



Multi-Homing Security Gateway CS-1000

User's Manual

Copyright

Copyright (C) 2006 PLANET Technology Corp. All rights reserved.

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 B 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 Multi-Homing 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:

- ◆ Multi-Homing 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 Multi-Homing Security Gateway

Model: CS-1000

Rev: 1.0 (April, 2006)

Part No. EM-CS1000v1

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 FEATURES	1
1.2 PACKAGE CONTENTS	2
1.3 MULTI-HOMING SECURITY GATEWAY FRONT VIEW	3
1.4 MULTI-HOMING SECURITY GATEWAY REAR PANEL	3
1.5 SPECIFICATION.....	3
CHAPTER 2: GETTING STARTED	5
2.1 WEB CONFIGURATION	5
2.2 CONFIGURE WAN1 INTERFACE.....	6
2.3 CONFIGURE WAN2 INTERFACE.....	7
2.4 CONFIGURE DMZ INTERFACE	7
2.5 CONFIGURE POLICY.....	8
CHAPTER 3: WEB CONFIGURATION	10
3.1 SYSTEM.....	10
3.1.1 Admin.....	11
3.1.2 Permitted IPs.....	13
3.1.3 Software Update	15
3.1.4 Setting	15
3.1.5 Date/Time.....	20
3.1.6 Multiple Subnet.....	21
3.1.7 Route Table.....	26
3.1.8 DHCP.....	27
3.1.9 Dynamic DNS.....	29
3.1.10 Host Table.....	31
3.1.11 Language	33
3.1.12 Logout	34
3.2 INTERFACE	34
3.2.1 LAN.....	34
3.2.2 WAN.....	35
3.2.3 DMZ.....	39
3.3 POLICY OBJECT	40
3.3.1 Address	40
3.3.1.1 LAN.....	40
3.3.1.2 LAN Group.....	42

3.3.1.3 WAN.....	45
3.3.1.4 WAN Group.....	47
3.3.1.5 DMZ.....	50
3.3.1.6 DMZ Group.....	52
3.3.2 Service.....	54
3.3.2.1 Pre-defined.....	55
3.3.2.2 Custom.....	56
3.3.2.3 Group.....	58
3.3.3 Schedule.....	60
3.3.4 QoS.....	62
3.3.5 Authentication.....	66
3.3.5.1 Auth Setting.....	66
3.3.5.2 Auth User.....	67
3.3.5.3 Auth Group.....	70
3.3.5.4 Radius Serve.....	73
3.3.5.5 POP3.....	74
3.3.6 Content Blocking.....	75
3.3.6.1 URL Blocking.....	75
3.3.6.2 Scripts.....	77
3.3.6.3 P2P.....	78
3.3.6.4 IM.....	79
3.3.6.5 Download.....	79
3.3.6.6 Upload.....	80
3.3.7 Virtual Server.....	81
3.3.7.1 Mapped IP.....	82
3.3.7.2 Virtual Server.....	84
3.3.8 VPN.....	89
3.3.8.1 IPSec Autokey.....	89
3.3.8.2 PPTP Server.....	92
3.3.8.3 PPTP Client.....	95
3.3.8.4 Trunk.....	97
3.4 POLICY.....	158
3.4.1 Outgoing.....	158
3.4.2 Incoming.....	162
3.4.3 WAN To DMZ & LAN To DMZ.....	166
3.4.4 DMZ To WAN & DMZ To LAN.....	169
3.5 MAIL SECURITY.....	173
3.5.1 Configure.....	174
3.5.2 Anti-Spam.....	177

3.5.2.1 Setting.....	178
3.5.2.2 Rule	179
3.5.2.3 Whitelist.....	182
3.5.2.4 Blacklist.....	184
3.5.2.5 Training.....	187
3.5.2.6 Spam Mail.....	193
3.5.3 Anti-Virus.....	193
3.5.3.1 Setting.....	193
3.5.3.2 Virus Mail.....	194
3.6 IDP.....	195
3.6.1 Setting	195
3.6.2 Signature.....	196
3.6.3 IDP Report.....	199
3.7 ANOMALY FLOW IP	200
3.8 MONITOR.....	201
3.8.1 Log.....	201
3.8.1.1 Traffic.....	201
3.8.1.2 Event	203
3.8.1.3 Connection	205
3.8.1.4 Log Backup.....	206
3.8.2 Accounting Report.....	208
3.8.2.1 Setting.....	208
3.8.2.2 Outbound.....	209
3.8.2.3 Inbound.....	212
3.8.3 Statistic.....	214
3.8.3.1 WAN Statistics.....	215
3.8.3.2 Policy Statistics.....	216
3.8.4 Status.....	217
3.8.4.1 Interface Status.....	217
3.8.4.2 Authentication.....	218
3.8.4.3 ARP Table.....	219
3.8.4.4 DHCP Clients	219

Chapter 1: Introduction

Thank you for purchasing new model of Planet's Security Gateway CS-1000, a special designed of security gateway, adopts Heuristics Analysis to filter spam and virus mail, auto-training system can raise identify rate of spam, and built-in Clam virus scan engine can detect viruses, worms and other threats from email transfer.

CS-1000 does not just provide the same feature as the previous generation product CS-500, such as Content Blocking to block specific URL, Scripts, IM/P2P program, IPSec and PPTP VPN server, QoS, Authentication etc. Built-in two WAN interfaces allow CS-1000 to support outbound load balance and wan fail-over feature. Furthermore, the VPN Trunk provides VPN fail-over and load balance features, that can offer a VPN redundant mechanism to keep your VPN connection being on line.

CS-1000 not only can filter spam and virus mail, but also is a high performance VPN firewall. Moreover, built-in IDP and firewall function can defense hacker and blaster attack from Internet or Intranet. The completely function in one device can provide you an excellent security solution and the secure environment than ever.

1.1 Features

- ◆ **Anti-Spam Filtering:** Multiple defense layers (Head Analysis, Text Analysis, Blacklist & Whitelist, Bayesian Filtering, Spam Fingerprint, Checking sender account and IP address), and Heuristics Analysis to block over 95% spam mail. Customizable notification options and spam mail report are provided for administrator. Varied actions toward spam mail include: Delete, Deliver, and Forward. Built-in auto-training system to rise identify rate of spam mail substantially.
- ◆ **Anti-Virus Protection:** Built-in Clam virus scan engine can detect viruses, worms, and other threats from email transfer. Scan mission-critical content protocols-SMTP, POP3 in real time as traffic enters the network to provide maximum protection. Customizable notification options and virus mail report are provided for administrator. Varied actions toward spam mail include: Delete, Deliver, and Forward.
- ◆ **VPN Connectivity:** The security gateway support PPTP server/client and IPSec VPN. With 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, CS-1000 will detect the difference and update the Content Filtering pattern to renew the filtering mechanism.

- ◆ **IDP:** CS-1000 provides three kinds of the Signature to complete the intrusion detection system, user can select to configure “**Anomaly**”, “**Pre-defined**” and “**Custom**” according to the current environment's request.
- ◆ **Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS:** The CS-1000 not only can provide Anti-virus feature for mail, it also can filter the virus from varied protocol. The virus pattern can be updated automatically or manually.
- ◆ **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:** You can control the outbound and inbound Upstream/Downstream Bandwidth by configuring the QoS based on the WAN bandwidth.
- ◆ **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 CS-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.

1.2 Package Contents

The following items should be included:

CS-1000

- CS-1000 x 1
- Power Adapter x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Console cable x 1
- RJ-45 cable
- Rack-mount ear

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

1.3 Multi-Homing Security Gateway Front View

CS-1000 Front Panel



LED	Description	
PWR	Power is supplied to this device.	
STATUS	Blinks to indicate this device 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

1.4 Multi-Homing Security Gateway Rear Panel

CS-1000 Rear Panel



1.5 Specification

Product		Multi-Homing Security Gateway
Model		CS-1000
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
Power		100~250 VAC, 50~60 Hz, 0.6A
Operating Environment		Temperature: 0~60°C Relative Humidity: 5%~95%
Dimension W x D x H, mm		237 x 440 x 43
Regulatory		FCC, CE Mark
Software		
Management		Web

Network Connection	Transparent mode (WAN to DMZ), NAT, Multi-NAT
Routing Mode	Static Route, RIPv2
Concurrent Sessions	110,000
New session / second	10,000
Email Capacity per Day	120,000
Firewall Throughout	100Mbps
3DES Throughout	17Mbps
Firewall	Policy-based firewall rule with schedule, NAT/NAPT, SPI firewall
VPN Tunnels	100/200
VPN Function	PPTP server and client, IPSec DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN VPN Trunk
Content Filtering	URL Blocking Blocks Popup, Java Applet, cookies and Active X P2P Application Blocking Instant Message Blocking Download Blocking
IDP	Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS Automatic or manual update virus and signature database Anomaly: Syn Flood, UDP Flood, ICMP Flood and more. Pre-defined : Backdoor, DDoS, DoS, Exploit, NetBIOS and Spyware. Custom: User defined based on TCP, UDP, ICMP or IP protocol.
Scanning Mail Settings	The allowed size of scanned mail: 10 ~ 512Kbytes
Anti-Virus	Email attachment virus scanning by SMTP, POP3 Inbound scanning for internal and external Mail Server Action of infected mail: Delete, Deliver to the recipient, forward to an account Automatic or manual update virus database
Anti-Spam	Inbound scanning for external and internal Mail Server Support Spam Fingerprint, Bayesian filtering, checking sender account and IP to filter the spam mail Black list and white list support auto training system Action of spam mail : Delete, Deliver to the recipient, forward to an account
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 statistics for WAN interface and policies Graphic display
Others	Dynamic DNS, NTP, DHCP server, Virtual server,

Chapter 2: Getting Started

2.1 Web Configuration

STEP 1:

Connect both the Administrator's PC and the LAN port of the Multi-Homing Security Gateway to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Multi-Homing Security Gateway has an embedded web server used for management and configuration. Use a web browser to display the configurations of the Multi-Homing Security Gateway (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of the Multi-Homing Security Gateway is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2– 192.168.1.254

If the company's LAN IP Address is not subnet of 192.168.1.0, (i.e. LAN IP Address is 172.16.0.1), then the Administrator must change his/her PC IP address to be within the same range of the LAN subnet (i.e. 172.16.0.2). Reboot the PC if necessary.

By default, the Multi-Homing Security Gateway is shipped with its DHCP Server function enabled. This means the client computers on the LAN network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the Multi-Homing Security Gateway.

STEP 2:

Once the Administrator PC has an IP address as the same network as the Multi-Homing Security Gateway, open up an Internet web browser and type in <http://192.168.1.1> in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required to connect to the Multi-Homing Security Gateway. Enter the default login username and password of Administrator (see below).

Username: admin

Password: admin

Click OK.



2.2 Configure WAN1 interface

After entering the username and password, the Multi-Homing Security Gateway WEB UI screen will display.

Select the **Interface** tab on the left menu then click on WAN below it.

Click on Modify button of WAN NO.1. The following page is shown.

Planet Networking & Communication

Interface > WAN

System

Interface

LAN

WAN

DMZ

Policy Object

Policy

Mail Security

IDP

Anomaly Flow IP

Monitor

WAN1 Interface

Service : DNS DNS Server IP Address : Assist

Domain name : Assist

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

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

IP Address

Netmask

Default Gateway

DNS Server 1

DNS Server 2

Max. Downstream Bandwidth Kbps (Max. 50 Mbps)

Max. Upstream Bandwidth Kbps (Max. 50 Mbps)

Enable ☐ Ping ☐ HTTP

OK Cancel

Alive Indicator Site IP: This feature is used to ping an address for detecting WAN connection status.

Service: ICMP You can select an IP address by **Assist**, or type an IP address manually.

Service: DNS You can select a DNS IP and Domain name by **Assist**, or type the related data manually.

PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect.

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Service-On-Demand:

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

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

MAC Address: This is the MAC Address of the device. Some ISPs require specified MAC address. If the required MAC address is your PC's, click **Clone MAC Address**.

Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: You can specify your own domain name or leave it blank.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN port of the device.

Netmask: This will be the Netmask of the WAN network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP Address of the DNS server.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the WAN network.

HTTP: Select this will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.


2.3 Configure WAN2 interface

If you want to connect WAN 2 to another ISP connection, click **Modify** button of **WAN No. 2** then repeat above procedures to setup.

2.4 Configure DMZ interface

Depends on your network requirement, you can disable the DMZ port, make DMZ port transparent to WAN or enable NAT function on it.

To configure the DMZ port, select the **Interface** tab on the left menu, then click on DMZ, the following page is shown.



Interface > DMZ

- System
- Interface
 - LAN
 - WAN
 - DMZ
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor

DMZ Interface	Disable	
IP Address	Disable	.0.0
Netmask	NAT	.0.0
	DMZ_TRANSPARENT	.0.0

☐ Enable
 ☐ Ping
 ☐ HTTP

OK Cancel

2.5 Configure Policy

STEP 1:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** (LAN to WAN) from the sub-function list.

STEP 2:

Click on **New Entry** button.

STEP 3:

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


Source Address – select “**Inside_Any**”

Destination Address – select “**Outside_Any**”

Service - select “**ANY**”

Action - select “**Permit, ALL**”

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



Policy > Outgoing

- System
- Interface
- Policy Object
- Policy
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor

Comment :

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None

OK Cancel

STEP 4:

The configuration is successful when the screen below is displayed.



The screenshot displays the PLANET Multi-Homing Security Gateway configuration interface. The top navigation bar shows "Policy > Outgoing". On the left, a sidebar menu lists various configuration sections: System, Interface, Policy Object, Policy (selected), Mail Security, IDP, Anomaly Flow IP, and Monitor. Under the "Policy" section, a tree view shows "Outgoing" selected, with sub-items: Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, and DMZ To LAN. The main content area displays a table with the following data:

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

Below the table, there is a "New Entry" button.

Please make sure that all the computers connected to LAN port must set their Default Gateway IP Address to the Multi-Homing Security Gateway's LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately. If a Multi-Homing Security Gateway filter function is required, please refer to the Policy section in chapter 3.

Chapter 3: Web Configuration

3.1 System

The Multi-Homing Security Gateway Administration and monitoring configuration is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

1. Add and change the sub Administrator's names and passwords;
2. Back up all Multi-Homing Security Gateway settings into local files;

"System" is the managing of settings such as the privileges of packets that pass through the Multi-Homing Security Gateway and monitoring controls. Administrators may manage, monitor, and configure Multi-Homing Security Gateway settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the Multi-Homing Security Gateway.

System setting can divide into two parts: **Administration**, **Configure** and **Logout**.

Administration:

Admin: controls user access right to the Multi-Homing Security Gateway. User can add/remove users and change passwords.

Permitted IPs: Enables the Administrator to authorize specific internal/external IP address(es) for gateway managing.

Software Update: The administrator can update the device's software with the latest version downloaded from Planet's website, in order to optimize the performance and keep up with the latest fixes for intruding attacks.

Configure:

Setting: The Administrator may use this function to backup Multi-Homing Security Gateway configurations and export (save) them to a computer; or restore a configuration file to the device; or reset the Multi-Homing Security Gateway back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the Multi-Homing Security Gateway has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP (Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.

Date/Time: This function enables the Multi-Homing Security Gateway to be synchronized based on an Internet Time Server or with the client computer's clock.

Multiple Subnet: This function allows local port to be set with multiple IP subnet, and allow all clients connecting to the internet via WAN IP Address.

Route Table: Use this function to configure static route for the networks when the dynamic route is not efficient enough.

DHCP: Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Dynamic DNS: The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.

Host Table: The Multi-Homing Security Gateway Administrator may use the Host Table function to make the Multi-Homing Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then to come back through the Multi-Homing Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one. This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up Host Table so all the LAN network computers will use the Multi-Homing Security Gateway as a DNS server, which acts as the DNS Proxy.

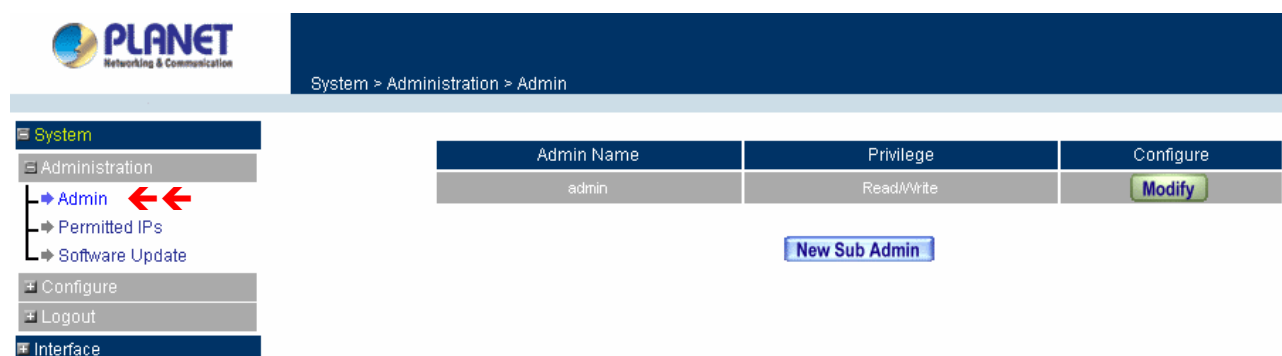
Language: Both Chinese and English are supported in the Multi-Homing Security Gateway.

Logout:

Logout: Administrator logs out the Multi-Homing Security Gateway. This function protects your system while you are away.

3.1.1 Admin

On the left hand menu, click on **Administration**, and then select **Admin** below it. The current list of Administrator(s) shows up.



The screenshot shows the Planet Security Gateway web interface. The top navigation bar includes the Planet logo and the breadcrumb path: System > Administration > Admin. On the left, a sidebar menu shows 'System' expanded, with 'Administration' selected, and 'Admin' highlighted with red arrows. The main content area displays a table of administrators.

Admin Name	Privilege	Configure
admin	Read/Write	Modify

Below the table is a button labeled 'New Sub Admin'.

Settings of the Administration table

Admin Name: The username of Administrators for the Multi-Homing Security Gateway. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)

The username of the main Administrator is **Admin** with **read / write** privilege.

Sub Admin may be created by clicking **New Sub Admin**. Sub Admin have **read only** privilege.

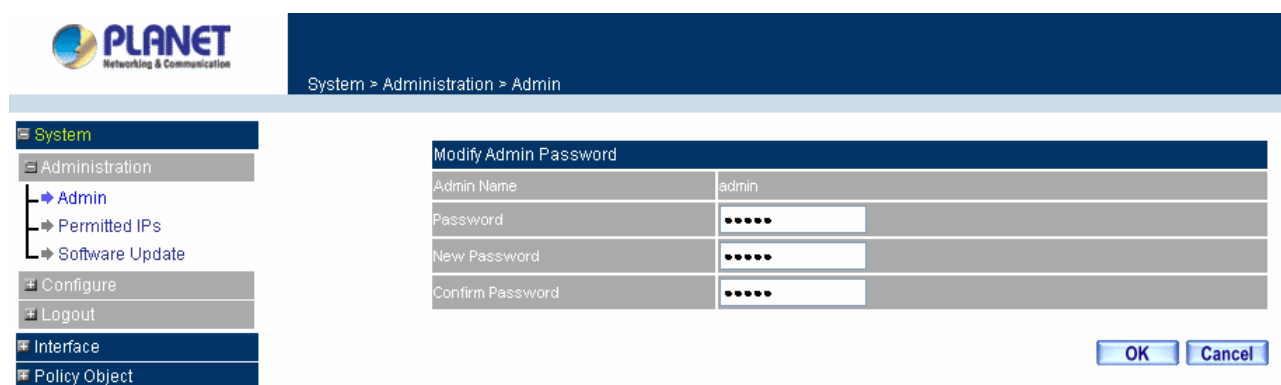
Configure: Click **Modify** to change the “Sub Admin” password and click **Remove** to delete a “Sub Admin”.

Changing the Main/Sub-Admin's Password

Step 1. The **Modify Admin Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.



The screenshot shows the Planet Network Administration web interface. The top navigation bar includes the Planet logo and the breadcrumb 'System > Administration > Admin'. A left sidebar contains a tree view with 'System' expanded, showing 'Administration' (with 'Admin' selected), 'Permitted IPs', 'Software Update', 'Configure', and 'Logout'. Below this are 'Interface' and 'Policy Object'. The main content area displays the 'Modify Admin Password' form. The form has four fields: 'Admin Name' (pre-filled with 'admin'), 'Password' (masked with dots), 'New Password' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom right of the form are 'OK' and 'Cancel' buttons.

Adding a new Sub Admin

Step 1. In the **Add New Sub Admin** window:

- **Sub Admin Name:** enter the username of new **Sub Admin**.
- **Password:** enter a password for the new **Sub Admin**.
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.

PLANET Networking & Communication

System > Administration > Admin

System

- Administration
 - Admin**
 - Permitted IPs
 - Software Update
- Configure
- Logout
- Interface

Add New Sub Admin

Sub Admin name	planet
Password	*****
Confirm Password	*****

OK Cancel

Removing a Sub Admin

- Step 1. In the Administration table, locate the Admin name you want to edit, and click on the **Remove** option in the Configure field.
- Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

PLANET Networking & Communication

System > Administration > Admin

System

- Administration
 - Admin**
 - Permitted IPs
 - Software Update
- Configure
- Logout
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP

Admin Name	Privilege	Configure
admin	Read/Write	Modify
planet	Read	Modify Remove

New Sub Admin

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

3.1.2 Permitted IPs

Only the authorized IP address is permitted to manage the Multi-Homing Security Gateway.

PLANET Networking & Communication

System > Administration > Permitted IPs

System

- Administration
 - Admin
 - Permitted IPs** ←←
 - Software Update
- Configure

Name	IP Address / Netmask	Ping	HTTP	Configure
------	----------------------	------	------	-----------

New Entry

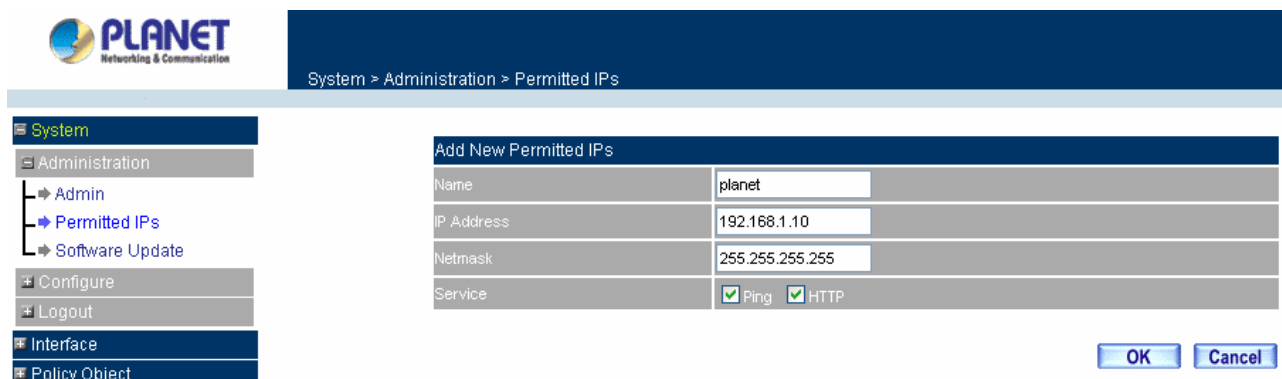
Add Permitted IPs Address

- Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **Name:** Enter the host name for the authorized IP address.
- **IP Address:** Enter the LAN IP address or WAN IP address.
- **Netmask:** Enter the netmask of LAN/WAN.
- **Ping:** Select this to allow the external network to ping the IP Address of the Firewall.
- **HTTP:** Check this item, Web User can use HTTP to connect to the Setting window of Multi-Homing Security Gateway.

Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.



The screenshot shows the Planet Network Administration interface. The left sidebar contains a tree view with 'System' expanded, showing 'Administration' > 'Permitted IPs'. The main area displays the 'Add New Permitted IPs' form. The form fields are: Name (planet), IP Address (192.168.1.10), Netmask (255.255.255.255), and Service (checked for Ping and HTTP). At the bottom right are 'OK' and 'Cancel' buttons.

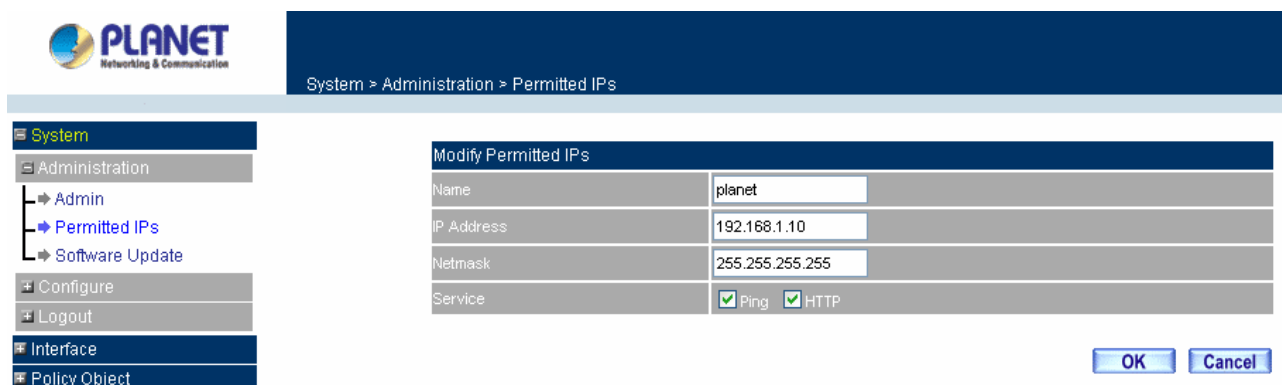
Add New Permitted IPs	
Name	planet
IP Address	192.168.1.10
Netmask	255.255.255.255
Service	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP

Modify Permitted IPs Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IPs**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.



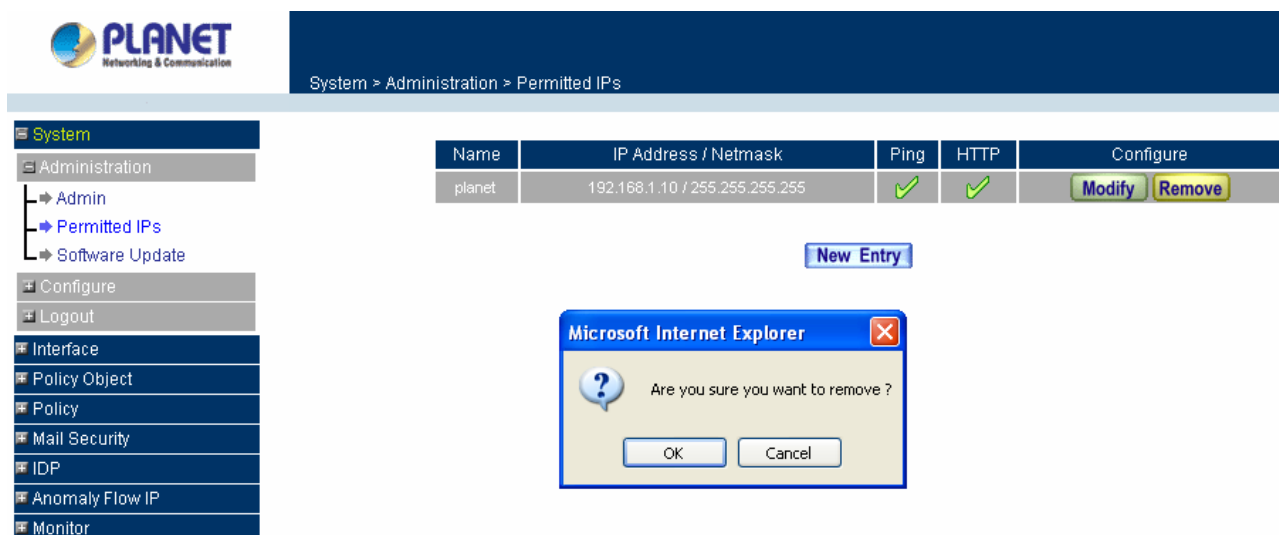
The screenshot shows the Planet Network Administration interface. The left sidebar contains a tree view with 'System' expanded, showing 'Administration' > 'Permitted IPs'. The main area displays the 'Modify Permitted IPs' form. The form fields are: Name (planet), IP Address (192.168.1.10), Netmask (255.255.255.255), and Service (checked for Ping and HTTP). At the bottom right are 'OK' and 'Cancel' buttons.

Modify Permitted IPs	
Name	planet
IP Address	192.168.1.10
Netmask	255.255.255.255
Service	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP

Remove Permitted IPs Addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.



System > Administration > Permitted IPs

Name	IP Address / Netmask	Ping	HTTP	Configure
planet	192.168.1.10 / 255.255.255.255	✓	✓	Modify Remove

New Entry

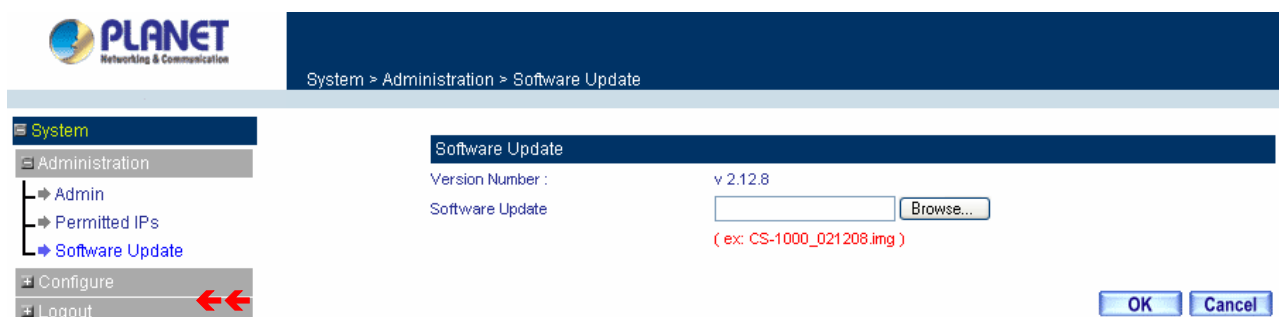
Microsoft Internet Explorer
Are you sure you want to remove ?
OK Cancel

3.1.3 Software Update

Under **Software Update**, the admin may update the device's software with newer software. You may acquire the current version number of software in **Version Number**. Administrators may visit Planet's website to download the latest version and save it in server's hard disk.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.



System > Administration > Software Update

Software Update

Version Number : v 2.12.8

Software Update [Browse...](#)
(ex: CS-1000_021208.img)

OK Cancel


NOTE: It takes three minutes to update the software. The system will restart automatically after updating the software.

3.1.4 Setting

The Administrator may use this function to backup Multi-Homing Security Gateway configurations and export (save) them to the "Administrator" computer or anywhere on the network; or restore a configuration file to the device; or restore the Multi-Homing Security Gateway back to default factory settings.

Entering the Settings window

Click **Setting** in the **Configure** menu to enter the **Settings** window. The **Setting** will be shown on the screen.



System > Configure > Setting

System
Administration
Configure
Setting
Date/Time
Multiple Subnet
Route Table
DHCP
Dynamic DNS
Host Table
Language
Logout
Interface
Policy Object
Policy
Mail Security
IDP
Anomaly Flow IP
Monitor

Backup / Restore Configuration

Export System Setting to Client [Download](#)

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

☐ Reset Factory Setting

System Name Setting

Device Name (ex: Multi-Homing Security Gateway)

E-mail Setting

☐ Enable E-mail Alert Notification

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

MTU Setting

MTU Bytes

Link Speed / Duplex Mode Setting

WAN1 ▼

WAN2 ▼

Dynamic Routing (RIPv2)

Enable ☐ LAN ☐ WAN1 ☐ WAN2 ☐ DMZ

Routing information update timer Seconds

Routing information timeout Seconds

To-Appliance Packets Log

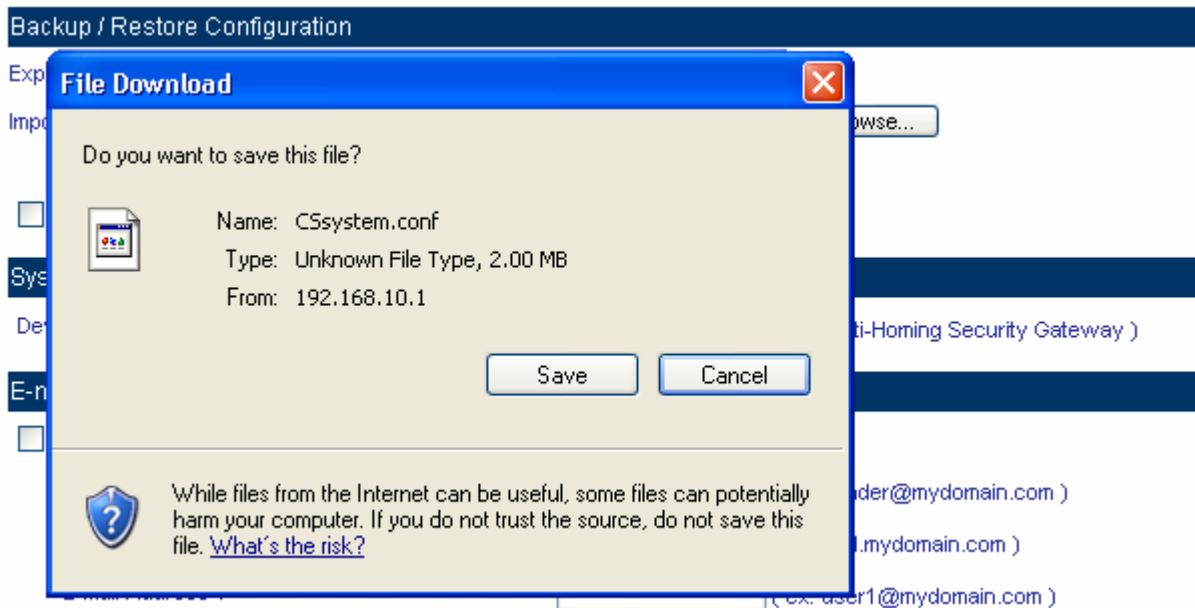
☒ Enable To-Appliance Packets Log

System Reboot

Reboot Multi-Homing Security Gateway Appliance [Reboot](#)

Exporting Multi-Homing Security Gateway settings

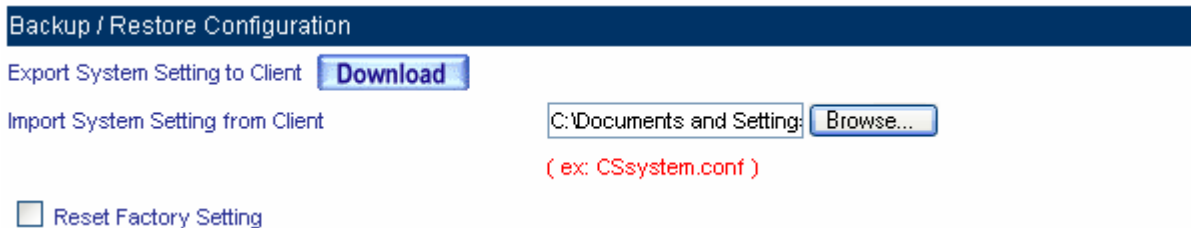
- Step 1. Under **Backup/Restore Configuration**, click on the **Download** button next to **Export System Settings to Client**.
- Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.



Importing Multi-Homing Security Gateway settings

Under **Backup/Restore Configuration**, click on the **Browse** button next to **Import System Settings from Client**. When the **Choose File** pop-up window appears, select the file which contains the saved Multi-Homing Security Gateway Settings, then click **OK**.

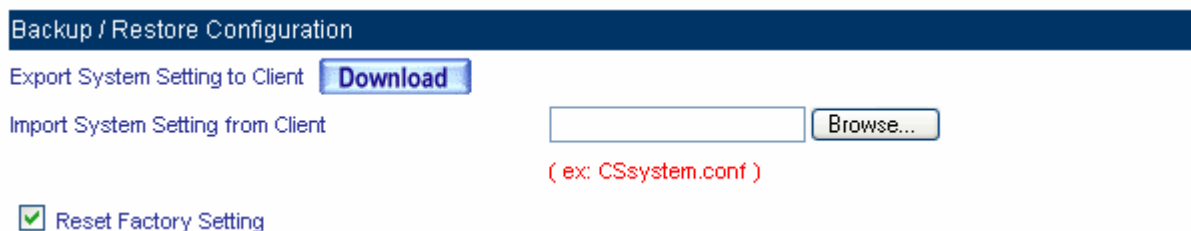
Click **OK** to import the file into the **Multi-Homing Security Gateway** or click **Cancel** to cancel importing.



Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Backup/Restore Configuration**.

Step 2. Click **OK** at the bottom-right of the screen to restore the factory settings.



System Name Setting

Input the name you want into **Device Name** column to be the device name.

Email Setting

Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Setting**. This function will enable the Multi-Homing Security Gateway to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Click **OK** on the bottom-right of the screen to enable E-mail alert notification.

Web Management (WAN Interface)

The administrator can change the port number used by HTTP port anytime. (Remote UI Management)

Step 1. **Set Web Management (WAN Interface).** The administrator can change the port number used by HTTP port anytime.

MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. **MTU Setting.** Modify the networking packet length.

Link Speed / Duplex Mode Setting

This function allows administrator to set the transmission speed and mode of WAN Port.

Link Speed / Duplex Mode Setting	
WAN1	Auto Mode
WAN2	Auto Mode
Dynamic Routing (RIPv2)	
Enable	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> DMZ
Routing information update timer	30 Seconds

Dynamic Routing (RIPv2)

Enable Dynamic Routing (RIPv2), CS-1000 will advertise an IP address pool to the specific network so that the address pool can be provided to the network. You can choose to enable LAN, WAN or DMZ interface to allow RIP protocol supporting.

Routing information update timer: CS-1000 will send out the RIP protocol in a period of time to update the routing table, the default timer is 30 seconds.

Routing information timeout: If CS-1000 does not receive the RIP protocol from the other router in a period of time, it will cut off the routing automatically until it receives RIP protocol again. The default timer is 180 seconds.

Dynamic Routing (RIPv2)	
Enable	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> DMZ
Routing information update timer	30 Seconds
Routing information timeout	180 Seconds

To-Appliance Packet Logging

When the function is selected, the CS-1000 will record the packets that contain the IP address of CS-1000 in source or destination, the records will display in Traffic Log for administrator to inquire about.

To-Appliance Packets Log
<input checked="" type="checkbox"/> Enable To-Appliance Packets Log

System Reboot

Once this function is enabled, the Multi-Homing Security Gateway will be rebooted.

Reboot Appliance: Click **Reboot**.

A confirmation pop-up box will appear. Follow the confirmation pop-up box, click **OK** to restart Multi-Homing Security Gateway or click **Cancel** to discard changes.

The screenshot displays the configuration interface of a Multi-Homing Security Gateway. The interface is divided into several sections, each with a dark blue header. The sections visible are:

- MTU Setting:** Contains a label 'MTU' and a text input field with the value '1500' followed by the unit 'Bytes'.
- Link Speed / Duplex Mode Setting:** Contains labels 'WAN1' and 'WAN2', and a dropdown menu currently set to 'Auto Mode'.
- Dynamic Routing (RIPv2):** Contains an 'Enable' checkbox and three checkboxes for 'LAN', 'WAN1', and 'WAN2'. Below these are labels for 'Routing information update timer' and 'Routing information timeout'.
- To-Appliance Packets Log:** Contains a checked checkbox labeled 'Enable To-Appliance Packets Log'.
- System Reboot:** Contains the text 'Reboot Multi-Homing Security Gateway Appliance' and a blue 'Reboot' button.

A modal dialog box titled 'Microsoft Internet Explorer' is overlaid on the 'Dynamic Routing (RIPv2)' section. The dialog has a yellow background and a question mark icon. It contains the text 'Are you sure to Reboot ?' and two buttons at the bottom: 'OK' and 'Cancel'.

3.1.5 Date/Time

Synchronizing the Multi-Homing Security Gateway with the System Clock

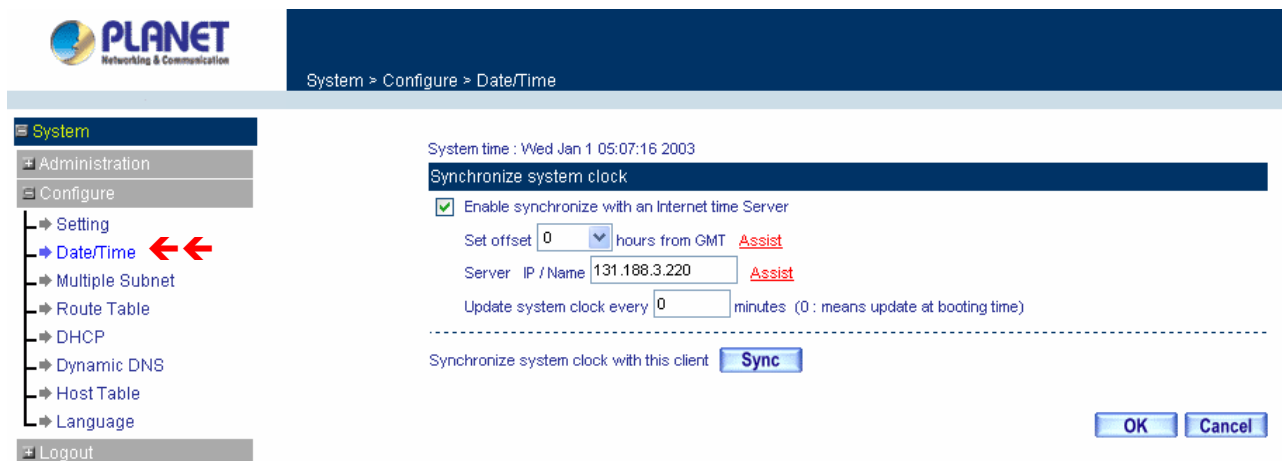
Administrator can configure the [Multi-Homing](#) Security Gateway's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

Follow these steps to sync to an Internet Time Server

- Step 1.** Enable synchronization by checking the box.
- Step 2.** Click the down arrow to select the offset time from GMT.
- Step 3.** Enter the Server IP Address or Server name with which you want to synchronize.
- Step 4.** **Update system clock every minutes** You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer's clock.

- Step 1.** Click on the **Sync** button.
- Click **OK** to apply the setting or click **Cancel** to discard changes.



The screenshot shows the PLANET System Configuration web interface. The breadcrumb path is "System > Configure > Date/Time". The left sidebar menu includes "System", "Administration", "Configure", "Setting", "Date/Time" (highlighted with red arrows), "Multiple Subnet", "Route Table", "DHCP", "Dynamic DNS", "Host Table", "Language", and "Logout". The main content area displays the system time as "Wed Jan 1 05:07:16 2003" and the "Synchronize system clock" section. This section includes a checked checkbox for "Enable synchronize with an Internet time Server", a "Set offset" of 0 hours from GMT, a "Server IP / Name" of 131.168.3.220, and an "Update system clock every" 0 minutes. There are "Assist" links for both the offset and server fields. A "Sync" button is present for synchronizing with the client. At the bottom right are "OK" and "Cancel" buttons.

3.1.6 Multiple Subnet

NAT mode

Multiple Subnet allows local port to set multiple subnet works and connect with the Internet through WAN IP Addresses.

For instance, 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 works for the purpose of convenient management. The settings are as the following:

1. R&D department sub-network: 192.168.1.11/24 (LAN) \leftrightarrow 168.85.88.253 (WAN)
2. Service department sub-network: 192.168.2.11/24 (LAN) \leftrightarrow 168.85.88.252 (WAN)
3. Sales department sub-network: 192.168.3.11/24 (LAN) \leftrightarrow 168.85.88.251 (WAN)
4. Procurement department sub-network: 192.168.4.11/24 (LAN) \leftrightarrow 168.85.88.250 (WAN)
5. Accounting department sub-network: 192.168.5.11/24 (LAN) \leftrightarrow 168.85.88.249 (WAN)

The first department (R&D department) was set while setting interface IP, the other four ones have to be added in Multiple Subnet, after completing the settings, each department use the different WAN IP address to connect to the internet. The settings of LAN computers on Service department are as the following:

Service IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.11

The other departments are also set by groups, this is the function of Multiple Subnet.

Multiple Subnet settings

Click **System** on the left side menu bar, select **Configure** then click **Multiple Subnet** to enter Multiple Subnet window.

System > Configure > Multiple Subnet

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
168.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	Modify Remove

[New Entry](#)

Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP address and Forwarding Mode.

Interface: Indicate the multiple subnet location in LAN or DMZ site.

Alias IP of Interface / Netmask: Local port IP address and subnet Mask.

Configure: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click Delete to delete settings.

Add a Multiple Subnet NAT Mode.

Step 1: Click the **New Entry** button below to add Multiple Subnet.

Step 2: Enter the IP address in the website name column of the new window.

Alias IP of Interface: Enter Local port IP address.

Netmask: Enter Local port subnet Mask.

WAN Interface IP: Add WAN IP.

Forwarding Mode: Click the NAT button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.

System > Configure > Multiple Subnet

Add New Multiple Subnet IP

Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
Alias IP of Interface	192.168.2.1	
Netmask	255.255.255.0	

WAN Interface IP		Forwarding Mode
WAN	168.85.88.252 Assist	<input checked="" type="radio"/> NAT <input type="radio"/> Routing


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

Modify a Multiple Subnet

Step 1: Find the IP address you want to modify and click Modify.

Step 2: Enter the new IP address in Modify Multiple Subnet window.

Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



System > Configure > Multiple Subnet

System
Administration
Configure
Setting
Date/Time
Multiple Subnet
Route Table
DHCP
Dynamic DNS
Host Table
Language
Logout

Modify Multiple Subnet IP


Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
Alias IP of Interface	<input type="text" value="192.168.2.1"/>	
Netmask	<input type="text" value="255.255.255.0"/>	

WAN Interface IP		Forwarding Mode
WAN	<input type="text" value="168.85.88.252"/> Assist	<input checked="" type="radio"/> NAT <input type="radio"/> Routing

Removing a Multiple Subnet

Step 1: Find the IP address you want to delete and click Delete.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



System > Configure > Multiple Subnet

System
Administration
Configure
Setting
Date/Time
Multiple Subnet
Route Table
DHCP
Dynamic DNS
Host Table
Language
Logout
Interface

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
168.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Microsoft Internet Explorer

Are you sure you want to remove ?

Routing Mode

Multiple Subnet allows local port to set Multiple Subnet Routing Mode and connect with the Internet through WAN IP address.

For example, the leased line of a company applies several real IP Addresses 168.85.88.0/24 and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. The company can distinguish each department by different sub-network for the purpose of convenient management.

The settings are as the following:

R&D: Alias IP of LAN interface - 168.85.88.1, Netmask: 255.255.255.192

Sales: Alias IP of LAN interface - 168.85.88.65, Netmask: 255.255.255.192

Procurement: Alias IP of LAN interface - 168.85.88.129, Netmask: 255.255.255.192

Accounting: Alias IP of LAN interface - 168.85.88.193, Netmask: 255.255.255.192

Click System on the left side menu bar, then click Multiple Subnet below Configure menu. Enter Multiple Subnet window.

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
--- / Routing	LAN	168.85.88.1 / 255.255.255.192	Modify Remove

New Entry

Multiple Subnet functions

WAN Interface IP / Forwarding Mode: Display WAN Port IP address and Forwarding Mode which is NAT Mode or Routing Mode.

Interface: Indicate the multiple subnet location in LAN or DMZ site.

Alias IP of Interface / Netmask: Local port IP address and subnet Mask.

Configure: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click Delete to delete settings.

Adding a Multiple Subnet Routing Mode

Step 1: Click the Add button below to add Multiple Subnet.

Step 2: Enter the IP address in Add Multiple Subnet window.

Alias IP of Interface: Enter Local port IP Address.

Netmask: Enter Local port subnet Mask.

WAN Interface IP: Add WAN IP

Forwarding Mode: Click the Routing button below to setup.

Step 3: Click OK to add Multiple Subnet or click Cancel to discard changes.

WAN Interface IP		Forwarding Mode
WAN	0.0.0.0 Assist	NAT Routing

OK Cancel

Step 4: Adding a new WAN to LAN Policy. In the Incoming window, click the New Entry button.



Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▼


- System
- Interface
- Policy Object
- Policy
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ

Modify a Multiple Subnet Routing Mode

Step 1: Find the IP address you want to modify in Multiple Subnet menu, then click Modify button, on the right side of the service providers, click OK.

Step 2: Enter the new IP address in Modify Multiple Subnet window.

Step 3: Click the OK button below to change the setting or click Cancel to discard changes.



System > Configure > Multiple Subnet

- System
- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Logout

Modify Multiple Subnet IP

Interface: ☒ LAN ☐ DMZ

Alias IP of Interface:


Netmask:

WAN Interface IP		Forwarding Mode
WAN	<input type="text" value="0.0.0.0"/> <input type="button" value="Assist"/>	<input type="radio"/> NAT <input checked="" type="radio"/> Routing

Removing a Multiple Subnet Routing Mode

Step 1: Find the IP Address you want to delete in Multiple Subnet menu, then click Delete button, on the right side of the service providers, click OK.

Step 2: A confirmation pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.



System > Configure > Multiple Subnet

- System
- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Logout
- Interface

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
--- / Routing	LAN	168.85.88.1 / 255.255.255.192	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Microsoft Internet Explorer

Are you sure you want to remove ?

3.1.7 Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen

- Step 1. Click **System** on the left hand side menu bar, then click **Route Table** below the **Configure** menu. The Route Table window appears, in which current route settings are shown.

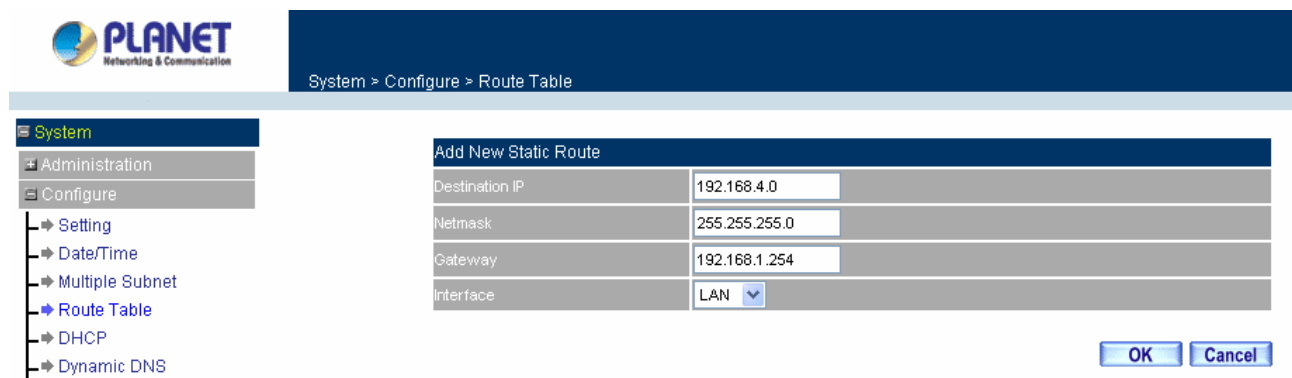


Route Table functions

- **Interface:** Destination network, LAN or WAN networks.
- **Destination IP / Netmask:** IP address and subnet mask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

Adding a new Static Route

- Step 1. In the Route Table window, click the **New Entry** button.
- Step 2. In the Add New Static Route window, enter new static route information.
- Step 3. In the Interface field's pull-down menu, choose the network to connect (LAN, WAN, DMZ).
- Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.



Modifying a Static Route:

- Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the

Configure field.

Step 2. In the **Modify Static Route** window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

PLANET Networking & Communication

System > Configure > Route Table

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table**
 - DHCP
 - Dynamic DNS

Modify Static Route

Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN

OK Cancel

Removing a Static Route

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.

PLANET Networking & Communication

System > Configure > Route Table

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table**
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Logout
- Interface

Interface	Destination IP / Netmask	Gateway	Configure
LAN	192.168.4.0 / 255.255.255.0	192.168.1.254	Modify Remove

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

3.1.8 DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN network.

Entering the DHCP window

Click **System** on the left hand side menu bar, then to click **DHCP** below the **Configure** menu. The DHCP window appears in which current DHCP settings are shown on the screen.



System > Configure > DHCP

System		Dynamic IP Address	
Administration		Subnet	192.168.1.0
Configure		Netmask	255.255.255.0
Setting		Gateway	192.168.1.1
Date/Time		Broadcast	192.168.1.255
Multiple Subnet			
Route Table			
DHCP			
Dynamic DNS			
Host Table			
Language			
Logout			
Interface			
Policy Object			
Policy			
Mail Security			
IDP			
Anomaly Flow IP			
Monitor			

<input checked="" type="checkbox"/> Enable DHCP Support			
Domain Name	<input type="text"/> (ex: dhcp.domain_name)		
<input type="checkbox"/> Automatically Get DNS			
DNS Server 1	<input type="text"/> 192.168.1.1		
DNS Server 2	<input type="text"/>		
WINS Server 1	<input type="text"/>		
WINS Server 2	<input type="text"/>		
LAN Interface :			
Client IP Range 1	<input type="text"/> 192.168.1.2	To	<input type="text"/> 192.168.1.254
Client IP Range 2	<input type="text"/>	To	<input type="text"/>
DMZ Interface :			
Client IP Range 1	<input type="text"/> 192.168.10.2	To	<input type="text"/> 192.168.10.254
Client IP Range 2	<input type="text"/>	To	<input type="text"/>
Leased Time	<input type="text"/> 24	hours	

Dynamic IP Address functions

- **Subnet:** LAN network's subnet
- **Netmask:** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

Enabling DHCP Support

Step 1. In the Dynamic IP Address window, click **Enable DHCP Support**.

Domain Name: The Administrator may enter the name of the LAN network domain if preferred.

Automatically Get DNS: Check this box to automatically detect DNS server.

DNS Server 1: Enter the distributed IP address of DNS Server 1.

DNS Server 2: Enter the distributed IP address of DNS Server 2.

WINS Server 1: Enter the distributed IP address of WINS Server 1.

WINS Server 2: Enter the distributed IP address of WINS Server 2.

LAN interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

DMZ interface:

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

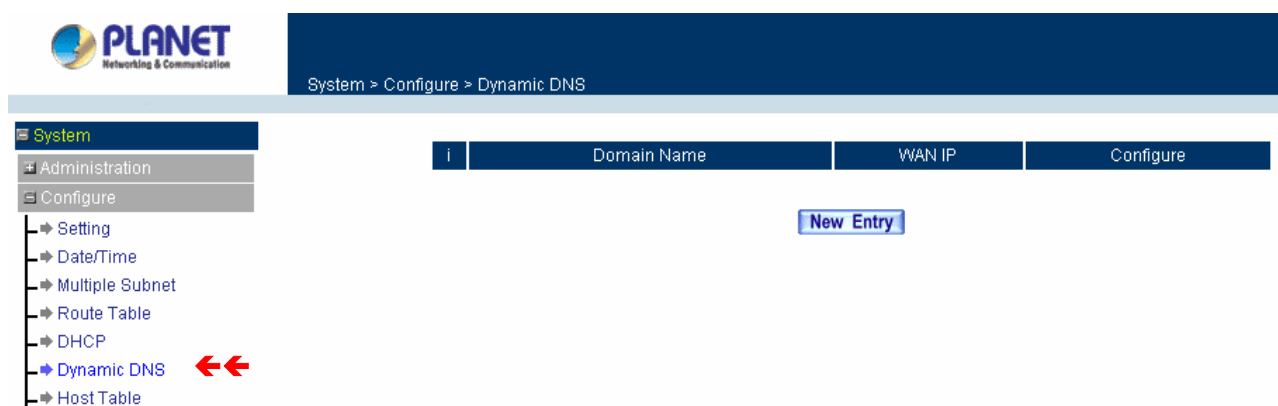
Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Leased Time: Enter the leased time for DHCP.

Step 2. Click **OK** to enable DHCP support.

3.1.9 Dynamic DNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.



Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window.

The icons in Dynamic DNS window:

!: Update Status, Connecting; Update succeed; Update fail; Unidentified error.

Domain name: Enter the password provided by ISP.

WAN IP Address: IP address of the WAN port.

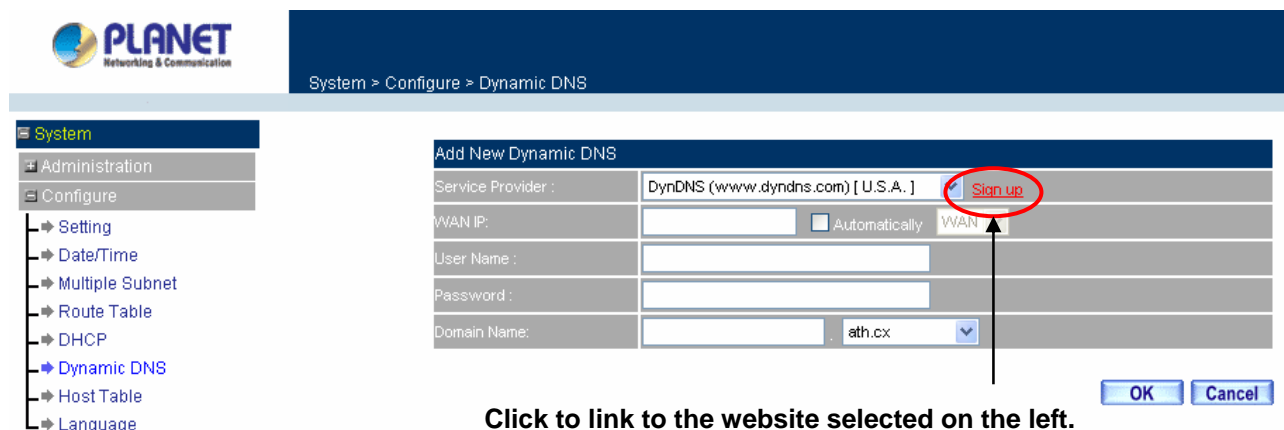
Configure: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

How to use dynamic DNS:

The Multi-Homing Security Gateway provides many service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

How to register:

Firstly, Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window, then click **Add** button on the right side of the service providers, click **Sign up**, the service providers' website will appear, please refer to the website for the way of registration.



System > Configure > Dynamic DNS

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS**
 - Host Table
 - Language

Add New Dynamic DNS

Service Provider : DynDNS (www.dyndns.com) [U.S.A.] [Sign up](#)

WAN IP: ☐ Automatically WAN

User Name :

Password :

Domain Name: ath.cx

Click to link to the website selected on the left.

OK Cancel

Add Dynamic DNS settings

Step 1. Click **Add** button.

Step 2. Click the information in the column of the new window.

Service providers: Select service providers.

Sign up: to the service providers' website.

WAN IP Address: IP Address of the WAN port.

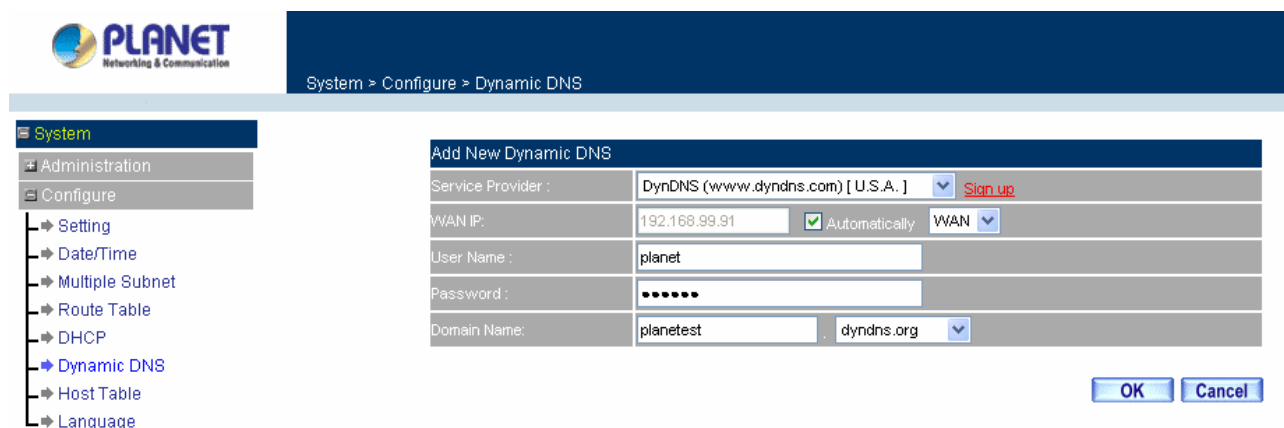
☐ **Automatically** : Check to automatically fill in the WAN IP.

User Name: Enter the registered user name.

Password: Enter the password provided by ISP (Internet Service Provider).

Domain name: Your host domain name provided by ISP.

Click **OK** to add dynamic DNS or click **Cancel** to discard changes.



System > Configure > Dynamic DNS

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS**
 - Host Table
 - Language

Add New Dynamic DNS

Service Provider : DynDNS (www.dyndns.com) [U.S.A.] [Sign up](#)

WAN IP: 192.168.99.91 ☒ Automatically WAN

User Name : planet

Password :

Domain Name: planetest dyndns.org


OK Cancel

Modify dynamic DNS

Step 1. Find the item you want to change and click **Modify**.

Step 2. Enter the new information in the Modify Dynamic DNS window.

Click **OK** to change the settings or click **Cancel** to discard changes.



System > Configure > Dynamic DNS

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS**
 - Host Table
 - Language

Modify Dynamic DNS

Service Provider : DynDNS (www.dyndns.com) [U.S.A.] [Sign up](#)

WAN IP: 192.168.99.91 ☒ Automatically WAN

User Name : planet


Password :

Domain Name: planetest dyndns.org

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

Remove Dynamic DNS


- Step 1. Find the item you want to change and click **Remove**.
- Step 2. A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.



System > Configure > Dynamic DNS

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS**
 - Host Table
 - Language
- Logout
- Interface

i	Domain Name	WAN IP	Configure
	planetest.dyndns.org	192.168.99.91	Modify Remove

[New Entry](#)

Microsoft Internet Explorer

Are you sure you want to remove ?

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

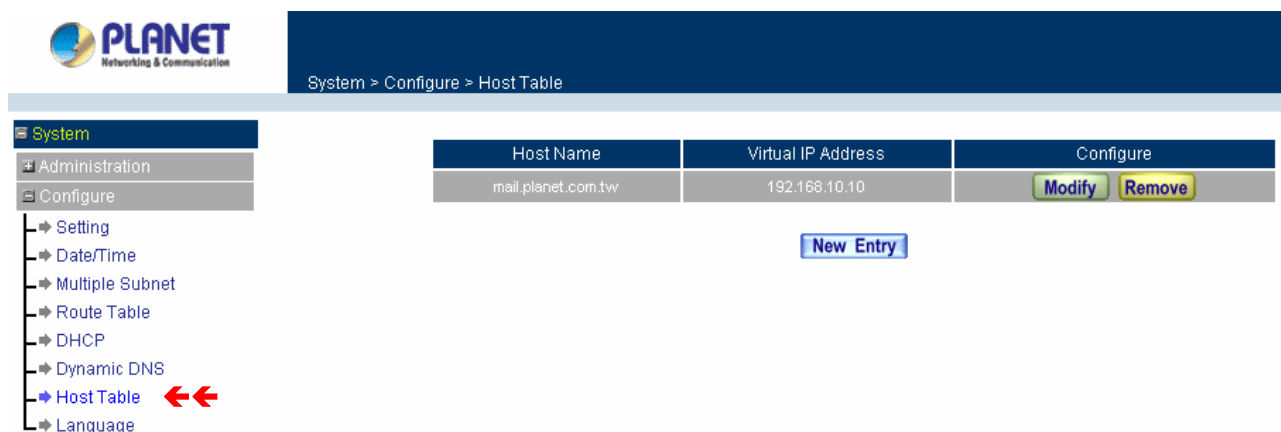
3.1.10 Host Table

The Multi-Homing Security Gateway's Administrator may use the Host Table function to make the Multi-Homing Security Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Multi-Homing Security Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw), they would have to go out to the Internet, then to come back through the Multi-Homing Security Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one.

This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up Host Table so all the LAN network computers will use the Multi-Homing Security Gateway as a DNS server, which acts as the DNS proxy.

If you want to use the Host Table function of the device, the end user's main DNS server IP address should be the same IP Address as the device.

Click on **System** in the menu bar, then to click on **Host Table** below the **Configure** menu. The Host Table window will appear.



Below is the information needed for setting up the **Host Table**:

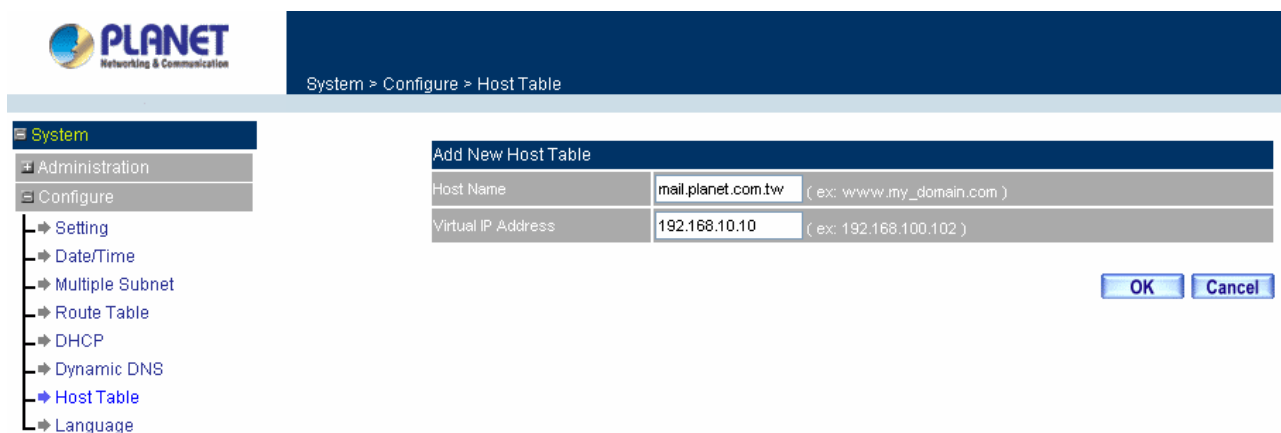
- **Host Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to Host Table
- **Configure:** modify or remove each Host Table policy

Adding a new Host Table

Step 1: Click on the **New Entry** button and the **Add New Host Table** window will appear.

Step 2: Fill in the appropriate settings for the domain name and virtual IP address.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.



Modifying a Host Table

- Step 1:** In the **Host Table** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.
- Step 2:** Make the necessary changes needed.
- Step 3:** Click **OK** to save changes or click on **Cancel** to cancel modifications.

The screenshot shows the Planet Networking & Communication web interface. The breadcrumb path is 'System > Configure > Host Table'. On the left is a navigation tree with 'System' expanded, showing 'Administration', 'Configure', and 'Interface'. Under 'Configure', 'Host Table' is selected. The main area displays the 'Modify Host Table' dialog box with two input fields: 'Host Name' (containing 'mail.planet.com.tw' with a hint '(ex: www.my_domain.com)') and 'Virtual IP Address' (containing '192.168.10.10' with a hint '(ex: 192.168.100.102)'). At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Removing a Host Table

- Step 1:** In the **Host Table** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.
- Step 2:** A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.

The screenshot shows the Planet Networking & Communication web interface. The breadcrumb path is 'System > Configure > Host Table'. On the left is a navigation tree with 'System' expanded, showing 'Administration', 'Configure', and 'Interface'. Under 'Configure', 'Host Table' is selected. The main area displays a table with columns 'Host Name', 'Virtual IP Address', and 'Configure'. The table contains one entry: 'mail.planet.com.tw' with '192.168.10.10'. In the 'Configure' column, there are 'Modify' and 'Remove' buttons. Below the table is a 'New Entry' button. A 'Microsoft Internet Explorer' confirmation dialog box is open in the foreground, asking 'Are you sure you want to remove?' with 'OK' and 'Cancel' buttons.

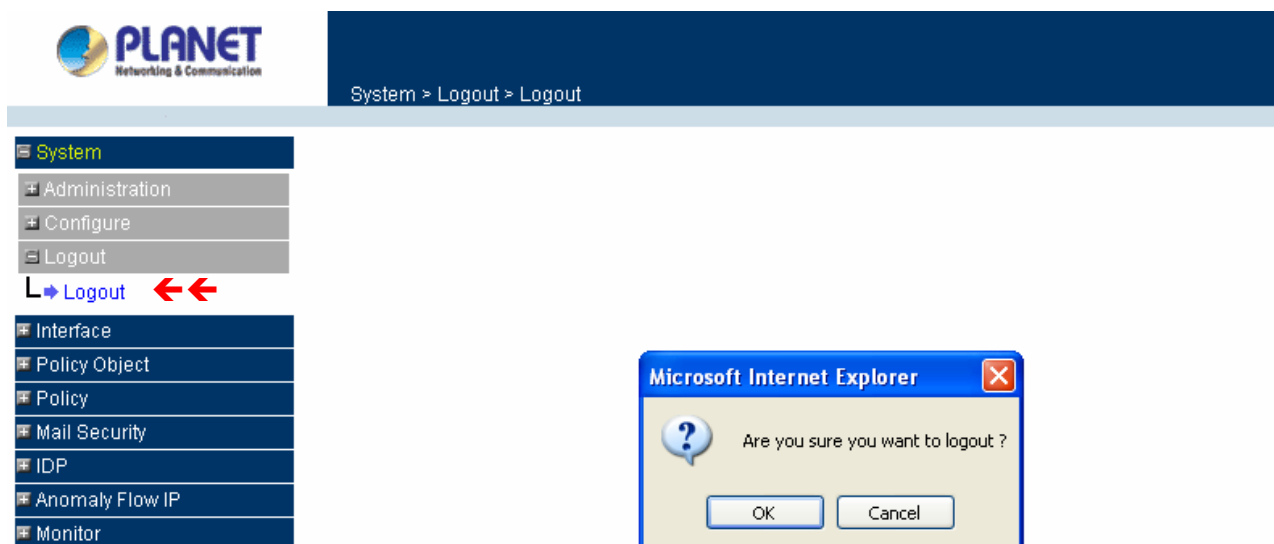
3.1.11 Language

Administrator can configure the Multi-Homing Security Gateway to select the Language version.

- Step 1. Select the Language version (**English Version**, **Traditional Chinese Version** or **Simplified Chinese Version**).
- Step 2. Click **[OK]** to set the Language version or click **Cancel** to discard changes.

3.1.12 Logout

- Step 1. Select this option to the device's **Logout** the Multi-Homing Security Gateway. This function protects your system while you are away.
- Step 2. Click Logout the Multi-Homing Security Gateway.
- Step 3. Click **OK** to logout or click **Cancel** to discard the change.



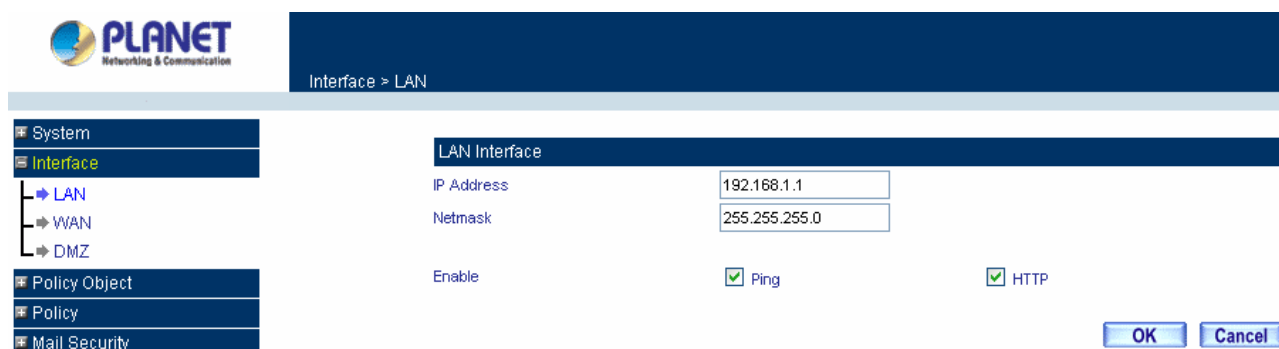
3.2 Interface

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 network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

3.2.1 LAN

Entering the Interface menu:

Click on **Interface** in the left menu bar. Then click on **LAN** below it. The current settings of the interface addresses will appear on the screen.



Configuring the Interface Settings

Using the LAN **Interface**, the Administrator sets up the LAN network. The LAN network will use a private IP scheme. The private IP network will not be routable on the Internet.

IP Address: The private IP address of the Multi-Homing Security Gateway's LAN network is the IP address of the LAN port of the device. The default IP address is 192.168.1.1. If the new LAN IP Address is not 192.168.1.1, the Administrator needs to set the IP Address on the computer to be the same subnet as the Multi-Homing Security Gateway and restart the System to make the new IP address effective. For example, if the Multi-Homing Security Gateway's new LAN IP Address is 172.16.0.1, then enter the new LAN IP Address 172.16.0.1 in the URL field of browser to connect to Multi-Homing Security Gateway.

NetMask: This is the subnet mask of the LAN network. The default netmask of the device is 255.255.255.0.

Ping: Select this to allow the LAN network to ping the IP Address of the Multi-Homing Security Gateway. If set to enable, the device will respond to ping packets from the LAN network.

HTTP: Select this to allow the device WEBUI to be accessed from the LAN network.

3.2.2 WAN

Entering the Interface menu

Click on Interface in the left menu bar. Then click on WAN below it. The current settings of the interface addresses will appear on the screen.

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Static IP	210.66.155.90	1	✓	✓	Modify	1
2	(Disable)	---	0	---	---	Modify	0

Balance Mode:

Auto: CS-1000 distributes the WAN 1/2 download by proportion automatically according to the WAN download bandwidth. (For users who are using various download bandwidth)

Round-Robin: CS-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: CS-1000 distributes the WAN 1/2 download bandwidth by traffic. (For users who are connected to the Internet via a fixed WAN IP address)

By Session: CS-1000 distributes the WAN 1/2 download bandwidth by session. (For users who are connected to the Internet via a fixed WAN IP address)

By Packet: CS-1000 distributes the WAN 1/2 download bandwidth by packet and saturated connection. (For users who are connected to the Internet via a fixed WAN IP address)

WAN No: WAN port 1 or 2.

Connect Mode: Display the current connection mode: PPPoE, Dynamic IP Address (Cable Modem User) or Static IP Address.

IP Address: Display the current WAN IP Address.

Saturated Connections: Set the number for saturation whenever session numbers reach it, the CS-1000 switches to the next WAN port on the list. This function is only applicable for **By Session** mode.

Ping / HTTP: Display Ping/HTTP functions of WAN 1/2 to show if they are enabled or disabled.

Configure: Click **Modify** to modify WAN 1/2 settings.

Priority: Set priority of WAN 1/2 for Internet Access.

WAN 1/2 Interface

Using the WAN 1/2 **Interface**, the Administrator can set up the **WAN 1/2** network. These IP addresses are real public IP Addresses, and are routable on the Internet.

Alive Indicator Site IP: This feature is used to ping an address for detecting WAN connection status.

Service: ICMP You can select an IP address by Assist, or type an IP address manually.

Service: DNS You can select a DNS IP and Domain name by Assist, or type the related data manually.

PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect.

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If it sets to enable, the device will respond to echo request packets from the WAN 1/2 network.

HTTP: Select this to allow the device WEBUI to be accessed from the WAN 1 network. This will allow WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

Interface > WAN

System

Interface

- LAN
- WAN
- DMZ

Policy Object

Policy

Mail Security

IDP

Anomaly Flow IP

Monitor

WAN Interface

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

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: Kbps (Max. 30 Mbps)

Max. Upstream Bandwidth: Kbps (Max. 30 Mbps)

☒ Service-On-Demand

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

Enable ☐ Ping ☐ HTTP

Connecting Disconnect OK Cancel

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by CS-1000 from the ISP will be displayed here. This is the IP address of the WAN 1 (WAN 2) port of the device.

MAC Address: This is the MAC Address of the device. Some ISPs require specified MAC address. If the required MAC address is your PC's, click **Clone MAC Address**.

Hostname: This will be the name assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Domain Name: You can specify your own domain name or leave it blank.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If it sets to enable, the device will respond to echo request packets from the WAN 1/2 network.

HTTP: Select this to allow the device WEBUI to be accessed from the WAN 1 network. This will allow WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

PLANET
Networking & Communication

Interface > WAN

System

Interface

- LAN
- WAN**
- DMZ

Policy Object

Policy

Mail Security

IDP

Anomaly Flow IP

Monitor

WAN Interface

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

IP Address: 0.0.0.0 Renew Release
 MAC Address: 00:30:4F:44:A2:F5 Clone MAC Address
 Hostname:
 Domain Name:
 User Name (Required by DHCP+ protocol):
 Password (Required by DHCP+ protocol):

Max. Downstream Bandwidth: 30000 Kbps (Max. 30 Mbps)
 Max. Upstream Bandwidth: 30000 Kbps (Max. 30 Mbps)

☐ Enable ☐ Ping ☐ HTTP

OK Cancel

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN 1 port of the device.

Netmask: This will be the Netmask of the WAN 1 network. (i.e. 255.255.255.0)


Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP Address of the DNS server.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP.

Ping: Select this to allow the WAN 1 network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If it sets to enable, the device will respond to echo request packets from the WAN 1/2 network.

HTTP: Select this to allow the device WEBUI to be accessed from the WAN 1 network. This will allow WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.



Interface > WAN

System
Interface
 LAN
 WAN
 DMZ
Policy Object
Policy
Mail Security
IDP
Anomaly Flow IP
Monitor

WAN Interface

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

IP Address: 192.168.99.98
Netmask: 255.255.255.0
Default Gateway: 192.168.99.253
DNS Server 1: 168.95.1.1
DNS Server 2:


Max. Downstream Bandwidth: 30000 Kbps (Max. 30 Mbps)
Max. Upstream Bandwidth: 30000 Kbps (Max. 30 Mbps)

Enable: ☒ Ping ☒ HTTP

OK Cancel

3.2.3 DMZ

The Administrator uses the **DMZ Interface** to set up the DMZ network. The DMZ network consists of server computers such as FTP, SMTP, and HTTP (web). These server computers are put in the DMZ network so they can be isolated from the LAN (LAN) network traffic. Broadcast messages from the LAN network will not cross over to the DMZ network to cause congestions and slow down these servers. This allows the server computers to work efficiently without any slowdowns.



Interface > DMZ

System
Interface
 LAN
 WAN
 DMZ
Policy Object
Policy
Mail Security
IDP

DMZ Interface

DMZ Interface: Disable

IP Address: 0.0.0.0
Netmask: 0.0.0.0

Enable: ☐ Ping ☐ HTTP

OK Cancel

DMZ Interface: Display NAT Mode or TRANSPARENT Mode functions of DMZ to show if they are enabled or disabled.

IP Address: The private IP address of the Multi-Homing Security Gateway's DMZ interface. This will be the IP address of the DMZ port. If it is in NAT mode, the IP address will be a private one and cannot use the same network as the WAN or LAN subnet.

NetMask: This will be the subnet mask of the DMZ network.

Ping: Select this to allow the DMZ network to ping the IP Address of the Multi-Homing Security Gateway. This will allow people from the Internet to be able to ping the Multi-Homing Security Gateway. If set to enable, the device will respond to echo request packets from the DMZ network.

HTTP: Select this to allow the device WebUI to be accessed from the DMZ network. This will allow the WebUI

to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

3.3 Policy Object

The Policy Object is the pre-setting item for Policy editing. The administrator can configure all necessary items here before he wants to configure Multi-Homing Security Gateway Policy. The contents include **Address, Service, Schedule, QoS, Authentication, Content Blocking, Virtual server** and **VPN**.

3.3.1 Address

The Multi-Homing Security Gateway allows the Administrator to set addresses of the LAN network, LAN network group, WAN network, WAN group, DMZ network and DMZ group.

What is the Address Table?

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 and 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 Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.


How to use Address Table

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 built 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.

3.3.1.1 LAN

Entering the LAN window

- Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.



Policy Object > Address > LAN

System	Name	IP / Netmask	MAC Address	Configure
Interface	Inside_Any	0.0.0.0/0.0.0.0		In Use

Address

- LAN ←←
- LAN Group
- WAN
- WAN Group

New Entry

Definition

Name: Name of LAN network address.

IP / Netmask: IP address and subnet mask of LAN network


MAC Address: MAC address corresponded with LAN IP address.

Configure: You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN network. Click **Remove** to delete the settings.

In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

Adding a new LAN Address

- Step 1. In the LAN window, click the **New Entry** button.
- Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.
- Step 3. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.



Policy Object > Address > LAN

System	Name	IP Address	Netmask	MAC Address	Configure
Interface	sebastien	192.168.1.2	255.255.255.255	00:0E:A6:0F:8B:92	Clone MAC Address

Address

- LAN
- LAN Group
- WAN
- WAN Group
- DMZ
- DMZ Group

Service

Get static IP address from DHCP Server.

OK Cancel

If you want to enable **Get Static IP address from DHCP Server** function, enter the MAC Address then check the **Get Static IP address from DHCP Server**.

Modifying an LAN Address

- Step 1. In the LAN window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.
- Step 2. In the **Modify Address** window, fill in the new address.
- Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

The screenshot shows the PLANET Networking & Communication software interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object (selected), Address, LAN (selected), LAN Group, WAN, WAN Group, DMZ, DMZ Group, Service, Schedule, and QoS. The main area displays the 'Policy Object > Address > LAN' configuration. The 'Modify Address' window is open, showing the following fields:

Name	sebastien
IP Address	192.168.1.2
Netmask	255.255.255.255
MAC Address	00:0E:A6:0F:8B:92

Below the MAC Address field is a checkbox labeled 'Get static IP address from DHCP Server.' and a 'Clone MAC Address' button. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Removing a LAN Address

- Step 1. In the LAN window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.
- Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

The screenshot shows the PLANET Networking & Communication software interface. The left sidebar is the same as in the previous screenshot. The main area displays the 'Policy Object > Address > LAN' configuration. A table lists the LAN addresses:

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
sebastien	192.168.1.2/255.255.255.255	00:0E:A6:0F:8B:92	Modify Remove

A 'New Entry' button is located above the table. A confirmation dialog box titled 'Microsoft Internet Explorer' is open, asking 'Are you sure you want to remove?' with 'OK' and 'Cancel' buttons.

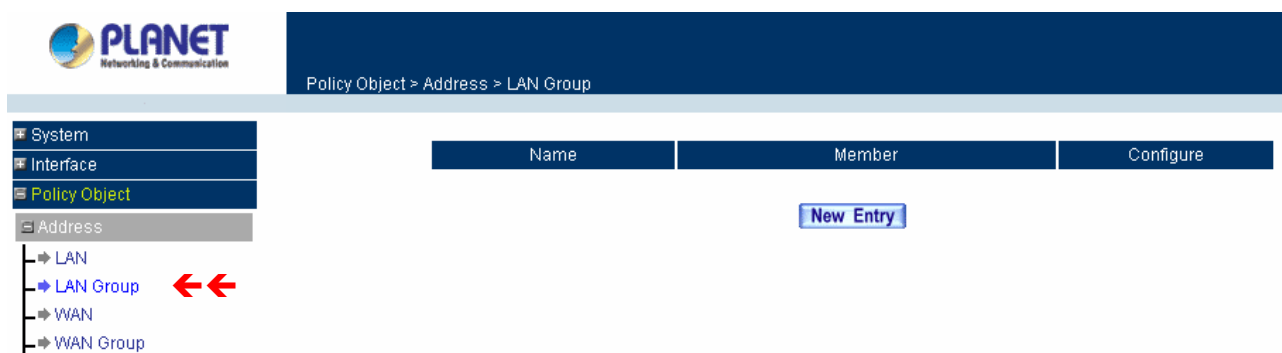
3.3.1.2 LAN Group

Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

- Step 1. Click LAN **Group** under the **Address** menu to enter the LAN Group window. The current setting

information for the LAN network group appears on the screen.



Definitions

Name: Name of the LAN group.

Member: Members of the group.

Configure: Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click

Remove to delete the group.

In the **LAN Group** window, if one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group.

Name	Member	Configure
ENM	sebastien	In Use

You have to delete or pause the Group in **Policy** window, and then you are allowed to configure the LAN Group.

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

Adding a LAN Group

Step 1. In the **LAN Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

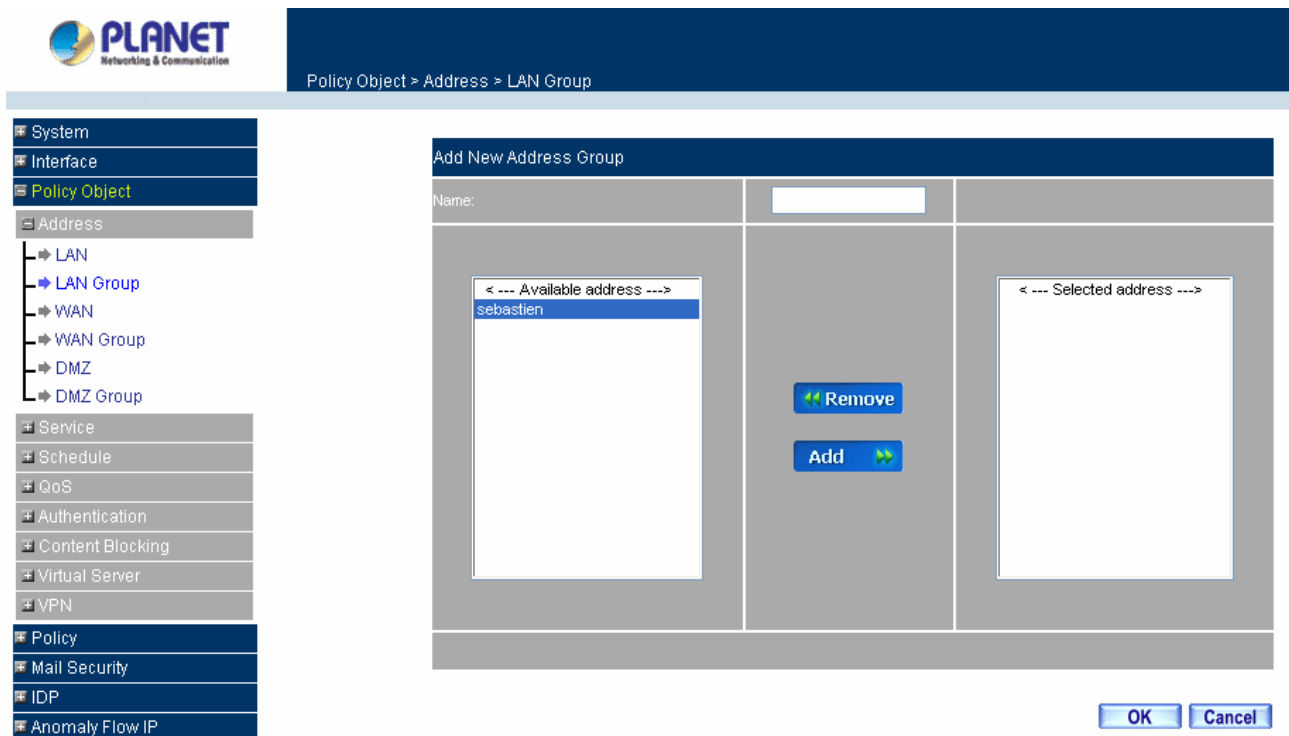
Step 2. In the Add New Address Group window:

- **Available address:** list the names of all the members of the LAN network.
- **Selected address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available address list, and click the **Add>>** button to add them to the Selected address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click **Cancel** to discard changes.



Modifying a LAN Group

Step 1. In the **LAN Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

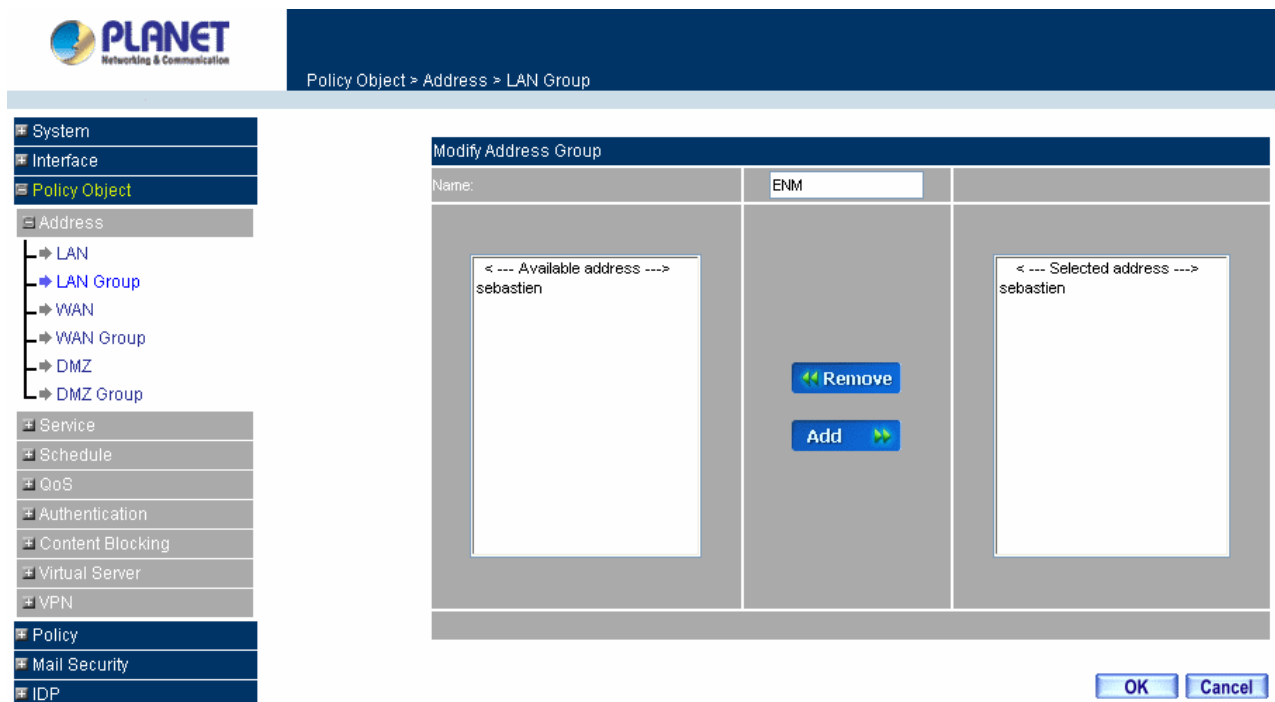
Step 2. A window displaying the information of the selected group appears:

- **Available address:** list names of all members of the LAN network.
- **Selected address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.

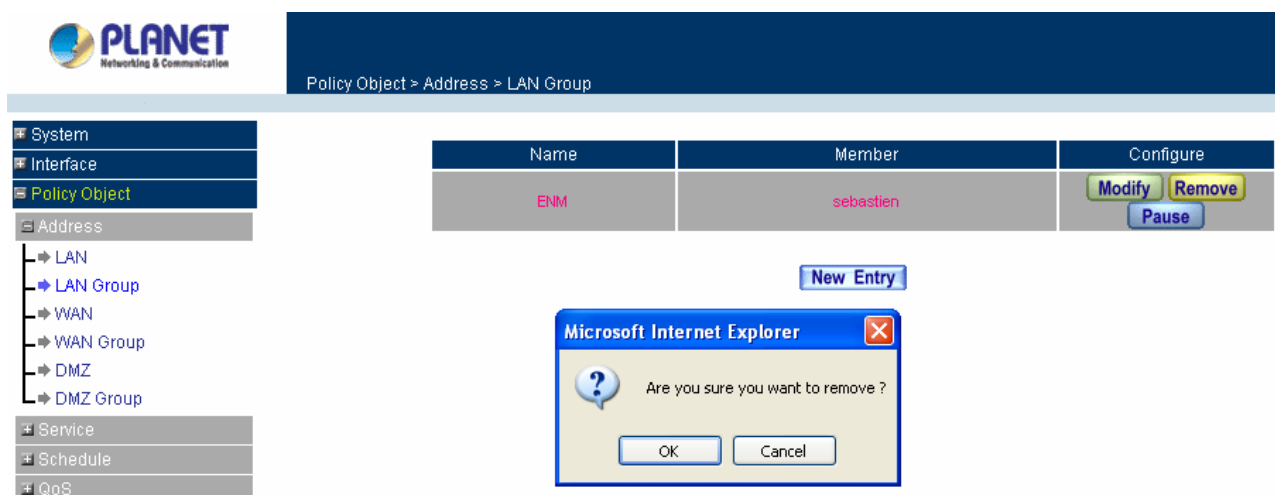
Step 4. **Remove members:** Select names in the **Selected address** list, and click the **<<Remove** button to remove these members from the **Selected address** list.

Click **OK** to save changes or click **Cancel** to discard changes.



Removing a LAN Group

- Step 1. In the LAN **Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.
- Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



3.3.1.3 WAN

Entering the WAN window

- Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.



PLANET Networking & Communication

Policy Object > Address > WAN

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use

New Entry

System

Interface

Policy Object

Address

- LAN
- LAN Group
- WAN
- WAN Group
- DMZ
- DMZ Group

Service

Definitions

Name: Name of WAN network address.

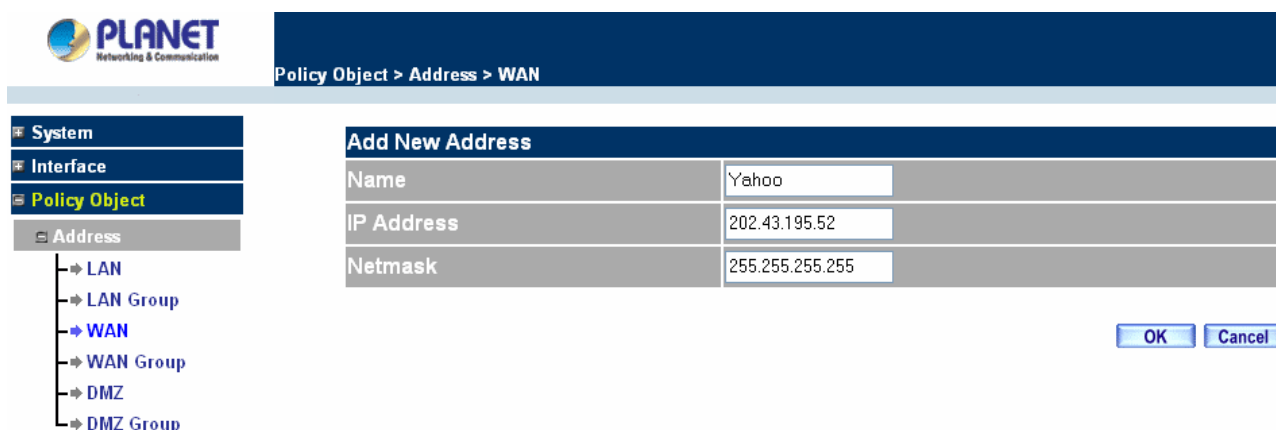
IP/Netmask: IP address/Netmask of WAN network.

Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network. Click **Remove** to delete the setting of WAN network.

NOTE: In the **WAN** window, if one of the members has been added to **Policy** or **WAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.

Adding a new WAN Address

- Step 1. In the **WAN** window, click the **New Entry** button.
- Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.
- Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.



PLANET Networking & Communication

Policy Object > Address > WAN

Add New Address

Name	Yahoo
IP Address	202.43.195.52
Netmask	255.255.255.255

OK Cancel

System

Interface

Policy Object

Address

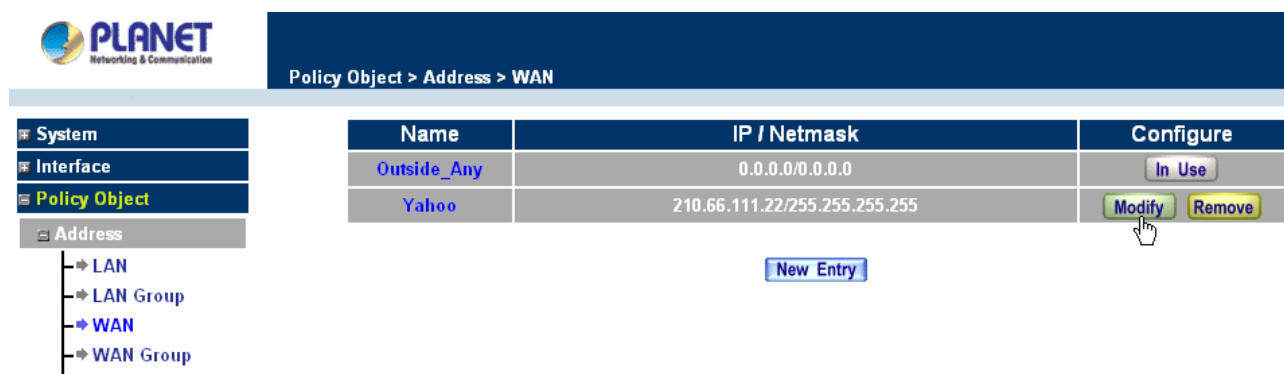
- LAN
- LAN Group
- WAN
- WAN Group
- DMZ
- DMZ Group

Modifying an WAN Address

- Step 1. In the WAN table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new address.

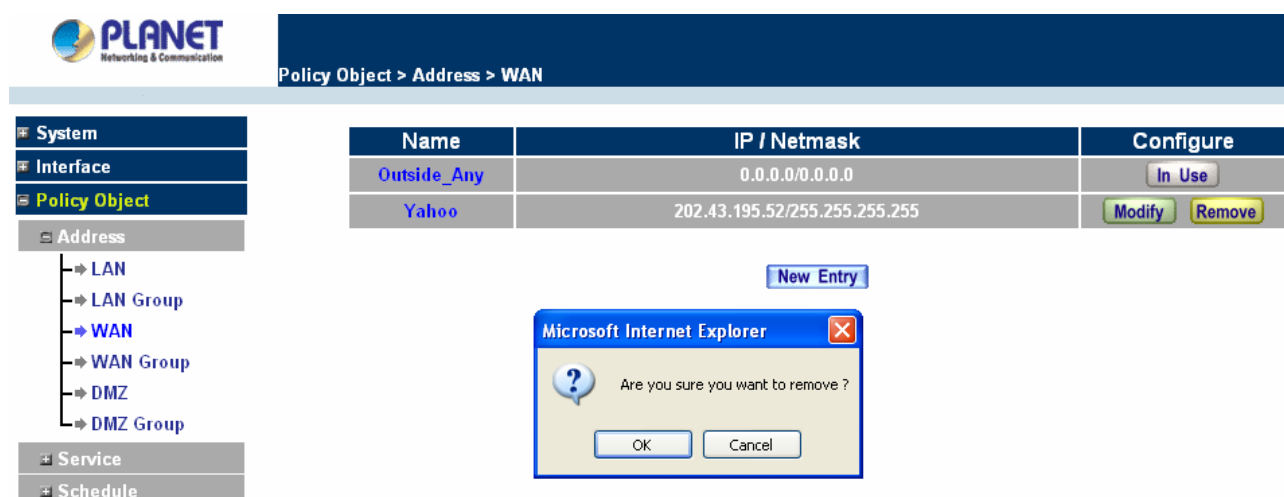
Step 3. Click **OK** to save changes or click **Cancel** to discard changes.



Removing an WAN Address

Step 1. In the WAN table, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

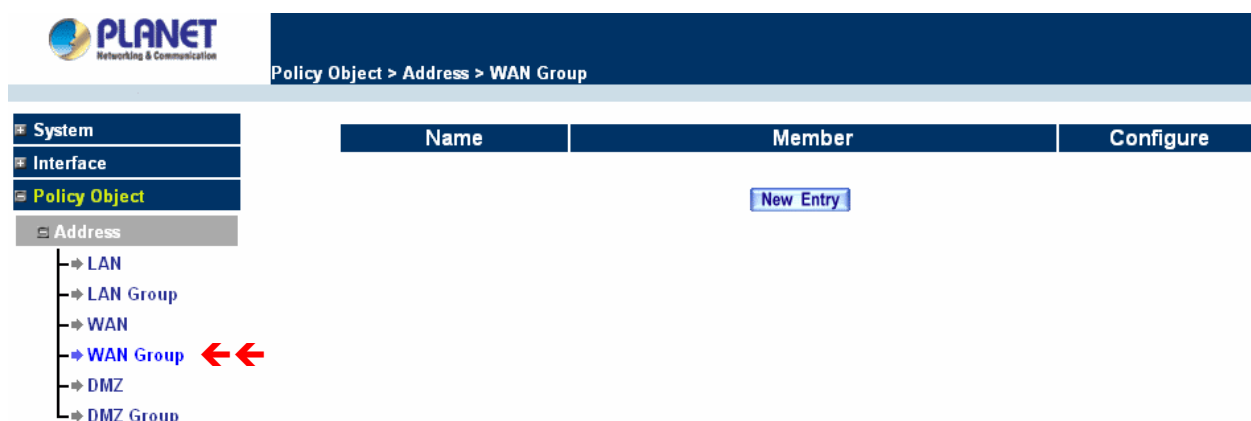


3.3.1.4 WAN Group

Entering the WAN Group window

Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current

settings for the WAN network group(s) will appear on the screen.



Definitions:

Name: Name of the WAN group.

Member: Members of the group.

Configure: Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group. Click **Remove** to delete the selected group.

NOTE: In the **WAN Group** window, if one of the members has been added to the **Policy**, “**In Use**” message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the **Policy** window to remove the setting, and then you can configure.

Adding an WAN Group

Step 1. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 2. In the **Add New Address Group** window the following fields will appear:

- **Name:** enter the name of the new group.
- **Available address:** List the names of all the members of the WAN network.
- **Selected address:** List the names to assign to the new group.
- **Add members:** Select the names to be added in the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.
- **Remove members:** Select the names to be removed in the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.

Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.

The screenshot shows the PLANET Networking & Communication web interface. The breadcrumb navigation at the top reads "Policy Object > Address > WAN Group". On the left, a sidebar menu shows the navigation tree with "Policy Object" expanded and "Address" selected. The "Add New Address Group" dialog box is open, featuring a "Name:" field at the top. Below it are two list boxes: "Available address" containing "Yahoo" and an empty "Selected address" box. Between these lists are "Remove" and "Add" buttons. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Modifying a WAN Group

- Step 1. In the **WAN Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.
- Step 2. A window displaying the information of the selected group appears:
 - **Available address:** list the names of all the members of the WAN network.
 - **Selected address:** list the names of the members that have been assigned to this group.
- Step 3. **Add members:** Select the names to be added in the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.
- Step 4. **Remove members:** Select the names to be removed in the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.
- Step 5. Click **OK** to save changes or click **Cancel** to discard changes.

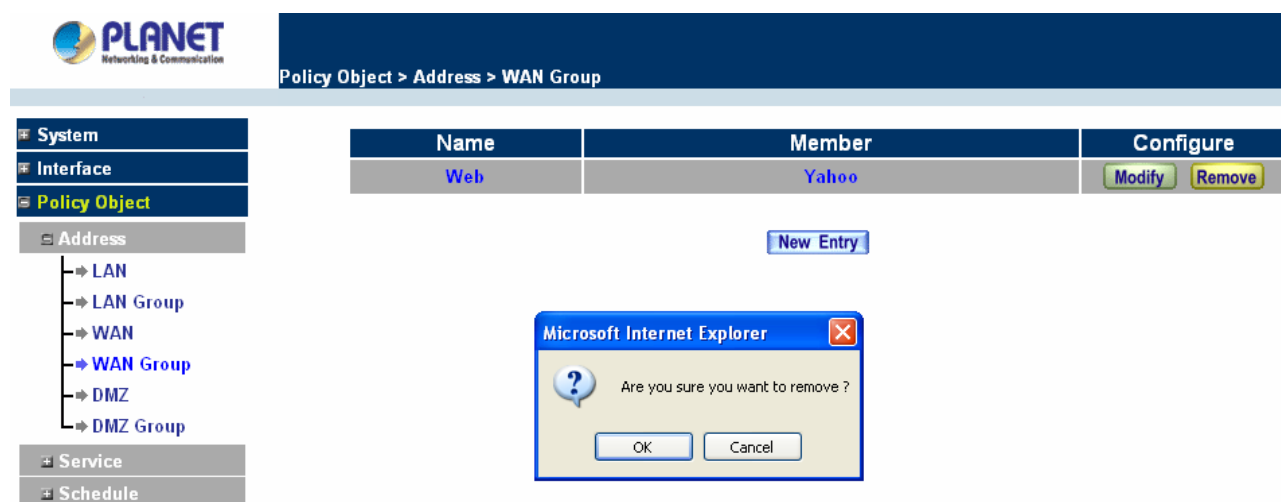
The screenshot shows the PLANET Networking & Communication web interface with the breadcrumb navigation "Policy Object > Address > WAN Group". The left sidebar menu is the same as in the previous screenshot. The main area displays a table with the following structure:

Name	Member	Configure
Web	Yahoo	<div>Modify</div> <div>Remove</div>

Below the table is a "New Entry" button. A mouse cursor is pointing at the "Modify" button in the "Configure" column of the table row.

Removing a WAN Group

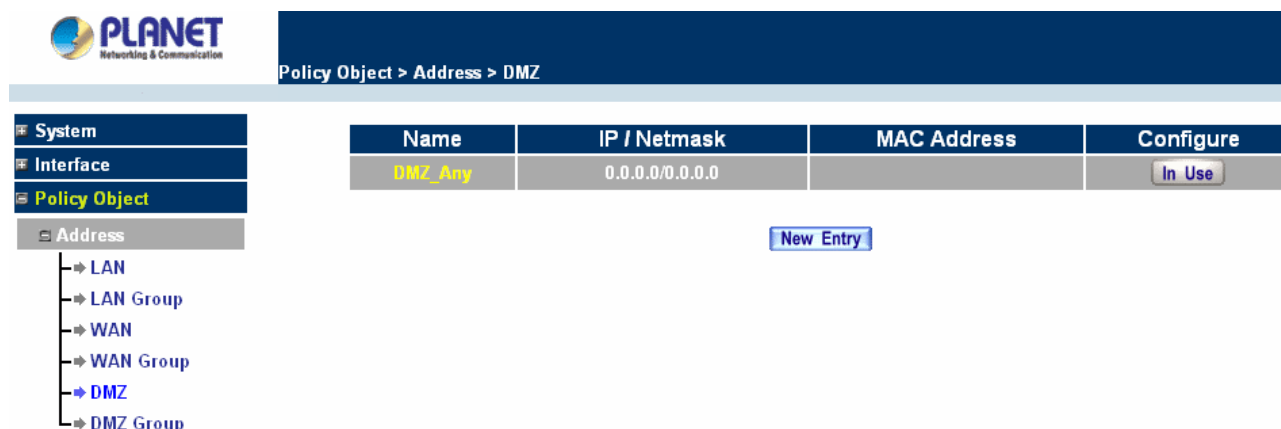
- Step 1.** In the **WAN Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.
- Step 2.** In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



3.3.1.5 DMZ

Entering the DMZ window:

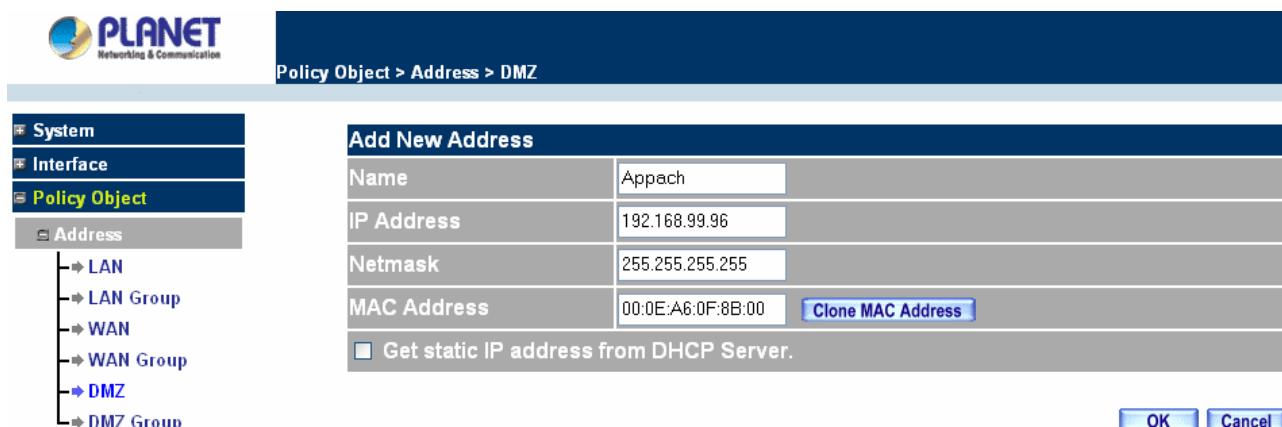
Click **DMZ** under the **Address** menu to enter the **DMZ** window. The current setting information such as the name of the LAN network, IP, and Netmask addresses will show on the screen.



Adding a new DMZ Address:

- Step 1.** In the DMZ window, click the **New Entry** button.
- Step 2.** In the **Add New Address** window, enter the settings for a new DMZ address.

Step 3. Click **OK** to add the specified DMZ or click **Cancel** to discard changes.



The screenshot shows the PLANET Networking & Communication interface. The breadcrumb trail is 'Policy Object > Address > DMZ'. On the left, a tree view shows 'System', 'Interface', 'Policy Object', and 'Address' (selected). Under 'Address', there are links for LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group. The main area is titled 'Add New Address' and contains the following fields:

Name	Appach
IP Address	192.168.99.96
Netmask	255.255.255.255
MAC Address	00:0E:A6:0F:8B:00 Clone MAC Address
<input type="checkbox"/> Get static IP address from DHCP Server.	

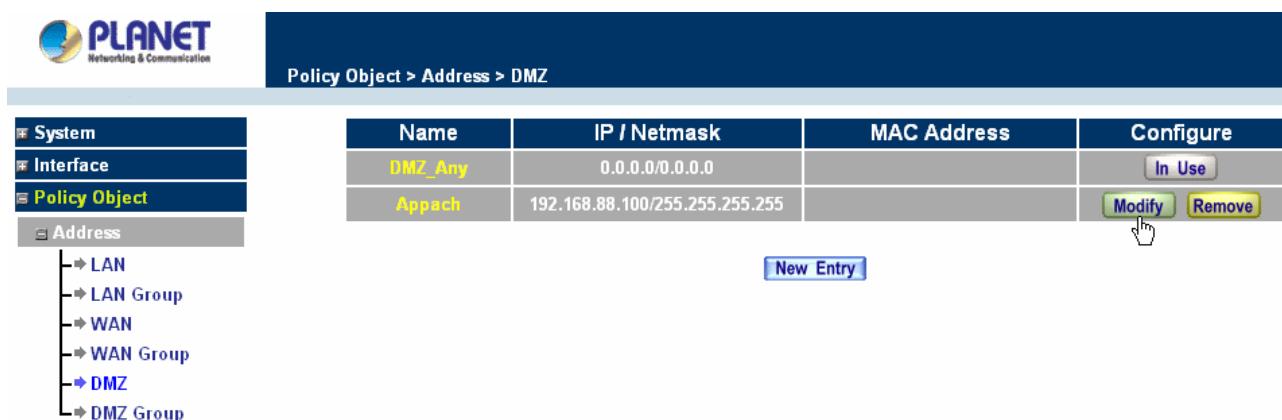
At the bottom right, there are 'OK' and 'Cancel' buttons.

Modifying a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** on save the changes or click **Cancel** to discard changes.



The screenshot shows the PLANET Networking & Communication interface. The breadcrumb trail is 'Policy Object > Address > DMZ'. On the left, a tree view shows 'System', 'Interface', 'Policy Object', and 'Address' (selected). Under 'Address', there are links for LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group. The main area displays a table of DMZ addresses:

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Appach	192.168.88.100/255.255.255.255		Modify Remove

Below the table, there is a 'New Entry' button. A mouse cursor is pointing at the 'Modify' button in the 'Configure' column for the 'Appach' entry.

Removing a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

Planet Network & Communication

Policy Object > Address > DMZ

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0	00:0E:A6:0F:8B:00	In Use
Appsch	192.168.99.96/255.255.255.255	00:0E:A6:0F:8B:00	Modify Remove

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

3.3.1.6 DMZ Group

Entering the DMZ Group window

Click **DMZ Group** under the **Address** menu to enter the **DMZ** window. The current settings information for the DMZ group appears on the screen.

Planet Network & Communication

Policy Object > Address > DMZ Group

Name	Member	Configure
------	--------	-----------

New Entry

Adding a DMZ Group:

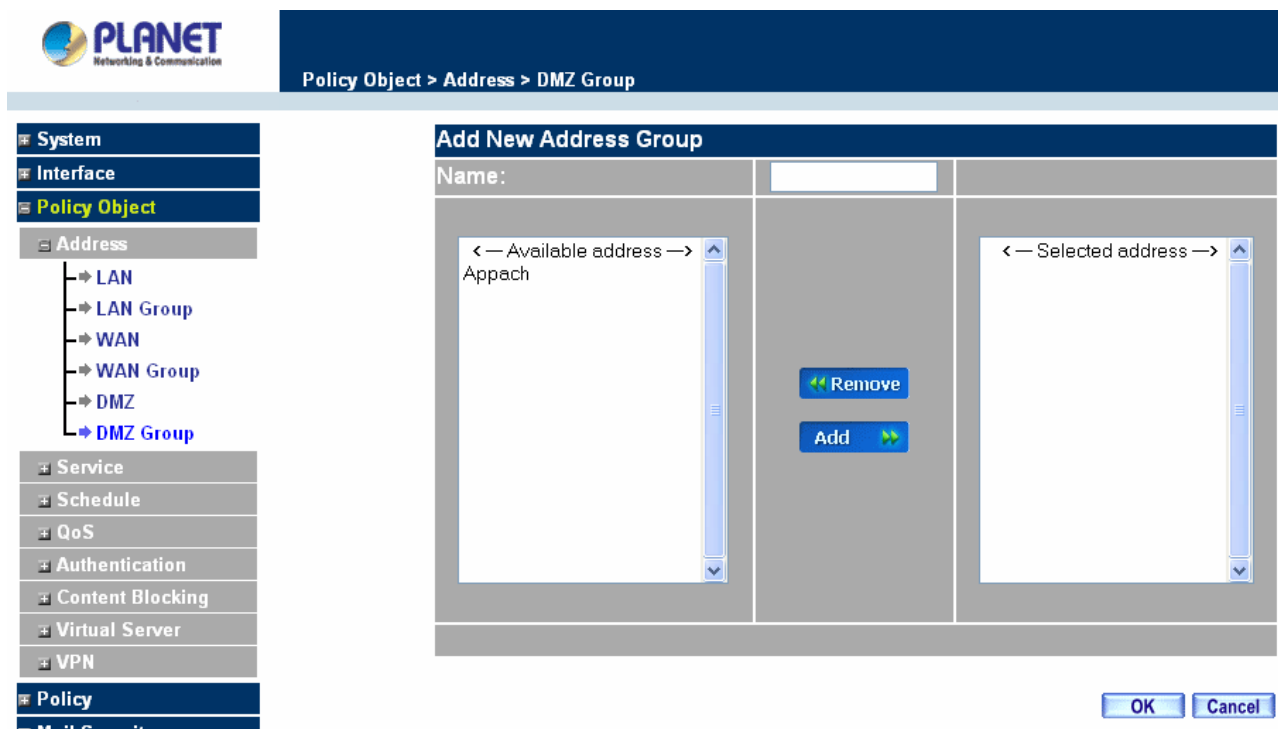
Step 1. In the DMZ Group window, click the **New Entry** button.

Step 2. In the **Add New Address** Group window:

- **Available address:** list names of all members of the DMZ.
- **Selected address:** list names to assign to a new group.

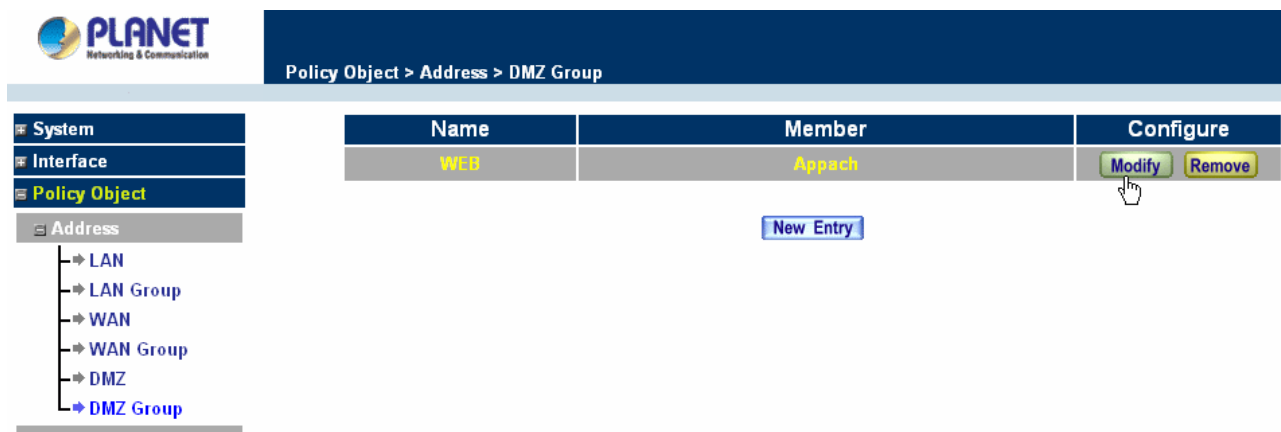
Step 3. Name: enter a name for the new group.

- Step 4. Add members:** Select the names to be added from the **Available address** list, and click the **Add>>** button to add them to the **Selected address** list.
- Step 5. Remove members:** Select names to be removed from the **Selected address** list, and click the **<<Remove** button to remove them from the **Selected address** list.
- Step 6.** Click **OK** to add the new group or click **Cancel** to discard changes.



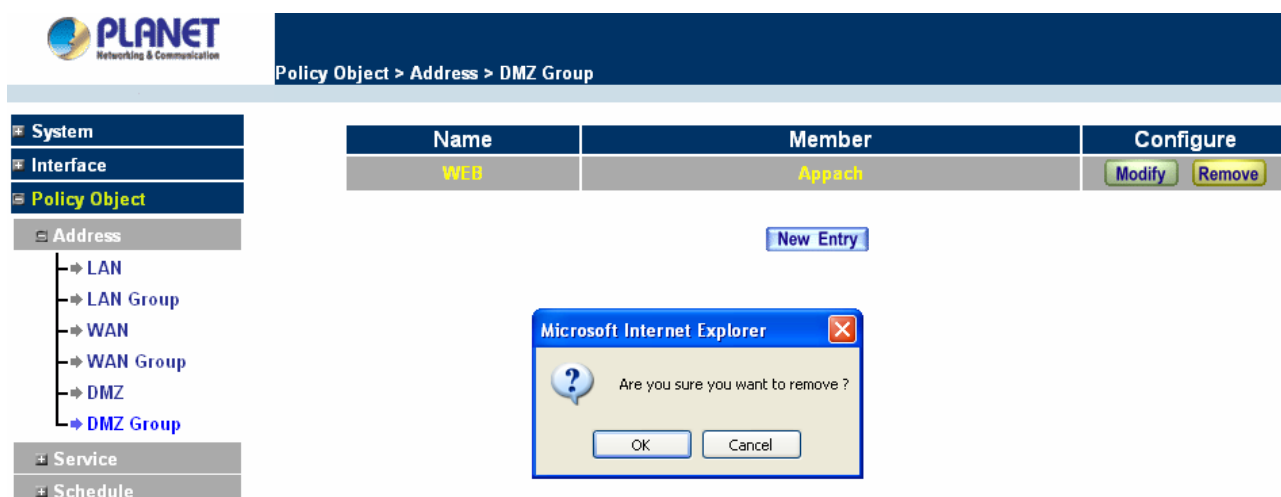
Modifying a DMZ Group:

- Step 1.** In the **DMZ** Group window, locate the **DMZ** group to be modified and click its corresponding **Modify** button in the **Configure** field.
- Step 2.** A window displaying information about the selected group appears:
- **Available address:** list the names of all the members of the DMZ.
 - **Selected address:** list the names of the members that have been assigned to this group.
- Step 3. Add members:** Select names to be added from the **Available Address** list, and click the **Add>>** button to add them to the **Selected address** list.
- Step 4. Remove members:** Select names to be removed from the **Selected address** list, and click the **<<Remove** button to remove them from **Selected address** list.
- Step 5.** Click **OK** to save changes or click **Cancel** to cancel editing.



Removing a DMZ Group:

- Step 1.** In the **DMZ Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.
- Step 2.** In the **Remove confirmation** pop-up box, click **OK** to remove the group.



3.3.2 Service

In this section, 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.

What is 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), POP3(110), etc. The Multi-Homing Security Gateway defines 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 1023.

How do I 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.

3.3.2.1 Pre-defined

Entering a Pre-defined window

- Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.

Policy Object > Service > Pre-defined

ANY ANY (Any)	TCP IMAP (143)	TCP POP3 (110)	TCP TELNET (23)
TCP AFPOverTCP (548)	TCP InterLocator (389)	TCP PPTP (1723)	UDP TFTP (69)
TCP AOL (5190-5194)	TCP IRC (6660-6669)	TCP Real-Media (7070)	ICMP Traceroute (3,11)
TCP BGP (179)	TCP L2TP (1701)	UDP RIP (520)	UDP UDP ANY (Any)
UDP DNS (53)	TCP LDAP (389)	TCP RLOGIN (513)	UDP UUCP (540)
TCP FINGER (79)	TCP NetMeeting (389&1503&1720)	TCP SMTP (25)	TCP VDO-Live (7000-7010)
TCP FTP (20-21)	UDP NFS (111)	UDP SNMP (161)	TCP WAIS (210)
TCP GOPHER (70)	TCP NNTP (119)	TCP SSH (22)	TCP WINFRAME (1494)
TCP HTTP (80)	UDP NTP (123)	UDP SYSLOG (514)	TCP X-Windows (6000-6063)
TCP HTTPS (443)	UDP PC-Anywhere (5631-5632)	UDP TALK (517-518)	TCP MSN (1863)
UDP IKE (500)	ICMP PING (Any)	TCP TCP-ANY (Any)	

Icons and Descriptions

Figur	Description
	TCP services, e.g. AFPOverTCP, AOL, BGP, FINGER, FTP, GOPHER, HTTP, HTTPS, IMAP, InterLocator, IRC, L2TP, LDAP, NetMeeting, NNTP, POP3, PPTP, Real-Media, RLOGIN, SMTP, SSH, TCP-ANY, TELNET, VDO-Live, WAIS, WINFRAME, X-Windows, MSN, etc.
	UDP services, e.g. DNS, IKE, NFS, NTP, PC-Anywhere, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP, etc.
	ICMP services, i.g. PING, Traceroute, etc.

3.3.2.2 Custom

Entering the Custom window

Step 1. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.



Definitions:

Service name: The defined service name.

Protocol: Network protocol used in the basic setting. Such as TCP、UDP or others.

Client port: The range of Client port in defined service. If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

Service port: The range of Service port in defined service.

If the number of ports entered in the two fields of Service port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Service port is identical, it means that the entered port number is opened.

Configure: Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.

NOTE: In the **Custom** window, if one of the services has been added to **Policy** or **Group**, "In Use" message will appear in the **Configure** column. In this case you are not allowed to modify or remove the settings. Go to the **Policy** or **Group** window to delete the setting, and then you can configure the settings.

Adding a new Service

In the **Custom** window, click the **New Entry** button and a new service table appears.

In the new service table:

- New Service Name: This will be the name referencing the new service.
- Protocol: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- Client Port: enter the range of port number of new clients.
- Server Port: enter the range of port number of new servers.

The client port and server port ranges are from 0 to 65535.

Step 1. Click **New Entry** to add new services.

Step 2. Click **OK** to accept editing, or click **Cancel**.

PLANET
Networking & Communication

Policy Object > Service > Custom

Add User Defined Service

Service NAME :

#	Protocol	Client Port	Server Port
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	0 : 65535	0 : 0
2	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
3	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other	0 : 0	0 : 0

OK Cancel

Modifying Custom Services

Step 1. A table showing the current settings of the selected service appears on the screen

Step 2. Enter the new values.

Step 3. Click **OK** to accept editing; or click **Cancel**.

PLANET
Networking & Communication

Policy Object > Service > Custom

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	0:65535	4661:4665	Modify Remove

New Entry

Removing Custom Services

Step 1. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.

PLANET Network & Communication

Policy Object > Service > Custom

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	0:65535	4661:4665	Modify Remove

New Entry

[JavaScript Application] Are you sure you want to remove ?

OK Cancel

3.3.2.3 Group

Accessing the Group window

Step 1. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.

PLANET Network & Communication

Policy Object > Service > Group

Group name	Service	Configure
------------	---------	-----------

New Entry

System
Interface
Policy Object
Address
Service
Pre-defined
Custom
Group

Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

Configure: Configure the settings of Group. Click **Modify** to change the parameters of the Group. Click **Remove** to delete the Group.

NOTE: In the **Group** window, if one of the Service Groups has been added to **Policy**. "In Use" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the Policy window, remove the Service group first, and then you are allowed to configure the setting.

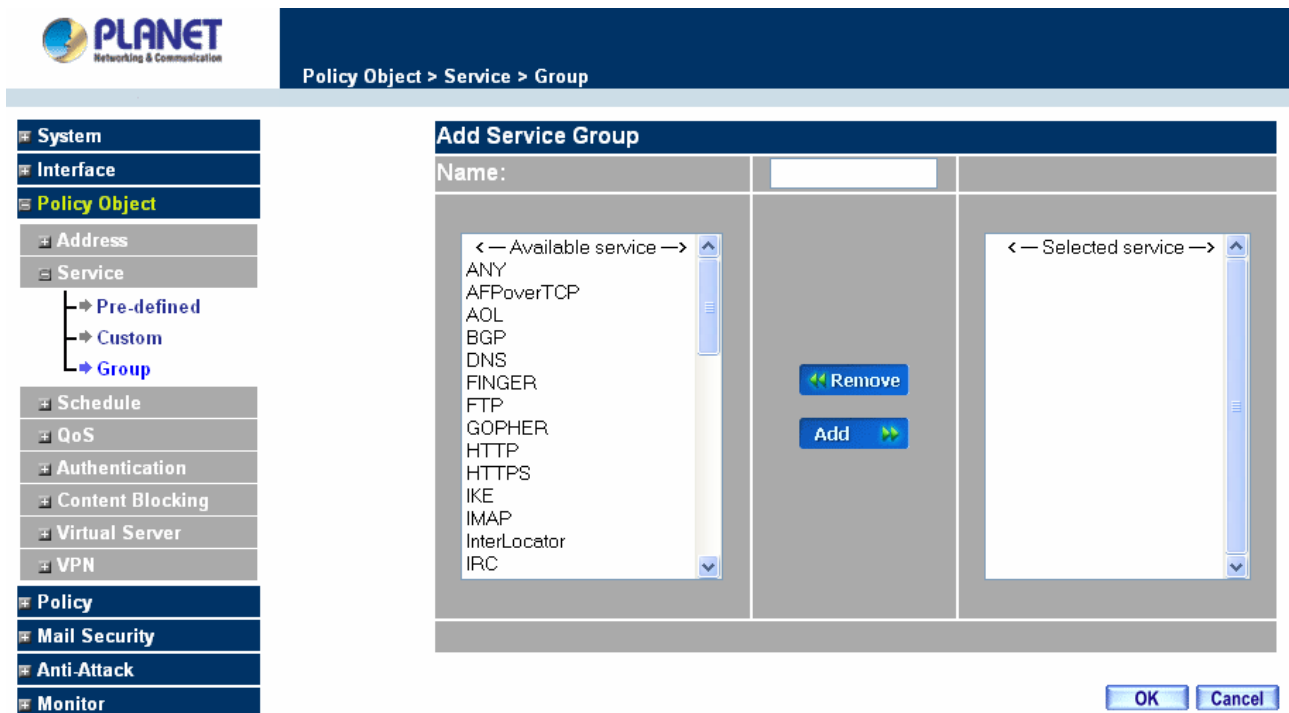
Adding Service Groups

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

- **Available service:** list all the available services.
- **Selected service:** list services to be assigned to the new group.

- Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.
- Step 4. **To add new services:** Select the services desired to be added in the **Available service** list and then click the **Add>>** button to add them to the group.
- Step 5. **To remove services:** Select services desired to be removed in the **Available service**, and then click the **<<Remove** button to remove them from the group.
- Step 6. Click **OK** to add the new group.



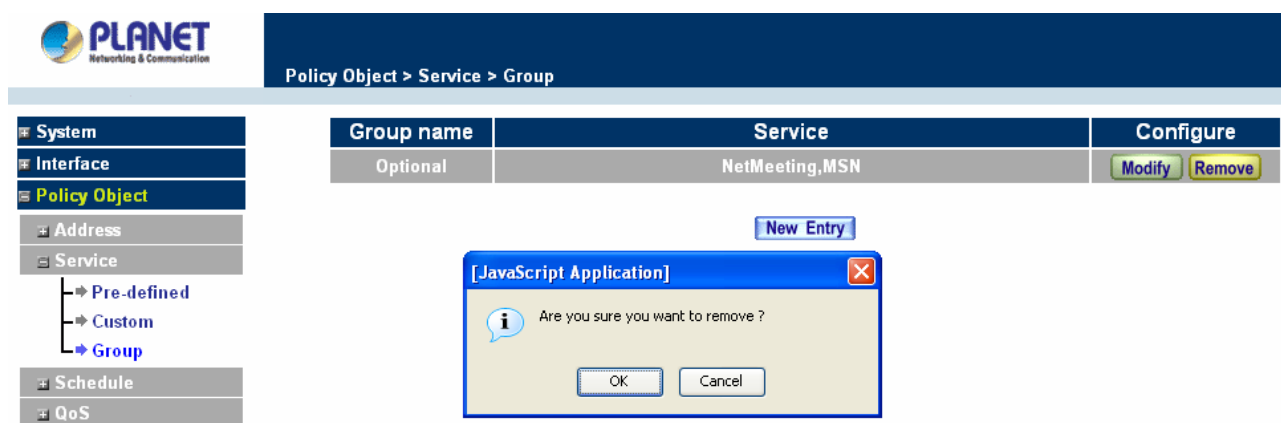
Modifying Service Groups

- Step 1. In the Mod (modify) group window the following fields are displayed:
- **Available service:** lists all the available services.
 - **Selected service:** list services that have been assigned to the selected group.
- Step 2. **Add new services:** Select services in the **Available service** list, and then click the **Add>>** button to add them to the group.
- Step 3. **Remove services:** Select services to be removed in the **Selected service** list, and then click the **<<Remove** button to remove theses services from the group.
- Step 4. Click **OK** to save editing changes.



Removing Service Groups

In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.



3.3.3 Schedule

The Multi-Homing Security Gateway allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Multi-Homing Security Gateway policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Multi-Homing Security Gateway policies therefore will likely not be permitted to pass through the Multi-Homing Security Gateway. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Multi-Homing Security Gateway to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Multi-Homing Security Gateway to work Monday-Friday, 8AM - 5PM only. During the non-work hours, the Multi-Homing Security Gateway will not allow Internet access.

Accessing the Schedule window

Step 1. Click on **Setting** on the **Schedule** menu bar and the schedule window will appear displaying the active schedules.



The following items are displayed in this window:

Name: the name assigned to the schedule

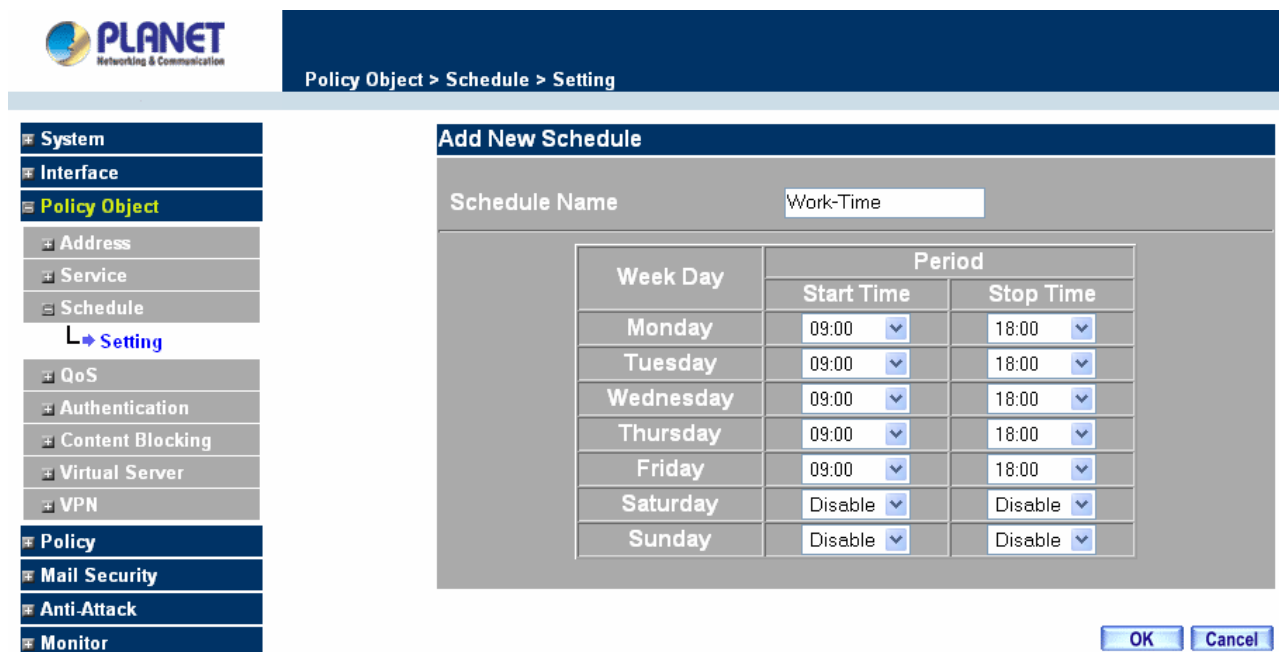
Configure: modify or remove

Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

- **Schedule Name:** Fill in a name for the new schedule.
- **Period:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click **Cancel** to cancel adding the new schedule.

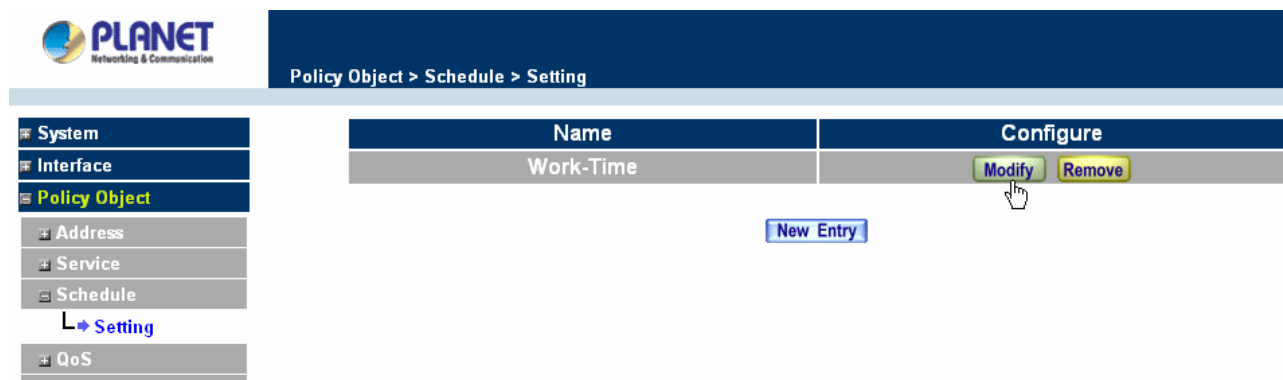


NOTE: In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

Modifying a Schedule

Step 1. In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field. Make needed changes.

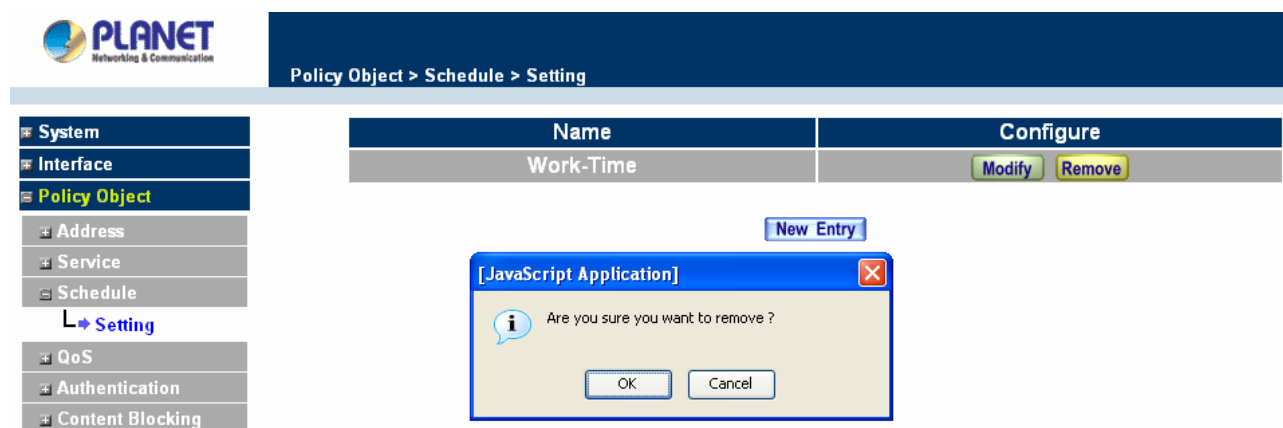
Step 2. Click **OK** to save changes.



Removing a Schedule

Step 1. In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the schedule.



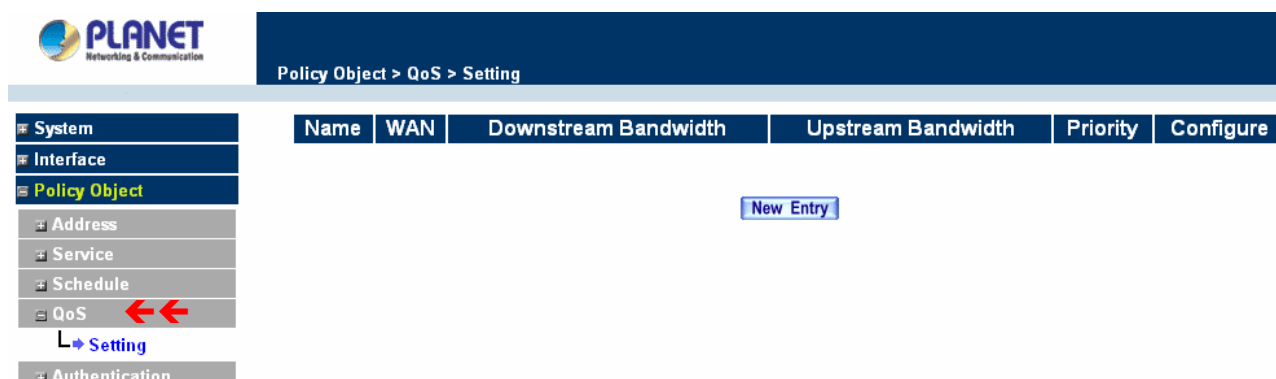
3.3.4 QoS

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth.

Before to configure QoS setting, the WAN port downstream and upstream bandwidth setting must be configured first, or the QoS setting will not be available to be configured.

Configuration of QoS

Click QoS in the menu bar on the left hand side.



Definitions:

Name: The name of the QoS you want to configure.

WAN: Display WAN interface.

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

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

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

Add New QoS

Step 1. Click QoS in the menu bar on the left hand side.

Step 2. Click the **New Entry** button to add new QoS.

Definition

Name: The name of the QoS you want to configure.

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.

Click the **OK** button to add new QoS.

Modify QoS

Step 1. In the QoS window, find the QoS you want to modify, and click **Modify** in the **Configure** column.

Step 2. Click the **OK** button to modify QoS



Policy Object > QoS > Setting

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP	1	G.Bandwidth = 128Kbps M.Bandwidth = 512Kbps	G.Bandwidth = 64 Kbps M.Bandwidth = 128 Kbps	High	Modify Remove


[New Entry](#)

System
Interface
Policy Object
Address
Service
Schedule
QoS
Setting
Authentication

Delete QoS

Step 1. In the QoS window, find the QoS you want to change, and click **Delete** in the **Configure** column.

Step 2. In the Delete QoS window, click **OK** to delete the QoS or click Cancel to discard the change.



Policy Object > QoS > Setting

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP	1	G.Bandwidth = 128Kbps M.Bandwidth = 512Kbps	G.Bandwidth = 64 Kbps M.Bandwidth = 128 Kbps	High	Modify Remove

[JavaScript Application]
Are you sure you want to remove ?
OK Cancel

System
Interface
Policy Object
Address
Service
Schedule
QoS
Setting
Authentication
Content Blocking

Example about how to configure QoS correctly

Step 1. Select and configure the correct connection type, including downstream/upstream bandwidth.

PLANET
Networking & Communication

Interface > WAN

System
Interface
 → LAN
 → **WAN**
 → DMZ
Policy Object
Policy
Mail Security
Anti-Attack
Monitor

WAN Interface

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

IP Address: 210.66.155.90
 Netmask: 255.255.255.224
 Default Gateway: 210.66.155.94
 DNS Server 1: 168.95.1.1
 DNS Server 2:

Max. Downstream Bandwidth: 4096 Kbps (Max. 30 Mbps)
 Max. Upstream Bandwidth: 672 Kbps (Max. 30 Mbps)

Enable: ☒ Ping ☒ HTTP

OK Cancel

Step 2. Configure the LAN host or WAN host IP address that need to filter with QoS feature. Be aware that the Netmask must set to 255.255.255.255 if you only want to configure a single IP address.

PLANET
Networking & Communication

Policy Object > Address > LAN

System
Interface
Policy Object
 → Address
 → LAN
 → LAN Group
 → WAN
 → WAN Group
 → DMZ
 → DMZ Group

Add New Address

Name: Alice
 IP Address: 192.168.1.20
 Netmask: 255.255.255.255
 MAC Address: [Clone MAC Address](#)
☐ Get static IP address from DHCP Server.

OK Cancel

Step 3. Set up the QoS rule.

PLANET
Networking & Communication

Policy Object > QoS > Setting

System
Interface
Policy Object
 → Address
 → Service
 → Schedule
 → QoS
 → **Setting**
 → Authentication

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Alice_QoS	G.Bandwidth = 128 Kbps M.Bandwidth = 512 Kbps	G.Bandwidth = 64 Kbps M.Bandwidth = 128 Kbps	Middle	Modify Remove

[New Entry](#)

Step 4. Enable the QoS rule in Outgoing or Incoming Policy.

PLANET
Networking & Communication

Policy > Outgoing

System
Interface
Policy Object
Policy
 Outgoing
 Incoming
 WAN To DMZ
 LAN To DMZ
 DMZ To WAN
 DMZ To LAN
Mail Security
IDP
Anomaly Flow IP
Monitor

Comment :

Add New Policy

Source Address	Alice
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	Alice_QoS

OK Cancel

3.3.5 Authentication

By configuring the Authentication, you can control the user's access right time of LAN to WAN. The administrator can configure the authentication according to the authentication account and password. CS-1000 configures the authentication of LAN user by setting account and password to identify the privilege.

3.3.5.1 Auth Setting

The administrator can specify the port number and authentication time of authentication management system for LAN user to access WAN network.

Configuration of Authentication

Click **Authentication** in the menu bar on the left hand side and click **Auth Setting**.

The screenshot shows the PLANET web interface. On the left is a navigation menu with categories: System, Interface, Policy Object (selected), Address, Service, Schedule, QoS, Authentication, Content Blocking, Virtual Server, VPN, Policy, and Mail Security. Under the Authentication category, the following items are listed: Auth Setting (selected), Auth User, Auth Group, RADIUS, and POP3. The main content area is titled 'Authentication Management' and contains the following settings:

- 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:** (empty text box)
- Messages to display when user login:** (empty text area)

At the bottom right of the settings area are 'OK' and 'Cancel' buttons.

Authentication Port: The port number used for user login page.

Generally, when user wants to access WAN network and the authentication (Policy -> Outgoing) is enabled, the user only need to open a web page and the User Login page will pop up.

But if user does not need to open the web page and also want to access Internet resource such as FTP, then the user has to send http request with this port number, and CS-1000 will send a User Login page for user to input user name and password.

For example, if the gateway IP address is 192.168.1.1 and authentication port is 82, user have to open a web browser and input <http://192.168.1.1:82> on the address file to have the user login page.

Re-Login if Idle: When the LAN users access to WAN network and stop to access Internet for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes.

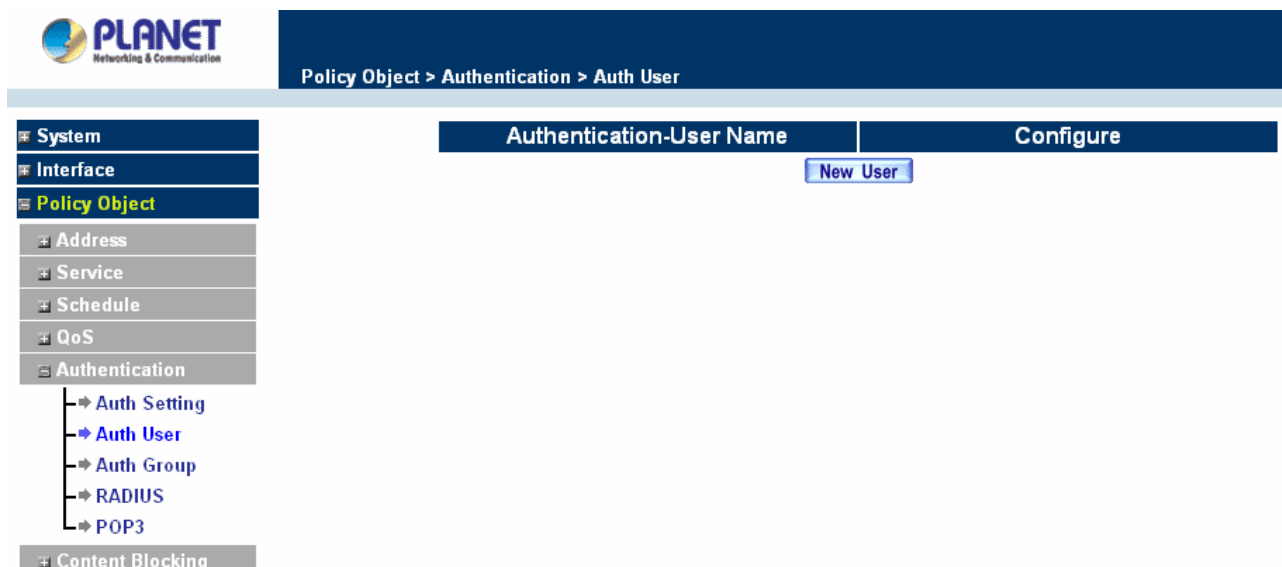
Re-Login after user login successfully: You can limit the access time for the LAN user, when time is up LAN user will need to re-login again. If the time setting sets to 0, that means unlimited. Select **Disallow Re-login if the auth user has login** will disable this feature.

URL to redirect when authentication succeed: You can set up the default webpage, the function will force user to access the default webpage first when user passes the authentication.

Messages to display when user login: You can specify a message to display at user's login page.

3.3.5.2 Auth User

Click **Authentication** in the menu bar on the left hand side and click **Auth User**.



Definitions:

Name : The name of the Authentication you want to configure.

Configure: Modify settings or remove users.

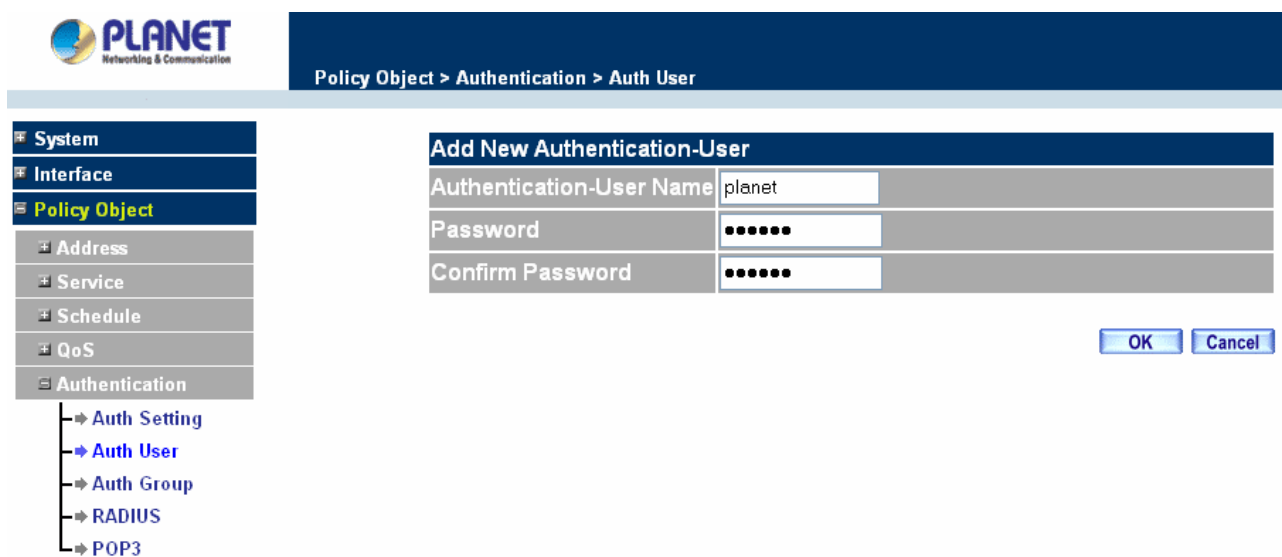
Adding a new Auth User

Step 1. In the **Authentication** window, click the **New Entry** button to create a new **Auth User**.

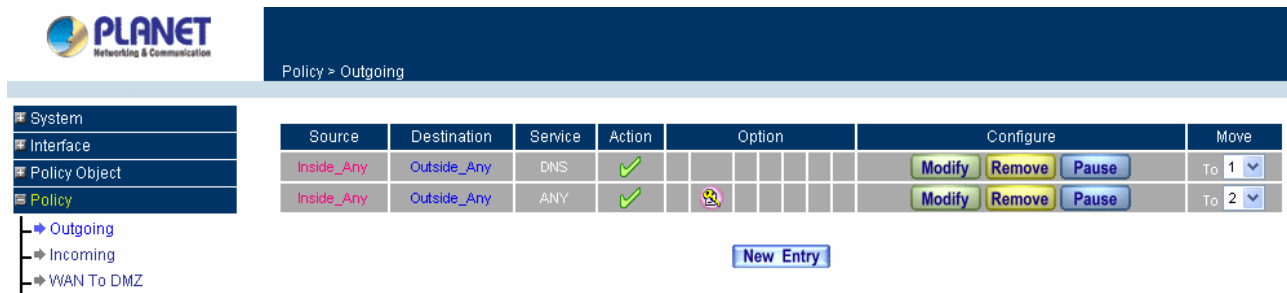
Step 2. In the **Auth-User** window:

- **Auth-User Name**: enter the username of new **Authentication**.
- **Password**: enter a password for the new **Authentication**.
- **Confirm Password**: enter the password again.

Step 3. Click **OK** to add the user or click **Cancel** to cancel the addition.



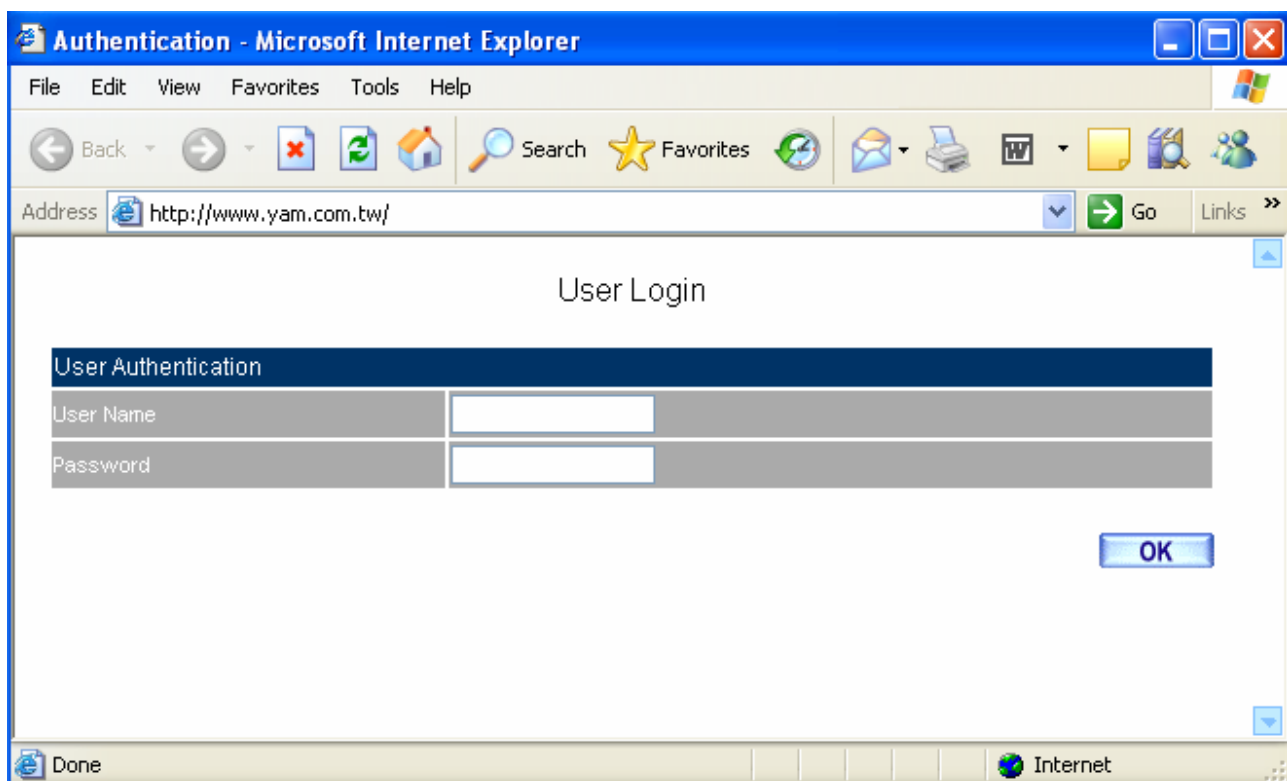
Step 4. Create an Outgoing Policy rule to allow DNS protocol pass through first, then to create another Outgoing Policy rule to enable Authentication-User Function.



Step 5. Before user can access Internet, the User Login Page will pop up as following, then to input the user name and password.

User Login Page Definitions:

- **User Name:** The name of the Authentication you want to configure.
- **Password:** The input carries on the authentication the password



Modifying the Authentication User

Step 1. In the **Authentication** window, locate the **Auth-User** name you want to edit, and click on **Modify** in the **Configure** field.

Step 2. The **Modify Auth-User Password** window will appear. Enter in the required information:

- **Auth-User:** show original authentication user.

- **Password:** show original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 3. Click **OK** to confirm authentication user change or click **Cancel** to cancel it.

The screenshot shows the PLANET web interface. On the left is a navigation menu with 'System', 'Interface', 'Policy Object', 'Address', 'Service', 'Schedule', 'QoS', and 'Authentication'. Under 'Authentication', there are links for 'Auth Setting', 'Auth User' (highlighted), and 'Auth Group'. The main area has a breadcrumb 'Policy Object > Authentication > Auth User'. A table titled 'Modify Authentication-User Password' contains the following fields:

Modify Authentication-User Password	
Authentication-User Name	planet
Password	planet
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

At the bottom right of the table are 'OK' and 'Cancel' buttons.

Removing a Authentication User

Step 1. In the Authentication table, locate the Auth-User name you want to edit, and click on the Remove option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear.

Step 3. Click **OK** to remove that Authentication User or click **Cancel** to cancel.

The screenshot shows the PLANET web interface. The navigation menu is the same as in the previous screenshot. The main area has the breadcrumb 'Policy Object > Authentication > Auth User'. A table with two columns, 'Authentication-User Name' and 'Configure', is shown. The first row has 'planet' in the first column and 'Modify' and 'Remove' buttons in the second column. Below the table is a 'New User' button. A 'Microsoft Internet Explorer' dialog box is open in the foreground with the title 'Are you sure you want to remove ?' and 'OK' and 'Cancel' buttons.

3.3.5.3 Auth Group

Accessing the Auth Group window

Click **Authentication** in the menu bar on the left hand side of the window, then to click **Auth Group** under it.

A window will appear with a table displaying current Auth Group settings.



Adding Auth Group

Step 1. In the Auth Group window, click the **New Entry** button.

In the Auth Group window, the following fields will appear:

- **Name:** Enter the new Auth Group name.
- **Available auth user:** List all the available Auth User.
- **Selected auth user:** List Auth User to be assigned to the new group.

Step 2. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 3. To add new Auth User: Select the Auth User desired to be added in the **Available auth user** list, and then click the **Add>>** button to add them to the group.


Step 4. To remove Auth User: Select Auth User desired to be removed in the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.

Step 5. Click **OK** to add the new group.

The screenshot shows the PLANET web interface. On the left is a navigation menu with categories: System, Interface, Policy Object (selected), Authentication (expanded), Content Blocking, Virtual Server, VPN, Policy, and Mail Security. Under Authentication, the sub-items are Auth Setting, Auth User, Auth Group (selected), RADIUS, and POP3. The main area displays the 'New Authentication Group' window. At the top, the breadcrumb is 'Policy Object > Authentication > Auth Group'. The window has a 'Name:' field containing 'ENM'. Below it are two lists: 'Available Authentication User' and 'Selected Authentication User'. The 'Available' list contains 'planet (Radius User)' and 'planet (POP3 User)'. The 'Selected' list contains 'planet'. Between the lists are 'Remove' and 'Add' buttons. At the bottom right are 'OK' and 'Cancel' buttons.

Modifying Auth Group

- Step 1.** In the Auth Group window, locate the Auth Group to be edited. Click its corresponding **Modify** option in the **Configure** field.
- Step 2.** In the **Modify Auth group** window the following fields are displayed::
- **Name:** Enter the new Auth Group name .
 - **Available auth user:** List all the available Auth User.
 - **Selected auth user:** List Auth User to be assigned to the new group.
- Step 3.** **To add new Auth User:** Select the Auth User desired to be added to the **Available auth user** list, and then click the **Add>>** button to add them to the group.
- Step 4.** **To remove Auth User:** Select Auth User desired to be removed from the **Available auth user** list, and then click the **<<Remove** button to remove them from the group.
- Step 5.** Click **OK** to modify the Group.



Policy Object > Authentication > Auth Group

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Auth Setting

Auth User

Auth Group

RADIUS

POP3

Content Blocking

Virtual Server

VPN

Policy

Mail Security

Modify Authentication-User

Name: ENM

< — Available Authentication User —>

planet
(Radius User)
(POP3 User)

< — Selected Authentication User —>

planet


Remove

Add

OK Cancel

Removing Auth Group

- Step 1.** In the **Auth Group** window, locate the Auth Group to be removed and click its corresponding **Remove** option in the **Configure** field.
- Step 2.** In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.



Policy Object > Authentication > Auth Group

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Auth Setting

Auth User

Auth Group

RADIUS

Name	Member	Radius	POP3	Configure
ENM	planet			Modify Remove

New Entry


Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

3.3.5.4 Radius Serve

Click **Authentication** on the left side menu bar, then click **Radius Server** below it. The following window is shown.



Policy Object > Authentication > RADIUS

System
Interface
Policy Object
Address
Service
Schedule
QoS
Authentication
 Auth Setting
 Auth User
 Auth Group
 RADIUS
 POP3

RADIUS Server
☒ Enable RADIUS Server Authentication
RADIUS Server IP
RADIUS Server Port
Shared Secret
☐ Enable 802.1x RADIUS Server Authentication


OK Cancel

Definition

- **Enable RADIUS Server:** Enable RADIUS Server Authentication.
- **RADIUS Server IP:** Enter RADIUS Server IP address.
- **RADIUS Server Port:** Enter RADIUS Server Port. The default port is 1812.
- **Shared Secret:** The Password for CS-1000 to access RADIUS Server.
- **Enable 802.1x RADIUS Server Authentication:** Enable 802.1x RADIUS Server Authentication.

3.3.5.5 POP3

Click **Authentication** on the left side menu bar, then click **POP3** below it. The following window is shown.



Policy Object > Authentication > POP3

System
Interface
Policy Object
Address
Service
Schedule
QoS
Authentication
 Auth Setting
 Auth User
 Auth Group
 RADIUS
 POP3

POP3 Server
☒ Enable POP3 Server Authentication
POP3 Server (IP or Domain Name)
POP3 Server Port

OK Cancel

Definition

- **Enable POP3 Server:** Enable POP3 Server Authentication.
- **POP3 Server :** Enter POP3 Server IP address or domain name.

- **POP3 Server Port:** Enter POP3 Server Port. The default port is 110.
-

3.3.6 Content Blocking

Content Blocking includes “**URL**”, “**Scripts**”, “**P2P**”, “**IM**”, “**Download**” and “**Upload**”.

URL: The administrator can use a complete domain name or key word to make rules for specific websites.

Scripts : To let Popup、ActiveX、Java、Cookie in or keep them out.

P2P : Block P2P program, include “eDonkey”, “Bit Torrent” and “WinMX”.

IM : Block Internet Message program, include “MSN”, “Yahoo Messenger”, “ICQ”, “QQ” and “Skype”.

Download : Block download connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

Upload : Block upload connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

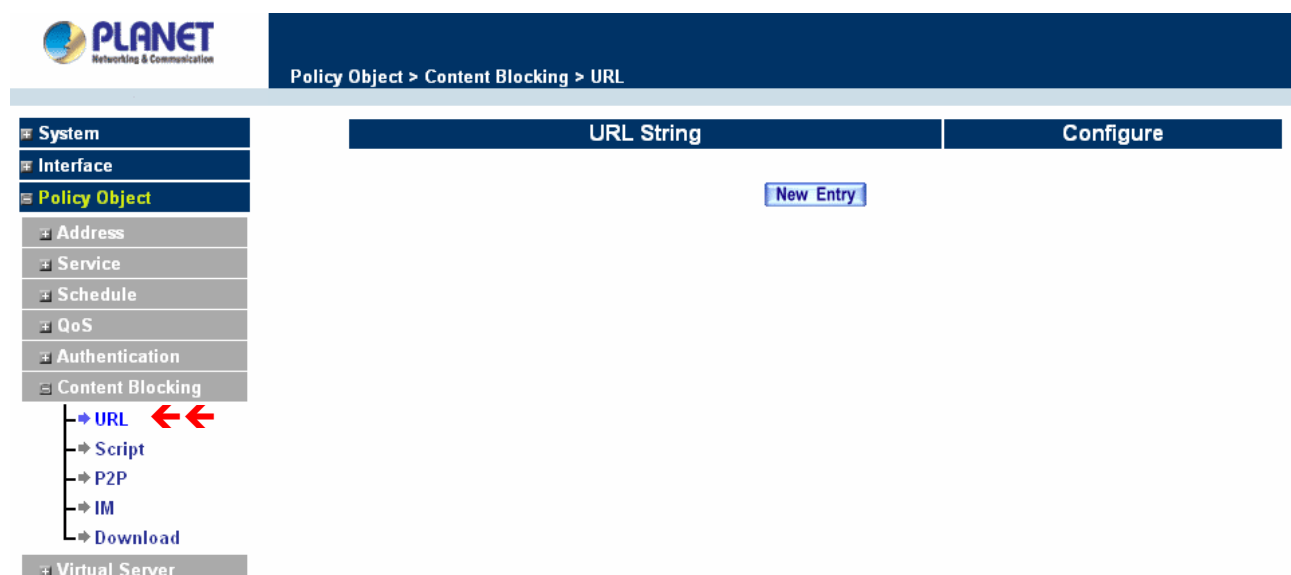
3.3.6.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from LAN network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window

Step 1. Click on **URL** under the **Content Blocking** menu bar.

Step 2. Click on **New Entry**.



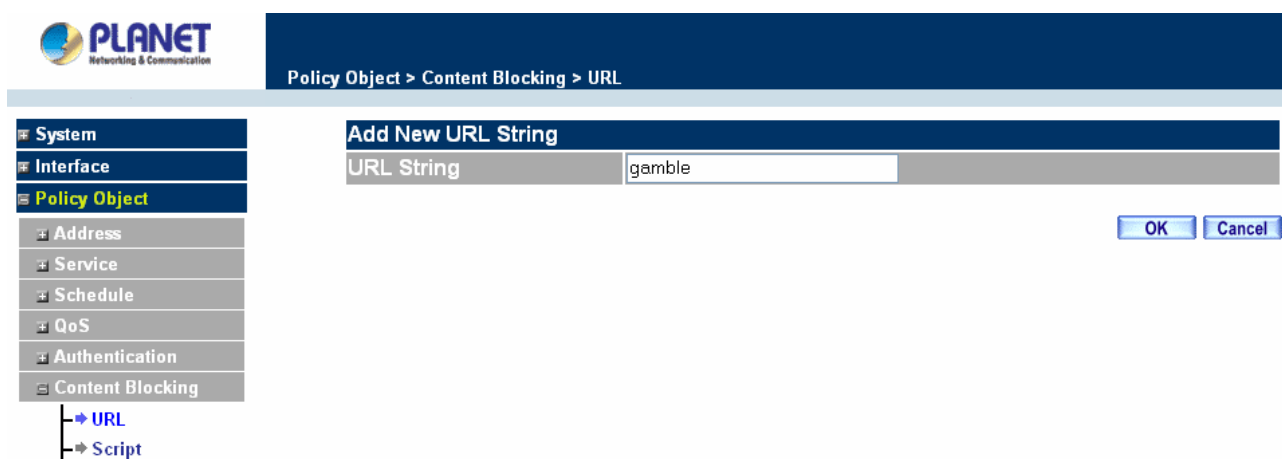
Definition:

URL String: The domain name that is blocked to enter by Multi-Homing Security Gateway.

Configure: To change the settings of URL Blocking, click **Modify** to change the parameters; click **Delete** to delete the settings.

Adding a URL policy

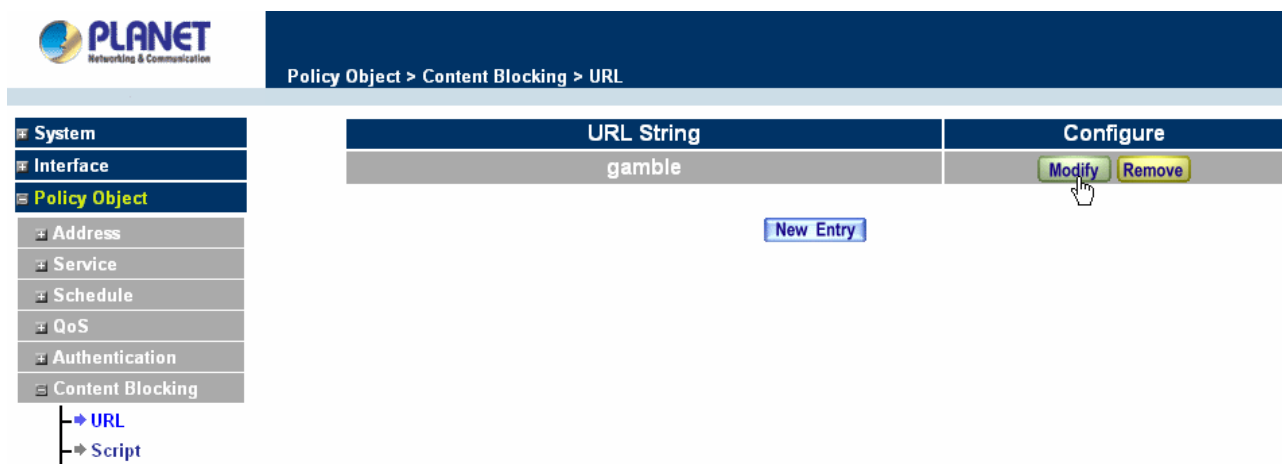
- Step 1. After clicking **New Entry**, the **Add New URL String** window will appear.
- Step 2. Enter the URL of the website to be blocked.
- Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.
- Step 4. Configure Outgoing Policy rule to enable Content Blocking Function.



When the system detects the setting, the Multi-Homing Security Gateway will spontaneously work.

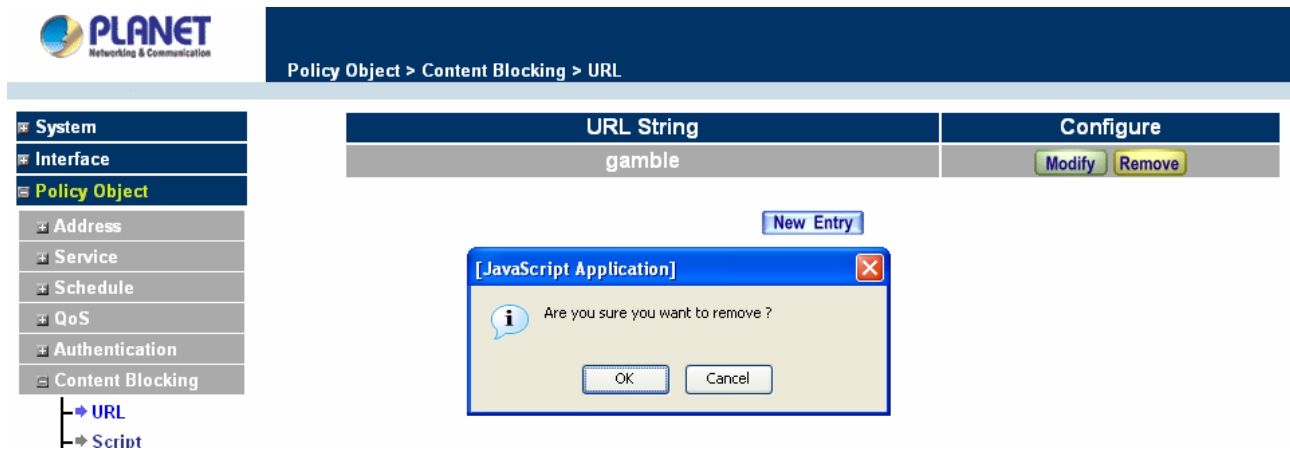
Modifying a URL String Policy

- Step 1. In the **URL** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.
- Step 2. Make the necessary changes needed.
- Step 3. Click on **OK** to save changes or click on **Cancel** to discard changes.



Removing a URL String policy

- Step 1. In the **URL** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.
- Step 2. A confirmation pop-up box will appear, click on **OK** to remove the policy or click on **Cancel** to discard changes.



3.3.6.2 Scripts

To let Popup, ActiveX, Java, or Cookies in or keep them out.

Step 1: Click **Scripts** below **Content Blocking** menu.

Step 2: Select **Scripts** detective functions:

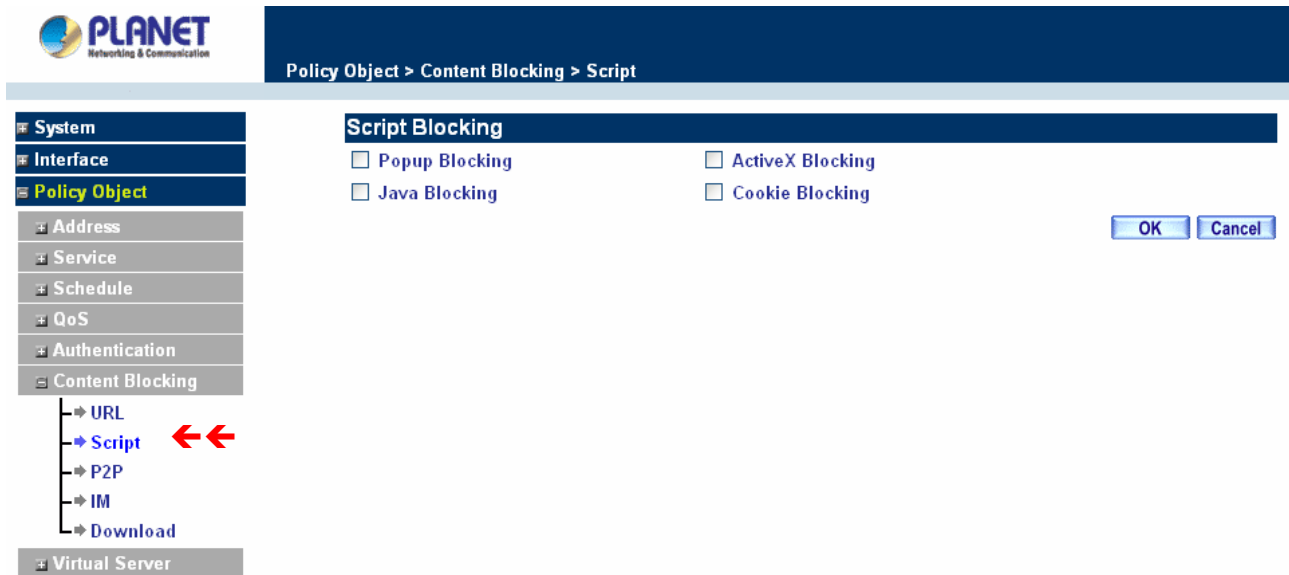
Popup Blocking: Prevent pop-up boxes from appearing.

ActiveX Blocking: Prevent ActiveX packets.

Java Blocking: Prevent Java packets.

Cookie Blocking: Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.



Step 4: Configure Outgoing Policy rule to enable Content Blocking Function.

When the system detects the setting, the Multi-Homing Security Gateway will spontaneously work.

3.3.6.3 P2P

Step 1: Click **P2P** below **Content Blocking** menu.

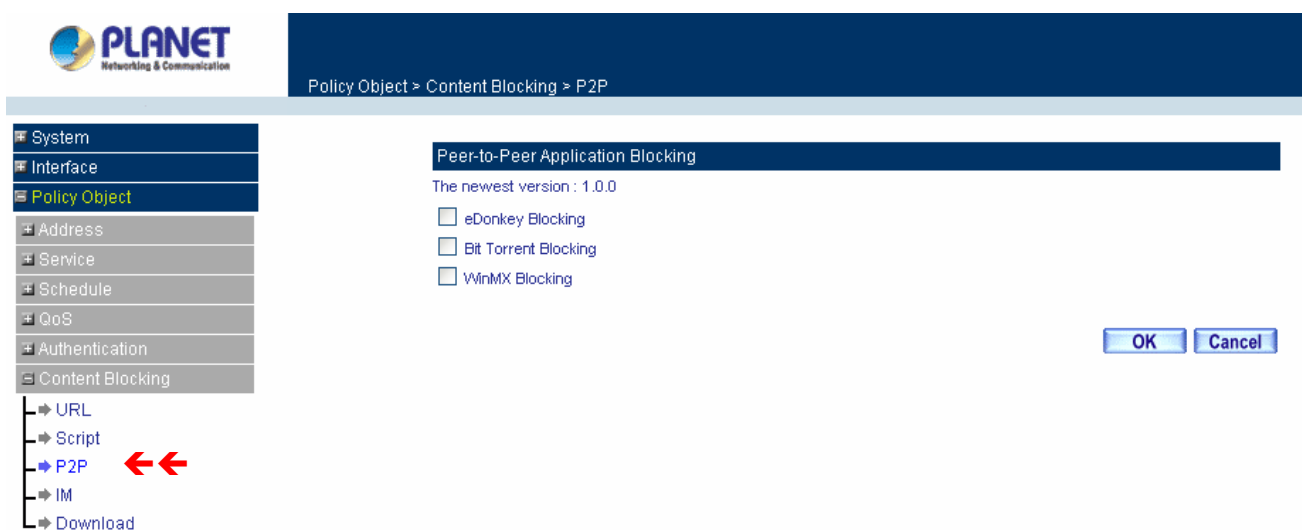
Step 2: Select **P2P** detective functions:

eDonkey Blocking: Prevent eDonkey connection built up.

Bit Torrent Blocking: Prevent Bit Torrent connection built up.

WinMX Blocking: Prevent WinMX connection built up.

Step 3: After selecting each function, click the **OK** button below.



Step 4: Configure Outgoing Policy rule to enable Content Blocking Function.

CS-1000 provides a feature that will auto detect the P2P program version. When it detects a new version P2P program in the LAN site, CS-1000 will connect to Internet and download the pattern to update the P2P Blocking function, and to keep the function working well to block new version P2P program. The current pattern version will display at the top side.

3.3.6.4 IM

Step 1: Click **IM** below **Content Blocking** menu.

Step 2: Select **IM** detective functions:

MSN Messenger Blocking: Select to block MSN Messenger.

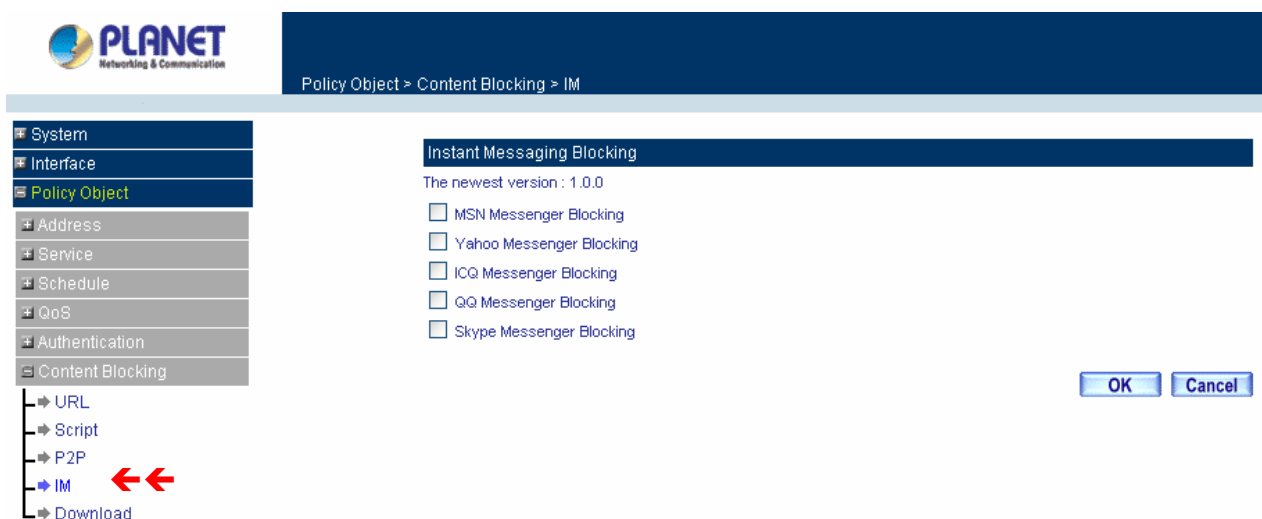
Yahoo Messenger Blocking: Select to block Yahoo Messenger.

ICQ Blocking: Select to block ICQ.

QQ Blocking: Select to block QQ.

Skype Messenger Blocking: Select to block Skype.

Step 3: After selecting each function, click the **OK** button below.



Step 4: Configure Outgoing Policy rule to enable Content Blocking Function.

CS-1000 provides a feature that will auto detect the IM program version. When it detects a new version IM program in the LAN site, CS-1000 will connect to Internet and download the pattern to update the IM Blocking function, and to keep the function working well to block new version IM program. The current pattern version will display at the top side.

3.3.6.5 Download

Step 1: Click **Download** below **Content Blocking** menu.

Step 2: Select **Download** detective functions:

All Types Block: To block all types of the files downloading from web page.

Audio and Video Types block: To block audio and video downloading from web page.

Extensions Block: To block specific extensions name of the files from web page.

Step 3: After selecting each function, click the **OK** button below.

The screenshot shows the PLANET Security Gateway configuration interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object (selected), Address, Service, Schedule, QoS, Authentication, Content Blocking, and Virtual Server. Under 'Content Blocking', the following sub-items are listed: URL, Script, P2P, IM, Download, Upload (highlighted with a blue arrow and two red arrows), and Virtual Server. The main area displays the 'Policy Object > Content Blocking > Upload' configuration. The 'Upload Blocking' section has a checkbox for 'All Types Blocking' which is unchecked. Below this is the 'Extension Blocking' section, which contains a grid of checkboxes for various file extensions: .exe, .iso, .doc, .pdf, .bat, .scr, .pif, .reg, .mpg, .zip, .bin, .xl?, .tgz, .dll, .vb?, .msi, .mp3, .rar, .rpm, .ppt, .gz, .hta, .wps, .com, and .mpeg. All checkboxes are currently unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 4: Configure Outgoing Policy rule to enable Content Blocking Function.

3.3.6.6 Upload

Step 1: Click **Upload** below **Content Blocking** menu.

Step 2: Select **Upload** detective functions:

All Types Block: To block all types of the files downloading from web page.

Extensions Block: To block specific extensions name of the files from web page.

Step 3: After selecting each function, click the **OK** button below.

This screenshot is identical to the one above, showing the PLANET Security Gateway configuration interface. The left sidebar shows the 'Policy Object' menu expanded, with 'Content Blocking' > 'Upload' selected. The main area shows the 'Upload Blocking' configuration with the 'All Types Blocking' checkbox unchecked and the 'Extension Blocking' section containing a grid of unchecked checkboxes for various file extensions (.exe, .iso, .doc, .pdf, .bat, .scr, .pif, .reg, .mpg, .zip, .bin, .xl?, .tgz, .dll, .vb?, .msi, .mp3, .rar, .rpm, .ppt, .gz, .hta, .wps, .com, .mpeg). 'OK' and 'Cancel' buttons are at the bottom right.

Step 4: Configure Outgoing Policy rule to enable Content Blocking Function.

3.3.7 Virtual Server

The Multi-Homing Security Gateway separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally, 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 Multi-Homing Security Gateway's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

The Multi-Homing Security Gateway's Virtual Server can solve this problem. A virtual server has set the real IP address of the Multi-Homing Security Gateway's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Multi-Homing Security Gateway translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server 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 sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping (also called DMZ, De-Militarization Zone) scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which are opposite to NAT), but there are still some differences:

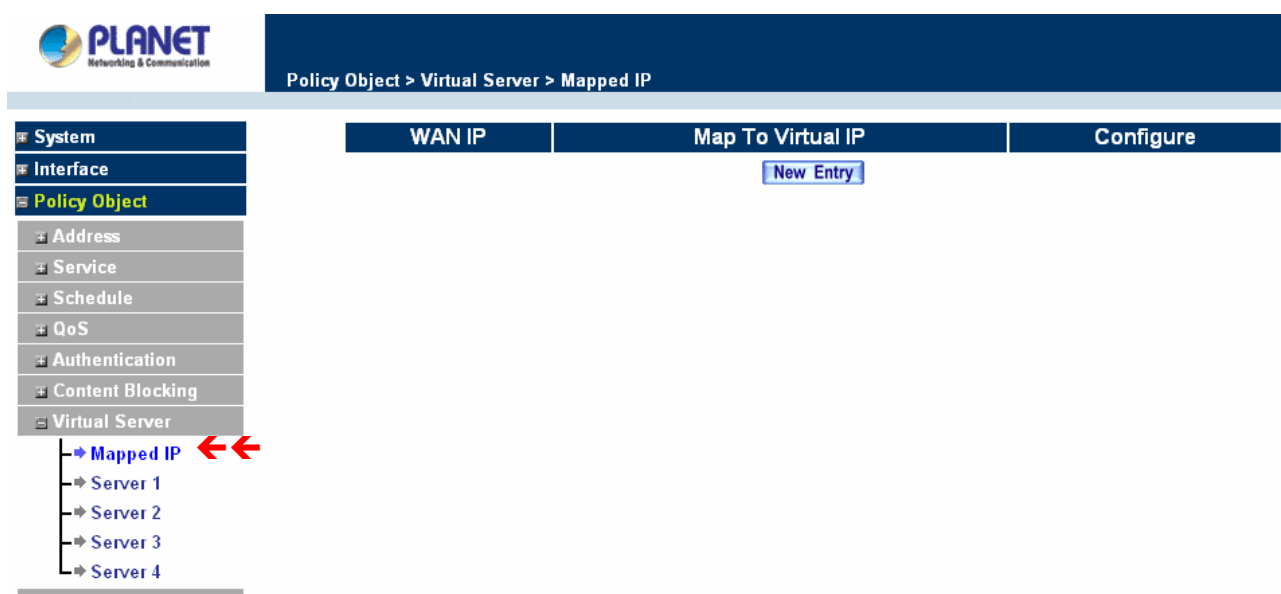
- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

3.3.7.1 Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real WAN IP address is mapped to one private LAN IP address.

Entering the Mapped IP window

- Step 1. Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.



Definition:

WAN IP: WAN IP Address.

Map to Virtual IP: The IP address which WAN maps to the virtual network in the server.


Configure: To change the setting, click Configure to modify the parameters; click delete to delete the setting.

Adding a new IP Mapping

- Step 1. In the **Mapped IP** window, click the New Entry button. The Add New Mapped IP window will appear.

- **WAN IP:** select the WAN public IP address to be mapped.
- **Map to Virtual IP:** enter the LAN private IP address will be mapped 1-to-1 to the WAN IP address.

- Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.



Policy Object > Virtual Server > Mapped IP


System
Interface
Policy Object
Address
Service
Schedule
QoS
Authentication
Content Blocking
Virtual Server
Mapped IP
Server 1
Server 2
Server 3

Add New Mapped IP

WAN IP	<input type="text"/>	Assist
Map To Virtual IP	<input type="text"/>	

Modifying a Mapped IP

- Step 1. In the **Mapped IP** table, locate the Mapped IP you want to be modified and click its corresponding Modify option in the Configure field.
- Step 2. Enter settings in the Modify Mapped IP window.
- Step 3. Click **OK** to save change or click **Cancel** to cancel.



Policy Object > Virtual Server > Mapped IP

System	WAN IP	Map To Virtual IP	Configure
Interface	210.66.155.91	192.168.1.12	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

System
Interface
Policy Object
Address
Service
Schedule
QoS
Authentication
Content Blocking
Virtual Server
Mapped IP
Server 1

NOTE: A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.

Removing a Mapped IP

- Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.
- Step 2. In the Remove confirmation pop-up window, click **OK** to remove the Mapped IP or click **Cancel** to cancel.

Planet Network & Communication

Policy Object > Virtual Server > Mapped IP

System	WAN IP	Map To Virtual IP	Configure
Interface	210.66.155.91	192.168.1.12	Modify Remove

[New Entry](#)

[JavaScript Application]

Are you sure you want to remove ?

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

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Content Blocking

Virtual Server

→ Mapped IP

→ Server 1

→ Server 2

3.3.7.2 Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds a WAN IP to a LAN IP, virtual server binds WAN IP ports to LAN IP ports.

Planet Network & Communication

Policy Object > Virtual Server > Server 1

Virtual Server Real IP [click here to configure](#)

Service	WAN Port	Server Virtual IP	Configure

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Content Blocking

Virtual Server

→ Mapped IP

→ Server 1

→ Server 2

→ Server 3

→ Server 4

Definition:

Virtual Server Real IP: The WAN IP address configured by the virtual server. Click “**Click here to configure**” button to add a real IP address.

Service: The service name that provided by the virtual server.

WAN Port: The TCP/UDP ports that present the service items provided by the virtual server.

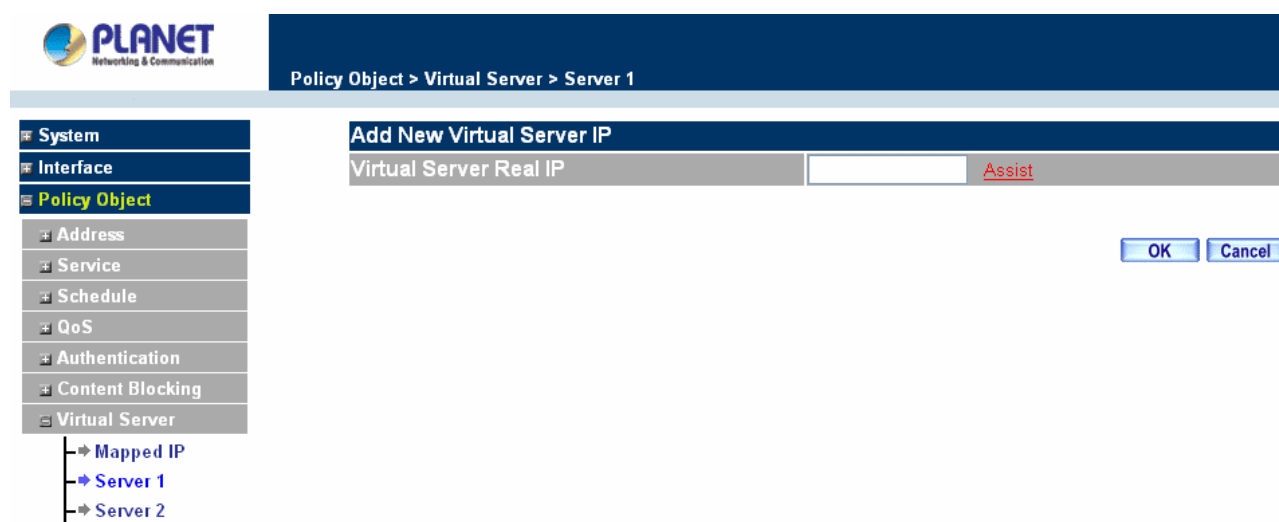
Server Virtual IP: The virtual IP which mapped by the virtual server.

Configure: To change the service configuration, click **Configure** to change the parameters; click **Delete** to delete the configuration.

This virtual server provides four real IP addresses, which means you can setup four virtual servers at most. The administrator can select Virtual Server1/2/3/4 under Virtual Server selection in the menu bar on the left hand side, click **Server Virtual IP** to add or change the virtual server IP address; click “**Click here to configure**” to add or change the virtual server service configuration.

Configuring a Real IP for a Virtual Server

- Step 1. Click an available virtual server from **Server 1/2/3/4** in the **Virtual Server** menu bar to enter the virtual server configuration window.
- Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the WAN network.
- Step 3. Select an IP address from the drop-down list of available WAN network IP addresses.
- Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.



Modifying a Virtual Server IP Address

- Step 1. Click the **Server 1/2/3/4** to modify the configuration under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.
- Step 2. Click on the Virtual Server's IP Address button at the top of the screen.
- Step 3. Choose a new IP address from the drop-down list.
- Step 4. Click **OK** to save new IP address or click **Cancel** to discard changes.

The screenshot shows the Planet Networking & Communication web interface. The breadcrumb navigation at the top reads "Policy Object > Virtual Server > Server 1". On the left, a sidebar menu is expanded to "Virtual Server", showing sub-items: "Mapped IP", "Server 1", and "Server 2". The main content area displays "Virtual Server Real IP" with the value "210.66.155.91" in a text box. Below this is a table with four columns: "Service", "WAN Port", "Server Virtual IP", and "Configure". A "New Entry" button is located below the table.

Removing a Virtual Server

- Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.
- Step 2. Click the Virtual Server's IP Address button at the top of the screen.
- Step 3. Delete the IP address.
- Step 4. Click **OK** to remove the virtual server.

The screenshot shows the Planet Networking & Communication web interface with the same breadcrumb navigation and sidebar menu as the previous screenshot. A dialog box titled "Add New Virtual Server IP" is open. It contains a "Virtual Server Real IP" field with a text input box and a red "Assist" link. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Adding New Virtual Server Service Configuration

- Step 1. Select Virtual Server in the menu bar on the left hand side, and then select Server 1/2/3/4 sub-selections.
- Step 2. In Server 1/2/3/4 Window, click "**New Entry**" button.
- Step 3. Enter the parameters in the Virtual Server Configuration column.



Policy Object > Virtual Server > Server 1

System	Virtual Server Configuration	
Interface	Virtual Server Real IP	210.66.155.91
Policy Object	Service	HTTP (80) <input type="button" value="v"/>
Address	External Service Port	80
Service	Load Balance Server	Server Virtual IP
Schedule	1	192.168.1.20
QoS	2	192.168.1.21
Authentication	3	192.168.1.22
Content Blocking	4	192.168.1.23
Virtual Server		

- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- **Service (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.

NOTE:

1. Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.
2. The services in the drop-down list are all defined in the Pre-defined and Custom section of the **Service** menu.

Modifying the Virtual Server configurations

- Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.
- Step 2. In the Virtual Server Configuration window, enter the new settings.
- Step 3. Click **OK** to save modifications or click **Cancel** to discard changes.



Policy Object > Virtual Server > Server 1

- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - QoS
 - Authentication
 - Content Blocking
 - Virtual Server
 - Mapped IP
 - Server 1
 - Server 2

Virtual Server Real IP 210.66.155.91

Service	WAN Port	Server Virtual IP	Configure
HTTP (80)	80	192.168.1.20	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
		192.168.1.21	
		192.168.1.22	
		192.168.1.23	

Click **OK** to execute the change of the virtual server, or click **Cancel** to discard changes.

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server, you have to remove this configuration of Policy, and then you can execute the modification or configuration.

Removing the Virtual Server service

- Step 1. In the Virtual Server window's service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.
- Step 2. In the Remove confirmation pop-up box, click **OK** to remove the service or click **Cancel** to cancel removing.

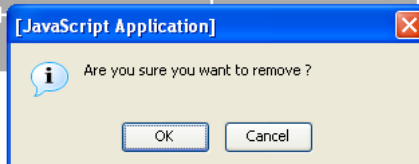


Policy Object > Virtual Server > Server 1

- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - QoS
 - Authentication
 - Content Blocking
 - Virtual Server
 - Mapped IP
 - Server 1
 - Server 2

Virtual Server Real IP 210.66.155.91

Service	WAN Port	Server Virtual IP	Configure
		192.168.1.20	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
		192.168.1.21	
		192.168.1.22	
		192.168.1.23	



NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server unless you have already removed this configuration of Policy.

3.3.8 VPN

The CS-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. It also provides the remote users a safe encryption way to have best efficiency and encryption when delivering data. CS-1000 provides two kinds of VPN service and the PPTP client.

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. It also can set up IPSec Lifetime and Preshared Key of the CS-1000.

PPTP Server: The System Manager can set up VPN-PPTP Server functions at CS-1000 in this chapter.

PPTP Client: The System Manager can set up VPN-PPTP Client functions at CS-1000 in this chapter.

Trunk: To define local and remote VPN device with related information, it also can be configured to enable VPN Trunk function. **Trunk** entry must be selected in **Policy** to submit the further function to the VPN traffic.

What is New?

CS-1000 isolates the **Trunk** setting in order to allow **Policy** rule controlling VPN traffic. So user can filter the VPN packets with **QoS**, **IDP** rule, and record the connection in **Traffic Log** or **Statistic**. Hence, to set up a **Virtual Private Network** (VPN), you need to configure CS-1000 with following setting:

1. Configure **IPSec Autokey** for the encryption and authentication or **PPTP Server/Client** setting.
2. Configure **Trunk** for the information of local and remote VPN device.
3. Configure **Policy** rule to combine VPN traffic with QoS, IDP and the other function.

3.3.8.1 IPSec Autokey

This chapter describes steps to create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. For example, with two Multi-Homing Security Gateway devices, IKE allows new keys to be generated after a set amount of time has passed or a certain threshold of traffic has been exchanged.

Accessing the Autokey IKE window

Click **IPSec Autokey** under the VPN menu to enter the **IPSec Autokey** window. The **IPSec Autokey** table displays current configured VPNs.



The fields in the IPsec Autokey window are:

- **Name:** The VPN name to identify the VPN tunnel definition. The name must be different with Trunk name and the other IPsec rule name.
- **WAN:** The specific WAN port to be configured as VPN tunnel.
- **Gateway IP:** The other side WAN interface IP address of VPN Gateway.
- **IPsec Algorithm:** The display the Algorithm way.
- **Configure:** Modify and Delete.

Adding the Autokey IKE

Step 1: Click the **New Entry** button and the **IPsec Autokey** window will appear. It divides into two parts of the setting, **Necessary Item** and **Optional Item**.

Policy Object > VPN > IPsec Autokey

Necessary Item

Name:

WAN interface: ☒ WAN 1 ☐ WAN 2

To Destination: ☒ Remote Gateway or Client -- Fixed IP or Domain Name

☐ Remote Gateway or Client -- Dynamic IP

Authentication Method:

Preshared Key:

Encapsulation:

ENC Algorithm:

AUTH Algorithm:

Group:

IPsec Algorithm: ☒ Data Encryption + Authentication

ENC Algorithm:

AUTH Algorithm:

☐ Authentication Only

Optional Item

Perfect Forward Security:

ISAKMP Lifetime: Seconds

IPsec Lifetime: Seconds

Mode: ☒ Main mode ☐ Aggressive mode

My ID:

Peer ID:

GRE/IPsec:

GRE Remote IP:

Dead Peer Detection: Retry times Timeout Second (Retry 0 : means disable)

OK Cancel

Step 2: Configure **Necessary Item** parameters.

Name: Specify a name for the VPN rule.

WAN interface: Select WAN 1 or WAN 2 to be the WAN port of VPN connection.

To Destination:

- **Remote Gateway – Fixed IP or Domain Name:** Specify the fixed IP address or domain name of the remote side VPN gateway.
- **Remote Gateway or Client – Dynamic IP:** Select **Remote Gateway or Client** if there is only one user or device in remote site and dials up to Internet with PPPoE or cable modem.

Preshared Key: The IKE VPN must be defined with a Preshared Key.

Encapsulation

ISAKMP Algorithm

- **ENC Algorithm:** ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. The available encryption algorithms including: 56 bit DES-CBC, 168-bit 3DES-CBC, AES 128-bit, AES 192-bit or AES 256-bit encryption algorithm. The default algorithm 56 bit DES-CBC.
- **AUTH Method:** Authentication Method. Selects MD5 (128-bit hash) or SHA-1 (160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.
- **Group:** Selects Group 1 (768-bit modulus), Group 2 (1024-bit modulus) or Group 5 (1536-bit modulus). The larger the modulus, the more secure the generated key is. However, the larger the modulus, the longer the key generation process takes. Both side of VPN tunnels must agree to use the same group. The default algorithm is Group 1.

IPSec Algorithm: Select Data Encryption + Authentication or Authentication Only.

Data Encryption + Authentication

- **Encryption Algorithm:** Selects 56 bit DES-CBC, 168-bit 3DES-CBC, AES 128-bit, AES 192-bit or AES 256-bit encryption algorithm. The default algorithm is 56 bit DES-CBC.
- **Authentication Algorithm:** Selects MD5 (128-bit hash) or SHA-1 (160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.

Authentication Only: Select this function the IPSec Algorithm will only be authenticated with preshared key.

Step 3: Configure **Optional Item** paremeters if necessary.

- **Perfect Forward Secrecy:** Select Group 1, Group 2 or Group 5 to enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. The default is NO-PFS.
- **ISAKMP Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 3600 seconds (one hours). Selection of small values could lead to frequent re-keying, which could affect performance.

- **IPSec Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 28800 seconds (eight hours). Selection of small values could lead to frequent re-keying, which could affect performance.
- **Mode:** Select Main mode or Aggressive mode algorithm.
- **My ID/Peer ID:** My ID and Peer ID are optional parameters. If we choose to enter My ID/ Peer ID, they couldn't be the same. For instance, My ID is 11.11.11.11 and Peer ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123A and @abcd123.
- **GRE/IPSec:** Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology. You may enter IP to be identified for both VPN gateways. The GRE/IPsec IP address can not set as the same as CS-1000's WAN or LAN IP subnet.
- **Dead Peer Detection Retry times Timeout Second:** CS-1000 will check the VPN tunnel status according to this configuration, when CS-1000 does not receive the response, it will stops the VPN connection and keep detecting the VPN status in order to revive the VPN connection. Retry 0 times means to disable the function.

For the complete VPN setting, you can refer to the example for more detail information.

3.3.8.2 PPTP Server

This function allows the remote client dialup to your local network and access local resources by PPTP (Point to Point Tunnel Protocol) client software.

Entering the PPTP Server window: Select **VPN**→**PPTP Server**.



- **PPTP Server :** Click **Modify** to select Enable or Disable.
- **Client IP Range:** Display the IP addresses range for PPTP Client connection.
- **User Name :** Displays the PPTP Client user's name for authentication.
- **Client IP :** Displays the PPTP Client's IP address for authentication.

- **Uptime** : Displays the connection time between PPTP Server and Client.
- **Configure** : Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Modifying PPTP Server Design

- Step 1. Select **VPN**→**PPTP Server**.
- Step 2. Click **Modify** after the Client IP Range.
- Step 3. In the **Modify** Server Design Window, enter appropriate settings.

- **Disable PPTP**: Check to disable PPTP Server.
- **Enable PPTP**: Check to enable PPTP Server.
Encryption: the default is set to disabled.
Client IP Range: Enter the IP range allocated for PPTP Clients when they connect to the PPTP server.
- **Allow remote client to connect to Internet**: Check to allow remote PPTP client accessing Internet via PPTP tunnel.
- **Auto-Disconnect if idle minutes**: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Echo-Request Retry times Timeout Second**: CS-1000 will check the VPN tunnel status according to this configuration, when CS-1000 does not receive the response, it will stops the VPN connection and keep detecting the VPN status in order to revive the VPN connection. Retry 0 times means to disable the function.

- Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Adding PPTP Server

Step 1. Select **VPN**→**PPTP Server**. Click **New Entry**.

Step 2. Enter appropriate settings in the following window.

- User name: Specify the PPTP client. This should be unique.
- Password: Specify the PPTP client password.
- Client IP assigned by:
 1. IP Range: check to enable auto-allocating IP for PPTP client to connect.
 2. Fixed IP: check and enter a fixed IP for PPTP client to connect.

The screenshot shows the PLANET Network & Communication web interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object (selected), Address, Service, Schedule, QoS, Authentication, Content Blocking, Virtual Server, and VPN. Under the VPN item, there are sub-items: IPsec Autokey, PPTP Server (selected), PPTP Client, and Tunnel. The main content area has a breadcrumb trail: Policy Object > VPN > PPTP Server. The 'Add New PPTP Server' window is open, showing the following fields: User Name (text input), Password (text input), Client IP assigned by (radio buttons for IP Range and Fixed IP). The IP Range radio button is selected. There are OK and Cancel buttons at the bottom right.

Step 3. Click **OK** to save modifications or click **Cancel** to cancel modifications.

Modifying PPTP Server

Step 1. Select **VPN**→**PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you want to modify. Click **Configure** and click **Modify**.

Step 3. Enter appropriate settings.

The screenshot shows the PLANET Network & Communication web interface. The left sidebar is the same as in the previous screenshot. The main content area has a breadcrumb trail: Policy Object > VPN > PPTP Server. The 'PPTP Server (Enable, Encryption:ON)' window is open. It shows the Client IP Range: 192.238.6.1-254 and a Modify button. Below this is a table with the following columns: i, User Name, Client IP, Uptime, and Configure. The table contains one entry with User Name 'planet' and Client IP '0.0.0.0'. The Configure column for this entry has Modify and Remove buttons. A New Entry button is located below the table.

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

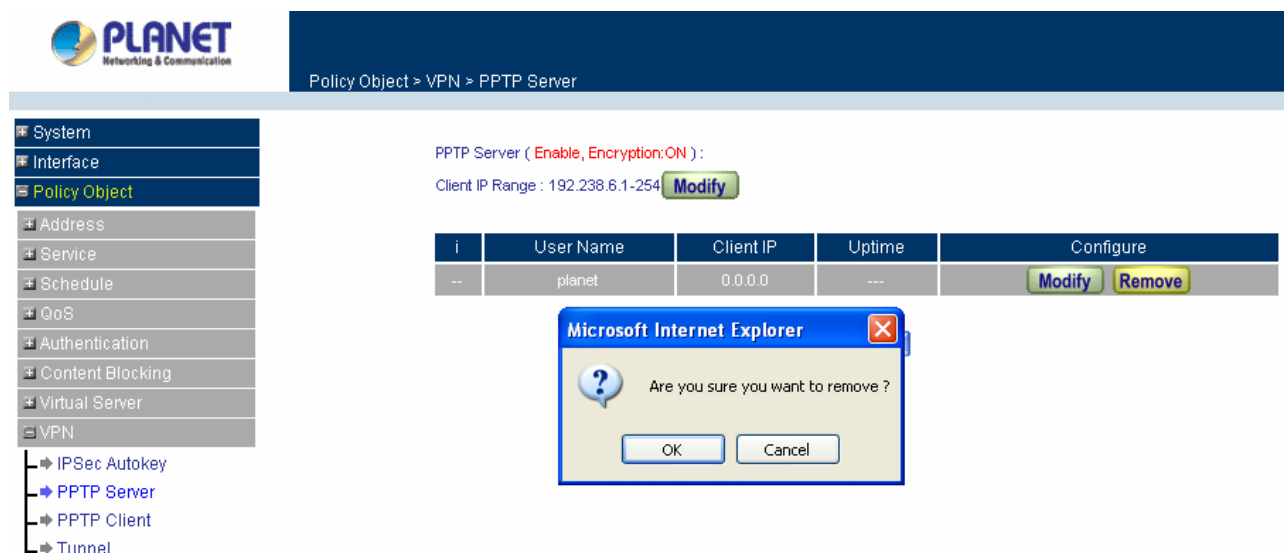
Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Server

Step 1. Select **VPN**→**PPTP Server**.

Step 2. In the **PPTP Server** window, find the PPTP server that you want to modify. Click **Configure** and click **Remove**.

Step 3. Click **OK** to remove the PPTP server or click **Cancel** to exit without removing.



PLANET Networking & Communication

Policy Object > VPN > PPTP Server

PPTP Server (Enable, Encryption:ON):

Client IP Range : 192.238.6.1-254 [Modify](#)

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

Microsoft Internet Explorer

Are you sure you want to remove ?

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

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Content Blocking

Virtual Server

VPN

IPSec Autokey

PPTP Server

PPTP Client

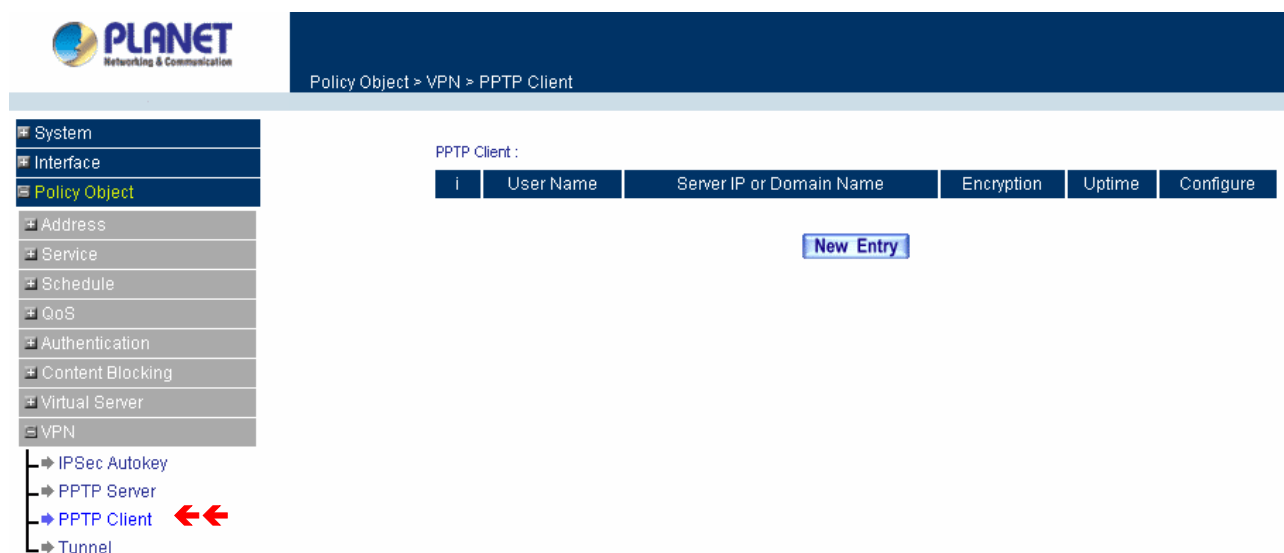
Tunnel

3.3.8.3 PPTP Client

This function allows the Multi-Homing Security Gateway dial-up to remote PPTP server and accesses the network resources on remote network.

Entering the PPTP Client window

Step 1. Select **VPN**→**PPTP Client**.



PLANET Networking & Communication

Policy Object > VPN > PPTP Client

PPTP Client :

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

System

Interface

Policy Object

Address

Service

Schedule

QoS

Authentication

Content Blocking

Virtual Server

VPN

IPSec Autokey

PPTP Server

PPTP Client ←←

Tunnel

- **User Name** : Displays the PPTP Client user's name for authentication.
- **Server IP or Domain Name** : Displays the PPTP Server's IP address or Domain name.
- **Encryption** : Displays the PPTP Client Encryption ON or OFF.
- **Uptime** : Displays the connection time between PPTP Server and Client.
- **Configure** : Click **Modify** to modify the PPTP Client settings or click **Remove** to remove the item.

Adding a PPTP Client

Step 1. Select **VPN**→**PPTP Client**.

The screenshot shows the PLANET Network & Communication web interface. On the left is a navigation tree with the following items: System, Interface, Policy Object (highlighted), Address, Service, Schedule, QoS, Authentication, Content Blocking, Virtual Server, and VPN. Under the VPN item, there are sub-items: IPsec Autokey, PPTP Server, PPTP Client (highlighted with a blue arrow), and Tunnel. The main content area has a breadcrumb trail: Policy Object > VPN > PPTP Client. A modal window titled 'Add New PPTP Client' is open, containing the following fields:

- User Name : planet
- Password : (masked with four dots)
- Server IP or Domain Name : 61.20.30.40
- Encryption : ☒ (checked)
- NAT(Connect to Windows PPTP Server) : ☐ (unchecked)

 At the bottom right of the modal are 'OK' and 'Cancel' buttons.

Step 2. Configure the parameters.

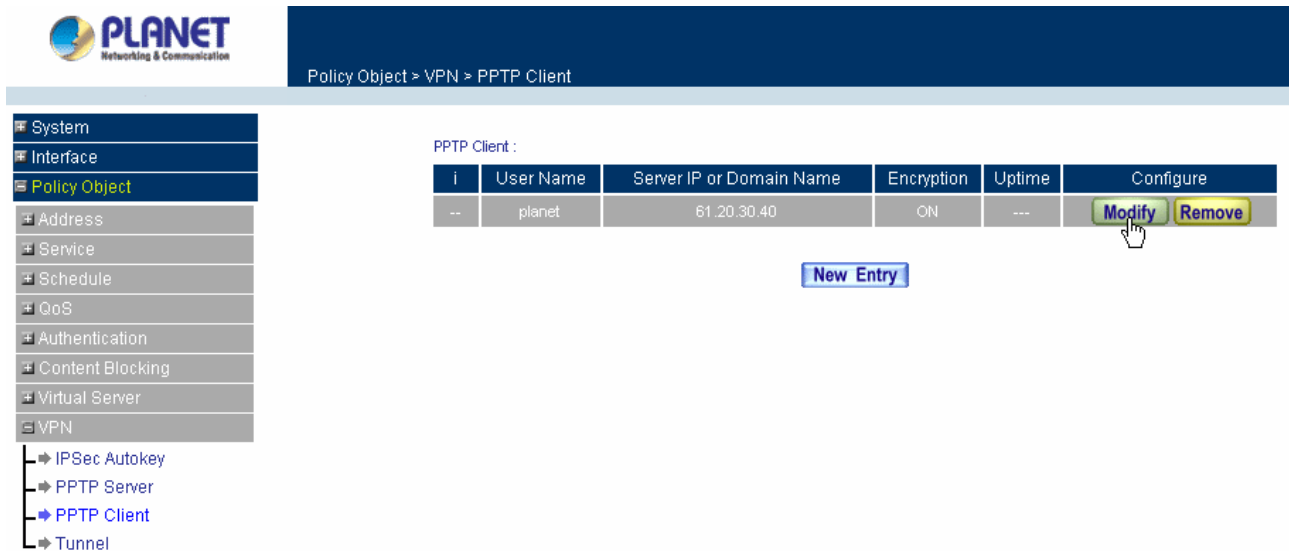
- **User name**: Specify the PPTP client. This should be unique.
- **Password**: Specify the PPTP client password.
- **Server IP or Domain Name**: Enter the PPTP Server's IP address.
- **Encryption**: Enable or Disabled the Encryption.
- **WAN interface**: Check to select WAN interface to connect PPTP server.
- **NAT (Connect to Windows PPTP Server)**: Select this function to setup the connection with PPTP VPN Client of CS-1000 and Windows PPTP Server.

Modifying PPTP Client

Step 1. Select **VPN**→**PPTP Client**.

Step 2. In the **PPTP Client** window, find the PPTP server that you want to modify and click **Modify**.

Step 3. Enter appropriate settings.



PLANET Networking & Communication

Policy Object > VPN > PPTP Client

PPTP Client :

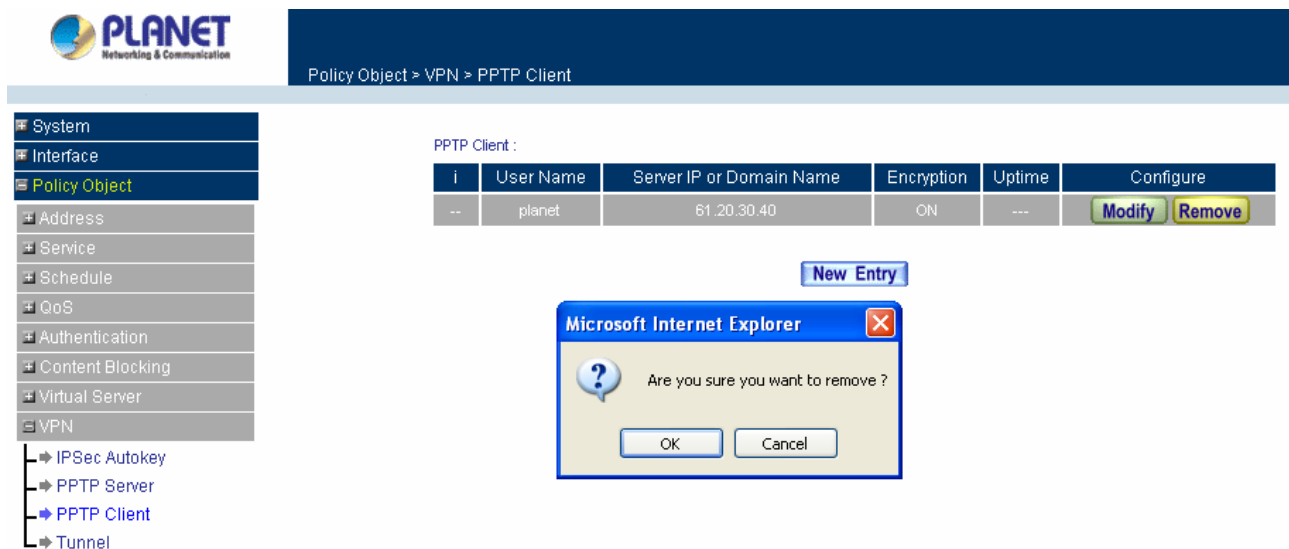
i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	planet	61.20.30.40	ON	---	Modify Remove

New Entry

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Client

- Step 1. Select **VPN**→**PPTP Client**.
- Step 2. In the **PPTP Client** window, find the PPTP client that you want to modify and click **Remove**.
- Step 3. Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.



PLANET Networking & Communication

Policy Object > VPN > PPTP Client

PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	planet	61.20.30.40	ON	---	Modify Remove

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

3.3.8.4 Trunk

This function allows to be configured the related information for local and remote VPN device, then to select the **Trunk** entry in **Policy** rule for combining the further function.

Entering the Trunk window

- Step 1. Select **VPN**→**Trunk**.



Policy Object > VPN > Tunnel

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


- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - QoS
 - Authentication
 - Content Blocking
 - Virtual Server
 - VPN
 - IPSec Autokey
 - PPTP Server
 - PPTP Client
 - Tunnel

Step 2. Configure the parameters

- **Name:** Specify the Trunk name. This should be unique and can not be the same as the name of IPSec Autokey rule.
- **Source Subnet:** Specify the source LAN network subnet.
- **Destination Subnet:** Specify the destination LAN network subnet.
- **Tunnel:** Indicate the Tunnel type for IPSec or PPTP.
- **Configure :** Click **Modify** to modify the Trunk settings, **Pause** to stop the VPN tunnel, or **Remove** to remove the item.

Adding a Trunk

Step 1. Select VPN→Tunnel.



Policy Object > VPN > Tunnel

- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - QoS
 - Authentication
 - Content Blocking
 - Virtual Server
 - VPN
 - IPSec Autokey
 - PPTP Server
 - PPTP Client
 - Tunnel

New Entry Tunnel

Name	IPSecTunnel		
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
From Source Subnet / Mask	192.168.1.0	/	255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client		
	192.168.0.0	/	255.255.255.0
IPSec / PPTP Setting	CS500		
Keep alive IP :	192.168.0.1		
<input type="checkbox"/> Show remote Network Neighborhood			

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

Step 2. Configure the parameters

- **Name:** Specify the Trunk name. This should be unique and can not be the same as the name of IPSec Autokey rule.

- **From Source:** Specify the VPN source to LAN or DMZ site.
- **From Source Subnet / Mask:** Specify the source's LAN network subnet and Mask.
- **To Destination:**
 - **To Destination Subnet / Mask:** Specify the destination LAN network subnet and Mask.
 - **Remote Client:** Select **Remote Client** if there is only one user and dials up to Internet with PPPoE or cable modem.
- **Tunnel:**
 - **Add VPN tunnel:** Select the VPN tunnel you want to add in **Available Tunnel**, and click the **Add>>** button to add them to the **Select Tunnel**.
 - **Remove VPN tunnel:** Select the VPN tunnel you want to remove in **Select Tunnel**, and click the **Remove>>** button to remove them to the **Available Tunnel**.
- **Keep Alive IP:** Specify **Remote Gateway**'s LAN IP address to keep alive the VPN tunnel
- **Show remote Network Neighborhood:** Select to show the remote Network Neighborhood.

Modifying a Trunk

- Step 1. Select **VPN→Trunk**.
- Step 2. In the **Trunk** window, find the Trunk that you want to modify and click **Modify**.
- Step 3. Enter appropriate settings.

PLANET Networking & Communication

Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

New Entry

Removing Trunk

- Step 1. Select **VPN→Trunk**.
- Step 2. In the **Trunk** window, find the Trunk that you want to remove and click **Remove**.

PLANET Networking & Communication

Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

Microsoft Internet Explorer

Are you sure you want to remove "IPSecTunnel" ?

OK Cancel

Click **OK** to remove the Trunk or click **Cancel** to exit without removal.

Pausing a Trunk

Step 1. Select **VPN**→**Trunk**.

Step 2. In the **Trunk** window, find the Trunk that you want to modify and click **Pause**.

PLANET Networking & Communication

Policy Object > VPN > Tunnel

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSecTunnel	192.168.1.0	192.168.0.0	CS500	Modify Remove Pause

Microsoft Internet Explorer

Are you sure you want to pause ? This entry will not be effective.

OK Cancel

Step 3. When Trunk setting is paused, you will be able to change the VPN setting without to remove the Trunk setting first.

There are 5 examples of VPN setting.

Example 1. Create a VPN connection between two Multi-Homing Security Gateways.

Example 2. Create a VPN connection between the Multi-Homing Security Gateway and Windows XP Professional VPN Client.

Example 3. Create a VPN connection between two Multi-Homing Security Gateways using Aggressive mode Algorithm (3DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Example 4. Create a VPN trunk connection between CS-1000 (Company A) and CS-1000 (Company B), using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

Example 5. Create a VPN connection between Multi-Homing Security Gateway and PLANET VRT-311 VPN Router.

Example 1. Create a VPN connection between two Multi-Homing Security Gateways.

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPsec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item	
Name	VPN_A
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare ▼
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

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

Step 6. In IPsec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPsec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPsec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.

Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
------	--

Step 9. Click OK to finish the IPsec Aotkey setting of Company A.

Policy Object > VPN > IPsec Autokey					
i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	Modify Remove

Step 10. Click Trunk and press New Entry to configure the further setting.

Step 11. Enter Site_A as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	Site_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.

To Destination

<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.20.0	/	255.255.255.0
<input type="radio"/> Remote Client			

Step 13. In Tunnel, select VPN_A tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel

< --- Available Tunnel ---> VPN_A	< --- Selected Tunnel --->
<div>Remove</div> <div>Add</div>	

Step 14. Fill company B's gateway IP 192.168.20.1 in Keep alive IP to keep VPN tunnel connecting.

Keep alive IP :

192.168.20.1

Step 15. Click OK to finish the Trunk setting of Company A.

Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	Site_A	192.168.10.0	192.168.20.0	VPN_A	<div>Modify</div> <div>Remove</div> <div>Pause</div>

Step 16. If you want to configure bi-direction VPN connection, you should enable Trunk setting in Outgoing and Incoming Policy.

Policy > Outgoing

Comment :

Modify Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	Site_A
Action, WAN Port	None Site_A
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None

Outgoing Policy:

Policy > Outgoing

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

Incoming Policy:

Policy > Incoming

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

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's Multi-Homing Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPsec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item

Name	VPN_B
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare ▼
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.

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

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 1 ▼
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.

Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
------	--

Step 9. Click OK to finish the IPSec Aotkey setting of Company B.

Policy Object > VPN > IPSec Autokey

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

Step 10. Click Trunk and press New Entry to configure the further setting.

Step 11. Enter Site_B as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.

New Entry Trunk

Name	<input type="text" value="Site_B"/>	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	<input type="text" value="192.168.20.0"/>	<input type="text" value="255.255.255.0"/>

Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	<input type="text" value="192.168.10.0"/> / <input type="text" value="255.255.255.0"/>
<input type="radio"/> Remote Client	

Step 13. In Tunnel, select VPN_B tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel	
<div>< --- Available Tunnel ---></div> <div>VPN_B</div>	<div>< --- Selected Tunnel ---></div> <div>VPN_B</div>
Remove	
Add >>	

Step 14. Fill company A's gateway IP 192.168.10.1 in Keep alive IP to keep VPN tunnel connecting.

Keep alive IP :	<input type="text" value="192.168.10.1"/>
-----------------	---

Step 15. Click OK to finish the Trunk setting of Company B.

Policy Object > VPN > Trunk

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

Step 16. If you want to configure bi-direction VPN connection, you should enable Trunk setting in Outgoing and Incoming Policy.

Outgoing Policy:

Policy > Outgoing										
Source	Destination	Service	Action	Option				Configure		
Inside_Any	Outside_Any	ANY	VPN					Modify	Remove	Pause
Inside_Any	Outside_Any	ANY	✓					Modify	Remove	Pause
										To 1 ▼
										To 2 ▼

Incoming Policy:

Policy > Incoming										
Source	Destination	Service	Action	Option				Configure		
Outside_Any	Inside_Any(Routing)	ANY	VPN					Modify	Remove	Pause
										To 1 ▼

Example 2. Create a VPN connection between the Multi-Homing Security Gateway and Windows XP Professional VPN Client.

Preparation Task:

Company A External IP is 210.66.155.90, Internal IP is 192.168.10.X

Remote User External IP is 210.66.155.91

Remote user with an external IP wants to create a VPN connection with company A and connect to 192.168.10.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Configuration of CS-1000

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPsec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item	
Name	VPN_A
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In to Destination table, choose Remote Gateway or Client – Dynamic IP.

To Destination	
<input type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text"/>
<input checked="" type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare ▼
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item		
Perfect Forward Secrecy	GROUP 2 ▼	
ISAKMP Lifetime	3600	Seconds
IPSec Lifetime	28800	Seconds

Step 8. Select main mode as the algorithm.

Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
------	--

Step 9. Click OK to finish the IPSec Aotkey setting of Company A.

Policy Object > VPN > IPSec Autokey

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

Step 10. Click Trunk and press New Entry to configure the further setting.

Step 11. Enter Site_A as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	Site_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 12. In To Destination table, select Remote Client.

To Destination	
<input type="radio"/> To Destination Subnet / Mask	
<input checked="" type="radio"/> Remote Client	

Step 13. In Tunnel, select VPN_A tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel		
<div>< --- Available Tunnel ---></div> <div>VPN_A</div>	<div>< --- Selected Tunnel ---></div>	<div>Remove</div> <div>Add >></div>

Step 14. Click OK to finish the Trunk setting of Company A.

Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	Site_A	192.168.10.0	Remote Client	VPN_A	Modify Remove Pause

Step 15. Enable Trunk setting in Incoming Policy.

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Trunk	None ▾
Action	None ▾ Site_A
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0: means unlimited)
QoS	None ▾
NAT	<input type="checkbox"/> Enable

Step 16. Click OK to finish the Policy setting of Company A.

Policy > Incoming									
Source	Destination	Service	Action	Option				Configure	
Outside_Any	Inside_Any(Routing)	ANY	VPN					Modify	Remove
								Pause	
									Move To 1 ▾

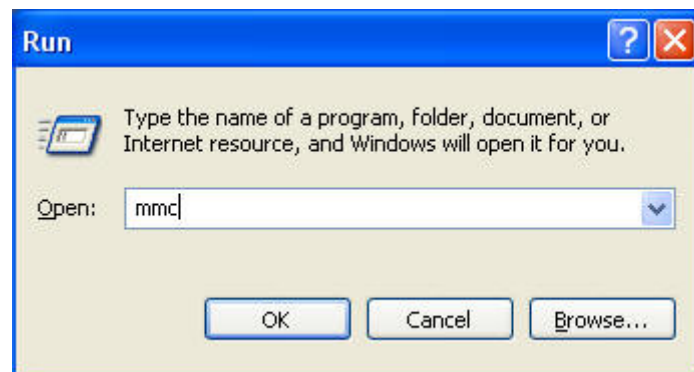
Configuration of WinXP

The IP of remote user is 210.66.155.91. The settings of remote user are as the following.

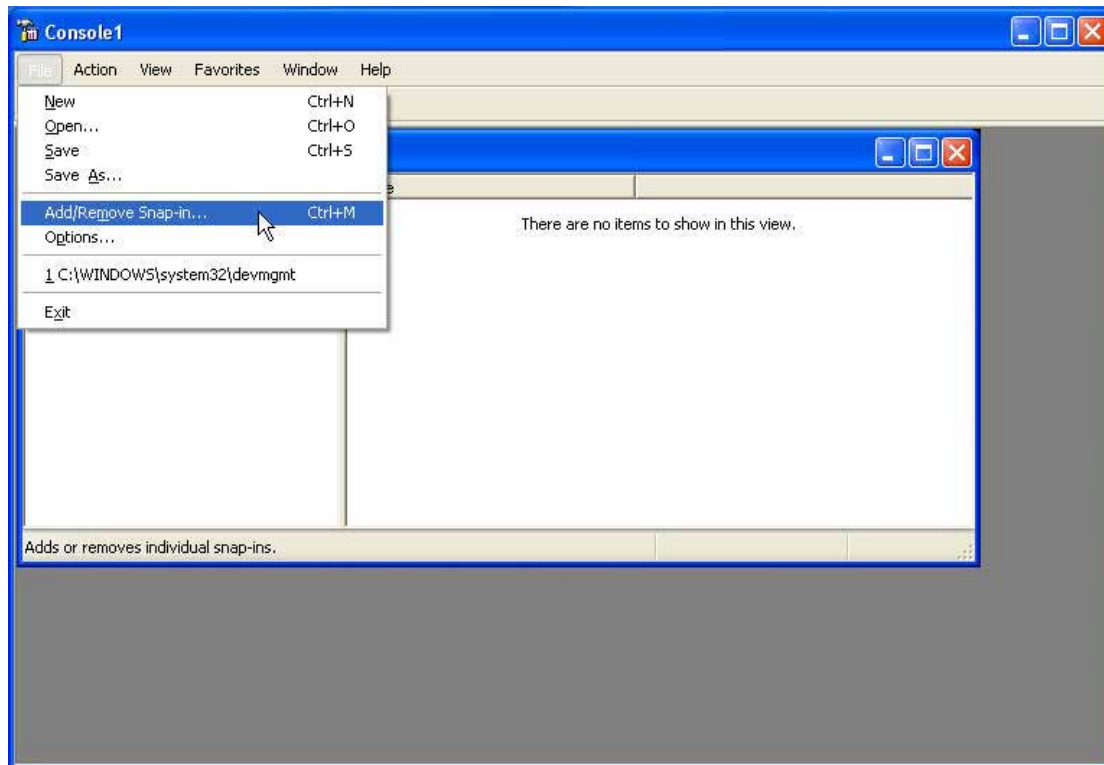
Step 1. Enter Windows XP, click Start and click Execute function.



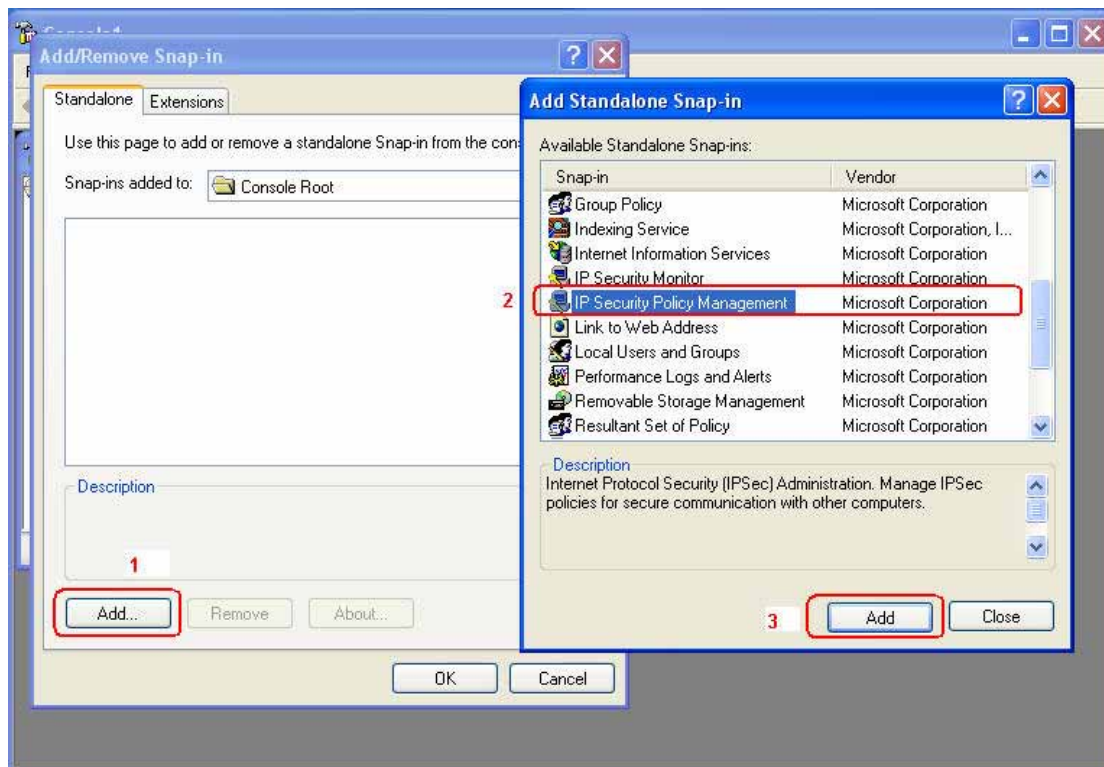
Step 2. In the Execute window, enter the command, mmc in Open.



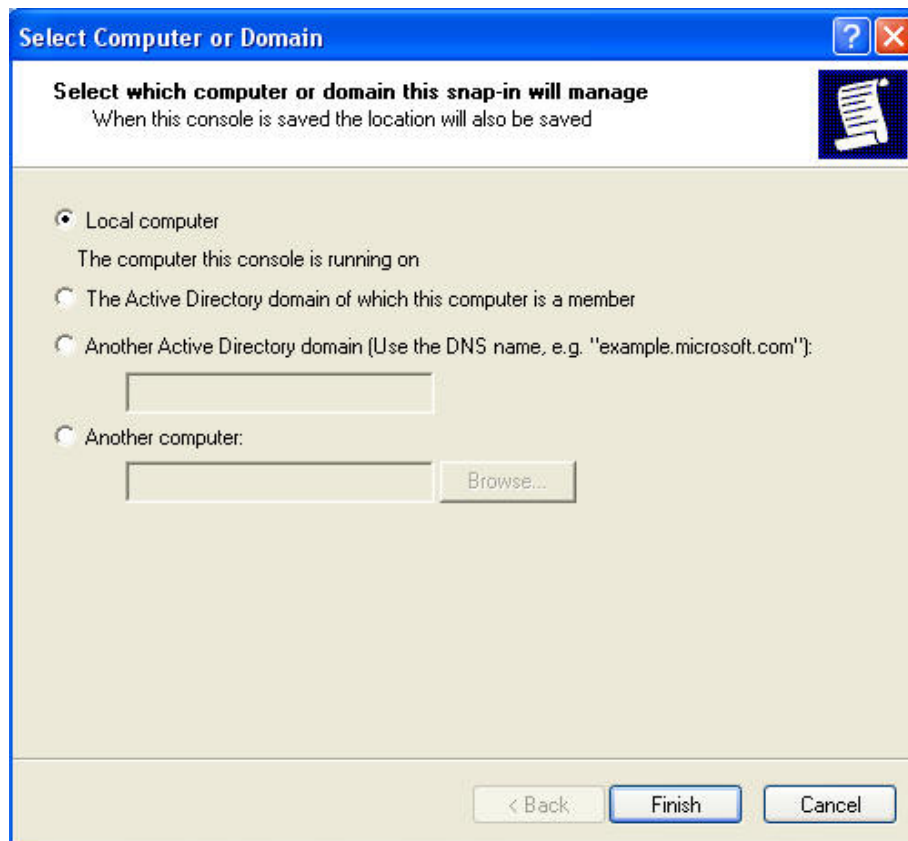
Step 3. Enter the Console window, click Console(C) option and click Add/Remove Embedded Management Option.



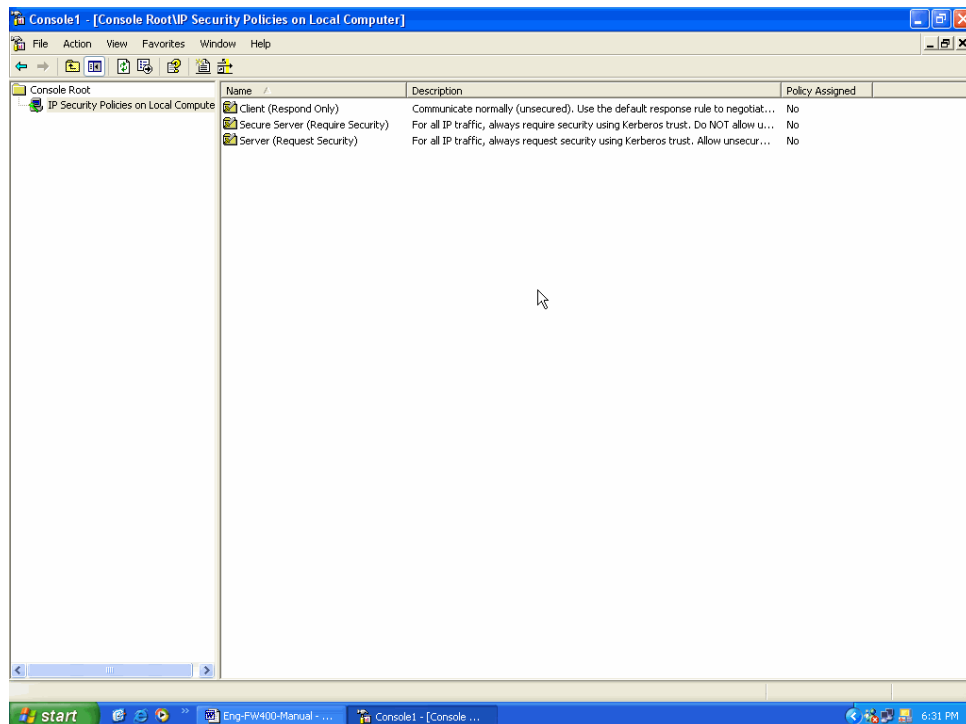
Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.



Step 5. Choose Local Machine (L) for finishing the setting of Add.

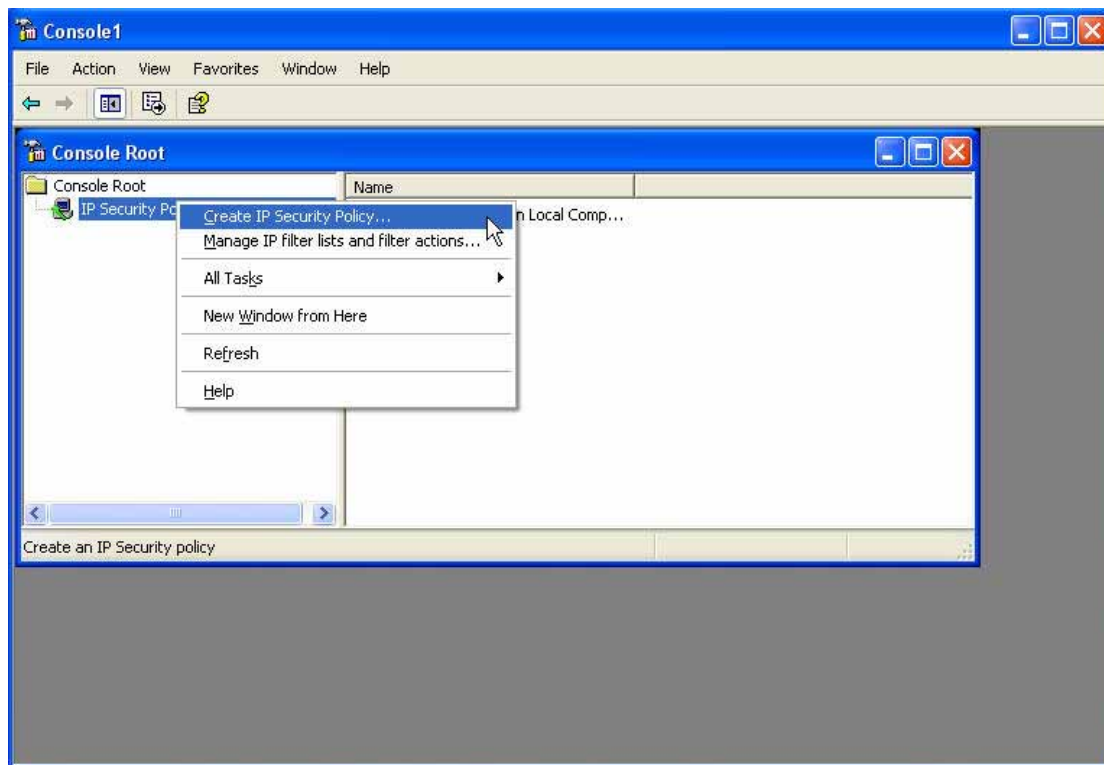


Step 6. Finish the setting of Add.

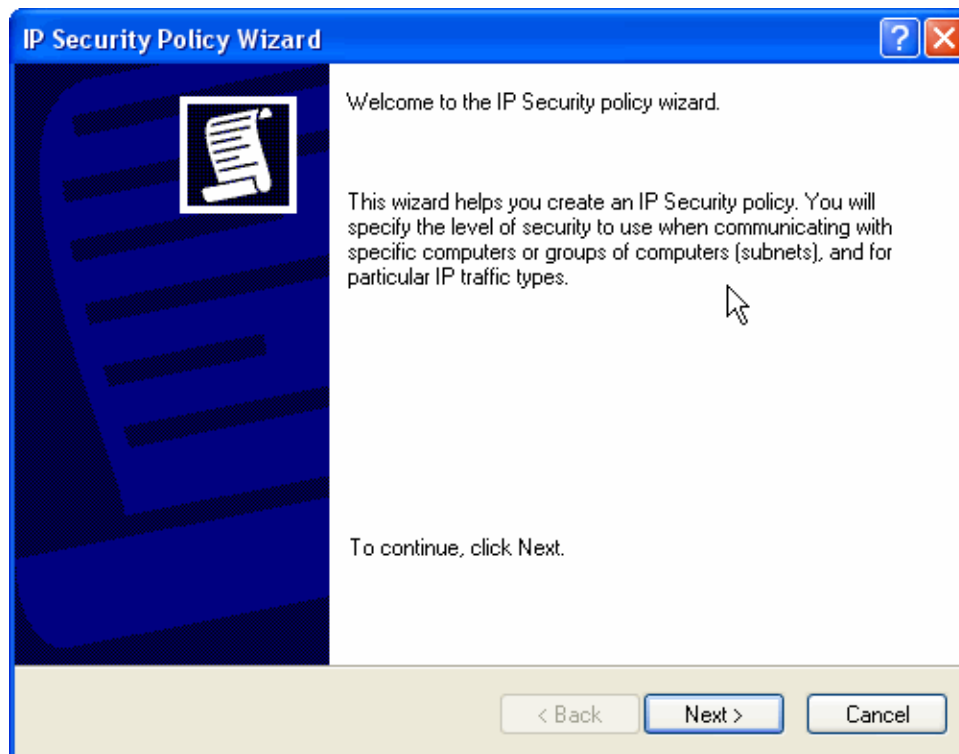


Step 7. Click the right button of mouse in IP Security Policies on Local Machine and choose Create IP

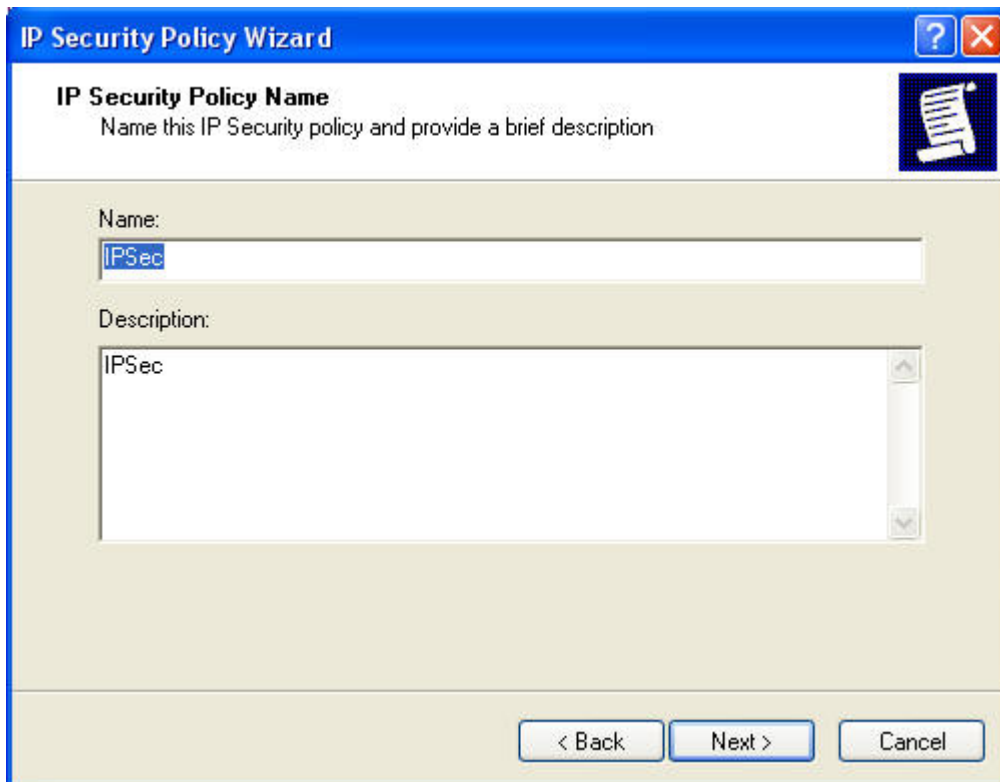
Security Policy(C) option.



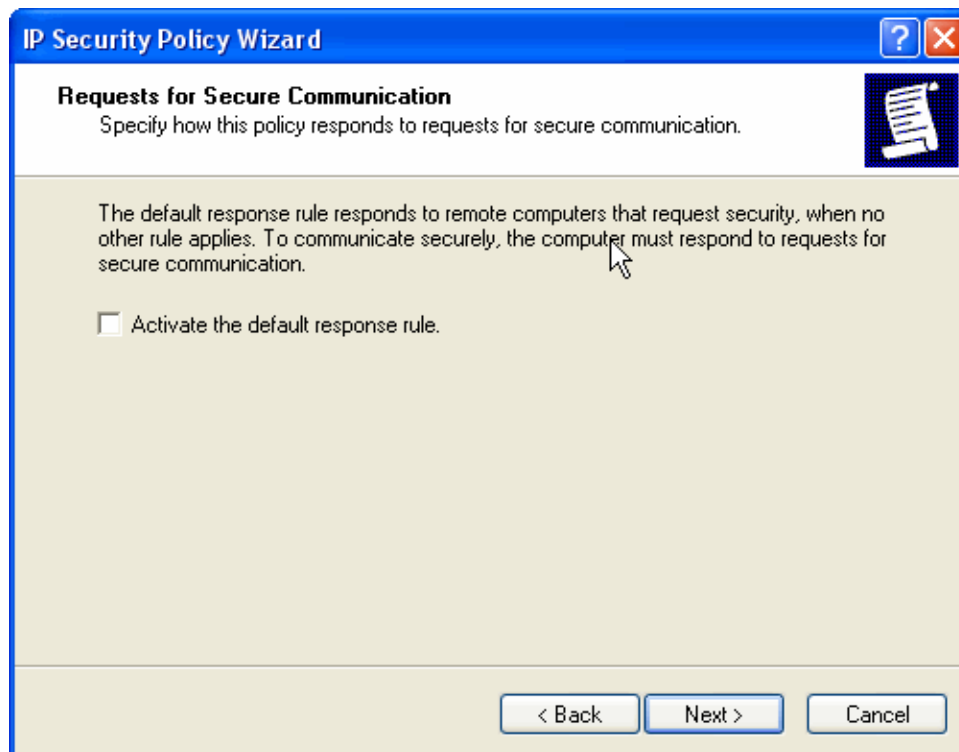
Step 8. Click Next.



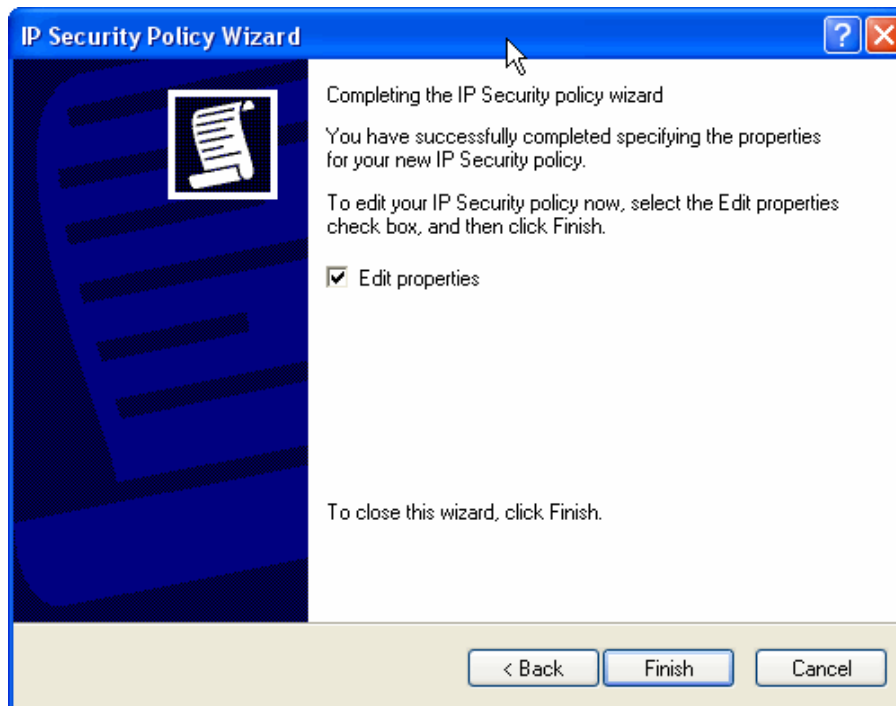
Step 9. Enter the Name of this VPN and optionally give it a brief description.



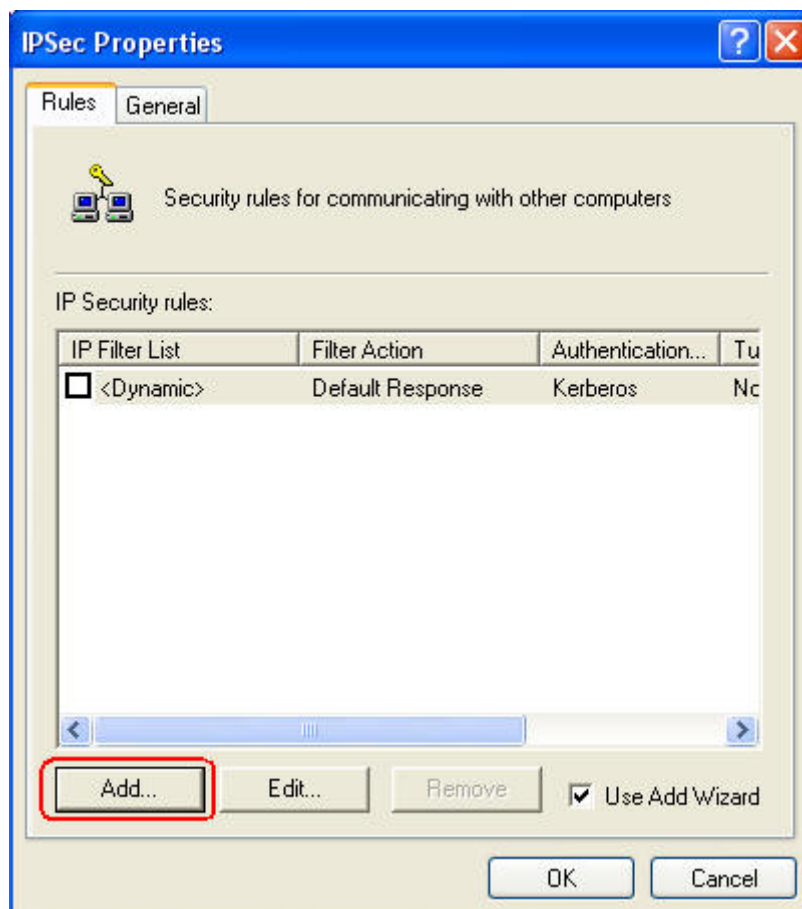
Step 10. Disable **Activate the default response rule**. And click Next.



Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.



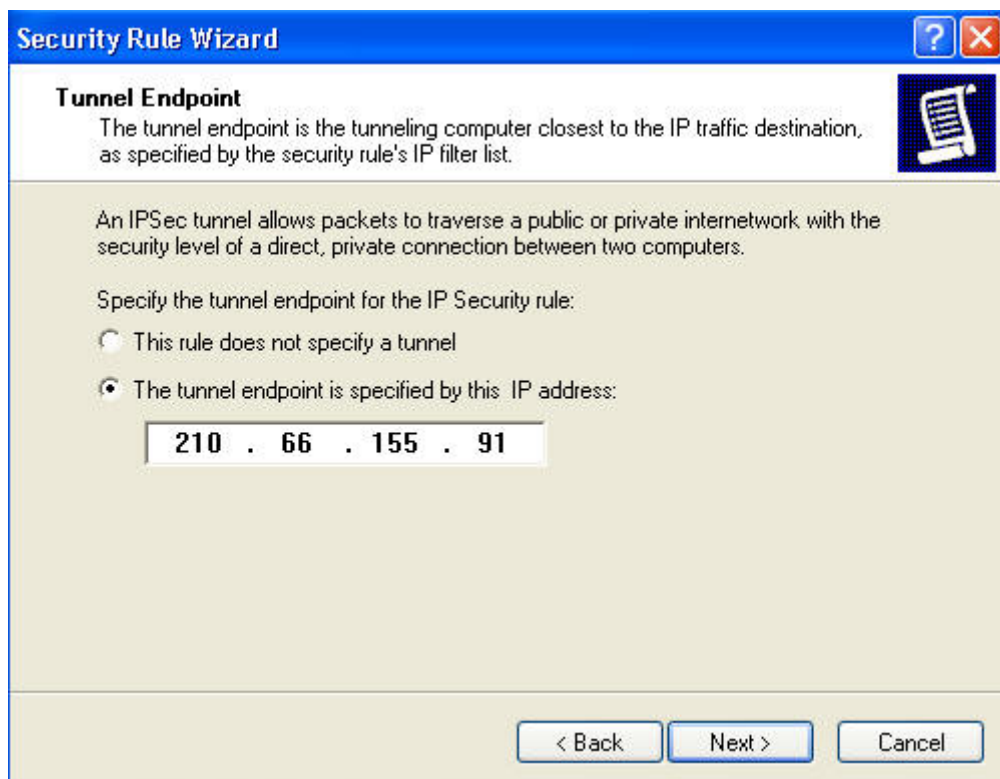
Step 12. In window, click Add and click Use Add Wizard.



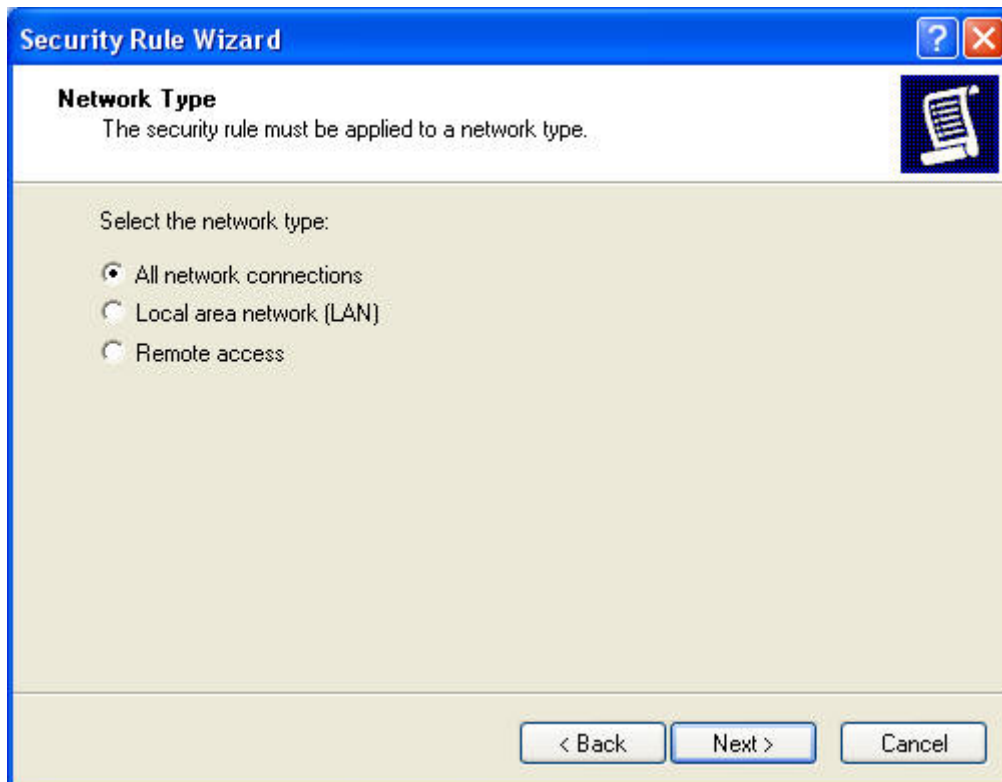
Step 13. Click next.



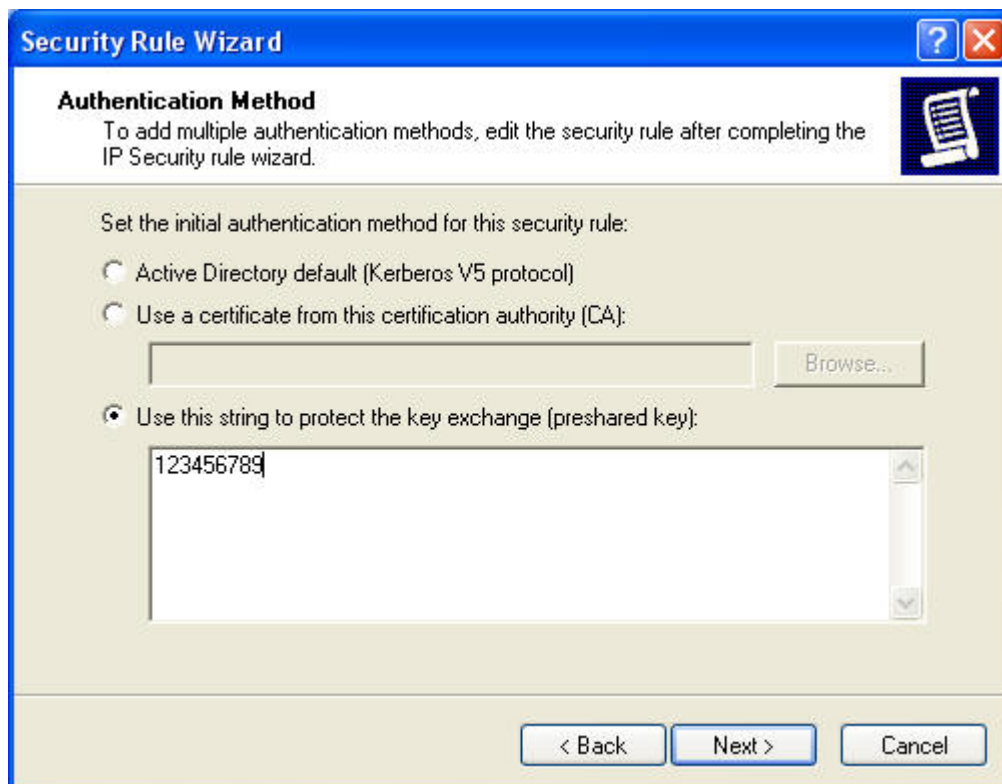
Step 14. Enter the WAN IP of Remote user, 210.66.155.91.



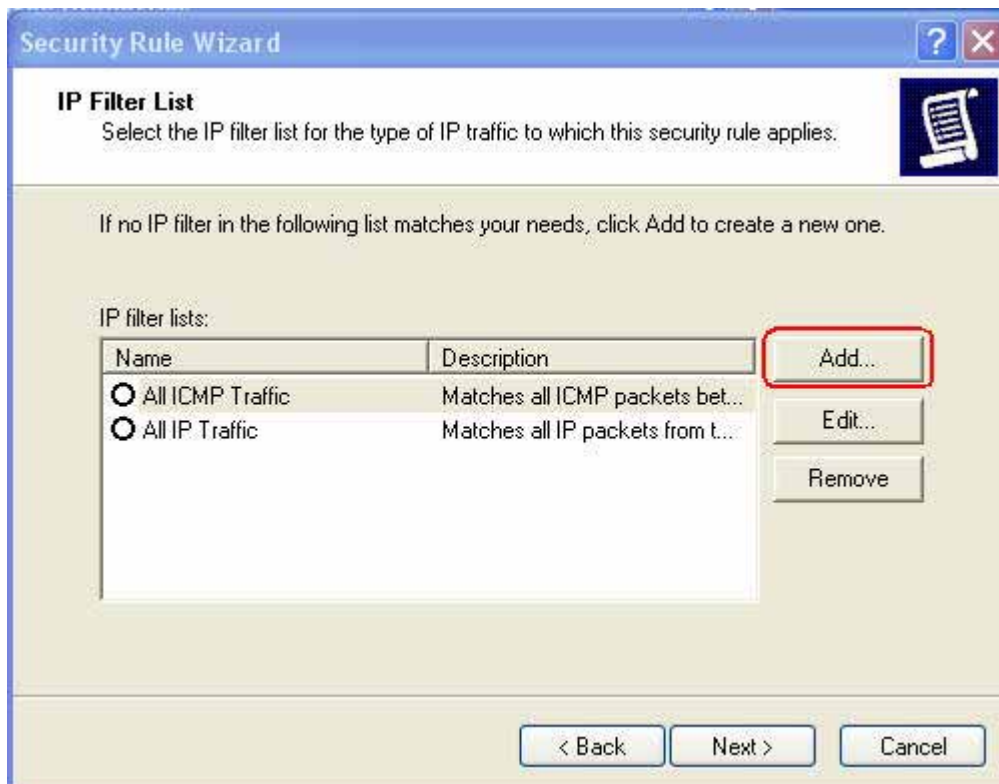
Step 15. click all network connections.



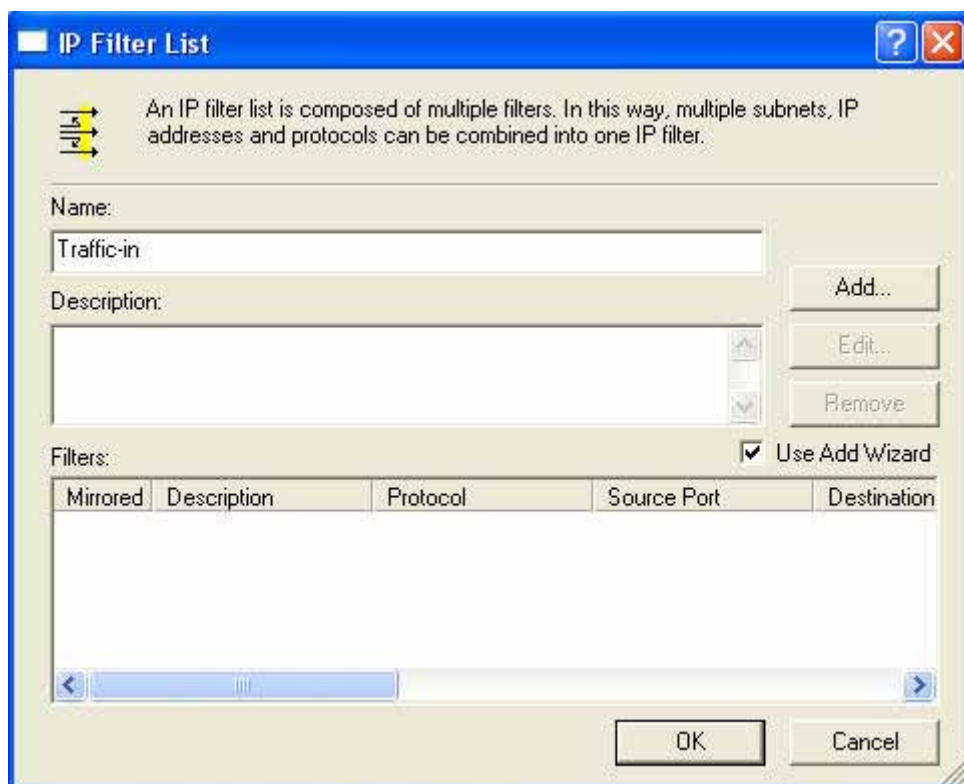
Step 16. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



Step 17. Click Add.



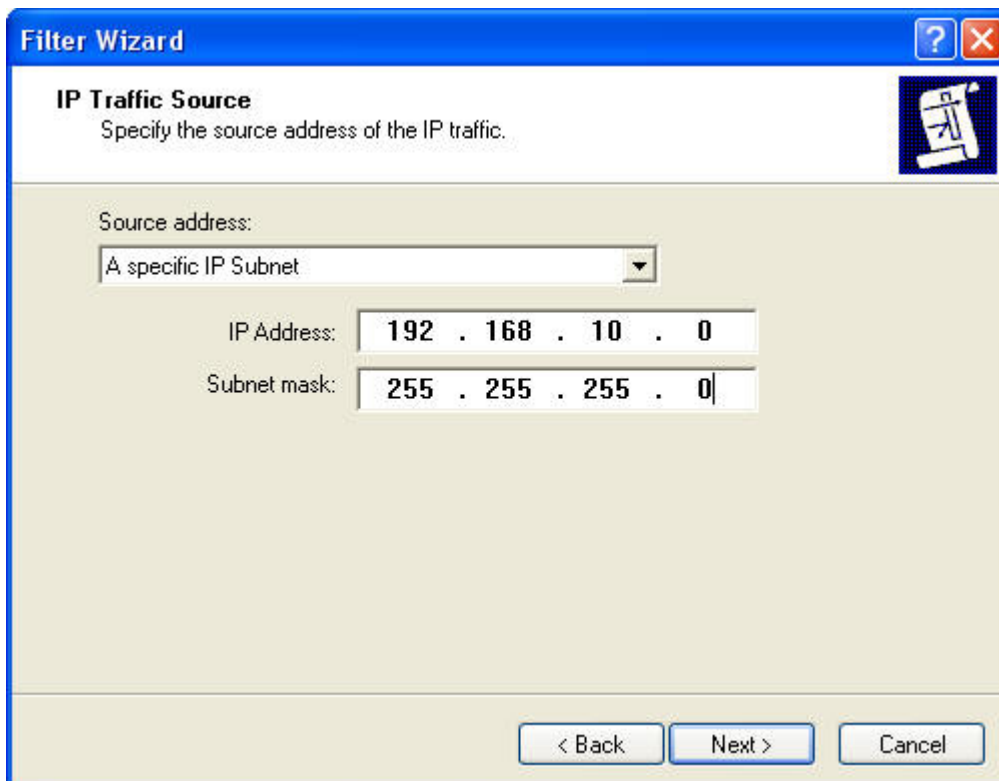
Step 18. Enter the name of IP filter and click "Add..".



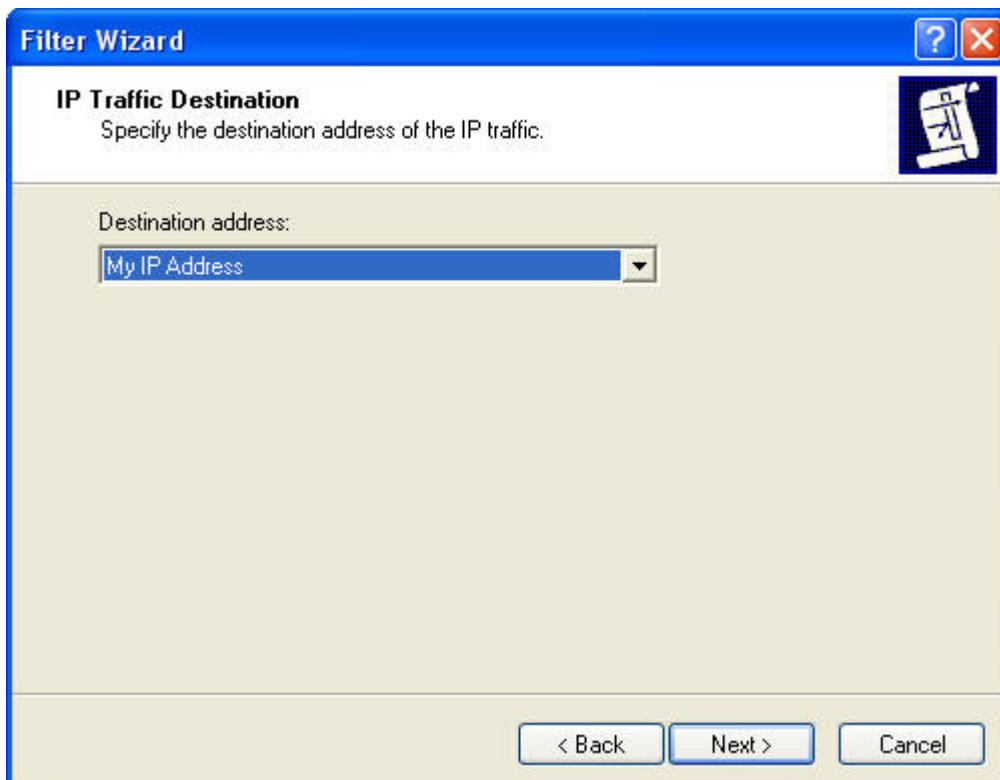
Step 19. Click next.



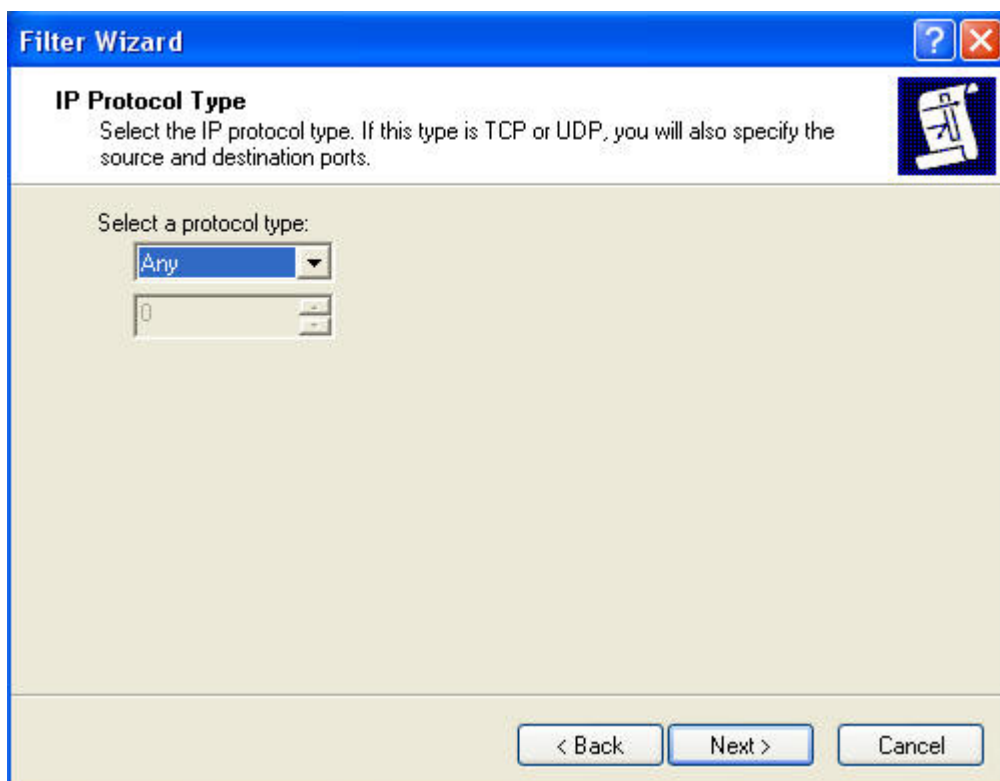
Step 20. In Source address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.



Step 21. In Destination address, click down the arrow to select the My IP Address.



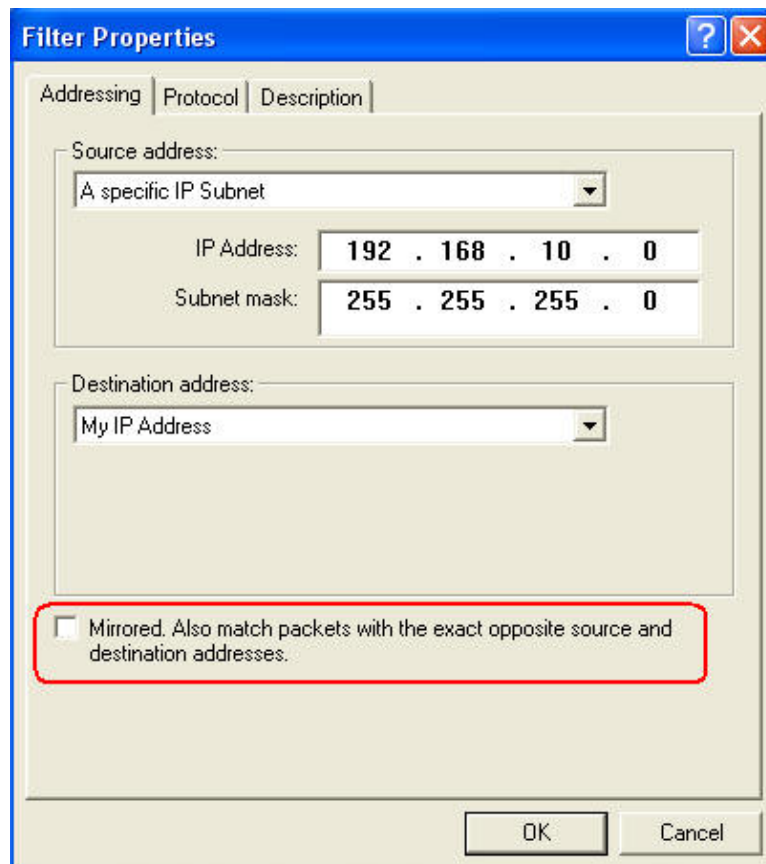
Step 22. Click next.



Step 23. Please enable edit properties, and click finish.



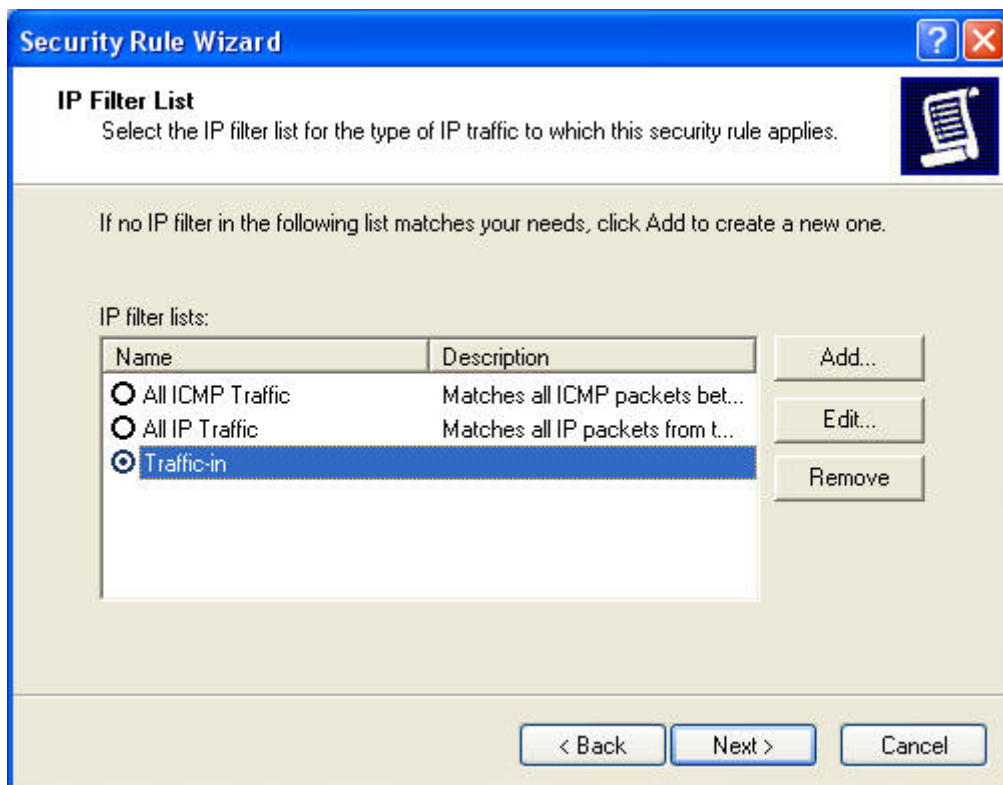
Step 24. Please don't enable Mirrored, and click OK.



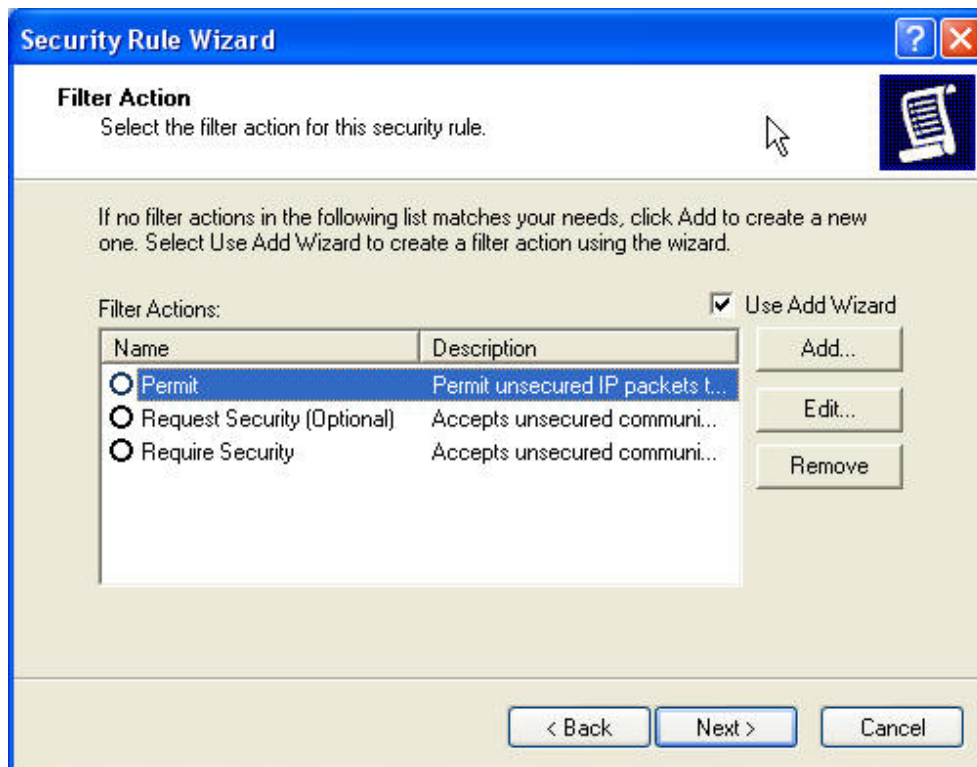
Step 25. Click OK.



Step 26. Select Traffic-in and click next.



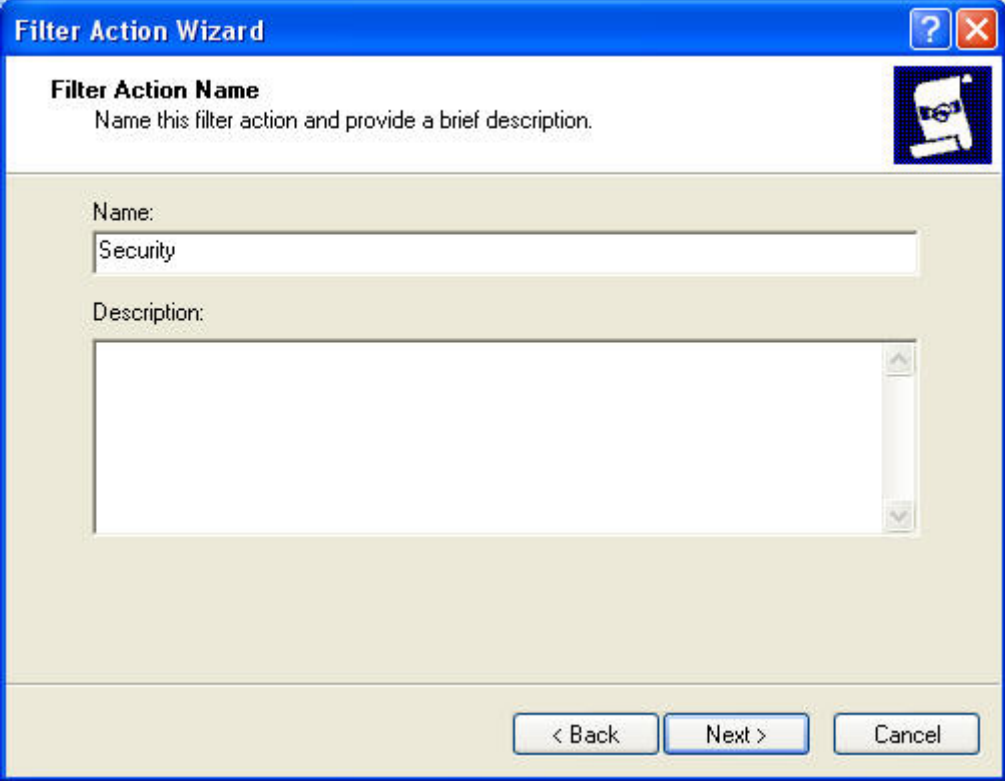
Step 27. Enable User Add Wizard and click add.



Step 28. Click next.

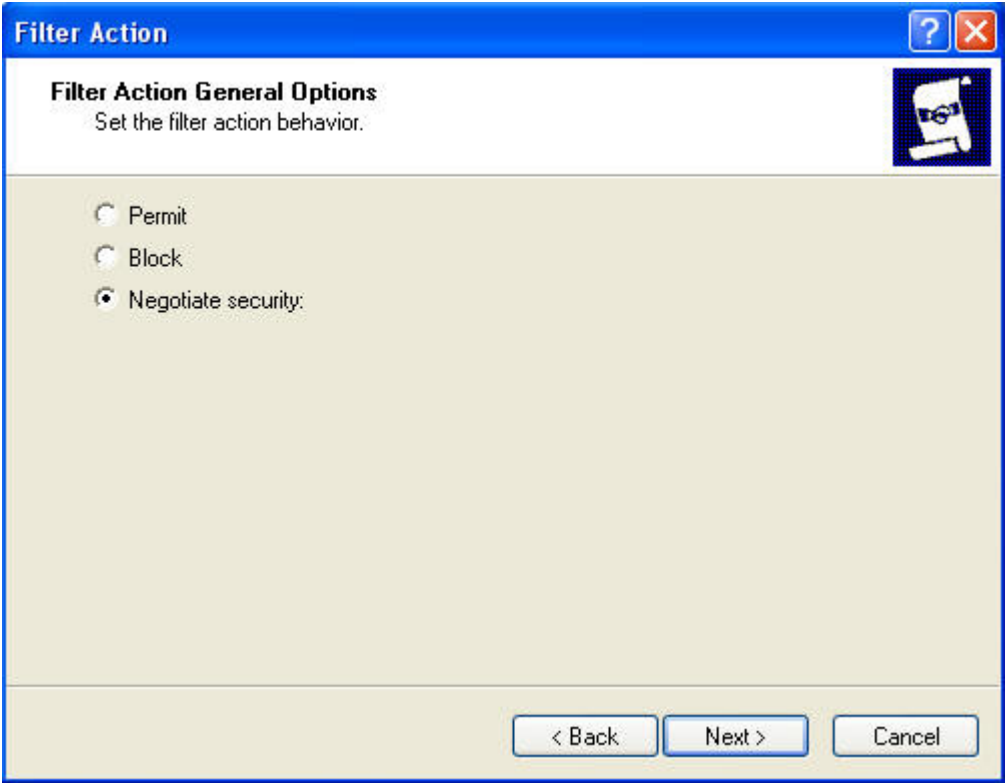


Step 29. Enter the name of filter action and click next.



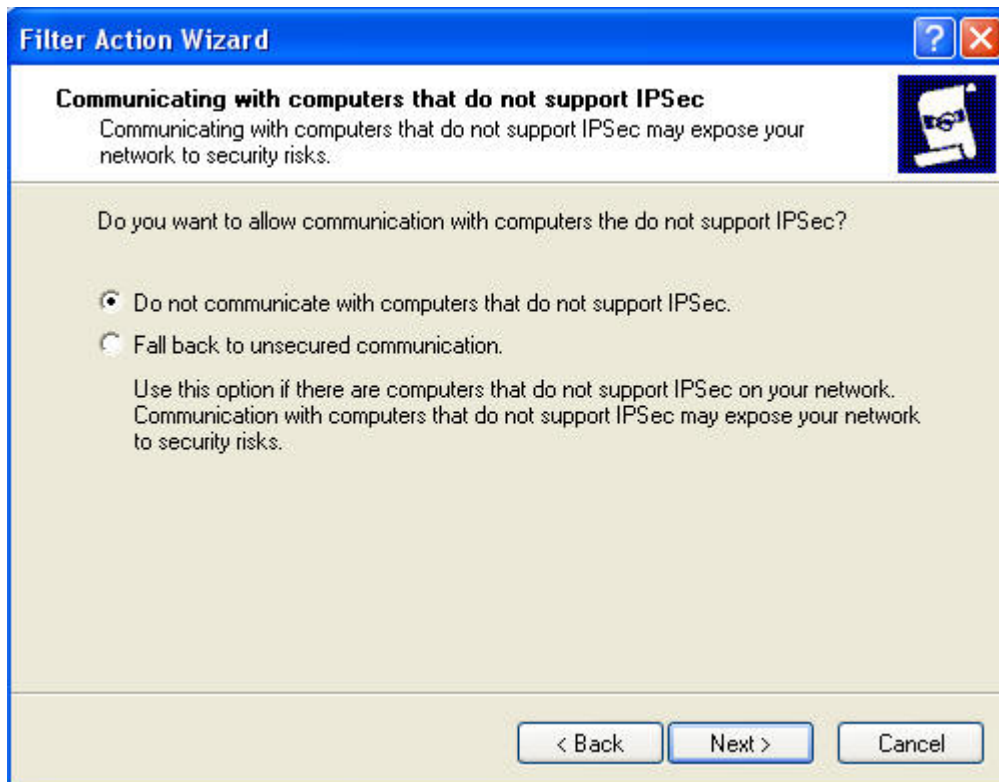
The **Filter Action Wizard** dialog box is shown. It has a blue title bar with a question mark icon and a close button. The main area is titled **Filter Action Name** and contains the instruction "Name this filter action and provide a brief description." Below this, there is a text box labeled "Name:" containing the word "Security". Below that is a larger text box labeled "Description:". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Step 30. Select Negotiate security and click next.

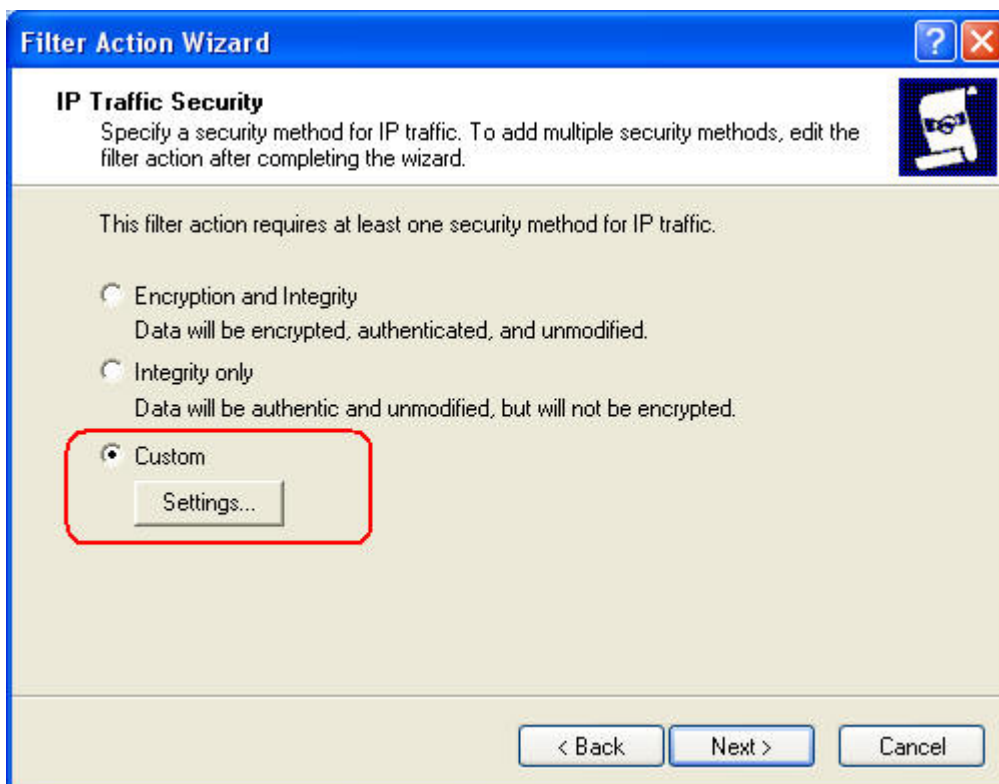


The **Filter Action** dialog box is shown. It has a blue title bar with a question mark icon and a close button. The main area is titled **Filter Action General Options** and contains the instruction "Set the filter action behavior." Below this, there are three radio button options: "Permit", "Block", and "Negotiate security:". The "Negotiate security:" option is selected. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

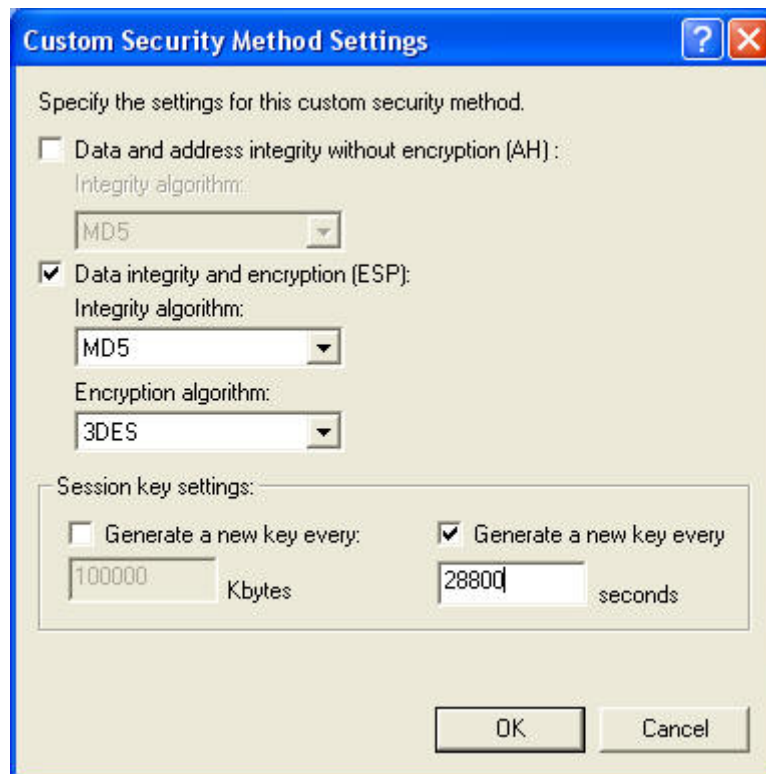
Step 31. Click next.



Step 32. Select Custom and click settings.



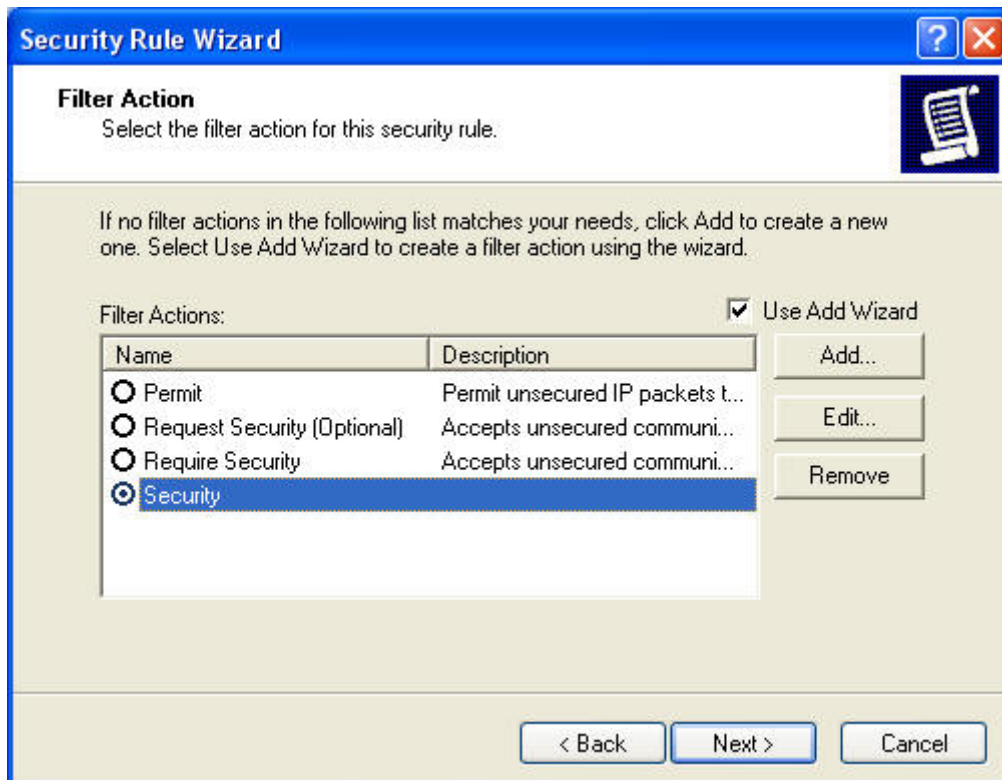
Step 33. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



Step 34. Click finish.



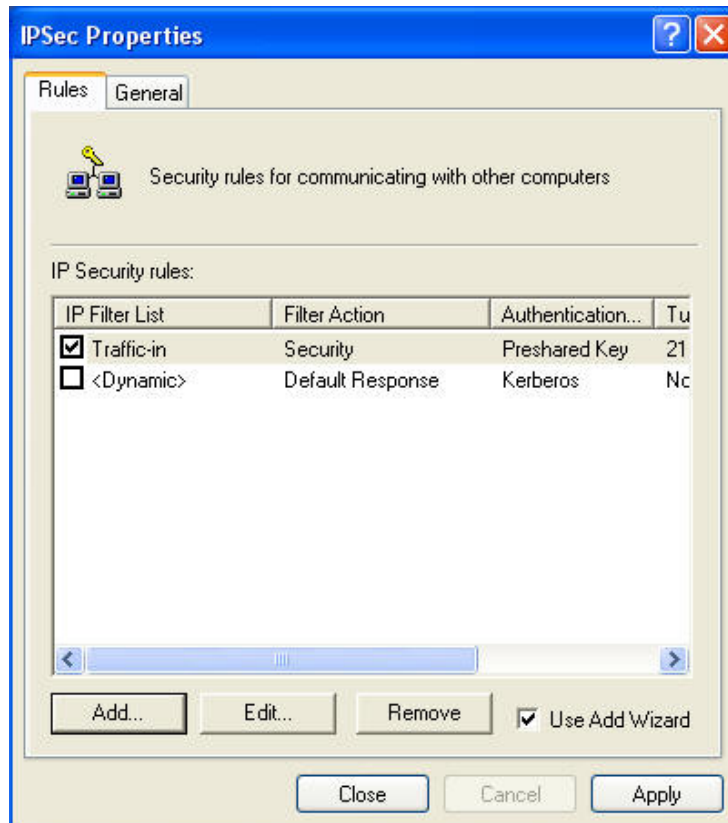
Step 35. Select security and click next.



Step 36. Click finish.



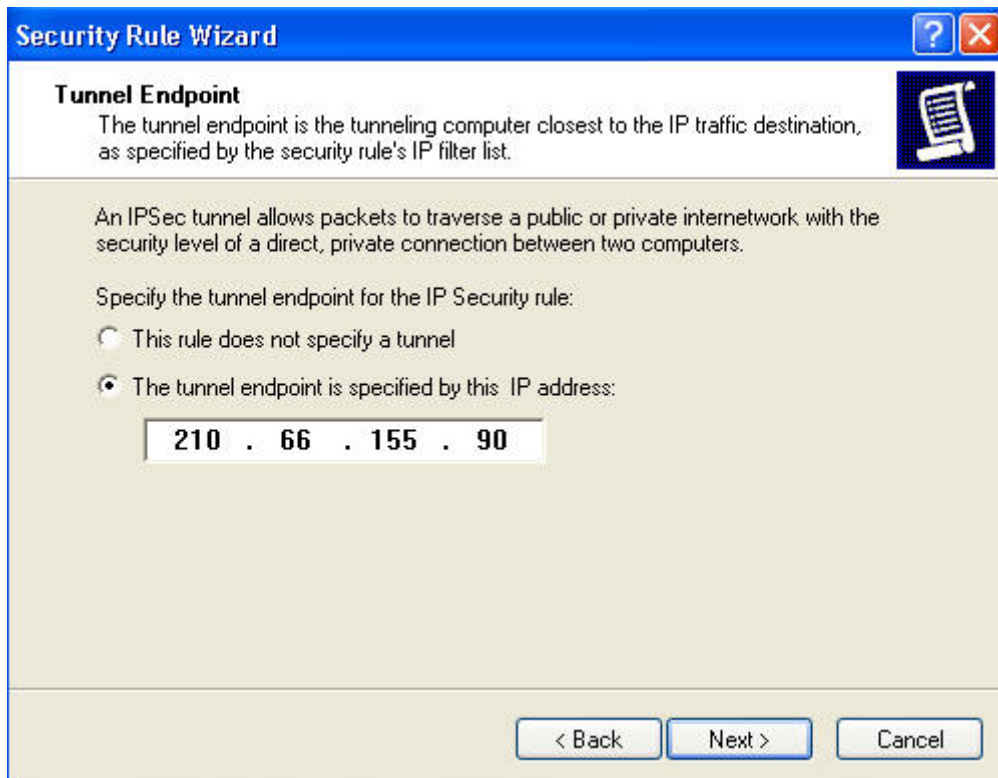
Step 37. Click Add.



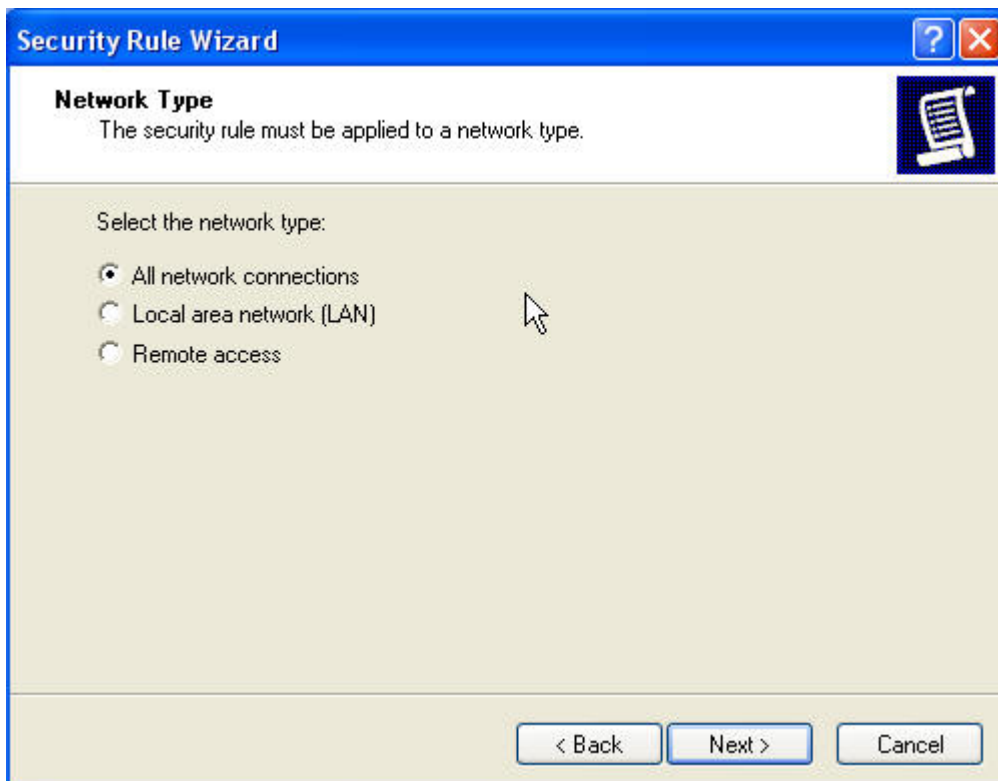
Step 38. Click next.



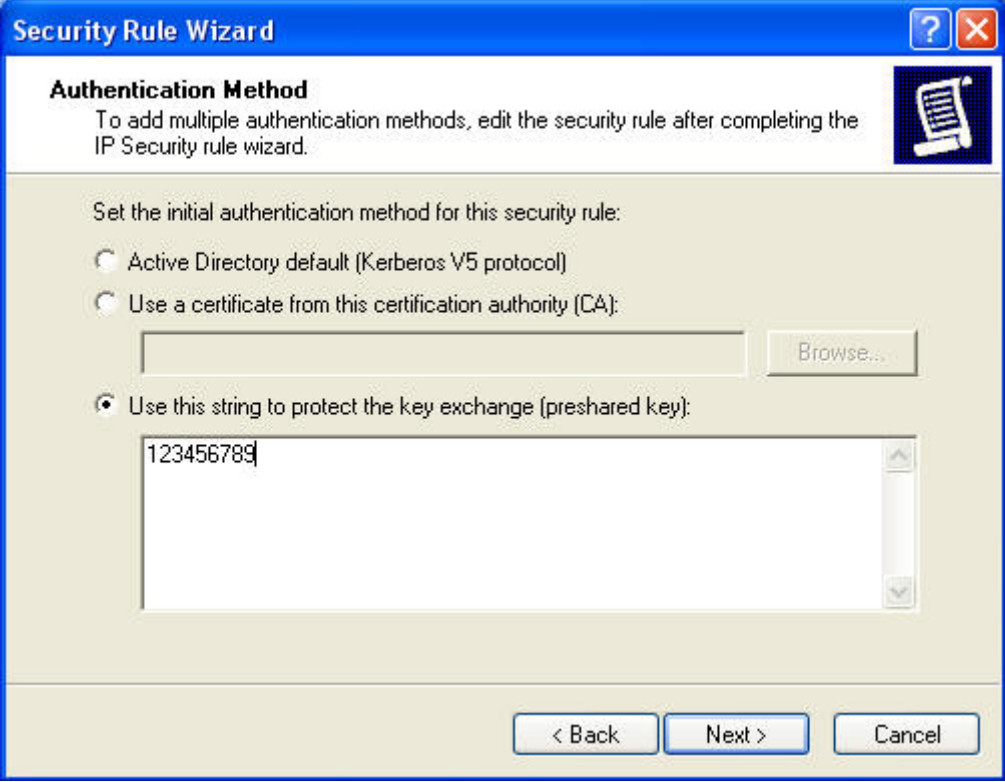
Step 39. Enter the WAN IP of company A, 210.66.155.90.



Step 40. Select All network connections and click next.



Step 41. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.




Security Rule Wizard

Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

- ☐ Active Directory default (Kerberos V5 protocol)
- ☐ Use a certificate from this certification authority (CA):
- ☒ Use this string to protect the key exchange (preshared key):

Step 42. Click Add.



Security Rule Wizard

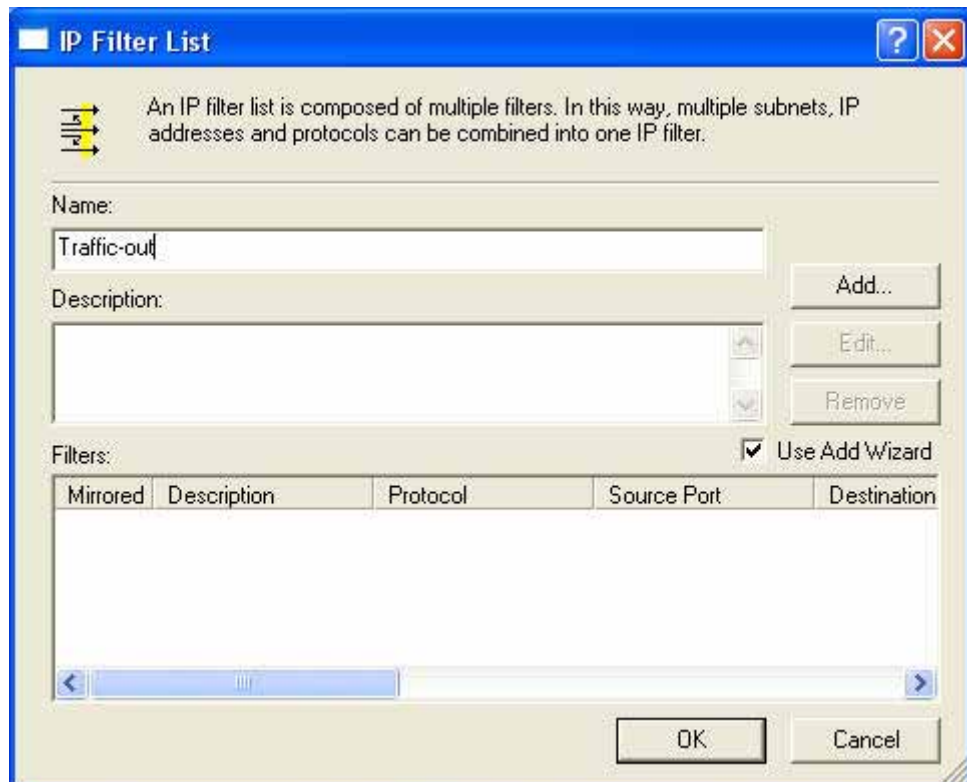
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
<input checked="" type="radio"/> All ICMP Traffic	Matches all ICMP packets bet...
<input type="radio"/> All IP Traffic	Matches all IP packets from t...
<input type="radio"/> Traffic-in	

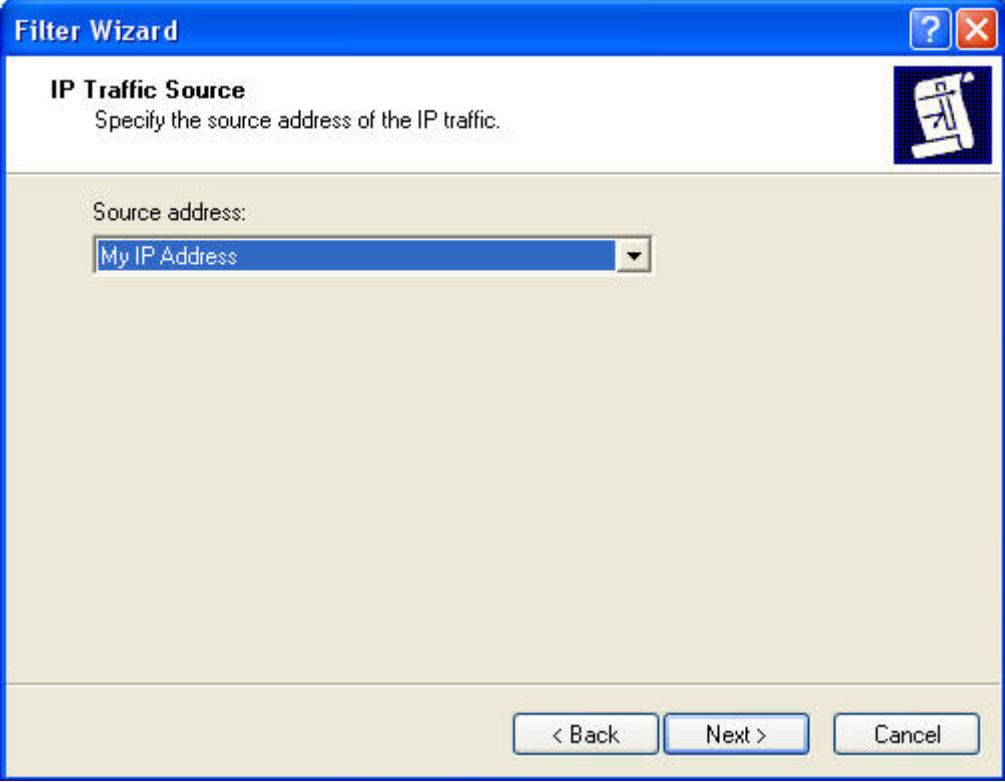
Step 43. Enter the name of IP filter and click "Add..."



Step 44. Click next



Step 45. In Source address, click down the arrow to select the My IP Address.



The image shows a Windows-style dialog box titled "Filter Wizard". It has a blue title bar with a question mark icon and a close button. The main area is titled "IP Traffic Source" and contains the instruction "Specify the source address of the IP traffic." Below this, there is a label "Source address:" followed by a dropdown menu. The dropdown menu is open, showing "My IP Address" as the selected option. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

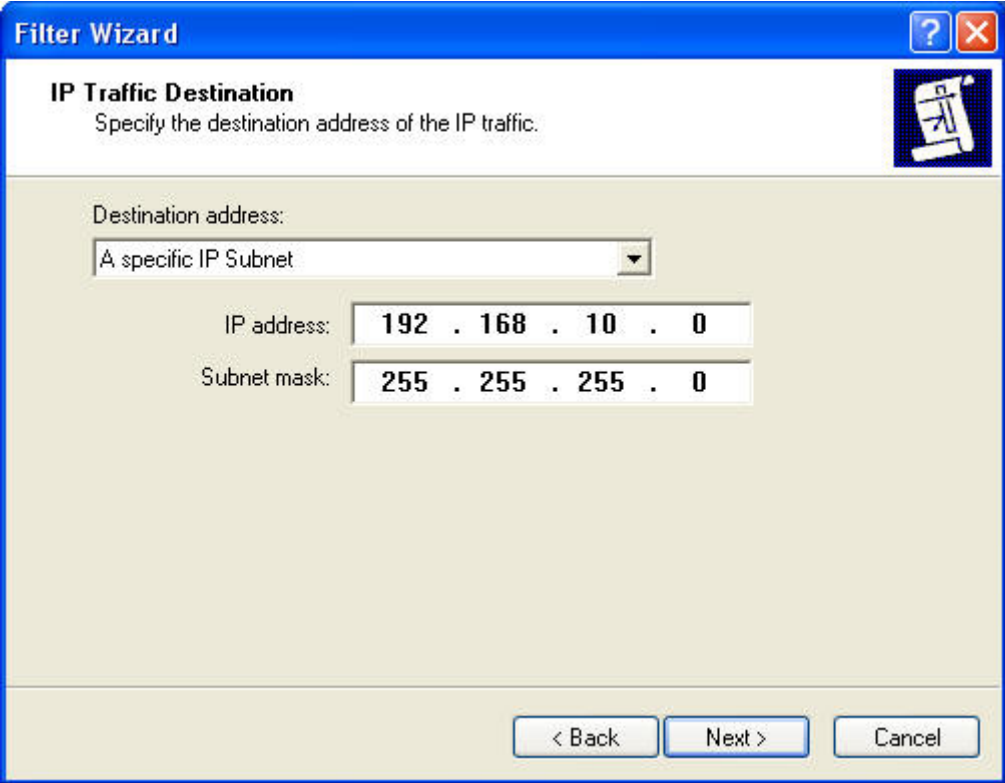
Filter Wizard

IP Traffic Source
Specify the source address of the IP traffic.

Source address:
My IP Address

< Back Next > Cancel

Step 46. In Destination address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.



The image shows a Windows-style dialog box titled "Filter Wizard". It has a blue title bar with a question mark icon and a close button. The main area is titled "IP Traffic Destination" and contains the instruction "Specify the destination address of the IP traffic." Below this, there is a label "Destination address:" followed by a dropdown menu. The dropdown menu is open, showing "A specific IP Subnet" as the selected option. Below the dropdown, there are two rows of input fields. The first row is labeled "IP address:" and contains the value "192 . 168 . 10 . 0". The second row is labeled "Subnet mask:" and contains the value "255 . 255 . 255 . 0". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Filter Wizard

IP Traffic Destination
Specify the destination address of the IP traffic.

Destination address:
A specific IP Subnet

IP address: 192 . 168 . 10 . 0
Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

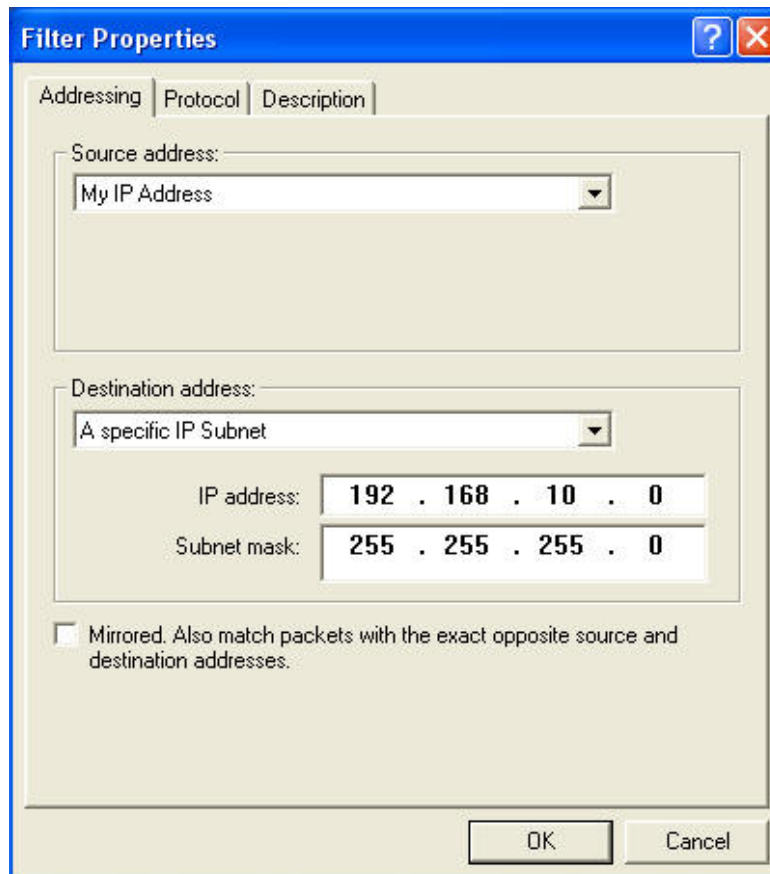
Step 47. Click next.



Step 48. Please enable Edit properties and click finish.

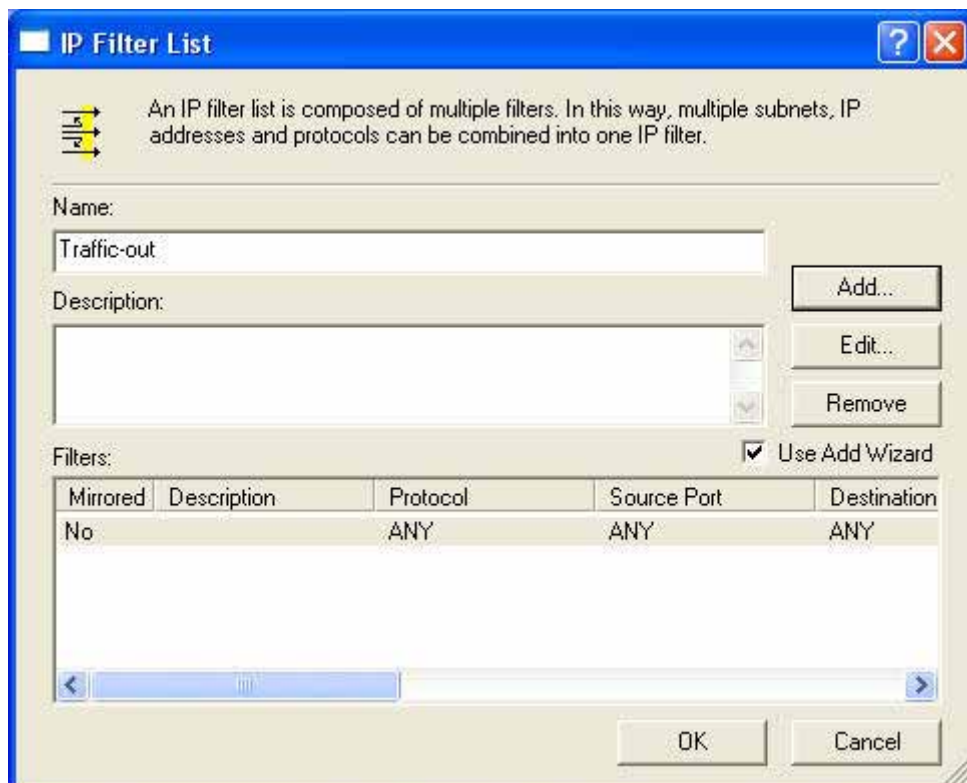


Step 49. Please don't enable Mirrored and click ok.



The **Filter Properties** dialog box has three tabs: **Addressing**, **Protocol**, and **Description**. The **Addressing** tab is active. It contains two dropdown menus: **Source address:** with the value **My IP Address**, and **Destination address:** with the value **A specific IP Subnet**. Below these are two rows of IP address fields. The **IP address:** row contains the values **192 . 168 . 10 . 0**. The **Subnet mask:** row contains the values **255 . 255 . 255 . 0**. At the bottom, there is a checkbox labeled **Mirrored. Also match packets with the exact opposite source and destination addresses.** which is currently unchecked. **OK** and **Cancel** buttons are at the bottom right.

Step 50. Click ok.



The **IP Filter List** dialog box contains an icon of a list with arrows and a text box explaining: "An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter." Below this is a **Name:** text box containing **Traffic-out** and a **Description:** text box. To the right of the description box are three buttons: **Add...**, **Edit...**, and **Remove**. Below these is a **Filters:** section with a checkbox **Use Add Wizard** which is checked. It contains a table with the following data:

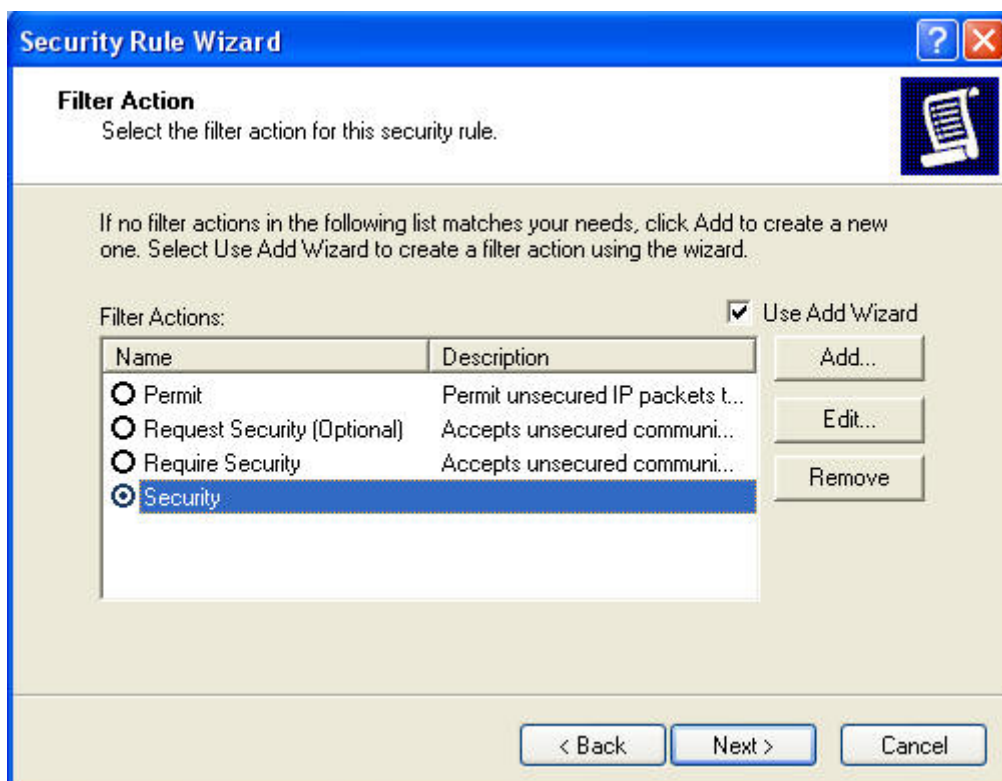
Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

At the bottom are **OK** and **Cancel** buttons.

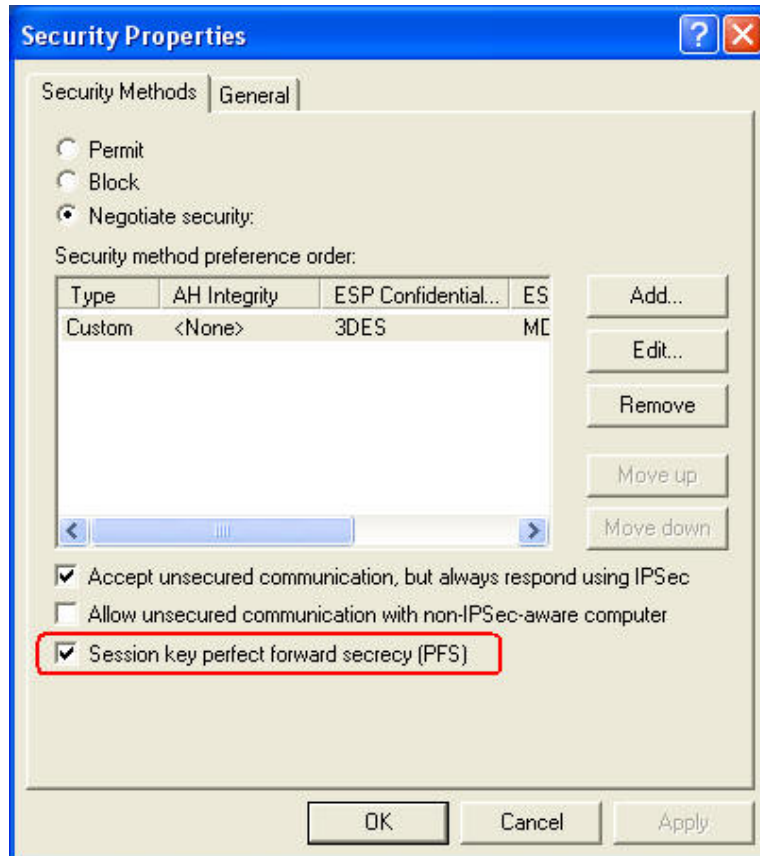
Step 51. Select Traffic-out and click next.



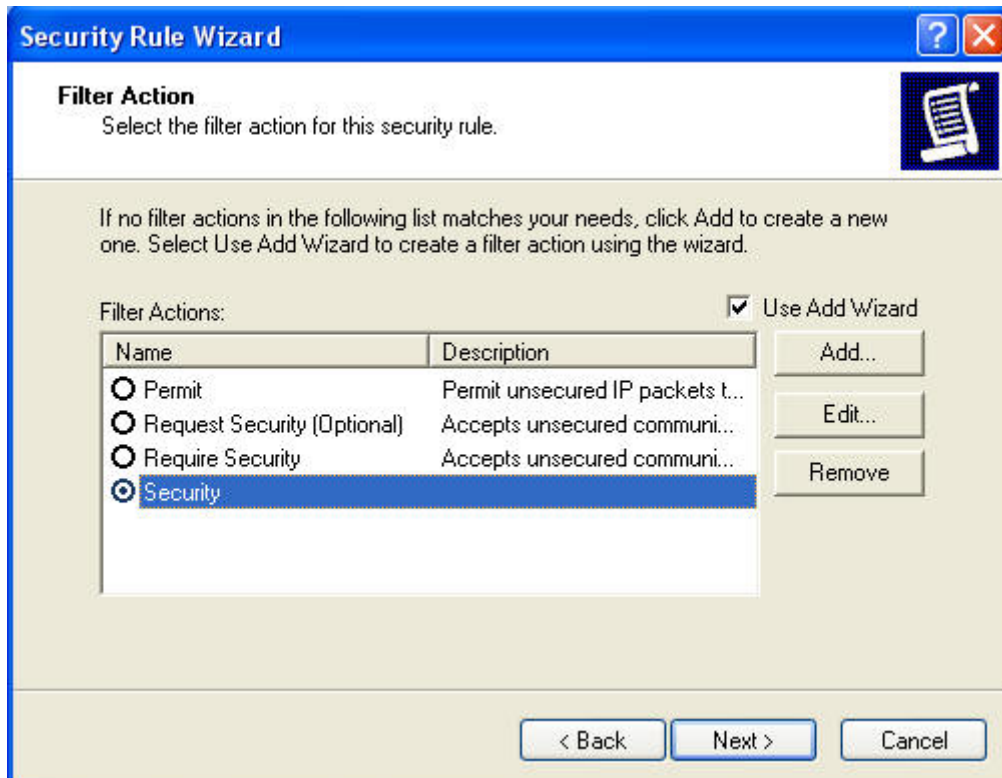
Step 52. Select Security and click edit.



Step 53. Enable Session key perfect forward secrecy (PFS) and click ok.



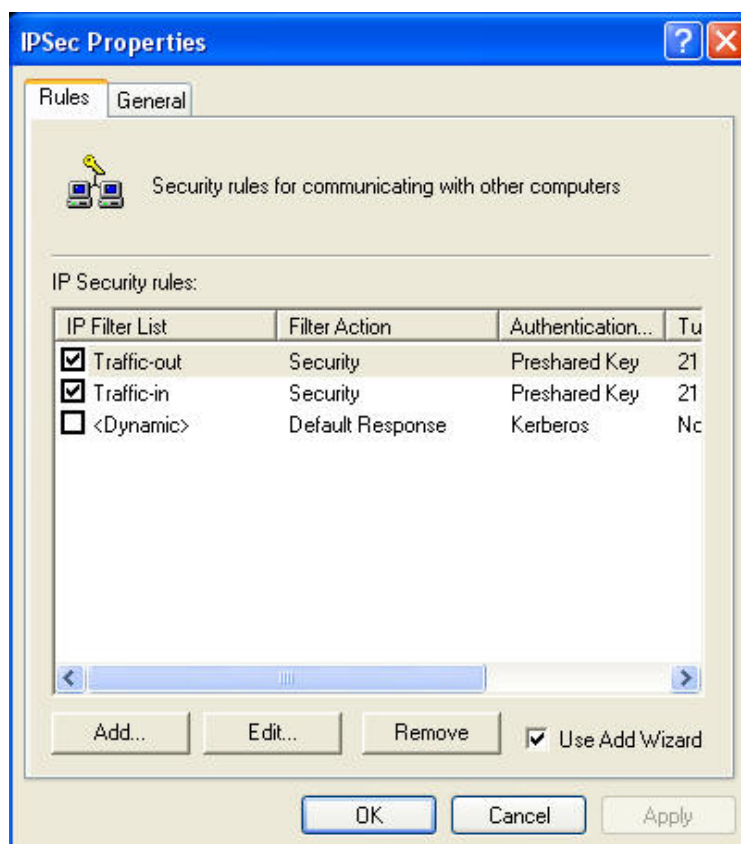
Step 54. Select Security and click next.



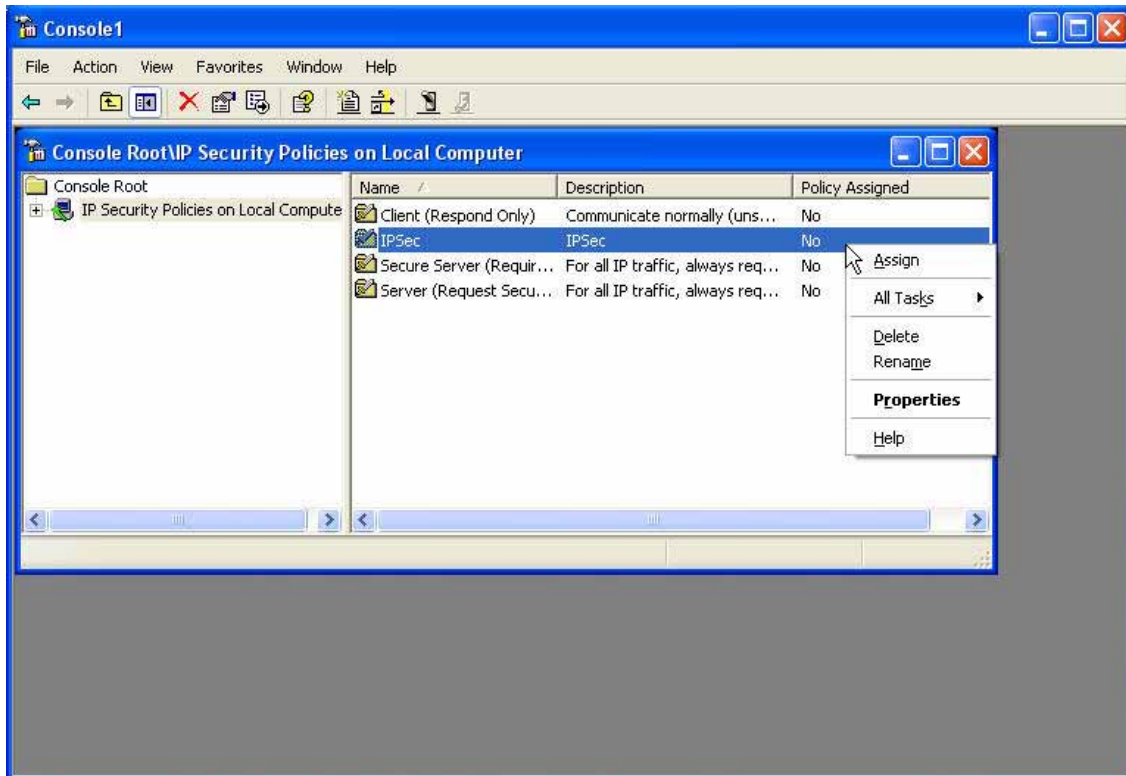
Step 55. Please don't enable Edit properties and click finish.



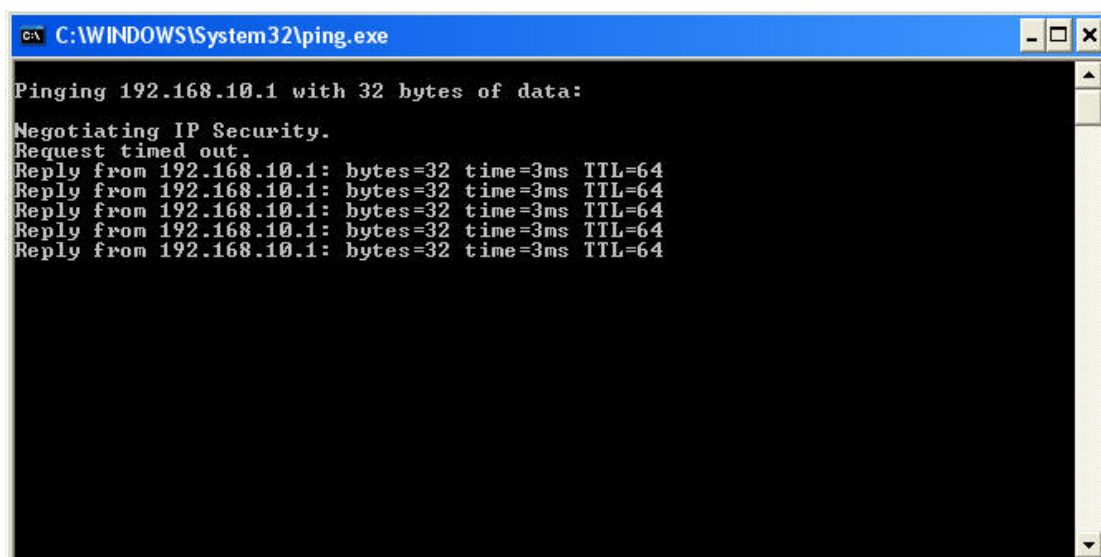
Step 56. Click apply first and then click ok.



Step 57 Click the right button of mouse in IPSec choose Assign option.



Step 58. Ping the remote gateway of Company A, the VPN tunnel is created successfully.



Example 3. Create a VPN connection between two Multi-Homing Security Gateways using Aggressive mode Algorithm (3DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Preparation Task:

Company A External IP is 61.11.11.11

Internal IP is 192.168.10.X

Company B External IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPsec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item	
Name	VPN_A
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Multi-Homing Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	@123
Peer ID	@abc

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Click OK to finish the setting of Company A.

Policy Object > VPN > IPSec Autokey					
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	Modify Remove

Step 9. Click Trunk and press New Entry to configure the further setting.

Step 10. Enter Site_A as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	Site_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 11. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.

To Destination

☒ To Destination Subnet / Mask 192.168.20.0 / 255.255.255.0

☐ Remote Client

Step 12. In Tunnel, select VPN_A tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel

< --- Available Tunnel --->

VPN_A

Remove

Add >>

< --- Selected Tunnel --->

Step 13. Click OK to finish the Trunk setting of Company A.

Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	Site_A	192.168.10.0	192.168.20.0	VPN_A	<div>Modify</div> <div>Remove</div> <div>Pause</div>

Step 14. If you want to configure bi-direction VPN connection, you should enable Trunk setting in Outgoing and Incoming Policy.

Policy > Outgoing

Comment :

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	Site_A
Action, WAN Port	<div>None</div> <div>Site_A</div>
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Outgoing Policy:

Policy > Outgoing											
Source	Destination	Service	Action	Option					Configure		
Inside_Any	Outside_Any	ANY	VPN						Modify	Remove	Pause
Inside_Any	Outside_Any	ANY	✓						Modify	Remove	Pause

Incoming Policy:

Policy > Incoming											
Source	Destination	Service	Action	Option					Configure		
Outside_Any	Inside_Any(Routing)	ANY	VPN						Modify	Remove	Pause

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's Multi-Homing Security Gateway, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_B in IPsec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item	
Name	VPN_B
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Multi-Homing Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼
Mode	
	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	@abc
Peer ID	@123

Step 6. In IPsec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 1 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPsec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 1 ▼
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Click OK to finish the setting of Company B.

Policy Object > VPN > IPsec Autokey					
i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	Modify Remove

Step 9. Click Trunk and press New Entry to configure the further setting.

Step 10. Enter Site_B as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	Site_B
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0

Step 11. In To Destination table, fill company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
<input type="radio"/> Remote Client	

Step 12. In Tunnel, select VPN_B tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel		
<div style="border: 1px solid black; padding: 5px;"> <div style="text-align: center; border-bottom: 1px solid black;">< --- Available Tunnel ---></div> <div>VPN_B</div> </div>	<div style="border: 1px solid black; padding: 5px; margin: 5px;"> <div style="text-align: center; border-bottom: 1px solid black;">< --- Selected Tunnel ---></div> <div>VPN_B</div> </div>	
<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 5px; background-color: #4f81bd; color: white;">Remove</div> <div style="border: 1px solid black; padding: 5px; background-color: #4f81bd; color: white;">Add >></div> </div>		

Step 13. Click OK to finish the Trunk setting of Company B.

Policy Object > VPN > Trunk					
i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	Site_A	192.168.10.0	192.168.20.0	VPN_A	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid black; padding: 2px; background-color: #c6e0b4;">Modify</div> <div style="border: 1px solid black; padding: 2px; background-color: #ffcc00;">Remove</div> <div style="border: 1px solid black; padding: 2px; background-color: #6699ff;">Pause</div> </div>

Step 14. If you want to configure bi-direction VPN connection, you should enable Trunk setting in Outgoing and Incoming Policy.

Outgoing Policy:

Policy > Outgoing

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

Incoming Policy:

Policy > Incoming							
Source	Destination	Service	Action	Option			Configure
Outside_Any	Inside_Any(Routing)	ANY	VPN				<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
							Move To <input type="button" value="1"/>

Example 4. Create a VPN trunk connection between CS-1000 (Company A) and CS-1000 (Company B), using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

Preparation Task:

Company A's External WAN 1 IP is 61.11.11.11

WAN 2 IP is 61.22.22.22

Internal IP is 192.168.10.X

Company B's External WAN 1 IP is 211.11.11.11

WAN 2 IP is 211.22.22.22

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN trunk connection with company B, 192.168.20.100 for downloading the sharing file by GRE/ IPSec Algorithm.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's CS-1000, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, Site_A_1 in IPSec Autokey window, select WAN 1 as the interface to create the first VPN connection.

Necessary Item	
Name	<input type="text" value="Site_A_1"/>
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain name, enter the Company B's WAN 1 IP address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="211.11.11.11"/>
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table, enter the Preshared Key.

Authentication Method	Preshare ▼
Preshared Key	123456789

Step 5. In Encapsulation / ISAKMP Algorithm, choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

Step 6. In IPsec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose Perfect Forward Secrecy as GROUP 2, and enter 3600 seconds in ISAKMP Lifetime, 28800 seconds in IPsec Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 2 ▼
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Choose GRE/ IPsec and enter GRE Local IP, 10.0.0.1 and GRE Remote IP, 10.0.0.254.

NOTE: The Local IP and Remote IP should be in the same IP subnet, and they also can not be the same IP subnet with both devices' WAN or LAN IP subnet

GRE/IPSec	
GRE Local IP	10.0.0.1
GRE Remote IP	10.0.0.254

Step 9. Click OK to finish the WAN 1 setting of Company A.

Policy Object > VPN > IPSec Autokey					
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	Site_A_1	WAN1	211.11.11.11	3DES / MD5	Modify Remove

Step 10. Follow the previous steps to create WAN 2 VPN rule.

Step 11. Enter the VPN name, Site_A_2 in IPSec Autokey window, select WAN 2 as the interface to create the first VPN connection.

Necessary Item	
Name	Site_A_2
WAN interface	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2

Step 12. In To Destination table, choose Remote Gateway-Fixed IP or Domain name, enter the Company B's WAN 2 IP address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 13. In Authentication Method Table, enter the Preshared Key. If the value is different with Site_A_1 that will be better.

Authentication Method	Preshare ▼
Preshared Key	987654321

Step 14. Follow Step 5, 6, 7 to configure related encryption and authentication setting.

Step 15. Choose GRE/ IPSec and enter GRE Local IP, 10.1.1.1 and GRE Remote IP, 10.1.1.254.

NOTE: The Local IP and Remote IP should be in the same IP subnet, and they also can not be the same IP subnet with both devices' WAN, LAN and Site_A_1 GRE setting's IP subnet.

GRE/IPSec	
GRE Local IP	10.1.1.1
GRE Remote IP	10.1.1.254

Step 16. Click OK to finish the WAN 2 setting of Company A.

Policy Object > VPN > IPSec Autokey					
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	Site_A_1	WAN1	211.11.11.11	3DES / MD5	Modify Remove
--	Site_A_2	WAN2	211.22.22.22	3DES / MD5	Modify Remove

Step 17. Click Trunk and press New Entry to configure the further setting.

Step 18. Enter VPN_Trunk_A as the new trunk name, and select LAN interface as the VPN source. Fill LAN

IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

Modify VPN_Trunk_B Trunk	
Name	VPN_Trunk_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0


Step 19. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.

To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Client	

Step 20. Select Site_A_1 and Site_A_2 in **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel	
<div style="border: 1px solid black; padding: 5px;"> < --- Available Tunnel ---> Site_A_1 Site_A_2 </div>	<div style="text-align: center;"> <div style="background-color: #0070C0; color: white; padding: 5px; margin: 5px; display: inline-block;"> << Remove </div> <div style="background-color: #0070C0; color: white; padding: 5px; margin: 5px; display: inline-block;"> Add >> </div> </div>
	<div style="border: 1px solid black; padding: 5px; height: 100px;"> < --- Selected Tunnel ---> </div>

Step 21. Click OK to finish the Trunk setting of Company A.

Policy Object > VPN > Trunk					
i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	VPN_Trunk_A	192.168.10.0	192.168.20.0	Site_A_1 ...	<div style="text-align: center;"> <div style="background-color: #0070C0; color: white; padding: 2px 5px; margin: 2px;">Modify</div> <div style="background-color: #FFD700; color: black; padding: 2px 5px; margin: 2px;">Remove</div> <div style="background-color: #0000FF; color: white; padding: 2px 5px; margin: 2px;">Pause</div> </div>

Step 22. Enable Trunk setting in Outgoing and Incoming Policy.

Outgoing Policy:

Policy > Outgoing										
Source	Destination	Service	Action	Option				Configure		
Inside_Any	Outside_Any	ANY	VPN					Modify	Remove	Pause
Inside_Any	Outside_Any	ANY	✓					Modify	Remove	Pause

Incoming Policy:

Policy > Incoming							
Source	Destination	Service	Action	Option			Configure
Outside_Any	Inside_Any(Routing)	ANY	VPN				<div>Modify</div> <div>Remove</div> <div>Pause</div>
							Move To 1 ▾

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP 192.168.20.1 of Company B's CS-1000. Click VPN in the menu bar on the left hand side, and then select the sub-select IPsec Autokey. Click Add.

Step 2. Enter the VPN name, Site_B_1 in IPsec Autokey window, select WAN 1 as the interface to create the first VPN connection.

Necessary Item	
Name	Site_B_1
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain name, enter the Company A's WAN 1 IP address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	61.11.11.11
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key.

Authentication Method	Preshare ▾
Preshared Key	123456789

Step 5. In Encapsulation -> ISAKMP Algorithm, choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

Step 6. In IPsec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose Perfect Forward Secrecy as GROUP 2, and enter 3600 seconds in ISAKMP Lifetime, 28800 seconds in IPSec Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Choose GRE/ IPSec and enter GRE Local IP, 10.0.0.254 and GRE Remote IP, 10.0.0.1.

NOTE: The Local IP and Remote IP should be in the same IP subnet, and they also can not be the same IP subnet with both devices' WAN or LAN IP subnet

GRE/IPSec	
GRE Local IP	10.0.0.254
GRE Remote IP	10.0.0.1

Step 10. Click OK to finish the WAN 1 VPN setting of Company B.

Policy Object > VPN > IPSec Autokey					
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	Site_B_1	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Step 11. Follow the previous steps to create WAN 2 VPN rule.

Step 12. Enter the VPN name, Site_B_2 in IPSec Autokey window, select WAN 2 as the interface to create the first VPN connection.

Necessary Item	
Name	Site_B_2
WAN interface	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2

Step 13. In To Destination table, choose Remote Gateway-Fixed IP or Domain name, enter the Company A's WAN 2 IP address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	61.22.22.22
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 14. In Authentication Method Table, choose Preshare and enter the Preshared Key.

Authentication Method	Preshare ▼
Preshared Key	987654321

Step 15. Follow Step 5, 6, 7 to configure related encryption and authentication setting.

Step 16. Choose GRE/ IPSec and enter GRE Local IP, 10.1.1.254 and GRE Remote IP, 10.1.1.1.

NOTE: The Local IP and Remote IP should be in the same IP subnet, and they also can not be the same IP subnet with both devices' WAN or LAN IP subnet

GRE/IPSec	
GRE Local IP	10.1.1.254
GRE Remote IP	10.1.1.1

Step 17. Click OK to finish the WAN 2 VPN setting of Company B.

Policy Object > VPN > IPSec Autokey					
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	Site_B_1	WAN1	61.11.11.11	3DES / MD5	Modify Remove
--	Site_B_2	WAN2	61.22.22.22	3DES / MD5	Modify Remove

Step 17. Click Trunk and press New Entry to configure the further setting.

Step 18. Enter VPN_Trunk_B as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	VPN_Trunk_B
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0

Step 19. In To Destination table, fill company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 20. Select Site_B_1 and Site_B_2 in **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel

< --- Available Tunnel --->

Site_B_1
Site_B_2

Remove
Add

< --- Selected Tunnel --->

Step 21. Click OK to finish the Trunk setting of Company B.

Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	VPN_Trunk_B	192.168.20.0	192.168.10.0	Site_B_1...	Modify Remove Pause

Step 22. Enable Trunk setting in Outgoing and Incoming Policy.

Outgoing Policy:

Policy > Outgoing

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

Incoming Policy:

Policy > Incoming

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

Example 5. Create a VPN connection between Multi-Homing Security Gateway and PLANET VRT-311 VPN Router.

Preparation Task:

Company A External IP is 210.66.155.90

Internal IP is 192.168.10.X

Company B External IP is 210.66.155.92

Internal IP is 192.168.20.X

To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's Multi-Homing Security Gateway, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and select the WAN interface you want to create the VPN tunnel.

Necessary Item	
Name	CS
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

Step 3. In To Destination table, choose Remote Gateway-Fixed IP or Domain Name, enter the IP address desired to be connected.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	210.66.155.92
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

Step 4. In Authentication Method Table enters the Preshared Key.

Authentication Method	Preshare
Preshared Key	12345678

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

Step 6. In IPSec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800

seconds in IPsec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	3600 Seconds
IPsec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.

Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
------	--

Step 9. Click OK to finish the IPsec Autokey setting of Company A.

Policy Object > VPN > IPsec Autokey					
i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
--	CS	WAN1	210.66.155.92	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Step 10. Click Trunk and press New Entry to configure the further setting.

Step 11. Enter Site_A as the new trunk name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Trunk	
Name	CSVN
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0

Step 12. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0 respectively.

To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client	192.168.20.0 / 255.255.255.0

Step 13. In Tunnel, select VPN_A tunnel **Available Tunnel**, and click the **Add>>** button to add it to the **Select Tunnel**.

Tunnel	
<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px; text-align: center;">< --- Available Tunnel ---></div> <div style="background-color: #0056b3; color: white; padding: 2px;">CS</div> </div>	<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #0056b3; color: white; padding: 2px; text-align: center;">< --- Selected Tunnel ---></div> <div style="background-color: #0056b3; color: white; padding: 2px;">CS</div> </div>
<input type="button" value="Remove"/>	
<input type="button" value="Add"/>	

Step 14. Fill company B's gateway IP 192.168.20.1 in Keep alive IP to keep VPN tunnel connecting.

Keep alive IP :

Step 15. Click OK to finish the Trunk setting of Company A.





Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	CSVPN	192.168.10.0	192.168.20.0	CS	Modify Remove Pause

Step 16. If you want to configure bi-direction VPN connection, you should enable Trunk setting in Outgoing and Incoming Policy.



Outgoing Policy:

Policy > Outgoing

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

Incoming Policy:

Policy > Incoming

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

Step 2: Configure VRT-311 VPN policy as the following:

VPN Policy Definition

Name: ☒ Enable Policy
☐ Allow NetBIOS traffic

Remote VPN endpoint ☐ Dynamic IP
☒ Fixed IP:
☐ Domain Name:

Local IP addresses
 Type: IP address: ~
 Subnet Mask:

Remote IP addresses
 Type: IP address: ~
 Subnet Mask:

Authentication & Encryption
☐ AH Authentication
☒ ESP Encryption Key Size: (AES only)
☒ ESP Authentication
☐ Manual Key Exchange
☒ IKE (Internet Key Exchange)
 Direction:
 Local Identity Type:
 Local Identity Data:
 Remote Identity Type:
 Remote Identity Data:
 Authentication: ☐ RSA Signature (requires certificate)
 ☒ Pre-shared Key

 Authentication Algorithm:
 Encryption: Key Size: (AES only)
 Exchange Mode:
 IKE SA Life Time: (secs)
 ☒ IKE Keep Alive Ping IP Address:
 IPSec SA Life Time: (secs)
 DH Group:
 IKE PFS:
 IPSec PFS:

3.4 Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Multi-Homing Security Gateway.

What is Policy?

The device uses policies to filter packets. Based on source addresses, a packet can be categorized into:

- (1)Outgoing: a client is in the LAN networks while a server is in the WAN networks.
- (2) Incoming, a client is in the WAN networks, while a server is in the LAN networks.
- (3) To DMZ: a client is either in the LAN networks or in the WAN networks while, server is in DMZ.
- (4) From DMZ, a client is in DMZ while server is either in the LAN networks or in the WAN networks.

How do I use Policy?

Source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

Policy Directions:

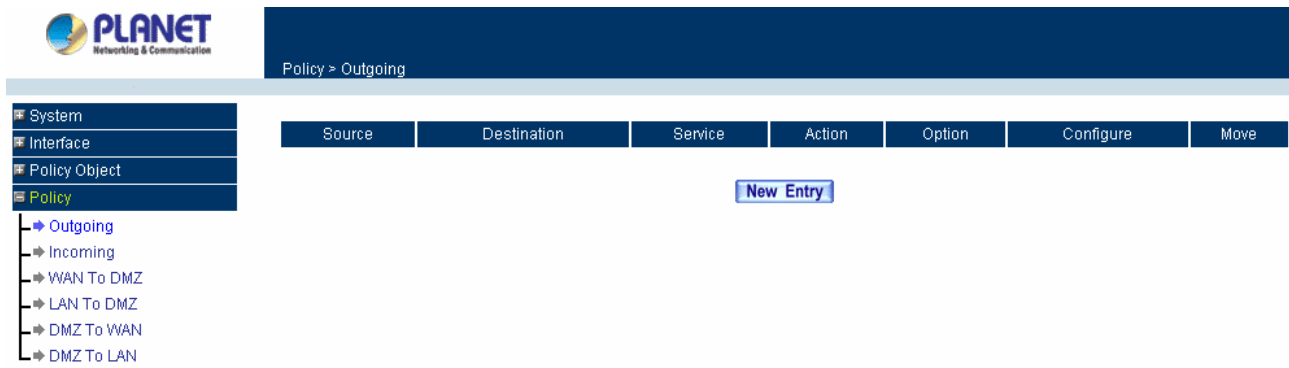
- Step 1.** In **Address**, set names and addresses of source networks and destination networks.
- Step 2.** In **Service**, set services.
- Step 3.** In **Virtual Server**, set names and addresses of mapped IP or virtual server (only applied to **Incoming policies**).
- Step 4.** Set control policies in **Policy**.

3.4.1 Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN network.

Entering the Outgoing window:

Click **Policy** on the left hand side menu bar, then click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.



The fields in the Outgoing window are:

- **Source:** Source network addresses that are specified in the LAN section of **Address** menu, or all the LAN network addresses.
- **Destination:** Destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- **Service:** Specify services provided by WAN network servers.
- **Action:** Control actions to permit or deny packets from LAN networks to WAN network travelling through the Multi-Homing Security Gateway.
- **Option:** Specify the monitoring functions on packets from LAN networks to WAN networks travelling through the Multi-Homing Security Gateway.
- **Configure:** Modify settings.
- **Move:** This sets the priority of the policies, number 1 being the highest priority.

Adding a new Outgoing Policy

Step 1: Click on the New Entry button and the Add New Policy window will appear.



Policy > Outgoing

Comment :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None

Step 2: Configure all the parameters.

Source Address: Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the **Address** window. To create a new destination address, please go to the WAN section under the **Address** menu.

Service: Specified services provided by WAN network servers. These are services/application that are allowed to pass from the LAN network to the WAN network. Choose ANY for all services.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Authentication User: Select the item listed in the Authentication User to enable the policy to automatically execute the function in a certain time and range.

Trunk: Check to allow VPN traffic passing through.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Traffic Log: Check to enable flow monitoring.

Statistics: Check to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Check to enable Content Blocking.

Max. Concurrent Sessions: The maximum concurrent sessions that allows passing through CS-1000. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a

certain time and range.

Step 3: Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

Modifying an Outgoing policy

Step 1: In the **Outgoing** policy section, locate the name of the policy desired to be modified and click its corresponding Modify option under the Configure field.

Step 2: In the **Modify Policy** window, fill in new settings.

NOTE: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→ [Pre-defined], [Custom] or Group under **Service**).

Step 3: Click **OK** to do confirm modification or click **Cancel** to cancel it.

The screenshot displays the Planet Network Management System interface. On the left is a navigation tree with categories: System, Interface, Policy Object, and Policy. Under Policy, there are sub-items: Outgoing (selected), Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, and DMZ To LAN. Below these are Mail Security, IDP, Anomaly Flow IP, and Monitor. The main area shows the 'Policy > Outgoing' configuration. At the top, there's a 'Comment' text box. Below it is the 'Modify Policy' section with various settings:

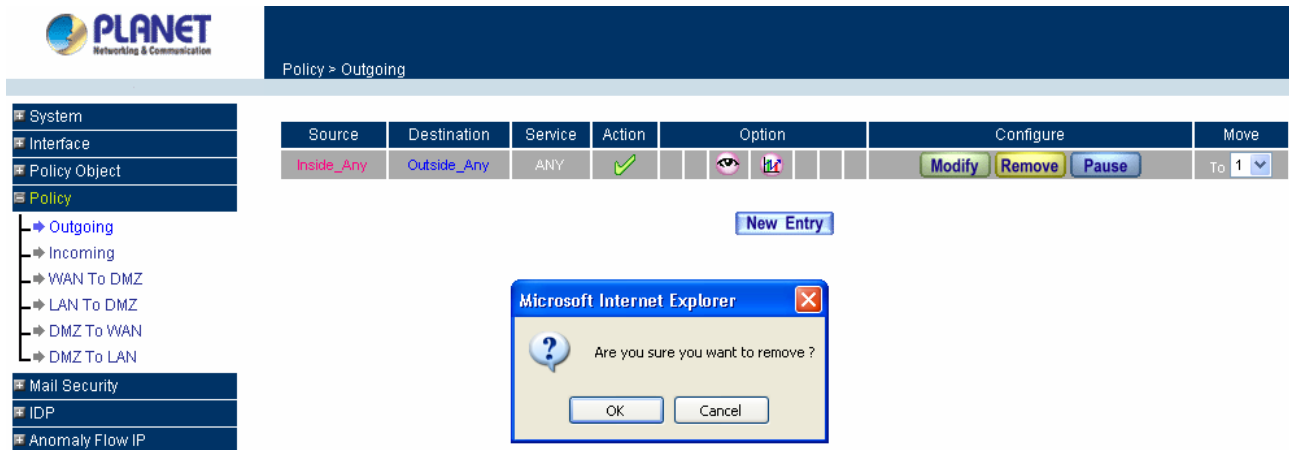
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None

At the bottom right of the window are 'OK' and 'Cancel' buttons.

Removing the Outgoing Policy

Step 1. In the **Outgoing** policy section, locate the name of the policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

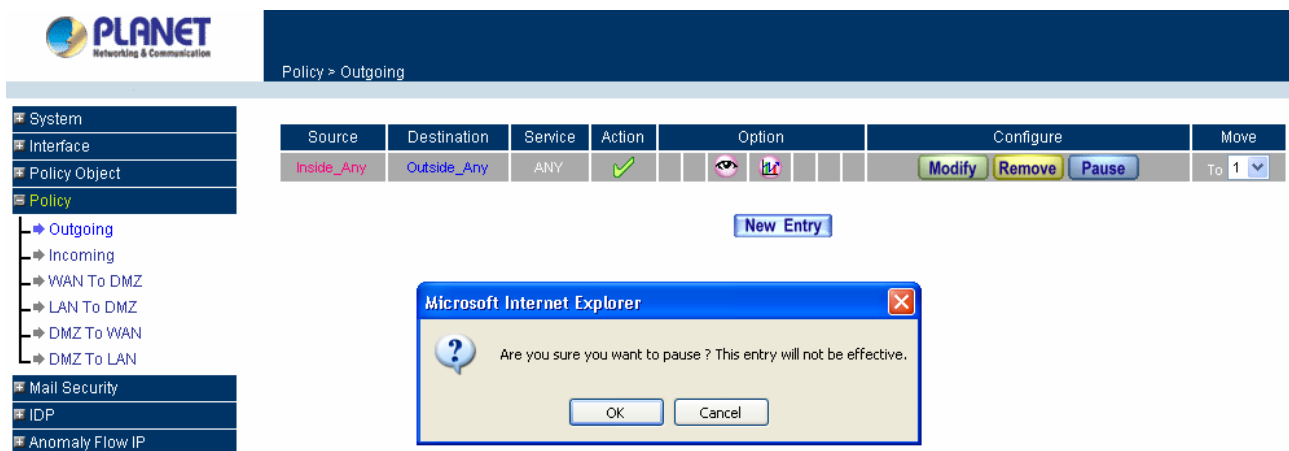
Step 2. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.



Pausing the Outgoing Policy

Step 1. In the **Outgoing** policy section, locate the name of the policy desired to be paused and click its corresponding **Pause** option in the **Configure** field.

Step 2. In the **Pause** confirmation dialogue box, click **OK** to pause the policy or click **Cancel** to cancel pausing.



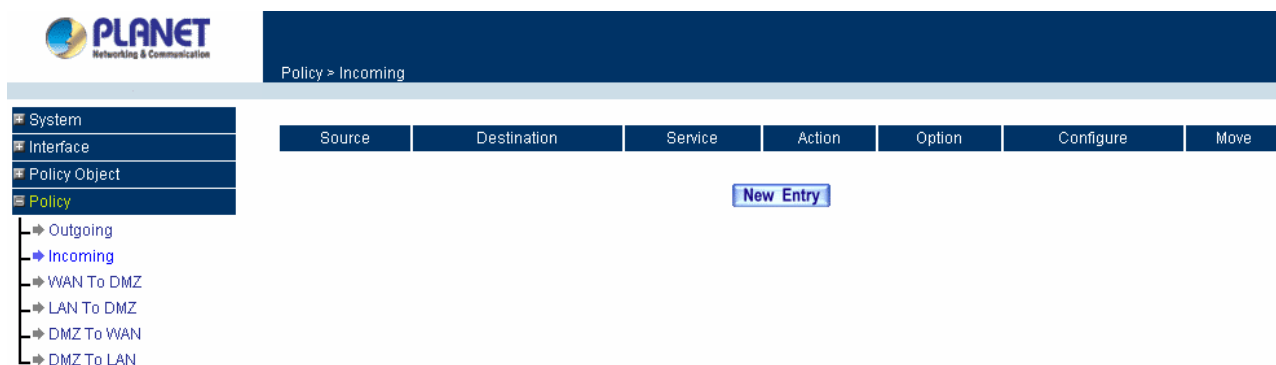
Step 3. When Policy is paused, administrator can modify the Policy Object without removing the Policy.

3.4.2 Incoming

This section describes steps to create policies for packets and services from the WAN network to the LAN network including Mapped IP and Virtual Server.

Enter Incoming window

Step 1: Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the WAN network to assigned Mapped IP or Virtual Server.



Step 2: The fields of the **Incoming** window are:

- **Source:** Source networks which are specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.
- **Destination:** Destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.
- **Service:** Services supported by Virtual Servers (or Mapped IP).
- **Action:** Control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.
- **Option:** Specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Multi-Homing Security Gateway.
- **Configure:** Modify settings or remove incoming policy.
- **Move:** This sets the sequence of the policies, number 1 being the first policy to proceed.

Adding an Incoming Policy

Step 1: Under **Incoming** of the **Policy** menu, click the New Entry button.

Step 2: Configure the parameters

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the Address menu. To create a new source address, please go to the LAN section under the Address menu.

Destination Address: Select names of the LAN networks from the drop down list. The drop down list contains the names of IP mapping addresses specified in the **Mapped IP** or the **Virtual Server** sections of **Virtual Server** menu. To create a new destination address, please go to the **Virtual Server** menu.

Service: Specified services provided by LAN network servers. These are services / application that are allowed to pass from the network to the LAN network. Choose ANY for all services.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Trunk: Check to allow VPN traffic passing through.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the specified WAN network and Virtual Server/Mapped IP.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-1000. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

NAT: Select enable to allow WAN user or DMZ user to access LAN resource using with LAN interface's IP address.


Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding new incoming policy.

Modifying Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

Step 3: Click **OK** to save modifications or click **Cancel** to cancel modifications.



Policy > Incoming

- System
- Interface
- Policy Object
- Policy**
 - Outgoing
 - Incoming**
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor

Comment :


Modify Policy	
Source Address	Outside_Any
Destination Address	Virtual Server 1(210.66.155.90)
Service	FTP(21)
Schedule	None
Trunk	None
Action	PERMIT
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None
NAT	<input type="checkbox"/> Enable

OK Cancel

Removing an Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be removed and click its corresponding **[Remove]** in the Configure field.

Step 2: In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.



Policy > Incoming

- System
- Interface
- Policy Object
- Policy**
 - Outgoing
 - Incoming**
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- IDP
- Anomaly Flow IP

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server1(210.66.155.90)	FTP(21)			Modify Remove Pause	To 1

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

Pausing the Incoming Policy

Step 1. In the **Incoming** policy section, locate the name of the policy desired to be paused and click its corresponding **Pause** option in the **Configure** field.

Step 2. In the **Pause** confirmation dialogue box, click **OK** to pause the policy or click **Cancel** to cancel pausing.

Step 3. When Policy is paused, administrator can modify the Policy Object without removing the Policy.

3.4.3 WAN To DMZ & LAN To DMZ

This section describes steps to create policies for packets and services from the WAN networks to the DMZ networks. Please follow the same procedures for LAN networks to DMZ networks.

Enter [WAN To DMZ] or [LAN To DMZ] window:

Click **WAN To DMZ** under **Policy** menu to enter the **WAN To DMZ** window. The WAN To DMZ table will show up displaying currently defined policies. Before to set up **WAN To DMZ** rule, you need to enable DMZ first.

The fields in WAN To DMZ window:

Source: Source networks, which are addresses specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.

Destination: Destination networks, which are addresses specified in **DMZ** section of the **Address** menu and **Mapped IP** addresses of the **Virtual Server** menu.

Service: Services supported by servers in DMZ network.

Action: Control actions, to permit or deny packets from WAN networks to DMZ travelling

through the Multi-Homing Security Gateway.

Option: Specify the monitoring functions of packets from WAN network to DMZ network travelling through Multi-Homing Security Gateway.

Configure: Modify settings or remove policies.

Move: This sets the priority of the policies, number 1 being the highest priority.

Adding a new WAN To DMZ Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.

The screenshot shows the Planet Networking & Communication web interface. On the left is a navigation menu with categories: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, and Monitor. The 'Policy' category is expanded, showing sub-items: Outgoing, Incoming, WAN To DMZ (highlighted), LAN To DMZ, DMZ To WAN, and DMZ To LAN. The main content area is titled 'Policy > WAN To DMZ' and contains the 'Add New Policy' form. The form includes a 'Comment' field and various configuration options:

Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Schedule	None
Trunk	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None
NAT	<input type="checkbox"/> Enable

At the bottom right of the form are 'OK' and 'Cancel' buttons.

Step 2: Configure the parameters.

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the **WAN** section of the **Address** menu. To create a new source address, please go to the **LAN** section under the **Address** menu.

Destination Address: Select the name of the DMZ network from the drop down list. The drop down list contains the names of the DMZ network created in the **Address** menu. It will also contain Mapped IP addresses from the **Virtual Server** menu that were created for the DMZ network. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to the sections entitled **Address** and **Virtual Server** for details)

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the WAN network to the DMZ network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu. (Please refer to the section entitled **Services** for details)

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Trunk: Check to allow VPN traffic passing through.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified WAN network to the DMZ network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-1000. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

NAT: Select enable to allow WAN or LAN user to access DMZ resource using with DMZ interface's IP address.

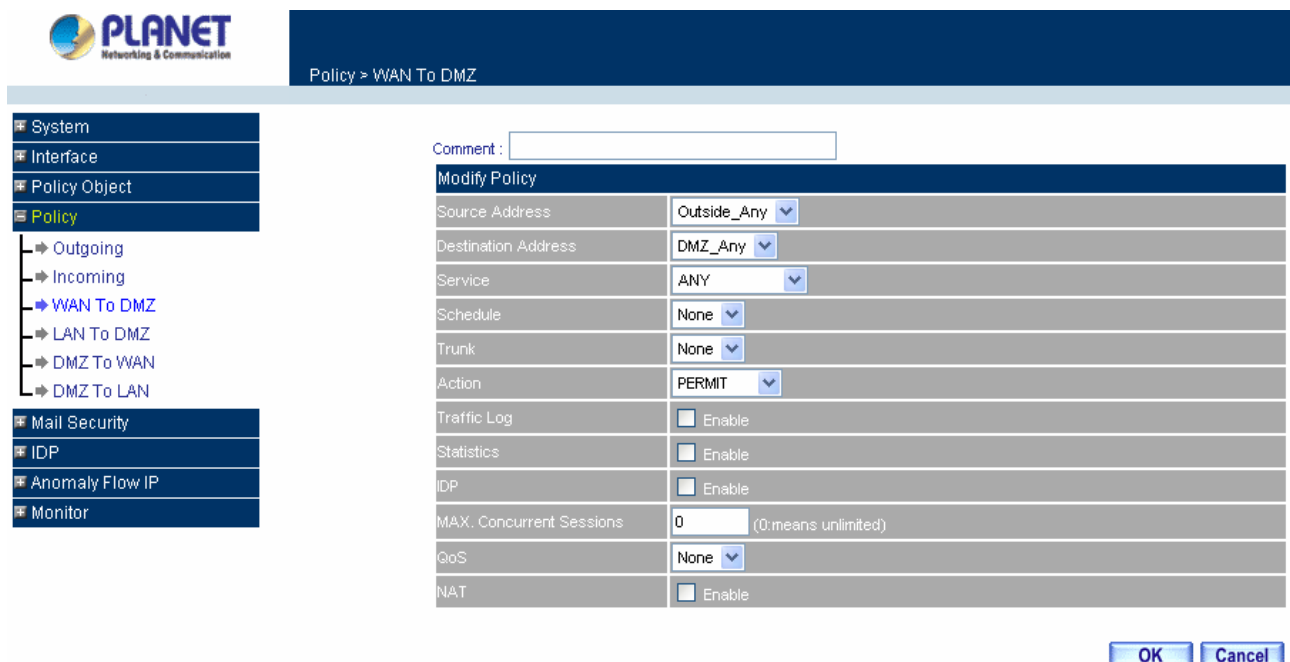
Step 3: Click **OK**.

Modifying a WAN To DMZ policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be modified and click its corresponding **Modify** option in the **Configure** field.

Step 2: In the **Modify Policy** window, fill in new settings.

Step 3: Click **OK** to do save modifications.



The screenshot displays the Planet Networking & Communication software interface. On the left is a navigation tree with categories: System, Interface, Policy Object, and Policy. Under 'Policy', there are sub-items: Outgoing, Incoming, WAN To DMZ (highlighted with a blue arrow), LAN To DMZ, DMZ To WAN, and DMZ To LAN. Below this are Mail Security, IDP, Anomaly Flow IP, and Monitor. The main area shows the 'Policy > WAN To DMZ' configuration window. At the top, there's a 'Comment' field. Below it is the 'Modify Policy' table with the following settings:

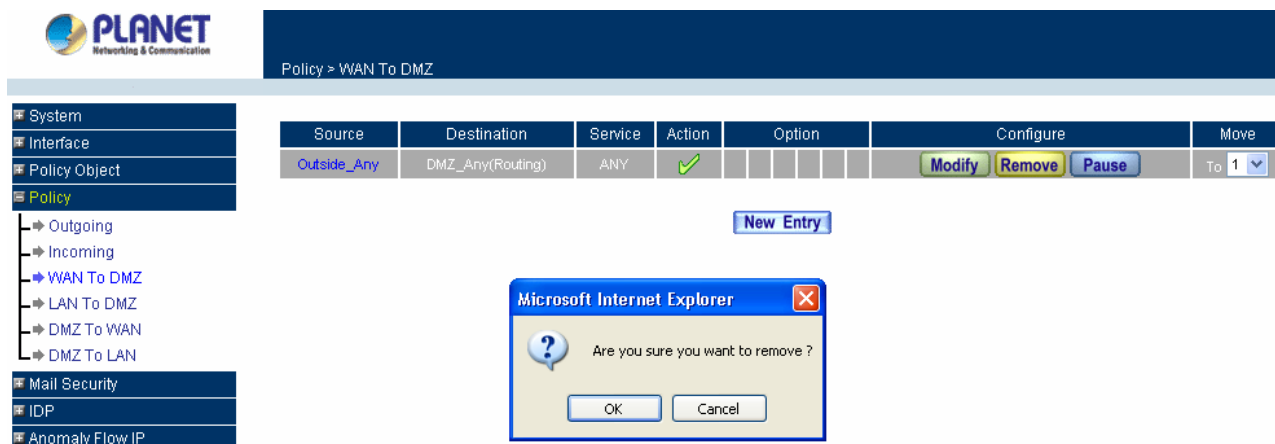
Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Schedule	None
Trunk	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None
NAT	<input type="checkbox"/> Enable

At the bottom right of the window are 'OK' and 'Cancel' buttons.

Removing a WAN To DMZ Policy:

Step 1: In the **WAN To DMZ** window, locate the name of policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

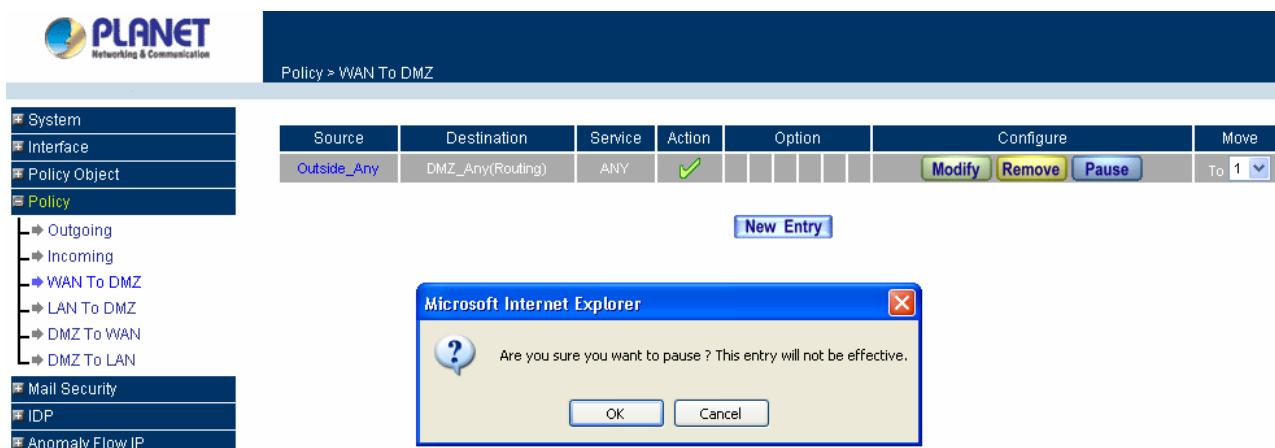
Step 2: In the **Remove** confirmation pop-up box, click **OK** to remove the policy.



Pausing the Incoming Policy

Step 1. In the **WAN to DMZ** or **LAN to DMZ** policy section, locate the name of the policy desired to be paused and click its corresponding **Pause** option in the **Configure** field.

Step 2. In the **Pause** confirmation dialogue box, click **OK** to pause the policy or click **Cancel** to cancel pausing.



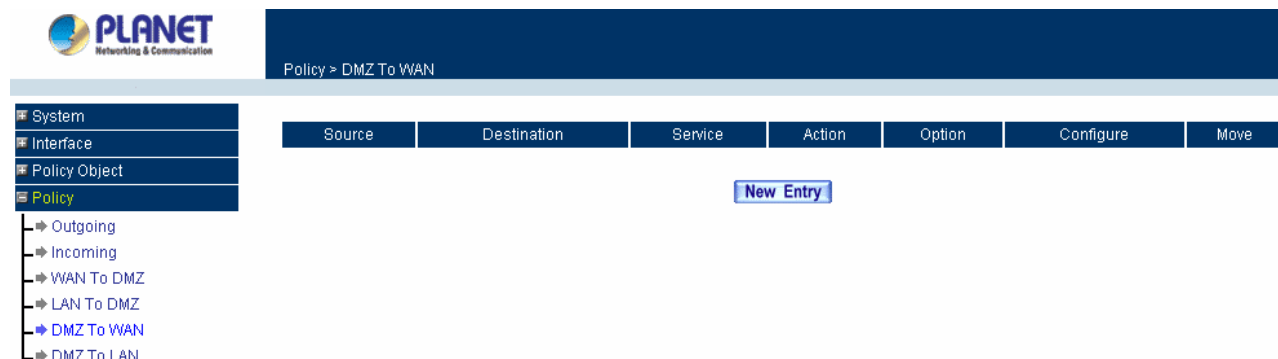
Step 3. When Policy is paused, administrator can modify the Policy Object without removing the Policy.

3.4.4 DMZ To WAN & DMZ To LAN

This section describes steps to create policies for packets and services from DMZ networks to WAN networks. Please follow the same procedures for DMZ networks to LAN networks.

Entering the DMZ To WAN window:

Click **DMZ To WAN** under **Policy** menu and the **DMZ To WAN** table appears displaying currently defined **DMZ To WAN** policies.

**The fields in the DMZ To WAN window are:**

Source: Source network addresses which are specified in the **DMZ** section of the **Address** window.

Destination: Destination networks, which is the WAN network address

Service: Services supported by Servers of WAN networks.

Action: Control actions, to permit or deny packets from the DMZ network to WAN networks travelling through the Multi-Homing Security Gateway.

Option: Specify the monitoring functions on packets from the DMZ network to WAN networks travelling through the Multi-Homing Security Gateway.

Configure: Modify settings or remove policies

Move: This sets the sequence of the policies, number 1 being the first policy to proceed.

Adding a DMZ To WAN Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Policy > DMZ To WAN

Comment :

Add New Policy

Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT_ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0:means unlimited)
QoS	None

Step 2: Configure the parameters.

Source Address: Select the name of the DMZ network from the drop down list. The drop down list will contain names of DMZ networks defined in **DMZ** section of the **Address** menu. To add a new source address, please go to the **DMZ** section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list lists names of addresses defined in **WAN** section of the **Address** menu. To add a new destination address, please go to **WAN** section of the **Address** menu.

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the DMZ network to the WAN network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Authentication User: Select the item listed in the Authentication User to enable the policy to automatically execute the function in a certain time and range.

Trunk: Check to allow VPN traffic passing through.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified DMZ network to the WAN network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Select Enable to enable Content Blocking.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-1000. 0 means it is unlimited.

QoS: Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding.

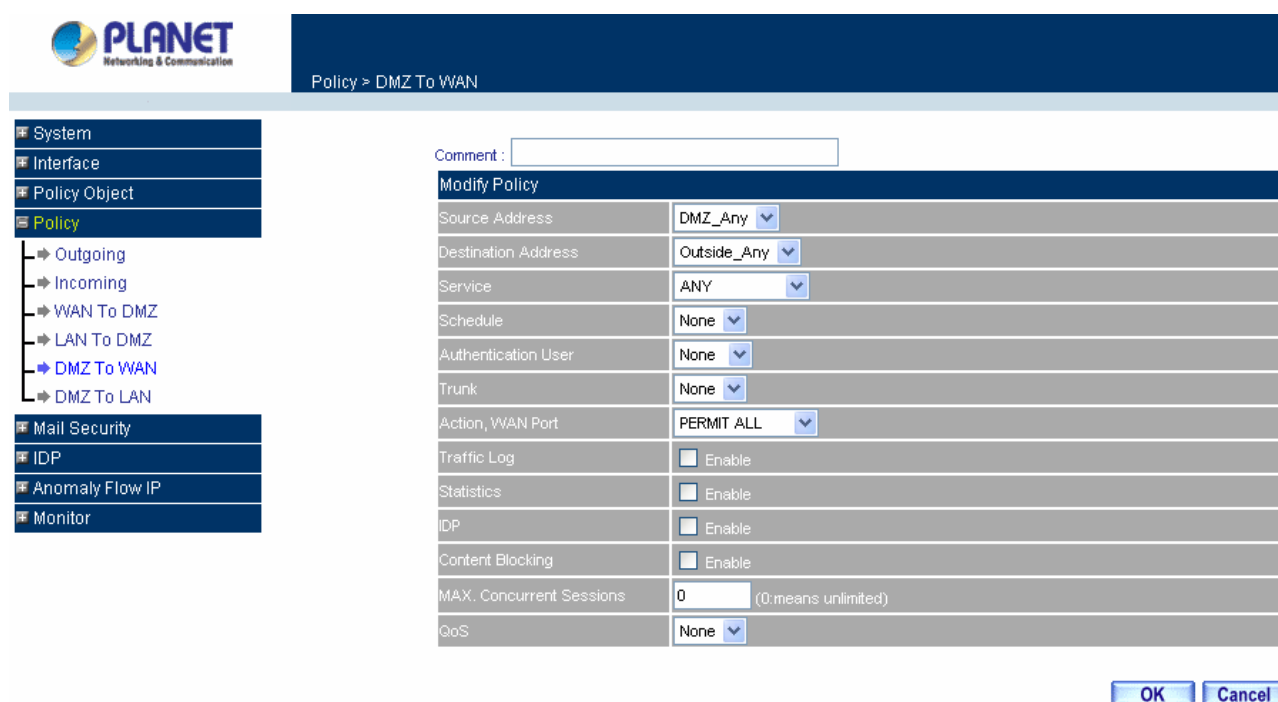
Modifying a DMZ To WAN policy:

Step 1: In the DMZ To WAN window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

NOTE: To change or add selections in the drop-down list, go to the section where the selections are setup. (Source Address → DMZ of Address; Destination Address → WAN, Service → Pre-defined Service, Custom or Group under Service.)

Step 3: Click OK to save modifications or click Cancel to cancel modifications.



The screenshot displays the PLANET Networking & Communication web interface. On the left is a navigation menu with options: System, Interface, Policy Object, Policy (selected), Mail Security, IDP, Anomaly Flow IP, and Monitor. Under the 'Policy' section, there are sub-options: Outgoing, Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN (highlighted), and DMZ To LAN. The main area shows the 'Policy > DMZ To WAN' configuration window. At the top, there is a 'Comment' text box. Below it is the 'Modify Policy' section with various settings:

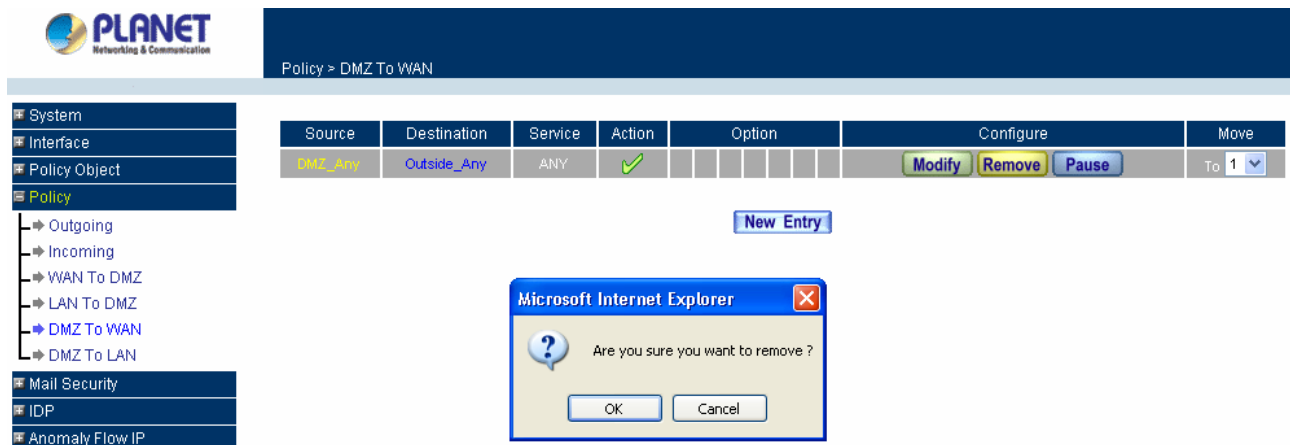
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Trunk	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0 (0 means unlimited)
QoS	None

At the bottom right of the window are 'OK' and 'Cancel' buttons.

Removing a DMZ To WAN Policy:

Step 1. In the **DMZ To WAN** window, locate the name of policy desired to be removed and click its corresponding Remove option in the Configure field.

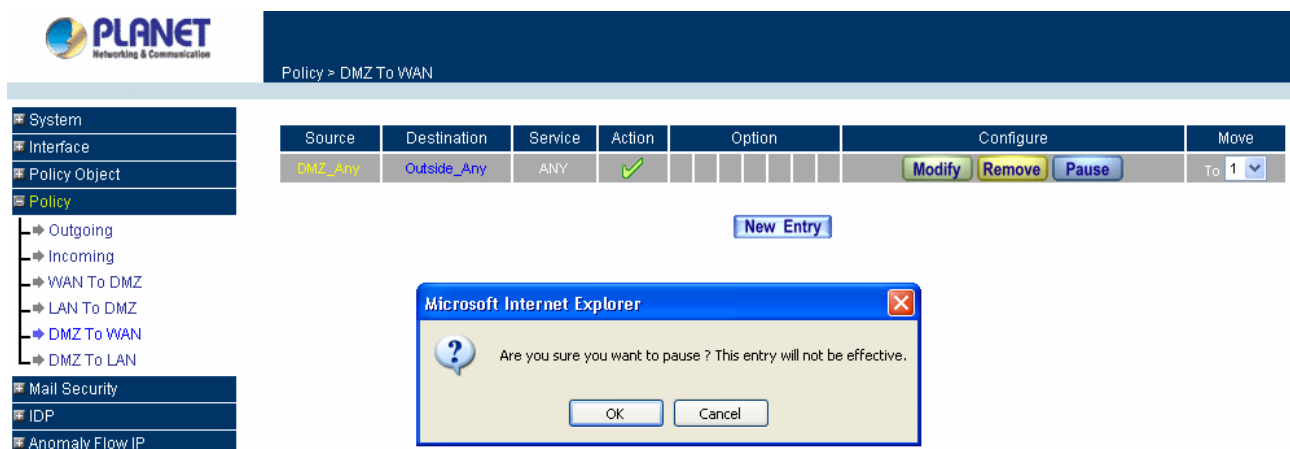
Step 2. In the **Remove confirmation** dialogue box, click **OK**.



Pausing the DMZ to WAN or DMZ to LAN Policy

Step 1. In the **DMZ to WAN** or **DMZ to LAN** policy section, locate the name of the policy desired to be paused and click its corresponding **Pause** option in the **Configure** field.

Step 2. In the **Pause** confirmation dialogue box, click **OK** to pause the policy or click **Cancel** to cancel pausing.



Step 3. When Policy is paused, administrator can modify the Policy Object without removing the Policy.

3.5 Mail Security

This section provides the Administrator to configure Mail Security rule for protecting client PC from virus and spam mail attacking. Meanwhile, CS-1000 provides the ability to update virus pattern by schedule or manually, and it also provides auto-learning system to raise the rate of spam mail judging. For more detail information please check the related chapter.

3.5.1 Configure

About the Mail Security Configure function, it means the dealing standard towards mail of CS-1000. In this chapter, it is defined as Setting and Mail Relay.

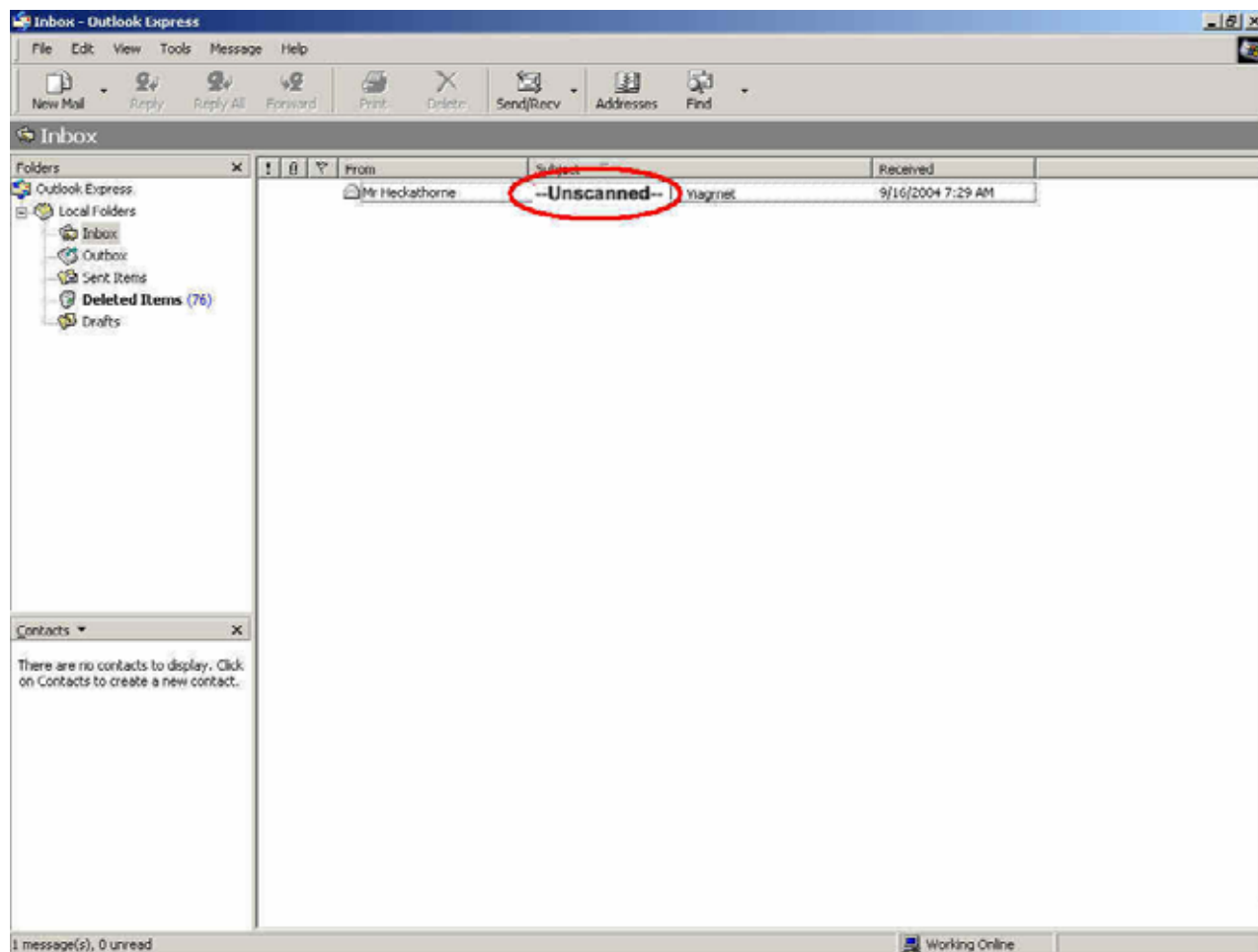
Setting:

Define the required fields of setting:

Scanned Mail Setting: Setup to deal with the mail size in order to judge the mail should be scanned or not.

Unscanned Mail Setting: If the mail does not be scanned via CS-1000, it can be marked an unscanned message in the mail subject. For example, if the mail size is larger than the **Scanned Mail Setting**, when you receive mail you will find out the subject with the mark "Unscanned".

When receive unscanned mail, it will add the tag in front of the e-mail subject.



Mail Relay: After scanning the mails that sent to Internal Mail Server by **Anti-Spam** and **Anti-Virus** function of CS-1000, then to setup the relevant setting in **Mail Relay** function. For the examples below you can understand more about how to configure your setting.

Example 1: To setup CS-1000 as Gateway (Mail Server in DMZ, Transparent Mode)

Preparation:

WAN Port IP: 61.11.11.11

Mail Server IP: 61.11.11.12

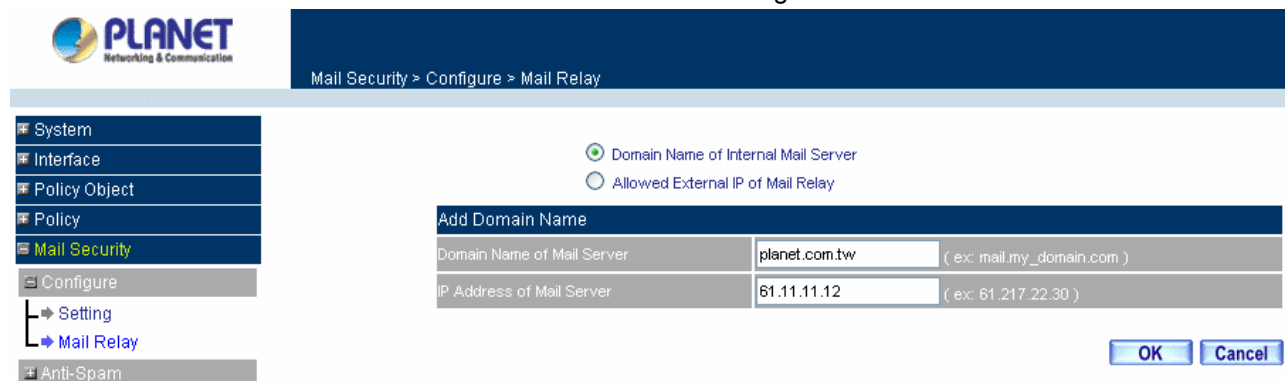
Map the DNS Domain Name that apply from ISP (planet.com.tw) to DNS Server IP (setup MX record is Mail Server IP)

When external sender sends mail to the recipient account of the planet.com.tw domain, add the following Mail Relay setting:

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

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

Mail Relay setting is complete. The external mails send to planet.com.tw that will be received by CS-1000 and redirect to the mail server after filtering.



The screenshot shows the Planet CS-1000 configuration interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security (highlighted), Configure, Setting, Mail Relay (highlighted), and Anti-Spam. The main content area is titled 'Mail Security > Configure > Mail Relay'. It features two radio buttons: 'Domain Name of Internal Mail Server' (selected) and 'Allowed External IP of Mail Relay'. Below these is a table titled 'Add Domain Name' with two rows: 'Domain Name of Mail Server' with the value 'planet.com.tw' (example: mail.my_domain.com) and 'IP Address of Mail Server' with the value '61.11.11.12' (example: 61.217.22.30). At the bottom right are 'OK' and 'Cancel' buttons.

Example 2: To setup CS-1000 between the original Gateway and Mail Server (Mail Server in DMZ, Transparent Mode)

Preparation:

The Original Gateway's LAN Subnet: 172.16.1.0/16

WAN Port IP: 61.11.11.11

CS-1000's WAN Port IP: 172.16.1.12

Mail Server IP: 172.16.1.13

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

When LAN (172.16.1.0/16) users send mail from the sender account of planet.com.tw mail server to the recipient account in external mail server, the configuration should need to add the following mail relay setting:

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

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

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

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

Example 3: The Headquarters setup CS-1000 as Gateway (Mail Server in DMZ, Transparent Mode) to make the Branch office's employees can send mails via Headquarters' Mail Server

Preparation:

WAN Port IP of CS-1000: 61.11.11.11

Mail Server IP: 61.11.11.12

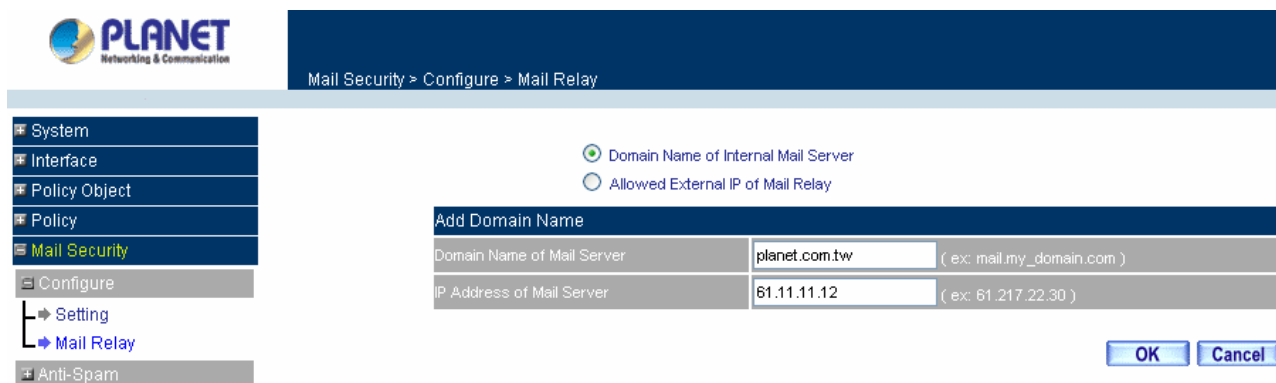
WAN Port IP of the Branch office's Firewall: 211.22.22.22

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

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

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

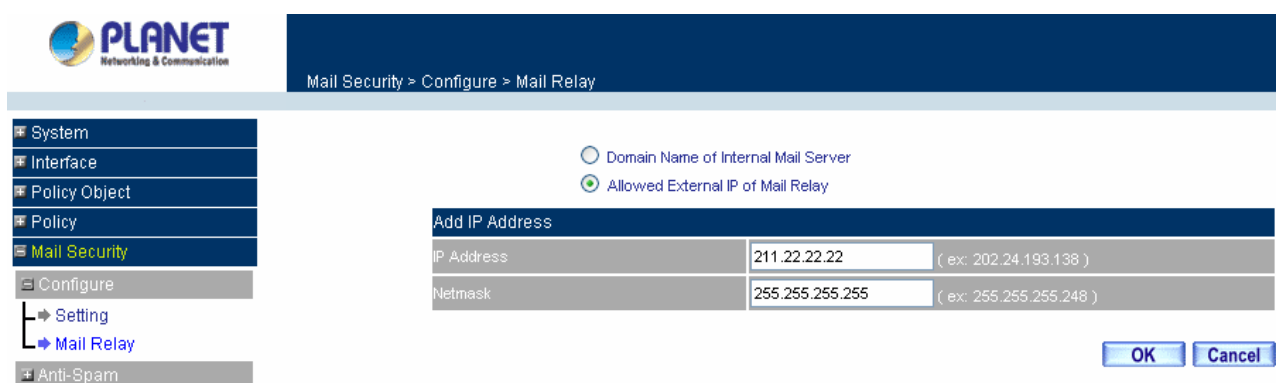
- Select **Domain Name of Internal Mail Server**
- **Domain Name of Mail Server:** Enter the Domain Name
- **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.



The screenshot shows the Planet Security Gateway configuration interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security (highlighted), Configure, Setting, Mail Relay (highlighted), and Anti-Spam. The main content area is titled "Mail Security > Configure > Mail Relay". It features two radio buttons: "Domain Name of Internal Mail Server" (selected) and "Allowed External IP of Mail Relay". Below the radio buttons is a form titled "Add Domain Name" with two input fields: "Domain Name of Mail Server" (containing "planet.com.tw" with a hint "(ex: mail.my_domain.com)") and "IP Address of Mail Server" (containing "61.11.11.12" with a hint "(ex: 61.217.22.30)"). At the bottom right are "OK" and "Cancel" buttons.

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

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



The screenshot shows the Planet Security Gateway configuration interface. The left sidebar is identical to the previous screenshot. The main content area is titled "Mail Security > Configure > Mail Relay". It features two radio buttons: "Domain Name of Internal Mail Server" and "Allowed External IP of Mail Relay" (selected). Below the radio buttons is a form titled "Add IP Address" with two input fields: "IP Address" (containing "211.22.22.22" with a hint "(ex: 202.24.193.138)") and "Netmask" (containing "255.255.255.255" with a hint "(ex: 255.255.255.248)"). At the bottom right are "OK" and "Cancel" buttons.

3.5.2 Anti-Spam

CS-1000 can filter the e-mails that are going to send to the mail server of enterprise, in order to make sure the e-mail account that communicates with outside won't receive a mass advertisement or Spam mail. Meanwhile, it can reduce the burden of mail server. Also can prevent the users to pick up the message he/she needs from a mass of useless mails; or delete the needed mail mistakenly while deleting mails. It will raise the work efficiency of the employees and will not lose the important information of enterprise.

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

3.5.2.1 Setting

The Administrator can choose the inspection way of the mails, where the mail server is placed in Internal (LAN or DMZ) or External (WAN). CS-1000 also can inspect all of the mails that are sent to the enterprise, and add a score tag or message to the subject line of Spam mail while it exceeds the standard. Meanwhile, it supports to check sender address in blacklist of anti-spam website to determine if it is spam mail or not.

PLANET
Networking & Communication

Mail Security > Anti-Spam > Setting

Spam Setting

☒ Enable Anti-Spam

The Mail Server is placed in ☐ Internal (LAN or DMZ) (Please set Mail Relay first) ☒ External (WAN)

The threshold score of spam mail is (Max. 256 characters)

Add the message to the subject line (Max. 256 characters)

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

☒ Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)

☒ Check sender account

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

☒ Add score tag to the subject line

Action of Spam Mail

Internal Mail Server:

☐ Delete the spam mail

☐ Deliver to the recipient

☐ Forward to : (ex: user@mydomain.com)

External Mail Server:

☒ Deliver to the recipient (Always enable)

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

Definition:

Enable Anti-Spam: Select to enable Anti-Spam function.

The Mail Server is placed in Internal (LAN or DMZ) or External (WAN): Select to choose the location of the mail server. In order to enable Anti-Spam feature in **Internal** Mail server, administrator must configure **Mail Relay** setting first.

The threshold score of spam mail is: CS-1000 allows the Administrator to decide the threshold to be the standard of judging the spam mail.

Add the message to the subject line: If the mail has been judged to the spam mail, CS-1000 will add a message in the mail's subject. You can configure the message you want, by default, it will be add "---SPAM---" in the subject.

Check spam fingerprint: Select to allow CS-1000 checking spam mail with Fingerprint system.

Enable Bayesian filtering: Except to select fingerprinter system to distinguish spam mail, you also can select Bayesian filtering system to scan spam mail.

Check sender account: Select to allow CS-1000 checking sender's account when it receives the mail, if the sender's account is faked, CS-1000 will treat the mail as the spam.

Check sender IP address in RBL (Realtime Blackhole List): Select this function to allow CS-1000 checking mail with RBL list to Judge the spam mail.

Add score tag to the subject line: If select this function, all received mail will be added a score tag in the mail subject.

Action of Spam Mail: When CS-1000 filters the spam mail, there are three kinds of actions for Internal Mail Server and one action for External Mail server to arrange the spam mail:

Delete the spam mail: If select this option, the spam mail will be deleted without any notification.

Deliver to the recipient: Pass the mail to the recipient, and add a "SPAM" in the mail subject. This function is available for Internal and External Mail Server.

Forward to: Select to forward spam mail to a specific mail account; that can be easily to manage the spam mail.

Configure an Anti- Spam setting

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

1. The Mail Server is placed in **Internal (LAN or DMZ)**
2. **The threshold score:** Enter 5
3. **Add the message to the subject line:** Enter ---spam---
4. Select the spam mail filtering system to enable the Anti-spam function
5. Select **Add score tag to the subject line**
6. Select **Deliver to the recipient**
7. Click **OK**.

3.5.2.2 Rule

The Multi-Homing Security Gateway's Administrator may use the rule setting to classify the spam mail based on a certain condition. The rule also can allow CS-1000 to record the mail type by auto-learning system in order to judge the spam mail.

Click on **Mail Security** in the menu bar, then click on **Rule** below the **Anti-Spam** menu. The Rule window will appear.



Below is the information needed for setting up the **Rule**:

- **Rule Name:** The name of the custom spam mail determination rule.
- **Comments:** To explain the meaning of the custom rule.
- **Combination:**
 - And:** It must be fit in with all of the custom mail rules that would be considered as spam mail or ham mail.
 - Or:** Only be fit in with one of the custom mail rule that would be considered as spam mail or ham mail.
- **Classification:**
 - Spam:** It will classify the mails that correspond to the rule as spam mail.
 - Ham (Non-Spam):** It will classify the mails that correspond to the rule as ham mail.
- **Action:** This function will be available only when **Classification** is set as **Spam**. You can choose the action to **Delete spam mail**, **Deliver to the recipient**, **Forward to** another mail account, or the **Same as Spam Setting**.
- **Auto-Training:** If **Classification** is set as **Spam** and enable this function, the mails that correspond to this rule will be trained to identify as spam mail; or if **Classification** is set as **Ham (Non-Spam)** and enable this function, the mails correspond to this rule will be trained to identify as ham (non-spam) mail according to the setting in Training function
- **Item:** The items use to judge the spam mail according to **Header**, **Body** and **Size** of the mail. The packet Header includes: **Received**, **Envelope-To**, **Form**, **To**, **Cc**, **Bcc**, **Subject**, **Sender**, **Reply-To**, **Errors-To**, **Message-ID**, **Date**, **Header**, **Body**, **Attach File Name** and **Size (Kbytes)**.
- **Condition:**
 - Item set to Header or Body:** The available conditions are: **Contains**, **Does Not Contain**, **Is Equal To**, **Is Not Equal To**, **Starts With**, **Ends With**, **Exist** and **Does Not Exist**.
 - Item set to Size:** The available conditions are: **More Than**, **Is Equal To**, **Is Not Equal To** and **Less Than**.
- **Pattern:** Enter the relevant value in **Item** and **Condition** field. For example: **From** Item and use **Contains** Condition, and enter "josh" as a characteristics. When the sender and receiver's mail account has "josh" inside and then it will be considered as spam mail or ham mail

Adding a new Rule

Step 1: Click on the **New Entry** button and the **Rule** window will appear.

Step 2: Fill in the appropriate settings for the related information.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

The screenshot shows the Planet Networking & Communication web interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security (selected), Configure, Anti-Spam, Setting, Rule (selected), Whitelist, Blacklist, Training, and Spam Mail. The main content area is titled "Mail Security > Anti-Spam > Rule". It contains the following fields:

- Rule Name:
- Comments:
- Combination:
- Classification:
- Action:
- Auto-Training:

Below these fields is a table with four columns: Item, Condition, Pattern, and Configure. The first row contains the following data:

Item	Condition	Pattern	Configure
<input type="text" value="Received"/>	<input type="text" value="Contains"/>	<input type="text"/>	<input type="button" value="Next Row"/>

At the bottom right of the main content area are two buttons: and .

Modifying a Rule

Step 1: In the **Rule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

Removing a Rule

Step 1: In the **Rule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.

The screenshot shows the Planet Networking & Communication web interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security (selected), Configure, Anti-Spam, Setting, Rule (selected), Whitelist, Blacklist, Training, and Spam Mail. The main content area is titled "Mail Security > Anti-Spam > Rule". It contains a table with the following columns: Rule Name, Classification, Action, Comments, Configure, and Move. The first row contains the following data:

Rule Name	Classification	Action	Comments	Configure	Move
test	Spam	Delete spam mail		<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To 1 <input type="text"/>

Below the table is a button: .

A confirmation dialog box titled "Microsoft Internet Explorer" is displayed in the foreground. It contains a question mark icon and the text "Are you sure you want to remove?". At the bottom of the dialog are two buttons: and .

3.5.2.3 Whitelist

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

Below is the information needed for setting up the **Whitelist**

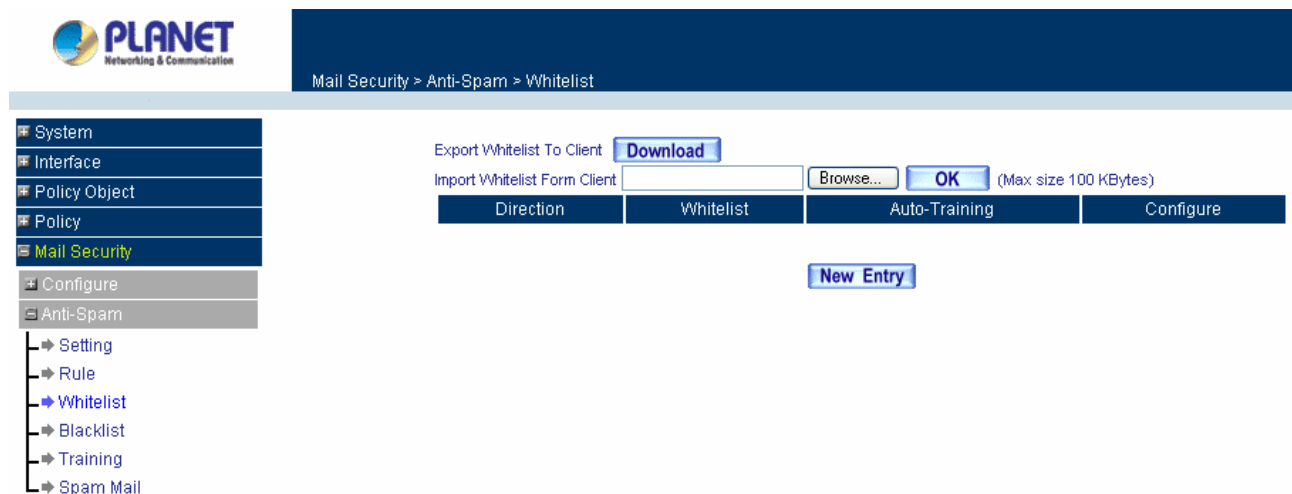
- **Whitelist:** Specify the key word or with wildcard for the Whitelist field.
- **Direction:**
 - From:** To judge the sending address of the mail.
 - To:** To judge the receiving address of the mail.
- **Auto-Training:** Select enable to allow Auto-Training system updating the CS-1000's database.

Adding a new Whitelist

Step 1: Click on the **New Entry** button and the **Whitelist** window will appear.

Step 2: Fill in the appropriate settings for the related information..

Step 3: Click **OK** to save the policy or **Cancel** to cancel.



Modifying a Whitelist

Step 1: In the **Whitelist** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.



Mail Security > Anti-Spam > Whitelist

- System
- Interface
- Policy Object
- Policy
- Mail Security
 - Configure
 - Anti-Spam
 - Setting
 - Rule
 - Whitelist
 - Blacklist
 - Training
 - Spam Mail

Modify Whitelist

Whitelist: (ex: *yahoo*, *: wildcard)


Direction:

Auto-Training:

Removing a Whitelist

Step 1: In the **Rule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



Mail Security > Anti-Spam > Whitelist

- System
- Interface
- Policy Object
- Policy
- Mail Security
 - Configure
 - Anti-Spam
 - Setting
 - Rule
 - Whitelist
 - Blacklist
 - Training
 - Spam Mail
 - Anti-Virus

Export Whitelist To Client

Import Whitelist Form Client (Max size 100 KBytes)

Direction	Whitelist	Auto-Training	Configure
From	planet		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
To	hotmail		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

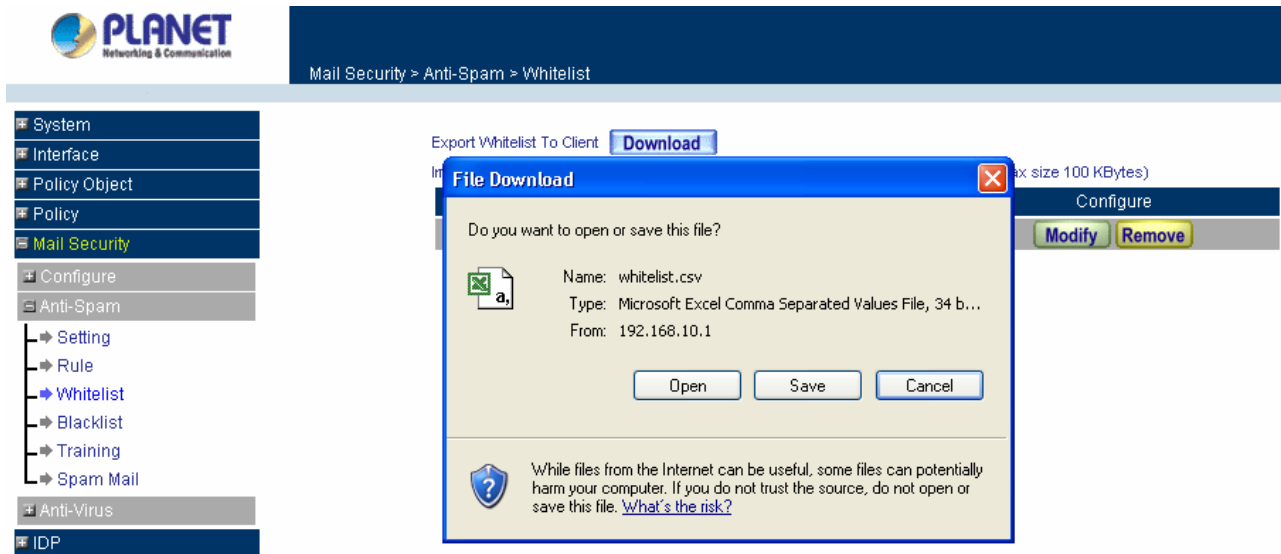
Microsoft Internet Explorer

Are you sure you want to remove ?

Export Whitelist To Client

Step 1: Press **Download** button to save the Whitelist as a file. The file format is *.csv type.

Step 2: Select the destination path you want to save the file, then press **Save** to save the file.



Import Whitelist From Client

Step 1: Press **Browse** to select the file you want to import, then press **OK** to import file to Whitelist.



Note: The file can be modified first before importing to CS-1000, use Notepad program and type the data as following:

```
Direction,Whitelist
From,planet
To,hotmail
```

3.5.2.4 Blacklist

To determine the mail comes from specific mail address that will be filtered or restricted.

Below is the information needed for setting up the **Blacklist**

- **Blacklist:** Specify the key word or with wildcard for the Blacklist field.
- **Direction:**
 - From:** To judge the sending address of the mail.
 - To:** To judge the receiving address of the mail.
- **Auto-Training:** Select enable to allow Auto-Training system updating the CS-1000's database.

Adding a new Blacklist

Step 1: Click on the **New Entry** button and the **Blacklist** window will appear.

Step 2: Fill in the appropriate settings for the related information..

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

Modifying a Blacklist

Step 1: In the **Blacklist** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

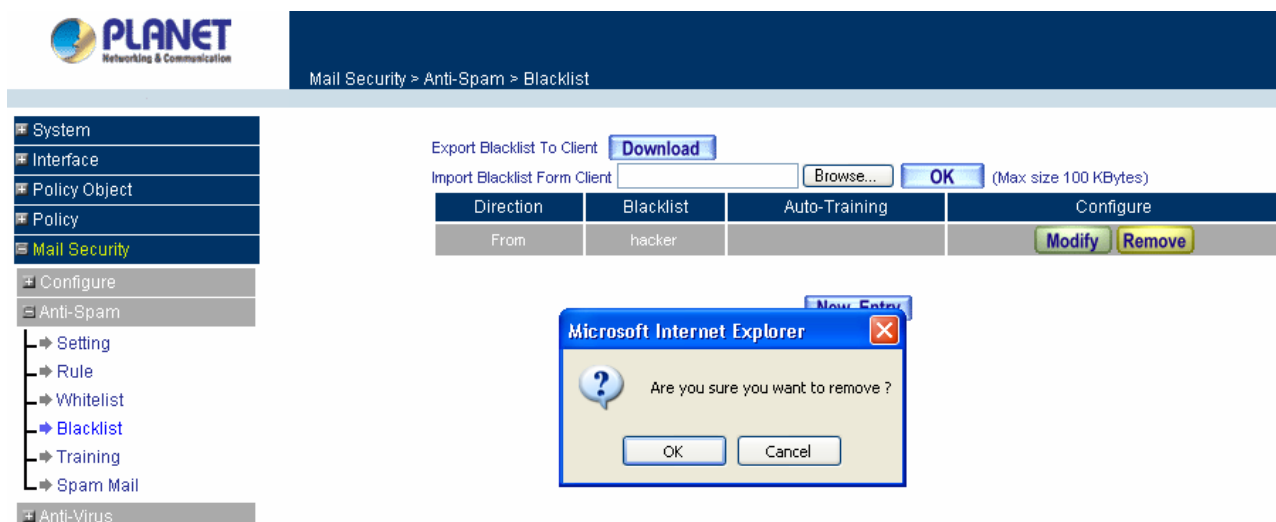
Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

Removing a Blacklist

Step 1: In the **Blacklist** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

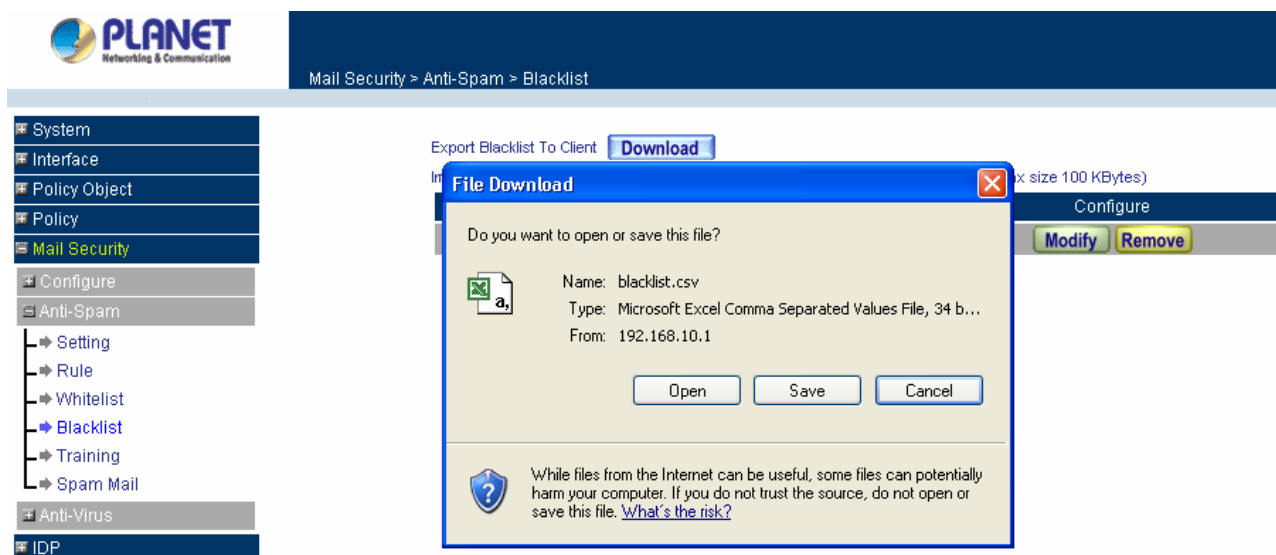
Step 2: A confirmation pop-up box will appear, click **OK** to remove the Host Table or click **Cancel**.



Export Blacklist To Client

Step 1: Press **Download** button to save the Blacklist as a file. The file format is *.csv type.

Step 2: Select the destination path you want to save the file, then press **Save** to save the file.



Import Blacklist From Client

Step 1: Press **Browse** to select the file you want to import, then press **OK** to import file to Blacklist.



Note: The file can be modified first before importing to CS-1000, use Notepad program and type the data as following:

Direction,Whitelist
From,planet
To,hotmail

3.5.2.5 Training

CS-1000 provides a training system to improve the identify rate of spam, the database can be updated by manually or from the rule setting. Below is the information needed for setting up the **Training**.

- **Training Database:** The System Manager can Import or Export Training Database here.
- **Spam Mail for Training:** The System Manager can import the file which is not determined as spam mail here. To raise the judgment rate of spam mail after the CS-1000 learning the file.
- **Ham Mail for Training:** The System Manager can import the file which is determined as spam mail here. To raise the judgment rate of ham mail after the CS-1000 learning the file
- **Spam Account for Training:** You can specify a mail account in your mail server, and redirect all the spam mail to this account. When the related configuration is set, such as **POP3 server**, **User name** and **Password**, CS-1000 will search the spam mail in this account and update the spam type to the database in a regular time.
- **Ham Account for Training:** You can specify a mail account in your mail server, and redirect all the ham mail to this account. When the related configuration is set, such as **POP3 server**, **User name** and **Password**, CS-1000 will search the ham mail in this account and update the ham type to the database in a regular time.
- **Training Time:** The System Manager can set the training time for CS-1000 to import the file per each day.

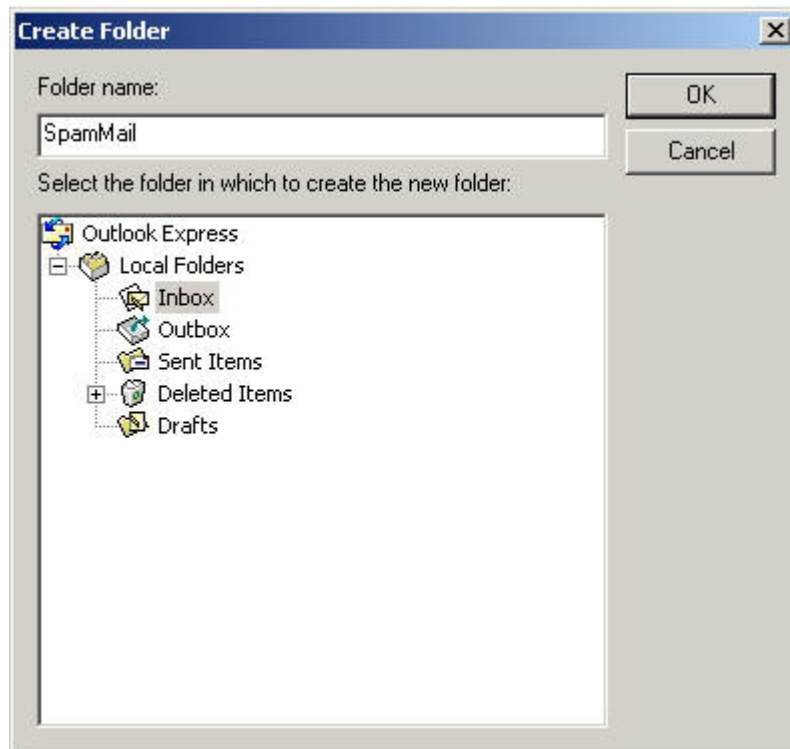
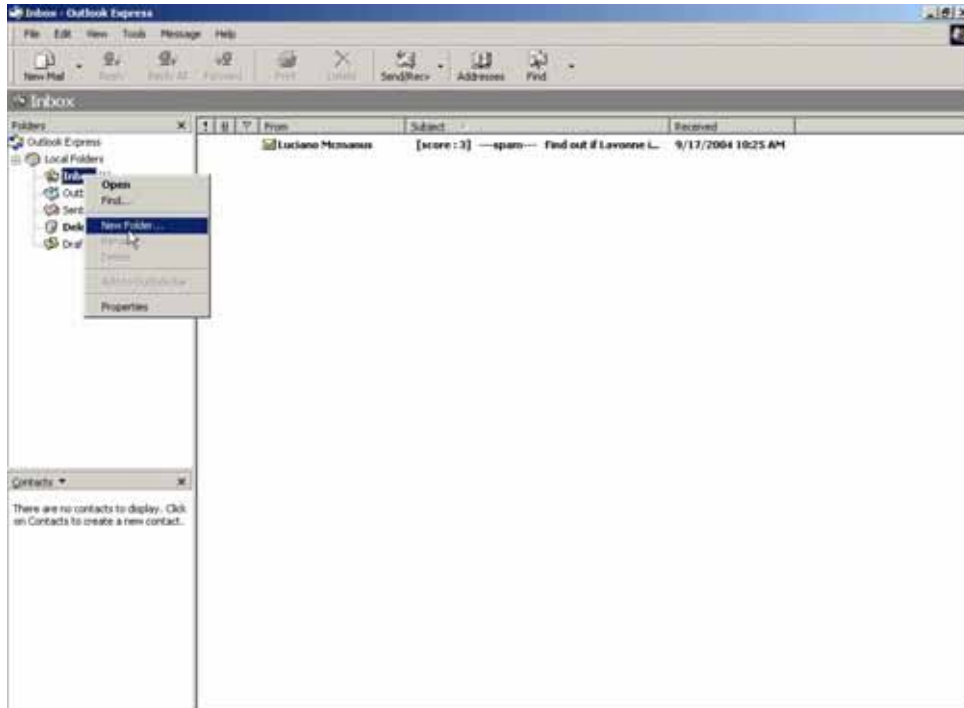


Mail Security > Anti-Spam > Training

<ul style="list-style-type: none"> System Interface Policy Object Policy Mail Security <ul style="list-style-type: none"> Configure Anti-Spam <ul style="list-style-type: none"> Setting Rule Whitelist Blacklist Training Spam Mail Anti-Virus IDP Anomaly Flow IP Monitor 	<p>Free space for training: 876 KBytes The amount of spam mail : 0 The amount of ham mail : 0 Bayesian filtering works until database has at least 200 spams and 200 hams</p> <p>Training Database</p> <p>Export Training Database <input type="button" value="Download"/></p> <p>Import Training Database <input type="text"/> <input type="button" value="Browse..."/></p> <p>Reset Training Database <input type="button" value="Reset Database"/></p> <p>Spam Mail for Training</p> <p>Import Spam Mail from Client <input type="text"/> <input type="button" value="Browse..."/></p> <p>Ham Mail for Training</p> <p>Import Ham Mail from Client <input type="text"/> <input type="button" value="Browse..."/></p> <p>Spam Account for Training</p> <p>POP3 Server <input type="text"/> (ex: my_domain.com)</p> <p>User name <input type="text"/> (ex: spam)</p> <p>Password <input type="text"/> (ex: 5d2#k...)</p> <p>Spam account test <input type="button" value="Account Test"/></p> <p>Ham Account for Training</p> <p>POP3 Server <input type="text"/> (ex: my_domain.com)</p> <p>User name <input type="text"/> (ex: ham)</p> <p>Password <input type="text"/> (ex: 5d2#k...)</p> <p>Ham account test <input type="button" value="Account Test"/></p> <p>Training time</p> <p>Training database starts at <input type="text" value="00:00"/> / day</p> <p>Training immediately : <input type="button" value="Training NOW"/></p> <p style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>
---	--

Example: How to train mail into CS-1000**STEP 1 . Create a new folder SpamMail in Outlook Express:**

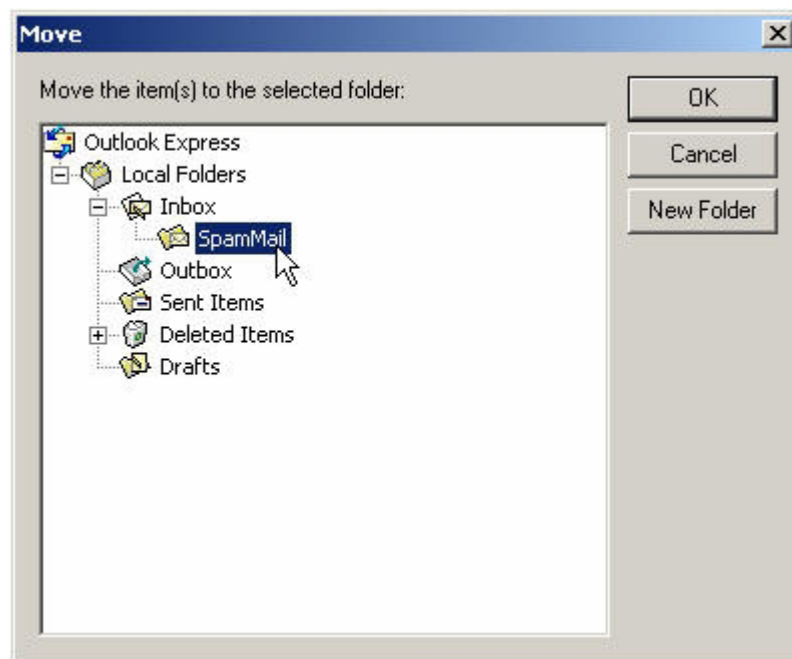
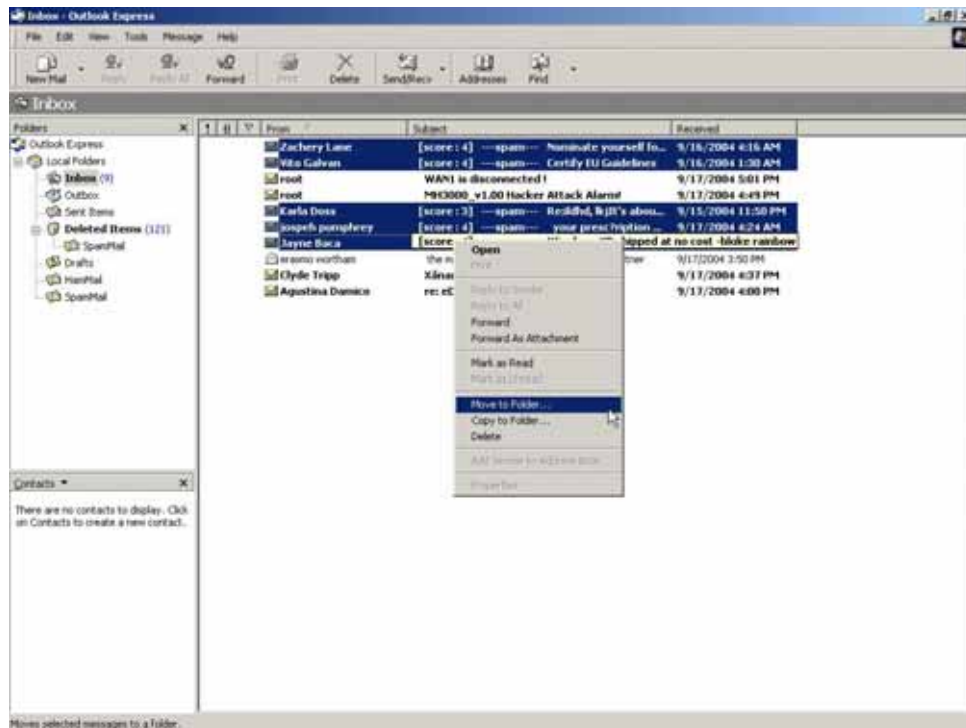
- Press the right key of the mouse and select **New Folder**.
- In **Create Folder** WebUI and enter the Folder's Name as SpamMail, and then click on OK.

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

- In Inbox, select all of the spam mails that do not judge correctly and press the right key of

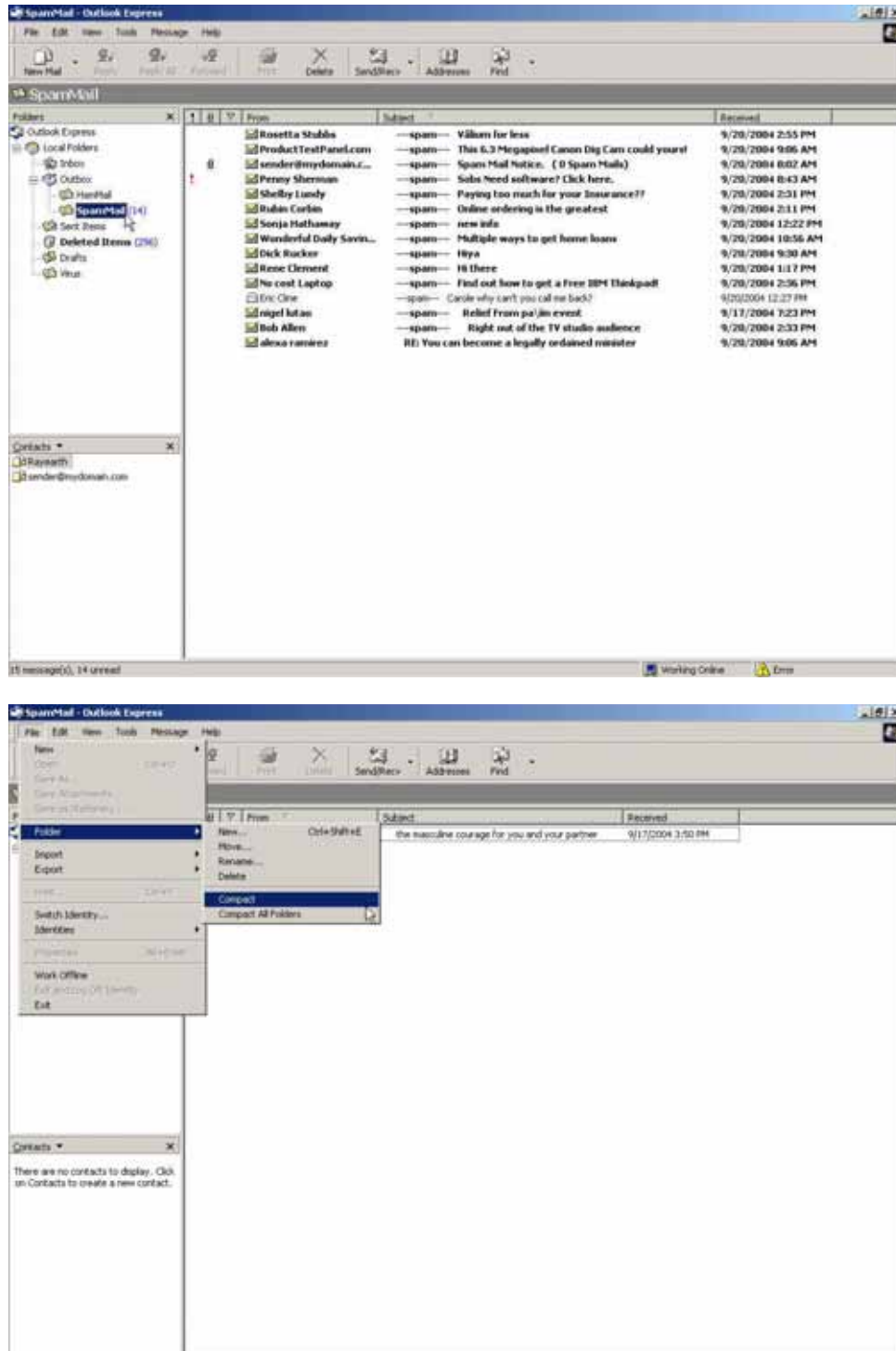
the mouse and move to the folder.

- In **Move WebUI**, select **SpamMail** Folder and click **OK**.



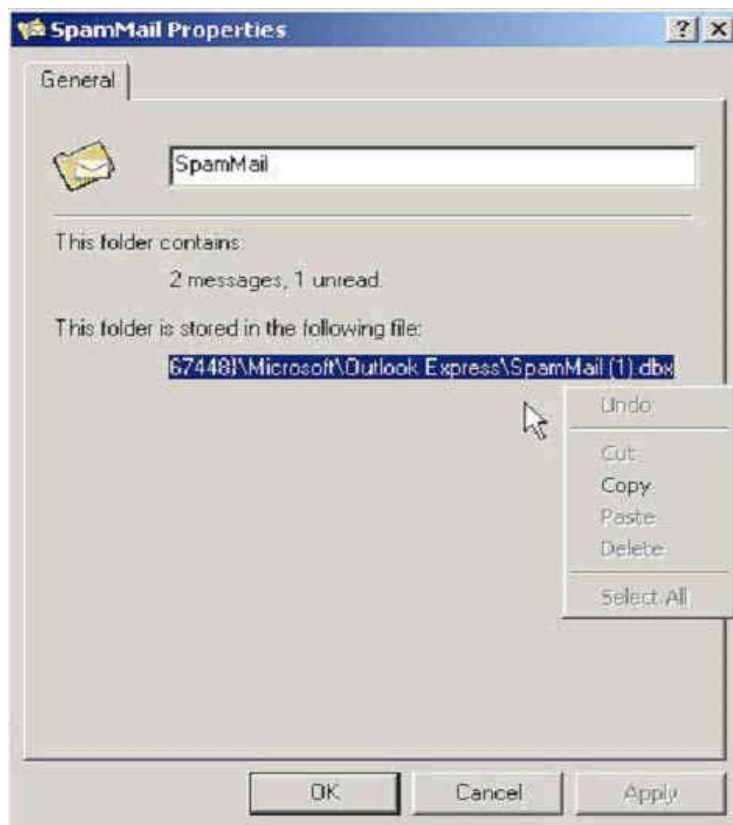
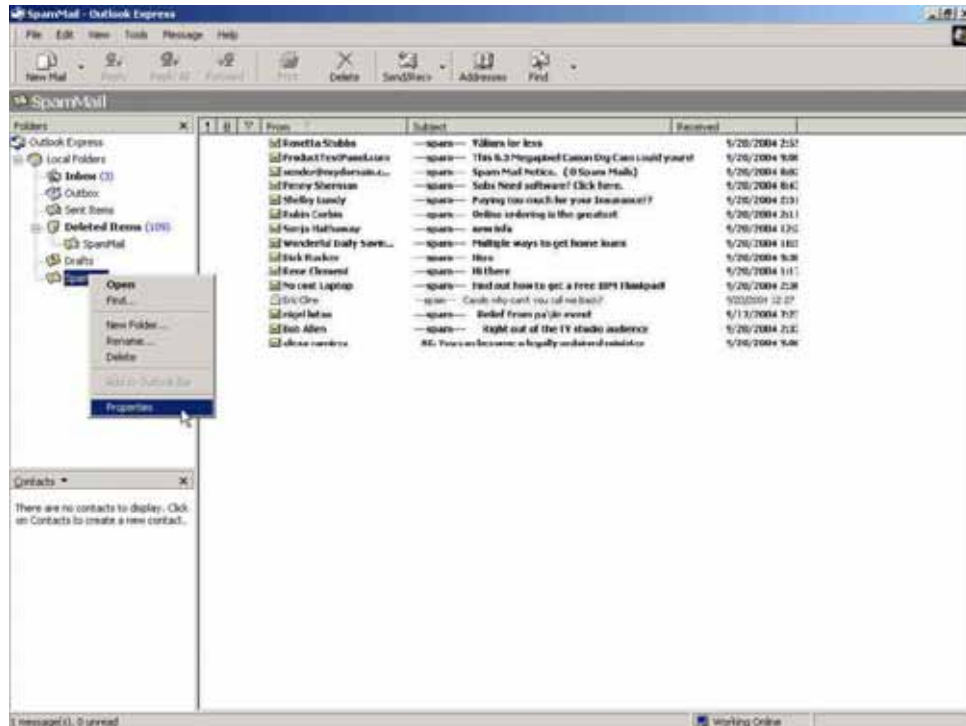
STEP 3 . Compress the SpamMail Folder in **Outlook Express** to shorten the data and upload to CS-1000 for training:

- Select **SpamMail** Folder
- Select **Compact** function in selection of the folder



STEP 4 . To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to CS-1000.

- Press the right key of the mouse in SpamMail file and select **Properties** function.
- Copy the file address in **SpamMail Properties** WebUI.



STEP 5 . Paste the route of copied from SpamMail file to the **Spam Mail for Training** field in **Training** function of **Anti-Spam**. And press **OK** to deliver this file to CS-1000 instantly and to learn the uploaded mail file as spam mail in the appointed time.

Training Database

Export Training Database

Download

Import Training Database

Browse...

Reset Training Database

Reset Database**Spam Mail for Training**

Import Spam Mail from Client

Browse...

Ham Mail for Training

Import Ham Mail from Client

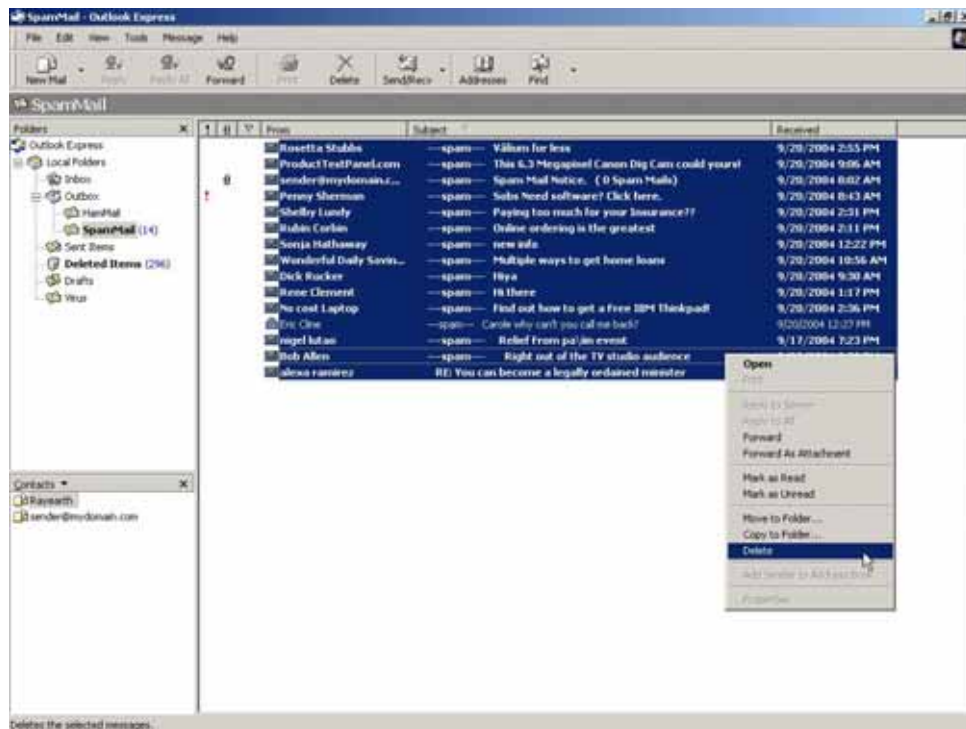
Browse...

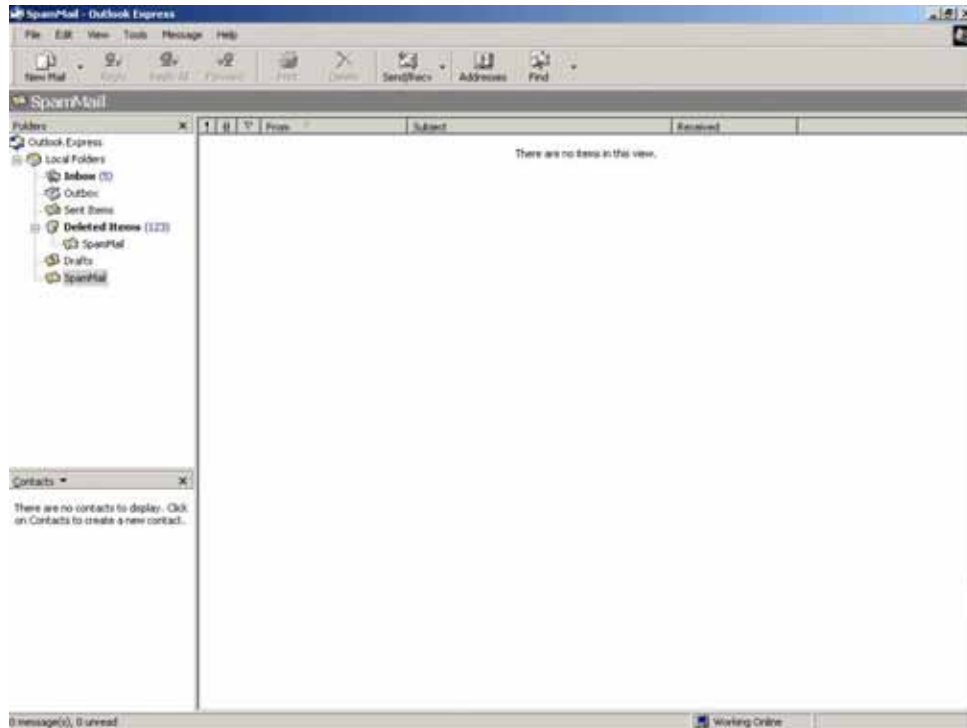
Note:

1. The training file that uploads to CS-1000 can be any data file and not restricted in its sub-name, but the file must be ACSII form.
2. When the training file of CS-1000 is Microsoft Office Outlook exporting file [.pst], it has to close Microsoft Office Outlook first to start Importing.

STEP 6 . Remove all of the mails in **SpamMail** File in **Outlook Express** so that new mails can be compressed and upload to CS-1000 to training directly next time.

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





3.5.2.6 Spam Mail

This item will show the top chart that represents the received and sent spam mail from recipient. In **Top Total Spam** report, you can choose to display the scanned mails that sent to **Internal Mail Server** or received from **External Mail Server**. It also can sort the mail according to **Recipient**, **Total Spam** and **Total Mail**.

No.	Recipient	Total Spam	Total Mail	Duration	Spam %
No spam mail in the External Mail Server					

3.5.3 Anti-Virus

CS-1000 built-in Clam virus scanning engine can protect your LAN network from being infected virus.

3.5.3.1 Setting

PLANET
Networking & Communication

Mail Security > Anti-Virus > Setting

Anti-Virus Setting

Virus Scan Engine: Disable

The Mail Server is placed in: ☐ Internal (LAN or DMZ) (Please set Mail Relay first) ☐ External (WAN)

Add the message to the subject line: (Max. 256 characters)

The latest update time: 2004/7/7 (Update virus definitions every ten minutes)

The newest version: 0.0

Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) Update NOW Test

Action of Infected Mail

Internal Mail Server:

☐ Delete the virus mail

☐ Deliver to the recipient

☐ Deliver a notification mail instead of the original virus mail

☐ Deliver the original virus mail

☐ Forward to: (ex: user@mydomain.com)

External Mail Server:

☐ Deliver to the recipient (Always enable)

☐ Deliver a notification mail instead of the original virus mail

☐ Deliver the original virus mail

OK Cancel

Definition:

Virus Scan Engine: Select **Clam** to enable Anti-virus function or Select **Disable** to disable it.

The Mail Server is placed in Internal (LAN or DMZ) or External (WAN): Select to choose the location of the mail server.

Add the message to the subject line: If the mail has been filtered as virus mail, CS-1000 will add a message in the mail's subject.

Update virus definitions immediately: Press **Update NOW** to update CS-1000 virus database.

Action of Infected Mail: When CS-1000 filters the infected mail, there are three kinds of actions for Internal Mail Server and one action for External Mail server to arrange the infected mail:

Delete the virus mail: If select this option, the virus mail will be deleted without any notification.

Deliver to the recipient: This action is available for Internal Mail Server and External Mail Server setting.

Deliver a notification mail instead of the original virus mail: Recipient will only receive a notification, and virus mail will be deleted.

Deliver the original virus mail: Recipient will receive the original virus mail, the virus will not be arranged, but CS-1000 will add a "VIRUS" message at the subject.

Forward to: You can configure CS-1000 to forward virus mail to a specific mail account; it will be easily to manage the infected mail.

3.5.3.2 Virus Mail

This item will show the top chart that represents the received and sent virus mail from recipient. In **Top Total Virus** report, you can choose to display the scanned mails that sent to **Internal Mail Server** or received from

External Mail Server. It also can sort the mail according to Recipient, Total Virus and Total Mail.

PLANET
Networking & Communication

Mail Security > Anti-Virus > Virus Mail

System
Interface
Policy Object
Policy
Mail Security
 Configure
 Anti-Spam
 Anti-Virus
 Setting
 Virus Mail

External

No.	Recipient	Total Virus	Total Mail	Duration	Virus %
No virus mail in the External Mail Server !					

3.6 IDP

CS-1000 can aim at abnormal traffic and packets content to inspect, alert, and handle by the obstructive, separateness, interference, or alarm to administrator, to prevent suspicious program invades the host. So when CS-1000 detects the attack behavior come from internal or external, it can provide the protection to network and obstruct to the attack behavior, let the network can still work normally and increase the information transmission security.

3.6.1 Setting

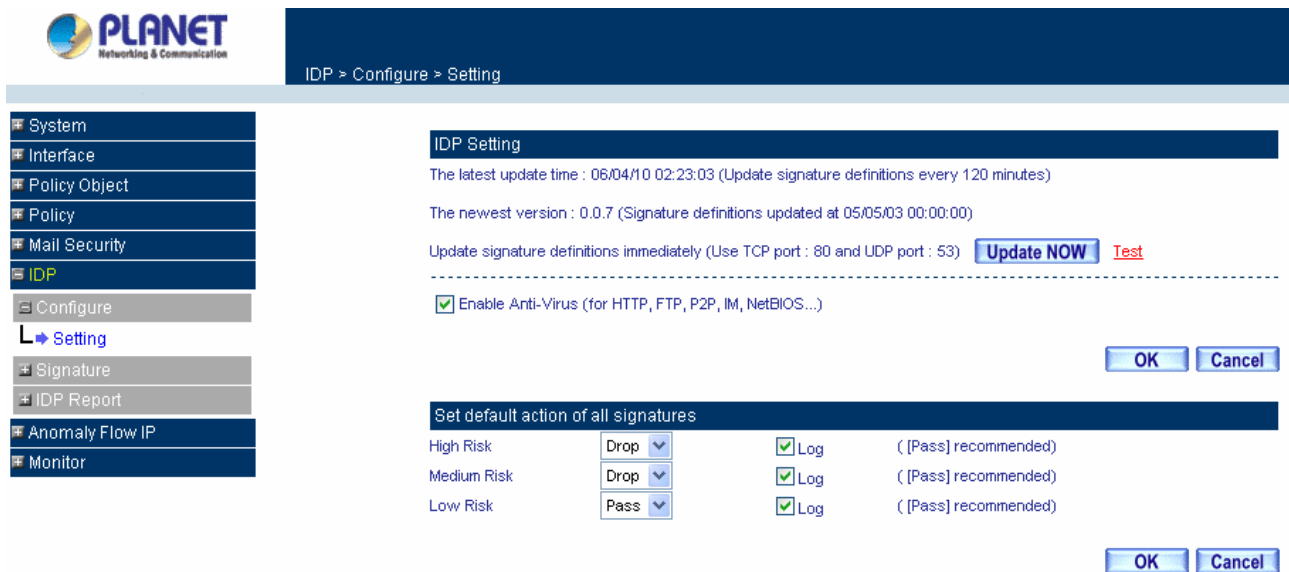
- It can update signature definitions for every 120 minutes. Or update signature definitions immediately. It will show the update time and version at the same time.
- It can detect virus to the file which have no encryption and compression.

Note: User can test if CS-1000 can connect to IDP server to update the signature definitions on internet by **Test** function.

Set default action of all signatures:

- According to attack behavior's threat to divide: **High Risk**, **Medium Risk**, and **Low Risk**. The different risk attack behavior can be handled by the pass, drop, and log action.
 - ◆ Add the following settings in this function:
 1. Select **Enable Anti-Virus** (Disable Anti-virus function will abate the IDP function in virus protection).
 2. Click **OK**.
 3. **High Risk**: Select drop and log function.
 4. **Medium Risk**: Select drop and log function.
 5. **Low Risk**: Select pass and log function.

6. Click **OK**.
7. Enable **IDP** function in policy.



The screenshot shows the PLANET Networking & Communication configuration interface. The breadcrumb trail is IDP > Configure > Setting. The left sidebar shows a tree view with 'IDP' selected, and 'Setting' is highlighted under the 'Configure' sub-menu. The main content area is titled 'IDP Setting' and contains the following information:

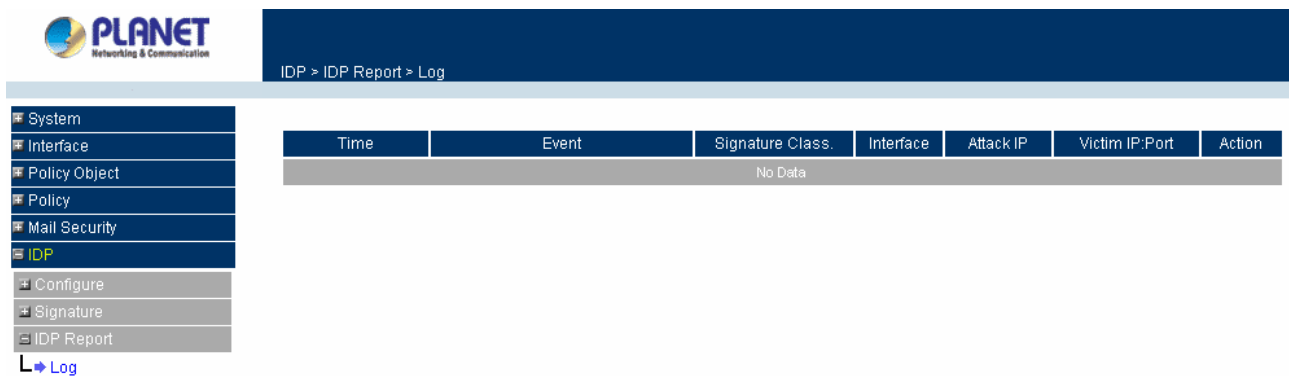
- The latest update time : 06/04/10 02:23:03 (Update signature definitions every 120 minutes)
- The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00)
- Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) with buttons for **Update NOW** and **Test**.
- A checkbox for **Enable Anti-Virus (for HTTP, FTP, P2P, IM, NetBIOS...)** is checked.
- Buttons for **OK** and **Cancel**.

Below this, there is a section titled 'Set default action of all signatures' with a table:

Set default action of all signatures			
High Risk	Drop	<input checked="" type="checkbox"/> Log	([Pass] recommended)
Medium Risk	Drop	<input checked="" type="checkbox"/> Log	([Pass] recommended)
Low Risk	Pass	<input checked="" type="checkbox"/> Log	([Pass] recommended)

Buttons for **OK** and **Cancel** are at the bottom right of this section.

- ◆ When the attack behavior matches the signature, CS-1000 will produce log as follows in **Log** function of **IDP Report**.



The screenshot shows the PLANET Networking & Communication configuration interface. The breadcrumb trail is IDP > IDP Report > Log. The left sidebar shows a tree view with 'IDP' selected, and 'Log' is highlighted under the 'IDP Report' sub-menu. The main content area displays a table with the following columns: Time, Event, Signature Class, Interface, Attack IP, Victim IP:Port, and Action. The table is currently empty, showing 'No Data'.

3.6.2 Signature

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

Anomaly:

Anomaly signature can allow user to define the signature, in order to detect and prevent the irregular attack behavior. Take **Syn Flood** as the example:

Definition:

Enable: Check to enable the protection for Syn Flood signature.

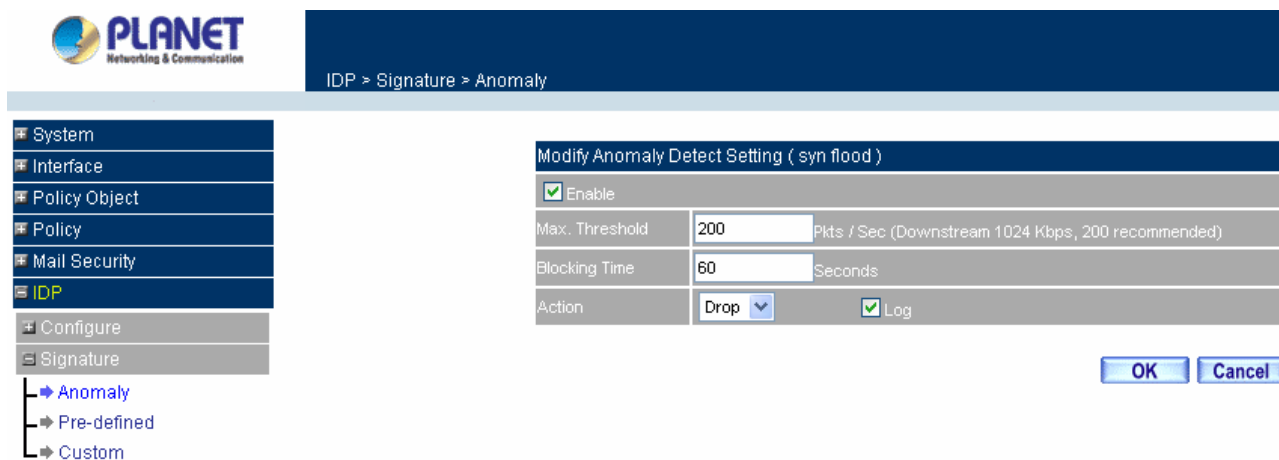
Max. Threshold ☐ **Pkts / Sec:** Configure the value to define the **Syn Flood** signature.

Blocking Time: Set up the timing to block the attacked connection. The function is available when the **Action** sets to **Drop**.

Action: When the packets match the signature, select **Pass** to pass the packets, or select **Drop** to discard

the packets.

Log: Check **Log** function to record the log in **IDP Report**.



The screenshot shows the PLANET web interface. The breadcrumb trail is 'IDP > Signature > Anomaly'. On the left, a navigation menu has 'IDP' expanded, showing 'Configure', 'Signature', and a sub-menu with 'Anomaly' (selected), 'Pre-defined', and 'Custom'. The main content area is titled 'Modify Anomaly Detect Setting (syn flood)'. It contains the following settings:

- ☒ Enable
- Max. Threshold: 200 Pkts / Sec (Downstream 1024 Kbps, 200 recommended)
- Blocking Time: 60 Seconds
- Action: Drop (dropdown menu) ☒ Log

At the bottom right are 'OK' and 'Cancel' buttons.

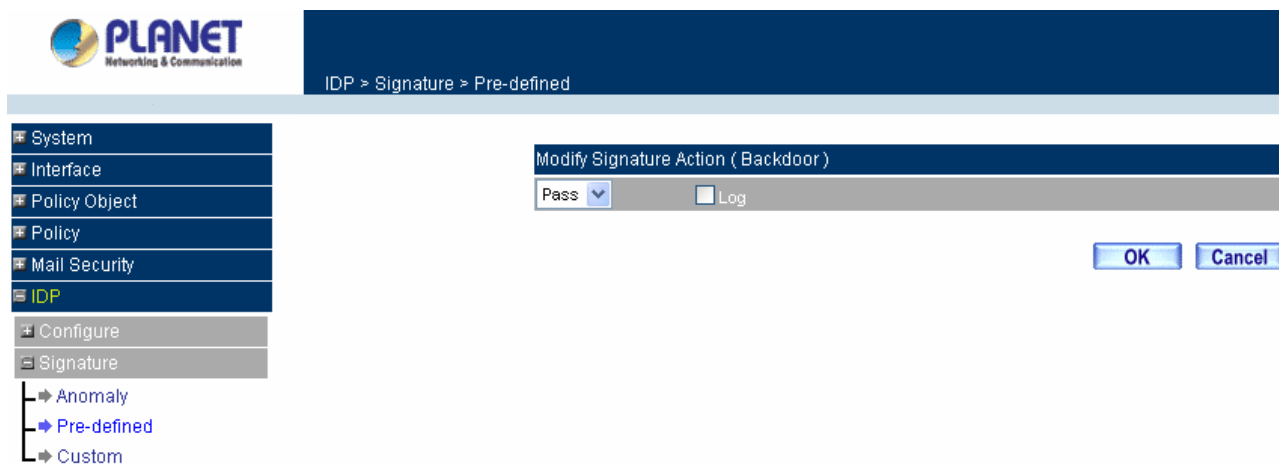
Pre-defined:

Pre-defined signatures can detect and prevent to intrusive pattern which can be discovered at present. These signatures can not be modified and deleted.

Definition:

Action: Select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check **Log** function to record the log in **IDP Report**.



The screenshot shows the PLANET web interface. The breadcrumb trail is 'IDP > Signature > Pre-defined'. On the left, the navigation menu has 'Pre-defined' selected under the 'IDP' > 'Signature' path. The main content area is titled 'Modify Signature Action (Backdoor)'. It contains the following settings:

- Pass (dropdown menu) ☐ Log

At the bottom right are 'OK' and 'Cancel' buttons.

Custom:

Custom signatures can allow user to create the signature according to their requirement, works to detect and prevent the internal and external attack behavior which are not including in **Pre-defined** signatures.

Definition:

Name: The System Manager can name the signature.

Protocol: Select the protocol which wants to be detected and prevented, it can be divided: TCP, UDP, ICMP and IP.

Source Port: Configure the port number that is used to attack the PC. (The range can be from 0 to 65535).

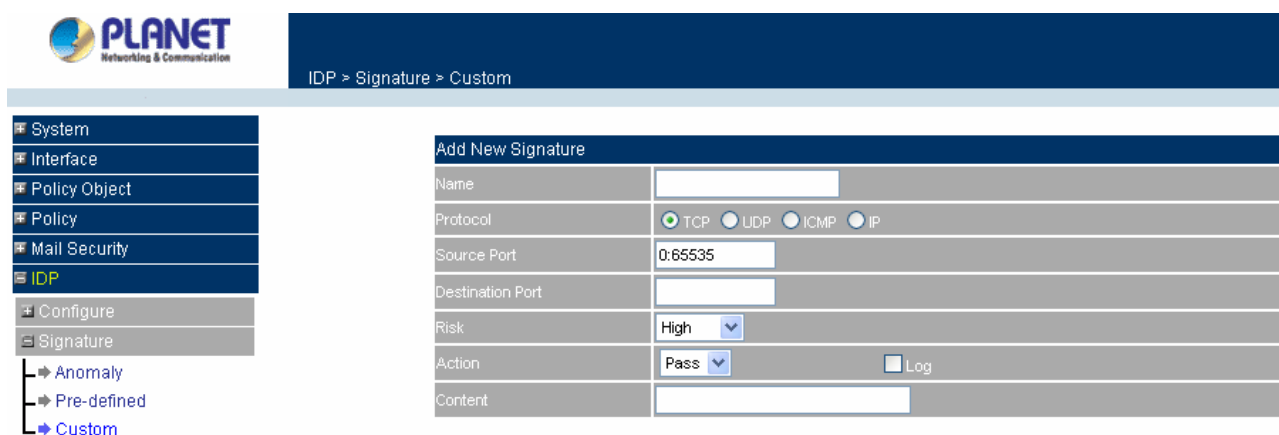
Destination Port: Configure the port number that the client PC is used to be attacked.

Risk: Define the threat about attack packets.

Action: Select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check **Log** function to record the log in **IDP Report**.

Content: Define the attack packets content.

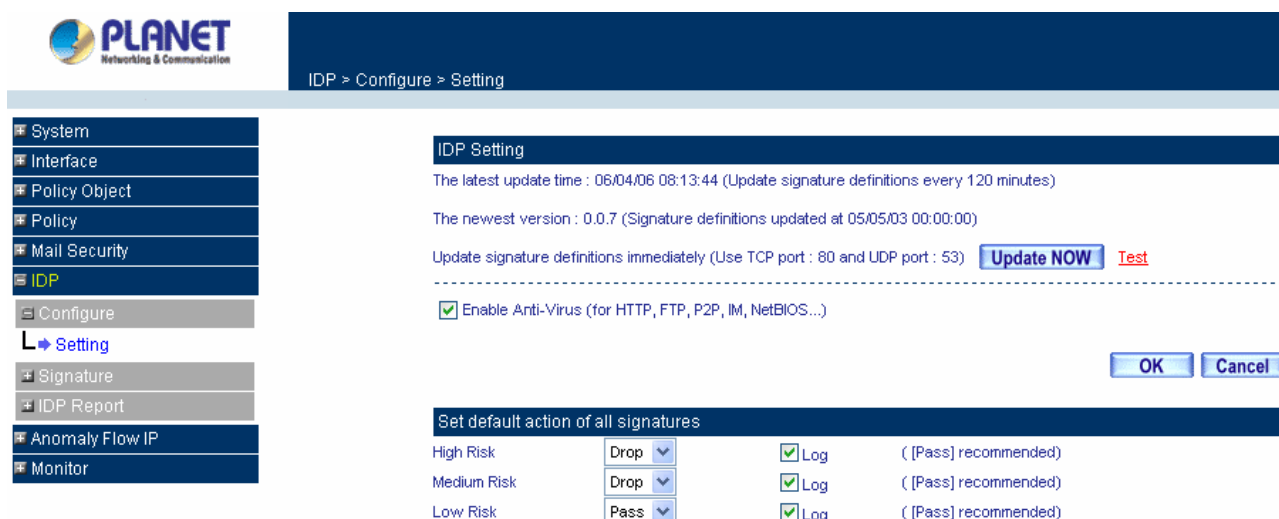


The screenshot shows the PLANET Networking & Communication web interface. The breadcrumb trail is "IDP > Signature > Custom". On the left, a navigation menu lists: System, Interface, Policy Object, Policy, Mail Security, IDP (selected), Configure, Signature, Anomaly, Pre-defined, and Custom. The main area is titled "Add New Signature" and contains the following fields:

- Name: [Empty text box]
- Protocol: Radio buttons for TCP (selected), UDP, ICMP, and IP.
- Source Port: [0:65535]
- Destination Port: [Empty text box]
- Risk: [High] (dropdown menu)
- Action: [Pass] (dropdown menu) and a checkbox for Log.
- Content: [Empty text box]

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

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



The screenshot shows the PLANET Networking & Communication web interface. The breadcrumb trail is "IDP > Configure > Setting". On the left, a navigation menu lists: System, Interface, Policy Object, Policy, Mail Security, IDP (selected), Configure, Setting (selected), Signature, IDP Report, Anomaly Flow IP, and Monitor. The main area is titled "IDP Setting" and contains the following information:

- The latest update time : 06/04/06 08:13:44 (Update signature definitions every 120 minutes)
- The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00)
- Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) [Update NOW] [Test]
- ☒ Enable Anti-Virus (for HTTP, FTP, P2P, IM, NetBIOS...)


At the bottom, there is a section titled "Set default action of all signatures" with the following table:

Risk Level	Action	Log	Recommendation
High Risk	Drop	<input checked="" type="checkbox"/> Log	([Pass] recommended)
Medium Risk	Drop	<input checked="" type="checkbox"/> Log	([Pass] recommended)
Low Risk	Pass	<input checked="" type="checkbox"/> Log	([Pass] recommended)

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

- Click **New Entry**.
- **Name:** Enter Software_Crack_Website.
- **Protocol:** Select TCP.
- **Source Port:** Enter 0:65535.
- **Destination Port:** Enter 80:80.
- **Risk:** Select High.
- **Action:** Select Drop and enable Log function.

- **Content:** Enter cracks.



IDP > Signature > Custom

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
 - Configure
 - Signature
 - Anomaly
 - Pre-defined
 - Custom

Add New Signature

Name: Software_Crack_Website

Protocol: ☒ TCP ☐ UDP ☐ ICMP ☐ IP

Source Port: 0:65535


Destination Port: 80:80

Risk: High

Action: Drop ☒ Log

Content: cracks

Click OK to finish the IDP setting.




IDP > Signature > Custom

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
 - Configure
 - Signature
 - Anomaly
 - Pre-defined
 - Custom

Name	Protocol	Src. Port	Dst. Port	Risk	Action	Log	Configure
Software_Crack_Website	TCP	0:65535	80:80	H	X	✓	Modify Remove

[New Entry](#)

STEP 3. Enter the following settings in **Outgoing Policy** to enable the **IDP** function:



Policy > Outgoing

- System
- Interface
- Policy Object
- Policy
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor

Comment:

Modify Policy

Source Address: Inside_Any

Destination Address: Outside_Any

Service: ANY

Schedule: None

Authentication User: None

Trunk: None

Action, WAN Port: PERMIT ALL

Traffic Log: ☐ Enable

Statistics: ☐ Enable

IDP: ☒ Enable

Content Blocking: ☐ Enable

MAX. Concurrent Sessions: 0 (0 means unlimited)

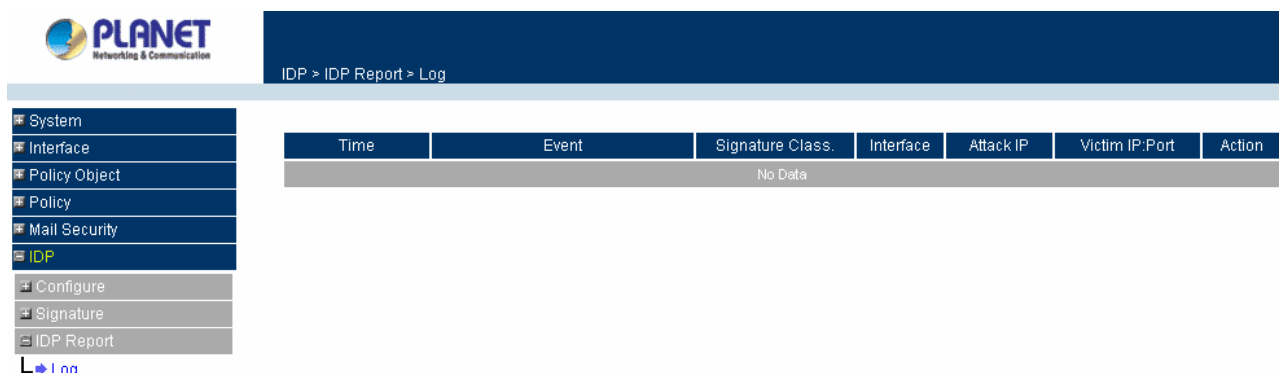
QoS: None

3.6.3 IDP Report

CS-1000 can make intrusion detection and prevention record to a Log report, and allow administrator to know

the network security status for the overall network.

STEP 1. In **Log** of **IDP Report** function, it will display the situation about intrusion detection and prevention of CS-1000.



Icon Definition:

1. Action:

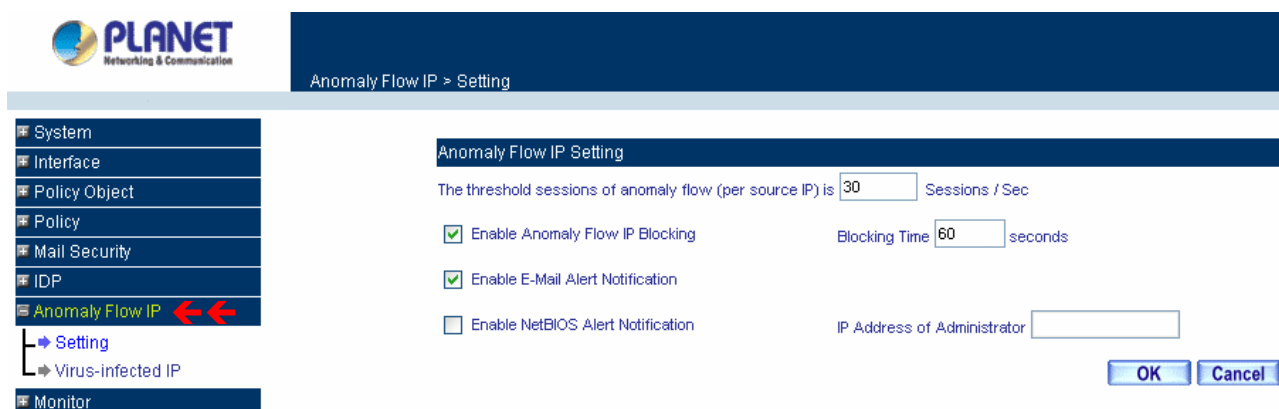
Pass	Drpo

2. Risk:

High Risk	Medium Risk	Low Risk

3.7 Anomaly Flow IP

The Administrator can enable the device's auto detect functions for Anomaly Flow IP attacking the local network. When abnormal conditions occur, CS-1000 will send an e-mail alert to notify the Administrator, and also display warning messages in the Virus-infected IP window.



Anomaly Flow IP Settings

- **Enable Anomaly Flow IP Blocking:** Select this option to enable the Anomaly Flow IP blocking function. Once the Anomaly Flow IP attacked is detected, it will block the

connection for user-drefined blocking time.

- **Enable E-mail Alert Notification:** When Anomaly Flow IP attacked is detected, send alert e-mail to administrator by using e-mail address defined on System -> Setting.
- **Enable NetBIOS Alert Notification:** When Anomaly Flow IP attacked is detected, send alert message to administrator by using "Net send" command.

After enabling the needed options, click OK to activate the changes.

3.8 Monitor

CS-1000 provides varied of information that can be used to check the status.

3.8.1 Log

The Multi-Homing Security Gateway supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the Multi-Homing Security Gateway.

What is Log?

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

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.

3.8.1.1 Traffic

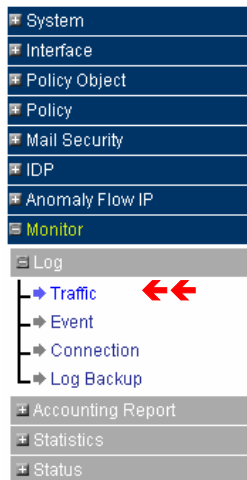
The Administrator queries the Multi-Homing Security Gateway for information, such as source address, destination address, start time, and Protocol port of all connections.

Entering the Traffic Log window

- Step 1. Click the **Traffic** option under **Log** menu to enter the Traffic Log window.



Monitor > Log > Traffic



Apr 10 04:13:49

[Next](#)

Time	Source	Destination	Protocol	Port	Disposition
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1160 => 80	✓
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1159 => 80	✓
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1158 => 80	✓
Apr 10 04:12:45	192.168.10.3	192.168.10.1	TCP	1157 => 80	✓
Apr 10 04:12:45	192.168.10.3	192.168.10.1	TCP	1156 => 80	✓
Apr 10 04:11:14	192.168.10.3	192.168.10.1	TCP	1155 => 80	✓
Apr 10 04:11:14	192.168.10.3	192.168.10.1	TCP	1154 => 80	✓
Apr 10 04:10:29	192.168.10.3	192.168.10.1	TCP	1153 => 80	✓
Apr 10 04:10:11	192.168.10.3	192.168.10.1	TCP	1152 => 80	✓
Apr 10 04:10:11	192.168.10.3	192.168.10.1	TCP	1151 => 80	✓
Apr 10 04:09:21	192.168.10.3	192.168.10.1	TCP	1150 => 80	✓
Apr 10 04:09:20	192.168.10.3	192.168.10.1	TCP	1149 => 80	✓
Apr 10 04:06:45	192.168.10.3	192.168.10.1	TCP	1148 => 80	✓
Apr 10 04:06:44	192.168.10.3	192.168.10.1	TCP	1147 => 80	✓
Apr 10 04:05:37	192.168.10.3	192.168.10.1	TCP	1146 => 80	✓
Apr 10 04:05:37	192.168.10.3	192.168.10.1	TCP	1145 => 80	✓
Apr 10 04:04:49	192.168.10.3	192.168.10.1	TCP	1144 => 80	✓
Apr 10 04:02:12	192.168.10.3	192.168.10.1	TCP	1144 => 80	✓

Clear Logs

Download Logs

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

- **Time:** The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol:** Protocol type of the specific connection.
- **Port:** Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

Clearing the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.

The screenshot shows the Planet Networking & Communication Multi-Homing Security Gateway interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor, Log, Accounting Report, Statistics, and Status. The 'Log' item is expanded, showing sub-items: Traffic, Event, Connection, and Log Backup. The main area displays the 'Monitor > Log > Traffic' window. At the top right, there is a date/time selector set to 'Apr 10 04:13:49' and a 'Next' link. Below this is a table of traffic logs. A 'Microsoft Internet Explorer' dialog box is overlaid on the table, asking 'Do you really want to clean?' with 'OK' and 'Cancel' buttons. At the bottom of the window, there are 'Clear Logs' and 'Download Logs' buttons.

Time	Source	Destination	Protocol	Port	Disposition
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1160 => 80	✓
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1159 => 80	✓
Apr 10 04:13:49	192.168.10.3	192.168.10.1	TCP	1158 => 80	✓
Apr 10 04:12:45	192.168.10.3	192.168.10.1	TCP	1157 => 80	✓
Apr 10 04:12:45	192.168.10.3	192.168.10.1	TCP	1156 => 80	✓
Apr 10 04:11:14	192.168.10.3	192.168.10.1	TCP	1155 => 80	✓
Apr 10 04:11:14	192.168.10.3	192.168.10.1	TCP	1154 => 80	✓
Apr 10 04:10:29	192.168.10.3	192.168.10.1	TCP	1153 => 80	✓
Apr 10 04:10:11	192.168.10.3	192.168.10.1	TCP	1152 => 80	✓
Apr 10 04:10:11	192.168.10.3	192.168.10.1	TCP	1151 => 80	✓
Apr 10 04:09:21	192.168.10.3	192.168.10.1	TCP	1150 => 80	✓
Apr 10 04:09:20	192.168.10.3	192.168.10.1	TCP	1149 => 80	✓
Apr 10 04:06:45	192.168.10.3	192.168.10.1	TCP	1148 => 80	✓
Apr 10 04:06:44	192.168.10.3	192.168.10.1	TCP	1147 => 80	✓
Apr 10 04:05:37	192.168.10.3	192.168.10.1	TCP	1146 => 80	✓
Apr 10 04:05:37	192.168.10.3	192.168.10.1	TCP	1145 => 80	✓
Apr 10 04:04:49	192.168.10.3	192.168.10.1	TCP	1144 => 80	✓
Apr 10 04:02:12	192.168.10.3	192.168.10.1	TCP	1144 => 80	✓

3.8.1.2 Event

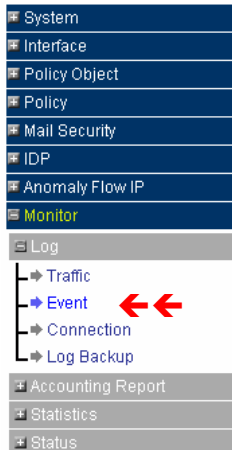
When the Multi-Homing Security Gateway WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.



Monitor > Log > Event



Apr 10 04:02:12

[Next](#)

Time	Event
Apr 10 04:02:12	admin Export [Blacklist] (Export File To Client) from 192.168.10.3
Apr 10 04:01:03	admin Add [Blacklist] (Blacklist Address: hacker Direction: From Training: Disable) from 192.168.10.3
Apr 10 03:55:13	admin Export [Whitelist] (Export File To Client) from 192.168.10.3
Apr 10 03:55:11	admin Add [Whitelist] (Whitelist Address: planet Direction: From Training: Disable) from 192.168.10.3
Apr 10 03:54:21	admin Remove [Whitelist] (Whitelist Address: Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:54:18	admin Remove [Whitelist] (Whitelist Address: hotmail Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:52:57	admin Remove [Spam Rule] (Rule Name : test) from 192.168.10.3
Apr 10 03:52:19	admin Add [Spam Rule] (Rule Name : test) from 192.168.10.3
Apr 10 03:48:57	admin Remove [Spam Rule] (Rule Name : test) from 192.168.10.3
Apr 10 03:39:54	admin Remove [Mail Relay] (Subnet / Mask: 204.22.193.23 / 255.255.255.0) from 192.168.10.3
Apr 10 03:36:46	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.10.3
Apr 10 03:34:19	admin Modify [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.10.3
Apr 10 03:33:34	(null) Add [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.10.3
Apr 10 03:12:27	(null) Add [Multiple Subnet] (Internal IP : 192.168.2.1 Netmask : 255.255.255.0) from 192.168.10.3
Apr 10 03:04:31	(null) WAN1 is disconnected
Apr 10 02:42:31	user admin [Login success] from 192.168.10.3
Apr 9 23:56:30	(null) WAN1 is connected
Apr 9 23:56:00	(null) WAN1 is disconnected

Clear Logs

Download Logs

Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

Clearing the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.

PLANET
Networking & Communication

Monitor > Log > Event

Apr 10 04:02:12 [Next](#)

Time	Event
Apr 10 04:02:12	admin Export [Blacklist] (Export File To Client) from 192.168.10.3
Apr 10 04:01:03	admin Add [Blacklist] (Blacklist Address: hacker Direction: From Training: Disable) from 192.168.10.3
Apr 10 03:55:13	admin Export [Whitelist] (Export File To Client) from 192.168.10.3
Apr 10 03:55:11	admin Add [Whitelist] (Whitelist Address: hacker Direction: From Training: Disable) from 192.168.10.3
Apr 10 03:54:21	admin Add [Whitelist] (Whitelist Address: hacker Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:54:18	admin Add [Whitelist] (Whitelist Address: hacker Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:52:57	admin Add [Whitelist] (Whitelist Address: hacker Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:52:19	admin Add [Whitelist] (Whitelist Address: hacker Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:48:57	admin Add [Whitelist] (Whitelist Address: hacker Direction: To Training: Disable) from 192.168.10.3
Apr 10 03:39:54	admin Remove [Mail Relay] (Subnet / Mask: 204.22.193.23 / 255.255.255.0) from 192.168.10.3
Apr 10 03:36:46	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.10.3
Apr 10 03:34:19	admin Modify [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.10.3
Apr 10 03:33:34	(null) Add [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.10.3
Apr 10 03:12:27	(null) Add [Multiple Subnet] (Internal IP : 192.168.2.1 Netmask : 255.255.255.0) from 192.168.10.3
Apr 10 03:04:31	(null) WAN1 is disconnected
Apr 10 02:42:31	user admin [Login success] from 192.168.10.3
Apr 9 23:56:30	(null) WAN1 is connected
Apr 9 23:56:00	(null) WAN1 is disconnected

[Clear Logs](#) [Download Logs](#)

3.8.1.3 Connection

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.

PLANET
Networking & Communication

Monitor > Log > Connection

Jan 1 00:02:49 [Next](#)

Time	Connection Log
Jan 1 00:02:49	including NAT-Traversal patch (Version 0.6)
Jan 1 01:12:17	added connection description "Site_B_1"
Jan 1 01:12:24	listening for IKE messages
Jan 1 01:12:24	adding interface ipsec0/eth1 192.168.99.92
Jan 1 01:12:24	adding interface ipsec0/eth1 192.168.99.92:4500
Jan 1 01:12:27	"Site_B_1" #1: initiating Main Mode
Jan 1 01:12:37	"Site_B_1" #1: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Jan 1 01:12:50	"Site_B_1": unroute-host command exited with status 7
Jan 1 01:12:51	"Site_B_1": deleting connection
Jan 1 01:12:54	added connection description "Site_B_1"
Jan 1 01:13:01	listening for IKE messages
Jan 1 01:13:01	forgetting secrets
Jan 1 01:13:05	"Site_B_1" #2: initiating Main Mode
Jan 1 01:13:16	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first IKE message
Jan 1 01:13:53	"Site_B_1": terminating SAs using this connection
Jan 1 01:13:55	"Site_B_1": unroute-host command exited with status 7
Jan 1 01:13:55	"Site_B_1": deleting connection
Jan 1 01:14:08	added connection description "Site_B_1"

[Clear Logs](#) [Download Logs](#)

Definition:

Time: The start and end time of connection.

Connection Log: Event description during connection.

Download Logs

- Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.
- Step 2. In Connection Log window, click the **Download Logs** button.
- Step 3. In the Download Logs window, save the logs to the specified location.

Clear Logs

- Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.
- Step 2. In Connection Log window, click the **Clear Logs** button.
- Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.

The screenshot shows the Planet Network & Communication software interface. The left sidebar contains a menu with options: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor, Log, Traffic, Event, Connection, Log Backup, Accounting Report, Statistics, and Status. The 'Log' option is selected, and the 'Connection Log' window is displayed. The window shows a table of connection logs with columns for Time and Connection Log. A dialog box titled 'Microsoft Internet Explorer' is overlaid on the table, asking 'Do you really want to clean?' with 'OK' and 'Cancel' buttons. Below the table, there are two buttons: 'Clear Logs' and 'Download Logs'.

Time	Connection Log
Jan 1 00:02:49	including NAT-Traversal patch (Version 0.6)
Jan 1 01:12:17	added connection description "Site_B_1"
Jan 1 01:12:24	listening for IKE messages
Jan 1 01:12:24	adding interface ipsec0/eth1 192.168.99.92
Jan 1 01:12:24	adding interface ipsec0/eth1 192.168.99.92
Jan 1 01:12:27	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:12:37	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:12:50	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:12:51	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:12:54	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:13:01	listening for IKE messages
Jan 1 01:13:01	forgetting secrets
Jan 1 01:13:05	"Site_B_1" #2: initiating Main Mode
Jan 1 01:13:16	"Site_B_1" #2: max number of retransmissions (0) reached STATE_MAIN_I1. No acceptable response to our first
Jan 1 01:13:53	"Site_B_1" #2: terminating SAs using this connection
Jan 1 01:13:55	"Site_B_1" #2: unroute-host command exited with status 7
Jan 1 01:13:55	"Site_B_1" #2: deleting connection
Jan 1 01:14:08	added connection description "Site_B_1"

3.8.1.4 Log Backup

Click **Log** → **Log Backup**.

PLANET
Networking & Communication

Monitor > Log > Log Backup

System
Interface
Policy Object
Policy
Mail Security
IDP
Anomaly Flow IP
Monitor
Log
 Traffic
 Event
 Connection
 Log Backup

Log Mail Configuration

☐ Enable Log Mail Support

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

You must enable the E-mail Alarm

Syslog Setting

☐ Enable Syslog Messages

Syslog Host IP Address (ex: 192.168.1.61)

Syslog Host Port (ex: 514)

OK Cancel

Log Mail Configuration: When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

NOTE: Before enabling this function, you have to configure E-mail Settings in System -> Settings.

Syslog Settings: If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

NOTE: To restart Connection Log, click the **Refresh** button on the right hand side in Log window.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

- Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.
- Step 2. Go to **Log →Log Backup**. Check **enable Log Mail Support**. Click **OK**.

Syslog Settings/Enable Syslog Message

- Step 1. Check to enable **Syslog Message**. Enter the Host IP Address and Host Port number to send out message to syslog server.
- Step 2. Click **OK**.

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The top navigation bar includes the Planet logo and the text 'Monitoring & Communication'. Below this, a breadcrumb trail reads 'Monitor > Log > Log Backup'. On the left, a sidebar menu lists various system components: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor, and Log. The 'Log' menu item is expanded, showing sub-items: Traffic, Event, Connection, and Log Backup. The main content area is titled 'Log Mail Configuration' and 'Syslog Setting'. Under 'Log Mail Configuration', there is a checkbox for 'Enable Log Mail Support' which is currently unchecked. Below this checkbox, a note states: 'When Log Full (300Kbytes), Multi-Homing Security Gateway Appliance sends Log. You must enable the E-mail Alarm'. Under 'Syslog Setting', there is a checkbox for 'Enable Syslog Messages' which is checked. Below this, there are two input fields: 'Syslog Host IP Address' with the value '192.168.1.10' and a hint '(ex: 192.168.1.61)', and 'Syslog Host Port' with the value '514' and a hint '(ex: 514)'. At the bottom right of the configuration area, there are 'OK' and 'Cancel' buttons.

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG → Log Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG → Log Backup**. Uncheck to disable Settings Message. Click **OK**.

3.8.2 Accounting Report

Accounting Report can be divided into three parts, **Setting**, **Outbound** and **Inbound**.

3.8.2.1 Setting

Select **Setting** to configure what type of Accounting Report will be logged at CS-1000. There are three types of report can be select: **Source IP**, **Destination IP** and **Service**.

Outbound Accounting Report: the statistics of the downstream and upstream for the LAN, WAN and all kinds of communication services.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.


Inbound Accounting Report: the statistics of downstream and upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN host connects to LAN host via CS-1000.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service for all the user's IP that passes through CS-1000.



Monitor > Accounting Report > Setting

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor**
- Log
- Accounting Report
 - Setting
 - OutBound
 - InBound

Accounting Report Setting

Outbound Accounting Report

☒ Source IP

☒ Destination IP

☒ Service

Inbound Accounting Report

☒ Source IP


☒ Destination IP

☒ Service

OK Cancel

3.8.2.2 Outbound

Click the **Accounting Report** function, and then select **Outbound**. There are three options for outbound accounting report: Source IP, Destination IP and Services.



Monitor > Accounting Report > OutBound

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor**
- Log
- Accounting Report
 - Setting
 - OutBound** ←←
 - InBound

Top: 1 - 2


Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
Total Traffic		3.3 MB		327.8 KB		Reporting time Mon Apr 10 04:23:45 2006			

[Reset Counters](#)

Outbound Source IP Accounting Report

Pull down the menu and select **Source IP** to show the outbound source IP accounting report.



Monitor > Accounting Report > OutBound

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor**
- Log
- Accounting Report
 - Setting
 - OutBound**
 - InBound

Top: 1 - 2

Starting Time : Thu Apr 6 11:16:10 2006

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
Total Traffic		3.3 MB		327.8 KB		Reporting time Mon Apr 10 04:23:45 2006			

[Reset Counters](#)

When LAN users connect to WAN service server through CS-1000, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The LAN user's IP address connects to CS-1000 to access WAN service server.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Reset Counters: Click **Reset Counters** button to refresh Accounting Report.

Outbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the outbound destination IP accounting report.

Planet Networking & Communication

Monitor > Accounting Report > OutBound

Top: 1 - 1

Starting Time : Thu Apr 6 11:16:10 2006

No.	Destination IP	Downstream	Upstream	First Packet	Last Packet	Duration	Action
1	203.128.173.176	64.0 B 100.0%	46.0 B 100.0%	04/07 02:07:13	04/07 02:07:13	00:00:00	Remove
Total Traffic		54.0 B	46.0 B	Reporting time Sun Apr 9 02:38:22 2006			

Reset Counters

When LAN user connect to WAN service server through CS-1000, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Destination IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The WAN Server's IP address.

Downstream: The percentage of downstream and the statistic value of the connection from LAN user to WAN server.

Upstream: The percentage of upstream and the statistic value of the connection from WAN server to LAN user.

First Packet: The time record of the first packet that was sent to LAN user from WAN service server.

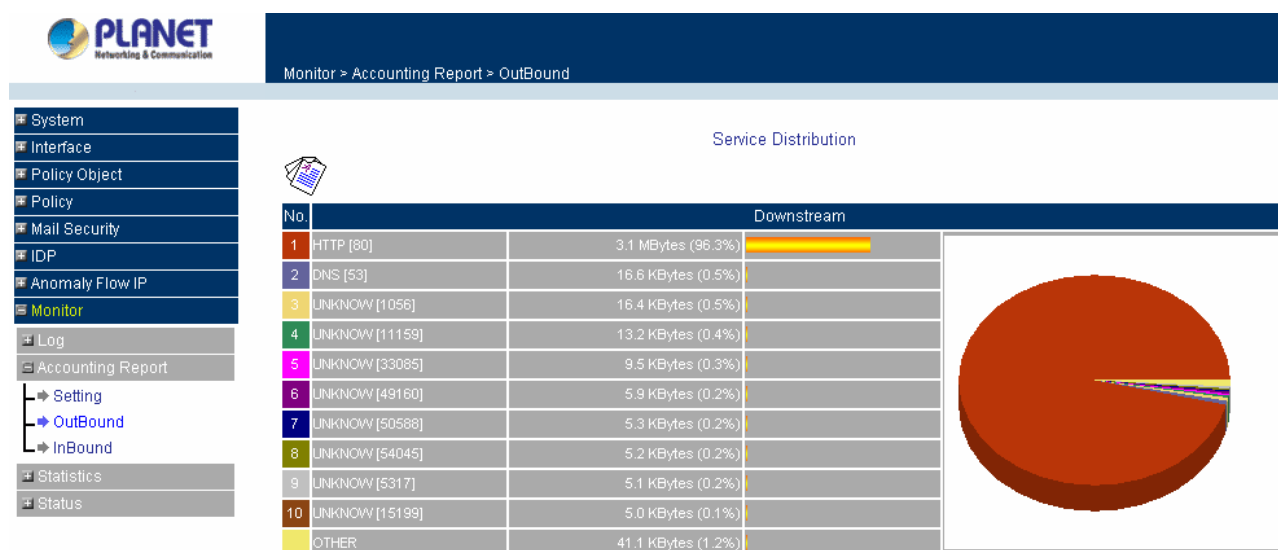
Last Packet: The time record of the last packet sent from LAN user and received by the WAN server

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Outbound Service Accounting Report

Pull down the menu and select **Service** to show the outbound service accounting report.



When LAN users connect to WAN Service Server through CS-1000, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when LAN users connect to WAN service server through CS-1000. **(Port)** indicates the protocol port number.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user

Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from LAN user to WAN service server.

NOTE: To correctly display the pizza chart, please install the latest java VM for <http://www.java.com>.

3.8.2.3 Inbound

Click the **Accounting Report** function, and then select **Inbound**. There are three options for Inbound accounting report: Source IP, Destination IP and Service.

The screenshot shows the Planet Security Gateway web interface. The left sidebar contains a menu with options: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor (highlighted), Log, Accounting Report, Setting, OutBound, InBound (highlighted with red arrows), and Statistics. The main content area displays the 'Monitor > Accounting Report > InBound' report. At the top, there is a 'Top: 1 - 6' dropdown and a 'Starting Time : Thu Apr 6 11:16:10 2006' timestamp. Below this is a table with columns: No., Source IP, Upstream, Downstream, First Packet, Last Packet, Duration, and Action. The table contains 6 rows of data, each with a 'Remove' button. At the bottom of the table, it shows 'Total Traffic' as 13.6 MB Upstream and 213.0 KB Downstream. A 'Reset Counters' button is located at the bottom right.

No.	Source IP	Upstream	Downstream	First Packet	Last Packet	Duration	Action
1	211.75.117.114	13.6 MB 100.0%	211.0 KB 99.1%	04/07 12:43:10	04/07 13:10:23	00:27:13	Remove
2	82.226.135.163	1.0 KB 0.0%	675.0 B 0.3%	04/08 06:46:30	04/08 13:29:13	06:42:43	Remove
3	67.78.0.138	935.0 B 0.0%	655.0 B 0.3%	04/07 17:11:59	04/08 06:07:30	12:55:31	Remove
4	83.19.250.74	477.0 B 0.0%	336.0 B 0.2%	04/07 14:37:26	04/07 14:37:32	00:00:06	Remove
5	67.71.33.201	467.0 B 0.0%	284.0 B 0.1%	04/08 13:03:05	04/08 13:03:06	00:00:01	Remove
6	80.51.174.70	44.0 B 0.0%	88.0 B 0.0%	04/08 13:11:28	04/08 13:11:29	00:00:01	Remove
Total Traffic		13.6 MB	213.0 KB	Reporting time Mon Apr 10 04:26:07 2006			

Inbound Source IP Accounting Report

Pull down the menu and select **Source IP** to show the inbound source IP accounting report.

This screenshot is identical to the one above, showing the 'Monitor > Accounting Report > InBound' report with the same table of data and interface elements.

When WAN users connect to LAN service server through CS-1000, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The IP address used by WAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from LAN host to WAN host via CS-1000.

Upstream: The percentage of Upstream and the statistic value of the connection from WAN host to LAN host via CS-1000.

First Packet: The time record of the first packet that was sent from WAN host to LAN host.

Last Packet: The time record of the last packet that sent from WAN host to LAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from WAN host to LAN host.

Inbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the inbound destination IP accounting report.

The screenshot shows the PLANET Monitoring & Communication software interface. On the left is a navigation menu with options: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor (highlighted), Log, Accounting Report, Setting, OutBound, and InBound. The main area displays the 'Monitor > Accounting Report > InBound' report. At the top right, it says 'Top: 1 - 1' and 'Starting Time : Thu Apr 6 11:16:10 2006'. Below this is a table with columns: No., Destination IP, Upstream, Downstream, First Packet, Last Packet, Duration, and Action. The table contains one data row for destination IP 192.168.10.2 and a summary row for 'Total Traffic'. A 'Remove' button is next to the first row, and a 'Reset Counters' button is at the bottom right.

No.	Destination IP	Upstream	Downstream	First Packet	Last Packet	Duration	Action
1	192.168.10.2	13.6 MB	213.0 KB	04/07 12:43:10	04/08 13:29:13	10:00:46:03	Remove
Total Traffic		13.6 MB	213.0 KB	Reporting time Mon Apr 10 04:27:39 2006			

When WAN host connect to LAN through CS-1000, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The IP address used by LAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS-1000.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-1000.

First Packet: The time record of the first packet that was sent from LAN host to WAN host.

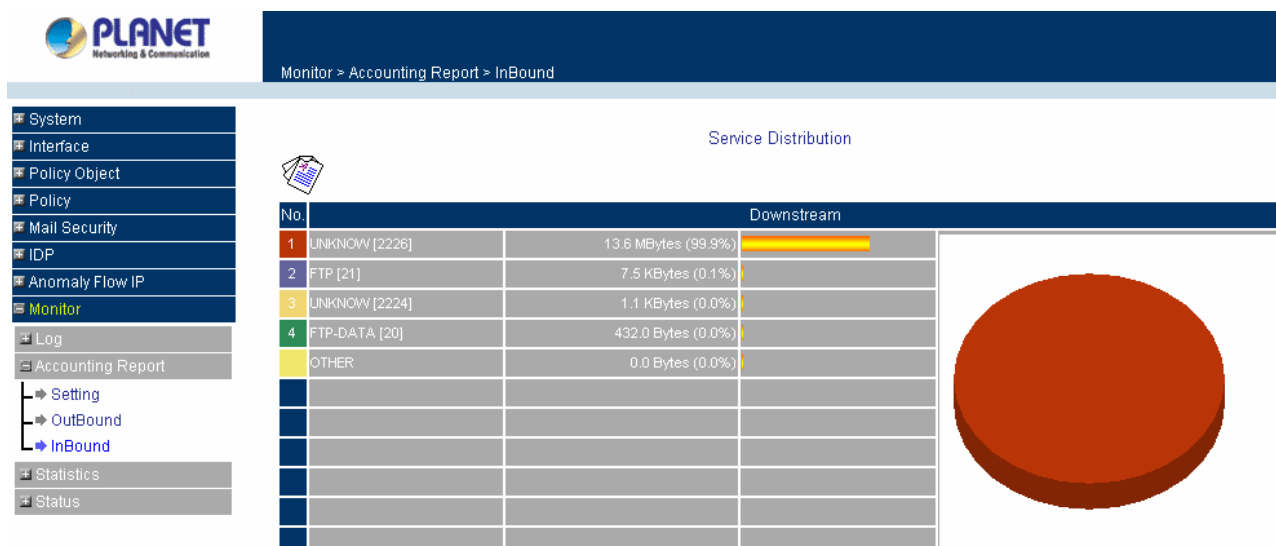
Last Packet: The time record of the last packet that sent from LAN host to WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from LAN host to WAN host.

Inbound Service Accounting Report

Pull down the menu and select **Service** to show the inbound service accounting report.



When WAN host connect to LAN host through CS-1000, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when WAN host connect to LAN host through CS-1000. (Port) indicates the protocol port number.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS1000.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-1000.

First Packet: The time record of the first packet that was sent to LAN host from WAN host.

Last Packet: The time record of the last packet sent to LAN host from WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-1000 will record the sum of upstream/downstream packets from WAN host to LAN host.

NOTE: To correctly display the pizza chart, please install the latest java VM for <http://www.java.com>.

3.8.3 Statistic

In this chapter, the Administrator queries the Multi-Homing Security Gateway for statistics of packets and data which passes across the Multi-Homing Security Gateway. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the Multi-Homing Security Gateway by control policies

setup by the Administrator.

How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to manage networks.

How to apply WAN Statistics

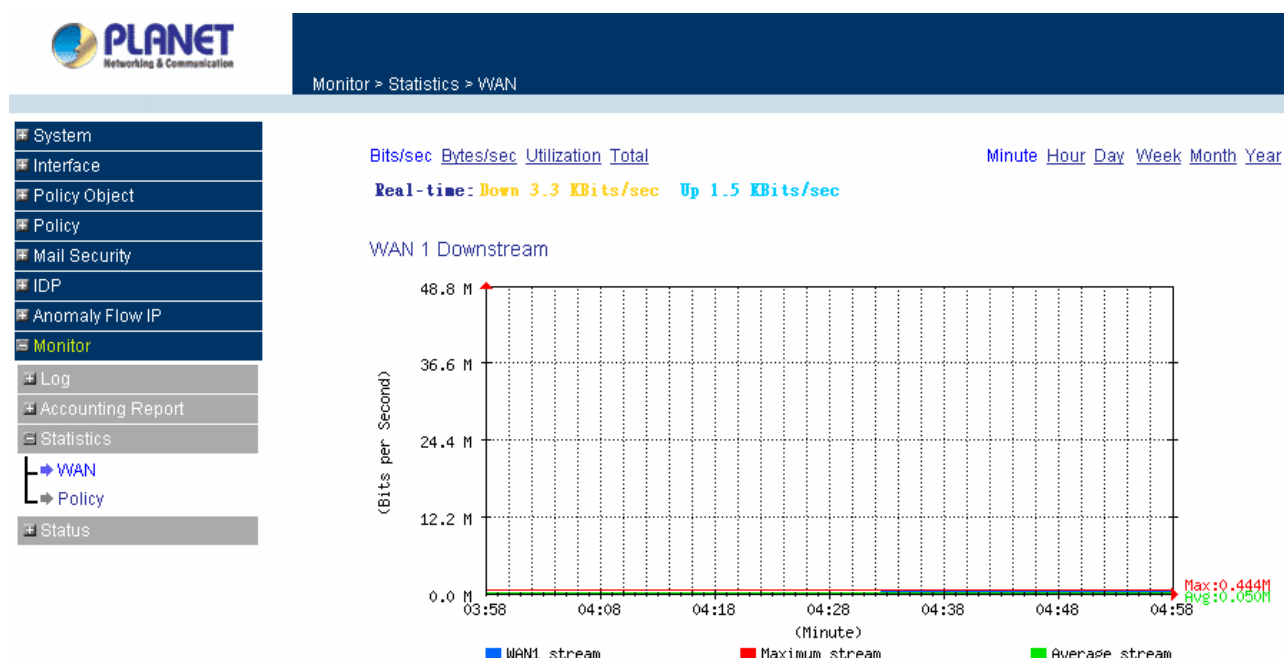
The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics. In this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

The administrator needs to go to the Policy to set the network IP of the statistics. By the WAN statistics you can obtain the status of the network.

3.8.3.1 WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN.

Step 2. The WAN Statistics will be displayed. It displays statistics of WAN network connections (downstream and upstream as well) in a total amount by minute (60 minutes), hour (24 hours), day (30 days), Month and Year. Select the time units (minute, hour, day, month or year) of the graph.



Y-Coordinate: Four options are available: Total, Bits/sec, Bytes/sec, and Utilization.

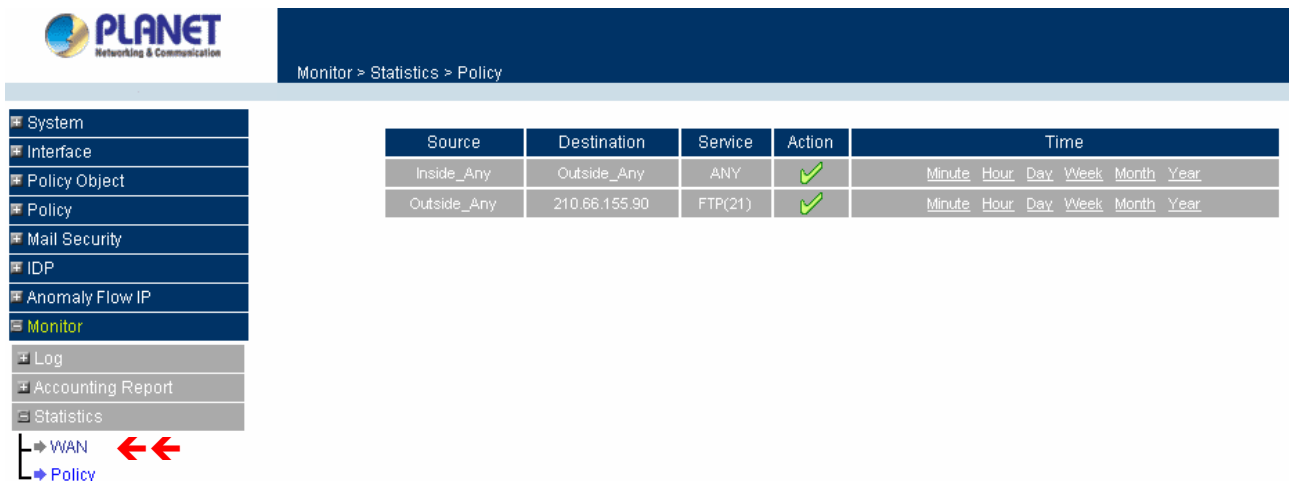
X-Coordinate: Time (Minute/Hour/Day/Week/Month/Year) .

3.8.3.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, days, week, month and year.



Monitor > Statistics > Policy

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	✓	Minute Hour Day Week Month Year
Outside_Any	210.66.155.90	FTP(21)	✓	Minute Hour Day Week Month Year

Left sidebar menu items: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor (selected), Log, Accounting Report, Statistics, WAN, Policy.

NOTE: To use Statistics, the administrator needs to go to Policy to enable Statistics function.

Entering the Policy Statistics

- Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **Policy Statistics**.
- Step 2. In Statistics window, find the policy you want to view
- Step 3. In the Statistics window, click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate: There are three options: Total, Kbit/sec, Kbytes/sec.

X-Coordinate: Time (Minute/Hour/Day/Week/Month/Year).



Monitor > Statistics > Policy

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor
- Log
- Accounting Report
- Statistics
- WAN
- Policy
- Status

Bits/sec Bytes/sec Total

Inside_Any to Outside_Any

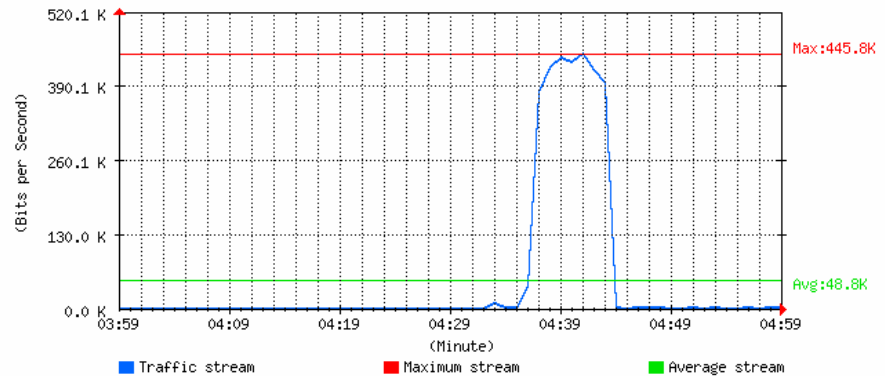
Service : ANY

Action : PERMIT

Minute Hour Day Week Month Year

Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec

Downstream



3.8.4 Status

In this section, the device displays the status information about the Multi-Homing Security Gateway. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Multi-Homing Security Gateway.

3.8.4.1 Interface Status

Entering the Interface Status window

Click on **Status** in the menu bar, then click **Interface Status** below it. A window will appear providing information from the Configuration menu. **Interface Status** will list the settings for **LAN Interface**, **WAN 1/2 Interface**, and the **DMZ Interface**.



Monitor > Status > Interface

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor
- Log
- Accounting Report
- Statistics
- Status
 - Interface
 - Authentication
 - ARP Table
 - DHCP Clients

Active Sessions Number : 3

System Uptime : 5 Day 20 Hour 56 Min 46 Sec

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Disable	NAT
WAN Connection	---			---
Max. Downstream / Upstream	---	50000 / 50000 Kbps	---	---
Downstream Alloca.	---	100%	0%	---
Upstream Alloca.	---	100%	0%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:e0:98:00:00:11	00:e0:98:00:00:12	00:e0:98:00:00:13	00:e0:98:00:00:14
IP Address	192.168.10.1	210.66.155.90	0.0.0.0	192.168.30.1
Netmask	255.255.255.0	255.255.255.224	0.0.0.0	255.255.255.0
Default Gateway	---	210.66.155.94	0.0.0.0	---
DNS1	---	168.95.1.1	0.0.0.0	---
DNS2	---	0.0.0.0	0.0.0.0	---
Rx Pkts, Error Pkts	54046, 0	1005976, 0	0, 0	0, 0
Tx Pkts, Error Pkts	59726, 0	854635, 0	0, 0	3, 0
Ping			---	
HTTP			---	---

3.8.4.2 Authentication

Entering the Auth Status window

Click on **Status** in the menu bar, then click Authentication below it. A window will appear and provide information from the Auth User menu. Authentication Status will list the settings for Auth User login status.



Monitor > Status > Authentication

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor
- Log
- Accounting Report
- Statistics
- Status
 - Interface
 - Authentication
 - ARP Table
 - DHCP Clients

IP Address	Authentication-User Name	Login Time	Configure
192.168.10.3	planet	2006/4/10 5:6:8	

IP Address: The IP address of the host computer.

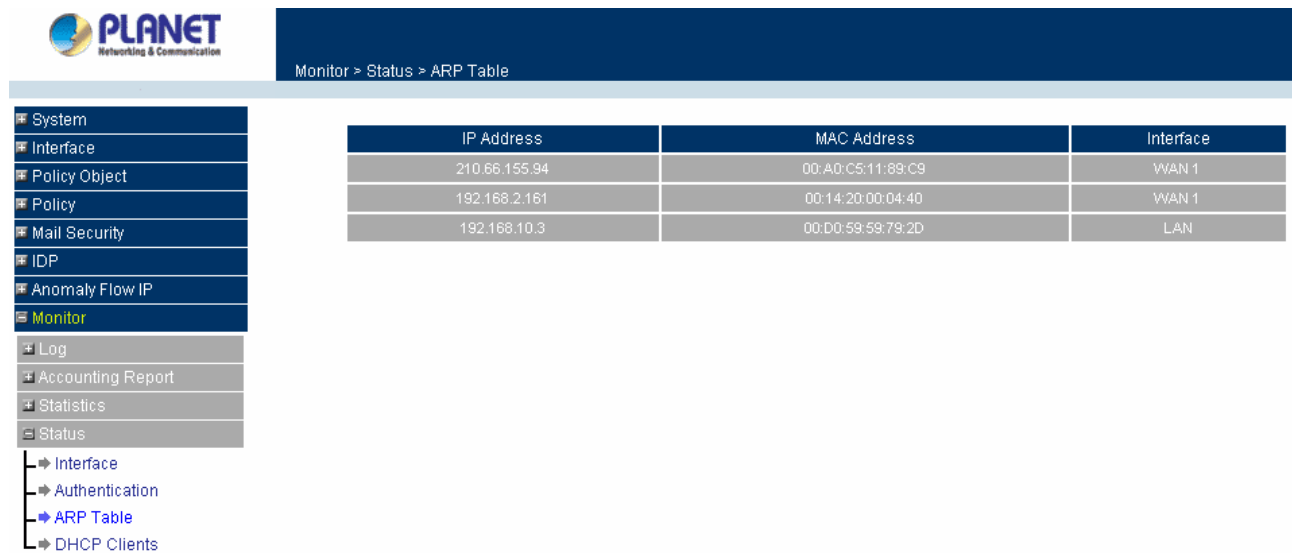
Auth-User Name: The Auth User Name of that host computer.

Login time: The Auth User login in time.

3.8.4.3 ARP Table

Entering the ARP Table window

Click on **Status** in the menu bar, then click **ARP Table** below it. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN, and DMZ network that replies to an ARP packet, the device will list them in this ARP table.



The screenshot shows the Planet Multi-Homing Security Gateway web interface. The top navigation bar includes the Planet logo and the text "Monitoring & Communication". Below this, a breadcrumb trail reads "Monitor > Status > ARP Table". On the left side, there is a vertical menu with various system components. The "Monitor" section is expanded, showing sub-items like "Log", "Accounting Report", "Statistics", and "Status". Under "Status", further sub-items are listed: "Interface", "Authentication", "ARP Table" (which is highlighted in blue), and "DHCP Clients". The main content area on the right displays a table with three columns: "IP Address", "MAC Address", and "Interface".

IP Address	MAC Address	Interface
210.66.155.94	00:A0:C5:11:89:C9	WAN 1
192.168.2.161	00:14:20:00:04:40	WAN 1
192.168.10.3	00:D0:59:59:79:2D	LAN

IP Address: The IP address of the host computer

MAC Address: The MAC address of that host computer

Interface: The port that the host computer is connected to (LAN, WAN 1/2, DMZ)

3.8.4.4 DHCP Clients

Entering the DHCP Clients window

Click on **Status** in the menu bar, then to click on **DHCP Clients** below it. A window will appear displaying the table of DHCP clients that are connected to the device. The table will list host computers on the LAN network that obtain its IP address from the Multi-Homing Security Gateway's DHCP server function.



Monitor > Status > DHCP Clients

- System
- Interface
- Policy Object
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor
- Log
- Accounting Report
- Statistics
- Status
 - Interface
 - Authentication
 - ARP Table
 - DHCP Clients

IP Address	MAC Address	Leased Time	
		Start	End
192.168.10.3	00:d0:59:59:79:2d	2006/4/10 2:41:34	2006/4/11 2:41:34
192.168.10.2	00:0e:a6:0f:8b:92	2006/4/10 1:19:10	2006/4/11 1:19:10

IP Address: the IP address of the LAN host computer

MAC Address: MAC address of the LAN host computer

Leased Time: The Start and End time of the DHCP lease for the LAN host computer.