



ALL7008

User's Manual

# Table of Contents

## System

Chapter 1	Administration .....	5
	Admin .....	7
	Permitted IPs .....	9
	Logout .....	10
	Software Update .....	11
Chapter 2	Configure .....	13
	Setting .....	18
	Date/Time .....	23
	Multiple Subnet .....	24
	Route Table .....	27
	DHCP .....	36
	DDNS .....	38
	Host Table .....	40
	Language .....	41

## Interface

Chapter 3	Interface .....	43
	LAN .....	48
	WAN .....	49
	DMZ .....	57

## Policy Object

Chapter 4	Address .....	59
	Example .....	62

Chapter 5	Service .....	<b>69</b>
	Custom .....	<b>72</b>
	Group .....	<b>76</b>
Chapter 6	Schedule .....	<b>79</b>
Chapter 7	QoS .....	<b>83</b>
	Example .....	<b>87</b>
Chapter 8	Authentication .....	<b>91</b>
	Auth User .....	<b>97</b>
	Auth User Group .....	<b>101</b>
	RADIUS .....	<b>105</b>
	POP3 Server .....	<b>126</b>
Chapter 9	Content Blocking .....	<b>129</b>
	URL .....	<b>133</b>
	Script .....	<b>136</b>
	P2P .....	<b>138</b>
	IM .....	<b>140</b>
	Download .....	<b>142</b>
Chapter10	Virtual Server.....	<b>145</b>
	Example .....	<b>149</b>
Chapter11	VPN .....	<b>165</b>
	Example.....	<b>172</b>
Chapter12	Policy.....	<b>275</b>
	Example .....	<b>281</b>

## **Mail Security**

Chapter13	Configure .....	301
	Mail Relay .....	304
Chapter14	Anti-Spam .....	309
	Example .....	324
Chapter15	Anti-Virus .....	365
	Example .....	371

## **Anti-Attack**

Chapter16	Alert Setting .....	381
	Internal Alert .....	386
Chapter17	Attack Alarm .....	391
	Internal Alarm .....	393
	External Alarm .....	394

## **Monitor**

Chapter18	LOG .....	397
	Traffic Log .....	399
	Event Log .....	404
	Connection Log .....	407
	Log Backup .....	410
Chapter19	Alarm .....	413
	Traffic Alarm .....	414
Chapter20	Statistics .....	417
	WAN .....	419
	Policy .....	421



Chapter21	Status .....	423
	Interface .....	424
	Authentication .....	426
	ARP Table .....	427
	DHCP Clients .....	428

## Chapter 1

# Administration

“System” is the managing of settings such as the privileges of packets that pass through the ALL7008 and monitoring controls. The System Administrators can manage, monitor, and configure the ALL7008 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 ALL7008.

## Define the required fields of Administrator

### Administrator Name:

- The username of Administrators and Sub Administrator for the ALL7008. 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.”

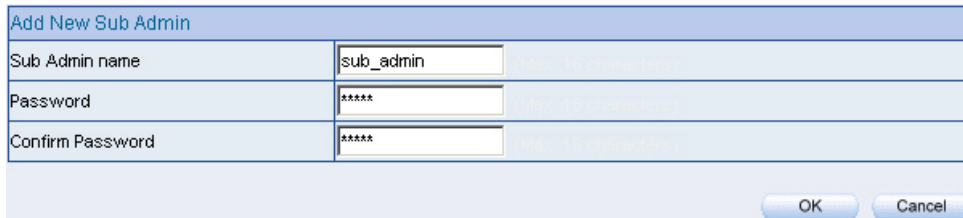
## Adding a new Sub Administrator

**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.



Add New Sub Admin	
Sub Admin name	sub_admin
Password	*****
Confirm Password	*****

OK Cancel

**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.

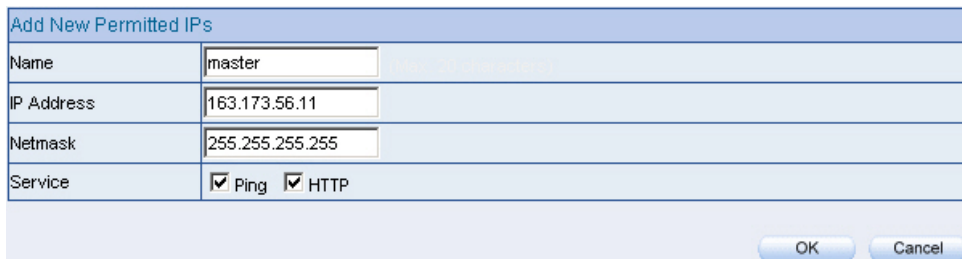
Modify Admin Password	
Admin Name	admin
Password	<input type="password" value="*****"/>
New Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

**Figure1-2 Modify Admin Password**

## Add Permitted IPs

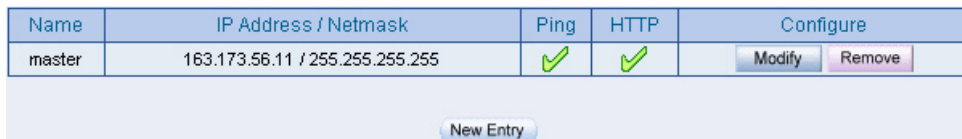
**STEP 1** . Add the following setting in **Permitted IPs** of **Administration**:  
(Figure1-3)

- **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)



Add New Permitted IPs	
Name	master
IP Address	163.173.56.11
Netmask	255.255.255.255
Service	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP

**Figure1-3 Setting Permitted IPs WebUI**



Name	IP Address / Netmask	Ping	HTTP	Configure
master	163.173.56.11 / 255.255.255.255	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**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 ALL7008 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)

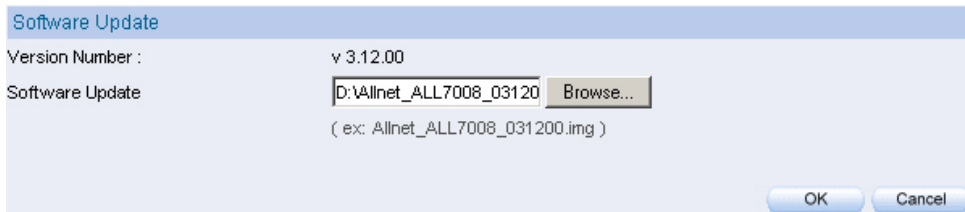


Figure1-6 Logout WebUI Message

## 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 ALL7008
- 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 ALL7008. 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

### ALL7008 Configuration:

- The Administrator can import or export the system settings. Click **OK** to import the file into the ALL7008 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 ALL7008 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 ALL7008 will record packet which source IP or destination address is ALL7008. And record in Traffic Log for System Manager to inquire about.

## **Define the required fields of Time Settings**

### **Synchronize Time/Date:**

- Synchronizing the ALL7008 with the System Clock. The administrator can configure the ALL7008'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)  $\leftrightarrow$  168.85.88.253(WAN)
2. Service department subnet : 192.168.2.1/24(LAN)  $\leftrightarrow$  168.85.88.252(WAN)
3. Sales department subnet : 192.168.3.1/24(LAN)  $\leftrightarrow$  168.85.88.251(WAN)
4. Procurement department subnet  
192.168.4.1/24(LAN)  $\leftrightarrow$  168.85.88.250(WAN)
5. Accounting department subnet  
192.168.5.1/24(LAN)  $\leftrightarrow$  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

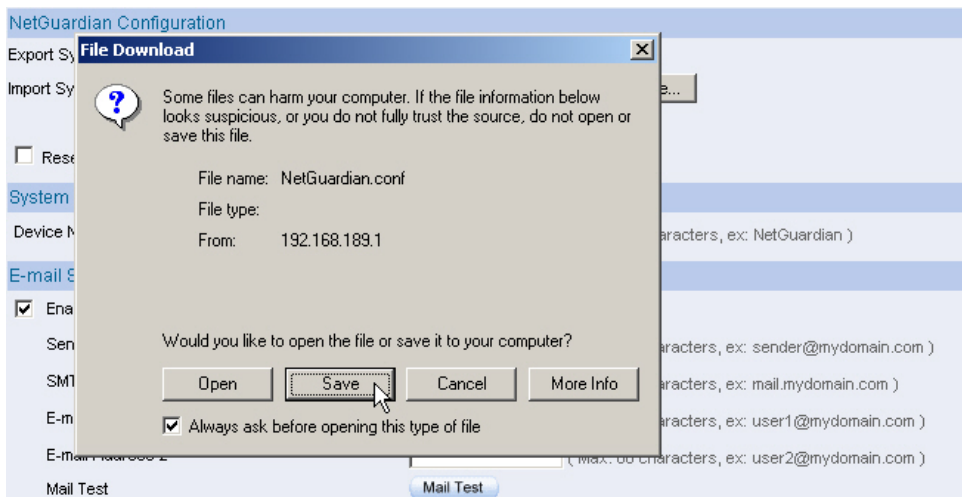
### Virtual IP Address:

- 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 ALL7008 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 ALL7008 Settings, then click **OK**. (Figure2-2)

**STEP 2 .** Click **OK** to import the file into the ALL7008 (Figure2-3)

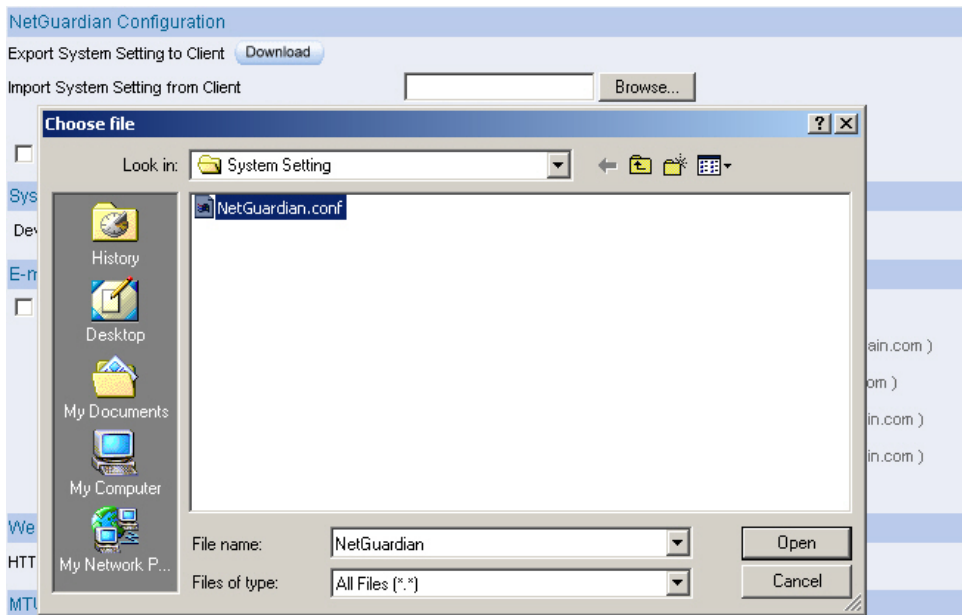


Figure 2-2 Enter the File Name and Destination of the Imported File

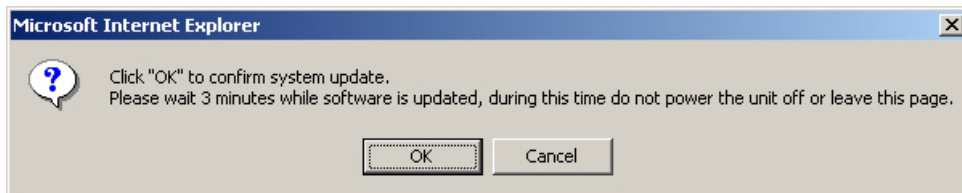


Figure 2-3 Upload the Setting File WebUI



## Restoring Factory Default Settings

**STEP 1 .** Select **Reset Factory Settings** in ALL7008 **Configuration** WebUI

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

The screenshot displays the 'NetGuardian Configuration' web interface. The 'Reset System to Factory Setting' checkbox is checked. Other visible settings include 'System Name Setting' (Device Name), 'E-mail Setting' (Sender Address, SMTP Server, E-mail Address 1, E-mail Address 2, Mail Test), 'Web Management (WAN Interface)' (HTTP Port), 'MTU Setting' (MTU), 'Link Speed / Duplex Mode Setting' (WAN1, WAN2), 'Dynamic Routing (RIPv2)' (Enable, LAN, WAN1, WAN2, DMZ, Routing information update timer, Routing information timeout), 'SIP protocol pass-through' (Enable SIP protocol pass-through), 'Administration Packet Logging' (Enable Administration Packet Logging), and 'System Reboot' (Reboot the NetGuardian Device). The 'OK' button is located at the bottom right.

NetGuardian Configuration

Export System Setting to Client [Download](#)

Import System Setting from Client  [Browse...](#)  
( ex: NetGuardian.conf )

☒ Reset System to Factory Setting

System Name Setting

Device Name  ( Max. 30 characters, ex: NetGuardian )

E-mail Setting

☐ Enable E-mail Alert Notification

Sender Address  ( Max. 60 characters, ex: sender@mydomain.com )

SMTP Server  ( Max. 80 characters, ex: mail.mydomain.com )

E-mail Address 1  ( Max. 60 characters, ex: user1@mydomain.com )

E-mail Address 2  ( Max. 60 characters, ex: user2@mydomain.com )

Mail Test [Mail Test](#)

Web Management (WAN Interface)

HTTP Port  80 ( Range: 1 - 65535 )

MTU Setting

MTU  1500 Bytes ( Range: 40 - 1500 )

Link Speed / Duplex Mode Setting

WAN1  Auto Mode

WAN2  Auto Mode

Dynamic Routing (RIPv2)

Enable ☐ LAN ☐ WAN1 ☐ WAN2 ☐ DMZ

Routing information update timer  30 Seconds ( Range: 5 - 99999 )

Routing information timeout  180 Seconds ( Range: 5 - 99999 )

SIP protocol pass-through

☐ Enable SIP protocol pass-through

Administration Packet Logging

☐ Enable Administration Packet Logging

System Reboot

Reboot the NetGuardian Device [Reboot](#)

[OK](#) [Cancel](#)

**Figure2-4 Reset Factory Settings**

## Enabling E-mail Alert Notification

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

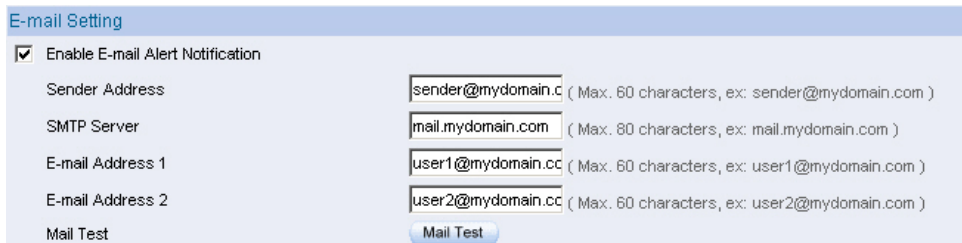
**STEP 2 . Sender Address:** Enter the Sender Address. (Required by some ISPs.)

**STEP 3 . SMTP Server IP:** Enter SMTP server's IP address.

**STEP 4 . E-Mail Address 1:** Enter the e-mail address of the first user to be notified.

**STEP 5 . E-Mail Address 2:** Enter the e-mail address of the second user to be notified. (Optional)

**STEP 6 .** Click **OK** on the bottom-right of the screen to enable E-mail Alert Notification. (Figure2-5)



**E-mail Setting**

☒ Enable E-mail Alert Notification

Sender Address  (Max. 60 characters, ex: sender@mydomain.com )

SMTP Server  (Max. 80 characters, ex: mail.mydomain.com )

E-mail Address 1  (Max. 60 characters, ex: user1@mydomain.com )

E-mail Address 2  (Max. 60 characters, ex: user2@mydomain.com )

Mail Test

**Figure2-5 Enable E-mail Alert Notification**



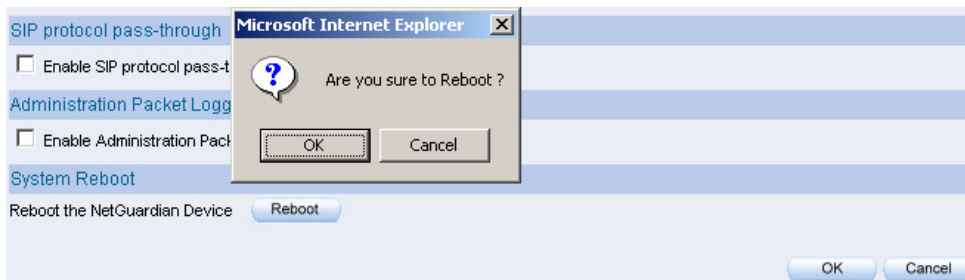
Click on **Mail Test** to test if E-mail Address 1 and E-mail Address 2 can receive the Alert Notification correctly.

## Reboot ALL7008

**STEP 1** . Reboot ALL7008 : Click **Reboot** button next to **Reboot ALL7008 Appliance**.

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

**STEP 3** . Follow the confirmation pop-up page; click **OK** to restart ALL7008.  
(Figure2-6)



**Figure2-6 Reboot ALL7008**

## 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.

System time : Thu Nov 15 19:51:59 2007

Synchronize system clock

☒ Synchronize system clock with an Internet time server

Set offset  hours from GMT [Assist](#)

☒ Enable daylight saving time setting

From  /  To  /

Server IP / Name  [Assist](#)

Update system clock every  minutes ( Range: 1 - 99999, 0: system clock updates at boot up )

Synchronize system clock with this client

Figure2-7 System Time Setting



Click on the **Sync** button and then the ALL7008'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

ALL7008 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)

Add New Multiple Subnet IP			
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
Alias IP of Interface	<input type="text" value="162.172.50.1"/>		
Netmask	<input type="text" value="255.255.0.0"/>		
WAN Interface IP			Forwarding Mode
WAN1	<input type="text" value="10.10.10.1"/> <a href="#">Assist</a>	<input type="radio"/> NAT <input checked="" type="radio"/> Routing	
WAN2	<input type="text" value="211.22.22.22"/> <a href="#">Assist</a>	<input checked="" type="radio"/> NAT <input type="radio"/> Routing	
<div>OK Cancel</div>			

Figure 2-8 Add Multiple Subnet WebUI

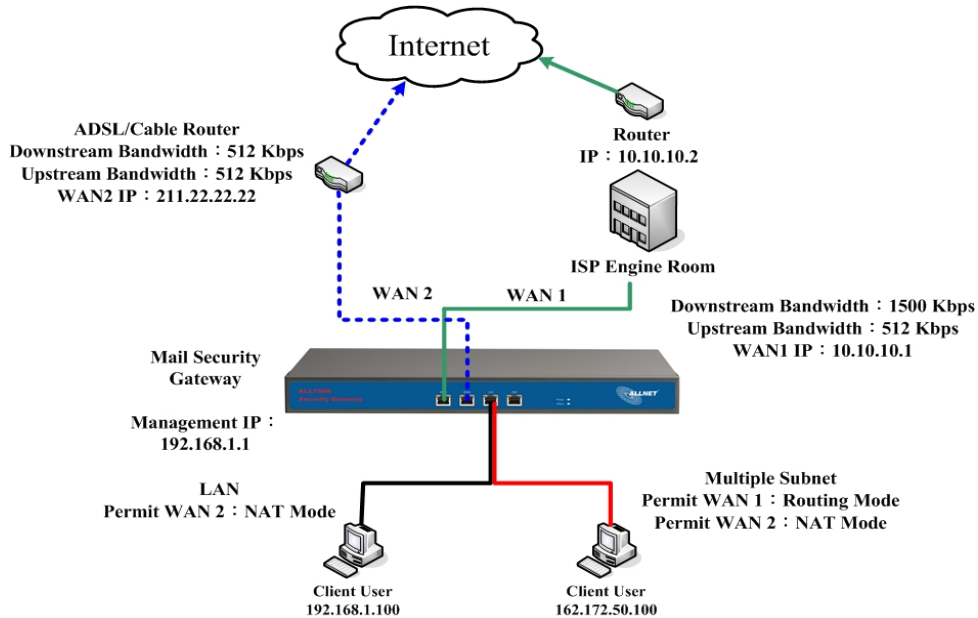


**WAN1** and **WAN2** Interface can use **Assist** to enter the data.



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 ALL7008'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 ALL7008 and makes them to connect to Internet through ALL7008**

### 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)

Add New Static Route	
Destination IP	192.168.10.1
Netmask	255.255.255.0
Gateway	192.168.1.252
Interface	LAN

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)

Add New Static Route	
Destination IP	192.168.20.1
Netmask	255.255.255.0
Gateway	192.168.1.252
Interface	LAN

Figure2-11 Add New Static Route2

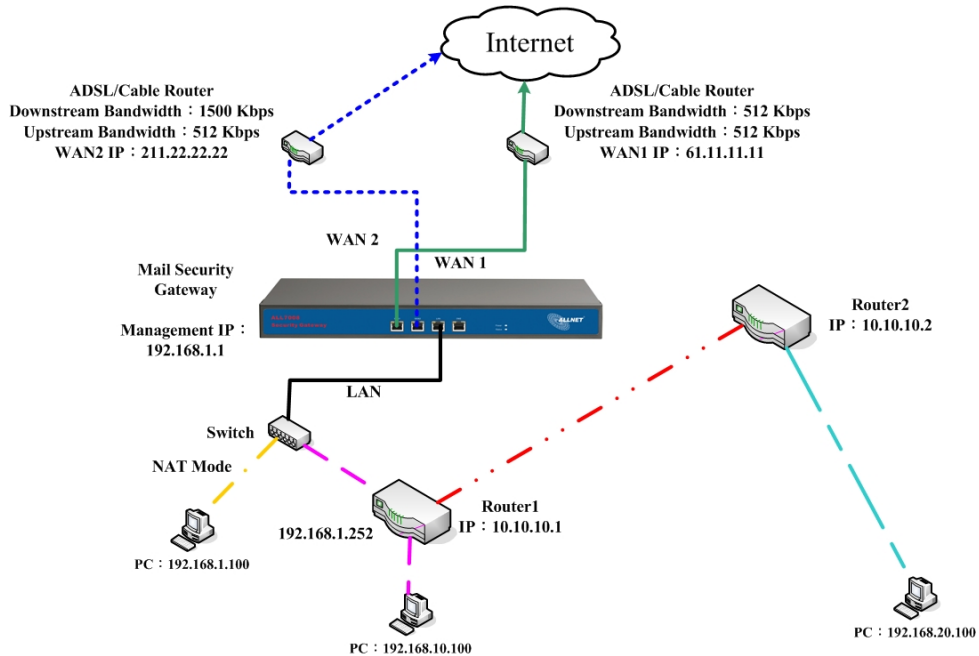
**STEP 3** . Enter the following setting in **Route Table** in **System** function:

- **【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)

Add New Static Route	
Destination IP	<input type="text" value="10.10.10.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.252"/>
Interface	<input type="text" value="LAN"/>

**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**

# Setting PPTP VPN connection between two ALL7008

## Preparation

Company A    **WAN IP: 61.11.11.11**  
                  **LAN IP: 192.168.10.X**  
                  **Multiple Subnet: 192.168.85.X**

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

This example takes two ALL7008 as flattop. Suppose Company B **192.168.20.100** is going to have VPN connection with Company A **192.168.10.100, 192.168.85.100** and download the resource.

**STEP 1** . Enter the following setting in **PPTP Server** of **VPN** function in the ALL7008 of Company A (Figure 2-14, 2-15)

Add New PPTP Server

User Name :	PPTP_Connection
Password :	*****
Client IP assigned by	
<input checked="" type="radio"/> IP Range	
<input type="radio"/> Fixed IP :	
<input type="checkbox"/> Manual Disconnect	

OK Cancel

**Figure 2-14 PPTP VPN Server Connection Setting**

PPTP Server ( Enable, Encryption:ON ) :

Client IP Range : 192.168.168.1-254 [Modify](#)

i	User Name	Client IP	Uptime	Configure
--	PPTP_Connection	0.0.0.0	---	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

**Figure 2-15 Complete PPTP VPN Server Setting**

**STEP 2 .** Add the following settings in **PPTP Server** of **VPN** function in the ALL7008 of Company B: (Figure2-16, 2-17)

Add New PPTP Client

User Name :	PPTP_Connection	
Password :	*****	
Server IP or Domain Name :	61.11.11.11	<input checked="" type="checkbox"/> Encryption
WAN interface :	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2	
<input type="checkbox"/> NAT		
<input type="checkbox"/> Manual Connect		
		OK Cancel

**Figure 2-16 PPTP VPN Client Setting**

PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure	
--	PPTP_Connection	61.11.11.11	ON	---	Modify	Remove

New Entry

**Figure 2-17 Complete PPTP VPN Client Setting**

**STEP 3 .** Enter the following setting in **Route Table** in **Configure** function in ALL7008 of Company B:

- **【Destination IP】** : Enter 192.168.85.0
- **【Netmask】** : Enter 255.255.255.0
- **【Gateway】** : Enter nothing
- **【Interface】** : LAN
- Click **OK** (Figure 2-18, 2-19)

Add New Static Route	
Destination IP	<input type="text" value="192.168.85.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text"/>
Interface	<input type="text" value="LAN"/>

**Figure2-18 Add New Static Route**

Interface	Destination IP / Netmask	Gateway	Configure
LAN	192.168.85.0 / 255.255.255.0		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure 2-19 Complete Adding New Static Route**

#### STEP 4 . Complete PPTP VPN Connection. (Figure 2-20)

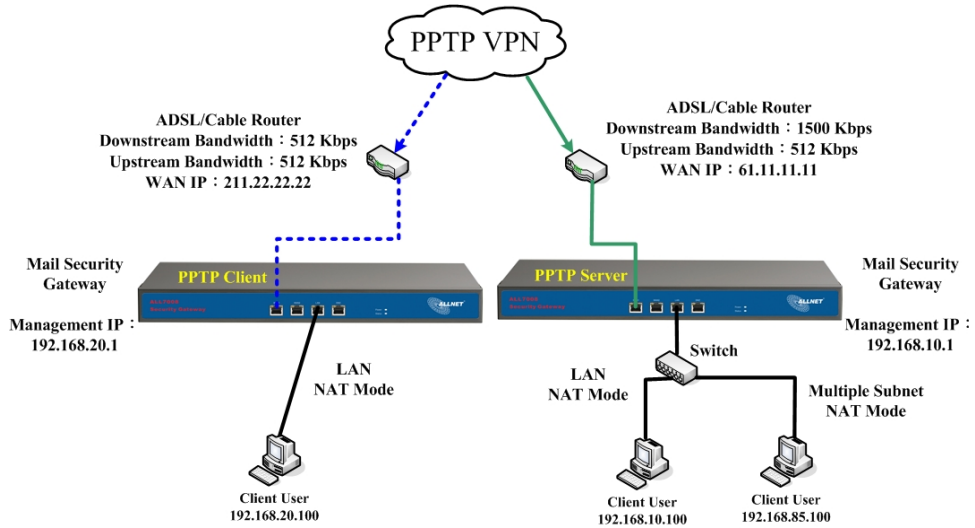


Figure 2-20 PPTP VPN Connection Setting



## 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. (Figure2-21)

Dynamic IP Address			
Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

---

☒ Enable DHCP Support

Domain Name  ( Max. 40 characters, ex: dhcp.domain\_name )

☐ Automatically Get DNS

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

LAN Interface :

Client IP Range 1  To

Client IP Range 2  To

Lease Time  hours ( Range: 0 - 99999 )

Figure 2-21 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 (Figure2-22). 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. (Figure2-23)

Add New Dynamic DNS			
Service Provider :	DynDNS (www.dyndns.com) [ U.S.A. ] <a href="#">Sign up</a>		
WAN IP:	61.11.11.11	<input checked="" type="checkbox"/> Automatically	WAN2
User Name :	test_jab@dyndns.org		
Password :	*****		
Domain Name:	test_jab	.	dyndns.org
<div>OK Cancel</div>			

Figure2-22 DDNS WebUI

i	Domain Name	WAN IP	Configure
	test_jab.dyndns.org	61.11.11.11	<div>Modify Remove</div>
<div>New Entry</div>			

Figure 2-23 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.

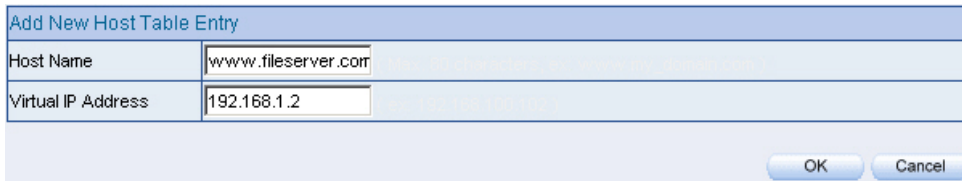


If you do not select **Automatically fill in the WAN IP** and then you can enter a specific IP in **WAN IP**. Let DDNS to correspond to that specific IP address.

## 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. (Figure2-24)



Add New Host Table Entry	
Host Name	www.fileserver.com
Virtual IP Address	192.168.1.2
<div>OK Cancel</div>	

**Figure2-24 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 ALL7008. That is, the default gateway.

## Language

Select the Language version (**English Version/ Traditional Chinese Version** or **Simplified Chinese Version**) and click **OK**. (Figure2-25)



Figure2-25 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 ALL7008.

### 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 ALL7008 from Interface IP.

### WAN:

- The System Administrator can set up the WAN network of ALL7008.

### Balance Mode:

- **Auto:** The ALL7008 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 ALL7008 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 ALL7008 distributes the WAN 1/2 download bandwidth by accumulative traffic.
- **By Session:** The ALL7008 distributes the WAN 1/2 download bandwidth by saturated connections.
- **By Packet:** The ALL7008 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 ALL7008 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.

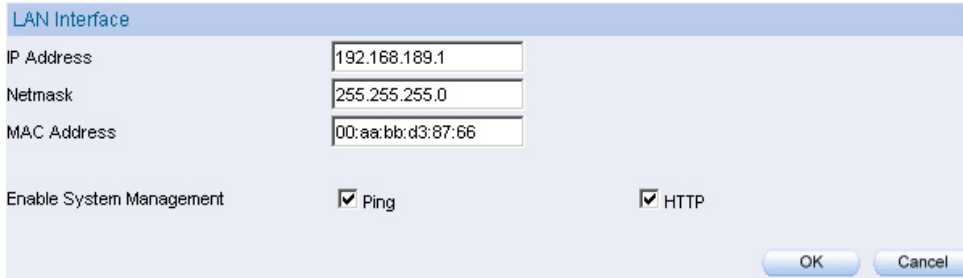
We set up four Interface Address examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	<b>LAN</b>	Modify LAN Interface Settings	<b>48</b>
Ex2	<b>WAN</b>	Setting WAN Interface Address	<b>49</b>
Ex3	<b>DMZ</b>	Setting DMZ Interface Address (NAT Mode)	<b>57</b>
Ex4	<b>DMZ</b>	Setting DMZ Interface Address (Transparent Mode)	<b>58</b>

## 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)



The screenshot shows a web-based configuration window titled "LAN Interface". It contains three input fields: "IP Address" with the value "192.168.189.1", "Netmask" with "255.255.255.0", and "MAC Address" with "00:aa:bb:d3:87:66". Below these fields, there are two checkboxes: "Enable System Management" with a checked "Ping" option, and another checked "HTTP" option. At the bottom right, there are "OK" and "Cancel" buttons.

**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 ALL7008'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)

WAN2 Interface: Enable  
Service: ICMP  
Indicator Site IP:   
[Assist](#)

**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.

WAN1 Interface

Service :  Alive Indicator Site IP :  [Assist](#)

Wait  seconds between the sending of each alive packet. ( Range: 0 - 99, 0: do not check )

**Figure3-3 ICMP Connection**

WAN1 Interface

Service :  DNS Server IP Address :  [Assist](#)

Domain name :  [Assist](#) (Max. 55 characters)

Wait  seconds between the sending of each alive packet. ( Range: 0 - 99, 0: do not check )

**Figure 3-4 DNS Service**



Connection test is used for ALL7008 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)



☒ PPPoE (ADSL User)  
☐ Dynamic IP Address (Cable Modem User)  
☐ Static IP Address

Current Status: Disconnected Connect  
 IP Address: 0.0.0.0 Disconnect

User Name: 82457216 (Max. 60 characters)  
 Password: \*\*\*\*\* (Max. 60 characters)

IP Address obtained from ISP via:
   
☒ Dynamic
   
☐ Fixed
   
 IP Address: 
  
 Netmask: 
  
 Default Gateway:

Max. Downstream Bandwidth: 51200 Kbps (Range: 1 - 51200 )  
 Max. Upstream Bandwidth: 51200 Kbps (Range: 1 - 51200 )

Auto Disconnect if idle for: 0 minutes (Range: 1 - 99999, 0: means always connected )

Enable System Management:
   
☒ Ping ☒ HTTP

OK Cancel

Figure3-5 PPPoE Connection

Balance Mode: Auto

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	PPPoE	61.228.168.60	<span>1</span>	<span>✓</span>	<span>✓</span>	<span>Modify</span>	<span>1</span>
2	(Disable)	---	<span>0</span>	---	---	<span>Modify</span>	<span>0</span>

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)

☐ PPPoE (ADSL User)

☒ **Dynamic IP Address (Cable Modem User)**

☐ Static IP Address

IP Address: 0.0.0.0 [Renew] [Release]

MAC Address: 00:AA:BB:D3:87:64 [Clone MAC]

Hostname: [ ] (Max. 50 characters)

Domain Name: [ ] (Max. 80 characters)

User Name (Required by DHCP+ protocol): [ ] (Max. 127 characters)

Password (Required by DHCP+ protocol): [ ] (Max. 127 characters)

Max. Downstream Bandwidth: 51200 Kbps ( Range: 1 - 51200 )

Max. Upstream Bandwidth: 51200 Kbps ( Range: 1 - 51200 )

Enable System Management: ☒ Ping ☒ HTTP

[OK] [Cancel]

**Figure3-7 Dynamic IP Address Connection**

Balance Mode : <input type="text" value="Auto"/>							
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Dynamic IP	220.132.112.108	1 <input type="text"/>			<input type="button" value="Modify"/>	1 <input type="text"/>
2	(Disable)	---	0 <input type="text"/>	---	---	<input type="button" value="Modify"/>	0 <input type="text"/>

**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)

The screenshot shows a configuration window for a Static IP Address. It has three radio buttons at the top: 'PPPoE (ADSL User)', 'Dynamic IP Address (Cable Modem User)', and 'Static IP Address', with the last one selected. Below are several input fields: 'IP Address' (211.22.22.18), 'Netmask' (255.255.255.0), 'MAC Address' (00:AA:BB:D3:87:64), and 'Default Gateway' (211.22.22.18). Then there are two more input fields for 'Max. Downstream Bandwidth' and 'Max. Upstream Bandwidth', both set to 51200 Kbps, with a range of 1 to 51200. At the bottom, there are two checkboxes: 'Ping' and 'HTTP', both of which are checked. The window has 'OK' and 'Cancel' buttons at the bottom right.

<input type="radio"/> PPPoE (ADSL User)	
<input type="radio"/> Dynamic IP Address (Cable Modem User)	
<input checked="" type="radio"/> Static IP Address	
IP Address	211.22.22.18
Netmask	255.255.255.0
MAC Address	00:AA:BB:D3:87:64
Default Gateway	211.22.22.18
Max. Downstream Bandwidth	51200 Kbps ( Range: 1 - 51200 )
Max. Upstream Bandwidth	51200 Kbps ( Range: 1 - 51200 )
Enable System Management	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
OK Cancel	

**Figure3-9 Static IP Address Connection**

Balance Mode : <span>Auto</span>							
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Static IP	211.22.22.18	<span>1</span>	✓	✓	<span>Modify</span>	<span>1</span>
2	(Disable)	---	<span>0</span>	---	---	<span>Modify</span>	<span>0</span>

**Figure3-10 Complete Static IP Address Connection Setting**



When selecting **Ping** and **WebUI** on **WAN** network Interface, users will be able to ping the ALL7008 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)

The screenshot shows a web interface for configuring the DMZ Interface. At the top, there is a tab labeled "DMZ Interface" and a dropdown menu set to "NAT". Below this, there are three input fields: "IP Address" with the value "192.168.189.222", "Netmask" with the value "255.255.255.0", and "MAC Address" with the value "00:aa:bb:d3:87:67". At the bottom, there is a section for "Enable System Management" with two checkboxes: "Ping" and "HTTP", both of which are checked. At the very bottom right, there are "OK" and "Cancel" buttons.

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

## Setting DMZ Interface Address (Transparent Mode)

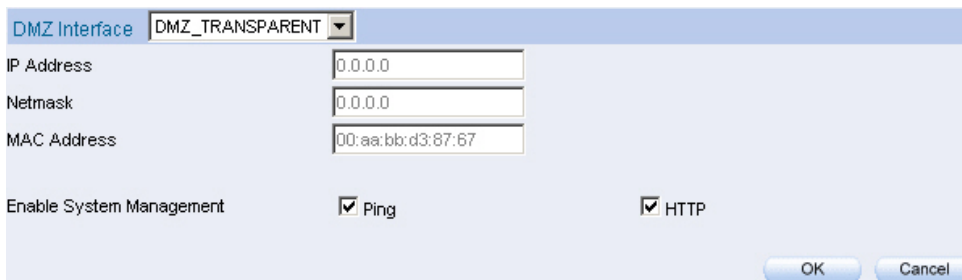
**STEP 1 .** Select **DMZ** Interface

**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)



DMZ Interface: DMZ\_TRANSPARENT

IP Address: 0.0.0.0

Netmask: 0.0.0.0

MAC Address: 00:aa:bb:d3:67:67

Enable System Management: ☒ Ping ☒ HTTP

OK Cancel

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 ALL7008 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	<b>LAN</b>	Under DHCP circumstances, assign the specific IP to static users and restrict them to access FTP net service only through policy.	<b>62</b>
Ex2	<b>LAN Group WAN</b>	Set up a policy that only allows partial users to connect with specific IP (External Specific IP)	<b>65</b>

## 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)

Add New Address	
Name	Rayearth
IP Address	192.168.3.2
Netmask	255.255.255.255
MAC Address	00:B0:18:25:F5:89 <span>Clone MAC</span>
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.	
<span>OK</span> <span>Cancel</span>	

**Figure 4-1 Setting LAN Address Book WebUI**

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<span>In Use</span>
Rayearth	192.168.3.2/255.255.255.255	00:B0:18:25:F5:89	<span>Modify</span> <span>Remove</span>

New Entry

**Figure4-2 Complete the Setting of LAN**

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

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	Rayearth
Destination Address	Outside_Any
Service	FTP
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)**

Source	Destination	Service	Action	Option				Configure			Move
Rayearth	Outside_Any	FTP	✓					Modify	Remove	Pause	To 1
New Entry											

**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 ALL7008 to fill out the user's MAC Address automatically.



In **LAN** of **Address** function, the ALL7008 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		<input type="button" value="In Use"/>
Rayearth	192.168.3.2/255.255.255.255	00:B0:18:25:F5:89	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
JJ	192.168.3.12/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
AJ	192.168.3.15/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Isaac	192.168.3.166/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>			

**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)

Add New Address Group

Name: TestTeam

<--- Available address --->  
Rayearth  
JJ  
AJ  
Isaac

<--- Selected address --->  
JJ  
AJ

Add

Remove

OK Cancel

**Figure4-6 Add New LAN Address Group**

Name	Member	Configure
TestTeam	JJ, AJ	<div>Modify Remove</div> <div>Pause</div>

New Entry

**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)

Add New Address	
Name	yahoo
IP Address	202.1.237.21
Netmask	255.255.255.255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Figure4-8 Add New WAN Address**

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
yahoo	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>		

**Figure4-9 Complete the Setting of WAN Address**



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

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	Rayearth
Destination Address	yahoo
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> 0 Kbps Upstream <input type="text"/> 0 Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/> 0
MAX. Concurrent Sessions	<input type="text"/> 0

OK Cancel

**Figure4-10 To Exercise Address Setting in Policy**

Source	Destination	Service	Action	Option					Configure			Move
Rayearth	yahoo	ANY	✓						Modify	Remove	Pause	To 1

New Entry

**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 ALL7008 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	<b>Custom</b>	Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15325-15333, UDP 15325-15333)	<b>72</b>
Ex2	<b>Group</b>	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)	<b>76</b>

**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)**

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
VoIP_01	192.168.1.2/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_02	192.168.1.3/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_03	192.168.1.4/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_04	192.168.1.5/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>			

**Figure5-1 Setting LAN Address Book WebUI**

Name	Member	Configure
VoIP_Group	VoIP_01, VoIP_02, VoIP_03...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>		

**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)

Add User Defined Service				
Service NAME :		VoIP		
#	Protocol ( Range: 1 - 255 )	Client Port ( Range: 0 - 65535 )	Server Port ( Range: 0 - 65535 )	
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0 : 65535	1720	01720
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0 : 65535	15328	15333
3	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other 17	0 : 65535	15328	15333
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0 : 0	0	0

OK Cancel

**Figure5-3 Add User Define Service**

Service name	Protocol	Client Port	Server Port	Configure
VoIP	TCP	0:65535	1720:01720	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

New Entry

**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)

Virtual Server Real IP

Service	WAN Port	Server Virtual IP	Configure
VoIP	From-Service(Custom)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

New Entry

Figure5-5 Compare Service to Virtual Server

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

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(59.124.36.173)	VoIP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

New Entry

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)

Source	Destination	Service	Action	Option	Configure	Move
VoIP_Group	Outside_Any	VoIP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

New Entry

Figure5-7 Complete the Policy for Internal VoIP to Connect with External VoIP



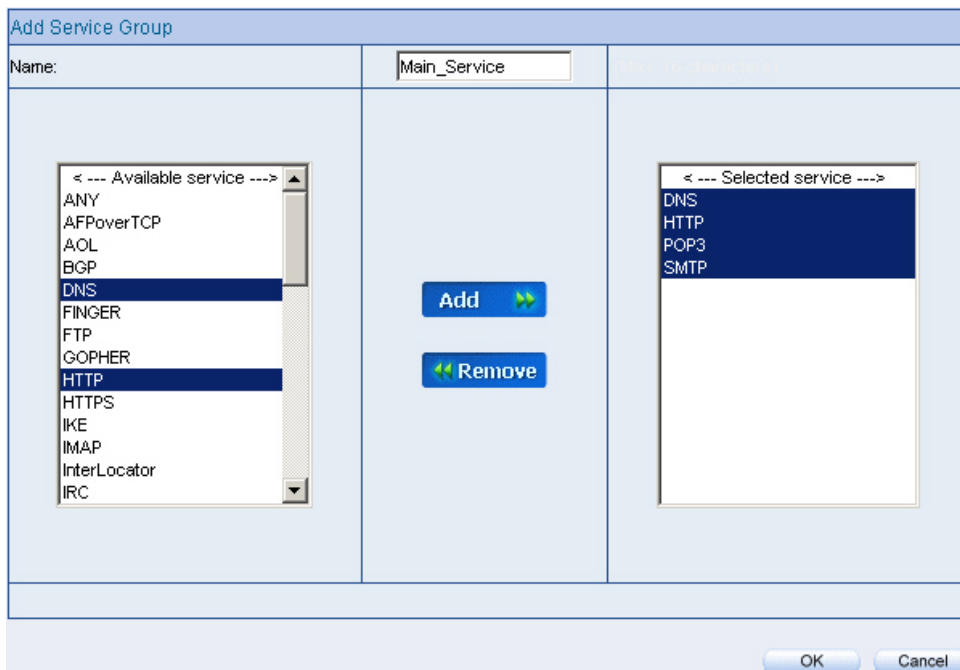
**Service** must cooperate with **Policy** and **Virtual Server** that the function can take effect



**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**

Group name	Service	Configure	
Main_Service	DNS,HTTP,POP3...	Modify	Remove
New Entry			

**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)**

Name	Member	Configure
laboratory	Isaac, AJ, Owen	<div>Modify Remove</div> <div>Pause</div>
<div>New Entry</div>		

**Figure5-10 Setting Address Book Group**

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

Source	Destination	Service	Action	Option					Configure	Move
laboratory	Outside_Any	Main_Service	✓						<div>Modify Remove Pause</div>	To 1 ▾
<div>New Entry</div>										

**Figure5-11 Setting Policy**

In this chapter, the ALL7008 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)

Day	Period	
	Start Time	Stop Time
Monday	08:30	18:30
Tuesday	08:30	18:30
Wednesday	08:30	18:30
Thursday	08:30	18:30
Friday	All day	All day
Saturday	Disable	Disable
Sunday	Disable	Disable

**Figure6-1 Setting Schedule WebUI**

Name	Configure
WorkingTime	<button>Modify</button> <button>Remove</button>

New Entry

**Figure6-2 Complete the Setting of Schedule**

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

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	✓	🕒					Modify	Remove	Pause	To 1 ▾
New Entry												

Figure6-3 Complete the Setting of Comparing Schedule with Policy



The Schedule must compare with **Policy** or **VPN** (Figure6-4, 6-5, 6-6)

GRE Local IP	<input type="text"/>
GRE Remote IP	<input type="text"/>
Schedule	WorkingTime ▾
QoS	None ▾
Authentication-User	None ▾
<input type="checkbox"/> Show remote Network Neighborhood	
OK Cancel	

Figure6-4 Compare Policy with VPN or IPSec Autokey

Client IP Range :	<input type="text" value="192.230.182.1"/> -- <input type="text" value="254"/>
Auto-Disconnect if idle	<input type="text" value="0"/> minutes (0: means always connected)
Schedule	WorkingTime ▾
OK Cancel	

Figure6-5 Compare Schedule with VPN or PPTP Server

<input type="checkbox"/> Auto-Connect when sending packet through the link	
Auto-Disconnect if idle	<input type="text" value="0"/> minutes (0: means always connected)
Schedule	WorkingTime ▾

Figure6-6 Compare Schedule with VPN or PPTP Server



## 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 ALL7008 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The ALL7008 also makes it convenient for the administrator to make the Bandwidth to reach the best utility. (Figure7-1, 7-2)

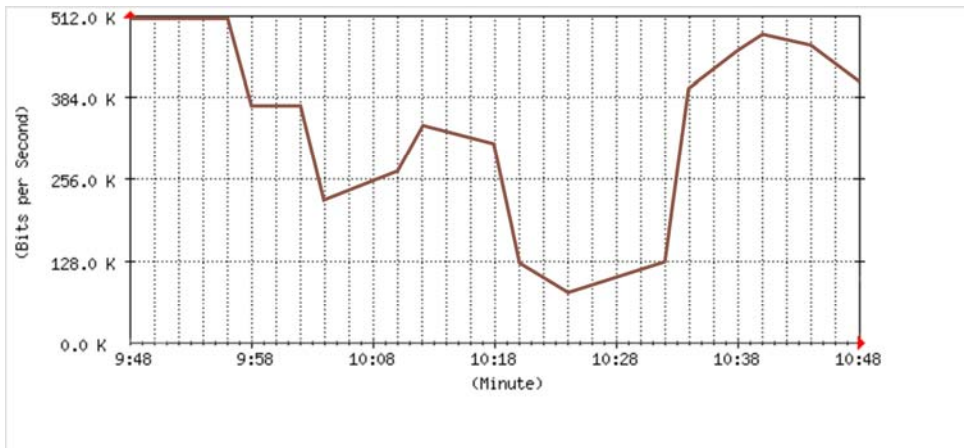


Figure7-1 the Flow Before Using QoS



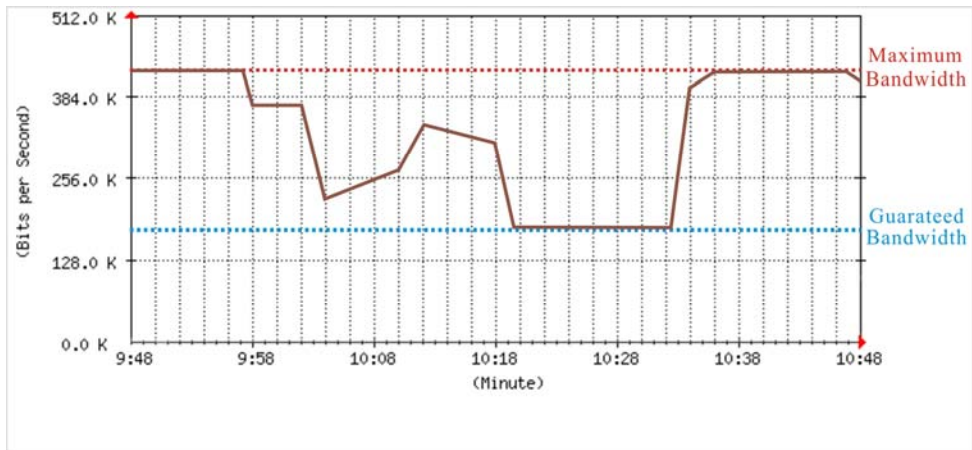


Figure7-2 the Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

## 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	<b>QoS</b>	Setting a policy that can restrict the user's downstream and upstream bandwidth.	<b>87</b>
Ex2	<b>QoS</b>	Setting a connection of IPSec Autokey in VPN that can restrict the traffic.	<b>89</b>

# 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)

Add New QoS

Name

Policy\_Qos

WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority
1	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	Middle
2	G.Bandwidth = 300 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 64 Kbps	

OK

Cancel

Figure7-3 QoS WebUI Setting

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Policy_Qos	1	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	Middle	<div>Modify</div> <div>Remove</div>
	2	G.Bandwidth = 300 Kbps M.Bandwidth = 400 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 64 Kbps		

New Entry

Figure7-4 Complete the QoS Setting

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



Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	WorkingTime
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	Policy_Qos
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> 0 Kbps Upstream <input type="text"/> 0 Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/> 0
MAX. Concurrent Sessions	<input type="text"/> 0

OK Cancel

**Figure7-5 Setting the QoS in Policy**

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

**Figure7-6 Complete Policy Setting**

# Setting a connection of IPSec Autokey in VPN that can restrict the traffic

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

- Click **New Entry** (Figure7-7)
- **Name**: The name of the QoS you want to configure.
- Enter the bandwidth you want to restrict in **Downstream Bandwidth** and **Upstream Bandwidth**
- **QoS Priority** : Select Middle
- Click **OK** (Figure7-8)

Add New QoS

Name

VPN\_Qos

WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority
1	G.Bandwidth = <input type="text" value="100"/> Kbps M.Bandwidth = <input type="text" value="200"/> Kbps	G.Bandwidth = <input type="text" value="100"/> Kbps M.Bandwidth = <input type="text" value="150"/> Kbps	Middle ▾
2	G.Bandwidth = <input type="text" value="200"/> Kbps M.Bandwidth = <input type="text" value="300"/> Kbps	G.Bandwidth = <input type="text" value="20"/> Kbps M.Bandwidth = <input type="text" value="30"/> Kbps	

OK

Cancel

Figure7-7 QoS WebUI Setting

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
VPN_Qos	1	G.Bandwidth = 100 Kbps M.Bandwidth = 200 Kbps	G.Bandwidth = 100 Kbps M.Bandwidth = 150 Kbps	Middle	<div>Modify</div> <div>Remove</div>
	2	G.Bandwidth = 200 Kbps M.Bandwidth = 300 Kbps	G.Bandwidth = 20 Kbps M.Bandwidth = 30 Kbps		

New Entry

Figure7-8 Complete the QoS Setting

**STEP 2 .** Select the QoS that set by STEP1 in **IPSec** of **VPN**. (Figure7-9)

Schedule	None ▾
QoS	VPN_QoS ▾
Authentication-User	None ▾
<input type="checkbox"/> Show remote Network Neighborhood	
<div>OK Cancel</div>	

**Figure7-9 QoS Setting of IPSec**



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.

# Authentication

By configuring the Authentication, you can control the user's (Internal user or remote user who connect by VPN and IPSec) connection authority. The user has to pass the authentication to access to Internet.

The ALL7008 configures the authentication of LAN's user by setting account and password to identify the privilege. Or by the RADIUS that set by yourself. The system administrator can use this two mode to manage the Authentication.



## Define the required fields of Authentication

### Authentication Management

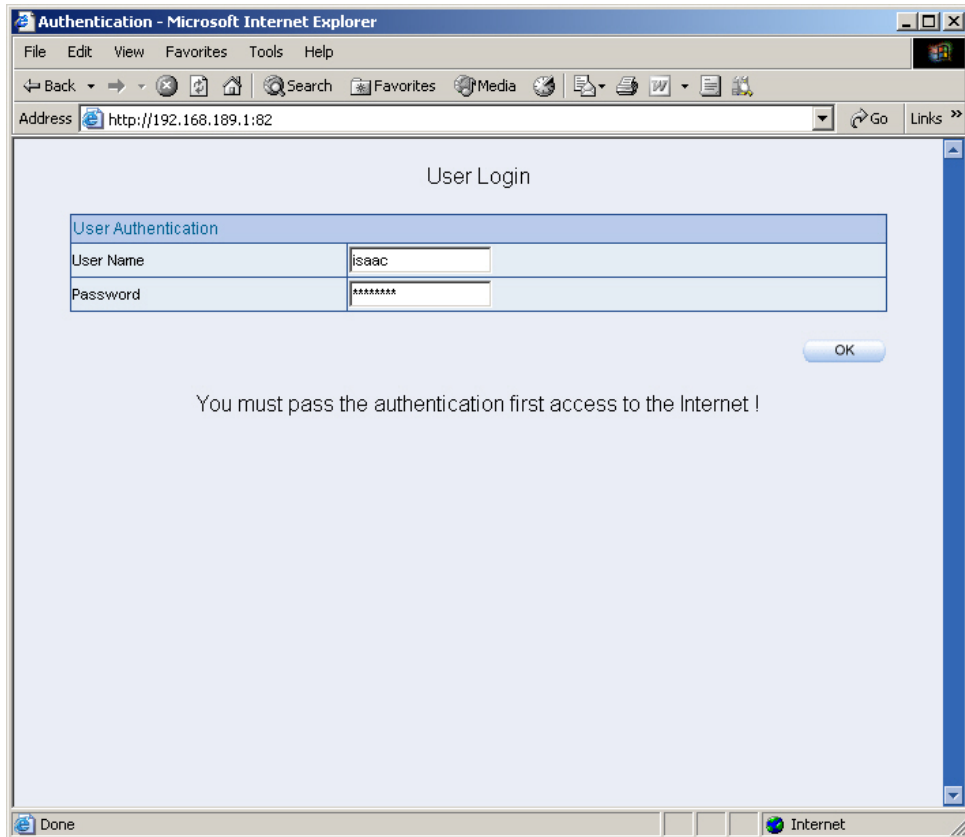
- Provide the Administrator the port number and valid time to setup ALL7008 authentication. (Have to setup the Authentication first)
  - ◆ **Authentication Port:** The internal user have to pass the authentication to access to the Internet when enable ALL7008.
  - ◆ **Re-Login if Idle:** When the internal 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)

The screenshot shows the 'Authentication Management' web interface. It contains several input fields and a text area. The 'Authentication Port' is set to 82. 'Re-Login if Idle' is set to 30 minutes. 'Re-Login after user login successfully' is set to 0 hours. There is a checkbox for 'Deny multi-login if the auth user has login' which is unchecked. The 'URL to redirect when authentication succeed' is set to 'www.nusoft.com.tw'. The 'Messages to display when user login' text area contains the message: 'You must pass the authentication first access to the Internet !'. At the bottom right are 'OK' and 'Cancel' buttons.

Authentication Management	
Authentication Port	82 ( Range: 1 - 65535, Deny multi-login if the auth user has login )
Re-Login if Idle	30 Minutes ( Range: 1 - 1000 )
Re-Login after user login successfully	0 Hours ( Range: 0 - 24, 0: means unlimited )
<input type="checkbox"/> Deny multi-login if the auth user has login	
URL to redirect when authentication succeed	www.nusoft.com.tw (Max. 60 characters)
Messages to display when user login	
You must pass the authentication first access to the Internet !	
OK Cancel	

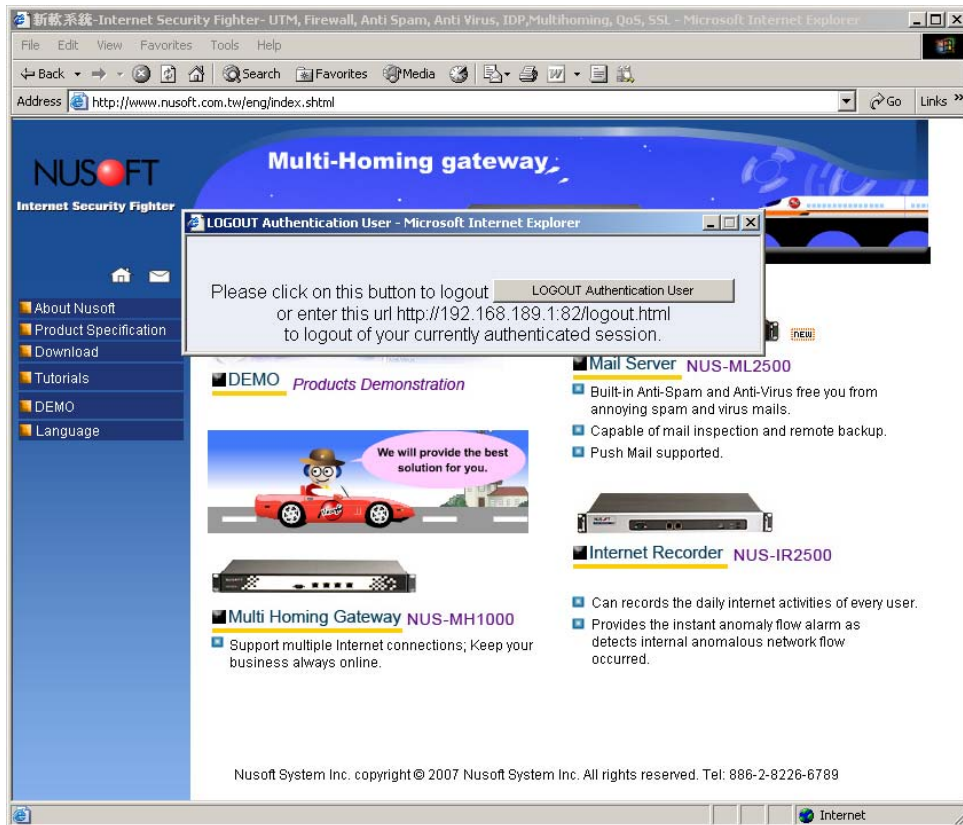
Figure8-1 Authentication Setting WebUI

- 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

**Shared Secret:**

- The password for authentication of the ALL7008 and RADIUS Server

**802.1xRADIUS:**

- The Authentication to RADIUS Server of wireless network

We set up four Authentication examples in this chapter:

No	Suitable Situation	Example	Page
Ex1	<b>Auth User</b>	Setting a specific user to connect with external network only before passing the authentication of policy. ( Adopt the built-in Auth User Function )	<b>97</b>
Ex2	<b>Auth Group</b>	Setting external users to connect with internal network only before passing the authentication of VPN IPsec Autokey. ( Adopt the built-in Auth User Group Function )	<b>101</b>
Ex3	<b>RADIUS</b>	Setting the users to connect with external network only before passing the authentication of policy. (Adopt the external RADIUS Server built-in Windows 2003 Server Authentication)	<b>105</b>
Ex4	<b>POP3</b>	Setting the users to connect with external network only before passing the authentication of policy. (Adopt the external POP3 Server Authentication)	<b>126</b>

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

**STEP 1** . Setting the user's Address in **LAN** of **Address** function. (Figure8-4)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
user_01	192.168.3.5/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure8-4 LAN Address Setting



To use Authentication, the DNS Server of the user's network card must be the same as the LAN Interface Address of ALL7008.

**STEP 2 .** Enter the following setting in **Auth** of **Authentication** function:

- Click **New User**
- **Auth-User Name:** Enter guest
- **Password:** Enter 1234
- **Confirm Password:** Enter 1234
- Click **OK**
- Complete Authentication Setting (Figure8-5)

Add New Authentication User	
Authentication User Name	<input type="text" value="guest"/>
Password	<input type="password" value="****"/>
Confirm Password	<input type="password" value="****"/>

**Figure8-5 Add New Auth-User WebUI**

**STEP 3 .** Add a policy in **Outgoing Policy** and input the Address and Authentication of STEP1, 2 (Figure8-6, 8-7)

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	user_01
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**Figure8-6 Auth-User Policy Setting**

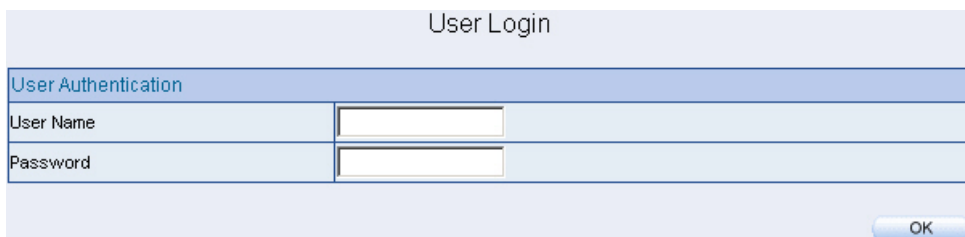
Source	Destination	Service	Action	Option					Configure			Move
user_01	Outside_Any	ANY	✓						Modify	Remove	Pause	To 1
New Entry												

**Figure8-7 Complete the Policy Setting of Auth-User**



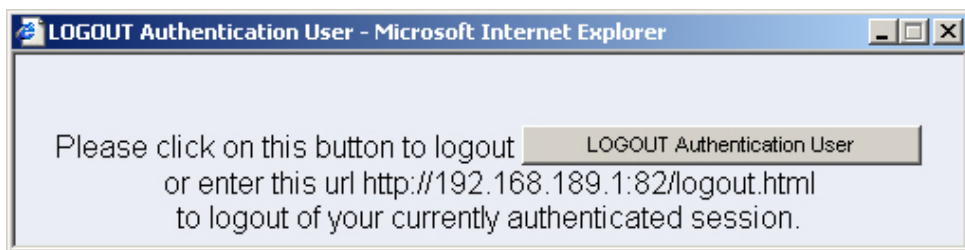
**STEP 4 .** When user\_01 is going to access to Internet through browser, the authentication UI will appear in Browser. After entering the correct user name and password, click **OK** to access to Internet. (Figure8-8)

**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](http://LAN Interface: Authentication port number/logout.html)) to logout (Figure8-9)



The image shows a web form titled "User Login". It has a light blue header bar with the title. Below the header is a section titled "User Authentication" in a darker blue bar. Under this section, there are two input fields: "User Name" and "Password". Each field has a small white text box with a cursor. To the right of the "Password" field is an "OK" button with a blue gradient and white text.

**Figure8-8 Access to Internet through Authentication WebUI**



**Figure8-9 Logout Auth-User WebUI**

**Setting external users to connect with internal network only before passing the authentication of VPN IPsec Autokey. (Adopt the built-in Auth User Group Function)**

**STEP 1 .** Setup several **Auth User** in **Authentication**. (Figure8-10)

Authentication User Name	Configure	
isaac	Modify	Remove
guest	Modify	Remove
ajaj	Modify	Remove
owen	Modify	Remove
New Entry		

**Figure8-10 Setting Several Auth Users WebUI**

**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 (Figure8-11)

New Authentication Group

Name: laboratory

< ---Available Authentication User --->

- isaac
- guest
- ajaj
- owen
- (Radius User)
- (POP3 User)

Add

Remove

< --- Selected Authentication User --->

- isaac
- guest
- ajaj
- owen

OK Cancel

**Figure8-11 Setting Auth Group WebUI**

**STEP 3 .** Add a IPSec Autokey rule in **VPN** includes the Auth User Group of STEP 2. (Figure8-12)

Schedule	None
QoS	None
Authentication-User	laboratory
<input type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

**Figure8-12 Compare Authentication with IPSec Autokey**

**STEP 4 .** When external users try to connect with the PC of the ALL7008 by IPSec Autokey, they must pass the authentication first. (Figure8-13)

User Login

User Authentication	
User Name	<input type="text"/>
Password	<input type="password"/>

OK

**Figure8-13 Set Up the IPSec VPN Connection by Authentication**

**STEP 5** . If the remote user does not need connection and is going to logout, he/she can click the **LOGOUT Auth-User** button or enter the Logout Authentication WebUI ([http:// LAN Interface: Authentication port number/logout.html](http://LAN Interface: Authentication port number/logout.html)) to logout (Figure8-14)



**Figure8-14 Logout Auth-User WebUI**

## Setting the users to connect with external network only before passing the authentication of policy. (Adopt external RADIUS Server built-in Windows 2003 Server Authentication)

### ※ Windows 2003 RADIUS Server Setting Way

**STEP 1** . Click [Start] → [Control Panel] → [Add/Remove Program], Choose [Add/Remove Windows] and then you can see [Window Component Wizard]

**STEP 2** . Choose **Networking Services** and click **Details** (Figure8-15)

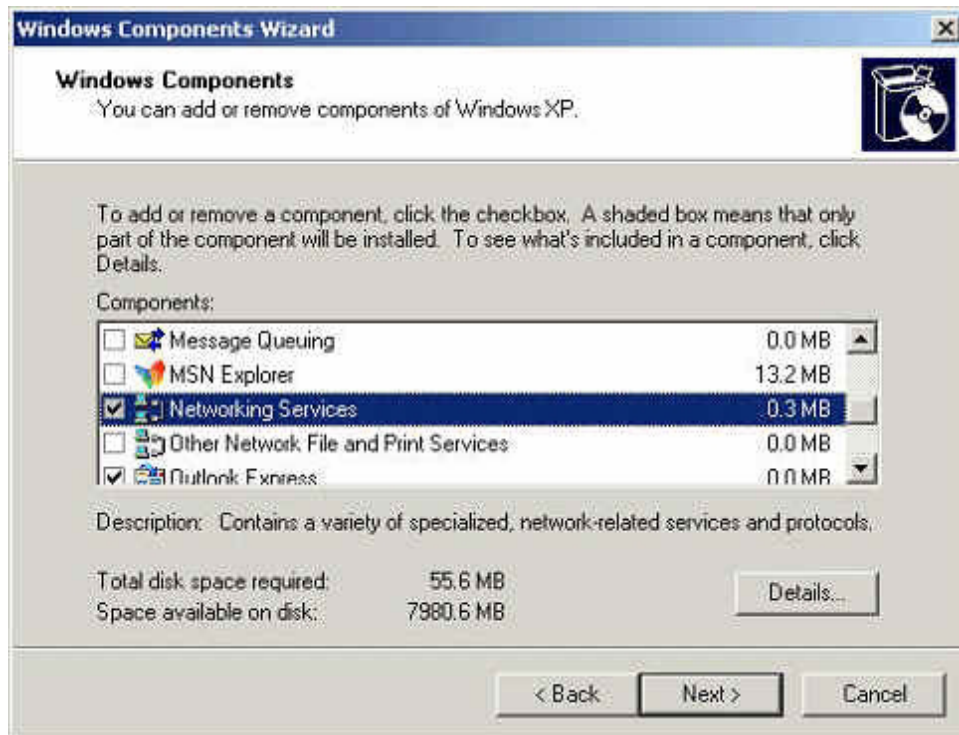


Figure8-15 Add Windows Components WebUI

### STEP 3 . Choose Internet Authentication Service (IAS) (Figure8-16)

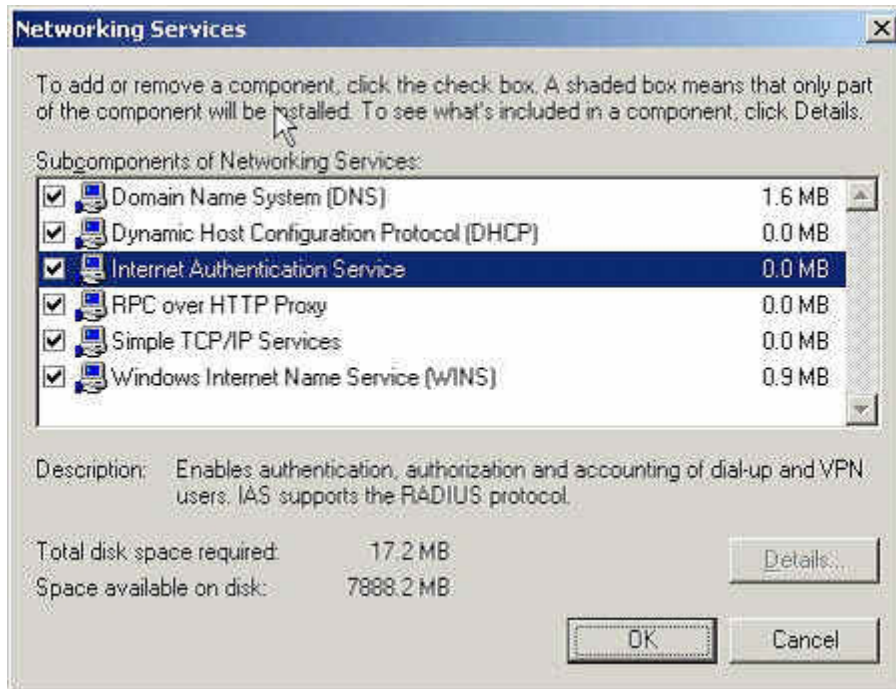
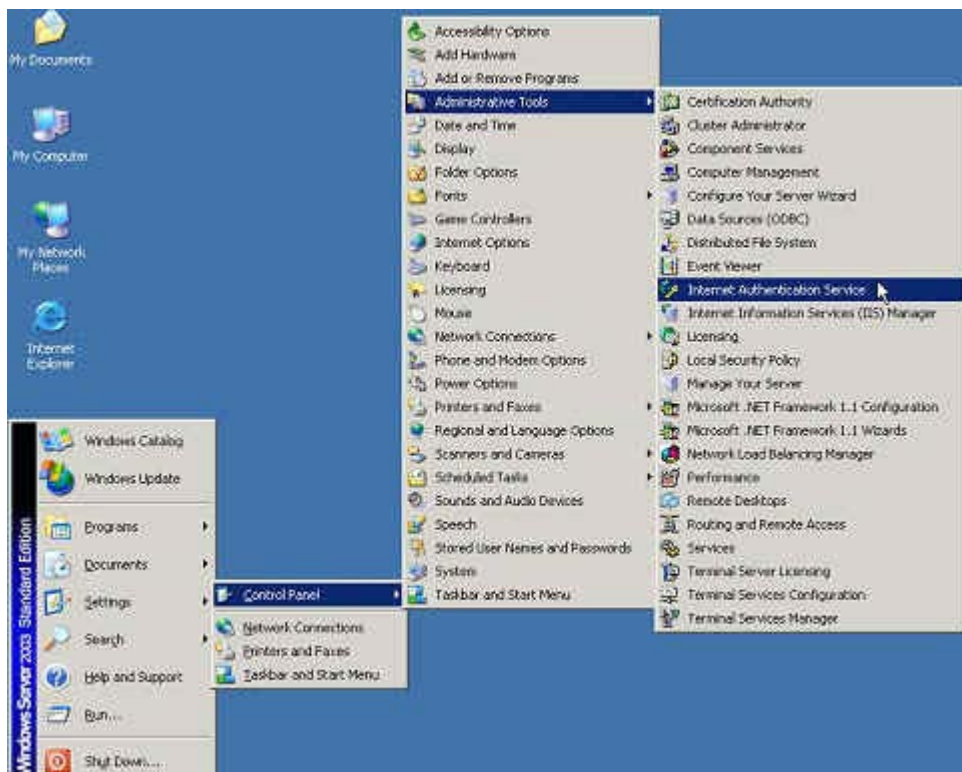


Figure8-16 Add New Internet Authentication Services WebUI

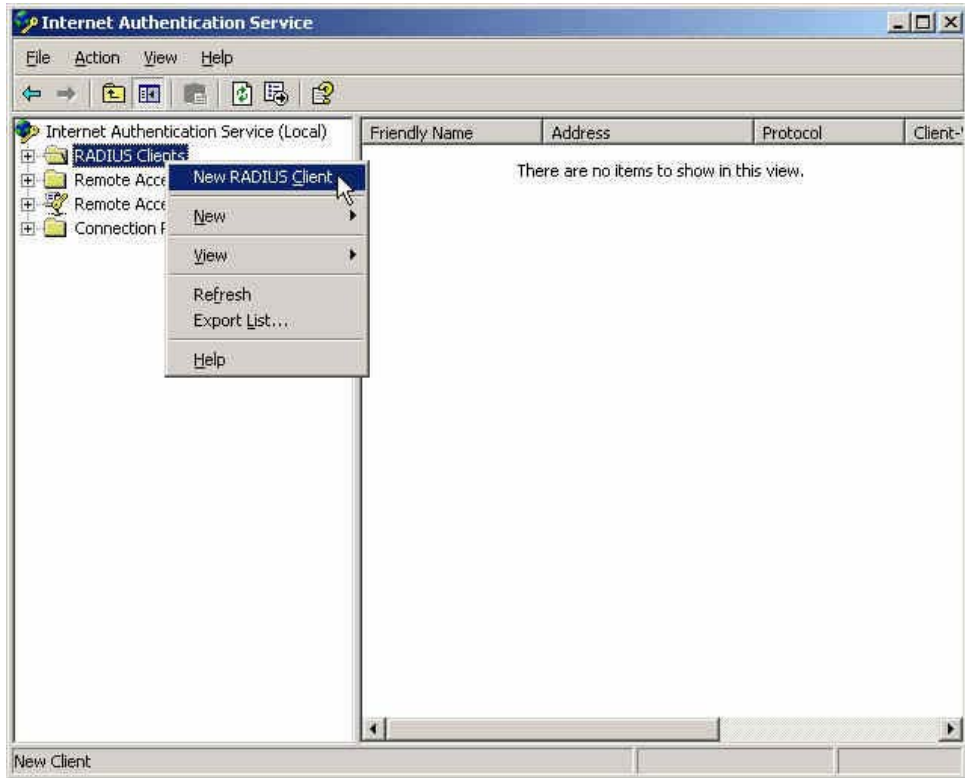
**STEP 4 .** Click [Start] → [Control Panel] → [Administrative Tools], Choose [Internet Authentication Service] (Figure8-17)



**Figure8-17 Choose Internet Authentication Service**

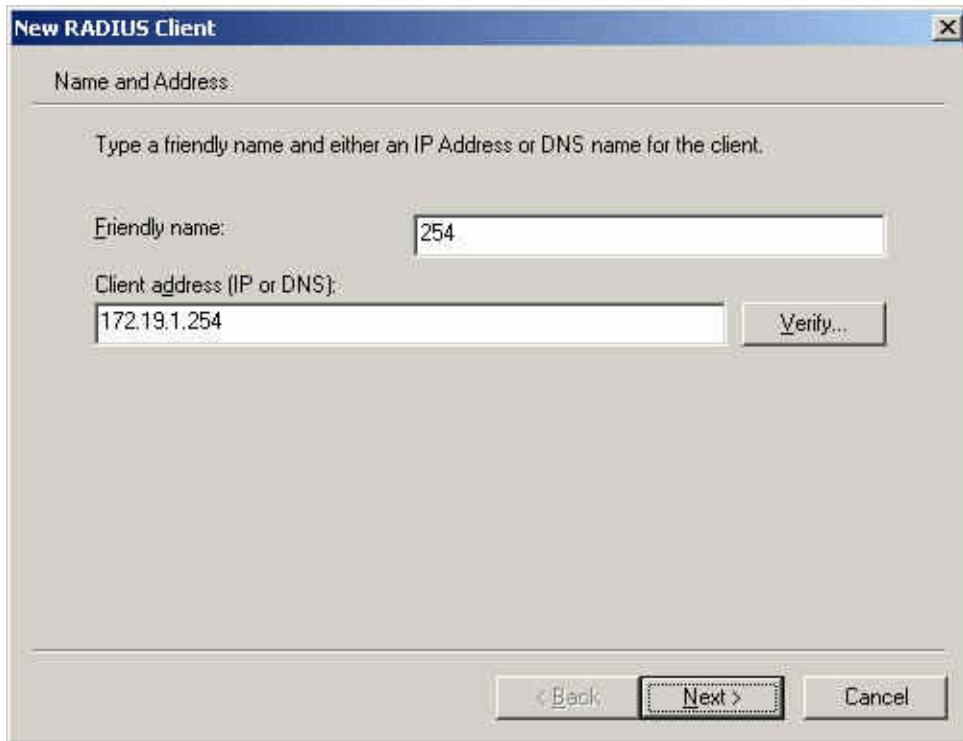


**STEP 5 .** Press right button on **RADIUS Clients** and choose **New RADIUS Client** (Figure8-18)



**Figure8-18 Add New RADIUS Client**

**STEP 6 .** Enter the **Name** and **Client Address** (also the ALL7008 IP)  
(Figure8-19)

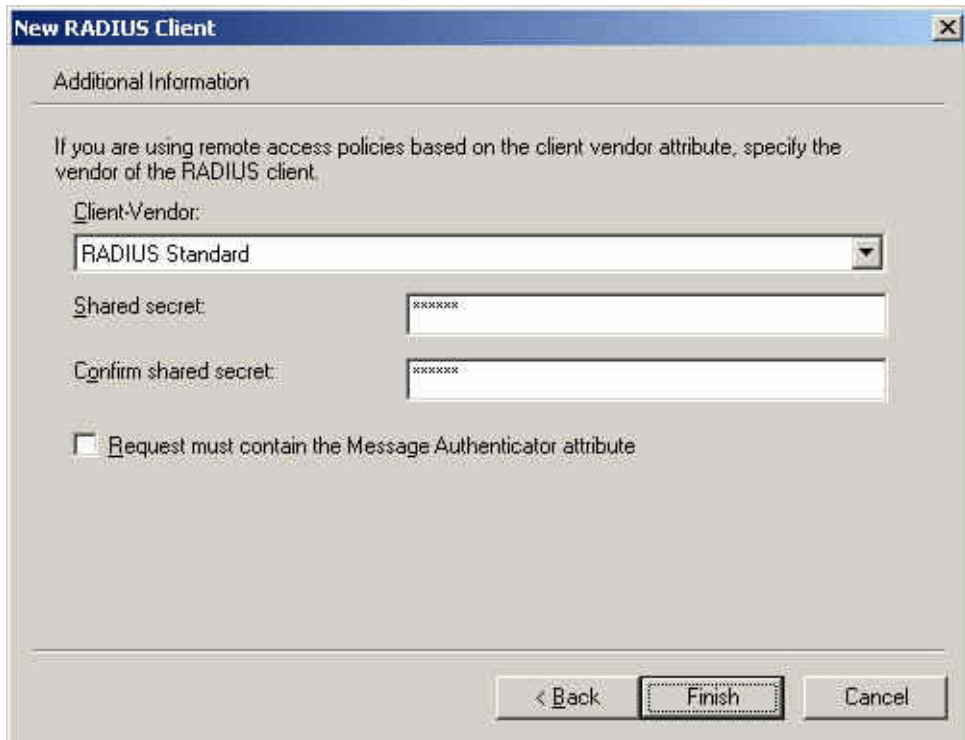


The image shows a Windows-style dialog box titled "New RADIUS Client". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the following elements:

- A section header "Name and Address:" followed by a horizontal line.
- Instructional text: "Type a friendly name and either an IP Address or DNS name for the client."
- A label "Friendly name:" followed by a text input field containing the value "254".
- A label "Client address (IP or DNS):" followed by a text input field containing the value "172.19.1.254".
- A "Verify..." button located to the right of the client address input field.
- At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

**Figure8-19 Add New RADIUS Client Name and Address**

**STEP 7 .** Choose **RADIUS Standard**; enter **Shared Secret** and **Confirm Shared Secret**. (The settings must be the same as RADIUS of ALL7008) (Figure8-20)



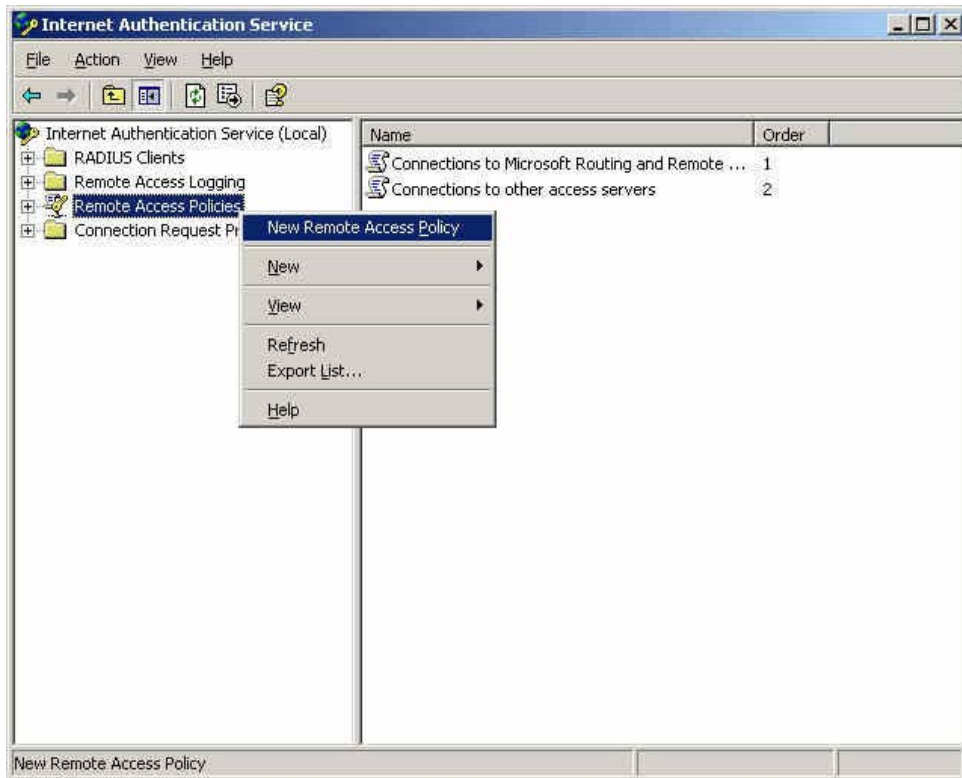
The image shows a Windows-style dialog box titled "New RADIUS Client". It has a blue title bar with a close button (X) in the top right corner. The main area is titled "Additional Information" and contains the following elements:

- A text label: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client."
- A label "Client-Vendor:" followed by a dropdown menu currently showing "RADIUS Standard".
- A label "Shared secret:" followed by a text input field containing "XXXXXXXX".
- A label "Confirm shared secret:" followed by a text input field containing "XXXXXXXX".
- A checkbox labeled "Request must contain the Message Authenticator attribute", which is currently unchecked.

At the bottom of the dialog, there are three buttons: "< Back", "Finish" (which is highlighted with a dashed border), and "Cancel".

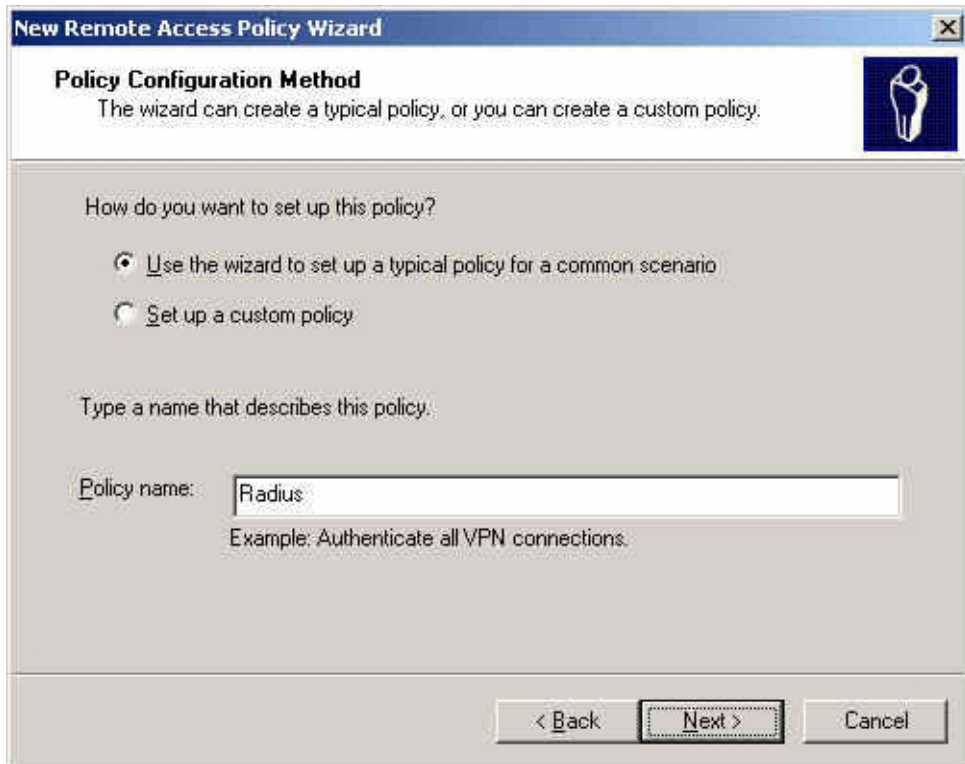
**Figure8-20 Add New RADIUS Client and Password WebUI**

**STEP 8 .** Press the right button on **Remote Access Policies** and select to add **New Remote Access Policy**. (Figure8-21)



**Figure8-21 Add New Remote Access Policy**

**STEP 9 .** Select **Use the wizard to set up a typical policy for a common scenario** and enter the **Policy name**. (Figure8-22)



The image shows a Windows-style dialog box titled "New Remote Access Policy Wizard". It has a blue header bar with the title and a close button (X). Below the header, there's a section titled "Policy Configuration Method" with a small icon of a person. The text says "The wizard can create a typical policy, or you can create a custom policy." Below this, there's a question "How do you want to set up this policy?" with two radio button options: "Use the wizard to set up a typical policy for a common scenario" (which is selected) and "Set up a custom policy". Below the options, there's a text prompt "Type a name that describes this policy:" followed by a text input field containing the word "Radius". Below the input field, there's an example text: "Example: Authenticate all VPN connections." At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

**New Remote Access Policy Wizard**

**Policy Configuration Method**  
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

☒ Use the wizard to set up a typical policy for a common scenario

☐ Set up a custom policy

Type a name that describes this policy:

Policy name:

Example: Authenticate all VPN connections.

< Back   Next >   Cancel

**Figure8-22 Add Remote Access Policy and Name**

## STEP 10 . Select **Ethernet** (Figure8-23)



**Figure8-23 Add New Remote Access Policy Method**

## STEP 11 . Choose **User** (Figure8-24)

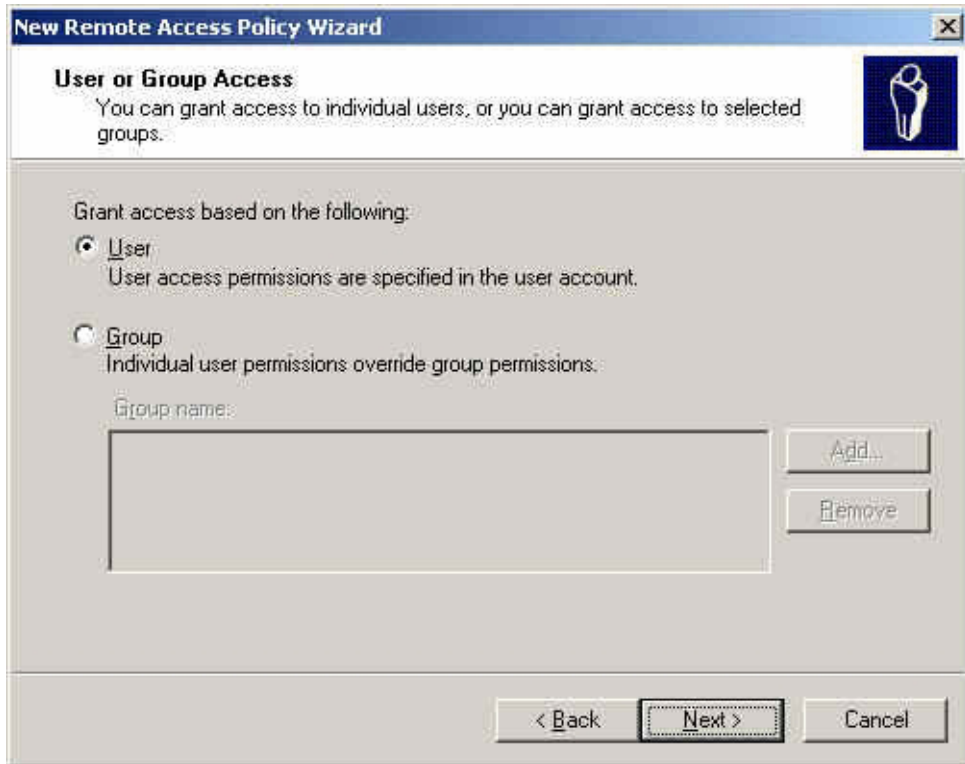
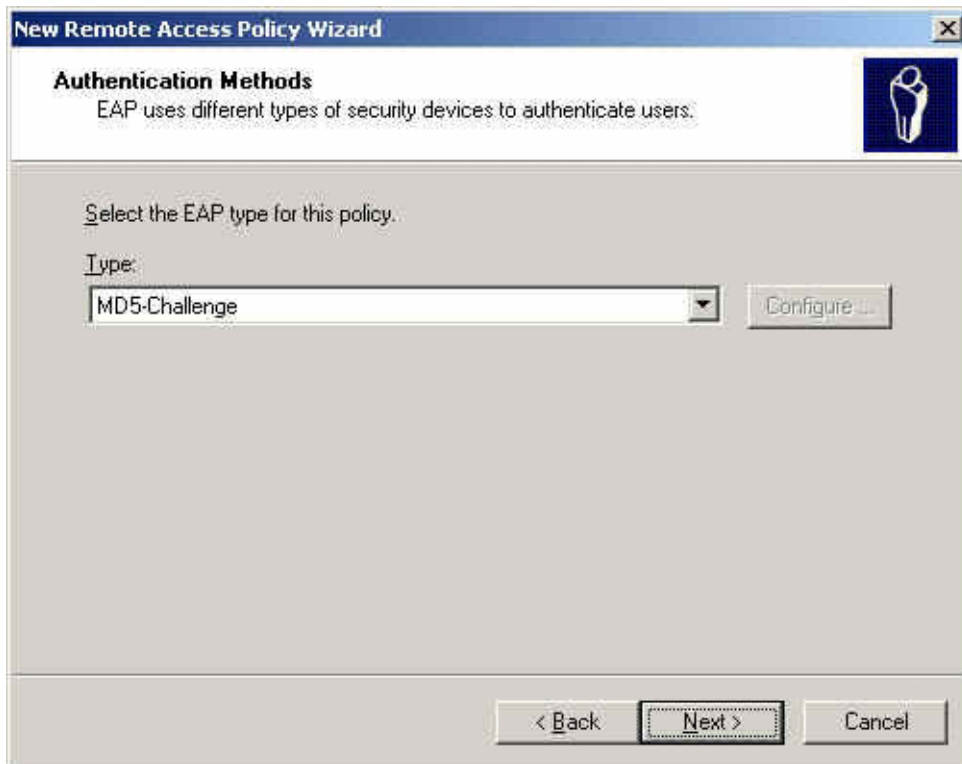


Figure8-24 Add New Remote Access Policy of User or Group Access

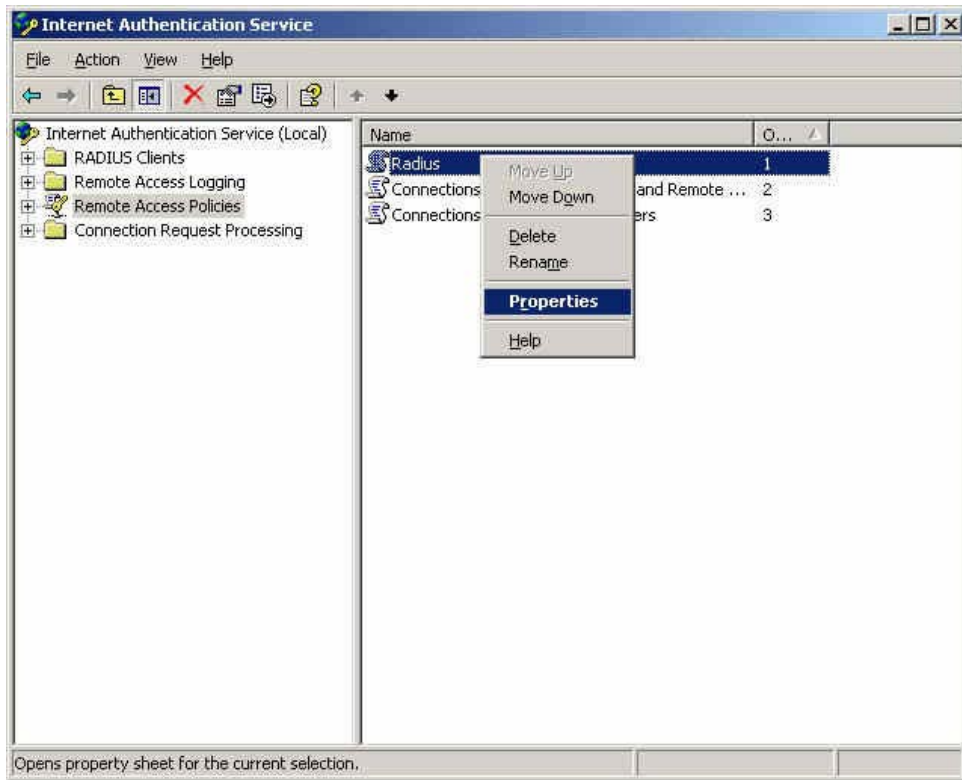
**STEP 12 . Select MD5-Challenge (Figure8-25)**



**Figure8-25 Authentication Methods of Adding New Remote Access Policy**

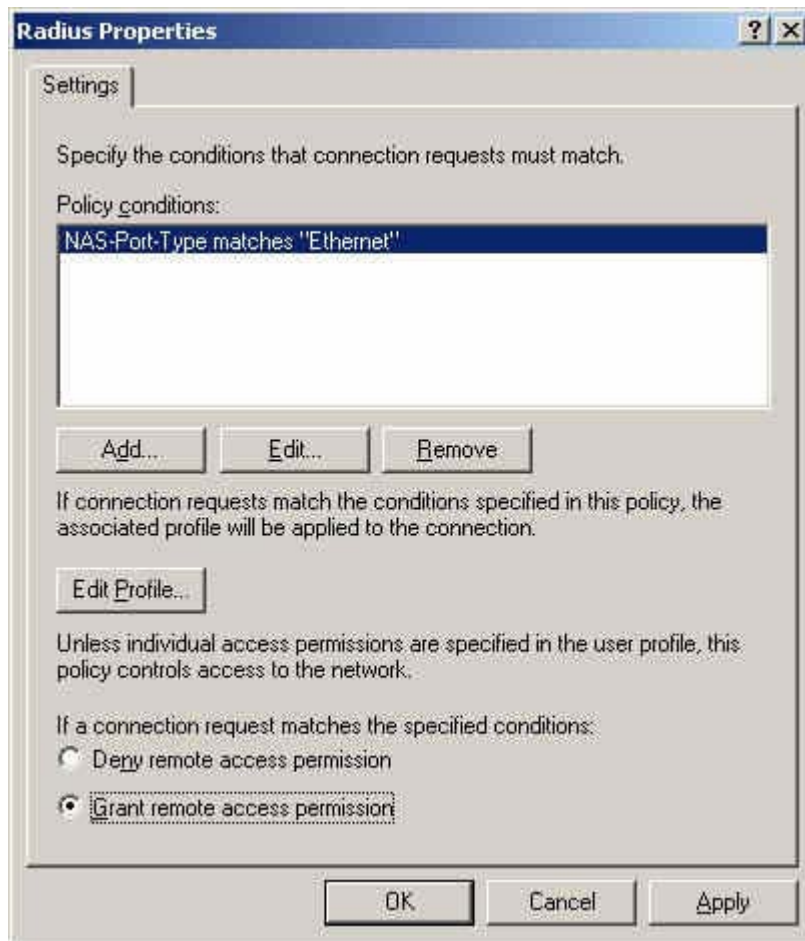


**STEP 13 .** Press the right button on **Radius** and choose **Properties**.  
(Figure8-26)



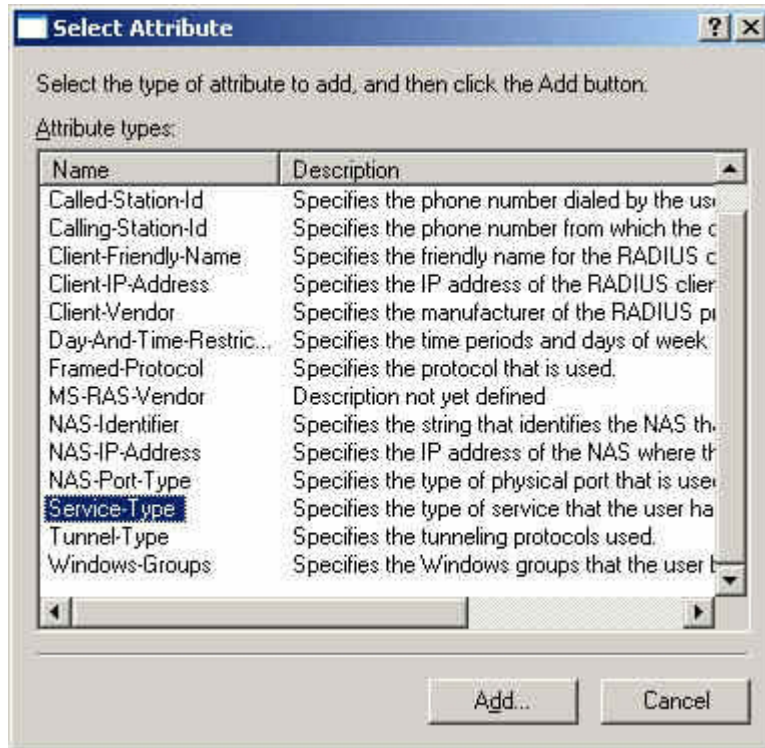
**Figure8-26 Internet Authentication Service Setting WebUI**

**STEP 14 .** Select **Grant remote access permission** and **Remove** the original setting, click **Add** to add a new one. (Figure8-27)



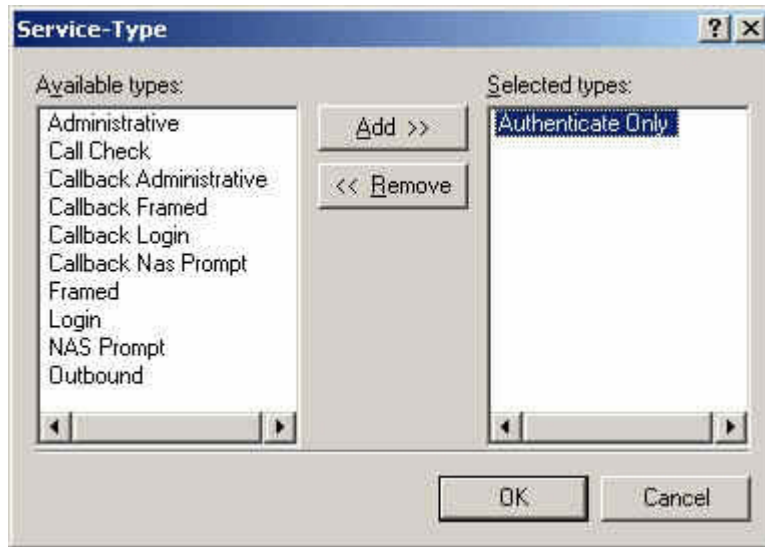
**Figure8-27 RADIUS Properties Settings**

## STEP 15 . Add **Service-Type** (Figure8-28)



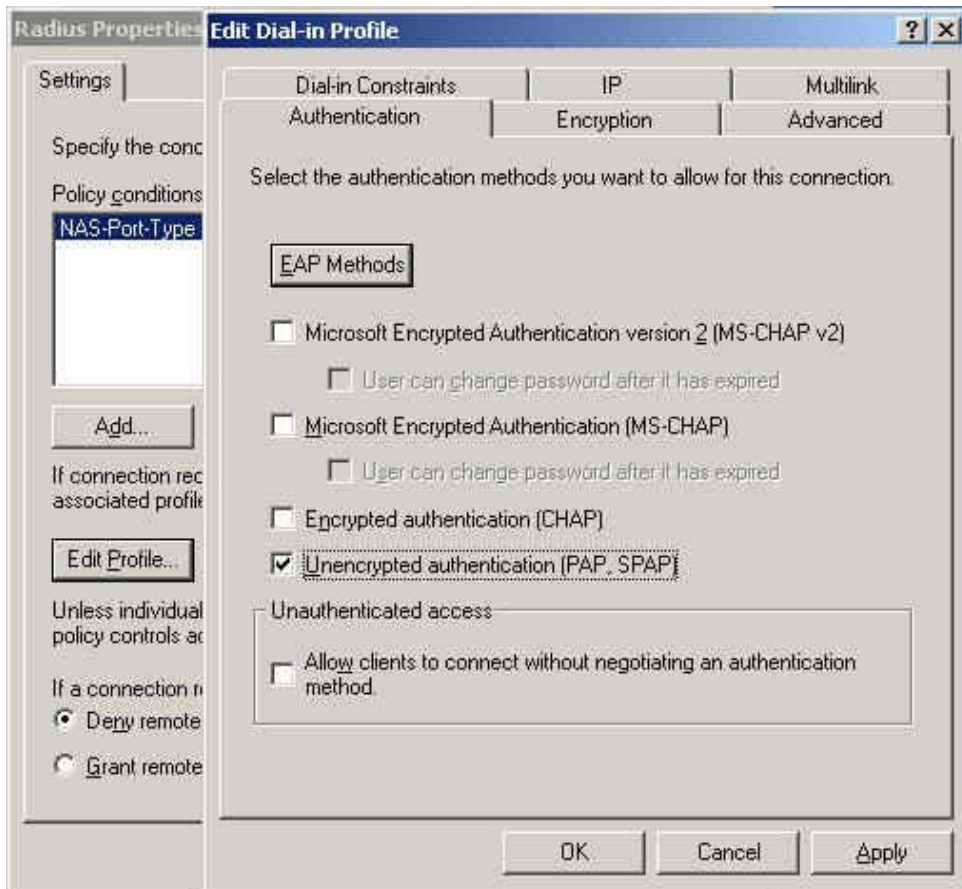
**Figure8-28 Add New RADIUS Attribute**

**STEP 16 . Add **Authenticate Only** from the left side. (Figure8-29)**



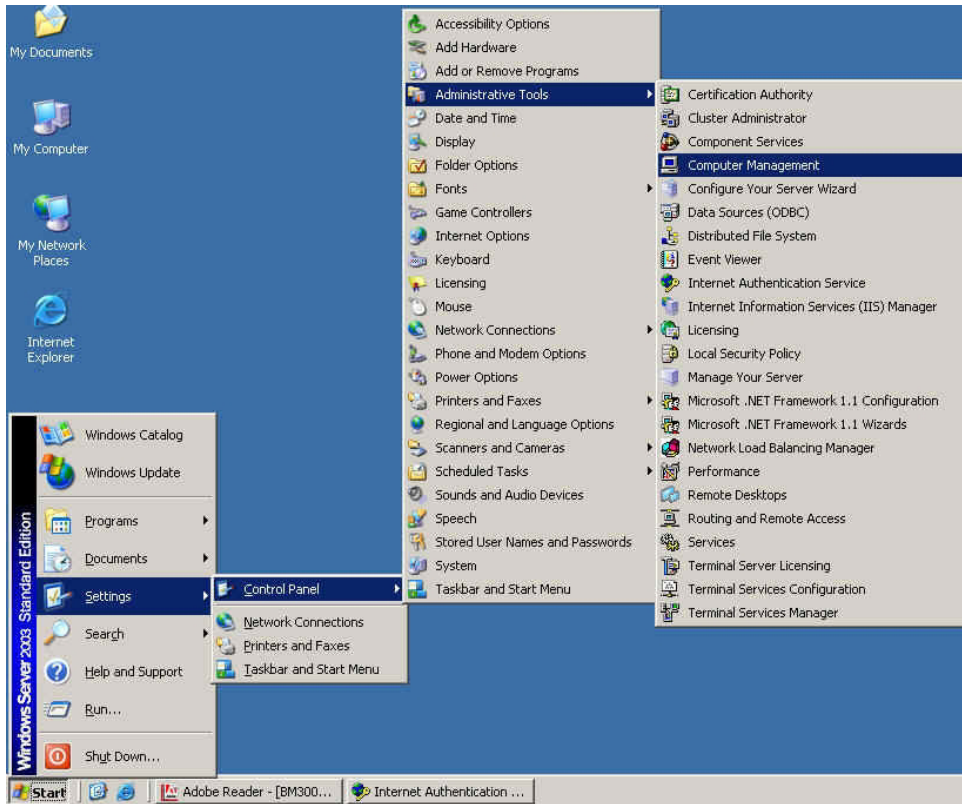
**Figure8-29 Add RADIUS Service-Type**

**STEP 17 . Press **Edit Profile** button and select **Authentication** and select **Unencrypted authentication (PAP, SPAP)** (Figure8-30)**



**Figure8-30 Edit DADIUS Dial-in Property**

**STEP 18 . Add Auth User.** Click [Start] → [Setting]→ [Control Panel] → [Administrative Tools], Choose [Computer Management] (Figure8-31)



**Figure8-31 Enter Computer Management**

**STEP 19 .** Press the right button on the **Users** and select **New User**.  
(Figure8-32)



**Figure8-32 Add New User**

**STEP 20 .** Complete the setting of Windows 2003 RADIUS Server.

**STEP 21 . Enter IP, Port and Shared Secret** (The setting must be the same as RADIUS Server) in **RADIUS of Authentication** (Figure8-33)

The screenshot shows a window titled "RADIUS Server" with a light blue header. Inside, there are two main sections. The first section has a checked checkbox labeled "Enable RADIUS Server Authentication". Below it are three input fields: "RADIUS Server IP" with the value "172.19.250.10" and a note "(Max. 60 characters)", "RADIUS Server Port" with the value "1812" and a note "( Range: 1025 - 65535 )", and "Shared Secret" with the value "master" and a note "(Max. 80 characters)". The second section has an unchecked checkbox labeled "Enable 802.1x RADIUS Server Authentication". At the bottom right are "OK" and "Cancel" buttons.

Figure8-33 Setting RADIUS Server

**STEP 22 . Add Radius User in Auth User Group of Authentication.**  
(Figure8-34)

The screenshot shows a window titled "New Authentication Group" with a light blue header. It has a "Name:" label and a text box containing "Radius". Below this is a large area divided into three parts. On the left is a list box titled "<--- Available Authentication User --->" containing the items: "isaac", "guest", "ajaj", "owen", "(Radius User)", and "(POP3 User)". The "(Radius User)" item is selected. In the center are two buttons: "Add" with a right-pointing arrow and "Remove" with a left-pointing arrow. On the right is a list box titled "<--- Selected Authentication User --->" containing the item "(Radius User)". At the bottom right are "OK" and "Cancel" buttons.

Figure8-34 Add New RADIUS Auth Group



**STEP 23 . Add a policy of **Auth User Group** (RADIUS) that set by **STEP 22** in **Outgoing Policy**. (Figure8-35, 8-36)**

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	Radius
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

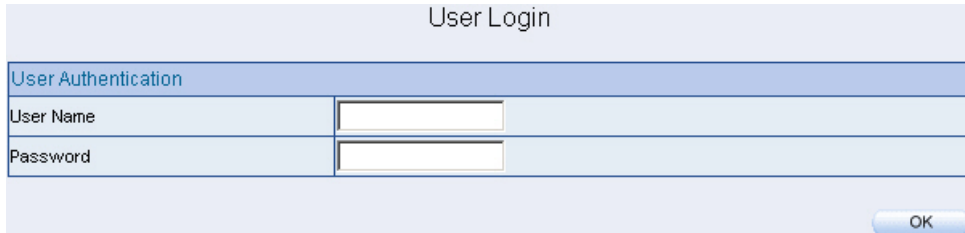
OK Cancel

**Figure8-35 RADIUS Authentication Policy Setting WebUI**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	✓	🔑					Modify	Remove	Pause	To 1
New Entry												

**Figure8-36 Complete RADIUS Authentication of Policy Setting**

**STEP 24 .** When the user is going to connect with Internet through browser, the Authentication windows will appear in browser. After entering the correct account and password can connect with Internet through ALL7008. (Figure8-37)



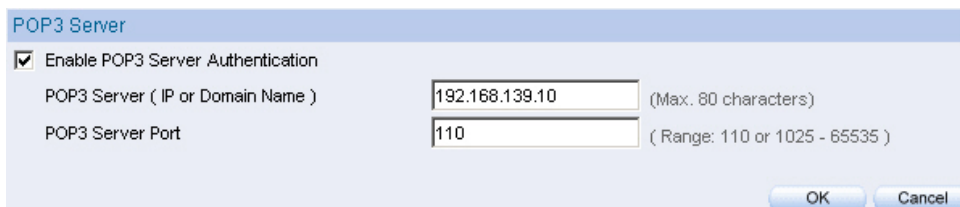
The image shows a web-based authentication window titled "User Login". It features a light blue header bar with the title. Below the header is a section titled "User Authentication" in a darker blue bar. This section contains two input fields: "User Name" and "Password", each with a corresponding text box. At the bottom right of the window is a blue button labeled "OK".

User Login	
User Authentication	
User Name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="OK"/>	

**Figure8-37 Access to Internet by Authentication WebUI**

## Setting the users to connect with external network only before passing the authentication of policy. (Adopt the external POP3 Server Authentication)

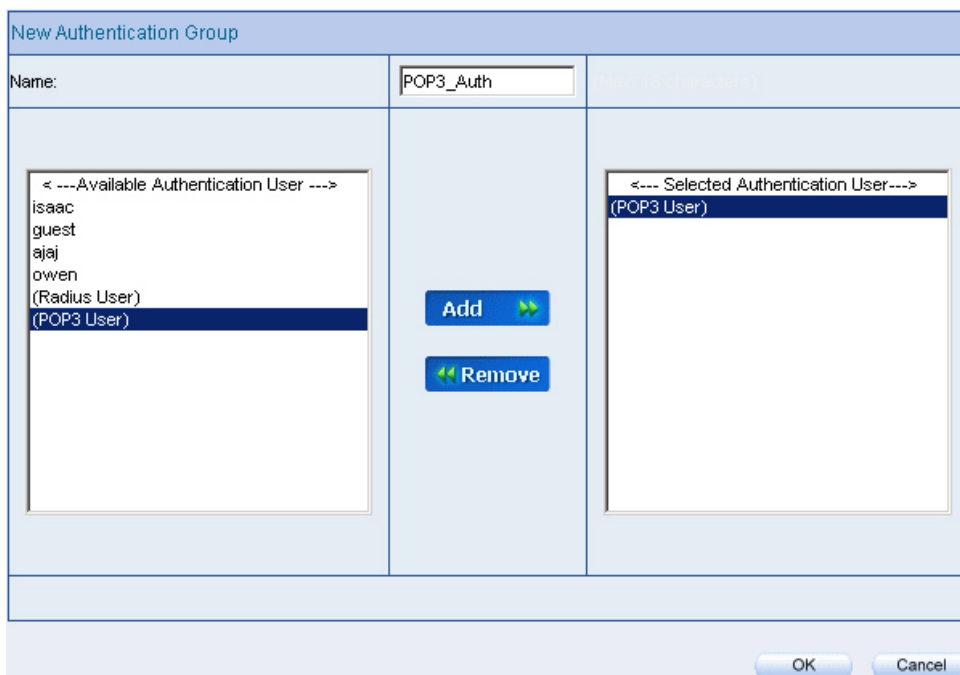
**STEP 1** . Enter the following setting in **POP3** in **Authentication** (Figure8-38)



The screenshot shows the 'POP3 Server' configuration window. It has a title bar 'POP3 Server'. Inside, there is a checkbox 'Enable POP3 Server Authentication' which is checked. Below it are two input fields: 'POP3 Server ( IP or Domain Name )' with the value '192.168.139.10' and a note '(Max. 80 characters)', and 'POP3 Server Port' with the value '110' and a note '( Range: 110 or 1025 - 65535 )'. At the bottom right are 'OK' and 'Cancel' buttons.

Figure8-38 POP3 Server Setting WebUI

**STEP 2** . Add POP3 User in **New Authentication Group**. (Figure8-39)



The screenshot shows the 'New Authentication Group' configuration window. It has a title bar 'New Authentication Group'. The 'Name:' field contains 'POP3\_Auth'. Below the name field are two list boxes. The left list box is titled '<--- Available Authentication User --->' and contains the following items: 'isaac', 'guest', 'ajaj', 'owen', '(Radius User)', and '(POP3 User)'. The '(POP3 User)' item is selected. The right list box is titled '<--- Selected Authentication User --->' and contains the item '(POP3 User)'. Between the two list boxes are two buttons: 'Add' with a right-pointing arrow and 'Remove' with a left-pointing arrow. At the bottom right are 'OK' and 'Cancel' buttons.

Figure8-39 Add New POP3 User WebUI

**STEP 3 . Add a policy of **Authentication User Group** that set in STEP2 in **Outgoing Policy**. (Figure8-40, 8-41)**

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	POP3_Auth
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

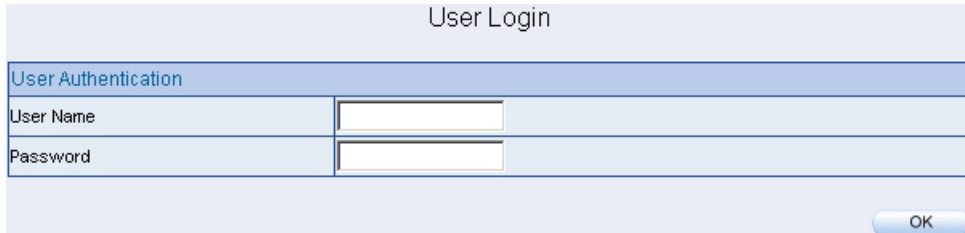
OK Cancel

**Figure8-40 POP3 Server Authentication Policy Setting**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	✓	🔑					Modify	Remove	Pause	To 1
New Entry												

**Figure8-41 Complete POP3 Server Authentication Policy Setting**

**STEP 4** . When the user is going to access to Internet by browser, the Authentication WebUI will display in the browser. After entering correct account and password, click on **OK** and then can access to Internet by ALL7008: (Figure8-42)



The image shows a web interface for user authentication. At the top, there is a light blue header bar with the text "User Login" centered. Below this is a section titled "User Authentication" in a darker blue bar. Underneath, there are two input fields: "User Name" and "Password". Each field has a small text label to its left and a corresponding text input box. The "User Name" field is currently empty, and the "Password" field is also empty. At the bottom right of the form, there is a blue button with the text "OK" in white.

User Login	
User Authentication	
User Name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="OK"/>	

**Figure8-42 the Authentication 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 metacharacter (～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	<b>URL Blocking</b>	Restrict the Internal Users only can access to some specific Website	<b>133</b>
Ex2	<b>Script Blocking</b>	Restrict the Internal Users to access to Script file of Website.	<b>136</b>
Ex3	<b>P2P Blocking</b>	Restrict the Internal Users to access to the file on Internet by P2P.	<b>138</b>
Ex4	<b>IM Blocking</b>	Restrict the Internal Users to send message, files, video and audio by Instant Messaging.	<b>140</b>
Ex5	<b>Download Blocking</b>	Restrict the Internal Users to access to video, audio, and some specific sub-name file from http or ftp protocol directly.	<b>142</b>

## 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)

URL String	Configure	
~yahoo	Modify	Remove
~google	Modify	Remove
*	Modify	Remove
New Entry		

**Figure9-1 Content Filtering Table**

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

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)

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

New Entry

**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)

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)

Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY	✓					Modify	Remove	Pause	To 1
New Entry											

**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)

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)

Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY	✓					Modify	Remove	Pause	To 1
New Entry											

**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:  
(Figure9-11)

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)

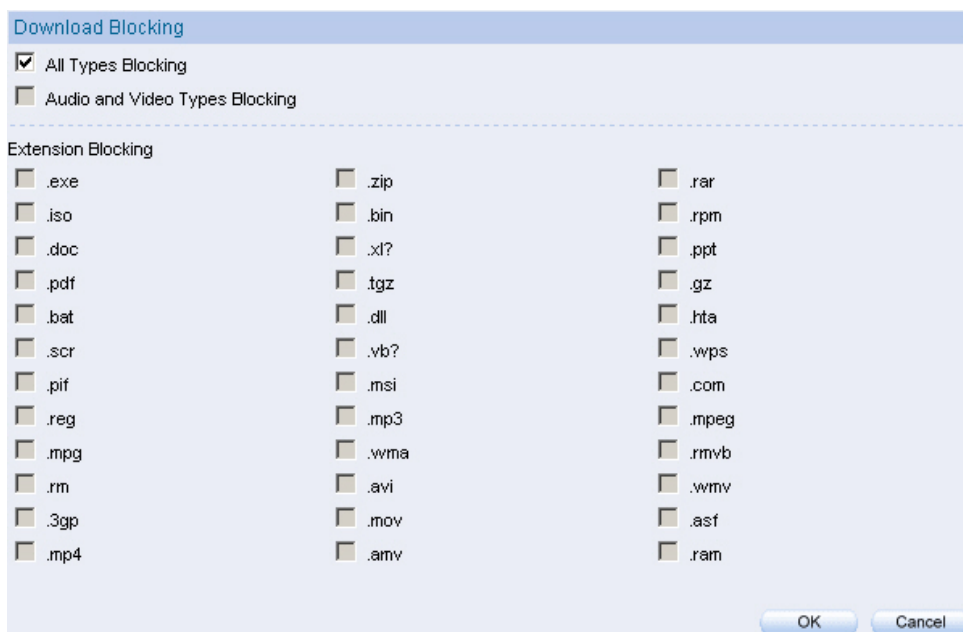
Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY	✓				⊘	Modify	Remove	Pause	To 1
New Entry											

**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)

Comment :  (Max. 32 characters)

**Modify Policy**

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**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)

Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY	✓				⊘	Modify	Remove	Pause	To 1
New Entry											

**Figure9-15 Complete Download Blocking Policy Setting**



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 ALL7008'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 ALL7008's Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the ALL7008's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the ALL7008 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 ALL7008's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the ALL7008. 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	<b>Mapped IP</b>	Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy.	<b>149</b>
Ex2	<b>Virtual Server</b>	Make several servers that provide a single service, to provide service through policy by Virtual Server. (Take Web service for example)	<b>152</b>
Ex3	<b>Virtual Server</b>	The external user use VoIP to connect with VoIP of LAN. (VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)	<b>155</b>
Ex4	<b>Virtual Server</b>	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)	<b>159</b>

## 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)

Add New Address	
Name	Main_Server
IP Address	192.168.1.100
Netmask	255.255.255.255
MAC Address	00:48:54:55:E1:07 <a href="#">Clone MAC</a>
<input type="checkbox"/> Get static IP address from DHCP Server.	
<a href="#">OK</a> <a href="#">Cancel</a>	

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)

Add New Mapped IP	
WAN IP	61.11.11.12 <a href="#">Assist</a>
Map To Virtual IP	192.168.1.100
<a href="#">OK</a> <a href="#">Cancel</a>	

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)

Group name	Service	Configure	
Main_Service	DNS,HTTP,POP3...	Modify	Remove
Mail_Service	DNS,POP3,SMTP	Modify	Remove

New Entry

**Figure10-3 Service Setting**

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

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Mapped IP(61.11.11.12)	Main_Service	✓					Modify	Remove	Pause	To 1 ▼

New Entry

**Figure10-4 Complete the Incoming Policy**

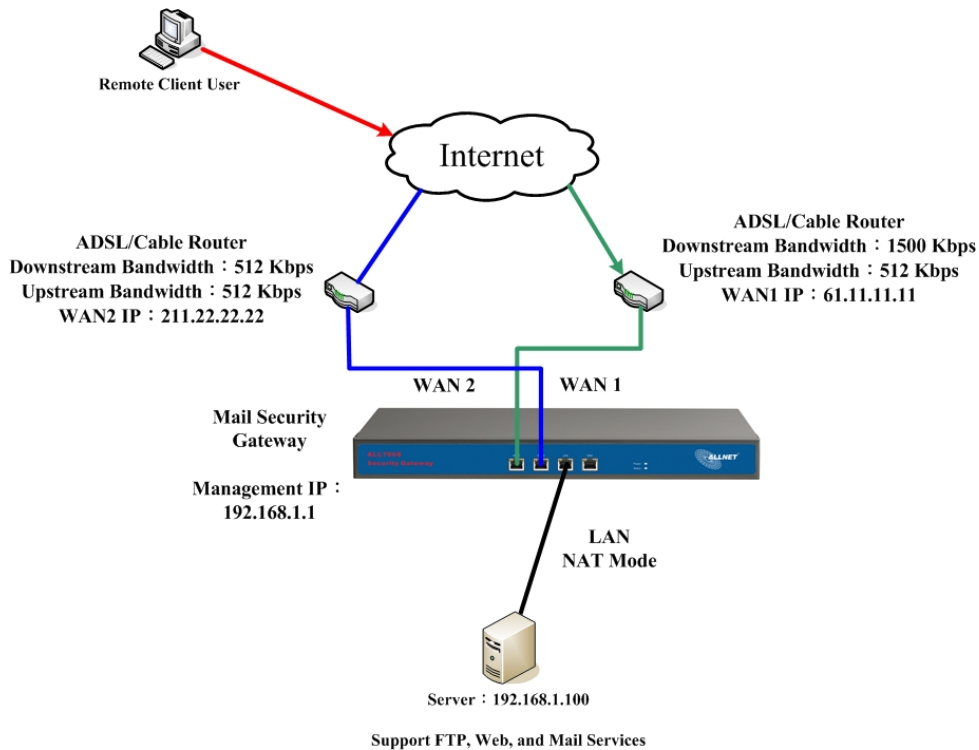
**STEP 6 .** Add a policy that includes STEP2, 4 in **Outgoing Policy**. It makes the server to send e-mail to external mail server by mail service. (Figure10-5)

Source	Destination	Service	Action	Option				Configure			Move
Main_service	Outside_Any	Mail_Service	✓					Modify	Remove	Pause	To 1 ▼

New Entry

**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)

Add New Virtual Server IP	
Virtual Server Real IP	211.22.22.23 WAN2 <a href="#">Assist</a>
OK Cancel	

**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)

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	HTTP (80)
External Service Port	8080
Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104
OK Cancel	

**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)

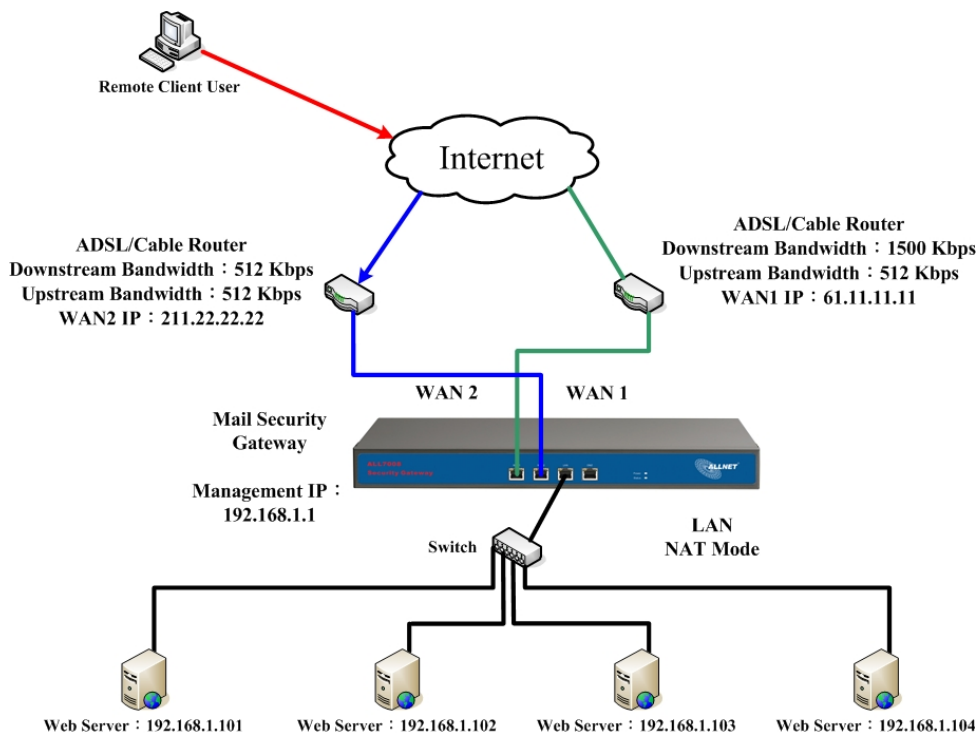
Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(211.22.22.23)	HTTP(8080)	✓					Modify	Remove	Pause	To 1 ▼
New Entry											

**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)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
VoIP	192.168.1.100/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure10-11 Setting LAN Address WebUI**

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

Service name	Protocol	Client Port	Server Port	Configure
VoIP_Service	TCP	0:65535	1720:01720	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**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)

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.13
Service	(Custom Service)VoIP_Service
External Service Port	From-Service(Custom)
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

**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)

Source	Destination	Service	Action	Option					Configure			Move
Outside_Any	Virtual Server 1(61.11.11.13)	VoIP_Service	✓						Modify	Remove	Pause	To 1 ▾
New Entry												

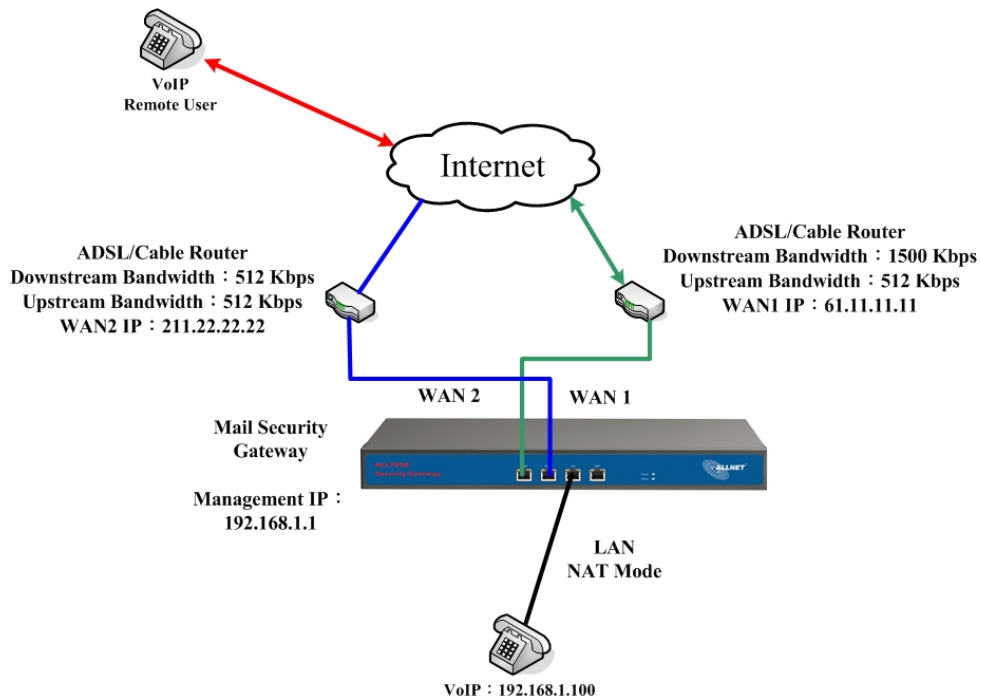
**Figure10-15 Complete the Policy includes Virtual Server Setting**

**STEP 6 .** Enter the following setting of the internal users using VoIP to connect with external network VoIP in **Outgoing Policy**: (Figure10-16)

Source	Destination	Service	Action	Option					Configure			Move
VoIP	Outside_Any	VoIP_Service	✓						Modify	Remove	Pause	To 1 ▾
New Entry												

**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		<input type="button" value="In Use"/>
Server_01	192.168.1.101/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Server_02	192.168.1.102/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Server_03	192.168.1.103/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Server_04	192.168.1.104/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>			

**Figure10-18 Mapped IP Setting of Virtual Server in Address**

Name	Member	Configure
Server_Group	Server_01, Server_02, Server_03...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
<input type="button" value="New Entry"/>		

**Figure10-19 Group Setting of Virtual Server in Address**

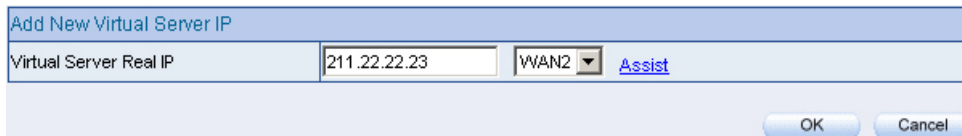
**STEP 3 .** Group the service of server in **Custom** of **Service**. Add a Service Group for server to send e-mail at the same time. (Figure10-20)

Group name	Service	Configure	
Main_Service	DNS,HTTP,POP3...	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
Mail_Service	DNS,POP3,SMTP	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

**Figure10-20 Add New Service Group**

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

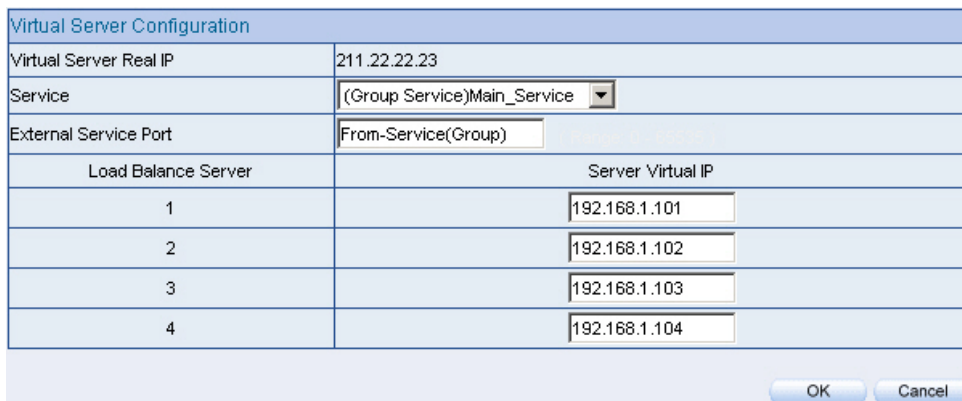
- Click the button next to **Virtual Server Real IP** (“click here to configure”) in **Server1**
- **Virtual Server Real IP:** Enter 211.22.22.23 (click **Assist** for assistance)
- Click **OK** (Figure10-21)



Add New Virtual Server IP	
Virtual Server Real IP	211.22.22.23 WAN2 <a href="#">Assist</a>
OK Cancel	

**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)



Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	(Group Service)Main_Service
External Service Port	From-Service(Group)
Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104
OK Cancel	

**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)

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(211.22.22.23)	Main_Service	✓					Modify	Remove	Pause	To 1 ▼
New Entry											

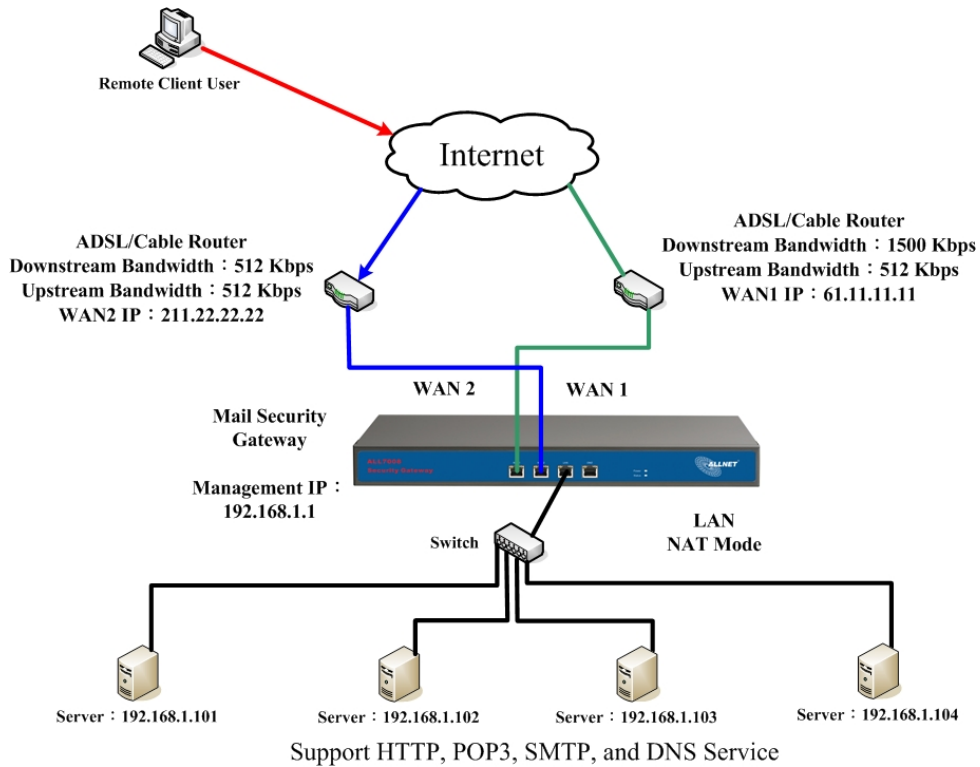
**Figure10-23 Complete Incoming Policy Setting**

**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)

Source	Destination	Service	Action	Option				Configure			Move
Server_Group	Outside_Any	Mail_Service	✓					Modify	Remove	Pause	To 1 ▼
New Entry											

**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**





The ALL7008 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 ALL7008.

**【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 don't need to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet, Destination Gateway, Destination Subnet, Authentication Method, Preshare key, Encapsulation and IPSec lifetime. The Gateway on both ends must use the same Preshare key and IPSec lifetime 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

### Name:

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

### Gateway IP:

- The WAN interface IP address of the remote Gateway.

### Destination Subnet:

- Destination network subnet

### Algorithm:

- To display the Algorithm way

### Status:

- To display the current situation of VPN (Connect or Disconnect)

### Configure:

- Click **Modify** to change the argument of IPSec; click **Delete** to remote the setting; click **Connect** to start the connection with destination gateway; click **Disconnect** to end off the connection with destination gateway. (Figure11-1)

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
New Entry					

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

### 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

### Status:

- Display current connection status between PPTP Server and PPTP Client

### Configure:

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

PPTP Server ( [Disable](#) ) :

Client IP Range : 192.168.168.1-255 [Modify](#)

i	User Name	Client IP	Uptime	Configure
---	-----------	-----------	--------	-----------

[New Entry](#)

Figure11-2 PPTP Server WebUI

## Define the required fields of PPTP Client Function

### User Name :

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

### Server Address :

- Display the PPTP Server IP addresses when connecting to PPTP Server

### Uptime :

- Displays the connection time between PPTP Server and Client

### Status :

- Displays current connection status between PPTP Server and PPTP client

### Configure:

- Click **Modify** to change the argument of PPTP Client; click **Delete** to remote the setting; click **Connect** to start the connection between PPTP Client and PPTP Server; click **Disconnect** to end off the connection between PPTP Client and PPTP Server. (Figure11-3)

PPTP Client :					
i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
New Entry					

Figure11-3 PPTP Client WebUI

We set up six VPN examples in this chapter:

No.	Suitable Situation	Example	Page
Ex1	<b>IPSec Autokey</b>	Setting IPSec VPN connection between two ALL7008	<b>172</b>
Ex2	<b>IPSec Autokey</b>	Setting VPN connection between ALL7008 IPSec VPN and Windows 2000 IPSec VPN	<b>180</b>
Ex3	<b>IPSec Autokey</b>	Setting IPSec VPN connection between two ALL7008 (Connection adopts Aggressive Mode Algorithm) (Data adopts IPSec Algorithm, Encryption: 3DES, Authentication: MD5)	<b>236</b>
Ex4	<b>IPSec Autokey</b>	Setting IPSec VPN connection between two ALL7008 (Connection adopts: ISAKMP Algorithm, Encryption: 3DES, Authentication: MD5) (Data adopt IPSec Algorithm, Encryption: 3DES, Authentication: MD5) (Adopt GRE packet)	<b>245</b>
Ex5	<b>PPTP</b>	Setting PPTP VPN connection between two ALL7008	<b>255</b>
Ex6	<b>PPTP</b>	Setting VPN connection between ALL7008 PPTP VPN and Windows 2000 PPTP VPN	<b>260</b>



# Setting IPSec VPN connection between two ALL7008

## 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 ALL7008 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 ALL7008 192.168.10.1. Follow the steps below:**

**STEP 1 .** Enter the default IP of Gateway of Company A's ALL7008, 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure11-4)

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
New Entry					

Figure11-4 IPSec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_A**, and select **LAN** in From Source. Also fill in Subnet: 192.168.10.0 and Mask: 255.255.255.0 (Figure11-5)

VPN Auto Keyed Tunnel	
Name	VPN_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.10.0 / 255.255.255.0

Figure11-5 IPSec VPN Autokey Tunnel Setting

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the IP Address, **Subnet** 192.168.20.0, and **Mask** 255.255.255.0 of Company B. (Figure11-6)

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

Figure11-6 IPSec To Destination Setting

**STEP 4 .** Select **Preshare** in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-7)

Authentication Method	Preshare
Preshared Key	123456789

Figure11-7 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. (Figure11-8)

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

Figure11-8 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 (Figure11-9)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Figure11-9 IPSec Algorithm Setting

**STEP 7 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, also can enter the **Keep Alive IP** of Company B: 192.168.20.100 to prevent disconnection. (Figure11-10)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.20.100

Figure11-10 IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Select **Schedule** and if it is permissive to transfer data with each other by **Show remote Network Neighborhood**. (Figure11-11)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

Figure11-11 IPSec Schedule and QoS Setting

**STEP 9 .** Click **OK** to complete the setting of Company A (Figure11-12)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure		
VPN_A	211.22.22.22	192.168.20.0	None	Disconnect	Connecting	Modify	Remove

New Entry

Figure11-12 Complete Company A IPSec VPN Setting

The Default Gateway of Company B is the LAN IP of the ALL7008 192.168.20.1. Follow the steps below:

**STEP 1 .** Enter the default IP of Gateway of Company B's ALL7008, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry** (Figure11-13)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
<div>New Entry</div>					

Figure11-13 IPSec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_B**, and select **LAN** in From Source. Also fill in Subnet: 192.168.20.0 and Mask: 255.255.255.0 (Figure11-14)

VPN Auto Keyed Tunnel	
Name	VPN_B
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.20.0 / 255.255.255.0

Figure11-14 IPSec VPN Auto keyed Tunnel Setting

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the IP Address, **Subnet** 192.168.10.0, and **Mask** 255.255.255.0 of Company A. (Figure11-15)

<b>To Destination</b>	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	61.11.11.11
Subnet / Mask	192.168.10.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

Figure11-15 IPSec To Destination Setting

**STEP 4 .** Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-16)

Authentication Method	Preshare
Preshared Key	123456789

Figure11-16 IPSec Authentication Method Setting

**STEP 5 .** Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for Group. (Both sides have to choose the same group) (Figure11-17)

<b>Encapsulation</b>	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP1

Figure11-17 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. (Figure11-18)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Figure11-18 IPSec Algorithm Setting

**STEP 7 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, also can enter the **Keep Alive IP** of Company A: 192.168.10.100 to prevent disconnection. (Figure11-19)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.10.100

Figure11-19 IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Select **Schedule** and if it is permissive to transfer data by **Show remote Network Neighborhood**. (Figure11-20)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

Figure11-20 IPSec Schedule and QoS Setting

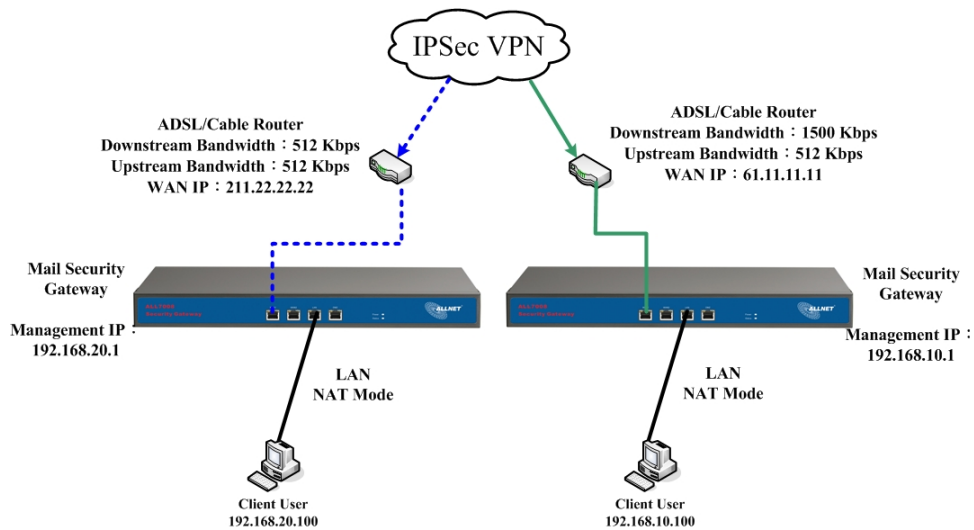
**STEP 9 .** Click **OK** to complete the setting of Company B (Figure11-21)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure		
VPN_B	61.11.11.11	192.168.10.0	None	Disconnect	Connecting	Modify	Remove

New Entry

**Figure11-21 Complete Company B IPSec VPN Setting**

**STEP 10 .** Complete IPSec VPN Connection (Figure11-22)



**Figure11-22 IPSec VPN Setting**



# Setting VPN connection between ALL7008 IPsec VPN and Windows 2000 IPsec VPN

## Preparation

Company A    ALL7008  
              **WAN IP: 61.11.11.11**  
              **LAN IP: 192.168.10.X**  
Company B    Windows2000 PC  
              **WAN IP: 211.22.22.22**

This example takes one ALL7008 and Windows 2000 IPsec VPN as work platform. Suppose Company B, 211.22.22.22 create a VPN connection with Company A, 192.168.10.100 for downloading the sharing file.

**The Default Gateway of Company A is the LAN IP of ALL7008 192.168.10.1. Follow the steps below:**

**STEP 1 .** Enter the default IP of ALL7008 in Company A 192.168.10.1 and select **IPsec Autokey** in **VPN**. Click **New Entry**. (Figure11-23)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
New Entry					

Figure11-23 IPsec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_A**, and select **LAN** in From Source. Also fill in Subnet: 192.168.10.0 and Mask: 255.255.255.0 (Figure11-24)

VPN Auto Keyed Tunnel	
Name	VPN_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.10.0 / 255.255.255.0

Figure11-24 IPSec VPN Auto keyed Tunnel Setting

**STEP 3 .** Select **Remote Client-Fixed IP or Dynamic IP** In **To Destination** list. (Figure11-25)

To Destination	
<input type="radio"/> Remote Gateway -- Fixed IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input checked="" type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

Figure11-25 IPSec To Destination Setting

**STEP 4 .** Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-26)

Authentication Method	Preshare
Preshared Key	123456789

Figure11-26 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 GROUP2 for Group. (Figure11-27)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 2

Figure11-27 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. (Figure11-28)

IPsec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Figure11-28 IPsec Algorithm Setting

**STEP 7 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, also can enter the **Keep Alive IP** of Company B: 211.22.22.22 to prevent disconnection. (Figure11-29)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	211.22.22.22

Figure11-29 IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Select **Schedule**, **QoS**, and **Authentication-User** and if it is permissive to transfer data with each other by **Show remote Network Neighborhood**. (Figure11-30)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

Figure11-30 IPSec Schedule and QoS Setting

**STEP 9 .** Click **OK** to complete the setting of Company A (Figure11-31)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN_A	No IP !	VPN Client	None	Disconnect	Modify Remove

New Entry

Figure11-31 Complete Company A IPSec VPN Setting

The PC of Company B use Real IP Address: 211.22.22.22. Follow the steps below:

**STEP 1** . Enter Windows2000 and select **Run** in **Start**. (Figure11-32)

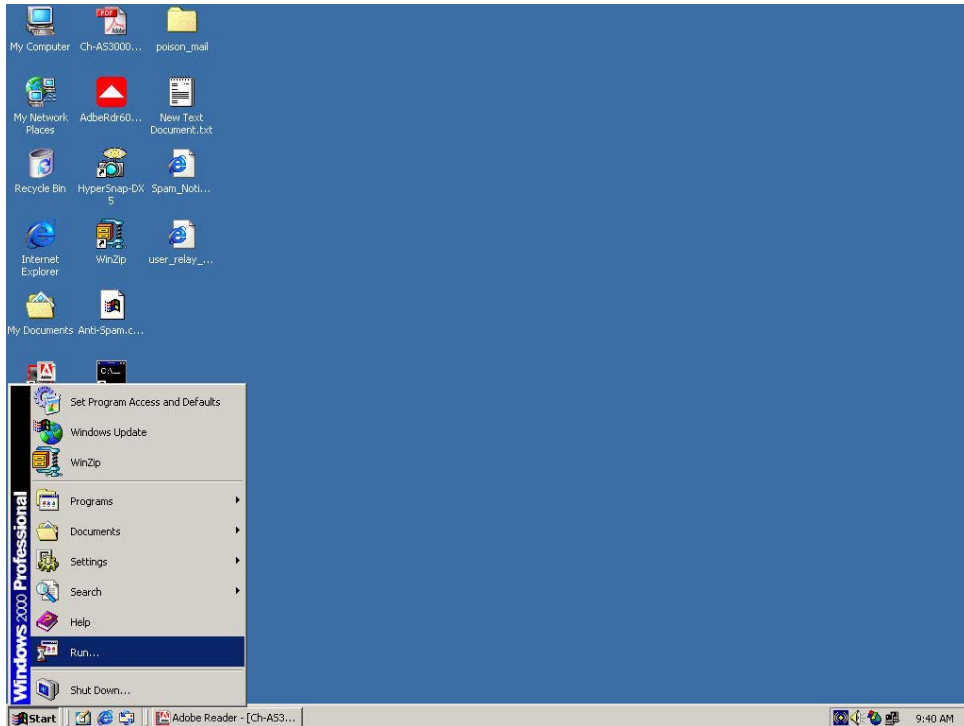


Figure11-32 Start Windows 2000 IPsec VPN Setting

**STEP 2 .** In the **Run** WebUI, enter the command: mmc in **Open** field.  
(Figure11-33)



Figure11-33 Enable Windows 2000 IPsec VPN Setting

**STEP 3 .** Enter File in **Console1** WebUI, select **File** option and then select **Add/Remote Snap-ins** Option. (Figure11-34)

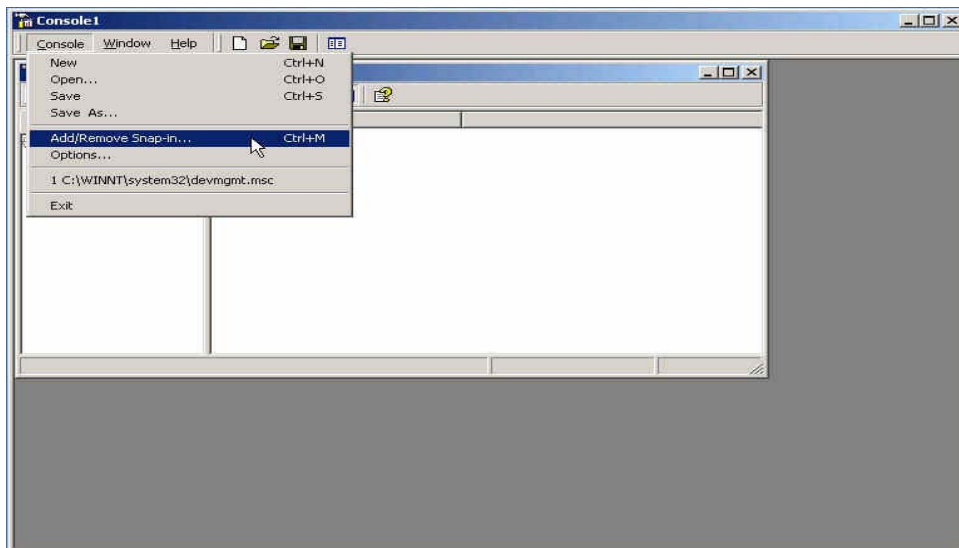
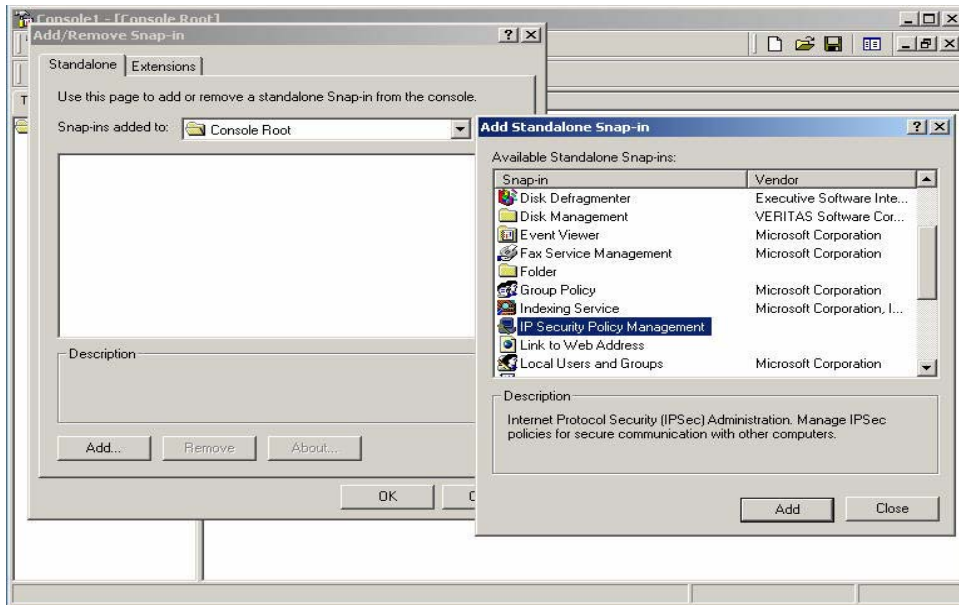


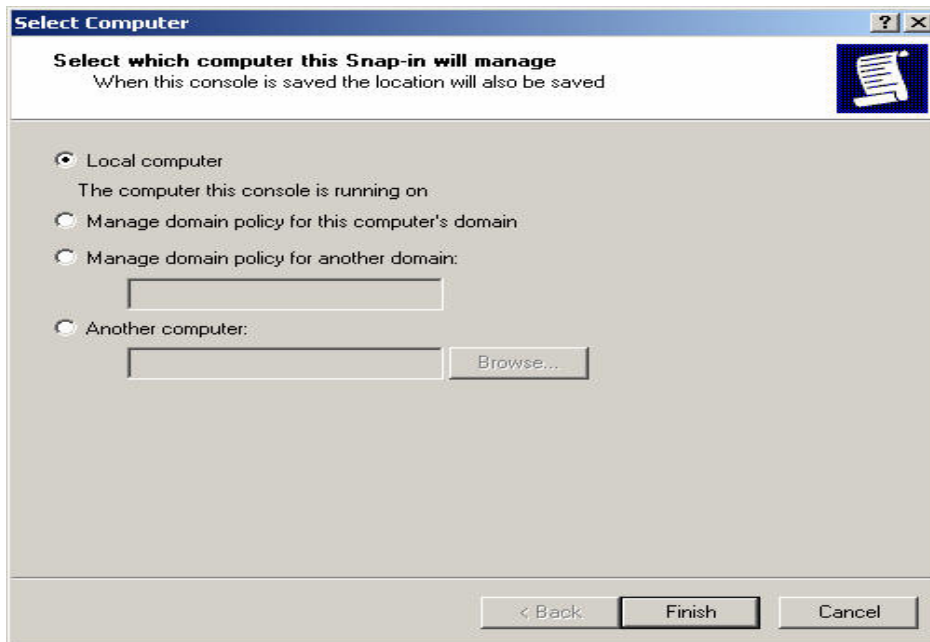
Figure11-34 Add/Remote Snap-ins

**STEP 4 . Enter Add in Add/Remote Snap-ins. And add IP Security Policy Management in Add Standalone Snap-in WebUI. (Figure11-35)**



**Figure11-35 Add IP Security Policy Management**

**STEP 5 . Select Local computer** to complete adding (Figure11-36)



**Figure11-36 Select Computer or Domain**



## STEP 6 . Complete adding IP Security Policy Management (Figure11-37)

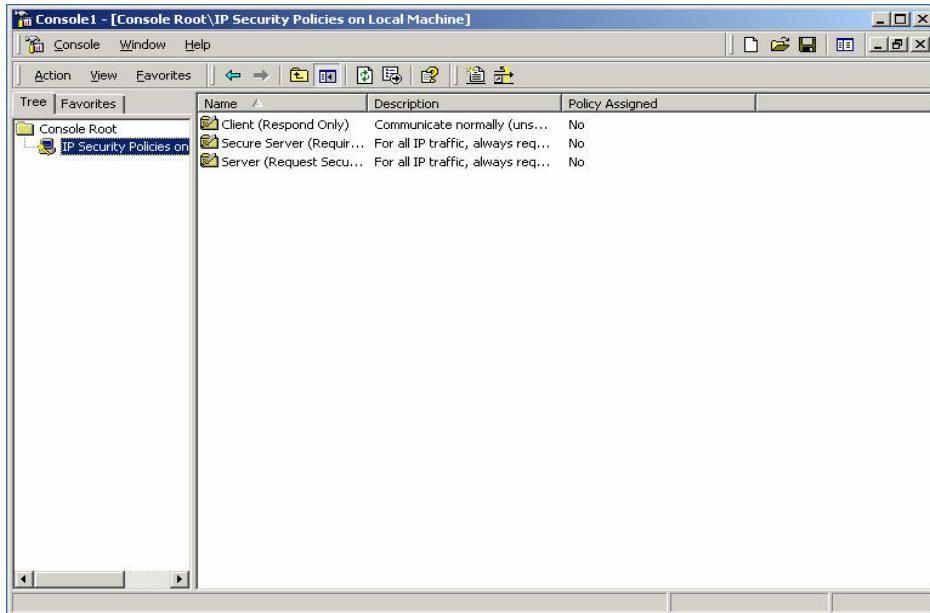
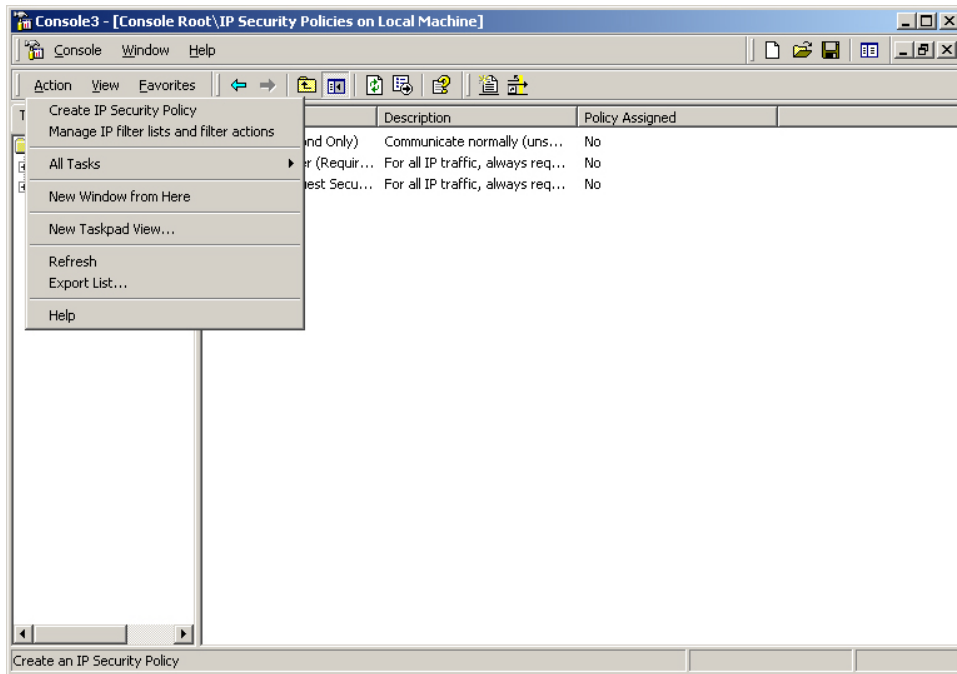


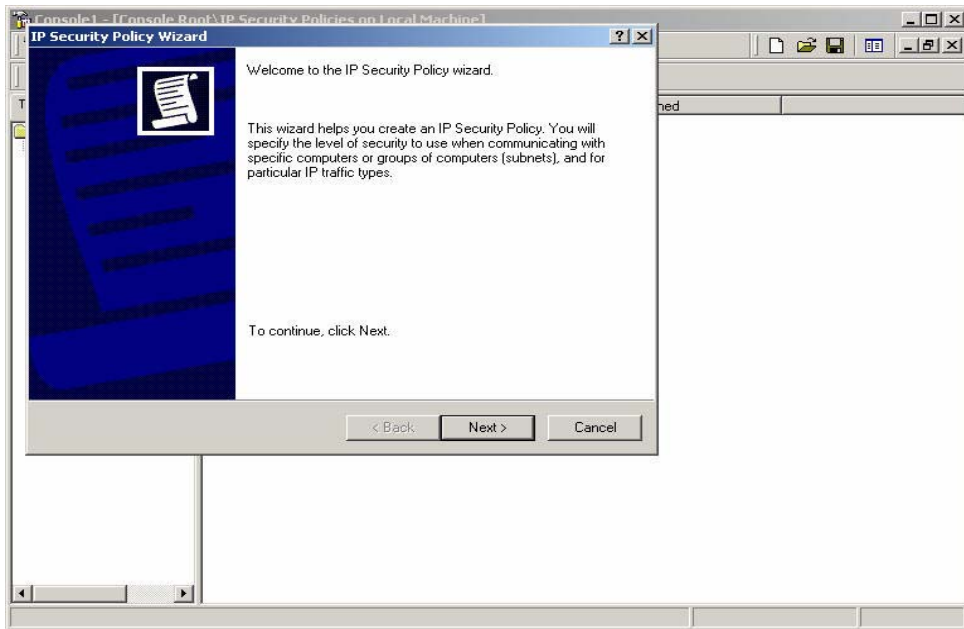
Figure11-37 Complete Adding IP Security Policy Management

**STEP 7 .** Press the right button of the mouse in **IP Security Policies on Local Computer** selection and select **Create IP Security Policy**.  
(Figure11-38)



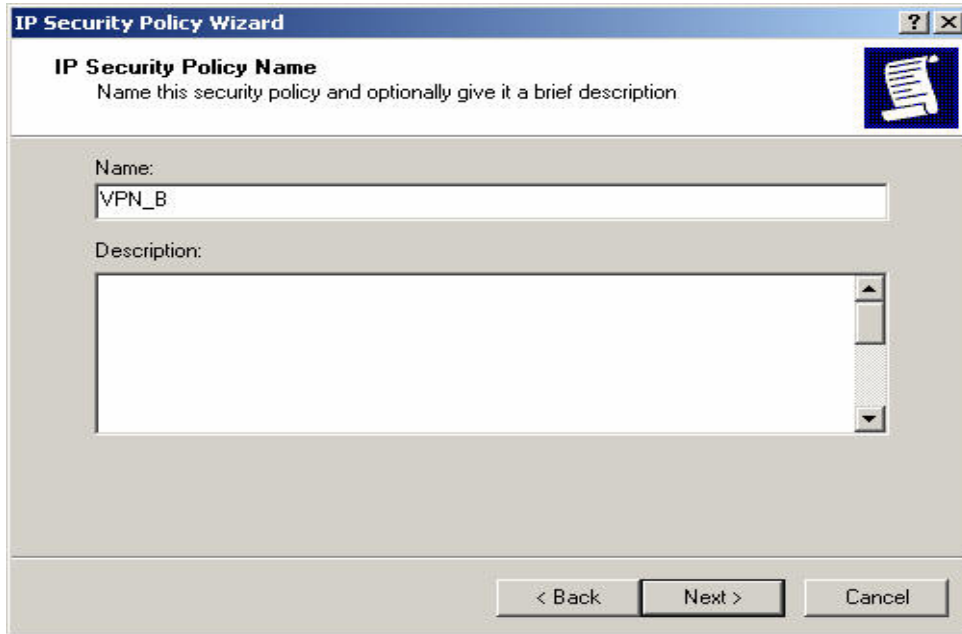
**Figure11-38 Create IP Security Policy**

**STEP 8 . Click on **Next** (Figure11-39)**



**Figure11-39 Enable IP Security Policy**

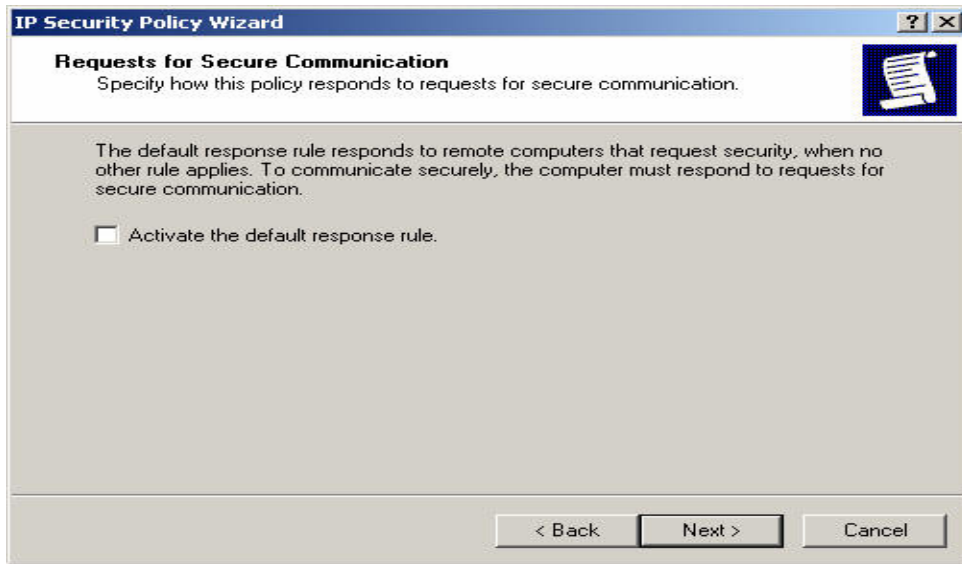
**STEP 9 .** Enter **IP Security Policy Name** and **Description** and click on **Next** in IP Security Policy Wizard WebUI. (Figure11-40)



The screenshot shows a web-based wizard window titled "IP Security Policy Wizard". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). Below the header, the main content area is divided into two sections. The first section is titled "IP Security Policy Name" and contains the instruction "Name this security policy and optionally give it a brief description". To the right of this text is a small icon of a document with a pencil. The second section contains two input fields: a text box labeled "Name:" with the value "VPN\_B" entered, and a larger text area labeled "Description:" which is currently empty. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted, indicating it is the next step in the wizard.

**Figure11-40 Setting IP Security Policy Name and Description**

**STEP 10 .** Please cancel **Active the default response rule** selection and click on **Next**. (Figure11-41)



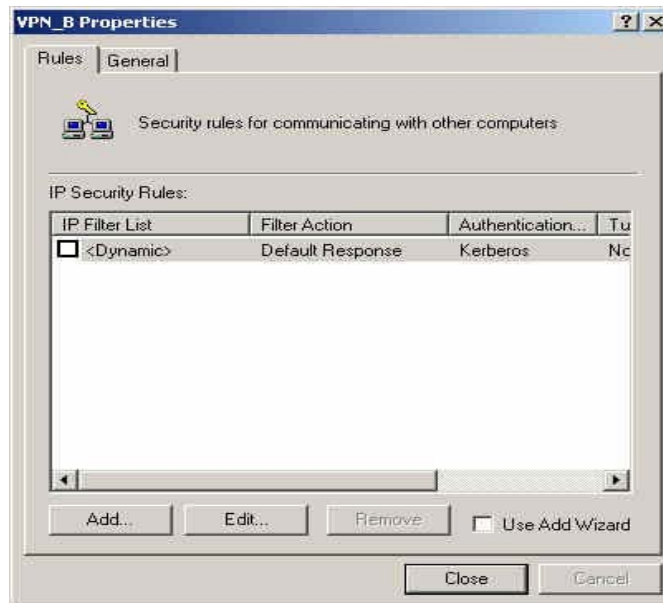
**Figure11-41 Cancel Active the Default Response Rule Selection**

**STEP 11 .** Complete setting IP Security Policy and click on **Finish**. Select the **Edit properties** (Figure11-42)



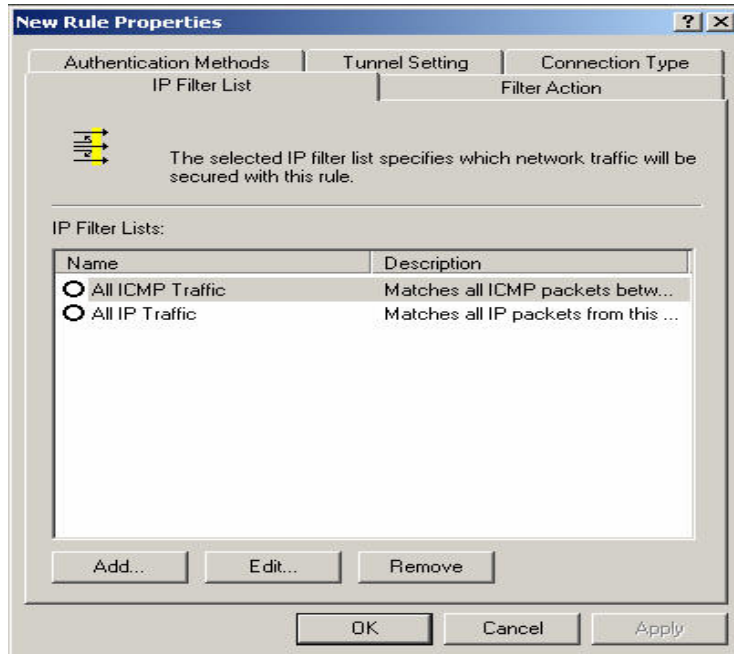
**Figure11-42 Complete the IP Security Policy Wizard**

**STEP 12 .** Enter **VPN\_B Properties** WebUI and do not select Use Add Wizard.  
Select **Add** and enter **Edit Properties** (Figure11-43)



**Figure11-43 VPN\_B Properties WebUI**

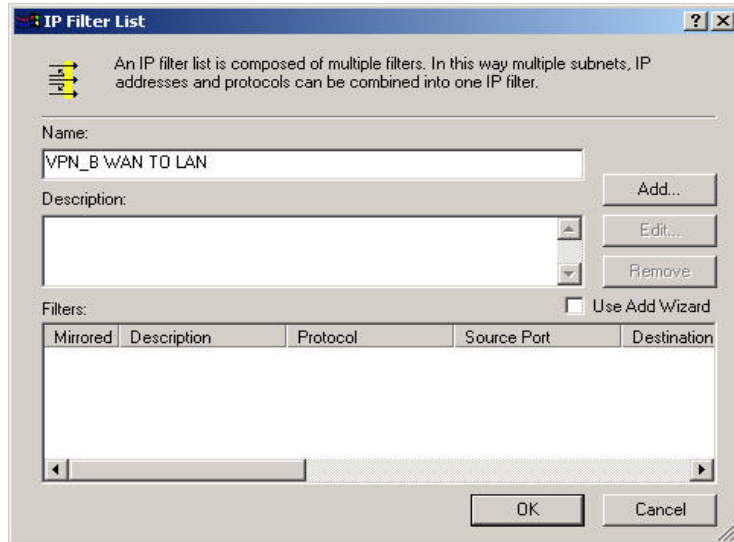
**STEP 13 .** Click on **Add** in **New Rule Properties** WebUI (Figure11-44)



**Figure11-44 Add New IP Filter List**



**STEP 14** . Please do not select Use Add Wizard in **IP Filter List**. Change the name as **VPN\_B WAN TO LAN** and click **Add** (Figure11-45)



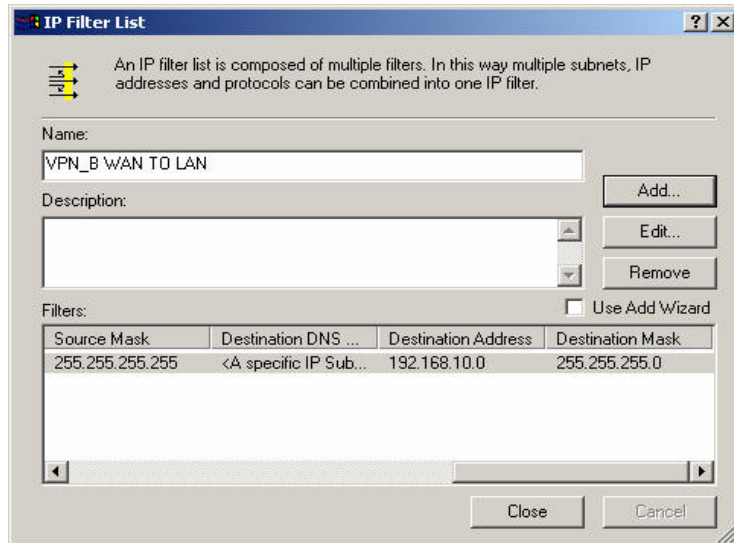
**Figure11-45 IP Filter List WebUI**

**STEP 15 .** After entering **Filter Properties**, please select **A specific IP Address** in Source address and enter the WAN IP of Company B: 211.22.22.22, Subnet Mask: 255.255.255.255. And select **A specific IP Subnet** in Destination address and enter the LAN IP of Company A: 192.168.10.0, Subnet Mask: 255.255.255.0. Please do not select Mirrored: Also match packets with the exact opposite source and destination addresses. (Figure11-46)

The screenshot shows a 'Filter Properties' dialog box with three tabs: 'Addressing', 'Protocol', and 'Description'. The 'Addressing' tab is active. It contains two main sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu is set to 'A specific IP Address', with the IP Address field containing '211 . 22 . 22 . 22' and the Subnet mask field containing '255 . 255 . 255 . 255'. In the 'Destination address' section, a dropdown menu is set to 'A specific IP Subnet', with the IP Address field containing '192 . 168 . 10 . 0' and the Subnet mask field containing '255 . 255 . 255 . 0'. At the bottom, there is a checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' which is currently unchecked. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

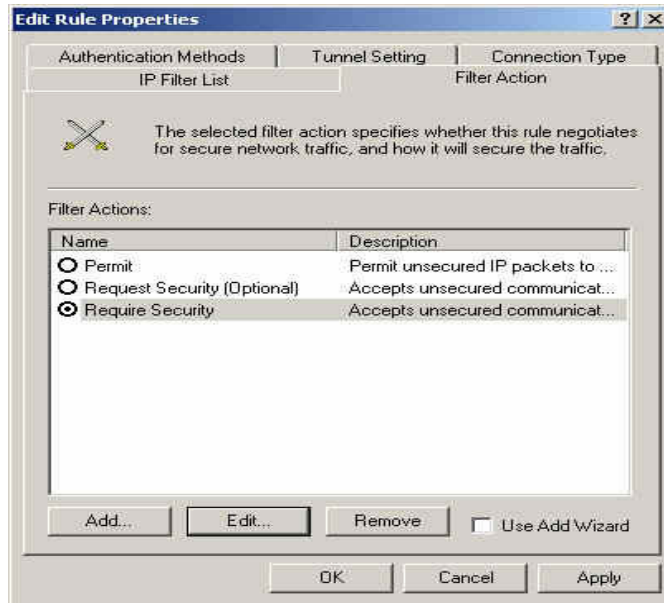
Figure11-46 Filter Properties WebUI

**STEP 16 .** Complete the setting and close **IP Filter List** Window. (Figure11-47)



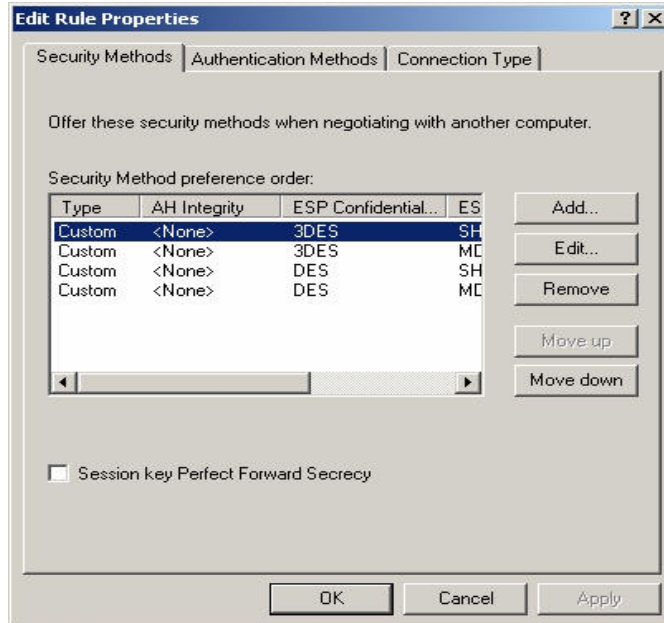
**Figure11-47 Complete IP Filter List**

**STEP 17 .** Select **Require Security** in **Filter Action** WebUI and click **Edit**.  
(Figure11-48)



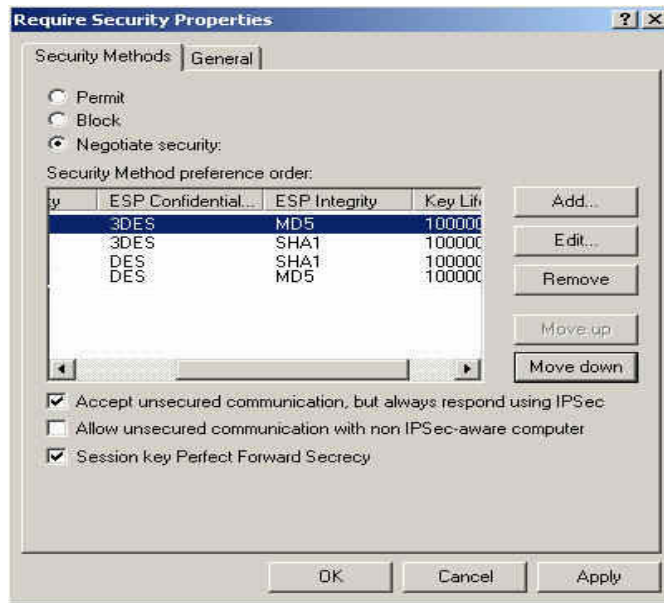
**Figure11-48 Filter Action Setting**

**STEP 18 .** Enter Require Security Properties WebUI and select **Negotiate security.** (Figure11-49)



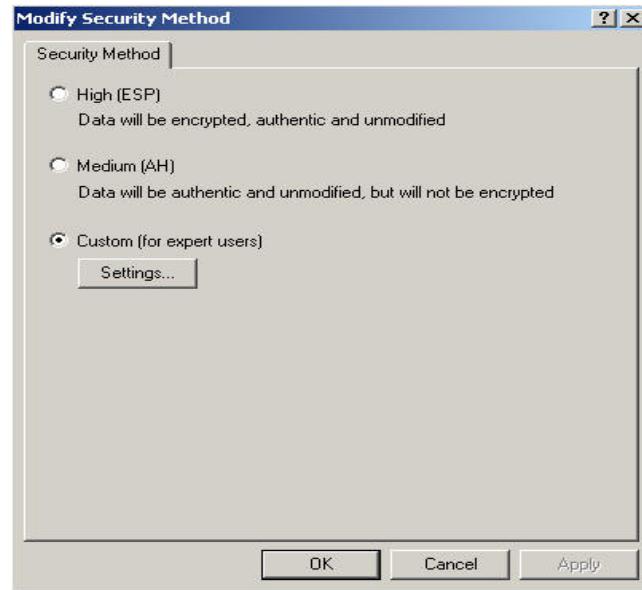
**Figure11-49 Select Session key perfect forward secrecy**

**STEP 19 .** Please select **Custom/None/3DES/MD5** and click **Edit** (Figure11-50)



**Figure11-50 Edit Security Method**

**STEP 20 .** Click **Custom** (provide for professional users) and select **Settings**.  
(Figure11-51)



**Figure11-51 Custom Security Method**

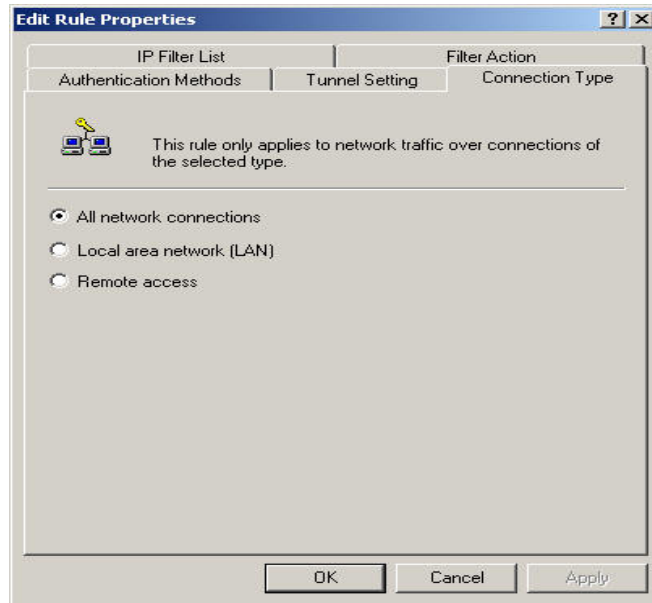
**STEP 21** . Please select **ESP** and choose MD5 and 3DES. Also select **Generate a new key every**. Enter 28800 seconds and click **OK** triple times to go back to Rule Properties. (Figure11-52)



**Figure11-52 Custom Security Method Settings**

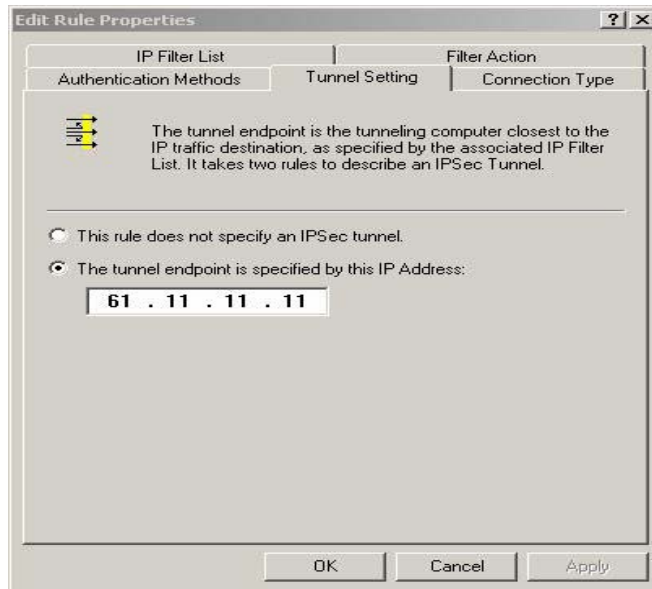


**STEP 22 . Enter **Connection Type** and select **All network connections****  
(Figure11-53)



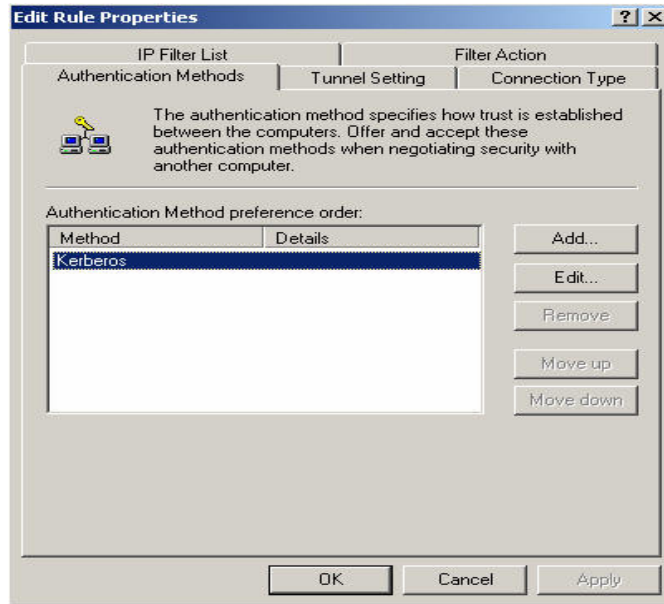
**Figure11-53 Connection Type Setting**

**STEP 23 .** Enter Tunnel Setting WebUI. Select **The tunnel endpoint is specified by this IP address** and enter the WAN IP of Company A. (Figure11-54)



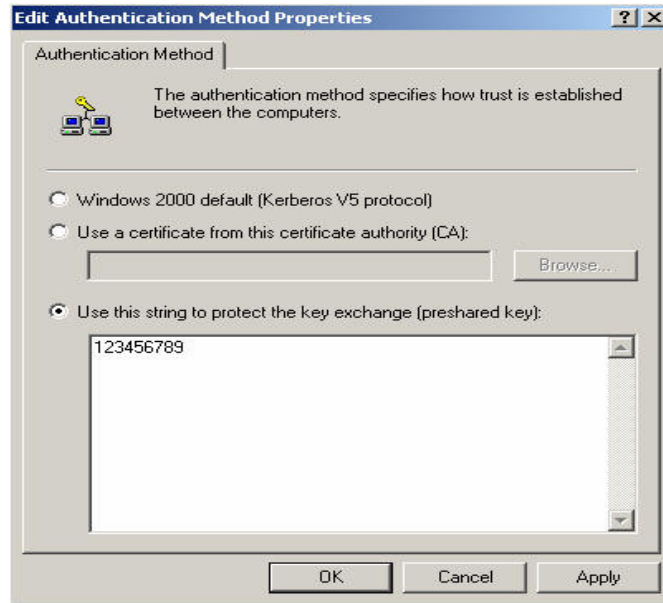
**Figure11-54 Tunnel Setting**

**STEP 24 .** Enter **Authentication Methods** WebUI and select **Edit**.  
(Figure11-55)



**Figure11-55 Authentication Method Setting WebUI**

**STEP 25 .** Select the item **Use this string** to protect preshared key and enter the preshared key: 123456789 (Figure11-56)



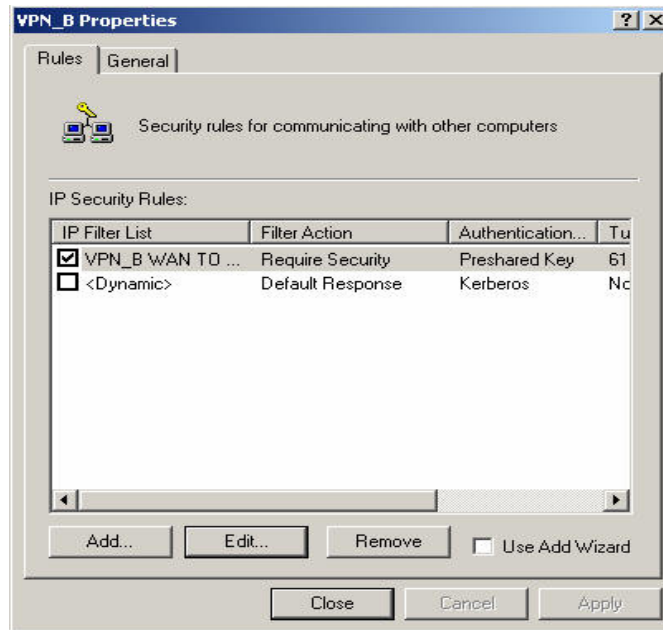
**Figure11-56 Setting VPN Connection Preshared Key**

**STEP 26 .** Complete Setting and close the WebUI (Figure11-57)



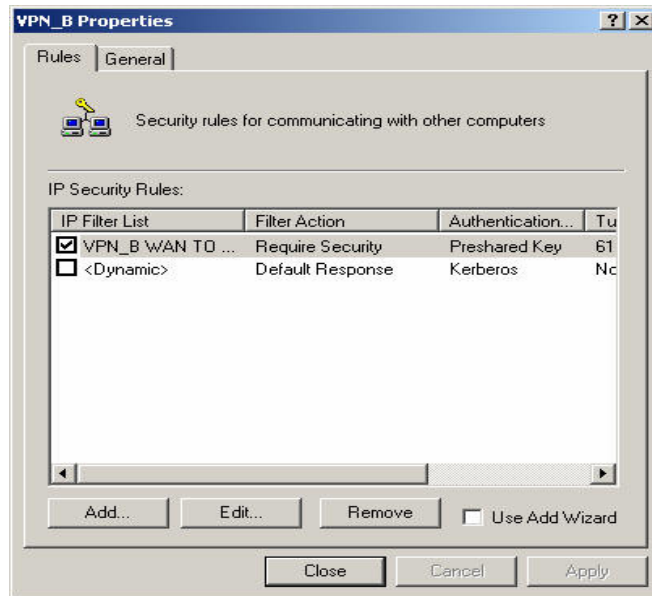
**Figure11-57 Complete Authentication Methods Setting**

**STEP 27 . Complete the VPN\_B WAN TO LAN Settings (Figure11-58)**



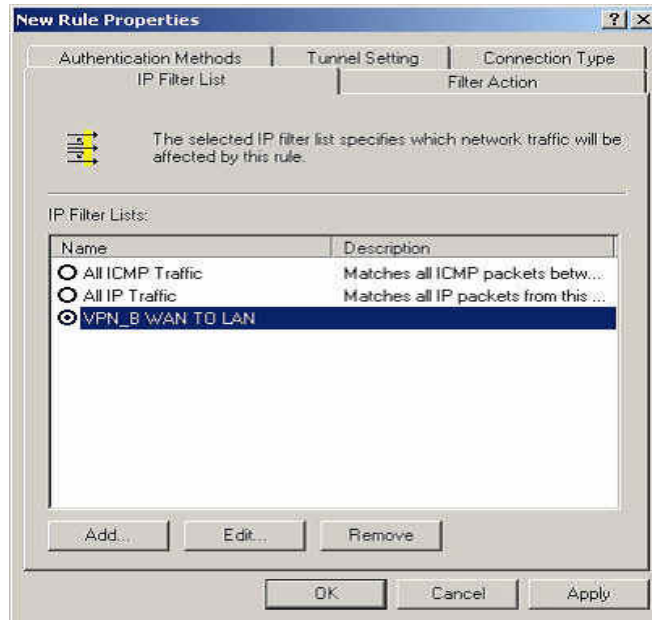
**Figure11-58 Complete VPN\_B WAN TO LAN Setting**

**STEP 28 .** Please enter **VPN\_B Properties** WebUI again and do not select Use Add Wizard. Select **Add** to enter **Edit Properties** (Figure11-59)



**Figure11-59 VPN\_B Properties WebUI**

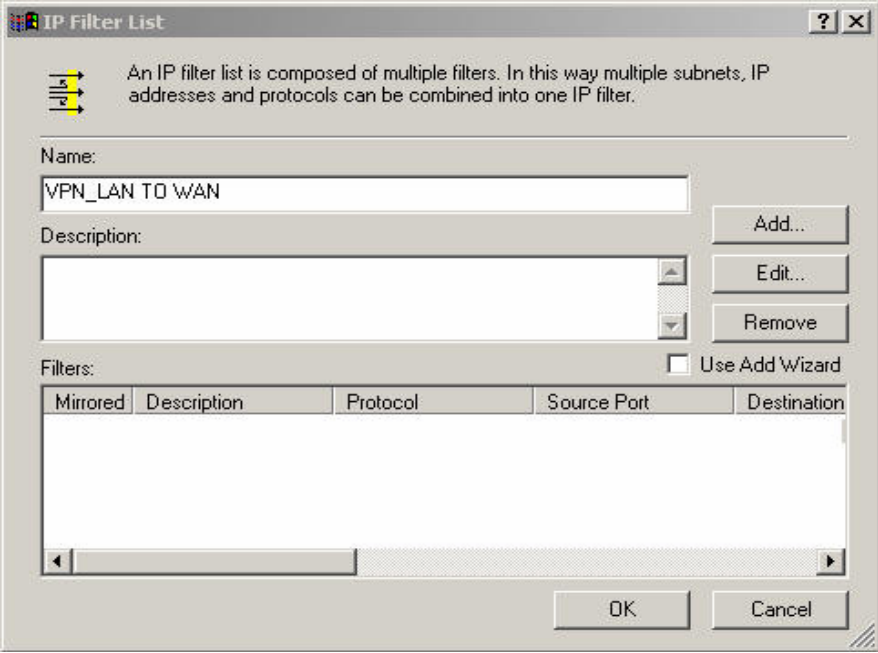
**STEP 29 .** Please select **Add** in **New Rule Properties** WebUI. (Figure11-60)



**Figure11-60 Add New Rule Properties WebUI**



**STEP 30** . Please do not select Use Add Wizard in IP Filter List. Please change the name as VPN\_B LAN TO WAN and select **Add**. (Figure11-61)



The screenshot shows the 'IP Filter List' web interface. At the top, there is a title bar with a question mark and a close button. Below the title bar, there is a help icon and a text box explaining that an IP filter list is composed of multiple filters. The main form has a 'Name' field containing 'VPN\_LAN TO WAN', a 'Description' field, and three buttons: 'Add...', 'Edit...', and 'Remove'. Below these fields, there is a 'Filters' section with a checkbox labeled 'Use Add Wizard' which is unchecked. A table with five columns (Mirrored, Description, Protocol, Source Port, Destination) is shown below the checkbox. The table is currently empty. At the bottom of the form, there are 'OK' and 'Cancel' buttons.

IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: VPN\_LAN TO WAN

Description:

Add... Edit... Remove

Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
----------	-------------	----------	-------------	-------------

OK Cancel

**Figure11-61 IP Filter List WebUI**

**STEP 31** . Enter **Filter Properties** and select **A specific IP Subnet** in Source address and enter the LAN IP of Company A: 192.168.10.0, Subnet mask: 255.255.255.0. Select **A specific IP Address** in Destination address and enter the WAN IP of Company B: 211.22.22.22, Subnet mask: 255.255.255.255. Please do not select Mirrored. Also match packets with the exact opposite source and destination addresses. (Figure11-62)

**Filter Properties**

Addressing | Protocol | Description

Source address:

A specific IP Subnet

IP Address: 192 . 168 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address:

A specific IP Address

IP Address: 211 . 22 . 22 . 22

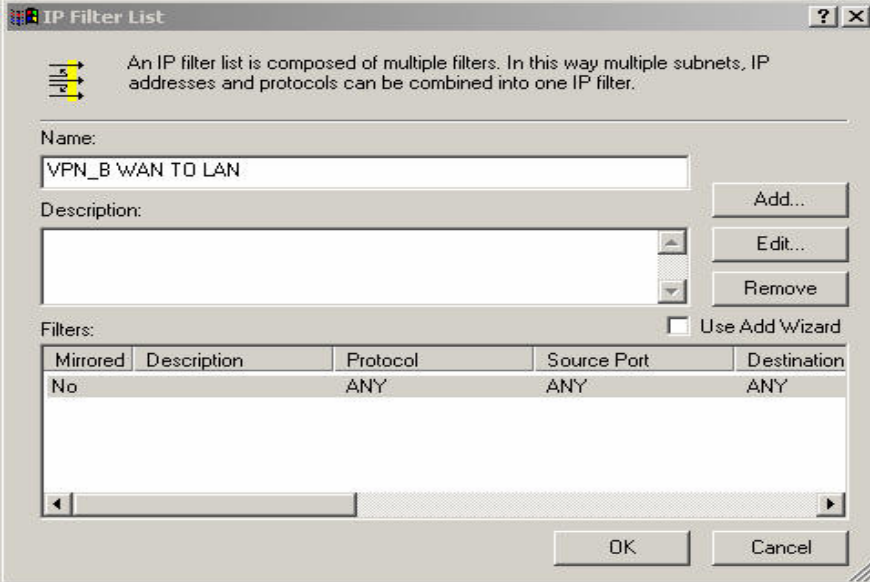
Subnet mask: 255 . 255 . 255 . 255

☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel Apply

**Figure11-62 Filter Properties WebUI**

**STEP 32 . Complete Setting and close IP Filter List WebUI (Figure11-63)**



The screenshot shows the 'IP Filter List' window. At the top, there is a title bar with a question mark and a close button. Below the title bar, there is a small icon of three arrows pointing right and a text box explaining that an IP filter list is composed of multiple filters. The main area contains a 'Name' field with the text 'VPN\_B WAN TO LAN', a 'Description' field, and three buttons: 'Add...', 'Edit...', and 'Remove'. Below these fields, there is a 'Filters' section with a checkbox labeled 'Use Add Wizard'. A table with five columns is shown: 'Mirrored', 'Description', 'Protocol', 'Source Port', and 'Destination'. The first row has the values 'No', 'ANY', 'ANY', and 'ANY'. The table has a scrollbar at the bottom. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:  
VPN\_B WAN TO LAN

Description:

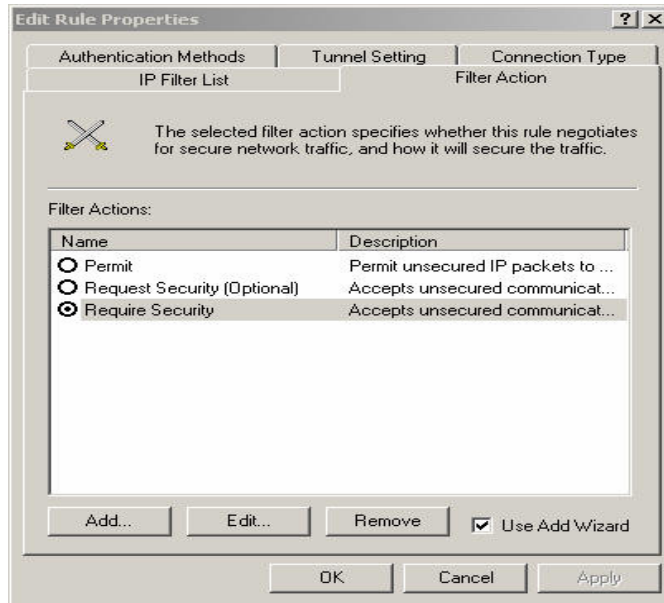
Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

OK Cancel

**Figure11-63 Complete IP Filter List Setting**

**STEP 33 .** Select **Require Security** in **Filter Action** WebUI and click **Edit** (Figure11-64)



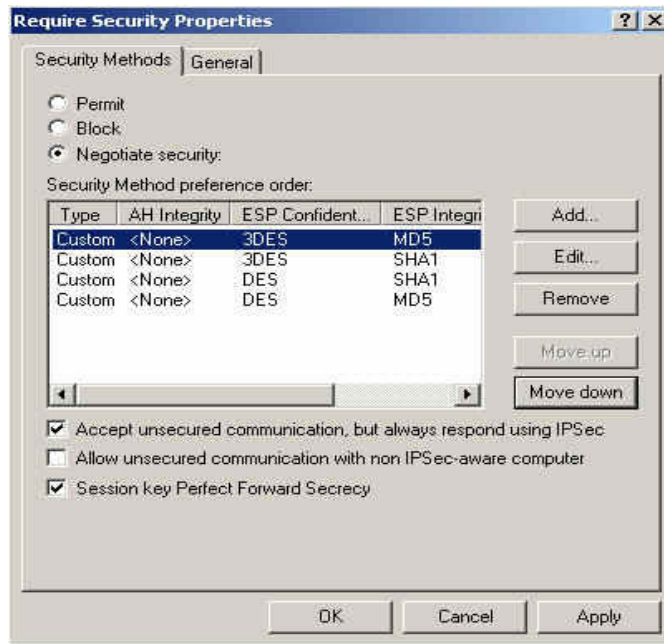
**Figure11-64 Filter Action WebUI**

**STEP 34 . Enter Require Security Properties WebUI and select Session key perfect forward secrecy (PFS) (Figure11-65)**



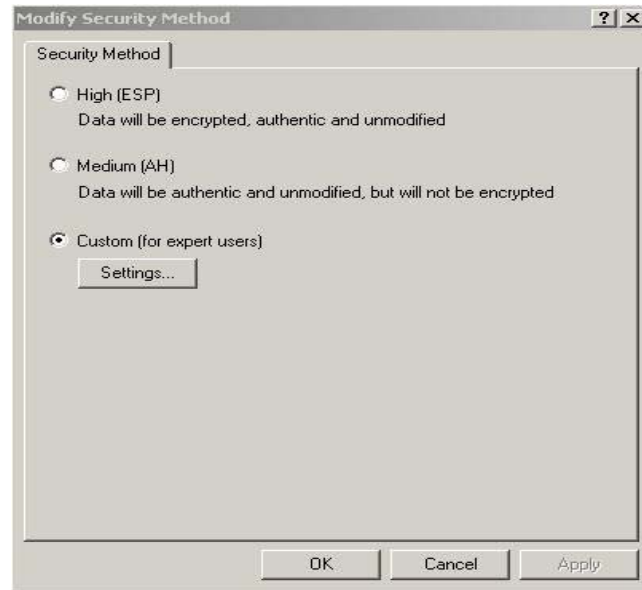
**Figure11-65 Select PFS**

**STEP 35 .** Select **Custom/ None/ 3DES/ MD5** and choose **Edit** (Figure11-66)



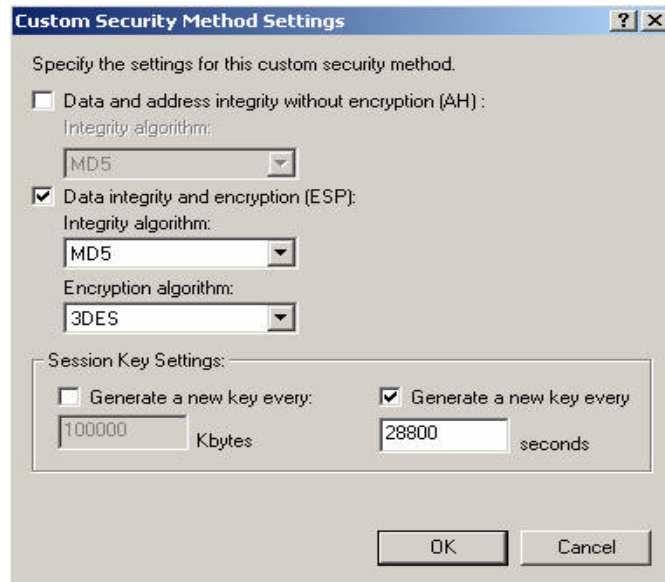
**Figure11-66 Setting Security Methods**

**STEP 36 .** Select **Custom** (provide for professional users) and click **Settings** (Figure11-67)



**Figure11-67 Modify Security Method**

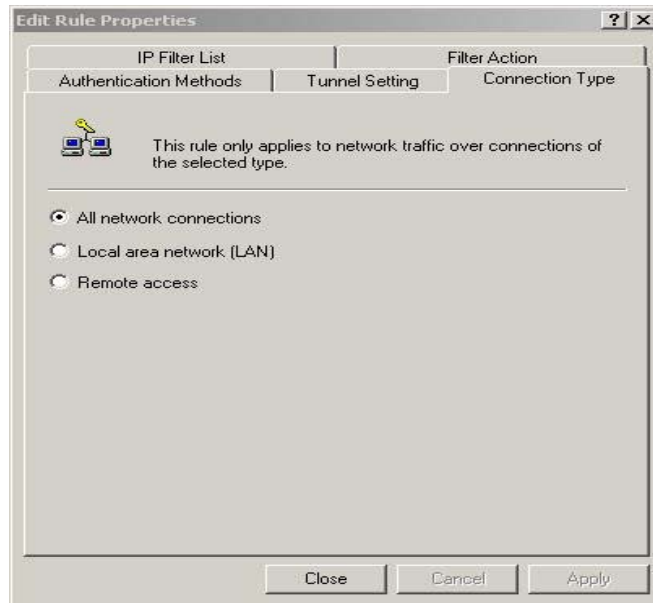
**STEP 37 .** Please select **Data integrity and encryption (ESP)** and choose MD5 and 3DES. Also select **Generate a new key every**. Enter 28800 seconds and click **OK** triple times to go back to **Rule Properties WebUI**. (Figure11-68)



**Figure11-68 Complete Custom Security Method Setting**

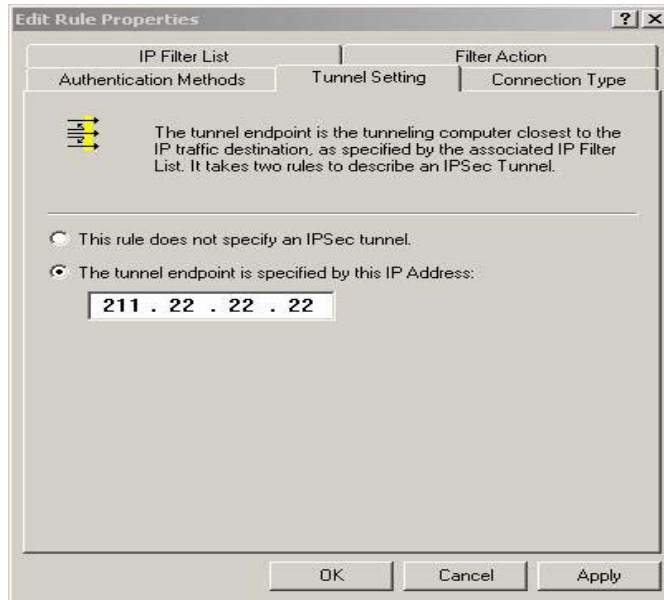


**STEP 38 .** Select **All network connections** in **Connection Type**. (Figure11-69)



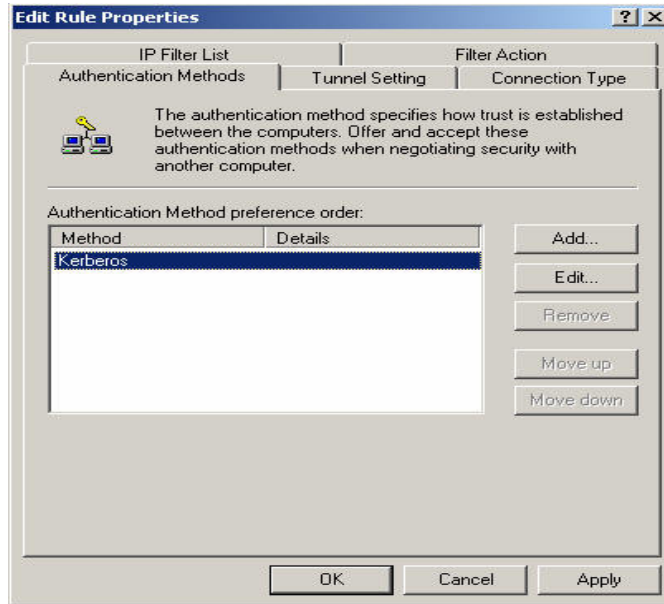
**Figure11-69 Connection Type Setting**

**STEP 39 .** Enter **Tunnel Setting** WebUI. Select **The tunnel endpoint is specified by this IP address** and enter the WAN IP of Company B: 211.22.22.22 (Figure11-70)



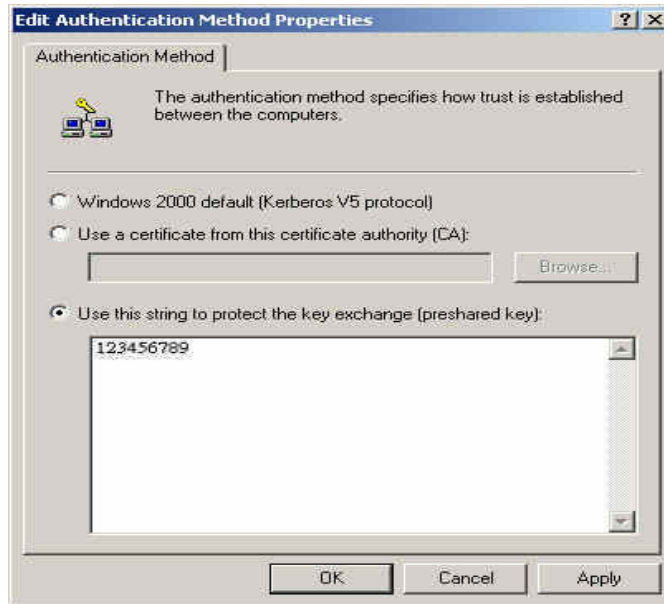
**Figure11-70 Tunnel Setting WebUI**

**STEP 40 .** Enter **Authentication Methods** WebUI and select **Edit**.  
(Figure11-71)



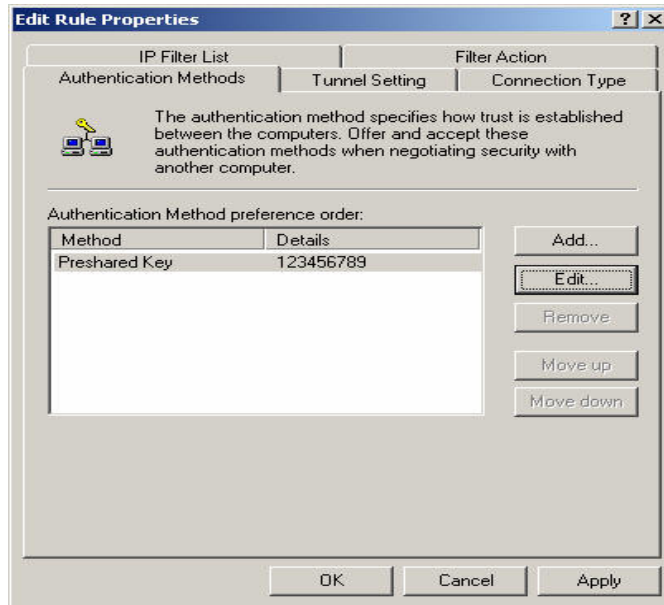
**Figure11-71 Authentication Methods Setting WebUI**

**STEP 41** . Select the item **Use this string (presared key) to protect the key exchange (presared key)** and enter the preshared key: 123456789 (Figure11-72)



**Figure11-72 Complete Authentication Method Setting**

**STEP 42 . Complete Setting and close the WebUI (Figure11-73)**



**Figure11-73 Complete New Rule Properties Setting**

### STEP 43 . Complete VPN\_B LAN TO WAN Settings (Figure11-74)

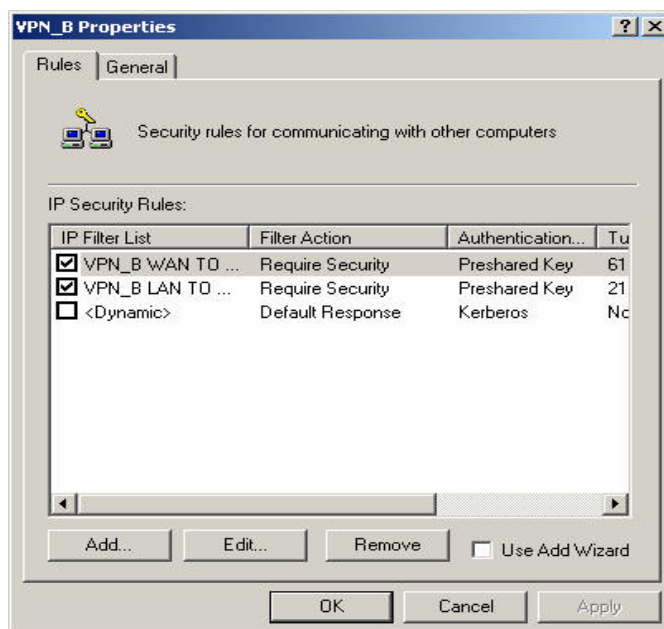
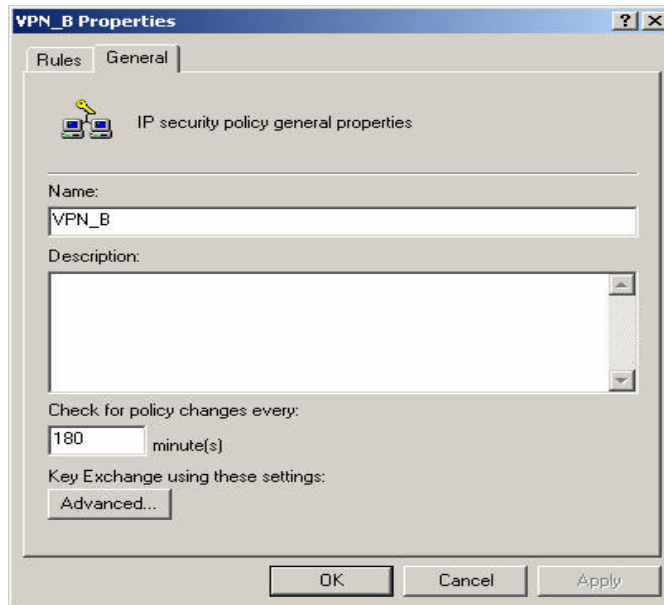


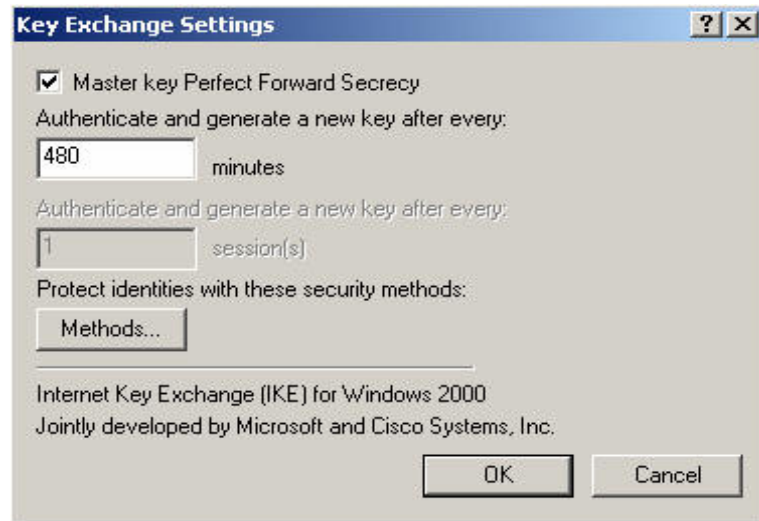
Figure11-74 Complete VPN\_B LAN TO WAN Setting

**STEP 44** . Please enter **General** in **VPN\_B Properties** WebUI and click **Advanced** (Figure11-75)



**Figure11-75 VPN\_B Properties General WebUI**

**STEP 45 .** Please select **Master key perfect forward secrecy (PFS)** and click **Methods.** (Figure11-76)



**Figure11-76 Key Exchange Settings WebUI**

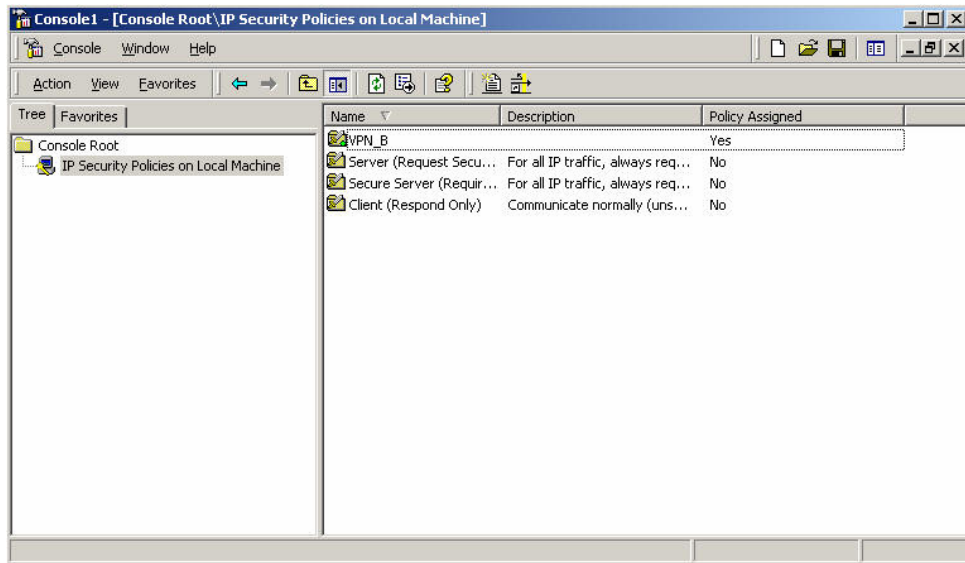


**STEP 46 .** Please move **IKE/ 3DES/ MD5 /Medium (2)** to the top and complete all the settings. (Figure11-77)



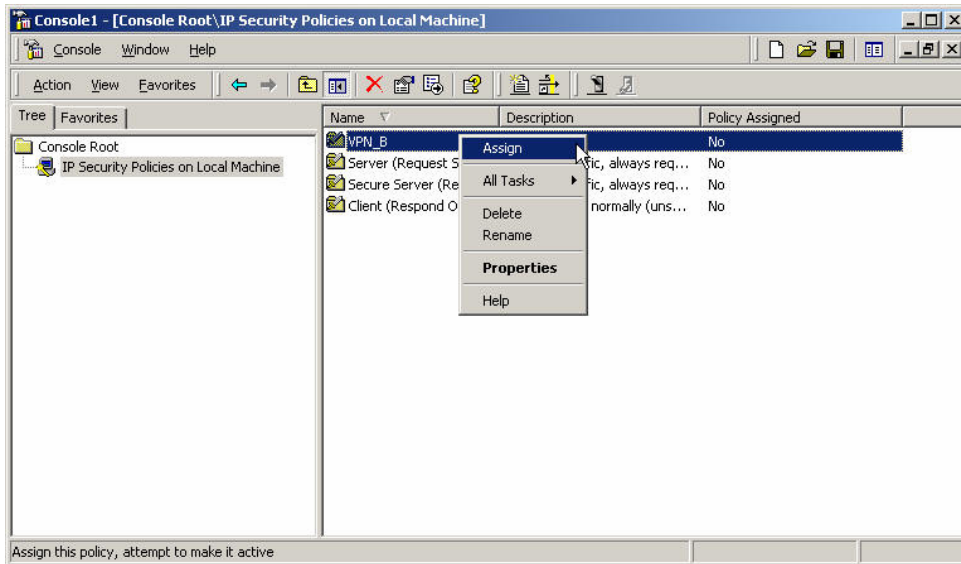
**Figure11-77 To Adjust Security Method Order**

**STEP 47 .** Complete all the Window2000 VPN Setting of Company B  
(Figure11-78)



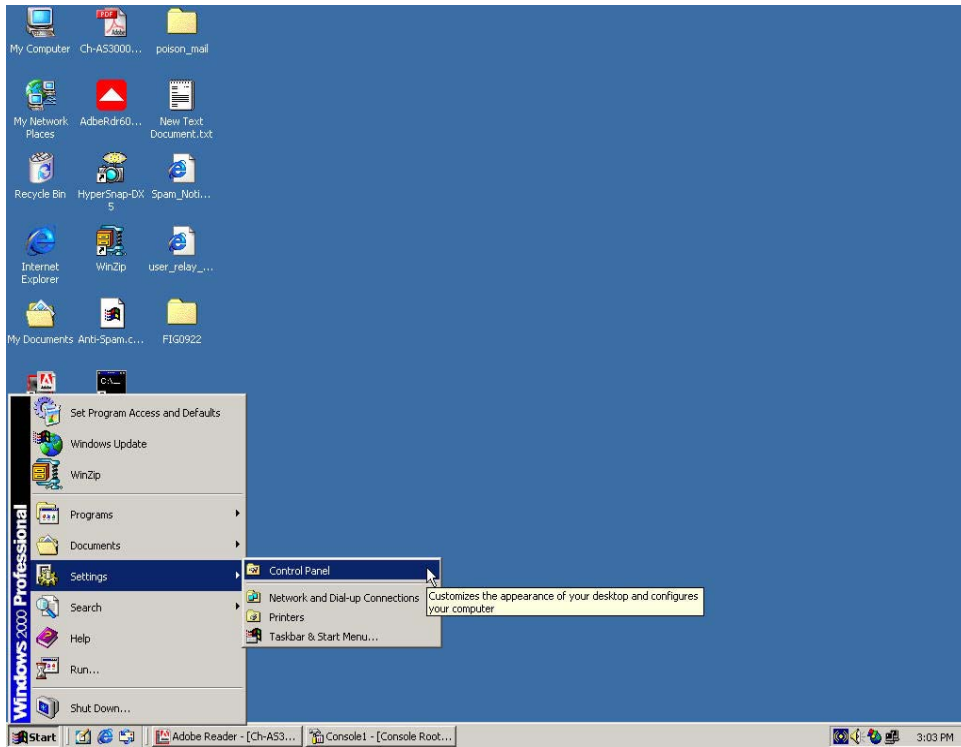
**Figure11-78 Complete Windows2000 IPsec VPN Setting**

**STEP 48 .** Please press the right button of the mouse on **VPN\_B** and enable VPN\_B. (Figure11-79)



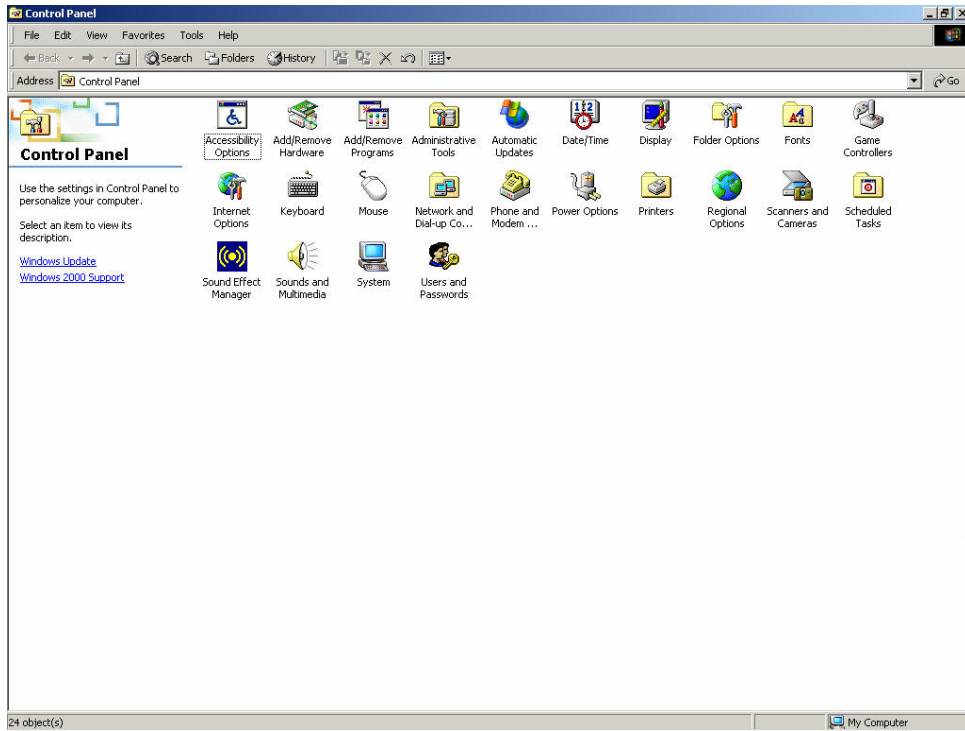
**Figure11-79 Enable VPN\_B Security Method**

**STEP 49 .** To reboot IPSec Service, please begin with **Start** and select **Settings** then enter **Control Panel**. (Figure11-80)



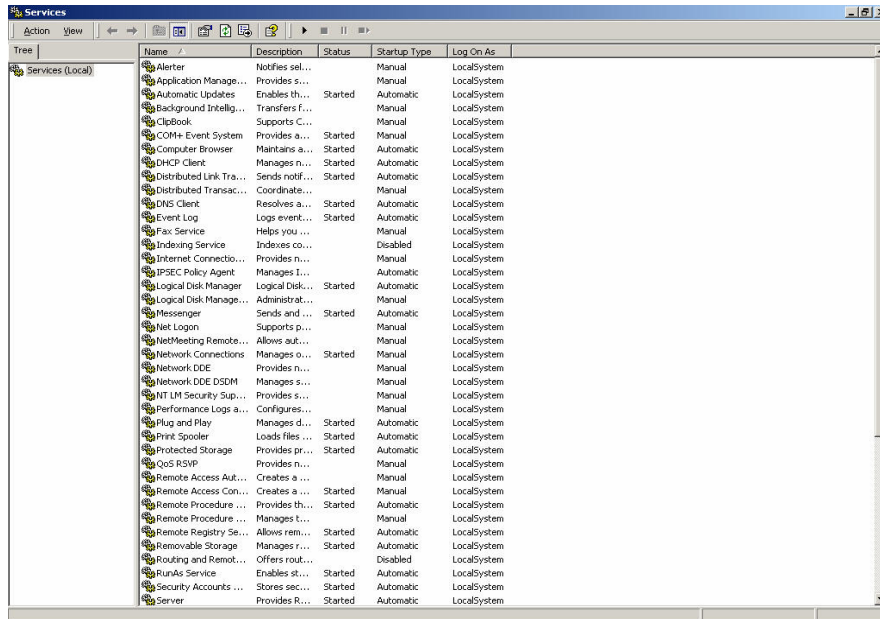
**Figure11-80 Enter Control Panel**

**STEP 50 .** After entering **Control Panel** WebUI, please enter **Administrative Tools**. (Figure11-81)



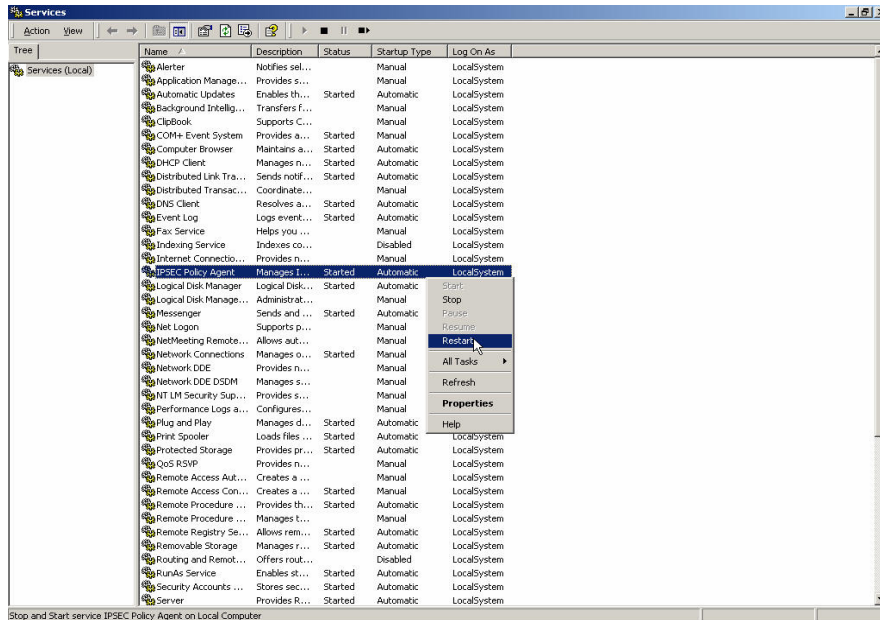
**Figure11-81 Enter Administrative Tools**

**STEP 51 . Please select **Services** item after entering **Administrative Tools**.  
(Figure11-82)**



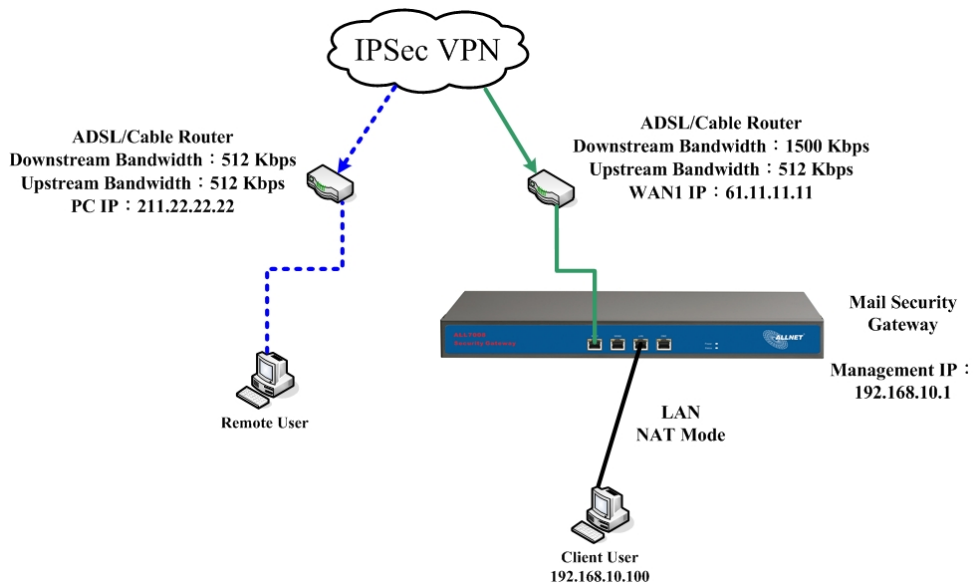
**Figure11-82 Enter Services item**

**STEP 52 .** After entering Services, please select **IPSec Services** to restart.  
(Figure11-83)



**Figure11-83 Restart IPsec Policy Agent**

**STEP 53 .** Complete all of the settings. (Figure11-84)



**Figure11-84 The IPSec VPN Setting of ALL7008 and Windows 2000**



## Setting IPsec VPN connection between two ALL7008 (Connection adopts Aggressive Mode Algorithm)

### 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 ALL7008 as flattop. Suppose Company A **192.168.10.100** is going to have VPN connection with Company B **192.168.20.100** and download the resource. (Connection adopts Aggressive Mode Algorithm)

**The Default Gateway of Company A is the LAN IP of the ALL7008 192.168.10.1. Follow the steps below:**

**STEP 1** . Enter the default gateway of ALL7008 of Company A 192.168.10.1, and select **IPsec Autokey** in **VPN** function. Click **New Entry** (Figure11-85)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
New Entry					

Figure11-85 IPsec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_A**, and select **LAN** in From Source. Also select **WAN1** in Use interface and fill in Subnet: 192.168.10.0 and Mask: 255.255.255.0 (Figure11-86)

<b>VPN Auto Keyed Tunnel</b>	
Name	VPN_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.10.0 / 255.255.255.0

**Figure11-86 IPSec VPN Autokey Tunnel Setting**

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the IP Address, **Subnet** 192.168.20.0, and **Mask** 255.255.255.0 of Company B. (Figure11-87)

<b>To Destination</b>	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

**Figure11-87 IPSec To Destination Setting**

**STEP 4 .** Select **Preshare** in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-88)

Authentication Method	Preshare
Preshared Key	123456789

**Figure11-88 IPSec Authentication Method Setting**

**STEP 5 .** Select **Aggressive Mode Algorithm** in **Encapsulation**. When setup connection, it will choose the Algorithm as 3DES ENC Algorithm, MD5 AUTH Algorithm, and GROUP2 automatically.

**My ID/ Peer ID** can choose to enter nothing; or enter different IP Address if you are willing to input. For example: 11.11.11.11, 22.22.22.22. If you are going to input numbers or alphabets for detection, add @ in the front. For example: @123A, @Abcd1. (Figure11-89)

<input checked="" type="checkbox"/> Aggressive mode	
My ID	11.11.11.11
Peer ID	@abc123

Figure11-89 IPSec Aggressive Mode Setting

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

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 encryption way for connection. (Figure11-90)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Figure11-90 IPSec Algorithm Setting List

**STEP 7 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, also can enter the **Keep Alive IP** of Company B: 192.168.20.100, to prevent disconnection. (Figure11-91)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.20.100

Figure11-91 IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Select **Schedule**, **QoS**, and **Authentication-User** and if it is permissive to connect with each other by **Show remote Network Neighborhood**. (Figure11-92)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

Figure11-92 IPSec Schedule and QoS Setting

**STEP 9 .** Click **OK** to complete the setting of Company A (Figure11-93)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN_A	211.22.22.22	192.168.20.0	None	Disconnect	Connecting Modify Remove

New Entry

Figure11-93Complete Company A IPSec VPN Setting

The Default Gateway of Company B 192.168.20.100 is the LAN IP of the ALL7008 192.168.20.1. Follow the steps below:

**STEP 1** . Enter the default gateway of the ALL7008 of Company B 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry** (Figure11-94)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
<div>New Entry</div>					

Figure11-94 IPSec Autokey WebUI

**STEP 2** . In the list of **IPSec Autokey**, fill in Name with **VPN\_B**, and select **LAN** in From Source. Also fill in Subnet: 192.168.20.0 and Mask: 255.255.255.0 (Figure11-95)

VPN Auto Keyed Tunnel	
Name	VPN_B
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.20.0 / 255.255.255.0

Figure11-95 IPSec VPN Autokey Tunnel Setting

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the Remote IP Address, **Subnet** 192.168.10.0, and **Mask** 255.255.255.0 of Company A. (Figure11-96)

<b>To Destination</b>	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	61.11.11.11
Subnet / Mask	192.168.10.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

**Figure11-96 IPSec To Destination Setting**

**STEP 4 .** Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-97)

Authentication Method	Preshare ▼
Preshared Key	123456789

**Figure11-97 IPSec Authentication Method Setting**

**STEP 5 .** Select **Aggressive Mode Algorithm** in **Encapsulation**. When setup connection, it will choose the Algorithm as 3DES ENC Algorithm, MD5 AUTH Algorithm, and GROUP2 automatically.

**My ID/ Peer ID** can choose to enter nothing; or enter different IP Address if you are willing to input. For example: 11.11.11.11, 22.22.22.22. If you are going to input numbers or alphabets for detection, add @ in the front. For example: @123A, @Abcd1. (Figure11-98)

<input checked="" type="checkbox"/> <b>Aggressive mode</b>	
My ID	<input type="text" value="@abc123"/>
Peer ID	<input type="text" value="11.11.11.11"/>

Figure11-98 IPSec Aggressive Mode Setting

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

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 connection. (Figure11-99)

<b>IPSec Algorithm</b>	
<input checked="" type="radio"/> <b>Data Encryption + Authentication</b>	
ENC Algorithm	<input type="text" value="3DES"/>
AUTH Algorithm	<input type="text" value="MD5"/>
<input type="radio"/> <b>Authentication Only</b>	

Figure11-99 IPSec Algorithm Setting

**STEP 7 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, also can enter the **Keep Alive IP** of Company A: 192.168.10.100 to prevent disconnection. (Figure11-100)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.10.100

Figure11-100 IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Select **Schedule**, **QoS**, and **Authentication-User** and if it is permissive to connect with each other by **Show remote Network Neighborhood**. (Figure11-101)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

Figure11-101 IPSec Schedule and QoS Setting

**STEP 9 .** Click **OK** to complete the setting of Company B (Figure11-102)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure		
VPN_B	61.11.11.11	192.168.10.0	None	Disconnect	Connecting	Modify	Remove

New Entry

Figure11-102 Complete CompanyB IPSec VPN Setting



## STEP 10 . Complete IPsec VPN Aggressive Mode Settings: (Figure11-103)

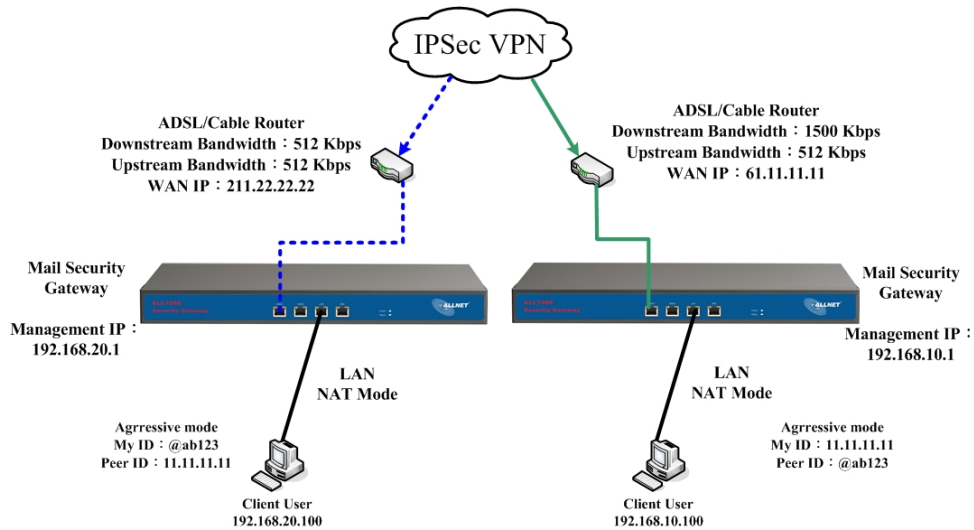


Figure11-103 IPsec VPN Aggressive Mode Settings

## Setting IPSec VPN connection between two ALL7008 (Adopt GRE Packets)

### 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 ALL7008 as work platform. Suppose Company A **192.168.10.100** is going to have VPN connection with Company B **192.168.20.100** and download the resource. (Connection adopts GRE/IPSec Algorithm)

**The Default Gateway of Company A is the LAN IP of the ALL7008 192.168.10.1. Follow the steps below:**

**STEP 1 .** Enter the default gateway of ALL7008 of Company A 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry** (Figure11-104)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
New Entry					

Figure11-104 IPSec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_A**, and select **LAN** in From Source. Also fill in Subnet: 192.168.10.0 and Mask: 255.255.255.0 of Company A. (Figure11-105)

<b>VPN Auto Keyed Tunnel</b>	
Name	VPN_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
Subnet / Mask	192.168.10.0 / 255.255.255.0

**Figure11-105 IPSec VPN Autokey Tunnel Setting**

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the IP Address, **Subnet** 192.168.20.0, and **Mask** 255.255.255.0 of Company B. (Figure11-106)

<b>To Destination</b>	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	211.22.22.22
Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

**Figure11-106 IPSec To Destination Setting**

**STEP 4 .** Select **Preshare** in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-107)

Authentication Method	Preshare
Preshared Key	123456789

**Figure11-107 IPSec Authentication Method Setting**

**STEP 5 .** Select **ISAKMP Algorithm** in **Encapsulation**. 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 connection. (Figure11-108)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP1

Figure11-108 IPSec Encapsulation Setting

**STEP 6 .** Select **GRE/IPSec** and enter **GRE Local IP**: 192.168.50.100. **GRE Remote IP**: 192.168.50.200. (GRE Local IP must be at the same subnet (C class)) (Figure11-109)

<input checked="" type="checkbox"/> GRE/IPSec	
GRE Local IP	192.168.50.100
GRE Remote IP	192.168.50.200

Figure11-109 GRE/IPSec Setting

**STEP 7 .** Select **Data Encryption+Authentication** in **IPSec Algorithm**. You can choose **Data Encryption+Authentication** or **Authentication Only** to communicate:

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 connection. (Figure11-110)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Figure11-110 IPSec Algorithm Setting

**STEP 8 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, but the **Keep Alive IP** field must be blank. (Figure11-111)

<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	

Figure11-111 IPSec Perfect Forward Secrecy Setting

**STEP 9 .** Select **Schedule**, **QoS**, and **Authentication-User** of Company A and if it is permissive to connect with each other by **Show remote Network Neighborhood**. (Figure11-112)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	
OK Cancel	

Figure11-112 IPSec Schedule and QoS Setting

**STEP 10** . Click **OK** to complete the setting of Company A (Figure11-113)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure		
VPN_A	211.22.22.22	192.168.20.0	None	Disconnect	Connecting	Modify	Remove
New Entry							

Figure11-113 Complete IPSec VPN Setting of Company A

The Default Gateway of Company B is the LAN IP of the ALL7008: 192.168.20.1. Follow the steps below:

**STEP 1** . Enter the default gateway of ALL7008 of Company B 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry** (Figure11-114)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
<div>New Entry</div>					

Figure11-114 IPSec Autokey WebUI

**STEP 2** . In the list of **IPSec Autokey**, fill in Name with **VPN\_B**, and select **LAN** in From Source and **WAN1** in Use Interface. Also fill in Subnet: 192.168.20.0 and Mask: 255.255.255.0 (Figure11-115)

VPN Auto Keyed Tunnel		
Name	<input type="text" value="VPN_B"/>	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
Use interface	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2	
Subnet / Mask	<input type="text" value="192.168.20.0"/> / <input type="text" value="255.255.255.0"/>	

Figure11-115 IPSec VPN Autokey Tunnel Setting

**STEP 3 .** Select **Remote Gateway-Fixed IP** In **To Destination** list and enter the Remote IP Address, **Subnet** 192.168.10.0, and **Mask** 255.255.255.0 of Company A. (Figure11-116)

<b>To Destination</b>	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	61.11.11.11
Subnet / Mask	192.168.10.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	

Figure11-116 IPSec To Destination Setting

**STEP 4 .** Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits) (Figure11-117)

Authentication Method	Preshare
Preshared Key	123456789

Figure11-117 IPSec Authentication Method Setting

**STEP 5 .** Select **ISAKMP Algorithm** in **Encapsulation**. 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 connection. (Figure11-118)

<b>Encapsulation</b>	
<b>ISAKMP Algorithm</b>	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

Figure11-118 IPSec Encapsulation Setting



**STEP 6 .** Select **GRE/IPSec** and enter **GRE Local IP:** 192.168.50.200. **GRE Remote IP:** 192.168.50.100. (GRE Local IP must be at the same subnet (C class)) (Figure11-119)

<input checked="" type="checkbox"/> <b>GRE/IPSec</b>	
GRE Local IP	192.168.50.200
GRE Remote IP	192.168.50.100

**Figure11-119 GRE/IPSec Setting**

**STEP 7 .** Select **Data Encryption+Authentication** in **IPSec Algorithm**. You can choose **Data Encryption+Authentication** or **Authentication Only** to communicate:

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 connection. (Figure11-120)

<b>IPSec Algorithm</b>	
<input checked="" type="radio"/> <b>Data Encryption + Authentication</b>	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> <b>Authentication Only</b>	

**Figure11-120 IPSec Algorithm Setting**

**STEP 8 .** After selecting **Perfect Forward Secrecy** and enter 28800 seconds in **IPSec Lifetime**, but the **Keep Alive IP** field must be blank. (Figure11-121)

<input checked="" type="checkbox"/> <b>Perfect Forward Secrecy</b>	
IPSec Lifetime	28800 Seconds
Keep alive IP :	

**Figure11-121 IPSec Perfect Forward Secrecy Setting**

**STEP 9 .** Select **Schedule**, **QoS**, and **Authentication-User** and if it is permissive to connect with each other by **Show remote Network Neighborhood**. (Figure11-122)

Schedule	Schedule_1
QoS	QoS_1
Authentication-User	All_NET
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

Figure11-122 IPSec Schedule and QoS Setting

**STEP 10 .** Click **OK** to complete the setting of Company B (Figure11-123)

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure		
VPN_B	61.11.11.11	192.168.10.0	None	Disconnect	Connecting	Modify	Remove

Figure11-123 Complete IPSec VPN Setting of Company B

## STEP 11 . Complete IPsec VPN GRE/IPsec Setting (Figure11-124)

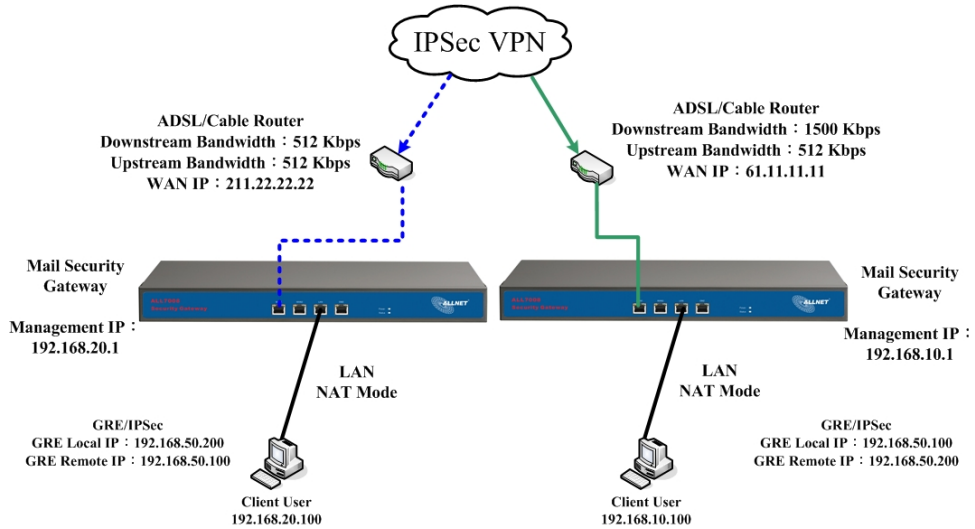


Figure11-124 IPsec VPN GRE/IPsec Setting

# Setting PPTP VPN connection between two ALL7008

## 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 ALL7008 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.

**STEP 1 .** Enter **PPTP Server** of **VPN** function in the ALL7008 of Company A.

Select **Modify**:

- Select **Encryption**
- **Client IP Range**: Enter 192.44.75.1-254
- Idle Time: Enter 0
- **Schedule**: Select Schedule\_1 (Figure11-125)

Modify Server Design	
<input type="radio"/> Disable PPTP	
<input checked="" type="radio"/> Enable PPTP	
<input checked="" type="checkbox"/> Encryption	
Client IP Range :	192.44.75.1 -- 254
Auto-Disconnect if idle <input type="text" value="0"/> minutes (0: means always connected)	
Schedule	Schedule_1 ▼
<div>OK Cancel</div>	

Figure11-125 Modify 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 ALL7008 of Company A:

- Select **New Entry**
- **User Name:** Enter PPTP\_Connection
- **Password:** Enter 123456789
- **Remote Client:** Select **Multi-Machine** and enter 192.168.20.0 in **IP Address**; **Netmask:** 255.255.255.0
- **Client IP assigned by:** Select **IP Range** (Figure11-126)

Add New PPTP Server		
User Name :	<input type="text" value="PPTP_Connection"/>	
Password :	<input type="password" value="*****"/>	
Remote Client		
<input type="radio"/> Single Machine		
<input checked="" type="radio"/> Multi-Machine		
	IP Address :	<input type="text" value="192.168.20.0"/>
	Netmask :	<input type="text" value="255.255.255.0"/>
Client IP assigned by		
<input checked="" type="radio"/> IP Range		
<input type="radio"/> Fixed IP : <input type="text"/>		
<div>OK Cancel</div>		

Figure11-126 PPTP VPN Server Setting

**STEP 3 .** Add the following settings in **PPTP Client** of **VPN** function in the ALL7008 of Company B:

- Select **New Entry**
- **User Name:** Enter PPTP\_Connection
- **Password:** Enter123456789
- **Server Address:** Enter 61.11.11.11
- Select **Encryption**
- **Remote Server:** Select Multi-Machine and enter 192.168.10.0 in IP Address; Netmask: 255.255.255.0
- Select **Auto-Connect when sending packet through the link**
- Idle Time: Enter 0
- **Schedule:** Select Schedule\_1
- Complete the setting of PPTP Server (Figure11-127)

Add New PPTP Client	
User Name :	PPTP_Connection
Password :	*****
Server Address :	61.11.11.11 <input checked="" type="checkbox"/> Encryption
Remote Server	
<input type="radio"/> Single Machine	
<input checked="" type="radio"/> Multi-Machine	
IP Address :	192.168.10.0
Netmask :	255.255.255.0
<input type="checkbox"/> always-connect	
<input checked="" type="checkbox"/> Auto-Connect when sending packet through the link	
Auto-Disconnect if idle <input type="text" value="0"/> minutes (0: means always connected)	
Schedule	Schedule_1
<input type="checkbox"/> NAT(Connect to Windows PPTP Server)	
OK Cancel	

**Figure11-127 PPTP VPN Client Setting**

#### STEP 4 . Complete PPTP VPN Connection (Figure11-128)

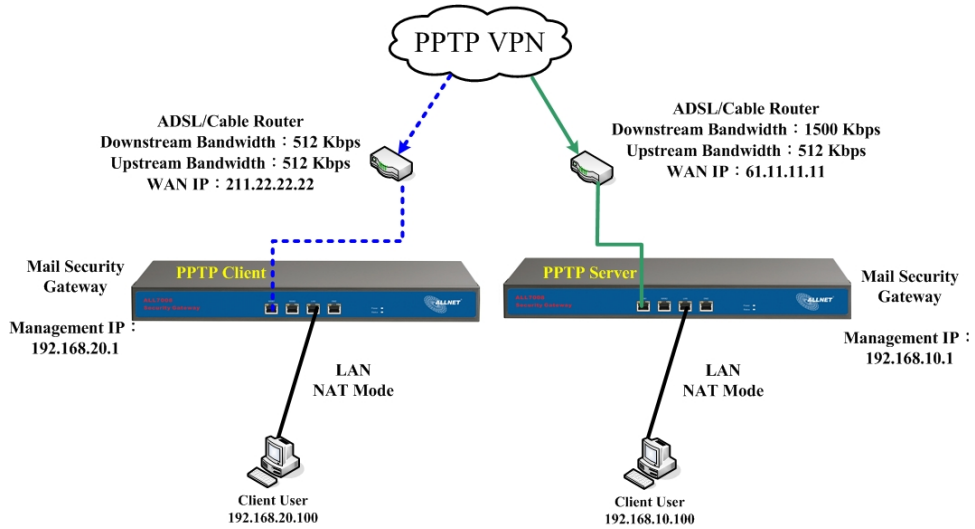


Figure11-128 PPTP VPN Connection Setting



## Setting VPN connection between ALL7008 PPTP VPN and Windows 2000 PPTP VPN

### Preparation

Company A    ALL7008

**WAN IP: 61.11.11.11**

**LAN IP: 192.168.10.X**

Company B    Windows 2000 PC

**WAN IP: 211.22.22.22**

This example takes one ALL7008 and one Windows 2000 VPN-PPTP as flaptop. Suppose Company B **211.22.22.22** is going to have VPN connection with Company A **192.168.10.100** and download or share the resource.

The default gateway of Company A is the LAN IP of the ALL7008. Enter the following setting:

**STEP 1 .** Enter **PPTP Server** of **VPN** function in the ALL7008 of Company A.

Select **Modify**:

- Select **Encryption**
- **Client IP Range**: Enter 192.44.75.1-254
- Idle Time: Enter 0
- **Schedule**: Select Schedule\_1 (Figure11-129)

Modify Server Design	
<input type="radio"/> Disable PPTP	
<input checked="" type="radio"/> Enable PPTP	
<input checked="" type="checkbox"/> Encryption	
Client IP Range :	192.44.75.1 -- 254
Auto-Disconnect if idle <input type="text" value="0"/> minutes (0: means always connected)	
Schedule	Schedule_1 ▼
<div>OK Cancel</div>	

Figure11-129 Modify PPTP VPN Server Setting



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

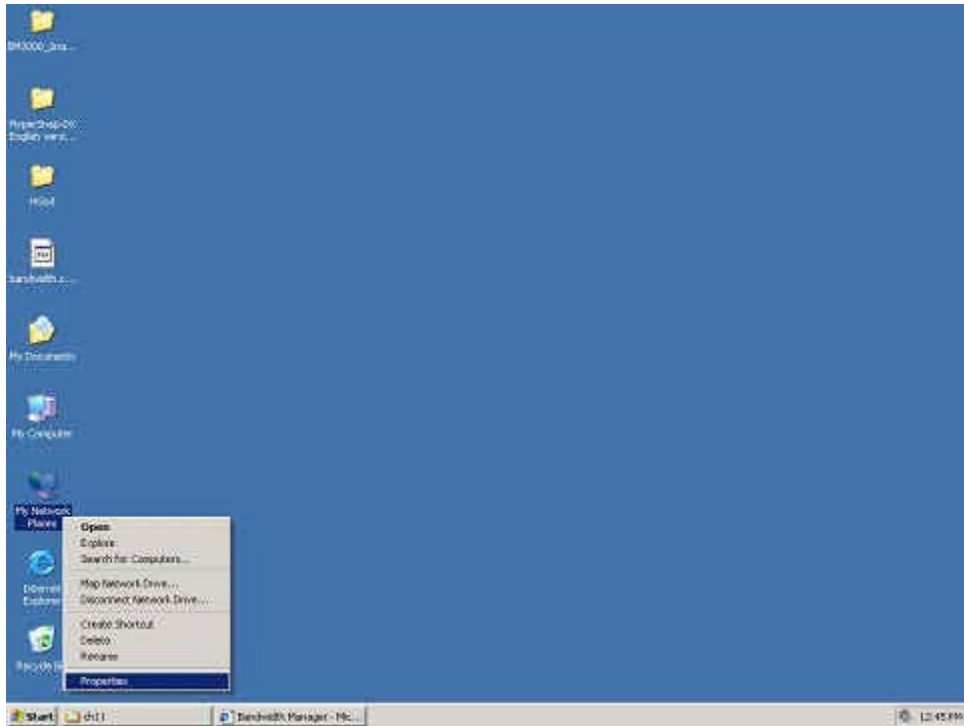
**STEP 2 .** Add the following settings in **PPTP Server** of **VPN** function in the ALL7008 of Company A:

- Select **New Entry**
- **User Name:** Enter PPTP\_Connection
- **Password:** Enter 123456789
- **Remote Client:** Select Single Machine
- **Client IP assigned by:** Select IP Range (Figure11-130)

Add New PPTP Server		
User Name :	<input type="text" value="PPTP_Connection"/>	
Password :	<input type="password" value="*****"/>	
Remote Client		
<input checked="" type="radio"/> Single Machine		
<input type="radio"/> Multi-Machine		
	IP Address :	<input type="text"/>
	Netmask :	<input type="text"/>
Client IP assigned by		
<input checked="" type="radio"/> IP Range		
<input type="radio"/> Fixed IP : <input type="text"/>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

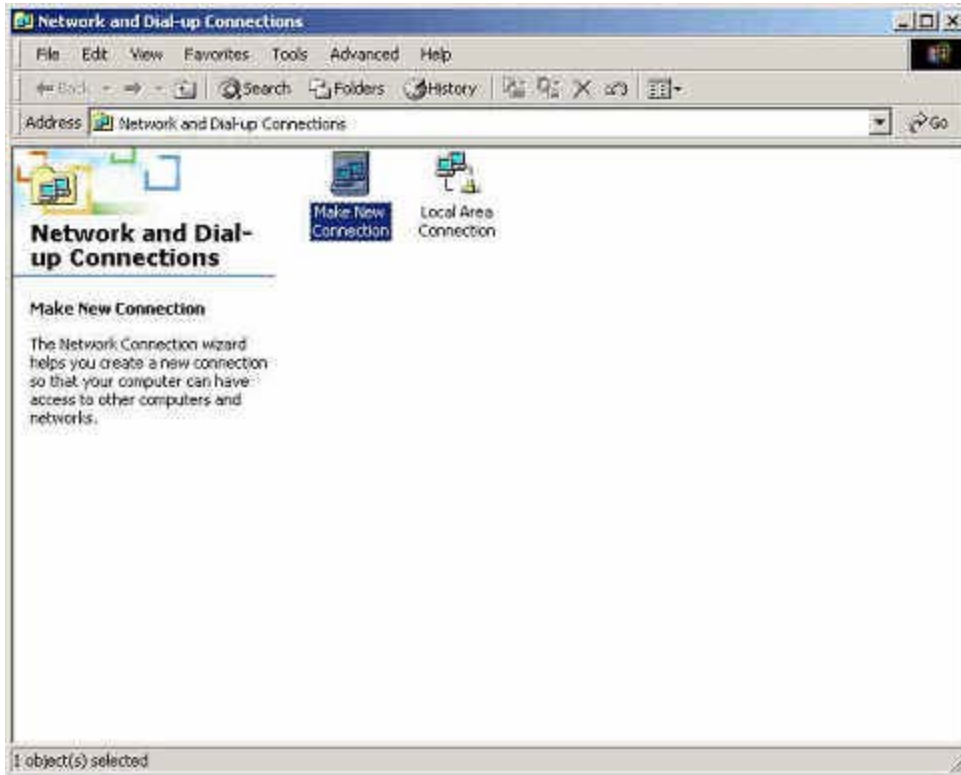
Figure11-130 Modify PPTP VPN Server Connection Setting

**STEP 1 .** Enter Windows 2000, press the right key of the mouse in **My Network Place** and select **Properties**. (Figure11-131)



### Figure11-131 Start out Windows 2000 PPTP VPN Setting

**STEP 2 . Enter **Network and Dial-up Connections** WebUI and then enter **Make New Connection.** (Figure11-132)**



**Figure11-132 Network and Dial-up Connections WebUI**

**STEP 3 .** In the **Location Information** WebUI, enter **country/region**, **city code**, and the **phone system** you use, and then click **OK** (Figure11-133)

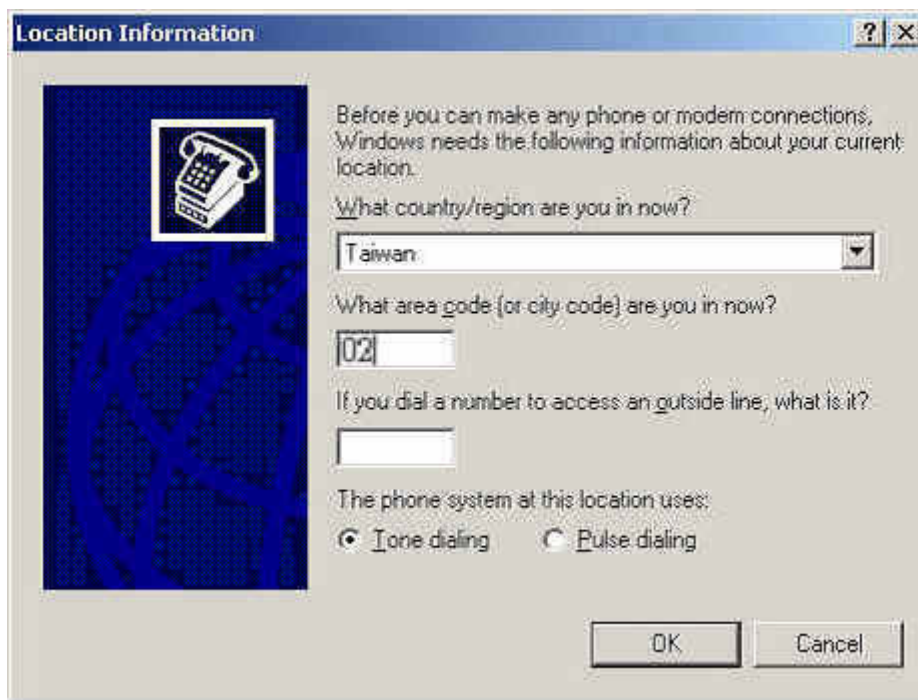
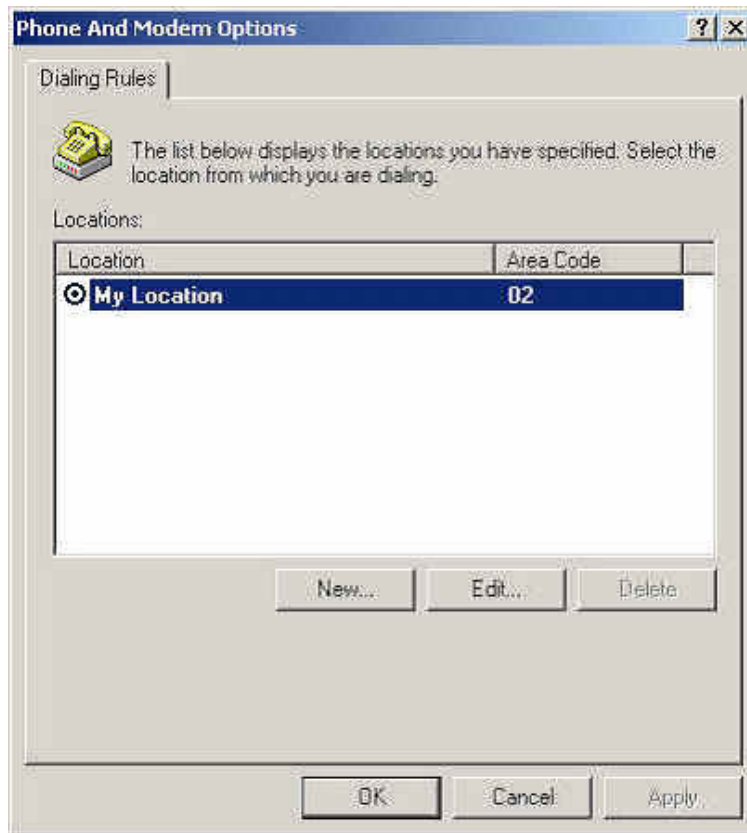


Figure11-133 Setup Location Information WebUI

**STEP 4 . Click OK in Phone And Modem Options WebUI. (Figure11-134)**



**Figure11-134 Phone and Modem Options WebUI**

**STEP 5 .** Click on **Next** in **Network Connection Wizard**. (Figure11-135)



**Figure11-135 Network Connection Wizard WebUI**

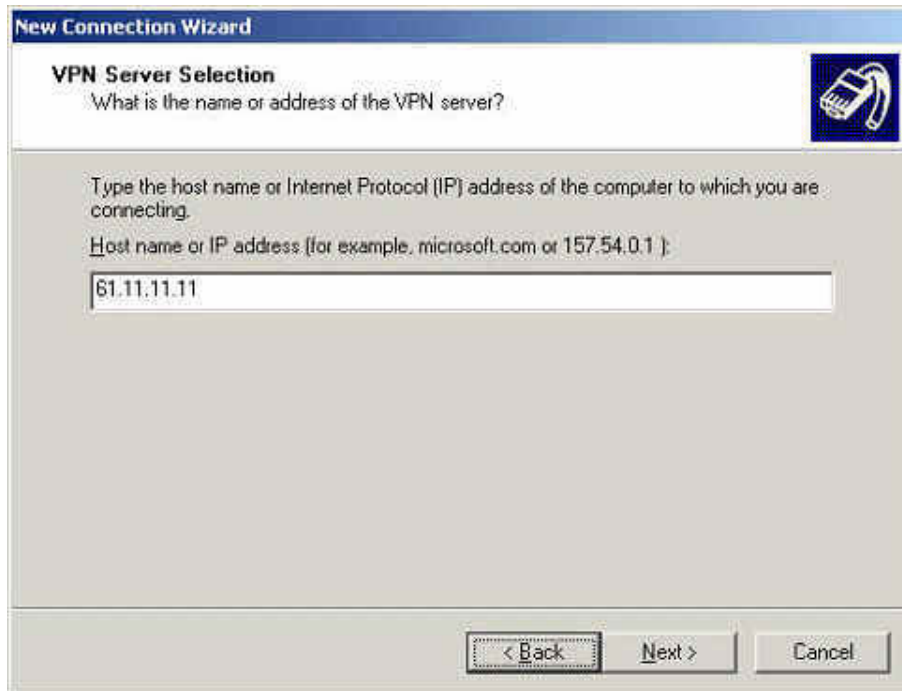


**STEP 6 .** Select **Connect to a private network through the Internet** in **Network Connection Wizard** WebUI and click on **Next** (Figure11-136)



**Figure11-136 Setup to connect to a private network through the Internet**

**STEP 7 .** Enter **IP Address** in **Network Connection Wizard** WebUI and click **Next**. (Figure11-137)



**New Connection Wizard**

**VPN Server Selection**

What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

61.11.11.11

< Back    Next >    Cancel

**Figure11-137 Host Name or IP Address Setting**

**STEP 8 .** In **Network Connection Wizard** WebUI, create the connection **For all users** and click on **Next**. (Figure11-138)



**Figure11-138 Connection Availability Setting**

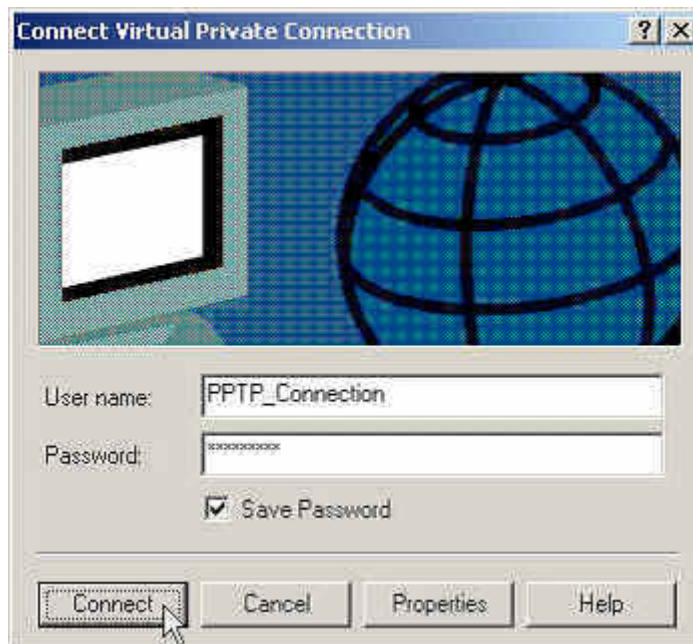
**STEP 9 .** Click on **Finish** on **Network Connection Wizard** WebUI to Complete the New Connection Wizard setting (Figure11-139)



**Figure11-139 Complete the Network Connection Wizard Setting**

**STEP 10 .** Enter the following settings in **Connect Virtual Private Connection** function: (Figure11-140)

- **User name:** Enter PPTP\_Connection
- **Password:** Enter 123456789
- Select **Save Password**
- Click on **Connect**
- Connecting VPN\_Connection WebUI show up (Figure11-141)
- At last is Connection Complete WebUI (Figure11-142)



**Figure11-140 Connect Virtual Private Connection Setting WebUI**



**Figure11-141 Connecting VPN Connection**



**Figure11-142 PPTP VPN Connection Complete**

## STEP 11 . Complete PPTP VPN Connection Settings (Figure11-143)

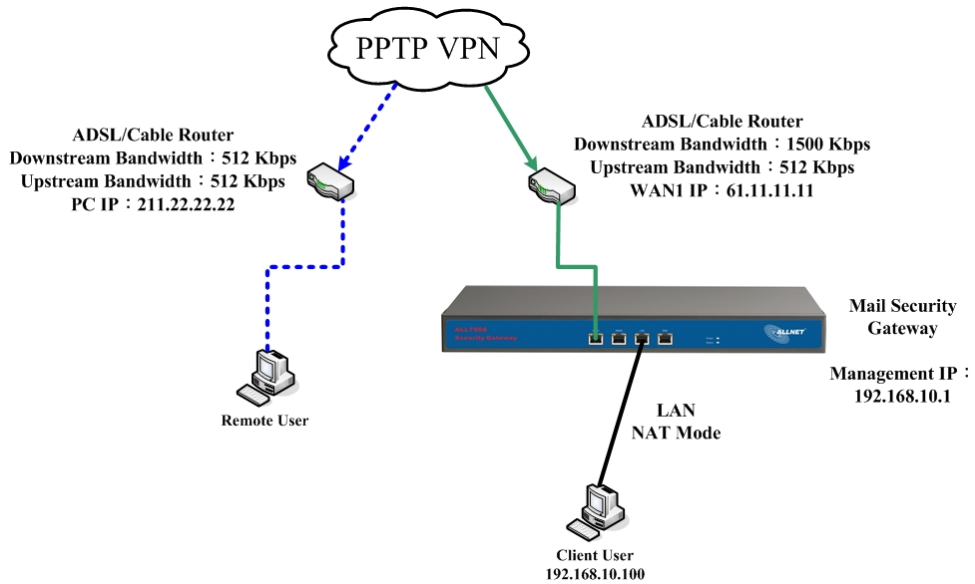


Figure11-143 PPTP VPN Connection Setting

Every packet has to be detected if it corresponds with Policy or not when it passes the ALL7008. When the conditions correspond with certain policy, it will pass the ALL7008 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 ALL7008.



### 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 ALL7008 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 ALL7008'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 ALL7008 (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
	Alarm Threshold	Enable Alarm Threshold

**Traffic Log:**

- Record all the packets that go through policy. Click  If you want to check the packets through certain 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

**Alarm Threshold:**

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

**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 ALL7008 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	<b>Outgoing</b>	Set up the policy that can monitor the internal users. (Take Logging, Statistics, Alarm Threshold for example)	<b>281</b>
Ex2	<b>Outgoing</b>	Forbid the users to access to specific network. (Take specific WAN IP and Content Blocking for example)	<b>285</b>
Ex3	<b>Outgoing</b>	Only allow the users who pass Authentication to access to Internet in particular time.	<b>290</b>
Ex4	<b>Incoming</b>	The external user control the internal PC through remote control software (Take pcAnywhere for example)	<b>292</b>
Ex5	<b>WAN to DMZ</b>	Under DMZ NAT Mode, set a FTP Server and restrict the download bandwidth from external, Quota per Day, and MAX. Concurrent Sessions.	<b>294</b>
Ex6	<b>WAN to DMZ DMZ to WAN LAN to DMZ</b>	Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode	<b>296</b>

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

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

- Click **New Entry**
- Select **Traffic Log**
- Select **Statistics**
- Click **OK** (Figure12-1)

Comment :	<input type="text"/> (Max. 32 characters)		
<a href="#">Add New Policy</a>			
Source Address	Inside_Any ▾		
Destination Address	Outside_Any ▾		
Service	ANY ▾		
Schedule	None ▾		
Authentication User	None ▾		
Trunk	None ▾		
Action, WAN Port	PERMIT ALL ▾		
Traffic Log	<input checked="" type="checkbox"/> Enable		
Statistics	<input checked="" type="checkbox"/> Enable		
IDP	<input type="checkbox"/> Enable		
Content Blocking	<input type="checkbox"/> Enable		
IM / P2P Blocking	None ▾		
QoS	None ▾		
MAX. Bandwidth Per Source IP	Downstream	<input type="text"/> 0 Kbps	Upstream <input type="text"/> 0 Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/> 0		
MAX. Concurrent Sessions	<input type="text"/> 0		
<div>OK Cancel</div>			

**Figure12-1 Setting the different Policies**

**STEP 2 .** Complete the setting of Traffic Log and Statistics in **Outgoing Policy**:  
(Figure12-2)

Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY	✓		☞	🇮🇹		Modify	Remove	Pause	To 1 ▾
New Entry											

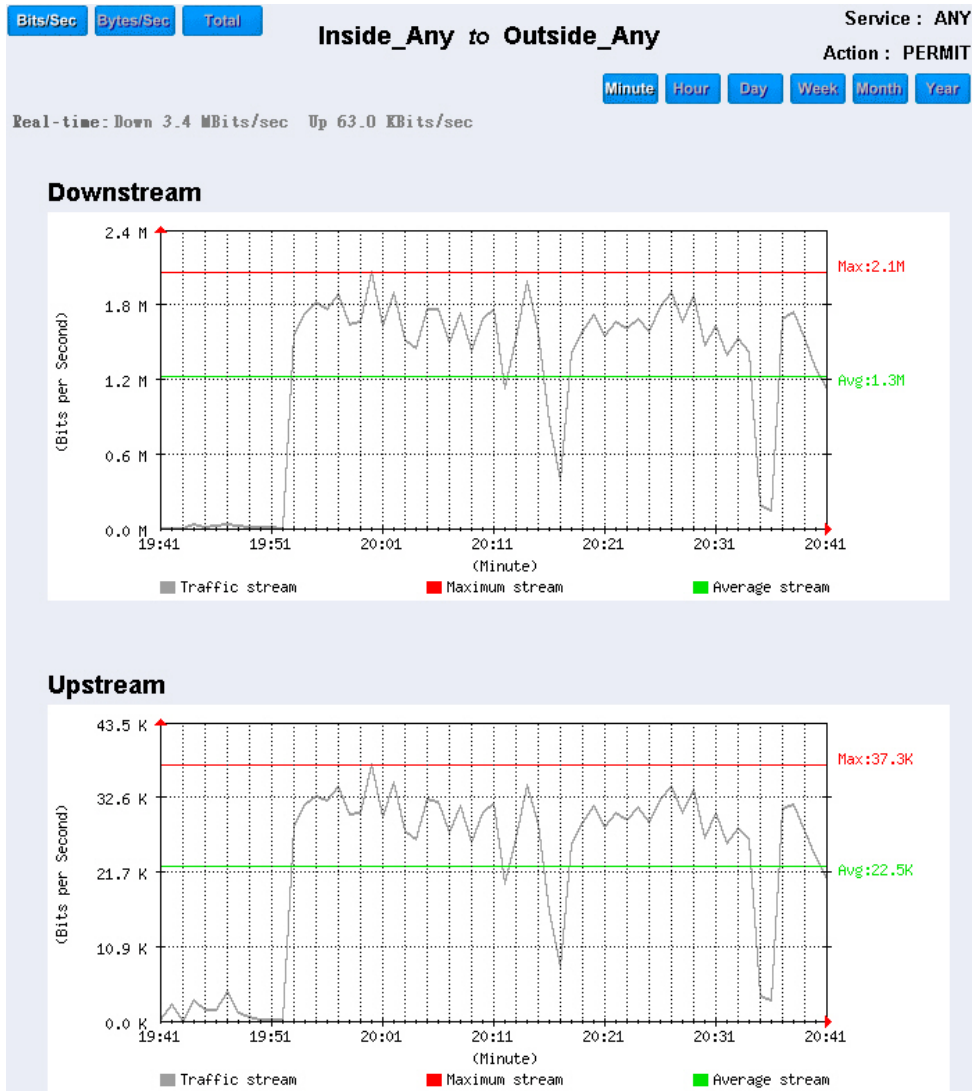
**Figure12-2 Complete Policy Setting**

**STEP 3 .** Obtain the information in **Traffic** of **Log** function if you want to monitor all the packets of the ALL7008. (Figure12-3)

Nov 16 13:19:52 ▾						Next
Time	Source	Destination	Protocol	Port	Disposition	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2207 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2207	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2207	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2207 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2207	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2204 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2207	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2207 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2207	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2204 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2204	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2204	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.5	TCP	2204 => 80	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2204	✓	
Nov 16 13:19:52	211.75.83.5	192.168.189.10	TCP	80 => 2204	✓	
Nov 16 13:19:52	192.168.189.10	211.75.83.7	TCP	2208 => 80	✓	
Nov 16 13:19:52	211.75.83.7	192.168.189.10	TCP	80 => 2208	✓	
Nov 16 13:19:52	211.75.83.7	192.168.189.10	TCP	80 => 2208	✓	
Clear						Download

**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**



**STEP 5** . It will show up the policy rule when the internal users use exceeds the default Alarm Threshold in **Traffic Alarm** of **Alarm** function. (Figure12-5)

Jul 3 20:30~20:45 ▾

Time	Source	Destination	Service	Traffic
Jul 3 20:30~20:45	Inside_Any	Outside_Any	ANY	179.770K/Sec
Jul 3 20:15~20:30	Inside_Any	Outside_Any	ANY	205.314K/Sec
Jul 3 20:00~20:15	Inside_Any	Outside_Any	ANY	220.051K/Sec
Jul 3 19:45~20:00	Inside_Any	Outside_Any	ANY	129.139K/Sec

Clear AlarmDownload Alarms

Figure12-5 Traffic Alarm 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: (Figure12-6, 12-7, 12-8, 12-9, 12-10)

URL String	Configure	
~yahoo	Modify	Remove
~google	Modify	Remove
*	Modify	Remove
New Entry		

**Figure12-6 URL Blocking Setting**

<b>Script Blocking</b>	
<input checked="" type="checkbox"/> Popup Blocking	<input checked="" type="checkbox"/> ActiveX Blocking
<input checked="" type="checkbox"/> Java Blocking	<input checked="" type="checkbox"/> Cookie Blocking
OK Cancel	

**Figure12-7 Script Blocking Setting**

<b>Peer-to-Peer Application Blocking</b>	
<input checked="" type="checkbox"/> eDonkey Blocking	
<input checked="" type="checkbox"/> Bit Torrent Blocking	
<input checked="" type="checkbox"/> WinMX Blocking	
OK Cancel	

**Figure12-8 P2P Blocking Setting**



Figure12-9 IM Blocking Setting

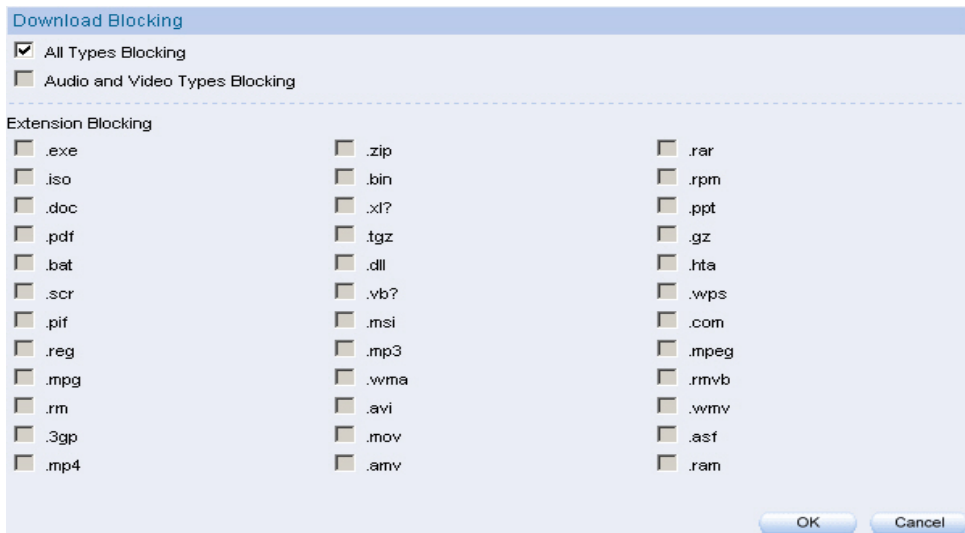


Figure12-10 Download Blocking Setting



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:  
(Figure12-11, 12-12)

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<b>In Use</b>
Remote_Server1	61.221.36.19/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Remote_Server2	221.29.56.36/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Figure12-11 Setting the WAN IP that going to block**

Name	Member	Configure
WAN_Group	Remote_Server1, Remote_Server2	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

**Figure12-12 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** (Figure12-13)

Comment : <input type="text" value=""/>		(Max. 32 characters)
<b>Modify Policy</b>		
Source Address	Inside_Any	
Destination Address	WAN_Group	
Service	ANY	
Schedule	None	
Authentication User	None	
Trunk	None	
Action, WAN Port	DENY ALL	
Traffic Log	<input type="checkbox"/> Enable	
Statistics	<input type="checkbox"/> Enable	
IDP	<input type="checkbox"/> Enable	
Content Blocking	<input type="checkbox"/> Enable	
IM / P2P Blocking	None	
QoS	None	
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps	Upstream <input type="text" value="0"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/>	
MAX. Concurrent Sessions	<input type="text" value="0"/>	
<div>OK Cancel</div>		

**Figure12-13 Setting Blocking Policy**

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

- Click **New Entry**
- Select **Content Blocking**
- Click **OK** (Figure12-14)

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**Figure12-14 Setting Content Blocking Policy**

**STEP 5 .** Complete the setting of forbidding the users to access to specific network. (Figure12-15)

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	WAN_Group	ANY	✗						Modify	Remove	Pause	To 1
Inside_Any	Outside_Any	ANY	✓						Modify	Remove	Pause	To 2

New Entry

**Figure12-15 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: (Figure12-16)

Name	Configure
WorkingTime	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>	

Figure12-16 Add New Schedule

**STEP 2 .** Enter the following in **Auth User** and **Auth User Group** in **Authentication** function: (Figure12-17)

Name	Member	Radius	POP3	Configure
laboratory	joy, john, jack			<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>				

Figure12-17 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** (Figure12-18)

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	WorkingTime
Authentication User	laboratory
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**Figure12-18 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. (Figure12-19)

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

New Entry

**Figure12-19 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: (Figure12-20)

Virtual Server Real IP 61.11.11.12			
Service	WAN Port	Server Virtual IP	Configure
PC_Anywhere	From-Service(Custom)	192.168.1.2	<div>Modify Remove</div> <div>Pause</div>
<div>New Entry</div>			

**Figure12-20 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
- Click **OK** (Figure12-21)

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	Outside_Any
Destination Address	Virtual Server 1(61.11.11.12)
Service	PC_Anywhere
Schedule	None
Trunk	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> 0 Kbps Upstream <input type="text"/> 0 Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/> 0
MAX. Concurrent Sessions	<input type="text"/> 0
NAT	<input type="checkbox"/> Enable

OK Cancel

**Figure12-21 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. (Figure12-22)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	PC_Anywhere	✓		Modify Remove Pause	To 1

New Entry

**Figure12-22 Complete Policy Setting**

## Set a FTP Server under DMZ NAT Mode and restrict the download bandwidth from external, Quota per Day, and MAX. Concurrent Sessions.

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

**STEP 2** . Enter the following setting in **Virtual Server1** of **Virtual Server** function: (Figure12-23)

Virtual Server Real IP 61.11.11.12

Service	WAN Port	Server Virtual IP	Configure
FTP (21)	21	192.168.3.2	<div>Modify Remove</div> <div>Pause</div>

New Entry

Figure12-23 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**: (Figure12-24)

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

New Entry

Figure12-24 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
- **Quota Per Day**: Enter 100000 Mbytes
- Click **OK** (Figure12-25)

Add New Policy	
Source Address	Outside_Any
Destination Address	Virtual Server 1 (61.11.11.12)
Service	FTP(21)
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
Trunk	None
MAX. Concurrent Sessions	100 (0:means unlimited)
QoS	FTP_QoS
<div>OK Cancel</div>	

Figure12-25 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) (Figure12-26)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	FTP(21)	✓		<div>Modify Remove</div>	To 1
<div>New Entry</div>						

Figure12-26 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: (Figure12-27)

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Mail_Server	61.11.11.12/255.255.255.255	00:48:54:55:E1:07	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure12-27 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: (Figure12-28)

Group name	Service	Configure
E-mail	DNS,POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure12-28 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** (Figure12-29)

Add New Policy	
Source Address	Outside_Any
Destination Address	Mail_Server
Service	E-mail
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

OK Cancel

Figure12-29 Setting a Policy to access Mail Service by WAN to DMZ

**STEP 5 .** Complete the policy to access mail service by **WAN to DMZ**.  
(Figure12-30)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mail_Server	E-mail	✓		Modify Remove	To 1

New Entry

Figure12-30 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** (Figure12-31)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Mail_Server ▾
Service	E-mail ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None ▾
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

Figure12-31 Setting a Policy to access Mail Service by LAN to DMZ

**STEP 7 .** Complete the policy to access mail service by **LAN to DMZ** (Figure12-32)

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	E-mail	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To <input type="button" value="1"/>

Figure12-32 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** (Figure12-33)

Add New Policy	
Source Address	Mail_Server
Destination Address	Outside_Any
Service	E-mail
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
Anti-Virus	<input type="checkbox"/> HTTP / WEBMAIL <input type="checkbox"/> FTP
Authentication User	None
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Figure12-33 Setting the Policy of Mail Service by DMZ to WAN

**STEP 9 .** Complete the policy access to mail service by **DMZ to WAN**.  
(Figure12-34)

Source	Destination	Service	Action	Option	Configure	Move
Mail_Server	Outside_Any	E-mail	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To 1

Figure12-34 Complete the Policy access to Mail Service by DMZ to WAN





# Configure

According to the Mail Security Configure function, it means the dealing standard towards mail of ALL7008. In this chapter, it is defined as Setting and Mail Relay.



After scanning the mails that sent to Internal Mail Server by **Anti-Spam** and **Anti-Virus** function of ALL7008, then to setup the relevant setting in **Mail Relay** function.

## Define the required fields of Setting:

### Scanned Mail Setting:

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

### Unscanned Mail Setting:

- According to the unscanned mail, it can add an unscanned message in the mail subject.
  - ◆ For example, add the following setting in this function:
    1. The scanned mail size is less than 200Kbytes
    2. Add the message to the subject line --Unscanned--
    3. Click OK (Figure13-1)

Scanned Mail Setting

The scanned spam mail size is less than  KBytes ( Range: 10 - 512 )

The scanned virus mail size is less than  KBytes ( Range: 10 - 512 )

Unscanned Mail Setting

☒ Add the message to the subject line  (Max. 255 characters)

OK Cancel

**Figure13-1 Scanned Mail Setting**

- ◆ When receive unscanned mail, it will add the tag in front of the e-mail subject. (Figure13-2)

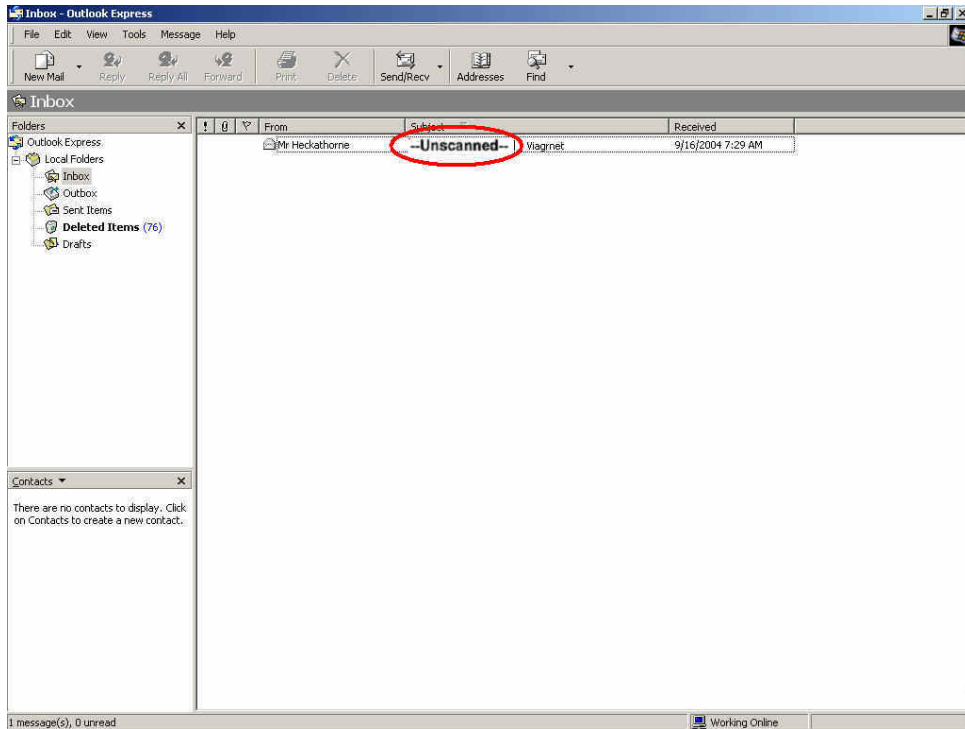


Figure13-2 The Unscanned Mail Subject WebUI

## To setup ALL7008 as Gateway (Mail Server is in DMZ, Transparent Mode)

### Preparation

WAN Port IP: 61.11.11.11

Mail Server IP: 61.11.11.12

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

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

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

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to
- **Mail Relay** setting is complete. The mails from external and its destination mail server have to be in the domain name setting, that can be received by ALL7008 and be sent to the appointed mail server after filtering. (Figure13-3)

<input checked="" type="radio"/> Domain Name of Internal Mail Server	
<input type="radio"/> Allowed External IP of Mail Relay	
Add Domain Name	
Domain Name of Mail Server	broadband.com.tw
IP Address of Mail Server	61.11.11.12
OK Cancel	

Figure13-3 Mail Relay Setting WebUI

## **To setup ALL7008 between the original Gateway and Mail Server (Mail Server is in DMZ, Transparent Mode)**

### **Preparation**

The Original Gateway's LAN Subnet: 172.16.1.0/16

WAN Port IP: 61.11.11.11

ALL7008's WAN Port IP: 172.16.1.12

Mail Server IP: 172.16.1.13

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

When LAN (172.16.1.0/16) user use the sender account of broadband.com.tw mail server to send mail to the recipient account in external mail server, have to add the following mail relay setting

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

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to (Figure13-4)

The screenshot shows a web interface for configuring Mail Relay. At the top, there are two radio buttons: 'Domain Name of Internal Mail Server' (which is selected) and 'Allowed External IP of Mail Relay'. Below this, there is a section titled 'Add Domain Name' in blue. This section contains two input fields: 'Domain Name of Mail Server' with the value 'broadband.com.tw' and 'IP Address of Mail Server' with the value '172.16.1.13'. At the bottom right, there are 'OK' and 'Cancel' buttons.

**Figure13-4 The First Mail Relay Setting WebUI**

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

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting (Figure13-5)

The screenshot shows the same web interface as Figure 13-4, but with the 'Allowed External IP of Mail Relay' radio button selected. The 'Add IP Address' section now contains two input fields: 'IP Address' with the value '61.11.11.11' and 'Netmask' with the value '255.255.255.255'. The 'OK' and 'Cancel' buttons are still at the bottom right.

**Figure13-5 The Second Mail Relay Setting WebUI**

**The Headquarters setup ALL7008 as Gateway (Mail Server is in DMZ, Transparent Mode) to make the Branch Company's employees can send mails via Headquarters' Mail Server**

### **Preparation**

WAN Port IP of ALL7008: 61.11.11.11

Mail Server IP: 61.11.11.12

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

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

When the branch company's users send mail to the external mail server's recipient account by mail server's sender account of broadband.com.tw, add the following Mail Relay setting:



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

- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to (Figure13-6)

The screenshot shows a web interface for configuring mail relay. At the top, there are two radio buttons: 'Domain Name of Internal Mail Server' (which is selected) and 'Allowed External IP of Mail Relay'. Below this, there is a section titled 'Add Domain Name' in blue text. Under this section, there are two input fields: 'Domain Name of Mail Server' with the value 'broadband.com.tw' and 'IP Address of Mail Server' with the value '61.11.11.12'. At the bottom right, there are 'OK' and 'Cancel' buttons.

**Figure13-6 The First Mail Relay Setting WebUI**

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

- Select **Allowed External IP of Mail Relay**
- **IP Address:** Enter the IP Address of external sender
- Enter the **Netmask**
- Complete Mail Relay setting (Figure13-7)

The screenshot shows the same web interface as Figure 13-6, but with the 'Allowed External IP of Mail Relay' radio button selected. The 'Add IP Address' section is now active, showing two input fields: 'IP Address' with the value '211.22.22.22' and 'Netmask' with the value '255.255.255.255'. The 'OK' and 'Cancel' buttons are still at the bottom right.

**Figure13-7 The Second Mail Relay Setting WebUI**

## Chapter 14

# Anti-Spam

ALL7008 can filter the e-mails that are going to send to the mail server of enterprise. In order to make sure the e-mail account that communicates with outside won't receive a mass advertisement or Spam mail, meanwhile, it can reduce the burden of mail server. Also can prevent the users to pick up the message he/she needs from a mass of useless mails; or delete the needed mail mistakenly while deleting mails. It will raise the work efficiency of the employees and will not lose the important information of enterprise.

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

## **Define the required fields of Setting:**

### **Spam Setting:**

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

## Action of Spam Mail:

- The mail that considered as spam mail can be coped with **Delete mail**, **Deliver to the recipient**, **Forward to** another mail account
  - ◆ After setup the relevant settings in **Mail Relay** function of **Configure**, add the following settings in this function:
    1. The Mail Server is placed in **Internal (LAN or DMZ)**
    2. **The threshold score**: Enter 5
    3. **Add the message to the subject line**: Enter ---spam---
    4. Select **Add score tag to the subject line**
    5. Select **Deliver to the recipient**
    6. Click **OK** (Figure14-1)

The screenshot displays the 'Spam Setting' web interface. The top section, 'Spam Setting', includes a header bar and a list of configuration options. The 'Enable Anti-Spam' checkbox is checked. Under 'The Mail Server is', 'Internal (LAN or DMZ)' is selected. 'The threshold score of spam mail is' is set to 5. 'Add the spam string to the subject line' is set to ---spam---. Several optional features are listed with checkboxes: 'Check spam fingerprint', 'Enable Bayesian filtering', 'Enable spam signature push update', 'Verify sender account is valid', and 'Check sender IP address in RBL' are all unchecked, while 'Add score tag to the subject line' is checked. The bottom section, 'Action of Spam Mail', is divided into 'Internal Mail Server' and 'External Mail Server'. Under 'Internal Mail Server', 'Deliver to the recipient' is checked, and 'Forward to' is empty. Under 'External Mail Server', 'Deliver to the recipient' is checked. The interface concludes with 'OK' and 'Cancel' buttons.

**Spam Setting**

☒ Enable Anti-Spam

The Mail Server is ☒ Internal (LAN or DMZ) ☐ External (WAN)

The threshold score of spam mail is

Add the spam string to the subject line  (Max. 256 characters)

☐ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)

☐ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)

☐ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)

☐ Verify sender account is valid

☐ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)

☒ Add score tag to the subject line

**Action of Spam Mail**

Internal Mail Server:

☐ Delete the spam mail

☒ Deliver to the recipient

☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com )

External Mail Server:

☒ Deliver to the recipient (Always enable)

OK Cancel

Figure14-1 Anti-Spam Setting WebUI

- ◆ When receive Spam mail, it will add **score tag** and **message** in front of the subject of the E-mail. (Figure14-2)

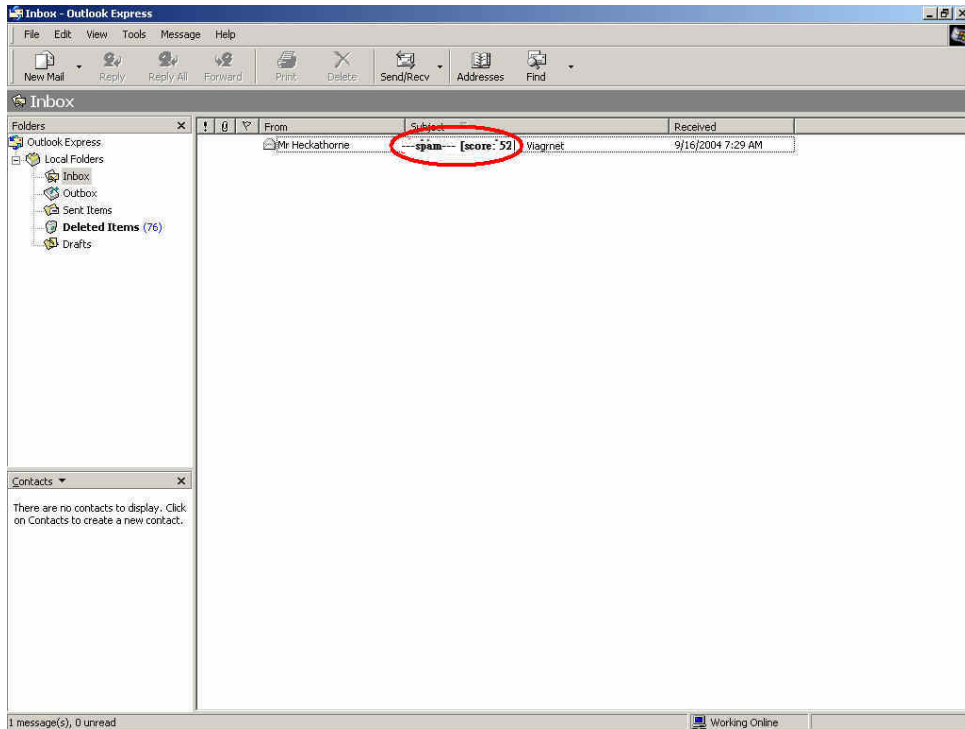


Figure14-2 the subject of the mail that considered as spam mail WebUI

- ◆ When receive Ham mail, it will only add **score tag** in front of the e-mail's subject (Figure14-3)

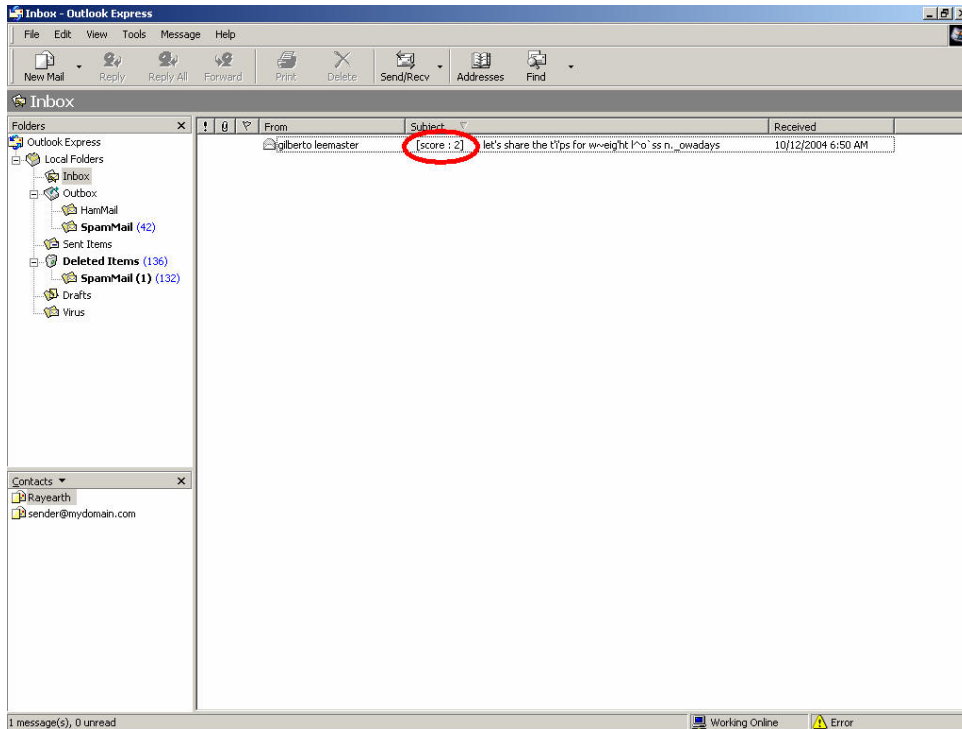


Figure14-3 the subject of the mail that considered as Spam mail WebUI

## Define the required fields of Rule

### Rule Name:

- The name of the custom spam mail determination rule

### Comment:

- To explain the meaning of the custom rule

### Combination:

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

### Classification:

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

### Action:

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

### Auto-Training:

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

### Item:

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

### Condition:

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

### Pattern:

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



## Define the required fields of Whitelist

### Whitelist:

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

### Direction:

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

## Define the required fields of Blacklist

### Blacklist:

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

## Define the required fields of Training

### Training Database:

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

### Spam Mail for Training:

- The System Manager can import the file which is not determined as spam mail here. To raise the judgment rate of spam mail after the ALL7008 learning the file.

### Ham Mail for Training:

- The System Manager can import the file which is determined as spam mail here. To raise the judgment rate of ham mail after the ALL7008 learning the file

### Training time:

- The System Manager can set the training time for ALL7008 to learn the import file each day here.

## Define the required fields of Spam Mail

### Top Total Spam:

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



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



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

**Advance Instruction:**

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

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

## The flow of delivering e-mail:

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

- **MUA (Mail User Agent):** The PC of client cannot send mail directly. It must deliver mail by MUA. No matter to send or to receive the mail, the Client user still has to use mail system by MUA that provided by operation system. For example: Outlook Express in Windows is MUA. The main function of MUA is to receive or send e-mail from mail master and provide the function for users to browse and edit mail
- **MTA (Mail Transfer Agent):** When the user sending or receiving mails, they are both completed by MTA. Basically, its functions are as below:
  1. To receive the mail that sent by external master: when receiving the mails from external; only if the recipient exists in MTA internal account then this mail will be received by MTA.
  2. To send mail for user: Only if the user has the authority to use MTA, and then the mail can be sent by MTA.
  3. To let user to receive his/her own mail: The user can take the mails to his/her own PC from mail master.



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

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

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

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

- Use MUA to send mail to MTA: Enter the following setting while the user write e-mail by MUA:
  1. The e-mail address and the mail server of the sender (To receive the MTA that sent by MTA from the sender)
  2. The e-mail address and the mail server of the recipient (To receive the MTA that sent from the external master)

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

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

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

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



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

1. Sending e-mail: It is a function of the process of sending the mail from MUA to MTA, and transfer mail from MTA to the next MTA. At present, most of the mail server uses SMTP Protocol (Simple Mail Transfer Protocol), and the Port Number is 25.
2. Receiving e-mail: MUA connect to MTA user's Mailbox by POP (Post Office Protocol) in order to read or download the mail in user's mailbox. At present, common POP Protocol is POP3 (Post Office Protocol version 3), and the Port Number is 110.



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



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



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



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

We set up four Anti-Spam examples in this chapter:

No.	Example	Page
Ex 1	To detect if the mail from External Mail Server is spam mail or not	<b>324</b>
Ex 2	Take ALL7008 as Gateway and use Whitelist and Blacklist to filter the mail. (Mail Server is in DMZ and use Transparent Mode)	<b>328</b>
Ex 3	Place ALL7008 between the original Gateway and Mail Server to set up the Rule to filter the mail. (Mail Server is in DMZ and use Transparent Mode)	<b>335</b>
Ex 4	Use Training function of ALL7008 to make the mail be determined as spam mail or ham mail after training. (Take Outlook Express for example)	<b>341</b>



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

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

**STEP 2** . In **LAN** of **Address** function, add the following settings: (Figure14-4)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Josh	192.168.139.12/255.255.255.255		Modify Remove

New Entry

Figure14-4 Mapped IP of Internal User's PC in Address Book

**STEP 3** . Add the following setting in **Group** of **Service**. (Figure14-5)

Group name	Service	Configure
Mail_Service	DNS,POP3,SMTP	Modify Remove

New Entry

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

**STEP 4** . Add the following setting in **Outgoing Policy**: (Figure14-6)

Source	Destination	Service	Action	Option					Configure	Move
Josh	Outside_Any	Mail_Service	✓						Modify Remove	To 1

New Entry

Figure14-6 Outgoing Policy Setting

**STEP 5 .** Add the following setting in **Setting** of **Anti-Spam** function:  
(Figure14-7)

The screenshot shows a configuration window titled "Spam Setting" with a light blue header. The "Spam Setting" section includes a checked checkbox for "Enable Anti-Spam". Below it, "The Mail Server is" is set to "External (VLAN)" with a checked checkbox, while "Internal (LAN or DMZ)" is unchecked. "The threshold score of spam mail is" is set to "5" in a dropdown menu. "Add the spam string to the subject line" has a text input field containing "---spam---" with a "(Max. 256 characters)" note. Below these are several checkboxes: "Check spam fingerprint" (checked, with a "Test" link), "Enable Bayesian filtering" (checked, with a note about database requirements), "Enable spam signature push update" (unchecked, with a "Test" link), "Verify sender account is valid" (unchecked), "Check sender IP address in RBL" (unchecked, with a "Test" link), and "Add score tag to the subject line" (unchecked). The "Action of Spam Mail" section has a light blue header and is divided into "Internal Mail Server:" and "External Mail Server:". Under "Internal Mail Server:", there are three options: "Delete the spam mail" (unchecked), "Deliver to the recipient" (unchecked), and "Forward to:" (unchecked, with a text input field and a "(Max. 128 characters, ex: user@mydomain.com)" note). Under "External Mail Server:", "Deliver to the recipient" is checked with a note "(Always enable)". At the bottom right are "OK" and "Cancel" buttons.

**Spam Setting**

☒ Enable Anti-Spam

The Mail Server is ☐ Internal (LAN or DMZ) ☒ External (VLAN)

The threshold score of spam mail is **5**

Add the spam string to the subject line  (Max. 256 characters)

☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)

☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)

☐ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)

☐ Verify sender account is valid

☐ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)

☐ Add score tag to the subject line

**Action of Spam Mail**

Internal Mail Server:

☐ Delete the spam mail

☐ Deliver to the recipient

☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com )

External Mail Server:

☒ Deliver to the recipient (Always enable)

OK Cancel

**Figure14-7 Action of Spam Mail and Spam Setting**



**Anti-Spam** function is enabled in default status. So the System Manager does not need to set up the additional setting and then the ALL7008 will filter the spam mail according to the mails that sent to the internal mail server or received from external mail server. (Figure14-8)

**Spam Setting**

☒ Enable Anti-Spam

The Mail Server is

☒ Internal (LAN or DMZ)

☒ External (WAN)

The threshold score of spam mail is

Add the spam string to the subject line  (Max. 256 characters)

☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)

☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)

☐ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)

☐ Verify sender account is valid

☐ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)

☐ Add score tag to the subject line

**Action of Spam Mail**

Internal Mail Server:

☐ Delete the spam mail

☒ Deliver to the recipient

☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com )

External Mail Server:

☒ Deliver to the recipient (Always enable)

OK Cancel

**Figure14-8 Default Value of Spam Setting**



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

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

**STEP 6 .** When the internal users are receiving the mail from external mail account (js1720@ms21.pchome.com.tw), the ALL7008 will filter the mail at the same time and the chart will be in the **Spam Mail** in **Anti-Spam** function. (At this time, choose **External** to see the mail account chart) (Figure14-9)

Top Total Spam: 1-1

Internal External

No.	Recipient	Total Spam	Total Mail	Duration	Spam %
1	js1720@ms21.pchome.com.tw	1	2	00H	50.0%
Total		1	2		50.0%

Clear Data

Figure14-9 Report Function Chart



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

## Take ALL7008 as Gateway and use Whitelist and Blacklist to filter the mail. (Mail Server is in DMZ and use Transparent Mode)

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

**STEP 2** . Enter the following setting in **DMZ** of **Address** function: (Figure14-10)

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Mail_Server	61.11.11.12/255.255.255.255	00:48:54:55:E1:07	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure14-10 Mapped Name Setting in Address of Mail Server

**STEP 3** . Enter the following setting in **Group** in **Service** function: (Figure14-11)

Group name	Service	Configure
Mail_Service_01	POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Mail_Service_02	DNS,POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure14-11 Setting Service Group that include POP3, SMTP or DNS

**STEP 4** . Enter the following setting in **WAN to DMZ Policy**: (Figure14-12)

Source	Destination	Service	Action	Option			Configure		Move
Outside_Any	Mail_Server	Mail_Service_01		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	To <input type="text" value="1"/>

New Entry

Figure14-12 WAN to DMZ Policy Setting

**STEP 5 .** Enter the following setting in **DMZ to WAN Policy**: (Figure14-13)

Source	Destination	Service	Action	Option					Configure	Move
Mail_Server	Outside_Any	Mail_Service_02	1						Modify Remove	To 1
New Entry										

**Figure14-13 DMZ to WAN Policy Setting**

**STEP 6 .** Enter the following setting in **Mail Relay** function of **Setting**: (Figure14-14)

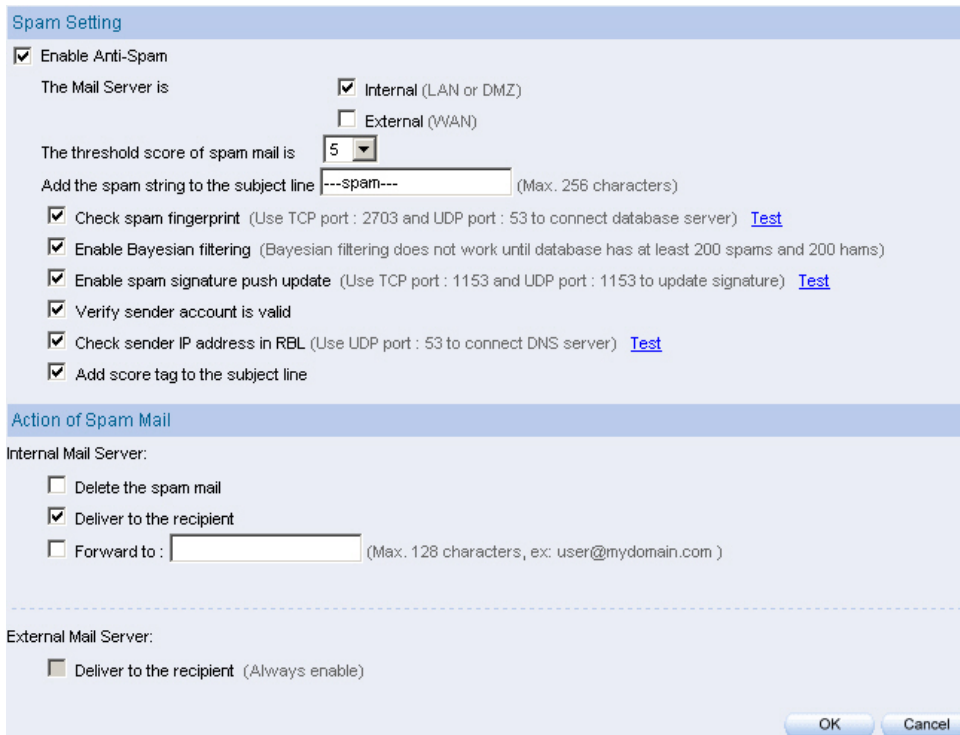
Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
broadband.com.tw ( 61.11.11.12 )	Modify Remove
New Entry	

**Figure14-14 Mail Relay Setting of External Mail to Internal Mail Server**



**Mail Relay** function makes the mails that sent to DMZ's mail server could be relayed to its mapped mail server by ALL7008

**STEP 7 .** Enter the following setting in **Setting** function of **Anti-Spam:**  
(Figure14-15)



The screenshot shows a configuration window titled "Spam Setting" with two main sections: "Spam Setting" and "Action of Spam Mail".

**Spam Setting**

- ☒ Enable Anti-Spam
- The Mail Server is:
  - ☒ Internal (LAN or DMZ)
  - ☐ External (WAN)
- The threshold score of spam mail is:
- Add the spam string to the subject line:  (Max. 256 characters)
- ☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)
- ☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)
- ☒ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)
- ☒ Verify sender account is valid
- ☒ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)
- ☒ Add score tag to the subject line

**Action of Spam Mail**

Internal Mail Server:

- ☐ Delete the spam mail
- ☒ Deliver to the recipient
- ☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com )

External Mail Server:

- ☐ Deliver to the recipient (Always enable)

Buttons: OK, Cancel

**Figure14-15 Spam Setting and Action of Spam Mail**



When select **Delete mail** in **Action of Spam Mail**, and then the other functions (**Deliver to the recipient**, or **Forward to**) cannot be selected. So when ALL7008 had scanned spam mail, it will delete it directly. But still can check the relevant chart in **Spam Mail** function.



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

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

- Click **New Entry**
- **Whitelist:** Enter share2k01@yahoo.com.tw
- **Direction:** Select From
- Enable **Auto-Training**
- Click **OK** (Figure14-16)
- Enter **New Entry** again
- **Whitelist:** Enter josh@broadband.com.tw
- **Direction:** Select To
- Enable **Auto-Training**
- Click **OK** (Figure14-17)
- Complete setting (Figure14-18)

Add Whitelist	
Mail Account	share2k01@yahoo.com.tw
Direction	From ▼
Auto-Training	Enable ▼
<div>OK Cancel</div>	

**Figure14-16 Add Whitelist Setting 1**

Add Whitelist	
Mail Account	josh@broadband.com.tw
Direction	To ▼
Auto-Training	Enable ▼
<div>OK Cancel</div>	

**Figure14-17 Add Whitelist Setting 2**



Export Whitelist To Client

Import Whitelist From Client    (Max size 100 KBytes)

Direction	Mail Account	Auto-Training	Configure
From	share2k01@yahoo.com.tw	✓	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
To	josh@broadband.com.tw	✓	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

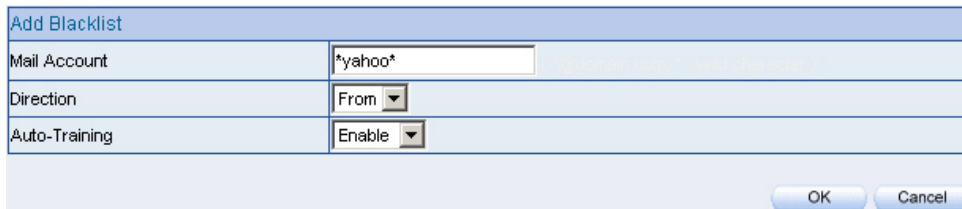
**Figure14-18 Complete Whitelist Setting**



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

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

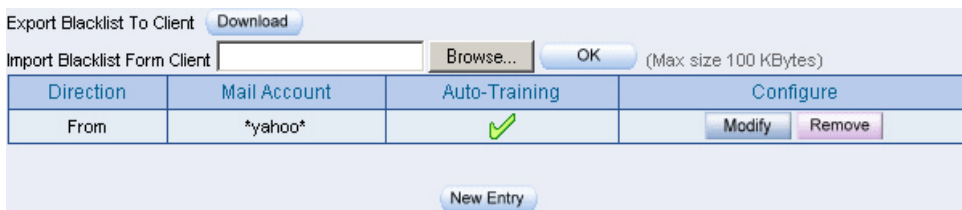
- Enter **New Entry**
- **Blacklist:** Enter \*yahoo\*
- **Direction:** Select From
- Enable **Auto-Training**
- Click **OK** (Figure14-19)
- Complete the Setting (Figure14-20)



The dialog box titled "Add Blacklist" contains three rows of settings. The first row is "Mail Account" with a text input field containing "\*yahoo\*". The second row is "Direction" with a dropdown menu set to "From". The third row is "Auto-Training" with a dropdown menu set to "Enable". At the bottom right are "OK" and "Cancel" buttons.

Add Blacklist	
Mail Account	*yahoo*
Direction	From
Auto-Training	Enable

**Figure14-19 Add Blacklist Setting**



The window shows the "Export Blacklist To Client" section with a "Download" button. Below it is the "Import Blacklist Form Client" section with a text input field, a "Browse..." button, and an "OK" button. A note "(Max size 100 KBytes)" is next to the "OK" button. Below this is a table with four columns: "Direction", "Mail Account", "Auto-Training", and "Configure". The table has one row with "From", "\*yahoo\*", a green checkmark, and "Modify" and "Remove" buttons. At the bottom is a "New Entry" button.

Direction	Mail Account	Auto-Training	Configure
From	*yahoo*	✓	Modify Remove

**Figure14-20 Complete Blacklist Setting**



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



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



The privilege of **Whitelist** is greater than **Blacklist**. So when ALL7008 is filtering the spam mail, it will adopt the standard of **Whitelist** first and then adopt **Blacklist** next.

**STEP 10 .** When the external yahoo mail account send mail to the recipient account of mail server of broadband.com.tw in ALL7008; josh@broadband.com.tw and steve@broadband.com.tw

- If the sender account is share2k01@yahoo.com.tw, then these two recipient accounts both will receive the mail that sent by this sender account.
- If it comes from other yahoo sender account (share2k003@yahoo.com.tw), and then there will only be josh@broadband.com.tw can receive the mail that sent from this sender account; the mail that sent to steve@broadband.com.tw will be considered as spam mail.
- After ALL7008 had filtered the mail above, it will bring the chart as follows in the **Spam Mail** function of **Anti-Spam**. (Figure14-21)

Top Total Spam: 1-1 ▼

No.	Recipient ▼	Total Spam ▼	Total Mail ▼	Duration	Spam %
1	steve@broadband.com.tw	1	2	00H	50.0%
2	josh@broadband.com.tw	0	2	00H	0.0%
總計		1	4		25.0%

Clear Data

**Figure14-21 Chart of Report Function**



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

**Place ALL7008 between the original Gateway and Mail Server to set up the Rule to filter the mail. (Mail Server is in DMZ, Transparent Mode)**

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

The WAN IP of ALL7008: 172.16.1.12

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

**STEP 2** . Enter the following setting in **DMZ Address Book**: (Figure14-22)

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Mail_Server	172.16.1.13/255.255.255.255	00:48:54:55:E1:07	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure14-22 Mapped IP Setting of Mail Server in Address Book

**STEP 3** . Enter the following setting in **Service Group**. (Figure14-23)

Group name	Service	Configure
Mail_Service_01	POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Mail_Service_02	DNS,POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure14-23 Setting Service Group includes POP3, SMTP or DNS

**STEP 4 .** Enter the following setting in **WAN to DMZ Policy**: (Figure14-24)

Source	Destination	Service	Action	Option				Configure		Move
Outside_Any	Mail_Server	Mail_Service_01	✓					Modify	Remove	To 1 ▾
New Entry										

Figure14-24 WAN to DMZ Policy Setting

**STEP 5 .** Enter the following setting in **DMZ to WAN Policy**: (Figure14-25)

Source	Destination	Service	Action	Option				Configure		Move
Mail_Server	Outside_Any	Mail_Service_02	1					Modify	Remove	To 1 ▾
New Entry										

Figure14-25 DMZ to WAN Policy Setting

**STEP 6 .** Add the following setting in **Mail Relay** in **Configure**: (Figure14-26)

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
broadband.com.tw ( 172.16.1.13 )	Modify Remove
New Entry	

Figure14-26 Mail Relay Setting of External Mail to Internal Mail Server

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

- Enter **New Entry**
- **Rule Name:** Enter HamMail
- **Comments:** Enter Ham Mail
- **Combination:** Select Or
- **Classification:** Select Ham (Non-Spam)
- Enable **Auto-Training**
- In the first field **Item:** Select From; **Condition:** Select Contains;  
**Pattern:** share2k01
- Click **Next Row**
- In the second **Item** field: Select To; **Condition:** Select Contains;  
**Pattern:** josh (Figure14-27)
- Press **OK** (Figure14-28)

Rule Name :	HamMail	(Max. 16 characters)	Comments :	Ham Mail	(Max. 20 characters)
Combination :	Or		Classification :	Ham(Non-Spam)	
Auto-Training :	Enable		Action :	Delete spam mail	(Max. 128 characters)
Item	Condition	Pattern (Max. 30 characters)	Configure		
From	Contains	share2k01	Remove		
To	Contains	josh	Next Row Remove		
OK Cancel					

**Figure14-27 The First Rule Item Setting**

Rule Name	Classification	Action	Comments	Configure	Move
HamMail	Ham	---	Ham Mail	Modify Remove	To 1
New Entry					

**Figure14-28 Complete First Rule Setting**



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

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

- Enter **New Entry**
- **Rule Name:** Enter SpamMail
- **Comments:** Enter Spam Mail
- **Combination:** Select And
- **Classification:** Select Spam
- **Action:** Select Deliver to the recipient
- Enable **Auto-Training**
- **Item:** Select From; **Condition:** Select Contains; **Pattern:** yahoo (Figure14-29)
- Press **OK** (Figure14-30)

Rule Name :	SpamMail (Max. 16 characters)	Comments :	Spam Mail (Max. 20 characters)
Combination :	And	Classification :	Spam
Auto-Training :	Enable	Action :	Delete spam mail
Item	Condition	Pattern (Max. 30 characters)	Configure
From	Contains	yahoo	Next Row
OK Cancel			

**Figure14-29 The Second Rule Setting**

Rule Name	Classification	Action	Comments	Configure	Move
HamMail	Ham	---	Ham Mail	Modify Remove	To 1
SpamMail	Spam	Deliver to the recipient	Spam Mail	Modify Remove	To 2

New Entry

**Figure14-30 Complete the Second Rule Setting**



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



The privilege of **Rule** is greater than **Whitelist** and **Blacklist**. And in **Rule** function, the former rule has the greater privilege. So when the ALL7008 is filtering the spam mail, it will take **Rule** as filter standard first and then is **Whitelist**; **Blacklist** is the last one be taken.



Select one of the mails in **Outlook Express**. Press the right key of the mouse and select **Content**, and select **Details** in the pop-up page. It will show all of the headers for the message to be taken as the reference value of **Condition** and **Item** of the **Rule**. (Figure14-31)

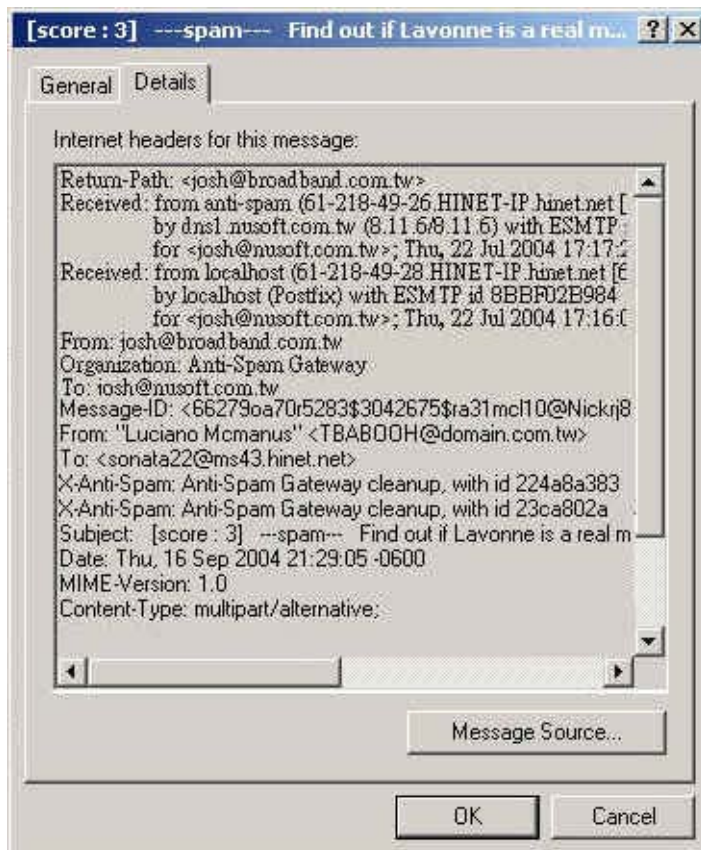


Figure14-31 The Detailed Data of the Mail



- If the sender account is share2k01@yahoo.com.tw, then these two recipient accounts both will receive the mail that sent by this sender account.
- If it comes from other yahoo sender account (share2k003@yahoo.com.tw), and then there will only be josh@broadband.com.tw can receive the mail that sent from this sender account; the mail that sent to steve@broadband.com.tw will be considered as spam mail.
- After ALL7008 had filtered the mail above, it will bring the chart as follows in the **Spam Mail** function of **Anti-Spam**.  
(Figure14-32)

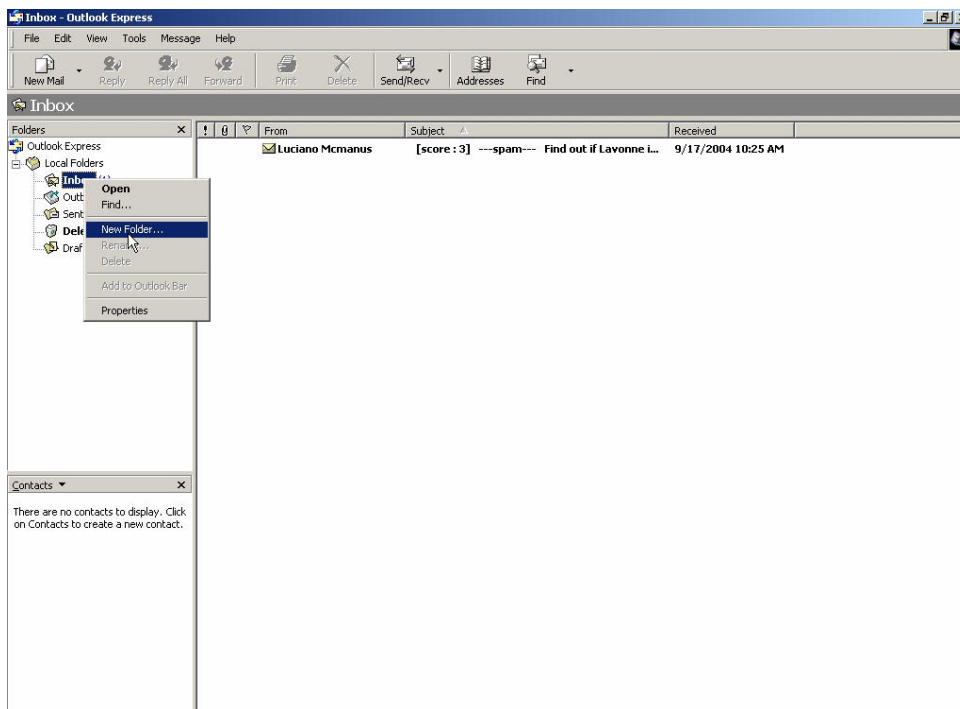
### Figure14-32 Chart of Report Function

**Use Training function of the ALL7008 to make the mail be determined as Spam mail or Ham mail after Training. (Take Outlook Express for example)**

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

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

- Press the right key of the mouse and select **New Folder**. (Figure14-33)
- In **Create Folder** WebUI and enter the Folder's Name as SpamMail, and then click on OK. (Figure14-34)



**Figure14-33 Select New Folder Function WebUI**

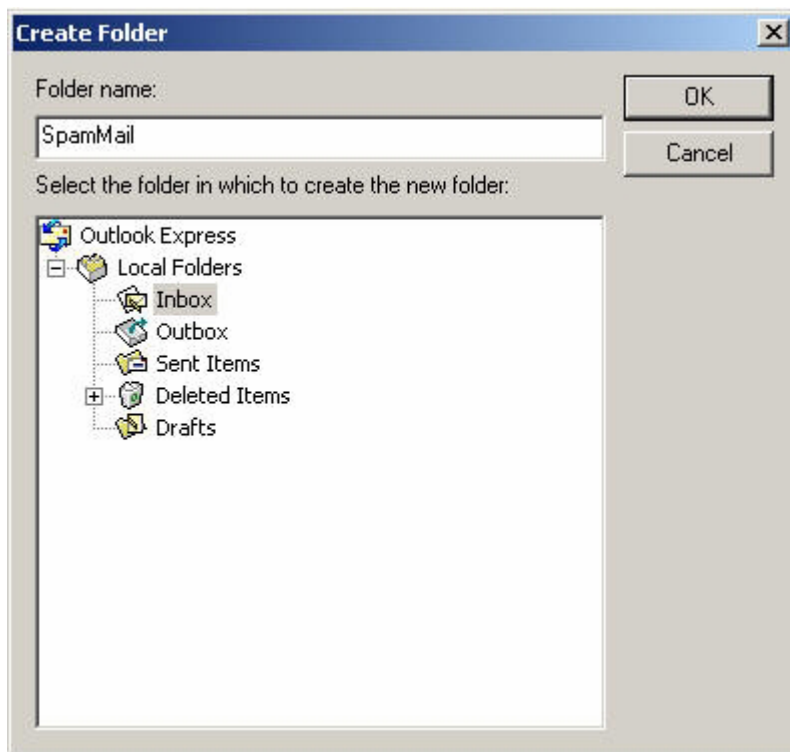


Figure14-34 Create Folder WebUI

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

- In Inbox, select all of the spam mails that do not judge correctly and press the right key of the mouse and move to the folder.  
(Figure14-35)
- In **Move** WebUI, select **SpamMail** Folder and click **OK**  
(Figure14-36)

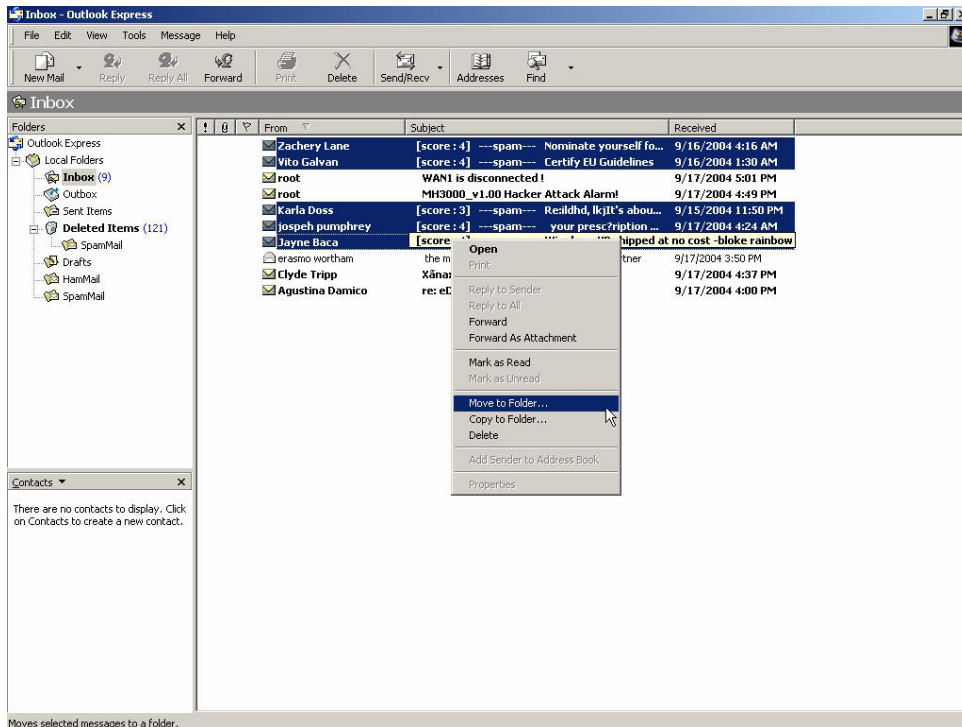


Figure14-35 Move Spam Mail WebUI

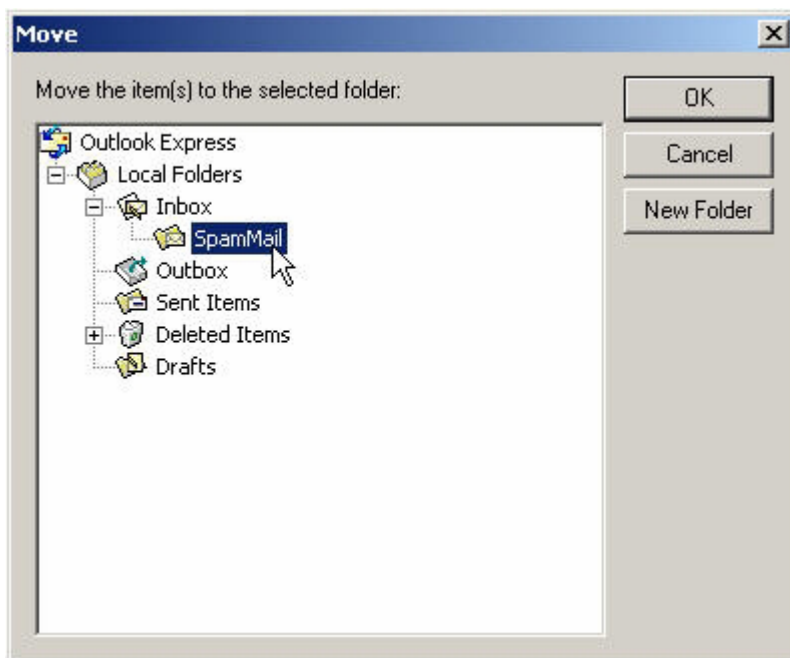
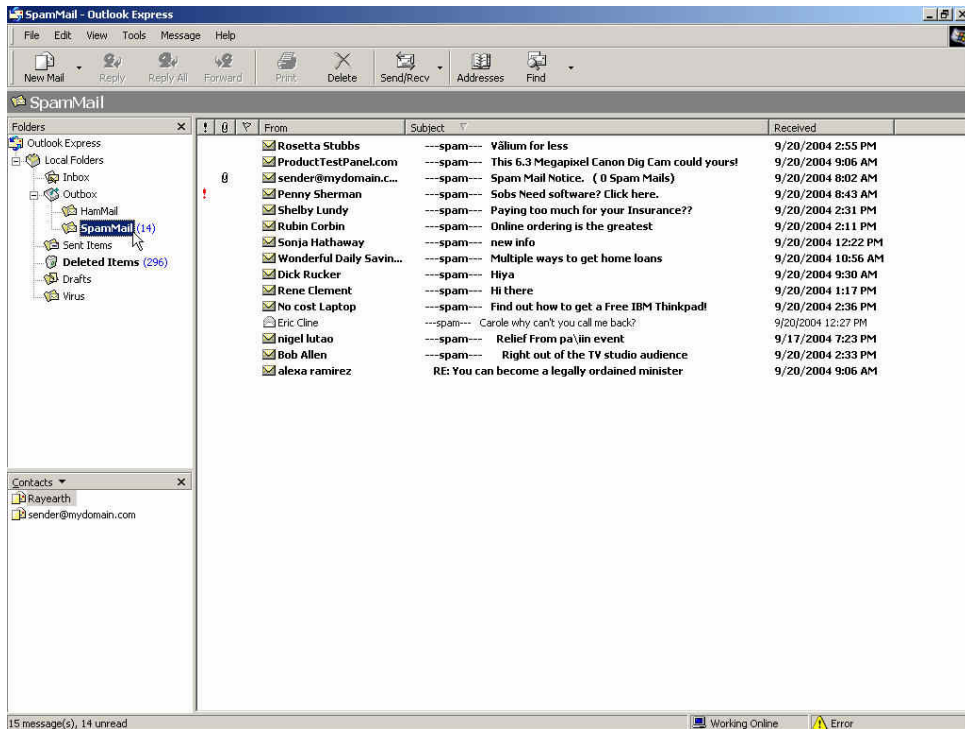


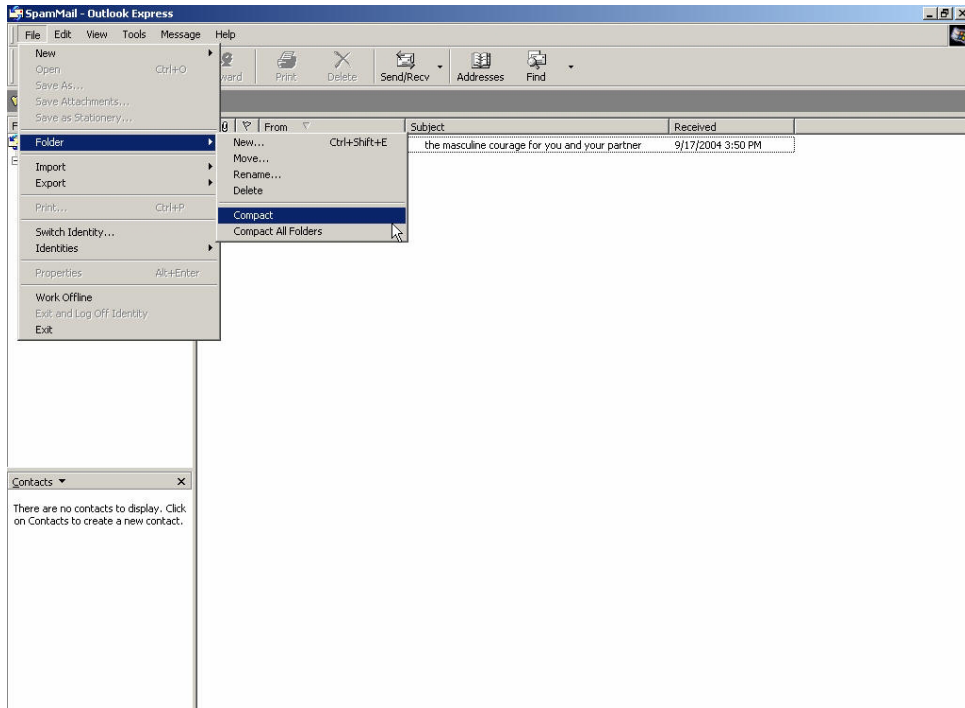
Figure14-36 Select Folder for Spam Mail to move to

**STEP 3 .** Compress the SpamMail Folder in **Outlook Express** to shorten the data and upload to ALL7008 for training:

- Select **SpamMail** Folder (Figure14-37)
- Select **Compact** function in selection of the folder (Figure14-38)



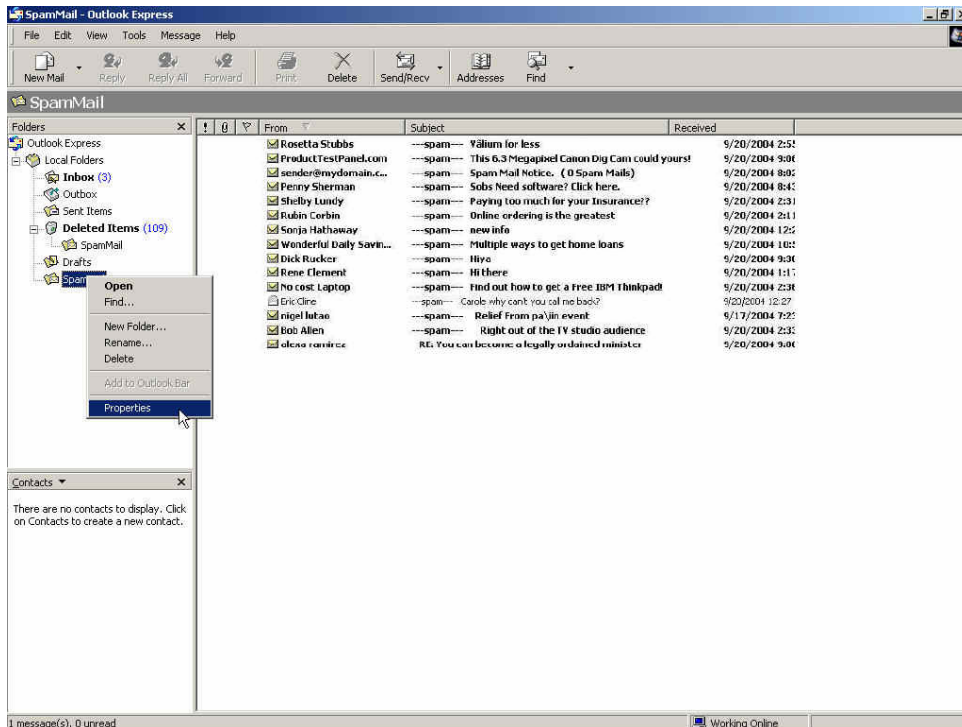
**Figure14-37 Select SpamMail Folder**



**Figure14-38 Compact SpamMail Folder**

**STEP 4 .** To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to ALL7008:

- Press the right key of the mouse in SpamMail file and select **Properties** function. (Figure14-39)
- Copy the file address in **SpamMail Properties** WebUI. (Figure14-40)



**Figure14-39 Select SpamMail File Properties Function**



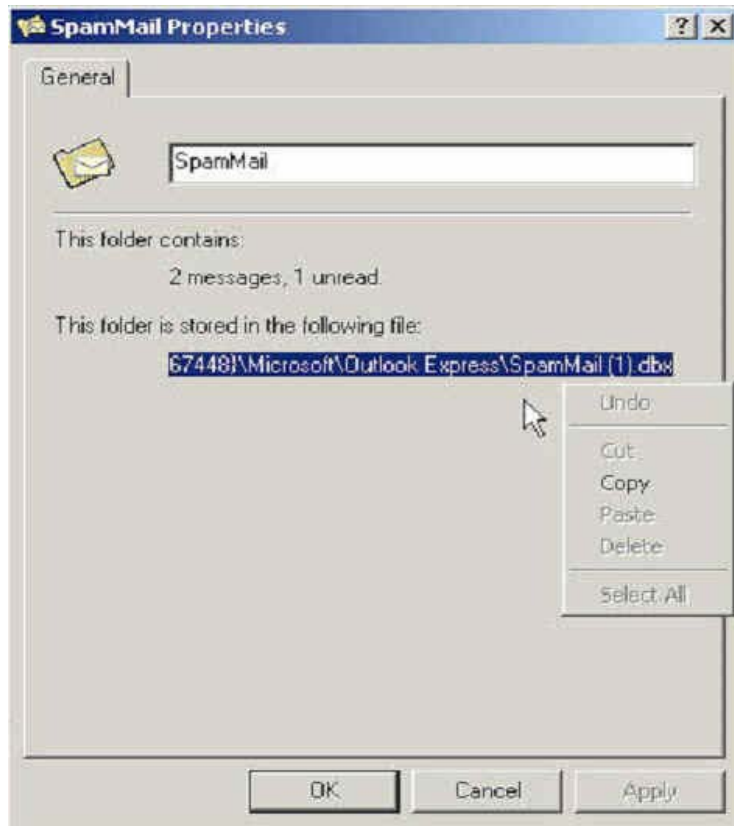


Figure14-40 Copy the File Address that SpamMail File Store

**STEP 5 .** Paste the route of copied from SpamMail file to the **Spam Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to deliver this file to ALL7008 instantly and to learn the uploaded mail file as spam mail in the appointed time. (Figure14-41)

Free space for training: 876 KBytes  
The amount of spam mail : 2083  
The amount of ham mail : 524  
Bayesian filtering works until database has at least 200 spams and 200 hams

**Training Database**  
Export Training Database   
Import Training Database    
Reset Training Database

**Spam Mail for Training**  
Import Spam Mail from Client

**Ham Mail for Training**  
Import Ham Mail from Client

**Spam Account for Training**  
POP3 Server  ( ex: my\_domain.com )  
User name  ( ex: spam )  
Password  ( ex: 5d2#k... )  
Spam account test

**Ham Account for Training**  
POP3 Server  ( ex: my\_domain.com )  
User name  ( ex: ham )  
Password  ( ex: 5d2#k... )  
Ham account test

**Training time**  
Training database starts at  / day  
Training immediately :

**Figure14-41 Paste the File Address that SpamMail File Save to make ALL7008 to be Trained**



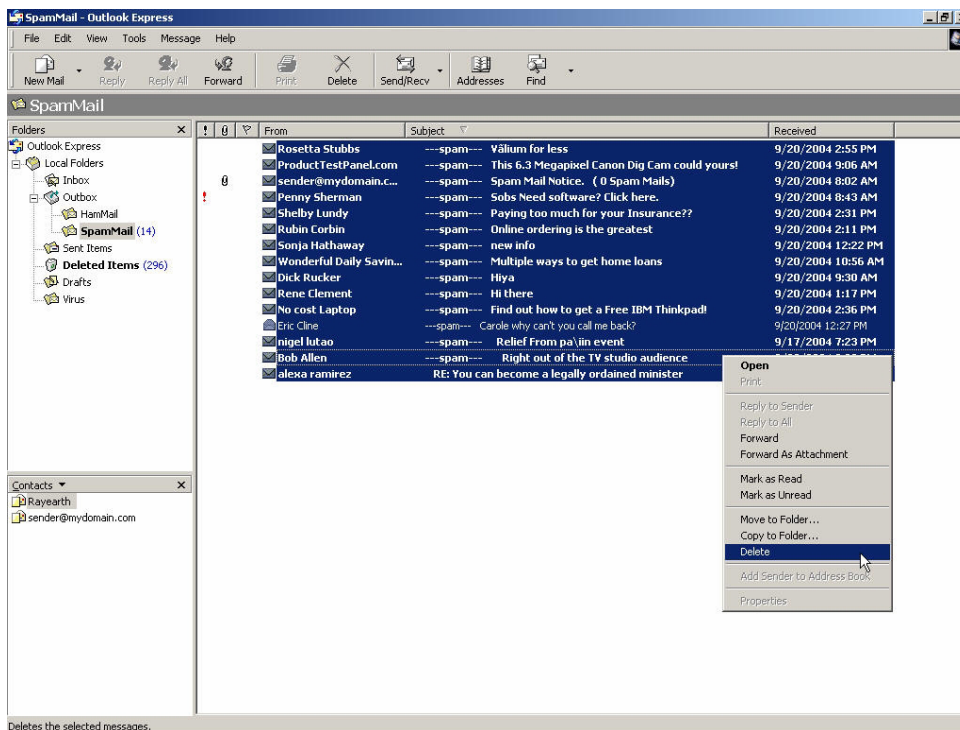
The training file that uploads to ALL7008 can be any data file and not restricted in its sub-name, but the file must be ACS11 form.



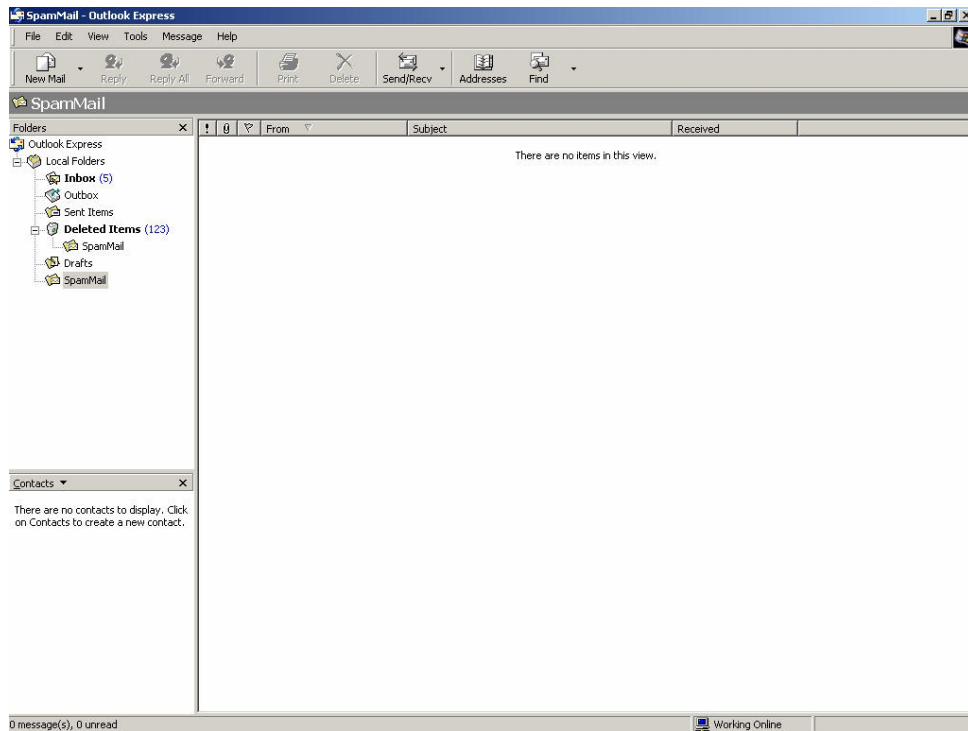
When the training file of ALL7008 is Microsoft Office Outlook exporting file [.pst], it has to close Microsoft Office Outlook first to start Importing

**STEP 6 .** Remove all of the mails in **SpamMail** File in **Outlook Express** so that new mails can be compressed and upload to ALL7008 to training directly next time.

- Select all of the mails in **SpamMail** File and press the right key of the mouse to select **Delete** function. (Figure14-42)
- Make sure that all of the mails in SpamMail file had been deleted completely. (Figure14-43)



**Figure14-42 Delete all of the mails in SpamMail File**

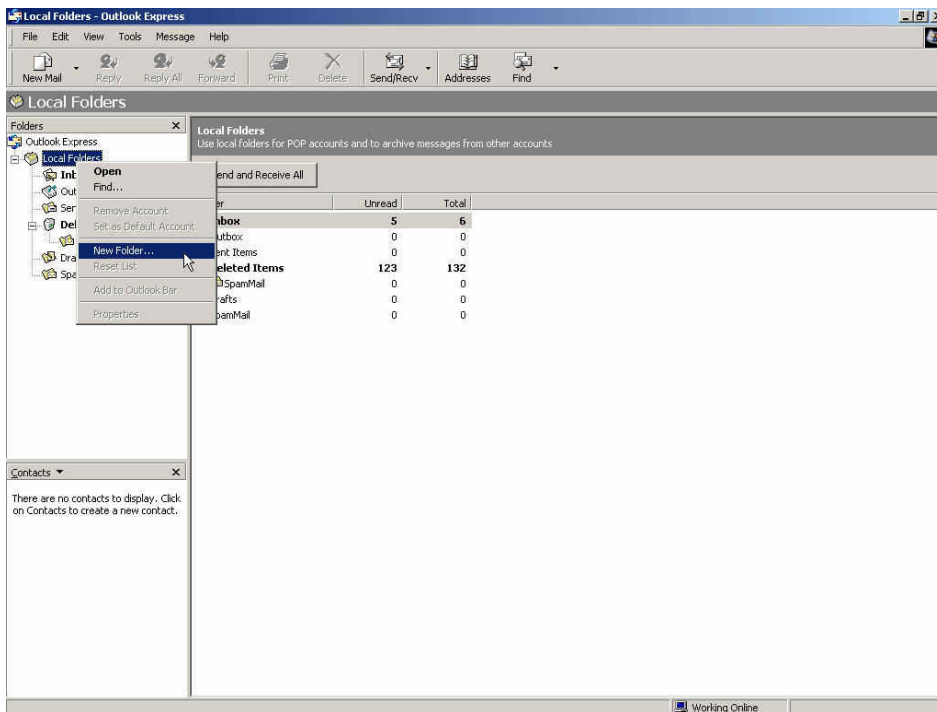


**Figure14-43 Confirm that All of the Mail in SpamMail File had been Deleted**

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

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

- Press the right key of the mouse in **Local Folders** and select **New Folder**. (Figure14-44)
- Enter HamMail in **Folder Name** in **Create Folder** WebUI and click **OK**. (Figure14-45)



**Figure14-44 Select Create New Folder Function WebUI**

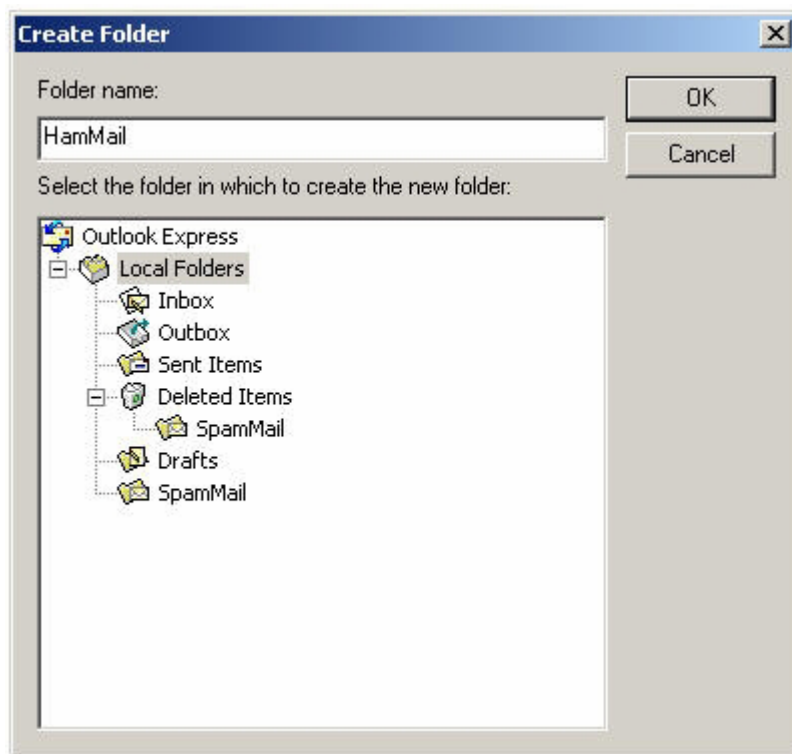


Figure14-45 Create Folder Function WebUI

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

- In Inbox, select the spam mail that all of the recipients need and press the right key of the mouse on the mail and choose **Move to Folder** function. (Figure14-46)
- Select HamMail folder in **Move WebUI** and click **OK**. (Figure14-47)

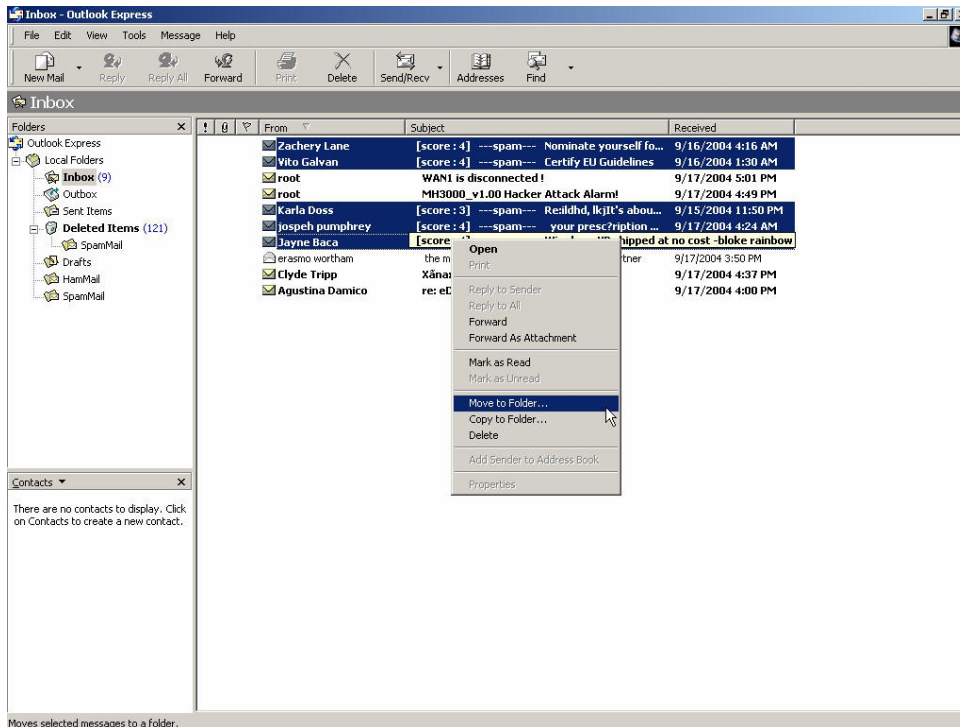
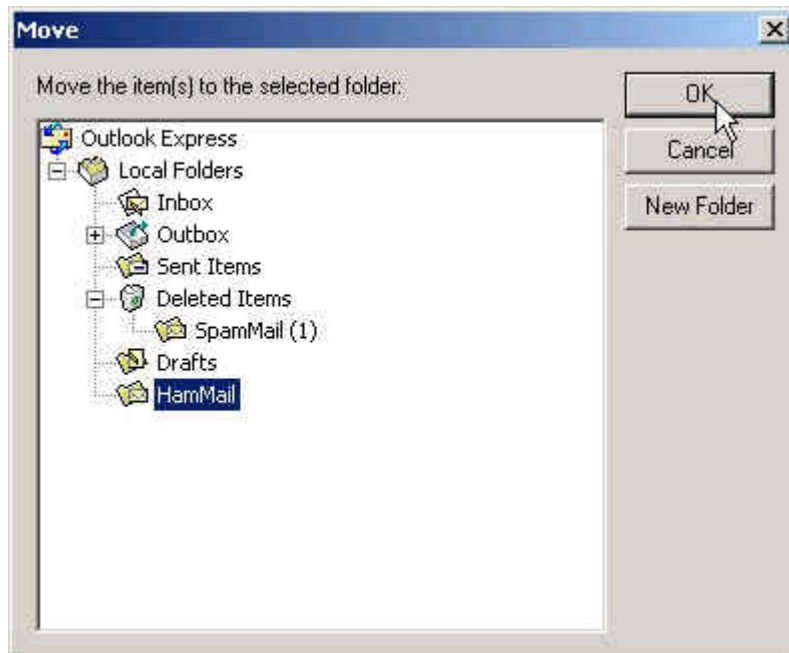


Figure14-46 Move the Needed Spam Mail WebUI

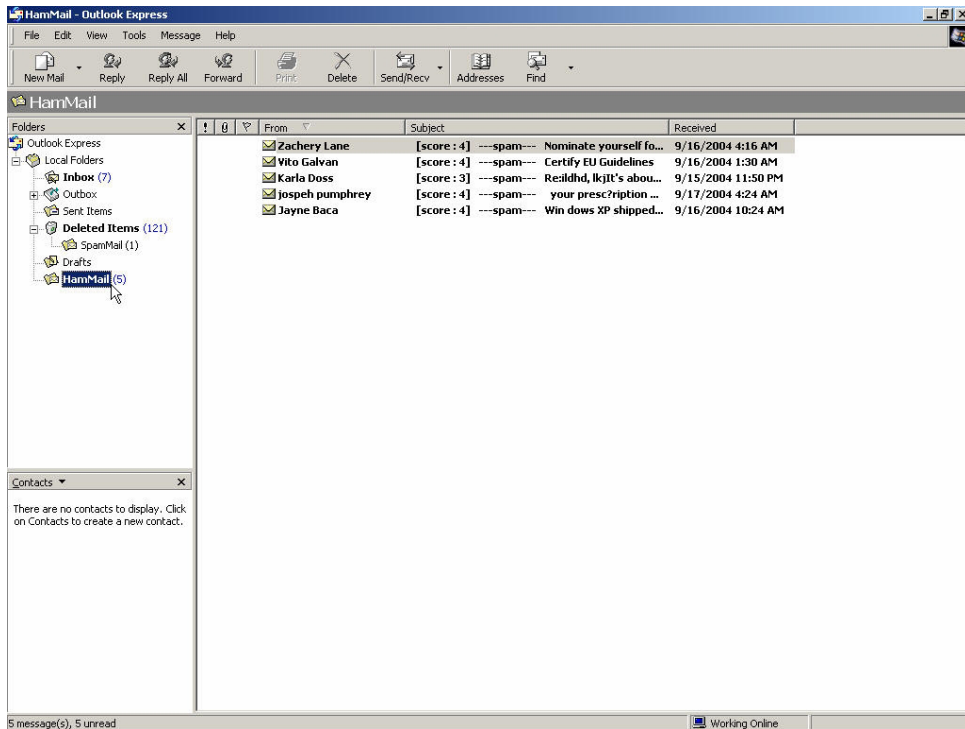




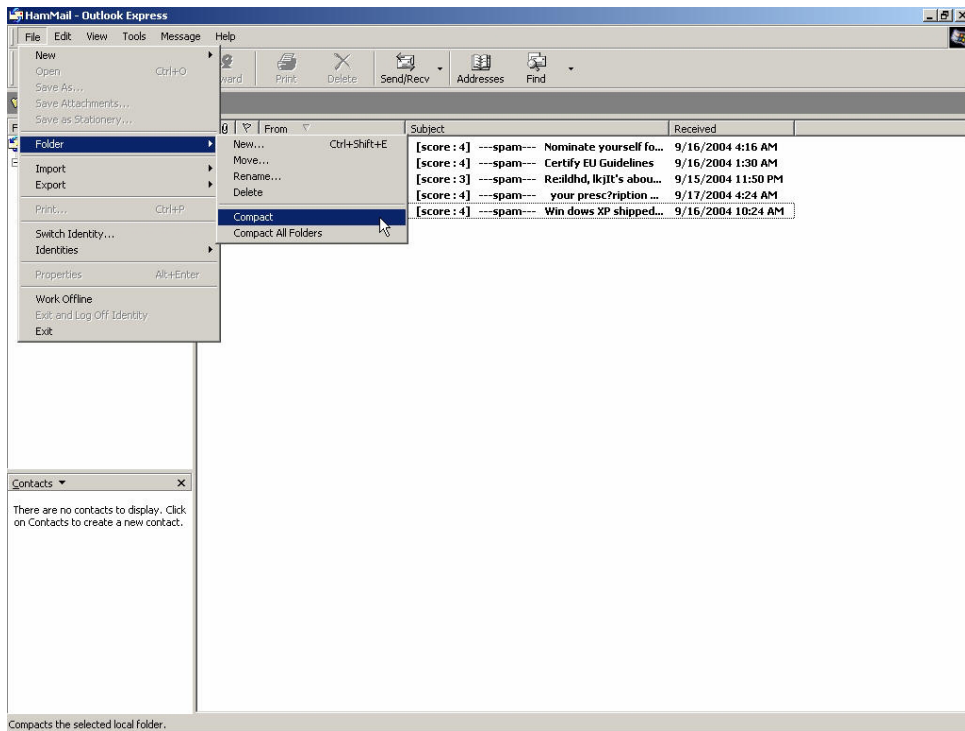
**Figure14-47 Select the Folder for Needed Spam Mail to Move to**

**STEP 3 .** Compact the HamMail folder in **Outlook Express** to shorten the data and upload to ALL7008 for training:

- Select HamMail File (Figure14-48)
- Select **Compact** function in selection of File (Figure14-49)



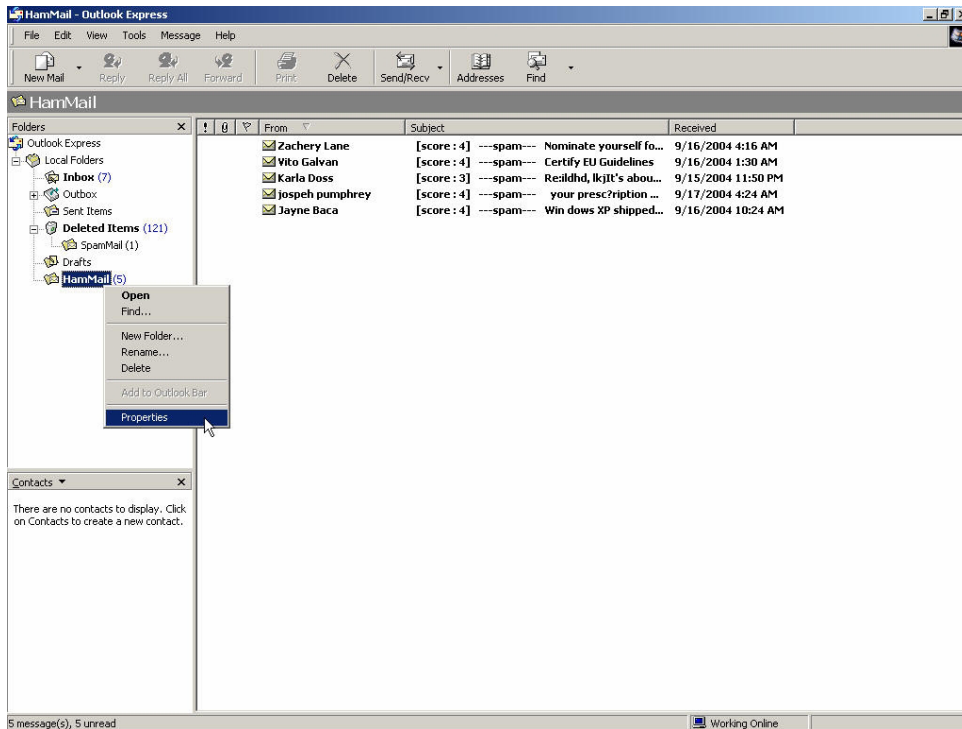
**Figure14-48 Select HamMail File**



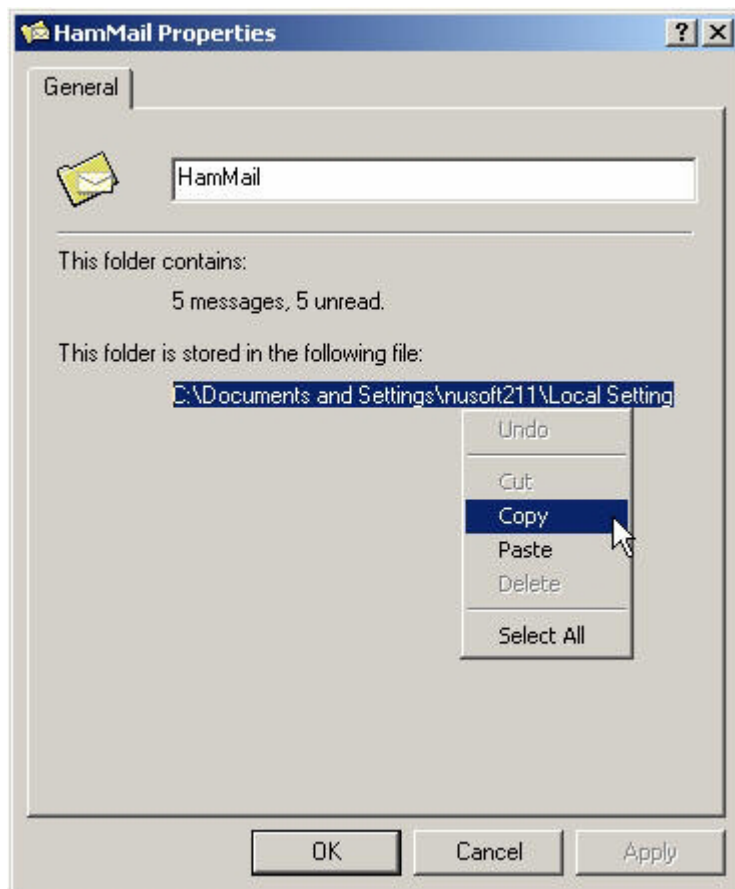
**Figure14-49 Compact HamMail File**

**STEP 4 .** To copy the route of HamMail Folder in **Outlook Express** to convenient to upload the training to ALL7008:

- Press the right key of the mouse in HamMail file and select **Properties** function. (Figure14-50)
- Copy the file address in HamMail **Properties** WebUI. (Figure14-51)



**Figure14-50 Select Properties of HamMail File WebUI**



**Figure14-51 Copy the File Address that HamMail File Store**

**STEP 5 .** Paste the route of copied HamMail file to the **Ham Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to transfer this file to the ALL7008 instantly and to learn the uploaded mail file as ham mail in the appointed time. (Figure14-52)

Free space for training: 876 KBytes  
The amount of spam mail : 2083  
The amount of ham mail : 524  
Bayesian filtering works until database has at least 200 spams and 200 hams

**Training Database**

Export Training Database

Import Training Database

Reset Training Database

**Spam Mail for Training**

Import Spam Mail from Client

**Ham Mail for Training**

Import Ham Mail from Client

**Spam Account for Training**

POP3 Server  ( ex: my\_domain.com )

User name  ( ex: spam )

Password  ( ex: 5d2#k... )

Spam account test

User name  ( ex: ham )

Password  ( ex: 5d2#k... )

Ham account test

**Training time**

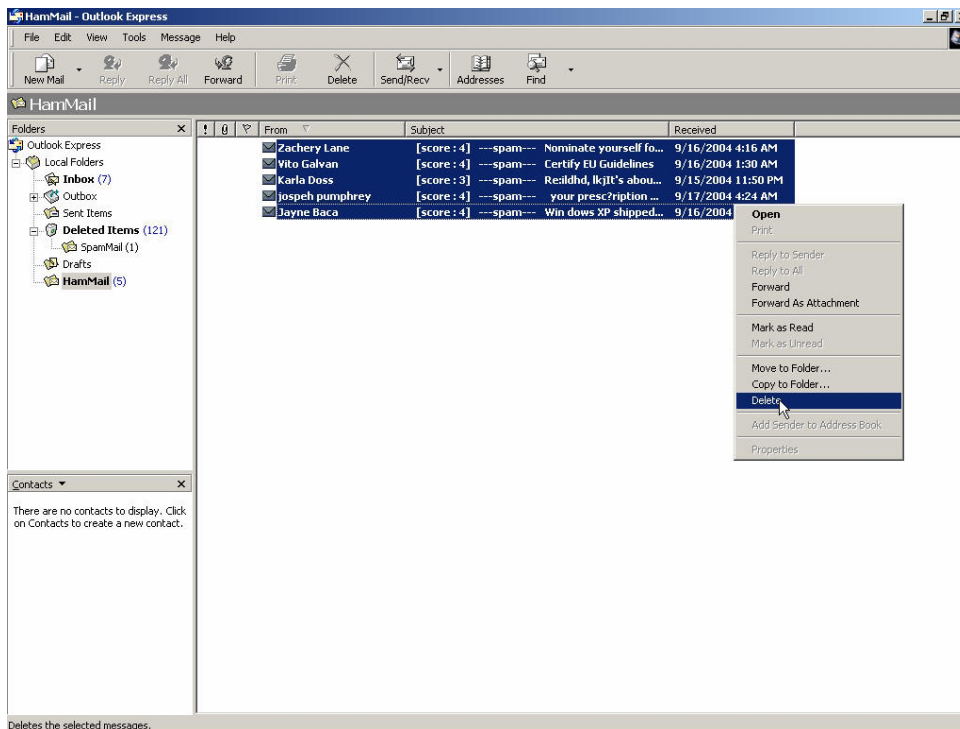
Training database starts at  / day

Training immediately :

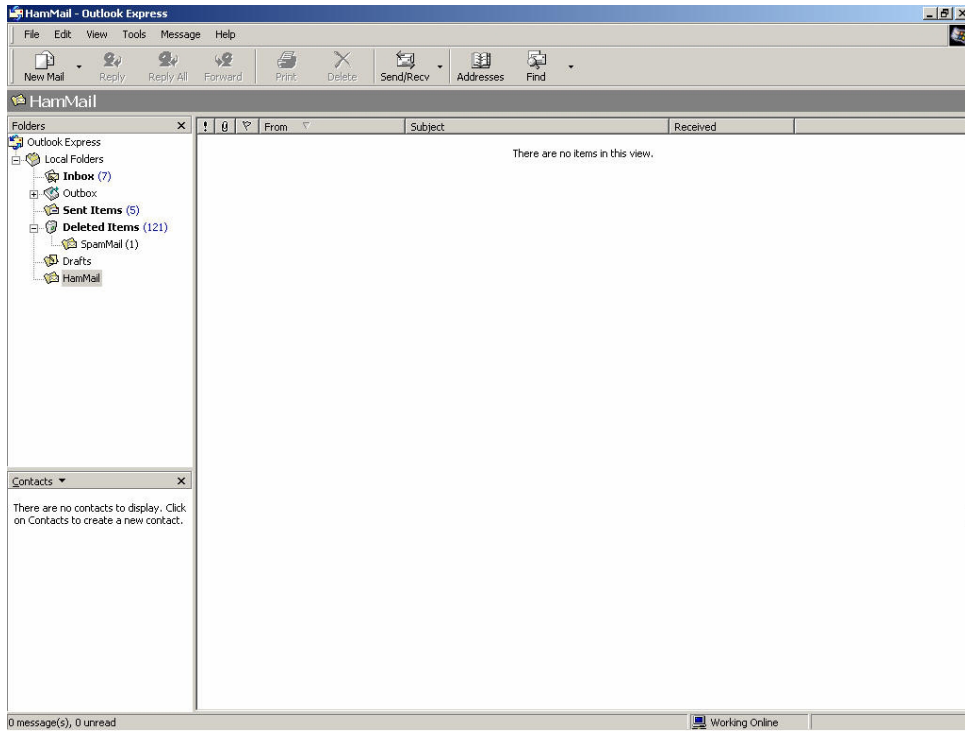
Figure14-52 Paste the File Address that HamMail File Save to make ALL7008 to be Trained

**STEP 6 .** Remove all of the mails in **HamMail** File in **Outlook Express** so that new mails can be compressed and upload to ALL7008 to training directly next time.

- Select all of the mails in **HamMail** and press the right key of the mouse to select **Delete** function. (Figure14-53)
- Make sure that all of the mails in HamMail file had been deleted completely. (Figure14-54)



**Figure14-53 Delete All of Mails in HamMail File**



**Figure14-54 Make Sure all of the Mails in HamMail File had been Deleted**





## Chapter 15

# Anti-Virus

ALL7008 can scan the mail that sent to Internal Mail Server and prevent the e-mail account of enterprise to receive mails include virus so that it will cause the internal PC be attacked by virus and lose the important message of enterprise.

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

## **Define the required fields of Setting:**

### **Anti-Virus Settings:**

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

## Action of Infected Mail:

- The mail that had been detected have virus can choose to Delete mail, Deliver to the recipient, or Forward to another mail account
- ◆ After setup the relevant settings in **Mail Relay** function of **Configure**, add the following settings in this function:
  1. **Virus Scanner:** Select Clam
  2. **The Mail Server is placed in** Internal (LAN or DMZ)
  3. **Add the message to the subject line** ---virus---
  4. Select **Remove virus mail and the attached file**
  5. Select **Deliver to the recipient**
  6. Click **OK** (Figure15-1)

The screenshot displays the 'Anti-Virus Setting' web interface. The top section, 'Anti-Virus Setting', includes a 'Virus Scan Engine' dropdown set to 'Clam', a 'The Mail Server is' section with 'Internal (LAN or DMZ)' selected, and a text field for 'Add the virus string to the subject line' containing '---virus---'. Below this, it shows the last query time, current version, and an option to update virus definitions immediately. The bottom section, 'Action of Infected Mail', is divided into 'Internal Mail Server' and 'External Mail Server' settings. In the 'Internal Mail Server' section, 'Deliver to the recipient' is selected, and 'Forward to' is empty. In the 'External Mail Server' section, 'Deliver to the recipient (Always enable)' is selected. 'OK' and 'Cancel' buttons are at the bottom right.

Anti-Virus Setting

Virus Scan Engine: Clam

The Mail Server is: ☒ Internal (LAN or DMZ) ☐ External (WAN)

Add the virus string to the subject line: ---virus--- (Max: 256 characters)

Last queried on : 2006/01/31 16:29:37 (Query virus definitions every ten minutes)

Current version : 44.4808 (Clam definitions updated at 06/01/31 16:08:34)

Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) [Update Now](#) [Test](#)

Action of Infected Mail

Internal Mail Server:

☐ Delete the virus mail

☒ Deliver to the recipient

☒ Deliver a notification mail instead of the original virus mail

☐ Deliver the original virus mail

☐ Forward to : (Max: 128 characters, ex: user@mydomain.com)

External Mail Server:

☒ Deliver to the recipient (Always enable)

☐ Deliver a notification mail instead of the original virus mail

☐ Deliver the original virus mail

OK Cancel

Figure15-1 Anti-Virus Settings WebUI

- ◆ Add the message ---virus---in the subject line of infected mail (Figure15-2)

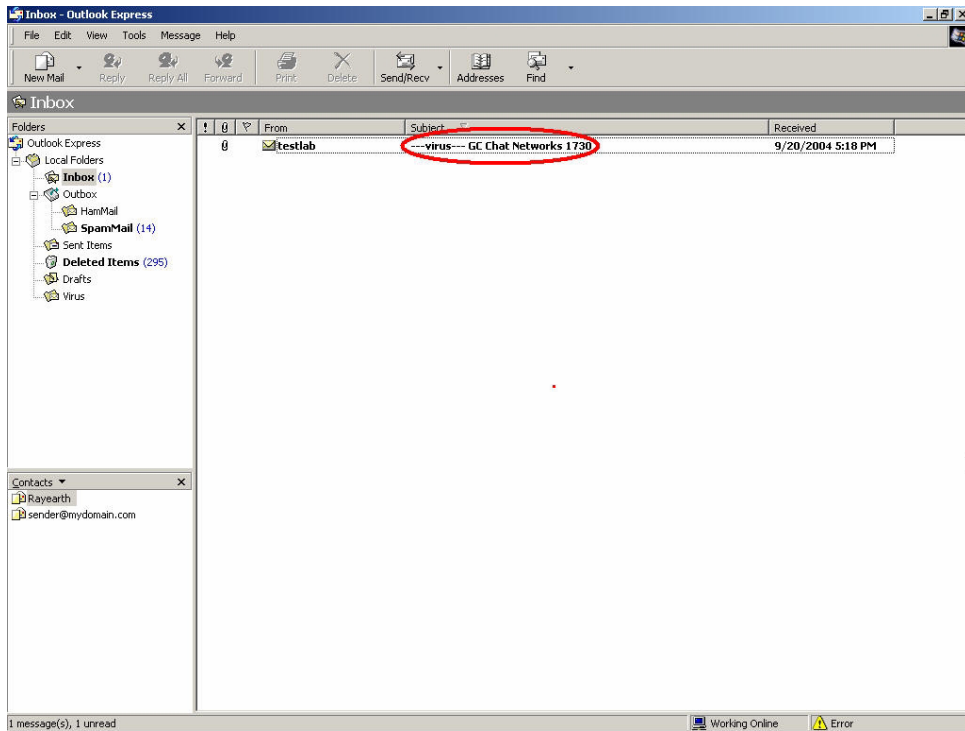


Figure15-2 The Subject of Infected Mail WebUI



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

## Define the required fields of Virus Mail:

### Top Total Virus:

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



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



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

We set up two Anti-Virus examples in this chapter:

No.	Example	Page
Ex 1	To detect if the mail that received from external Mail Server have virus or not.	<b>371</b>
Ex 2	To detect the mail that send to Internal Mail Server have virus or not. (Mail Server is in LAN, NAT Mode)	<b>375</b>

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

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

**STEP 2 .** In **LAN** of **Address** function, add the following settings: (Figure15-3)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Josh	192.168.139.12/255.255.255.255		Modify Remove

New Entry

Figure15-3 Mapped IP of Internal User's PC in Address Book

**STEP 3 .** Add the following setting in **Group** of **Service**. (Figure15-4)

Group name	Service	Configure
Mail_Service	DNS,POP3,SMTP	Modify Remove

New Entry

Figure15-4 Service Group that includes POP3, SMTP, or DNS

**STEP 4 .** Add the following setting in **Outgoing Policy**: (Figure15-5)

Source	Destination	Service	Action	Option	Configure	Move
Josh	Outside_Any	Mail_Service	✓		Modify Remove	To 1

New Entry

Figure15-5 Outgoing Policy Setting



**STEP 5 .** Add the following setting in **Setting** of **Anti-Virus** function:  
(Figure15-6)

- **Virus Scanner:** Select Clam
- **The Mail Server is placed in** External (WAN)
- **Add the message to the subject line:** ---virus---
- **Select Remove virus mail and the attached file** (Figure15-6)

**Anti-Virus Setting**

Virus Scan Engine: **Clam**

The Mail Server is: ☐ Internal (LAN or DMZ) ☒ External (WAN)

Add the virus string to the subject line: **---virus---** (Max. 256 characters)

---

Last queried on : 2006/01/31 16:29:37 (Query virus definitions every ten minutes)  
Current version : 44.4808 (Clam definitions updated at 06/01/31 16:08:34)  
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) [Update Now](#) [Test](#)

---

**Action of Infected Mail**

Internal Mail Server:

- ☒ Delete the virus mail
- ☐ Deliver to the recipient
  - ☐ Deliver a notification mail instead of the original virus mail
  - ☐ Deliver the original virus mail
- ☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com )

External Mail Server:

- ☒ Deliver to the recipient (Always enable)
  - ☐ Deliver a notification mail instead of the original virus mail
  - ☐ Deliver the original virus mail

OK Cancel

**Figure15-6 Action of Infected Mail and Anti-Virus Settings**



**Anti-Virus** function is enabled in default status. So the System Manager does not need to set up the additional setting and then the ALL7008 will scan the mails automatically, which sent to the internal mail server or received from external mail server. (Figure15-7)

**Anti-Virus Setting**

Virus Scan Engine: Clam

The Mail Server is: ☒ Internal (LAN or DMZ) ☒ External (WAN)

Add the virus string to the subject line: ---virus--- (Max. 256 characters)

---

Last queried on : 2006/01/31 16:29:37 (Query virus definitions every ten minutes)  
 Current version : 44.4808 (Clam definitions updated at 06/01/31 16:08:34)  
 Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) [Update Now](#) [Test](#)

**Action of Infected Mail**

Internal Mail Server:

☐ Delete the virus mail  
☒ Deliver to the recipient  
     ☒ Deliver a notification mail instead of the original virus mail  
     ☐ Deliver the original virus mail  
☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com)

External Mail Server:

☒ Deliver to the recipient (Always enable)  
     ☒ Deliver a notification mail instead of the original virus mail  
     ☐ Deliver the original virus mail

OK Cancel

**Figure15-7 Default Value of Virus Mail Setting**



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

1. In **Action of Virus Mail**, no matter choose **Delete mail**, **Deliver to the recipient**, or **Forward to**, it will add the message in the subject line of infected mail and send it to the recipient.

**STEP 6 .** When the internal users are receiving the mail from external mail account (js1720@ms21.pchome.com.tw), the ALL7008 will scan the mail at the same time and the chart will be in the **Virus Mail** in **Anti-Virus** function. (At this time, choose **External** to see the mail account chart) (Figure15-8)

Top Total Virus: 1-1

Internal External

No.	Recipient	Total Virus	Total Mail	Duration	Virus %
1	js1720@ms21.pchome.com.tw	1	2	00H	50.0%
Total		1	2		50.0%

Clear Data

Figure15-8 Report Function Chart



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

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

WAN IP of ALL7008: 61.11.11.12

LAN Subnet of ALL7008: 192.168.2.0/24

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

**STEP 2** . Enter the following setting in **LAN** of **Address** function: (Figure15-9)

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Mail_Server	192.168.2.12/255.255.255.255	00:E0:1B:25:F5:89	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure15-9 Mapped IP Setting in Address of Mail Server

**STEP 3** . Enter the following setting in **Group** in **Service** function: (Figure15-10)

Group name	Service	Configure
Mail_Service_01	POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Mail_Service_02	DNS,POP3,SMTP	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure15-10 Setting Service Group that include POP3, SMTP or DNS

**STEP 4 .** Enter the following setting in **Server1** in **Virtual Server** function:  
(Figure15-11)

Virtual Server Real IP

Service	WAN Port	Server Virtual IP	Configure
Mail_Service_01	From-Service (Group)	192.168.2.12	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure15-11 Virtual Server Setting WebUI

**STEP 5 .** Enter the following setting in **Incoming Policy**: (Figure15-12)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	Mail_Service_01	✓	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To <input type="text" value="1"/>

Figure15-12 Incoming Policy Setting

**STEP 6 .** Enter the following setting in **Outgoing Policy**: (Figure15-13)

Source	Destination	Service	Action	Option	Configure	Move
Mail_Server	Outside_Any	Mail_Service_02	1	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To <input type="text" value="1"/>

Figure15-13 Outgoing Policy Setting

**STEP 7 .** Enter the following setting in **Mail Relay** function of **Configure:**  
(Figure15-14)

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
broadband.com.tw ( 192.168.2.12 )	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>	

**Figure15-14 Mail Relay Setting of External Mail to Internal Mail Server**



**Mail Relay** function makes the mails that sent to LAN's mail server could be relayed to its mapped mail server by ALL7008.

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

- **Virus Scanner:** Select Clam
- **The Mail Server is placed in** Internal (LAN or DMZ)
- **Add the message to the subject line:** ---virus---
- Select **Remove virus mail and the attached file**
- **Action of Infected Mail:** Select Deliver to the recipient (Figure15-15)

**Anti-Virus Setting**

Virus Scan Engine: Clam

The Mail Server is: ☒ Internal (LAN or DMZ) ☐ External (WAN)

Add the virus string to the subject line: ---virus--- (Max. 256 characters)

---

Last queried on : 2006/01/31 16:33:17 (Query virus definitions every ten minutes)  
Current version : 44.4808 (Clam definitions updated at 06/01/31 16:08:34)  
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) [Update Now](#) [Test](#)

**Action of Infected Mail**

Internal Mail Server:

☐ Delete the virus mail  
☒ Deliver to the recipient  
    ☒ Deliver a notification mail instead of the original virus mail  
    ☐ Deliver the original virus mail  
☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com)

External Mail Server:

☒ Deliver to the recipient (Always enable)  
☐ Deliver a notification mail instead of the original virus mail  
☐ Deliver the original virus mail

OK Cancel

**Figure15-15 Infected Mail Definition and Action of Infected Mail**



When select **Delete mail** in **Action of Infected Mail**, and then the other functions (**Deliver to the recipient**, or **Forward to**) cannot be selected. So when ALL7008 had scanned mail that have virus, it will delete it directly. But still can check the relevant chart in **Virus Mail** function.

- If the mails are from the sender account, share2k01@yahoo.com.tw, which include virus in the attached file.
- If it comes from other yahoo sender account share2k003@yahoo.com.tw, which attached file is safe includes no virus.
- After ALL7008 had scanned the mails above, it will bring the chart as follows in the **Virus Mail** function of **Anti-Virus**.  
(Figure15-16)

### Figure15-16 Report Chart







# Alert Setting

When the ALL7008 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/ALL7008. 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/ALL7008. 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 ALL7008 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 ALL7008 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/ALL7008. 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 / ALL7008. 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 ALL7008 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 ALL7008 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/ALL7008. 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/ALL7008. 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 ALL7008 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 ALL7008 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 ALL7008 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.

## ALL7008 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 100 Sessions/Sec)
- Select **Enable Blaster Blocking** and enter the **Blocking Time** (the default time is 600 seconds)
- Select **Enable E-Mail Alert Notification**
- Select **Enable NetBIOS Alert Notification**
- **IP Address of Administrator:** Enter 192.168.1.10
- Click **OK**
- Internal Alert Setting is completed. (Figure16-1)

Anomaly Flow IP Setting

The threshold sessions of anomaly flow (per source IP) is  Sessions / Sec ( Range: 1 - 9999 )

☒ Enable Anomaly Flow IP Blocking Blocking Time  seconds ( Range: 1 - 999 )

☒ Enable E-Mail Alert Notification

☒ Enable SNMP Trap Alert Notification

☒ Enable NetBIOS Alert Notification IP Address of Administrator

OK Cancel

**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 ALL7008 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

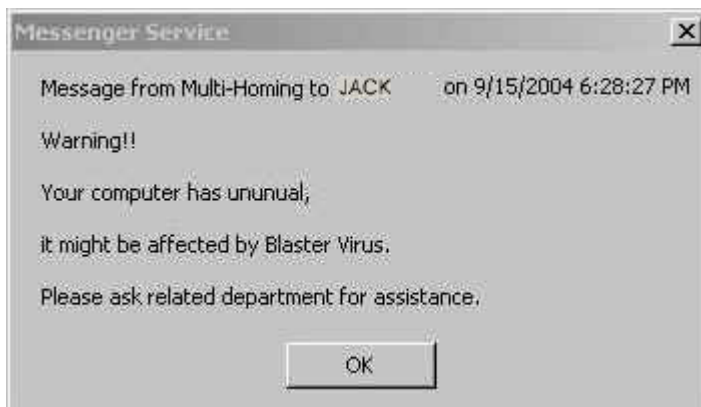
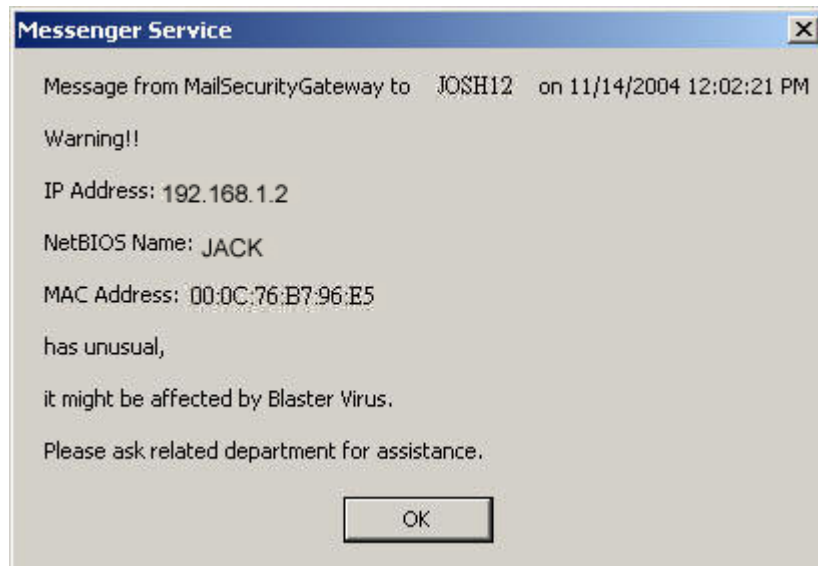


Figure16-3 NetBIOS Alert Notification to the Infected PC





**Figure16-4 NetBIOS Alert Notification to Administrator's PC**

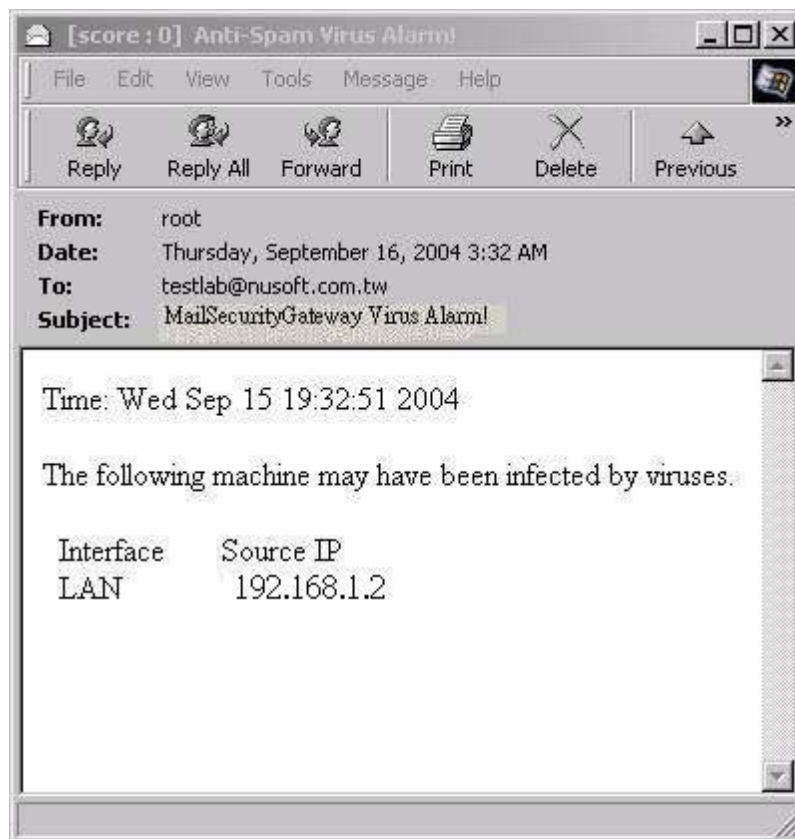


Figure16-5 E-mail Virus Alert



# Attack Alarm

ALL7008 has two alarm forms: **Internal Alarm**, and **External Alarm**.

**Internal Alarm:** When the ALL7008 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 ALL7008 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 unusual 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	<b>Internal Alarm</b>	To record the DDoS attack alarm from internal PC	<b>393</b>
Ex 2	<b>External Alarm</b>	To record the attack alarm about Hacker attacks the ALL7008 and Intranet	<b>394</b>

## 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 ALL7008 and Intranet

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

**DoS / Anti-Hacker Setting**

<input checked="" type="checkbox"/> Sasser Block	<input checked="" type="checkbox"/> MSBlaster Block
<input checked="" type="checkbox"/> Code Red Block	<input checked="" type="checkbox"/> Nimda Block
<input checked="" type="checkbox"/> Detect SYN Attack	SYN Flood Threshold (Total) <input type="text" value="200"/> Pkts/Sec
	SYN Flood Threshold (Per Source IP) <input type="text" value="50"/> Pkts/Sec
	SYN Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds
<input checked="" type="checkbox"/> Detect ICMP Flood	ICMP Flood Threshold (Total) <input type="text" value="1000"/> Pkts/Sec
	ICMP Flood Threshold (Per Source IP) <input type="text" value="300"/> Pkts/Sec
	ICMP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds
<input checked="" type="checkbox"/> Detect UDP Flood	UDP Flood Threshold (Total) <input type="text" value="1000"/> Pkts/Sec
	UDP Flood Threshold (Per Source IP) <input type="text" value="300"/> Pkts/Sec
	UDP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds
<input checked="" type="checkbox"/> Detect Ping of Death Attack	<input checked="" type="checkbox"/> Detect Tear Drop Attack
<input checked="" type="checkbox"/> Detect IP Spoofing Attack	<input checked="" type="checkbox"/> Filter IP Route Option
<input checked="" type="checkbox"/> Detect Port Scan Attack	<input checked="" type="checkbox"/> Detect Land Attack

OK Cancel

Figure17-2 External Alert Setting WebUI

**STEP 2 .** When Hacker attacks the ALL7008 and Intranet, select **External Alarm** in **Attack Alarm** function to have detailed records about the hacker attacks. (Figure17-3)

Jul 4 11:46:03 ▾

Time	Event
Jul 4 11:46:03	The system has detected the attack of TCP port scan , suspected to be 172.19.50.130
Jul 4 11:45:46	The system has detected the attack of TCP port scan , suspected to be 172.19.50.130
Jul 4 11:45:32	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:27	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:24	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:06	The system has detected the attack of TCP port scan , suspected to be 172.19.50.100
Jul 4 11:45:02	The system has detected the attack of TCP port scan , suspected to be 172.19.50.100
Jul 4 11:44:59	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:48	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:45	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:34	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:44:28	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:44:25	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:41:58	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:39:50	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:21	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:16	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:16	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12

Clear Alarm
Download Alarms

Figure17-3 External Alarm WebUI





# LOG

**Log** records all connections that pass through the ALL7008'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 ALL7008. 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	<b>Traffic Log</b>	To detect the information and Protocol port that users use to access to Internet or Intranet by ALL7008.	<b>399</b>
Ex 2	<b>Event Log</b>	To record the detailed management events (such as Interface and event description of ALL7008) of the Administrator	<b>404</b>
Ex 3	<b>Connection Log</b>	To detect event description of WAN Connection	<b>407</b>
Ex 4	<b>Log Backup</b>	To save or receive the records that sent by the ALL7008	<b>410</b>

## To detect the information and Protocol port that users use to access to Internet or Intranet by ALL7008

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

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps
MAX. Concurrent Sessions Per IP	<input type="text"/>
MAX. Concurrent Sessions	<input type="text"/>

OK Cancel

**Figure18-1 Logging Policy Setting**

**STEP 2 .** Complete the Logging Setting in **DMZ to WAN Policy**: (Figure18-2)

Source	Destination	Service	Action	Option					Configure		Move
DMZ_Any	Outside_Any	ANY							Modify	Remove	To <input type="text"/>

New Entry

**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)

Jul 4 12:02:59 ▾
[Next](#)

Time	Source	Destination	Protocol	Port	Disposition
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	✓

Clear Logs
Download Logs

Figure18-3 Traffic Log WebUI

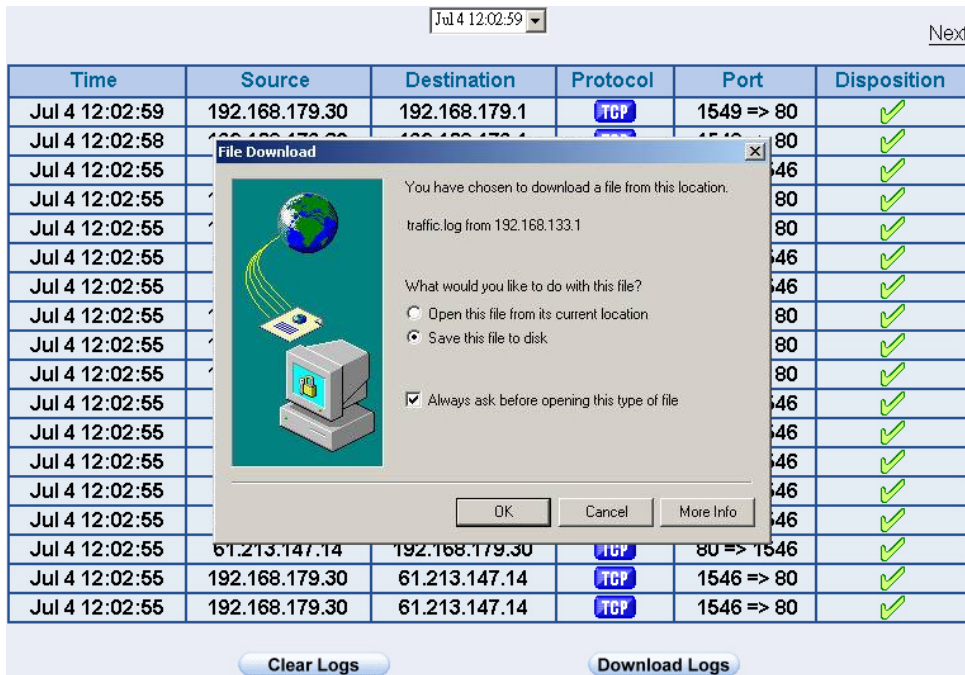
**STEP 4** . Click on a specific IP of **Source IP** or **Destination IP** in Figure18-3, it will prompt out a WebUI about Protocol and Port of the IP. (Figure18-4)

Refresh manually Jul 4 12:04:15 Next

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 ALL7008 instantly. (Figure18-6)

Jul 4 12:02:59 Next

Time	Source	Destination	Protocol	Port	Disposition
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
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	✓

Clear Logs
Download Logs

Figure18-6 Clearing Traffic Log Records WebUI



## To record the detailed management events (such as Interface and event description of ALL7008) of the Administrator

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

Jul 4 12:05:11 ▾

Next

Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1) from 192.168.179.30
Jul 4 11:59:13	admin Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:58:26	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:50:33	(null) WAN1 is connected
Jul 4 11:50:16	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:48:22	(null) Remove [Mapped IP] (External IP : 172.19.0.2 Internal IP : 192.168.179.2) from 192.168.179.30
Jul 4 11:39:09	user admin [Login success] from 192.168.179.30
Jul 4 11:36:07	(null) Modify [Mapped IP] (External IP : 172.19.0.2 Internal IP : 192.168.179.2) from 172.19.50.12
Jul 4 11:35:35	(null) Add [Mapped IP] (External IP : 172.19.0.2 Internal IP : 12.168.179.2) from 172.19.50.12
Jul 4 11:35:16	(null) Remove [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:58	(null) Add [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:09	user admin [Login success] from 172.19.50.12
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

Clear Logs

Download Logs

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)

Jul 4 12:05:11 Next

Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1)
Jul 4 11:59:13	
Jul 4 11:58:26	
Jul 4 11:50:33	
Jul 4 11:50:16	
Jul 4 11:48:22	
Jul 4 11:39:09	
Jul 4 11:36:07	
Jul 4 11:35:35	
Jul 4 11:35:16	
Jul 4 11:34:58	
Jul 4 11:34:09	
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

Clear Logs Download Logs

**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 ALL7008. (Figure18-9)

Jul 4 12:05:11 Next

Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1) from 192.168.179.30
Jul 4 11:59:13	admin Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:58:26	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:50:33	(null) WAN1 is connected
Jul 4 11:50:16	(null) Modify [WAN2 Interface] from 192.168.179.30
Jul 4 11:48:22	(null) Remove [WAN2 Interface] from 192.168.179.2
Jul 4 11:39:09	user admin [Login success] from 172.19.50.12
Jul 4 11:36:07	(null) Modify [WAN2 Interface] from 172.19.50.12
Jul 4 11:35:35	(null) Add [Mapped IP] (External IP : 172.19.0.2 Internal IP : 12.168.179.2) from 172.19.50.12
Jul 4 11:35:16	(null) Remove [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:58	(null) Add [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:09	user admin [Login success] from 172.19.50.12
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

Clear Logs Download Logs

**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 ALL7008. (Figure18-10)

Jul 3 19:41:14 

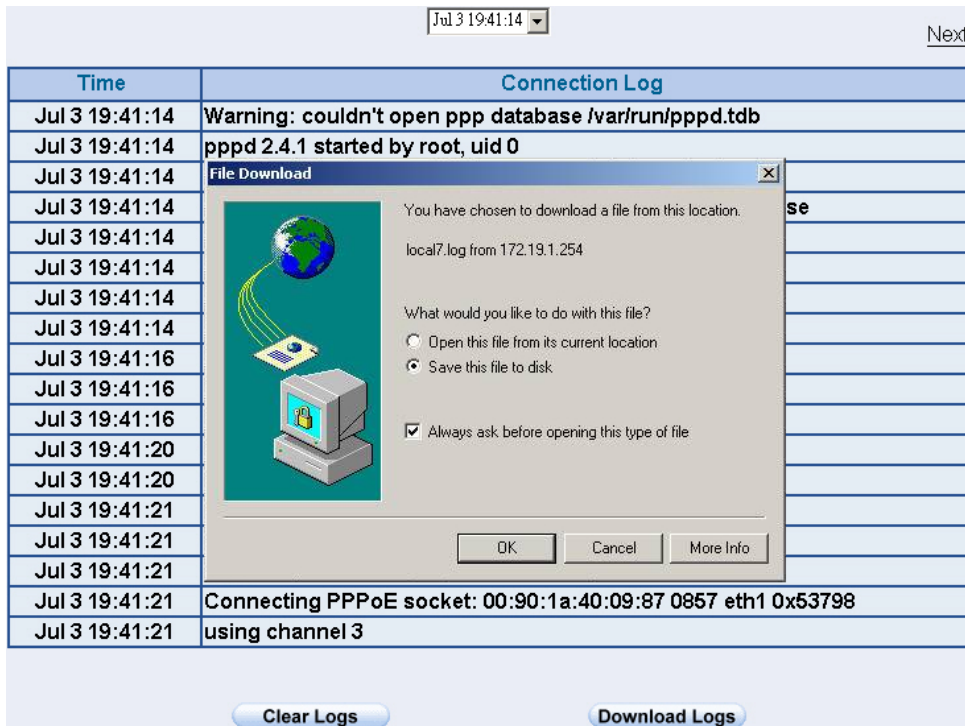
Next

Time	Connection Log
Jul 3 19:41:14	Warning: couldn't open ppp database /var/run/pppd.tdb
Jul 3 19:41:14	pppd 2.4.1 started by root, uid 0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	Couldn't allocate PPP unit -1073449922 as it is already in use
Jul 3 19:41:14	Using interface ppp0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	PPPoE : Couldn't increase MTU to 1500
Jul 3 19:41:14	Couldn't increase MRU to 1500
Jul 3 19:41:16	local IP address 10.64.64.64
Jul 3 19:41:16	remote IP address 10.114.136.19
Jul 3 19:41:16	linkname : wan1 interface : ppp0
Jul 3 19:41:20	Sending PADI
Jul 3 19:41:20	HOST_UNIQ successful match
Jul 3 19:41:21	HOST_UNIQ successful match
Jul 3 19:41:21	Got connection: 857
Jul 3 19:41:21	pads
Jul 3 19:41:21	Connecting PPPoE socket: 00:90:1a:40:09:87 0857 eth1 0x53798
Jul 3 19:41:21	using channel 3

Clear LogsDownload Logs

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 ALL7008 instantly. (Figure18-12)

Jul 3 19:41:14 Next

Time	Connection Log
Jul 3 19:41:14	Warning: couldn't open ppp database /var/run/pppd.tdb
Jul 3 19:41:14	pppd 2.4.1 started by root, uid 0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	Couldn't allocate PPP unit -1073449922 as it is already in use
Jul 3 19:41:14	Using interface ppp0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	PPPoE : Couldn't increase MTU to 1500
Jul 3 19:41:14	Couldn't in
Jul 3 19:41:16	local IP ad
Jul 3 19:41:16	remote IP a
Jul 3 19:41:16	linkname :
Jul 3 19:41:20	Sending P
Jul 3 19:41:20	HOST_UNIQ successful match
Jul 3 19:41:21	HOST_UNIQ successful match
Jul 3 19:41:21	Got connection: 857
Jul 3 19:41:21	pads
Jul 3 19:41:21	Connecting PPPoE socket: 00:90:1a:40:09:87 0857 eth1 0x53798
Jul 3 19:41:21	using channel 3

Clear Logs
Download Logs

**Figure18-12 Clearing Connection Log Records WebUI**

## To save or receive the records that sent by the ALL7008

**STEP 1 .** Enter **Setting** in **System**, select **Enable E-mail Alert Notification** function and set up the settings. (Figure18-13)

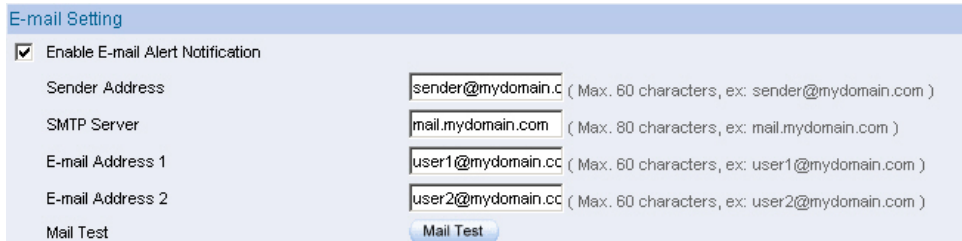


Figure18-13 E-mail Setting WebUI

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



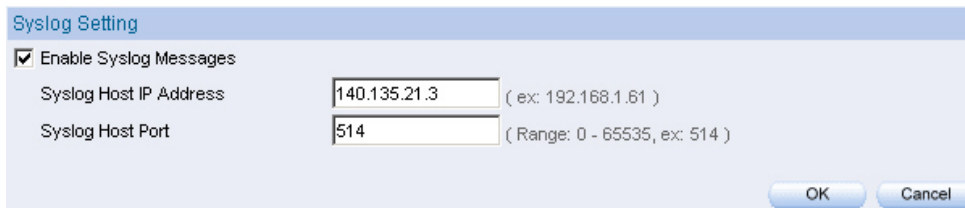
Figure18-14 Log Mail Configuration WebUI



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)

A screenshot of the 'Syslog Setting' web interface. The title bar is light blue with the text 'Syslog Setting'. Below the title bar, there is a checkbox labeled 'Enable Syslog Messages' which is checked. Underneath, there are two input fields. The first is labeled 'Syslog Host IP Address' and contains the text '140.135.21.3', with a hint '( ex: 192.168.1.61 )' to its right. The second is labeled 'Syslog Host Port' and contains the text '514', with a hint '( Range: 0 - 65535, ex: 514 )' to its right. At the bottom right of the form, there are two buttons: 'OK' and 'Cancel'.

**Figure18-15 Syslog Messages Setting WebUI**





# Alarm

**Traffic Alarm:** In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

## To show the alarm message about exceeding the Alarm Threshold of Policy

**STEP 1** . Add the following setting in **DMZ to WAN Policy**:

- **Alarm Threshold:** Enter 10 Kbytes/Sec
- Click **OK** (Figure19-1)

Modify Policy	
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
Anti-Virus	<input type="checkbox"/> HTTP / WEBMAIL <input type="checkbox"/> FTP
Authentication User	None
Schedule	None
Alarm Threshold	10 KBytes/Sec
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Figure19-1 Alarm Threshold Policy Setting

**STEP 2** . Complete the **Traffic Alarm** setting in **DMZ to WAN Policy** function:  
(Figure19-2)

Source	Destination	Service	Action	Option				Configure		Move
DMZ_Any	Outside_Any	ANY	✓				⚠	Modify	Remove	To 1
<input type="button" value="New Entry"/>										

Figure19-2 Complete Traffic Alarm Setting in DMZ to WAN Policy

**STEP 3** . When the internal PC access to Internet through the policy and its traffic exceeds the Alarm Threshold, the detail of policy will be listed when entering **Traffic** of **Alarm** function. (Figure19-3)

Jul 3 20:30~20:45 ▾

Time	Source	Destination	Service	Traffic
Jul 3 20:30~20:45	Inside_Any	Outside_Any	ANY	179.770K/Sec
Jul 3 20:15~20:30	Inside_Any	Outside_Any	ANY	205.314K/Sec
Jul 3 20:00~20:15	Inside_Any	Outside_Any	ANY	220.051K/Sec
Jul 3 19:45~20:00	Inside_Any	Outside_Any	ANY	129.139K/Sec

Clear AlarmDownload Alarms

Figure19-3 Traffic Alarm WebUI



**Traffic Alarm** considers 15 minutes as one unit time. Take the average traffic in one unit (15 min.) time to compare with the **Alarm Threshold** of **Policy**, the ALL7008 will send warning in **Traffic Alarm** if exceeds the value.



# 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 ALL7008 for statistics of packets and data that passes across the ALL7008. 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	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
WAN 2	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
All WAN Interface	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>

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)

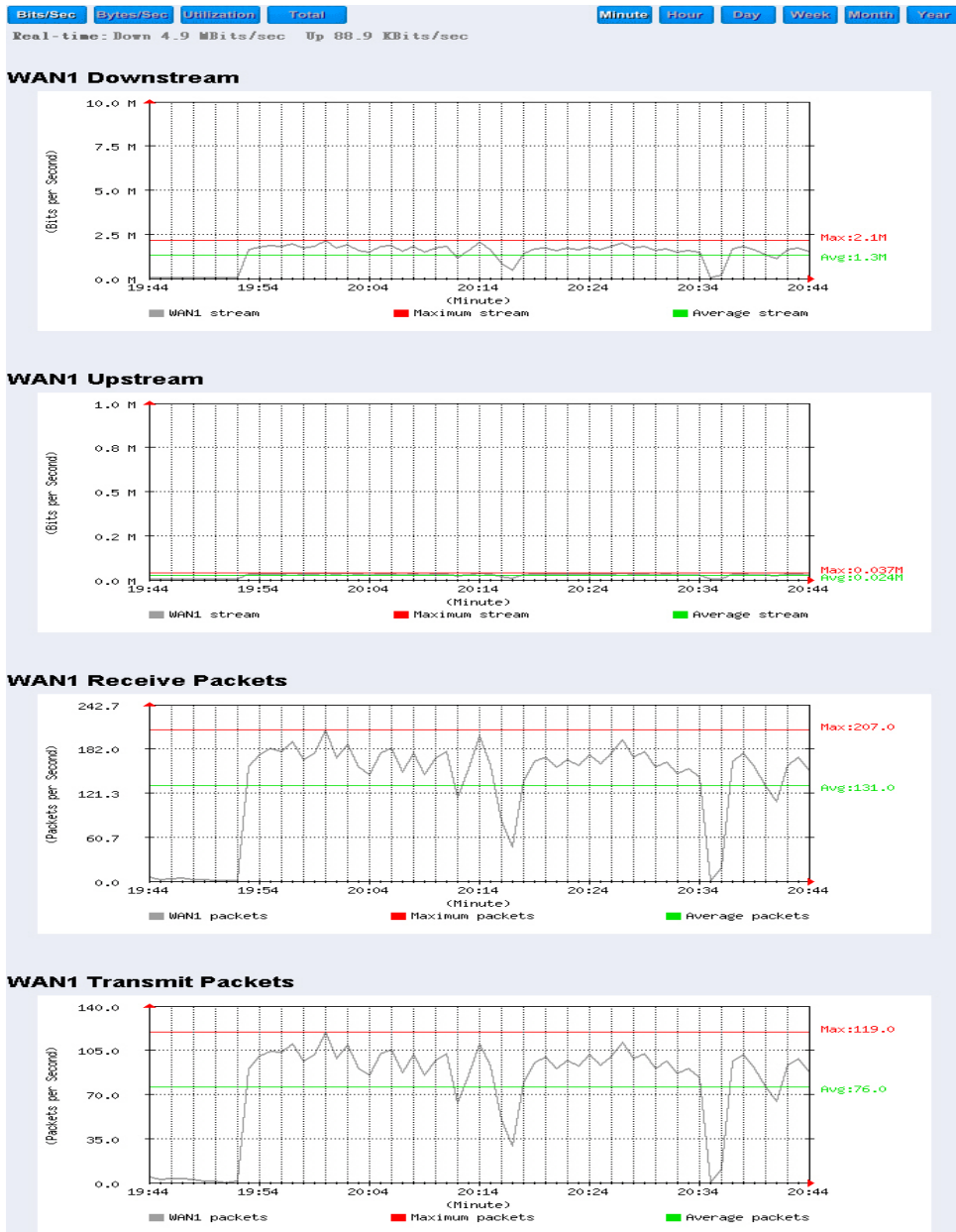


Figure20-2 To Detect WAN Statistics

## 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	<u>Minute</u>	<u>Hour</u>	<u>Day</u>	<u>Week</u>	<u>Month</u>	<u>Year</u>
DMZ_Any	Outside_Any	ANY	PERMIT	<u>Minute</u>	<u>Hour</u>	<u>Day</u>	<u>Week</u>	<u>Month</u>	<u>Year</u>

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)

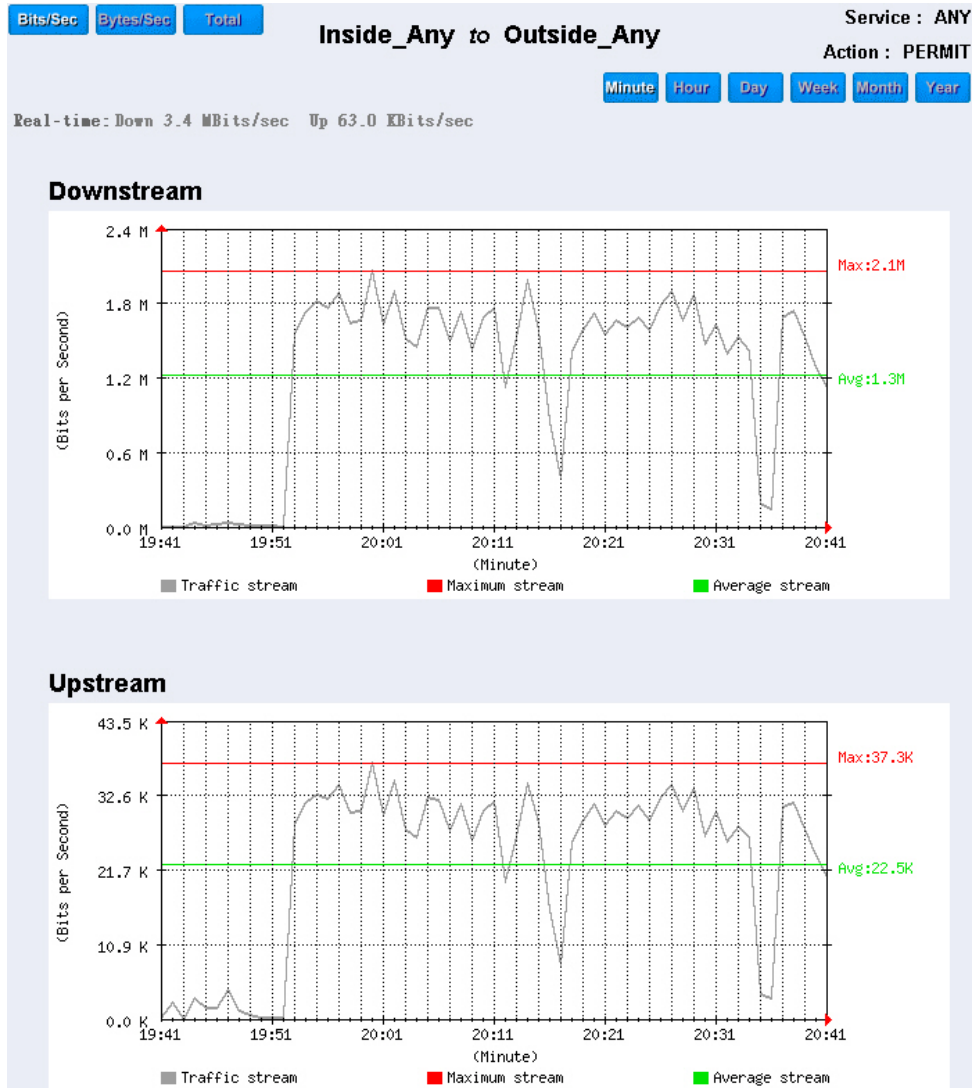


Figure20-4 To Detect Policy Statistics

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 ALL7008
- **Authentication:** The Authentication information of ALL7008
- **ARP Table:** Record all the ARP that connect to the ALL7008
- **DHCP Clients:** Display the table of DHCP clients that are connected to the ALL7008.

## 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 ALL7008 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 ALL7008 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	NAT
WAN Connection	---			---
Max. Downstream / Upstream	---	51200 / 51200 Kbps	51200 / 51200 Kbps	---
Downstream Alloca.	---	100%	0%	---
Upstream Alloca.	---	83%	16%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:aa:bb:d3:87:66	00:aa:bb:d5:46:24	00:aa:bb:d3:87:64	00:aa:bb:d3:87:67
IP Address	192.168.189.1	59.124.36.173	61.11.11.12	192.168.3.1
Netmask	255.255.255.0	255.255.255.240	255.255.255.0	255.255.255.0
Default Gateway	---	59.124.36.161	61.11.11.11	---
DNS1	---	168.95.1.1	168.95.1.1	---
DNS2	---	168.95.192.1	168.95.192.1	---
Rx Pkts, Error Pkts	43945, 0	12240, 0	0, 0	0, 0
Tx Pkts, Error Pkts	12975, 0	9281, 0	1555, 0	3, 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

Figure21-2 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 ALL7008: (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 ALL7008: (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



23.11.07

Germering, den

## **CE-Kennzeichnung und EG-Konformitätserklärung**

Für das folgend bezeichnete Erzeugnis

### **ALL7008 Security Gateway**

CE-Kennzeichnung



Dieses Gerät erfüllt die Anforderungen der EU-Richtlinie:

89/336/EG Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit und die gegenseitige Anerkennung ihrer Konformität.

Die Konformität mit der o.a. Richtlinie wird durch das CE-Zeichen auf dem Gerät bestätigt.

EG Konformitätserklärung

Wird hiermit bestätigt, dass der ALLNET ALL7008 Security Gateway den Anforderungen entspricht, die in der Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (1989/336/EG) festgelegt sind.

Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMI: EN 55022: 1998+A1: 2000+A2: 2003  
EN 61000-3-2: 2000  
EN 61000-3-3: 1995+A1: 2001

EMS: EN 55024: 1998+A1: 2001+A2: 2003

Diese Erklärung wird verantwortlich für den Hersteller/Bevollmächtigten abgegeben:

ALLNET Computersysteme GmbH  
Maistr. 2  
82110 Germering

Die Konformitätserklärung kann unter der oben genannten Adresse oder im Internet unter <http://www.allnet.de/ce-certificates/> eingesehen werden.