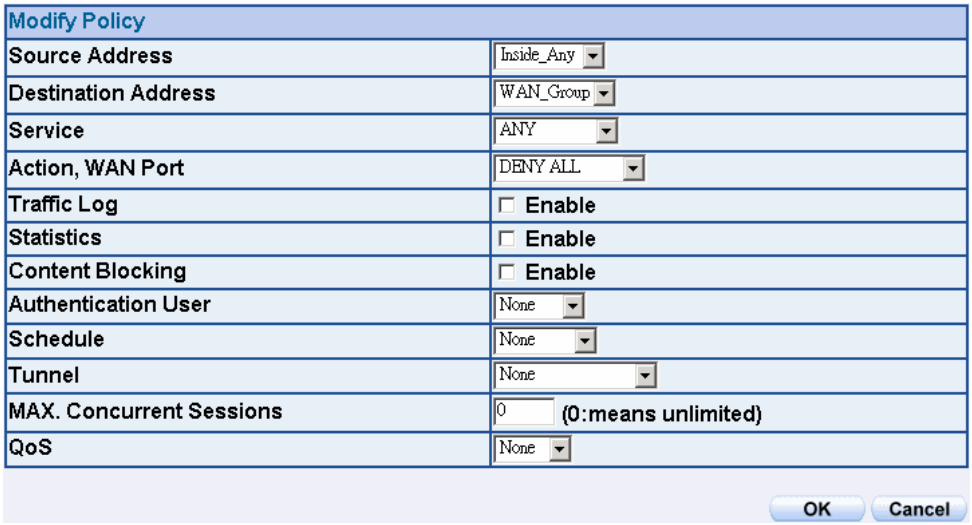


Figure12-12 Setting Blocking Policy

STEP 4 . Enter the following setting in **Outgoing Policy**:

- Click **New Entry**
- Select **Content Blocking**
- Click **OK** (Figure12-13)

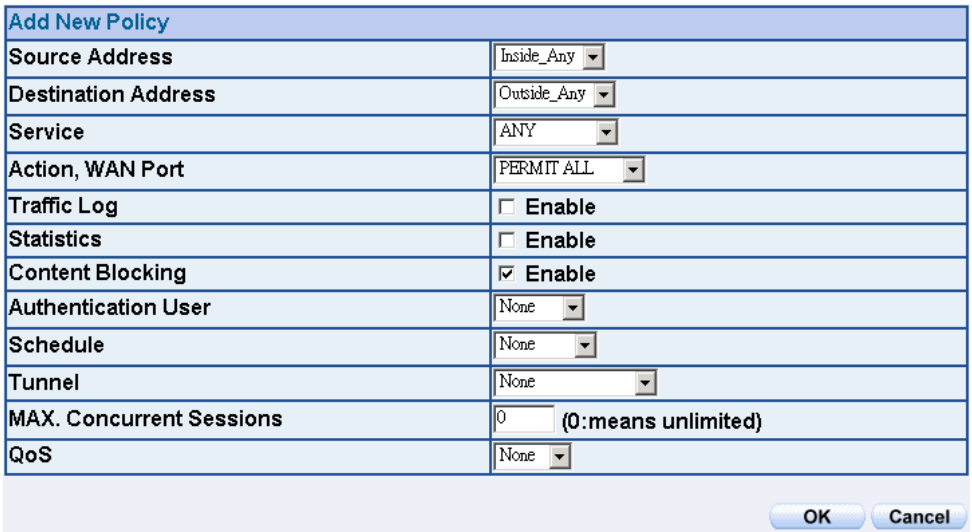


Figure12-13 Setting Content Blocking Policy

STEP 5 . Complete the setting of forbidding the users to access to specific network. (Figure12-14)

Figure12-14 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: (Figure12-15)

Figure12-15 Add New Schedule

STEP 2 . Enter the following in **Auth User** and **Auth User Group** in **Authentication** function**:** (Figure12-16)

Figure12-16 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 WorkingTime
- Click **OK** (Figure12-17)

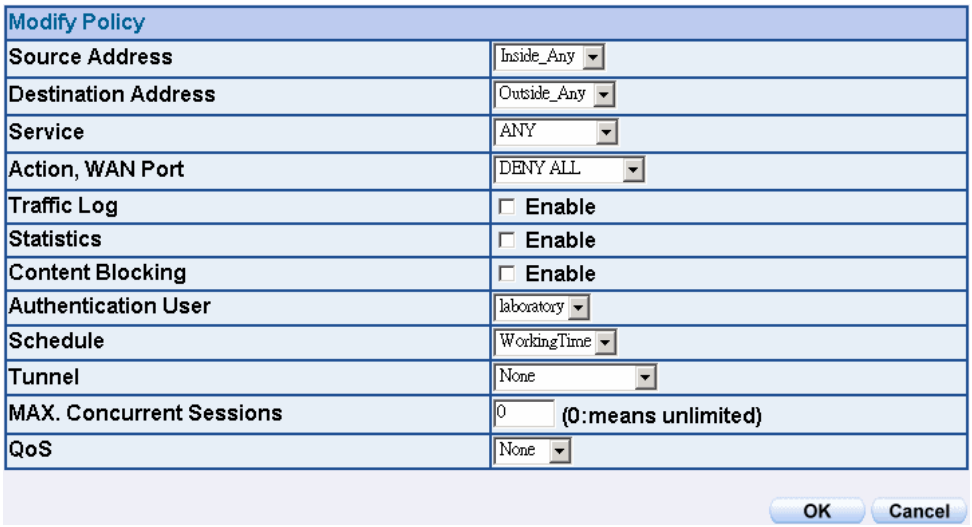


Figure12-17 Setting a Policy of Authentication and Schedule

STEP 4 . Complete the policy rule of only allows the users who pass authentication to access to Internet in particular time. (Figure12-18)

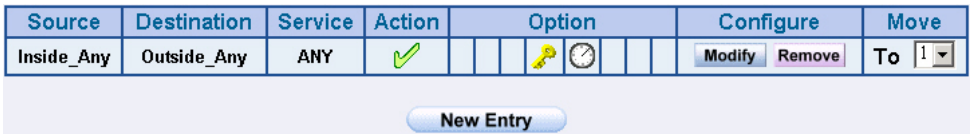


Figure12-18 Complete Policy Setting

The external user control 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**:** (Figure12-19)

Figure12-19 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** (Figure12-20)

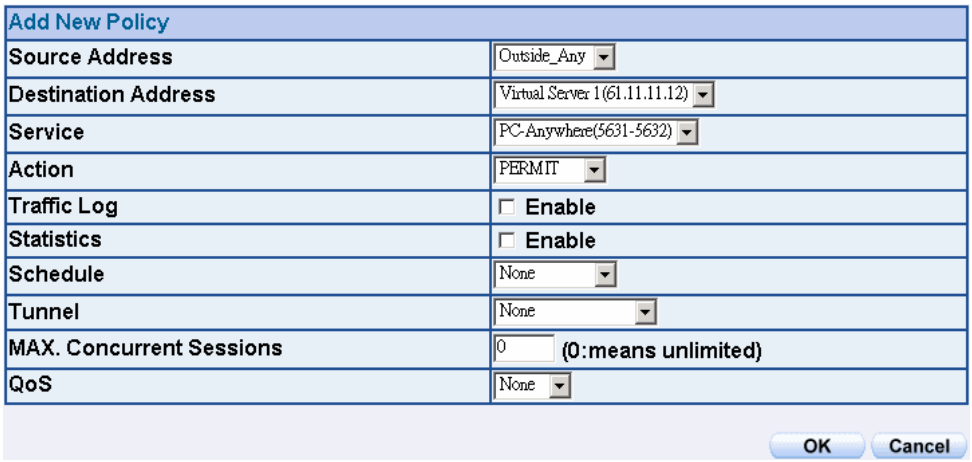


Figure12-20 Setting the External User Control the Internal PC Policy

STEP 4 . Complete the policy for the external user to control the internal PC through remote control software. (Figure12-21)

Figure12-21 Complete Policy Setting

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

STEP 1． Set a FTP Server under **DMZ**, which IP is 192.168.3.2 (The DMZ Interface Address is192.168.3.1/24)

STEP 2． Enter the following setting in **Virtual Server1** of **Virtual Server** function**:** (Figure12-22)

Virtual Server Real IP 61.11.11.12

Service	WAN Port	Server Virtual IP	Configure
FTP (21)	21	192.168.3.2	Modify Remove

New Entry

Figure12-22 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 being attacked by Hacker easily.

STEP 3． Enter the following in **QoS:** (Figure12-23)

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP_QoS	1	G.Bandwidth = 100Kbps M.Bandwidth = 500Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 200 Kbps	Middle	Modify Remove
	2	G.Bandwidth = 500Kbps M.Bandwidth = 512Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 60 Kbps		

New Entry

Figure12-23 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** (Figure12-24)

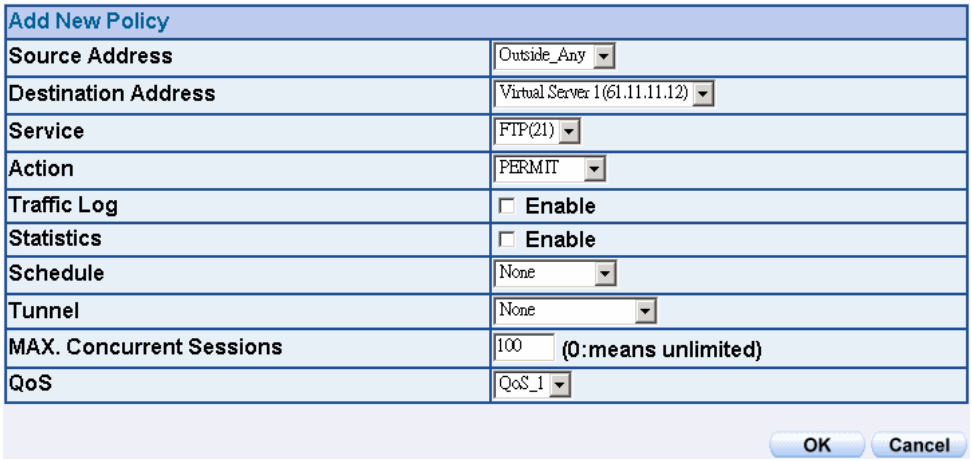


Figure12-24 Add New Policy

STEP 5 . Complete the policy of restricting the external users to access to internal network server (which may occupy the resource of network) (Figure12-25)

Figure12-25 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**:** (Figure12-26)

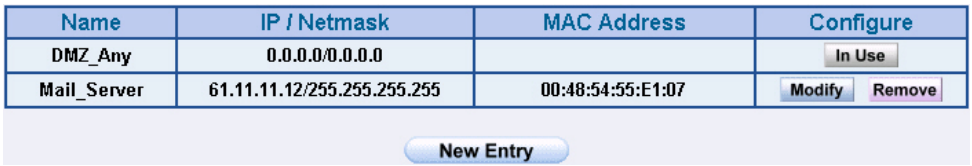


Figure12-26 the Mail Server's IP Address Corresponds to Name Setting in Address Book of Mail Server

STEP 3． Add the following setting in **Group** of **Service** function: (Figure12-27)

Figure12-27 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** (Figure12-28)

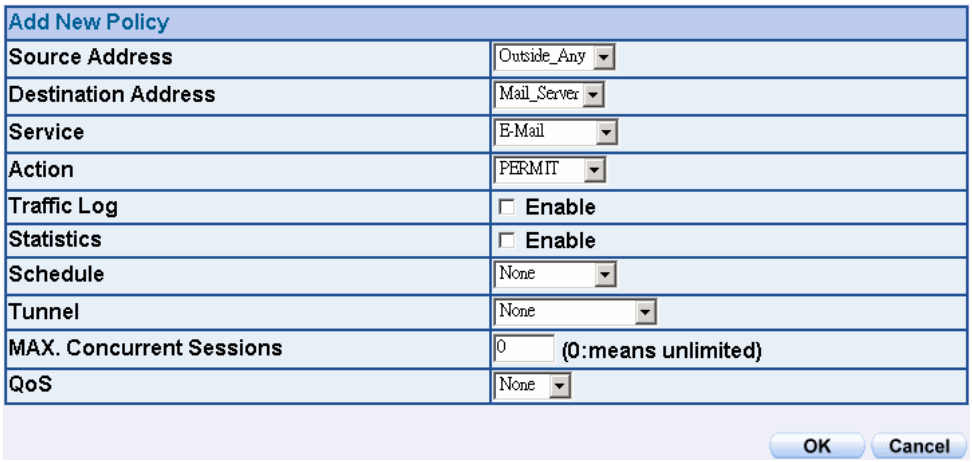


Figure12-28 Setting a Policy to access Mail Service by WAN to DMZ

STEP 5 . Complete the policy to access mail service by **WAN to DMZ**. (Figure12-29)

Figure12-29 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** (Figure12-30)

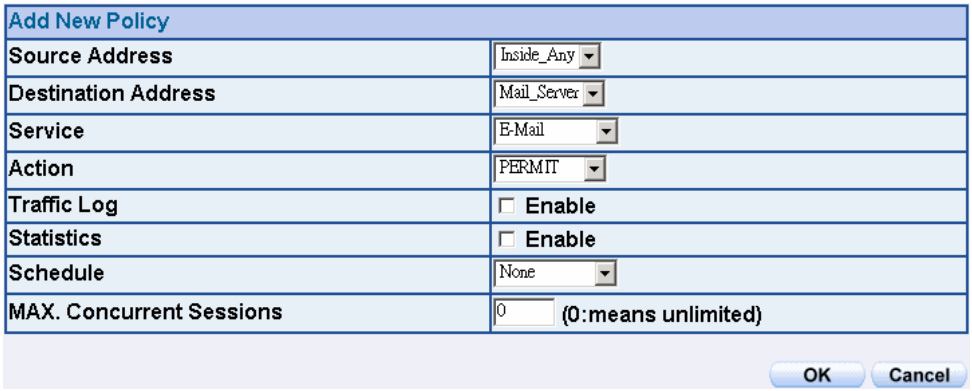


Figure12-30 Setting a Policy to access Mail Service by LAN to DMZ

STEP 7 . Complete the policy to access mail service by **LAN to DMZ** (Figure12-31)

Figure12-31 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** (Figure12-32)

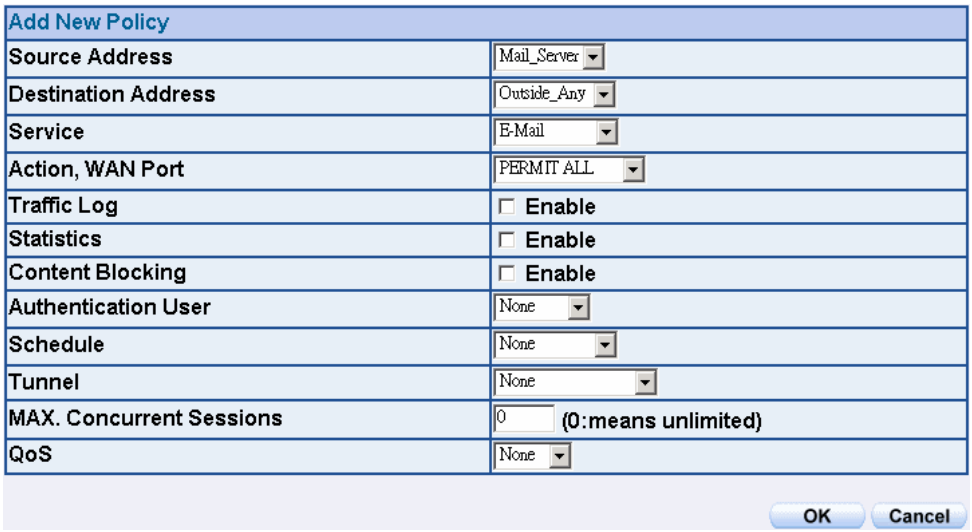


Figure12-32 Setting the Policy of Mail Service by DMZ to WAN

STEP 9 . Complete the policy access to mail service by **DMZ to WAN**. (Figure12-33)

Figure12-33 Complete the Policy access to Mail Service by DMZ to WAN

Chapter 16

Alert Setting

When the ALL7000 had detected attacks from hackers and the internal PC sending large DDoS attacks. The **Internal Alert** and **External Alert** will start on blocking these packets to maintain the whole network.

In this chapter, we will have the detailed illustration about **Internal Alert** and **External Alert:**

Define the required fields of Hacker Alert

Detect SYN Attack:

- Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will cause valid users cannot connect to the servers.
  - **【SYN Flood Threshold(Total) Pkts/Sec】:** The system Administrator can enter the maximum number of SYN packets per second that is allowed to enter the network/ALL7000. If the value exceeds the setting one, and then the device will determine it as an attack.
  - **【SYN Flood Threshold(Per Source IP) Pkts/Sec】:** The system Administrator can enter the maximum number of SYN packets per second from attacking source IP Address that is allowed to enter the network/ALL7000. And if value exceeds the setting one, and then the device will determine it as an attack.
  - **【SYN Flood Threshold Blocking Time(Per Source IP) Seconds】:** When the ALL7000 determines as being attacked, it will block the attacking source IP address in the blocking time you set. After blocking for certain seconds, the device will start to calculate the max number of SYN packets from attacking source IP Address. And if the max number still exceed the define value, it will block the attacking IP Address continuously.

Detect ICMP Attack:

- When Hackers continuously send PING packets to all the machines of the LAN networks or to the ALL7000 via broadcasting, your network is experiencing an ICMP flood attack.
  - **【ICMP Flood Threshold(Total) Pkts/Sec】:** The System Administrator can enter the maximum number of ICMP packets per second that is allow to enter the network/ALL7000. If the value exceeds the setting one, and then the device will determine it as an attack.
  - **【ICMP Flood Threshold(Per Source IP)Pkts/Sec】:** The System

Administrator can enter the maximum number of ICMP packets per second from attacking source IP Address that is allow to enter the network / ALL7000. If the value exceeds the setting one, and then the device will determine it as an attack.

- **【ICMP Flood Threshold Blocking Time(Per Source IP)Seconds】:**When the ALL7000 determines as being attacked, it will block the attacking source IP address in the blocking time you set. After blocking for certain seconds, the device will start to calculate the max number of ICMP packets from attacking source IP Address. And if the max number still exceed the define value, it will block the attacking IP Address continuously.

Detect UDP Attack:

- When Hackers continuously send PING packets to all the machines of the LAN networks or to the ALL7000 via broadcasting, your network is experiencing an UDP attack.
  - **【UDP Flood Threshold(Total)Pkts/Sec】:** The System Administrator can enter the maximum number of UDP packets per second that is allow to enter the network/ALL7000. If the value exceeds the setting one, and then the device will determine it as an attack.
  - **【UDP Flood Threshold(Per Source IP)Pkts/Sec】:** The System Administrator can enter the maximum number of UDP packets per second from attacking source IP Address that is allow to enter the network/ALL7000. If the value exceeds the setting one, and then the device will determine it as an attack.
  - **【UDP Flood Threshold Blocking Time (Per Source IP) Seconds】:** When ALL7000 determines as being attacked, it will block the attacking source IP in the blocking time you set. After blocking for certain seconds, the device will start to calculate the max number of UPD packets from attacking source IP. If the max number still exceed the define value, it will block the attacking IP Address continuously.

Detect Ping of Death Attack:

- Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction. This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.

Detect IP Spoofing Attack:

- Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the ALL7000 System and invade the network.

Detect Port Scan Attack:

- Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.

Detect Tear Drop Attack:

- Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.

Filter IP Route Option:

- Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade LAN networks and send LAN networks' data back to them.

Detect 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.

 After System Manager enable **External Alert**, if the ALL7000 has detected any abnormal situation, the alarm message will appear in **External Alarm** in **Attack Alarm**. 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.

ALL7000 Alarm and to prevent the computer which being attacked to send DDoS packets to LAN network

STEP 1 . Select **Internal Alert** in **Alert Setting** and enter the following settings:

- Enter **The threshold sessions of infected Blaster (per Source IP)** (the default value is 30 Sessions/Sec)
- Select **Enable Blaster Blocking** and enter the **Blocking Time** (the default time is 60 seconds)
- Select **Enable E-Mail Alert Notification**
- Select **Enable NetBIOS Alert Notification**
- **IP Address of Administrator:** Enter 192.168.1.10
- Click **OK**
- Internal Alert Setting is completed. (Figure16-1)

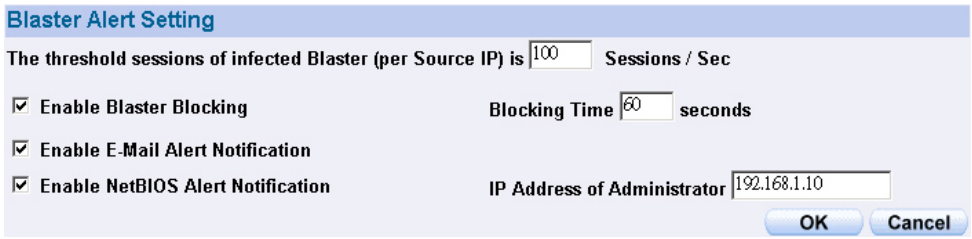


Figure16-1 Internal Alert Settings

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 **Internal Alarm** in **Attack Alarm** or send NetBIOS Alert notification to the infected PC Administrator's PC (Figure16-2, 16-3, 16-4)

If the Administrator starts the **E-Mail Alert Notification** in **Setting**, the ALL7000 will send e-mail to Administrator automatically. (Figure16-5)

Interface	Virus infected IP	Alarm Time
LAN	192.168.1.2	2004-11-15 12:03:41

Figure16-2 Internal Alert Record

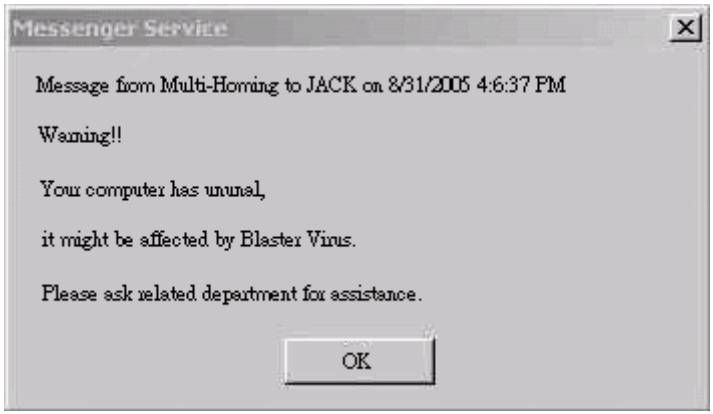


Figure16-3 NetBIOS Alert Notification to the Infected PC

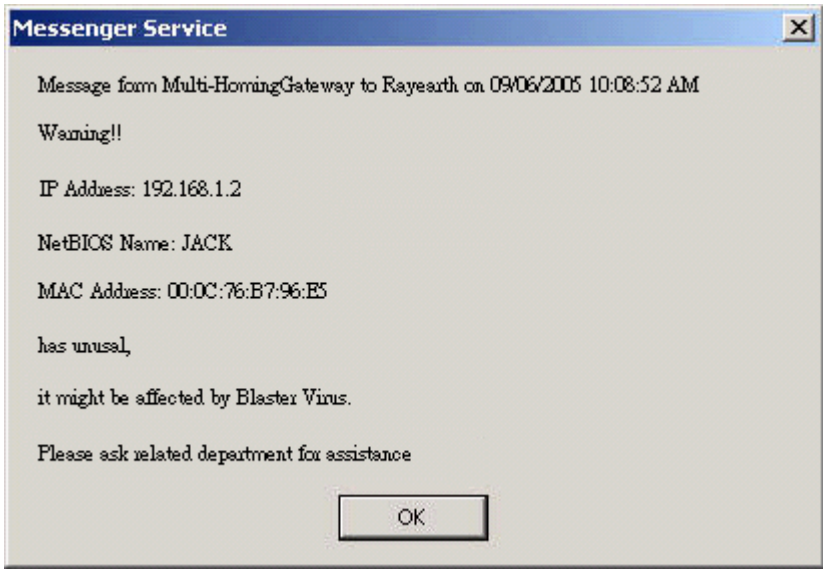


Figure16-4 NetBIOS Alert Notification to Administrator's PC

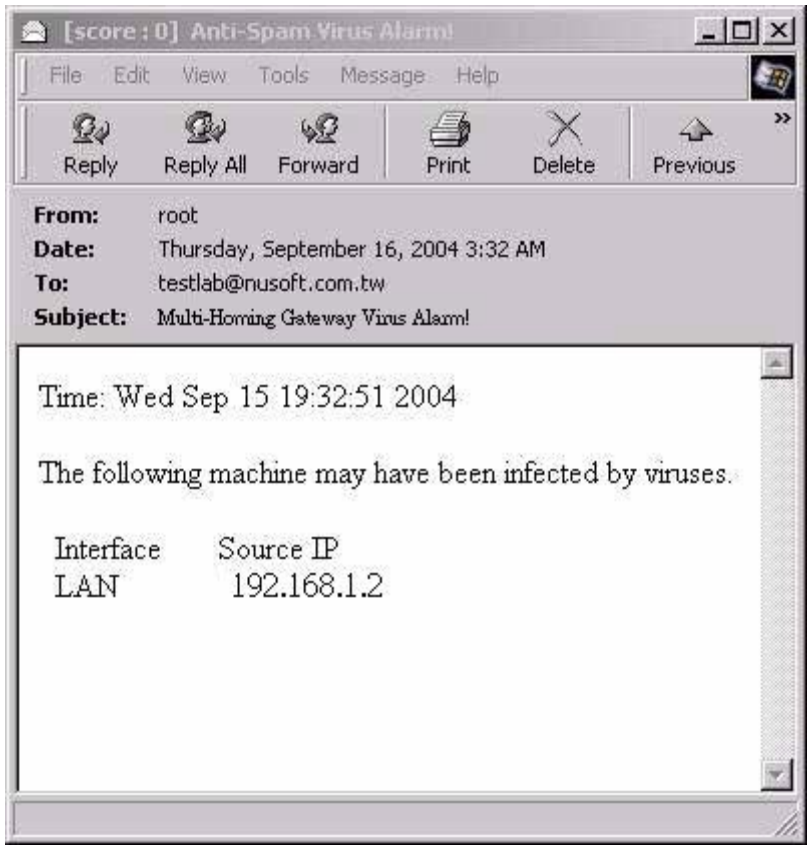


Figure16-5 E-mail Virus Alert

Chapter 17

Attack Alarm

ALL7000 has two alarm forms: **Internal Alarm,** and **External Alarm**.

Internal Alarm: When the ALL7000 had detected the internal PC sending large DDoS attacks and then the Internal Alarm will start on blocking these packets to maintain the whole network.

External Alarm: When ALL7000 detects attacks from hackers, it writes attacking data in the External Alarm file and sends an e-mail alert to the Administrator to take emergency steps.

How to use Attack Alarm

The Administrator can be notified the unusal affair in Intranet from Attack Alarms. And the Administrator can backup the Internal Alarm, and External Alarm and then delete the records to maintain the network status.

We set up two Alarm examples in the chapter:

No.	Suitable Situation	Example	Page
Ex 1	**Internal Alarm**	To record the DDoS attack alarm from internal PC	**192**
Ex 2	**External Alarm**	To record the attack alarm about Hacker attacks the ALL7000 and Intranet	**193**

To record the DDoS attack alarm from internal PC

STEP 1． Select **Internal Alarm** in **Attack Alarm** when the device detects DDoS attacks, and then can know which computer is being affected. (Figure17-1)

Interface	Virus infected IP	Alarm Time
DMZ	192.168.1.2	201-11-16 17:45:56

Figure17-1 Internal Alarm WebUI

To record the attack alarm about Hacker attacks the ALL7000 and Intranet

STEP 1． Select the following settings in **External Alert** in **Alert Setting** function: (Figure17-2)

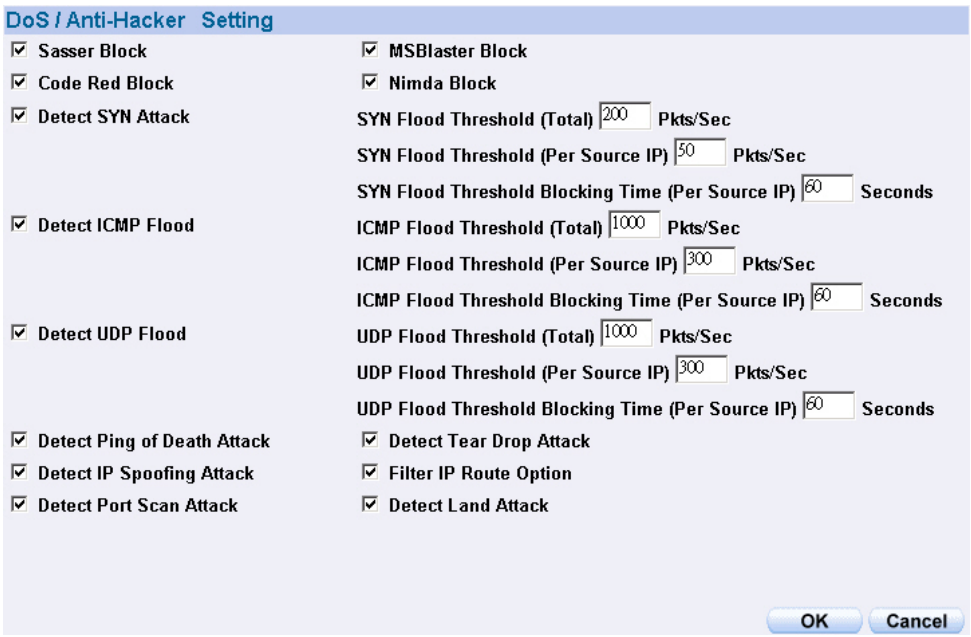


Figure17-2 External Alert Setting WebUI

STEP 2 . When Hacker attacks the ALL7000 and Intranet, select **External Alarm** in **Attack Alarm** function to have detailed records about the hacker attacks. (Figure17-3)

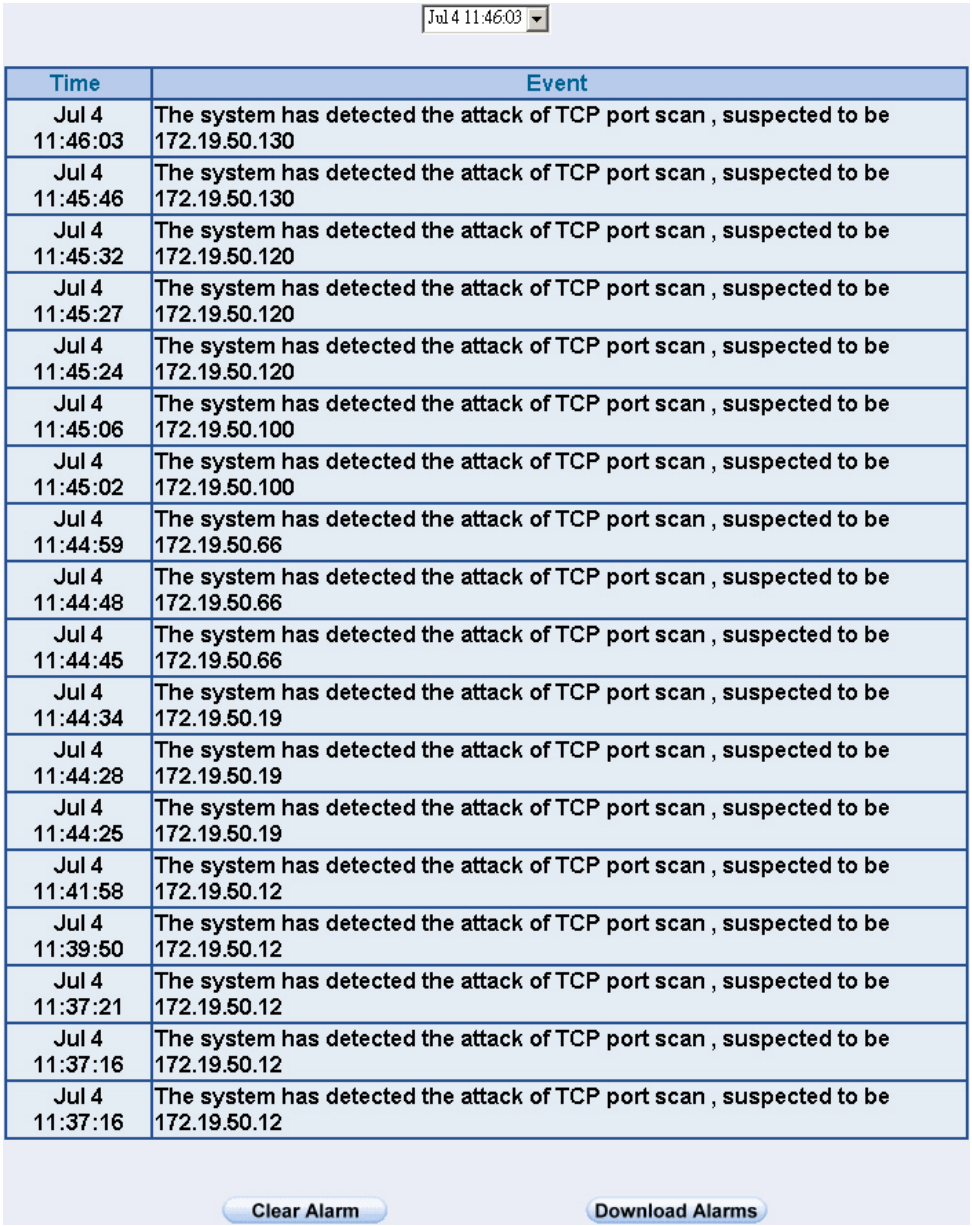


Figure17-3 External Alarm WebUI

Chapter 18

LOG

Log records all connections that pass through the ALL7000'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 ALL7000. When the connection occurs some problem, the Administrator can trace back the problem from the information.

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.

We set up four LOG examples in the chapter:

No.	Suitable Situation	Example	Page
Ex 1	**Traffic Log**	To detect the information and Protocol port that users use to access to Internet or Intranet by ALL7000.	**197**
Ex 2	**Event Log**	To record the detailed management events (such as Interface and event description of ALL7000) of the Administrator	**202**
Ex 3	**Connection Log**	To detect event description of WAN Connection	**205**
Ex 4	**Log Backup**	To save or receive the records that sent by the ALL7000	**208**

To detect the information and Protocol port that users use to access to Internet or Intranet by ALL7000

STEP 1． Add new policy in **DMZ to WAN** of **Policy** and select **Enable Logging**: (Figure18-1)

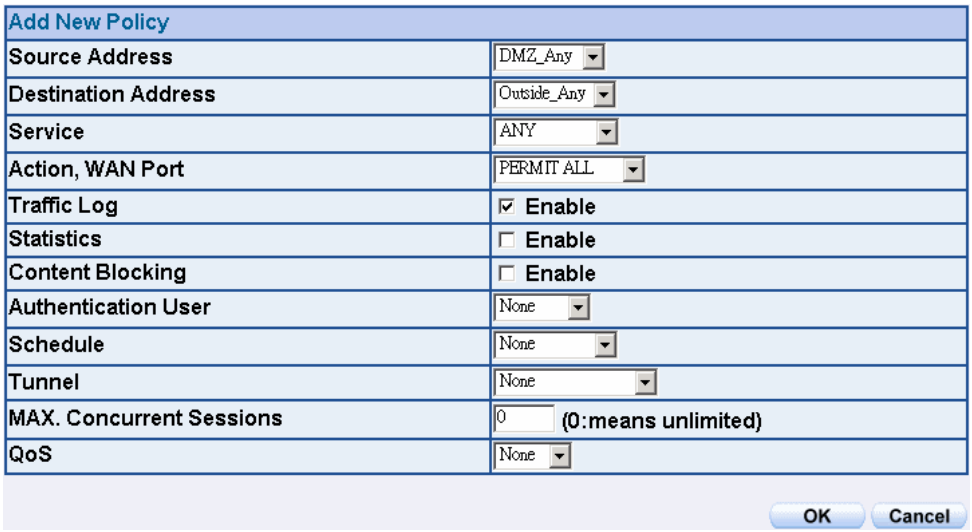


Figure18-1 Logging Policy Setting

STEP 2． Complete the Logging Setting in **DMZ to WAN Policy**: (Figrue18-2)

Figure18-2 Complete the Logging Setting of DMZ to WAN

STEP 3 . Click **Traffic Log**. It will show up the packets records that pass this policy. (Figure18-3)

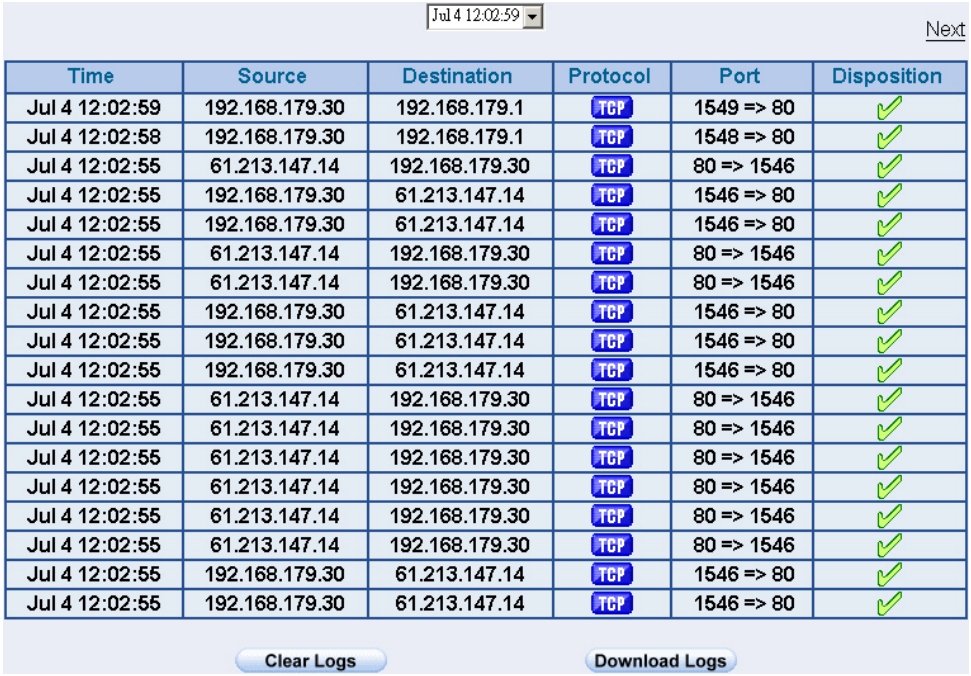
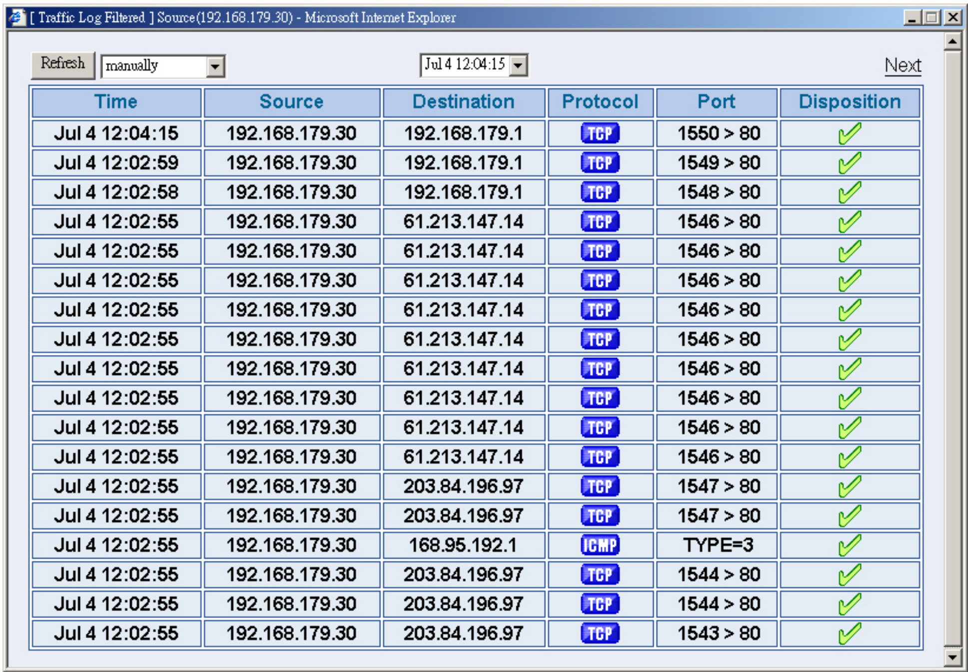


Figure18-3 Traffic Log WebUI

STEP 4 . Click on a specific IP of **Source IP** or **Destination IP** in Figure18-3, it will prompt out a WebUI about Protocol and Port of the IP. (Figure18-4)



Time	Source	Destination	Protocol	Port	Disposition
Jul 4 12:04:15	192.168.179.30	192.168.179.1	TCP	1550 > 80	✓
Jul 4 12:02:59	192.168.179.30	192.168.179.1	TCP	1549 > 80	✓
Jul 4 12:02:58	192.168.179.30	192.168.179.1	TCP	1548 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 > 80	✓
Jul 4 12:02:55	192.168.179.30	203.84.196.97	TCP	1547 > 80	✓
Jul 4 12:02:55	192.168.179.30	203.84.196.97	TCP	1547 > 80	✓
Jul 4 12:02:55	192.168.179.30	168.95.192.1	ICMP	TYPE=3	✓
Jul 4 12:02:55	192.168.179.30	203.84.196.97	TCP	1544 > 80	✓
Jul 4 12:02:55	192.168.179.30	203.84.196.97	TCP	1544 > 80	✓
Jul 4 12:02:55	192.168.179.30	203.84.196.97	TCP	1543 > 80	✓

Figure18-4 The WebUI of detecting the Traffic Log by IP Address

STEP 5 . Click on **Download Logs** and select **Save** in **File Download** WebUI. And then choose the place to save in PC and click **OK**; the records will be saved instantly. (Figure18-5)

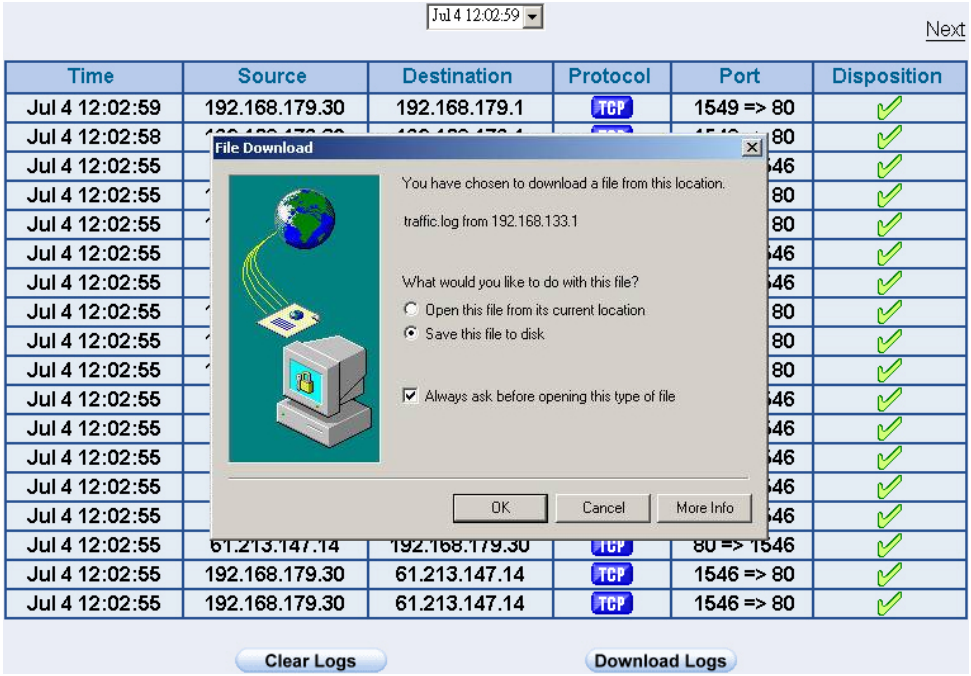


Figure18-5 Download Traffic Log Records WebUI

STEP 6． Click **Clear Logs** and click **OK** on the confirm WebUI; the records will be deleted from the ALL7000 instantly. (Figure18-6)

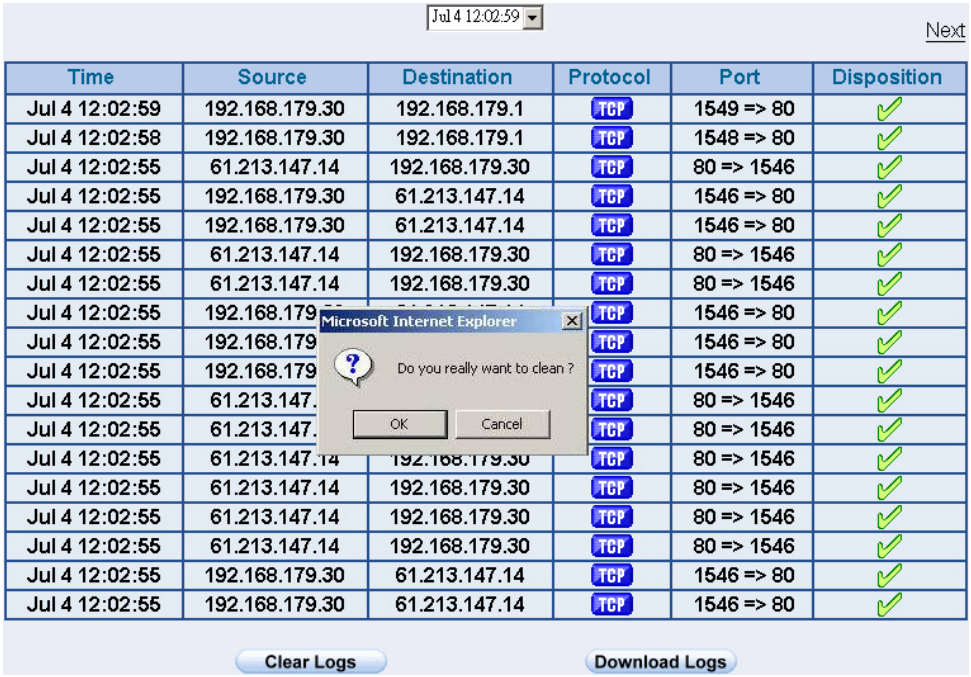


Figure18-6 Clearing Traffic Log Records WebUI

To record the detailed management events (such as Interface and event description of ALL7000) of the Administrator

STEP 1 . Click **Event** log of **LOG**. The management event records of the administrator will show up (Figure18-7)

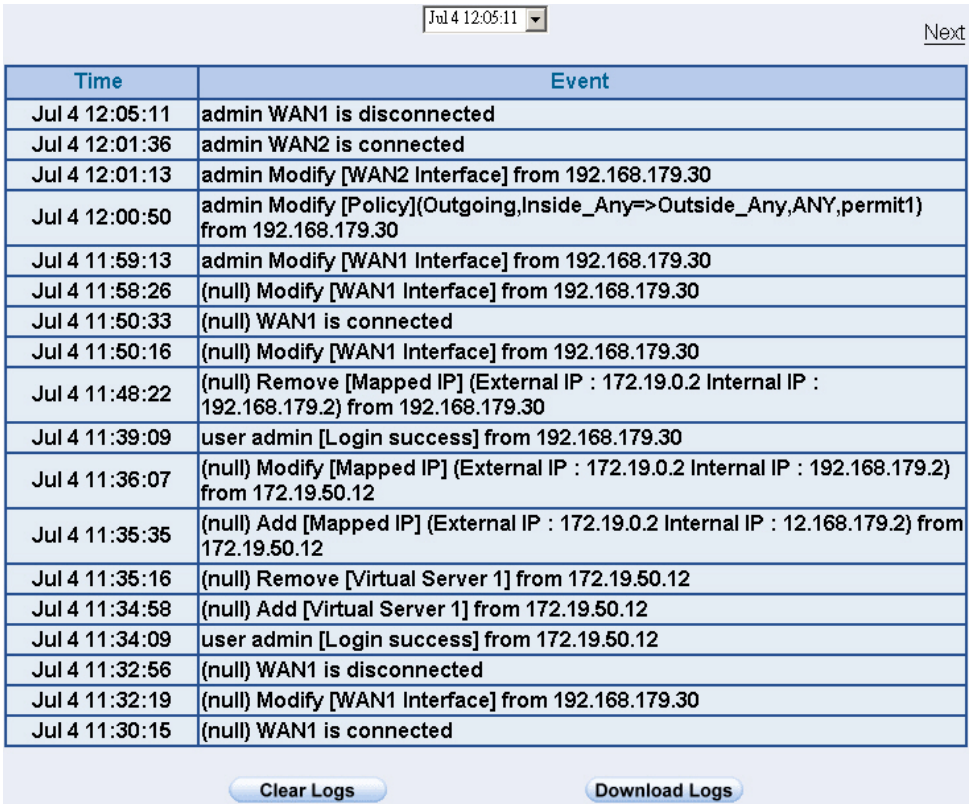


Figure18-7 Event Log WebUI

STEP 2 . Click on **Download Logs** and select **Save** in **File Download** WebUI. And then choose the place to save in PC and click **OK**; the records will be saved instantly. (Figure18-8)

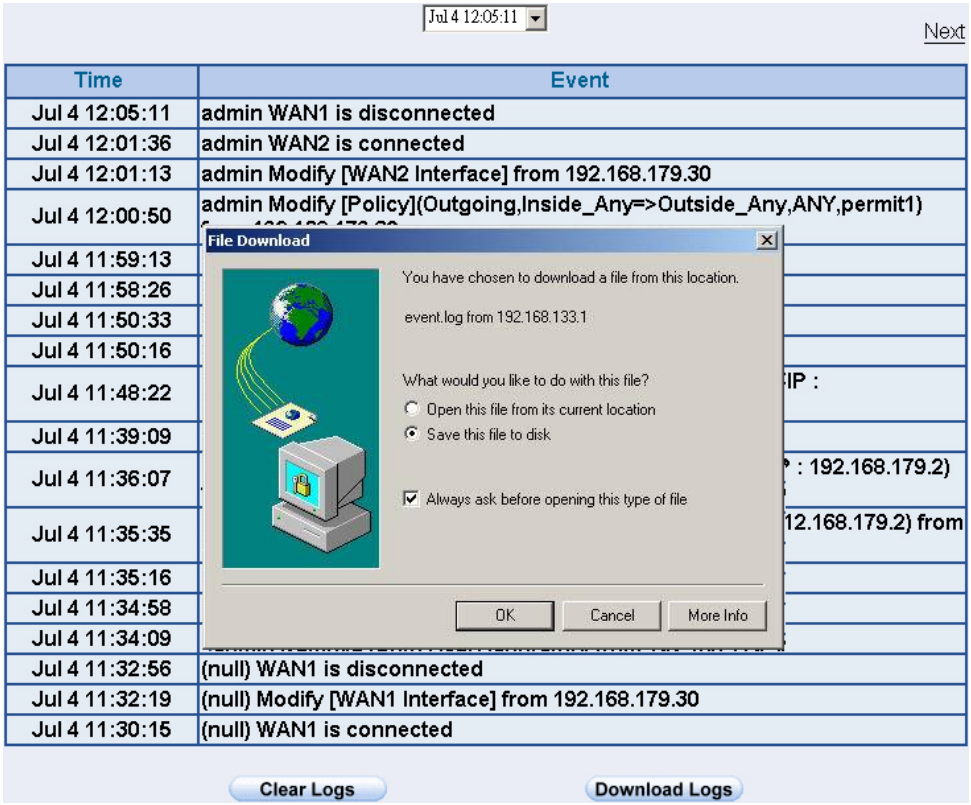


Figure18-8 Download Event Log Records WebUI

STEP 3 . Click **Clear Logs** and click **OK** on the confirm WebUI; the records will be deleted from the ALL7000. (Figure18-9)

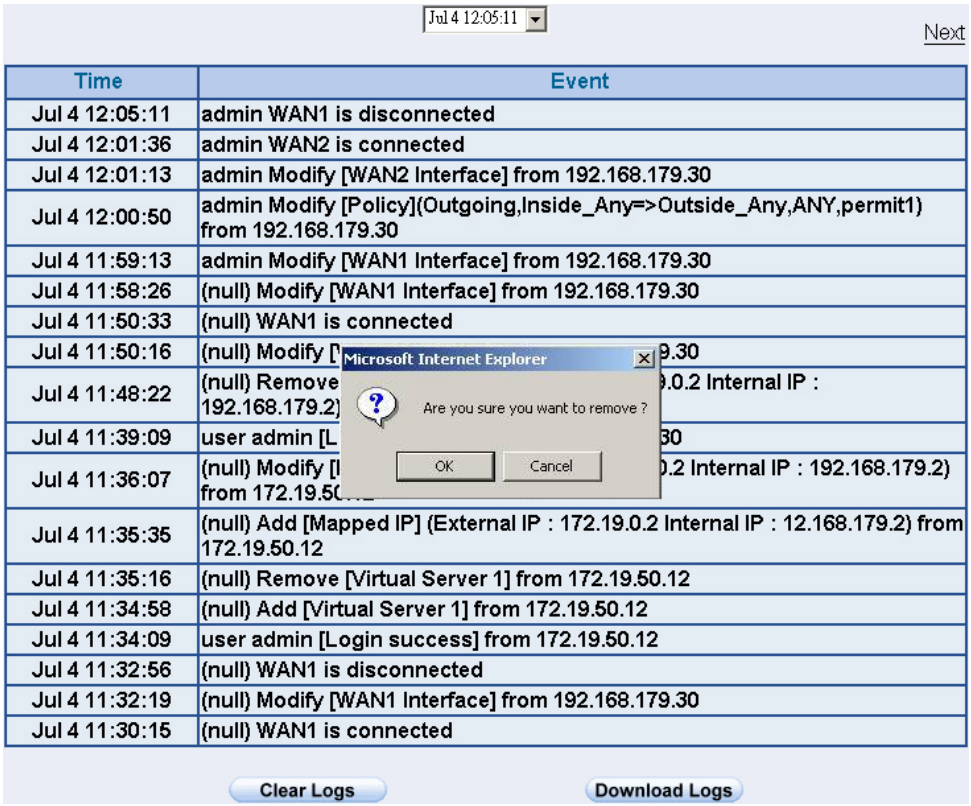


Figure18-9 Clearing Event Log Records WebUI

To Detect Event Description of WAN Connection

STEP 1． Click **Connection** in **LOG**. It can show up WAN Connection records of the ALL7000. (Figure18-10)

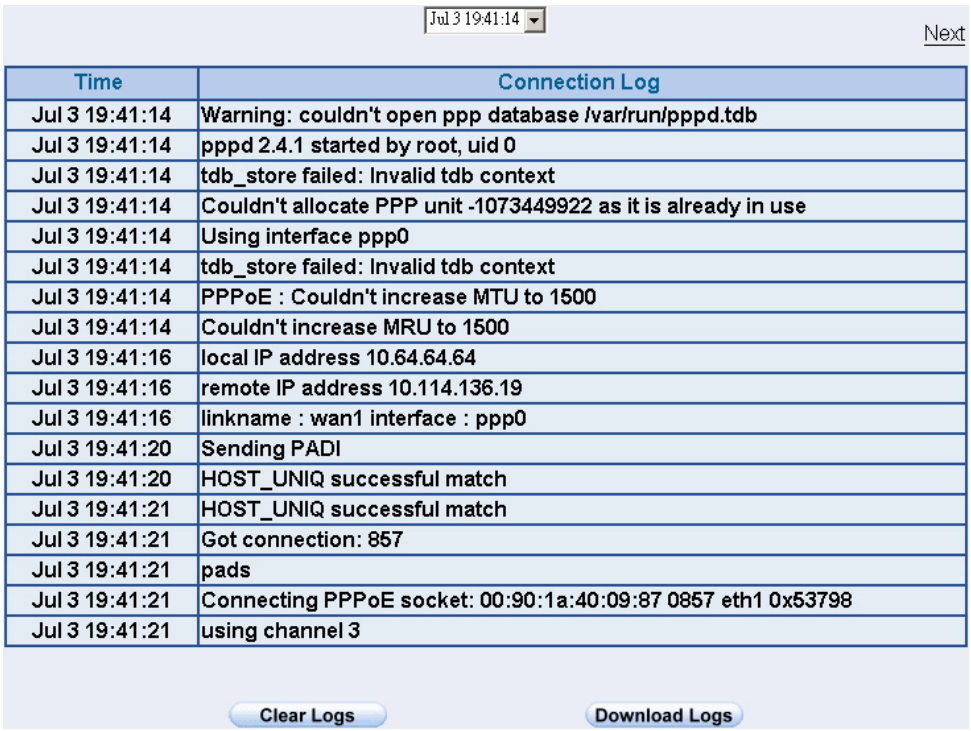


Figure18-10 Connection records WebUI

STEP 2 . Click on **Download Logs** and select **Save** in **File Download** WebUI. And then choose the place to save in PC and click **OK**; the records will be saved instantly. (Figure18-11)

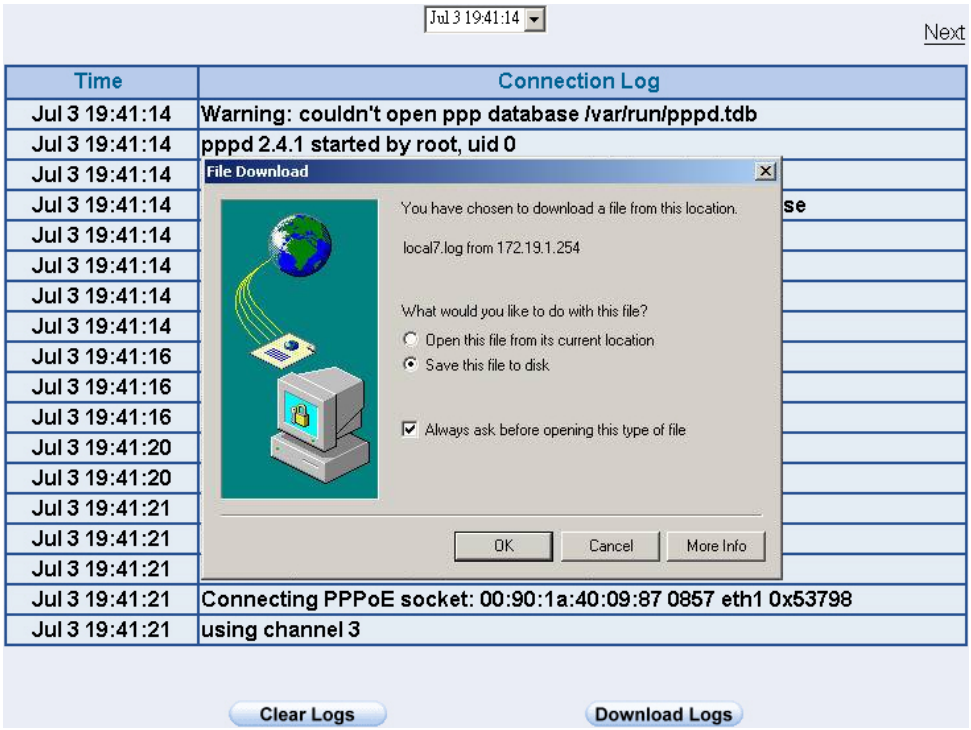


Figure18-11 Download Connection Log Records WebUI

STEP 3． Click **Clear Logs** and click **OK** on the confirm WebUI, the records will be deleted from the ALL7000 instantly. (Figure18-12)

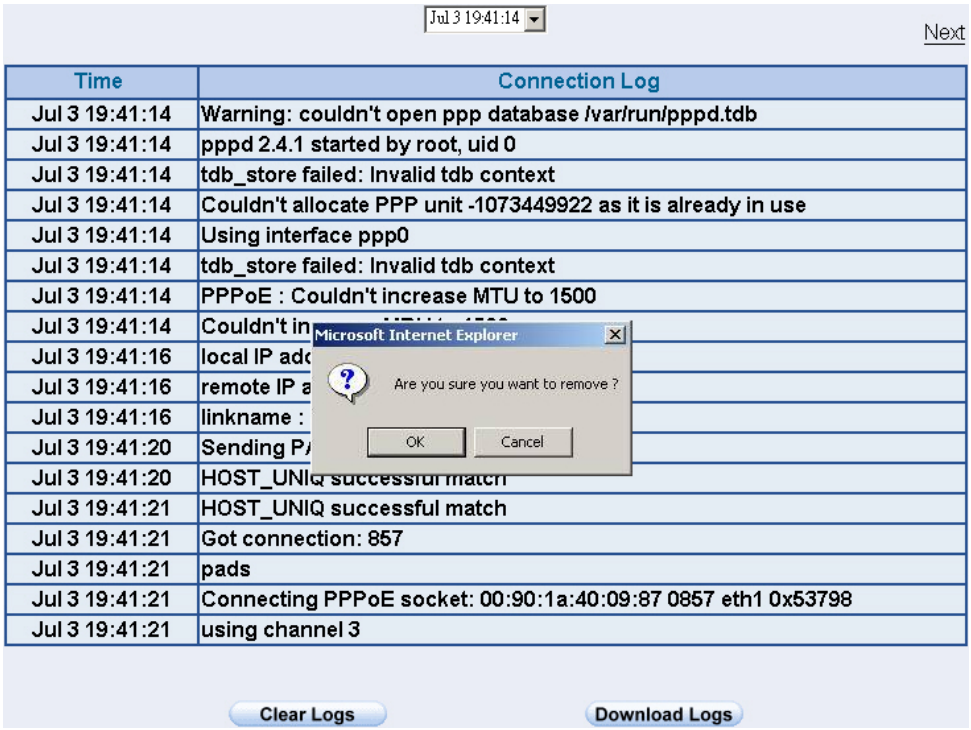


Figure18-12 Clearing Connection Log Records WebUI

To save or receive the records that sent by the ALL7000

STEP 1 . Enter **Setting** in **System**, select **Enable E-mail Alert Notification** function and set up the settings. (Figrue18-13)

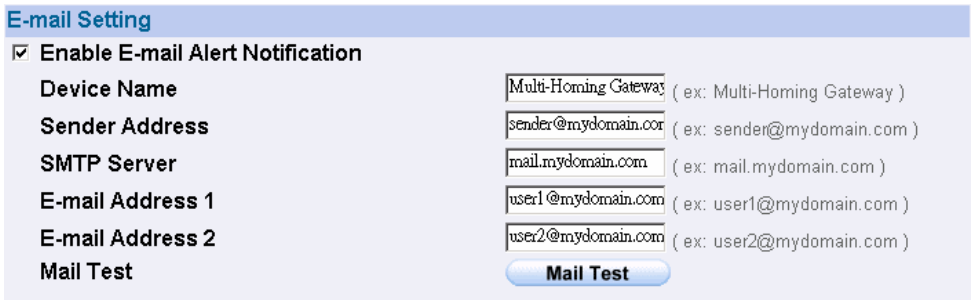


Figure18-13 E-mail Setting WebUI

STEP 2 . Enter **Log Backup** in **Log**, select **Enable Log Mail Support** and click **OK** (Figure18-14)

Figure18-14 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 (Figure18-15)

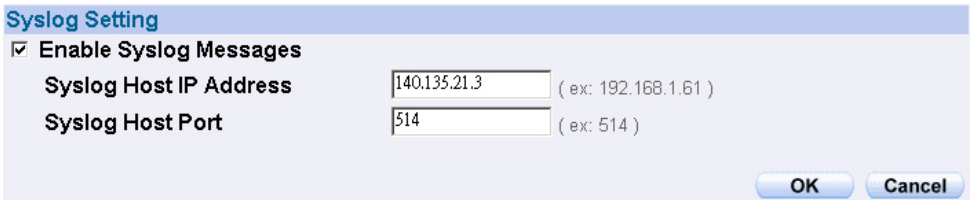


Figure18-15 Syslog Messages Setting WebUI

Chapter 19

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** of all the user's IP that passes the ALL7000.

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 ALL7000.

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 ALL7000

Destination IP：

- The IP address used by WAN service server which uses ALL7000.

Service：

- The communication service which listed in the menu when LAN users use ALL7000 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 when WAN user uses ALL7000 to connect to LAN Service Server.

Source IP：

- The IP address used by WAN users who use ALL7000

Destination IP：

- The IP address used by LAN service server who use ALL7000

Service：

- The communication service which listed in the menu when WAN users use ALL7000 to connect to LAN Service server.

Outbound

STEP 1 . Enter **Outbound** in **Accounting Report** and select **Top Users** to inquire the statistics of Send / Receive packets, **Downstream / Upstream, First packet/Last packet/Duration** and the service from the LAN or DMZ user's IP that pass the ALL7000. (Figure19-1)

- **TOP:** Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

- **Source IP**：The IP address used by LAN users who use ALL7000 to connect to WAN service server.
- **Downstream**：The percentage of downstream and the value of each WAN service server which uses ALL7000 to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who uses ALL7000 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 ALL7000.
- **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 ALL7000.
- **Duration**：The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.
- **Reset Counter**：Click Reset Counter button to refresh Accounting Report.

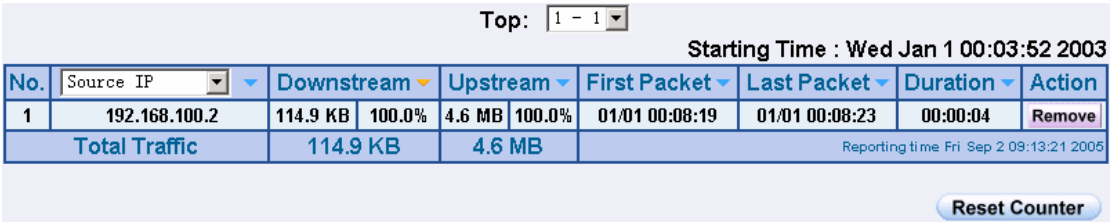


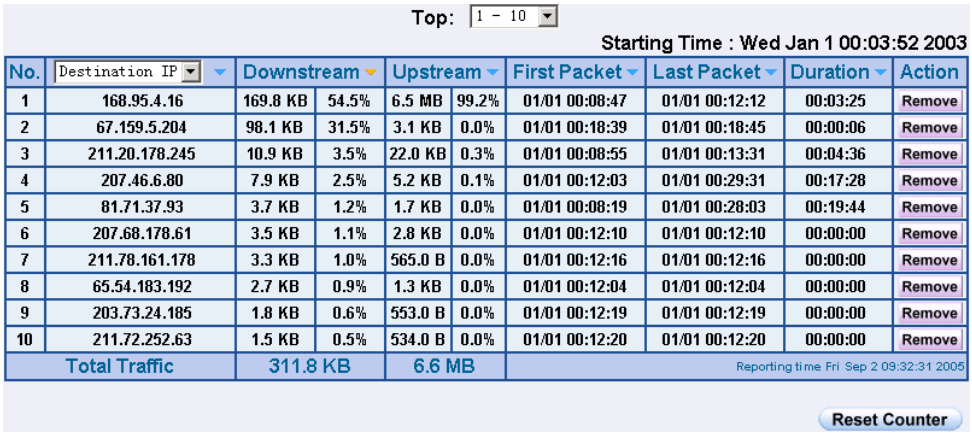
Figure19-1 Outbound Source IP Statistics Report

STEP 2 . Enter **Outbound** in **Accounting Report** and select **Top Sites** 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 ALL7000. (Figure19-2)

- **TOP**：Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

- **Destination IP**：The IP address used by WAN service server which uses ALL7000.
- **Downstream**：The percentage of downstream and the value of each WAN service server which uses ALL7000 to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who uses ALL7000 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 ALL7000.
- **Last Packet**：When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the ALL7000.
- **Duration**：The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 will record the sum of time and show the percentage of each WAN service server’s upstream/downstream to LAN user.
- **Reset Counter**：Click Reset Counter button to refresh Accounting Report.



Top: 1 - 10

Starting Time : Wed Jan 1 00:03:52 2003

No.	Destination IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	168.95.4.16	169.8 KB	54.5%	6.5 MB	99.2%	01/01 00:08:47	01/01 00:12:12	00:03:25	Remove
2	67.159.5.204	98.1 KB	31.5%	3.1 KB	0.0%	01/01 00:18:39	01/01 00:18:45	00:00:06	Remove
3	211.20.178.245	10.9 KB	3.5%	22.0 KB	0.3%	01/01 00:08:55	01/01 00:13:31	00:04:36	Remove
4	207.46.6.80	7.9 KB	2.5%	5.2 KB	0.1%	01/01 00:12:03	01/01 00:29:31	00:17:28	Remove
5	81.71.37.93	3.7 KB	1.2%	1.7 KB	0.0%	01/01 00:08:19	01/01 00:28:03	00:19:44	Remove
6	207.68.178.61	3.5 KB	1.1%	2.8 KB	0.0%	01/01 00:12:10	01/01 00:12:10	00:00:00	Remove
7	211.78.161.178	3.3 KB	1.0%	565.0 B	0.0%	01/01 00:12:16	01/01 00:12:16	00:00:00	Remove
8	65.54.183.192	2.7 KB	0.9%	1.3 KB	0.0%	01/01 00:12:04	01/01 00:12:04	00:00:00	Remove
9	203.73.24.185	1.8 KB	0.6%	553.0 B	0.0%	01/01 00:12:19	01/01 00:12:19	00:00:00	Remove
10	211.72.252.63	1.5 KB	0.5%	534.0 B	0.0%	01/01 00:12:20	01/01 00:12:20	00:00:00	Remove
Total Traffic		311.8 KB		6.6 MB		Reporting time Fri Sep 2 09:32:31 2005			

Reset Counter

Figure19-2 Outbound Destination IP Statistics Report

STEP 3 . Enter **Outbound** 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 ALL7000. (Figure19-3)

- **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. (Figure19-4)

Pull-down menu selection

- **Service**：The report of Communication Service when LAN users use the ALL7000 to connect to WAN service server.
- **Downstream**：The percentage of downstream and the value of each WAN service server who uses ALL7000 to connect to LAN user.
- **Upstream**：The percentage of upstream and the value of each LAN user who uses ALL7000 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 ALL7000.
- **Last Packet**：When the last packet is sent from the WAN Service Server, the sent time will be recorded by the ALL7000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server.
- **Reset Counter**：Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 10

Starting Time : Wed Jan 1 00:03:52 2003

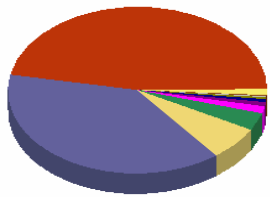
No.	Service	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	SMTP [25]	150.0 KB	47.0%	6.5 MB	99.0%	01/01 00:08:47	01/01 00:11:19	00:02:32	Remove
2	HTTP [80]	123.7 KB	38.8%	35.7 KB	0.5%	01/01 00:08:22	01/01 00:18:31	00:10:09	Remove
3	POP3 [110]	21.5 KB	6.7%	2.2 KB	0.0%	01/01 00:11:24	01/01 00:12:15	00:00:51	Remove
4	MSN [1863]	9.7 KB	3.0%	7.0 KB	0.1%	01/01 00:12:02	01/01 00:38:31	00:26:29	Remove
5	UNKNOW [4446]	4.4 KB	1.4%	2.1 KB	0.0%	01/01 00:08:19	01/01 00:35:45	00:27:26	Remove
6	HTTPS [443]	2.7 KB	0.8%	1.4 KB	0.0%	01/01 00:08:21	01/01 00:12:04	00:03:43	Remove
7	UNKNOW [1368]	1.2 KB	0.4%	1.2 KB	0.0%	01/01 00:08:25	01/01 00:36:38	00:28:13	Remove
8	UNKNOW [4652]	1.2 KB	0.4%	1.7 KB	0.0%	01/01 00:08:25	01/01 00:36:13	00:27:48	Remove
9	UNKNOW [63756]	549.0 B	0.2%	963.0 B	0.0%	01/01 00:08:25	01/01 00:36:38	00:28:13	Remove
10	UNKNOW [22453]	500.0 B	0.2%	882.0 B	0.0%	01/01 00:08:25	01/01 00:36:39	00:28:14	Remove
	Total Traffic	319.1 KB		6.6 MB		Reporting time Fri Sep 2 09:42:01 2005			

Reset Counter

Figure19-3 Outbound Services Statistics Report

Service Distribution

No.	Downstream
1	SMTP [25] 150.0 KBytes (46.9%)
2	HTTP [80] 123.7 KBytes (38.7%)
3	POP3 [110] 21.5 KBytes (6.7%)
4	MSN [1863] 10.1 KBytes (3.2%)
5	UNKNOW [4446] 4.4 KBytes (1.4%)
6	HTTPS [443] 2.7 KBytes (0.8%)
7	UNKNOW [4652] 1.6 KBytes (0.5%)
8	UNKNOW [1368] 1.2 KBytes (0.4%)
9	UNKNOW [63756] 549.0 Bytes (0.2%)
10	UNKNOW [22453] 500.0 Bytes (0.2%)
	OTHER 3.6 KBytes (1.1%)



No.	Upstream
1	SMTP [25] 6.5 MBytes (99.0%)
2	HTTP [80] 35.7 KBytes (0.5%)
3	MSN [1863] 7.7 KBytes (0.1%)
4	POP3 [110] 2.2 KBytes (0.0%)
5	UNKNOW [4446] 2.1 KBytes (0.0%)
6	UNKNOW [4652] 2.1 KBytes (0.0%)
7	UNKNOW [3198] 1.6 KBytes (0.0%)
8	HTTPS [443] 1.4 KBytes (0.0%)
9	UNKNOW [1368] 1.2 KBytes (0.0%)
10	UNKNOW [63756] 963.0 Bytes (0.0%)
	OTHER 15.7 KBytes (0.2%)

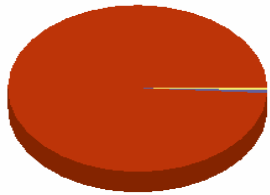


Figure19-4 According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart

Press to return to **Accounting Report** window.

Inbound

STEP 1． Enter **Inbound** in **Accounting Report** and select **Top Users** to inquire the statistics website of **Send / Receive packets**, **Downstream / Upstream, First packet/Last packet / Duration** and the service from the WAN user to pass the ALL7000. (Figure19-5)

- **TOP**：Select the data you want to view. It presents 10 pages in one page.

Select from the Pull-down menu

- **Source IP**：The IP address used by WAN users who use ALL7000.
- **Downstream**：The percentage of Downstream and the value of each WAN user who uses ALL7000 to LAN service server.
- **Upstream**：The percentage of Upstream and the value of each LAN service server who uses ALL7000 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 ALL7000.
- **Last Packet**：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the ALL7000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 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.

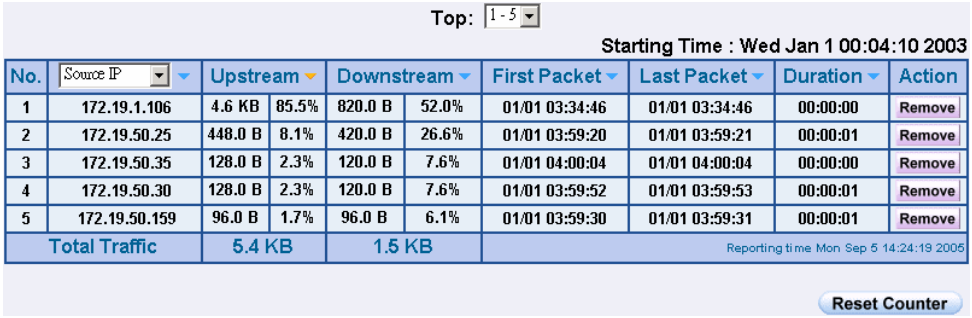


Figure19-5 Inbound Top Users Statistics Report

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** and the service from the WAN user to pass the ALL7000. (Figure19-6)

- **TOP**：Select the data you want to view. It presents 10 pages in one page.

Pull-down menu selection

- **Destination IP**：The IP address used by WAN users who uses ALL7000.
- **Downstream**：The percentage of Downstream and the value of each WAN user who uses ALL7000 to LAN service server.
- **Upstream**：The percentage of Upstream and the value of each LAN service server who uses ALL7000 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 ALL7000.
- **Last Packet**：When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the ALL7000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 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.

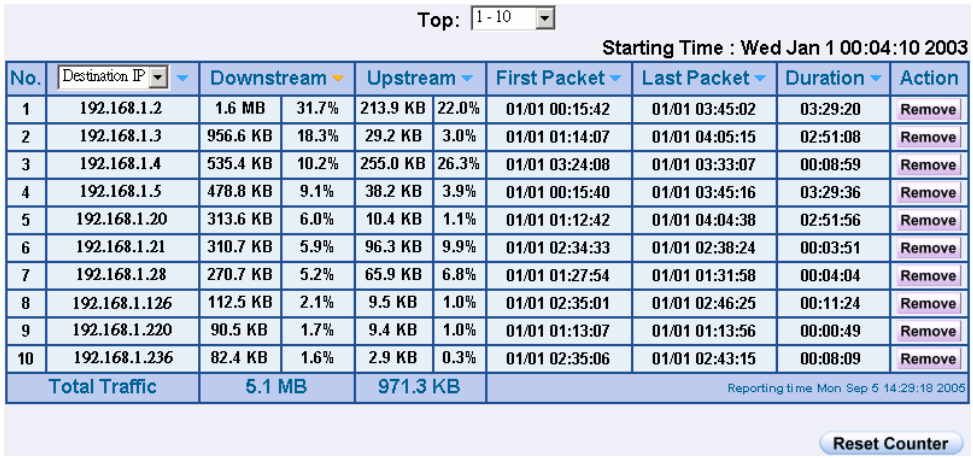


Figure19-6 Inbound Destination IP Statistics Report

STEP 2 . 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 ALL7000. (Figure19-7)

- **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. (Figure19-8)

Pull-down menu selection

- **Service**：The report of Communication Service when WAN users use the ALL7000 to connect to LAN service server.
- **Downstream**：The percentage of downstream and the value of each WAN user who uses ALL7000 to LAN service server.
- **Upstream**：The percentage of upstream and the value of each LAN service server who uses ALL7000 to WAN user.
- **First Packet**：When the first packet is sent to the LAN Service Server, the sent time will be recorded by the ALL7000.
- **Last Packet**：When the last packet is sent from the LAN Service Server, the sent time will be recorded by the ALL7000.
- **Duration**：The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic**：The ALL7000 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.

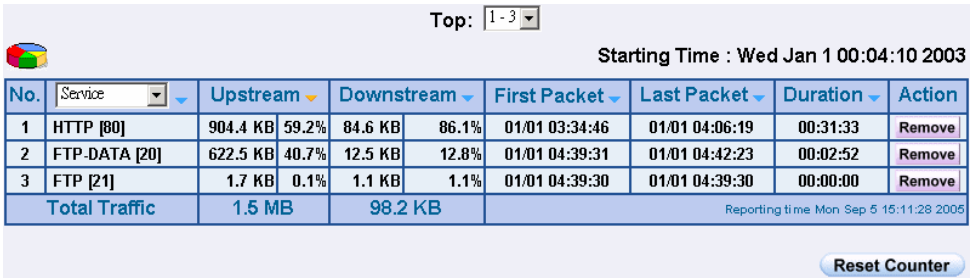


Figure19-7 Inbound Services Statistics Report

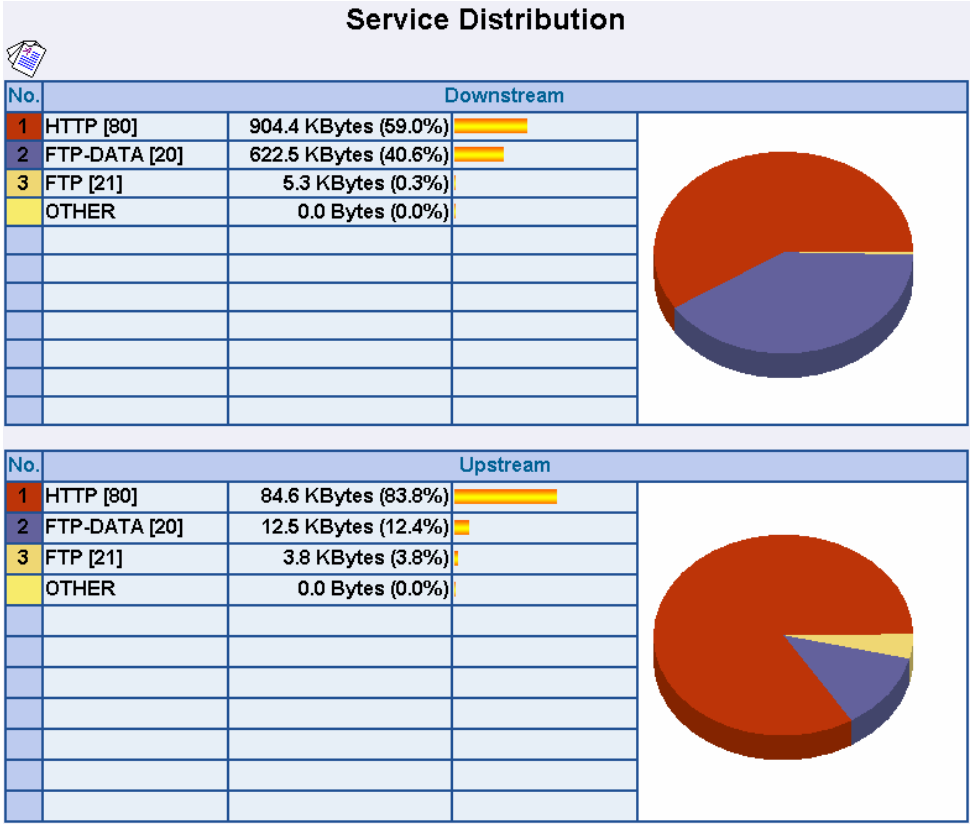


Figure19-8 According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart

Chapter 20

Statistics

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 ALL7000 for statistics of packets and data that passes across the ALL7000. 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. (Figure20-1)

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

Figure20-1 WAN Statistics function

- **Time:** To detect the statistics by minutes, hours, days, 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 (Figure20-2)

- **Y-Coordinate**：Network Traffic（Kbytes/Sec）
- **X-Coordinate**：Time（Hour/Minute）

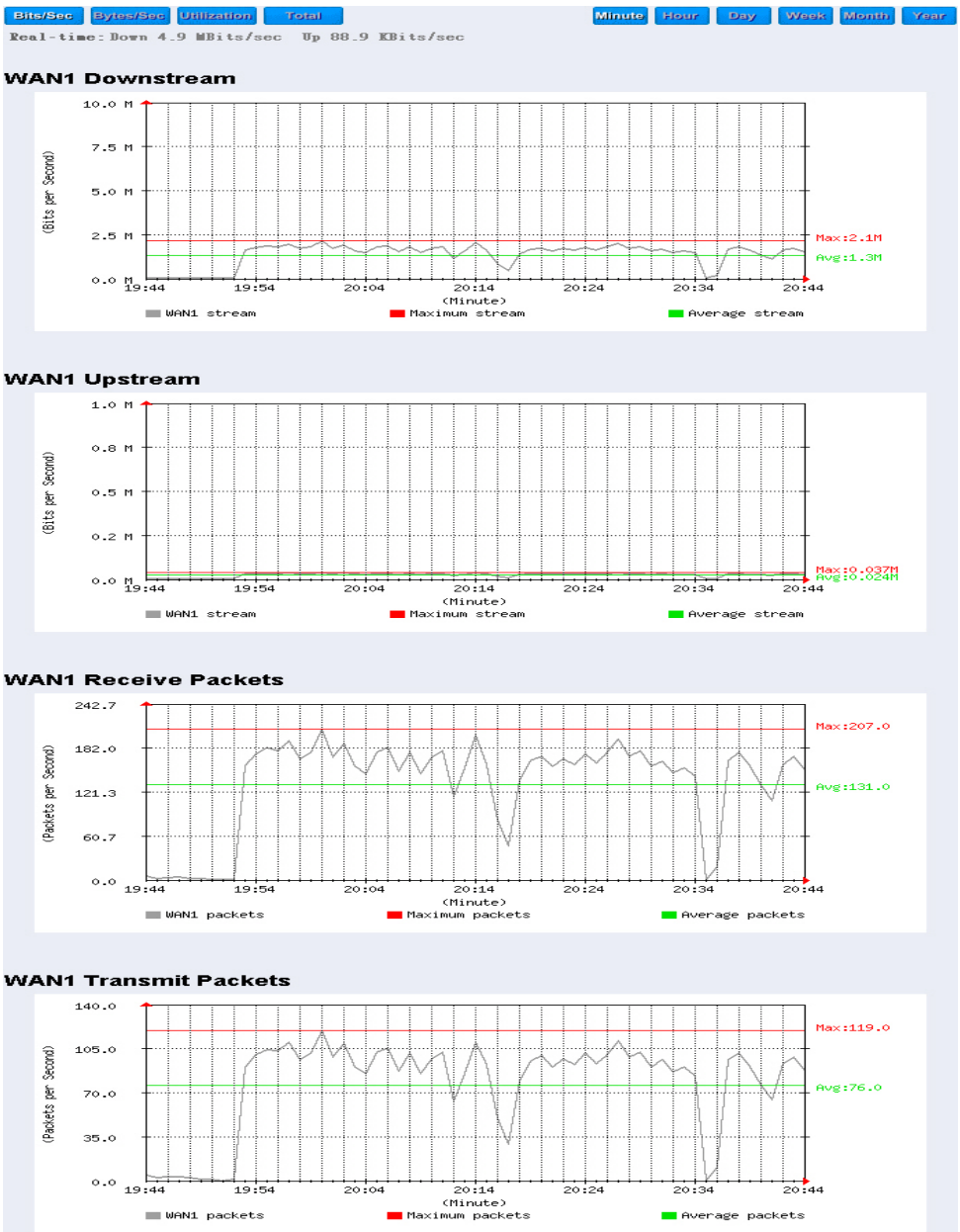


Figure20-2 To Detect WAN Statistics

Policy Statistics

STEP 1 . If you had select **Statistics** in **Policy**, it will start to record the chart of that policy in **Policy Statistics**. (Figure20-3)

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	PERMIT	Minute Hour Day Week Month Year
DMZ_Any	Outside_Any	ANY	PERMIT	Minute Hour Day Week Month Year

Figure20-3 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 (Figure20-4)

- **Y-Coordinate**：Network Traffic（Kbytes/Sec）
- **X-Coordinate**：Time（Hour/Minute/Day）

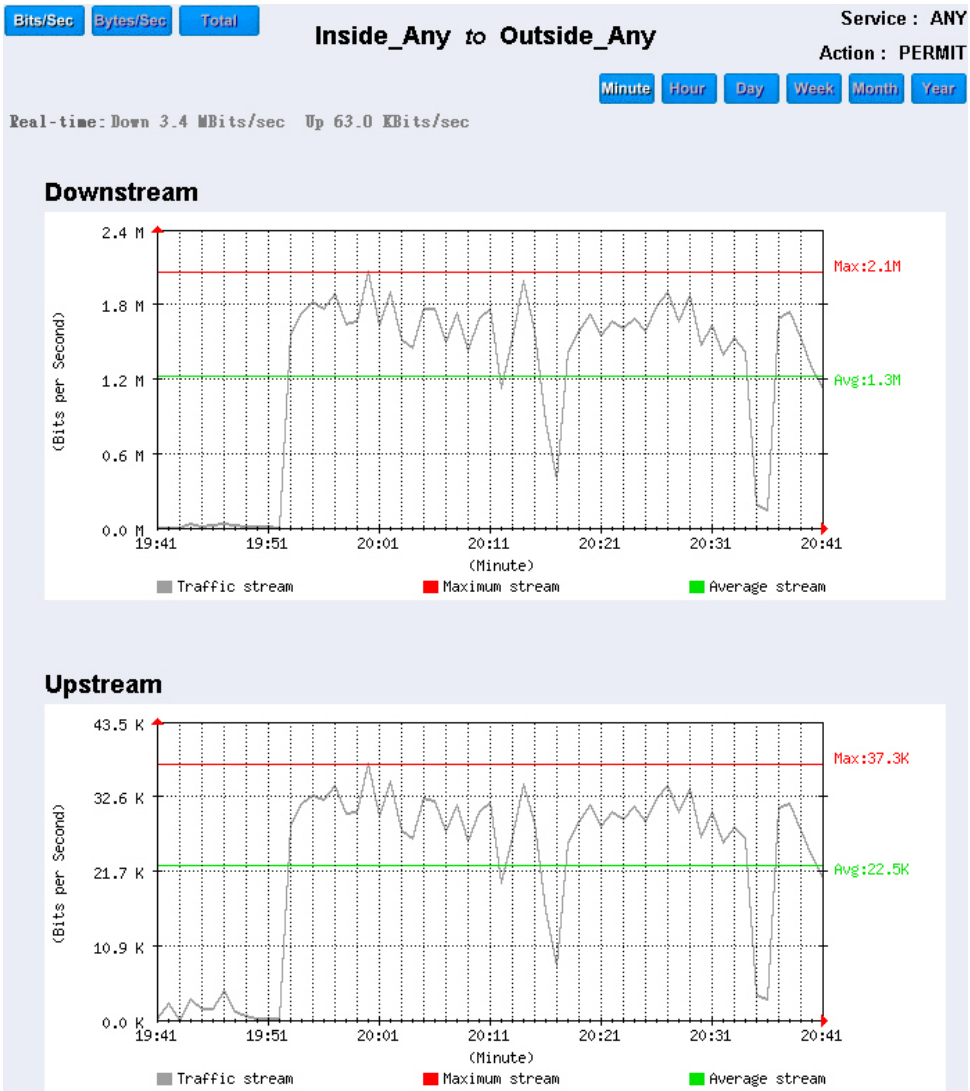


Figure20-4 To Detect Policy Statistics

Chapter 21

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 ALL7000
- **Authentication:** The Authentication information of ALL7000
- **ARP Table:** Record all the ARP that connect to the ALL7000
- **DHCP Clients:** Display the table of DHCP clients that are connected to the ALL7000.

Interface

STEP 1． Enter **Interface** in **Status** function; it will list the setting for each Interface: (Figure21-1)

- **PPPoE Con. Time:** The last time of the ALL7000 to be enabled
- **MAC Address:** The MAC Address of the Interface
- **IP Address/ Netmask:** The IP Address and its Netmask of the Interface
- **Rx Pkts, Err. Pkts:** To display the received packets and error packets of the Interface
- **Tx Pkts, Err. Pkts:** To display the sending packets and error packets of the Interface
- **Ping, WebUI:** To display whether the users can Ping to the ALL7000 from the Interface or not; or enter its WebUI
- **Forwarding Mode:** The connection mode of the Interface
- **Connection Status:** To display the connection status of WAN
- **DnS/ UpS Kbps:** To display the Maximum DownStream/UpStream Bandwidth of that WAN (set from **Interface**)
- **DnStream Alloca.:** The distribution percentage of DownStream according to WAN traffic
- **UpStream Alloca.:** The distribution percentage of UpStream according to WAN traffic
- **Default Gateway:** To display the Gateway of WAN
- **DNS1:** The DNS1 Server Address provided by ISP
- **DNS2:** The DNS2 Server Address provided by ISP

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Static IP	Transparent
WAN Connection	---			---
Max. Downstream / Upstream	---	512 / 512 Kbps	50000 / 50000 Kbps	---
Downstream Alloca.	---	0%	100%	---
Upstream Alloca.	---	41%	58%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:e0:98:00:00:09	00:e0:98:00:00:0a	00:e0:98:00:00:0b	00:e0:98:00:00:0c
IP Address	192.168.159.1	61.11.11.12	211.22.22.22	0.0.0.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	---	61.11.11.254	211.22.22.254	---
DNS1	---	168.95.1.1	168.95.1.1	---
DNS2	---	0.0.0.0	0.0.0.0	---
Rx Pkts, Error Pkts	98471, 0	0, 0	2408, 0	0, 0
Tx Pkts, Error Pkts	12173, 0	13068, 0	15066, 0	15112, 0
Ping	✓	✓	✓	✓
HTTP	✓	✓	✓	✓

Figure21-1 Interface Status

Authentication

STEP 1 . Enter **Authentication** in **Status** function, it will display the record of login status: (Figure21-2)

- **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)

IP Address	Authentication-User Name	Login Time
192.168.179.30	josh	2003/1/1 0:18:10

Figrue21-2 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 ALL7000: (Figure21-3)

- **NetBIOS Name:** The identified name of the network
- **IP Address:** The IP Address of the network
- **MAC Address:** The identified number of the network card
- **Interface:** The Interface of the computer

IP Address	MAC Address	Interface
172.19.100.6	00:0C:76:B7:96:4E	LAN
172.19.66.33	00:0C:76:B7:97:7E	LAN
172.19.1.101	00:03:62:80:02:9D	LAN
61.218.49.25	10:02:8A:C0:38:9E	WAN 1
172.19.1.106	00:50:BA:AF:50:ED	LAN
172.19.50.17	00:E0:98:C1:92:D0	LAN
172.19.88.88	00:0C:7C:00:04:4B	LAN
61.218.49.28	10:02:44:76:57:10	WAN 1
172.19.100.45	00:02:44:8E:B7:C7	LAN
172.19.100.64	00:D0:C9:92:07:59	LAN
61.218.49.29	00:48:54:5C:78:99	DMZ
172.19.50.12	00:0C:76:B7:96:3B	DMZ
61.218.49.30	00:40:C7:85:6C:73	DMZ
172.19.20.11	00:01:80:41:D0:AE	LAN
172.19.20.100	00:0C:76:B7:96:49	LAN
172.19.100.54	00:E0:7D:9F:17:64	LAN
172.19.50.12	00:0C:76:B7:96:3B	LAN
172.19.50.15	00:05:5D:95:FF:9E	LAN
172.19.100.89	00:90:0B:00:EE:87	LAN
172.19.55.66	00:10:F3:05:1C:04	LAN
172.19.100.88	00:90:0B:04:5B:9F	LAN
172.19.66.33	00:0C:76:B7:97:7E	DMZ
172.19.100.30	00:0E:F5:00:08:01	LAN

Figure21-3 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 ALL7000: (Figure21-4)

- **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
192.168.179.2	00:0c:76:b7:97:7e	2003/1/1 0:9:49	2003/1/2 0:9:49
192.168.179.4	56:49:54:41:4c:bd	2003/1/1 0:4:54	2003/1/2 0:4:54

Figure21-4 DHCP Clients WebUI

Germering, 06.07.06

EC – Declaration of conformity

for

ALL7000 Load-balancing VPN Gateway

This equipment conforms with the requirements of the Council Directive **89/336/EC** on the approximation of the laws of the member states relating to Electromagnetic Compatibility Directive and the mutual recognition of their conformity.

The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL7000 Load-balancing VPN Gateway conforms to the European Directive 89/336/EC and 2002/95/EC (RoHS Directive).
This equipment meets the following conformance standards:

EMI: EN 55022 :1998 (A1 :2000 Class B)
EN 6100-3-2 :2000 Class A
EN6100-3-3:1995+A1:2001

EMS: EN 55024 :1998 (A1 :2001)

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET Computersysteme GmbH
Maistr. 2
82110 Germering

and can be downloaded from http://www.allnet.de/ce-certificates/ .