

# <u>ALL7007</u>

# User's Manual

# **Table of Contents**

System		
Chapter 1	Administrator	6
	Admin	8
	Permitted IPs	10
	Logout	11
	Software Update	12
Chapter 2	Configure	13
	Setting	22
	Date/Time	27
	Multiple Subnet	28
	Route Table	33
	DHCP	37
	DDNS	39
	Host Table	41
	Language	42

## Interface

Chapter 3	Interfac	се	 	 	 	 	 	 43
	LAN		 	 	 	 	 	 47
	WAN		 	 	 	 	 	 48
	DMZ		 	 	 	 	 	 52

# Policy Object

Chapter 4	Address Example	54 56
Chapter 5	Service Custom Group	64 67 71
Chapter 6	Schedule	74
Chapter 7	QoS Example	77 80
Chapter 8	Authentication Example	83 88
Chapter 9	Content Blocking URL Script P2P IM Download	117 121 124 126 128 130
Chapter 10	Virtual Server Example	132 135
Chapter 11	VPN Example	151 158

# Policy

Chapter 12 Deliev	102
Chapter 12 Policy	 105

	Example	188
Mail Secur	ity	
Chapter 13	Configure	203
	Mail Relay	206
Chapter 14	Anti-Spam	211
	Example	225
Chapter 15	Anti-Virus	272
	Example	277
IDP Chapter 16	Configure	287
Chapter 17	Signature	291
Chapter 18	IDP Report	297
Monitor		
Chapter 19	Log	299
	Traffic	301
	Event	305

Event	 305
Connection	 308
Log Backup	 311

Chapter 20 Statisti	CS	313
WAN		315
Policy		317

Chapter 21	Status	319
	Interface	320
	ARP Table	321
	DHCP Clients	322

# **Chapter 1**

# System

"System" is the managing of settings such as the privileges of packets that pass through ALL7007 and monitoring controls. The System Administrators can manage, monitor, and configure the ALL7007 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 ALL7007.

# Define the required fields of Administrator

#### Administrator Name:

The username of Administrators and Sub-Administrator for the ALL7007. 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 or click Cancel to cancel it.

Modify Admin Passwor	d	
Admin Name	admin	
Password	****	
New Password	****	
Confirm Password	****	
		OK Cancel
		OK Cancel

Figure1-2 Modify Admin Password

# **Add Permitted IPs**

- STEP 1. Add the following setting in **Permitted IPs** of **Administration**: (Figure 1-3)
  - Name: Enter master
  - IP Address: Enter 163.173.56.11
  - Netmask: Enter 255.255.255.255
  - Service: Select Ping and WebUI
  - Click OK
  - Complete add new permitted IPs (Figure1-4)

Add New Permitted IPs	
Name	Enter master
IP Address	163.173.56.11
Netmask	255.255.255.255
Service	Ping Pitre
	OK Cancel

Figure1-3 Setting Permitted IPs WebUI

Enter_master 163.173.56.11 / 255.255.255.255 🖌 🖌 Modify Remove	Name	IP Address / Netmask	Ping	HTTP	Configure
	Enter_master	163.173.56.11 / 255.255.255.255	1	1	Modify Remove
New Entry		New Entry			

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 ALL7007 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 ALL7007
- Click **Browse** and choose the latest software version file.
- Click **OK** and the system will update automatically. (Figure1-7)

Software Update		
Version Number :	v 2.00	
Software Update	Allnet_ALL7007_020000.img 瀏覽	
	( ex: Allnet_ALL7007_020000.img )	
		OK Cancel
	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 ALL7007. In this chapter the definition is Setting, Date/Time, Multiple Subnet, Hacker Alert, Blaster Alert, Route Table, DHCP, Dynamic DNS, Hosts Table, Mail Relay, SNMP and Language settings.

# Define the required fields of Settings

# ALL7007 Configuration:

The Administrator can import or export the system settings. Click OK to import the file into the ALL7007 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 ALL7007 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 ALL7007 will record packet which source IP or destination address is ALL7007. And record in Traffic Log for System Manager to inquire about.

# Define the required fields of Time Settings

### Synchronize Time/Date:

Synchronizing the ALL7007 with the System Clock. The administrator can configure the ALL7007'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

### **Multiple Mode:**

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

#### WAN Interface Address:

■ The IP address that Multiple Subnet corresponds to WAN.

### LAN Interface Address/Subnet Netmask:

■ The Multiple Subnet range.

# NAT Mode:

- It allows Internal Network to set multiple subnet address and connect with the Internet through different WAN IP Addresses. For example : The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet for the purpose of managing conveniently. The settings are as the following :
  - 1. R&D department subnet : 192.168.1.1/24(LAN) ← → 168.85.88.253(WAN)
  - 2. Service department subnet : 192.168.2.1/24(LAN) ←→ 168.85.88.252(WAN)
  - 3. Sales department subnet : 192.168.3.1/24(LAN) ←→ 168.85.88.251(WAN)
  - Procurement department subnet
    192.168.4.1/24(LAN) ← → 168.85.88.250(WAN)
  - 5. Accounting department subnet 192.168.5.1/24(LAN) ←→ 168.85.88.249(WAN)

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

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

# **Routing Mode:**

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

# Define the required fields of 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/ALL7007. 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/ALL7007. 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 ALL7007 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 ALL7007 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/ALL7007. 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 / ALL7007. 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 ALL7007 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 ALL7007 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/ALL7007. 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/ALL7007. 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 ALL7007 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 ALL7007 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 start **Hacker Alert**, if the ALL7007 has detected any abnormal situation, the alarm message will appear in **Alarm- Event 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. As for to enable **SNMP Trap Alert Notification** in **SNMP** function, then instant message can appear in the software of SNMP Trap client.

# 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 <u>Download</u> 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 ALL7007 will copy to the appointed site instantly. (Figure2-1)

NetGuardian Conf File Download	iauration	×
	You have chosen to download a file from this location. Mail-Security.conf from 172.19.100.85	· 瀏覽… Jian.conf)
2	What would you like to do with this file? C Open this file from its current location C Save this file to disk	( ex: NetGuardian )
	Always ask before opening this type of file	( ex: sender@mydomain.com ) ( ex: sender@mydomain.com )
	OK Cancel More Info	(ex: user1@mydomain.com) (ex: user2@mydomain.com)

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 ALL7007 Settings, then click OK. (Figure2-2)
- **STEP 2**. Click **OK** to import the file into the ALL7007 (Figure 2-3)

NetGuardian Configuration Export System Setting to ClientDown	nload
Import System Setting from Client	(ex: NetGuardian.conf)
Choose file	<u>? × </u>
E Look in: 🔄 Mail_Security_Config	
Mail-Security.conf History	ian) nydomain.com) nydomain.com) ydomain.com) ydomain.com)
My Network P	
N Files of type: All Files (*.*)	Cancel
Link Speed / Duplex Mode Setting	

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

Microsoft	t Internet Explorer	X
2	If you click "OK", software will upload. Please wait for 1 minute. Don't power off updated.	or leave this page during system is
	OK Cancel	

Figure 2-3 Upload the Setting File WebUI

# **Restoring Factory Default Settings**

- STEP 1 . Select Reset Factory Settings in ALL7007 Configuration WebUI
- STEP 2 . Click OK at the bottom-right of the page to restore the factory settings. (Figure2-4)

NetGuardian Configuration	
Export System Setting to Client 🔵 Download	
Import System Setting from Client	<b>瀏覽</b> ( ex: NetGuardian.conf )
Reset Factory Setting	
E-mail Setting	
Enable E-mail Alert Notification	
Device Name	( ex: NetGuardian )
Sender Address (Required by some ISPs)	( ex: sender@mydomain.com )
SMTP Server	( ex: sender@mydomain.com )
E-mail Address 1	( ex: user1@mydomain.com )
E-mail Address 2	( ex: user2@mydomain.com )
Mail Test	Mail Test
Web Management (WAN Interface)	
HTTP Port	80
MTU Setting	
MTU	1500 Bytes
Link Speed / Duplex Mode Setting	
WAN	Auto Mode
Dynamic Routing (RIPv2)	
Enable 🗆 LAN 🗆 WAN 🗆 DMZ	
Routing information update timer	<sup>30</sup> Seconds
Routing information timeout	180 Seconds
Administration Packet Logging	
Enable Administration Packet Logging	
System Reboot	
Reboot NetGuardian Appliance 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 . Device Name: Enter the Device Name or use the default value.
- STEP 3 . Sender Address: Enter the Sender Address. (Required by some ISPs.)
- STEP 4 . SMTP Server IP: Enter SMTP server's IP address.
- STEP 5 . E-Mail Address 1: Enter the e-mail address of the first user to be notified.
- STEP 6 . E-Mail Address 2: Enter the e-mail address of the second user to be notified. (Optional)
- **STEP 7** . Click **OK** on the bottom-right of the screen to enable E-mail Alert Notification. (Figure2-5)

E-mail Setting	
Enable E-mail Alert Notification	
Device Name	NetGuardian (ex: NetGuardian)
Sender Address (Required by some ISPs)	sender@mydomain.cor (ex: sender@mydomain.com)
SMTP Server	mydomain.com ( ex: sender@mydomain.com )
E-mail Address 1	userl@mydomain.com ( ex: userl@mydomain.com )
E-mail Address 2	user2@mydomain.com ( ex: user2@mydomain.com )
Mail Test	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 ALL7007

- STEP 1 . Reboot ALL7007 : Click Reboot button next to Reboot ALL7007 Appliance.
- **STEP 2** . A confirmation pop-up page will appear.
- **STEP 3**. Follow the confirmation pop-up page; click **OK** to restart ALL7007. (Figure2-6)

Dyn	amic Routing (RIPv2)					
Eng		DMZ				
Ro		timer	30	Seconds		
Ro	Are you sure to Reboot?		180	Seconds		
Adı	OK Caprel	ng				
		cket Logging				
Sys	tem Reboot					
Reb	oot NetGuardian Appliar	nce Reboot				
					OK Cance	

Figure2-6 Reboot ALL7007

# **Date/Time Settings**

- STEP 1 . Select Enable synchronize with an Internet time Server (Figure 2-7)
- 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. If you set it to 0, it means the device will not synchronize automatically.

System time : Mon Aug 8 11:20:08 2005
Synchronize system clock
Enable synchronize with an Internet time Server
Set offset 🔍 🔽 hours from GMT Assist
Server IP / Name 131.188.3.220 Assist
Update system clock every ominutes (0 : means update at booting time)
Synchronize system clock with this client Sync
OK Cancel

Figure 2-7 System Time Setting

Click on the **Sync** button and then the ALL7007'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

To connect to Internet, WAN IP (211.22.22.22) connect 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 172.16.30.1
- Netmask : Enter 255.255.255.0
- WAN : Enter Interface IP211.22.22.22, and choose NAT in Forwarding Mode
- Click OK
- Complete Adding Multiple Subnet (Figure 2-8)

Add New Multiple Subnet IP				
Alias IP of LAN Interface	172.16.30.1			
Netmask	255.255.255.0			
WAN	Interface IP		Forwarding Mode	
WAN	211.22.22.22	Assist	⊙ NAT ○ Routing	
			OK Cancel	

Figure2-8 Add Multiple Subnet WebUI

WAN 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 172.16.30.0/24. So if LAN IP is:

- 192.168.1.xx, it must use NAT Mode to connect to the Internet.
- 162.172.50.xx, it's also use NAT mode through WAN (The Internet Server can see your WAN IP directly). (Figure2-9)





 The ALL7007's Interface Status: WAN IP : 211.22.22.22
 LAN Port IP : 192.168.1.1
 LAN Port Multiple Subnet : 172.16.30.1 WAN IP (10.10.10.1) connect to the Router of ISP (10.10.10.2) directly. The IP address provided by ISP is 162.172.50.0/24

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
- WAN : Enter Interface IP: 10.10.10.1, and choose Routing in Forwarding Mode
- Click OK
- Complete Adding Multiple Subnet (Figure2-10)

Add New Multiple Subnet IP				
Alias IP of LAN Interface	162.172.50.1			
Netmask	255.255.255.0			
WAI	l Interface IP		Forwarding Mode	
WAN	0.0.0	Assist	○ NAT . ⓒ Routing	
			OK Cancel	

Figure2-10 Multiple Subnet WebUI Setting

After setting, if LAN IP of ALL7007 is 162.172.50.xx, it uses Routing Mode (Internet Server can see your IP 162.172.50.xx directly) (Figure2-11)





 The ALL7007's Interface Status: WAN IP : 10.10.10.1 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 ALL7007 and makes them to connect to Internet through ALL7007

#### Preparation

Company A: WAN (61.11.11.11) 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).

#### 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 2-12)

Add New Static Rou	ute	
Destination IP	192.168.10.1	
Netmask	255.255.255.0	
Gateway	192.168.1.252	
Interface	LAN 🔽	
		OK Cancel

Figure2-12 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 2-13)

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

OK Cancel

Figure2-13 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 2-14)

Add New Static Rou	te	
Destination IP	10.10.10.0	
Netmask	255.255.255.0	
Gateway	192.168.1.252	
Interface	LAN 🔽	
		OK Cancel

Figure2-14 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 2-15)



Figure 2-15 Route Table Setting
# **DHCP Setting**

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

- Domain Name : Enter the Domain Name of DHCP
- **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 start DMZ Interface)
- Leased Time: Enter the leased time for DHCP. The default time is 24 hours.
- Click **OK** and DHCP setting is completed. (Figure2-16)

Dynamic IP	Address				
Subnet	192.168.1.0	Netmask	255.255.	255.0	
Gateway	192.168.1.1	Broadcast	192.168.	1.255	
✓ Enable D	HCP Support				
Domain Nan	ne		( ex	: dhcp.domain_name )	
Automati	cally Get DNS	,			
DNS Server	-	192.168.1.1			
DNS Server	2				
WINS Serve	- r 1				
WINS Serve	r 2				
	-				
LAN Interfac	:e :				
Client IP Rai	nge 1	192.168.1.2	То	192.168.1.254	
Client IP Rai	nge 2		То		
DMZ Interfac	:e :				
Client IP Rai	nge 1	192.168.3.2	То	192.168.3.254	
Client IP Rai	nge 2		То		
Leased Time	9	<sup>24</sup> hours			
				OK	Cancel

Figure2-16 DHCP WebUI

When selecting **Automatically Get DNS**, the DNS Server will lock it as LAN Interface IP.

# **Dynamic DNS Settings**

- STEP 1 . Select Dynamic DNS in System function and enter the following setting: (Figure2-17).
  - Click **New Entry** button
  - Service Provider : Select service provider
  - Automatically fill in the WAN IP : Check to automatically fill in the WAN IP
  - User Name : Enter the registered user name
  - **Password** : Enter the password
  - Domain name : Enter host domain name
  - Click **OK** to complete adding Dynamic DNS. (Figure 2-18)

Add New Dynamic DNS				
Service Provider : DynDNS (www.dyndns.org) [U.S.A.] 🔽 Sign up				
WAN IP:	61.11.11.11 CAutomatically WAN			
User Name :	Rayearth			
Password :	*****			
Domain Name:	rayearth _ dyndns.org 🔽			
	OK Cancel			

#### Figure2-17 DDNS WebUI

i	Domain Name	WAN IP	Configure		
$\checkmark$	rayearth.dyndns.org	61.11.11.11	Modify Remove		
New Entry					

Figure 2-18 Complete DDNS Setting

Chart	V	×	<b>P</b>	1
Explanation	Update	Incorrect	Connecting	Unknown error
	successfully	username or	to server	
		password		

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** field. Let DDNS to correspond to that specific IP address.

## Adding a new Hosts Table

STEP 1 . Select Host Table in Settings function and enter the following setting:

- Click on New Entry
- Host Name: The domain name of the server
- Virtual IP Address: The virtual IP address that Host Table mapped to
- Click **OK** and complete adding Host Table. (Figure2-19)

Add New Host Table			
Host Name	www.filesever.com		
Virtual IP Address	192.168.1.1		
	OK Cance		

Figure2-19 Add New Host Table WebUI

To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of ALL7007. That is, the default gateway.

# Language

Select the Language version (English Version/ Traditional Chinese Version or Simplified Chinese Version) and click OK. (Figure 2-20)

Language Setting	
<ul> <li>English Version</li> </ul>	
• Traditional Chinese Version	
O Simplified Chinese Version	
	OK Cancel

Figure2-20 Language Setting WebUI

# Interface

In this chapter, 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 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 ALL7007.

## Ping:

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

## WebUI:

Select to enable the user to enter the WebUI of ALL7007 from Interface IP.

### WAN:

■ The System Administrator can set up the WAN network of ALL7007.

## **Connect Mode:**

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

# 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	Example	Page
	Situation		
Ex1	LAN	Modify LAN Interface Settings	47
Ex2	WAN	Setting WAN Interface Address	48
Ex3	DMZ	Setting DMZ Interface Address (NAT Mode)	52
Ex4	DMZ	Setting DMZ Interface Address (Transparent	53
		Mode)	

# **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 **WebUI**
- Click **OK** (Figure3-1)

Figure 3-1 Setting LAN Interface WebUI

The default LAN IP Address of ALL7007 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 ALL7007's WebUI from LAN.

# **Setting WAN Interface Address**

- STEP 1 . Select WAN in Interface and click Modify
- STEP 2 . Select the Connecting way:
  - **PPPoE (ADSL User)** (Figure 3-2):
    - 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 WebUI
    - 7. Click OK

WAN Interface			
• PPPoE (ADSL User)			
C Dynamic IP Address (Cable Mo	idem User)		
O Static IP Address			
Current Status	Disconnected	Co	onnecting
IP Address	0.0.0.0	Di	sconnect
User Name	ALLNET		
Password	****		
IP Address provided by ISP	Dynamic		
IF Address provided by ISF	© Dynamic © Eived		
	IP Address		
	Netmask		
	Default Gateway		
Max. Downstream Bandwidth	<sup>30000</sup> Kbps (Max	30 Mbps)	
Max. Upstream Bandwidth	<sup>30000</sup> Kbps (Max	30 Mbps)	
Service-On-Demand			
Auto Disconnect if idle 🔍 mi	nutes (0 : means alv	ays connected)	
Enable	Ping	☑ HTTP	
			OK Cancel

Figure3-2 PPPoE Connection

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

- **Dynamic IP Address (Cable Modem User)** (Figure 3-3):
  - 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.
  - 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 WebUI
  - 9. Click OK

WAN Interface		
C PPPoE (ADSL User)		
Oynamic IP Address (Cable Mod	em User)	
O Static IP Address		
IR Address	0000	Renew
IF Address	0.0.0.0	Release
MAC Address	00:E0:98:C3:32:62	Clone MAC Address
Hostname		
Domain Name		
User Name (Required by DHCP+ protocol)		
Password (Required by DHCP+ protocol)		
Max. Downstream Bandwidth	<sup>30000</sup> Kbps (Max	. 30 Mbps)
Max. Upstream Bandwidth	<sup>30000</sup> Kbps (Max	. 30 Mbps)
Enable	🗹 Ping	☑ HTTP
		OK Cancel

Figure 3-3 Dynamic IP Address Connection

- **Static IP Address** (Figure 3-4)
  - 1. Select Static IP Address
  - 2. Enter **IP Address**, **Netmask**, and **Default Gateway** that provided by ISP
  - 3. Enter DNS Server1 or DNS Server2
  - 4. Enter Max. Downstream Bandwidth and Max. Upstream Bandwidth (According to the flow that user apply)
  - 5. Select Ping and WebUI
  - 6.Click OK

WAN Interface			
C PPPoE (ADSL User)			
C Dynamic IP Address (Cable Mo	dem User)		
Static IP Address			
IP Address	211.22.22.18		
Netmask	255.255.255.0		
Default Gateway	211.22.22.17		
DNS Server 1	168.95.1.1		
DNS Server 2			
Max. Downstream Bandwidth	<sup>30000</sup> Kbps (Max. 30 N	/lbps)	
Max. Upstream Bandwidth	<sup>30000</sup> Kbps (Max. 30 M	/bps)	
Enable	✓ Ping	HTTP	
			OK Cancel

Figure 3-4 Static IP Address Connection

When selecting **Ping** and **WebUI** on **WAN** network Interface, users will be able to ping the ALL7007 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 in Interface function

- STEP 2 . Select NAT Mode in DMZ Interface
  - Select NAT in DMZ Interface
  - Enter IP Address and Netmask
- STEP 3 . Select Ping and WebUI
- **STEP 4** . Click **OK** (Figure 3-5)

DMZ Interface NAT			
IP Address	172.19.20.17		
Netmask	255.255.0.0		
Enable	Ping	HTTP	
			OK Cancel
			OK Cancel

Figure 3-5 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
  - Enter IP Address and Netmask
- STEP 3 . Select Ping and WebUI
- STEP 4 . Click OK (Figure 3-6)

DMZ Interface	DMZ_TRANSPARENT		
IP Address	0.0.0.0		
Netmask	0.0.0		
Enable	🗵 Ping	HTTP	
			OK Cancel

Figure3-6 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 ALL7007 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	Example	Page
	Situation		
Ex1	LAN	Under DHCP circumstances, assign the specific IP	57
		to static users and restrict them to access FTP net	
		service only through policy.	
Ex2	LAN Group	Set up a policy that only allows partial users to	60
	WAN	connect with specific IP (External Specific IP)	

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

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

- Click **New Entry** button (Figure 4-1)
- 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** (Figure 4-2)

Modify Address				
Name	Rayearth			
IP Address	192.168.3.2			
Netmask	255.255.255.255			
MAC Address	00:01:80:41:D0:AE Clone MAC Address			
☑ Get static IP address from DHCP Server.				
		OK Cancel		

Figure4-1 Setting LAN Address Book WebUI

Name	IP / Netmask	MAC Address	Configure	
Inside_Any	0.0.0/0.0.0		In Use	
Rayearth	192.168.3.2/255.255.255.255	00:01:80:41:D0:AE	Modify Remove	
New Entry				

Figure 4-2 Complete the Setting of LAN

STEP 2 . Adding the following setting in Outgoing Policy: (Figure 4-3)

Modify Policy	
Source Address	Rayearth 🔽
Destination Address	Outside_Any 💌
Service	FIP
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	🗆 HTTP / WEBMAIL 🗖 FTP
Authentication User	None
Schedule	None -
Tunnel	None -
MAX. Concurrent Sessions	0:means unlimited)
QoS	None -
	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	2								Modify Remove	To 1 🗖
tion Linty												

Figure4-4 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 ALL7007 to fill out the user's MAC

Address automatically.

In LAN of Address function, the ALL7007 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		In Use
Rayearth	192.168.1.2/255.255.255.255	00:01:80:41:D0:AE	Modify Remove
Josh	192.168.1.4/255.255.255.255		Modify Remove
SinSan	192.168.1.5/255.255.255.255	00:01:80:41:D0:88	Modify Remove
Daniel	192.168.1.7/255.255.255.255	00:01:80:41:43:17	Modify Remove
Luke	192.168.1.8/255.255.255.255		Modify Remove
	-	-	·

New Entry

Figure 4-5 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** (Figure4-7)

Add New Address Group			
Name:	TestTeam		
< Available address> Rayearth Josh SinSan Daniel Luke	👯 Remove Add 🛛 🔅	< Selected address> Rayearth Josh SinSan	
		OK Cancel	

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

Name	Member	Configure			
TestTeam	Rayearth, Josh, SinSan	Modify Remove			
New Entry					

Figure 4-7 Complete Adding LAN Address Group

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

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

- Click **New Entry** (Figure 4-8)
- Enter the following data (Name, IP Address, Netmask)
- Click **OK** (Figure 4-9)

Add New Address			
Name	Yahoo		
IP Address	202.1.137.21		
Netmask	255.255.255.255		

OK Cancel

#### Figure 4-8 Add New WAN Address

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0	In Use
Yahoo	202.1.137.21/255.255.255.255	Modify Remove

New Entry

Figure 4-9 Complete the Setting of WAN Address

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

Add New Policy	
Source Address	TestTeam 💌
Destination Address	Yahoo
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	None 🔽
Schedule	None 🗸
Tunnel	None 🗸
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None
	OK Cancel

Figure4-10 To Exercise Address Setting in Policy

Source	Destination	Service	Action	Option	Configure	Move
TestTeam	Yahoo	ANY	1		Modify Remove	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 ALL7007 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	Any Service
TCP	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	UDP Service, For example : IKE, DNS, NTP, IRC, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP,etc.
ICMP	ICMP Service, Foe example : PING, TRACEROUTEetc.

#### 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	Example	Page
	Situation		
Ex1	Custom	Allow external user to communicate with internal	67
		user by VoIP through policy. (VoIP Port: TCP	
		1720, TCP 15325-15333, UDP 15325-15333)	
Ex2	Group	Setting service group and restrict the specific	71
		users only can access to service resource that	
		provided by this group through policy. (Group:	
		HTTP, POP3, SMTP, DNS)	

Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15325-15333, UDP 15325-15333)

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		In Use
VoIP_01	192.168.1.2/255.255.255.255		Modify Remove
VoIP_02	192.168.1.3/255.255.255.255		Modify Remove
VoIP_03	192.168.1.4/255.255.255.255		Modify Remove
VoIP_04	192.168.1.5/255.255.255.255		Modify Remove
	-		

New Entry

Figure 5-1 Setting LAN Address Book WebUI

Name	Member	Configure
VoIP_Group	VoIP_01, VoIP_02, VoIP_03	Modify Remove
	New Entry	

Figure 5-2 Setting LAN Group Address Book WebUI

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

- Click **New Entry** (Figure 5-3)
- Service Name: Enter the preset name VoIP
- Protocol#1 select TCP, need not to change the Client Port, and set the Server Port as: 1720:1720
- Protocol#2 select TCP, need not to change the Client Port, and set the Server Port as: 15328:15333
- Protocol#3 select UDP, need not to change the Client Port, and set the Server Port as: 15328:15333
- Click **OK** (Figure 5-4)

Мо	Modify User Defined Service						
Service NAME :		VoIP_Service					
#	Protocol	Client Port	Server Port				
1	⊙ TCP ◯ UDP ◯ Other 🧉	0 : 65535	1720 : 1720				
2	⊙ TCP ◯ UDP ◯ Other 🧉	0 : 65535	15328 : 15333				
3	○ TCP	0 : 65535	15328 : 15333				
4	୦ TCP ୦ UDP ☉ Other 🔍	0 : 0	0:0				
5	◯ TCP ◯ UDP ☉ Other 🔍	0 : 0	0:0				
6	◯ TCP ◯ UDP ☉ Other 🔍	0 : 0	0:0				
7	◯ TCP ◯ UDP ☉ Other 🔍	0 : 0	0:0				
8	◯ TCP ◯ UDP ☉ Other 🔍	0 : 0	0 : 0				

OK Cancel

Figure 5-3 Add User Define Service

Service name	Protocol	Client Port	Server Port	Configure			
VoIP_Service	тср	0:65535	1720:1720	Modify Remove			
New Entry							

Figure 5-4 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. (Figure 5-5)

Virtual Server Real IP 172.19.20.11					
Service	WAN Port	Server Virtual IP	Configure		
VoIP_Service	From-Service (Custom)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	Modify Remove		
New Entry					



#### STEP 4 . Compare Virtual Server to Incoming Policy. (Figure 5-6)

Source	Destination	Service	Action	0	pti	on	Configure	Move
Outside_Any	Virtual Server 1 (172.19.20.11)	VoIP_Service	6				Modify Remove	To 1 🗖
New Entry								

Figure 5-6 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_Service	<b>V</b>		Modify Remove	To 1 🗖	
New Entry							
	New Entry						

Figure 5-7 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

ame:	Main_ Service	
< Available service> ANY AFPoverTCP AOL BGP DNS FINGER FTP GOPHER HTTP HTTPS IKE IMAP InterLocator IRC	Kemove Add	< Selected service> DNS HTTP POP3 SMTP

■ Click **OK** (Figure 5-9)

Figure 5-8 Add Service Group

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

Figure 5-9 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	Rayearth, Josh, SinSan	Modify Remove
	New Entry	

Figure 5-10 Setting Address Book Group

#### STEP 3 . Compare Service Group to Outgoing Policy. (Figure 5-11)

Inside_Any Outside_Any M	Main_Service	1						Г		
					Modify Remove	10 🗠 💌				
New Entry										

Figure 5-11 Setting Policy

## **Chapter 6**

# Schedule

In this chapter, the ALL7007 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.



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)

dule Nar	ne	WorkingTime				
	Week Day	Period				
	Monday	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	Modify Remove						
New Entry							

Figure 6-2 Complete the Setting of Schedule

#### STEP 2 . Compare Schedule with Outgoing Policy (Figure 6-3)

Source	Destination	Service	Action	Option				Configure	Move
Inside_Any	Outside_Any	ANY	2			0		Modify Remove	To 1 🗖
New Entry									

Figure 6-3 Complete the Setting of Comparing Schedule with Policy

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 ALL7007 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The ALL7007 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** 



Figure 7-2 the Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

# Define the required fields of QoS

#### WAN:

Display WAN network

#### 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 one QoS examples in this chapter:

No	Suitable	Example	Page
	Situation		
Ex1	QoS	Setting a policy that can restrict the user's	81
		downstream and upstream bandwidth.	

# 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 WAN.
- Select **QoS Priority**
- Click **OK** (Figure7-4)

Modify QoS		
Name	Policy_QoS	
	·	
Downstream Bandwidth	Upstream Bandwidth	QoS Priority
G.Bandwidth = 200 Kbps	G.Bandwidth = 200 Kbps	Middle
M.Bandwidth = 400 Kbps	M.Bandwidth = 400 Kbps	HIRODE -
		OK Cancel

#### Figure 7-3 QoS WebUI Setting

Name	Downstream Bar	ndwidth	Upstream Ban	dwidth	Priority	Configure		
Policy_QoS	G.Bandwidth = M.Bandwidth =	200Kbps 400Kbps	G.Bandwidth = M.Bandwidth =	200 Kbps 400 Kbps	Middle	Modify Remove		
New Entry								

Figure 7-4 Complete the QoS Setting

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

Modify Policy	
Source Address	Inside_Any 🔽
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	🗆 Enable
IDP	🗆 Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	None -
Schedule	None -
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Policy_QoS 💌

OK Cancel

Figure 7-5 Setting the QoS in Policy

Source	Destination	Service	Action	Option	Configure	Move		
Inside_Any	Outside_Any	ANY	2		Modify Remove	To 1 🗖		
New Entry								

Figure7-6 Complete Policy Setting

## **Chapter 8**

# 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 ALL7007 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 ALL7007 authentication. (Have to setup the Authentication first)
  - Authentication Port: The internal user have to pass the authentication to access to the Internet when enable ALL7007.
  - 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)

Authentication Management			
Authentication Port	82		
Re-Login if Idle	30	Minutes	
Re-Login after user login successfully	0	Hours (0: means unli	imited)
Disallow Re-Login if the auth user has login	n		
URL to redirect when authentication succeed	http://www	/.allnet.de/	
Messages to display when user login			
You must pass the authentication first access to Internet!	the	×	
		ОК	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)



Figure 8-3 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 ALL7007 and RADIUS Server

#### 802.1xRADIUS:

■ The Authentication to RADIUS Server of wireless network

We set up four Authentication examples in this chapter:

No	Suitable	Example	Page
	Situation		
Ex1	Auth User	Setting a specific user to connect with external	89
		network only before passing the authentication	
		of policy.	
		(Adopt the built-in Auth User Function)	
Ex2	RADIUS	Setting the users to connect with external	93
		network only before passing the authentication	
		of policy.	
		(Adopt the external RADIUS Server built-in	
		Windows 2003 Server Authentication)	
Ex3	POP3	Setting the users to connect with external	114
		network only before passing the authentication	
		of policy. (Adopt the external POP3 Server	
		Authentication)	

## 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		In Use				
user_01	192.168.1.2/255.255.255.255	00:01:80:41:D0:AE	Modify Remove				
New Entry							

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 ALL7007.

#### 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-U	ser
Authentication-User Name	guest
Password	****
Confirm Password	****
	OK Cancel

Figure8-5 Add New Auth-User WebUI

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

Modify Policy	
Source Address	user_01
Destination Address	Outside_Any 💌
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	guest 💌
Schedule	None -
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

OK Cancel

#### Figure8-6 Auth-User Policy Setting

Source De	stination	Service	Action	Option		Option Configure		Mo	ve				
user_01 Ou	utside_Any	ANY	N				<u></u>				Modify Remove	То	1 🗸

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) to logout (Figure8-9)

	User Login	
User Authentication		
User Name		
Password		
		OK

#### Figure 8-8 Access to Internet through Authentication WebUI

🖉 LOGOUT Authentication-User - Microsoft Internet .	Explorer						
Please click on this	button to logout						
LOGOUT Authe	ntication-User						
or enter this url http://192.168.1.1:82/logout.html							
to logout of your currently authenticated session.							

Figure8-9 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 (Figure 8-10)

onents of Windows XP.	Ĩ
it, click the checkbox, A sh istalled. To see what's inclu	aded box means that only ded in a component, click
	0.0 MB 🔺
	13.2 MB
	0.3 MB
d Print Services	0.0 MB
	OOMB
and a second second second second	ated services and protocols.
	nents of Windows XP. t, click the checkbox, A sh istalled. To see what's inclu

Figure8-10 Add Windows Components WebUI

### STEP 3 . Choose Internet Authentication Service (IAS) (Figure8-11)

etworking S	ervices			×	
To add or ren of the compo Sub <u>c</u> ompone	nove a component nent will be Pasta rits of Networkin	ent, click the check alled. To see what's ng Services:	box. A shaded box r included in a compo	neans that only part nent, click Details.	
🕑 🚚 Doma	ain Name System	n (DNS)		1.6 MB 🔼	
🗹 🦲 Dyna	mic Host Config	CP)	0.0 MB		
🗹 曼 Intern	net Authenticatio	n Service		0.0 MB	
RPC BRPC	over HTTP Pro		0.0 MB		
🗹 🛄 Simpl	e TCP/IP Servi		0.0 MB		
🗹 👼 Wind	ows Internet Na	me Service (WINS)		0.9 MB	
Description:	Enables authe users, IAS sup	ntication, authorizati ports the RADIUS p	ion and accounting ( rotocol.	of dial-up and VPN	
Total disk spa	ace required:	17.2 MB		Details	
Space availa	ble on disk:	7888.2 MB			
			OK	Cancel	

Figure8-11 Add New Internet Authentication Services WebUI

STEP 4 . Click [Start] → [Control Panel] → [Administrative Tools], Choose [Internet Authentication Service] (Figure8-12)



Figure8-12 Choose Internet Authentication Service

### STEP 5 . Press right button on RADIUS Clients and choose New RADIUS Client (Figure8-13)

🐤 Internet Auther	ntication Service				- 🗆 🗵	
Eile Action View	<u>H</u> elp					
🗢 🔶 🗈 🖬	n 🛛 🔁 😰					
P Internet Authentio	cation Service (Local)	Friendly Name	Address	Protocol	Client-'	
Remote Acce     Remote Acce     Remote Acce     Connection F	New RADIUS Client		There are no items to sl			
	New 1					
	⊻iew •	•				
	Refresh Export <u>L</u> ist					
	Help					
		•			Ŀ	
New Client						

Figure8-13 Add New RADIUS Client

# STEP 6. Enter the Name and Client Address (also the ALL7007 IP) (Figure 8-14)

Type a friendly name and	d either an IP Address or DNS	name for the client.
Eriendly name:	254	
Client address (IP or DN	5);	
172.19.1.254		⊻erify

Figure8-14 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 ALL7007) (Figure8-15)

endor of the RADIUS client.	
<u>Client-Vendor:</u>	
RADIUS Standard	
<u>S</u> hared secret:	******
Confirm shared secret:	XXXXXXX
Bequest must contain the	Message Authenticator attribute
Todaes mas condition	

Figure8-15 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. (Figure8-16)

Internet Authentication !	Service				- 🗆 ×
<u>File Action View H</u> elp					
⇔ → 🗈 🖬 🔂 🖏	ß				
Internet Authentication Serv	ice (Local)	Name		Order	
ADIUS Clients     Remote Access Logging     Remote Access Policies		Connections to Connections to	o Microsoft Routing and Remote other access servers	1 2	
🗄 🍎 Connection Request Pr	New Remot	e Access <u>P</u> olicy			
	New	F			
	⊻iew	Þ			
Refresh Export List					
	Help				
New Remote Access Policy			i) (	j.	

Figure8-16 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. (Figure8-17)

w Remote Acce	ss Policy Wizard	
Policy Configu The wizard o	ration Method an create a typical policy, or you can create a custom policy.	Ø
How do you v	vant to set up this policy?	
	e wizard to set up a typical policy for a common scenario	
C Set up	a custom policy	
Type a name t Policy name:	hat describes this policy. Radius	
	Example: Authenticate all VPN connections.	
	Const Naves	Canool

Figure8-17 Add Remote Access Policy and Name

# STEP 10 . Select Ethernet (Figure8-18)

New Remote Access Policy Wizard	x
Access Method Policy conditions are based on the method used to gain access to the network.	
Select the method of access for which you want to create a policy.	
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.	
C Dial-up	
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.	
C Wireless	
Use for wireless LAN connections only.	
C Ethernet	
Use for Ethernet connections, such as connections that use a switch.	
	_
< Back Next> Cancel	1
	-

Figure8-18 Add New Remote Access Policy Method

# STEP 11 . Choose User (Figure8-19)

w Remote Access Policy Wizard	
User or Group Access You can grant access to individual us groups.	ers, or you can grant access to selected
Grant access based on the following:	
<ul> <li>User</li> <li>User access permissions are specifie</li> </ul>	ed in the user account.
<ul> <li><u>Group</u></li> <li>Individual user permissions override g</li> <li>Group name</li> </ul>	group permissions.
	Add
	Elemove
	<u>K</u> ack <u>Next</u> Lancel

Figure8-19 Add New Remote Access Policy of User or Group Access

### STEP 12 . Select MD5-Challenge (Figure8-20)

w Remote Access Policy Wizard	
Authentication Methods EAP uses different types of security of	devices to authenticate users.
Select the EAP type for this policy.	
<u>⊥</u> ype:	
MD5-Challenge	Configure
	< <u>Back</u> Next> Lancel

Figure8-20 Authentication Methods of Adding New Remote Access Policy

# STEP 13 . Press the right button on Radius and choose Properties. (Figure 8-21)

PInternet Authentication Service					- 0 ×
<u>File Action View H</u> elp					
⇔ → 🖻 🖬 🗙 📽 🗔 😢 -	e 🔹				
Internet Authentication Service (Local)     ADIUS Clients     Remote Access Logging     W Remote Access Policies	Name			0 A	
	Connections	Mave Up Move D <u>o</u> wn	and Remote	1	
E Connection Request Processing		<u>D</u> elete Rena <u>m</u> e	Brs	8 <b>0</b> 0	
		Properties			
		Help			
Opens property sheet for the current selection	6.).				

Figure8-21 Internet Authentication Service Setting WebUI

# STEP 14 . Select Grant remote access permission and Remove the original setting, click Add to add a new one. (Figure8-22)

adius Properties				<u>? ×</u>
Settings				
Specify the cond	litions that conne	ection request:	s must match.	
Policy conditions	c<			
NAS-Port-Type	matches "Etherr	net"		
A <u>d</u> d	<u>E</u> dit	 <u>R</u> emove	1	
If connection rec associated profile	uests match the e will be applied	conditions sp to the connec	ecified in this polic tion.	cy, the
Edit Protile				
Unless individua policy controls a	access permiss	ions are specil work.	ied in the user pro	ofile, this
If a connection r	equest matches	the specified (	conditions;	
C Deny remote	access permissi	ion		
<ul> <li>Grant remote</li> </ul>	access permiss	ion		
		aaad		
	1	02	Canada 11	Analu
		UN	Lance	SPPPy

Figure8-22 RADIUS Properties Settings

Name	Description	
Called-Station-Id	Specifies the phone number dialed by the us	51
Calling-Station-Id	Specifies the phone number from which the	c
Client-Friendly-Name	Specifies the friendly name for the RADIUS	с
Client-IP-Address	Specifies the IP address of the RADIUS clie	r
Client-Vendor	Specifies the manufacturer of the RADIUS p	24
Day-And-Time-Restric	Specifies the time periods and days of week	2
Framed-Protocol	Specifies the protocol that is used.	
MS-RAS-Vendor	Description not yet defined	
NAS-Identifier	Specifies the string that identifies the NAS the	<b>)</b> .
VAS-IP-Address	Specifies the IP address of the NAS where t	ł
NAS-Port-Type	Specifies the type of physical port that is use	31
Service-Type	Specifies the type of service that the user ha	э
Tunnel-Type	Specifies the tunneling protocols used.	
Windows-Groups	Specifies the Windows groups that the user	t-
		1

Figure8-23 Add New RADIUS Attribute

### STEP 16 . Add Authenticate Only from the left side. (Figure8-24)

Available types:		Selected types:
Administrative Call Check Callback Administrative Callback Framed Callback Login Callback Nas Prompt Framed Login NAS Prompt Dutbound	Add >> << <u>R</u> emove	Authenticate Only
<u>•</u> •		OK Cancel

Figure8-24 Add RADIUS Service-Type

# STEP 17 . Press Edit Profile button and select Authentication and select Unencrypted authentication (PAP, SPAP) (Figure 8-25)

Radius Properties <mark>E</mark>	dit Dial-in Profile		?>	<				
Settings	Dial-in Constraints Authentication	IP Encryption	Multilink Advanced					
Policy <u>c</u> onditions	Select the authentication m	iethods you want to allow	for this connection.					
	EAP Methods	Suthentication version 2 (	MS-CHAP v2)					
	User can char	ge password after it has i	expired					
Add	Microsoft Encrypted	Authentication (MS-CHAF	2)	l				
If connection rec associated profile	L Uger can char Encrypted authentica	ige password after it has i ation (CHAP)	expired					
Edit Profile	Unencrypted authent	I Unencrypted authentication (PAP, SPAP)						
Unless individual policy controls ac If a connection n © Deny remote	Allow clients to connect without negotiating an authentication method.							
○ <u>G</u> rant remote								
		OK Ca	ancel Apply	1				

Figure8-25 Edit DADIUS Dial-in Property
STEP 18 . Add Auth User. Click [Start] → [Setting]→ [Control Panel] → [Administrative Tools], Choose [Computer Management] (Figure8-26)



Figure8-26 Enter Computer Management

STEP 19. Press the right button on the Users and select New User. (Figure 8-27)



Figure8-27 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 (Figure 8-28)

RADIUS Server	
Enable RADIUS Server Authentication	
RADIUS Server IP 172.19.250.10	
RADIUS Server Port 1812	
Shared Secret master	
Enable 802.1x RADIUS Server Authentication	
	OK Cancel

Figure8-28 Setting RADIUS Server

STEP 22 . Add Radius User in Auth User Group of Authentication.

(Figure8-29)

New Authentication Group							
Name:	Radius						
< Available Authentication User> (Radius User) (POP3 User)	K Remove	< Selected Authentication User> (Radius User)					
		OK Cancel					

Figure8-29 Add New RADIUS Auth Group

## STEP 23 . Add a policy of Auth User Group (RADIUS) that set by STEP 22 in Outgoing Policy. (Figure8-30, 8-31)

Modify Policy	
Source Address	user_01
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	🗆 Enable
IDP	Enable
Content Blocking	🗆 Enable
Anti-Virus	□ HTTP / WEBMAIL □ FTP
Authentication User	Radius 💌
Schedule	None
Tunnel	None 🗸
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

OK Cancel

Figure8-30 RADIUS Authentication Policy Setting WebUI

user_01 Outside_Any ANY 🏏 🛛 🎤 🛛 Modify Remove To া 🚽	Source	Destination	Service	Action	Option	Configure	Move
	user_01	Outside_Any	ANY	1	<i>~</i>	Modify Remove	To 1 🗖

New Entry

Figure8-31 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 ALL7007. (Figure8-32)

User Login						
User Authentication						
User Name						
Password						
	ок					

Figure 8-32 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 (Figure 8-33)

POP3 Server		
Enable POP3 Server Authentication		
POP3 Server (IP or Domain Name)	192.168.139.10	
POP3 Server Port	110	
		OK Cancel

Figure8-33 POP3 Server Setting WebUI

STEP 2 . Add POP3 User in New Authentication Group. (Figure 8-34)

Modify Authentication-User							
Name:	POP3_Auth						
< Available Authentication User> (Radius User) (POP3 User)	K Remove	< Selected Authentication User> (POP3 User)					
		OK Cancel					

Figure8-34 Add New POP3 User WebUI

## STEP 3 . Add a policy of Authentication User Group that set in STEP2 in Outgoing Policy. (Figure 8-35, 8-36)

Add New Policy	
Source Address	Inside_Any 🗸
Destination Address	Outside_Any 💌
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	□ HTTP / WEBMAIL □ FTP
Authentication User	POP3_Auth
Schedule	None 💌
Tunnel	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

OK Cancel

Figure8-35 POP3 Server Authentication Policy Setting

Inside_Any Outside_Any ANY 🏏 🛛 🔑 Modify Remove To 1	Source	Destination	Service	Action		0	otio	n		Configure	Move
	Inside_Any	Outside_Any	ANY	2			P	•		Modify Remove	To 1 🗖

New Entry

Figure8-36 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 ALL7007: (Figure8-37)

	User Login
User Authentication	
User Name	
Password	
	ОК

Figure8-37 the Authentication WebUI

### **Content Blocking**

Content Blocking 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  $(\sim \text{and } *)$ .

**[Script Blocking]**: The access authority of Popup, ActiveX, Java, Cookies

**[P2P Blocking]:** The authority of sending files by eDonkey, eMule, BitTorrent, and WinMX

**[IM Blocking]**: To restrict the authority of receiving video, file and message from MSN Messenger, Yahoo Messenger, ICQ, QQ, and Skype.

**[ 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

### **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	Example	Page
	Situation		
Ex1	URL Blocking	Restrict the Internal Users only can access to	121
		some specific Website	
Ex2	Script	Restrict the Internal Users to access to Script	124
	Blocking	file of Website.	
Ex3	P2P Blocking	Restrict the Internal Users to access to the	126
		file on Internet by P2P.	
Ex4	IM Blocking	Restrict the Internal Users to send message,	128
		files, video and audio by Instant Messaging.	
Ex5 Download		Restrict the Internal Users to access to video,	130
	Blocking	audio, and some specific sub-name file from	
		http protocol directly.	

# Restrict the Internal Users only can access to some specific Website

### **%URL Blocking:**

<u>Symbol:</u>  $\sim$  means open up; \* means metacharacter

<u>Restrict not to enter specific website:</u> Enter the 「complete domain name」 or 「key word \_of the website you want to restrict in **URL String**. For example: <u>www.kcg.gov.tw</u> or gov.

Only open specific website to enter:

- 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.
- 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 Blocking 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 Blocking Table

### STEP 2 . Add a Outgoing Policy comparing to Content Blocking function:

(Figure9-2)	
Modify Policy	
Source Address	Inside_Any 🗸
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	🔽 Enable
Anti-Virus	HTTP / WEBMAIL  FTP
Authentication User	None 🗸
Schedule	None
Tunnel	None 💌
MAX. Concurrent Sessions	0:means unlimited)
QoS	None 🗸
-	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										
Γ	Inside_Any Outside_Any ANY 🧭 📮 🛛 Modify Remove To া									
New Entry										
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)

ActiveX Blocking	
🗹 Cookie Blocking	
	OK Cancel
	☑ ActiveX Blocking ☑ Cookie Blocking

Figure9-4 Script Blocking WebUI

#### STEP 2 . Add a new Outgoing Policy comparing to Content Blocking function:

(Figure9-5)	
Modify Policy	
Source Address	Inside_Any 🔽
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	HTTP / WEBMAIL  FTP
Authentication User	None -
Schedule	None
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None 🔽
	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 🖌									
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)

Peer-to-Peer Application Blocking	
🗹 eDonkey Blocking	
🗹 Bit Torrent Blocking	
✓ WinMX Blocking	
	OK Cancel



### STEP 2 . Add a new Outgoing Policy comparing to Content Blocking function:

(Figure9-8)	
Modify Policy	
Source Address	Inside_Any 🗸
Destination Address	Outside_Any -
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	🗆 Enable
IDP	🗆 Enable
Content Blocking	🗹 Enable
Anti-Virus	HTTP / WEBMAIL  FTP
Authentication User	None -
Schedule	None
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None 🗸
	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 To 🖅									
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 comparing to Content Blocking function:

(Figure9-11)	
Modify Policy	
Source Address	Inside_Any 💌
Destination Address	Outside_Any 💌
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	□ HTTP / WEBMAIL □ FTP
Authentication User	None 🗸
Schedule	None
Tunnel	None 🔽
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None 🗸
-	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)

Inside_Any Outside_Any ANY V States	Source Destination Service Action Option Configure Move									
Num Falar	Inside_Any Outside_Any ANY 🖌 🗧 🕻 Modify Remove To 🗔									
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 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)

Download Blocking			
All Types Blocking			
Audio and Video Types I	Blocking		
Extension Blocking			
.exe	🗖 .zip	🗖 .rar	
🗖 .iso	🗖 .bin	🗖 .rpm	
.doc	□ .xl?	🗖 .ppt	
🗖 .pdf	🗖 .tgz	🗖 .gz	
🗖 .bat	llb. 🗖	🗖 .hta	
.scr	.vb?	🗖 .wps	
🗖 .pif			
			OK Cancel

Figure9-13 Download Blocking WebUI

#### STEP 2 . Add a new Outgoing Policy comparing to Content Blocking function:

(Figure9-14)

Modify Policy	
Source Address	Inside_Any 🗸
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	🗆 Enable
Content Blocking	Enable
Anti-Virus	HTTP / WEBMAIL  FTP
Authentication User	None -
Schedule	None
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -
	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		Option Configure		Configure	Move
Inside_Any	Outside_Any	ANY	1			Modify Remove	To 1 🗖		
New Entry									

Figure9-15 Complete Download Blocking Policy Setting

### Chapter 10

### **Virtual Server**

The real IP address provided from ISP is always not enough for all the users when the system manager applies the network connection from ISP. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through ALL7007'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 ALL7007's Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the ALL7007's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the ALL7007 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 ALL7007's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the ALL7007. 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	Example	Page
	Situation		
Ex1	Mapped IP	Make a single server that provides several	136
		services such as FTP, Web, and Mail, to	
		provide service by policy.	
Ex2	Virtual Server	Make several servers that provide a single	140
		service, to provide service through policy by	
		Virtual Server. (Take Web service for example)	
Ex3	Virtual Server	The external user use VoIP to connect with	143
		VoIP of LAN. (VoIP Port: TCP 1720, TCP	
		153210-15333, UDP 153210-15333)	
Ex4	Virtual Server	Make several servers that provide several	147
		same services, to provide service through	
		policy by Virtual Server. (Take HTTP, POP3,	
		SMTP, and DNS Group for example)	

### Preparation

Apply for two ADSL that have static IP (WAN static IP is 61.11.11.10~ 61.11.11.14)

# 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)

Name	IP / Netmask	MAC Address	Configure					
Inside_Any 0.0.0.0/0.0.0			In Use					
Mail_Server	192.168.1.100/255.255.255.255	00:01:80:41:D0:AE	Modify Remove					
New Entry								

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	Assist
Map To Virtual IP	192.168.1.100	
		OK Cancel

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					
Mail_Service	DNS,HTTP,POP3	Modify Remove					
Main_Service	DNS,FTP,HTTP	Modify Remove					
New Entry							



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

Source	Destination	Service	Action	0	Option		Option			Configure	M	ove
Outside_Any	Mapped IP(61.11.11.12)	Main_Service	2	✓		Modify Remove	То	1 🗸				
New Likty												

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			
Inside_Any	Outside_Any	Mail_Service	<b>V</b>		Modify Remove	To 1 🗖			
New Entry									

Figure10-5 Complete the Outgoing Policy

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



Server : 192.168.1.100

Support FTP, Web, and Mail Services

Figure 10-6 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 61.11.11.12 (click Assist for assistance)
- Click **OK** (Figure10-7)

Add New Virtual Server IP		
Virtual Server Real IP	61.11.11.12 <u>Assist</u>	
		OK Cancol
		Cancer

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	61.11.11.12						
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						

Figure 10-8 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		Option		Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	HTTP(8080)	٧					Modify Remove	To 1 🔽

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 153210-15333, UDP 153210-15333)

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			In Use				
VoIP	192.168.1.100/255.255.255.255		Modify Remove				
New Entry							

Figure10-11 Setting LAN Address WebUI

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

Service name	ervice name Protocol Clie		Server Port	Configure					
VoIP_Service	e TCP 0:65535		1720:1720	Modify Remove					
New Entry									

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)

OK Cancel

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	61.11.11.12
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	
-	

OK Cancel

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		Option		Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	VoIP_Service	6					Modify Remove	To 1
New Entry									



**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		Option		Configure	Move	
VoIP	Outside_Any	VoIP_Service	V						Modify Remove	To 1 🗾
New Entry										

Figure 10-16 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)



Figure 10-17 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		In Use
Server_01	192.168.1.101/255.255.255.255		In Use
Server_02	192.168.1.102/255.255.255.255		In Use
Server_03	192.168.1.103/255.255.255.255		In Use
Server_04	192.168.1.104/255.255.255.255		In Use

New Entry

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



#### 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				
Mail_Service	DNS,HTTP,POP3	Modify Remove				
Main_Service	DNS,FTP,HTTP	Modify Remove				
New Entry						

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 61.11.11.12 (click Assist for assistance)
- Click **OK** (Figure10-21)

12 Assis	
	1
	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	n
Virtual Server Real IP	61.11.11.12
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	C	Option			Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	Main_Service	6				Modify Remove	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)

		OCTAICC	Action	Option Configure		Move	
Sever_Group	Outside_Any	Mail_Service	<b>V</b>		Modify Remove	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

## Chapter 11

# VPN

The ALL7007 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 ALL7007.

**(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



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

# Define the required fields of VPN:

## RSA:

■ A public-key cryptosystem for encryption and authentication.

## **Preshared Key:**

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

## ISAKMP (Internet Security Association Key Management Protocol):

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

#### Main Mode:

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

### Aggressive mode:

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

### AH (Authentication Header):

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

### ESP (Encapsulating Security Payload):

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

## **DES (Data Encryption Standard):**

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

## Triple-DES (3DES):

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

## AES (Advanced Encryption Standard):

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

### NULL Algorithm:

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

### SHA-1 (Secure Hash Algorithm-1):

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

#### MD5:

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

### **GRE/IPSec:**

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

# **Define the required fields of IPSec Function**

#### i:

To display the VPN connection status via icon •

Chart		9	맵
Meaning	Not be applied	Disconnect	Connecting

#### Name:

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

#### **Gateway IP:**

■ The WAN interface IP address of the remote Gateway.

#### **IPSec Algorithm:**

To display the Algorithm way.

#### **Configure:**

 Click Modify to change the argument of IPSec; click Remove to remote the setting. (Figure11-1)

i	Name	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

#### i:

To display the VPN connection status via icon •

Chart		9	<b>2</b>
Meaning	Not be applied	Disconnect	Connecting

#### **User Name:**

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

#### **Client IP:**

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

#### Uptime:

Display the connection time between PPTP Server and Client.

#### **Configure:**

 Click Modify to modify the PPTP Server Settings or click Remove to remove the setting (Figure 11-2)

PPTP Server ( Disable ) : Client IP Range : 192.119.58.1-254 Modify							
i.	User Name	Client IP	Uptime	Configure			
New Entry							

Figure11-2 PPTP Server WebUI

# **Define the required fields of PPTP Client Function**

#### i:

To display the VPN connection status via icon •

Chart		Щ.	<b>2</b>
Meaning	Not be applied	Disconnect	Connecting

#### User Name:

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

#### Server IP or Domain Name:

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

#### **Encryption:**

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

#### Uptime:

Displays the connection time between PPTP Server and Client.

#### Configure:

 Click Modify to change the argument of PPTP Client; click Remove to remote the setting. (Figure 11-3)



Figure11-3 PPTP Client WebUI

# Define the required fields of Tunnel Function

#### i:

■ To display the VPN connection status via icon ∘

Chart		9	<b>1</b>
Meaning	Not be applied	Disconnect	Connecting

#### Name:

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

#### Source Subnet:

Displays the Source Subnet.

#### **Destination Subnet:**

Displays the Destination Subnet.

#### **IPSec / PPTP:**

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

#### Configure:

 Click Modify to change the argument of VPN Tunnel; click Remove to remote the setting.(Figure11-4)

i Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	(	New Entry		

Figure11-4 VPN Tunnel Web UI

We set up two VPN examples in this chapter:

No.	Suitable	Example	Page
	Situation		
Ex1	IPSec Autokey	Setting IPSec VPN connection between two	159
		ALL7007	
Ex2	РРТР	Setting PPTP VPN connection between two	165
		ALL7007	

## Setting IPSec VPN connection between two ALL7007

#### 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 ALL7007 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 ALL7007 192.168.10.1. Follow the steps below:

**STEP 1.**Enter the default IP of Gateway of Company A's ALL7007, 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure11-5)

i	Name	Gateway IP	IPSec Algorithm	Configure	
New Entry					

Figure11-5 IPSec Autokey WebUI

STEP 2.In the list of IPSec Autokey, fill in Name with VPN\_A. (Figure11-6)

Necessary Item	
Name	VPN_A

Figure11-6 IPSec Autokey Name Setting

### STEP 3.Select Remote Gateway-Fixed IP or Domain Name In To Destination

list and enter the IP Address.(Figure11-7)

To Destination		
<ul> <li>Remote Gateway Fixed IP or Domain Name</li> </ul>	211.22.22.22	
C Remote Gateway or Client Dynamic IP		

Figure11-7 IPSec To Destination Setting

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

Authentication Method	Preshare 🗸
Preshared Key	123456789

Figure11-8 IPSec Authentication Method Setting

STEP 5.Select ISAKMP Algorithm in Encapsulation list. Choose the Algorithm when setup connection. Please select ENC Algorithm (3DES/DES/AES), AUTH Algorithm (MD5/SHA1), and Group (GROUP1, 2,5). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group. (Figure11-9)

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

Figure11-9 IPSec Encapsulation Setting

STEP 6. You can choose Data Encryption + Authentication or Authentication

Only to communicate in IPSec Algorithm list:

ENC Algorithm: 3DES/DES/AES/NULL

AUTH Algorithm: **MD5/SHA1** 

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission (Figure11-10)

IPSec Algorithm	
O Data Encryption + Authentication	
ENC Algorithm	3DES 🔽
AUTH Algorithm	MD5 V
C Authentication Only	

Figure11-10 IPSec Algorithm Setting

STEP 7.After selecting GROUP1 in Perfect Forward Secrecy, enter 3600 seconds in ISAKMP Lifetime, enter 28800 seconds in IPSec Lifetime, and selecting Main mode in Mode. (Figure11-11)

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	<sup>3600</sup> Seconds
IPSec Lifetime	28800 Seconds
Mode	• Main mode ○ Aggressive mode         • O Agg

Figure11-11 IPSec Perfect Forward Secrecy Setting

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

i.	Name	Gateway IP	IPSec Algorithm	Configure			
	VPN_A	211.22.22.22	3DES / MD5	Modify Remove			
	New Entry						

Figure11-12 Complete Company A IPSec Autokey Setting

STEP 9.Enter the following setting in Tunnel of VPN function: (Figure 11-13)

- Enter a specific Tunnel **Name**.
- From Source: Select LAN
- From Source Subnet / Mask: Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- To Destination Subnet / Mask: Enter 192.168.20.0 / 255.255.255.0.
- IPSec / PPTP Setting: Select VPN\_A.
- Select Show remote Network Neighborhood.
- Click **OK**. (Figure11-14)

New Entry Tunnel		
Name	PSec_VPN_Tunnel	
From Source	⊙LAN ○ DMZ	
From Source Subnet / Mask	192.168.10.0	1 255.255.255.0
To Destination		
To Destination Subnet / Mask	192.168.85.0	1 255.255.255.0
○ Remote Client		
IPSec / PPTP Setting	VPN_A -	
Keep alive IP :		
Show remote Network Neighborhood	bd	
		OK Cancel

Figure11-13 New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
Щ,	IPSec_VPN_Tu	192.168.10.0	192.168.85.0	VPN_A	Modify Remove

New Entry

Figure11-14 Complete New Entry Tunnel Setting

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

- Authentication User: Select All\_NET.
- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.(Figure11-16)

Add New Policy	
Source Address	Inside_Any 💌
Destination Address	Outside_Any 🗸
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	🗆 HTTP / WEBMAIL 🗖 FTP
Authentication User	All_NET -
Schedule	Schedule_1
Tunnel	IPSec_VPN_Tunnel -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	

OK Cancel

#### Figure11-15 Setting the VPN Tunnel Outgoing Policy

Source	Destination	Service	Action	Action Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Configure	M	ove
Inside_Any	Outside_Any	ANY	VPN	808		Modify Remove	То	1 🗸																								
( New Entry																																

Figure11-16 Complete the VPN Tunnel Outgoing Policy Setting

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

- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.(Figure11-18)

Add New Policy	
Source Address	Outside_Any 🔽
Destination Address	Inside_Any 💌
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	🗆 Enable
Schedule	Schedule_1
Tunnel	IPSec_VPN_Tunnel
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1 -
MAX. Concurrent Sessions ଢ୦S	0 (0:means unlimited) ହିଣ୍ଣ 🔽

OK Cancel

Figure11-17 Setting the VPN Tunnel Incoming Policy

Source	Destination	Service	Action		Ор	tion		Configure	M	ove
Outside_Any	Inside_Any(Routing)	ANY	VIPIN			Ø	8	Modify Remove	То	1 💌
New Entry										

Figure11-18 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the ALL7007 192.168.20.1. Follow the steps below:

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

WAN Interface IP / Forwarding Mode	Alias IP of Internal Interface / Netmask	Confi	igure		
211.22.22.22 / NAT	192.168.85.1 / 255.255.255.0	Modify	Remove		
New Entry					
Figure11-19 Multiple Subnet Setting					

**STEP 2.**Enter the default IP of Gateway of Company B's ALL7007, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**. (Figure11-20)

i.	Name	Gateway IP	IPSec Algorithm	Configure			
	New Entry						



STEP 3.In the list of IPSec Autokey, fill in Name with VPN\_B. (Figure 11-21)

Necessary Item		
Name	VPN_B	

Figure11-21 IPSec Autokey Name Setting

## STEP 4.Select Remote Gateway-Fixed IP or Domain Name In To Destination

list and enter the IP Address.(Figure11-22)

<ul> <li>Remote Gateway</li> <li>Fixed IP or Domain Name</li> </ul>	61.11.11.11		
C Remote Gateway or Client Dynamic IP			

Figure11-22 IPSec To Destination Setting

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

Authentication Method	Preshare -
Preshared Key	123456789

Figure11-23 IPSec Authentication Method Setting

STEP 6.Select ISAKMP Algorithm in Encapsulation list. Choose the Algorithm when setup connection. Please select ENC Algorithm (3DES/DES/AES), AUTH Algorithm (MD5/SHA1), and Group (GROUP1, 2,5). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group. (Figure11-24)

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

Figure11-24 IPSec Encapsulation Setting

**STEP 7.**You can choose Data Encryption + Authentication or Authentication

Only to communicate in IPSec Algorithm list:

ENC Algorithm: 3DES/DES/AES/NULL

AUTH Algorithm: **MD5/SHA1** 

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission. (Figure11-25)

IPSec Algorithm					
O Data Encryption + Authentication					
ENC Algorithm	3DES 🔽				
AUTH Algorithm	MD5 V				
C Authentication Only					

Figure11-25 IPSec Algorithm Setting

STEP 8.After selecting GROUP1 in Perfect Forward Secrecy, enter 3600 seconds in ISAKMP Lifetime, enter 28800 seconds in IPSec Lifetime, and selecting Main mode in Mode. (Figure11-26)

Optional Item					
Perfect Forward Secrecy	GROUP 1				
ISAKMP Lifetime	3600 Seconds				
IPSec Lifetime	28800 Seconds				
Mode	ⓒ Main mode ○ Aggressive mode				

Figure11-26 IPSec Perfect Forward Secrecy Setting

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

i.	i Name Gateway IP IPSec Algorithm Configure									
	VPN_B	61.11.11.11	3DES / MD5	Modify Remove						
New Entry										

Figure11-27 Complete Company B IPSec Autokey Setting

STEP 10.Enter the following setting in Tunnel of VPN function: (Figure 11-28)

- Enter a specific Tunnel **Name**.
- From Source: Select LAN
- From Source Subnet / Mask: Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- To Destination Subnet / Mask: Enter 192.168.10.0 / 255.255.255.0.
- IPSec / PPTP Setting: Select VPN\_B.
- Select Show remote Network Neighborhood.
- Click **OK**. (Figure11-29)

New Entry Tunnel		
Name	PSec_VPN_Tunnel	
From Source	⊙LAN ○ DMZ	
From Source Subnet / Mask	192.168.85.0	1 255.255.255.0
To Destination		
To Destination Subnet / Mask	192.168.10.0	1 255.255.255.0
○ Remote Client		
IPSec / PPTP Setting	VPN_B	
Keep alive IP :		
Show remote Network Neighborhood	bd	
		OK Cancel

Figure11-28 New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
Щ,	IPSec_VPN_Tu	192.168.85.0	192.168.10.0	VPN_B	Modify Remove

New Entry

Figure11-29 Complete New Entry Tunnel Setting

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

- Authentication User: Select All\_NET.
- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.(Figure11-31)

Add New Policy	
Source Address	Inside_Any 💌
Destination Address	Outside_Any 🗸
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	🗆 HTTP / WEBMAIL 🗖 FTP
Authentication User	All_NET -
Schedule	Schedule_1
Tunnel	IPSec_VPN_Tunnel -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

OK Cancel

#### Figure11-30 Setting the VPN Tunnel Outgoing Policy

Source	Destination	Service	Action				0	ptio	n			Configure	M	ove
Inside_Any Outside_Any ANY VIN						Modify Remove	То	1 🗸						

New Entry

Figure11-31 Complete the VPN Tunnel Outgoing Policy Setting

**STEP 12.**Enter the following setting in **Incoming Policy:** (Figure 11-32)

- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.(Figure11-33)

Outside_Any 🔽
Inside_Any -
ANY
PERMIT
🗆 Enable
🗆 Enable
Enable
Schedule_1 -
IPSec_VPN_Tunnel
0 (0:means unlimited)
Q65_1 -

OK Cancel

Figure11-32 Setting the VPN Tunnel Incoming Policy

Outside_Any     Inside_Any(Routing)     ANY     Image: Constraint of the second seco	Source	Destination	stination Service Action Option Configure						M	ove		
	Outside_Any	Inside_Any(Routing)	ANY	VPN				0	8	Modify Remove	То	1 🗸
New Entry												

Figure 11-33 Complete the VPN Tunnel Incoming Policy Setting

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



Figure11-34 IPSec VPN Connection Deployment

# Setting PPTP VPN connection between two ALL7007

#### 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 ALL7007 as flattop. Suppose Company B 192.168.20.100 is going to have VPN connection with Company A 192.168.10.100 and download the resource.

The Default Gateway of Company A is the LAN IP of the ALL7007 192.168.10.1. Follow the steps below:

**STEP 1.**Enter **PPTP Server** of **VPN** function in the ALL7007 of Company A. Select **Modify** and enable PPTP Server:

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

Modify Server Design	
O Disable PPTP	
Enable PPTP	
Encryption	
Client IP Range :	192.44.75.1 254
Auto-Disconnect if idle 🛛 mi	nutes (O: means always connected)
	OK Cancel

Figure11-35 Enable PPTP VPN Server Settings

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

**STEP 2.**Add the following settings in **PPTP Server** of **VPN** function in the ALL7007 of Company A:

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

Add New PPTP Server			
User Name:	PPTP_Connection		
Password :	****		
Client IP assigned by			
IP Range			
○ Fixed IP :			
			OK Cancel
Figure11-	36 PPTP VPN S	erver Setting	
PPTP Server (Enable, Encryption:O	N):		
Client IP Range : 192.44.75.1-254 Mo	dify		

i.	User Name	Client IP	Uptime	Configure
	PPTP_Connection	0.0.0.0		Modify Remove
			_	
		New Entry		

Figure11-37 Complete PPTP VPN Server Setting

STEP 3.Enter the following setting in Tunnel of VPN function: (Figure 11-38)

- Enter a specific Tunnel **Name**.
- From Source: Select LAN
- From Source Subnet / Mask: Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- To Destination Subnet / Mask: Enter 192.168.20.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP\_Server\_PPTP\_Connection.
- Select Show remote Network Neighborhood.
- Click **OK**. (Figure11-39)

New Entry Tunnel				
Name	PPTP_VPN_Tunnel			
From Source				
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0			
To Destination				
To Destination Subnet / Mask	192.168.20.0 / 255.255.255.0			
<ul> <li>Remote Client</li> </ul>	·			
IPSec / PPTP Setting	PPTP_Server_PPTP_Connection 💌			
Keep alive IP :				
Show remote Network Neighborhood				
	OK Cancel			

#### Figure11-38 New Entry Tunnel Setting

i.	Name	Source Subnet	<b>Destination Subnet</b>	IPSec / PPTP	Configure	
₽,	PPTP_VPN_Tun	192.168.10.0	192.168.20.0	PPTP_Ser	Modify Remove	
	New Entry					

Figure11-39 Complete New Entry Tunnel Setting

STEP 4.Enter the following setting in Outgoing Policy: (Figure 11-40)

- Authentication User: Select All\_NET.
- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.(Figure11-41)

Add New Policy	
Source Address	Inside_Any 🔽
Destination Address	Outside_Any 🗸
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	All_NET -
Schedule	Schedule_1
Tunnel	PPTP_VPN_Tunnel
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Qc&_1 -

OK Cancel

#### Figure11-40 Setting the VPN Tunnel Outgoing Policy

Source	Destination	Service	ervice Action Option		Configure	Move
Inside_Any	Outside_Any	ANY	VIPIN	20 🔍	Modify Remove	To 1 🔽
New Entry						

Figure11-41 Complete the VPN Tunnel Outgoing Policy Setting

STEP 5.Enter the following setting in Incoming Policy: (Figure 11-42)

- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.(Figure11-43)

Add New Policy	
Source Address	Outside_Any 🔽
Destination Address	Inside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	Enable
Schedule	Schedule_1
Tunnel	PPTP_VPN_Tunnel
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1 -

OK Cancel

Figure11-42 Setting the VPN Tunnel Incoming Policy

Source	Destination	Service	Action		Option		Option		ion Configure		Configure	Mov	/e
Outside_Any	Inside_Any(Routing)	ANY	VPN		08		8	Modify Remove	To 🛛	-			
		6	New Entry	1									

Figure11-43 Complete the VPN Tunnel Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the ALL7007 192.168.20.1. Follow the steps below:

**STEP 1.**Add the following settings in **PPTP Client** of **VPN** function in the ALL7007 of Company B:

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

Add New PPTP Client	
User Name:	PPTP_Connection
Password :	******
Server IP or Domain Name :	61.11.11.11 F Encryption
NAT(Connect to Windows PPTP	Server)
	OK Cancel

#### Figure 11-44 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 11-45 Complete PPTP VPN Client Setting

STEP 2.Enter the following setting in Tunnel of VPN function: (Figure 11-46)

- Enter a specific Tunnel **Name**.
- From Source: Select LAN
- From Source Subnet / Mask: Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- To Destination Subnet / Mask: Enter 192.168.10.0 / 255.255.255.0.
- IPSec / PPTP Setting: Select PPTP\_Client\_PPTP\_Connection.
- Select Show remote Network Neighborhood.
- Click **OK**. (Figure11-47)

New Entry Tunnel				
Name	PPTP_VPN_Tunnel			
From Source	⊙LAN ○ DMZ			
From Source Subnet / Mask	192.168.20.0	1 255.255.255.0		
To Destination				
To Destination Subnet / Mask	192.168.10.0	1 255.255.255.0		
C Remote Client				
IPSec / PPTP Setting	PPTP_Client_PPTP_Connection(61.1	1.11.11) 🔽		
Keep alive IP :				
☑ Show remote Network Neighborhood				
		OK Cancel		

Figure11-46 New Entry Tunnel Setting

i.	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure	
Щ,	PPTP_VPN_Tun	192.168.20.0	192.168.10.0	PPTP_Cli	Modify Remove	
	New Entry					

Figure11-47 Complete New Entry Tunnel Setting

STEP 3.Enter the following setting in Outgoing Policy: (Figure 11-48)

- Authentication User: Select All\_NET.
- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.(Figure11-49)

Add New Policy	
Source Address	Inside_Any 🗸
Destination Address	Outside_Any 🗸
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	🗆 Enable
Content Blocking	Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	
Schedule	Schedule_1 -
Tunnel	PPTP_VPN_Tunnel
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1 -

OK Cancel

#### Figure11-48 Setting the VPN Tunnel Outgoing Policy

Source	Destination	Service	Action	Option								Configure	Move	
Inside_Any	Outside_Any	ANY	VPN					se .	0	8		Modify Remove	То	1 💌

New Entry

Figure11-49 Complete the VPN Tunnel Outgoing Policy Setting
STEP 4.Enter the following setting in Incoming Policy: (Figure 11-50)

- **Schedule:** Select Schedule\_1.
- **QoS:** Select QoS\_1.
- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.(Figure11-51)

Add New Policy	
Source Address	Outside_Any -
Destination Address	Inside_Any 💌
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Schedule	Schedule_1
Tunnel	PPTP_VPN_Tunnel
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Qc&_1 🔽

OK Cancel

Figure11-50 Setting the VPN Tunnel Incoming Policy

Outside_Any     Inside_Any(Routing)     ANY     Image: Constraint of the second seco	Source	Destination	Service	Action	Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option Configure		Configure	M	ove
	Outside_Any	Inside_Any(Routing)	ANY	VPN				0	8	Modify Remove	То	1 🗸																			
New Entry																															

Figure11-51 Complete the VPN Tunnel Incoming Policy Setting

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



Figure 11-52 PPTP VPN Connection Deployment

### Policy

Every packet has to be detected if it corresponds with Policy or not when it passes the ALL7007. When the conditions correspond with certain policy, it will pass the ALL7007 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, Destination, Service, Action, WAN Port, Logging, Statistics, Content Blocking, Authentication User, Schedule, Alarm Threshold, QoS, Max. Concurrent Sessions, Quota Per Session, and Quota Per Day.Control policies decide whether packets from different network objects, network services, and applications are able to pass through the ALL7007.



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 ALL7007 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 ALL7007'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 ALL7007 (See the chart and illustration below)

Chart	Name	Illustration
	Permit all WAN network	Allow the packets that correspond with policy to
<b>1</b>	Interface	be transferred by WAN Port
×	DENIX ALI	Reject the packets that correspond with policy to
	DENT ALL	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
ģ	Logging	Enable traffic log
<b>N</b>	Statistics	Enable traffic statistics
0	Schodulo	Enable the policy to automatically execute the function
0	Schedule	in a certain time
0	Content Blocking	Enable Content Blocking

### Logging:

Record all the packets that go through policy.

### Statistics:

• Chart of the traffic that go through policy

### **Content Blocking:**

To restrict the packets that passes through the policy

### 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.

#### Move:

Every packet that passesALL7007 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 four Policy examples in this chapter:

No.	Suitable	Example	Page
	Situation		
Ex1	Outgoing	Set up the policy that can monitor the internal	189
		users. (Take Logging, Statistics, Alarm Threshold	
		for example)	
Ex2	Outgoing	Forbid the users to access to specific network.	192
		(Take specific WAN IP and Content Blocking for	
		example)	
Ex3	Incoming	The external user control the internal PC through	197
		remote control software (Take pcAnywhere for	
		example)	
Ex4	WAN to DMZ	Set a Mail Server to allow the internal and external	199
	DMZ to WAN	users to receive and send e-mail under DMZ	
	LAN to DMZ	Transparent Mode	

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

STEP 1 . Enter the following setting in Outgoing Policy:

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

Add New Policy	
Source Address	Inside_Any 🔽
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	🔽 Enable
Statistics	Enable
IDP	Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	None
Schedule	None
Tunnel	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -

**Figure12-1 Setting the different Policies** 

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

Source	Destination	Service	Action		Option		Option				Option			Option		Configure	M	ove												
Inside_Any	Outside_Any	ANY	V	Modify Remove To 1				1 🗸																						
New Entry																														

Figure12-2 Complete Policy Setting

**STEP 3**. To obtain the information in **Traffic Log** function if you want to monitor all the packets of ALL7007. (Figure12-3)

Aug 9 07:32:20 💌					
Time	Source	Destination	Protocol	Port	Disposition
Aug 9 07:32:20	207.55.238.73	192.168.1.2	TCP	1984 => 1576	V
Aug 9 07:32:19	192.168.1.2	207.55.238.73	TCP	1576 => 1984	<u>/</u>
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1631 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1704 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1604 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1603 => 80	6
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1703 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1697 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.62	TCP	1713 => 80	2
Aug 9 07:32:16	192.168.1.2	61.213.147.47	TCP	1636 => 80	2
Aug 9 07:32:10	202.43.195.101	192.168.1.2	TCP	80 => 1750	2
Aug 9 07:32:10	192.168.1.2	202.43.195.101	TCP	1750 => 80	2
Aug 9 07:32:10	192.168.1.2	202.43.195.101	TCP	1750 => 80	2
Aug 9 07:32:10	192.168.1.2	202.43.195.101	TCP	1750 => 80	2
Aug 9 07:32:10	202.43.195.101	192.168.1.2	TCP	80 => 1750	2
Aug 9 07:32:10	202.43.195.101	192.168.1.2	TCP	80 => 1750	2
Aug 9 07:32:10	202.43.195.101	192.168.1.2	TCP	80 => 1750	✓
Aug 9 07:32:10	192.168.1.2	202.43.195.101	TCP	1750 => 80	✓

Clear Logs

Download Logs

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. (Figure 12-4)



Figure12-4 Statistics WebUI

(Minute)

🗖 Average packets

Maximum packets

🔳 WAN packets

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

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

 URL String
 Configure

 ~yahoo
 Modify
 Remove

 ~google
 Modify
 Remove

 ~edu
 Modify
 Remove

 \*
 Modify
 Remove

New Entry







Peer-to-Peer Application Blocking	
🗵 eDonkey Blocking	
🗵 Bit Torrent Blocking	
🗹 WinMX Blocking	
	OK Cancel

#### Figure12-7 P2P Blocking Setting



#### Figure12-8 IM Blocking Setting

Download Blocking	Download Blocking						
☑ All Types Blocking							
📕 Audio and Video Types Blocking							
Extension Blocking							
.exe	🗖 .zip	🔲 .гаг					
🗖 .iso	🗖 .bin	🔲 .грт					
🗖 .doc	□ .xl?	🗖 .ppt					
🗖 .pdf	🗖 .tgz	🗖 .gz					
🗖 .bat	🗖 .dll	🔲 .hta					
🗖 .scr	□ .vb?	🔲 .wps					
🗖 .pif							
			OK Cancel				

Figure12-9 Download Blocking Setting

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

- 2. **Script Blocking** can restrict the Internal Users to access to Script file of Website. (Java, Cookies...etc.) (Ex: Stock Exchange Market Net)
- 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: (Figure 12-10, 12-11)

Name	IP / Netmask	Configure			
Outside_Any	0.0.0/0.0.0	In Use			
Remote_Server1	61.219.38.39/255.255.255.255	Modify Remove			
Remote_Server2	202.1.237.21/255.255.255.255	Modify Remove			
New Entry					

Figure12-10 Setting the WAN IP that going to block



Figure12-11 WAN Address Group

The System 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: Select DENY ALL
- Click **OK** (Figure12-12)

Add New Policy	
Source Address	Inside_Any 🔽
Destination Address	WAN_Group
Service	ANY
Action	DENY ALL
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	None -
Schedule	None
Tunnel	None 💌
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

OK Cancel

Figure12-12 Setting Blocking Policy

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

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

Add New Policy	
Source Address	Inside_Any 🔽
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	Enable
Content Blocking	✓ Enable
Anti-Virus	🗆 HTTP / WEBMAIL 🗖 FTP
Authentication User	None -
Schedule	None
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -
	OK Cancel

Figure12-13 Setting Content Blocking Policy

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

Source	Destination	Service	Action	Option				Move	
Inside_Any	WAN_Group	ANY	×					Modify Remove	To 1 🗖
Inside_Any	Outside_Any	ANY	1					Modify Remove	To 2
New Entry									

Figure12-14 Complete Policy Setting

**Deny** in Policy can block the packets that fit in with the policy rule. The System Administrator can put the policy rule in the first priority to prevent the user connecting with specific IP.

## 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 Server 1 of Virtual Server function: (Figure 12-15)

Virtual Server Real IP 61.11.11.12			
Service	WAN Port	Server Virtual IP	Configure
PC-Anywhere (5631-5632)	5631-5632	192.168.1.2	Modify Remove
	New Entry		

Figure12-15 Setting Virtual Server

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

- Click New Entry
- **Destination Address:** Select Server 1 (61.11.11.12)
- Service: Select PC-Anywhere (5631-5632)
- Click **OK** (Figure12-16)

Add New Policy	
Source Address	Outside_Any 🔽
Destination Address	Virtual Server 1(61.11.11.12)
Service	PC-Anywhere(5631-5632)
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	Enable
Schedule	None
Tunnel	None 🗸
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -
	OK Cancel

Figure12-16 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. (Figure12-17)

Source	Destination	Service	Action	(	Opti	on	Conf	īgure	M	ove
Outside_Any	Virtual Server 1 (61.11.11.12)	PC-Anywhere(5631-5632)	6				Modify	Remove	То	1 🗸
New Entry										

Figure12-17 Complete 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: (Figure 12-18)

Name	IP / Netmask	MAC Address	Configure			
DMZ_Any	0.0.0/0.0.0		In Use			
Mail_Server	61.11.11.12/255.255.255.255	00:01:80:41:D0:AE	Modify Remove			
New Entry						

Figure12-18 The Mapped Name in Address Book of Mail Server

STEP 3 . Add the following setting in Group of Service function: (Figure 12-19)

Group name	Service	Configure
E-Mail	DNS,POP3,SMTP	Modify Remove
	Nou: Entry	
	New Entry	

Figure12-19 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** (Figure12-20)

Add New Policy	
Source Address	Outside_Any 🔽
Destination Address	Mail_Server 💌
Service	E-Mail
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	🗆 Enable
Schedule	None 🔽
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None 💌
	OK Cancel

Figure12-20 Setting a WAN to DMZ Policy to access Mail Service

STEP 5 . Complete the WAN to DMZ policy to access mail service. (Figure12-21)

Source	Destination	Service	Action		Opt	ion	Configure	Move
Outside_Any	Mail_Server	E-Mail	6				Modify Remove	To 1 🗾
		C	New Ent	ry				

Figure12-21 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** (Figure12-22)

Add New Policy	
Source Address	Inside_Any 🗸
Destination Address	Mail_Server 💌
Service	E-Mail
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Schedule	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
	OK Cancel
	On Calicel

Figure12-22 Setting a LAN to DMZ Policy to access Mail Service

STEP 7 . Complete the LAN to DMZ policy to access mail service (Figure 12-23)

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	E-Mail	6		Modify Remove	To 1 🗖
New Entry						

Figure12-23 Complete the LAN to DMZ Policy to access Mail Service

#### 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** (Figure12-24)

Add New Policy	
Source Address	Mail_Server -
Destination Address	Outside_Any 🔽
Service	E-Mail
Action	PERMIT
Traffic Log	🗆 Enable
Statistics	Enable
IDP	🗆 Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL      FTP
Authentication User	None 🗸
Schedule	None
Tunnel	None 🗸
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -

Figure12-24 Setting the DMZ to WAN Policy of Mail Service

### STEP 9 . Complete the DMZ to WAN policy to access to mail service. (Figure 12-25)

Source	Destination	Service	Action	Option	Configure	Move	
Mail_Server	Outside_Any	E-Mail	2		Modify Remove	To 1 🗖	
New Entry							

Figure12-25 Complete the DMZ to WAN Policy to access to Mail Service

### Chapter 13

### Configure

According to the Mail Security Configure function, it means the dealing standard towards mail of ALL7007. 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 ALL7007, 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 mail size is less than KBytes (10 - 512 KBytes)	
Unscanned Mail Setting	
✓ Add the message to the subject lineUnscanned	
	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)

🖨 Inbox - Outlook Express				<u>_8×</u>
File Edit View Tools Mes	ssage Help			<b>E</b>
New Mail Reply Reply	All Forward Print Delete	Send/Recv Addresses Find		
🗇 Inbox				
Folders :	× ! 0 % From	Subject	Received	
© Outook Express ⊖ ♥ Local Folders – ♥ Inbox – ♥ Outbox – ♥ Sent Rens – ♥ Deleted Items (76) ♥ Drafts	<u> @</u> Mr Hediathorne	-Unscanned- Visynet	9/16/2004 7:29 AM	
Contacts ▼ : There are no contacts to display. Clic on Contacts to create a new contact	×.			
1 message(s), 0 unread			🖳 Working Online	

Figure13-2 The Unscanned Mail Subject WebUI

# To setup ALL7007 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 ALL7007 and be sent to the appointed mail server after filtering. (Figure 13-3)

<ul> <li>Domain Name of Internal Mail Server</li> <li>Allowed External IP of Mail Relay</li> </ul>						
Add Domain Name						
Domain Name of Mail Server	ex mail my domain.com )					
IP Address of Mail Server 61.11.11.12						
		OK Cancel				

Figure13-3 Mail Relay Setting WebUI

### To setup ALL7007 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 ALL7007'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 (Figure 13-4)

<ul> <li>Domain Name of Internal Mail Server</li> <li>Allowed External IP of Mail Relay</li> </ul>						
Add Domain Name	Add Domain Name					
Domain Name of Mail Server broadband.com.tw						
IP Address of Mail Server 17.16.1.13						
		OK Cancel				

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)

	<ul> <li>Domain Name of Internal Mail Server</li> <li>Allowed External IP of Mail Relay</li> </ul>			
Add IP Address				
IP Address		61.11.11.11	(av: 202.24.191.130.)	
Netmask		255.255.255.255	(av. 255,255,255,240))	
-		•	OK Cancel	

Figure13-5 The Second Mail Relay Setting WebUI

# The Headquarters setup ALL7007 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 ALL7007: 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 (Figure 13-6)

<ul> <li>Domain Name of Internal Mail Server</li> <li>Allowed External IP of Mail Relay</li> </ul>						
Modify Domain Name						
Domain Name of Mail Server broadband.com.tw						
IP Address of Mail Server 61.11.11.12						
OK Cancel						

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)

<ul> <li>Domain Name of Internal Mail Server</li> <li>Allowed External IP of Mail Relay</li> </ul>				
Modify IP Address				
IP Address	211.22.22.22	(av. 202.24.103.104.)		
Netmask	255.255.255.255	(ac 255 255 255 245 )		
	·	OK Cancel		



### Chapter 14

### Anti-Spam

ALL7007 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)

Spam Setting
✓ Enable Anti-Spam
The Mail Server is placed in 🛛 🔽 Internal (LAN or DMZ) (Please set Mail Relay first)
External (WAN)
The threshold score of spam mail is 5 🗾
Add the message to the subject linespan (Max. 256 characters)
Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test
R Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)
Check sender IP address in RBL (Use UDP port : 53) 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 :
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)

🚔 Inbox - Outlook Express				X
File Edit View Tools Messa	age Help See Help See Help Print Delete	Send/Recv Addresses Find		
🕏 Inbox				
Folders ×	! 0 ♥ From	Subject	Received	
© Outdok Express ■ ♥ Local Folders ■ ♥ Local Folders ■ ♥ Outbox ■ ♥ Outbox ■ ♥ Deleted Items ■ ♥ Deleted Items (76) ■ ♥ Drafts	<u></u> Mr Hedrathorne		9/16/2004 7:29 AM	
Contacts				
on Contacts to create a new contact.				
1 message(s), 0 unread			💻 Working Online	

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)

🚔 Inbox - Outlook Express						_ 8 ×
File Edit View Tools Me	ssage Help		<b>1</b> 51 1301	R		
New Mail Reply Reply	All Forward	Print Delete	Send/Recv Addresses	Find		
🕏 Inbox						
Folders	× ! 0 P	From	Subject 🗸		Received	
Contacts *	×	⊴giberto leemaster	[score : 2] let's st	are the tYps for w⊶eight / o`ss nowadays	10/12/2004 6:50 AM	
1 message(s), 0 unread				📕 W	orking Online	1

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, Form, To, Cc, Bcc, Subject, Sender, Reply-To, Errors-To, Message-ID, and Date.

#### **Condition:**

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

#### Pattern:

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

# 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 ALL7007 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 ALL7007 learning the file

#### Training time:

The System Manager can set the training time for ALL7007 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: acoount@server.name. In front of the @ means the account; behinds the @ mean the Master's name.

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

#### The flow of delivering e-mail:

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

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

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

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

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

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

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

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

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

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

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



- 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.
- 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 five 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	226
Ex 2	Take ALL7007 as Gateway and use Whitelist and Blacklist to filter	230
	the mail. (Mail Server is in DMZ and use Transparent Mode)	
Ex 3	Place ALL7007 between the original Gateway and Mail Server to	237
	set up the Rule to filter the mail. (Mail Server is in DMZ and use	
	Transparent Mode)	
Ex 4	Use Training function of ALL7007 to make the mail be determined	243
	as spam mail or ham mail after training. (Take Outlook Express for	
	example)	
Ex 5	Use Spam(Ham) account for training function to let Bayesian	265
	Filtering have high resolution	

# 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	In Use								
Josh 192.168.139.12/255.255.255 Modify Remove									
New Entry									

Figure 14-4 Mapped IP of Internal User's PC in Address Book

STEP 3 . Add the following setting in Group of Service. (Figure 14-5)

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: (Figure 14-6)

Source	Destination	Service	Action	Option		Option		Option		Option		Option		Option		Option		Option		Configure	M	ove
Josh	Outside_Any	Mail_Service	2					Modify Remove	То	1 🗸												
New Entry																						

Figure14-6 Outgoing Policy Setting

# **STEP 5**. Add the following setting in **Setting** of **Anti-Spam** function: (Figure 14-7)

Spam Setting         Image: The Mail Server is placed in Immersion in Internal (LAN or DMZ) (Please set Mail Relay first)         Image: The Mail Server is placed in Immersion in Internal (LAN or DMZ) (Please set Mail Relay first)         Image: The Mail Server is placed in Immersion Immersion in Immersion Immersis Immersion Immer	
<ul> <li>✓ Enable Anti-Spam</li> <li>The Mail Server is placed in  Internal (LAN or DMZ) (Please set Mail Relay first)</li> <li>✓ External (WAN)</li> <li>The threshold score of spam mail is  ✓ </li> <li>Add the message to the subject line  (Max. 256 characters)</li> <li>✓ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test</li> <li>✓ Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)</li> <li>Check sender IP address in RBL (Use UDP port : 53) Test</li> <li>✓ Add score tag to the subject line</li> </ul> Action of Spam Mail Internal Mail Server: <ul> <li>Delete the spam mail</li> <li>Deliver to the recipient</li> <li>Forward to :</li> </ul> External Mail Server: <ul> <li>Ø Deliver to the recipient (Always enable)</li> </ul>	Spam Setting
The Mail Server is placed in Internal (LAN or DMZ) (Please set Mail Relay first) F External (WAN) The threshold score of spam mail is Add the message to the subject linespam (Max. 256 characters) Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams) Check sender IP address in RBL (Use UDP port : 53) 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 : External Mail Server: Deliver to the recipient (Always enable)	🗹 Enable Anti-Spam
✓ External (WAN)   The threshold score of spam mail is   ✓ Add the message to the subject line   → Spam   ✓ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test   ✓ Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)   ○ Check sender IP address in RBL (Use UDP port : 53) 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 :   External Mail Server:     Ø Deliver to the recipient (Always enable)	The Mail Server is placed in 🛛 📕 Internal (LAN or DMZ) (Please set Mail Relay first)
The threshold score of spam mail is <ul> <li>✓</li> <li>Add the message to the subject line</li> <li> <li></li></li></ul>	🔽 External (WAN)
Add the message to the subject linespam (Max. 256 characters)  Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test  Check sender IP address in RBL (Use UDP port : 53) Test Check sender IP address in RBL (Use UDP port : 53) 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 :  External Mail Server:  Deliver to the recipient (Always enable)	The threshold score of spam mail is 5 🔽
<ul> <li>Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test</li> <li>Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)</li> <li>Check sender IP address in RBL (Use UDP port : 53) Test</li> <li>Add score tag to the subject line</li> </ul> Action of Spam Mail Internal Mail Server: <ul> <li>Delete the spam mail</li> <li>Deliver to the recipient</li> <li>Forward to :</li> </ul> External Mail Server: <ul> <li>Deliver to the recipient (Always enable)</li> </ul>	Add the message to the subject line
<ul> <li>Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)</li> <li>Check sender IP address in RBL (Use UDP port : 53) Test</li> <li>Add score tag to the subject line</li> </ul> Action of Spam Mail Internal Mail Server: <ul> <li>Delete the spam mail</li> <li>Deliver to the recipient</li> <li>Forward to :</li> </ul> External Mail Server: <ul> <li>ØY Occepted</li> </ul>	Check spam fingerprint (Use TCP port : 2703 and UDP port : 53) Test
<ul> <li>Check sender IP address in RBL (Use UDP port : 53) Test</li> <li>Add score tag to the subject line</li> </ul> Action of Spam Mail Internal Mail Server: <ul> <li>Delete the spam mail</li> <li>Deliver to the recipient</li> <li>Forward to :</li> </ul> External Mail Server: I Deliver to the recipient (Always enable)	Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)
<ul> <li>Add score tag to the subject line</li> <li>Action of Spam Mail</li> <li>Internal Mail Server: <ul> <li>Delete the spam mail</li> <li>Deliver to the recipient</li> <li>Forward to :</li> </ul> </li> <li>External Mail Server: <ul> <li>Deliver to the recipient (Always enable)</li> </ul> </li> </ul>	Check sender IP address in RBL (Use UDP port : 53) Test
Action of Spam Mail Internal Mail Server: Delete the spam mail Deliver to the recipient Forward to : External Mail Server: Deliver to the recipient (Always enable)	Add score tag to the subject line
Internal Mail Server: Delete the spam mail Deliver to the recipient Forward to : External Mail Server: Deliver to the recipient (Always enable)	Action of Spam Mail
Delete the spam mail Deliver to the recipient Forward to :	Internal Mail Server:
Deliver to the recipient Forward to :	Delete the spam mail
Forward to :  External Mail Server:  Deliver to the recipient (Always enable)	Deliver to the recipient
External Mail Server:	Forward to :
Deliver to the recipient (Always enable)	External Mail Server:
	C Deliver to the recipient (Always enable)
OK Canad	
OK Cancel	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 ALL7007 will filter the spam mail according to the mails that sent to the internal mail server or received from external mail server. (Figure 14-8)

Spam Setting	
🗵 Enable Anti-Spam	
The Mail Server is placed in	☑ Internal (LAN or DMZ) (Please set Mail Relay first)
	🔽 External (WAN)
The threshold score of spam	mail is 5 🔽
Add the message to the subje	ct linespan (Max. 256 characters)
🗹 Check spam fingerprint (U	se TCP port : 2703 and UDP port : 53) Test
Enable Bayesian filtering	(Bayesian filtering works until database has at least 200 spams and 200 hams)
Check sender IP address i	n RBL (Use UDP port : 53) Test
Add score tag to the subje	ct line
Action of Spam Mail	
Internal Mail Server:	
Delete the spam mail	
Deliver to the recipient	
□ Forward to :	
External Mail Server:	
Deliver to the recipient (Alw	ays enable)
	OK Cancel
T.*	140D.C.147.L. CC

Figure14-8 Default Value of Spam Setting

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

- 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 ALL7007 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 💌								
					External			
No.	Recipient 🗸	<u>Total Spam</u> 🗸	<u>Total Mail</u> 👻	Duration	Spam %			
1	js1720@ms21.pchome.com.tw	2	2	00H	100.0%			
	Total	2	2		100.0%			
					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 ALL7007 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	In Use								
Mail_Server	Modify Remove								
New Entry									

Figure14-10 Mapped Name Setting in Address of Mail Server

STEP 3 . Enter the following setting in Group in Service function: (Figure 14-11)

Group name	Service	Configure
Mail_Service_01	POP3,SMTP	Modify Remove
Mail_Service_02	Modify Remove	
	New Entry	

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

STEP 4 . Enter the following setting in WAN to DMZ Policy: (Figure 14-12)

Outside_Any     Mail_Server     Mail_Service_01     V     Modify     Remove	Source	Destination	Service	Action	(	Option		Option Configure		Configure	Move	,
	Outside_Any	Mail_Server	Mail_Service_01	6					Modify Remove	To 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	N	ove	
Mail_Server	Outside_Any	Mail_Service_02							Modify Remove	То	1 🗸
New Entry											

Figure14-13 DMZ to WAN Policy Setting

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

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 ALL7007

STEP 7 . Enter the following setting in Setting function of Anti-Spam: (Figure14-15)

Spam Setting	
Enable Anti-Spam	
The Mail Server is placed in	☑ Internal (LAN or DMZ) (Please set Mail Relay first)
	External (WAN)
The threshold score of spam i	nail is 5 🔽
Add the message to the subje	ct linespam (Max. 256 characters)
🗹 Check spam fingerprint (Us	se TCP port:2703 and UDP port:53) <b>Test</b>
🗵 Enable Bayesian filtering (	Bayesian filtering works until database has at least 200 spams and 200 hams)
Check sender IP address in	n RBL (Use UDP port : 53) Test
Add score tag to the subject	ct line
Action of Spam Mail	
Internal Mail Server:	
Delete the spam mail	
Deliver to the recipient	
□ Forward to :	
External Mail Server:	
Deliver to the recipient (Alwa	ays enable)
	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 ALL7007 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)

Modify Whitelist	
Whitelist	share2k01@yahoo.com.tv
Direction	From 💌
Auto-Training	Enable 💌
	OK Cancel



Add Whitelist	
Whitelist	josh@broadband.com.tw
Direction	Το
Auto-Training	Enable 💌
	OK Cancel

Figure14-17 Add Whitelist Setting 2

From         share2k01@yahoo.com.tw         V         Modify         Remove           To         josh@broadband.com.tw         V         Modify         Remove	Direction	Whitelist	Auto-Training	Configure
To josh@broadband.com.tw 🖌 Modify Remove	From	share2k01@yahoo.com.tw	V	Modify Remove
	То	josh@broadband.com.tw	V	Modify Remove

New Entry

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)

Add Blacklist		
Blacklist	*yahoo*	
Direction	From 💌	
Auto-Training	Enable 💌	
		OK Cancel



Direction	Blacklist	Auto-Training	Configure				
From	*yahoo*	V	Modify Remove				
New Entry							

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 ALL7007 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 ALL7007; 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 ALL7007 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: 1-2								
					Internal External				
No.	Recipient 🗸	<u>Total Spam</u> 🗸	<u>Total Mail</u> 👻	Duration	Spam %				
1	steve@broadband.com.tw	2	3	00H	66.7%				
2	josh@broadband.com.tw	0	1	00H	0.0%				
	Total	2	4		50.0%				
				<u> </u>	Clear Data				
					Store Suite				

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 ALL7007 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 ALL7007: 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 In Use							
Mail_Server 172.16.1.13/255.255.255 00:01:80:41:D0:AE Modify Remove							
New Entry							

Figure14-22 Mapped IP Setting of Mail Server in Address Book

STEP 3 . Enter the following setting in Service Group. (Figure 14-23)

Group name	Service	Configure					
Mail_Service_01	POP3,SMTP	Modify Remove					
Mail_Service_02	DNS,POP3,SMTP	Modify Remove					
New Entry							

Figure14-23 Setting Service Group includes POP3, SMTP or DNS

STEP 4 . Enter the following setting in WAN to DMZ Policy: (Figure 14-24)

Source	Destination	Service	Action	0	ptio	on	Configure	Move
Outside_Any	Mail_Server	Mail_Service_01	2				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		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Option		Conf	igure	M	ove
Mail_Server	Outside_Any	Mail_Service_02	6							Modify	Remove	То	1 -																																						
		6	New F	Intro	,	2																																													

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					

Figure 14-26 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 YahooMail
- **Comments:** Enter Yahoo 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 : YahooM	l Comments : Yahoo Ham Mail					
Combination : Or	nbination : Or 🚽 Classification : Ham(Non-Spam) 🔽					
Action : Delete spam ma	il 🔽	Auto-Training : Enable				
ltem	Condition	Pattern	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	
	YahooMail	Ham		Yahoo Ham Mail	Modify Remove	To 1 💌	
ĺ							
	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 YahooSpamMail
- Comments: Enter Anti Yahoo 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 : YahooSp	amMail	Comments : Anti Yahoo Spam I	Mail
Combination : And	•	Classification : Spam	
Action : Deliver to the re	cipient 💌 🕞	Auto-Training : Enable	
ltem	Condition	Pattern	Configure
From	Contains 💌	yah∞	Next Row
			OK Cancel

Figure14-29 The Second Rule Setting

Rule Name	Classification	Action	Comments	Configure	Move			
YahooMail	Ham		Yahoo Ham Mail	Modify Remove	To 1 💌			
YahooSpamMail	Spam	Deliver to the recipient	Anti Yahoo Spam Mail	Modify Remove	To 💵			
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 ALL7007 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**. (Figure 14-31)

Return-Path:	rs for this message: josh@broad.band.com.tw> n.anh.mam.fc1_218_49_26.HINET_IP.hinet.net [
by of for	soch@nusoft.com.tw (8.11 6/8.11 6) with ESMTP
Received : from by J	n localhost (61-218-49-28 HINET-IP hinet net [6 ocalhost (Postfix) with ESMTP id 8BBF02B984
for From: josh@b	<josh@nusoft.com.tw>; Thu, 22 Jul 2004 17:16:C roadband.com.tw</josh@nusoft.com.tw>
Organization	Web 25 (Star 2000) 79 ( Zoning and
To: iosh@nus	Anu-span caneway off.com.tw
To: iosh@nus Message-ID: « From: "Lucian	And-Spein Gateway off.com.tw 66279oa70/5283\$3042675\$ra31mcl10@Nickrj8 o Mcmanus'' <tbab00h@domain.com.tw></tbab00h@domain.com.tw>
To: iosh@nus Message-ID: From: "Lucian To: <sonata2 X-Anti-Spam: /</sonata2 	And-Spain Gateway off.com.tw 662730a70r5283\$3042675\$ra31mcH0@Nickrj8 o Mcmanus'' <tbab00h@domain.com.tw> 2@ms43.hinet.net&gt; Anti-Spain Gateway cleanup, with id 224a8a383</tbab00h@domain.com.tw>
To: iosh@nus Message-ID From: "Lucian To: <sonata2. X-Anti-Spam. X-Anti-Spam. Subject: [scc</sonata2. 	And-Spain Gateway off.com.tw (66279oa70r5283\$3042675\$ra31mcl10@Nickrj8 o Mcmanus'' <tbab00h@domain.com.tw> @ms43.hinet.net&gt; Anti-Spain Gateway cleanup, with id 224a8a383 Anti-Spain Gateway cleanup, with id 23ca802a re : 3]spain Find out if Lavonne is a real m</tbab00h@domain.com.tw>
To iosh@nus Message-ID: From "Lucian To: <sonata22 X-Anti-Spam: / X-Anti-Spam: / Subject: [scc Date: Thu, 16 MIME-Version</sonata22 	And-Span Gateway off.com.tw (66279oa70r5283\$3042675\$ra31mcl10@Nickrj8 o Momanus'' <tbabd0h@domain.com.tw> 2@ms43.hinet.net&gt; Anti-Spam Gateway cleanup, with id 224a8a383 Anti-Spam Gateway cleanup, with id 23ca802a rre : 3]spam Find out if Lavonne is a real m Sep 2004 21:29:05-0600 : 1.0</tbabd0h@domain.com.tw>
To: iosh@nus Message-ID: From 'Lucian To: <sonata22 X-Anti-Spam: / Subject: [sor Date: Thu, 16 MIME-Version Content-Type:</sonata22 	And-Spein Gateway off.com.tw (66279oa70r5283\$3042675\$ra31mcl10@Nickrj8 of Momanus'' <tbabd0h@domain.com.tw> 2@ms43.hinet.net&gt; Anti-Spam Gateway cleanup, with id 224a8a383 Anti-Spam Gateway cleanup, with id 23ca802a re : 3]spam Find out if Lavonne is a real m Sep 2004 21:29:05 -0600 1.0 multipart/alternative;</tbabd0h@domain.com.tw>
To: iosh@nus Message-ID: From: 'Lucian To: (sonata2: XAnti-Spam: / XAnti-Spam: / Subject: [soc Date: Thu, 16 MIME-Version Content-Type:	And Span Gateway off.com.tw 662790a70:5283\$3042675\$ra31mcl10@Nickrj8 o Momanus'' <tbab00h@domain.com.tw> 2@ms43.hinet.net&gt; Anti-Spam Gateway cleanup, with id 224a8a383 Anti-Spam Gateway cleanup, with id 23ca802a re : 3]spam Find out if Lavonne is a real m Sep 2004 21:29:05 -0600 1.0 multipart/alternative;</tbab00h@domain.com.tw>

Figure14-31 The Detailed Data of the Mail

- **STEP 9**. When the external yahoo mail account send mail to the recipient account of mail server of broadband.com.tw in ALL7007; 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 ALL7007 had filtered the mail above, it will bring the chart as follows in the Spam Mail function of Anti-Spam. (Figure14-32)

	Top Total	Spam: 1-2 🗸			
					Internal External
No.	Recipient 🗸	<u>Total Spam</u> 🗸	<u>Total Mail</u> 👻	Duration	Spam %
1	steve@broadband.com.tw	2	3	00H	66.7%
2	josh@broadband.com.tw	0	1	00H	0.0%
	Total	2	4		50.0%
				<u> </u>	Clear Data

Figure14-32 Chart of Report Function

# Use Training function of the ALL7007 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)

🗐 Inbox - Outlook	Express										<u>- 8 ×</u>
File Edit View	Tools N	Message	Help								
New Mail Re	iply Rep	aly All	Sorward	Print	X Delete	iend/Recv	Addresses	Find -	•		
🗇 Inbox											
Folders		×	99	From		Subject	Δ.,			Received	
Gutlook Express				<b>U</b> Lucian	o Mcmanus	[score	:3]spa	m Find c	out if Lavonne i	9/17/2004 10:25 AM	
E- Cocal Folders											
Outt OI	pen										
- 🖄 Sent 🔤	nd		-								
- 🕖 Dele Ne	ew Folder	¢.									
EQJ Draf No De	elete										
Ac		ik Bar	-								
Pr	operties		-								
	operado										
		~									
Contacts *		_									
There are no contacts	s to display.	Click									
	o d non con										
		- 1									

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 ALL7007 for training:
  - Select **SpamMail** Folder (Figure14-37)
  - Select **Compact** function in selection of the folder (Figure14-38)



Figure14-37 Select SpamMail Folder

🗿 SpamMail - Outlook Expre	ess	×
File Edit View Tools I New Open C Save As Save Attachments	Message Help Crit+O vard Print Delete Send/Recv Addresses Find	
Save as Stationery		
Folder Import Export	New Ctrl+Shift+E the masculine courage for you and your partner 9/17/2004 3:50     Move     Rename     Delete	) PM
Print C	Ctrl+P Compact	
Switch Identity Identities	Compact All Folders	
Properties A	Alt+Enter	
Exit and Log Off Identity Exit	y. Clck ntact.	

#### Figure14-38 Compact SpamMail Folder

- **STEP 4**. To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to ALL7007:
  - 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)

New Mail Reply Reply All Forwar	nd Print Delete Send	Recv Addresses Find		
SpamMail		a revenue a companya da com		
idders × 1 0 Coultoble Express Coultoble Express Coultoble Express Coultoble Express Coultoble Express Coultoble Express Coultoble Express Section Coultoble Fred Rename Delete Add to Outlook Bar Properties There are no contacts to display. Click n contacts to create a new contact.	Period       Resetta Stubbs       Provlatt TestPanct.com       Seadedrightomain.c.,       District TestPanct.com       Statistic testPanct.com       Dick Ratcker       Renet Clement       Dick Statistic       Bob Alten       Globes remaince.	Subject         R          span-         Yalium for less          span-         Soft Need software? Click here.          span-         -span-          span-         Neing software? Click here.          span-         -span-          span-         Neing software? Click here.          span-         -span-          span-         Neing software? Lick here.          span-         Neing software? Lick here.          span-         Neing software? Neing software?          span-         Neing software?      <	eceived 9/201/2004 23: 9/201/2004 836 9/201/2004 845 9/201/2004 845 9/201/2004 845 9/201/2004 821 9/201/2004 821 9/201/2004 825 9/201/2004 825 9/201/2004 826 9/201/2004 827 9/201/2004 827 9/201/2004 827 9/201/2004 827 9/201/2004 827 9/201/2004 826 9/201/2004 826 9/201/2004 826	

Figure14-39 Select SpamMail File Properties Function

eneral				
	SpamMail			
This fold	er contains			
	2 messages, 1 un	read.		
This fold	er is stored in the follo	wing file:		
	67448}\Microsoft	\Outlook Exp	ress\Spamh	tail (1) dbs
			R.	undo
				Cut
				Paste
				Delete
				Select All
	-	100	1	

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 ALL7007 instantly and to learn the uploaded mail file as spam mail in the appointed time. (Figure14-41)

Free space for training: 801 KBytes The amount of spam mail : 0 The amount of ham mail : 0 Bayesian filtering works until database has at	least 200 spams and 200 hams
Training Database	
Export Training Database	Download
Import Training Database	瀏覽
Reset Training Database	Reset Database
Spam Mail for Training	
Import Spam Mail from Client	C.VDocuments and Settings Ra 1000000
Ham Mail for Training	Cut
Import Ham Mail from Client	Paste 瀏覽 Delete 以
Spam Account for Training	Select All
POP3 Server	( ex: my_domain.com )
User name	(ex:spam)
Password	(ex: 5d2#k)
Spam account test	Account Test
Ham Account for Training	
POP3 Server	( ex: my_domain.com )
User name	(ex: ham)
Password	(ex: 5d2#k)
Ham account test	Account Test
Training time	
Training database starts at 🚾 🛛 / day	
Training immediately : <u>Training NOW</u>	
	OK Cancel

Figure 14-41 Paste the File Address that SpamMail File Save to make ALL7007 to be Trained

The training file that uploads to ALL7007 can be any data file and not restricted in its sub-name, but the file must be ACS11 form.

When the training file of ALL7007 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 ALL7007 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)

🖨 SpamMail - Outlook Express		_ 6
File Edit View Tools Messag	s Help	
New Mail Reply Reply All	Forward Print Delete Sendificary Addresses End	
🛸 SpamMail		
Folders ×	! @ ♥ From Subject ♡	Received
© Outbook Express © Local Folders → Thox © Outboox ⇒ HamMal ⇒ HamMal ⇒ SpamMall (14) → Sent Rems → Drafts → Virus	Rosetta Stubbs    spam Välium for less     Product TestPaneLcom	9/20/2004 2:55 PM 9/20/2004 9:06 AM 9/20/2004 8:02 AM 9/20/2004 8:32 AM 9/20/2004 8:33 RM 9/20/2004 2:31 PM 9/20/2004 2:31 PM 9/20/2004 2:32 PM 9/20/2004 10:56 AM 9/20/2004 10:56 PM 9/20/2004 10:35 PM 9/20/2004 2:35 PM
	Migel lutao    spam     Relief From pa∖iin event     Bob Allen    spam     Right out of the TV studio audience     Op     V     alexa ramirez     RE: You can become a legally ordained minister     P     P     Re     Fe     Fe	9/17/2004 7:23 PM pen nk ply to Sender ply to All wward As Attachment
Contacts ▼ ×	Ma Ma	ark as Read ark as Unread
B sender@mydomain.com	Me Co Pe	ave to Folder py to Folder elete
	Pri	operties
Deleter the relacted marriage		

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. (Figure 14-44)
- Enter HamMail in Folder Name in Create Folder WebUI and click OK. (Figure14-45)

Elle Edit	's - Outlook Express	Help					_ # ×
	Q. Q.	180 180	X D	•	<b>.</b>		
🔅 Local Ec	olders	annara anna.	Donali Donali Cort	Hadrosses	1.410		
Folders	×						
🗐 Outlook Expr	ess	Jse local folders for POP ac		nessages from o			
E 🗇 Local Feb	Open	1	l.				
i int	Find	end and Receive All					
Ser Ser	Demoke Account	er	Unread	Total			
🖃 🞯 Del	Set as Default Account.	nbox	5	6			
<u>i (6</u>	NEW CARL	utbox	0	0			
- 🕼 Dra	Recentlich	eleted Items	123	0			
🦾 Spa	100 00 10	DSpamMail	0	0			
-	Add to Outlook bar	afts	0	0			
	Properties	pamMail	0	0			
<u>Contacts</u> ▼ There are no cor on Contacts to c	x ntacts to display. Cikk reate a new contact.						
						 Working Opline	

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 ALL7007 for training:
  - Select HamMail File (Figure14-48)
  - Select **Compact** function in selection of File (Figure14-49)

🚔 HamMail - Outlook Express		
File Edit View Tools Messag	e Help	Here and the second
D . 24 24	😡 🎒 X 🗐 🖉 🖗 .	
New Mail Reply Reply All	Forward Print Delete SendjRecv Addresses Find	
HamMall		
Folders ×	! 0 ♡ From ♡ Subject	Received
- M Local Folders	Zachery Lane [score : 4]spam Nominate yourself io	9/16/2004 4:16 AM 9/16/2004 1:30 AM
🕞 Inbox (7)		9/15/2004 11:50 PM
🗉 💞 Outbox	iospeh pumphrey [score:4]spam your presc?ription	9/17/2004 4:24 AM
- Canal Sent Items	🖾 Jayne Baca [score : 4]spam Win dows XP shipped	9/16/2004 10:24 AM
Deleted Items (121)		
Drafts		
HamMail (5)		
<u>⊂</u> ontacts ▼ X		
There are no contacts to display. Click		
on Contacts to create a new contact.		
e		
5 message(s), 5 unread		🚔 working Unline

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 ALL7007:
  - 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)

🛱 HamMail - Outlook Express		_ <u>8 ×</u>
File Edit View Tools Messag	ige Help	
New Mail Reply Reply All	Service Send/Recv Addresses Find	
🗯 HamMail		
Folders ×	! 🔋 🖗 🏱 From 🗸 Subject Received	
Outbook Express Outbook Express Outbook Formess Outbook Open Find New Folder Rename Delete Add to Outbook Propertes	W Zachery Lane       [score: 4]      spam       Nominate yourself (a9/16/2004 11:30 AM         W Yito Galvan       [score: 3]      spam       Certify EU Guidelines       9/16/2004 11:30 PM         W Karla Doss       [score: 3]      spam       Nerildhi, kjlt's about9/15/2004 11:50 PM         Ø Jospeh pumphrey       [score: 4]      spam       Your presc?ription9/17/2004 42:4 AM         Ø Jayne Baca       [score: 4]      spam       Win dows XP shipped9/16/2004 10:24 AM	
<u>Contacts</u> <b>* X</b> There are no contacts to display. Click on Contacts to create a new contact.		
5 message(s), 5 unread	, 🖳 Working Online	

Figure14-50 Select Properties of HamMail File WebUI

HamMail Properties	?
aeneral	
HamMail	
This folder contains:	
5 messages, 5 unread.	
This folder is stored in the following fi	le:
C:\Documents and Setti	ngs\nusoft211\Local Setting
	Undo
	Cut
	Сору
	Paste h
	Delete
	Select All
ОК	Cancel Apply

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 ALL7007 instantly and to learn the uploaded mail file as ham mail in the appointed time. (Figure14-52)

Free space for training: 801 KBytes The amount of spam mail : 0 The amount of ham mail : 0 Bayesian filtering works until database has a	t least 200 spams and 200 hams
Training Database	
Export Training Database	Download
Import Training Database	瀏覽
Reset Training Database	Reset Database
Spam Mail for Training	
Import Spam Mail from Client	瀏覽
Ham Mail for Training	
Import Ham Mail from Client	C.VDcourments and Settings Raj 瀏覽 Undo
Spam Account for Training	Cut
POP3 Server	Paste ( ex: my_domain.com )
User name	Delete K (ex: spam)
Password	Select All (ex: 5d2#k)
Spam account test	Account Test
Ham Account for Training	
POP3 Server	( ex: my_domain.com )
User name	(ex: ham)
Password	(ex: 5d2#k)
Ham account test	Account Test
Training time	
Training database starts at 🚾 🗸 / day	
Training immediately : Training NOW	
	OK Cancel

Figure 14-52 Paste the File Address that HamMail File Save to make ALL7007 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 ALL7007 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)

nie Lait view Tools Message Help
P         P
🛸 HamMail
There must bogy recurrent bogy recurrent box     Part Lee (structurent box     Part Lee (structurent box       Coldook Express     Image: Structurent box     Image: Struct

Figure14-53 Delete All of Mails in HamMail File



Figure14-54 Make Sure all of the Mails in HamMail File had been Deleted

# Use Spam(Ham) account for training function to let Bayesian Filtering have high resolution

**STEP 1.**Create a spam account in mail server.(ex: spam@nusec.com.tw)

**STEP 2.**Create a ham(non-spam) account in mail server.(ex: ham@nusec.com.tw)

- **STEP 3.**Enter settings as follows in **Spam Account for Training** item to receive mail of the account: spam@nusec.com.tw in **Training** of **Anti-Spam** function:
  - **POP3 Server:** Enter nusec.com.tw.
  - **User Name:** Enter spam.
  - **Password:** Enter spam.
  - Enter OK.

**STEP 4.**Enter settings as follows in **Ham Account for Training** item to receive mail of the account: ham@nusec.com.tw in **Training** of **Anti-Spam** function:

- **POP3 Server:** Enter nusec.com.tw.
- **User Name:** Enter ham.
- **Password:** Enter ham.
- Enter **OK**. (Figure14-55)

Free space for training: 876 KBytes The amount of spam mail : 0 The amount of ham mail : 0				
Bayesian filtering works until database has at	least 200 spams and 200 hams			
Training Database				
Export Training Database	Download			
Import Training Database	Browse			
Reset Training Database	Reset Database			
Spam Mail for Training				
Import Spam Mail from Client	Browse			
Ham Mail for Training				
Import Ham Mail from Client	Browse			
Spam Account for Training				
POP3 Server	nusec.com.tw (ex: my_domain.com)			
User name	spam (ex: spam)			
Password	***** (ex:5d2#k)			
Spam account test	Account Test			
Ham Account for Training				
POP3 Server	nusec.com.tw (ex: my_domain.com)			
User name	ham (ex:ham)			
Password	••••• (ex:5d2#k)			
Ham account test	Account Test			
Training time				
Training database starts at 🔟 🗹 I day				
Training immediately : Training NOW				
	OK Cancel			

Figure14-55 Spam and Ham Account for Training settings

#### Training the mail to be spam mail

**STEP 5.**Forward the spam mail in **Inbox** of **Outlook Express** as attachment to the spam mail response account:

- Click the mouse right key and select Forward As Attachment function on all selected spam mail in Inbox.(Figure14-56)
- In New Mail window, To: Enter spam@nusec.com.tw, Subject: Enter Spam, mail content is blank, and Click Send.(Figure14-57)



Figure 14-56 Select spam mail

<u>a</u> Spam		. 8 ×
File E	dit View Insert Format Tools Message Help	- E
Send	Image: Image	
From:	Josh@nusec.com.tw (nusec.com.tw)	•
To:	spam@nuec.com.tw	
Cc:	[	
Bcc:	[	
Subject:	Span	
Attach:	Car Ranke your lides to software (2.4018) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, ALPRAZZOLAM, TRAMADOOL, A (1.70 KB) Car Ray, CALLS, EUTRIAN, MERLIDIA, EUTRIAN, EUTRIAN	•
Arial	▼ 10 ▼ 頁 B Z U A, 旧日律律 書主言言 - % 2	
		4
1		

Figure 14-57 Forward spam mail

#### Training the mail to be ham(non-spam) mail

**STEP 6.**Forward the ham mail in **Inbox** of **Outlook Express** as attachment to the ham(non-spam) mail response account:

- Click the mouse right key and select Forward As Attachment function on all selected ham(non-spam) mail in Inbox.(Figure14-58)
- In New Mail window, To: Enter ham@nusec.com.tw, Subject: Enter Ham, mail content is blank, and Click Send.(Figure14-59)

🎒 Inbox - Outlook Express				_ 8 ×
File Edit View Tools Messag	ge Help			<u>E</u>
New Mail Reply Reply All	₩2 🥌 🗙 É Forward Print Delete Send/	경 · 관계 및 · · · · · · · · · · · · · · · · · ·		
🕸 Inbox				
Folders x Goldens x Goldens Express Goldens (17) → Goldens (17) → Golden	1       Ø       From         Investigation       Investigation         Inter gartner       Stosfpdaoos@yahoo         Inter gartner       David James         Inter gartner       Sthanna Romero         Inter gartner       Yania Marta         Inter gartner       Josh(Nusoft)         Inter gartner       Stharezk01@yahoo	Subject Remarkable You Have to try Thisl pure Bleeding-sigs Digest, Vol 7, Issue 4 korey It's me and my sister Jessica on this pics FWD fromAna Kelly+Size Matters - Sunday TL Office software - very low price Your women will be happy! Dear Sir, i am interested in it If a relaxing moment turns into the right mo Let's make your idea to software! Message subject XANA, LORAAZEPAH, \/ALUUM, \/IIGRA, CALL Best offer for you, YIAGRA for the best price! Windows XP - 75% OFF MAX PDIP Connections MAX COS support for old 802.1118 USB device	Received         ▲           8/12/2005 6:43         8/12/2005 6:45           8/12/2005 6:50         8/12/2005 6:50	
<u>Contacts</u> ▼ X There are no contacts to display. Click on Contacts to create a new contact.			Mark as Read Mark as Unread Move to Folder Copy to Folder Delete	
		,	Add Sender to Address Book	
		1	Properties	
Creates a message with current message	(c) as attachments.			

Figure 14-58 Select ham(non-spam) mail

n Ham	_ <del>_</del> _ <del>/</del> ×
File Edit View Insert Format Tools Message Help	E Contraction (1997)
J Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline	
From: josh@nusec.com.tw (nusec.com.tw)	-
19 To: ham@nusec.com.tw	
Subject: Ham	
Attach: Attach	
Arial 🔽 10 🖳 🗒 🖌 U 🗛   日 日 存 存   目 主 主 三 🗐 🚽 🌚	
	<u></u>
	~

Figure 14-59 Forward ham(non-spam) mail

#### **STEP 7.**Multi Security Firewall will retrieve mail from account("spam@nusec.com.tw" and "ham@nusec.com.tw") at a fixed time, and training the mail to be spam or ham(non-spam) mail at specific time.(Figure14-60)

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	Download Browse			
Reset Training Database	Reset Database			
Spam Mail for Training				
Import Spam Mail from Client	Browse			
Ham Mail for Training				
Import Ham Mail from Client	Browse			
Spam Account for Training				
POP3 Server	nusec.com.tw (ex: my_domain.com)			
User name	spam (ex: spam)			
Password	(ex: 5d2#k)			
Spam account test	Account Test			
Ham Account for Training				
POP3 Server	nusec.com.tw (ex: my_domain.com)			
User name	ham (ex: ham)			
Password				
Ham account test	Account Test			
Training time				
Training database starts at 🛛 🖸 🖬 / day				
Training immediately : Training NOW				
	OK Cancel			

Figure 14-60 Set the training time

### Anti-Virus

ALL7007 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)

Anti-Virus Setting							
Virus Scan Engine Clame  The Mail Server is placed in Internal (LAN or DMZ) External (WAN)							
						(Max. 256 chara	acters)
The latest update time : 03/01/01 04:31:12 (Update virus definitions every ten n	ninutes)						
The newest version: 33.1011 (Clam definitions updated at 03/01/01 00:55:20)							
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53)	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 :							
External Mail Server:							
Deliver to the recipient (Always enable)							
Oeliver a notification mail instead of the original virus mail							
<ul> <li>Deliver the original virus mail</li> </ul>							
	OK Cancel						

Figure15-1 Anti-Virus Settings WebUI



🖨 Inbox - Outlook Express			
File Edit View Tools Messag	je Help		
New Mail Reply Reply All	Forward Print Del	ete Send/Recv Addresses Find	
🗇 Inbox			
Folders ×	! 0 또 From	Subject 2	Received
© Unlook Express © © Local Folders → © Tubber (1) ⊖ © Outbox ↓ © HennMal → © SpamMail (14) → © Sent Items → © Deleted Items (295) → © Undrs ↓ Virus	û ⊠testlab	virus GC Chat Networks 1733	9/20/2004 5:18 PM
Contacts ▼ X PRayearth B sender@mydomain.com			
1 message(s), 1 unread			💻 Working Online 🔥 Error

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	278
	virus or not.	
Ex 2	To detect the mail that send to Internal Mail Server have virus or	282
	not. (Mail Server is in LAN, NAT Mode)	

## 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: (Figure 15-3)

Name	IP / Netmask	MAC Address	Configure				
Inside_Any	0.0.0/0.0.0		In Use				
Josh	192.168.139.12/255.255.255.255		Modify Remove				
New Entry							

Figure 15-3 Mapped IP of Internal User's PC in Address Book

STEP 3 . Add the following setting in Group of Service. (Figure 15-4)

Group name	Service	Configure
Mail_Service	DNS,POP3,SMTP	Modify Remove
	Now Entry	
	New Entry	

Figure15-4 Service Group that includes POP3, SMTP, or DNS

STEP 4 . Add the following setting in Outgoing Policy: (Figure 15-5)

Source	Destination	Service	Action	Option		Option		Configure	M	love
Josh	Outside_Any	Mail_Service	1			Modify Remove	То	1 🗸		

Figure15-5 Outgoing Policy Setting

STEP 5 . Add the following setting in Setting of Anti-Virus function: (Figure 15-6)

- 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 placed in 🛛 🔲 Internal (LAN or DMZ)
External (MAN)
Add the message to the subject line [virus] (Max. 256 characters)
The latest update time : 03/01/01 04:31:12 (Update virus definitions every ten minutes)
The newest version : 33.1011 (Clam definitions updated at 03/01/01 00:55:20)
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53) 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 :
External Mail Server:
Deliver to the recipient (Always enable)
<ul> <li>Deliver a notification mail instead of the original virus mail</li> </ul>
<ul> <li>Deliver the original virus mail</li> </ul>
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 ALL7007 will scan the mails automatically, which sent to the internal mail server or received from external mail server. (Figure 15-7)

Anti-Virus Setting	
Virus Scan Engine 🛛 🔽 🔽	
The Mail Server is placed in 🛛 🖂	Internal (LAN or DMZ) (Please set Mail Relay first)
	External (WAN)
Add the message to the subject i	Ine [
The latest update time : 03/01/01	04:31:12 (Update virus definitions every ten minutes)
The newest version : 33.1011 (Cla	m definitions updated at 03/01/01 00:55:20)
Update virus definitions immedia	tely (Use TCP port : 80 and UDP port : 53) Update NOW Test
Action of Infected Mail	
Internal Mail Server:	
Delete the virus mail	
Deliver to the recipient	
Oeliver a notification mail	instead of the original virus mail
○ Deliver the original virus	mail
Eopward to :	
External Mail Server:	
Deliver to the recipient (Alw	ays enable)
Oeliver a notification mail	instead of the original virus mail
○ Deliver the original virus	mail
-	
	OK Cancel

Figure15-7 Default Value of Virus Mail Setting



 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 ALL7007 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 🗸	<u>Total Virus</u> 🗸	<u>Total Mail</u> 🔫	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 ALL7007: 61.11.11.12 LAN Subnet of ALL7007: 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: (Figure 15-9)

Name	IP / Netmask	MAC Address	Configure				
Inside_Any	0.0.0/0.0.0		In Use				
Mail_Server 192.168.2.12/255.255.255.255		00:01:80:41:D0:AE	Modify Remove				
New Entry							

Figure15-9 Mapped IP Setting in Address of Mail Server

STEP 3 . Enter the following setting in Group in Service function: (Figure 15-10)

Group name	Service	Configure
Mail_Service_01	POP3,SMTP	Modify Remove
Mail_Service_02	DNS,POP3,SMTP	Modify Remove
	New Entry	

Figure15-10 Setting Service Group that include POP3, SMTP or DNS

STEP 4. Enter the following setting in Server1 in Virtual Server function: (Figure 15-11)

Virtual Server Real IP61.11.11.12	]		
Service	WAN Port	Server Virtual IP	Configure
Mail_Service_01	From-Service (Group)	192.168.2.12	Modify Remove
	New Entry		

Figure15-11 Virtual Server Setting WebUI

STEP 5 . Enter the following setting in WAN to LAN Policy: (Figure 15-12)

Source	Destination	Service	Action	Option		on	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	Mail_Service_01	6	✓			Modify Remove	To 1 🗖
New Entry								

Figure15-12 WAN to LAN Policy Setting

STEP 6 . Enter the following setting in LAN to WAN Policy: (Figure 15-13)

Source	Destination	Service	Action	Option			Configure	Move			
Mail_Server	Outside_Any	Mail_Service_02	6						Modify Remove	То	1 🗸
New Entry											

Figure15-13 LAN to WAN 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 )	Modify Remove		
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 ALL7007.

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 (Figure 15-15)

Anti Minun Catting							
Anti-Virus Setting							
Virus Scan Engine Clam 🗾							
The Mail Server is placed in 🔽 Internal (LAN or DMZ) (Please set Mail Relay first)							
External (WAN)							
Add the message to the subject lineVirus (Max. 256 characters)							
The latest update time : 2003/01/01 05:13:16 (Update virus definitions every ten minutes)							
The newest version : 33.1011 (Clam definitions updated at 03/01/01 00:55:20)							
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53) Update NOW Te	<u>ist</u>						
Action of Infected Mail							
Internal Mail Server:							
Delete the virus mail							
Deliver to the recipient							
<ul> <li>Deliver a notification mail instead of the original virus mail</li> </ul>							
<ul> <li>Deliver the original virus mail</li> </ul>							
□ Forward to :							
External Mail Server:							
Deliver to the recipient (Always enable)							
<ul> <li>Deliver a notification mail instead of the original virus mail</li> </ul>							
<ul> <li>Deliver the original virus mail</li> </ul>							
ОК	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 ALL7007 had scanned mail that have virus, it will delete it directly. But still can check the relevant chart in **Virus Mail** function.

- STEP 9. When the external yahoo mail account sends mail to the recipient account of mail server of broadband.com.tw in ALL7007; josh@broadband.com.tw
  - If the mails are from the sender account, share2k01@yahoo.com.tw, which include virus in the attached file.
  - If it comes from other yahoo sender account share2k003@yahoo.com.tw, which attached file is safe includes no virus.
  - After ALL7007 had scanned the mails above, it will bring the chart as follows in the Virus Mail function of Anti-Virus. (Figure15-16)

	Top Total Virus: 1-1 🗸								
					Internal External				
No.	Recipient 🗸	<u>Total Virus</u> 🗸	<u>Total Mail</u> 🗸	Duration	Virus %				
1	josh@broadband.com.tw	1	2	00H	50.0%				
Total		1	2		50.0%				
				<u> </u>	Clear Data				



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

## Configure

ALL7007 can aim at abnormal traffic and packets content to inspect and alert, and handle by the obstructive, separateness, interference, or alarm to administrator way to prevent suspicious program invade the host. So when ALL7007 detects the attack behavior come from internal or external, it can provide the protection to network and obstruct to the attack behavior, let the network can still work normally and increase the information transmission security.

According to the IDP Configure function, it means the dealing standard towards attack behavior of ALL7007. In this chapter, it is defined as Setting.

### Define the required fields of Setting:

#### **IDP Setting:**

- It can update signature definitions for every 30 minutes. Or update signature definitions immediately. It will show the update time and version at the same time.
- It can detect virus to the file which have no encryption and compression.
- Virus scan engine:
  - Clam: It is the system default setting can be free used immediately.

ALL7007 can test if can connect to IDP server to update the signature definitions on internet by **Test** function.
#### Set default action of all signatures:

- According to attack behavior's threat to divide: high risk, medium risk, and low risk. The different risk attack behavior can be handled by the pass, drop, and log action.
  - Add the following settings in this function:
    - 1. Select Enable Anti-Virus.
    - 2. Click OK.
    - 3. High Risk: Select drop and log function.
    - 4. Medium Risk: Select drop and log function.
    - 5. Low Risk: Select pass and log function.
    - 6. Click **OK**. (Figure16-1)
    - 7. Enable IDP function in policy.

IDP Setting				
The latest update	time : 05/08/25	5 10:37:34 (Update	signature definitions every thir	ty minutes)
The newest version	on : 0.0.4 (Sign	ature definitions update	ed at 03/01/01 00:03:47)	
Update signature	definitions im	mediately (Use TCF	port : 80 and UDP port : 53)	Update NOW Test
🗷 Enable Anti-Vir	rus (for P2P, IM, I	NetBIOS)		
				OK Cancel
Set default actio	n of all signatu	ires		
High Risk	Drop 👻	🔽 Log	( [Pass] recommended)	
Medium Risk	Drop 👻	🖂 Log	( [Pass] recommended)	
Low Risk	Pass 💌	🖂 Log	( [Pass] recommended)	
				OK Cancel

Figure16-1 IDP Setting

 When the attack behavior which conform signature will produce log as follows in Log function of IDP Report: (Figure16-2)

2005-08-24 13:16:20 💌							
Time		Event	Signature Class.	Interface	Attack IP	Victim IP:Port	Action
2005-08-24 13:16:20	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:16:02	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:15:52	0	(spp_clamav) Virus Found: Troj	Anomaly	WAN	216.127.33.119	192.168.179.30:4318	×
2005-08-24 13:15:48	0	(spp_clamav) Virus Found: Troj	Anomaly	WAN	216.127.33.119	192.168.179.30:4318	×
2005-08-24 13:15:45	0	(spp_clamav) Virus Found: Troj	Anomaly	WAN	216.127.33.119	192.168.179.30:4318	×
2005-08-24 13:15:45	0	(spp_clamav) Virus Found: Troj	Anomaly	WAN	216.127.33.119	192.168.179.30:4318	×
2005-08-24 13:15:44	0	(spp_clamav) Virus Found: Troj	Anomaly	WAN	216.127.33.119	192.168.179.30:4318	×
2005-08-24 13:15:10	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	X
2005-08-24 13:14:44	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:14:44	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×

Clear Data

Figure16-2 IDP Log

### Chapter 17

## Signature

Provide relative compare rule to different attack behavior, include two sections: **Pre-defined** and **Custom**.

**Pre-defined** signatures can detect and prevent to intrusive pattern which can be discovered at present. These signatures can not be modifyed and deleted. **Custom** signatures can let user to according there requirement to detect and prevent the internal and external attack behavior which is outside of **Pre-defined** signatures.

## Define the required fields of Signature

#### Pre-defined:

- It can be divided: Backdoor, DDoS, DoS, Exploit, NetBIOS, and Spyware category, they have the respectively subordinate attack signature.
- It can change handling action of each category and its respective subordinate signature: Pass, Drop, or Log.
- It can show the attribute of all attack signatures which are Name, Risk, Action, and Log.

#### Name:

■ The System Manager can name the signature.

#### Protocol:

Setting the protocol which want to be detected and prevented, it can be divided: TCP, UDP, ICMP and IP.

#### Source Port:

Setting the port number is used by the attack end PC.(The range can be 1024~65535).

#### **Destination Port**:

Setting the port number is used by the PC which is attacked. (The range can be 1024~65535).

#### Risk:

Define the threat about attack packets.

#### Action:

■ The handling action to attack packets.

#### Content:

■ Setting the attack packets content.

# Use Pre-defined and Custom signature settings to detect and prevent attack behaviors

**STEP 1.**Enter the following setting in **Setting** of **Configure** function:

(Figure17-1)

IDP Setting				
The latest update	time : 05/08/20	5 12:56:18 (Update	signature definitions every thirt	y minutes)
The newest version	on : 0.0.4 (Sign	nature definitions update	d at 03/01/01 00:03:47)	
Update signature	definitions im	mediately (Use TCP	port : 80 and UDP port : 53)	Update NOW Test
☑ Enable Anti-Vir	us (for P2P, IM,	NetBIOS)		
				OK Cancel
				Cancer
Set default action	n of all signati	ures		
High Risk	Drop 👻	🗹 Log	( [Pass] recommended)	
Medium Risk	Drop 👻	I Log	( [Pass] recommended)	
Low Risk	Pass 👻	🗹 Log	( [Pass] recommended)	
				OK Cancel

Figure17-1 IDP Setting

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

- Click **New Entry**.(Figure17-2)
- Name: Enter Software\_Crack\_Website.
- **Protocol**: Select TCP.
- Source Port: Enter 0:65535.
- **Destination Port**: Enter 80:80.
- **Risk**: Select High.
- Action: Select Drop and enable Log function.
- **Content**: Enter cracks.(Figure17-3)

Add New Signature				
Name	Software_Crack_Website			
Protocol				
Source Port	0.65535			
Destination Port	80:80			
Risk	High			
Action	Pass 🔽 🔽 Log			
Content	Cracks			
	OK Cancel			

Figure17-2 Custom Signature Setting

Name	Protocol	Src. Port	Dst. Port	Risk	Action	Log	Config	gure
Software_Crack_Website	ware_Crack_Website TCP 0:65535 80:80 🕻 🗢 🛛 🖬 🖬 🛛		Modify	Remove				

Figure17-3 Complete Custom Signature Setting

**Content** can fill in the character string which want to detect, or transform the ASCII code into hexa-decimals (ex.: cracks can transform into |63 726,163 6b 73|).

**STEP 3.** Enter the following settings in **Outgoing Policy** which enable the **IDP** function: (Figure17-4, 17-5)

Add New Policy	
Source Address	Inside_Any 💌
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	✓ Enable
Content Blocking	Enable
Authentication User	None
Schedule	None
Tunnel	None 🗸
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None 💌

OK Cancel

#### Figure17-4 IDP Policy Setting

Source	Destination	Service	Action		Option		Configure	Move
Inside_Any	Outside_Any	ANY	6	1		Modify Remove	To 1 🔽	

Figure17-5 Complete IDP Policy Setting

## **IDP** Report

MUS-MS300 can make intrusion detection and prevention record to be Log report, let the enterprise to know the data transmission security of overall network.

In this chapter, we will have the detailed illustration about IDP Report:

# **STEP 1.** In **Log** of **IDP Report** function, it will display the situation about intrusion detection and prevention of ALL7007. (Figure18-1)

2005-08-24 13:11:09 💌							
Time		Event	Signature Class.	Interface	Attack IP	Victim IP:Port	Action
2005-08-24 13:11:09	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:11:03	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:11:03	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:11:03	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:10:59	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:10:59	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 13:10:59	0	[SPYWARE] ISearchTech.com XXXP	A Network Trojan was	LAN	192.168.179.30	216.127.33.119:80	×
2005-08-24 12:58:05	0	[CUSTOM] Custom Signature- Soft	User Define level of	LAN	192.168.179.30	66.249.89.99:80	×
2005-08-24 12:57:42	0	[CUSTOM] Custom Signature- Soft	User Define level of	LAN	192.168.179.30	66.249.89.99:80	×
2005-08-24 12:57:29	0	[CUSTOM] Custom Signature- Soft	User Define level of	LAN	192.168.179.30	66.249.89.99:80	×
2005-08-24 12:57:23	0	[CUSTOM] Custom Signature- Soft	User Define level of	LAN	192.168.179.30	66.249.89.99:80	×

Clear Data





#### 1.Action:

Icon	ſ	×
	Pass	Drpo

#### 2.**Risk**:

Icon	6	8		
	High Risk	Medium Risk	Low Risk	

# LOG

The ALL7007 supports **Traffic Log** and **Event Log** to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the ALL7007.

Log records all connections that pass through the ALL7007's control policies. **Traffic Log**'s parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. **Event Log** record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.



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	Example	Page
	Situation		
Ex 1	Traffic Log	To detect the information and Protocol port that	301
		users use to access to Internet or Intranet by	
		ALL7007.	
Ex 2	Event Log	To record the detailed management events (such	305
		as Interface and event description of ALL7007)	
		of the Administrator	
Ex 3	Connection	To detect event description of WAN Connection	308
	Log		
Ex 4	Log Backup	To save or receive the records that sent by the	311
		ALL7007	

# To detect the information and Protocol port that users use to access to Internet or Intranet by ALL7007

STEP 1 . Add new policy in DMZ to WAN of Policy and select Enable Logging: (Figure19-1)

Add New Policy	
Source Address	DMZ_Any 💌
Destination Address	Outside_Any 🔽
Service	ANY
Action	PERMIT
Traffic Log	Enable
Statistics	🗆 Enable
IDP	🗆 Enable
Content Blocking	🗆 Enable
Anti-Virus	HTTP / WEBMAIL  FTP
Authentication User	None -
Schedule	None -
Tunnel	None -
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None -
	OK Cancel

Figure19-1 Logging Policy Setting

#### STEP 2 . Complete the Logging Setting in DMZ to WAN Policy: (Figure 19-2)

Source	Destination	Service	Action		Opt	ion	Configure	Move
DMZ_Any	Outside_Any	ANY	2	ĝ			Modify Remove	To 1
New Entry								

Figure19-2 Complete the Logging Setting of DMZ to WAN

STEP 3 . Click Traffic Log. It will show up the packets records that pass this policy. (Figure19-3)

Aug 10 10:03:01 💌 Next					
Time	Source	Destination	Protocol	Port	Disposition
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	2
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V

Clear Logs

Download Logs

Figure19-3 Traffic Log WebUI

STEP 4 . 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. (Figure19-4)

Aug 10 10:03:01 💌					
Time	Source	Destination	Protocol	Port	Disposition
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	2
Aug 1 File Download			×	80 => 4262	2
Aug 1	You have chose	e to download a file from this	location	4263 => 80	2
Aug 1	Tou nave chose	n to download a file from this	location.	4262 => 80	2
Aug 1	traffic.log from 17	2.19.100.85		4263 => 80	2
Aug 1				80 => 4263	2
Aug 1	What would you	like to do with this file?		4262 => 80	2
Aug 1	Open this file	from its current location		80 => 4262	2
Aug 1	Save this file	to disk.		80 => 4262	2
Aug 1				4263 => 80	2
Aug 1	Always ask b	efore opening this type of file		80 => 4263	2
Aug 1	$\geq$			4263 => 80	V
Aug 1				80 => 4263	V
Aug 1				80 => 4263	2
Aug 1		Cancel	More Info	4262 => 80	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	2
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	Clear Logs	)	Downloa	d Logs	

Figure19-4 Download Traffic Log Records WebUI

STEP 5 . Click Clear Logs and click OK on the confirm WebUI, the records will be deleted from the ALL7007 instantly. (Figure19-5)

Aug 10 10:03:01 💌					
Time	Source	Destination	Protocol	Port	Disposition
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	2
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	2
Aug 10 10:03:01	192.1 Microsoft In	nternet Explorer 🛛 🔀	TCP	4262 => 80	V
Aug 10 10:03:01	203.84.		TCP	80 => 4262	V
Aug 10 10:03:01	203.84. 🖓 🕻	Do you really want to clean?	TCP	80 => 4262	V
Aug 10 10:03:01	192.1		TCP	4263 => 80	$\swarrow$
Aug 10 10:03:01	203.84.		TCP	80 => 4263	2
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4263 => 80	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	2
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4263	$\swarrow$
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	$\swarrow$
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V
Aug 10 10:03:01	192.168.1.2	203.84.196.97	TCP	4262 => 80	V
Aug 10 10:03:01	203.84.196.97	192.168.1.2	TCP	80 => 4262	V

Clear Logs

Download Logs

Figure19-5 Clearing Traffic Log Records WebUI

### To record the detailed management events (such as Interface and event description of ALL7007) of the Administrator

STEP 1 . Click Event log of LOG. The management event records of the administrator to login ALL7007 will show up (Figure 19-6)

	Aug 11 00:20:10 - Next
Time	Event
Aug 11 00:20:10	user admin [Login success] from 192.168.1.2
Aug 10 23:54:19	user admin [Login success] from 192.168.1.2
Aug 10 10:02:03	admin Add [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Aug 10 10:01:53	admin Delete [Policy] (Outgoing,Mail_Server=>Outside_Any,Mail_Service_02,permit) from 192.168.1.2
Aug 10 10:01:37	admin Modify [Setting] from 192.168.1.2
Aug 10 10:00:31	admin Modify [WAN1 Interface] from 192.168.1.2
Jan 1 05:31:24	admin Modify [WAN1 Interface] from 192.168.1.2
Jan 1 05:30:59	admin Remove [Virtual Server 1] from 192.168.1.2
Jan 1 05:30:46	admin Delete [Policy] (Incoming,Outside_Any=>61.11.11.12,Mail_Service_01,permit) from 192.168.1.2
Jan 1 05:29:26	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2
Jan 1 05:10:28	admin Modify [Mail Relay] (Mail Server Domain Name: broadband.com.tw Mail Server IP Address: 192.168.2.12) from 192.168.1.2
Jan 1 05:09:22	admin Add [Policy] (Outgoing,Mail_Server=>Outside_Any,Mail_Service_02,permit) from 192.168.1.2
Jan 1 05:08:06	(null) Add [Policy] (Incoming,Outside_Any=>61.11.11.12,Mail_Service_01,permit) from 192.168.1.2
Jan 1 05:06:35	(null) Add [Mail_Service_01] (Virtual Server 1) from 192.168.1.2
Jan 1 05:06:08	(null) Add [Virtual Server 1] from 192.168.1.2
Jan 1 05:04:15	(null) Modify [WAN1 Interface] from 192.168.1.2
Jan 1 05:03:10	(null) Add [Service Group] Mail_Service_02 from 192.168.1.2
Jan 1 05:02:37	(null) Modify [Service Group] Mail_Service_01 from 192.168.1.2

Clear Logs

Download Logs

Figure19-6 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. (Figure 19-7)

Aug 11 00-20-10 💌 Nex				
Time	Event			
Aug 11 00:20:10	user admin [Login success] from 192.168.1.2			
Aug 10 23:54:19	user admin [Login success] from 192.168.1.2			
Aug 10 File Downloa	d X	ide_Any,ANY,permit) from		
Aug 10	You have chosen to download a file from this location. event.log from 61.218.49.28	ice_02,permit) from		
Aug 10 Aug 10 Jan 1 0	What would you like to do with this file? © Open this file from its current location © Save this file to disk			
Jan 1 0 Jan 1 0	Always ask before opening this type of file	2 ce_01,permit) from		
Jan 1 0		Outside_Any,ANY,permit)		
Jan 1 0	OK Cancel More Info	lame: broadband.com.tw 68.1.2		
Jan 1 05:09:22	admin Add [Policy] (Outgoing,Mail_Server=>Outside_Any,Mail_Serv 192.168.1.2	/ice_02,permit) from		
Jan 1 05:08:06	(null) Add [Policy] (Incoming,Outside_Any=>61.11.11.12,Mail_Serv 192.168.1.2	ice_01,permit) from		
Jan 1 05:06:35	(null) Add [Mail_Service_01] (Virtual Server 1) from 192.168.1.2			
Jan 1 05:06:08	(null) Add [Virtual Server 1] from 192.168.1.2			
Jan 1 05:04:15	(null) Modify [WAN1 Interface] from 192.168.1.2			
Jan 1 05:03:10	(null) Add [Service Group] Mail_Service_02 from	192.168.1.2		
Jan 1 05:02:37	(null) Modify [Service Group] Mail_Service_01 fr	om 192.168.1.2		
	Clear Logs Downloa	d Logs		

Figure19-7 Download Event Log Records WebUI

# STEP 3 . Click Clear Logs and click OK on the confirm WebUI; the records will be deleted from the ALL7007. (Figure19-8)

Aug 11 00:20:10 - Ne			
Time	Event		
Aug 11 00:20:10	user admin [Login success] from 192.168.1.2		
Aug 10 23:54:19	user admin [Login success] from 192.168.1.2		
Aug 10 10:02:03	admin Add [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2		
Aug 10 10:01:53	admin Delete [Policy] (Outgoing,Mail_Server=>Outside_Any,Mail_Service_02,permit) from 192.168.1.2		
Aug 10 10:01:37	admin Modify [Setting] from 192.168.1.2		
Aug 10 10:00:31	admi Microsoft Internet Explorer x pm 192.168.1.2		
Jan 1 05:31:24	admi pm 192.168.1.2		
Jan 1 05:30:59	admi O you really want to delete? rom 192.168.1.2		
Jan 1 05:30:46	admi (Inco <u>ок Cancel</u> 1.12,Mail_Service_01,permit) from 192.1		
Jan 1 05:29:26	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2		
Jan 1 05:10:28	admin Modify [Mail Relay] (Mail Server Domain Name: broadband.com.tw Mail Server IP Address: 192.168.2.12) from 192.168.1.2		
Jan 1 05:09:22	admin Add [Policy] (Outgoing,Mail_Server=>Outside_Any,Mail_Service_02,permit) from 192.168.1.2		
Jan 1 05:08:06	(null) Add [Policy] (Incoming,Outside_Any=>61.11.11.12,Mail_Service_01,permit) from 192.168.1.2		
Jan 1 05:06:35	(null) Add [Mail_Service_01] (Virtual Server 1) from 192.168.1.2		
Jan 1 05:06:08	(null) Add [Virtual Server 1] from 192.168.1.2		
Jan 1 05:04:15	(null) Modify [WAN1 Interface] from 192.168.1.2		
Jan 1 05:03:10	(null) Add [Service Group] Mail_Service_02 from 192.168.1.2		
Jan 1 05:02:37	(null) Modify [Service Group] Mail_Service_01 from 192.168.1.2		

Clear Logs

Download Logs

Figure19-8 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 ALL7007. (Figure 19-9)

	Jan 1 00:04:23 💌 Next
Time	Connection Log
Jan 1 00:04:23	Warning: couldn't open ppp database /var/run/pppd.tdb
Jan 1 00:04:23	pppd 2.4.1 started by root, uid 0
Jan 1 00:04:23	tdb_store failed: Invalid tdb context
Jan 1 00:04:23	Couldn't allocate PPP unit -1073449922 as it is already in use
Jan 1 00:04:23	Using interface ppp0
Jan 1 00:04:23	tdb_store failed: Invalid tdb context
Jan 1 00:04:23	PPPoE : Couldn't increase MTU to 1500
Jan 1 00:04:23	Couldn't increase MRU to 1500
Jan 1 00:04:25	local IP address 10.64.64.64
Jan 1 00:04:25	remote IP address 10.99.203.143
Jan 1 00:04:25	linkname : wan1 interface : ppp0
Jan 1 00:04:26	Sending PADI
Jan 1 00:04:26	HOST_UNIQ successful match
Jan 1 00:04:27	HOST_UNIQ successful match
Jan 1 00:04:27	Got connection: 1444
Jan 1 00:04:27	pads
Jan 1 00:04:27	Connecting PPPoE socket: 00:90:1a:40:09:87 1444 eth1 0x537e8
Jan 1 00:04:27	using channel 1

Clear Logs

Download Logs

Figure19-9 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. (Figure19-10)

Jan 1 00:04:23 💌			
Time	Connection Log		
Jan 1 00:04:23	Warning: couldn't open ppp database /var/run/pppd.tdb		
Jan 1 (0.04.23	nnnd 2 / 1 started hv root uid 0		
Jan 1 (			
Jan 1 (	You have chosen to download a file from this location. already in use		
Jan 1 (	local7.log from 172.19.100.85		
Jan 1 (			
Jan 1 (	What would you like to do with this file?		
Jan 1 (	O Dpen this file from its current location		
Jan 1 (	Save this file to disk		
Jan 1 (			
Jan 1 (	Always ask before opening this type of file		
Jan 1 (			
Jan 1 (			
Jan 1 (			
Jan 1 (	OK Cancel More Info		
Jan 1 60.04.21	paus		
Jan 1 00:04:27 Connecting PPPoE socket: 00:90:1a:40:09:87 1444 eth1 0x537e8			
Jan 1 00:04:27	using channel 1		
	Clear Logs Download Logs		

Figure19-10 Download Connection Log Records WebUI

STEP 3 . Click Clear Logs and click OK on the confirm WebUI, the records will be deleted from the ALL7007 instantly. (Figure19-11)

	Jan 1 00:04:23 💌 Next		
Time	Connection Log		
Jan 1 00:04:23	Warning: couldn't open ppp database /var/run/pppd.tdb		
Jan 1 00:04:23	pppd 2.4.1 started by root, uid 0		
Jan 1 00:04:23	tdb_store failed: Invalid tdb context		
Jan 1 00:04:23	Couldn't allocate PPP unit -1073449922 as it is already in use		
Jan 1 00:04:23	Using interface ppp0		
Jan 1 00:04:23	tdb_store failed		
Jan 1 00:04:23	PPPoE : Could		
Jan 1 00:04:23	Couldn't increa		
Jan 1 00:04:25	local IP addres		
Jan 1 00:04:25	remote IP addr OK Cancel		
Jan 1 00:04:25	linkname : wan <del>n mænace . pppo</del>		
Jan 1 00:04:26	Sending PADI		
Jan 1 00:04:26	HOST_UNIQ successful match		
Jan 1 00:04:27	HOST_UNIQ successful match		
Jan 1 00:04:27	Got connection: 1444		
Jan 1 00:04:27	pads		
Jan 1 00:04:27	Connecting PPPoE socket: 00:90:1a:40:09:87 1444 eth1 0x537e8		
Jan 1 00:04:27	using channel 1		

Clear Logs

Download Logs

Figure19-11 Clearing Connection Log Records WebUI

#### To save or receive the records that sent by the ALL7007

**STEP 1**. Enter **Setting** in **System**, select **Enable E-mail Alert Notification** function and set up the settings. (Figure19-12)

E-mail Setting	
Enable E-mail Alert Notification	
Device Name	NetGuardian (ex: NetGuardian)
Sender Address	<b>sender@mydomain.cor</b> (ex: sender@mydomain.com)
SMTP Server	mydomain.com ( ex: sender@mydomain.com )
E-mail Address 1	user1@mydomain.com ( ex: user1@mydomain.com )
E-mail Address 2	user2@mydomain.com (ex: user2@mydomain.com)
Mail Test	Mail Test

Figure19-12 E-mail Setting WebUI

STEP 2 . Enter Log Backup in Log, select Enable Log Mail Support and click OK (Figure19-13)

Log Mail Configuration			
Enable Log Mail Support			
When Log Full (300Kbytes)	When Log Full (300Kbytes), NetGuardian Appliance sends Log		
From SMTP Server	mydomain.com		
To E-mail Address 1	user1@mydomain.com		
E-mail Address 2	user2@mydomain.com		

Figure19-13 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 (Figure19-14)

Syslog Setting		
Enable Syslog Messages		
Syslog Host IP Address	140.35.21.3 (ex: 192.168.1.61)	
Syslog Host Port	514 (ex: 514)	
		OK Cancel

Figure19-14 Syslog Messages Setting WebUI

## **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 ALL7007 for statistics of packets and data that passes across the ALL7007. 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/Day)

#### 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, or days

#### 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)
  - **Time:** To detect the statistics by minutes, hours, or days

WAN Statistics is the additional function of WAN Interface. When enable WAN Interface, it will enable WAN Statistics too.

#### STEP 2 . Statistics Chart (Figure 20-1)

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



Figure20-1 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. (Figure 20-2)

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

**Figure 20-2 Policy Statistics Function** 

Solution with 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 chart every week; click Month to check the Statistics chart every month; click Year to check the Statistics chart every year

#### STEP 3 . Statistics Chart (Figure 20-3)

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



Figure 20-3 To Detect Policy Statistics

## Status

The users can know the connection status in Status. For example: LAN IP, WAN IP, Subnet Netmask, Default Gateway, DNS Server Connection, and its IP...etc.

- Interface Status: Display all of the current Interface status of the ALL7007
- **ARP Table:** Record all the ARP that connect to the ALL7007
- DHCP Clients: Display the table of DHCP clients that are connected to the ALL7007.

#### Interface

- **STEP 1** . Enter **Interface** in **Status** function; it will list the setting message for LAN, WAN, and DMZ Interface: (Figure21-1)
  - PPPoE Con. Time: The last time of the ALL7007 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 ALL7007 from the network Interface or not; or enter its WebUI
  - Forwarding Mode: The connection mode of the Interface
  - Default Gateway: To display the Gateway of WAN
  - DNS1: The DNS1 Server Address provided by ISP
  - DNS2: The DNS2 Server Address provided by ISP

Active Sessions Number : 16		0	System Uptime Day 0 Hour 48 Min 42 Sec
	LAN	WAN	DMZ
Forwarding Mode	NAT	Static IP	NAT
Max. Downstream / Upstream		30000 / 30000 Kbps	
PPPoE Con. Time			
MAC Address	00:e0:98:c3:32:61	00:e0:98:c3:32:62	00:e0:98:c3:32:63
IP Address	192.168.1.1	172.19.20.11	192.168.2.1
Netmask	255.255.255.0	255.255.0.0	255.255.255.0
Default Gateway		172.19.1.254	
DNS1		168.95.1.1	
DNS2		0.0.0	
Rx Pkts, Error Pkts	10194, 0	4490, 0	0, 0
Tx Pkts, Error Pkts	8238, 0	3333, 0	106, 0
Ping	V	V	V
НТТР	V	V	V

**Figure21-1 Interface Status Function** 

### **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 ALL7007: (Figure21-2)
  - 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
172.19.1.254	00:0C:7C:00:04:39	WAN
172.19.1.106	00:0C:76:B4:E4:CE	WAN
192.168.1.2	00:01:80:41:D0:AE	LAN

Figure21-2 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 ALL7007: (Figure21-3)
  - 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		
ii Address		Start	End	
192.168.1.2	00:01:80:41:d0:ae	2005/8/11 9:20:23	2005/8/12 9:20:23	

Figure 21-3 DHCP Clients WebUI



Germering, den

27.04.05

#### CE-Kennzeichnung und EG-Konformitätserlärung

Für das folgend bezeichnete Erzeugnis

#### ALL7007 Anti-Spam Anti-Virus Firewall

#### **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 ALL7007 Anti-Spam Anti-Virus Firewall 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 50022 :1998 (A1 :2000 Class B), EN 61000-3-2 :2000 Class A, EN 61000-3-3 :1995+A1 :2001

EMS: EN 55024 :1998 (A1 :2001)

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 <u>http://www.allnet.de/ce-certificates/</u> eingesehen werden.