



# **UTM Content Security Gateway**

**CS-2000**

**User's Manual**

## Copyright

Copyright© 2007 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## 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.

## 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.

## CE mark Warning

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

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

## FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

## R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## WEEE Caution



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

## Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## Customer Service

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

<http://www.test.com>

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

- ◆ UTM 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 UTM Content Security Gateway

Model: CS-2000

Rev: 1.0 (July, 2007)

PartNo: EM-CS2000v1

## Table of Contents

<b>CHAPTER 1: INTRODUCTION .....</b>	<b>1</b>
1.1 FEATURES .....	1
1.2 PACKAGE CONTENTS .....	2
1.3 CS-2000 FRONT VIEW .....	3
1.4 SPECIFICATION .....	3
<b>CHAPTER 2: HARDWARE INSTALLATION.....</b>	<b>5</b>
<b>CHAPTER 3: SYSTEM .....</b>	<b>7</b>
3.1 ADMINISTRATION.....	7
3.1.1 Admin .....	9
3.1.2 Permitted IPs .....	11
3.1.3 Software Update .....	12
3.2 CONFIGURE .....	13
3.2.1 Setting.....	17
3.2.2 Date/Time.....	23
3.2.3 Multiple Subnet .....	24
3.2.4 Route Table .....	27
3.2.5 DHCP.....	31
3.2.6 DDNS.....	33
3.2.7 Host Table .....	35
3.2.8 SNMP.....	36
3.2.9 Language .....	38
3.3 LOGOUT .....	39
<b>CHAPTER 4: INTERFACE.....</b>	<b>40</b>
4.1 LAN .....	42
4.2 WAN.....	43
4.3 DMZ .....	48
<b>CHAPTER 5: POLICY OBJECT .....</b>	<b>50</b>
5.1 ADDRESS .....	50
5.2 SERVICE .....	60
5.3 SCHEDULE .....	69
5.4 QoS.....	71
5.5 AUTHENTICATION .....	75
5.5.1 Example 1 User & User Group Authentication .....	81



---

5.5.2 Example 2 RADIUS Server Authentication .....	84
5.5.3 Example 3 POP3 Server Authentication .....	98
5.5.4 Example 4 LDAP Server Authentication .....	101
5.6 CONTENT BLOCKING .....	115
5.7 IM/P2P BLOCKING .....	127
5.8 VIRTUAL SERVER.....	134
5.9 VPN.....	148
5.9.1 VPN Wizard.....	151
5.9.2 Example 1 .....	158
5.9.3 Example 2 .....	173
5.9.4 Example 3.....	219
5.9.5 Example 4.....	233
5.9.6 Example 5.....	253
<b>CHAPTER 6: POLICY .....</b>	<b>266</b>
<b>CHAPTER 7: MAIL SECURITY .....</b>	<b>294</b>
7.1 CONFIGURE .....	294
7.1.1 Setting.....	295
7.1.2 Mail Relay .....	299
7.1.3 Mail Account.....	305
7.1.4 Mail Notice .....	314
7.2 ANTI-SPAM.....	327
7.2.1 Setting.....	328
7.2.2 Personal Rule .....	332
7.2.3 Global Rule .....	333
7.2.4 Whitelist.....	335
7.2.5 Blacklist.....	335
7.2.6 Training .....	336
7.2.7 Spam Mail.....	337
7.2.8 The Advanced Description.....	339
7.2.9 Anti-Spam Examples.....	343
7.3 ANTI-VIRUS.....	390
7.3.1 Setting.....	391
7.3.2 Virus Mail .....	394
7.3.3 Anti-Virus Examples.....	396
7.4 MAIL REPORT .....	407
7.4.1 Setting.....	408
7.4.2 Statistics.....	414
7.4.3 Log .....	416

<b>CHAPTER 8: IDP .....</b>	<b>420</b>
8.1 CONFIGURE .....	420
8.2 SIGNATURE .....	425
8.2.1 <i>Anomaly</i> .....	426
8.2.2 <i>Pre-defined</i> .....	427
8.3 IDP REPORT .....	434
8.3.1 <i>Setting</i> .....	435
8.3.2 <i>Statistics</i> .....	440
8.3.3 <i>Log</i> .....	442
<b>CHAPTER 9: ANOMALY FLOW IP .....</b>	<b>446</b>
<b>CHAPTER 10: WEB VPN/SSL VPN .....</b>	<b>451</b>
<b>CHAPTER 11: ADVANCE .....</b>	<b>461</b>
11.1 INBOUND BALANCE .....	461
11.1.1 <i>Inbound Load Balance Examples</i> .....	471
11.2 HIGH AVAILABILITY .....	501
<b>CHAPTER 12: MONITOR .....</b>	<b>511</b>
12.1 LOG .....	511
12.1.1 <i>Log Examples</i> .....	517
12.2 ACCOUNTING REPORT .....	526
12.3 STATISTICS .....	539
12.4 DIAGNOSTIC .....	545
12.5 WAKE ON LAN .....	551
12.6 STATUS .....	553
12.6.1 <i>Interface</i> .....	554
12.6.2 <i>System Info</i> .....	556
12.6.3 <i>Authentication</i> .....	558
12.6.4 <i>ARP Table</i> .....	559
12.6.5 <i>Sessions Info</i> .....	560
12.6.6 <i>DHCP</i> .....	563

## 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. New model of Planet's UTM Content Security Gateway CS-2000, a special designed of security gateway, adopts Heuristics Analysis to filter spam and virus mail, auto-training system can raise identify rate of spam. The built-in 80GB Hard Disk can store the spam mail in Quarantine. Anti-virus has double virus scan engines - Clam and Sophos, can detect viruses, worms and other threats from E-mail transfer and Internet network. It also provides the mail report by Daily, Weekly, Monthly and Yearly, that helps the administrator easy to monitor the mail status.

The CS-2000 not only can filter spam and virus mail, the IDP and firewall functions can defense hacker and blaster attack from Internet or Intranet. The completely function in one device can provide you an excellent security solution and the secure environment than ever.

The CS-2000 not only just provides the same features as previous product CS-1000, such as Content Blocking to block specific URL, Scripts, IM/P2P program, IPSec, PPTP VPN server/Client, QoS and Authentication etc, but also provides the higher performance than CS-1000 and has more advanced functions, such as SSL VPN, High Availability and Inbound Load-Balancing etc. Built-in two WAN interfaces allow CS-2000 to support Outbound/Inbound load balance and wan fail-over feature. Furthermore, the VPN Trunk provides VPN fail-over and load balance features, that can offer a VPN redundant mechanism to keep your VPN connection being on line.

### 1.1 Features

- **Anti-Spam Filtering:** Multiple defense layers (Spam Fingerprint, Blacklist & Whitelist, Bayesian Filtering, Spam Signature, Graylist, Checking sender account and IP address in RBL), 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, Forward and Store in the quarantine. Built-in auto-training system to rise identify rate of spam mail substantially.
- **Anti-Virus Protection:** Built-in double virus scan engines can detect viruses, worms, and other threats from email transfer. Scan mission-critical content protocols-SMTP, POP3 in real time as traffic enters the network to provide maximum protection. Customizable notification options and virus mail report are provided for administrator. Varied actions toward spam mail include: Delete, Deliver, Forward and Store in the quarantine.
- **Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS:** The CS-2000 not only can provide Anti-virus feature for mail, it also can filter the virus from varied protocol. The virus pattern can be updated automatically or manually.
- **VPN Connectivity:** The CS-2000 supports several VPN features -- IPSec VPN, SSL VPN and PPTP server/client. The VPN Tunnel with DES / 3DES / AES encryption and SHA-1 / MD5 authentication that provide secured network traffic over public Internet. VPN Wizard can help administrator to have an easy way to configure VPN settings.
- **SSL VPN:** SSL VPN does not need to install any software or hardware. Only need to use the web browser and easily establish VPN connections for transferring the data by SSL encryption.

- **VPN Trunk:** VPN trunk function provides VPN load balance and VPN fail-over feature to keep the VPN connection more reliable.
- **Content Filtering:** The CS-2000 can block network connection based on **URLs**, **Scripts** (The Pop-up, Java Applet, cookies and Active X), **P2P** (eDonkey, Bit Torrent, WinMX and more), **Instant Messaging** (MSN, Yahoo Messenger, ICQ, QQ, Skype and Google Talk) and **Download / Upload**. If there are new updated version of P2P or IM software in client side, CS-2000 will detect the difference and update the Content Filtering pattern to renew the filtering mechanism.
- **IDP:** Built-in IDP function can detect and prevent the Hacker attacks, Anomaly Flow, and Signatures from Internet. CS-2000 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.
- **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including SYN attack, ICMP flood, UDP flood, Ping of Death, etc. The access control function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- **QoS:** Network packets can be classified based on IP address, IP subnet and TCP/UDP port number and give guarantee and maximum bandwidth with three levels of priority.
- **User Authentication:** Web-based authentication allows users to be authenticated by web browser. User database can be configured on the devices; CS-2000 also supports the authenticated database through external RADIUS, POP3 and LDAP server.
- **WAN Backup:** The CS-2000 can monitor each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including "Auto", "Round-Robin", "By Traffic", "By Session" and "By Packet". User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- **Inbound Load Balancing:** The CS-2000 provides the Inbound Load Balancing for enterprise's internal server. The Inbound Load Balancing can reduce the server loading and system crash risks, in order to improve the server working efficiency.
- **Multiple NAT:** Multiple NAT allows local port to set multiple subnet works and connect to the Internet through different WAN IP addresses.
- **High Availability:** The CS-2000 provides High Availability function, and the redundant system will avoid influencing the network traffic because of the device crash down.

## 1.2 Package Contents

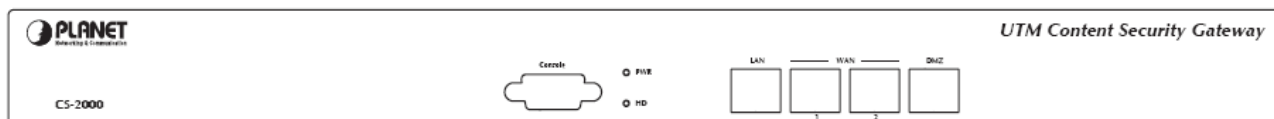
The following items should be included:

- CS-2000 x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Power cord x 1
- Console cable x 1
- Cat5 Cable x 3
- Cat5 Cross Cable x 1
- Rack-mount ear x 2
- Mat x 4

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

## 1.3 CS-2000 Front View

### CS-2000 Front Panel



### LED / Port Definition

LED / Port	Description	
<b>PWR</b>	Power is supplied to this device.	
<b>HD</b>	Blinks to indicate this device is being to access the Hard Disk.	
<b>Console</b>	Connect this serial port by console cable which setting is <b>9600, 8, N, 1</b> and <b>none flow control</b> . You can check the interface setting and reset to factory setting.	
<b>WAN1, WAN2, LAN, DMZ</b>	Orange	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
	Green	Steady on indicates the port is connected at 100Mbps speed

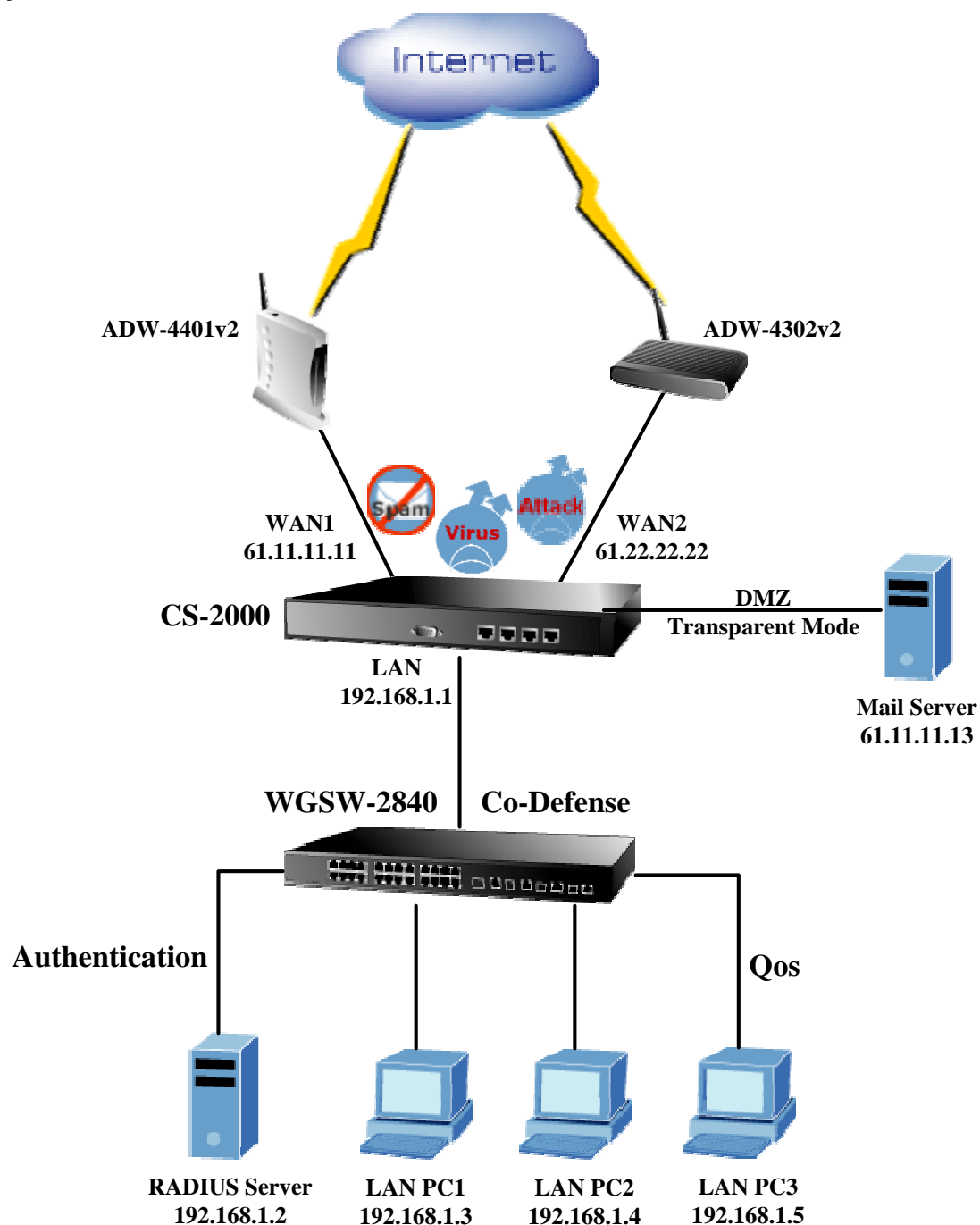
## 1.4 Specification

Product		UTM Content Security Gateway
Model		CS-2000
Hardware		
Ethernet	LAN	1 x 10/100 Based-TX RJ-45
	WAN	2 x 10/100 Based-TX RJ-45
	DMZ	1 x 10/100 Based-TX RJ-45
Console		1 x RS-232 (DB9)
Hard Disk		80 GB
H/W Watch-Dog		Auto reboot when detecting system fail
Software		
Management		Web (English, Traditional Chinese, Simplified Chinese)
Operation Mode		DMZ_Transparent, DMZ_NAT, NAT
Routing Protocol		Static Route, RIPv2
Concurrent Sessions		582,000
New session / second		20,000
Email Capacity per Day		600,000
Firewall Performance		100Mbps
VPN Performance		46Mbps
VPN 3DES Performance		30Mbps
Firewall Security		Policy-based access control Stateful Packet Inspection (SPI) NAT / NAPT

VPN Tunnels (Connection/Configure)	200 / 1000
VPN Function	IPSec, SSL VPN, PPTP server and client DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN
Content Filtering	URL Blocking Script Blocking (Popup, Java Applet, cookies and Active X) IM blocking (MSN, Yahoo Messenger, ICQ, QQ, Skype and Google Talk) P2P blocking (eDonkey, Bit Torrent, WinMX and more) Download and Upload blocking
IDP	Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS Automatic or manual update virus and signature database Anomaly: Syn Flood, UDP Flood, ICMP Flood and more Pre-defined: Backdoor, DDoS, DoS, Exploit, NetBIOS and Spyware Custom: User defined based on TCP, UDP, ICMP or IP protocol Yearly, Monthly, Weekly and Daily Report support
Anti-Virus	Virus scan engine: Two scan engines - Sophos and Clam Email attachment virus scanning by SMTP, POP3 Inbound scanning for internal and external Mail Server Action of infected mail: Delete, Deliver to the recipient, forward to an account and store in quarantine Automatic or manual update virus database
Anti-Spam	Inbound scanning for external and internal Mail Server Support Spam Fingerprint, Bayesian, Signature, RBL and Graylist filtering, checking sender account and IP to filter the spam mail Black list and white list support auto training system Action of spam mail: Delete, Deliver to the recipient, forward to an account and store in quarantine Yearly, Monthly, Weekly and Daily Report support
QoS	Policy-based bandwidth management Guarantee and maximum bandwidth with 3 priority levels Classify traffics based on IP, IP subnet, TCP/UDP port
User authentication	Built-in user database with up to 500 entries Support local database, RADIUS, POP3 and LDAP authentication
Logs	Traffic Log, Event Log and Connection Log Log can be saved from web, backup by e-mail or syslog server
Accounting Report	Record Inbound and Outbound traffic's utilization by Source IP, Destination IP and Service Backup Accounting Report for Outbound and Inbound traffic
Statistics	WAN Ports traffic statistic and policies statistic with graph display
Others	Dynamic DNS NTP support Multiple Server load balancing Outbound / Inbound load balancing High Availability Multiple Subnet SNMP v1

## Chapter 2: Hardware Installation

### Deployment



The CS-2000 appliance deployment

■ The CS-2000 interface in details:

LAN Port= 192.168.1.1

WAN 1 Port= 61.11.11.11

WAN 2 Port= 61.22.22.22

DMZ Port= 61.11.11.13

The CS-2000's Web UI contains two panes. The right pane is an "operation window". At the top of the "operation window" is a bar that shows Main Function → Sub Function and under the bar is a "working window." The left pane is the "function column" which depends on the function that user select in the left pane, the right pane displays the CS-2000 status and existing settings for MIS engineer to control and manage.

Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			Modify Remove Pause	To 1
test1	Outside_Any	ANY			Modify Remove Pause	To 2
Inside_Any	*CNC	RIP			Modify Remove Pause	To 3

New Entry

The CS-2000 appliance Web UI



## Chapter 3: System

### 3.1 Administration

Generally speaking, the system administration refers to the privileges of log in/out, monitor and control the CS-2000 appliance with some relevant settings. In this Chapter, the system administration will be defined as the management of the **MIS engineer**, **Permitted IPs**, **System Log-Out** and **Software Update**.

Chief administrator configures and manages the CS-2000 appliance. The administrator can add, delete or modify system settings and monitor system status while sub-administrator (title named set by chief MIS engineer) is read-only.

## Administrator

### Administrator:

- The title of chief administrator and sub administrator. Administrator is the default name and cannot be removed. But other sub administrator can be modified or removed.



The default administrator **Account: admin; Password: admin**



The default chief administrator can add or modify the other admin to be the sub admin or chief admin; otherwise the other chief admin can modify its privilege to be the sub admin but can not be deleted. The CS-2000 appliance still force to reserve a chief admin.

### Privilege:

- Chief administrator has the **Write/Read/View** privilege. Administrator is allowed to modify the configurations, monitor the system status, and add or remove the other administrator.
- Sub administrator only has **Read** privilege. He is only allowed to view the system configuration.

### Password/New Password/Confirm Password:

- Can add or modify the password of chief / sub administrator.

### 3.1.1 Admin

**Step 1.** Click **Admin** → **New Sub-Admin**.

**Step 2.** In **Add New Sub Admin**, add the settings :

- **Sub Admin name:** sub\_admin.
- **Password:** 12345.
- **Confirm Password:** 12345.



If the admin select **Write Access and View Log & Report Privilege**, the new sub-admin becomes chief admin.

**Step 3.** Click **OK** for the user to log in, or click **Cancel** to cancel adding new sub admin.

Add New Sub Admin		
Sub Admin name	<input type="text" value="sub_admin"/>	(Max. 16 characters)
Password	<input type="password" value="...."/>	(Max. 16 characters)
Confirm Password	<input type="password" value="...."/>	(Max. 16 characters)
<input type="checkbox"/> Write Access		
<input type="checkbox"/> View Log & Report Privilege		

**Add new sub admin**

## Changing the Main/Sub-Administrator's Password

**Step 1.** In **Admin**, select the admin to change, correspond to the **Configure**→ **Modify**.

**Step 2.** In **Modify Admin Password** , enter the following information:

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

**Step 3.** Click **OK** to change the password, or click **Cancel** to cancel the modification.

Modify Admin Password	
Admin Name	admin
Password	<input type="password"/> (Max. 16 characters)
New Password	<input type="password"/> (Max. 16 characters)
Confirm Password	<input type="password"/> (Max. 16 characters)
<input checked="" type="checkbox"/> Write Access	
<input checked="" type="checkbox"/> View Log & Report Privilege	

**Modify the admin password**

### 3.1.2 Permitted IPs

**Step 1.** In **Administration** → **Permitted IPs** → **New Entry**, add the settings :

- **Name** : Enter master
- **IP Address** : Enter 163.173.56.11
- **Netmask** : Enter 255.255.255.255
- **Service** : Check Ping, HTTP and HTTPS
- Click **OK**
- Complete adding **Permitted IPs**

Add New Permitted IPs	
Name	master (Max. 20 characters)
IP Address	163.173.56.11
Netmask	255.255.255.255
Service	<input checked="" type="checkbox"/> Ping / Traceroute <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Add new permitted IPs setting

Name	IP Address / Netmask	Ping / Traceroute	HTTP	HTTPS	Configure
master	163.173.56.11 / 255.255.255.255				<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Complete adding Permitted IPs



To activate Permitted IPs, click **Interface** → **LAN**, **WAN** and **DMZ** to uncheck **Ping**, **HTTP** and **HTTPS**.

However, **Permitted IPs** must be set before the cancellation of HTTP and HTTPS, or MIS engineer can not enter CS-2000's Web UI via the appointed interface.

### 3.1.3 Software Update

**Step1.** In **System→Administration→Software Update**

- In **Version Number**, to know the version number, then connect to network and download the latest version in the CS-2000 appliance.
- Click **Browse → Choose File**, select the latest update file and open it.
- Click **OK** to run automatic software update.

Software Update

Version Number :

v3.07.00

Software Update

C:\Documents and Setting

Browse

( ex: CS-2000\_030700.img )

OK

Cancel

Update the software



It takes 3 minutes to run software update then the system will restart. Please do not turn off the system or quit the web page during the update process, or it will cause an unpredictable error. (It recommends updating through LAN.)

## 3.2 Configure

The so called configuration here is about the basic operating settings of the CS-2000 appliance. In this Chapter, it will be defined as **Setting**, **Date/Time**, **Multiple Subnet**, **Route Table**, **DHCP**, **Dynamic DNS**, **Host Table**, **SNMP** and **Language**.

### Setting

#### Multi Security Firewall Configuration

- The MIS engineer can export or import system setting files, reset factory setting, and format the CS-2000's hard disk.

#### System Name Setting

- The administrator can set up the company name and device name.

#### E-mail Setting

- Enabling this function and the CS-2000 appliance will automatically send instant e-mail alert notification to the MIS engineer when the system is attacked or some urgent events occurred.

#### Web Management

- The MIS engineer can remote the CS-2000 appliance anywhere via Web UI. In addition, the MIS engineer can change the used port number in CS-2000's remote management.
- Set up the idle timeout as the MIS engineer log into the CS-2000 appliance. The CS-2000 appliance will forced to logout the Web UI as the MIS engineer did not process any system monitoring or management.



After changed HTTP or HTTPS port number, if the MIS engineer want to log in to Web UI from the WAN , he must change the web browser's port when log in to Web UI ( For example , <http://61.62.108.172:8080> and <https://61.62.108.172:1025> )

#### MTU Setting

- The MIS engineer can modify the length of the sent and received packets anytime. The default value is 1500 Bytes.

#### Scanned HTTP / FTP Setting

- Can set the file size to be scanned via HTTP and FTP.

#### Dynamic Routing (RIPv2)

- By enable LAN, WAN or DMZ Port to send and receive RIPv2 packets, the CS-2000 appliance can communicate with internal or external routers and dynamically update the route table. (The MIS engineer can set up routing information update timer and routing information timeout when it stop to receive the RIPv2 packets and the router will automatically cancel the dynamic routing table.)

#### SIP Protocol pass-through

- If enable the function, all the SIP packets pass through the CS-2000 will be first processed then sent out.

#### Administration Packet Logging

- After enabled this function, the system will record its packet information in **Monitor → Log → Traffic** for the MIS engineer to query.

### Date / Time:

#### Synchronize System Clock

- Synchronize the CS-2000 appliance time to the MIS engineer's PC or the external time server.

#### GMT

- International Standard Time (Greenwich Mean Time)

#### Daylight saving time :

- Daylight saving time (also called DST or Summer Time) is the portion of the year in which a region's local time is advanced by (usually) one hour from its standard official time.

### Multiple Subnet:

#### WAN Interface IP

- The WAN interface IP which a multiple subnet corresponds to.

#### Forwarding Mode

- To indicate the multiple subnet use NAT or Routing mode.

#### Interface

- To indicate the multiple subnet interface is LAN or DMZ interface.

#### Alias IP of Interface/Netmask

- The multiple subnet segment range.

#### NAT Mode

Allow the internal network to set up multiple subnet addresses and connect to network via different WAN IP addresses. For example, the company applies several real IP addresses 168.85.88.0/24 for its lease



line and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. For easy management, assign different IP segment for each department. The settings are as the following:

<b>R&amp;D Dep.</b>	<b>192.168.1.1/24 (Internal) ↔ 168.85.88.253(External)</b>
<b>Customer Service Dep.</b>	<b>192.168.2.1/24 (Internal) ↔ 168.85.88.252(External)</b>
<b>Sales Dep.</b>	<b>192.168.3.1/24 (Internal) ↔ 168.85.88.251(External)</b>
<b>Procurement Dep.</b>	<b>192.168.4.1/24 (Internal) ↔ 168.85.88.250(External)</b>
<b>Accounting Dep.</b>	<b>192.168.5.1/24 (Internal) ↔ 168.85.88.249(External)</b>

**R&D Dep.** has already been set up in **Interface** configurations, so set up the reserving four departments by adding 4 new Multiple Subnets. After completing the settings, every department can connect to network via its own WAN IP address. The settings of each department are as the following:

	Customer Service	Sales	Procurement	Accounting
<b>IP Address</b>	192.168.2.2~254	192.168.3.2~254	192.168.4.2~254	192.168.5.2~254
<b>Netmask</b>	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
<b>Default Gateway</b>	192.168.2.1	192.168.3.1	192.168.4.1	192.168.5.1

### Routing Mode

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

## DHCP

### Subnet

- The domain belongs to internet network.

### Netmask

- The domain name netmask belongs to the internet network.

### Gateway

- Internal network default gateway.

### Broadcast

- LAN broadcast address.

## Dynamic DNS

### Domain Name

- The domain name that the MIS engineer applied from the DDNS provider.

### WAN IP

- The real IP which the domain name correspond to.

## Host Table

### Host Name


- Customized by the MIS engineer. The internal user can access the resources provided by a corresponded host.

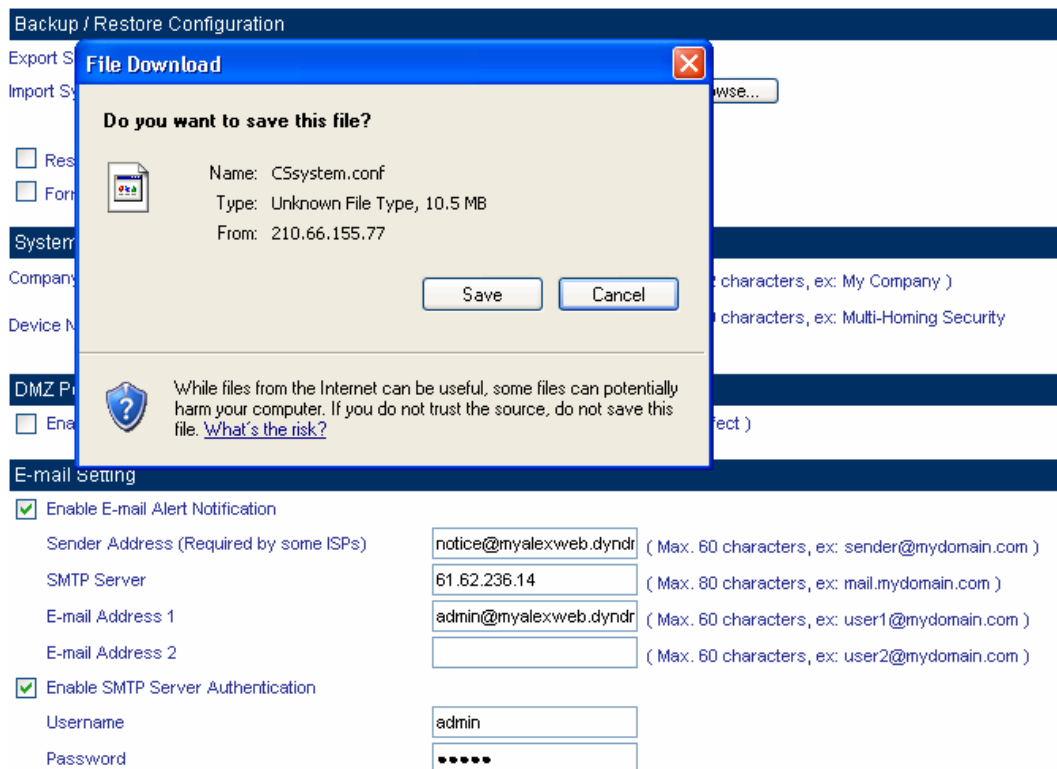
### Virtual IP Address

- The mapped virtual IP Address corresponds to the host name. It must be the LAN or DMZ IP address.

### 3.2.1 Setting

#### Exporting CS-2000 settings

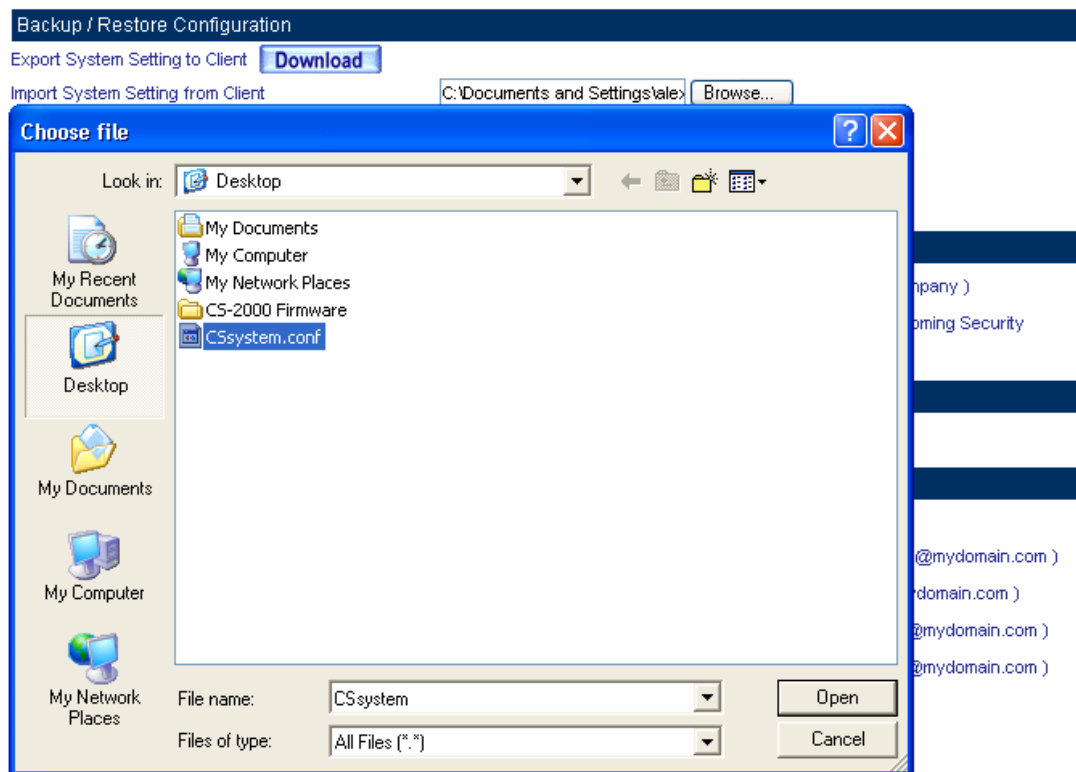
- Step1.** In **System→Configure→Setting →Multi Security Firewall Configuration**, click  near **Export System Setting to Client**.
- Step2.** In **File Download** window, click **Save**. Then, choose the destination location to save the exported file. Finally, click **Save** for CS-2000 to copy the configuration file to the appointed storage location.



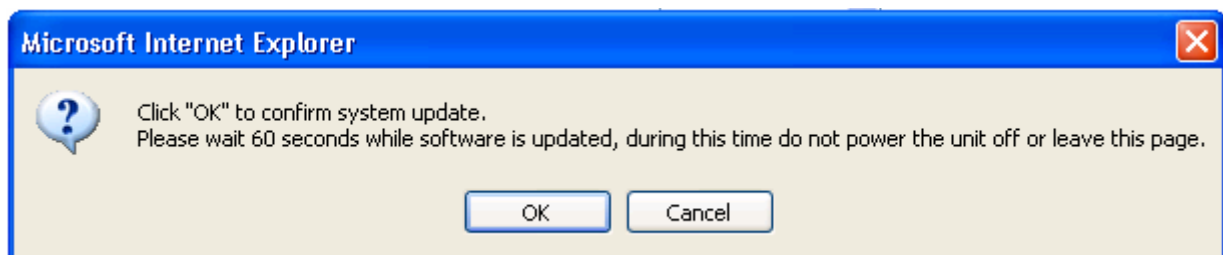
**Choose the save location**

## Importing CS-2000 settings

- Step1.** In **Setting** window, click **Browse** near **Import System Setting from Client**.
- Step2.** In **Choose File** window, select the previously saved settings and click **Open**.
- Step3.** Click **Open**, and a confirmation dialogue box pop out.
- Step4.** Click the **OK** to import the configuration file.



Imported the files

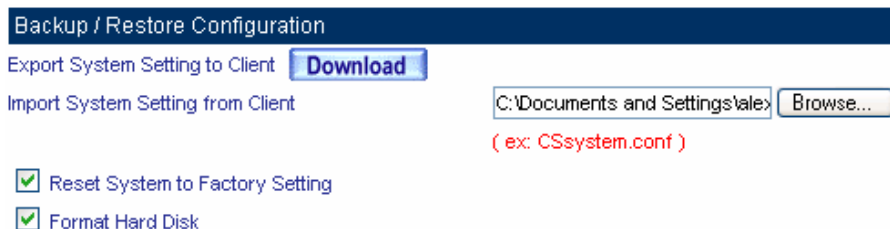


File import confirmation

## Restoring Factory Settings and Format Hard Disk

**Step1.** In **Setting → Backup/Restore Configuration**, select **Restore Factory Setting** and **Format Hard Disk**.

**Step2.** Click **OK** to restore the default settings and format the hard disk at the same time.



Backup / Restore Configuration

Export System Setting to Client [Download](#)

Import System Setting from Client  [Browse...](#)

( ex: CSsystem.conf )

☒ Reset System to Factory Setting

☒ Format Hard Disk

Select reset factory setting

## System Name Setting and Email Setting

- Step1.**      **Company Name:** Enter the unit name which the CS-2000 appliance objects to.
- Step2.**      **Device Name:** Enter the title name of the CS-2000 appliance.
- Step3.**      In **E-Mail Setting**→**Enable Email Alert Notification**.
- Step4.**      **Sender Address:** Enter the sender's email address. (Required by some ISP).
- Step5.**      **SMTP Server:** Enter the IP address of the SMTP server.
- Step6.**      **E-mail Address 1:** Enter the first e-mail address to receive the notification.
- Step7.**      **E-mail Address 2:** Enter the second e-mail address to receive the notification.
- Step8.**      Click **OK** to enable this function.

System Name Setting	
Company Name	alex ( Max. 32 characters, ex: My Company )
Device Name	Multi Security Firewall ( Max. 30 characters, ex: Multi-Homing Security Gateway )

DMZ Port Switch	
<input type="checkbox"/>	Enable DMZ port switch to WAN port ( System will reboot for the new setting to take effect )

E-mail Setting	
<input checked="" type="checkbox"/>	Enable E-mail Alert Notification
Sender Address (Required by some ISPs)	notice@myalexweb.dyndr ( Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	61.62.236.14 ( Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	admin@myalexweb.dyndr ( Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	( Max. 60 characters, ex: user2@mydomain.com )
<input checked="" type="checkbox"/>	Enable SMTP Server Authentication
Username	admin
Password	.....
Mail Test	<b>Mail Test</b>

### Enable email alert notification



Click **Mail Test** to test if e-mail address 1 and e-mail address 2 can receive the notification or not.



If the MIS engineer wants to send the mails via the authentication, then he must **enable SMTP Server**

**Authentication.**

## Web Management (WAN Interface)

The administrator can change the port number used by HTTP port anytime. (Remote WebUI management)



After HTTP and HTTPS port have changed, if the administrator want to enter WebUI from WAN, will have to change the port number of browser. (For example: http://61.62.108.172:8080)

**Step 1. Set Web Management (WAN Interface).** Enter the new port number used by HTTP and HTTPS port. ( Range 1 – 65535 )

**Step 2.** Click **OK** at the bottom-right of the screen.

Web Management	
HTTP Port	<input type="text" value="80"/> ( Range: 1 - 65535 )
HTTPS Port	<input type="text" value="443"/> ( Range: 443 or 1025 - 65535 )
Idle Timeout	<input type="text" value="0"/> Minutes ( Range: 0 or 5 - 1440, 0 : no timeout )

### Web Management

## MTU (set networking packet length)

The administrator can modify the networking packet length.

**Step 1. MTU Setting.** Modify the networking packet length. ( Range 40 – 1500 )

**Step 2.** Click **OK** at the bottom-right of the screen.

MTU Setting	
MTU	<input type="text" value="1500"/> Bytes ( Range: 40 - 1500 )

### MTU Setting

## Dynamic Routing (RIPv2)

Enable Dynamic Routing (RIPv2), CS-2000 will switch the routing information of RIP. The routers which support RIP can connect automatically. You can choose to enable LAN, WAN1, WAN2 or DMZ interface to allow RIP protocol supporting.

**Routing information update timer:** CS-2000 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-2000 does not receive the RIP protocol from the other router in a period of time, CS-2000 will cut off the routing automatically until it receives RIP protocol again. The default timer is 180 seconds.

Dynamic Routing (RIPv2)	
Enable	<input type="checkbox"/> LAN <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> DMZ
Routing information update timer	<input type="text" value="30"/> Seconds ( Range: 5 - 99999 )
Routing information timeout	<input type="text" value="180"/> Seconds ( Range: 5 - 99999 )

### Enable Dynamic Routing

## SIP protocol pass-through

Select this option to the device's **SIP protocol pass-through**. Once this function is enabled, the SIP packets will be allowed to pass-through via CS-2000.

### SIP protocol pass-through

☒ Enable SIP protocol pass-through

[Enable SIP protocol pass-through](#)

## To-Appliance Packets Log

Select this option to the device's **To-Appliance Packets Log**. Once this function is enabled, every packet to this appliance will be recorded for system administrator to trace.

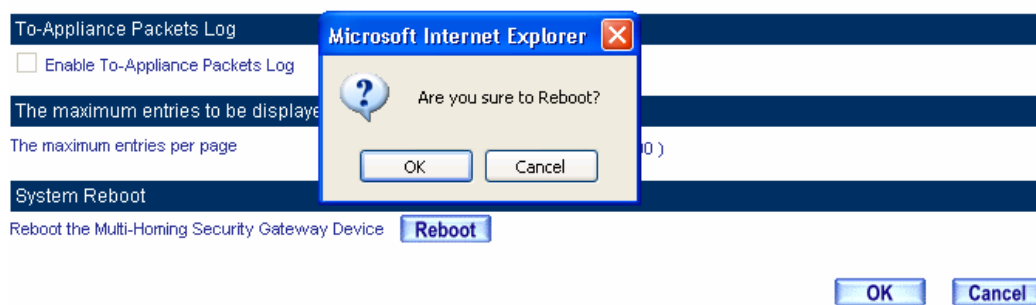
### To-Appliance Packets Log

☒ Enable To-Appliance Packets Log

[Enable To-Appliance Packets Log](#)

## System Reboot

- Step1.** To restart the CS-2000 appliance, Click **Reboot** near **Reboot Multi Security Firewall Appliance**.
- Step2.** It shows the confirm dialogue of **Are you sure to reboot?**
- Step3.** Click **OK** to restart, or click Cancel to terminate the action.



[Start to reboot](#)



### 3.2.2 Date/Time

- Step1.** To select **Enable synchronize with an Internet time Server**.
- Step2.** In **Set offset hours from GMT**, select the correct option.
- Step3.** Enter the time server's IP address in **Server IP / Name**.
- Step4.** Enter the update time.

System time : Tue Jul 3 15:38:26 2007

#### Synchronize system clock

☒ Synchronize system clock with an Internet time server

Set offset  hours from GMT [Assist](#)

☐ Enable daylight saving time setting

From  /  To  /

Server IP / Name  [Assist](#)

Update system clock every  minutes ( Range: 1 - 99999, 0: system clock updates at boot up )

Synchronize system clock with this client

**Sync**

**OK**

**Cancel**

#### Set the system clock



Click **Sync** near **Synchronize system clock with this client**, to synchronize the CS-2000 time to the MIS engineer's PC.



Click **Assist** near Set Offset from GMT or Server IP / Name to consult the setting value.

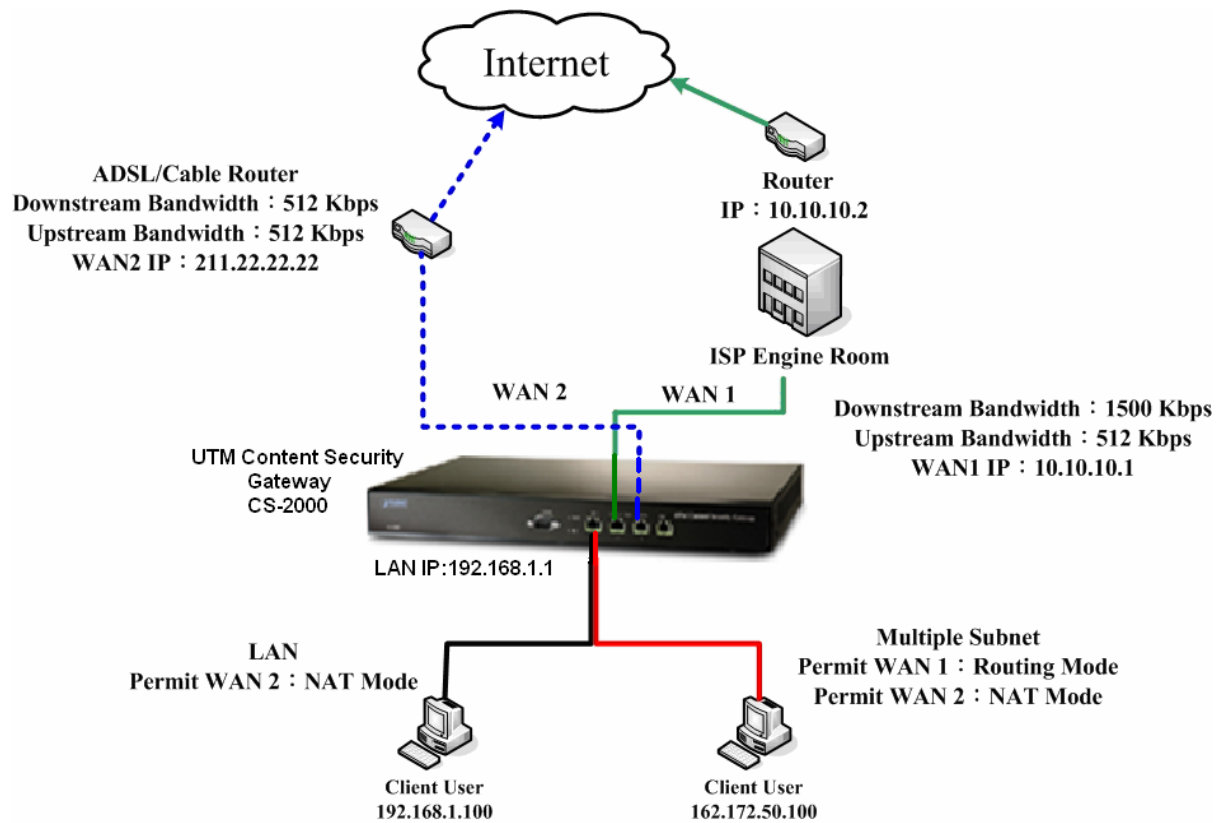
### 3.2.3 Multiple Subnet

Internal users use the IP address to link the internet via the multiple subnet NAT or Routing mode.

#### Exercise Preparations

Connect the CS-2000 appliance WAN 1(10.10.10.1) to the ISP's Router(10.10.10.2). The segment is 162.172.50.0/24 (Distributed by the ISP.)

Connect the CS-2000's WAN 2 (211.22.22.22) to ATUR to link to the network.



#### Multiple subnet deployment

##### ■ The CS-2000 Interface:

WAN1 IP : 10.10.10.1  
 WAN2 IP : 211.22.22.22  
 LAN Port IP : 192.168.1.1  
 LAN Port Multiple Subnet : 162.172.50.1

## Add a Multiple Subnet with Routing Mode:

**Step1.** Click **Configure → Multiple Subnet**

- Click **New Entry**.
- **Interface** : select **LAN**
- **Alias IP of Interface** : enter 162.172.50.1
- **Netmask** : enter 255.255.255.0
- **WAN 1**: 10.10.10.1 , **Forwarding Mode** : select routing
- **WAN 2**: 211.22.22.22 , **Forwarding Mode** : select NAT
- Click **OK**.
- Complete to add new multiple subnet IP.

Add New Multiple Subnet IP			
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
Alias IP of Interface	<input type="text" value="162.172.50.1"/>		
Netmask	<input type="text" value="255.255.0.0"/>		
WAN Interface IP			Forwarding Mode
WAN1	<input type="text" value="0.0.0.0"/>	<a href="#">Assist</a>	<input type="radio"/> NAT <input checked="" type="radio"/> Routing
WAN2	<input type="text" value="211.22.22.22"/>	<a href="#">Assist</a>	<input checked="" type="radio"/> NAT <input type="radio"/> Routing
WAN3	<input type="text" value="0.0.0.0"/>	<a href="#">Assist</a>	<input type="radio"/> NAT <input type="radio"/> Routing

Add new multiple subnet



Can enter the interface IP of **WAN 1** & **WAN 2** by **Assist**.



After completed the settings, there are two LAN segment 192.168.1.0/24 (the default LAN segment) and 162.172.50.0/24. Therefore, if the LAN IP is:

- 192.168.1.xx –Use the NAT Mode to connect to the network (As regulated in **Policy**, one can only connect to network via WAN2. If use Routing mode via WAN 1, an virtual IP can't be used to connect to network).
- 162.172.50.xx—WAN 1: Routing mode (MIS engineer IP 162.172.50.xx can be seen by the internet server ) ; WAN2: NAT mode (The IP seen by the internet server is WAN2's IP)

### 3.2.4 Route Table

Make the Router which deploy in two different segments can link to the internet via the CS-2000 appliance.

#### Preparations

##### Company A

Connect WAN 1 ( 61.11.11.11 ) to ATUR and link to network.

Connect WAN 2 ( 211.22.22.22 ) to ATUR and link to network.

LAN segment is 192.168.1.1/24.

LAN Router1 ( 10.10.10.1, supporting RIPv2 ) , the LAN segment is 192.168.10.1/24.


##### Company B



Router2 ( 10.10.10.2, supporting RIPv2 ) , the LAN segment is 192.168.20.1/24.

Company A's Router1 ( 10.10.10.1 ) is connected to B company's Router2 ( 10.10.10.2 ) by lease line directly.

**Step1. In Configure → Route Table**


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



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

**Add new static route—1****Step2. In Configure → Route Table**

- **Destination IP**: Enter 192.168.20.1
- **Netmask**: Enter 255.255.255.0
- **Gateway** : Enter 192.168.1.252
- **Interface** : Select **LAN** .
- Click **OK**


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



 

**Add new static route—2**

**Step3.** In **Configure → Route Table**

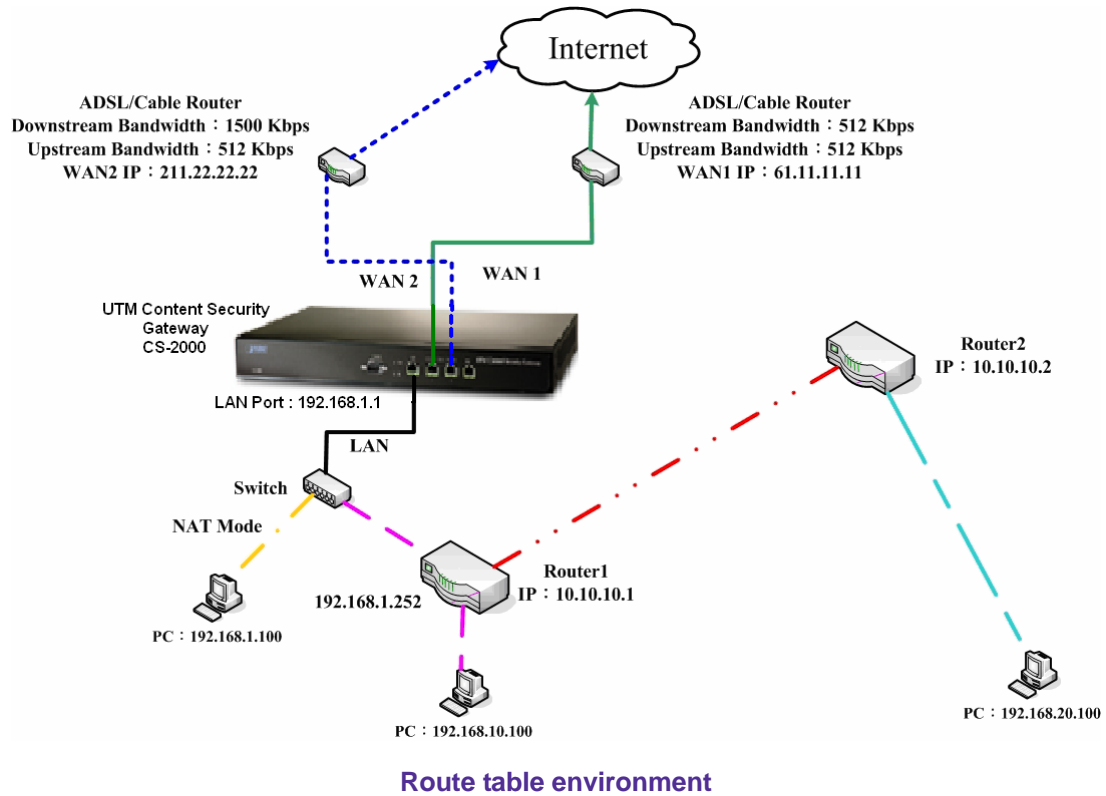
- **Destination IP:** Enter 10.10.10.0
- **Netmask:** Enter 255.255.255.0
- **Gateway:** Enter 192.168.1.252
- **Interface:** Select **LAN**.
- Click **OK**

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

**Fig. 2-12 Add new static route-- 3**

**Step4.** As completed all. The CS-2000 appliance can translate the virtual IP to real IP. Therefore, the LAN subnet PC 192.168.10.1/24, 192.168.20.1/24 and 192.168.1.1/24 can communicate to each other via the CS-2000 appliance.





### 3.2.5 DHCP

**Step1.** In **Configure → DHCP** , to select and set the following setting:

- **Domain Name:** Enter the domain name in private LAN.
- **DNS Server 1:** Enter the IP address distributed to DNS server 1.
- **DNS Server 2:** Enter the IP address distributed to DNS server 2.
- **WINS Server 1:** Enter the IP address distributed to WIN server 1.
- **WINS Server 2:** Enter the IP Address distributed to WIN server 2.
- **LAN Interface:**
  - ◆ Client IP range 1: Enter the first starting and ending IP addresses, the default value is 192.168.1.2 to 192.168.1.254. (it must be at the same domain).
  - ◆ Client IP range 2: Enter the second starting and ending IP addresses (it must be at the same domain as Client Range 1).
- **DMZ Interface:** Set as the LAN interface address. (Except to enable **DMZ Interface**, click **Interface→DMZ.**)
- **Leased Time:** The lease time of the dynamic IP and the default value is 24 hours.
- Click **OK**.
- Complete **DHCP** settings.

Dynamic IP Address			
Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

---

☒ Enable DHCP Support

Domain Name  ( Max. 40 characters, ex: dhcp.domain\_name )

☐ Automatically Get DNS

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

LAN Interface :

Client IP Range 1  To

Client IP Range 2  To

DMZ Interface :

Client IP Range 1  To

Client IP Range 2  To

Lease Time  hours ( Range: 0 - 99999 )

### DHCP setting



When the LAN network adaptor set to **Automatically Get DNS**, the DNS Server will auto lock the LAN interface IP. (Note: When enabled the **Authentication**, the first DNS server must correspond to the LAN interface IP).

### 3.2.6 DDNS

**Step1.** In **Configure → DDNS**.





- Click **New Entry**.
- **Service Provider**: Select from the drop-down menu.
- Select **Automatically** and select a WAN interface to correspond from the menu.
- **User Name** and **Password**: Enter the applied name and password.
- **Domain Name**: Enter the applied domain name.
- Click **OK**.
- Complete **DDNS** setting.

Add New Dynamic DNS			
Service Provider :	DynDNS (www.dyndns.com) [ U.S.A. ] <span>Sign up</span>		
WAN IP:	61.62.236.15	<input checked="" type="checkbox"/> Automatically	WAN1
User Name :	alexten (Max. 59 characters)		
Password :	•••••• (Max. 44 characters)		
Domain Name:	myalexweb	dyndns.tv	(Max. 34 characters)

#### DDNS setting WebUI

i	Domain Name	WAN IP	Configure
	myalexweb.dyndns.tv	61.62.236.15	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete the DDNS setting

Icon				
Connotation	Connection Succeeds	Wrong Password	Connecting	Errors



If the MIS engineer have not apply the DDNS account, then he can choose the proper DDNS supplier, click **Sign up**, and then it will display the registration web page.



If the MIS engineer do not select **Automatically correspond to the WAN interface Address**, then they can enter the specific IP at **WAN IP**. It can let DDNS correspond to the static IP.

### 3.2.7 Host Table

**Step1.** In **Configure → Host Table**

- **Host Name** enter the customaries domain name
- **Virtual IP Address** enters the host name that corresponds to the virtual IP address.
- Click **OK**.
- Complete **Host Table** setting.

Modify Host Table Entry	
Host Name	<input type="text" value="www.fileserver.com"/> ( Max. 80 characters, ex: www.my_domain.com )
Virtual IP Address	<input type="text" value="192.168.1.10"/> ( ex: 192.168.100.102 )

**Host table setting**



Use the Host Table of the CS-2000 appliance, the first DNS Server in Client PC must correspond to the LAN or DMZ Port IP; that is the default gateway of the computer.

### 3.2.8 SNMP

**Step1.** In **Configure → SNMP → Enable SNMP Agent** and enter the following setting:

- **Appliance Name:** Can customize the name. Default setting is Multi Security Firewall.
- **Appliance Location:** Can customize the settings. Default setting is Taipei, Taiwan.
- **Community:** Can customize the settings. Default setting is public.
- **Contact Person:** Can customize the settings. Default setting is root@public.
- **Description:** Can customize the settings. Default setting is Multi Security Firewall Appliance.
- Click **OK**.
- Complete the **SNMP Agent** settings. The MIS engineer can monitor CS-2000'S operating status by the SNMP Agent message recipient installed in administrator's PC.

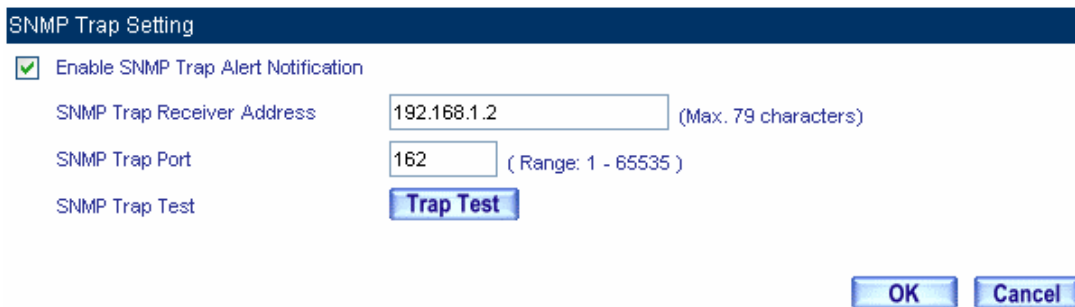
SNMP Agent Setting	
<input checked="" type="checkbox"/> Enable SNMP Agent	
Device Name	<input type="text" value="Multi Security Firewall"/> (Max. 255 characters)
Device Location	<input type="text" value="Taipei, Taiwan."/> (Max. 255 characters)
Community	<input type="text" value="public"/> (Max. 255 characters)
Contact Person	<input type="text" value="root@public"/> (Max. 255 characters)
Description	<input type="text" value="Multi Security Firewall Appliance"/> (Max. 255 characters)

#### SNMP agent setting

## Enable SNMP Trap Alert Notification

**Step1.** In **Configure → SNMP** , select **Enable SNMP Trap Alert Notification** and enter the following setting:

- **SNMP Trap Recipient Address:** enter SNMP trap recipient IP.
- **SNMP Trap Port:** Enter the port number. (Default value: 162).
- Click **OK**.
- Complete the **SNMP Trap** setting. The MIS engineer can use the SNMP Trap software and receive the alarm notification from the CS-2000 appliance. ( it will send the notification about connection / disconnection and the attacks information to the SNMP Trap recipient address.



### SNMP Trap setting WebUI



The MIS engineer can click  to test if SNMP Trap can work normally.

### 3.2.9 Language

**Step1.** In **Configure** → **Language** to select the language, click **OK**.

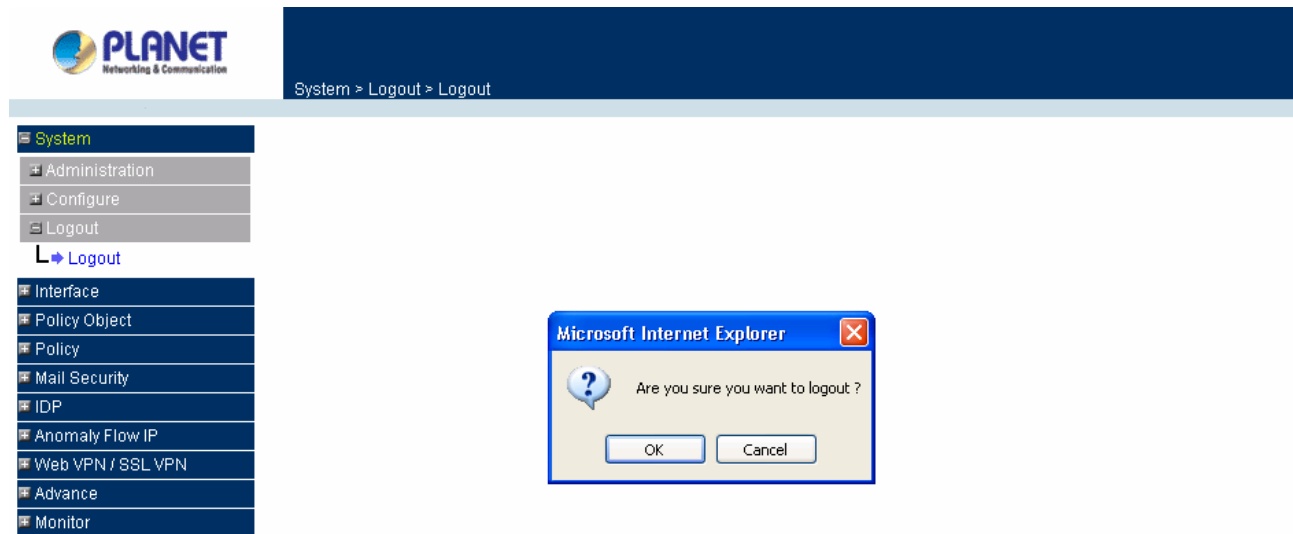


Language Version setting



### 3.3 Logout

**STEP 1** . Click **Logout** in **System** to protect the system while Administrator is away.



#### Confirm Logout WebUI

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

#### Multi-Homing Security Gateway Web Server Information

Your current connection has expired, you have now been logged out.  
If you want to login, please restart your browser.

#### Logout WebUI Message

## Chapter 4: Interface

# Interface

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

### Definition

#### Interface

##### LAN

- Can set up the LAN network.

##### Ping

- Can test the IP via Ethernet interface.

##### HTTP

- From the Ethernet interface to the CS-2000 WebUI through HTTP.

##### HTTPS

- From the Ethernet interface to the CS-2000 Web UI through HTTPS.

##### WAN

- Can set the external connection.

#### Balance Mode

- **Auto** : Can auto adjust the usage of WAN depends on the downstream and upstream status.
- **Round-Robin** : Forced to use the 1:1 cycling distribution of network download connection (it is appropriate to the users who use the same download bandwidth.)
- **By Traffic** : Allocate the download bandwidth by accumulated network flow.
- **By Session** : Adjust the WAN connection depends on the saturated connections.
- **By Packet** : Allocate the download bandwidth by accumulated packets.

### Connect Mode

- The WAN network connection mode can be divided into :
  - ◆ PPPoE (ADSL user )
  - ◆ Dynamic IP Address (cable modem user)
  - ◆ Static IP address (static connection or ADSL static line users )

### Saturated Connections

- Can set the WAN connections depend on the traffic, connections and packets.

### Priority

- Set the WAN interface priority by balance mode choice.

### Service

- To test if the WAN can work or not. The testing includes two parts:
  - ◆ ICMP : Ping the IP to see if the connection can work.
  - ◆ DNS : Use the domain name to see if the connection can work.

### Downstream Bandwidth and Upstream Bandwidth

- Can set the proper bandwidth of the WAN interface.

### The Idle Time

- As the WAN interface set to be the PPPoE (ADSL users) settings, the MIS engineer can set the idle time when the WAN port is not in use. (Its unit is minute)

### DMZ

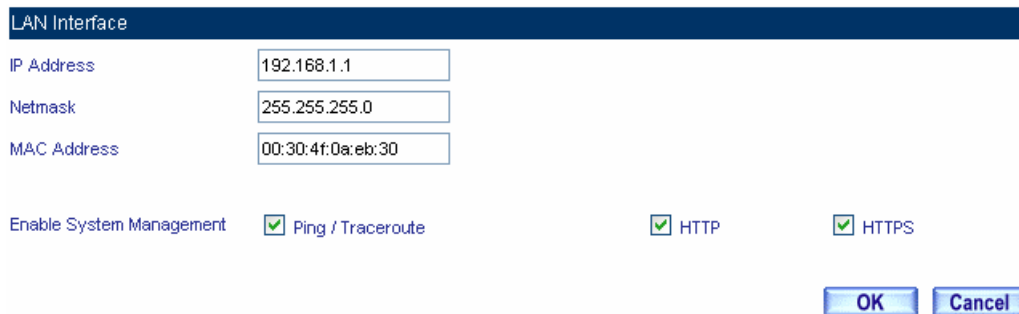
- Can set the DMZ in the CS-2000 appliance.
- The DMZ includes two modes:
  - ◆ NAT : The DMZ is an isolated virtual domain. (But it can not be at the same segment as LAN).
  - ◆ TRANSPARENT : The DMZ and WAN interface are both in the same domain.

## 4.1 LAN

### Modify the LAN Interface Address

**Step1.** In **Interface** → **LAN** to enter the following settings:

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



LAN interface setting



The default LAN interface address is 192.168.1.1. After the MIS engineer has modified the LAN IP address, he has to set the PC to obtain the latest IP, and then use the modified LAN interface IP address to log in Web UI. (When the PC set to obtain the IP by DHCP)



Before set the **Permitted IP**, never uncheck HTTP and HTTPS or the MIS engineer will not able to log in the CS-2000 Web UI via LAN.

## 4.2 WAN

### Set the WAN Interface Address

**Step1.** Interface → WAN, click Modify of WAN 1.



WAN 2/3 Interface's settings are almost the same as WAN 1 setting. The difference is that WAN 2/3 has the additional **Disable** function. The MIS engineer can use this function to disable WAN Interface 2/3.

WAN2 Interface		Enable	
Service :	DNS	Disable	
		Enable	
DNS Server IP Address :		168.95.1.1	<a href="#">Assist</a>
Domain name :		www.google.com.tw	<a href="#">Assist</a> (Max. 55 characters)

#### Disable the WAN interface

**Step2.** The way to test the connection (ICMP and DNS):

- ICMP: enter the persistent ping IP. (Or click **Assist**).
- DNS : Enter the DNS server IP address and domain name. (Or click **Assist**.)
- Sets the interval seconds during the packets transferring. (Per seconds).

WAN1 Interface	
Service :	ICMP
Alive Indicator Site IP :	61.64.127.16 <a href="#">Assist</a>
Wait	1 seconds between the sending of each alive packet. ( Range: 0 - 99 , 0: do not check )

#### ICMP connection test

WAN1 Interface	
Service :	DNS
DNS Server IP Address :	168.95.1.1 <a href="#">Assist</a>
Domain name :	www.google.com.tw <a href="#">Assist</a> (Max. 55 characters)
Wait	3 seconds between the sending of each alive packet. ( Range: 0 - 99 , 0: do not check )

#### DNS connection test



Both of the two connection test is the standard to see if the WAN can work properly. The testing such as the IP address, IP address for DNS server and the domain name all must be working forever long, or it will make the CS-2000 appliance error.

**Step3.** Choose the network connection.

■ **PPPoE (ADSL User)**

1. Select **PPPoE (ADSL User)**
2. Enter **User Name** as an account.
3. **Password** as the applied password.
4. Select **Dynamic** or **Fixed** in **IP Address provided by ISP**. It depends on the user's network status, click **Fixed** option, please enter the **IP address**.
5. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (※It depends on the network bandwidth which the user applied.)
6. Select **Ping**, **HTTP**, and **HTTPS**.
7. Click **OK**.

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

Current Status: Disconnected Connect  
 IP Address: 0.0.0.0 Disconnect  
 User Name: t0399199  
 Password:   
 IP Address obtained from ISP via: ☒ Dynamic ☐ Fixed  
 IP Address:   
 Netmask:   
 Default Gateway:   
 Max. Downstream Bandwidth: 2048 Kbps ( Range: 1 - 102400 )  
 Max. Upstream Bandwidth: 256 Kbps ( Range: 1 - 102400 )  
 Auto Disconnect if idle for 0 minutes ( Range: 1 - 99999, 0: means always connected )

### Use PPPoE

Balance Mode: Auto ( Auto recommended )

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping / Traceroute	HTTP	HTTPS	Configure	Priority
1	Static IP	61.62.236.15	2				Modify	1
2	Static IP	210.66.155.77	1			---	Modify	2
3	(Disable)	---	0	---	---	---	Modify	0

### To Complete PPPoE connection setting



If use the PPPoE, the MIS engineer can set the WAN interface auto connect when it disconnect (**it is recommended enable this function**) or set the WAN interface disconnect as idle (**Not Recommended**).

### ■ Dynamic IP Address ( cable modem user )

1. Click **Dynamic IP Address**.
2. Click **IP Address**→**Renew**, and then get the Dynamic IP.
3. If the ISP requires entering the MAC address, Click **MAC Address**→**Clone MAC**, then gets the MAC address.
4. **User Name** : Require by the ISP to enter the provided user name.
5. **Domain Name** : Require by the ISP to enter the provided domain name.
6. **Username** and **Password** :The IP mechanism of DHCP authentication.( According to the ISP in Mainland China )
7. Enter **Downstream Bandwidth** and **Upstream Bandwidth** (※ According to the bandwidth which applied by the user)
8. Select **Ping**, **HTTP** and **HTTPS**.
9. Click **OK**.

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

IP Address: 0.0.0.0 Renew Release  
 MAC Address: 00:30:4f:0A:EB:31 Clone MAC Address  
 Hostname:  (Max. 50 characters)  
 Domain Name:  (Max. 80 characters)  
 User Name (Required by DHCP+ protocol):  (Max. 127 characters)  
 Password (Required by DHCP+ protocol):  (Max. 127 characters)

Max. Downstream Bandwidth:  2048 Kbps ( Range: 1 - 102400 )  
 Max. Upstream Bandwidth:  256 Kbps ( Range: 1 - 102400 )

Enable System Management ☒ Ping / Traceroute ☒ HTTP ☒ HTTPS

OK Cancel

### Set the Dynamic IP address

Balance Mode :  Auto ( Auto recommended )

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping / Traceroute	HTTP	HTTPS	Configure	Priority
1	Dynamic IP	10.10.10.3	2				Modify	1
2	Static IP	210.66.155.77	1			---	Modify	2
3	(Disable)	---	0	---	---	---	Modify	0

### Complete to set the Dynamic IP address



## ■ Static IP address ( For Static or ADSL user )

1. Select **Static IP Address**.
2. Enter **IP Address**, **Netmask** and **Default Gateway**.
3. Enter **DNS Server 1** or **DNS Server 2**.
4. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth**. (※ According to the bandwidth applied by the user)
5. Select **Ping**, **HTTP** and **HTTPS**.
6. Click **OK**

☒ PPPoE (ADSL User)

☐ Dynamic IP Address (Cable Modem User)

☒ Static IP Address

IP Address	<input type="text" value="61.62.236.15"/>
Netmask	<input type="text" value="255.255.255.0"/>
MAC Address	<input type="text" value="00:30:4f:0a:eb:31"/>
Default Gateway	<input type="text" value="61.62.236.254"/>
DNS Server 1	<input type="text" value="168.95.1.1"/>
DNS Server 2	<input type="text"/>
Max. Downstream Bandwidth	<input type="text" value="2048"/> Kbps ( Range: 1 - 102400 )
Max. Upstream Bandwidth	<input type="text" value="256"/> Kbps ( Range: 1 - 102400 )
Enable System Management	<input checked="" type="checkbox"/> Ping / Traceroute <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

### Set the Static IP address

Balance Mode :  ( Auto recommended )

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping / Traceroute	HTTP	HTTPS	Configure	Priority
1	Static IP	61.62.236.15	<input type="text" value="2"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Modify"/>	<input type="text" value="1"/>
2	Static IP	210.66.155.77	<input type="text" value="1"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	---	<input type="button" value="Modify"/>	<input type="text" value="2"/>
3	(Disable)	---	<input type="text" value="0"/>	---	---	---	<input type="button" value="Modify"/>	<input type="text" value="0"/>

### Complete the Static IP address setting



In WAN 2 Interface, the MIS engineer has no need to set the DNS server as setting the Static IP address.



When selecting Ping, HTTP and HTTPS in WAN interface, the user can ping the CS-2000 appliance and it's WebUI. This action may cause the network security problem. It's recommended do not select the Ping, HTTP and HTTPS after confirming all the setting is completed. If the MIS engineer wants to log in to the WebUI through WAN, he can use **System → Administration → Permitted IPs**.

## 4.3 DMZ

### Sets DMZ Interface (NAT Mode)

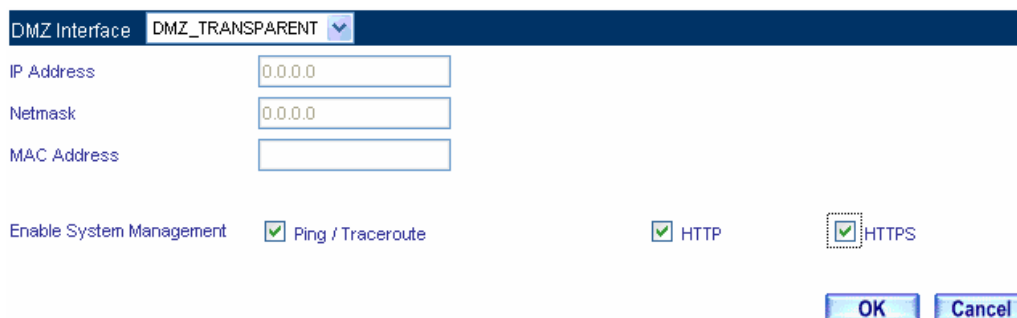
- Step1.** In **Interface** → **DMZ**.
- Step2.** In **DMZ Interface**, select **NAT** mode.
- In **DMZ Interface**, select **NAT** from the drop-down menu.
  - Enter the value in **IP Address** and **Netmask**.
- Step3.** Select **Ping**, **HTTP** and **HTTPS**.
- Step4.** Click **OK**

The screenshot shows a configuration window titled "DMZ Interface" with a dropdown menu set to "NAT". Below the title bar, there are three input fields: "IP Address" with the value "10.0.0.1", "Netmask" with the value "255.0.0.0", and "MAC Address" with the value "00:30:4f:0a:eb:33". At the bottom, there are four checkboxes: "Enable System Management" (unchecked), "Ping / Traceroute" (checked), "HTTP" (checked), and "HTTPS" (checked). The "HTTPS" checkbox is highlighted with a dashed border. At the bottom right, there are two buttons: "OK" and "Cancel".

Select the NAT mode

## Sets DMZ Interface (Transparent Mode)

- Step1.** In **Interface** → **DMZ**.
- Step2.** In **DMZ Interface**, select **Transparent Mode**.
- In **DMZ Interface**, select **DMZ\_ Transparent Mode** from the drop-down menu.
- Step3.** Select **Ping**, **HTTP**, and **HTTPS**.
- Step4.** Click **OK**



Select the DMZ\_TRANSPARENT mode



The MIS engineer has to set the static IP address in WAN interface and select the DMZ\_TRANSPARENT mode in DMZ interface.

## Chapter 5: Policy Object

### 5.1 Address

# Address

In this chapter, it includes the definition of the chief MIS engineer, LAN, LAN group, WAN, WAN group, DMZ and DMZ group.

The IP address recorded in **Address** is probably a host IP address, or represents many IP address in the Domain .The MIS engineer can set an easy to identify name to represent the IP address. Basically , the IP address can divided into three types : Internal IP address, WAN IP address and DMZ IP address. The MIS can apply the different IP address packets filtering rules to the same policy, he can set these IP address in LAN group, WAN group or DMZ group.



After finished the Address setting, the MIS engineer can apply the address setting to the policy (source address or destination address). In other words, the Address setting must be set before the policy setting, so that it can shows the correct IP Address in Address setting.

**Definition****Name**

- The MIS engineer can set the easy to identify name of IP address.

**IP**

- It can be a host IP address or one of the domain IP address. It included three different types: internal IP address, external IP address and DMZ IP address.

**Netmask**

- Correspond to the single static IP address, the setting must be: 255.255.255.255.
- Correspond to many IP address in a specific domain. For example, IP Address 192.168.100.1 in C Class segment, the setting must be 255.255.255.0.

**MAC Address**

- Mapped the MAC address to its IP address. It can prevent the user to modify the IP address and access the unauthorized network service through the policy.

**Get IP address from DHCP Server**

- When enable this function , LAN or DMZ will get the PC 's IP address via the DHCP server in the CS-2000 appliance, and the PC's IP address will correspond to the MAC address.

**We set two address application environments.**

<b>No.</b>	<b>Range</b>	<b>The Application Environment</b>	<b>Pages</b>
<b>Example 1</b>	<b>LAN</b>	When use the DHCP, to distribute the static IP address to the specific user and limit the user can only access the FTP resources through policy.	<b>53</b>
<b>Example 2</b>	<b>LAN Group and WAN</b>	To set the policy which allow part of users connect to the remote static IP address.	<b>56</b>

## Example 1

When use the DHCP, to distribute the static IP address to the specific user and limit the user can only access the FTP resources through policy.

**Step1.** In **Address→LAN** , make the setting as following :

- Click **New Entry**.
- **Name**, enter the user's identified name, Rayearth.
- **IP Address**, enter the user's IP 192.168.3.2.
- **Netmask**, enter 255.255.255.255.
- **MAC Address**, enter MAC Address 00:B0:18:25:F5:89.
- Select **Get static IP address from DHCP Server**.
- Click **OK**

Add New Address

Name	Rayearth	(Max. 16 characters)
IP Address	192.168.3.2	
Netmask	255.255.255.255	( 255.255.255.255 means the specified PC ) ( 255.255.255.0 means class C subnet )
MAC Address	00:30:4f:25:f5:89	<a href="#">Clone MAC Address</a>
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.		

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

### LAN address setting

Total entry : 2 [Assist add](#)

Name▼	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<a href="#">In Use</a>
Rayearth	192.168.3.2/255.255.255.255	00:30:4f:25:f5:87	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Complete the LAN address setting

**Step2.** In **Policy → Outgoing**, add the new settings :

Modify Policy	
Source Address	Rayearth
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )

To limit the single user accessing the network resources through specific service

**Step3.** In **Policy → Outgoing**, to complete the settings to appoint the static IP to the specific user and limit the user can only accessing FTP resources through policy.

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

[New Entry](#)

Complete the settings to limit the single user accessing the network resources through policy





When the MIS engineer set the Address settings , he can click **Clone MAC Address** , in order to let the CS-2000 can automatically copy the user's network adapter MAC address .



In **Address → LAN** , the CS-2000 appliance will automatically set an **Inside\_Any Address** , it represents the whole LAN . The WAN or DMZ also has its **Outside\_Any and DMZ\_Any** default address setting to represents its whole domain.



In **Address→WAN and DMZ**, the setting is the same as **LAN**. The only difference is that the WAN can not set the MAC address.

## Example 2

To set the policy which allow part of users connect to the remote static IP address.

**Step1.** Set many LAN address.

Total entry : 7 [Assist add](#)

Name▼	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Rayearth	192.168.3.2/255.255.255.255	00:30:4F:25:F5:89	<input type="button" value="In Use"/>
alex	192.168.1.5/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
jonas	192.168.1.4/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
eva	192.168.1.6/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
joe	192.168.1.9/255.255.255.255	00:30:4F:25:F5:45	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
james	192.168.1.15/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

To set the LAN address

**Step2. In Address → LAN Group**, to set the setting as following.

- Click **New Entry**.
- To set the group **Name**.
- In available address, select the user in the group and click **Add**.
- Click **OK**.

Add New Address Group

Name:  (Max. 16 characters)

<--- Available address --->

- Rayearth
- alex
- jonas
- eva
- joe
- james

Remove

Add

<--- Selected address --->

- alex
- jonas
- eva
- joe

OK Cancel

### To group the LAN address

Total entry : 1

Name▼	Member	Configure
Test_Team	alex, jonas, eva...	Modify Remove Pause

New Entry

### Complete the LAN group setting



In Address→**WAN Group** and **DMZ Group**, the setting is the same as LAN Group.

**Step3.** In **Address** → **WAN** , add the setting as following

- Click **New Entry**
- Enter the remote static IP information. ( **Name** , **IP** , **Netmask** )
- Click **OK**

Add New Address		
Name	<input type="text" value="yahoo"/>	(Max. 16 characters)
IP Address	<input type="text" value="202.1.237.21"/>	
Netmask	<input type="text" value="255.255.255.255"/>	( 255.255.255.255 means the specified PC )
( 255.255.255.0 means class C subnet )		

### Set the WAN address

Name▼	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
yahoo	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the WAN address setting

**Step4.** To apply **Step 1~3** to policy.

Add New Policy	
Source Address	Test_Team
Destination Address	yahoo
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 kBytes ( Range: 0 - 999999 )

#### Apply the address setting to policy

Source	Destination	Service	Action	Option					Configure			Move
Test_Team	yahoo	ANY							Modify	Remove	Pause	To 1

[New Entry](#)

#### Complete the policy setting



The Address function works by apply it to policy.

## 5.2 Service

# Service

The TCP Protocol and UDP Protocol can provide different services and every service has its TCP port or UDP port number. For example , TELNET(23) , FTP(21), SMTP(25) , POP3(110) , and so on . The Service function includes two parts: Pre-defined and Custom.

The Pre-defined included the common used and pre-identified TCP service or UDP service .This kind of service can not be modified and canceled. On the other hand, the user can set the proper TCP and UDP port number in Custom Service function. When sets the Custom Service function, the Client port number range is 1024 to 65535; the server port is 0 to 65535.

In this chapter, we will introduce the three common use services, for example, Pre-defined, Custom and Group. The MIS engineer can define the Protocol and port number in every network applied communication by the following steps. The client port can transfer the data by using different server.







How to use the Service ?

In **Service** → **Group**, the MIS engineer can add the new group name. In the Group function, the MIS engineer can simply many process when setting the policy. For example, there are 10 different IP address to access 5 different services via the server, for example, such as the HTTP, FTP, SMTP, POP3 and TELNET. If the MIS engineers do not use the Group function, he has to set 50 policies ( $10 \times 5 = 50$ ). Actually the MIS engineer only need to apply these services to the service group with one policy.

## Service

### Pre-defined

Icon	The Definition
	Any service.
	TCP service , for example , FTP , FINGER , HTTP , HTTPS , IMAP , SMTP , POP3 , ANY , AOL , BGP , GOPHER , InterLocator , IRC , L2TP , LDAP , NetMeeting , NNTP , PPTPReal , Media , RLOGIN , SSH , TCP ANY , TELNET , VDO Live , WAIS , WINFRAME , X-WINDOWS .
	UDP service , for example , IKE , DNS , NTP , IRC , RIP , SNMP , SYSLOG , TALK , TFTP , UDP-ANY , UUCP .
	ICMP service, for example, PING, TRACEROUTE.

### Service name

- The MIS engineer can define the service name.

### Protocol

- The Protocol that is made of the communication between the devices. It included the TCP and UDP mode.

### Client Port

- The Port number of the network adapter of the Client PC, the range is 1024 to 65535, it is recommended to use the default range.

### Server Port

- The MIS engineer can enter the port number in Custom Service function.

**We set two service application environments.**

<b>No.</b>	<b>Range</b>	<b>The application environment</b>	<b>Pages</b>
<b>Example. 1</b>	<b>Custom</b>	To permit the WAN users communicate to LAN user via the network phone through policy. ( VoIP port number : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )	<b>63</b>
<b>Example. 2</b>	<b>Group</b>	To group the services , and limit the specific user accessing the network resources which provided by the group service through Policy. ( Group : HTTP , POP3 , SMTP , DNS )	<b>67</b>



## Example 1

To permit the WAN users communicate to LAN user via the network phone through policy. ( VoIP port number : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )

**Step1.** In **Address** → **LAN** and **LAN Group** , add the following setting :

Name▼	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
VoIP_01	192.168.1.2/255.255.255.255		Modify Remove
VoIP_02	192.168.1.3/255.255.255.255		Modify Remove
VoIP_03	192.168.1.4/255.255.255.255		Modify Remove
VoIP_04	192.168.1.5/255.255.255.255		Modify Remove

[New Entry](#)

The LAN address setting

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

[New Entry](#)

The LAN group address setting

**Step2.** In **Service** → **Custom** add the setting as following :

- Click **New Entry**.
- **Service NAME**, enters the default name, VoIP.
- **Protocol # 1** , select TCP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 1720 : 1720.
- **Protocol #2** , select TCP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 15328 : 15333.
- **Protocol #3** , select UDP , **Client Port** 's setting reserve the default value , **Server Port** , enter the value of 15328 : 15333.
- Click **OK**.

Add User Defined Service					
Service NAME :		VoIP (Max. 16 characters)			
#	Protocol ( Range: 0 - 255 )	Client Port ( Range: 0 - 65535 )		Server Port ( Range: 0 - 65535 )	
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0	65535	1720	1720
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other 6	0	65535	15328	15333
3	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other 17	0	65535	15328	15333
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0	0	0	0
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0	0	0	0
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0	0	0	0
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0	0	0	0
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other 0	0	0	0	0

### The custom setting

Service name▼	Protocol	Client Port	Server Port	Configure
VoIP	TCP	0:65535	1720:1720	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Complete the VoIP custom setting



Normally, the default client port number is range from 0 to 65535. It is recommended not to modify the port number range in **Custom Service** function.



To enter the port number in the client port, if the MIS engineer has to enter two different port numbers in server port, then enter the range of 15328:15333. To enter the same port number in the server port, the MIS engineer has to enter two same port numbers, for example, enter the range of 1720: 1720.

**Step3.** Apply the **Service** setting to **Virtual Server**.Virtual Server Real IP 

Total entry : 1

Service	WAN Port	Server Virtual IP	Configure
VoIP	From-Service(Custom)	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5	<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

[New Entry](#)**Apply the Server setting to Virtual Server****Step4.** Apply **Virtual Service** to **Policy → Incoming**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(10.10.10.3)	VoIP			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 

[New Entry](#)**Complete the Incoming VoIP Policy****Step5.** In **Policy → Outgoing**, to complete the Outgoing VoIP setting.

Source	Destination	Service	Action	Option	Configure	Move
VoIP_Group	Outside_Any	VoIP			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 

[New Entry](#)**Complete the Outgoing VoIP policy**The service setting must apply to **Policy** and **Virtual Server**, to make it works.

## Example 2

To Group the Service, and limit the user can only access the Network resources provided by the Group through Policy Object. ( Group : HTTP , POP3 , SMTP , DNS )

**Step1.** In **Service** → **Group** , add the new setting as following :

- Click **New Entry**.
- Set the **Name** to be the default name of **Main Service**.
- In **Available service**, select HTTP, POP3, SMTP, DNS, Click **Add**.
- Click **OK**.

The service group setting

Group name ▼	Service	Configure
mail_service	DNS,IMAP,POP3...	In Use
Main_Service	DNS,HTTP,POP3...	Modify Remove

New Entry

Complete the service group setting



If the MIS engineer wants to remove the group service, then he can choose the **Selected service**, and click **Remove**.

**Step2.** In **Address → LAN Group**, to set the LAN group which can only access the specific service.

Name	Member	Configure
Test_Team	alex, eva, jonas	<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

[New Entry](#)

The LAN group setting

**Step3.** Apply **Service Group** to **Policy → Outgoing**.

Source	Destination	Service	Action	Option							Configure	Move
Test_Team	Outside_Any	Main_Service									<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 

[New Entry](#)

The policy setting

## 5.3 Schedule

# Schedule

In this chapter, the MIS engineer can define the network connection and the process time period in Schedule. In other words, the MIS engineer can select the specific time period for internal user to transfer the data packets by policy management.



### How to use Schedule ?

The MIS engineer can use the Schedule function to auto set the packets flow in different time period by **Policy** management.

## Example

To set the valid time of LAN user can access the network data everyday through the policy management.

**Step1.** In **Schedule** , add the new setting as following :

- Click **New Entry**
- Set the **Schedule Name**.
- Use the drop down menu to select the time period everyday.
- Click **OK**

Add New Schedule

Schedule Name  (Max. 16 characters)

Day	Period	
	Start Time	Stop Time
Monday	09:00 ▾	18:00 ▾
Tuesday	09:00 ▾	18:00 ▾
Wednesday	09:00 ▾	18:00 ▾
Thursday	09:30 ▾	18:00 ▾
Friday	All day ▾	All day ▾
Saturday	Disable ▾	Disable ▾
Sunday	Disable ▾	Disable ▾

OK Cancel

The schedule setting

Name ▾	Configure
Working_Time	Modify Remove

New Entry

Complete the schedule setting

**Step2.** Apply schedule setting to **Policy** → **Outgoing**

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

New Entry

Complete to apply the schedule setting to policy



The **Schedule** setting must applied into **Policy**.



## 5.4 QoS

### QoS

The CS-2000 appliance can manage the downstream and upstream bandwidth through the bandwidth parameter setting .

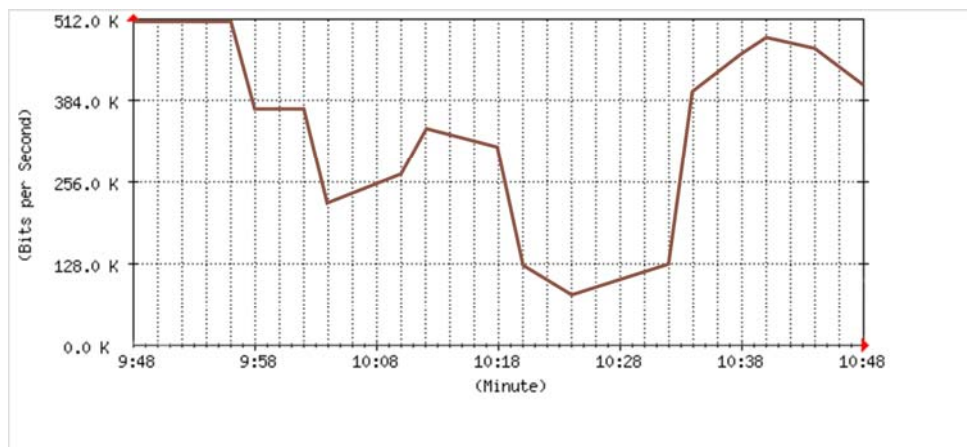
The MIS engineer can set the bandwidth depends on the provided WAN bandwidth.

**Downstream Bandwidth** : Can set the G.Bandwidth and M.Bandwidth .

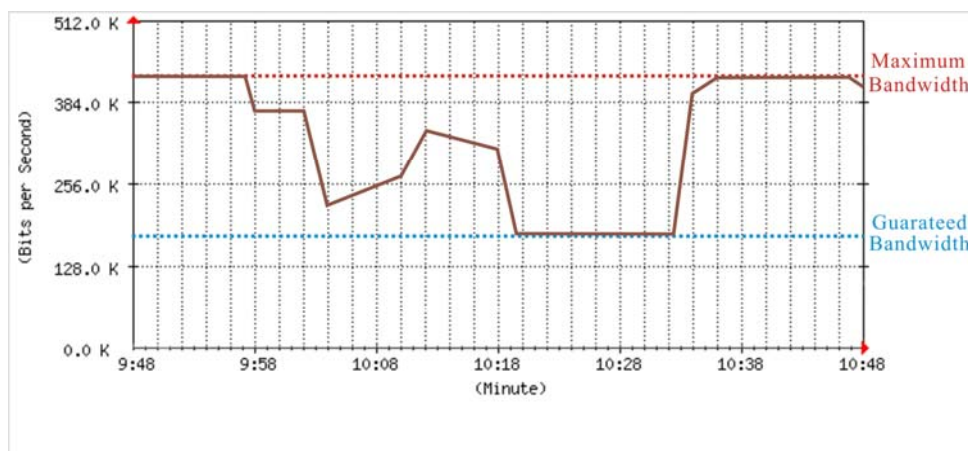
**Upstream Bandwidth** : Can set the G.Bandwidth and M.Bandwidth .

**QoS Priority** : Can set the QoS priority of upstream and downstream bandwidth .

The CS-2000 appliance can set the outgoing bandwidth depends on different QoS , and can select the proper QoS setting by policy . It can let the MIS engineer efficiently to distribute the bandwidth.



The unused QoS flow



The used QoS flow ( M.Bandwidth : 400 Kbps , G.Bandwidth : 200Kbps )

## QoS :

### WAN

- Includes WAN 1 and WAN 2.

### Downstream Bandwidth

- The maximum bandwidth and guarantee bandwidth of downstream bandwidth.

### Upstream Bandwidth

- The maximum bandwidth and guarantee bandwidth of upstream bandwidth.

### QoS Priority

- To set the unused upstream and downstream bandwidth in QoS priority.

### G.Bandwidth

- The basic bandwidth in QoS. The **policy** which applied to the QoS, will at least reserve the QoS settings.

### M.Bandwidth

- The maximum bandwidth in QoS. The **Policy** which applied to the QoS, its bandwidth will not over the QoS Setting.

## Example

### Sets the Policy of the Upstream Bandwidth and Downstream Bandwidth.

**Step1.** In **QoS** , add the new setting as following :

- Click **New Entry**
- In **Name**, to set the QoS name.
- In WAN 1and 2, enter the parameter of limited bandwidth.
- To select the **QoS Priority**.
- Click **OK**.

Modify QoS				
Name <input type="text" value="ftp"/> (Max. 16 characters)				
WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority	
1	G.Bandwidth = <input type="text" value="1024"/> Kbps( Range: 1 - 1536 ) M.Bandwidth = <input type="text" value="2048"/> Kbps( Range: 1024 - 2048 )	G.Bandwidth = <input type="text" value="128"/> Kbps( Range: 1 - 200 ) M.Bandwidth = <input type="text" value="256"/> Kbps( Range: 128 - 256 )	High <input type="button" value="v"/>	
2	G.Bandwidth = <input type="text" value="256"/> Kbps( Range: 1 - 512 ) M.Bandwidth = <input type="text" value="1024"/> Kbps( Range: 256 - 1024 )	G.Bandwidth = <input type="text" value="128"/> Kbps( Range: 1 - 256 ) M.Bandwidth = <input type="text" value="512"/> Kbps( Range: 128 - 512 )		
3 (Disabled)	G.Bandwidth = <input type="text" value="0"/> Kbps M.Bandwidth = <input type="text" value="0"/> Kbps	G.Bandwidth = <input type="text" value="0"/> Kbps M.Bandwidth = <input type="text" value="0"/> Kbps		

#### The QoS setting

Name▼	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
ftp	1	G.Bandwidth = 1024 Kbps M.Bandwidth = 2048 Kbps	G.Bandwidth = 128 Kbps M.Bandwidth = 256 Kbps	High	<input type="button" value="In Use"/>
	2	G.Bandwidth = 256 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 128 Kbps M.Bandwidth = 512 Kbps		
	3	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		
mail	1	G.Bandwidth = 512 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 56 Kbps M.Bandwidth = 256 Kbps	Middle	<input type="button" value="In Use"/>
	2	G.Bandwidth = 512 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 256 Kbps M.Bandwidth = 512 Kbps		
	3	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		

#### Complete the QoS setting

**Step2.** In **Policy → Outgoing** , to apply the QoS Setting in **Step 1**

Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	FTP ▾
Schedule	None ▾

To select the QoS Service

Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	ftp ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )

To set the QoS policy

Source	Destination	Service	Action	Option							Configure			Move
Inside_Any	Outside_Any	FTP												To 1 

[New Entry](#)

Complete the policy setting



When the MIS engineer setting the QoS, he must use the correct range of upstream and downstream bandwidth in **interface → WAN**.

## 5.5 Authentication

# Authentication

The CS-2000 appliance can manage the user's connection by authentication. The user has to pass the authentication to connect the network .

The CS-2000 appliance provided 4 authentication modes . The User and User Group built in ; others are RADIUS , POP3 and LDAP self-built Authentication Server. The MIS engineer can use the 5 modes , to manage the authentication.

## Authentication :

### Authentication Management

- It can provide the authentication port to the MIS engineer and the valid authentication time. (The MIS engineer has to set the Authentication function first.)
  - ◆ **Authentication Port** : When enable the Authentication, the LAN user must pass the authentication to login to the WAN. And the authentication port number is the default value of 82.
  - ◆ **Re-Login if Idle** : When the LAN users connect to the WAN, the MIS engineer can set the Idle time after the Authentication. When the login Idle time has over the default Idle time settings of 30 minutes. The authentication will automatically invalid.
  - ◆ **Re-Login after user login successfully** : When the LAN user connect to the WAN through the authentication. The available authentication time depends on the time limit, if over the default time setting, the authentication will be invalid.
  - ◆ **Disallow Re-Login if the auth user has login** : When enable this function through **User, User Group, RADIUS, POP3 or LDAP** to access the authentication, the authorized account can not be used by other people.
  - ◆ **URL to redirect when authentication succeed** : To direct the authorized LAN user to the assigned web site. The default value is blank. ( It will directly link the user to the login web site )
  - ◆ **Messages to display when user login** : It shows the login messages in the authentication window (it supports the HTML), the default setting is blank. ( it will not show any message in the authentication window.

- To add the settings in the authentication management :

The screenshot shows the 'Authentication Management' configuration window. It has a dark blue header with the title. Below the header, there are three rows of settings, each with a label, a text input field, and a description in parentheses. The first row is 'Authentication Port' with the value '82' and description '( Range: 1 - 65535, 0: means authentication disabled )'. The second row is 'Re-login if idle for' with the value '30' and description 'Minutes ( Range: 1 - 1000 )'. The third row is 'Re-login after user has logged in for' with the value '0' and description 'Hours ( Range: 0 - 24, 0: means unlimited )'. Below these rows is a dashed line. Then there is a checkbox labeled 'Disable re-login' which is checked. Below that is a label 'Redirect successfully authenticated users to URL:' followed by an empty text input field and the text '( Max. 60 characters )'. Another dashed line follows. Then there is a label 'Message to display upon successful login' above a large text area containing the text 'Welcome to CS-2000 Test Authentication Page!!!!'. At the bottom right of the window are two buttons: 'OK' and 'Cancel'.

Authentication Management

Authentication Port  ( Range: 1 - 65535, 0: means authentication disabled )

Re-login if idle for  Minutes ( Range: 1 - 1000 )

Re-login after user has logged in for  Hours ( Range: 0 - 24, 0: means unlimited )

-----

☒ Disable re-login

Redirect successfully authenticated users to URL:  ( Max. 60 characters )

-----

Message to display upon successful login

Welcome to CS-2000 Test Authentication Page!!!!

OK Cancel

### The authentication management

- When the user connect to the WAN through the authentication , it shows the following window :

The screenshot shows a Microsoft Internet Explorer window titled 'Cannot find server - Microsoft Internet Explorer'. The address bar shows 'http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome'. The main content area displays a 'User Login' window. This window has a dark blue header with the title 'User Authentication'. Below the header, there are two rows of input fields: 'User Name' with the value 'auth\_1' and a hint '( ex: auth\_user1 )', and 'Password' with masked characters '\*\*\*'. Below these fields is an 'OK' button. At the bottom of the 'User Login' window, it says 'Welcome to CS-2000 Test Authentication Page!!!!'. The Internet Explorer window has a status bar at the bottom showing 'Done' and 'Internet'.

Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS Feeds

Address <http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome> Go Links

User Login

User Authentication

User Name  ( ex: auth\_user1 )

Password

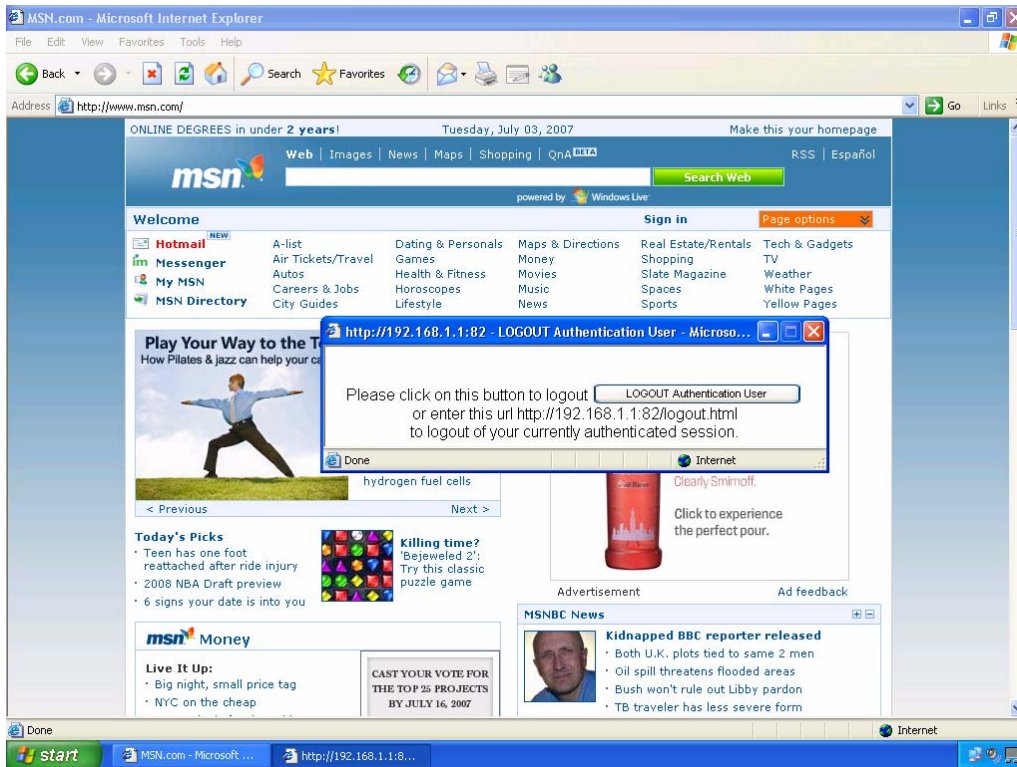
OK

Welcome to CS-2000 Test Authentication Page!!!!

Done Internet

### The authentication login window

- After the authentication , it will redirect to the assigned web site :



**Redirect to the assigned web site after authenticated**



If the users want to require the authentication, then he can enter the CS-2000's LAN interface IP and the authentication port number in the URL address, then shows the authentication window.

### Authentication - User Name

- The user's authentication account.

### Password

- Create the authentication password.

### Confirm Password

- To enter the same password as in the password column.

### Shared Secret

- The required password when accessing the authentication between the CS-2000 appliance and RADIUS server.

### 802.1x RADIUS

- The authentication between the CS-2000 appliance and RADIUS server which included the wireless network.



### Search Distinguished Name

- The identify name of LDAP server.

### LDAP Filter

- To assign the specific account in LDAP server.

### User Distinguished Name

- The required account in the authentication between the CS-2000 appliance and LDAP server.

**We set 4 authentication application environments.**

No.	Range	The Application Environments	Pages
<b>Example 1</b>	<b>User</b> <b>User Group</b>	To plan the LAN user connect to the WAN through the authentication by policy. ( <b>To use the built-in user and user group authentication.</b> )	<b>81</b>
<b>Example 2</b>	<b>RADIUS</b>	To plan the user connect to the WAN through the authentication in policy . <b>To use the WAN RADIUS server ( Windows 2003 Server built-in authentication . )</b>	<b>84</b>
<b>Example 3</b>	<b>POP3</b>	To plan the user connect to the WAN through the authentication by policy.( <b>To use the WAN POP3 server authentication</b> )	<b>98</b>
<b>Example 4</b>	<b>LDAP</b>	To plan the user connect to the WAN through the authentication by policy .( <b>To use the WAN LDAP server ( Windows 2003 Server built-in authentication )</b>	<b>101</b>

### 5.5.1 Example 1 User & User Group Authentication

To plan the LAN user connect to the WAN through the authentication by policy. (To use the built-in user and user group authentication.

**Step1.** In **Authentication → User**, to add the Authentication – User Name.

Authentication User Name▼	Configure
alex	<button>Modify</button> <button>Remove</button>
eva	<button>Modify</button> <button>Remove</button>
joe	<button>Modify</button> <button>Remove</button>

[New Entry](#)

The Authentication – User Name setting



The user's DNS server must correspond to the LAN interface through the CS-2000 appliance, in order to enable the authentication.

**Step2.** In **Authentication → User Group**, add the new setting as following :

- Click **New Entry**.
- **Name**, enter auth\_group.
- Click **Add**, to add the available authentication user to the selected authentication user in the same user group.
- Click **OK**.
- Complete the user group settings in authentication.

New Authentication Group

Name:

auth\_group

(Max. 16 characters)

<--- Available Authentication User --->

alex

eva

joe

(Radius User)

(POP3 User)

(LDAP User)

<--- Selected Authentication User --->

alex

eva

joe

Remove

Add

OK

























Cancel

The user group authentication setting

**Step3.** In **Policy → Outgoing**, add a new policy, and apply the Step 1, 2 into the new policy setting.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	auth_group ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

The authentication user policy setting

Source	Destination	Service	Action	Option								Configure			Move
Inside_Any	Outside_Any	DNS													To 1 ▾
Inside_Any	Outside_Any	ANY													To 2 ▾

[New Entry](#)

Complete the authentication user policy setting

- Step4.** When the LAN users want to connect to the network via browser, it will show the authentication window. After enter the correct user name and password, Click **OK** , to connect to the network via the CS-2000 appliance

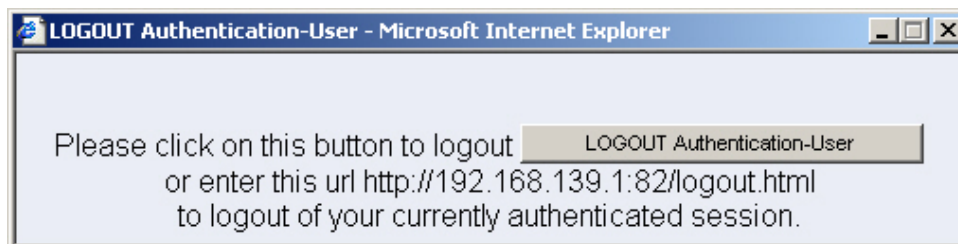
User Login

User Authentication	
User Name	<input type="text" value="alex"/> ( ex: auth_user1 )
Password	<input type="password" value="...."/>

Welcome to CS-2000 Test Authentication Page!!!!

**To create the IPSec VPN connection via the authentication**

- Step5.** If the remote user want to logout , click **Logout Auth-User** in **Auth-User Logout window** ( The logout window will appear when pass the authentication ) , the MIS engineer can also log in **Auth-User Logout** window ( [http:// LAN Interface : Authentication Port /logout.html](http://LAN Interface : Authentication Port /logout.html) ) , click **Logout Auth-User**.



**The Logout confirmation**

### 5.5.2 Example 2 RADIUS Server Authentication

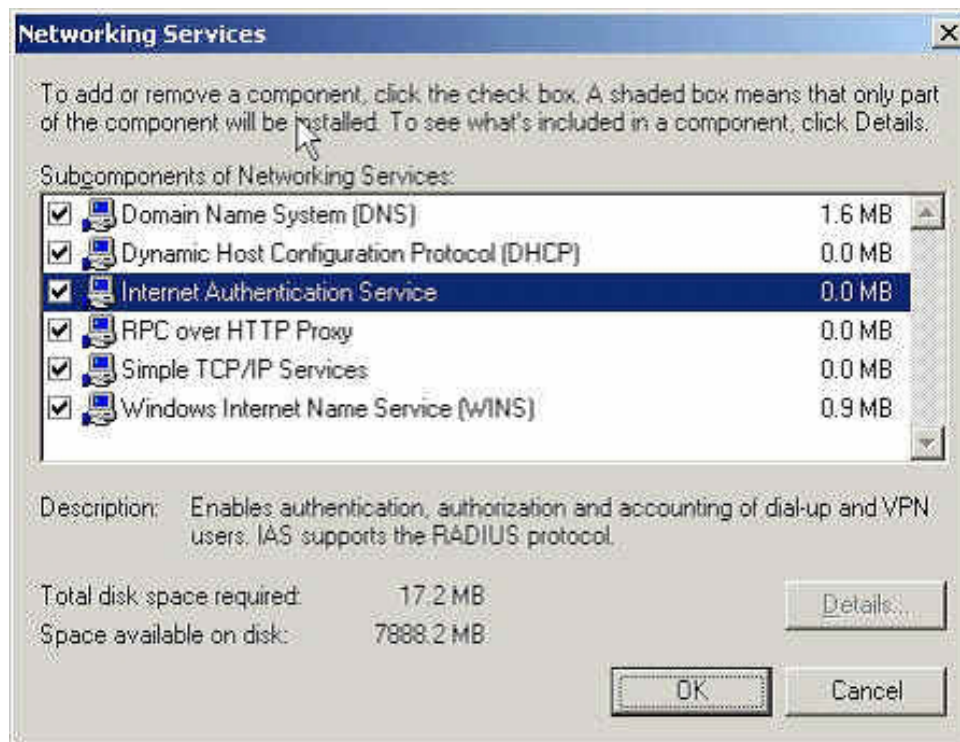
To plan the user connect to the WAN through the authentication in policy .To use the WAN RADIUS server ( Windows 2003 Server built-in authentication . )

#### ※ Windows 2003 RADIUS Server Deployment

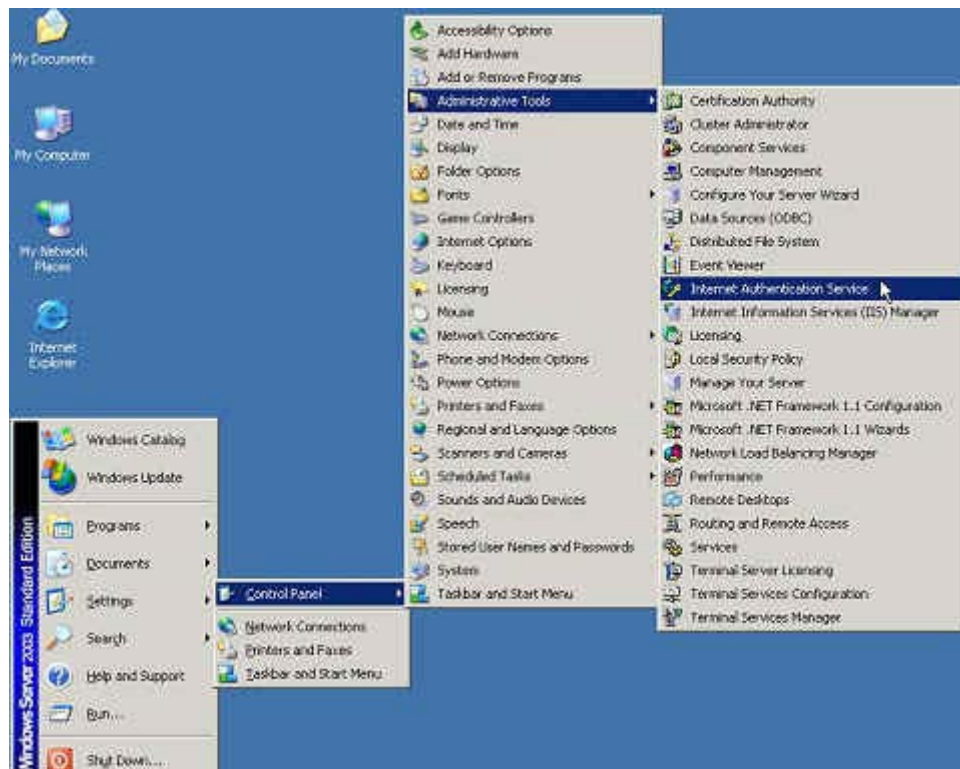
- Step1.** Click **Start → Control Panel → Add / Remove Programs**, select **Add / Remove Windows Components**, then it shows the **Windows Components Wizard**.
- Step2.** Select **Networking Services**, and then click **Details**.



Windows components wizard

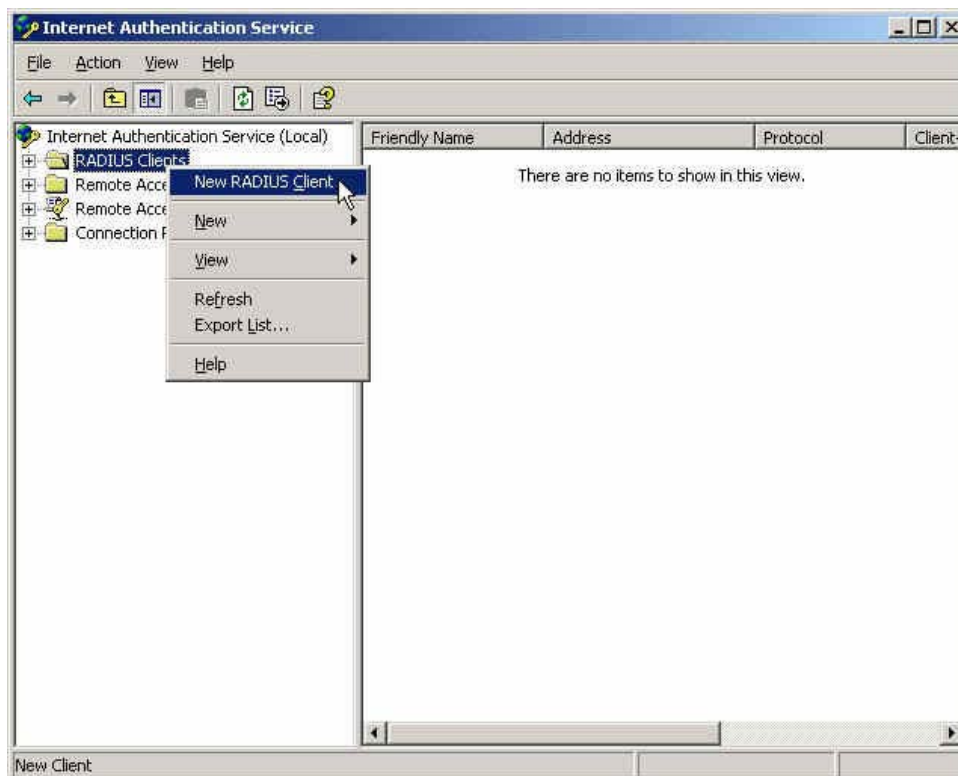
**Step3. Select Internet Authentication Service**

Add new network authentication service components

**Step4. Click Start → Control Panel → Administrative Tools, select Network Authentication Service.**

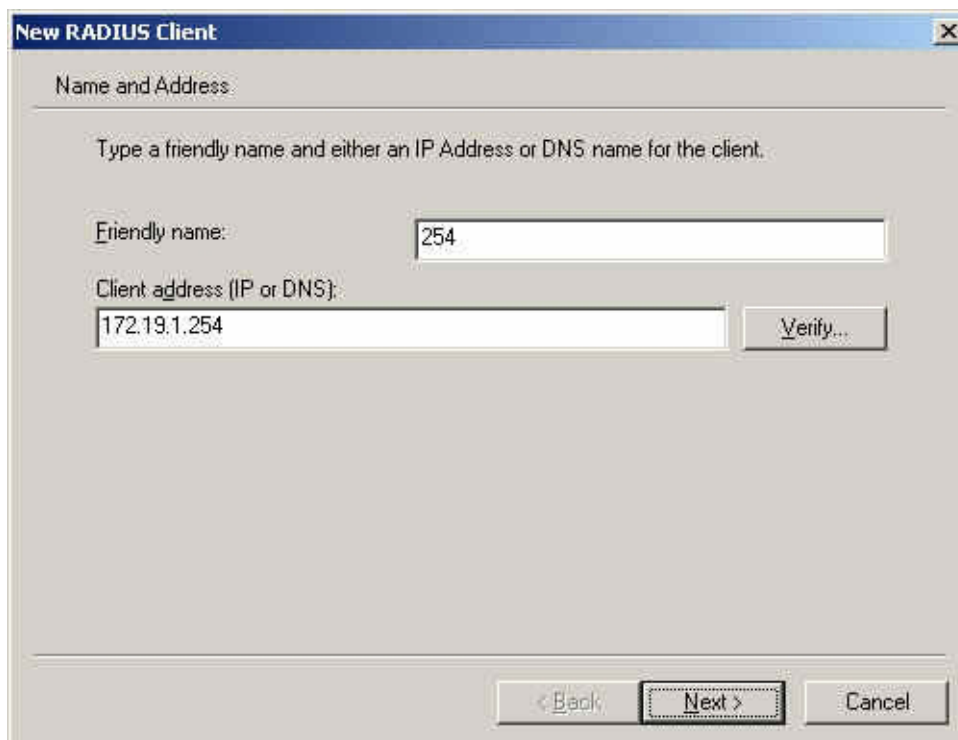
Select network authentication service

**Step5.** Right click **RADIUS Clients** → **New RADIUS Client**



**Add new RADIUS client**

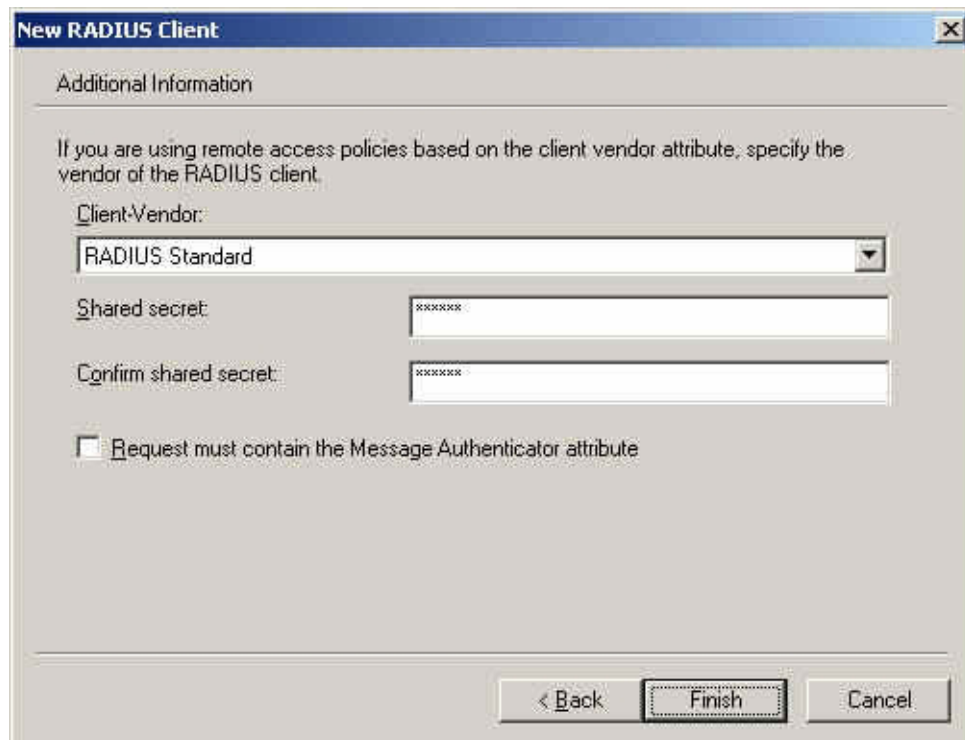
**Step6.** Enter the **Name and Client Address** (It is the same as CS-2000 IP Address).



**Add New RADIUS client name and IP address setting**



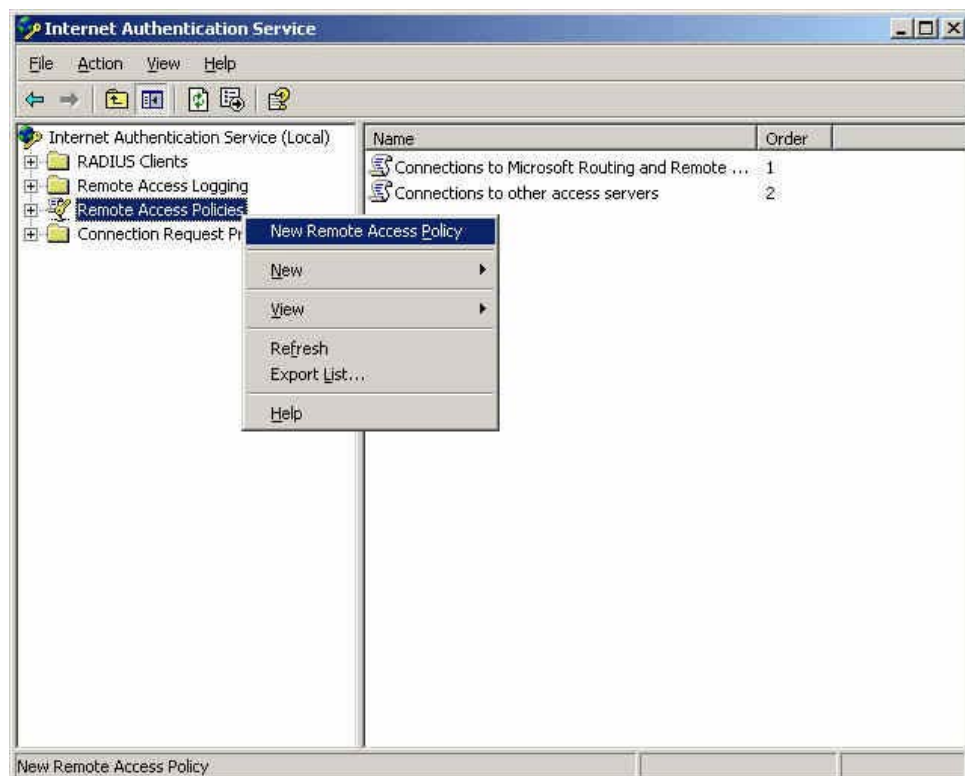
- Step7.** Select **RADIUS Standard**; enter the Shared secret and Confirm Shared secret. (It must be the same setting as RADIUS in CS-2000).



The 'New RADIUS Client' dialog box is shown. It has a title bar 'New RADIUS Client' with a close button. Below the title bar is a section 'Additional Information'. Inside this section, there is a text instruction: 'If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.' Below this instruction is a 'Client-Vendor:' label followed by a dropdown menu currently showing 'RADIUS Standard'. Below the dropdown are two text input fields: 'Shared secret:' and 'Confirm shared secret:', both containing masked text (asterisks). Below these fields is a checkbox labeled 'Request must contain the Message Authenticator attribute' which is currently unchecked. At the bottom of the dialog are three buttons: '< Back', 'Finish', and 'Cancel'.

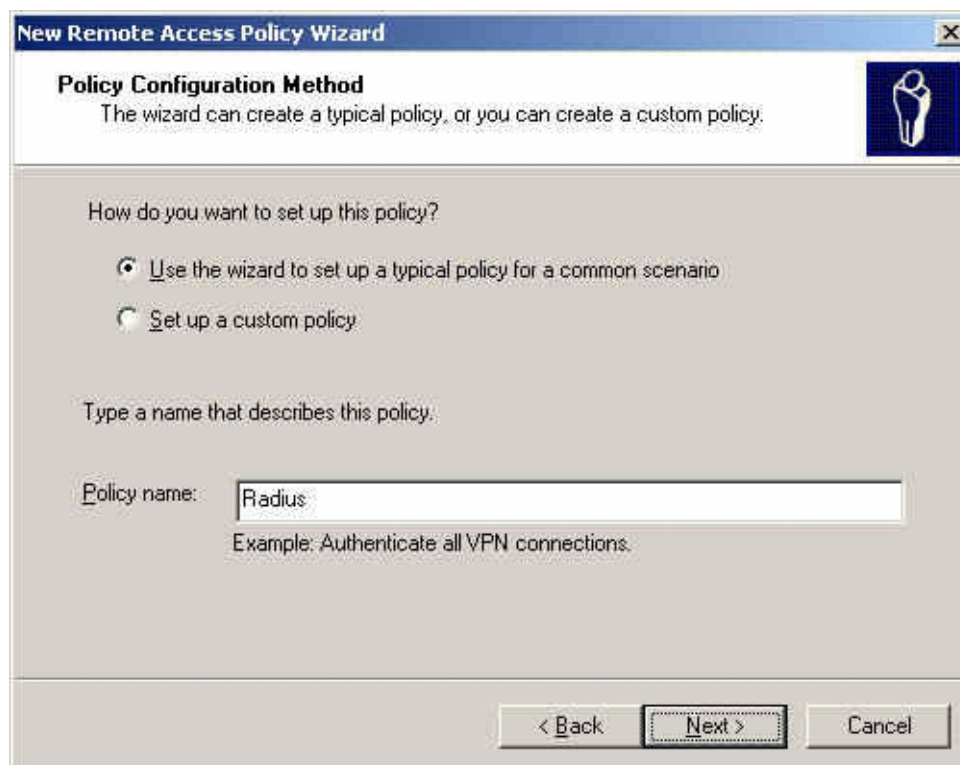
**Add new RADIUS client-vendor and shared secret**

- Step8.** Right click on **Remote Access Policies**→ **New Remote Access Policy**



**Add new remote access policies**

- Step9.** Select **Use the wizard to set up a typical policy for a common scenario** , and enter the **Policy name**



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

How do you want to set up this policy?

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

☐ Set up a custom policy.

Type a name that describes this policy:

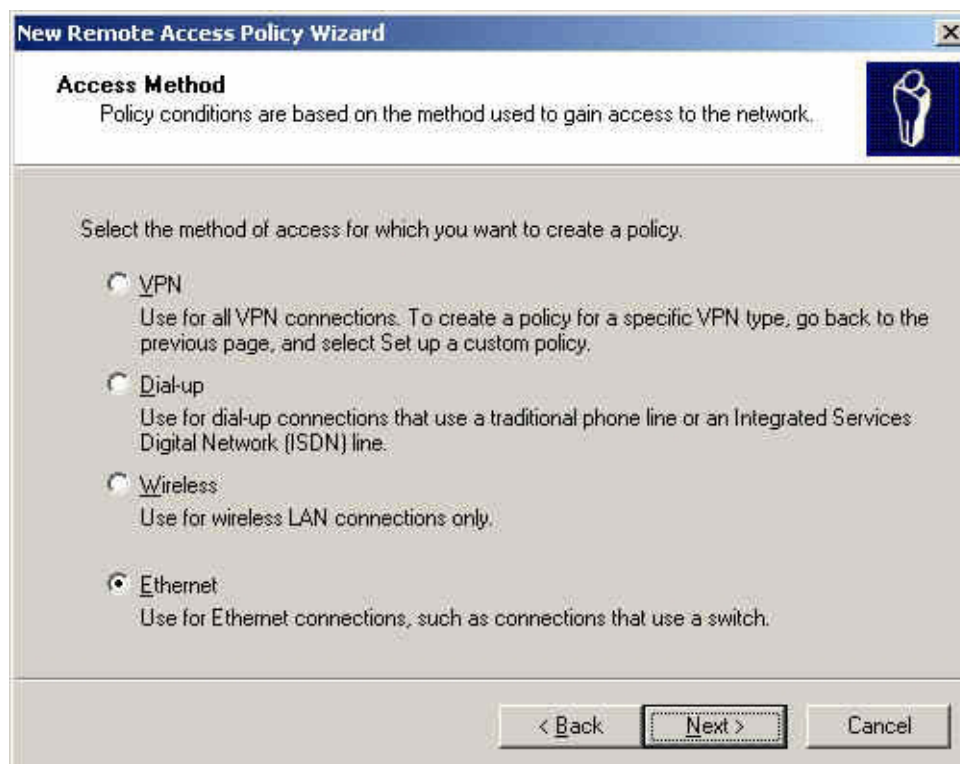
Policy name:

Example: Authenticate all VPN connections.

< Back   Next >   Cancel

Add new remote access policies and policy name

- Step10.** Select **Ethernet**.



Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

☐ VPN  
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

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

☐ Wireless  
Use for wireless LAN connections only.

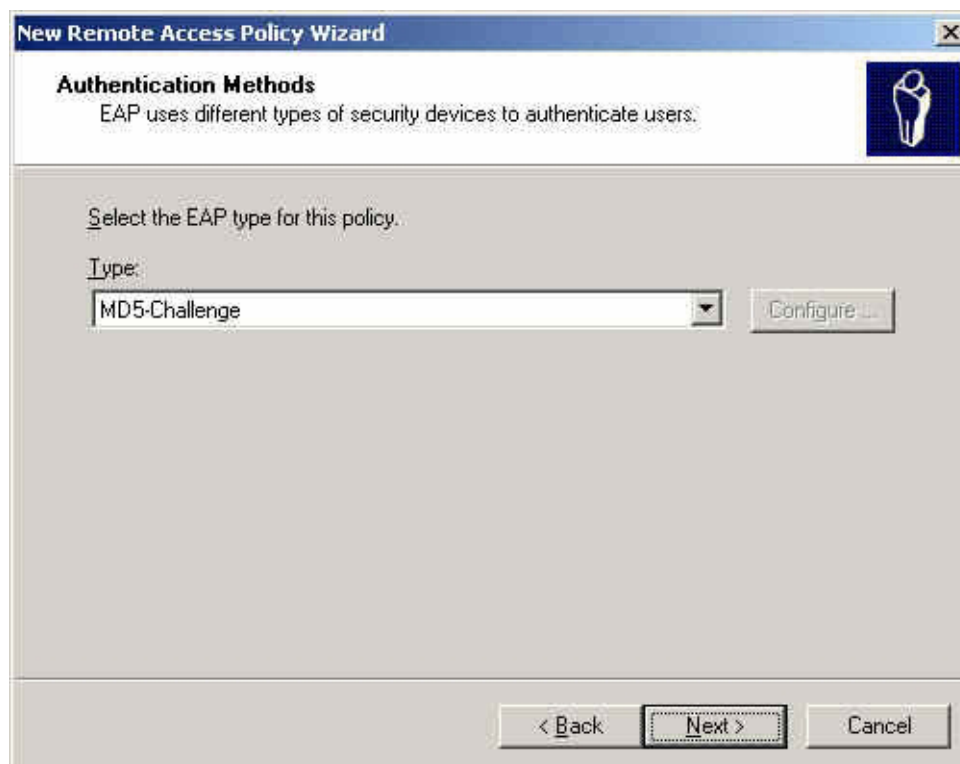
☒ Ethernet  
Use for Ethernet connections, such as connections that use a switch.

< Back   Next >   Cancel

The way to add new remote access policy

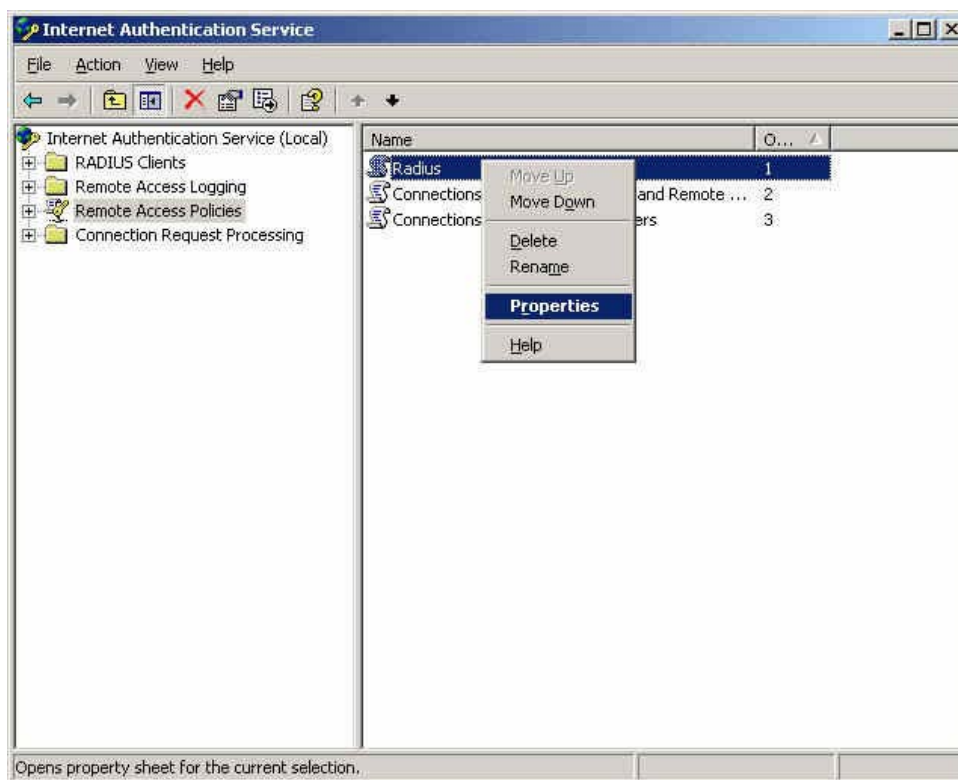
**Step11. Select User**

Add new remote access policy user and group

**Step12. Select MD5-Challenge.**

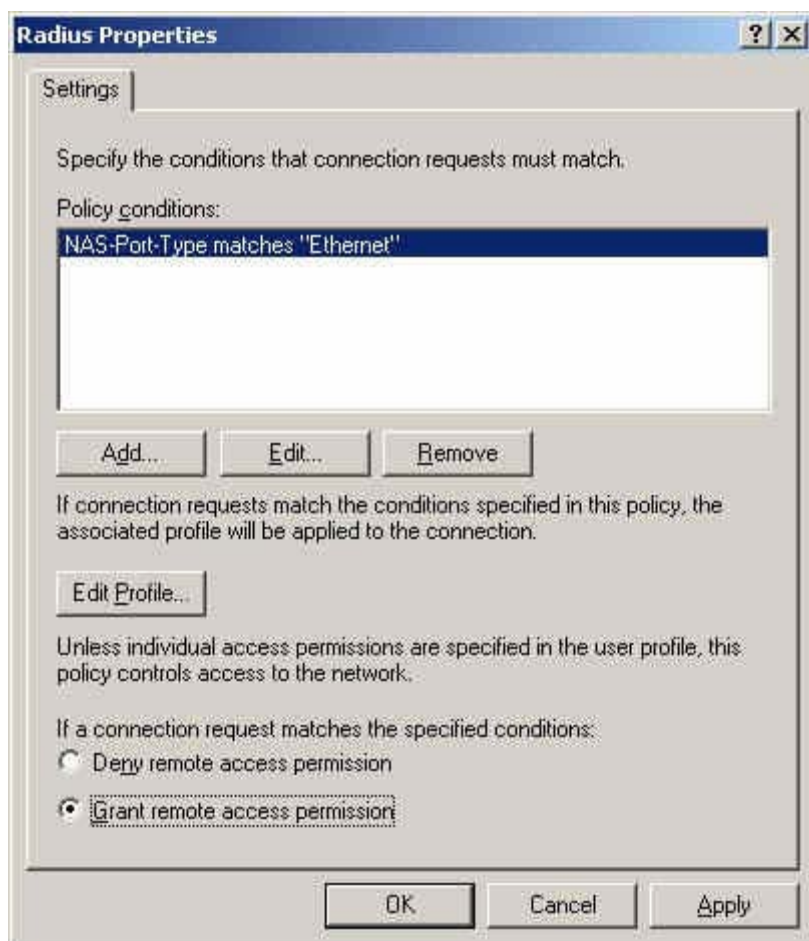
The authentication of add new remote access policy

**Step13.** Right click on the **Radius** → **Properties**

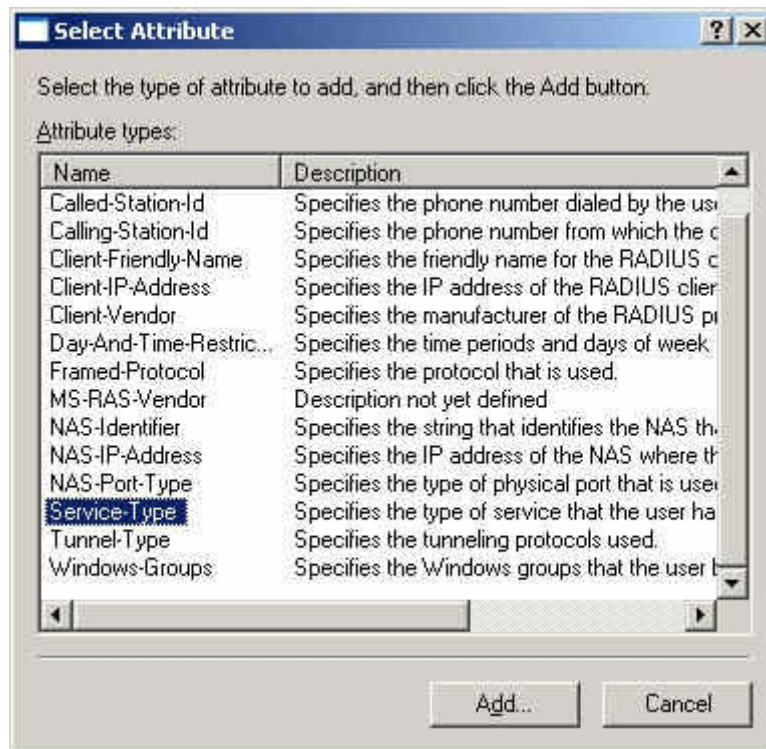


**The network authentication service setting**

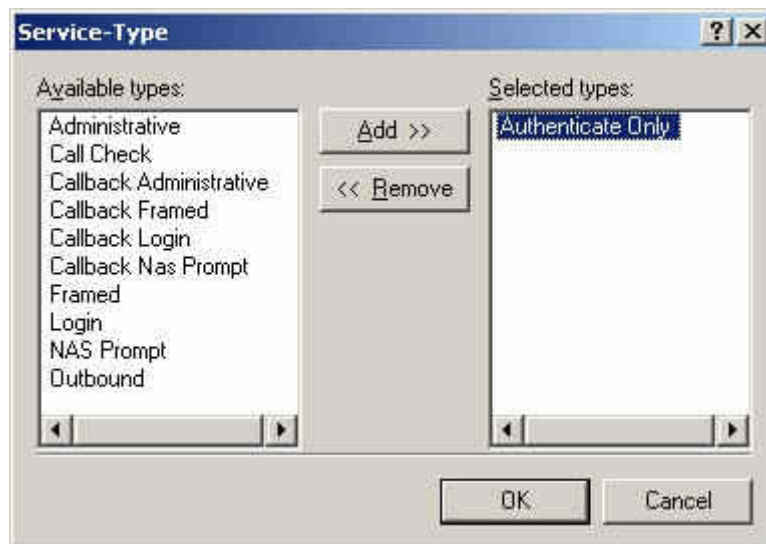
**Step14.** Select **Grant remote access permission**, and **Remove** the original setting, then click **Add**.



**The RADIUS properties settings**

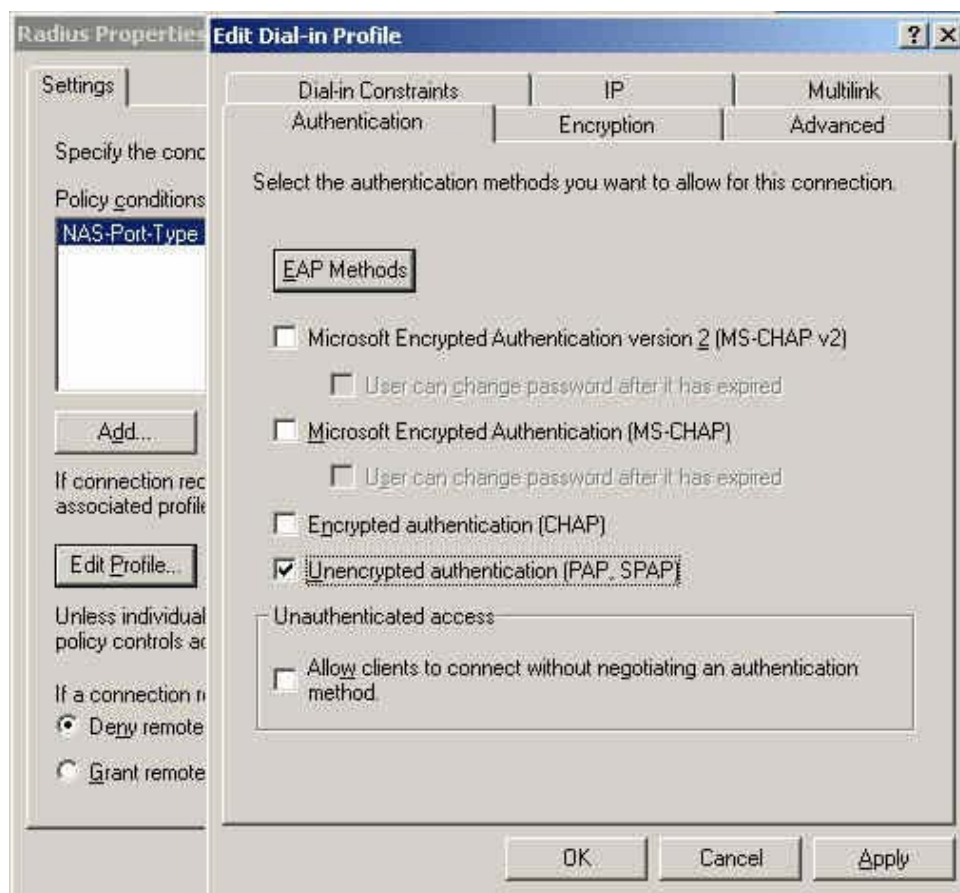
**Step15. Add Service-Type.**

**Add new RADIUS properties attribute**

**Step16. Add Authenticate Only from the left side.**

**Add RADIUS properties service-type**

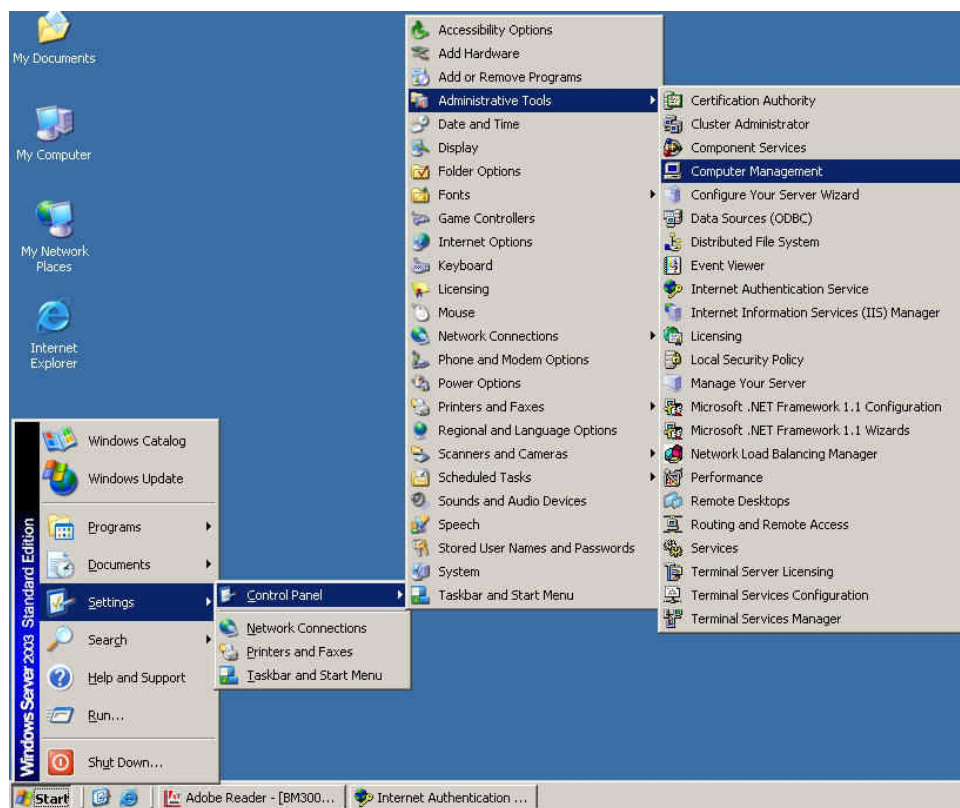
**Step17.** Click **Edit Profile**, select **Authentication**, and check **Unencrypted authentication (PAP, SPAP)** .



**Edit RADIUS service-type dial-in property**



**Step18.** Add Auth User, click **Start** → **Setting** → **Control Panel**→**Administrative Tools**, select **Computer Management**



Enter computer management

**Step19.** Right click on **Users**, select **New User**.



Add new user



**Step20.** Complete the Windows 2003 RADIUS Server Settings.

**Step21.** In **Authentication** → **RADIUS** function, enter **IP**, **Port** and **Shared Secret**. (The setting must be the same as RADIUS server).

RADIUS Server		
<input checked="" type="checkbox"/> Enable RADIUS Server Authentication	<a href="#">Test</a>	
RADIUS Server ( IP or Domain Name )	172.19.250.10	( Max. 80 characters )
RADIUS Server Port	1812	( Range: 1025 - 65535 )
Shared Secret	radius	( Max. 80 characters )
<input type="checkbox"/> Enable 802.1x RADIUS Server Authentication		
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

### The RADIUS server setting



Click **Test** , it can detect if the CS-2000 and RADIUS server can real working .

**Step22.** In **Authentication** → **User Group**, add new **Radius User**.



New Authentication Group		
Name:	Radius	(Max. 16 characters)
<div> <div>&lt;--- Available Authentication User ---&gt;</div> <div> alex eva joe (Radius User) (POP3 User) (LDAP User) </div> </div>	<input type="button" value="Remove"/>  <input type="button" value="Add"/>	<div> <div>&lt;--- Selected Authentication User ---&gt;</div> <div> (Radius User) </div> </div>
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

### Add new RADIUS user

**Step23.** In **Policy → Outgoing**, apply the **Authentication Group** (RADIUS included) in Step22. To add the new policy.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	RADIUS ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

To add the RADIUS authentication policy

Source	Destination	Service	Action	Option								Configure			Move
Inside_Any	Outside_Any	DNS										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 ▾
Inside_Any	Outside_Any	ANY										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 2 ▾

[New Entry](#)

Complete the RADIUS authentication policy setting

- Step24.** When the users connect to the network via the browser, it will show the authentication window. Enter the user name and password, click **OK**, and then link to the network through the CS-2000.

User Login

User Authentication	
User Name	<input type="text" value="alex"/> ( ex: auth_user1 )
Password	<input type="password" value="••••"/>

Welcome to CS-2000 Test Authentication Page!!!!

[Link to the network through the authentication window](#)

### 5.5.3 Example 3 POP3 Server Authentication

To plan the users connect to the WAN through the authentication by policy. (To use the WAN POP3 server authentication)

**Step1.** In **Authentication** → **POP3**, add the new setting as following.

POP3 Server IP or Domain Name / Port	Configure
planet.com.tw / 110	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### The POP3 server setting



Click **Test** , it can detect if the CS-2000 and POP3 server can real working .

**Step2.** In **Authentication** → **User Group**, add new **POP3 User**.

New Authentication Group

Name:

POP3\_auth

(Max. 16 characters)

<--- Available Authentication User --->

alex

eva

joe

(Radius User)

**(POP3 User)**

(LDAP User)

Remove

Add

<--- Selected Authentication User --->

(POP3 User)

OK




Cancel

Add new POP3 user

**Step3.** In **Policy → Outgoing**, apply Step2 (The authentication group) in to the policy.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	POP3_auth ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

The POP3 server authentication in policy setting

Source	Destination	Service	Action	Option								Configure			Move
Inside_Any	Outside_Any	DNS										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 ▾
Inside_Any	Outside_Any	ANY										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 2 ▾

[New Entry](#)

Complete the POP3 server authentication in policy setting

- Step4.** When the users want to connect to the network via browser, it will show the authentication window. Enter the user name and password, click **OK**, and then link to the network through the CS-2000 appliance.

User Login

User Authentication	
User Name	<input type="text" value="alex"/> ( ex: auth_user1 )
Password	<input type="password" value="...."/>

Welcome to CS-2000 Test Authentication Page!!!!

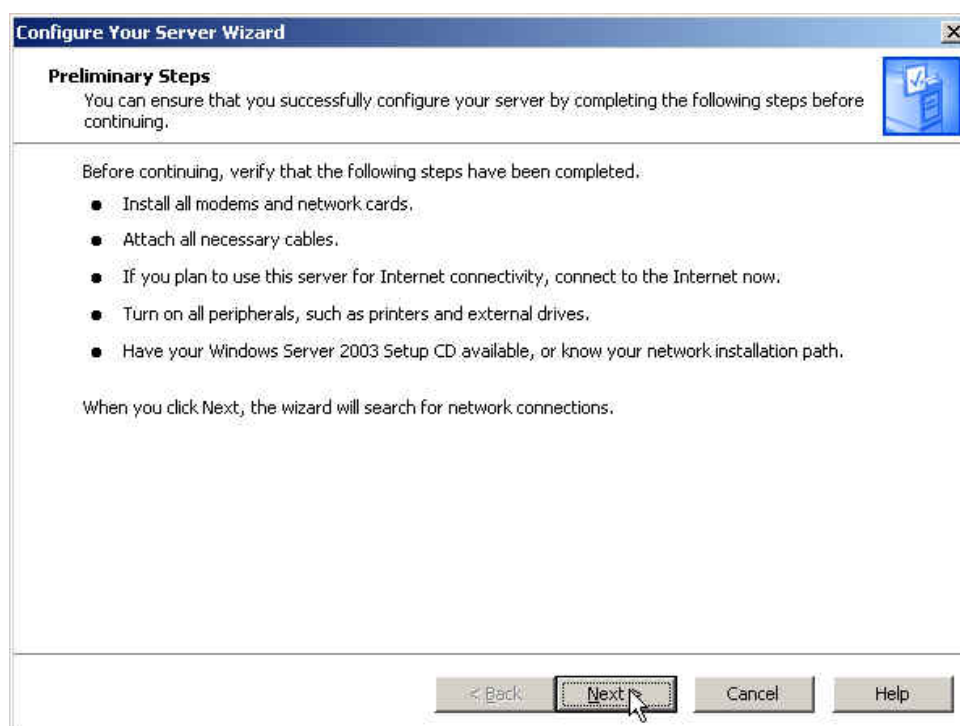
**[Link to the network through the authentication window](#)**

### 5.5.4 Example 4 LDAP Server Authentication

To plan the users connect to the WAN through the authentication by policy. (To use the WAN LDAP server ( Windows 2003 Server built-in authentication )

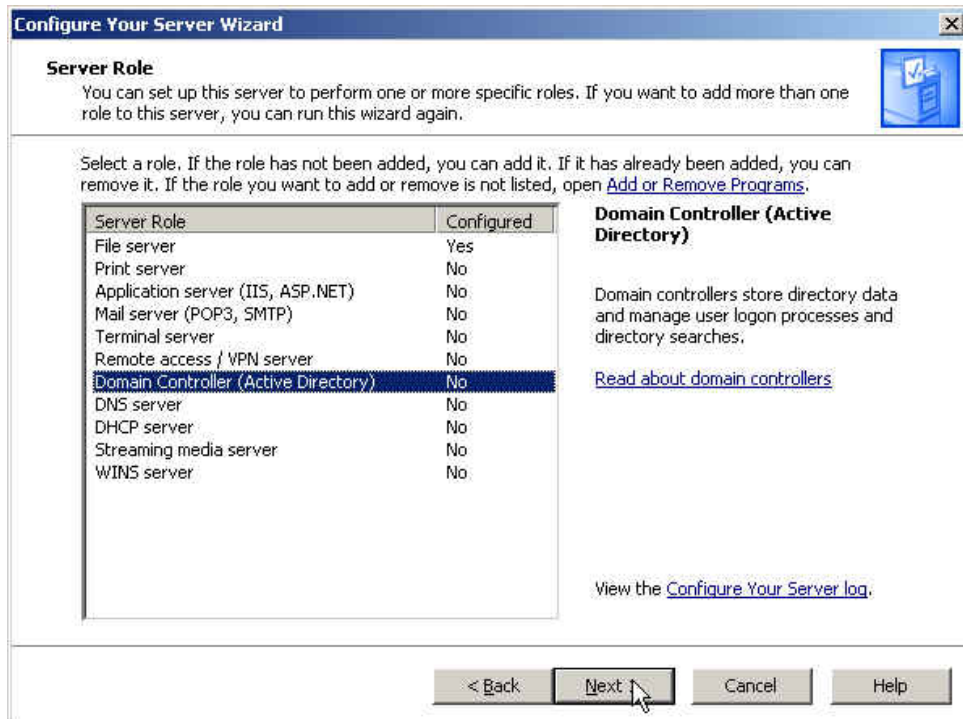
#### ※ Windows 2003 LDAP Server Deployment

- Step1.** Click **Start → Program → Administrative Tools → Manage MIS engineer Server.**
- Step2.** In **Manage MIS engineer Server** window, click **Add or remove a role → Configure MIS engineer Server Wizard.**
- Step3.** In **Preliminary Steps** window, click **next.**



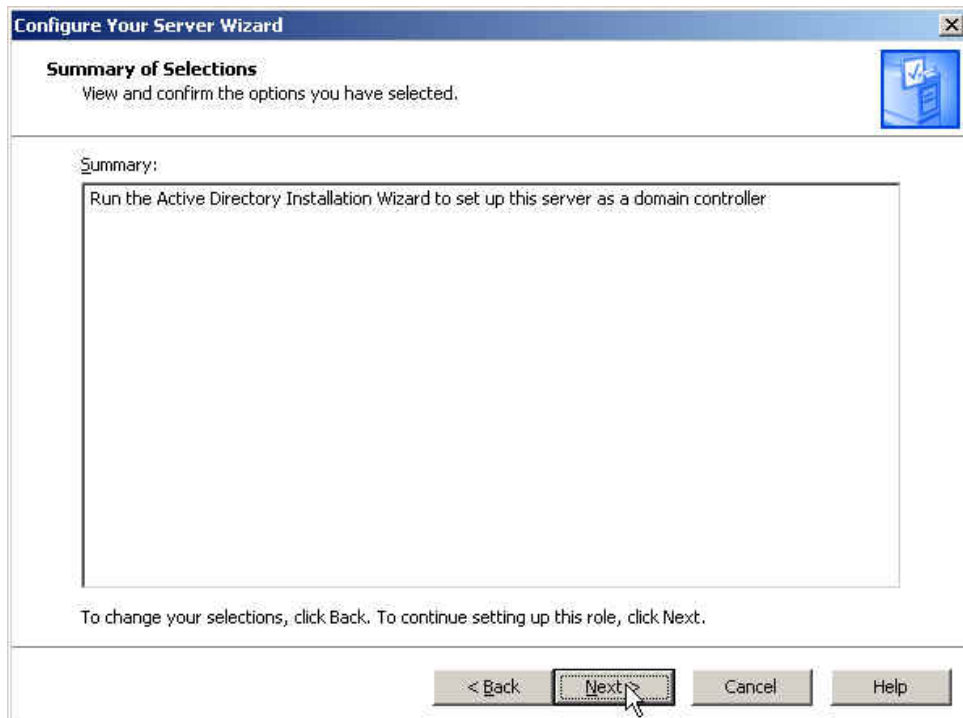
The Preliminary steps Web UI

**Step4.** In **Server Role** window, select **Active Directory** and click **Next**.



The server role window

**Step5.** In **Summary of Selections** window, click **Next**.



The summary of selections window

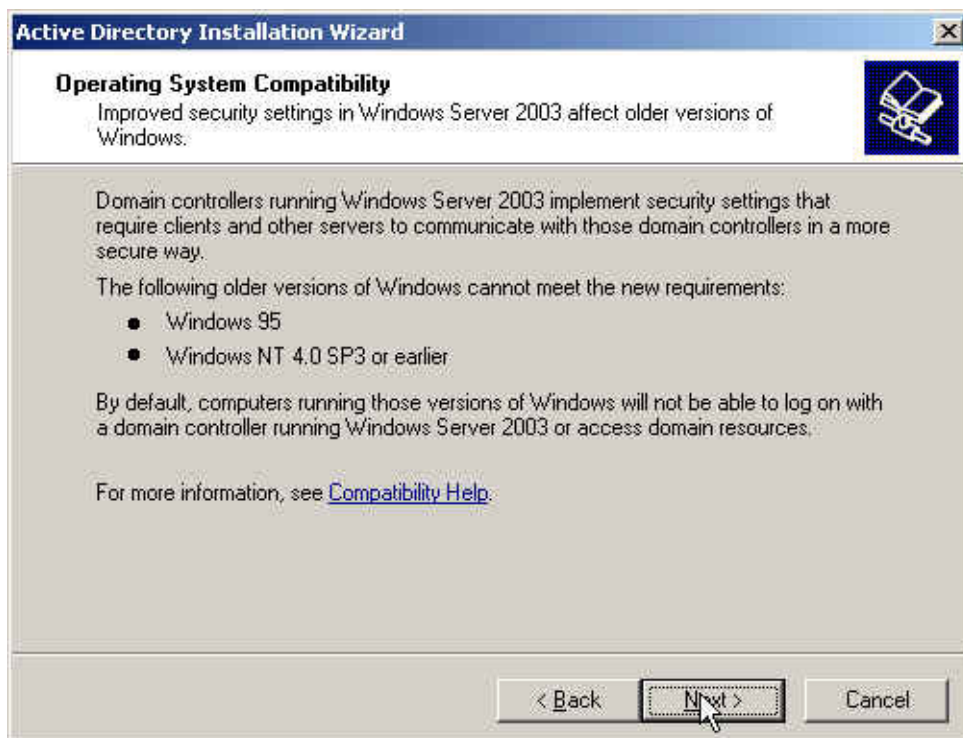


**Step6.** In **Active Directory Installation Wizard** window, click **Next**.



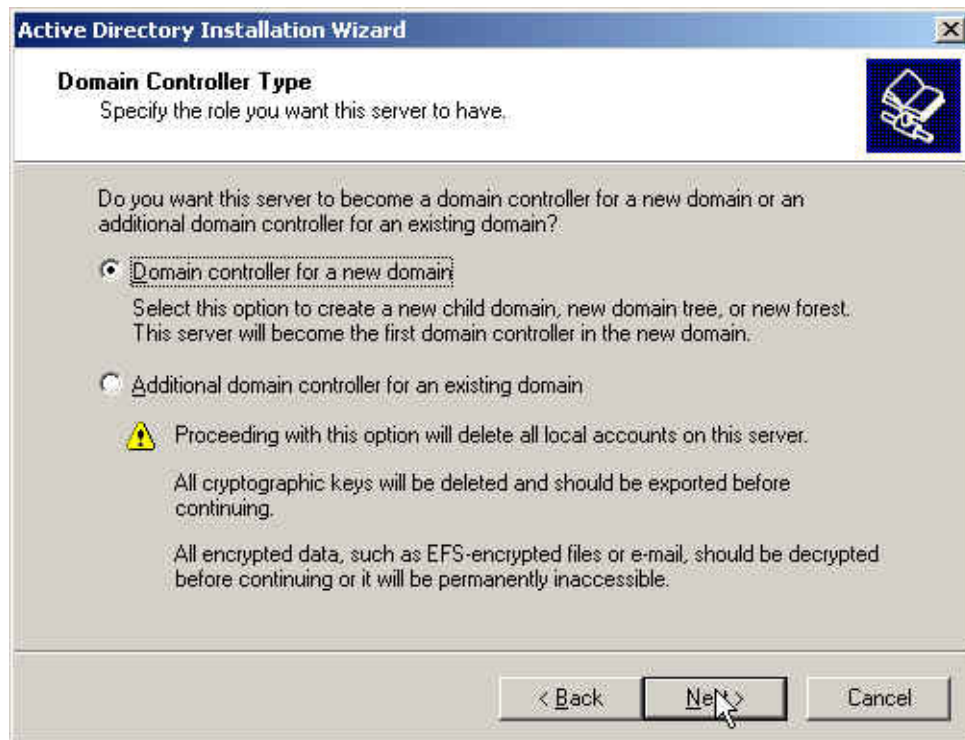
Active directory installation wizard

**Step7.** In **Operating System Compatibility** window, click **Next**.



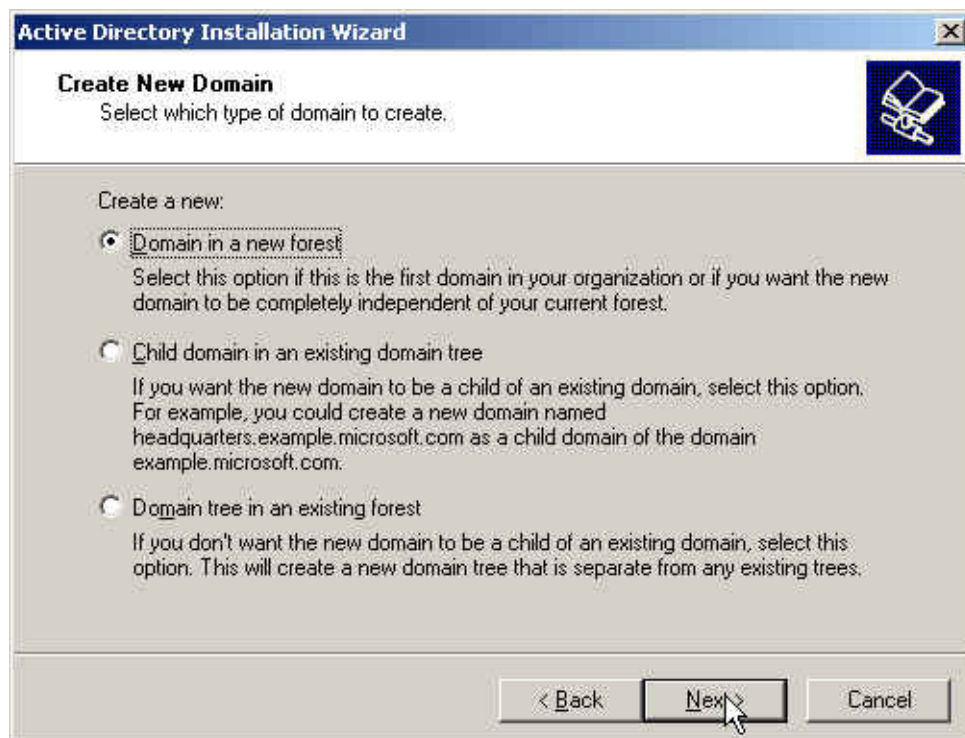
The operating system compatibility window

**Step8.** In **Domain Controller Type** window, select **Domain controller for a new domain** click **Next**.



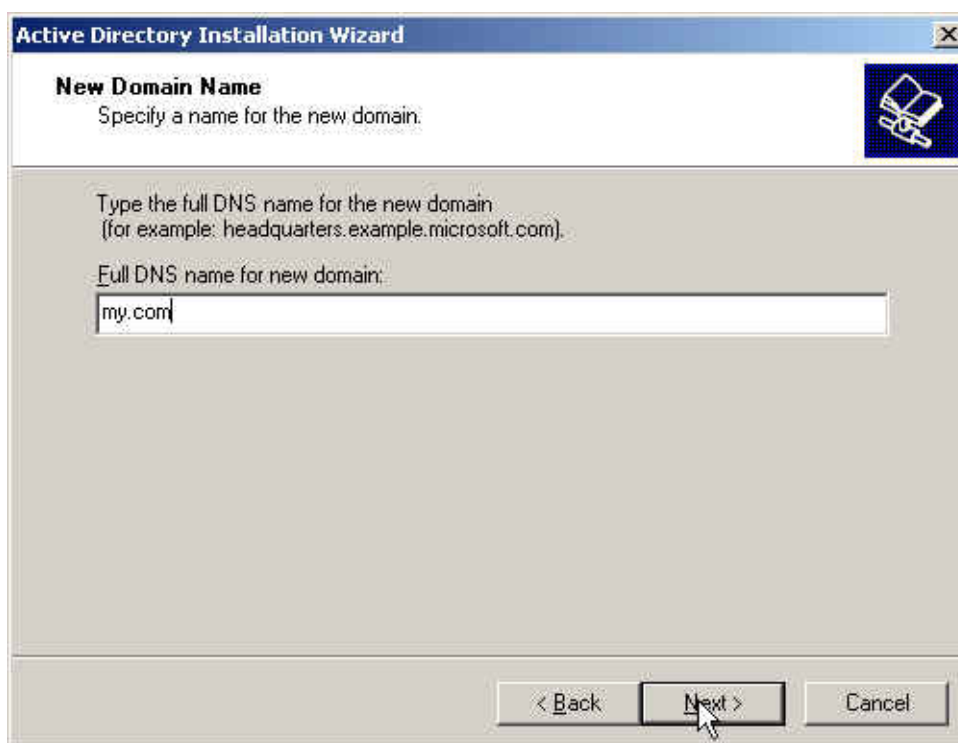
The domain controller type window

**Step9.** In **Create New Domain** window, select **Domain in a new forest**, click **Next**.



Create new domain window


**Step10.** In **New Domain Name** window, enter the **Full DNS name for new domain**, click **Next**.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'New Domain Name' step. The window has a title bar with the text 'Active Directory Installation Wizard' and a close button. Below the title bar, the section 'New Domain Name' is displayed with the instruction 'Specify a name for the new domain.' To the right of this section is a blue icon of a computer with a hand. The main area of the window contains the text 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' followed by 'Full DNS name for new domain:' and a text input field containing 'my.com'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

The new domain name window

**Step11.** In **NetBIOS Domain Name** window, enter the **Domain NetBIOS name**, click **Next**.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'NetBIOS Domain Name' step. The window has a title bar with the text 'Active Directory Installation Wizard' and a close button. Below the title bar, the section 'NetBIOS Domain Name' is displayed with the instruction 'Specify a NetBIOS name for the new domain.' To the right of this section is a blue icon of a computer with a hand. The main area of the window contains the text 'This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.' followed by 'Domain NetBIOS name:' and a text input field containing 'My'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

The NetBIOS domain name window

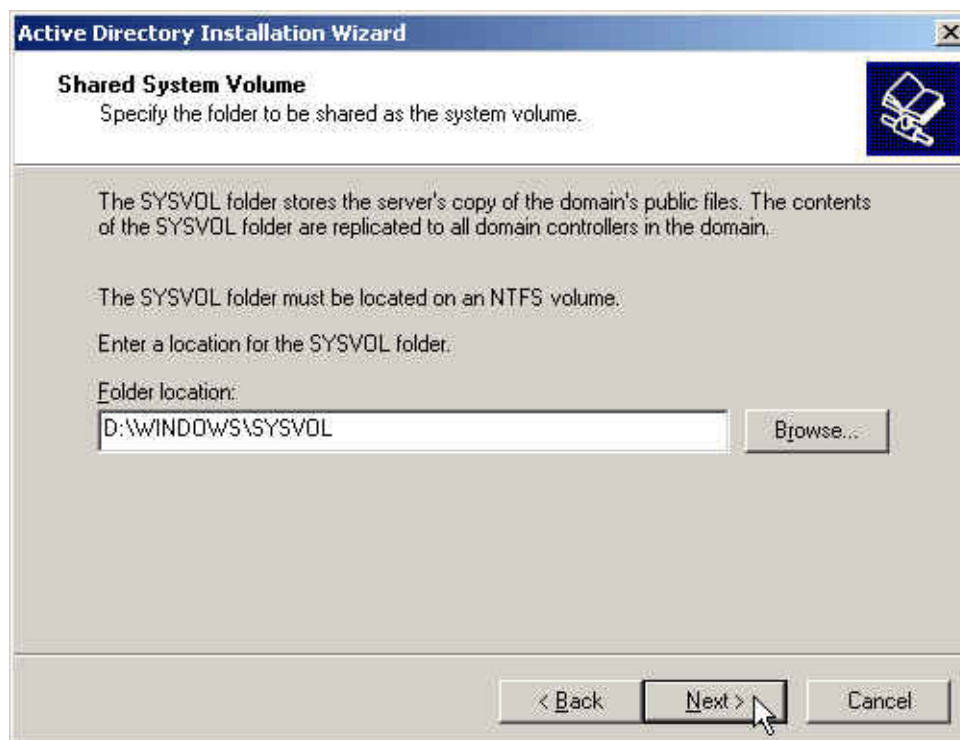
- Step12.** In **Database and Log Folders** window, enter the routes of **Database folder** and **Log folder**, click **Next**.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Database and Log Folders' step. The window title is 'Active Directory Installation Wizard'. The main heading is 'Database and Log Folders' with a sub-instruction: 'Specify the folders to contain the Active Directory database and log files.' Below this, a note states: 'For best performance and recoverability, store the database and the log on separate hard disks.' The first question is 'Where do you want to store the Active Directory database?' followed by a text box labeled 'Database folder:' containing 'D:\WINDOWS\NTDS' and a 'Browse...' button. The second question is 'Where do you want to store the Active Directory log?' followed by a text box labeled 'Log folder:' containing 'D:\WINDOWS\NTDS' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

**The database and log folder window**

- Step13.** In **Shared System Volume** window, enter the **Folder location**, click **Next**.

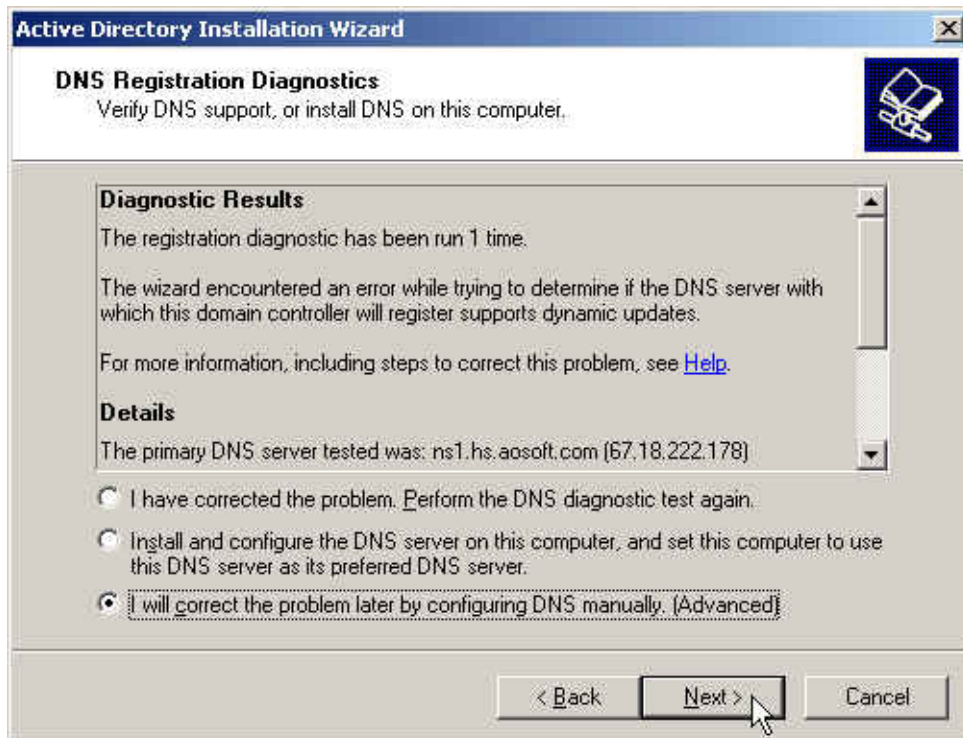


The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Shared System Volume' step. The window title is 'Active Directory Installation Wizard'. The main heading is 'Shared System Volume' with a sub-instruction: 'Specify the folder to be shared as the system volume.' Below this, a note states: 'The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.' Another note states: 'The SYSVOL folder must be located on an NTFS volume.' The instruction is 'Enter a location for the SYSVOL folder.' followed by a text box labeled 'Folder location:' containing 'D:\WINDOWS\SYSVOL' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

**The shared system volume window**

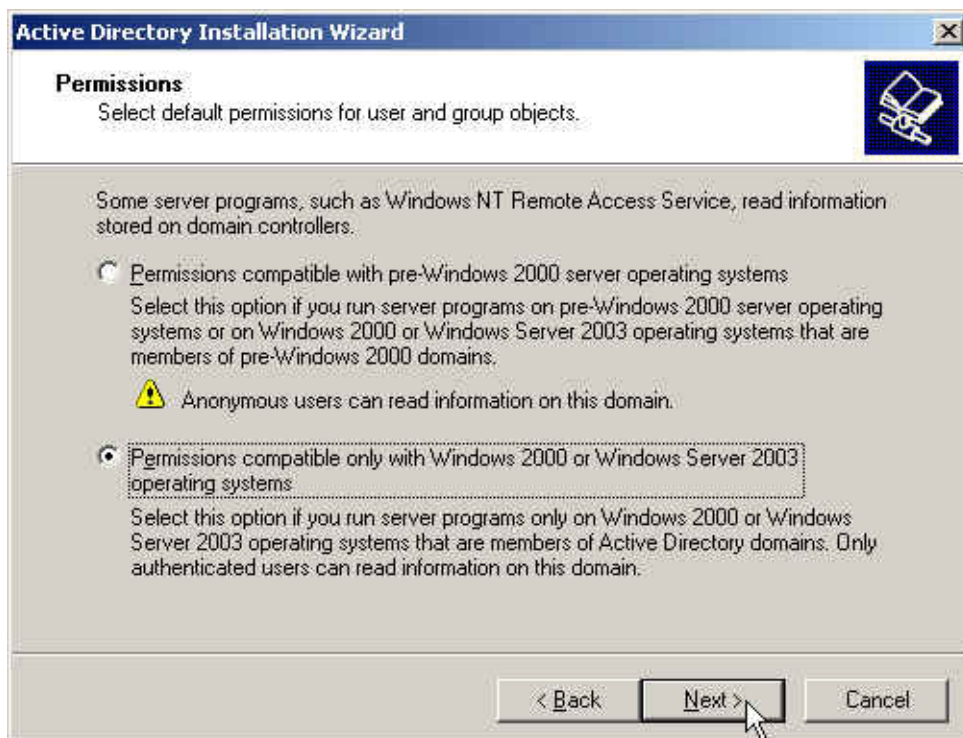


- Step14.** In **DNS Registration Diagnostics** window, select **I will correct the problem later by configuring DNS manually (Advanced)**, click **Next**.



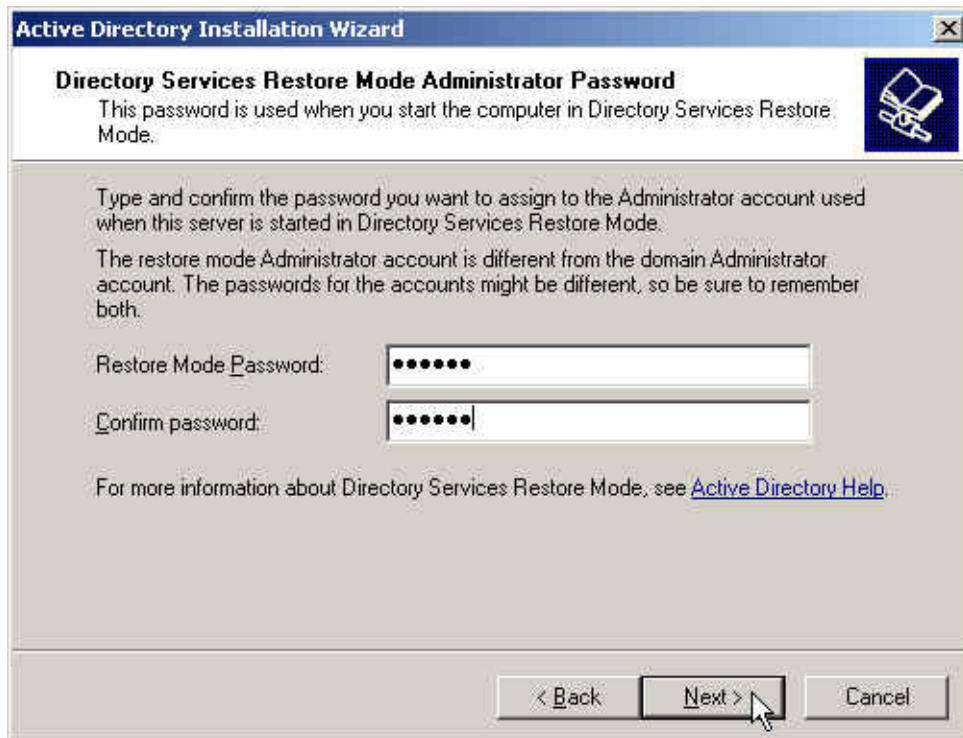
**The DNS registration diagnostics window**

- Step15.** In **Permissions** window, select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**, click **Next**.



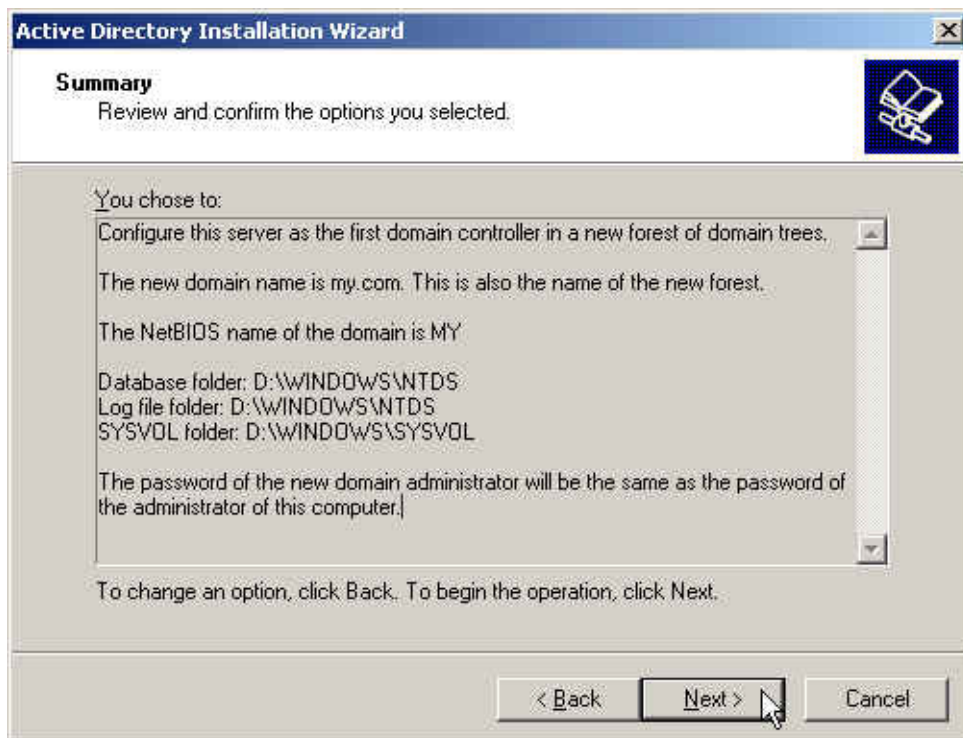
**The permissions window**

- Step16.** In **Directory Services Restore Mode Administrator Password** window, enter the **Restore Mode Password** and **Confirm password**, click **Next**.



The directory services restore mode administrator password window

- Step17.** In **Summary** window, click **Next**.



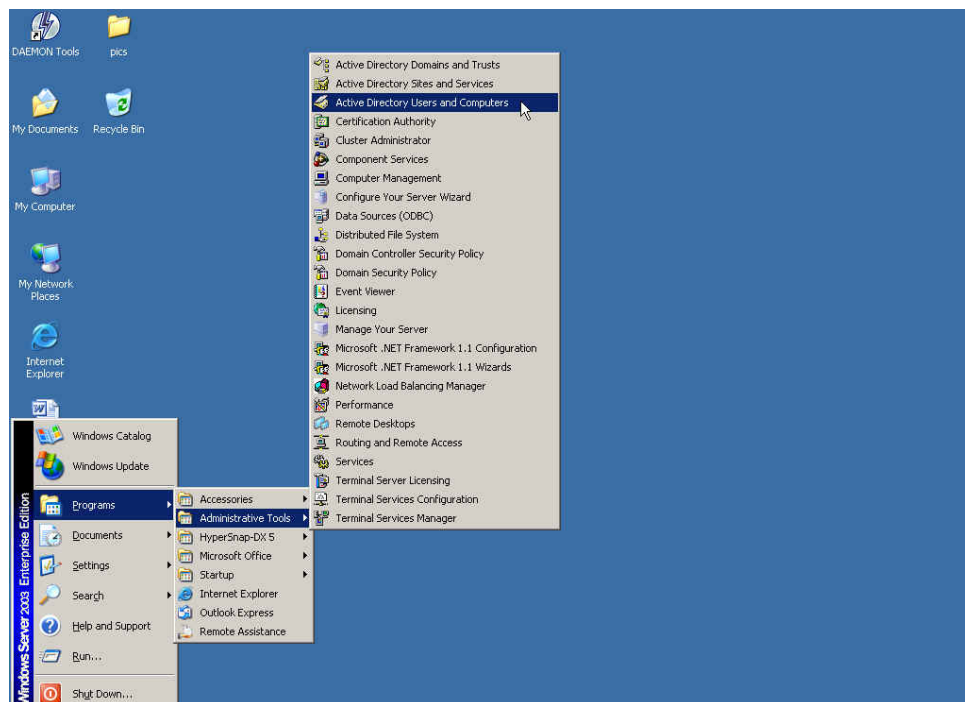
The summary window

**Step18.** Complete the Active Directory installation wizard.



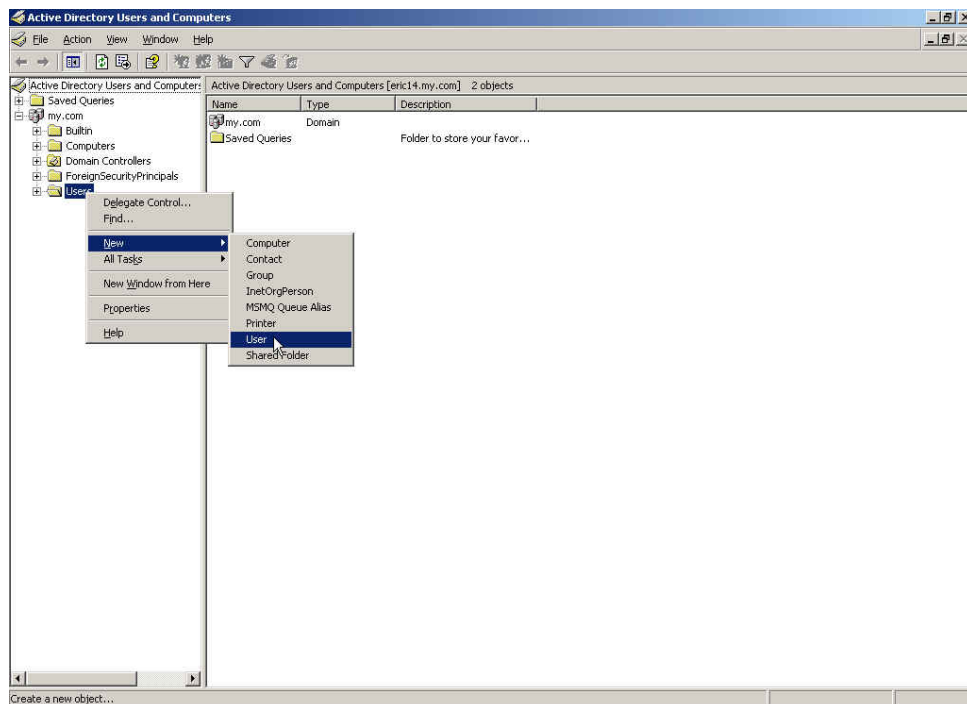
Complete the active directory installation wizard

**Step19.** Click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.



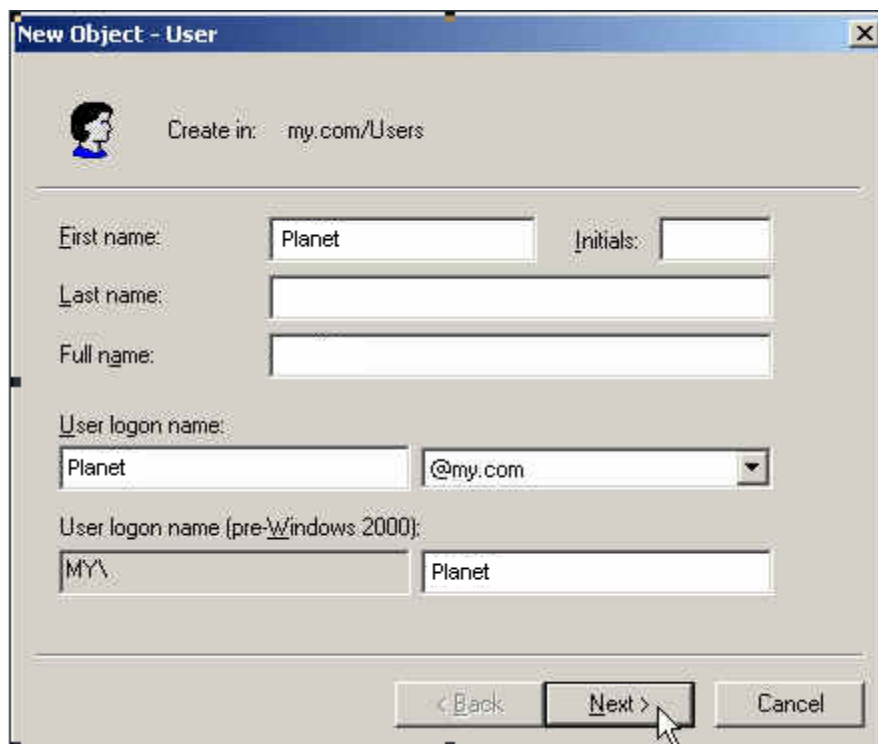
Enable active directory users and computers

**Step20.** In **Active Directory Users and Computers** window, right click on the **Users**, select **New → User**.



Add new active directory user


**Step21.** In **New Object–User** window, enter the settings, click **Next**.



The new object – user setting window 1



**Step22.** In **New Object –User** window, enter the password, click **Next**.



The screenshot shows the 'New Object - User' window. At the top, it says 'Create in: my.com/Users'. Below this, there are two password input fields. The first is labeled 'Password:' and the second is labeled 'Confirm password:'. Both fields contain a series of dots. Below the password fields, there are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

**The new object – user setting window 2**

**Step23.** Complete to add the user.



The screenshot shows the 'New Object - User' window. At the top, it says 'Create in: my.com/Users'. Below this, there is a text box that says 'When you click Finish, the following object will be created:'. Inside this text box, there are three lines of text: 'Full name: Planet', 'User logon name: Planet@my.com', and 'The password never expires:'. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. A mouse cursor is pointing at the 'Finish' button.

**Complete to add the user**

**Step24.** In **Authentication → LDAP** , enter the following setting :

LDAP Server		
<input checked="" type="checkbox"/> Enable LDAP Server Authentication	<a href="#">Test</a>	
LDAP Server ( IP or Domain Name )	192.168.1.10	( Max. 80 characters )
LDAP Server Port	389	( Range: 389 or 1025 - 65535 )
Search Distinguished Name	dc=my,dc=com	( Max. 511 characters, ex: dc=mydomain,dc=com )
LDAP Filter	(objectClass=*)	( Max. 255 characters, ex: (objectClass=*) )
User Distinguished Name	cn=Planet,cn=Users,dc=m	( Max. 1023 characters, ex: cn=users,dc=mydomain,dc=com )
Password	*****	( Max. 127 characters )

#### The LDAP server setting



Click **Test** , it can detect if the CS-2000 and LDAP server can real working .

**Step25.** In **Authentication → User Group**, add **LDAP User**.




New Authentication Group		
Name:	LDAP_auth	(Max. 16 characters)
<div> <div>&lt;--- Available Authentication User ---&gt;</div> <div> alex eva joe (Radius User) (POP3 User) (LDAP User) </div> </div>	<div> <div>Remove</div> <div>Add</div> </div>	<div> <div>&lt;--- Selected Authentication User ---&gt;</div> <div> (LDAP User) </div> </div>

#### Add new LDAP user

**Step26.** In **Policy → Outgoing**, apply Step25. (The authentication group) in to the policy setting.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	LDAP_auth ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

### The LDAP server authentication in policy setting

Source	Destination	Service	Action	Option								Configure			Move
Inside_Any	Outside_Any	DNS										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 ▾
Inside_Any	Outside_Any	ANY										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 2 ▾

[New Entry](#)

### Complete the LDAP server authentication in policy setting

**Step27.** When the users want to connect to the network, it will show the authentication window. Enter the user name and password , click **OK**, then link to the network through the CS-2000 appliance

User Login

User Authentication	
User Name	<input type="text"/> ( ex: auth_user1 )
Password	<input type="password"/>

Welcome to CS-2000 Test Authentication Page!!!!

**[Link to the network through the authentication](#)**

## 5.6 Content Blocking

# **Content Blocking**

The content blocking included the **URL, Script, Upload and Download**.

1. **URL** : The MIS engineer can decide to open or limit the specific web site through the complete domain name, keywords and wildcards. ( ~ and \* ) .
2. **Script** : The access competency of Pop-up, ActiveX, Java Applet, Cookie in the blocking URL.
3. **Download** : To limit the competency of downloading the specific extension files and media files from the internet by http or ftp protocol.
4. **Upload** : To limit the privilege of uploading the specific extension files by http or ftp protocol.

## **Content Blocking :**

### **URL String**

- The domain name restricted by the CS-2000 appliance which can decide to allow or limit the competency to use the domain.

### **Popup**

- Can block the popup window when browsing the web site.

### **ActiveX**

- Can block the ActiveX packets from the web site.

### **Java Applet**

- Can block the Java packets from the web site.

### **Cookie**

- Can block the cookie packets from the web site.

### **Audio and Video Types**

- Can limit the user to transfer the audio and video files through http or ftp.

### **Extension**

- Can limit the user to transfer the extension files through http or ftp.

### **All Types**

- Can limit the user to transfer the audio, video and specific extension files through http or ftp.

**We set 4 application environments of Content Blocking.**

<b>No.</b>	<b>Range</b>	<b>The Application Environment</b>	<b>Pages</b>
<b>Example 1</b>	<b>URL</b>	Only permit the LAN user to access the data in specific web site.	<b>118</b>
<b>Example 2</b>	<b>Script</b>	To limit the LAN user to access the script data in the web site.	<b>121</b>
<b>Example 3</b>	<b>Download</b>	To limit the LAN user to download the extension files, video and audio files in the internet through http or ftp.	<b>123</b>
<b>Example 4</b>	<b>Upload</b>	To limit the LAN user to upload the extension files on the internet through http or ftp.	<b>125</b>

## Example 1. URL

**Only permit the LAN user to access the data in specific web site.**

※ The way to use the content blocking

**Symbol** : ~ , the symbol means to open ; \* , the symbol means the Wildcards .

**To limit the user not to enter the specific web site. :**

In add new URL string, enter the complete domain name or keywords in the forbidden web site.

For example : [www.kcg.gov.tw](http://www.kcg.gov.tw) or gov.

**To permit the user to enter the specific web site :**

1. First of all, enter the complete **Domain Name** or **Keywords** in to the URL blocking setting, and add the symbol “ ~ “ which represents permitted to enter.  
For example , ~[www.kcg.gov.tw](http://www.kcg.gov.tw) or ~gov .
2. Complete all the setting of opened web site; add the new URL blocking policy to forbid all the web site. Type the Wildcard of \* in the URL string to forbid all.



**Attention !** The forbidden command must be placed in the end of all the setting process. If the MIS engineer wants to add the URL to opened, he has to remove all the forbidden command then enter the new domain name. After complete all the process, he has to enter all the forbidden command again.



**Step1.** In **Content Blocking** → **URL** , add the following setting :

- Click **New Entry**.
- **URL String**, enter ~yahoo. Click **OK**.
- Click **New Entry**.
- **URL String**, enter ~google. Click **OK**.
- Click **New Entry**.
- **URL String** , enter \* . Click **OK**.
- Complete the URL setting.

URL String▼	Configure
~yahoo	<a href="#">Modify</a> <a href="#">Remove</a>
~google	<a href="#">Modify</a> <a href="#">Remove</a>
*	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

The URL setting

**Step2.** In **Policy → Outgoing**, apply the **Content Blocking** setting in to the policy.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**The URL content blocking setting in policy**

**Step3.** In **Policy → Outgoing**, complete the setting to permit the user can only access the data in specific web site through the policy.

Source	Destination	Service	Action	Option				Configure			Move
Inside_Any	Outside_Any	ANY						<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1
<a href="#">New Entry</a>											

**Completer the URL content blocking setting in policy**



The user can only browse the domain name of “yahoo” and “google” in the web site through the policy.

## Example 2. Script

To limit the LAN user to access the script data in the web site.

**Step1.** In **Content Blocking** → **Script** , select the following setting :

- Select **Popup**.
- Select **ActiveX**.
- Select **Java**.
- Select **Cookie**.
- Click **OK**.
- Complete the script setting



**The script setting**

**Step2.** In **Policy → Outgoing** , apply the **Script Content Blocking Setting** in to policy :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input checked="" type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**The script content blocking in policy setting**

**Step3.** In **Policy → Outgoing** , to complete the settings to limit the LAN user accessing the script data in the web site through the policy :

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

**Complete the script content blocking settings**



The user can not use the specific function in the web site (For example, JAVA, cookie...) when browsing the web pages through the policy. This function can forbid the user to browse the stock exchange web site and so on. (The browser can not display the market summary charts)

### Example 3. Download Blocking

To limit the LAN user to download the extension files, video and audio files in the internet through http or ftp.

**Step1.** In **Content Blocking** → **Download**, add the following settings :

- Select **All Types**.
- Click **OK**.
- Complete the settings

Download

☒ All Types  
☐ Audio and Video Types

Extension

<input type="checkbox"/> .exe	<input type="checkbox"/> .zip	<input type="checkbox"/> .rar
<input type="checkbox"/> .iso	<input type="checkbox"/> .bin	<input type="checkbox"/> .rpm
<input type="checkbox"/> .doc	<input type="checkbox"/> .xl?	<input type="checkbox"/> .ppt
<input type="checkbox"/> .pdf	<input type="checkbox"/> .tgz	<input type="checkbox"/> .gz
<input type="checkbox"/> .bat	<input type="checkbox"/> .dll	<input type="checkbox"/> .hta
<input type="checkbox"/> .scr	<input type="checkbox"/> .vb?	<input type="checkbox"/> .wps
<input type="checkbox"/> .pif	<input type="checkbox"/> .msi	<input type="checkbox"/> .com
<input type="checkbox"/> .reg	<input type="checkbox"/> .mp3	<input type="checkbox"/> .mpeg
<input type="checkbox"/> .mpg	<input type="checkbox"/> .wma	<input type="checkbox"/> .rmvb
<input type="checkbox"/> .rm	<input type="checkbox"/> .avi	<input type="checkbox"/> .wmv
<input type="checkbox"/> .3gp	<input type="checkbox"/> .mov	<input type="checkbox"/> .asf
<input type="checkbox"/> .mp4	<input type="checkbox"/> .amv	<input type="checkbox"/> .ram

OK Cancel

Download blocking setting

**Step2.** In **Policy → Outgoing**, apply the **Download Content Blocking** settings in to the policy.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input checked="" type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**The download content block setting in policy**

**Step3.** In **Policy → Outgoing**, complete the settings to limit the LAN user to transfer the video and audio files and specific extension files in the network.

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY							<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1

[New Entry](#)

**Complete the download content blocking setting in policy**

## Example 4. Upload Blocking

To limit the LAN user to upload the extension files on the internet through http or ftp.

**Step1.** In **Content Blocking→ Upload Blocking** , set the following settings :

- Select **ALL Types Blocking**.
- Click **OK**.
- Complete the upload setting.

Upload

☒ All Types

Extension

<input type="checkbox"/> .exe	<input type="checkbox"/> .zip	<input type="checkbox"/> .rar
<input type="checkbox"/> .iso	<input type="checkbox"/> .bin	<input type="checkbox"/> .rpm
<input type="checkbox"/> .doc	<input type="checkbox"/> .xl?	<input type="checkbox"/> .ppt
<input type="checkbox"/> .pdf	<input type="checkbox"/> .tgz	<input type="checkbox"/> .gz
<input type="checkbox"/> .bat	<input type="checkbox"/> .dll	<input type="checkbox"/> .hta
<input type="checkbox"/> .scr	<input type="checkbox"/> .vb?	<input type="checkbox"/> .wps
<input type="checkbox"/> .pif	<input type="checkbox"/> .msi	<input type="checkbox"/> .com
<input type="checkbox"/> .reg	<input type="checkbox"/> .mp3	<input type="checkbox"/> .mpeg
<input type="checkbox"/> .mpg	<input type="checkbox"/> .wma	<input type="checkbox"/> .rmvb
<input type="checkbox"/> .rm	<input type="checkbox"/> .avi	<input type="checkbox"/> .wmv
<input type="checkbox"/> .3gp	<input type="checkbox"/> .mov	<input type="checkbox"/> .asf
<input type="checkbox"/> .mp4	<input type="checkbox"/> .amv	<input type="checkbox"/> .ram

OK Cancel

The upload setting

**Step2.** In **Policy → Outgoing**, apply the **Upload Content Blocking** settings in to the policy.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input checked="" type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

The upload content block setting in policy

**Step3.** In **Policy → Outgoing**, complete the settings to limit the LAN user to upload the video and audio files and specific extension files in the network.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1

[New Entry](#)

Complete the upload content blocking setting in policy



## 5.7 IM/P2P Blocking

# **IM/P2P Blocking**

MIS engineer can limit user to use IM and P2P software by using **IM / P2P Blocking** function.

### **1. IM :**

Set the login privilege of MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger, Skype, Google Talk and Gadu-Gadu Messenger.

### **2. P2P :**

Set the connection privilege of eDonkey, eMule, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, VNN Client, PPLive, UltraSurf and PPStream.

## Setting

### IM/P2P Signature Definitions

- System can update the IM / P2P signature definitions every one hour, or user can manually update it instantly. System will show the update time and version of IM / P2P signature definitions.

### IM Blocking

- Set the login privilege of MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger, Skype, Google Talk and Gadu-Gadu Messenger.

### P2P Blocking

- Set the connection privilege of eDonkey, eMule, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, VNN Client, PPLive, UltraSurf and PPStream.

We set two examples:

No.	Range	Environment	Pages
Example 1	IM	Limit internal user transfer messages, files and media files by IM software.	130
Example 2	P2P	Limit internal user access internet resources by P2P software.	132

## Example 1. IM Blocking

Limit internal user transfer messages, files and media files by IM software.

**Step1.** In **IM / P2P Blocking** → **Setting**, add the following settings :

- Click **New Entry**
- Enter the **Name** called IM\_Blocking.
- Select **MSN Messenger, Yahoo Messenger, ICQ Messenger, QQ Messenger, Skype, Google Talk and Gadu-Gadu Messenger.**
- Click **OK**.
- Complete the settings

**Add IM / P2P Blocking**

Name  (Max. 16 characters)

Instant Messaging

☒ MSN ☒ Yahoo ☒ ICQ

☒ QQ ☒ Skype ☒ Google Talk

☒ Gadu-Gadu

---

Peer-to-Peer Application

☐ Edonkey ☐ Bit Torrent ☐ WinMX

☐ Foxy ☐ KuGoo ☐ AppleJuice

☐ AudioGalaxy ☐ DirectConnect ☐ iMesh

☐ MUTE ☐ Thunder5 ☐ VNN Client

☐ PPLive ☐ UltraSurf ☐ PPStream

**IM blocking setting**

**IM / P2P Signature Definitions**

Last updated on : 07/07/04 13:09:41 (Update signature definitions every one hour)

Current version: 1.2.7 (Signature definitions updated at 07/06/25 13:11:41 )

Update signature definitions immediately (Use TCP port: 80 and UDP port: 53)  [Test](#)

---

**IM / P2P Blocking**

Total entry : 1

Name	IM	P2P	Configure
IM_Blocking	MSN,Yahoo,ICQ...	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Complete the IM blocking setting**

**Step2.** In **Policy → Outgoing**, add one policy applied to IM blocking setting.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
M / P2P Blocking	IM_Blocking
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**Set the policy applied to IM blocking setting**

**Step3.** In **Policy → Outgoing**, complete the policy setting of limit internal user to transfer messages, files and media files.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1

[New Entry](#)

**Complete the policy setting of IM blocking**

## Example 2. P2P Blocking

Limit internal user access internet resources by P2P software.

**Step1.** In **IM / P2P Blocking** → **Setting**, add the following settings :

- Click **New Entry**.
- Enter the **Name** of P2P\_Blocking.
- Select **eDonkey, eMule, Bit Torrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, VNN Client, PPLive, UltraSurf and PPStream**.
- Click **OK**.
- Complete the settings.

Add IM / P2P Blocking

Name  (Max. 16 characters)

Instant Messaging

☐ MSN ☐ Yahoo ☐ ICQ

☐ QQ ☐ Skype ☐ Google Talk

☐ Gadu-Gadu

---

Peer-to-Peer Application

☒ Edonkey ☒ Bit Torrent ☒ WinMX

☒ Foxy ☒ KuGoo ☒ AppleJuice

☒ AudioGalaxy ☒ DirectConnect ☒ iMesh

☒ MUTE ☒ Thunder5 ☒ VNN Client

☒ PPLive ☒ UltraSurf ☒ PPStream

**P2P blocking setting**

IM / P2P Signature Definitions

Last updated on : 07/07/04 13:09:41 (Update signature definitions every one hour)

Current version: 1.2.7 (Signature definitions updated at 07/06/25 13:11:41 )

Update signature definitions immediately (Use TCP port: 80 and UDP port: 53)  [Test](#)

---

IM / P2P Blocking

Total entry : 1

Name▼	IM	P2P	Configure
P2P_Blocking	---	Edonkey, Bit Torrent, WinMX...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Complete the P2P blocking setting**

**Step2.** In **Policy → Outgoing**, add one policy applied to P2P blocking setting.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	P2P_Blocking
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**Set the policy applied to P2P blocking**

**Step3.** In **Policy → Outgoing**, complete the policy setting of limit internal user to access internet resources by P2P software.

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

[New Entry](#)

**Complete the Policy setting of P2P blocking**



Use P2P will seriously occupy network bandwidth and it can change its service port. So the MIS engineer not only set the service port in **Service**, but also need to set **IM / P2P Blocking → P2P Blocking**.

## 5.8 Virtual Server

# Virtual Server

When the MIS engineer apply the network connection from the ISP provider, the provided real IP is usually not enough to give to all the users. Normally, the MIS engineer can use the private IP address transfer to the real IP address via the CS-2000's NAT (Network Address Translation) function, in order to give the sufficient IP address to every user. If the MIS engineer set the server which provides the external service in LAN, then the external user can not link to the internal private IP address.

According to this problem, the MIS engineer can use the CS-2000's virtual server function to solve the problem. The so called virtual server is to map the real IP address to the private IP address via the CS-2000 appliance.

The virtual server also includes the features, called **One to Many** map function. It means one real IP address can map to the private IP address in four LAN servers which provide the same service. It is because the virtual server can provide the **Load Balance** function which can provide the proper bandwidth to the LAN server group depends on the sessions. In other words, the function can reduce the problem of **System Crash and bandwidth distribution**, to make the server can work more efficiently.

In this Chapter, we will make the introduction of **Mapped IP** and **Server 1/2/3/4**.

### **Mapped IP :**

The LAN IP address is a kind of private IP address which is transferred via the NAT (Network Address Translation). So the external user can not directly link to the private IP address. In other words, the external user has to link the CS-2000's external **real IP address**, then map to the internal private IP address via the CS-2000 appliance. That means the external real IP address mapped to the LAN private IP address.

### **Server 1/2/3/4 Interface :**

It is almost the same as the IP mapped function. The difference is that the virtual server use the **one to many** IP mapped. That means one real IP address mapped to 1~4 LAN private IP address. The virtual server also provides the service items as the same in the **Service** function.



## Virtual Server

### WAN IP

- The external IP address (**Real** IP Address).

### Mapped To Virtual IP

- The WAN real IP address mapped to the LAN server private IP address.

### Virtual Server Real IP

- The virtual server mapped to the WAN IP address.

### Service

- The service provided by the virtual server.

### WAN Port

- The external port provided by the virtual server. If the selected service using only single port, then the MIS engineer can change its external port.( For example, the MIS engineer can modify the http port to be 8080; If the external user want to browse the web site, then he must change the port. )

### Server Virtual IP

- The virtual IP address which the virtual server mapped to.

**We set 4 virtual server application environments.**

No .	Range	The Application Environment	Pages
<b>Example 1</b>	<b>Mapped IP</b>	To make the single internal server which provides the services of FTP, web, mail, can real working by the policy.	<b>137</b>
<b>Example 2</b>	<b>Virtual Server</b>	Use the virtual server instead of many of the internal server which only provides single service by policy management. (For example, use the web service).	<b>140</b>
<b>Example 3</b>	<b>Virtual Server</b>	The external users use the VoIP to communicate to the internal user. ( VoIP service port : TCP 1720 , TCP 15328-15333 , UDP 15328-15333 )	<b>142</b>
<b>Example 4</b>	<b>Virtual Server</b>	Use the virtual server instead of many of the internal server which provide the same services by policy management.(For example , use the HTTP , POP3 , SMTP , DNS service group)	<b>145</b>

### **The Deployment**

To apply two ADSL lines included the static IP address.

( WAN1 static IP is 61.11.11.10 ~ 61.11.11.14 )

( WAN2 static IP is 211.22.22.18 ~ 211.22.22.30 )

## Example 1

To make the single internal server which provides the services of FTP, web, mail, can real working by the policy.

- Step1.** Sets one LAN server which provides the multiple services. The network adapter IP setting is 192.168.1.100, and the DNS setting correspond to the WAN DNS server.
- Step2.** In **Address** → **LAN**, add the following settings.

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

New Entry

The server setting in address

- Step3.** In **Virtual Server** → **Mapped IP** , add the following settings :
- Click **New Entry**.
  - **WAN IP**, enter 61.11.11.12 ( Or click **Assist** to select ) .
  - **Map To Virtual IP**, enter 192.168.1.100.
  - Click **OK**.
  - Complete the mapped IP setting.

Add New Mapped IP			
WAN IP	61.11.11.12	WAN1 ▼	<a href="#">Assist</a>
Map To Virtual IP	192.168.1.100		

OK Cancel

The mapped IP setting

**Step4.** In **Service → Group**, to group the services (DNS, FTP, HTTP, POP3, SMTP...) provided by the server. Add the new mail service group which can send the mail to external.

Group name▼	Service	Configure
mail_service	DNS,IMAP,POP3...	<a href="#">In Use</a>
Main_Service	DNS,HTTP,POP3...	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

The service group setting

**Step5.** In **Policy → Incoming**, add the new policy included Step 3, Step 4.

Source	Destination	Service	Action	Option					Configure			Move
Outside_Any	Mapped IP(61.11.11.12)	Main_Service							<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 ▼

[New Entry](#)

Complete the incoming setting in policy

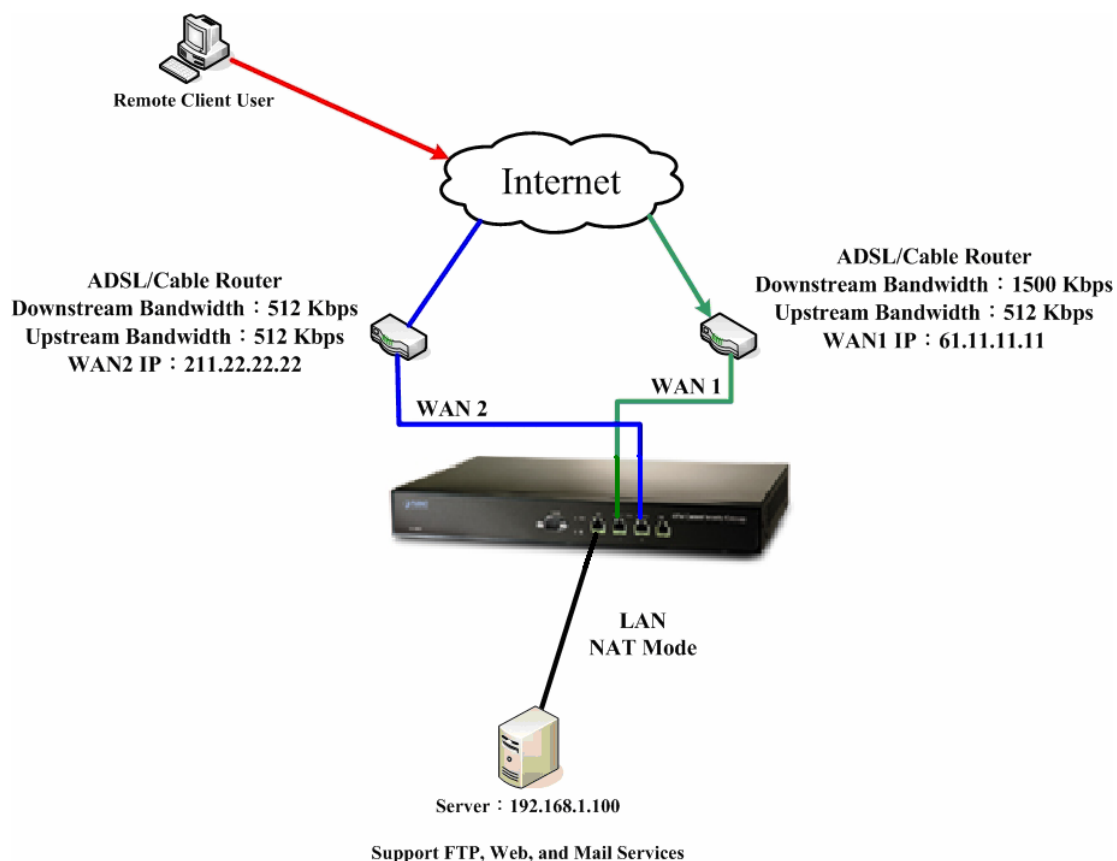
**Step6.** In **Policy → Outgoing**, add the new policy included Step2, Step 4; It can make the server send the e-mail to external mail server via the mail service.

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	Main_Service							<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 ▼

[New Entry](#)

Complete the outgoing setting in policy

**Step7.** Complete the IP mapped setting which provided the multiple services to external.



**Set up the single server environment which provided the multiple services via IP mapped**



When the MIS engineer set the IP mapped by policy, it is strongly recommended not to select **ANY** in **Service** function. Because that may cause the IP mapped user is attacked.

## Example 2

Use the virtual server instead of many of the internal server which only provides single service by policy management. (For example, use the web service)

**Step1.** To set up many LAN server which provide the web service. The IP addresses are 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104.

**Step2.** In **Virtual Server → Server 1**, add the new following settings :

- Click **Virtual Server Real IP → Click Here to configure.**
- **Virtual Server Real IP**, enter 211.22.22.23. ( Or click **Assist** to select )
- Click **OK**.
- Click **New Entry**.
- **Service**, select HTTP (80).
- External service port, enter 8080.
- **Load Balance Port 1**, enter 192.168.1.101.
- **Load Balance Port 2**, enter 192.168.1.102.
- **Load Balance Port 3**, enter 192.168.1.103.
- **Load Balance Port 4**, enter 192.168.1.104.
- Click **OK**.
- Complete the virtual server setting.

Add New Virtual Server IP		
Virtual Server Real IP	211.22.22.23	WAN2 <a href="#">Assist</a>

### The virtual server IP setting

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	HTTP (80)
External Service Port	8080 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104

### The virtual server configuration

**Step3.** In **Policy → Incoming**, add the new policy include Step 2(The virtual server setting.

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

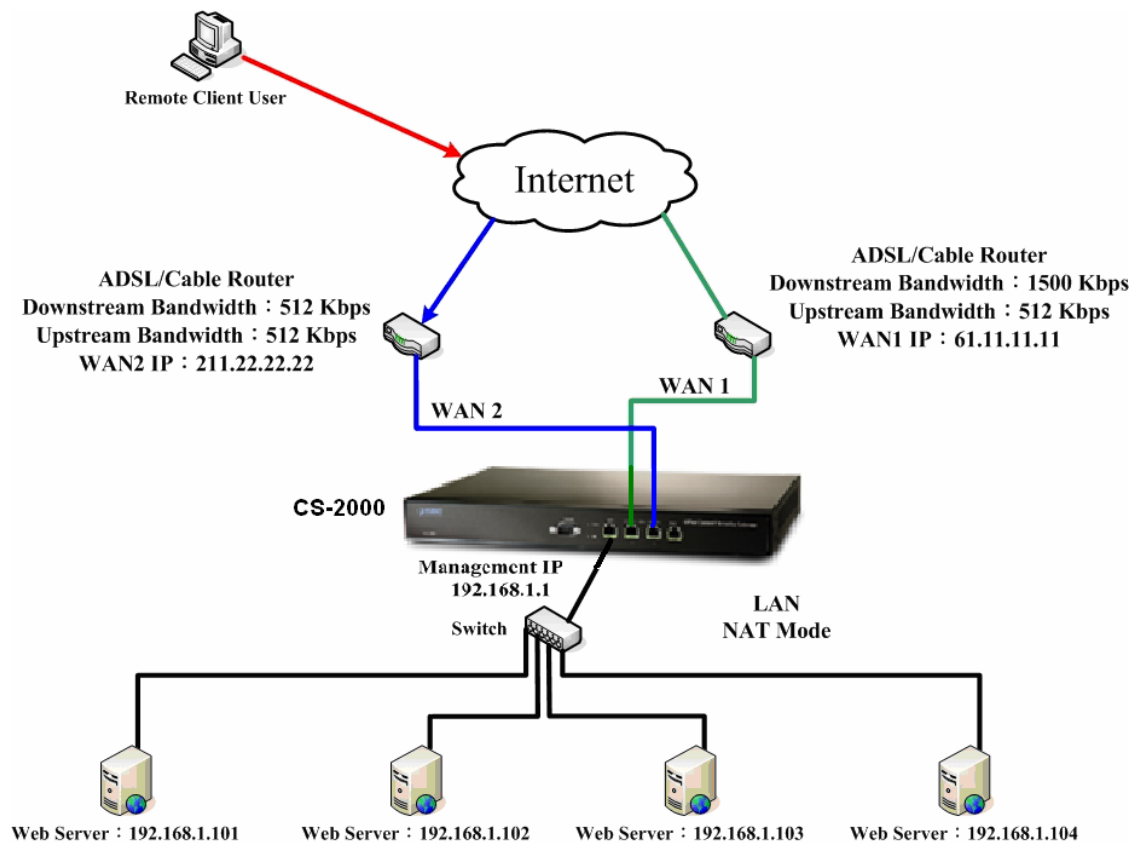
[New Entry](#)

**Complete the virtual server setting in the policy**



If the external user want to link to the homepage provided by the web server , then the user has to modify the port into 8080.

**Step4.** Make the virtual server can provide the single service to external.



**Use the virtual server instead of many internal servers to provide the single service**

### Example 3

The external users use the VoIP to communicate to the internal user. ( VoIP service port : TCP 1720, TCP 15328-15333, and UDP 15328-15333 )

**Step1.** To set the LAN VoIP, its IP address is 192.168.1.100.

**Step2.** In **Address** → **LAN**, add the new following setting.

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

New Entry

The LAN address setting

**Step3.** In **Service** → **Custom**, add new VoIP service group.

Service name▼	Protocol	Client Port	Server Port	Configure
VoIP	TCP	0:65535	1720:1720	Modify Remove

New Entry

Add the custom service



**Step4.** In **Virtual Server → Server 1** , add the new following settings :

- **Virtual Server Real IP → click here to configure.**
- **Virtual Server Real IP**, enter 61.11.11.12 ( Or click **Assist** to select ) .
- Click **OK**.
- Click **New Entry**.
- **Service**, select (Custom Service) VoIP\_Service.
- **External Service Port**, auto set From-Service (Custom).
- **Load Balance Server 1**, enter 192.168.1.100.
- Click **OK**.
- Complete the virtual server setting.

Add New Virtual Server IP	
Virtual Server Real IP	61.11.11.12 <span>WAN1</span> <a href="#">Assist</a>
<div>OK Cancel</div>	

#### The virtual server real IP setting

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.12
Service	(Custom Service)VoIP
External Service Port	From-Service(Custom) ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	
<div>OK Cancel</div>	

#### The virtual server setting



If the **Custom Service** only use **single port**, the MIS engineer can modify the external port in **Virtual Server** ; Contrarily, when the **Custom Service** uses **more than one port**, the MIS engineer can not modify the external service port in **Virtual Server**.

**Step5.** In **Policy → Incoming**, add the new policy included Step4. ( The virtual server setting )

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 2(61.11.11.12)	VoIP			Modify Remove Pause	To 1

[New Entry](#)

Complete the virtual server setting in policy

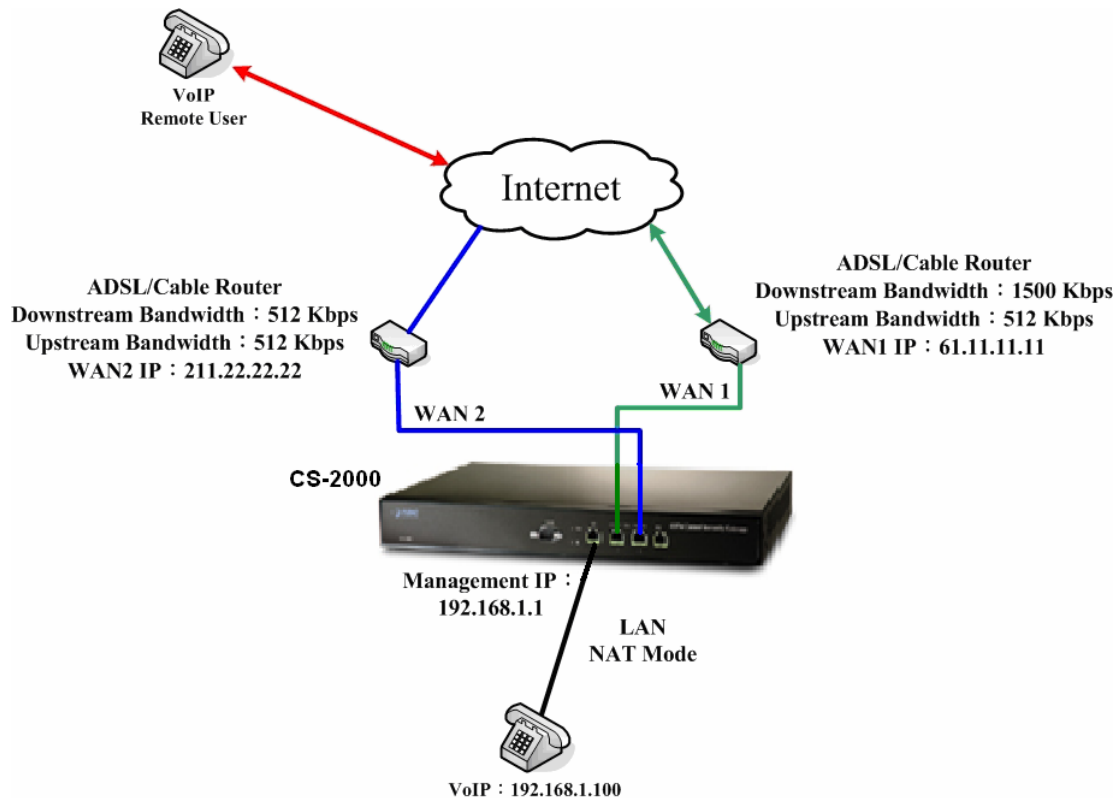
**Step6.** In **Policy → Outgoing**, complete the setting of LAN user use VoIP to communicate to external user.

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

[New Entry](#)

Complete the VoIP setting in policy

**Step7.** Make the virtual server provide the communication service between the internal and external user.



The deployment of using the communication service between the internal and external user via the virtual server

## Example 4

Use the virtual server instead of many of the internal server which provides the same services by policy management. (For example, use the HTTP, POP3, SMTP, DNS service group)

**Step1.** Sets many LAN server which provide multiple services , its network adapter IP address are 192.168.1.101 , 192.168.1.102 , 192.168.1.103 , 192.168.1.104 , and the DNS is correspond to the external DNS server .

**Step2.** In **Address → LAN** and **LAN Group**, add the new following setting.

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

New Entry

The setting of server mapped to name in address

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

New Entry

The LAN server group setting in address

**Step3.** In **Service → Group**, group the service. And add the new policy of service group for the server which can send the mails to external.

Group name▼	Service	Configure
mail_service	DNS,IMAP,POP3...	In Use
Main_Service	DNS,HTTP,POP3...	Modify Remove

New Entry

Add new service group

**Step4.** In **Virtual Server → Server 1** , add the new following settings :

- **Virtual Server Real IP → click here to configure**
- **Virtual Server Real IP**, enter 211.22.22.23 ( Or click **Assist** to select ) .
- Click **OK**.
- Click **New Entry**.
- **Service**, select (Group Service) Main\_ Service.
- **External Service Port**, auto set From-Service (Group).
- **Load Balance Server**, enter the server virtual IP.
- Click **OK**.
- Complete the virtual server setting.

Add New Virtual Server IP		
Virtual Server Real IP	211.22.22.23	WAN2 <a href="#">Assist</a>

#### The virtual server real IP setting

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.23
Service	(Group Service)Main_Service
External Service Port	From-Service(Group) ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104

#### The virtual server setting

**Step5.** In **Policy → Incoming**, add the new policy included Step4. ( The virtual server setting )

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(211.22.22.23)	Main_Service			<button>Modify</button> <button>Remove</button> <button>Pause</button>	To 1

[New Entry](#)

Complete the incoming setting in policy

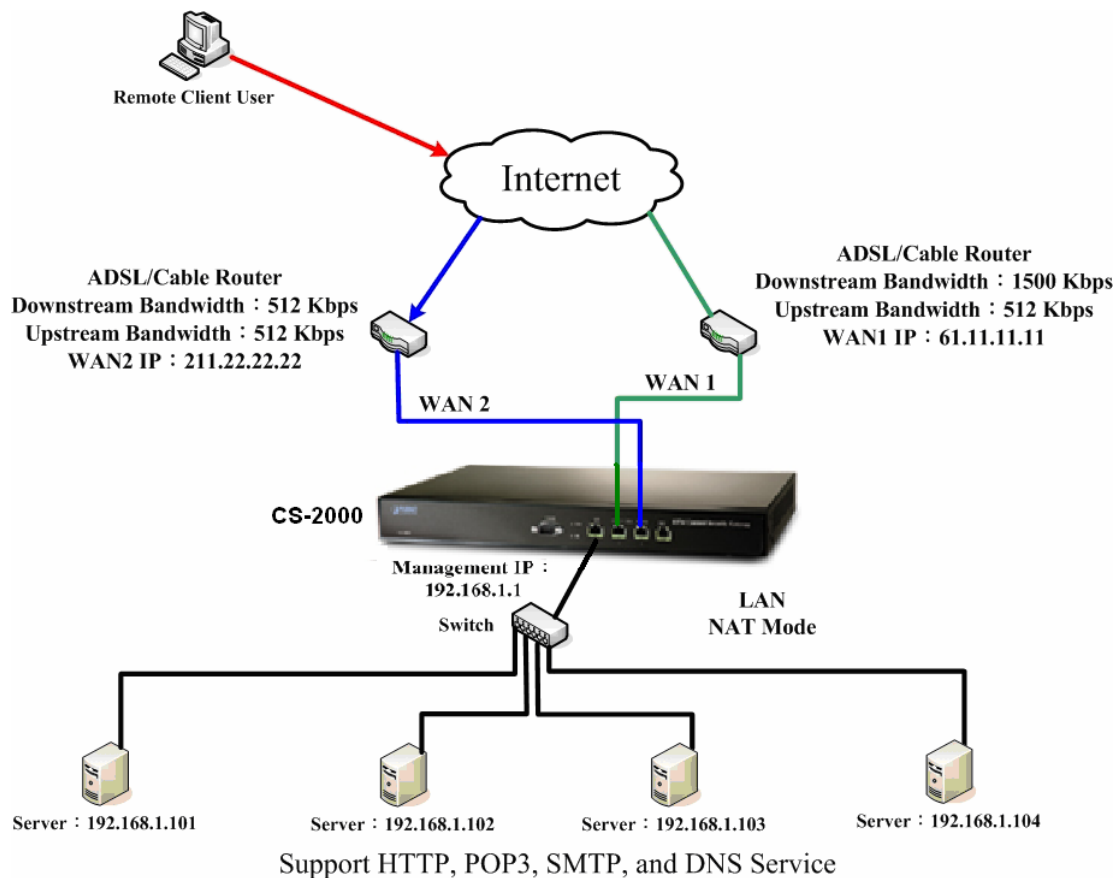
**Step6.** In **Policy → Outgoing**, add the new policy included Step2, Step3, to make the server can send the e-mail to external mail server via the mail service.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	Main_Service			<button>Modify</button> <button>Remove</button> <button>Pause</button>	To 1

[New Entry](#)

Complete the outgoing setting in policy

**Step7.** Make the virtual server provide multiple services to external.



**Deployment of using the virtual server instead of many internal servers which provide multiple services to external**

## 5.9 VPN

# VPN

The CS-2000 appliance provides the features of data encryption and authentication with the IKE (Internet Key Exchange) support. And its IPSec VPN module offers the secure network protection with the high performance data encryption. To create a virtual network between the branch offices to headquarter internal network via the internet instead of the high costs dial – up telecommunication, can reduce the company's telecommunication online costs. Provides the easiest way for the headquarter company to link its branch office, whatever the remote appliance are the CS-2000 appliance, smaller office gateway or any IPSec VPN compatible equipment.

**IPSec Autokey** : Create the data encryption of the connection by IPSec Autokey. Can randomly auto update the IPSec Autokey as the CS-2000 appliance start up, according to the IPSec Lifetime setting.

PPTP Server : The MIS engineer can set the VPN-PTP server setting.

PPTP Client : The MIS engineer can set the VPN-PTP client setting.

VPN Trunk : The MIS engineer can set the load balance and VPN trunk settings. ( With the GRE /IPSec function . )



### How to use the VPN ?

Create the Virtual Private Network (VPN) by applying the IPSec Autokey, PPTP Server or PPTP Client settings into the VPN trunk function. Then apply the VPN trunk settings in **Policy**, can offering the most secure and stable VPN environment.

## VPN

### RSA

- The RSA is a kind of asymmetric cryptography. User has two keys, one is the secret key can use it to encrypt as connected. The other one is the opened key, which the sender can get it if authenticated, and use it to encrypt the data to recipient.

### Preshared Key

- Use the Preshared Key to process the IPSec authentication in VPN.

### ISAKMP

- The IP Security Association Key Management Protocol (ISAKMP), provides the way to create the Security Association (SA) between two PCs. The SA can access the encoding between two PCs, and the MIS engineer can assign which key size or Preshared Key and algorithm to use. The SA also includes many connection ways, for instance, use the ISAKMP SA between two PCs, and assign which ENC algorithm (DES, triple DES, 40 bytes DES or not to use) and authentication to use.

### Main mode

- When starting the IKE process in VPN, will provides main mode and aggressive mode to select. The main mode request the user authentication with 6 messages as starting the data exchange, can enhance the data transferring security.

### Aggressive mode

- The aggressive mode still request the user authentication with only provides 3 messages as starting the data exchange.

### AH (Authentication Header)

- The Authentication Header is a mechanism for providing strong integrity and authentication for IP datagram.

### ESP

- The Encapsulated Security Payload provides the authentication and authentication test. Also provides the secure and protective data exchange.

### DES

- The data encryption standard for encrypting data and using a 56-byte key.

### 3DES

- The triple strength version of the DES cryptographic standard, usually using a 168-byte key.

### AES

- The advanced encryption standard (AES) is a symmetric key encryption technique, usually using a 128-byte, 192-byte and 256-byte key which will replace the commonly used DES standard.

### NULL Algorithm

- The NULL Algorithm provides the convenient connection mode. Can ensure the identity authentication and privacy without the encryption, and is usually instead of using the ESP (Encapsulating Security Payload) Protocol.

### SHA1 (Secure Hash Algorithm, SHA)

- The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions and can calculate the 160-bytes algorithm.

### MD5 Algorithm

- The MD5 (Message Digest algorithm 5) is a widely-used cryptographic hash function with a 128-byte hash value.

### GRE

- The GRE only provide the data packets without monitoring and encryption. Normally, the GRE can combine the IPsec encryption and provides more secure service to users.



## 5.9.1 VPN Wizard

### VPN Wizard

- VPN Wizard will guide user to finish the VPN settings.
  - ◆ In **VPN → VPN Wizard**, add the following settings :
    - ◆ Select the VPN connection method, and click **Next**.
    - ◆ Build up the VPN Policy setting, and click **Next**.
    - ◆ Set the VPN Trunk and click **Next**.
    - ◆ Select all VPN Trunk in **Policy setting**.
    - ◆ Click **Finish**.
    - ◆ Then system will build up VPN connection according to the applied VPN Trunk policy settings.

VPN Wizard

☒ IPsec Autokey  
☐ PPTP Server  
☐ PPTP Client

Select the method to build up VPN

i	Name ▾	WAN	Gateway IP	IPsec Algorithm	Configure
--	VPN_A	WAN1	210.66.155.76	DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Create VPN policy

i	Name ▾	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.1.0	10.10.10.0	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Set VPN Trunk

**Policy Setting**

☒ Select all Trunk

< --- Available Trunk --->  
 IPsec\_VPN\_Tunnel

Remove

Add

< --- Selected Trunk --->

< Back

Finish

Select the VPN Trunk setting to apply to VPN policy

Policy Object > VPN > VPN Wizard

- System
- Interface
- Policy Object
  - Address
  - Service
  - Schedule
  - QoS
  - Authentication
  - Content Blocking
  - IM / P2P Blocking
  - Virtual Server
  - VPN
    - VPN Wizard
    - IPSec Autokey
    - PPTP Server
    - PPTP Client
    - Trunk
- Policy
- Mail Security
- IDP
- Anomaly Flow IP
- Web VPN / SSL VPN
- Advance

VPN settings completed.

VPN setup finished

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

New Entry

Complete the outgoing policy setting of VPN Trunk

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



New Entry

Complete the incoming policy setting of VPN Trunk

## The icons and terms in IPSec Autokey option

### i

- Use the icon to display the VPN connection status.

Icon	--		
Connotation	The Policy is not used	Disconnected	Connected

### Name

- To define the name of IPSec AutoKey without repeating.

### WAN

- The local interface IP address.

### Gateway IP



- The destination interface IP address.

### IPSec Algorithm

- Display the data encryption mode in VPN connection.

### Configure

- To change the IPSec VPN Setting. Click **Configure**, or click **Remove** to delete the setting.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
	vpn	WAN1	210.66.155.76	DES / MD5	<a href="#">In Use</a>
	VPN_A	WAN1	210.66.155.76	DES / MD5	<a href="#">In Use</a>

[New Entry](#)

## The IPSec Autokey setting



In the default setting, the CS-2000 use the **Dead Peer Detection** mechanism to auto create the VPN Connection. In **To Destination → Remote Gateway → Fixed IP or Domain Name**, the MIS engineer can use **Manual Connect**, to create the IPSec VPN connection.

## The icons and terms in PPTP server option

### PPTP Server



- Can enable or disable the function.

### Client IP Range

- Can set the PPTP Client IP range.

### i

- Use the icon to display the VPN connection status.

Icon	--		
Connotation	The Policy is not used	Disconnected	Connected

### User Name

- The user name which the PPTP client used to login.

### Client IP

- The client IP which the PPTP client used to link the PPTP server.

### Uptime

- Display the PPTP client and PPTP server connection duration.

### Configure

- To change the PPTP VPN server setting, Click **Modify** , to modify the PPTP server parameter ; Or click **Remove** to delete the setting.

PPTP Server (Disable) :

Client IP Range : 192.158.244.1-254

**Modify**

Total entry : 0

i	User Name ▼	Client IP	Uptime	Configure
---	-------------	-----------	--------	-----------

**New Entry**

### PPTP Server setting





In the default setting, the CS-2000 use the **Echo-Request** mechanism to auto create the PPTP VPN. On the other hand, enable the **Manual Disconnect**, the MIS engineer can disconnect the VPN link to PPTP server.

## The icons and terms in PPTP Client option

### i

- Use the Icon to display the VPN connection status.

Icon	--		
Connotation	The Policy is not used	Disconnected	Connected

### User Name

- The user name used by the PPTP client to link the PPTP server.

### Server IP or Domain Name

- The server IP used by the PPTP client to link the PPTP server.

### Encryption

- Display if enabled the encryption of the PPTP client to PPTP server connection.

### Uptime

- Shows the PPTP client to PPTP server connection duration.

### Configure

- To change the PPTP VPN client settings. Click **Modify**, to change the PPTP client parameter, click **Remove**.

PPTP Client :

Total entry : 0

i	User Name ▼	Server IP or Domain Name	Encryption	Uptime	Configure
---	-------------	--------------------------	------------	--------	-----------

[New Entry](#)

### PPTP client





There are two ways to create the VPN connection: To let the CS-2000 auto build up the VPN connection by **Echo-Request** mechanism, or the MIS engineer can manually create the VPN connection.

## The icons and terms in VPN Trunk option

### i

- Use the icon to display the VPN trunk connection status.

Icon	--		
Connotation	The Policy is not used	Disconnected	Connected

### Name

- To define the VPN trunk name without repeating.

### Source Subnet

- Represents the source subnet IP address.

### Destination Subnet


- Represents the destination subnet IP address.

### Tunnel

- Shows all the VPN tunnels (IPSec , PPTP Server , PPTP Client) in the VPN trunk .

### Configure

- To modify the VPN trunk setting, click **Modify** to change the encryption parameter or click **Remove** to delete the setting. Click **Pause**, can stop the setting to effect or click **In Use**, to enable setting.

i	Name▼	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.1.0	10.10.10.0	VPN_A	<b>In Use</b>

[New Entry](#)

### VPN Trunk

**We set 6 VPN application environments.**

<b>No.</b>	<b>Range</b>	<b>The Application Environments</b>	<b>Pages</b>
<b>Example 1</b>	<b>IPSec Autokey</b>	To access the static subnet resources via the IPSec VPN connection between two CS-2000 appliances.	<b>158</b>
<b>Example 2</b>	<b>IPSec Autokey</b>	The way to set the CS-2000 appliance IPSec VPN connection in Windows 2000.	<b>173</b>
<b>Example 3</b>	<b>IPSec Autokey</b>	The way to set the IPSec VPN connection between two CS-2000 appliances. ( aggressive mode) (The IPSec algorithm, 3DES encryption.MD5 authentication.)	<b>219</b>
<b>Example 4</b>	<b>IPSec Autokey</b>	The way to set the outbound load balance connection in IPSec VPN between two CS-2000 appliances. ( RSA-SIG authentication ) (The ISAKMP algorithm, 3DES encryption.MD5 authentication.) (The IPSec algorithm, 3DES encryption .MD5 authentication.) (The GRE packets.)	<b>233</b>
<b>Example 5</b>	<b>PPTP</b>	The way to set the CS-2000 appliance PPTP VPN connection in Windows 2000.	<b>253</b>

### 5.9.2 Example 1

To access the static subnet resources via the IPSec VPN connection between two CS-2000 appliances.

#### The Deployment

A Company      **WAN IP is 61.11.11.11**  
                    **LAN IP is 192.168.10.X**

B Company      **WAN IP is 211.22.22.22**  
                    **LAN IP is 192.168.20.X**  
                    **Multiple Subnet is 192.168.85.X**

We use two CS-2000 devices to be the platform. We assume the A Company IP **192.168.10.100** connects to B Company IP **192.168.85.100** by using the **VPN**, to access the files download.

The A Company default gateway is CS-2000's LAN IP 192.168.10.1. Add the following settings :

**Step1.**      Enter A Company's CS-2000 default IP address 192.168.10.1. In **VPN → IPSec Autokey → New Entry**

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

[New Entry](#)

#### The IPSec Autokey setting



**Step2.** In **IPSec Autokey** → **Name**, enter VPN\_A. In **WAN Interface**, select **WAN 1**, to build up the VPN connection. ( A Company )

Necessary Item	
Name	<input type="text" value="VPN_A"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

**The name and WAN interface settings in IPSec VPN**

**Step3.** In **To Destination**, **Remote Gateway --Fixed IP or Domain Name**, enter the remote IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="211.22.22.22"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

**The destination setting**

**Step4.** In **Authentication Method**, select **Preshare**, and enter the **Preshared Key**. (The maximum Preshared Key is 100 byte)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

**The authentication method setting**

- Step5.** In **Encapsulation**, select **ISAKMP Algorithm**, as both sides start to build the connection, and select the algorithm to use. In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 1, the both sides need to select the same group.

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


#### The IPSec encapsulation setting

- Step6.** In **IPSec Algorithm**, select **Data Encryption + Authentication**, or select **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the Data Encryption + Authentication Method.

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

#### The IPSec algorithm

**Step7.** In **Perfect Forward Secrecy** ( NO-PFS/ GROUP 1,2,5 ), select GROUP 1. In **ISAKMP Lifetime**, enter 3600. In **IPSec Lifetime**, enter 28800. In **Mode**, select Main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1 
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step8.** Complete the IPSec Autokey setting.

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



### Complete the IPSec Autokey setting

**Step9.** In **VPN → VPN Trunk** , add the following settings :

- In **Name**, enter the Trunk Name.
- In **From Source**, select LAN.
- In **From Source Subnet /Mask**, enter A Company LAN address 192.168.10.0 and **Mask** 255.255.255.0.
- In **To Destination**, select To Destination Subnet / Mask.
- Enter B Company LAN Address 192.168.85.0 and Mask 255.255.255.0.
- In **Tunnel**, select **Add**, the add the VPN\_A's IPSec VPN connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0
To Destination		
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.85.0	/ 255.255.255.0
<input type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 30%;"> &lt;--- Available Tunnel ---&gt;  VPN_A </div> <div style="text-align: center; width: 30%;"> Remove  Add </div> <div style="border: 1px solid gray; padding: 5px; width: 30%;"> &lt;--- Selected Tunnel ---&gt;  VPN_A </div> </div>		
Keep alive IP :		
<input checked="" type="checkbox"/> Show remote Network Neighborhood		

OK Cancel

Add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.10.0	192.168.85.0	VPN_A	Modify Remove Pause

New Entry

Complete to add the VPN trunk setting

**Step10.** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )

### Set the outgoing policy included VPN trunk

Source	Destination	Service	Action	Option							Configure			Move																																																																																																																																																																																																																																																																																																																																																
Inside_Any	Outside_Any	ANY																																																																																																																																																																																																																																																																																																																																																												

[New Entry](#)

### Complete the outgoing policy setting included VPN trunk

**Step11. In Policy → Incoming :**

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy setting included VPN trunk**

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

[New Entry](#)

**Complete the incoming policy setting included VPN trunk**

The B Company's default gateway is the LAN IP 192.168.20.1 of the CS-2000.

**Step1.** In **System → Multiple Subnet** , add the following setting :

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
WAN 1 : 211.22.22.22 / NAT WAN 2 : Disable WAN 3 : Disable	LAN	192.168.85.1 / 255.255.255.0	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Multiple Subnet

**Step2.** Enter the B Company's default IP 192.168.20.1 in the CS-2000. In **Policy Object → VPN → IPSec Autokey**, click **New Entry**.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

[New Entry](#)

### IPSec Autokey

**Step3.** In **IPSec Autokey**, enter VPN\_B in the **VPN Name**. In **WAN interface**, select WAN 1, to build the B Company's VPN connection.

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

#### The IPSec VPN connection name and WAN interface setting

**Step4.** In **To Destination**, select **Remote Gateway—Fixed IP or Domain Name**, enter the remote IP address to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### The IPSec To Destination setting

**Step5.** In **Authentication Method**, select **Preshare**, enter the **Preshared Key** (the maximum Preshared Key is 100 bytes).

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

#### The IPSec Authentication Method setting



**Step6.** In **Encapsulation**, select **ISAKMP Algorithm**, and choose the needed algorithm as build up the connection.

In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 1, both sides need to select the same group.

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

#### The IPSec Encapsulation setting

**Step7.** In **IPSec Algorithm** , select **Data Encryption + Authentication** or select **Authentication Only** :

In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the Data Encryption + Authentication Method.

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

#### The IPSec algorithm setting

**Step8.** In **Perfect Forward Secrecy** (NO-PFS/ GROUP 1, 2, 5) , select GROUP 1. In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step9.** Complete the IPSec Autokey setting.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPB_B	WAN1	61.11.11.11	3DES / MD5	

### Complete the IPSec Autokey setting

**Step10.** In **VPN → VPN Trunk** , add the following setting :

- **Name**, enter the Trunk name.
- **From Source**, select LAN.
- **From Source Subnet / Mask** , enter LAN IP address (B Company) 192.168.85.0 and mask 255.255.255.0
- **To Destination**, select To Destination Subnet / Mask.
- **To Destination Subnet / Mask**, enter LAN IP address (A Company) 192.168.10.0 and mask 255.255.255.0.
- **Tunnel**, Click **Add**, to add the VPN\_B's IPsec VPN connection setting.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.85.0	/ 255.255.255.0
To Destination		
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.10.0	/ 255.255.255.0
<input type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div> <p>&lt;--- Available Tunnel ---&gt;</p> <div style="border: 1px solid black; padding: 2px;">VPN_B</div> </div> <div style="text-align: center;"> <p>Remove</p> <p>Add</p> </div> <div> <p>&lt;--- Selected Tunnel ---&gt;</p> <div style="border: 1px solid black; padding: 2px;">VPN_B</div> </div> </div>		
Keep alive IP :		
<input type="checkbox"/> Show remote Network Neighborhood		

To add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.85.0	192.168.10.0	VPN_B	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete the VPN trunk setting

**Step11.** In **Policy → Outgoing**, add the following setting :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 kBytes ( Range: 0 - 999999 )

**Set the outgoing policy setting included VPN trunk**

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

[New Entry](#)

**Complete the outgoing policy setting included VPN trunk**

**Step12.** In **Policy → Incoming** , add the following settings :

- **Schedule**, select **Working\_Time**.
- **Qos**, select **QoS\_1**.
- **VPN Trunk**, select **IPSec\_VPN\_Tunnel**.
- Click **OK**.

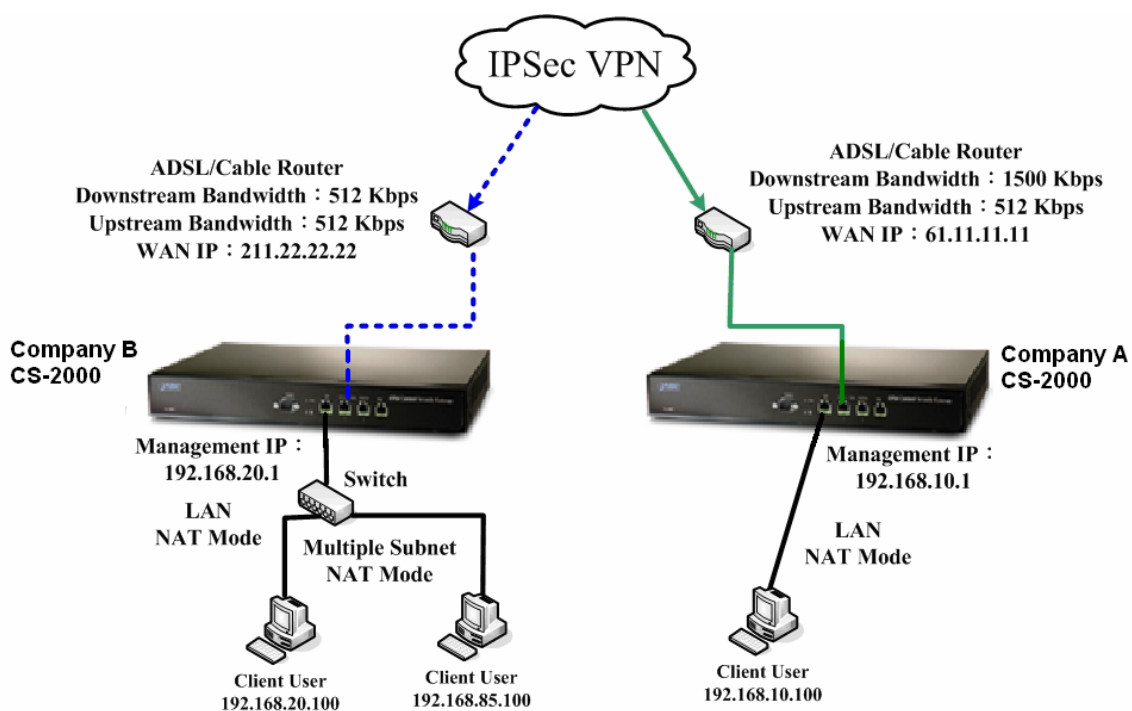
Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy setting included VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<div> <div>Modify</div> <div>Remove</div> <div>Pause</div> </div>

[New Entry](#)

**Complete the incoming policy setting included VPN trunk**

**Step13. Complete to set the IPSec VPN connection.**

**The IPSec VPN deployment**

### 5.9.3 Example 2

**The way to set the CS-2000 appliance IPSec VPN connection in Windows 2000.**

#### The Deployment

A Company    Use the CS-2000

**WAN IP is 61.11.11.11**

**LAN IP is 192.168.10.X**

B Company    The PC with Windows 2000 inside.

**WAN IP is 211.22.22.22**

We use the CS-2000 and Windows 2000 VPN-IPsec to be the platform. On the other hand, we assume that B Company **211.22.22.22** want to build the VPN to A Company **192.168.10.100**, in order to download the shared document.

The A Company's default gateway is the LAN IP 192.168.10.1 in the CS-2000. Add the following settings :

- Step1.** Enter the A Company's CS-2000 default IP 192.168.10.1. Click **VPN → IPSec Autokey → New Entry**.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

New Entry

### IPSec Autokey

- Step2.** In **IPSec Autokey**, enter VPN\_A in **Name**. In **WAN interface**, select WAN 1, in order to build up the A Company's VPN connection.

Necessary Item	
Name	VPN_A (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

### The IPSec VPN name and WAN interface setting

- Step3.** In **To Destination**, select **Remote Gateway or Client—Dynamic IP**.

To Destination	
<input type="radio"/> Remote Gateway -- Fixed IP or Domain Name	(Max. 99 characters)
<input checked="" type="radio"/> Remote Gateway or Client -- Dynamic IP	

### The IPSec To Destination setting

- Step4.** In **Authentication Method**, select **Preshare**, enter the **Preshared Key**. (The maximum Preshared Key is 100 bytes).

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

### The IPSec Authentication Method setting



**Step5.** In **Encapsulation** → select **ISAKMP Algorithm**. Select the needed algorithm as both sides start the connection.

In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 2. The both sides need to select the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
Group	GROUP 2 ▼

#### The IPSec Encapsulation setting

**Step6.** In **IPSec Algorithm** , select **Data Encryption + Authentication** or **Authentication Only** :  
**ENC Algorithm** (3DES/DES/AES/NULL), select **3DES**. **AUTH Algorithm** (MD5/SHA1), select **MD5**. To assure the Data Encryption + Authentication Method.

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

#### The IPSec algorithm setting

**Step7.** In **Perfect Forward Secrecy** ( NO-PFS/ GROUP 1,2,5 ), select GROUP 1. In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step8.** Complete the IPSec Autokey setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Complete the IPSec Autokey setting

**Step9.** In **VPN → VPN Trunk** , add the following settings :

- **Name**, enter the Trunk Name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter Source LAN IP 192.168.10.0 (A Company), and Mask 255.255.255.0.
- **To Destination**, select Remote Client.
- **Tunnel**, add the connection setting of VPN\_A's IPsec VPN.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.10.0	255.255.255.0
To Destination		
<input type="radio"/> To Destination Subnet / Mask		
<input checked="" type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 30%;"> &lt;--- Available Tunnel ---&gt;  VPN_A </div> <div style="text-align: center; width: 30%;"> Remove  Add </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> &lt;--- Selected Tunnel ---&gt;  VPN_A </div> </div>		
Keep alive IP :		
<input type="checkbox"/> Show remote Network Neighborhood		

Add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.10.0	Remote Client	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete to add the VPN trunk setting

**Step10.** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **QoS**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )

**Set the outgoing policy setting included the VPN trunk**

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

[New Entry](#)

**Complete the outgoing policy setting included the VPN trunk**

**Step11.** In **Policy → Incoming** , add the following settings :

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy setting included the VPN trunk**

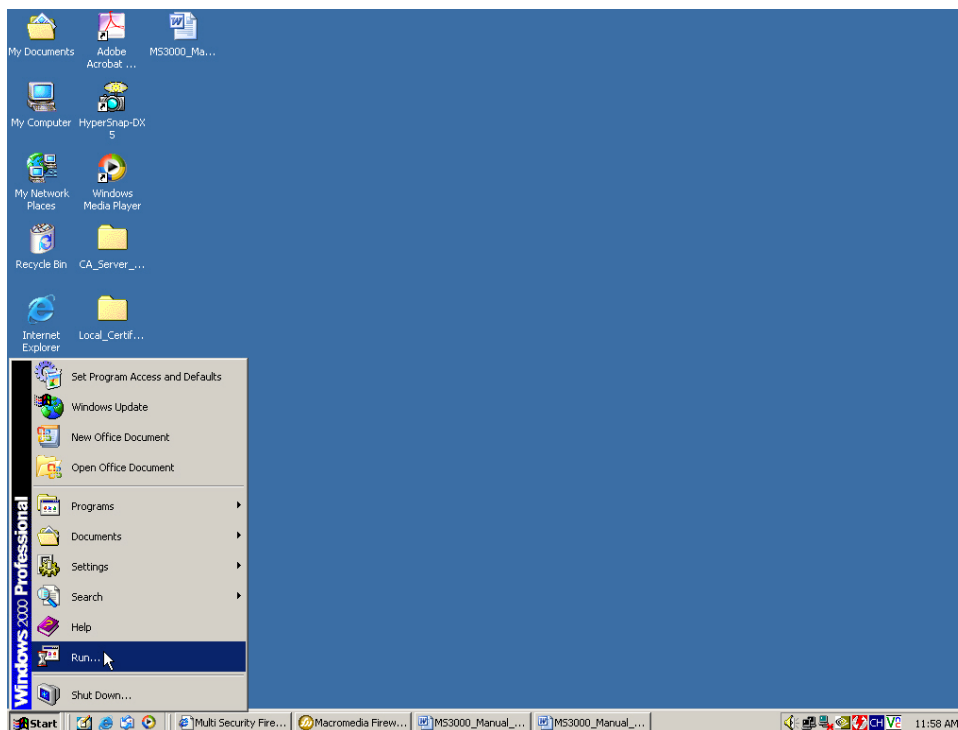
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				
						
						

[New Entry](#)

**Complete the incoming policy setting included the VPN trunk**

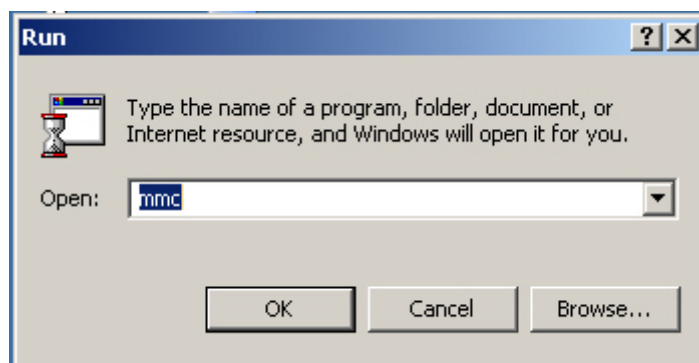
**The B Company's PC Real IP is 211.22.22.22, add the following settings:**

**Step1.** Click **Start** → **Run** in Windows 2000.



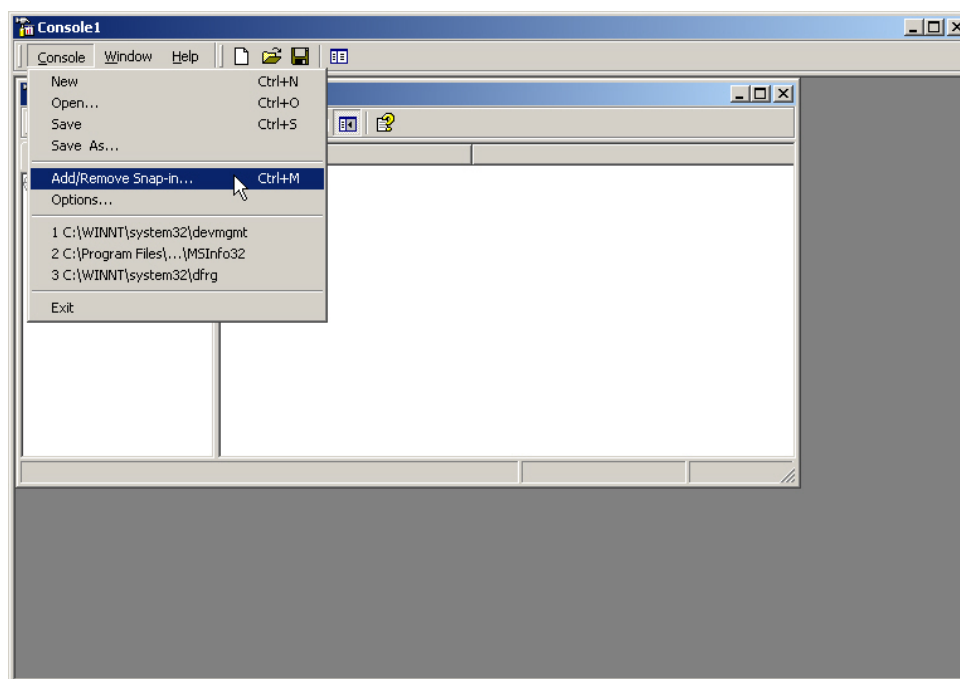
**Start the IPSec VPN setting in Windows 2000**

**Step2.** In **Run** → **Open** column, enter **mmc**.



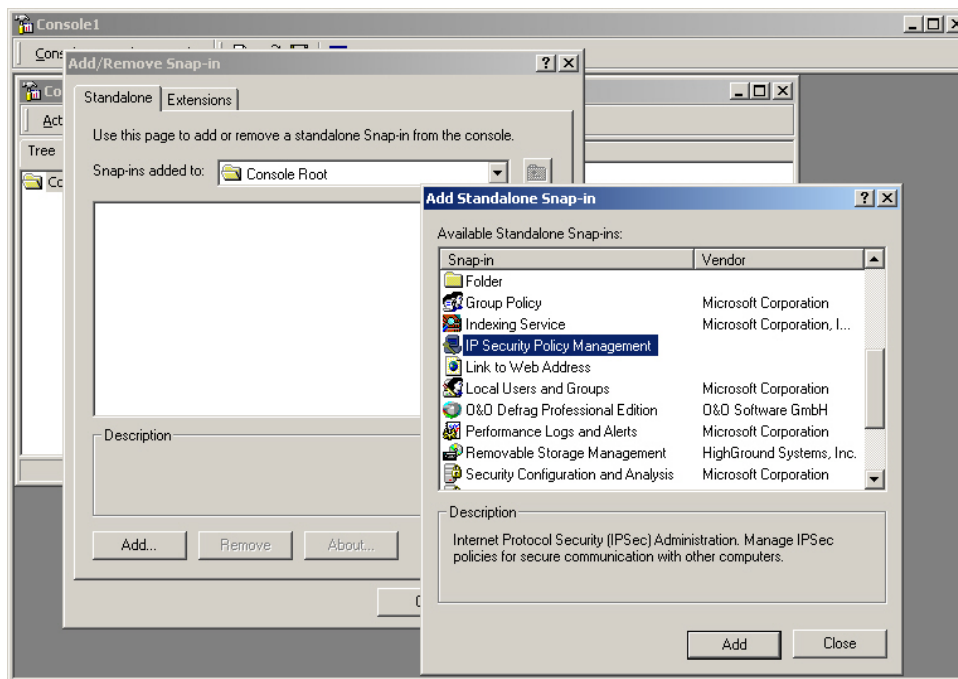
To startup the Windows 2000 IPsec VPN setting

**Step3.** In **Console 1** → **Console** → **Add/Remove Snap-in**.



Add / Remove Snap-in

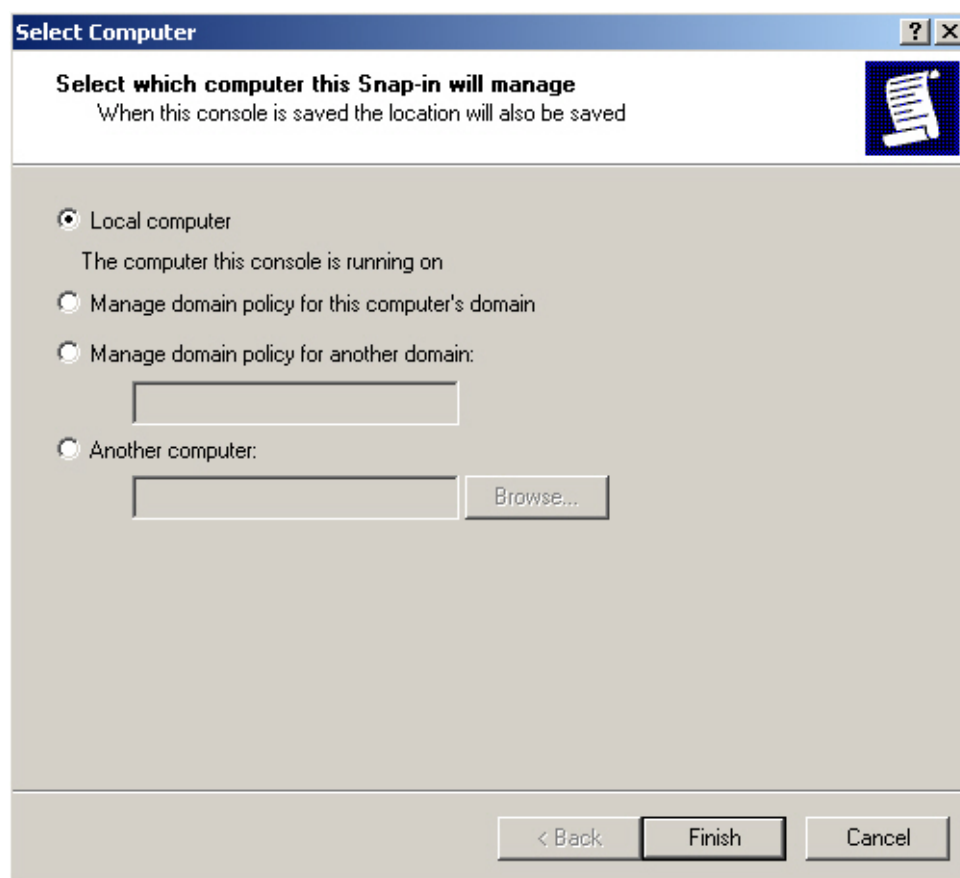
**Step4.** In **Add / Remove Snap-in**, click **Add**. In **Add Standalone Snap-ins**, add **IP Security Policy Management**.



**Add IP Security Policy Management**

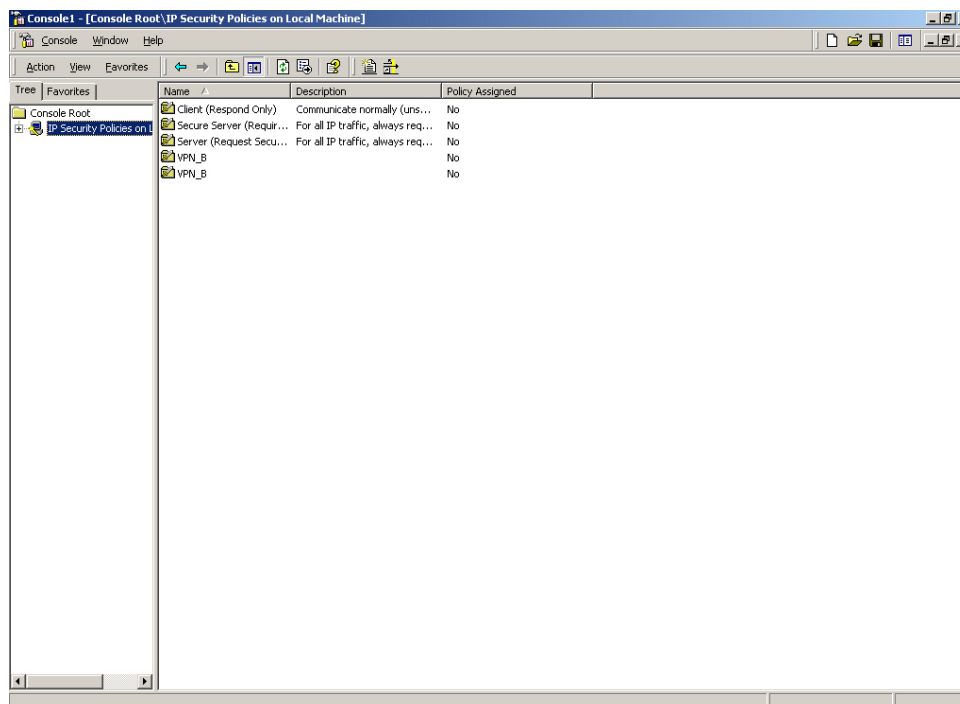


**Step5.** Select **Local Computer**, click **finish**.



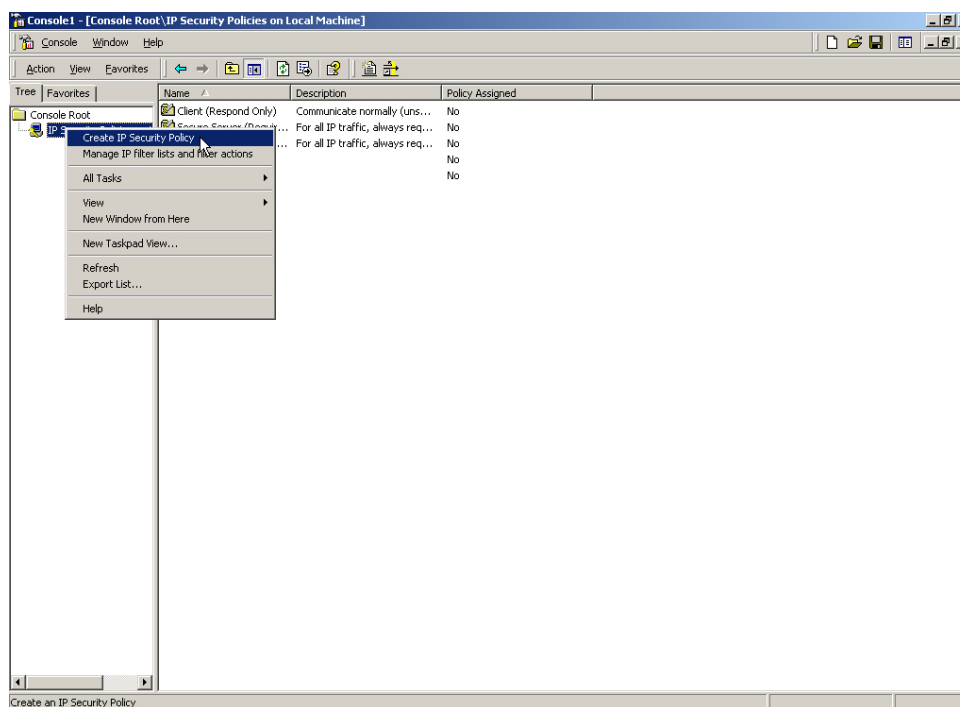
**Select the type of IP Security Policy Management**

**Step6.** Complete to set the IP Security Policy Management.



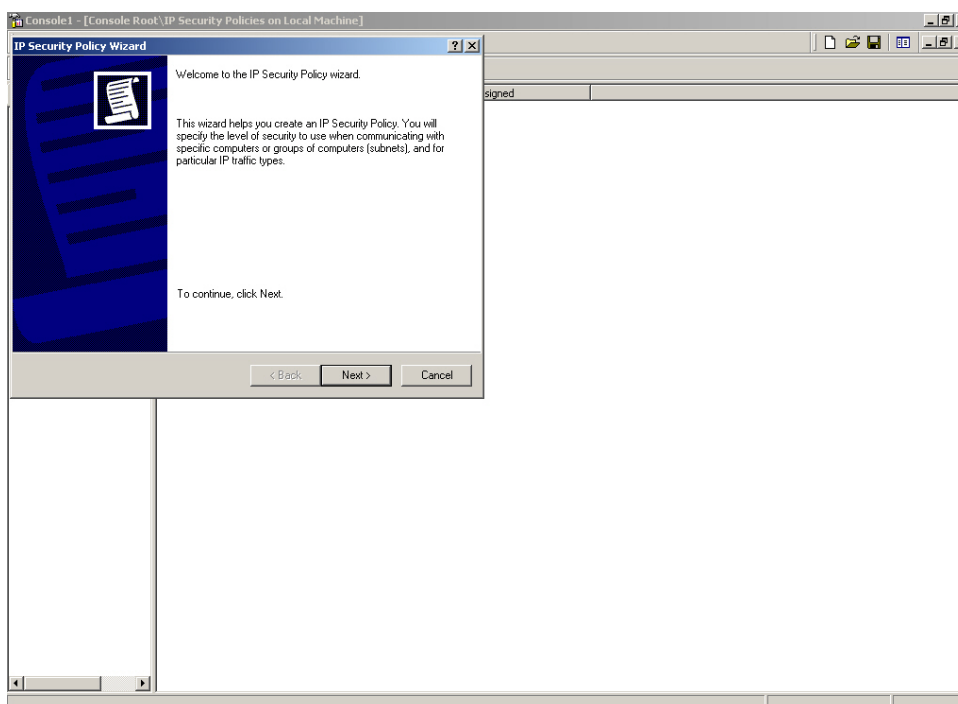
**Complete to set the IP Security Policy Management**

**Step7.** Right click on the **IP Security Policies on Local Machine**, and select **Create IP Security Policy**.



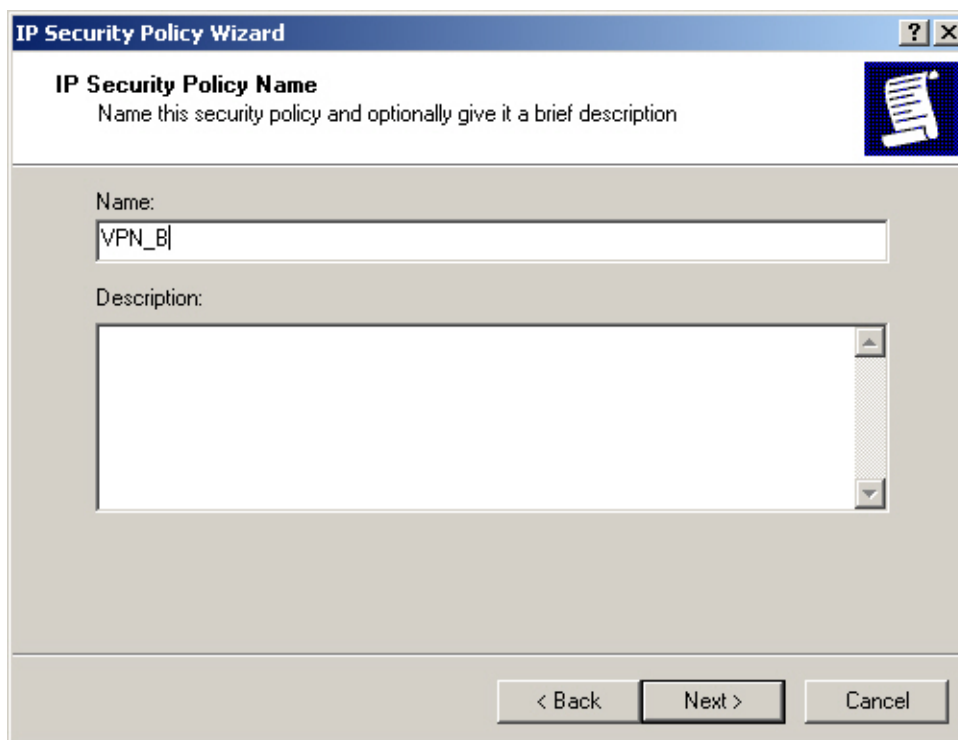
**Create IP Security Policy**

**Step8.** Click **Next**.



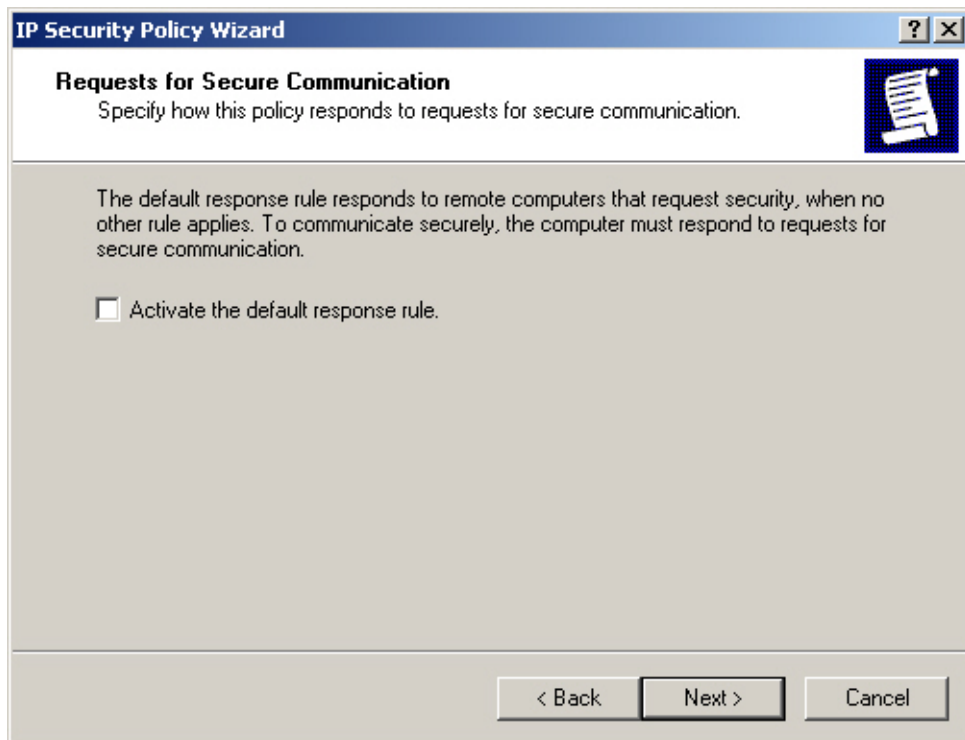
Open IP Security Policy Wizard

**Step9.** Enter the VPN **Name** and **Description**, and click **Next**.



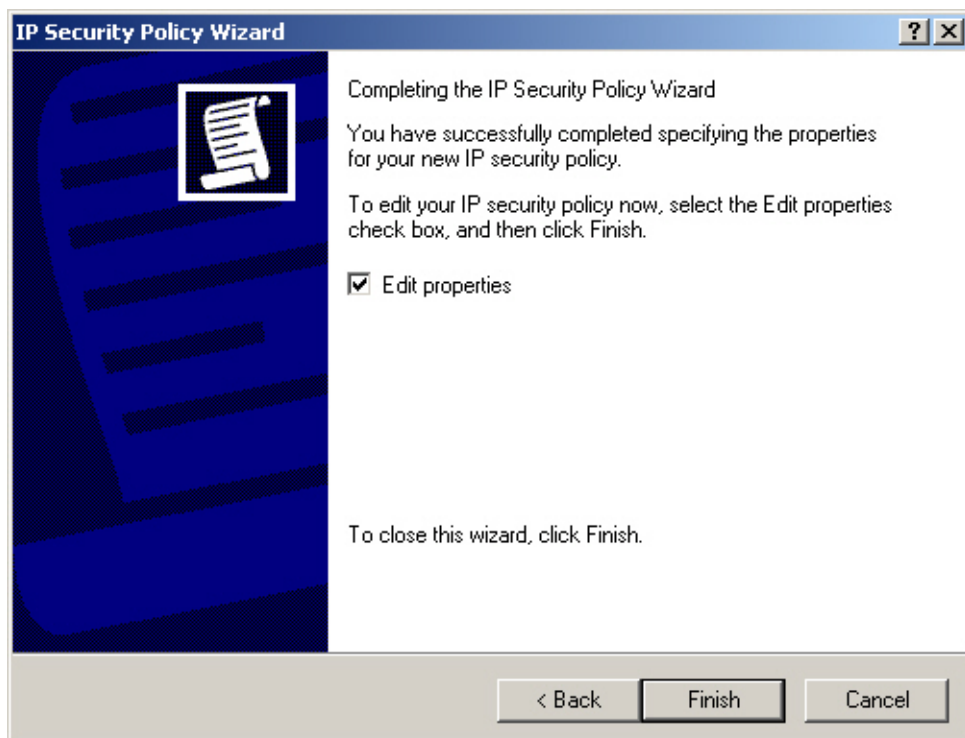
Set the VPN name and description

**Step10.** Disable to **Activate the default response rule**, and click **Next**.



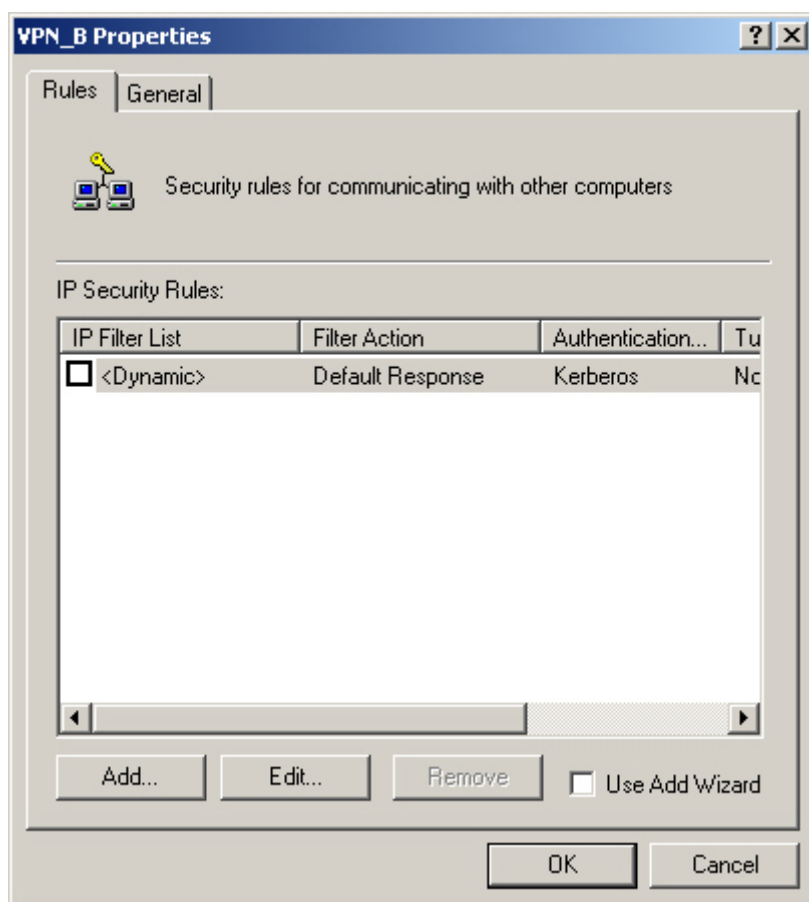
Disable to activate the default response rule

**Step11.** In **IP Security Policy Wizard**, select **Edit properties**, click **Finish**.



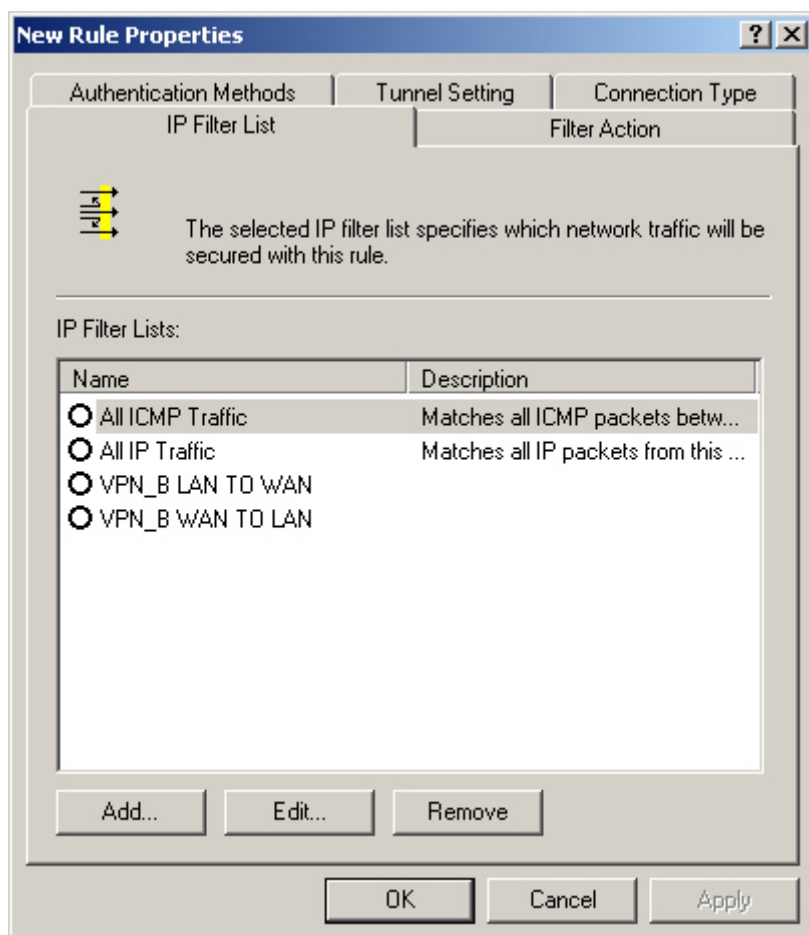
Complete the IP Security Policy Wizard settings

**Step12.** In **VPN\_B Properties**, do not select **Use Add Wizard**, and click **Add**.



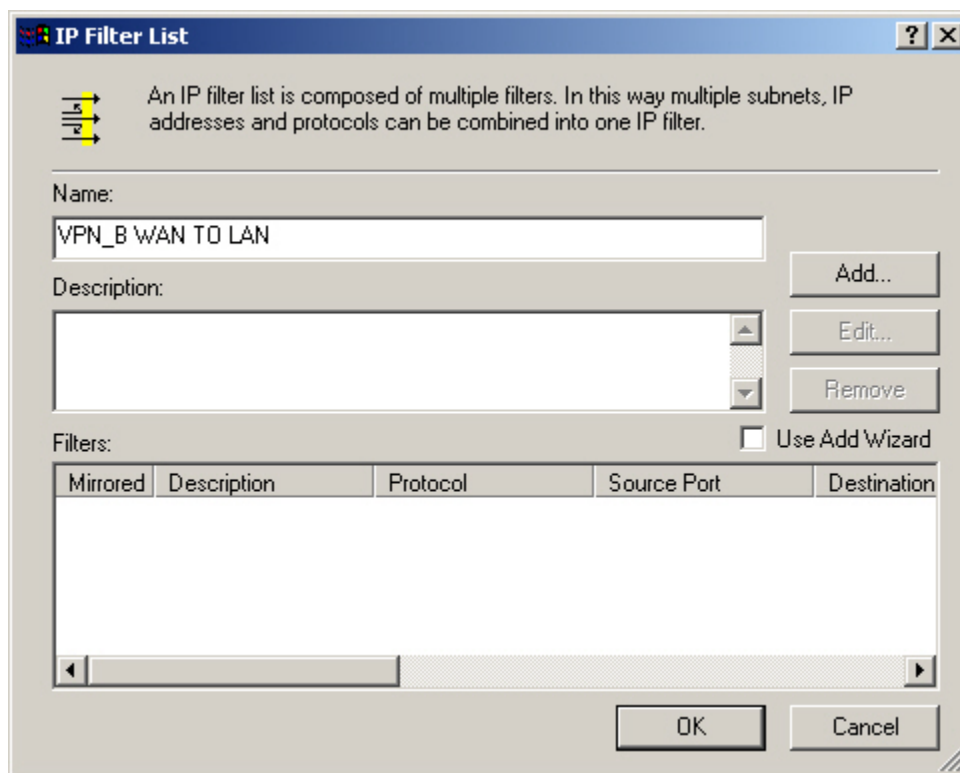
**VPN\_B Properties**

**Step13.** In **New Rule Properties**, Click **Add**.



**New Rule Properties**

**Step14.** In **IP Filter List**, do not select **Use Add Wizard**. Modify the **Name** into VPN\_B WAN TO LAN, click **Add**.



IP Filter List

- Step15.** In **Filter Properties** → **Source address** → **A specific IP Address**, enter B Company's WAN IP address 211.22.22.22 , Subnet mask 255.255.255.255 . In **Destination address** → **A specific IP Subnet**, enter A Company's LAN IP address 192.168.10.0, subnet mask 255.255.255.0. Do not select **Mirrored**. Also match packets with the exact opposite source and destination addresses.

**Filter Properties**

Addressing | Protocol | Description

Source address:

A specific IP Address

IP Address: 211 . 22 . 22 . 22

Subnet mask: 255 . 255 . 255 . 255

Destination address:

A specific IP Subnet

IP Address: 192 . 168 . 10 . 0

Subnet mask: 255 . 255 . 255 . 0

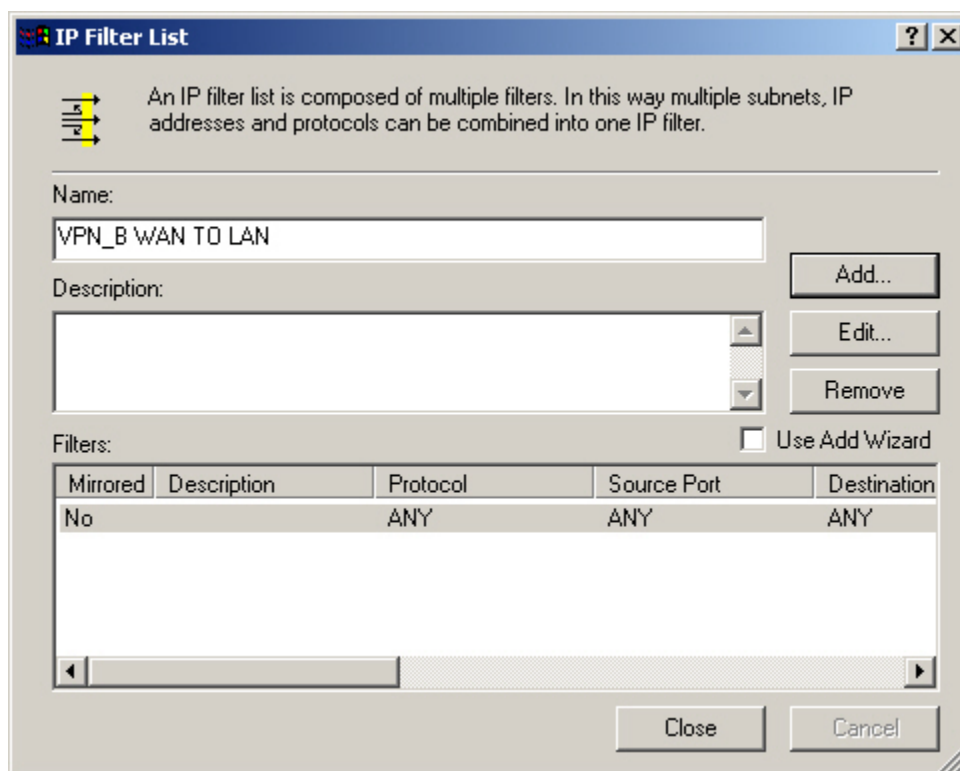
☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel Apply

**Filter Properties**



**Step16.** Complete the setting, and close the **IP Filter List**.

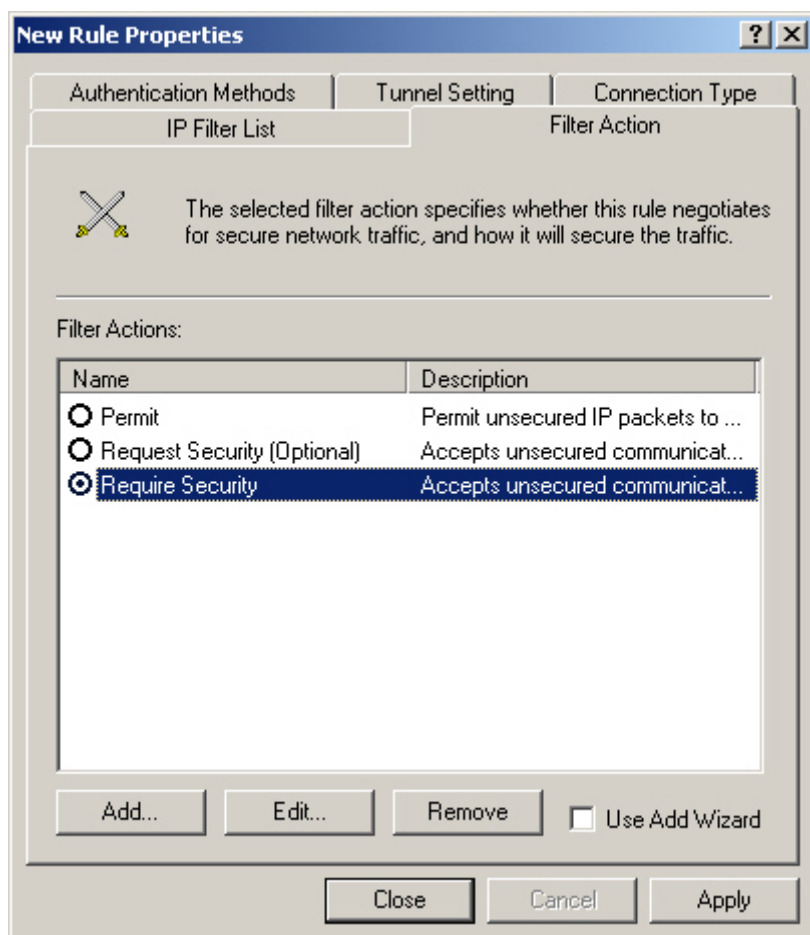


The **IP Filter List** window contains the following elements:

- Header:** A blue title bar with the text "IP Filter List" and standard window controls.
- Help/Intro:** A small icon of a list with arrows, followed by the text: "An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter."
- Name:** A text input field containing "VPN\_B WAN TO LAN".
- Description:** A large text area for additional details.
- Buttons:** "Add...", "Edit...", and "Remove" buttons are located to the right of the Name and Description fields.
- Filters:** A section with a checkbox labeled "Use Add Wizard" and a table below it.
- Table:** A table with 5 columns: "Mirrored", "Description", "Protocol", "Source Port", and "Destination". It contains one row with the values "No", "", "ANY", "ANY", and "ANY".
- Footer:** "Close" and "Cancel" buttons at the bottom right.

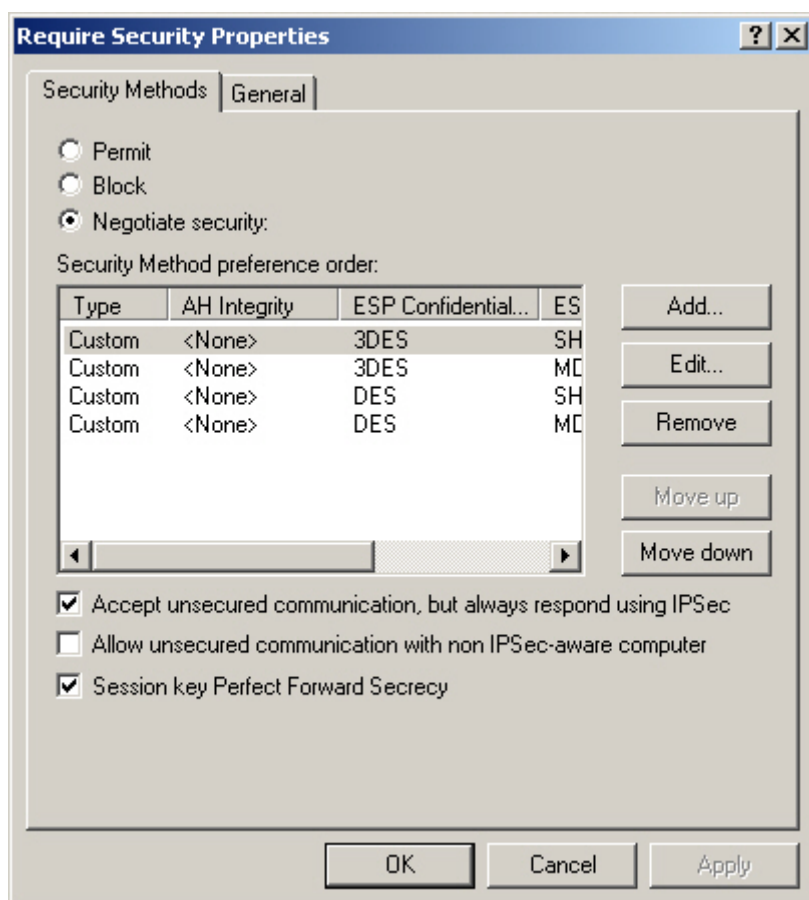
**Complete the IP Filter List setting**

**Step17.** In **New Rule Properties** → **Filter Action** → **Require Security**. Click **Edit**.



**Filter Action setting**

**Step18.** In **Require Security Properties**, select **Session Key Perfect Forward Secrecy**.



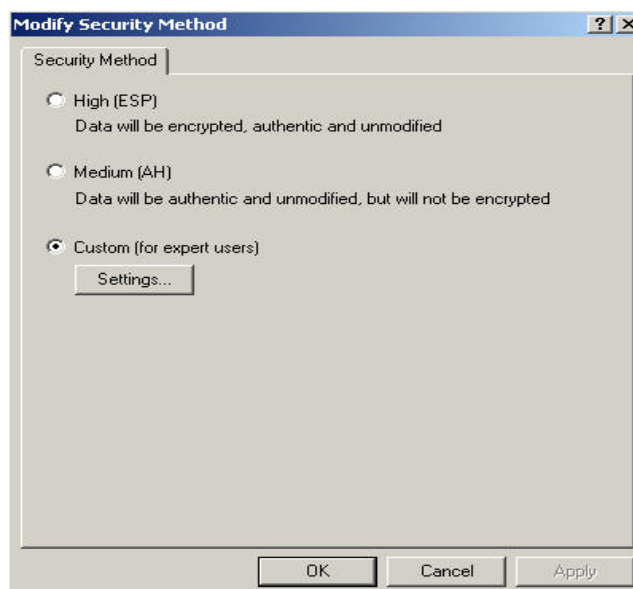
**Select Session Key Perfect Forward Secrecy**

**Step19.** Select **Custom / None / 3DES / MD5** Security Method, click **Edit**.



**Edit the Security Method**

**Step20.** Click **Custom (for expert users)**, and click **Settings**.



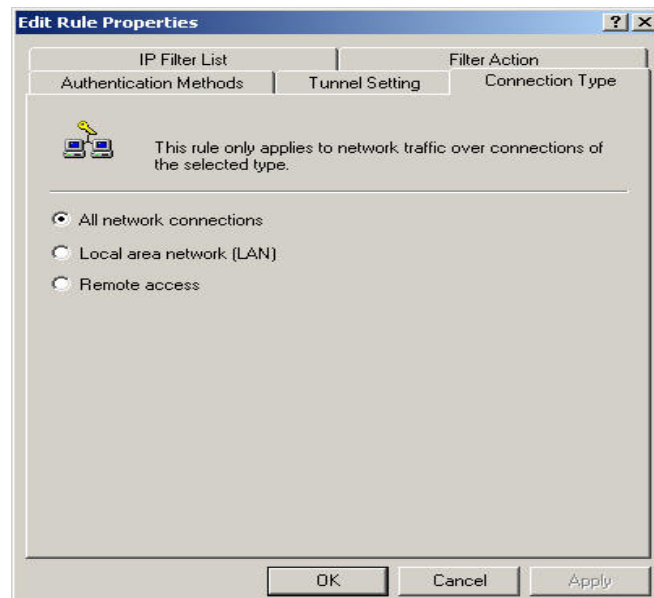
**Custom Security Method**

**Step21.** Select **Data integrity and encryption**, choose **Integrity algorithm** → **MD5**. **Encryption algorithm** → **3DES**. Select **Generate a new key every**, enter 28800 seconds, then click **OK** to back to **New Rule Properties**.



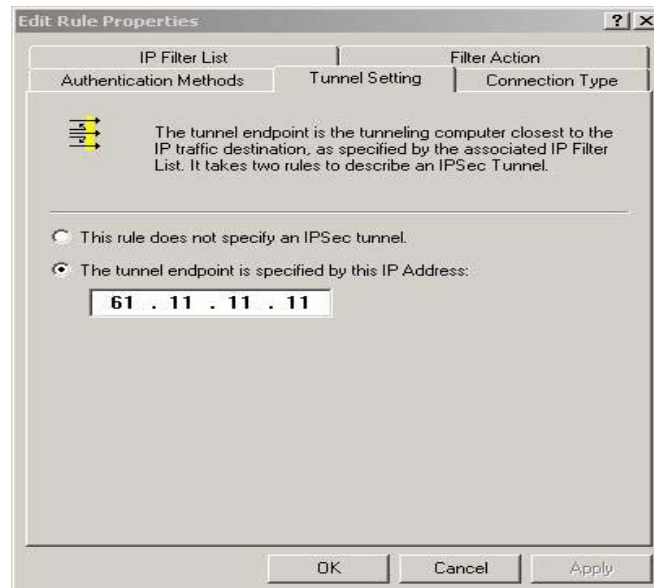
Custom Security Method settings

**Step22.** In **New Rule Properties** → **Connection Type**, select **All network connections**.



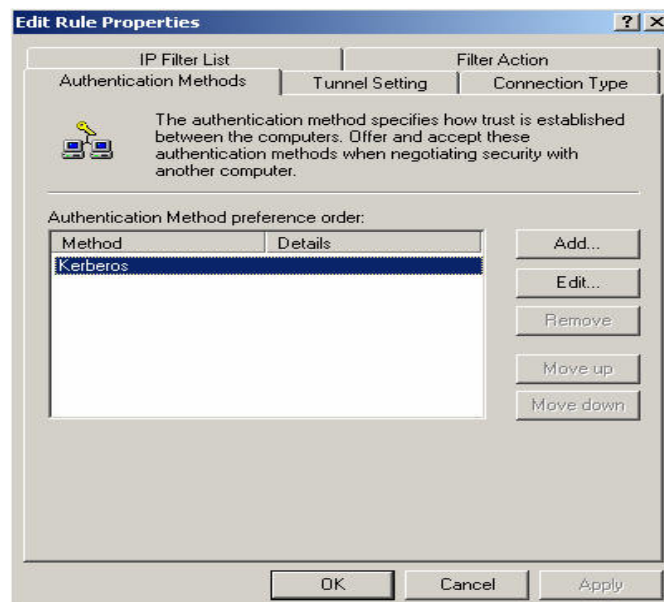
Connection Type setting

**Step23.** In **New Rule Properties → Tunnel Setting**, select **The tunnel endpoint is specified by this IP Address**. Enter A Company's WAN IP address - 61.11.11.11.



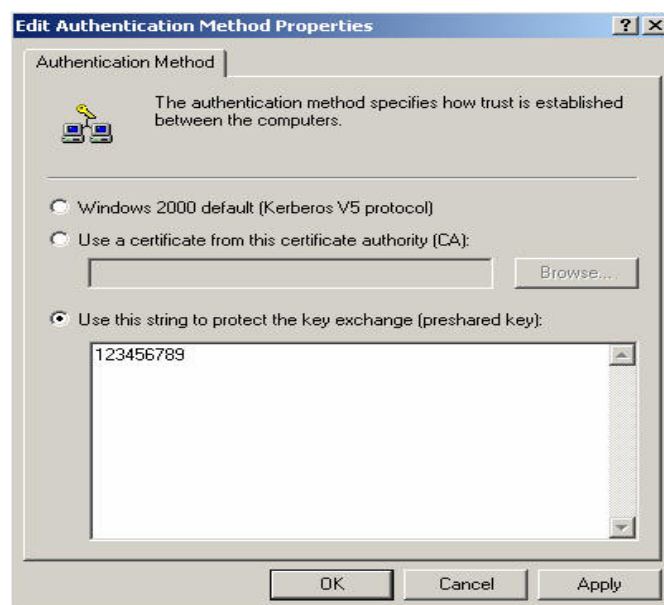
**Tunnel setting**

**Step24.** In **New Rule Properties → Authentication Methods**, click **Edit**.



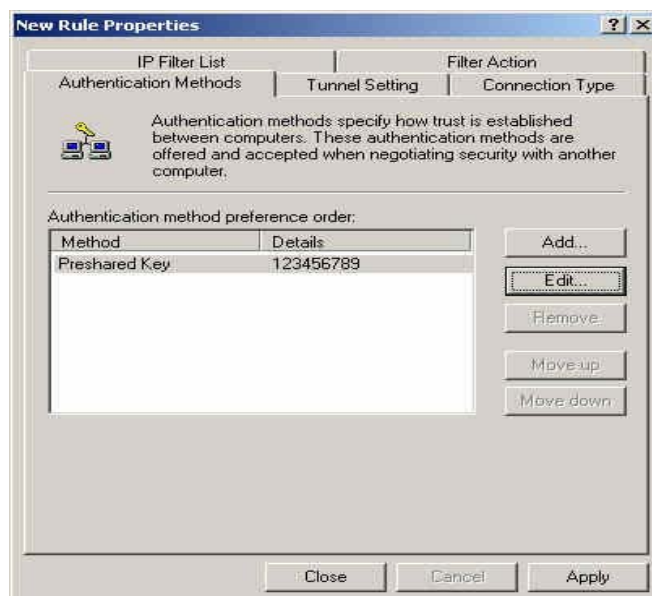
**Authentication Methods setting**

- Step25.** Select **Use this string to protect the key exchange (preshared key)**, enter the Preshared Key, 123456789.



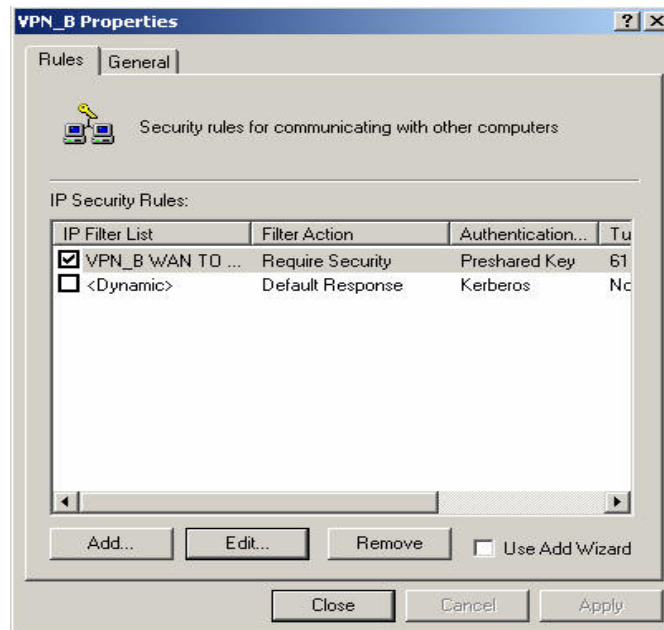
**Set the VPN Preshared Key**

- Step26.** Click **Apply** → **OK** → **Close**.



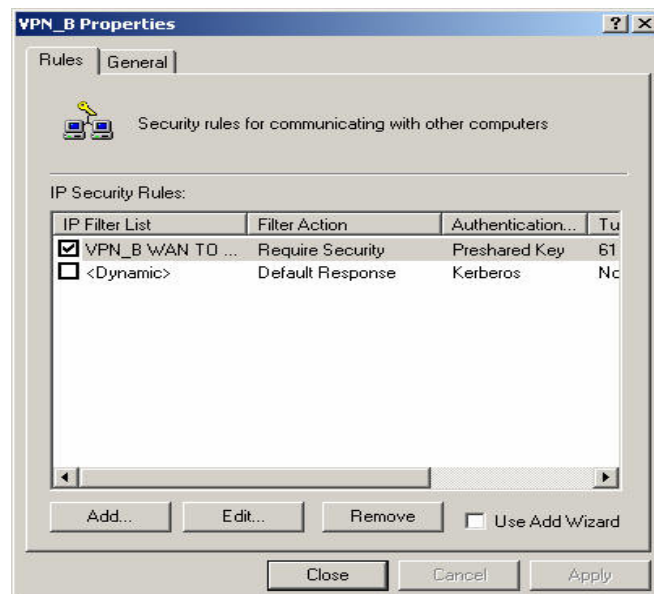
**Complete the Authentication Methods setting**

**Step27.** Complete the VPN\_B WAN TO LAN settings.



**Complete the VPN\_B WAN TO LAN policy setting**

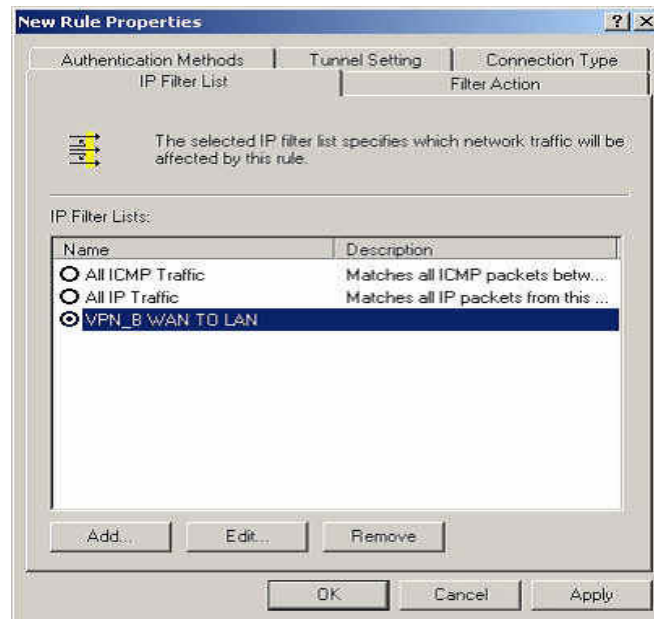
**Step28.** In **VPN \_B Properties**, do not select **Use Add Wizard**. Click **Add**, to add the second IP security policy.



**The VPN\_B Properties**

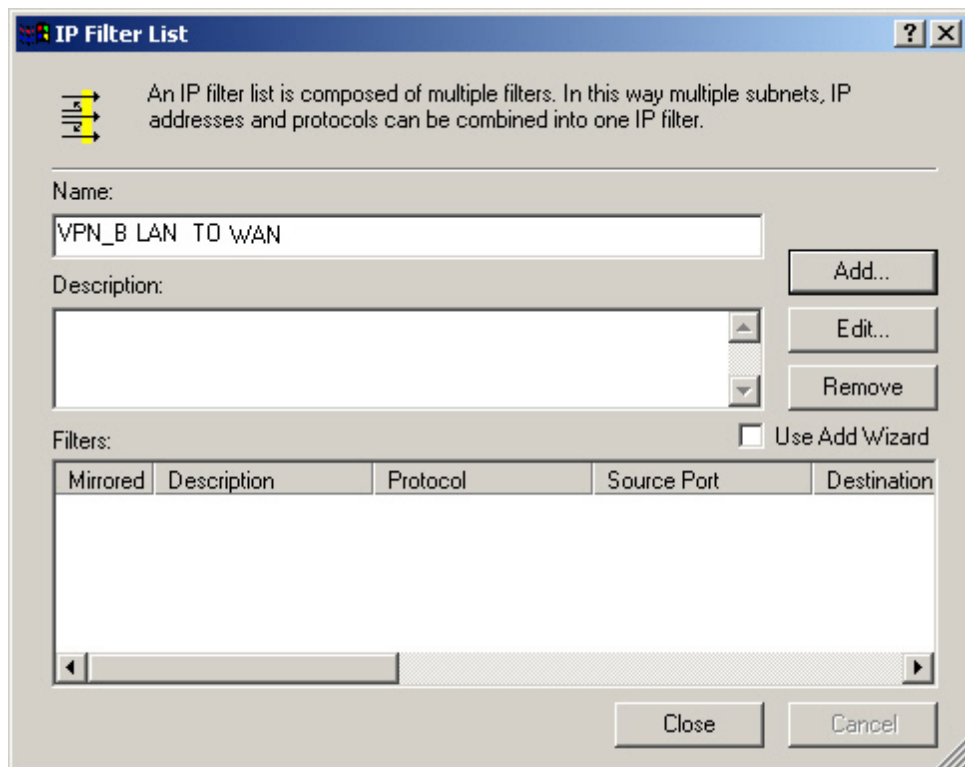


**Step29.** In **New Rule Properties**, click **Add**.



**New Rule Properties**

**Step30.** In **IP Filter List**, do not select **Use Add Wizard**. Modify the **Name** into VPN\_B LAN TO WAN, click **Add**.



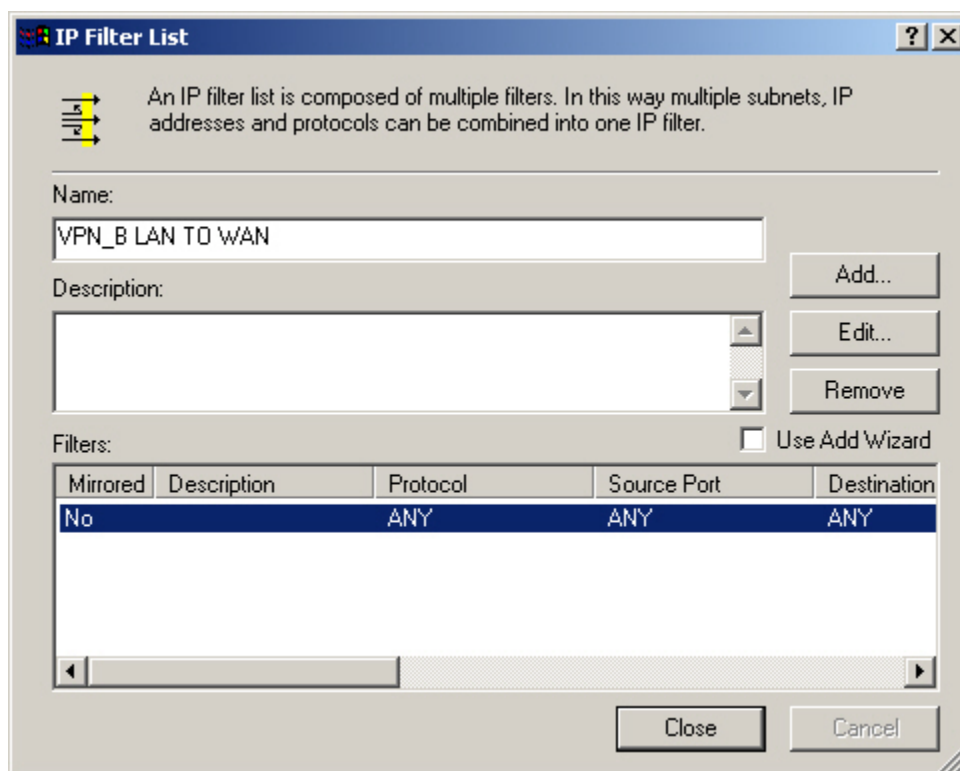
**IP Filter List**

**Step31.** In **Filter Properties**→ **Source address**, select **A specific IP Subnet**, enter A Company's LAN IP Address 192.168.10.0, subnet mask 255.255.255.0. In **Destination address**, select **A specific IP Address**, enter B Company's WAN IP Address 211.22.22.22, subnet mask 255.255.255.255. Do not select **Mirrored, Also match packets with the exact opposite source and destination addresses**.

The screenshot shows the 'Filter Properties' dialog box with the 'Addressing' tab active. It contains two main sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu shows 'A specific IP Subnet', and below it, the IP Address is '192 . 168 . 10 . 0' and the Subnet mask is '255 . 255 . 255 . 0'. In the 'Destination address' section, a dropdown menu shows 'A specific IP Address', and below it, the IP Address is '211 . 22 . 22 . 22' and the Subnet mask is '255 . 255 . 255 . 255'. At the bottom, there is an unchecked checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' and three buttons: 'OK', 'Cancel', and 'Apply'.

**Filter Properties**

**Step32.** Complete the settings, close the **IP Filter List**.



The IP Filter List dialog box contains a title bar with a help icon and a close button. Below the title bar is a help text area with a yellow arrow icon and the text: "An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter." Below this is a "Name:" label followed by a text box containing "VPN\_B LAN TO WAN". To the right of the text box are three buttons: "Add...", "Edit...", and "Remove". Below the name field is a "Description:" label followed by a large empty text box. Below the description field is a "Filters:" label and a checkbox labeled "Use Add Wizard". Below these is a table with five columns: "Mirrored", "Description", "Protocol", "Source Port", and "Destination". The table has one row with the values "No", "ANY", "ANY", and "ANY". Below the table is a horizontal scrollbar. At the bottom right of the dialog are "Close" and "Cancel" buttons.

Name: VPN\_B LAN TO WAN

Description:

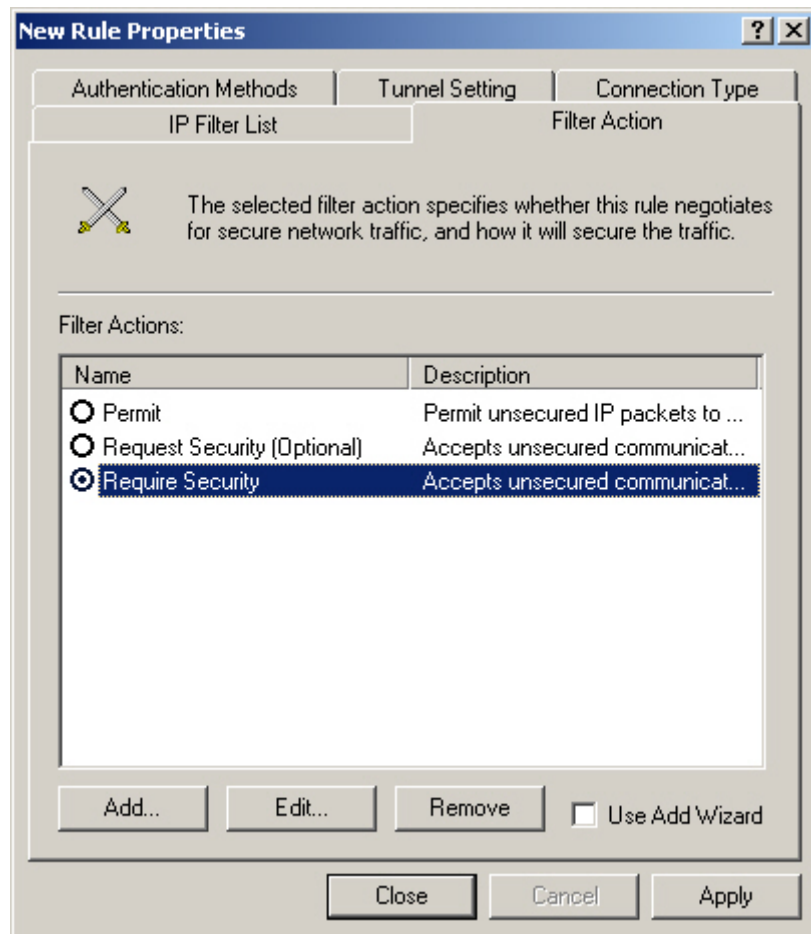
Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Close Cancel

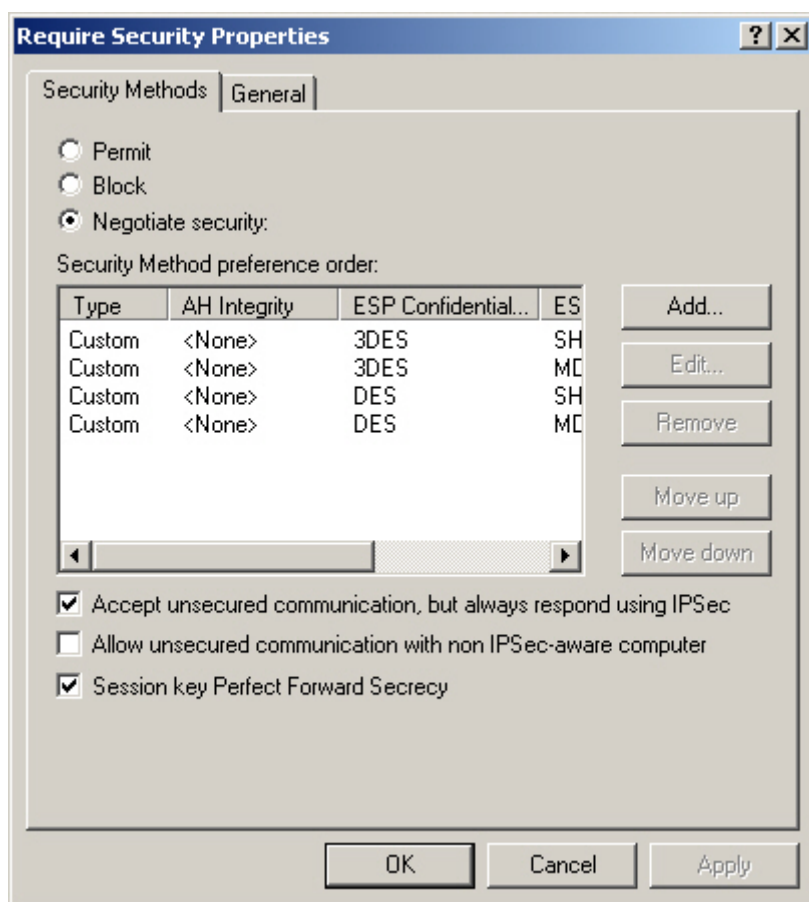
Complete the IP Filter List setting

**Step33.** In **New Rule Properties** → **Filter Action**, select **Required Security**, then click **Edit**.



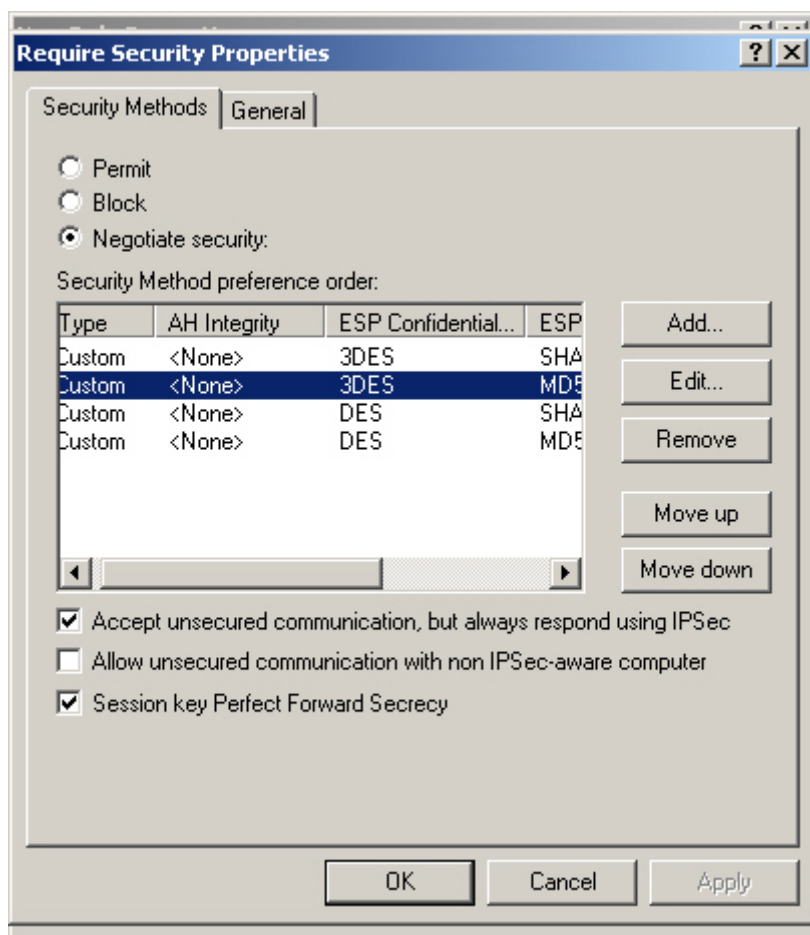
**Filter Action**

**Step34.** In **Require Security Properties**, select **Session key Perfect Froward Secrecy**.



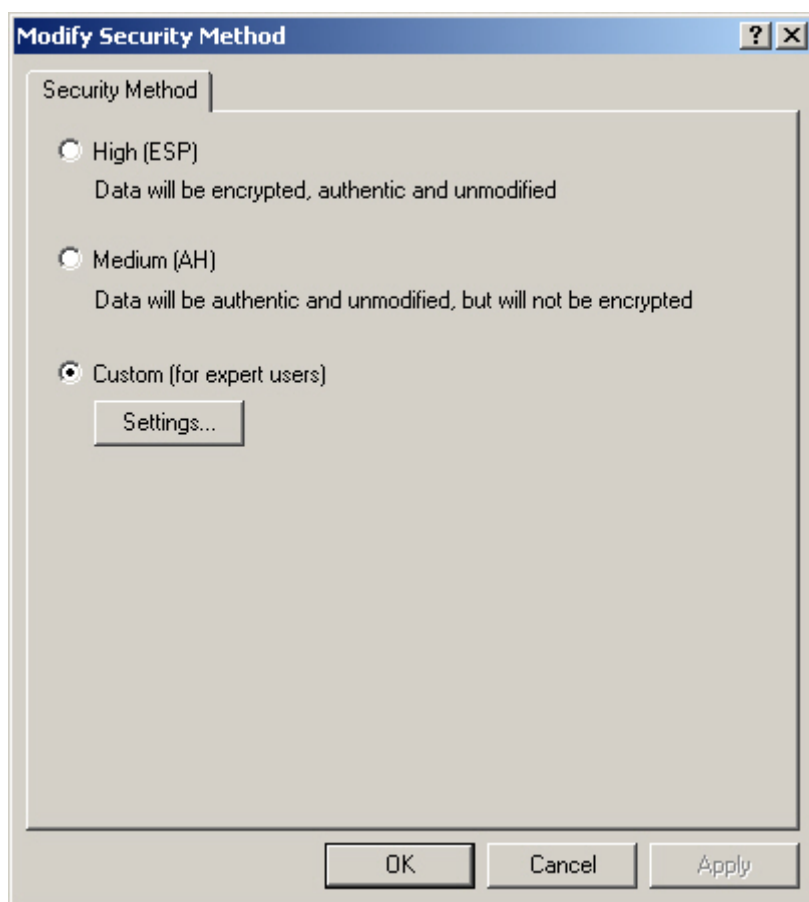
**Select Session key Perfect Forward Secrecy**

**Step35.** Select **Custom / None / 3DES / MD5** Security Method. Click **Edit**.



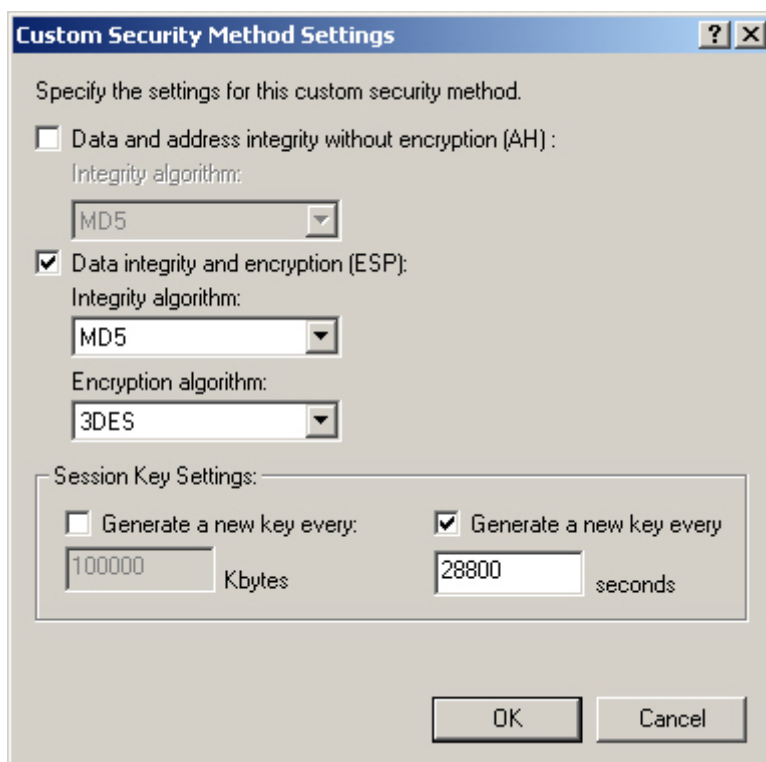
**Set the Security Method**

**Step36.** Select **Custom (for expert users)**, click **Settings**.



**Custom Security Method settings**

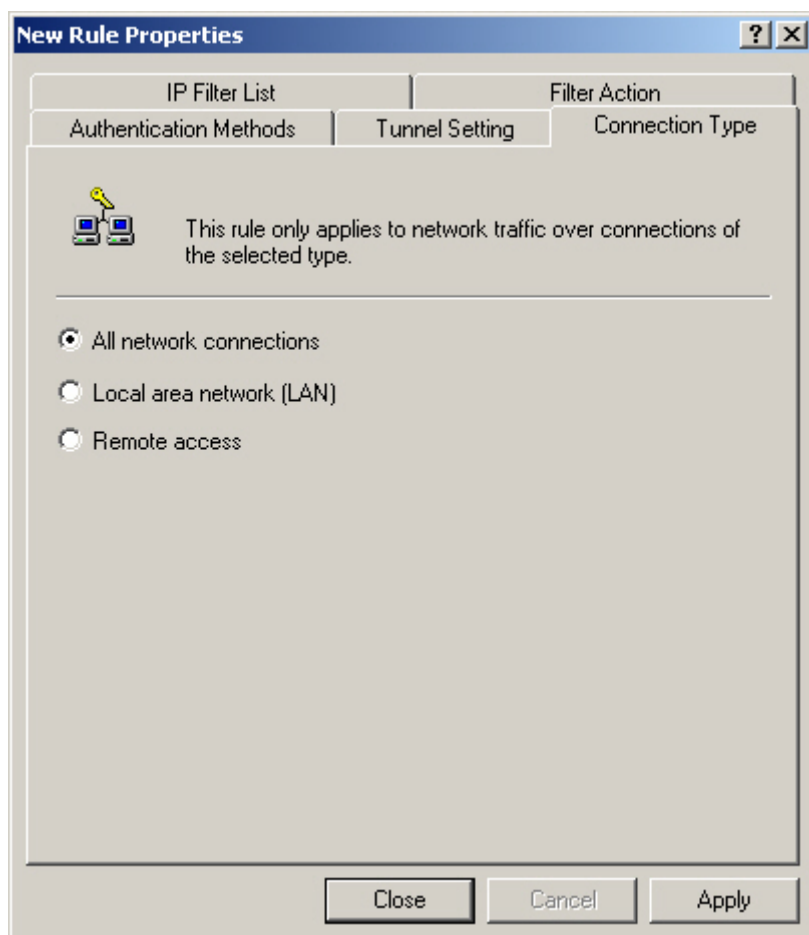
**Step37.** Select **Data integrity and encryption (ESP)**. **Integrity algorithm**, select MD5. **Encryption algorithm**, select 3DES. Also select **Generate a new key every**, enter 28800 seconds. Click **OK** to back to **New Rule Properties**.



**Complete the Custom Security Methods setting**

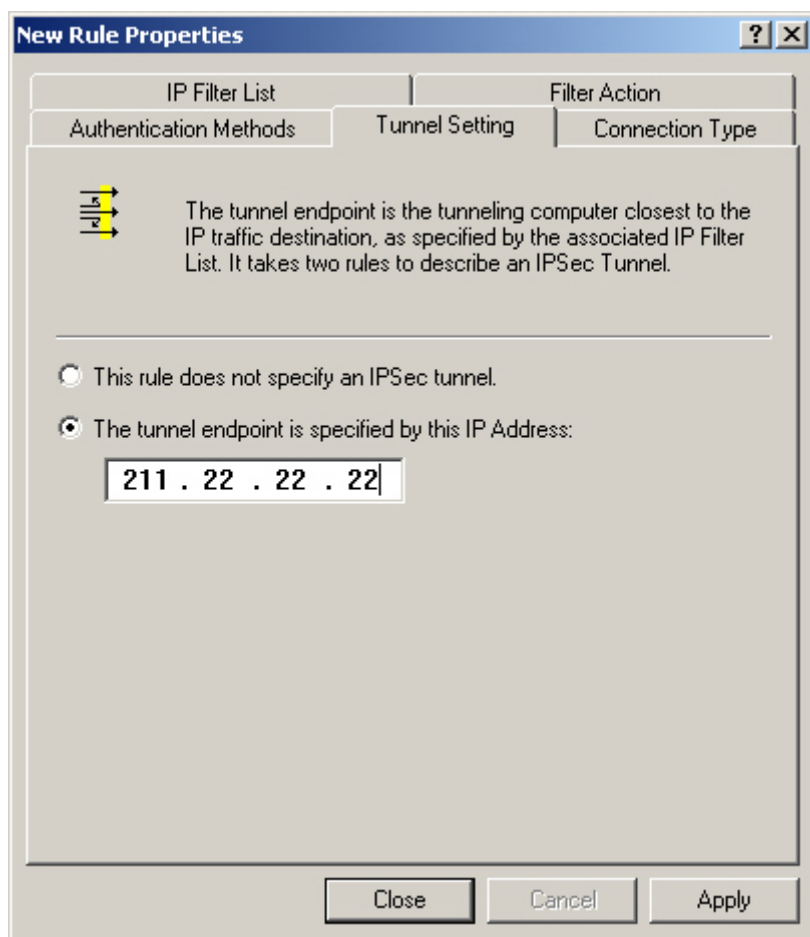


**Step38.** In **New Rule Properties** → **Connection Type**, select **All network connections**.



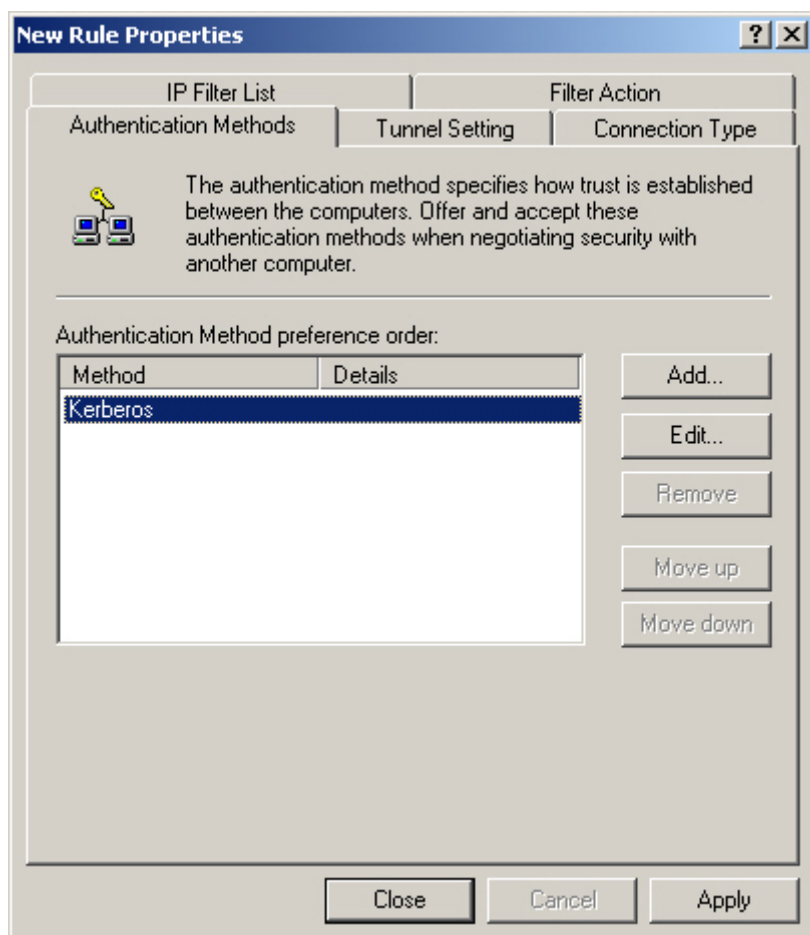
**Connection Type setting**

**Step39.** In **New Rule Properties** → **Tunnel Setting**, select **The tunnel endpoint is specified by this IP Address**. Enter B Company's WAN IP address 211.22.22.22.



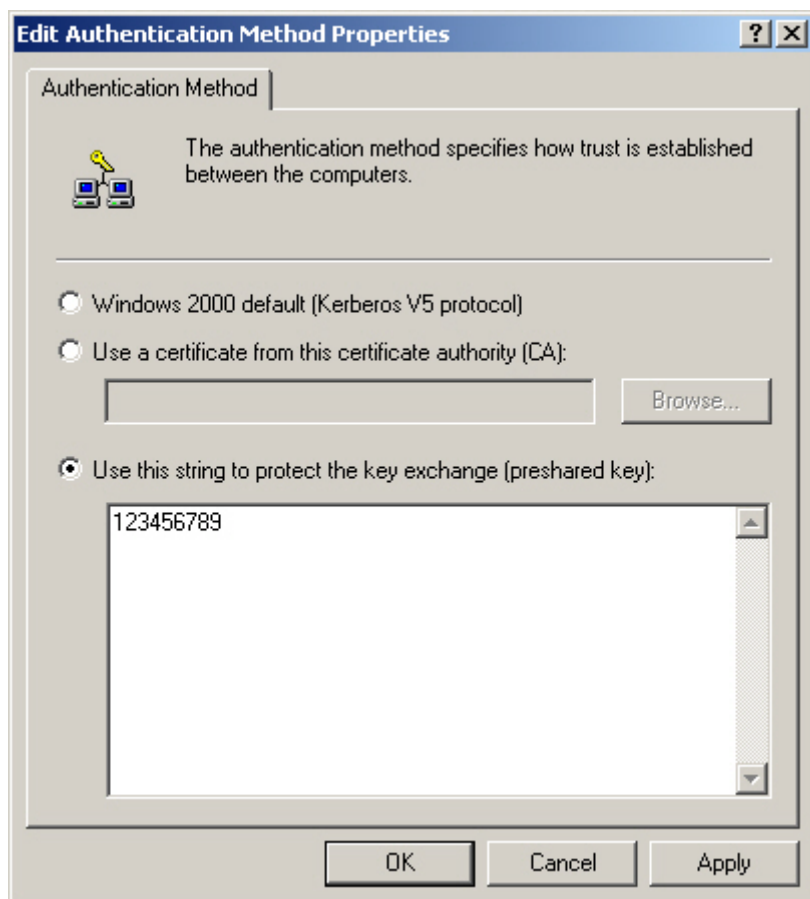
**Tunnel setting**

**Step40.** In **New Rule Properties** → **Authentication Methods**, click **Edit**.



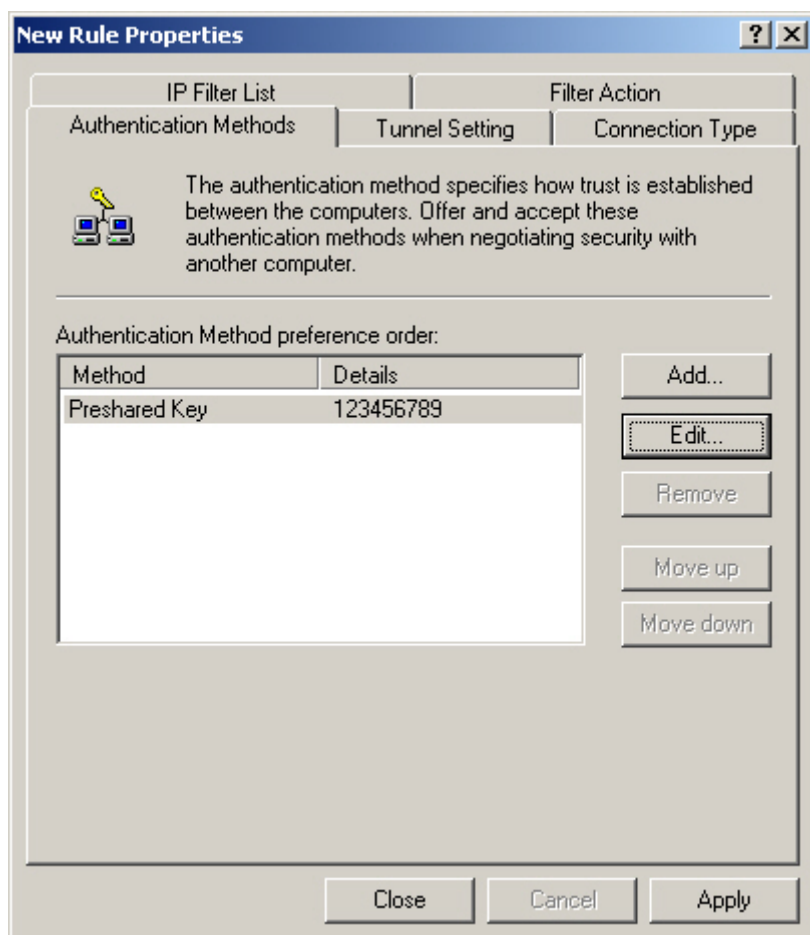
**Authentication Methods**

**Step41.** Select **Use this string to protect the key exchange (preshared key)**. Enter the Preshared Key - 123456789.



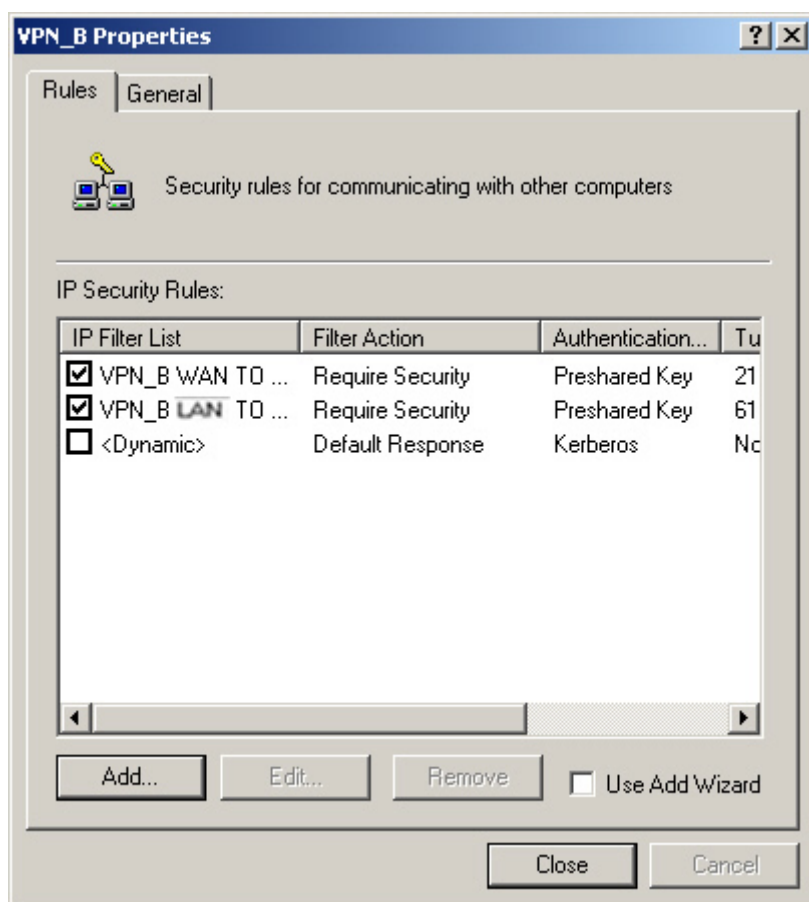
**VPN Preshared key setting**

**Step42.** Click **Apply** and **close** the setting window.



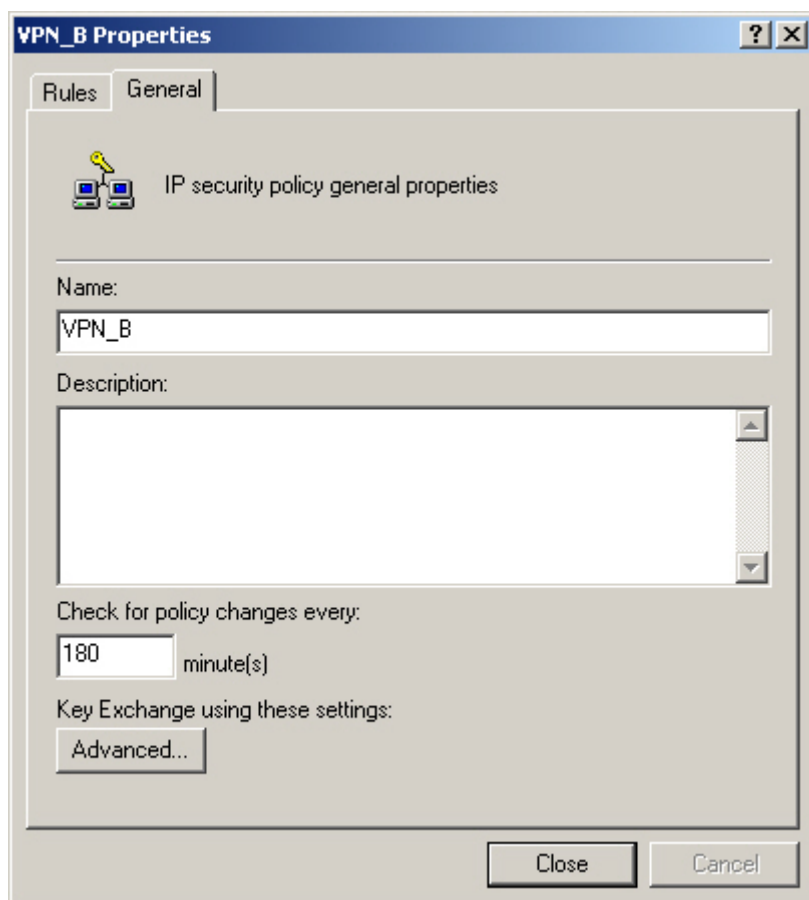
**Complete the New Rule setting**

**Step43.** Complete the VPN\_B LAN TO WAN setting.



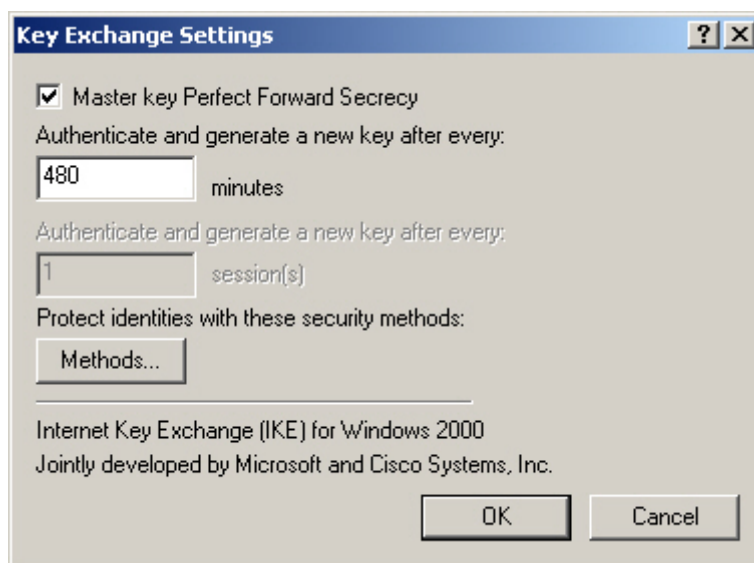
**Complete the VPN\_B LAN TO WAN Rule setting**

**Step44.** In **VPN\_B Properties** → **General**, click **Advanced**.



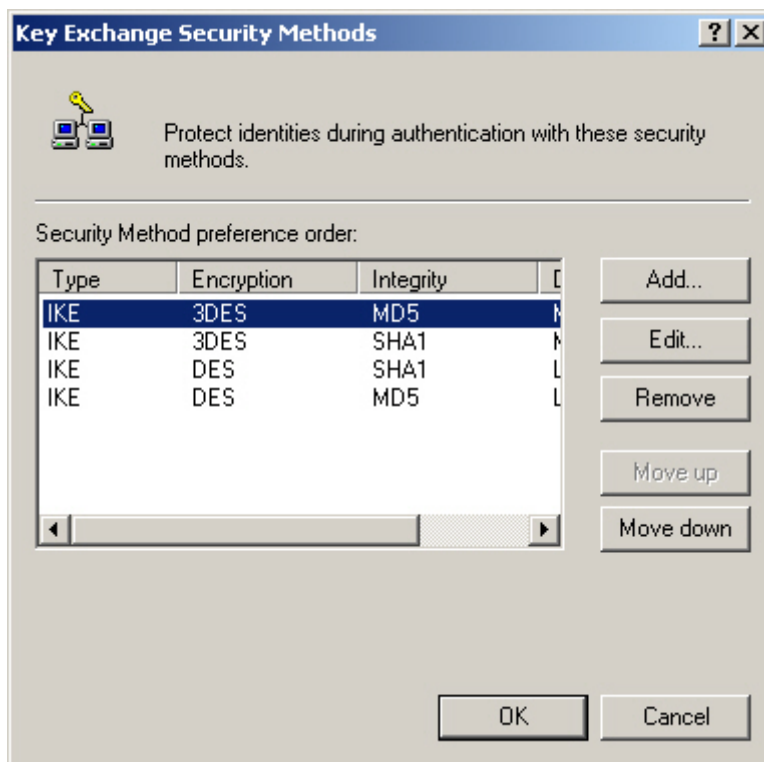
**The VPN\_B General setting**

**Step45.** Select **Master Key Perfect Forward Secrecy**, click **Methods**.



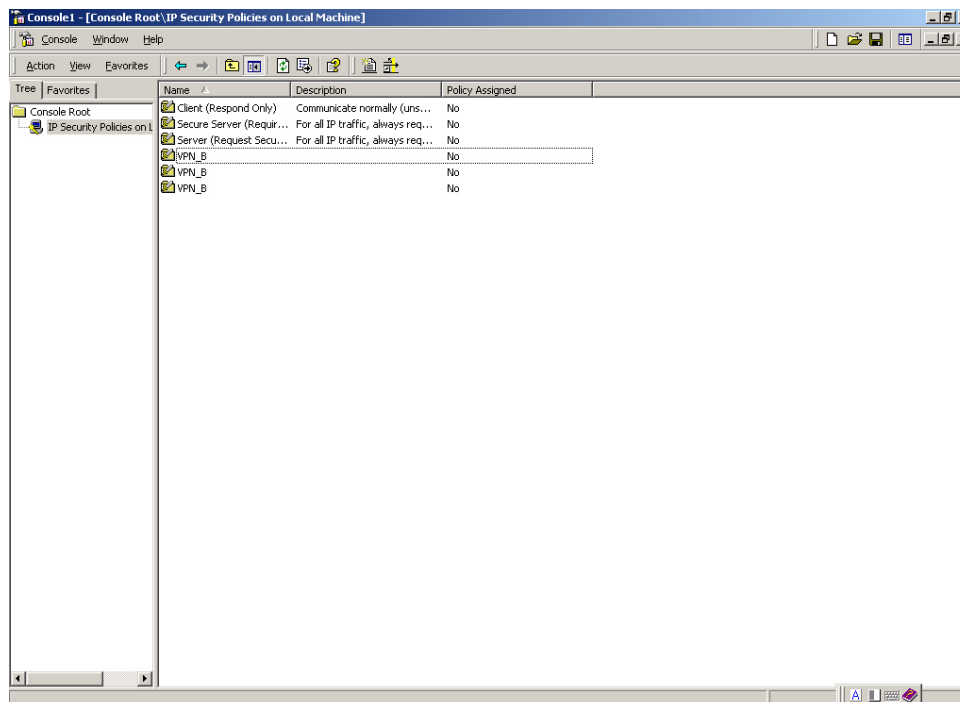
**Key Exchange settings**

**Step46.** Click **Move up** or **Move down** to arrange IKE / 3DES / MD5 / to the Top, and click **OK**.



To arrange the Security Methods

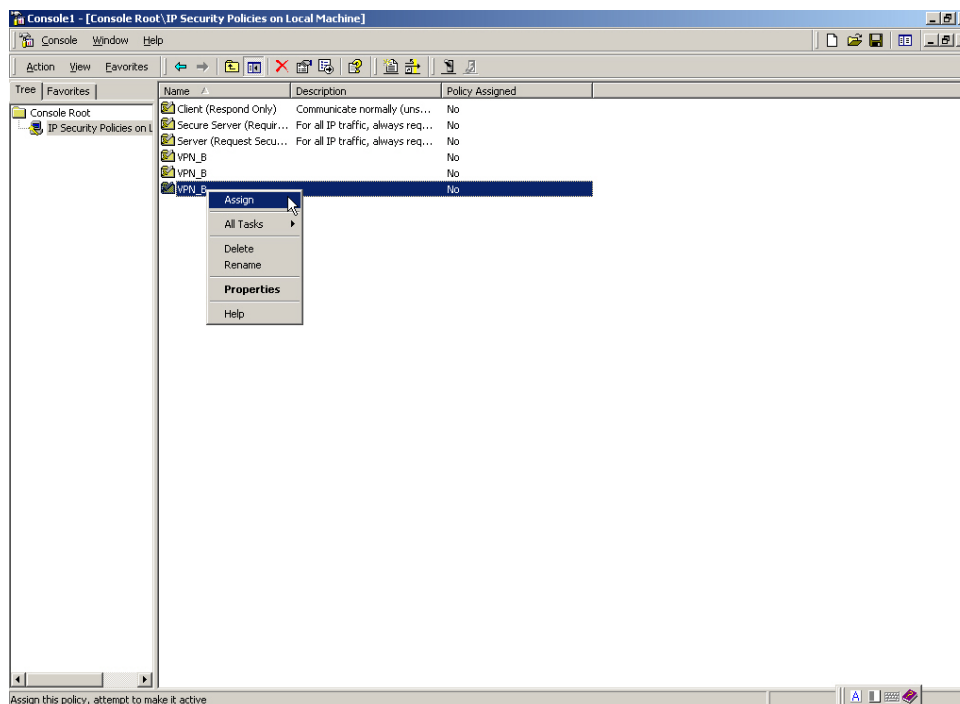
**Step47.** Complete all the Windows 2000 VPN settings.



Complete all the Windows 2000 IPsec VPN settings

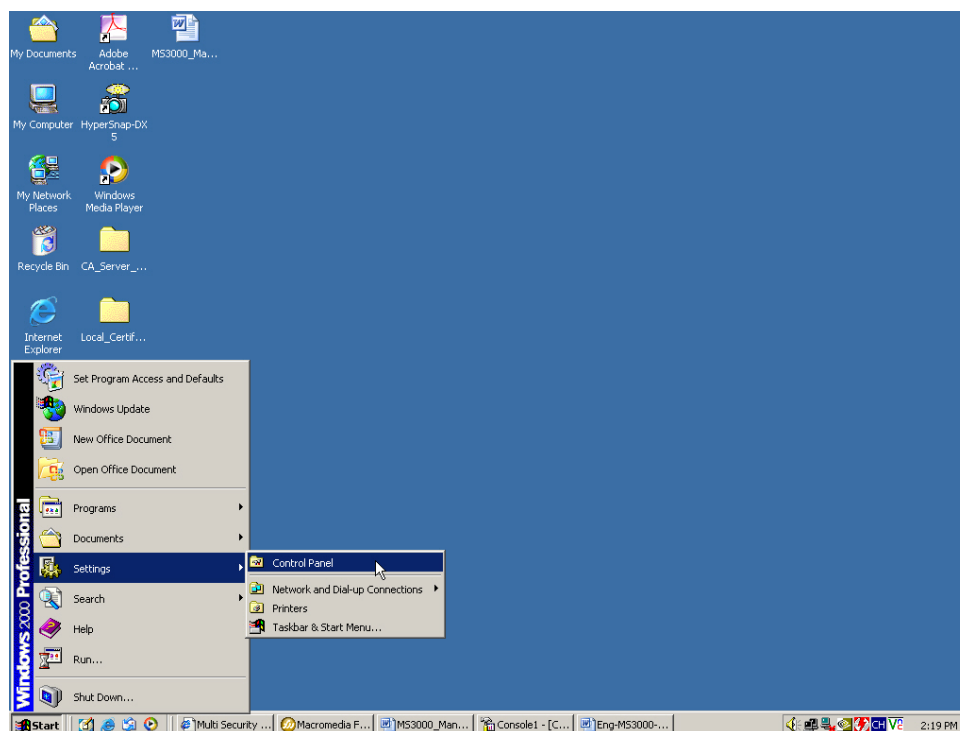


**Step48.** Right click on VPN\_B, select **Assign**.



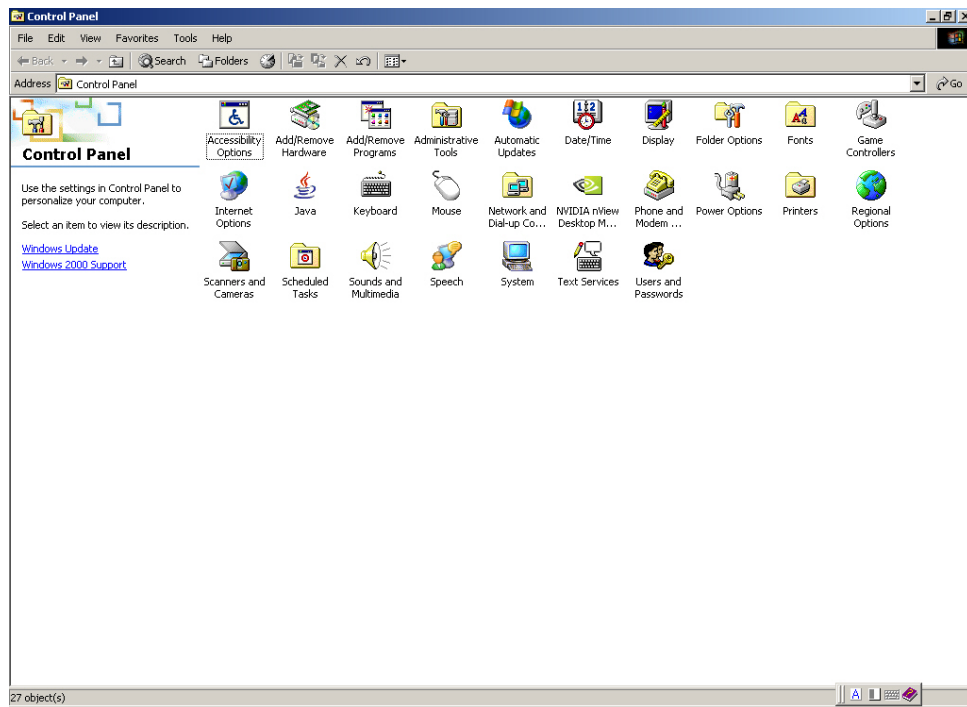
To assign the VPN\_B Security Rules

**Step49.** We need to restart the IPsec Service. Click **Start** → **Setting** → **Control Panel**.



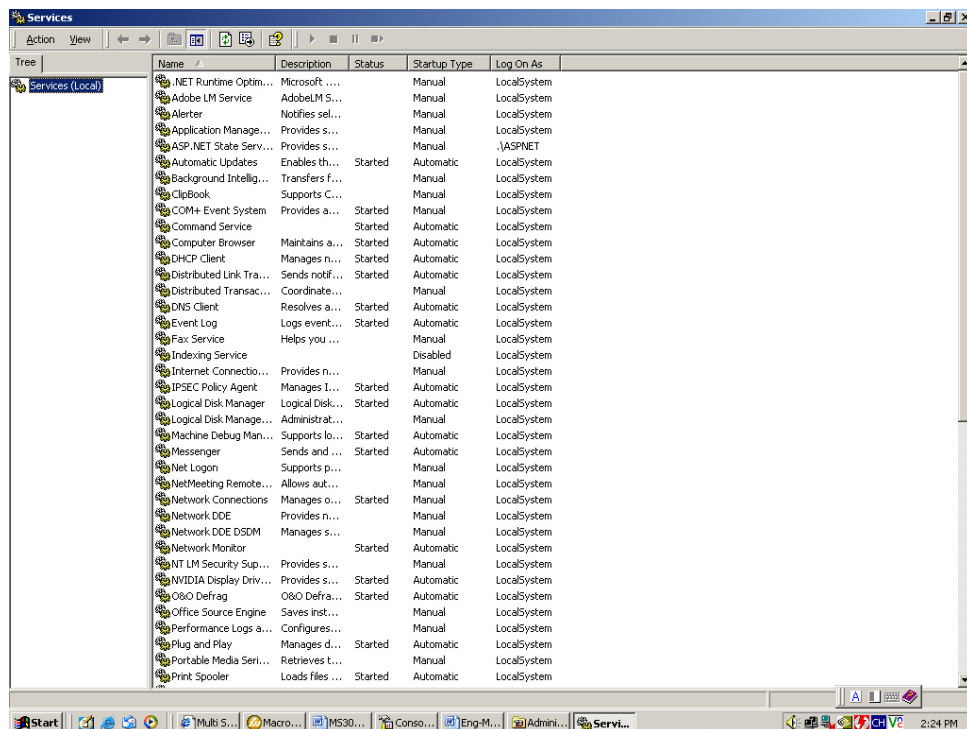
Enter the Control Panel

**Step50.** In **Control Panel**, double click **Administrative Tools** icon.



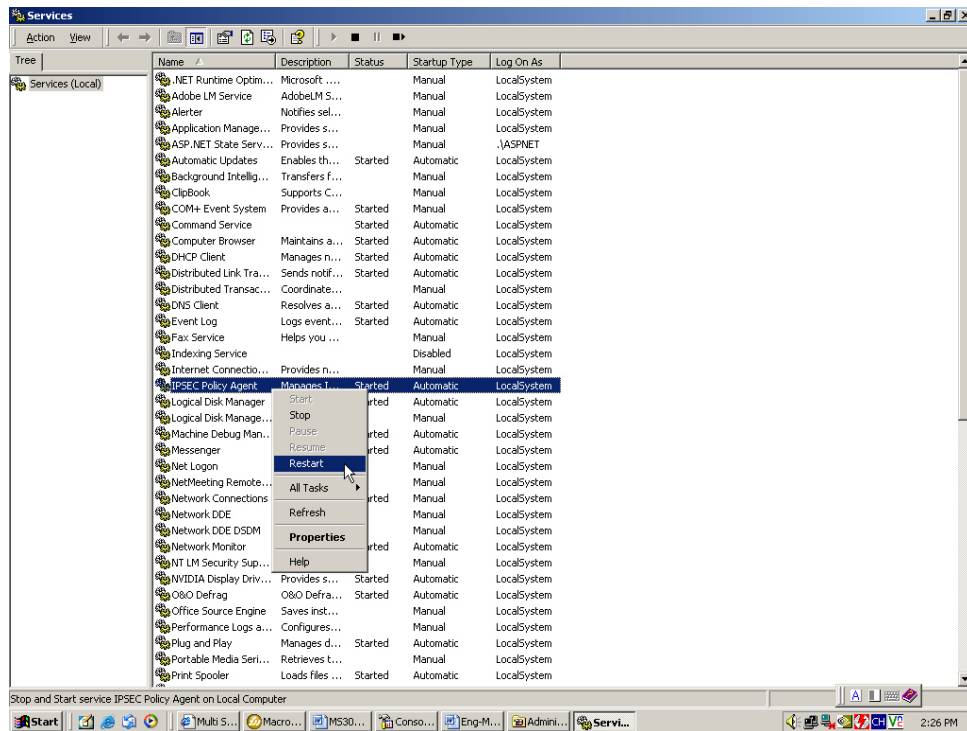
Enter the Administrative Tools

**Step51.** In **Administrative Tools**, double click **Services** icon.



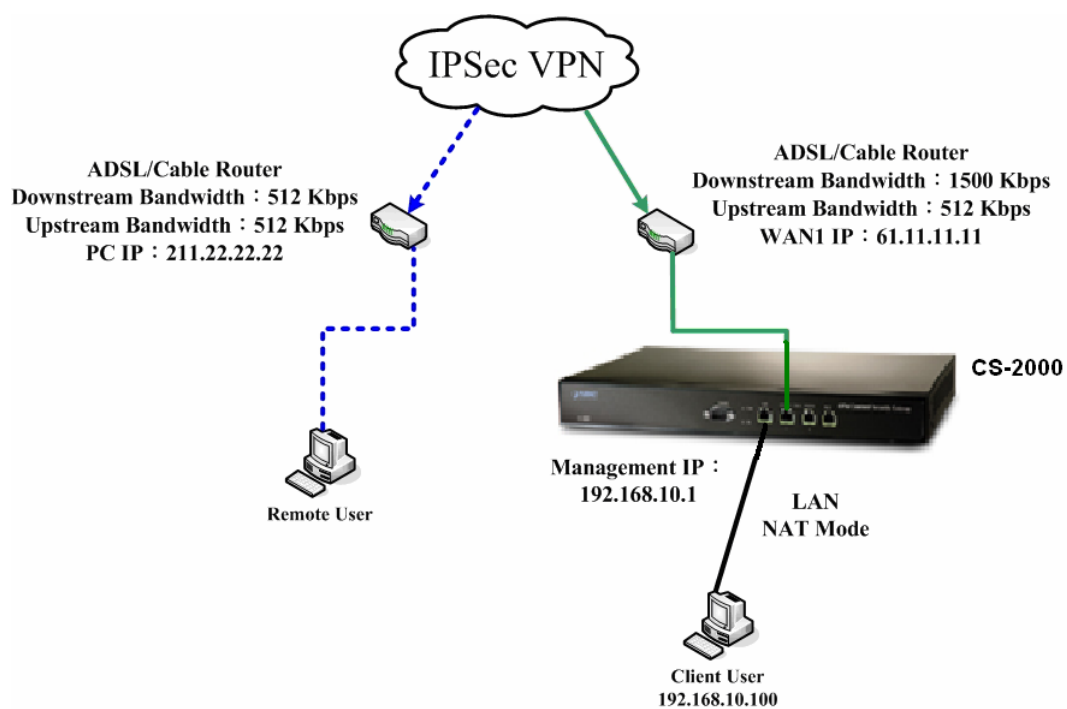
Enter the Services

**Step52.** In **Services**, right click on **IPsec Policy Agent**, select **Restart**.



**Restart IPsec Policy Agent**

**Step53.** Complete all the settings.



**The CS-2000 and Windows 2000 IPSec VPN deployment**

### 5.9.4 Example 3

The way to set the IPSec VPN connection between two CS-2000 appliances. (Aggressive mode)(The IPSec algorithm, 3DES encryption.MD5 authentication.)

#### The Deployment

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

We use two CS-2000 devices to be the platform .Assume that A Company **192.168.10.100** want to build the **VPN** to B Company **192.168.20.100**, in order to download the shared documents. (Aggressive mode).

**The A Company's default gateway is the CS-2000 LAN IP 192.168.10.1. Make the following settings:**

**Step1**    Enter A Company's CS-2000 default IP Address 192.168.10.1. In **Policy Object → VPN → IP Sec Autokey → New Entry**.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

[New Entry](#)

**IPSec Autokey**

- Step2** In **IPSec Autokey**, enter VPN\_A in the VPN **Name**. In **WAN interface**, select **WAN 1**, which the A Company uses it to build the VPN.

Necessary Item	
Name	<input type="text" value="VPN_A"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

**The IPSec VPN name and WAN interface setting**

- Step3** In To Destination, select Remote Gateway – Fixed IP or Domain Name. Enter the Remote IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="211.22.22.22"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

**The IPSec To Destination setting**

- Step4** In **Authentication Method**, select **Preshare**, enter the **Preshared Key**. (The maximum Preshared Key is 100 bytes).

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

**The IPSec Authentication Method setting**

- Step5** In **Encapsulation**, select **ISAKMP Algorithm**, to select the needed algorithm.  
In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select SHA1. In **Group** (GROUP 1, 2, 5), select Group 2, the both sides need to choose the same group.

ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼

#### The IPSec Encapsulation setting

- Step6** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**.  
In **ENC Algorithm** (3DES/DES/AES/NULL) select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. To assure the Authentication Method.

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

#### The IPSec Algorithm setting

**Step7** In **Perfect Forward Secrecy** ( NO-PFS/ GROUP 1,2,5 ), select GROUP 1. In **ISAKMP Lifetime**, enter 3600 seconds, and the **IPSec Lifetime**, enter 28800 seconds.

Optional Item	
Perfect Forward Secrecy	GROUP 1 ▼
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

#### The IPSec Perfect Forward Secrecy setting

**Step8** In **Mode**, select Aggressive mode.

In **My ID**, select not to enter.

If the both sides need to enter the My ID / Peer ID, then the MIS engineer must enter the different IP address. For example, 11.11.11.11 or 22.22.22.22. If the MIS engineer want to enter the Authentication number or alphabet, then he must add the @ in front of the number or alphabet. For example , @123a 、@abcd1.

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	11.11.11.11 (Max. 39 characters)
Peer ID	@abc123 (Max. 39 characters)

#### The IPSec Aggressive mode setting

**Step9** Complete the IPSec Autokey Setting.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Complete the IPSec Autokey setting



**Step10** In **VPN → VPN Trunk** add the following settings :

- **Name**, enter the Trunk name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the LAN address (A Company) 192.168.10.0 and Mask 255.255.255.0.
- **To Destination**, select To Destination Subnet / Mask.
- Enter the destination LAN IP address (B Company) 192.168.20.0 and mask 255.255.255.0.
- In **Tunnel**, click **Add**, to add the VPN\_A's IPsec VPN.
- Select **show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.10.0	/ 255.255.255.0
To Destination		
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.20.0	/ 255.255.255.0
<input type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 30%;">           &lt;--- Available Tunnel ---&gt;            VPN_A         </div> <div style="text-align: center; width: 30%;"> <input type="button" value="Remove"/>   <input type="button" value="Add"/> </div> <div style="border: 1px solid gray; padding: 5px; width: 30%;">           &lt;--- Selected Tunnel ---&gt;            VPN_A         </div> </div>		
Keep alive IP :	<input type="text"/>	
<input type="checkbox"/> Show remote Network Neighborhood		

Add the VPN trunk setting

i	Name▼	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.10.0	192.168.20.0	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete the VPN trunk setting

**Step11** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPSec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps         Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="0"/> KBytes ( Range: 0 - 999999 )

### Set the outgoing policy included the VPN trunk

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

[New Entry](#)

### Complete the outgoing policy setting included the VPN trunk

**Step12** In **Policy → Incoming** , add the following settings :

- **Schedule**, select **Working\_Time**.
- **Qos**, select **QoS\_1**.
- **VPN Trunk**, select **IPSec\_VPN\_Tunnel**.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<div> <div>Modify</div> <div>Remove</div> <div>Pause</div> </div> <div>To 1</div>

[New Entry](#)

**Complete the incoming policy setting included the VPN trunk**

The B Company's default gateway is the CS-2000's LAN IP 192.168.20.1. Add the following settings.

**Step1** Enter B Company's default IP address 192.168.20.1. Click **VPN → IPsec Autokey**, click **New Entry**.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

New Entry

### IPSec Autokey

**Step2** In **IPSec Autokey**, enter VPN\_B in **Name**. In **WAN interface**, select WAN 1, in order to build the B Company's VPN.

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

Set the IPSec VPN name and WAN interface setting

**Step3** In **To Destination**, select **Remote Gateway --Fixed IP or Domain Name**, enter the Remote IP address to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### The IPSec To Destination IP setting

**Step4** In Authentication Method, select Preshare, enter the Preshared Key. (The maximum Preshared Key is 100 bytes.)

Authentication Method	Preshare ▼
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

#### The IPSec Authentication Setting

**Step5** In **Encapsulation**, select ISAKMP Algorithm, choose the needed algorithm.  
In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select SHA1. In **Group** (GROUP 1, 2, 5), select GROUP 2. The both sides need to select the same group.

ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼

#### The IPSec Encapsulation setting

- Step6** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**.  
In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the authentication methods.

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

#### The IPSec Algorithm setting

- Step7** In **Perfect Forward Secrecy**( NO-PFS/ GROUP 1,2,5 ), select GROUP 1 . In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

#### The IPSec Perfect Forward Secrecy setting

- Step8** In **My ID**, select Aggressive mode.  
In **My ID / Peer ID**, the MIS engineer can select not to enter.  
In **My ID / Peer ID**, if the MIS engineer wants to enter the IP, then it must be the two different IP address. For example, 11.11.11.11, 22.22.22.22. If the MIS engineer want to add the number or alphabet to access the authentication, then he must add the @ in front of the alphabet or the numbers. For example, @123a, @abcd1.

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	@abc123 (Max. 39 characters)
Peer ID	11.11.11.11 (Max. 39 characters)

#### The IPSec Aggressive mode setting

- Step9** Complete the IPSec Autokey settings.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPB_B	WAN1	61.11.11.11	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Complete the IPSec Autokey setting

**Step10** In **VPN → Trunk → New Entry**, add the following settings :

- **Name**, enter the Trunk Name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the LAN IP address (B Company) 192.168.20.0 and mask 255.255.255.0.
- **To Destination**, select To Destination Subnet / Mask.
- Enter To Destination LAN IP (A Company) 192.168.10.0 and mask 255.255.255.0.
- In **Tunnel**, add the VPN\_B's IPSec VPN setting.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.20.0	255.255.255.0
To Destination		
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.10.0	255.255.255.0
<input type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px;"> &lt;--- Available Tunnel ---&gt;  VPN_B </div> <div style="text-align: center;"> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">Remove</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">Add</div> </div> <div style="border: 1px solid black; padding: 5px;"> &lt;--- Selected Tunnel ---&gt;  VPN_B </div> </div>		
Keep alive IP :		
<input type="checkbox"/> Show remote Network Neighborhood		

Add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.20.0	192.168.10.0	VPN_B	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete to add the VPN trunk setting

**Step11** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )

**Set the outgoing policy included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1

[New Entry](#)

**Complete the outgoing policy setting included the VPN trunk**



**Step12** In **Policy → Incoming**, add the following settings :

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

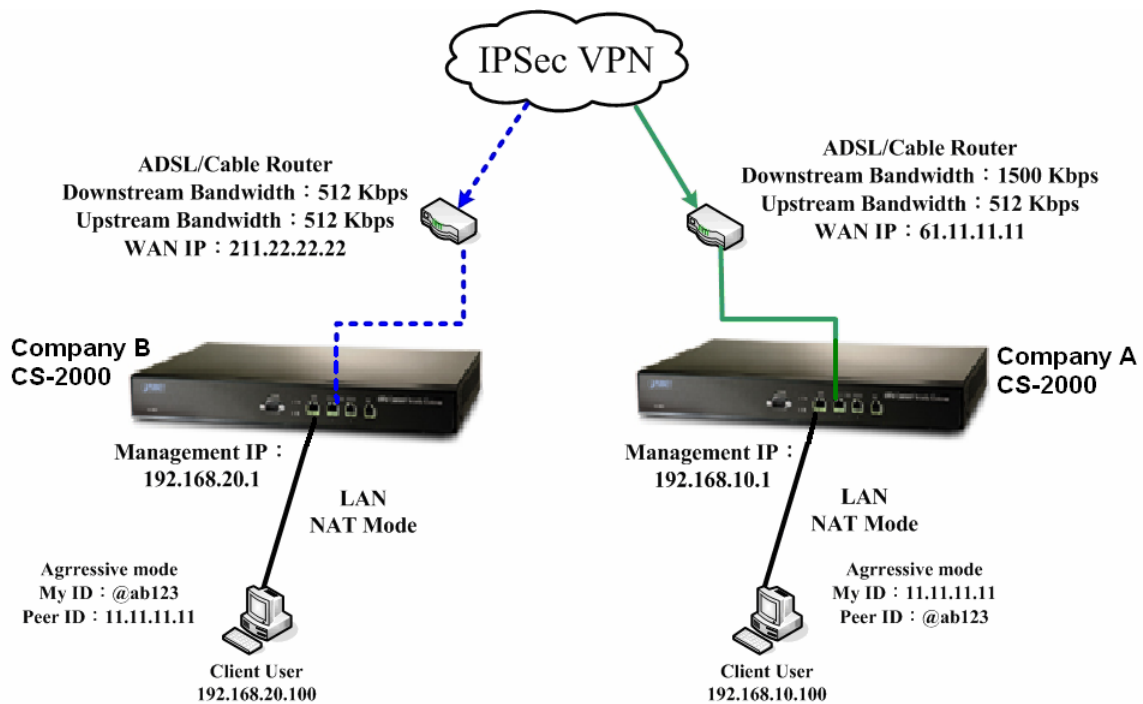
Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

[New Entry](#)

**Complete the incoming policy setting included the VPN trunk**

**Step13** Complete the IPSec VPN aggressive mode settings.

**The IPSec VPN aggressive mode deployment**

### 5.9.5 Example 4

The way to set the outbound load balance connection in IPSec VPN between two CS-2000 appliances. (The GRE / IPSec packets algorithm.)

#### The Deployment

A Company	WAN1 IP is 61.11.11.11
	WAN2 IP is 61.22.22.22
	LAN IP is 192.168.10.X
B Company	WAN1 IP is 211.22.22.22
	WAN2 IP is 211.33.33.33
	LAN IP is 192.168.20.X

The A and B Company applicated two local certificates from different CA Server.

The **A Company's WAN 1** built up the IPSec VPN to **B Company's WAN 1**.

The **A Company's WAN 2** built up the IPSec VPN to **B Company's WAN 2**.

We use two CS-2000 devices to be the platform. Assume that the A Company 192.168.10.100 want to build up the **VPN** to B Company 192.168.20.100, in order to download the shared documents. (Use the **GRE/IPSec packets algorithm**)

The A Company's default gateway is the LAN IP 192.168.10.1 in CS-2000.

**Step1** Enter the A Company's default IP address 192.168.10.1. In **VPN → IPsec Autokey**, click **New Entry**.

i	Name▼	WAN	Gateway IP	IPsec Algorithm	Configure
---	-------	-----	------------	-----------------	-----------

**IPsec Autokey**

**Step2** In **IPsec Autokey → Name**, enter VPN\_01. In **WAN interface**, select WAN 1.

Necessary Item	
Name	VPN_01 (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

**The IPsec VPN name and WAN interface setting**

**Step3** In **To Destination**, select **Remote Gateway—Fixed IP or Domain Name**, enter the remote (WAN 1) IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

**The IPsec To destination setting**

**Step4** In **Authentication Method**, select RSA-SIG. In **Local PEM**, select Site\_A\_01. In **Remote PEM**, select Site\_B\_01.

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

**The IPsec Authentication Method setting**

- Step5** In **Encapsulation**, select ISAKMP algorithm, to select the needed algorithm.  
In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 1. The both sides need to select the same group.

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

#### The IPSec Encapsulation setting

- Step6** In **IPSec Algorithm**, select Data Encryption + Authentication or Authentication Only. In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the data authentication method.

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

#### The IPSec Algorithm setting

**Step7** In **Perfect Forward Secrecy** ( NO-PFS/ GROUP 1, 2, 5 ) , select GROUP 1 . In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

#### The IPSec Perfect Forward Secrecy setting

**Step8** In **GRE/IPSec → GRE Local IP** , enter 192.168.50.100. In **GRE Remote IP** , enter 192.168.50.200 ( The local IP and remote IP must be in the same subnet of C class . )

GRE/IPSec			
GRE Local IP		192.168.50.100	
GRE Remote IP		192.168.50.200	
Dead Peer Detection	Delay	5	Second
	Timeout	60	Second (Delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)
<input type="checkbox"/> Manual Connect			

#### The GRE/IPSec setting

**Step9** Complete the VPN\_01 setting in IPSec Autokey.

i	Name▼	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	Modify Remove

[New Entry](#)

#### Complete the IPSec Autokey setting

**Step10** Enter the A Company's default IP address 192.168.10.1. In **VPN → IPsec Autokey**, click **New Entry**.

i	Name▼	WAN	Gateway IP	IPsec Algorithm	Configure
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### IPsec Autokey window

**Step11** In **IPsec Autokey → Name**, enter VPN\_02. In **WAN interface**, select WAN 2, which the A Company uses it to build up the VPN.

Necessary Item	
Name	VPN_02 (Max. 12 characters)
WAN interface	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3

#### The IPsec VPN name and WAN interface setting

**Step12** In **To Destination**, select **Remote Gateway—Fixed IP or Domain Name**, enter the remote WAN 2 IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.33.33.33 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### The IPsec To Destination setting

**Step13** In **Authentication Method**, select **Preshare**. And enter the number of **Preshared Key**.

Authentication Method	Preshare ▼
Preshared Key	987654321 (Max. 103 characters)

#### The IPsec Authentication Method setting

- Step14** In **Encapsulation**, select ISAKMP algorithm, to choose the needed algorithm.  
In **ENC Algorithm** (3DES/DES/AES), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**. In **Group** (GROUP 1, 2, 5), select **GROUP 1**. The both sides need to choose the same group.

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

#### The IPSec Encapsulation setting

- Step15** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**.  
In **ENC Algorithm** (3DES/DES/AES/NULL), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**, to assure the data authentication method.

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

#### The IPSec Algorithm setting



**Step16** In **Perfect Forward Secrecy** (NO-PFS/ GROUP 1,2,5), select **GROUP 1**. In **ISAKMP Lifetime**, enter **3600** seconds. In **IPSec Lifetime**, enter **28800** seconds. In **Mode**, select **main mode**.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step17** In **GRE/IPSec → GRE Local IP**, enter 192.168.60.100. In **GRE Remote IP**, enter 192.168.60.200 . ( the local IP and remote IP must be in the same segment of C class )

GRE/IPSec			
GRE Local IP	192.168.60.100		
GRE Remote IP	192.168.60.200		
Dead Peer Detection	Delay	5 Second	Timeout 60 Second (Delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)
<input type="checkbox"/> Manual Connect			

### The GRE/IPSec setting

**Step18** Complete the VPN\_02 setting in IPSec Autokey.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_01	WAN1	211.22.22.22	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>
--	VPN_02	WAN2	211.33.33.33	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Complete the IPSec Autokey setting

**Step19** In **VPN → VPN Trunk** , add the following settings :

- **Name**, enter the Trunk Name.
- **From Source**, select LAN.
- In **From Source Subnet / Mask**, enter the LAN source IP (A Company) 192.168.10.0 and mask 255.255.255.0.
- In **To Destination**, select **To Destination Subnet / Mask**.
- In **To Destination Subnet / Mask**, enter the LAN IP address 192.168.20.0 (B Company) and mask 255.255.255.0.
- In **Tunnel**, add the VPN\_01 and VPN\_02 IPsec VPN setting.
- Select **Show remoter Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.10.0	255.255.255.0
To Destination		
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.20.0	255.255.255.0
<input type="radio"/> Remote Client		
Tunnel		
<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 30%;">           &lt;--- Available Tunnel ---&gt;            VPN_01            VPN_02         </div> <div style="text-align: center; width: 30%;"> <input type="button" value="Remove"/>   <input type="button" value="Add"/> </div> <div style="border: 1px solid black; padding: 5px; width: 30%;">           &lt;--- Selected Tunnel ---&gt;            VPN_01            VPN_02         </div> </div>		
Keep alive IP :		
<input type="checkbox"/> Show remote Network Neighborhood		

To add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure		
	IPsec_VPN_Tu...	192.168.10.0	192.168.20.0	VPN_01, ...	Modify	Remove	Pause

Complete to add the VPN trunk setting

**Step20** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )

**Set the outgoing policy setting included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY				

[New Entry](#)

**Complete the outgoing policy setting included the VPN trunk**

**Step21** In **Policy → Incoming** , add the following settings :

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy setting included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<div> <div>Modify</div> <div>Remove</div> <div>Pause</div> </div>

[New Entry](#)

**Complete the incoming policy setting included the VPN trunk**

**Step1** Enter the B Company's default IP address 192.168.20.1. In **VPN → IPsec Autokey → New Entry**.

i	Name▼	WAN	Gateway IP	IPsec Algorithm	Configure
<div>New Entry</div> <div>IPsec Autokey</div>					

**Step2** In **IPsec Autokey → Name**, enter VPN\_01. In **WAN interface**, select WAN 1, which the B Company uses it to build the VPN.

Necessary Item	
Name	VPN_01 (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2 <input type="radio"/> WAN 3

To set the IPsec VPN name and WAN interface setting

**Step3** In **To Destination**, select **Remote Gateway – Fixed IP or Domain Name**, enter the remote (WAN 1) IP address, to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	61.11.11.11 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

The IPsec To Destination setting

**Step4** In **Authentication Method**, select **Preshare**, and enter the number of **Preshared Key**.

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

The IPsec Authentication Method setting

- Step5** In **Encapsulation**, select ISAKMP algorithm, to choose the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 1. The both sides need to choose the same group.

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

#### The IPSec Encapsulation setting

- Step6** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the data authentication method.

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

#### The IPSec Algorithm setting

**Step7** In **Perfect Forward Secrecy**( NO-PFS/ GROUP 1,2,5 ), select GROUP 1 . In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step8** In **GRE/IPSec → GRE Local IP**, enter 192.168.50.200. In **GRE Remote IP**, enter 192.168.50.100. ( the local IP and remote IP must be in the same C class segment. )

GRE/IPSec			
GRE Local IP		192.168.50.200	
GRE Remote IP		192.168.50.100	
Dead Peer Detection	Delay 5 Second	Timeout 60 Second	(Delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)
<input type="checkbox"/> Manual Connect			

### The GRE/IPSec setting

**Step9** Complete the IPSec Autokey VPN\_01 setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Complete to set the IPSec Autokey setting

**Step10** Enter the B Company's default IP address 192.168.20.1. In **VPN → IPsec Autokey → New Entry**.

i	Name▼	WAN	Gateway IP	IPsec Algorithm	Configure
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### The IPsec Autokey

**Step11** In **IPsec Autokey → Name**, enter VPN\_02. In **WAN interface**, select WAN 2, which the B Company uses it to build the VPN.

Necessary Item	
Name	<input type="text" value="VPN_02"/> (Max. 12 characters)
WAN interface	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3

### To set the IPsec VPN name and WAN interface setting

**Step12** In **To Destination**, select **Remote Gateway – Fixed IP or Domain Name**, enter the remote (WAN 2) IP address, to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.22.22.22"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

### The IPsec To Destination setting

**Step13** In **Authentication Method**, select **Preshare**. Enter the number of **Preshared Key**

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="987654321"/> (Max. 103 characters)

### The IPsec Authentication setting



**Step14** In **Encapsulation**, select ISAKMP algorithm, to choose the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 1. The both sides need to choose the same group

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

#### The IPSec Encapsulation setting

**Step15** In **IPSec Algorithm**, select **Data Encrytion + Authentication** or **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5, to assure the data authentication method.

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

#### The IPSec Algorithm setting

**Step16** In **Perfect Forward Secrecy**( NO-PFS/ GROUP 1,2,5 ), select GROUP 1 . In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

### The IPSec Perfect Forward Secrecy setting

**Step17** In **GRE/IPSec → GRE Local IP**, enter 192.168.60.200. In **GRE Remote IP**, enter 192.168.60.100. ( the local IP and remote IP must be in the same C class segment. )

GRE/IPSec			
GRE Local IP	192.168.60.200		
GRE Remote IP	192.168.60.100		
Dead Peer Detection	Delay 5 Second	Timeout 60 Second	(Delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)
<input type="checkbox"/> Manual Connect			

### The GRE/IPSec setting

**Step18** Complete the IPSec Autokey VPN\_02 setting

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_01	WAN1	61.11.11.11	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>
--	VPN_02	WAN2	61.22.22.22	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Complete the IPSec Autokey setting

**Step19** In **VPN → VPN Trunk** , add the following settings :

- In **Name**, enter the trunk name.
- **From Source**, select LAN.
- In **From Source Subnet/ Mask**, enter B Company's LAN source IP 192.168.20.0 and mask 255.255.255.0.
- In **To Destination**, select To Destination Subnet / Mask.
- In **To Destination Subnet / Mask**, enter A Company's LAN IP 192.168.10.0 and mask 255.255.255.0.
- In **Tunnel**, to **Add** the VPN\_01 and VPN\_02 IPsec VPN setting.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	IPsec_VPN_Tunnel (Max. 16 characters)	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.20.0	255.255.255.0
To Destination		
	<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.10.0 / 255.255.255.0
	<input type="radio"/> Remote Client	
Tunnel		
	<div style="border: 1px solid black; padding: 5px;"> <div style="text-align: center;">&lt;--- Available Tunnel ---&gt;</div> <div>VPN_01</div> <div>VPN_02</div> </div>	<div style="border: 1px solid black; padding: 5px;"> <div style="text-align: center;">&lt;--- Selected Tunnel ---&gt;</div> <div>VPN_01</div> <div>VPN_02</div> </div>
	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 2px 10px; background-color: #4f81bd; color: white;">Remove</div> <div style="border: 1px solid black; padding: 2px 10px; background-color: #4f81bd; color: white;">Add</div> </div>	
Keep alive IP :	<input type="text"/>	
<input type="checkbox"/> Show remote Network Neighborhood		

To add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPsec_VPN_Tu...	192.168.20.0	192.168.10.0	VPN_01, ...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete to add the VPN trunk setting

**Step20** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Trunk.
- Click **OK**.

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )

To set the outgoing policy included the VPN trunk

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

New Entry

Complete to set the outgoing policy included the VPN trunk

**Step21** In **Policy → Incoming** , add the following settings :

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

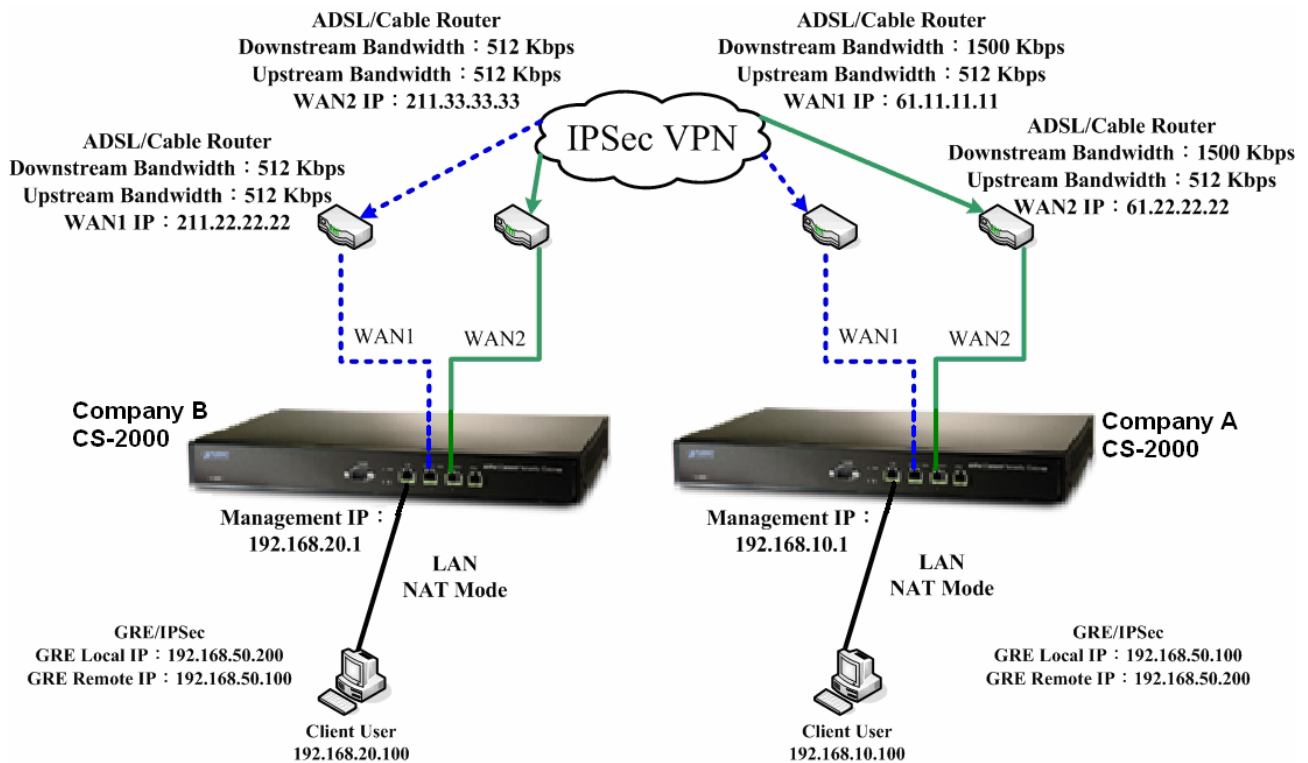
Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	IPsec_VPN_Tunnel
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**To set the incoming policy included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

[New Entry](#)

**Complete to set the incoming policy included the VPN trunk**

**Step22 Complete the IPSec VPN GRE/IPSec settings.****The IPSec VPN GRE/IPSec deployment**

### 5.9.6 Example 5

**The way to set the CS-2000 appliance PPTP VPN connection in Windows 2000.**

#### The Deployment

A Company Use the CS-2000.

**WAN IP is 61.11.11.11**

**LAN IP is 192.168.10.X**

B Company Use the Windows 2000 PC.

**WAN IP is 211.22.22.22**

We use the CS-2000 and Windows 2000 VPN-PPTP to be the platform. Assume the B Company **211.22.22.22** link to A Company **192.168.10.100** via the VPN, in order to download the shared files.

The A Company's default gateway is the LAN IP 192.168.10.1 in CS-2000 , add the following settings :

**Step1** In A Company 's CS-2000 , **VPN → PPTP Server** , click **Modify**, select **Enable PPTP** :

- Select **Encryption**.
- **Client IP Range**, enter 192.44.75.1 – 254.
- Select **Allow remote client to connect to Network**.
- **Auto-Disconnect if idle**, enter 0.

Modify PPTP Server Setting	
<input type="radio"/> Disable PPTP	
<input checked="" type="radio"/> Enable PPTP	
<input checked="" type="checkbox"/> Encryption	
Client IP Range :	192.44.75.1 .. 254
DNS Server 1	
DNS Server 2	
WINS Server 1	
WINS Server 2	
<input checked="" type="checkbox"/> Allow PPTP client to connect to the Internet via the WAN port	
<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> WAN3	
Auto-Disconnect if idle <input type="text" value="0"/> minutes ( Range: 0 - 999999, 0: means always connected )	
Echo-Request Retry <input type="text" value="3"/> times Timeout <input type="text" value="15"/> Second (Retry: 0 - 9, 0: means disable; Timeout: 1 - 30)	
<input type="checkbox"/> Enable RADIUS Server Authentication	
( IP or Domain Name )	
RADIUS Server Port	<input type="text" value="1812"/> ( Range: 1 - 65535 )
Shared Secret	<input type="text"/> (Max. 40 characters)

**To enable PPTP VPN setting**



As create the CS-2000 PPTP server VPN, the MIS engineer can allow or limit the external user to link to network via the CS-2000.



**Auto-Disconnect if idle** : When the VPN is not in use, it will automatically disconnect. ( Time unit : minute )



**Step2** In A Company's CS-2000 , **VPN → PPTP Server** , add the following settings :

- Click **New Entry**.
- **User Name**, enter PPTP\_Connection.
- **Password**, enter 123456789.
- **Client IP assigned by**, select IP Range.
- Click **OK**.

Add New PPTP Server

User Name :	PPTP_Connection	(Max. 16 characters)
Password :	*****	(Max. 19 characters)
Client IP assigned by		
<input checked="" type="radio"/> IP Range		
<input type="radio"/> Fixed IP : <input type="text"/>		
<input type="checkbox"/> Manual Disconnect		

### The PPTP VPN setting

PPTP Server (Enable, Encryption:ON) :

Client IP Range : 192.44.75.1-254

Total entry : 1

i	User Name ▼	Client IP	Uptime	Configure	
--	PPTP_Connection	0.0.0.0	---	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

### Complete to set the PPTP VPN setting

**Step3** In **VPN → VPN Trunk** , add the following settings :

- **Name**, enter the trunk name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the A Company's LAN IP address 192.168.10.0 and mask 255.255.255.0.
- **To Destination**, select Remote Client.
- In **Tunnel**, to **add** the PPTP\_Server\_PPTP\_Connection PPTP VPN setting.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Trunk**

Name	PPTP_VPN_Trunk (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	<input type="radio"/> To Destination Subnet / Mask <input checked="" type="radio"/> Remote Client
Tunnel	<div style="display: flex; justify-content: space-between;"> <div> <p>&lt;--- Available Tunnel ---&gt;</p> <p>PPTP_Server_PPTP_Connection</p> </div> <div> <p>Remove</p> <p>Add</p> </div> <div> <p>&lt;--- Selected Tunnel ---&gt;</p> <p>PPTP_Server_PPTP_Connection</p> </div> </div>
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

To add the VPN trunk setting

i	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	PPTP_VPN_Tru...	192.168.10.0	Remote Client	PPTP_Ser...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete to set the VPN trunk setting

**Step4** In **Policy → Outgoing** , add the following settings :

- **Authentication User**, select auth\_group.
- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select PPTP\_VPN\_Trunk.
- Click **OK**.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

**To set the outgoing policy included the VPN trunk**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY				<div> <div>Modify</div> <div>Remove</div> <div>Pause</div> </div> <div>To 1</div>

[New Entry](#)

**Complete to set the outgoing policy included the VPN trunk**

**Step5** In **Policy → Incoming** , add the following settings :

- **Schedule**, select Working\_Time.
- **Qos**, select QoS\_1.
- **VPN Trunk**, select PPTP\_VPN\_Trunk.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Working_Time
VPN Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

**To set the incoming policy included the VPN trunk**

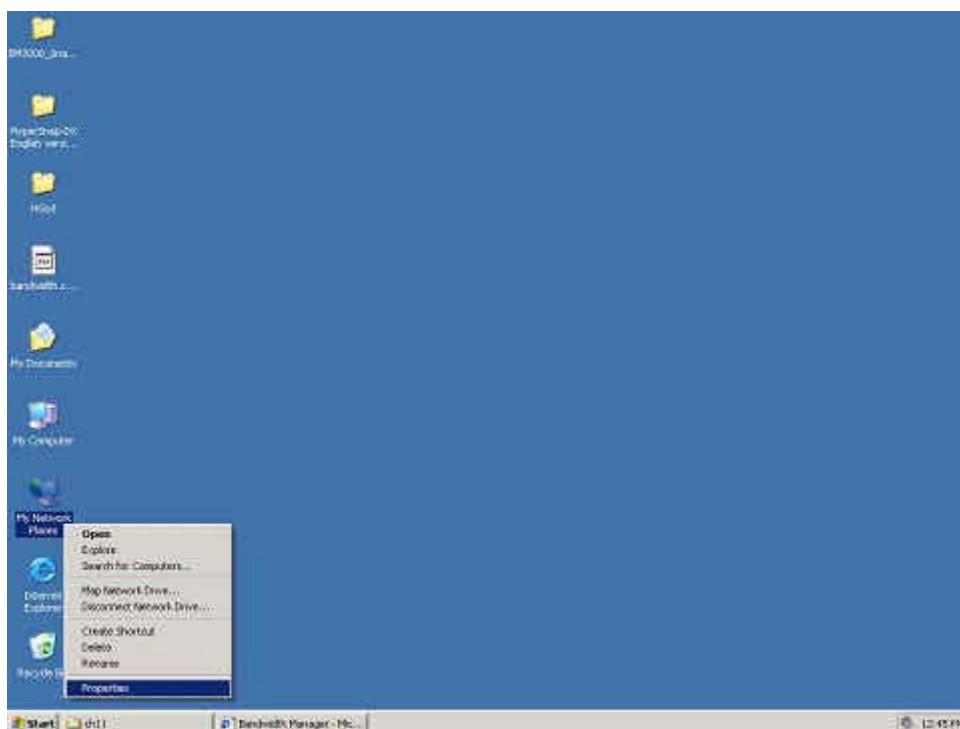
Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY				<div> <div>Modify</div> <div>Remove</div> <div>Pause</div> </div>

[New Entry](#)

**Complete to set the incoming policy included the VPN trunk**

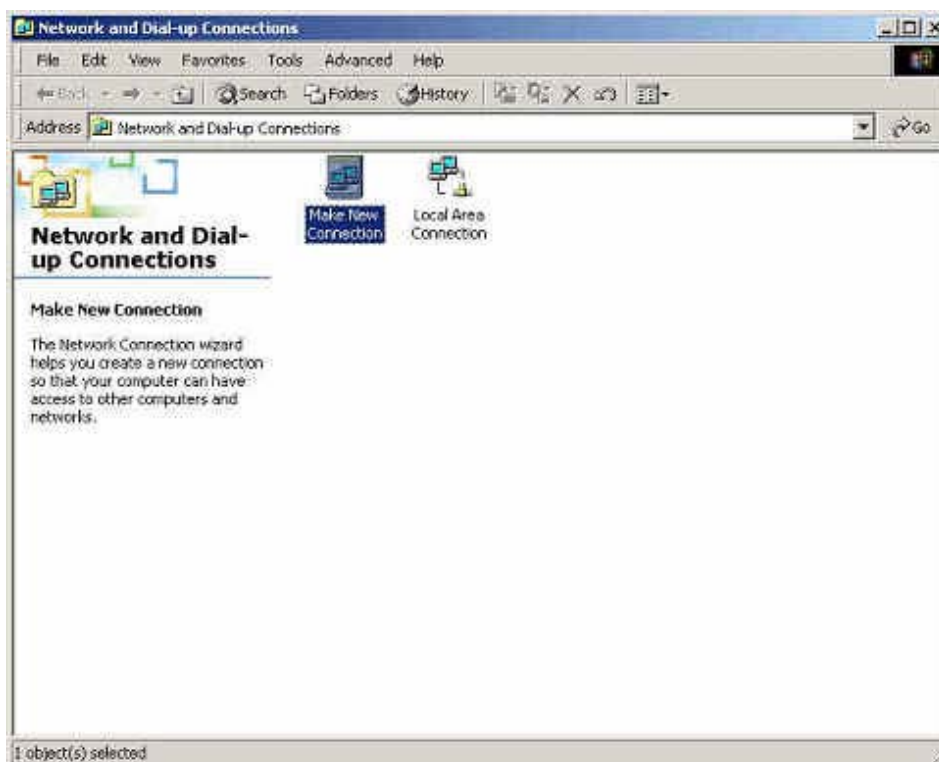
The B Company's PC use the Real IP ( **211.22.22.22** ) . Add the following settings :

**Step1** Right click on **My Network Places**, and select **Properties**.



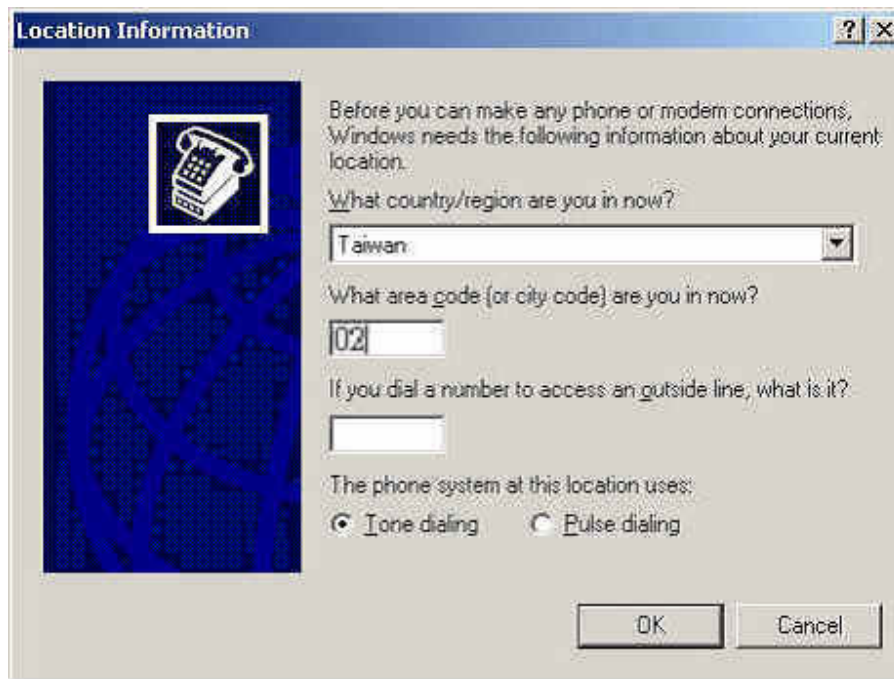
To start the Windows 2000 PPTP VPN setting

**Step2** In **Network and Dial-up Connection**, click **Make New Connection**.



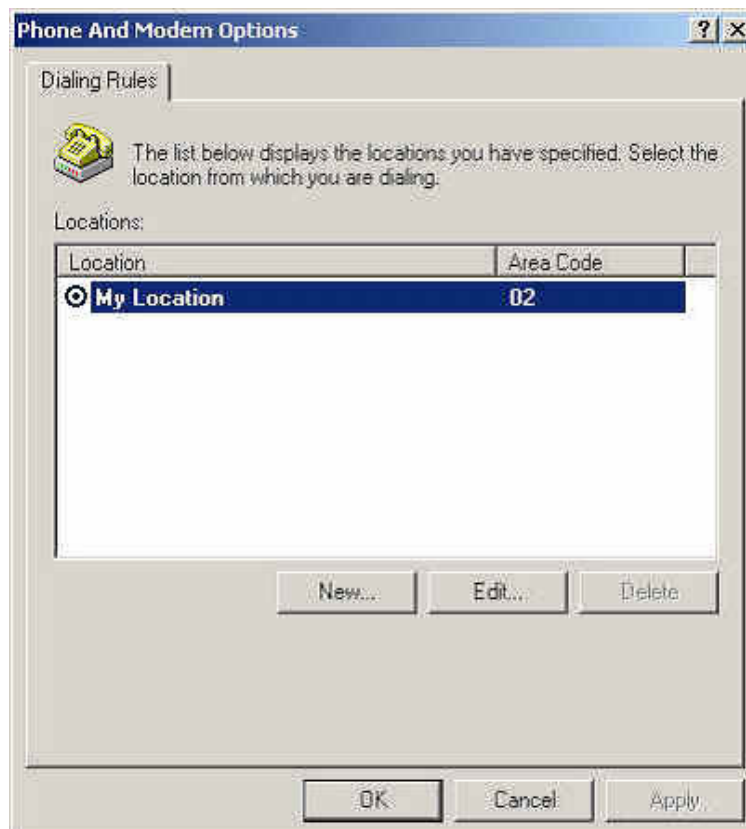
Network and Dial-up Connection

- Step3** In **Location Information**, enter the **Country /Region**, **Area code** and select the **phone system**, then click **OK**.



The Local Information setting

- Step4** In **Phone And Modem Options**, click **OK**.



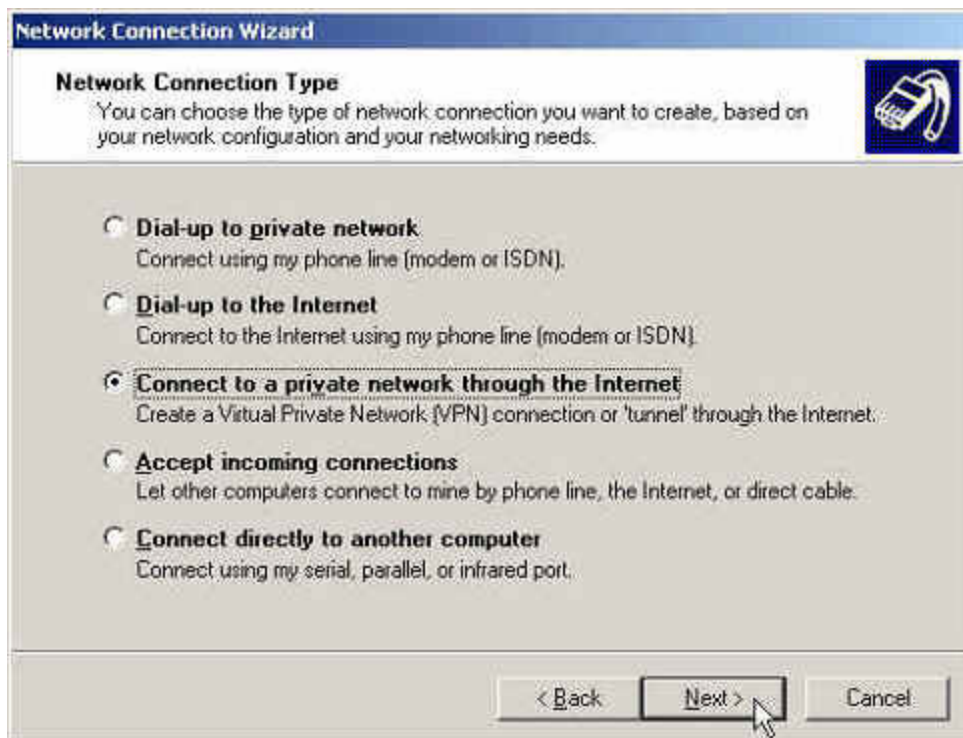
Phone and Modem Options

**Step5** In **Network Connection Wizard**, click **Next**.



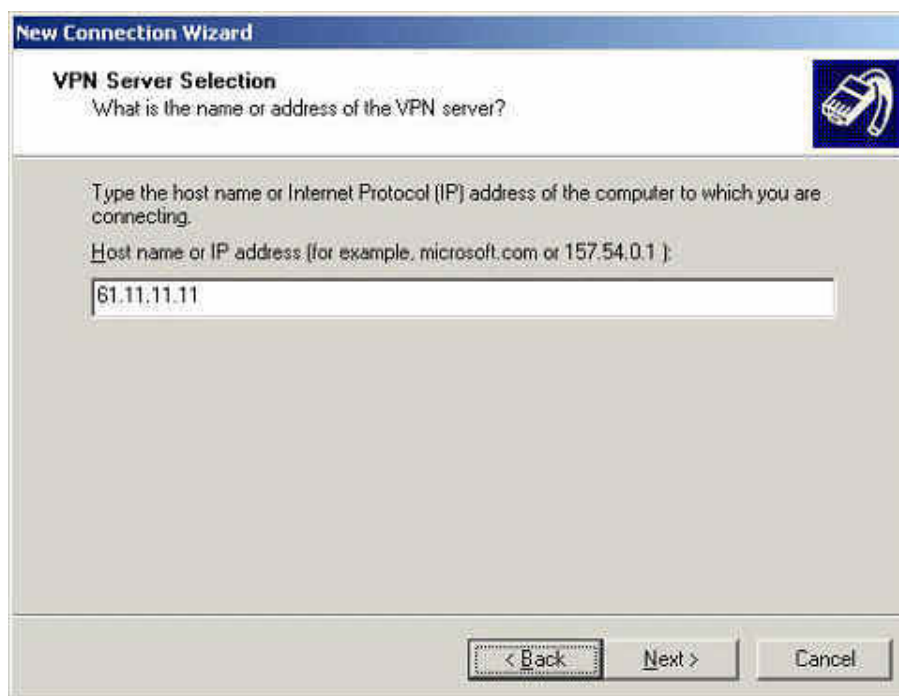
**Network Connection Wizard**

**Step6** In **Network Connection Wizard**, select **Connect to a private network through the Network**. Click **Next**.



**To connect to a private network through the Internet**

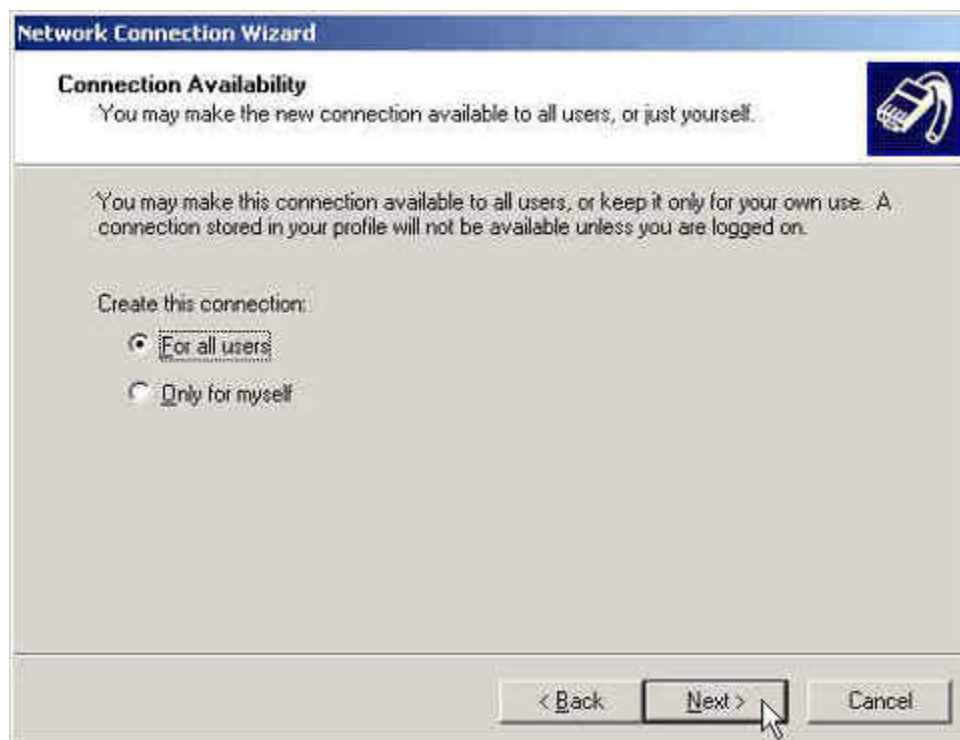
**Step7** In **New Connection Wizard**, enter the **IP Address**, and then click **Next**.



The screenshot shows the 'New Connection Wizard' window with the 'VPN Server Selection' tab selected. The window has a blue title bar and a small icon of a computer with a network cable in the top right corner. The main text asks 'What is the name or address of the VPN server?'. Below this, it says 'Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.' and 'Host name or IP address (for example, microsoft.com or 157.54.0.1):'. A text box contains the IP address '61.11.11.11'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Setup the Host name or IP address**

**Step8** In **Network Connection Wizard** → **Connection Availability**, select **For all users**. Click **Next**.



The screenshot shows the 'Network Connection Wizard' window with the 'Connection Availability' tab selected. The window has a blue title bar and a small icon of a computer with a network cable in the top right corner. The main text says 'You may make the new connection available to all users, or just yourself.' Below this, it says 'You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.' Under the heading 'Create this connection:', there are two radio button options: 'For all users' (which is selected) and 'Only for myself'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

**Setup the Connection Availability**



**Step9** In **New Connection Wizard**, enter the **Connection Name**, click **Finish**.



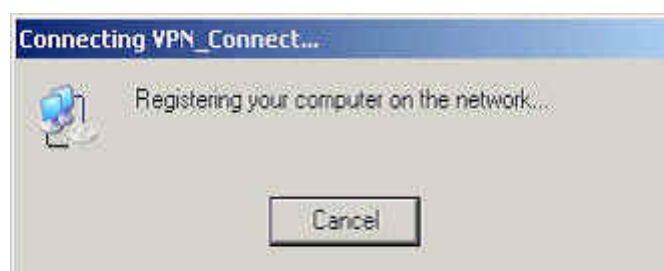
**Complete the New Connection Wizard**

**Step10** In **Connect Virtual Private Connection**, add the following settings :

- **User Name**, enter PPTP\_Connection.
- **Password**, enter 123456789.
- Select **Save Password**.
- Click **Connect**.
- It shows **Connecting to Virtual Private Connection** window.
- **Connection Complete**.



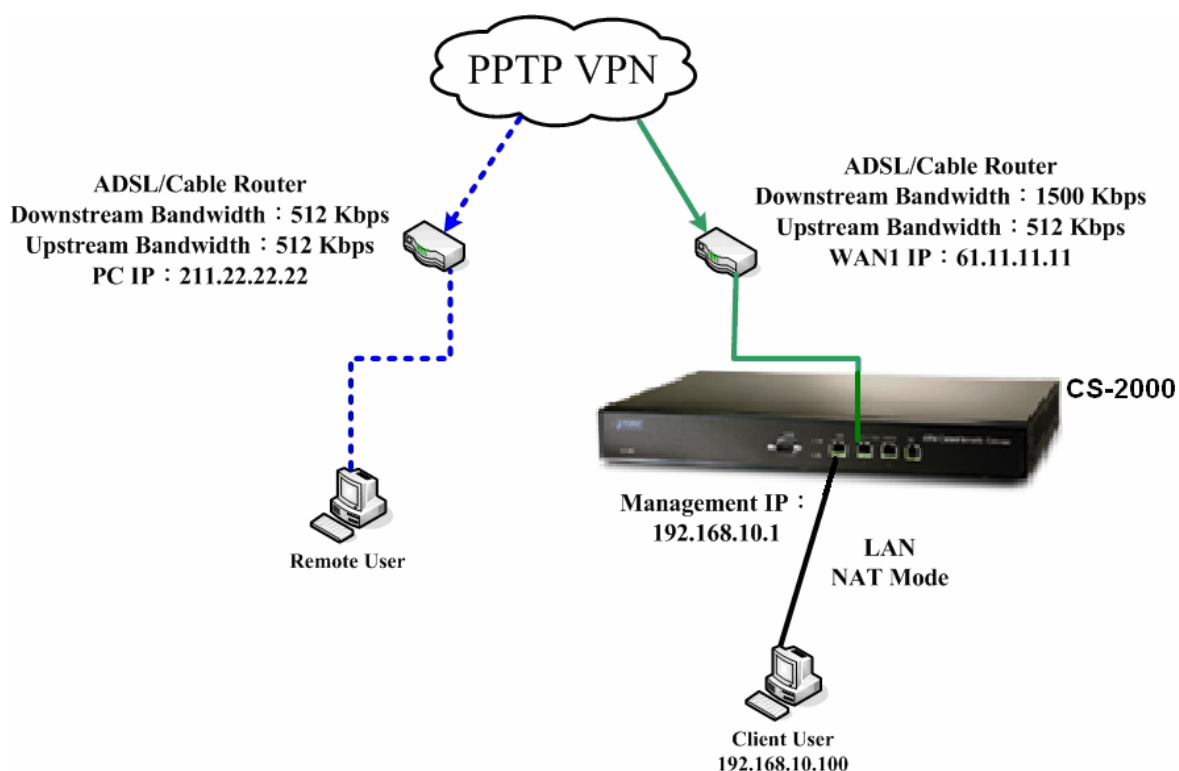
**Connect Virtual Private Connection**



**Creating the PPTP VPN Connection**



**Complete to setup the PPTP VPN connection**

**Step11** Complete to setup the PPTP VPN connection.

**The PPTP VPN deployment**

## Chapter 6: Policy

# Policy

The CS-2000 can detect every packet pass by the devices, and to valuate if the packets can fit the policy. When the packets can qualified by the policy, the CS-2000 will allow the packets to go through the policy. In other words, if the packets can not fit the policy, then it will be blocked.

The policy parameter included the source address , destination address , service , schedule , authenticatoin user , VPN trunk , action, WAN port , traffic log , statistics , IDP , content blocking , anti-virus , Qos , MAX.concurrent sessions , quota per session and quota per day . The MIS engineer can use these parameters to set the outgoing and incoming service in data transmission by policy management.



### How to use the Policy ?

The CS-2000 can divide the Policy into 6 function depends on the data packets in different source address . The MIS engineer can easy to set the policy of source IP , source port , destination IP and destination port by data packets .

1. **Outgoing** : The source IP is in LAN and the destination IP is in WAN .The MIS engineer can set the outgoing policy included the network packets and services.
2. **Incoming** : The source IP is in WAN and the destination IP is in LAN (For example, the IP mapped and virtual server) . The MIS engineer can set the incoming policy included the network packets and services.
3. **WAN To DMZ** : The source IP is in WAN and the destination IP is in DMZ (For example, the IP mapped and virtual server) .The MIS engineer can set the WAN To DMZ policy included the network packets and services.
4. **LAN To DMZ** : The source IP is in LAN and the destination IP is in DMZ. The MIS engineer can set the LAN To DMZ policy included the network packets and services.
5. **DMZ To LAN** : The source IP is in DMZ and the destination IP is in LAN. The MIS engineer can set the DMZ To LAN policy included the network packets and services.
6. **DMZ To WAN** : The source IP is in DMZ and the destination IP is in WAN. The MIS engineer can set the DMZ To WAN policy included the network packets and services.



All the packets need to be permitted by the policy in CS-2000. The MIS engineer has to set the fitness policy in CS-2000, in order to make the LAN, WAN and DMZ connection works.



The CS-2000's VPN function use the trunk technology by policy management, in order to monitor the packets through the data exchange.

## Policy

### Comment

- The description of policy.

### Source Address and Destination Address










- The active connection is the source IP and the passive connection is the destination IP .

### Service

- It represents the service item. The MIS engineer can select to use the system default setting or choose the **Policy Object → Service → Custom**, to use the custom setting.

### Option

- Use the icon to display as the option enabled.

Icon	Name	Definition
	Schedule	Enable the schedule auto run on certain time.
	Authentication User	Authentication is enabled.
	Traffic Log	Traffic Log is enabled.
	Statistics	Statistics is enabled.
	IDP	IDP is enabled.
	Content Blocking	Content Blocking is enabled.
	IM/P2P Blocking	IM/P2P blocking is enabled.
	Anti-Virus	Anti-Virus is enabled.
	Qos	Qos management is enabled.

### Schedule

- Set the schedule time by policy.

### Authentication User







- User has to pass the authentication, and then connect to the network by Policy.

### VPN Trunk


- To apply the IPSec and PPTP VPN into VPN trunk by policy.

### Action

- To assign the path when the data packets pass through the WAN1, WAN2, WAN3 or WAN4 in the CS-2000 or select to deny.

Icon	Name	Definition
	PERMIT ALL	To permit the qualified packets can go through WAN1, WAN2, and WAN3.
	PERMIT WAN1	To permit the qualified Packets can pass by WAN1.
	PERMIT WAN2	To permit the qualified Packets can pass by WAN2.
	PERMIT VPN Trunk	To permit the VPN Trunk qualified by Policy.
	DENY	To deny the Packets qualified by Policy.
	PAUSE	To stop the Policy.

### Traffic Log

- To record all the packets pass through the policy. The MIS engineer can click  to view.

### Statistics

- Use the graphic charts to display the flow statistics.

### IDP

- IDP can filter the packets which applied policy.

### Content Blocking

- To manage the packet contents which applied policy.

### IM/P2P Blocking

- Can limit the connection of IM and P2P.

### Anti-Virus

- To detect if the files has attached virus through the HTTP / WebMail, FTP and SMTP policy.

### Qos

- To setup the MAX.Bandwidth and G.Bandwidth by policy. ( The Bandwidth is shared by the user qualified by policy . )

### MAX. Concurrent Sessions Per IP

- To assign the maximum sessions for every IP by policy management. If the sessions are over the limit, then it will not build successfully.

### MAX. Concurrent Sessions

- To assign the maximum sessions by policy management. If the sessions are over the limit, then it will not build successfully.



If the value of **MAX. Concurrent Sessions per IP** has **over** the value of **MAX. Concurrent Sessions**, **then** the entire sessions pass through the policy will be limited by **MAX. Concurrent Sessions**.

#### Quota Per Session

- To allocate the max flow (KBytes) in every session by policy management.

#### Quota Per Day

- To allocate the max flow (MBytes/Sec) in everyday.

#### NAT

- When the packets pass through the LAN (DMZ) from external, the packets source IP will change into the CS-2000's LAN (DMZ) IP address.

#### Pause

- If it is necessary to modify the applied option in policy management (address, Qos....), then the MIS engineer can stop the policy and disable the  , to modify the contents.

#### Move

- To click the drop down menu and change the policy sorting. (The CS-2000 will check the passing packet depends on the policy sorting.)



**We will setup 6 Policy Application Environments.**

No.	Range	The Application Environment	Pages
<b>Example. 1</b>	<b>Outgoing</b>	To set the policy to monitor the internal user link to the network. (use traffic log , statistics and quota per session)	<b>272</b>
<b>Example. 2</b>	<b>Outgoing</b>	To deny the user to access the specify network resources. ( For example, the static IP and content blocking. )	<b>276</b>
<b>Example. 3</b>	<b>Outgoing</b>	To permit the authenticated user can access the network resources on specific time.	<b>283</b>
<b>Example. 4</b>	<b>Incoming</b>	The external user use the remote control software to control the internal PCs. ( For example , pcAnywhere )	<b>285</b>
<b>Example. 5</b>	<b>WAN To DMZ</b>	Sets a FTP server in the DMZ by NAT mode, and to limit the external user's downstream bandwidth, MAX. Concurrent sessions and quota per day.	<b>287</b>
<b>Example. 6</b>	<b>WAN To DMZ</b> <b>DMZ To WAN</b> <b>LAN To DMZ</b>	Sets a mail server in the DMZ by TRANSARENT mode, and to permit the internal and external user to send and receive e-mail.	<b>290</b>

\* DMZ = Demilitarized Zone

## Example 1

To set the policy to monitor the internal user link to the network. (Use traffic log, statistics and quota per session)

**Step1** In **Policy → Outgoing** , add the following settings :

- Click **New Entry**.
- Select **Traffic Log**.
- Select **Statistics**.
- In **Quota Per Session**, enter 10KBytes/Sec.
- Click **OK**.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="10"/> KBytes ( Range: 0 - 999999 )

**To Set the new policy**

**Step2** In **Policy → Outgoing**, to complete the traffic log, statistics and quota per session setting.

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

[New Entry](#)

Complete to set the policy

**Step3** In **Traffic Log Filtered** window, click to monitor packets through the policy.

- In **Traffic Log Filtered** window, click the drop down menu at the upper left, to select the Refresh frequency.
- In **Traffic Log Filtered**, click the IP address displayed in the window, then it will filter the IP packets record.
- If the MIS engineers want to monitor all the CS-2000's packets, click **Traffic Log → Traffic**.

http://210.66.155.77 - [ Traffic Log Filtered ] Source IP(211.75.117.114) List - Microsoft Internet Explorer

Refresh manually

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 5 10:02:17	211.75.117.114	210.66.155.77	TCP	1306 => 80	136 B	
Jul 5 10:01:43	211.75.117.114	210.66.155.77	TCP	1303 => 80	30 KB	
Jul 5 10:01:43	211.75.117.114	210.66.155.77	TCP	1304 => 80	20 KB	
Jul 5 10:01:25	211.75.117.114	210.66.155.77	TCP	1302 => 80	11 KB	
Jul 5 10:00:47	211.75.117.114	210.66.155.77	TCP	1300 => 80	11 KB	
Jul 5 10:00:46	211.75.117.114	210.66.155.77	TCP	1299 => 80	22 KB	
Jul 5 09:59:25	211.75.117.114	210.66.155.77	TCP	1295 => 80	38 KB	
Jul 5 09:59:25	211.75.117.114	210.66.155.77	TCP	1296 => 80	19 KB	
Jul 5 09:59:07	211.75.117.114	210.66.155.77	TCP	1292 => 80	5 KB	
Jul 5 09:59:05	211.75.117.114	210.66.155.77	TCP	1294 => 80	11 KB	
Jul 5 09:59:00	211.75.117.114	210.66.155.77	TCP	1293 => 80	12 KB	
Jul 5 09:58:57	211.75.117.114	210.66.155.77	TCP	1291 => 80	8 KB	
Jul 5 09:57:10	211.75.117.114	210.66.155.77	TCP	1290 => 80	15 KB	
Jul 5 09:57:10	211.75.117.114	210.66.155.77	TCP	1289 => 80	18 KB	
Jul 5 09:55:46	211.75.117.114	210.66.155.77	TCP	1288 => 80	39 KB	
Jul 5 09:55:46	211.75.117.114	210.66.155.77	TCP	1287 => 80	38 KB	
Jul 5 09:42:20	211.75.117.114	210.66.155.77	TCP	1277 => 80	5 KB	
Jul 5 09:42:18	211.75.117.114	210.66.155.77	TCP	1278 => 80	28 KB	
Jul 5 09:33:46	211.75.117.114	210.66.155.77	TCP	1275 => 80	169 KB	
Jul 5 09:33:46	211.75.117.114	210.66.155.77	TCP	1276 => 80	24 KB	

The Traffic Log Filtered window

1 / 2 [Next](#)

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 5 10:01:26	211.75.117.114	210.66.155.77	TCP	1303 => 80	1 KB	
Jul 5 10:01:26	211.75.117.114	210.66.155.77	TCP	1304 => 80	2 KB	
Jul 5 10:01:25	211.75.117.114	210.66.155.77	TCP	1302 => 80	11 KB	
Jul 5 10:00:47	211.75.117.114	210.66.155.77	TCP	1300 => 80	11 KB	
Jul 5 10:00:46	211.75.117.114	210.66.155.77	TCP	1299 => 80	22 KB	
Jul 5 09:59:25	211.75.117.114	210.66.155.77	TCP	1295 => 80	38 KB	
Jul 5 09:59:25	211.75.117.114	210.66.155.77	TCP	1296 => 80	19 KB	
Jul 5 09:59:21	201.141.13.205	210.66.155.77	ICMP	---	122 B	
Jul 5 09:59:20	201.141.13.205	210.66.155.77	ICMP	---	122 B	
Jul 5 09:59:11	218.86.105.204	210.66.155.77	ICMP	---	122 B	
Jul 5 09:59:10	218.86.105.204	210.66.155.77	ICMP	---	122 B	
Jul 5 09:59:07	211.75.117.114	210.66.155.77	TCP	1292 => 80	5 KB	
Jul 5 09:59:05	211.75.117.114	210.66.155.77	TCP	1294 => 80	11 KB	
Jul 5 09:59:00	211.75.117.114	210.66.155.77	TCP	1293 => 80	12 KB	
Jul 5 09:58:57	211.75.117.114	210.66.155.77	TCP	1291 => 80	8 KB	
Jul 5 09:57:10	211.75.117.114	210.66.155.77	TCP	1289 => 80	18 KB	
Jul 5 09:57:10	211.75.117.114	210.66.155.77	TCP	1290 => 80	15 KB	
Jul 5 09:55:46	211.75.117.114	210.66.155.77	TCP	1287 => 80	38 KB	
Jul 5 09:55:46	211.75.117.114	210.66.155.77	TCP	1288 => 80	39 KB	
Jul 5 09:42:20	211.75.117.114	210.66.155.77	TCP	1277 => 80	5 KB	

1 / 2 [Next](#)

### Traffic Log Web UI

**Step4** In **Monitor → Statistics → Policy**, it shows the traffic statistics through the policy.

[Bits/sec](#) [Bytes/sec](#) [Total](#)

Inside\_Any to Outside\_Any

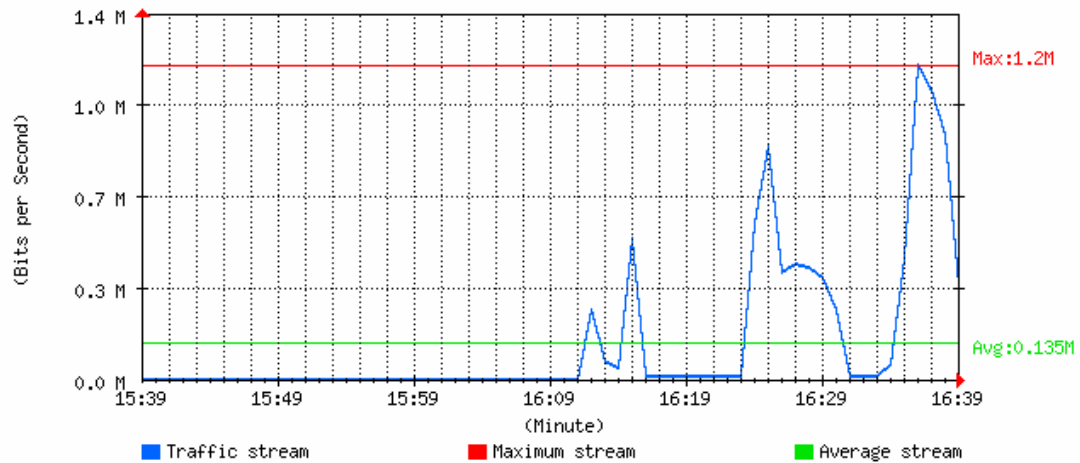
Service : AN

Action : perr

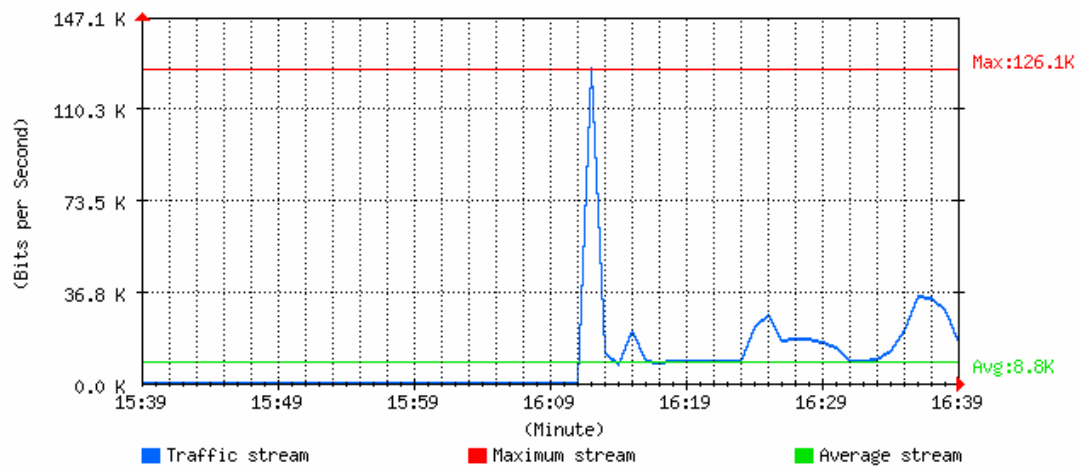
[Minute](#) [Hour](#) [Day](#) [Week](#) [Month](#) [Ye:](#)

Real-time: Down 382.8 KBits/sec Up 15.6 KBits/sec

#### Downstream



#### Upstream



#### Traffic statistics

## Example 2

To deny the user to access the specific network resources. ( For example, the static IP and content blocking.)

**Step1** In **Content Blocking** → **URL** → **Script** → **P2P** → **IM** → **Download** , add the following settings :

URL String▼	Configure
~yahoo	<a href="#">Modify</a> <a href="#">Remove</a>
~google	<a href="#">Modify</a> <a href="#">Remove</a>
*	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Content blocking setting

Script	
<input checked="" type="checkbox"/> Popup	<input checked="" type="checkbox"/> ActiveX
<input checked="" type="checkbox"/> Java	<input checked="" type="checkbox"/> Cookie
<a href="#">OK</a> <a href="#">Cancel</a>	

Script setting

**Download**

☒ All Types  
☐ Audio and Video Types

Extension

<input type="checkbox"/> .exe	<input type="checkbox"/> .zip	<input type="checkbox"/> .rar
<input type="checkbox"/> .iso	<input type="checkbox"/> .bin	<input type="checkbox"/> .rpm
<input type="checkbox"/> .doc	<input type="checkbox"/> .xl?	<input type="checkbox"/> .ppt
<input type="checkbox"/> .pdf	<input type="checkbox"/> .tgz	<input type="checkbox"/> .gz
<input type="checkbox"/> .bat	<input type="checkbox"/> .dll	<input type="checkbox"/> .hta
<input type="checkbox"/> .scr	<input type="checkbox"/> .vb?	<input type="checkbox"/> .wps
<input type="checkbox"/> .pif	<input type="checkbox"/> .msi	<input type="checkbox"/> .com
<input type="checkbox"/> .reg	<input type="checkbox"/> .mp3	<input type="checkbox"/> .mpeg
<input type="checkbox"/> .mpg	<input type="checkbox"/> .wma	<input type="checkbox"/> .rmvb
<input type="checkbox"/> .rm	<input type="checkbox"/> .avi	<input type="checkbox"/> .wmv
<input type="checkbox"/> .3gp	<input type="checkbox"/> .mov	<input type="checkbox"/> .asf
<input type="checkbox"/> .mp4	<input type="checkbox"/> .amv	<input type="checkbox"/> .ram

OK

Cancel

**Download blocking setting**

**Upload**

☒ All Types

Extension

<input type="checkbox"/> .exe	<input type="checkbox"/> .zip	<input type="checkbox"/> .rar
<input type="checkbox"/> .iso	<input type="checkbox"/> .bin	<input type="checkbox"/> .rpm
<input type="checkbox"/> .doc	<input type="checkbox"/> .xl?	<input type="checkbox"/> .ppt
<input type="checkbox"/> .pdf	<input type="checkbox"/> .tgz	<input type="checkbox"/> .gz
<input type="checkbox"/> .bat	<input type="checkbox"/> .dll	<input type="checkbox"/> .hta
<input type="checkbox"/> .scr	<input type="checkbox"/> .vb?	<input type="checkbox"/> .wps
<input type="checkbox"/> .pif	<input type="checkbox"/> .msi	<input type="checkbox"/> .com
<input type="checkbox"/> .reg	<input type="checkbox"/> .mp3	<input type="checkbox"/> .mpeg
<input type="checkbox"/> .mpg	<input type="checkbox"/> .wma	<input type="checkbox"/> .rmvb
<input type="checkbox"/> .rm	<input type="checkbox"/> .avi	<input type="checkbox"/> .wmv
<input type="checkbox"/> .3gp	<input type="checkbox"/> .mov	<input type="checkbox"/> .asf
<input type="checkbox"/> .mp4	<input type="checkbox"/> .amv	<input type="checkbox"/> .ram

OK

Cancel

**Upload blocking setting**

**Step2.** In **IM / P2P Blocking** → **New Entry**, add IM / P2P blocking setting.

**Add IM / P2P Blocking**

Name:  (Max. 16 characters)

**Instant Messaging**

☒ MSN ☒ Yahoo ☒ ICQ  
☒ QQ ☒ Skype ☒ Google Talk  
☒ Gadu-Gadu

**Peer-to-Peer Application**

☒ Edonkey ☒ Bit Torrent ☒ WinMX  
☒ Foxy ☒ KuGoo ☒ AppleJuice  
☒ AudioGalaxy ☒ DirectConnect ☒ iMesh  
☒ MUTE ☒ Thunder5 ☒ VNN Client  
☒ PPLive ☒ UltraSurf ☒ PPStream

**OK Cancel**

### Set IM / P2P blocking setting

**IM / P2P Signature Definitions**

Last updated on : 07/07/05 15:35:44 (Update signature definitions every one hour)  
 Current version: 1.2.8 (Signature definitions updated at 07/07/04 15:09:41 )  
 Update signature definitions immediately (Use TCP port: 80 and UDP port: 53) **Update NOW** [Test](#)

---

**IM / P2P Blocking**

Total entry : 1

Name▼	IM	P2P	Configure
IM_P2P_Blocking	MSN,Yahoo,ICQ...	Edonkey,Bit Torrent,WinMX...	<b>Modify Remove</b>

**New Entry**

### Complete IM /P2P blocking setting



1. The MIS engineer can limit the user to browse only specific web site through the content blocking by policy management.
2. The Script policy setting can deny the user to use the specific function, for example Java, cookie, market exchange web site.
3. The Peer to Peer application policy can limit the user to use the Peer to Peer application , for example , eDonkey , BT , WinMX , Foxy , KuGoo , AppleJuice , AudioGalaxy , DirectConnect , iMesh and MUTE.
4. The IM policy can limit the user to use the MSN messenger, Yahoo messenger, ICQ, QQ and Skype.
5. The Download policy can limit the user to access the specific Video and Audio files, extension files via HTTP and FTP.



**Step2** In **Address→WAN and WAN Group** , add the following settings :

Name▼	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
Remote_Server1	61.219.38.98/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Remote_Server2	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Set the WAN IP to block**

Name▼	Member	Configure
*CHINA_TELECOM	-----	<input type="button" value="In Use"/> <input type="button" value="Remove"/>
*CNC	-----	<input type="button" value="In Use"/> <input type="button" value="Remove"/>
WAN_Group	Remote_Server1, Remote_Server2	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

\*CHINA\_TELECOM AND \*CNC [Comments](#)

**Group the WAN**



The MIS engineer can customize to group the address and apply it to policy.

**Step3** In **Policy → Outgoing** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select **WAN\_Group** set in Step2. ( Use the IP to block . )
- **Action, WAN Port**, select **DENY ALL**.
- Click **OK**.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	WAN_Group ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input type="checkbox"/> PERMIT ALL <input checked="" type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Set the policy included blocking function**

**Step4** In **Policy → Outgoing** , add the following settings :

- Click **New Entry**.
- Select **Content Blocking**.
- Select **IM/P2P Blocking**.
- Click **OK**.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> URL <input checked="" type="checkbox"/> Script <input checked="" type="checkbox"/> Download <input checked="" type="checkbox"/> Upload
IM / P2P Blocking	IM_P2P_Blocking ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="0"/> KBytes ( Range: 0 - 999999 )

**To set the content blocking policy**

**Step5** Complete to set the policy to deny users access the network resources.

Source	Destination	Service	Action	Option								Configure			Move
Inside_Any	WAN_Group	ANY										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 
Inside_Any	Outside_Any	ANY										<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 2 

[New Entry](#)

**Complete to set the policy to deny users access the network resources**



The DENY action can block the packets correspond to the policy .The MIS engineer can move the policy to first priority, to limit users link to the specific IP address.

### Example 3

To permit the authenticated user can access the network resources on specific time.




**Step1** In **Schedule** , add the following settings :

Name▼	Configure
Working_Time	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Add new schedule

**Step2** In **Authentication → User and User Group**, add the following settings :

Name▼	Member	Radius	POP3	LDAP	Configure
auth_group	alex, eva, joe				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>
Radius	---				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>
POP3_auth	---				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>
LDAP_auth	---				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

[New Entry](#)

The authentication user group setting



The MIS engineer can use the group function in **Authentication** and **Service**, to easily set the policy.

**Step3** In **Policy → Outgoing** , add the following setting :

- Click **New Entry**.
- **Authentication User**, select laboratory.
- **Schedule**, select Working\_Time.
- Click **OK**.

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Working_Time
Authentication User	auth_group
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

#### To set the authentication and schedule policy

**Step4** Complete the setting to permit the user can access the network resources on specific time via the authentication.

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

[New Entry](#)

**Complete to set the authentication and schedule policy**

## Example 4

The external user use the remote control software to control the internal PCs. ( For example, PcAnywhere )

**Step1** To set up a LAN PC remote by the external PC, the server virtual IP is 192.168.1.2.

**Step2** In **Virtual Server** → **Server 1**, add the following settings :

Virtual Server Real IP

Total entry : 1

Service▼	WAN Port	Server Virtual IP	Configure
PC-Anywhere (5631-5632)	5631-5632	192.168.1.2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Set the virtual server

**Step3** In **Policy → Incoming** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select Virtual Server 1(203.67.31.11).
- **Service**, select PC-Anywhere (5631-5632).
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Virtual Server 1(203.67.31.11)
Service	PC-Anywhere(5631-5632)
Schedule	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	<input type="text" value="0"/> KBytes ( Range: 0 - 999999 )
Quota Per Day	<input type="text" value="0"/> MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

To set the policy of LAN PC remote by the external PC

**Step4** Complete to set the policy of LAN PC remote by the external PC.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(203.67.31.11)	PC-Anywhere(5631-5632)			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

Complete to set the policy of LAN PC remote by the external PC



## Example 5

Sets a FTP server in the DMZ by NAT mode, and to limit the external user's downstream bandwidth, MAX.concurrent sessions and quota per day.

**Step1** In **DMZ**, to set up a FTP server and the server virtual IP is 192.168.3.2. ( The DMZ interface address is 192.168.3.1/24 )

**Step2** In **Virtual Server → Server 1** , add the following settings :

Virtual Server Real IP

Total entry : 1





Service▼	WAN Port	Server Virtual IP	Configure
FTP (21)	21	192.168.3.2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Set the virtual server correspond to FTP server



In **Policy → Incoming** or **WAN To DMZ**, it is strongly recommended not to select the **Service** to be **ANY**, to avoid the internal PC be attacked.

**Step3** In **Qos** , add the following settings :

Name▼	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP_QoS	1	G.Bandwidth = 1024 Kbps M.Bandwidth = 2048 Kbps	G.Bandwidth = 128 Kbps M.Bandwidth = 256 Kbps	High	 
	2	G.Bandwidth = 256 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 128 Kbps M.Bandwidth = 512 Kbps		
	3	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		
mail	1	G.Bandwidth = 512 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 56 Kbps M.Bandwidth = 256 Kbps	Middle	 
	2	G.Bandwidth = 512 Kbps M.Bandwidth = 1024 Kbps	G.Bandwidth = 256 Kbps M.Bandwidth = 512 Kbps		
	3	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		


**Set the QoS****Step4** In **Policy → WAN To DMZ** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select Virtual Server 1(61.11.11.12).
- **Service**, select FTP (21).
- **Qos**, select FTP\_QoS .
- **MAX. Concurrent Sessions** enter 100.
- **Quota Per Day**, enter 100000 Mbytes.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any ▼
Destination Address	Virtual Server 2(61.11.11.12) ▼
Service	FTP(21) ▼
Schedule	None ▼
VPN Trunk	None ▼
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	FTP_QoS ▼
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	100 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	100000 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable



**Add new policy**

**Step5** Limit users access the DMZ server services and network resources.

Source	Destination	Service	Action	Option			Configure			Move
Outside_Any	Virtual Server 2(61.11.11.12)	FTP(21)					<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 

[New Entry](#)

Complete to set the policy

## Example 6

Sets a mail server in the DMZ by TRANSARENT mode, and to permit the internal and external user to send and receive e-mail.

**Step1** In **DMZ**, to set a mail server and the IP is 61.11.11.12. The DNS set to correspond to the external DNS server.

**Step2** In **Address → DMZ** , add the following settings :

Name▼	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Mail_Server	61.11.11.12/255.255.255.255		Modify Remove

New Entry

To set the mail server correspond to the IP address

**Step3** In **Service → Group** , add the following settings :

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

New Entry

To set up the service group included the POP3, SMTP and DNS

**Step4** In **Policy → WAN To DMZ** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select Mail\_Server.
- **Service**, select Mail\_Service.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any
Destination Address	Mail_Server
Service	Mail_Service
Schedule	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

To set the WAN To DMZ mail service policy

**Step5** Complete to set the WAN To DMZ mail service policy.

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

Complete to set the WAN To DMZ mail service policy

**Step6** In **Policy → LAN To DMZ** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select Mail\_Server.
- **Service**, select Mail\_Service.
- Click **OK**

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Mail_Server ▾
Service	Mail_Service ▾
Schedule	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
Quota Per Session	0 KBytes ( Range: 0 - 999999 )
Quota Per Day	0 MBytes ( Range: 0 - 999999 )
NAT	<input type="checkbox"/> Enable

To set the LAN To DMZ mail service policy

**Step7** Complete to set the LAN To DMZ mail service policy.

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	Mail_Service			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

Complete to set the LAN To DMZ mail service policy

**Step8** In **Policy → DMZ To WAN** , add the following settings :

- Click **New Entry**.
- **Destination Address**, select Mail\_Server.
- **Service**, select Mail\_Service.
- Click **OK**

Add New Policy	
Source Address	Mail_Server ▼
Destination Address	Outside_Any ▼
Service	Mail_Service ▼
Schedule	None ▼
Authentication User	None ▼
VPN Trunk	None ▼
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▼
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▼
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**To set the DMZ To WAN Mail service policy**

**Step9** Complete to set the DMZ To WAN mail service policy.

Source	Destination	Service	Action	Option								Configure			Move
Mail_Server	Outside_Any	Mail_Service													To 1 ▼



**Complete to set the DMZ To WAN mail service policy**

## Chapter 7: Mail Security

### 7.1 Configure

# Configure

The so called mail configure is the CS-2000's mail process standard. In this Chapter, we will define it to be the mail setting, mail relay, mail account and mail notice.



Only set the mail relay function as scanning the mails in internal mail server through the CS-2000's anti-spam and anti-virus process.



### 7.1.1 Setting

#### Scanned Mail Setting

- The MIS engineer can set the scanned spam and virus mail size separately, and let the CS-2000 to self-identify which mail to scan.

#### Unscanned Mail Setting

- It is focus on the mail which is over the scanning standard. The MIS engineer can select to add the unscanned mail message to the subject line.

#### Mail Notice use the IP (or domain name) for retrieving spam / virus mails

- The MIS engineer can set the internal mail server to send / retrieve spam / virus mails to the external mail server by use the LAN, DMZ or domain name mapped to the WAN port, in order to send the mail notice. In the Mail Notice, recipients can select to use the mail transferred IP or domain name for retrieving spam / virus mails.

#### Mail Notice Message Setting

- The MIS engineer can customize the mail notice subject and attached messages. If he does not do any modification, then system will use the default value to send the mail notice.

### Storage lifetime of spam / virus mails in the quarantine

- The MIS engineer can assign the storage lifetime of spam/virus mails in the quarantine, and also delete these spam/virus mails on the expire date.

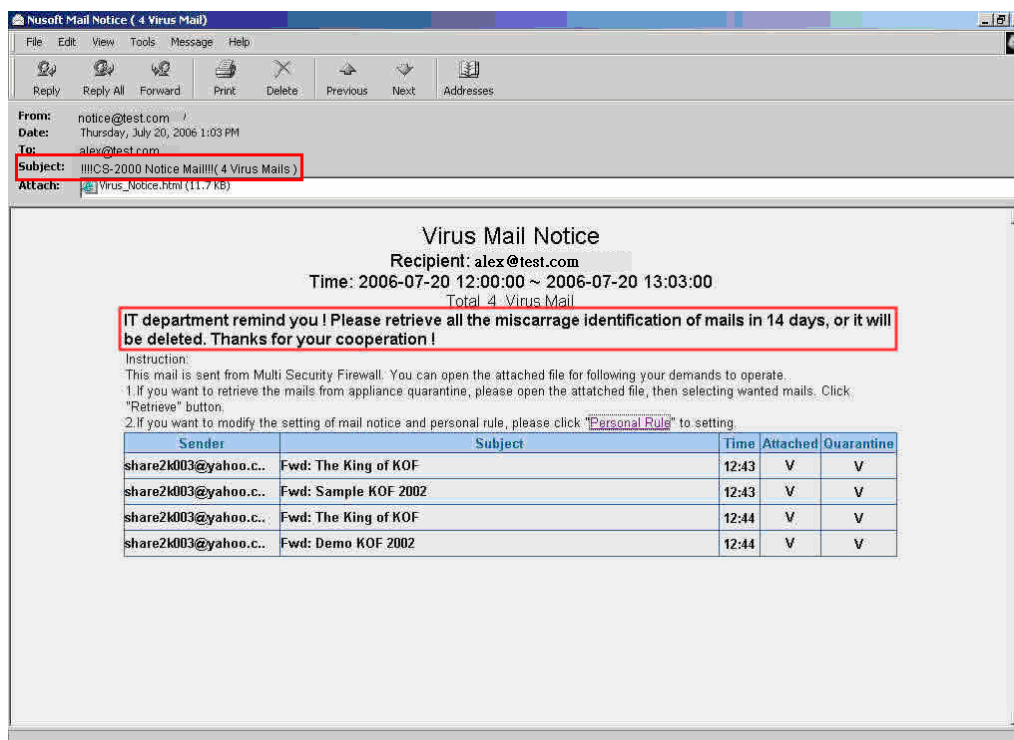
### Login Authentication of Personal Rule

- The MIS engineer can modify the login port and select the login authentication method.
- Add the following settings :
  1. **The scanned spam mail size is less than**, enter 512Kbytes.
  2. **The scanned virus mail size is less than**, enter 512Kbytes.
  3. **Unscanned Mail Setting**, select Add the message to the subject line ---Unscanned---.
  4. **Mail Notice use the IP ( or domain name ) for retrieving spam / virus mails** , enter 61.11.11.11 ( WAN1 IP ) .
  5. Enter the **Mail Notice Subject** and **Message of notice mail content**.
  6. **Storage lifetime of spam / virus mails in the quarantine**, enter 14 Days.
  7. Enter 89 in **login port**.
  8. Enable **POP3** and **Local Database** in **login authentication**.
  9. Click **OK**.

<b>Scanned Mail Setting</b>	
The scanned spam mail size is less than	512 KBytes ( Range: 10 - 5120 )
The scanned virus mail size is less than	1024 KBytes ( Range: 10 - 5120 )
<b>Unscanned Mail Setting</b>	
<input checked="" type="checkbox"/> Add the message to the subject line	---CS-200_Unscanned--- (Max. 255 characters)
<b>Mail Notice use the IP (or domain name) for retrieving spam / virus mails</b>	
IP Address (or Domain Name)	203.67.31.11 <a href="#">Assist</a> (WAN1 IP recommended)
<b>Mail Notice Message Setting</b>	
Mail Notice Subject	!!! CS-2000 Notice mail !!!
Message of notice mail content	
This is CS-2000 Notice mail !!! You have 7 Days for retrieve the Spam mails!!!!	
<b>Storage lifetime of spam / virus mails in the quarantine</b>	
Storage lifetime	14 Days ( Range: 1 - 365 )
<input type="checkbox"/> Disable multi-retrieve of quarantined mails	
<b>Login Authentication of Personal Rule</b>	
Login Port	89 ( Range : 1-65535 )
<input checked="" type="checkbox"/> Enable personal rule	
Login Authentication :	
<input checked="" type="checkbox"/> POP3	
<input checked="" type="checkbox"/> Local Database	
<div>OK</div> <div>Cancel</div>	

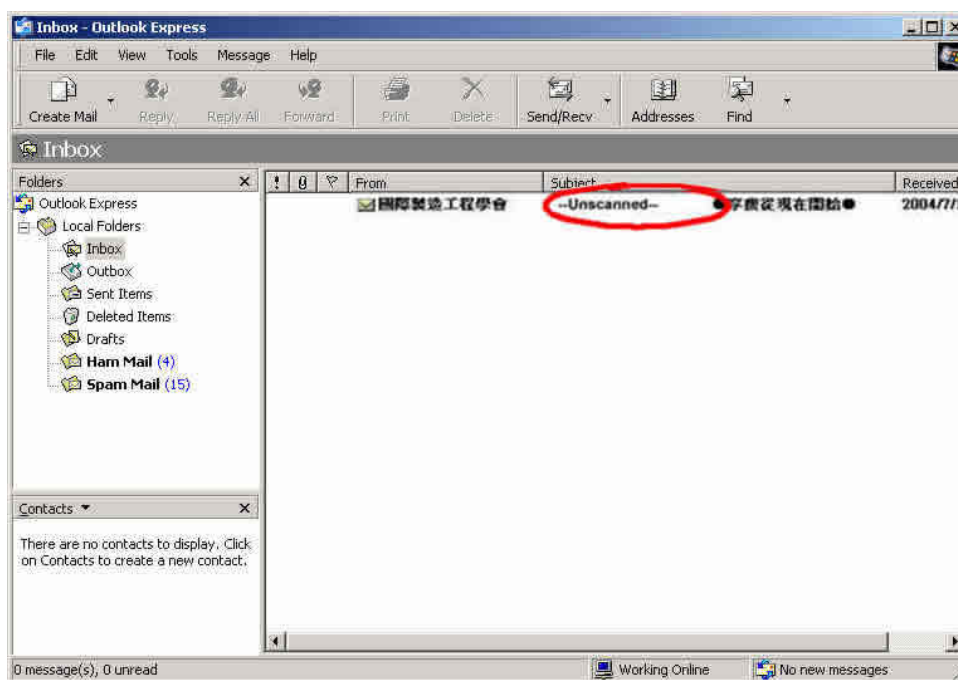
### The Mail Security Configuration

- When received the notice mail, it shows the customized mail subject and notice contents.



Notice mail include the customized mail subject and contents

- When the user received the unscanned mail, the system will add the message to the subject line.



To display the unscanned mail message to the subject line

## 7.1.2 Mail Relay

### Example 1

We use the CS-2000 to be the Gateway ( To set the mail server in DMZ , and use the Transparent mode )

#### The Deployment

WAN1 IP is 61.11.11.11

Mail Server IP is 61.11.11.12

To mapped the DNS domain name (test.com) applied from the ISP , to the DNS server IP ( To set the MX record correspond to the mail server IP )

When the external sender want to send the mail to recipient's account via the test.com mail Server , add the mail relay setting :

**Step1** In **Configure → Mail Relay** , add the following settings :

- Select **Domain Name of Internal Mail Server**.
- **Domain Name of Mail Server**, enter the applied domain name.
- **IP Address of Mail Server**, enter the IP address mapped to mail server domain name.
- Complete the mail relay setting. When the external user send the mail to the internal mail server which must be defined in the domain setting. So that the CS-2000 can filter and send the mails to assigned mail server.

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

Modify Domain Name	
Domain Name of Mail Server	test.com (Max. 200 characters, ex: mail.my_domain.com)
IP Address of Mail Server	61.11.11.12 ( ex: 61.217.22.30 )
<input type="checkbox"/> Enable LDAP <span style="color: red;">Test</span>	
LDAP Server IP	( ex: 172.16.1.2 )
LDAP Server Port	( Range: 1 - 65535, ex: 389 )
LDAP Search Base	(Max. 255 characters, ex: dc=mail,dc=my_domain,dc=com)
User Name	(Max. 63 characters, ex: username)
Password	(Max. 63 characters, ex: 5d2#k...)

#### Mail relay setting



In **Mail Relay → Domain Name of internal Mail Server**, to **Enable LDAP** and the CS-2000 can get the permitted relay account information from LDAP server every 30 minutes, in order to valuate the mail relay necessity. ( When the **LDAP** is disable , the CS-2000 will confirm if the mail account exist in mail server , to valuate the mail relay necessity. )



After completed the LDAP server settings, Click **LDAP test**, to detect if the CS-2000 can link to LDAP server.



When enabled the SMTP authentication in internal mail server , if the internal user want to use the legal mail account to send mail to external users , the MIS engineer does not need to select **Mail Relay → Allowed External IP of Mail Relay**.

## **Example 2**

**To put the CS-2000 between the Company's original gateway and mail server. (To set the mail server in DMZ, and use the Transparent mode.)**

### **The Deployment**

**The Company's original Gateway is 172.1.1.0/16 (LAN segment)**

**WAN IP is 61.11.11.11**

**CS-2000's WAN1 IP is 172.16.1.12**

**Mail Server IP is 172.16.1.13**

The DNS domain name ( test.com ) applied from the ISP , which correspond to the DNS server IP ( To set the MX record correspond to the mail server IP ) .

When the LAN ( 172.16.1.0/16 ) user want to use the sender account to send mails to external recipient account on external mail server via the test.com mail server, add the following mail relay settings :

**Step1** In **Configure→ Mail Relay** , add the first setting :

- Select **Domain Name of Internal Mail Server**.
- **Domain Name of Mail Server**, enter the applied domain name.
- **IP Address of Mail Server**, enter the IP address which the domain name of mail server correspond to.

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

Modify Domain Name	
Domain Name of Mail Server	test.com (Max. 200 characters, ex: mail.my_domain.com)
IP Address of Mail Server	172.16.1.13 ( ex: 61.217.22.30 )
<input type="checkbox"/> Enable LDAP <span style="color: red;">Test</span>	
LDAP Server IP	( ex: 172.16.1.2 )
LDAP Server Port	( Range: 1 - 65535, ex: 389 )
LDAP Search Base	(Max. 255 characters, ex: dc=mail,dc=my_domain,dc=com)
User Name	(Max. 63 characters, ex: username)
Password	(Max. 63 characters, ex: 5d2#k...)

### The first mail relay setting

**Step2** In **Configure → Mail Relay** , add the second mail relay setting :

- Select **Allowed External IP of Mail Relay**.
- **IP Address**, enter the external sender IP address.
- Enter the **Netmask**.
- Complete the mail relay setting.

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

Add IP Address	
IP Address	61.11.11.11 ( ex: 202.24.193.138 )
Netmask	255.255.255.255 ( ex: 255.255.255.248 )

### The second mail relay setting



### Example 3

The headquarter company use CS-2000 to be the gateway (To set the mail server in DMZ, and use Transparent mode), in order to let the employees can send mails through the mail server.

#### The Deployment

**CS-2000's WAN1 IP is 61.11.11.11**

**Mail Server IP is 61.11.11.12**

**Branch office firewall WAN IP is 211.22.22.22**

The DNS domain name ( test.com ) applied from the ISP , correspond to the DNS server IP ( To set the MX record correspond to the mail server IP ) .

When the branch office user use the sender account to send mails to external recipient account on external mail server via the test.com mail server, add the following mail relay settings :

**Step1** In **Configure → Mail Relay** , add the first setting :

- Select **Domain Name of Internal Mail Server**.
- **Domain Name of Mail Server**, enter the applied domain name.
- **IP Address of Mail Server**, enter the IP address which the domain name of mail server correspond to.

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

Modify Domain Name	
Domain Name of Mail Server	test.com (Max. 200 characters, ex: mail.my_domain.com)
IP Address of Mail Server	61.11.11.12 ( ex: 61.217.22.30 )
<input type="checkbox"/> Enable LDAP <a href="#">Test</a>	
LDAP Server IP	( ex: 172.16.1.2 )
LDAP Server Port	( Range: 1 - 65535, ex: 389 )
LDAP Search Base	(Max. 255 characters, ex: dc=mail,dc=my_domain,dc=com)
User Name	(Max. 63 characters, ex: username)
Password	(Max. 63 characters, ex: 5d2#k...)

#### The first mail relay setting

**Step2** In **Configure → Mail Relay** , add the second setting :

- Select **Allowed External IP of Mail Relay**.
- **IP Address**, enter the external sender IP address.
- Enter the **Netmask**.
- Complete the mail relay setting.

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

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

#### The second mail relay setting

### 7.1.3 Mail Account

Use the CS-2000's mail account, to allow or deny mails from the internal mail server.

**Step1** In **Configure → Mail Relay** , add the following settings :

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
myalexweb.dyndns.tv ( 61.62.236.14 )	<a href="#">Modify</a> <a href="#">Remove</a>
61.64.127.16 / 255.255.255.255	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

The mail relay setting

**Step2** In **Configure → Mail Account** , it shows the domain name of internal mail server :

- Click **Modify**, it shows the **Mail Account→ Scanned Account** list, which is confirmed by the internal mail server.

Domain Name of Internal Mail Server	Account
myalexweb.dyndns.tv	<a href="#">Modify</a>

The domain name of internal mail server

Mail Account

Export mail account to Client [Download](#)

Import address book from Client  [Browse](#) [Assist](#)

Add new mail account : [New Entry](#)

Remove all of Unscanned Account : [Remove](#)

1 / 1

[Select All](#)
[Invert](#)

<--- Unscanned / Invalid Account --->

1 / 1

[Select All](#)
[Invert](#)

<--- Scanned Account --->  
admin@myalexweb.dyndns.tv  
alex@myalexweb.dyndns.tv  
eva@myalexweb.dyndns.tv  
joe@myalexweb.dyndns.tv  
notice@myalexweb.dyndns.tv

[Remove](#)

[Add](#)

☒ Add new accounts to the scanned account list automatically, the unscanned accounts' mails would be rejected.

☐ Only the scanned accounts' mails can be received and filtered. Other mails would be rejected.

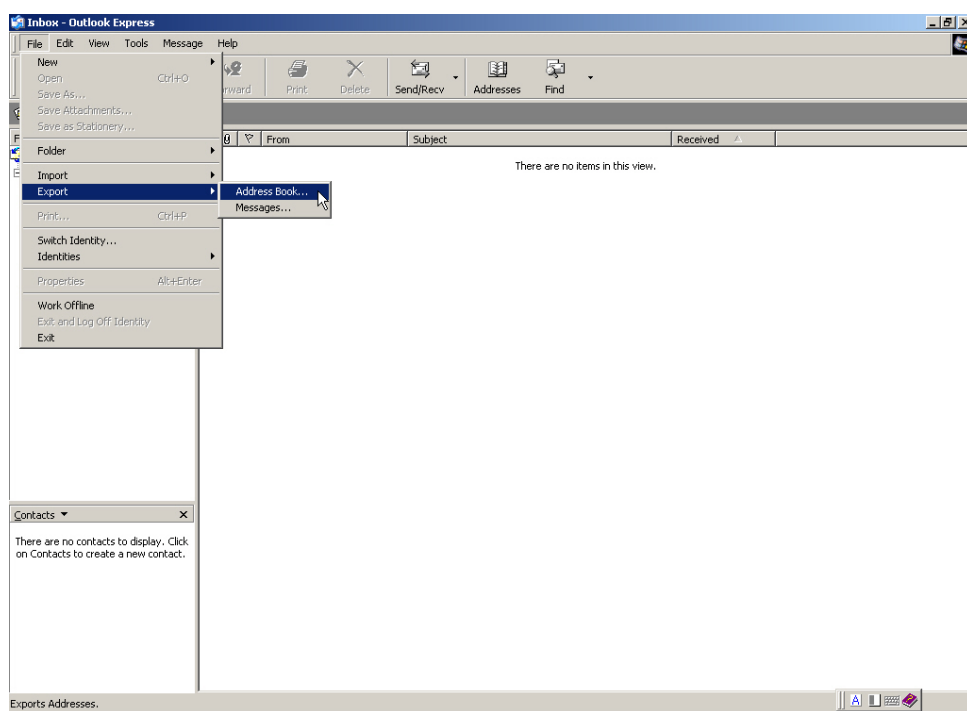
☐ Only the scanned accounts' mails can be filtered. Other mails would send to mail server directly and not be filtered.

The mail account list

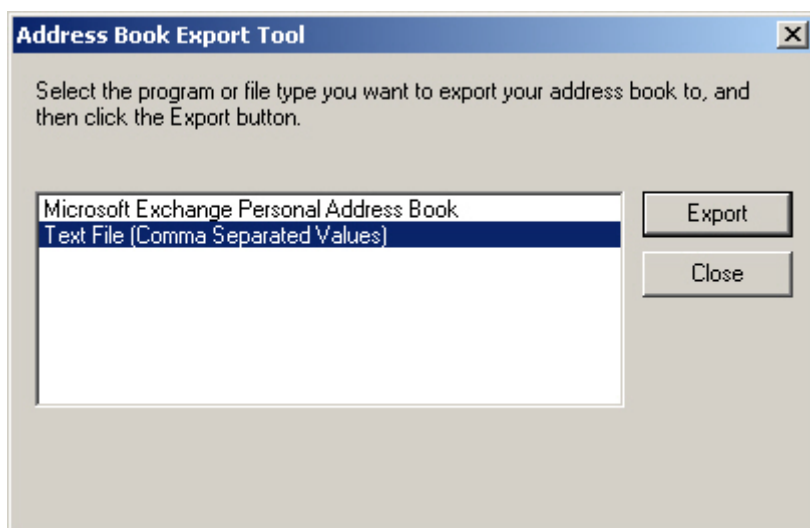


After complete to set the **Mail Relay** settings, the MIS engineer can add the legal Mail account into the **Scanned Account** list by importing address book, the MIS engineer can select to use the function **to import address book from Client** in **Mail Account** . ( For example , use the Outlook Express ) :

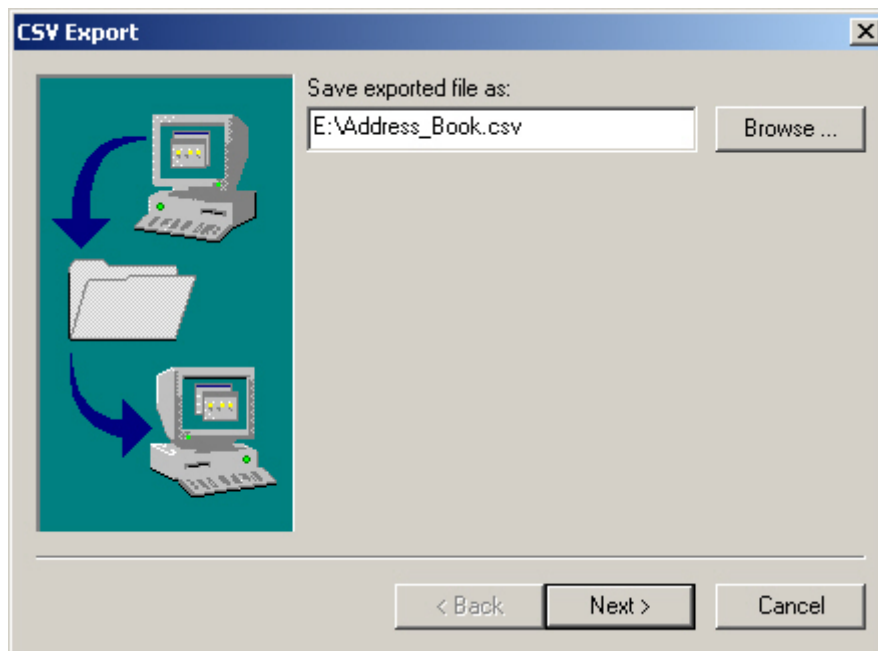
1. Select **Only the scanned accounts' mails can be received and filtered. Other mails would be rejected.**
2. Running outlook express , click **File → Export → Address Book.**
  - a. In **Address Book Export Tool**, select **Text File (Comma Separated Values)**, click **Export**.
  - b. In **Save exported files as** window, enter the exported address book file name and saved path, click **Next**.
  - c. In **Select the fields MIS engineer wish to export**, only select **E-mail Address**, and click **Finish**.
  - d. In **Address Book** window, click **OK**.
  - e. In **Address Book Export Tool** window, click **Close**.
3. In **Import address book from Client** column, enter the address book file saved path, and click **OK**.



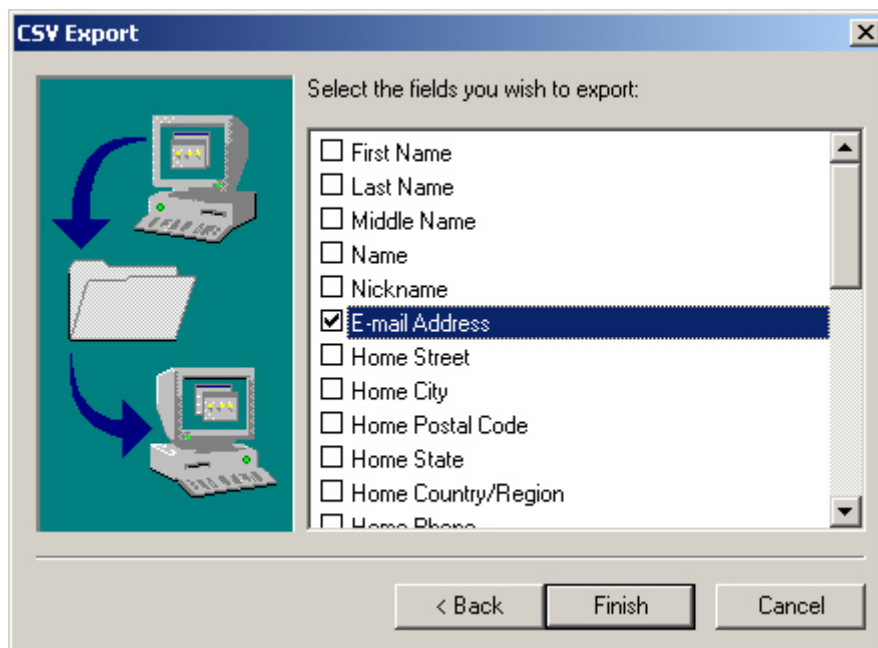
### Export the Address Book



### The Address Book Export Tool



Save exported files



Select the fields MIS engineer wish to export



Complete to export the address book

 A screenshot of the "Mail Account" management interface. At the top, there's a "Download" button for "Export mail account to Client". Below that, an "Import address book from Client" section shows a file path "E:\Address\_Book.csv" with "Browse" and "Assist" buttons. Further down, there are buttons for "New Entry" (Add new mail account) and "Remove" (Remove all of Unscanned Account). The main area is divided into two panes: "Unscanned / Invalid Account" on the left and "Scanned Account" on the right. Each pane has "Select All" and "Invert" buttons. Between the panes are "Remove" and "Add" buttons. At the bottom, there are three radio button options for account management:
 

- ☒ Add new accounts to the scanned account list automatically, the unscanned accounts' mails would be rejected.
- ☐ Only the scanned accounts' mails can be received and filtered. Other mails would be rejected.
- ☐ Only the scanned accounts' mails can be filtered. Other mails would send to mail server directly and not be filtered.

Import address book from client

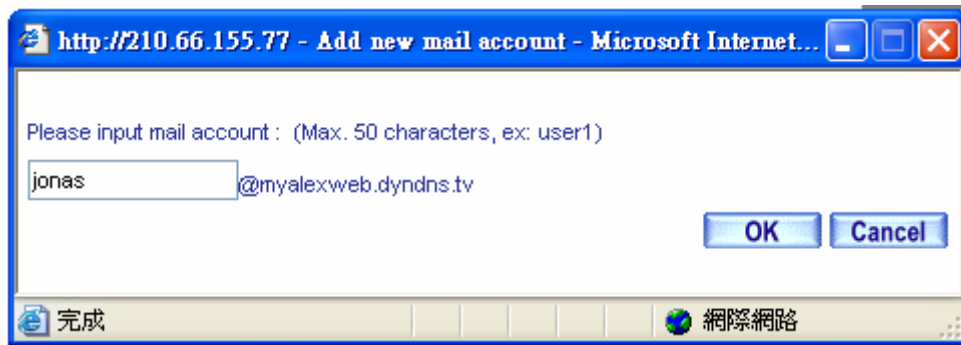


The MIS engineer can use **Mail Account → Add new accounts to the scanned account list automatically, the unscanned accounts' mails would be rejected**, in order to result the scanned account list. On the other hand, the MIS engineer can store or clean the legal mail account in internal mail server by export the mail account. The CS-2000 can re-export the list when the **Scanned Account** is missing.

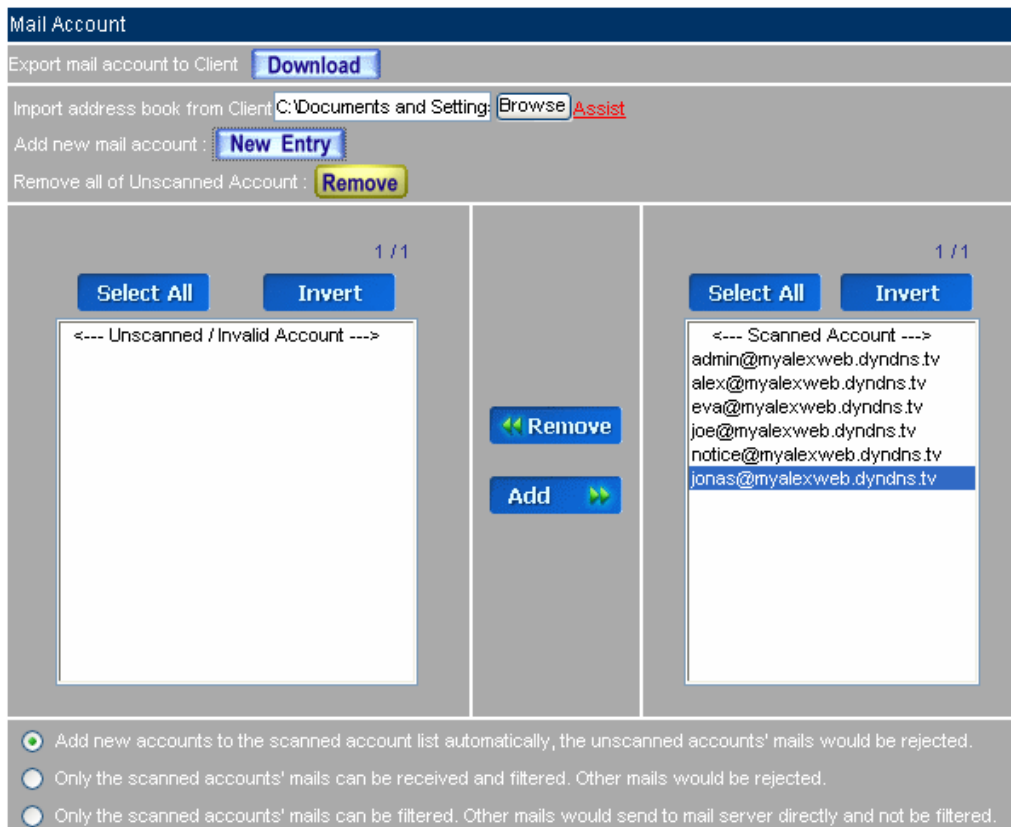


**Step3** In **Mail Account** , add new mail account :

- **Add new mail account, click New Entry.**
- In **Add new mail account**, enter the new mail account.
- Click **OK**.
- In **Mail Account** window, click **OK** again.



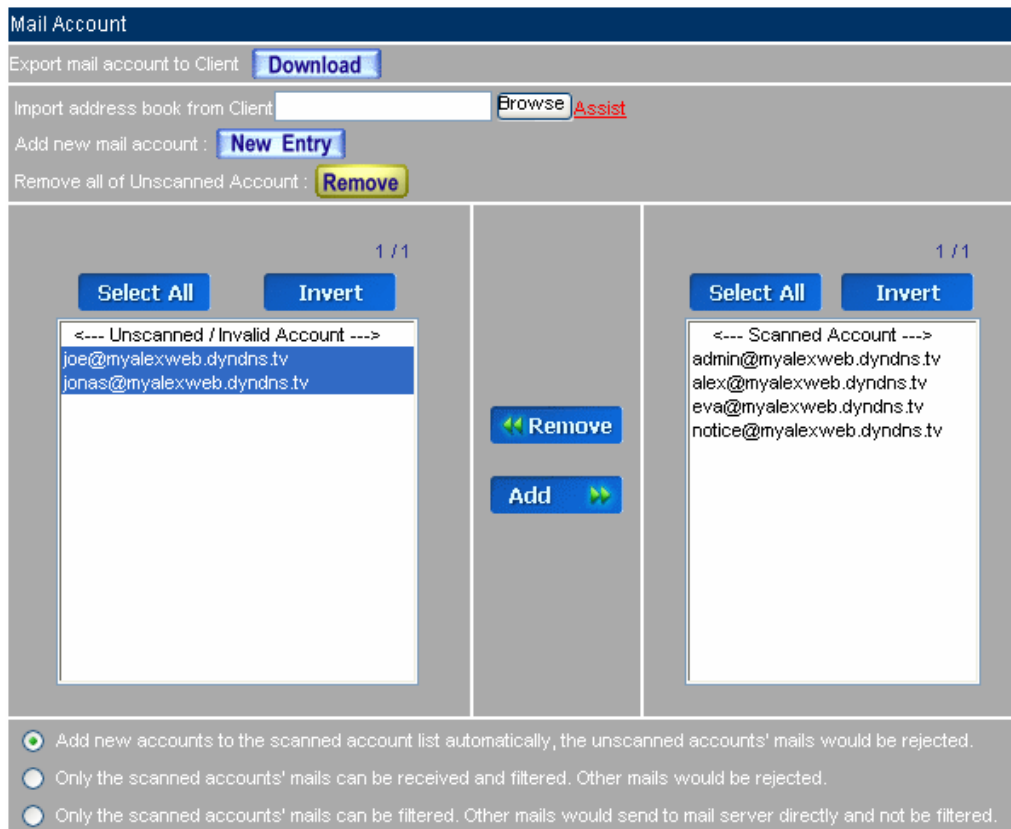
**Add new mail account**



**Complete to add new mail account**

**Step4** To set which recipient account is not allowed receiving mails in internal mail server.

- In **Scanned Account**, select the mail account which is not allowed to receive the mail.
- Click **Remove**, to remove the selected mail accounts to **Unscanned / Invalid Account** list.
- In **Mail Account**, click **OK**.



Mail Account

Export mail account to Client [Download](#)

Import address book from Client  [Browse](#) [Assist](#)

Add new mail account : [New Entry](#)

Remove all of Unscanned Account : [Remove](#)

1 / 1

[Select All](#) [Invert](#)

<--- Unscanned / Invalid Account --->

- joe@myalexweb.dyndns.tv
- jonas@myalexweb.dyndns.tv

[Remove](#)

[Add](#)

1 / 1

[Select All](#) [Invert](#)

<--- Scanned Account --->

- admin@myalexweb.dyndns.tv
- alex@myalexweb.dyndns.tv
- eva@myalexweb.dyndns.tv
- notice@myalexweb.dyndns.tv

☒ Add new accounts to the scanned account list automatically, the unscanned accounts' mails would be rejected.
 ☐ Only the scanned accounts' mails can be received and filtered. Other mails would be rejected.
 ☐ Only the scanned accounts' mails can be filtered. Other mails would send to mail server directly and not be filtered.

**To set which recipient account is not allowed to receive mails in internal mail server**

**Step5** In **Mail Account** → **Scanned Account**, the CS-2000 will confirm if the recipient mail account is legal mail account, and then send the external sender's mail to internal mail server.



The CS-2000 will confirm if the recipient's mail account (receive mails sent from the external sender) is fit to the **Mail Account** list by the internal mail server's confirmation.

1. When the recipient's mail account fit to **Scanned Account** , the CS-2000 will send the mails to internal mail server .
2. When the recipient's mail account fit to **Unscanned / Invalid Account**, the CS-2000 will delete these mails.



The CS-2000 will confirm the recipient's **Mail Account** to be the **Scanned Account** by the internal mail server and add the recipient account into scanned account when selecting **Add new accounts to the scanned account list automatically** , the unscanned accounts' mails would be rejected .



In **Mail Account → Scanned Account** , if the mail account is belong to the illegal account , then **Remove** it to the **Unscanned / Invalid Account** , and click **Remove all of Unscanned Account → Remove** .



When select **Only the scanned accounts' mails can be filtered** .Other mails would send to mail server **directly without filtering** .The CS-2000 will directly send the **Unscanned / Invalid Account** to Internal Mail Server.



In **Mail Account → Unscanned / Invalid Account** list, the user can **Remove** the **Scanned Account** to be the **Unscanned / Invalid Account**.

### 7.1.4 Mail Notice

#### Example 1

Use the CS-2000's mail notice, to send the spam mail (virus) notification to recipient. In other words, the recipient can select the needed mails from the list. (For example, use the Outlook Express)

**Step1** In **Configure → Mail Relay** , add the following settings :

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
myalexweb.dyndns.tv ( 61.62.236.14 )	<a href="#">Modify</a> <a href="#">Remove</a>
61.64.127.16 / 255.255.255.255	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

The mail relay setting

**Step2** In **Configure → Mail Notice** , it shows the domain name of internal mail server :

- Click **Modify**, the mail account will displayed in mail notice selectable list.

Domain Name of Internal Mail Server	Account
myalexweb.dyndns.tv	<a href="#">Modify</a>

The domain name of internal mail server

**Mail Notice (Internal mail server only)**

☐ Enable Notice : Both ▼

☐ Send Mail Notice on weekend

1st Time : 10:00 ▼ 4th Time : Disable ▼ Mail Type : Attached ▼ [Notice Now](#) [Help](#)

2nd Time : Disable ▼ 5th Time : Disable ▼ Sender : notice@myalexweb.dyndns.tv

3rd Time : Disable ▼ 6th Time : Disable ▼ (Max. 99 characters, ex: user@mydomain.com)

[Select All](#) [Invert](#)

admin@myalexweb.dyndns.tv  
alex@myalexweb.dyndns.tv  
eva@myalexweb.dyndns.tv  
joe@myalexweb.dyndns.tv  
notice@myalexweb.dyndns.tv

[Remove](#)

[Add](#)

[Select All](#) [Invert](#)

<--- Selected Account --->

☒ Add Notice Account Automatically

The mail notice list

**Step3** In **Configure → Mail Notice**, add the following settings :

- Select **Enable Notice → Both**.
- Select **Send Mail Notice on weekend**.
- **1 st**, select 00:00.
- **2 nd**,select 04:00.
- **3 rd**, select 08:00.
- **4 th**, select 12:00.
- **5 th**, select 16:00.
- **6 th**, select 20:00.
- **Mail Type**, select HTML.
- **Sender** , enter notice@test.com.tw ( the default setting ) .
- Select the selectable mail account to be noticed, click **Add** to move to the **Selected Account**.
- Select **Add Notice Account Automatically**.
- Click **OK**.
- When add the new account in **Mail Account**, the new account will synchronize added into the **Selected Account**. The CS-2000 will send the spam mail (virus) notification to the recipients' mail box on time.

Mail Notice (Internal mail server only)

☒ Enable Notice : **Both** ▼

☒ Send Mail Notice on weekend

1st Time : 00:00 ▼ 4th Time : 12:00 ▼ Mail Type : HTML ▼ [Notice Now](#) [Help](#)

2nd Time : 04:00 ▼ 5th Time : 16:00 ▼ Sender : notice@myalexweb.dyndns.tv

3rd Time : 08:00 ▼ 6th Time : 20:00 ▼ (Max. 99 characters, ex: user@mydomain.com)

**Select All** **Invert**

joe@myalexweb.dyndns.tv  
notice@myalexweb.dyndns.tv

**Remove**

**Add**

**Select All** **Invert**

<--- Selected Account --->  
admin@myalexweb.dyndns.tv  
alex@myalexweb.dyndns.tv  
eva@myalexweb.dyndns.tv

☒ Add Notice Account Automatically

**The mail notice setting**



The CS-2000 will send the spam (virus) mail notice to the selected account, when CS-2000 detected the internal to external sender and external to internal recipient started to transfer the spam Mail (Virus) to each other.



In 1<sup>st</sup> to 6<sup>th</sup> notice time setting, the CS-2000 will send the spam (virus) mail notice to the recipient depends on the time priority.



After the recipient got the spam (virus) mail notice, the CS-2000 will not send any mail notice if the recipient did not receive any spam mail from the external mail server via the internal mail server before the next spam (virus) mail notice start to send.



The MIS engineer can choose to **Select All** or **Invert**, to **Remove** the **Selected Account** to **Select Account** list, in other words, the Select Account list will not get the spam (virus) mail notice.

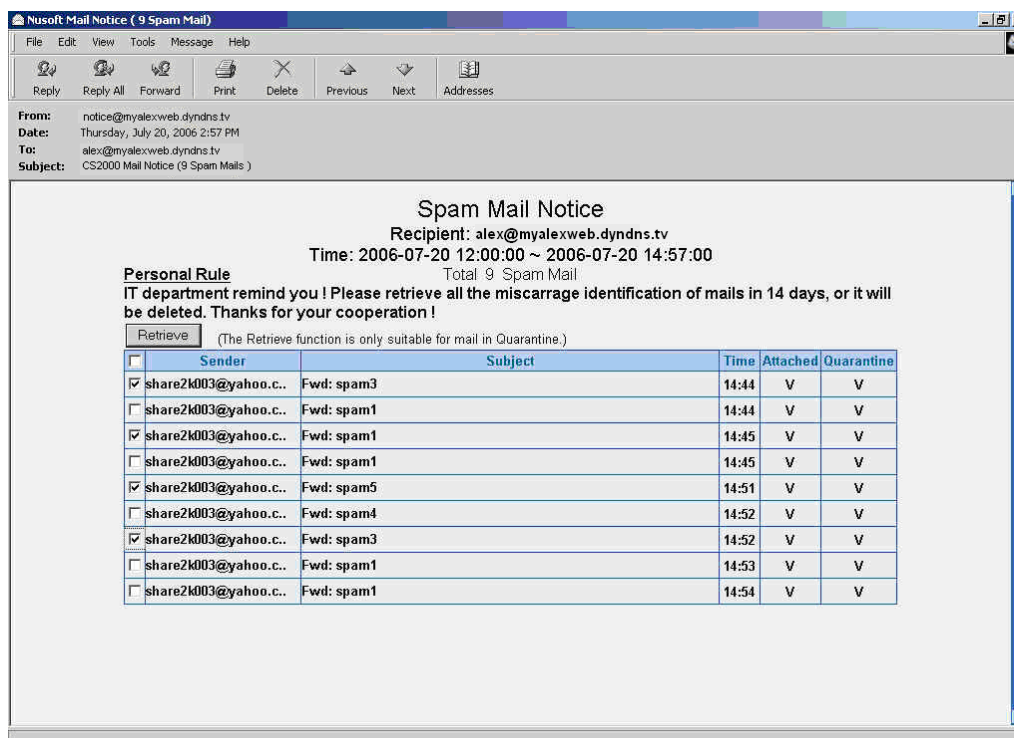


When disable **Send Mail Notice on weekend**, the mail notice on every weekend will be delay to send on Monday's earliest notice time.



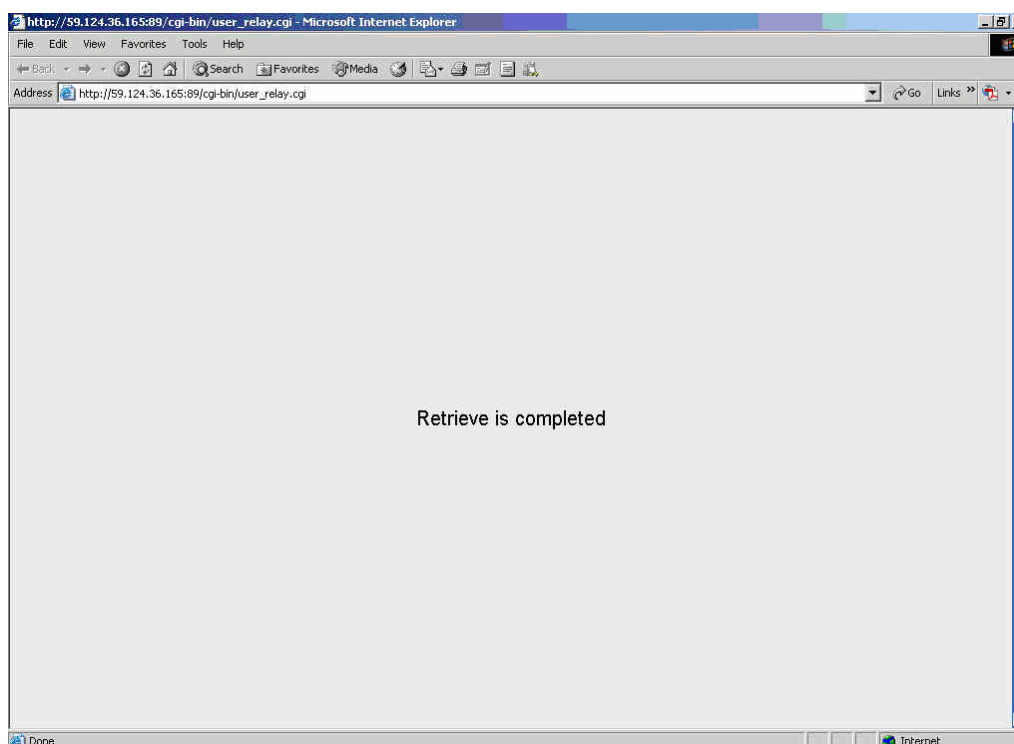
After disabled **Add Notice Account Automatically**, the CS-2000 will not send any mail notice to the recipient when add new account in **Mail Account** and also synchronize to add the account in selected account list.

- Step4** When the recipient receive the **Spam Mail Notice** ( or Virus Mail Notice):
- In **Inbound** list, choose the spam (virus) mail to retrieve, click Retrieve.
  - After the CS-2000 sends the spam (virus) mails, it shows the message of **Retrieve is Completed.**



Select the spam (virus) mail to retrieve





Complete to retrieve the spam (virus) mail



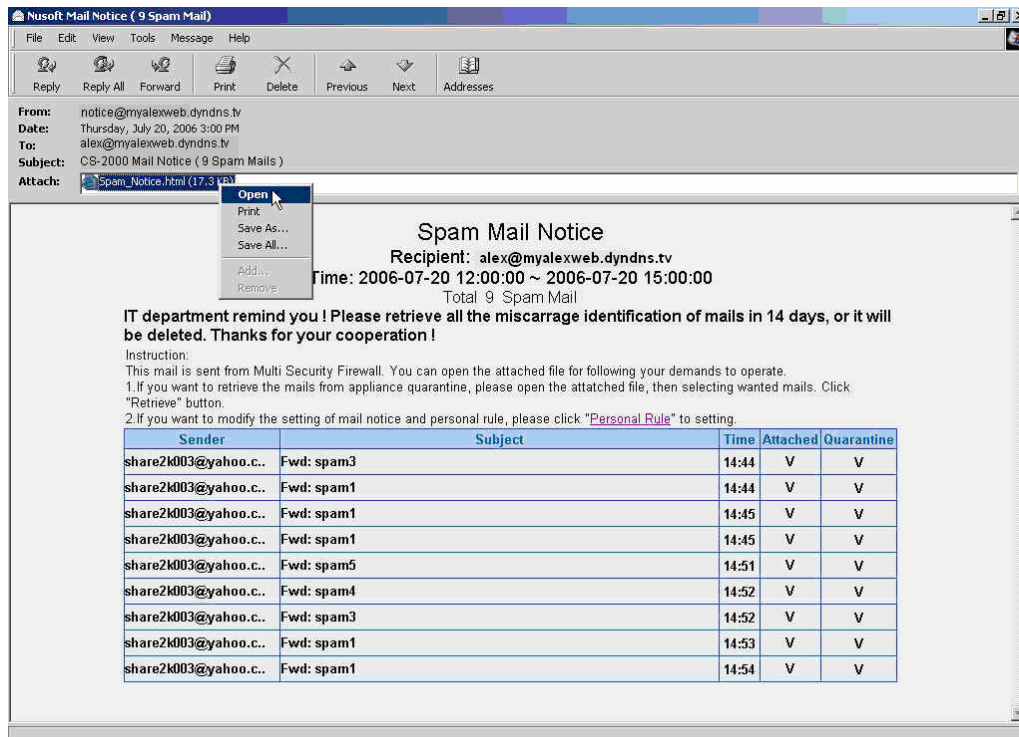
There are two ways to retrieve all the **spam / virus mails** in **spam / virus mail notice**.

**A :**

- When receive the **spam / virus mail notice** by **attached** type, user has to open the attachment.
- In **Open Attachment Warning** window, select **Open it** and click **OK**.
- Select all the **Inbound** list and click **Retrieve**, then retrieve all the spam (virus) mails.

**B :**

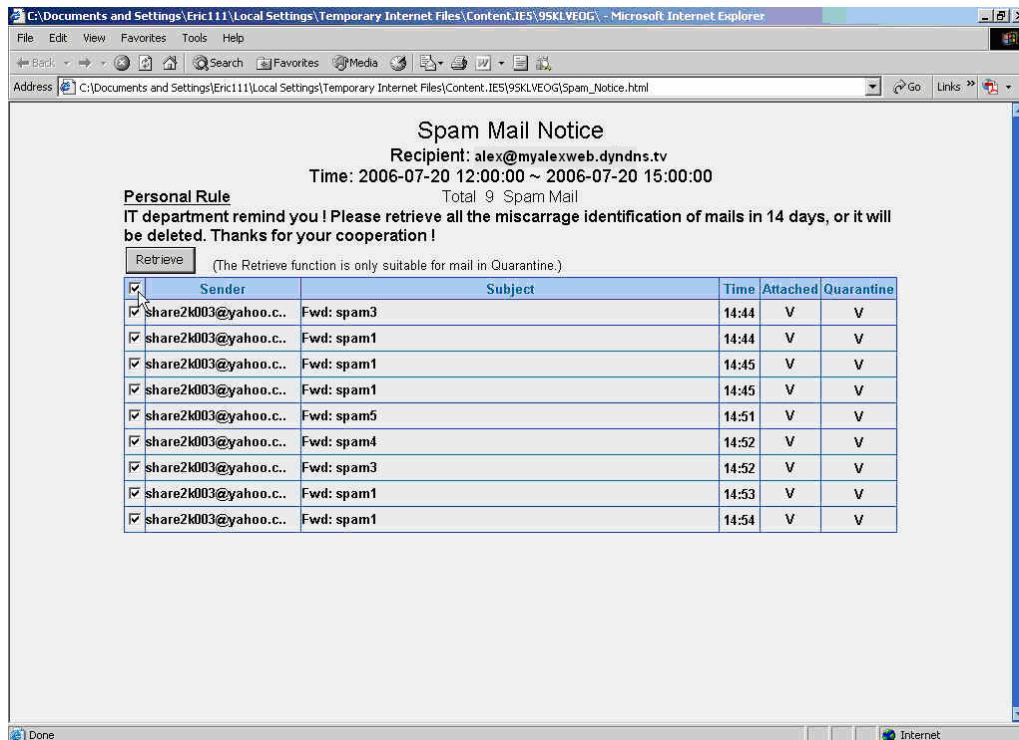
- When receive the **spam / virus mail notice** by **HTML** type :
  - ◆ In **Outlook Express** mail preview window , it can not run the Java Script in default situation, so that we need do :
    1. Separately select the **Inbound** list and click **Retrieve**, then retrieve all the spam (virus) mails.
  - ◆ If select **Outlook Express** → **Tools** → **Options** → **Security** → **Virus Protection** → **Internet zone**. Then user can select all the list to process retrieve and resend all the spam (virus) mails. ( it's the same as method A )



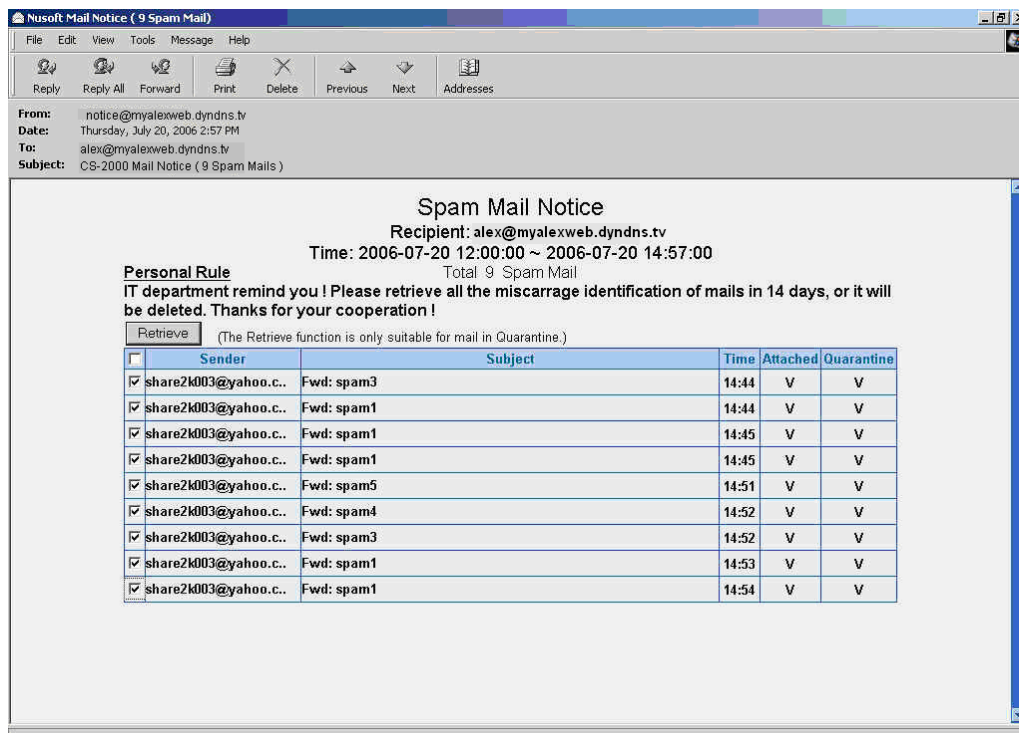
Open the attachment in spam (virus) mail notice



Confirm to open the attachment



To retrieve all the spam (virus) mails from the spam (virus) mail notice

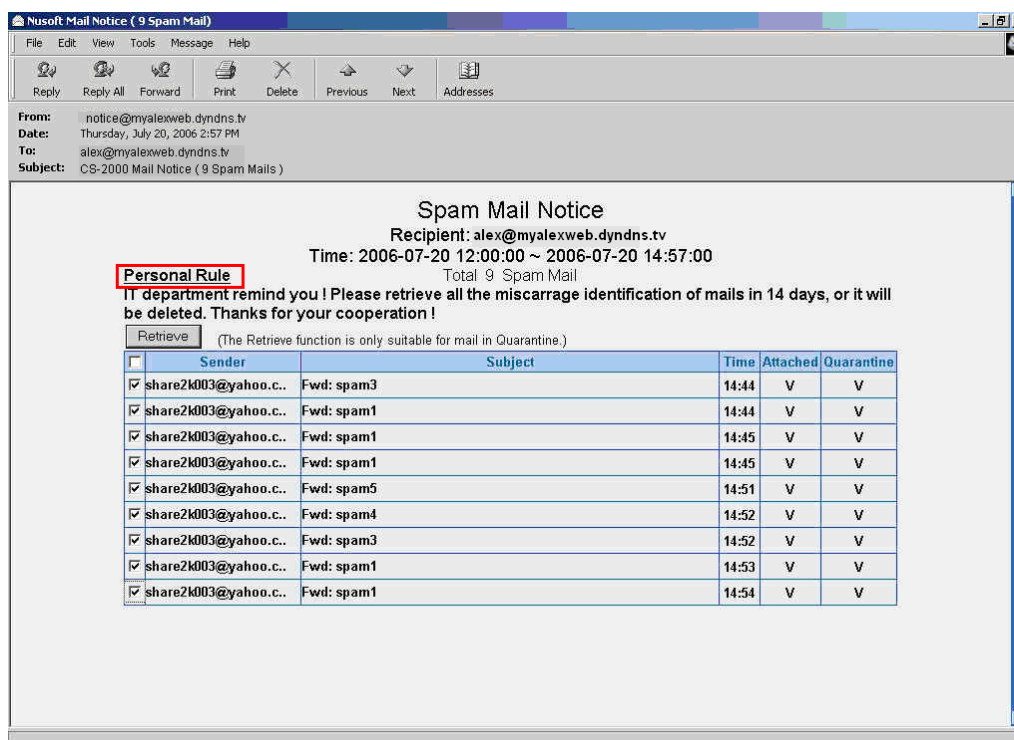


To retrieve all the spam (virus) mail from the preview spam (virus) mail notice

## Example 2

### Personal Rule Setting

**Step1.** Click **Spam (Virus) Mail Notice** → **Personal Rule**.



Login the personal rule

**Step2.** In personal rule setting window, add the following settings :

- Click **Notice**.
- Select **Enable Notice**→ **Both**.
- Disable **Send Mail Notice on weekend**.
- **Mail Type**→ **HTML**.
- Click **OK**.
- Click **Language**.
- Select **English Version**.
- Click **OK**.
- Complete to set the recipient can receive the CS-2000 mail notice of English version by the rule setting from Monday to Friday.

The screenshot shows a web interface with a navigation bar at the top containing buttons: Search, WhiteList, BlackList, Language, Notice, and Password. The 'Notice' button is highlighted. To the right of the navigation bar is the email address 'alex@myalexweb.dyndns.tv'. Below the navigation bar is a dashed line. The main content area is titled 'Mail Notice Setting' and contains the following settings: 'Enable Notice' is checked and set to 'Both'; 'Send Mail Notice on weekend' is checked; 'Mail Type' is set to 'HTML'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**The personal rule mail notice setting**

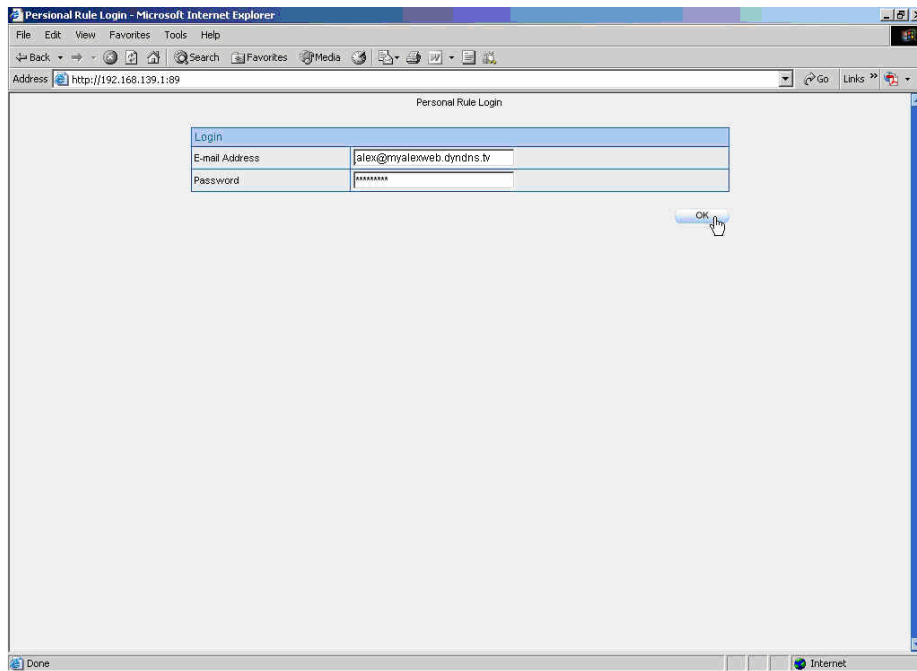
The screenshot shows the same web interface as the previous one, but the 'Language' button in the navigation bar is highlighted. Below the navigation bar is a 'Previous' button. The main content area is titled 'Mail Notice Language Setting' and contains three radio button options: 'English Version' (which is selected), 'Traditional Chinese Version', and 'Simplified Chinese Version'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**The mail notice language setting**

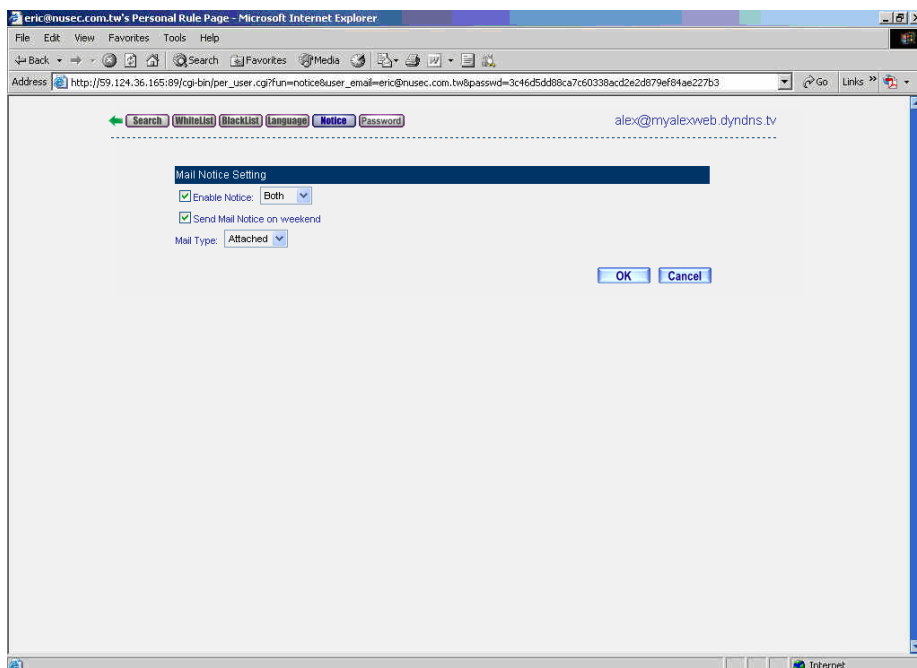


In **Personal Rule**→ **Notice**, disable the **Enable Notice**, and then user can not receive the mail notice from CS-2000. The way to solve the problem:

1. Login the CS-2000 89 port→ **Personal Rule Login**→ **Notice** → **Enable Notice**.
2. Open the spam ( virus ) mail notice , click **Personal Rule**→ **Notice** → **Enable Notice**.
3. Contact the MIS engineer, and then **add** the recipient account to **selected account** in **Mail Notice** function.



Login personal rule management interface



The mail notice setting in personal rule

**Step1.** Allow the user to customize the login password :

- Enable the **local database** in **Login Authentication of Personal Rule**.
- Click **Password**.
- Enter 123456789 of **Password**.
- Click OK.
- Enter the **E-mail address** and **password** as using the 89 port to login the personal rule via the CS-2000.
- Click **OK**.
- Complete to login the personal rule.

Scanned Mail Setting	
The scanned spam mail size is less than	512 KBytes ( Range: 10 - 5120 )
The scanned virus mail size is less than	1024 KBytes ( Range: 10 - 5120 )

Unscanned Mail Setting	
<input checked="" type="checkbox"/> Add the message to the subject line	---CS-200_Unscanned--- (Max. 255 characters)

Mail Notice use the IP (or domain name) for retrieving spam / virus mails	
IP Address (or Domain Name)	203.67.31.11 <a href="#">Assist</a> (WAN1 IP recommended)

Mail Notice Message Setting	
Mail Notice Subject	!!! CS-2000 Notice mail !!!
Message of notice mail content	
<div>This is CS-2000 Notice mail !!! You have 7 Days for retrieve the Spam mails!!!!</div>	

Storage lifetime of spam / virus mails in the quarantine	
Storage lifetime	14 Days ( Range: 1 - 365 )
<input type="checkbox"/> Disable multi-retrieve of quarantined mails	

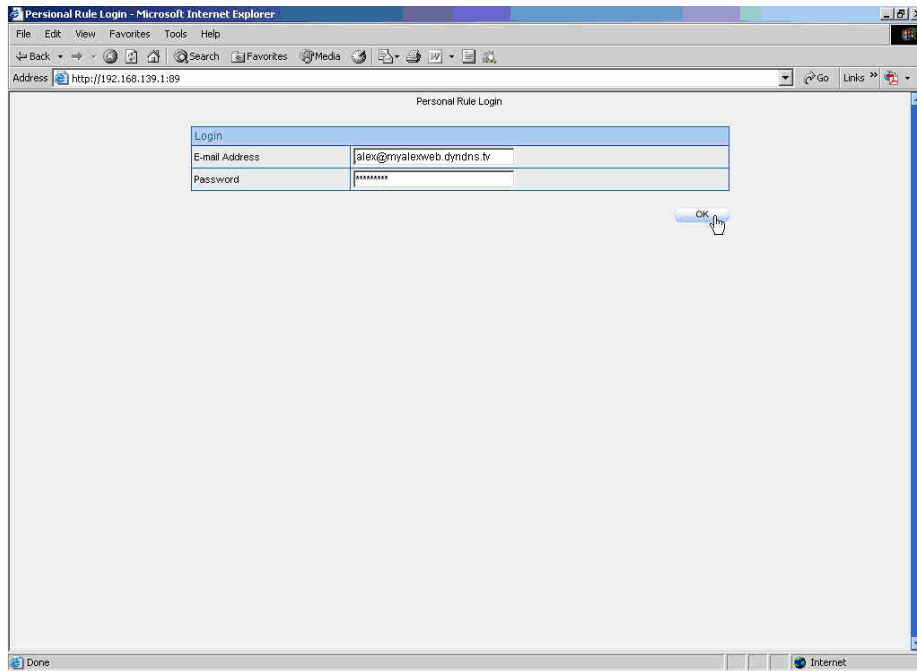
Login Authentication of Personal Rule	
Login Port	89 ( Range : 1-65535 )
<input checked="" type="checkbox"/> Enable personal rule	
Login Authentication :	
<input checked="" type="checkbox"/> POP3	
<input checked="" type="checkbox"/> Local Database	

**Enable the local database function**

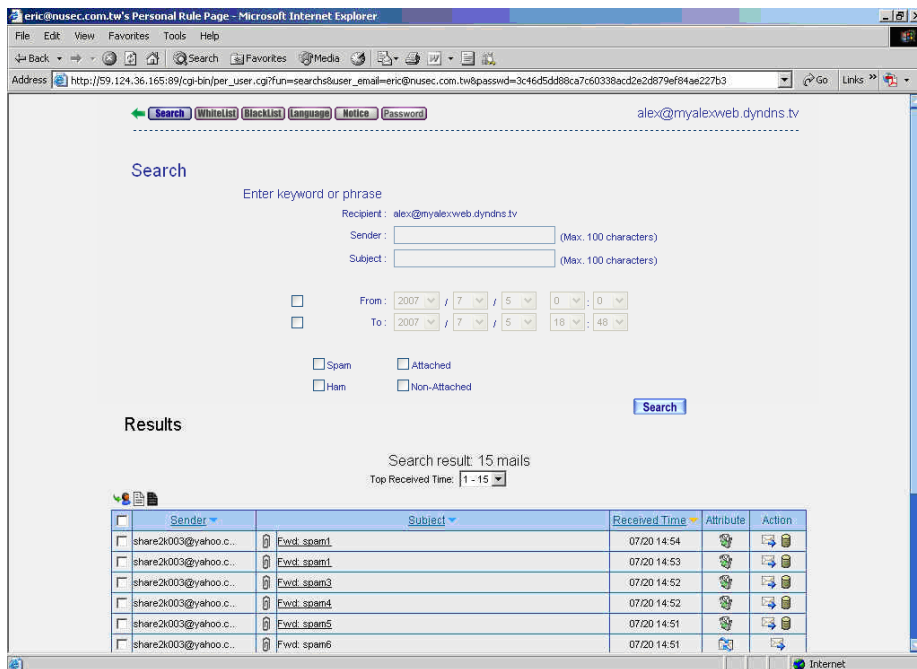
[Search](#) [WhiteList](#) [BlackList](#) [Language](#) [Notice](#) [Password](#) alex@myalexweb.dyndns.tv

Password  
123456789 (Max. 16 characters)

Type the password



Log in the personal rule authentication window



Complete to login the personal rule



## 7.2 Anti-Spam

# Anti-Spam

The CS-2000 can filter the mails in internal and external mail server. The function can also improve the efficiency of the company's mail server and let recipients can select to read the needed mails. In other words, it can also improve the employee's working efficiency; otherwise the staffs will not lose any important information. Actually, the CS-2000 can accurately identify which mails to be the spam mail.

In this Chapter, we will make the introduction of **Anti-Spam**.

## 7.2.1 Setting

### Spam Setting

- Can make the inbound and outbound mail inspection.
- If the mails has over the threshold score, then add the message or select to add the score tag to the subject line. If the mails have not over the threshold score, then the MIS engineer can only add the score tag to the subject line.
- We can use the many methods to distinguish if the mails are spam mails in the CS-2000 :
  - ◆ Check spam fingerprint : To compare the mail's ID (after calculated) to the mail server's spam mail ID list.
  - ◆ Enable Bayesian filtering : Bayesian filtering can compare the mail header item to the training database filtering rules.
  - ◆ Spam signature push update : To compare the mail algorithm values to the mail classification values in server database.
  - ◆ Check sender account : To send the check packets to sender account.
  - ◆ Check sender IP address in RBL : To compare the sender IP to the blacklist in mail server.
- When adjust the spam mail scanning options, the CS-2000 can compare the priority of **Personal Rule** and **Global Rule**.



The CS-2000 will use the default rules to scan the mails if the MIS engineer did not select any spam mail action.



The Bayesian filtering works until training database has at least 200 spams and 200 hams.

The amount of spams in the database : 5878

The amount of hams in the database : 1023

Bayesian filtering works until database has at least 200 spams and 200 hams

### The amount mail in Bayesian training database

## Action of Spam Mail

- The CS-2000 can delete the inbound spam mail, select to deliver to the recipient or forward it to another mail account or just save it in quarantine.
- The CS-2000 can directly send the inbound spam mail to the recipient and also save it in quarantine.
- Add the following setting :
  1. **The Mail Server is placed in**, select Internal.
  2. **The threshold score of spam mail is**, select 5.
  3. **Add the spam string to the subject line**, enter --spam--.
  4. Select **Add score tag to the subject line**.
  5. In **Action of Spam Mail** → **Internal Mail Server**, select **Deliver to the recipient**.
  6. Click **OK**.

Spam Setting

☒ Enable Anti-Spam

The Mail Server is ☒ Internal (External user sends emails to internal mail server)  
☒ External (Internal user receives emails from external mail server)

---

The threshold score of spam mail is 5

Add the spam string to the subject line ---Spam--- (Max. 256 characters)

☐ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) Test

☐ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)

☐ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) Test

☐ Drop the first connection of new sender account (Greylist Filtering)

☐ Verify sender account is valid (Use TCP port : 25 and UDP port : 53 to connect mail server)

☐ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) Test

☒ Add score tag to the subject line

---

Rule Priority: ☒ Personal Rule priority higher than Global Rule  
☐ Global Rule priority higher than Personal Rule

Action of Spam Mail

Internal Mail Server (External user sends emails to internal mail server) :

☐ Delete the spam mail

☒ Deliver to the recipient

☐ Forward to : notice@myalexweb.dyndns (Max. 128 characters, ex: user@mydomain.com)

☐ Store in the quarantine

---

External Mail Server (Internal user receives emails from external mail server) :

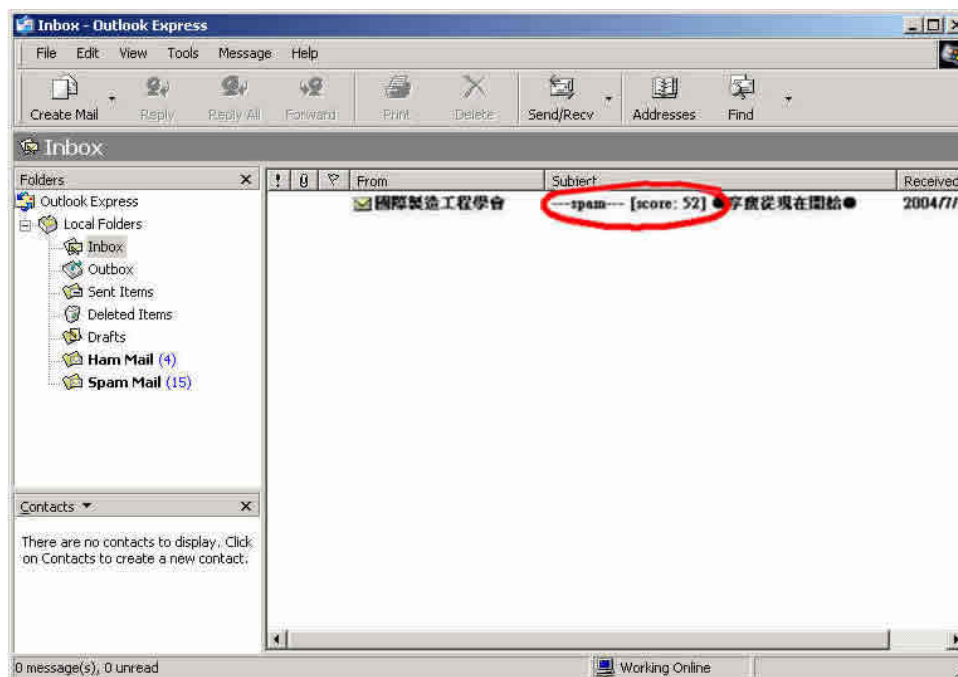
☒ Deliver to the recipient (Always enable)

☒ Store in the quarantine

OK
Cancel

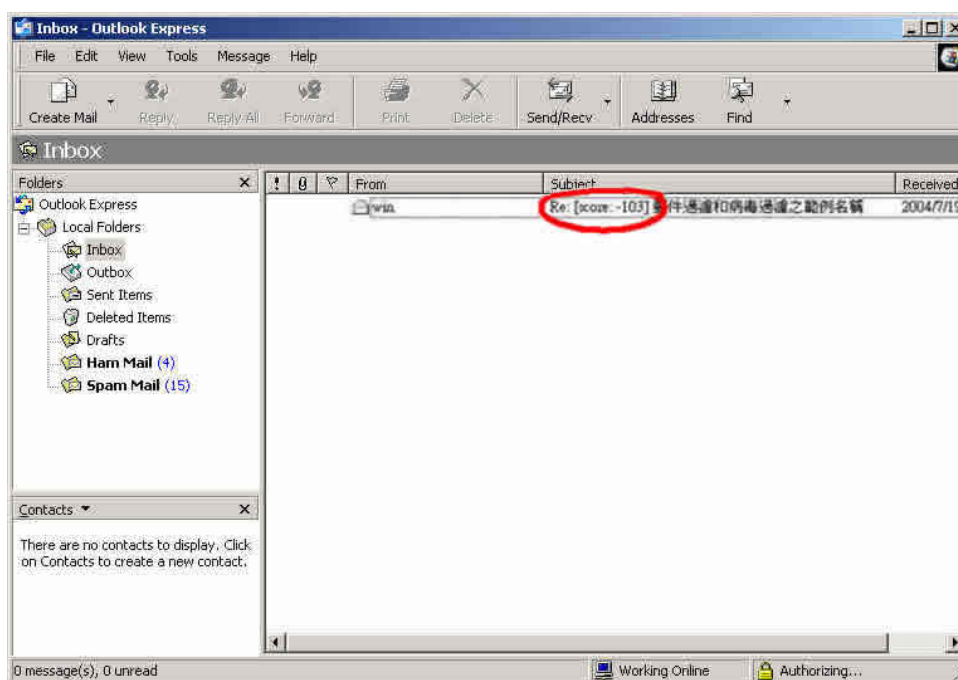
## The spam filtering setting

- The internal and external recipient will received the spam mail which has been added the score tag and spam string to the subject line.



The spam mail subject line included the score tag and spam string

- The internal and external recipient received the non-spam mail which has been only added the score tag in subject line.



The non-spam mail subject line only included the score tag

## 7.2.2 Personal Rule

### Personal Rule :

#### Search

- To search the recorded mails which filtered by the CS-2000.
- Add the searched sender mail address into whitelist or blacklist.
- To identify the non – spam mails in quarantine through training.
- Can retrieve the mails stored in quarantine.

#### Whitelist

- To assign the allowed personal send / retrieve mail address.

#### Blacklist

- To assign the denied personal send / retrieve mail address.

#### Language

- To assign the language Web UI in personal mail notice. (Default language is the same as the Web UI)

#### Notice

- To assign the personal mail notice type.
- Select to enable / disable the mail notice according to the personal settings.

#### Password

- Use the password to log in personal rule.
- The MIS engineer can use the password and apply it to original mail account to log in personal rule as enabled the local database authentication of personal rule.



When the MIS login Web UI, it shows the **Training** function in **Personal Rule → Search, Global Rule → Search, Global Rule, Whitelist and Blacklist**. On the other hand , when the normal user login **Personal Rule → Search , Whitelist and Blacklist** setting through **Mail Notice** or **CS-2000 interface 89 Port** , it will not shows the **Training** function.

### 7.2.3 Global Rule

#### Global Rule :

##### Rule Name

- To customize the mail rule name.

##### Comments

- The description of customized mail rules.

##### Combination

- And : To identify the spam or ham mail depends on the mails which must be corresponding to all the customized mail rules.
- Or : To identify the spam or ham mail depends on the mails which correspond to one or above customized mail rules.

##### Action

- To enable **Action**, select **Classification → Spam**, it is because only the spam mails need to use the action function.
- Can delete the spam mail, send the spam mail to the original recipient, and forward the spam mail to another mail account or save it to quarantine.

##### Classification

- When select **Spam**, it will classify the mails to be spam mails, which correspond to the mail rules.
- When select **Ham (Non-Spam)**, it will classify the mails to be ham mails, which correspond to the mail rules.

##### Auto-Training

- To enable **Classification → Spam**, the **Training** will identify the mail to be the spam mails in the time setting which is correspond to the mail rules.
- To enable **Classification → Ham (Non-Spam)**, the **Training** will identify the mail to be the ham mails in the time setting which is correspond to the mail rules.

### Item

- To identify if the mail signature of Header, Body, and Attach File Name correspond to the Spam Mail depends on the condition.
- The detected mail 's Header Item included Received , Envelope-To , From , To , Cc , Bcc , Subject , Sender , Reply-To , Errors-To , Message-ID and Date.

### Condition

- When select **Item → Header and Body** , the available condition includes Contains , Does Not Contain , Is Equal To , Is Not Equal To , Starts With , Ends With , Exists and Does Not Exists .
- When select **Item → Attach File Name**, the available condition includes Contains, Does Not Contain, Is Equal To, Is Not Equal To, Starts With and Ends With.
- When select **Item → Size**, the available condition includes More Than, Is Equal To , Is Not Equal To and Less Than.

### Pattern

- In **Item** and **Condition**, enter the related values. For example, select **Item → From**, **Condition → Contains**, and enter **josh** in **Pattern**. In other words, once the sender mail account includes **josh**, will be defined to spam or ham mail.



## 7.2.4 Whitelist

**Whitelist :**

### Whitelist

- To allow the specific mail account can freely send / retrieve mails.

### Direction

- **From** : To distinguish the mail sender address.
- **To** : To distinguish the mail recipient addresses.

## 7.2.5 Blacklist

**Blacklist :**

### Blacklist

- To forbid the specific mail account to send / retrieve mails.

### Direction

- **From** : To distinguish the mail sender address.
- **To** : To distinguish the mail recipient addresses.

## 7.2.6 Training

### Training :

#### Training Database

- The MIS engineer can export, import files or reset the training database.

#### Spam Mail for Training

- The MIS engineer can import spam mail files, in order to improve the spam mail filtering accuracy.

#### Ham Mail for Training

- The MIS engineer can import ham mail files, in order to improve the ham mail filtering accuracy.

#### Spam Account for Training

- User can send the spam mail to assigned mail address, and the CS-2000 can receive these mails from the mail account on time, in order to improve the spam mail filtering accuracy.

#### Ham Account for Training

- User can send the ham mail to assigned mail address. And the CS-2000 can receive these mails from the mail account on time, in order to improve the ham mail filtering accuracy.

#### Training time

- The MIS engineer can select the training time which let the CS-2000 can import the files in training database on the time setting.
- The CS-2000 can instant training the imported training files in training database.

## 7.2.7 Spam Mail

### Spam Mail :

#### Search

- To search all the records correspond to the condition in CS-2000 , according to the keywords or phrases of Recipient , Sender , Subject , Received Time , Spam Mail , Ham Mail , Attached and Non-Attached .
- Add the following settings :
  1. **Recipient**, enter the mail account or keywords. ( For example, admin, admin@test.com ) .
  2. To enable and set the function of search the records at assigned date.
  3. Select **Spam, Ham, Attached, Non-Attached**.
  4. Click **Search**.

#### Search

Mail Direction : Inbound  
Mail Server : Internal

Enter keyword or phrase

Recipient :  ( Max. 100 characters )

Sender :  ( Max. 100 characters )

Subject :  ( Max. 100 characters )

☒ From : 2007 / 7 / 2 0 : 0  
☒ To : 2007 / 7 / 6 9 : 10  
☒ Spam ☒ Attached  
☒ Ham ☒ Non-Attached

#### Results

Search result: 9 mails

Top Received Time: 1 - 9

	Sender	Recipient	Subject	Received Time	Mail Size	Spam	Quarantine
	nobody@yahoo.edyna..	admin@myalexweb.dy..	- 田 肇坪 您好 帶給您最新Au...	07/06 06:33	16.6 KB		
	123654@edm.yam.com	admin@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨..	07/06 06:22	52.6 KB		
	1482@mail.ms-edm.c..	admin@myalexweb.dy..	- 七月份TechNet Webcast 研討..	07/06 03:45	26.1 KB		
	edm@cms5.so-net.ne..	admin@myalexweb.dy..	- 密切鎖定！史上最強的電玩大帝..	07/06 02:34	27.7 KB		
	vincechase@ms96.ur..	admin@myalexweb.dy..	- 7月6日工作分配	07/06 00:40	68.3 KB		
	m15001.s4734.c2456..	admin@myalexweb.dy..	- NBA Daily - Sonics Sign Dura..	07/06 00:23	16.7 KB		
	v-npadb_bhjmfmlc_..	admin@myalexweb.dy..	- Most surprising teams in bas..	07/05 23:50	26.1 KB		
	epaper@news.gameto..	admin@myalexweb.dy..	- 《唯舞獨尊online》會員突破百..	07/05 20:29	15.6 KB		
	epaper@news.gameto..	admin@myalexweb.dy..	- 《唯舞獨尊online》會員突破百..	07/05 20:29	15.6 KB		

To search the specific record



In **Spam Mail** , the MIS engineer can select to display the searched inbound or outbound filtered mails.



In **Spam Mail**, click the **Recipient** mail address, it shows the **Sender List**. In **Sender List**, click the **Sender mail address**, it shows the **Spam List**.



In **Spam List and Search → Search Results** , to select the specific mails :

1. The CS-2000 will identify the related mails to be the ham mails through **Training** function . ( The CS-2000 can only training the mails stored in quarantine. )
2. The CS-2000 will send the mails to assigned mail account through **Retrieve** function. ( The CS-2000 can only send the mails stored in quarantine. )



In **Spam Mail** and **Sender List** , the CS-2000 can make the sorting by the recipient , sender , total spam and total mail . In **Spam List**, the CS-2000 can make the sorting by the subject and received time.

### 7.2.8 The Advanced Description

The so called mail server is the medium between the mail send and retrieve process. The E-mail address format is: For example, [account@server.name](#) , the mail account is in front of the @, the server name is after the @.

When MIS engineer send an e-mail to [josh@yahoo.com.tw](#) , MIS engineer mail sending software will first search the destination mail server name which correspond to the IP and MX record. The e-mail will be first send to the MX mail server which correspond to the MX record , then the MX server send the mails to the destination address ( It is the yahoo.com.tw mail server ) . If the mail server corresponds to many MX records, then the E-mail will be sent to the top priority MX server, then continue the process. If there is no correspond MX record except the IP record, the mail will be first sent to user mail server and transfer to yahoo.com.tw mail server. The yahoo.com.tw mail server will send the mail to every recipient according to the **Account** in front of the @.

**Mail Transferring Process :**

The 3 elements of the e-mail send / retrieve : MUA, MTA, MDA.

- **MUA ( Mail User Agent )** : The client PC needs to use the MUA provided by the OS to process send / retrieve. For example, the outlook express is a kind of MUA. The MUA can receive or send the mails via the mail server, and also provide the user to read and edit mails.
- **MTA ( Mail Transfer Agent )** : User need to use MTA to send / retrieve the mails. The MTA includes 3 functions :
  1. To retrieve the mails from external mail server : The MTA will receive the mails from the external mail server, when the recipient mail account existed in the MTA.
  2. To help user to send the mails : When the user has the authority to use the MTA, then he can send the mails via MTA.
  3. To let the user can receive his own mails : User can receive his own mails from the mail server.



The mail server is a kind of MTA.

- **MDA ( Mail Delivery Agent )** : The MDA can deliver the mails to destination local user's mailbox from the MTA, or send the mails from the current MTA to next MTA.

**Mail transferring process (sends and retrieves)**

There are several steps of mail sending process :

- To send the mails to MTA via MUA : The user has to make the following settings , when edit the mails through MUA :
  1. The sender mail address and sender mail server (The sender send the mails to MTA via MUA.)
  2. The recipient mail address and recipient mail server (The recipient MTA which receive the mails from the external mail server.)

The user use the MUA (For example, outlook express) to send the mails to assigned MTA.

- If the mail server is the MTA itself , then it will send the received mails to recipient account mailbox via MDA
- The MTA use mail relay to send the mails : The MTA use the mail relay to send the mails if the recipient account is not existed in MTA.
- The remote MTA received the mails from local MTA : The Remote MTA received the mails from Local MTA, and then sends the mails to remote user via MDA. User can download these mails as login MUA.

The process of users receive the mails :

Remote user can check if there are the mails in remote user mailbox via MDA .If there are the mails existed, and then remote MTA will send mails to user's MUA. According to the MUA Setting, MUA can delete or remain the mails. ( As the user use the MUA to receive the mails again, and then the remained mail will be downloading again. )



The Protocol used in the mail send / retrieve process :

1. **Send E-Mail** : It means the process of users send the mails to MTA via MUA and transfer the mails to the next MTA. Most of the mail server use the SMTP Protocol ( Simple Mail Transfer Protocol ) , and the port number is 25 .
2. **Retrieve E-Mail** : It means the recipient use MUA to link to MTA mailbox through the POP Protocol ( Post Office Protocol ) , in order to read or download the mails from mailbox . The most common used POP Protocol is POP3 ( Post Office Protocol version 3 ) , and its port number is 110 .



Basically, the MTA need at least two Protocols, and it included SMTP and POP3. Both of the MUA and MTA can communicate to each other only if the MUA and MTA support SMTP and POP3.



The MTA can analyze the received mails to check if the recipient mail account existed in MTA or it will relay the mails to the next MTA.



The **Open Relay** mail server can allow anyone to use one of the mail server to send the mails. To avoid this problem, most of the mail server setting still disable the relay function. The Mail Server only enable the relay function to **Local host**, so that the MTA can receive the mails from the network with the recipient mail account existed in MTA server. Basically, there is no big problem with MTA mail **Retrieve** function except one condition. Normally, the MTA only enable the relay function to some local host with regulated IP and domain. The Client PC can freely send / retrieve the mails. In other words, the sender mail will be blocked if it is not in the regulated range. We can use the **SMTP** to solve the problem.



The so called SMTP is that the MTA server will **require to check the MUA User's Mail Account and Password**, then MTA will provide the relay function to the authenticated user without regulating the IP and domain. It is because the MTA can analyze the sender Authentication information via **Authentication** function. After the authentication, MTA will continue to relay the sender mails.



## 7.2.9 Anti-Spam Examples

**We set 5 anti-spam environments.**

No.	The Application Environments	Pages
<b>Example. 1</b>	To detect if the received mails are spam mails on mail server.	<b>344</b>
<b>Example. 2</b>	Set the CS-2000 to be the gateway, and use the whitelist and blacklist to filter the mails. (Set the mail server in DMZ and use transparent mode.)	<b>350</b>
<b>Example. 3</b>	Set the CS-2000 between the company's original gateway and mail server. Use the global rule to filter mails. (Set the mail server in DMZ, and use transparent mode.)	<b>361</b>
<b>Example. 4</b>	Use spam or non-spam mail training to improve the Bayesian filtering. ( For example , Outlook Express )	<b>371</b>
<b>Example. 5</b>	Use spam or non-spam mail account training to improve the Bayesian filtering.	<b>384</b>

## Example 1

To detect if the received mails are spam mails on mail server.

**Step1** To allow the **LAN** PC can receive mails from the external mail server. Set the network adapter IP correspond to the external DNS server.

**Step2** In **Service → Group** , add the following setting :

Group name ▼	Service	Configure
Mail_Service	DNS,IMAP,POP3...	<a href="#">In Use</a>
Main_Service	DNS,HTTP,POP3...	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Set the group included POP3 and SMTP or DNS

**Step3** In **Policy → Outgoing** , add the following settings :

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	Mail_Service			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▼

[New Entry](#)

Set the outgoing policy

**Step4** In **Anti-Spam → Setting** , add the following settings :

**Spam Setting**

☒ **Enable Anti-Spam**

The Mail Server is ☒ Internal (External user sends emails to internal mail server)  
☒ External (Internal user receives emails from external mail server)

---

The threshold score of spam mail is  (Max. 256 characters)

Add the spam string to the subject line  (Max. 256 characters)

☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)  
☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)  
☒ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)  
☒ Drop the first connection of new sender account (Greylist Filtering)  
☒ Verify sender account is valid (Use TCP port : 25 and UDP port : 53 to connect mail server)  
☒ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)  
☐ Add score tag to the subject line

---

Rule Priority: ☒ Personal Rule priority higher than Global Rule  
☐ Global Rule priority higher than Personal Rule

**Action of Spam Mail**

Internal Mail Server (External user sends emails to internal mail server) :

☐ Delete the spam mail  
☐ Deliver to the recipient  
☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com)  
☐ Store in the quarantine

---

External Mail Server (Internal user receives emails from external mail server) :

☒ Deliver to the recipient (Always enable)  
☒ Store in the quarantine

### Set the anti-spam mail action



The default setting of **Anti-Spam** is enabled. The MIS engineer only need to add the mail relay setting, then the CS-2000 will start the anti-spam action to the internal mail server and external mail server.

Spam Setting	
<input checked="" type="checkbox"/> Enable Anti-Spam	
The Mail Server is	
<input checked="" type="checkbox"/> Internal (External user sends emails to internal mail server)	
<input checked="" type="checkbox"/> External (Internal user receives emails from external mail server)	
-----	
The threshold score of spam mail is	5
Add the spam string to the subject line	---Spam--- (Max. 256 characters)
<input checked="" type="checkbox"/> Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server)	<a href="#">Test</a>
<input checked="" type="checkbox"/> Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)	
<input checked="" type="checkbox"/> Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature)	<a href="#">Test</a>
<input type="checkbox"/> Drop the first connection of new sender account (Greylist Filtering)	
<input type="checkbox"/> Verify sender account is valid (Use TCP port : 25 and UDP port : 53 to connect mail server)	
<input type="checkbox"/> Check sender IP address in RBL (Use UDP port : 53 to connect DNS server)	<a href="#">Test</a>
<input type="checkbox"/> Add score tag to the subject line	
-----	
Rule Priority:	
<input checked="" type="radio"/> Personal Rule priority higher than Global Rule	
<input type="radio"/> Global Rule priority higher than Personal Rule	
Action of Spam Mail	
Internal Mail Server (External user sends emails to internal mail server) :	
<input type="checkbox"/> Delete the spam mail	
<input type="checkbox"/> Deliver to the recipient	
<input type="checkbox"/> Forward to :	notice@myalexweb.dyndr (Max. 128 characters, ex: user@mydomain.com)
<input checked="" type="checkbox"/> Store in the quarantine	
-----	
External Mail Server (Internal user receives emails from external mail server) :	
<input checked="" type="checkbox"/> Deliver to the recipient (Always enable)	
<input checked="" type="checkbox"/> Store in the quarantine	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### The default setting of anti-spam



When start the anti-spam action to the mails on retrieve mail server :

1. In **Action of Inbound Spam Mail** → **External Mail Server** and **Action of Outbound Spam Mail** → **Internal Mail Server**, please always enable **Deliver to the recipient** option, because it is the default setting. On the other hand, the user can select to **Store in the quarantine**. The CS-2000 will add the message to the subject line when it detects the spam mail, whatever the spam mail action that MIS engineer has selected.
2. To use the **Global Rule, Whitelist, or Blacklist** to filter the spam mail.
3. The CS-2000 will not send the spam list to the recipient through **Mail Notice**.

- Step5** When the internal user receive mails from the external mail account [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw) , the CS-2000 will filter these mails and results the list in **Anti-Spam → Spam Mail**. ( Click Inbound and External )

Mail Direction : Inbound Inbound  
 Mail Server : Internal External

The Duration of Today

No.	Recipient ▼	Total Spam ▼	Total Mail ▼	Duration	Spam %
1	<a href="mailto:js1720@ms21.pchome.com.tw">js1720@ms21.pchome.com.tw</a>	1	7	06H	14.3%
2	<a href="mailto:eva@myalexweb.dyndns.tw">eva@myalexweb.dyndns.tw</a>	1	7	06H	14.3%
3	<a href="mailto:ioe@myalexweb.dyndns.tw">ioe@myalexweb.dyndns.tw</a>	1	7	06H	14.3%
Total		3	21		14.3%

Clear Data

### The spam mail list

- Step6** Click **Recipient** of [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw) , then it shows the sender list, look the **Total Spam** and **Total Mail** from the sender account.

### Sender List

1 / 2
←
Recipient: [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw)

No.	Sender ▼	Total Spam ▼	Total Mail ▼	Duration	Spam %
1	(No Sender)	1	5	00H	20.0%
2	<a href="mailto:liann_paul@xuite.net">liann_paul@xuite.net</a>	1	1	00H	100.0%
3	<a href="mailto:bellahaw@cm1.hinet.net">bellahaw@cm1.hinet.net</a>	1	1	00H	100.0%
4	<a href="mailto:sheng.mi@gmail.com">sheng.mi@gmail.com</a>	1	1	00H	100.0%
5	<a href="mailto:catherinesylvia@hotmail.com">catherinesylvia@hotmail.com</a>	1	1	00H	100.0%
6	<a href="mailto:mostanley@yahoo.com.sg">mostanley@yahoo.com.sg</a>	1	1	00H	100.0%
7	<a href="mailto:yloou@yahoo.com.cn">yloou@yahoo.com.cn</a>	1	1	00H	100.0%
8	<a href="mailto:richard_sunny@msa.hinet.net">richard_sunny@msa.hinet.net</a>	1	1	00H	100.0%
9	<a href="mailto:service@so-net.net.tw">service@so-net.net.tw</a>	0	1	00H	0.0%
10	<a href="mailto:jordan.bear@msa.hinet.net">jordan.bear@msa.hinet.net</a>	0	2	00H	0.0%
11	<a href="mailto:support@dyndns.com">support@dyndns.com</a>	0	1	00H	0.0%
12	<a href="mailto:chnserv@eettaiwan.com">chnserv@eettaiwan.com</a>	0	1	00H	0.0%
13	<a href="mailto:reply@coversexperts.messages1.com">reply@coversexperts.messages1.com</a>	0	1	00H	0.0%
14	<a href="mailto:tcevent@microsoft.com">tcevent@microsoft.com</a>	0	1	00H	0.0%
15	<a href="mailto:edm@maildj.com">edm@maildj.com</a>	0	2	00H	0.0%
16	<a href="mailto:reply@wagerline.messages1.com">reply@wagerline.messages1.com</a>	0	1	00H	0.0%
17	<a href="mailto:hola@mh.easyuse.com.tw">hola@mh.easyuse.com.tw</a>	0	1	00H	0.0%

### The sender list

**Step7** Click **Sender** mail address of magafifa@pchome.com.tw, it shows the Attached, Received Time, Subject, Mail Size, and Quarantine information.

- Select the mails saved in Quarantine to training. In **Spam List**, click **Training**.
- In the spam list confirm window, click **OK**, then the mails will be training to be the non-spam mails.
- Select the mails saved in quarantine to retrieve. In **Spam List**, click **Retrieve**.
- In retrieve mail window, set the **Sender** and **Recipient** then click **OK**. The mails can be retrieved by the assigned recipient.

Spam List				
Top Received Time: 1 - 1				
richard.sunny@msa.hinet.net -> alex_tien@mail2000-7.so-net.net.tw				
	Subject	Received Time	Mail Size	Quarantine
<input type="checkbox"/>	- **S** 4	07/05 20:32	3.7 KB	

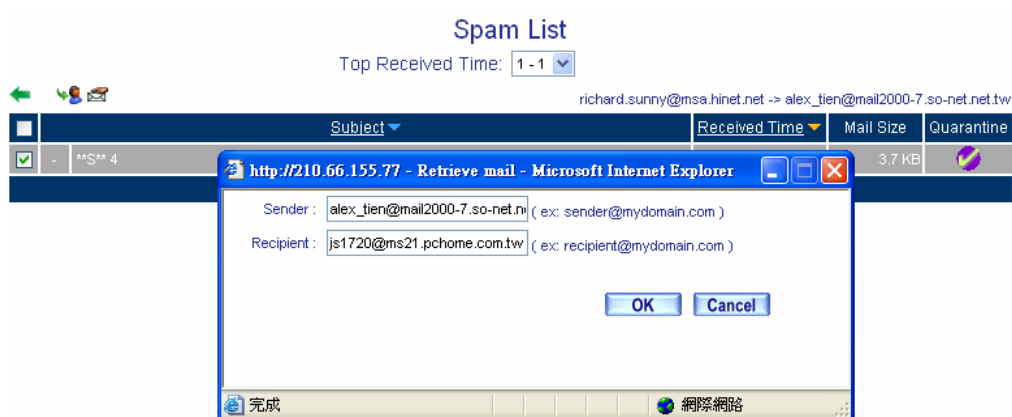
The spam list



In **Sender List**, the MIS engineer can only click the mail account which has been detected to send the spam mail.



Spam mail for training



Retrieve the spam mail

## Example 2

Set the CS-2000 to be the gateway, and use the whitelist and blacklist to filter the mails. (Set the mail server in DMZ and use transparent mode.)

**Step1** In **DMZ**, set a mail server, the network adapter IP is 61.11.11.12, DNS correspond to the external DNS server, and server name is test.com.

**Step2** In **Address** → **DMZ**, add the following settings :

Name▼	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Mail_Server	61.11.11.12/255.255.255.255	00:11:D8:70:FF:84	In Use

The mail server correspond to name in address

**Step3** In **Service** → **Group**, add the following setting :

Group name▼	Service	Configure
Mail_Service	DNS,IMAP,POP3...	In Use
Main_Service	DNS,HTTP,POP3...	Modify Remove

New Entry

To set the group included POP3 and SMTP, or DNS

**Step4** In **Policy** → **WAN To DMZ** , add the following setting :

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mail_Server	Mail_Service			Modify Remove Pause	To 1 ▼

New Entry

Set the WAN To DMZ policy



**Step5** In **Policy → DMZ To WAN** , add the following settings :

Source	Destination	Service	Action	Option							Configure			Move
Mail_Server	Outside_Any	Mail_Service									Modify	Remove	Pause	To 1 ▼

[New Entry](#)

**Set the DMZ To WAN policy**

**Step6** In **Configure → Mail Relay** , add the following settings :

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
test.com ( 61.11.11.12)	Modify Remove
61.64.127.16 / 255.255.255.255	Modify Remove

[New Entry](#)

**The mail relay setting of the external mails send to internal mail server**



In **Mail Relay**, it can relay the mail to the assigned domain name which corresponds to the mail server.

**Step7** In **Anti-Spam → Setting**, add the following.

**Spam Setting**

☒ **Enable Anti-Spam**

The Mail Server is ☒ Internal (External user sends emails to internal mail server)  
☒ External (Internal user receives emails from external mail server)

---

The threshold score of spam mail is  (Max. 256 characters)

Add the spam string to the subject line  (Max. 256 characters)

☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)  
☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)  
☒ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)  
☒ Drop the first connection of new sender account (Greylist Filtering)  
☒ Verify sender account is valid (Use TCP port : 25 and UDP port : 53 to connect mail server)  
☒ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)  
☐ Add score tag to the subject line

---

Rule Priority: ☒ Personal Rule priority higher than Global Rule  
☐ Global Rule priority higher than Personal Rule

**Action of Spam Mail**

Internal Mail Server (External user sends emails to internal mail server) :

☐ Delete the spam mail  
☐ Deliver to the recipient  
☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com)  
☒ Store in the quarantine

---

External Mail Server (Internal user receives emails from external mail server) :

☒ Deliver to the recipient (Always enable)  
☒ Store in the quarantine

### The action of anti-spam setting



In **Action of Spam Mail**, when select **Delete the Spam mail**, the MIS engineer can not select **Deliver to the recipient**, **Store in the quarantine** and **Notice to the sender**. In other words, the CS-2000 will delete all the spam mails. In the **Spam Mail**, it still shows the related Lists.

**Step8** In **Anti-Spam → Whitelist** , add the following settings :

- Click **New Entry**.
- **Whitelist**, enter [share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw) .
- **Direction**, select **From**.
- Enable **Auto-Training**.
- Click **OK**.
- Click **New Entry** again.
- **Whitelist**, enter [share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw) .
- **Direction**, select **To**.
- Enable **Auto-Training**.
- Click **OK**.
- Click **New Entry** again .
- **Whitelist**, enter [josh@test.com](mailto:josh@test.com) .
- **Direction**, select **From**.
- Enable **Auto-Training**.
- Click **OK**.
- Click **New Entry** again.
- **Whitelist**, enter [josh@test.com](mailto:josh@test.com) .
- **Direction**, select **To**.
- Enable **Auto-Training**.
- Click **OK**.
- Complete the settings.

Add New Whitelist	
Mail Account	<input type="text" value="share2k01@yahoo.com.tw"/> <small><a href="#">Assist</a> (*@domain.com, * : wild character)</small>
Direction	From <input type="button" value="v"/>
Auto-Training	Enable <input type="button" value="v"/>

**Add whitelist setting 1**

Add New Whitelist	
Mail Account	share2k01@yahoo.com.tw <a href="#">Assist</a> (*@domain.com, * : wild character)
Direction	To ▼
Auto-Training	Enable ▼

### Add whitelist setting 2

Add New Whitelist	
Mail Account	josh@test.com <a href="#">Assist</a> (*@domain.com, * : wild character)
Direction	From ▼
Auto-Training	Enable ▼

### Add whitelist setting 3

Add New Whitelist	
Mail Account	josh@test.com <a href="#">Assist</a> (*@domain.com, * : wild character)
Direction	To ▼
Auto-Training	Enable ▼

### Add whitelist setting 4

Export Whitelist To Client

Import Whitelist From Client    (Max size 1 MBytes.)

Direction	Mail Account ▲	Auto-Training	Configure
From	share2k01@yahoo.com.tw		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
To	share2k01@yahoo.com.tw		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
From	josh@test.com		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
To	josh@test.com		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the whitelist setting



The MIS engineers can **Import Whitelist From Client**, in order to manage the related settings. On the other hand, the CS-2000 can clear the List and **Import Whitelist From Client**, when the **Whitelist** is in disorder.



When enable **Auto-Training**, the CS-2000 will identify the **Whitelist** to be the non-spam mails through training function depends on the training time setting.

**Step9** In **Anti-Spam → Blacklist** , add the following settings :

- Click **New Entry**.
- **Blacklist**, enter \*yahoo\*.
- **Direction**, select **From**.
- Enable **Auto-Training**.
- Click **OK**.
- Click **New Entry**.
- **Blacklist**, enter \*yahoo\*.
- **Direction**, select **To**.
- Enable **Auto-Training**.
- Click **OK**.
- Complete the settings.

Add New Blacklist	
Mail Account	*yahoo* <a href="#">Assist</a> (*@domain.com, * : wild character)
Direction	From ▼
Auto-Training	Enable ▼



**Add new blacklist setting 1**

Add New Blacklist	
Mail Account	*yahoo* <a href="#">Assist</a> (*@domain.com, * : wild character)
Direction	To ▼
Auto-Training	Enable ▼

**Add new blacklist setting 2**

Export Blacklist To Client

Import Blacklist From Client    (Max size 1 MBytes.)

Direction	Mail Account ▲	Auto-Training	Configure
From	*yahoo*		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
To	*yahoo*		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the blacklist setting



The MIS engineers can **Export Blacklist To Client**, in order to manage the related settings. On the other hand, the CS-2000 can clear the list and **Import Blacklist From Client**, when the **Blacklist** is disorder.



When enable **Auto-Training**, the CS-2000 will identify the **Blacklist** to be the spam mails through training function depends on the training time setting.



The MIS engineer can set the whitelist and blacklist **Address** to be the complete mail address ( For example, [josh@test.com](mailto:josh@test.com) , or string included \* ( For example , \*yahoo\* , it represents the mail account included the “ yahoo” string . )



The whitelist competency is higher than blacklist, so the CS-2000 will first filter the **Whitelist mails**, and then process the **Blacklist mails**.

- Step10** When the external yahoo mail account send the mails to the recipient of [josh@test.com](mailto:josh@test.com) and [steve@test.com](mailto:steve@test.com) in test.com mail server under CS-2000 :
- If the sender mail account is [share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw) , both of the two recipient mail account will receive the sender's mails.
  - If the sender mail account is come from another sender's mail account ([share2k003@yahoo.com.tw](mailto:share2k003@yahoo.com.tw)) , then only [josh@test.com](mailto:josh@test.com) can receive the sender's mails. In other words, the CS-2000 will identify the mails send to [steve@test.com](mailto:steve@test.com) to be the spam mails and save it in quarantine.
  - After the CS-2000 filtered this mails, it will results the list in **Anti-Spam → Spam Mail**.  
( Click **Inbound → Internal** , to see the internal List . )

The Duration of Today ▼ Mail Direction : Inbound Inbound Mail Server : Internal External

No.	Recipient ▼	Total Spam ▼	Total Mail ▼	Duration	Spam %
1	<a href="mailto:steve@test.com">steve@test.com</a>	1	7	06H	14.3%
2	<a href="mailto:josh@test.com">josh@test.com</a>	1	7	06H	14.3%
Total		2	14		14.3%

Clear Data

### The spam mail list

- Step11** Click **Recipient** mail address of [steve@test.com](mailto:steve@test.com) . In **Sender List**, to check the **Total Spam** and **Total Mail**.

### Sender List

Recipient: [steve@test.com](mailto:steve@test.com)

No.	Sender ▼	Total Spam ▼	Total Mail ▼	Duration	Spam %
1	<a href="mailto:share2k003@yahoo.com.tw">share2k003@yahoo.com.tw</a>	1	1	00H	100.0%
2	<a href="mailto:123654@edm.yam.com">123654@edm.yam.com</a>	0	1	00H	0.0%
3	<a href="mailto:1482@mail.ms-edm.com.tw">1482@mail.ms-edm.com.tw</a>	0	1	00H	0.0%
4	<a href="mailto:edm@cms5.so-net.net.tw">edm@cms5.so-net.net.tw</a>	0	1	00H	0.0%
5	<a href="mailto:n15001.s4734.c24563683.t4527.i30.e448546377.d0@fans.nba.com">n15001.s4734.c24563683.t4527.i30.e448546377.d0@fans.nba.com</a>	0	1	00H	0.0%
6	<a href="mailto:nobody@yahoo.edyna.com">nobody@yahoo.edyna.com</a>	0	1	00H	0.0%
7	<a href="mailto:vincechase@ms96.url.com.tw">vincechase@ms96.url.com.tw</a>	0	1	00H	0.0%
Total		1	7		14.3%

### The sender list



- Step12** Click the **sender** mail address of [share2k003@yahoo.com.tw](mailto:share2k003@yahoo.com.tw) , it shows the information of the Attached, Subject, Received Time, Mail Size and Quarantine.
- Select the mail saved in quarantine to training. In **Spam List**, click **Training**.
  - In confirm training dialogue box, Click **OK**, the CS-2000 will identify mails to be non-spam mails.
  - Select the mails saved in quarantine to retrieve. In **Spam List**, click **Retrieve**.
  - In retrieve mail window, set the sender and recipient mail account, and then Click **OK**. To retrieve mails from the assigned recipient.

**Spam List**

Top Received Time: 1 - 1

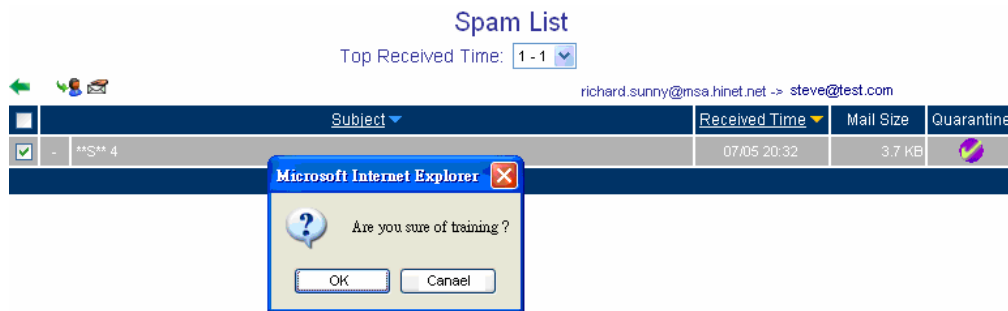
richard.sunny@msa.hinet.net -> steve@test.com

<input type="checkbox"/>	Subject	Received Time	Mail Size	Quarantine
<input type="checkbox"/>	- **S** 4	07/05 20:32	3.7 KB	

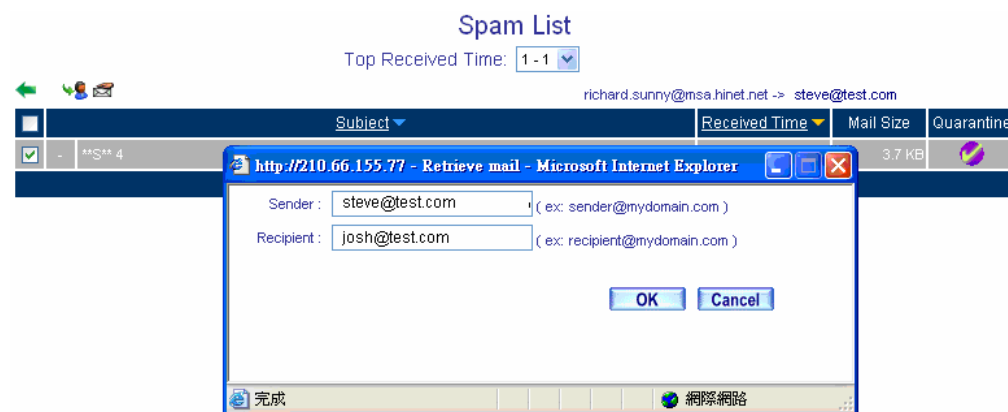
**The spam list**



In **Sender List**, the MIS engineer can only click the sender mail account which had been detected to send the spam mails.



The confirm training window



The retrieve mail window



When use the **Training** or **Retrieve** function, the MIS engineer must select the spam mails saved in **Quarantine**.



In **Anti-Spam → Spam Mail**, click **Clear**, and then the CS-2000 will delete all the list records. In other words, the MIS engineer can not find this deleted file in **Spam Mail** function.

### Example 3

Set the CS-2000 between the company's original gateway and mail server. Use the global rule to filter mails. (Set the mail server in DMZ, and use transparent mode.)

The Company's LAN segment : 172.16.1.0/16 in original gateway

WAN port IP is 61.11.11.11

CS-2000's WAN1 port IP is 172.16.1.12

**Step1** In **DMZ**, set a mail server, the network adapter IP is 172.16.1.13, DNS correspond to the external DNS server, and server name is test.com.

**Step2** In **Address → DMZ**, add the following settings :

Name▼	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
Mail_Server	172.16.1.13 / 255.255.255.255	00:11:D8:70:FF:84	In Use

The mail server correspond to name in address

**Step3** In **Service → Group**, add the following setting :

Group name▼	Service	Configure
Mail_Service	DNS,IMAP,POP3...	In Use
Main_Service	DNS,HTTP,POP3...	Modify Remove

New Entry

To set the group included POP3 and SMTP or DNS

**Step4** In **Policy → WAN To DMZ** , add the following setting :

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Mail_Server	Mail_Service						Modify	Remove	Pause	To 1 ▼

[New Entry](#)

Set the WAN To DMZ policy

**Step5** In **Policy → DMZ To WAN** , add the following settings :

Source	Destination	Service	Action	Option				Configure			Move
Mail_Server	Outside_Any	Mail_Service						Modify	Remove	Pause	To 1 ▼

[New Entry](#)

Set the DMZ To WAN policy

**Step6** In **Configure → Mail Relay** , add the following settings :

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
test.com ( 172.16.1.13 )	Modify Remove
61.64.127.16 / 255.255.255.255	Modify Remove

[New Entry](#)

The mail relay of the external mails send to internal mail server



In **Mail Relay**, it can relay the mail to the assigned domain name which corresponds to the mail server. On the other hand, the function also can allow specific external IP use the internal mail account to send mails.

**Step7** In **Anti-Spam → Setting** , add the following settings :

**Spam Setting**

☒ Enable Anti-Spam

The Mail Server is ☒ Internal (External user sends emails to internal mail server)  
☒ External (Internal user receives emails from external mail server)

---

The threshold score of spam mail is  (Max. 256 characters)

Add the spam string to the subject line  (Max. 256 characters)

☒ Check spam fingerprint (Use TCP port : 2703 and UDP port : 53 to connect database server) [Test](#)  
☒ Enable Bayesian filtering (Bayesian filtering does not work until database has at least 200 spams and 200 hams)  
☒ Enable spam signature push update (Use TCP port : 1153 and UDP port : 1153 to update signature) [Test](#)  
☒ Drop the first connection of new sender account (Greylist Filtering)  
☒ Verify sender account is valid (Use TCP port : 25 and UDP port : 53 to connect mail server)  
☒ Check sender IP address in RBL (Use UDP port : 53 to connect DNS server) [Test](#)  
☐ Add score tag to the subject line

---

Rule Priority: ☒ Personal Rule priority higher than Global Rule  
☐ Global Rule priority higher than Personal Rule

**Action of Spam Mail**

Internal Mail Server (External user sends emails to internal mail server) :

☐ Delete the spam mail  
☐ Deliver to the recipient  
☐ Forward to :  (Max. 128 characters, ex: user@mydomain.com)  
☒ Store in the quarantine

---

External Mail Server (Internal user receives emails from external mail server) :

☒ Deliver to the recipient (Always enable)  
☒ Store in the quarantine

### The action of anti-spam setting



The mails which fit to the **Global Rule**, will be processed depends on **Global Rule → Action** .

**Step8** In **Anti-Spam → Global Rule** , add the following settings :

- Click **New Entry**.
- **Rule Name**, enter HamMail.
- **Comments**, enter Ham Mail.
- **Combination**, select **Or**.
- **Classification**, select Ham (Non-Spam).
- Enable **Auto-Training**.
- In first **Item**, select **From**. **Condition**, select Contains. **Pattern**, enter share2k01.
- Click **Next Row**.
- In second **Item**, select **To**. **Condition**, select Contains. **Pattern**, enter share2k01.
- Click **Next Row**.
- In third **Item**, select **From**. **Condition**, select Contains. **Pattern**, enter josh.
- Click **Next Row**.
- In fourth **Item**, select **To**. **Condition**, select Contains. **Pattern**, enter josh.
- Click **OK**.

Rule Name :  (Max. 16 characters)    Comments :  (Max. 20 characters)

Combination :     Action :

Classification :     Auto-Training :     [Assist](#)

Item	Condition	Pattern (Max. 30 characters)	Configure
<input type="button" value="From"/>	<input type="button" value="Contains"/>	<input type="text" value="share2k01"/>	<input type="button" value="Remove"/>
<input type="button" value="To"/>	<input type="button" value="Contains"/>	<input type="text" value="share2k01"/>	<input type="button" value="Remove"/>
<input type="button" value="From"/>	<input type="button" value="Contains"/>	<input type="text" value="josh"/>	<input type="button" value="Remove"/>
<input type="button" value="To"/>	<input type="button" value="Contains"/>	<input type="text" value="josh"/>	<input type="button" value="Next Row"/> <input type="button" value="Remove"/>

**The first global rule setting**

Rule Name	Classification	Action	Comments	Configure	Move
HamMail	Ham	- - -	Ham Mail	<a href="#">Modify</a> <a href="#">Remove</a>	To 1 

[New Entry](#)

### Complete the first global rule setting



In **Global Rule** setting, when the MIS engineer select **Classification** → **Ham (Non-Spam)**, the **Action** function would be disabled. It is because the CS-2000 will send the non-spam mails to recipient directly without any additional process.

**Step9** In **Anti-Spam → Global Rule** , add the following settings :

- Click **New Entry**.
- **Rule Name**, enter SpamMail.
- **Comments** enter Spam Mail.
- **Combination**, select **Or**.
- **Action**, select Store in quarantine.
- **Classification**, select **Spam**.
- Enable **Auto-Training**.
- In first **Item**, select **From**. **Condition**, select Contains. **Pattern**, enter yahoo.
- Click **Next Row**.
- In second **Item**, select **To**. **Condition**, select Contains. **Pattern**, enter yahoo.
- Click **OK**.

Rule Name :  (Max. 16 characters)    Comments :  (Max. 20 characters)

Combination :     Action :  ---

Classification :     Auto-Training :  Assist

Item	Condition	Pattern (Max. 30 characters)	Configure
<input type="text" value="From"/>	<input type="text" value="Contains"/>	<input type="text" value="yahoo"/>	<input type="button" value="Remove"/>
<input type="text" value="To"/>	<input type="text" value="Contains"/>	<input type="text" value="yahoo"/>	<input type="button" value="Next Row"/> <input type="button" value="Remove"/>

### The second global rule setting

Rule Name	Classification	Action	Comments	Configure	Move
HamMail	Ham	---	Ham Mail	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To 1 <input type="button" value="v"/>
SpamMail	Spam	Store in quarantine	Spam Mail	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To 2 <input type="button" value="v"/>

### Complete the second global rule setting



In **Global Rule**, when MIS engineer select **Classification → Spam**, then he can only select one of the options in **Action → Store in quarantine, Delete spam mail, Deliver to the recipient or Forward to**.





The CS-2000's Anti-Spam default rule priority are **Whitelist of Personal Rule → Blacklist of Personal Rule → Global Rule → Whitelist → Blacklist → The default mail filtering rule setting → check fingerprint database → Bayesian filtering → spam signature → check sender account → check sender IP address in RBL** . In **Global Rule**, the CS-2000 will make the comparison depends on rule priority.



Select one of the mails from **Outlook Express** , and **right click on the mail → Properties → Details** , it shows all the mail headers, the system can use these mail headers to be the reference in **Global Rule → Condition and Item**.

**Step10** When the external yahoo mail account send the mails to the recipient of [josh@test.com](mailto:josh@test.com) and [steve@test.com](mailto:steve@test.com) in test.com mail server under CS-2000 :

- If the sender mail account is [share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw) , both of the two recipient mail account will receive the sender's mails.
- If the sender mail account is come from another sender's mail account ([share2k003@yahoo.com.tw](mailto:share2k003@yahoo.com.tw)) , then only [josh@test.com](mailto:josh@test.com) can receive the sender's mails. In other words, the CS-2000 will identify the mails send to [steve@test.com](mailto:steve@test.com) to be the spam mails and save it in quarantine.
- After the CS-2000 filtered this mails, it will results the list in **Anti-Spam → Spam Mail**.  
( Click **Inbound → Internal**, to see the Internal list. )

Mail Direction: **Inbound** **Inbound**  
Mail Server: **Internal** **External**

The Duration of Today

No.	Recipient	Total Spam	Total Mail	Duration	Spam %
1	<a href="mailto:steve@test.com">steve@test.com</a>	1	7	06H	14.3%
2	<a href="mailto:josh@test.com">josh@test.com</a>	1	7	06H	14.3%
Total		2	14		14.3%

[Clear Data](#)

### The spam mail list

**Step11** Click **Recipient** mail address of [steve@test.com](mailto:steve@test.com) . In **Sender List**, to check the **Total Spam** and **Total Mail**.

### Sender List

Recipient: [steve@test.com](mailto:steve@test.com)

No.	Sender	Total Spam	Total Mail	Duration	Spam %
1	<a href="mailto:share2k003@yahoo.com.tw">share2k003@yahoo.com.tw</a>	1	1	00H	100.0%
2	<a href="mailto:123654@edm.yam.com">123654@edm.yam.com</a>	0	1	00H	0.0%
3	<a href="mailto:1482@mail.ms-edm.com.tw">1482@mail.ms-edm.com.tw</a>	0	1	00H	0.0%
4	<a href="mailto:edm@cms5-so-net.net.tw">edm@cms5-so-net.net.tw</a>	0	1	00H	0.0%
5	<a href="mailto:n15001.s4734.c24563683.t4527.130.e448546377.d0@fans.nba.com">n15001.s4734.c24563683.t4527.130.e448546377.d0@fans.nba.com</a>	0	1	00H	0.0%
6	<a href="mailto:nobody@yahoo.edyna.com">nobody@yahoo.edyna.com</a>	0	1	00H	0.0%
7	<a href="mailto:vincechase@ms96.url.com.tw">vincechase@ms96.url.com.tw</a>	0	1	00H	0.0%
Total		1	7		14.3%

### The sender list

- Step12** Click the **Sender** mail address of [share2k003@yahoo.com.tw](mailto:share2k003@yahoo.com.tw) , it shows the information of the Attached, Subject, Received Time, Mail Size and Quarantine.
- Select the mail saved in quarantine to training. In **Spam List**, click **Training**.
  - In confirm training dialogue box, Click **OK**, the CS-2000 will identify mails to be non-spam mails.
  - Select the mails saved in quarantine to retrieve. In **Spam List**, click **Retrieve**.
  - In retrieve mail window, set the sender and recipient mail account, and then Click **OK**. To retrieve mails from the assigned recipient.

**Spam List**

Top Received Time: 1 - 1

richard.sunny@msa.hinet.net -> steve@test.com

<input type="checkbox"/>	Subject	Received Time	Mail Size	Quarantine
<input type="checkbox"/>	- **S** 4	07/05 20:32	3.7 KB	

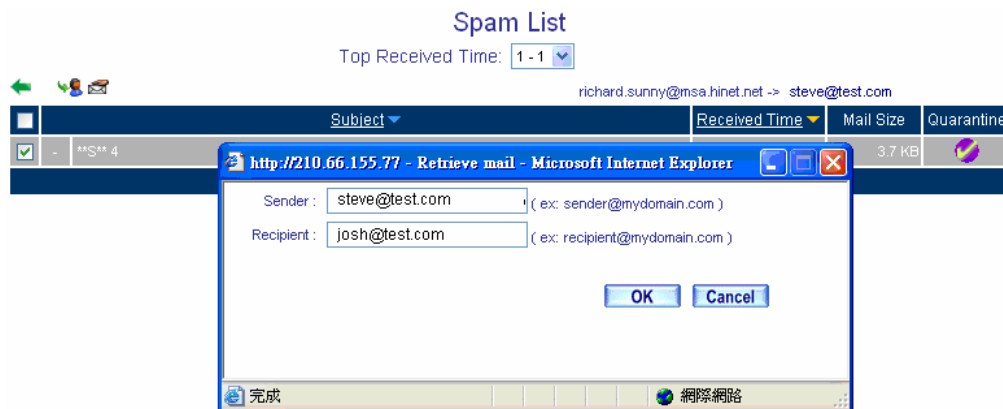
**The Spam List**



In **Sender List**, the MIS engineer can only click the sender mail account which had been detected to send the spam mails.



The confirm training window



The retrieve mail window



When use the **Training** or **Retrieve** function, the MIS engineer must select the spam mails saved in **Quarantine**.



In **Anti-Spam → Spam Mail**, click **Clear**, and then the CS-2000 will delete all the list records. In other words, the MIS engineer can not find this deleted file in **Spam Mail** function.

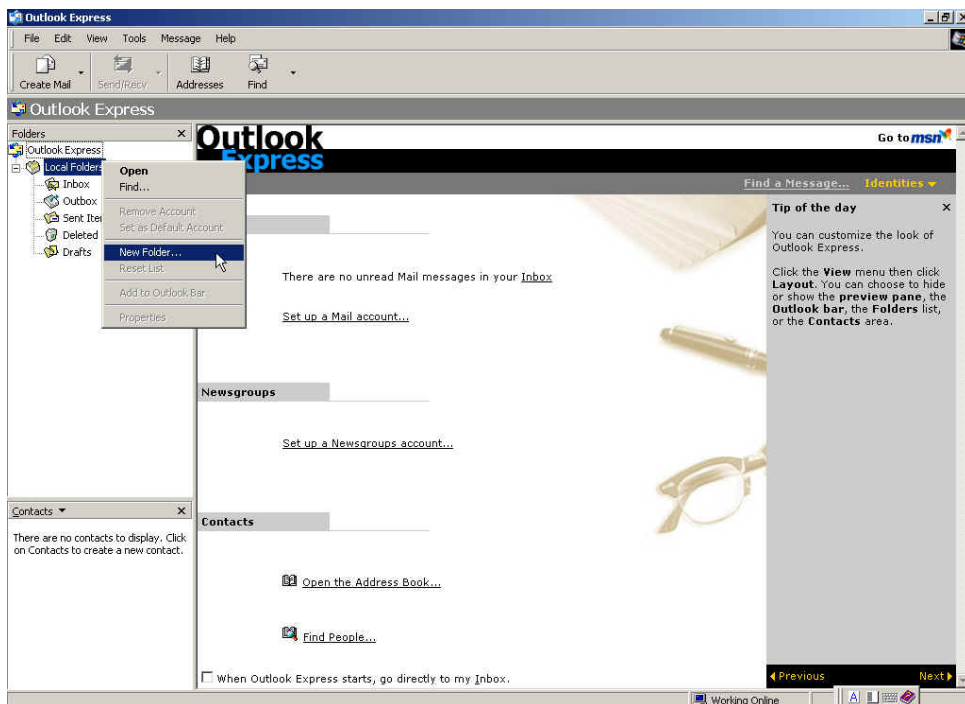
## Example 4

Use spam or non-spam mail training to improve the Bayesian filtering. ( For example, Outlook Express )

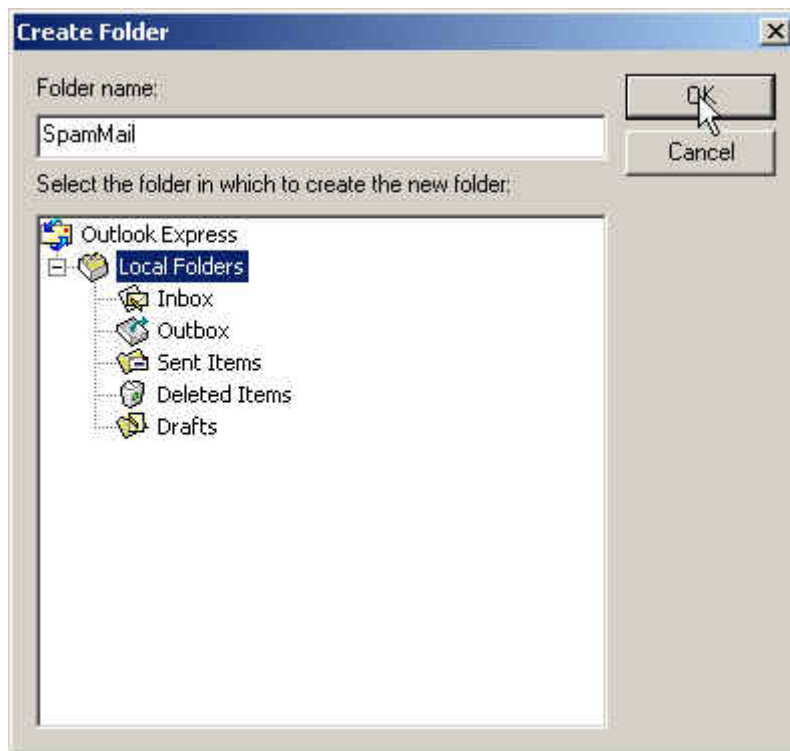
To identify the mails to be spam mails through training.

**Step1** In **Outlook Express** , add a new folder called **SpamMail** :

- Right click on **Local Folders**, and select **New Folder**.
- In **Create Folder** → **Folder name**, enter **SpamMail**, and then click **OK**.



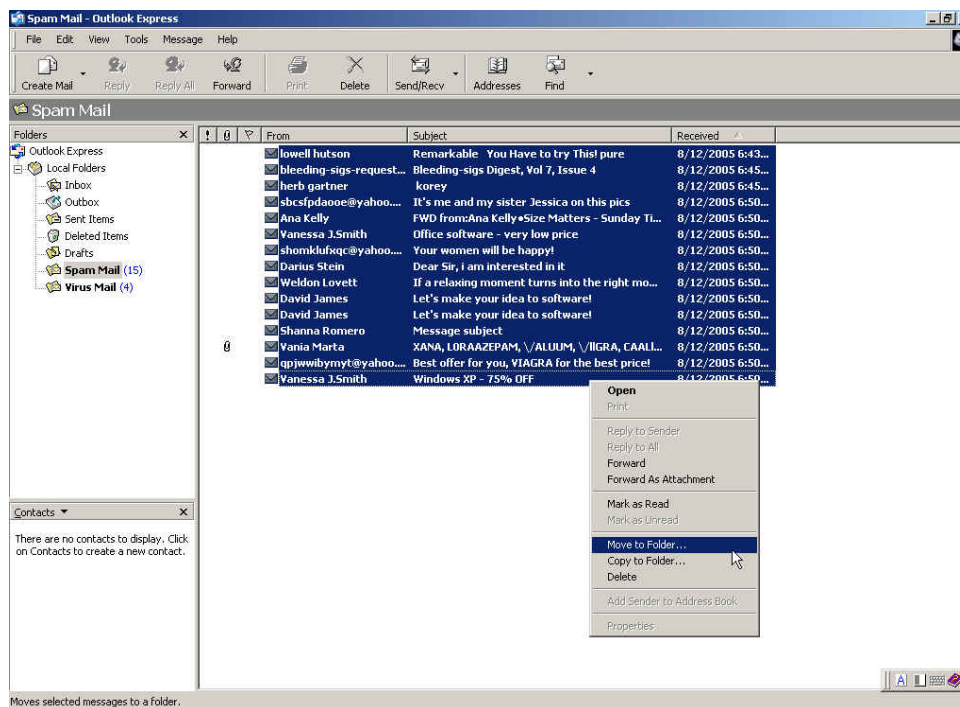
Create new folder



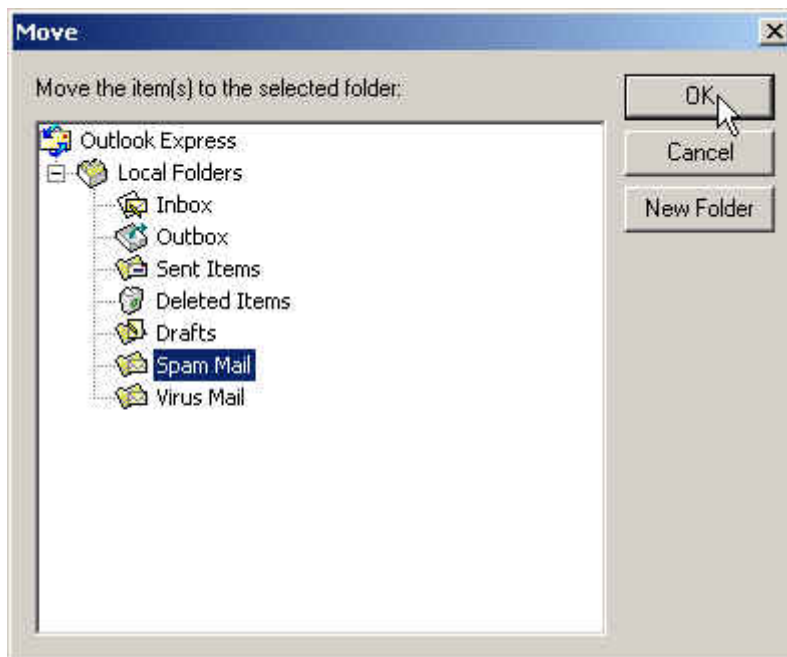
The create folder window

**Step2** In **Outlook Express** → **Inbox** , move the spam mails to the spam mail folder :

- In **Inbox**, right click on all the selected spam mails, and select **Move to Folder**.
- In **Move** window, select **Spam mail** folder, click **OK**.



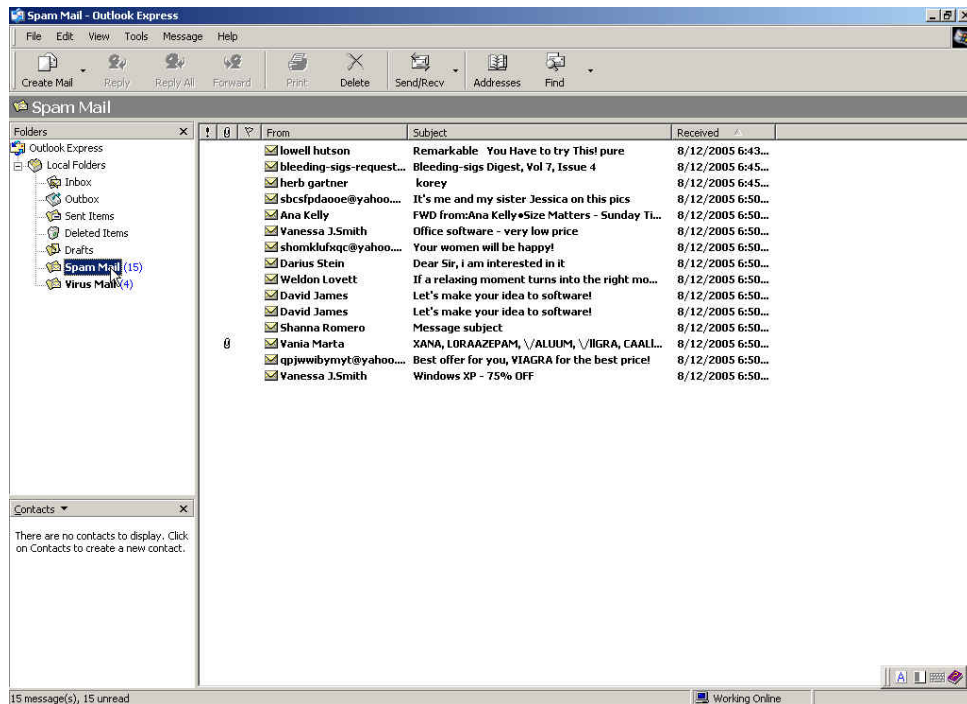
Move all the selected spam mails



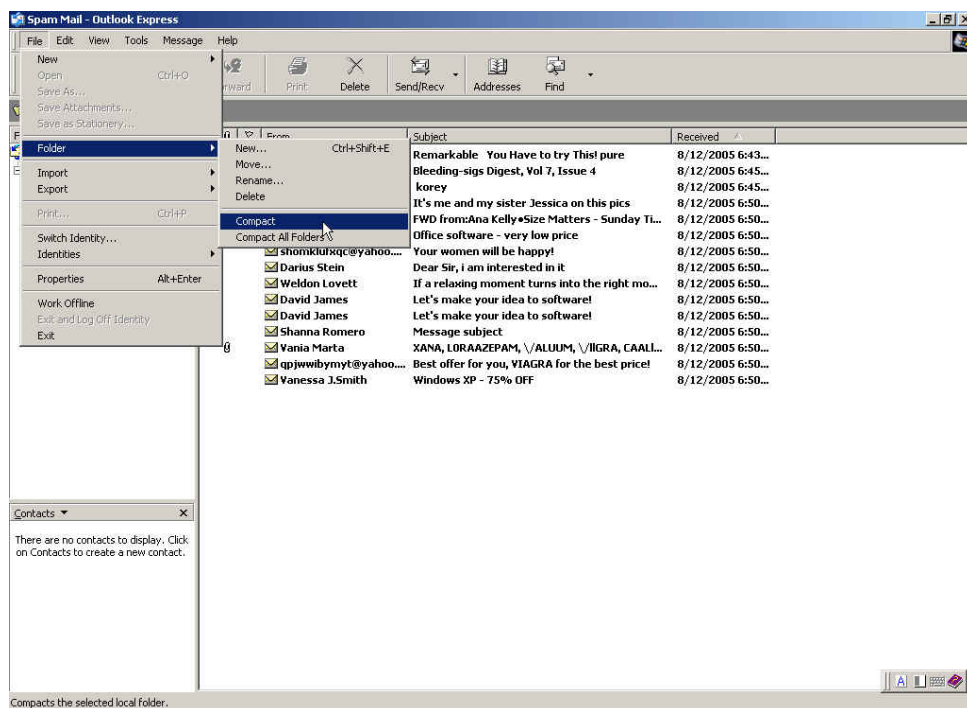
Move all the selected spam mails to the spam mail folder

**Step3** In **Outlook Express** → **SpamMail** folder, to compact the spam mail folder and import it to CS-2000's training system.

- Click **Spam Mail** folder.
- In **File**, select **Folder** → **Compact**.



Select spam mail folder

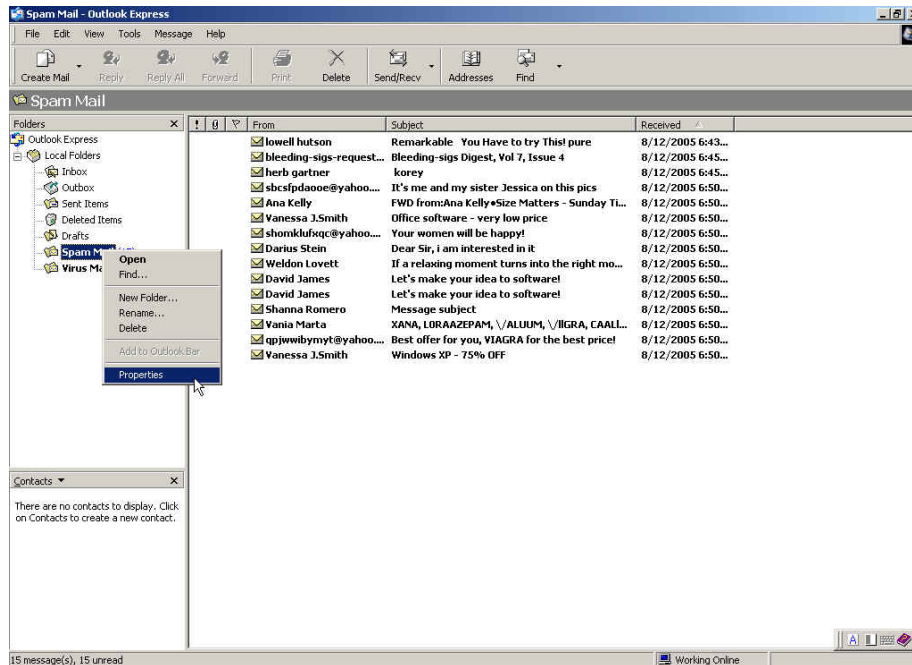


Compact the spam mail folder

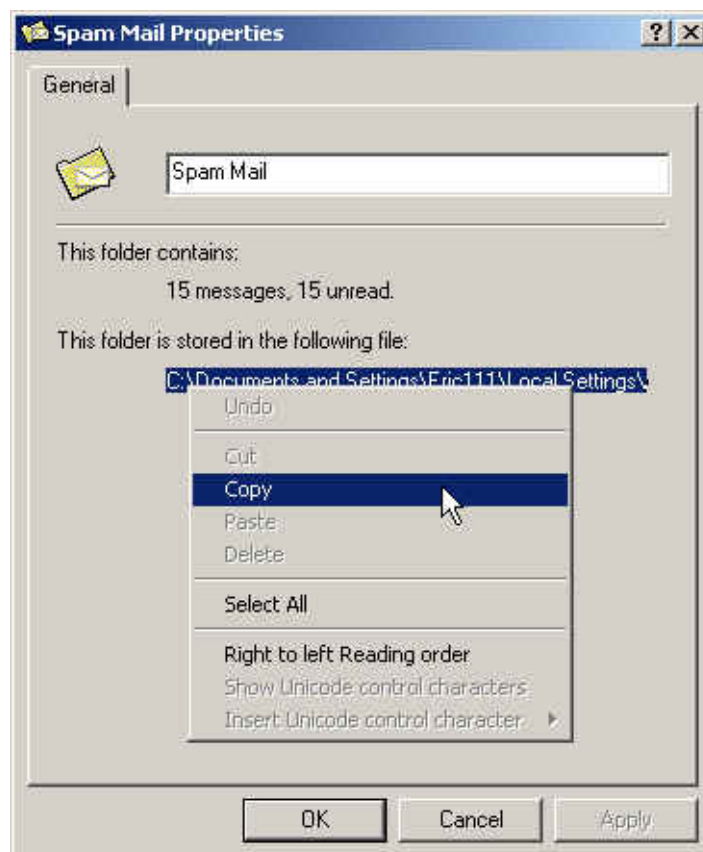


**Step4** In **Outlook Express** → **SpamMail** , copy the folder path and import it to CS-2000's training system :

- Right click on **SpamMail** folder, and select **Properties**.
- In **SpamMail Properties**, copy the folder saved path.



Select spam mail folder



Copy the spam mail folder saved path

**Step5** In **Anti-Spam → Training → Spam Mail for Training** , enter the following settings :

- In **Import Spam Mail for Training**, paste the **SpamMail folder** saved path.
- Click **OK**, to import the folder into CS-2000 and define the mails to be spam mails depends on the assigned training time.

The amount of spams in the database : 388

The amount of hams in the database : 195

Bayesian filtering does not work until database has at least 200 spams and 200 hams

### Import the spam mail file log



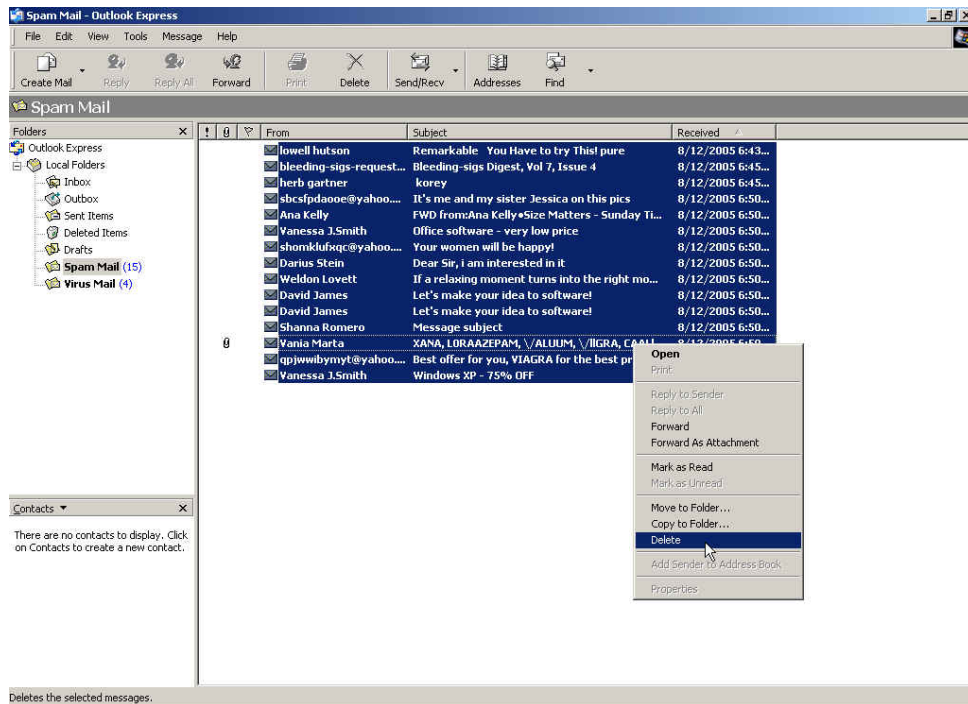
The imported training data can be any database files, and it has no extension restriction. On the other hand, the data format must be the ASCII.



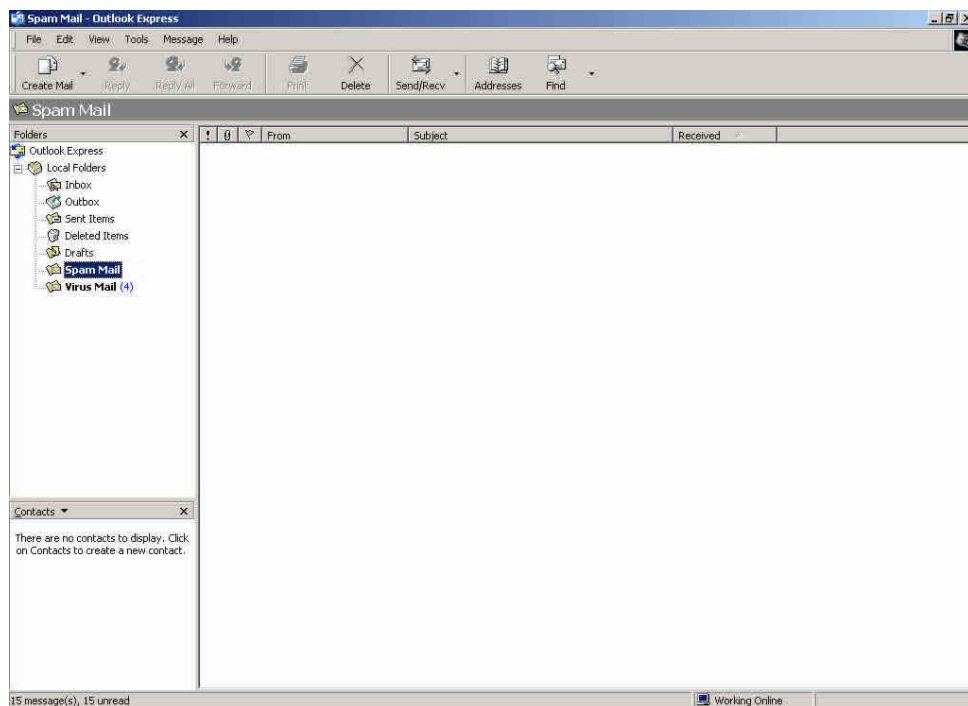
If the CS-2000's training data is a kind of **.pst** files which exported from the Microsoft Office Outlook , the MIS engineer must close the Microsoft Office Outlook then import the training data to CS-2000.

**Step6** In **Outlook Express** → **SpamMail** , delete all the spam mails , in order to easy compact and import the training data into CS-2000 :

- In **SpamMail** folder, right click on all the selected mails, and select **Delete**.
- In **SpamMail** folder, to confirm all the mails are deleted.



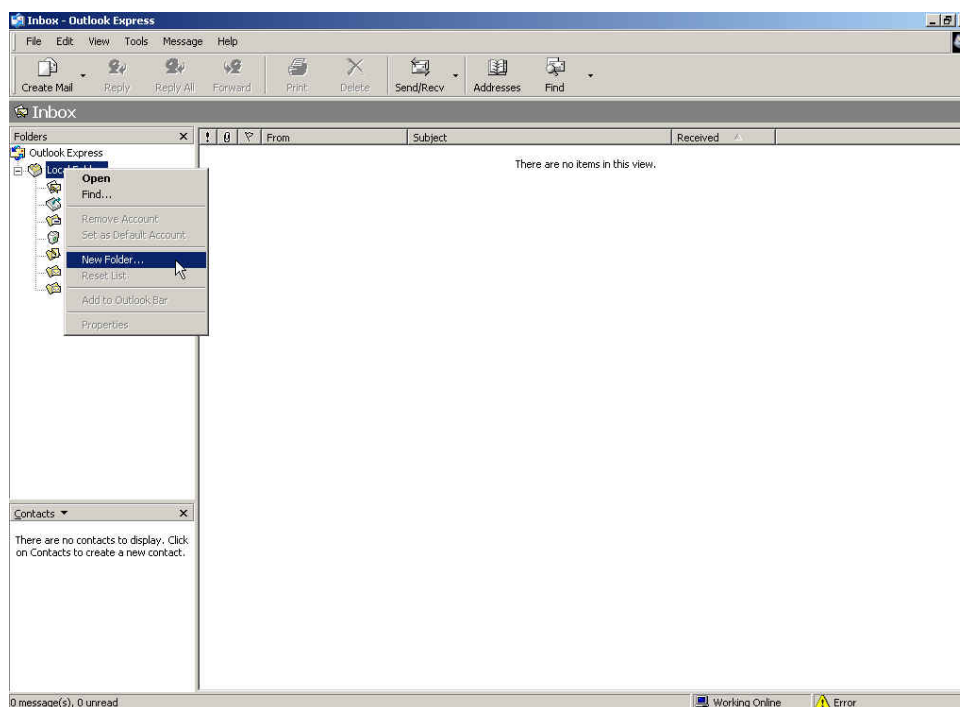
To delete all the spam mails in the folder



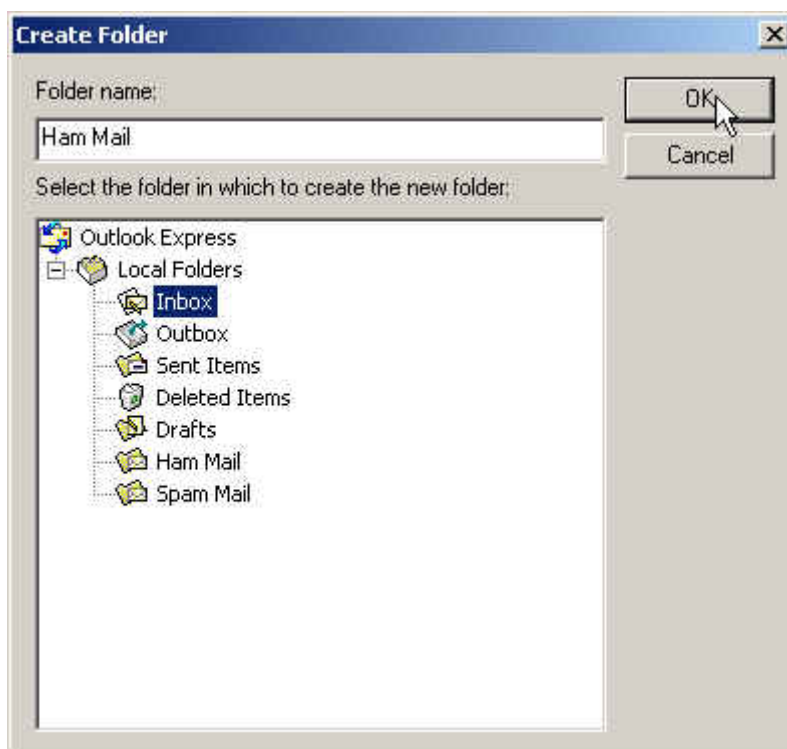
To confirm all the spam mails are deleted in the folder

To identify the mails to be the non-spam mails through training.

- Step1** In **Outlook Express** , add a new folder called **HamMail** :
- Right click on **Local Folders**, and select **New Folder**.
  - In **Create Folder** → **Folder name**, enter **HamMail**, and then click **OK**.



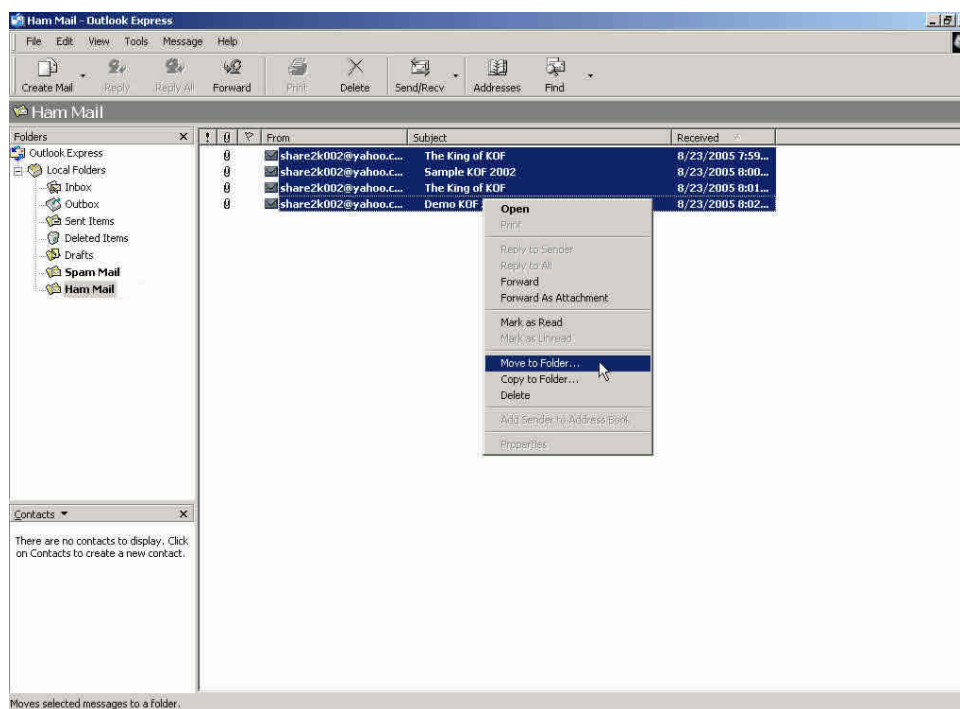
Select to add new folder



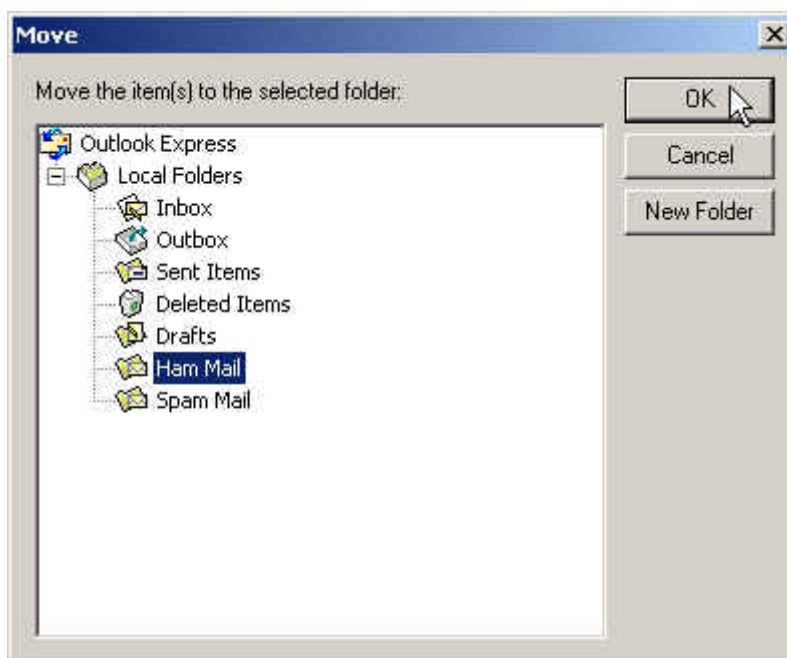
The create folder window

**Step2** In **Outlook Express → Inbox** , move the non- spam mails to the ham mail folder :

- In **Inbox**, right click on all the selected non-spam mails, and select **Move to Folder**.
- In **Move** window, select **Ham Mail Folder**, click **OK**.



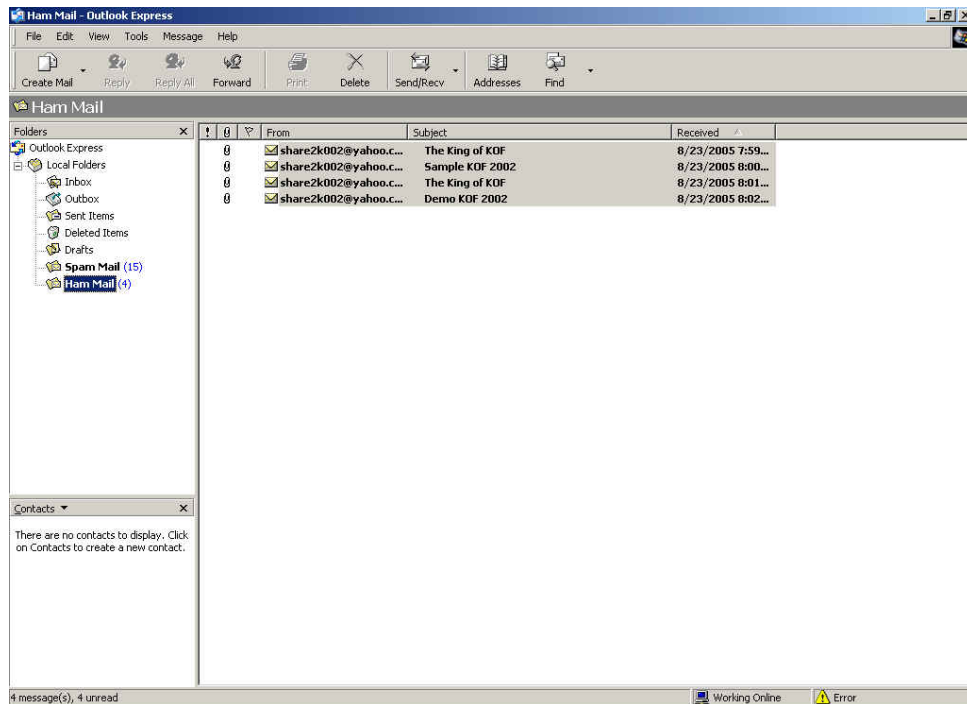
**Move the non-spam mails**



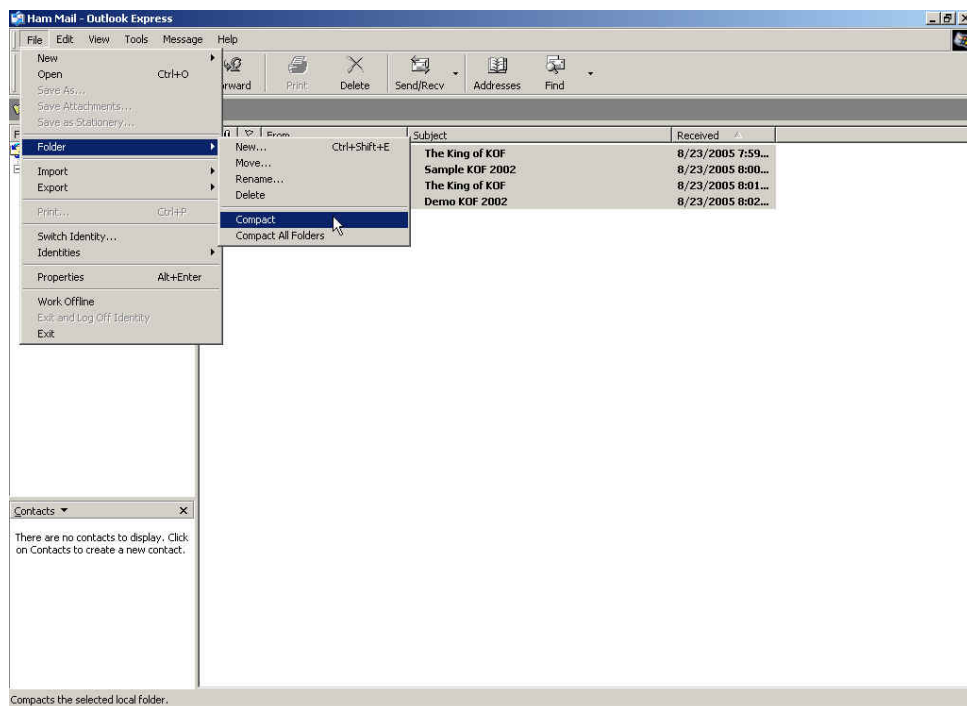
**To move the selected non-spam mails to the ham folder**

**Step3** In **Outlook Express** → **HamMail** folder, to compact the ham mail folder and import it to CS-2000's training system.

- Click **Ham Mail** folder.
- In **File**, select **Folder** → **Compact**.



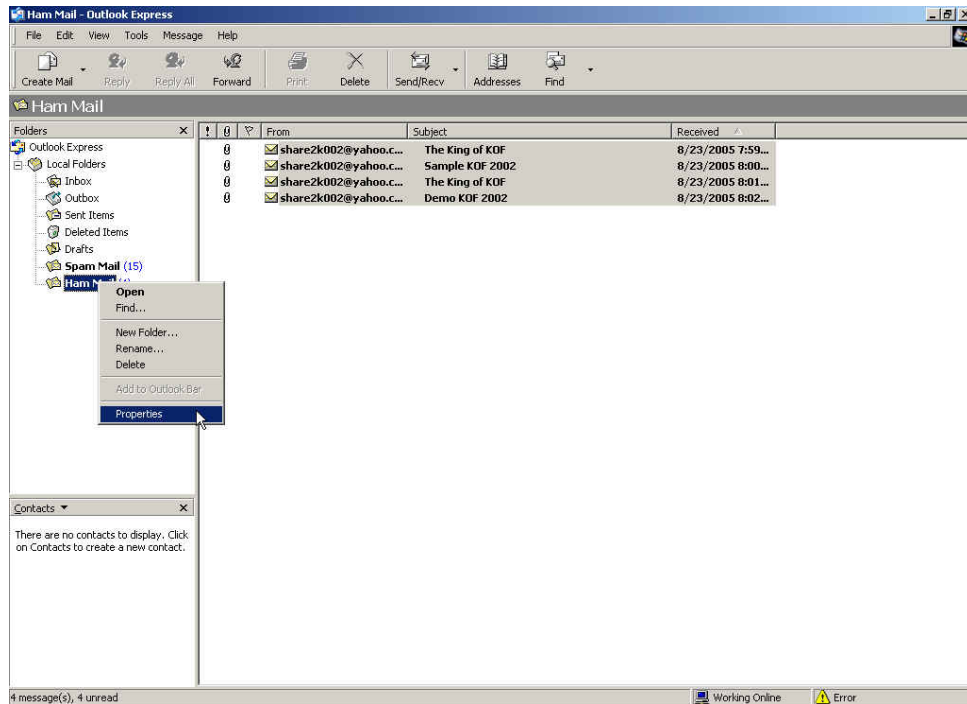
Select the ham mail folder



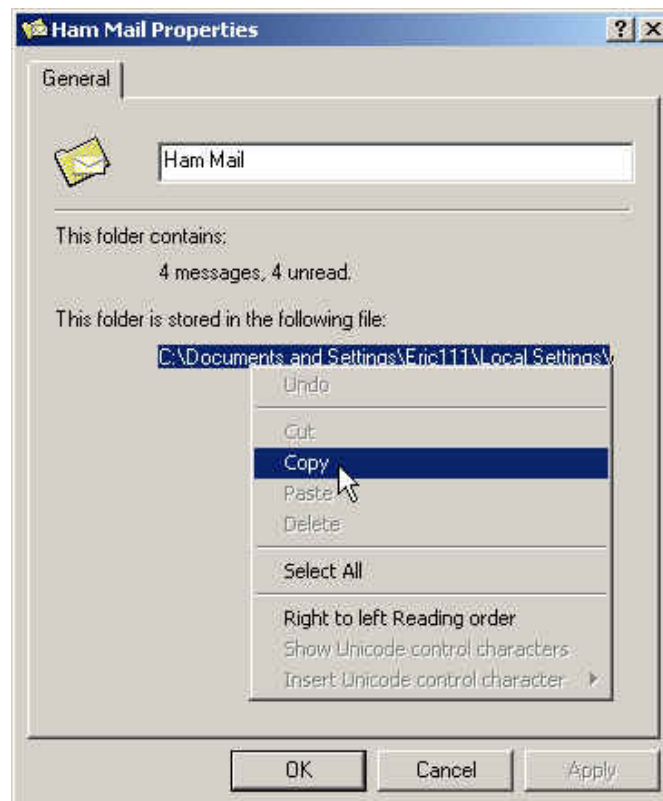
Compact the ham mail folder

**Step4** In **Outlook Express** → **HamMail** , copy the folder path and import it to CS-2000's training system :

- Right click on **HamMail** folder, and select **Properties**.
- In **HamMail Properties**, copy the folder saved path.



Select the ham mail properties



Copy the ham mail folder saved path

**Step5** In **Anti-Spam → Training → Ham Mail for Training** , enter the following settings :

- In **Import Ham Mail for Training**, paste the **HamMail folder** saved path.
- Click **OK**, to import the folder into CS-2000 and define the mails to be ham mails depends on the assigned training time.

The amount of spams in the database : 388

The amount of hams in the database : 195

Bayesian filtering does not work until database has at least 200 spams and 200 hams

**Training Database**

Export Training Database [Download](#)

Import Training Database  [Browse](#)

Reset Training Database [Reset Database](#)

**Spam Mail for Training**

Import Spam Mail from Client  [Browse](#) [Assist](#)

**Ham Mail for Training**

Import Ham Mail from Client  [Browse](#) [Assist](#)

**Spam Account for Training**

POP3 Server  characters, ex: my\_domain.com)

User name  characters, ex: spam)

Password  characters, ex: 5d2#k...)

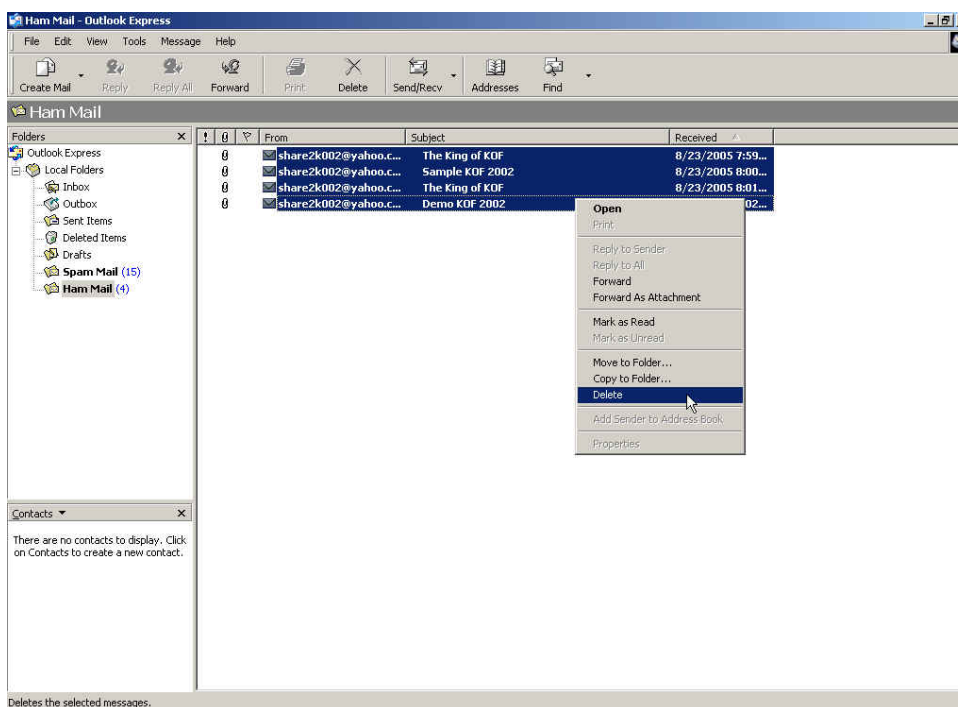
Spam account test [Account Test](#)

**To import the ham mail files into CS-2000**

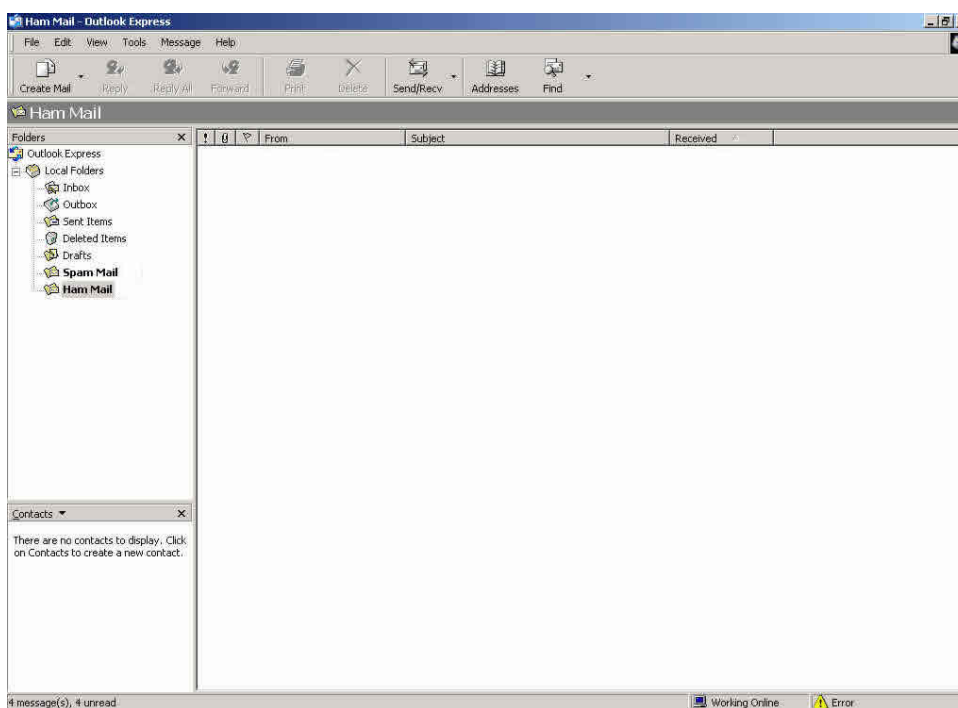


**Step6** In **Outlook Express** → **HamMail**, delete all the ham mails , in order to easy compact and import the training data into CS-2000 :

- In **HamMail** folder, right click on all the selected mails, and select **Delete**.
- In **HamMail** folder, to confirm all the mails are deleted.



To delete all the mails in ham mail folder



To confirm all the ham mails are deleted

## Example 5

Use spam or non-spam mail account training to improve the Bayesian filtering.

**Step1** To add a spam mail responds account in the mail server . ( For example, spam@test.com ) .

**Step2** To add a ham mails respond account in the mail server . ( For example, ham@test.com ) .

**Step3** In **Anti-Spam → Training → Spam Account for Training** , enter the recipient account setting (spam@test.com) :

- **POP3 Server**, enter test.com.
- **User Name**, enter spam.
- **Password**, enter spam.
- Click **OK**.

**Step4** In **Anti-Spam → Training → Ham Account for Training** , enter the recipient account setting (ham@test.com) :

- **POP3 Server**, enter test.com.
- **User Name**, enter ham.
- **Password**, enter ham.
- Click **OK**.

The amount of spams in the database : 388

The amount of hams in the database : 195

Bayesian filtering does not work until database has at least 200 spams and 200 hams

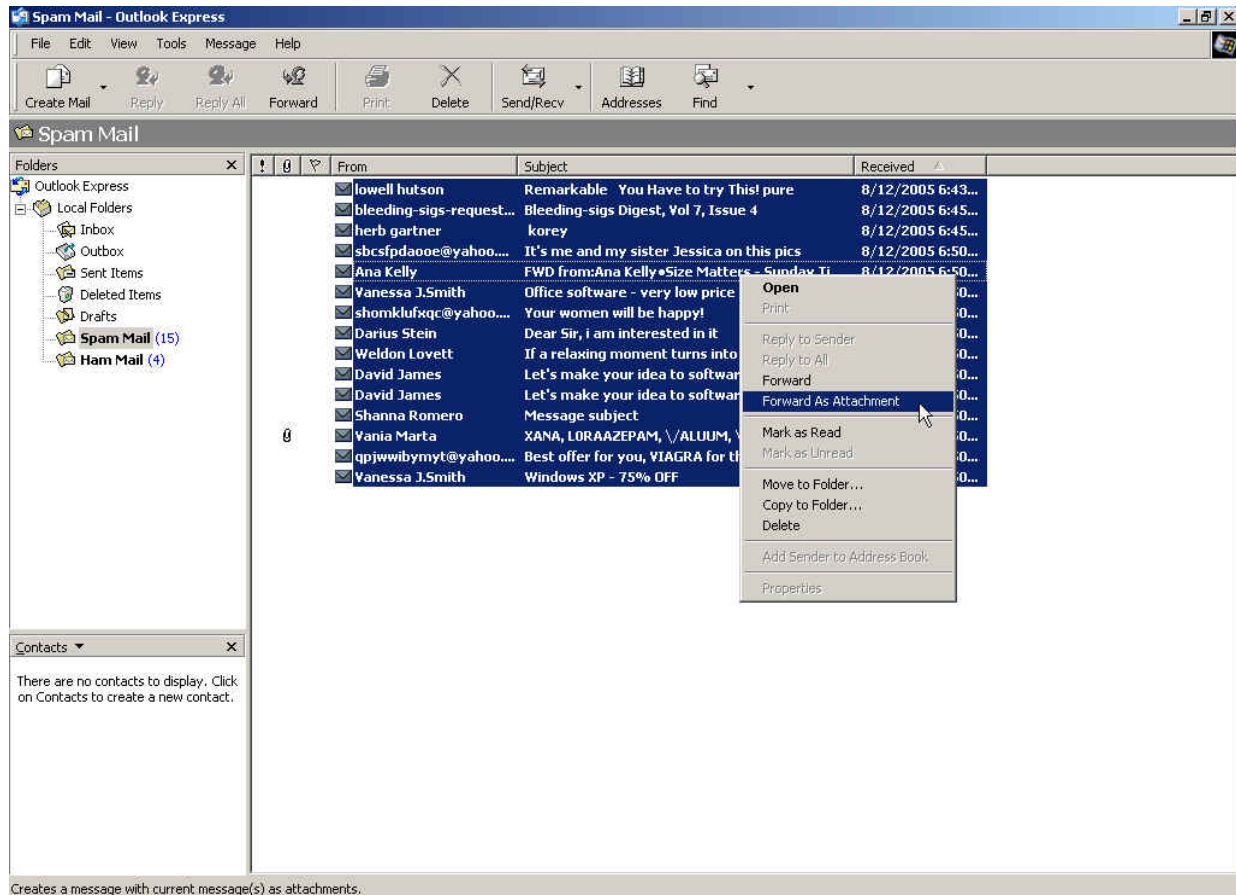
<b>Training Database</b>	
Export Training Database	<input type="button" value="Download"/>
Import Training Database	<input type="text"/> <input type="button" value="瀏覽..."/>
Reset Training Database	<input type="button" value="Reset Database"/>
<b>Spam Mail for Training</b>	
Import Spam Mail from Client	<input type="text"/> <input type="button" value="瀏覽..."/> <a href="#">Assist</a>
<b>Ham Mail for Training</b>	
Import Ham Mail from Client	<input type="text"/> <input type="button" value="瀏覽..."/> <a href="#">Assist</a>
<b>Spam Account for Training</b>	
POP3 Server	<input type="text" value="test.com"/> (Max. 60 characters, ex: my_domain.com)
User name	<input type="text" value="spam"/> (Max. 60 characters, ex: spam)
Password	<input type="password" value="...."/> (Max. 63 characters, ex: 5d2#k...)
Spam account test	<input type="button" value="Account Test"/>
<b>Ham Account for Training</b>	
POP3 Server	<input type="text" value="test.com"/> (Max. 80 characters, ex: my_domain.com)
User name	<input type="text" value="ham"/> (Max. 60 characters, ex: ham)
Password	<input type="password" value="..."/> (Max. 63 characters, ex: 5d2#k...)
Ham account test	<input type="button" value="Account Test"/>
<b>Training time</b>	
Training database starts at	<input type="text" value="01:00"/> / day
Train Now :	<input type="button" value="Training NOW"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

The ham and spam mail account for training

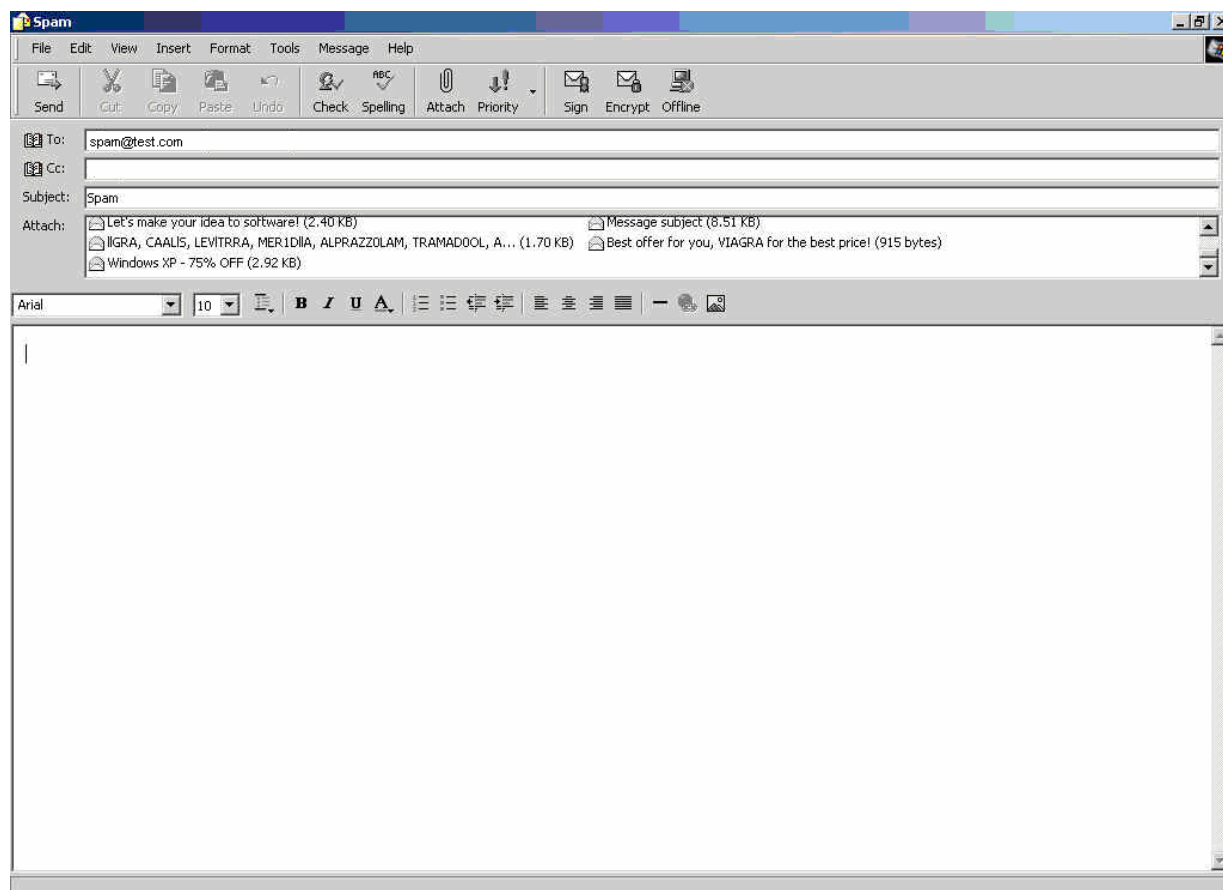
## To identify the mails to be spam mails through training

**Step5** In **Outlook Express**→ **Inbox** , to send the attached spam-mails to spam mails respond account via forwarding :

- In **Inbox**, Right click on the selected spam mails and select **Forward As Attachment**.
- In **New Message** → **To : ( Recipient )** , enter [spam@test.com](mailto:spam@test.com). **Subject**, enter Spam, and the content remained blank, and then click **Send**.



**To select all the spam mails**

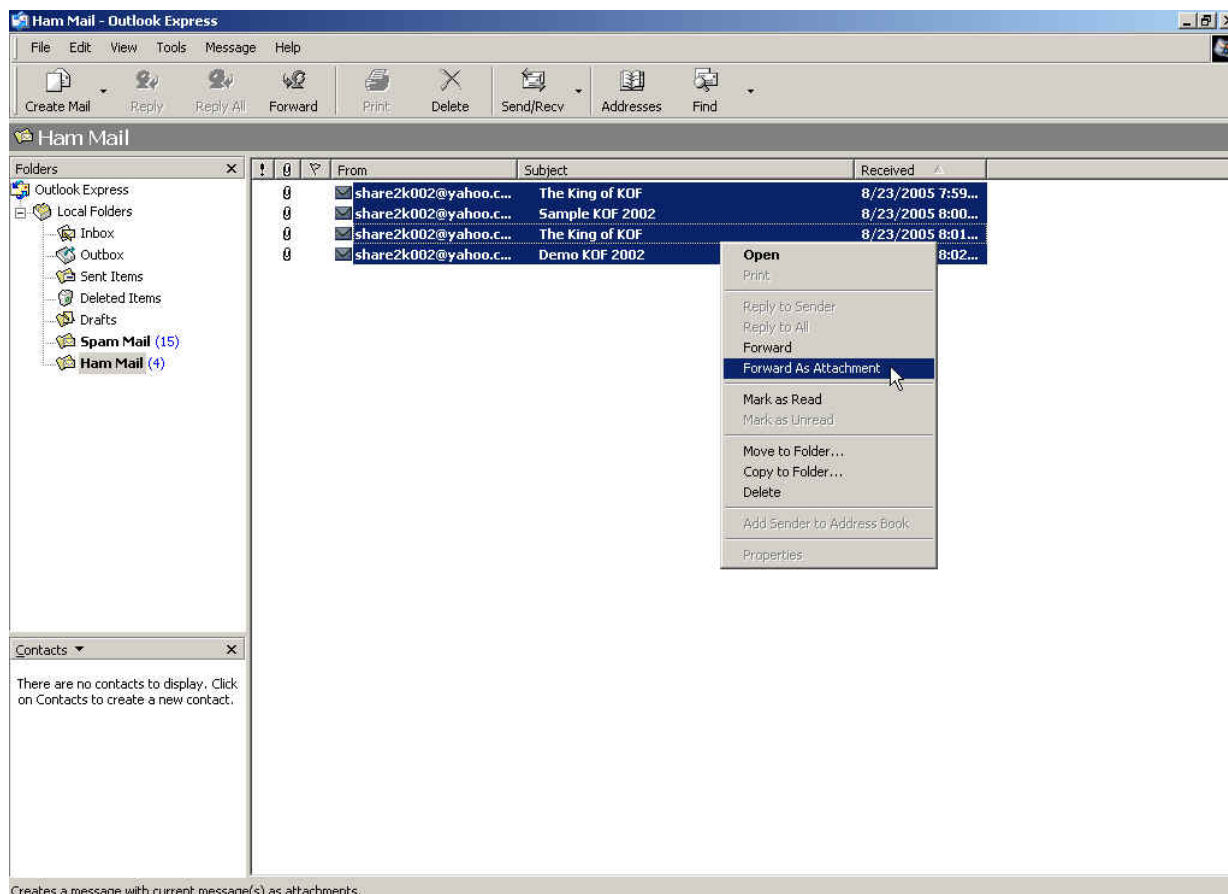


Forward the spam mails

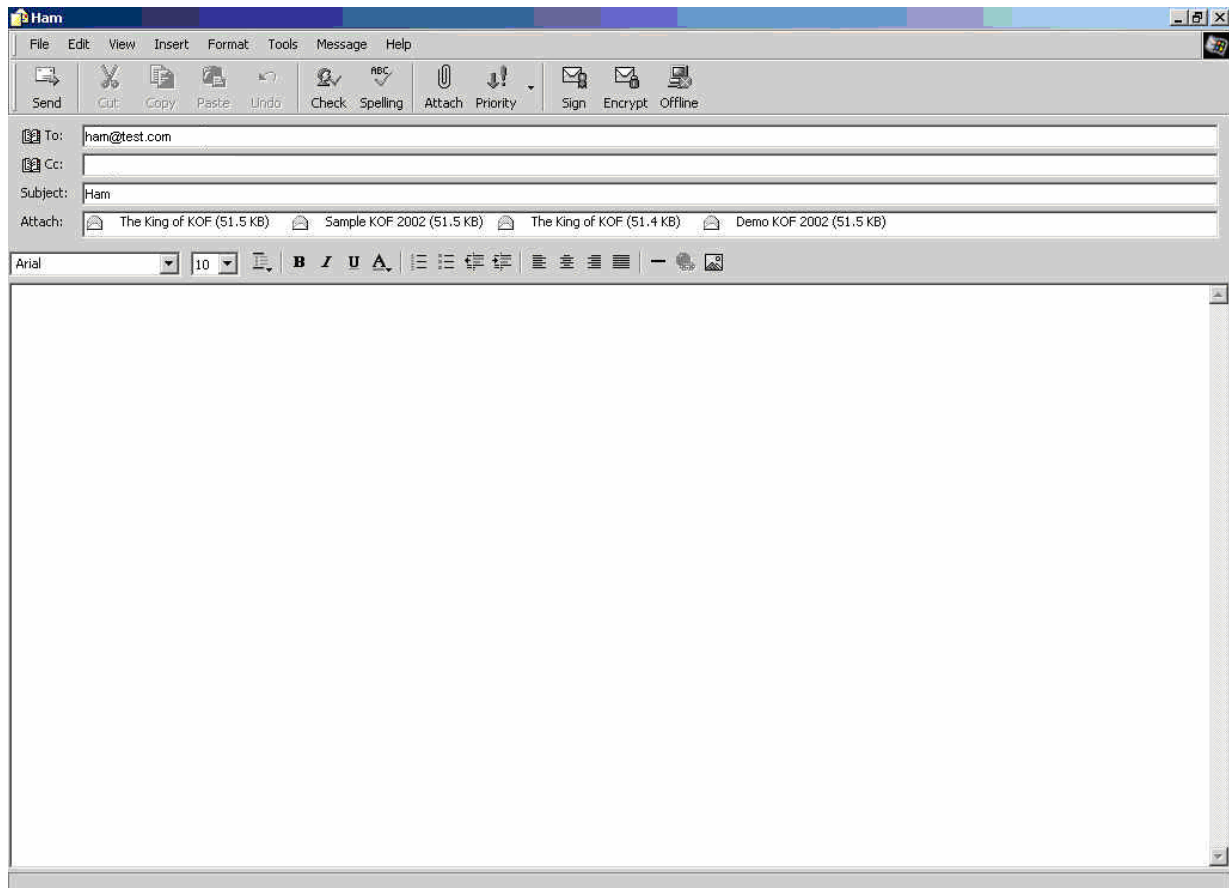
## To identify the mails to be ham mails through training

**Step6** In **Outlook Express**→ **Inbox** , to send the attached ham-mails to ham mails respond account via forwarding :

- In **Inbox**, Right click on the selected ham-mails and select **Forward As Attachment**.
- In **New Message** → **To : ( Recipient )** , enter [Ham@test.com](mailto:Ham@test.com) . **Subject**, enter Ham, and the content remained blank, and then click **Send**.



Select all the ham mails



### Forward the ham mails

**Step7** The CS-2000 will receive mails from the respond mail account on time , and identify these mails to be spam mails( [spam@test.com](mailto:spam@test.com) )or ham mails( [ham@test.com](mailto:ham@test.com) )depends on the assigned training time.



### The training time settings

## 7.3 Anti-Virus

# Anti-Virus

The CS-2000 can detect mails from the internal and external mail server. It can also prevent the company to be paralyzed by the virus mails.

In this Chapter, we will make the introduction of **Anti-Virus**.



### 7.3.1 Setting

#### Setting

- To do the anti-virus inspection of the inbound and outbound mails.
- To add the messages to the subject line if it has detected the infected mails.
- To update virus definition every ten minutes automatically or use manual update .It can also display the latest update time and version.
- The virus scan engine includes :
  - ◆ Clam : It is **free charge** to use the function. (Default setting is free charge to use).
  - ◆ Sophos : Users have to pay the charge.



The MIS engineer can check if the CS-2000 can connect to the virus definition server through **Test** function.

### Action of Infected Mail

- The MIS engineer can select to delete the virus mail, deliver to the recipient (Deliver a notification mail instead of the original virus mail or just deliver the original virus mail), Forward to another mail account or store in the quarantine, when the CS-2000 has detected the inbound mails infected.
- The MIS engineer can select to deliver virus mails to the recipient (Deliver a notification mail instead of the original virus mail or just deliver the original virus mail), or store in the quarantine, when the CS-2000 has detected the inbound mail infected.
- Add the following settings :
  1. **Virus Scan Engine**, select Clam.
  2. **The Mail Server is placed in**, select **Internal**.
  3. **Add the message to the subject line**, enter ---virus---.
  4. In **Action of Inbound infected Mail → Internal Mail Server**, select **Deliver to the recipient → Deliver a notification mail instead of the original virus mail**.
  5. Click **OK**.

Anti-Virus Setting

Virus Scan Engine

Clam

(There is a yearly fee for using Sophos, please contact distributors for pricing.)

The Mail Server is

☒ Internal (External user sends emails to internal mail server)
 ☒ External (Internal user receives emails from external mail server)

Add the virus string to the subject line

---Virus---

(Max. 256 characters)

---

Last updated on :

07/07/06 10:46:20

(Update virus definitions every ten minutes)

Current version :

43.3607 (Clam definitions updated at 07/07/06 08:03:32)

419 (Sophos definitions updated at 07/07/06 04:19:10)

Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server)

Update NOW

Test

Action of Infected Mail

Internal Mail Server (External user sends emails to internal mail server) :

☐ Delete the virus mail
 ☒ Deliver to the recipient
 

☒ Deliver a notification mail instead of the original virus mail
 ☐ Deliver the original virus mail

☐ Forward to : 

admin@myalexweb.dyndr

 (Max. 128 characters, ex: user@mydomain.com)
 ☐ Store in the quarantine

---

External Mail Server (Internal user receives emails from external mail server) :

☒ Deliver to the recipient (Always enable)
 

☒ Deliver a notification mail instead of the original virus mail
 ☐ Deliver the original virus mail

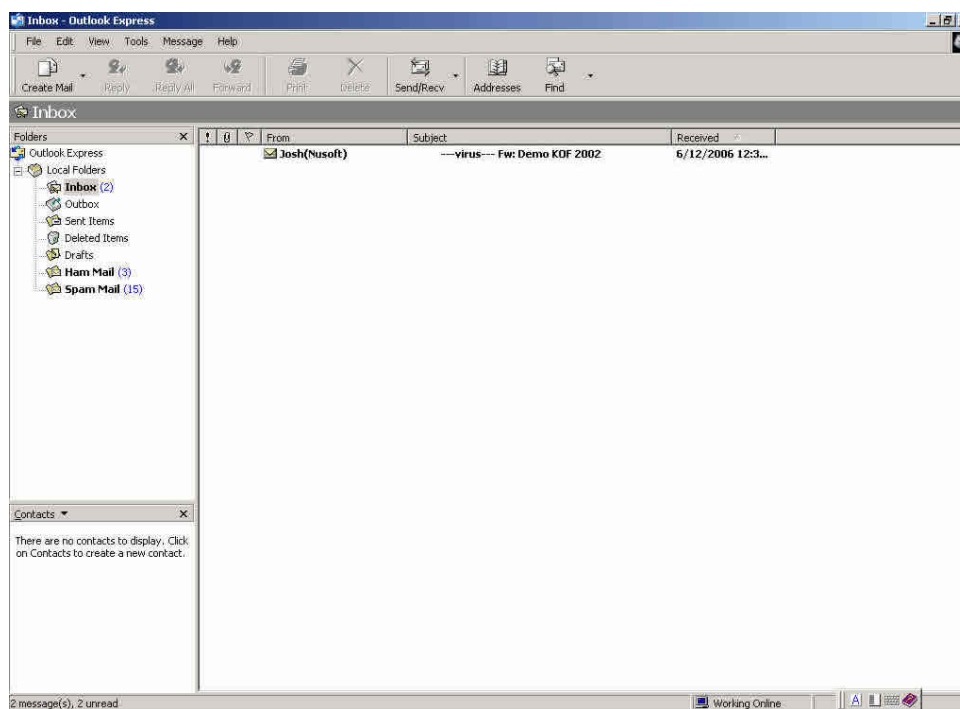
☒ Store in the quarantine

OK

Cancel

### The anti-virus setting

- ◆ If the internal and external recipient received the infected mails, the CS-2000 would add the messages to the subject line.



The infected mails with the messages in subject line



The **Virus Scan Engine** included Clam, Sophos and Clam+Sophos.

## 7.3.2 Virus Mail

### Search

- It can search the record stored in CS-2000 depends on Recipient , Sender , Subject , Virus Name , Date , Virus , Non-Virus , Attached , Non-Attached , such keywords or phrases .
- Add the following settings :
  1. **Recipient**, enter the mail account keywords . ( For example, alex, alex@test.com ) .
  2. In **after this date** and **before this date**, to search the record in selected date.
  3. Select **Virus**, **Non-Virus**, **Attached** and **Non-Attached**.
  4. Click **Search**.

### Search

Mail Direction : Inbound  
Mail Server : External

Enter keyword or phrase

Recipient :  ( Max. 100 characters )

Sender :  ( Max. 100 characters )

Subject :  ( Max. 100 characters )

Virus Name :  ( Max. 100 characters )

☒ From : 2007 / 1 / 6 0 : 0  
☒ To : 2007 / 7 / 6 10 : 59  
☒ Virus ☒ Attached  
☒ Non-Virus ☒ Non-Attached

[Search](#)

### Results

Search result: 150 mails

1 / 8 [Next](#) Top Received Time: 1 - 20

	Sender ▼	Recipient ▼	Subject ▼	Received Time ▼	Virus Name	Mail Size	Quarantine
	epaper@news.gameto..	alex_tien@mail2000..	- 《唯舞獨尊online》會員突破百..	07/05 20:32	---	15.5 kB	
	enews@mh3prd.sinoc..	alex_tien@mail2000..	- SNOOPY夏日鮮活主張! 汽車椅套..	07/05 20:32	---	5.7 kB	
	holy.tw@gmail.com	alex_tien@mail2000..	- 美國原裝，超好吸收液體營養補..	07/05 20:32	---	25.0 kB	
	qualitymen@gmail.c..	alex_tien@mail2000..	- 免費!免費!免費!還送你看書..	07/05 20:32	---	33.1 kB	
	bellahaw@cm1.hinet..	alex_tien@mail2000..	- **S** 政府立案,10年信用融資當..	07/05 20:32	---	3.0 kB	
	richard.sunny@msa...	alex_tien@mail2000..	- **S** 4	07/05 20:32	---	3.7 kB	
	lawrence.rebecca@m..	alex_tien@mail2000..	- **S** Wii 最新 遊戲&eMone..	07/05 20:32	---	4.0 kB	
	nba@fans.nba.com	alex_tien@mail2000..	- NBA Daily - Sonics Set To Hir..	07/05 20:32	---	17.2 kB	
	epaper@news.gameto..	alex_tien@mail2000..	- 消費滿百，夏日天使就是你！	07/05 20:32	---	14.3 kB	
	reply@covers.messa..	alex_tien@mail2000..	- Cappers getting bad vibe from..	07/05 20:32	---	25.9 kB	
	(No Sender)	alex_tien@mail2000..	- 7月5日工作分配	07/05 20:32	---	62.1 kB	
	mostanley@yahoo.co..	alex_tien@mail2000..	- **S** Hide IP Platinum 2.91 ..	07/05 20:32	---	4.8 kB	
	ylou@yahoo.com.cn	alex_tien@mail2000..	- **S** 3分鐘告知您可貸額度及最..	07/05 20:32	---	2.2 kB	
	sylvia robin@msn.co..	alex_tien@mail2000..	- **S** 拒絕當卡奴	07/05 20:32	---	2.1 kB	
	an_sang@gmail.com	alex_tien@mail2000..	- **S** 想賺錢...女生...看過來	07/05 20:32	---	2.3 kB	
	edm@maildij.com	alex_tien@mail2000..	- Combi 品牌月- 特價組合超優惠 ..	07/05 20:32	---	25.0 kB	

To search the specific record



In **Virus Mail**, the MIS engineer can select to display the inbound or outbound scanned mails.



In **Virus Mail**, click the **Recipient** mail address, then it shows the **Sender List**. Click the sender mail address, and then it shows **Virus List**.



Select the specific mails in **Virus List** and **Search → Search Results**.

1. Use the **Retrieve** function › to send the virus mails to assigned mail account. (The CS-2000 can only send the mails stored in quarantine.)



In **Virus List** and **Sender List**, the CS-2000 can make the sorting by Recipient, Sender, Total Virus and Total Mail. In **Virus Mail Results**, the CS-2000 can make the sorting by subject and received time.

### 7.3.3 Anti-Virus Examples

We set 2 anti-virus environments.

No.	The Application Environment	Pages
<b>Example. 1</b>	To detect the infected mails on mail server.	<b>397</b>
<b>Example. 2</b>	Use CS-2000 to be the gateway , in order to detect the infected mails in internal or external mail server.( Set the mail server in LAN and use the NAT mode)	<b>402</b>

## Example 1

To detect the infected mails on mail server.

**Step1** To allow the **LAN** PC can receive the mails from external mail server, and set the network adapter DNS correspond to external DNS server.

**Step2** In **Service → Group**, add the following settings.

Group name▼	Service	Configure
Mail_Service	DNS,IMAP,POP3...	<a href="#">In Use</a>
Main_Service	DNS,HTTP,POP3...	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Set the group included POP3 and SMTP or DNS

**Step3** In **Policy → Outgoing**, add the following setting :

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	Mail_Service			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▼

[New Entry](#)

Set the outgoing policy

**Step4** In Anti-Virus → Setting , add the following settings :

Anti-Virus Setting	
Virus Scan Engine	Clam (There is a yearly fee for using Sophos, please contact distributors for pricing.)
The Mail Server is	<input checked="" type="checkbox"/> Internal (External user sends emails to internal mail server) <input checked="" type="checkbox"/> External (Internal user receives emails from external mail server)
Add the virus string to the subject line	---Virus--- (Max. 256 characters)
-----	
Last updated on : 07/07/06 10:46:20 (Update virus definitions every ten minutes)	
Current version : 43.3607 (Clam definitions updated at 07/07/06 08:03:32)	
419 (Sophos definitions updated at 07/07/06 04:19:10)	
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) <a href="#">Update NOW</a> <a href="#">Test</a>	
Action of Infected Mail	
Internal Mail Server (External user sends emails to internal mail server) :	
<input type="checkbox"/> Delete the virus mail <input checked="" type="checkbox"/> Deliver to the recipient <input checked="" type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input type="checkbox"/> Forward to : admin@myalexweb.dyndr (Max. 128 characters, ex: user@mydomain.com) <input type="checkbox"/> Store in the quarantine	
-----	
External Mail Server (Internal user receives emails from external mail server) :	
<input checked="" type="checkbox"/> Deliver to the recipient (Always enable) <input checked="" type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input checked="" type="checkbox"/> Store in the quarantine	
<a href="#">OK</a> <a href="#">Cancel</a>	

**The setting of infected mails inspection and action**





The default setting of Anti-Virus is enabled. The MIS engineer only need to add the **Mail Relay** setting, then the CS-2000 will automatically execute Anti-Virus function to the mails sent from the external mail server or the inbound mails. (The mails sent to the internal mail server, and receive the mails from external mail server.)

Anti-Virus Setting	
Virus Scan Engine	Clam (There is a yearly fee for using Sophos, please contact distributors for pricing.)
The Mail Server is	<input checked="" type="checkbox"/> Internal (External user sends emails to internal mail server) <input checked="" type="checkbox"/> External (Internal user receives emails from external mail server)
Add the virus string to the subject line	---Virus--- (Max. 256 characters)
Last updated on : 07/07/06 10:56:22 (Update virus definitions every ten minutes) Current version : 43.3607 (Clam definitions updated at 07/07/06 08:03:32) 419 (Sophos definitions updated at 07/07/06 04:19:10) Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) <a href="#">Update NOW</a> <a href="#">Test</a>	
Action of Infected Mail	
Internal Mail Server (External user sends emails to internal mail server) :	
<input type="checkbox"/> Delete the virus mail <input type="checkbox"/> Deliver to the recipient <input type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input type="checkbox"/> Forward to : admin@myalexweb.dyndr (Max. 128 characters, ex: user@mydomain.com) <input checked="" type="checkbox"/> Store in the quarantine	
External Mail Server (Internal user receives emails from external mail server) :	
<input checked="" type="checkbox"/> Deliver to the recipient (Always enable) <input checked="" type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input checked="" type="checkbox"/> Store in the quarantine	
<a href="#">OK</a> <a href="#">Cancel</a>	

### The default setting of anti-virus



When the CS-2000 only scan the mails from received mail server :

1. In **Action of Infected Mail** → **External Mail Server**, the default setting of **Deliver to the recipient** is always enabled, it can not be disabled. On the other hand, the user can select to **Store the Infected Mail in the quarantine**. The CS-2000 can add the messages to the subject line or deliver a notification mail instead of the original virus mail or deliver the original virus mail whatever the actions we selected.

- Step5** When the internal user receive mails from the external mail account [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw) , the CS-2000 will filter these mails and results the list in Anti-Virus → Virus Mail. (Click **Inbound** and **External**)

Mail Direction : **Inbound** **Inbound**  
Mail Server : **Internal** **External**

The Duration of Today

No.	Recipient	Total Virus	Total Mail	Duration	Virus %
1	<a href="mailto:js1720@ms21.pchome.com.tw">js1720@ms21.pchome.com.tw</a>	1	8	10H	0.0%
Total		1	24		0.0%

[Clear Data](#)

### The virus mail list

- Step6** Click **Recipient** of [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw) , then it shows the sender list, look the **Total Virus** and **Total Mail** from the sender account.

### Sender List

Recipient: : [js1720@ms21.pchome.com.tw](mailto:js1720@ms21.pchome.com.tw)

No.	Recipient	Total Virus	Total Mail	Duration	Virus %
1	<a href="mailto:js1720@ms21.pchome.com.tw">js1720@ms21.pchome.com.tw</a>	1	1	00H	100.0%
2	<a href="mailto:123654@edm.yam.com">123654@edm.yam.com</a>	0	1	00H	0.0%
3	<a href="mailto:1482@mail.ms-edm.com.tw">1482@mail.ms-edm.com.tw</a>	0	1	00H	0.0%
4	<a href="mailto:edm@cms5.so-net.net.tw">edm@cms5.so-net.net.tw</a>	0	1	00H	0.0%
5	<a href="mailto:n15001.s4734.c24563683.14527.130_e448546377_d0@fans.nba.com">n15001.s4734.c24563683.14527.130_e448546377_d0@fans.nba.com</a>	0	1	00H	0.0%
6	<a href="mailto:nobody@yahoo.edyna.com">nobody@yahoo.edyna.com</a>	0	1	00H	0.0%
7	<a href="mailto:vincechase@ms96.url.com.tw">vincechase@ms96.url.com.tw</a>	0	1	00H	0.0%
Total		1	7		14.3%

### The sender list

**Step7** Click **Sender** mail address of [magafifa@pchome.com.tw](mailto:magafifa@pchome.com.tw) , it shows the Attached , Received Time , Subject , Virus Name , Mail Size , and Quarantine information .

- Select the mails saved in quarantine to retrieve. In **Virus List**, click **Retrieve**.
- In retrieve mail window, set the **Sender** and **Recipient** then click **OK**. The mails can be retrieved by the assigned recipient.

**Virus List**

Top Received Time: 1 - 1

richard.sunny@msa.hinet.net -> js1720@ms21.pchome.com.tw

	Subject	Received Time	Virus Name	Mail Size	Quarantine
<input type="checkbox"/>	**S** 4	07/05 20:32	W32Nets...	3.7 KB	

**The virus mail list**



In **Sender List**, the MIS engineer can only click the mail account which has been detected to send the virus mail.

**Virus List**

Top Received Time: 1 - 1

richard.sunny@msa.hinet.net -> js1720@ms21.pchome.com.tw

	Subject	Received Time	Virus Name	Mail Size	Quarantine
<input type="checkbox"/>	**S** 4	07/05 20:32	W32Nets...	3.7 KB	

http://210.66.155.77 - Retrieve mail - Microsoft Internet Explorer

Sender:  (ex: sender@mydomain.com)

Recipient:  (ex: recipient@mydomain.com)

OK Cancel

**Retrieve the virus mail**

## Example 2

Use CS-2000 to be the gateway, in order to detect the infected mails in internal or external mail server. (Set the mail server in LAN and use the NAT mode)

CS-2000 WAN1 IP is 61.11.11.12

CS-2000 LAN segment is 192.168.2.0 / 24

**Step1** In **LAN**, setup a mail server, the network adapter IP is 192.168.2.12, DNS correspond to the external DNS server, and server name is test.com.

**Step2** In **Address** → **LAN** , add the following settings :

Name▼	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Mail_Server1	192.168.2.12/255.255.255.255		Modify Remove

New Entry

Set the mail server correspond to name in address

**Step3** In **Service** → **Group**, add the following settings.

Group name▼	Service	Configure
Mail_Service	DNS,IMAP,POP3...	In Use
Main_Service	DNS,HTTP,POP3...	Modify Remove

New Entry

Set the group included POP3 and SMTP, or DNS

**Step4** In **Virtual Server** → **Server 1** , add the following setting :

Virtual Server Real IP

Total entry : 1

Service	WAN Port	Server Virtual IP	Configure
Mail_Service	From-Service(Group)	192.168.2.12	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Virtual server setting

**Step5** In **Policy** → **Incoming** , add the following setting :

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	Mail_Service			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 <input type="button" value="v"/>

Set the incoming policy

**Step6** In **Policy** → **Outgoing** , add the following setting :

Source	Destination	Service	Action	Option	Configure	Move
Mail_Server1	Outside_Any	Mail_Service			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 <input type="button" value="v"/>

Set the outgoing policy

**Step7** In **Configure** → **Mail Relay** , add the following setting :

Domain Name of Internal Mail Server or Allowed External IP of Mail Relay	Configure
test.com ( 192.168.2.12 )	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
61.64.127.16 / 255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Set the inbound mail relay setting



The **Mail Relay** function can relay mails to the specific domain name which corresponded to the mail server.

**Step8** In **Anti-Virus → Setting** , add the following settings :

Anti-Virus Setting	
Virus Scan Engine	Clam (There is a yearly fee for using Sophos, please contact distributors for pricing.)
The Mail Server is	<input checked="" type="checkbox"/> Internal (External user sends emails to internal mail server) <input checked="" type="checkbox"/> External (Internal user receives emails from external mail server)
Add the virus string to the subject line	---Virus--- (Max. 256 characters)
-----	
Last updated on : 07/07/06 10:56:22 (Update virus definitions every ten minutes)	
Current version : 43.3607 (Clam definitions updated at 07/07/06 08:03:32)	
419 (Sophos definitions updated at 07/07/06 04:19:10)	
Update virus definitions immediately (Use TCP port : 80 and UDP port : 53 to connect virus definition server) <a href="#">Update NOW</a> <a href="#">Test</a>	
Action of Infected Mail	
Internal Mail Server (External user sends emails to internal mail server) :	
<input type="checkbox"/> Delete the virus mail <input type="checkbox"/> Deliver to the recipient <input type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input type="checkbox"/> Forward to : admin@myalexweb.dyndr (Max. 128 characters, ex: user@mydomain.com) <input checked="" type="checkbox"/> Store in the quarantine	
-----	
External Mail Server (Internal user receives emails from external mail server) :	
<input checked="" type="checkbox"/> Deliver to the recipient (Always enable) <input checked="" type="radio"/> Deliver a notification mail instead of the original virus mail <input type="radio"/> Deliver the original virus mail <input checked="" type="checkbox"/> Store in the quarantine	
<a href="#">OK</a> <a href="#">Cancel</a>	

**The setting of anti-virus and action**

If the MIS engineer selects **Action of Infected Mail → Delete the virus mail**, then he can not select **Deliver to the recipient**, **Forward to**, **Store in the quarantine** and **Notice to the sender**. In other words, the CS-2000 will delete all the infected mails after it has detected the virus mails. In **Virus Mail**, the MIS engineer still can see some related Lists.

**Step9** When the external yahoo mail account send mails to the recipient of [josh@test.com](mailto:josh@test.com) on test.com mail server under CS-2000 :

- The sender account ([share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw)) send the virus mail.
- The sender account ([share2k003@yahoo.com.tw](mailto:share2k003@yahoo.com.tw)) send the non-virus mail.
- After the CS-2000 filtered this mails, it will results the list in **Anti-Virus → Virus Mail.** ( Click **Inbound → Internal**, to see the internal list. )

Mail Direction : **Inbound** **Inbound**  
Mail Server : **Internal** **External**

The Duration of Today

No.	Recipient ▼	Total Virus ▼	Total Mail ▼	Duration	Virus %
1	<a href="mailto:josh@test.com">josh@test.com</a>	1	8	10H	0.0%
Total		1	24		0.0%

[Clear Data](#)

#### The virus mail list

**Step10** Click **Recipient** mail address of [josh@test.com](mailto:josh@test.com) . In **Sender List**, to check the **Total Virus** and **Total Mail**.

#### Sender List

Recipient: : [josh@test.com](mailto:josh@test.com)

No.	Recipient ▼	Total Virus ▼	Total Mail ▼	Duration	Virus %
1	<a href="mailto:share2k01@yahoo.com.tw">share2k01@yahoo.com.tw</a>	1	1	00H	100.0%
2	<a href="mailto:123654@edm.yam.com">123654@edm.yam.com</a>	0	1	00H	0.0%
3	<a href="mailto:1482@mail.ms-edm.com.tw">1482@mail.ms-edm.com.tw</a>	0	1	00H	0.0%
4	<a href="mailto:edm@cms5.so-net.net.tw">edm@cms5.so-net.net.tw</a>	0	1	00H	0.0%
5	<a href="mailto:n15001.s4734.c24563683.14527.130.e448546377.d0@fans.nba.com">n15001.s4734.c24563683.14527.130.e448546377.d0@fans.nba.com</a>	0	1	00H	0.0%
6	<a href="mailto:nobody@yahoo.edyna.com">nobody@yahoo.edyna.com</a>	0	1	00H	0.0%
7	<a href="mailto:vincechase@ms96.url.com.tw">vincechase@ms96.url.com.tw</a>	0	1	00H	0.0%
Total		1	7		14.3%

#### The sender list

**Step11** Click the **Sender** mail address of [share2k01@yahoo.com.tw](mailto:share2k01@yahoo.com.tw) , it shows the information of the Attached, Subject, Received Time, Virus Name, Mail Size and Quarantine.

- Select the mails saved in quarantine to retrieve. In **Virus Mail List**, click **Retrieve**.
- In retrieve mail window, set the sender and recipient mail account, then Click **OK**. To retrieve mails from the assigned recipient.

**Virus List**

Top Received Time: 1 - 1

richard.sunny@msa.hinet.net -> josh@test.com

	Subject	Received Time	Virus Name	Mail Size	Quarantine
<input type="checkbox"/>	**S** 4	07/05 20:32	W32Nets..	3.7 KB	

**The virus mail list**



In **Sender List**, the MIS engineer can only click the sender mail account which had been detected to send the virus mails.

**Virus List**

Top Received Time: 1 - 1

richard.sunny@msa.hinet.net -> josh@test.com

	Subject	Received Time	Virus Name	Mail Size	Quarantine
<input type="checkbox"/>	**S** 4	07/05 20:32	W32Nets..	3.7 KB	

http://210.66.155.77 - Retrieve mail - Microsoft Internet Explorer

Sender: [share2k01@yahoo.com.tw] (ex: sender@mydomain.com)

Recipient: [josh@test.com] (ex: recipient@mydomain.com)

OK Cancel

**The retrieve virus mail window**



When use the **Retrieve** function, the MIS engineer must select the infected mails saved in **Quarantine**



In **Anti-Virus** → **Virus Mail**, click **Clear**, and then the CS-2000 will delete all the List records. In other words, the MIS engineer can not find this deleted file in **Virus Mail** function.



## 7.4 Mail Report

# Mail Report

The CS-2000 can display the mail scanned record by statistics and logs, it can let the user easy to know the status of mail process.

In this Chapter, we will make the introduction of **Mail Report**.

## 7.4.1 Setting

### Periodic Report

- It can send the period report to recipient according to the selected date.

### History Report

- It can send the history report according to the assigned date.
  - In **System → Configure → Setting**, enable **E-mail Alert Notification**. On the other hand , add the following settings in **Mail Report** :
    1. **Enable sending periodic report by mail**, select **Yearly report, Monthly report, Weekly report, Daily report**.
    2. Click **OK**.
    3. When the time arrived, the CS-2000 will send the report to recipient.
    4. In **History Report**, select the date to send the report.
    5. Click **Send Report**.
    6. It will send the related report to the user.



The periodic report will result at the following time period:

1. **Yearly report** ; It results in 00:00 AM, January first, yearly.
2. **Monthly report** : It results in 00:00 AM, first day, Monthly.
3. **Weekly report** : It results in 00:00 AM, first day, Weekly.
4. **Daily report** : It results in 00:00, Daily.

**Periodic Report**

☒ Enable sending periodic report by mail

☒ Yearly report ☒ Monthly report ☒ Weekly report ☒ Daily report

**OK** **Cancel**

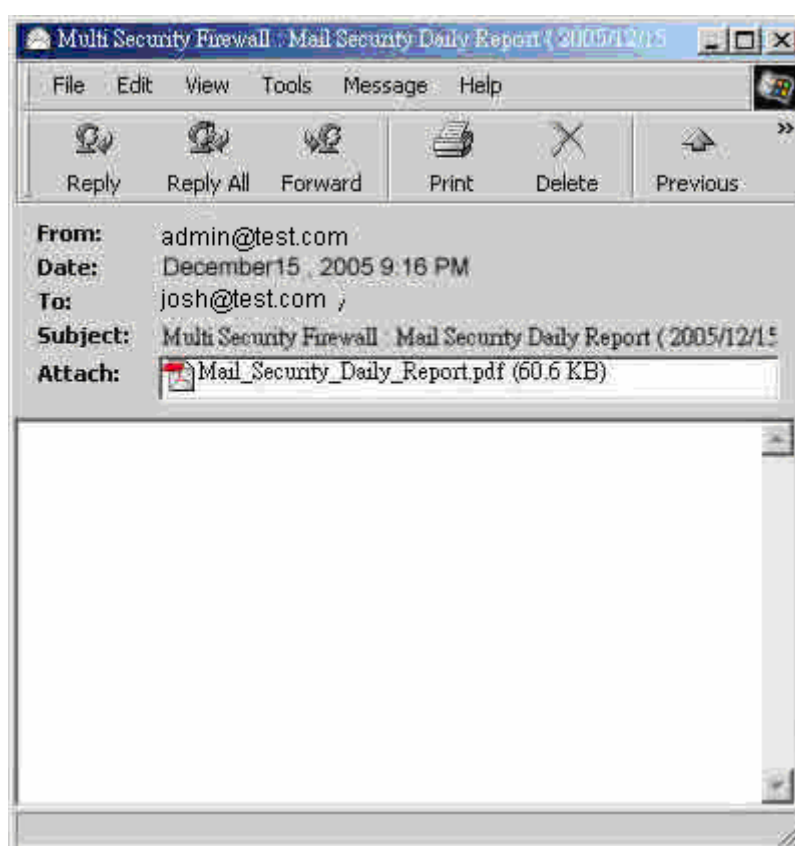
**History Report**

☐ Yearly report ☐ Monthly report ☐ Weekly report ☐ Daily report

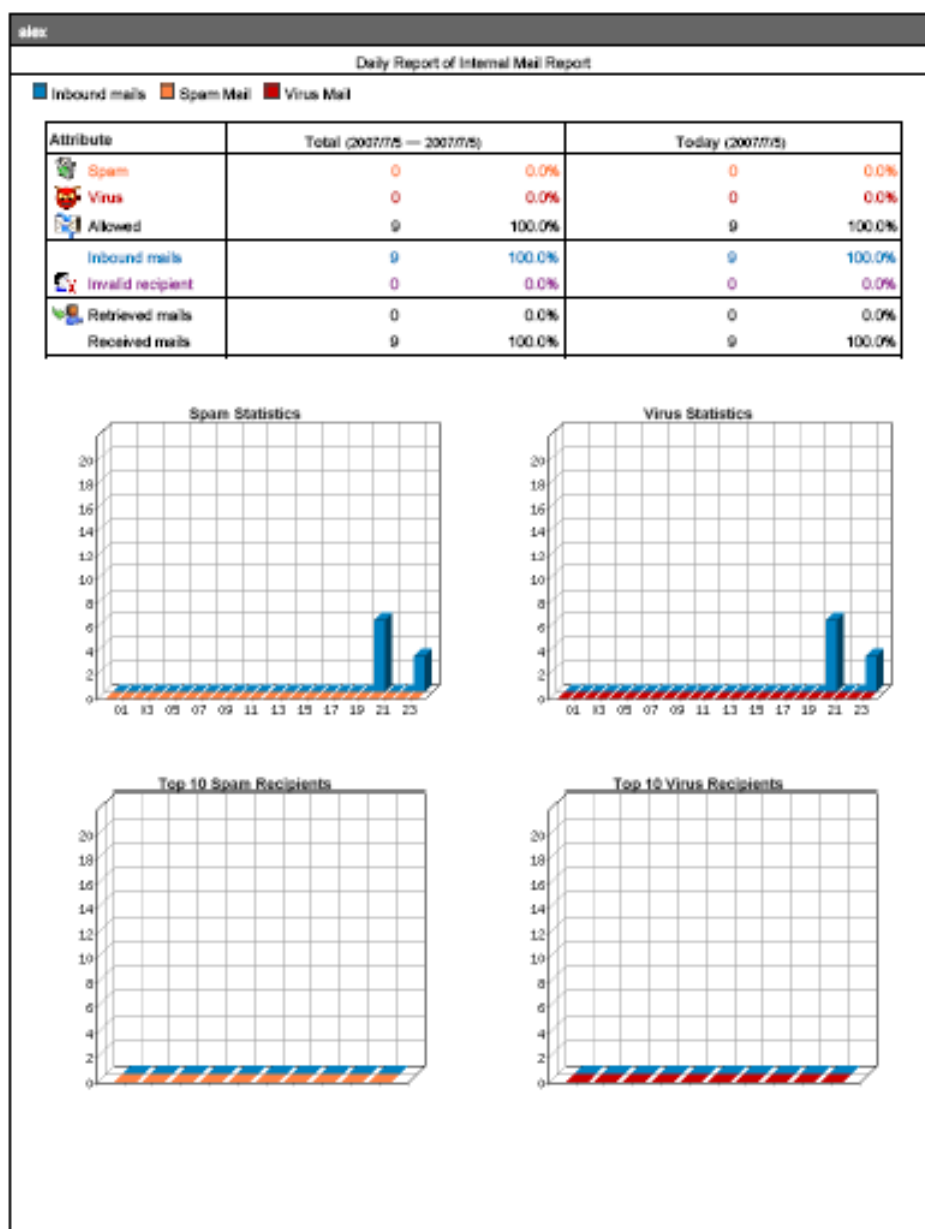
2007 07 01 06

**Send Report**

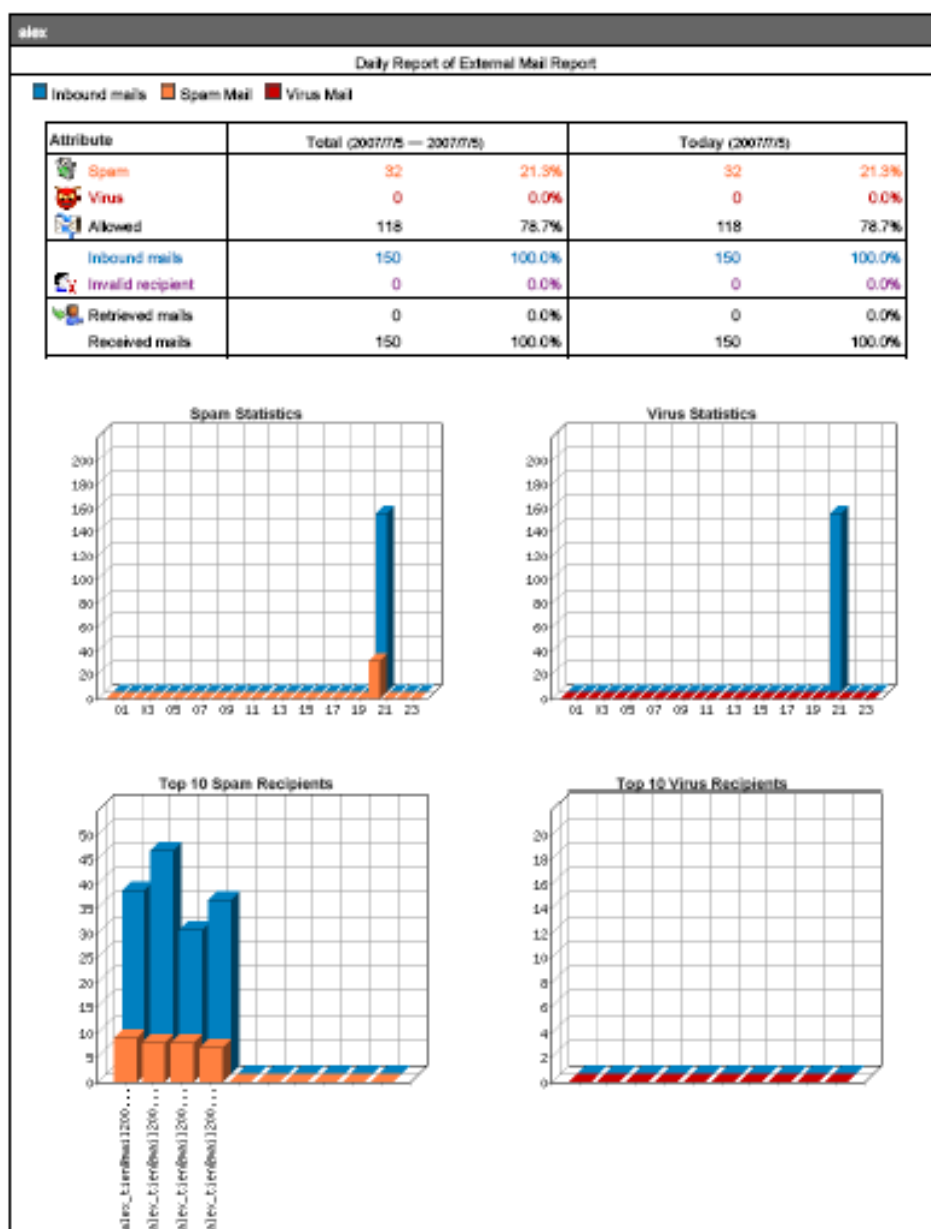
To send the period report



Receive the period report



The first page in period report



The second page in period report



The mail report will attached as PDF format to send to the recipient.

**Periodic Report**

☒ Enable sending periodic report by mail

☒ Yearly report ☒ Monthly report ☒ Weekly report ☒ Daily report

**OK** **Cancel**

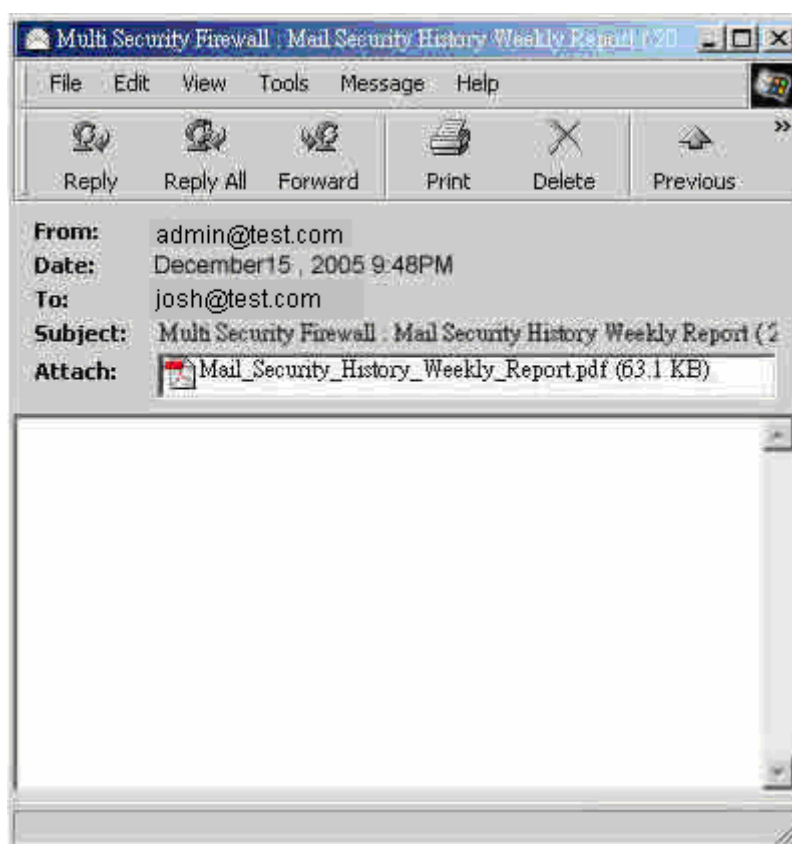
**History Report**

☐ Yearly report ☐ Monthly report ☒ Weekly report ☐ Daily report

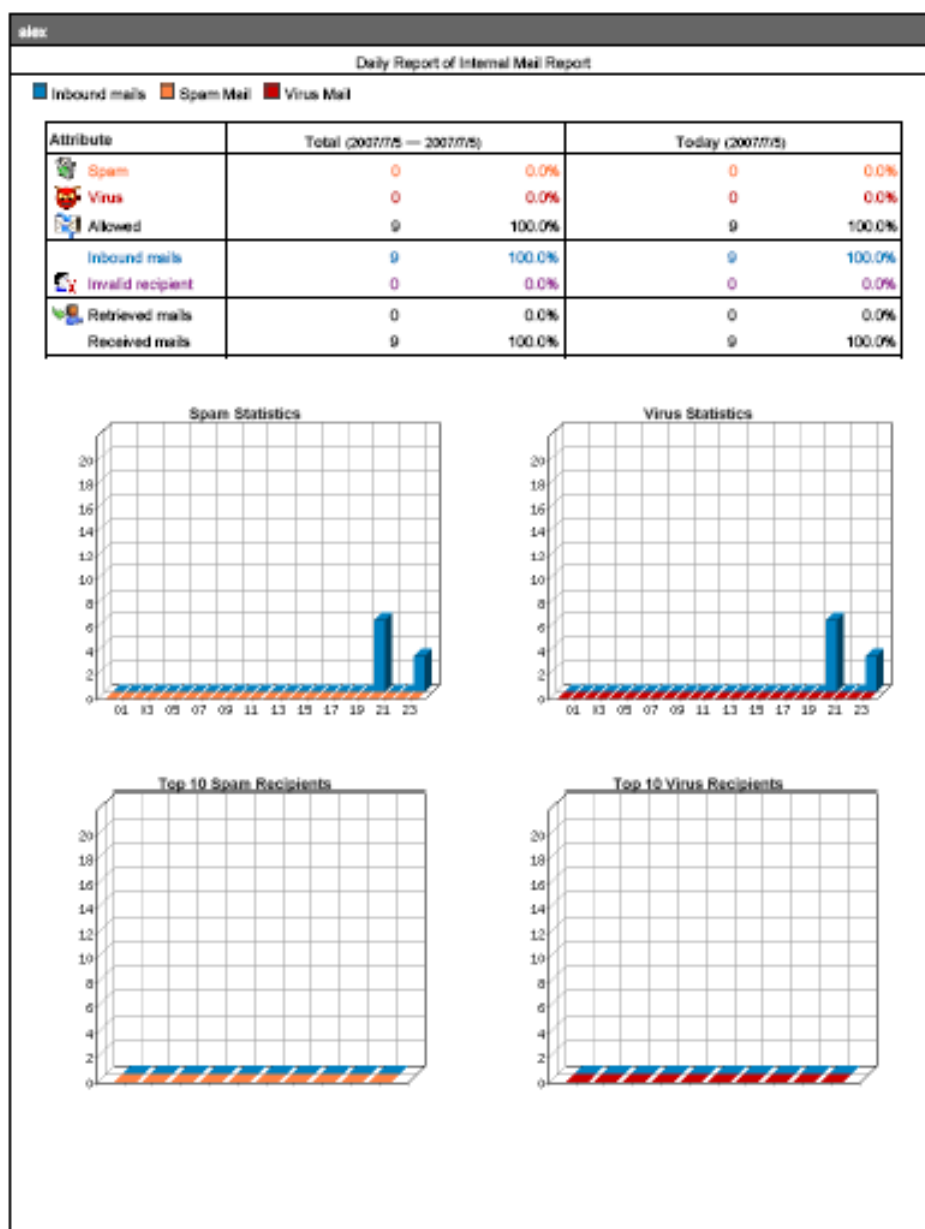
2007 07 01

**Send Report**

### The history report setting



### Received the history report



The first page in history report



The mail report will be attached as PDF format to send to the recipient.

## 7.4.2 Statistics

**Step1** In **Mail Report → Statistics**, it shows the scanned mail statistics report in CS-2000.

**Step2** In **Statistics**, click **Day**, to view the daily report. Click **Week**, to view the weekly report. Click **Month**, to view the monthly report. Click **Year**, to view the yearly report.

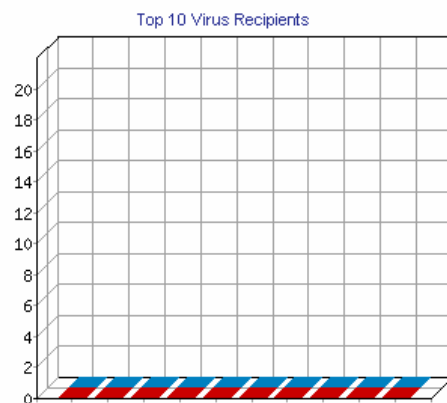
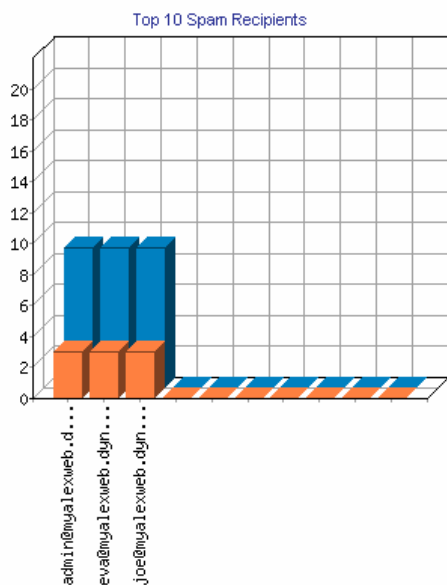
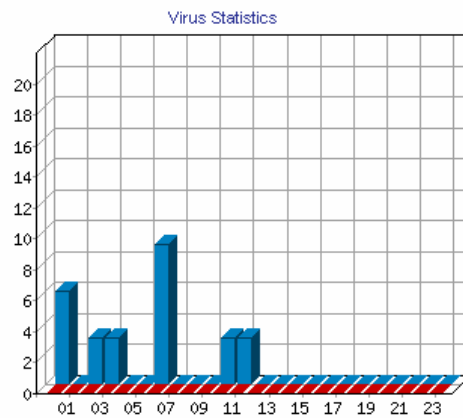
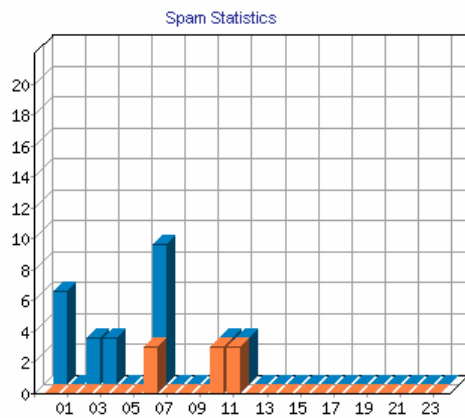
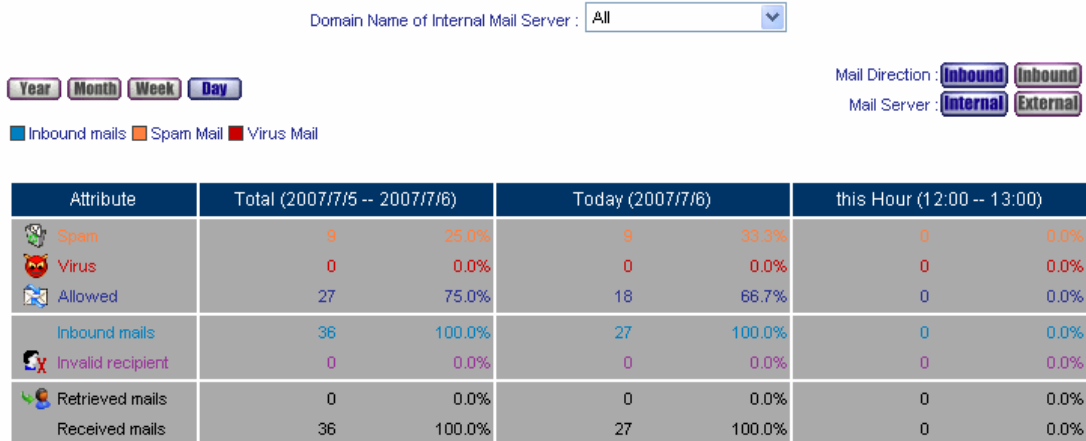


If the MIS engineer selects **Inbound → Internal**, then he can view the scanned mail statistics in **every domain name of internal mail server**.



**Step3** The mail scanned statistics.

- Ordinate : The amount of scanned mails.
- Horizontal ordinate : Time.

**The mail scanned statistics**

### 7.4.3 Log

#### Search

- It can search all the records correspond to the condition in CS-2000, depends on the Recipient , Sender , Subject , IP Address , Date , Attribute , Action , Attached or Non-Attached .
  - Add the following settings :
    1. **Recipient** , enter the mail account keywords . ( For example ,alex , alex@test.com )
    2. Select the date in **after this date** and **before this date**.
    3. **Attribute**, select All.
    4. **Action**, select All.
    5. Select **Attached** and **Non – Attached**.
    6. Click **Search**.

## Search

Mail Direction : Inbound  
Mail Server : Internal

Enter keyword or phrase

Recipient :  ( Max. 100 characters )

Sender :  ( Max. 100 characters )

Subject :  ( Max. 100 characters )

IP Address :

☒ From : 2007 / 6 / 6 0 0  
☒ To : 2007 / 7 / 6 13 28

Attribute :

Action :

☐ Attached ☒ Non-Attached

[Search](#)

## Results

Search result: 34 records

1 / 2 [Next](#)

Top Date: 1 - 20

<input type="checkbox"/>	Sender	Recipient	Subject	Date	Attribute	Action
<input type="checkbox"/>	lsadoris@cm1.hi...	joe@myalexweb.dy..	- **SM [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi...	eva@myalexweb.dy..	- **SM [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi...	admin@myalexweb...	- **SM [SPAM]	07/06 11:13		
<input type="checkbox"/>	alex_tien@email...	joe@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	eva@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	admin@myalexweb...	- varigated football team	07/06 10:52		
<input type="checkbox"/>	nobody@yahoo.edy..	joe@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	eva@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	admin@myalexweb...	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	123654@edm.yam.c..	joe@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	eva@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	admin@myalexweb...	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	1482@mail.ms-edm..	joe@myalexweb.dy..	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	1482@mail.ms-edm..	eva@myalexweb.dy..	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	1482@mail.ms-edm..	admin@myalexweb...	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	edm@cms5.so-net...	joe@myalexweb.dy..	- 密切鎖定！史上最強的電玩大帝國，震..	07/06 02:34		
<input type="checkbox"/>	edm@cms5.so-net...	eva@myalexweb.dy..	- 密切鎖定！史上最強的電玩大帝國，震..	07/06 02:34		

## To search the specific record



In **Statistics** and **Log**, MIS engineer can select the inbound or outbound mail report to display.



In **Log**, click **Sender** mail address, then it shows the **Recipient List**. If the user clicks **Recipient** mail address, then it shows the **Sender List**.



In **Log**, **Recipient List** and **Sender List**, the CS-2000 can make sorting by the Sender, Recipient, Subject, and Date.

**Step1** In **Mail Report** → **Log**, it shows the mail scan status in CS-2000.

1 / 2 [Next](#)

Mail Direction : [Inbound](#) [Inbound](#)  
Mail Server : [Internal](#) [External](#)

	Sender	Recipient	Subject	Date	Attribute	Action
<input type="checkbox"/>	lsadoris@cm1.hi..	joe@myalexweb.dy..	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi..	eva@myalexweb.dy..	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi..	admin@myalexweb...	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	alex_tien@email...	joe@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	eva@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	admin@myalexweb...	- varigated football team	07/06 10:52		
<input type="checkbox"/>	nobody@yahoo.edy..	joe@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	eva@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	admin@myalexweb...	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	123654@edm.yam.c..	joe@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	eva@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	admin@myalexweb...	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	1482@mail.ms-edm..	joe@myalexweb.dy..	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	1482@mail.ms-edm..	eva@myalexweb.dy..	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	1482@mail.ms-edm..	admin@myalexweb...	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		
<input type="checkbox"/>	edm@cms5_so-net...	joe@myalexweb.dy..	- 密切鎖定！史上最強的電玩大帝國，震..	07/06 02:34		
<input type="checkbox"/>	edm@cms5_so-net...	eva@myalexweb.dy..	- 密切鎖定！史上最強的電玩大帝國，震..	07/06 02:34		

[Clear Data](#)

1 / 2 [Next](#)

### The scanned mail log



In **Log**, to display the spam and virus mails stored in quarantine, which can be **Retrieved** by the specific recipient or click **Subject** to view the mail contents.

1 / 2 [Next](#)

Mail Direction : [Inbound](#) [Inbound](#)  
Mail Server : [Internal](#) [External](#)

	Sender	Recipient	Subject	Date	Attribute	Action
<input checked="" type="checkbox"/>	lsadoris@cm1.hi..	joe@myalexweb.dy..	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi..	eva@myalexweb.dy..	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	lsadoris@cm1.hi..	admin@myalexweb...	- **S** [SPAM]	07/06 11:13		
<input type="checkbox"/>	alex_tien@email...	joe@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	eva@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	alex_tien@email...	admin@myalexweb...	- varigated football team	07/06 10:52		
<input type="checkbox"/>	wan-samuel@umail..	joe@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	wan-samuel@umail..	eva@myalexweb.dy..	- varigated football team	07/06 10:52		
<input type="checkbox"/>	wan-samuel@umail..	admin@myalexweb...	- varigated football team	07/06 10:52		
<input type="checkbox"/>	nobody@yahoo.edy..	joe@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	eva@myalexweb.dy..	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	nobody@yahoo.edy..	admin@myalexweb...	- 田 肇坪 您好 帶給您最新AussieBu..	07/06 06:33		
<input type="checkbox"/>	123654@edm.yam.c..	joe@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	eva@myalexweb.dy..	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	123654@edm.yam.c..	admin@myalexweb...	- 強檔港劇「識法代言人」網路獨家首播..	07/06 06:22		
<input type="checkbox"/>	1482@mail.ms-edm..	joe@myalexweb.dy..	- 七月份TechNet Webcast 研討會--MDO..	07/06 03:45		

**http://210.66.155.77 - Retrieve mail - Microsoft Internet Explorer**

Sender : joe@myalexweb.dyndns.tv ( ex: sender@mydomain.com )  
Recipient : joe@myalexweb.dyndns.tv ( ex: recipient@mydomain.com )

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

完成 網路網路

To retrieve the spam or virus mails stored in quarantine



The Icon description in **Log** :

**1.Attribute :**

Icon					
Description	Allowed	Spam	Virus	Unscanned	Invalid Recipient

**2.Action :**

Icon					
Description	Delete	Deliver	Forward	Store	Retrieved

**3.Attached :**

## Chapter 8: IDP

### 8.1 Configure

# Configure

The CS-2000 can detect the anomaly flow packets and notice the MIS engineer to handle the situation, in order to prevent any suspicious program to invade the destination PC. In other words, the CS-2000 can provide the instant network security protection as detects any internal or external attacks, in order to enhance the enterprises network stability.

The so called IDP configure is defined to be the IDP setting.

## Setting

### Setting

- The CS-2000 can update signature definitions every 30 minutes or the MIS engineer can select to use manual update. It also shows the latest update time and version.
- The MIS engineer can enable anti-virus to the compact or non-encryption files.
- Virus engine :
  - ◆ Clam : It is the default setting and no charges to pay.
- The CS-2000 can send the NetBIOS notification through e-mail when system detected the attacks and infected files.



The MIS engineer can click **Test**, in order to make sure the CS-2000 can connect to the signature definition server normally.

### Set default action of all signatures

- The internet attack risks included High, Medium and Low. The MIS engineer can select the action of Pass, Drop, Log or Alarm to the default signatures.
- In **System → Configure → Setting**, select **Enable E-mail Alert Notification**, and add the following settings :
  1. Select **Enable Anti-Virus**.
  2. Select **Enable NetBIOS Alert Notification**.
  3. **IP Address of MIS engineer**, enter 192.168.1.10.
  4. Click **OK**.
  5. **High Risk**, select Drop, Log and Alarm.
  6. **Medium Risk**, select Drop, Log and Alarm.
  7. **Low Risk**, select Pass, Log and Alarm.
  8. Click **OK**.
  9. Select enable **IDP** in policy.

IDP Setting

Last updated on : 07/07/05 13:35:13 (Update signature definitions every 120 minutes)  
 Current version : 0.1.0 (Signature definitions updated at 07/07/04 15:34:32)  
 Update signature definitions immediately (Use TCP port : 80 and UDP port : 53)
 Update NOW
Test

---

☒ Enable Anti-Virus (for P2P, IM, NetBIOS...)

---

☒ Enable NetBIOS Alert Notification  
 IP Address of Administrator

OK Cancel

Set default action of all signatures

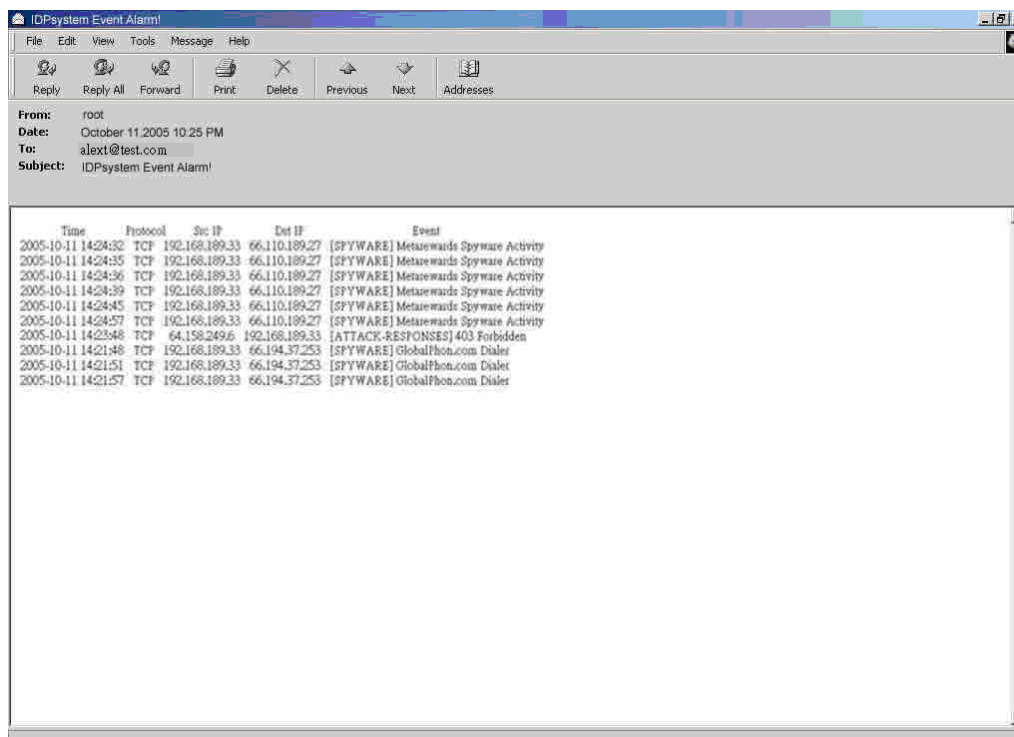
High Risk	<input type="text" value="Drop"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)
Medium Risk	<input type="text" value="Pass"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)
Low Risk	<input type="text" value="Pass"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)

OK Cancel

### The IDP setting



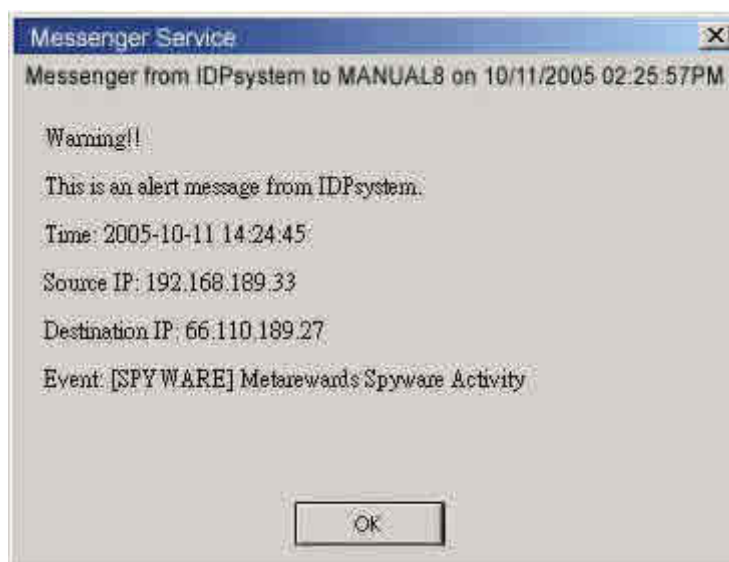
- ◆ When the CS-2000 detected the attack types corresponded to the signature, then it will send the NetBIOS notification through e-mail and results the **Log in IDP → IDP Report**.



Send the IDP notification



The MIS engineer must enable the alarm function to send mail notification in **Anomaly, Pre-defined and Custom**.



Send the NetBIOS notification to MIS engineer

1 / 823 [Next](#)

Time ▼	Event ▼	Signature Class. ▼	Interface ▼	Attack IP ▼	Victim IP:Port ▼	Action ▼
2007-06-15 09:26:46	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	58.244.79.22:11110	
2007-06-15 09:26:45	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	125.91.19.204:8097	
2007-06-15 09:24:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	61.189.185.246:19984	
2007-06-15 09:23:17	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	172.142.14.210:30000	
2007-06-15 09:22:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	201.10.78.176:11707	
2007-06-15 09:21:53	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	59.39.52.41:9539	
2007-06-15 09:19:06	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	85.178.71.24:50040	
2007-06-15 09:18:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	121.34.103.215:14187	
2007-06-15 09:18:53	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	61.228.152.1:29091	
2007-06-15 09:18:20	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	58.82.203.203:14541	
2007-06-15 09:18:13	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	211.230.82.229:26154	
2007-06-15 09:18:01	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	89.247.76.97:52910	
2007-06-15 09:18:00	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	91.122.43.182:50401	
2007-06-15 09:17:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	211.76.81.37:14690	
2007-06-15 09:17:51	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:17:49	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	60.16.94.173:2937	

### The IDP Log



The MIS engineer must enable the Log function in **Anomaly, Pre-defined and Custom**, in order to result the IDP log.

## 8.2 Signature

# Signature

The CS-2000 can provide the correspond comparison rules included **Anomaly**, **Pre-defined** and **Custom** according to different attack types.

The **Anomaly** can detect and prevent the anomaly flow and packets via the signature updating. The **Pre-defined** can also detect and prevent the intrusion through the signature updating. Both the anomaly and pre-defined signatures can not be deleted or modified. The **Custom** can detect the other internet attacks, anomaly flow packets except the original **Anomaly** and **Pre-defined** detection according to the user demand.

## 8.2.1 Anomaly

### Anomaly

- It includes the syn flood, udp flood, icmp flood, syn fin, tcp no flag, fin no ack, tcp land, larg icmp, ip record route, ip strict src record route, ip loose src record route, invalid url, winnuke, bad ip protocol, portscan and http inspect , such Anomaly detection signatures.
- User can enable the anomaly packets signature to detect, depends on the user demand.
- User can manage the specific anomaly flow packets.
- User can modify the action of pass, drop, log or alarm.
- The CS-2000 can display all the anomaly detection signature attribute of name, enable, risk, action, log and alarm.

Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
udp flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
icmp flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
syn fin	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
tcp no flag	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
fin no ack	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
tcp land	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
large icmp	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip strict src record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip loose src record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
invalid url	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
winnuke	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
bad ip protocol	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
portscan	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>		<a href="#">Modify</a>
http inspect	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>

The anomaly signature setting

## 8.2.2 Pre-defined

### Pre-defined

- It includes the Attack Responses, Backdoor, Bad Traffic, Chat, DDoS, Deleted, DNS, DoS, Exploit, Finger, FTP, ICMP, IMAP, Info, Misc, Multimedia, MySQL, NetBIOS, NNTP, Oracle, P2P, Policy, POP2, POP3, Porn, RPC, Rservices, Scan, Sellcode, SMTP, SNMP, Spyware, SQL, Telnet, TFTP, Web Acctacks, Web CGI, Web Client, Web Coldfusion, Web Frontpage, Web IIS, Web Misc, Web PHP and X11. On the other hand, every type included its attack signature.
- User can modify the signature action of pass, drop, log or alarm in every type.
- The CS-2000 can display all the attack signature attribute of name, risk, action, log and alarm.

Total IDP Signatures Number : 2913

Name	Risk	Action	Log	Alarm	Configure
+ Attack Responses (16)					Modify
+ Backdoor (75)					Modify
+ Bad Traffic (13)					Modify
+ Chat (31)					Modify
+ DDoS (33)					Modify
+ Deleted (169)					Modify
+ DNS (19)					Modify
+ DoS (19)					Modify
+ Exploit (76)					Modify
+ Finger (13)					Modify
+ FTP (70)					Modify
+ ICMP (18)					Modify
+ IMAP (39)					Modify
+ Info (9)					Modify
+ Misc (56)					Modify
+ Multimedia (10)					Modify
+ MySQL (2)					Modify
+ NetBIOS (201)					Modify
+ NNTP (13)					Modify
+ Oracle (298)					Modify
+ P2P (18)					Modify
+ Policy (21)					Modify
+ POP2 (4)					Modify
+ POP3 (27)					Modify
+ Porn (21)					Modify
+ RPC (76)					Modify
+ Rservices (13)					Modify
+ Scan (17)					Modify
+ Shellcode (21)					Modify
+ SMTP (59)					Modify
+ SNMP (17)					Modify
+ Spyware (313)					Modify
+ SQL (44)					Modify
+ Telnet (13)					Modify
+ TFTP (11)					Modify
+ Web Attacks (46)					Modify
+ Web CGI (349)					Modify
+ Web Client (18)					Modify
+ Web Coldfusion (35)					Modify
+ Web Frontpage (35)					Modify
+ Web IIS (115)					Modify
+ Web Misc (329)					Modify
+ Web PHP (126)					Modify
+ X11 (2)					Modify
+ Other (3)					Modify

### The pre-defined setting



In **Configure → Setting**, the CS-2000 will access the default action of risk setting when the user modifies the **Pre-defined**. User can modify the action of every signature depends on the user demand after the IDP configuration.

### Name

- The MIS engineer can define the signature name.

### Protocol

- The detection and prevention protocol setting includes TCP, UDP, ICMP and IP.

### Source Port

- To set the attack PC port. ( Range:0~65535 ) .

### Destination Port

- To set the attacked (victim) PC port. ( Range:0~65535 )

### Risk

- To define the threats of attack packets.

### Action

- The measures to deal with attack packets.

### Content

- To set the attack packets content.

### Advance Option

- It can filter the inbound and outbound attack packets.
- The user can choose to process the packets filtering according to the text case in signatures contents.

## Example 1

To detect the anomaly flow and packets with the custom and pre-defined settings, in order to detect and prevent the intrusion.

**Step1** In **Configure → Setting** , add the following settings :

The image shows two screenshots of the IDP configuration interface. The top screenshot is the 'IDP Setting' window, which displays update information and two checked options: 'Enable Anti-Virus (for P2P, IM, NetBIOS...)' and 'Enable NetBIOS Alert Notification'. The 'IP Address of Administrator' is set to 192.168.1.10. The bottom screenshot is the 'Set default action of all signatures' window, which shows a table for configuring actions for High, Medium, and Low risk signatures. Both windows have 'OK' and 'Cancel' buttons.

**IDP Setting**

Last updated on : 07/07/05 13:35:13 (Update signature definitions every 120 minutes)

Current version : 0.1.0 (Signature definitions updated at 07/07/04 15:34:32)

Update signature definitions immediately (Use TCP port : 80 and UDP port : 53) **Update NOW** [Test](#)

☒ Enable Anti-Virus (for P2P, IM, NetBIOS...)

☒ Enable NetBIOS Alert Notification

IP Address of Administrator

**OK** **Cancel**

**Set default action of all signatures**





High Risk	<input type="text" value="Drop"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)
Medium Risk	<input type="text" value="Pass"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)
Low Risk	<input type="text" value="Pass"/>	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Alarm	( [Pass] recommended)

**OK** **Cancel**

**The IDP configure setting**



**Step2** In **Signature** → **Anomaly** , add the following settings :

Name	Enable	Risk	Action	Log	Alarm	Configure
syn flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
udp flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
icmp flood	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
syn fin	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
tcp no flag	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
fin no ack	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
tcp land	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
large icmp	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip strict src record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
ip loose src record route	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
invalid url	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
winnuke	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
bad ip protocol	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>
portscan	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>		<a href="#">Modify</a>
http inspect	<input checked="" type="checkbox"/>	H		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Modify</a>

The anomaly setting

**Step3** In **Signature → Custom** , add the following setting :

- 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, Log and Alarm.
- **Content**, enter cracks.
- **Advance Option**, select Non-direction and Disregard text case.

Add New Signature	
Name	Software_Crack_Website (Max. 30 characters, ex: external_mounted_access)
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> IP
Source Port	0:65535 ( Range: 1 - 65535, ex: 80 or 80:80 )
Destination Port	80:80 ( Range: 1 - 65535, ex: 111:112 )
Risk	High ▼
Action	Drop ▼ <input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Alarm
Content	cracks (Max. 50 characters, ex: mount or \x6d\x6f\x75\x6e\x74)
Advance Option	
<input checked="" type="checkbox"/> Non-direction	
<input checked="" type="checkbox"/> Disregard text case	

#### The custom setting

Name	Protocol	Source Port	Destination Port	Risk	Action	Log	Alarm	Configure
Software_Crack_Website	TCP	0:65535	80:80			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete the custom setting



In **Content** , the MIS engineer can enter the string to detect or transfer it to the 16 carries ASCII code .  
 ( For example : cracks can be transfer to [63 72 61 63 6b 73] ) .

**Step4** In **Policy → Outgoing** , add the new policy and enable **IDP** :

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
VPN Trunk	None ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input checked="" type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None ▾
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

The IDP setting in policy

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

[New Entry](#)

Complete the IDP setting in policy

## 8.3 IDP Report

# **IDP Report**

The CS-2000 can display the IDP record by statistics and log. So that the enterprises can easily know the whole network status.

In this Chapter, we will make the introduction of **IDP Report**.

### 8.3.1 Setting

#### Periodic Report

- It can send the period report to recipient according to the selected date.

#### History Report

- It can send the history report according to the assigned date.
  - In **System → Configure → Setting**, enable **E-mail Alert Notification**. On the other hand , add the following settings in **IDP Report** :
    1. **Enable sending period report by mail, select Yearly report, Monthly report, Weekly report, Daily report.**
    2. **Click OK.**
    3. When the time arrived, the CS-2000 will send the report to recipient.
    4. In **History Report**, select the date to send the report.
    5. Click **Send Report**.
    6. It will send the related report to the user.



The periodic report will result in the following date:

1. **Yearly report** : It results in 00:00 AM, January first, yearly.
2. **Monthly report** : It results in 00:00 AM, first day, Monthly.
3. **Weekly report** : It results in 00:00 AM, first day, Weekly.
4. **Daily report** : It results in 00:00, Daily.

**Periodic Report**

☒ Enable sending periodic report by mail

☒ Yearly report   ☒ Monthly report   ☒ Weekly report   ☒ Daily report

---

**History Report**

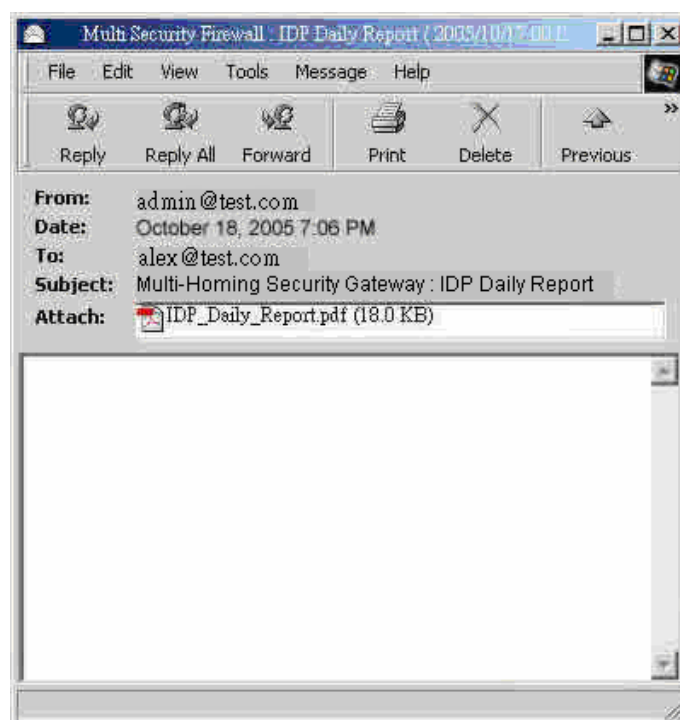
☐ Yearly report   2007

☐ Monthly report   2007   07

☐ Weekly report   2007   07   01

☐ Daily report   2007   07   05

### The periodic report setting

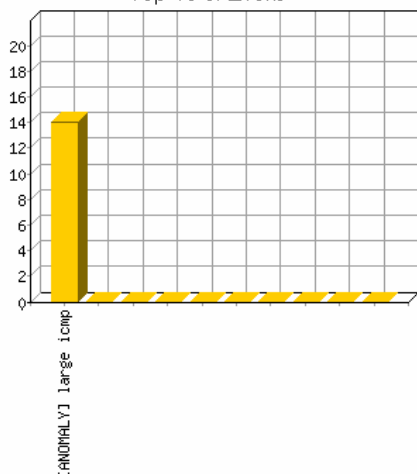


### Receive the periodic report

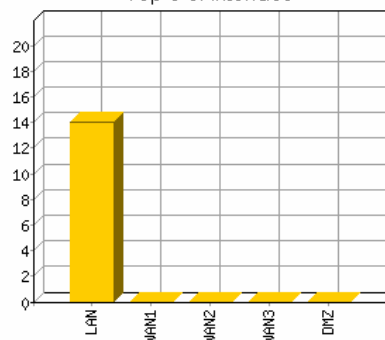
Year Month Week Day

Duration	2007-07-05 00:00:00 ~ 2007-07-05 14:31:34				
Total Unique Events	1	Total Events	14	TCP	0
First Event	2007-07-05 14:25:21	Last Event	2007-07-05 14:26:32	UDP	0
Attack IPs	1	Victim IPs	1	ICMP	14
Attack Interface	LAN	WAN1	WAN2	WAN3	DMZ
Attack Events	14	0	0	0	0

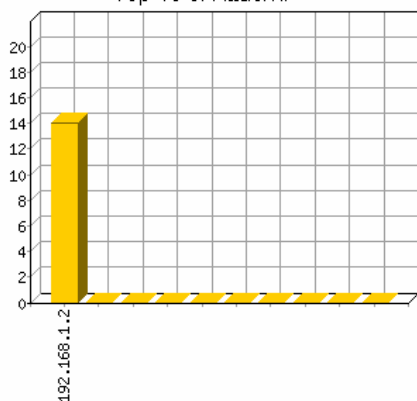
Top 10 of Event



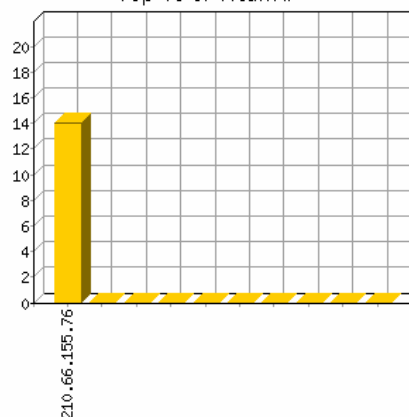
Top 5 of Interface



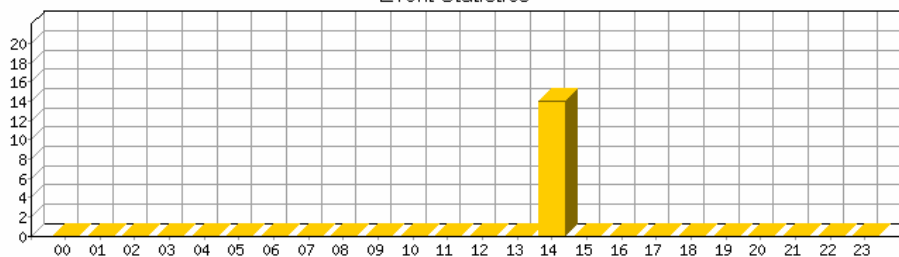
Top 10 of Attack IP



Top 10 of Victim IP



Event Statistics



### The IDP report content

**Periodic Report**

☒ Enable sending periodic report by mail

☒ Yearly report   ☒ Monthly report   ☒ Weekly report   ☒ Daily report

OK Cancel

---

**History Report**

☐ Yearly report   2007

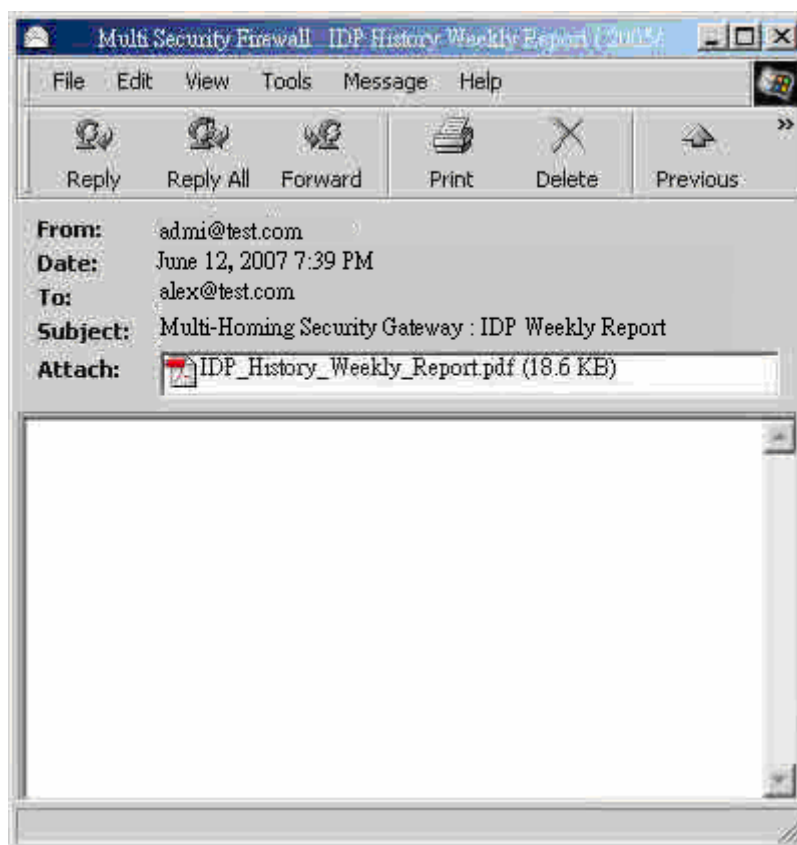
☐ Monthly report   2007   07

☒ Weekly report   2007   06   01

☐ Daily report   2007   07   05

**Send Report**

The history report setting



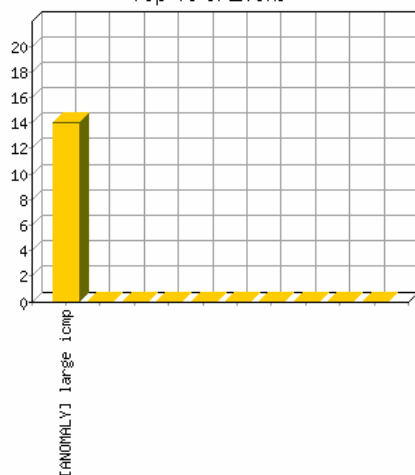
Receive the history report



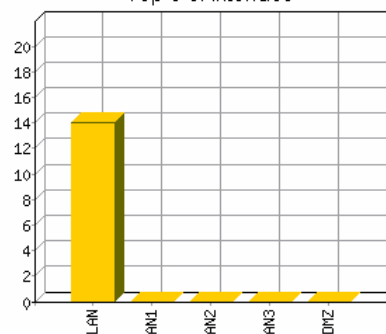
Year Month Week Day

Duration	2007-07-01 00:00:00 ~ 2007-07-05 14:40:37				
Total Unique Events	1	Total Events	14	TCP	0
First Event	2007-07-05 14:25:21	Last Event	2007-07-05 14:26:32	UDP	0
Attack IPs	1	Victim IPs	1	ICMP	14
Attack Interface	LAN	WAN1	WAN2	WAN3	DMZ
Attack Events	14	0	0	0	0

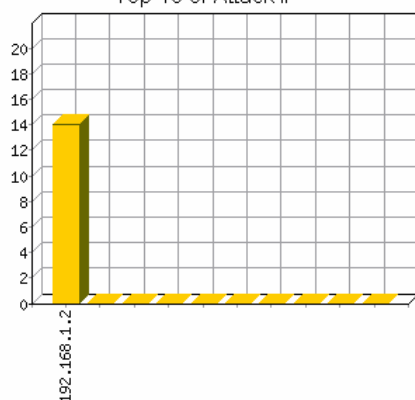
Top 10 of Event



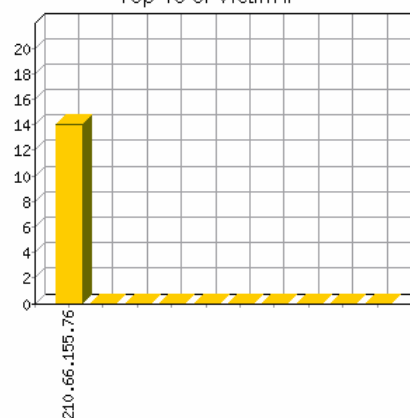
Top 5 of Interface



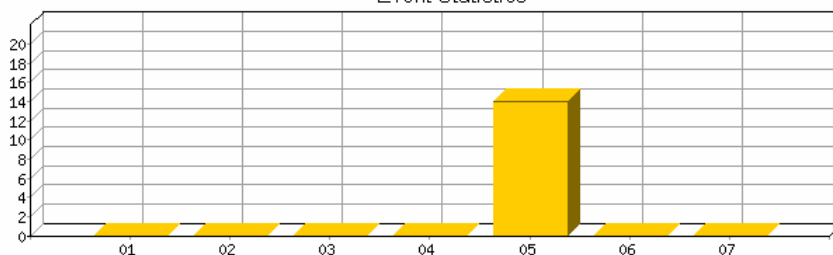
Top 10 of Attack IP



Top 10 of Victim IP



Event Statistics



### The history report content



The IDP report will attached as PDF format to send to the recipient.

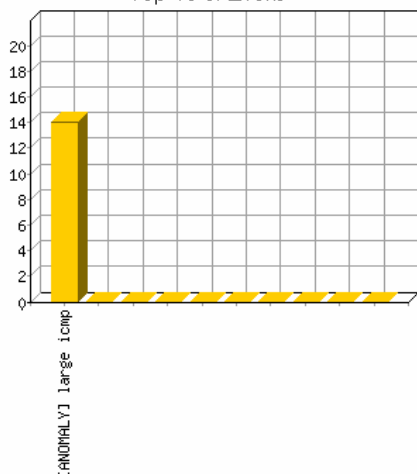
### 8.3.2 Statistics

- Step1** In **IDP Report** → **Statistics**, it shows the scanned mail statistics report in CS-2000.
- Step2** In **Statistics**, click **Day**, to view the daily report. Click **Week**, to view the Weekly report. Click **Month**, to view the Monthly report. Click **Year**, to view the Yearly report.
- Step3** The IDP Statistics.
- Ordinate : The amount signatures of detected anomaly packets and attacks.
  - Horizontal ordinate : Time.

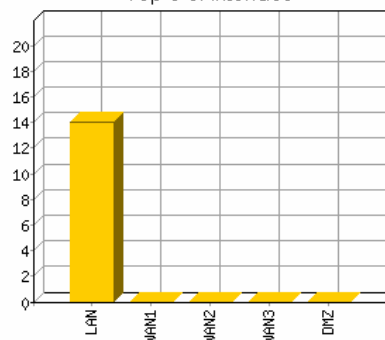
Year Month Week Day

Duration	2007-07-05 00:00:00 ~ 2007-07-05 14:31:34				
Total Unique Events	1	Total Events	14	TCP	0
First Event	2007-07-05 14:25:21	Last Event	2007-07-05 14:26:32	UDP	0
Attack IPs	1	Victim IPs	1	ICMP	14
Attack Interface	LAN	WAN1	WAN2	WAN3	DMZ
Attack Events	14	0	0	0	0

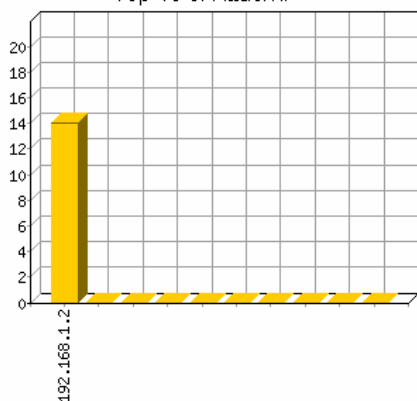
Top 10 of Event



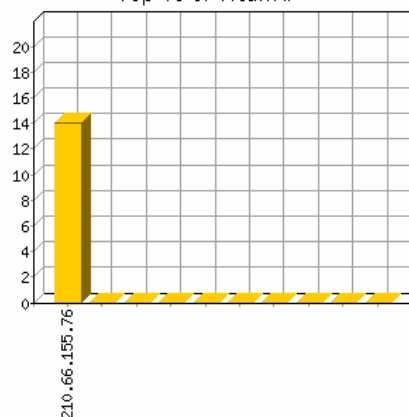
Top 5 of Interface



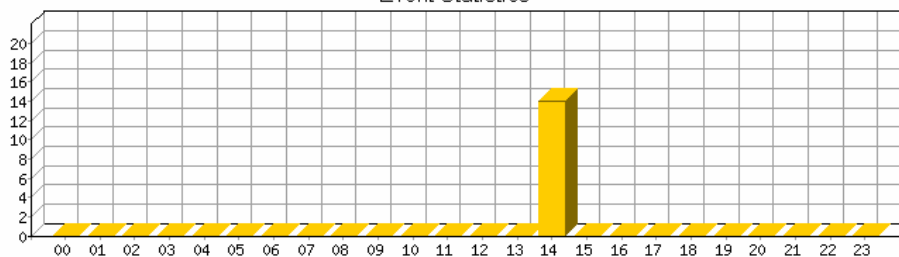
Top 10 of Attack IP



Top 10 of Victim IP



Event Statistics



### The IDP statistics

### 8.3.3 Log

#### Search

- The CS-2000 can search the records correspond to the condition depends on the Event , Signature Classification , Attack IP , Victim IP , Interface , Date and Risk .
  - Add the following settings :
    1. **Event**, enter the keyword of anomaly and attack packets events.
    2. **Interface**, select **ALL**.
    3. Select **after this date and before this date**, in order to search the record in date period.
    4. **Risk**, select **ALL**.
    5. Click **Search**.

## Search

Enter keyword or phrase

Event:  (Max. 100 characters)Signature Classification:  (Max. 100 characters)Attack IP: Victim IP: Interface: 
☒ From: 2007 / 6 / 1 0 : 0  
☒ To: 2007 / 7 / 5 14 : 44
Risk: **Search**

## Results

Search result: 3076 records

1 / 154 [Next](#)Top Time: 

Time	Event	Signature Class.	Interface	Attack IP	Victim IP	Action
2007-06-15 09:17:51	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:02:33	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:02:09	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:01:57	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:01:51	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 09:01:48	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:57:05	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	218.19.241.50:6882	
2007-06-15 08:47:59	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:38:21	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:32:20	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	71.113.231.64:6881	
2007-06-15 08:27:05	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:26:01	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	222.211.114.172:6883	
2007-06-15 08:08:26	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	218.19.241.50:6882	
2007-06-15 08:08:22	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	218.19.241.50:6882	
2007-06-15 08:07:52	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:06:11	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:03:57	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	
2007-06-15 08:03:42	[P2P] eDonkey transfer	application-Medium_r..	WAN1	61.217.152.252	192.168.1.2:4242	
2007-06-15 08:00:14	[P2P] BitTorrent transfer	application-Medium_r..	LAN	192.168.1.2	219.153.45.191:6882	

1 / 154 [Next](#)**To search the specific record**



In **Log** → **Search**, click Time link, then it shows the **Event Detail**.

#### Event Detail

Time	Event	Interface
2007-06-15 09:10:13	 [P2P] BitTorrent transfer	LAN

#### IP Header

Version	IHL	TOS	Length	
4	5	0	108	
ID			Flags	Offset
16144			0	0
TTL		Protocol	Checksum	
127		6	61816	
Source Address				
192.168.1.2				
Destination Address				
219.153.45.191				

#### TCP Header

Source Port			Destination Port		
1354			6882		
Sequence Number					
1460322597					
Acknowledgment Number					
958354565					
Data offset	Reserved		Flags	Windows	
5	0		24	65535	
Checksum				Urgent pointer	
65491				0	

#### Packet Data

Data Payload	
0000 13 42 69 74 54 6F 72 72 65 6E 74 20 70 72 6F 74	. B i t T o r r e n t p r o t
0010 6F 63 6F 6C 65 78 00 00 00 00 00 00 4A 2D 73 97	o c o l e x . . . . . J - s .
0020 59 C9 A0 3D 5F CE EE C0 ED 11 D2 9E EC 90 BB C4	Y . . = _ . . . . .
0030 2D 42 43 30 30 37 30 2D DF A0 E6 1B D8 73 33 69	- B C 0 0 7 0 - . . . . . s 3 i
0040 C1 70 0B 18	. p . .

The event detail



In Log, the CS-2000 can make the sorting by Time, Event, Signature Classification, Interface, Attack IP, Victim IP Port and Action.

**Step1** In IDP Report → Log, it shows the IDP status in CS-2000.

1 / 823 [Next](#)



Time ▼	Event ▼	Signature Class. ▼	Interface ▼	Attack IP ▼	Victim IP:Port ▼	Action ▼
2007-07-05 14:26:32	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:26:27	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:26:21	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:26:16	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:26:10	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:26:05	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:59	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:54	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:48	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:43	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:37	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:32	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:26	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-07-05 14:25:21	[ANOMALY] large icmp	Anomaly	LAN	192.168.1.2	210.66.155.76	
2007-06-15 09:26:46	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	58.244.79.22:11110	
2007-06-15 09:26:45	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	125.91.19.204:8097	
2007-06-15 09:24:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	61.189.185.246:19984	
2007-06-15 09:23:17	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	172.142.14.210:30000	
2007-06-15 09:22:56	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	201.10.78.176:11707	
2007-06-15 09:21:53	(portscan) Portscan detected!	Anomaly	LAN	192.168.1.2	59.39.52.41:9539	

[Clear Data](#)

1 / 823 [Next](#)

### The IDP log



The icon description in Log :

#### 1.Action :

Icon		
Description	Pass	Drop

#### 2.Risk :

Icon			
Description	High Risk	Medium Risk	Low Risk

## Chapter 9: Anomaly Flow IP

# **Anomaly Flow IP**

When the CS-2000 received the intrusion packets from internal PCs, it will block this abnormal packets, to prevent the Company's network be paralyzed.

**In this chapter, we will make the introduction and settings of Anomaly Flow IP.**



## Example 1

The CS-2000 can make the alert and also prevent the DDoS attack packets from the internal virus-infected PCs.

Step1. In **Anomaly IP → Setting** :

- The threshold sessions of virus-infected is ( default is 100 sessions/sec)
- Select **Enable Virus-infected IP Blocking** ( Blocking Time 600 seconds)
- Select **Enable E-Mail alert notification**.
- Select **Enable Snmp Trap Alert Notification**.
- Select **Enable NetBIOS Alert Notification**.
- Enter 192.168.189.30 in **IP Address of Administrator**.
- Click **OK**.

Anomaly Flow IP Setting

The threshold sessions of anomaly flow (per Source IP) is  Sessions / Sec ( Range: 1 - 999 )

☒ Enable Anomaly Flow IP Blocking      Blocking Time  seconds ( Range: 1 - 999 )

☒ Enable E-Mail Alert Notification

☒ Enable SNMP Trap Alert Notification

☒ Enable NetBIOS Alert Notification      IP Address of Administrator

☐ Enable Core Switch Port Blocking

Alert message to be displayed to the internal user from which anomalous flow is detected [Preview](#)

CS-2000 Alart Message Page !!!!

The anomaly flow IP setting



Enable **Co-Defense System**, then the CS-2000 can send the defense message to the assigned **Switch Model**. And the switch will block the anomaly flow packets which sent to this switch model.

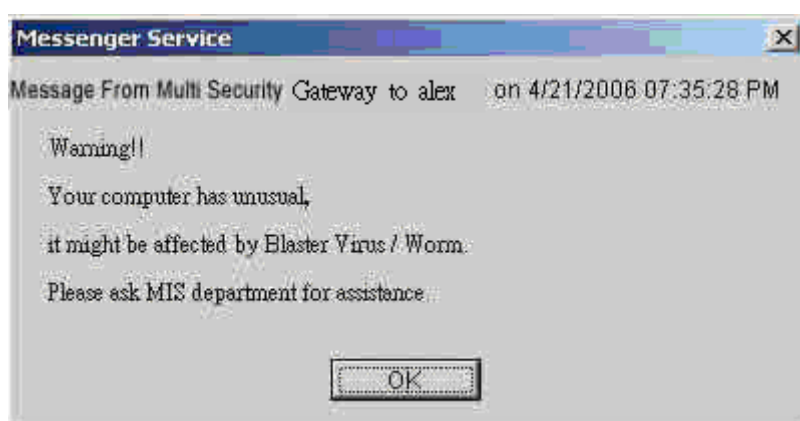


User can add **Non-detect IP**, and system will not detect the flow of Non-detect IP.

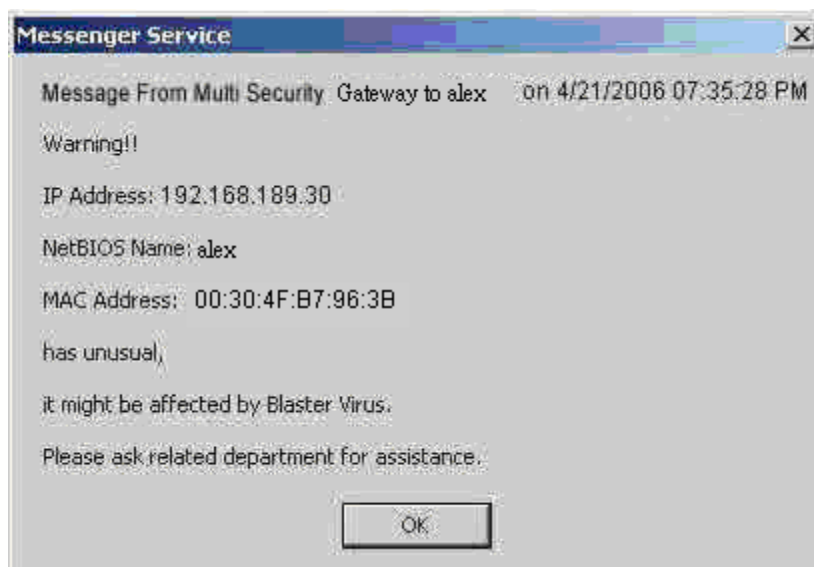
- Step2.** After complete the **setting of anomaly flow IP**, the system will show the alert message in **Anomaly Flow IP→ Virus-Infected IP** or instant send the **NetBIOS alert notification** to the virus-infected PC and MIS engineer's PC when the CS-2000 detect the amount of DDoS attack occurred.

Threshold Sessions / Sec : 100			
Interface	Virus-infected IP	MAC Address	Alarm Time
LAN	192.168.169.30	00 30 4f b2 96 3b	2006-04-21 19:35:28

#### The virus-infected IP

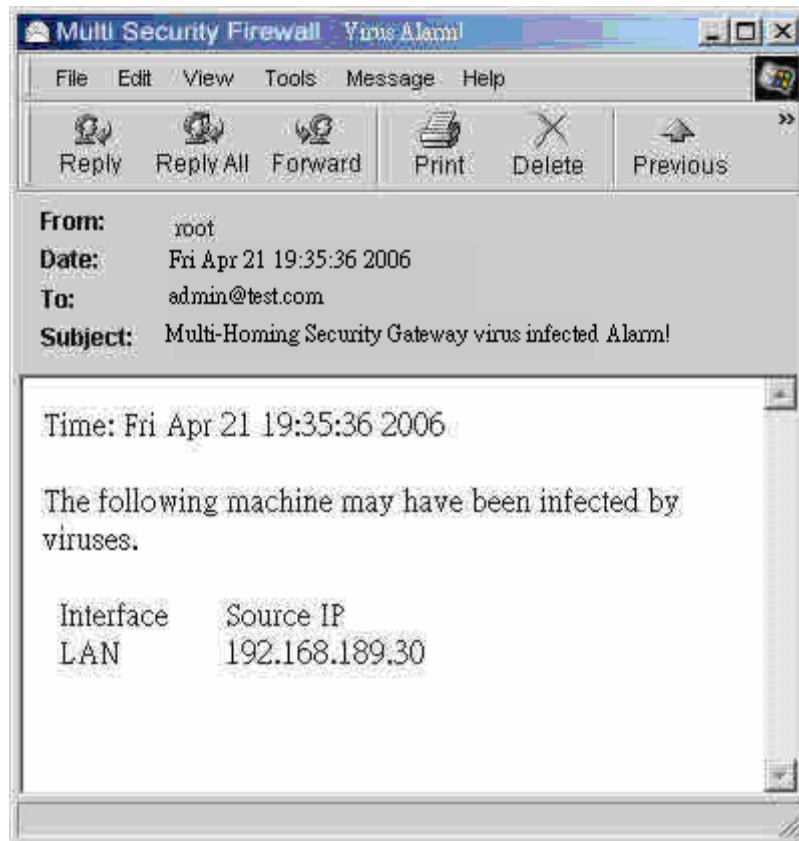


#### Send the NetBIOS alert notification to virus-infected PCs



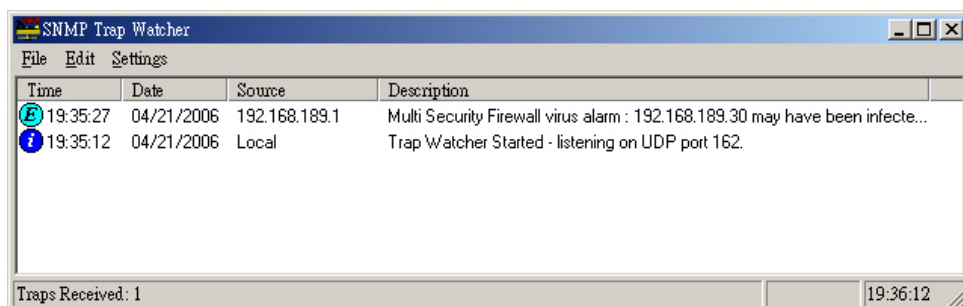
#### Send the NetBIOS alert notification to the MIS engineer

- Step3.** If the MIS engineer enabled the **e-mail alert notification** in **System → Configure → Setting**, then the CS-2000 will automatically send the mail notification to the MIS engineer.



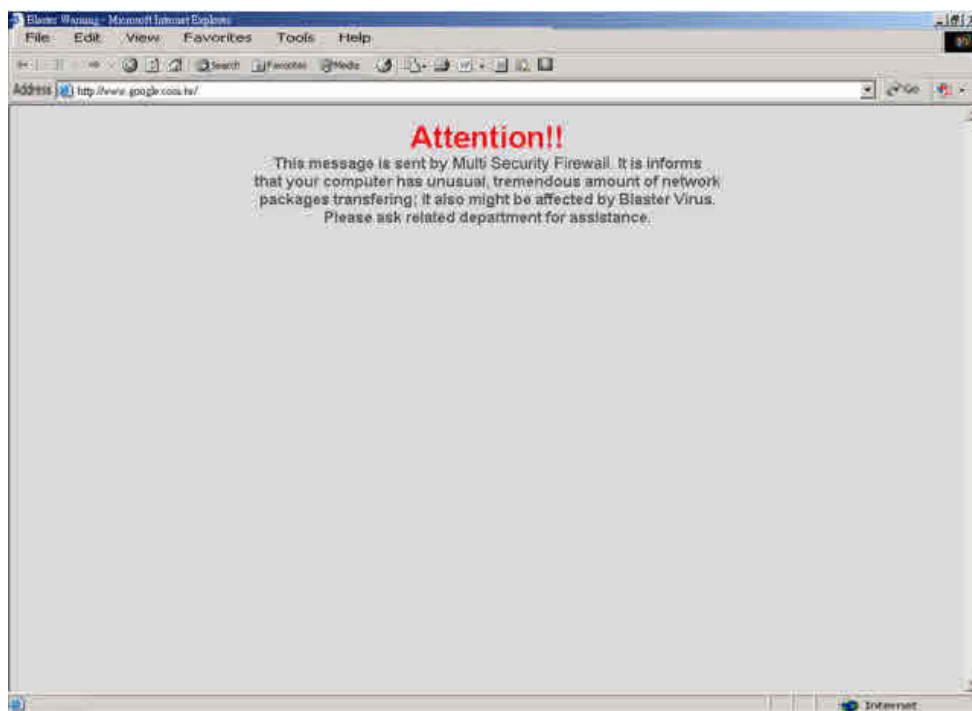
Internal virus alarm

- Step4.** If the MIS engineer set the settings of **System → Configure → SNMP → Enable SNMP Trap Alert Notification**, then the CS-2000 will show the instant alert message on the SNMP Trap client software installed in administrative PC.



The SNMP Trap client receive the virus alert by the client software

- Step5.** When internal PCs got virus-infected, the CS-2000 will show the alert message at first time (If the virus-infected user can not solve the problem then the CS-2000 will restrict the virus-infected user and it will make the link speed slow and will not show any alert message again.)



**Show the alert message**

## Chapter 10: Web VPN/SSL VPN

### **Web VPN / SSL VPN**

Since the network secure remote access high demanding large enterprise has risen up. To the users, the most reliable solution is the SSL VPN without installing any software or hardware. Only need to use the web browser and easily access the data transferring by SSL encryption.

## The VPN terms

### DES

- The DES (Data Encryption Standard) is a kind of NIST W with 56 bytes preshared key.

### 3DES

- The 3DES (Triple Data Encryption Standard) is more secure than DES with 168 bytes.

### AES

- The AES is the high standard of data encryption, and its standard is more strict than the DES. The AES Key Size can divide into 128 bytes, 192 bytes and 256 bytes.

## Setting

### VPN IP of Client

Creates the SSL VPN between the client and the CS-2000 appliance by login authentication, VPN IP range, encryption algorithm, Protocol, server port and connecting time. And set the end user can use the IP address distribute by the DNS or WINS server, to access the internal resources through the NAT mode.

■



The SSL VPN IP range can not be the same as the segment of LAN (LAN, Multiple Subnet, DMZ), WAN and PPTP server.

### Internal Subnet of Server

- To set the client user can access the internal subnet of server.

## Status

### User Name

- To display the authentication name used by client.

### Real IP

- To display the client real IP.

### VPN IP

- To display the client IP distributed by the CS-2000.

### Uptime

- To display the uptime between client and CS-2000.

### Configure

- The MIS engineer can choose to disconnect the SSL VPN.

User Name	Real IP	VPN IP	Uptime	Configure
No Data				

### Status list

## Example 1

### Set the Web / SSL VPN between CS-2000 and WAN Client

**Step1** In **Interface** → **WAN**, enable HTTPS.

Balance Mode: Auto ( Auto recommended )

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping / Traceroute	HTTP	HTTPS	Configure	Priority
1	Static IP	61.62.236.15	2				<a href="#">Modify</a>	1
2	Static IP	210.66.155.77	1				<a href="#">Modify</a>	2
3	(Disable)	---	0	---	---	---	<a href="#">Modify</a>	0

#### WAN interface setting

**Step2** In **Authentication** → **User** , add the following settings :

<u>Authentication User Name</u>	Configure
alex	<a href="#">In Use</a>
eva	<a href="#">In Use</a>
joe	<a href="#">In Use</a>

#### Authentication user setting

**Step3** In **Authentication** → **User Group** , add the following settings :

<u>Name</u>	Member	Radius	POP3	LDAP	Configure
Auth_Group	alex, eva, joe				<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>

#### Authentication user group setting



**Step4** In **Web VPN / SSL VPN → Setting** , add the following settings :

- Click **Modify**.
- **Enable Web VPN**.
- **VPN IP Range**, enter 192.168.222.0 / 255.255.255.0.
- **Encryption Algorithm**, select 3DES.
- **Protocol**, select TCP.
- **Server Port**, enter the default value of 1194.
- **Authentication User or Group**, select laboratory.
- **Auto-Disconnect if idle** enter 0.
- Click **OK**.
- It will automatically add the LAN interface which is the segment that allow the client to access.

**Web VPN Setting**

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

VPN IP Range  /

Encryption Algorithm

Protocol

Server Port  ( Range: 1024 - 65535 )

☐ Enable DNS and WINS server addresses to clients

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

☐ Enable NAT mode

Authentication User or Group

Auto-disconnect if idle for  Minutes ( Range: 0 - 120, 0: means always connected )

### Enable Web VPN

**VPN IP of Client**

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

VPN IP Range : 192.168.222.0

Netmask : 255.255.255.0

Encryption Algorithm : AES-128

Authentication User or Group : Auth\_Group

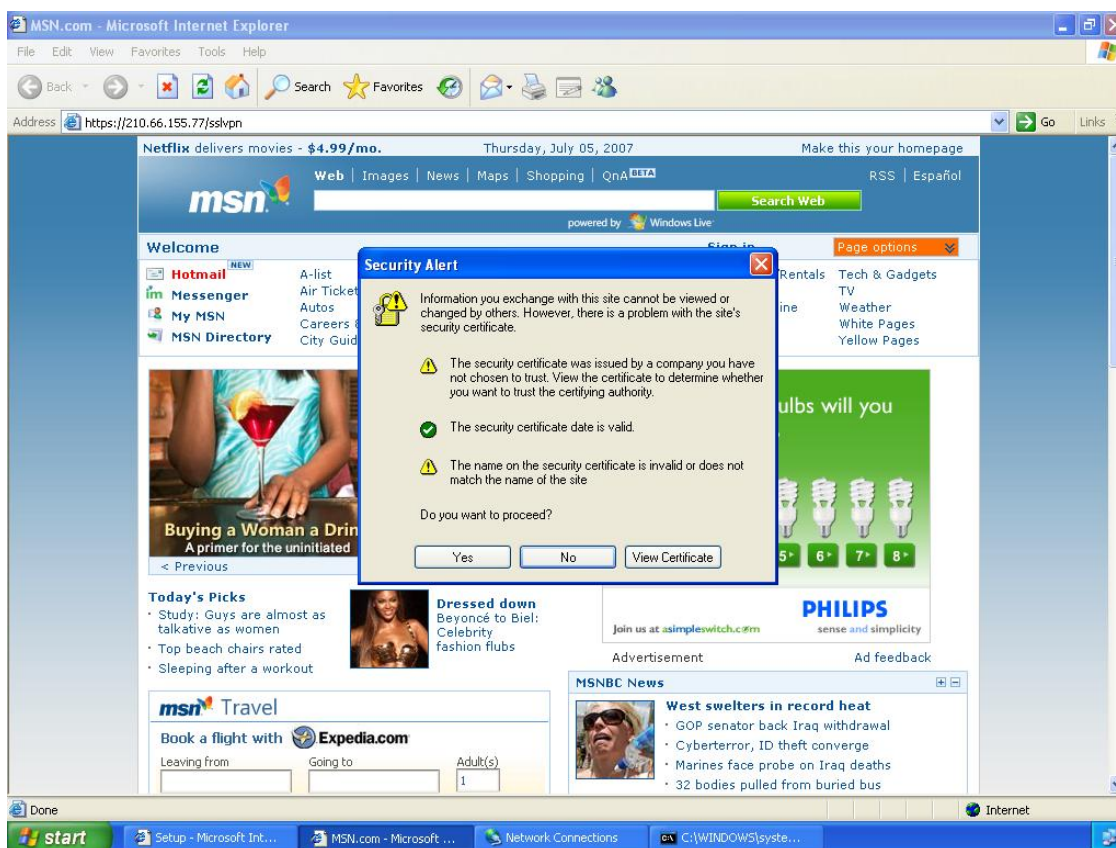
**Internal Subnet of Server**

Internal Subnet	Netmask	Configure
192.168.1.0	255.255.255.0	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Enable Web VPN

**Step5** Enter the following settings in client web browser :

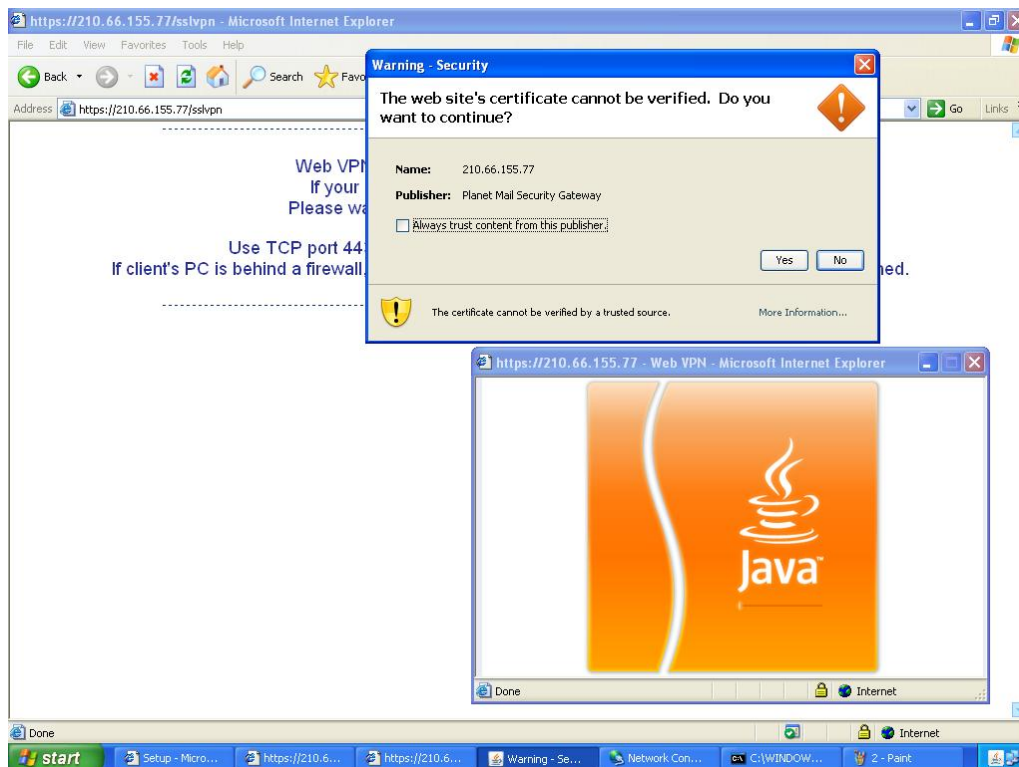
- In **Address**, enter `http://210.66.155.77/sslvpn` or `http://210.66.155.77/webvpn` ( It is the CS-2000 interface add the sslvpn or webvpn string ) .
- Click **Enter**.
- In **Security Alert**, click **OK**.
- In **Security Alert**, click **OK**.
- In **Warning HTTPS**, click **Yes**.
- In **Warning Security**, click **Yes**.
- In **Authentication**, enter josh in **User Name** and 123456789 in **Password**.
- Click **OK**.



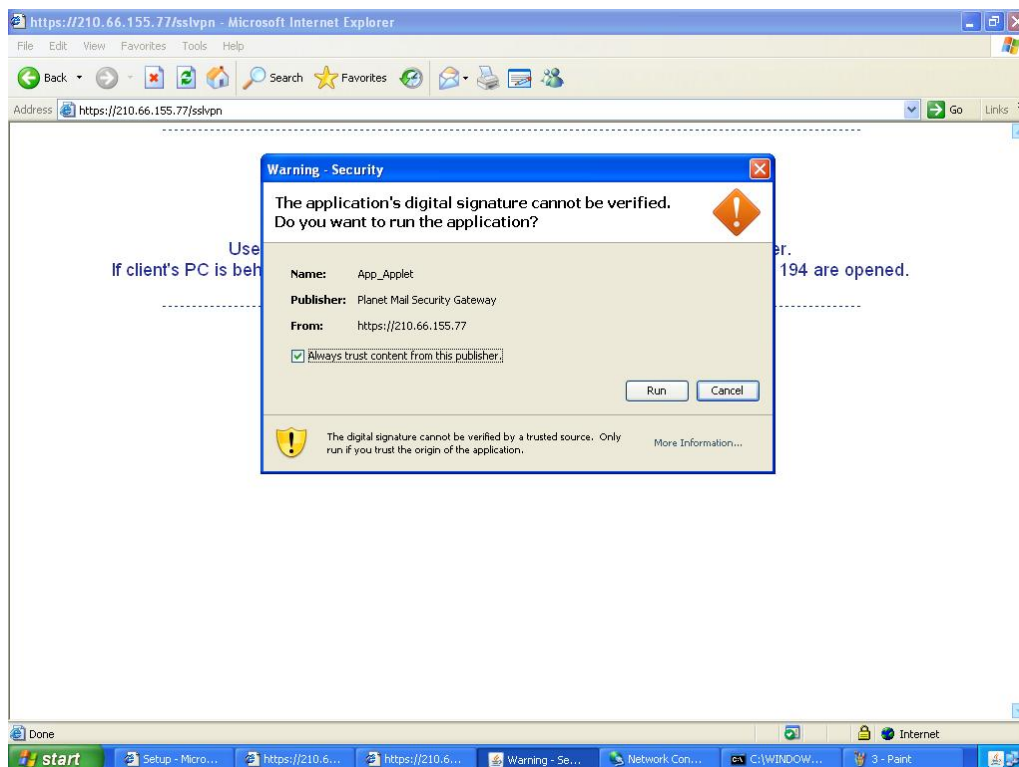
**Login SSL VPN**



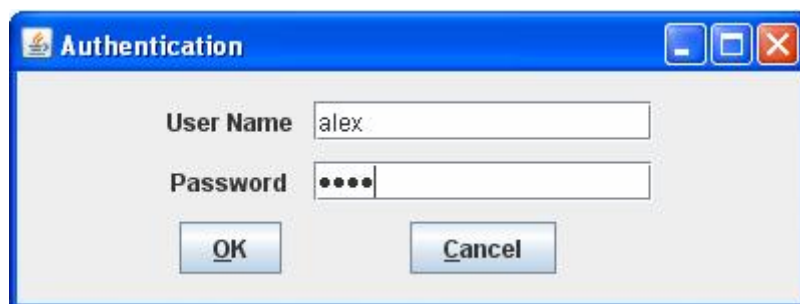
The warning security window



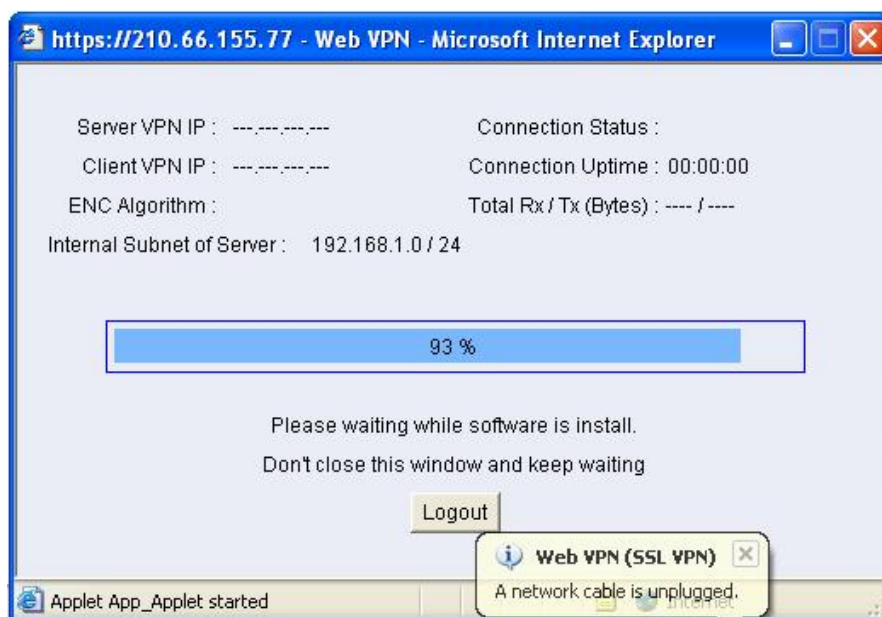
The warning security window



The warning security window



The authentication window



The SSL VPN connection



Complete the SSL VPN connection

**Step6** In **Web VPN / SSL VPN → Status**, it shows the connection status :

User Name	Real IP	VPN IP	Uptime	Configure
alex	210.66.155.80	192.168.222.10	0:02:59	<a href="#">Disconnect</a>

SSL VPN status



When the client PC is not installed the SUN JAVA runtime environment software , it will automatically download and install this software as in SSL VPN connection.



The Java runtime environment plug-in CA certificate



The Java runtime environment plug-in installation

## Chapter 11: Advance

### 11.1 Inbound Balance

# **Inbound Balance**

The CS-2000 provides the inbound balance to company's web site. When the main network connection disconnected, the customer can use another connection to link to company's web site. The CS-2000 can also provide the load balance function to the service connection, and distribute the proper load of to the internal server group. The Load Balance can reduce the server load and system crash risks, in order to improve the server working efficiency.

**In this Chapter, we will make the introduction of InBound Balance.**



## Inbound Balance

### Domain Name

- It represents the name of DNS which the user applied it from ISP. To the User, the IP address is not suitable to memorize and manage. Because of the reason, we can use domain to instead of the IP address, and its format is xx.xx.xx.xx (For example, <ftp.ccu.edu.tw> , [www.ccu.edu.tw](http://www.ccu.edu.tw) ).In other words, we use the English string of ccu.edu.tw instead of the IP, and then the English string is the domain name.

The address includes two parts , the host name and domain name. If the user wants to browse Yahoo web site, then he can enter [www.yahoo.com](http://www.yahoo.com) . In fact, the Yahoo IP address is 66.218.71.84. The MIS engineer can create the domain name mapped to IP between the [www.yahoo.com](http://www.yahoo.com) domain name and IP via the DNS server.

**Enable DNS Zone** : To enable DNS zone setting in inbound load balance.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☐ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
<input type="button" value="New Entry"/>						

### Inbound load balance setting

### DNS Configuration

- To apply the DNS from the address register web site.
  - Register a domain name of test.net.tw.
  - Assume the IP address are :
    - 61.11.11.10 ~ 61.11.11.14
    - 211.22.22.18 ~ 211.22.22.30
  - The main host is
    - Host Name : dns1.test.net.tw
    - IP Address : 61.11.11.11
 The second Host is
    - Host Name : dns2.test.net.tw
    - IP Address : 211.22.22.22



**Select type** : A, CNAME and MX.

### 1.A :

To set the host name mapped to IP address.

**Example 1** : Set up the host name mapped to IP address :

Host Name	Type	IP
host1.test.net.tw	A	61.11.11.12
host2.test.net.tw	A	61.11.11.13
host2.test.net.tw	A	211.22.22.23

**Server name mapped to IP address**

The "A" represents the address. To record the host name mapped to IP address. The DNS has two address records; because of host2 has two addresses. The DNS search can be define to search a host name which can reply more than one record. The DNS search results can be ordered by address-sorting or round –robin.

### 2. CNAME

Provided the domain name mapped to address, and offers external user use another (or more than one) domain name to search. The CNAME can be define to mapped to the domain name which mapped to address, but it's not recommended to use another domain name which the CNAME correspond to.

#### Example 2 :

The CNAME is used to map the Alias to its formal name.

Host Name	Type	Address
host23.test.net.tw	A	61.11.11.14
host5.test.net.tw	CNAME	host23.test.net.tw

**The CNAME can mapped the alias to its formal name**

In other words, the CNAME of host5.test.net.tw is mapped to the formal name of host23.test.net.tw.

If we ping the host5.test.net.tw in DOS, then it will shows the IP address of 61.11.11.14.

### 3. MX

The MX can precede the mail transfer by the DNS search. If user want to change the mail server, then he only need to modify the DNS record, in other words, the destination mail server has no need to know which mail server that the user used to transfer mails.

#### Example 3 :

The MX represents the mail exchange; it is a kind of DNS record used to provide the e-mail service.

Host Name	Type	Address
host25.test.net.tw	A	211.22.22.24
mail.test.net.tw	MX	host25.test.net.tw

**The MX mapped relations**

If we type `nslookup -type=MX mail.test.net.tw` in DOS. ( The nslookup is the DNS search command, and the strings after -type represents the DNS record. The mail.test.net.tw is the searched DNS host name which mapped to the host25.test.net.tw mail exchange and it also mapped to the IP address of 211.22.22.24.

We assume that test Customer Service Center sends the e-mail to [mary@mail.test.net.tw](mailto:mary@mail.test.net.tw) . The Customer Service people send the mails through the test.com.tw (SMTP Server), and the SMTP Server will ask mail.test.net.tw of which way to send mails via the DNS search. The way to search the MX record in mail .test.net.tw. :

Host Name	Type	Address
host3.test.net.tw	A	61.11.11.10
mail.test.net.tw	MX	host3.test.net.tw

**The way to search the MX record in mail.test.net.tw**

The mail server of mail.test.net.tw will send e-mails to the address of host3.test.net.tw via SMTP Protocol.

- **Name** : It represents the host name in front of domain name. (User can define the name)
- **Reverse** : We can use the IP address to search the domain name. The DNS included two mapped functions : Positive and reverse. For example, if we type [www.test.com](http://www.test.com) , the DNS will help us to translate it to 61.218.49.29, and it is the kind of positive results, vice versa.

**Example 4 :**

For example, we use the nslookup command in DOS, to test if the positive and reverse results are correct.

```
C:\>nslookup host1.test.net.tw ----->Positive Search
```

```
Server:  dns.hinet.net
```

```
Address: 168.95.1.1
```

```
Name : host1.test.net.tw
```

```
Address : 61.11.11.12
```

```
C:\>nslookup 61.11.11.12 ----->Reverse Search
```

```
Server:  dns.hinet.net
```

```
Address: 168.95.1.1
```

```
Name : host1.test.net.tw
```

```
Address : 61.11.11.12
```

The IP address of 61.11.11.12 mapped to host1.test.net.tw.

### Balance Mode

- **Round-Robin** : It use the round-robin mode depends on the weight and priority.
- **Backup** : After user confirms the backup mode and it will enabled as disconnection occurred.

#### It shows the setting list:

- **Name** : It represents the service name used by domain name.
- **Type** : It represents the server type. A (Address) CNAME (Canonical NAME) MX (Mail exchanger)
- **Address** : It represents the IP address used by internal server.
- **Backup** : To confirm if the internal server use backup function. (the user can select WAN 1 or WAN 2)
- **Weight** : The internal server will distribute the round-robin weight depends on the settings, and every number represents the round-robin times.
- **Priority** : To adjust the use priority of every internal server.

**Advanced Description**

The so called DNS mapped represents the domain is managed by which DNS server, and all the domain name internet records are recorded in the DNS host. For example, the real IP address in web site or mail server, so the DNS server must correctly link to internet and its DNS record must be correct.

According to the international rule, the DNS must correspond to two DNS server, in order to assure the network stability. Both of the DNS servers can provide the backup function if any of them breaks down. On the other hand, the backup function not only assures the internet stability but also ensure the fluency of the user to use the domain name.

**Example :**

We can set a server which applied the following situation.

- 1 · To register a domain name called test.net.tw.
- 2 · The primary server IP is 61.11.11.11. Host name is dns1.test.net.tw.  
The secondary server IP is 211.22.22.22. Host name is dns2.test.net.tw.
- 3 · Prepare the internet leased line or ADSL to link to internet.
- 4 · The server to analyzed :  
www.test.net.tw (192.168.1.100) web server  
mail.test.net.tw (192.168.1.101) e-mail server

First of all, we must apply two ADSL static IP (or Network Leased Line) from the ISP.

The IP address are :

61.11.11.10 ~ 61.11.11.14

211.22.22.18 ~ 211.22.22.30

To register the DNS setting from the address register web site.

Primary host server

Host name : dns1.test.net.tw

IP address : 61.11.11.11

Secondary host server

Host name : dns2.test.net.tw

IP address : 211.22.22.22

\* The DNS domain name applied from the registered web site, which must be correspond to the static IP.

Add the following settings of inbound load balance :

Name	Type	Address	Reverse	Weight	Priority
test.net.tw	A	61.11.11.11	O	1	1
test.net.tw	A	211.22.22.22	O	1	2

**The Primary and Secondary DNS Name mapped to IP**

The **backup** can let the secondary DNS replace the primary DNS when the primary DNS is broken.

For example, we can use the nslookup command in DOS, in order to test if the reverse and positive analysis is correct.

```
C:\>nslookup test.net.tw
```

```
Server:  dns.hinet.net
```

```
Address: 168.95.1.1
```

```
Name: test.net.tw
```

```
Addresses: 61.11.11.11, 211.22.22.22 ----->To test if the DNS Domain Name correctly mapped  
to the IP. (Positive)
```

```
C:\>nslookup 61.11.11.11
```

```
Server:  dns.hinet.net
```

```
Address: 168.95.1.1
```

```
Name: test.net.tw
```

```
Address: 61.11.11.11 ----->To test if the DNS Domain Name correctly mapped to  
the IP. (Reverse)
```

Set the following settings of InBound Load Balance :

Name	Type	Address	Weight	Priority
web.test.net.tw	A	61.11.11.11	1	1
web.test.net.tw	A	211.22.22.22	2	2
www.test.net.tw	CNAME	web.test.net.tw	--	--

**The CNAME record in [www.test.net.tw](#)**

For example, we can use the nslookup command in DOS, in order to test if the positive analysis results the following situation.

C:\>nslookup

Default Server : dns.hinet.net

Address : 168.95.1.1

> server 61.11.11.11 ----->Switch to the original built DNS Server

Default Server : web.test.net.tw

Address : 61.11.11.11

> www.test.net.tw ----->To test if the web correctly mapped to the IP (Positive)

Server : web.test.net.tw

Address : 61.11.11.11

Name : web.test.net.tw ----->The Alias of [www.test.net.tw](#) mapped to the formal name of web.test.net.tw.

Addresses : 61.11.11.11, 211.22.22.22 ----->The results is correct.

Aliases : www.test.net.tw -----> The Alias of web.test.net.tw

The web.test.net.tw mapped to the Host Name and other IP Address via DNS.

In Fig. 21-6

Users enter the [www.test.net.tw](http://www.test.net.tw) depends on the following priority.

The 1st user enter 61.11.11.11 server

The 2nd user enter 211.22.22.22 server

The 3rd user enter 211.22.22.22 server

**(Finished to distribute the Round-Robin Priority)**

The 4th user enter 61.11.11.11 server

**(Restart to distribute the Round-Robin Priority)**

The 5th user enter 211.22.22.22 server

The 6<sup>th</sup> user enter 211.22.22.22 server

When the 3<sup>rd</sup> user enter [www.test.net.tw](http://www.test.net.tw) , the enter timing is over 1 in the setting of the weight priority with the IP (61.11.11.11) , so the inbound load balance will distribute the 3<sup>rd</sup> user to the weight priority of 2 with the IP (211.22.22.22) . When finished all the weight priority allocate, the system will re-connect all the user and follow the weight priority distribution again. This is the so called inbound load balance, which can distribute the round – robin mode to many users who link to the Alias of [www.test.net.tw](http://www.test.net.tw) web server depends on the weight priority.

The less MX priority number has the highest priority. For example, the user A sends a mail to user B of [mary@mail.test.net.tw](mailto:mary@mail.test.net.tw).

The user A send the mail through hinet.net.tw (SMTP server), and the hinet.net.tw will determine which way the mail.test.net.tw to send the mails depends on the DNS search. First of all, we can look for the MX record in mail.test.net.tw. :

Name	Type	Address	Reverse	Weight	Priority
mail.test.net.tw	MX	smtp1.test.net.tw	X	--	1
mail.test.net.tw	MX	smtp2.test.net.tw	X	--	2

**The MX record in mail.test.net.tw**

It is because the 1 number has the top priority, so the server will try to send mails through the host of smtp1.test.net.tw (through SMTP Protocol). If it failed to send these mails, then the mails would be sending through the second priority of smtp2.test.net.tw.



### 11.1.1 Inbound Load Balance Examples

We set 4 inbound balance environments.

No.	Application Environment	Pages
<b>Example. 1</b>	Set the web server settings in <b>InBound Load Balance→ A Type → Backup.</b>	<b>472</b>
<b>Example. 2</b>	Set the web server settings in <b>InBound Load Balance→ A Type → Round-Robin.</b>	<b>477</b>
<b>Example. 3</b>	Set the web server settings in <b>InBound Load Balance→ CNAME→ Round-Robin.</b>	<b>484</b>
<b>Example. 4</b>	Set the mail server settings in <b>InBound Load Balance→ Round-Robin.</b>	<b>492</b>

#### Deployment

The DNS domain name has corresponded to the static IP.

##### Interface → WAN

**WAN1 IP is 61.11.11.11**

**WAN2 IP is 211.22.22.22**

To apply two ADSL lines with static IP

( WAN1, static IP is 61.11.11.10 ~ 61.11.11.14 )

( WAN2, static IP is 211.22.22.18 ~ 211.22.22.30 )

To Apply the DNS domain name (test.com) from the ISP.

To apply the DNS setting from the registered web site.

##### The Primary Name Server

host name : dns1.test.com

IP address : 61.11.11.11

##### The Secondary Name Server

host name : dns2.test.com

IP address : 211.22.22.22

## Example 1

**Set the web server settings in InBound Load Balance→ A Type → Backup.**

**Backup** : In order to keep the network stability as the web server disconnected. We can add the backup settings in InBound Load Balance :

**Step1** In InBound Balance → New Entry.

**Step2** In **Domain Name**, enter test.com (applied from the ISP). **Enable DNS zone**→ **OK**→ **New Entry**.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
-----------	------	---------	--------	--------	----------	-----------

Add new domain name

**Step3** In InBound Balance → Setting → Modify → Inbound Balance Configuration → Select type → A (Address).

**Step4** Add the first record, **Name**, enter **www**.

In **Address**, select WAN 1, click Assist, select 61.11.11.11. The IP address will appear in **Address**. In **Balance Mode** → **Round Robin** → **OK**.

The screenshot shows the 'InBound Balance Configuration' dialog box. At the top, there are three radio buttons for 'Select type': 'A (Address)' is selected, followed by 'CNAME (Canonical NAME)' and 'MX (Mail eXchanger)'. Below this is a 'Host Name' field containing 'www' with a note '(Max. 255 characters, ex: www)'. The 'Address' section has a text field with '61.11.11.11', a dropdown menu set to 'WAN1', a red 'Assist' button, and a checked 'Reverse' checkbox. The 'Balance Mode' section has three radio buttons: 'Round-Robin' is selected, followed by 'Backup', and a dropdown menu set to 'WAN2'. At the bottom right are 'OK' and 'Cancel' buttons.

**The first inbound balance setting****Step5** Add the second record, **Name**, enter **www**.

In **Address**, select WAN 2, click Assist, select 211.22.22.22. The IP address will appear in **Address**. In **Balance Mode** → **Backup** → **OK**.

The screenshot shows the 'InBound Balance Configuration' dialog box for the second record. The 'Select type' section remains the same with 'A (Address)' selected. The 'Host Name' field still contains 'www'. In the 'Address' section, the text field now contains '211.22.22.22', the dropdown menu is set to 'WAN2', the 'Assist' button is red, and the 'Reverse' checkbox is unchecked. In the 'Balance Mode' section, the 'Backup' radio button is now selected, and the dropdown menu is set to 'WAN1'. The 'OK' and 'Cancel' buttons are at the bottom right.

**The second inbound balance setting**

**Step6** Complete the settings.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
www	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
www	A	211.22.22.22(WAN2)	WAN1	1	2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>



Complete the settings

**Step7** In **Virtual Server** → **Server 1** → click here to configure.**Step8** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 1), click **OK**. Click **New Entry** → **Service** → **HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service	HTTP (80)
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

Server 1 setting

**Step9** In **Policy → Incoming**, add the following settings, and click **OK**.


Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)						<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1 

[New Entry](#)

Add the first policy

**Step10** In **Virtual Server → Server 2**→ **Click here to configure**.



**Step11** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 2), click **OK**. Click **New Entry**→ **Service** → **HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service	HTTP (80) 
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

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

Server 2 setting

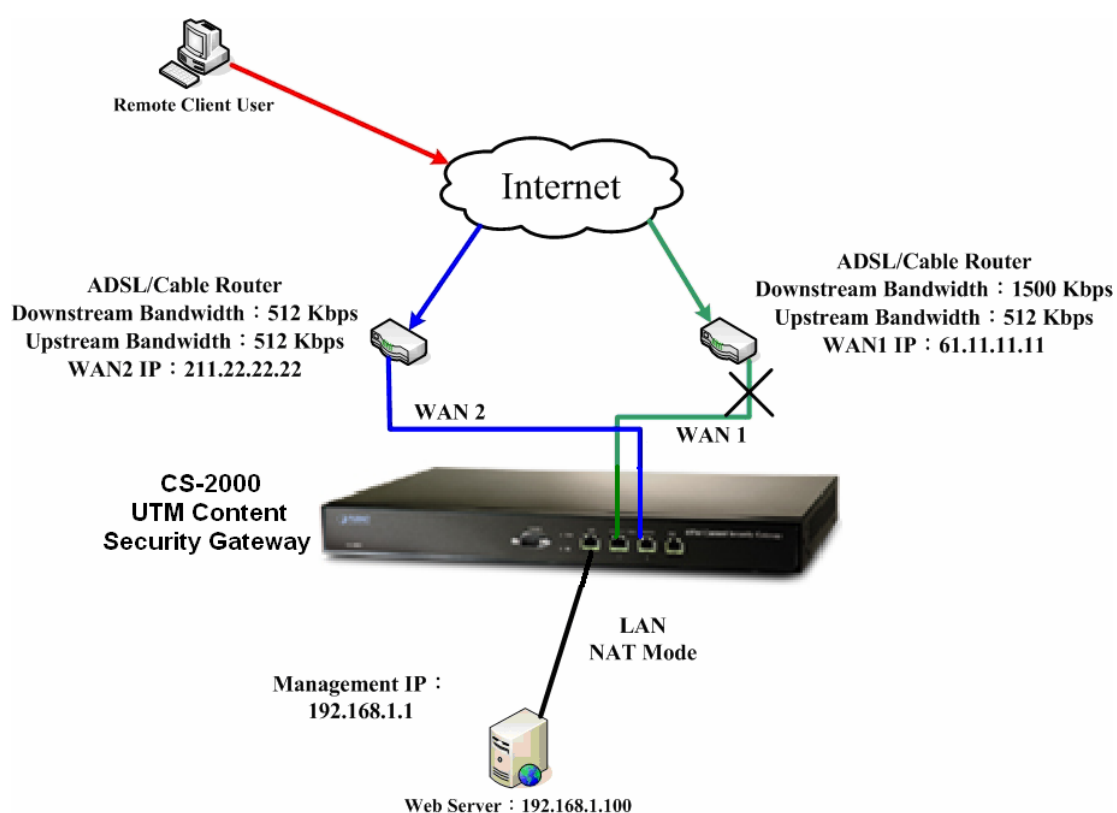
**Step12** In **Policy→ Outgoing**, add the following setting, and click OK.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 <input type="button" value="v"/>
Outside_Any	Virtual Server 2(211.22.22.22)	HTTP(80)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 2 <input type="button" value="v"/>

[New Entry](#)

Add the second policy

**Step13** Complete the settings.



To deploy the web server backup environment

■ **CS-2000 interface :**

WAN1 IP : 61.11.11.11

WAN2 IP : 211.22.22.22

LAN Port IP : 192.168.1.1

The WAN 2 will enable as WAN 1 breaks down.

## Example 2

**Set the web server settings in InBound Load Balance→ A Type → Round-Robin.**

Round-Robin let the web server can provide service to user depends on the priority and weight of inbound load balance. We will make the inbound load balance settings as following :

**Step1** In **Inbound Load Balance**, click **New Entry**.

**Step2** In **Domain Name**, enter test.com (applied from the ISP). **Enable DNS zone**→ **OK**→ **New Entry**.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
-----------	------	---------	--------	--------	----------	-----------

Add new domain name

**Step3** In **InBound Balance Configuration**→**Select type**→**A (Address)**.

**Step4** Add the first record, **Name**, enter **www**.

In **Address**, select WAN 1, click **Assist**, select 61.11.11.11. The IP address will appear in **Address**. In **Balance Mode** → **Round Robin** → **OK**.

**InBound Balance Configuration**

Select type: ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :    ☒ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup

The first inbound balance setting

**Step5** **Weight**, select 1, **Priority**, select 1 and complete the settings.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone


Host Name	Type	Address	Backup	Weight	Priority	Configure
www	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>



The first setting of weight and priority of inbound load balance

**Step6** In **Virtual Server** → **Server 1** → **Click here to configure**.







**Step7** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 1), click **OK**. Click **New Entry** → **Service** → **HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service	HTTP (80) 
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

#### Server 1 setting

**Step8** In **Policy** → **Incoming**, add the following settings , and click **OK**.

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)									To 1 



#### Add the first policy

**Step9** Add the second record, **Name**, enter **www**.

In **Address**, select WAN 2, click **Assist**, select 211.22.22.22. The IP address will appear in **Address**. In **Balance Mode** → **Round-Robin** → **OK**.

InBound Balance Configuration

Select type: ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :    ☐ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup

The second inbound balance setting

**Step10** **Weight**, select 2, **Priority**, select 2 and complete the setting.


Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone



Host Name	Type	Address	Backup	Weight	Priority	Configure
www	A	61.11.11.11(WAN1)	--	<input type="button" value="1"/>	<input type="button" value="1"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
www	A	211.22.22.22(WAN2)	--	<input type="button" value="2"/>	<input type="button" value="2"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The second setting of weight and priority of inbound load balance

**Step11** In **Virtual Server → Server 2→ Click here to configure.**











**Step12** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 2), click **OK**. Click **New Entry→ Service → HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service	HTTP (80) 
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

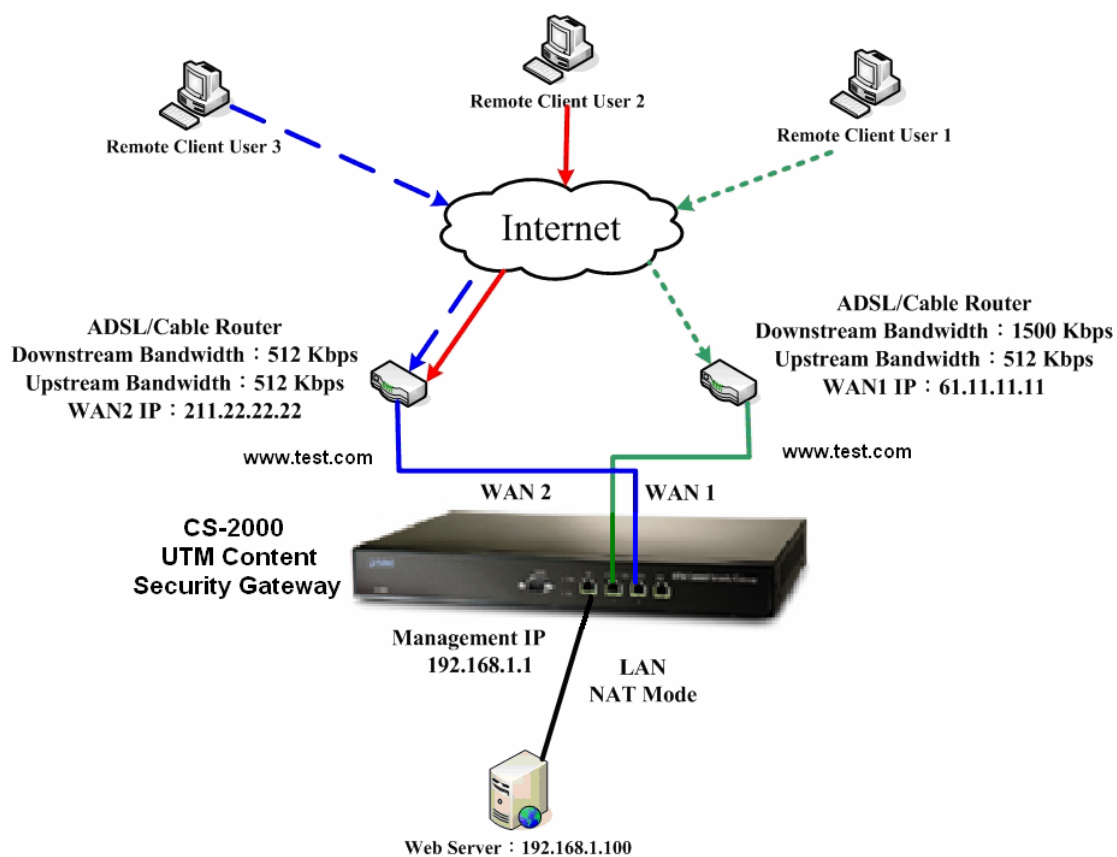
#### Server 2 setting

**Step13** In **Policy→ Incoming**, add the following settings, and click OK.

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)									To 1 
Outside_Any	Virtual Server 2(211.22.22.22)	HTTP(80)									To 2 



#### Add the second policy

**Step14** Complete the settings.

To deploy the web server Round-Robin environment

- **CS-2000 interface :**  
WAN1 IP : 61.11.11.11  
WAN2 IP : 211.22.22.22  
LAN Port IP : 192.168.1.1

Name	Type	Address	Weight	Priority
www.test.com	A	61.11.11.11	1	1
www.test.com	A	211.22.22.22	2	2

**The weight and priority of web server**

When user link to [www.test.com](http://www.test.com) , to look for the web server service. Web server will distribute round-robin depends on the weight and priority.

The way to distribute the round-robin weight and priority :

The 1st user enter 61.11.11.11 server

The 2nd user enter 211.22.22.22 server

The 3rd user enter 211.22.22.22 server

**(Finished to distribute the Round-Robin Priority)**

The 4th user enter 61.11.11.11 server

**(Restart to distribute the Round-Robin Priority)**

The 5th user enter 211.22.22.22 server

The 6<sup>th</sup> user enter 211.22.22.22 server

### Example 3

**Set the web server settings in InBound Load Balance→ CNAME→ Round-Robin .**

To deploy the web server environment. (use the CNAME) :

Round-Robin let the web server can provide service to user depends on the priority and weight of inbound load balance. We will make the inbound load balance settings as following :

**Step1** In **Inbound Load Balance**, click **New Entry**.

**Step2** In **Domain Name**, enter test.com (applied from the ISP). **Enable DNS zone→ OK→ New Entry**.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
-----------	------	---------	--------	--------	----------	-----------

**Add new domain name**

**Step3** In **InBound Balance Configuration→Select type→A (Address)**.

**Step4** Add the first record, **Name**, enter **web**.

In **Address**, select WAN 1, click **Assist**, select 61.11.11.11. The IP address will appear in **Address**. In **Balance Mode** → **Round Robin** → **OK**.

**InBound Balance Configuration**

Select type: ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :    ☐ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup

The first inbound balance setting

**Step5** **Weight**, select 1, **Priority**, select 1 and complete the setting.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
web	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The first setting of weight and priority of inbound load balance

**Step6** In **InBound Balance Configuration** → **Select type** → **A (Address)**.

**Step7** Add the second record, **Name**, enter **web**.

In **Address**, select WAN 2, click **Assist**, select 211.22.22.22. The IP address will appear in **Address**. In **Balance Mode** → **Round-Robin** → **OK**.

**InBound Balance Configuration**

Select type: ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :    ☐ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup

### The second inbound balance setting

**Step8** **Weight**, select 2, **Priority**, select 2 and complete the settings.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
web	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
web	A	211.22.22.22(WAN2)	--	1	2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### The second setting of weight and priority of Inbound Load Balance

**Step9** In **InBound Balance Configuration**→**Select type**→**CNAME** (Canonical Name).



**Step10** Alias Name, enter **www**. Real Name, enter **web.test.com**.

InBound Balance Configuration

Select type ☐ A (Address) ☒ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Alias Name :  ( ex: web )

Real Name :  ( ex: web.broadband.com.tw )

### CNAME (alias) setting

**Step11** Complete the settings.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
web	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
web	A	211.22.22.22(WAN2)	--	1	2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
www	CNAME	web.test.com	--	--	--	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the CNAME (alias) setting

**Step12** In **Virtual Server** → **Server 1** → **Click here to configure**.

**Step13** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 1), click **OK**. Click **New Entry** → **Service** → **HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service	HTTP (80) ▼
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

#### Server 1 setting


**Step14** In **Policy** → **Incoming**, add the following setting, and click **OK**.



Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▼

#### Add the first policy

**Step15** In **Virtual Server → Server 2**→ **Click here to configure**.











**Step16** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 2), click **OK**. Click **New Entry**→ **Service** → **HTTP (80)** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service	HTTP (80) 
External Service Port	80 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

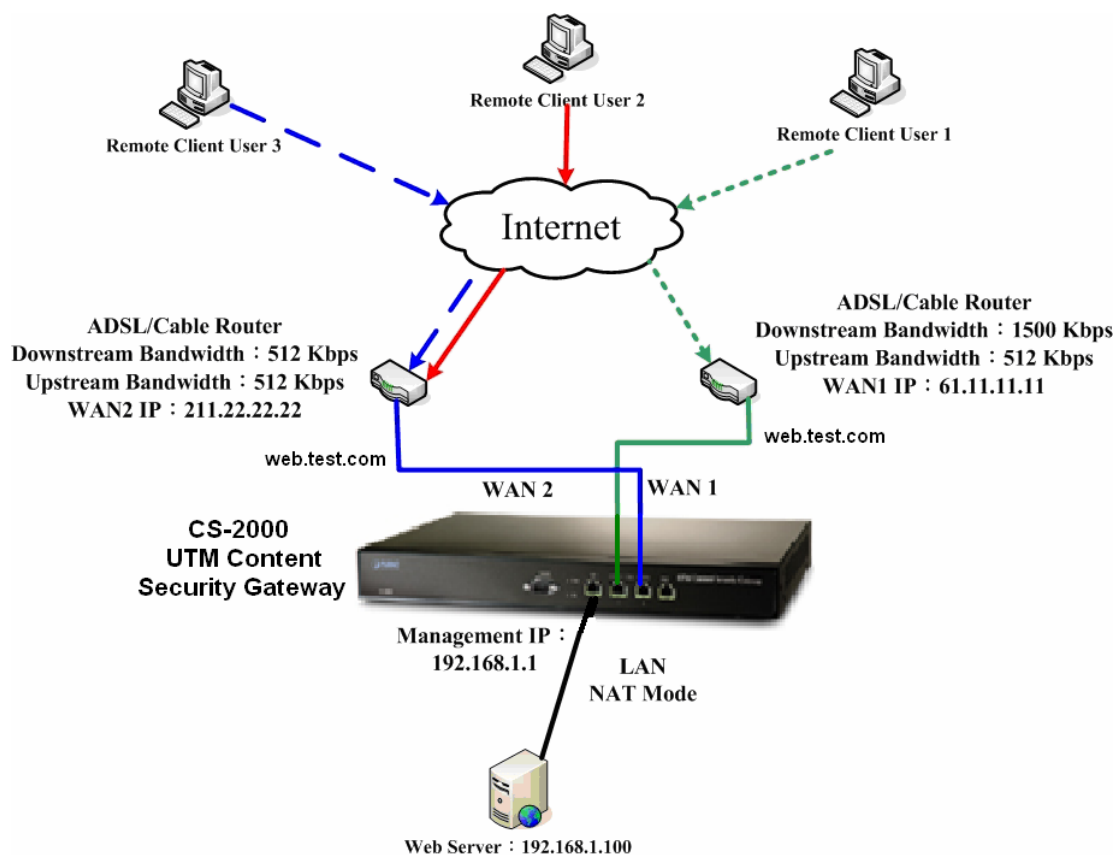
#### Server 2 setting

**Step17** In **Policy**→ **Incoming**, add the following setting, and click **OK**.

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(61.11.11.11)	HTTP(80)									To 1 
Outside_Any	Virtual Server 2(211.22.22.22)	HTTP(80)									To 2 



#### Add the second policy

**Step18 Complete the setting.**

Use CNAME to deploy the web server environment

■ **CS-2000 interface :**

WAN1 IP : 61.11.11.11

WAN2 IP : 211.22.22.22

LAN Port IP : 192.168.1.1

Name	Type	Address	Weight	Priority
web.test.com	A	61.11.11.11	1	1
web.test.com	A	211.22.22.22	2	2
www.test.com	CNAME	web.test.com	--	--

**The weight, priority and CNAME setting of web server**

When user link to the CNAME of [www.test.com](http://www.test.com) , to look for the web server service and will correspond to the real name of web.test.com. Web server will distribute round-robin depends on the weight and priority.

The way to distribute the round-robin weight and priority :

The 1st user enter 61.11.11.11 server

The 2nd user enter 211.22.22.22 server

The 3rd user enter 211.22.22.22 server

**(Finished to distribute the Round-Robin Priority)**

The 4th user enter 61.11.11.11 server

**(Restart to distribute the Round-Robin Priority)**

The 5th user enter 211.22.22.22 server

The 6<sup>th</sup> user enter 211.22.22.22 server

## Example 4

**Set the mail server settings in InBound Load Balance→ Round-Robin.**

To deploy the mail server, we will make the inbound load balance settings as following:

**Step1** In **InBound Balance** → **New Entry**.

**Step2** In **Domain Name**, enter test.com (applied from the ISP). **Enable DNS zone**→ **OK**→ **New Entry**.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
-----------	------	---------	--------	--------	----------	-----------

Add new domain name

**Step3** In **InBound Balance Configuration**→**Select type**→**A (Address)**.

**Step4** Add the first record, **Name**, enter **main**.

In **Address**, select WAN 1, click **Assist**, select 61.11.11.11. The IP address will appear in **Address**. In **Balance Mode** → **Round Robin** → **OK**.

**InBound Balance Configuration**

Select type ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :    ☐ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup

The first inbound balance setting

**Step5** **Weight**, select 1, **Priority**, select 1 and complete the setting.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
Main	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The first setting of weight and priority of inbound load balance

**Step6** In **InBound Balance Configuration**→**Select type**→**A (Address)**.

**Step7** Add the first record, **Name**, enter **main**.

In **Address**, select WAN 2, click **Assist**, select 61.11.11.11. The IP address will appear in **Address**. In **Balance Mode** → **Round Robin** → **OK**.

**InBound Balance Configuration**

Select type ☒ A (Address) ☐ CNAME (Canonical NAME) ☐ MX (Mail eXchanger)

Host Name :  (Max. 255 characters, ex: www)

Address :  WAN2 ▾ Assist ☐ Reverse

Balance Mode : ☒ Round-Robin ☐ Backup WAN1 ▾

OK Cancel

### The second inbound balance setting

**Step8** **Weight**, select 2, **Priority**, select 2 and complete the setting.

Domain Name :  OK (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
Main	A	61.11.11.11(WAN1)	--	1 ▾	1 ▾	<span>Modify</span> <span>Remove</span>
Main	A	211.22.22.22(WAN2)	--	2 ▾	2 ▾	<span>Modify</span> <span>Remove</span>

New Entry

### The second setting of weight and priority of inbound load balance



**Step9** In InBound Balance Configuration→Select type→MX (Mail exchanger).

**Step10** Name, enter mail. Mail Server, enter main.test.com.

InBound Balance Configuration

Select type ☐ A (Address) ☐ CNAME (Canonical NAME) ☒ MX (Mail eXchanger)

Host Name :  ( ex: mail )

Mail Server :  ( ex: mail.broadband.com.tw )

### MX ( mail exchanger ) setting

**Step11** Complete the settings.

Domain Name :   (Max. 255 characters, ex: broadband.com.tw) ☒ Enable DNS zone

Host Name	Type	Address	Backup	Weight	Priority	Configure
Main	A	61.11.11.11(WAN1)	--	1	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Main	A	211.22.22.22(WAN2)	--	2	2	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Mail	MX	main.test.com	--	--	1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the MX ( mail exchanger ) setting

**Step12** In **Virtual Server** → **Server 1** → **Click here to configure**.

**Step13** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 1), click **OK**. Click **New Entry** → **Service** → **POP3 110** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service	POP3 (110) ▼
External Service Port	110 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

OK Cancel

**Server 1 setting**

**Step14** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 1), click **OK**. Click **New Entry**→ **Service** → **SMTP 25** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	61.11.11.11
Service	SMTP (25) ▼
External Service Port	25 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

The second setting in Server1

**Step15** In **Policy**→ **Incoming**, add the following setting, and click **OK**.

Source	Destination	Service	Action	Option				Configure			Move
Outside_Any	Virtual Server 1(61.11.11.11)	POP3(110)						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▼
Outside_Any	Virtual Server 1(61.11.11.11)	SMTP(25)						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 2 ▼

Add the first and second policy

**Step16** In **Virtual Server** → **Server 2**→ **Click here to configure**.

**Step17** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 2), click **OK**. Click **New Entry**→ **Service** → **POP3 110** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service	POP3 (110) ▼
External Service Port	110 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

The first setting in Server 2

**Step18** In **Add New Virtual Server IP**, enter the virtual server real IP (WAN 2), click **OK**. Click **New Entry**→ **Service** → **SMTP 25** and click **OK**.

Virtual Server Configuration	
Virtual Server Real IP	211.22.22.22
Service	SMTP (25) ▼
External Service Port	25 ( Range: 1 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.100
2	
3	
4	

The second setting in Server2

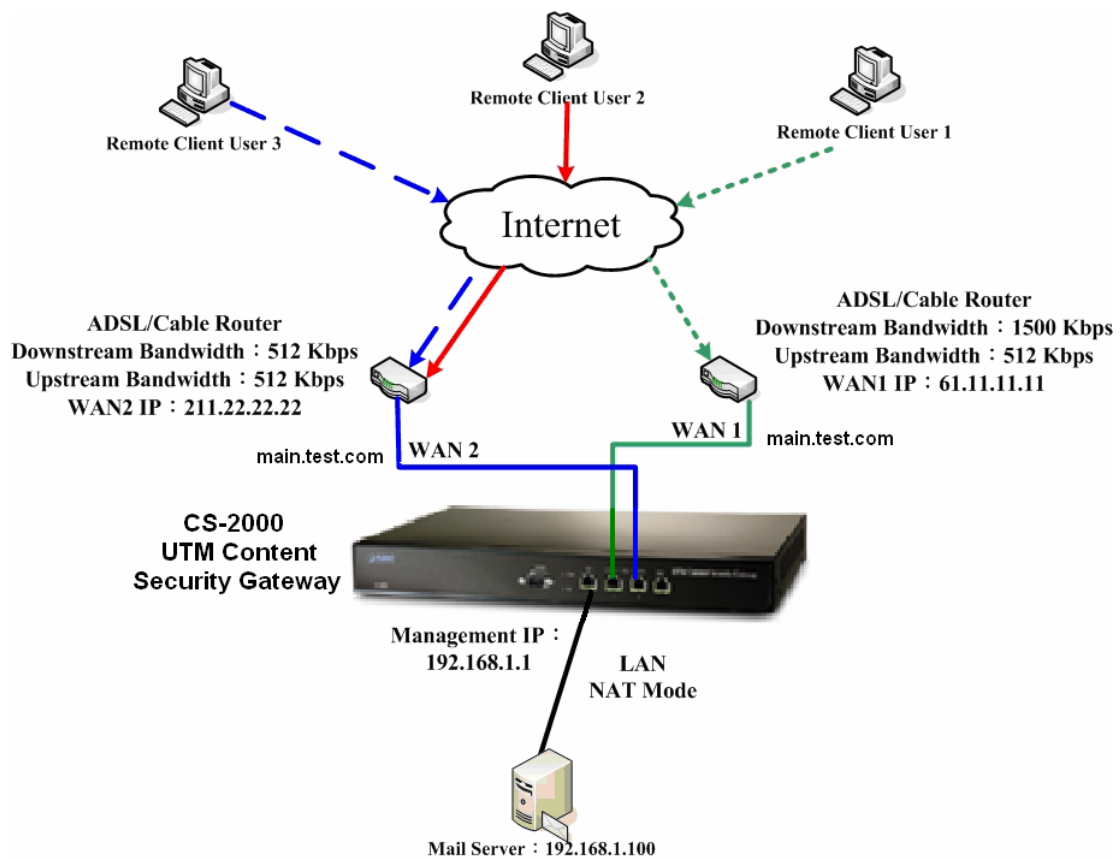
**Step19** In **Policy→Incoming**, add the following settings, and click **OK**.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.11)	POP3(110)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1
Outside_Any	Virtual Server 1(61.11.11.11)	SMTP(25)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 2
Outside_Any	Virtual Server 2(211.22.22.22)	POP3(110)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 3
Outside_Any	Virtual Server 2(211.22.22.22)	SMTP(25)			<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 4

[New Entry](#)

The third and fourth settings in policy

**Step20** Complete the settings.



To deploy the mail server environment

■ **CS-2000 interface :**

WAN1 IP : 61.11.11.11

WAN2 IP : 211.22.22.22

LAN Port IP : 192.168.1.1

Name	Type	Address	Weight	Priority
main.test.com	A	61.11.11.11	1	1
main.test.com	A	211.22.22.22	2	2
mail.test.com.	MX	main.test.com	--	--

**The weight, priority and MX setting of web server**

When user link to the CNAME of [mail.test.com](mailto:mail.test.com) , to look for the web server service and will correspond to the real name of main.test.com. Web server will distribute round-robin depends on the weight and priority :

The way to distribute the round-robin weight and priority :

The 1st user enter 61.11.11.11 server

The 2nd user enter 211.22.22.22 server

The 3rd user enter 211.22.22.22 server

**(Finished to distribute the Round-Robin Priority)**

The 4th user enter 61.11.11.11 server

**(Restart to distribute the Round-Robin Priority)**

The 5th user enter 211.22.22.22 server

The 6<sup>th</sup> user enter 211.22.22.22 server

## 11.2 High Availability

# **High Availability**

CS-2000 offers the high availability function. If there is one of the CS-2000 device malfunction, then the backup device can replace the master device to ensure the network stability.

**In this chapter, we will make the specific introduction of high availability.**

## **High Availability**

### **IP Address (for Management)**

After enabled high availability function, MIS engineer can respectively use two IP addresses to log in the CS-2000 master and backup devices via Web UI. ( The two IP addresses must be different and at the same segment as in LAN port interface. )

### **High Availability Mode**

This mode is to distinguish the settings in CS-2000 master and backup devices.

### **Synchronize configuration settings of system**

- In high availability mode, MIS engineer can set the CS-2000 master device to backup settings to backup device in daily specific time.

### **Synchronize configuration settings of MASTER and BACKUP immediately**

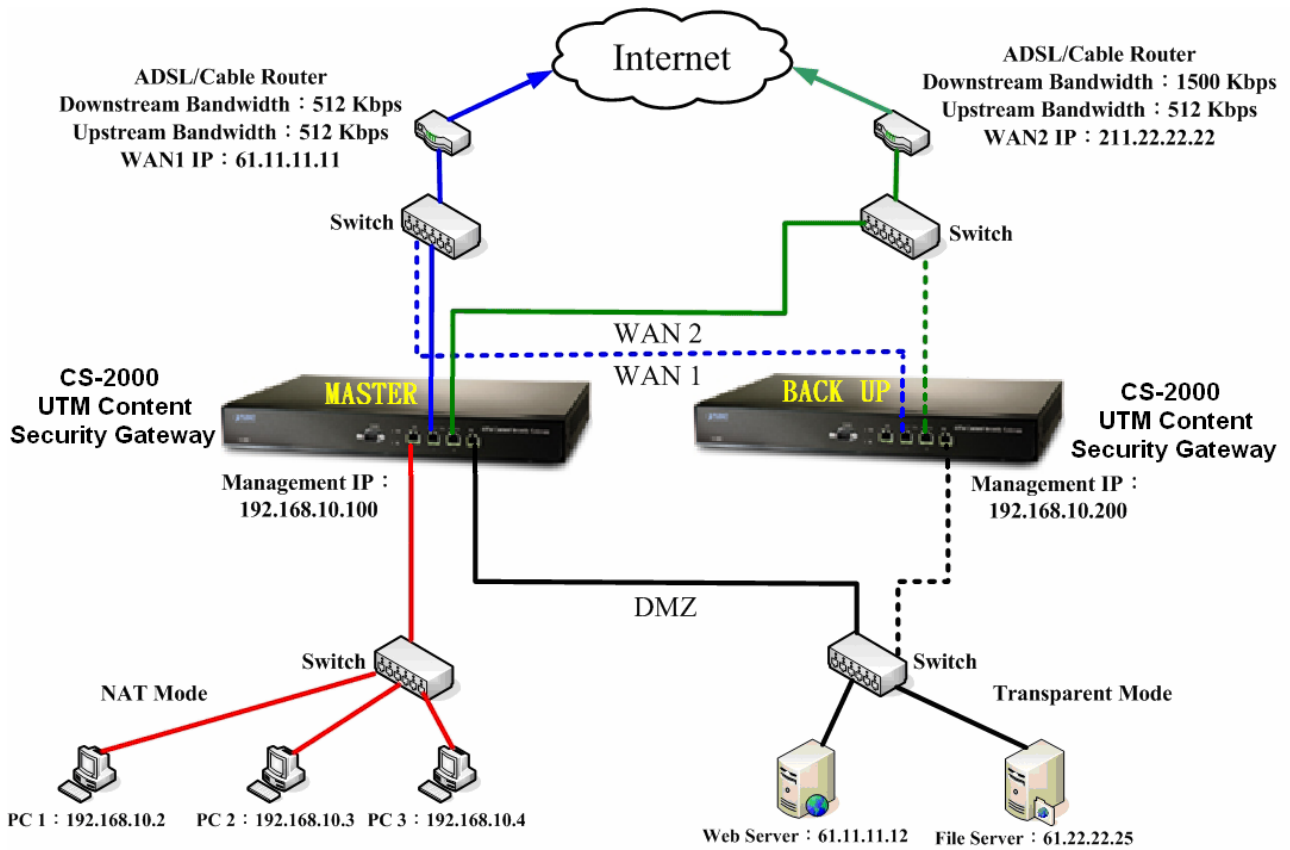
- In high availability mode, CS-2000 master device can instantly backup the settings to backup device.



## Example 1

To deploy a high availability environment :

**Step1** Set a CS-2000 master device connect to the Switch which connected to LAN.



To deploy the master device environment in high availability mode

**Step2** Set the high availability settings in master device :

- **Interface → LAN → IP address**, enter 192.168.10.1.
- **High Availability → Enable High Availability.**
- **IP Address (for Management) →** enters 192.168.10.100.
- **High Availability Mode → MASTER.**
- In **Synchronize configuration settings of system**, select the hour of a day, to let the master device can synchronize configure settings. (The function only enabled by select **master** device, and the **backup** device will reboot.)
- Complete the master device setting.

LAN Interface

IP Address	192.168.10.1
Netmask	255.255.255.0
MAC Address	00:30:4f:0a:eb:30

Enable System Management
☒ Ping / Traceroute
☒ HTTP
☒ HTTPS

OK
Cancel

#### LAN interface IP address

High Availability Setting

☒ Enable High Availability

IP Address (for Management)	192.168.10.100
High Availability Mode	MASTER ▼
Synchronize system configurations daily at :	23 : 00 ▼ / Day

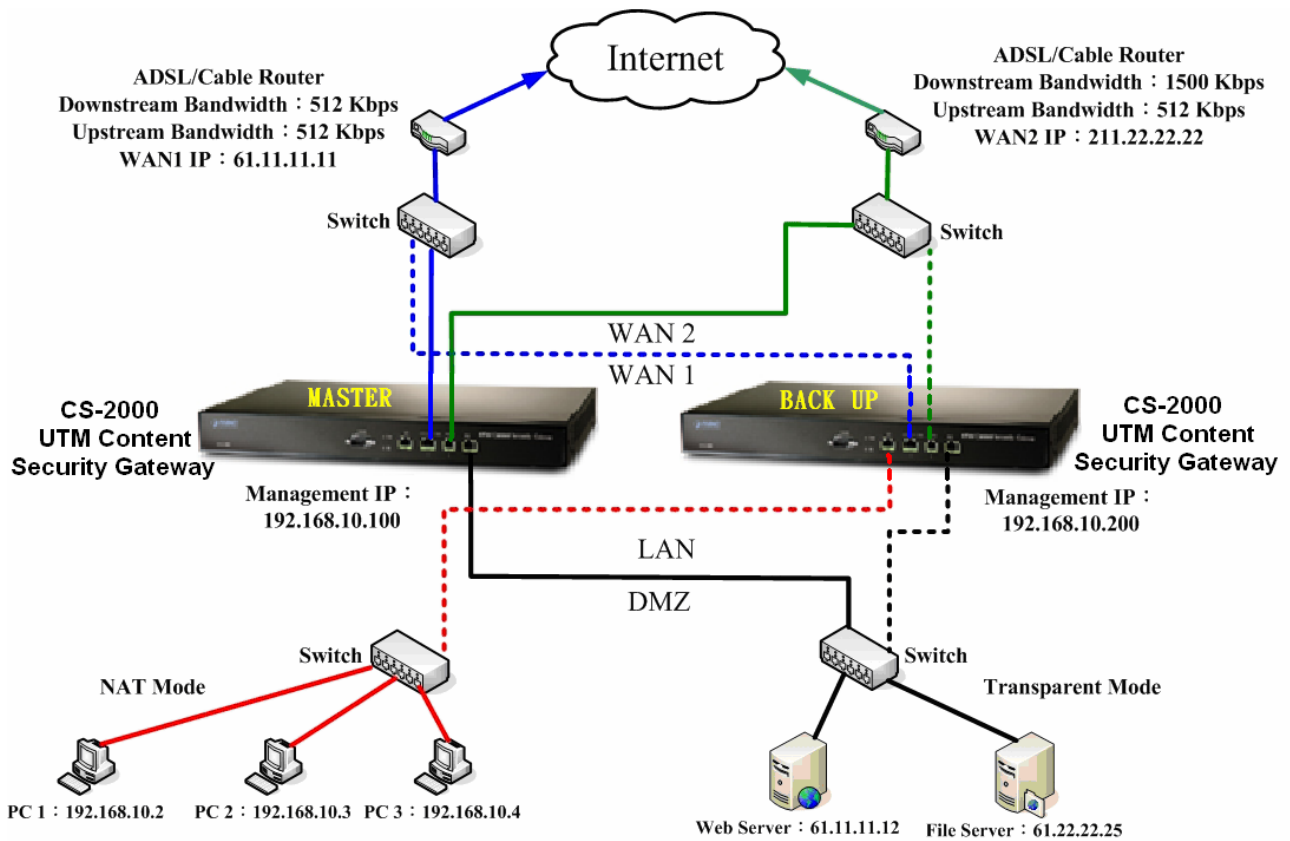
---

Synchronize configuration settings of MASTER and BACKUP immediately
 Sync NOW

OK
Cancel

#### The master device setting Web UI in high availability mode

**Step3** To take the master device LAN port away from the LAN Switch port and connect the backup device to LAN Switch port.



**To deploy the backup device environment in high availability mode**

**Step4** Set the backup device settings in high availability mode.

- **Interface** → **LAN**, to make sure the LAN IP is the same as master LAN IP. (192.168.10.1 )
- **High Availability** → **Enable High Availability**.
- In **Permitted IPs**, enter the IP 192.168.10.200, which is differing from master device but in the same segment as LAN.
- **High Availability** → **High Availability Mode**, select **BACKUP**.
- Complete the backup device setting.
- To connect the LAN Switch to master device.
- Complete the high availability deployment. The master and backup device's LAN, WAN and DMZ port need to be connected to the same switch.

LAN Interface

IP Address 192.168.10.1

Netmask 255.255.255.0

MAC Address 00:30:4f:0a:eb:30

Enable System Management ☒ Ping / Traceroute ☒ HTTP ☒ HTTPS

OK Cancel

LAN interface setting

High Availability Setting

☒ Enable High Availability

IP Address (for Management) 192.168.10.200

High Availability Mode BACKUP

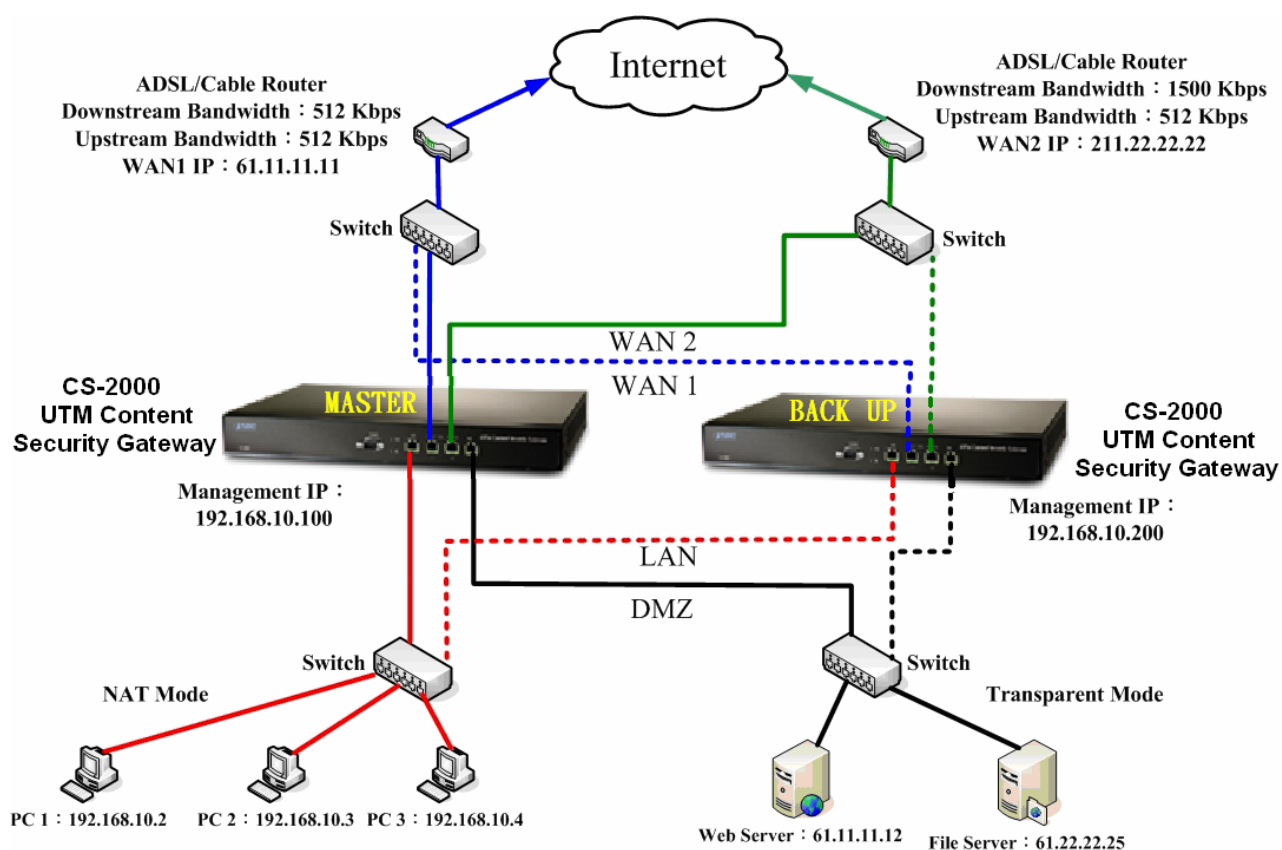
Synchronize system configurations daily at : 23 : 00 / Day

-----

Synchronize configuration settings of MASTER and BACKUP immediately Sync NOW

OK Cancel

The backup device setting Web UI in high availability mode



**The high availability deployment**

■ **CS-2000 interface :**

WAN1 IP : 61.11.11.11

WAN2 IP : 211.22.22.22

LAN Port IP : 192.168.10.1

DMZ Port : Transparent Mode

MASTER Management IP : 192.168.10.100

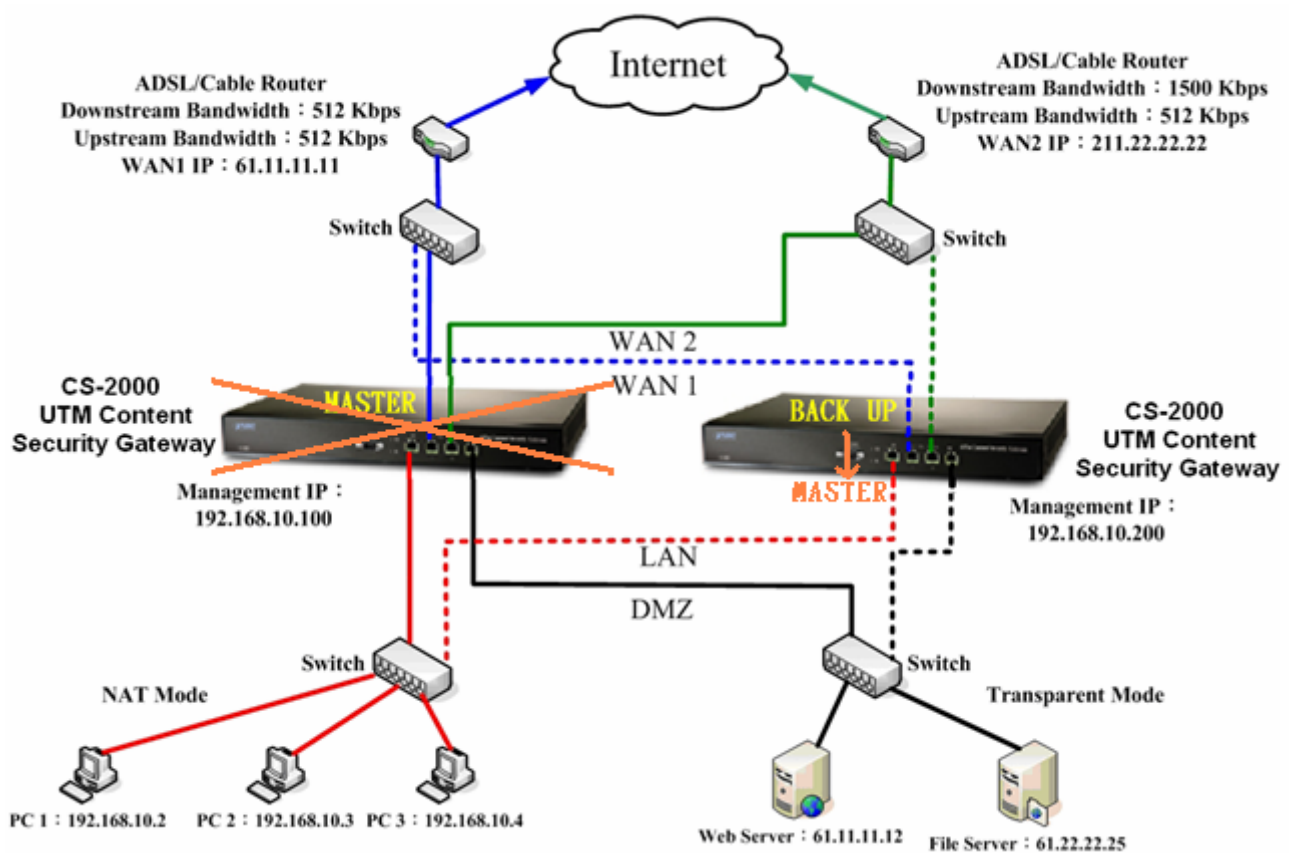
BACKUP Management IP : 192.168.10.200

**Step5** Synchronize configuration settings of master and backup immediately.

- Enter the LAN IP in address (the address column in browser), and log in to the high availability mode Web UI in CS-2000 master device.
- Continue the unfinished settings.
- In **High Availability**, click **Sync Now**.
- The backup device will reboot after complete all the synchronized configuration settings.
- After the backup device reboot , enter the backup device managed IP address to check if the settings are the same as master device. ( After finish the master device settings, MIS engineer can use the **Sync Now** function in backup device , to easily synchronize configuration settings of the two devices. )

## Comments

1. After finished the deployment, the backup device offers the backup function when the master device is malfunction.
2. When the **synchronize configuration settings of time** arrived, the master device will confirm if the backup device has the same settings, if not, the master device will synchronize configuration settings to backup device. The backup device will reboot.
3. When master device is malfunction, the backup device will replace the master device.



When the master device is malfunction, the backup device will replace master device.



Use restriction:

1. **High Availability mode** :

- a. Set the WAN Port to be Static IP or non-Static IP, the device can process the system configuration and session backup.
  - b. When set the WAN port to be the non-Static IP and enable the HA backup, the session backup will stop after regain the WAN port IP.
  - c. The LAN port IP, MASTER management IP and BACKUP management IP need to be the unused and different IP at the same segment.
2. **VPN → IPsec** : MIS engineer need to set the Keep Alive IP in VPN Trunk, to instantly create the VPN when access the backup function.
3. **VPN → PPTP** : The PPTP is disabled in HA backup environment.



## Chapter 12: Monitor

# Monitor

### 12.1 Log

**Log**, includes the information of traffic, event and connection.

MIS engineer can set the **Traffic** parameters in **Policy**, or select **View Log & Report Privilege** in **System**.

- **Log**, record the data packets contents by **Policy** setting. **Traffic** function can also record the CS-2000 destination and source data packets by **System** setting.
- **Event**, record the CS-2000 system configuration of the modified contents, users, time, parameters and the log in IP address.
- **Connection**, record all the CS-2000 connecting information. MIS engineer can easily to know the status depends on the connecting information when the problems happened.



#### How to use Monitor?

1. **Traffic**, MIS engineer can view the connection status includes time, source IP, destination IP and disposition. CS-2000 can backup the traffic log and refresh the online record on specific time period.
2. **Event**, if CS-2000 detected some events happened, MIS engineer can know the events description and backup it.
3. **Connection**, can record the connection status by this function.
4. **Log Backup**, MIS engineer can set the CS-2000 to automatically send the email alarm of traffic and events or instantly send the log to assigned syslog server.

## Setting

### Log Backup Setting

- In **System → Configure → Setting**, enable **E-mail Alert Notification**. When log full of 300 Kbytes, CS-2000 will send the log to assigned recipient.
- To send the log to assigned syslog server.
- The settings of traffic , event and connection :
  - ◆ MIS engineer can assign the storage lifetime and CS-2000 can refresh and delete all the record correspond to the setting, when storage lifetime arrived.
  - ◆ MIS engineer can respectively enable E-mail log and Syslog message.

## Traffic

### Search

- MIS engineer can search the record depends on the keywords of Policy, NO, Source IP, Destination IP, Port, From, To.
  - Add the following setting :
    1. **Policy**, select All Policy.
    2. **NO**, select ALL.
    3. To enable the **From** and **To** function, to assign the time period.
    4. Click **Search**.
    5. Click **Download**, to backup the searched records.

## Search

Enter keyword or phrase

Policy :

NO :

Source IP :

Destination IP :

Port :  =>  (Range : 1 - 65535)



From :  /  /  :  :



To :  /  /  :  :

[Search](#)

## Results

Search result: 3941 records

1 / 198 [Next](#)

View:

[Download](#)

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 5 11:41:50	192.168.1.2	210.64.125.10	TCP	1746 => 80 (WAN2)	37 KB	
Jul 5 11:41:35	192.168.1.2	62.30.79.153	UDP	42777 => 37564 (WAN1)	198 B	
Jul 5 11:41:27	192.168.1.2	84.250.2.65	UDP	42777 => 1441 (WAN1)	106 B	
Jul 5 11:41:27	192.168.1.2	86.101.126.28	UDP	42777 => 6220 (WAN1)	199 B	
Jul 5 11:41:17	192.168.1.2	201.208.136.72	UDP	42777 => 11871 (WAN1)	219 B	
Jul 5 11:41:09	192.168.1.2	69.138.146.215	UDP	42777 => 29382 (WAN1)	208 B	
Jul 5 11:41:02	192.168.1.2	86.101.126.28	UDP	42777 => 6220 (WAN1)	199 B	
Jul 5 11:39:35	192.168.1.2	86.101.126.28	UDP	42777 => 6220 (WAN1)	199 B	
Jul 5 11:39:35	192.168.1.2	80.42.66.234	UDP	42777 => 37480 (WAN1)	198 B	
Jul 5 11:39:17	192.168.1.2	85.226.146.71	UDP	42777 => 7244 (WAN1)	195 B	
Jul 5 11:39:16	192.168.1.2	69.125.55.183	UDP	42777 => 59339 (WAN1)	190 B	
Jul 5 11:38:50	192.168.1.2	62.162.183.19	UDP	42777 => 46781 (WAN1)	202 B	
Jul 5 11:38:45	192.168.1.2	86.101.126.28	UDP	42777 => 6220 (WAN1)	200 B	
Jul 5 11:38:37	192.168.1.2	133.87.66.153	UDP	42777 => 26042 (WAN1)	545 B	
Jul 5 11:38:27	192.168.1.2	84.250.2.65	UDP	42777 => 1441 (WAN1)	106 B	
Jul 5 11:38:26	192.168.1.2	124.211.60.185	TCP	1581 => 80 (WAN2)	5 KB	
Jul 5 11:38:25	192.168.1.2	220.130.117.62	TCP	1580 => 80 (WAN2)	1 KB	
Jul 5 11:38:16	192.168.1.2	201.208.136.72	UDP	42777 => 11871 (WAN1)	219 B	
Jul 5 11:38:16	192.168.1.2	80.42.66.234	UDP	42777 => 37480 (WAN1)	198 B	
Jul 5 11:38:05	192.168.1.2	139.175.250.167	TCP	1749 => 80 (WAN2)	18 KB	

1 / 198 [Next](#)

**Search the specific record**

## Event

### Search

- MIS engineer can search the record depends on the keywords of time and event.
  - Add the following settings :
    1. To enable the **From** and **To** function, to assign the time period.
    2. Click **Search**.
    3. Click **Download**, to backup the searched records.

1 / 44 [Next](#)



Time	Admin Name	IP Address	Event	Detail
Jul 5 11:33:19	admin	192.168.1.2	[Policy] Add [Incoming] (Outside_Any=>Inside_Any (Routing),ANY,permit)	
Jul 5 11:33:14	---	LOCALHOST	WAN1 is connected	-
Jul 5 11:29:11	---	LOCALHOST	WAN1 is disconnected	-
Jul 5 11:20:15	admin	192.168.1.2	[Login success]	-
Jul 5 11:18:24	admin	192.168.1.2	[Login success]	-
Jul 5 11:17:03	admin	211.75.117.114	[Login success]	-
Jul 5 10:00:11	---	LOCALHOST	Notice Send Notice Mails Completely.(myalexweb.dyndns.tv)	-
Jul 5 10:00:11	---	LOCALHOST	Notice Begin Sending Notice Mails.(myalexweb.dyndns.tv)	-
Jul 5 09:56:52	admin	211.75.117.114	[Policy] Add [Outgoing] (Inside_Any=>Outside_Any,ANY,permit)	
Jul 5 09:55:26	admin	211.75.117.114	[Policy] Delete [Outgoing] (Inside_Any=>Outside_Any,ANY,deny)	
Jul 5 09:41:57	admin	211.75.117.114	[Policy] Delete [Outgoing] (Inside_Any=>Outside_Any,ANY,permit)	
Jul 5 09:33:32	admin	211.75.117.114	[Login success]	-
Jul 5 09:33:27	admin	211.75.117.114	[Policy] Pause [Incoming] (Inside_Any=>Outside_Any,ANY,deny)	
Jul 5 09:33:10	admin	211.75.117.114	[Policy] Modify [Outgoing] (Inside_Any=>Outside_Any,ANY,deny)	
Jul 5 09:32:49	admin	211.75.117.114	[Policy] Modify [Outgoing] (Inside_Any=>Outside_Any,ANY,permit2)	
Jul 5 09:32:24	admin	211.75.117.114	[Policy] Modify [Outgoing] (Inside_Any=>Outside_Any,ANY,permit1)	
Jul 5 09:31:42	admin	211.75.117.114	[Policy] Add [Outgoing] (Inside_Any=>Outside_Any,ANY,permit)	
Jul 5 09:31:33	admin	211.75.117.114	[Policy] Restart [Incoming] (Inside_Any=>Outside_Any,ANY,permit)	
Jul 5 09:31:03	admin	211.75.117.114	[Policy] Pause [Incoming] (Inside_Any=>Outside_Any,ANY,permit)	
Jul 5 09:27:12	admin	211.75.117.114	[Policy] Modify [Outgoing] (Inside_Any=>Outside_Any,ANY,permit)	

1 / 44 [Next](#)

### Search the specific record

## Connection

### Search

- MIS engineer can search the record depends on the keywords of time and event.
- Add the following settings :
  1. To enable the **From** and **To** function, to assign the time period.
  2. Click **Search**.
  3. Click **Download**, to backup the searched records.

1 / 4141 [Next](#)

Time	Event
Jul 5 11:32:56	dhcpd[6607]: DHCP_ACK received from to (203.67.31.1)
Jul 5 11:32:56	dhcpd[6607]: sending DHCP_REQUEST for 203.67.31.11 to 203.67.31.1
Jul 5 11:32:56	dhcpd[6607]: Lease time : 4294967295 secs
Jul 5 11:32:56	dhcpd[6607]: Domain name server 2 : 168.95.1.1
Jul 5 11:32:56	dhcpd[6607]: Domain name server 1 : 168.95.1.1
Jul 5 11:32:56	dhcpd[6607]: Default gateway : 203.67.31.1
Jul 5 11:32:56	dhcpd[6607]: Netmask : 255.255.255.0
Jul 5 11:32:56	dhcpd[6607]: IP Address : 203.67.31.11
Jul 5 11:32:56	dhcpd[6607]: verified 203.67.31.11 address is not in use
Jul 5 11:32:56	dhcpd[6607]: broadcasting ARP_REQUEST for 203.67.31.11
Jul 5 11:32:56	dhcpd[6607]: DHCP_ACK received from to (203.67.31.1)
Jul 5 11:32:56	dhcpd[6607]: broadcasting DHCP_REQUEST for 203.67.31.11
Jul 5 11:32:56	dhcpd[6607]: DHCP_OFFER received from to (203.67.31.1)
Jul 5 11:32:56	dhcpd[6607]: broadcasting second DHCP_DISCOVER
Jul 5 11:32:56	dhcpd[6607]: broadcastAddr option is missing in DHCP server response. Assuming 203.67.31.255
Jul 5 11:32:27	dhcpd[6062]: terminating on signal 15
Jul 5 11:31:23	dhcpd[5477]: terminating on signal 15
Jul 5 11:30:18	dhcpd[4906]: terminating on signal 15
Jul 5 11:29:13	dhcpd[1215]: terminating on signal 15
Jul 5 11:29:12	dhcpd[1215]: sending DHCP_RELEASE for 203.67.31.11 to 203.67.31.1

[Clear Data](#)
1 / 4141 [Next](#)

Search the specific record

### 12.1.1 Log Examples

We set 4 monitoring environments.

No.	Range	The Application Environment	Pages
Example. 1	Traffic	View the user's used Protocol and Port, to access the internal and external resources via CS-2000.	518
Example. 2	Event	View the status of MIS engineer log into CS-2000 to process the management and external interface.	522
Example. 3	Connection	View the external interface record of bandwidth management.	523
Example. 4	Log Backup	MIS engineer can receive or save the record results from the CS-2000.	525

## Example 1. Traffic

View the user's used Protocol and Port, to access the internal and external resources via CS-2000.

**Step1**     **Policy → DMZ To WAN** , add the following settings :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
VPN Trunk	None
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P Blocking	None
Anti-Virus	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

### Traffic setting in policy

**Step2**     **Policy → DMZ To WAN** , complete the traffic setting in policy :

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY							<a href="#">Modify</a>	<a href="#">Remove</a>	<a href="#">Pause</a>	To 1

[New Entry](#)

Complete the DMZ To WAN traffic setting in policy



**Step3**    **Monitor → Traffic**, it shows the packets traffic through policy.

1 / 2   [Next](#)



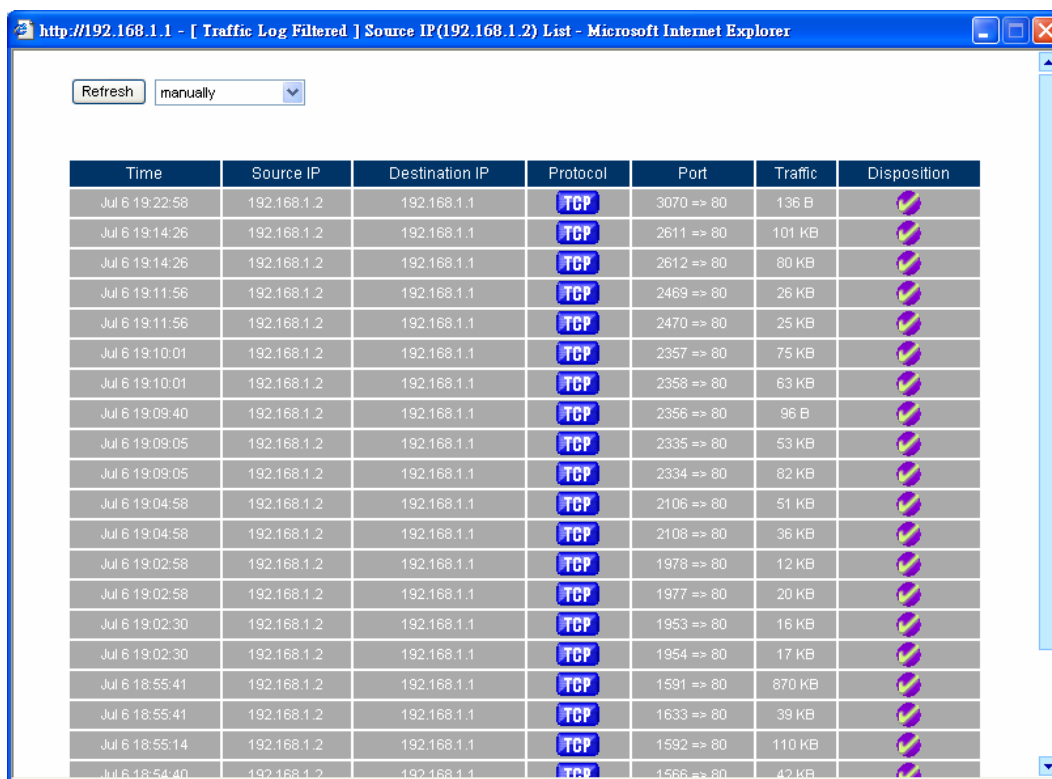
Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 6 19:14:10	192.168.1.2	192.168.1.1	TCP	2611 => 80	65 KB	
Jul 6 19:14:10	192.168.1.2	192.168.1.1	TCP	2612 => 80	73 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2469 => 80	26 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2470 => 80	25 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2357 => 80	75 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2358 => 80	63 KB	
Jul 6 19:09:40	192.168.1.2	192.168.1.1	TCP	2356 => 80	96 B	
Jul 6 19:09:05	192.168.1.2	192.168.1.1	TCP	2334 => 80	82 KB	
Jul 6 19:09:05	192.168.1.2	192.168.1.1	TCP	2335 => 80	53 KB	
Jul 6 19:04:58	192.168.1.2	192.168.1.1	TCP	2106 => 80	51 KB	
Jul 6 19:04:58	192.168.1.2	192.168.1.1	TCP	2108 => 80	36 KB	
Jul 6 19:02:58	192.168.1.2	192.168.1.1	TCP	1978 => 80	12 KB	
Jul 6 19:02:58	192.168.1.2	192.168.1.1	TCP	1977 => 80	20 KB	
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1954 => 80	17 KB	
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1953 => 80	16 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1591 => 80	870 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1633 => 80	39 KB	
Jul 6 18:55:14	192.168.1.2	192.168.1.1	TCP	1592 => 80	110 KB	
Jul 6 18:54:40	192.168.1.2	192.168.1.1	TCP	1566 => 80	42 KB	
Jul 6 18:54:40	192.168.1.2	192.168.1.1	TCP	1567 => 80	41 KB	

Clear Data

1 / 2   [Next](#)

The traffic log Web UI

**Step4** Click **Source IP** or **Destination IP**, it shows the Protocol, Port and Traffic information.



Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 6 19:22:58	192.168.1.2	192.168.1.1	TCP	3070 => 80	136 B	
Jul 6 19:14:26	192.168.1.2	192.168.1.1	TCP	2611 => 80	101 KB	
Jul 6 19:14:26	192.168.1.2	192.168.1.1	TCP	2612 => 80	80 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2469 => 80	26 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2470 => 80	25 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2357 => 80	75 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2358 => 80	63 KB	
Jul 6 19:09:40	192.168.1.2	192.168.1.1	TCP	2356 => 80	96 B	
Jul 6 19:09:05	192.168.1.2	192.168.1.1	TCP	2335 => 80	53 KB	
Jul 6 19:09:05	192.168.1.2	192.168.1.1	TCP	2334 => 80	82 KB	
Jul 6 19:04:58	192.168.1.2	192.168.1.1	TCP	2106 => 80	51 KB	
Jul 6 19:04:58	192.168.1.2	192.168.1.1	TCP	2108 => 80	36 KB	
Jul 6 19:02:58	192.168.1.2	192.168.1.1	TCP	1978 => 80	12 KB	
Jul 6 19:02:58	192.168.1.2	192.168.1.1	TCP	1977 => 80	20 KB	
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1953 => 80	16 KB	
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1954 => 80	17 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1591 => 80	870 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1633 => 80	39 KB	
Jul 6 18:55:14	192.168.1.2	192.168.1.1	TCP	1592 => 80	110 KB	
Jul 6 18:54:40	192.168.1.2	192.168.1.1	TCP	1566 => 80	42 KB	

The IP address traffic log Web UI

**Step5** Click **Clear**, it shows the confirm window, and then click **OK**. All the records will be deleted in CS-2000.

1 / 2 [Next](#)



Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jul 6 19:14:10	192.168.1.2	192.168.1.1	TCP	2611 => 80	65 KB	
Jul 6 19:14:10	192.168.1.2	192.168.1.1	TCP	2612 => 80	73 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2469 => 80	26 KB	
Jul 6 19:11:56	192.168.1.2	192.168.1.1	TCP	2470 => 80	25 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2357 => 80	75 KB	
Jul 6 19:10:01	192.168.1.2	192.168.1.1	TCP	2358 => 80	63 KB	
Jul 6 19:09:40	192.168.1.2	192.168.1.1	TCP	2356 => 80	96 B	
Jul 6 19:09:05	192.168.1.2	192.168.1.1	TCP	2334 => 80	82 KB	
Jul 6 19:09:05	192.168.1.2	<div><div>Microsoft Internet Explorer</div><div> Are you sure you want to clear all data?</div><div><input type="button" value="OK"/> <input type="button" value="Cancel"/></div></div>	2335 => 80	53 KB		
Jul 6 19:04:58	192.168.1.2		2106 => 80	51 KB		
Jul 6 19:04:58	192.168.1.2		2108 => 80	36 KB		
Jul 6 19:02:58	192.168.1.2		1978 => 80	12 KB		
Jul 6 19:02:58	192.168.1.2		1977 => 80	20 KB		
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1954 => 80	17 KB	
Jul 6 19:02:30	192.168.1.2	192.168.1.1	TCP	1953 => 80	16 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1591 => 80	870 KB	
Jul 6 18:55:41	192.168.1.2	192.168.1.1	TCP	1633 => 80	39 KB	
Jul 6 18:55:14	192.168.1.2	192.168.1.1	TCP	1592 => 80	110 KB	
Jul 6 18:54:40	192.168.1.2	192.168.1.1	TCP	1566 => 80	42 KB	
Jul 6 18:54:40	192.168.1.2	192.168.1.1	TCP	1567 => 80	41 KB	

Clear Data

1 / 2 [Next](#)

Delete all the traffic log

## Example 2. Event

View the status of the WAN interface and the MIS engineer action as his log into the CS-2000 appliance.

**Step1**     **Monitor → Event**, it shows the status of MIS engineer log into CS-2000 to process the management and external interface.

1 / 43 [Next](#)



Time	Admin Name	IP Address	Event	Detail
Jul 6 15:47:18	admin	192.168.1.2	[Policy] Add [Incoming] (Outside_Any=>211.22.22.22,SMTP(25),permit)	
Jul 6 15:47:13	admin	192.168.1.2	[Policy] Add [Incoming] (Outside_Any=>211.22.22.22,POP3(110),permit)	
Jul 6 15:47:04	admin	192.168.1.2	[Policy Object] Add [SMTP] (Virtual Server 2)	
Jul 6 15:45:57	admin	192.168.1.2	[Policy Object] Modify [HTTP] (Virtual Server 2)	
Jul 6 15:44:49	admin	192.168.1.2	[Policy] Add [Incoming] (Outside_Any=>61.11.11.11,SMTP(25),permit)	
Jul 6 15:44:40	admin	192.168.1.2	[Policy] Add [Incoming] (Outside_Any=>61.11.11.11,POP3(110),permit)	
Jul 6 15:44:14	admin	192.168.1.2	[Policy Object] Add [SMTP] (Virtual Server 1)	
Jul 6 15:43:39	admin	192.168.1.2	[Policy Object] Modify [HTTP] (Virtual Server 1)	
Jul 6 15:42:42	admin	192.168.1.2	[Policy] Delete [Incoming] (Outside_Any=>211.22.22.22,HTTP(80),permit)	
Jul 6 15:42:40	admin	192.168.1.2	[Policy] Delete [Incoming] (Outside_Any=>61.11.11.11,HTTP(80),permit)	
Jul 6 15:41:52	admin	192.168.1.2	[Advance] Add [DNS Server] (Zone Name : Mail, Address : main.test.com)	
Jul 6 15:40:06	admin	192.168.1.2	[Advance] Modify [DNS Server] (Weight) Name:Main, Address:211.22.22.22	
Jul 6 15:40:01	admin	192.168.1.2	[Advance] Add [DNS Server] (Zone Name : Main, Address : 211.22.22.22)	
Jul 6 15:38:52	admin	192.168.1.2	[Advance] Modify [DNS Server] (Zone Name : web, Address : 61.11.11.11)	
Jul 6 15:38:19	admin	192.168.1.2	[Advance] Remove [DNS Server] (Zone Name : web, Address : 211.22.22.22)	
Jul 6 15:38:16	admin	192.168.1.2	[Advance] Remove [DNS Server] (Zone Name : www, Address : web.test.com)	
Jul 6 15:30:30	admin	192.168.1.2	[Advance] Add [DNS Server] (Zone Name : www, Address : web.test.com)	
Jul 6 15:28:59	admin	192.168.1.2	[Advance] Add [DNS Server] (Zone Name : web, Address : 211.22.22.22)	
Jul 6 15:27:44	admin	192.168.1.2	[Advance] Modify [DNS Server] (Zone Name : www, Address : 61.11.11.11)	
Jul 6 15:26:41	admin	192.168.1.2	[Advance] Remove [DNS Server] (Zone Name : www, Address : 211.22.22.22)	

1 / 43 [Next](#)

### Event log Web UI

## Example 3. Connection

View the external interface connection record as process the bandwidth management.

**Step1**     **Monitor→ Connection** , it shows the external interface connection status in CS-2000

1 / 4155   [Next](#)



Time	Event
Jul 6 14:46:49	[Web VPN] TCP/UDP: Closing socket
Jul 6 14:46:49	[Web VPN] Client/210.66.155.80:1131 SIGUSR1[soft,ping-restart] received, client-instance restarting
Jul 6 14:46:49	[Web VPN] Client/210.66.155.80:1131 [Client] Inactivity timeout (--ping-restart), restarting
Jul 6 14:31:37	[Web VPN] Client/210.66.155.80:1131 MULTI: primary virtual IP for Client/210.66.155.80:1131: 192.168.222.10
Jul 6 14:31:37	[Web VPN] Client/210.66.155.80:1131 MULTI: Learn: 192.168.222.10 -> Client/210.66.155.80:1131
Jul 6 14:31:37	[Web VPN] 210.66.155.80:1131 [Client] Peer Connection Initiated with 210.66.155.80:1131
Jul 6 14:31:37	[Web VPN] 210.66.155.80:1131 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Jul 6 14:31:36	[Web VPN] 210.66.155.80:1131 VERIFY OK: depth=0, /C=TW/ST=Taiwan/L=Taipei/O=Generic/OU=Client/CN=Client/emailAddress=client@generic.com.tw
Jul 6 14:31:36	[Web VPN] 210.66.155.80:1131 VERIFY OK: depth=1, /C=TW/ST=Taiwan/L=Taipei/O=Generic/CN=Multi_Home_Gateway
Jul 6 14:31:36	[Web VPN] 210.66.155.80:1131 TLS: Initial packet from 210.66.155.80:1131, sid=50e4df69 dc2ce041
Jul 6 14:31:36	[Web VPN] TCPv4_SERVER link remote: 210.66.155.80:1131
Jul 6 14:31:36	[Web VPN] TCPv4_SERVER link local: [undef]
Jul 6 14:31:36	[Web VPN] TCP connection established with 210.66.155.80:1131
Jul 6 14:31:36	[Web VPN] Data Channel MTU parms [ L:1559 D:1450 EF:59 EB:4 ET:0 EL:0 ]
Jul 6 14:31:36	[Web VPN] Control Channel MTU parms [ L:1559 D:168 EF:68 EB:0 ET:0 EL:0 ]
Jul 6 14:31:36	[Web VPN] Re-using SSL/TLS context
Jul 6 14:31:36	[Web VPN] MULTI: multi_create_instance called
Jul 6 14:22:31	[Web VPN] TCP/UDP: Closing socket
Jul 6 14:22:31	[Web VPN] Client/210.66.155.80:1233 SIGUSR1[soft,ping-restart] received, client-instance restarting
Jul 6 14:22:31	[Web VPN] Client/210.66.155.80:1233 [Client] Inactivity timeout (--ping-restart), restarting

[Clear Data](#)

1 / 4155   [Next](#)

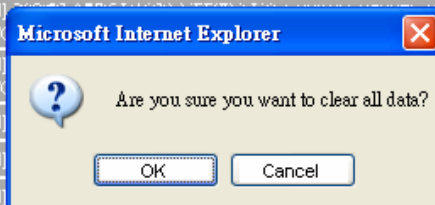
**Connection log Web UI**

**Step2** Click **Clear**, it shows the confirm window, and then click **OK**. All the records will be deleted in CS-2000.

1 / 4155 [Next](#)



Time	Event
Jul 6 14:46:49	[Web VPN] TCP/UDP: Closing socket
Jul 6 14:46:49	[Web VPN] Client/210.66.155.80:1131 SIGUSR1[soft,ping-restart] received, client-instance restarting
Jul 6 14:46:49	[Web VPN] Client/210.66.155.80:1131 [Client] Inactivity timeout (--ping-restart), restarting
Jul 6 14:31:37	[Web VPN] Client/210.66.155.80:1131 MULTI: primary virtual IP for Client/210.66.155.80:1131: 192.168.222.10
Jul 6 14:31:37	[Web VPN] Client/210.66.155.80:1131 MULTI: Learn: 192.168.222.10 -> Client/210.66.155.80:1131
Jul 6 14:31:37	[Web VPN] 210.66.155.80:1131 [Client] Peer Connection Initiated with 210.66.155.80:1131
Jul 6 14:31:37	[Web VPN] 210.66.155.80:1131 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Jul 6 14:31:36	[Web VPN] depth=0, /client/emailAddress=client@generic.com.tw
Jul 6 14:31:36	[Web VPN] depth=1, /Gateway
Jul 6 14:31:36	[Web VPN] 5.80:1131, sid=50e4df69 dc2ce041
Jul 6 14:31:36	[Web VPN]
Jul 6 14:31:36	[Web VPN]
Jul 6 14:31:36	[Web VPN] TCP connection established with 210.66.155.80:1131
Jul 6 14:31:36	[Web VPN] Data Channel MTU parms [ L:1559 D:1450 EF:59 EB:4 ET:0 EL:0 ]
Jul 6 14:31:36	[Web VPN] Control Channel MTU parms [ L:1559 D:168 EF:68 EB:0 ET:0 EL:0 ]
Jul 6 14:31:36	[Web VPN] Re-using SSL/TLS context
Jul 6 14:31:36	[Web VPN] MULTI: multi_create_instance called
Jul 6 14:22:31	[Web VPN] TCP/UDP: Closing socket
Jul 6 14:22:31	[Web VPN] Client/210.66.155.80:1233 SIGUSR1[soft,ping-restart] received, client-instance restarting
Jul 6 14:22:31	[Web VPN] Client/210.66.155.80:1233 [Client] Inactivity timeout (--ping-restart), restarting



**Clear Data**

1 / 4155 [Next](#)

**Delete all the connection log**

## Example 4. Log

MIS engineer can receive and save the record results from the CS-2000.

**Step1**     **System → Configure**, enable **E-mail Alert Notification** and enter the e-mail settings.

E-mail Setting	
<input checked="" type="checkbox"/> Enable E-mail Alert Notification	
Sender Address (Required by some ISPs)	notice@myalexweb.dyndr ( Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	61.62.236.14 ( Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	admin@myalexweb.dyndr ( Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	( Max. 60 characters, ex: user2@mydomain.com )
<input checked="" type="checkbox"/> Enable SMTP Server Authentication	
Username	admin
Password	*****
Mail Test	<input type="button" value="Mail Test"/>

E-mail setting Web UI

**Step2**     **Monitor → Log → Setting** , add the following settings :

Log Backup Setting	
Email Alarm Setting	
Send logs when Log database is full (300Kbytes)	
From SMTP Server	61.62.236.14
To E-mail Address 1	admin@myalexweb.dyndns.tv
Syslog Message Setting	
Syslog Host IP Address	192.168.1.10 ( ex: 192.168.1.61 )
Syslog Host Port	514 (Range : 1 - 65535, ex: 514)
Traffic Log Setting	
Storage lifetime	7 Days (Range : 1 - 99)
<input checked="" type="checkbox"/> Enable E-mail Log	
<input checked="" type="checkbox"/> Enable Syslog Message	
Event Log Setting	
Storage lifetime	7 Days (Range : 1 - 99)
<input checked="" type="checkbox"/> Enable E-mail Log	
<input checked="" type="checkbox"/> Enable Syslog Message	
Connection Log Setting	
Storage lifetime	7 Days (Range : 1 - 99)
<input checked="" type="checkbox"/> Enable E-mail Log	
<input checked="" type="checkbox"/> Enable Syslog Message	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

The log backup setting



Select **Enable E-mail Log**, CS-2000 sends e-mail log when log full 300kbytes then clear all the log.

## 12.2 Accounting Report

# **Accounting Report**

MIS engineer can use **Accounting Report** to view all the internal and external user's network accessing activities. (Includes the policy and VPN). **Accounting Report** can record user's upstream/downstream, first packet / last packet/duration, service and also provides the IP traffic and distribution charts.



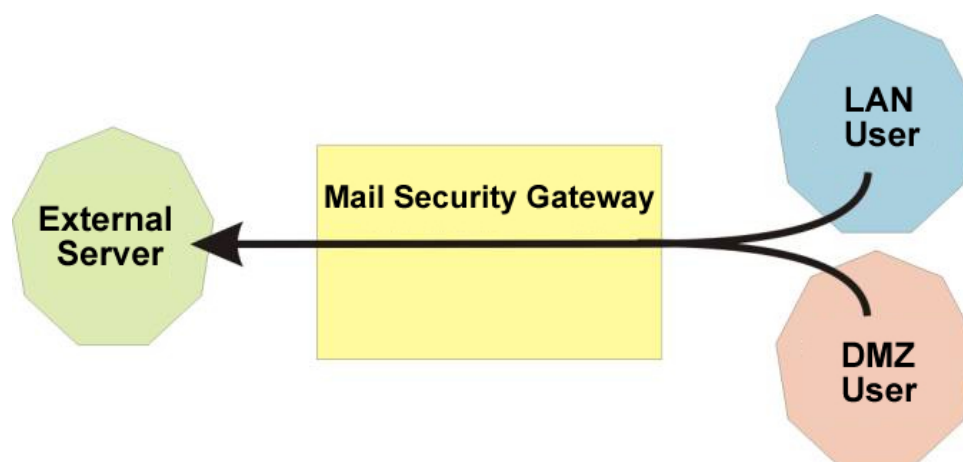
## Setting

### Setting

- Enable the account report, to record the inbound and outbound information in CS-2000.

Accounting Report includes **Outbound** and **Inbound**.

### Outbound Accounting Report



Account report can record any downstream /upstream service traffic used by LAN and DMZ user via CS-2000.

#### **USER** User

- Display LAN and DMZ user's accounting report.

#### **SITE** Site

- Display external server accounting report.

#### **SERVICE** Service

- Accounting report can record the service traffic used by LAN or DMZ user via CS-2000.

## Inbound Accounting Report



Account report can record any service downstream /upstream traffic used from external user to LAN or DMZ user via CS-2000.

### **USER** User

- Display the external user's accounting report.

### **SITE** Site

- Display the LAN and DMZ server accounting report.

### **SERVICE** Service

- Accounting report can record the service traffic used from external user to LAN or DMZ server via CS-2000.

## Example 1. Outbound

**Step1 Accounting Report → Outbound** , click **User** , it shows the accounting report of send / retrieve packets in downstream , upstream, first packet , last packet , duration from the external server to access user IP address in CS-2000.

- **User** : To view the needed record, and every 50 records to be a page.
- Select **USER** .
- **Source IP** : It is the LAN or DMZ user's IP address; click the source IP to show the user's information.
- **Downstream** : The percentage of user's traffic and total downstream from external server to access LAN or DMZ user via CS-2000.
- **Upstream** : The percentage of user's traffic and total upstream from LAN or DMZ user to access external server via CS-2000.
- **First Packet** : Record the first packet from LAN or DMZ user to access external server via CS-2000.
- **Last Packet** : Record the last packet from LAN or DMZ user to access external server via CS-2000.
- **Duration** : Record the duration (the first packet to last packet) from LAN or DMZ user to access external server via CS-2000.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from LAN or DMZ user to access external server.
- **Remove** : Delete the record.
- **Reset** : Clear all records and restart the accounting report.

Top Users: 1 - 7

<b>USER</b>		<b>SITE</b>		<b>SERVICE</b>					<b>Download</b>
No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	ENM-CHINESE	2.1 GB	60.2%	1.9 GB	72.1%	06/08 18:52:42	06/11 17:09:16	2D 22:16:34	<b>Remove</b>
2	ENM-ALEX	1.3 GB	38.5%	686.8 MB	26.6%	05/31 19:24:02	07/05 11:57:07	34D 16:33:05	<b>Remove</b>
3	592E03-001	25.6 MB	0.7%	1.0 MB	0.0%	06/01 15:40:19	07/04 11:39:03	32D 19:58:44	<b>Remove</b>
4	ENM10F	18.5 MB	0.5%	30.2 MB	1.2%	06/01 18:46:44	06/01 18:54:46	00:08:02	<b>Remove</b>
5	ENM-2003	694.1 KB	0.0%	1.2 MB	0.0%	05/31 19:39:14	06/27 00:00:15	26D 04:21:01	<b>Remove</b>
6	192.168.0.5	0.0 B	0.0%	152.0 B	0.0%	06/20 16:26:59	06/20 16:27:55	00:00:56	<b>Remove</b>
7	169.254.180.178	0.0 B	0.0%	152.0 B	0.0%	06/20 16:27:35	06/20 16:27:35	00:00:00	<b>Remove</b>
<b>Total Traffic</b>		3.5 GBytes		2.6 GBytes		Report time Thu Jul 5 11:57:12 2007			

**Reset Counters**

### Outbound user's accounting report

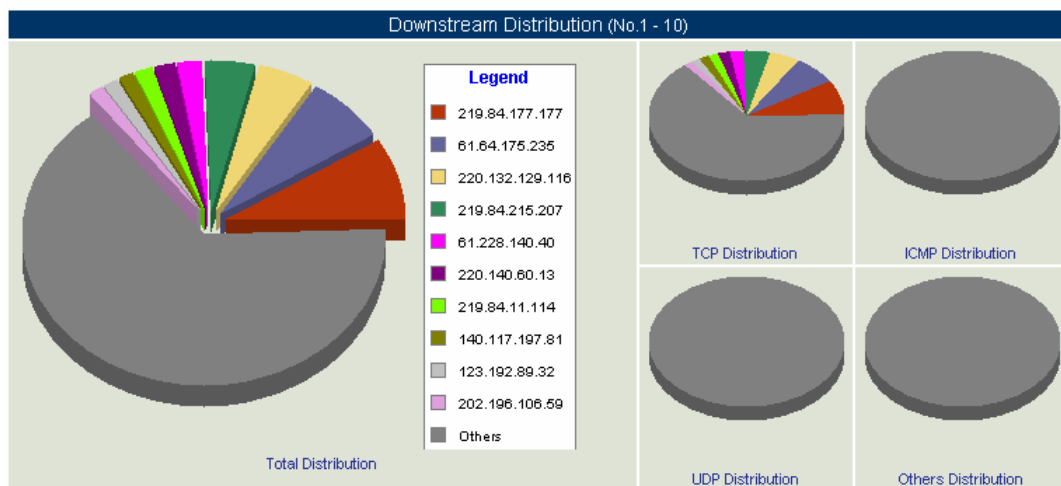
## ENM-ALEX Information

[Download](#)

IP Address	192.168.1.2
First / Last Packet (Duration)	05/31 19:24:02 -- 07/05 11:58:54 [34D 16:34:52]
DNS Name	
NetBIOS Name (Group)	ENM-ALEX (PLANET)
MAC Address (NIC Vendor)	00:30:4F:27:60:EF (PLANET Technology Corporation)
Total Data Downstream / Upstream	1.3 GBytes / 686.8 MBytes


1 / 4843 [Next](#)Top Sites: 1 - 10 

No.	Destination IP	Downstream		TCP		UDP		ICMP		Others	
1	219.84.177.177	117.4 MB	8.8%	117.4 MB	8.9%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
2	61.64.175.235	94.1 MB	7.1%	94.1 MB	7.2%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
3	220.132.129.116	65.9 MB	4.9%	65.9 MB	5.0%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
4	219.84.215.207	58.4 MB	4.4%	58.4 MB	4.4%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
5	61.228.140.40	27.5 MB	2.1%	27.5 MB	2.1%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
6	220.140.60.13	24.9 MB	1.9%	24.9 MB	1.9%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
7	219.84.11.114	21.0 MB	1.6%	21.0 MB	1.6%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
8	140.117.197.81	20.7 MB	1.5%	20.7 MB	1.6%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
9	123.192.89.32	20.3 MB	1.5%	20.3 MB	1.5%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
10	202.196.106.59	17.8 MB	1.3%	17.8 MB	1.4%	0.0 B	0.0%	0.0 B	0.0%	0.0 B	0.0%
Total Traffic		1.3 GBytes		1.3 GBytes		20.3 MBytes		808.1 KBytes		0.0 Bytes	



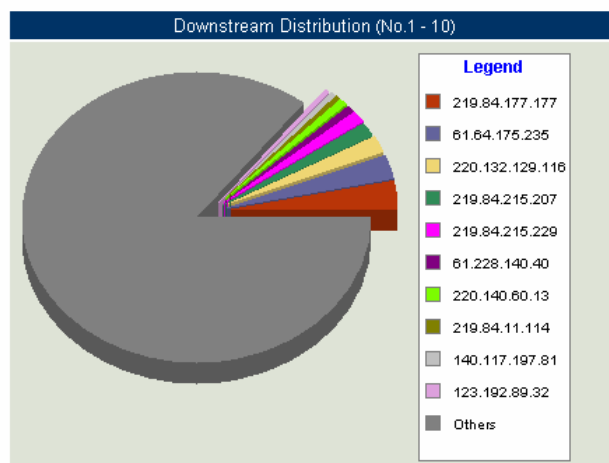
## Outbound user's information

**Step2**     **Accounting Report → Outbound** , click **Site** , it shows the send/retrieve packet traffic report of downstream , upstream    and downstream distribution used by external server via the CS-2000 IP address

- **Site** : View the needed record, and every 10 records to be one page.
- Select  .
- **Destination IP (User)** : It means the external server IP or represents the LAN or DMZ user numbers to access the external server.
- **Source IP** : It means the LAN or DMZ user's IP address, to access the external server.
- **Downstream** : The percentage of traffic and total downstream traffic from external server to access LAN or DMZ user via CS-2000.
- **Upstream** : The percentage of traffic and total upstream traffic from LAN or DMZ user to access external server via CS-2000.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from LAN or DMZ user to access external server.
- **Downstream Distribution** : Display the distribution charts depends on the real downstream traffic.

1 / 8432 [Next](#) Top Sites: 1 - 10 [Download](#)

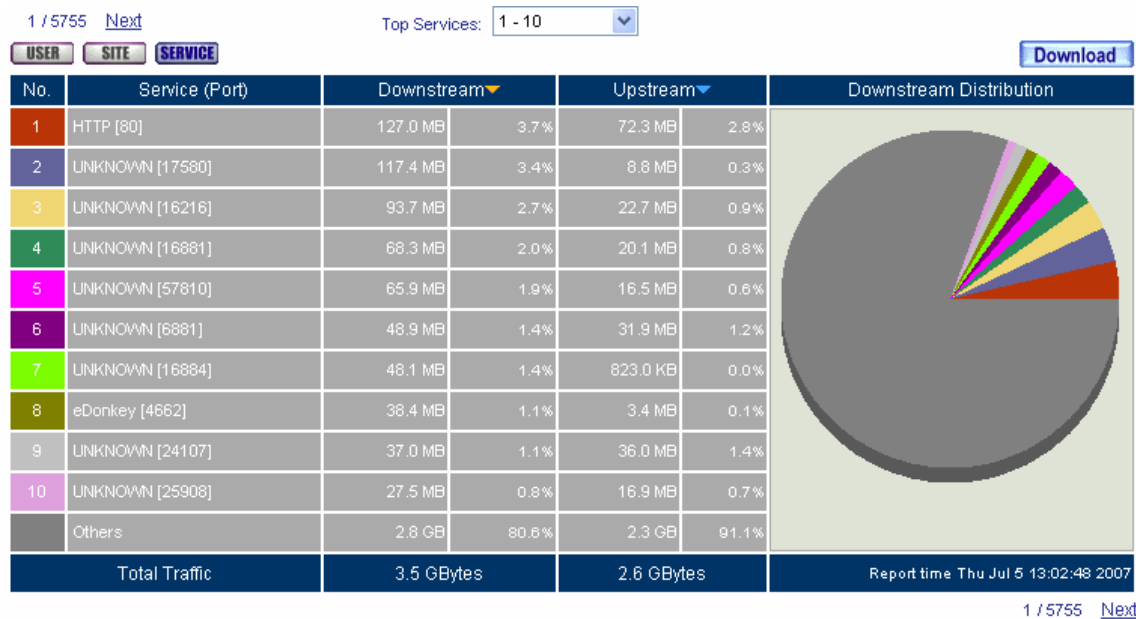
No.	Destination IP (User)	Source IP	Downstream		Upstream	
1	219.84.177.177 (1)	(1) ENM-ALEX [192.168.1.2]	117.4 MB	3.4%	8.8 MB	0.3%
2	61.64.175.235 (1)	(1) ENM-ALEX [192.168.1.2]	94.1 MB	2.7%	22.8 MB	0.9%
3	220.132.129.116 (1)	(1) ENM-ALEX [192.168.1.2]	65.9 MB	1.9%	16.5 MB	0.6%
4	219.84.215.207 (1)	(1) ENM-ALEX [192.168.1.2]	58.4 MB	1.7%	9.5 MB	0.4%
5	219.84.215.229 (1)	(1) ENM-CHINESE [192.168.1.5]	48.1 MB	1.4%	820.7 KB	0.0%
6	61.228.140.40 (1)	(1) ENM-ALEX [192.168.1.2]	27.5 MB	0.8%	16.9 MB	0.7%
7	220.140.60.13 (1)	(1) ENM-ALEX [192.168.1.2]	24.9 MB	0.7%	24.4 MB	0.9%
8	219.84.11.114 (1)	(1) ENM-ALEX [192.168.1.2]	21.0 MB	0.6%	25.3 MB	1.0%
9	140.117.197.81 (1)	(1) ENM-ALEX [192.168.1.2]	20.7 MB	0.6%	1.1 MB	0.0%
10	123.192.89.32 (1)	(1) ENM-ALEX [192.168.1.2]	20.3 MB	0.6%	16.5 MB	0.6%
Total Traffic			3.5 GBytes		2.6 GBytes	



Outbound site accounting report


**Step3 Accounting Report → Outbound** , click **Service** , it shows the statistics and distribution charts of user's service downstream , upstream and downstream distribution from LAN or DMZ to external server.

- **Service** : View the needed record, and every 10 records to be one page.
- Select **SERVICE** .
- **Service (Port)** : It means the service name used from the LAN or DMZ user to access external server.
- **Downstream** : It means the percentage of traffic and total downstream traffic from external server to access LAN or DMZ user via CS-2000.
- **Upstream** : It means the percentage of traffic and total upstream traffic from LAN or DMZ user to access external server via CS-2000.
- **Total Traffic** : Accumulate every service percentage and total traffic of downstream / upstream.
- **Downstream Distribution** : Display the distribution charts depends on the real downstream traffic.



### Outbound service accounting report

## Example 2. Inbound

- Step1**    **Accounting Report → Inbound** , click **User** , it shows the accounting report of send / retrieve packets in downstream , upstream, first packet , last packet   duration from external server to access the user IP address in CS-2000.
- **User** : To view the needed record, and every 50 records to be a page.
  - Select 
  - **Source IP** : It is the external user IP address; click the source IP to show the user's information.
  - **Upstream** : The percentage of user's traffic and total upstream from LAN or DMZ server to access external user via CS-2000.
  - **Downstream** : The percentage of user's traffic and total downstream from external user to access LAN or DMZ server via CS-2000.
  - **First Packet** : Record the first packet from external user to access LAN or DMZ server via CS-2000.
  - **Last Packet** : Record the last packet from external user to access LAN or DMZ server via CS-2000.
  - **Duration** : Record the duration (the first packet to last packet) from external user to access LAN or DMZ server via CS-2000.
  - **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from external user to access LAN or DMZ server.
  - **Remove** : Delete the record.
  - **Reset** : Clear all records and restart the accounting report.



1 / 2 [Next](#)

Top Users: 1 - 20

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	myalexxweb....br	41.1 MB	56.8%	1.1 MB	62.2%	06/01 14:21:43	06/25 09:56:14	23D 19:34:31	<input type="button" value="Remove"/>
2	203.128.255.14	15.9 MB	22.0%	311.1 KB	18.1%	06/08 21:42:15	06/13 23:05:54	5D 01:23:39	<input type="button" value="Remove"/>
3	203.128.255.25	14.2 MB	19.7%	286.5 KB	16.6%	06/08 15:47:08	06/08 21:53:55	06:06:47	<input type="button" value="Remove"/>
4	M89E11-001	1.1 MB	1.5%	49.0 KB	2.8%	06/06 14:39:39	06/07 10:07:55	19:28:16	<input type="button" value="Remove"/>
5	203.128.255.74	1.9 KB	0.0%	1.3 KB	0.1%	06/09 14:45:15	06/09 14:48:06	00:02:51	<input type="button" value="Remove"/>
6	24.249.124.45	523.0 B	0.0%	484.0 B	0.0%	06/08 13:32:54	06/08 13:32:54	00:00:00	<input type="button" value="Remove"/>
7	67.153.136.250	199.0 B	0.0%	168.0 B	0.0%	06/06 21:29:14	06/06 21:29:14	00:00:00	<input type="button" value="Remove"/>
8	62.93.184.4	199.0 B	0.0%	168.0 B	0.0%	06/25 03:27:14	06/25 03:27:14	00:00:00	<input type="button" value="Remove"/>
9	146.145.161.34	199.0 B	0.0%	216.0 B	0.0%	06/05 17:56:04	06/05 17:56:04	00:00:00	<input type="button" value="Remove"/>
10	68.160.80.130	199.0 B	0.0%	168.0 B	0.0%	06/25 02:49:17	06/25 02:49:17	00:00:00	<input type="button" value="Remove"/>
11	209.200.241.95	199.0 B	0.0%	168.0 B	0.0%	06/24 09:37:01	06/24 09:37:01	00:00:00	<input type="button" value="Remove"/>
12	67.55.237.38	191.0 B	0.0%	248.0 B	0.0%	06/11 05:41:13	06/11 05:41:13	00:00:00	<input type="button" value="Remove"/>
13	61.63.28.132	0.0 B	0.0%	80.0 B	0.0%	06/06 08:27:55	06/06 08:42:07	00:14:12	<input type="button" value="Remove"/>
14	61.106.56.10	0.0 B	0.0%	96.0 B	0.0%	06/21 12:51:54	06/21 12:51:58	00:00:04	<input type="button" value="Remove"/>
15	218.62.75.202	0.0 B	0.0%	40.0 B	0.0%	06/23 15:40:14	06/23 15:40:14	00:00:00	<input type="button" value="Remove"/>
16	165.207.52.6	0.0 B	0.0%	96.0 B	0.0%	06/24 13:48:35	06/24 13:48:35	00:00:00	<input type="button" value="Remove"/>
17	61.23.171.224	0.0 B	0.0%	96.0 B	0.0%	06/20 09:40:52	06/20 09:40:52	00:00:00	<input type="button" value="Remove"/>
18	64.235.253.129	0.0 B	0.0%	120.0 B	0.0%	06/20 09:29:29	06/20 09:29:29	00:00:00	<input type="button" value="Remove"/>
19	61.62.93.11	0.0 B	0.0%	192.0 B	0.0%	06/15 18:07:59	06/15 18:29:54	00:21:55	<input type="button" value="Remove"/>
20	216.127.76.3	0.0 B	0.0%	120.0 B	0.0%	06/14 10:03:49	06/14 10:03:49	00:00:00	<input type="button" value="Remove"/>
Total Traffic		72.4 MBytes		1.7 MBytes		Report time: Thu Jul 5 13:03:58 2007			

1 / 2 [Next](#)

## Inbound user accounting report

## M89E11-001 Information

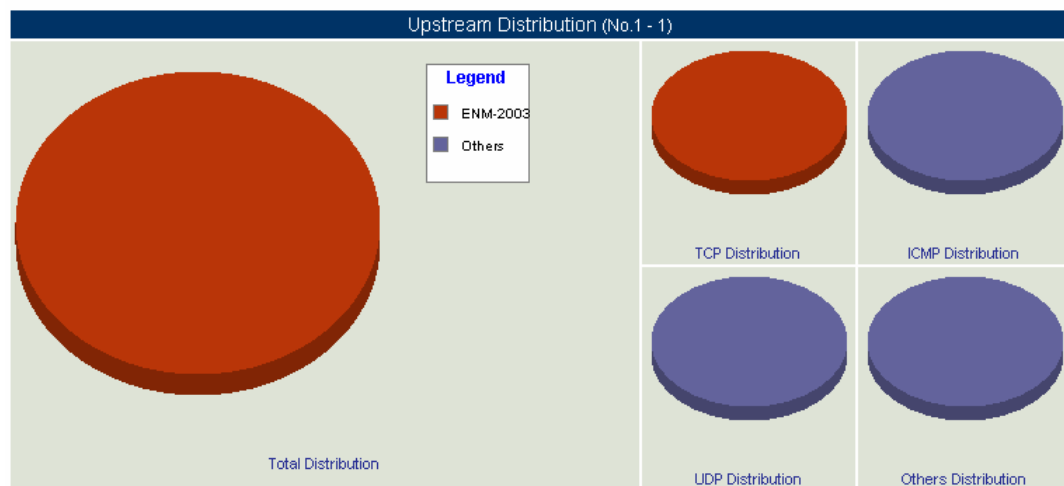
[Download](#)

IP Address	210.66.155.76
First / Last Packet (Duration)	06/06 14:39:39 -- 06/07 10:07:55 [19:28:16]
DNS Name	
NetBIOS Name (Group)	M89E11-001 (WORKGROUP)
MAC Address (NIC Vendor)	10:C0:02:FF:F1:08 (UNKNOWN)
Total Data Downstream / Upstream	49.0 KBytes / 1.1 MBytes

Top Sites: 1 - 1



No.	Destination IP	Upstream	TCP	UDP	ICMP	Others
1	ENM-2003	1.1 MB 100.0%	1.1 MB 100.0%	0.0 B 0.0%	0.0 B 0.0%	0.0 B 0.0%
Total Traffic		1.1 MBytes	1.1 MBytes	0.0 Bytes	0.0 Bytes	0.0 Bytes



## Inbound user's information

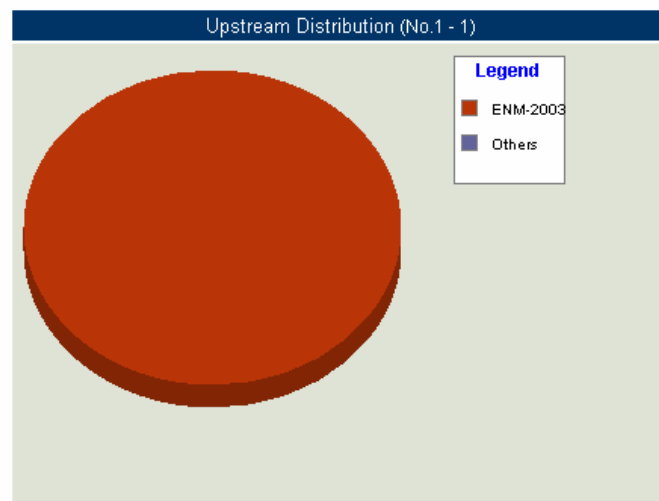
**Step2 Accounting Report → Inbound** , click **Site** , it shows the send / retrieve packet traffic report of downstream , upstream and upstream distribution used by LAN or DMZ server via the CS-2000 IP address

- **Site** : View the needed record, and every 10 records to be one page.
- Select **SITE**
- **Destination IP (User)** : It means the LAN or DMZ server IP or represents the external user numbers to access the LAN or DMZ server.
- **Source IP** : It means the external user's IP address, to access the LAN or DMZ server.
- **Downstream** : The percentage of traffic and total downstream traffic from external user to access LAN or DMZ server via CS-2000.
- **Upstream** : The percentage of traffic and total upstream traffic from LAN or DMZ server to access external user via CS-2000.
- **Total Traffic** : Accumulate every user's total downstream / upstream traffic and its percentage from external user to access LAN or DMZ server.
- **Upstream Distribution** : Display the distribution charts depends on the real upstream traffic.

Top Sites: 1 - 1

[USER](#)
[SITE](#)
[SERVICE](#)
[Download](#)

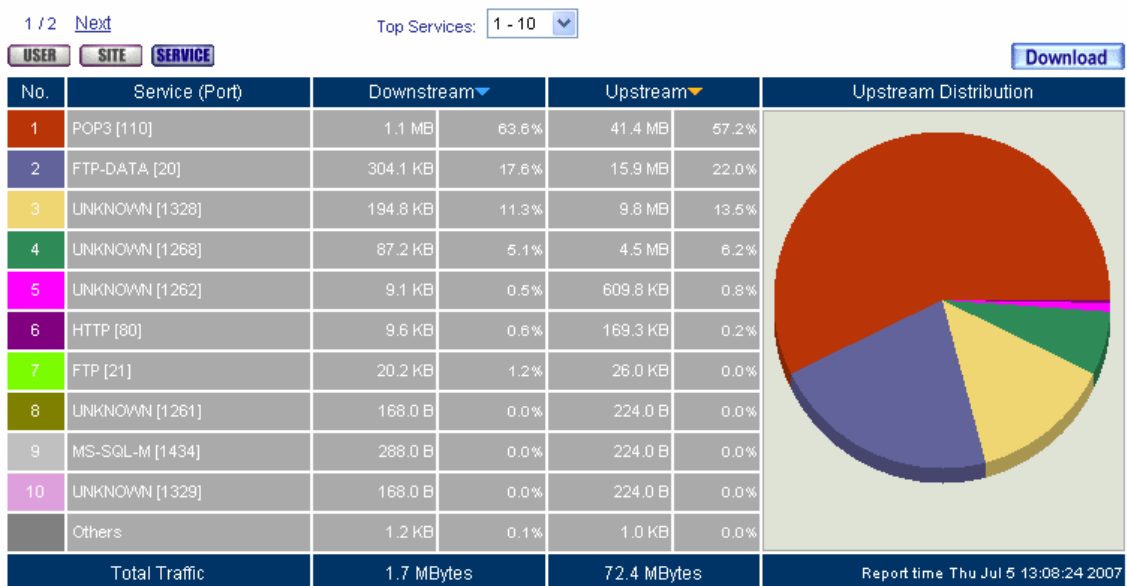
No.	Destination IP (User)	Source IP	Downstream		Upstream	
1	ENM-2003 (26)	(1) myalexweb.dyndns.tv	1.7 MB	100.0%	72.4 MB	100.0%
Total Traffic			1.7 MBytes		72.4 MBytes	



**Inbound site accounting report**

**Step3 Accounting Report → Inbound** , click **Service** , it shows the statistics and distribution charts of user's service downstream , upstream and upstream distribution from external user to LAN or DMZ server.

- **Service** : View the needed record, and every 10 records to be one page.
- Select **SERVICE**
- **Service (Port)** : It means the service name used from the external user to access LAN or DMZ server.
- **Downstream** : It means the percentage of traffic and total downstream traffic from external user to access LAN or DMZ server via CS-2000.
- **Upstream** : It means the percentage of traffic and total upstream traffic from LAN or DMZ server to access external user via CS-2000.
- **Total Traffic** : Accumulate every service percentage and total traffic of downstream/upstream.
- **Upstream Distribution** : Display the distribution charts depends on the real upstream traffic.



1 / 2 [Next](#)

### Inbound service accounting report

## 12.3 Statistics

# Statistics

**WAN statistics**, it includes all the upstream / downstream packets pass through the WAN interface and traffic log in upstream / downstream.

**Policy statistics**, it includes all the upstream / downstream packets pass through the Policy and traffic log in upstream/downstream.

**MIS engineer can use the statistics to easily know the status of WAN or the packet and stream in policy.**

## Statistics

### Statistics charts

- Ordinate : Network stream.
- Horizontal ordinate : Time ( hour / minute ) .

### Source, Destination, Service, Action

- Record the original **Policy** setting, MIS engineer can easily know the **Policy statistics** belongs to which **Policy**.

### Time

- MIS engineer can respectively to view the statistics according to time unit of minute , hour , day , week , Month and Year.



#### MIS engineer can select the time unit :

1. **Minute** : Refresh the statistics charts every minute.
2. **Hour** : Refresh the statistics charts every hour.
3. **Day** ; Refresh the statistics charts every day.
4. **Week** : Refresh the statistics charts every week.
5. **Month** : Refresh the statistics charts every month.
6. **Year** : Refresh the statistics charts every year.

### Bytes/sec Bytes/sec Utilization Total

- MIS engineer can modify the ordinate stream unit in statistics charts.
  - ◆ Utilization : The maximum stream of CS-2000 (according to the stream setting in **Interface**.)
  - ◆ Total : Use the accumulated total stream to be the ordinate in time unit.

## Example 1. WAN

**Step1**     **Statistics → WAN**, it shows all the downstream / upstream packets and statistics pass through **WAN interface**.

- Time : View the statistics charts according to the unit of minute, hour, day, week, month, and year.

WAN	Time
WAN 1	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
WAN 2	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
All WAN Interface	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>

The WAN statistics



The **WAN statistics** is the attached function of **WAN interface**. The **WAN statistics** enabled as enabled the **WAN interface**.

**Step2**     **Statistics → WAN**, select the WAN to view.

- Click **Minute**, to view the statistic charts results in every minute.
- Click **Hour**, to view the statistic charts results in every hour.
- Click **Day**, to view the statistic charts results in every day.
- Click **Week**, to view the statistics charts results in every week.
- Click **Month**, to view the statistics results in every month.
- Click **Year**, to view the statistics charts results in every year.

**Step3**     Statistic charts

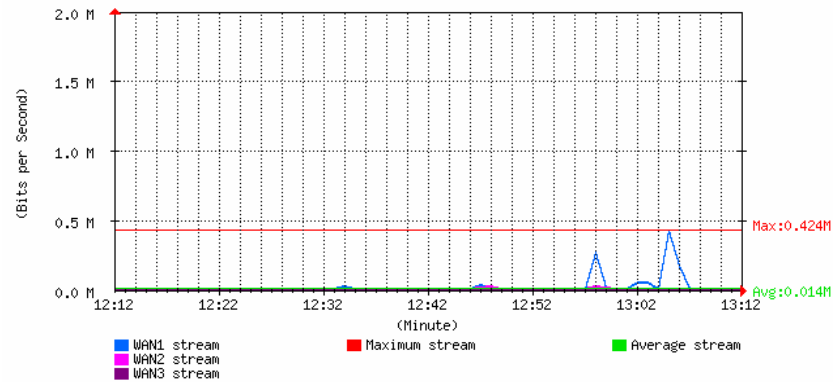
- Ordinate : Network flow.
- Horizontal ordinate : Time (hour / minute).

Bits/sec Bytes/sec Utilization Total

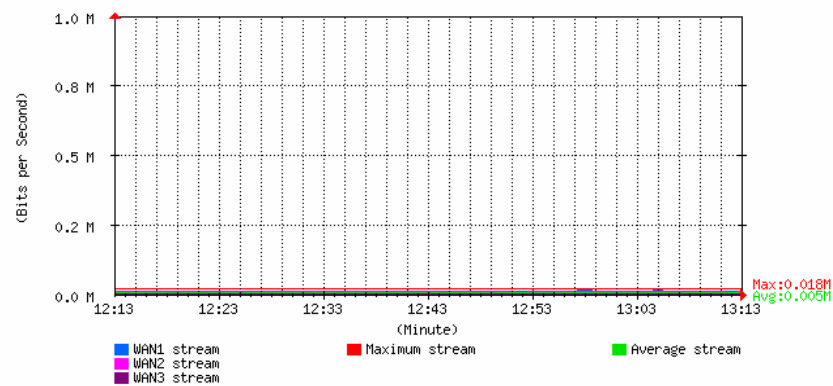
Minute Hour Day Week Month Yes

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

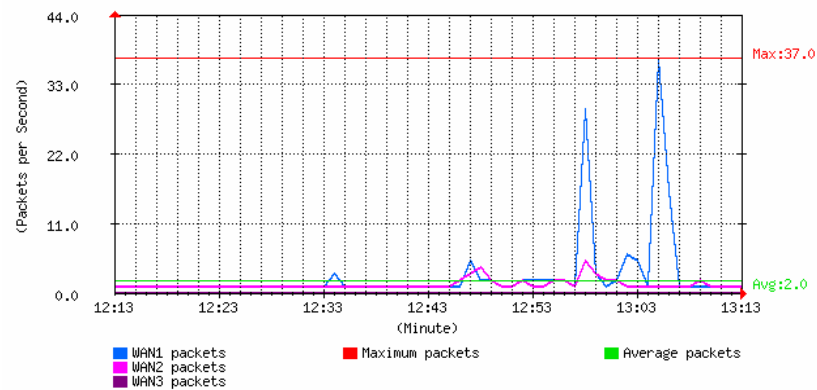
#### Downstream



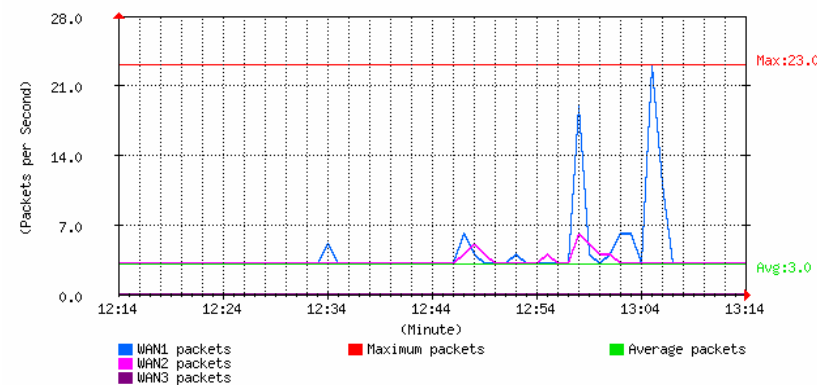
#### Upstream



#### Receive Packets



#### Transmit Packets



[View the network flow](#)



## Example 2. Policy

**Step1** As enabled **Policy → Statistics** option, then the **Policy statistics charts** enabled in **Statistics → Policy**.

Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY		<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
Outside_Any	Inside_Any(Routing)	ANY		<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>

The policy statistics



If the MIS engineer wants to enable the **Policy Statistics**, then he must enable the statistic option in **Policy**.

**Step2** **Statistics → Policy**, select the policy to view.

- Click **Minute**, to view the statistic charts results in every minute.
- Click **Hour**, to view the statistic charts results in every hour.
- Click **Day**, to view the statistic charts results in every day.
- Click **Week**, to view the statistics charts results in every week.
- Click **Month**, to view the statistics results in every month.
- Click **Year**, to view the statistics charts results in every year.

**Step3** Network flow statistic charts.

- Ordinate : Network flow.
- Horizontal ordinate : Time ( hour/minute ) .

[Bits/sec](#) [Bytes/sec](#) [Total](#)

Inside\_Any to Outside\_Any

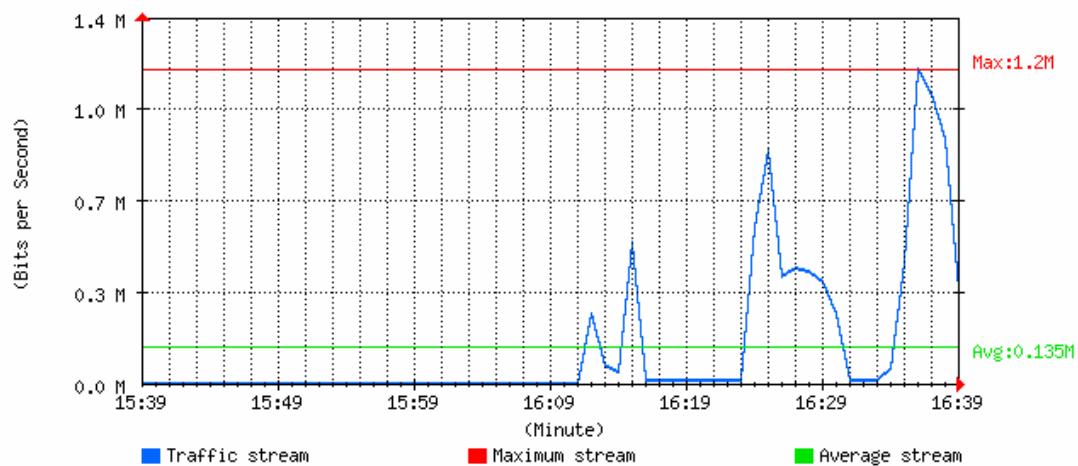
Service : AN

Action : perr

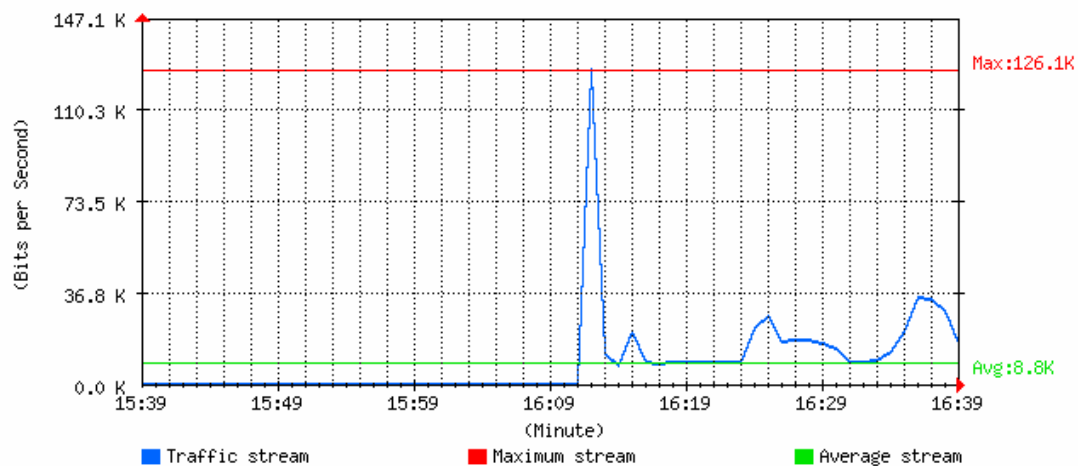
[Minute](#) [Hour](#) [Day](#) [Week](#) [Month](#) [Ye](#)

Real-time: Down 382.8 KBits/sec Up 15.6 KBits/sec

## Downstream



## Upstream



[View the policy statistics charts](#)

## 12.4 Diagnostic

# **Diagnostic**

The MIS engineer can set the CS-2000 proactively send the packets (Ping and Traceroute) to detect the status of WAN interface.

We will make the introduction of Diagnostic function.

## Example 1. Ping

**Step1.** In **Diagnostic → Ping**, the MIS engineer can set the CS-2000 send the packets to specific address, to detects the status of WAN interface :

- Enter the **Destination IP / Domain name**.
- Enter the **Packet size**. ( Default setting is 32 Bytes )
- Enter **Count** value. ( Default setting is 4)
- Enter **Wait time**. ( Default setting is 1 second)
- Enter the source packets **Interface**.
- Click **OK**.

Ping Setting	
Destination IP / Domain name	<input type="text" value="www.google.com"/> (Max. 30 characters)
Packet size	<input type="text" value="32"/> Bytes ( Range: 1 - 9999 )
Count	<input type="text" value="4"/> ( Range: 0 - 9999, 0: means unlimited )
Wait time	<input type="text" value="1"/> Seconds ( Range: 1 - 9999 )
Interface	<input type="text" value="WAN1"/> <input type="text" value="203.67.31.11"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Ping Result		
<table><thead><tr><th>Result</th></tr></thead><tbody><tr><td>There is no message!</td></tr></tbody></table>	Result	There is no message!
Result		
There is no message!		

Ping setting

Ping Setting	
Destination IP / Domain name	<input type="text" value="www.google.com"/> (Max. 30 characters)
Packet size	<input type="text" value="32"/> Bytes ( Range: 1 - 9999 )
Count	<input type="text" value="4"/> ( Range: 0 - 9999, 0: means unlimited )
Wait time	<input type="text" value="1"/> Seconds ( Range: 1 - 9999 )
Interface	<input type="text" value="WAN1"/> <input type="text" value="203.67.31.11"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Ping Result										
<table><thead><tr><th>Result</th></tr></thead><tbody><tr><td>PING www.l.google.com (72.14.235.104) from 203.67.31.11 : 32 bytes of data.</td></tr><tr><td> </td></tr><tr><td>Reply from 72.14.235.104: bytes=32 icmp_seq=0 ttl=248 time=38.483 msec</td></tr><tr><td>Reply from 72.14.235.104: bytes=32 icmp_seq=1 ttl=247 time=36.201 msec</td></tr><tr><td>Reply from 72.14.235.104: bytes=32 icmp_seq=2 ttl=248 time=50.127 msec</td></tr><tr><td>Reply from 72.14.235.104: bytes=32 icmp_seq=3 ttl=248 time=40.488 msec</td></tr><tr><td> </td></tr><tr><td>4 packets transmitted, 4 packets received, 0% packet loss</td></tr><tr><td>round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms</td></tr></tbody></table>	Result	PING www.l.google.com (72.14.235.104) from 203.67.31.11 : 32 bytes of data.		Reply from 72.14.235.104: bytes=32 icmp_seq=0 ttl=248 time=38.483 msec	Reply from 72.14.235.104: bytes=32 icmp_seq=1 ttl=247 time=36.201 msec	Reply from 72.14.235.104: bytes=32 icmp_seq=2 ttl=248 time=50.127 msec	Reply from 72.14.235.104: bytes=32 icmp_seq=3 ttl=248 time=40.488 msec		4 packets transmitted, 4 packets received, 0% packet loss	round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms
Result										
PING www.l.google.com (72.14.235.104) from 203.67.31.11 : 32 bytes of data.										
Reply from 72.14.235.104: bytes=32 icmp_seq=0 ttl=248 time=38.483 msec										
Reply from 72.14.235.104: bytes=32 icmp_seq=1 ttl=247 time=36.201 msec										
Reply from 72.14.235.104: bytes=32 icmp_seq=2 ttl=248 time=50.127 msec										
Reply from 72.14.235.104: bytes=32 icmp_seq=3 ttl=248 time=40.488 msec										
4 packets transmitted, 4 packets received, 0% packet loss										
round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms										
<input type="button" value="Clear Data"/>										

**Ping results**



If the MIS engineer select **VPN** of Interface, then he must enter the local CS-2000 LAN interface IP , and enter the remote LAN IP (which can send or receive packets via VPN) in to **Destination IP / Domain name** column.

- Use the following method to detect the VPN status of local 192.168.189.X/24 segment and remote 192.168.169.X/24 segment.

Ping Setting	
Destination IP / Domain name	192.168.168.30 (Max. 30 characters)
Packet size	32 Bytes ( Range: 1 - 9999 )
Count	4 ( Range: 0 - 9999, 0: means unlimited )
Wait time	1 Seconds ( Range: 1 - 9999 )
Interface	VPN 192.168.189.1
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Ping Result								
<table border="1"> <thead> <tr> <th>Result</th> </tr> </thead> <tbody> <tr> <td>PING 192.168.169.30(192.168.169.30) from 192.168.189.1 : 32 bytes of data.</td> </tr> <tr> <td>Reply from 192.168.169.30 : bytes=32 icmp_seq=0 ttl=248 time=38.483 msec</td> </tr> <tr> <td>Reply from 192.168.169.30 : bytes=32 icmp_seq=1 ttl=247 time=36.201 msec</td> </tr> <tr> <td>Reply from 192.168.169.30 : bytes=32 icmp_seq=2 ttl=248 time=50.127 msec</td> </tr> <tr> <td>Reply from 192.168.169.30 : bytes=32 icmp_seq=3 ttl=248 time=40.488 msec</td> </tr> <tr> <td>4 packets transmitted, 4 packets received, 0% packet loss</td> </tr> <tr> <td>round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms</td> </tr> </tbody> </table>	Result	PING 192.168.169.30(192.168.169.30) from 192.168.189.1 : 32 bytes of data.	Reply from 192.168.169.30 : bytes=32 icmp_seq=0 ttl=248 time=38.483 msec	Reply from 192.168.169.30 : bytes=32 icmp_seq=1 ttl=247 time=36.201 msec	Reply from 192.168.169.30 : bytes=32 icmp_seq=2 ttl=248 time=50.127 msec	Reply from 192.168.169.30 : bytes=32 icmp_seq=3 ttl=248 time=40.488 msec	4 packets transmitted, 4 packets received, 0% packet loss	round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms
Result								
PING 192.168.169.30(192.168.169.30) from 192.168.189.1 : 32 bytes of data.								
Reply from 192.168.169.30 : bytes=32 icmp_seq=0 ttl=248 time=38.483 msec								
Reply from 192.168.169.30 : bytes=32 icmp_seq=1 ttl=247 time=36.201 msec								
Reply from 192.168.169.30 : bytes=32 icmp_seq=2 ttl=248 time=50.127 msec								
Reply from 192.168.169.30 : bytes=32 icmp_seq=3 ttl=248 time=40.488 msec								
4 packets transmitted, 4 packets received, 0% packet loss								
round-trip min/avg/max/mdev = 36.201/41.324/50.127/5.309 ms								
<input type="button" value="Clear Data"/>								

The Ping results of VPN

## Example 2. Traceroute

**Step1.** In **Diagnostic → Traceroute**, the MIS engineer can set the CS-2000 send the packets to specific address by traceroute command, to detects the status of WAN interface :

- Enter the **Destination IP / Domain name**.
- Enter the **Packet size**.( Default setting is 40 Bytes )
- Enter the **MAX Time-to-Live**.( Default setting is 30 Hops)
- Enter the **Wait time**.( Default setting is 2 seconds)
- Select the source packets **Interface**.
- Click **OK**.

Traceroute Setting	
Destination IP / Domain name	<input type="text" value="www.hinet.net"/> (Max. 30 characters)
Packet size	<input type="text" value="40"/> Bytes ( Range: 40 - 9999 )
Max Time-to-Live	<input type="text" value="30"/> Hops ( Range: 1 - 255 )
Wait time	<input type="text" value="2"/> Seconds ( Range: 2 - 9999 )
Interface	<input type="text" value="WAN1"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Traceroute Result		
<table><thead><tr><th>Result</th></tr></thead><tbody><tr><td>There is no message!</td></tr></tbody></table>	Result	There is no message!
Result		
There is no message!		

Traceroute setting

Traceroute Setting	
Destination IP / Domain name	<input type="text" value="www.hinet.net"/> (Max. 30 characters)
Packet size	<input type="text" value="40"/> Bytes ( Range: 40 - 9999 )
Max Time-to-Live	<input type="text" value="30"/> Hops ( Range: 1 - 255 )
Wait time	<input type="text" value="2"/> Seconds ( Range: 2 - 9999 )
Interface	<input type="text" value="WAN1"/> ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Traceroute Result																		
<table><thead><tr><th>Result</th></tr></thead><tbody><tr><td>traceroute: Warning: www.hinet.net has multiple addresses; using 203.66.88.89</td></tr><tr><td>traceroute to www.hinet.net (203.66.88.89), 30 hops max, 40 byte packets from 203.67.31.11</td></tr><tr><td>From 203.67.31.11</td></tr><tr><td>To hop 1 : IP = 203.67.31.1 round-trip min/avg/max = 0.572/0.671/0.790 ms</td></tr><tr><td>To hop 2 : IP = 61.62.236.254 round-trip min/avg/max = 34.114/38.033/43.546 ms</td></tr><tr><td>To hop 3 : IP = 61.64.191.181 round-trip min/avg/max = 34.322/34.515/34.662 ms</td></tr><tr><td>To hop 4 : IP = 61.64.126.5 round-trip min/avg/max = 34.592/41.666/55.523 ms</td></tr><tr><td>To hop 5 : IP = 61.64.126.26 round-trip min/avg/max = 34.437/39.157/48.532 ms</td></tr><tr><td>To hop 6 : IP = 61.64.212.170 round-trip min/avg/max = 34.361/34.812/35.088 ms</td></tr><tr><td>To hop 7 : IP = 61.64.212.222 round-trip min/avg/max = 34.975/35.324/35.531 ms</td></tr><tr><td>To hop 8 : IP = 203.75.228.70 round-trip min/avg/max = 35.185/35.550/36.079 ms</td></tr><tr><td>To hop 9 : IP = 211.22.32.82 round-trip min/avg/max = 34.615/34.824/34.944 ms</td></tr><tr><td>To hop 10: IP = 220.128.2.86 round-trip min/avg/max = 35.062/35.173/35.370 ms</td></tr><tr><td>To hop 11: IP = 220.128.2.117 round-trip min/avg/max = 35.004/35.146/35.381 ms</td></tr><tr><td>To hop 12: IP = 211.22.35.37 round-trip min/avg/max = 35.007/35.406/35.686 ms</td></tr><tr><td>To hop 13: IP = 203.66.88.89 round-trip min/avg/max = 34.959/35.457/35.924 ms</td></tr><tr><td>Traceroute complete</td></tr></tbody></table>	Result	traceroute: Warning: www.hinet.net has multiple addresses; using 203.66.88.89	traceroute to www.hinet.net (203.66.88.89), 30 hops max, 40 byte packets from 203.67.31.11	From 203.67.31.11	To hop 1 : IP = 203.67.31.1 round-trip min/avg/max = 0.572/0.671/0.790 ms	To hop 2 : IP = 61.62.236.254 round-trip min/avg/max = 34.114/38.033/43.546 ms	To hop 3 : IP = 61.64.191.181 round-trip min/avg/max = 34.322/34.515/34.662 ms	To hop 4 : IP = 61.64.126.5 round-trip min/avg/max = 34.592/41.666/55.523 ms	To hop 5 : IP = 61.64.126.26 round-trip min/avg/max = 34.437/39.157/48.532 ms	To hop 6 : IP = 61.64.212.170 round-trip min/avg/max = 34.361/34.812/35.088 ms	To hop 7 : IP = 61.64.212.222 round-trip min/avg/max = 34.975/35.324/35.531 ms	To hop 8 : IP = 203.75.228.70 round-trip min/avg/max = 35.185/35.550/36.079 ms	To hop 9 : IP = 211.22.32.82 round-trip min/avg/max = 34.615/34.824/34.944 ms	To hop 10: IP = 220.128.2.86 round-trip min/avg/max = 35.062/35.173/35.370 ms	To hop 11: IP = 220.128.2.117 round-trip min/avg/max = 35.004/35.146/35.381 ms	To hop 12: IP = 211.22.35.37 round-trip min/avg/max = 35.007/35.406/35.686 ms	To hop 13: IP = 203.66.88.89 round-trip min/avg/max = 34.959/35.457/35.924 ms	Traceroute complete
Result																		
traceroute: Warning: www.hinet.net has multiple addresses; using 203.66.88.89																		
traceroute to www.hinet.net (203.66.88.89), 30 hops max, 40 byte packets from 203.67.31.11																		
From 203.67.31.11																		
To hop 1 : IP = 203.67.31.1 round-trip min/avg/max = 0.572/0.671/0.790 ms																		
To hop 2 : IP = 61.62.236.254 round-trip min/avg/max = 34.114/38.033/43.546 ms																		
To hop 3 : IP = 61.64.191.181 round-trip min/avg/max = 34.322/34.515/34.662 ms																		
To hop 4 : IP = 61.64.126.5 round-trip min/avg/max = 34.592/41.666/55.523 ms																		
To hop 5 : IP = 61.64.126.26 round-trip min/avg/max = 34.437/39.157/48.532 ms																		
To hop 6 : IP = 61.64.212.170 round-trip min/avg/max = 34.361/34.812/35.088 ms																		
To hop 7 : IP = 61.64.212.222 round-trip min/avg/max = 34.975/35.324/35.531 ms																		
To hop 8 : IP = 203.75.228.70 round-trip min/avg/max = 35.185/35.550/36.079 ms																		
To hop 9 : IP = 211.22.32.82 round-trip min/avg/max = 34.615/34.824/34.944 ms																		
To hop 10: IP = 220.128.2.86 round-trip min/avg/max = 35.062/35.173/35.370 ms																		
To hop 11: IP = 220.128.2.117 round-trip min/avg/max = 35.004/35.146/35.381 ms																		
To hop 12: IP = 211.22.35.37 round-trip min/avg/max = 35.007/35.406/35.686 ms																		
To hop 13: IP = 203.66.88.89 round-trip min/avg/max = 34.959/35.457/35.924 ms																		
Traceroute complete																		

Traceroute results



## **12.5 Wake on Lan**

# **Wake on Lan**

The MIS engineer can use the CS-2000 appliance to start up the internal PCs ( by sending packets) which included the network bootable network adapter and can additionally use the remote monitor software such as VNC, Terminal Service and PC Anywhere.

In this chapter, we will make the introduction of Wake on Lan.

## Example 1

### Remote monitor the internal PC

**Step1.** The internal PC to be remote monitored, and its MAC is 00:30:4F:25:96:3B.

**Step2.** In **Wake on Lan → Setting**, add the following settings :

- Click **New Entry**.
- **Name**, enter alex.
- **MAC Address**, enter 00:30:4F:25:96:3B
- Click **OK**.

Add Wake on Lan setting						
Name	alex (Max. 20 characters)					<a href="#">Assist</a>
MAC Address	00	: 30	: 4F	: 25	: 96	: 3B

**Set the internal PC to be monitored**

**Step3.** Click **Wake Up**, to start up the internal PC.

Name	MAC Address	Configure
alex	00:30:4F:25:96:3B	<input type="button" value="Wake Up"/> <input type="button" value="Modify"/> <input type="button" value="Remove"/>

**Start up the PC**

## 12.6 Status

# Status

MIS engineer can easily know the status of network connection anytime. For example, the information of area network and WAN interface IP address, netmask, default gateway, DNS server IP address etc.

1. **Interface** : It shows the all the interface status in CS-2000.
2. **System Info** : It shows the CPU utilization, memory utilization and Ramdisk utilization.
3. **Authentication** : It records the authentication information in CS-2000.
4. **ARP Table** : It records all the ARP information in host PC which connected to the CS-2000.
5. **Sessions Info** : It records all the session packets pass through CS-2000.
6. **DHCP Clients** : It records the IP address status distributed by the DHCP server in CS-2000.












### 12.6.1 Interface

**Step1**     **Status → Interface**, it shows all the interface information in CS-2000.

- **System Uptime** : The operating uptime of CS-2000.
- **Active Sessions Number** : It shows the real sessions pass through CS-2000.
- **MAC Address** : The MAC address of interface.
- **IP Address/Netmask** : The IP address and netmask of interface.
- **Rx Pkts , Err.Pkts** : It shows the received packets and error packets of interface.
- **Tx Pkts , Err.Pkts** : It shows the transferred packets and error packets.
- **Ping , HTTP , HTTPS** : It shows if the user can ping the CS-2000 interface, or enter the Web UI through HTTP and HTTPS.
- **Forwarding Mode** : It shows the interface connection mode.
- **WAN Connection** : It shows the WAN interface connection status.
- **DnS / UpS kbps** : It shows the maximum downstream / upstream bandwidth in WAN. ( MIS engineer can set the max downstream / upstream bandwidth in **Interface**)
- **DnStream Alloca.** : The CS-2000 can allocate the downstream percentage depends on the WAN interface network flow.
- **UpStream Alloca.** : The CS-2000 can allocate the upstream percentage depends on the WAN interface network flow.
- **PPPoE Con.Time** : When using the PPPoE connection, it will show the connection uptime.
- **Default Gateway** : It shows the WAN gateway address.
- **DNS 1** : It means the DNS 1 server IP address applied from the ISP.
- **DNS 2** : It means the DNS 2 server IP address applied from the ISP.

Active Sessions Number : 71

System Uptime : 0 Day 21 Hour 58 Min 14 Sec

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Dynamic IP	Static IP	---
WAN Connection	---			---
DnS / UpS Kbps	---	2048 / 256	1024 / 1024	---
DnStream Alloca.	---	45%	54%	---
UpStream Alloca.	---	47%	52%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:30:4f:0a:eb:30	00:30:4f:0a:eb:31	00:30:4f:0a:eb:32	00:30:4f:0a:eb:33
IP Address	192.168.1.1	203.67.31.11	210.66.155.77	0.0.0.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.224	0.0.0.0
Default Gateway	---	203.67.31.1	210.66.155.94	---
DNS1	---	168.95.1.1	168.95.1.1	---
DNS2	---	168.95.1.1	168.95.1.1	---
Rx Pkts, Err. Pkts	50725, 0	132792, 0	152882, 0	0, 0
Tx Pkts, Err. Pkts	20400, 0	262396, 0	215056, 0	0, 0
Ping				---
HTTP				---
HTTPS				---

The interface information

## 12.6.2 System Info

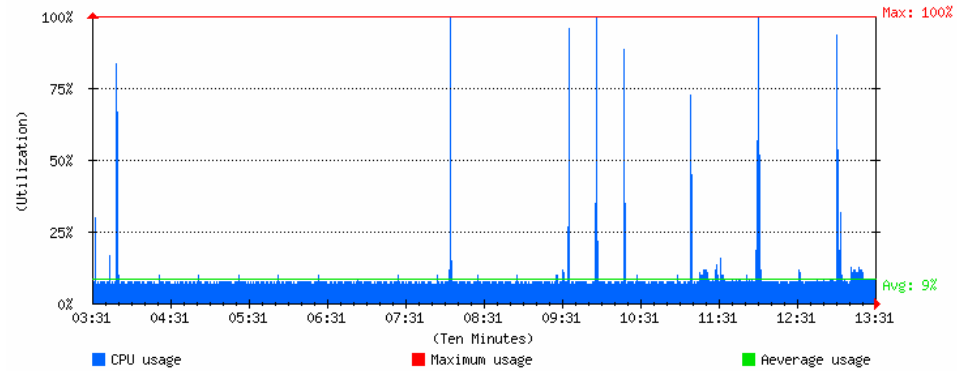
**Step1**     **Status → System Info**, it shows the real system information.

- CPU Utilization : The CPU utilization in CS-2000.
- HardDisk Utilization : The hard disk utilization in CS-2000.
- Memory Utilization : The memory utilization in CS-2000.
- RamDisk Utilization : The ram disk utilization in CS-2000.

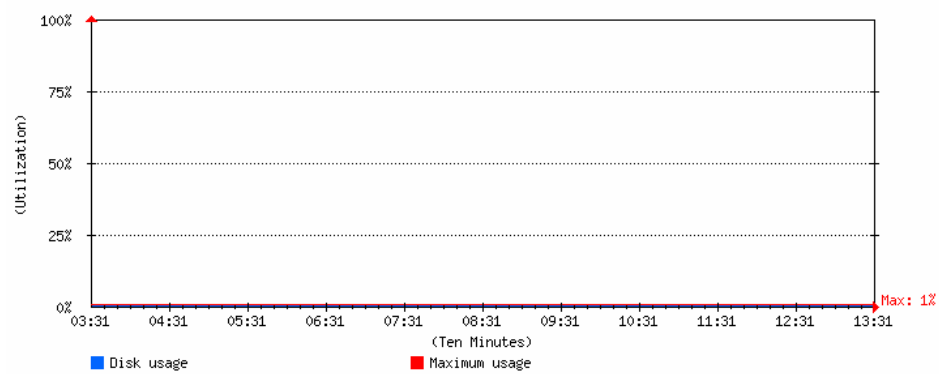
Memory Size: 512 MB

Hard Disk Status: ok

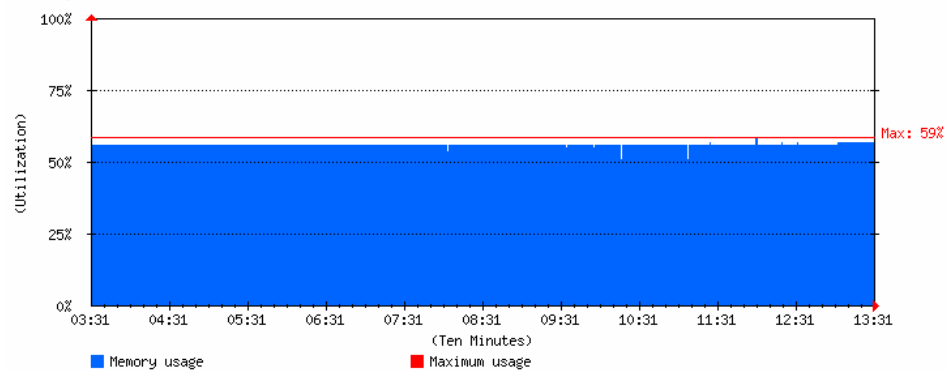
#### CPU Utilization



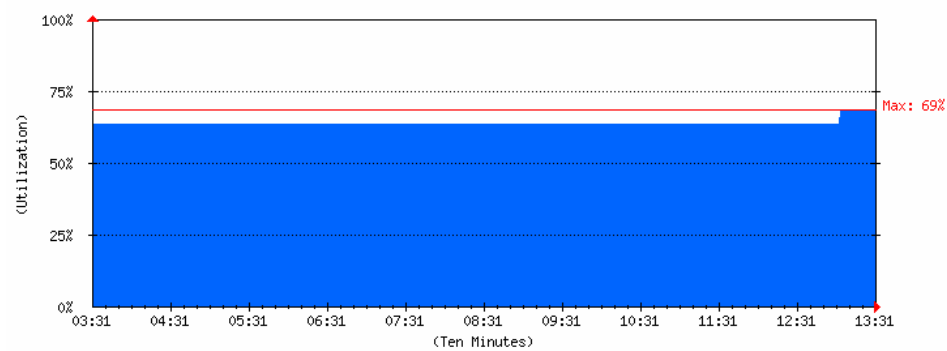
#### Hard Disk Utilization



#### Memory Utilization



#### RAM Disk Utilization



### The system information

### 12.6.3 Authentication

**Step1**    **Status → Authentication**, it shows the authentication information in CS-2000.

- **IP Address** : It represents the authenticated user IP address.
- **Authentication – User Name** : It represents the authenticated login name used by authentication user.
- **Login Time** : It represents the user's login time (year / month / day / hour / minute / second.)

IP Address	Authentication-User Name	Login Time	Configure
192.168.1.2	alex	2007/7/5 13:35:19	<a href="#">Remove</a>

The authentication status Web UI



Click **Remove**, to delete the policy authenticated by CS-2000.



## 12.6.4 ARP Table

**Step1**    **Status → ARP Table**, it shows the information of Net BIOS name, IP address, MAC address and interface.

- **Net BIOS Name** : The PC's network identification name.
- **IP Address** : The PC's IP address.
- **MAC Address** : The computer's network adapter identification number.
- **Interface** : The computer's network interface position.

Anti-ARP virus software [Download](#) [Comment](#)

Total MACs : 4

Static <input type="checkbox"/>	NetBIOS Name▼	IP Address▼	MAC Address▼	Interface▼	Configure
<input type="checkbox"/>	----	210.66.155.94	00:A0:C5:11:89:C9	WAN2	<a href="#">Remove</a>
<input type="checkbox"/>	ENM-BRIAN	210.66.155.73	00:E0:18:4E:C9:71	WAN2	<a href="#">Remove</a>
<input type="checkbox"/>	----	203.67.31.1	00:06:4F:60:1E:81	WAN1	<a href="#">Remove</a>
<input type="checkbox"/>	ENM-ALEX	192.168.1.2	00:30:4F:27:60:EF	LAN	<a href="#">Remove</a>

[New Entry](#)

[OK](#)

[Cancel](#)

The ARP Table Web UI

## 12.6.5 Sessions Info

**Step1**     **Status** → **Sessions Info**, and click one of the source IP, then shows the information of sessions packets pass through CS-2000.



Source IP▼	Duration▼	Total Traffic▼	Session Number▼
ENM-ALEX	00:00:41	1.5 MB	179

### The sessions information Web UI

**Step2.**     Click **Source IP**, system shows its flow by the used port to access internet resources.

1 / 9   [Next](#)     Sorting by Start Time: 1 - 20 ▼

Protocol▼	Source IP▼	Destination IP▼	Port▼	Start Time▼	Traffic▼	Policy▼	Configure
ICMP	ENM-ALEX	M89E11-001	Type: 8	13:39:02	1.0 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2433->80	13:38:20	5.6 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2434->80	13:38:20	7.7 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2435->80	13:38:20	13.3 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2424->80	13:38:19	5.3 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.yimg.com	2425->80	13:38:19	5.7 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2426->80	13:38:19	12.6 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2427->80	13:38:19	5.0 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2428->80	13:38:19	6.3 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2429->80	13:38:19	5.5 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2431->80	13:38:19	10.7 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2432->80	13:38:19	9.8 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2417->80	13:38:19	9.8 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2418->80	13:38:19	12.7 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2419->80	13:38:19	2.1 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.yimg.com	2420->80	13:38:19	1.6 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.yimg.com	2421->80	13:38:19	20.3 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.image.shopping.yahoo.com	2422->80	13:38:19	13.1 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.yimg.com	2423->80	13:38:19	2.2 KB		<a href="#">Drop</a>
TCP	ENM-ALEX	tw.yimg.com	2402->80	13:38:18	9.5 KB		<a href="#">Drop</a>

1 / 9   [Next](#)

### System sessions Web UI 2

**Step2** Click **Source IP** or **Destination IP**, it shows the traffic statistics by user's IP , host name or domain name to access the network resources in pop up window.



Protocol	Source IP	Destination IP	Port	Start Time	Traffic	Policy	Configure
ICMP	ENM-ALEX	M89E11-001	Type: 8	13:41:48	1.0 KB		Drop
UDP	ENM-ALEX	69.125.55.183	42777->59339	13:41:37	426.0 B		Drop
UDP	ENM-ALEX	84.250.2.65	42777->1441	13:41:18	300.0 B		Drop
UDP	ENM-ALEX	ENM-BRIAN	42777->63654	13:41:18	450.0 B		Drop
UDP	ENM-ALEX	80.42.66.234	42777->37480	13:41:17	498.0 B		Drop
UDP	ENM-ALEX	18.250.5.162	42777->1399	13:41:17	381.0 B		Drop
UDP	ENM-ALEX	82.237.13.126	42777->37375	13:41:17	510.0 B		Drop
UDP	ENM-ALEX	201.208.136.72	42777->11871	13:41:17	524.0 B		Drop
TCP	ENM-ALEX	79.178.37.104	2368->25688	13:38:13	2.3 KB		Drop

Use the IP address to look up the sessions information



Click **Drop**, can immediately stop specific session send packets.

## Sessions Info

### Search

- To search the record depends on the Policy, No, Source IP, Destination IP and Port in CS-2000.
  - Add the following settings :
    1. **Policy**, select All Policy.
    2. **NO**, select ALL.
    3. Click **Search**.

### Search

Enter keyword or phrase

Policy: All Policy ▼

NO: ALL ▼

Source IP:

Destination IP:

Port:  -->  ( Range: 1 - 65535 )

**Search**

### Results

Search results : 6 records

Protocol▼	Source IP▼	Destination IP▼	Port▼	Start Time▼	Traffic▼	Policy▼	Configure
<b>ICMP</b>	ENM-ALEX	M89E11-001	Type: 8	13:47:01	1.0 KB		<b>Drop</b>
<b>UDP</b>	ENM-ALEX	194.204.104.80	42777->1254	13:45:16	1.6 KB		<b>Drop</b>
<b>UDP</b>	ENM-ALEX	195.216.173.98	42777->47878	13:45:16	1.6 KB		<b>Drop</b>
<b>UDP</b>	ENM-ALEX	60.53.90.7	42777->38174	13:45:16	500.0 B		<b>Drop</b>
<b>UDP</b>	ENM-ALEX	194.158.42.29	42777->62339	13:45:16	500.0 B		<b>Drop</b>
<b>TCP</b>	ENM-ALEX	79.178.37.104	2368->25688	13:38:13	5.5 KB		<b>Drop</b>

Search the specific record

## 12.6.6 DHCP

**Step1**    **Status → DHCP Clients**, it shows the status of IP address distributed by the DHCP server in CS-2000.

- **Net BIOS Name** : The PC's network identification name of IP address distributed by DHCP server.
- **IP Address** : The PC's dynamic IP address distributed by DHCP server.
- **MAC Address** : The computer's dynamic IP address mapped to MAC address.
- **Leased Time** : The effect date in dynamic IP address. (start date / end date) ( year / month / day / hour / minute / second ) .

NetBIOS Name	IP Address	MAC Address	Leased Time	
			Start	End
ENM-ALEX	192.168.1.2	00:30:4f:27:60:ef	2007/7/5 11:32:56	2007/7/5 11:32:56

The DHCP Clients Web UI