

Content Security Gateway CS-500

User's Manual

Download from Www.Somanuals.com. All Manuals Search And Download.

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: 3.0 (May, 2006)

Part No. EM-CS500v3

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 Features	
1.2 PACKAGE CONTENTS	2
1.3 CONTENT SECURITY GATEWAY FRONT VIEW	2
1.4 Content Security Gateway Rear Panel	2
1.5 SPECIFICATION	
CHAPTER 2: HARDWARE INSTALLATION	5
2.1 INSTALLATION REQUIREMENTS	5
2.2 OPERATION MODE	
2.2.1 Transparent Mode Connection Example	
2.2.2 NAT Mode Connecting Example	
CHAPTER 3: GETTING STARTED	7
3.1 Web Configuration	7
3.2 CONFIGURE WAN INTERFACE	
3.3 CONFIGURE DMZ INTERFACE	9
3.4 Configure Policy	9
CHAPTER 4: WEB CONFIGURATION	11
4.1 System	
4.1.1 Admin	
4.1.2 Permitted IPs	
4.1.3 Software Update	
4.1.4 Setting	
4.1.5 Date/Time	
4.1.6 Multiple Subnet	
4.1.7 Route Table	
4.1.8 DHCP	
4.1.9 Dynamic DNS	
4.1.10 Host Table	
4.1.11 Language	
4.1.12 Logout	
4.2 INTERFACE	
4.2.1 LAN	
4.2.2 WAN	
4.2.3 DMZ	

4.3 POLICY OBJECT	
4.3.1 Address	
4.3.1.1 LAN	
4.3.1.2 LAN Group	
4.3.1.3 WAN	
4.3.1.4 WAN Group	
4.3.1.5 DMZ	
4.3.1.6 DMZ Group	
4.3.2 Service	
4.3.2.1 Pre-defined	
4.3.2.2 Custom	
4.3.2.3 Group	
4.3.3 Schedule	
4.3.4 QoS	
4.3.5 Authentication	
4.3.5.1 Auth Setting	
4.3.5.2 Auth User	
4.3.5.3 Auth Group	
4.3.5.4 Radius Serve	
4.3.5.5 POP3	
4.3.6 Content Blocking	
4.3.6.1 URL Blocking	
4.3.6.2 Scripts	
4.3.6.3 P2P	
4.3.6.4 IM	
4.3.6.5 Download	
4.3.6.6 Upload	
4.3.7 Virtual Server	
4.3.7.1 Mapped IP	
4.3.7.2 Virtual Server	
4.3.8 VPN	
4.3.8.1 IPSec Autokey	
4.3.8.2 PPTP Server	
4.3.8.3 PPTP Client	
4.3.8.4 Tunnel	
4.4 Policy	
4.4.1 Outgoing	
4.4.2 Incoming	
4.4.3 WAN To DMZ & LAN To DMZ	

4.4.4 DMZ To WAN & DMZ To LAN	
4.5 MAIL SECURITY	
4.5.1 Configure	
4.5.2 Anti-Spam	
4.5.2.1 Setting	
4.5.2.2 Rule	
4.5.2.3 Whitelist	
4.5.2.4 Blacklist	
4.5.2.5 Training	
4.5.2.6 Spam Mail	
4.5.3 Anti-Virus	
4.5.3.1 Setting	
4.5.3.2 Virus Mail	
4.6 IDP	
4.6.1 Setting	
4.6.2 Signature	
4.6.3 IDP Report	
4.7 ANOMALY FLOW IP	
4.8 MONITOR	
4.8.1 Log	
4.8.1.1 Traffic	
4.8.1.2 Event	
4.8.1.3 Connection	
4.8.1.4 Log Backup	
4.8.2 Accounting Report	
4.8.2.1 Setting	
4.8.2.2 Outbound	
4.8.2.3 Inbound	
4.8.3 Statistic	
4.8.3.1 WAN Statistics	
4.8.3.2 Policy Statistics	
4.8.4 Status	
4.8.4.1 Interface Status	
4.8.4.2 Authentication	
4.8.4.3 ARP Table	
4.8.4.4 DHCP Clients	

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 concerned for the enterprise. Planet's Content Security Gateway CS-500, a special designed of 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 IDP and firewall function can defense hacker and blaster attack from Internet. Moreover, built-in QoS feature can let you configure the traffic per specific protocol more flexibly. The completely function in one device can offers an excellent security solution and the secure environment for the SMB or SOHO users.

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, WinMX and Foxy), Instant Messaging (MSN, Yahoo Messenger, ICQ, QQ and Skype), Download and Upload.
- IDP: CS-500 provides three kinds of the Signature to complete the intrusion detection system, user can select to configure "Anomaly", "Pre-defined" and "Custom" according to the current environment's request.
- **QoS:** You can control the outbound and inbound Upstream/downstream Bandwidth by configuring the QoS based on the WAN bandwidth.
- User Authentication: Web-based authentication allows users to be authenticated by web browser. User database can be configured on the devices or through external RADIUS server.
- 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

- Content Security Gateway
- User's Manual CD-ROM
- This Quick Installation Guide
- 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

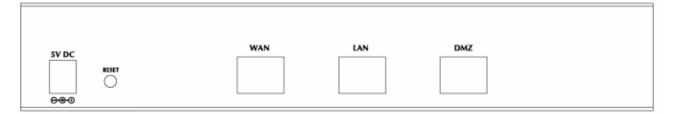
CS-500 Front Panel

					C	Content S	Security Gateway
CS-500	● LNK ☆ ACT) Dmz) LAN) WAN) STATUS) PWR	

LED	Description
PWR	Power is supplied to this device.
STATUS	Blinks to indicate this devise is being turned on and booting. After one minute, this LED indicator will stop blinking, it means this device is now ready to use.
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	1	POWER, STATUS, 10/100 and LNK/ACT for each LAN and WAN port			
Power		5VDC, 2.4A			
Operating En	vironment	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 Con	nection	Transparent mode (WAN to DMZ), NAT, Multi-NAT			
Routing Mode	е	Static Route, RIPv2			
Concurrent S	essions	110,000			
New session	/ second	8,000			
Email Capaci	ty per Day	90,000			
Firewall Thro	ughout	100Mbps			
3DES Throug	ghput	15Mbps			
Firewall		Policy-based firewall rule with schedule, NAT/NAPT, SPI firewall			
VPN Tunnels		200			
VPN Functior	า	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 Filter	ring	URL, P2P application, Instant Message, download & upload blocking			
		Popup, Java Applet, cookies and Active X blocking			
Anomaly Flow	v IP	Hacker Alert:			
		Sasser, Code Red, Syn Flood, ICMP Flood, UDP Flood, Blaster Alert			
Scanning Ma	il 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			
Anti Chan		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 specif			
		account			
		uoovunt			

חחו	Anomaly Over Flood, UDD Flood, JOND Flood, and more
IDP	Anomaly: Syn Flood, UDP Flood, ICMP Flood and more.
	Pre-defined : Backdoor, DDoS, DoS, Exploit, NetBIOS and Spyware.
	Custom: User defined based on TCP, UDP, ICMP or IP protocol.
QoS	Policy rules with Inbound/Outbound traffic management
	Guaranteed and maximum bandwidth
	Scheduled in unit of 30 minutes
	3 Priorities
User Authentication	Built-in user database with up to 500 entries
	Support local database, RADIUS and POP3 authentication
Logs	Log and alarm for event and traffic
	Log can be saved from web, sent by e-mail or 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.

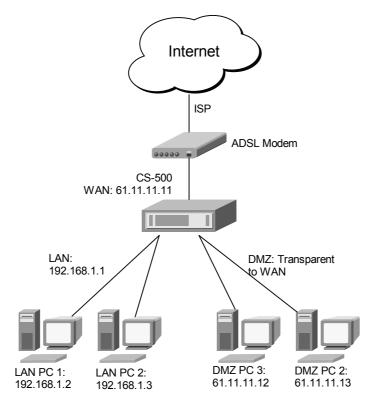
- Network Requirements

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

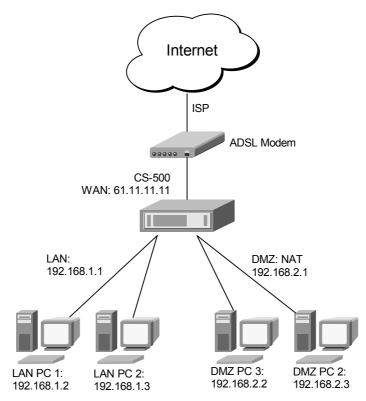
CS-500 DMZ port supports three operation modes, Disable, NAT and Transparent. In Disable mode, the DMZ port is not active. In transparent mode, CS-500 works as proxy with forward DMZ packet to WAN and forward WAN packet to DMZ, the DMZ and WAN side IP addresses are in the same subnet. In NAT mode, DMZ 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 then 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 <u>http://192.168.1.1</u> 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 19	2.168.1.1 🛛 🛛 🔀
R	G
Bandwidth Admin	istration Tools
User name:	🖸 admin 🕑
Password:	•••••
	Remember my password
	OK Cancel
	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.

	Interface > WAN		
 System Interface ↓ LAN ↓ WAN ↓ DMZ Policy Object Policy Mail Security IDP Anomaly Flow IP Monitor 	WAN Interface PPPoE (ADSL User) Dynamic IP Address (Cable Model) Static IP Address PPTP (European User Only) IP Address Netmask Default Gateway DNS Server 1 DNS Server 2 Max. Downstream Bandwidth Max. Upstream Bandwidth Enable	em User) 192.168.99.97 255.255.255.0 192.168.99.253 168.95.1.1 30000 Kbps (Max. 30 Mbps) 30000 Kbps (Max. 30 Mbps) W Ping	
			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.

<u>Ping</u>: 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.

PLANET Retworking & Communication	Interface ≻ DMZ			
≡ System				
■ Interface	DMZ Interface	Disable 🔽		
-⇒ LAN	IP Address	Disable I.O.O		
_♦ WAN	Netmask	DMZ_TRANSPARENT 0.0		
L⇒ DMZ				
🎟 Policy Object	Enable	Ping	HTTP	
🖬 Policy				
🎟 Mail Security				OK Cancel
IDP 🗉				
🗉 Anomaly Flow IP				
🗉 Monitor				

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" Click on OK to apply the changes.

Polic	y ≻ Outgoing	
■ System ■ Interface	Comment :	
Policy Object	Modify Policy	
Policy	Source Address	Inside_Any 🔽
- ⇒ Outgoing	Destination Address	Outside_Any 🔽
_→ Incoming	Service	ANY
-⇒ WAN To DMZ	Schedule	None 🗸
-⇒ LAN To DMZ	Authentication User	None V
-⇒ DMZ To WAN -⇒ DMZ To LAN	Tunnel	None V
Mail Security	Action	PERMIT V
IDP	Traffic Log	Enable
Anomaly Flow IP	Statistics	Enable
Monitor	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (0:means unlimited)
	QoS	None V

OK Cancel

STEP 4:

The configuration is successful when the screen below is displayed.

PLANET Retworking & Communication	Policy > Outgoir	ng					
≖ System							
■ Interface	Source	Destination	Service	Action	Option	Configure	Move
🖬 Policy Object	Inside_Any	Outside_Any		6		Modify Remove Pause	то 1 💌
写 Policy							
→ Outgoing					New Entry		
_⇒ Incoming							

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, Configure and Logout.

Administration:

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

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

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 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.

Logout:

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

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.

PLANET Retworking & Communication Syste	em > Administration > Admin		
⊟ System I⊐ Administration	Admin Name	Privilege	Configure
Admin ← ←	admin	ReadMirite	Modify
–♦ Permitted IPs			
L		New Sub Admin	
■ Configure			
🗉 Logout			
🗉 Interface			

Settings of the Administration table

<u>Admin Name</u>: 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 Admin with read / write privilege.

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

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

Changing the Main/Sub-Admin's Password

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

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

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

	System > Administration > Admin		
■ System	Modify Admin Password		
⊒ Administration	Admin Name	admin	
–♦ Admin	Admin Name	admin	
→ Permitted IPs	Password	•••••	
▲● Software Update	New Password	•••••	
■ Configure	Confirm Password		
■ Logout			
🗷 Interface			OK Cancel
🗷 Policy Object			

Adding a new Sub Admin

Step 1. In the Add New Sub Admin window:

- **Sub Admin Name:** enter the username of new **Sub Admin.**
- Password: enter a password for the new Sub Admin.
- Confirm Password: enter the password again.
- Step 2. Click OK to add the user or click Cancel to cancel the addition.

PLANET Networking & Communication	System > Administration > Admin		
■ System	Add New Sub Admin		
■ Administration			
_⇒ Admin	Sub Admin name	planet	
→ Permitted IPs	Password	•••••	
L⇒ Software Update	Confirm Password		
■ Configure			
🗉 Logout			OK Cancel
📧 Interface			

Removing a Sub Admin

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

	System > Administration >	Admin		
⊑ System		Admin Name	Privilege	Configure
In Administration In Administration		admin	ReadMvrite	Modify
→ Permitted IPs			Read	Modify Remove
L⇒ Software Update				
■ Configure			New Sub Admin	
I Logout		Microsoft Interr	et Explorer 🛛 🔀	
🗉 Interface		MICTOSOTT IIITETT		
🗉 Policy Object		Are you	sure you want to remove ?	
Policy		~	,	
🎟 Mail Security		ОК	Cancel	
IDP				
📧 Anomaly Flow IP				

4.1.2 Permitted IPs

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

	System > Administration > Permitte	ed IPs			
System Administration Admin Permitted IPs Software Update Configure	Name	IP Address / Netmask New Ent	Ping	HTTP	Configure

Add Permitted IPs Address

Step 1. Click New Entry button.

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

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

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

	System > Administration > Permitted IPs	
l≡ System I≣ Administration	Add New Permitted IPs	
L → Admin	Name	planet
→ Permitted IPs	IP Address	192.168.1.10
L	Netmask	255.255.255.255
 ■ Configure ■ Logout 	Service	Ping HTTP
■ Interface ■ Policy Object		OK Cancel

Modify Permitted IPs Address

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

- Step 2. In Modify Permitted IPs, enter new IP address.
- Step 3. Click OK to modify or click Cancel to discard changes.

	System > Administration > Permitted IPs		
■ System ■ Administration	Modify Permitted IPs		
 L⇒ Admin	Name	planet	
→ Permitted IPs	IP Address	192.168.1.10	
L⇒ Software Update	Netmask	255.255.255.255	
I Configure	Service	Ping HTTP	
I Logout ≇ Interface ≢ Policy Object		ОК	Cancel

Remove Permitted IPs Addresses

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

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

PLANET Retworking & Communication	System > Administration :	> Permitted IPs			
System	Name	IP Address / Netmask	Ping	НТТР	Configure
Administration	planet	192.168.1.10 / 255.255.255.255	6	V	Modify Remove
Permitted IPs Software Update Configure		New	Entry		
Logout nterface		Microsoft Internet Explorer			
Policy Object		Are you sure you want to rea	nove ?		
olicy Iail Security DP		OK Cancel			
Anomaly Flow IP Monitor					

4.1.3 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.

	System > Administration > Software Update		
l≡ System	Software Update		
 Administration Admin ⇒ Permitted IPs ⇒ Software Update ←← 	Version Number : Software Update	v 2.12 Browse (ex: CS-500_021200.ing)	
 ■ Configure ■ Logout 			OK Cancel

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

4.1.4 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 Configure menu to enter the Settings window. The Setting will be shown on the screen.

	tem > Configure > Setting	
 ■ System ■ Administration ■ Configure ➡ Setting ← ← 	Backup / Restore Configuration Export System Setting to Client Download Import System Setting from Client	Browse
– ➡ Date/Time – ➡ Multiple Subnet – ➡ Route Table	Reset Factory Setting	(ex: CSsystem.conf)
→ DHCP → Dynamic DNS	System Name Setting Device Name	Content Security Gat (ex: Content Security Gateway)
 → Host Table → Language ✓ Logout ✓ Interface ✓ Policy Object ✓ Policy ✓ Mail Security ✓ IDP ✓ Anomaly Flow IP 	E-mail Setting Enable E-mail Alert Notification Sender Address (Required by some ISPs) SMTP Server E-mail Address 1 E-mail Address 2 Mail Test	(ex: sender@mydomain.com) (ex: mail.mydomain.com) (ex: user1@mydomain.com) (ex: user2@mydomain.com)
Monitor	Web Management (WAN Interface)	80
	HTTP Port MTU Setting MTU	au 1500 Bytes
	Link Speed / Duplex Mode Setting WAN	Auto Mode 🗸
	Dynamic Routing (RIPv2) Enable LAN VVAN DMZ Routing information update timer Routing information timeout	30 Seconds 180 Seconds
	To-Appliance Packets Log C Enable To-Appliance Packets Log	
	System Reboot Reboot Content Security Gateway Appliance	boot
		OKCancel

Exporting Content Security Gateway settings

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

	System > Configure :	> Setting		
 System Administration Configure Setting Date/Time Multiple Subnet Route Table DHCP Dynamic DNS Host Table Language Logout 	Bac	kup / Restore Configuration File Download File Download Do you want to save this file Name: CSsys	em.conf wn File Type, 2.00 MB	Cancel der@mydomain.com)
⊯ Policy Object ⊯ Policy ⊯ Mail Security			Internet can be useful, some files c r. If you do not trust the source, do <u>?</u>	
■ IDP ■ Anomaly Flow IP		Mail Test	Mail Test	

Importing Content Security Gateway settings

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

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

	System > Configure > Setting	
⊫ System		
	Backup / Restore Configuration	
■ Administration □ Configure	Export System Setting to Client Download	
L⇒ Setting	Import System Setting from Client	C:\Documents and Setting: Browse
_+ Date/Time		(ex: CSsystem.conf)
_⇒ Multiple Subnet	Reset Factory Setting	
→ Route Table		
-⇒DHCP	System Name Setting	
→ Dynamic DNS	Device Name	(ex: Content Security Gateway)
_♦ Host Table	C	
L⇒ Language	E-mail Setting	
± Logout	Enable E-mail Alert Notification	
F Interface	Sender Address (Required by some ISPs)	(ex: sender@mydomain.com)

Restoring Factory Default Settings

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

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

PLANET Retworking & Communication	System > Configure > Setting	
■ System ■ Administration	Backup / Restore Configuration	
■ Auministration ⊟ Configure	Export System Setting to Client Download	
L→ Setting	Import System Setting from Client	Browse
_⇒ Date/Time		(ex: CSsystem.conf)
→ Multiple Subnet	Reset Factory Setting	
→ Route Table	System Name Setting	
→ Dynamic DNS	Device Name	(ex: Content Security Gateway)
_⇒ Host Table _⇒ Language	E-mail Setting	
Logout	Enable E-mail Alert Notification	

System Name Setting

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

Email Setting

- Step 1. Select Enable E-mail Alert Notification under E-Mail Setting. This function will enable the 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
	oystem - Conligue - Detting
■ System	
	Backup / Restore Configuration
🖻 Configure	Export System Setting to Client Download
L → Setting	Import System Setting from Client Browse
_♦ Date/Time	(ex: CSsystem.conf)
→ Multiple Subnet	Reset Factory Setting
→ Route Table	
-+ DHCP	System Name Setting
■● Dynamic DNS	Device Name CS-500 (ex: Content Security Gateway)
_♦ Host Table	E-mail Setting
L⇒ Language	
⊞ Logout	Enable E-mail Alert Notification
🗉 Interface	Sender Address (Required by some ISPs) support@planet.com (ex: sender@mydomain.com)
🗉 Policy Object	SMTP Server [dex: mail.mydomain.com]
🗉 Policy	E-mail Address 1 admin@planet.com.tv (ex: user1@mydomain.com)
🏽 Mail Security	
IDP	
🗷 Anomaly Flow IP	Mail Test

Web Management (WAN Interface)

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.

PLANET		
Retworking & Communication	system > Configure > Setting	
System		
Administration	Backup / Restore Configuration	
E Configure	Export System Setting to Client Download	
_♦ Setting	Import System Setting from Client	Browse
_→ Date/Time		(ex: CSsystem.conf)
-⇒ Multiple Subnet	Reset Factory Setting	
-⇒ Route Table		
.⇒ DHCP	System Name Setting	
➡ Dynamic DNS	Device Name	CS-500 (ex: Content Security Gateway)
➡ Host Table	E-mail Setting	
➡ Language		
Logout	Enable E-mail Alert Notification	
Interface	Sender Address (Required by some ISPs)	(ex: sender@mydomain.com)
Policy Object	SMTP Server	(ex: mail.mydomain.com)
Policy	E-mail Address 1	(ex: user1@mydomain.com)
Mail Security	E-mail Address 2	
DP		(ex: user2@mydomain.com)
Anomaly Flow IP	Mail Test	Mail Test
Monitor	Web Management (WAN Interface)	
	HTTP Port	80

MTU (set networking packet length)

The administrator can modify the networking packet length.

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

PLANET Retworking & Communication	System > Configure > Setting	
🗏 System	SMTP Server	(ex: mail.mydomain.com)
■ Administration	E-mail Address 1	(ex: user1@mydomain.com)
⊟ Configure	E-mail Address 2	(ex: user2@mydomain.com)
→ Setting	Mail Test	Mail Test
_♦ Date/Time		
→ Multiple Subnet	Web Management (WAN Interface)	
_⇒ Route Table	HTTP Port	80
-⇒ DHCP	MTU Setting	
■● Dynamic DNS	-	
_⇒ Host Table	MTU	1500 Bytes

Link Speed / Duplex Mode Setting

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

	System > Configure > Setting	
■ System	SMTP Server	(ex: mail.mydomain.com)
	E-mail Address 1	(ex:user1@mydomain.com)
■ Administration		(ox door regin) domain only
∃ Configure	E-mail Address 2	(ex: user2@mydomain.com)
_ ⇒ Setting	Mail Test	Mail Test
_⇒ Date/Time		
→ Multiple Subnet	Web Management (WAN Interface)	
_	HTTP Port	80
-+ DHCP	MTU Setting	
→ Dynamic DNS		
➡ Host Table	MTU	1500 Bytes
Language	Link Speed / Duplex Mode Setting	
' Logout	WAN	Auto Mode
🗉 Interface		Auto Mode
🗉 Policy Object	Dynamic Routing (RIPv2)	10M Half Duplex 10M Full Duplex
E Policy	Enable 📃 LAN 📃 WAN 📃 DMZ	100M Half Duplex
🗉 Mail Security	Routing information update timer	100M Full Duplex 30 Seconds
IDP	Routing information timeout	180 Seconds
T Anomoly Flow IP		3600 mus

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.

	System > Configure > Setting	
 System Administration Configure Setting 	SMTP Server E-mail Address 1 E-mail Address 2 Mail Test	(ex: mail.mydomain.com) (ex: user1@mydomain.com) (ex: user2@mydomain.com) Mail Test
 ⇒ Date/Time ⇒ Multiple Subnet ⇒ Route Table ⇒ DHCP ⇒ Dynamic DNS 	Web Management (WAN Interface) HTTP Port MTU Setting	80
 	MTU Link Speed / Duplex Mode Setting WAN	1500 Bytes Auto Mode
F Policy Object F Policy Mail Security F IDP F Assembly Flow ID	Dynamic Routing (RIPv2) Enable V LAN VWAN V DMZ Routing information update timer Routing information timeout	30 Seconds 180 Seconds

To-Appliance 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.

	System > Configure > Setting
 System Administration Configure Setting Date/Time Date/Time Multiple Subnet Route Table DHCP DHCP DHCP Longuage Longuage Longuat Interface Policy Mail Security IDP Anomaly Flow IP Monitor 	SMTP Server Central Address 1 Central Address 1 Central Address 2 Mail Test
	System Reboot Reboot Content Security Gateway Appliance Reboot

4.1.5 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 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.

PLANET Retworking & Communication	System > Configure > Date/Time	
 System Administration Configure Setting Date/Time ← ← Multiple Subnet Route Table DHCP Dynamic DNS Host Table Language 	System > Conligure > Date/Time System time : Wed Jan 1 05:07:16 2003 Synchronize system clock	OK
⊞ Logout		

4.1.6 Multiple Subnet

NAT mode

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

For instance: The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet works for the purpose of convenient management. The settings are as the following:

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

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

Service IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.11

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

Multiple Subnet settings

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

PLANET Retworking & Communication	System ≻ Config	gure > Multiple Subnet			
■ System		1020 Million Service ID / Democratic on Marche	lute de co	Alles ID solute for a 4 blater solu	0
■ Administration		WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
🖻 Configure		168.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	Modify Remove
→ Setting			_		
_⇒ Date/Time			N	ew Entry	
🗕 🌩 Multiple Subnet 🛛 🗲 🗲					
→ Route Table					
_ ⇒ DHCP					

Multiple Subnet functions

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

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

Alias IP of 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.

PLANET Retworking & Communication	System > Configure > Multiple Subnet		
≣ System	Add New Multiple Subnet IP		
Administration	Interface	●LAN ●DMZ	
Configure			
_⇒ Setting	Alias IP of Interface	192.168.2.1	
_⇒ Date/Time	Netmask	255.255.255.0	
→ Multiple Subnet			
→ Route Table	WANI	Interface IP	Forwarding Mode
-⇒DHCP			
→ Dynamic DNS	WAN	168.85.88.252 <u>Assist</u>	💿 NAT 🔍 Routing
→ Host Table			
L⇒ Language			OK Cancel
≇ Logout			

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	Modify Multiple Subnet IP		
	Interface	●LAN ●DMZ	
_⇒ Setting	Alias IP of Interface	192.168.2.1	
_♦ Date/Time	Netmask	255.255.255.0	
→ Multiple Subnet			
→ Route Table	WA	N Interface IP	Forwarding Mode
–● DHCP –● Dynamic DNS	WAN	168.85.88.252 <u>Assist</u>	NAT OR Routing
- → Host Table - → Language			OK Cancel
I Logout			

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	e Subnet			
⊫ System					
■ aystern ■ Administration	WAN Interf	ace IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
■ Auministration E Configure	16	68.85.88.252 / NAT	LAN	192.168.2.1 / 255.255.255.0	Modify Remove
L⇒ Setting			_		
_⇒ Date/Time			N	ew Entry	
→ Multiple Subnet					
→ Route Table					
-⇒DHCP		Microsoft Internet E	cplorer		
→ Dynamic DNS		9			
→ Host Table		Are you sure	/ou want to i	remove ?	
L⇒ Language					
I Logout		ОК	Cancel		
🎟 Interface					

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 > Config	ure > Multiple Subnet			
🖻 System		WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
Administration		/ Routing	LAN	168.85.88.1 / 255.255.255.192	Modify Remove
 ❑ Configure → Setting → Date/Time 			N	ew Entry	
→ Multiple Subnet → Route Table					

Multiple Subnet functions

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

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

Alias IP of 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.

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.

PLANET Retworking & Communication			
	System > Configure > Multiple Subnet		
■ System			
	Add New Multiple Subnet IP		
I Configure	Interface	● LAN ● DMZ	
L ⇒ Setting	Alias IP of Interface	168.85.88.1	
_⇒ Date/Time	Netmask	255.255.255.192	
_➡ Multiple Subnet			
→ Route Table	V/J	AN Interface IP	Forwarding Mode
→ DHCP	WAN		NAT Routing
→ Dynamic DNS		0.0.0.0 <u>Assist</u>	INAT I Rouling
–♦ Host Table			OK Canad
L⇒ Language			OK Cancel
' Logout			

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

	Policy > Incoming						
🗉 System							
Interface	Source	Destination	Service	Action	Option	Configure	Move
🗷 Policy Object	Outside_Any	Inside_Any(Routing)	ANY	 ✓ 		Modify Remove Pause	То 1 💌
E Policy							
-+ Outgoing					New Entry		
-+ Incoming							
-+ WAN To DMZ							
-→ LAN To DMZ							

Modify a Multiple Subnet Routing Mode

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

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

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

	System > Configure > Multiple Subnet		
l≡ System	Modify Multiple Subnet IP		
■ Administration			
⊟ Configure	Interface OLAN ODMZ		
_♦ Setting	Alias IP of Interface 168.85.88.1		
_♦ Date/Time	Netmask 255.255.255.192		
→ Multiple Subnet			
→ Route Table	WAN Interface IP		Forwarding Mode
-⇒ DHCP			
→ Dynamic DNS	VVAN 0.0.00	<u>Assist</u>	🔍 NAT 💿 Routing
_⇒ Host Table			
L⇒ Language			OK Cancel
≖ Logout			

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.

PLANET Retworking & Communication	System > Config	jure > Multiple Subnet			
≣ System		WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
Administration Configure		/ Routing	LAN	168.85.88.1 / 255.255.255.192	Modify Remove
Setting Date/Time Multiple Subnet Route Table				ew Entry	
➡ DHCP ➡ Dynamic DNS ➡ Host Table		Microsoft Internet E		remove ?	
L ⇒ Language ■ Logout ■ Interface		ОК	Cancel		

4.1.7 Route Table

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

Entering the Route Table screen

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

	System > Confi	gure > Route Table			
≣ System					
■ Administration		Interface	Destination IP / Netmask	Gateway	Configure
∃ Configure					
_♦ Setting			New Entry		
_♦ Date/Time					
■ Multiple Subnet					
🗕 🕈 Route Table 🛛 🗲 🗲					
_♦ DHCP					

Route Table functions

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

Adding a new Static Route

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

PLANET Refuerking & Communication	stem > Configure > Route Table		
⊠ System	Add New Static Route		
Administration Configure	Destination IP	192.168.4.0	
L→ Setting	Netmask	255.255.255.0	
_⇒ Date/Time	Gateway	192.168.1.254	
→ Multiple Subnet	Interface	LAN 🔽	
→ DHCP → Dynamic DNS			OK Cancel

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.

	System > Configure > Route Table		
⊟ System	Modify Static Route		
Administration	Destination IP	192.168.4.0	
L → Setting	Netmask	255.255.255.0	
_♦ Date/Time	Gateway	192.168.1.254	
→ Multiple Subnet	Interface	LAN 🔽	
→ Route Table → DHCP → Dynamic DNS			OK Cancel

Removing a Static Route

- **Step 1.** In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.
- **Step 2.** In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.

PLANET Networking & Communication	System > Configure > Route Ta	able		
m	Interface	Destination IP / Netmask	Gateway	Configure
inistration figure	LAN	192.168.4.0 / 255.255.255.0	192.168.1.254	Modify Remove
etting ate/Time ultiple Subnet		New	Entry	
oute Table HCP		Microsoft Internet Explorer		
mamic DNS ost Table		Are you sure you want to rem	nove?	
inguage put		OK Cancel		
ace				

4.1.8 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.

	System > Configure	> DHCP						
⊫ System	Due	namic IP Addre						_
■ Administration			192,168,1.0	Netmask		255,255,255,0		
E Configure		Subnet 192.168.1.0 Gateway 192.168.1.1		Broadcast		192.168.1.255		
→ Setting		Galeway 132.100.1.1		Di Daucasi		132.100.1.233		
→ Date/Time								
→ Multiple Subnet	v							
→ Route Table		Domain Name			((ex: dhcp.domain_name)		
■ Dynamic DNS ■ Host Table	DNS Server 1			192.168.1.1				
Language		DNS Server 2						
I Logout		WINS Server 1						
Interface	1							
Interface Policy Object		WINS Server 2						
Policy Object								
■ Folicy ■ Mail Security		LAN Interface :						
		Client IP Range 1			To	o [192.168.1.254	
Anomaly Flow IP		Client IP Range 2			То	b [
Monitor						L		
Mornton		DMZ Interface	:					
		Client IP Range	e1	192.168.10.2	То	. [192.168.10.254	
		Client IP Range			, то	. [
		Caencie (Valige	. 2		1	· [
		Leased Time		24 hours				
							O	Cancel

Dynamic IP Address functions

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

Enabling DHCP Support

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

Domain Name: The Administrator may enter the name of the LAN network domain if preferred. **Automatically Get DNS:** Check this box to automatically detect DNS server.

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

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

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

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

LAN interface:

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

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

DMZ interface:

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

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

Leased Time: Enter the leased time for DHCP.

Step 2. Click OK to enable DHCP support.

4.1.9 Dynamic DNS

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

	System > Configure > Dyna	mic DNS		
■ System ■ Administration	i.	Domain Name	WAN IP	Configure
⊴ Configure				
_♦ Setting			New Entry	
_♦ Date/Time				
■ Multiple Subnet				
→ Route Table				
-⇒DHCP				
🗕 🕈 Dynamic DNS 🛛 🗲 🗲				
→ Host Table				

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.

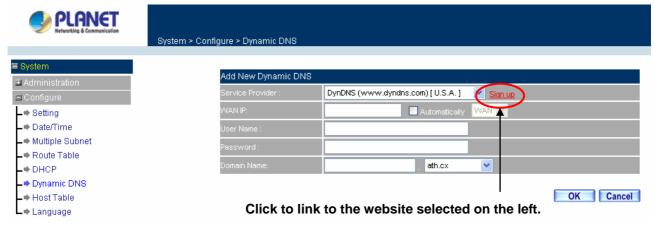
Configure: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

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.



Add Dynamic DNS settings

Step 1. Click Add button.

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

Service providers: Select service providers.

Sign up: to the service providers' website.

WAN IP Address: IP Address of the WAN port.

□ Automatically : Check to automatically fill in the WAN IP.。

User Name: Enter the registered user name.

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

Domain name: Your host domain name provided by ISP.

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

	System > Configure > Dynamic DNS	
■ System ■ Administration	Add New Dynamic DN	48
E Configure	Service Provider :	DynDNS (www.dyndns.com) [U.S.A.] 🛛 🔽 Sign up
_♦ Setting	WAN IP:	192.168.99.91 🗹 Automatically WAN 💌
■◆ Date/Time	User Name :	planet
■ Multiple Subnet	Password :	
-♦ Route Table -♦ DHCP	Domain Name:	planetest dyndns.org
–✦ Dynamic DNS –✦ Host Table –✦ Language		OKCancel

Modify dynamic DNS

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

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

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

	System > Configure > Dynamic DNS	
■ System ■ Administration	Modify Dynamic DNS	
E Configure	Service Provider :	DynDNS (www.dyndns.com) [U.S.A.] 🛛 🔽 Sian up
→ Setting	WAN IP:	192.168.99.91 🔽 Automatically WAN 💌
_♦ Date/Time	User Name :	planet
→ Multiple Subnet	Password :	
→ Route Table → DHCP	Domain Name:	planetest dyndns.org
 → Dynamic DNS → Host Table → Language 		OKCancel

Remove Dynamic DNS

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

	System > Configure > Dyr	namic DNS		
System	i	Domain Name	WAN IP	Configure
Administration Gonfigure	×	planetest.dyndns.org	192.168.99.91	Modify Remove
→ Setting → Date/Time → Multiple Subnet → Route Table → DHCP		Microsoft Internet Ex	New Entry	
- ➡ Dynamic DNS - ➡ Host Table - ➡ Language		Are you sure yo	ou want to remove ?	
Logout Interface			Cancel	

4.1.10 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.

PLANET Retworking & Communication	System > Config	jure > HostTable		
i System		Host Name	Virtual IP Address	Configure
■ Administration ⊒ Configure		mail.planet.com.tvv	192.168.10.10	Modify Remove
_→ Setting _→ Date/Time			New Entry	
-⇒ Multiple Subnet				
■ Route Table				
-⇒ DHCP				
Dynamic DNS				
🔺 Host Table 🛛 🗲 🗲				
_⇒ Language				

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.

PLANET Retworking & Communication	system > Configure > Host Table		
■ System	Add New Host Table		
Administration Gonfigure	Host Name	mail.planet.com.tw (ex: www.my_domain.com)	
-⇒ Setting	Virtual IP Address	192.168.10.10 (ex: 192.168.100.102)	
_♦ Date/Time			
→ Multiple Subnet			OK Cancel
→ Route Table			
-+ DHCP			
■ Dynamic DNS			
→ Host Table			
L⇒ Language			

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.

	System > Configure > Host Table		
■ System ■ Administration	Modify Host Table		
∃ Configure	Host Name	mail.planet.com.tw	(ex:www.my_domain.com)
_♦ Setting	Virtual IP Address	192.168.10.10	(ex: 192.168.100.102)
_♦ Date/Time			
→ Multiple Subnet			OK Cancel
→ Route Table			
-⇒ DHCP			
■ Dynamic DNS			
_♦ Host Table			
_⇒ Language			

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**.

PLANET Retworking & Communication	System > Configure > Host Table						
⊫ System							
	Host Name	Virtual IP Address	Configure				
⊟ Configure	mail.planet.com.tw	192.168.10.10	Modify Remove				
→ Setting							
_⇒ Date/Time		New Entry					
→ Multiple Subnet							
→ Route Table							
-⇒ DHCP	Microsoft Int	ternet Explorer 🛛 🔀					
_ ➡ Dynamic DNS	(?) Are						
_ ➡ Host Table	Are	you sure you want to remove ?					
L⇒ Language							
		K Cancel					
🗉 Interface							

4.1.11 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.

4.1.12 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.

	System > Logout > Logout	
🗏 System		
■ Administration		
■ Configure		
🖻 Logout		
L⇒Logout ←←		
🗉 Interface		
🗉 Policy Object		Microsoft Internet Explorer
🖬 Policy		
🎟 Mail Security		Are you sure you want to logout ?
■ IDP		~
🖬 Anomaly Flow IP		OK Cancel
🎟 Monitor		

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.

PLANET Hetworking & Communication	Interface > LAN					
≖ System						
⊫ Interface		LAN Interface				
LAN	1	P Address	192.168.1.1]		
→ WAN	1	Netmask	255.255.255.0			
L⇒ DMZ						
🗉 Policy Object	I	Enable	🗹 Ping		🗹 НТТР	
🗉 Policy						
📧 Mail Security						OK Cancel

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.

HTTP: 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 Retworking & Communication	Interface > WAN		
 System Interface ↓ LAN ↓ WAN ↓ DMZ Policy Object Policy Mail Security IDP Anomaly Flow IP Monitor 	WAN Interface ○ PPPoE (ADSL User) ○ Dynamic IP Address (Cable M ③ Static IP Address ○ PPTP (European User Only) IP Address Netmask Default Gateway DNS Server 1 DNS Server 2 Max. Downstream Bandwidth Max. Upstream Bandwidth Enable	Aodem User) 192.168.99.98 255.255.255.0 192.168.99.253 168.95.1.1 30000 Kbps (Max. 30 Mbps) 30000 Kbps (Max. 30 Mbps) 30000 Kbps (Max. 30 Mbps) W Ping	✓ HTTP

WAN Interface

Using the WAN **Interface**, the Administrator can sets 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.

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

HTTP: 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 IDP Anomaly Flow IP Monitor 	WAN Interface ● PPPoE (ADSL User) ● Dynamic IP Address (Cable M ● Static IP Address ● PPTP (European User Only) Current Status IP Address User Name Password IP Address provided by ISP	odem User) Disconnected 0.0.0 0.0.0 0 Dynamic 0 Fixed IP Address Netmask Default Gateway	Connecting Disconnect
	Max. Downstream Bandwidth Max. Upstream Bandwidth ✔ Service-On-Demand Auto Disconnect if idle Enable	30000 Kbps (Max. 30 Mbps) 30000 Kbps (Max. 30 Mbps) minutes (0 : means always connected) 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 assign to the device. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

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

User Name: The user name is provided by ISP.

Password: The password is provided by ISP.

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

Ping: Select this to allow the WAN 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.

HTTP: 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.

	Interface > WAN
¥ System System Interface ↓ LAN WAN DMZ Policy Object Policy Mail Security FIDP Anomaly Flow IP Monitor	WAN Interface PPPoE (ADSL User) Dynamic IP Address (Cable Modem User) Static IP Address PPTP (European User Only) IP Address 0.0.0.0 MAC Address 00:30:4F:44:A2:F5 Hostname Clone MAC Address Domain Name User Name (Required by DHCP+ protocol) Max. Downstream Bandwidth 30000 Kbps (Max. 30 Mbps) Max. Upstream Bandwidth 30000 Kbps (Max. 30 Mbps)
	Enable Ping HTTP
	OK

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.

Max. Upstream/Downstream Bandwidth: The bandwidth 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.

HTTP: 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 IDP Anomaly Flow IP Monitor 	WAN Interface PPPoE (ADSL User) Dynamic IP Address (Cable Mod Static IP Address PPTP (European User Only) IP Address Netmask Default Gateway DNS Server 1 DNS Server 2 Max. Downstream Bandwidth Max. Upstream Bandwidth Enable	dem User) 192.168.99.98 255.255.255.0 192.168.99.253 168.95.1.1 30000 Kbps (Max. 30 Mbps) 30000 Kbps (Max. 30 Mbps) W Ping	✓ HITP

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.

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

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.

HTTP: 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 Retworking & Communication	Interface > WAN			
 ♥ System ♥ Interface ● LAN ● WVAN ● DMZ ♥ Policy Object ♥ Policy ♥ Mail Security ♥ IDP ♥ Anomaly Flow IP ♥ Monitor 	Interface > WAN WAN Interface PPPoE (ADSL User) Dynamic IP Address (Cable M Static IP Address PTP (European User Only) Current Status IP Address User Name Password IP Address provided by ISP PTP Gateway Connect ID Max. Downstream Bandwidth Max. Upstream Bandwidth Max. Upstream Bandwidth Max. Upstream Bandwidth BEZEQ-ISRAEL Service-On-Demand	Disconnected 0.0.0.0 Obtain an IP addre MAC Address Hostname Domain Name O Use the following IP Address Netmask Default Gateway Source Address Netmask Default Gateway MAC Address Netmask Default Gateway MAC Address Mathematical Mathematical	00:30:4F:44:A2:F5	Connecting Disconnect
	Auto Disconnect if idle 0	∫minutes (0 : means always c		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 Retworking & Communication	Interface > DMZ			
■ System ■ Interface	DMZ Interface Disable	v		
LAN	IP Address	0.0.0.0		
-⇒ WAN -⇒ DMZ	Netmask	0.0.0.0		
🗷 Policy Object	Enable	Ping	HTTP	
🗉 Policy				
📧 Mail Security				OK Cancel
IDP				

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.

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

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, QoS, Authentication, 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 Retworking & Communication	Policy Object > /	Address ≻ LAN			
🗷 System					
🗉 Interface		Name	IP / Netmask	MAC Address	Configure
Policy Object		Inside_Any			In Use
🖻 Address					
L⇒LAN ←←			N	ew Entry	
-+ LAN Group					
– ♦ WAN					
-+ WAN Group					

Definition

Name: Name of LAN network address.

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

MAC Address: MAC address corresponded with LAN IP address.

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

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

Adding a new LAN Address

Step 1. In the LAN window, click the New Entry button.

Step 2. In the Add New Address window, enter the settings of a new LAN network address.

Step 3. Click OK to add the specified LAN network or click Cancel to cancel the changes.

	Policy Object > Address > LAN			
System	Add New Addres	s		
E Policy Object	Name	sebastien		
∃ Address	IP Address	192.168.1.2		
–♦ LAN	Netmask	255.255.255.255		
→ LAN Group	MAC Address	00:0E:A6:0F:8B:92	Clone MAC Address	
→ WAN Group	🔲 Get static IP ad	ddress from DHCP Server.		
■ → DMZ ■ → DMZ Group ■ Service				OK Cancel

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

Modifying an LAN Address

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

PLANET Retworking & Communication	Policy Object > Address	s ≻ LAN			
■ System ■ Interface	Modify	Address			
■ Policy Object	Name		sebastien		
∃ Address	IP Addr	ress	192.168.1.2		
–⇒ LAN	Netmas	sk	255.255.255.255		
– ➡ LAN Group – ➡ WAN	MAC A	ddress	00:0E:A6:0F:8B:92	Clone MAC Address	
_♦ WAN Group	🔲 Ge	et static IP address f	from DHCP Server.		
 → DMZ → DMZ Group 					OK Cancel
■ Service					

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.

	Policy Object > Ad	dress ≻ LAN			
ቛ System ≢ Interface		Name	IP / Netmask	MAC Address	Configure
E Policy Object		Inside_Any	0.0.0.0/0.0.0		In Use
⊒ Address		sebastien	192.168.1.2/255.255.255.255	00:0E:A6:0F:8B:92	Modify Remove
LAN LAN Group WAN WAN Group DMZ DMZ Group Service Schedule QoS		Micro		X	

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.

	Policy Object > A	\ddress > LAN Group		
≖ System				
🗉 Interface		Name	Member	Configure
🗏 Policy Object				
∃ Address			New Entry	
_ ⇒ LAN				
🗕 📥 LAN Group				
_ ♦ WAN				
→ WAN Group				

Definitions

Name: Name of the LAN group.

Member: Members of the group.

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

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

Nan	ne	Member	Configure
ENM	٨	sebastien	In Use

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

Group.

Source	Destination	Service	Action	Option	Configure	Move
ENM	Outside_Any	ANY	1		Modify Remove Pause	То 1 💌

Adding a LAN Group

- Step 1. In the LAN Group window, click the New Entry button to enter the Add New Address Group window.
- Step 2. In the Add New Address Group window:
 - Available address: list the names of all the members of the LAN network.
 - Selected address: list the names to be assigned to the new group.
 - **Name:** enter the name of the new group in the open field.
- Step 3. Add members: Select names to be added in Available address list, and click the Add>> button to add them to the Selected address list.
- **Step 4. Remove members:** Select names to be removed in the Selected Address list, and click the <<**Remove** button to remove these members from Selected Address list.
- Step 5. Click OK to add the new group or click Cancel to discard changes.

PLANET Retworking & Communication	Policy Object > Addr	ess > LAN Group		
■ System ■ Interface ■ Policy Object	Ado	l New Address Group ne:	_	
 Address Address Andress AN Group WAN WAN Group DMZ DMZ Group Schedule QoS Authentication Content Blocking Virtual Server VPN Policy Mail Security 		< Available address> sebastien	K Remove Add	< Selected address>
■ IDP ■ Anomaly Flow IP				OK Cancel

Modifying a LAN Group

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

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

- Available address: list names of all members of the LAN network.
- **Selected address:** list names of members which have been assigned to this group.
- Step 3. Add members: Select names in Available address list, and click the Add>> button to add them to the Selected address list.
- Step 4. Remove members: Select names in the Selected address list, and click the <<Remove button to remove these members from the Selected address list.

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

	Delia: Objects Addr			
System Finterface Policy Object Address LaN	Policy Object > Addro Moo Nam	Jify Address Group	ENM	
 → LAN Group → WAN → WAN Group → DMZ → DMZ Group # Service 		< Available address> sebastien	K Remove	<> Selected address> sebastien
Schedule Contentication Content Blocking Content Blocking Content Server Content Server Content Server	_			
■ VFN ■ Policy ■ Mail Security ■ IDP				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.

PLANET Retworking & Communication	Policy Object > A	\ddress ≻ LAN Group		
≖ System				
🗉 Interface		Name	Member	Configure
■ Policy Object		ENM	sebastien	Modify Remove
⊟ Address				Pause
-→ LAN				
-→ LAN Group			New Entry	
-+ WAN				
-+ WAN Group		Microsoft Inte	ernet Explorer 🛛 🔀	
-⇒ DMZ				
L → DMZ Group		📿 Arey	you sure you want to remove ?	
■ Schedule			Cancel	
∃ QoS				

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.

	Policy Object > Address > WAN		
≖ System	Name	IP / Netmask	Configure
■ Interface	Outside_Any	0.0.0.0/0.0.0	In Use
≡ Policy Object			
⊟ Address		New Entry	
–⇒ LAN			
–⇒ LAN Group			
-⇒WAN ←←			
-⇒WAN Group			
-⇒ DMZ			
→ DMZ Group			
Ξ Service			

Definitions

Name: Name of WAN network address.

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

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

NOTE: In the WAN 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.

	Policy Object > Address > WAN		
≖ Sy stem	Add New Address		
■ Interface ■ Policy Object	Name	Yahoo	
S Foncy object	IP Address	202.43.195.52	
-⇒ LAN	Netmask	255.255.255.255	
–⇒LAN Group			
-⇒ WAN			OK Cancel
-⇒WAN Group			
-⇒DMZ			
► DMZ Group			

Modifying an WAN Address

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

	IP / Netmask	Configure
🖩 System 🛛 🛛 Name		Configure
■ Interface Outside_Any	0.0.0.0/0.0.0	In Use
E Policy Object Yahoo	210.66.111.22/255.255.255.255	Modify Remove
⊟ Address		40
-⇒LAN	New Entry	
-⇒LAN Group		
-⇒WAN		
-⇒WAN Group		

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.

	Policy Object > Address > WAN		
≖ System	Name	IP / Netmask	Configure
Interface	Outside_Any	0.0.0.0/0.0.0	In Use
≡ Policy Object	Yahoo	202.43.195.52/255.255.255.255	Modify Remove
Address Address		New Entry	

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.

PLANET Retworking & Communication	Policy Object > Address > WAN Grou	up	
■ System ■ Interface	Name	Member	Configure
 ⇒ Policy Object ⇒ LAN ⇒ LAN Group ⇒ WAN Group ⇒ DMZ ⇒ DMZ Group 	÷	New Entry	

Definitions:

Name: Name of the WAN group.

Member: Members of the group.

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

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

Adding an WAN Group

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

window will appear.

- Step 2. In the Add New Address Group window the following fields will appear:
 - **Name:** enter the name of the new group.
 - Available address: List the names of all the members of the WAN network.
 - **Selected address:** List the names to assign to the new group.
 - Add members: Select the names to be added in the Available address list, and click the Add>> button to add them to the Selected address list.
 - Remove members: Select the names to be removed in the Selected address list, and click the <<Remove button to remove them from the Selected address list.</p>

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

	Policy Object > Address > WAN Group		
≖ System ≖ Interface	Add New Address Group Name:		
 ⇒ Policy Object Address ⇒ LAN ⇒ LAN Group ⇒ WAN ⇒ WAN Group ⇒ DMZ ⇒ DMZ Group ⇒ Service ⇒ Schedule ⇒ QoS ⇒ Authentication ⇒ Content Blocking ⇒ Virtual Server ⇒ VPN 	 Available address → Yahoo 	K Remove	Selected address ->
≖ Policy = Mail Canada			OK Cancel

Modifying a WAN Group

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

	Policy Object > Address > WAN Group		
≡ Sys tem	Name	Member	Configure
≡ Interface	Web	Yahoo	Modify Remove
≡ Policy Object			
⊟ Address		New Entry	
-⇒LAN			
-⇒LAN Group			
-⇒ WAN			
-⇒WAN Group			
-⇒DMZ			

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.

PLANET Returning & Communication	Policy Object > Address > WAN Gro	ıp	
≖ System	Name	Member	r Configure
■ Interface ■ Policy Object	Web	Yahoo	Modify Remove
⊑ Address		New Entry	
-⇒ LAN Group -⇒ WAN	Micro	osoft Internet Explorer 🛛 🔀	
-⇒ WAN Group -⇒ DMZ	2		
→ DMZ Group ± Service		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.

	Policy Object > Address > D	MZ		
⊯ System ⊯ Interface	Name	IP / Netmask	MAC Address	Configure
S Policy Object	0MZ_Any	0.0.0/0.0.0.0		In Use
⊆ Address		Ne	w Entry	
–⇒ LAN Group –⇒ WAN				
-⇒WAN Group				
-⇒ DMZ -⇒ DMZ Group				

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.

	Policy Object > Address > DMZ			
≖ System	Add New Address			
■ Interface	Name	Appach		
□ Policy Object □ Address	IP Address	192.168.99.96		
-⇒ LAN	Netmask	255.255.255.255		
–⇒ LAN Group –⇒ WAN	MAC Address	00:0E:A6:0F:8B:00	Clone MAC Address	
-⇒ WAN Group	Get static IP addr	ress from DHCP Server	r.	
→ DMZ → DMZ Group				OK

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		
≖ Sys tem	Name	IP / Netmask	MAC Address	Configure
🗉 Interface	DMZ_Any	0.0.0/0.0.0.0		In Use
≡ Policy Object	Appach	192.168.88.100/255.255.255.255		Modify Remove
 Address → LAN → LAN Group → WAN → WAN Group → DMZ → DMZ Group 		New	v Entry	40

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 > D	MZ		
■ System	N	ame	IP / Netmask	MAC Address	Configure
■ Interface	DM	Z_Any	0.0.0.0/0.0.0		In Use
Policy Object	Ap		192.168.99.96/255.255.255.255	00:0E:A6:0F:8B:00	Modify Remove
-⇒ LAN -⇒ LAN Group -⇒ WAN -⇒ WAN Group -⇒ DMZ -⇒ DMZ Group -⇒ DMZ Group -⇒ Schedule			New Microsoft Internet Explorer Are you sure you want to remo OK Cancel	X	

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.

	Policy Object > Address > DMZ Group		
⊯ System ⊯ Interface	Name	Member	Configure
© Policy Object		New Entry	
⊐ Address → LAN			
–⇒LAN Group –⇒WAN			
-> WAN Group			
–⇒ DMZ –⇒ DMZ Group			

Adding a DMZ Group:

- Step 1. In the DMZ Group window, click the New Entry button.
- Step 2. In the Add New Address Group window:
 - Available address: list names of all members of the DMZ.
 - Selected address: list names to assign to a new group.
- **Step 3.** Name: enter a name for the new group.

Step 4. Add members: Select the names to be added from the Available address list, and click the Add>> button to add them to the Selected address list.

Step 5. Remove members: Select names to be removed from the **Selected address** list, and click the <<**Remove** button to remove them from the **Selected address** list.

Step 6. Click OK to add the new group or click Cancel to discard changes.

PLANET Retworking & Communication	Policy Object >	• Address > DMZ Group		
 System Interface Policy Object Address → LAN → LAN Group → WAN Group → WAN Group → DMZ Group Service Schedule QoS Authentication Content Blocking 		Add New Address Group Name: Available address -> Appach	Kemove Add	Selected address ->
■ Virtual Server ■ VPN ■ Policy ■ Moli Security				OK Cancel

Modifying a DMZ Group:

Step 1. In the **DMZ** Group window, locate the **DMZ** group to be modified and click its corresponding **Modify** button in the **Configure** field.

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

- Available address: list the names of all the members of the DMZ.
- **Selected address:** list the names of the members that have been assigned to this group.

Step 3. Add members: Select names to be added from the available Address list, and click the Add>> button to add them to the Selected address list.

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

Step 5. Click OK to save changes or click Cancel to cancel editing.

Policy	Object > Address > DMZ Group		
⊯ System	Name	Member	Configure
≡ Interface	WHE IS	Appach	Modify Remove
🖻 Policy Object			dm
⊟ Address		New Entry	
–⇒ LAN			
–⇒LAN Group			
-⇒ WAN			
-⇒WAN Group			
-⇒DMZ			
L⇒ DMZ Group			

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.

PLANET Retworking & Communication	Policy Object > Address > DMZ Grou	P	
⊯ System ⊯ Interface	Name	Member	Configure
© Policy Object ⊆ Address → LAN	WED	Appeca New Entry	Modify Remove
→ + LAN Group → WAN → WAN Group → DMZ → DMZ Group Service Schedule	Micro 2	Are you sure you want to remove ?	

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.

	°olicy Object > Service > Pre₋de	fined		
	oncy object > Service > Pre-de	meu		
≖ System	ANY (Any)	TCP IMAP (143)	TCP POP3 (110)	TCP TELNET (23)
■ Interface	TCP AFPoverTCP (548)	TCP InterLocator (389)	TCP PPTP (1723)	UDP TETP (69)
■ Policy Object	TCP AOL (5190-5194)	TGP IRC (6660-6669)	TCP Real-Media (7070)	ICMP Traceroute (3,11)
≖ Address	TCP BGP (179)	TCP L2TP (1701)	UDP RIP (520)	UDP UDP ANY (Any)
⊟ Service	UDP DNS (63)	TCP LDAP (389)	TCP RLOGIN (513)	UDP UUCP (540)
- → Pre-defined 🗲 🗲	TCP FINGER (79)	TCP NetMeeting (389&1503&1720)	TCP SMTP (25)	TCP VDO-Live (7000-7010)
-⇒ Custom	TCP FTP (20-21)	UDP NES (111)	UDP SNMP (161)	TCP WAIS (210)
└ ⇒ Group	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)
■ Content Blocking	TCP HTTPS (443)	UDP PC Anywhere (5631-5632)	UDP TALK (617-618)	TCP MSN (1863)
	UDP IKE (600)	ICMP PING (Any)	TCP-ANY (Any)	

Icons and Descriptions

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

	Policy Ob	ject > Service > Custom				
■ System		Service name	Protocol	Client Port	Server Port	Configure
▼ Interface ∋ Policy Object				New Entry		
–⇒Pre-defined –⇒Custom						
⇒ Group						

Definitions:

Service name: The defined service name.

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

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

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

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

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

Adding a new Service

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

In the new service table:

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

The client port 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.



Policy Object > Service > Custom

⊯ System	Ad	d User
≡ Interface	Se	rvice N
≡ Policy Object	#	
∓ Address	1	۲
⊟ Service	2	0
– ➡ Pre-defined	3	0
- ♥ Custom	4	0
L⇒ Group	5	0
≝ Schedule	6	0
⊞ QoS	7	0
Authentication	8	0
± VPN		

Ado	dd User Defined Service							
Ser	vice NAME :							
#	Protocol	Client Port Server Port						
1	● TCP ● UDP ● Other 6	0 : 65535 0 : 0						
2	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
3	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
4	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
5	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
6	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
7	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						
8	● TCP ● UDP ● Other <mark>0</mark>	0 : 0 0 : 0						

OK Cancel

Modifying Custom Services

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

Step 2. Enter the new values.

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

	Polic	y Object > Service > (Custom			
≖ Sys tem		Service name	Protocol	Client Port	Server Port	Configure
≖ Interface		eDonkey	тср	0:65535	4661:4665	Modify Remove
🖻 Policy Object						- 4p
∃ Address				New Entry		
⊟ Service						
→ Pre-defined						
-⇒ Custom						
L⇒ Group						
T Sebedule						

Removing Custom Services

- Step 1. Click its corresponding Remove option in the Configure field.
- Step 2. In the Remove confirmation pop-up box, click OK to remove the selected service or click Cancel to cancel action.

PLANET Retworking & Communication	Policy Object >	Service >	Custom			
≖ System	Servic	e name	Protocol	Client Port	Server Port	Configure
≖ Interface	eDo	nkey	ТСР	0:65535	4661:4665	Modify Remove
⊫ Policy Object						
⊞ Address				New Entry		
⊟ Service		[Jav	aScript Applica	tion]	$\overline{\mathbf{X}}$	
–⇒ Pre-defined –⇒ Custom		G	Are you sure y	rou want to remove ?		
-⇒ Group		2-				
⊒ Schedule ⊒ QoS			ОК	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.

	Policy Object > Service > Group		
≖ System ≖ Interface	Group name	Service	Configure
 Interface Policy Object Address Service → Pre-defined → Custom → Group ◆ Group ◆ 		New Entry	

Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

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

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

Adding Service Groups

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

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

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

- **Step 3.** Enter the new group name in the group **Name** field. This will be the name referencing the created group.
- **Step 4.** To add new services: Select the services desired to be added in the Available service list and then click the Add>> button to add them to the group.
- **Step 5.** To remove services: Select services desired to be removed in the Available service, and then click the <<Remove button to remove them from the group.
- PLANET Policy Object > Service > Group system Add Service Group 🗉 Interface lame: 🗉 Policy Object 🗄 Address <-- Available service --> 📩 < — Selected service —> A ANY Service AFPoverTCP → Pre-defined AOL -+ Custom BGP L⇒ Group DNS **44** Remove FINGER Schedule FTP GOPHER ⊞ QoS Add HTTP Authentication HTTPS IKE **Ξ** Content Blocking IMAP InterLocator \pm VPN IRC 🗉 Policy 🖬 Mail Security 🗉 Anti-Attack OK Cancel 🔳 Monitor
- Step 6. Click OK to add the new group.

Modifying Service Groups

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

- Available service: lists all the available services.
- **Selected service:** list services that have been assigned to the selected group.
- Step 2. Add new services: Select services in the Available service list, and then click the Add>> button to add them to the group.
- Step 3. Remove services: Select services to be removed in the Selected service list, and then click the <<Remove button to remove theses services from the group.</p>
- Step 4. Click OK to save editing changes.

	Policy Object > Service > Group		
≡ System	Group name	Service	Configure
🗉 Interface	WEB	NetMeeting,MSN	Modify Remove
🖻 Policy Object			46
∓ Address		New Entry	
⊟ Service			
→ Pre-defined			
-⇒ Custom			
L⇒ Group			

Removing Service Groups

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

PLANET Retworking & Communication	Policy Object > Service :	> Group	
≖ System	Group name	Service	Configure
≖ Interface	Optional	NetMeeting,MSN	Modify Remove
🖻 Policy Object			
≖ Address		New Entry	
⊟ Service		avaScript Application]	
–♥ Pre-defined –♥ Custom –♥ Group		Are you sure you want to remove ?	
		OK Cancel	

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.

	Policy Object > Schedule > Setting	
≖ System	Name	Configure
■ Interface		5
⊫ Policy Object	New	Entry
⊞ Address		
⊞ Service		
⊟ Schedule		
L⇒ Setting		
⊒ QoS		

The following items are displayed in this window:

Name: the name assigned to the schedule

Configure: modify or remove

Adding a new Schedule

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

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

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

System	Add New S	chedule		
Interface				
Policy Object	Schedule	Name	Work-Time	
∓ Address				
 ■ Service		Week Day		riod
⊒ Schedule			Start Time	Stop Time
L⇒ Setting		Monday	09:00 💌	18:00 💌
QoS		Tuesday	09:00 💌	18:00 💌
Authentication		Wednesday	09:00 💌	18:00 💌
		Thursday	09:00 💌	18:00 💌
∓ Virtual Server		Friday	09:00 💌	18:00 💌
≖ VPN		Saturday	Disable 🔽	Disable 💌
Policy		Sunday	Disable 🔽	Disable 💌
Mail Security		J	,	,

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	
≖ Sys tem	Name	Configure
≖ Interface	Work-Time	Modify Remove
⊫ Policy Object		45
∓ Address	New	Entry
≖ Service		
⊟ Schedule		
L⇒ Setting		
⊞ QoS		

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.

	Policy Object > Schedule > Setting	
≖ System	Name	Configure
⊯ Interface	Work-Time	Modify Remove
⊫ Policy Object		
∓ Address	New	Entry
⊒ Service	[JavaScript Application]	
⊟ Schedule	[remeaning the obligation]	
L ⇒ Setting	Are you sure you want to remove ?	
± Q₀S	2-	
∓ Authentication	OK Cancel	
≖ Content Blocking		

4.3.4 QoS

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

The administrator can configure the bandwidth according to the WAN bandwidth.

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

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

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

CS-500 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. CS-500 also makes it convenient for the administrator to use CS_500 with the best Utility.

Configuration of QoS

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

PLANET Retworking & Communication	Policy Object > QoS >	Setting			
≖ System	Name WAN	Downstream Bandwidth	Upstream Bandwidth	Priority Configur	е
≖ Interface					_
≡ Policy Object		E.N.	ew Entry		
⊞ Address		THE OWNER OF THE OWNER	ew Entry		
 ≝ Service					
⊞ Schedule					
L⇒ Setting					

Definitions:

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

WAN: Display WAN interface.

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

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

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

Add New QoS

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

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

	Policy Object > QoS >	Setting		
≡ Sys tem	Add New QoS			
≖ Interface	Name	FTP		
⊫ Policy Object				
≖ Address	WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority
⊞ Service		G.Bandwidth = 128 Kbps	G.Bandwidth = <mark>64</mark> Kbps	
■ Schedule	1	M.Bandwidth = 512 Kbps	M.Bandwidth = 128 Kbps	High 💌
⊒ QoS L⇒ Setting				
∓ Authentication			L. L. L.	OK Cancel

Definition

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

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

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

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

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

Modify QoS

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

PLANET Retworking & Communication	Policy Obje	ct > QoS :	> Setting					
≡ Sys tem	Name	WAN	Downstream Ban	dwidth	Upstream Band	dwidth	Priority	Configure
🖬 Interface	FTP	1	G.Bandwidth =	128Kbps	G.Bandwidth =	64 Kbps	High	Modify Ref. Ve
≡ Policy Object		'	M.Bandwidth =	512Kbps	M.Bandwidth =	128 Kbps	riigii	Rei
⊞ Address								
■ Service				E No.	w. Entry			
■ Schedule				Ne	w Entry			
⊒QoS								
→ Setting								
 								

Click the Modify button to modify QoS.

Definition:

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

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

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

QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth. Click the **OK** button to modify QoS.

Delete QoS

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

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

PLANET Retworking & Communication	Policy Obje	ct > QoS	> Setting				
≡ Sys tem	Name	WAN	Downstream Bandwidth	Upstream Band	width	Priority	Configure
🖬 Interface	FTP	4	G.Bandwidth = 128Kbps	G.Bandwidth =	64 Kbps	High	Modify
⊫ Policy Object			M.Bandwidth = 512Kbps	M.Bandwidth =	128 Kbps	nıgıı	Remove
⊞ Address							
≖ Service			[JavaScript Application]				
≆ Schedule							
⊒ QoS			Are you sure you want to remove ?				
L⇒ Setting							
■ Authentication			OK Cancel				

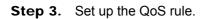
Example about how to install QoS correctly

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

PLANET Networking & Communication				
	Interface > WAN			
≖ System	WAN Interface			
⊫ Interface	O PPPoE (ADSL User)			
-⇒ LAN	O Dynamic IP Address (Cable M	odem User)		
-⇒ WAN	Static IP Address			
L⇒ DMZ	O PPTP (European User Only)			
⊯ Policy Object				
¤ Polic y			7	
⊯ Mail Security	IP Address	210.66.155.90		
⊯ Anti-Attack	Netmask	255.255.255.224		
⊯ Monitor	Default Gateway	210.66.155.94		
	DNS Server 1	168.95.1.1]	
	DNS Server 2]	
	Max. Downstream Bandwidth	4096 Kbps (M	lax. 30 Mbps)	
	Max. Upstream Bandwidth	672 Kbps (M	lax. 30 Mbps)	
	Enable	Ping	✓ HTTP	
				OK Cancel

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

PLANET Retworking & Communication	Policy Object > Address > LAN			
≖ System ■ Interface	Add New Address			
Interface Policy Object	Name	Alice		
🖻 Address	IP Address	192.168.1.20		
–⇒ LAN	Netmask	255.255.255.255		
→ LAN Group	MAC Address		Clone MAC Address	
– ➡ WAN Group – ➡ DMZ	Get static IP address f	from DHCP Server.		
L⇒ DMZ Group				OK Cancel



	Policy Object > QoS > S	Getting					
System Interface	Name	Downstream Bandw	/idth	Upstream Bandv	vidth	Priority	Configure
olicy Object Address	Alice_QoS		128 Kbps 512 Kbps		64 Kbps 128 Kbps	Middle	Modify Remove
iervice Ichedule				New Entry			
⊇oS ▶Setting							
Authentication							

PLANET		
P	olicy > Outgoing	
■ System		
📧 Interface	Comment :	
🗉 Policy Object	Add New Policy	
E Policy	Source Address	
→ Outgoing	Destination Address	Outside_Any 🔽
_⇒ Incoming	Service	ANY
-+ WAN To DMZ	Schedule	None 🗸
→ LAN To DMZ	Authentication User	None 💙
→ DMZ To WAN		
L DMZ TO LAN	Tunnel	None 💙
🗷 Mail Security	Action	PERMIT
IDP	Traffic Log	Enable
🗷 Anomaly Flow IP	Statistics	Enable
🗉 Monitor	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (0:means unlimited)
	QoS	
		OKCance

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

4.3.5 Authentication

By configuring the Authentication, you can control the user's access right time of LAN to WAN. The administrator can configure the authentication according to the authentication account and password. CS-500 configures the authentication of LAN's user by setting account and password to identify the privilege.

4.3.5.1 Auth Setting

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

Configuration of Authentication

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

	Policy Object >	Authentication > Auth Setting				
	T oncy object +	Addrenitation - Addreeting				
🗉 System						
🗉 Interface		Authentication Management				
■ Policy Object		Authentication Port		82		
± Address	1	Re-Login if Idle		30	Minutes	
± Service		Re-Login after user login successfully		0	Hours (0: means unlimited)	I
∃ Schedule						
∎ QoS		Disallow Re-Login if the auth user				
∃ Authentication		URL to redirect when authentication su	loceed			
Auth Setting		Messages to display when user login				
_ ➡ Auth User		messages to display when doer login				
→ Auth Group						
-⇒ RADIUS						
L⇒ POP3						
∃ Virtual Server						
∃ VPN						
E Policy						
🎟 Mail Security						OK Cancel

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

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

But if user does not need to open the web page and also want to access Internet resource such as FTP, then the user has to send http request with this port number, and CS-500 will send a User Login page for user to input user name and password.

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

Re-Login if Idle: When the LAN users access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes.

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

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

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

4.3.5.2 Auth User

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

	Policy Object > Authentication > Auth User	
≡ System	Authentication-User Name	Configure
≖ Interface	New L	Jser
≡ Policy Object		
∃ Address		
⊞ Service		
≖ Schedule		
⊒ QoS		
Authentication		
– ⇒ Auth Setting		
–⇒ Auth User		
-⇒Auth Group		
-⇒ RADIUS -⇒ POP3		
→ POP5 → Content Blocking		

Definitions:

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

Configure: modify settings or remove users.

Adding a new Auth User

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

- Step 2. In the Auth-User window:
 - Auth-User Name: enter the username of new Authentication.
 - **Password:** enter a password for the new **Authentication**.
 - **Confirm Password:** enter the password again.

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

	Policy Object > Authentication > Auth U	er	
System	Add New Authenticatio	n-User	
Interface	Authentication-User N	ame planet	
Policy Object ≇ Address	Password	•••••	
± Service	Confirm Password	•••••	
■ Schedule ■ QoS ■ Authentication			OK
-⇒ Auth Setting -⇒ Auth User -⇒ Auth Group -⇒ RADIUS			
P0P3			

NOTE*:* When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "Authentication"-> "Auth Setting" page.

PLANET		
Vetworking & Communication	· > Outgoing	
🗷 System	Current.	
📧 Interface	Comment :	
📧 Policy Object	Modify Policy	
E Policy	Source Address	Inside_Any 💟
→ Outgoing	Destination Address	Outside_Any 🔽
_+ Incoming	Service	ANY 💌
→ WAN To DMZ	Schedule	None 🗸
→ LAN To DMZ	Authentication User	planet 🗸
→ DMZ To WAN		
L → DMZ To LAN	Tunnel	None 💌
🗷 Mail Security	Action	PERMIT
IDP	Traffic Log	Enable
🖬 Anomaly Flow IP	Statistics	Enable
🎟 Monitor	IDP	
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (0:means unlimited)
	QoS	None

In the form of controlling the [Outgoing] Policy, enable the Authentication-User Function.

OK Cancel

User Login Page Definitions:

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

Authentication - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	At 1997
🕞 Back 🔹 🕥 👻 📓 😭 🔎 Search 🥎 Favorites 🤣 🔗 - 🕌	🗹 • 📙 🎇 🦓
Address 🗃 http://www.yam.com.tw/	🔽 🔁 Go 🛛 Links 🎽
User Login	
User Authentication	
User Name	
Password	
	ОК
E Done	🎱 Internet

Modifying the Authentication User

- Step 1. In the Authentication window, locate the Auth-User name you want to edit, and click on Modify in the Configure field.
- Step 2. The Modify Auth-User Password window will appear. Enter in the required information:
 - Auth-User: show original authentication user.
 - **Password:** show original password.
 - New Password: enter new password
 - **Confirm Password:** enter the new password again.
- Step 3. Click OK to confirm authentication user change or click Cancel to cancel it.

	Policy Object > Authentication > Auth	User	
■ System ■ Interface	Modify Authentication		
Policy Object	Password	planet	
■ Address	New Password		
■ Service ■ Schedule	Confirm Password		
≡ QoS			
S Authentication			OK Cancel
– ⇒ Auth Setting – ⇒ Auth User – ⇒ Auth Group			

Removing a Authentication User

- **Step 1.** In the Authentication table, locate the Auth-User name you want to edit, and click on the Remove option in the Configure field.
- Step 2. The Remove confirmation pop-up box will appear.
- Step 3. Click OK to remove that Authentication User or click Cancel to cancel.

PLANET Retworking & Communication	Policy Object > Authentication > Auth User	
≖ System ≖ Interface ≡ Policy Object	Authentication-User Name planet	Configure Modify Remove
 Poincy Object Address Service Schedule QoS Authentication → Auth Setting → Auth Group 	Microsoft Internet Explorer Image: Comparison of the second sec	User

4.3.5.3 Auth Group

Accessing the Auth Group window

Click **Authentication** in the menu bar on the left hand side of the window. Click **Auth Group** under it. A window will appear with a table displaying current Auth Group settings by the Administrator.

PLANET Retworking & Communication	Policy Object > Authentica	tion > Auth Group		
System	Name	Member	Radius POP3	Configre
Interface Policy Object		New Entry	7	
≝ Address				
⊒ QoS				
In Authentication → Auth Setting				
– ⇒ Auth User				
–⇒ Auth Group				
-⇒ RADIUS				
-⇒POP3				

Adding Auth Group

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

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

- **Name:** Enter the new Auth Group name.
- Available auth user: List all the available Auth User.
- Selected auth user: List Auth User to be assigned to the new group.
- **Step 2.** Enter the new group name in the group **Name** field. This will be the name referencing the created group.
- Step 3. To add new Auth User: Select the Auth User desired to be added in the Available auth user list, and then click the Add>> button to add them to the group.
- Step 4. To remove Auth User: Select Auth User desired to be removed in the Available auth user list, and then click the <<Remove button to remove them from the group.
- Step 5. Click OK to add the new group.

New Authentication Group Name: < Available Authentication User>	ENM	
planet (Radius User) (POP3 User)	Image: Contract of the second seco	Selected Authentication User —> planet
	(POP3 User)	** Remove

Modifying Auth Group

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

Vetworking & Communication	Policy Object > Authentication > Auth G	roup	
 System Interface Policy Object Address Service Schedule QoS Authentication Auth Setting Auth Group Auth Group Auth Group Auth Group POP3 Content Blocking Virtual Server VPN 	Modify Authentication-Us Name : (— Available Authentication U planet (Radius User) (POP3 User)	ENM	Selected Authentication User —> planet
			OK Cancel

Removing Auth Group

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

PLANET Retworking & Communication	Policy Object > Authenticatio	on > Auth Group			
≖ System	Name	Member	Radius	POP3	Configre
■ Interface	ENM	planet			Modify Remove
^Ξ Policy Object ≇ Address		New Entry			
■ Service ■ Schedule					
±QoS		Aicrosoft Internet Explorer 🛛 🔀			
Authentication → Auth Setting		Are you sure you want to remove ?			
–⇒ Auth User –⇒ Auth Group		OK Cancel			
-⇒ RADIUS					

4.3.5.4 Radius Serve

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

	Policy Object > Authentication > RADIUS	
n	RADIUS Server	
face	Enable RADIUS Server Authent	tication
olicy Object	RADIUS Server IP	
ddress	RADIUS Server Port	1812
rvice	Shared Secret	
Schedule	Enable 802.1x RADIUS Server A	Authentication
oS		
uthentication		
Auth Setting		
♦ Auth User		
♦ Auth Group		
➡ RADIUS		
-⇒P0P3		

Definition

- Enable RADIUS Server: Enable RADIUS Server Authentication.
- RADIUS Server IP: Enter RADIUS Server IP address.
- **RADIUS Server Port**: Enter RADIUS Server Port. The default port is 1812.
- Shared Secret: The Password for CS-500 to access RADIUS Server.
- Enable 802.1x RADIUS Server Authentication: Enable 802.1x RADIUS Server Authentication.

4.3.5.5 POP3

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

PLANET Networking & Communication	Policy Object > Authentication > POP3		
≖ System	POP3 Server		
Interface	Enable POP3 Server Authentication		
■ Policy Object	POP3 Server (IP or Domain Name)		
≖ Address	POP3 Server Port	110	
⊞ Service			
■ Schedule			OK Cancel
⊒ QoS			
Authentication ■ Authentication ■			
– ♦ Auth Setting			
– ⇒ Auth User			
–⇒Auth Group			
-⇒ RADIUS			
► ♥ POP3			

Definition

- Enable POP3 Server: Enable POP3 Server Authentication.
- **POP3 Server** : Enter POP3 Server IP address or domain name.
- POP3 Server Port: Enter POP3 Server Port. The default port is 110.

4.3.6 Content Blocking

Content Blocking includes "URL", "Scripts", "P2P", "IM", "Download" and "Upload".

URL: The administrator can use a complete domain name or key word to make rules for specific websites. **Scripts :** To let Popup、ActiveX、Java、Cookie in or keep them out.

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

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

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

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

4.3.6.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from 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.

PLANET Retworking & Communication	Policy Object > Content Blocking > URL	
⊯ System	URL String	Configure
⊯ Interface		
⊫ Policy Object	New Entry	
∓ Address		
⊞ Service		
 ∎ QoS		
■ Authentication		
Content Blocking		
-> URL 🗲 🗲		
-⇒ Script		
-⇒ P2P		
–⇒ IM –⇒ Download		

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.

	Policy Object > Content Bloc	king > URL	
≖ System	Add New URL Str	ing	
≡ Interface	URL String	gamble	
≡ Policy Object			
⊞ Address			OKCanc
⊞ Service			
⊞ Schedule			
⊞ QoS			
■ Authentication			
⊟ Content Blocking			
-⇒ URL			
–♦ Script			

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.

	Policy Object > Content Blocking > URL	
≖ Sys tem	URL String	Configure
≖ Interface	gamble	Modify Remove
🖻 Policy Object		
∓ Address	New Entry	
≖ Service		
≖ Schedule		
≖ QoS		
Authentication		
■ Content Blocking		
-⇒ URL		
–⇒ Script		
-		

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.

	Policy Object > Content Blocking > URL	
≖ Sys tem	URL String	Configure
≡ Interface	gamble	Modify Remove
≡ Policy Object		
∓ Address	New Entry	
⊞ Service	[JavaScript Application]	
⊞ Schedule		
 ∎ QoS	Are you sure you want to remove ?	
⊟ Content Blocking	OK Cancel	
-+ URL		
-⇒ Script		

4.3.6.2 Scripts

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

Step 1: Click Scripts below Content Blocking menu.

Step 2: Select Scripts detective functions:

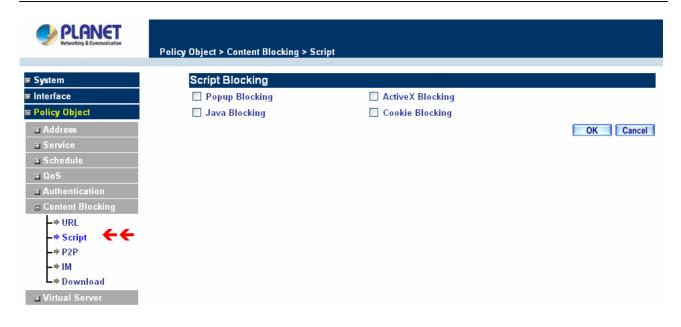
Popup Blocking: Prevent pop-up boxes from appearing.

ActiveX Blocking: Prevent ActiveX packets.

Java Blocking: Prevent Java packets.

Cookie Blocking: Prevent Cookie packets.

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



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

4.3.6.3 P2P

Step 1: Click P2P below Content Blocking menu.

Step 2: Select P2P detective functions:

eDonkey Blocking: Prevent eDonkey connection built up.

Bit Torrent Blocking: Prevent Bit Torrent connection built up.

WinMX Blocking: Prevent WinMX connection built up.

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

	Policy Object > Content Blocking > P2P
🗷 System	
🗉 Interface	Peer-to-Peer Application Blocking
🗏 Policy Object	The newest version : 1.0.0
⊞ Address	eDonkey Blocking
	Bit Torrent Blocking
⊞ Schedule	WinMX Blocking
∃ Q0S	
■ Authentication	OK Cancel
⊟ Content Blocking	
L⇒ URL	
_⇒ Script 🛛 🗲 🗲	
_⇒ P2P	
_ → IM	
L⇒ Download	

CS-500 provides a feature that will auto detect the P2P program version. When it detects a new version P2P program in the LAN site, CS-500 will connect to Internet and download the pattern to update the P2P Blocking function, and to keep the function working well to block new version P2P program. The current pattern version

will display at the top side.

4.3.6.4 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.

PLANET Retworking & Communication	Policy Object > Content Blocking > IM	
System Interface Policy Object Address Service Schedule GoS Authentication Content Blocking URL Script P2P	Instant Messaging Blocking The newest version : 1.0.0 MSN Messenger Blocking Yahoo Messenger Blocking ICQ Messenger Blocking QQ Messenger Blocking Skype Messenger Blocking	OK
-→ IM		

CS-500 provides a feature that will auto detect the IM program version. When it detects a new version IM program in the LAN site, CS-500 will connect to Internet and download the pattern to update the IM Blocking function, and to keep the function working well to block new version IM program. The current pattern version will display at the top side.

4.3.6.5 Download

Step 1: Click Download below Content Blocking menu.

Step 2: Select Download detective functions:

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

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

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

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

PLANET Networking & Communication	Policy Object > Content Blocking > Downl	heni		
	Toney object content blocking borning			
🗉 System				
🗉 Interface	Download Blocking			
🗏 Policy Object	All Types Blocking			
 Address	🔲 Audio and Video Types	Blocking		
■ Service	Extension Blocking			
■ Schedule	.exe	.zip	.rar	
∎ QoS	.iso	.bin	rpm	
■ Authentication	.doc	.xl?		
⊟ Content Blocking	.pdf	.tgz	gz	
-+> URL	.bat	.dll	.hta	
_♦ Script	.scr	.vb?	.wps	
_⇒ P2P	.pif	📃 .msi	.com	
-⇒IM	reg	.mp3	mpeg	
🗅 Download	mpg			
■ VPN			OKCan	cel
■ Policy				

4.3.6.6 Upload

Step 1: Click Upload below Content Blocking menu.

Step 2: Select Upload detective functions:

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

Audio and Video Types block: To block audio and video uploading 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.

📣 PLANET				
Vetworking & Communication	Policy Object > Content Blocking > Uploa	d		
🗉 System				
🗉 Interface	Upload Blocking			
■ Policy Object	All Types Blocking			
Address	Extension Blocking			
± Service	.exe	zip	🔲 .rar	
± Schedule	.iso	.bin	rpm	
∎ QoS	.doc		.ppt	
■ Authentication	.pdf	tgz	gz	
⊟ Content Blocking	.bat	.dll	🔲 .hta	
_♦ URL	.scr	.vb?	.wps	
_♦ Script	.pif	.msi	.com	
_⇒ P2P	.reg	.mp3	mpeg	
—⇒ IM	mpg			
→ Download				
L⇒ Upload			OKCa	incel
▪ Virtual Server			On Ga	11001

4.3.7 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:

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

4.3.7.1 Mapped IP

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

Entering the Mapped IP window

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

	r Object > Virtual Server > Ma	pped IP	
 System Interface Policy Object Address Service Schedule QoS Authentication Content Blocking Virtual Server Server 1 Server 2 Server 3 Server 4 	WAN IP	Map To Virtual IP New Entry	Configure

Definition:

WAN IP: WAN IP Address.

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

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

Adding a new IP Mapping

- Step 1. In the Mapped IP window, click the New Entry button. The Add New Mapped IP window will appear.
 - WAN IP: select the WAN public IP address to be mapped.
 - 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.

PLANET Hetworking & Communication	Policy Object > Virtual Server > Mapp	ed IP	
⊯ System	Add New Mapped IP		
Interface	WAN IP	Assist	
🖻 Policy Object	Map To Virtual IP		
 			
≝ Service			OK Cancel
⊞ QoS			
≖ Authentication			
■ Content Blocking			
⊟ Virtual Server			
-⇒ Mapped IP			
–♦ Server 1			
-⇒ Server 2			
Sanvar 3			

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.

PLANET Retworking & Communication	icy Object > Virtual Server > Mapped I	p	
≖ System	WAN IP	Map To Virtual IP	Configure
≡ Interface	210.66.155.91	192.168.1.12	Modify Remove
≡ Policy Object		New Entry	<u></u>
≖ Address			
≖ Service			
⊞ Schedule			
⊒ QoS			
■ Authentication			
≖ Content Blocking			
⊒ Virtual Server			
-⇒Mapped IP			
–♦ Server 1			

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

Removing a Mapped IP

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

PLANET Retworking & Communication Poli	cy Object > Virtual Server > Mapped	IP	
System	WAN IP	Map To Virtual IP	Configure
Interface	210.66.155.91	192.168.1.12	Modify Remove
Policy Object		New Entry	
 ∎ Address			
∓ Service	[JavaScript Applic	ation]	
∓ Schedule	Louveset the whole		
± QoS	Are you sure	you want to remove ?	
∓ Authentication			
≖ Content Blocking	0	Cancel	
⊒ Virtual Server			
-⇒Mapped IP			
–♦ Server 1			
–♦ Server 2			

4.3.7.2 Virtual Server

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

PLANET Networking & Communication	Policy Object > Virtual Server > Server 1			
≆ System ≆ Interface	Virtual Server Real IP			
🖻 Policy Object	Service	WAN Port	Server Virtual IP	Configure
∓ Address				
≖ Service				
≖ Schedule				
<u>∎</u> QoS				
■ Authentication				
■ Content Blocking				
⊒ Virtual Server				
–⇒Mapped IP				
- Server 1 🗧 🗲 🗲				
-⇒ Server 2				
-⇒ Server 3				
L⇒ Server 4				

Definition:

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

Service: The service 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.

	Policy Object > Virtual Server > Server 1		
∎ System	Add New Virtual Server IP		
∎ Interface	Virtual Server Real IP	Assist	
≡ Policy Object			
∓ Address			
 ∃ Service			OK Cano
Schedule			
∃ QoS			
■ Content Blocking			
⊟ Virtual Server			
–⇒Mapped IP			
–♦ Server 1			
→ Server 2			

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.

	Policy Object > Virtual Server > Server 1			
≖ System ≖ Interface	Virtual Server Real IP 210.66.155.9	_		
⊫ Policy Object	Service	WAN Port	Server Virtual IP	Configure
≖ Address ≖ Service		New Entry		
⊞ QoS				
■ Authentication				
■ Content Blocking				
■ Virtual Server				
–♦ Mapped IP				
–♦ Server 1				
→ Server 2				

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.

PLANET Retworking & Communication	Policy Object > Virtual Server > Server 1		
≖ System	Add New Virtual Server IP		
≖ Interface	Virtual Server Real IP	Assist	
≡ Policy Object			
∓ Address			
≖ Service			OK Cano
≖ Schedule			
⊞ QoS			
■ Content Blocking			
⊒ Virtual Server			
–⇒Mapped IP			
–♦ Server 1			
-⇒ Server 2			

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

Server (Load Balance Server).

- External Service Port: Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- Load Balance Server: The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.
- **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.

PLANET Retworking & Communication	Policy Object > Virtual Server > Serv	er 1		
≖ System	Virtual Server Configurat	ion		
≖ Interface	Virtual Server Real IP	210.66.155.91		
⊫ Policy Object	Service	ANY (0-65535)	v	
+ Address	External Service Port	0-65535		
≖ Service	Load Balance Server		Server Virtual IP	
■ Schedule	1			
∎ QoS	2			
∓ Authentication	3			
	4			
⊒ Virtual Server	4			
-⇒Mapped IP				OK Cancel
–♥ Server 1				United
–♦ Server 2				

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.

	Virtual Server Configurati	on	
e	Virtual Server Real IP	210.66.155.91	
bject	Service	HTTP (80)	
ss	External Service Port	80	
ce	Load Balance Server	Server V	irtual IP
lule	1	192.168.1.	.20
	2	192.168.1.	.21
ntication	3	192.168.1.	.22
nt Blocking I Server	4	192.168.1.	.23

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

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

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.

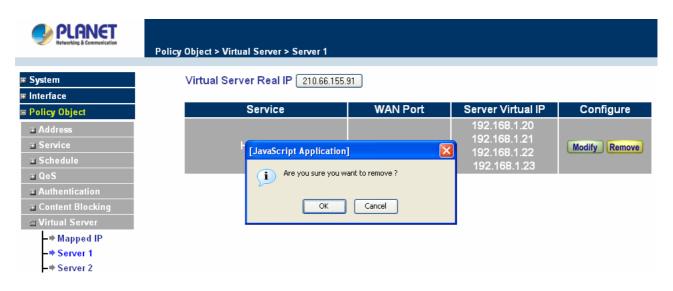
PLANET Networking & Communication	Policy Object > Virtual Server > Server 1			
⊯ System ⊯ Interface	Virtual Server Real IP 210.66.155.	91		
⊫ Policy Object	Service	WAN Port	Server Virtual IP	Configure
Address Service Schedule	HTTP (80)	80	192.168.1.20 192.168.1.21 192.168.1.22 192.168.1.23	Modify Remove
QoS Authentication Content Blocking Virtual Server		New Entry		
–⇒ Mapped IP –⇒ Server 1 –⇒ Server 2				

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.



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.

4.3.8 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.

Tunnel: To define local and remote VPN device with related information, then the **Tunnel** entry can be selected in **Policy** in order to submit the further function to the VPN traffic.

What is New?

CS-500 isolates the **Tunnel** setting in order to allow **Policy** rule controlling VPN traffic. So user can filter the VPN packets with **QoS**, **IDP** rule, and record the connection in **Traffic Log** or **Statistic**. Hence, to set up a **Virtual Private Network** (VPN), you need to configure CS-500 with following setting:

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

4.3.8.1 IPSec Autokey

This chapter describes steps to create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. For example, with two 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.

	Policy Object > VP	N > IPSec Autokev			
≖ System		,			
■ o,etern: ■ Interface	i	Name	Gateway IP	IPSec Algorithm	Configure
E Policy Object					
≖ Address			New	Entry	
± Service					
∃ Schedule					
∎ QoS					
■ Authentication					
■ Content Blocking					
Virtual Server					
S VPN					
IPSec Autokey					

The fields in the IPSec Autokey window are:

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

- Gateway IP: The other side WAN interface IP address of VPN Gateway.
- IPSec Algorithm: The display the Algorithm way.
- **Configure:** Modify and Delete.

Adding the Autokey IKE

Step 1: Click the New Entry button and the VPN Auto Keyed Tunnel window will appear. It divides into two parts of the setting, Necessary Item and Optional Item.

Networking & Communication	Policy Object > VPN > IPSec Autokey	
n		
 ace	Necessary Item	
Object	Name	(Max. 12 characters)
ess	To Destination	
ice	Remote Gateway Fixed IP or Domain Name	(Max. 99 characters)
dule	Remote Gateway or Client Dynamic IP	
entication	Authentication Method	Preshare 🗸
tent Blocking	Preshared Key	(Max. 103 characters)
al Server	Encapsulation	(wax. ros characters)
	ISAKMP Algorithm	
Sec Autokey	ENC Algorithm	DES
PTP Server	AUTH Algorithm	MD5 V
PTP Client		GROUP 1
innel	Group	
У	IPSec Algorithm	
Becurity	Data Encryption + Authentication	
	ENC Algorithm	DES
naly Flow IP or	AUTH Algorithm	MD5 💌
lur	 Authentication Only 	
	Optional Item	
	Perfect Forward Secrecy	NO-PFS 💌
	ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
	IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
	Mode	● Main mode ● Aggressive mode
	My ID	(Max. 39 characters)
	Peer ID	(Max. 39 characters)
	GRE/IPSec	
	GRE Local IP	
	GRE Remote IP	
	Dead Peer Detection Retry <mark>5 t</mark> imes Timeout <mark>5</mark> 10)	Second (Retry Range: 0 - 10, 0: means disable; Timeout Rang

Step 2: Configure Necessary Item paremeters.

Name: Specify a name for the VPN rule.

To Destination:

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

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

ISAKMP Algorithm

ENC 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 or AES 256-bit encryption algorithm. The default algorithm 56 bit DES-CBC.

AUTH Method: Authentication Method. Selects MD5 (128-bit hash) or SHA-1 (160-bit hash) authentication algorithm. In general, SHA-1 is more secured than MD5. The default algorithm is MD5.

Group: Selects Group 1 (768-bit modulus), Group 2 (1024-bit modulus) or Group 5 (1536-bit modulus). The larger the modulus, the more secure the generated key is. However, the larger the modulus, the longer the key generation process takes. Both side of VPN tunnels must agree to use the same group. The default algorithm is Group 1.

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

Data Encryption + Authentication

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

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

Step 3: Configure Optional Item paremeters if necessary.

- Perfect Forward Secrecy: Select Group 1, Group 2 or Group 5 to enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. The default is NO-PFS.
- ISAKMP Lifetime: New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 3600 seconds (one hours). Selection of small values could lead to frequent re-keying, which could affect performance.
- IPSec Lifetime: New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 28800 seconds (eight hours). Selection of small values could lead to frequent re-keying, which could affect performance.
- **Mode:** Select Main mode or Aggressive mode algorithm.

- My ID/Peer ID: My ID and Peer ID are optional parameters. If we choose to enter My ID/ Peer ID, they couldn't be the same. For instance, My ID is 11.11.11.11 and Peer ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123A and @abcd123.
- GRE/IPSec: Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology. You may enter IP to be identified for both VPN gateways.
- Dead Peer Detection : Configure the timing to detect the VPN status. If failed, CS-500 will disconnect the VPN tunnel.

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

4.3.8.2 PPTP Server

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

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

	Policy Object > VPN > PPTP Server			
■ System ■ Interface ■ Policy Object	PPTP Server(Disable): Client IP Range:192.238.6.1-254 Modify	1		
Address Service	i User Name	Client IP	Uptime	Configure
Schedule QoS Authentication Content Blocking Virtual Server VPN PPTP Server PPTP Client Tunnel		New Entry		

- **PPTP Server** : Click **Modify** to select Enable or Disable.
- **Client IP Range**: Display the IP addresses range for PPTP Client connection.
- User Name : Displays the PPTP Client user's name for authentication.
- Client IP : Displays the PPTP Client's IP address for authentication.
- Uptime : Displays the connection time between PPTP Server and Client.
- Configure : Click Modify to modify the PPTP Client settings or click Remove to remove the item.

Modifying PPTP Server Design

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

	Policy Object > VPN > PPTP Server
🗷 System	Madife Canada Daning
🎟 Interface	Modify Server Design
🖻 Policy Object	Disable PPTP
 ≇ Address	
■ Service	Enable PPTP
™ Schedule	Encryption
 ∎ Q08	Client IP Range : 192.238.6.1 254
■ Authentication	Allow remote client to connect to Internet.
■ Content Blocking	
E VPN	Auto-Disconnect if idle <mark>0</mark> minutes (Range: 0 - 999999, 0: means always connected)
→ IPSec Autokey	Echo-Request Retry 4 times Timeout 30 Second (Retry Range: 0 - 9, 0: means disable; Timeout Range: 1 -
■ PPTP Server	60)

- **Disable PPTP:** Check to disable PPTP Server.
- Enable PPTP: Check to enable PPTP Server.

Encryption: the default is set to disabled.

- **Client IP Range:** Enter the IP range allocated for PPTP Clients when they connect to the PPTP server.
- Allow remote client to connect to Internet: Check to allow remote PPTP client accessing Internet via PPTP tunnel.
- Auto-Disconnect if idle minutes: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- Echo-Request: Configure the timing to detect the VPN status. If failed, CS-500 will disconnect the VPN tunnel.
- Step 4. Click OK to save modifications or click Cancel to cancel modifications

Adding PPTP Server

- Step 1. Select VPN→PPTP Server. Click New Entry.
- Step 2. Enter appropriate settings in the following window.
 - User name: Specify the PPTP client. This should be unique.
 - Password: Specify the PPTP client password.
 - Client IP assigned by:
 - 1. IP Range: check to enable auto-allocating IP for PPTP client to connect.
 - 2. Fixed IP: check and enter a fixed IP for PPTP client to connect.

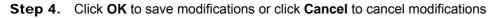
	olicy Object > VPN > PPTP Server	
lystem		
nterface	Add New PPTP Server	
olicy Object	User Name:	
Address	Password :	
Service	Client IP assigned by	Ĩ.
Schedule	• IP Range	
QoS	Fixed IP :	
Authentication		
Content Blocking		OK Cance
/irtual Server		OK
(PN		
IPSec Autokey		
PPTP Server		
PPTP Client		
➡ Tunnel		

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 > Pf	PTP Server			
■ System ■ Interface ■ Policy Object		rver (Enable, Encryption: C Range : 192.238.6.1-254			
■ Address ■ Service	i	User Name	Client IP	Uptime	Configure
Schedule		planet	0.0.0.0		Modify Remove
I QoS					
■ Authentication			ſ	New Entry	
■ Content Blocking					
I VPN					
→ IPSec Autokey					
→ PPTP Server					
→ PPTP Client					
L. → Tunnel					



Removing PPTP Server

- Step 1. Select VPN→PPTP Server.
- **Step 2.** In the **PPTP Server** window, find the PPTP server that you WAN t to modify. Click **Configure** and click **Remove**.
- Step 3. Click OK to remove the PPTP server or click Cancel to exit without removing.

PLANET Retworking & Communication	Policy Object > VPN > F	PPTP Server			
📧 System					
■ Interface	PPTP S	erver (Enable, Encryption:	ON):		
Policy Object	Client IF	Range : 192.238.6.1-254	Modify		
± Address					
± Service	- i	User Name	Client IP	Uptime	Configure
■ Schedule			0.0.0.0		Modify Remove
 ∎ QoS					
		Microsoft I	nternet Explorer		
■ Content Blocking		2 Ar	e you sure you want t		
		Ar	e you sure you want t	o remove ?	
I VPN				_	
→ IPSec Autokey			OK Cancel		
→ PPTP Server					
→ PPTP Client					
L					

4.3.8.3 PPTP Client

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

Entering the PPTP Client window

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

📣 PLANET					
Vetworking & Communication	Policy Object > VPN > PPTP Client				
🗉 System					
🗉 Interface	PPTP Client :				
🗏 Policy Object	i User Name	Server IP or Domain Name	Encryption	Uptime	Configure
∃ Address					
∃ Service		New Entry			
± Schedule					
∎QoS					
■ Content Blocking					
E VPN					
➡ IPSec Autokey					
→ PPTP Server					
_⇒ PPTP Client					
L					

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

Adding a PPTP Client

Step 1. Select VPN → PPTP Client. PLANET Policy Object > VPN > PPTP Client 🗉 System Add New PPTP Client 🗉 Interface planet 🗏 Policy Object ∃ Address ∃ Service 61.20.30.40 🗹 Encryptic ∃ Schedule ∓QoS NAT(Connect to Windows PPTP Serve ■ Authentication ■ Content Blocking OK Cancel I Virtual Server SIVPN L. ♦ IPSec Autokey -+ PPTP Server ■ PPTP Client L⇒ Tunnel

Step 2. Configure the parameters.

- **User name:** Specify the PPTP client. This should be unique.
- **Password:** Specify the PPTP client password.
- Server IP or Domain Name: Enter the PPTP Server's IP address.
- **Encryption:** Enable or Disabled the Encryption.
- NAT (Connect to Windows PPTP Server): Select this function to setup the connection with PPTP VPN Client of CS-500 and Windows PPTP Server.

Modifying PPTP Client

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

📣 PLANET					
Wetworking & Communication	Policy Object > VPN > PPTP Client				
System					
Interface	PPTP Client :				
Policy Object	i User Name	Server IP or Domain Name	Encryption	Uptime	Configure
∓ Address	planet	61.20.30.40	ON		Modify Remove
+ Service					<i>d</i>)
■ Schedule		New E	ntry		
∎ QoS					
■ Authentication					
Content Blocking					
▪ Virtual Server					
E VPN					
■ IPSec Autokey					
■ PPTP Server					
■ PPTP Client					
L⇒ Tunnel					

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

Removing PPTP Client

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

PLANET Networking & Communication	Policy Object > VPN > P	PTP Client				
■ System ■ Interface	PPTP CI	ient :				
■ Policy Object	i i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
. ■ Address		planet		ON		Modify Remove
■ Service						
⊞ Schedule			New E	ntry		
∎ QoS						
■ Authentication		MICT	osoft Internet Explorer	×		
■ Content Blocking		?	Are you sure you want to remov	e 7		
		~		C :		
E VPN			OK Cancel			
→ IPSec Autokey						
PPTP Server						
■● PPTP Client						
L						

4.3.8.4 Tunnel

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

Entering the Tunnel window

Step 1. Select V	/PN→Tunnel.					
	Policy Object > VPN >	• Tunnel				
🗷 System						
🗉 Interface	i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
🗏 Policy Object						
∃ Address				New Entry		
■ Service						
± Schedule						
±QoS						
■ Authentication						
■ Content Blocking						
E VPN						
→ IPSec Autokey						
■● PPTP Server						
→ PPTP Client						
L+ Tunnel						

Step 2. Configure the parameters

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

Adding a Tunnel

Step 1. Sel	ect VPN→Tunnel .
-------------	-------------------------

PLANET						
Wetworking & Communication	Policy Object > VPN > Tunnel					
l System						
Interface	New Entry Tunnel					
Policy Object		IPC as Turned				
± Address	Name	IPSecTunnel				
■ Service	From Source	💿 lan 🔘 dmz	●LAN ● DMZ			
■ Schedule	From Source Subnet / Mask	192.168.1.0	/ 255.255.255.0			
± QoS	To Destination					
■ Authentication	To Destination Subnet / Mask	192.168.0.0	/ 255.255.255.0			
Content Blocking	 Remote Client 					
■ Virtual Server	IPSec / PPTP Setting	CS500	~			
E VPN						
■● IPSec Autokey	Keep alive IP :	192.168.0.1				
■● PPTP Server	Show remote Network Neighborhood					
■● PPTP Client						
→ Tunnel			OK Cancel			
Policy						

- Step 2. Configure the parameters
 - Name: Specify the Tunnel name. This should be unique and can not be the same as the name of IPSec Autokey rule.
 - From Source: Specify the VPN source to LAN or DMZ site.
 - From Source Subnet / Mask: Specify the source LAN network subnet and Mask.
 - To Destination:
 - **To Destination Subnet / Mask:** Specify the destination LAN network subnet and Mask.
 - **Remote Client:** Select **Remote Client** if there is only one user and dials up to Internet with PPPoE or cable modem.
 - IPSec/PPTP Setting: Select the specific VPN tunnel for this Tunnel rule, you need to pre-define IPSec or PPTP setting first.
 - Keep Alive IP: Specify Remote Gateway's LAN IP address to keep alive the VPN tunnel
 - Show remote Network Neighborhood: Select the remote Network Neighborhood enable to show.

Modifying a Tunnel

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

PLANET Networking & Communication						
	Policy Object >	VPN ≻ Tunnel				
System						
Interface	i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
E Policy Object						Modify Ren. ve
± Address	– <mark>문</mark> . –	IPSecTunnel	192.168.1.0			Ren_ve
± Service						Pause
± Schedule						
±QoS			l	New Entry		
E Authentication						
▪ Content Blocking						
Virtual Server						
I VPN						
■ IPSec Autokey						
■● PPTP Server						
→ PPTP Client						
L⇒ Tunnel						

Removing Tunnel

Step 1. Select VPN→Tunnel.

Step 2. In the Tunnel window, find the Tunnel that you want to modify and click Remove.

	Policy Object > V	′PN > Tunnel				
lystem						
Interface	i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configur
Policy Object						Modify
Address	– <mark>믣</mark> .					Remove
Service						Pause
Schedule						
QoS				New Entry		
Authentication		Microsoft	Internet Explorer			
Content Blocking						
Virtual Server		· ? ·	Are you sure you want to remo	ive "IPSecTunnel" ?		
IVPN						
IPSec Autokey			OK Cancel			
PPTP Server						
PPTP Client						
-+ Tunnel						

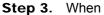
Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.

Pausing a Tunnel

Step 1. Select VPN→Tunnel.

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

🌒 PLANET						
Vetworking & Communication	Policy Object > \	/PN > Tunnel				
	1 6110 / 6 6 / 6 6 / 6					
Bystem						
Interface	i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configur
Policy Object						Modify
Address	₽.		192.168.1.0			Remove
Service						Pause
Schedule						
QoS				New Entry		
Authentication		Microsoft Intern	net Explorer			
Content Blocking						
Virtual Server		🕐 Are you	u sure you want to pause ? This	entry will not be effective.		
VPN						
-			OK Cancel			
PPTP Server						
PPTP Client						
.⇒Tunnel						



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 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.

Necessary Item		
Name	VPN_A	(Max. 12 characters)

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

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

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

Authentication Method	Preshare 💌
Preshared Key	123456789

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

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

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

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

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

Optional Item			
Perfect Forward Secrecy	GROUP 1	•	
ISAKMP Lifetime	3600	Seconds	
IPSec Lifetime	28800	Seconds	
Step 8. Select main mode as the algorithm.			

So Main mode ○ Aggressive mode

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



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

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

New Entry Tunnel		
Name	Site_A	(Max. 16 characters)
From Source	●LAN ● DMZ	
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0

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

respectively.

To Destination			
• To Destination Subnet / Mask	192.168.20.0	/ 255.255.255.0	
 Remote Client 			

Step 13. In IPSec / PPTP Setting, select VPN_A as the available tunnel.

|--|

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

Karan albua ID .	
Keep alive IP :	192.168.20.1

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

Step 16. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing

PLANET		
Vetworking & Communication	/ > Outgoing	
	odigonig	
■ System	Comment :	(Max, 32 characters)
■ Interface ■ Policy Object	Modify Policy	
E Policy	Source Address	Inside_Any 💌
L⇒ Outgoing	Destination Address	Outside_Any 🔽
_→ Incoming	Service	ANY
-+ WAN To DMZ	Schedule	None 🗸
→ LAN TO DMZ	Authentication User	None 🗸
	Tunnel	None 🗸
Mail Security	Action	None
■ IDP	Traffic Log	
🖻 Anomaly Flow IP	Statistics	
🎟 Monitor	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	O (Range: 1 - 99999, 0: means unlimited)
	QoS	None 💙

OK Cancel

Outgoing Policy:

and Incoming Policy.

Policy > Outgoin	ng					
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1 💌
Inside_Any	Outside_Any	ANY	1		Modify Remove Pause	то 2 💌

Incoming Policy:

Policy > Incomin	g					
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	то 1 💌

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

Step 1. Enter the default IP of Company B's 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.

Necessary Item		
Name	VPN_B	(Max. 12 characters)

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

To Destination	
 Remote Gateway Fixed IP or Domain Name 	61.11.11.11
Remote Gateway or Client Dynamic IP	

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

Authentication Method	Preshare 💌
Preshared Key	123456789

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

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

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

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

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

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

Step 8. Select main mode as the algorithm.

Mode	⊙ Main mode
------	-------------

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



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

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

New Entry Tunnel					
Name	Site_B	(Max. 16 characters)			
From Source	●LAN ● DMZ				
From Source Subnet / Mask	192.168.20.0	/ 255.255.255.0			

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

respectively. To Destination

 To Destination Subnet / Mask 	192.168.10.0	/ 255.255.255.0	
 Remote Client 			

Step 13. In IPSec / PPTP Setting, select VPN_B as the available tunnel.

	IPSec / PPTP Setting	VPN B 🗸
--	----------------------	---------

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

e IP : 192.168.10.1

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

 Policy Object > VPN > Tunnel

 i
 Name
 Source Subnet
 Destination Subnet
 IPSec / PPTP
 Configure

 Image: Imag

Step 16. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing

and Incoming Policy.

Outgoing Policy:

Policy ≻ Outgoir	ng					
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	то 1 💌
Inside_Any	Outside_Any	ANY	 Ø 		Modify Remove Pause	то 2 💌

Incoming Policy:

Policy > Incoming	g					
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	то 1 🔽

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

Preparation Task:

Company A External IP is 210.66.155.90, Internal IP is 192.168.10.X

Remote User External IP is 210.66.155.91

Remote user with an external IP wants to create a VPN connection with company A and connect to 192.168.10.100 for downloading the sharing file.

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

Configuration of CS-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.

Necessary Item			
Name		VPN_A	(Max. 12 characters)
Step 3. In to Destination table, choose	Remote Gateway o	r Client – Dyi	namic IP.
To Destination			
 Remote Gateway Fixed IP or Domain Name 			
• Remote Gateway or Client Dynamic IP			

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

Authentication Method	Preshare 💌
Preshared Key	123456789

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

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

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

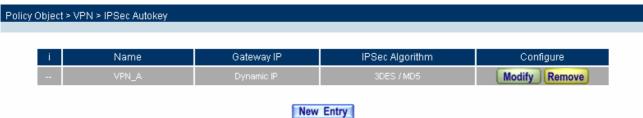
Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item				
Perfect Forward Secrecy	GROUP 2 💌			
ISAKMP Lifetime	3600 Seconds			
IPSec Lifetime	28800 Seconds			

Step 8. Select main mode as the algorithm.

Mode	● Main mode ● Aggressive mode
------	-------------------------------

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



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

Step 11. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP

subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Tunnel					
Name	Site_A	(Max. 16 characters)			
From Source	●LAN ● DMZ				
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0			

Step 12. In To Destination table, select Remote Client.

To Destination		
To Destination Subnet / Mask	7	
• Remote Client		

Step 13. In IPSec / PPTP Setting, select VPN_A as the available tunnel.

PSec / PPTP Setting	VPN_A 💌
---------------------	---------

Step 14. Click OK to finish the Tunnel setting of Company A.

Policy Object > VPN > Trunk

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
삍.	Site_A	192.168.10.0	Remote Client	VPN_A	Modify Remove Pause

Step 15. Enable Tunnel setting in Incoming Policy.

Modify Policy	
Source Address	Outside_Any 🔽
Destination Address	Inside_Any
Service	ANY
Schedule	None 💌
Tunnel	Site_B 💌
Action	None Site_B
Traffic Log	
Statistics	Enable
IDP	Enable
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
QoS	None 💌
NAT	Enable

Step 16. Click OK to finish the Policy setting of Company A.

Policy > Incoming	g					
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	То 1 💌

Configuration of WinXP

The IP of remote user is 210.66.155.91. The settings of remote user are as the following.

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



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

Run	? 🛛
Open:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
	OK Cancel Browse

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

🚡 Console1			
Action View Fa	avorites Window Help		
New	Ctrl+N		
Open	Ctrl+O		
<u>S</u> ave	Ctrl+S		
Save <u>A</u> s			
Add/Remove Snap-in Options	Ctrl+M	There are no items to show in this view.	
Sector of the se			
<u>1</u> C:\WINDOWS\system	32\devmgmt		
E <u>x</u> it			
Adds or removes individual	span-inc		
Hads of Temores Individual	andp ins.		

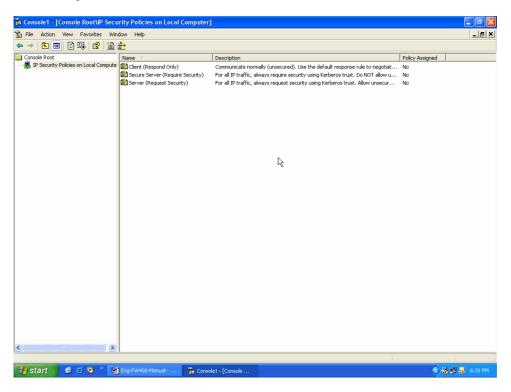
Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.

Add/Remove Snap-in	2 🗙		
Standalone Extensions	Add Standalone Snap-in		? 🔀
Use this page to add or remove a standalone Snap-in from the con			
Snap-ins added to: 🔄 Console Root	Group Policy Indexing Service Internet Information Services IP Security Monitor Link to Web Address Local Users and Groups Performance Logs and Alerts Removable Storage Management	Vendor Microsoft Corporation, I. Microsoft Corporation, I. Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
Description 1 Add Remove About	Description Internet Protocol Security (IPSec) Administra policies for secure communication with othe		se
ОК	Cancel		

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

Select Computer or Domain
Select which computer or domain this snap-in will manage When this console is saved the location will also be saved
 Local computer The computer this console is running on The Active Directory domain of which this computer is a member Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"): Another computer: Browse
K Back Finish Cancel

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.

🚡 Console1					
File Action View	Favorites Window	Help			
⇔ → 🖪 🗟	ß				
🚡 Console Root					
Console Root		Name			
IP Security Po		and filter actions 🗟	n Local Comp		
	All Tasks	•			
	New <u>W</u> indow from He	ere			
	Refresh				
	Help	ũ.			
<	8				
Create an IP Security p	policy				

Step 8. Click Next.



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

IP Security Policy Wizard	? 🛛
IP Security Policy Name Name this IP Security policy and provide a	a brief description
Name:	
IPSec	
Description:	
IPSec	
	< Back Next > Cancel

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

IP Security Policy Wizard 🔹 💽
Requests for Secure Communication Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
< Back Next > Cancel

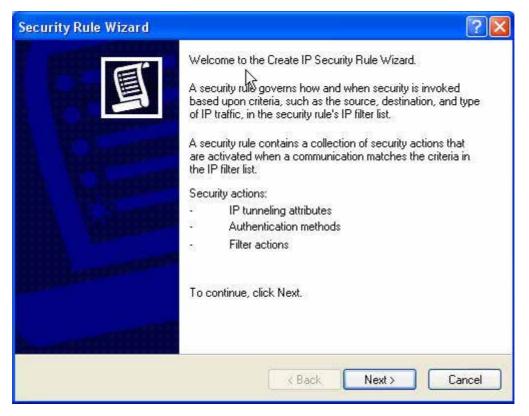


Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.

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

Security	rules for communicating with	other computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
Comparise	Default Response	Kerberos	. K.I.,
	Derauk nesponse	Keibeius	No
	Derauk mesponse	Keibeius	N

Step 13. Click next.



Step 14. Enter the WAN IP of Remote user, 210.66.155.91.

	ule Wiza	rd						
Tunnel E	Indpoint							E
	unnel endp ecified by t					the IP traffic	destination,	
					a public or pr between two		work with the	
Spec	ify the tunn	el endpo	oint for the	IP Secu	ity rule:			
C T	his rule doe	s not sp	ecify a tur	inel				
10 1	ne tunnel e	napoint	is specified	a by this	IP address:			
1	210 .	66	. 155	. 91				
						STATE.		

Step 15. click all network connections.

Security Rule Wizard	? 🔀
Network Type The security rule must be applied to a network type.	Ĩ
Select the network type:	
All network connections	
C 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.

Security Rule Wizard	? 🛛
Authentication Method To add multiple authentication methods, edit the security rule after completi IP Security rule wizard.	ng the
Set the initial authentication method for this security rule: C Active Directory default (Kerberos V5 protocol) C Use a certificate from this certification authority (CA):	
	Browse
123456789	~
	*
< Back Next >	Cancel

Step 17. Click Add.

IP filter lists: Name Description Add O All ICMP Traffic Matches all ICMP packets bet Edit O All IP Traffic Matches all IP packets from t Edit) list matches your needs, click Add to create	a new one.
O All IP Traffic Matches all IP packets from t	0	Description	Add
	O All ICMP Traffic	NAMES AND ADDRESS NO. NO. NO.	
Remove	O All IP Traffic	Matches all IP packets from t	E dit
			Remove

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

Traffic-in				2000 and
Description	r			Add
				Edit
				Remove
Filters:			U 되	se Add Wizard
Mirrored	Description	Protocol	Source Port	Destinatio

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.

r Wizard ? Traffic Source Specify the source address	of the IP	' tra	ffic.					
Source address:								
A specific IP Subnet		_		_		-		
IP Address:	192		168		10	3	0	
Subnet mask:	255		255		255		0	
			Г	<	Back	ור	Next >	Cance

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

Filter Wizard	? 🔀
IP Traffic Destination Specify the destination address of the IP traf	ffic.
Destination address:	
My IP Address	•
	<pre></pre>

Step 22. Click next.

Filter Wizard	? 🛛
IP Protocol Type Select the IP protocol type. If this type is TCP or UDP source and destination ports.	', you will also specify the
Select a protocol type:	
< Ba	ck Next > Cancel

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



Step 24. Please don't enable Mirrored, and click OK.

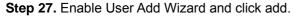
A specific IP Subnet			•	
IP Address:	192 .	168 .	10 .	0
Subnet mask:	255 .	255 .	255 .	0
Mirrored. Also match pag	kets with the	exact op	posite sourc	ce and
Mirrored. Also match par destination addresses.	:kets with the	exact op	posite sourc	ce and

Step 25. Click OK.

Name:				
Traffic-in			i)	
Description	n:		1	Add
				Edit
			~	Remove
Filters:			U 되	se Add Wizard
Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Step 26. Select Traffic-in and click next.

	g list matches your needs, click Add to create	anow one.
IP filter lists: Name	Description	Add
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	Edit
O Traffic-in		Remove



ecurity rule.	4
create a filter action using the wizard.	
	Add
Permit unsecured IP packets t Accepts unsecured communi	Edit
Accepts unsecured communi	Remove
< Back Nex	t> Cancel
	 Accepts unsecured communi Accepts unsecured communi

Step 28. Click next.



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

Filter Action Wizard	? 🛛
Filter Action Name Name this filter action and provide a brief description.	193
Name:	
Security	
Description:	
	~
	M
< Back Next >	Cancel

Step 30. Select Negotiate security and click next.

Filter Action	? 🔀
Filter Action General Options Set the filter action behavior.	100
C Permit	
C Block	
Negotiate security:	
	< Back Next > Cancel

Step 31. Click next.

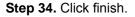
ilter Ac	tion Wizard 🔹 💽
Co	unicating with computers that do not support IPSec ommunicating with computers that do not support IPSec may expose your atwork to security risks.
Do	you want to allow communication with computers the do not support IPSec?
(•	Do not communicate with computers that do not support IPSec.
C	Fall back to unsecured communication.
	Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.
	< Back Next > Cancel

Step 32. Select Custom and click settings.

ter Action Wizard	?
IP Traffic Security Specify a security method for IP traffic. To add multiple security method filter action after completing the wizard.	ds, edit the
This filter action requires at least one security method for IP traffic.	
C Encryption and Integrity	
Data will be encrypted, authenticated, and unmodified.	
C Integrity only	
Data will be authentic and unmodified, but will not be encrypted.	
Custom Settings	
Kart Kart Kart Kart Kart Kart Kart Kart	> Cancel

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.

Custom Security Method Settin	es 🛛 🥐 🔀
Specify the settings for this custom sec Data and address integrity without Integrity algorithm:	
MD5 💽 Data integrity and encryption (ESP Integrity algorithm:):
MD5 Encryption algorithm:	
3DES	
Session key settings: Generate a new key every: 100000 Kbytes	Generate a new key every
	OK Cancel

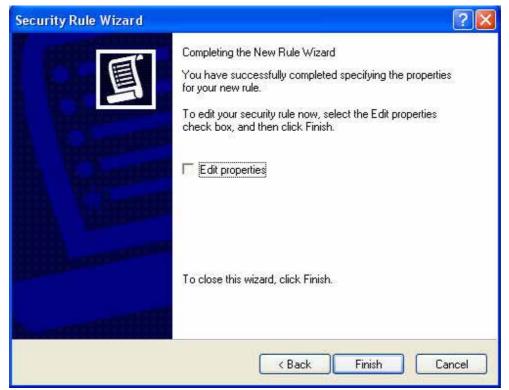




Step 35. Select security and click next.

curity Rule Wizard Filter Action Select the filter action for this secu	urity rule.	
If no filter actions in the following li one. Select Use Add Wizard to cre Filter Actions:	ist matches your needs, click Add to eate a filter action using the wizard.	o create a new Use Add Wizard
Name	Description	Add
O Permit O Request Security (Optional)	Permit unsecured IP packets t Accepts unsecured communi	Edit
Require Security Security	Accepts unsecured communi	Remove
	< Back Nex	t> Cancel

Step 36. Click finish.



Step 37. Click Add.

D.C		
P Security rules: IP Filter List	Filter Action	Authentication
☑ Traffic-in	Security	Preshared Key 21

Step 38. Click next.



Step 39. Enter the WAN IP of company A, 210.66.155.90.

Inel 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 specified by this IP address: 210 . 66 210 . 66	irity Rule Wi	/izard			?
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:		endpoint is the tunneling com		⁹ traffic destination,	
 This rule does not specify a tunnel The tunnel endpoint is specified by this IP address: 					
The tunnel endpoint is specified by this IP address:	Specify the tu	tunnel endpoint for the IP Se	curity rule:		
	C This rule o	e does not specify a tunnel			
210 . 66 . 155 . 90	The tunne	nel endpoint is specified by th	is IP address:		
	210	0 . 66 . 155 . 9	30		
	1				
<pre></pre>			(Pack	Nevt S (ancel

Step 40. Select All network connections and click next.

curity Rule Wizard	?
Network Type The security rule must be applied to a	a network type.
Select the network type: All network connections Local area network (LAN) Remote access	Ŗ
	< Back Next > Cancel

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

Security Rule Wizard	? 🛛
Authentication Method To add multiple authentication methods, edit the security rule after comp IP Security rule wizard.	oleting the
Set the initial authentication method for this security rule: C Active Directory default (Kerberos V5 protocol) C Use a certificate from this certification authority (CA):	
	Browse
 Use this string to protect the key exchange (preshared key): 123456789 	<u>×</u>
	×
< Back Next >	Cancel

Step 42. Click Add.

If no IP filter in the following	ng list matches your needs, click Add to create	a new one.
IP filter lists: Name	Description	Add
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	Edit
O Traffic-in		Remove

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

Vame: Traffic-out	pir.			
Description	r			Add
			1994	Edit
			~	Remove
Filters:			U 🟹	se Add Wizard
Mirrored	Description	Protocol	Source Port	Destination

Step 44. Click next



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

Filter Wizard	? 🔀
IP Traffic Source Specify the source address of the IP traffic.	E
Source address:	
My IP Address	×
(< Back Next > Cancel

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

Filter Wizard								? 🗙
IP Traffic Destination Specify the destination add	ress of th	ne IF	^o traffic	2				Ĩ
Destination address:								
A specific IP Subnet					-	•		
IP address:	192	•	168	14	10	34	0	
Subnet mask:	255	٠	255	82	255	3	0	
				<	Back		Next >	Cancel

Step 47. Click next.

Filter Wizard	? 🔀
IP Protocol Type Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.	T
Select a protocol type:	
< Back Next >	Cancel

Step 48. Please enable Edit properties and click finish.



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

ilter Properties				?
Addressing Protocol Descri	otion			
- Source address:				-
My IP Address			•	
I'm i manare				
- Destination address:				
A specific IP Subnet			-	
IP address:	192 . 1	68.	10 .	0
Subnet mask:	255 . 2	255 .	255 .	0
Mirrored. Also match pack	ata with the av	unch oper	anita anuna	
destination addresses.	ets with the ex	saci oppi	Jsite source	s anu
		3 <u></u>		
		1	ок 📘	Cancel

Step 50. Click ok.

Description:				Add
			<u>8</u>	Edit
			~	Remove
Filters:				Use Add Wizard
Mirrored [Description	Protocol	Source Port	Destinatio
No		ANY	ANY	ANY

Step 51. Select Traffic-out and click next.

	type of IP traffic to which this security rule a list matches your needs, click Add to create	E
IP filter lists: Name	Description	Add
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	Edit
O Traffic-in	Matches ain Plackets from t	Remove
O Traffic-out		

Step 52. Select Security and click edit.

Select the filter action for this secu	any rue.	
If no filter actions in the following li one. Select Use Add Wizard to cre	st matches your needs, click Add to eate a filter action using the wizard.	create a new
Filter Actions:	v	Use Add Wizard
Name	Description	Add
O Permit O Request Security (Optional)	Permit unsecured IP packets t Accepts unsecured communi	Edit
 Require Security Security 	Accepts unsecured communi	Remove

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

	ate security: ethod preference AH Integrity	order: ESP Confidential ES	Add
Custom	<none></none>	3DES ME	Edit
			Remove
			Move up
<			Move down
Γ Allow ι	insecured commu	nunication, but always respo inication with non-IPSec-awa vard secrecy (PFS)	and a second the second se

Step 54. Select Security and click next.

one. Select Use Add Wizard to cri	st matches your needs, click Add to eate a filter action using the wizard.	
Filter Actions:	Description	Use Add Wizard Add
O Permit O Request Security (Optional)	Permit unsecured IP packets t Accepts unsecured communi	Edit
O Require Security ⊙ Security	Accepts unsecured communi	Remove

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



Step 56. Click apply first and then click ok.

lules General		
Securit	y rules for communicating w	ith other computers
IP Security rules: IP Filter List	Filter Action	Authentication T
Traffic-out	Security	Preshared Key 21
🗹 Traffic-in	Security	Preshared Key 21
Oynamic>	Default Response	Kerberos Ni
<		
Add	Edit Remov	/e 🛛 🔽 Use Add Wizard

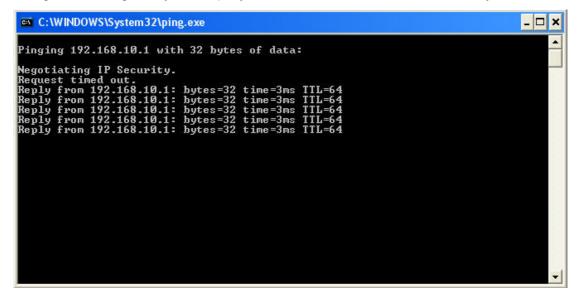
- 141 -

Download from Www.Somanuals.com. All Manuals Search And Download.

Console Root\IP Security Policie Console Root	Name 🛆	Description	Polic	y Assigned
晃 IP Security Policies on Local Compute		Communicate normally (uns	No	
	IPSec 🔛	IPSec	No	-N. e
		For all IP traffic, always req	No	Assign
	Server (Request Secu	For all IP traffic, always req	No	All Tas <u>k</u> s 🕨
				<u>D</u> elete
				Rena <u>m</u> e
				Properties
				Help
	<			>

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.

Necessary Item		
Name	VPN_A	(Max. 12 characters)

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

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

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

Authentication Method	Preshare 💌
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES 💌
AUTH Algorithm	SHA1 💌
Group	GROUP 2 💌
Mode	Main mode O Aggressive mode
My ID	@123
Peer ID	@abc

Download from Www.Somanuals.com. All Manuals Search And Download.

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

IPSec Algorithm	
 Data Encryption + Authentication 	
ENC Algorithm	3DES 💌
AUTH Algorithm	MD5 💙
 Authentication Only 	

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

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

Step 8. Click OK to finish the setting of Company A.



Step 9. Click Tunnel and press New Entry to configure the further setting.

Step 10. Enter Site_A as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.10.0 with subnet mask IP 255.255.255.0.

New Entry Tunnel				
Name	Site_A	(Max. 16 characters)		
From Source	●LAN ● DMZ			
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0		

Step 11. In To Destination table, fill company B's subnet IP and mask, 192.168.20.0 and 255.255.255.0

respectively.

To Destination					
• To Destination Subnet / Mask	192.168.20.0	/ 255.255.255.0			
Remote Client					

Step 12. In IPSec / PPTP Setting, select VPN_A as the available tunnel.

IPSec / PPTP Setting	VPN_A 💌
----------------------	---------

Step 13. Click OK to finish the Tunnel setting of Company A.

cy Object > Vi	PN > Tunnel				
i i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
믵.	Site_A	192.168.10.0	192.168.20.0	VPN_A	Modify Remove Pause
New Entry					

Step 14. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.

PLANET		
Vetworking & Communication	y ≻ Outgoing	
	y > Odigoling	
≖ System	Compart	(May 22 shavestave)
Therface	Comment : Modify Policy	(Max. 32 characters)
■ Policy Object ■ Policy	Source Address	Inside_Any 🗸
L⇒ Outgoing	Destination Address	Outside_Any 🗸
_⇒ Incoming	Service	ANY
-+ WAN To DMZ	Schedule	None 💙
-→ LAN To DMZ	Authentication User	
→ DMZ To WAN → DMZ To LAN	Tunnel	None 💌
■ Mail Security	Action	None
IDP	Traffic Log	
Anomaly Flow IP	Statistics	Enable
■ Monitor	IDP	Enable
	Content Blocking	
	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 💌

OK Cancel

Outgoing Policy:

Policy > Outgoing			

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	WPN		Modify Remove Pause	то 1 💌
Inside_Any	Outside_Any	ANY	 ✓ 		Modify Remove Pause	то 2 💌

Incoming Policy:

Policy > Incoming	g					
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	то 1 💌

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

Step 1. Enter the default IP of Company B's 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.

Necessary Item		
Name	VPN_B	(Max. 12 characters)

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

To Destination	
 Remote Gateway Fixed IP or Domain Name 	61.11.11.11
Remote Gateway or Client Dynamic IP	

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

Authentication Method	Preshare 💌
Preshared Key	123456789

Step 5. Enable Aggressive mode. For communication via VPN, the Content Security Gateway will force you to choose 3DES for ENC Algorithm, SHA-1 for AUTH Algorithm and select Group 2 to connect.

Local ID and Remote ID are optional parameters. If we choose to enter Local ID/ Remote ID, they couldn't be the same. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. If you want to use number or text, add @ in the front, for instance, @123 and @abc.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES 💌
AUTH Algorithm	SHA1 💌
Group	GROUP 2 💌

Mode	Main mode O Aggressive mode
My ID	@abc
Peer ID	@123

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

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

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

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

Step 8. Click OK to finish the setting of Company B.



Step 9. Click Tunnel and press New Entry to configure the further setting.

Step 10. Enter Site_B as the new tunnel name, and select LAN interface as the VPN source. Fill LAN IP subnet 192.168.20.0 with subnet mask IP 255.255.255.0.

New Entry Tunnel		
Name	Site_B	(Max. 16 characters)
From Source	오 LAN 🔍 DMZ	
From Source Subnet / Mask	192.168.20.0	/ 255.255.255.0

Step 11. In To Destination table, fill company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0

respectively.

To Destination			
• To Destination Subnet / Mask	192.168.10.0	/ 255.255.255.0	
Remote Client			

Step 12. In IPSec /PPTP Setting, select VPN_B tunnel as the available tunnel.

IDSec / DDTD Setting	

Step 13. Click OK to finish the Tunnel setting of Company B.

icy Object >	VPN > Tunnel				
i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
₽.	Site_B	192.168.20.0	192.168.10.0	VPN_B	Modify Remove Pause

Step 14. If you want to configure bi-direction VPN connection, you should enable Tunnel setting in Outgoing and Incoming Policy.

Outgoing Policy:

Policy > Outgoir	ng					
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	то 1 💌
Inside_Any	Outside_Any	ANY	6		Modify Remove Pause	то 2 💌

Incoming Policy:

Policy > Incoming	g					
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	Option	Modify Remove Pause	To 1 🔽

Example 4. Create a VPN connection between Content Security Gateway and PLANET VRT-311 VPN Router.

Preparation Task: Company A External IP is 210.66.155.90 Internal IP is 192.168.10.X Company B External IP is 210.66.155.92 Internal IP is 192.168.20.X To Allow Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for

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.

Necessary Item		
Name	cs	(Max. 12 characters)

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

To Destination	
 Remote Gateway Fixed IP or Domain Name 	210.66.155.92
Remote Gateway or Client Dynamic IP	

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

Authentication Method	Preshare 💌
Preshared Key	12345678

Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.

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

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

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

Step 7. Choose GROUP 2 as the Perfect Forward Secrecy setting, and leave the default setting with 28800 seconds in IPSec Lifetime and 3600 seconds for ISAKMP Lifetime.

Optional Item	
Perfect Forward Secrecy	GROUP 2 💌
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

Step 8. Select main mode as the algorithm.

	Mode	O Main mode O Aggressive mode
--	------	-------------------------------

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

Policy Object > \	/PN ≻ IPSec Autokey				
i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
	cs	WAN1	210.66.155.92	3DES / MD5	Modify Remove

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

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

New Entry Tunnel		
Name	CSVPN	(Max. 16 characters)
From Source	오 LAN 🕒 DMZ	
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0

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

To Destination			
• To Destination Subnet / Mask	192.168.20.0	/ 255.255.255.0	
Remote Client			

Step 13. In IPSec /PPTP Setting, select CS as the available tunnel.

IPSec / PPTP Setting	CS	Y							

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

Keep alive IP :	192.168.20.1	

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

Object ≻	VPN > Tunnel						
i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure		
₽.	CSVPN	192.168.10.0	192.168.20.0	cs	Modify Remove Pause		
New Entry							

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

Outgoing Policy:

Policy > Outgo	ing					
Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	то 1 💌
Inside_Any	Outside_Any	ANY	 Image: A set of the set of the		Modify Remove Pause	то 2 💌

Incoming Policy:

Policy > Incoming			

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

Step 2: Configure VRT-311 VPN policy as the following:

VPN Policy Defin	ition
Name: ^{MH}	Enable Policy
	Allow NetBIOS traffic
Remote VPN endpoint	⊙Dynamic IP
	• Fixed IP: 210, 66 , 155, 90
	O Domain Name:
Local IP addresses	
2.	IP address: 192,168,20,0 ~ 0
	Subnet Mask: 255, 255, 255, 0
Remote IP addresses	
Type: Subnet address 💌	IP address: 192,168,10,0~0
	Subnet Mask: 255, 255, 255, 0
Authentication & Encryp	tion
AH Authentication	MD5 🔽
■ESP Encryption	3DES 🔽 Key Size: 🗖 🔽 (AES only)
ESP Authentication	MD5 🔽
Manual Key Exchange	e
● IKE (Internet Key Exc	hange)
Direction	Both Directions 🗸
Local Identity Ty	De WAN IP Address
Local Identity Da	ta 210.66.155.92
Remote Identity	Type Remote WAN IP 🔽
Remote Identity I	Data 210.66.155.90
Authentication	○RSA Signature (requires certificate)
	Pre-shared Key
	Authentication Algorithm: MD5
Encryption:	3DES V Key Size: 🔊 V (AES only)
Exchange Mode	
IKE SA Life Time	e: 180 (secs)
🗹 IKE Keep Ali	ve Ping IP Address: 192.168.10.1
IPSec SA Life Ti	me: 300 (secs)
DH Group	Group 2 (1024 Bit)
IKE PFS	Group 2 (1024 Bit)
IPSec PFS	Group 2 (1024 Bit) 🐱

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.

	Policy ≻ Outgoir	ng					
🗷 System							
📧 Interface	Source	Destination	Service	Action	Option	Configure	Move
Policy Object	Inside_Any	Outside_Any	ANY	6		Modify Remove Pause	То 1 💌
E Policy							
→ Outgoing					New Entry		

The fields in the Outgoing window are:

- Source: Source network addresses that are specified in the LAN section of Address menu, or all the LAN network addresses.
- Destination: Destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- Service: Specify services provided by WAN network servers.
- Action: Control actions to permit or deny packets from LAN networks to WAN network travelling through the Content Security Gateway.
- Option: Specify the monitoring functions on packets from LAN networks to WAN networks travelling through the Content Security Gateway.
- **Configure:** Modify settings.
- Move: This sets the priority of the policies, number 1 being the highest priority.

Adding a new Outgoing Policy

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

and the second	Policy > Outgoing	
System	Comment :	(Max. 32 characters)
l Interface	Add New Policy	(Max. 32 characters)
Policy Object Policy	Source Address	Inside_Any 🗸
-⇒ Outgoing	Destination Address	Outside_Any V
_→ Incoming	Service	ANY
- ♦ WAN To DMZ	Schedule	None V
-♦ LAN To DMZ	Authentication User	None V
→ DMZ To WAN → DMZ To LAN	Tunnel	None V
Mail Security	Action	PERMIT V
IDP	 Traffic Log	
Anomaly Flow IP	- Statistics	Enable
Monitor	IDP	
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	 QoS	None V

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 net work servers. These are services/application that are allowed to pass from the LAN network to the WAN network. Choose ANY for all services.

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

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

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Select Enable to enable Content Blocking.

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

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

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

Modifying an Outgoing policy

Step 1: In the **Outgoing** policy section, locate the name of the policy desired to be modified and click its corresponding Modify option under the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

NOTE: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→ [Pre-defined], [Custom] or Group under **Service**).

Step 3: Click OK to do confirm modification or click Cancel to cancel it.

and the second secon	olicy > Outgoing	
Bystem	[
Interface	Comment :	(Max. 32 characters)
Policy Object	Modify Policy	
Policy	Source Address	Inside_Any V
Outgoing	Destination Address	Outside_Any 🚩
➡ Incoming	Service	ANY
♦ WAN To DMZ	Schedule	None 🗸
➡ LAN To DMZ	Authentication User	None 🗸
DMZ To WAN	Tunnel	None V
➡ DMZ To LAN	Action	PERMIT V
Mail Security		
IDP	Traffic Log	Enable
Anomaly Flow IP	Statistics	Enable
Monitor	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 🗸

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.

PLANET Retworking & Communication	Policy > Outgoing						
■ System	Source	Destination	Service	Action	Option	Configure	Move
Interface	Inside_Any	Outside_Any	ANY	- Ø		Modify Remove	To 1 💌
E Policy				New E	Intry		
- ⇒ Outgoing							
- ⇒ Incoming		Microsoft	Internet Exp	lorer	\mathbf{X}		
-⇒ WAN To DMZ							
-⇒LAN To DMZ		2	Are you sure yo	u want to remov	ve?		
-⇒DMZ To WAN		_					
→ DMZ To LAN			ок	Cancel			
■ Mail Security							

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.

	Policy > Incoming						
≢ System ≢ Interface	Source	Destination	Service	Action	Option	Configure	Move
Policy Object			E Ma	Entered			
■ Policy ■ Outgoing ■ Incoming			Ne	w Entry			

Step 2: The fields of the Incoming window are:

■ Source: Source networks which are specified in the WAN section of the Address menu, or all the WAN network addresses.

■ **Destination:** Destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.

■ Service: Services supported by Virtual Servers (or Mapped IP).

■ Action: Control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.

■ **Option:** Specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Content Security Gateway.

- **Configure:** Modify settings or remove incoming policy.
- Move: This sets the sequence of the policies, number 1 being the first policy to proceed.

Adding an Incoming Policy

Step 1: Under Incoming of the Policy menu, click the New Entry button.

PLANET		
Vetworking & Communication		
Policy	> Incoming	
🗷 System	0tu	
■ Interface	Comment : Add New Policy	(Max. 32 characters)
■ Policy Object ■ Policy	Source Address	Outside_Any 💙
L→ Outgoing	Destination Address	Inside_Any
_+ Incoming	Service	ANY
-++ WAN To DMZ	Schedule	None 🗸
-→ LAN To DMZ	Tunnel	None 💙
	Action	PERMIT V
■ Mail Security	Traffic Log	Enable
 ■ IDP	Statistics	Enable
🗖 Anomaly Flow IP	IDP	Enable
■ Monitor	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 👻
	NAT	

Step 2: Configure the parameters

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the WAN section of the Address menu. To create a new source address, please go to the LAN section under the Address menu.

Destination Address: Select names of the LAN networks from the drop down list. The drop down list contains the names of IP mapping addresses specified in the **Mapped IP** or the **Virtual Server** sections of **Virtual Server** menu. To create a new destination address, please go to the **Virtual Server** menu.

Service: Specified services provided by LAN network servers. These are services / application that are allowed to pass from the network to the LAN network. Choose ANY for all services.

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

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling between the specified WAN network and Virtual Server/Mapped IP.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

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

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

NAT: Select enable to replace Internet user's IP address with LAN interface IP, in order to allow Internet user to access LAN resource if the LAN server only allows to be accessed with the same IP subnet.

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.

PLANET		
Vetworking & Communication	Policy > Incoming	
	Fondy Amonimig	
System		
Interface	Comment :	(Max. 32 characters)
Policy Object	Modify Policy	
Policy	Source Address	Outside_Any 💌
- ♦ Outgoing	Destination Address	Inside_Any 💌
Incoming	Service	ANY
-♦ WAN To DMZ	Schedule	None 🗸
➡ LAN To DMZ	Tunnel	None 🗸
-⇒ DMZ To WAN		
-+ DMZ To LAN	Action	PERMIT
Mail Security	Traffic Log	Enable
IDP	Statistics	Enable
Anomaly Flow IP	IDP	Enable
Monitor	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 🗸
	NAT	

Removing an Incoming Policy

Step 1: In the **Incoming** window, locate the name of policy desired to be removed and click its corresponding **[Remove]** in the Configure field.

Step 2: In the Remove confirmation window, click Ok to remove the policy or click Cancel to cancel removing.

	Policy > Incoming						
■ System	Source	Destination	Service	Action	Option	Configure	Move
■ Interface ■ Policy Object	Outside_Any	Inside_Any(Routing)	ANY	- Ø		Modify Remove	То 1 💌
 Policy Outgoing Incoming WAN To DMZ LAN To DMZ DMZ To WAN DMZ To LAN Mail Security 		Microsoft Interne		remove ?			

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. Before to set up **WAN To DMZ** rule, you need to create **Virtual Server** or **Mapped IP** first.

	Policy > WAN To D	MZ					
■ System	Source	Destination	Service	Action	Option	Configure	Move
Interface		Please	specify the M	apped IP or	Virtual Serv	er	
🗉 Policy Object							
🗏 Policy							
-⇒ Outgoing							
-⇒ Incoming							
-⇒WAN To DMZ							
-⇒LAN To DMZ							
-⇒ DMZ To WAN							
→ DMZ To LAN							

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.

PLANET Networking & Communication		
	Policy > WAN To DMZ	
System		
Interface	Comment :	(Max. 32 characters)
Policy Object	Add New Policy	
Policy	Source Address	Outside_Any 🔽
Outgoing	Destination Address	DMZ_Any
Incoming	Service	ANY
♦ WAN To DMZ	Schedule	None V
➡ LAN To DMZ	Tunnel	None V
DMZ To WAN		
DMZ To LAN	Action	PERMIT
Mail Security	Traffic Log	Enable
IDP	Statistics	Enable
Anomaly Flow IP	IDP	Enable
Monitor	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 👻
	NAT	

Step 2: Configure the parameters.

Source Address: Select names of the WAN networks from the drop down list. The drop down list contains the names of all WAN networks defined in the **WAN** section of the **Address** menu. To create a new source address, please go to the **LAN** section under the **Address** menu.

Destination Address: Select the name of the DMZ network from the drop down list. The drop down list contains the names of the DMZ network created in the **Address** menu. It will also contain Mapped IP addresses from the **Virtual Server** menu that were created for the DMZ network. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to the sections entitled **Address** and **Virtual Server** for details)

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the WAN network to the DMZ network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu. (Please refer to the section entitled **Services** for details)

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

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified WAN network to the DMZ network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

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

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

NAT: Select enable to replace Internet user's IP address with DMZ interface IP, in order to allow Internet user to access DMZ resource if the DMZ server only allows to be accessed with the same IP subnet.

Step 3: Click OK.

Modifying a WAN To DMZ policy:

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

Step 2: In the Modify Policy window, fill in new settings.

Step 3: Click OK to do save modifications.

	Policy > WAN To DMZ	
■ System		
	Comment :	(Max. 32 characters)
■ Interface	Modify Policy	
Policy Object		
E Policy	Source Address	Outside_Any 🔽
→ Outgoing	Destination Address	DMZ_Any 💌
→ Incoming	Service	ANY
→ WAN To DMZ	Schedule	None 🗸
-→ LAN To DMZ		
→ DMZ To WAN	Tunnel	None 💌
L⇒ DMZ To LAN	Action	PERMIT 🔽
📧 Mail Security	Traffic Log	Enable
IDP	Statistics	Enable
🗉 Anomaly Flow IP	IDP	Enable
🗷 Monitor	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 🗸
	NAT	

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.

	Policy > WAN To D	MZ					
≖ System	Source	Destination	Service	Action	Option	Configure	Move
■ Interface	Outside_Any	Mapped IP(210.66.155.91)	ANY	- Ø		Modify Remove	То 1 🔽
≖ Policy Object							
 Policy •• Outgoing •• Incoming •• Incoming •• UAN To DMZ •• LAN To DMZ •• DMZ To WAN •• DMZ To LAN 		Microsoft Internet Ex Are you sure y OK	plorer	Entry ove ?			

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.

	Policy > DMZ To W	AN					
 System Interface Policy Object Policy Outgoing Incoming MAN To DMZ DMZ To WAN DMZ To LAN Mail Security 	Source	Destination	Service	Action ew Entry	Option	Configure	Move

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.

PLANET		
Wetworking & Communication		
Pol	icy ≻ DMZ To WAN	
🗷 System		
📧 Interface	Comment :	(Max. 32 characters)
📕 Policy Object	Add New Policy	
■ Policy	Source Address	DMZ_Any 💌
-⇒ Outgoing	Destination Address	Outside_Any 💌
_⇒ Incoming	Service	ANY 🔽
-+ WAN To DMZ	Schedule	None 👻
-→ LAN To DMZ	Authentication User	None 🔽
→ DMZ To WAN → DMZ To LAN	Tunnel	None 🔽
Mail Security	Action	PERMIT 🔽
E IDP	Traffic Log	
🗷 Anomaly Flow IP	Statistics	Enable
📧 Monitor	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 💌

Step 2: Configure the parameters.

Source Address: Select the name of the DMZ network from the drop down list. The drop down list will contain names of DMZ networks defined in **DMZ** section of the **Address** menu. To add a new source address, please go to the **DMZ** section under the **Address** menu.

Destination Address: Select the name of the WAN network from the drop down list. The drop down list lists names of addresses defined in **WAN** section of the **Address** menu. To add a new destination address, please go to **WAN** section of the **Address** menu.

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the DMZ network to the WAN network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu.

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

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

Tunnel: Select the specific VPN tunnel to enable the VPN traffic in Policy rule.

Action: Select Permit or Deny ALL from the drop down list to allow or reject the packets travelling from the specified DMZ network to the WAN network.

Traffic Log: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

IDP: Check to enable IDP feature.

Content Blocking: Select Enable to enable Content Blocking.

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

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

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

Modifying a DMZ To WAN policy:

- **Step 1:** In the DMZ To WAN window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.
- Step 2: In the Modify Policy window, fill in new settings.

NOTE: To change or add selections in the drop-down list, go to the section where the selections are setup. (Source Address \rightarrow DMZ of Address; Destination Address \rightarrow WAN, Service \rightarrow Pre-defined Service, Custom or Group under Service.)

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

Po	licy > DMZ To WAN	
■ System		
Interface	Comment :	(Max. 32 characters)
Policy Object	Modify Policy	
Policy	Source Address	DMZ_Any 💌
-→ Outgoing	Destination Address	Outside_Any 💙
_♦ Incoming	Service	ANY 🔽
→ WAN To DMZ	Schedule	None V
-⇒ LAN To DMZ	Authentication User	None V
→ DMZ To WAN		None V
-⇒ DMZ To LAN		
Mail Security	Action	PERMIT
IDP	Traffic Log	Enable
Anomaly Flow IP	Statistics	Enable
Monitor	IDP	Enable
	Content Blocking	
	MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
	QoS	None 💌

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.

	Policy > DMZ To	WAN					
≖ Sy stem	Source	Destination	Service	Action	Option	Configure	Move
Interface	DMZ_Any	Outside_Any	ANY	- Ø		Modify Remove	То 1 🛩
					Entry		
-⇒Incoming -⇒WAN To DMZ -⇒LAN To DMZ			ft Internet Ex Are you sure y		iove ?		
→ DMZ To WAN → DMZ To LAN		C	ок	Cancel			

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

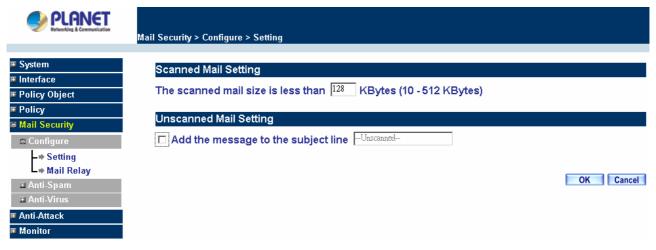
About the Mail Security Configure function, it means the dealing standard towards mail of CS-500. In this chapter, it is defined as Setting and Mail Relay.

Setting:

Define the required fields of setting:

Scanned Mail Setting: 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".



🤤 Inbox - Outlook Express				<u>_18 ×</u>
Pile Edit View Tools Messa 	soe Help 92	Sendificerv Addresses Find		
🖘 Inbox				
Folders ×	1 8 7 From	Sana	Received	
Cutlook Express Coal Folders Coal Folders Coal Folders Coal Folders Coal Folders Coal Folders Coal Sent Rems C	<u>M</u> Mr Hecksthorne	Unscanned Yragmet	9/16/2004 7:29 AM	
Contacts • X There are no contacts to display. Click on Contacts to create a new contact.				
1 message(s), 0 unvead	<u>]</u>		📕 Working Online	

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:

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

Mail Relay setting is complete. The external mails send to planet.com.tw that will be received by CS-500 and redirect to the mail server after filtering.

PLANET Retworking & Communication	Mail Security > Configure > Mail Relay		
≢ System ≢ Interface ≢ Policy Object		e of Internal Mail Serve mal IP of Mail Relay	ər
■ Policy ■ Mail Security	Modify Domain Name		
S Mail Security S Configure	Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
L⇒ Setting	IP Address of Mail Server	61.11.11.12	(ex: 61.217.22.30)
-⇒ Mail Relay			
≖ Anti-Spam			OK Cancel
. I Anti-Virus IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			
Anti-Attack			
🗷 Monitor			

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:

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

IP Address of Mail Server 172.16.1.13 (ex: 61.217.22.30) ■ Anti-Spam ■ Anti-Virus ■ Anti-Attack	figure > Mail Relay	RELAKET Retworking & Communication		
Security Modify Domain Name □ Configure Domain Name of Mail Server planet.com.tw (ex: mail.my_domain.cc L → Setting IP Address of Mail Server 172.16.1.13 (ex: 61.217.22.30) □ Anti-Spam OK Ca ▼ Anti-Attack Image: Calify Comment of Mail Server Image: Calify Calify Comment of Mail Server		■ Interface ■ Policy Object		r
Configure Domain Name of Mail Server planet.com.tw (ex: mail.my_domain.c Planet.orm.tw (ex: 61.217.22.30) PAddress of Mail Server 172.16.1.13 (ex: 61.217.22.30) OK Ca Anti-Virus Anti-Attack	/ Domain Name	-		
IP Address of Mail Server 172.16.1.13 (ex: 61.217.22.30)	in Name of Mail Server		planet.com.tw	(ex: mail.my_domain.com)
Mail Relay Anti-Spam OK Ca Anti-Virus Anti-Attack	ress of Mail Server		172.16.1.13	(ex: 61.217.22.30)
		→ Mail Relay		
■ Anti-Attack		∎ Anti-Spam		OK Cancel
		≖ Anti-Virus		
		🗉 Anti-Attack		
* Monitor		🗉 Monitor		

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

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

PLANET Retworking & Communication	Mail Security > Configure > Mail Relay		
■ System ■ Interface ■ Policy Object		ain Name of Internal Mail Server ved External IP of Mail Relay	
 ■ Policy ■ Mail Security ■ Configure > Setting -> Mail Relay 	Modify IP Address IP Address Netmask	61.11.11.11 255.255.255.255	(ex: 202.24.193.138) (ex: 255.255.255.248)
			OK Cancel

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:

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

ρ	1			C	г
-	u	1	N	5	

to.

System	O Domain Name	e of Internal Mail Serve	er
Interface		nal IP of Mail Relay	51
Policy Object	 Allowed Extern 	nam ormanicolay	
Policy	Modify Domain Name		
Mail Security			
🖻 Configure	Domain Name of Mail Server	planet.com.tw	(ex: mail.my_domain.com)
→ Setting	IP Address of Mail Server	61.11.11.12	(ex: 61.217.22.30)
L⇒ Mail Relay			
± Anti-Spam			OK Cancel
+ Anti-Virus			

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

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

	Security > Configure > Mail Relay		
System Interface Policy Object		ain Name of Internal Mail Server ved External IP of Mail Relay	
Policy	Modify IP Address		
Mail Security S Configure	IP Address	211.22.22.22	(ex: 202.24.193.138)
→ Setting	Netmask	255.255.255.255	(ex: 255.255.255.248)
L⇒ Mail Relay			
≝ Anti-Spam			OK Cancel
∃ Anti-Virus			
Anti-Attack			
Monitor			

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.

Wetworking & Communication	
	Mail Security > Anti-Spam > Setting
🗷 System	
🗉 Interface	Spam Setting
Policy Object	Enable Anti-Spam
Policy	The Mail Server is placed in Internal (LAN or DMZ) (Please set Mail Relay first)
■ Mail Security	🗹 External (WAN)
I Configure	The threshold score of spam mail is 🛛 5 💌
⊒ Anti-Spam	Add the message to the subject linespam (Max. 256 characters)
L⇒ Setting	Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) Test
→ Rule	Enable Bayesian filtering (Bayesian filtering works until database has at least 200 spams and 200 hams)
-→ Whitelist	
-→ Blacklist	Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) Test
-→ Training	Add score tag to the subject line
L⇒ Spam Mail	
I Anti-Virus	Action of Spam Mail
	Internal Mail Server:
IDP	Delete the spam mail
Anomaly Flow IP	Deliver to the recipient
🎟 Monitor	Forward to : (Max. 128 characters, ex: user@mydomain.com)
	External Mail Server:
	Deliver to the recipient (Always enable)
	OK Cancel

Definition:

Enable Anti-Spam: Select to enable Anti-Spam function.

The Mail Server is placed in Internal (LAN or DMZ) or External (WAN): Select to choose the location of the mail server.

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.

Check sender account: Select to allow CS-500 checking sender's account when it receives the mail, if the sender's account is faked, CS-500 will treat the mail as the spam.

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

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

Action of Spam Mail: When CS-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.

	Mail Security > Anti	-Spam > Rule				
≡ System	Rule Name	Classification	Action	Comments	Configure	Move
■ Interface ■ Policy Object						
E Policy			New Entry	y		
⊫ Mail Security						
≖ Configure						
⊟ Anti-Spam						
→ Setting						
–⇒ Rule						
– ⇒ Whitelist						
–⇒ Blacklist						
- ⇒ Training						
-⇒ Spam Mail						

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.

PLANET Networking & Communication	Mail Security > Anti-Spar	n > Rule		
	Rule Name : PLanet Combination : And Action : Delete spam	~	Comments : Classification : Spam Auto-Training : Enable v	✓
⊫ Mail Security	ltem	Condition	Pattern	Configure
≖ Configure	Received 🔽	Contains 🔽 🗸	support@planet.com.tw	Remove
⊑ Anti-Spam	From 🔽	Contains 🔽 🗸	test@test.com	Next Row Remove
– ⇒ Setting				
–⇒ Rule				OK Cancel
– ⇒ Whitelist				
–♦ Blacklist				
-→ Training				
→ Spam Mail				

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.

PLANET Retworking & Communication	Mail Security > Anti	-Spam > Rule			
≖ Sy stem	Rule Name	Classification	Action	Comments	Configure Move
■ Interface ■ Policy Object	PLanet	Spam	Delete spam mail		Modify Remove To 1 v
■ Policy					
■ Mail Security		Microsoft	New Ent		
⊑ Anti-Spam			Are you sure you want to remove		
–⇒ Setting –⇒ Rule		~			
– ⇒ Whitelist – ⇒ Blacklist			OK Cancel		
-⇒ Training L⇒ Spam Mail					

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.

PLANET Retworking & Communication	Mail Security > Anti-Spam > Whi	telist		
≖ System ≖ Interface	Direction	Whitelist	Auto-Training	Configure
Policy Object Policy			New Entry	
≡ Mail Security				
–⇒ Setting –⇒ Rule				
– ⇒ Whitelist – ⇒ Blacklist				
-⇒Training -⇒Spam Mail				

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.

PLANET Networking & Communication	Mail Security	y > Anti-Spam > Whitelist		
stem		Modify Whitelist		
terface		Whitelist	planet	(ex: *yahoo*, *: wildcard)
olicy Object		Direction	From 💌	
olicy ail Security		Auto-Training	Enable 🔽	
Configure				OK Car

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.

PLANET Retworking & Communication	Mail Security > Anti-Spam > \	Whitelist		
≖ System ≖ Interface	Direction	Whitelist	Auto-Training	Configur
■ Interface ■ Policy Object ■ Policy	From	planet	Ø	Modify
l≡ Mail Security			New Entry	
■ Configure ■ Anti-Spam → Setting		Microsoft Internet E	xplorer X	
–⇒ Rule –⇒ Whitelist		OK (Cancel	
–⇒ Blacklist –⇒ Training				
഻ ♦ Spam Mail				

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.

		18.4		
	Mail Security > Anti-Spam > Bla	icklist		
i System	Direction	Blacklist	Auto-Training	Configur
Interface				
Policy Object			New Entry	
i Policy				
Mail Security				
≖ Configure				
⊟ Anti-Spam				
–⇒ Setting				
–⇒ Rule				
– ⇒ Whitelist				
– ➡ Blacklist				
-⇒ Training				
-⇒ Spam Mail				

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.

PLANET			
Retworking & Communication	Mail Security > Anti-Spam > Blacklist		
= Curtore			
■ System	Modify Blacklist		
Interface	Blacklist	hacker	(ex: *yahoo*, *: wildcard)
Policy Object	Direction	From 🗸	
🗉 Policy	Auto-Training	Enable 🔽	
⊜ Mail Security			
≖ Configure			OK Cancel
⊟ Anti-Spam			
→ Setting			
− ⇒ Rule			
– ♦ Whitelist			
– ➡ Blacklist			
- ⇒ Training			
→ Spam Mail			

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.

PLANET Retworking & Communication	Mail Security > Anti-Spam > E	3lacklist		
System	Direction	Blacklist	Auto-Training	Configure
■ Interface	From	hacker	9	Modify Remove
Policy Object				
■ Policy			New Entry	
≡ Mail Security				
≖ Configure		Microsoft Internet Ex	plorer 🛛 🔀	
⊑ Anti-Spam				
– ⇒ Setting		🔹 Are you sure y	ou want to remove ?	
–⇒ Rule				
– ⇒ Whitelist		ОК	Cancel	
– ⇒ Blacklist				
-⇒ Training				
📥 Spam Mail				

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.

PLANET Retworking & Communication		
	Mail Security > Anti-Spam > Training	
System	Training Database	
Interface	Export Training Database	Download
Policy Object	Import Training Database	Browse
Policy		
fail Security	Spam Mail for Training (Free space for	r training: 876 KBytes)
± Configure	Import Spam Mail from Client	Browse
⊑ Anti-Spam		
-⇒ Setting	Ham Mail for Training (Free space for t	
–⇒ Rule	Import Ham Mail from Client	Browse
– ⇒ Whitelist	0	
– ➡ Blacklist	Spam Account for Training (Free spac	
→ Training	POP3 Server	(ex: my_domain.com)
∟⇒ Spam Mail	User name	(ex: spam)
± Anti-Virus	Password	(ex: 5d2#k)
Anti-Attack	Account test	Account Test
Monitor	Ham Account for Training (Free space	for training: 876 KBytes)
	POP3 Server	(ex: my_domain.com)
	User name	(ex: ham)
	Password	· · ·
	Account test	(ex: 5d2#k)
	Accountiest	Account rest
	Training time	
	System training starts at 🛛 00:00 💙 / day	y
	Training immediately : Training NOW	
		ОК С

Example: How to train mail into CS-500

STEP 1 . Create a new folder SpamMail in Outlook Express:

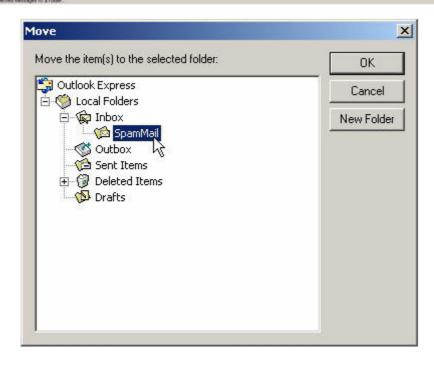
- Press the right key of the mouse and select **New Folder**.
- In **Create Folder** WebUI and enter the Folder's Name as SpamMail, and then click on OK.

Image: Second	E.N. New Tools Pla	tickage Mills				
Image:		AL FORMAT PORT DAMA	Sendifiers Addresses	£ -		
Image: Second and Second						
#### State ### contact Folder name: OK Folder name: OK SpamMail Cancel Select the folder in which to create the new folder: Cancel Select the folder in which to create the new folder: Select folders Soutbook Soutbook Soutbok Soutbook <	South Copen Count Prod. South Prod. South Prod. South Prod. South Prod.		ns [becore : 3] —opano-	– Tind out if Lavonne L	9/17/2004 18:25 AH	
Folder name: OK SpamMail Cancel Select the folder in which to create the new folder: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Select the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel Image: Cancel the folder in which to create the new folder: Image: Cancel	are no contacts to diplay. O	Dia .				
SpamMail Cancel Select the folder in which to create the new folder: Cancel Cancel Cancel Cancel Cancel Concel Con	A				F	×
Select the folder in which to create the new folder:	1					1
Cutlook Express Cutlook Express Local Folders Cutloox	15		to create the new	folder:	Cancel	
Drafts	÷-€	 Local Folders Inbox Outbox Sent Items Oeleted Item 	ns			

STEP 2 . In Inbox-Outlook Express, move spam mail to SpamMail Folder:

- In Inbox, select all of the spam mails that do not judge correctly and press the right key of the mouse and move to the folder.
- In Move WebUI, select SpamMail Folder and click OK.

Dabos - Outlook Express				26 2
File Edit view Jusis Plessa	or 146			
10. 2. 2.	V S X	a. u p.		
New Mall Rest/ Party All	Forward Print Delete 1	end/Recy Addresses Find		
·• Inbox				
	1 1 7 Prom	Stat	Received	
© Oxford Expresi ⇒ © Local Fielders ⇒ Discol Fielders ⇒ Discol Fielders ⇒ Oxford ⇒ Defected Interns (121) → © Sauettal → Sauettal ⇒ Franttal ⇒ Spanital	Cachery Lane Vito Galvan Vito Vito Galvan Vito Galvan	Open	fires 9/16/7004 1:30 AM 9/17/2004 5:01 PM 9/17/2004 6:49 PM elses 9/15/2004 11:50 PM	
Contacts • X There are no contacts to deplay. Clob un Contacts to oreale a new contact.		A A Frence In Adverse Text.		



- STEP 3 . Compress the SpamMail Folder in **Outlook Express** to shorten the data and upload to CS-500 for training:
 - Select SpamMail Folder
 - Select **Compact** function in selection of the folder

Spanetal - Outlook Express File Edit view Tools Piesia	× 148		
D . 2. 9.	12 2 Celete Send	3. B 과 . Sterv Abbenen Fred	
SpamMall			
slavs X	1 8 Y has	Sdad -	Received
Outlink Express	Rosetta Stubbe	—spam— Vällum for less	9/29/2004 2:55 PM
Control Folders	ProductTestPaneLcom	-spam This 6.3 Megapixel Canon Dig Cam could yourst	9/20/2004 9:06 AM
Cutter:	∅ I sender#mydomain.r ! I Penny Sherman	—spam— Spam Mail Notice. (0 Spam Mails) —spam— Sobs Need software? Click here.	9/28/2004 8:82 AM 9/28/2004 8:43 AM
CD Handlad	Shelley Lundy	-spam- Paying too much for your Insurance??	9/29/2004 2:31 FM
Sparrollad (14)	Sel Rubin Corbin	sport Online ordering is the groatest	9/20/2004 2:11 PM
Ca Sent Dome 13	Sonja Hathamay	-span-new info - span- Multiple ways to get home loans	9/20/2004 12:22 PM
- Deleted Rems (200)	Wunderful Daily Sevin	-spam - Hutger ways to get herse toars -spam - Hya	9/20/2004 10:56 AM 9/20/2004 9:30 AM
(C) Vinus	Rose Clement	-spam- 10 there	9/20/2004 1117 PM
	Me cest Laptop	-spam- Fiel out how to get a free 1814 Thickpadi	9/29/2004 2:36 PM
	EDX One		9/20/2004 12:27 PM 9/17/2004 7:23 PM
	Bob Allen	-span Right nut of the TV studio audience	9/29/2004 2:33 PM
	🔛 alexa ramirez	RE: You can become a legally ordained minister	9/20/2004 9:06 AM
	2010-00-00-004		
Ortats • X			
JiRayeath			
Baender@mydoman.com			
		- 1881 - <u>-</u>	
Smesage(s), 14 unread		📕 Working	Draine 🔥 Error
		🖉 Working	
SpanMad - Datlook Express		🖉 Working	Dakes
Spanvfall - Oxfook Express File: Edit: new Tools Pilota		🖉 Working	
SpannMail - Cuthook Express File: Edit View Tools Platta Tame	• a a × 3	3.9.2.	
B Sparrichail - Dathook Engress File: Edit View Tools Pleasa New	• a a × 3	및 working 33 - 교급 관 - Jähens Prid	
SpannMail - Cuthook Express File: Edit View Tools Platta Tame	• a a × 3	3.9.2.	
Separativitad - Challonde Engresse Pile E.M. New Toxis Pileses New Second	· · · · · · · · · · · · · · · · · · ·	경 · 교 후 ·	
StpansMad - Dotlook Express File Edit New Tools Mono New Comp Context Surve Automatics Surve Manamatics Surve Manamatics	* 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	성 · 실 · · Sher · Address Prod ·	
Strandfall - Dottook Express File Edit New Tools Mono New Common Common State State Managements State Statements Experiments	* 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	경 · 교 후 ·	
Spannen in Ducksik Engenen File f.d. New Took Moote New Common Common Service Common Common Service Common Common Service Common Problem	P P	성 · 실 · · Sher · Address Prod ·	
StpanoMad - Doblook Express Pile Edit New Tools Meso New Tools Communication Communication Communication Communication Communication Petitien	* 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	성 · 실 · · Sher · Address Prod ·	
Stramonial - Dublick Engineers File Edit New Tools Photo New Control Control Control Control Control Control Control Control Control Control	Prom Draft Send Prom ColeStativeE Non Non Delate	성 · 실 · · Sher · Address Prod ·	
StgannMad - Ovellook Express Pile Edit were took Penas Nere Services Servic	Property Control Service P	성 · 실 · · Sher · Address Prod ·	
Spannfall - Dutliek Engress File fall New Took Mesta New Control Control Control Control Control Control Fielder Engent	Prom Draft Send Prom ColeStativeE Non Non Delate	성 · 실 · · Sher · Address Prod ·	
Steamstad - Doctook Express File Edit New York Meson New Control Control Service Statements Export Export Export Export Export South Menthysis Menther	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Steamstad - Doctook Express File Edit New York Missis New Cool Cool Cool Cool Cool Cool Cool Cool	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Pie Edit www. South Petros Pie Edit www. South Petros Werk Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Con	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Stoarthad - Dotlook Everes File Edit New Yook Person New Comments	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Pie Edit wen turb Person Pie Edit wen turb Person Nen Com Com Com Com Com Com Com Com Com Com Com Com Com Com Com Com Com Com Com	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Stoarthad - Dotlook Everes File Edit New Yook Person New Comments	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Stoarthad - Dotlook Everes File Edit New Yook Person New Comments	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
StpannMad - Oxford Express Pile Edit New Social Petros New Communications Communi	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Stoarthad - Dotlook Everes File Edit New Yook Person New Comments	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Stoarthad - Dotlook Everes File Edit New Yook Person New Comments	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Statemental - Declarisk Experients File Edit New Toolo Petroso New Communication Communicatio	Pres Drive Send P	성 · 실 · · Sher · Address Prod ·	
Statemental - Declarisk Experients File Edit New Toolo Petroso New Communication Communicatio	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
New Color Colors	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Pierre Sud Alexandria Pierre Sud Reserved Server Sud Reserved Server Sud Reserved Server Sud Reserved Server Sud Reserved Server Sud Reserved Server Sud Statements Server Sud	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Stoamblad - Dotlink Express File Ed. Inen Tool Photo New Communication Communi	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Statements - Decision Experiences File Edit New York Petroson New Communications Communicat	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Pie Collection Express Pie Collection Tools Press Pier Statements Correction Collection Pier Statements Correction Collection Pier Statements Constant Collection Pier Statements Pier S	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Statements - Decision Experiences File Edit New York Petroson New Communications Communicat	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Stoamblad - Dotlink Express File Ed. Inen Tool Photo New Communication Communi	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Stoamblad - Dotlink Express File Ed. Inen Tool Photo New Communication Communi	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Stoamblad - Dotlink Express File Ed. Inen Sould Prints Nen Communication Service Statements Service S	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
SiganoMad - Oxforde Express Pile Ed. Intern Tool Petros Form Communication Communicati	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Signamblad - Oxforde Express File Edit were hold Petrick File Edit were hold Petrick File Experiments Generationsen Begent Expert Switch Identity Identities Switch Identity Identities File Edit Work Office Exit Petrick (Identity Exit Petrick (Identity) Exit	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	
Spannblad - Cortiscio Express File Edit were hold Petrica File Edit were hold Petrica File Edit - Cortiscio Petrica General Contents General Contents Depent Expent Switch Identity Mont Office Contents of Sector Exit Petrics - X Petrics - X Petrics - X Petrics - X Petrics - X Petrics - X	Pres Drief Sent P	성 · 실 · · Sher · Address Prod ·	

- STEP 4 . To copy the route of SpamMail File in **Outlook Express** to convenient to upload the training to CS-500:
 - Press the right key of the mouse in SpamMail file and select **Properties** function.
 - Copy the file address in **SpamMail Properties** WebUI.

		영 · 말 · ·	
M SparnMail			
Particle and Article and an	Y. From School States School States	Stand Page spars Values for loss spars This 5.3 People of Cason Day Caso is used your of opans - Spars-Fact Software (Schlaren, Sparse spars Software Software (Schlaren, Sparse spars Software Software (Schlaren, Sparse spars Software Software (Schlaren, Sparse spars Software (Schlaren, Schlaren, Sparse spars Software (Schlaren, Schlaren	Synd Sy
Contracts * X			

his folder contains: 2 messages, 1 unread. his folder is stored in the following file: (57449)\Microsoft\Outlook Express\SpamMail (1) dt (0 du Cut Copy Paste	Se lot	amMail		
his folder is stored in the following file:			ä.	
Cut Copy				
La Cut Copy	67	448}\Microsoft\0		
			13	Cut
Select				Select Al

STEP 5 . Paste the route of copied from SpamMail file to the Spam Mail for Training field in Training function of Anti-Spam. And press OK to deliver this file to CS-500 instantly and to learn the uploaded mail file as spam mail in the appointed time.

Training Database					
Export Training Database	Download				
Import Training Database	Browse				
Reset Training Database	Reset Database				
Spam Mail for Training (Free space for traini	ng: 876 KBytes)				
Import Spam Mail from Client	Browse				
Ham Mail for Training (Free space for training	g: 876 KBytes)				
Import Ham Mail from Client	Browse				

Note:

- 1. The training file that uploads to CS-500 can be any data file and not restricted in its sub-name, but the file must be ACSII form.
- 2. When the training file of CS-500 is Microsoft Office Outlook exporting file [.pst], it has to close Microsoft Office Outlook first to start Importing.
- STEP 6. Remove all of the mails in SpamMail File in Outlook Express so that new mails can be compressed and upload to CS-500 to training directly next time.
 - Select all of the mails in SpamMail File and press the right key of the mouse to select Delete function.
 - Make sure that all of the mails in SpamMail file had been deleted completely.

* SpamMall		
Contract of Contra		
alder: X Outlook Express Duccal Folders Duccal Folders Duc	Image: Solution of the second state of the	Pacewell 9/20/2004 2:55 PM 9/20/2004 2:55 PM 9/20/2004 8:06 APE 9/20/2004 8:03 APE 9/20/2004 8:05 APE 9/20/2004 9
artarta ▼ X Brannarth Blannder∯mydoman.com		Inter Control Annue Receiption 20 Proved An Attachment Mark as Unexal Move to Polder Copy to Polder Copy to Polder Copy to Polder

Span/Sol - Dublock Express					1012
	pr 146)				0
teres Mad - Series - Bark M	Parent Proce Da		H H -		
•• SpamMail					
Palan X Collect Expens Collect Expens Collectors C	3 4 7 Pres 7	Subset	There are no Retro in this vie	Received	
Contacts • × ×					
Them are no contacts to diplay. Och on Contacts to create a new contact.					
D message(s), O unread				📕 Working Online	1

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**.

PLANET Retworking & Communication						
networking & Commanication	Mail Security > An	ti-Spam > Spam Mail				
■ System						
■ Interface						External
■ Policy Object	No.	<u>Recipient</u> 🗸	<u>Total Spam</u> 🗸	<u>Total Mail</u> 🗸	Duration	Spam %
■ Policy		No spa	m mail in the External	Mail Server		
⊫ Mail Security						
≖ Configure						
⊟ Anti-Spam						
– ⇒ Setting						
-⇒ Rule						
– ⇒ Whitelist						
–						
→ Training						
→ Spam Mail						

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

	Mail Security > Anti-Virus > Setting
¥ System ¥ Interface Policy Object Policy Mail Security ⊈ Configure ▲ Anti-Spam Anti-Virus → Setting	Anti-Virus Setting Virus Scan Engine Clam ♥ The Mail Server is placed in Internal (LAN or DMZ) (Please set Mail Relay first)
L ⇒ Virus Mail Anti-Attack Monitor	Update virus definitions immediately Action of Infected Mail Internal Mail Server: Delete the virus mail Delete the recipient 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 ④ 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.

PLANET Retworking & Communication	Mail Security > A	nti-Virus > Virus Mail				
≖ System						
■ Interface						External
■ Policy Object	No.	<u>Recipient</u> 🗸	<u>Total Virus</u> 🗸	<u>Total Mail</u> 🔫	Duration	Virus %
■ Policy		No virus	mail in the External I	Mail Server !		
⊫ Mail Security						
≖ Configure						
⊒ Anti-Spam						
🖻 Anti-Virus						
–⇒ Setting –⇒ Virus Mail						

4.6 IDP

CS-500 can aim at abnormal traffic and packets content to inspect, alert, and handle by the obstructive, separateness, interference, or alarm to administrator, to prevent suspicious program invades the host. So when CS-500 detects the attack behavior come from internal or external, it can provide the protection to network and obstruct to the attack behavior, let the network can still work normally and increase the information transmission security.

4.6.1 Setting

- It can update signature definitions for every 120 minutes. Or update signature definitions immediately. It will show the update time and version at the same time.
- It can detect virus to the file which have no encryption and compression.

Note: User can test if CS-500 can connect to IDP server to update the signature definitions on internet by **Test** function.

Set default action of all signatures:

- According to attack behavior's threat to divide: High Risk, Medium Risk, and Low Risk. The different risk attack behavior can be handled by the pass, drop, and log action.
 - Add the following settings in this function:
 - 1. Select **Enable Anti-Virus** (Disable Anti-virus function will abate the IDP function in virus protection).

- 2. Click OK.
- 3. High Risk: Select drop and log function.
- 4. Medium Risk: Select drop and log function.
- 5. Low Risk: Select pass and log function.
- 6. Click OK.
- 7. Enable **IDP** function in policy.

PLANET							
Wetworking & Communication	DP > Configure > Setting						
	Dr & Connigare & Searing						
🗷 System							
📧 Interface	IDP Setting						
📧 Policy Object	The latest update tin	ne : 06/04/10 02:23:03	(Update signature de	finitions every 120 minutes)			
🗷 Policy	The newest version	: 0.0.7 (Signature def	initions updated at 05	/05/03 00:00:00)			
📧 Mail Security	Update signature de	Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) Update NOW					
I IDP			·		• <u> </u>		
🗉 Configure	🔽 Enable Anti-Viru	us (for HTTP, FTP, P2P	, IM, NetBIOS)				
L⇒ Setting							
I Signature					OK Cancel		
■ IDP Report	0.1.1.4.4.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.						
🗷 Anomaly Flow IP	Set default action	_					
I Monitor	High Risk	Drop 🚩	🗹 Log	([Pass] recommended)			
Monitor	Medium Risk	Drop 🔽	💌 Log	([Pass] recommended)			
	Low Risk	Pass 💌	💌 Log	([Pass] recommended)			
					OK Cancel		

When the attack behavior matches the signature, CS-500 will produce log as follows in Log function of IDP Report.

PLANET Networking & Communication	IDP > IDP Report > Lo	a					
		2					
■ System							
🗉 Interface	Time	Event	Signature Class.	Interface	Attack IP	Victim IP:Port	
🗉 Policy Object			No Data				
I Policy							
■ Mail Security							
B IDP							
■ Configure							
∃ Signature							
⊒ IDP Report							
L⇒ Log							

4.6.2 Signature

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

Anomaly:

Anomaly signature can allow user to define the signature, in order to detect and prevent the irregular attack behavior. Take **Syn Flood** as the example:

Definition:

Enable: Check to enable the protection for Syn Flood signature.

Max. Threshold
Pkts / Sec: Configure the value to define the Syn Flood signature.

Blocking Time: Set up the timing to block the attacked connection. The function is available when the **Action** sets to **Drop**.

Action: When the packets match the signature, select **Pass** to pass the packets, or select **Drop** to discard the packets.

Log: Check Log function to record the log in IDP Report.

PLANET Retworking & Communication	IDP > Signature > Anom:	aly		
🗷 System		Modify Anomaly D) otact Satting ((even flood)
🖬 Interface			verect berning ((syn nood)
🖬 Policy Object		🗹 Enable		
🗉 Policy		Max. Threshold	200	Pkts / Sec (Downstream 1024 Kbps, 200 recommended)
🎟 Mail Security		Blocking Time	60	Seconds
■ IDP		Action	Drop 🔽	Log
■ Configure		r lottori	Drop I	
⊟ Signature				OK Cancel
→ Anomaly				on ouncer
Pre-defined				
→ Custom				

Pre-defined:

Pre-defined signatures can detect and prevent to intrusive pattern which can be discovered at present. These signatures can not be modified and deleted.

Definition:

Action: Select Pass to pass the packets, or select Drop to discard the packets.

Log: Check Log function to record the log in IDP Report.

	IDP > Signature > Pre-defined
🗉 System	
🗉 Interface	Modify Signature Action (Backdoor)
🗉 Policy Object	Pass 💙 📃 Log
🗉 Policy	
🗷 Mail Security	OK Cancel
⊫ IDP	
■ Configure	
⊟ Signature	
→ Anomaly	
→ Pre-defined	
L+ Custom	

Custom:

Custom signatures can allow user to create the signature according to their requirement, works to detect and prevent the internal and external attack behavior which are not including in **Pre-defined** signatures.

Definition:

Name: The System Manager can name the signature.

Protocol: Select the protocol which wants to be detected and prevented, it can be divided: TCP, UDP, ICMP and IP.

Source Port: Configure the port number that is used to attack the PC. (The range can be from 0 to 65535).

Destination Port: Configure the port number that the client PC is used to be attacked.

Risk: Define the threat about attack packets.

Action: Select Pass to pass the packets, or select Drop to discard the packets.

Log: Check Log function to record the log in IDP Report.

Content: Define the attack packets content.

)P > Signature > Custom	
System		
Interface	Add New Signature	
Policy Object	Name	
Policy	Protocol	
Mail Security	Source Port	0:65535
DP	 Destination Port	
Configure		
Signature	Risk	High 💌
Anomaly	Action	Pass 💙 📃 Log
Pre-defined	Content	
_♦ Custom		

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

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

	IDP > Configure > Setting
System Interface Policy Object Policy Mail Security IDP Configure Astring Signature	IDP Setting The latest update time : 06/04/06 08:13:44 (Update signature definitions every 120 minutes) The newest version : 0.0.7 (Signature definitions updated at 05/05/03 00:00:00) Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) Update NOW Test
■ IDP Report ■ Anomaly Flow IP ■ Monitor	Set default action of all signatures High Risk Drop Image: Log ([Pass] recommended) Medium Risk Drop Image: Log ([Pass] recommended) Low Risk Pass Image: Log ([Pass] recommended)

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

- Click New Entry.
- Name: Enter Software_Crack_Website.
- Protocol: Select TCP.
- Source Port: Enter 0:65535.

- **Destination Port**: Enter 80:80.
- Risk: Select High.
- Action: Select Drop and enable Log function.
- **Content**: Enter cracks.

PLANET Retworking & Communication	IDP > Signature > Custom			
≖ System ■ Interface	Add New Signature			
Policy Object	Name	Software_Crack_Website		
I Policy	Protocol			
🖬 Mail Security	Source Port	0:65535		
■ IDP	Destination Port	80:80		
■ Configure ■ Signature	Risk	High 🔽		
Anomaly	Action	Drop 💽		
→ Pre-defined	Content	cracks		
L⇒ Custom				

Click OK to finish the IDP setting.

PLANET Vetworkling & Communication	IDP >	Signature > Custom							
Bystem									
Interface		Name	Protocol	Src. Port	Dst. Port	Risk	Action	Log	Configui
Policy Object		Software_Crack_Website	TCP	0:65535	80:80	•	×	v	Modify R
Policy									
Mail Security					New Entry				
IDP									
Configure	Ī								
∃ Signature									
→ Anomaly	-								
■ Pre-defined									
_⇒ Custom									

STEP 3. Enter the following settings in Outgoing Policy to enable the IDP function:

PLANET		
Wetworking & Communication	olicy > Outgoing	
em		
face	Comment :	
Object	Modify Policy	
ру	Source Address	Inside_Any 🔽
Itgoing	Destination Address	Outside_Any 🔽
ming	Service	ANY 🔽
To DMZ	Schedule	None 🗸
To DMZ	Authentication User	None 💙
o WAN		
o LAN	Trunk	None 💌
urity	Action, WAN Port	PERMIT ALL
	Traffic Log	Enable
Flow IP	Statistics	Enable
	IDP	Enable
	Content Blocking	Enable
	MAX. Concurrent Sessions	0 (0:means unlimited)
	QoS	None 🔽

4.6.3 IDP Report

CS-500 can make intrusion detection and prevention record to a Log report, and allow administrator to know the network security status for the overall network.

STEP 1. In Log of IDP Report function, it will display the situation about intrusion detection and

prevention of CS-500.

PLANET Retworking & Communication	IDP > IDP Report > Li	Dg					
System							
Interface	Time	Event	Signature Class.	Interface	Attack IP	Victim IP:Port	
Policy Object			No Data				
Policy							
🛙 Mail Security							
5 IDP							
± Configure							
± Signature							
IDP Report							
L⇒ Log							

Icon Definition:

1. Action:



2. Risk:

•	8	0
High Risk	Medium Risk	Low Risk

4.7 Anomaly Flow IP

The Administrator can enable the device's auto detect functions for Anomaly Flow IP attacking the local network. When abnormal conditions occur, CS-500 will send an e-mail alert to notify the Administrator, and also display warning messages in the Virus-infected IP window.

	Anomaly Flow IP > Setting
■ System	Anomaly Flow IP Setting
■ Interface ■ Policy Object	The threshold sessions of anomaly flow (per source IP) is 30 Sessions / Sec
■ Policy ■ Mail Security	Enable Anomaly Flow IP Blocking Blocking Time Booking Time Booking Time
🖩 IDP 🖻 Anomaly Flow IP 🛭 🗲 🗲	Enable E-Mail Alert Notification
→ Setting	Enable NetBIOS Alert Notification IP Address of Administrator
L → Virus-infected IP Monitor	OK Cancel

Anomaly Flow IP Settings

- Enable Anomaly Flow IP Blocking: Select this option to enable the Anomaly Flow IP blocking function. Once the Anomaly Flow IP attacked is detected, it will block the connection for user-drefined blocking time.
- Enable E-mail Alert Notification: When Anomaly Flow IP attacked is detected, send alert e-mail to administrator by using e-mail address defined on System -> Setting.
- Enable NetBIOS Alert Notification: When Anomaly Flow IP attacked is detected, send alart message to administrator by using "Net send" command.

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

4.8 Monitor

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

4.8.1 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.

4.8.1.1 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 1. Click the Traffic option under Log menu to enter the Traffic Log window.

PLANET Retworking & Communication	Monitor > Log > Traffic					
em			May 3 06:5	e-10 💀		
ace			Way 5 00.5	5.20		<u>N</u>
/ Object /	Time	Source	Destination	Protocol	Port	Disposition
	Maγ 3 06:58:20	192.168.1.2	192.168.1.1	TGP	3580 => 80	×
urity	Maγ 3 06:58:20	192.168.1.2	192.168.1.1	TCP	3579 => 80	×
	May 3 06:58:17	192.168.1.2	67.87.113.253	TCP	3576 => 443	×
w IP	May 3 06:58:17	67.87.113.253	192.168.1.2	TCP	443 => 3576	×
	May 3 06:58:16	192.168.1.2	67.87.113.253	TCP	3576 => 443	- /
++	May 3 06:57:36	67.11.214.24	192.168.1.2	UDP	31346 => 39230	V
	May 3 06:57:36	192.168.1.2	67.11.214.24	UDP	39230 => 31346	V
tion	May 3 06:57:25	221.88.90.16	192.168.1.2	UDP	32999 => 39230	V
kup	May 3 06:57:24	192.168.1.2	221.88.90.16	UDP	39230 => 32999	\checkmark

Traffic Log Table

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

Definition:

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

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

- Step 1. In the Traffic Log window, click the Download Logs button at the bottom of the screen.
- **Step 2.** Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

Clearing the Traffic Logs

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

- **Step 1.** In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.
- Step 2. In the Clear Logs pop-up box, click Ok to clear the logs or click Cancel to cancel it.

	Monitor > Log > Traffic					
≖ System ≖ Interface			Jun 29 08:05:49	-		
🗷 Policy Object	Time	Source	Destination	Protocol	Port	Disposition
■ Policy	Jun 29 08:05:49	211.75.117.114	210.66.155.90	TCP	47243 => 80	Ø
■ Mail Security	Jun 29 08:05:49	211.75.117.114	210.66.155.90	TCP	47242 => 80	Ø,
▼ Anti-Attack ■ Monitor ⊟ Log		Microsoft Interne	t Explorer 🔀	Download	Logs	
-⇒ Traffic -⇒ Event -⇒ Connection -⇒ Log Backup		OK	Cancel			

4.8.1.2 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		
- reservering a commensation	Monitor > Log > Event	
ystem		N. 000 50 57
nterface		May 3 06:53:57 💌
Policy Object	Time	Event
Policy		
fail Security	May 3 06:53:57	admin Modify [Accounting Report Setting] from 192.168.1.2
P	May 3 06:53:45	admin Add [Policy](Incoming,Outside_Any=>210.66.155.91,FTP(21),permit) from 192.168.1.2
nomaly Flow IP	May 3 06:53:31	admin Modify [Policy](Outgoing,Inside_Any=>Outside_Any,ANY,permit) from 192.168.1.2
lonitor	May 3 06:51:38	user admin [Login success] from 192.168.1.2
Log	May 3 06:51:36	user admin [Login failure] from 192.168.1.2
➡ Traffic	May 3 05:56:00	admin Add [Policy](DMZ to External,DMZ_Any=>Outside_Any,ANY,permit) from 192.168.1.2
⇒Event ←←	May 3 05:48:17	admin Add [Policy](External to DMZ,Outside_Any=>DMZ_Any(Routing),ANY,permit) from 192.168.1.2
Connection	May 3 05:44:46	admin Delete [Policy](Incoming,Outside_Any=>Inside_Any(Routing),ANY,permit) from 192.168.1.2
➡ Log Backup	May 3 05:45:44	admin Modify [DMZ Interface] from 192.168.1.2
Accounting Report	May 3 05:44:21	admin Add [Policy](Incoming,Outside_Any=>Inside_Any(Routing),ANY,permit) from 192.168.1.2
Statistics	May 3 04:01:29	user admin [Login success] from 192.168.1.2
Status	May 3 03:12:17	user admin [Login success] from 192.168.1.3

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

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

Clearing the Event Logs

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

- **Step 1.** In the Event Log window, click the Clear Logs button at the bottom of the screen.
- Step 2. In the Clear Logs pop-up box, click OK to clear the logs or click Cancel to cancel it.

PLANET Retworking & Communication	Monitor > Log > Event	
≖ System ≖ Interface		Jun 29 08:05:22 🐱
Policy Object	Time	Event
🗉 Policy	Jun 29 08:05:22	admin Clear [Traffic Log] from 211.75.117.114
≖ Mail Security	Jun 29 08:05:14	admin Clear [Event Log] from 211.75.117.114
Anti-Attack		Microsoft Internet Explorer 🛛 🔀
■ Monitor ■ Log → Traffic → Event		Do you really want to clean ?

4.8.1.3 Connection

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

PLANET Retworking & Communication	Monitor > Log > Connection	
■ System ■ Interface	Back	May 3 02:45:05 💌
■ Policy Object ■ Policy	Time	Connection Log
Mail Security	May 3 02:45:05	ipop: returning Configure-NAK
	May 3 02:45:05	MPPE 128 bit, stateless compression enabled
Anomaly Flow IP	May 3 02:45:05	ipop: returning Configure-ACK
Monitor	May 3 02:45:05	ipop: up
E Log	May 3 02:45:05	Cannot determine ethernet address for proxy ARP
→ Traffic	May 3 02:45:05	local IP address 192.221.117.1
_⇒ Event	May 3 02:45:05	remote IP address 192.238.6.1
-+ Connection	May 3 02:45:33	LCP terminated by peer (kM-C*(^@
➡ Log Backup	May 3 02:45:33	ipep: down
Accounting Report	May 3 02:45:33	tdb_store failed: Invalid tdb context
∎ Statistics	May 3 02:45:33	message repeated 2 times
± Status	May 3 02:45:37	GRE: read error: Bad file descriptor

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.

	Monitor > Log > Connecti	ion
■ System		Jan 1 00:08:44 🗸
■ Interface		
■ Policy Object	Time	Connection Log
■ Policy	Jan 1 00:08:44	including NAT-Traversal patch (Version 0.6)
≖ Mail Security		time moved backwards 89 seconds
Anti-Attack		
🗏 Monitor		
⊐Log		Clear Logs Download Logs
–♦ Traffic		
–⇒ Event		
-> Connection		
L⇒Log Backup		

4.8.1.4 Log Backup

Click Log →Log Backup.

PLANET Retworking & Communication	Monitor > Log > Log Backup
■ System ■ Interface ■ Policy Object ■ Policy ■ Mail Security	Log Mail Configuration Enable Log Mail Support When Log Full (300Kbytes), Content Security Gateway Appliance sends Log You must enable the E-mail Alarm
Traffic ◆ Event Connection Log Connection ↓ Log Backup	Syslog Setting Enable Syslog Messages Syslog Host IP Address (ex: 192.168.1.61) Syslog Host Port (Range: 0 - 65535, ex: 514)

Log Mail Configuration: When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

NOTE: Before enabling this function, you have to configure E-mail Settings in System -> Settings.

Syslog Settings: If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

NOTE: To restart Connection Log, click the **Refresh** button on the right hand side in Log window.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

- Step 1. Firstly, go to Admin –Select Enable E-mail Alert Notification under E-Mail Settings. Enter the e-mail address to receive the alarm notification. Click OK.
- Step 2. Go to LOG →Log Backup. Check 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.

	Monitor > Log > Log Backup	
≖ System ≖ Interface ≖ Policy Object	Log Mail Configuration Enable Log Mail Support When Log Full (300Kbytes), Conter 	nt Security Gateway Appliance sends Log
■ Policy ■ Mail Security	You must enable the E-mail Alarm	
■ Anti-Attack	Syslog Setting	
🗏 Monitor	Enable Syslog Messages	
⊟ Log	Syslog Host IP Address	192.168.1.10 (ex: 192.168.1.61)
– ⇔ Traffic – ⇔ Event – ⇒ Connection – ⇔ Log Backup	Syslog Host Port	514 (ex: 514)

Disable Log Mail Support & Syslog Message

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

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

4.8.2 Accounting Report

Accounting Report can be divided into three parts, Setting, Outbound and Inbound.

4.8.2.1 Setting

Select **Setting** to configure what type of Accounting Report will be logged at CS-500. There are three types of report can be select: **Source IP**, **Destination IP** and **Service**.

Outbound Accounting Report: the statistics of the downstream and upstream for the LAN, WAN and all kinds of communication services.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.

Inbound Accounting Report: the statistics of downstream and upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN host connects to LAN host via CS-500.

Source IP: Select to record the statistic based on Source IP address.

Destination IP: Select to record the statistic based on Destination IP address.

Service: Select to record the statistic based on Service.

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service for all of the user's IP that passes through CS-500.

PLANET Retworking & Communication	Monitor > Accounting Report > Setting
🗉 System	Accounting Report Setting
🎟 Interface	
🗉 Policy Object	Outbound Accounting Report
🗉 Policy	
🏽 Mail Security	Destination IP
IDP	✓ Service
🗉 Anomaly Flow IP	Inbound Accounting Report
🖻 Monitor	Source IP
'⊞ Log	Destination IP
E Accounting Report	Service
→ Setting	
→ OutBound	OK Cancel
L ➡ InBound	

4.8.2.2 Outbound

Click the **Accounting Report** function, and then select **Outbound**. There are three options for outbound acounting report: Source IP, Destination IP and Services.

PLANET Retworking & Communication	Mon	itor > Accounting Repor	: > OutBound	1						
■ System ■ Interface						Тор: 1-:	2 🗸	Star	ting Time : Thu Apr	6 11:16:10 2006
■ Policy Object ■ Policy	No.	Source IP 🛛 🔽 🔽	Down	stream 🔻	Upstrea	ım 🔻	First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
■ Mail Security	1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
IDP	2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
🗉 Anomaly Flow IP		Total Traffic	3.	3.3 MB 327.8 KB			Reporting time Mon Apr 10 04:23:45 200			
 Monitor ▲ Log Accounting Report → Setting → OutBound → InBound 									Res	et Counters

Outbound Source IP Accounting Report

Pull down the menu and select Source IP to show the outbound source IP accounting report.

■ System ■ Interface						Тор: 1 - :	2 🕶			
Policy Object								Star	ting Time : Thu Apr	6 11:16:10 20
Policy	No.	Source IP 🛛 🔽 🥆	Downs	stream 🥆	Upstream 🔻		First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
Mail Security	1	192.168.10.2	3.3 MB	99.9%	327.4 KB	99.9%	04/07 01:41:46	04/10 02:34:10	3D 00:52:24	Remove
IDP	2	192.168.10.3	3.4 KB	0.1%	470.0 B	0.1%	04/10 02:56:22	04/10 02:57:23	00:01:01	Remove
Anomaly Flow IP		Total Traffic	3.	3.3 MB 327.8 KB		КВ	Reporting time Mon A			
≣ Monitor										
≖ Log									Res	et Counters
E Accounting Report										

When LAN users connect to WAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The LAN user's IP address connects to CS-500 to access WAN service server.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user **Duration:** The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Reset Counters: Click Reset Counters button to refresh Accounting Report.

Outbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the outbound destination IP accounting report.

PLANET Retworking & Communication	Monit	tor > Accounting Report >	• OutBouni	1						
■ System						T [1	1			
🗉 Interface						Top: 1 -		~		
🛙 Policy Object								Star	ting Time : Thu Api	6 11:16:10 20
Policy	No.	Destination IP 🔽 🥆	Dowr	istream 🔻	Upstre	am 🔻	First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
Mail Security	1	203.128.173.176	54.0 B	100.0%	46.0 B	100.0%	04/07 02:07:13	04/07 02:07:13	00:00:00	Remove
IDP		Total Traffic	6	54.0 B	46.) 8		Repo	orting time Sun Api	9 02:38:22 20
Anomaly Flow IP										
■ Monitor									Res	set Counters
≖ Log										
E Accounting Report										
→ Setting										
-+ OutBound										
L⇒ InBound										

When LAN user connect to WAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Destination IP will be recorded.

Definition:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The WAN Server's IP address.

Downstream: The percentage of downstream and the statistic value of the connection from LAN user to WAN server.

Upstream: The percentage of upstream and the statistic value of the connection from WAN server to LAN user.

First Packet: The time record of the first packet that was sent to LAN user from WAN service server.

Last Packet: The time record of the last packet sent from LAN user and received by the WAN server

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

Outbound Service Accounting Report

Pull down the menu and select Service to show the outbound service accounting report.

PLANET Retworking & Communication	Monitor > Accounting Report > Ou	Bound	
System Interface Policy Object	1	Service Distribution	
Policy	No.	Downstream	
Mail Security	1 HTTP [80]	3.1 MBytes (96.3%)	
Anomaly Flow IP	2 DNS [53]	16.6 KBytes (0.5%)	
Monitor	3 UNKNOW [1056]	16.4 KBytes (0.5%)	
Log	4 UNKNOW [11159]	13.2 KBytes (0.4%)	
Accounting Report	5 UNKNOW [33085]	9.5 KBytes (0.3%)	
_→ Setting	6 UNKNOW [49160]	5.9 KBytes (0.2%)	
- OutBound	7 UNKNOW [50588]	5.3 KBytes (0.2%)	
_♦ InBound	8 UNKNOW [54045]	5.2 KBytes (0.2%)	
Statistics	9 UNKNOW [5317]	5.1 KBytes (0.2%)	
Status	10 UNKNOW [15199]	5.0 KBytes (0.1%)	
	OTHER	41.1 KBytes (1.2%)	

When LAN users connect to WAN Service Server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when LAN users connect to WAN service server through CS-500. (**Port**) indicates the protocol port number.

Downstream: The percentage of downstream and the statistic value of the connection from WAN server to LAN user.

Upstream: The percentage of upstream and the statistic value of the connection from LAN user to WAN server.

First Packet: The time record of the first packet that was sent to WAN service server from LAN user.

Last Packet: The time record of the last packet sent from WAN server and received by the LAN user

Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN user to WAN service server.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.8.2.3 Inbound

Click the **Accounting Report** function, and then select **Inbound**. There are three options for Inbound acounting report: Source IP, Destination IP and Service.

	Mon	itor > Accounting Report	> InAound							
■ System ■ Interface						Тор: 1-0	6 💌	Star	ing Time : Thu Apr	6 11:16:10 20
Policy Object Policy	No.	Source IP 🛛 🔽 🔽	Upstre	am 🔻	Downst	eam 🔻	First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
Mail Security	1	211.75.117.114	13.6 MB	100.0%	211.0 KB	99.1%	04/07 12:43:10	04/07 13:10:23	00:27:13	Remove
I IDP	2	82.226.135.163	1.0 KB	0.0%	675.0 B	0.3%	04/08 06:46:30	04/08 13:29:13	06:42:43	Remove
Anomaly Flow IP	3	67.78.0.138	935.0 B	0.0%	655.0 B	0.3%	04/07 17:11:59	04/08 06:07:30	12:55:31	Remove
i Monitor	4	83.19.250.74	477.0 B	0.0%	336.0 B	0.2%	04/07 14:37:26	04/07 14:37:32	00:00:06	Remove
■ Log ∃ Accounting Report	5	67.71.33.201	467.0 B	0.0%	284.0 B	0.1%	04/08 13:03:05	04/08 13:03:06	00:00:01	Remove
■Accounting Report	6	80.51.174.70	44.0 B	0.0%	88.0 B	0.0%	04/08 13:11:28	04/08 13:11:29	00:00:01	Remove
→ OutBound → InBound ← ← ← Statistics	- 7	Total Traffic	13.6	IMB_	213.0	IKB		Report	ing time Mon Apr 1	o 04:26:07 20 et Counters

Inbound Source IP Accounting Report

Pull down the menu and select Source IP to show the inbound source IP accounting report.

	Moni	tor > Accounting Repor	t > InBound							
System Interface Policy Object						Тор: 1-0	6 💙	Star	ting Time : Thu Apr	6 11:16:10 2
Policy	No.	Source IP 🛛 🔽 🔽	Upstre	eam 🔻	Downst	eam 🔻	First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
Mail Security	1	211.75.117.114	13.6 MB	100.0%	211.0 KB	99.1%	04/07 12:43:10	04/07 13:10:23	00:27:13	Remove
IDP	2	82.226.135.163	1.0 KB	0.0%	675.0 B	0.3%	04/08 06:46:30	04/08 13:29:13	06:42:43	Remove
Anomaly Flow IP	3	67.78.0.138	935.0 B	0.0%	655.0 B	0.3%	04/07 17:11:59	04/08 06:07:30	12:55:31	Remov
Monitor	4	83.19.250.74	477.0 B	0.0%	336.0 B	0.2%	04/07 14:37:26	04/07 14:37:32	00:00:06	Remov
Log Accounting Report	5	67.71.33.201	467.0 B	0.0%	284.0 B	0.1%	04/08 13:03:05	04/08 13:03:06	00:00:01	Remov
→ Setting	6				88.0 B		04/08 13:11:28		00:00:01	Remove
-→ OutBound -→ InBound		Total Traffic	13.6	i MB	213.0) KB		Report	ing time Mon Apr 1	0 04:26:07 2 et Counter

When WAN users connect to LAN service server through CS-500, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the source IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Source IP: The IP address used by WAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from LAN host to WAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from WAN host to LAN host via CS-500.

First Packet: The time record of the first packet that was sent from WAN host to LAN host.

Last Packet: The time record of the last packet that sent from WAN host to LAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from WAN host to LAN host.

Inbound Destination IP Accounting Report

Pull down the menu and select **Destination IP** to show the inbound destination IP accounting report.

PLANET Retworking & Communication	Mon	itor > Accounting Report >	• InBound							
■ System ■ Interface						Тор: 1 -	1 🔽			
Policy Object								Star	ting Time : Thu Apr	6 11:16:10 2006
Policy	No.	Destination IP 🔽 🔽	Upstr	eam 🔻	Downstr	eam 🔻	First Packet 🔻	Last Packet 🔻	Duration 🔻	Action
🗏 Mail Security	1	192.168.10.2	13.6 MB	100.0%	213.0 KB	100.0%	04/07 12:43:10	04/08 13:29:13	1D 00:46:03	Remove
IDP		Total Traffic	13.6	6 MB	213.0	КВ		Report	ing time Mon Apr 1	
🗷 Anomaly Flow IP										
🗏 Monitor									Res	et Counters
⊞ Log										
■ Accounting Report										
→ Setting										
→ OutBound										
InBound										

When WAN host connect to LAN through CS-500, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Destination IP: The IP address used by LAN host.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-500.

First Packet: The time record of the first packet that was sent from LAN host to WAN host.

Last Packet: The time record of the last packet that sent from LAN host to WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet.

Total Traffic: CS-500 will record the sum of upstream/downstream packets from LAN host to WAN host.

Inbound Service Accounting Report

Pull down the menu and select Service to show the inbound service accounting report.

	Monitor > Accounting Report > Ir	Bound	
■ System		Service Distributio	
🗉 Interface	A	Service Distributio	ri I
Policy Object	- X		
Policy	No.	Downstream	
🎟 Mail Security			
IDP	1 UNKNOW [2226]	13.6 MBytes (99.9%)	
🗷 Anomaly Flow IP	2 FTP [21]	7.5 KBytes (0.1%)	
🗏 Monitor	3 UNKNOW [2224]	1.1 KBytes (0.0%)	
⊞ Log	4 FTP-DATA [20]	432.0 Bytes (0.0%)	
Accounting Report	OTHER	0.0 Bytes (0.0%)	
→ Setting			
→ OutBound			
InBound			
■ Statistics			
⊞ Status			

When WAN host connect to LAN host through CS-500, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

Definitions:

Top: Select the data type you want to check. It presents 10 results in one page.

Service: The report of Communication Service when WAN host connect to LAN host through CS-500. **(Port)** indicates the protocol port number.

Downstream: The percentage of Downstream and the statistic value of the connection from WAN host to LAN host via CS-500.

Upstream: The percentage of Upstream and the statistic value of the connection from LAN host to WAN host via CS-500.

First Packet: The time record of the first packet that was sent to LAN host from WAN host.

Last Packet: The time record of the last packet sent to LAN host from WAN host.

Duration: The time statistic record that started from the first packet and end to the last packet

Total Traffic: CS-500 will record the sum of upstream/downstream packets from WAN host to LAN host.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.

4.8.3 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 mange networks.

How to apply WAN Statistics

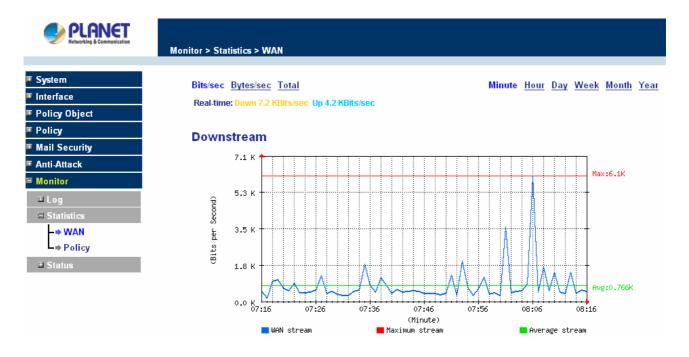
The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics. In this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

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.

4.8.3.1 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) .

4.8.3.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

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

	Monitor > Statistics >	Policy			
■ System	Source	Destination	Service	Action	Time
Interface	Inside_Any	Outside_Any	ANY	PERMIT	<u>Minute Hour Day Week Month Year</u>
Policy Object					
Policy					
Mail Security					
Anti-Attack					
Monitor					
∃Log					
Statistics					
+⇒ WAN					

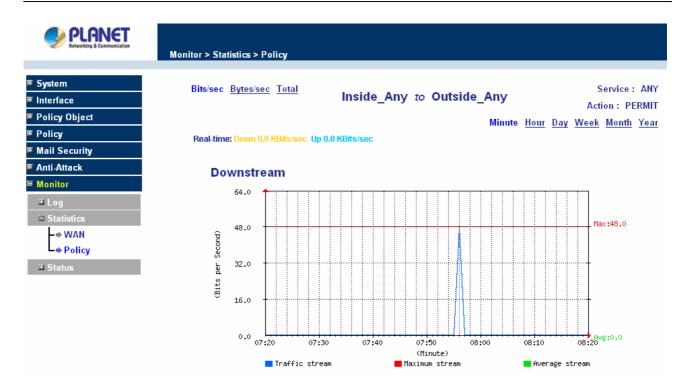
NOTE: To use Statistics, the administrator needs to go to Policy to enable Statistics function.

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).



4.8.4 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.

4.8.4.1 Interface Status

Entering the Interface Status window

Click on Status in the menu bar, then click Interface Status below it. A window will appear providing information from the Configuration menu. Interface Status will list the settings for LAN Interface, WAN Interface, and the DMZ Interface.

PLANET Networking & Communication	Monitor > Status > Interface			
≖ System	Active Sessions Number : 14			System Uptin
🗉 Interface		LAN	WAN	DMZ
■ Policy Object	Forwarding Mode	NAT	Static IP	NAT
∎ Policy	Max. Downstream / Upstream		10000 / 10000 Kbps	
Mail Security	PPPoE Con. Time			
Anti-Attack	MAC Address	00:30:4f:3d:9e:92	00:30:4f:3d:9e:93	00:30:4f:3d:9e:94
_	IP Address	192.168.1.1	210.66.155.90	192.168.88.1
5 Monitor	Netmask	255.255.255.0	255.255.255.224	255.255.255.0
⊞ Log	Default Gateway		210.66.155.94	
⊞ Alarm	DNS1		168.95.1.1	
	DNS2		0.0.0	
⊟ Status	Rx Pkts, Error Pkts	0, 0	19523, 0	0,0
1	Tx Pkts, Error Pkts	0, 0	5796, 0	0, 0
-⇒ Interface	Ping		Ø	
Authentication	HTTP	- V	- Ø	
–♦ ARP Table				
→ DHCP Clients				

4.8.4.2 Authentication

Entering the Auth Status window

Click on **Status** in the menu bar, then click Authentication below it. A window will appear and provide information from the Auth User menu. Authentication Status will list the settings for Auth User login status.

PLANET Networking & Communication	Monitor > Status > Authentica	tion	
<i>y</i> stem	IP Address	Authentication-User Name	Login Time
erface	192.168.1.2	planet	2005/6/29 8:24:12
icy Object			
icy			
il Security			
-Attack			
nitor			
og			
tatistics			
tatus			
➡ Interface			
Authentication			
⇒ARP Table			
-⇒DHCP Clients			

IP Address: The IP address of the host computer.

Auth-User Name: The Auth User Name of that host computer.

Login time: The Auth User login in time.

4.8.4.3 ARP Table

Entering the ARP Table window

Click on **Status** in the menu bar, then click **ARP Table** below it. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN, and DMZ network that replies to an ARP packet, the device will list them in this ARP table.

System	IP Address	MAC Address	Interface
Interface	210.66.155.94	00:A0:C5:11:89:C9	WAN
olicy Object			
olicy			
ail Security			
nti-Attack			
onitor			
Log			
Alarm			
Statistics			
Status			
-⇒Interface			
–⇒ Authentication			
-⇒ARP Table			
➡ DHCP Clients			

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)

4.8.4.4 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.

	Monitor > Status > DHCP Clie	ents		
system	IP Address	MAC Address	Leased Time	
Interface			Start	End
Policy Object	192.168.1.11	88:17:20:00:01:80	2005/6/23 16:56:1	2005/6/24 16:56:1
Polic y				
Mail Security				
Anti-Attack				
Monitor				
≖ Log				
≖ Alarm				
⊟ Status				
–♦ Interface				
→ Authentication				
-⇒ARP Table				
■ DHCP Clients				

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.

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com