PLANET
Networking & Communication

VPN Security Gateway

SG-1000

User’s Manual

Copyright

The products and programs described in this User’s Manual are licensed products of PLANET Technology, This User’s Manual contains proprietary information protected by copyright, and this User’s Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User’s Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User’s Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User’s Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User’s Manual. PLANET makes no commitment to update or keep current the information in this User’s Manual, and reserves the right to make improvements to this User’s Manual and/or to the products described in this User’s Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

This is a class A device, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Customer Service

For information on customer service and support for the VPN Security Gateway, please refer to the following Website URL:

http://www.planet.com.tw

Before contacting customer service, please take a moment to gather the following information:

- VPN Security Gateway serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User’s Manual for PLANET VPN Security Gateway

Model: SG-1000

Rev: 1.0 (October, 2006)

PartNo.EM-SG1000v1

Table of Contents

System

Interface

Policy Object

Policy

Web VPN / SSL VPN

Anti-Attack

Monitor

Chapter 1

Introduction

The innovation of the Internet has created a tremendous worldwide venue for E-business and information sharing, but it also creates network security problems. The security request will be the primary concerned for the enterprise. New model of Planet's VPN Security Gateway SG-1000, a special designed of VPN security gateway, provides SSL, IPSec, and PPTP VPN. The SSL VPN function supports up to 50 SSL VPN connection tunnels. The IPSec VPN feature provides IPSec VPN Trunk and IKE, SHA-1, and MD5 Authentication. The PPTP VPN function supports PPTP server and client.

The SG-1000 provides Content Blocking feature to block specific URL, Script, IM, P2P, and download file. Also, it is built-in Anomaly Flow IP function. This function supports Hacker and Blaster Alert. An administrator could use this function to watch and track an attacker.

This product is built-in two WAN ports. It supports WAN Load Balance and Fail-Over Feature. Also, the QoS function provides Guaranteed Bandwidth and Priority Bandwidth Utilization.

Product Features

- **VPN Connectivity:** The VPN security gateway supports SSL VPN, IPSec VPN, and PPTP server/client. The SSL VPN function supports up to 50 SSL VPN connection tunnels. The IPSec VPN has DES, 3DES, and AES encryption and SHA-1 / MD5 authentication. The network traffic over public Internet is secured.
- **VPN Trunk:** VPN trunk function provides VPN load balance and VPN fail-over feature to keep the VPN connection more reliable.
- **Content Filtering:** The security gateway can block network connection based on **URLs**, **Scripts** (The Pop-up, Java Applet, cookies and Active X), **P2P** (eDonkey, Bit Torrent and WinMX), **Instant Messaging** (MSN, Yahoo Messenger, ICQ, QQ and Skype) and **Download**. If there are new updated version of P2P or IM

software in client side, SG-1000 will detect the difference and update the Content Filtering pattern to renew the filtering mechanism.

- **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including SYN attack, ICMP flood, UDP flood, Ping of Death, etc. The access control function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- **QoS:** Network packets can be classified based on IP address, IP subnet and TCP/UDP port number and give guarantee and maximum bandwidth with three levels of priority.
- **Authentication:** Web-based authentication allows users to be authenticated by web browser. User database can be configured on the devices or through external RADIUS server.
- **WAN Backup:** The SG-1000 can monitor each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including “Auto”, “Round-Robin”, “By Traffic”, “By Session” and “By Packet”. User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- **Multiple NAT:** Multiple NAT allows local port to set multiple subnet works and connect to the Internet through different WAN IP addresses.

1.1 Package Contents

SG-1000 x 1

Power Cord x 1

Quick Installation Guide x 1

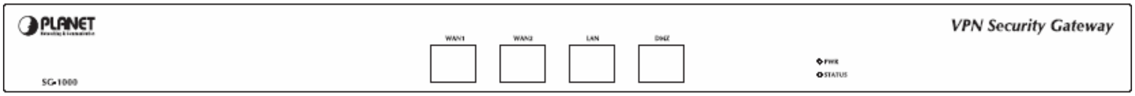
User’s Manual CD x 1

Console cable x 1

RJ-45 cable

Rack-mount ear

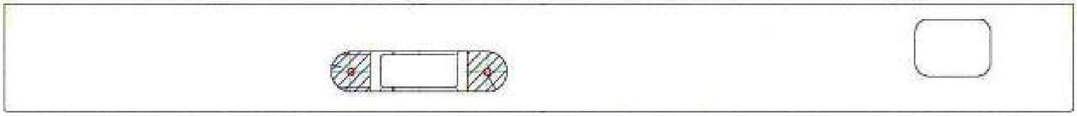
1.2 Front View



- LED definition

LED	Description	
PWR	Power is supplied to this device.	
STATUS	Blinks to indicate this devise is being turned on and booting. After one minute, this LED indicator will stop blinking, it means this device is now ready to use.	
WAN1, WAN2, LAN, DMZ	Green	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
	Orange	Steady on indicates the port is connected at 100Mbps speed

1.3 Rear View



1.4 Specification

Product		VPN Security Gateway
Model		SG-1000
Recommend concurrent user		30 ~ 50
Hardware		
Ethernet	LAN	1 x 10/100 Based-TX RJ-45
	WAN	2 x 10/100 Based-TX RJ-45
	DMZ	1 x 10/100 Based-TX RJ-45
Software		

Management	Web
Network Connection	Transparent mode, NAT, Multi-NAT
Routing Mode	Static Route, RIPv2
Concurrent Sessions	110,000
New session / second	10,000
WAN to LAN Throughput	100Mbps
VPN Throughput	18Mbps
VPN 3DES Throughput	17Mbps
VPN Function	SSL, IPSec, PPTP server and client DES, 3DES, and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN VPN Trunk
SSL VPN	Internal Subnet of Server: 10 Connection Tunnels: 50
IPSec VPN Trunk	50
VPN Connection Tunnels / Allow to Configure	IPSec: 100 / 200 PPTP Serve: 32 / 32 PPTP Client: 16 / 16
Content Filtering	URL Blocking Blocks Popup, Java Applet, cookies and Active X P2P Application Blocking Instant Message Blocking Download Blocking
Firewall	Policy-based Firewall rule with schedule NAT/ NAPT, SPI Firewall
QoS	Policy-based bandwidth management Guarantee and maximum bandwidth with 3 priority levels Classify traffics based on IP, IP subnet, TCP/UDP port
User authentication	Built-in user database with up to 200 entries Support local database, RADIUS and POP3 authentication
Logs	Log and alarm for event and traffic Log can be saved from web, sent by e-mail or sent to syslog server
Accounting Report	Record inbound and outbound traffic’s utilization by Source IP, Destination IP and Service
Statistics	Traffic statistic for WAN interface and policies Graphic display
Others	Dynamic DNS, NTP, DHCP server, Virtual server,

Chapter 2

Administration

“System” is the managing of settings such as the privileges of packets that pass through the SG-1000 and monitoring controls. The System Administrators can manage, monitor, and configure SG-1000 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 SG-1000.

Define the required fields of Administrator

Administrator Name:

- The username of Administrators and Sub Administrator for the SG-1000. 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.”

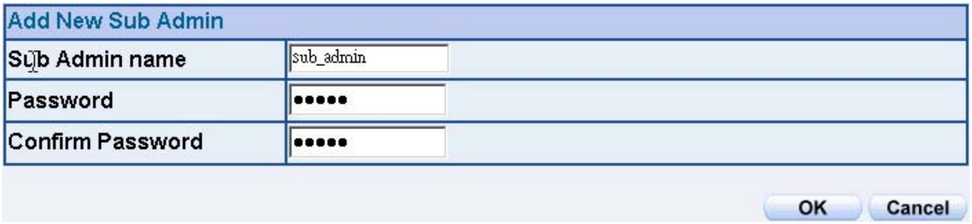
2.1 Adding a new Sub Administrator

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

STEP 2 . In the **Add New Sub Administrator** Web UI 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	●●●●●

Add New Sub Admin

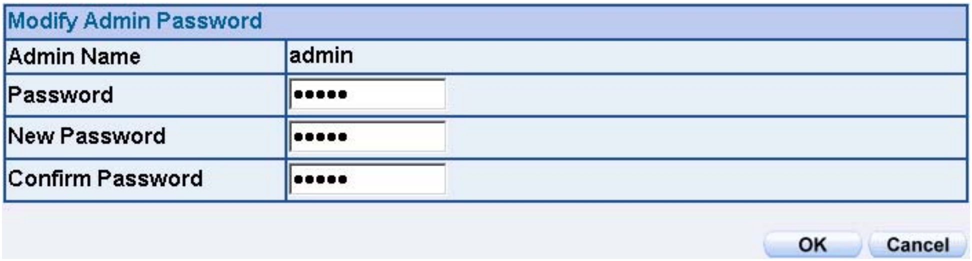
Modify the Administrator's Password

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

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

- **Password:** admin
- **New Password:** 52364
- **Confirm Password:** 52364

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



Modify Admin Password

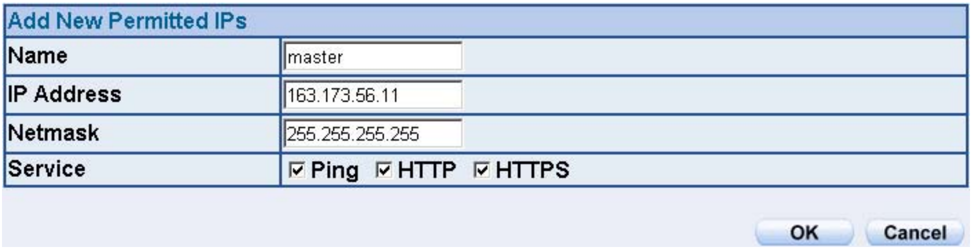
Admin Name	admin
Password	●●●●●
New Password	●●●●●
Confirm Password	●●●●●

Modify Admin Password

2.2 Add Permitted IPs

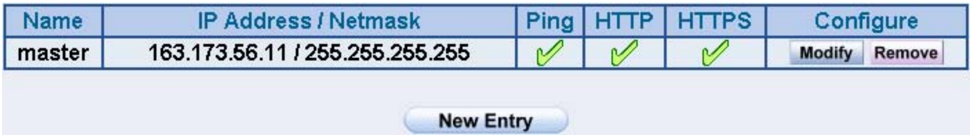
STEP 1．Add the following setting in **Permitted IPs** of **Administration**:

- **Name:** Enter master
- **IP Address:** Enter 163.173.56.11
- **Netmask:** Enter 255.255.255.255
- **Service:** Select Ping, HTTP, and HTTPS.
- Click **OK**
- Complete add new permitted IPs



Add New Permitted IPs	
Name	master
IP Address	163.173.56.11
Netmask	255.255.255.255
Service	☑ Ping ☑ HTTP ☑ HTTPS

Setting Permitted IPs Web UI



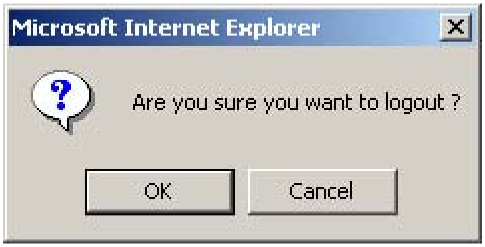
Name	IP Address / Netmask	Ping	HTTP	HTTPS	Configure
master	163.173.56.11 / 255.255.255.255	✓	✓	✓	Modify Remove

Complete Add New Permitted Ips

To make Permitted IPs be effective, it must cancel the **Ping**, **HTTP**, and **HTTPS** selection in the Web UI of SG-1000 that Administrator enter. (LAN, WAN, or DMZ Interface) Before canceling the **HTTP** and **HTTPS** selection of Interface, must set up the Permitted IPs first, otherwise, it would cause the situation of cannot enter Web UI by appointed Interface.

2.3 Logout

STEP 1 . Click **Logout** which locate in **Browser's** above right to protect the system while Administrator are away.

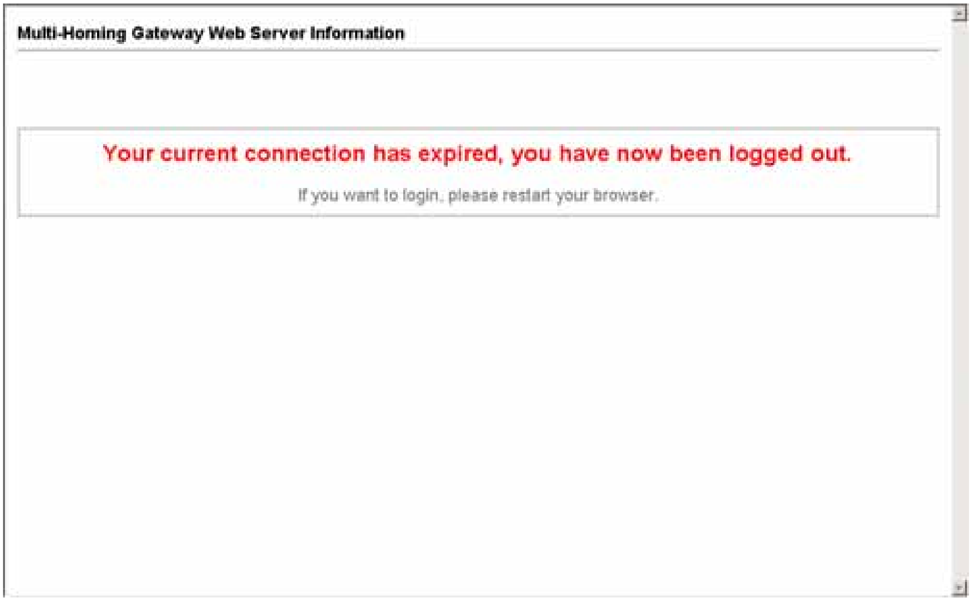


Microsoft Internet Explorer

Are you sure you want to logout ?

Confirm Logout Web UI

STEP 2．Click **OK** and the logout message will appear in Web UI.



Multi-Homing Gateway Web Server Information

Your current connection has expired, you have now been logged out.

If you want to login, please restart your browser.

Logout Web UI Message

2.4 Software Update

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

- To obtain the version number from **Version Number** and obtain the latest version from Internet. And save the latest version in the hardware of the PC, which manage the SG-1000
- Click **Browse** and choose the latest software version file.
- Click **OK** and the system will update automatically.

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 Web UI. It may cause some unexpected mistakes. (Strong suggests updating the software from LAN to avoid unexpected mistakes.)

Chapter 3

Configure

The Configure is according to the basic setting of the SG-1000. In this chapter the definition is Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Hosts Table, and Language settings.

Define the required fields of Settings

SG-1000 Configuration:

- The Administrator can import or export the system settings. Click **OK** to import the file into the SG-1000 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 SG-1000 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 Web UI management)

After HTTP port has changed, if the administrator want to enter Web UI 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 SG-1000 will record packet which source IP or destination address is SG-1000. And record in Traffic Log for System Manager to inquire about.

Define the required fields of Time Settings

Synchronize Time/Date:

- Synchronizing the SG-1000 with the System Clock. The administrator can configure the SG-1000’s date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer’s clock.

GMT:

- International Standard Time (Greenwich Mean Time)

Define the required fields of Multiple Subnet

Forwarding Mode:

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

WAN Interface Address:

- The IP address that Multiple Subnet corresponds to WAN.

LAN Interface Address/Subnet Netmask:

- The Multiple Subnet range

NAT Mode:

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

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

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

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

Routing Mode:

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

Define the required fields of DHCP

Subnet:

- The domain name of LAN

NetMask:

- The LAN Netmask

Gateway:

- The default Gateway IP address of LAN

Broadcast IP:

- The Broadcast IP of LAN

Define the required fields of DDNS

Domain Name:

- The domain name that provided by DDNS

WAN IP Address:

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

Define the required fields of Host Table

Domain Name:

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

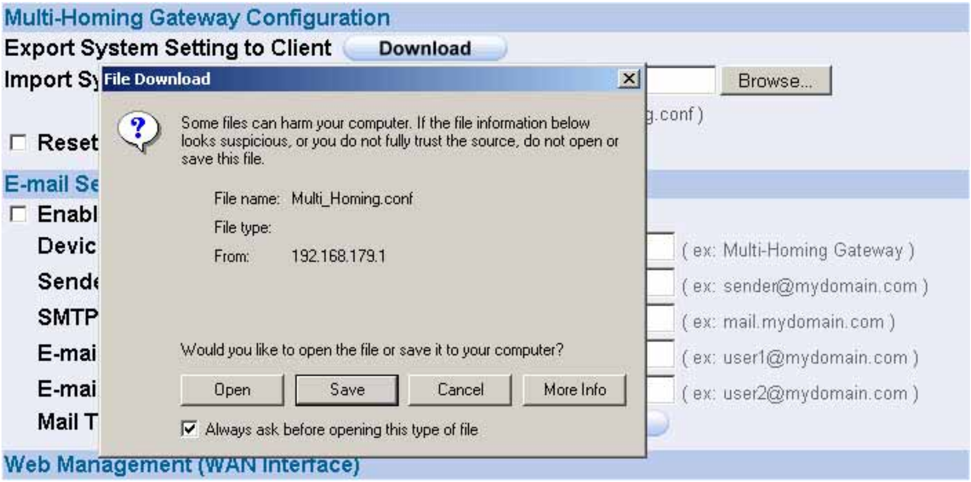
Virtual IP Address:

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

System Settings- Exporting

STEP 1． In System Setting Web UI, click on Download button next to Export System Settings to Client.

STEP 2． When the **File Download** pop-up window appears, choose the destination place where to save the exported file and click on **Save**. The setting value of SG-1000 will copy to the appointed site instantly.



Multi-Homing Gateway Configuration

Export System Setting to Client Download

Import Sy

Browse...

g.conf)

□ Reset

E-mail Se

□ Enabl

Devic (ex: Multi-Homing Gateway)

Sende (ex: sender@mydomain.com)

SMTP (ex: mail.mydomain.com)

E-mai (ex: user1@mydomain.com)

E-mai (ex: user2@mydomain.com)

Mail T

Web Management (WAN Interface)

File Download ☒

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: Multi_Homing.conf

File type:

From: 192.168.179.1

Would you like to open the file or save it to your computer?

Open | Save | Cancel | More Info

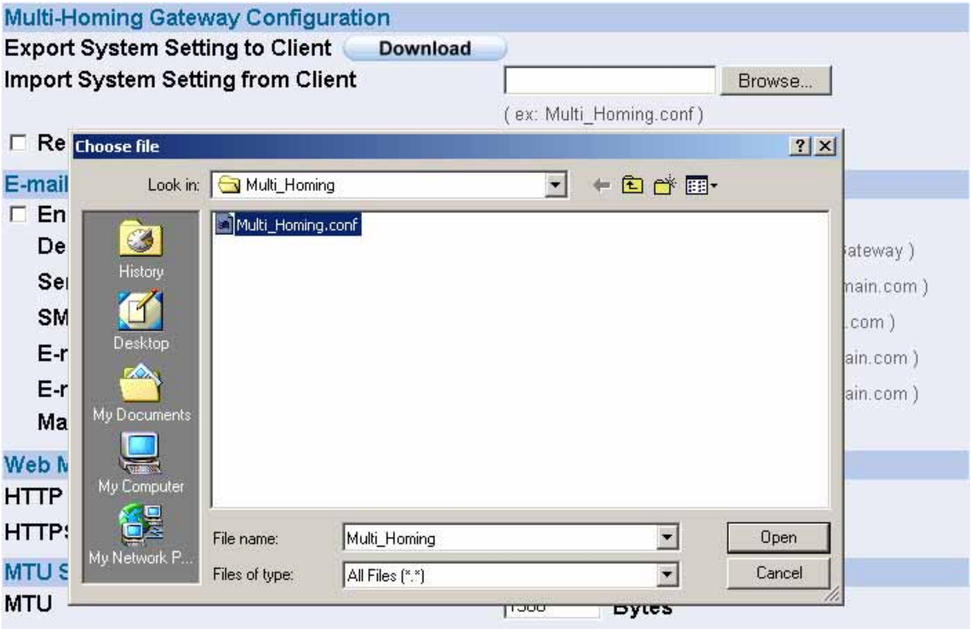
☑ Always ask before opening this type of file

Select the Destination Place to Save the Exported File

3.1 System Settings- Importing

STEP 1． In **System Setting** Web UI, 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 SG-1000 Settings, then click **OK**.

STEP 2． Click **OK** to import the file into the SG-1000



Multi-Homing Gateway Configuration

Export System Setting to Client Download

Import System Setting from Client Browse...

(ex: Multi_Homing.conf)

Choose file

Look in: Multi_Homing

Multi_Homing.conf

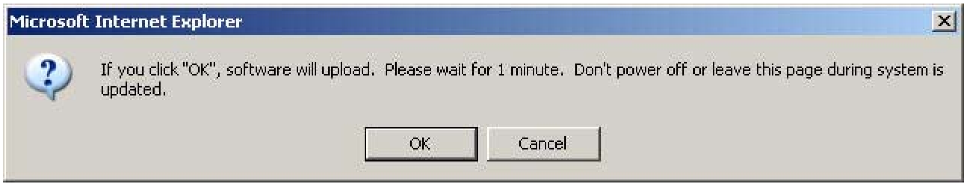
File name: Multi_Homing

Files of type: All Files (*.*)

Open

Cancel

Enter the File Name and Destination of the Imported File



Microsoft Internet Explorer

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

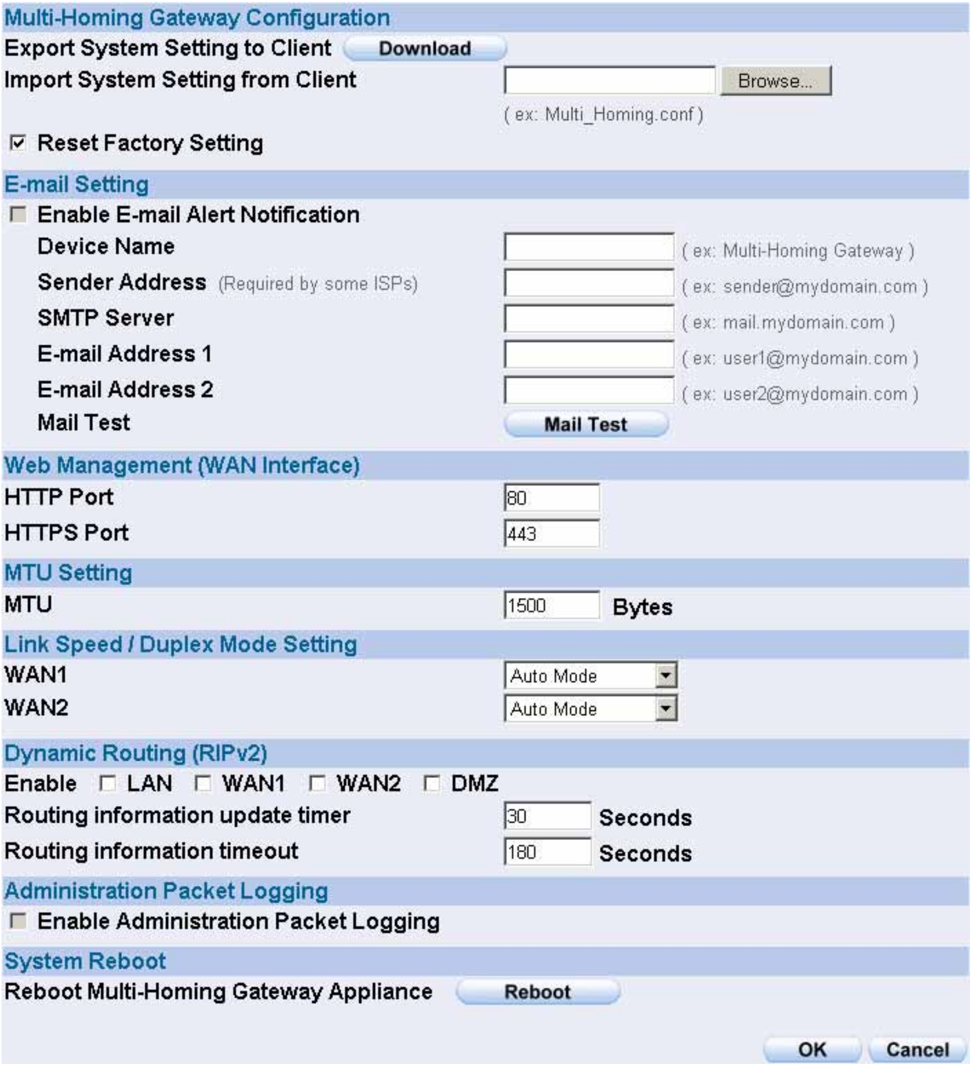
OK Cancel

Upload the Setting File Web UI

Restoring Factory Default Settings

STEP 1． Select **Reset Factory Settings** in SG-1000 **Configuration** Web UI

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



Multi-Homing Gateway Configuration

Export System Setting to Client [Download]

Import System Setting from Client [ ] [Browse...]

(ex: Multi_Homing.conf)

☑ Reset Factory Setting

E-mail Setting

□ Enable E-mail Alert Notification

Device Name [ ] (ex: Multi-Homing Gateway)

Sender Address (Required by some ISPs) [ ] (ex: sender@mydomain.com)

SMTP Server [ ] (ex: mail.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]

HTTPS Port [443]

MTU Setting

MTU [1500] Bytes

Link Speed / Duplex Mode Setting

WAN1 [Auto Mode]

WAN2 [Auto Mode]

Dynamic Routing (RIPv2)

Enable □ LAN □ WAN1 □ WAN2 □ DMZ

Routing information update timer [30] Seconds

Routing information timeout [180] Seconds

Administration Packet Logging

□ Enable Administration Packet Logging

System Reboot

Reboot Multi-Homing Gateway Appliance [Reboot]

[OK] [Cancel]

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.

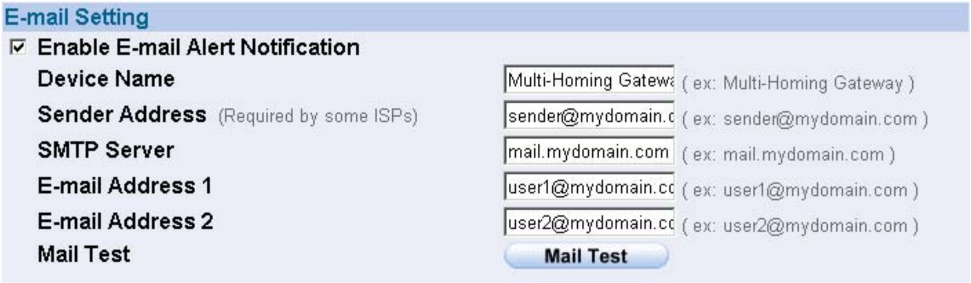
STEP 3．Sender Address: Enter the Sender Address. (Required by some ISPs.)

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.



E-mail Setting

☑ Enable E-mail Alert Notification

Device Name	Multi-Homing Gatewa	(ex: Multi-Homing Gateway)
Sender Address (Required by some ISPs)	sender@mydomain.c	(ex: sender@mydomain.com)
SMTP Server	mail.mydomain.com	(ex: mail.mydomain.com)
E-mail Address 1	user1@mydomain.cc	(ex: user1@mydomain.com)
E-mail Address 2	user2@mydomain.cc	(ex: user2@mydomain.com)
Mail Test	Mail Test	

Enable E-mail Alert Notification

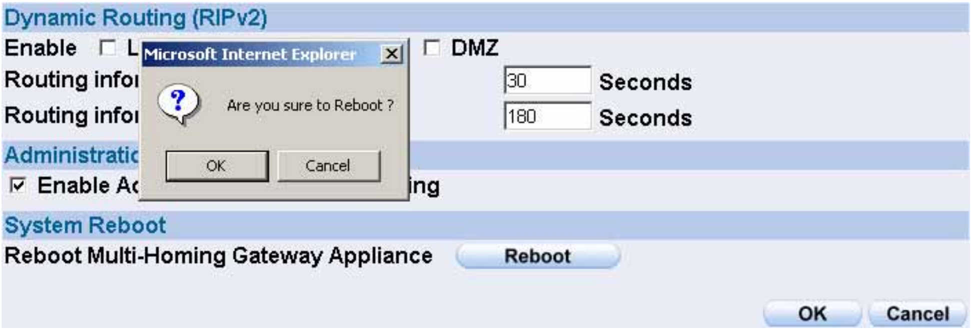
Click on **Mail Test** to test if E-mail Address 1 and E-mail Address 2 can receive the Alert Notification correctly.

Reboot SG-1000

STEP 1．Reboot SG-1000：Click **Reboot** button next to **Reboot SG-1000 Appliance.**

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

STEP 3．Follow the confirmation pop-up page; click **OK** to restart SG-1000.



Dynamic Routing (RIPv2)

Enable □ L □ DMZ

Routing infor 30 Seconds

Routing infor 180 Seconds

Administratic

☑ Enable Ac ing

System Reboot

Reboot Multi-Homing Gateway Appliance

Microsoft Internet Explorer

Are you sure to Reboot ?

Reboot SG-1000

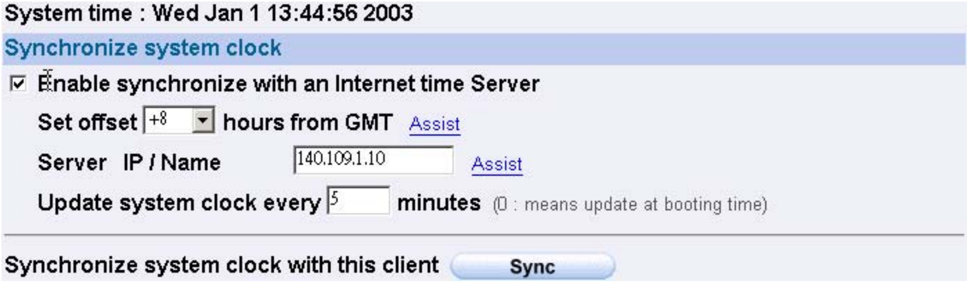
3.2 Date/Time Settings

STEP 1．Select **Enable synchronize with an Internet time Server**

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

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

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



System time : Wed Jan 1 13:44:56 2003

Synchronize system clock

☑ Enable synchronize with an Internet time Server

Set offset +8 hours from GMT Assist

Server IP / Name 140.109.1.10 Assist

Update system clock every 5 minutes (0 : means update at booting time)

Synchronize system clock with this client Sync

System Time Setting

Click on the **Sync** button and then the SG-1000'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**.

3.3 Multiple Subnet

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

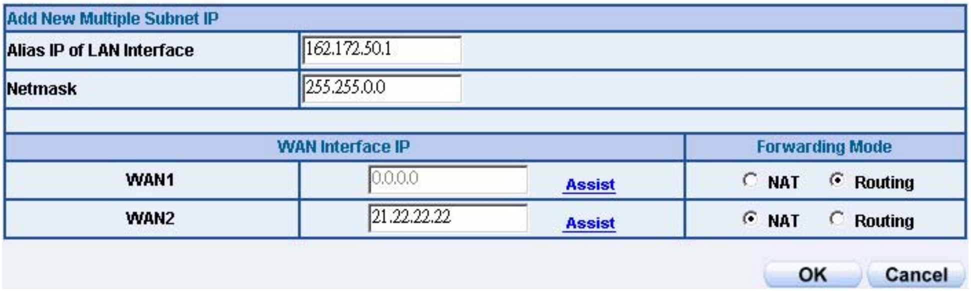
Preparation

SG-1000 WAN1 (10.10.10.1) connect to the ISP Router (10.10.10.2) and the subnet that provided by ISP is 162.172.50.0/24
To connect to Internet, WAN2 IP (211.22.22.22) connects with ATUR.

Adding Multiple Subnet

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

- Click on **New Entry**
- **Alias IP of LAN Interface**： Enter 162.172.50.1
- **Netmask**：Enter 255.255.255.0
- **WAN1:** Enter Interface IP 10.10.10.1, and choose **Routing** in **Forwarding Mode**
- **WAN2**：Enter Interface IP 211.22.22.22, and choose **NAT** in **Forwarding Mode**
- Click **OK**
- Complete Adding Multiple Subnet



Add New Multiple Subnet IP			
Alias IP of LAN Interface	162.172.50.1		
Netmask	255.255.0.0		
WAN Interface IP			Forwarding Mode
WAN1	0.0.0.0	Assist	○ NAT ● Routing
WAN2	21.22.22.22	Assist	● NAT ○ Routing

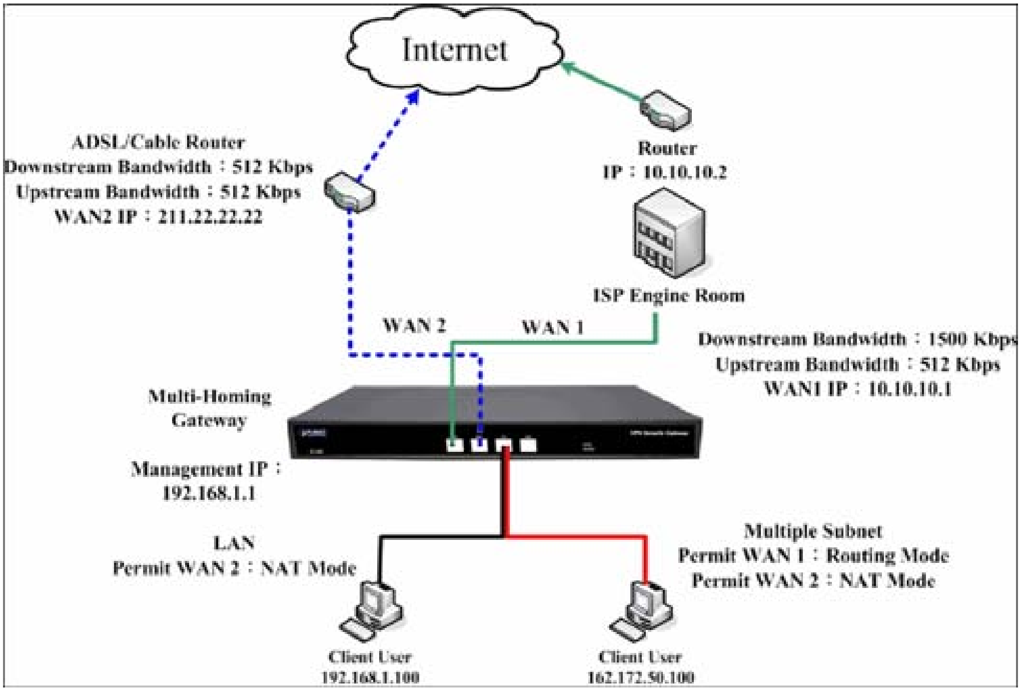
Add Multiple Subnet Web UI

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

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

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

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



Multiple Subnet Network

- The SG-1000’s Interface Status:
  WAN1 IP： 10.10.10.1
  WAN2 IP：211.22.22.22
  LAN Port IP：192.168.1.1
  LAN Port Multiple Subnet：162.172.50.1

3.4 Route Table

To connect two different subnet router with the SG-1000 and makes them to connect to Internet through SG-1000.

Preparation

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

WAN2 (211.22.22.22) connects with ATUR to Internet

LAN subnet: 192.168.1.1/24

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

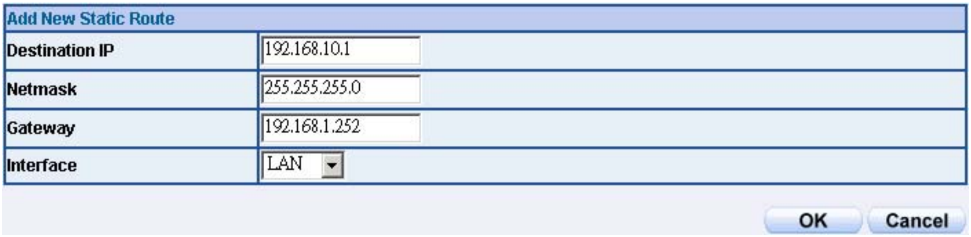
Company B: Router2 (10.10.10.2, support RIPv2), its LAN subnet is 192.168.20.1/24

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

Route Table

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

- 【Destination IP】: Enter 192.168.10.1
- 【Netmask】: Enter 255.255.255.0。
- 【Gateway】: Enter 192.168.1.252
- 【Interface】: Select LAN
- Click **OK**

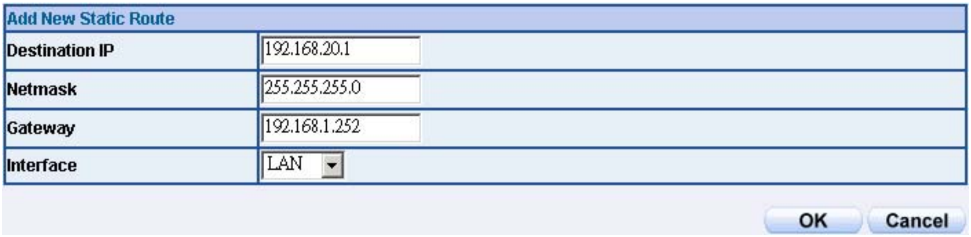


Add New Static Route	
Destination IP	192.168.10.1
Netmask	255.255.255.0
Gateway	192.168.1.252
Interface	LAN

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**

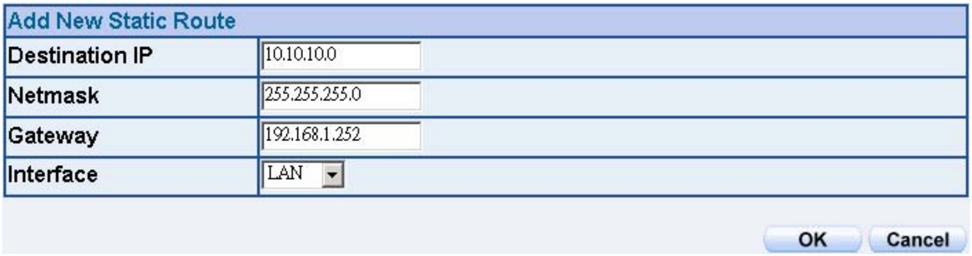


Add New Static Route	
Destination IP	192.168.20.1
Netmask	255.255.255.0
Gateway	192.168.1.252
Interface	LAN

Add New Static Route2

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

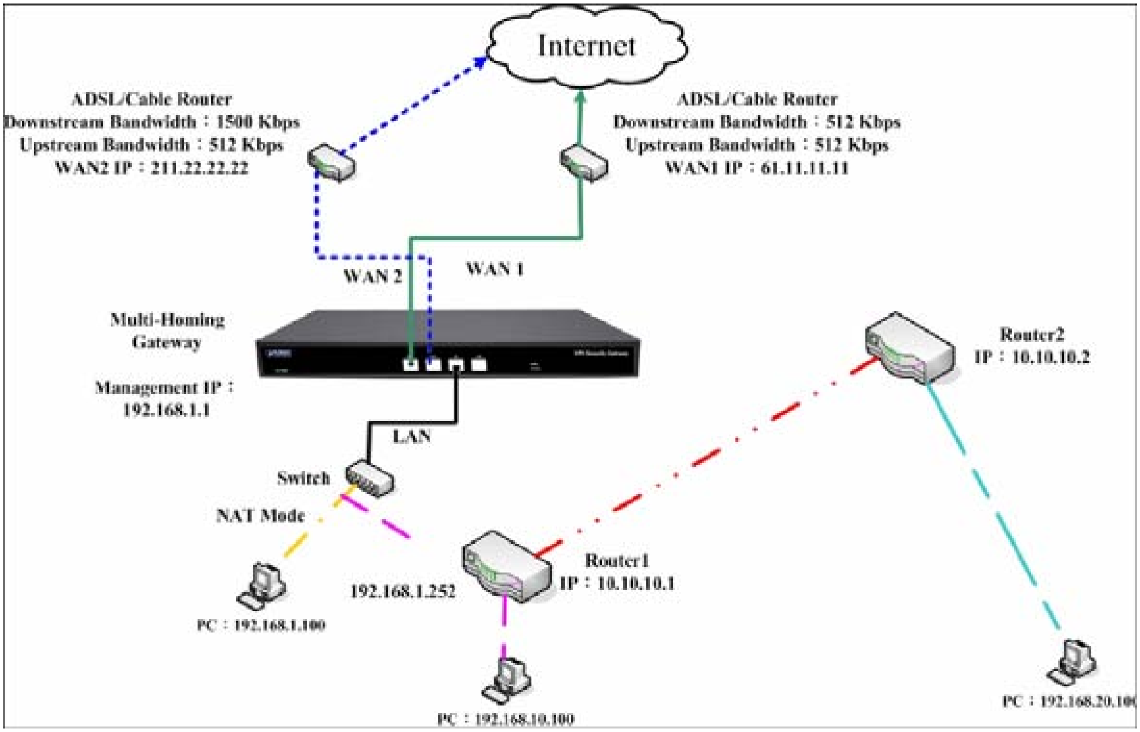
- 【Destination IP】: Enter 10.10.10.0
- 【Netmask】: Enter 255.255.255.0
- 【Gateway】: Enter 192.168.1.252
- 【Interface】: Select LAN
- Click **OK**



Add New Static Route	
Destination IP	10.10.10.0
Netmask	255.255.255.0
Gateway	192.168.1.252
Interface	LAN

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.

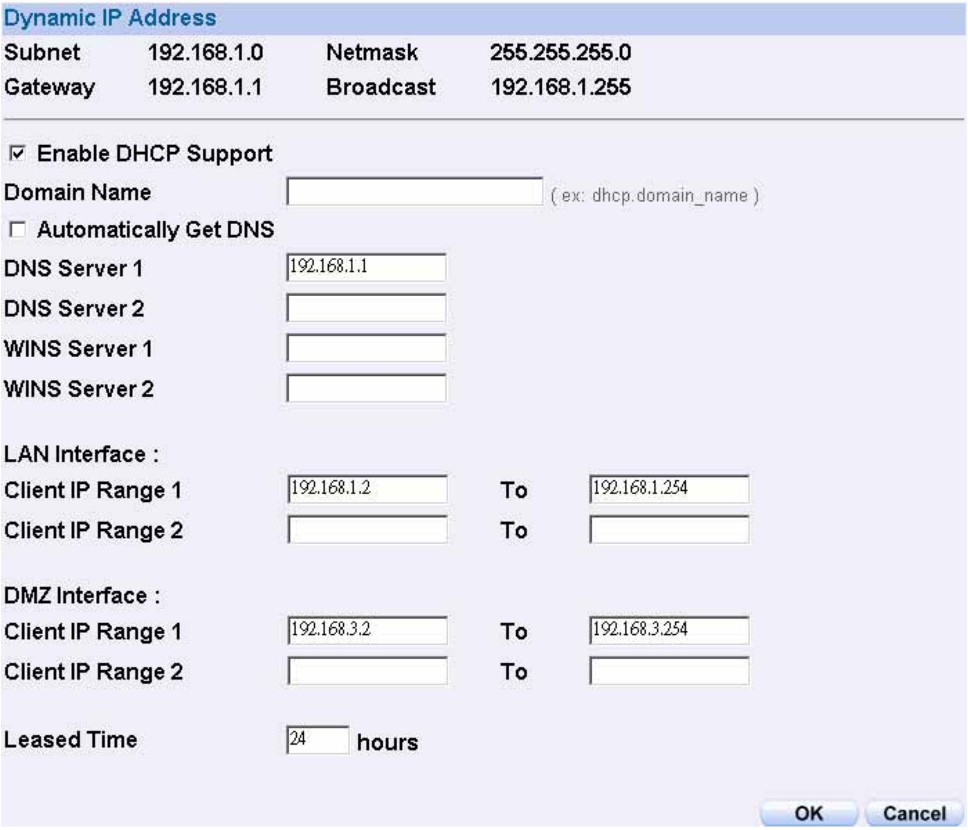


Route Table Setting

3.5 DHCP

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

- **Domain Name**：Enter the Domain Name
- **DNS Server 1**: Enter the distributed IP address of DNS Server1.
- **DNS Server 2**: Enter the distributed IP address of DNS Server2.
- **WINS Server 1**: Enter the distributed IP address of WINS Server1.
- **WINS Server 2:** Enter the distributed IP address of WINS Server2.
- **LAN Interface:**
    - **Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. The default value is 192.168.1.2 to 192.168.1.254 (it must be in the same subnet)
    - **Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. But it must in the same subnet as **Client IP Address Range 1** and the range cannot be repeated.
- **DMZ Interface:** the same as LAN Interface. (DMZ works only if to enable DMZ Interface)
- **Leased Time:** Enter the leased time for Dynamic IP. The default time is 24 hours.
- Click **OK** and DHCP setting is completed.



Dynamic IP Address

Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

☑ Enable DHCP Support

Domain Name (ex: dhcp.domain_name)

☐ Automatically Get DNS

DNS Server 1	192.168.1.1
DNS Server 2	
WINS Server 1	
WINS Server 2	

LAN Interface :

Client IP Range 1	192.168.1.2	To	192.168.1.254
Client IP Range 2		To	

DMZ Interface :

Client IP Range 1	192.168.3.2	To	192.168.3.254
Client IP Range 2		To	

Leased Time 24 hours

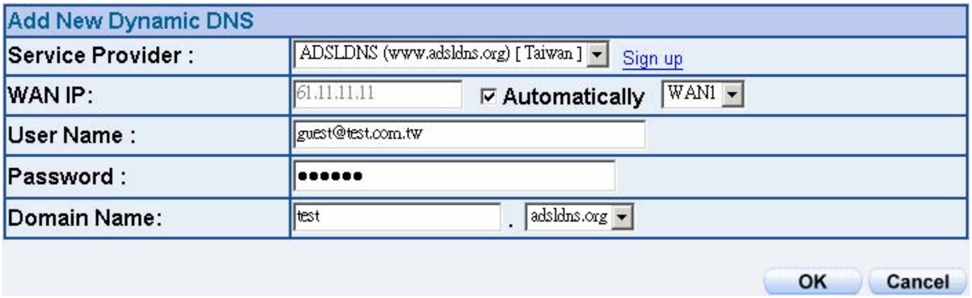
DHCP Web UI

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

3.6 Dynamic DNS Settings

STEP 1．Select **Dynamic DNS** in **System** function. Click **New Entry** button

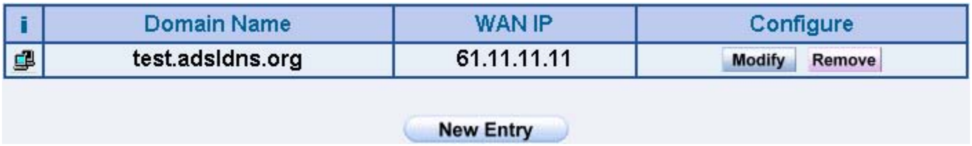
- **Service providers**：Select service providers.
- **Automatically fill in the WAN 1/2 IP**：Check to automatically fill in the WAN 1/2 IP.。
- **User Name**：Enter the registered user name.
- **Password**：Enter the password
- **Domain name**：Enter Your host domain name
- Click **OK** to add Dynamic DNS.



Add New Dynamic DNS

Service Provider :	ADSLDNS (www.adsldns.org) [Taiwan] ▾ Sign up
WAN IP:	61.11.11.11 ☑ Automatically WAN1 ▾
User Name :	guest@test.com.tw
Password :	••••••
Domain Name:	test . adsldns.org ▾

DDNS Web UI



i	Domain Name	WAN IP	Configure
🖧	test.adsldns.org	61.11.11.11	Modify Remove

Complete DDNS Setting

Chart	✓	✗	🖥	⚠
Meaning	Update successfully	Incorrect username or password	Connecting to server	Unknown error

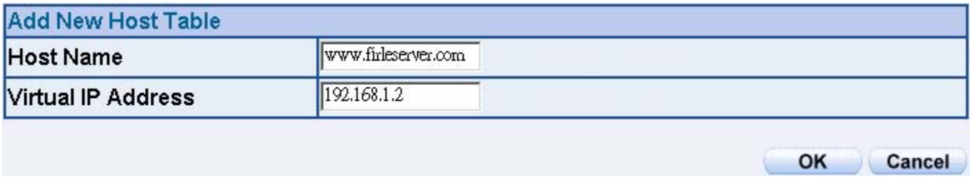
If System Administrator had not registered a DDNS account, click on **Sign up** then can enter the website of the provider.

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

3.7 Host Table

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

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



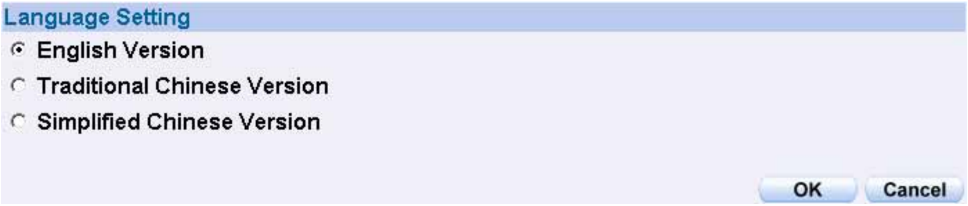
Add New Host Table	
Host Name	www.firleserver.com
Virtual IP Address	192.168.1.2

Add New Host Table

To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of SG-1000. That is, the default gateway.

3.8 Language

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



Language Setting

● English Version

○ Traditional Chinese Version

○ Simplified Chinese Version

Language Setting Web UI

Chapter 4

Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the LAN network, the WAN 1/2 network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

Define the required fields of Interface

LAN:

- Using the LAN **Interface**, the Administrator can set up the LAN network of SG-1000.

Ping:

- Select this function to allow the user to ping the Interface IP Address.

HTTP:

- Select to enable the user to enter the Web UI of SG-1000 from Interface IP through HTTP protocol.

HTTPS:

- Select to enable the user to enter the Web UI of SG-1000 from Interface IP through HTTPS protocol.

WAN:

- The System Administrator can set up the WAN network of SG-1000.

Balance Mode:

- **Auto:** The SG-1000 will adjust the WAN 1/2 utility rate automatically according to the downstream/upstream of WAN. (For users who are using various download bandwidth)
- **Round-Robin:** The SG-1000 distributes the WAN 1/2 download bandwidth 1:1, in other words, it selects the agent by order. (For users who are using same download bandwidths)
- **By Traffic:** The SG-1000 distributes the WAN 1/2 download bandwidth by accumulative traffic.
- **By Session:** The SG-1000 distributes the WAN 1/2 download bandwidth by saturated connections.
- **By Packet:** The SG-1000 distributes the WAN 1/2 download bandwidth by accumulated packets and saturated connection.

Connect Mode:

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

Saturated Connections:

- Set the number for saturation whenever session numbers reach it, the SG-1000 switches to the next agent on the list.

Priority:

- Set priority of WAN for Internet Access.

Connection Test:

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

Upstream/Downstream Bandwidth:

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

Auto Disconnect:

- The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter the amount of idle time before disconnection in the field. Enter “0” if you do not want the PPPoE connection to disconnect at all.

DMZ:

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

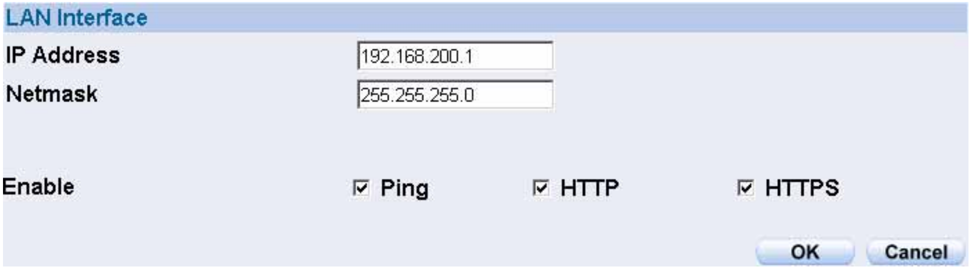
We set up four Interface Address examples in this chapter:

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

4.1 Modify LAN Interface Settings

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

- Enter the new **IP Address** and **Netmask**
- Select **Ping**, **HTTP**, and **HTTPS**.
- Click **OK**



LAN Interface

IP Address	192.168.200.1
Netmask	255.255.255.0
Enable	☑ Ping ☑ HTTP ☑ HTTPS

Setting LAN Interface Web UI

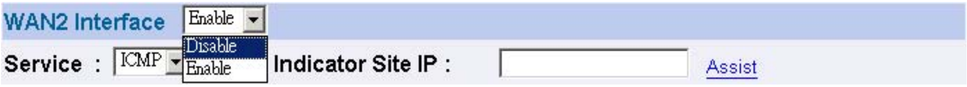
The default LAN IP Address is 192.168.1.1. After the Administrator setting the new LAN IP Address on the computer , he/she have to restart the System to make the new IP address effective. (when the computer obtain IP by DHCP)

Do not cancel Web UI selection before not setting Permitted IPs yet. It will cause the Administrator cannot be allowed to enter the SG-1000's Web UI from LAN.

4.2 Setting WAN Interface Address

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

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



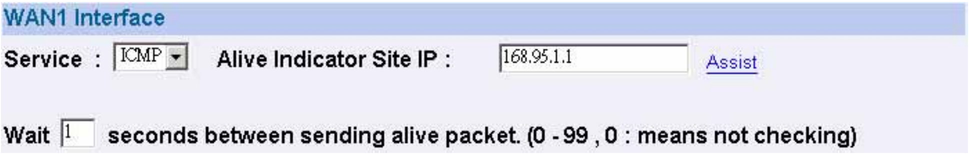
WAN2 Interface Enable ▾
Disable
Enable

Service : ICMP ▾ Indicator Site IP : Assist

Disable WAN2 Interface

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

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

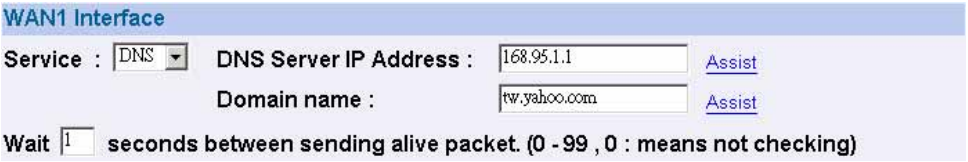


WAN1 Interface

Service : ICMP Alive Indicator Site IP : 168.95.1.1 Assist

Wait 1 seconds between sending alive packet. (0 - 99 , 0 : means not checking)

ICMP Connection



WAN1 Interface

Service : DNS DNS Server IP Address : 168.95.1.1 Assist

Domain name : tw.yahoo.com Assist

Wait 1 seconds between sending alive packet. (0 - 99 , 0 : means not checking)

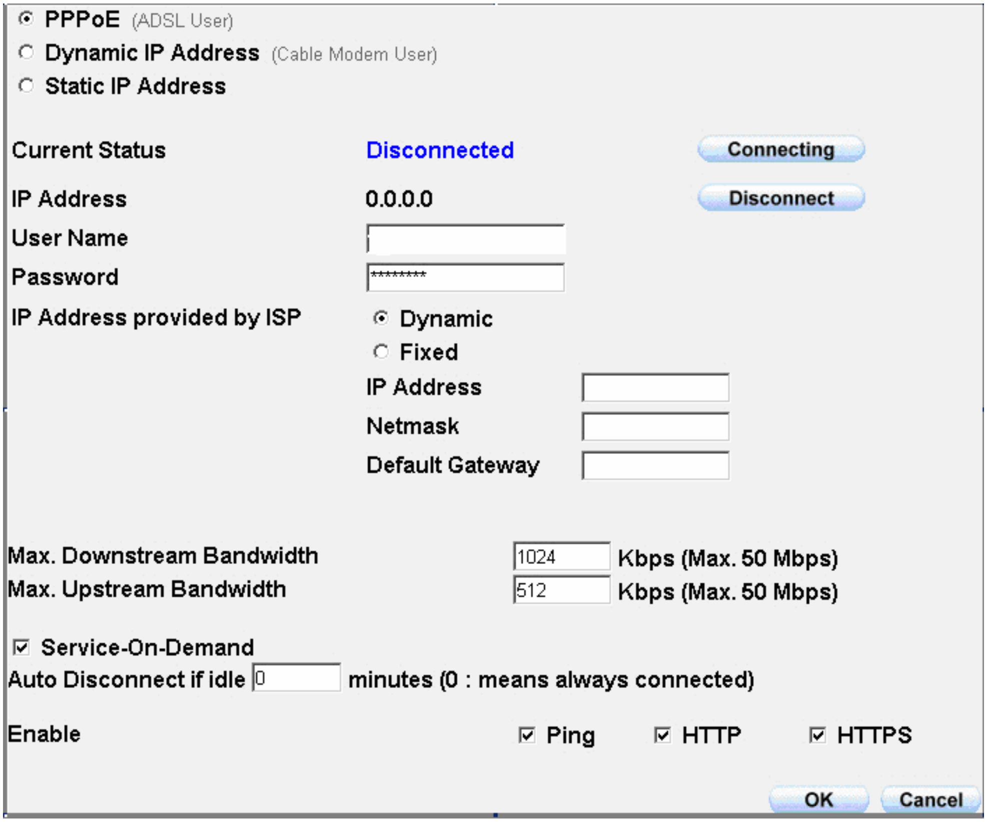
DNS Service

Connection test is used for SG-1000 to detect if the WAN can connect or not. So the **Alive Indicator Site IP**, **DNS Server IP Address**, or **Domain Name** must be able to use permanently. Or it will cause judgmental mistakes of the device.

STEP 3 . Select the Connecting way:

- **PPPoE (ADSL User)**:

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**, **HTTP**, and **HTTPS**.
7. Click **OK**



● PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
○ Static IP Address

Current Status: Disconnected

IP Address: 0.0.0.0

User Name:

Password: ********

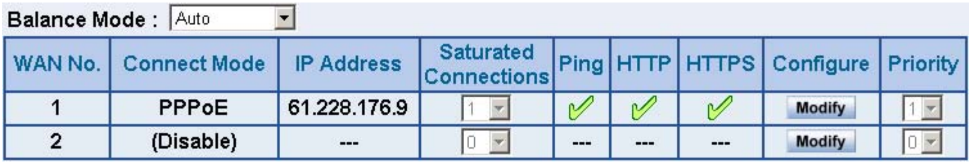
IP Address provided by ISP: ● Dynamic ○ Fixed
IP Address:
Netmask:
Default Gateway:

Max. Downstream Bandwidth: 1024 Kbps (Max. 50 Mbps)
Max. Upstream Bandwidth: 512 Kbps (Max. 50 Mbps)

☑ Service-On-Demand
Auto Disconnect if idle 0 minutes (0 : means always connected)

Enable ☑ Ping ☑ HTTP ☑ HTTPS

PPPoE Connection



Balance Mode : Auto

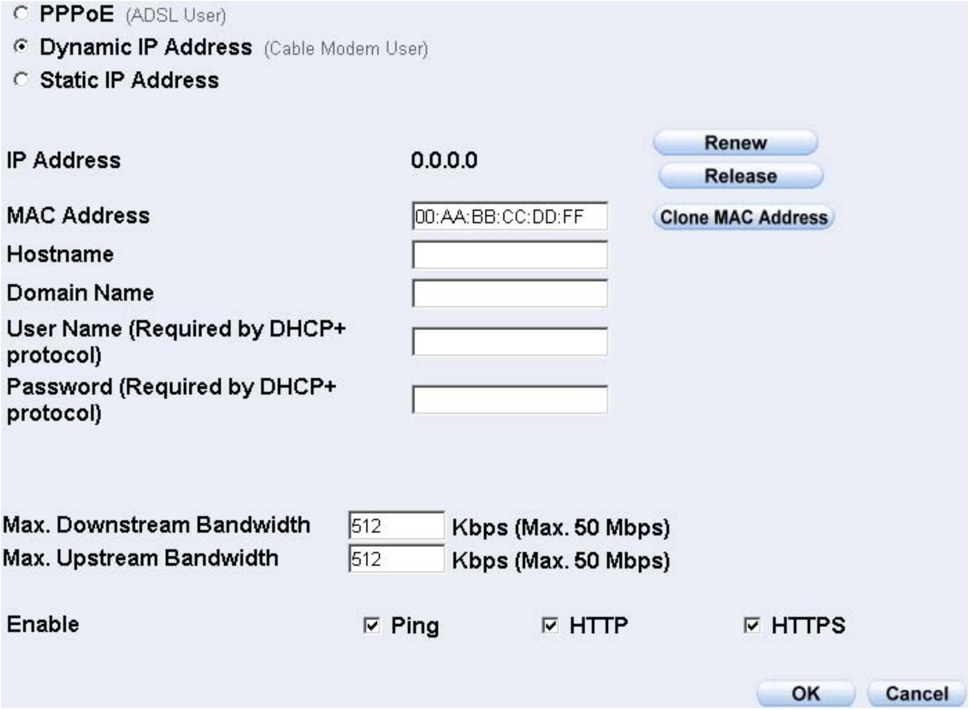
WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	PPPoE	61.228.176.9	1	✓	✓	✓	Modify	1
2	(Disable)	---	0	---	---	---	Modify	0

Complete PPPoE Connection Setting

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

- **Dynamic IP Address (Cable Modem User):**

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



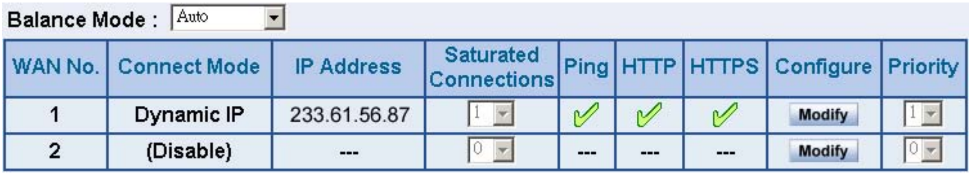
○ PPPoE (ADSL User)
● Dynamic IP Address (Cable Modem User)
○ Static IP Address

IP Address	0.0.0.0	Renew Release
MAC Address	00:AA:BB:CC:DD:FF	Clone MAC Address
Hostname		
Domain Name		
User Name (Required by DHCP+ protocol)		
Password (Required by DHCP+ protocol)		

Max. Downstream Bandwidth 512 Kbps (Max. 50 Mbps)
Max. Upstream Bandwidth 512 Kbps (Max. 50 Mbps)

Enable ☑ Ping ☑ HTTP ☑ HTTPS

Dynamic IP Address Connection



Balance Mode : Auto

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

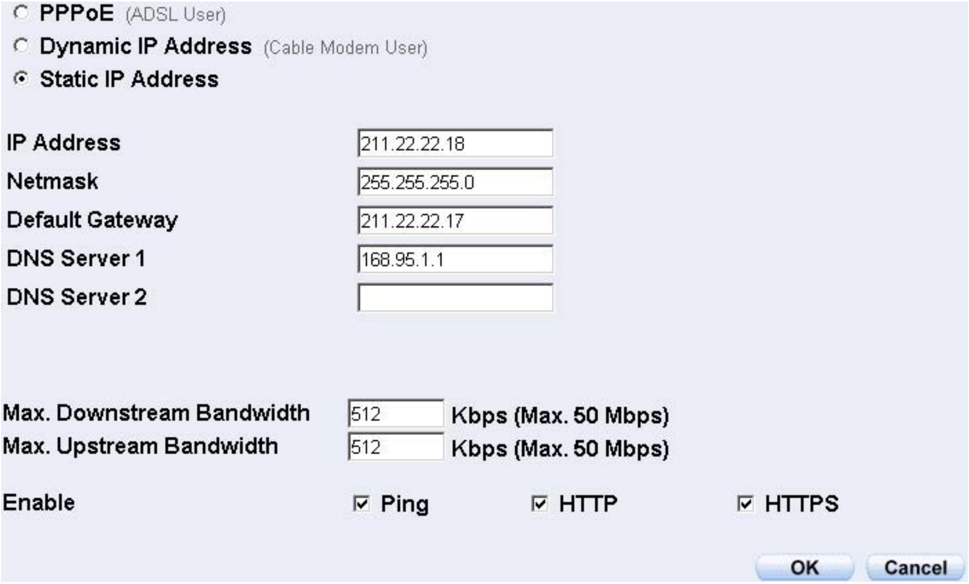
Complete Dynamic IP Connection Setting

- **Static IP Address**

1. Select **Static IP Address**
2. Enter **IP Address**, **Netmask**, and **Default Gateway** that provided by ISP
3. Enter **DNS Server1** and **DNS Server2**

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

4. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow that user apply)
5. Select **Ping**, **HTTP**, and **HTTPS**.
6. Click **OK**



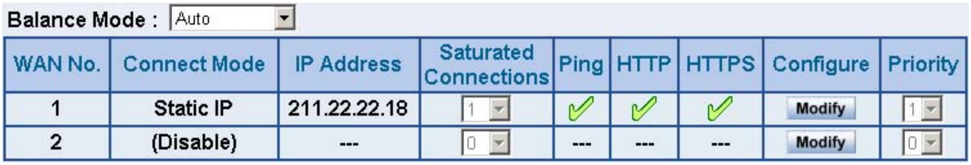
○ PPPoE (ADSL User)
○ Dynamic IP Address (Cable Modem User)
● Static IP Address

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 512 Kbps (Max. 50 Mbps)
Max. Upstream Bandwidth 512 Kbps (Max. 50 Mbps)

Enable ☑ Ping ☑ HTTP ☑ HTTPS

Static IP Address Connection



Balance Mode : Auto

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

Complete Static IP Address Connection Setting

When selecting **Ping** and **Web UI** on **WAN** network Interface, users will be able to ping the SG-1000 and enter the Web UI WAN network. It may influence network security. The suggestion is to **Cancel Ping** and **Web UI** 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.

4.3 Setting DMZ Interface Address (NAT Mode)

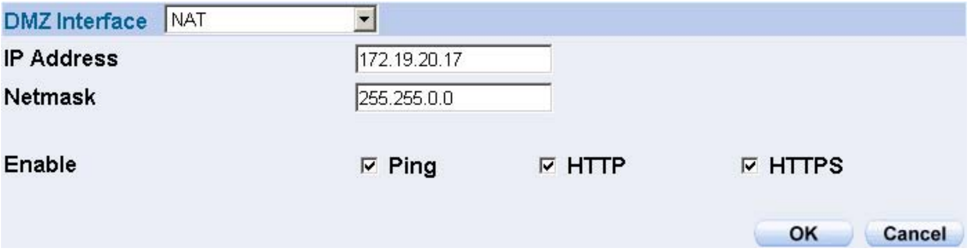
STEP 1 . Click **DMZ** Interface

STEP 2 . Select NAT Mode in DMZ Interface

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

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

STEP 4 . Click **OK**



DMZ Interface: NAT

IP Address: 172.19.20.17

Netmask: 255.255.0.0

Enable: ☑ Ping ☑ HTTP ☑ HTTPS

Setting DMZ Interface Address (NAT Mode) Web UI

Setting DMZ Interface Address (Transparent Mode)

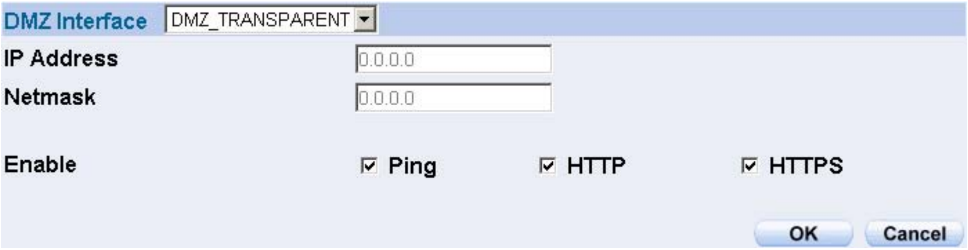
STEP 1 . Select **DMZ** Interface

STEP 2 . Select Transparent Mode in DMZ Interface

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

STEP 1 . Select **Ping**, **HTTP**, and **HTTPS**.

STEP 2 . Click **OK**



DMZ Interface: DMZ_TRANSPARENT

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Enable: ☑ Ping ☑ HTTP ☑ HTTPS

Setting DMZ Interface Address (Transparent Mode) Web UI

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

Chapter 5

Address

The SG-1000 allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN network, WAN network group, DMZ and DMZ group.

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address or DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN Group or the WAN Group and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.

✎ With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be setup before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

Define the required fields of Address

Name:

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

IP Address:

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

Netmask:

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

MAC Address:

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

Get Static IP address from DHCP Server:

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

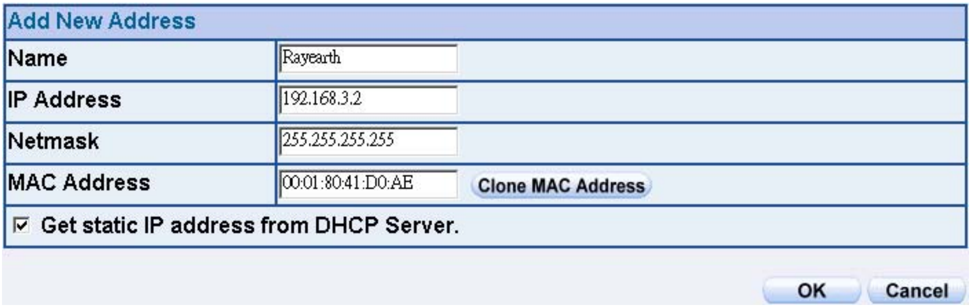
We set up two Address examples in this chapter:

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

5.1 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
- **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**

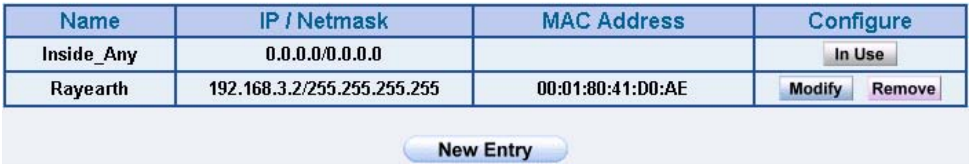


Add New Address

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.

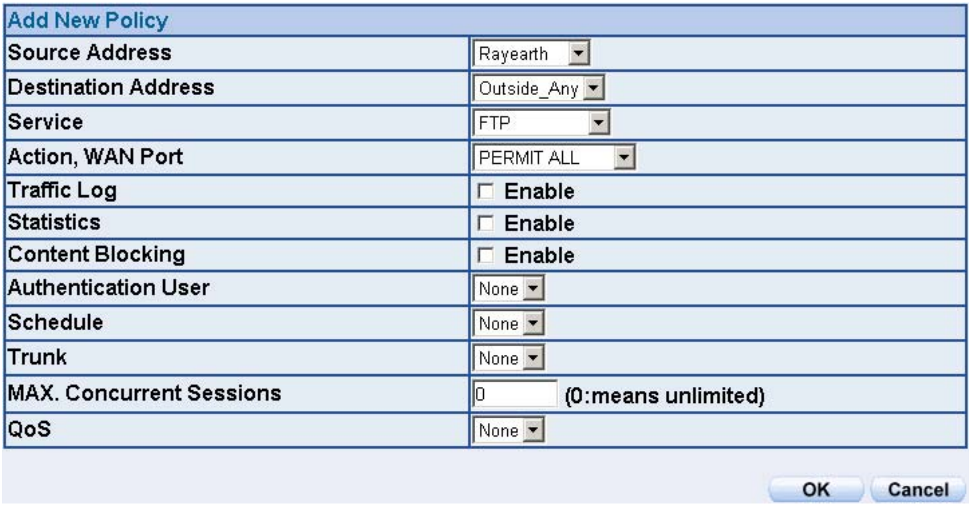
Setting LAN Address Book Web UI



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.3.2/255.255.255.255	00:01:80:41:D0:AE	Modify Remove

Complete the Setting of LAN

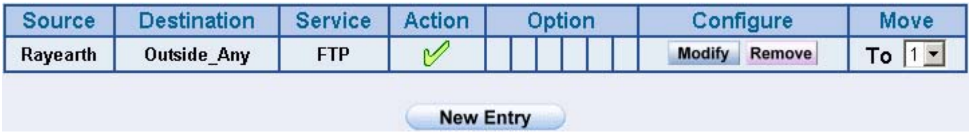
STEP 2． Adding the following setting in **Outgoing Policy**:



Add New Policy	
Source Address	Rayearth
Destination Address	Outside_Any
Service	FTP
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

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:



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

Complete the Policy of Restricting the Specific IP to Access to Internet

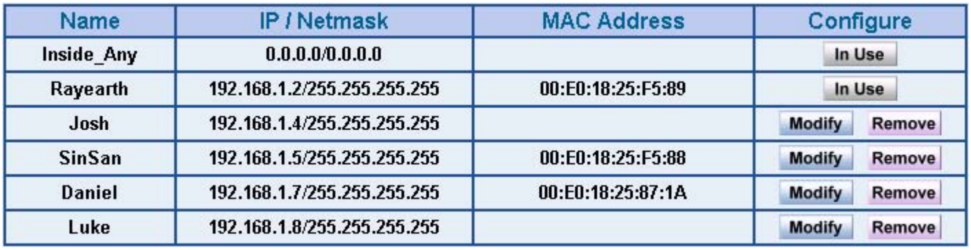
When the System Administrator setting the **Address** Book, he/she can choose the way of clicking on Clone MAC Address to make the SG-1000 to fill out the user's MAC Address automatically.

In **LAN** of **Address** function, the SG-1000 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.

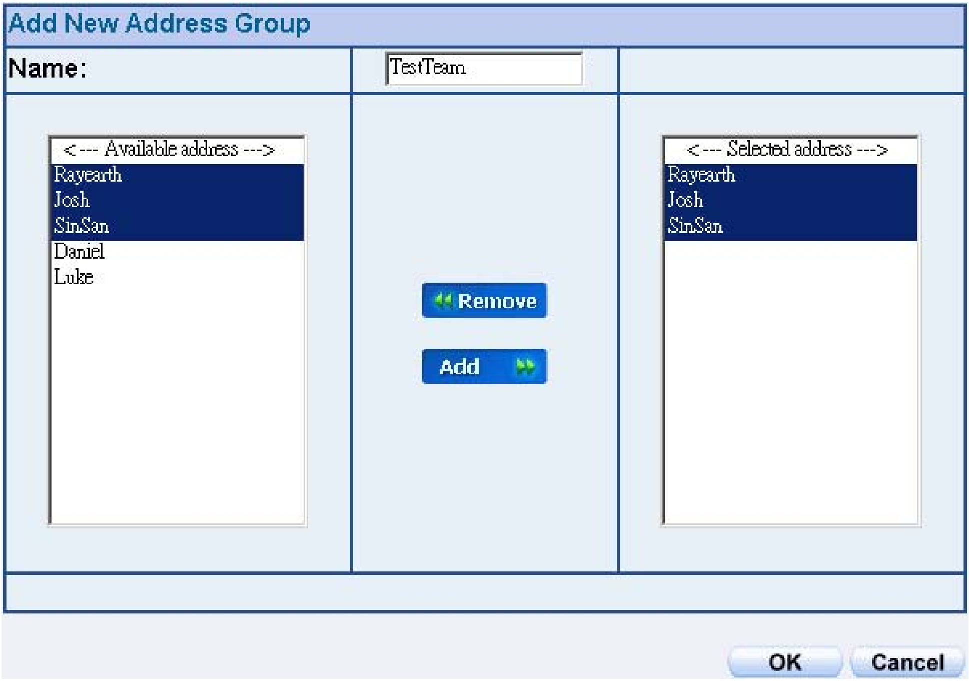


Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.1.2/255.255.255.255	00:E0:18:25:F5:89	In Use
Josh	192.168.1.4/255.255.255.255		Modify Remove
SinSan	192.168.1.5/255.255.255.255	00:E0:18:25:F5:88	Modify Remove
Daniel	192.168.1.7/255.255.255.255	00:E0:18:25:87:1A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

Setting Several LAN Network Address

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

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



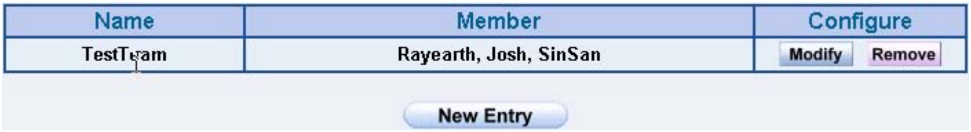
Add New Address Group

Name: TestTeam

<--- Available address --->
Rayearth
Josh
SinSan
Daniel
Luke

<--- Selected address --->
Rayearth
Josh
SinSan

Add New LAN Address Group



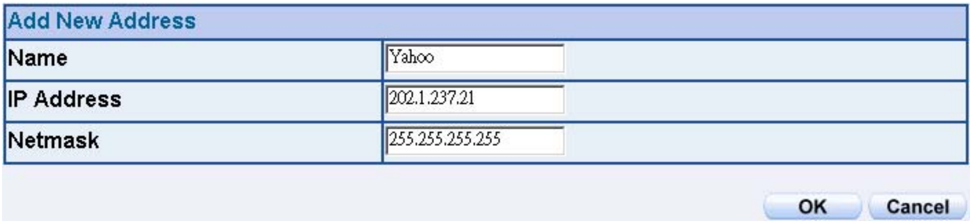
Name	Member	Configure
TestTeam	Rayearth, Josh, SinSan	Modify Remove

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:

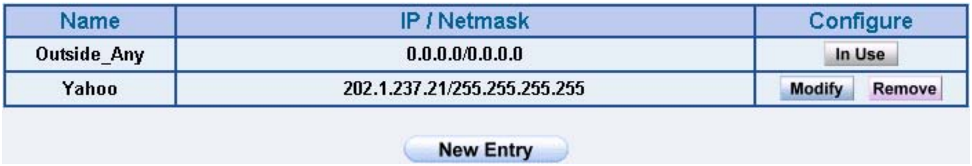
- Click **New Entry**
- Enter the following data (**Name, IP Address, Netmask**)
- Click **OK**



Add New Address

Name	Yahoo
IP Address	202.1.237.21
Netmask	255.255.255.255

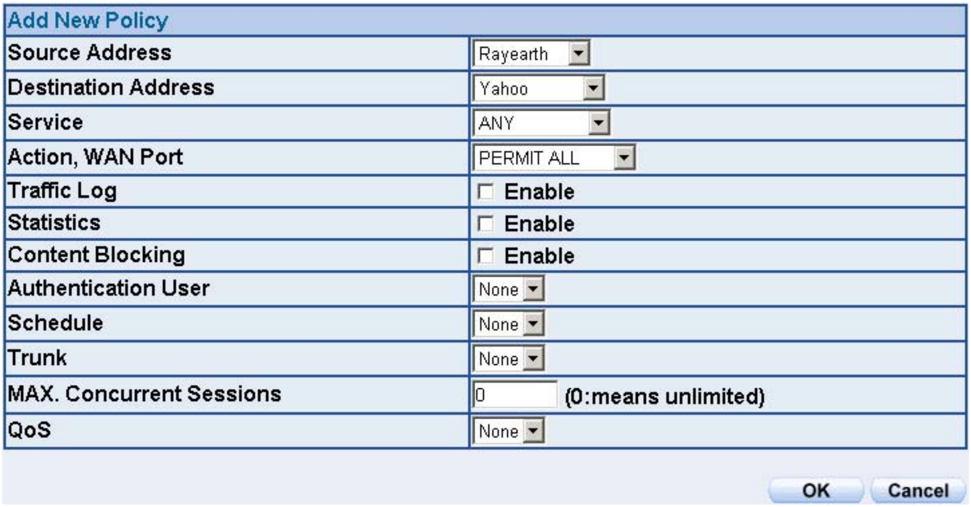
Add New WAN Address



Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
Yahoo	202.1.237.21/255.255.255.255	Modify Remove

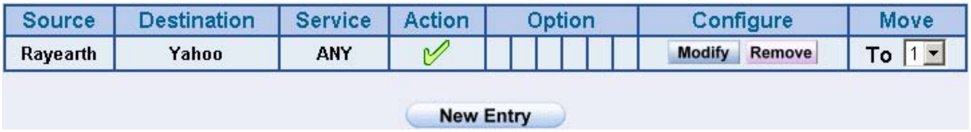
Complete the Setting of WAN Address

STEP 4．To exercise STEP1~3 in **Policy**



Add New Policy	
Source Address	Rayearth
Destination Address	Yahoo
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

To Exercise Address Setting in Policy



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

Complete the Policy Setting

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

Chapter 6

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 SG-1000 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 Web UI'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, TRACEROUTE…etc.

New Service Name:

- The System Manager can name the custom service.

Protocol:

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

Client Port:

- The port number of network card of clients. (The range is 1024~65535, suggest to use the default range)

Server Port:

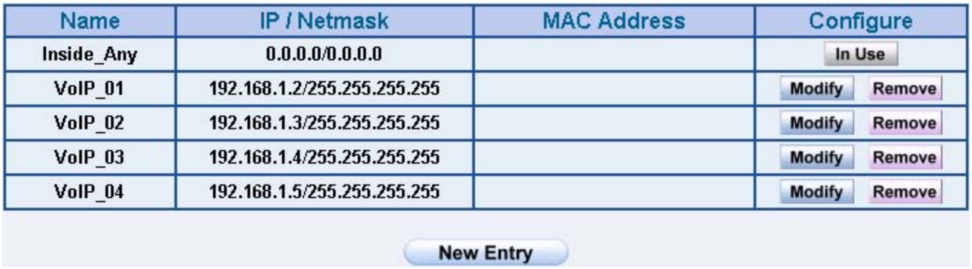
- The port number of custom service

We set up two Service examples in this chapter:

No	Suitable Situation	Example
Ex1	**Custom**	Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15325-15333, UDP 15325-15333)
Ex2	**Group**	Setting service group and restrict the specific users only can access to service resource that provided by this group through policy. (Group: HTTP, POP3, SMTP, DNS)

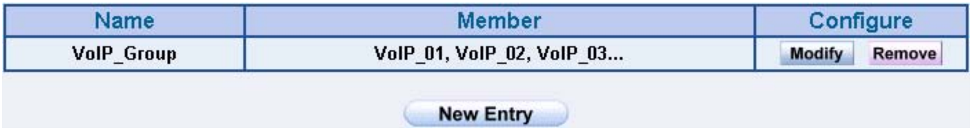
6.1 Allow external user to communicate with internal user by VoIP through policy. (VoIP Port: TCP 1720, TCP 15328-15333, UDP 15328-15333)

STEP 1．Set **LAN** and **LAN Group** in **Address** function as follows:



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		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

Setting LAN Address Book Web UI

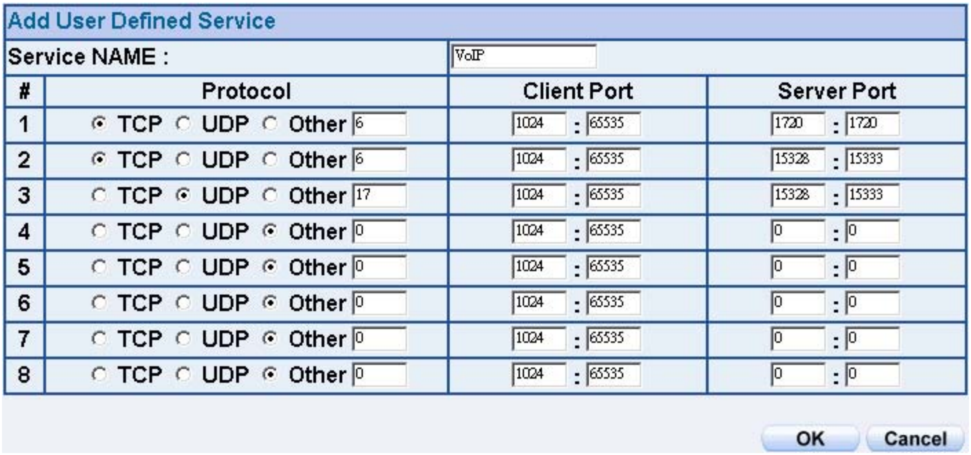


Name	Member	Configure
VoIP_Group	VoIP_01, VoIP_02, VoIP_03...	Modify Remove

Setting LAN Group Address Book Web UI

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

- Click **New Entry**
- **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**

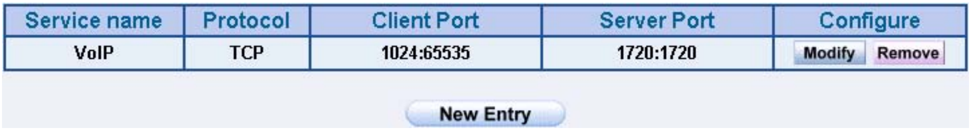


Add User Defined Service

Service NAME : VoIP

#	Protocol	Client Port	Server Port
1	● TCP ○ UDP ○ Other 6	1024 : 65535	1720 : 1720
2	● TCP ○ UDP ○ Other 6	1024 : 65535	15328 : 15333
3	○ TCP ● UDP ○ Other 17	1024 : 65535	15328 : 15333
4	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
5	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
6	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
7	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
8	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0

Add User Define Service



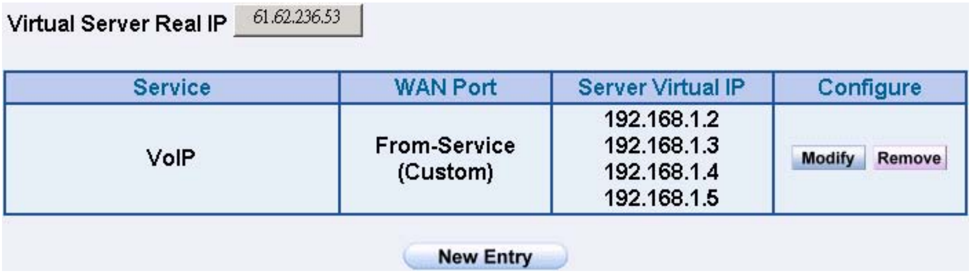
Service name	Protocol	Client Port	Server Port	Configure
VoIP	TCP	1024:65535	1720:1720	Modify Remove

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.**



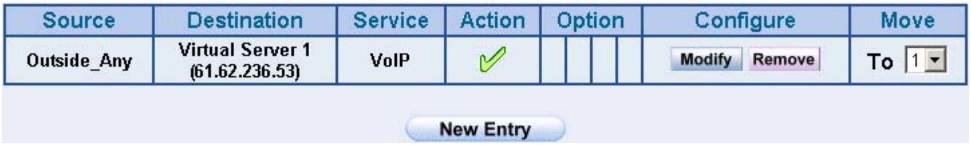
Virtual Server Real IP 61.62.236.53

Service	WAN Port	Server Virtual IP	Configure
VoIP	From-Service (Custom)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	Modify Remove

New Entry

Compare Service to Virtual Server

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

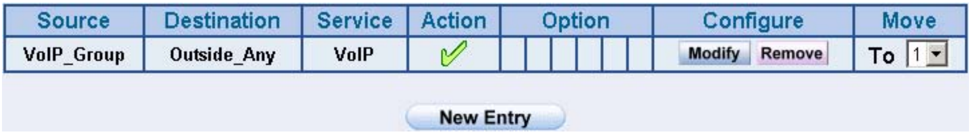


Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.62.236.53)	VoIP	✓		Modify Remove	To 1

New Entry

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:



Source	Destination	Service	Action	Option	Configure	Move
VoIP_Group	Outside_Any	VoIP	✓		Modify Remove	To 1

New Entry

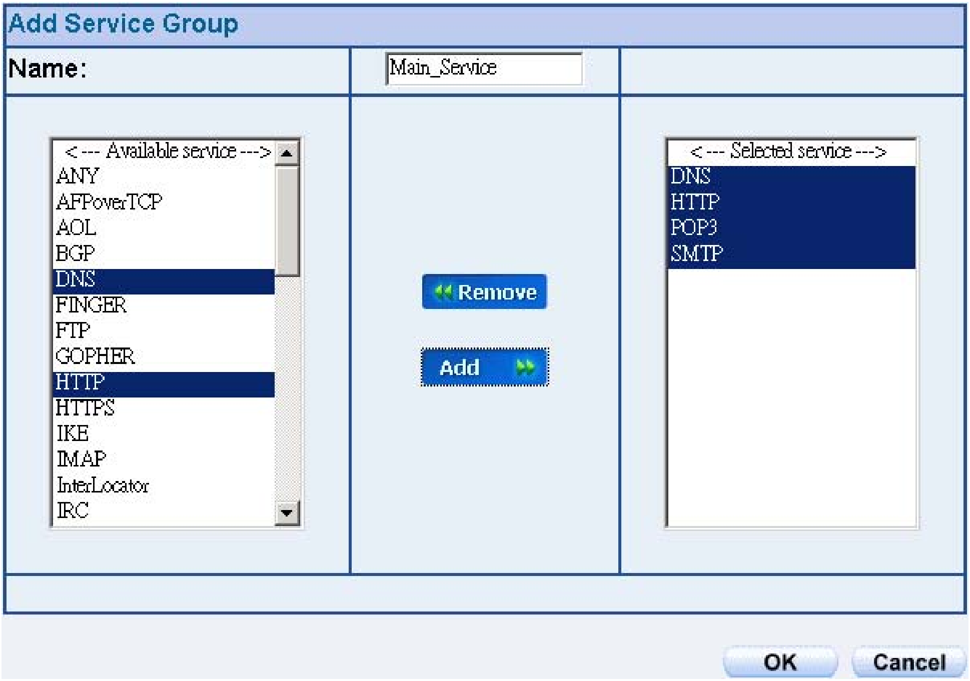
Complete the Policy for Internal VoIP to Connect with External VoIP

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

6.2 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**
- **Name:** Enter Main_Service
- Select HTTP, POP3, SMTP, DNS in **Available Service** and click **Add**
- Click **OK**



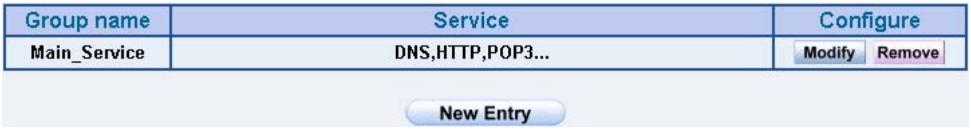
Add Service Group

Name: Main_Service

<--- Available service --->
ANY
AFPoverTCP
AOL
BGP
DNS
FINGER
FTP
GOPHER
HTTP
HTTPS
IKE
IMAP
InterLocator
IRC

<--- Selected service --->
DNS
HTTP
POP3
SMTP

Add Service Group

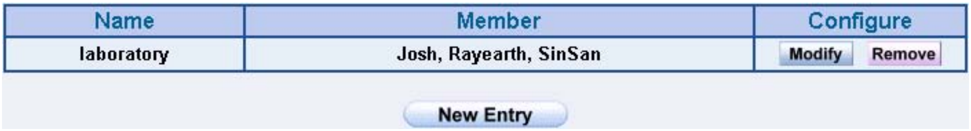


Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	Modify Remove

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.

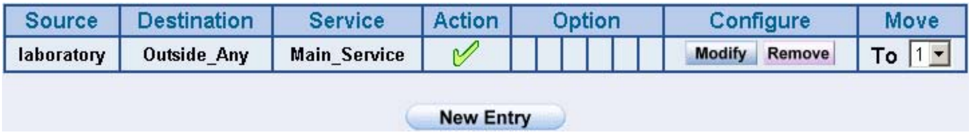


Name	Member	Configure
laboratory	Josh, Rayearth, SinSan	Modify Remove

New Entry

Setting Address Book Group

STEP 3．Compare **Service Group** to **Outgoing Policy.**



Source	Destination	Service	Action	Option	Configure	Move
laboratory	Outside_Any	Main_Service	✓		Modify Remove	To 1

New Entry

Setting Policy

Chapter 7

Schedule

In this chapter, the SG-1000 provides the Administrator to configure a schedule for policy to take effect and allow the policies to be used at those designated times. And then the Administrator can set the start time and stop time or VPN connection in **Policy** or **VPN**. By using the **Schedule** function, the Administrator can save a lot of management time and make the network system most effective.

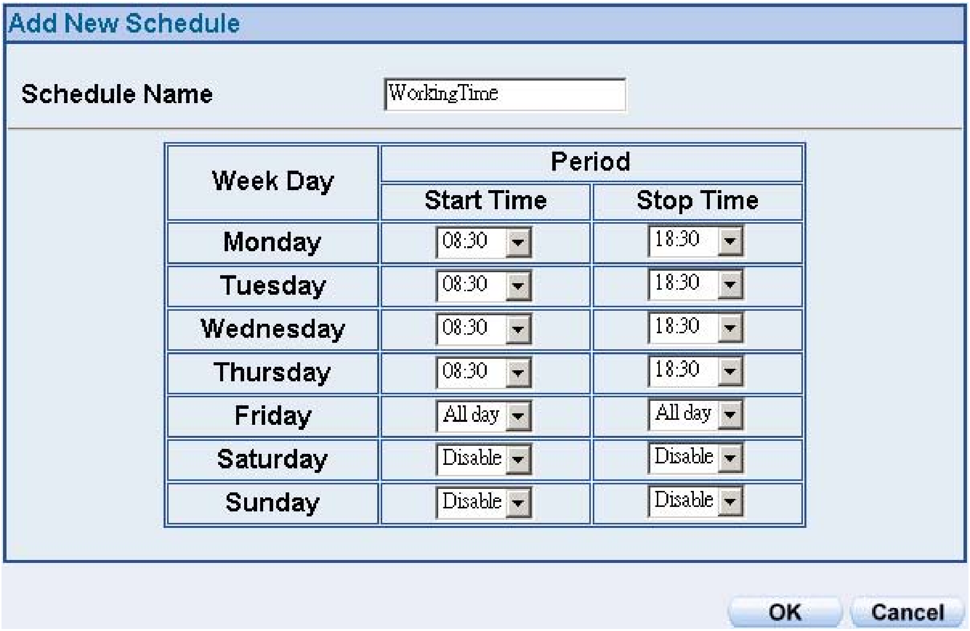
How to use the Schedule?

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

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

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

- Click **New Entry**
- Enter **Schedule Name**
- Set up the working time of Schedule for each day
- Click **OK**

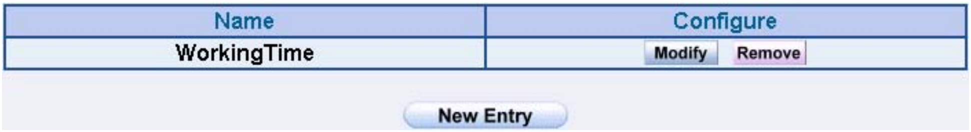


Add New Schedule

Schedule Name: WorkingTime

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

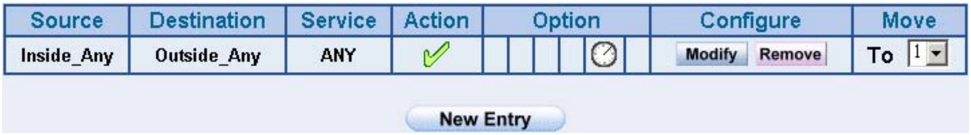
Setting Schedule Web UI



Name	Configure
WorkingTime	Modify Remove

Complete the Setting of Schedule

STEP 2．Compare **Schedule** with **Outgoing Policy**



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

New Entry

Complete the Setting of Comparing Schedule with Policy

Chapter 8

QoS

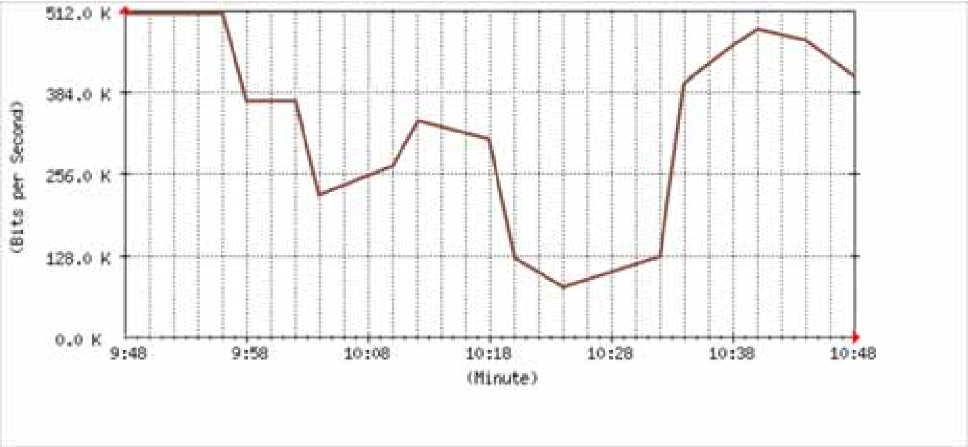
By configuring the QoS, you can control the OutBound and InBound Upstream/Downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth.

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

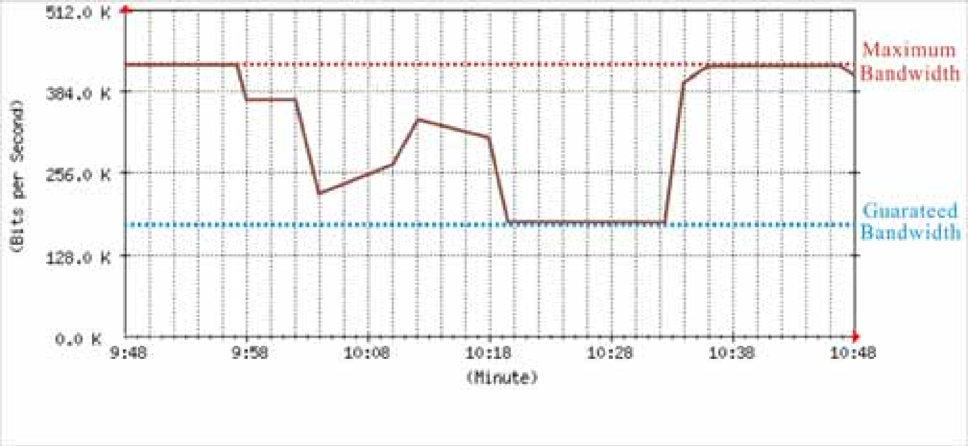
Upstream Bandwidth：To configure the Guaranteed Bandwidth and Maximum Bandwidth.

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

The SG-1000 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The SG-1000 also makes it convenient for the administrator to make the Bandwidth to reach the best utility.



The Flow Before Using QoS



The Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

Define the required fields of QoS

WAN:

- Display WAN1 and WAN2

Downstream Bandwidth:

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

Upstream Bandwidth:

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

Priority:

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

Guaranteed Bandwidth:

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

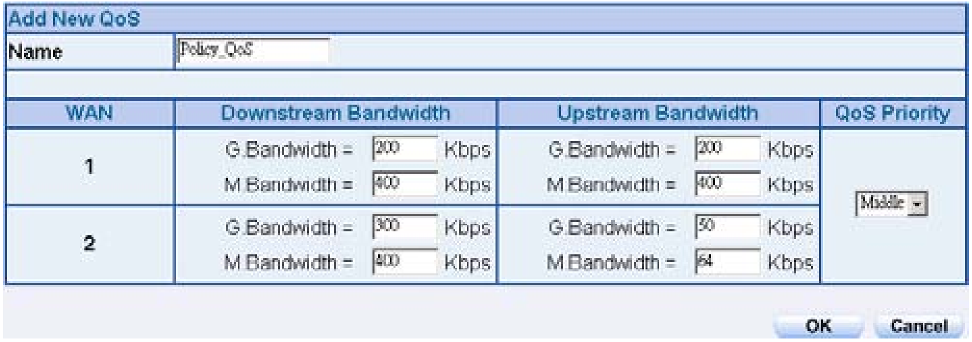
Maximum Bandwidth:

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

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

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

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



Add New QoS

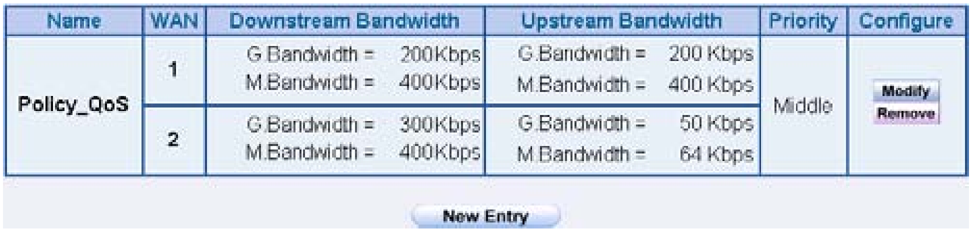
Name: Policy_QoS

WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority

1	G.Bandwidth = 200 Kbps
	M.Bandwidth = 400 Kbps
		G.Bandwidth = 200 Kbps
		M.Bandwidth = 400 Kbps
			Middle

2	G.Bandwidth = 300 Kbps
	M.Bandwidth = 400 Kbps
		G.Bandwidth = 50 Kbps
		M.Bandwidth = 64 Kbps	

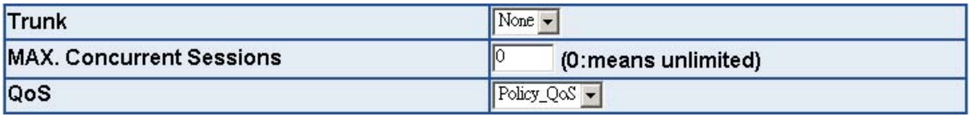
QoS Web UI Setting



Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Policy_QoS	1	G.Bandwidth = 200Kbps M.Bandwidth = 400Kbps	G.Bandwidth = 200 Kbps M.Bandwidth = 400 Kbps	Middle	Modify Remove
	2	G.Bandwidth = 300Kbps M.Bandwidth = 400Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 64 Kbps		

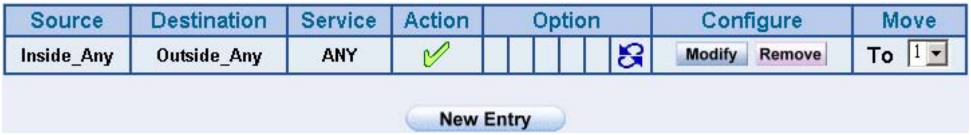
Complete the QoS Setting

STEP 2．Use the QoS that set by STEP1 in **Outgoing Policy.**



Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	Policy_QoS

Setting the QoS in Policy



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

Complete Policy Setting

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

Chapter 9

Authentication

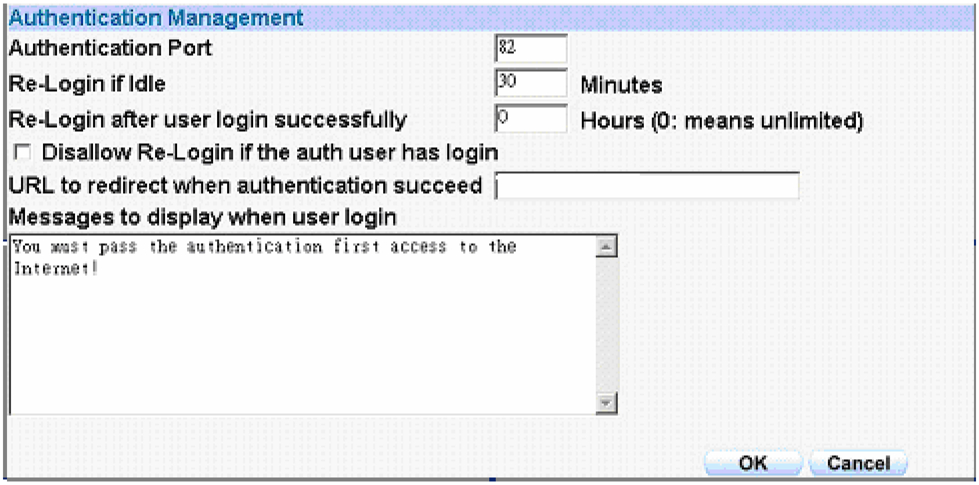
By configuring the Authentication, you can control the user’s (Internal user or remote user who connect by VPN and IPSec) connection authority. The user has to pass the authentication to access to Internet.

The SG-1000 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 SG-1000 authentication. (Have to setup the Authentication first)
  - **Authentication Port:** The internal user have to pass the authentication to access to the Internet when enable SG-1000.
  - **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 Web UI. (Support HTML) The default value is blank (display no message in authentication Web UI)
    - Add the following setting in this function:



Authentication Management

Authentication Port 82

Re-Login if Idle 30 Minutes

Re-Login after user login successfully 0 Hours (0: means unlimited)

□ Disallow Re-Login if the auth user has login

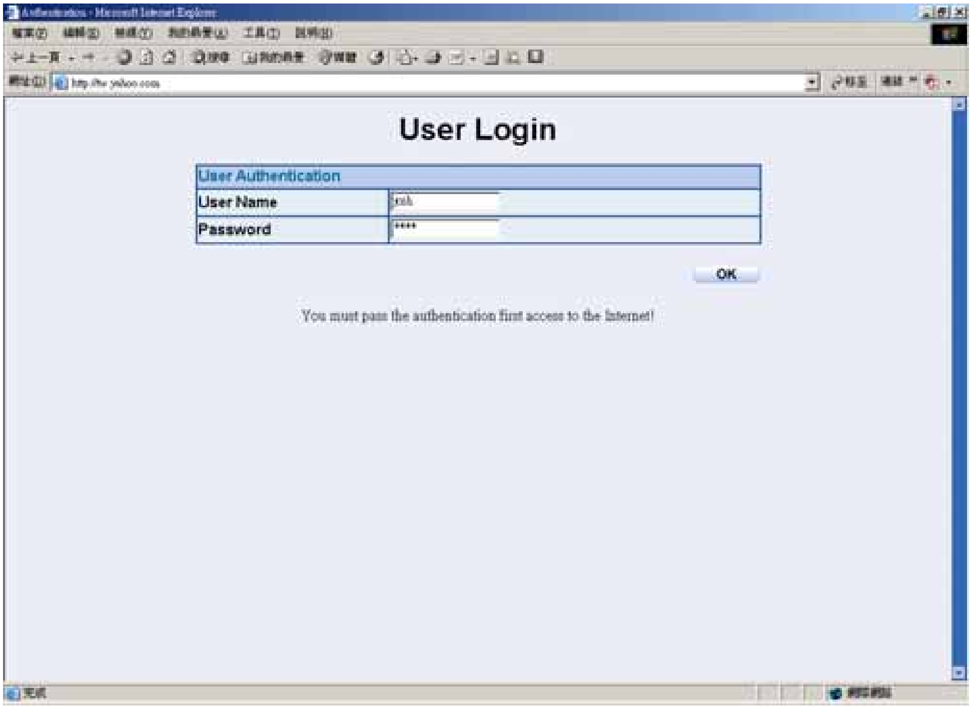
URL to redirect when authentication succeed

Messages to display when user login

You must pass the authentication first access to the Internet!

Authentication Setting Web UI

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


Authentication - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
http://tw.yahoo.com
移至
完成
網際網路

User Login

User Authentication	
User Name	xxh
Password	****

OK

You must pass the authentication first access to the Internet!

Authentication Login Web UI

- It will connect to the appointed website after passing Authentication.

If the user ask for authentication positively, can enter the LAN IP by the Authentication port number. And then the Authentication Web UI 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 SG-1000 and RADIUS Server

802.1xRADIUS:

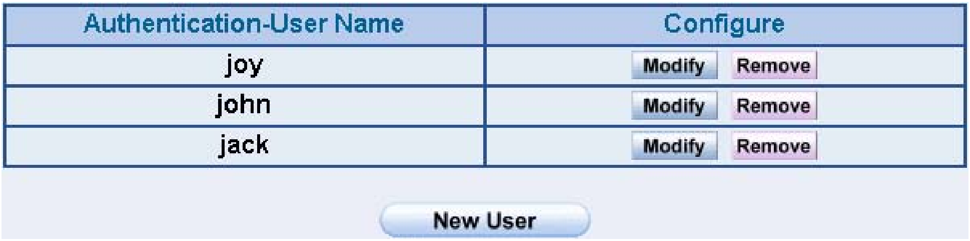
- The Authentication to RADIUS Server of wireless network

We set up four Authentication examples in this chapter:

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

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

STEP 1．Enter the following setting in **Auth User** of **Authentication**:



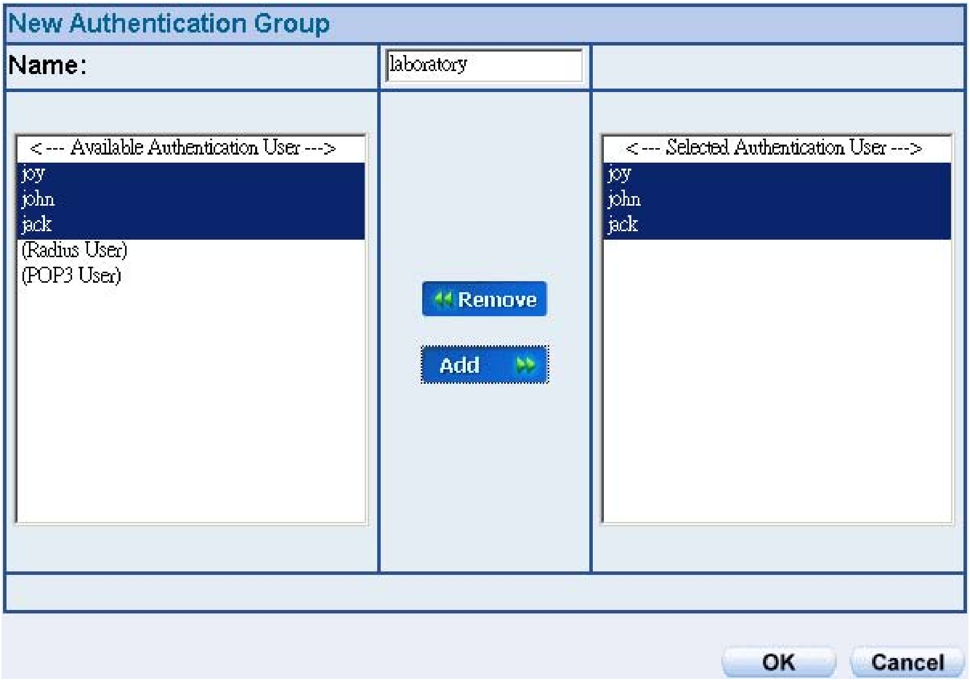
Authentication-User Name	Configure
joy	Modify Remove
john	Modify Remove
jack	Modify Remove

Auth User Setting Web UI

To use Authentication, the DNS Server of the user’s network card must be the same as the LAN Interface Address of SG-1000.

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

- Click **New Entry**.
- **Name:** Enter laboratory.
- Select **Available Authentication User** Add to **Selected Authentication User**.
- Click **OK**.
- Complete **Auth Group** Setting



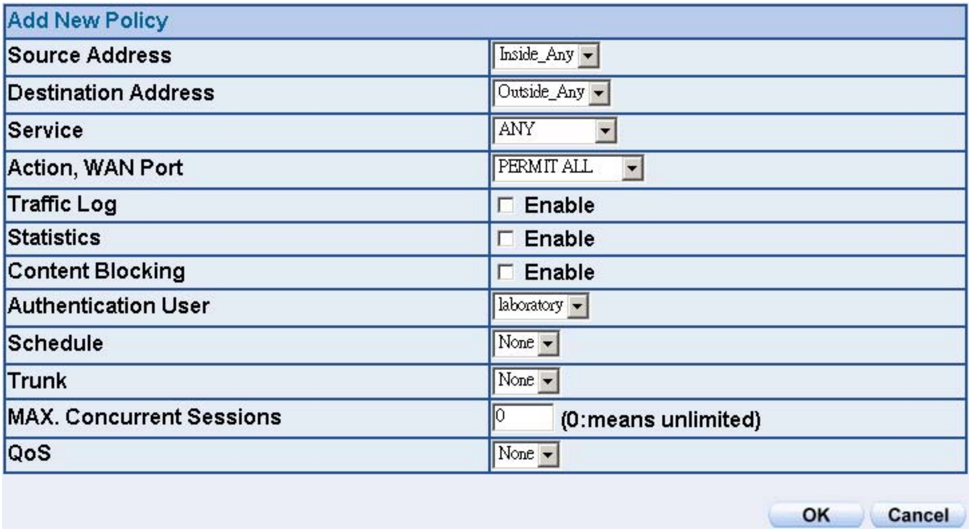
New Authentication Group

Name: laboratory

< --- Available Authentication User --->
joy
john
jack
(Radius User)
(POP3 User)
Remove
Add
< --- Selected Authentication User --->
joy
john
jack
OK
Cancel

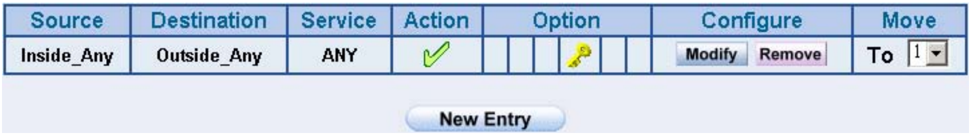
Auth Group Setting Web UI

STEP 3 . Add a policy in **Outgoing Policy** and input the Authentication setting of STEP1, 2



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	laboratory ▾
Schedule	None ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

Auth-User Policy Setting

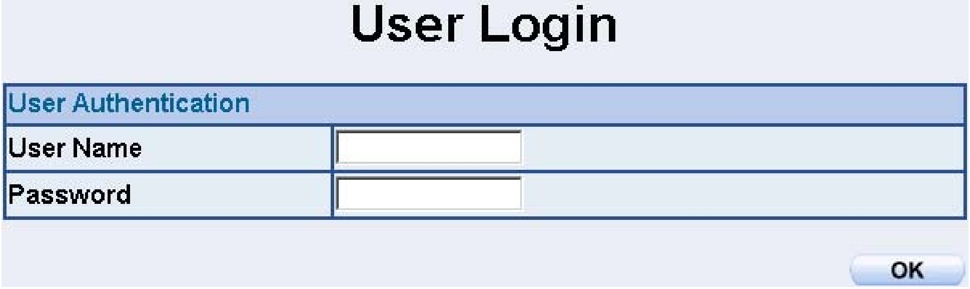


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	🔑	Modify Remove	To 1 ▾

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.

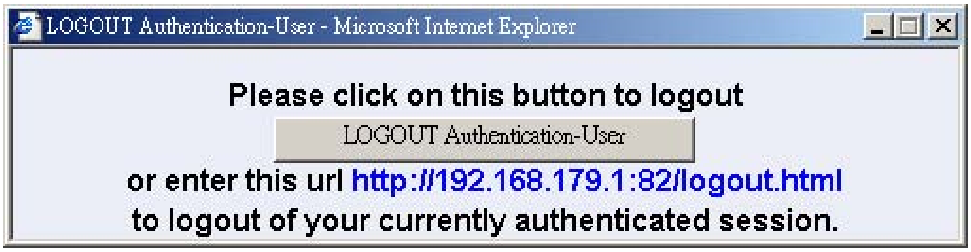
STEP 5． If the user does not need to access to Internet anymore and is going to logout, he/she can click **LOGOUT Auth-User** to logout the system. Or enter the Logout Authentication Web UI (http:// LAN Interface: Authentication port number/ logout.html) to logout



User Login

User Authentication	
User Name	
Password	

Access to Internet through Authentication Web UI



LOGOUT Authentication-User - Microsoft Internet Explorer

Please click on this button to logout

LOGOUT Authentication-User

or enter this url http://192.168.179.1:82/logout.html
to logout of your currently authenticated session.

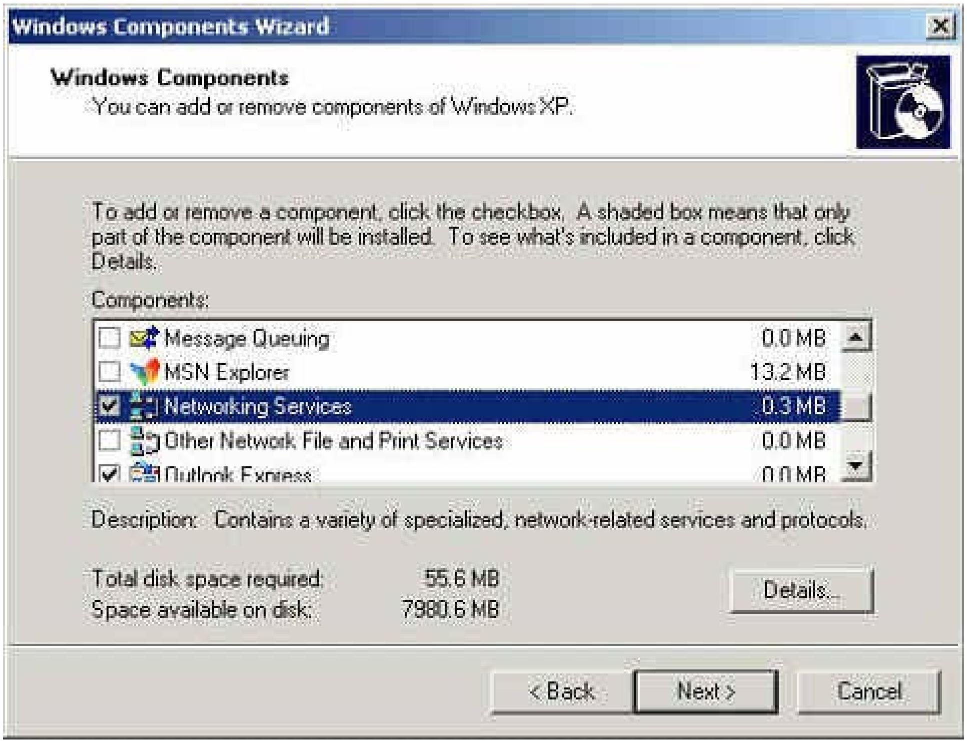
Logout Auth-User Web UI

9.2 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**


Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

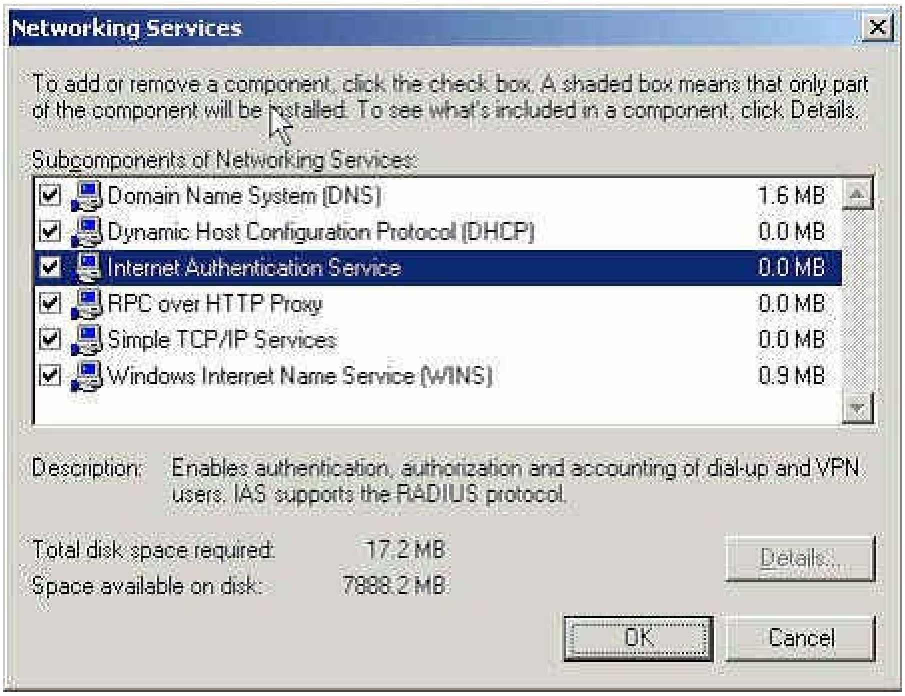
☐	Message Queuing	0.0 MB
☐	MSN Explorer	13.2 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB
☑	Outlook Express	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 55.6 MB
Space available on disk: 7980.6 MB

Add Windows Components Web UI

STEP 3 . Choose **Internet Authentication Service (IAS)**



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☑	Domain Name System (DNS)	1.6 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
☑	RPC over HTTP Proxy	0.0 MB
☑	Simple TCP/IP Services	0.0 MB
☑	Windows Internet Name Service (WINS)	0.9 MB

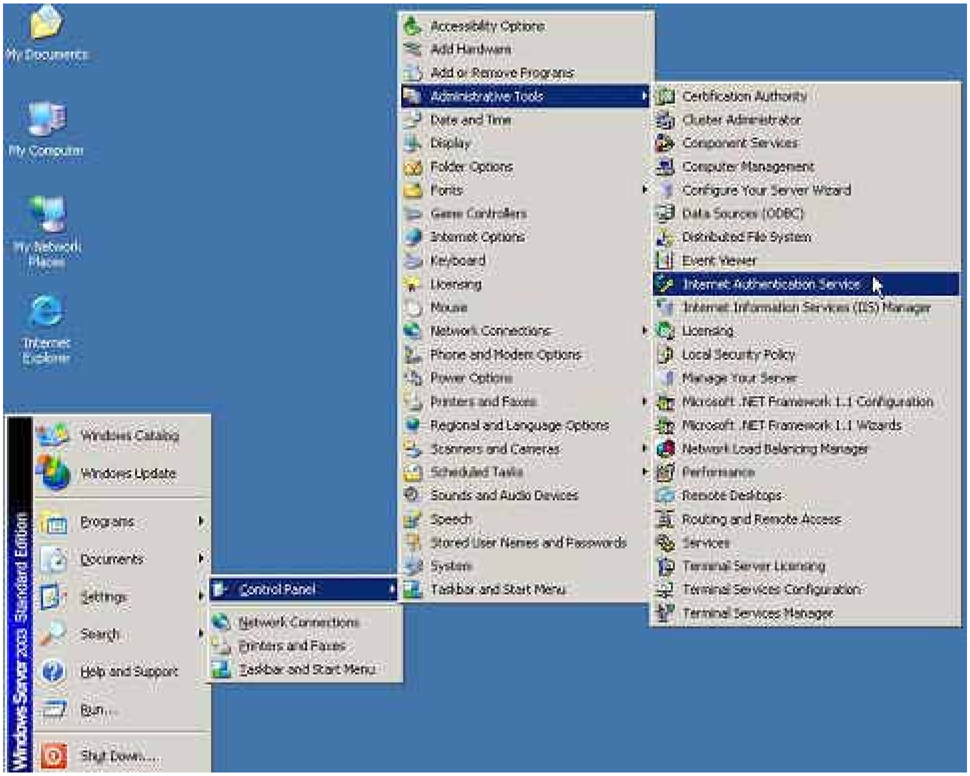
Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

Total disk space required: 17.2 MB

Space available on disk: 7888.2 MB

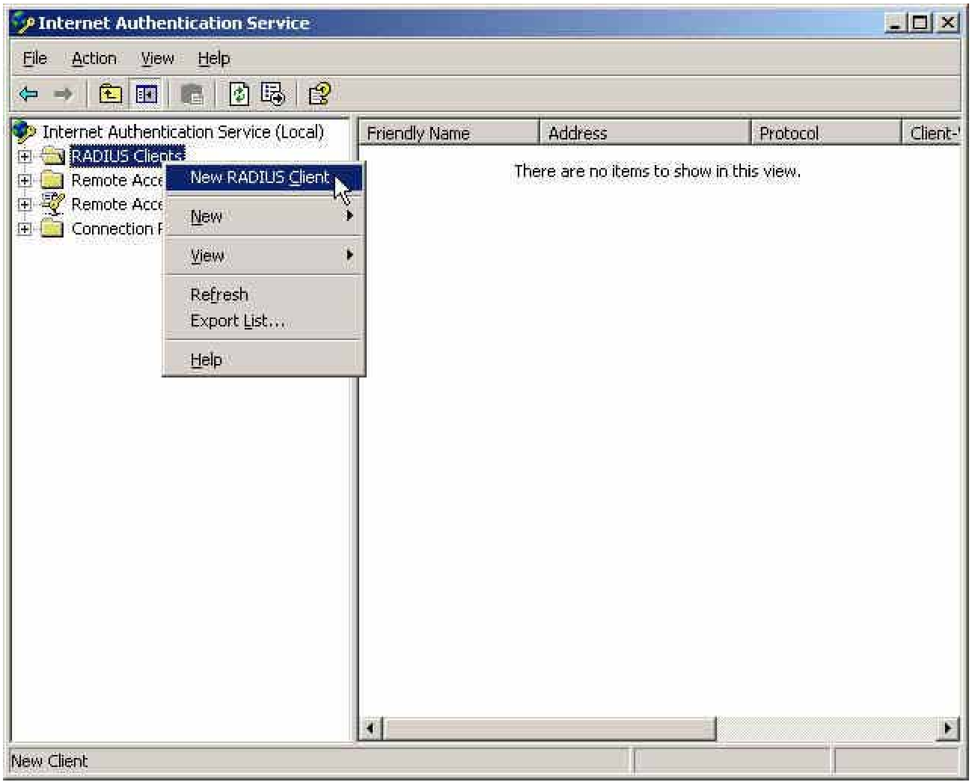
Add New Internet Authentication Services Web UI

STEP 4 . Click [Start] → [Control Panel] → [Administrative Tools], Choose [Internet Authentication Service]



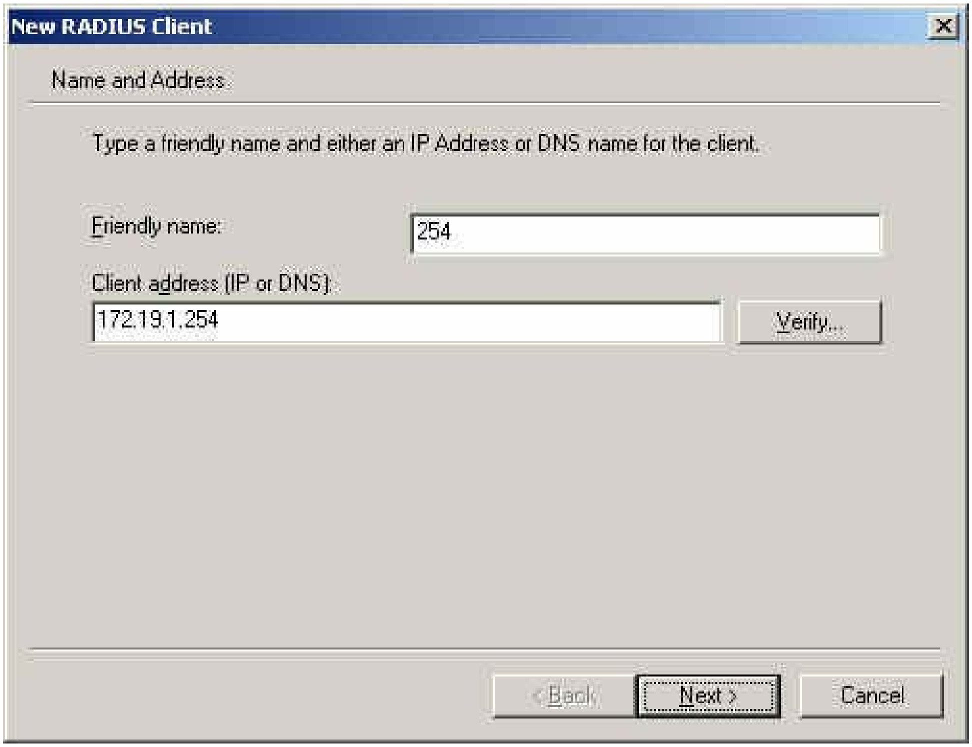
Choose Internet Authentication Service

STEP 5．Press right button on **RADIUS Clients** and choose **New RADIUS Client**



Add New RADIUS Client

STEP 6．Enter the **Name** and **Client Address** (also the SG-1000 IP)



New RADIUS Client

Name and Address

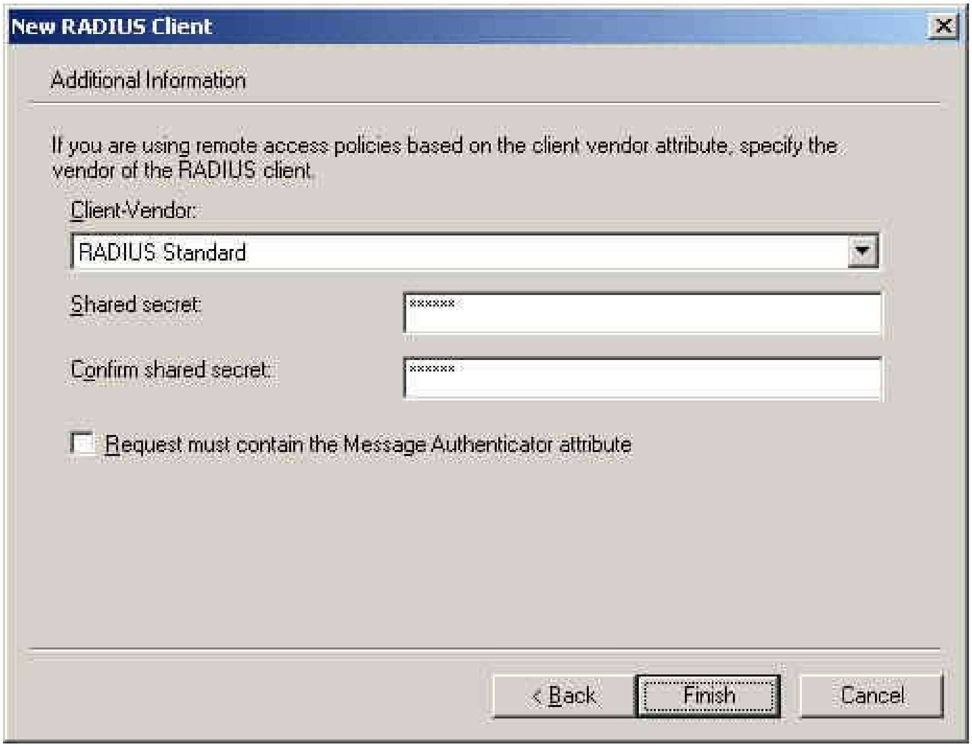
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: 254

Client address (IP or DNS): 172.19.1.254

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 SG-1000)


New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

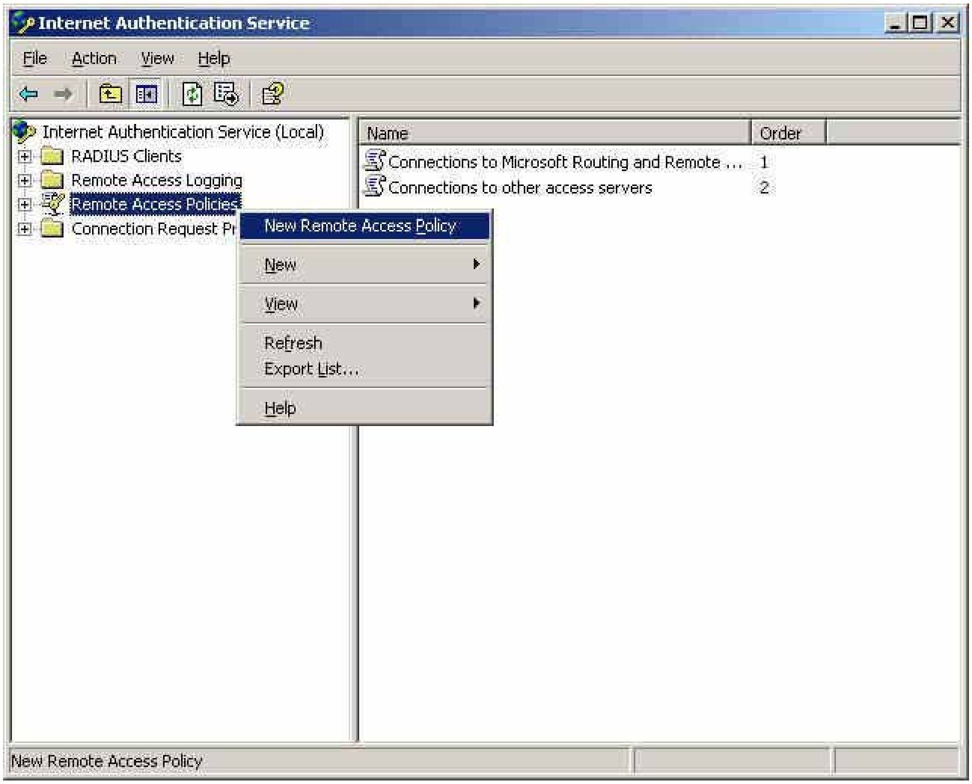
Shared secret: *******

Confirm shared secret: *******

□ Request must contain the Message Authenticator attribute

Add New RADIUS Client and Password Web UI

STEP 8 . Press the right button on **Remote Access Policies** and select to add **New Remote Access Policy**.

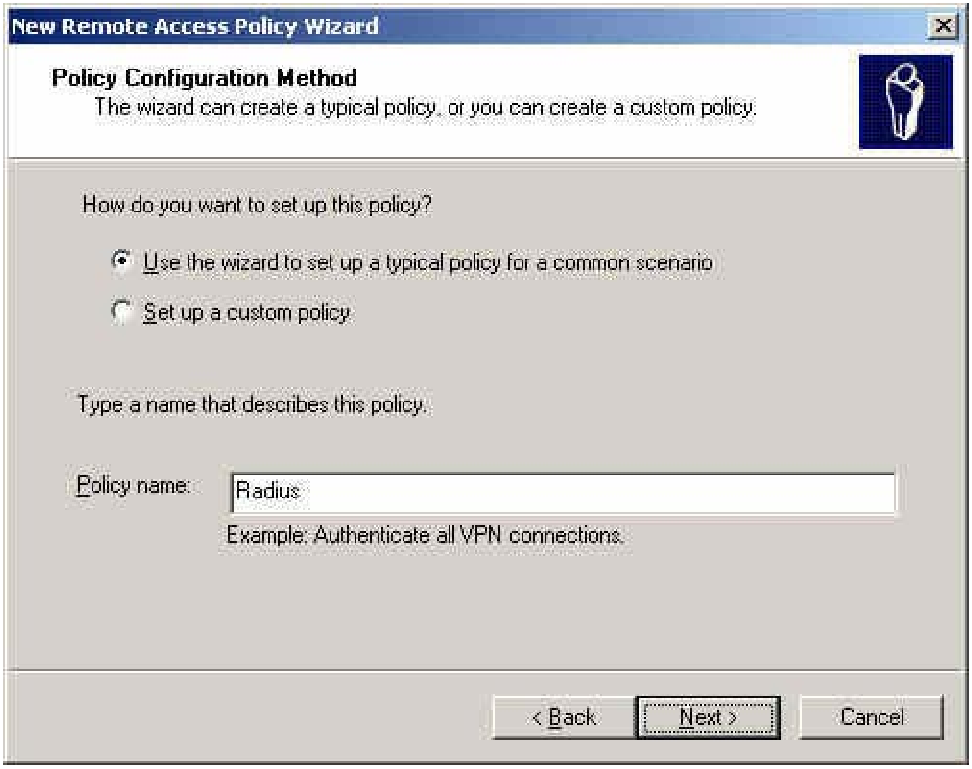


Name	Order
Connections to Microsoft Routing and Remote ...	1
Connections to other access servers	2

New Remote Access Policy

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**.



New Remote Access Policy Wizard

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

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

○ Set up a custom policy

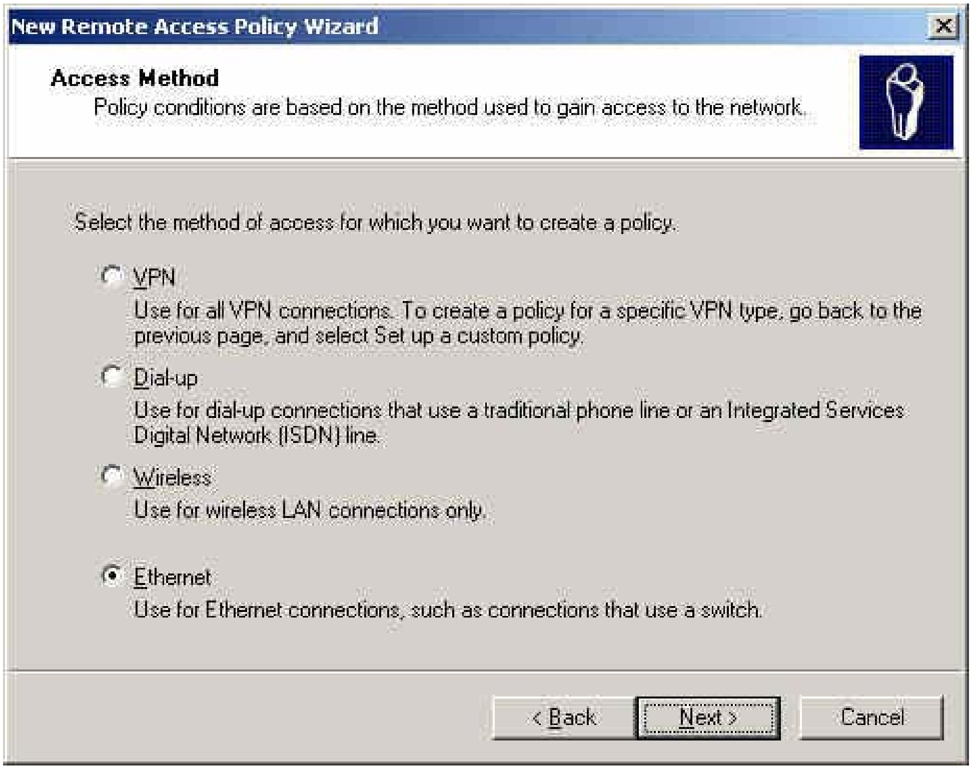
Type a name that describes this policy.

Policy name: Radius

Example: Authenticate all VPN connections.

Add Remote Access Policy and Name

STEP 10．Select **Ethernet**



New Remote Access Policy Wizard

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.

○ VPN

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.

○ Dial-up

Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

○ Wireless

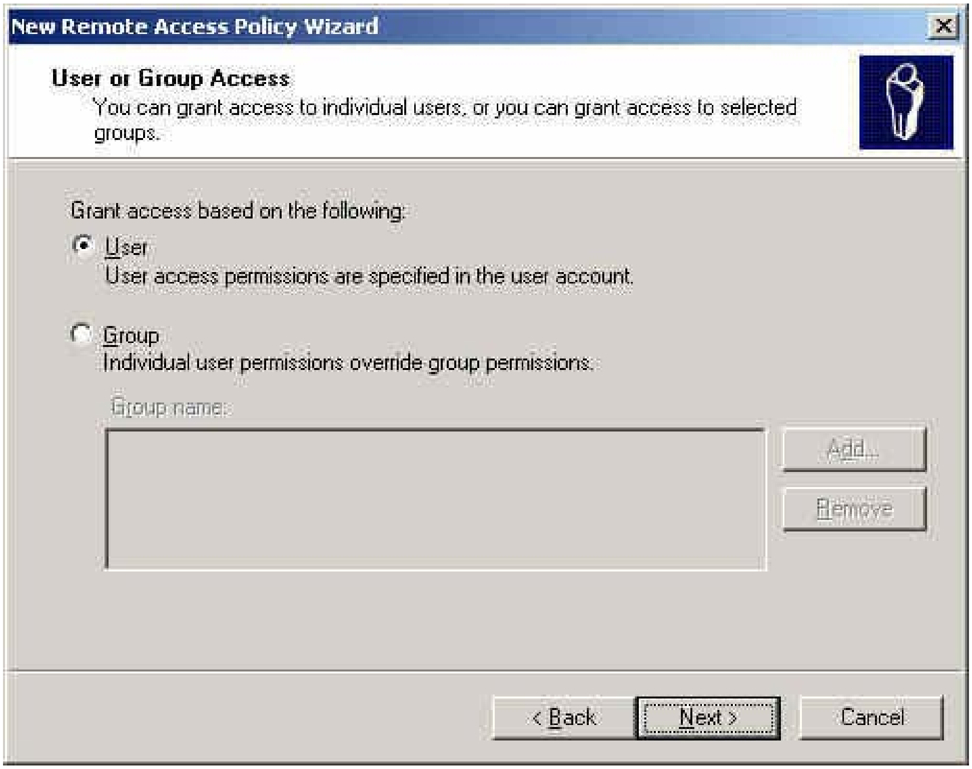
Use for wireless LAN connections only.

● Ethernet

Use for Ethernet connections, such as connections that use a switch.

Add New Remote Access Policy Method

STEP 11．Choose **User**



New Remote Access Policy Wizard

User or Group Access

You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

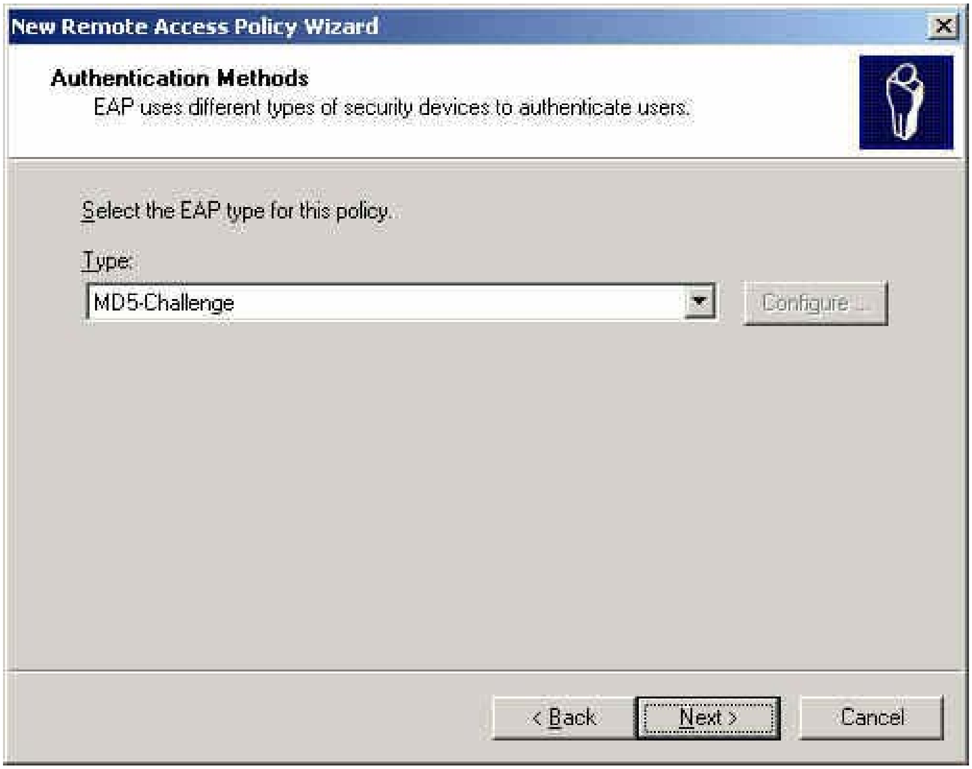
● User
User access permissions are specified in the user account.

○ Group
Individual user permissions override group permissions.

Group name:

Add New Remote Access Policy of User or Group Access

STEP 12．Select **MD5-Challenge**



New Remote Access Policy Wizard

Authentication Methods

EAP uses different types of security devices to authenticate users.

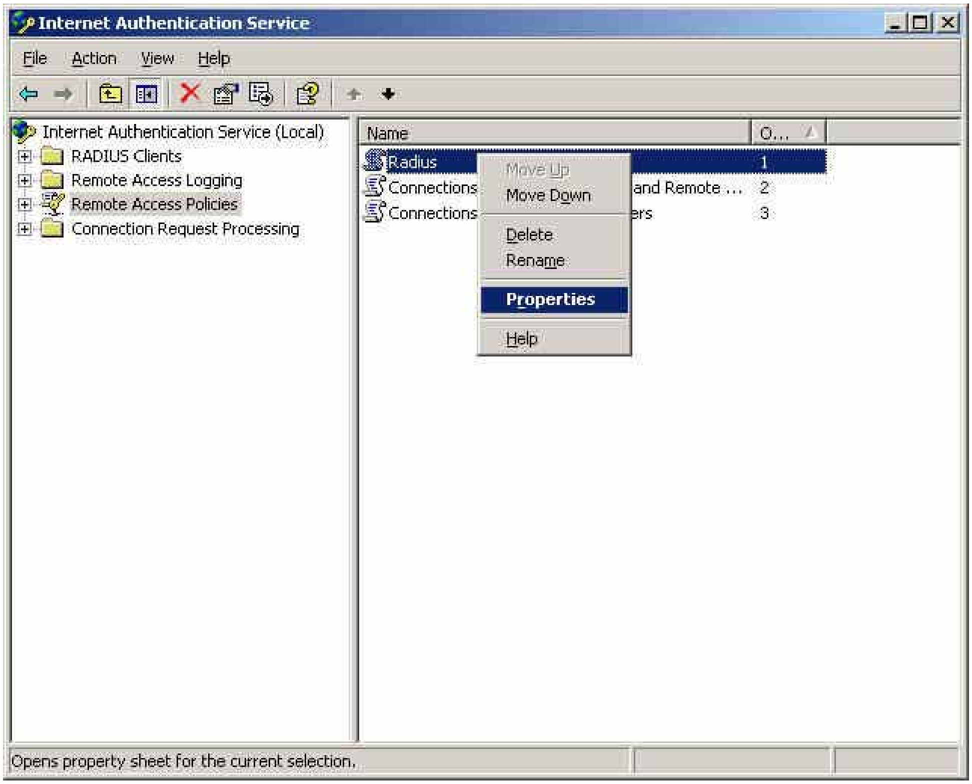
Select the EAP type for this policy.

Type:

MD5-Challenge

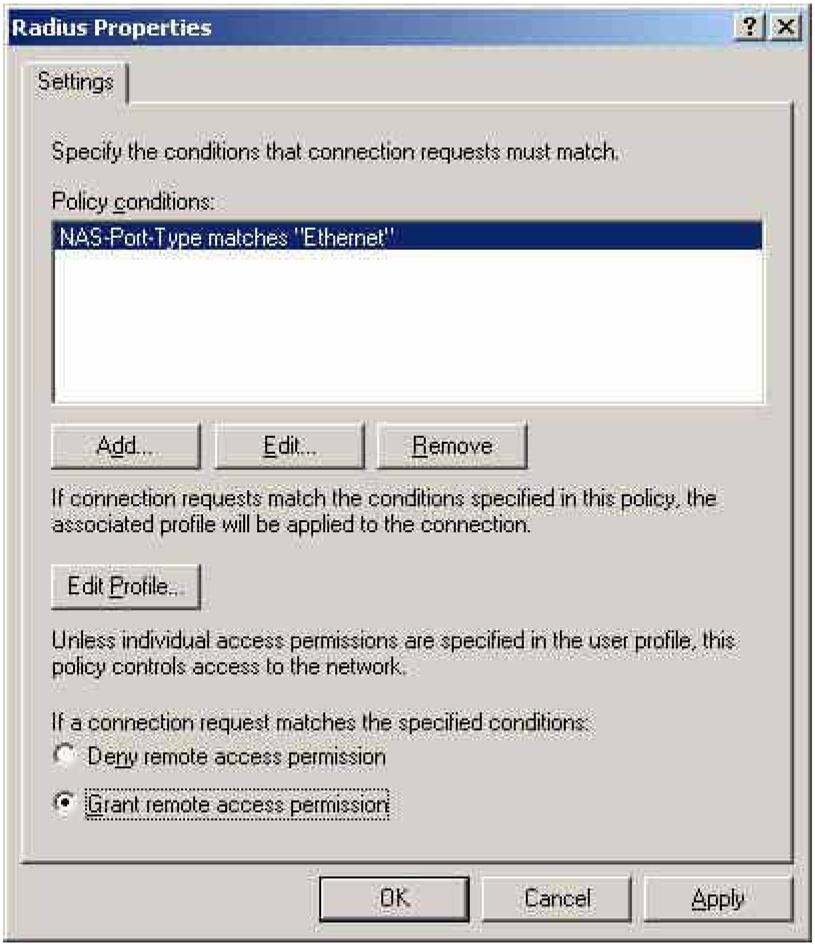
Authentication Methods of Adding New Remote Access Policy

STEP 13．Press the right button on **Radius** and choose **Properties**.



Internet Authentication Service Setting Web UI

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



Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Ethernet"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

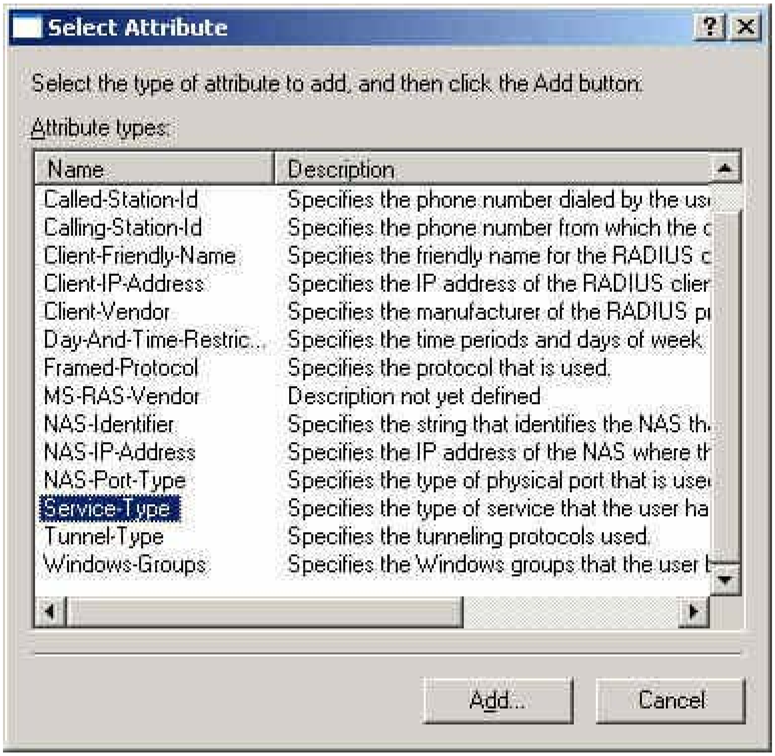
If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

RADIUS Properties Settings

STEP 15．Add **Service-Type**



Select Attribute

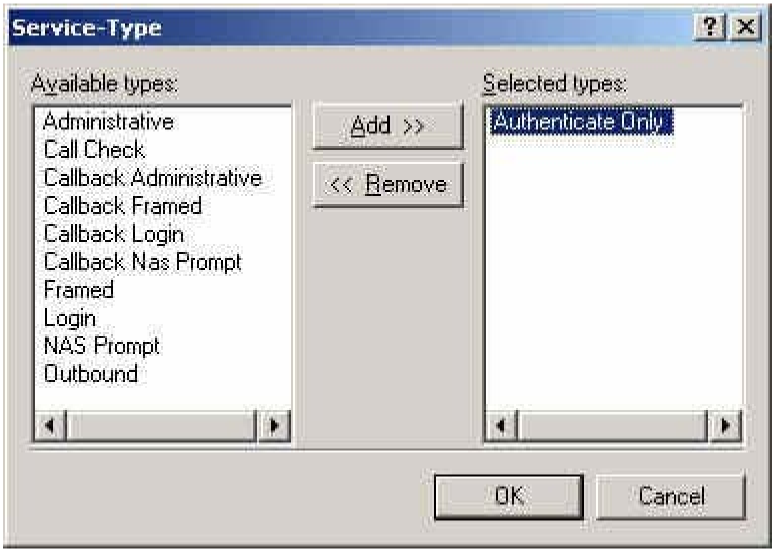
Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Specifies the phone number dialed by the us
Calling-Station-Id	Specifies the phone number from which the c
Client-Friendly-Name	Specifies the friendly name for the RADIUS c
Client-IP-Address	Specifies the IP address of the RADIUS clier
Client-Vendor	Specifies the manufacturer of the RADIUS pi
Day-And-Time-Restric...	Specifies the time periods and days of week
Framed-Protocol	Specifies the protocol that is used.
MS-RAS-Vendor	Description not yet defined
NAS-Identifier	Specifies the string that identifies the NAS th.
NAS-IP-Address	Specifies the IP address of the NAS where th
NAS-Port-Type	Specifies the type of physical port that is use
Service-Type	Specifies the type of service that the user ha
Tunnel-Type	Specifies the tunneling protocols used.
Windows-Groups	Specifies the Windows groups that the user b

Add New RADIUS Attribute

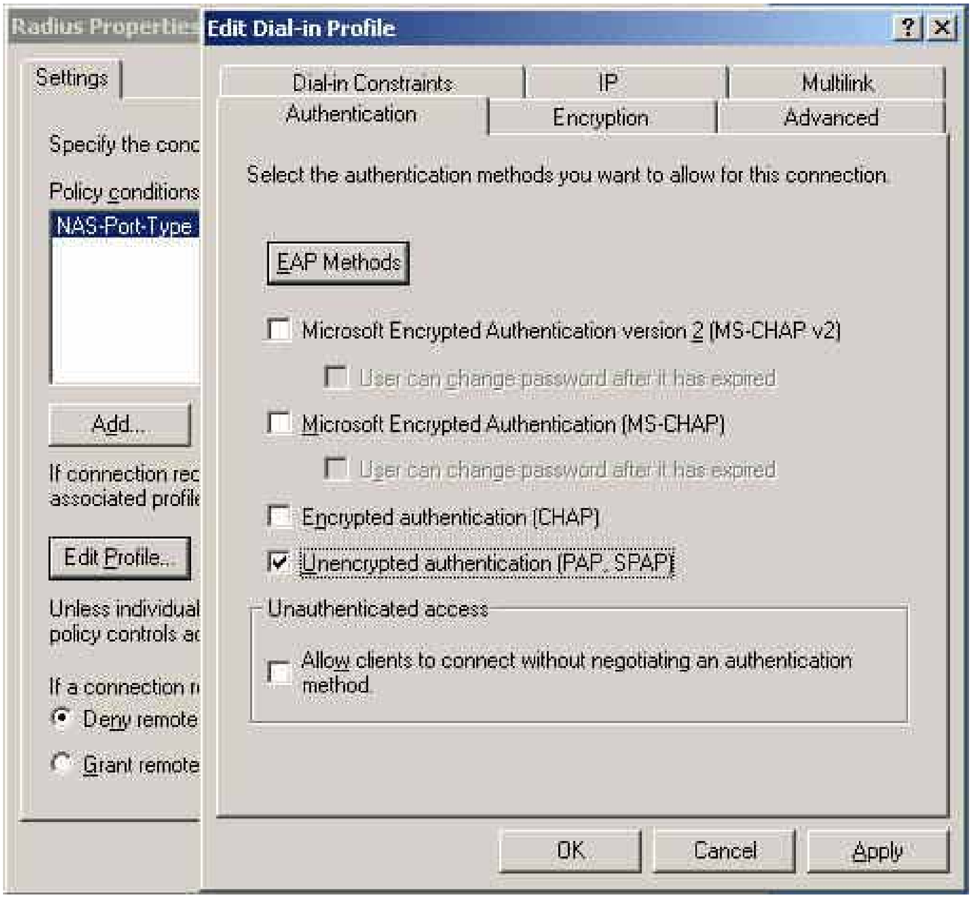
STEP 16．Add **Authenticate Only** from the left side.



Selected types: Authenticate Only

Add RADIUS Service-Type

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



Select the authentication methods you want to allow for this connection.

EAP Methods

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

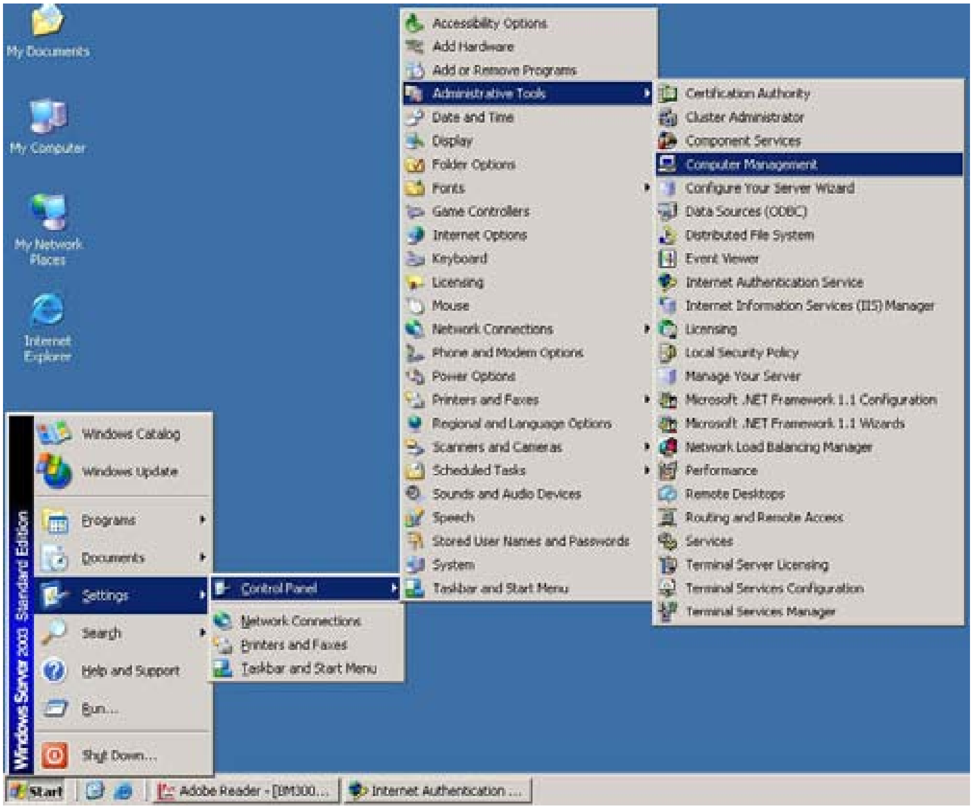
☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

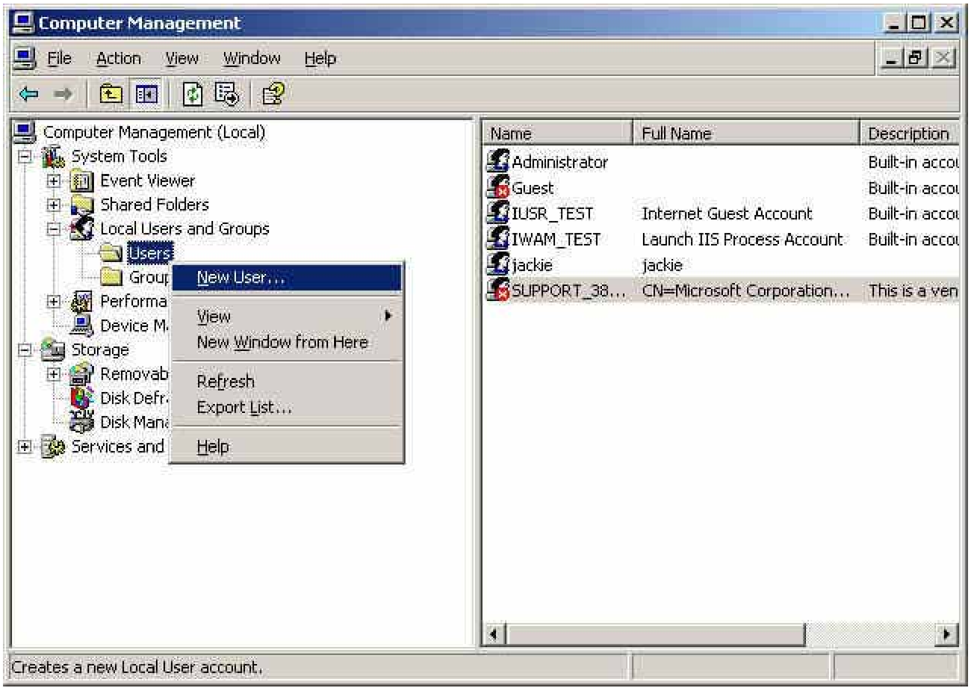
Edit DADIUS Dial-in Property

STEP 18．Add Auth User. Click [Start] → [Setting]→ [Control Panel] → [Administrative Tools], Choose [Computer Management]



Enter Computer Management

STEP 19． Press the right button on the **Users** and select **New User**.



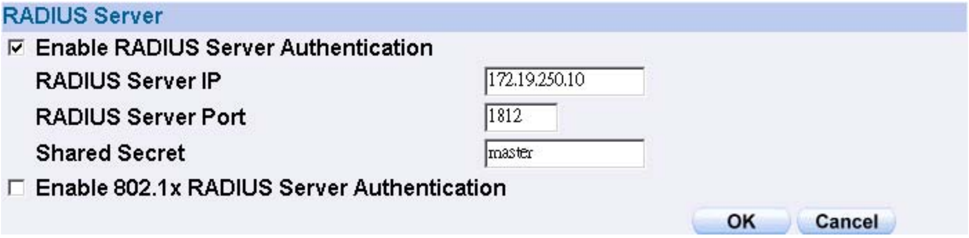
Name	Full Name	Description
Administrator		Built-in accou
Guest		Built-in accou
IUSR_TEST	Internet Guest Account	Built-in accou
IWAM_TEST	Launch IIS Process Account	Built-in accou
jackie	jackie	
SUPPORT_38...	CN=Microsoft Corporation...	This is a ven

Creates a new Local User account.

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**



RADIUS Server

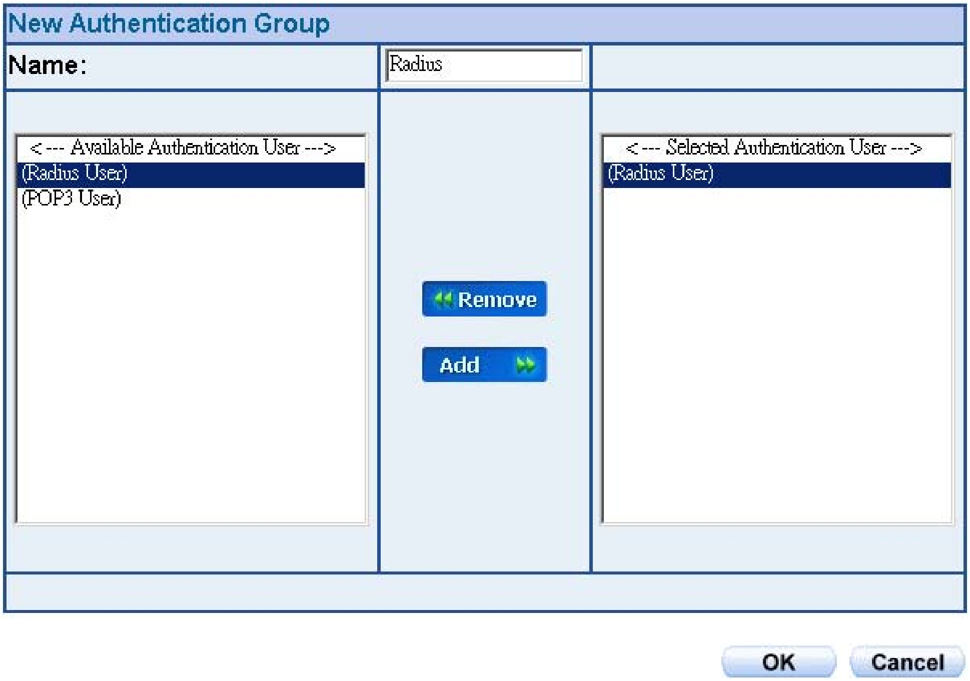
☑ Enable RADIUS Server Authentication

RADIUS Server IP	172.19.250.10
RADIUS Server Port	1812
Shared Secret	master

☐ Enable 802.1x RADIUS Server Authentication

Setting RADIUS Server

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



New Authentication Group

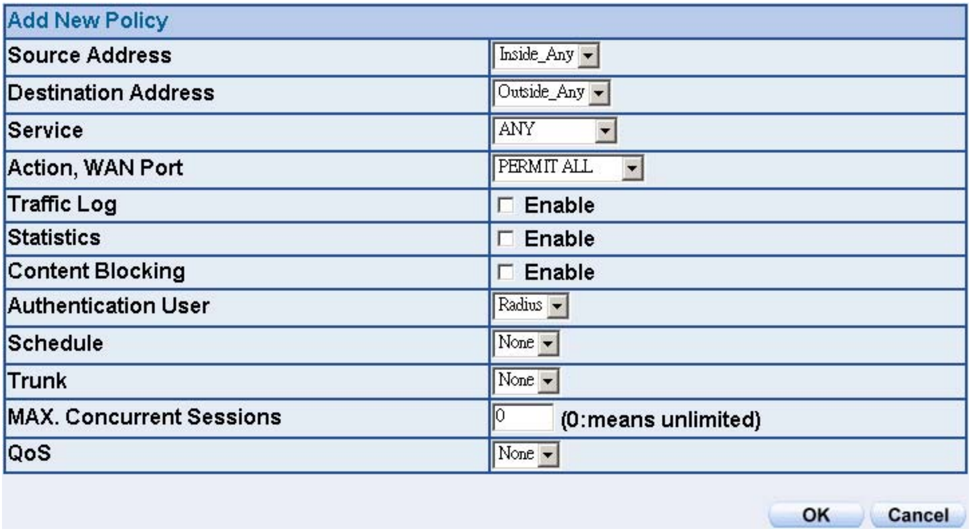
Name: Radius

<--- Available Authentication User --->
(Radius User)
(POP3 User)

<--- Selected Authentication User --->
(Radius User)

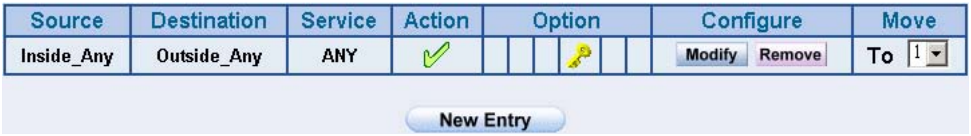
Add New RADIUS Auth Group

STEP 23． Add a policy of **Auth User Group** (RADIUS) that set by **STEP 22** in **Outgoing Policy.**



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	Radius
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

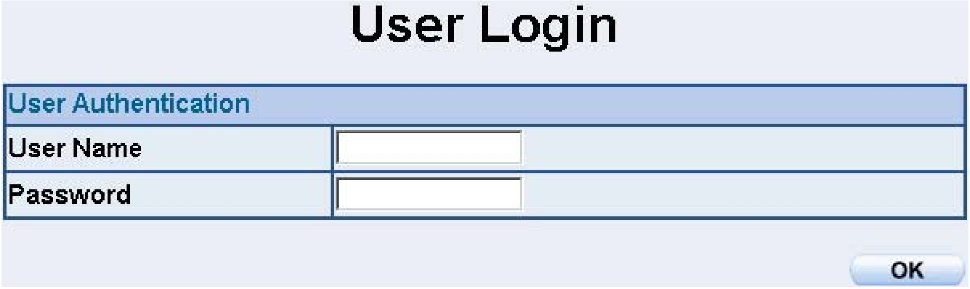
RADIUS Authentication Policy Setting Web UI



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

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 SG-1000.



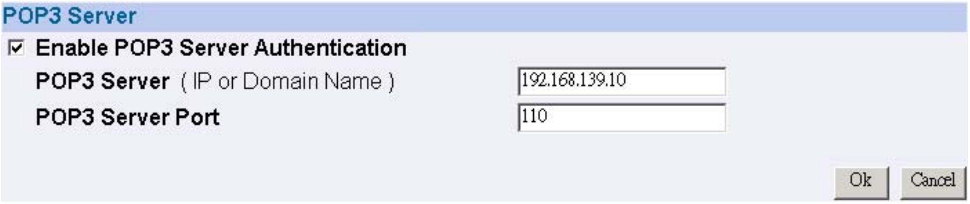
User Login

User Authentication	
User Name	
Password	

Access to Internet by Authentication Web UI

9.3 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**



POP3 Server

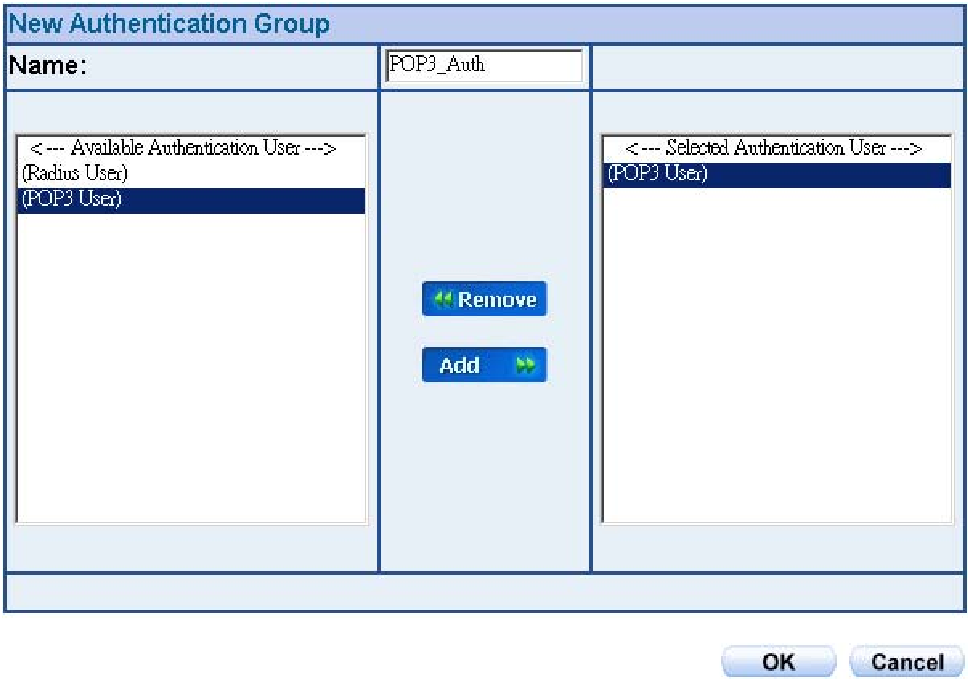
☑ Enable POP3 Server Authentication

POP3 Server (IP or Domain Name) 192.168.139.10

POP3 Server Port 110

POP3 Server Setting Web UI

STEP 2 . Add POP3 User in **New Authentication Group**.



New Authentication Group

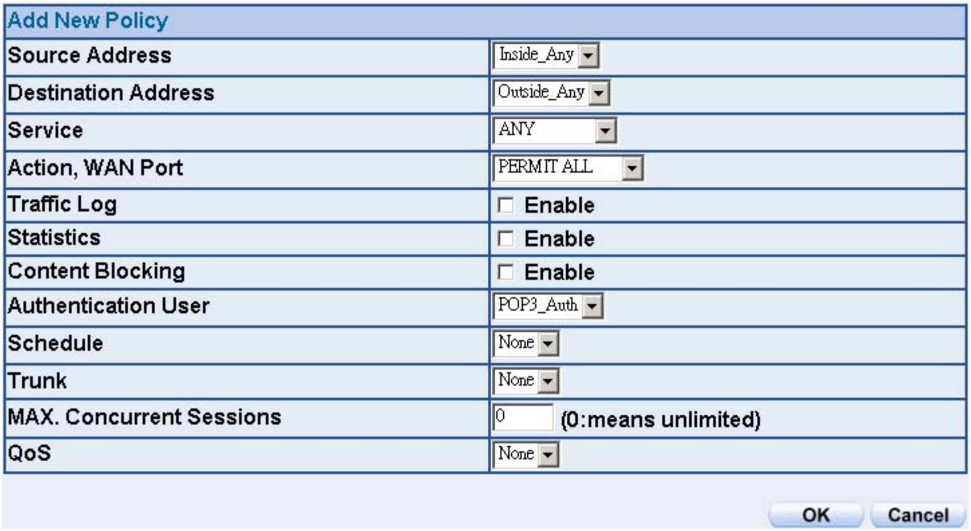
Name: POP3_Auth

< --- Available Authentication User --->
(Radius User)
(POP3 User)

< --- Selected Authentication User --->
(POP3 User)

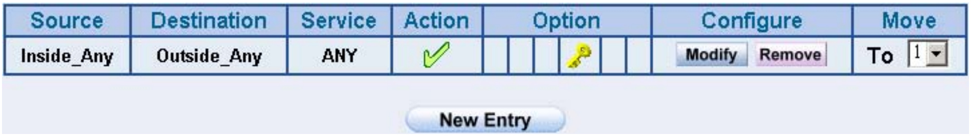
Add New POP3 User Web UI

STEP 3． Add a policy of **Authentication User Group** that set in STEP2 in **Outgoing Policy**.



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	POP3_Auth ▾
Schedule	None ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

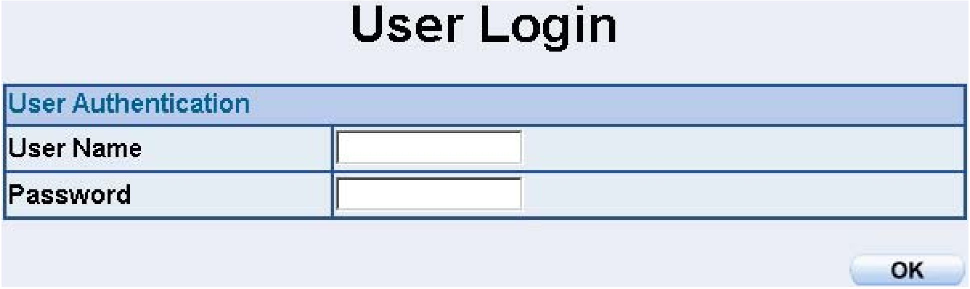
POP3 Server Authentication Policy Setting



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

Complete POP3 Server Authentication Policy Setting

STEP 4 . When the user is going to access to Internet by browser, the Authentication Web UI will display in the browser. After entering correct account and password, click on **OK** and then can access to Internet by SG-1000:



User Login

User Authentication	
User Name	
Password	

The Authentication Web UI

Chapter 10

Content Filtering

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

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

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

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

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

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

Define the required fields of Content Blocking

URL String:

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

Popup Blocking:

- Prevent the pop-up Web UI appearing

ActiveX Blocking:

- Prevent ActiveX packets

Java Blocking:

- Prevent Java packets

Cookies Blocking:

- Prevent Cookies packets

eDonkey Blocking:

- Prevent users to deliver files by eDonkey and eMule

BitTorrent Blocking:

- Prevent users to deliver files by BitTorrent

WinMX:

- Prevent users to deliver files by WinMX

IM Blocking:

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

Audio and Video Types:

- Prevent users to transfer sounds and video file by http

Sub-name file Blocking:

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

All Type:

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

We set up five Content Blocking examples in this chapter:

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

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

※URL Blocking:

Symbol: ～ means open up; ＊ means metacharacter

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

Only open specific website to enter:

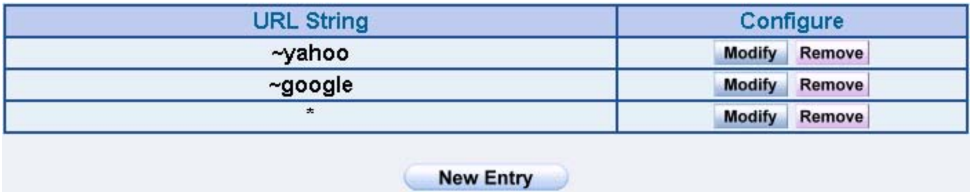
1. Add the website you want to open up in URL String. While adding, you must enter the symbol "~" in front of the 「complete domain name」 or 「key word」 that represents to open these website to enter". For example: ~www.kcg.gov.tw or ~gov.

2. After setting up the website you want to open up, enter an order to "forbid all" in the last URL String; means only enter ＊ in URL String.

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

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

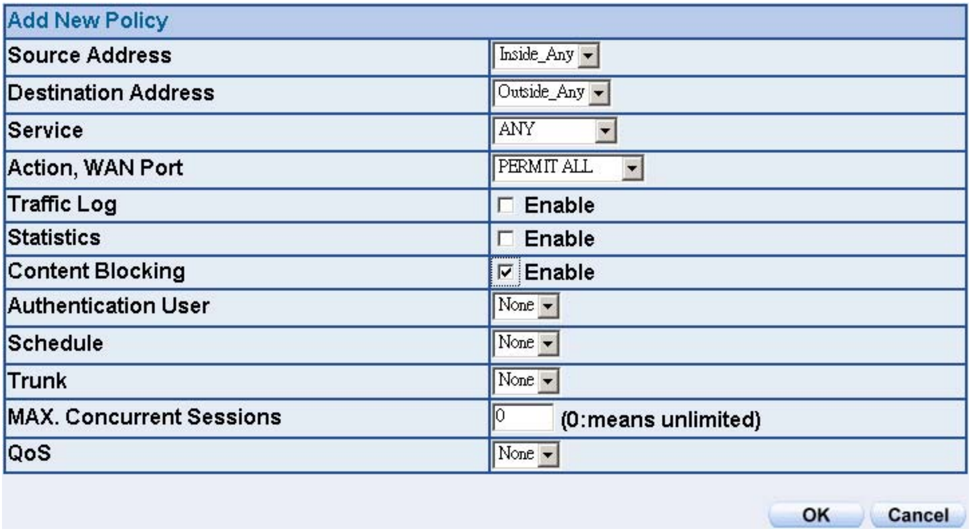
- Click **New Entry**
- **URL String:** Enter ~yahoo, and click **OK**
- Click **New Entry**
- **URL String:** Enter ~google, and click **OK**
- Click **New Entry**
- **URL String**: Enter ＊**,** and click **OK**
- Complete setting a URL Blocking policy



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

Content Filtering Table

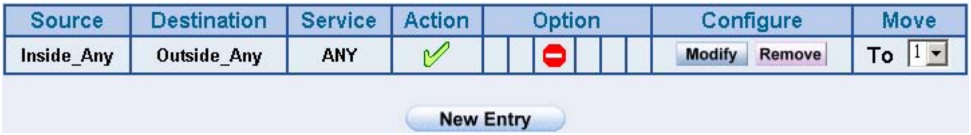
STEP 2． Add a **Outgoing Policy** and use in **Content Blocking** function:



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	☑ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

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:



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

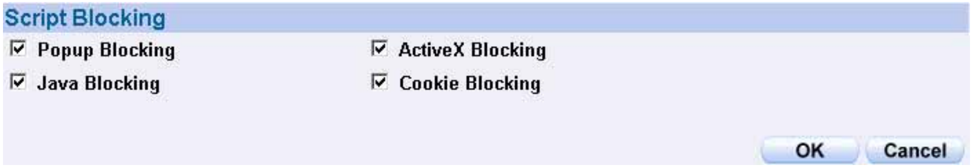
Complete Policy Settings

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

10.2 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



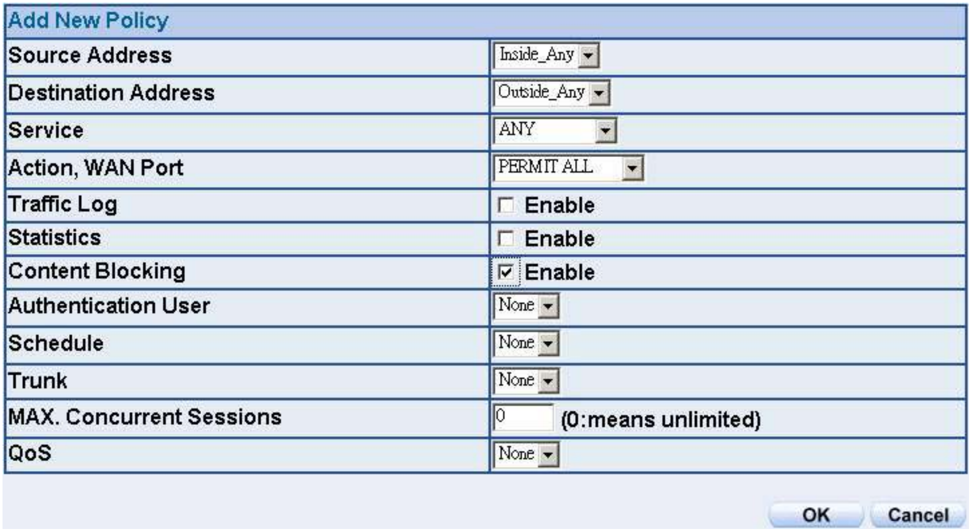
Script Blocking

☑ Popup Blocking ☑ ActiveX Blocking

☑ Java Blocking ☑ Cookie Blocking

Script Blocking Web UI

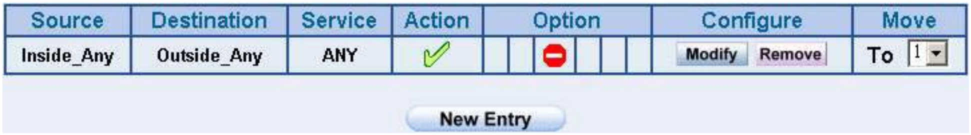
STEP 2．Add a new **Outgoing Policy** and use in **Content Blocking** function:



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	☐ Enable
Statistics	☐ Enable
Content Blocking	☑ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

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**:



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

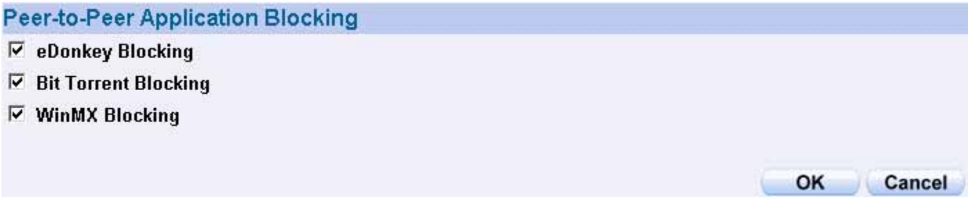
Complete Script Blocking Policy Setting

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.

10.3 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



Peer-to-Peer Application Blocking

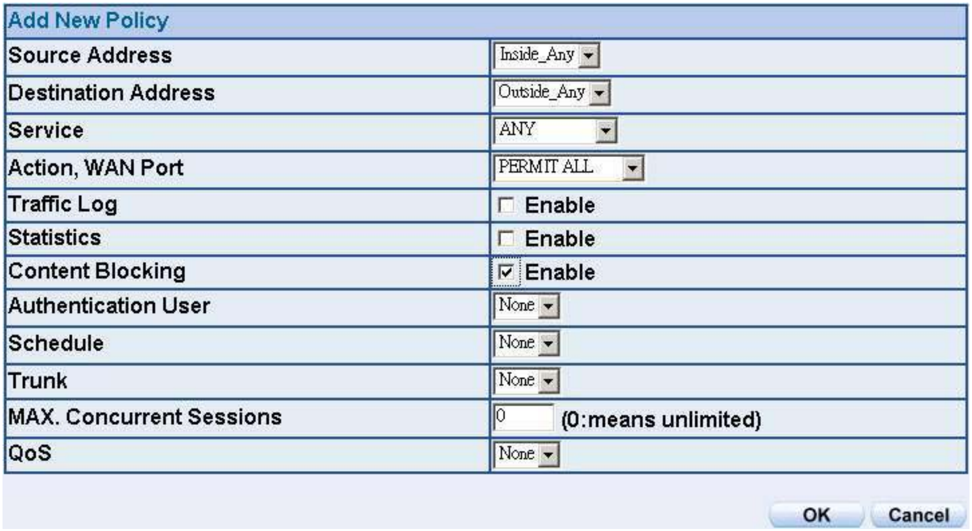
☑ eDonkey Blocking

☑ Bit Torrent Blocking

☑ WinMX Blocking

P2P Blocking Web UI

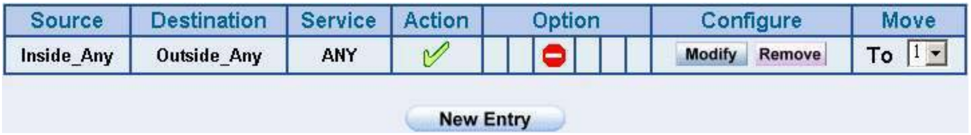
STEP 2 . Add a new **Outgoing Policy** and use in **Content Blocking** function:



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	☑ Enable
Authentication User	None ▾
Schedule	None ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

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**:



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

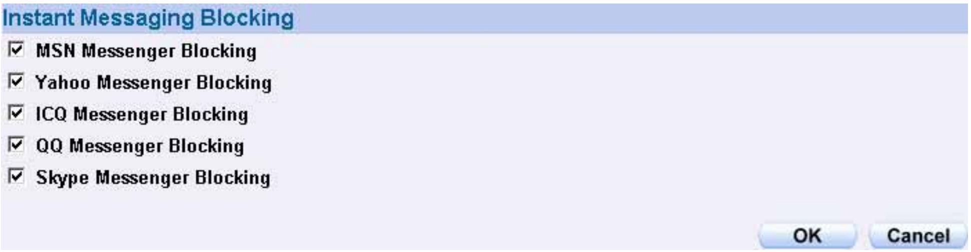
Complete P2P Blocking Policy Setting

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.

10.4 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.



Instant Messaging Blocking

☑ MSN Messenger Blocking

☑ Yahoo Messenger Blocking

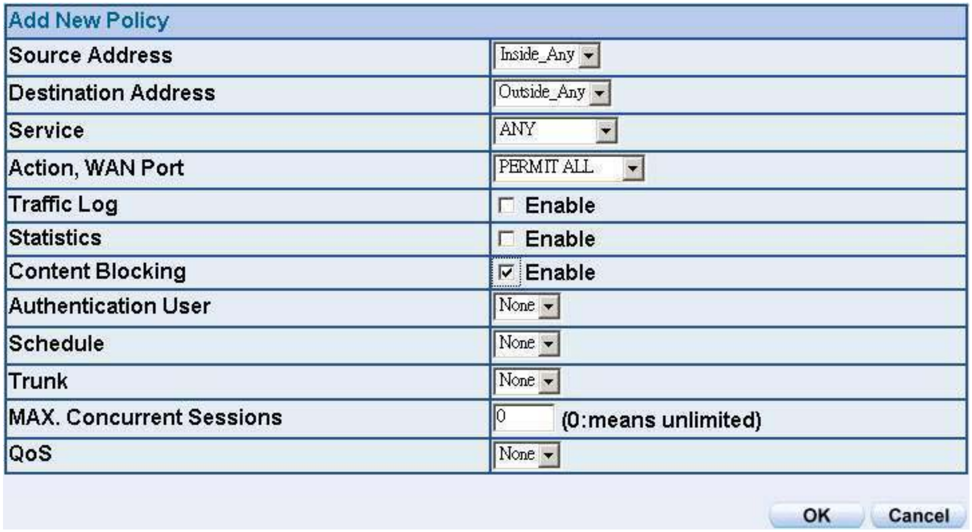
☑ ICQ Messenger Blocking

☑ QQ Messenger Blocking

☑ Skype Messenger Blocking

IM Blocking Web UI

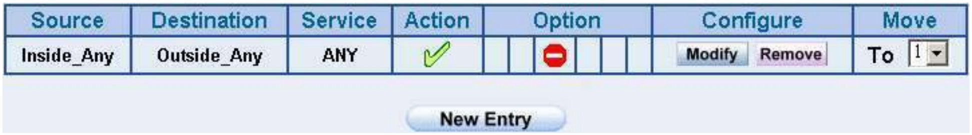
STEP 2 . Add a new **Outgoing Policy** and use in **Content Blocking** function:



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	☑ Enable
Authentication User	None ▾
Schedule	None ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

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:**



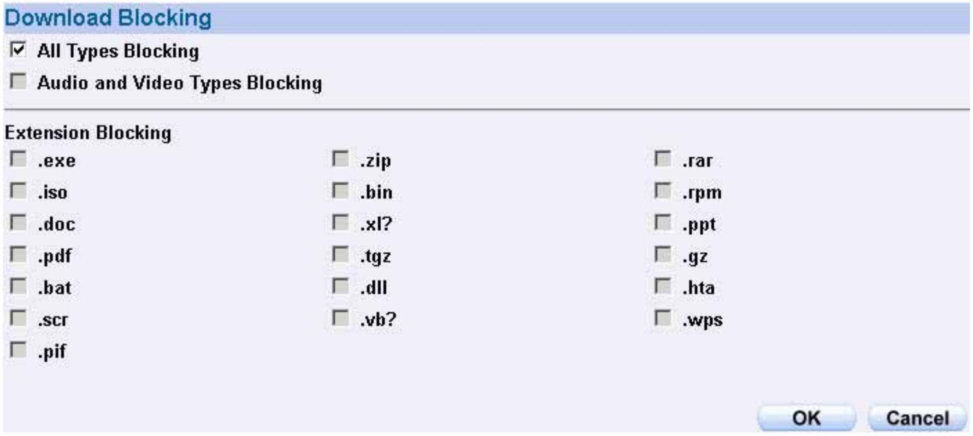
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	⛔	Modify Remove	To 1 ▾

Complete IM Blocking Policy Setting

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

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

- Select **All Types Blocking**
- Click **OK**
- Complete the setting of Download Blocking.



Download Blocking

☑ All Types Blocking

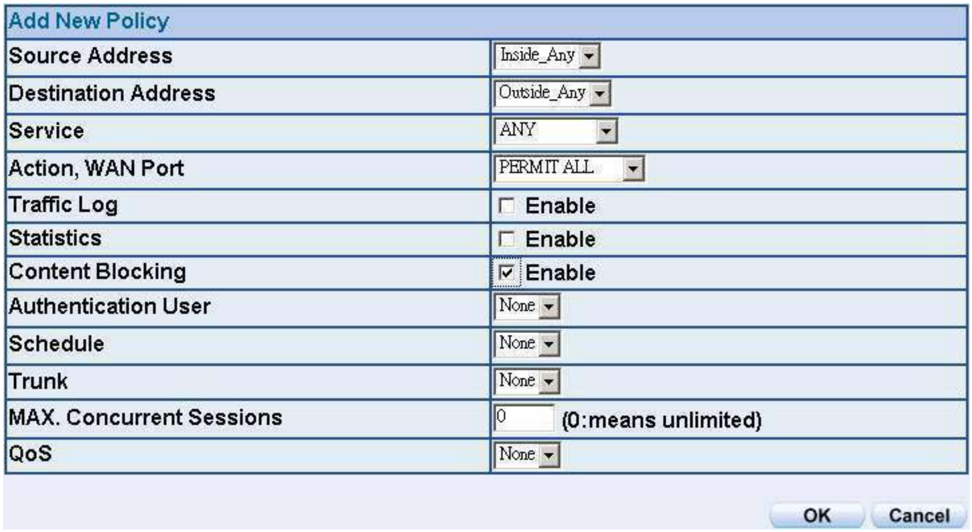
□ Audio and Video Types Blocking

Extension Blocking

□ .exe	□ .zip	□ .rar
□ .iso	□ .bin	□ .rpm
□ .doc	□ .xl?	□ .ppt
□ .pdf	□ .tgz	□ .gz
□ .bat	□ .dll	□ .hta
□ .scr	□ .vb?	□ .wps
□ .pif		

Download Blocking Web UI

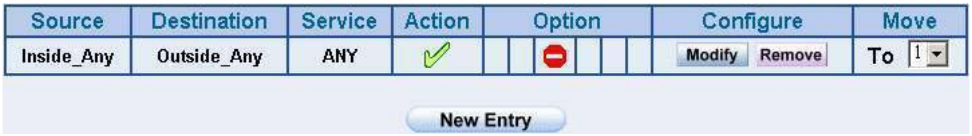
STEP 2． Add a new **Outgoing Policy** and use in **Content Blocking** function:



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	☑ Enable
Authentication User	None ▾
Schedule	None ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

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:



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

Complete Download Blocking Policy Setting

Chapter 11

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 SG-1000’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 SG-1000’s Virtual Server function can solve this problem. A Virtual Server has set the real IP address of the SG-1000’s WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the SG-1000 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 SG-1000's WAN subnet's Real IP and then map Real IP to Private IP of LAN by the SG-1000. It is a one-to-one mapping. That is, to map all the service of one WAN Real IP Address to one LAN Private IP Address.

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

Define the required fields of Virtual Server

WAN IP：

- WAN IP Address (Real IP Address)

Map to Virtual IP：

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

Virtual Server Real IP：

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

Service name (Port Number)：

- The service name that provided by the Virtual Server.

External Service Port：

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

Server Virtual IP：

- The virtual IP which mapped by the Virtual Server.

We set up four Virtual Server examples in this chapter:

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

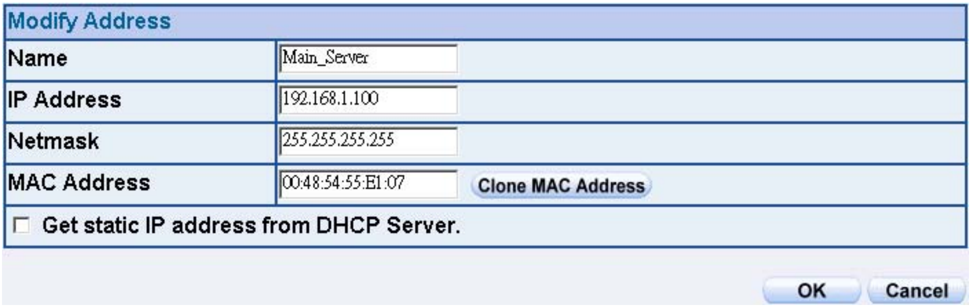
Preparation

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

11.1 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:



Modify Address

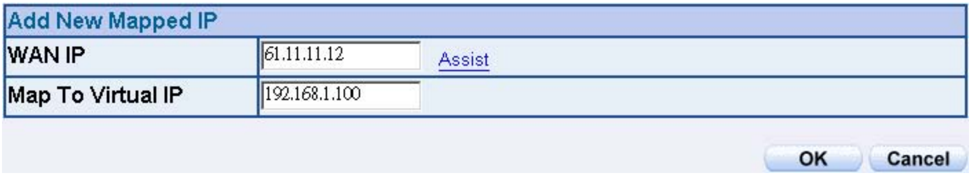
Name	Main_Server
IP Address	192.168.1.100
Netmask	255.255.255.255
MAC Address	00:48:54:55:E1:07 Clone MAC Address

□ Get static IP address from DHCP Server.

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

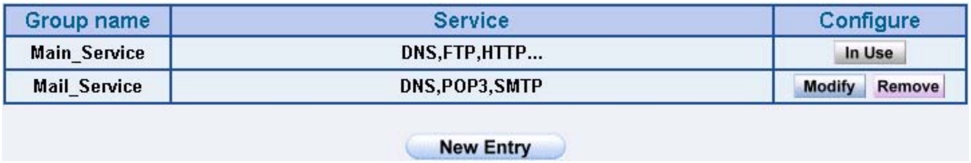


Add New Mapped IP

WAN IP	61.11.11.12 Assist
Map To Virtual IP	192.168.1.100

Mapped IP Setting Web UI

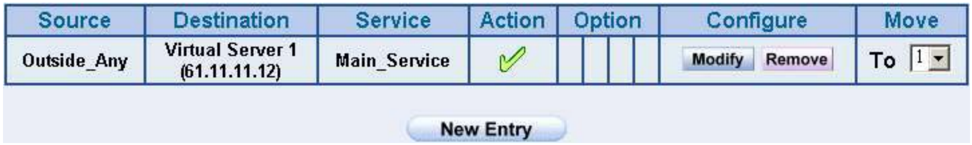
STEP 4． Group the services (DNS, FTP, HTTP, POP3, SMTP…) that provided and used by server in **Service** function. And add a new service group for server to send mails at the same time.



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

Service Setting

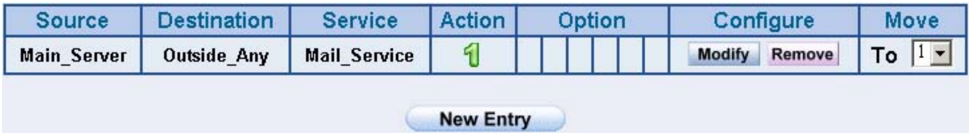
STEP 5． Add a policy that includes settings of STEP3, 4 in **Incoming Policy.**



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

Complete the Incoming Policy

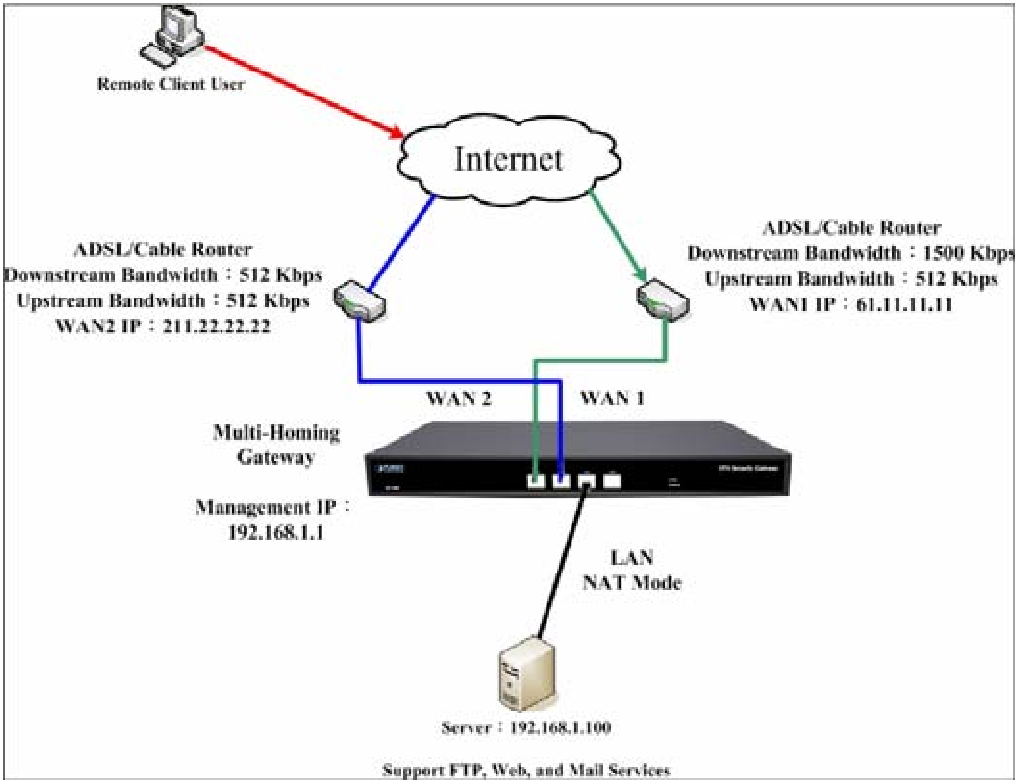
STEP 6． Add a policy that includes STEP2, 4 in **Outgoing Policy**. It makes the server to send e-mail to external mail server by mail service.



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

Complete the Outgoing Policy

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



A Single Server that Provides Several Services by Mapped IP

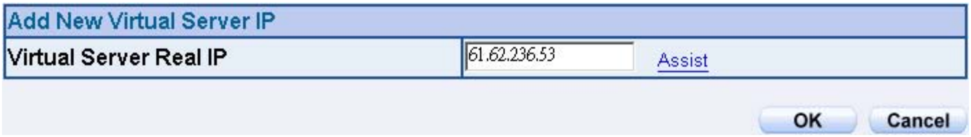
Strong suggests **not** to choose **ANY** when setting Mapped IP and choosing service. Otherwise the Mapped IP will be exposed to Internet easily and may be attacked by Hacker.

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

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

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

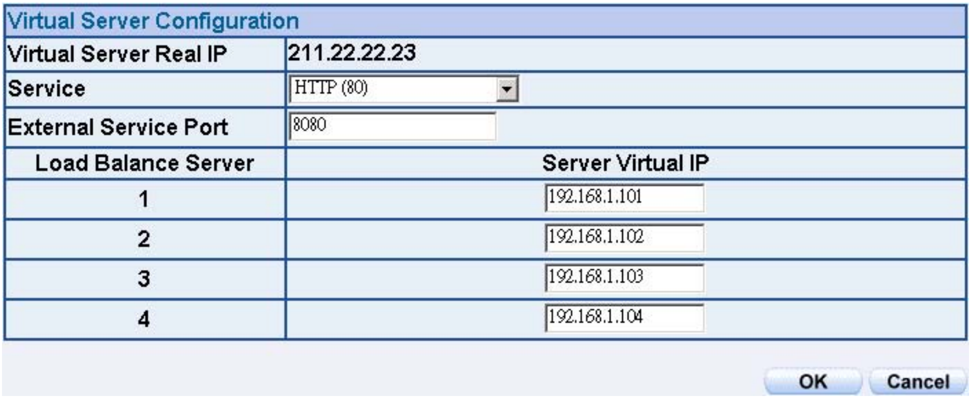
- Click the button next to **Virtual Server Real IP** (“**click here to configure**”) in **Server 1**
- **Virtual Server Real IP:** Enter 211.22.22.23 (click **Assist** for assistance)
- Click **OK**



Add New Virtual Server IP	
Virtual Server Real IP	61.62.236.53 Assist

Virtual Server Real IP Setting

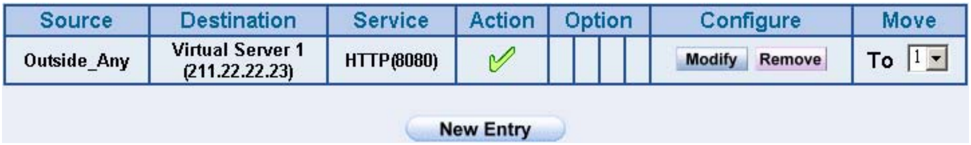
- Click **New Entry**
- **Service:** Select HTTP (80)
- **External Service Port:** Change to 8080
- **Load Balance Server1:** Enter 192.168.1.101
- **Load Balance Server2:** Enter 192.168.1.102
- **Load Balance Server3:** Enter 192.168.1.103
- **Load Balance Server4:** Enter 192.168.1.104
- Click **OK**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



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

Virtual Server Configuration Web UI

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



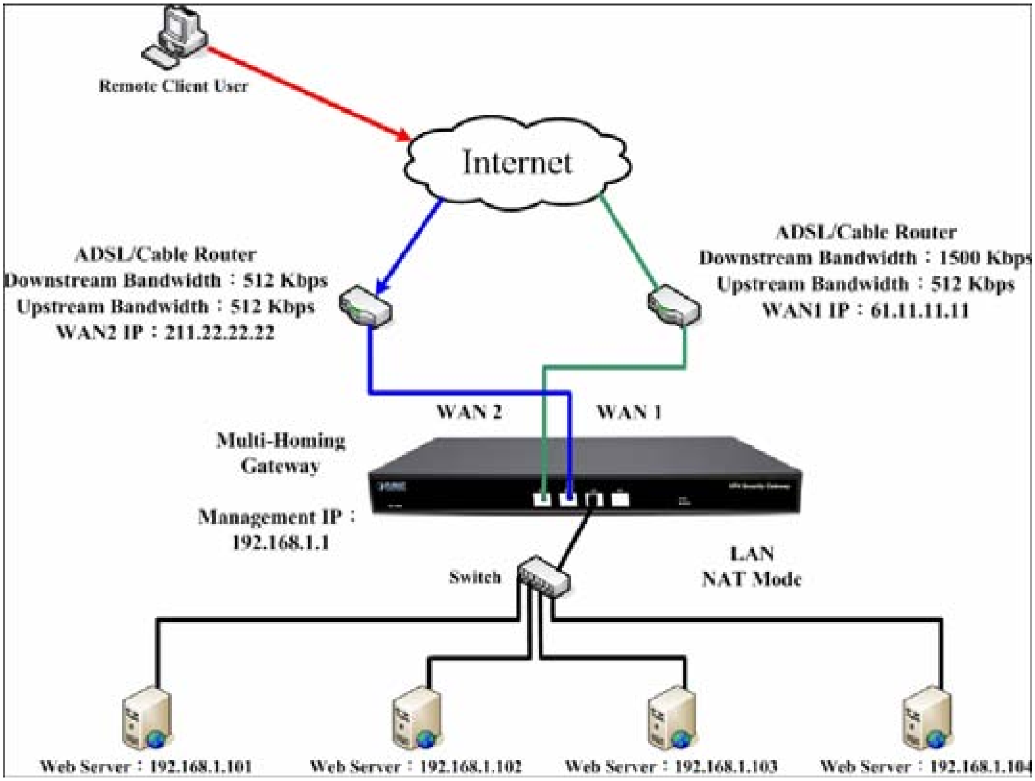
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (211.22.22.23)	HTTP(8080)	✓		Modify Remove	To 1

New Entry

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.

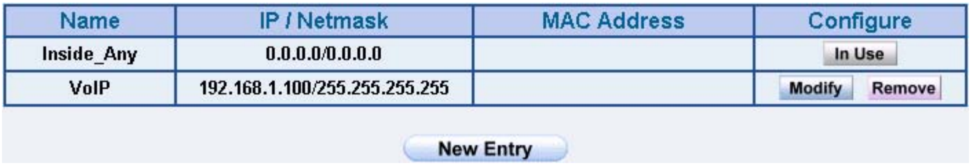


Several Servers Provide a Single Service by Virtual Server

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

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

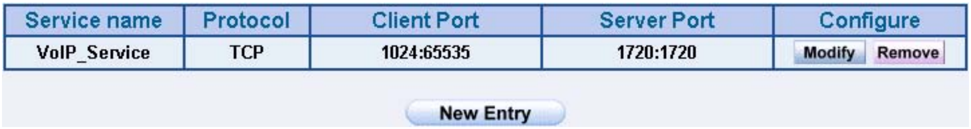
STEP 2． Enter the following setting in **LAN** of **Address** function:



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
VoIP	192.168.1.100/255.255.255.255		Modify Remove

Setting LAN Address Web UI

STEP 3． Add new VoIP service group in **Custom** of **Service** function.

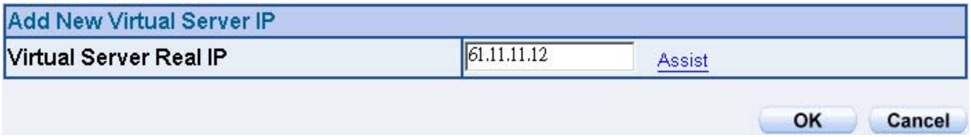


Service name	Protocol	Client Port	Server Port	Configure
VoIP_Service	TCP	1024:65535	1720:1720	Modify Remove

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**

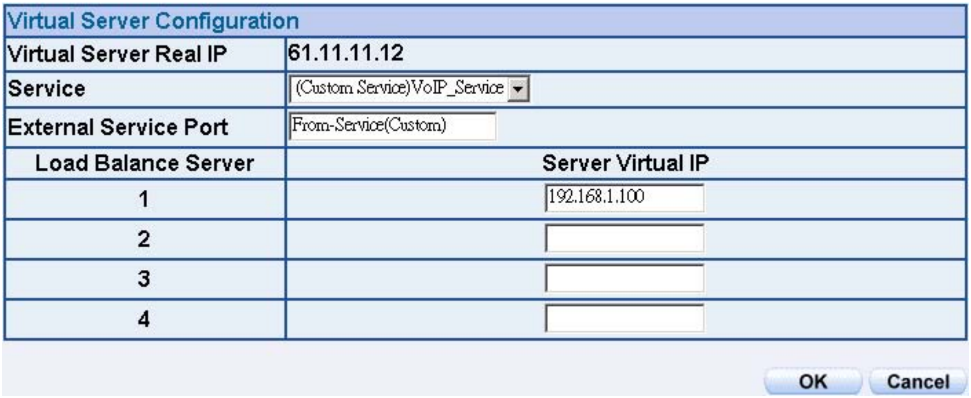


Add New Virtual Server IP

Virtual Server Real IP	61.11.11.12 Assist

Virtual Server Real IP Setting Web UI

- 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



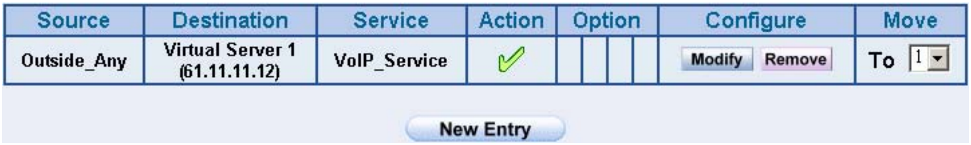
Virtual Server Configuration

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	

Virtual Server Configuration Web UI

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:

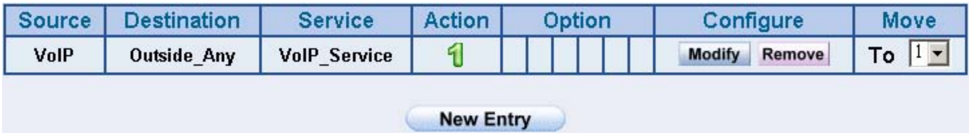


Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	VoIP_Service	✓		Modify Remove	To 1 ▾

New Entry

Complete the Policy includes Virtual Server Setting

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

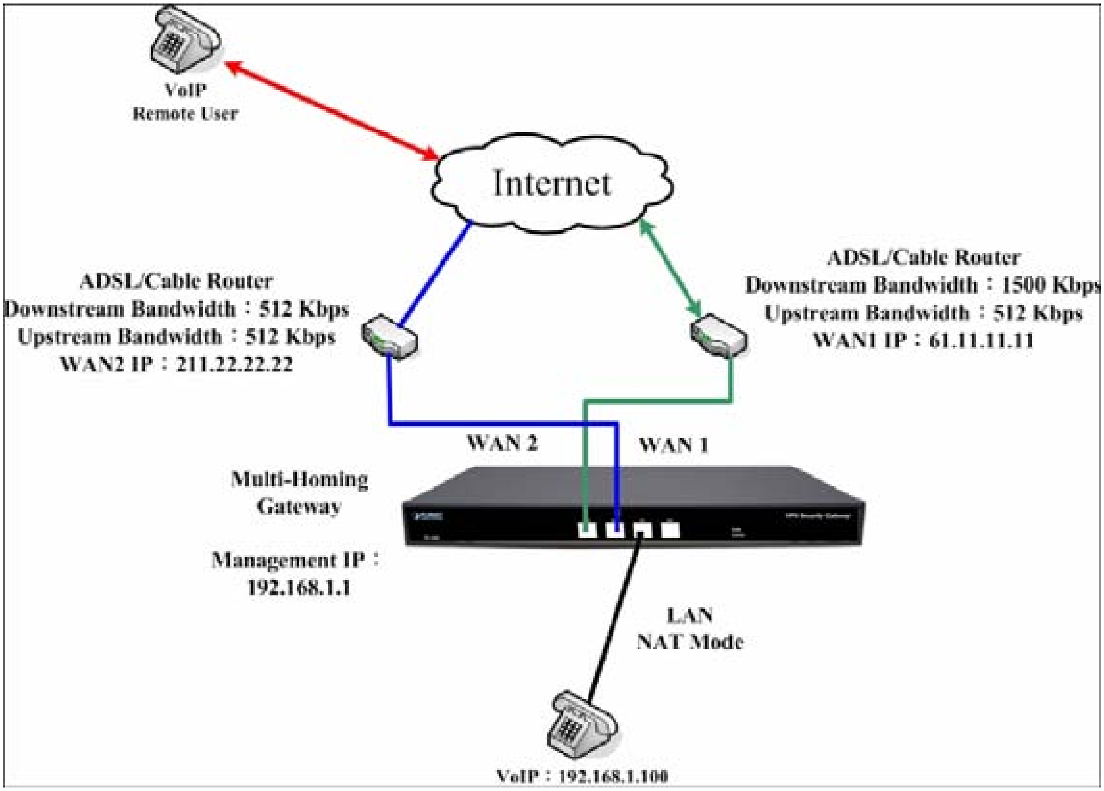


Source	Destination	Service	Action	Option	Configure	Move
VoIP	Outside_Any	VoIP_Service	↰		Modify Remove	To 1 ▾

New Entry

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.

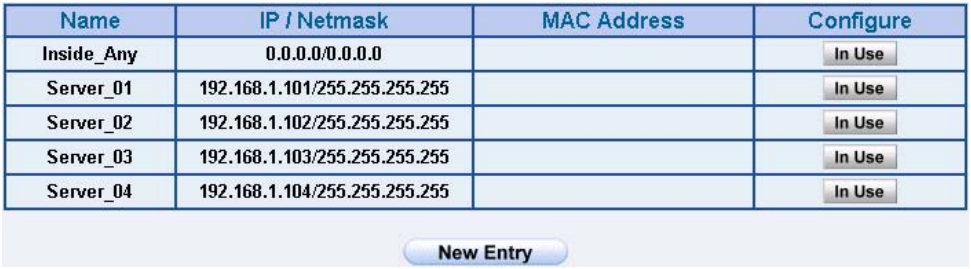


Complete the Setting of the External/Internal User using specific service to communicate with each other by Virtual Server

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.

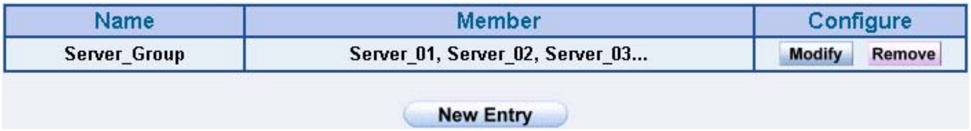
STEP 2．Enter the following in **LAN** and **LAN Group** of **Address** function:



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

New Entry

Mapped IP Setting of Virtual Server in Address

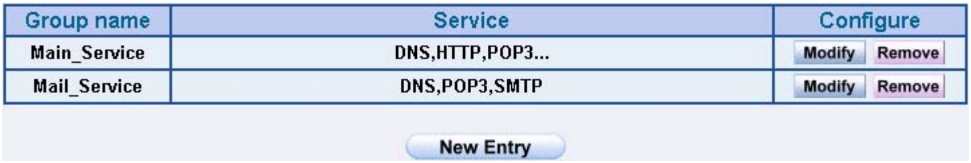


Name	Member	Configure
Server_Group	Server_01, Server_02, Server_03...	Modify Remove

New Entry

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.

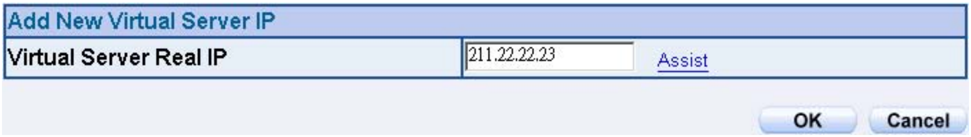


Group name	Service	Configure
Main_Service	DNS,HTTP,POP3...	Modify Remove
Mail_Service	DNS,POP3,SMTP	Modify Remove

Add New Service Group

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

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

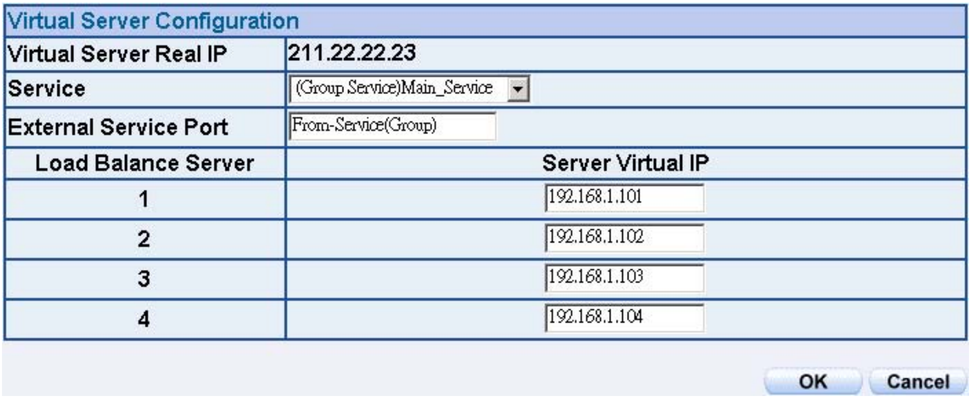


Add New Virtual Server IP

Virtual Server Real IP	211.22.22.23	Assist

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

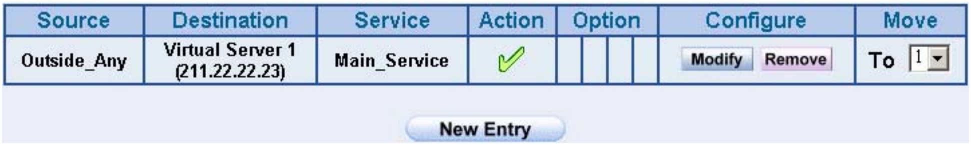


Virtual Server Configuration

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

Virtual Server Configuration Web UI

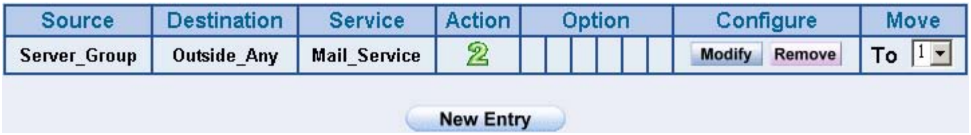
STEP 5 . Add a new **Incoming Policy,** which includes the virtual server that set by STEP 3:



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

Complete Incoming Policy Setting

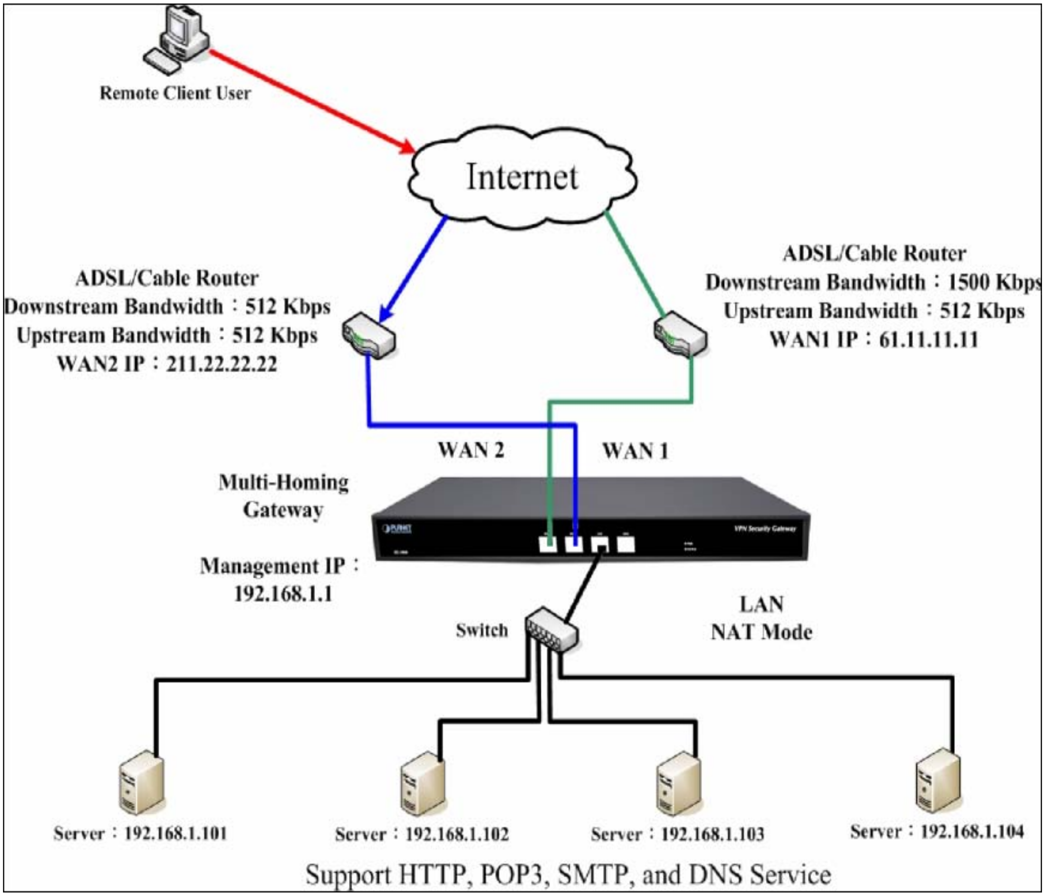
STEP 6 . Add a new policy that includes the settings of STEP2, 3 in **Outgoing Policy.** It makes server can send e-mail to external mail server by mail service.



Source	Destination	Service	Action	Option	Configure	Move
Server_Group	Outside_Any	Mail_Service	2		Modify Remove	To 1

Complete Outgoing Policy Setting

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



Complete the Setting of Providing Several Services by Several Virtual Server

Chapter 12

VPN

The SG-1000 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 SG-1000.

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

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

How to use VPN?

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

Define the required fields of VPN:

RSA:

- A public-key cryptosystem for encryption and authentication.

Preshared Key:

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

ISAKMP (Internet Security Association Key Management Protocol):

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

Main Mode:

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

Aggressive mode:

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

AH (Authentication Header):

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

ESP (Encapsulating Security Payload):

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

DES (Data Encryption Standard):

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

Triple-DES (3DES):

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

AES (Advanced Encryption Standard):

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

NULL Algorithm:

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

SHA-1 (Secure Hash Algorithm-1):

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

MD5:

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

GRE/IPSec:

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

Define the required fields of IPSec Function

i:

- To display the VPN connection status via icon。

Chart	--	🖥❌	🖧
Meaning	Not be applied	Disconnect	Connecting

Name:

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

WAN:

- The WAN interface of the local Gateway.

Gateway IP:

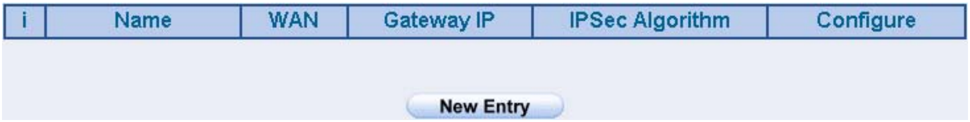
- The WAN interface IP address of the remote Gateway.

IPSec Algorithm:

- To display the Algorithm way.

Configure:

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



i	Name	WAN	Gateway IP	IPSec Algorithm	Configure

IPSec Autokey Web UI

Define the required fields of PPTP Server Function

PPTP Server:

- To select Enable or Disable

Client IP Range:

- Setting the IP addresses range for PPTP Client connection

i:

- To display the VPN connection status via icon。

Chart	--	🖥✗	🖥
Meaning	Not be applied	Disconnect	Connecting

User Name:

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

Client IP:

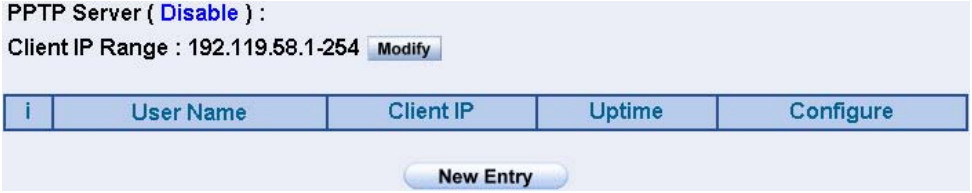
- Display the PPTP Client's IP address when connecting to PPTP Server.

Uptime:

- Display the connection time between PPTP Server and Client.

Configure:

- Click **Modify** to modify the PPTP Server Settings or click **Remove** to remove the setting.



PPTP Server (Disable) :

Client IP Range : 192.119.58.1-254 Modify

i	User Name	Client IP	Uptime	Configure

New Entry

PPTP Server Web UI

Define the required fields of PPTP Client Function

i:

- To display the VPN connection status via icon。

Chart	--	🖥❌	🖧
Meaning	Not be applied	Disconnect	Connecting

User Name:

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

Server IP or Domain Name:

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

Encryption:

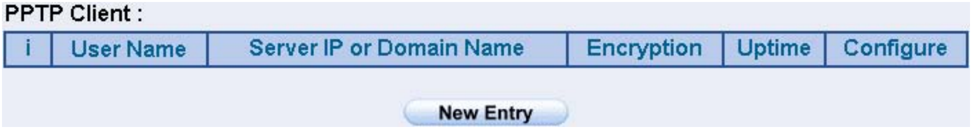
- Display PPTP Client and PPTP Server transmission, whether opens the encryption authentication mechanism.

Uptime:

- Displays the connection time between PPTP Server and Client.

Configure:

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



PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure

PPTP Client Web UI

Define the required fields of Trunk Function

i:

- To display the VPN connection status via icon。

Chart	--	🖥✗	🖧
Meaning	Not be applied	Disconnect	Connecting

Name:

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

Source Subnet:

- Displays the Source Subnet.

Destination Subnet:

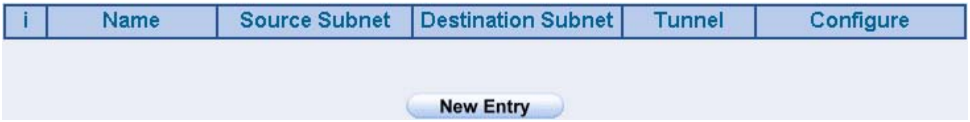
- Displays the Destination Subnet.

Tunnel:

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

Configure:

- Click **Modify** to change the argument of VPN Trunk; click **Remove** to remote the setting.



i	Name	Source Subnet	Destination Subnet	Tunnel	Configure

VPN Trunk Web UI

We set up two VPN examples in this chapter:

No.	Suitable Situation	Example
Ex1	**IPSec Autokey**	Setting IPSec VPN connection between two SG-1000
Ex2	**PPTP**	Setting PPTP VPN connection between two SG-1000

12.1 Setting IPSec VPN connection between two SG-1000

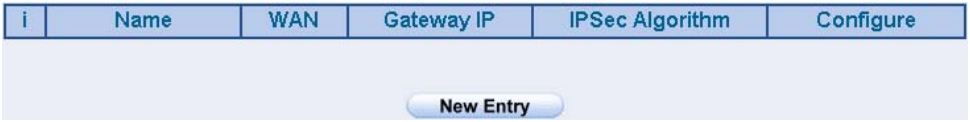
Preparation

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 SG-1000 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 SG-1000 192.168.10.1. Follow the steps below:

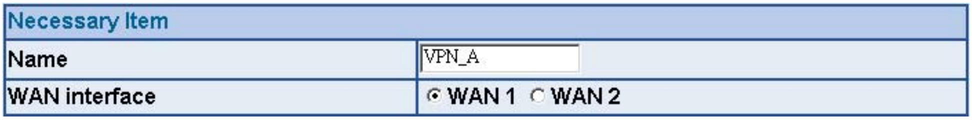
STEP 1．Enter the default IP of Gateway of Company A’s SG-1000, 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**.



i	Name	WAN	Gateway IP	IPSec Algorithm	Configure

IPSec Autokey Web UI

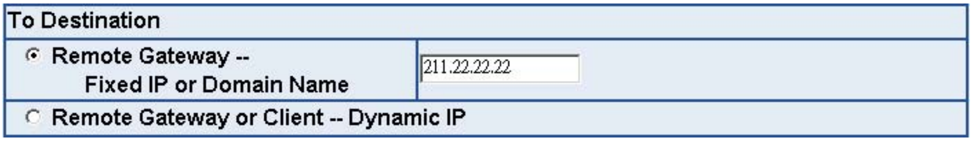
STEP 2．In the list of **IPSec Autokey**, fill in Name with **VPN_A** and select **WAN1** in WAN interface.



Necessary Item	
Name	VPN_A
WAN interface	● WAN 1 ○ WAN 2

IPSec Autokey Name Setting

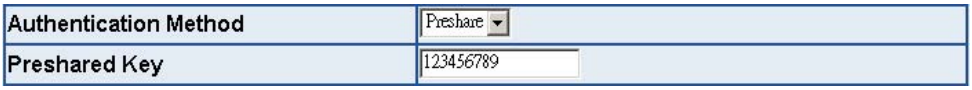
STEP 3． Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.



To Destination	
● Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
○ Remote Gateway or Client -- Dynamic IP	

IPSec To Destination Setting

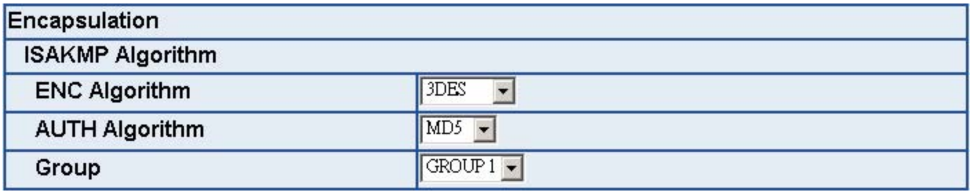
STEP 4． Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits)



Authentication Method	Preshare
Preshared Key	123456789

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.



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

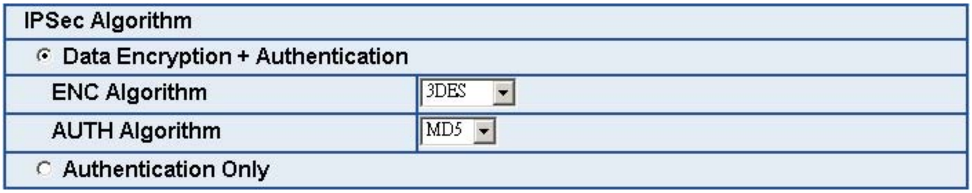
IPSec Encapsulation Setting

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**

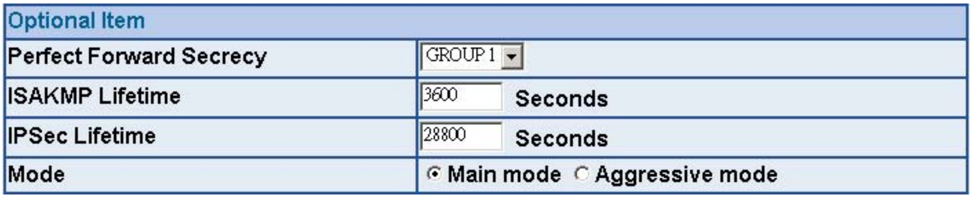
Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission



IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES ▾
AUTH Algorithm	MD5 ▾
○ Authentication Only	

IPSec Algorithm Setting

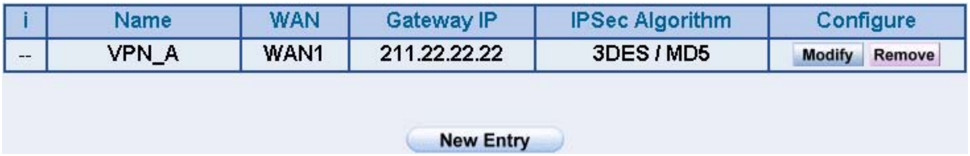
STEP 7． After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**.



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

IPSec Perfect Forward Secrecy Setting

STEP 8． Complete the IPSec Autokey setting.

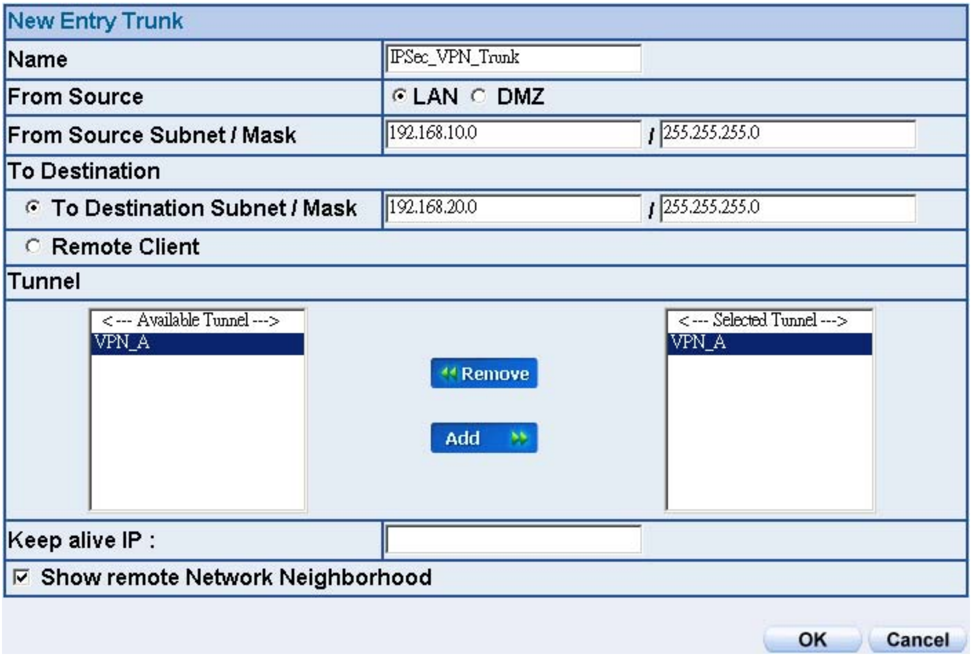


i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	Modify Remove

Complete Company A IPSec Autokey Setting

STEP 9．Enter the following setting in **Trunk** of **VPN** function**:**

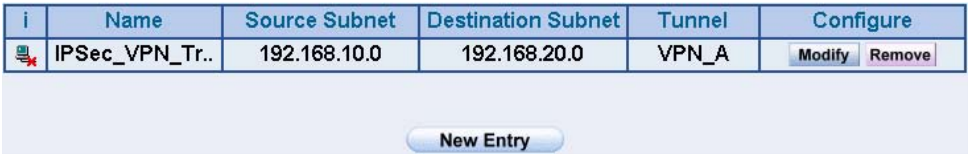
- Enter a specific Trunk **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **Tunnel:** Add VPN_A.
- Select **Show remote Network Neighborhood**.
- Click **OK**.



New Entry Trunk

Name	IPSec_VPN_Trunk
From Source	● LAN ○ DMZ
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
○ Remote Client	
Tunnel	
<--- Available Tunnel ---> VPN_A	<--- Selected Tunnel ---> VPN_A
Keep alive IP :	
☑ Show remote Network Neighborhood	

New Entry Trunk Setting

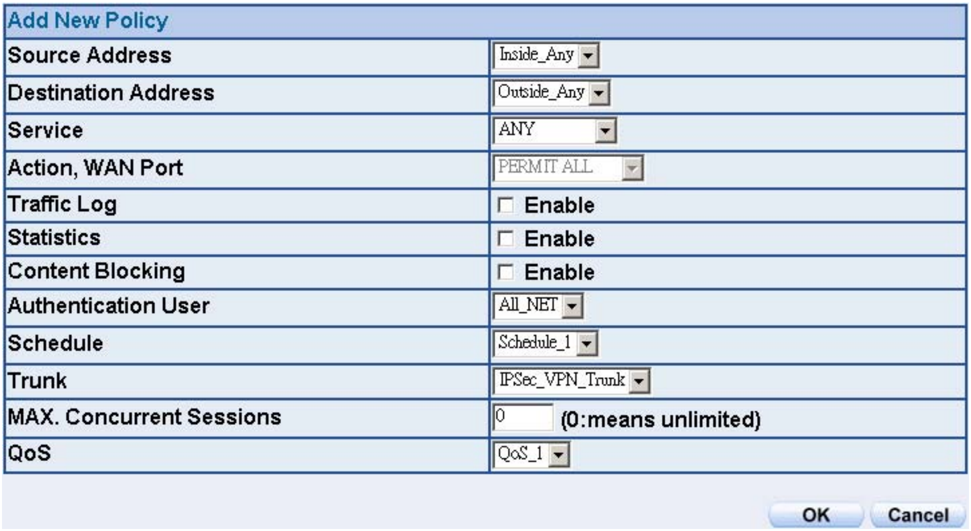


i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr..	192.168.10.0	192.168.20.0	VPN_A	Modify Remove

Complete New Entry Trunk Setting

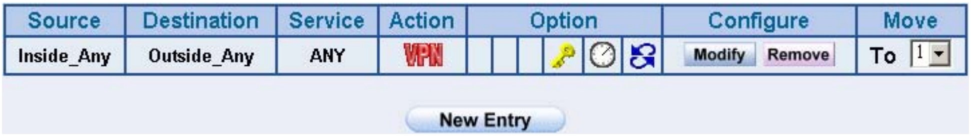
STEP 10 . Enter the following setting in **Outgoing Policy:**

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	All_NET
Schedule	Schedule_1
Trunk	IPSec_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

Setting the VPN Trunk Outgoing Policy

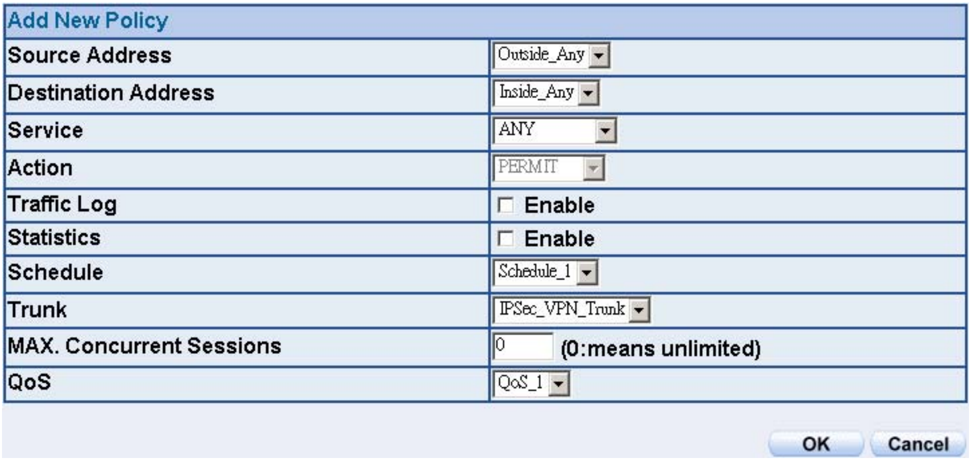


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Outgoing Policy Setting

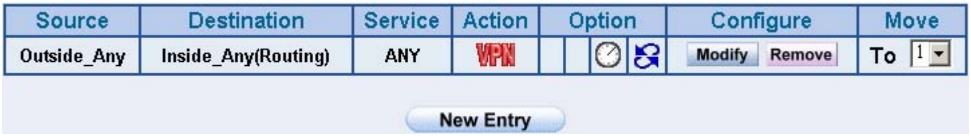
STEP 11． Enter the following setting in **Incoming Policy:**

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	Schedule_1
Trunk	IPSec_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

Setting the VPN Trunk Incoming Policy

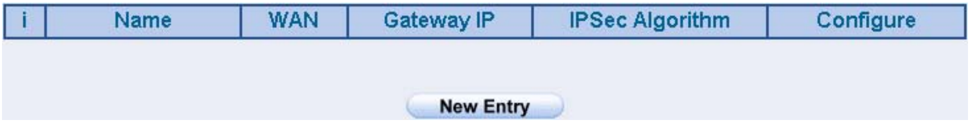


Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the SG-1000 192.168.20.1. Follow the steps below:

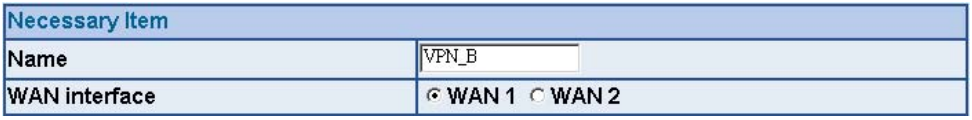
STEP 1. Enter the default IP of Gateway of Company B's SG-1000, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**.



i	Name	WAN	Gateway IP	IPSec Algorithm	Configure

IPSec Autokey Web UI

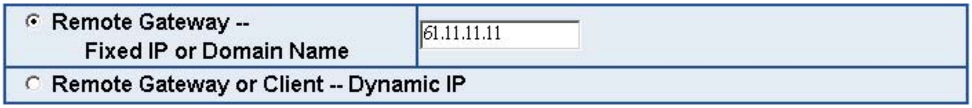
STEP 2. In the list of **IPSec Autokey**, fill in Name with **VPN_B** and select **WAN1** in WAN interface.



Necessary Item	
Name	VPN_B
WAN interface	● WAN 1 ○ WAN 2

IPSec Autokey Name Setting

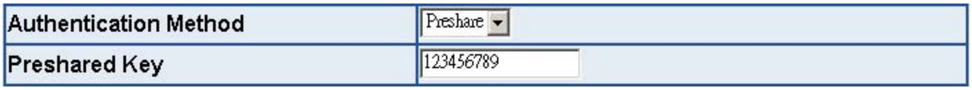
STEP 3. Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.



● Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
○ Remote Gateway or Client -- Dynamic IP	

IPSec To Destination Setting

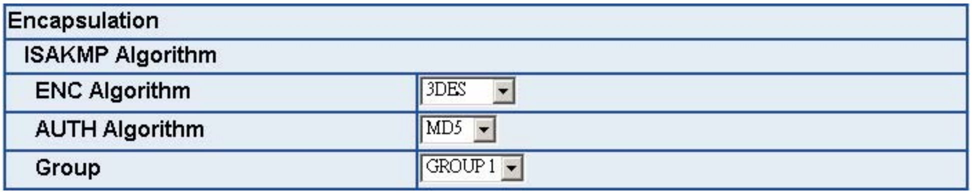
STEP 4. Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits)



Authentication Method	Preshare
Preshared Key	123456789

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.



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

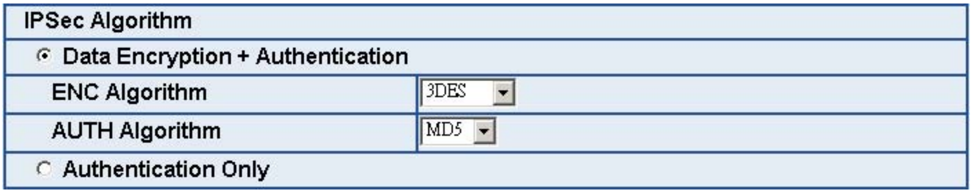
IPSec Encapsulation Setting

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**

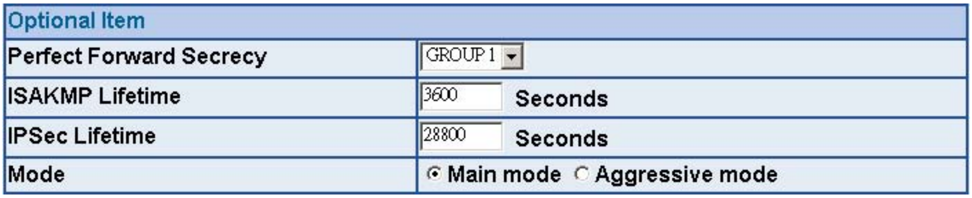
Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission.



IPSec Algorithm	
● Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
○ Authentication Only	

IPSec Algorithm Setting

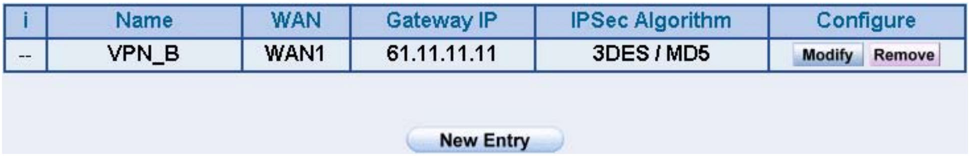
STEP 7. After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**.



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

IPSec Perfect Forward Secrecy Setting

STEP 8. Complete the IPSec Autokey setting.

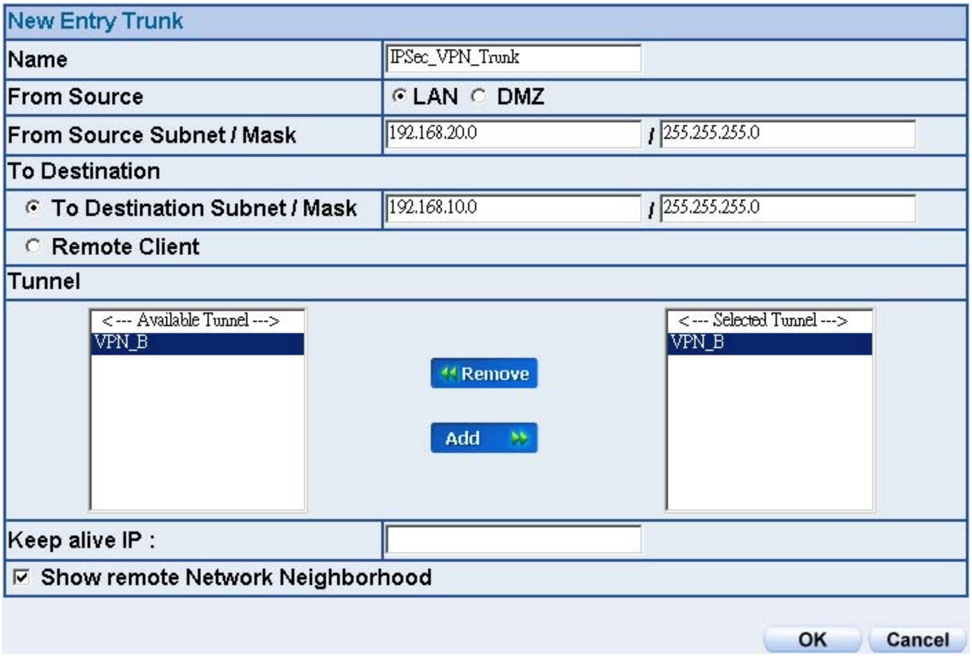


i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	Modify Remove

Complete Company B IPSec Autokey Setting

STEP 9. Enter the following setting in **Trunk** of **VPN** function**:**

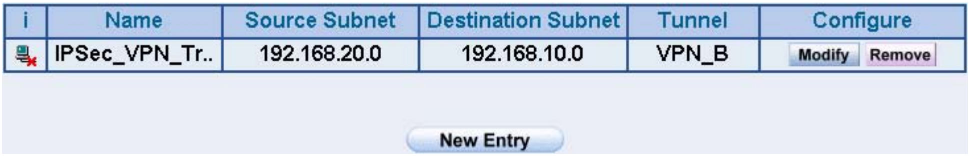
- Enter a specific Trunk **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **Tunnel:** Add VPN_B.
- Select **Show remote Network Neighborhood**.
- Click **OK**.



New Entry Trunk

Name	IPSec_VPN_Trunk
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0
To Destination	
● To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Client	
Tunnel	
<--- Available Tunnel ---> VPN_B	<--- Selected Tunnel ---> VPN_B
Keep alive IP :	
☑ Show remote Network Neighborhood	

New Entry Trunk Setting

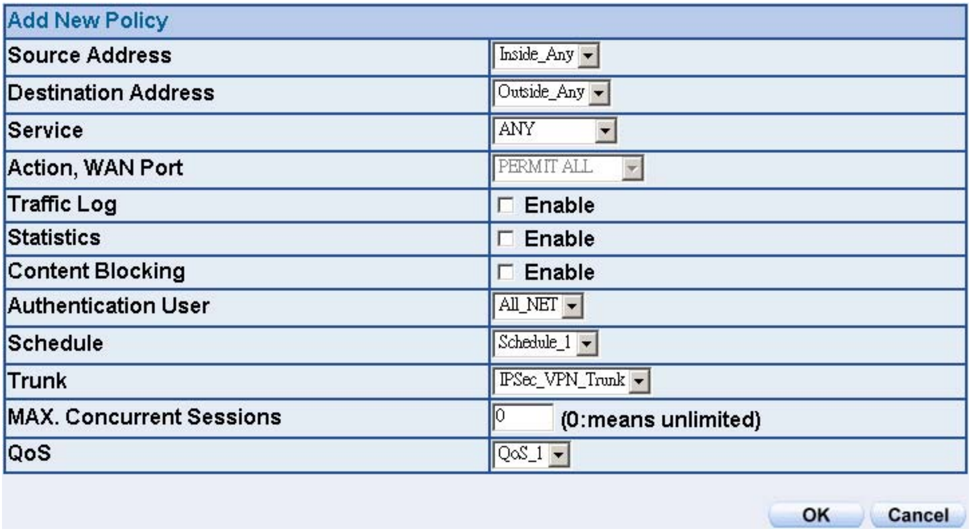


i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr..	192.168.20.0	192.168.10.0	VPN_B	Modify Remove

Complete New Entry Trunk Setting

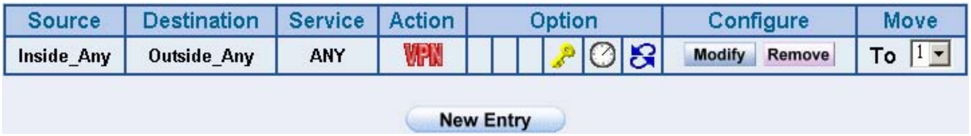
STEP 10. Enter the following setting in **Outgoing Policy:**

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	All_NET
Schedule	Schedule_1
Trunk	IPSec_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

Setting the VPN Trunk Outgoing Policy

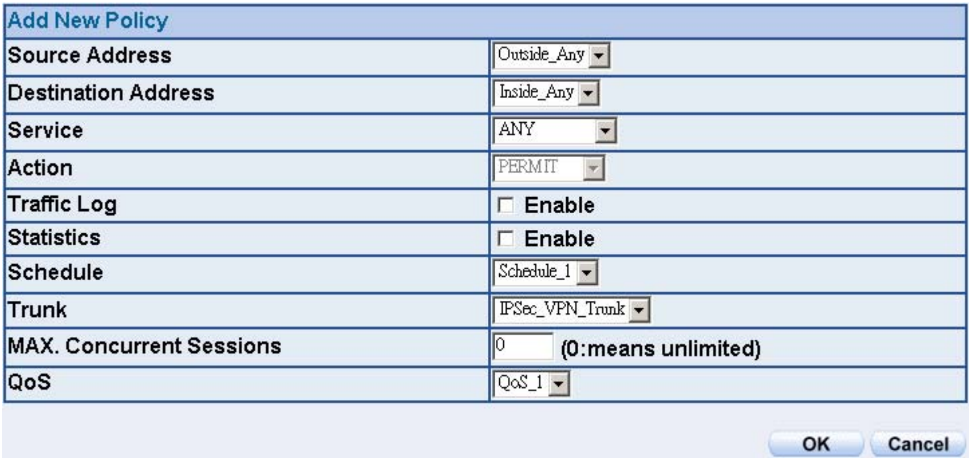


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Outgoing Policy Setting

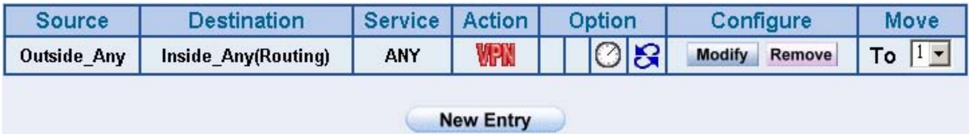
STEP 11. Enter the following setting in **Incoming Policy:**

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	Schedule_1
Trunk	IPSec_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

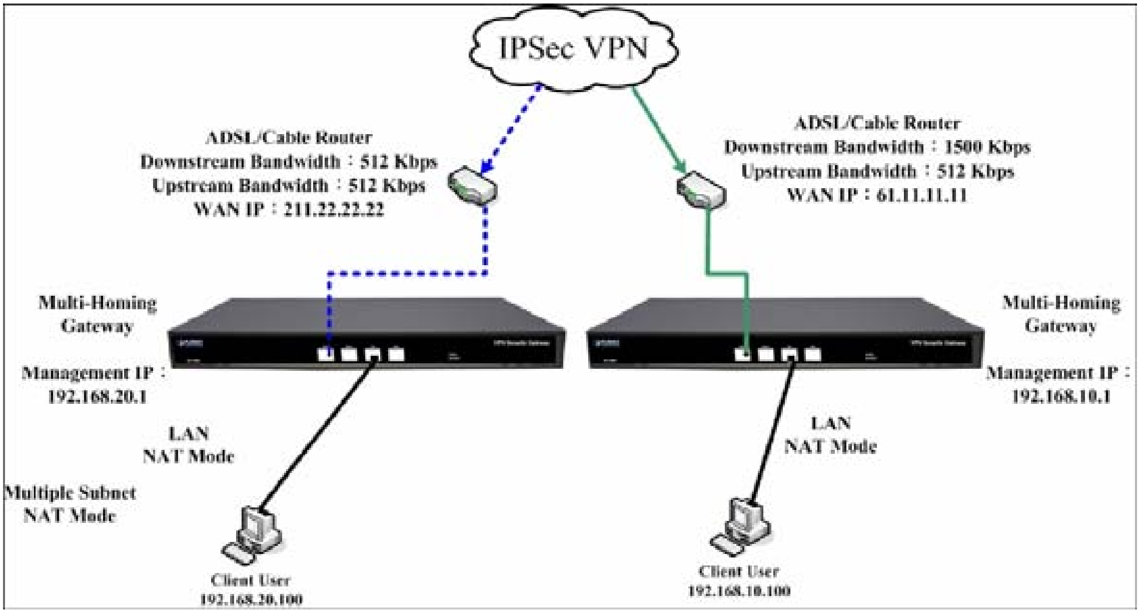
Setting the VPN Trunk Incoming Policy



Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	◷ ⟳	Modify Remove	To 1

Complete the VPN Trunk Incoming Policy Setting

STEP 12. Complete IPSec VPN Connection.


IPSec VPN
ADSL/Cable Router
Downstream Bandwidth：512 Kbps
Upstream Bandwidth：512 Kbps
WAN IP：211.22.22.22
ADSL/Cable Router
Downstream Bandwidth：1500 Kbps
Upstream Bandwidth：512 Kbps
WAN IP：61.11.11.11
Multi-Homing Gateway
Management IP：192.168.20.1
LAN NAT Mode
Multiple Subnet NAT Mode
Client User 192.168.20.100
Multi-Homing Gateway
Management IP：192.168.10.1
LAN NAT Mode
Client User 192.168.10.100

IPSec VPN Connection Deployment

Setting PPTP VPN connection between two SG-1000

Preparation

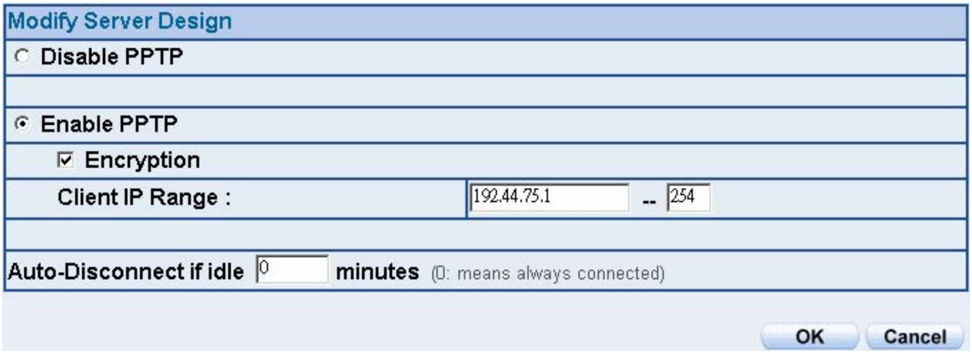
Company A **WAN IP: 61.11.11.11**
LAN IP: 192.168.10.X
Company B **WAN IP: 211.22.22.22**
LAN IP: 192.168.20.X

This example takes two SG-1000 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 SG-1000 192.168.10.1. Follow the steps below:

STEP 1. Enter **PPTP Server** of **VPN** function in the SG-1000 of Company A. Select **Modify** and enable PPTP Server:

- Select **Encryption**.
- **Client IP Range**: Enter 192.44.75.1-254.
- Idle Time: Enter 0.



Modify Server Design

○ Disable PPTP

● Enable PPTP

☑ Encryption

Client IP Range : 192.44.75.1 -- 254

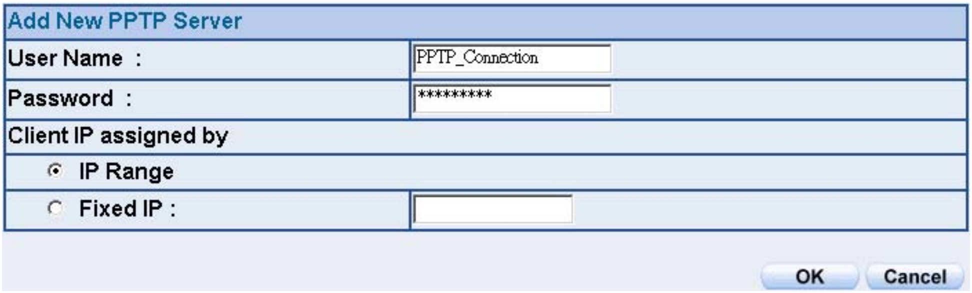
Auto-Disconnect if idle 0 minutes (0: means always connected)

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 SG-1000 of Company A:

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



Add New PPTP Server

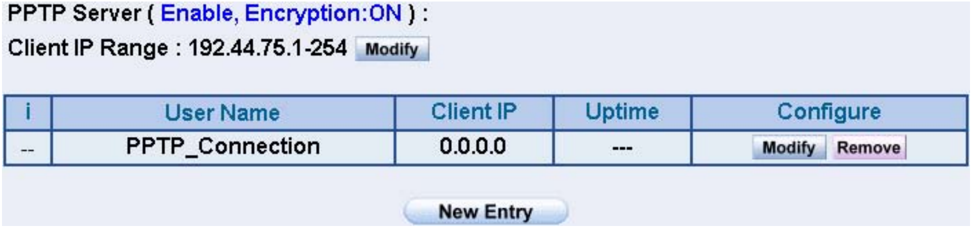
User Name :	PPTP_Connection
Password :	*********

Client IP assigned by

● IP Range

○ Fixed IP :

PPTP VPN Server Setting



PPTP Server (Enable, Encryption:ON) :

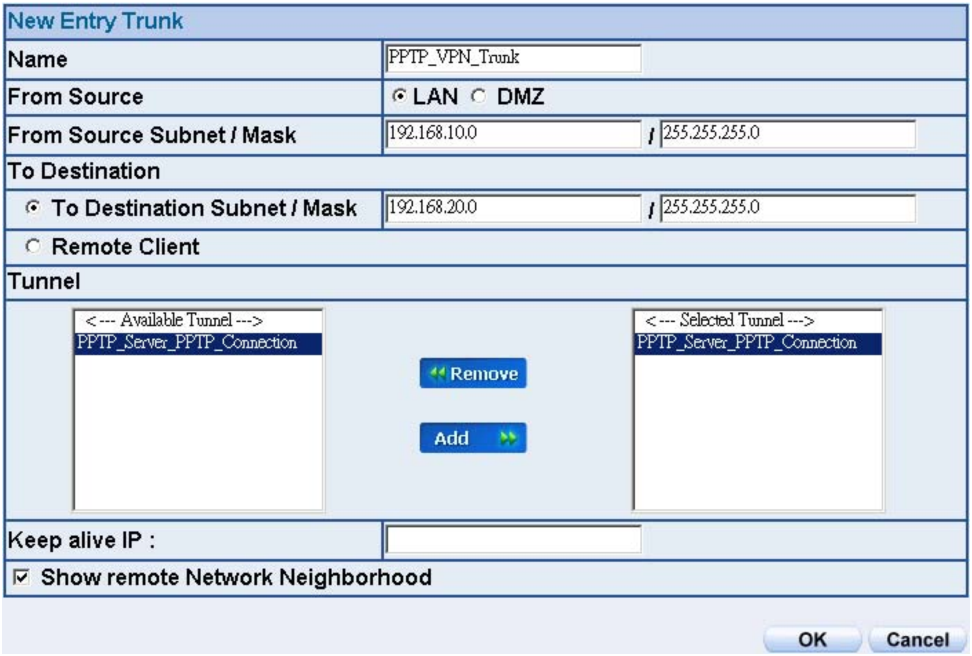
Client IP Range : 192.44.75.1-254 Modify

i	User Name	Client IP	Uptime	Configure
--	PPTP_Connection	0.0.0.0	---	Modify Remove

Complete PPTP VPN Server Setting

STEP 3. Enter the following setting in **Trunk** of **VPN** function**:**

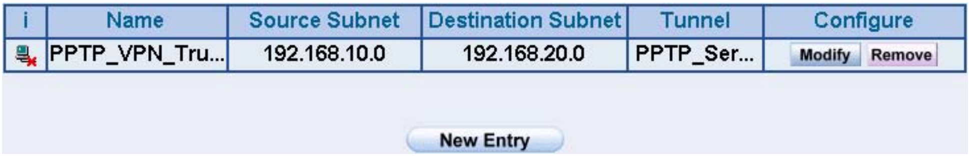
- Enter a specific Trunk **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **Tunnel:** Add PPTP_Server_PPTP_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.



New Entry Trunk

Name	PPTP_VPN_Trunk
From Source	● LAN ○ DMZ
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
○ Remote Client	
Tunnel	
<--- Available Tunnel ---> PPTP_Server_PPTP_Connection	<--- Selected Tunnel ---> PPTP_Server_PPTP_Connection
Keep alive IP :	
☑ Show remote Network Neighborhood	

New Entry Trunk Setting

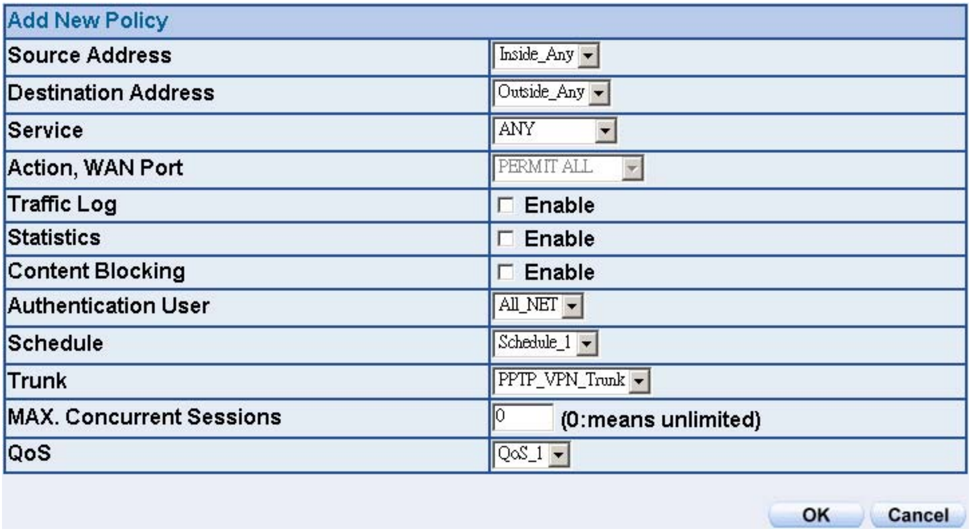


i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	PPTP_VPN_Tru...	192.168.10.0	192.168.20.0	PPTP_Ser...	Modify Remove

Complete New Entry Trunk Setting

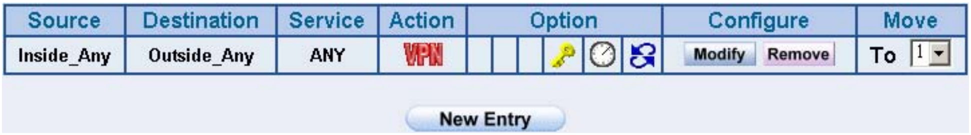
STEP 4. Enter the following setting in **Outgoing Policy:**

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select PPTP_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	All_NET
Schedule	Schedule_1
Trunk	PPTP_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

Setting the VPN Trunk Outgoing Policy

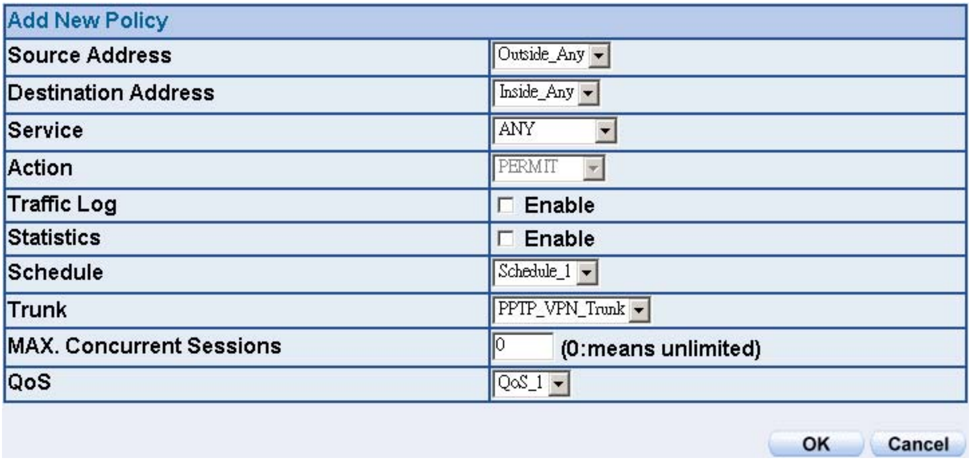


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Outgoing Policy Setting

STEP 5. Enter the following setting in **Incoming Policy:**

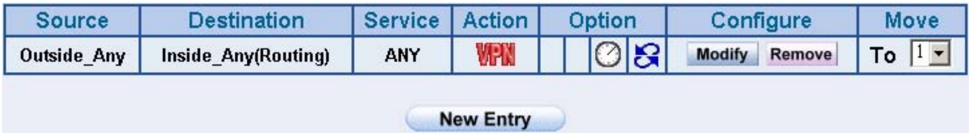
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select PPTP_VPN_Trunk.
- Click **OK**.



Add New Policy

Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Action	PERMIT ▾
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	Schedule_1 ▾
Trunk	PPTP_VPN_Trunk ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1 ▾

Setting the VPN Trunk Incoming Policy



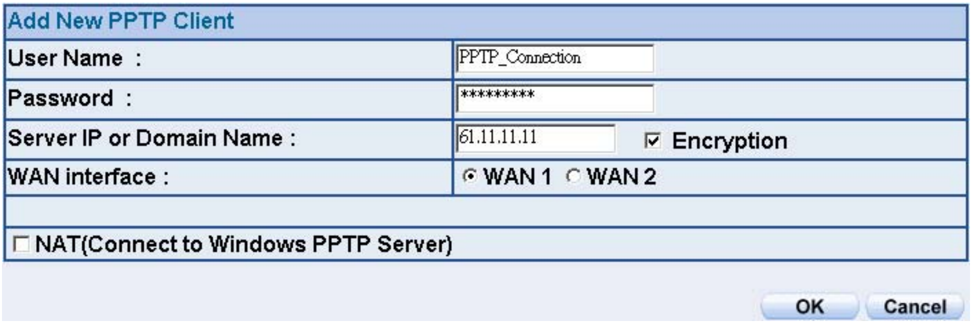
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	◷ ⟳	Modify Remove	To 1 ▾

Complete the VPN Trunk Incoming Policy Setting

The Default Gateway of Company B is the LAN IP of the SG-1000 192.168.20.1. Follow the steps below:

STEP 1. Add the following settings in **PPTP Client** of **VPN** function in the SG-1000 of Company B:

- Click **New Entry** Button.
- **User Name**: Enter PPTP_Connection.
- **Password**: Enter123456789.
- **Server IP or Domain Name**: Enter 61.11.11.11.
- Select **Encryption**.
- **WAN Interface**: Select WAN1.
- Click **OK**.

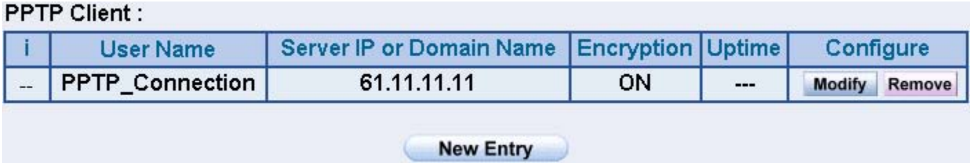


Add New PPTP Client

User Name :	PPTP_Connection
Password :	*********
Server IP or Domain Name :	61.11.11.11 ☑ Encryption
WAN interface :	● WAN 1 ○ WAN 2

□ NAT(Connect to Windows PPTP Server)

PPTP VPN Client Setting



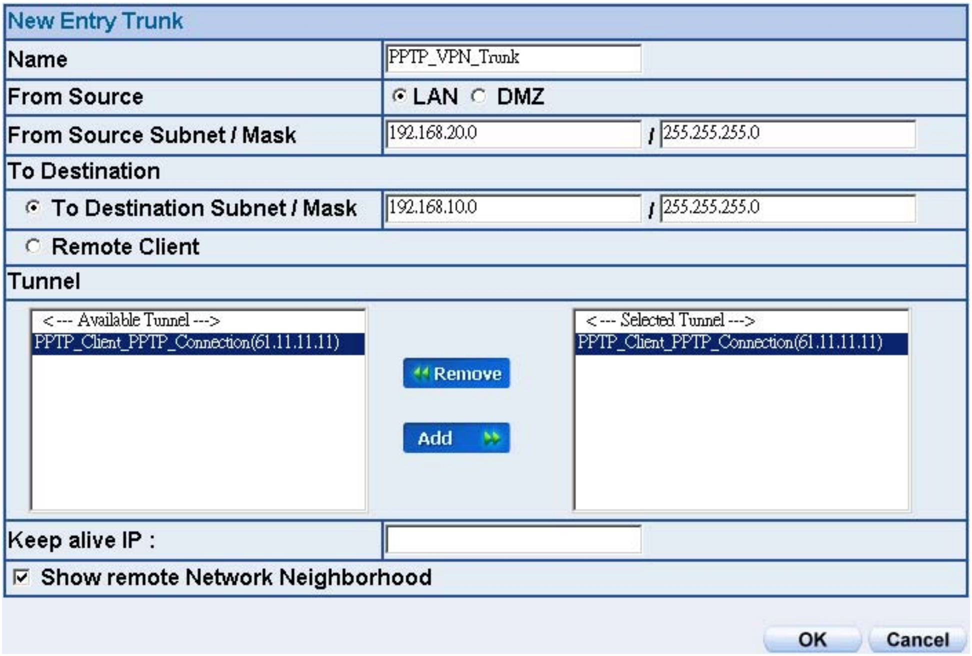
PPTP Client :

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

Complete PPTP VPN Client Setting

STEP 2. Enter the following setting in **Trunk** of **VPN** function**:**

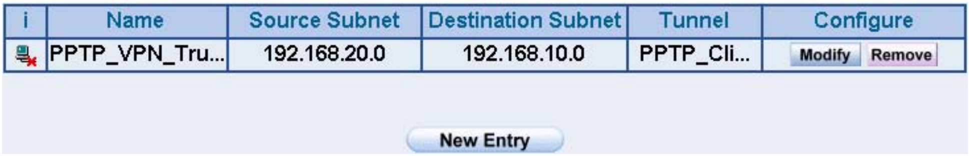
- Enter a specific Trunk **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **Tunnel:** Add PPTP_Client_PPTP_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.



New Entry Trunk

Name	PPTP_VPN_Trunk
From Source	● LAN ○ DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0
To Destination	
● To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
○ Remote Client	
Tunnel	
<--- Available Tunnel ---> PPTP_Client_PPTP_Connection(61.11.11.11)	<--- Selected Tunnel ---> PPTP_Client_PPTP_Connection(61.11.11.11)
Keep alive IP :	
☑ Show remote Network Neighborhood	

New Entry Trunk Setting

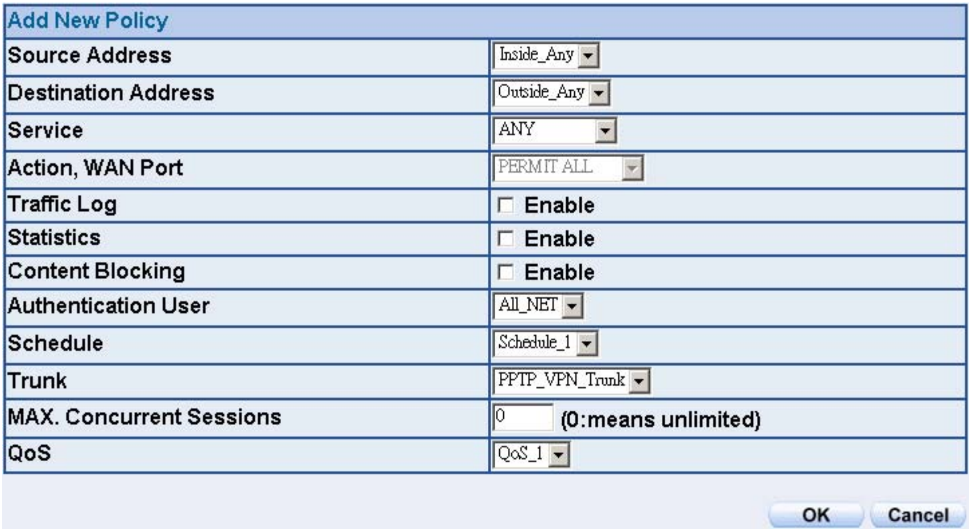


i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	PPTP_VPN_Tru...	192.168.20.0	192.168.10.0	PPTP_Cli...	Modify Remove

Complete New Entry Trunk Setting

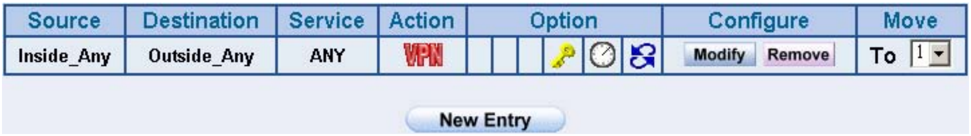
STEP 3. Enter the following setting in **Outgoing Policy:**

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select PPTP_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	All_NET
Schedule	Schedule_1
Trunk	PPTP_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

Setting the VPN Trunk Outgoing Policy

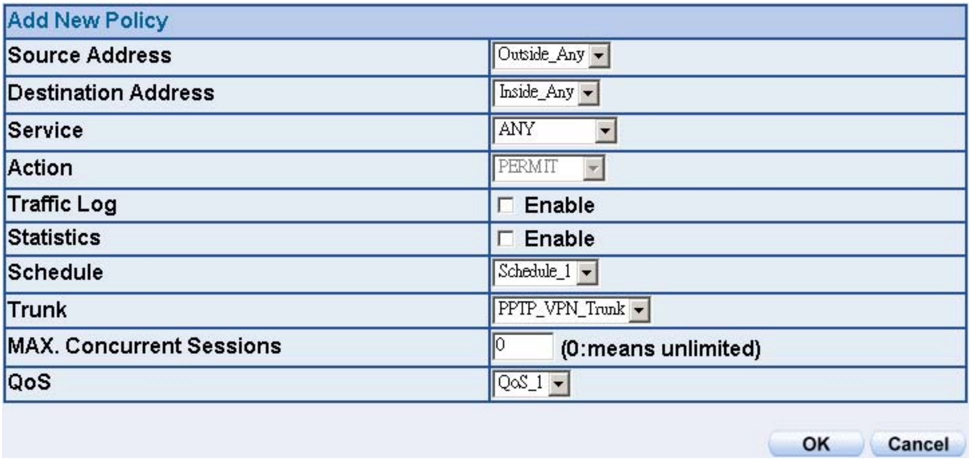


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Outgoing Policy Setting

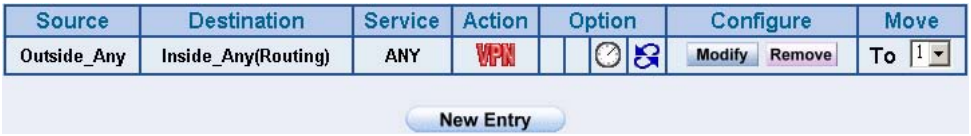
STEP 4. Enter the following setting in **Incoming Policy:**

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Trunk:** Select PPTP_VPN_Trunk.
- Click **OK**.



Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	Schedule_1
Trunk	PPTP_VPN_Trunk
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	QoS_1

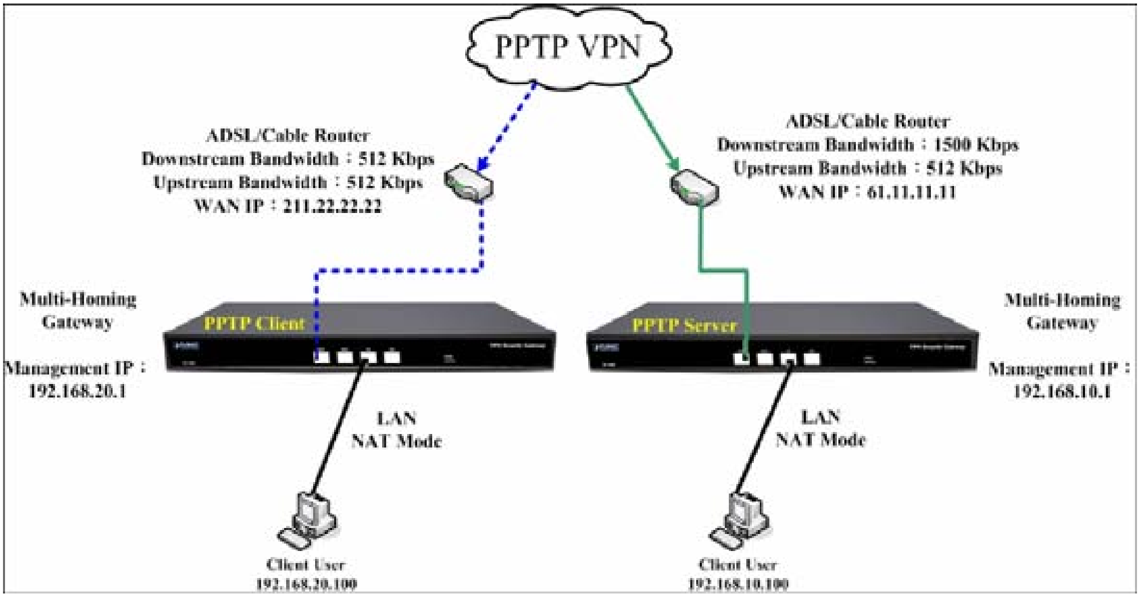
Setting the VPN Trunk Incoming Policy



Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove	To 1

Complete the VPN Trunk Incoming Policy Setting

STEP 5. Complete PPTP VPN Connection.



PPTP VPN Connection Deployment

Chapter 13

Policy

Every packet has to be detected if it corresponds with Policy or not when it passes the SG-1000. When the conditions correspond with certain policy, it will pass the SG-1000 by the setting of Policy without being detected by other policy. But if the packet cannot correspond with any Policy, the packet will be intercepted.

The parameter of the policy includes Source Address, Destination Address, Service, Action, WAN Port, Traffic Log, Statistics, Content Blocking, Anti-Virus, Authentication User, Schedule, Alarm Threshold, Trunk, Max. Concurrent Sessions, and QoS. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the SG-1000.

How to use Policy?

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

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

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

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

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

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

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

All the packets that go through SG-1000 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 SG-1000'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 SG-1000 (See the chart and illustration below)

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

Option:

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

Chart	Name	Illustration
👁	Traffic Log	Enable traffic log
📊	Statistics	Enable traffic statistics
🔑	Authentication User	Enable Authentication User
🕒	Schedule	Enable the policy to automatically execute the function in a certain time
⛔	Content Blocking	Enable Content Blocking
🔄	QoS	Enable QoS

Traffic Log:

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

Statistics:

- Chart of the traffic that go through policy

Content Blocking:

- To restrict the packets that passes through the policy

Authentication-User:

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

Schedule:

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

MAX. Concurrent Sessions:

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

QoS:

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

Move:

- Every packet that passes the SG-1000 is detected from the front policy to the last one. So it can modify the priority of the policy from the selection.

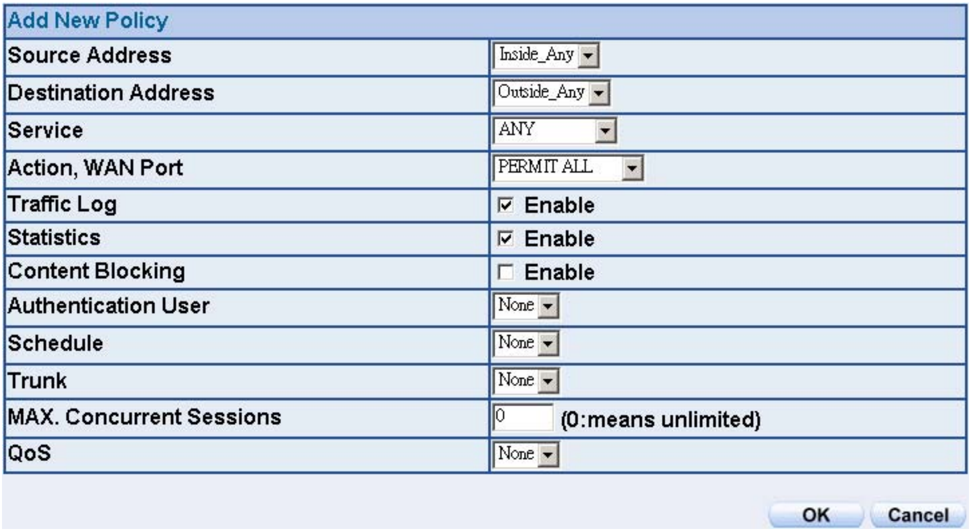
We set up six Policy examples in this chapter:

No.	Suitable Situation	Example
Ex1	**Outgoing**	Set up the policy that can monitor the internal users. (Take Logging, Statistics, Alarm Threshold for example)
Ex2	**Outgoing**	Forbid the users to access to specific network. (Take specific WAN IP and Content Blocking for example)
Ex3	**Outgoing**	Only allow the users who pass Authentication to access to Internet in particular time.
Ex4	**Incoming**	The external user control the internal PC through remote control software (Take pcAnywhere for example)
Ex5	**WAN to DMZ** **DMZ to WAN** **LAN to DMZ**	Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode

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

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

- Click **New Entry**
- Select **Logging**
- Select **Statistics**
- Click **OK**

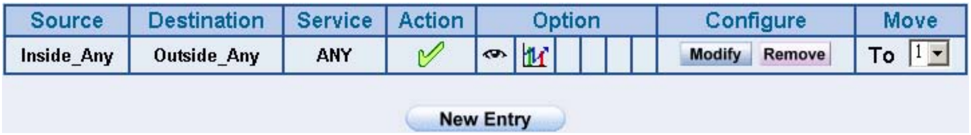


Add New Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	☑ Enable
Statistics	☑ Enable
Content Blocking	□ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Setting the different Policies

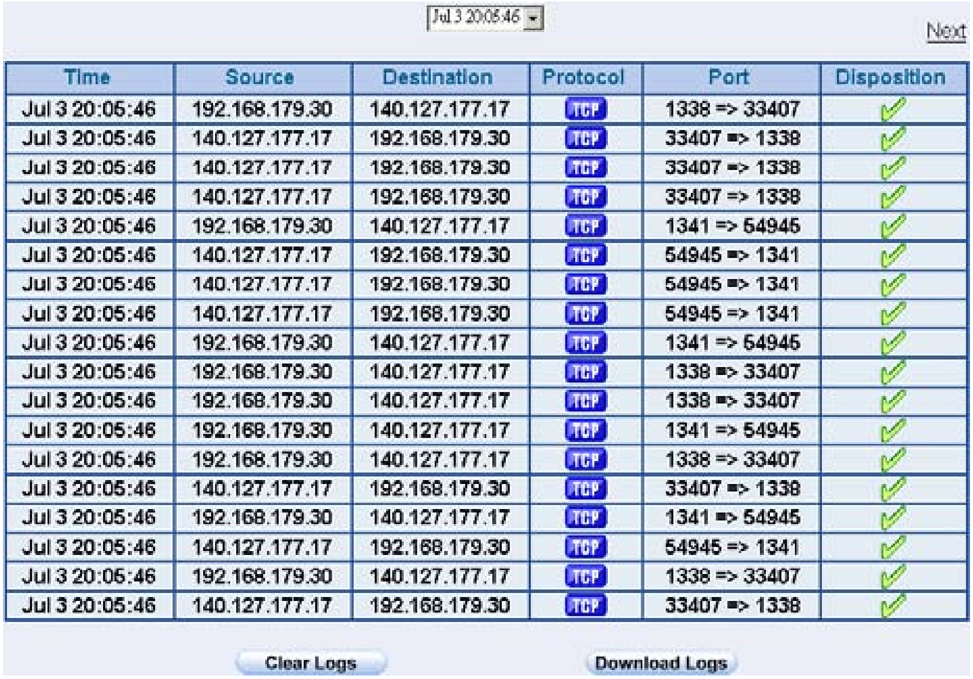
STEP 2．Complete the setting of Logging and Statistics in **Outgoing Policy**:



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

Complete Policy Setting

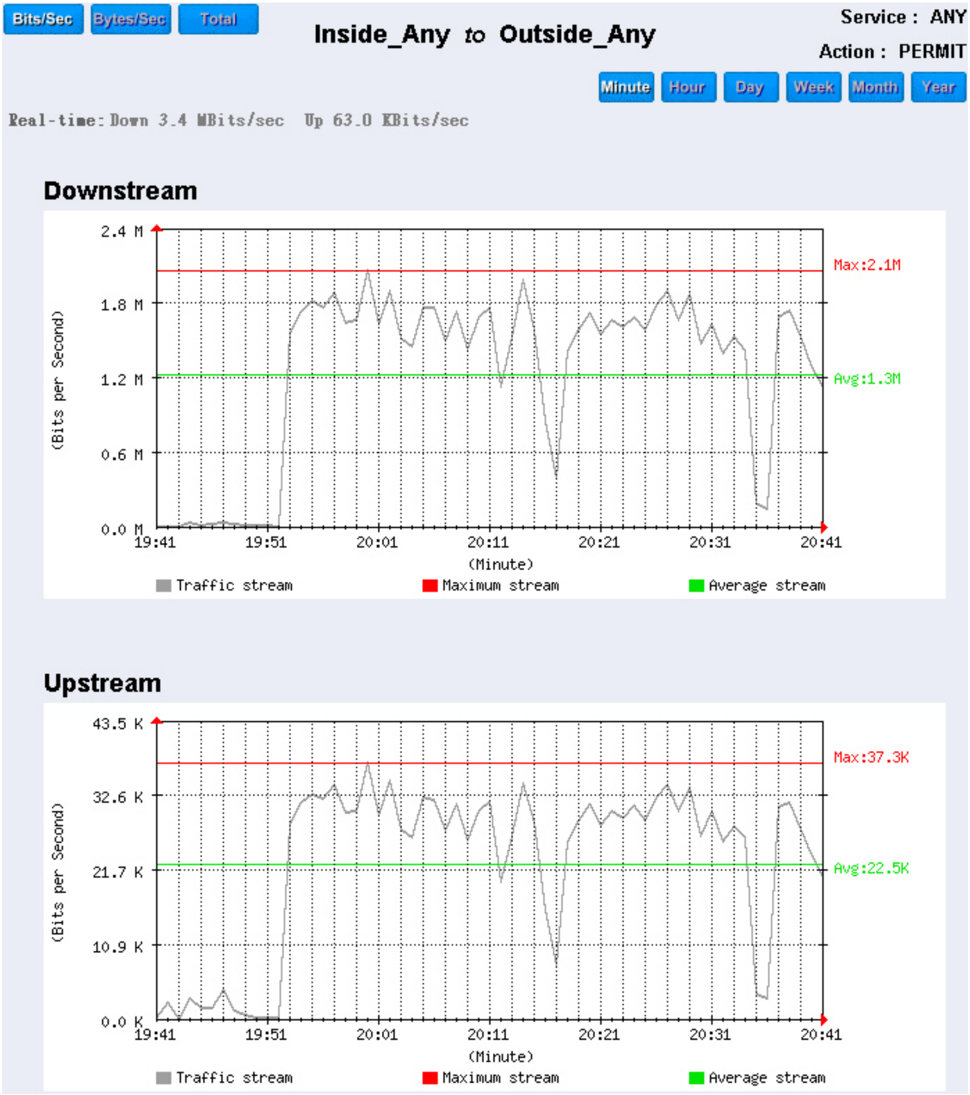
STEP 3．Obtain the information in **Traffic** of **Log** function if you want to monitor all the packets of the SG-1000.



Time	Source	Destination	Protocol	Port	Disposition
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1338 => 33407	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	33407 => 1338	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	33407 => 1338	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	33407 => 1338	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1341 => 54945	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	54945 => 1341	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	54945 => 1341	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	54945 => 1341	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1341 => 54945	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1338 => 33407	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1338 => 33407	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1341 => 54945	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1338 => 33407	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	33407 => 1338	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1341 => 54945	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	54945 => 1341	✓
Jul 3 20:05:46	192.168.179.30	140.127.177.17	TCP	1338 => 33407	✓
Jul 3 20:05:46	140.127.177.17	192.168.179.30	TCP	33407 => 1338	✓

Traffic Log Monitor Web UI

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



Inside_Any *to* Outside_Any

Service : ANY

Action : PERMIT

Real-time: Down 3.4 MBits/sec Up 63.0 KBits/sec

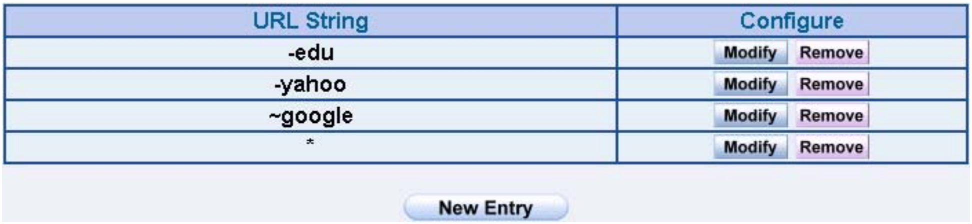
Downstream

Upstream

Statistics Web UI

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

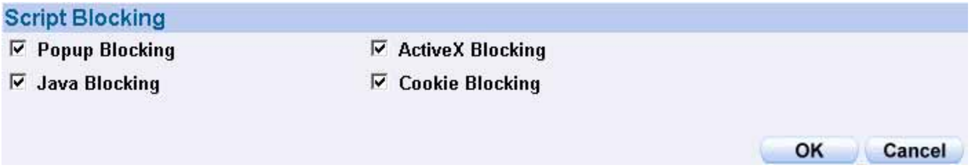
STEP 1 . Enter the following setting in **URL Blocking, Script Blocking, P2P Blocking, IM Blocking,** and **Download Blocking** in **Content Blocking** function:



URL String	Configure
-edu	Modify Remove
-yahoo	Modify Remove
~google	Modify Remove
*	Modify Remove

New Entry

URL Blocking Setting



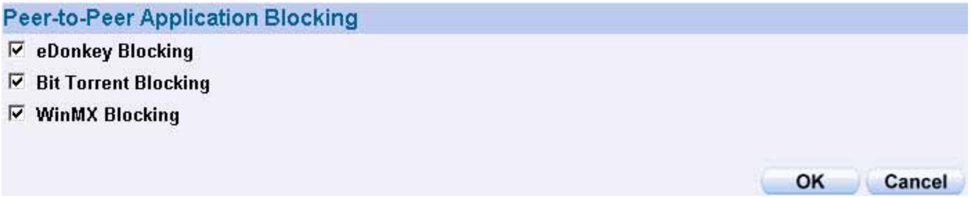
Script Blocking

☑ Popup Blocking ☑ ActiveX Blocking

☑ Java Blocking ☑ Cookie Blocking

OK Cancel

Script Blocking Setting



Peer-to-Peer Application Blocking

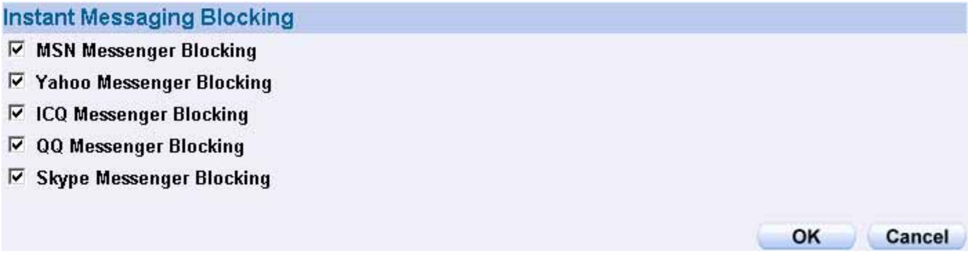
☑ eDonkey Blocking

☑ Bit Torrent Blocking

☑ WinMX Blocking

OK Cancel

P2P Blocking Setting



Instant Messaging Blocking

☑ MSN Messenger Blocking

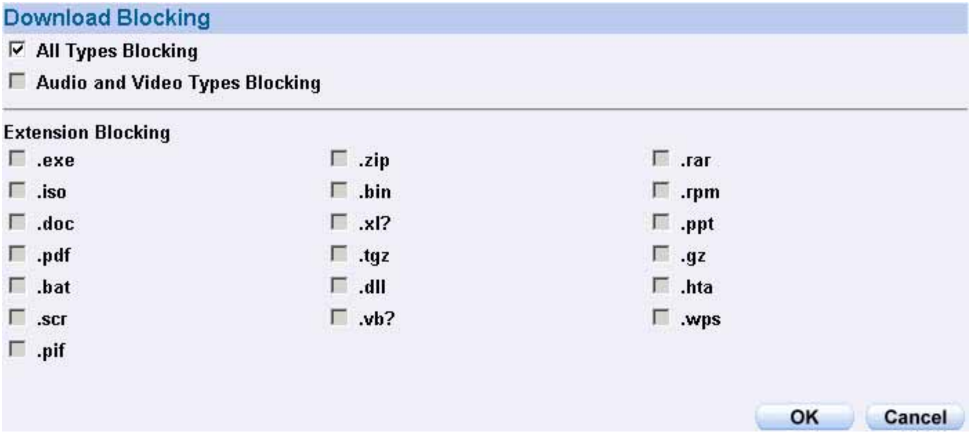
☑ Yahoo Messenger Blocking

☑ ICQ Messenger Blocking

☑ QQ Messenger Blocking

☑ Skype Messenger Blocking

IM Blocking Setting



Download Blocking

☑ All Types Blocking

□ Audio and Video Types Blocking

Extension Blocking

□ .exe
□ .iso
□ .doc
□ .pdf
□ .bat
□ .scr
□ .pif
□ .zip
□ .bin
□ .xl?
□ .tgz
□ .dll
□ .vb?
□ .rar
□ .rpm
□ .ppt
□ .gz
□ .hta
□ .wps

Download Blocking Setting

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

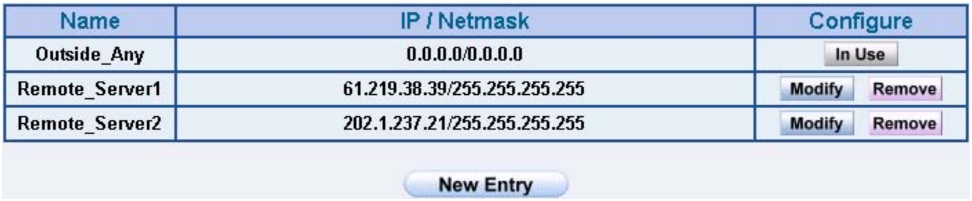
2. Script Blocking can restrict the Internal Users to access to Script file of Website. (Java, Cookies…etc.)

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

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

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

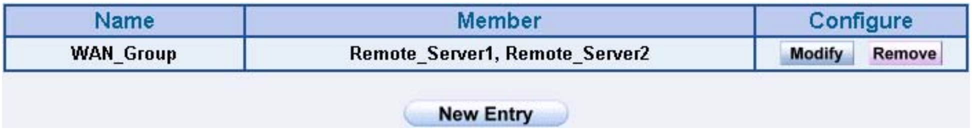
STEP 2．Enter as following in **WAN** and **WAN Group** of **Address** function:



Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	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

Setting the WAN IP that going to block



Name	Member	Configure
WAN_Group	Remote_Server1, Remote_Server2	Modify Remove

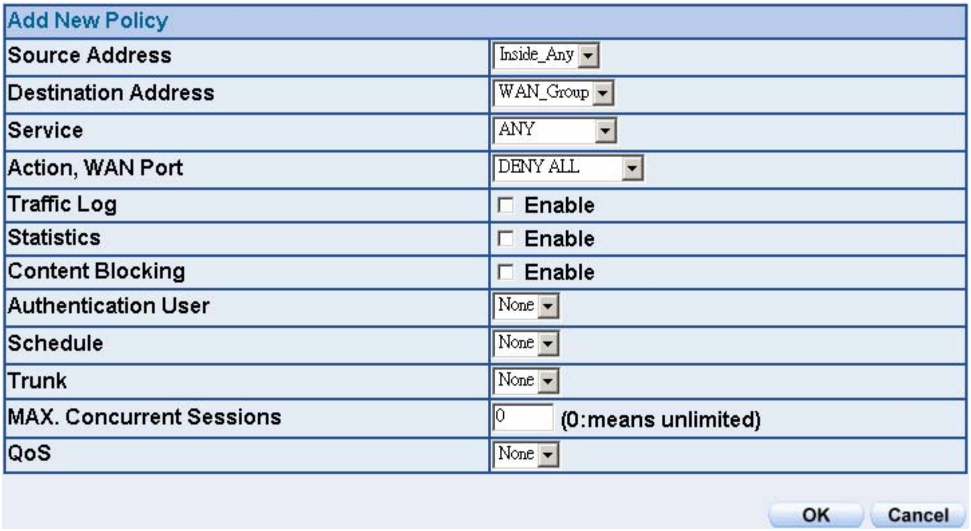
New Entry

WAN Address Group

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

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

- Click **New Entry**
- **Destination Address:** Select WAN_Group that set by **STEP 2**. (Blocking by IP)
- **Action, WAN Port:** Select **Deny**
- Click **OK**

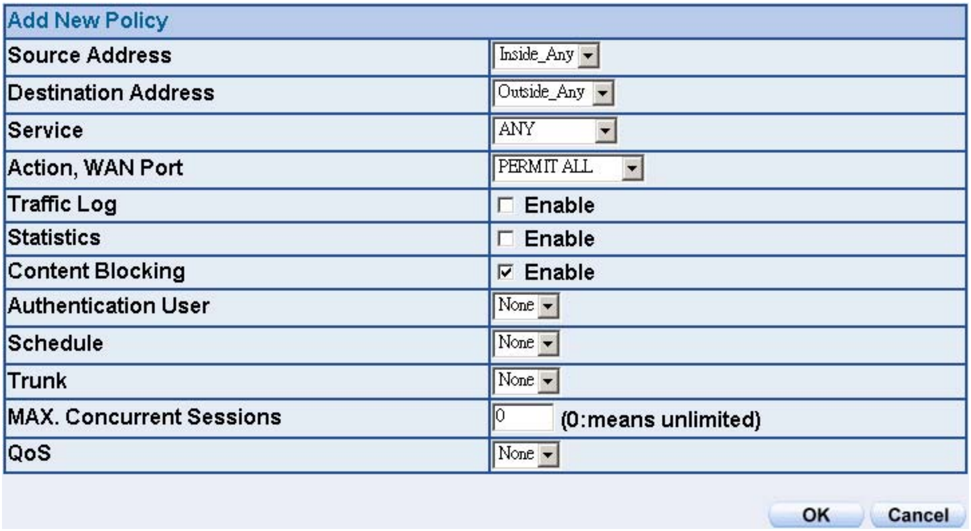


Add New Policy	
Source Address	Inside_Any
Destination Address	WAN_Group
Service	ANY
Action, WAN Port	DENY ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Setting Blocking Policy

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

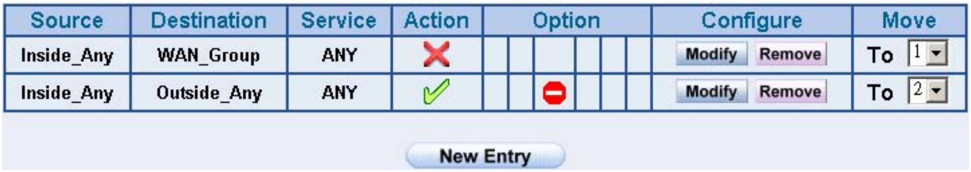
- Click **New Entry**
- Select **Content Blocking**
- Click **OK**



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	☑ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Setting Content Blocking Policy

STEP 5 . Complete the setting of forbidding the users to access to specific network.



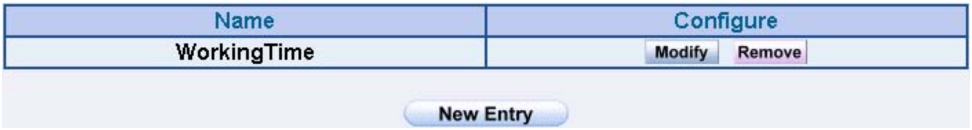
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	WAN_Group	ANY	✗		Modify Remove	To 1
Inside_Any	Outside_Any	ANY	✓	⛔	Modify Remove	To 2

Complete Policy Setting

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

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

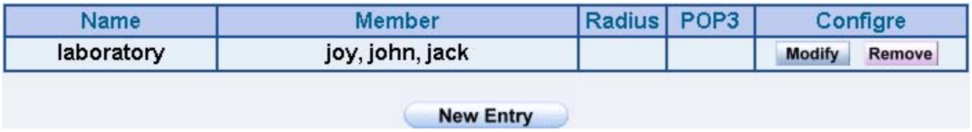
STEP 1 . Enter the following in **Schedule** function:



Name	Configure
WorkingTime	Modify Remove

Add New Schedule

STEP 2 . Enter the following in **Auth User** and **Auth User Group** in **Authentication** function**:**



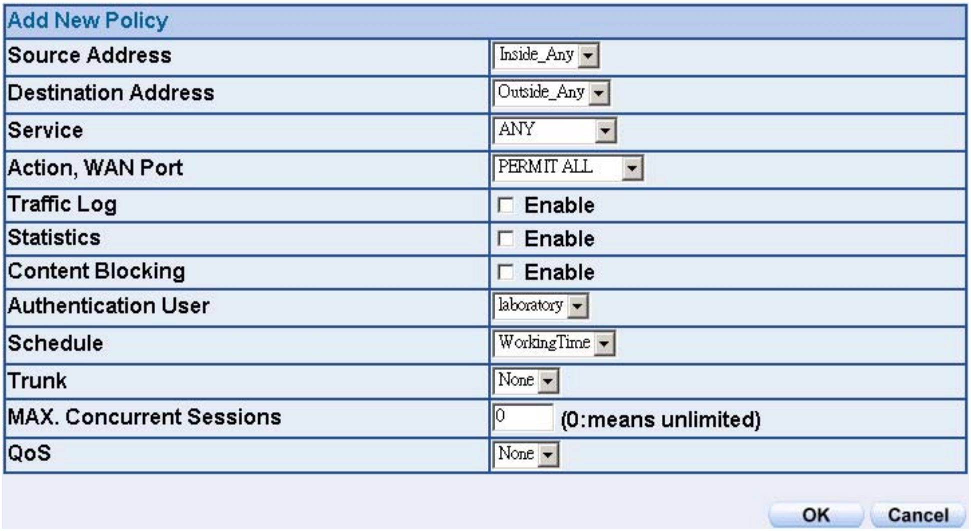
Name	Member	Radius	POP3	Configre
laboratory	joy, john, jack			Modify Remove

Setting Auth User Group

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

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

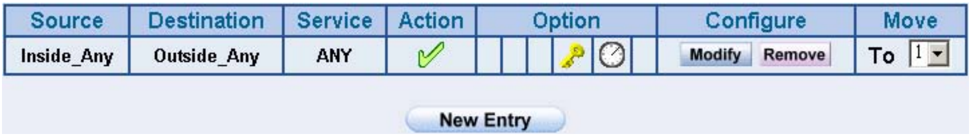
- Click **New Entry**
- **Authentication User:** Select laboratory
- **Schedule:** Select WorkingTime
- Click **OK**



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	□ Enable
Statistics	□ Enable
Content Blocking	□ Enable
Authentication User	laboratory ▾
Schedule	WorkingTime ▾
Trunk	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None ▾

Setting a Policy of Authentication and Schedule

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



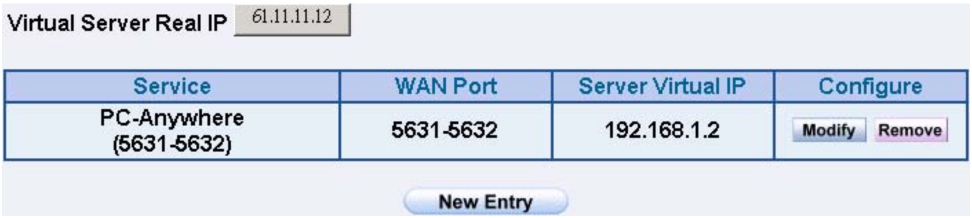
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓	🔑 ⏲	Modify Remove	To 1 ▾

Complete Policy Setting

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

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

STEP 2． Enter the following setting in **Virtual Server1** of **Virtual Server** function**:**



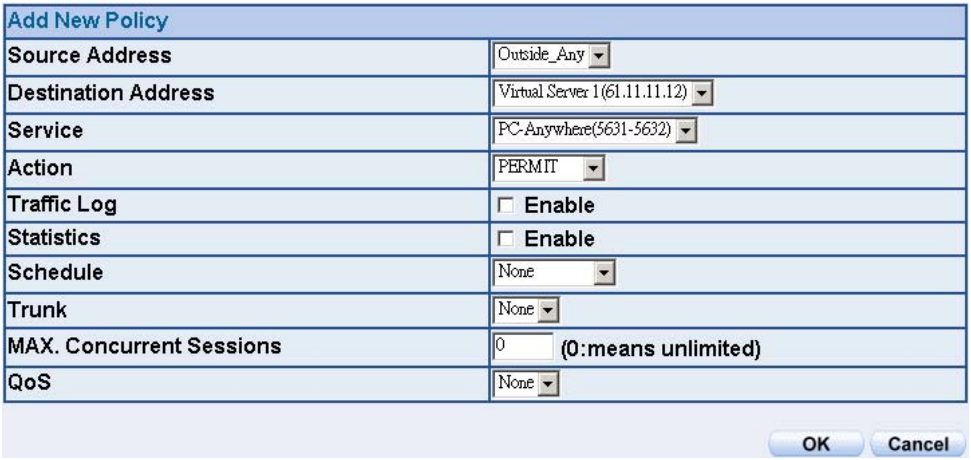
Virtual Server Real IP 61.11.11.12

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

Setting Virtual Server

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

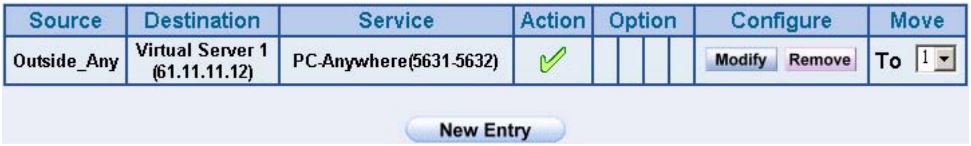
- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select PC-Anywhere (5631-5632)
- Click **OK**



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
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

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.



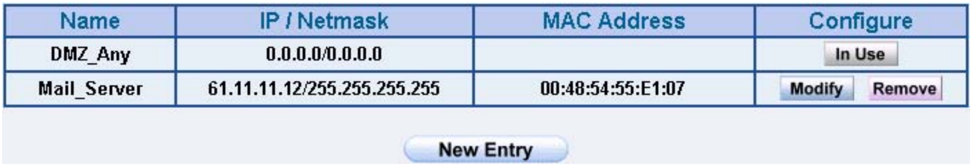
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1 (61.11.11.12)	PC-Anywhere(5631-5632)	✓		Modify Remove	To 1

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.

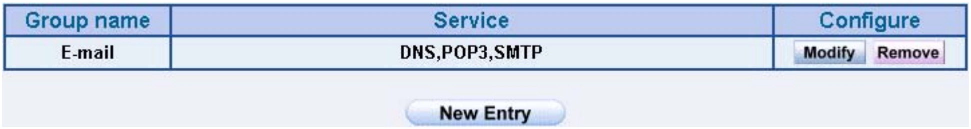
STEP 2 . Add the following setting in **DMZ** of **Address** function**:**



Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Mail_Server	61.11.11.12/255.255.255.255	00:48:54:55:E1:07	Modify Remove

The Mail Server's IP Address Corresponds to Name Setting in Address Book of Mail Server

STEP 3 . Add the following setting in **Group** of **Service** function:

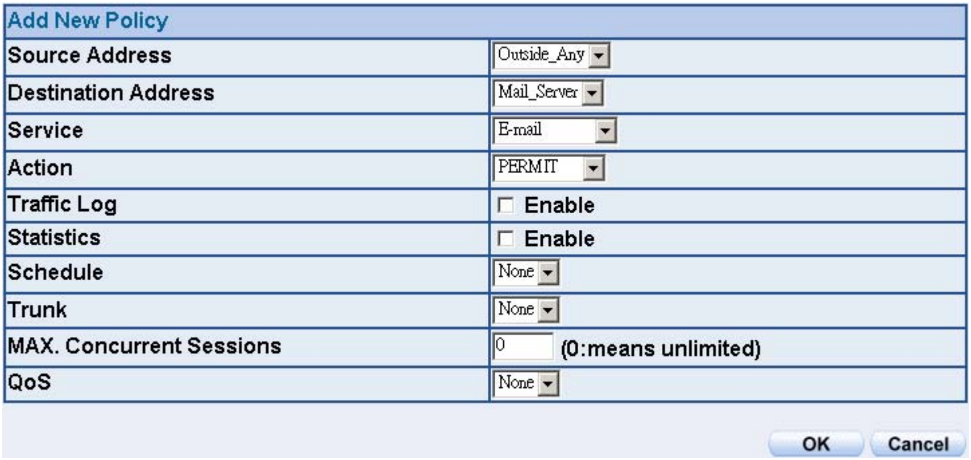


Group name	Service	Configure
E-mail	DNS,POP3,SMTP	Modify Remove

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

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

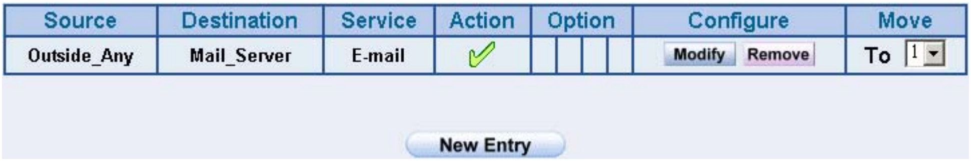
- Click **New Entry**
- **Destination Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK**



Add New Policy	
Source Address	Outside_Any
Destination Address	Mail_Server
Service	E-mail
Action	PERMIT
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Setting a Policy to access Mail Service by WAN to DMZ

STEP 5 . Complete the policy to access mail service by **WAN to DMZ**.

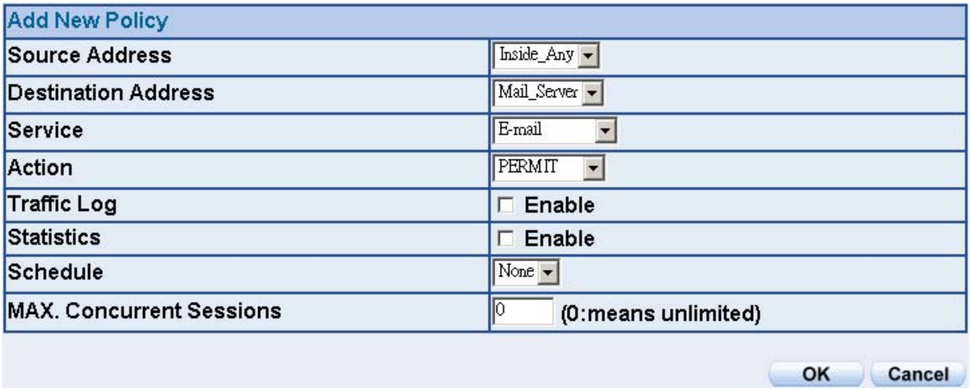


Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mail_Server	E-mail	✓		Modify Remove	To 1

Complete the Policy to access Mail Service by WAN to DMZ

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

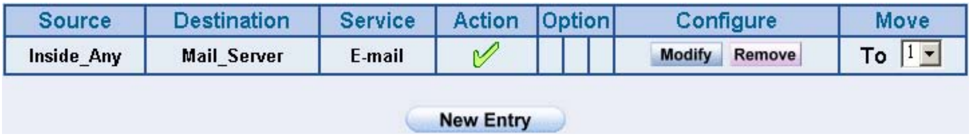
- Click **New Entry**
- **Destination Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK**



Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Mail_Server ▾
Service	E-mail ▾
Action	PERMIT ▾
Traffic Log	□ Enable
Statistics	□ Enable
Schedule	None ▾
MAX. Concurrent Sessions	0 (0:means unlimited)

Setting a Policy to access Mail Service by LAN to DMZ

STEP 7．Complete the policy to access mail service by **LAN to DMZ**

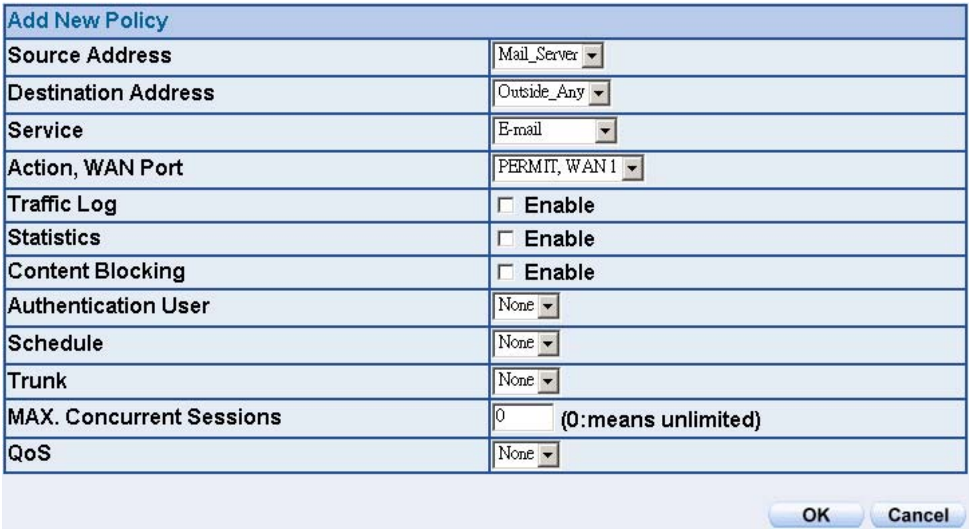


Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	E-mail	✓		Modify Remove	To 1 ▾

Complete the Policy to access Mail Service by LAN to DMZ

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

- Click **New Entry**
- **Source Address:** Select Mail_Server
- **Service:** Select E-mail
- Click **OK**

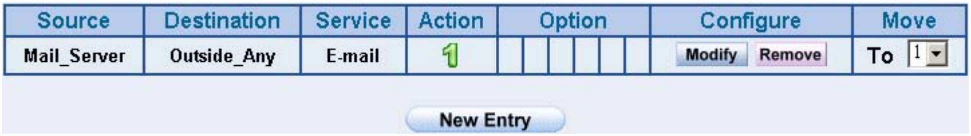


Add New Policy

Source Address	Mail_Server
Destination Address	Outside_Any
Service	E-mail
Action, WAN Port	PERMIT, WAN 1
Traffic Log	☐ Enable
Statistics	☐ Enable
Content Blocking	☐ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Setting the Policy of Mail Service by DMZ to WAN

STEP 9． Complete the policy access to mail service by **DMZ to WAN**.



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

Complete the Policy access to Mail Service by DMZ to WAN

Chapter 14

Web VPN / SSL VPN

As a result of the Internet universal application, the demand which the enterprise security about remote login also grows day by day. The most convenient security solution to user is nothing better than in SSL VPN, the user does not need to install any software or the hardware, and just use standard browser to transmit data through SSL safe encryption agreement.

Define the required fields of VPN:

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.

Define the required fields of Setting:

VPN IP of Client:

- Can set client and SG-1000 establish SSL VPN connection’s authentication account, IP range, encryption algorithm, protocol, server port, and idle time.

SSL VPN IP range can not the same with internal(LAN, Multiple Subnet, DMZ), external(WAN), and PPTP Server’s subnet.

Internal Subnet of Server:

- The client can be allowed to access internal subnet of server.

Define the required fields of Status:

User Name:

- Display authentication account which is used by client.

Real IP:

- Display the real IP which is used by client.

VPN IP:

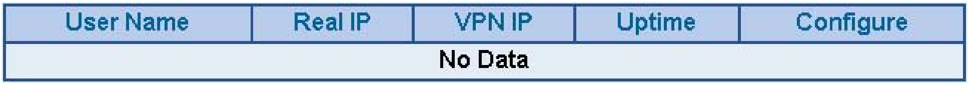
- Display the IP which is distributed to client by SG-1000.

Uptime:

- Display the connection time between Server and Client.

Configure:

- Can disconnect the SSL VPN connection.

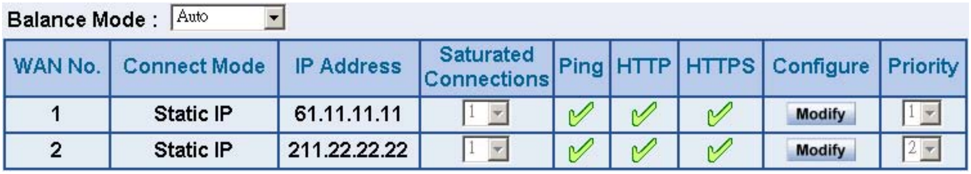


User Name	Real IP	VPN IP	Uptime	Configure
No Data				

Status Web UI

14.1 Setting Web VPN / SSL VPN Connection between External Client and SG-1000

STEP 1. Enable HTTPS in **WAN** of **Interface** function:

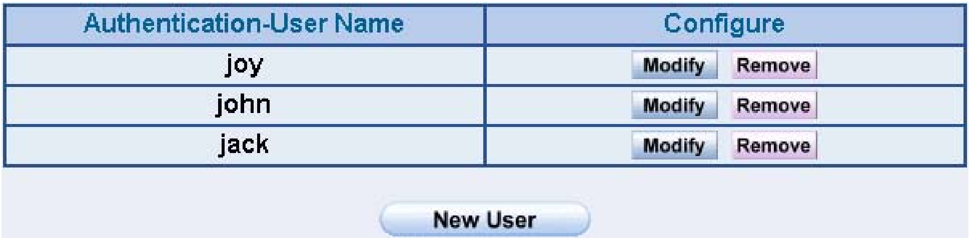


Balance Mode : Auto

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	HTTPS	Configure	Priority
1	Static IP	61.11.11.11	1	✓	✓	✓	Modify	1
2	Static IP	211.22.22.22	1	✓	✓	✓	Modify	2

WAN Interface Setting

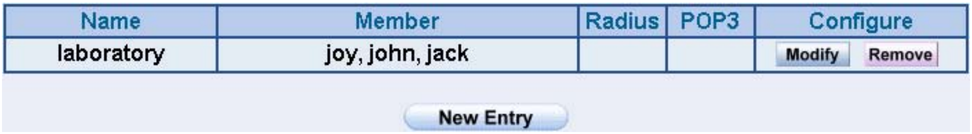
STEP 2. Enter the following setting in **Auth User** of **Authentication**:



Authentication-User Name	Configure
joy	Modify Remove
john	Modify Remove
jack	Modify Remove

Auth User Setting

STEP 3. Enter the following setting in **Auth Group** of **Authentication**:

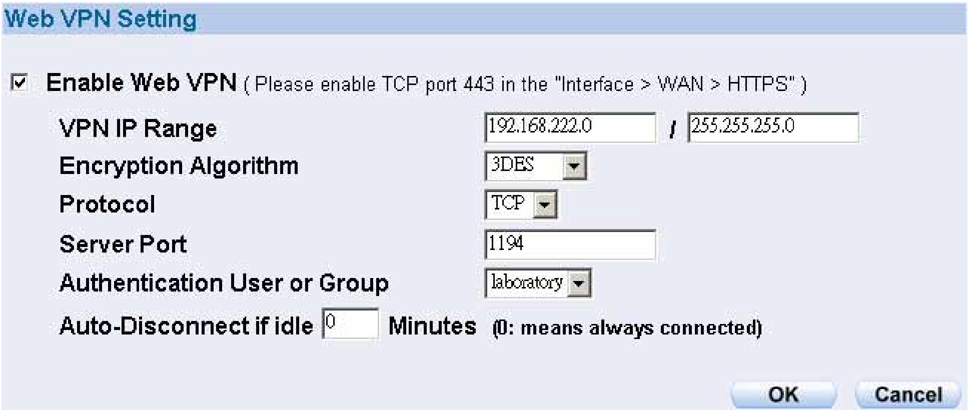


Name	Member	Radius	POP3	Configure
laboratory	joy, john, jack			Modify Remove

Auth Group Setting

STEP 4. Enter the following setting in **Setting** of **Web VPN / SSL VPN**:

- Click **Modify**.
- **Enable Web VPN** function.
- **VPN IP Range**: Enter 192.168.222.0 / 255.255.255.0.
- **Encryption Algorithm**: Select 3DES.
- **Protocol**: Select TCP.
- **Server Port**: Enter default setting1194.
- **Authentication User or Group**: Select laboratory.
- Idle time: Enter 0.
- Click **OK**.
- It will add LAN subnet automatically to be allowed to access by client.



Web VPN Setting

☑ Enable Web VPN (Please enable TCP port 443 in the "Interface > WAN > HTTPS")

VPN IP Range 192.168.222.0 / 255.255.255.0

Encryption Algorithm 3DES

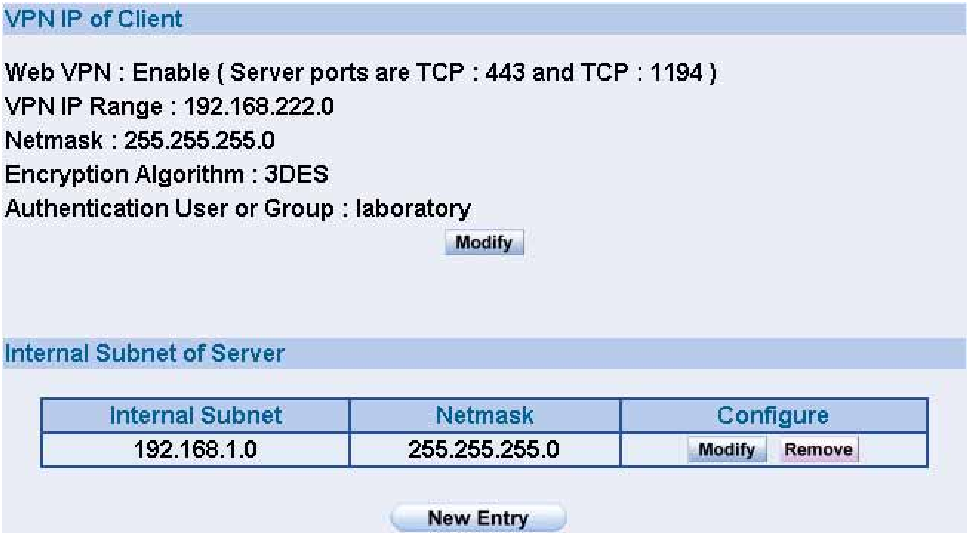
Protocol TCP

Server Port 1194

Authentication User or Group laboratory

Auto-Disconnect if idle 0 Minutes (0: means always connected)

Enable Web VPN Setting



VPN IP of Client

Web VPN : Enable (Server ports are TCP : 443 and TCP : 1194)

VPN IP Range : 192.168.222.0

Netmask : 255.255.255.0

Encryption Algorithm : 3DES

Authentication User or Group : laboratory

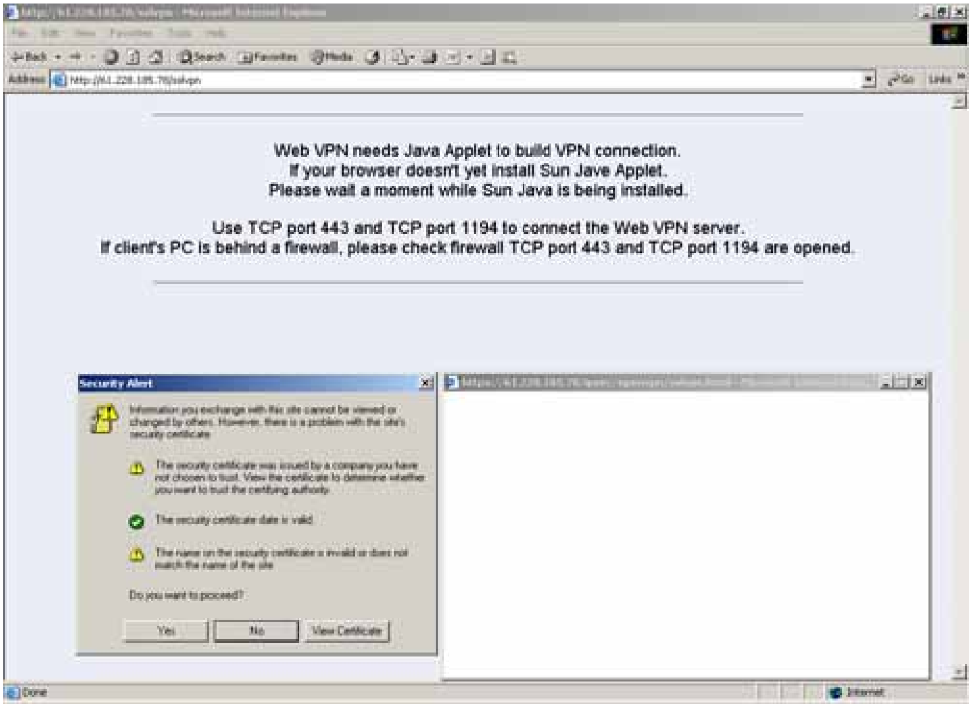
Internal Subnet of Server

Internal Subnet	Netmask	Configure
192.168.1.0	255.255.255.0	Modify Remove

Complete Enable Web VPN

STEP 5. Enter the following setting in **Browser**:

- **Address**: Enter http://61.11.11.11/sslvpn or http://61.11.11.11/webvpn. (It means to add "sslvpn" or "webvpn" character string to SG-1000's Web UI login IP.)。
- Click **Enter**.
- Click **Yes** in **Security Alert** window.
- Click **Yes** in **Warning - Security** window.
- Click **Yes** in **Warning - HTTPS** window.
- Click **Yes** in **Warning - Security** window.
- Enter **User Name** is john and **Password** is 123456789 in **Authentication** window.
- Click **OK**.



Web VPN needs Java Applet to build VPN connection.
If your browser doesn't yet install Sun Jave Applet.
Please wait a moment while Sun Java is being installed.

Use TCP port 443 and TCP port 1194 to connect the Web VPN server.
If client's PC is behind a firewall, please check firewall TCP port 443 and TCP port 1194 are opened.

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

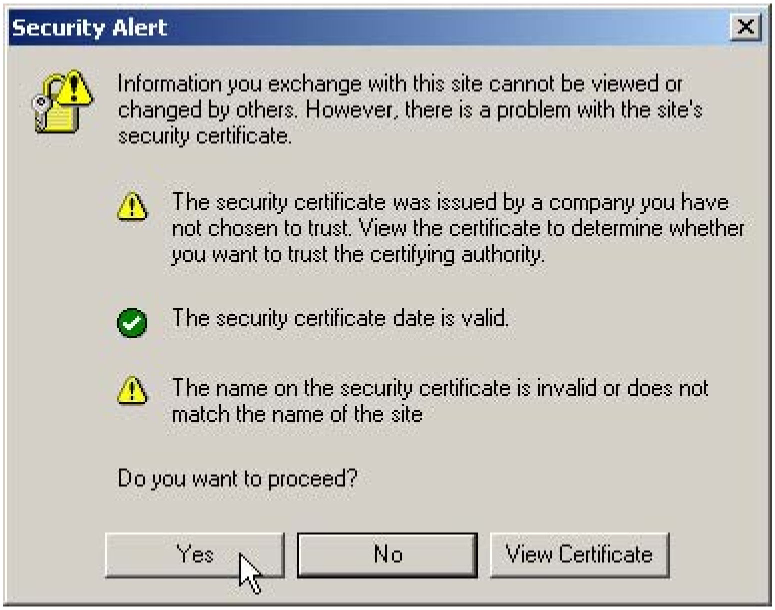
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Login SSL VPN Connection Web UI



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

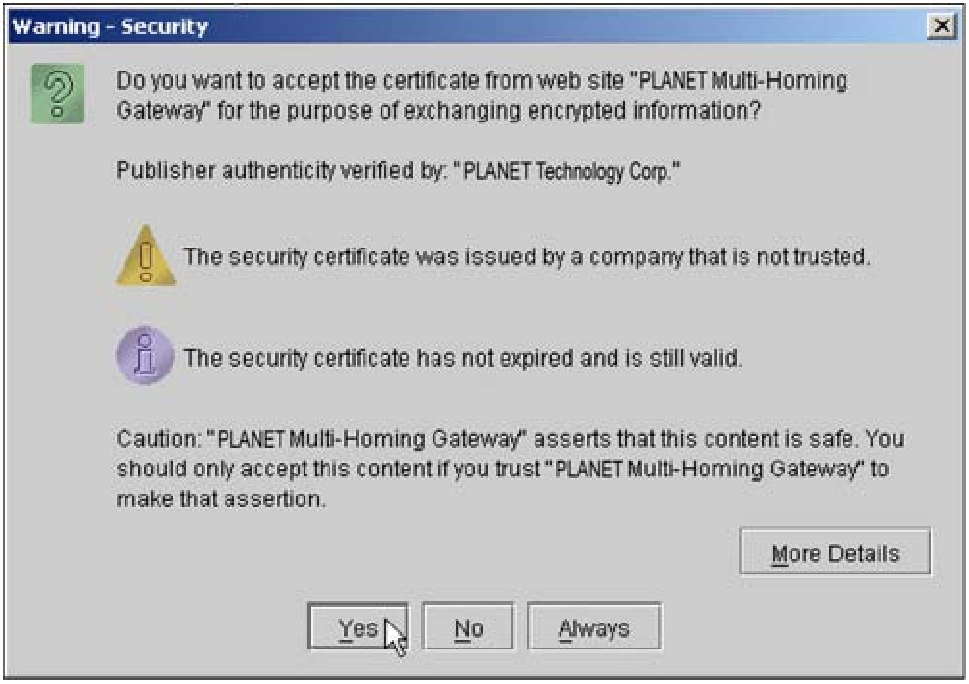
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Security Alert Window



Warning - Security

Do you want to accept the certificate from web site "PLANET Multi-Homing Gateway" for the purpose of exchanging encrypted information?

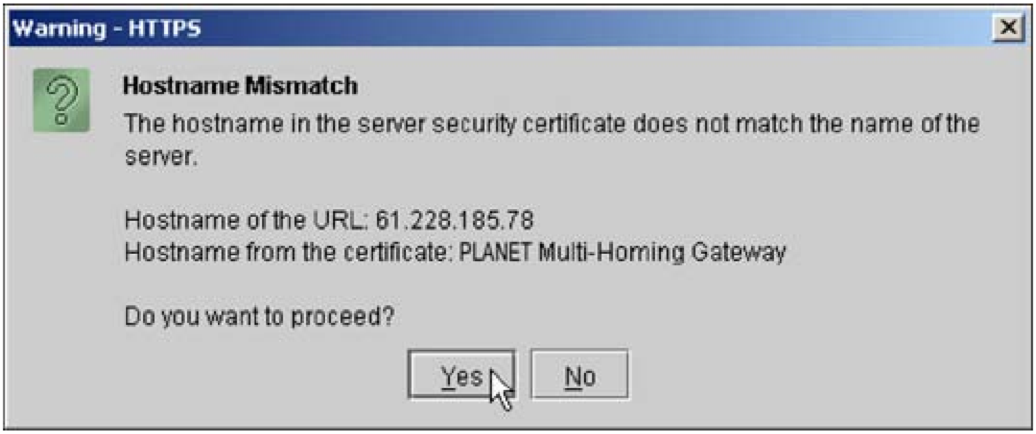
Publisher authenticity verified by: "PLANET Technology Corp."

⚠ The security certificate was issued by a company that is not trusted.

ℹ The security certificate has not expired and is still valid.

Caution: "PLANET Multi-Homing Gateway" asserts that this content is safe. You should only accept this content if you trust "PLANET Multi-Homing Gateway" to make that assertion.

Warning – Security Window



Warning - HTTPS

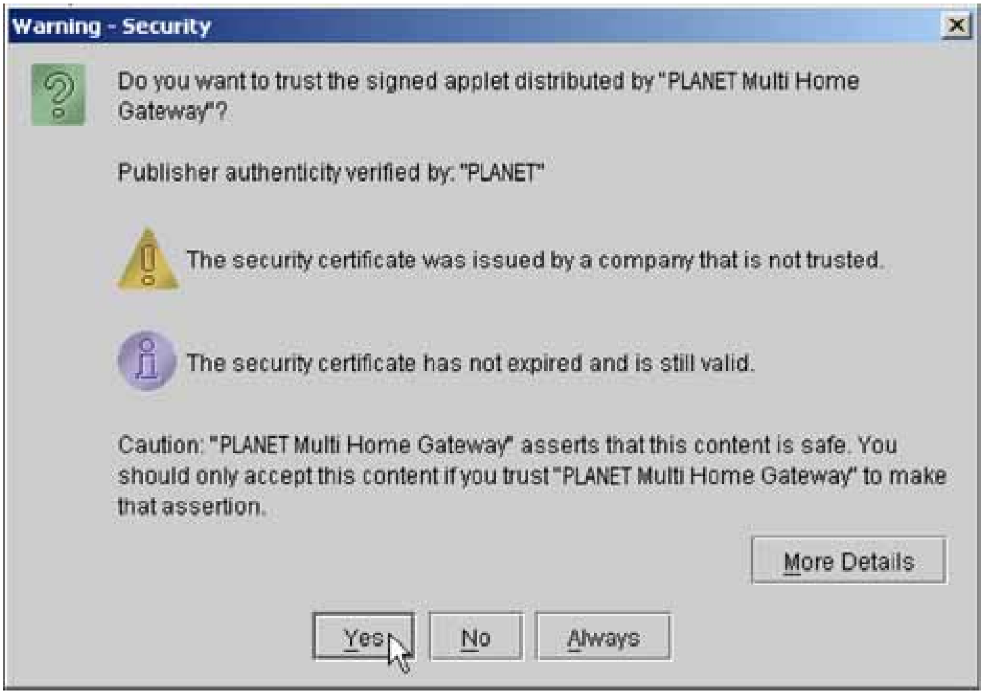
Hostname Mismatch

The hostname in the server security certificate does not match the name of the server.

Hostname of the URL: 61.228.185.78
Hostname from the certificate: PLANET Multi-Homing Gateway

Do you want to proceed?

Warning – HTTPS Window



Warning - Security

Do you want to trust the signed applet distributed by "PLANET Multi Home Gateway"?

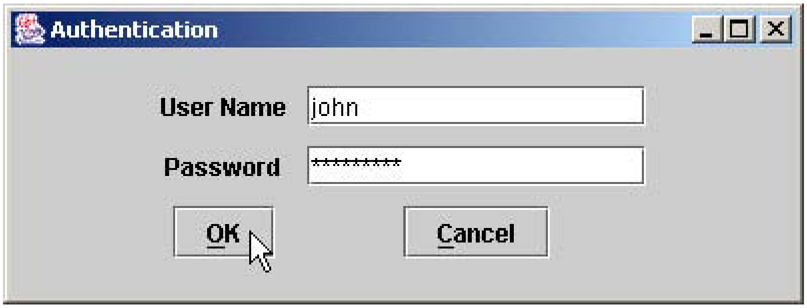
Publisher authenticity verified by: "PLANET"

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "PLANET Multi Home Gateway" asserts that this content is safe. You should only accept this content if you trust "PLANET Multi Home Gateway" to make that assertion.

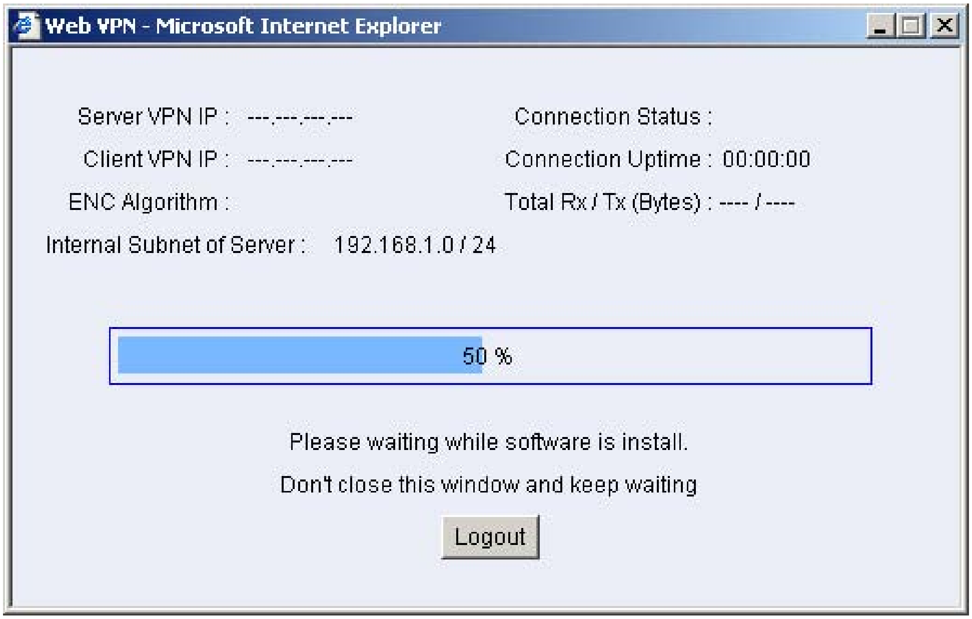
Warning – Security Window



User Name john

Password **********

Authentication Window



Server VPN IP : ---.---.---.---

Connection Status :

Client VPN IP : ---.---.---.---

Connection Uptime : 00:00:00

ENC Algorithm :

Total Rx / Tx (Bytes) : ---- / ----

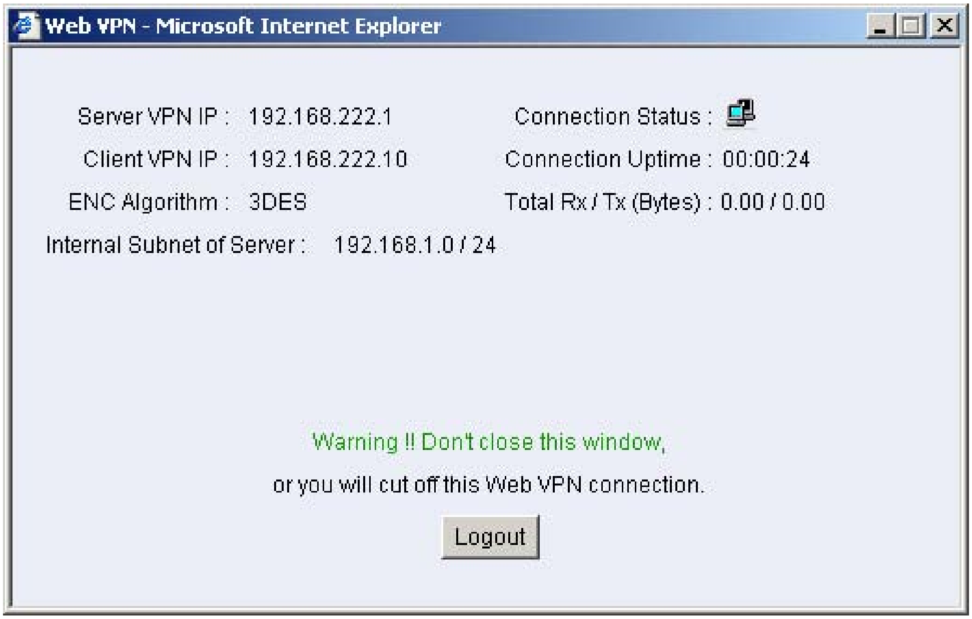
Internal Subnet of Server : 192.168.1.0 / 24

50 %

Please waiting while software is install.

Don't close this window and keep waiting

SSL VPN Connecting



Server VPN IP : 192.168.222.1

Connection Status :

Client VPN IP : 192.168.222.10

Connection Uptime : 00:00:24

ENC Algorithm : 3DES

Total Rx / Tx (Bytes) : 0.00 / 0.00

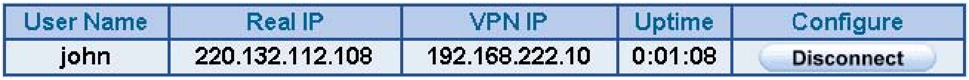
Internal Subnet of Server : 192.168.1.0 / 24

Warning !! Don't close this window,

or you will cut off this Web VPN connection.

Complete SSL VPN Connection

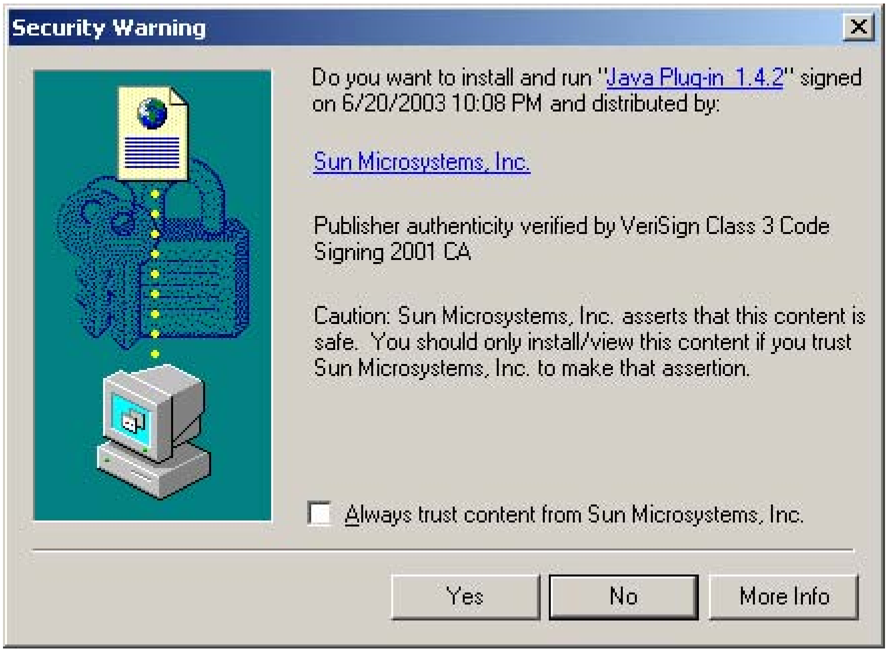
STEP 6. Display the following connection message in **Satus** of **Web VPN / SSL VPN**:



User Name	Real IP	VPN IP	Uptime	Configure
john	220.132.112.108	192.168.222.10	0:01:08	Disconnect

SSL VPN Connection Status

If client PC not install SUN JAVA Runtime Environment, when login SSL VPN connection Web UI, it will download anf install this software automatically.


Security Warning

Do you want to install and run "Java Plug-in 1.4.2" signed on 6/20/2003 10:08 PM and distributed by:

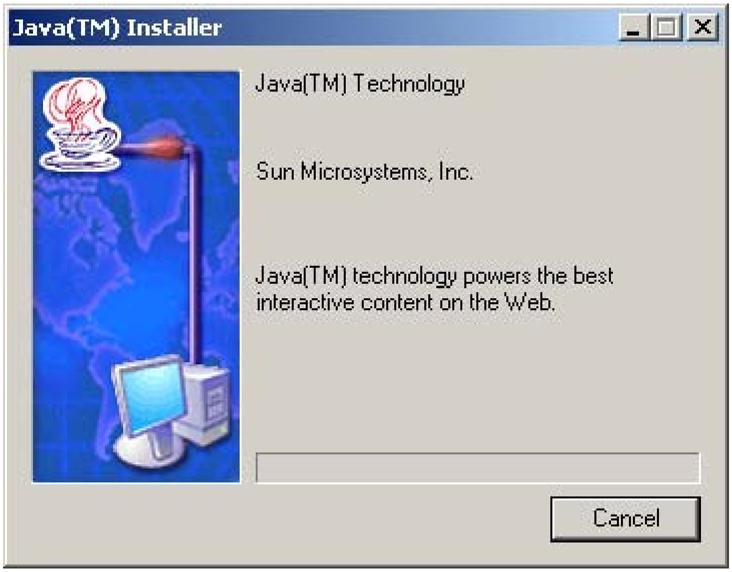
Sun Microsystems, Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: Sun Microsystems, Inc. asserts that this content is safe. You should only install/view this content if you trust Sun Microsystems, Inc. to make that assertion.

□ Always trust content from Sun Microsystems, Inc.

Install Java Runtime Environment Plug-in CA Authenticity


Java(TM) Installer

Java(TM) Technology

Sun Microsystems, Inc.

Java(TM) technology powers the best interactive content on the Web.

Installing Java Runtime Environment Plug-in

Chapter 15

Alert Setting

When the SG-1000 had detected attacks from hackers and the internal PC sending large DDoS attacks. The **Internal Alert** and **External Alert** will start on blocking these packets to maintain the whole network.

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

Define the required fields of Hacker Alert

Detect SYN Attack:

- ■ Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will cause valid users cannot connect to the servers.
  - ◆ **【SYN Flood Threshold(Total) Pkts/Sec】:** The system Administrator can enter the maximum number of SYN packets per second that is allowed to enter the network/SG-1000. 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/SG-1000. 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 SG-1000 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 SG-1000 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/SG-1000. 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 / SG-1000. 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 SG-1000 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 SG-1000 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/SG-1000. 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/SG-1000. 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 SG-1000 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 SG-1000 System and invade the network.

Detect Port Scan Attack:

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

Detect Tear Drop Attack:

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

Filter IP Route Option:

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

Detect Land Attack:

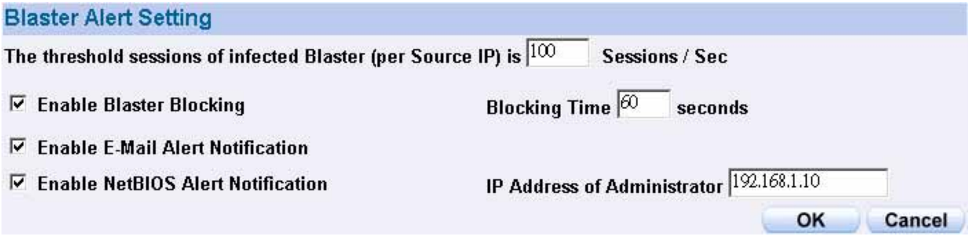
- Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when **SYN** on the TCP header is marked. Enable this function to detect such abnormal packets.

After System Manager enable **External Alert**, if the SG-1000 has detected any abnormal situation, the alarm message will appear in **External Alarm** in **Attack Alarm**. And if the system manager starts the **E-mail Alert Notification** in **Settings**, the device will send e-mail to alarm the system manager automatically.

15.1 SG-1000 Alarm and to prevent the computer which being attacked to send DDoS packets to LAN network

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

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



Blaster Alert Setting

The threshold sessions of infected Blaster (per Source IP) is 100 Sessions / Sec

☑ Enable Blaster Blocking   Blocking Time 60 seconds

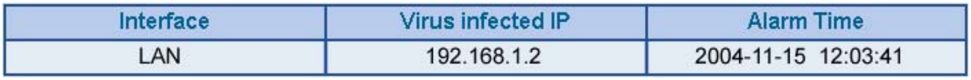
☑ Enable E-Mail Alert Notification

☑ Enable NetBIOS Alert Notification   IP Address of Administrator 192.168.1.10

Internal Alert Settings

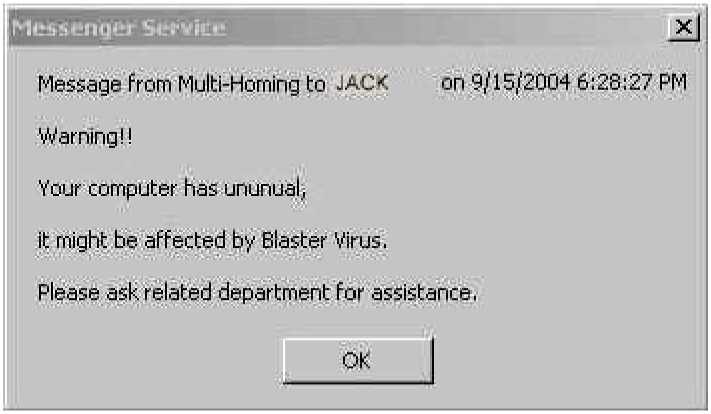
After complete the Internal Alert Settings, if the device had detected the internal computer sending large DDoS attack packets and then the alarm message will appear in the **Internal Alarm** in **Attack Alarm** or send NetBIOS Alert notification to the infected PC Administrator's PC

If the Administrator starts the **E-Mail Alert Notification** in **Setting**, the SG-1000 will send e-mail to Administrator automatically.



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

Internal Alert Record



Message from Multi-Homing to JACK on 9/15/2004 6:28:27 PM

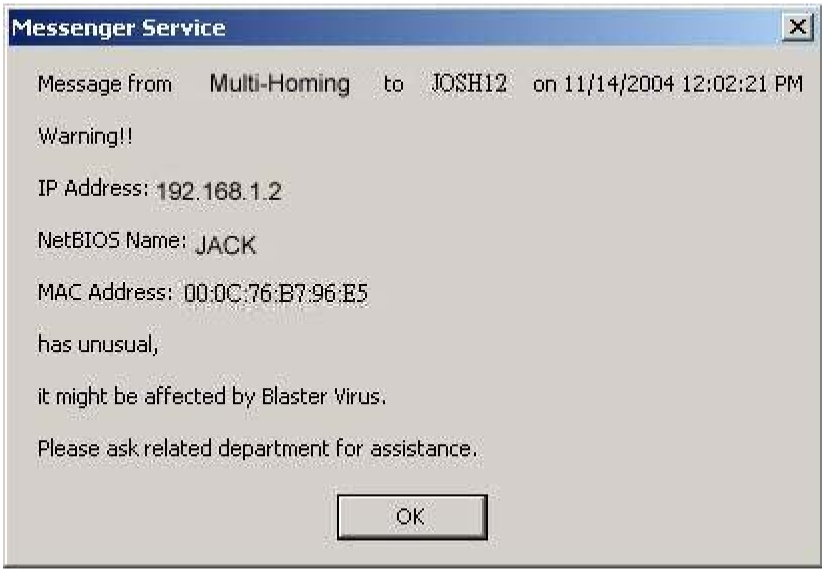
Warning!!

Your computer has ununual,

it might be affected by Blaster Virus.

Please ask related department for assistance.

NetBIOS Alert Notification to the Infected PC



Messenger Service

Message from Multi-Homing to JOSH12 on 11/14/2004 12:02:21 PM

Warning!!

IP Address: 192.168.1.2

NetBIOS Name: JACK

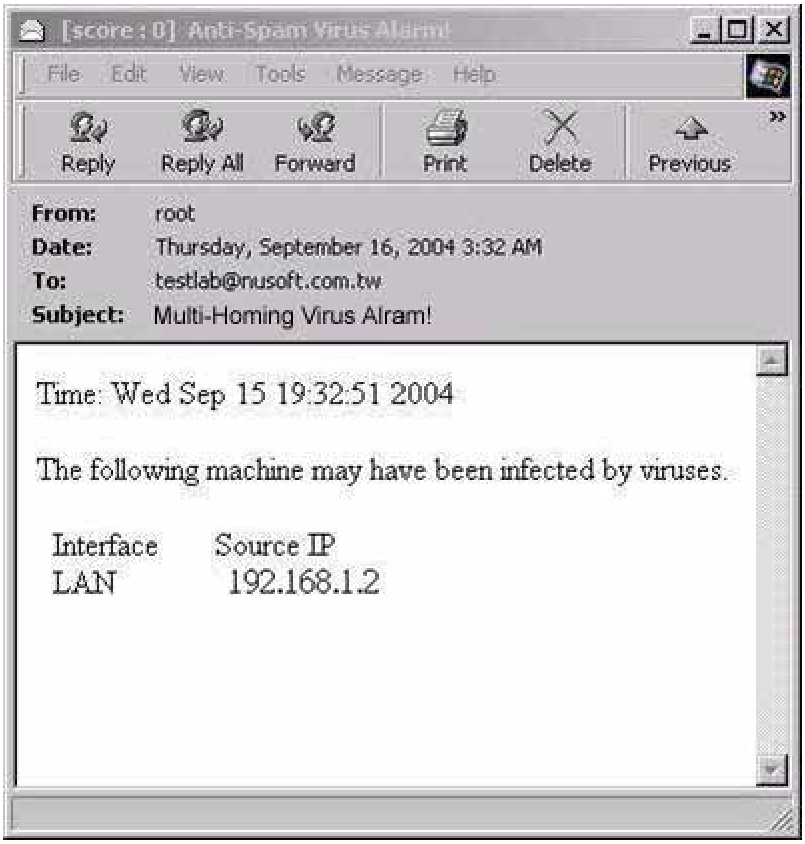
MAC Address: 00:0C:76:B7:96:E5

has unusual,

it might be affected by Blaster Virus.

Please ask related department for assistance.

NetBIOS Alert Notification to Administrator's PC



From: root
Date: Thursday, September 16, 2004 3:32 AM
To: testlab@nusoft.com.tw
Subject: Multi-Homing Virus Alram!

Time: Wed Sep 15 19:32:51 2004

The following machine may have been infected by viruses.

```
  Interface      Source IP
  LAN              192.168.1.2
```

E-mail Virus Alert

Chapter 16

Attack Alarm

SG-1000 has two alarm forms: **Internal Alarm,** and **External Alarm**.

Internal Alarm: When the SG-1000 had detected the internal PC sending large DDoS attacks and then the Internal Alarm will start on blocking these packets to maintain the whole network.

External Alarm: When SG-1000 detects attacks from hackers, it writes attacking data in the External Alarm file and sends an e-mail alert to the Administrator to take emergency steps.

How to use Attack Alarm

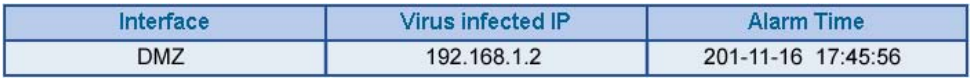
The Administrator can be notified the unusal affair in Intranet from Attack Alarms. And the Administrator can backup the Internal Alarm, and External Alarm and then delete the records to maintain the network status.

We set up two Alarm examples in the chapter:

No.	Suitable Situation	Example
Ex 1	**Internal Alarm**	To record the DDoS attack alarm from internal PC
Ex 2	**External Alarm**	To record the attack alarm about Hacker attacks the SG-1000 and Intranet

16.1 To record the DDoS attack alarm from internal PC

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

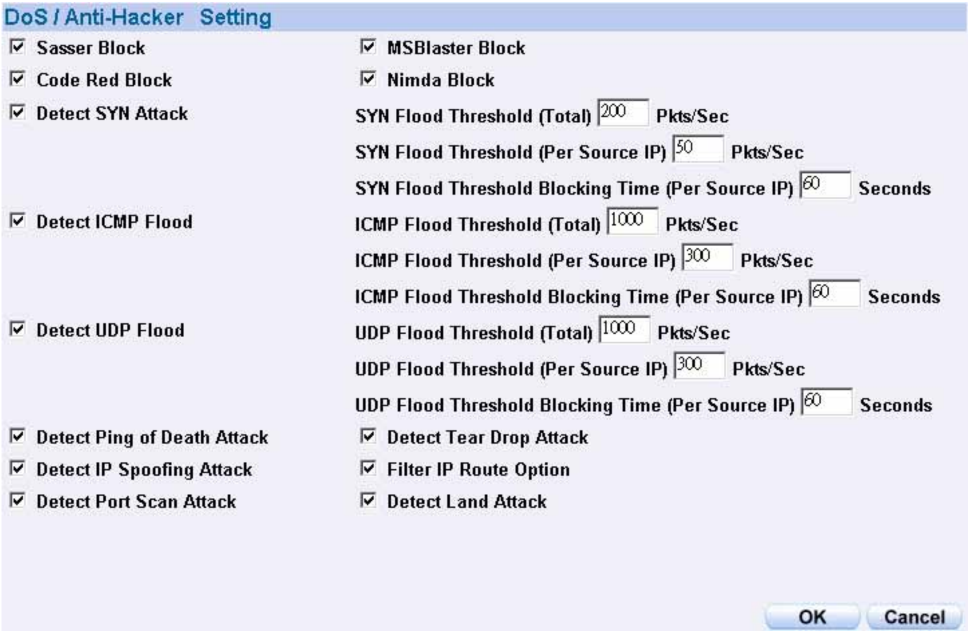


Interface	Virus infected IP	Alarm Time
DMZ	192.168.1.2	201-11-16 17:45:56

Internal Alarm Web UI

16.2 To record the attack alarm about Hacker attacks the SG-1000 and Intranet

STEP 1． Select the following settings in **External Alert** in **Alert Setting** function:



DoS / Anti-Hacker Setting

☑ Sasser Block

☑ MSBlaster Block

☑ Code Red Block

☑ Nimda Block

☑ Detect SYN Attack

SYN Flood Threshold (Total) 200 Pkts/Sec

SYN Flood Threshold (Per Source IP) 50 Pkts/Sec

SYN Flood Threshold Blocking Time (Per Source IP) 60 Seconds

☑ Detect ICMP Flood

ICMP Flood Threshold (Total) 1000 Pkts/Sec

ICMP Flood Threshold (Per Source IP) 300 Pkts/Sec

ICMP Flood Threshold Blocking Time (Per Source IP) 60 Seconds

☑ Detect UDP Flood

UDP Flood Threshold (Total) 1000 Pkts/Sec

UDP Flood Threshold (Per Source IP) 300 Pkts/Sec

UDP Flood Threshold Blocking Time (Per Source IP) 60 Seconds

☑ Detect Ping of Death Attack

☑ Detect Tear Drop Attack

☑ Detect IP Spoofing Attack

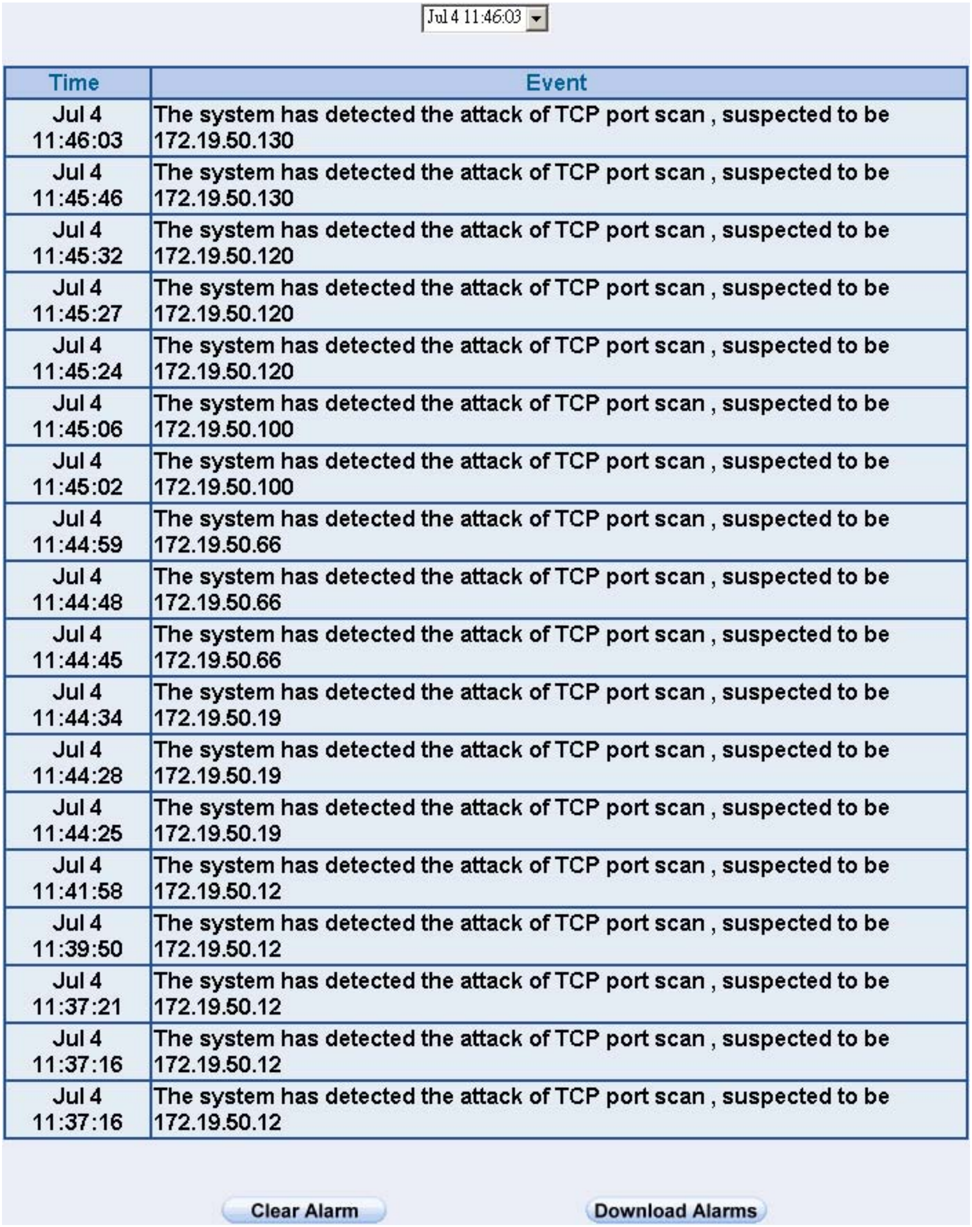
☑ Filter IP Route Option

☑ Detect Port Scan Attack

☑ Detect Land Attack

External Alert Setting Web UI

STEP 2 . When Hacker attacks the SG-1000 and Intranet, select **External Alarm** in **Attack Alarm** function to have detailed records about the hacker attacks.



Jul 4 11:46:03

Time	Event
Jul 4 11:46:03	The system has detected the attack of TCP port scan , suspected to be 172.19.50.130
Jul 4 11:45:46	The system has detected the attack of TCP port scan , suspected to be 172.19.50.130
Jul 4 11:45:32	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:27	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:24	The system has detected the attack of TCP port scan , suspected to be 172.19.50.120
Jul 4 11:45:06	The system has detected the attack of TCP port scan , suspected to be 172.19.50.100
Jul 4 11:45:02	The system has detected the attack of TCP port scan , suspected to be 172.19.50.100
Jul 4 11:44:59	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:48	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:45	The system has detected the attack of TCP port scan , suspected to be 172.19.50.66
Jul 4 11:44:34	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:44:28	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:44:25	The system has detected the attack of TCP port scan , suspected to be 172.19.50.19
Jul 4 11:41:58	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:39:50	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:21	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:16	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12
Jul 4 11:37:16	The system has detected the attack of TCP port scan , suspected to be 172.19.50.12

External Alarm Web UI

Chapter 17

LOG

Log records all connections that pass through the SG-1000's control policies. The information is classified as Traffic Log, Event Log, and Connection Log.

Traffic Log's parameters are setup when setting up policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy.

Event Log record the contents of System Configurations changes made by the Administrator such as the time of change, settings that change, the IP address used to log in…etc.

Connection Log records all of the connections of SG-1000. When the connection occurs some problem, the Administrator can trace back the problem from the information.

How to use the Log

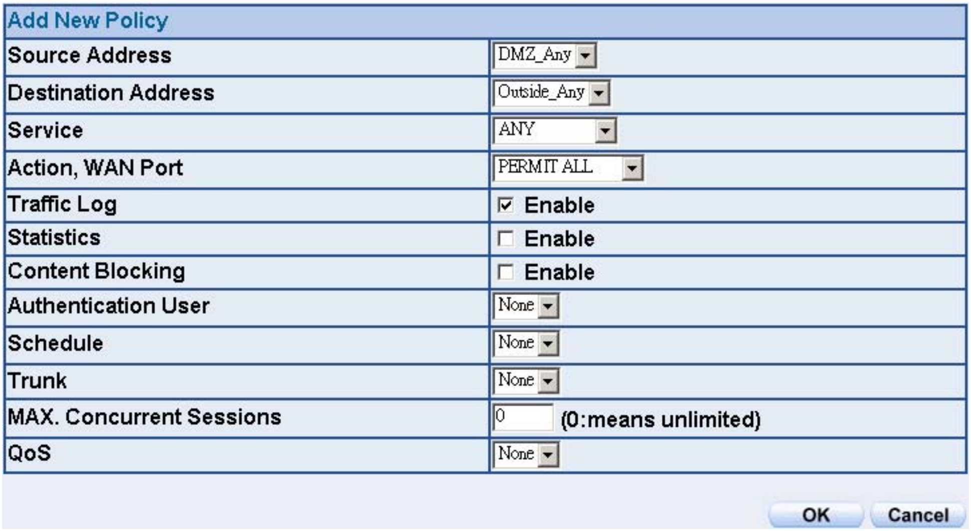
The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

We set up four LOG examples in the chapter:

No.	Suitable Situation	Example
Ex 1	**Traffic Log**	To detect the information and Protocol port that users use to access to Internet or Intranet by SG-1000.
Ex 2	**Event Log**	To record the detailed management events (such as Interface and event description of SG-1000) of the Administrator
Ex 3	**Connection Log**	To detect event description of WAN Connection
Ex 4	**Log Backup**	To save or receive the records that sent by the SG-1000

17.1 To detect the information and Protocol port that users use to access to Internet or Intranet by SG-1000

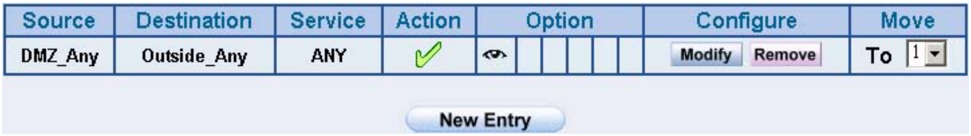
STEP 1．Add new policy in **DMZ to WAN** of **Policy** and select **Enable Logging**:



Add New Policy	
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Action, WAN Port	PERMIT ALL
Traffic Log	☑ Enable
Statistics	☐ Enable
Content Blocking	☐ Enable
Authentication User	None
Schedule	None
Trunk	None
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Logging Policy Setting

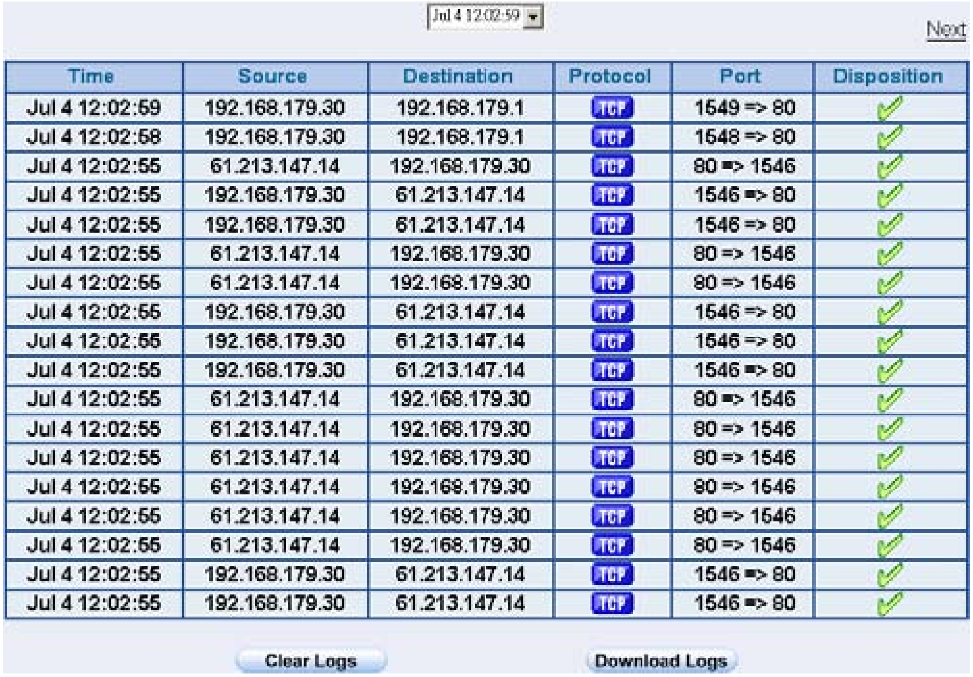
STEP 2．Complete the Logging Setting in **DMZ to WAN Policy**:



Source	Destination	Service	Action	Option	Configure	Move
DMZ_Any	Outside_Any	ANY	✓	👁	Modify Remove	To 1

Complete the Logging Setting of DMZ to WAN

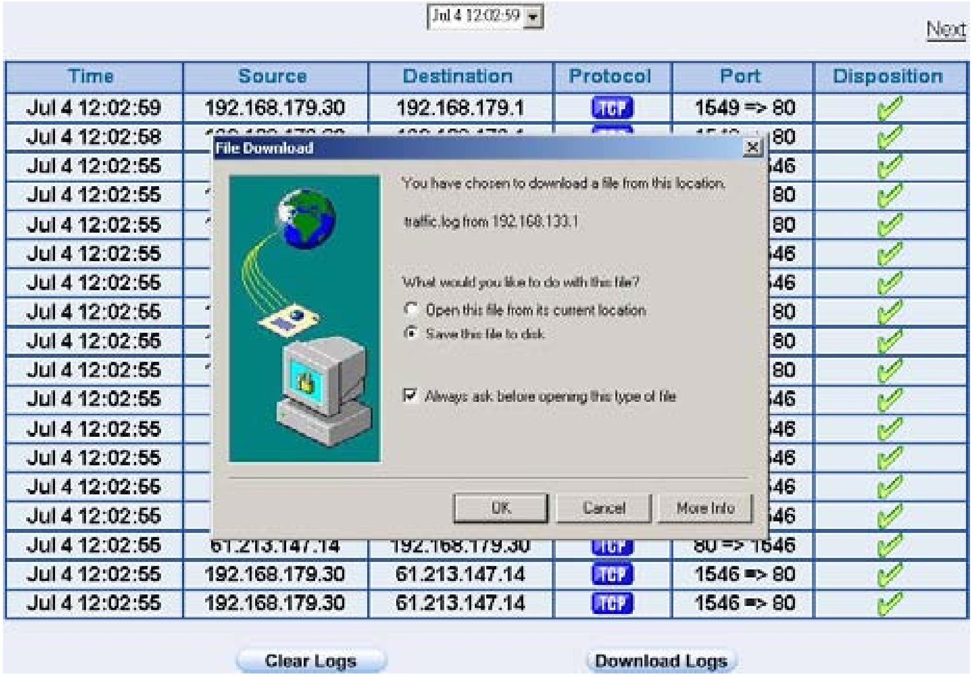
STEP 3．Click **Traffic Log**. It will show up the packets records that pass this policy.



Time	Source	Destination	Protocol	Port	Disposition
Jul 4 12:02:59	192.168.179.30	192.168.179.1	TCP	1549 => 80	✓
Jul 4 12:02:58	192.168.179.30	192.168.179.1	TCP	1548 => 80	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓

Traffic Log Web UI

STEP 4 . Click on **Download Logs** and select **Save** in **File Download** Web UI. And then choose the place to save in PC and click **OK**; the records will be saved instantly.



Jul 4 12:02:59 ▾

Next

Time	Source	Destination	Protocol	Port	Disposition
Jul 4 12:02:59	192.168.179.30	192.168.179.1	TCP	1549 => 80	✓
Jul 4 12:02:58				80	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				80	✓
Jul 4 12:02:55				80	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				80	✓
Jul 4 12:02:55				80	✓
Jul 4 12:02:55				80	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55				46	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓

File Download

You have chosen to download a file from this location.

traffic.log from 192.168.133.1

What would you like to do with this file?

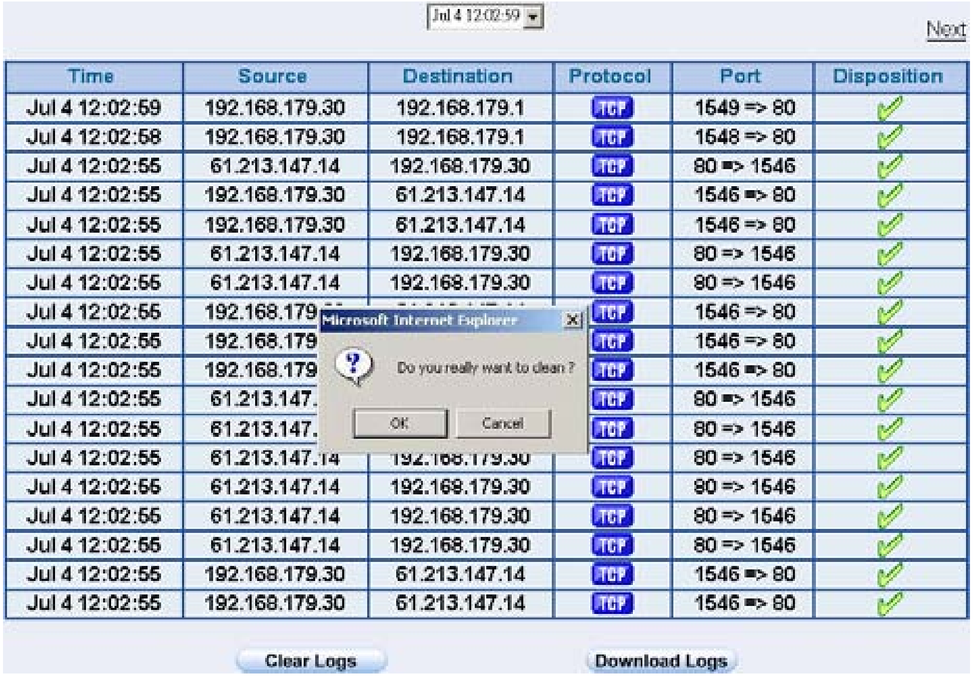
○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

Download Traffic Log Records Web UI

STEP 5 . Click **Clear Logs** and click **OK** on the confirm Web UI; the records will be deleted from the SG-1000 instantly.



Jul 4 12:02:59 ▾

Next

Time	Source	Destination	Protocol	Port	Disposition
Jul 4 12:02:59	192.168.179.30	192.168.179.1	TCP	1549 => 80	✓
Jul 4 12:02:58	192.168.179.30	192.168.179.1	TCP	1548 => 80	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179	[illegible]	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179	[illegible]	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179	[illegible]	TCP	1546 => 80	✓
Jul 4 12:02:55	61.213.147.	[illegible]	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.	[illegible]	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	61.213.147.14	192.168.179.30	TCP	80 => 1546	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓
Jul 4 12:02:55	192.168.179.30	61.213.147.14	TCP	1546 => 80	✓

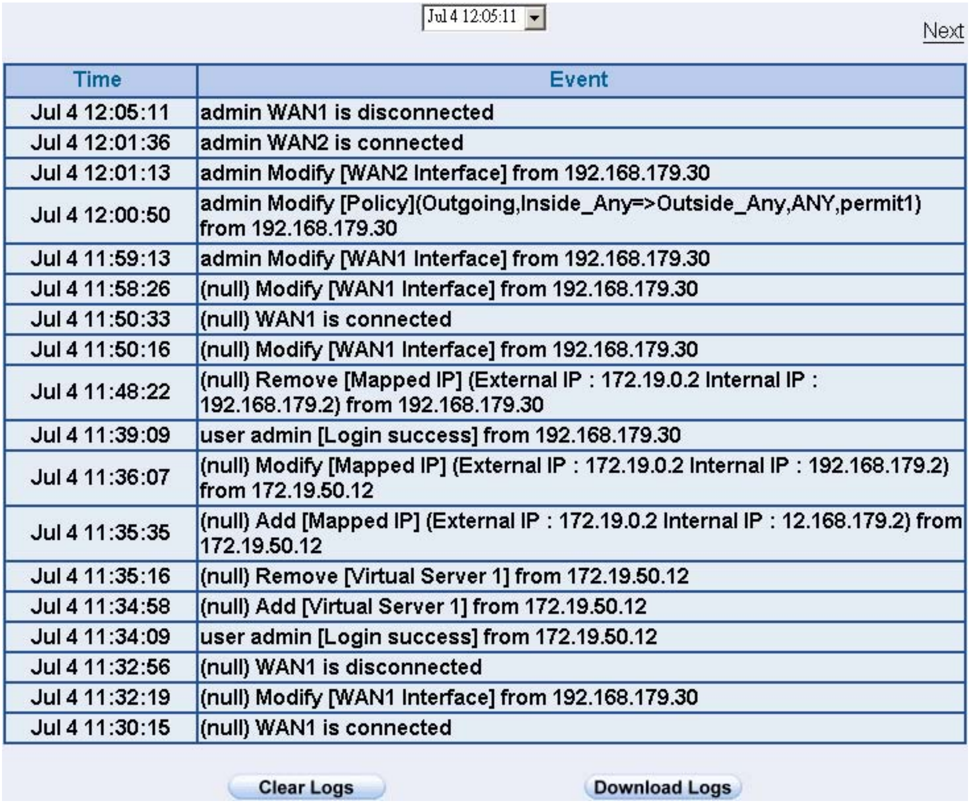
Microsoft Internet Explorer

Do you really want to clean ?

Clearing Traffic Log Records Web UI

17.2 To record the detailed management events (such as Interface and event description of SG-1000) of the Administrator

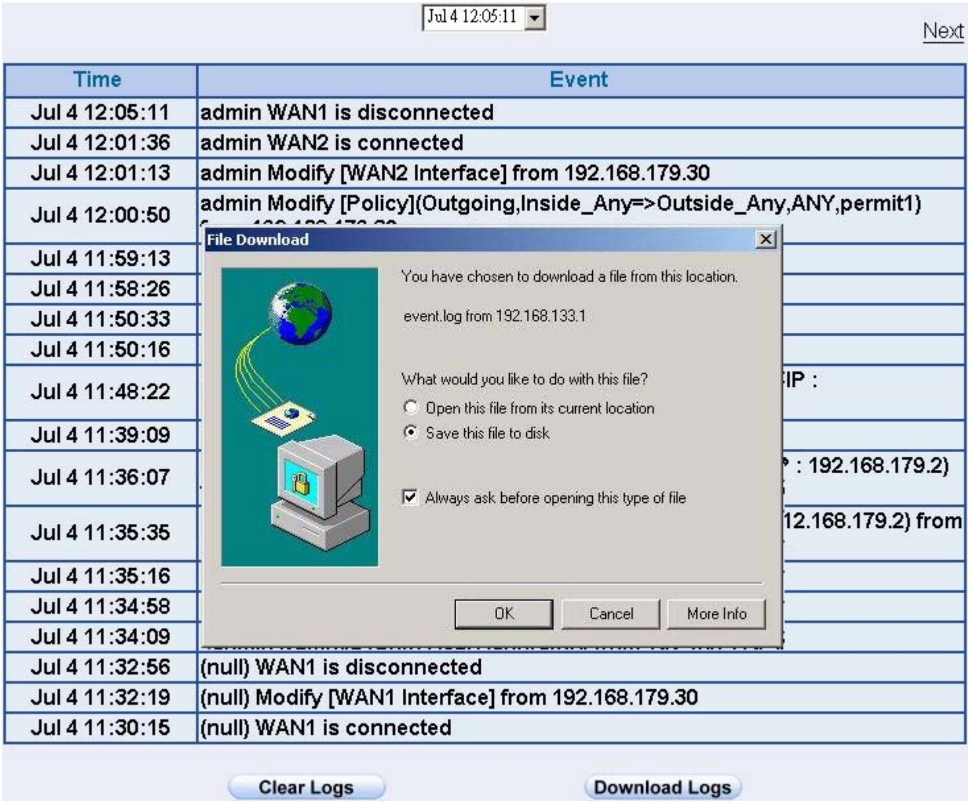
STEP 1 . Click **Event** log of **LOG**. The management event records of the administrator will show up.



Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1) from 192.168.179.30
Jul 4 11:59:13	admin Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:58:26	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:50:33	(null) WAN1 is connected
Jul 4 11:50:16	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:48:22	(null) Remove [Mapped IP] (External IP : 172.19.0.2 Internal IP : 192.168.179.2) from 192.168.179.30
Jul 4 11:39:09	user admin [Login success] from 192.168.179.30
Jul 4 11:36:07	(null) Modify [Mapped IP] (External IP : 172.19.0.2 Internal IP : 192.168.179.2) from 172.19.50.12
Jul 4 11:35:35	(null) Add [Mapped IP] (External IP : 172.19.0.2 Internal IP : 12.168.179.2) from 172.19.50.12
Jul 4 11:35:16	(null) Remove [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:58	(null) Add [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:09	user admin [Login success] from 172.19.50.12
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

Event Log Web UI

STEP 2 . Click on **Download Logs** and select **Save** in **File Download** Web UI. And then choose the place to save in PC and click **OK**; the records will be saved instantly.



Jul 4 12:05:11 ▾

Next

Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1)
Jul 4 11:59:13	
Jul 4 11:58:26	
Jul 4 11:50:33	
Jul 4 11:50:16	
Jul 4 11:48:22	IP :
Jul 4 11:39:09	
Jul 4 11:36:07	: 192.168.179.2)
Jul 4 11:35:35	12.168.179.2) from
Jul 4 11:35:16	
Jul 4 11:34:58	
Jul 4 11:34:09	
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

File Download

You have chosen to download a file from this location.

event.log from 192.168.133.1

What would you like to do with this file?

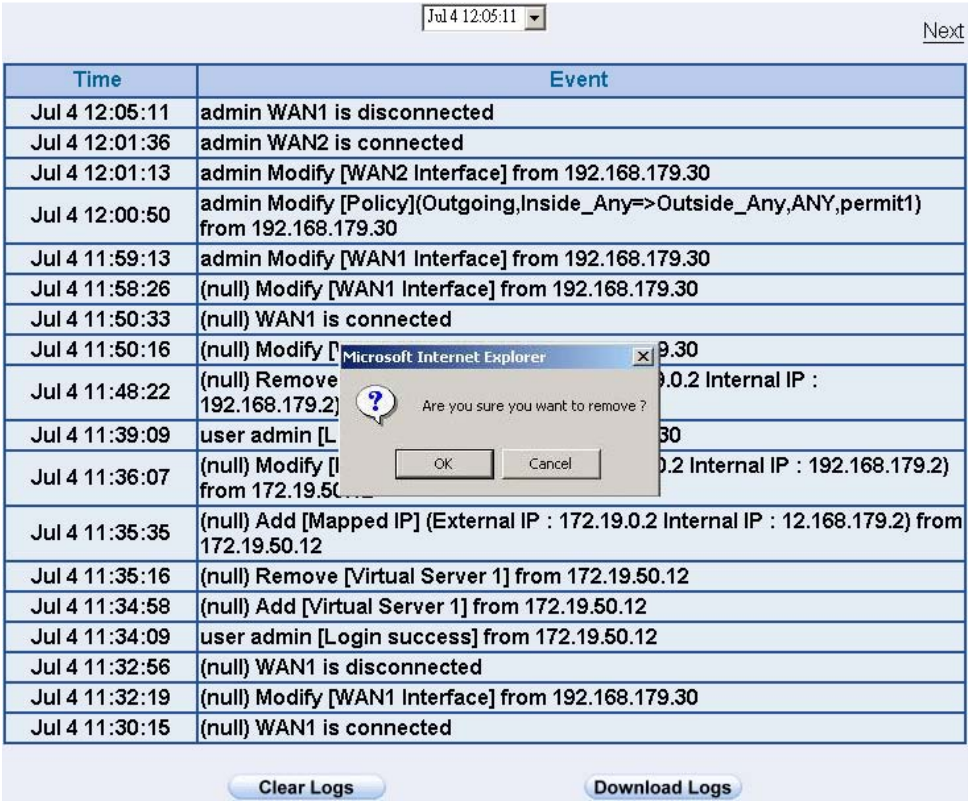
○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

Download Event Log Records Web UI

STEP 3 . Click **Clear Logs** and click **OK** on the confirm Web UI; the records will be deleted from the SG-1000.



Time	Event
Jul 4 12:05:11	admin WAN1 is disconnected
Jul 4 12:01:36	admin WAN2 is connected
Jul 4 12:01:13	admin Modify [WAN2 Interface] from 192.168.179.30
Jul 4 12:00:50	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit1) from 192.168.179.30
Jul 4 11:59:13	admin Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:58:26	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:50:33	(null) WAN1 is connected
Jul 4 11:50:16	(null) Modify [9.30
Jul 4 11:48:22	(null) Remove .0.2 Internal IP : 192.168.179.2)
Jul 4 11:39:09	user admin [L 30
Jul 4 11:36:07	(null) Modify [I .2 Internal IP : 192.168.179.2) from 172.19.5
Jul 4 11:35:35	(null) Add [Mapped IP] (External IP : 172.19.0.2 Internal IP : 12.168.179.2) from 172.19.50.12
Jul 4 11:35:16	(null) Remove [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:58	(null) Add [Virtual Server 1] from 172.19.50.12
Jul 4 11:34:09	user admin [Login success] from 172.19.50.12
Jul 4 11:32:56	(null) WAN1 is disconnected
Jul 4 11:32:19	(null) Modify [WAN1 Interface] from 192.168.179.30
Jul 4 11:30:15	(null) WAN1 is connected

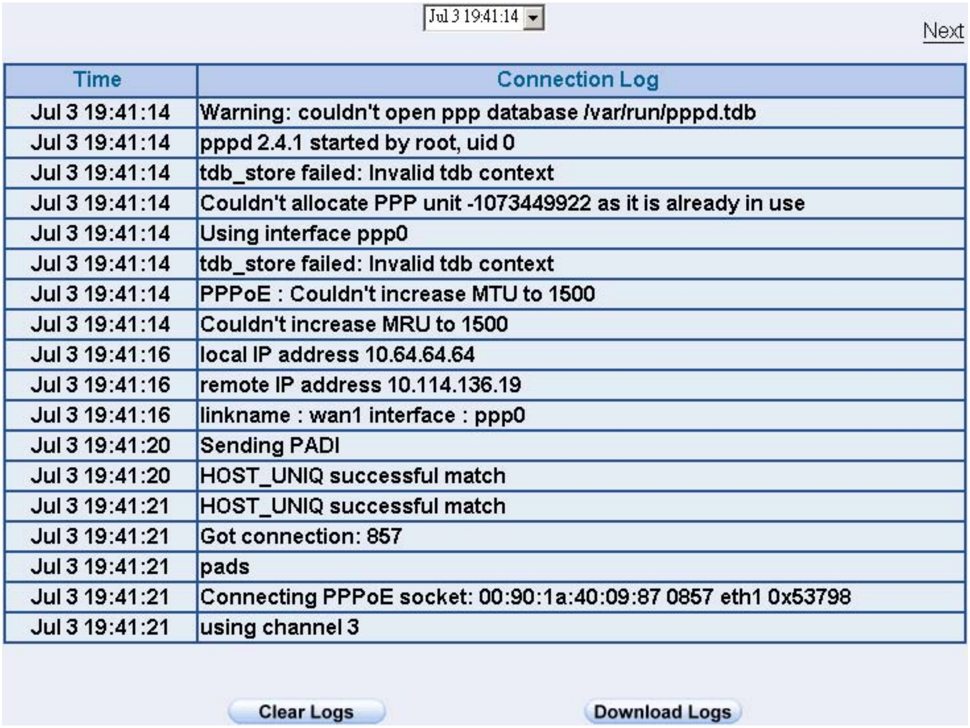
Microsoft Internet Explorer

Are you sure you want to remove ?

Clearing Event Log Records Web UI

17.3 To Detect Event Description of WAN Connection

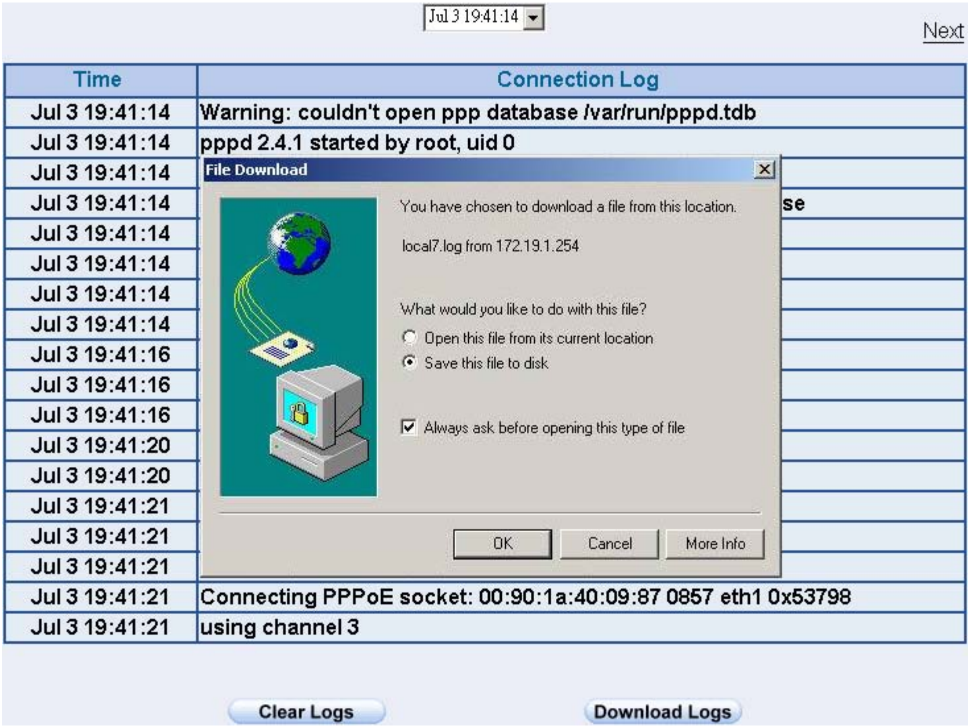
STEP 1 . Click **Connection** in **LOG**. It can show up WAN Connection records of the SG-1000.



Time	Connection Log
Jul 3 19:41:14	Warning: couldn't open ppp database /var/run/pppd.tdb
Jul 3 19:41:14	pppd 2.4.1 started by root, uid 0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	Couldn't allocate PPP unit -1073449922 as it is already in use
Jul 3 19:41:14	Using interface ppp0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	PPPoE : Couldn't increase MTU to 1500
Jul 3 19:41:14	Couldn't increase MRU to 1500
Jul 3 19:41:16	local IP address 10.64.64.64
Jul 3 19:41:16	remote IP address 10.114.136.19
Jul 3 19:41:16	linkname : wan1 interface : ppp0
Jul 3 19:41:20	Sending PADI
Jul 3 19:41:20	HOST_UNIQ successful match
Jul 3 19:41:21	HOST_UNIQ successful match
Jul 3 19:41:21	Got connection: 857
Jul 3 19:41:21	pads
Jul 3 19:41:21	Connecting PPPoE socket: 00:90:1a:40:09:87 0857 eth1 0x53798
Jul 3 19:41:21	using channel 3

Connection records Web UI

STEP 2 . Click on **Download Logs** and select **Save** in **File Download** Web UI. And then choose the place to save in PC and click **OK**; the records will be saved instantly.



Time	Connection Log
Jul 3 19:41:14	Warning: couldn't open ppp database /var/run/pppd.tdb
Jul 3 19:41:14	pppd 2.4.1 started by root, uid 0
Jul 3 19:41:14	
Jul 3 19:41:14	se
Jul 3 19:41:14	
Jul 3 19:41:14	
Jul 3 19:41:14	
Jul 3 19:41:14	
Jul 3 19:41:16	
Jul 3 19:41:16	
Jul 3 19:41:16	
Jul 3 19:41:20	
Jul 3 19:41:20	
Jul 3 19:41:21	
Jul 3 19:41:21	
Jul 3 19:41:21	
Jul 3 19:41:21	Connecting PPPoE socket: 00:90:1a:40:09:87 0857 eth1 0x53798
Jul 3 19:41:21	using channel 3

File Download

You have chosen to download a file from this location.

local7.log from 172.19.1.254

What would you like to do with this file?

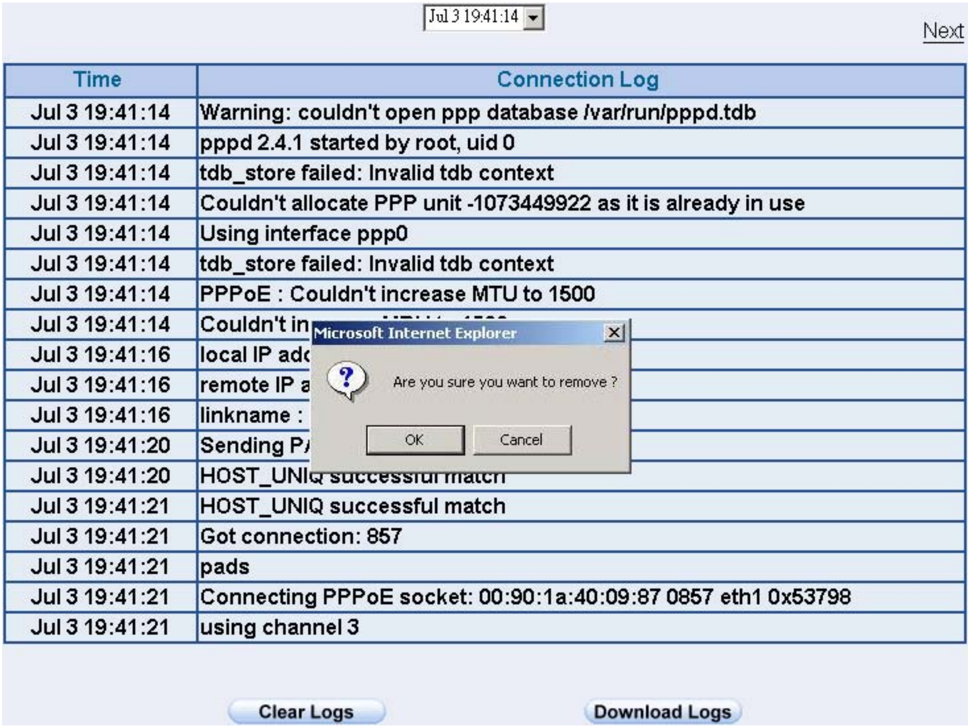
○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

Download Connection Log Records Web UI

STEP 3 . Click **Clear Logs** and click **OK** on the confirm Web UI, the records will be deleted from the SG-1000 instantly.



Time	Connection Log
Jul 3 19:41:14	Warning: couldn't open ppp database /var/run/pppd.tdb
Jul 3 19:41:14	pppd 2.4.1 started by root, uid 0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	Couldn't allocate PPP unit -1073449922 as it is already in use
Jul 3 19:41:14	Using interface ppp0
Jul 3 19:41:14	tdb_store failed: Invalid tdb context
Jul 3 19:41:14	PPPoE : Couldn't increase MTU to 1500
Jul 3 19:41:14	Couldn't in
Jul 3 19:41:16	local IP adc
Jul 3 19:41:16	remote IP a
Jul 3 19:41:16	linkname :
Jul 3 19:41:20	Sending P/
Jul 3 19:41:20	HOST_UNIQ successful match
Jul 3 19:41:21	HOST_UNIQ successful match
Jul 3 19:41:21	Got connection: 857
Jul 3 19:41:21	pads
Jul 3 19:41:21	Connecting PPPoE socket: 00:90:1a:40:09:87 0857 eth1 0x53798
Jul 3 19:41:21	using channel 3

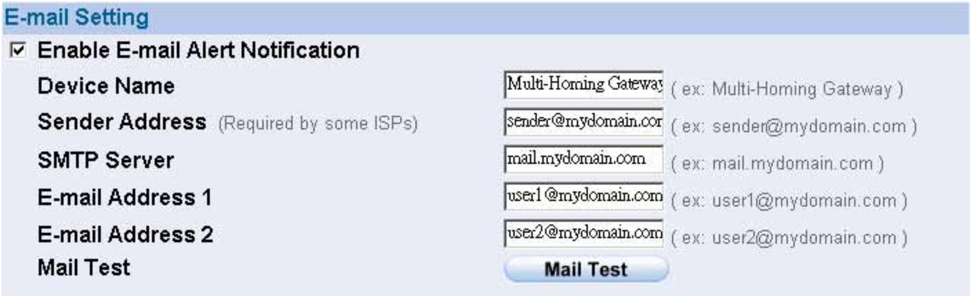
Microsoft Internet Explorer

Are you sure you want to remove ?

Clearing Connection Log Records Web UI

17.4 To save or receive the records that sent by the SG-1000

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



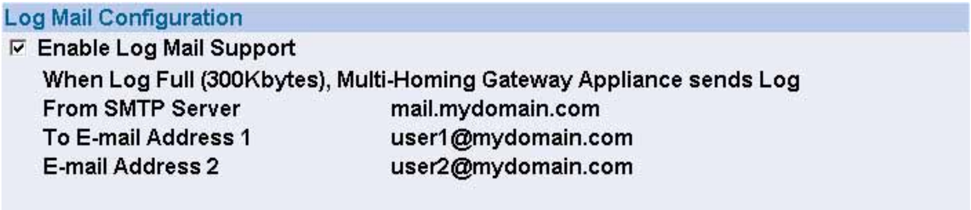
E-mail Setting

☑ Enable E-mail Alert Notification

Device Name	Multi-Homing Gatewa	(ex: Multi-Homing Gateway)
Sender Address (Required by some ISPs)	sender@mydomain.cor	(ex: sender@mydomain.com)
SMTP Server	mail.mydomain.com	(ex: mail.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	

E-mail Setting Web UI

STEP 2 . Enter **Log Backup** in **Log**, select **Enable Log Mail Support** and click **OK**



Log Mail Configuration

☑ Enable Log Mail Support

When Log Full (300Kbytes), Multi-Homing Gateway Appliance sends Log

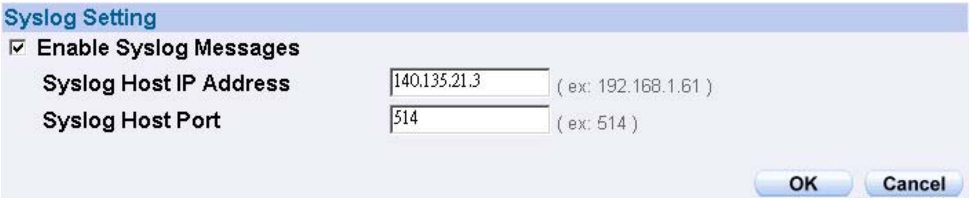
From SMTP Server	mail.mydomain.com
To E-mail Address 1	user1@mydomain.com
E-mail Address 2	user2@mydomain.com

Log Mail Configuration Web UI

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



Syslog Setting

☑ Enable Syslog Messages

Syslog Host IP Address 140.135.21.3 (ex: 192.168.1.61)

Syslog Host Port 514 (ex: 514)

Syslog Messages Setting Web UI

Chapter 18

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 SG-1000 for statistics of packets and data that passes across the SG-1000. The statistics provides the Administrator with information about network traffics and network loads.

Define the required fields of Statistics:

Statistics Chart:

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

Source IP, Destination IP, Service, and Action:

- These fields record the original data of Policy. From the information above, the Administrator can know which Policy is the Policy Statistics belonged to.

Time:

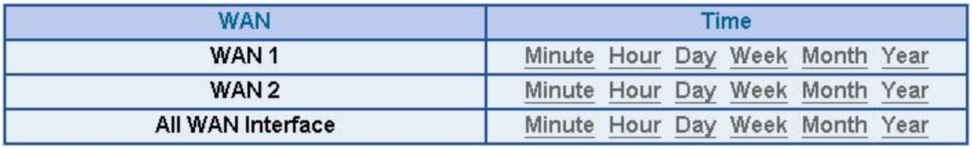
- To detect the statistics by minutes, hours, days, months, or years.

Bits/sec, Bytes/sec, Utilization, Total:

- The unit that used by Y-Coordinate, which the Administrator can change the unit of the Statistics Chart here.
  - **Utilization**：The percentage of the traffic of the Max. Bandwidth that System Manager set in Interface function.
  - **Total:** To consider the accumulative total traffic during a unit time as Y-Coordinate

18.1 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.



WAN	Time
WAN 1	Minute Hour Day Week Month Year
WAN 2	Minute Hour Day Week Month Year
All WAN Interface	Minute Hour Day Week Month Year

WAN Statistics function

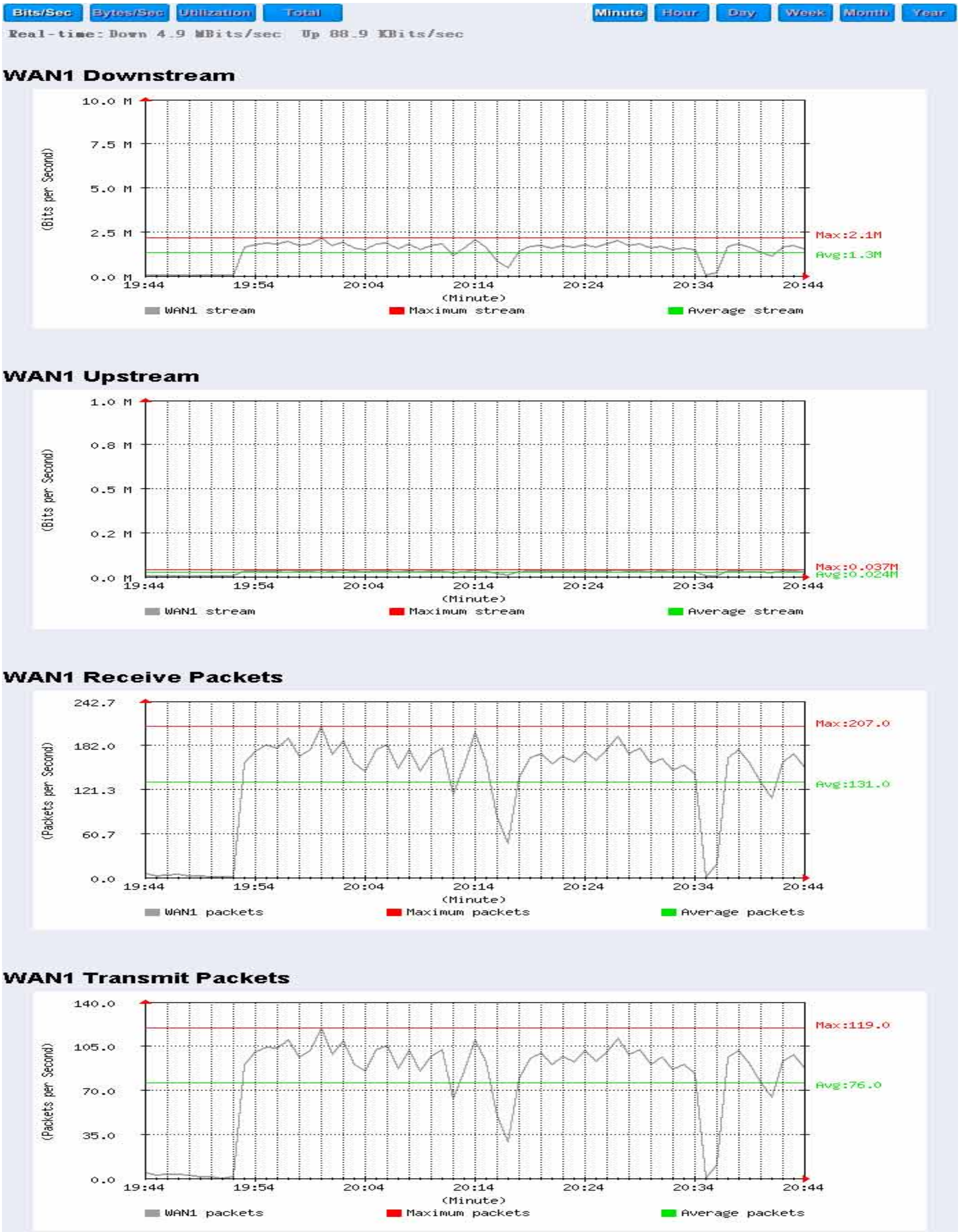
- **Time:** To detect the statistics by minutes, hours, days, months, or years.

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

STEP 2 . In the Statistics window, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics figure every minute; click **Hour** to check the Statistics figure every hour; click **Day** to check the Statistics figure every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

STEP 3 . Statistics Chart

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

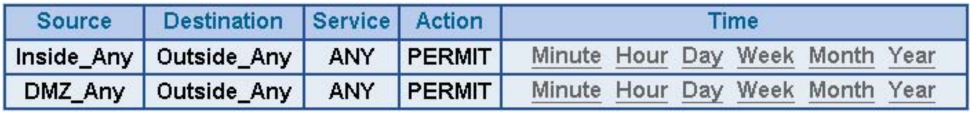


Real-time: Down 4.9 MBits/sec Up 88.9 KBits/sec

To Detect WAN Statistics

18.2 Policy Statistics

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



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

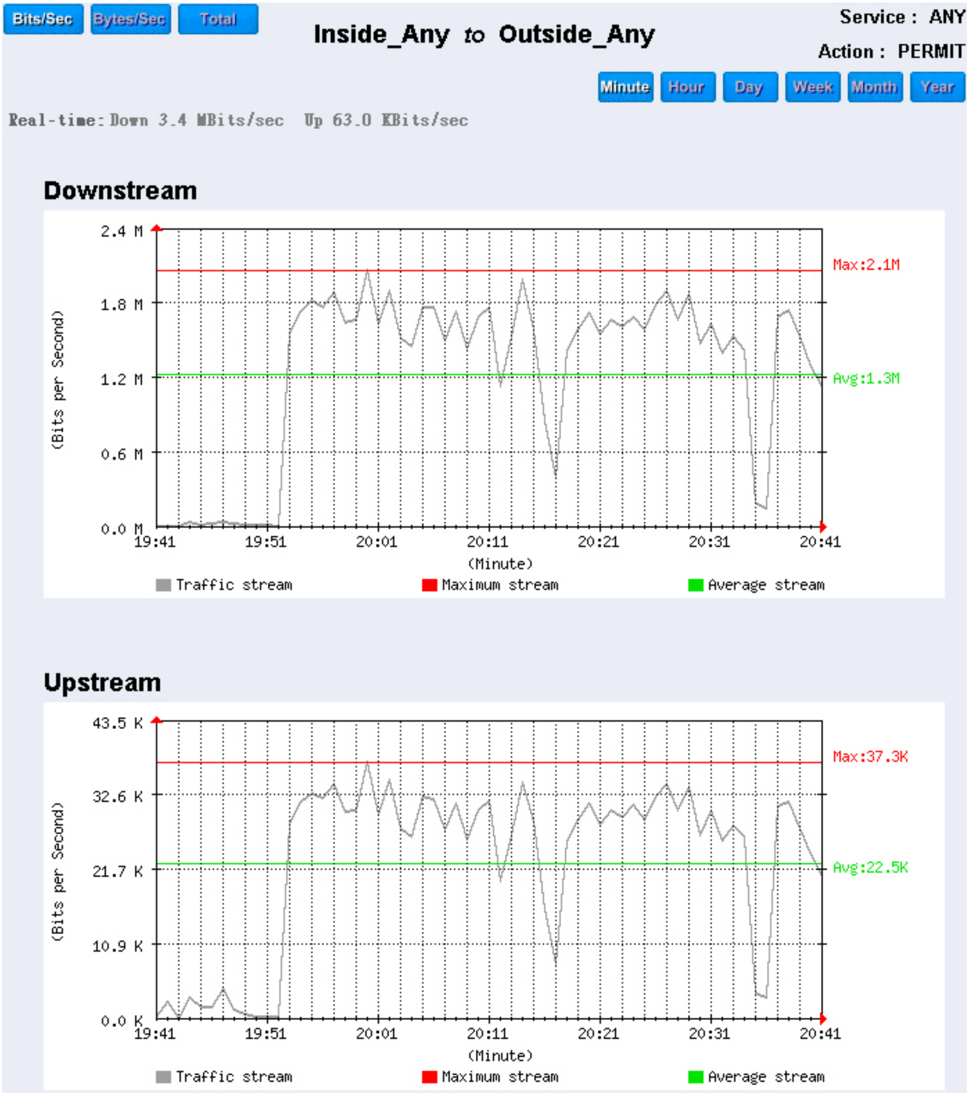
Policy Statistics Function

If you are going to use **Policy Statistics** function, the System Manager has to enable the **Statistics** in **Policy** first.

STEP 2 . In the **Statistics** Web UI, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics chart every minute; click **Hour** to check the Statistics chart every hour; click **Day** to check the Statistics chart every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

STEP 3．Statistics Chart

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



Inside_Any *to* Outside_Any

Service： ANY

Action： PERMIT

Real-time: Down 3.4 MBits/sec Up 63.0 KBits/sec

Downstream

Upstream

To Detect Policy Statistics

Chapter 19

Status

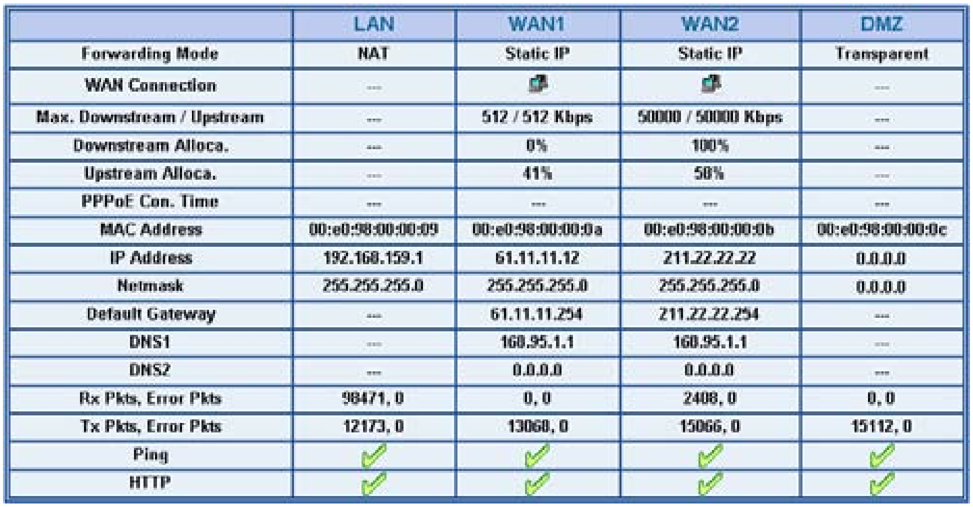
The users can know the connection status in Status. For example: LAN IP, WAN IP, Subnet Netmask, Default Gateway, DNS Server Connection, and its IP…etc.

- **Interface:** Display all of the current Interface status of the SG-1000
- **Authentication:** The Authentication information of SG-1000
- **ARP Table:** Record all the ARP that connect to the SG-1000
- **DHCP Clients:** Display the table of DHCP clients that are connected to the SG-1000.

19.1 Interface

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

- **PPPoE Con. Time:** The last time of the SG-1000 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, Web UI:** To display whether the users can Ping to the SG-1000 from the Interface or not; or enter its Web UI
- **Forwarding Mode:** The connection mode of the Interface
- **Connection Status:** To display the connection status of WAN
- **DnS/ UpS Kbps:** To display the Maximum DownStream/UpStream Bandwidth of that WAN (set from **Interface**)
- **DnStream Alloca.:** The distribution percentage of DownStream according to WAN traffic
- **UpStream Alloca.:** The distribution percentage of UpStream according to WAN traffic
- **Default Gateway:** To display the Gateway of WAN
- **DNS1:** The DNS1 Server Address provided by ISP
- **DNS2:** The DNS2 Server Address provided by ISP



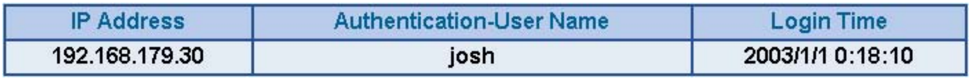
	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Static IP	Transparent
WAN Connection	---	🖧	🖧	---
Max. Downstream / Upstream	---	512 / 512 Kbps	50000 / 50000 Kbps	---
Downstream Alloca.	---	0%	100%	---
Upstream Alloca.	---	41%	58%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:e0:98:00:00:09	00:e0:98:00:00:0a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

Interface Status

19.2 Authentication

STEP 1 . Enter **Authentication** in **Status** function, it will display the record of login status:

- **IP Address:** The authentication user IP
- **Auth-User Name:** The account of the auth-user to login
- **Login Time:** The login time of the user (Year/Month/Day Hour/Minute/Second)



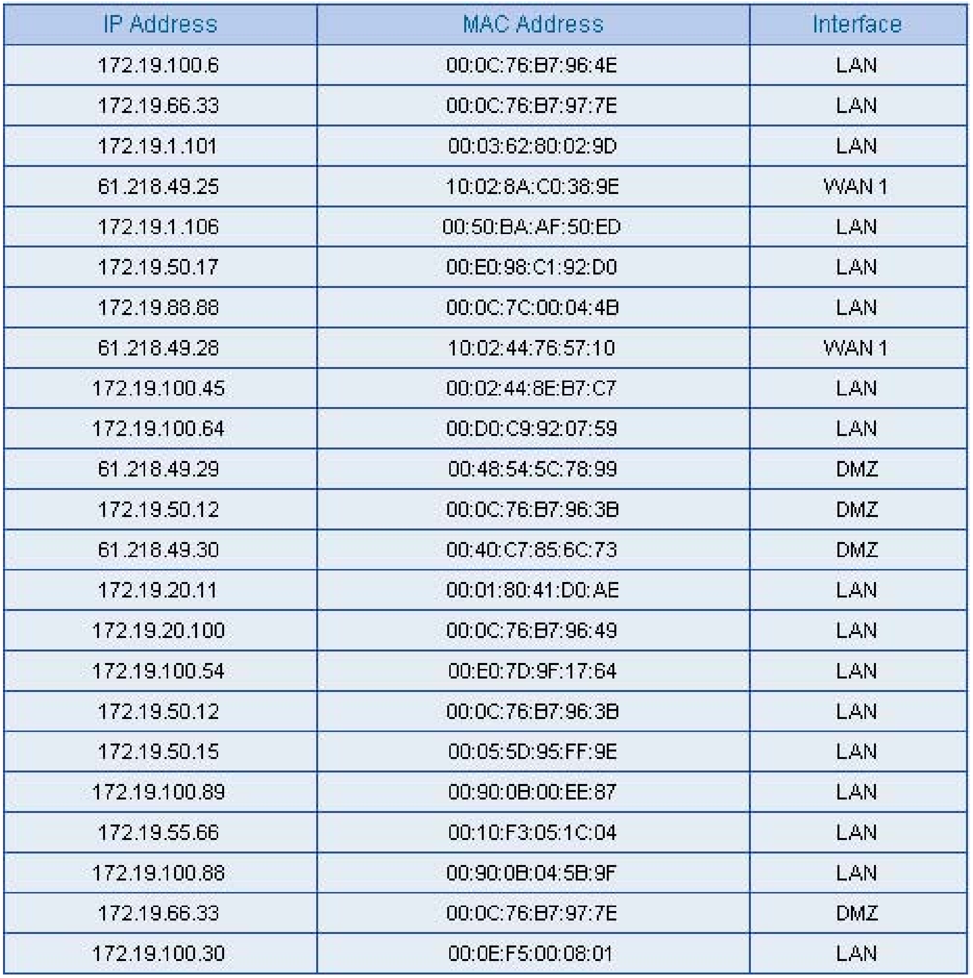
IP Address	Authentication-User Name	Login Time
192.168.179.30	josh	2003/1/1 0:18:10

Authentication Status Web UI

19.3 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 SG-1000:

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



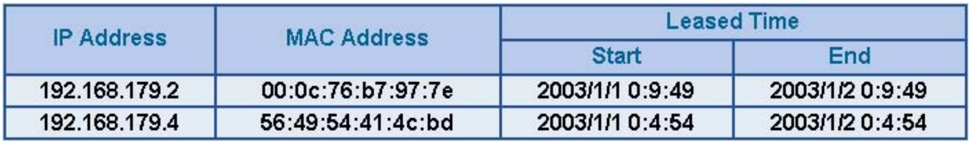
IP Address	MAC Address	Interface
172.19.100.6	00:0C:76:B7:96:4E	LAN
172.19.66.33	00:0C:76:B7:97:7E	LAN
172.19.1.101	00:03:62:80:02:9D	LAN
61.218.49.25	10:02:8A:C0:38:9E	WAN 1
172.19.1.106	00:50:BA:AF:50:ED	LAN
172.19.50.17	00:E0:98:C1:92:D0	LAN
172.19.88.88	00:0C:7C:00:04:4B	LAN
61.218.49.28	10:02:44:76:57:10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

ARP Table Web UI

19.4 DHCP Clients

STEP 1 . In **DHCP Clients** of **Status** function, it will display the table of DHCP Clients that are connected to the SG-1000:

- **IP Address:** The dynamic IP that provided by DHCP Server
- **MAC Address:** The IP that corresponds to the dynamic IP
- **Leased Time:** The valid time of the dynamic IP (Start/End) (Year/Month/Day/Hour/Minute/Second)



IP Address	MAC Address	Leased Time	
		Start	End
192.168.179.2	00:0c:76:b7:97:7e	2003/1/1 0:9:49	2003/1/2 0:9:49
192.168.179.4	56:49:54:41:4c:bd	2003/1/1 0:4:54	2003/1/2 0:4:54

DHCP Clients Web UI