



Content Security Gateway CS-500

User's Manual

Copyright

Copyright (C) 2005 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.

Customer Service

For information on customer service and support for the Content 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:

- ◆ Content 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 Content Security Gateway

Model: CS-500

Rev: 1.0 (Jan, 2005)

Part No. EM-CS500v1

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 FEATURES.....	1
1.2 PACKAGE CONTENTS	1
1.3 CONTENT SECURITY GATEWAY FRONT VIEW	2
1.4 CONTENT SECURITY GATEWAY REAR PANEL.....	2
1.5 SPECIFICATION	3
CHAPTER 2: HARDWARE INSTALLATION	4
2.1 INSTALLATION REQUIREMENTS	4
2.2 OPERATION MODE.....	4
2.2.1 <i>Transparent Mode Connection Example</i>	4
2.2.2 <i>NAT Mode Connecting Example</i>	5
CHAPTER 3: GETTING STARTED.....	7
3.1 WEB CONFIGURATION.....	7
3.2 CONFIGURE WAN INTERFACE	8
3.3 CONFIGURE DMZ INTERFACE.....	9
3.4 CONFIGURE POLICY	10
CHAPTER 4: WEB CONFIGURATION.....	12
4.1 SYSTEM	12
4.1.1 <i>Admin</i>	13
4.1.2 <i>Permitted IPs</i>	15
4.1.3 <i>Logout</i>	17
4.1.4 <i>Software Update</i>	18
4.1.5 <i>Setting</i>	18
4.1.6 <i>Date/Time</i>	25
4.1.7 <i>Multiple Subnet</i>	26
4.1.8 <i>Route Table</i>	31
4.1.9 <i>DHCP</i>	32
4.1.10 <i>Dynamic DNS</i>	34
4.1.11 <i>Host Table</i>	36
4.1.12 <i>Language</i>	38
4.2 INTERFACE.....	38
4.2.1 <i>LAN</i>	38
4.2.2 <i>WAN</i>	39
4.2.3 <i>DMZ</i>	44

4.3 POLICY OBJECT.....	45
4.3.1 Address.....	45
4.3.1.1 LAN.....	46
4.3.1.2 LAN Group.....	48
4.3.1.3 WAN.....	51
4.3.1.4 WAN Group.....	52
4.3.1.5 DMZ.....	56
4.3.1.6 DMZ Group.....	57
4.3.2 Service.....	60
4.3.2.1 Pre-defined.....	61
4.3.2.2 Custom.....	62
4.3.2.3 Group.....	64
4.3.3 Schedule.....	67
4.3.4 Content Blocking.....	70
4.3.4.1 URL Blocking.....	70
4.3.4.2 Scripts.....	72
4.3.4.3 P2P.....	73
4.3.4.4 IM.....	74
4.3.4.5 Download.....	74
4.3.5 Virtual Server.....	75
4.3.5.1 Mapped IP.....	76
4.3.5.2 Virtual Server.....	78
4.3.6 VPN.....	84
4.3.6.1 IPSec Autokey.....	84
4.3.6.2 PPTP Server.....	133
4.3.6.3 PPTP Client.....	136
4.4 POLICY.....	139
4.4.1 Outgoing.....	140
4.4.2 Incoming.....	145
4.4.3 WAN To DMZ & LAN To DMZ.....	148
4.4.4 DMZ To WAN & DMZ To LAN.....	151
4.5 MAIL SECURITY.....	154
4.5.1 Configure.....	154
4.5.2 Anti-Spam.....	159
4.5.2.1 Setting.....	159
4.5.2.2 Rule.....	160
4.5.2.3 Whitelist.....	163
4.5.2.4 Blacklist.....	164
4.5.2.5 Training.....	166

4.5.2.6 Spam Mail.....	167
4.5.3 Anti-Virus.....	168
4.5.3.1 Setting.....	168
4.5.3.2 Virus Mail.....	169
4.6 ANTI-ATTACK	169
4.6.1 Alert Setting.....	169
4.6.1.1 Internal Alert.....	169
4.6.1.2 External Alert.....	170
4.6.2 Attack Alarm	172
4.6.2.1 Internal Alarm.....	172
4.6.2.2 External Alarm.....	173
4.7 MONITOR	174
4.7.1 Log.....	174
4.7.1.1 Traffic.....	175
4.7.1.2 Event	176
4.7.1.3 Connection	178
4.7.1.4 Log Backup	179
4.7.2 Alarm	181
4.7.3 Statistic.....	182
4.7.3.1 WAN Statistics	183
4.7.3.2 Policy Statistics.....	184
4.7.4 Status.....	185
4.7.4.1 Interface Status.....	185
4.7.4.2 ARP Table.....	186
4.7.4.3 DHCP Clients.....	187

Chapter 1: Introduction

The innovation of the Internet has created a tremendous worldwide venue for e-business and information sharing, but it also creates network security problems, so the security request will be the primary concern for the enterprise. Planet's Content Security Gateway CS-500, a specially designed security gateway for small business, 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.

Meanwhile, Instant Messaging (IM) and peer-to-peer (P2P) are the fastest growing communications medium of all time, the spread of IM and P2P has created a network security threats and consumed amount of bandwidth. CS-500 also can prevent employees using varied IM and P2P like MSN, Yahoo Messenger, ICQ, QQ and Skype.

CS-500 not only can filter spam and virus mail, but also is a high performance VPN firewall. The firewall function can defense hacker and blaster attack from Internet.

1.1 Features

- ◆ **Anti-Spam Filtering:** Multiple defense layers (Head Analysis, Text Analysis, Blacklist & Whitelist, Bayesian Filtering), 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, POP 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.
- ◆ **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.
- ◆ **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.
- ◆ **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.
- ◆ **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

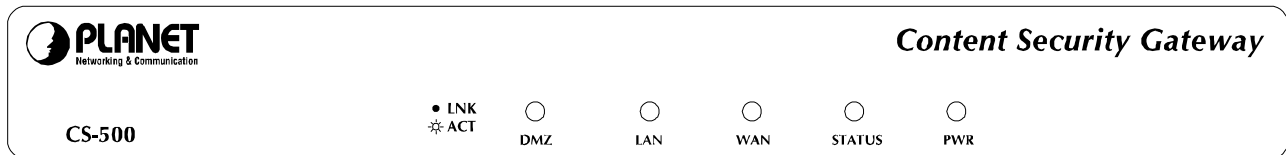
The following items should be included:

- CS-500
- n Content Security Gateway
- n User's Manual CD-ROM
- n This Quick Installation Guide
- n Power Adapter

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

1.3 Content Security Gateway Front View

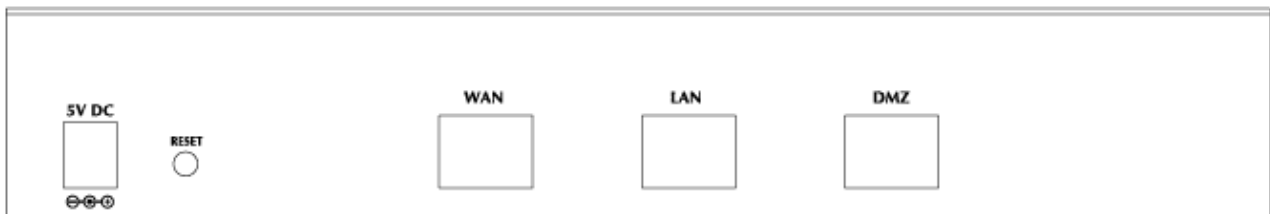
CS-500 Front Panel



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.
WAN, LAN, DMZ	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port

1.4 Content Security Gateway Rear Panel

CS-500 Rear Panel



Port or button	Description
RESET	Press this button to restore to factory default settings.
WAN	Connect to your xDSL/Cable modem or other Internet connection devices
LAN	Connect to your local PC, switch or other local network device
DMZ	Connect to your server or other network device

1.5 Specification

Product		Content Security Gateway
Model		CS-500
Hardware		
Ethernet	LAN	1 x 10/100Mbps RJ-45
	WAN	1 x 10/100Mbps RJ-45
	DMZ	1 x 10/100Mbps RJ-45
LED		POWER, STATUS, 10/100 and LNK/ACT for each LAN and WAN port
Power		5VDC, 2.4A
Operating Environment		Temperature: 0~50°C Relative Humidity: 10%~90%
Dimension W x D x H, mm		220 x 150 x 40
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		8,000
Email Capacity per Day		90,000
Firewall Throughout		100Mbps
3DES Throughout		15Mbps
Firewall		Policy-based firewall rule with schedule, NAT/NAPT, SPI firewall
VPN Tunnels		200
VPN Function		PPTP server and client, IPSec DES, 3DES and AES encryption, SHA-1 and MD5 authentication algorithm Remote access VPN (client-to-Site) and Site to Site VPN
Content Filtering		URL, P2P application, Instant Message, download blocking Popup, Java Applet, cookies and Active X blocking
Anti-Attack		Hacker Alert: Sasser, Code Red, Syn Flood, ICMP Flood, UDP Flood, Blaster Alert
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 a specific account Automatic or manual update virus database
Anti-Spam		Inbound scanning for external and internal Mail Server Check sender address in RBL Black list and white list support auto training system Action of spam mail: Delete, Deliver to the recipient, forward to a specific account Up to 100 spam mail rule entries
Logs		Log and alarm for event and traffic Log can be saved from web, sent by e-mail or send to syslog server
Statistics		Traffic statistics for WAN interface and policies Graphic display
Others		Dynamic DNS, NTP support, DHCP server, Virtual server, Mapping IP (DMZ)

Chapter 2: Hardware Installation

2.1 Installation Requirements

Before installing the Content Security Gateway, make sure your network meets the following requirements.

- Mechanical Requirements

The Content Security Gateway is to be installed between your Internet connection and local area network. The Content Security Gateway can be placed on the table or rack. Locate the unit near the power outlet.

- Electrical Requirements

The Content Security Gateway is a power-required device, it means, the Content Security Gateway will not work until it is powered. If your networked PCs will need to transmit data all the time, please consider use an UPS (Uninterrupted Power Supply) for your Content Security Gateway. It will prevent you from network data loss. In some area, installing a surge suppression device may also help to protect your Content Security Gateway from being damaged by unregulated surge or current to the Content Security Gateway.

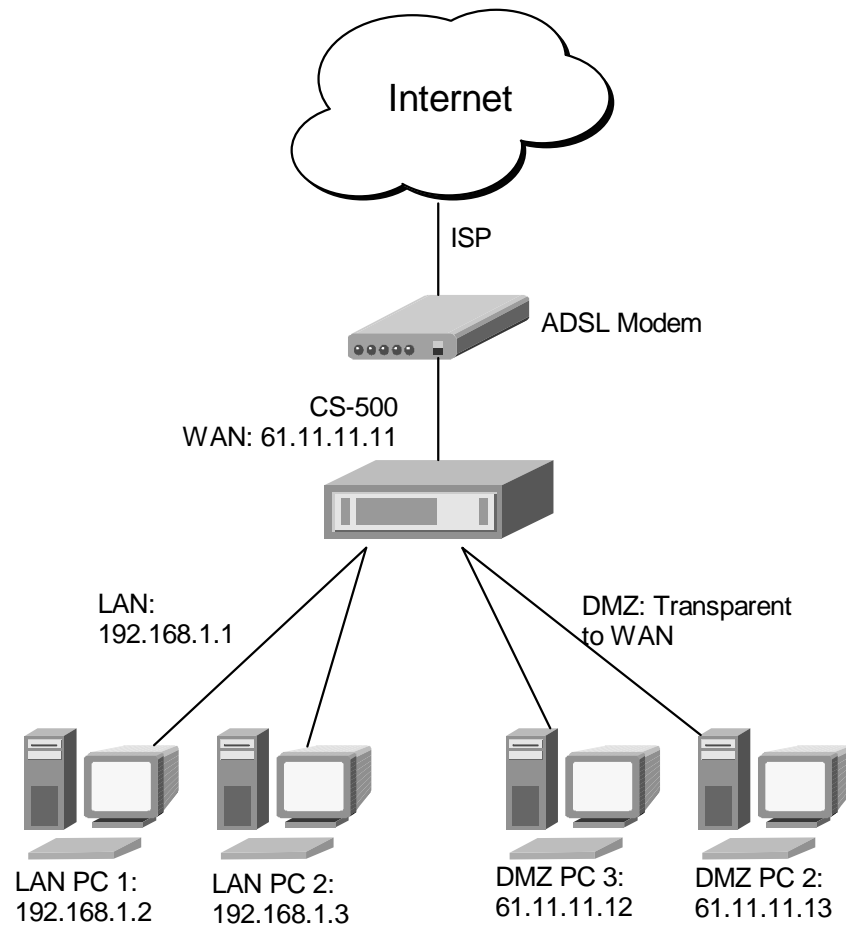
- Network Requirements

In order for Content Security Gateway to secure your network traffic, the traffic must pass through Content Security Gateway at a useful point in a network. In most situations, the Content Security Gateway should be placed behind the Internet connection device.

2.2 Operation Mode

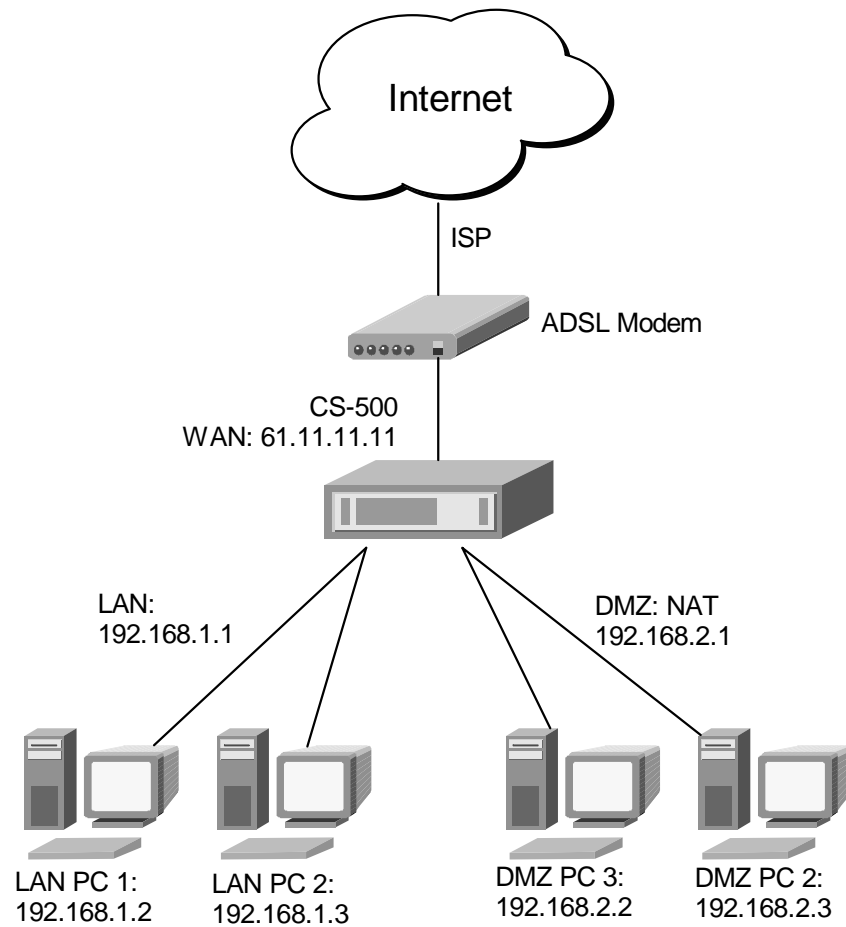
CS-500 DMZ port supports three operation modes, Disable, NAT and Transparent. In Disable mode, the DMZ port is not active. In transparent mode, CS-500 works as proxy with forward DMZ packet to WAN and forward WAN packet to DMZ, the DMZ and WAN side IP addresses are in the same subnet. In NAT mode, DMZ side user will share one public IP address of WAN port to make Internet connection. Please find the following two pictures for example.

2.2.1 Transparent Mode Connection Example



The WAN and DMZ side IP addresses are on the same subnet. This application is suitable if you have a subnet of IP addresses and you do not want to change any IP configuration on the subnet.

2.2.2 NAT Mode Connecting Example



DMZ and WAN IP addresses are on the different subnet. This provides higher security level than transparent mode.

Chapter 3: Getting Started

3.1 Web Configuration

STEP 1:

Connect both the Administrator's PC and the LAN port of the Content Security Gateway to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Content Security Gateway has an embedded web server used for management and configuration. Use a web browser to display the configurations of the Content 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 Content 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 Content 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 Content Security Gateway.

The following table is a list of private IP addresses. These addresses may not be used as a WAN IP address.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

STEP 2:

Once the Administrator PC has an IP address on the same network as the Content 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 Content Security Gateway. Enter the default login username and password of Administrator (see below).

Username: admin

Password: admin

Click OK.



Connect to 192.168.1.1

Bandwidth Administration Tools

User name:

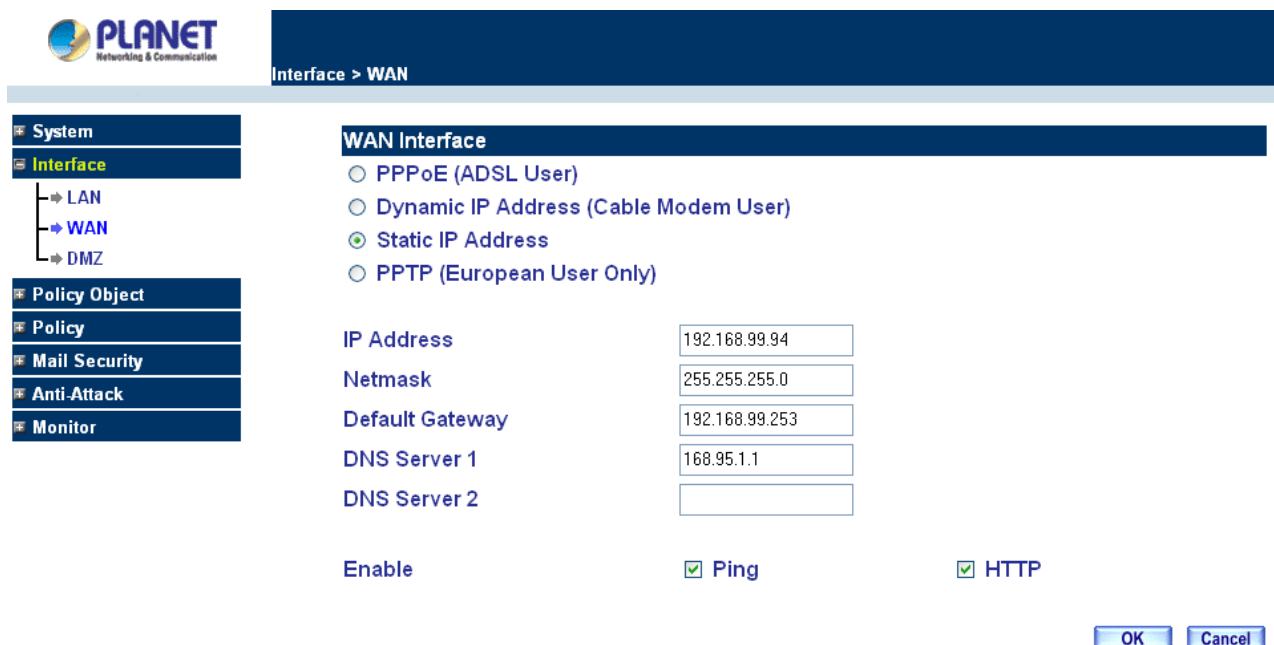
Password:

☒ Remember my password

OK Cancel

3.2 Configure WAN interface

After entering the username and password, the Content 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, the following page is shown.



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

Netmask

Default Gateway

DNS Server 1

DNS Server 2

Enable ☒ Ping ☒ HTTP

OK Cancel

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.

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.

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.

For PPTP (European User Only): This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.

PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.

Connect ID: This is the ID given by ISP. This is optional.

BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.

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.


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

WebUI: Select this to allow the device WEBUI to be accessed from the WAN 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 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	DMZ Interface DMZ_TRANSPARENT	
Interface	IP Address	0
<ul style="list-style-type: none"> LAN WAN DMZ 	Netmask	0
Policy Object	Enable	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
Policy		
Mail Security		
Anti-Attack		
Monitor		

OK Cancel

3.4 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	Modify Policy	
Interface	Source Address	Inside_Any
Policy Object	Destination Address	Outside_Any
Policy	Service	ANY
<ul style="list-style-type: none"> Outgoing Incoming WAN To DMZ LAN To DMZ DMZ To WAN DMZ To LAN 	Action	PERMIT
Mail Security	Logging	<input checked="" type="checkbox"/> Enable
Anti-Attack	Statistics	<input checked="" type="checkbox"/> Enable
Monitor	Content Filtering	<input checked="" type="checkbox"/> Enable
	Schedule	None
	Alarm Threshold	0.0 KBytes/Sec
	MAX. Concurrent Sessions	0 (0:means unlimited)



OK Cancel

STEP 4:

The configuration is successful when the screen below is displayed.



Policy > Outgoing

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

[New Entry](#)

- System
- Interface
- Policy Object
- Policy**
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- Anti-Attack
- Monitor

Please make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Content 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 Content Security Gateway filter function is required, please refer to the Policy section in chapter 4.

Chapter 4: Web Configuration

4.1 System

The Content 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 Content Security Gateway settings into local files;

"System" is the managing of settings such as the privileges of packets that pass through the Content Security Gateway and monitoring controls. Administrators may manage, monitor, and configure Content 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 Content Security Gateway.

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

Administration:

Admin: has control of user access to the Content Security Gateway. He/she can add/remove users and change passwords.

Permitted IP: Enables the Administrator to authorize specific internal/external IP address(es) for Managing Gateway.

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

Software Update: The administrator can update the device's software with the latest version.

Administrators may visit distributor's web site to download the latest firmware. Administrators may update the device firmware to optimize its performance and keep up with the latest fixes for intruding attacks.

Configure:

Setting: The Administrator may use this function to backup Content Security Gateway configurations and export (save) them to an "**Administrator**" computer or anywhere on the network; or restore a configuration file to the device; or restore the Content 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 Content 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 Content Security Gateway to be synchronized either with an Internet Server time or with the client computer's clock.

Multiple Subnet: This function allows local port to set multiple subnet works and connect with the internet through WAN IP Addresses.

Route Table: Use this function to enable the Administrator to add static routes 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.

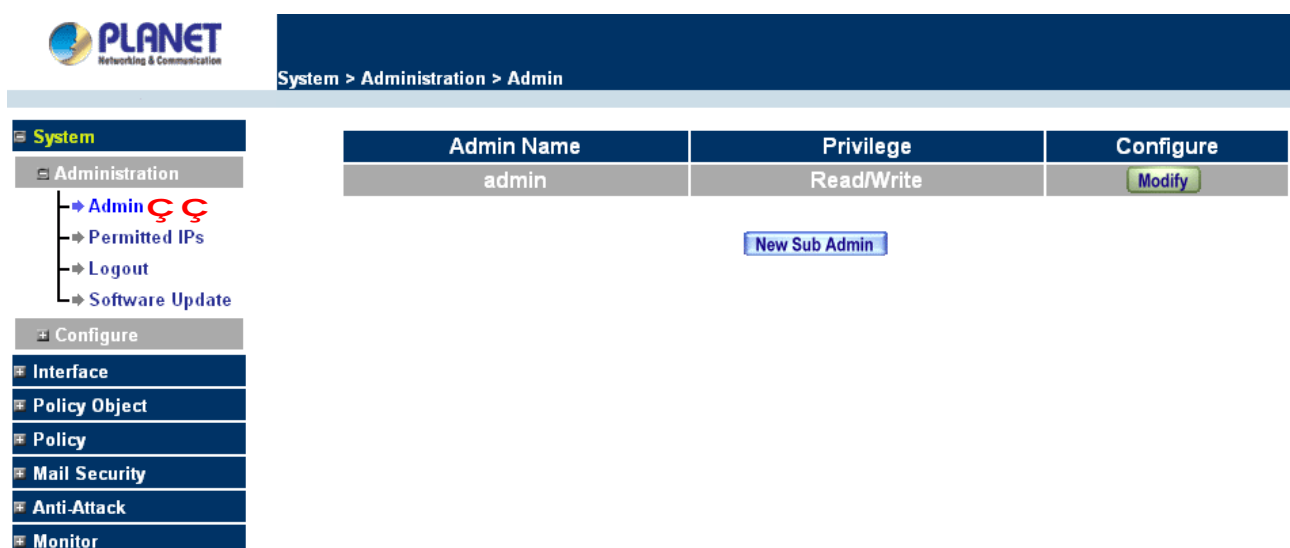
Dynamic DNS: The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP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

Host Table: The Content Security Gateway Administrator may use the Host Table function to make the Content 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 Content 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 come back through the Content 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 Content Security Gateway as a DNS server, which acts as the DNS Proxy.

Language: Both Chinese and English are supported in the Content Security Gateway.

4.1.1 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 Content Security Gateway web interface. The top navigation bar indicates the current path: System > Administration > Admin. On the left, a sidebar menu shows 'System' expanded, with 'Administration' selected, and 'Admin' highlighted with a red icon. Below 'Administration', other options like 'Permitted IPs', 'Logout', and 'Software Update' are visible. The main content area displays a table of administrators.

Admin Name	Privilege	Configure
admin	Read/Write	Modify

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

Settings of the Administration table

Administrator Name: The username of Administrators for the Content Security Gateway. The user **admin** cannot be removed.

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

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

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

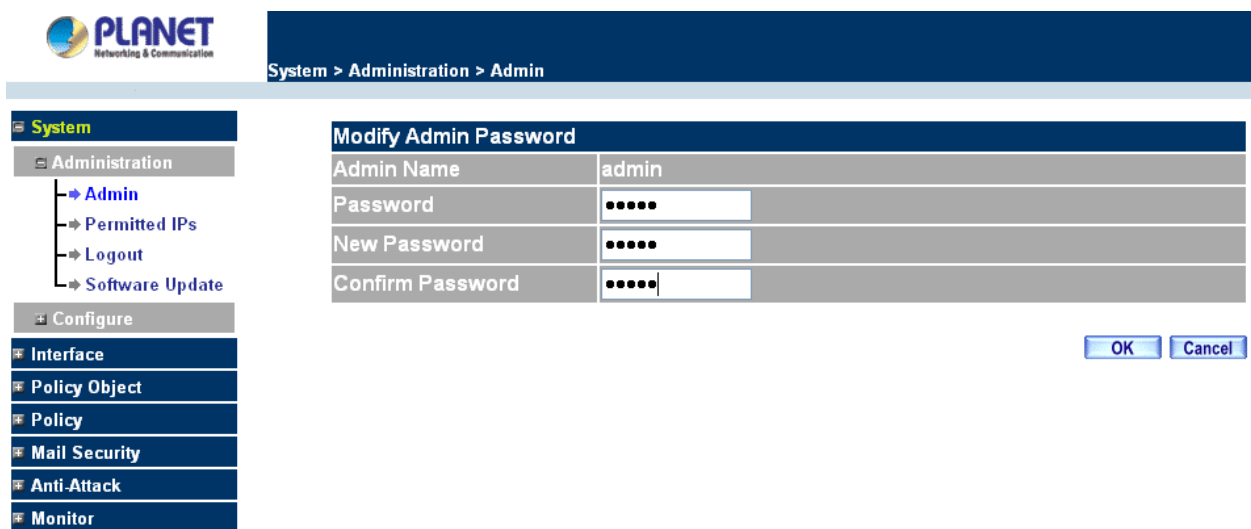
Configure: Click **Modify** to change the "Sub Administrator's" password and click **Remove** to delete a "Sub Administrator."

Changing the Main/Sub-Administrator's Password

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

- n **Password:** enter original password.
- n **New Password:** enter new password
- n **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 & Communication web interface. The breadcrumb navigation at the top reads "System > Administration > Admin". On the left, a sidebar menu shows "System" expanded, with "Administration" selected, and "Admin" highlighted. Below the sidebar, a "Configure" section lists various system settings. The main content area displays the "Modify Admin Password" window. This window contains a table with four rows: "Admin Name" (value: admin), "Password" (masked with dots), "New Password" (masked with dots), and "Confirm Password" (masked with dots). At the bottom right of the window are "OK" and "Cancel" buttons.

Modify Admin Password	
Admin Name	admin
Password
New Password
Confirm Password


OK Cancel

Adding a new Sub Administrator

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

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

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



System > Administration > Admin

System

- Administration
 - Admin
 - Permitted IPs
 - Logout
 - Software Update
- Configure
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor


Add New Sub Admin

Sub Admin name	planet
Password
Confirm Password

OK Cancel

Removing a Sub Administrator

- Step 1. In the Administration table, locate the Administrator 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.



System > Administration > Admin

System

- Administration
 - Admin
 - Permitted IPs
 - Logout
 - Software Update
- Configure
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

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

New Sub Admin

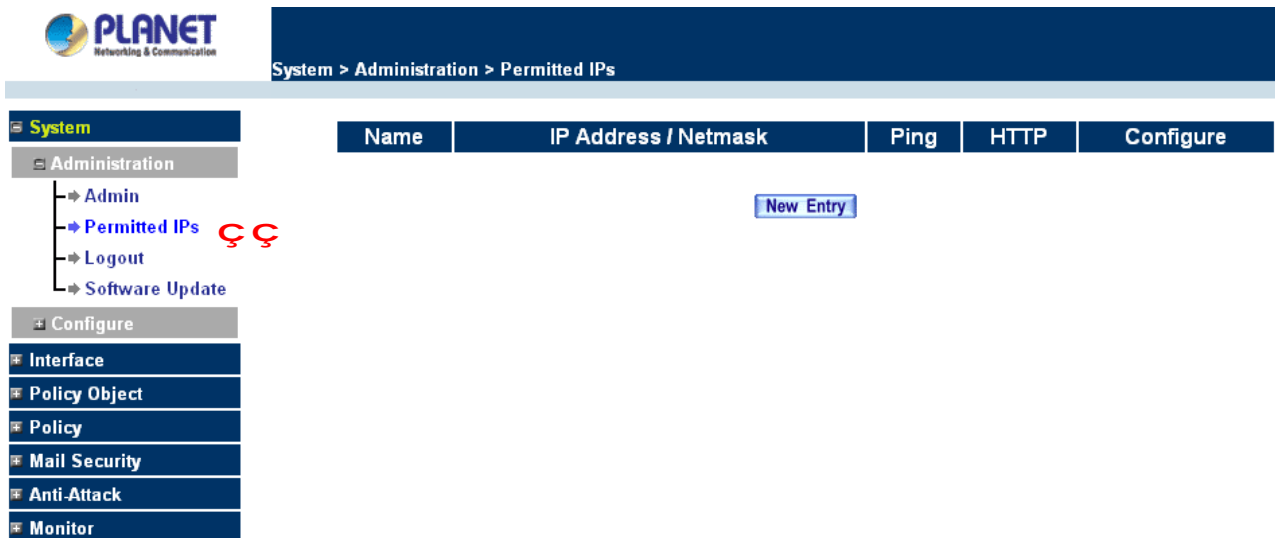
Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

4.1.2 Permitted IPs

Only the authorized IP address is permitted to manage the Content Security Gateway.



The screenshot shows the Planet Content Security Gateway Administration interface. The breadcrumb trail is **System > Administration > Permitted IPs**. On the left, there is a navigation menu with 'System' expanded, showing 'Administration' and 'Configure'. Under 'Administration', there are links for 'Admin', 'Permitted IPs' (highlighted with red arrows), 'Logout', and 'Software Update'. Under 'Configure', there are links for 'Interface', 'Policy Object', 'Policy', 'Mail Security', 'Anti-Attack', and 'Monitor'. The main content area has a table with the following headers: **Name**, **IP Address / Netmask**, **Ping**, **HTTP**, and **Configure**. A **New Entry** button is located to the right of the table.

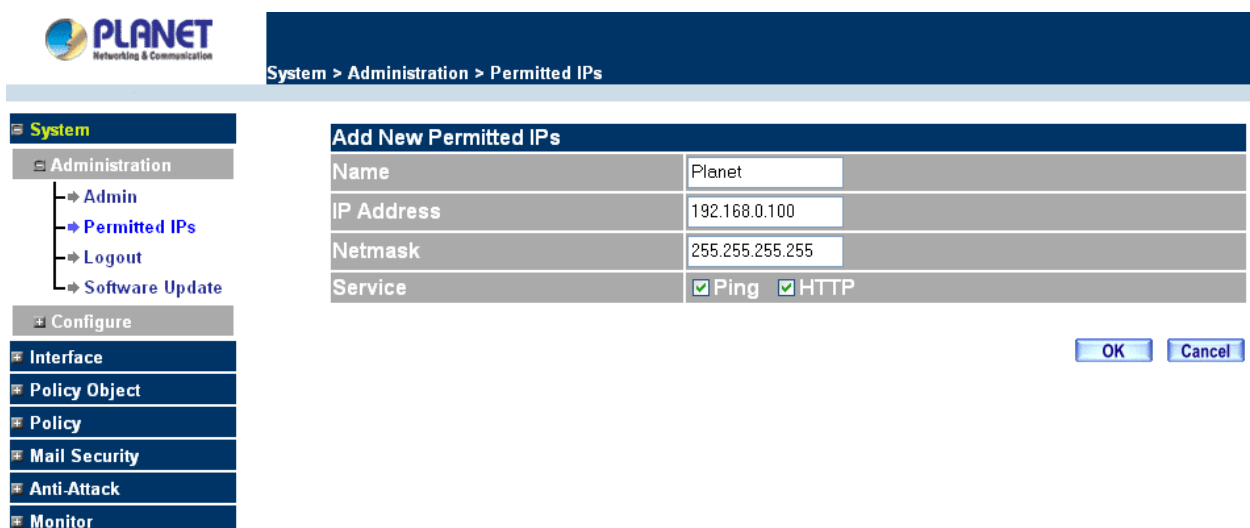
Add Permitted IPs Address

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

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

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

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



The screenshot shows the Planet Content Security Gateway Administration interface with the 'Add New Permitted IPs' form open. The breadcrumb trail is **System > Administration > Permitted IPs**. The left navigation menu is the same as in the previous screenshot. The form has the following fields: **Name** (Planet), **IP Address** (192.168.0.100), **Netmask** (255.255.255.255), and **Service** (with checkboxes for ☒ Ping and ☒ HTTP). **OK** and **Cancel** buttons are at the bottom right.

Modify Permitted IP 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 & Communication web interface. The breadcrumb navigation is 'System > Administration > Permitted IPs'. The left sidebar shows a tree view with 'System' expanded, 'Administration' selected, and 'Permitted IPs' highlighted. The main content area is titled 'Modify Permitted IPs' and contains a form with the following fields:

Name	Planet
IP Address	192.168.0.100
Netmask	255.255.255.255
Service	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP

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

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 **Remove Permitted IP**, enter new IP address.

Step 3. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.

The screenshot shows the Planet Network & Communication web interface. The breadcrumb navigation is 'System > Administration > Permitted IPs'. The left sidebar shows a tree view with 'System' expanded, 'Administration' selected, and 'Permitted IPs' highlighted. The main content area displays a table of Permitted IPs:

Name	IP Address / Netmask	Ping	HTTP	Configure
Planet	192.168.0.100 / 255.255.255.255			Modify Remove

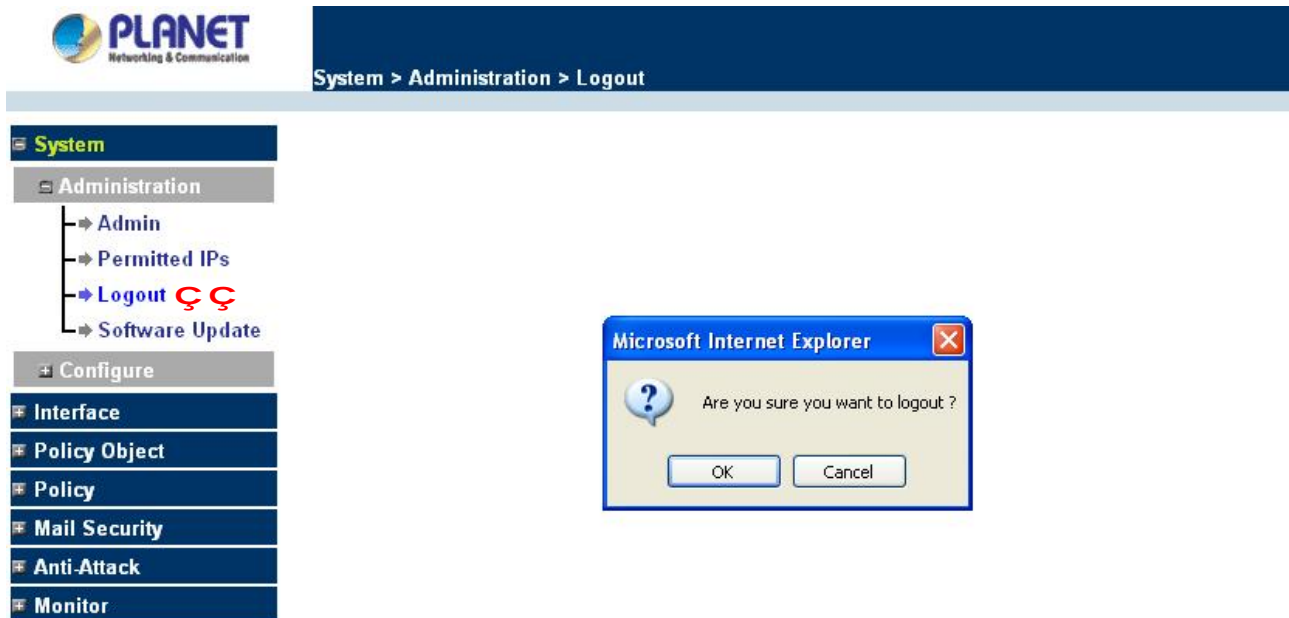
Below the table is a 'New Entry' button. A 'Microsoft Internet Explorer' dialog box is open, asking 'Are you sure you want to remove?' with 'OK' and 'Cancel' buttons.

4.1.3 Logout

Step 1. Select this option to the device's **Logout** the Content Security Gateway. This function protects your system while you are away.

Step 2. Click Logout the Content Security Gateway.

Step 3. Click **OK** to logout or click **Cancel** to discard the change.

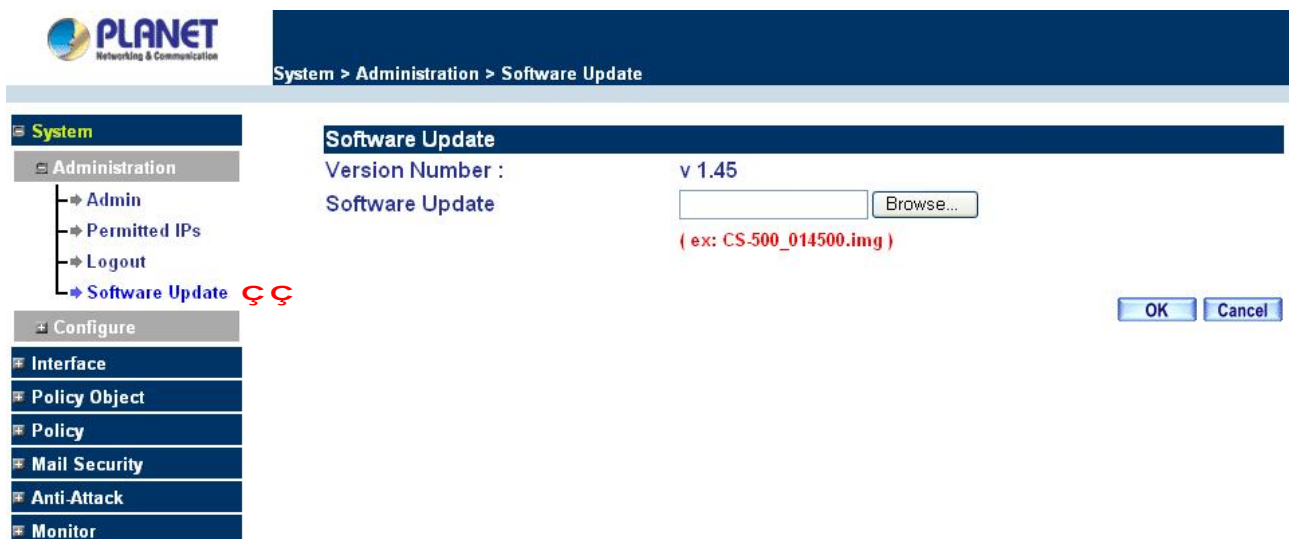


4.1.4 Software Update

Under **Software Update**, the admin may update the device's software with a newer software. You may acquire the current version number of software in **Version Number**. Administrators may visit distributor's web site 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.



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

4.1.5 Setting

The Administrator may use this function to backup Content Security Gateway configurations and export (save) them to an "**Administrator**" computer or anywhere on the network; or restore a configuration file to the

device; or restore the Content Security Gateway back to default factory settings.

Entering the Settings window

Click **Setting** in the **System** menu to enter the **Settings** window. The **Content Security Gateway Configuration** settings will be shown on the screen.

Content Security Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address Go

PLANET
Networking & Communication

System > Configure > Setting

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

Backup / Restore Configuration

Export System Setting to Client [Download](#)

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

☐ Reset Factory Setting

E-mail Setting

☐ Enable E-mail Alert Notification

Device Name (ex: ContentSecurityGateway)

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 [MailTest](#)

Web Management (WAN Interface)

HTTP Port

MTU Setting

MTU Bytes

Link Speed / Duplex Mode Setting

WAN

Dynamic Routing (RIPv2)

Enable ☐ LAN ☐ WAN ☐ DMZ

Routing information update timer Seconds

Routing information timeout Seconds

Administration Packet Logging

☒ Enable Administration Packet Logging

System Reboot

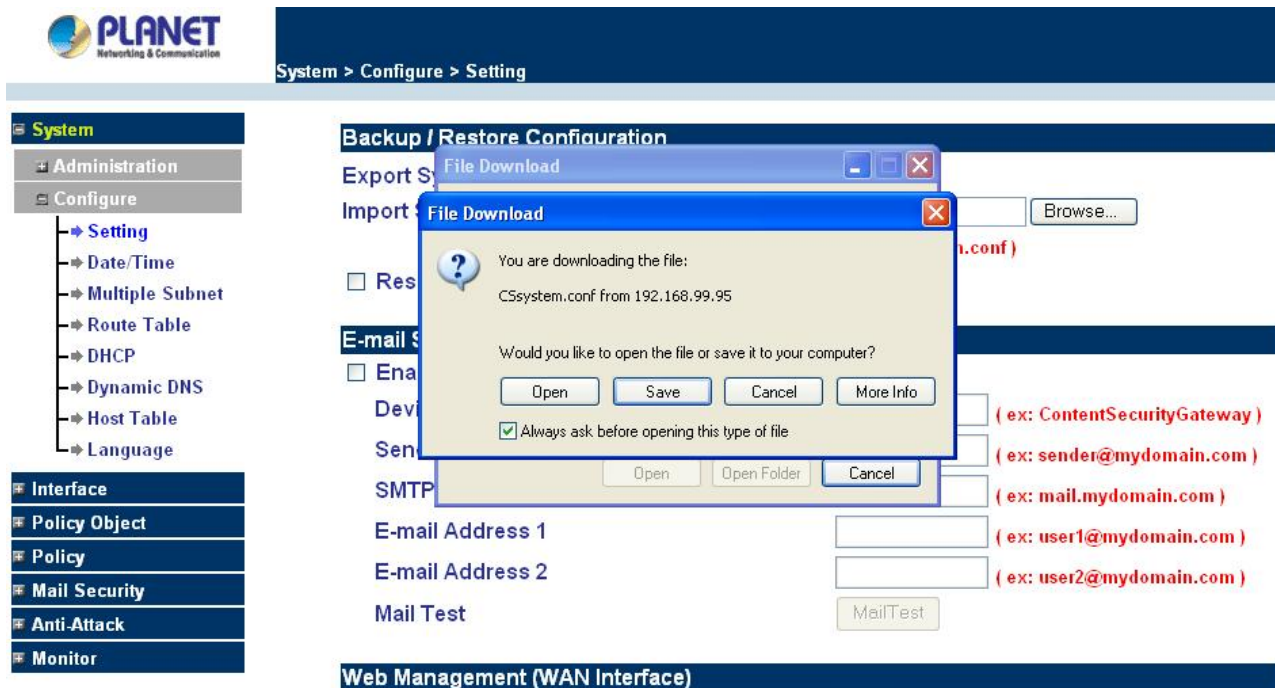
Reboot the System [Reboot](#)

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

Exporting Content Security Gateway settings

Step 1. Under **Configuration**, click on the **Download** button next to **Export System Settings to Client**.

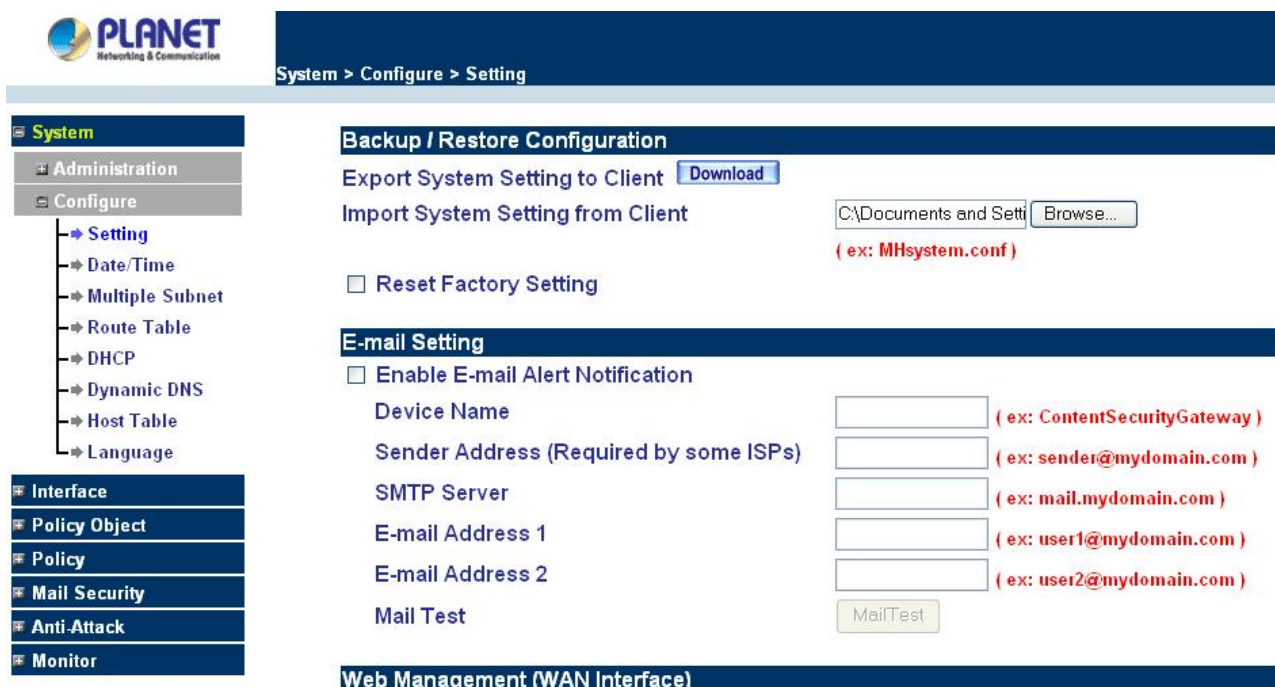
Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.



Importing Content Security Gateway settings

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

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



Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Configuration**.

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

The screenshot shows the PLANET Network & Communication configuration interface. The breadcrumb trail is 'System > Configure > Setting'. The left sidebar shows a tree view with 'System' expanded, containing 'Administration' and 'Configure'. Under 'Configure', 'Setting' is selected, with sub-items: Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Host Table, and Language. The main content area is titled 'Backup / Restore Configuration' and includes:

- 'Export System Setting to Client' with a 'Download' button.
- 'Import System Setting from Client' with a text input field and a 'Browse...' button. An example '(ex: MHsystem.conf)' is shown below.
- A checked checkbox for 'Reset Factory Setting'.
- An 'E-mail Setting' section with:
 - 'Enable E-mail Alert Notification' checkbox (unchecked).
 - 'Device Name' input field with example '(ex: ContentSecurityGateway)'.
 - 'Sender Address (Required by some ISPs)' input field with example '(ex: sender@mydomain.com)'.
 - 'SMTP Server' input field with example '(ex: mail.mydomain.com)'.
 - 'E-mail Address 1' input field with example '(ex: user1@mydomain.com)'.
 - 'E-mail Address 2' input field with example '(ex: user2@mydomain.com)'.
 - 'Mail Test' button.
- A 'Web Management (WAN Interface)' section at the bottom.

Enabling E-mail Alert Notification


Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Content 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.



System > Configure > Setting

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

Backup / Restore Configuration

Export System Setting to Client [Download](#)

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

☐ Reset Factory Setting

E-mail Setting

☒ Enable E-mail Alert Notification

Device Name (ex: ContentSecurityGateway)

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

Web Management (WAN Interface)

Web Management (WAN Interface) (Remote UI Management)


The administrator can change the port number used by HTTP port1 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.



System > Configure > Setting

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

Web Management (WAN Interface)

HTTP Port

MTU Setting

MTU Bytes

Link Speed / Duplex Mode Setting

WAN

Dynamic Routing (RIPv2)

Enable ☐ LAN ☐ WAN ☐ DMZ

Routing information update timer Seconds

Routing information timeout Seconds

Administration Packet Logging

☐ Enable Administration Packet Logging

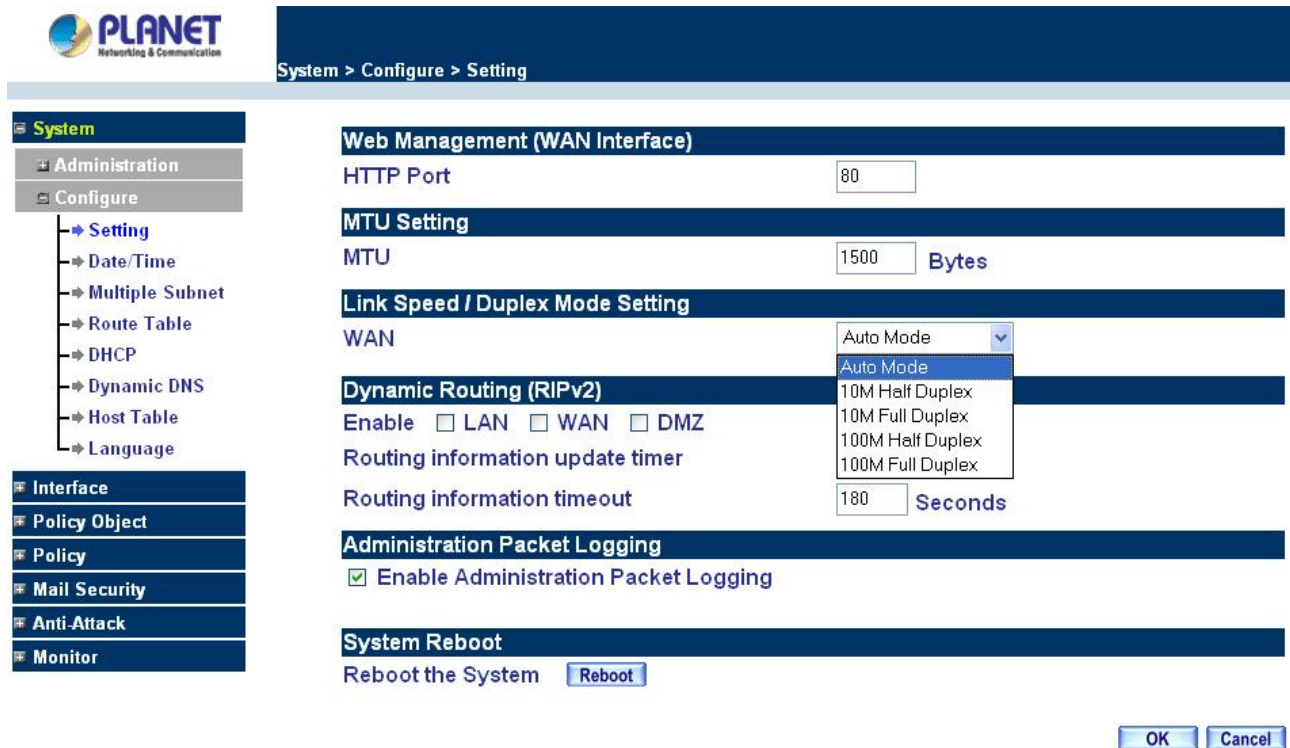
System Reboot

Reboot the System [Reboot](#)

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

Link Speed / Duplex Mode Setting

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



PLANET
Networking & Communication

System > Configure > Setting

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

Web Management (WAN Interface)

HTTP Port

MTU Setting

MTU Bytes

Link Speed / Duplex Mode Setting

WAN

- Auto Mode
- 10M Half Duplex
- 10M Full Duplex
- 100M Half Duplex
- 100M Full Duplex

Dynamic Routing (RIPv2)

Enable ☐ LAN ☐ WAN ☐ DMZ

Routing information update timer

Routing information timeout Seconds

Administration Packet Logging

☒ Enable Administration Packet Logging

System Reboot

Reboot the System

Dynamic Routing (RIPv2)

Enable Dynamic Routing (RIPv2), CS-500 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-500 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-500 does not receive the RIP protocol from the other router in a period of time, CS-500 will cut off the routing automatically until it receives RIP protocol again. The default timer is 180 seconds.

PLANET
Networking & Communication

System > Configure > Setting

System

- Administration
- Configure
 - Setting
 - Date/Time
 - Multiple Subnet
 - Route Table
 - DHCP
 - Dynamic DNS
 - Host Table
 - Language
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor

Web Management (WAN Interface)

HTTP Port

MTU Setting

MTU Bytes

Link Speed / Duplex Mode Setting

WAN

Dynamic Routing (RIPv2)

Enable ☒ LAN ☒ WAN ☒ DMZ

Routing information update timer Seconds

Routing information timeout Seconds

Administration Packet Logging

☒ Enable Administration Packet Logging

System Reboot

Reboot the System

Administration Packet Logging

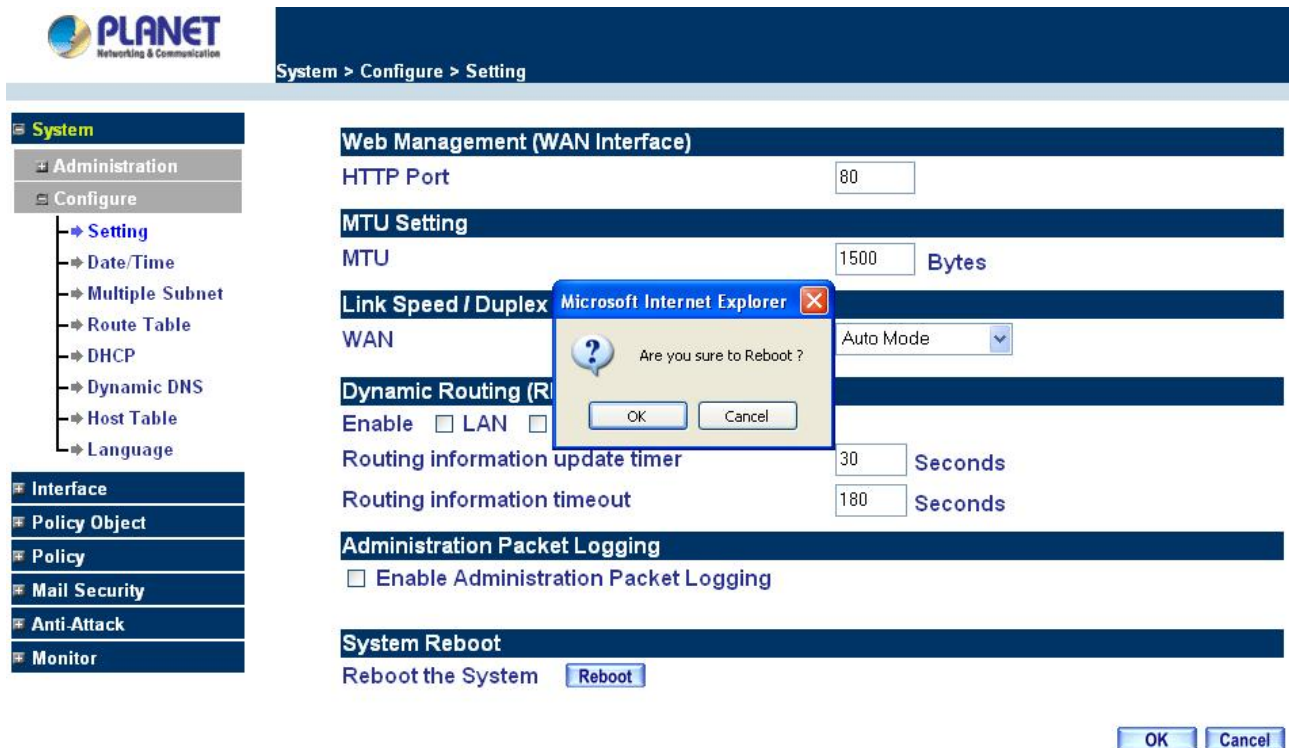
When the function is selected, the CS-500 will record the packets that contain the IP address of CS-500 in source or destination, the records will display in Traffic Log for administrator to inquire about.

System Reboot

Once this function is enabled, the Content 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 Content Security Gateway or click **Cancel** to discard changes.



4.1.6 Date/Time

Synchronizing the Content Security Gateway with the System Clock

Administrator can configure the Content 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 5 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 interface. The breadcrumb trail is "System > Configure > Date/Time". The left sidebar shows the "Configure" menu with options: Setting, Date/Time (selected), Multiple Subnet, Route Table, DHCP, Dynamic DNS, Host Table, and Language. The main content area displays the system time as "Thu Jan 20 08:42:00 2005". Below this is the "Synchronize system clock" section, which includes a checked checkbox for "Enable synchronize with an Internet time Server". The "Set offset" is set to "+8" hours from GMT, with an "Assist" link. The "Server IP / Name" is set to "131.188.3.220", also with an "Assist" link. The "Update system clock every" is set to "0" minutes, with a note "(0 : means update at booting time)". At the bottom of this section is a "Sync" button. At the very bottom of the interface are "OK" and "Cancel" buttons.

4.1.7 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) \rightarrow 168.85.88.253 (WAN)
2. Service department sub-network: 192.168.2.11/24 (LAN) \rightarrow 168.85.88.252 (WAN)
3. Sales department sub-network: 192.168.3.11/24 (LAN) \rightarrow 168.85.88.251 (WAN)
4. Procurement department sub-network: 192.168.4.11/24 (LAN) \rightarrow 168.85.88.250 (WAN)
5. Accounting department sub-network: 192.168.5.11/24 (LAN) \rightarrow 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 Multiple Subnet in the System menu to enter Multiple Subnet window.



System > Configure > Multiple Subnet

System	WAN Interface IP / Forwarding Mode	Alias IP of Internal Interface / Netmask	Configure
Administration	168.85.88.252 / NAT	192.168.2.1 / 255.255.255.0	Modify Remove
Configure	New Entry		
<ul style="list-style-type: none"> Setting Date/Time Multiple Subnet 			

Multiple Subnet functions

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

Alias IP of Int. 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 LAN 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


System	Add New Multiple Subnet IP								
Administration	Alias IP of LAN Interface	192.168.2.1							
Configure	Netmask	255.255.255.0							
<ul style="list-style-type: none"> Setting Date/Time Multiple Subnet Route Table DHCP Dynamic DNS 	<table border="1"> <thead> <tr> <th colspan="2">WAN Interface IP</th> <th>Forwarding Mode</th> </tr> </thead> <tbody> <tr> <td>WAN</td> <td>192.168.99.95 Assist</td> <td> <input checked="" type="radio"/> NAT <input type="radio"/> Routing </td> </tr> </tbody> </table>			WAN Interface IP		Forwarding Mode	WAN	192.168.99.95 Assist	<input checked="" type="radio"/> NAT <input type="radio"/> Routing
WAN Interface IP		Forwarding Mode							
WAN	192.168.99.95 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

Modify Multiple Subnet IP

Alias IP of LAN 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

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

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

[New Entry](#)

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

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.



System > Configure > Multiple Subnet

System	WAN Interface IP / Forwarding Mode	Alias IP of Internal Interface / Netmask	Configure
<ul style="list-style-type: none"> Administration Configure <ul style="list-style-type: none"> Setting Date/Time Multiple Subnet Route Table 	--- / Routing	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.

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

Modify: Modify the settings of Multiple Subnet. Click Modify to modify the parameters of Multiple Subnet or click **Remove** 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 LAN 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.



System > Configure > Multiple Subnet

System	Add New Multiple Subnet IP							
<ul style="list-style-type: none"> Administration Configure <ul style="list-style-type: none"> Setting Date/Time Multiple Subnet Route Table DHCP Dynamic DNS 	Alias IP of LAN Interface	168.85.88.1						
	Netmask	255.255.255.192						
	<table border="1"> <thead> <tr> <th colspan="2">WAN Interface IP</th> <th>Forwarding Mode</th> </tr> </thead> <tbody> <tr> <td>WAN</td> <td>0.0.0.0 Assist</td> <td> <input type="radio"/> NAT <input checked="" type="radio"/> Routing </td> </tr> </tbody> </table>		WAN Interface IP		Forwarding Mode	WAN	0.0.0.0 Assist	<input type="radio"/> NAT <input checked="" type="radio"/> Routing
	WAN Interface IP		Forwarding Mode					
WAN	0.0.0.0 Assist	<input type="radio"/> NAT <input checked="" type="radio"/> Routing						
<div> OK Cancel </div>								

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			Modify Remove	To 1

[New Entry](#)


- System
- Interface
- Policy Object
- Policy
 - Outgoing
 - Incoming
 - WAN 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

Modify Multiple Subnet IP

Alias IP of LAN Interface: 168.85.88.1

Netmask: 255.255.255.192


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

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

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

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

[New Entry](#)

Microsoft Internet Explorer

Are you sure you want to remove ?

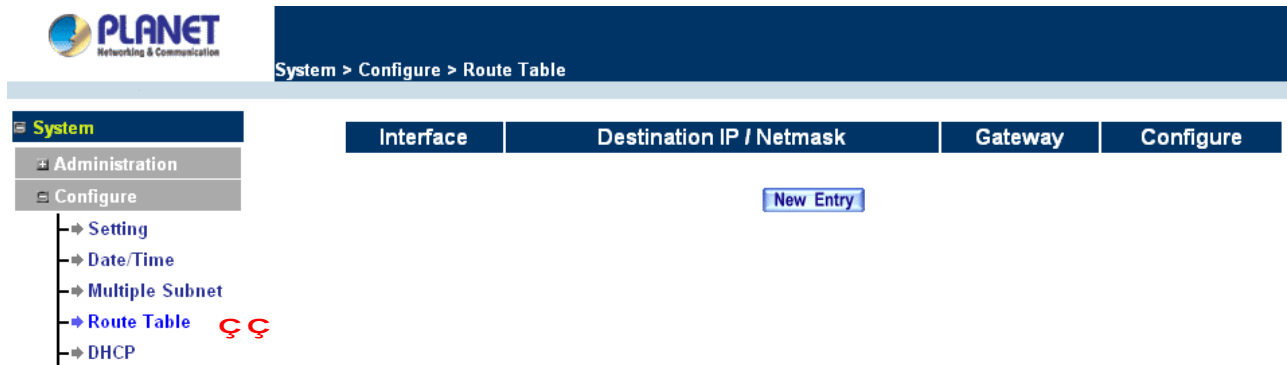
[OK](#) [Cancel](#)

4.1.8 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 side menu bar, then click **Route Table** below the Configure menu. The Route Table window appears, in which current route settings are shown.

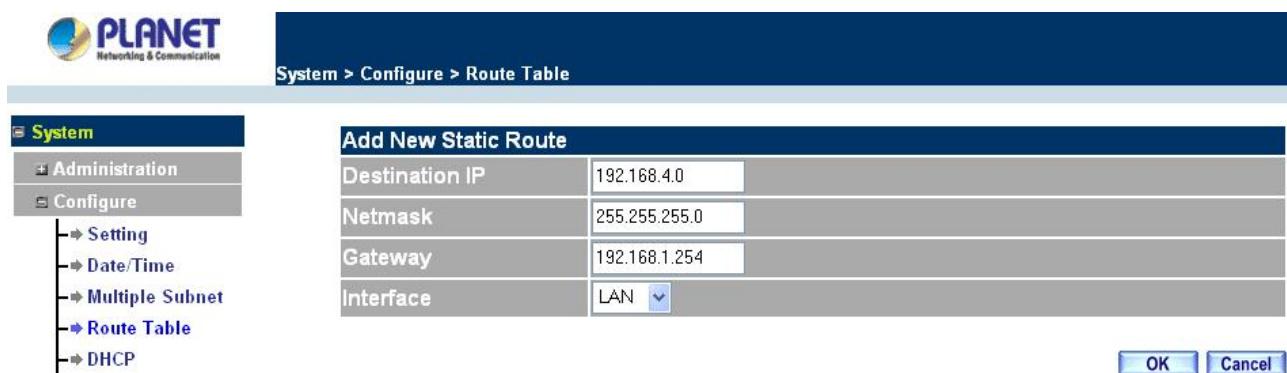


Route Table functions

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

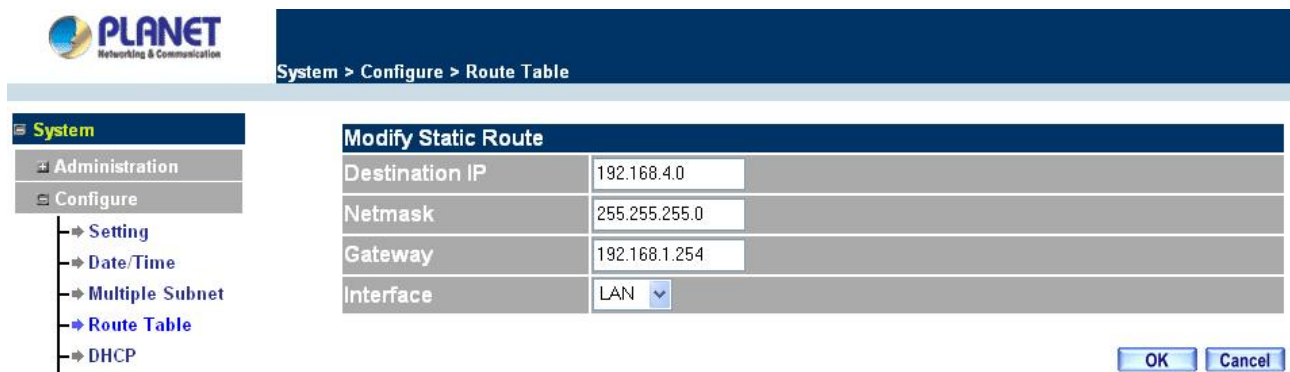
Adding a new Static Route

- 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.



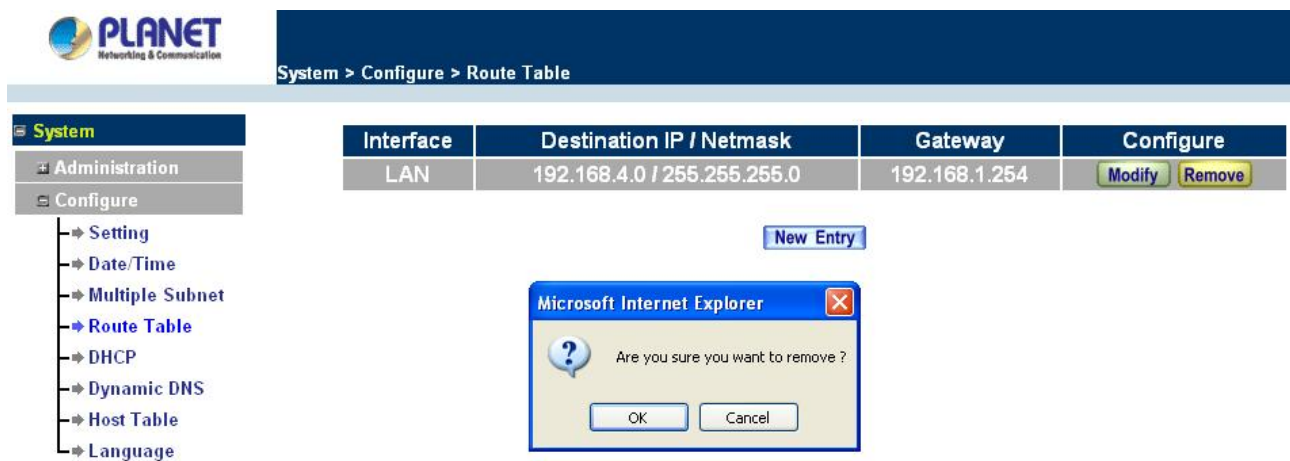
The screenshot shows the PLANET web interface with the breadcrumb 'System > Configure > Route Table'. On the left, a navigation menu has 'Route Table' selected. The main area displays the 'Modify Static Route' form with the following fields:

Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN

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

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.



The screenshot shows the PLANET web interface with the breadcrumb 'System > Configure > Route Table'. On the left, a navigation menu has 'Route Table' selected. The main area displays a table with route information:

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

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

4.1.9 DHCP

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

Entering the DHCP window

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

Dynamic IP Address functions

- n **Subnet:** LAN network's subnet
- n **Netmask:** LAN network's netmask
- n **Gateway:** LAN network's gateway IP address
- n **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.

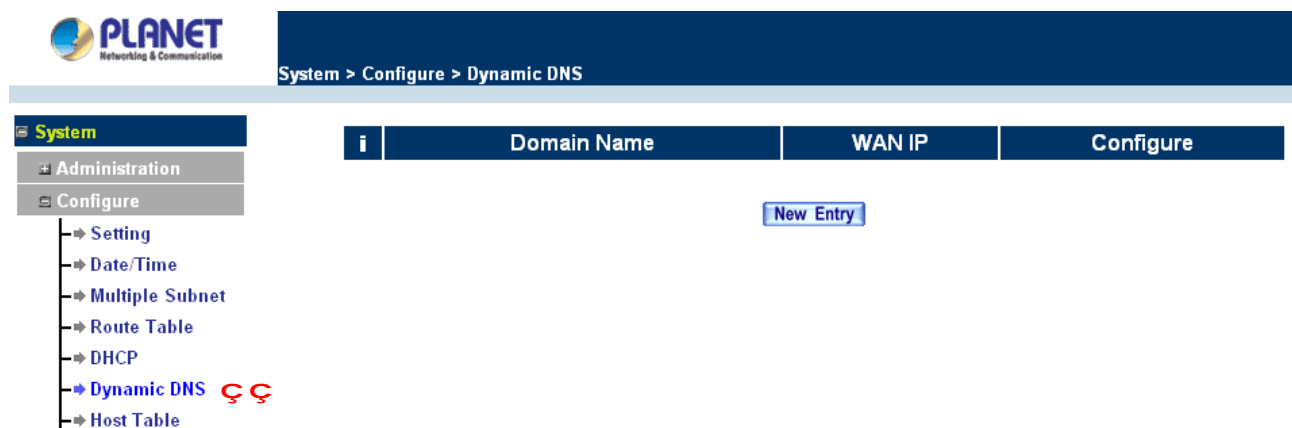
Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Leased Time: Enter the leased time for DHCP.

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

4.1.10 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.

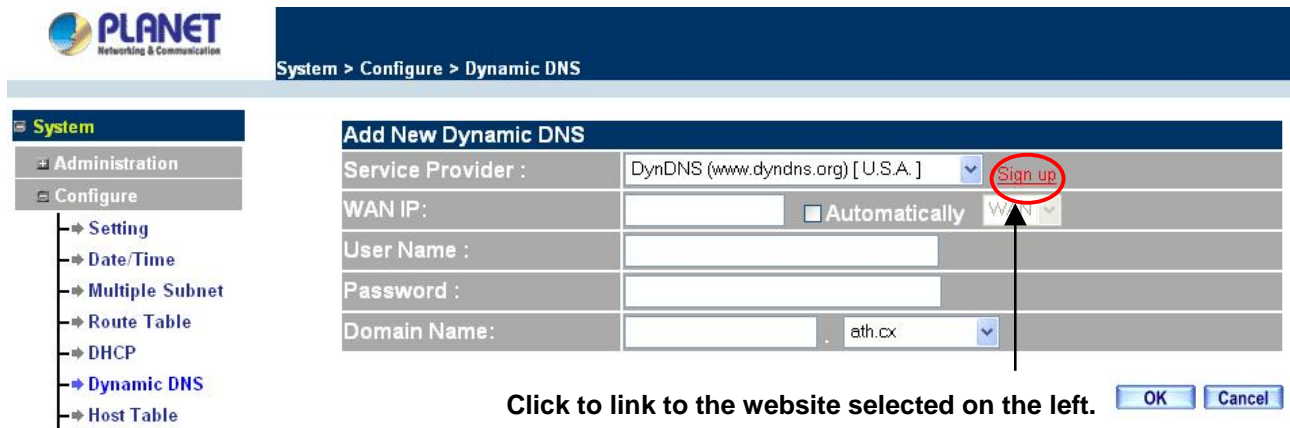
How to use dynamic DNS:

The Content 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

Add New Dynamic DNS

Service Provider :	DynDNS (www.dyndns.org) [U.S.A.]	Sign up
WAN IP:	<input type="text"/>	<input type="checkbox"/> Automatically WAN
User Name :	<input type="text"/>	
Password :	<input type="password"/>	
Domain Name:	<input type="text"/>	ath.cx

Click to link to the website selected on the left.

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.

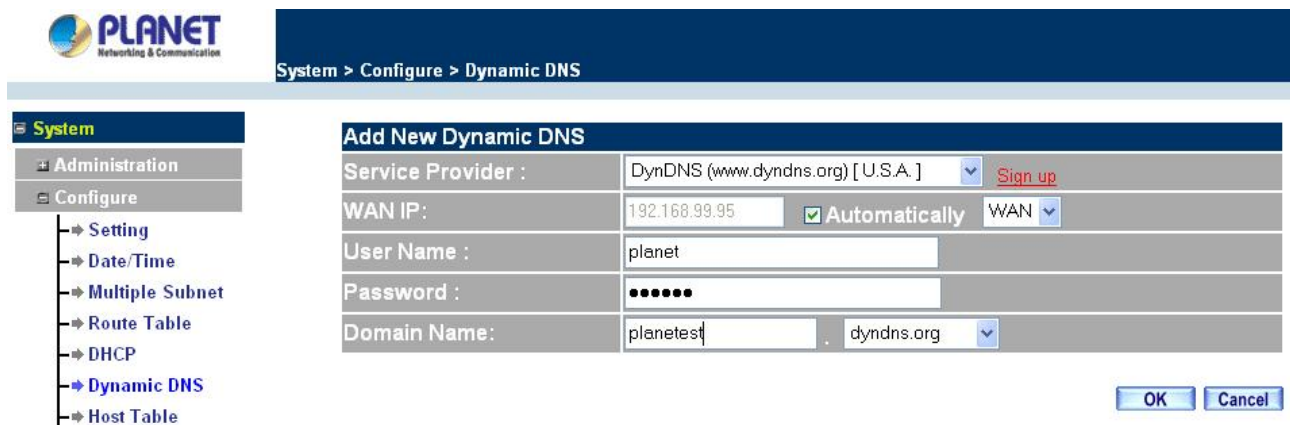
Automatically : Check to automatically fill in the WAN IP. °

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

Add New Dynamic DNS

Service Provider :	DynDNS (www.dyndns.org) [U.S.A.]	Sign up
WAN IP:	192.168.99.95	<input checked="" type="checkbox"/> Automatically WAN
User Name :	planet	
Password :	••••••	
Domain Name:	planetest	dyndns.org

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.

The screenshot shows the Planet Network & Communication web interface. The breadcrumb navigation is 'System > Configure > Dynamic DNS'. On the left, a sidebar menu shows 'System' expanded, with 'Configure' selected, and 'Dynamic DNS' highlighted. The main content area is titled 'Modify Dynamic DNS' and contains the following fields:

Service Provider :	DynDNS (www.dyndns.org) [U.S.A.]	Sign up
WAN IP :	192.168.99.95	<input checked="" type="checkbox"/> Automatically WAN
User Name :	planet	
Password :	••••••••	
Domain Name :	planetest	dyndns.org

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

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.

The screenshot shows the Planet Network & Communication web interface. The breadcrumb navigation is 'System > Configure > Dynamic DNS'. On the left, a sidebar menu shows 'System' expanded, with 'Configure' selected, and 'Dynamic DNS' highlighted. The main content area displays a table with the following data:

	Domain Name	WAN IP	Configure
	planetest.dyndns.org	192.168.99.95	Modify Remove

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

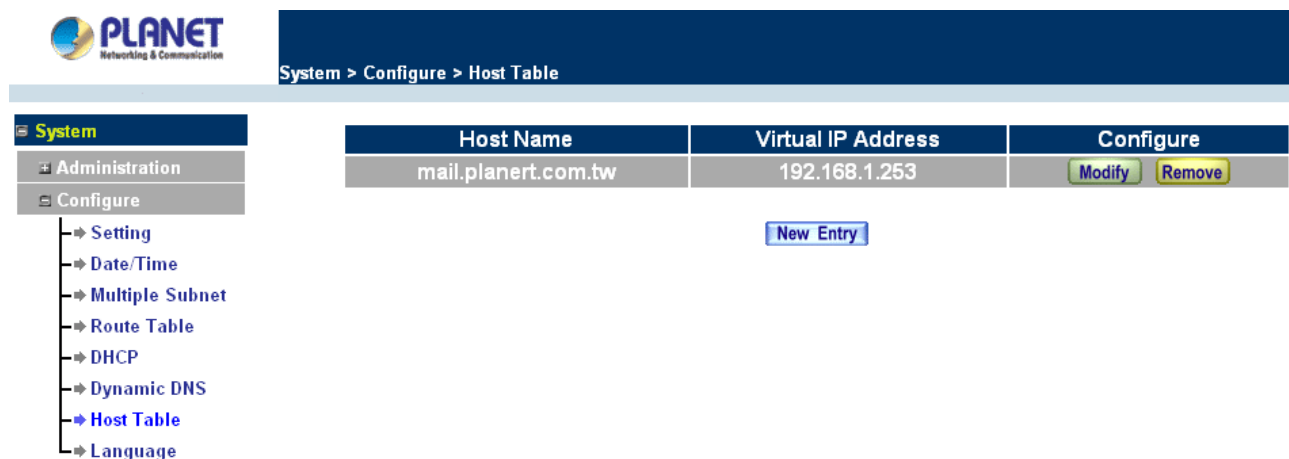
4.1.11 Host Table

The Content Security Gateway's Administrator may use the Host Table function to make the Content 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 Content 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 come back through the Content

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 Content 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 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.

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**.

4.1.12 Language

Administrator can configure the Content 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.



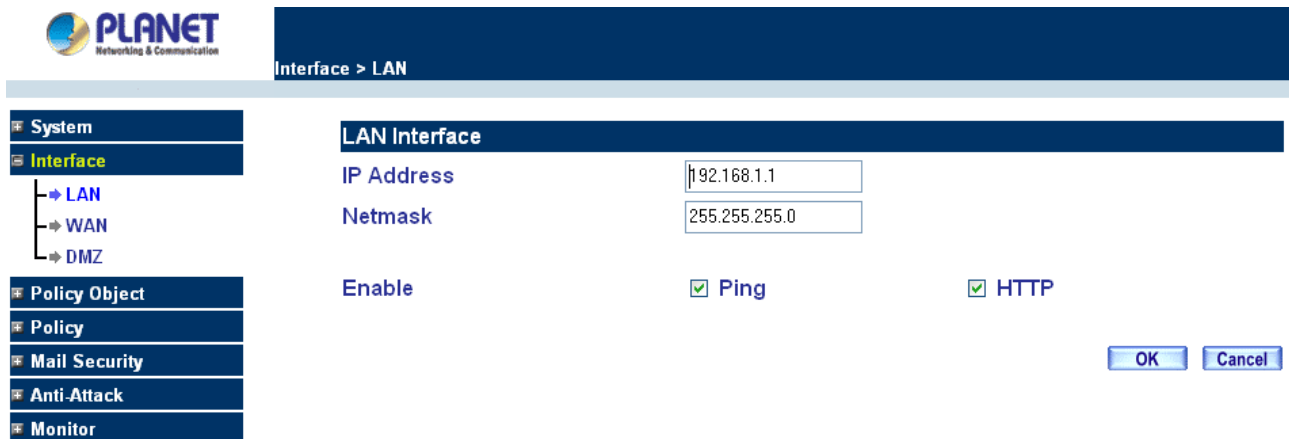
4.2 Interface

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.

4.2.1 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.



The screenshot shows the PLANET web interface. On the left is a navigation menu with options: System, Interface (selected), Policy Object, Policy, Mail Security, Anti-Attack, and Monitor. Under the 'Interface' menu, there are sub-options: LAN (selected), WAN, and DMZ. The main content area is titled 'Interface > LAN' and 'LAN Interface'. It contains configuration fields for 'IP Address' (192.168.1.1) and 'Netmask' (255.255.255.0). Below these are checkboxes for 'Enable', 'Ping' (checked), and 'HTTP' (checked). At the bottom right are 'OK' and 'Cancel' buttons.

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 Content 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 on the same subnet as the Content Security Gateway and restart the System to make the new IP address effective. For example, if the Content 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 Content 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 Content Security Gateway. If set to enable, the device will respond to ping packets from the LAN network.

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

4.2.2 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.

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
 Netmask
 Default Gateway
 DNS Server 1
 DNS Server 2

☐ Enable
 ☐ Ping
 ☐ HTTP

OK Cancel

WAN Interface

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

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

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP address of the PPPoE connection

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.

Service-On-Demand:

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 network to ping the IP address of the Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If it sets to enable, the device will respond to echo request packets from the WAN network.

WebUI: Select this to allow the device WebUI to be accessed from the WAN 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.



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)

Current Status	Disconnected	Connecting
IP Address	0.0.0.0	Disconnect
User Name	<input type="text"/>	
Password	<input type="text"/>	
IP Address provided by ISP	<input checked="" type="radio"/> Dynamic <input type="radio"/> Fixed	
	IP Address	<input type="text"/>
	Netmask	<input type="text"/>
	Default Gateway	<input type="text"/>

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

☐ Enable
☐ Ping
☐ HTTP

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 the Content Security Gateway from the ISP will be displayed here. This is the IP address of the WAN port of the device.

MAC Address: This is the MAC Address of the device.

Hostname: This will be the name assigned 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.

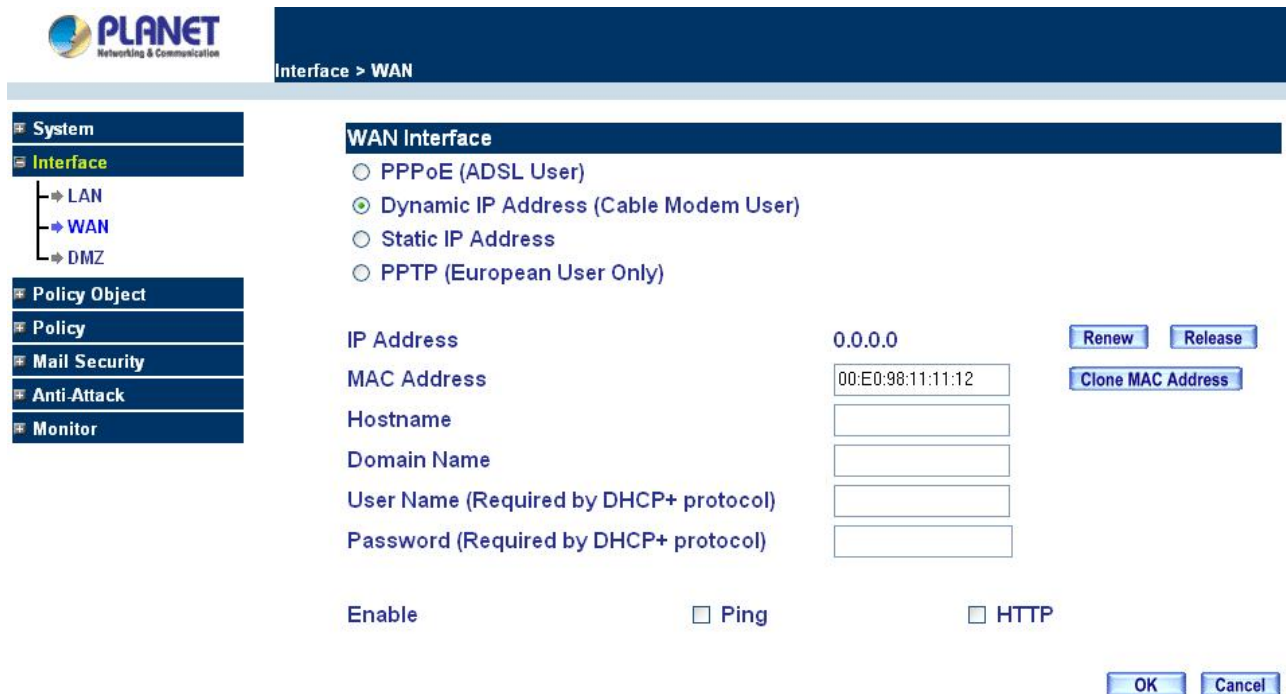
Domain Name: You can specify your own domain name or leave it blank.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

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

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



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: 0.0.0.0 Renew Release
 MAC Address: 00:E0:98:11:11:12 Clone MAC Address
 Hostname:
 Domain Name:
 User Name (Required by DHCP+ protocol):
 Password (Required by DHCP+ protocol):

☐ 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 port of the device.

Netmask: This will be the subnet mask 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.

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

WebUI: Select this to allow the device WebUI to be accessed from the WAN 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.

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: 192.168.99.95
 Netmask: 255.255.255.0
 Default Gateway: 192.168.99.253
 DNS Server 1: 168.95.1.1
 DNS Server 2: 168.95.192.1

☐ Enable
 ☒ Ping
 ☒ HTTP

OK Cancel

For PPTP (European User Only): This is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

IP Address: Enter the static IP address assigned to you by your ISP, or obtain an IP address automatically from ISP.

PPTP Gateway: Enter the PPTP server IP address assigned to you by your ISP.

Connect ID: This is the ID given by ISP. This is optional.

BEZEQ-ISRAEL: Select this item if you are using the service provided by BEZEQ in Israel.

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.

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

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

Content Security Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.1/ Go

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)

Current Status: Disconnected Connecting

IP Address: 0.0.0.0 Disconnect

User Name:

Password:

IP Address provided by ISP: ☒ Obtain an IP address automatically

MAC Address: 00:E0:98:11:11:12 Clone MAC Address

Hostname:

Domain Name:

☐ Use the following IP address

IP Address:

Netmask:

Default Gateway:

PPTP Gateway:

Connect ID:

☐ BEZEQ-ISRAEL
☒ Service-On-Demand

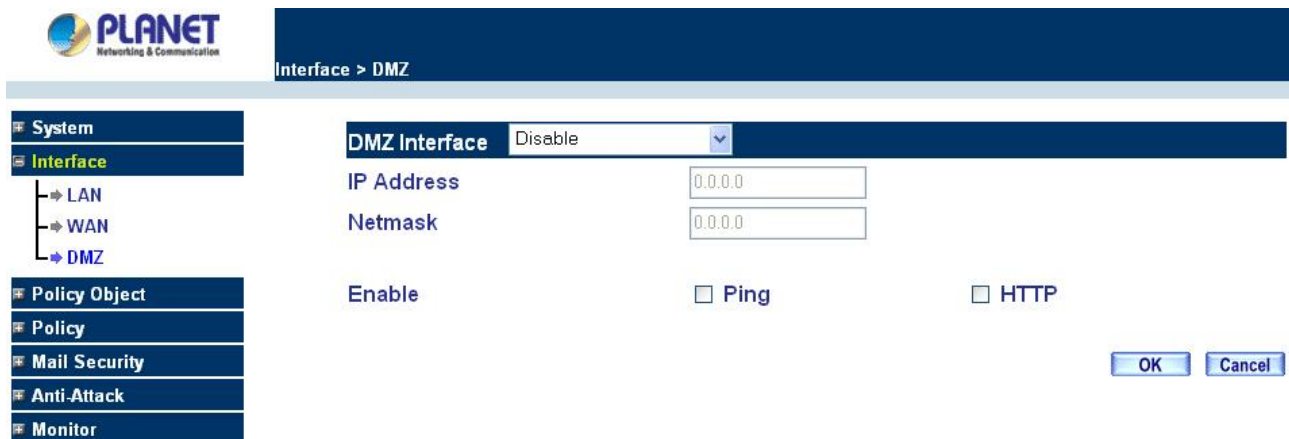
Auto Disconnect if idle: minutes (0 : means always connected)

Enable: ☒ Ping ☐ HTTP

OK Cancel

4.2.3 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.



PLANET
Networking & Communication

Interface > DMZ

System

Interface

- LAN
- WAN
- DMZ

Policy Object

Policy

Mail Security

Anti-Attack

Monitor

DMZ Interface: Disable

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Enable ☐ Ping ☐ HTTP

OK Cancel

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

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

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 Content Security Gateway. This will allow people from the Internet to be able to ping the Content Security Gateway. If set to enable, the device will respond to echo request packets from the DMZ network.

WebUI: 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.

4.3 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 Content Security Gateway Policy. The contents include **Address**, **Service**, **Schedule**, **Content Blocking**, **Virtual server** and **VPN**.

4.3.1 Address

The Content 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.

4.3.1.1 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.

PLANET Networking & Communication

Policy Object > Address > LAN

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

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.

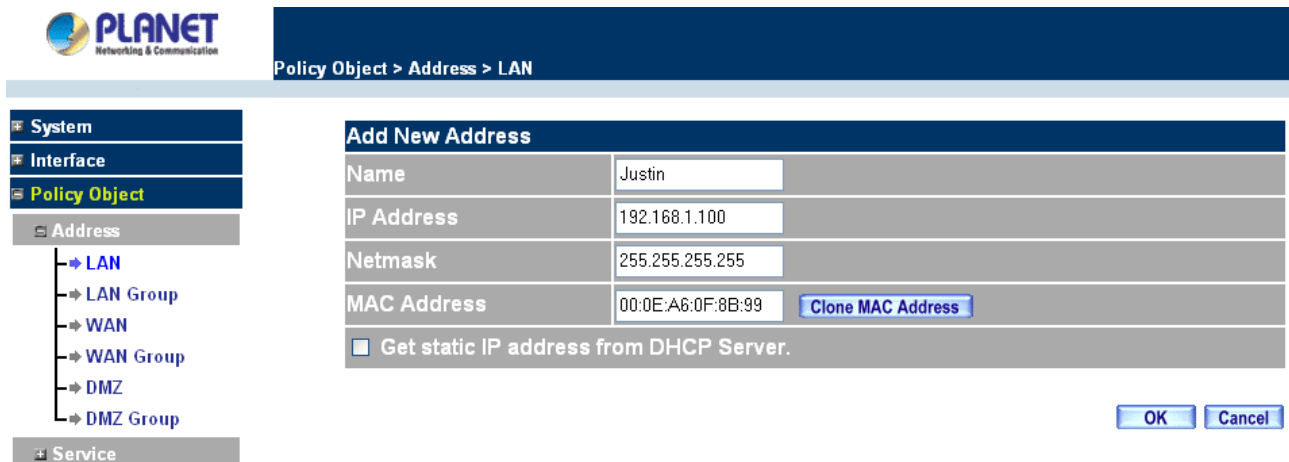
In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

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.

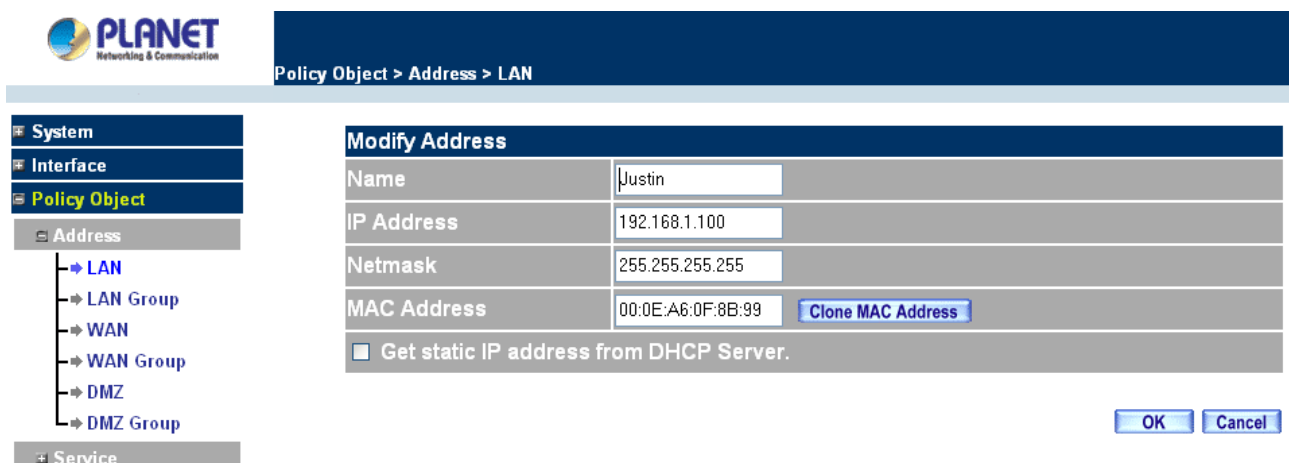


The screenshot shows the PLANET Network & Communication interface. The left sidebar has a tree view with 'System', 'Interface', 'Policy Object', 'Address', and 'Service'. Under 'Address', there are links for LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group. The main area is titled 'Policy Object > Address > LAN' and contains the 'Add New Address' form. The form has fields for Name (Justin), IP Address (192.168.1.100), Netmask (255.255.255.255), and MAC Address (00:0E:A6:0F:8B:99). There is a 'Clone MAC Address' button next to the MAC Address field. Below these fields is a checkbox labeled 'Get static IP address from DHCP Server.' which is currently unchecked. At the bottom right are 'OK' and 'Cancel' buttons.

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



This screenshot is identical to the previous one, showing the 'Add New Address' form. However, the title of the main form area is 'Modify Address' instead of 'Add New Address'. The fields and buttons are the same: Name (Justin), IP Address (192.168.1.100), Netmask (255.255.255.255), MAC Address (00:0E:A6:0F:8B:99) with a 'Clone MAC Address' button, and an unchecked checkbox for 'Get static IP address from DHCP Server.' with 'OK' and 'Cancel' buttons at the bottom right.

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.

PLANET Networking & Communication

Policy Object > Address > LAN

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Justin	192.168.1.100/255.255.255.255	00:0E:A6:0F:8B:99	Modify Remove

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

4.3.1.2 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.

PLANET Networking & Communication

Policy Object > Address > LAN Group

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

New Entry

Definitions (LAN group):

Name: Name of the LAN group.

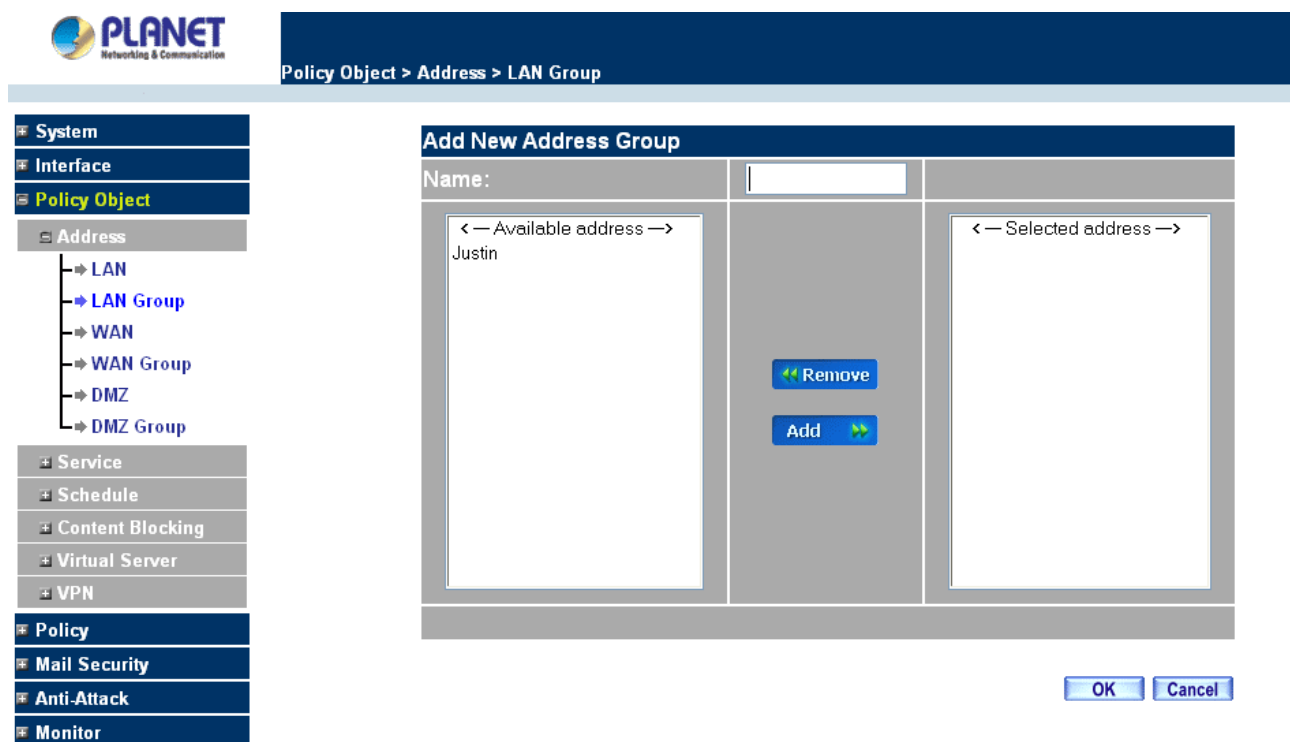
Member: Members of the group.

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

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:
 - n **Available address:** list the names of all the members of the LAN network.
 - n **Selected address:** list the names to be assigned to the new group.
 - n **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:
 - n **Available address:** list names of all members of the LAN network.
 - n **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.

 **Policy Object > Address > LAN Group**

System
Interface
Policy Object
 Address
 → LAN
 → LAN Group
 → WAN
 → WAN Group
 → DMZ
 → DMZ Group
 Service
 Schedule
 Content Blocking
 Virtual Server
 VPN
 Policy
 Mail Security
 Anti-Attack

Modify Address Group

Name: ENM

< — Available address —>
 Justin


< — Selected address —>
 Justin

Remove
Add

OK Cancel

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.

 **Policy Object > Address > LAN Group**

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

Name	Member	Configure
ENM	Justin	Modify Remove

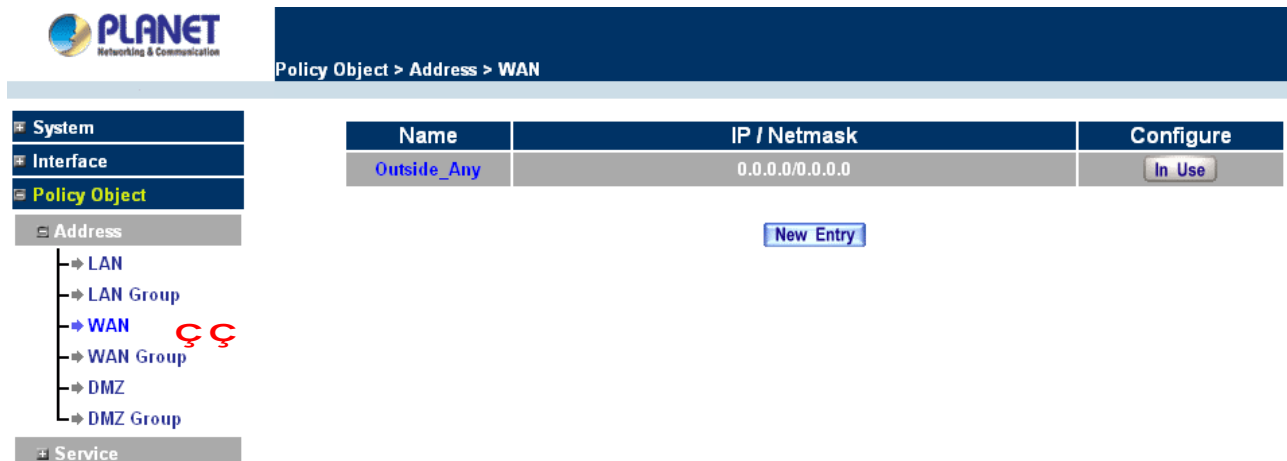
New Entry

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

4.3.1.3 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.



Definitions

Name: Name of WAN network address.

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

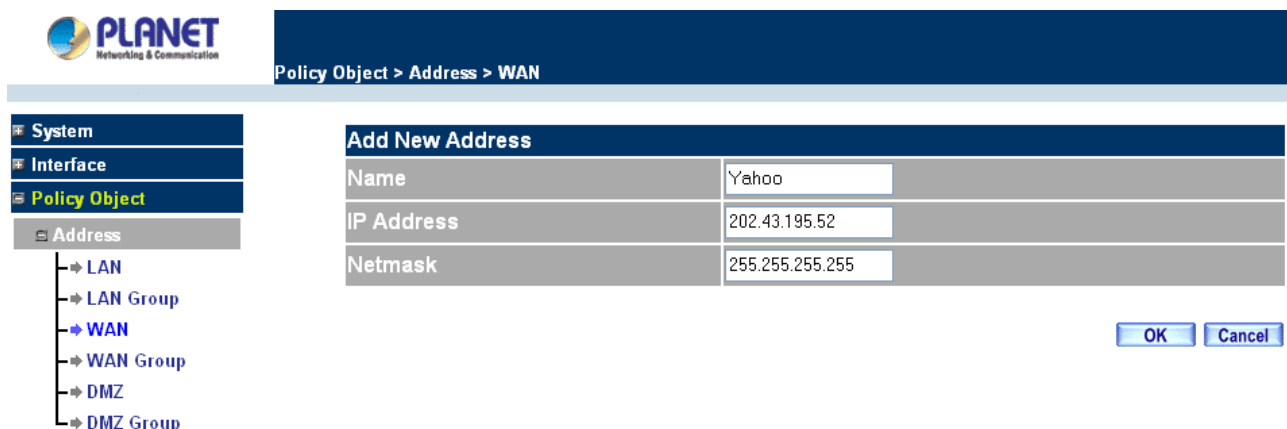
Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network.

Click **Remove** to delete the setting of WAN network.

NOTE: In the WAN Network 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 settings.

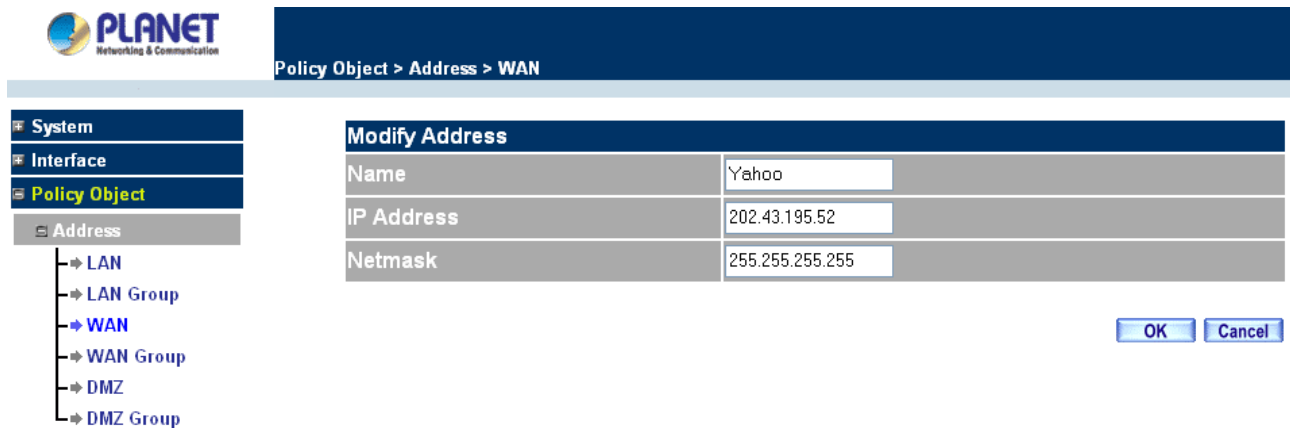
Adding a new WAN Address

- 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.



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



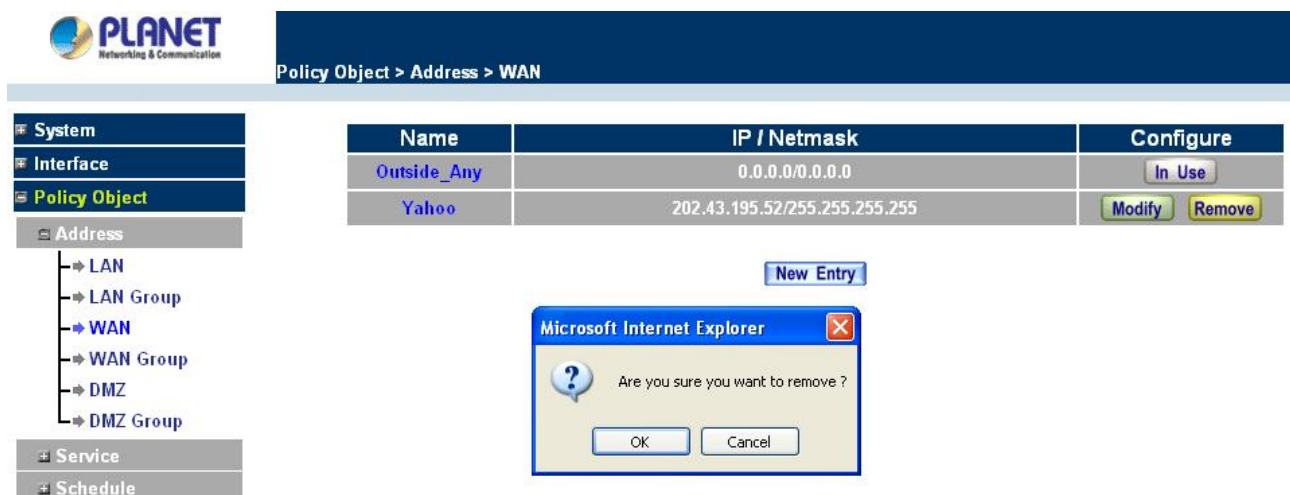
The screenshot shows the PLANET Policy Object > Address > WAN configuration window. On the left is a tree view with 'Policy Object' selected, and 'Address' expanded to show 'WAN'. The main area displays the 'Modify Address' dialog with the following fields:

Modify Address	
Name	Yahoo
IP Address	202.43.195.52
Netmask	255.255.255.255

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

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.



The screenshot shows the PLANET Policy Object > Address > WAN configuration window. On the left is a tree view with 'Policy Object' selected, and 'Address' expanded to show 'WAN'. The main area displays a table with WAN addresses:

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
Yahoo	202.43.195.52/255.255.255.255	Modify Remove

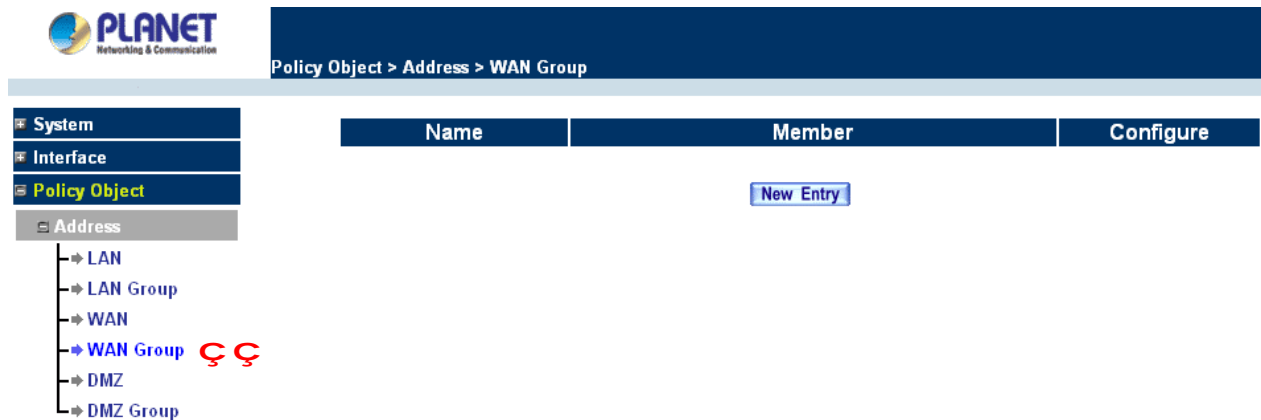
Below the table is a 'New Entry' button. A confirmation dialog box titled 'Microsoft Internet Explorer' is displayed, asking 'Are you sure you want to remove?' with 'OK' and 'Cancel' buttons.

4.3.1.4 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.

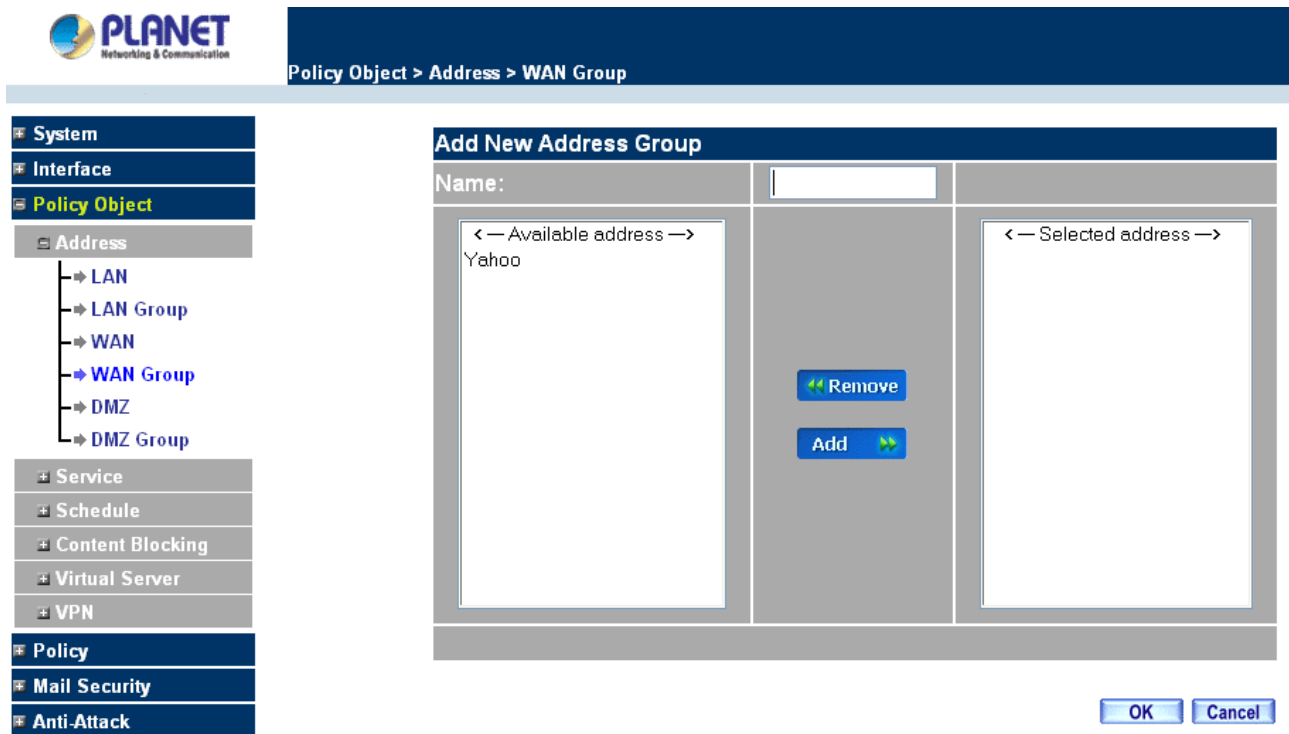
Adding an WAN Group

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:


- n **Name:** enter the name of the new group.
- n **Available address:** List the names of all the members of the WAN network.
- n **Selected address:** List the names to assign to the new group.
- n **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.
- n **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.



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:
 - n **Available address:** list the names of all the members of the WAN network.
 - n **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.



Policy Object > Address > WAN Group

- System
- Interface
- Policy Object
 - Address
 - LAN
 - LAN Group
 - WAN
 - WAN Group
 - DMZ
 - DMZ Group
 - Service
 - Schedule
 - Content Blocking
 - Virtual Server
 - VPN
- Policy
- Mail Security
- Anti-Attack

Modify Address Group

Name: Web

← Available address →
Yahoo


Remove
Add

← Selected address →
Yahoo

OK Cancel

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.



Policy Object > Address > WAN Group

- System
- Interface
- Policy Object
 - Address
 - LAN
 - LAN Group
 - WAN
 - WAN Group
 - DMZ
 - DMZ Group
 - Service
 - Schedule

Name	Member	Configure
Web	Yahoo	Modify Remove

New Entry

Microsoft Internet Explorer

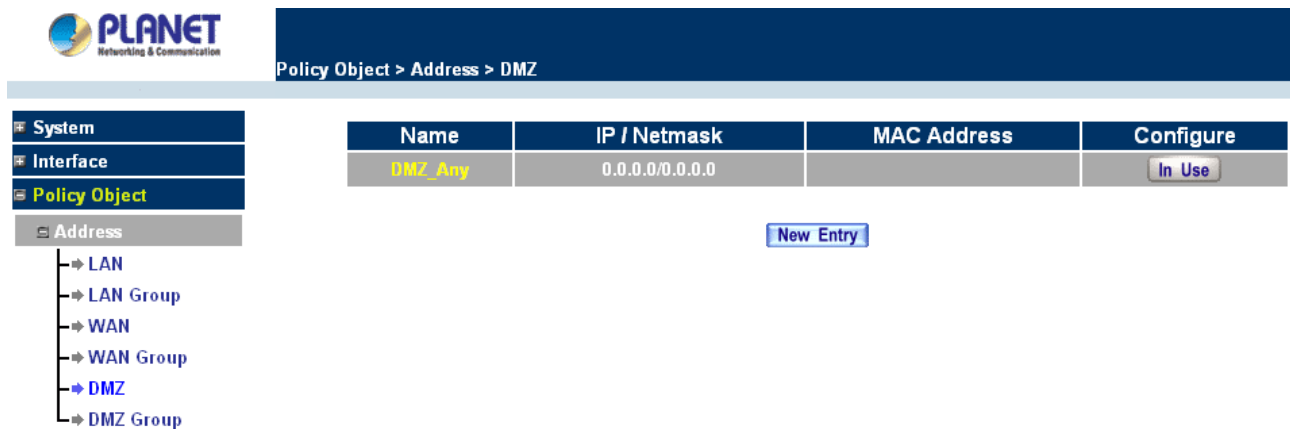
Are you sure you want to remove ?

OK Cancel

4.3.1.5 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.

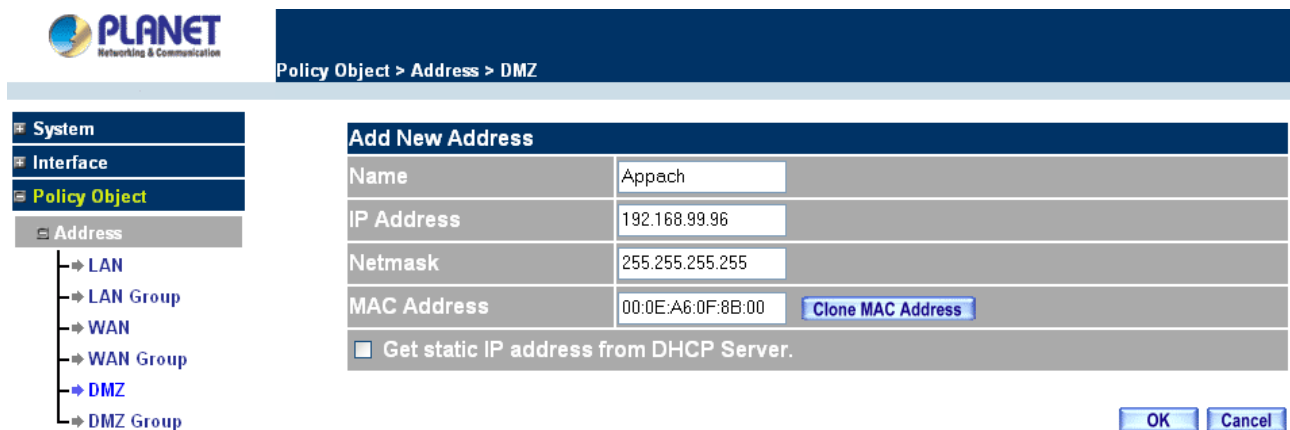


Adding a new DMZ Address:

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.




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.



Policy Object > Address > DMZ

System

Interface

Policy Object

Address

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

Service

Schedule

Modify Address

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.	

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

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.



Policy Object > Address > DMZ

System

Interface

Policy Object

Address

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

Service

Schedule

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

[New Entry](#)

Microsoft Internet Explorer

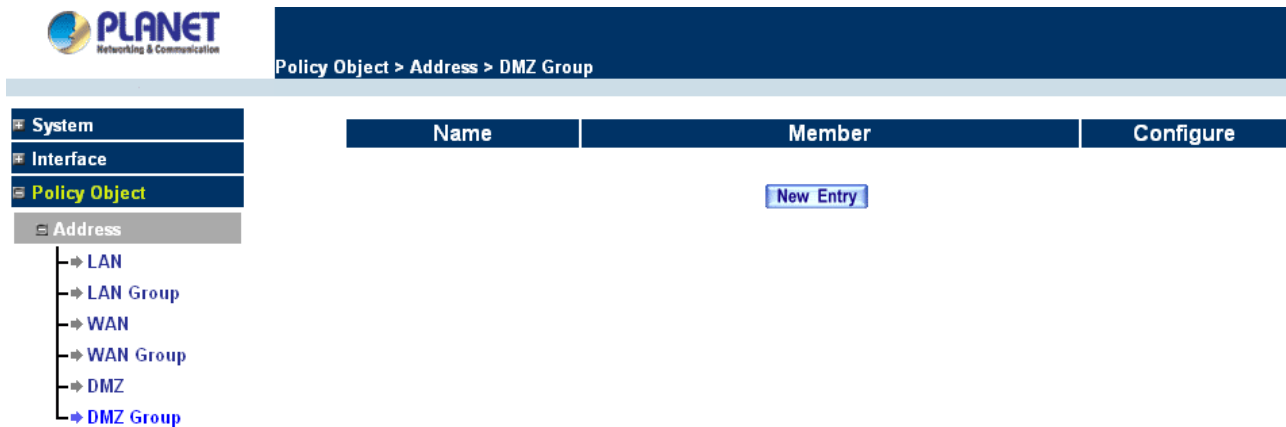
Are you sure you want to remove ?

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

4.3.1.6 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.



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:

- n **Available address:** list names of all members of the DMZ.
- n **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.

The screenshot shows the PLANET Content Security Gateway web interface. On the left is a navigation tree with categories: System, Interface, Policy Object, Address, Service, Schedule, Content Blocking, Virtual Server, VPN, Policy, Mail Security, and Anti-Attack. The 'Policy Object' category is expanded, showing 'Address' and its sub-items: LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group. The 'DMZ Group' is selected. The main area displays the 'Add New Address Group' dialog box. It has a 'Name:' field at the top. Below it are two lists: '← Available address →' containing 'Appach' and '← Selected address →' which is empty. Between the lists are 'Remove' and 'Add' buttons. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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.

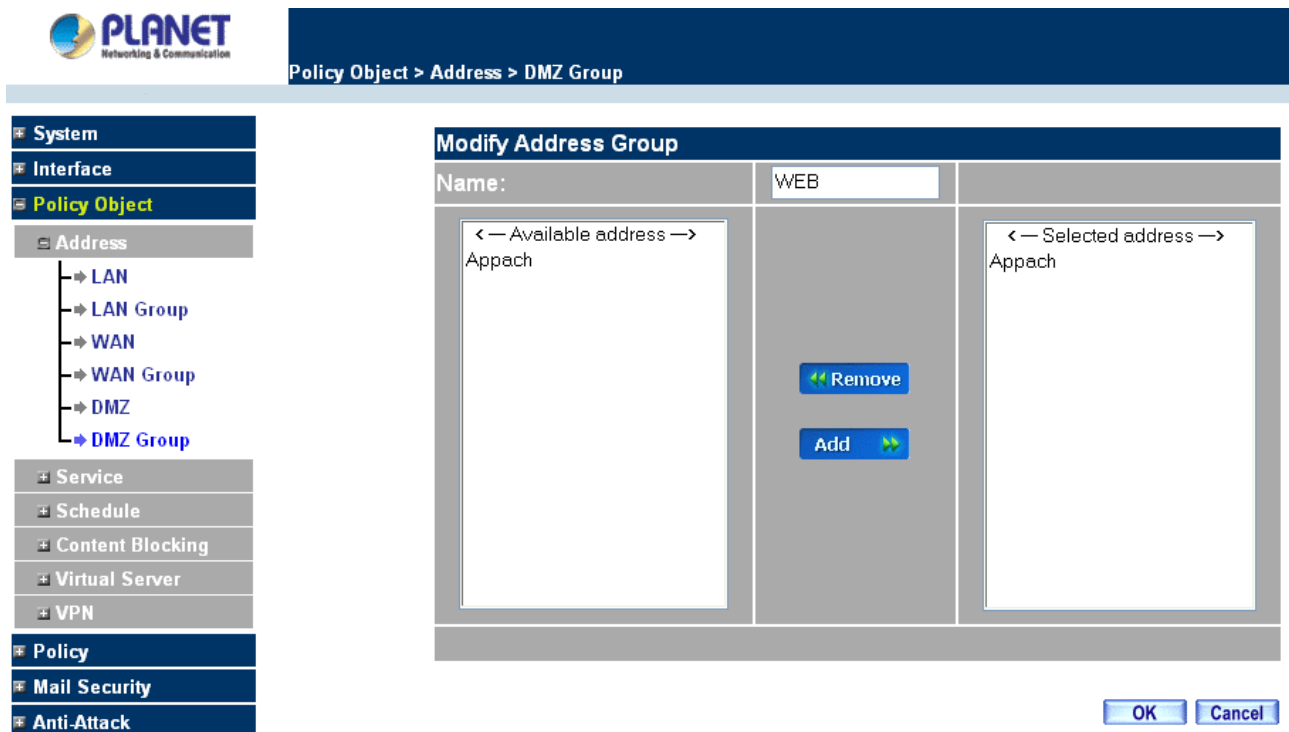
Step 2. A window displaying information about the selected group appears:

- n **Available address:** list the names of all the members of the DMZ.
- n **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.

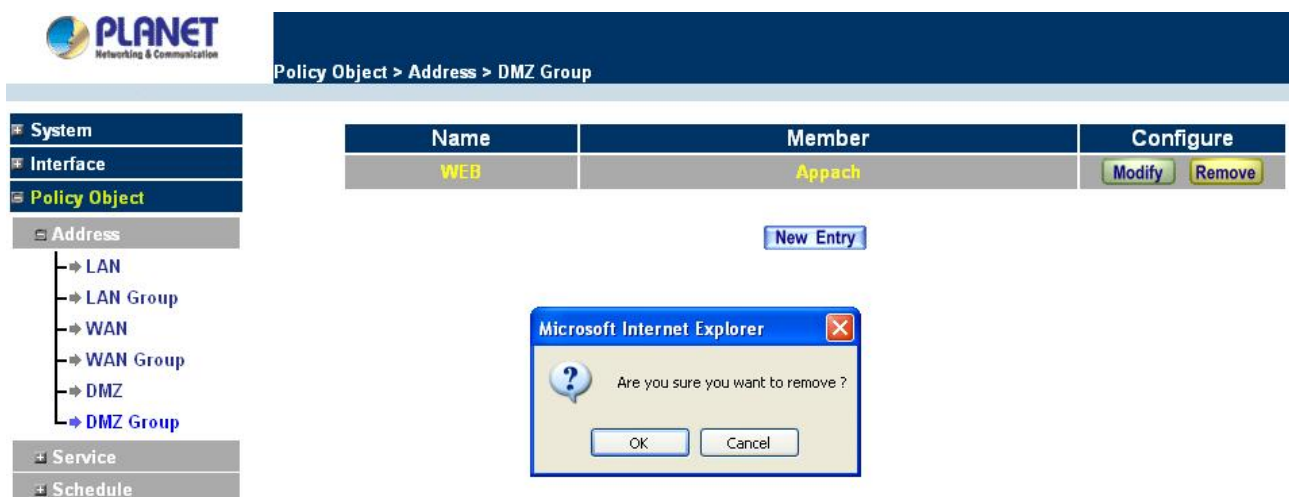
Step 4. Remove members: Select names to be removed from the **Selected address** list, and click the **<<Remove** button to remove them from **Selected address** list.

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.



4.3.2 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 Content 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.

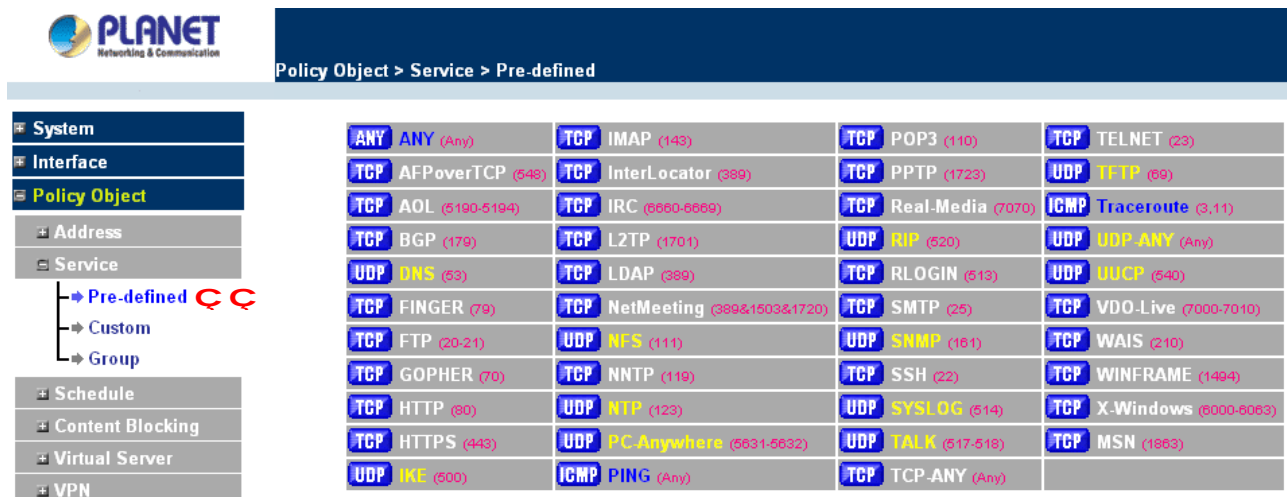
How do I use Service?

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.

4.3.2.1 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.






The screenshot shows the PLANET Policy Object > Service > Pre-defined window. On the left is a navigation menu with options: System, Interface, Policy Object (selected), Address, Service (expanded), Schedule, Content Blocking, Virtual Server, and VPN. Under the Service menu, 'Pre-defined' is selected. The main area displays a table of pre-defined services:

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

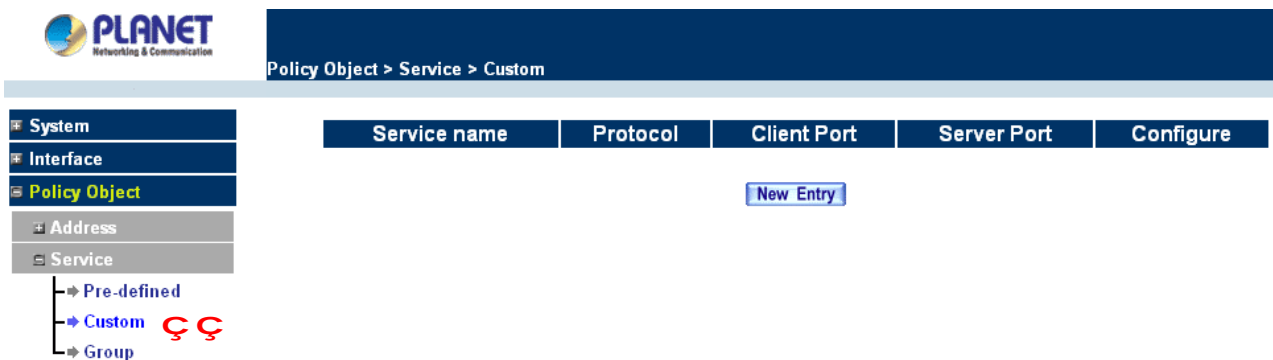
Figure	Description
--------	-------------

	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.

4.3.2.2 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.

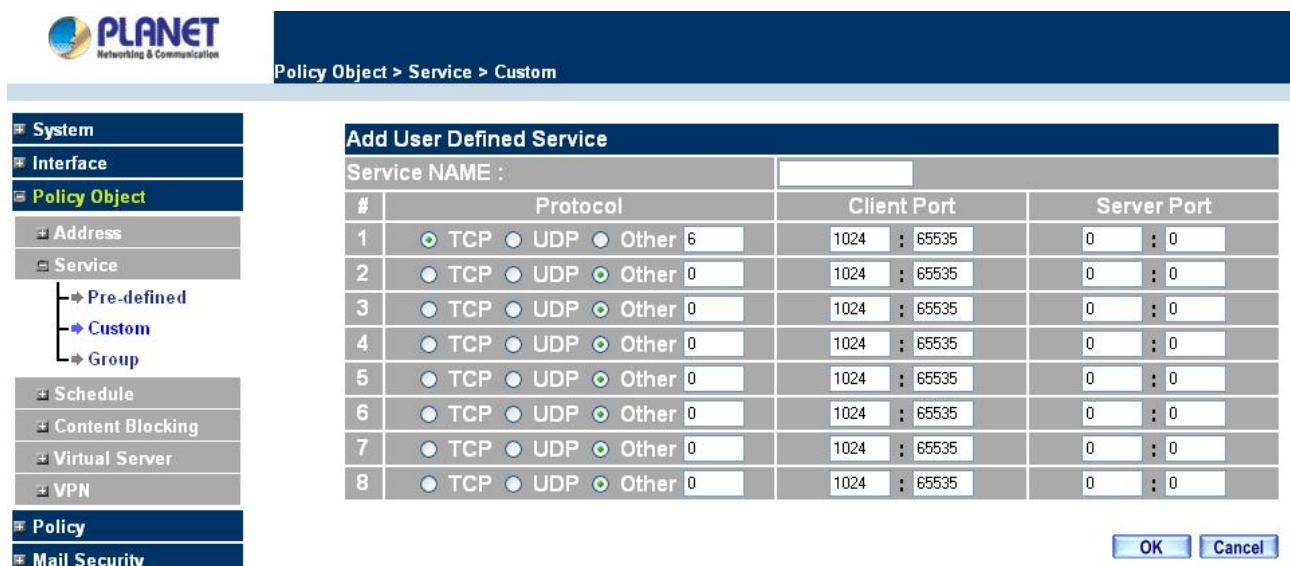
In the new service table:

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

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

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

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



The screenshot shows the PLANET Networking & Communication interface. The breadcrumb trail is 'Policy Object > Service > Custom'. On the left is a navigation tree with 'Policy Object' selected, containing sub-items like 'Address', 'Service', 'Schedule', 'Content Blocking', 'Virtual Server', 'VPN', 'Policy', and 'Mail Security'. The 'Service' item is expanded, showing 'Pre-defined' and 'Custom' (selected). The main area is titled 'Add User Defined Service' and contains a table with 8 rows. Each row has columns for '#', 'Protocol' (with radio buttons for TCP, UDP, and Other), and two port range fields: 'Client Port' and 'Server Port'. The first row is pre-filled with '6' for the protocol number, '1024 : 65535' for the client port, and '0 : 0' for the server port. At the bottom right are 'OK' and 'Cancel' buttons.


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 6	1024 : 65535	0 : 0
2	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
3	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0

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**.



Policy Object > Service > Custom

System

Interface

Policy Object

Address

Service

Pre-defined

Custom

Group

Schedule

Content Blocking

Virtual Server

VPN

Policy

Mail Security

Modify User Defined Service


Service NAME : eDonkey

#	Protocol	Client Port	Server Port
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	1024 : 65535	4661 : 4665
2	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
3	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	1024 : 65535	0 : 0

OK Cancel

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.



Policy Object > Service > Custom

System

Interface

Policy Object

Address

Service

Pre-defined

Custom

Group

Schedule

Content Blocking

Virtual Server

VPN

Policy

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	1024:65535	4661:4665	<div>Modify</div> <div>Remove</div>

New Entry

Microsoft Internet Explorer

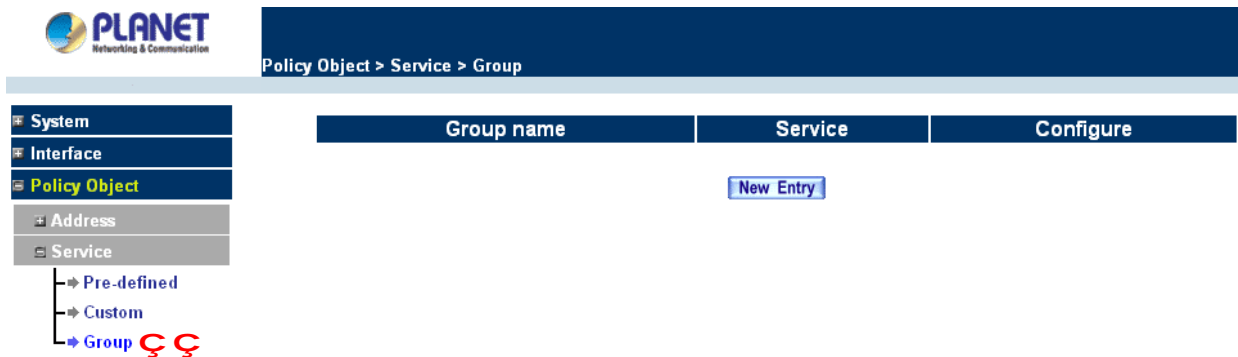
Are you sure you want to remove ?

OK Cancel

4.3.2.3 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.



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:

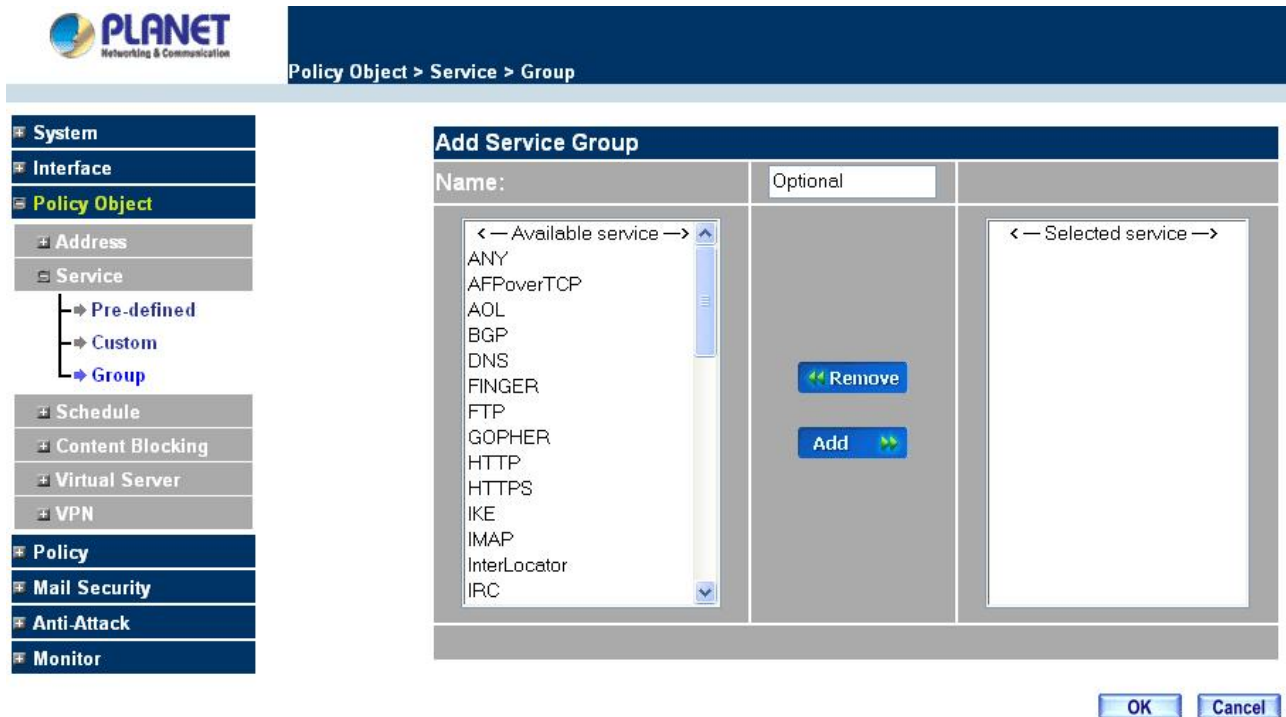
- n **Available service:** list all the available services.
- n **Selected service:** list services to be assigned to the new group.

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

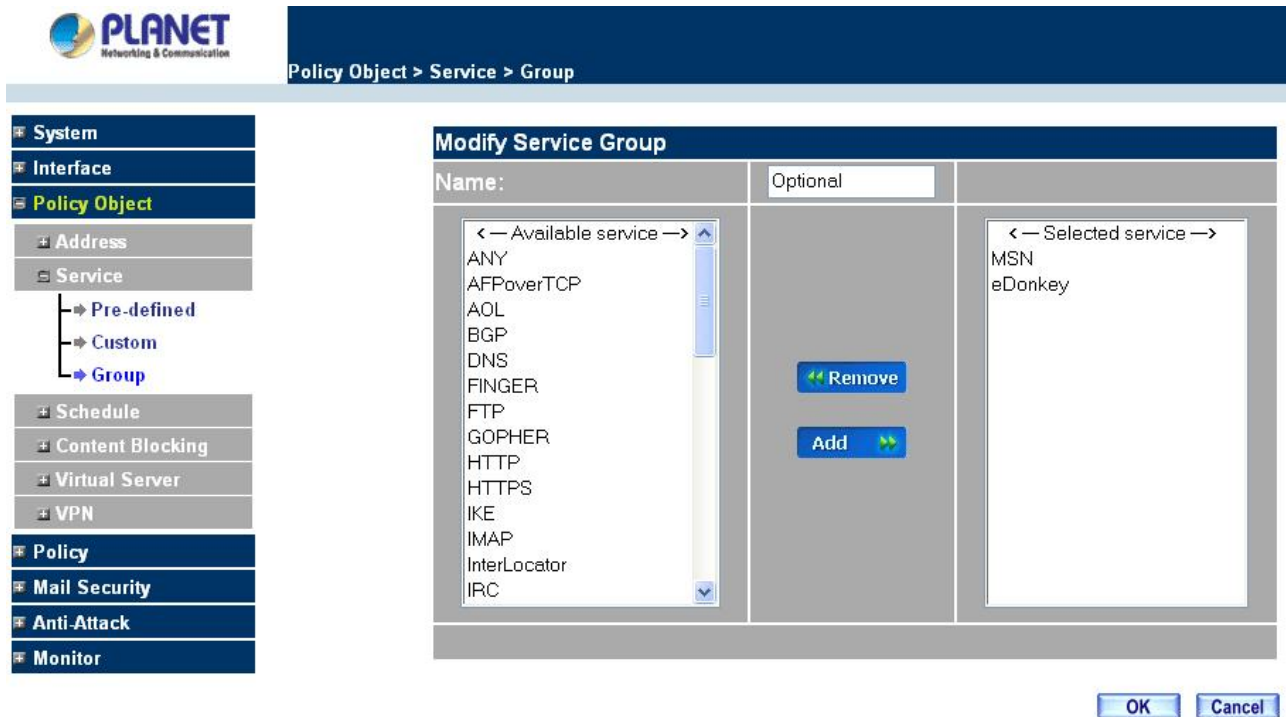
Step 1. In the Mod (modify) group window the following fields are displayed:

- n **Available service:** lists all the available services.
- n **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.

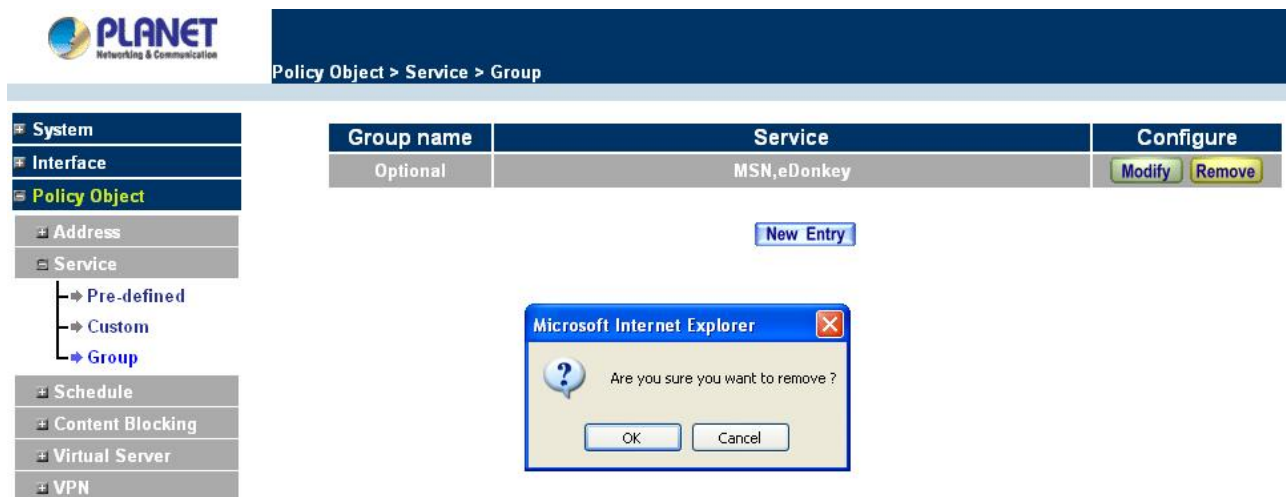
Step 3. Remove services: Select services to be removed in the **Selected service** list, and then click the **<<Remove** button to remove these services from the group.

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.



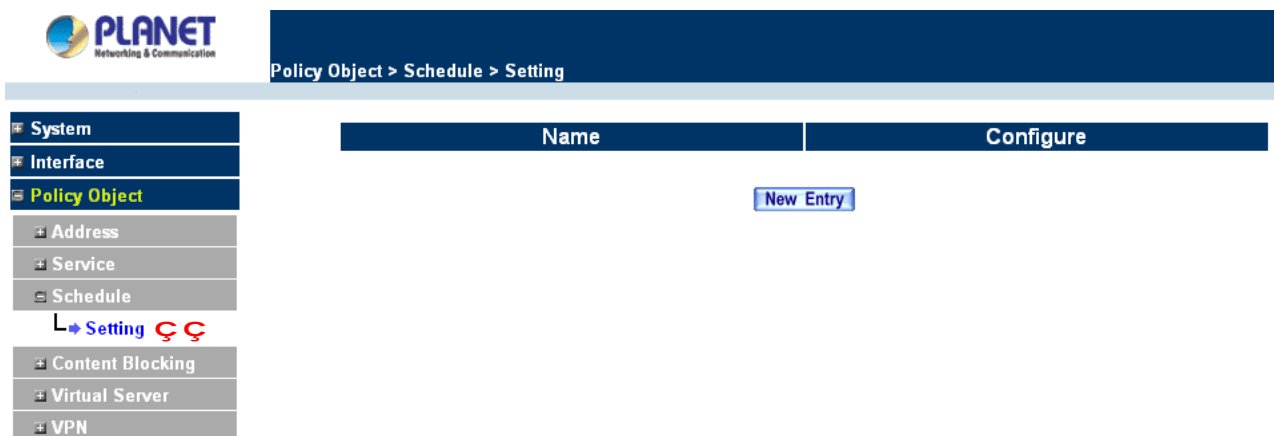
4.3.3 Schedule

The Content Security Gateway allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Content Security Gateway policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Content Security Gateway policies therefore will likely not be permitted to pass through the Content 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 Content 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 Content Security Gateway to work Monday-Friday, 8AM - 5PM only. During the non-work hours, the Content 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.

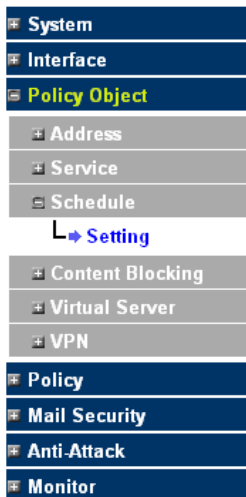
n Schedule Name: Fill in a name for the new schedule.

n 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.



Policy Object > Schedule > Setting



Add New Schedule

Schedule Name

Work-Time

Week Day	Period	
	Start Time	Stop Time
Monday	08:00	22:00
Tuesday	08:00	22:00
Wednesday	08:00	22:00
Thursday	08:00	22:00
Friday	08:00	22:00
Saturday	Disable	Disable
Sunday	Disable	Disable

OK

Cancel

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.



Policy Object > Schedule > Setting



Modify Schedule

Schedule Name

Work-Time

(ex: Schedule_1)

Week Day	Period	
	Start Time	Stop Time
Monday	08:00	22:00
Tuesday	08:00	22:00
Wednesday	08:00	22:00
Thursday	08:00	22:00
Friday	08:00	22:00
Saturday	Disable	Disable
Sunday	Disable	Disable

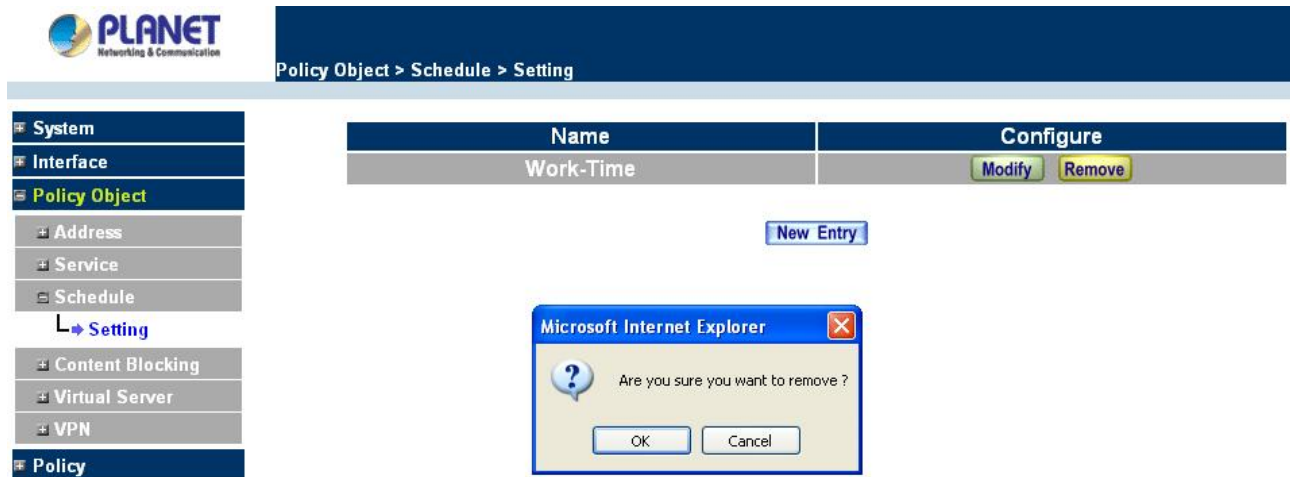
OK

Cancel

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.



4.3.4 Content Blocking

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

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.

4.3.4.1 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 an 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**.



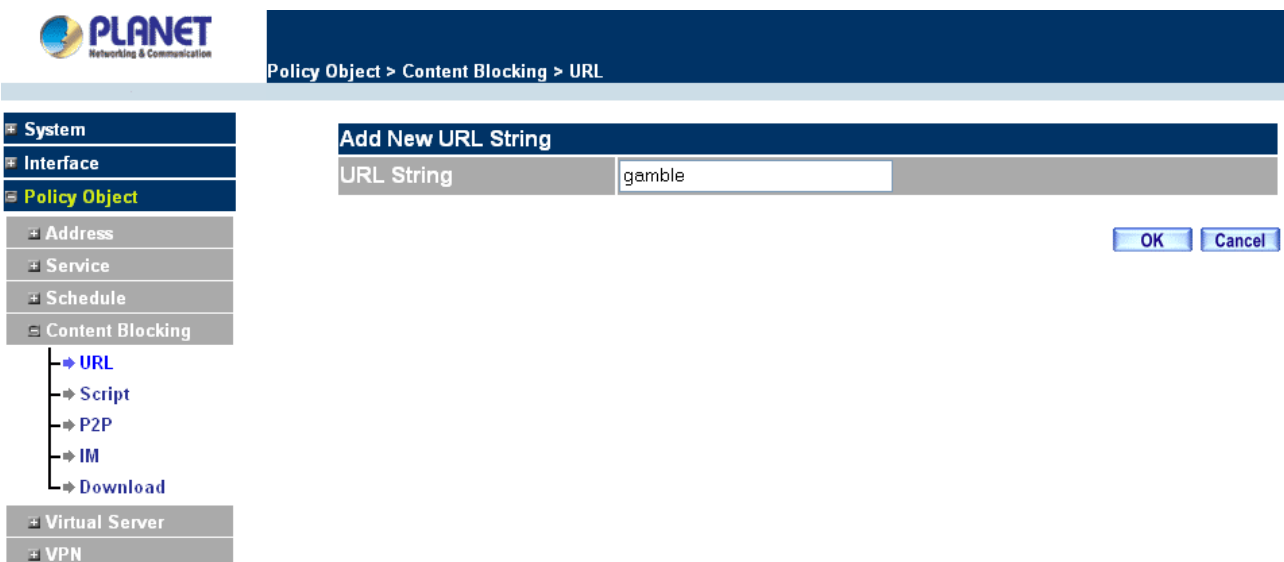
Definition:

URL String: The domain name that is blocked to enter by Content 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.



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.



4.3.4.2 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:

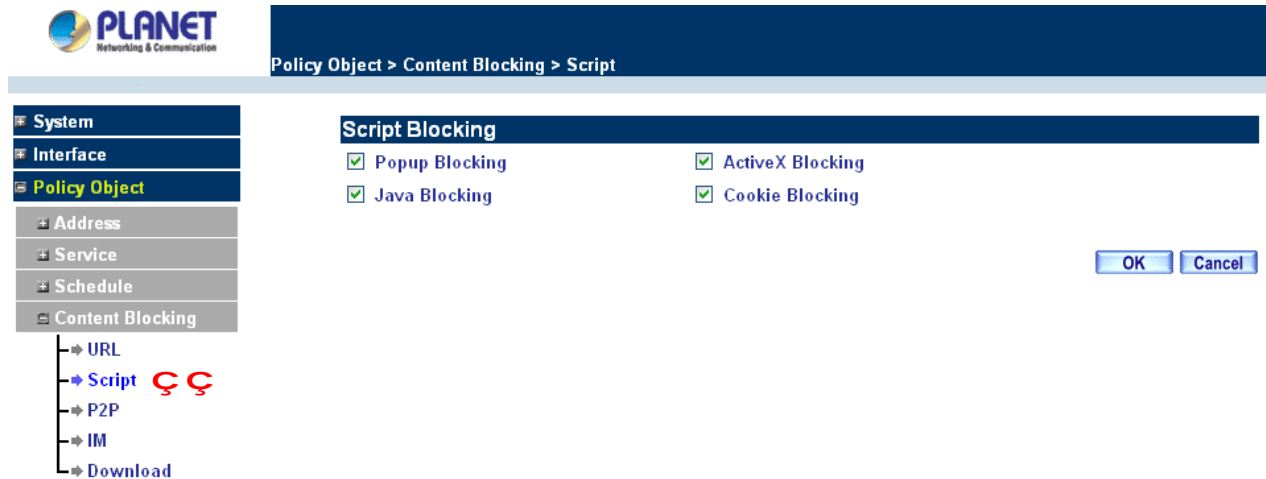
Popup Blocking: Prevent pop-up boxes from appearing.

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.



When the system detects the setting, the Content Security Gateway will spontaneously work.

4.3.4.3 P2P

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

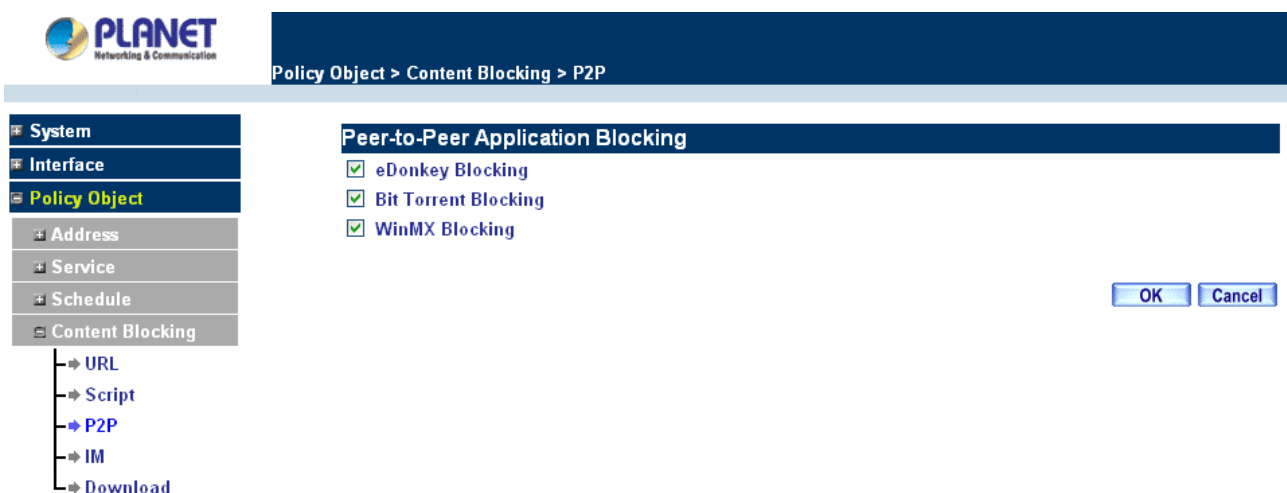
Step 2: Select **P2P** detective functions:

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.



4.3.4.4 IM

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

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

MSN Messenger Blocking: To select to block MSN Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

Yahoo Messenger Blocking: To select to block Yahoo Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

ICQ Blocking: Only to select to block ICQ **login**.

QQ Blocking: Only to select to block ICQ **login**.

Skype Messenger Blocking: To select to block Skype Messenger **login**, **File Transfer**, **Voice** or **Camera** transferring.

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



4.3.4.5 Download

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

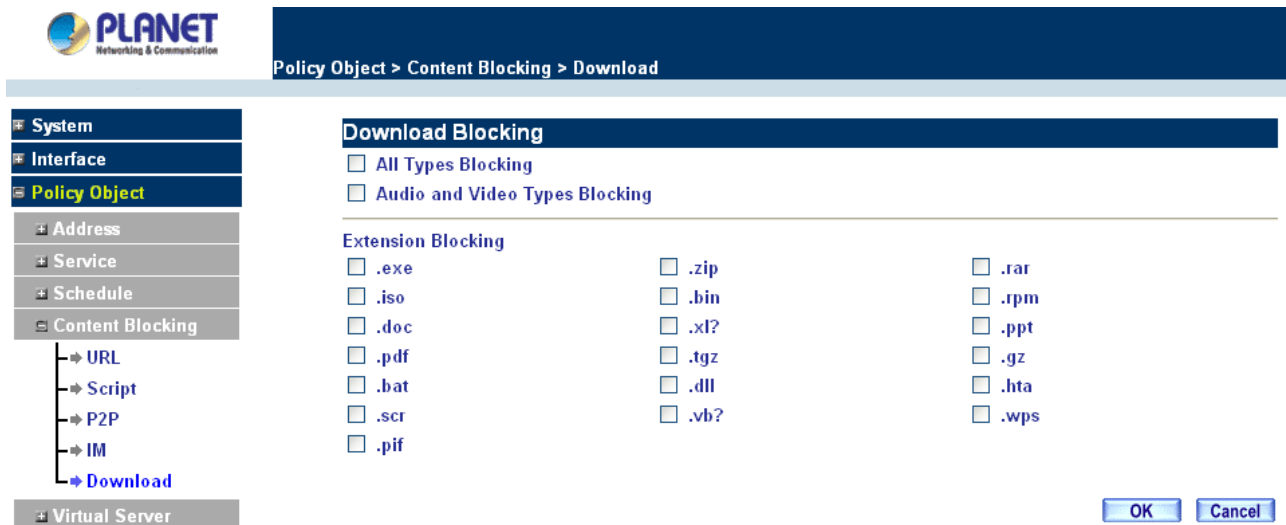
Step 2: Select **Download** detective functions:

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.



4.3.5 Virtual Server

The Content 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 Content 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 Content Security Gateway's Virtual Server can solve this problem. A virtual server has set the real IP address of the Content Security Gateway's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Content 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:

- n 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.

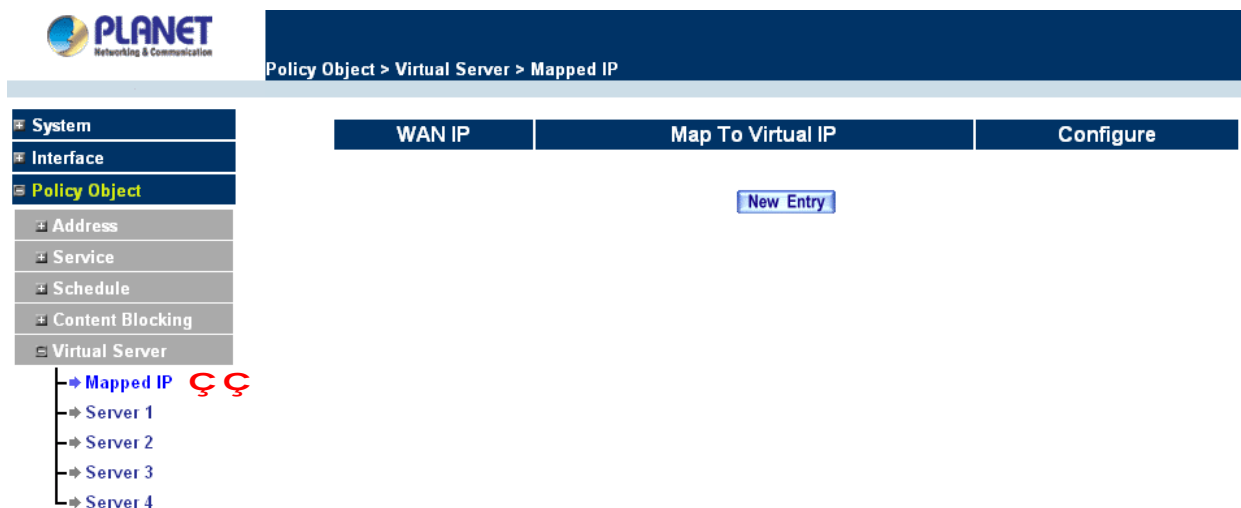
- n Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- n IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of 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.

4.3.5.1 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.

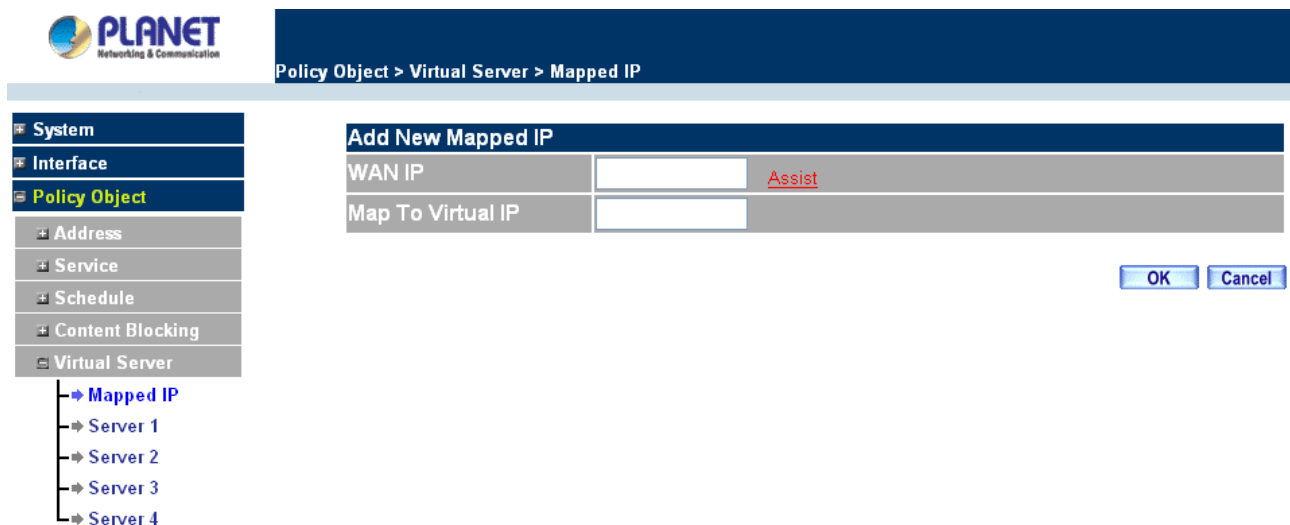
Adding a new IP Mapping

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

n **WAN IP:** select the WAN public IP address to be mapped.

n **Internal 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.



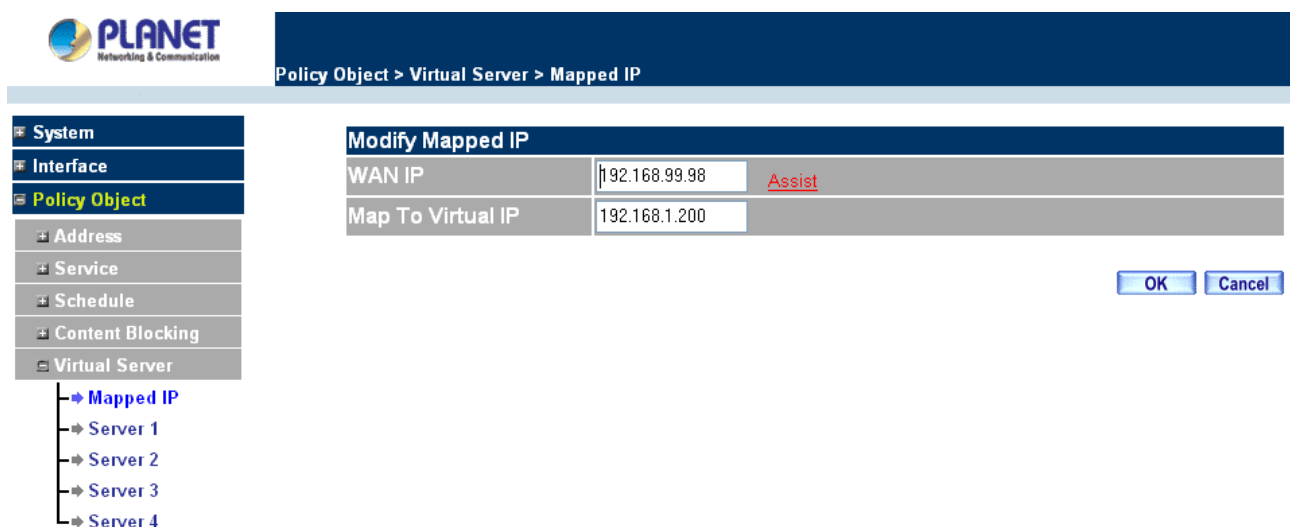
The screenshot shows the PLANET Network & Communication web interface. The breadcrumb navigation at the top reads "Policy Object > Virtual Server > Mapped IP". On the left, a sidebar menu is expanded to "Virtual Server", which contains sub-items: "Mapped IP", "Server 1", "Server 2", "Server 3", and "Server 4". The "Mapped IP" item is selected. The main content area displays the "Add New Mapped IP" dialog box. This dialog has two input fields: "WAN IP" and "Map To Virtual IP". The "WAN IP" field has a red "Assist" link next to it. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Modifying a Mapped IP

Step 1. In the **Mapped IP** table, locate the Mapped IP you want it 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.



The screenshot shows the PLANET Network & Communication web interface. The breadcrumb navigation at the top reads "Policy Object > Virtual Server > Mapped IP". On the left, the sidebar menu is the same as in the previous screenshot, with "Mapped IP" selected. The main content area displays the "Modify Mapped IP" dialog box. This dialog has two input fields: "WAN IP" and "Map To Virtual IP". The "WAN IP" field contains the value "192.168.99.98" and has a red "Assist" link next to it. The "Map To Virtual IP" field contains the value "192.168.1.200". At the bottom right of the dialog are "OK" and "Cancel" buttons.

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 Networking & Communication

Policy Object > Virtual Server > Mapped IP

System	Interface	Policy Object	Address	Service	Schedule	Content Blocking	Virtual Server
							<ul style="list-style-type: none"> Mapped IP Server 1 Server 2 Server 3 Server 4

WAN IP	Map To Virtual IP	Configure
192.168.99.98	192.168.1.200	Modify Remove

New Entry

Microsoft Internet Explorer

Are you sure you want to remove?

OK Cancel

4.3.5.2 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 Networking & Communication

Policy Object > Virtual Server > Server 1

System	Interface	Policy Object	Address	Service	Schedule	Content Blocking	Virtual Server
							<ul style="list-style-type: none"> Mapped IP Server 1 Server 2 Server 3 Server 4

Virtual Server Real IP click here to configure

Service	WAN Port	Server Virtual IP	Configure

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 names 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.

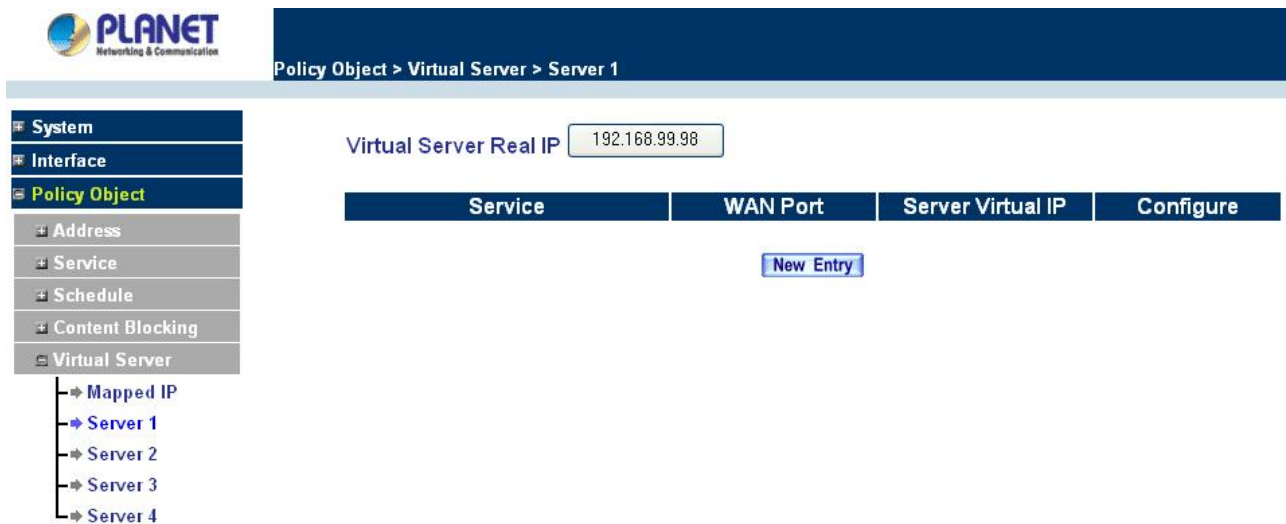
Configuring a Real IP for a Virtual Server

- 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 Network & Communication web interface. The breadcrumb navigation at the top reads "Policy Object > Virtual Server > Server 1". On the left sidebar, the "Policy Object" menu is expanded, and "Virtual Server" is selected, showing a list of servers: "Mapped IP", "Server 1", "Server 2", "Server 3", and "Server 4". "Server 1" is highlighted. The main content area displays "Virtual Server Real IP" with a text box containing "192.168.99.98". 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 same PLANET Network & Communication web interface. The breadcrumb navigation remains "Policy Object > Virtual Server > Server 1". The left sidebar is identical. The main content area now displays a dialog titled "Add New Virtual Server IP". It has a "Virtual Server Real IP" label and a text box. To the right of the text box is a red "Assist" link. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Setting the Virtual Server's services

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

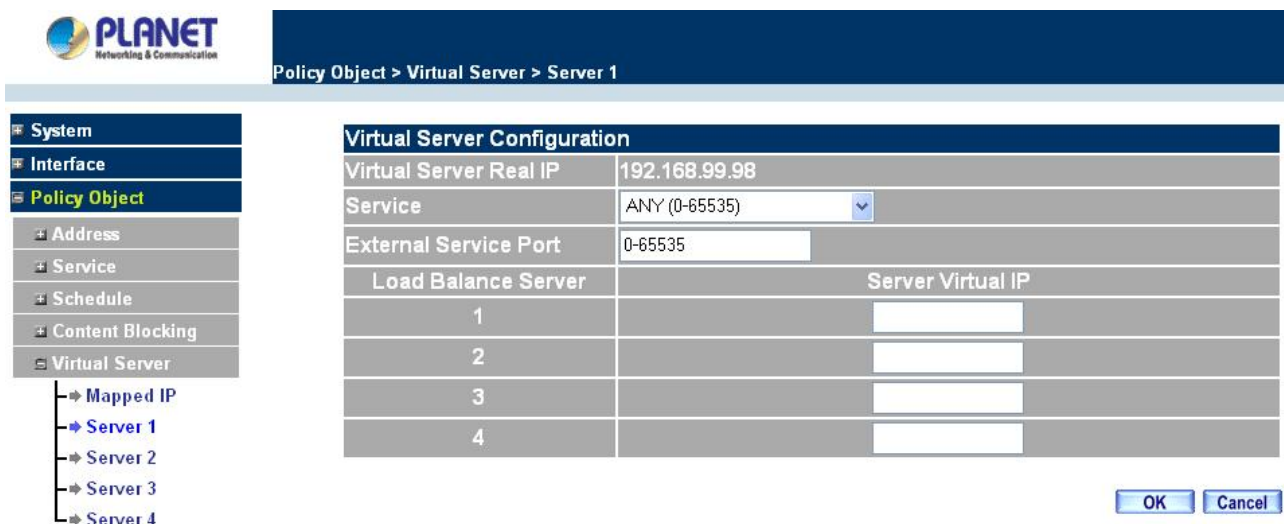
Step 2. In the Virtual Server Configurations window:

- n **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- n **Service (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- n **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.
- n **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.

Step 3. Enter the IP address of the LAN network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

NOTE: The services in the drop-down list are all defined in the Pre-defined and Custom section of the **Service** menu.



The screenshot shows the PLANET Network & Communication software interface. On the left is a navigation tree with the following items: System, Interface, Policy Object (selected), Address, Service, Schedule, Content Blocking, and Virtual Server. Under Virtual Server, there are sub-items: Mapped IP, Server 1 (selected), Server 2, Server 3, and Server 4. The main window displays the 'Virtual Server Configuration' for 'Server 1'. The configuration fields are as follows:

Virtual Server Configuration	
Virtual Server Real IP	192.168.99.98
Service	ANY (0-65535)
External Service Port	0-65535
Load Balance Server	Server Virtual IP
1	
2	
3	
4	

At the bottom right of the configuration window 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	192.168.99.98
Policy Object	Service	HTTP (80) <input type="button" value="v"/>
+ Address	External Service Port	80 <input type="text"/>
+ Service	Load Balance Server	Server Virtual IP
+ Schedule	1	192.168.1.20 <input type="text"/>
+ Content Blocking	2	192.168.1.21 <input type="text"/>
+ Virtual Server	3	192.168.1.22 <input type="text"/>
→ Mapped IP	4	192.168.1.23 <input type="text"/>
→ Server 1		
→ Server 2		
→ Server 3		
→ Server 4		
	<input type="button" value="OK"/> <input type="button" value="Cancel"/>	


- n **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- n **Service (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- n **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.
- n **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.

Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.

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

Content Blocking

Virtual Server

→ Mapped IP

→ **Server 1**

→ Server 2

→ Server 3

→ Server 4

Virtual Server Configuration	
Virtual Server Real IP	192.168.99.98
Service	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.20
2	192.168.1.21
3	192.168.1.22
4	192.168.1.23

OK Cancel


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

Content Blocking

Virtual Server

→ Mapped IP

→ **Server 1**

→ Server 2

→ Server 3

→ Server 4

Virtual Server Real IP 192.168.99.98

Service	WAN Port	Server Virtual IP	Configure
HTTP (80)	80	192.168.1.20 192.168.1.21 192.168.1.22 192.168.1.23	Modify Remove

Microsoft Internet Explorer

Are you sure you want to remove ?

OK Cancel

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.

4.3.6 VPN

The CS-500 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-500 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-500.

PPTP Server: The System Manager can set up VPN-PPTP Server functions at CS-500 in this chapter.

PPTP Client: The System Manager can set up VPN-PPTP Client functions at CS-500 in this chapter.

What is VPN?

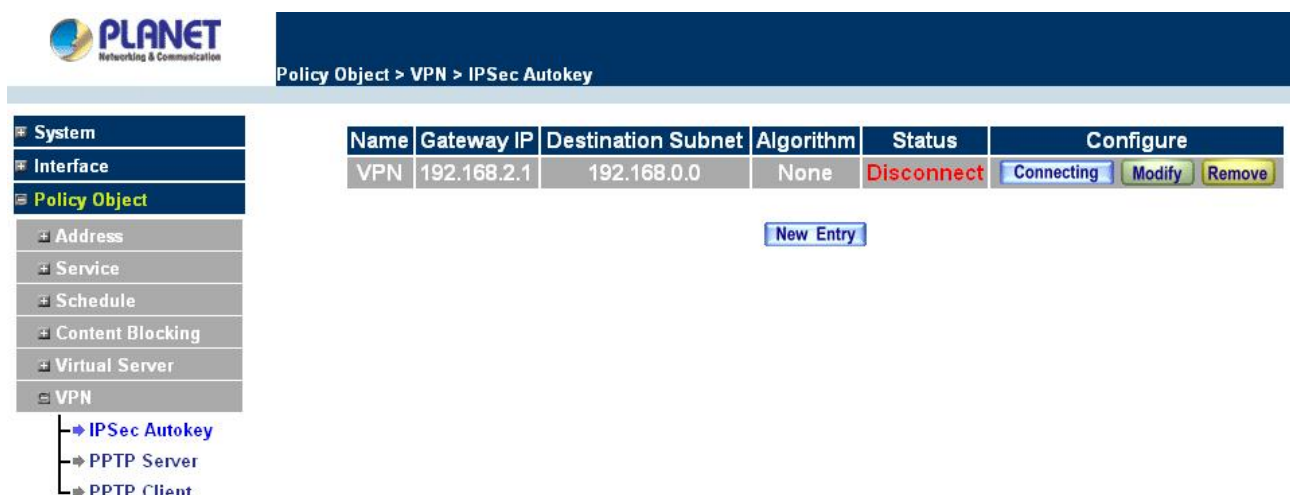
To set up a **Virtual Private Network** (VPN), you don't need to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet, Destination Gateway, Destination Subnet, Authentication Method, Preshare key, Encapsulation and IPSec lifetime. The Content Security Gateway with the other Gateway on both ends must use the same **Preshare** key and **IPSec** lifetime to make a **VPN** connection.

4.3.6.1 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 Content 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 screenshot shows the PLANET Network & Communication management interface. The breadcrumb navigation at the top reads "Policy Object > VPN > IPSec Autokey". On the left, a sidebar menu shows the "VPN" category expanded, with "IPSec Autokey" selected. The main content area displays a table of configured VPNs:

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN	192.168.2.1	192.168.0.0	None	Disconnect	Connecting Modify Remove

Below the table is a "New Entry" button.

The fields in the IPsec Autokey window are:

n Name: The VPN name to identify the VPN tunnel definition. The name must be different for the two sites creating the tunnel.

n Gateway IP: The other side WAN interface IP address of VPN Gateway.

n Destination Subnet: Destination LAN network subnet.

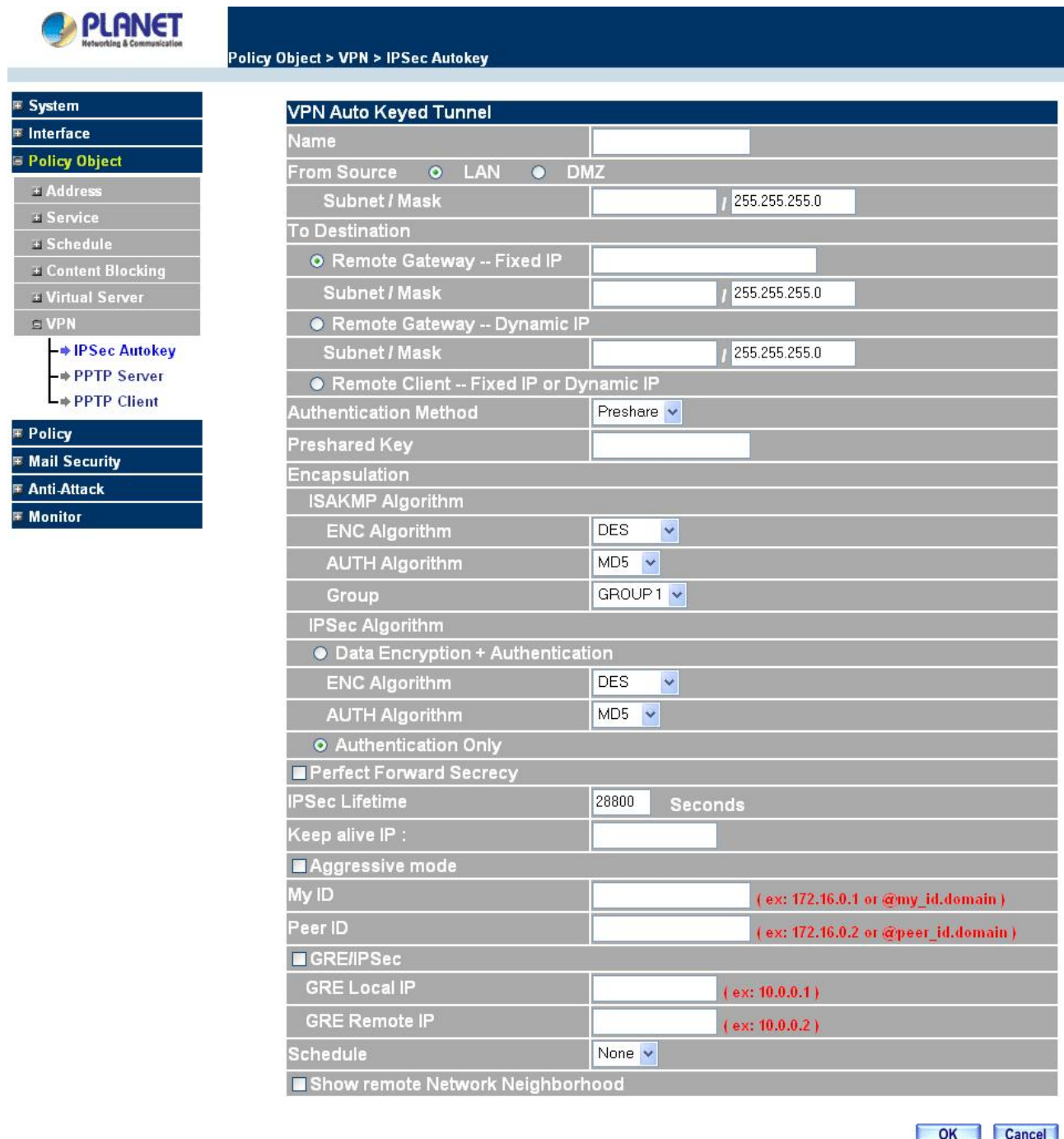
n Algorithm: The display the Algorithm way.

n Status: Connect/Disconnect or Connecting/Disconnecting.

n Configure: Connect, Disconnect, Modify and Delete.

Adding the Autokey IKE

Step 1: Click the **New Entry** button and the **VPN Auto Keyed Tunnel** window will appear.



PLANET
Networking & Communication

Policy Object > VPN > IPsec Autokey

VPN Auto Keyed Tunnel

Name:

From Source: ☒ LAN ☐ DMZ

Subnet / Mask: /

To Destination:

☒ Remote Gateway -- Fixed IP

Subnet / Mask: /

☐ Remote Gateway -- Dynamic IP

Subnet / Mask: /

☐ Remote Client -- Fixed IP or Dynamic IP

Authentication Method:

Preshared Key:

Encapsulation:

ISAKMP Algorithm:

ENC Algorithm:

AUTH Algorithm:

Group:

IPsec Algorithm:

☐ Data Encryption + Authentication

ENC Algorithm:

AUTH Algorithm:

☒ Authentication Only

☐ Perfect Forward Secrecy

IPsec Lifetime: Seconds

Keep alive IP:

☐ Aggressive mode

My ID: (ex: 172.16.0.1 or @my_id.domain)

Peer ID: (ex: 172.16.0.2 or @peer_id.domain)

☐ GRE/IPsec

GRE Local IP: (ex: 10.0.0.1)

GRE Remote IP: (ex: 10.0.0.2)

Schedule:

☐ Show remote Network Neighborhood

OK Cancel

Step 2: Configure the parameters.

Name: Specify a name for the VPN rule.

From Source: Select from LAN or DMZ to build up the VPN tunnel.

To Destination:

n Remote Gateway – Fixed IP: Specify the fixed IP address or domain name of the remote side VPN gateway.

– **Subnet / Mask:** Specify the LAN IP subnet and mask of the remote side VPN gateway.

n Remote Gateway – Dynamic IP: Select **Dynamic IP** if the remote side VPN gateway can not provide fixed IP or domain name to be configured.

– **Subnet / Mask:** Specify the LAN IP subnet and mask of the remote side VPN gateway.

n Remote Client – Fixed IP or Dynamic IP: Select **Remote Client** if there is only one user and dial up to Internet with PPPoE or cable modem.

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

Encapsulation

ISAKMP Algorithm

nENC Algorithm: ESP Encryption 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 and AES 256-bit encryption algorithm. The default algorithm 56 bit DES-CBC.

nAUTH 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.

n 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

n Encryption Algorithm: Selects 56 bit DES-CBC, 168-bit 3DES-CBC, AES or NULL encryption algorithm. The default algorithm is 56 bit DES-CBC.

n 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 preshare key.

Perfect Forward Secrecy

nIPSec 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.

n Keep alive IP: Check to allow Remote Client computer IP Address connected to keep alive.

Aggressive mode: Select Aggressive mode algorithm. You may enter IP or domain name to be identified for both VPN gateway.

GRE/IPSec: Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology. You may enter IP to be identified for both VPN gateways.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time.

Show remote Network Neighborhood: Select the remote Network Neighborhood enable to show.

There are 5 examples of VPN setting.

Example 1. Create a VPN connection between two Content Security Gateways.

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

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

Example 4. Create a VPN connection between two Content Security Gateways using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

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

Example 1. Create a VPN connection between two Content 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 Content 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 choose From Source to be LAN. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

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

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

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 Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to

keep connecting.

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

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None
----------	------

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

Policy Object > VPN > IPSec Autokey						
Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure	
VPN_A	211.22.22.22	192.168.20.0	None	Disconnect	Connecting	Modify Remove

New Entry

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 Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

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

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

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 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 Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

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

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None
----------	------

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

Policy Object > VPN > IPSec Autokey

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN_B	61.11.11.11	192.168.10.0	None	Disconnect	<input type="button" value="Connecting"/> <input type="button" value="Modify"/> <input type="button" value="Remove"/>

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

Preparation Task:

Company A External IP is 210.66.155.87, Internal IP is 192.168.10.X

Remote User External IP is 210.66.155.89

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-500

Step 1. Enter the default IP of Company A's Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel

Name	VPN_A	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
Subnet / Mask	192.168.10.0	/ 255.255.255.0

Step 3. In to Destination table, choose Remote Client – Fixed IP or Dynamic IP.

To Destination

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

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 1 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, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

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

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None ▼
----------	--------

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

Policy Object > VPN > IPSec Autokey

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

[New Entry](#)

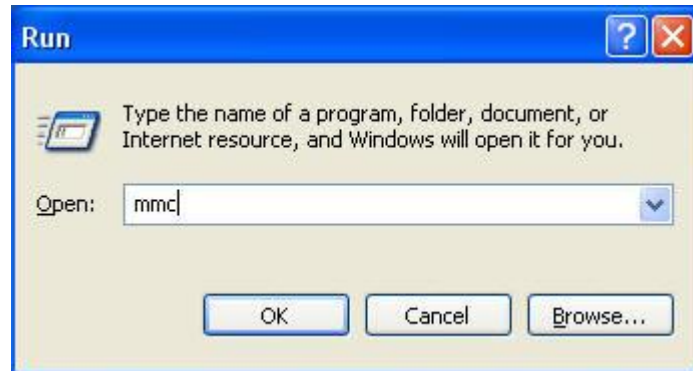
Configuration of WinXP

The IP of remote user is 210.66.155.89. The settings of remote user are as the following.

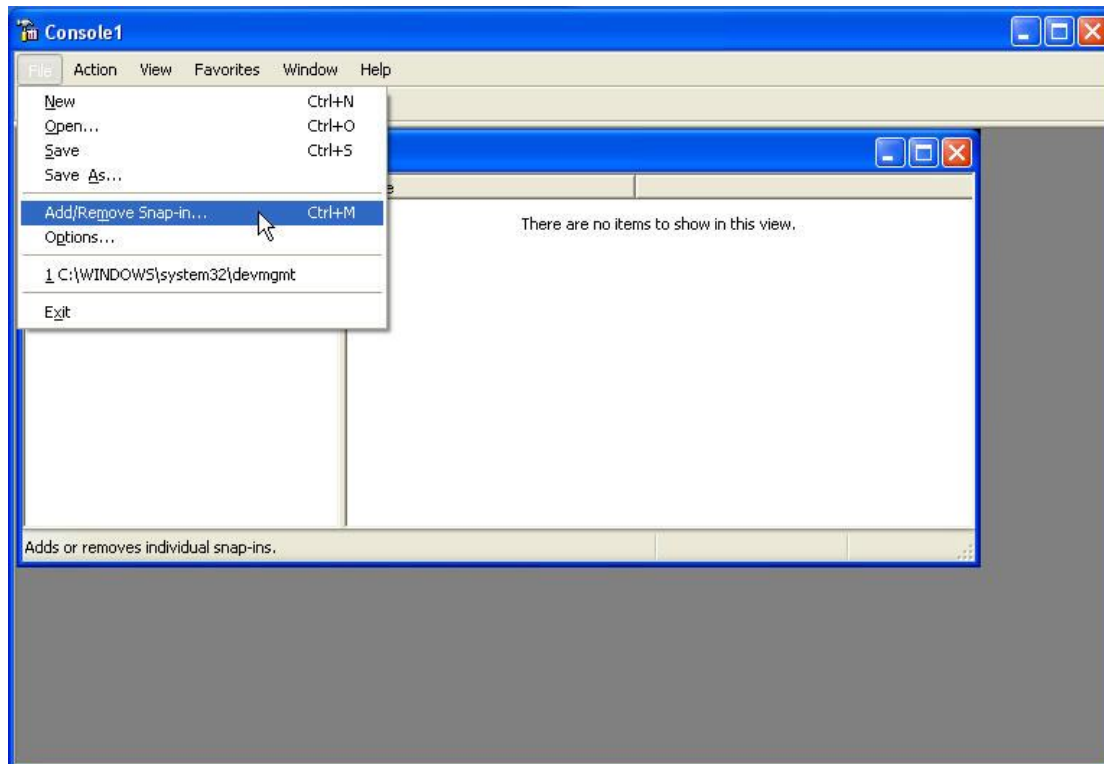
Step 1. Enter Windows XP, click Start and click Execute function.



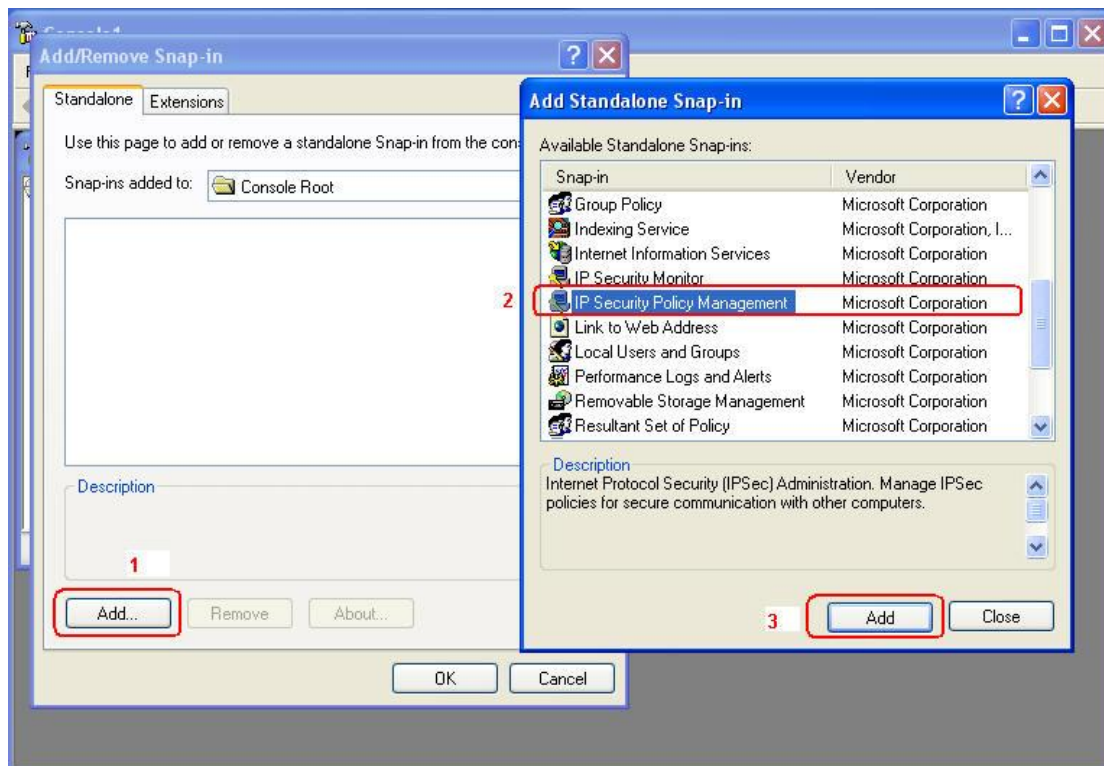
Step 2. In the Execute window, enter the command, mmc in Open.



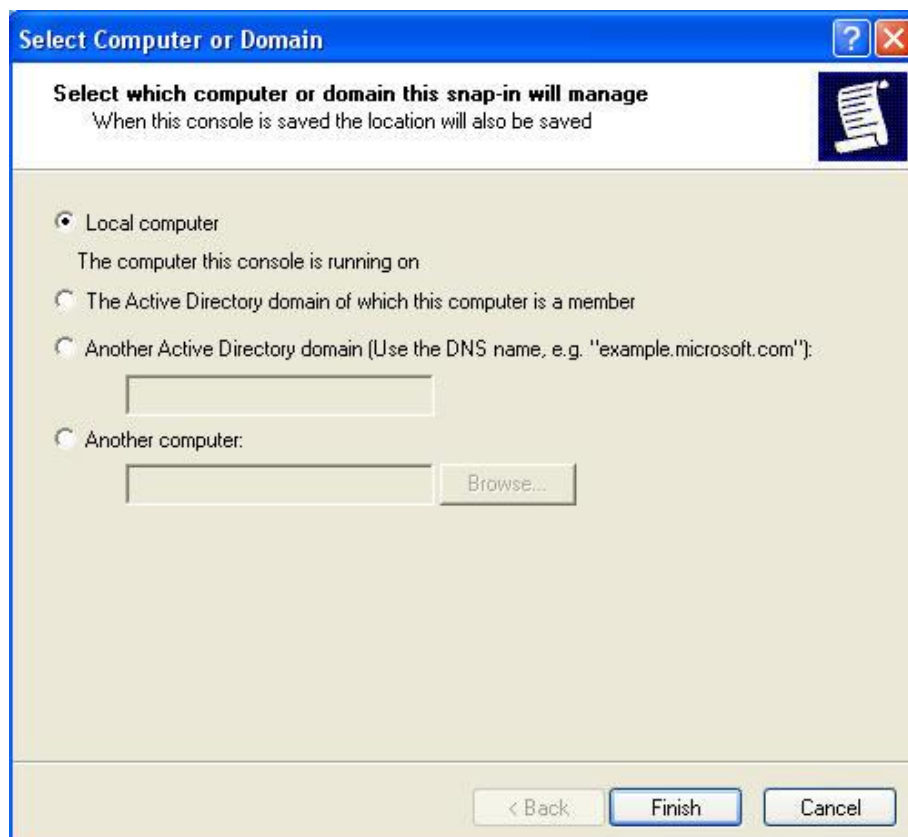
Step 3. Enter the Console window, click Console(C) option and click Add/Remove Embedded Management Option.



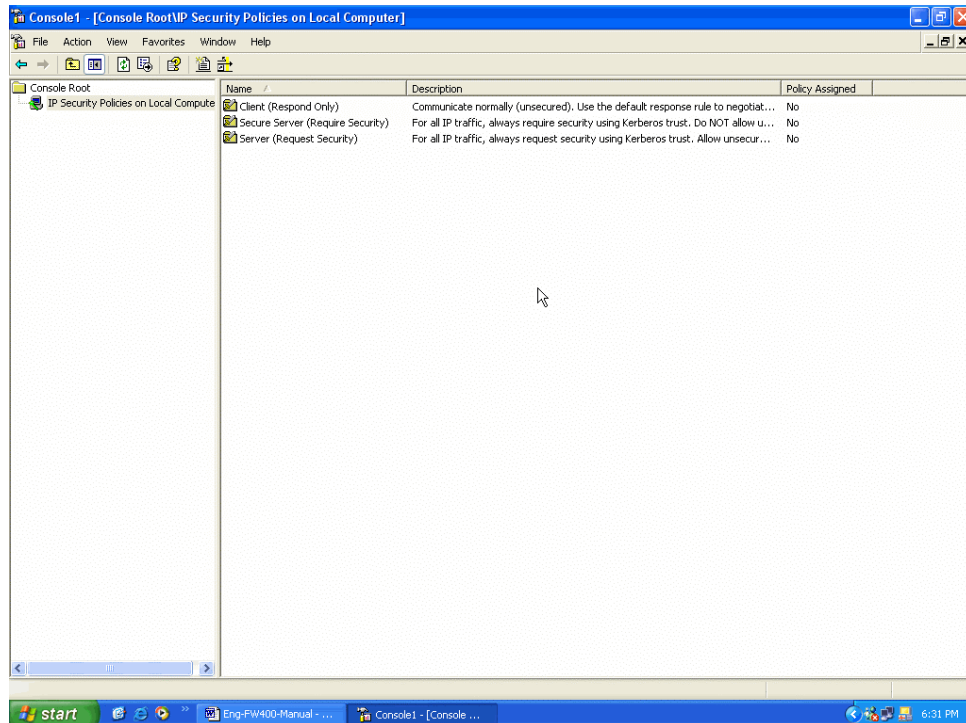
Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.



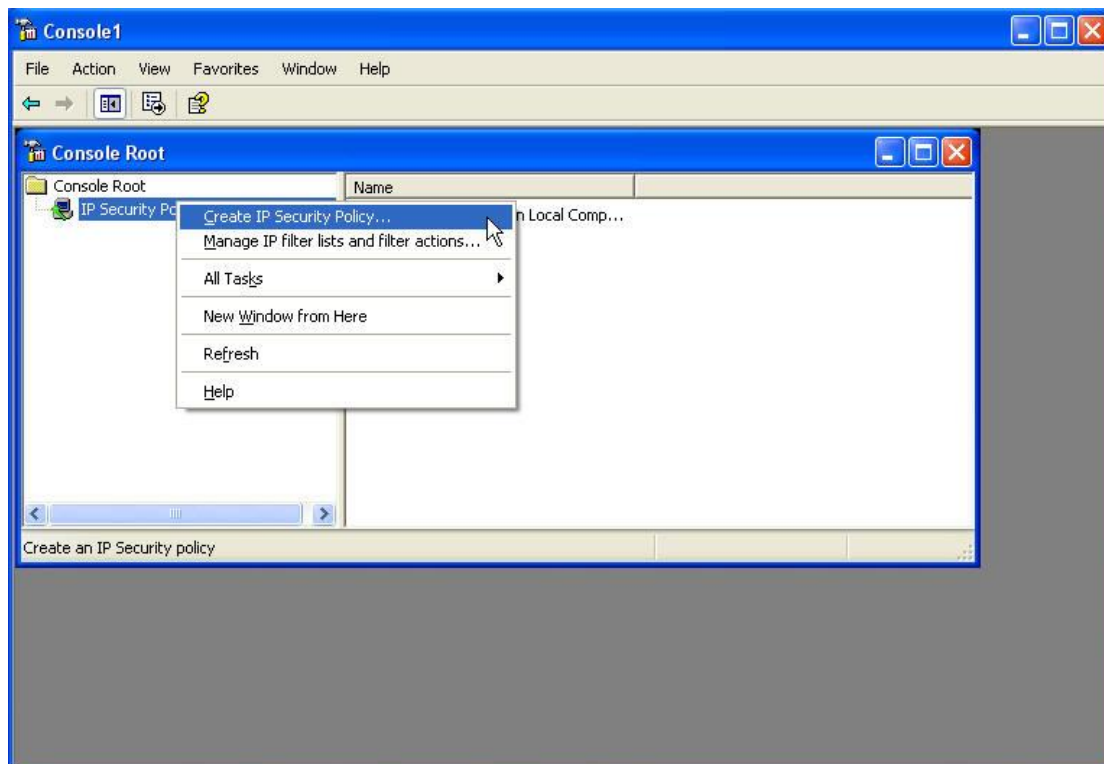
Step 5. Choose Local Machine (L) for finishing the setting of Add.



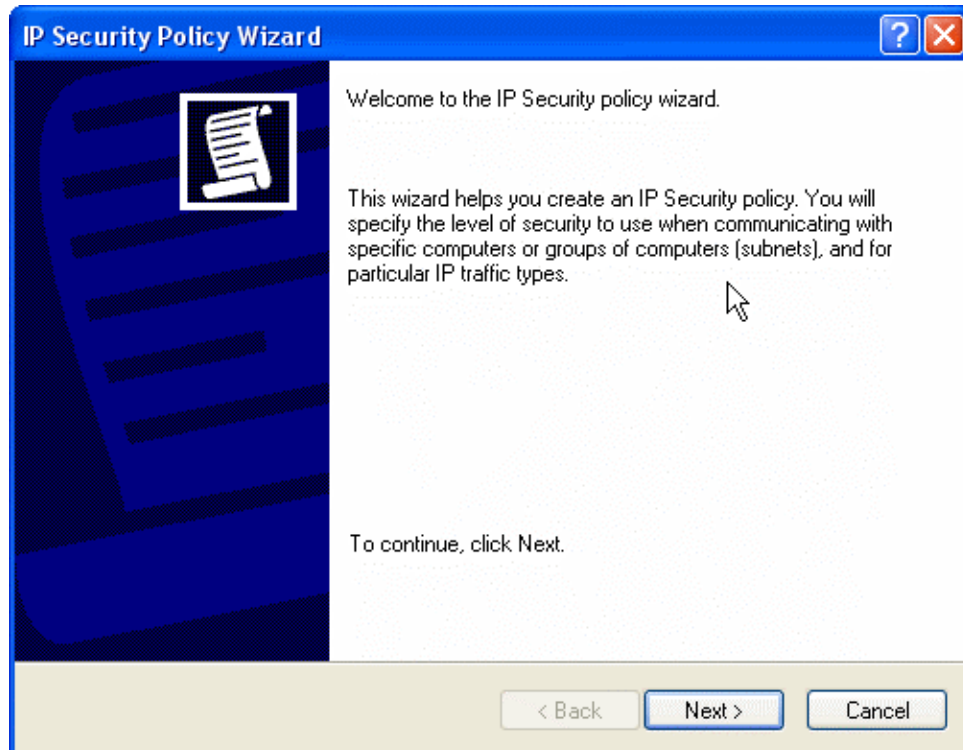
Step 6. Finish the setting of Add.



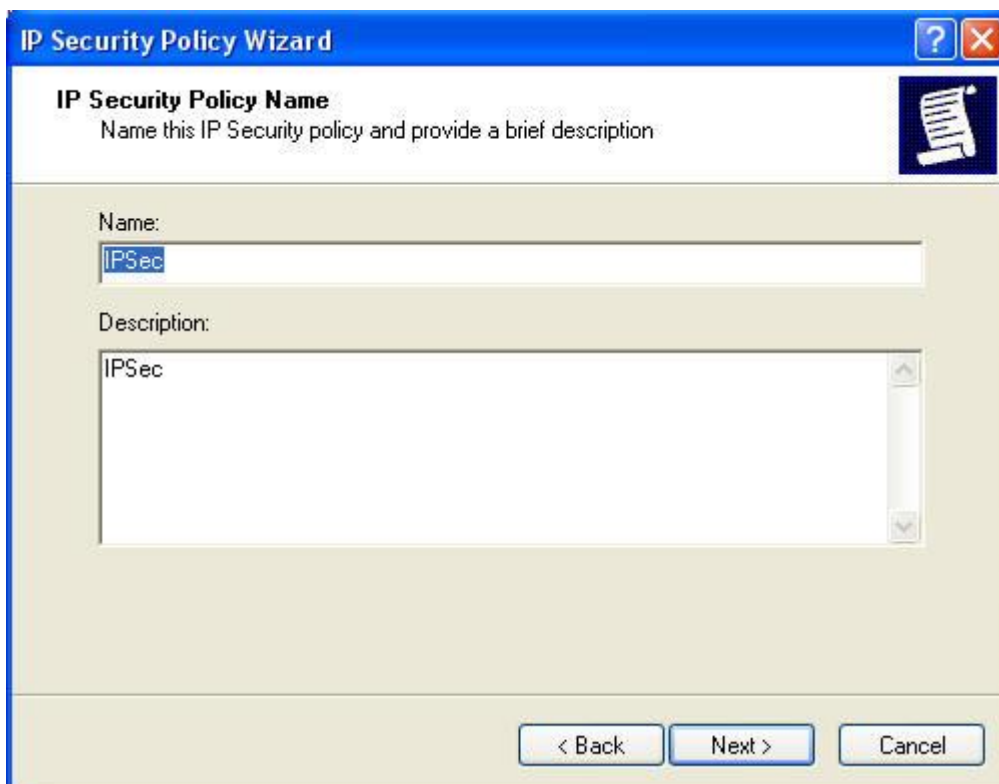
Step 7. Click the right button of mouse in IP Security Policies on Local Machine and choose Create IP Security Policy(C) option.



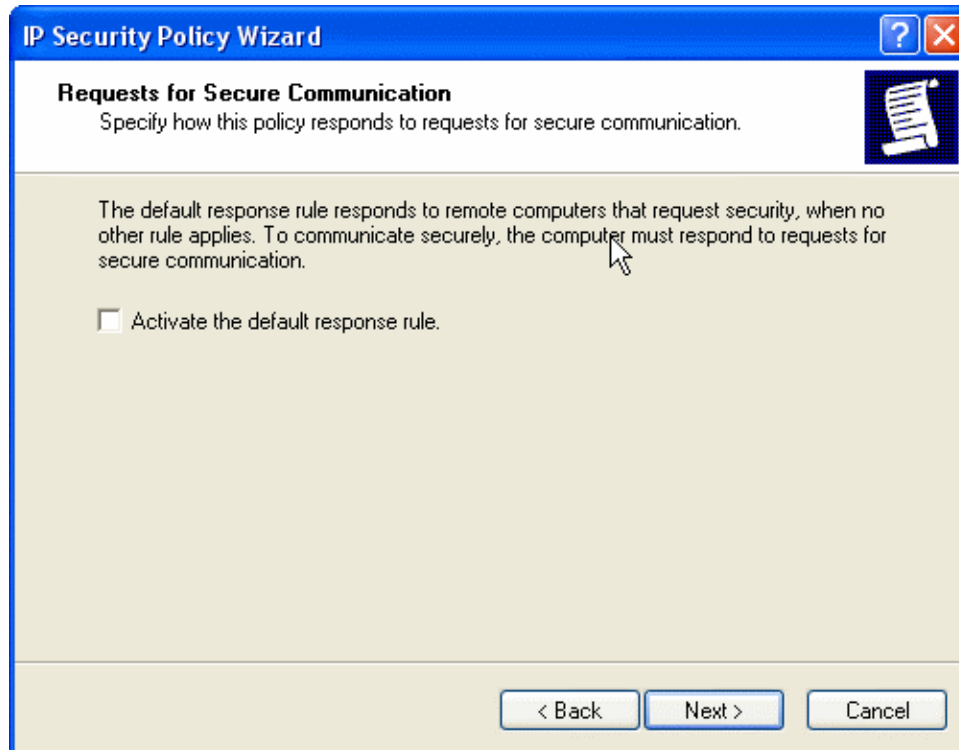
Step 8. Click Next.



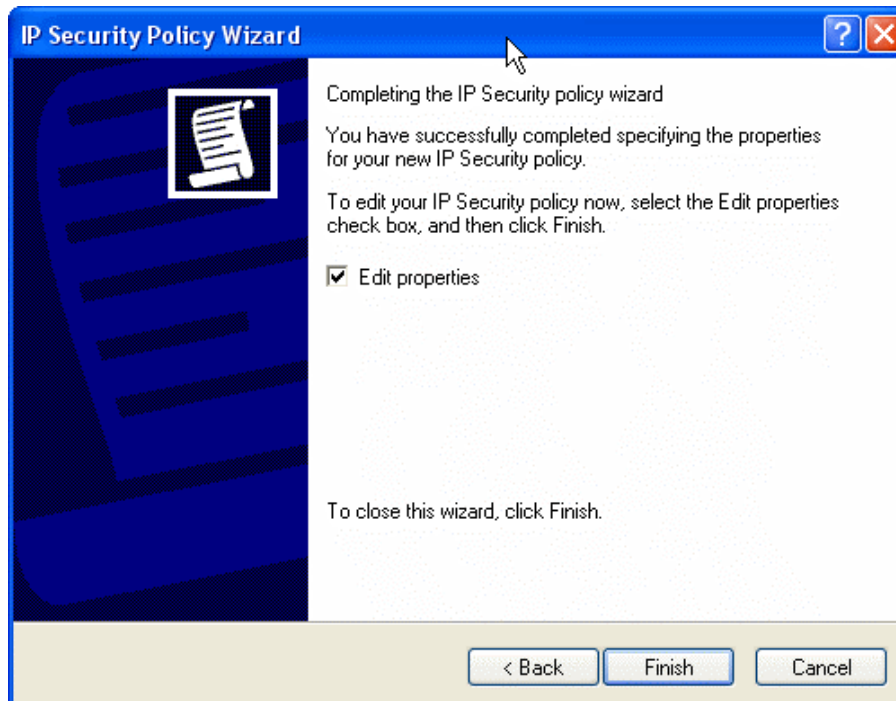
Step 9. Enter the Name of this VPN and optionally give it a brief description.



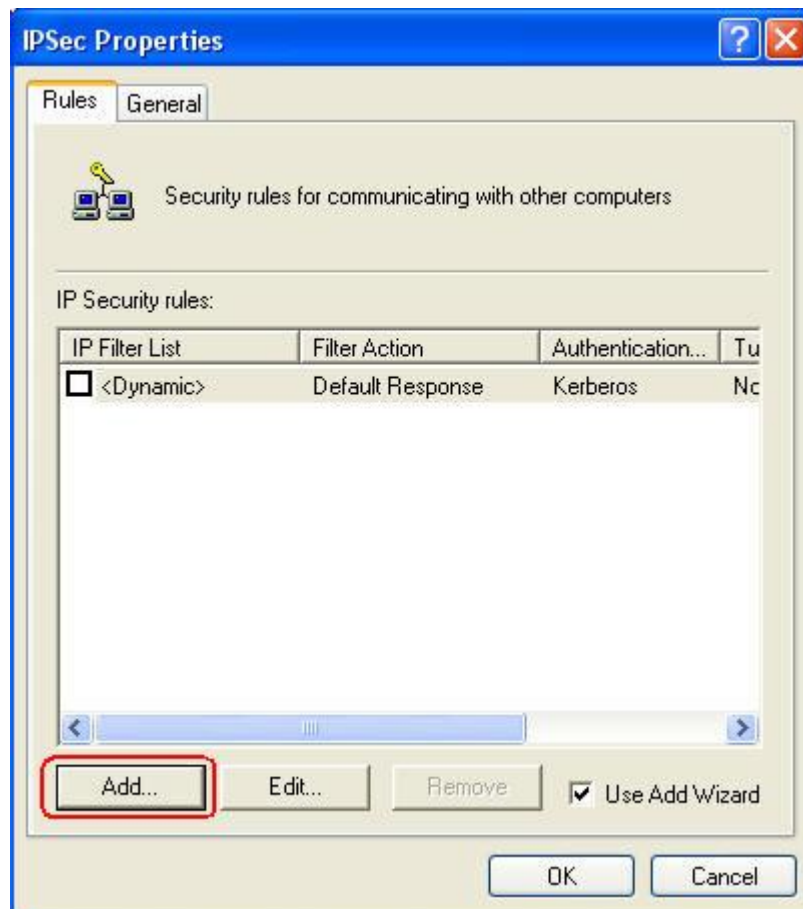
Step 10. Disable **Activate the default response rule**. And click Next.



Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.



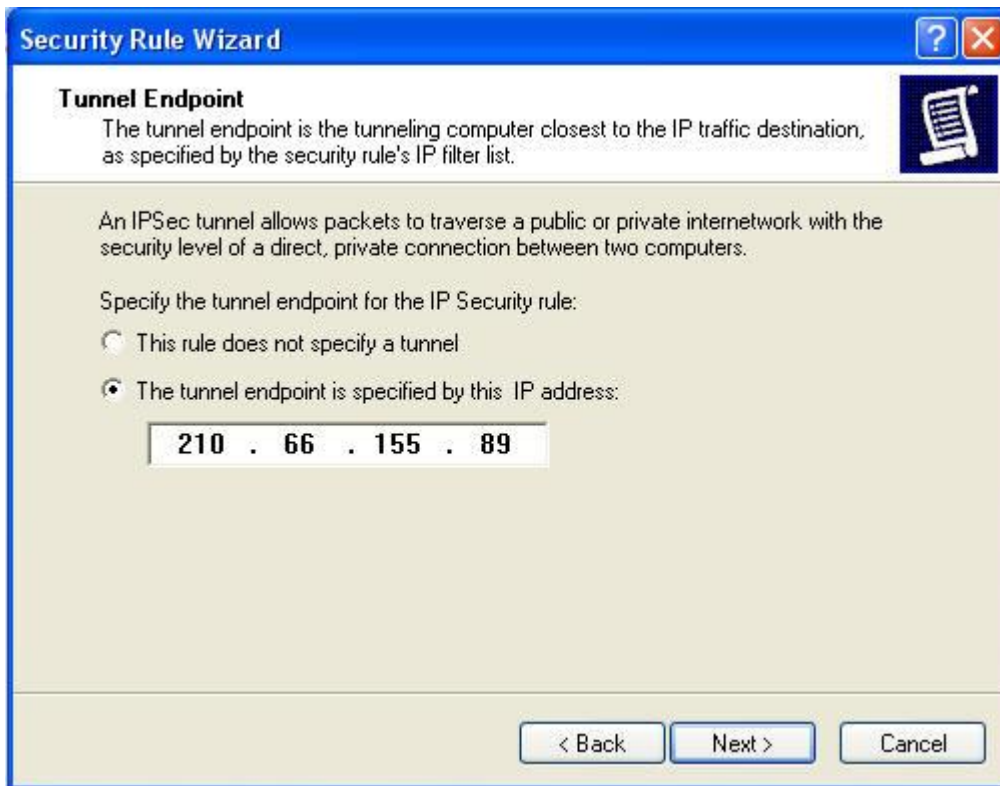
Step 12. In window, click Add and click Use Add Wizard.



Step 13. Click next.



Step 14. Enter the WAN IP of Remote user, 210.66.155.89.



The screenshot shows the 'Security Rule Wizard' window at the 'Tunnel Endpoint' step. The title bar is blue with a question mark and close button. The main area has a light beige background. At the top, the title 'Tunnel Endpoint' is in bold, followed by a description: 'The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.' Below this, a paragraph explains: 'An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.' Then, it says 'Specify the tunnel endpoint for the IP Security rule:' followed by two radio button options. The first option is 'This rule does not specify a tunnel'. The second option is 'The tunnel endpoint is specified by this IP address:', which is selected. Below the selected option is a text box containing the IP address '210 . 66 . 155 . 89'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP Security rule:

☐ This rule does not specify a tunnel

☒ The tunnel endpoint is specified by this IP address:

210 . 66 . 155 . 89

< Back Next > Cancel

Step 15. click all network connections.



The screenshot shows the 'Security Rule Wizard' window at the 'Network Type' step. The title bar is blue with a question mark and close button. The main area has a light beige background. At the top, the title 'Network Type' is in bold, followed by a description: 'The security rule must be applied to a network type.' Below this, it says 'Select the network type:' followed by three radio button options. The first option is 'All network connections', which is selected. The second option is 'Local area network (LAN)'. The third option is 'Remote access'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Network Type
The security rule must be applied to a network type.

Select the network type:

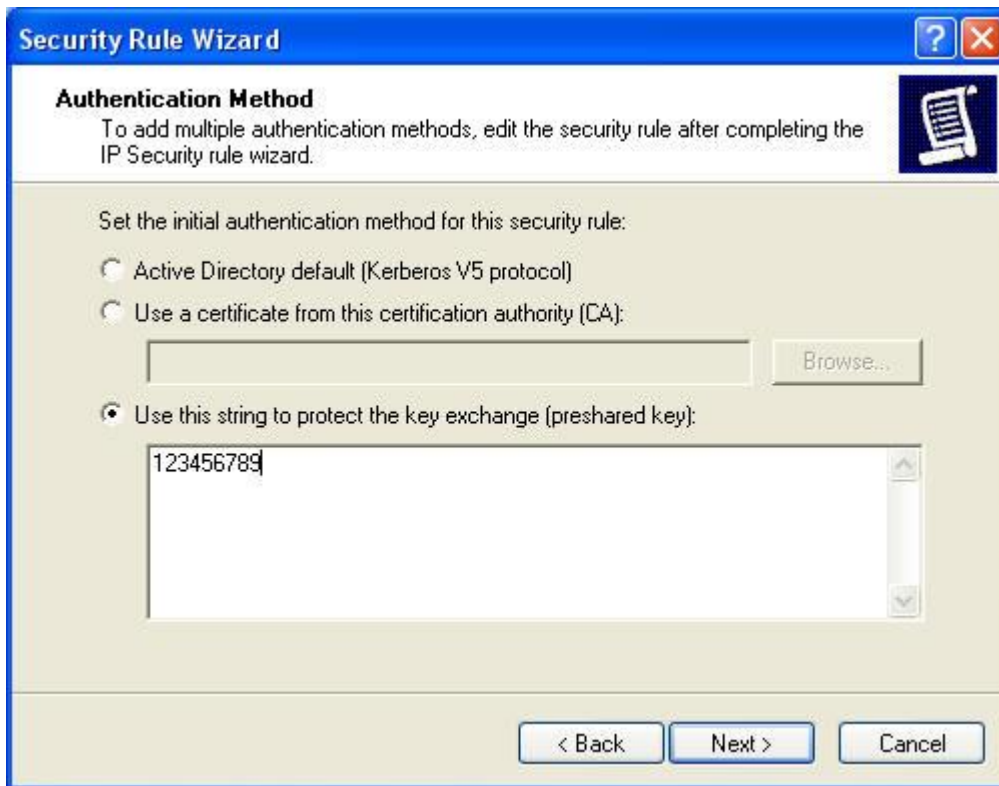
☒ All network connections

☐ Local area network (LAN)

☐ Remote access

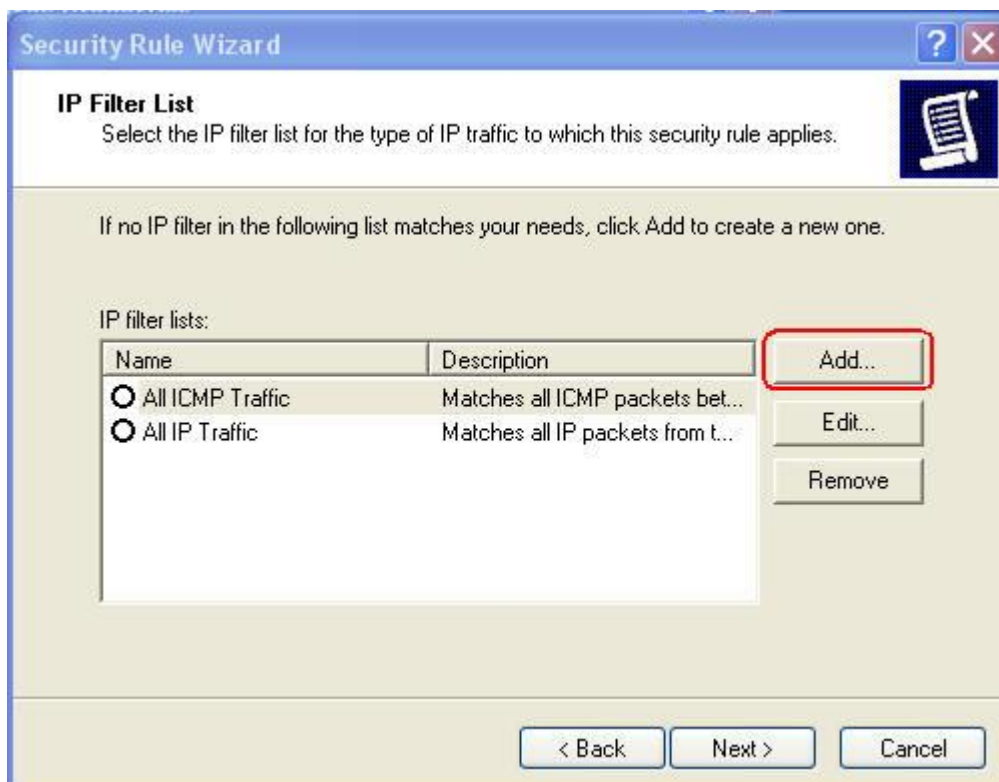
< Back Next > Cancel

Step 16. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



The screenshot shows the 'Authentication Method' step of the Security Rule Wizard. The title bar reads 'Security Rule Wizard'. Below the title, the section is 'Authentication Method' with a sub-instruction: 'To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.' There are three radio button options: 'Active Directory default (Kerberos V5 protocol)', 'Use a certificate from this certification authority (CA):' (with an empty text box and a 'Browse...' button), and 'Use this string to protect the key exchange (preshared key):' (which is selected). Below the selected option is a large text area containing the string '123456789'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

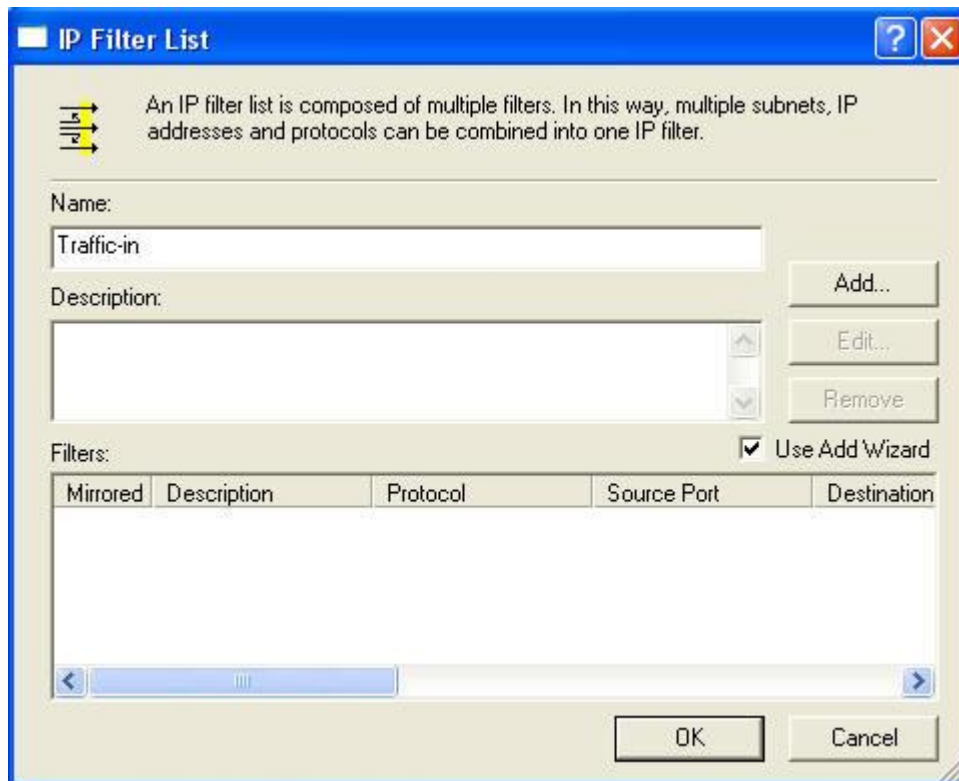
Step 17. Click Add.



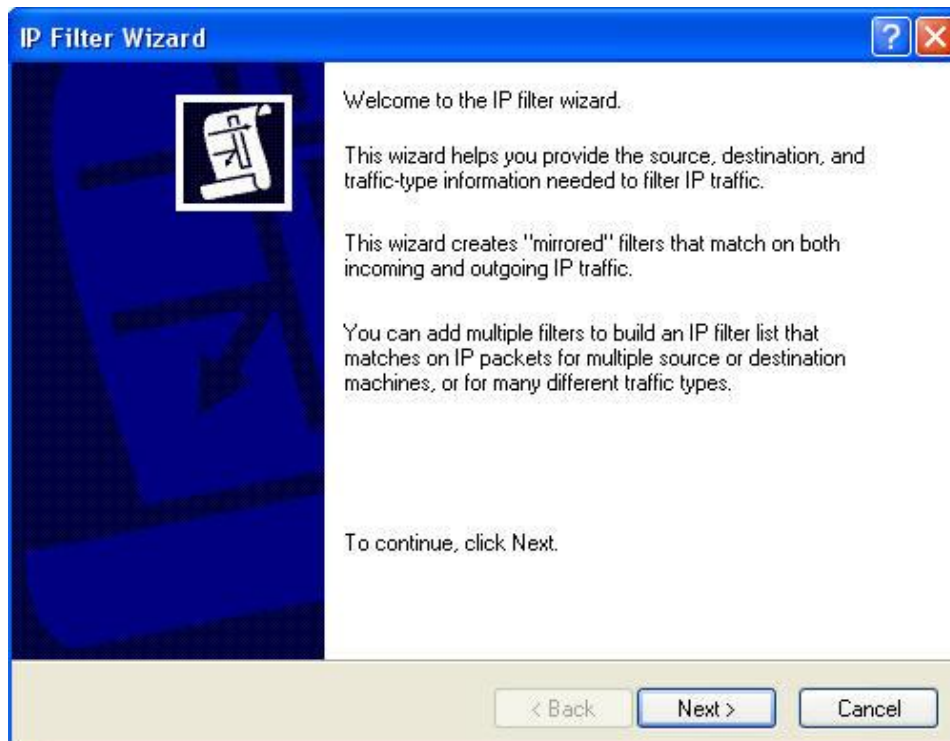
The screenshot shows the 'IP Filter List' step of the Security Rule Wizard. The title bar reads 'Security Rule Wizard'. Below the title, the section is 'IP Filter List' with a sub-instruction: 'Select the IP filter list for the type of IP traffic to which this security rule applies.' Below this, it says: 'If no IP filter in the following list matches your needs, click Add to create a new one.' There is a table with two columns: 'Name' and 'Description'. The table contains two entries: 'All ICMP Traffic' and 'All IP Traffic', both with radio button selection. To the right of the table are three buttons: 'Add...', 'Edit...', and 'Remove'. The 'Add...' button is highlighted with a red rectangle. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Name	Description
<input type="radio"/> All ICMP Traffic	Matches all ICMP packets bet...
<input type="radio"/> All IP Traffic	Matches all IP packets from t...

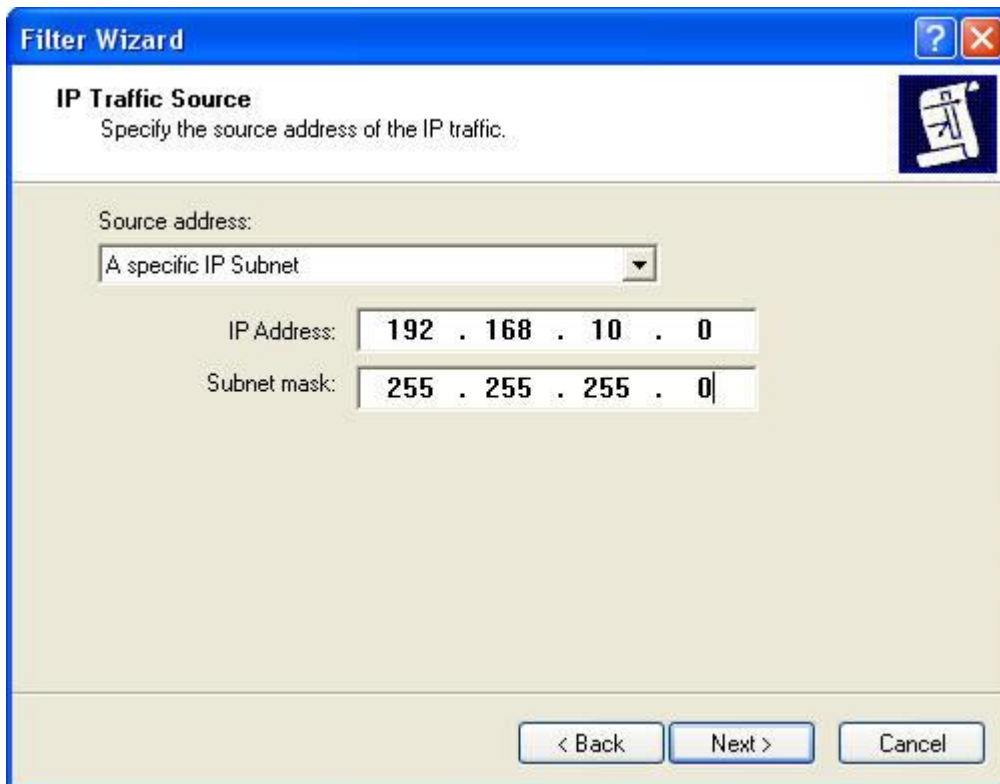
Step 18. Enter the name of IP filter and click “Add..”.



Step 19. Click next.

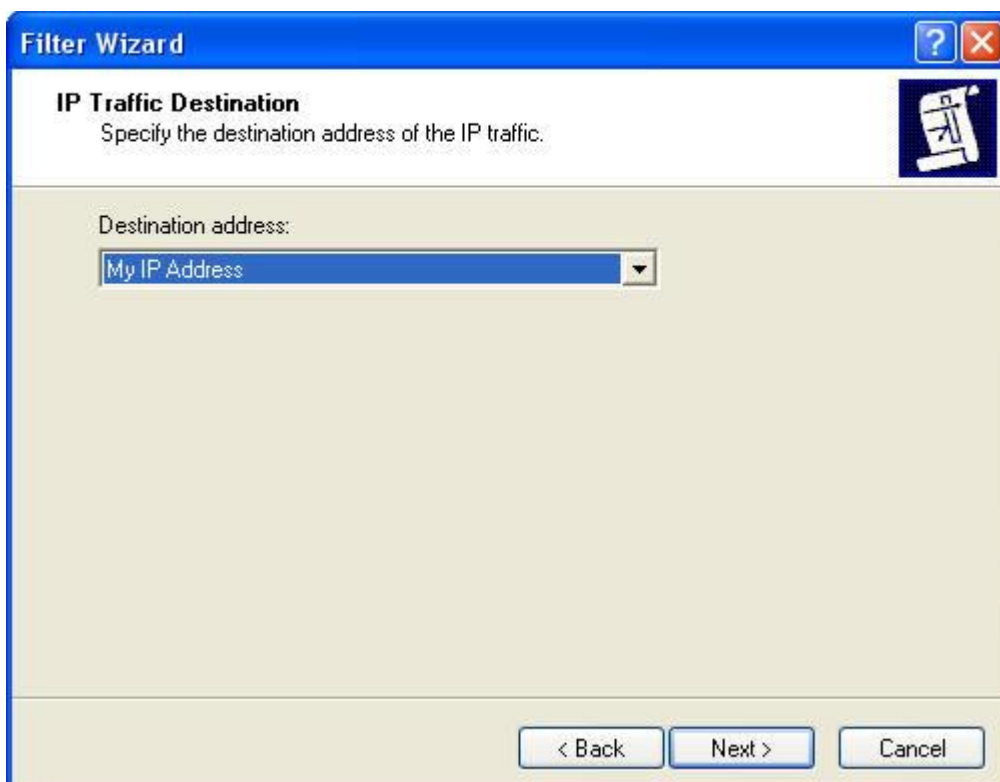


Step 20. In Source address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.



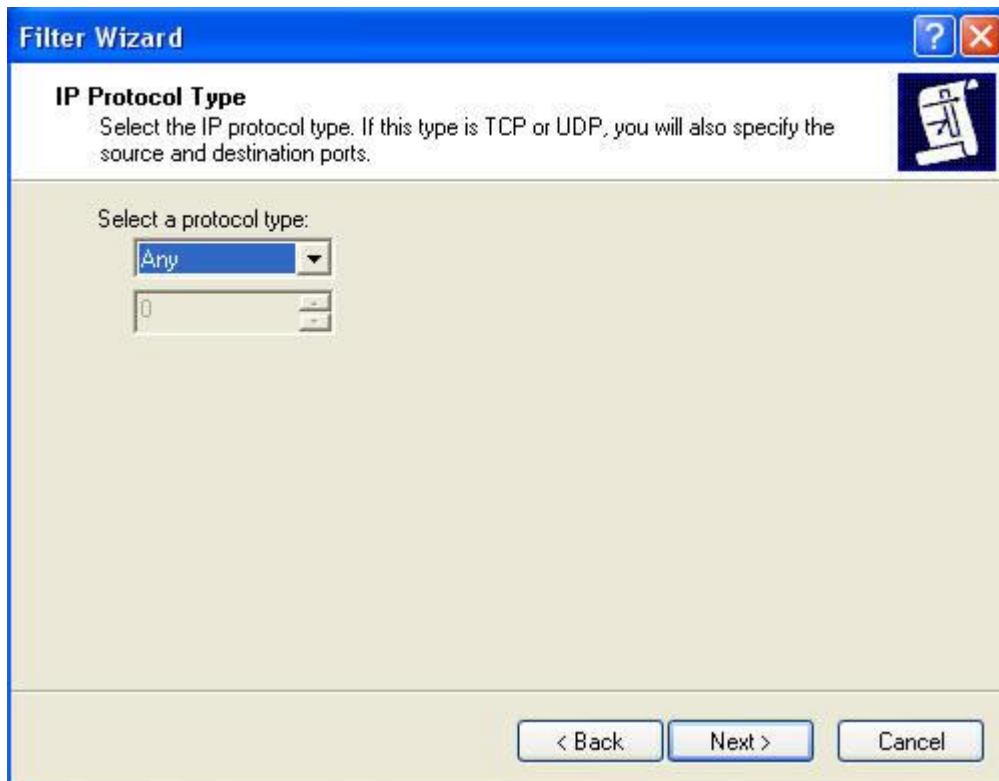
The image shows the 'Filter Wizard' window, specifically the 'IP Traffic Source' step. The window has a blue title bar with a question mark and a close button. Below the title bar, the text 'IP Traffic Source' is displayed, followed by the instruction 'Specify the source address of the IP traffic.' and a small icon of a document with a magnifying glass. The main area contains a 'Source address:' label above a dropdown menu currently showing 'A specific IP Subnet'. Below this, there are two input fields: 'IP Address:' with the value '192 . 168 . 10 . 0' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Step 21. In Destination address, click down the arrow to select the My IP Address.



The image shows the 'Filter Wizard' window, specifically the 'IP Traffic Destination' step. The window has a blue title bar with a question mark and a close button. Below the title bar, the text 'IP Traffic Destination' is displayed, followed by the instruction 'Specify the destination address of the IP traffic.' and a small icon of a document with a magnifying glass. The main area contains a 'Destination address:' label above a dropdown menu currently showing 'My IP Address'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Step 22. Click next.



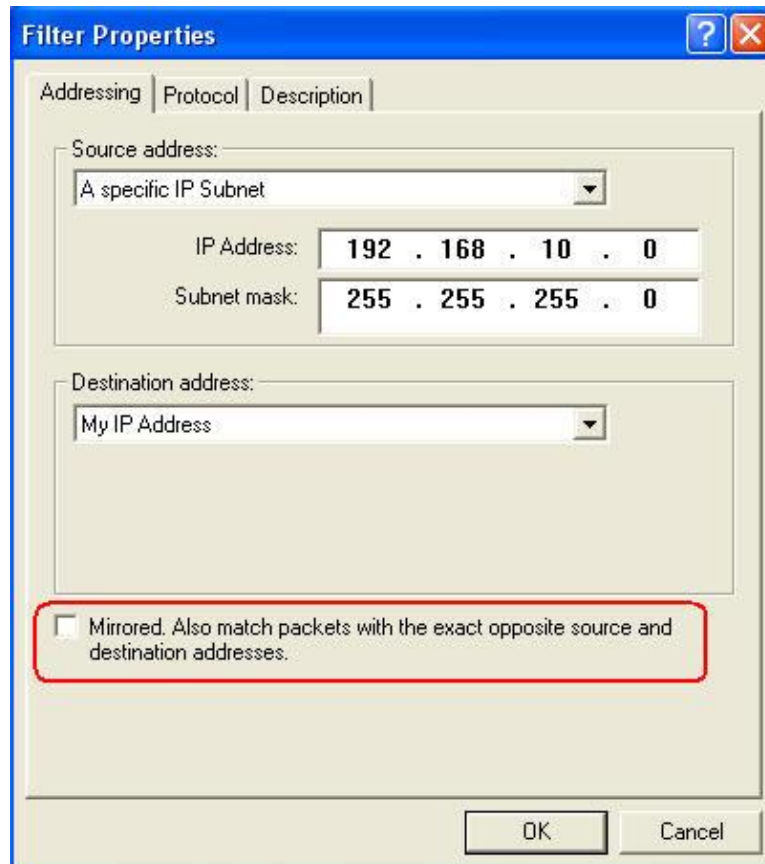
The **Filter Wizard** dialog box is shown. It has a blue title bar with a question mark and a close button. The main area is titled **IP Protocol Type** and contains the text: "Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports." Below this text is a label "Select a protocol type:" followed by a dropdown menu showing "Any" and a text box containing "0". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Step 23. Please enable edit properties, and click finish.



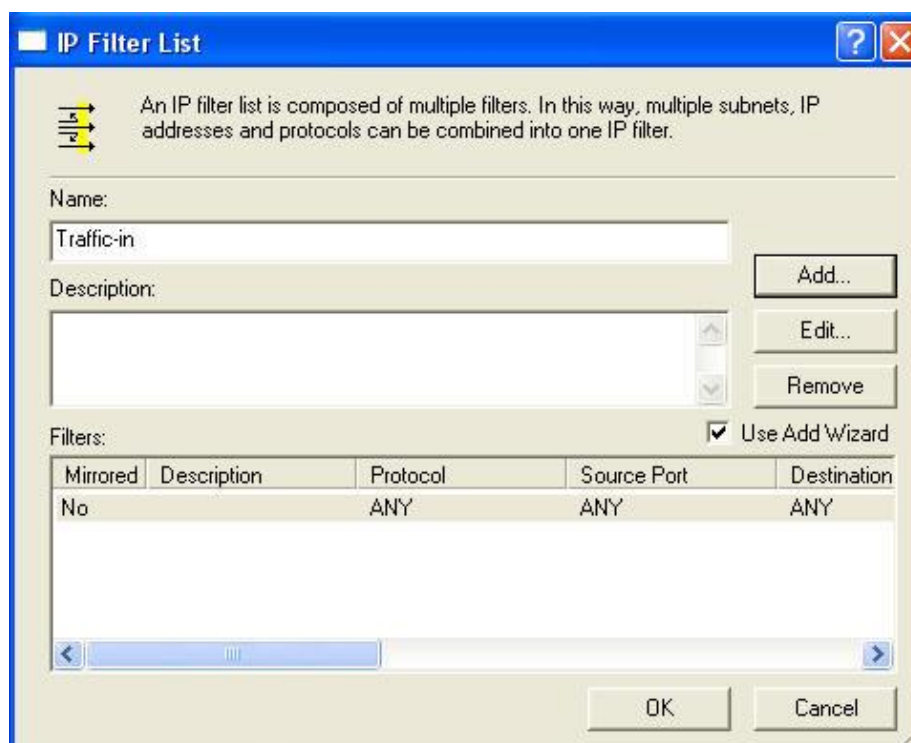
The **IP Filter Wizard** dialog box is shown. It has a blue title bar with a question mark and a close button. The main area is titled **Completing the IP filter wizard** and contains the text: "You have successfully completed the IP filter wizard." Below this text is a label "To edit your IP filter now, select the Edit properties check box, and then click finish." followed by a checked checkbox labeled "Edit properties". At the bottom are three buttons: "< Back", "Finish", and "Cancel".

Step 24. 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 sections: **Source address:** with a dropdown menu showing "A specific IP Subnet", and **Destination address:** with a dropdown menu showing "My IP Address". Below these are fields for **IP Address:** (192 . 168 . 10 . 0) and **Subnet mask:** (255 . 255 . 255 . 0). At the bottom, there is a checkbox labeled **Mirrored. Also match packets with the exact opposite source and destination addresses.** which is currently unchecked. The **OK** and **Cancel** buttons are at the bottom right.

Step 25. Click OK.

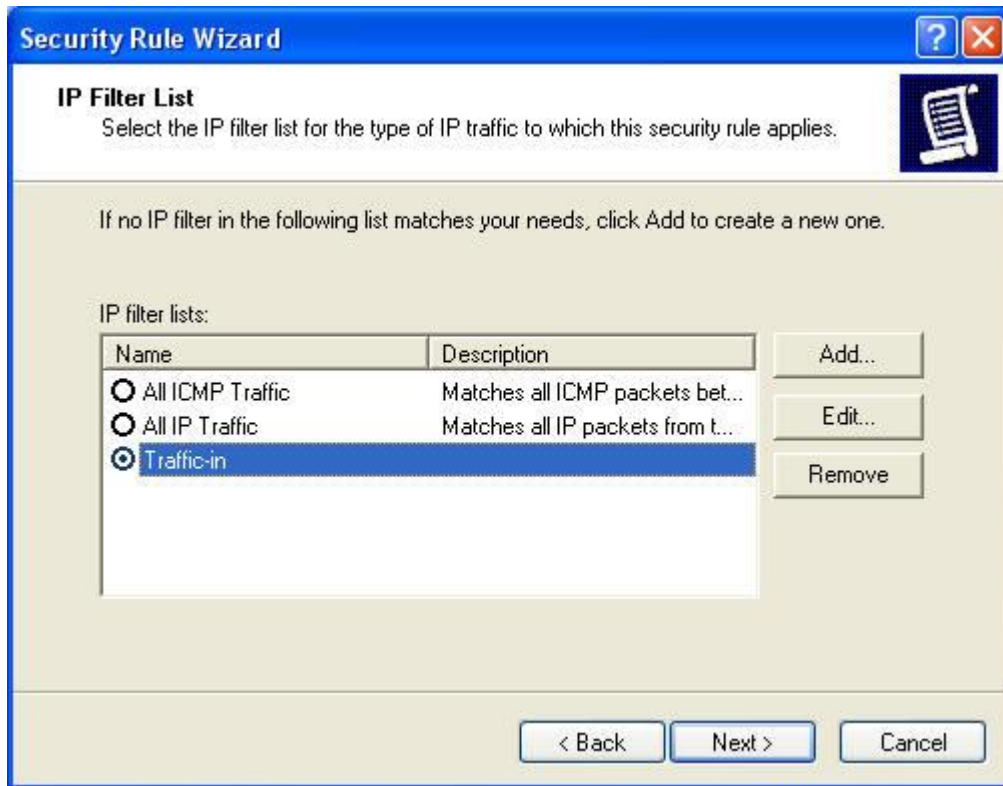


The **IP Filter List** dialog box contains an introductory text: "An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter." Below this is a **Name:** field with "Traffic-in" and a **Description:** text area. To the right of the description are **Add...**, **Edit...**, and **Remove** buttons. Below these is a **Filters:** section with a checked **Use Add Wizard** checkbox. A table lists the filters:

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

At the bottom are **OK** and **Cancel** buttons.

Step 26. Select Traffic-in and click next.



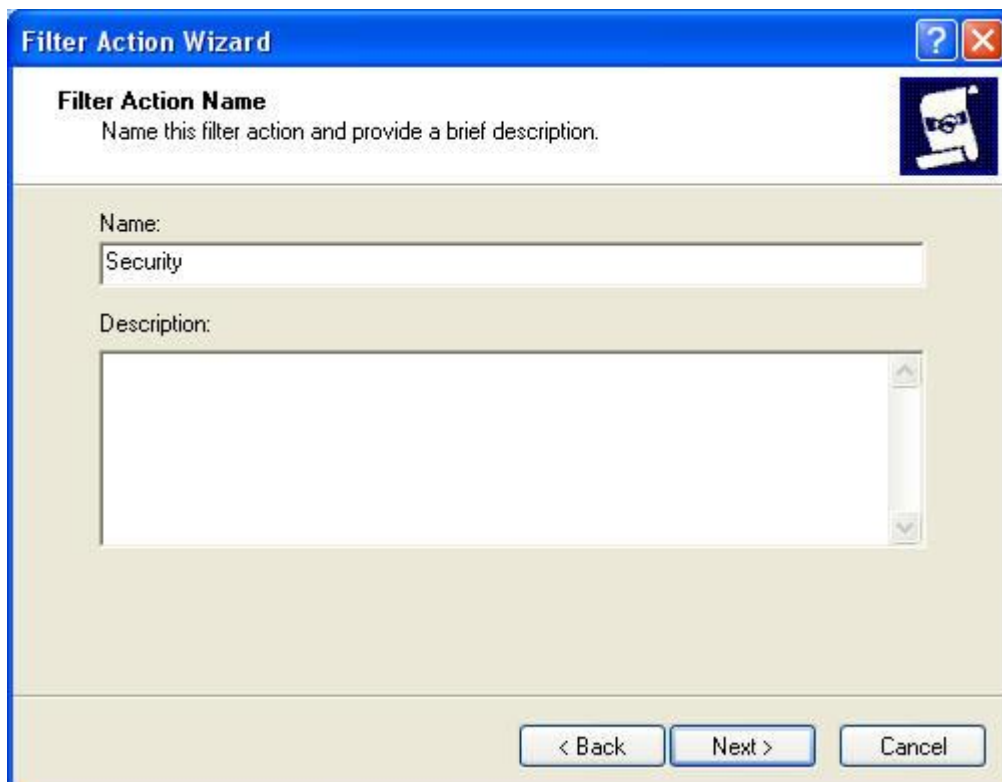
Step 27. Enable User Add Wizard and click add.



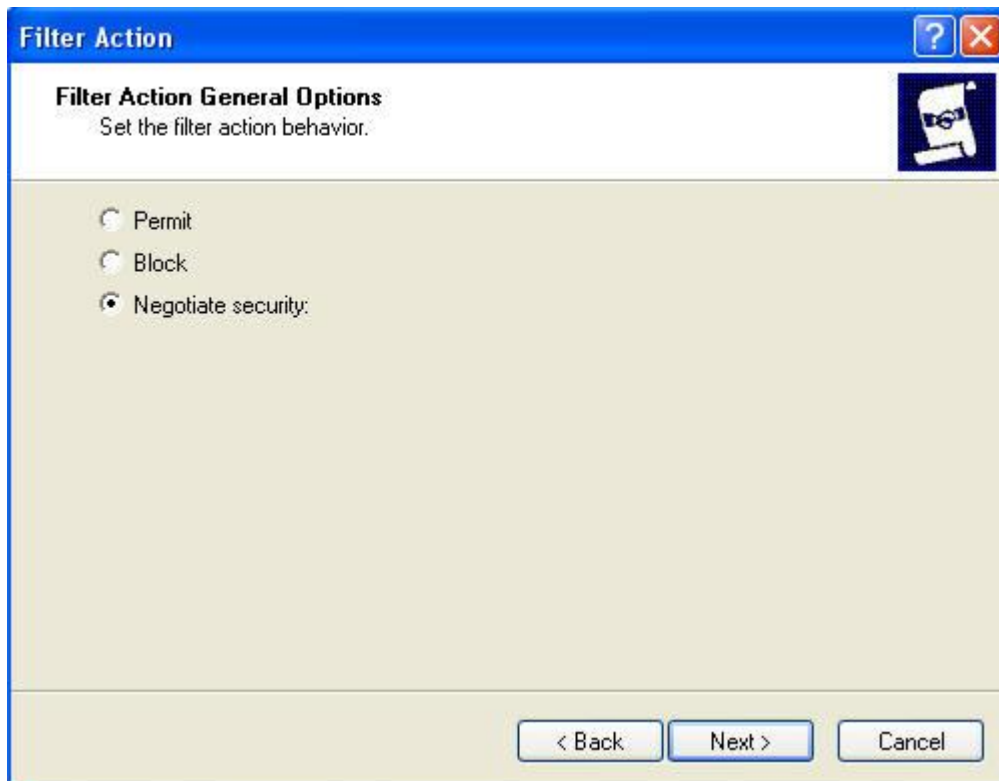
Step 28. Click next.



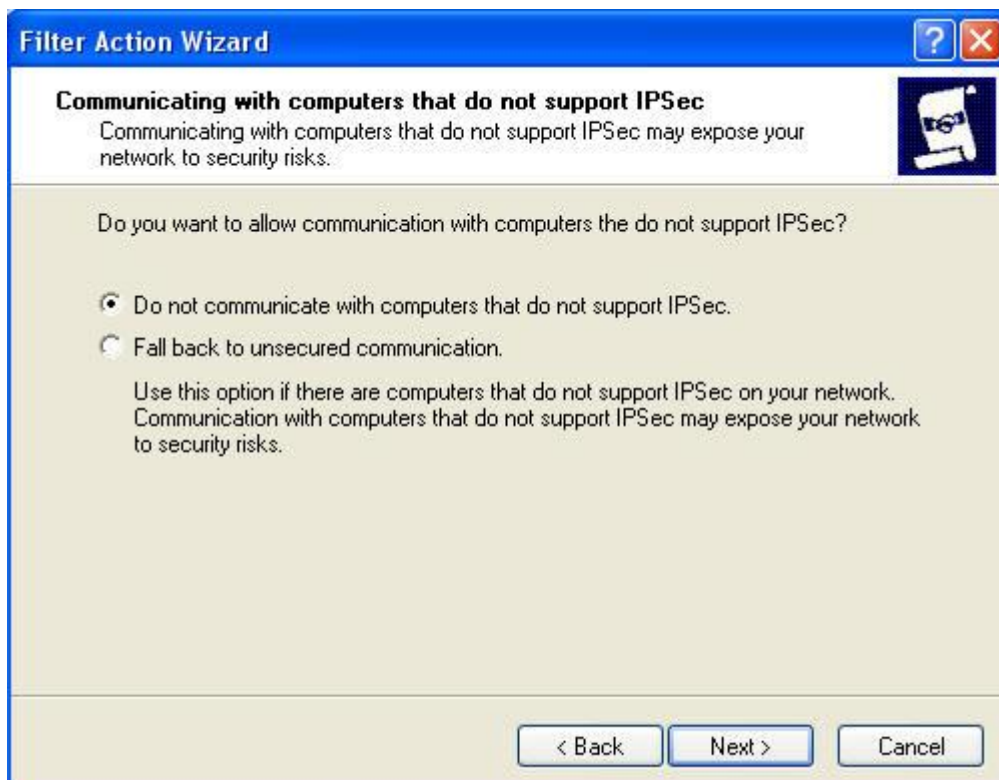
Step 29. Enter the name of filter action and click next.



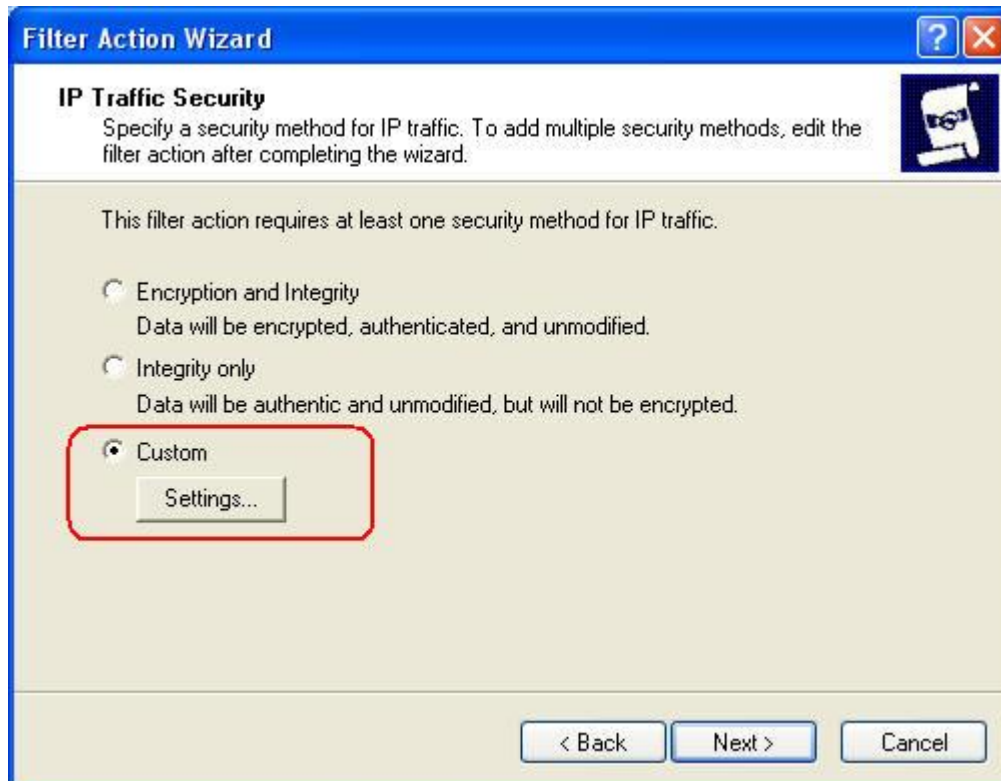
Step 30. Select Negotiate security and click next.



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.



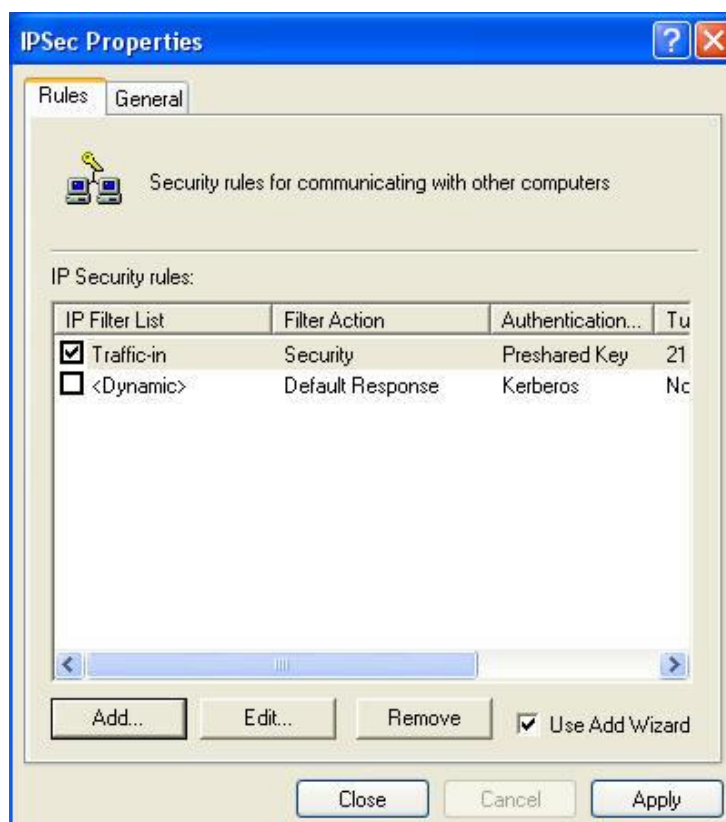
Step 35. Select security and click next.



Step 36. Click finish.



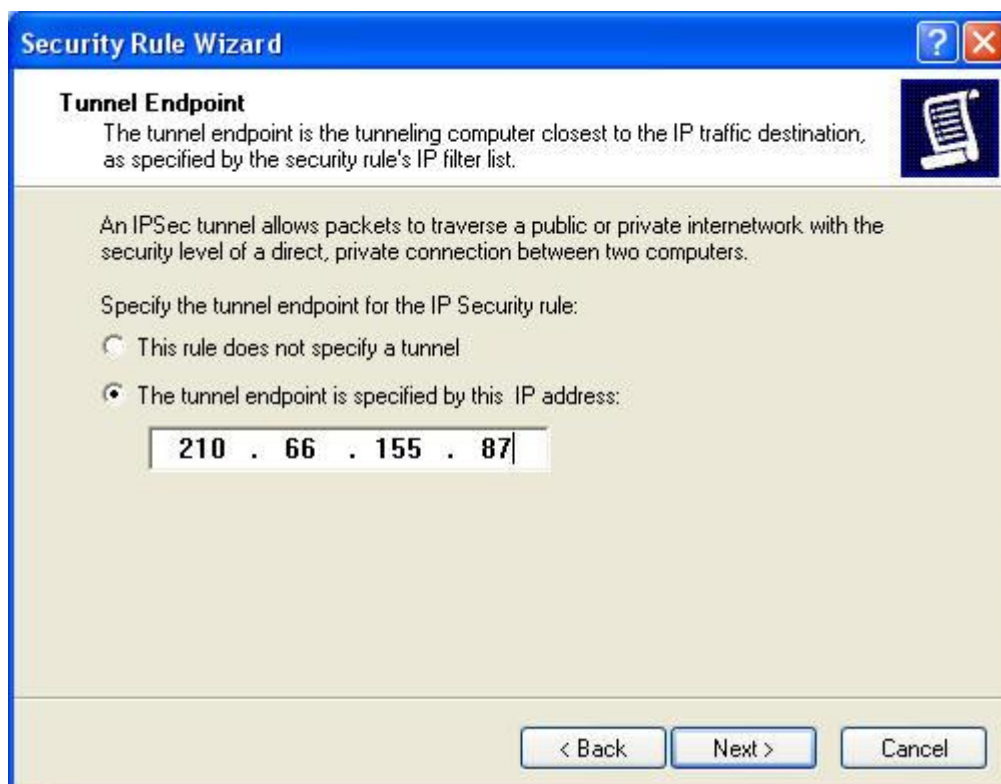
Step 37. Click Add.



Step 38. Click next.



Step 39. Enter the WAN IP of company A, 210.66.155.87.



Step 40. Select All network connections and click next.



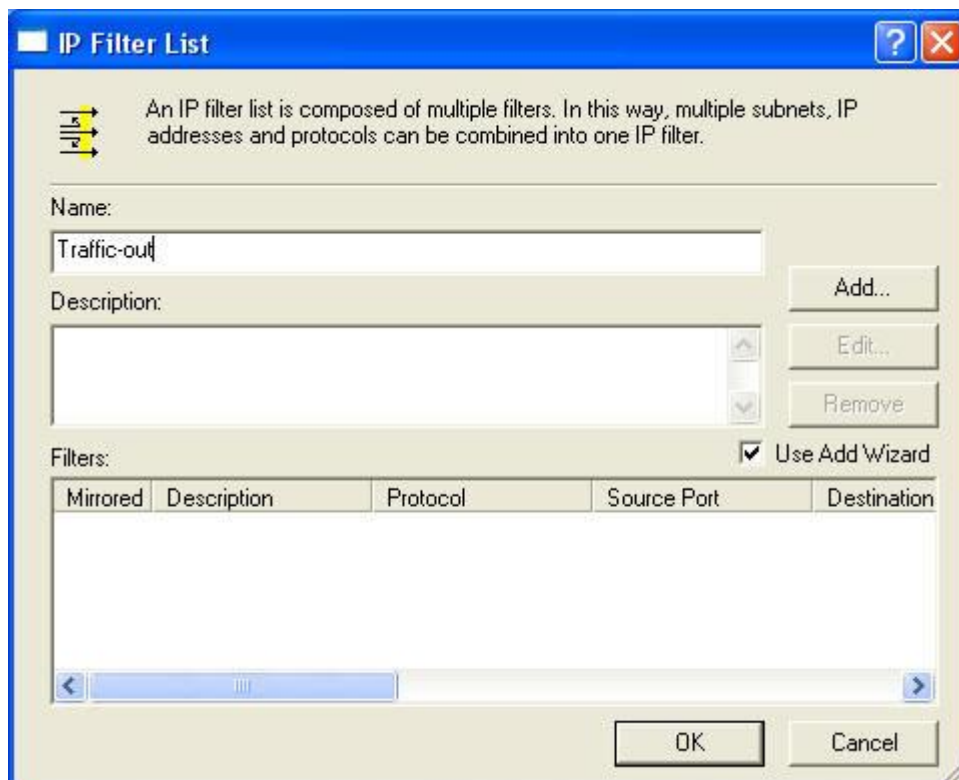
Step 41. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



Step 42. Click Add.



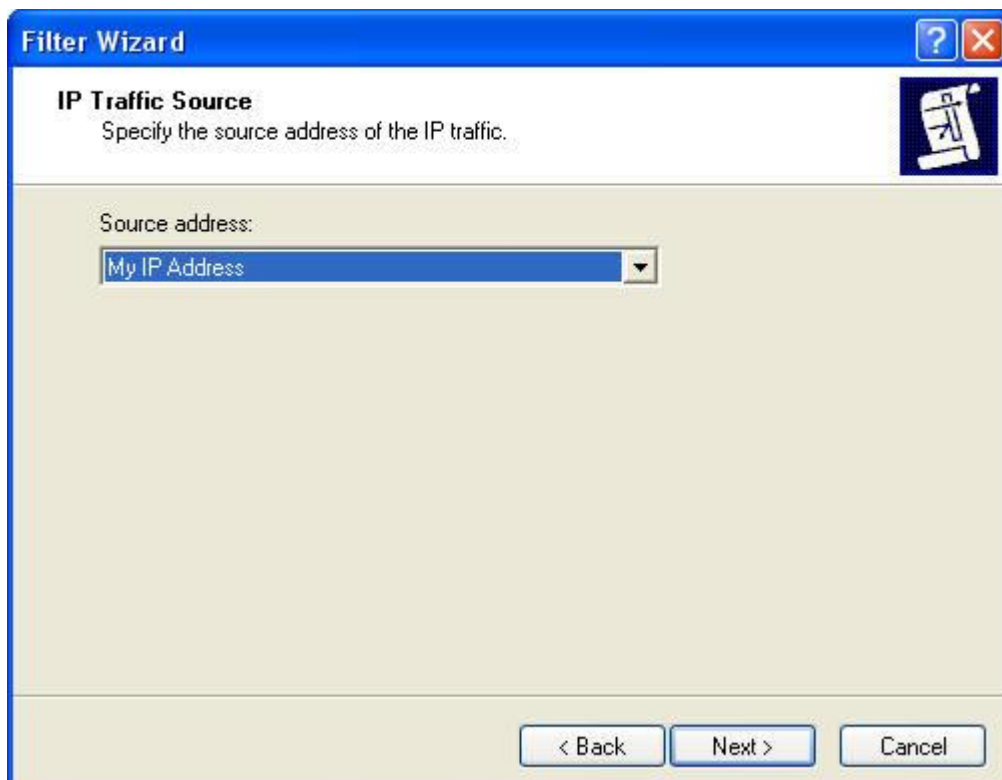
Step 43. Enter the name of IP filter and click "Add...".



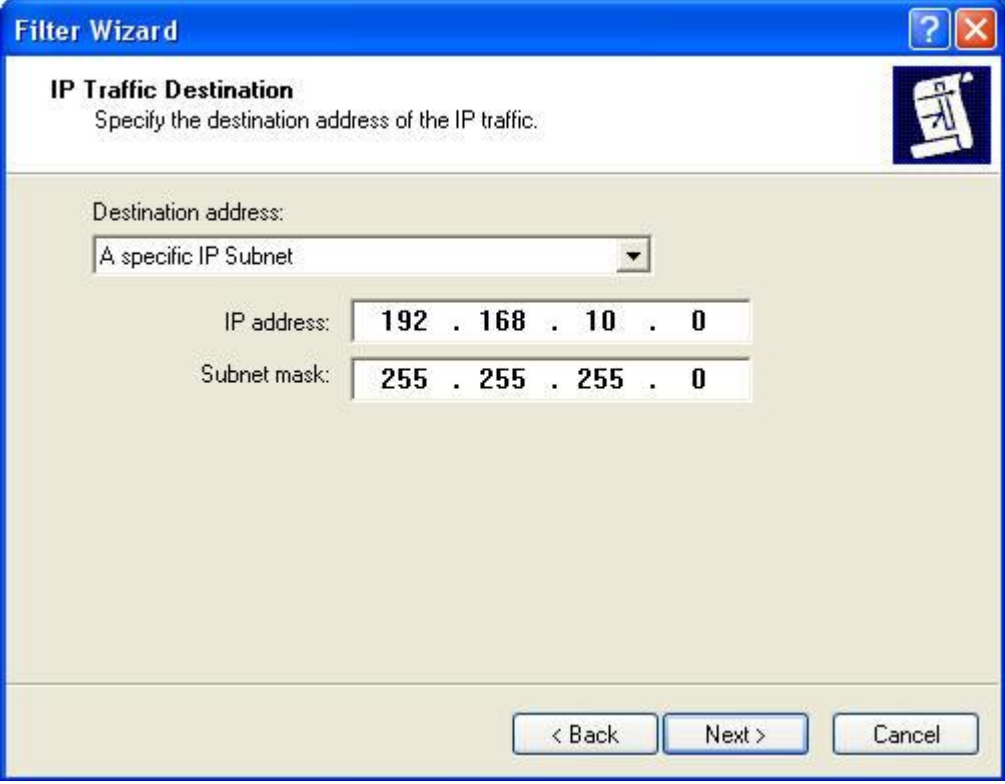
Step 44. Click next



Step 45. In Source address, click down the arrow to select the My IP Address.

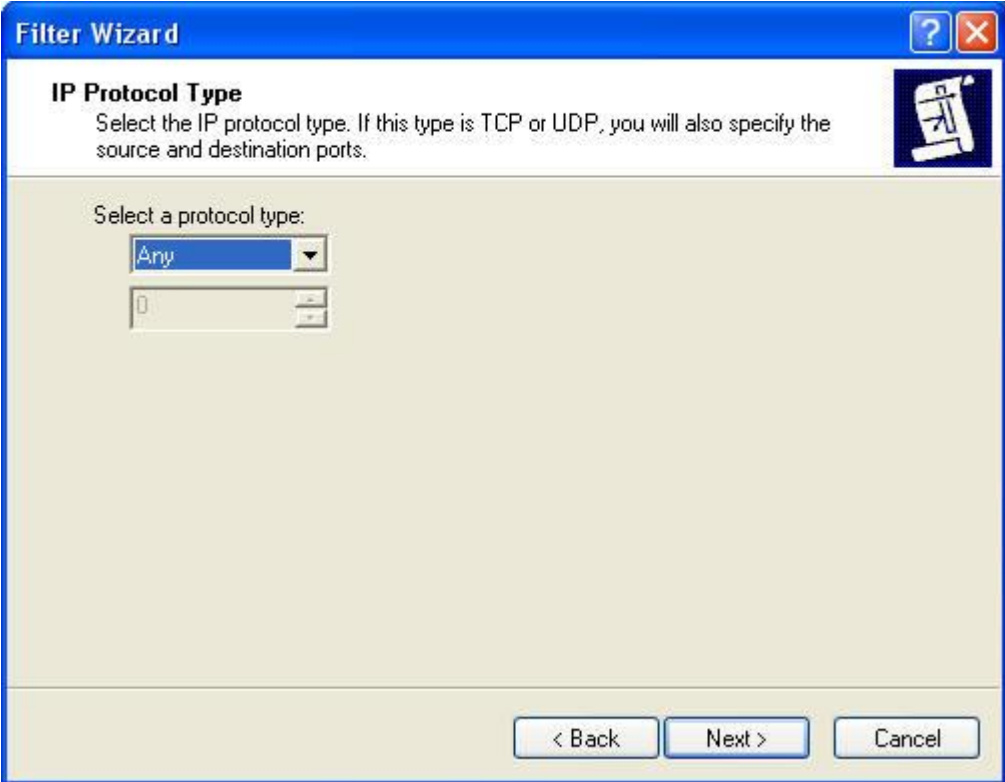


Step 46. In Destination address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.



The screenshot shows the 'Filter Wizard' window with the 'IP Traffic Destination' tab selected. The window has a blue title bar with a question mark and a close button. The main area is light beige. At the top, the title 'IP Traffic Destination' is in bold, followed by the instruction 'Specify the destination address of the IP traffic.' Below this, there is a 'Destination address:' label and a dropdown menu currently showing 'A specific IP Subnet'. Underneath the dropdown, there are two input fields: 'IP address:' with the value '192 . 168 . 10 . 0' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Step 47. Click next.

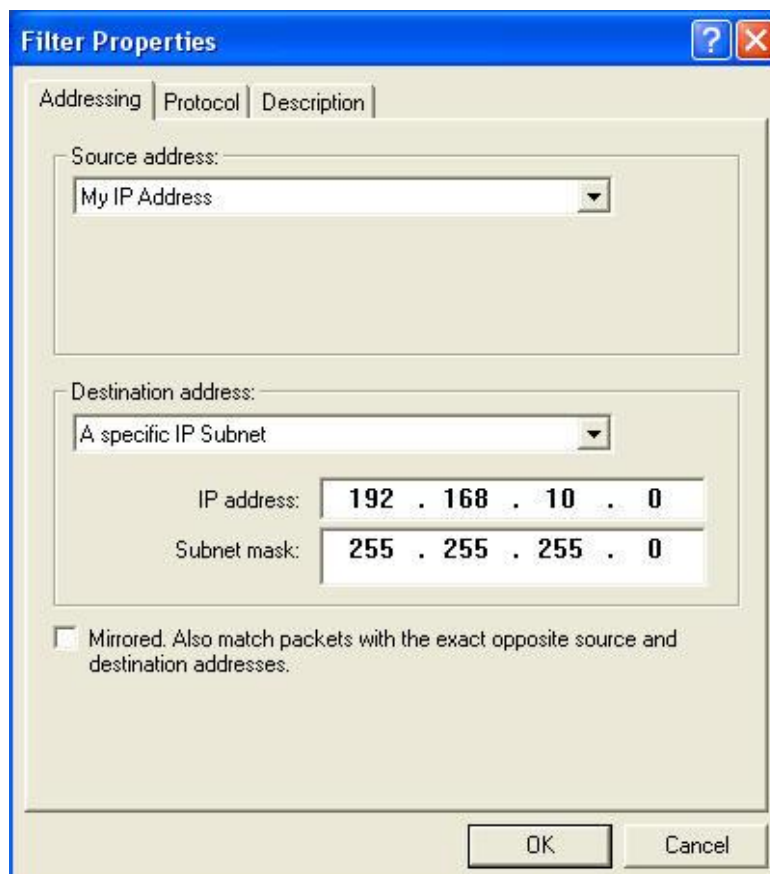


The screenshot shows the 'Filter Wizard' window with the 'IP Protocol Type' tab selected. The window has a blue title bar with a question mark and a close button. The main area is light beige. At the top, the title 'IP Protocol Type' is in bold, followed by the instruction 'Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.' Below this, there is a 'Select a protocol type:' label and a dropdown menu currently showing 'Any'. Underneath the dropdown, there is a small input field containing the number '0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

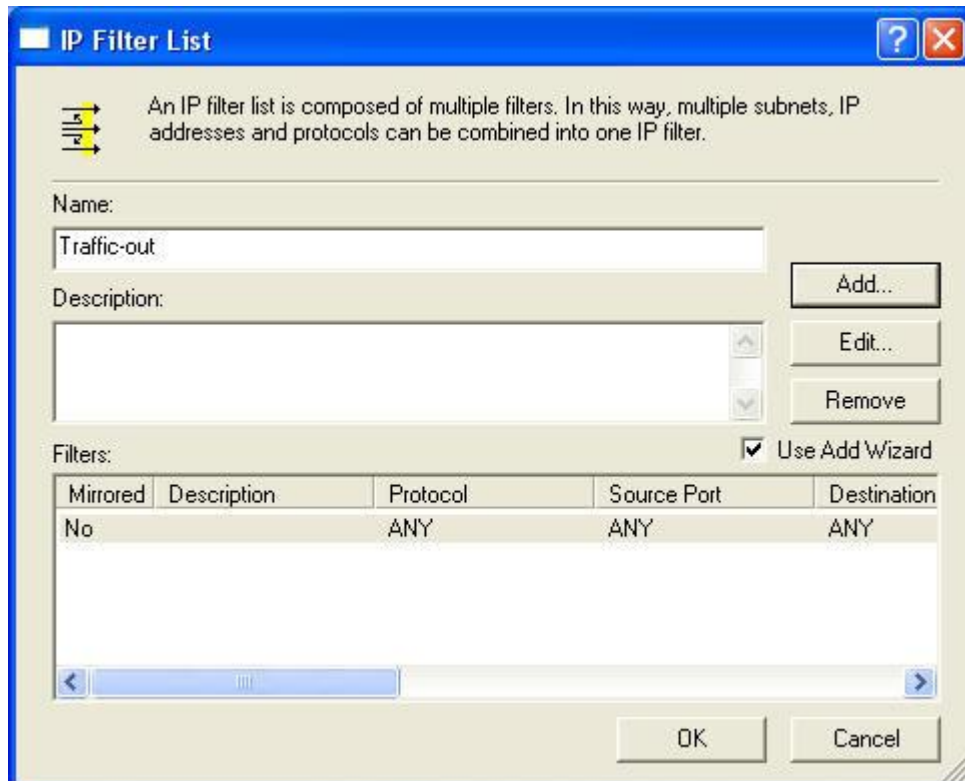
Step 48. Please enable Edit properties and click finish.



Step 49. Please don't enable Mirrored and click ok.



Step 50. Click ok.



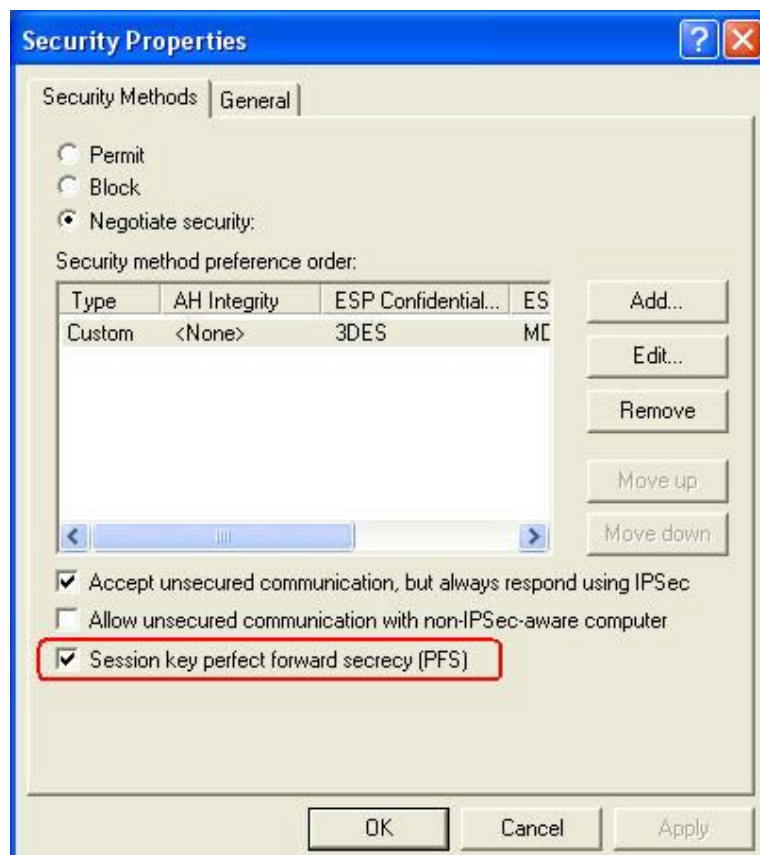
Step 51. Select Traffic-out and click next.



Step 52. Select Security and click edit.



Step 53. Enable Session key perfect forward secrecy (PFS) and click ok.



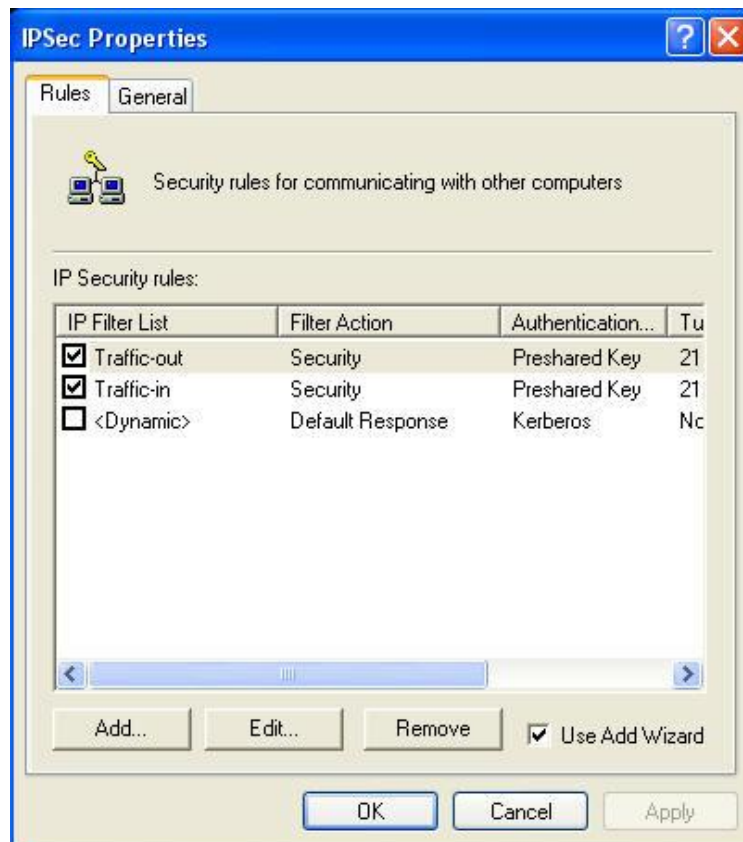
Step 54. Select Security and click next.



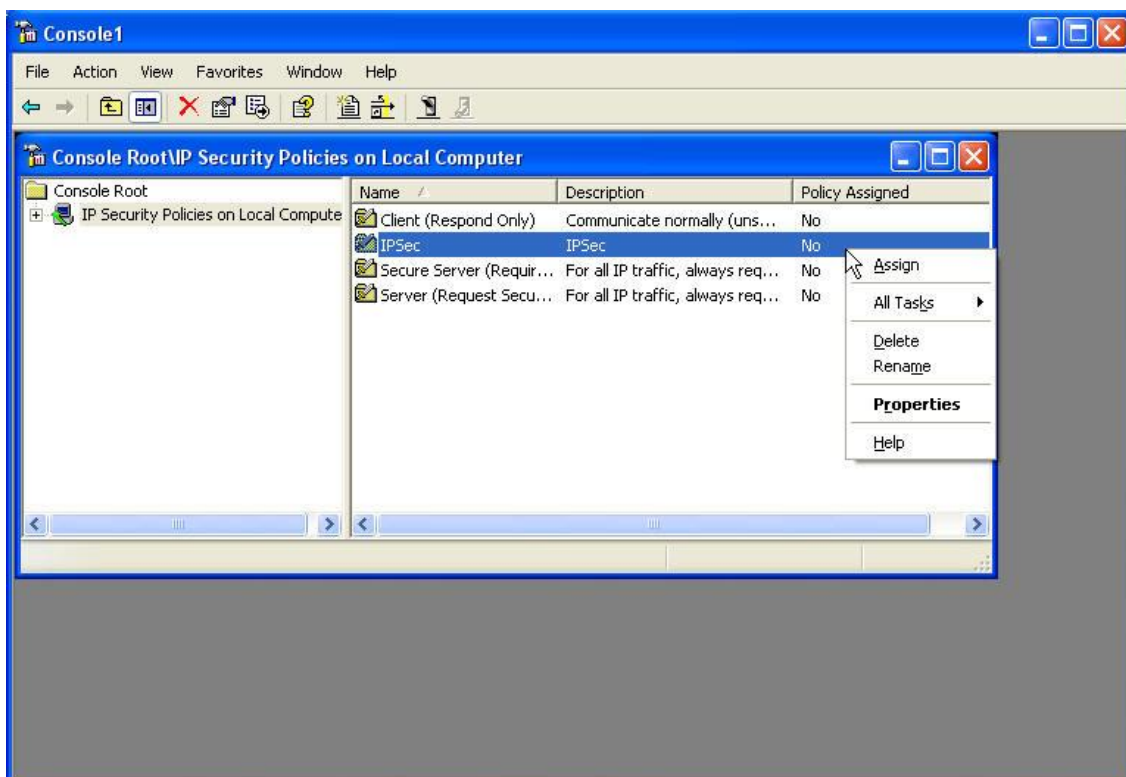
Step 55. Please don't enable Edit properties and click finish.



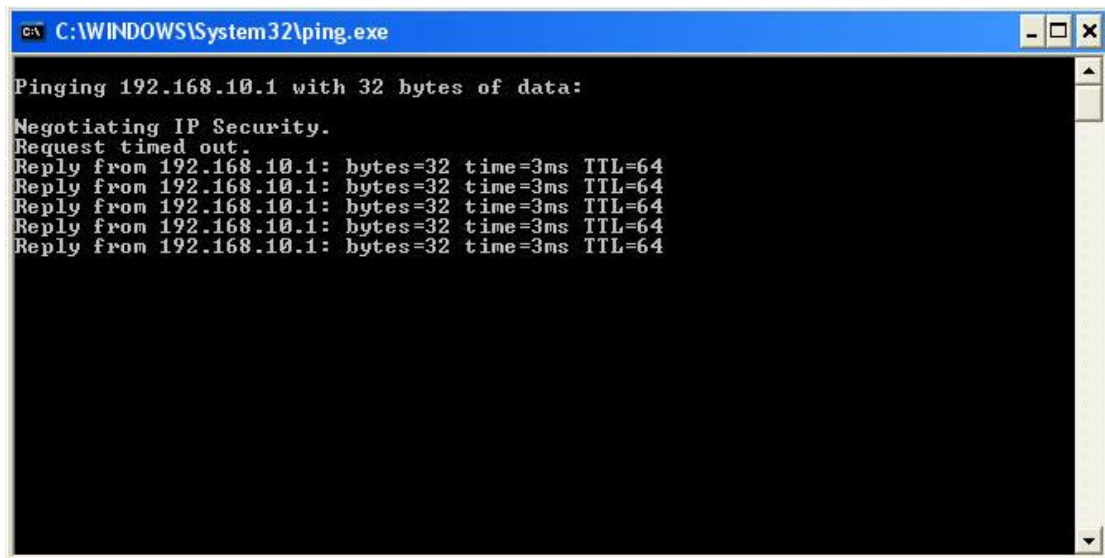
Step 56. Click apply first and then click ok.



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 Content Security Gateways using Aggressive mode Algorithm (3 DES 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 Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

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

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/>

Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will automatically choose 3DES for ENC Algorithm, MD5 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, @123A and @abcd123.

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

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	<input type="text" value="3DES"/>
AUTH Algorithm	<input type="text" value="MD5"/>
<input type="radio"/> Authentication Only	

Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

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

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None ▼
----------	--------

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

Policy Object > VPN > IPsec Autokey

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

[New Entry](#)

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 Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel

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

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bytes.)

Authentication Method	Preshare ▼
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will automatically choose 3DES for ENC Algorithm, MD5 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, @123A and @abcd123.

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

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, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

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

Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None
----------	------

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

IPSec Autokey

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN_B	61.11.11.11	192.168.10.0	None	Disconnect	<div style="display: inline-block; margin-right: 5px;">Connecting</div> <div style="display: inline-block; margin-right: 5px;">Modify</div> <div style="display: inline-block;">Remove</div>

New Entry

Example 4. Create a VPN connection between two Content Security Gateway using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

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 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 Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

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

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

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

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

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 1 to connect.

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

Step 6. Choose GRE/ IPSec and enter GRE Source IP, 192.168.50.100 and GRE Remote IP, 192.168.50.200.

NOTE: The Source IP and Remote IP should be in the same C Class.

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

Step 7. 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 8. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime.

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

Step 9. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None
----------	------

Step 10. Click OK to finish the setting of Company A.

Policy Object > VPN > IPSec Autokey

Name	Gateway IP	Destination Subnet	Algorithm	Status	Configure
VPN_A	211.22.22.22	192.168.20.0	None	Disconnect	<input type="button" value="Connecting"/> <input type="button" value="Modify"/> <input type="button" value="Remove"/>

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 Content 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 choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

VPN Auto Keyed Tunnel

Name

From Source ☒ LAN ☐ DMZ

Subnet / Mask /

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

To Destination

☒ Remote Gateway -- Fixed IP

Subnet / Mask /

☐ Remote Gateway -- Dynamic IP

Subnet / Mask /

☐ Remote Client -- Fixed IP or Dynamic IP

Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)

Authentication Method

Preshared Key

Step 5. In Encapsulation -> ISAKMP Algorithm, 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. Choose GRE/ IPsec and enter GRE Source IP, 192.168.50.200 and GRE Remote IP, 192.168.50.100.

Note. The Source IP and Remote IP should be in the same C Class.

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

Step 7. In IPsec Algorithm Table, choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.

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

Step 8. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPsec Lifetime.

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

Step 9. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Schedule	None
----------	------

Step 10. Click OK to finish the setting of Company B.

IPsec Autokey

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

[New Entry](#)

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

Preparation Task:

Company A External IP is 210.66.155.87

Internal IP is 192.168.10.X

Company B External IP is 210.66.155.89

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.

Step 1: Configure the Content Security Gateway as the following:

VPN Auto Keyed Tunnel	
Name	VPN_A
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	210.66.155.89
Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	
Subnet / Mask	/ 255.255.255.0
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	
Authentication Method	Preshare
Preshared Key	123456789
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2
IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
<input type="radio"/> Authentication Only	
<input checked="" type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
Keep alive IP :	192.168.20.1
<input checked="" type="checkbox"/> Aggressive mode	
My ID	(ex: 172.16.0.1 or @my_id.domain)
Peer ID	(ex: 172.16.0.2 or @peer_id.domain)
<input type="checkbox"/> GRE/IPSec	
GRE Local IP	(ex: 10.0.0.1)
GRE Remote IP	(ex: 10.0.0.2)
Schedule	None
<input type="checkbox"/> Show remote Network Neighborhood	

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:

4.3.6.2 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

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

PLANET Networking & Communication

Policy Object > VPN > PPTP Server

System

Interface

Policy Object

Address

Service

Schedule

Content Blocking

Virtual Server

VPN

IPsec Autokey

PPTP Server

PPTP Client

PPTP Server (Disable) :

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

User Name	Client IP	Uptime	Status	Configure
New Entry				

- n **PPTP Server** : Click **Modify** to select Enable or Disable.
- n **Client IP Range**: Display the IP addresses range for PPTP Client connection.
- n **User Name** : Displays the PPTP Client user's name for authentication.
- n **Client IP** : Displays the PPTP Client's IP address for authentication.
- n **Uptime** : Displays the connection time between PPTP Server and Client.
- n **Status** : Displays current connection status between PPTP Server and PPTP client.
- n **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.

PLANET
Networking & Communication

Policy Object > VPN > PPTP Server

System

Interface

Policy Object

Address

Service

Schedule

Content Blocking

Virtual Server

VPN

- IPsec Autokey
- PPTP Server**
- PPTP Client

Modify Server Design

☐ Disable PPTP

☒ Enable PPTP

☐ Encryption

Client IP Range : 192.238.6.1 -- 254

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

Schedule None

OK Cancel

n Disable PPTP : Check to disable PPTP Server.

n 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.

n 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.

n Schedule : Click the down arrow to select the schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

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.

n User name: Specify the PPTP client. This should be unique.

n Password: Specify the PPTP client password.

n Remote Client:

.. Single Machine: Check to connect to single computer.

.. Multi-Machine: Check to allow multiple computers connected to the PPTP server.


IP Address: Enter the PPTP Client IP address.

Netmask: Enter the PPTP Client subnet mask.

n 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.



Policy Object > VPN > PPTP Server

- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - Content Blocking
 - Virtual Server
 - VPN
 - IPSec Autokey
 - PPTP Server**
 - PPTP Client
- Policy
- Mail Security
- Anti-Attack

Add New PPTP Server

User Name :

Password :

Remote Client

☒ Single Machine

☐ Multi-Machine

IP Address :

Netmask :

Client IP assigned by

☒ IP Range

☐ Fixed IP :

OK Cancel


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.



Policy Object > VPN > PPTP Server

- System
- Interface
- Policy Object
 - Address
 - Service
 - Schedule
 - Content Blocking
 - Virtual Server
 - VPN
 - IPSec Autokey
 - PPTP Server**
 - PPTP Client
- Policy
- Mail Security
- Anti-Attack

Modify PPTP Server

User Name :

Password :

Remote Client

☒ Single Machine

☐ Multi-Machine

IP Address :

Netmask :

Client IP assigned by

☒ IP Range

☐ Fixed IP :

OK Cancel

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

User Name	Client IP	Uptime	Status	Configure
planet	0.0.0.0	---	Disconnect	Modify Remove

Microsoft Internet Explorer
Are you sure you want to remove?
[OK](#) [Cancel](#)

4.3.6.3 PPTP Client

This function allows the Content Security Gateway dial-up to remote PPTP server and access 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 :

User Name	Server Address	Encryption	Uptime	Status	Configure
New Entry					

- n **User Name** : Displays the PPTP Client user's name for authentication.
- n **Server Address** : Displays the PPTP Server's IP address for authentication.
- n **Encryption** : Displays the PPTP Client Encryption ON or OFF.
- n **Uptime** : Displays the connection time between PPTP Server and Client.

- n **Status** : Displays current connection status between PPTP Server and PPTP client.
- n **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**.

PLANET Network & Communication

Policy Object > VPN > PPTP Client

Add New PPTP Client

User Name :

Password :

Server Address : ☐ Encryption

Remote Server

☒ Single Machine

☐ Multi-Machine

IP Address :

Netmask :

☐ always-connect

☐ Auto-Connect when sending packet through the link

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

Schedule

☐ NAT(Connect to Windows PPTP Server)

OK Cancel

Step 2. Configure the parameters.

- n **User name:** Specify the PPTP client. This should be unique.
- n **Password:** Specify the PPTP client password.
- n **Server Address:** Enter the PPTP Server's IP address.
- n **Encryption:** Enable or Disabled the Encryption.
- n **Remote Server:**
 - **Single Machine:** Check to connect to single computer.
 - **Multi-Machine:** Check to allow connecting to multiple computers on remote site.
- n **IP Address :** Enter the PPTP Client IP address.
- n **Netmask:** Enter the PPTP Client subnet mask.
- n **Always-connect:** Select to keep on the connection working.
- n **Auto-Connect when sending packet through the link:** Check to enable the auto-connection whenever there's packet to transmit over the connection.
- n **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.
- n **Schedule :** Click the down arrow to select the schedule, which was pre-determined in Schedule.

Refer to the corresponding section for details.

- n **NAT (Connect to Windows PPTP Server):** Select this function to setup the connection with PPTP VPN Client of CS-500 and Windows PPTP Server.

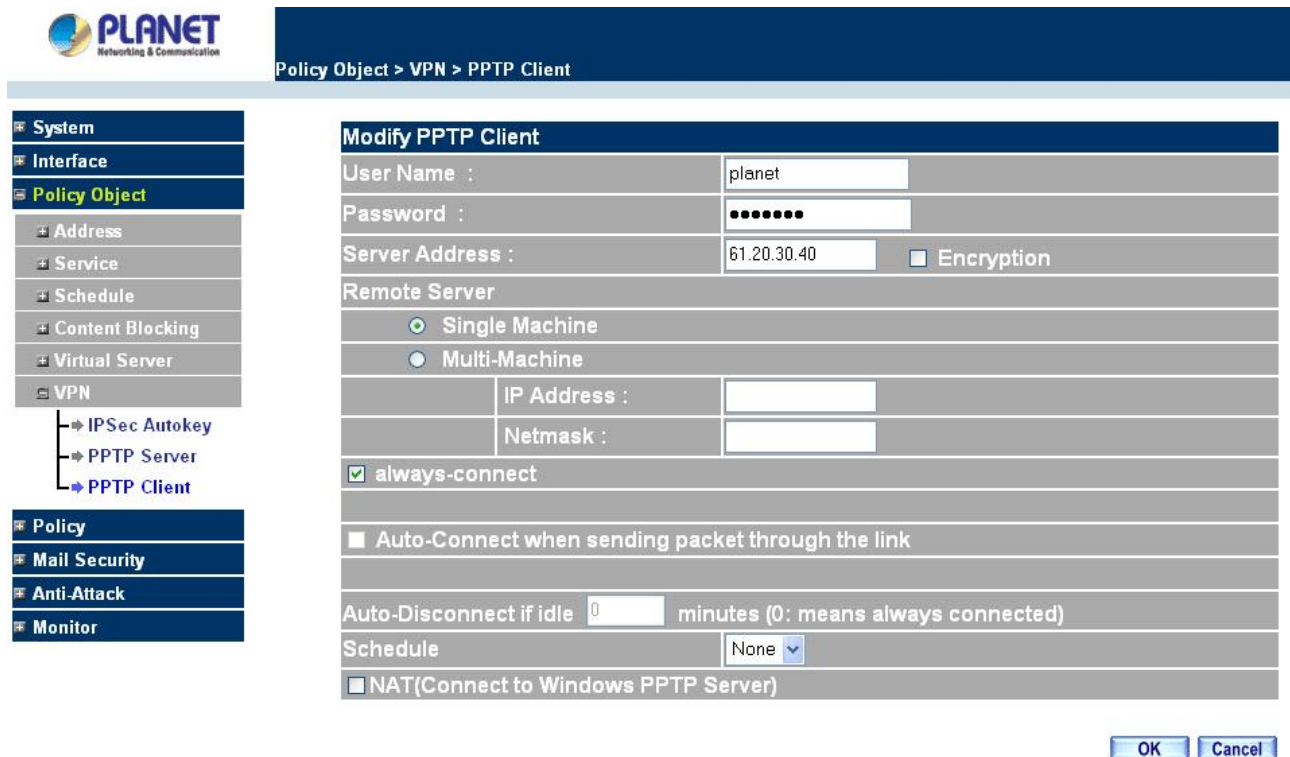
Click **OK** to save modifications or click **Cancel** to cancel modifications.

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.



The screenshot shows the PLANET Network & Communication software interface. On the left is a navigation tree with categories: System, Interface, Policy Object, Policy, Mail Security, Anti-Attack, and Monitor. Under 'Policy Object', there are sub-items: Address, Service, Schedule, Content Blocking, Virtual Server, and VPN. Under 'VPN', there are sub-items: IPsec Autokey, PPTP Server, and PPTP Client. The 'PPTP Client' item is selected. The main window displays the 'Modify PPTP Client' configuration form. The form includes fields for User Name (planet), Password (masked with dots), Server Address (61.20.30.40), and an Encryption checkbox. Below these are radio buttons for Remote Server type: Single Machine (selected) and Multi-Machine. Under Multi-Machine, there are fields for IP Address and Netmask. There is a checked checkbox for 'always-connect' and an unchecked checkbox for 'Auto-Connect when sending packet through the link'. The 'Auto-Disconnect if idle' field is set to 0 minutes, with a note '(0: means always connected)'. The 'Schedule' dropdown is set to 'None'. At the bottom, there is a checkbox for 'NAT(Connect to Windows PPTP Server)'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

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.



The screenshot shows the PLANET Policy Object configuration interface. On the left is a navigation tree with categories: System, Interface, Policy Object, Address, Service, Schedule, Content Blocking, Virtual Server, and VPN. Under VPN, there are sub-items: IPsec Autokey, PPTP Server, and PPTP Client. The main area displays the 'PPTP Client' configuration table:

User Name	Server Address	Encryption	Uptime	Status	Configure
planet	61.20.30.40	OFF	---	Disconnect	Connecting Modify Remove

Below the table, a Microsoft Internet Explorer dialog box is displayed with the message: 'Are you sure you want to remove?' and buttons for 'OK' and 'Cancel'.

4.4 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 Content Security Gateway.

What is Policy?

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

- (1) Outgoing: 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?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, 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**.

4.4.1 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.

PLANET Networking & Communication

Policy > Outgoing

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

New Entry

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

The fields in the Outgoing window are:

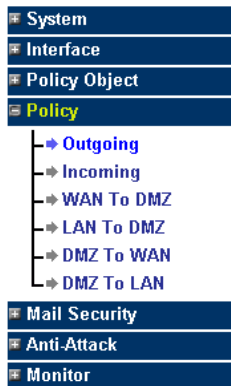
- n **Source:** Source network addresses that are specified in the LAN section of **Address** menu, or all the LAN network addresses.
- n **Destination:** Destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- n **Service:** Specify services provided by WAN network servers.
- n **Action:** Control actions to permit or deny packets from LAN networks to WAN network travelling through the Content Security Gateway.
- n **Option:** Specify the monitoring functions on packets from LAN networks to WAN networks travelling through the Content Security Gateway.
- n **Configure:** Modify settings.
- n **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



Add New Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Filtering	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

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.

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.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

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

Max. Concurrent Sessions: The maximum concurrent sessions that allows passing through CS-500. 0 means it is unlimited.

Step 3: Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

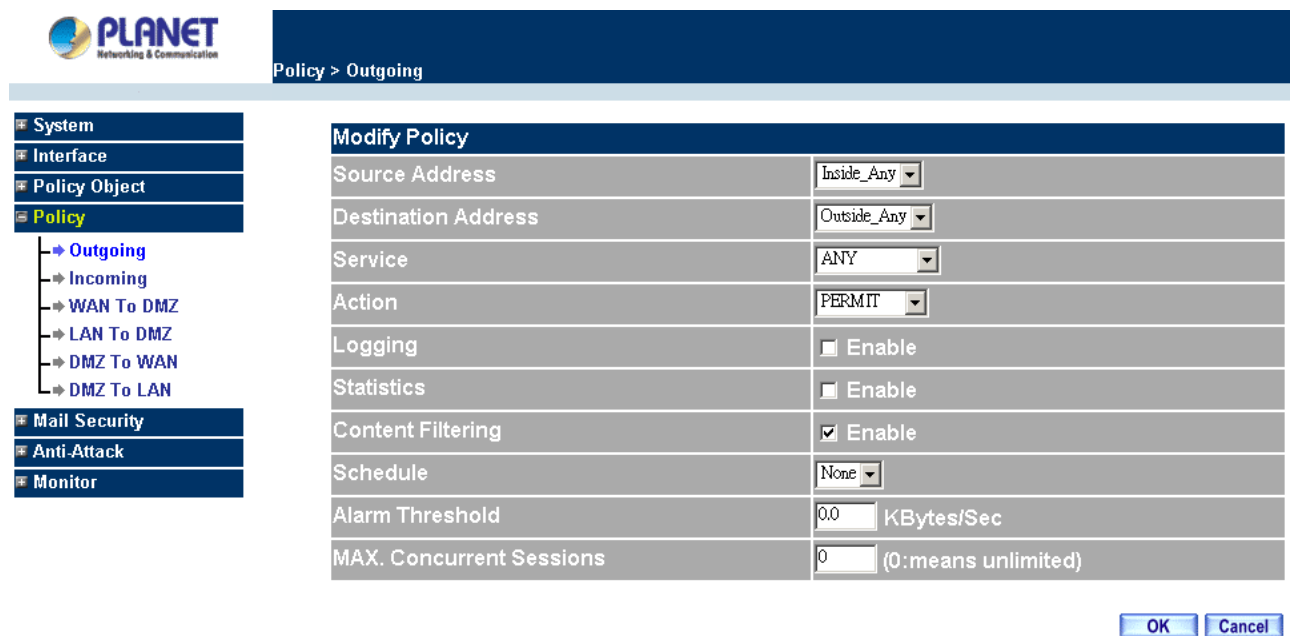
Modifying an Outgoing policy

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 shows the PLANET Network & Communication web interface. On the left is a navigation menu with options: System, Interface, Policy Object, Policy (selected), Outgoing (selected), Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, Anti-Attack, and Monitor. The main area is titled 'Policy > Outgoing' and contains a 'Modify Policy' form. The form has the following fields:


Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Filtering	<input checked="" type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

At the bottom right of the form are two buttons: **OK** and **Cancel**.

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.



Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			Modify Remove	To <input type="text" value="1"/>


[New Entry](#)

Microsoft Internet Explorer
Are you sure you want to remove ?
[确定](#) [取消](#)

- System
- Interface
- Policy Object
- Policy
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
- Mail Security
- Anti-Attack
- Monitor

Enabled Monitoring function:

Log: If Logging is enabled in the outgoing policy, the Content Security Gateway will log the traffic and event passing through the Content Security Gateway. The Administrator can click **Log** on the left menu bar to get the traffic and event logs of the specified policy.



Monitor > Log > Traffic

Jan 1 00:29:38

Time	Source	Destination	Protocol	Port	Disposition
Jan 1 00:29:38	192.168.1.11	192.168.1.1	TCP	1059 => 80	
Jan 1 00:29:38	192.168.1.11	192.168.1.1	TCP	1058 => 80	
Jan 1 00:29:38	192.168.1.11	192.168.1.1	TCP	1056 => 80	
Jan 1 00:29:38	192.168.1.11	192.168.1.1	TCP	1057 => 80	
Jan 1 00:28:15	192.168.1.11	192.168.1.1	TCP	1057 => 80	
Jan 1 00:28:14	192.168.1.11	192.168.1.1	TCP	1056 => 80	
Jan 1 00:24:53	192.168.1.11	192.168.1.1	TCP	1049 => 80	
Jan 1 00:24:53	192.168.1.11	192.168.1.1	TCP	1048 => 80	
Jan 1 00:14:57	192.168.1.11	192.168.1.1	TCP	1040 => 80	
Jan 1 00:14:56	192.168.1.11	192.168.1.1	TCP	1039 => 80	
Jan 1 00:08:43	192.168.1.11	192.168.1.1	TCP	1036 => 80	
Jan 1 00:08:43	192.168.1.11	192.168.1.1	TCP	1035 => 80	
Jan 1 00:08:43	192.168.1.11	192.168.1.1	TCP	1033 => 80	
Jan 1 00:08:43	192.168.1.11	192.168.1.1	TCP	1034 => 80	
Jan 1 00:07:18	192.168.1.11	192.168.1.1	TCP	1034 => 80	
Jan 1 00:07:12	192.168.1.11	192.168.1.1	TCP	1033 => 80	

[Clear Logs](#) [Download Logs](#)

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor
 - Log
 - Traffic
 - Event
 - Connection
 - Log Backup
 - Alarm
 - Statistics
 - Status

NOTE: System Administrator can back up and clear logs in this window. Check the chapter entitled “Log” to get details about the log and ways to back up and clear logs.

Alarm: If Logging is enabled in the outgoing policy, the Content Security Gateway will log the traffic alarms and event alarms passing through the Content Security Gateway. The Administrator can click **Alarm** on the left menu to get the logs of flow and event alarms of the specified policy.

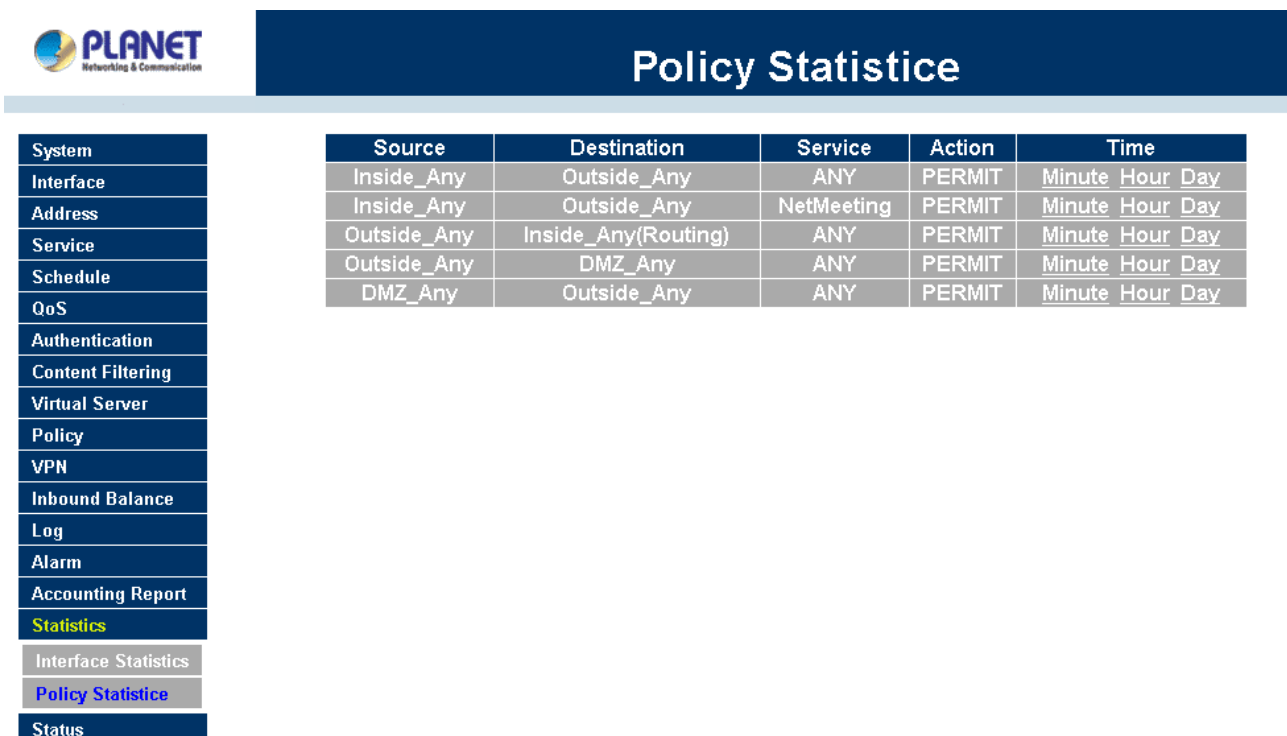


Monitor > Alarm > Traffic

Time	Source	Destination	Service	Traffic
There is no message !				

NOTE: The Administrator can also get information on alarm logs from the Alarm window. Please refer to the section entitled “**Alarm**” for more information.

Statistics: If statistics is enabled in the outgoing policy, the Content Security Gateway will display the flow statistics passing through the Content Security Gateway.



Policy Statistic

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	PERMIT	Minute Hour Day
Inside_Any	Outside_Any	NetMeeting	PERMIT	Minute Hour Day
Outside_Any	Inside_Any(Routing)	ANY	PERMIT	Minute Hour Day
Outside_Any	DMZ_Any	ANY	PERMIT	Minute Hour Day
DMZ_Any	Outside_Any	ANY	PERMIT	Minute Hour Day

NOTE: The Administrator can also get flow statistics in **Statistics**. Please refer to **Statistics** for more details.

4.4.2 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:

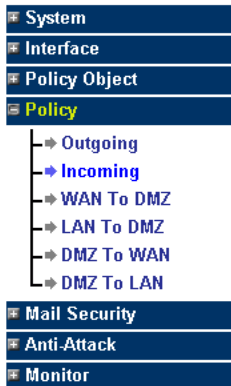
- n Source:** Source networks which are specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.
- n Destination:** Destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.
- n Service:** Services supported by Virtual Servers (or Mapped IP).
- n Action:** Control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.
- n Option:** Specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Content Security Gateway.
- n Configure:** Modify settings or remove incoming policy.
- n 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.



Policy > Incoming



Add New Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

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.

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.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

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

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

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.

The screenshot shows the Planet Network & Communication web interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy (selected), Outgoing, Incoming (selected), WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, Anti-Attack, and Monitor. The main content area is titled 'Policy > Incoming' and displays the 'Modify Policy' form. The form fields are as follows:

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0: means unlimited)

At the bottom right of the form are two buttons: **OK** and **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.

The screenshot shows the Planet Network & Communication web interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Policy > Incoming' and displays a table of incoming policies. The table has the following columns: Source, Destination, Service, Action, Option, Configure, and Move. The data row is as follows:

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

Below the table is a 'New Entry' button. A confirmation dialog box is displayed in the foreground, titled 'Microsoft Internet Explorer'. The dialog box contains a question mark icon and the text 'Are you sure you want to remove ?'. There are two buttons at the bottom: '确定' (OK) and '取消' (Cancel).

4.4.3 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.

The screenshot shows the PLANET Networking & Communication interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy (selected), Mail Security, Anti-Attack, and Monitor. Under the Policy menu, the following sub-items are listed: Outgoing, Incoming, WAN To DMZ (highlighted), LAN To DMZ, DMZ To WAN, and DMZ To LAN. The main area displays the 'Policy > WAN To DMZ' window. It features a table with the following columns: Source, Destination, Service, Action, Option, Configure, and Move. The table contains one entry with Source 'Outside_Any', Destination 'DMZ_Any', Service 'ANY', and Action represented by a purple circle icon. The Configure column has 'Modify' and 'Remove' buttons. The Move column has a 'To' dropdown menu showing '1'. A 'New Entry' button is located below the table.

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

New Entry

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 Content Security Gateway.

Option: Specify the monitoring functions of packets from WAN network to DMZ network travelling through Content Security Gateway.

Configure: Modify settings or remove policies.

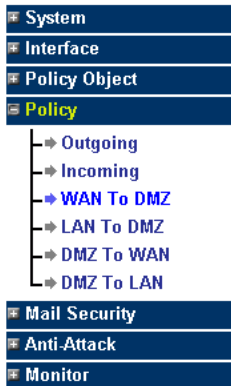
Move: This sets the priority of the policies, number 1 being the highest priority.

Adding a new WAN To DMZ Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Policy > WAN To DMZ



Add New Policy

Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

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)

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.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: Set a maximum flow rate (in Kbytes/Sec). An alarm will be send if a flow rate exceeds the specified value.

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

Step 3: Click **OK**.

Modifying an 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 shows the PLANET Network & Communication web interface. The left sidebar contains a navigation menu with the following items: System, Interface, Policy Object, Policy (highlighted), Outgoing, Incoming, WAN To DMZ (highlighted), LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, Anti-Attack, and Monitor. The main content area is titled 'Policy > WAN To DMZ' and displays the 'Modify Policy' configuration window. The configuration fields are as follows:

Modify Policy	
Source Address	Outside_Any
Destination Address	DMZ_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

At the bottom right of the configuration window, there are two buttons: **OK** and **Cancel**.

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.

PLANET Networking & Communication

Policy > WAN To DMZ

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

New Entry

Microsoft Internet Explorer

Are you sure you want to remove ?

確定 取消

4.4.4 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.

PLANET Networking & Communication

Policy > DMZ To WAN

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

New Entry

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 Content Security Gateway.

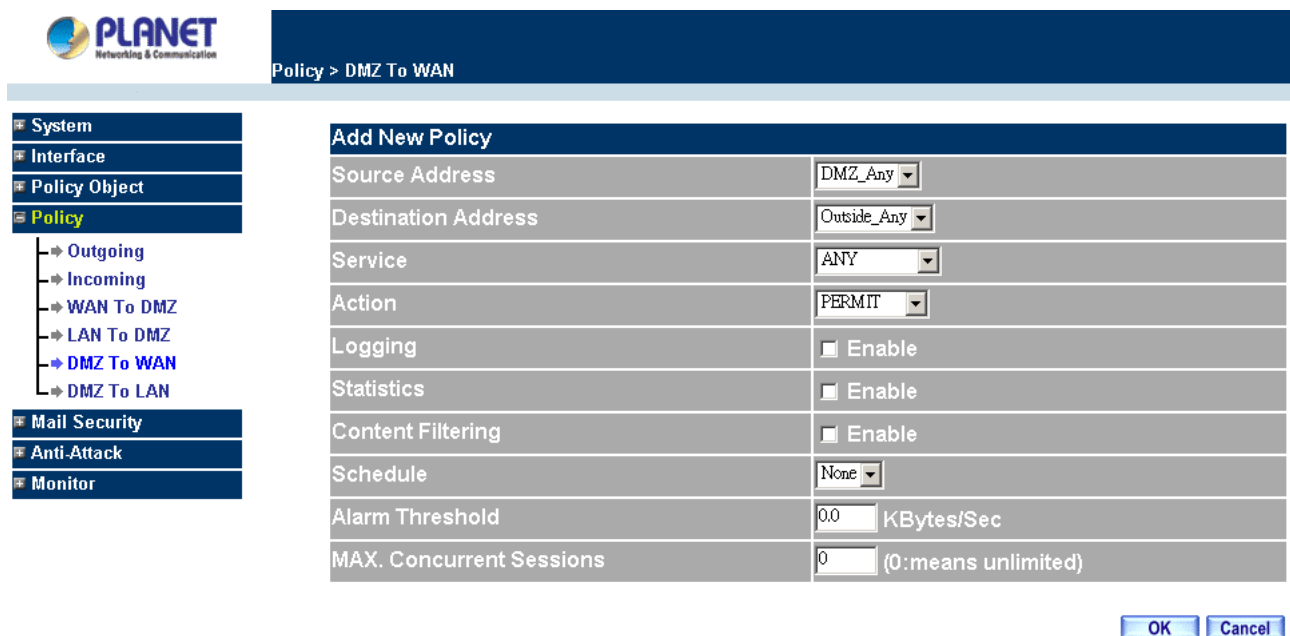
Option: Specify the monitoring functions on packets from the DMZ network to WAN networks travelling through the Content Security Gateway.

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.



The screenshot shows the PLANET web interface with the 'Policy > DMZ To WAN' menu path. On the left is a navigation tree with categories: System, Interface, Policy Object, Policy (selected), Mail Security, Anti-Attack, and Monitor. Under 'Policy', there are sub-items: Outgoing, Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN (selected), and DMZ To LAN. The main area displays the 'Add New Policy' form with the following fields:

Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Filtering	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

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

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.

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.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

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

Max. Concurrent Sessions: The maximum concurrent sessions that allows to pass through CS-500. 0 means it is unlimited.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding.

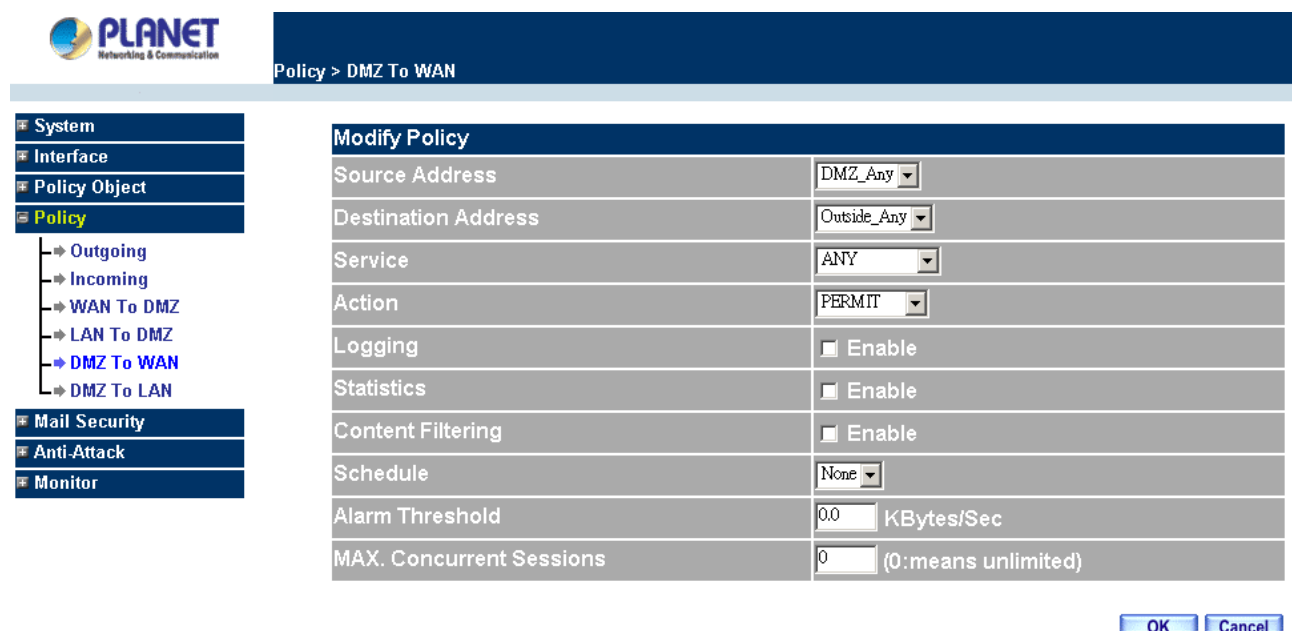
Modifying a DMZ To WAN policy:

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 Network & Communication software interface. On the left is a navigation tree with categories: System, Interface, Policy Object, Policy, Mail Security, Anti-Attack, and Monitor. The 'Policy' category is expanded, showing sub-items: Outgoing, Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN (highlighted), and DMZ To LAN. The main window title is 'Policy > DMZ To WAN'. The 'Modify Policy' form contains the following fields:

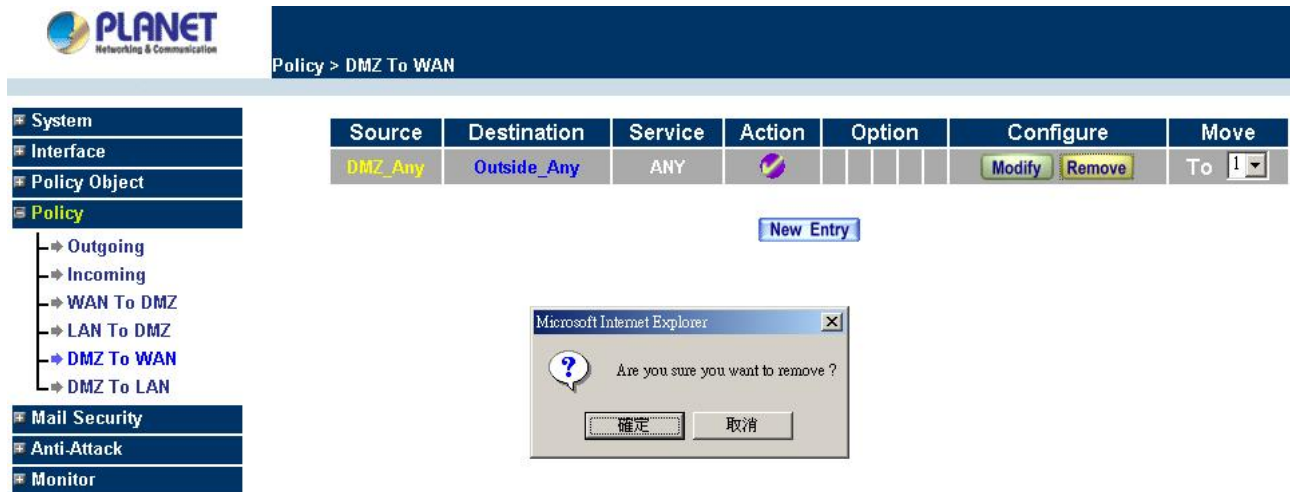
Source Address	DMZ_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Filtering	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
MAX. Concurrent Sessions	0 (0:means unlimited)

At the bottom right of the form 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**.



4.5 Mail Security

This section provides the Administrator to configure Mail Security rule for protecting client PC from virus and spam mail attacking. Meanwhile, CS-500 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.

4.5.1 Configure

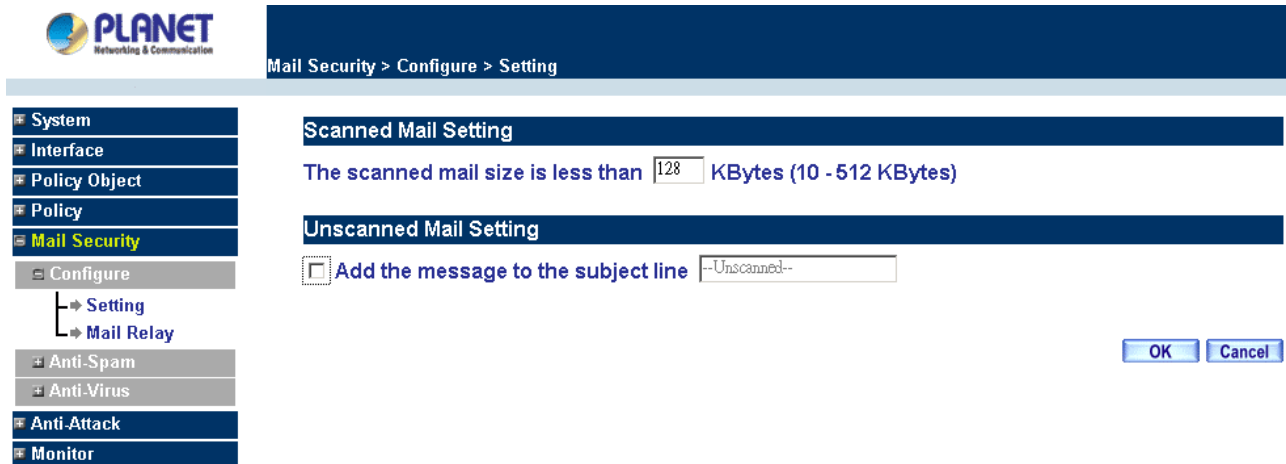
About the Mail Security Configure function, it means the dealing standard towards mail of CS-500. In this chapter, it is defined as Setting and Mail Relay.

Setting:

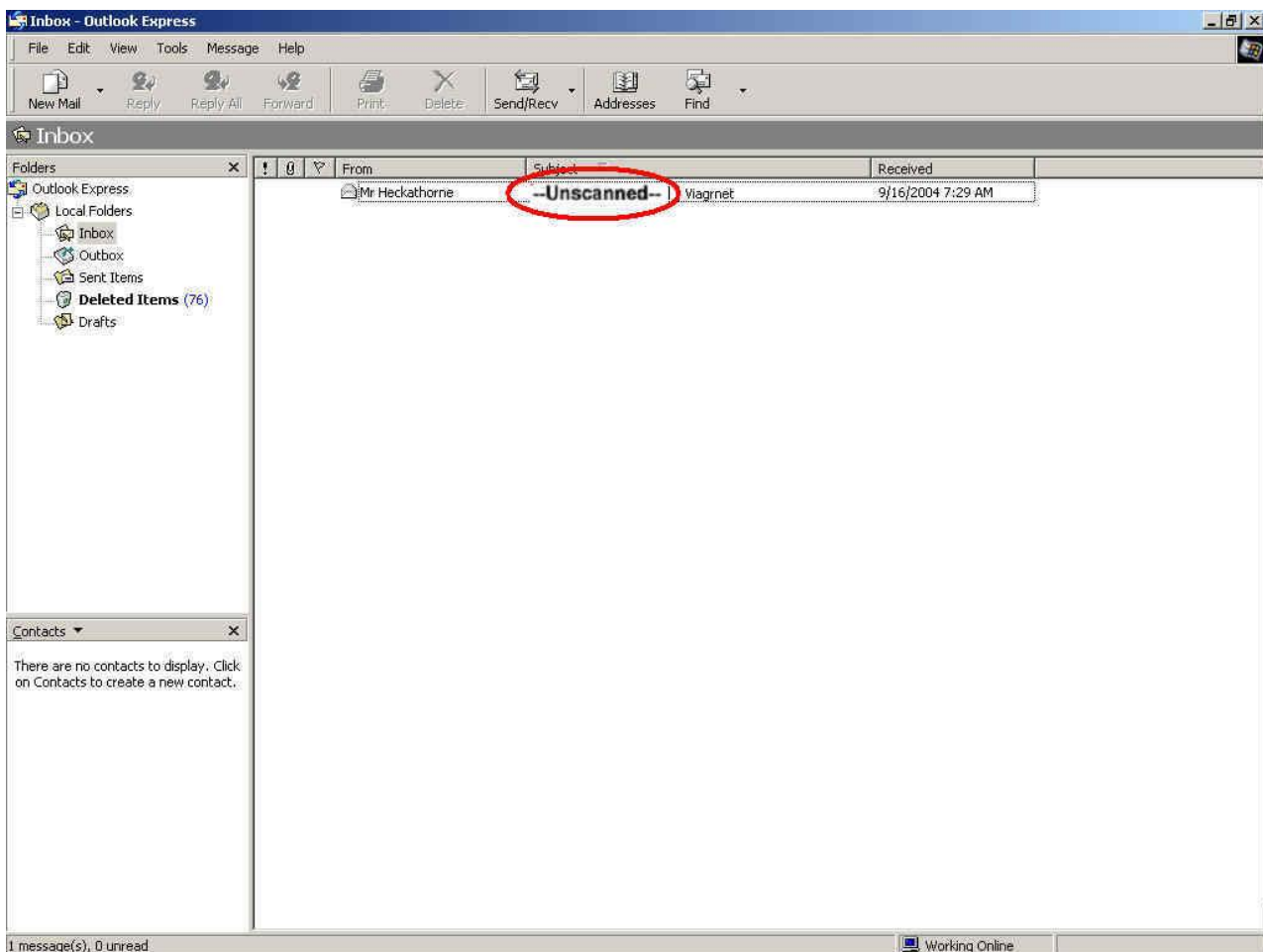
Define the required fields of setting:

Scanned Mail Setting: It can 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-500, it can be marked an unscanned message in the mail subject. For example, if the mail size is less 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-500, 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-500 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**:

- n Select **Domain Name of Internal Mail Server**
- n **Domain Name of Mail Server**: Enter the Domain Name
- n **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-500 and redirect to the mail server after filtering.

Example 2: To setup CS-500 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-500's WAN Port IP: 172.16.1.12

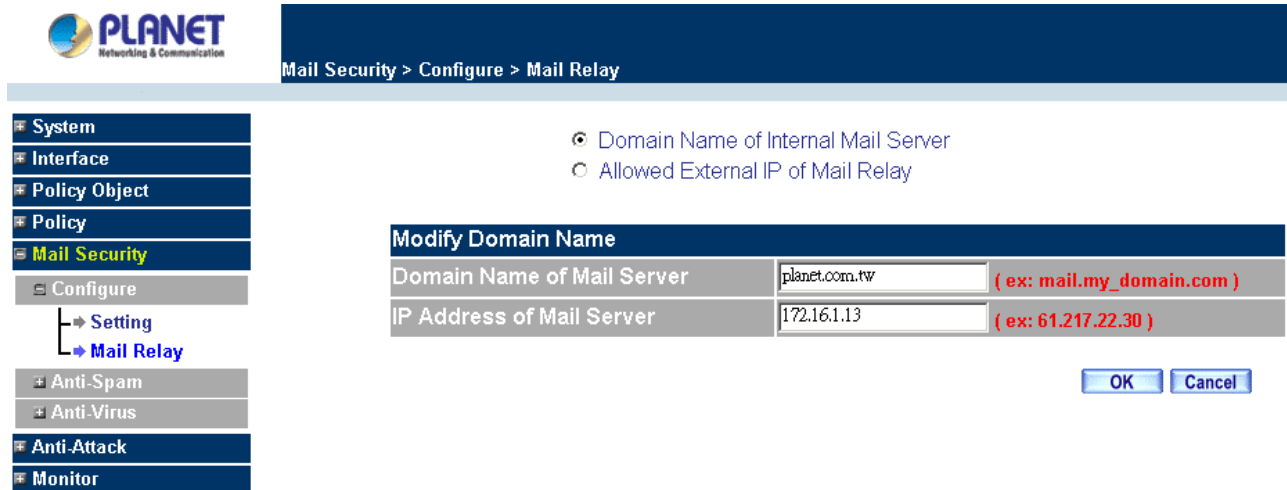
Mail Server IP: 172.16.1.13

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:

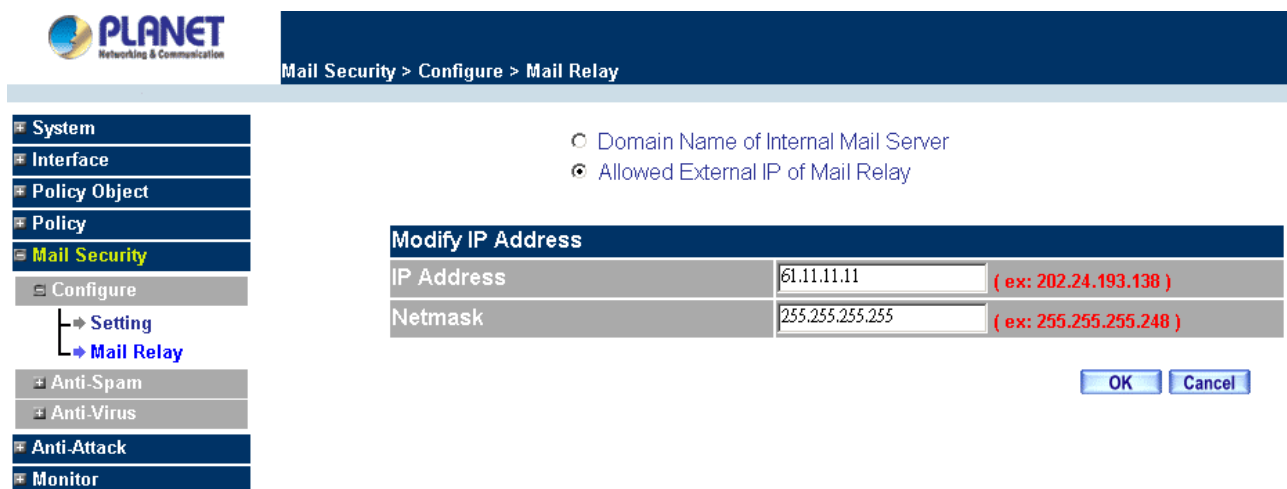
- n Select **Domain Name of Internal Mail Server**
- n **Domain Name of Mail Server:** Enter the Domain Name
- n **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.



The screenshot shows the PLANET Network & Communication interface. The breadcrumb trail is "Mail Security > Configure > Mail Relay". On the left, a navigation menu has "Mail Security" expanded, showing "Configure" and "Setting" (with "Mail Relay" selected). The main area has two radio buttons: "Domain Name of Internal Mail Server" (selected) and "Allowed External IP of Mail Server". Below is a "Modify Domain Name" form with two fields: "Domain Name of Mail Server" (value: planet.com.tw, example: mail.my_domain.com) and "IP Address of Mail Server" (value: 172.16.1.13, example: 61.217.22.30). "OK" and "Cancel" buttons are at the bottom right.

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

- n Select **Allowed External IP of Mail Relay**
- n **IP Address:** Enter the IP Address of external sender
- n Enter the **Netmask**
- n Complete Mail Relay setting



The screenshot shows the same PLANET interface. The breadcrumb trail is "Mail Security > Configure > Mail Relay". In the navigation menu, "Mail Relay" is selected under "Setting". The main area now has "Allowed External IP of Mail Relay" selected. Below is a "Modify IP Address" form with two fields: "IP Address" (value: 61.11.11.11, example: 202.24.193.138) and "Netmask" (value: 255.255.255.255, example: 255.255.255.248). "OK" and "Cancel" buttons are at the bottom right.

Example 3: The Headquarters setup CS-500 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-500: 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:

- n Select **Domain Name of Internal Mail Server**
- n **Domain Name of Mail Server:** Enter the Domain Name
- n **IP Address of Mail Server:** Enter the IP address that Mail Server's domain name mapped to.

Planet Network & Communication

Mail Security > Configure > Mail Relay

System
Interface
Policy Object
Policy
Mail Security
 Configure
 Setting
 Mail Relay
 Anti-Spam
 Anti-Virus
 Anti-Attack
 Monitor

☒ Domain Name of Internal Mail Server
☐ Allowed External IP of Mail Relay

Modify Domain Name		
Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
IP Address of Mail Server	61.11.11.12	(ex: 61.217.22.30)

OK Cancel

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

- n Select **Allowed External IP of Mail Relay**
- n **IP Address:** Enter the IP Address of external sender
- n Enter the **Netmask**
- n Complete Mail Relay setting

Planet Network & Communication

Mail Security > Configure > Mail Relay

System
Interface
Policy Object
Policy
Mail Security
 Configure
 Setting
 Mail Relay
 Anti-Spam
 Anti-Virus
 Anti-Attack
 Monitor

☐ Domain Name of Internal Mail Server
☒ Allowed External IP of Mail Relay

Modify IP Address		
IP Address	211.22.22.22	(ex: 202.24.193.138)
Netmask	255.255.255.255	(ex: 255.255.255.248)

OK Cancel

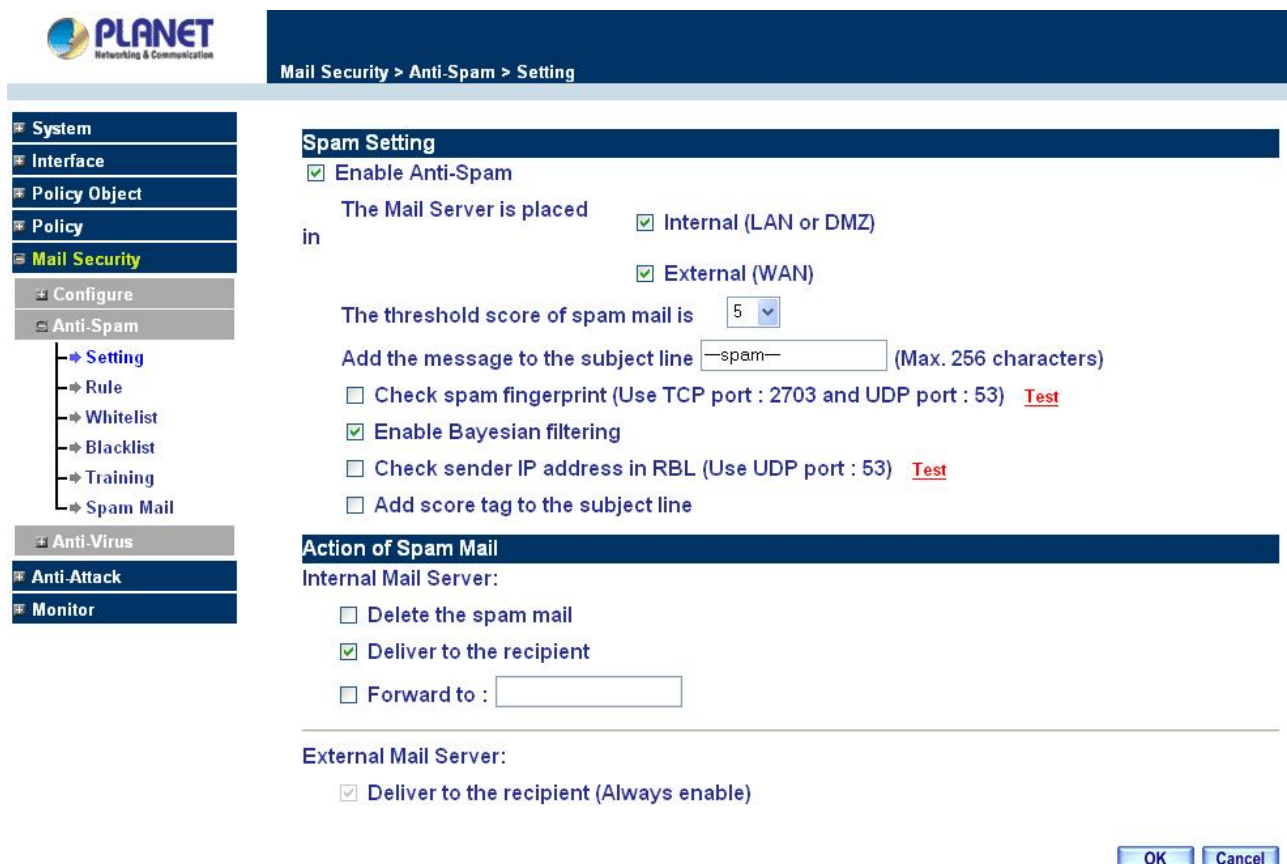
4.5.2 Anti-Spam

CS-500 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**:

4.5.2.1 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-500 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) ☒ External (WAN)

The threshold score of spam mail is

Add the message to the subject line (Max. 256 characters)

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

☒ Enable Bayesian filtering

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

☐ Add score tag to the subject line

Action of Spam Mail

Internal Mail Server:

☐ Delete the spam mail

☒ Deliver to the recipient

☐ Forward to :

External Mail Server:

☒ Deliver to the recipient (Always enable)

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

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.

The threshold score of spam mail is: CS-500 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-500 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-500 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.

Add score tag to the subject line: If select this function, all received mail will be added a score tag in the mail subject.

Check sender IP address in RBL (Realtime Blackhole List): Select this function to allow CS-500 checking mail with RBL list.

Action of Spam Mail: When CS-500 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: You can configure CS-500 to forward spam mail to a specific mail account; it will 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 **Add score tag to the subject line**
5. Select **Deliver to the recipient**
6. Click **OK**.

4.5.2.2 Rule

The Content 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-500 to record the mail type by auto-learning system 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.

PLANET
Networking & Communication

Mail Security > Anti-Spam > Rule

- System
- Interface
- Policy Object
- Policy
- Mail Security
 - Configure
 - Anti-Spam
 - Setting
 - Rule
 - Whitelist
 - Blacklist
 - Training
 - Spam Mail

Rule Name	Classification	Action	Comments	Configure	Move
New Entry					

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**, or **Forward to** another mail account.
- **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**, and **Date**.
- **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.

Mail Security > Anti-Spam > Rule

Rule Name : Comments :

Combination : Classification :

Action : Auto-Training :

Item	Condition	Pattern	Configure
<input type="text" value="Received"/>	<input type="text" value="Contains"/>	<input type="text" value="support@planet.com.tw"/>	<input type="button" value="Remove"/>
<input type="text" value="From"/>	<input type="text" value="Contains"/>	<input type="text" value="test@test.com"/>	<input type="button" value="Next Row"/> <input type="button" value="Remove"/>

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**.

Mail Security > Anti-Spam > Rule

Rule Name	Classification	Action	Comments	Configure	Move
PLanet	Spam	Delete spam mail		<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To <input type="text" value="1"/>

Microsoft Internet Explorer
Are you sure you want to remove ?

4.5.2.3 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**

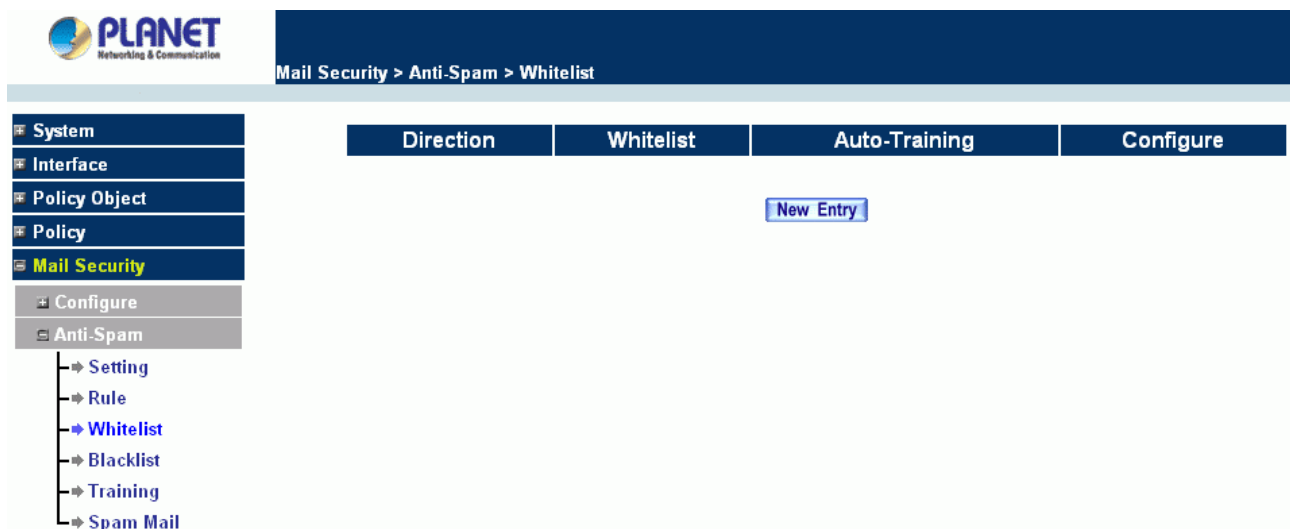
- **Whitelist:** Specify the key word or with wildcard for the Whitelist field..
- **Direction:**
 - From:** To judge the sending address of the mail.
 - To:** To judge the receiving address of the mail.
- **Auto-Training:** Select enable to allow Auto-Training system updating the CS-500's database.

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.

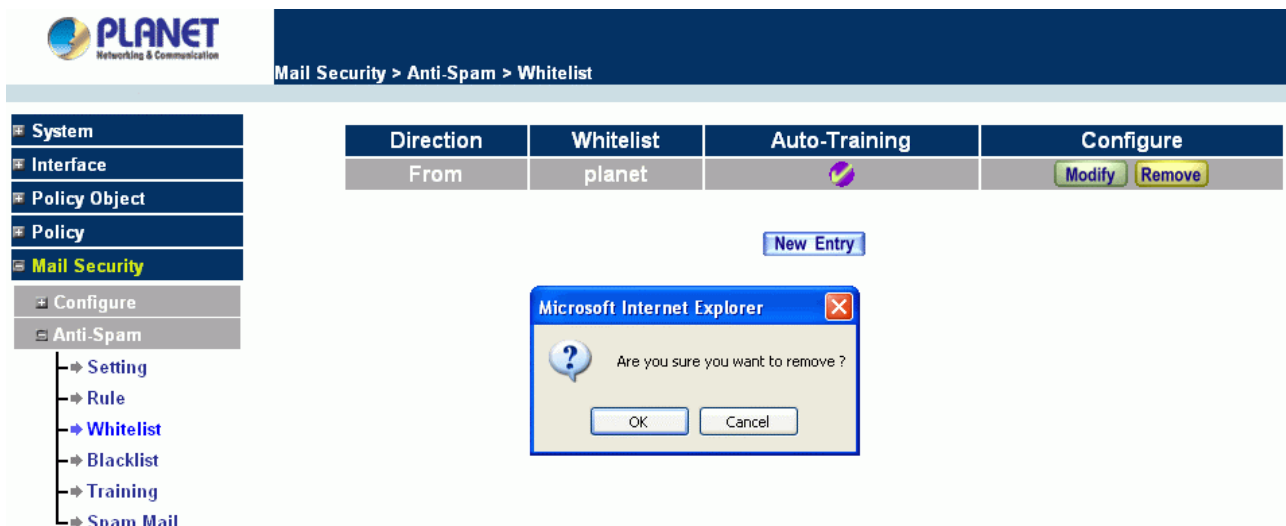
Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.



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**.



4.5.2.4 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-500'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.

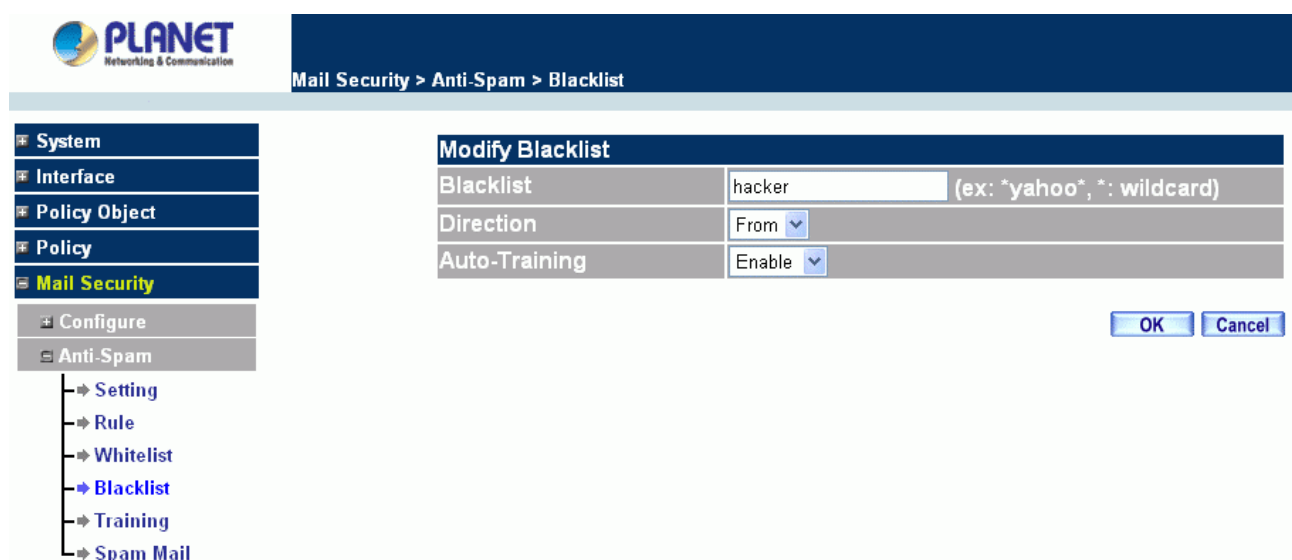


Modifying a Blacklist

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.

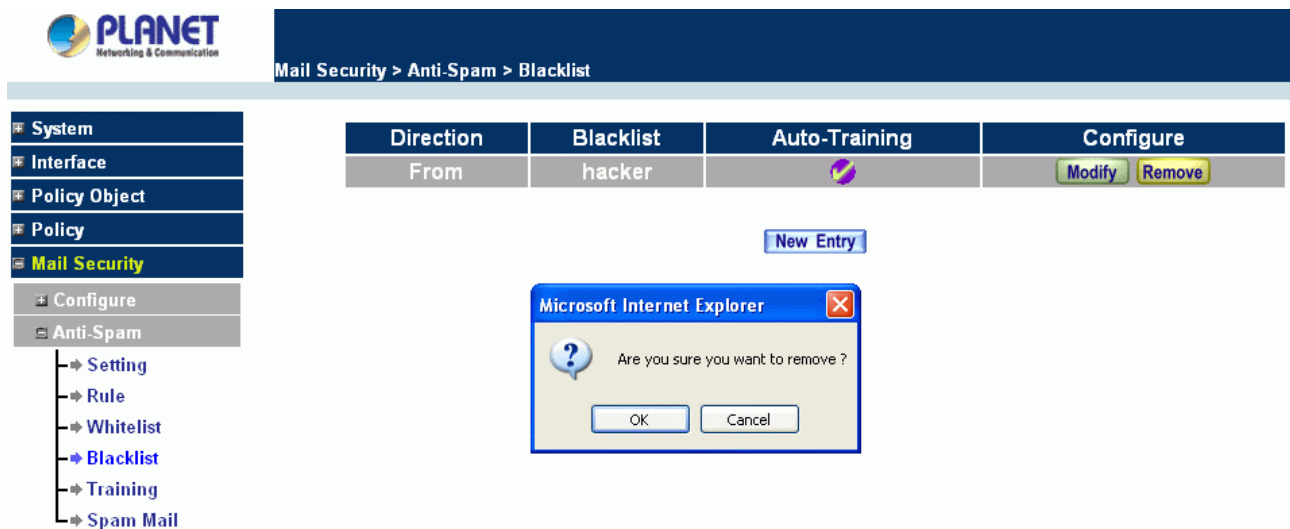
Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.



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**.



4.5.2.5 Training

CS-500 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-500 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-500 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-500 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-500 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-500 to learn the import file each day here.



Mail Security > Anti-Spam > Training

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Configure
- Anti-Spam
 - Setting
 - Rule
 - Whitelist
 - Blacklist
 - Training
 - Spam Mail
- Anti-Virus
- Anti-Attack
- Monitor

Training Database

Export Training Database Download

Import Training Database Browse...

Spam Mail for Training (Free space for training: 876 KBytes)

Import Spam Mail from Client Browse...

Ham Mail for Training (Free space for training: 876 KBytes)

Import Ham Mail from Client Browse...

Spam Account for Training (Free space for training: 876 KBytes)

POP3 Server (ex: my_domain.com)

User name (ex: spam)

Password (ex: 5d2#k...)

Account test Account Test

Ham Account for Training (Free space for training: 876 KBytes)

POP3 Server (ex: my_domain.com)

User name (ex: ham)

Password (ex: 5d2#k...)

Account test Account Test

Training time


System training starts at / day

Training immediately : Training NOW

OK
Cancel

4.5.2.6 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**.



Mail Security > Anti-Spam > Spam Mail

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Configure
- Anti-Spam
 - Setting
 - Rule
 - Whitelist
 - Blacklist
 - Training
 - Spam Mail

External

No.	Recipient	Total Spam	Total Mail	Duration	Spam %
No spam mail in the External Mail Server					

4.5.3 Anti-Virus

CS-500 built-in Clam virus scanning engine can protect your LAN network from being infected virus.

4.5.3.1 Setting

PLANET
Networking & Communication

Mail Security > Anti-Virus > Setting

Anti-Virus Setting

Virus Scan Engine

The Mail Server is placed in ☐ Internal (LAN or DMZ) (Please set Mail Relay first)
☒ External (WAN)

Add the message to the subject line (Max. 256 characters)

The latest update time : 2003/01/01 00:23:19 (Update virus definitions every ten minutes)
 The newest version : 0.0
 Update virus definitions immediately [Update NOW](#)

Action of Infected Mail

Internal Mail Server:

☐ Delete the virus mail
☐ Deliver to the recipient
☐ Deliver a notification mail instead of the original virus mail
☐ Deliver the original virus mail
☐ Forward to :

External Mail Server:

☒ Deliver to the recipient
☒ 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 to the virus mail, CS-500 will add a message in the mail's subject. You can configure the message you want, by default, it will be add "VIRUS" in the subject.

Update virus definitions immediately: Press **Update Now** to update CS-500 virus database.

Action of Infected Mail: When CS-500 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-500 will add a "VIRUS" message at the subject.

Forward to: You can configure CS-500 to forward virus mail to a specific mail account; it will be easily to manage the infected mail.

4.5.3.2 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.

The screenshot shows the PLANET Mail Security Anti-Virus Virus Mail interface. The sidebar menu includes System, Interface, Policy Object, Policy, Mail Security (expanded), Configure, Anti-Spam, Anti-Virus, Setting, and Virus Mail. The main area displays a table with the following headers: No., Recipient, Total Virus, Total Mail, Duration, and Virus %. A message states: "No virus mail in the External Mail Server!".

No.	Recipient	Total Virus	Total Mail	Duration	Virus %
No virus mail in the External Mail Server !					

4.6 Anti-Attack

CS-500 not only can filter virus from mail, it also can provide Anti-Attack function to prevent hacker intruding to your system. This chapter will introduce you how to configure the setting and check the alarm.

4.6.1 Alert Setting

The Administrator can configure the alert setting in here, it divides into **Internal Alert** and **External Alert**.

4.6.1.1 Internal Alert

The Administrator can enable the device's auto detect functions for blaster worm attacking the local network. When abnormal conditions occur, the Content Security Gateway will send an e-mail alert and/or SNMP trap and/or NetBIOS message to notify the Administrator, and also display warning messages in the **Internal Alarm** window.

PLANET
Networking & Communication

Anti-Attack > Alert Setting > Internal Alert

Blaster Alert Setting

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

☒ Enable Blaster Blocking Blocking Time seconds

☒ Enable E-Mail Alert Notification

☐ Enable NetBIOS Alert Notification IP Address of Administrator

Internal Alerts Settings

- n **The threshold sessions of infected Blaster (per Source IP) is ☐ Sessions /Sec:** You can set the threshold sessions for the IP who had infected Blaster worm. When the sessions exceed the threshold, CS-500 will block the connection.
- n **Enable Blaster Blocking:** Select this option to enable the blaster blocking function. Once the blaster worm is detected, it will block the TCP port 135 for user-dredefined blocking time.
- n **Enable E-mail Alert Notification:** When Blaster worm is detected, send alert e-mail to administrator by using e-mail address defined on System -> Configure -> Setting.
- n **Enalbe SNMP Trap Alert Notification:** When Blaster worm is detected, send SNMP trap to user-defined SNMP trap receiver IP address defined on System -> SNMP.
- n **Enable NetBIOS Alert Notification:** When Blaster worm is detected, send alert message to administrator by using "Net send" command.

After enabling the needed options, click OK to activate the changes.

4.6.1.2 External Alert

The Administrator can enable the device's auto detect functions for hacker attacking this section. When abnormal conditions occur, the Content Security Gateway will send an e-mail alert to notify the Administrator, and also display warning messages in the **External Alarm** window.



Anti-Attack > Alert Setting > External Alert

<ul style="list-style-type: none"> System Interface Policy Object Policy Mail Security Anti-Attack <ul style="list-style-type: none"> Alert Setting <ul style="list-style-type: none"> Internal Alert External Alert Attack Alarm Monitor 	DoS / SPI Setting <ul style="list-style-type: none"> <input type="checkbox"/> Sasser Block <input type="checkbox"/> Code Red Block <input type="checkbox"/> Detect SYN Attack <input type="checkbox"/> Detect ICMP Flood <input type="checkbox"/> Detect UDP Flood <input type="checkbox"/> Detect Ping of Death Attack <input type="checkbox"/> Detect IP Spoofing Attack <input type="checkbox"/> Detect Port Scan Attack <input type="checkbox"/> MSBlaster Block <input type="checkbox"/> Nimda Block SYN Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec SYN Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec SYN Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Seconds ICMP Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec ICMP Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec ICMP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Seconds UDP Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec UDP Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec UDP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Seconds <input type="checkbox"/> Detect Tear Drop Attack <input type="checkbox"/> Filter IP Route Option <input type="checkbox"/> Detect Land Attack
--	---

- n Some worms will attack your MS system in accordance with their weakness, such as **Sasser**, **Blaster**, **Code Red** and **Nimda**. Select the blocking function of CS-500 will prevent you to be attacking by these worms.
- n **Detect SYN Attack:** Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will prevent valid users from connecting to the servers. After enabling this function, the System Administrator can enter the number of SYN packets per second that is allowed to enter the network/Content Security Gateway. Once the SYN packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default SYN flood threshold is set to 200 Pkts/Sec
- n **Detect ICMP Flood:** Select this option to detect ICMP flood attacks. When hackers continuously send PING packets to all the machines of the LAN networks or to the Content Security Gateway, your network is experiencing an ICMP flood attack. This can cause traffic congestion on the network and slows the network down. After enabling this function, the System Administrator can enter the number of ICMP packets per second that is allowed to enter the network/Content Security Gateway. Once the ICMP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default ICMP flood threshold is set to 1000 Pkts/Sec.
- n **Detect UDP Flood:** Select this option to detect UDP flood attacks. A UDP flood attack is similar to an ICMP flood attack. After enabling this function, the System Administrator can enter the number of UDP packets per second that is allow to enter the network/Content

Security Gateway. Once the UDP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default UDP flood threshold is set to 1000 Pkts/Sec .

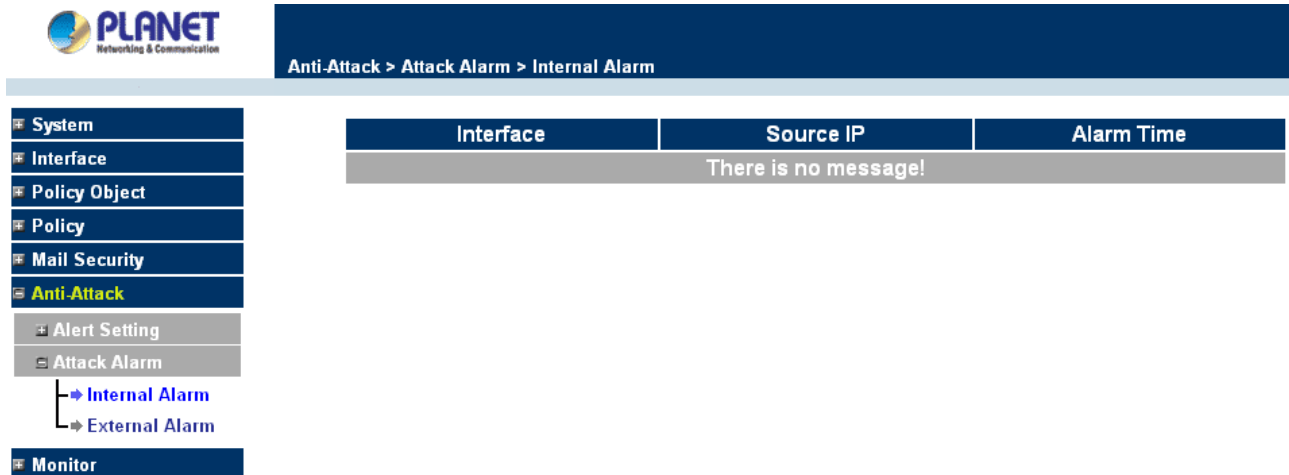
- n **Detect Ping of Death Attack:** Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction. This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.
- n **Detect Tear Drop Attack:** Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.
- n **Detect IP Spoofing Attack:** Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the Content Security Gateway System and invade the network.
- n **Filter IP Route Option:** Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade LAN networks and send LAN networks' data back to them.
- n **Detect Port Scan Attack:** Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.
- n **Detect Land Attack:** Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when SYN on the TCP header is marked.
Enable this function to detect such abnormal packets.

After enabling the needed detect functions, click OK to activate the changes.

4.6.2 Attack Alarm

4.6.2.1 Internal Alarm

- Step 1.** When the CS-500 had detected the internal PC sending large DDos attacks and then the Internal Alarm will start on blocking these packets to maintain the whole network.



Entering the Internal Alarm window

Step 1. Click the **Internal Alarm** option below the **Attack Alarm** of the **Anti-Attack** menu to enter the Internal Alarm window.

nInterface: Specify which interface received the attack packets.

nSource IP: Specify the IP address who is infected the virus and spreads the attack packets out.

nAlarm Time: Log time.

Downloading the Internal Alarm Logs

The Administrator can back up Internal alarm logs regularly by downloading it to a file on the computer.

Step 1. In the Internal Alarm window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the Internal alarm logs into specific directory on the hard drive.

Clearing Internal Alarm Logs

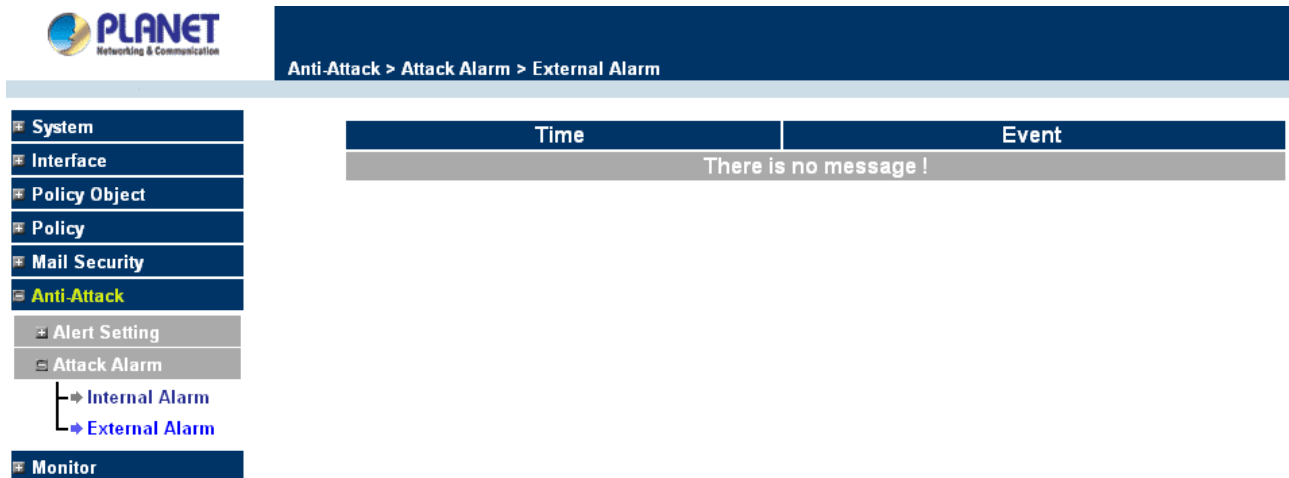
The Administrator may clear on-line logs to keep the most updated logs on the screen.

Step 1. In the Internal Alarm window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK**.

4.6.2.2 External Alarm

Step 2. When Content Security Gateway detects attacks from hackers, it writes attacking data in the external alarm file and sends an e-mail alert to the Administrator to take emergency steps.



Entering the External Alarm window

- Step 1.** Click the **External Alarm** option below the **Attack Alarm** of the **Anti-Attack** menu to enter the External Alarm window.

nTime: log time.

nEvent: event descriptions.

Downloading the External Alarm Logs

The Administrator can back up External alarm logs regularly by downloading it to a file on the computer.

- Step 3.** In the External Alarm window, click the **Download Logs** button at the bottom of the screen.

- Step 4.** Follow the File Download pop-up box to save the External alarm logs into specific directory on the hard drive.

Clearing External Alarm Logs

The Administrator may clear on-line logs to keep the most updated logs on the screen.

- Step 3.** In the External Alarm window, click the Clear Logs button at the bottom of the screen.

- Step 4.** In the Clear Logs pop-up box, click **OK**.

4.7 Monitor

CS-500 provides varied of information that can be used to check the status.

4.7.1 Log

The Content 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 Content Security Gateway.

What is Log?

Log records all connections that pass through the Content 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.

4.7.1.1 Traffic

The Administrator queries the Content Security Gateway for information, such as source address, destination address, start time, and Protocol port of all connections.

Entering the Traffic Log window

Step 3. Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.

Monitor > Log > Traffic

Jan 1 03:01:46 [Next](#)

Time	Source	Destination	Protocol	Port	Disposition
Jan 1 03:01:46	192.168.1.11	192.168.1.1	TCP	1190 => 80	
Jan 1 03:01:46	192.168.1.11	192.168.1.1	TCP	1189 => 80	
Jan 1 02:59:55	192.168.1.11	192.168.1.1	TCP	1188 => 80	
Jan 1 02:59:54	192.168.1.11	192.168.1.1	TCP	1187 => 80	
Jan 1 02:58:10	192.168.1.11	192.168.1.1	TCP	1185 => 80	
Jan 1 02:58:10	192.168.1.11	192.168.1.1	TCP	1184 => 80	
Jan 1 02:51:52	192.168.1.11	192.168.1.1	TCP	1179 => 80	
Jan 1 02:51:52	192.168.1.11	192.168.1.1	TCP	1178 => 80	
Jan 1 02:48:35	192.168.1.11	192.168.1.1	TCP	1177 => 80	
Jan 1 02:48:35	192.168.1.11	192.168.1.1	TCP	1176 => 80	
Jan 1 02:46:03	192.168.1.11	192.168.1.1	TCP	1170 => 80	
Jan 1 02:46:03	192.168.1.11	192.168.1.1	TCP	1169 => 80	
Jan 1 02:32:37	192.168.1.11	192.168.1.1	TCP	1163 => 80	
Jan 1 02:32:37	192.168.1.11	192.168.1.1	TCP	1162 => 80	
Jan 1 02:19:20	192.168.1.11	192.168.1.1	TCP	1152 => 80	
Jan 1 02:19:20	192.168.1.11	192.168.1.1	TCP	1151 => 80	
Jan 1 02:04:11	192.168.1.11	192.168.1.1	TCP	1142 => 80	
Jan 1 02:04:11	192.168.1.11	192.168.1.1	TCP	1141 => 80	

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

- n **Time:** The start time of the connection.
- n **Source:** IP address of the source network of the specific connection.
- n **Destination:** IP address of the destination network of the specific connection.
- n **Protocol:** Protocol type of the specific connection.
- n **Port:** Port number of the specific connection.
- n **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.

PLANET
Networking & Communication

Monitor > Log > Traffic

Time	Source	Destination	Protocol	Port	Disposition
Jan 1 03:01:46	192.168.1.11	192.168.1.1	TCP	1190 => 80	
Jan 1 03:01:46	192.168.1.11	192.168.1.1	TCP	1189 => 80	
Jan 1 02:59:55	192.168.1.11	192.168.1.1	TCP	1188 => 80	
Jan 1 02:59:54	192.168.1.11	192.168.1.1	TCP	1187 => 80	
Jan 1 02:58:10	192.168.1.11	192.168.1.1	TCP	1185 => 80	
Jan 1 02:58:10	192.168.1.11	192.168.1.1	TCP	1184 => 80	
Jan 1 02:51:52	192.168.1.11	192.168.1.1	TCP	1179 => 80	
Jan 1 02:51:52	192.168.1.11	192.168.1.1	TCP	1178 => 80	
Jan 1 02:48:35	192.168.1.11	192.168.1.1	TCP	1177 => 80	
Jan 1 02:48:35	192.168.1.11	192.168.1.1	TCP	1176 => 80	
Jan 1 02:46:03	192.168.1.11	192.168.1.1	TCP	1170 => 80	
Jan 1 02:46:03	192.168.1.11	192.168.1.1	TCP	1169 => 80	
Jan 1 02:32:37	192.168.1.11	192.168.1.1	TCP	1163 => 80	
Jan 1 02:32:37	192.168.1.11	192.168.1.1	TCP	1162 => 80	
Jan 1 02:19:20	192.168.1.11	192.168.1.1	TCP	1152 => 80	
Jan 1 02:19:20	192.168.1.11	192.168.1.1	TCP	1151 => 80	
Jan 1 02:04:11	192.168.1.11	192.168.1.1	TCP	1142 => 80	
Jan 1 02:04:11	192.168.1.11	192.168.1.1	TCP	1141 => 80	

Clear Logs Download Logs

4.7.1.2 Event

When the Content 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.

Planet Network & Communication

Monitor > Log > Event

Jan 1 01:14:30

Time	Event
Jan 1 01:14:30	admin Delete [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.11
Jan 1 01:05:40	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.11
Jan 1 01:05:29	admin Delete [Policy](External to DMZ,Outside_Any=>DMZ_Any,ANY,permit) from 192.168.1.11
Jan 1 00:48:12	admin Add [Policy](External to DMZ,Outside_Any=>DMZ_Any,ANY,permit) from 192.168.1.11
Jan 1 00:48:05	admin Delete [Policy](Incoming,Outside_Any=>Inside_Any (Routing),ANY,permit) from 192.168.1.11
Jan 1 00:44:35	admin Add [Policy](Incoming,Outside_Any=>Inside_Any (Routing),ANY,permit) from 192.168.1.11
Jan 1 00:07:18	user admin [Login success] from 192.168.1.11

Clear Logs Download Logs

Step 2. The table in the Event Log window displays the time and description of the events.

- n **Time:** time when the event occurred.
- n **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.

 **Monitor > Log > Event**

Jan 1 01:14:30

Time	Event
Jan 1 01:14:30	admin Delete [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.11
Jan 1 01:05:40	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.11
Jan 1 01:05:29	admin Add [Policy](DMZ to DMZ,Outside_Any=>DMZ_Any,ANY,permit) from 192.168.1.11
Jan 1 00:48:12	admin Add [Policy](DMZ to DMZ,Outside_Any=>DMZ_Any,ANY,permit) from 192.168.1.11
Jan 1 00:48:05	admin Add [Policy](Incoming,Outside_Any=>Inside_Any (Routing),ANY,permit) from 192.168.1.11
Jan 1 00:44:35	admin Add [Policy](Incoming,Outside_Any=>Inside_Any (Routing),ANY,permit) from 192.168.1.11
Jan 1 00:07:18	user admin [Login success] from 192.168.1.11

Clear Logs Download Logs

4.7.1.3 Connection

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.

 **Monitor > Log > Connection**

Jan 1 00:02:46 [Next](#)

Time	Connection Log
Jan 1 00:02:46	including NAT-Traversal patch (Version 0.6)
Jan 1 00:02:53	added connection description "VPN_A"
Jan 1 00:02:53	listening for IKE messages
Jan 1 00:02:53	adding interface ipsec0/br0:wan1 192.168.99.95
Jan 1 00:02:53	adding interface ipsec0/br0:wan1 192.168.99.95:4500
Jan 1 00:03:06	"VPN_A": deleting connection
Jan 1 00:03:16	added connection description "VPN_A"
Jan 1 00:03:17	truncated message from whack: got 0 bytes; expected 2532. Message ignored.
Jan 1 00:03:31	socket
Jan 1 00:03:31	Connect 61.20.30.40 now...
Jan 1 00:03:46	Connect timeout..Exit()
Jan 1 00:03:53	socket
Jan 1 00:03:53	Connect 61.20.30.40 now...
Jan 1 00:04:08	Connect timeout..Exit()
Jan 1 00:04:28	socket
Jan 1 00:04:28	Connect 61.20.30.40 now...
Jan 1 00:04:43	Connect timeout..Exit()
Jan 1 00:05:04	socket

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.

PLANET Network & Communication

Monitor > Log > Connection

Time	Connection Log
Jan 1 00:02:46	including NAT-Traversal patch (Version 0.6)
Jan 1 00:02:53	added connection description "VPN_A"
Jan 1 00:02:53	listening for IKE messages
Jan 1 00:02:53	adding interface ipsec0/br0:wan1 192.168.99.95
Jan 1 00:02:53	adding interface ipsec0/br0:wan1 192.168.99.95:4500
Jan 1 00:03:06	"VPN_A": deleting connection
Jan 1 00:03:16	ad Microsoft Internet Explorer "VPN_A"
Jan 1 00:03:17	tr Do you really want to clean ? got 0 bytes; expected 2532. Message
Jan 1 00:03:31	so
Jan 1 00:03:31	Co
Jan 1 00:03:46	Connect timeout..Exit()
Jan 1 00:03:53	socket
Jan 1 00:03:53	Connect 61.20.30.40 now...
Jan 1 00:04:08	Connect timeout..Exit()
Jan 1 00:04:28	socket
Jan 1 00:04:28	Connect 61.20.30.40 now...
Jan 1 00:04:43	Connect timeout..Exit()
Jan 1 00:05:04	socket

Clear Logs Download Logs

4.7.1.4 Log Backup

Click **Log à Log Backup**.

The screenshot shows the PLANET Network & Communication web interface. The breadcrumb trail is "Monitor > Log > Log Backup". The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Mail Security, Anti-Attack, Monitor (highlighted), Log (expanded), Alarm, Statistics, and Status. Under the "Log" item, there are sub-items: Traffic, Event, Connection, and Log Backup (highlighted with a red arrow). The main content area is divided into two sections: "Log Mail Configuration" and "Syslog Setting".

Log Mail Configuration

- ☐ Enable Log Mail Support
 - When Log Full (300Kbytes), Mail 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)

At the bottom right of the Syslog Setting section, there are two buttons: "OK" and "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.

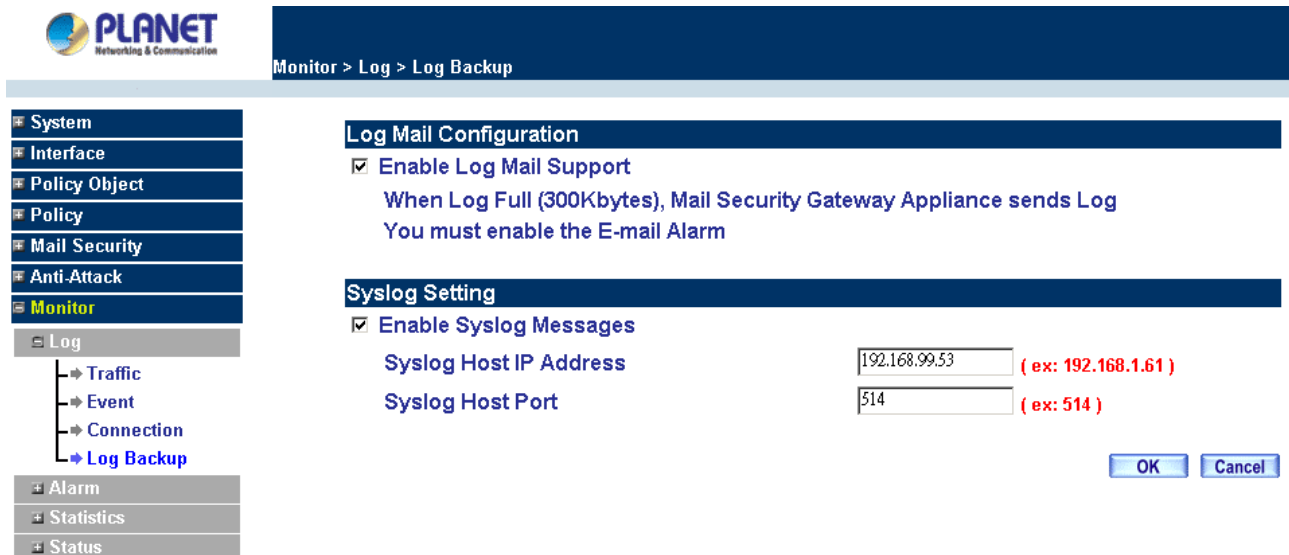
Enable Log Mail Support & Syslog Message

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 à Log Backup**. Check to enable **Log Mail Support**. Click **OK**.

System Settings/Enable Syslog Message

- Step 1.** Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.
- Step 2.** Click **OK**.



The screenshot shows the PLANET web interface. The top navigation bar includes 'Monitor > Log > Log Backup'. On the left, a sidebar menu lists 'System', 'Interface', 'Policy Object', 'Policy', 'Mail Security', 'Anti-Attack', 'Monitor' (highlighted), 'Log' (expanded), 'Alarm', 'Statistics', and 'Status'. Under 'Log', sub-items are 'Traffic', 'Event', 'Connection', and 'Log Backup' (selected). The main content area has two sections: 'Log Mail Configuration' and 'Syslog Setting'. In 'Log Mail Configuration', 'Enable Log Mail Support' is checked, with a note: 'When Log Full (300Kbytes), Mail Security Gateway Appliance sends Log. You must enable the E-mail Alarm'. In 'Syslog Setting', 'Enable Syslog Messages' is checked. Below this, 'Syslog Host IP Address' is set to '192.168.99.53' (example: 192.168.1.61) and 'Syslog Host Port' is set to '514' (example: 514). 'OK' and 'Cancel' buttons are at the bottom right.

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG à Log Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG à Log Backup**. Uncheck to disable Settings Message. Click **OK**.

4.7.2 Alarm

In this chapter, the Administrator can view traffic alarms that occur and the Content Security Gateway has logged.

Traffic alarm:

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

How to apply Traffic Alarm

The administrator can use Traffic Alarm to track the Source Address, Destination Address, network service and the status of network. The administrator can save Traffic Logs and Event Logs for a pre-determined time and then delete them to keep the newest log.

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Entering the Traffic Alarm window

Step 1. Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.



Monitor > Alarm > Traffic

System	Time	Source	Destination	Service	Traffic
Interface	There is no message !				
Policy Object					
Policy					
Mail Security					
Anti-Attack					
Monitor					
Log					
Alarm					
L Traffic					
Statistics					
Status					

Step 2. The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- n **Time:** The start and stop time of the specific connection.
- n **Source:** Name of the source network of the specific connection.
- n **Destination:** Name of the destination network of the specific connection.
- n **Service:** Service of the specific connection.
- n **Traffic:** Traffic (in Kbytes/Sec) of the specific connection.

Downloading the Traffic Alarm Logs

The Administrator can back up traffic alarm logs regularly and download it to a file on the computer.

Step 1. In the Traffic Alarm window, click the **Download Logs** button on the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.

Clearing the Traffic Alarm Logs

Step 1. In the Traffic Alarm 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.

4.7.3 Statistic

In this chapter, the Administrator queries the Content Security Gateway for statistics of packets and data which passes across the Content 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 Content 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

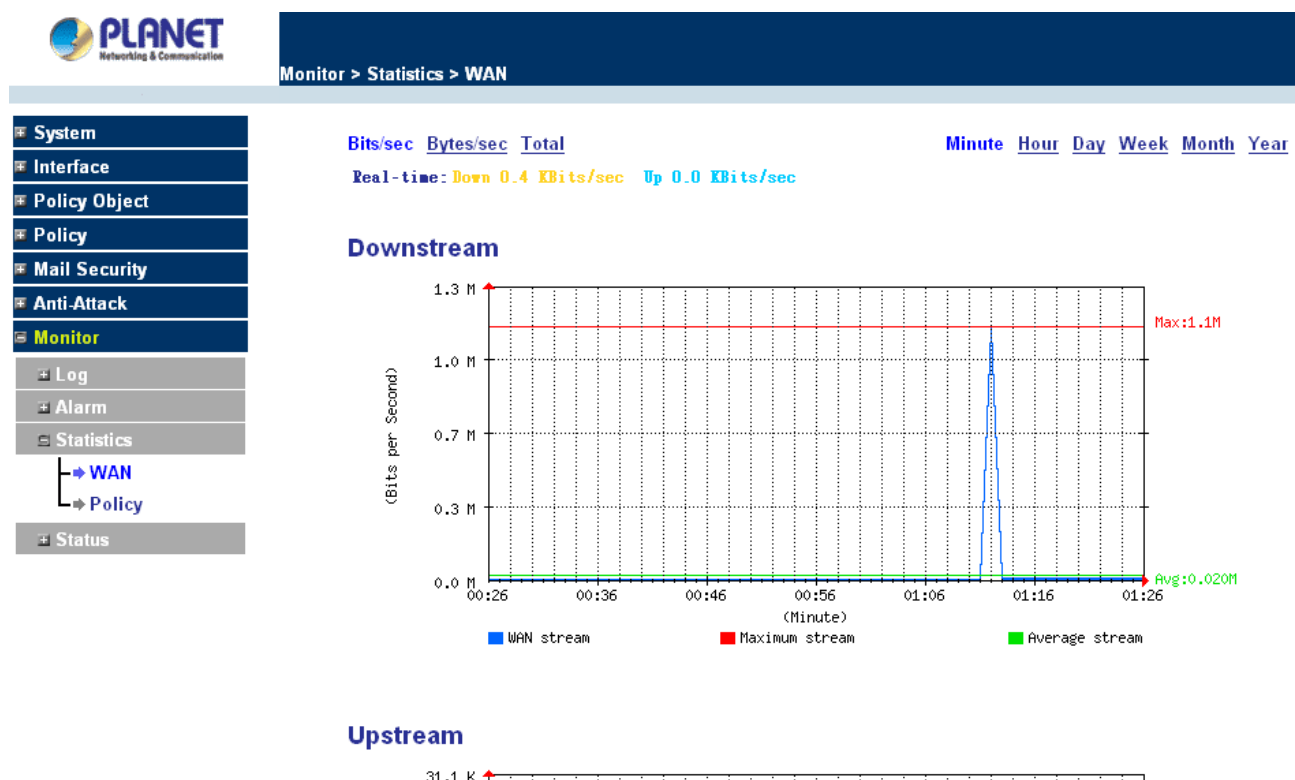
The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics. In this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

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.

4.7.3.1 WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN Statistics.

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 (Hour/Minute/Day) .

4.7.3.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

- n **Source:** the name of source address.
- n **Destination:** the name of destination address.
- n **Service:** the service requested.
- n **Action:** permit or deny
- n **Time:** viewable by minutes, hours, or days

PLANET Network & Communication

Monitor > Statistics > Policy

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

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 (Hour/Minute/Day).



Monitor > Statistics > Policy

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor
 - Log
 - Alarm
 - Statistics
 - WAN
 - Policy
- Status

Bits/sec Bytes/sec Total

Inside_Any to Outside_Any

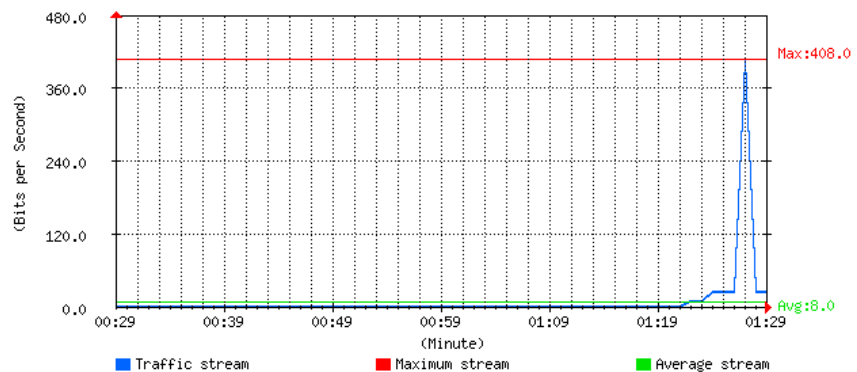
Service : ANY

Action : PERMIT

Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec

Minute Hour Day Week Month Year

Downstream



4.7.4 Status

In this section, the device displays the status information about the Content 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 Content Security Gateway.

4.7.4.1 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 Interface**, and the **DMZ Interface**.



Monitor > Status > Interface

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor**
 - Log
 - Alarm
 - Statistics
 - Status
 - Interface
 - ARP Table
 - DHCP Clients

Active Sessions Number : 9

 System Uptime
 0 Day 1 Hour 26 Min 30 Sec

	LAN	WAN	DMZ
Forwarding Mode	NAT	Static IP	Transparent
Connect Time	---	---	---
MAC Address	00:e0:98:11:11:11	00:e0:98:11:11:12	00:e0:98:11:11:13
IP Address	192.168.1.1	192.168.99.95	0.0.0.0
Netmask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	---	192.168.99.253	---
DNS1	---	168.95.1.1	---
DNS2	---	168.95.192.1	---
Rx Pkts, Error Pkts	4199, 0	13730, 0	13721, 0
Tx Pkts, Error Pkts	6923, 0	5873, 0	6049, 0
Ping			
HTTP			

4.7.4.2 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.



Monitor > Status > ARP Table

- System
- Interface
- Policy Object
- Policy
- Mail Security
- Anti-Attack
- Monitor**
 - Log
 - Alarm
 - Statistics
 - Status
 - Interface
 - ARP Table**
 - DHCP Clients

IP Address	MAC Address	Interface
192.168.1.2	00:0E:A6:0F:8B:92	LAN
192.168.99.253	00:03:79:01:0C:FF	WAN
192.168.99.222	00:50:8B:AD:E6:CD	WAN
192.168.99.250	00:C0:CA:10:A4:FD	WAN

IP Address: The IP address of the host computer

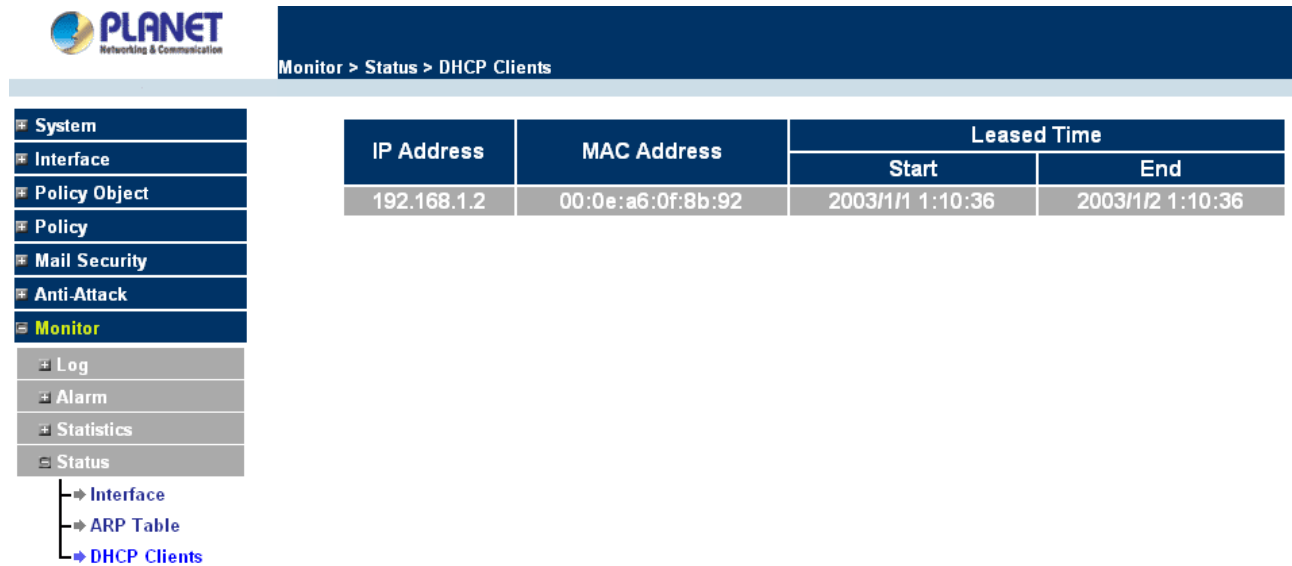
MAC Address: The MAC address of that host computer

Interface: The port that the host computer is connected to (LAN, WAN, DMZ)

4.7.4.3 DHCP Clients

Entering the DHCP Clients window

Click on **Status** in the menu bar, then 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 Content Security Gateway's DHCP server function.



IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.2	00:0e:a6:0f:8b:92	2003/1/1 1:10:36	2003/1/2 1:10:36

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.