PLANET
Networking & Communication

User's Manual

CS-2001

UTM Content Security Gateway

Copyright

Copyright© 2012 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-2001v2

Rev: 1.0 (April, 2012)

PartNo: EM-CS2001v2_v1.0

Table of Contents

Quick Installation Guide **8**
Hardware Installation **9**
Basic System Configuration **1**
S.1 Overview of Functions 9
System **16**
Chapter 1 Administration **17**
1.1 Admin 19
1.2 Permitted IPs 21
1.3 Logout 22
1.4 Updating Software 24
Chapter 2 Configuration **25**
2.1 Settings 35
2.2 Date / Time 40
2.3 Multiple Subnet 41
2.4 Route Table 55
2.5 DHCP 59
2.6 DDNS 64
2.7 Host Table 65
2.8 SNMP 66
2.9 Bulletin Board 68
2.10 Language 72
Interface **73**
Chapter 3 Interface **74**
3.1 Example 84
Policy Object **124**
Chapter 4 Address **125**
4.1 Example 128
Chapter 5 Service **136**
5.1 Example of Pre-defined 138
5.2 Example of Service Group 142
Chapter 6 Schedule **146**
6.1 Example 148
Chapter 7 QoS **150**
7.1 Example 152
Chapter 8 Authentication **156**
8.1 User / Group Authentication 162

8.2 RADIUS Authentication 166
8.3 POP3 Authentication 187
8.4 LDAP Authentication 190
Chapter 9 Application Blocking 204
9.1 Example 207
Chapter 10 Virtual Server 214
10.1 Example 216
Chapter 11 VPN 236
11.1 Example 249
Mail Security 407
Chapter 12 Configuration 408
12.1 Mail Domains 415
12.2 Account Manager 420
12.3 Mail Relay 434
12.4 Mail Notice 440
12.5 Queued Mail 443
12.6 Mail Signatures 445
Chapter 13 Anti-Spam 447
13.1 Example 458
Chapter 14 Anti-Virus 526
14.1 Example 529
Chapter 15 Mail Reports 550
15.1 Statistics 559
15.2 Logs 560
Web Filter 562
Chapter 16 Configuration 563
16.1 Example 570
Chapter 17 Reports 586
17.1 Statistics 591
17.2 Logs 595
IDP 596
Chapter 18 Configuration 597
Chapter 19 Signatures 602
19.1 Example 608
Chapter 20 IDP Report 615
20.1 Statistics 619
20.2 Logs 620
Web VPN / SSL VPN 621

Chapter 21 Web VPN / SSL VPN 622
21.1 Example 626
IM Recording 641
Chapter 22 Configuration 642
22.1 Example 644
Chapter 23 Reports 650
23.1 Statistics 657
23.2 Message History 659
Policy 659
Chapter 24 Policy 660
24.1 Example 666
Anomaly Flow IP 691
Chapter 25 Anomaly Flow IP 692
25.1 Example 693
Advance 697
Chapter 26 Inbound Balancing 698
26.1 Example 709
Chapter 27 High Availability 742
27.1 Example 744
Chapter 28 Co-Defense System 751
28.1 Example 754
Monitoring 759
Chapter 29 Logs 760
29.1 Traffic 768
29.2 Event 772
29.3 Connection 774
29.4 Viruses 776
29.5 Application Blocking 780
29.6 Concurrent Sessions 782
29.7 Quota 785
29.8 Log Backup 788
Chapter 30 Accounting Reports 791
30.1 Flow Analysis 797
30.2 Today's Top Chart 798
30.3 Historical Top Chart 805
Chapter 31 Traffic Grapher 806
31.1 WAN Traffic 808
31.2 Policy-Based Traffic 812

Chapter 32 Diagnostic Tools 816
32.1 Ping 817
32.2 Traceroute 820
32.3 Packet Capture 822
Chapter 33 Wake-On-LAN 823
33.1 Example 824
Chapter 34 Status 825
34.1 Interface 826
34.2 System Info 828
34.3 Authentication 830
34.4 ARP Table 831
34.5 Sessions Info 834
34.6 DHCP Clients 836
34.7 Host Info 837

Quick Installation Guide

Hardware Installation

Front panel:

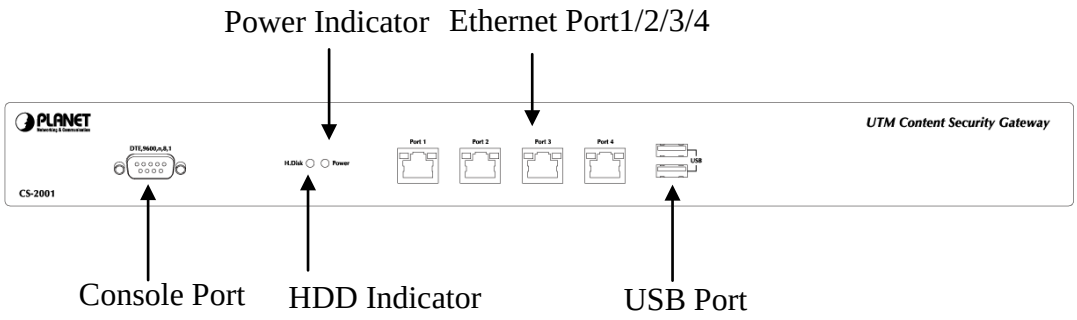


Figure 1a. Front Panel of the CS-2001

Rear panel:

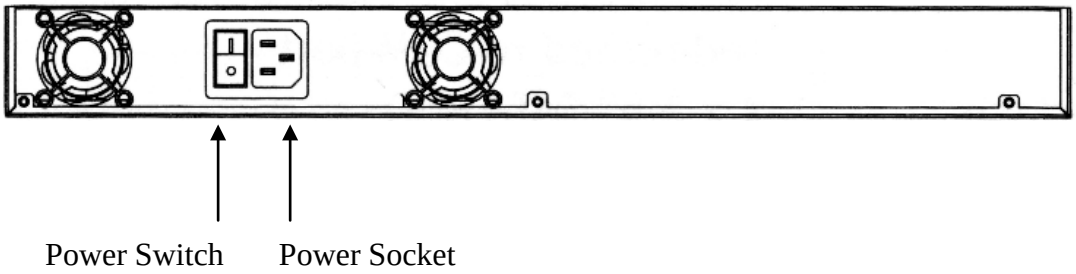


Figure 1b. Rear Panel of the CS-2001

- **Power Indicator:** Lights up when the power is on.
- **HDD Indicator:** Glitters when system is accessing data from the HDD.
- **Console Port (9600, 8, N, 1):** A RS-232 console cable connect this serial port for checking network interface setting and can reset to factory setting.
- **Ethernet Port 1/2/3/4** can be set as a:
  - LAN Port: Connects to the Intranet.
  - WAN Port: Connects to the perimeter router.
  - DMZ Port: The demilitarized zone (DMZ) is a physical subnet for securing the Local Area Network. It allows the externals users to access the company's external network.
  - USB Port: If the firmware damage issue result the device can't boot normally, use the USB device to upgrade (recovery) the firmware in order to make this be normal.

LED / Port	Description		
WAN **LAN** **DMZ**	LED1(Left)	Orange	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port
	LED2(Right)	Orange	Steady on indicates the port is connected at 1000Mbps speed
		Green	Steady on indicates the port is connected at 100Mbps speed
		Off	The LED off to indicate the port is connected at 10Mbps speed

CS-2001 Topology：

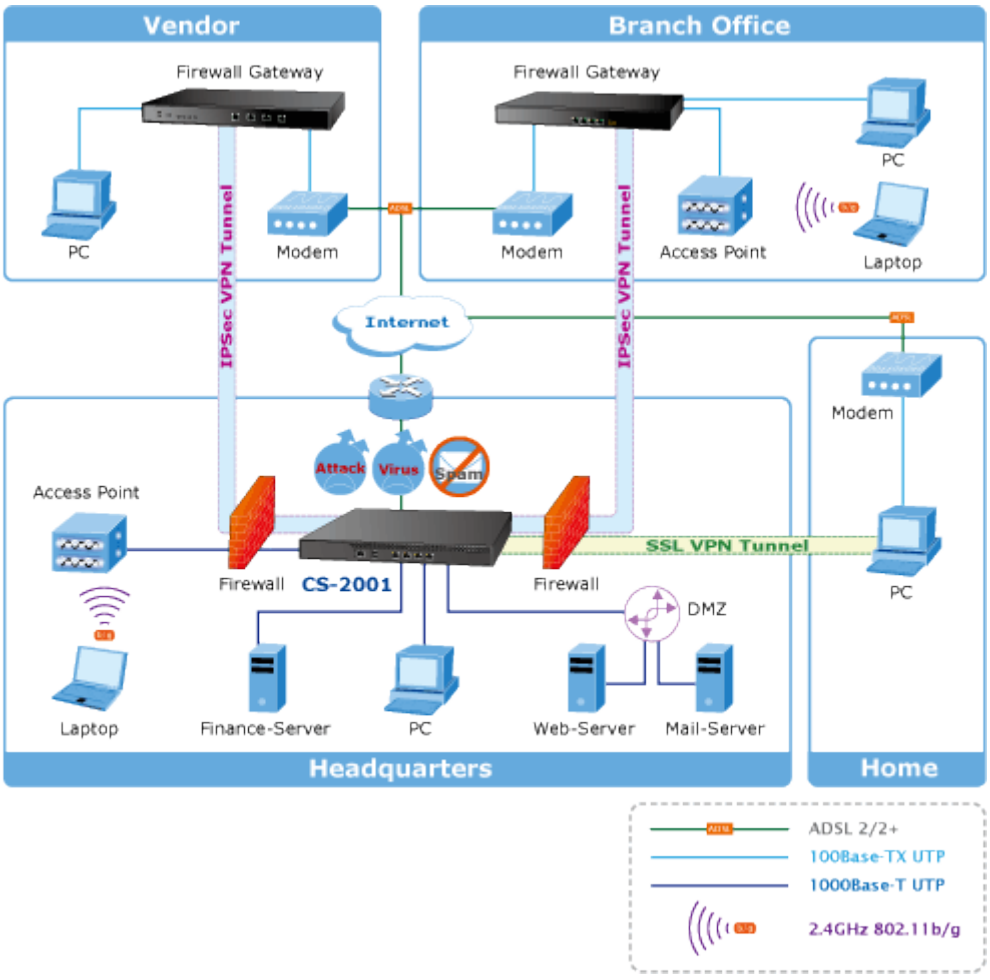


Figure2. Topology of the CS-2001

Basic System Configuration

Step 1. Connect both the IT administrator's PC and the device's LAN port to the same hub / switch, and launch a browser (e.g., IE or Firefox) to access the management interface address which is set to http://192.168.1.1 by default.

Step 2. You will be prompted for user name and password when accessing the management interface. (both of user name and password are "admin" by default)

Figure3. Typing the User Name and Password

Step 3. The user interface consists of the following two panels:

- Menu Panel: Presents all the available system configurations in a tree directory structure. (see Overview of Functions)
- Configuration Panel: Displays the data or configurable settings of the corresponding item selected on the Menu Panel.

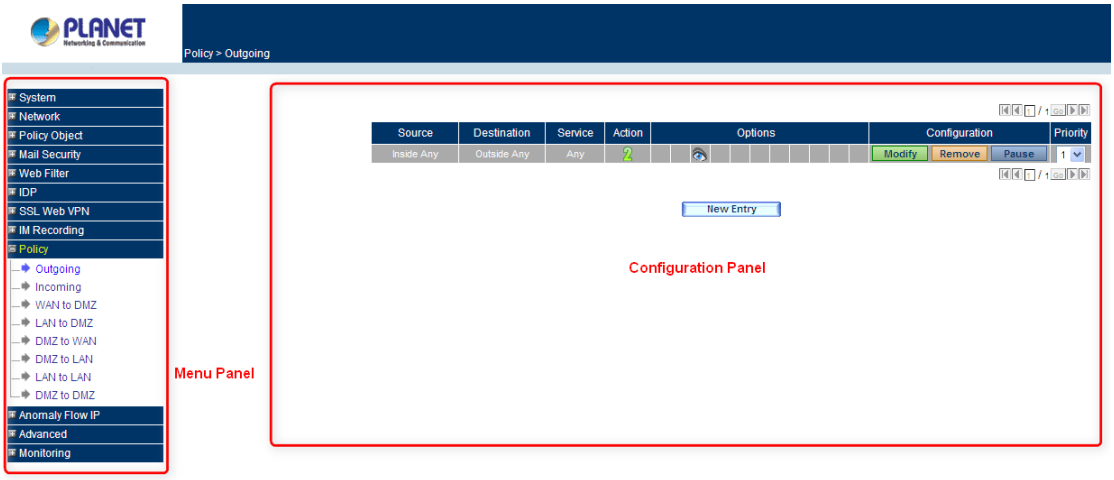


Figure4. The CS-2001 User Interface

Note：

1. For your reference, you may configure your management address based on the available subnet ranges below.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

Step 4. If it's the first time you've logged into the management interface, an install wizard will appear to guide you through setting some of the basic settings required. System > Configuration > Installation Wizard

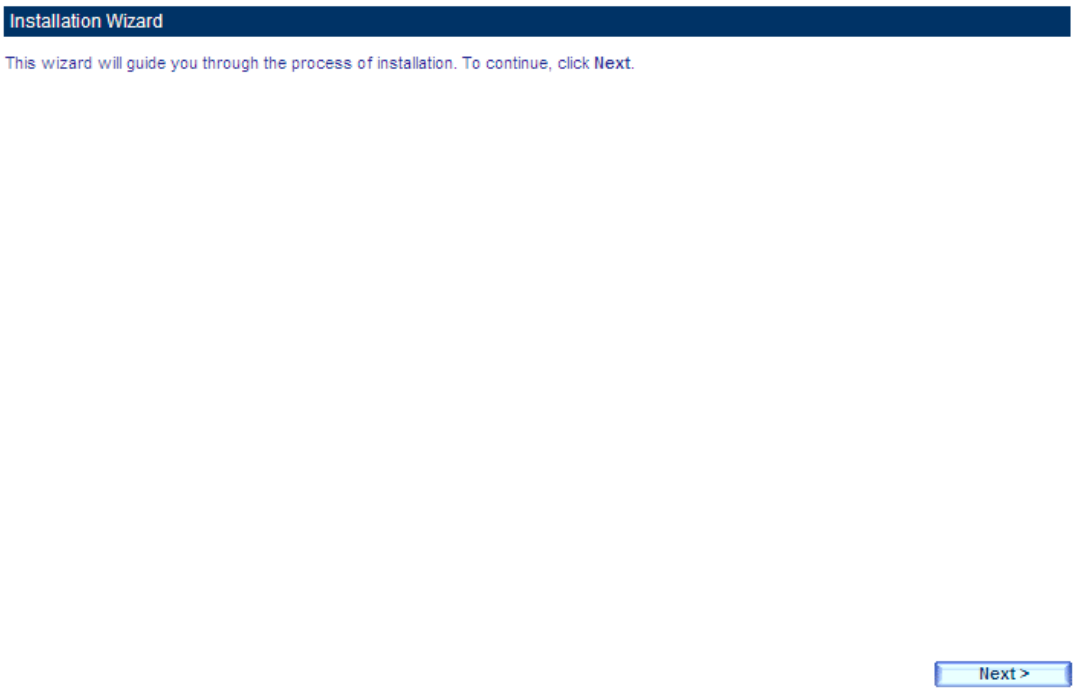


Figure5. The Install Wizard

Step 5. Select the language for the user interface and the default character encoding.

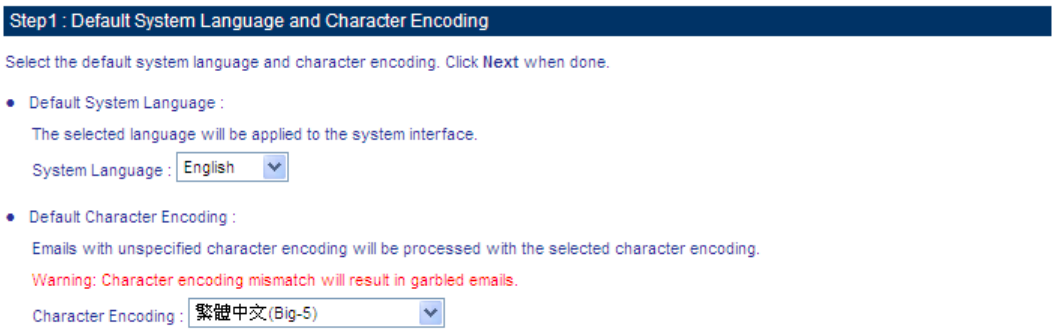


Figure6. Selecting the Language and Default Character Encoding

Important：

1. Any data saved on the interface will be saved as the selected default character encoding if the device is unable to recognize the encoding.

Step 6. The LAN interface address must reflect your network environment. The defualt LAN interface is set to 192.168.1.x/24. However, if the LAN interface was changed to 172.16.0.1 (subnet mask: 255.255.255.0), the IT administrator must configure each PC in the subnet using an available IP address from this subnet.

- **Setting**: Select Port1 (LAN1).
- **Interface**: Select LAN.
- **LAN Interface Mode**: Select NAT / Routing Mode.
- Fill in the **IP Address** and **Netmask** fields.

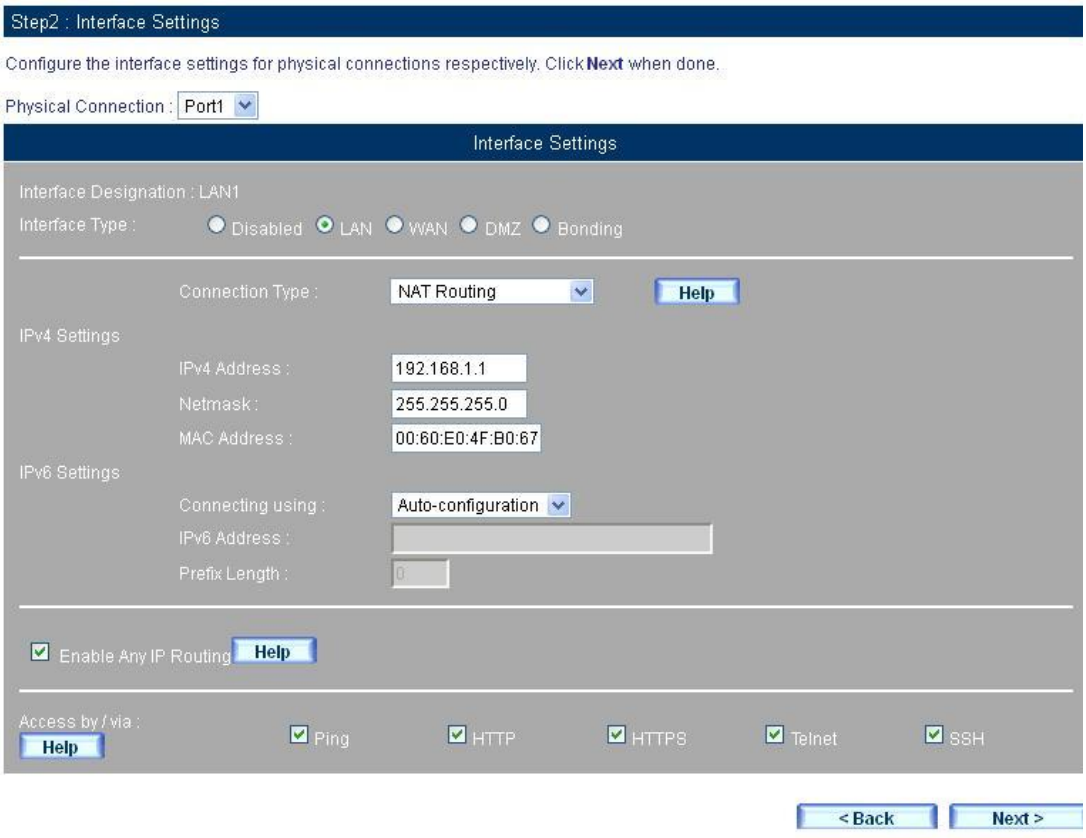


Figure7. Interface Settings

Important :

1. Note: Once the LAN interface is changed, please enter the new LAN IP address in the browser next time when you log in the CS-2001 Web UI.

Step 7. Configure theWAN Interface (please refer to your ISP for the settings).

- **Setting**: Select Port2(WAN1)
- **Interface**: Select WAN
- **Connection Mode:** Select the required mode
- Configure the remaining settings.

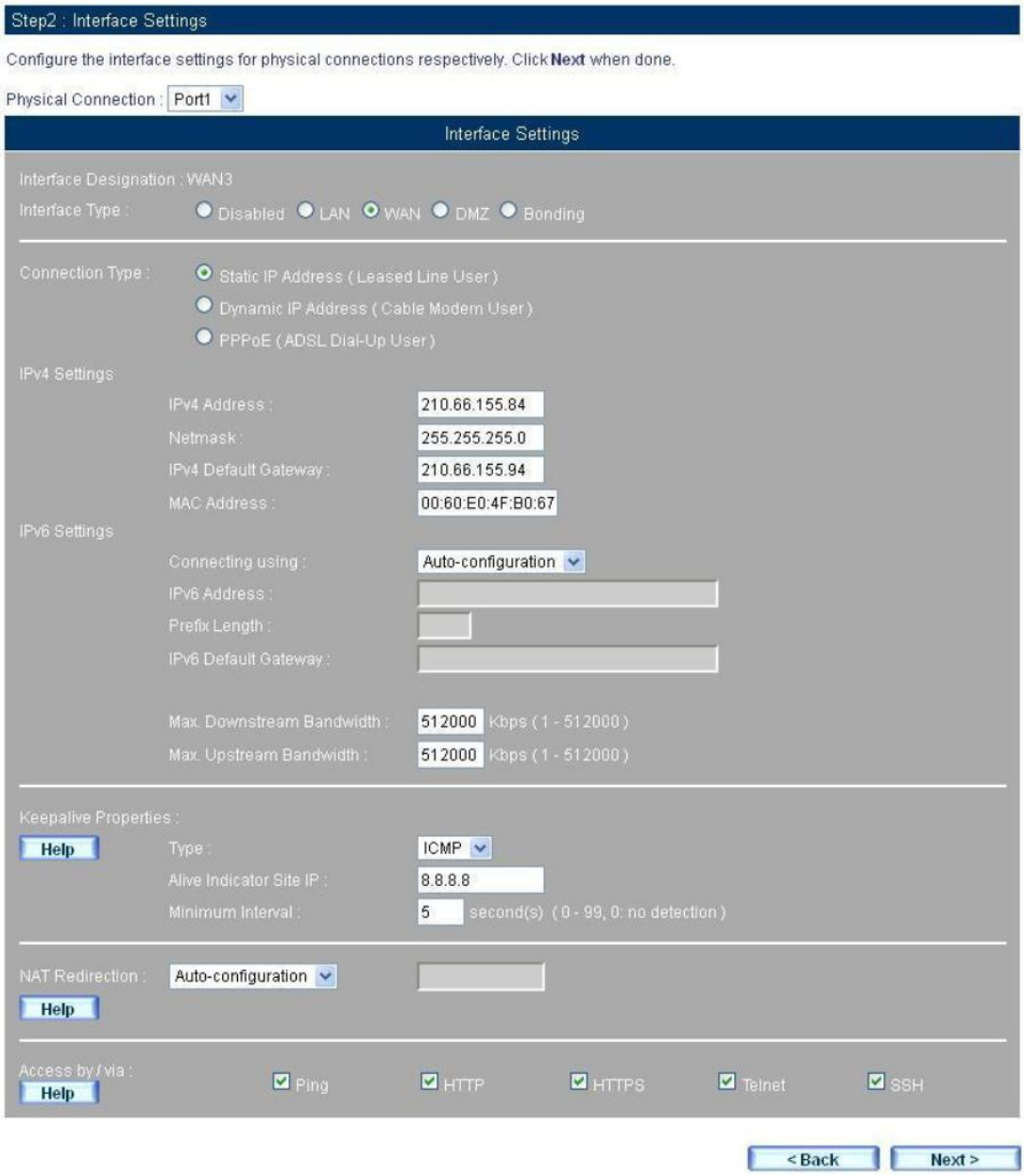


Figure8. The WAN Settings

Step 8. Tick the **Synchronize to an NTP Server** box to ensure the system is provided with the accurate time.

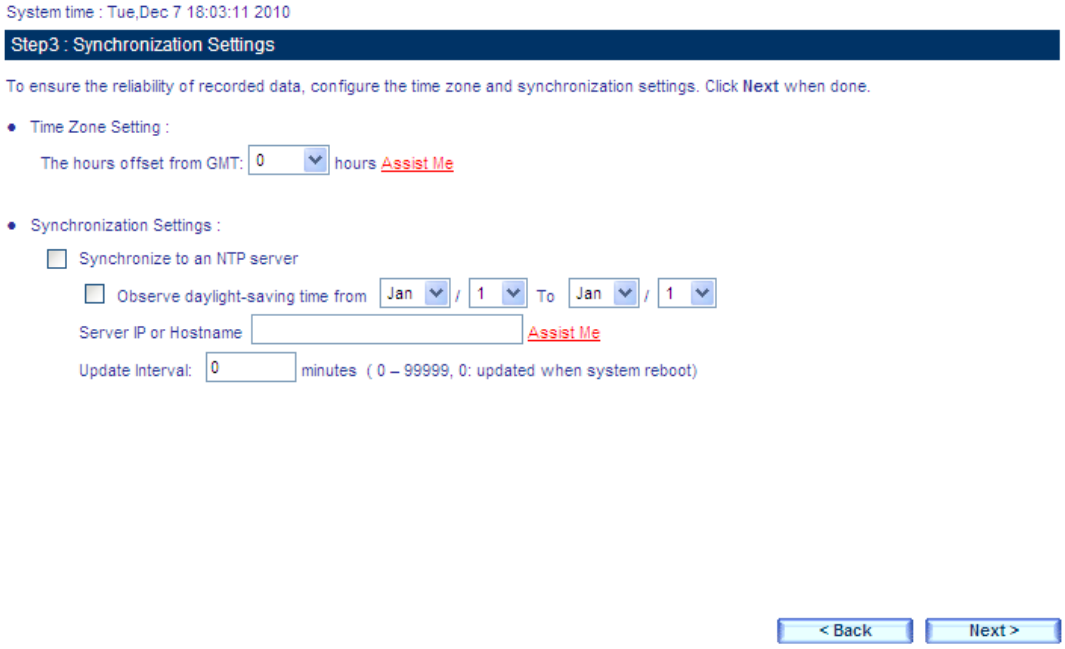


Figure9. Time Settings

Step 9. Enable **Outgoing**.

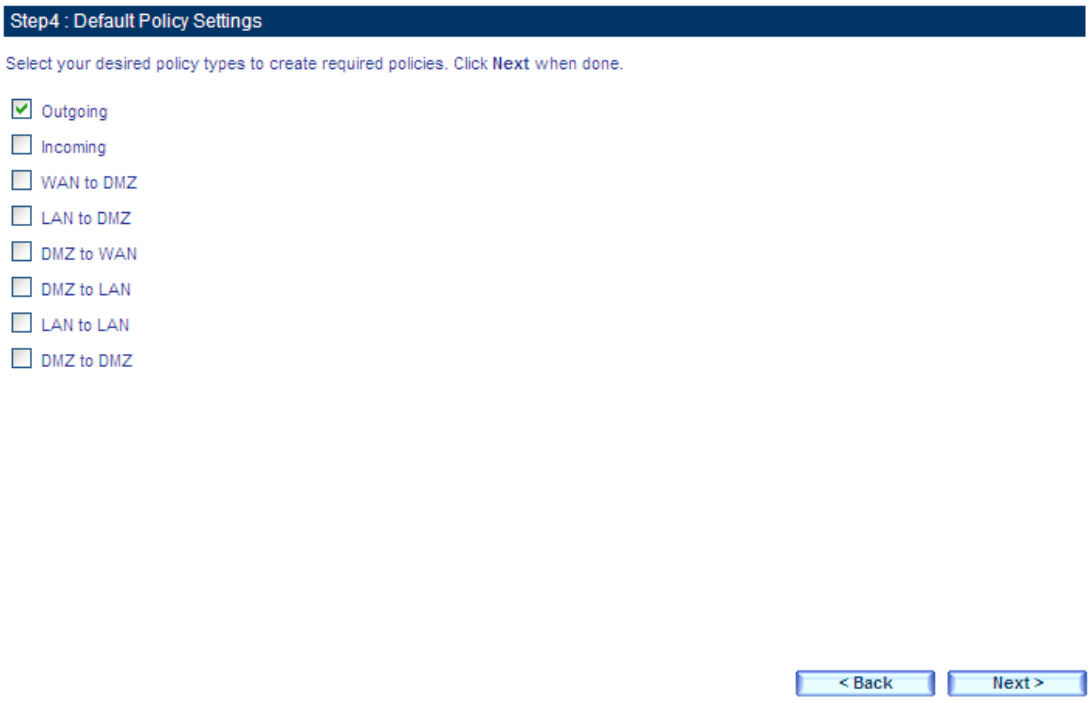


Figure10. Enabling an Outgoing Policy

Note：

1. Go to **Policy > Outgoing** and configure as below:
   - **Source Address:** Select Inside_Any
   - **Destination Address:** Select Outside_Any
   - **Service**: Select ANY

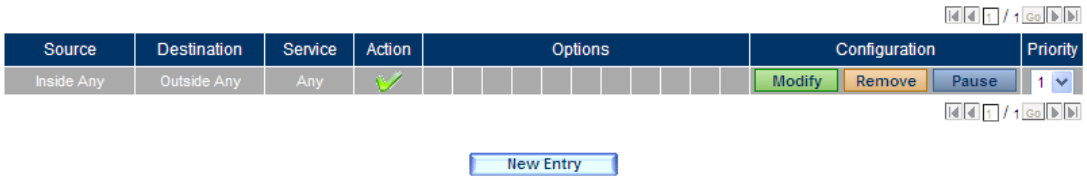


Figure11. A Policy Allowing LAN Users to Access Any External Network Services

2. Finally, configure all LAN PC addresses within the same domain as the LAN interface address, which is also the default gateway address for the LAN. Or, simply by using the DHCP to enable LAN PCs to obtain IP addresses, users may have Internet access right after configuring DHCP. To configure any network policies, please go to **Policy Object** and **Policy.**

Step 10. Provide the following CS-2001 interface information to LAN users.

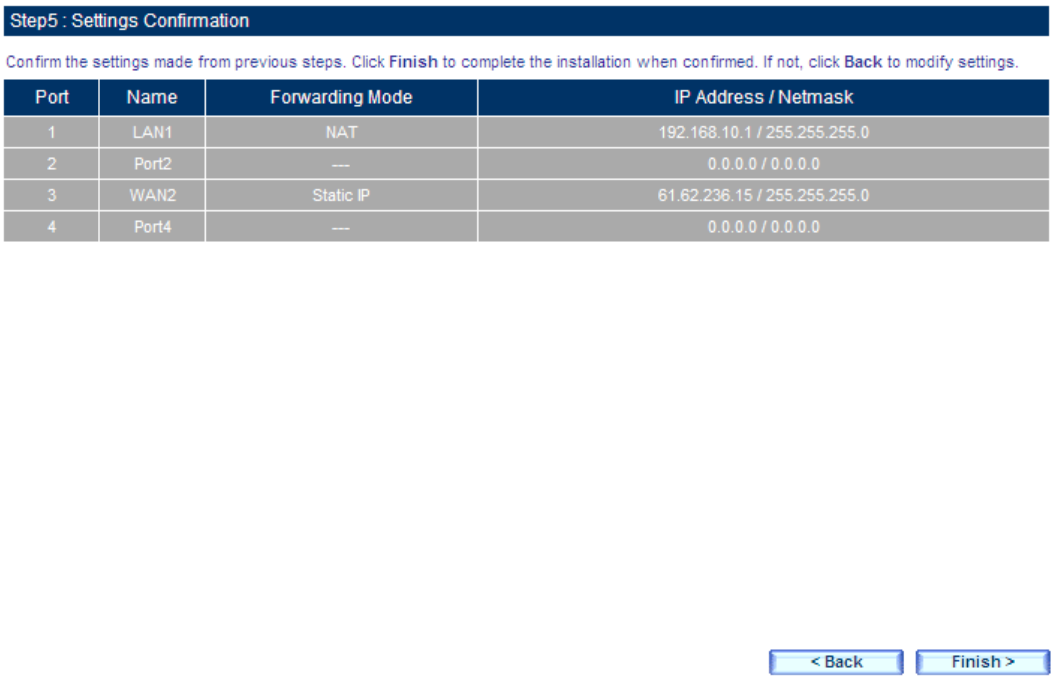


Figure12. Settings Confirmation

Step 11. Settings complete.

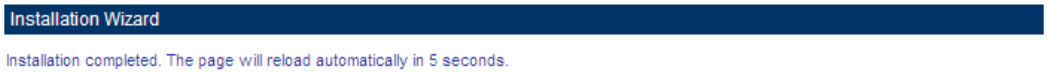


Figure13. Installation Wizard Completed

S.1 Overview of Functions

Category	Configurable Settings		Description	Index
System	Administration	Admin	Creates, modifies or removes administrator accounts.	Chapter 1
		Permitted IPs	Permits specific IP addresses to access the system.	
		Software Update	Update the system's software version.	
	Configuration	Settings	For importing or exporting the system settings, resetting the system to factory default settings, formatting the hard disk, enabling email alert notifications, configuring the Syslog settings, configuring the Web management port, configuring the Proxy settings, configuring the max. number of items shown per page, etc.	Chapter 2
		Date/ Time	Synchronizes the time between the system and the device.	
		Multiple Subnets	For Adding the multiple subnets to facilitate the internal network's distribution.	
		Routing Table	Assigns a gateway for packets going to specific destination addresses.	
		DHCP	Allocates IPs to LAN PCs.	
		Dynamic DNS	Maps a dynamic IP to specific domain name.	
		Host Table	Maps LAN IPs to customizable names to facilitate management.	
		SNMP	Captures real time information of the system.	
		Bulletin Board	Announces the information to	

			LAN and DMZ users.	
		Installation Wizard	For quick installation and configuration.	
		Language	Available languages include Traditional Chinese, Simplified Chinese and English.	
Network	Settings		For DNS settings, link speed / duplex settings, etc.	Chapter 3
	Interface		For configuring the interface type: LAN (IP address, netmask, MAC address, etc.), WAN (connection type, downstream / upstream bandwidth, etc.), DMZ (IP address, netmask, MAC address, etc.)	
	Interface Group		Grouping the ports into individual network interface.	
Policy Object	Address	LAN	Groups LAN IPs, WAN IPs and DMZ IPs.	Chapter 4
		LAN Group		
		WAN		
		WAN Group		
		DMZ		
		DMZ Group		
	Service	Predefined	Defines and classifies services.	Chapter 5
		Custom		
		Group		
	Schedule	Settings	Schedules the network’s usage.	Chapter 6
	QoS	Settings	Allocates downstream / upstream bandwidth for each WAN.	Chapter 7
	Authentication	Settings	Authenticates internal users using RADIUS, POP3 or LDAP or local authentication.	Chapter 8
		Account		
		Group		
		RADIUS		
		POP3		
		LDAP		
	Application Blocking	Settings	Blocks instant messenger login, file transfer over IM, peer-to-peer sharing, multimedia streaming,	Chapter 9

			Web-based mail, online gaming, VPN Tunneling, and remote controlling.	
	Virtual Server	Mapped IPs	Maps an internal host to an external IP address to provide a specific connection or service, such as PC-Anywhere, FTP, HTTP, etc.	Chapter 10
		Port Mapping		
		Port-Mapping Group		
	VPN	One-Step IPSec	For establishing secure and private connections, there are two connection methods, namely IPSec VPN and PPTP VPN. IPSec VPN is suitable for site-to-site connections; PPTP VPN is suitable for the connection between a site and a specific VPN client.	Chapter 11
		VPN Wizard		
		IPSec Autokey		
		PPTP Server		
		PPTP Client		
		Trunk		
		Trunk Group		
Mail Security	Configuration	Settings	Configures the max. virus / spam mail scanning size, tags for unscanned mail, IP address or domain name for Web mail notice, storage time of quarantined logs, etc.	Chapter 12
		Mail Domains	Filtering emails from different domain names and identifying the direction.	
		Account Manager	Manages the user accounts and enables them to access the Mail Archive viewer.	
		Mail Relay	Sends the scanned emails to the designated server based on the domain or IP address.	
		Mail Notice	For notifying the recipient of any spam or virus-laden emails.	
		Queued Mail	Displays the queued mail.	
		Mail Signatures	Configures the messages to be added in the scanned mail.	
	Anti-Spam	Settings	For filtering the spam mail. The	Chapter 13

		Personal Rule Global Rule Whitelist Blacklist Training	spam filtering is applied in the following order: Greylist Filtering > Personal Rule, Global Rule > Whitelist > Blacklist > Fingerprint > Bayesian Filtering > Spam Signature...	
	Anti-Virus	Settings	Scans for virus-infected mail using ClamAV and Sophos.	Chapter 14
	Mail Reports	Settings Statistics Logs	Provides a statistical mail report in the form of bar charts and tables. The report can be emailed to a designated recipient at a specific time. Logs show the handling of mail.	Chapter 15
Web Filter	Configuration	Settings	For configuring the web filter license, alert messages, storage lifetime of logs and max. file scanning size.	Chapter 16
		Whitelist Blacklist Category File Extensions MIME/Script Group	Blocks internal users from accessing specific URLs via HTTP, MIME / Script and blocks the transferring of specific file extension via FTP or HTTP.	
	Reports	Settings Statistics Logs	Provides the statistics in the form of logs and charts. The statistics can be sent to the designated recipient periodically.	Chapter 17
IDP	Configuration	Settings	Updating the signature definitions, enabling virus scanning, NetBIOS alert and syslog and configuring the action and process for each risk level.	Chapter 18
	Signatures	Anomaly Pre-defined Custom	Filters out any potential threats by three types of signatures, namely Anomaly, Pre-defined and Custom.	Chapter 19

	IDP Reports	Settings	Provides statistics in the form of graphs and logs. Statistics can be sent to the specific recipient periodically and logs can be searched based on the specified criteria.	Chapter 20
		Statistics		
		Logs		
SSL Web VPN	Settings		For configuring the VPN IP range, the protocol and the encryption algorithm.	Chapter 21
	Hardware Authentication		Provides hardware authentication based on the user's hardware to facilitate establishing Web VPN connection.	
	Status		Displays the status of Web VPN connection.	
IM Recording	Configuration	Settings	Records and monitors the use of QQ messenger.	Chapter 22
	Reports	Settings	Shows the statistics of the sent message and transferred file. Provides the statistics in the form of logs and charts. The statistics can be sent to the designated recipient periodically.	Chapter 23
		Statistics		
		Message History		
Policy	Outgoing		Manages the LAN, WAN and DMZ by configuring the source address, destination address, service, schedule, authentication, virtual server, VPN trunk, Web filter, application blocking, etc.	Chapter 24
	Incoming			
	WAN to DMZ			
	LAN to DMZ			
	DMZ to WAN			
	DMZ to LAN			
	LAN to LAN			
	DMZ to DMZ			
Anomaly Flow IP	Settings		Configuring the traffic threshold per IP, enabling the anomaly flow IP blocking, e-mail alert notification, core switch port blocking, anomaly traffic user warning message, detection-excluded IP, etc.	Chapter 25

	Virus-infected IP		Displays a list of IP addresses detected as having an anomaly flow.	
Advanced	Inbound Balancing	Settings	For distributing inbound flows to each port by its DNS controlling mechanism. The backup mode provides continuous access if one of the WAN links ceases to function.	Chapter 26
	High Availability	Settings	For installing two CS-2001 devices to ensure an uninterrupted network connection.	Chapter 27
	Co-Defense System	Core Switch	Provides control over anomaly flows by working with the network's core switch. In addition, the IP and MAC addresses over anything connected to each of the switch's ports can be obtained.	Chapter 28
		Edge Switch		
		MAC ADDR Table		
Monitoring	Logs	Settings	Configuring the storage lifetime of logs of traffic, event, connection, virus, application blocking, concurrent sessions, quota and SNMP Trap alert, etc.	Chapter 29
		Traffic	For checking the traffic log.	
		Events	For checking the event log.	
		Connections	For checking the connection log.	
		Viruses	For checking the virus log.	
		Application Blocking	For checking the application blocking log.	
		Concurrent Sessions	For checking the concurrent sessions log.	
		Quota	For checking the quota log.	
	Accounting Reports	Settings	Monitors web site access, service, traffic, etc, statistics of internal and external users.	Chapter 30
		Flow Analysis		
		Today’s Top Chart		

		Historical Top Chart		
	Traffic Grapher	WAN Traffic	Displays the usage statistics from the WAN interfaces.	Chapter 31
		Policy-Based Traffic	Displays the usage statistics of a configured policy.	
	Diagnostic Tools	Ping	Provides Ping, Traceroute and Packet Capture to diagnose the connection.	Chapter 32
		Traceroute		
		Packet Capture		
	Wake-On-LAN	Settings	PC’s in the LAN switched off but connected to a power source can be remotely switched on.	Chapter 33
	Status	Interface	Displays the interfaces’ status and settings.	Chapter 34
		System Info	Displays CPU and hard disk utilization statistics.	
		Authentication	Displays the auth user list.	
		ARP Table	Displays a list of all current IP and MAC addresses that have accessed the network.	
		Sessions Info	Displays outbound sessions established from internal users.	
		DHCP Clients	Displays a list of all current users who have obtained their IP address via DECO.	
		Host Info	Shows the list of NetBIOS and DNS.	

System

Chapter 1 Administration

This chapter mainly explains the authorization settings for accessing the CS-2001. It covers the subjects of *Admin*, *Permitted IPs*, *Software Update* and *Logout.*

The complete administrative authority lies in the hands of the IT administrator. Other than the IT administrator, any other administrator, also known as sub-administrator, is only granted with the permission to monitor the system status.

Terms in Admin

Admin Name

- The authentication name to log in the system.
- The IT administrator's name and password are assigned as *admin* which cannot be deleted.

Access Privilege

- The main IT administrator have the privilege of reading, writing and viewing. That means the main IT administrator is able to view and change the system configuration, logs and accounts.
- The sub-administrator is granted with view and read/ write privileges. They are permitted to view and read system configuration, sometimes, even report and logs.

Password / New Password / Confirm Password

- Add or modify the password of main administrator or sub-administrator.

1.1 Admin

1.1.1 Adding a Sub-Administrator

Step 1. Go to **System** > **Administration** > **Admin**, set as below: (**Figure 1-1**)

- Click the **New Sub-Admin** button to create a new sub-administrator.
- Enter the **Sub-Admin Name** and **Password**.
- Enter the password again in the **Confirm Password** field.
- Click **OK**.

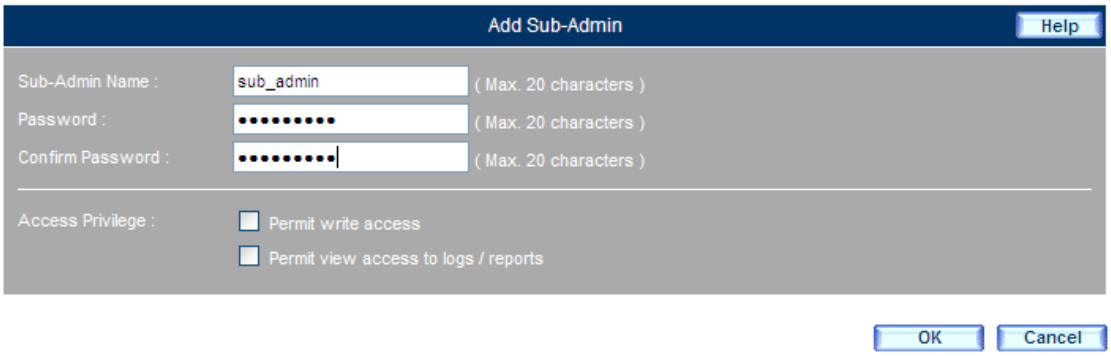


Figure 1-1 Adding New Sub Admin

Note：

1. The newly created administrator will be a main administrator if the **Permit write access** and **Permit view access to logs / reports** have been enabled. Otherwise, they will be a sub-administrator.

1.1.2 Modifying the Password

Step 1. Go to **System** > **Administration** > **Admin** and then set as below: (**Figure 1-2**)

- Click the **Modify** button of the admin you want to modify.
- Enter the original password in the **Password** field and then enter the new password in the **New Password** field.
- Enter the new password again in the **Confirm Password** field.
- Click **OK**.

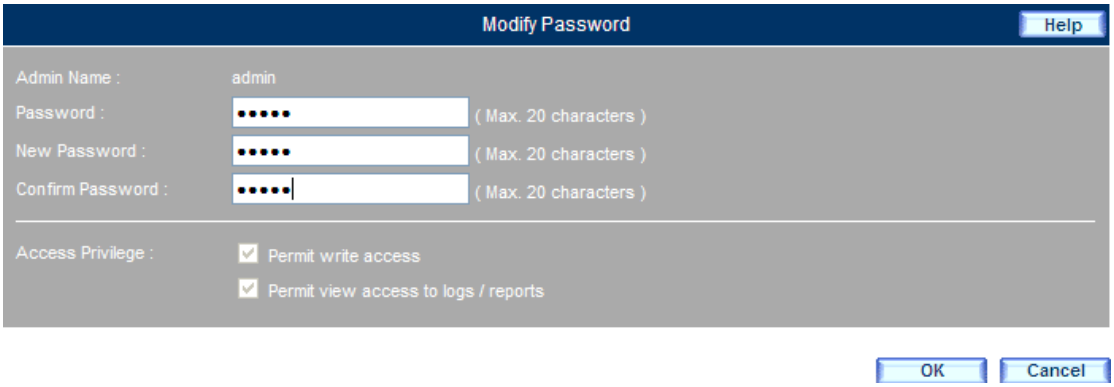


Figure 1-2 Modifying Admin Password

1.2 Permitted IPs

1.2.1 Adding a Permitted IP

Step 1. Under **System** > **Administrator** > **Permitted IPs**, click the **New Entry** button and then set as below: (**Figure 1-3**)

- Enter the name in the **Name** field.
- Select **IPv4** for Protocol.
- Enter the IP address.
- Enter the netmask. (255.255.255.255 indicates one IP Address)
- Select **Ping**, **HTTP** and **HTTPS** for Service.
- Click **OK.**

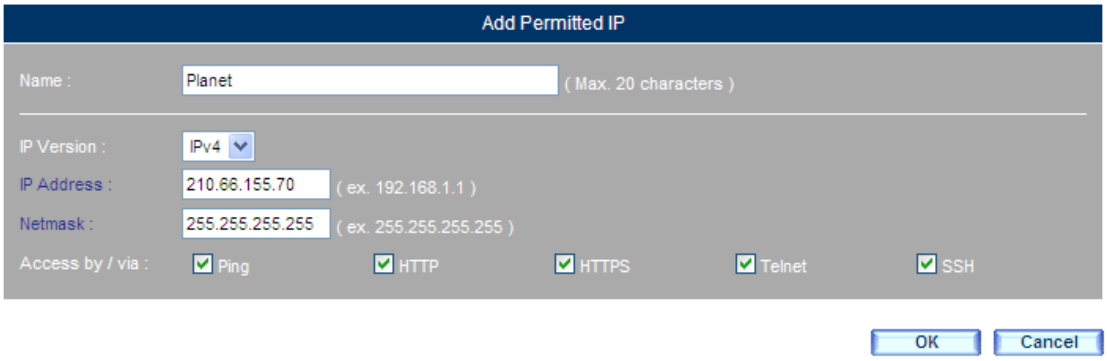


Figure 1-3 Adding New Permitted IPs

Important：

1. For Permitted IPs to be effective, the IT administrator must cancel the **Ping, HTTP, HTTPS, Telnet** and **SSH** selections under **Network** > **Interface**.
2. Configure the Permitted IPs before the cancellation of **HTTP** and **HTTPS**; otherwise, the management interface will be inaccessible.

1.3 Logout

1.3.1 Logging out the System

Step 1. Click **Logout** to protect the system from any unauthorized modification while being away.（**Figure 1-4, 1-5**）

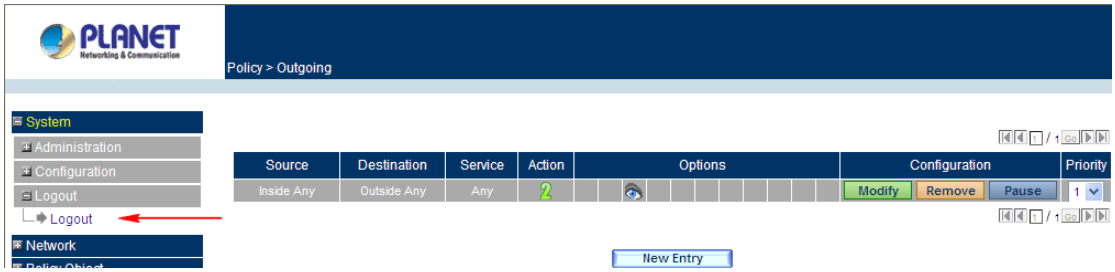


Figure 1-4 The Logout Screen

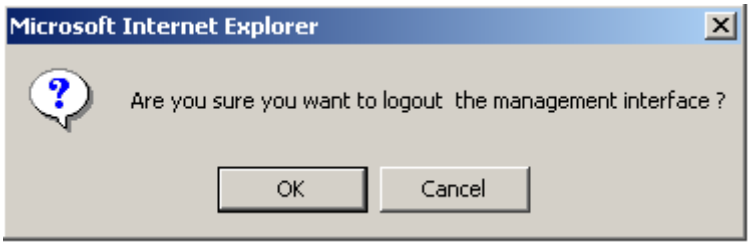


Figure 1-5 Confirming to Log Out

Step 2. Click **OK** and then the logout message appears.（**Figure 1-6**）

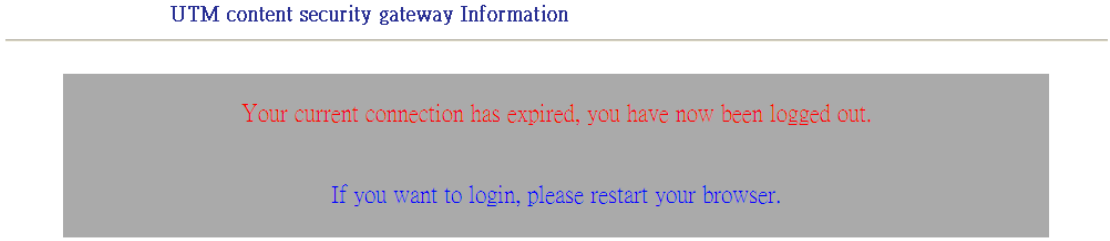


Figure 1-6 The Logout Message

1.4 Updating Software

Step 1. To run a software update, go to **System** > **Administration** > **Software Update** and follow the steps below:

- Click **Browse** to locate the software and then open it.
- Click **OK** to proceed to update the software.（**Figure 1-7**）

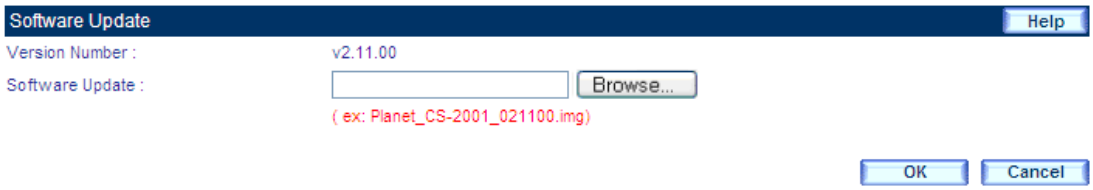


Figure 1-7 Updating the Software

Important：

1. It takes about 3 minutes to run through the update process, and will reboot after the update. During the update, please do not turn off the power, disconnect the Internet or close the management interface due to the possibility of causing system errors. It is strongly recommended to run the update from within the internal network.

Chapter 2 Configuration

Configuration includes the following system settings: System Settings, Date / Time, Multiple Subnets, Route Table, DHCP, Dynamic DNS, Host Table, SNMP and Language.

Terms in Setting

System Settings

- Allows the IT administrator to import / export system settings, perform a factory reset and format the built-in hard disk.

Configuration File Backup and Restore Utility (Used: 40KB, Free: 9MB, Capacity: 10MB)

- Saves a copy of the system settings file to the devices' s internal storage. The IT administrator can restore the system's settings based upon the file's date. This feature is ideal if the system's settings is required to be restored but no saved settings file is available on a local PC.
- The device automatically saves the system setting file daily at 0:00 hours. Alternatively, the IT administrator may choose to perform a manual backup at any time.
- Any of the setting files saved on the device may be exported to a local computer.

Hard Disk Formatting

- The IT administrator may format the built-in hard disk.

Name Settings

- Type your company name and name the device in the corresponding fields.

Email Notification Settings

- Any alerts or notifications from the device can be emailed to the designated recipient.

Syslog Message Settings

- Sends monitoring logs, network logs, IDP logs, etc., to the designated Syslog server.

Management Interface Settings

- Enables the device to be accessed remotely through the management interface using a web browser, from anywhere. The port number for the management interface can be modified.
- A user who has been idle for a period of time (specified in the **Idle Timeout** field) will be automatically logged out of the management interface.
- When a user exceeds the amount of consecutive incorrect login attempts, the

device can block their IP address for the specified amount of time. This helps to prevent any unauthorized tampering of the device.

Important:

1. If the HTTP or HTTPS port number is modified then the number has to to be appended to the management IP address, such as http://61.62.108.172:8080 and http://61.62.108.172:1025, in order to access the management interface from an external network..

Proxy Settings (for signature updates)

- Once the Proxy Server is deployed, the proxy settings must be configured for the CS-2001 to access the Internet.

SIP/ H.323 NAT Traversal Settings

- Enables SIP NAT Traversal or H.323 NAT traversal.

Page Display Configurations

- Configures the maximum number of entries displays per page.
- Configures the default character encoding.

Terms in Date / Time

Synchronization Settings

- The date and time settings can be configured by either synchronizing to an Internet Network Time Server (NTP) or synchronizing to the local computer.

GMT

- Greenwich Mean Time (GMT), is the international standard time.

Daylight Saving Time Setting

- If applicable in your region, the device's system clock can be automatically adjusted to allow for daylight savings time when this function is enabled.

Terms in Multiple Subnet

Name

- Designates a name for the subnet.

IP Version

- Designates the protocol to be used, namely IPv4 or IPv6.

IP Address / Netmask

- Specifies the subnets IP range.

Interface

- Denotes in which network, i.e. LAN or DMZ, the subnet resides.

VLAN ID

- Permits the interface on the CS-2001 to support VLAN tags belonging to the LAN or DMZ.

Terms in Routing Table

Dynamic Routing

- Routers exchange routing information to reflect any changes in the typology of the network. The convergence of routing information between routers depends on the size of the network and the protocol.
  - RIPv2 (Route Information Protocol) sends out RIPv2 packets to nearby routers. If a router that supports RIPv2 receives one of these packets, it will send its routing table back. This provides information to decide the shortest route to reach a destination.
  - Open Shortest Path First (OPSF), gathers link state information from available routers and constructs a topology map of the network. OSPF establishes and maintains neighbor relationships in order to exchange routing updates with other routers. OSPF uses path cost as its basic routing metric.
  - Border Gateway Protocol, is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rulesets. BGP was created to replace the Exterior Gateway Protocol (EGP) routing protocol to allow fully decentralized routing in order to allow the removal of the NSFNet Internet backbone network.
    - A unique ASN is allocated to each AS for use in BGP routing. AS numbers are important because the ASN uniquely identifies each network on the Internet.

Note：

1. Dynamic Routing Protocols can be categoried into the following two categories:
   - Distance-Vector Routing Protocol: Uses the Bellman-Ford algorithm to calculate paths. Examples of distance-vector routing protocols include RIPv1/2 and IGRP (Cisco's proprietary protocol). Using RIP, the maximum hop count from the first router to the destination is 15. Any destination greater than 15 hops away is considered unreachable. A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically and, in some cases, when a change is detected in the topology of a network. Its suitable for networks containing fewer than 100 hops (routers), or small networks that are not changed frequently.
   - Link state routing protocols use the Dijkstra algorthim to calculate the Shortest Path First (SPF) address some of the limitations of distance vector routing protocols. For example, link state routing protocols provide faster convergence than do distance vector routing protocols and have no limit to the amount of hops. VLSM and CIDR are also supported. Although link state routing protocols are more reliable and require less bandwidth than do distance vector routing protocols, they are also more complex, more memory-intensive, and place a greater load on the CPU.
2. Dynamic routing protocols depend on the location of the router in the Autonomous Sytstem (AS). There are two classifications:
   - IGP - Interior Gateway Protocol: Examples include: RIP, IGRP, EIGRP, OSPF and IS-IS are interior gateway protocols.
   - EGP - Exterior Gateway Protocol: Uses a simple tree topology, but posses some shortcomings that the Border Gateway Protocol (BGP) has fixed.
3. Within the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. Multiple organizations can run BGP using private AS numbers to an ISP that connects all those organizations to the Internet. Even though there are multiple Autonomous Systems supported by the ISP, the Internet only sees the routing policy of the ISP. That ISP must have an officially registered Autonomous System Number (ASN). A unique ASN is allocated to each AS for use in BGP routing. AS numbers are important because the ASN uniquely identifies each network on the Internet.
   - Until 2007, AS numbers were defined as 16-bit integers, which allowed for a maximum of 65536 assignments. The Internet Assigned Numbers Authority (IANA) has designated ASN numbers 64512 through 65534 to be used for

private purposes.

- In 2007 30-bit AS numbers were introduced. These numbers are written either as simple integers, or in the form *x.y*, where *x* and *y* are 16-bit numbers. Numbers of the form *0.y* are exactly the old 16-bit AS numbers, *1.y* numbers and 65535.65535 are reserved, and the remainder of the space is available for allocation.

Static Routing

- Provides a static route based on the IT adminisrator's configuration or a default route.
- Provides IPv4 or IPv6.

Terms in DHCP

Static IP Assignment

- DHCP can allocate IP addresses based upon the MAC address of PCs in the LAN or DMZ.

Terms in Dynamic DDNS

Domain Name

- The domain name registered at the DDNS service provider.

Real IP Address

- The real IP address that the domain name corresponds to.

Terms in Host Table

Host Name

- It is a user-definable setting. LAN users may access the host corresponding to the host name.

IP Version

- The network protocol used by the host table, namely IPv4 or IPv6.

IP Address

- The IP addresses that host names correspond to. They either reside in LAN or DMZ.

Terms in SNMP

SNMPv3

- SNMP is a protocol specially designed to monitor network-attached devices such as servers, switches, routers, workstations etc. By utilizing the information supplied by SNMP, IT administrators are able to instantly understand and resolve network issues as well as help with resource utilization and planning.
- A network implementing SNMP consists of three major components: the managed device, the agent (SNMP software that resides in the managed device) and the Network management station (NMS).
- There are currently three versions of SNMP:
  - SNMPv1: lacks encryption and authentication allowing information to be easily intercepted and read.
  - SNMPv2: provides a vast improvement for some of the security concerns associated with SNMPv1. SNMPv2 is not compatible with SNMPv1 and runs at a lower speed and as a result it has not been widely accepted.
  - SNMPv3: resolved the problems associated with the previous two versions. Not only does it provide encryption, but also the agent is able to authenticate the NMS and provide message integrity to ensure that a packet hasn't been tampered with. In addition, it can provide access control based upon a permission list.

Security Mode

- SNMP defines three authentication and privacy levels:
  - Level 1 provides neither privacy nor authentication and is referred to as NoAuthNoPriv. Under this setting, there is neither privacy nor authentication as would be the case when running SNMPv1. This is best suited to networks where there is no need for security.
  - Level 2 provides authentication without privacy and is referred to as AuthNoPriv.
  - Level 3 provides not only authentication for SMTP data but also encryption and is referred to as AuthPriv.

User Name

- The NMS uses this user name to access information from the CS-2001.

Auth Protocol

- Supports the authentication protocols of HMAC_MD5_96 and HMAC_SHA_96.

Auth Password

- The NMS uses this password to access information from the CS-2001.

Privacy Protocol

- Supports the cipher Data Encryption Standard (DES) that is based on a 56-bit Symmetric-key algorithm.

Privacy Password

- The NMS uses this password to access information from the CS-2001.

Terms in Bulletin Board

Bulletin Board Login Settings

- Configures the port number, username and password to log into the management interface.
- Enters the notification message.

Bulletin Board Announcements

- Configures the announcement subject, content, duration and target viewer.

The designated LAN users or DMZ users will see the announcement when they access the Internet.

2.1 Settings

2.1.1 Exporting System Settings

Step 1. Under **System** > **Configuration** > **Settings**, click Export next to **Export System Settings** under the **System Settings** section.

Step 2. Click **Save** in the **File Download** window, and then assign a storage folder. After that, click **Save** in the **Save As** window to complete exporting the system settings.（**Figure 2-1**）

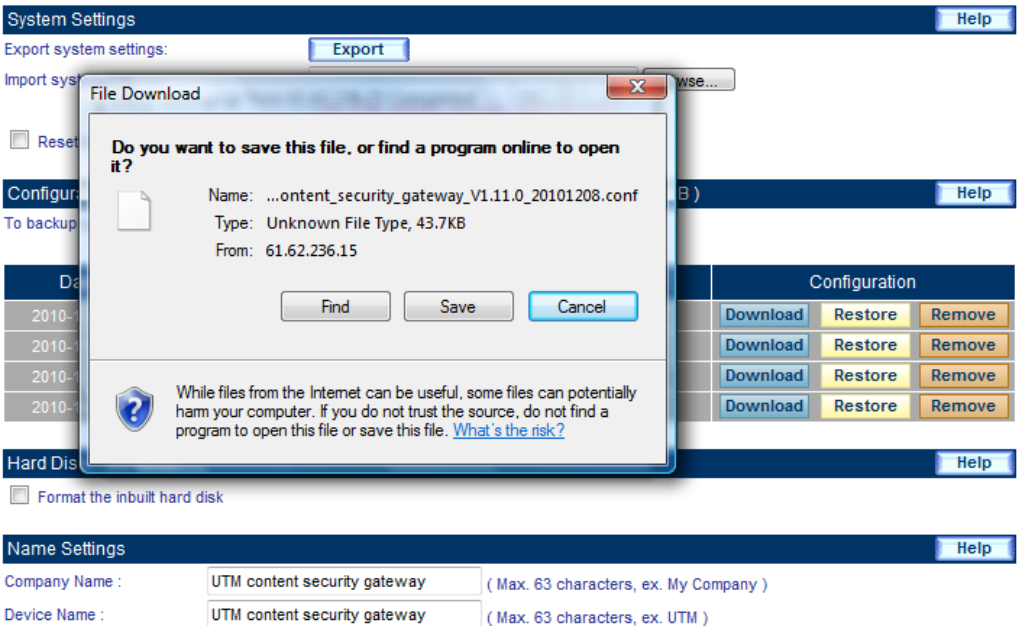


Figure 2-1 Exporting the Configuration File

2.1.2 Importing System Settings

Step 1. Under **System** > **Configuration** > **Settings**, click **Browse…** next to **Import System Settings** under the **System Settings** section. Next, in the **Choose File** window, select the configuration file and then click **Open**.（**Figure 2-2**）

Step 2. Click **OK** to confirm importing the file.（**Figure 2-3**）

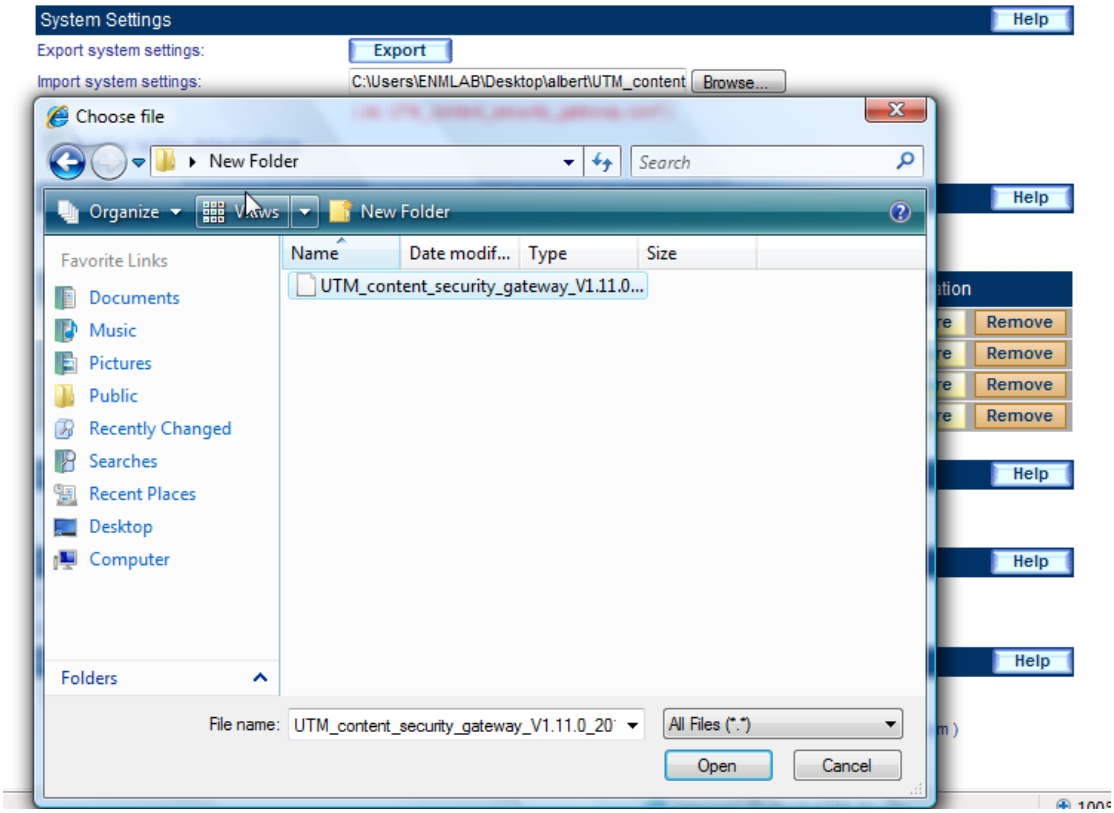


Figure 2-2 Selecting the Configuration File to Import

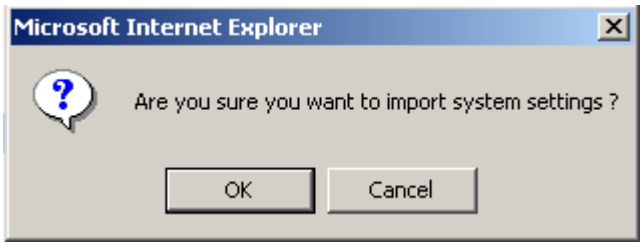


Figure 2-3 Confirming to Import the Configuration File

2.1.3 Resetting the System to Factory Default Settings and Formatting the Hard Drive

Step 1. Under **System** > **Configuration** > **Settings**, tick **Reset to factory default settings** and **Format the inbuilt hard disk** under the **Hard Disk Formatting** section.（**Figure 2-4**）

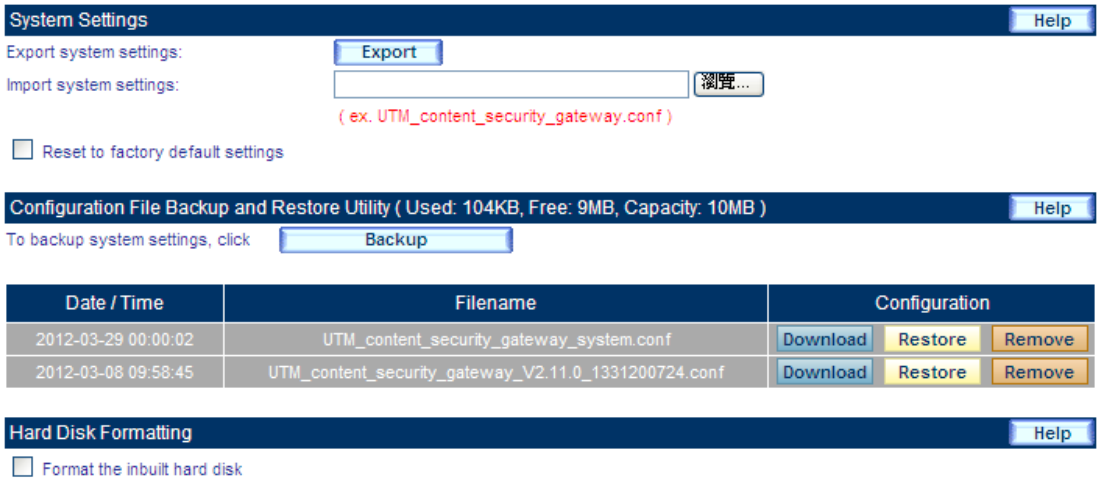


Figure 2-4 Resetting the Device to Factory Default

Step 2. Click **OK** in the lower right corner to execute the procedure.

2.1.4 Enabling Email Alert Notification

Step 1. Go to **System** > **Configuration** > **Settings.** Under the **Name Settings** section, configure the following settings:

- Type your company name in the **Company Name** field.
- Type a name in the **Device Name** field.

Step 2. Under the **Email Notification Settings** section, configure the following settings:

- Tick **Enable email notifications**.
- **Sender Address**: Type the sender address (Required for some ISPs).
- **SMTP Server**: Type the IP address of SMTP server.
- **Email Address 1**: Type the email address of the first user to be notified.
- **Email Address 2**: Type the email address of the second user to be notified.

Step 3. Click **OK** in the lower right corner to complete configuration.（**Figure 2-5**）

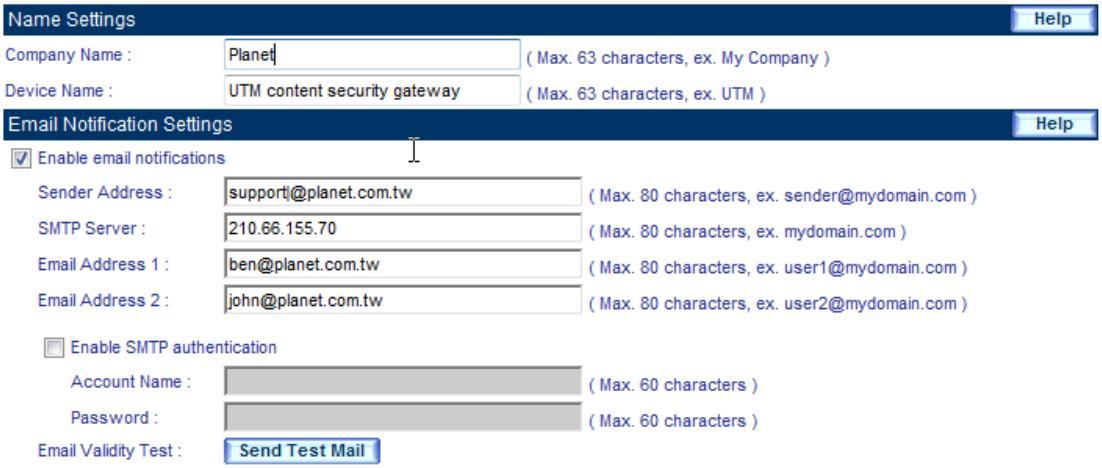


Figure 2-5 Enabling the Email Alert Notification

Note：

1. Click the **Send Now** button to test the validity of email address 1 and 2.
2. To enable SMTP authentication, you may tick **Enable SMTP Authentication** and then configure its related settings accordingly.

2.1.5 Rebooting the CS-2001

Step 1. To reboot the CS-2001, go to **System > Configuration > Settings.** Under the **Device Reboot** section click **Reboot** next to **To reboot the system, click**.

Step 2. A confirmation dialogue box will appear asking “Are you sure you want to reboot the system?

Step 3. Click **OK** to reboot or **Cancel** to cancel.（**Figure 2-6**）

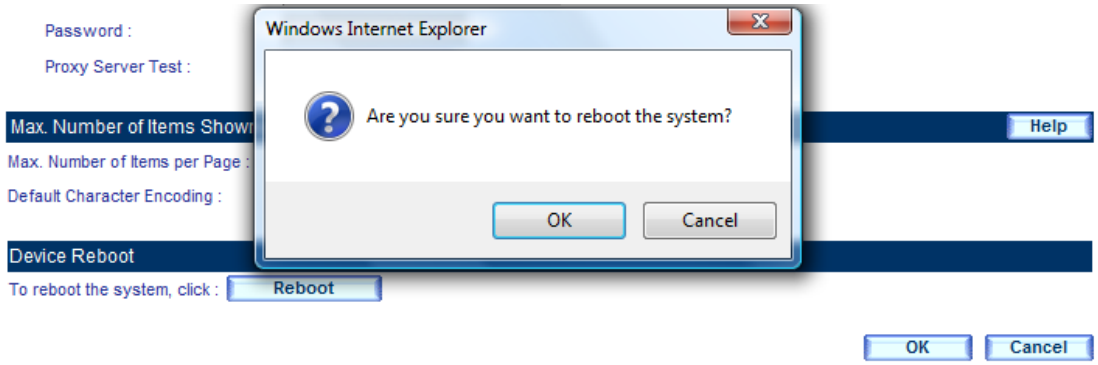


Figure 2-6 Rebooting the CS-2001

2.2 Date / Time

2.2.1 CS-2001 Time Settings

Step 1. Go to **System** > **Configuration** > **Date/Time** and configure the following settings:（**Figure 2-7**）

- Configure the GMT offset hours.
- Tick **Synchronize to an NTP server**.
- Type the IP address of Internet time server in the **NTP Server IP / Hostname** field.
- Set an interval time to update system clock.
- Click **OK**.

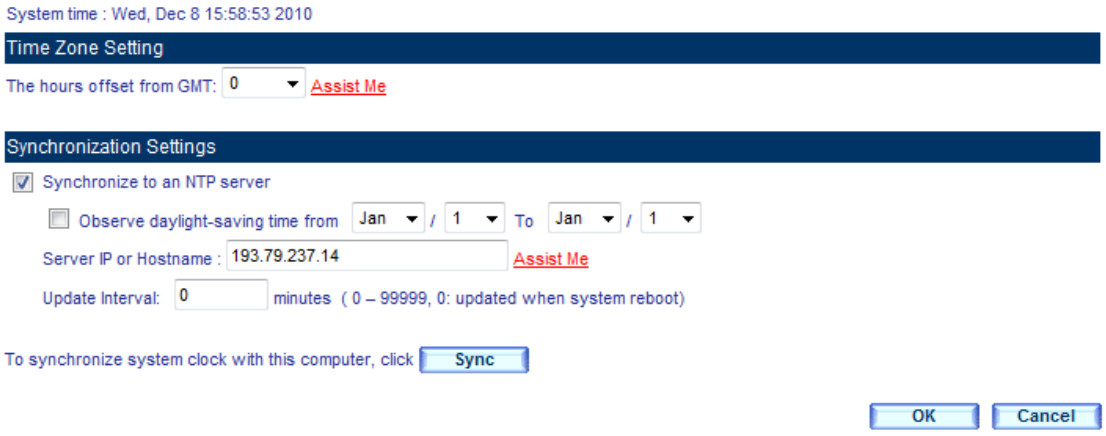


Figure 2-7 The System Clock Settings

Note：

1. Click **Sync** next to **To synchronize system clock with this computer, click** to synchronize the system clock with the time on the IT administrator's PC.
2. **Assist Me** provides help setting **hours offset from GMT** and **NTP Server IP/Name.**

2.3 Multiple Subnet

2.3.1 Using NAT / Routing Mode For LAN Users to Access the Internet

Prerequisite Setup (Note: IP addresses used as examples only)

Configure port 1 as LAN1 (192.168.1.1, NAT routing mode) and connect it to the LAN which is using the IP address range 192.168.1.x/24.
Configure port 2 as WAN1 (10.10.10.1) and connect it to the ISP router (10.10.10.2); the IP address range distributed by the local ISP is 162.172.50.0/24.

Packets traveling to an external network via Port2, which has a private IP address of 10.10.10.1, map to the real IP address 162.172.50.1 using NAT. This allows the signiature definition file to be updated via the Internet.

Configure port 3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Step 1. Under **System** > **Configuration** > **Multiple Subnets**, set as below: (**Figure 2-8**)

- Fill in the **Name** field.
- **Interface:** Select Port1 (LAN1)
- **IP Version:** Select IPv4.
- **IP Address:** Type “162.172.50.1”
- **Netmask**: Type “255.255.255.0”
- Click **OK**. (**Figure 2-9**)

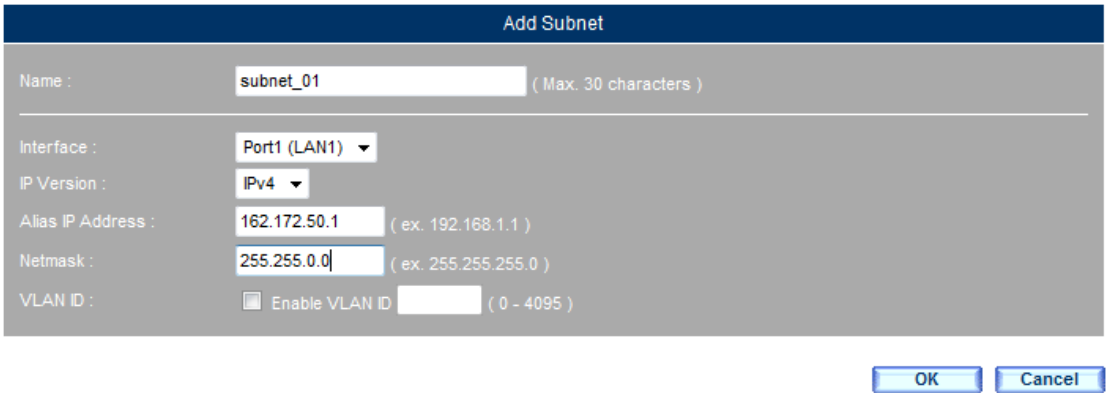


Figure 2-8 Configuring Multiple Subnet

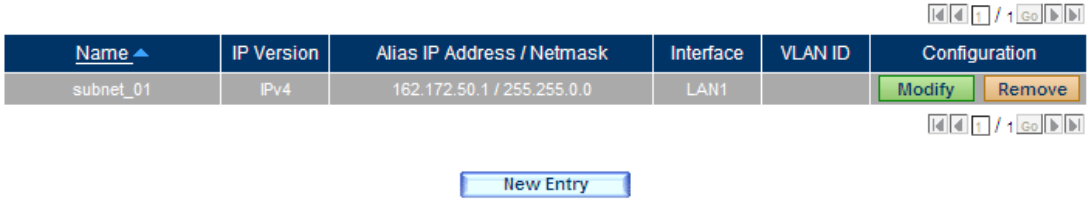


Figure 2-9 Settings Completed

Important:

1. When the PCs' subnets or IP addresses are not on the same Interface. You may go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**) to enable LAN to LAN connection. Or, You may go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**) to enable DMZ to DMZ connection.

Step 2. Under **Network** > **Interface**, set as below: (**Figure 2-10**)

- Click on Port 2's **Modify** button.
- For **Interface Type** select **WAN,** and enter all the relevant settings (provided by your ISP).
- For **WAN NAT Redirection**, select **A designated IP** and then enter 162.172.50.1.

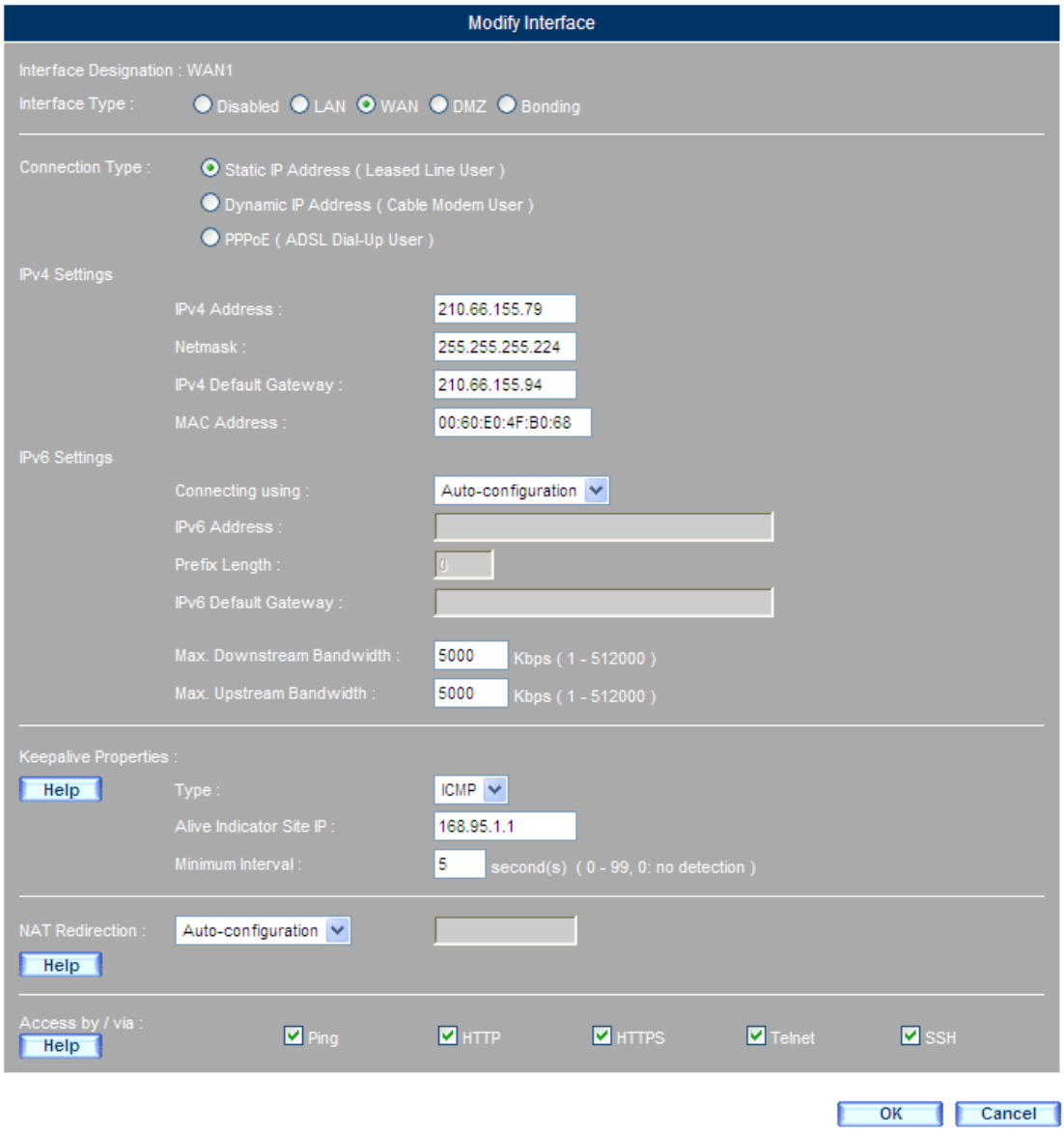


Figure 2-10 Configuring the WAN Settings

Step 3. Under **Policy Object** > **Address** > **LAN**, set as below: (**Figure 2-11**)

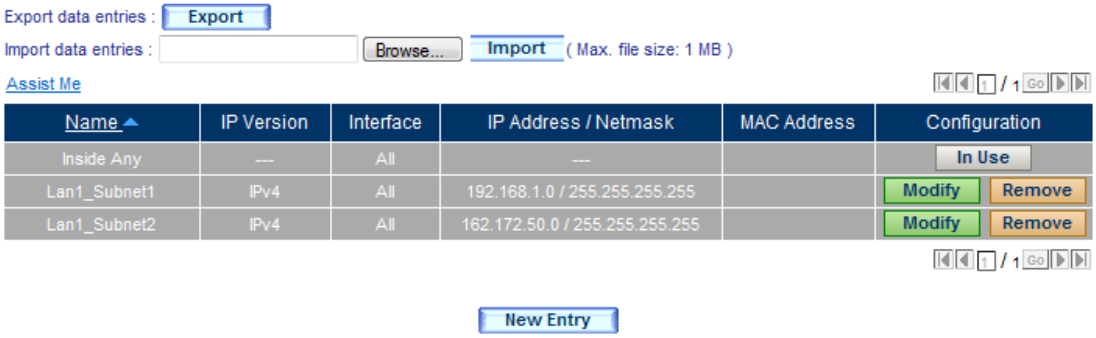


Figure 2-11 Address Settings for the LAN

Step 4. Go to **Policy** > **Outgoing** and configure the following settings:

- Click on **New Entry**.
- **Source Address**: Select the name of the LAN addresses. (LAN1_Subnet1)
- **Action**: Tick Port 3 (WAN2).
- Click on **Advanced Settings.** For **Port3 (WAN2)** select **Automatic.**
- Click on **OK.**（**Figure 2-12**）
- Click on **New Entry**.
- **Source Address:** Select the LAN subnet (LAN1_Subnet2)**.**
- **Action**: Tick the required WAN port.
- **Port 2 (WAN1):** Select Routing.
- **Port 3 (WAN2):** Select Automatic.
- Click **OK**.（**Figure 2-13, 2-14**）

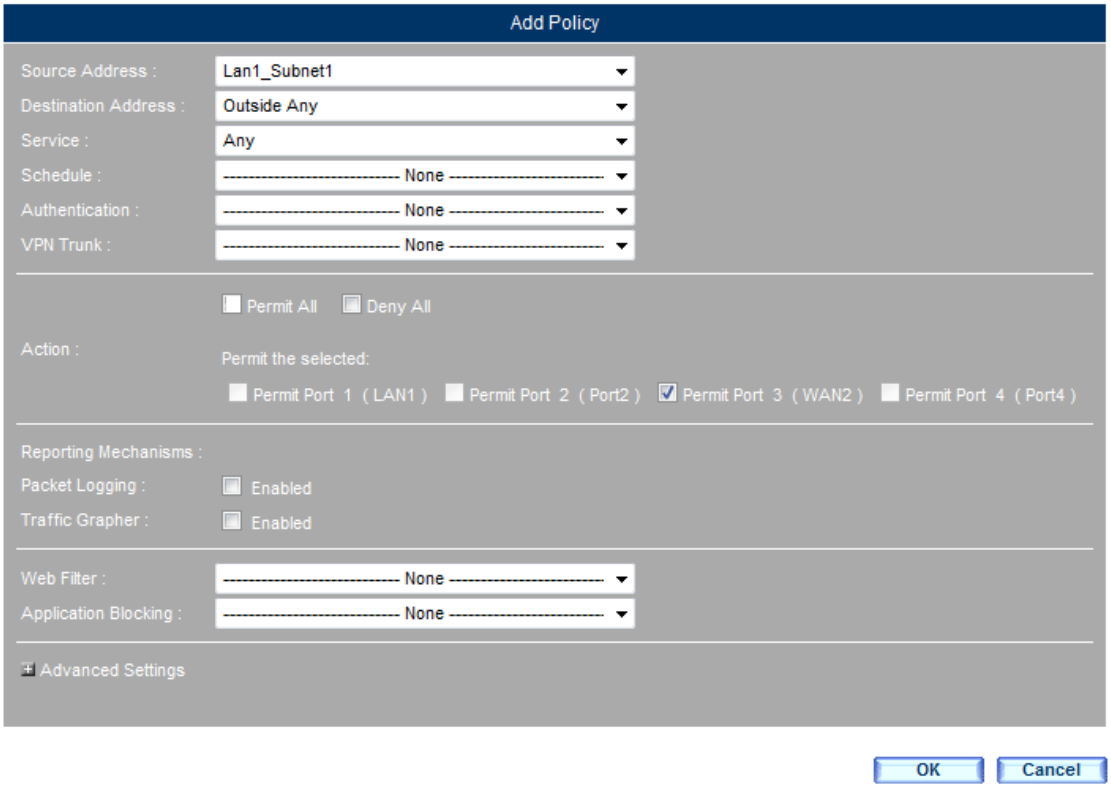


Figure 2-12 The First Outgoing Policy Settings

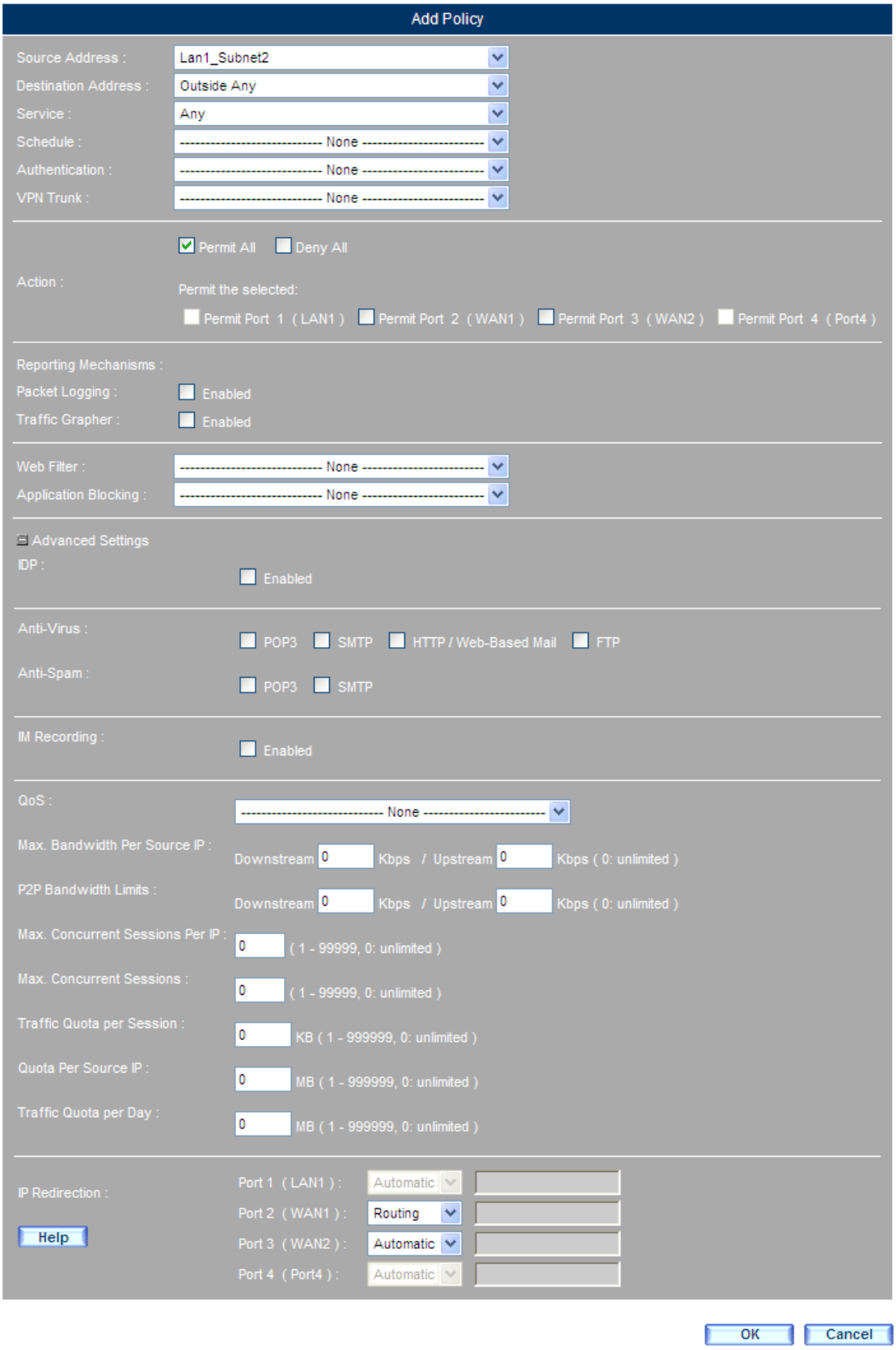


Figure 2-13 The Second Outgoing Policy Settings

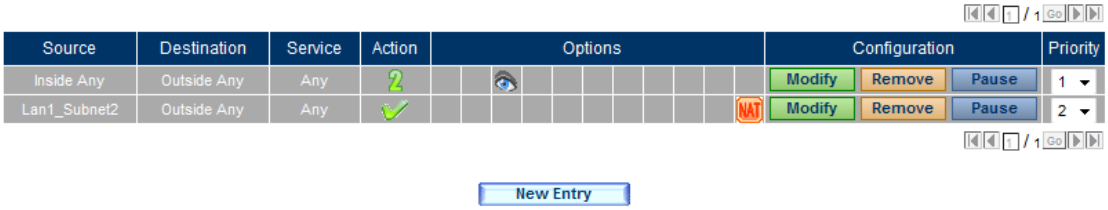


Figure 2-14 Policy Settings Completed

Step 5. The configuration of LAN1 to the Internet is now complete.（**Figure 2-15**）

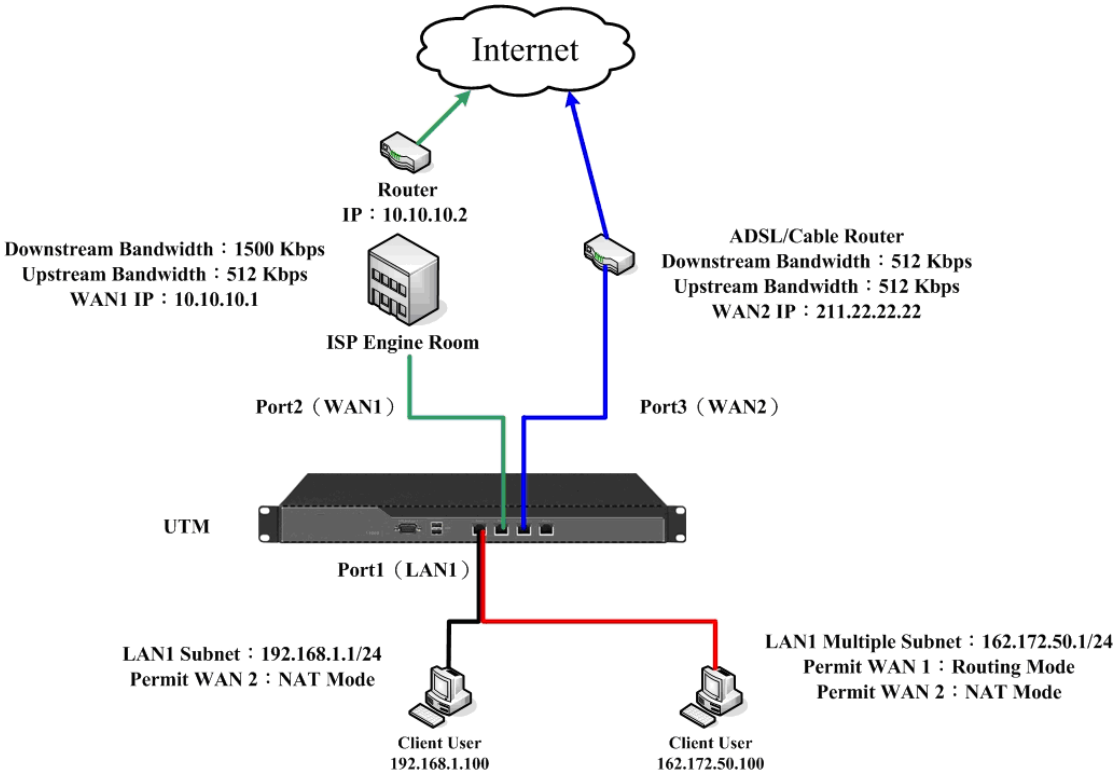


Figure 2-15 The LAN Configured Using Multiple Subnet

Note：

1. The LAN subnet 192.168.1.x/24 is only able to gain access to the Internet via WAN2 (using NAT). Therefore PC's in that subnet, which contain private IP addresses, are unable to access the Internet via WAN1 (using routing).
2. The LAN subnet 162.172.50.x/24 can access the Internet via WAN 1 (using routing) or alternatively via WAN 2 (using NAT).

2.3.2 Using Multiple Subnets to Establish a VLAN Gateway to Regulate VLAN Users to Access the Internet

Prerequisite Setup (Note: IP addresses used as examples only)

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing mode) and connect it to the LAN which is using 192.168.1.x/24.
VLAN ID 10 using 192.168.100.x/24.
VLAN ID 20 using 192.168.200.x/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote(ATUR) to access the Internet.
Configure Port3 as WAN2(211.22.22.22) and connect it to the ADSL Termination Unit Remote(ATUR) to access the Internet.

Step 1. Go to **System** > **Configuration** > **Multiple Subnet,** and set as below:

- Click on **New Entry**.
- Fill in the **Name** field.
- **Interface**: Select Port1 (LAN1).
- **IP Version**: Select IPv4.
- **IP Address:** Type 192.168.100.1.
- **Netmask**: Type 255.255.255.0.
- Tick the **VLAN ID** checkbox and type in 10 into the **VLAN ID** field.
- Click **OK**.（**Figure 2-16**）
- Click on **New Entry** again.
- Fill in the **Name** field.
- **Interface**: Select Port1 (LAN1).
- **IP Version**: Select IPv4.
- **IP Address:** Type 192.168.200.1.
- **Netmask**: Type 255.255.255.0.
- Tick the **VLAN ID** checkbox and type in 20 into the **VLAN ID** field.
- Click **OK**.（**Figure 2-17, 2-18**）

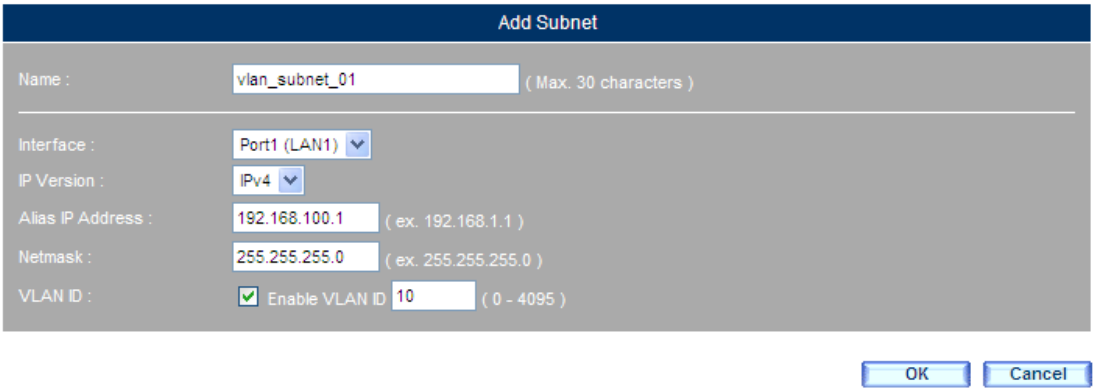


Figure 2-16 First Multiple Subnet Setting

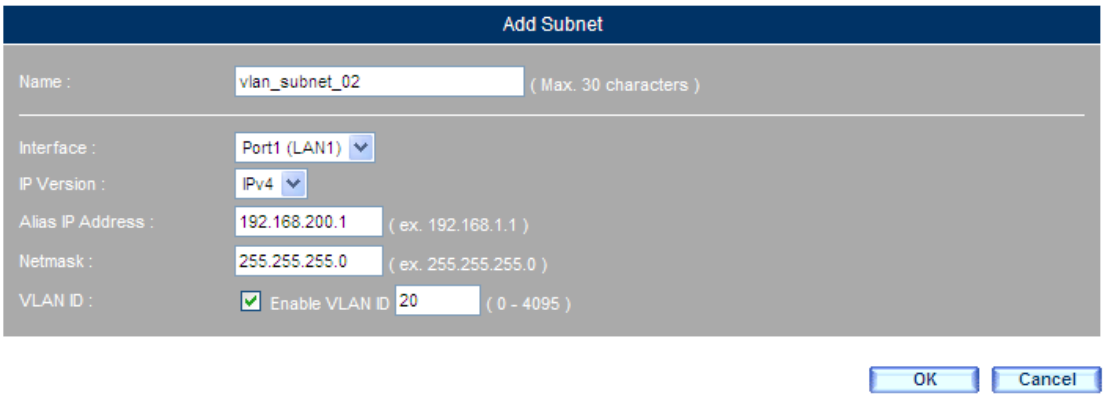


Figure 2-17 Second Multiple Subnet Setting

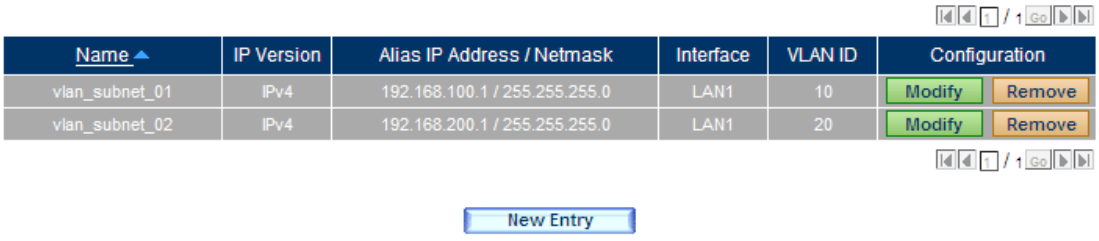


Figure 2-18 Multiple Subnet Settings Completed

Note：

1. The device's interface settings permits multiple VLAN gateways to control each of the VLAN's access to the Internet or communication amongst the VLANs.
2. When the PCs' subnets or IP addresses are not on the same Interface. You may go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**) to enable LAN to LAN connection. Or, You may go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**) to enable DMZ to DMZ connection.

Step 2. Go to **Policy Object > Address > LAN,** and set as below:（**Figure 2-19**）

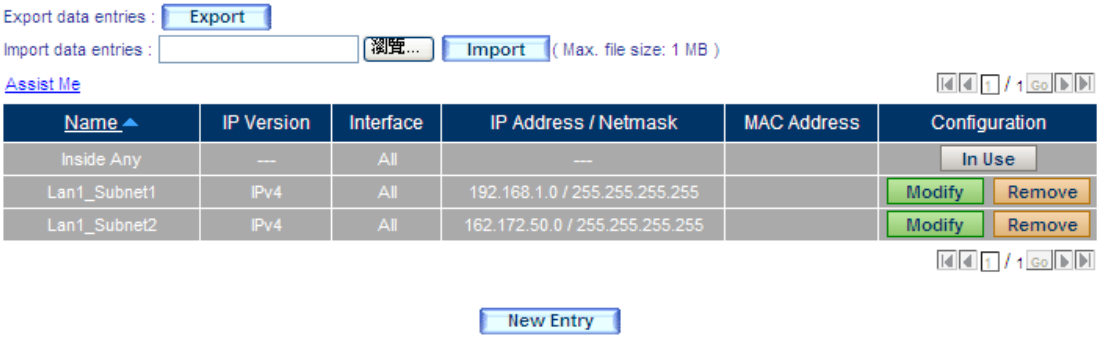


Figure 2-19 Address Settings for the LAN

Step 3. Go to **Policy Object > Address > LAN Group** and then set as below: **(Figure 2-20)**

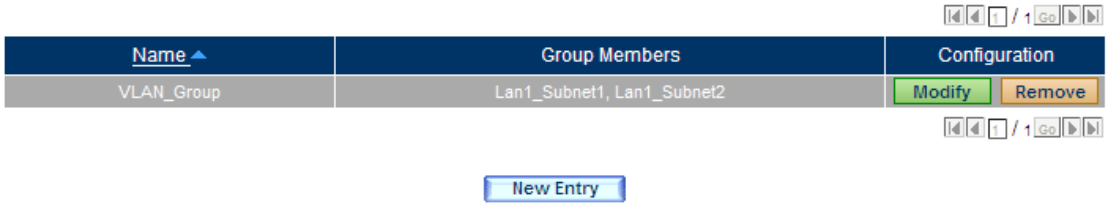


Figure 2-20 LAN Group Settings

Step 4. Go to **Policy > Outgoing**, set as below:

- Click on **New Entry**.
- **Source Address:** Select the name of the LAN addresses (VLAN_Group)
- Click **OK.**（**Figure 2-21, 2-22**）

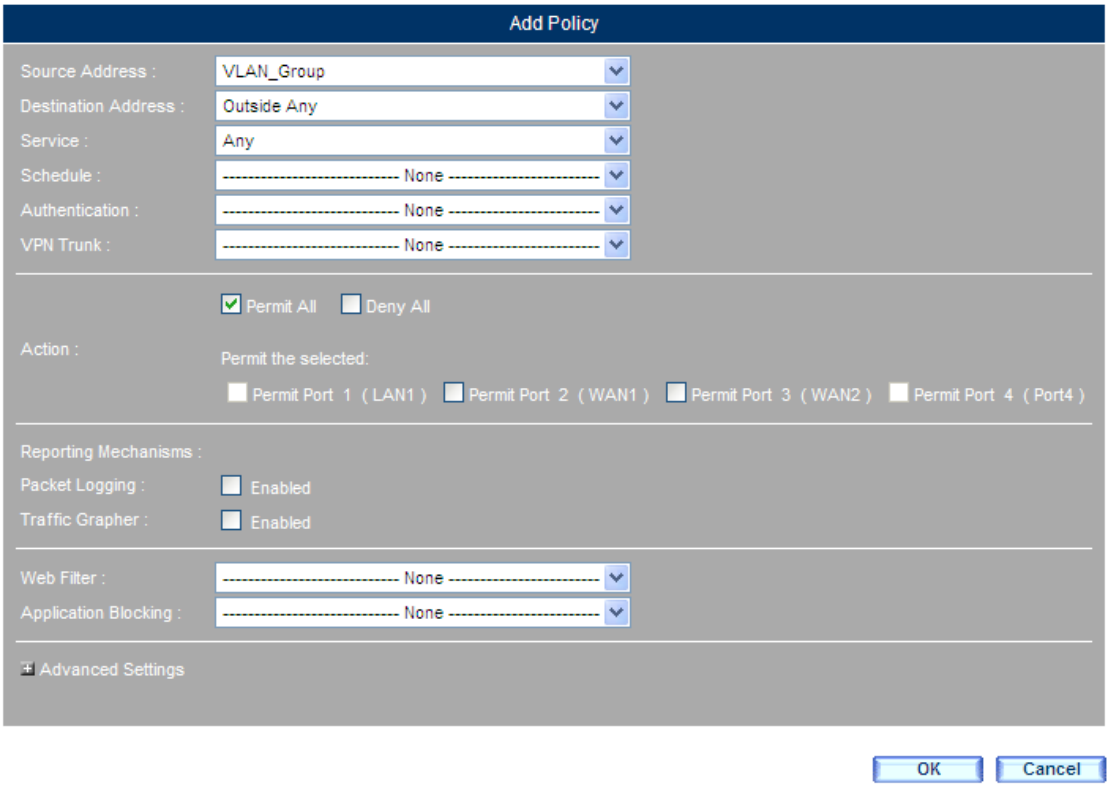


Figure 2-21 Applying the LAN Group to the Policy

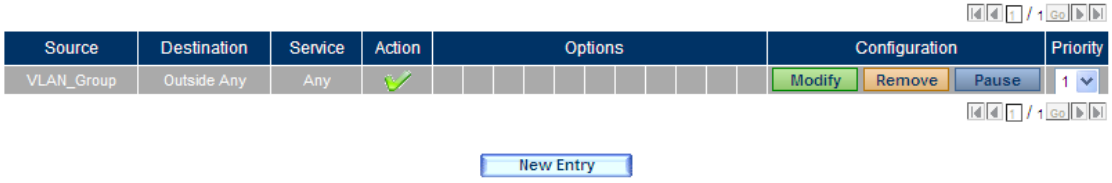


Figure 2-22 Policy Completed

Step 5. The internal network's VLAN. **(Figure 2-23)**

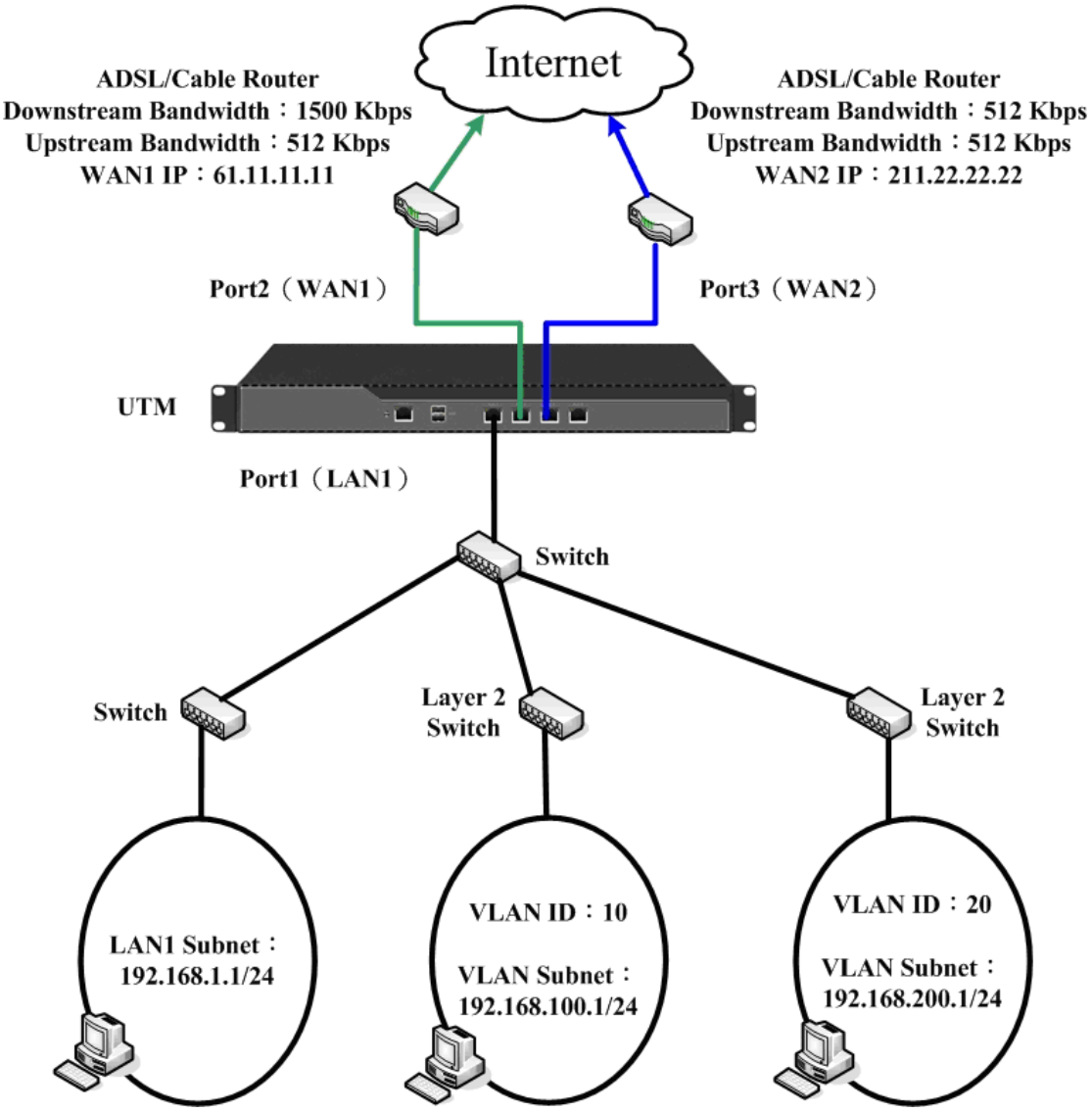


Figure 2-23 The Completed Mulitple Subnet VLAN Settings

2.4 Route Table

2.4.1 Enabling Two Networks Connected by a Router to Access the Internet via the CS-2001

Prerequisite Setup (Note: IP addresses used as examples only)

Company A: Port 1 is set as LAN 1 (192.168.1.1, NAT routing mode) which is connected to the LAN subnet 192.168.1.x/24. The LAN has the subnet 192.168.10.x/24 connected to Router 1 (10.10.10.1 with RIPv2). The LAN interface connected to Router 1 is 192.168.1.252. Port 2 is set as WAN 1 (61.11.11.11) and is connected to the Internet via the ATUR.
Port 3 is set as WAN 2 (211.22.22.22) and is connected to the Internet via the ATUR.

Company B is using Router 2 (10.10.10.2 with RIPv2) with the subnet 192.168.20.x/24 connected to it.

A leased line connects Company A's Router 1 (10.10.10.1) with Company B's Router 2 (10.10.10.2).

Step 1. Go to **System > Configuration > Route Table** and set as below:

- Click on **New Entry.**
- **IP Version :** Select IPv4.
- **IP Address:** Type 192.168.10.0.
- **Netmask:** 255.255.255.0.
- **Gateway :** 192.168.1.252.
- **Interface :** LAN1.
- Click **OK.**（**Figure 2-24**）
- Click on **New Entry.**
- **IP Version :** Select IPv4.
- **IP Address:** Type 192.168.20.0.
- **Netmask:** 255.255.255.0.
- **Gateway :** 192.168.1.252.
- **Interface :** LAN1.
- Click **OK.**（**Figure 2-25**）
- Click on **New Entry.**
- **IP Version :** Select IPv4。
- **IP Address:** Type 10.10.10.0.
- **Netmask:** 255.255.255.0.
- **Gateway :** 192.168.1.252.
- **Interface :** LAN1.
- Click **OK.**（**Figure 2-26, 2-27**）

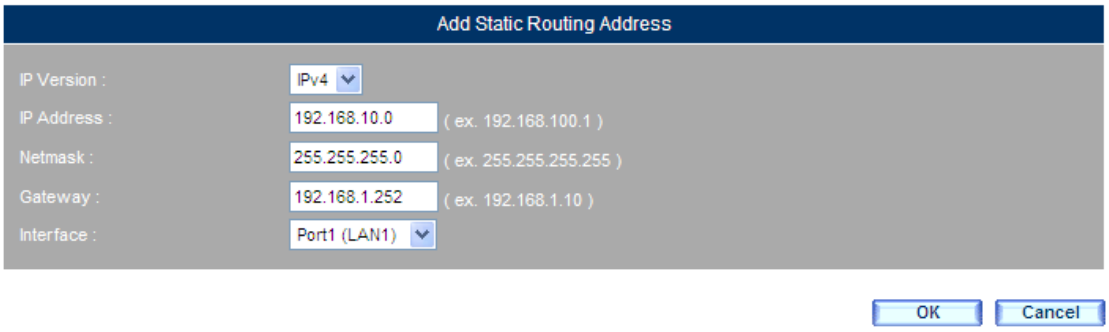


Figure 2-24 Static Route Settings

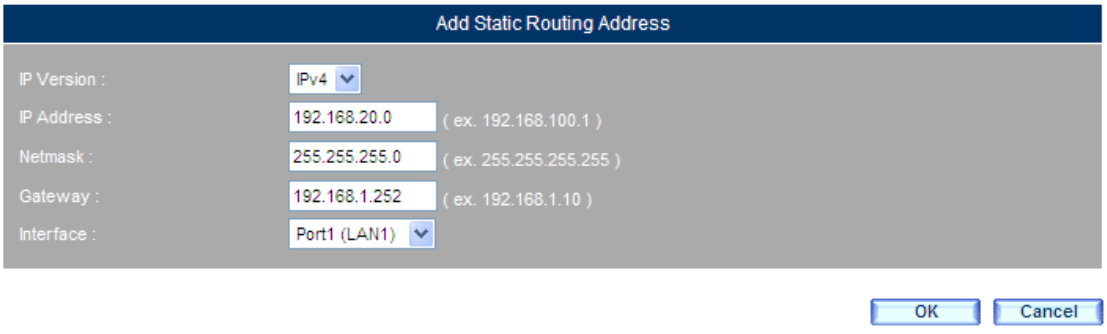


Figure 2-25 Static Route Settings

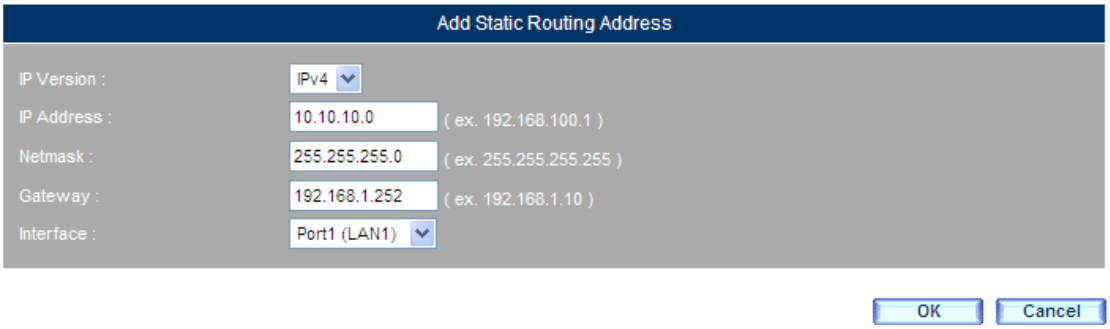


Figure 2-26 Static Route Setttings

Figure 2-27 The Completed Static Route Settings

⚠ Important:

1. To enable the LAN to LAN connection, go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**). To enable the DMZ to DMZ connection, go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**).

Step 2. The subnets 192.168.10.x/24,192.168.20.x/24 and 192.168.1.x/24 can now communicate with each other. In addition, these subnets may also access the Internet using real IP addresses assigned from the CS-2001 device's NAT mechanism.（**Figure 2-28**）

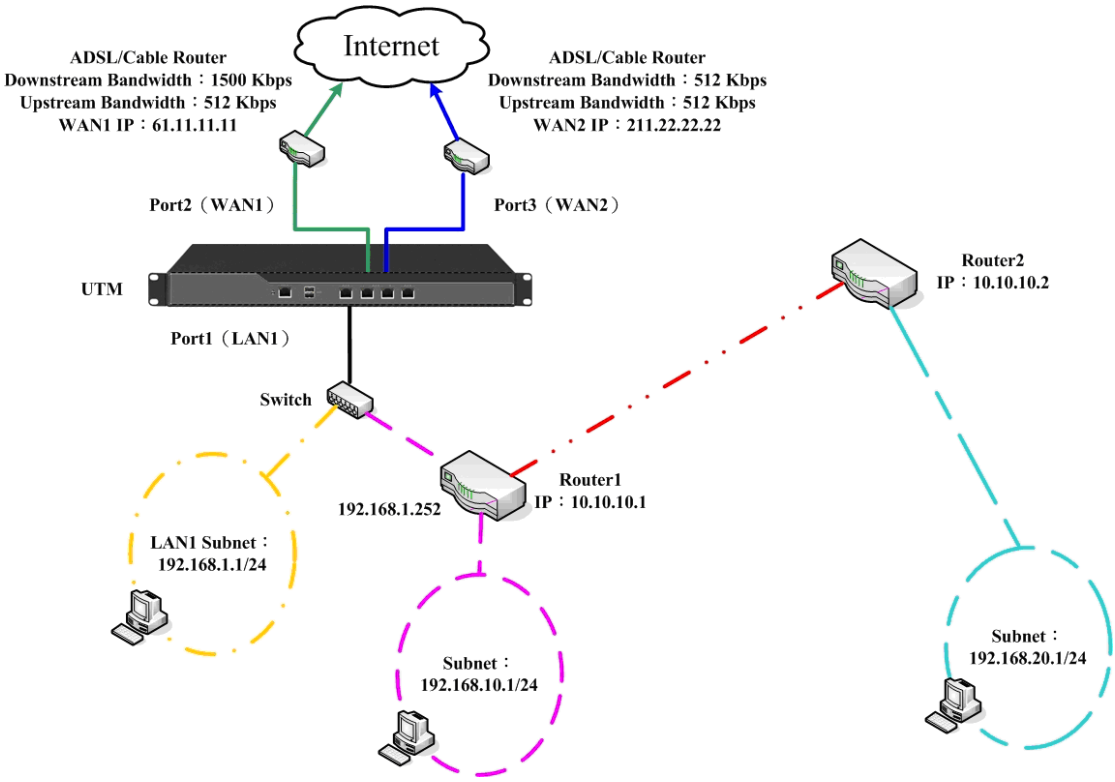


Figure 2-28 The Routing Table

2.5 DHCP

2.5.1 Using an External DHCP Server to Allocate IP Addresses to Internal PCs

Step 1. Go to **System** > **Configuration** > **DHCP,** and set as below: (**Figure 2-29**)

- Tick **Enable DHCP Relay**.
- From **DHCP Relay Interface** select the interface.
- In **DHCP Server IP** enter the IP address of the DHCP server.
- Click **OK** to complete the settings.

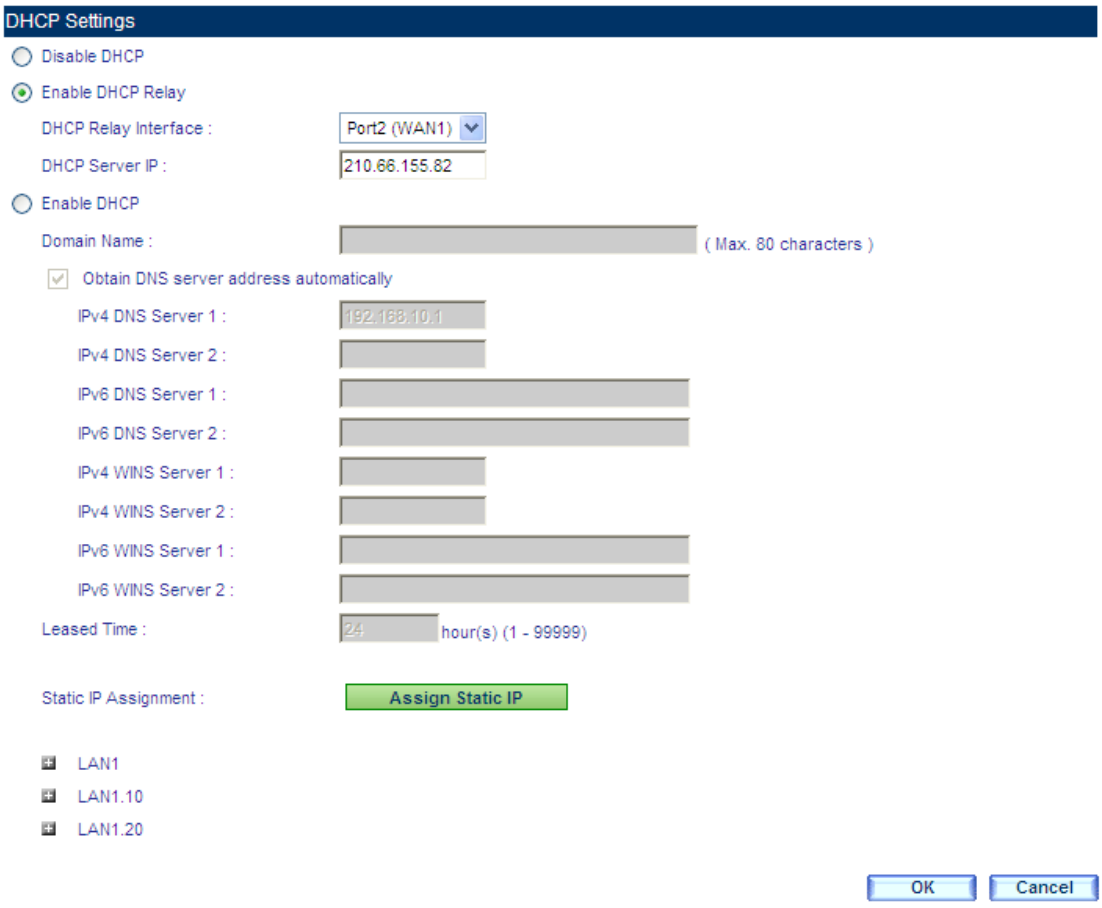


Figure 2-29 DHCP Relay Settings

Note:

1. When **Enable DHCP Relay Support** is enabled, internal PCs can obtain an IP address from the server through the specified interface (WAN1/2/3/4/5/6 or VPN-WAN1/2/3/4/5/6) of the CS-2001.

2.5.2 Using the CS-2001 to Allocate IP Addresses to LAN PCs

Step 1. Go to **System** > **Configuration** > **DHCP** and set as below: (**Figure 2-30**)

- Select **Enable DHCP.**
- Deselect **Obtain DNS server address automatically**.
- **DNS Server 1**: Type an IP address as DNS Server 1.
- **DNS Server 2**: Type an IP address as DNS Server 2.
- **WINS Server 1**: Type an IP address as WINS Server 1.
- **WINS Server 2**: Type an IP address as WINS Server 2.
- **Leased Time :**Type a lease time for the allocated IP addresses (24 hours is the default).
- Configure the following settings for the LAN or DMZ subnet:
  - **IPv4 Range 1 :** Type the IP address range. The default range is from 192.168.1.2 to 192.168.1.254 (Note: The IP address range must reside in the same subnet).
  - **IPv4 Range 2:** Type the second IP address range. (Note: The IP addresses must reside in the same subnet as **IPv4 Range 1** but must not overlap with the range specified in **IPv4 Range 1).**
- Click **OK.**

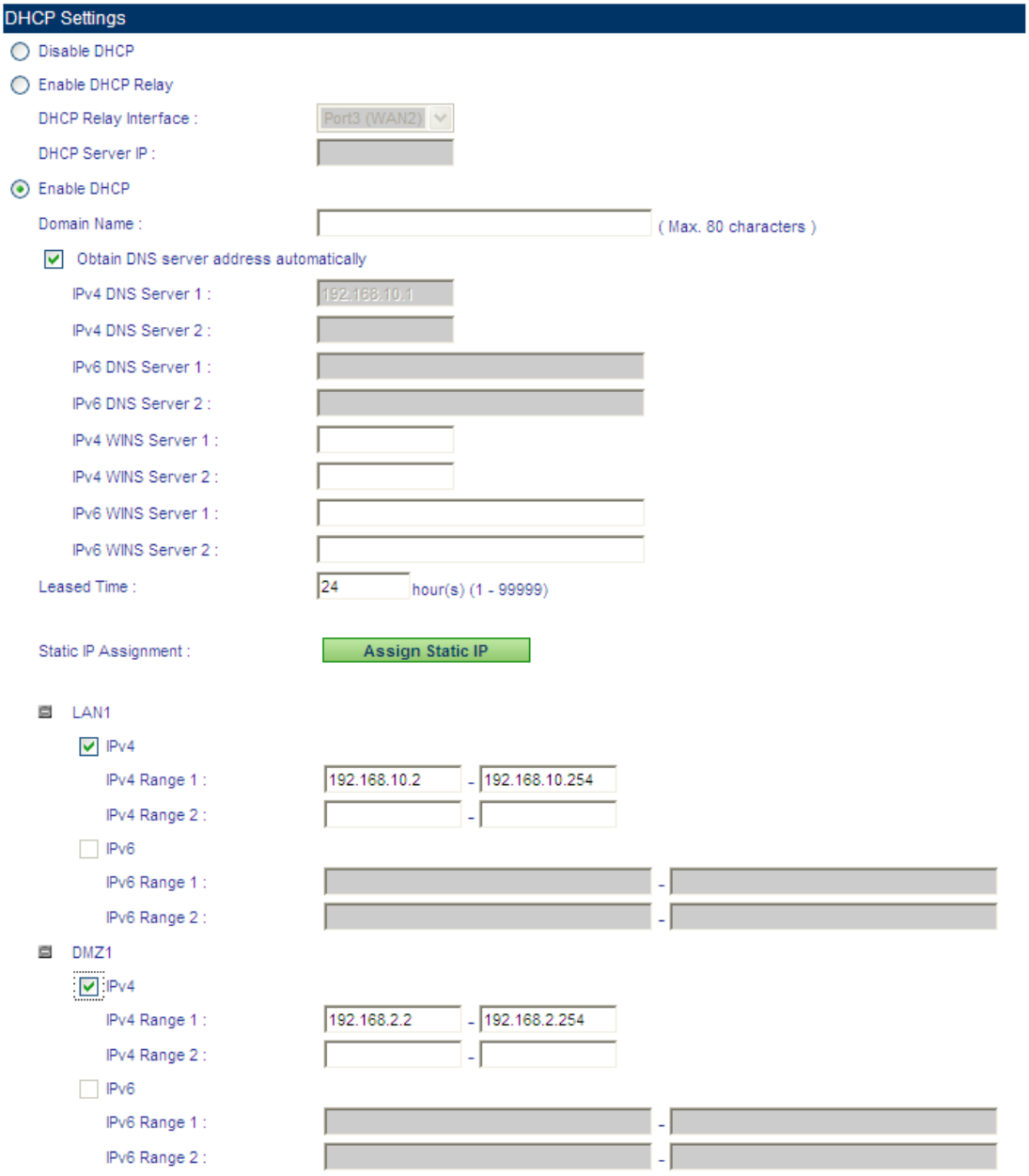


Figure 2-30 DHCP Settings

Note:

1. Enabling **Obtain DNS server address automatically** is intended for LAN users whom access the Internet via the device's authentication mechanism. LAN users need to configure their **Preferred DNS server** address to be the same as the LAN interface address of the CS-2001 in **Internet Protocol (TCP/IP) Properties.**

2.6 DDNS

Step 1. Go to **System** > **Configuration** > **Dynamic DNS,** and set as below: (**Figure 2-31**)

- Click **New Entry.** Select a **Service Provider** from the drop-down list.
- Tick **Use the IP of** on the right of **WAN IP** and then select a WAN port.
- Type the **Username**, **Password** and **Hostname** accordingly.
- Click **OK.** (**Figure 2-32**)

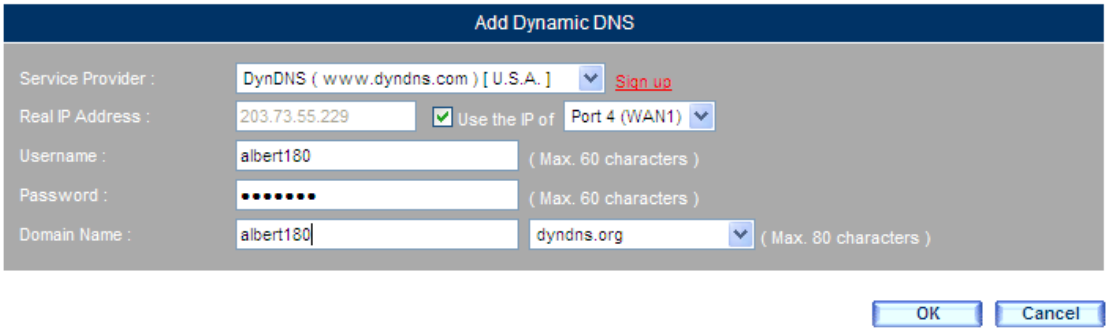


Figure 2-31 Configuring the Dynamic DNS Settings

Figure 2-32 Configuring the Dynamic DNS Settings

Note:

1. The meaning of the symbols used in DDNS are as follows:

Symbol			
Meaning	Successful Connection	Failed Connection	Connected

2. If you do not have a DDNS account, you may first select a desirable service provider from the pull-down menu and then click **Sign up** next to it to register an account.
3. You may configure the **WAN IP** by either ticking the **Automatically** checkbox or simply specifying it in the **WAN IP** field.

2.7 Host Table

Step 1. Go to **System** > **Configuration** > **Host Table** and set as below: (**Figure 2-33**)

- Configure the **Host Name** accordingly.
- Select IPv4 for **IP Version**.
- Type the virtual IP address that the host name corresponds to in the **Virtual IP Address** field.
- Click **OK.**

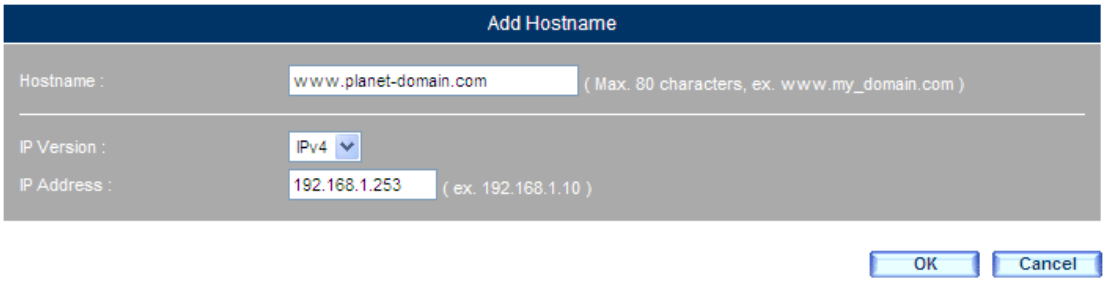


Figure 2-33 Host Table Settings

Note:

1. **Host Table** requires LAN users to configure their **Preferred DNS server** in **Internet Protocol (TCP/IP) Properties** to be the same as the LAN or DMZ interface address. This is the same IP address as the LAN user's default.

2.8 SNMP

2.8.1 SNMP Agent Settings

Step 1. Go to **System** > **Configuration** > **SNMP**. Under the **SNMP Agent Settings** section configure the following:（**Figure 2-34**）

- Tick the interfaces that are permitted to send SNMP agent messages.
- **Device Name**: Name the device. By default, it is **UTM**.
- **Device Location**: Type the geographic location of this device. By default, it is **Taipei**, **Taiwan.**
- **Community**: Type a screen name. By default, it is **public.**
- **Contact Person**: Type the email address of the contact person. By default, it is **root@public.**
- **Description**: Type a description for the device. By default, it is **UTM Appliance.**
- Click **OK.**
- Settings completed. From now on, the IT administrator will be kept up-to-date with the device's operating status through a SNMP Agent application.

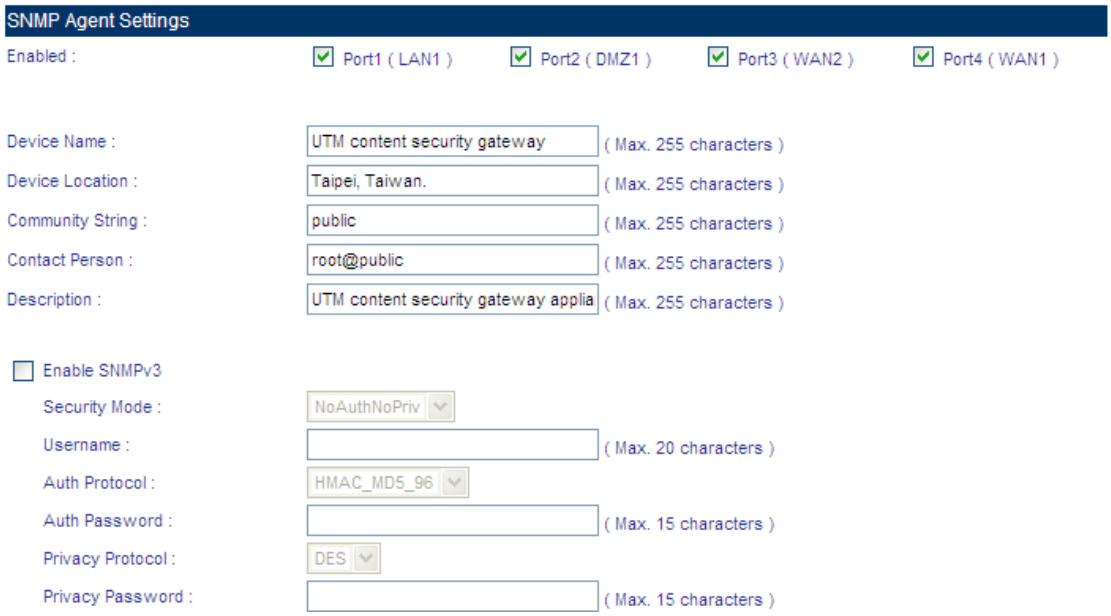


Figure 2-34 SNMP Agent Settings

2.8.2 SNMP Trap Settings

Step 1. Go to **System** > **Configuration** > **SNMP.** Under the **SNMP Trap Settings** section, configure the following settings:（**Figure 2-35**）

- Tick **Enable SNMP trap** a**lerts.**
- **SNMP Trap Recipient Address**: Type the IP address of the SNMP Trap recipient.
- **Port**: Type the port number of SNMP Trap. (Default value: 162)
- Click **OK.**
- The IT administrator may now install a SNMP Trap client to receive alerts from the CS-2001.

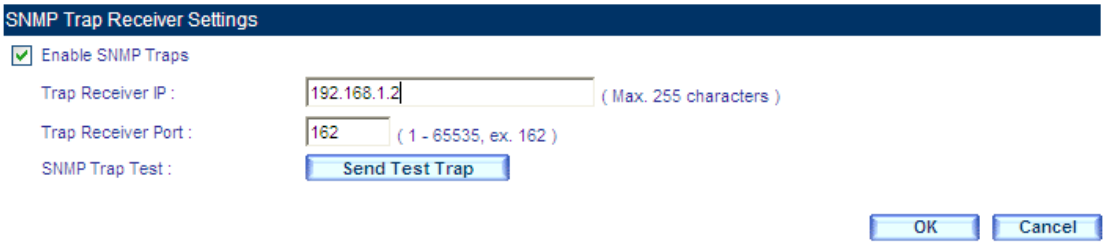


Figure 2-35 SNMP Trap Settings

Note:

1. The IT administrator may test the SNMP trap by clicking on Send Test Trap

2.9 Bulletin Board

2.9.1 Using CS-2001 to Announce the Information to LAN

Users and DMZ Users

Step 1. Go to **System** > **Configuration** > **Bulletin Board** and then configure the settings in the **Bulletin Board Login Settings** secion. **(Figure 2-36）**

- Tick **Enable bulletin board management interface.**.
- Enter the **Bulletin Board Port**.
- Enter the **Username** and the **Password**.
- Click **OK**.

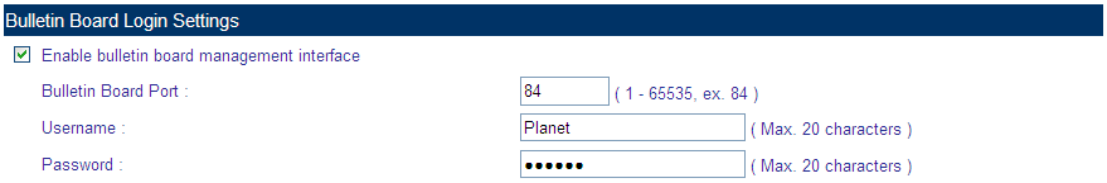


Figure 2-36 Configuring the Bulletin Board Login Settings

Step 2. Under **System > Configuration > Bulletin Board**, configure the settings in the **Bulletin Board Announcements** section.

- Click **New Entry**.（**Figure 2-37**）
- Enter the **Subject**.
- Specify the **Announcement Duration**.
- **Target Viewer**: tick **LAN Users** and select **Inside Any**; tick **DMZ Users** and select **DMZ Any**.
- Enter the **Announcement Message**.
- Click **OK**.（**Figure 2-38**）

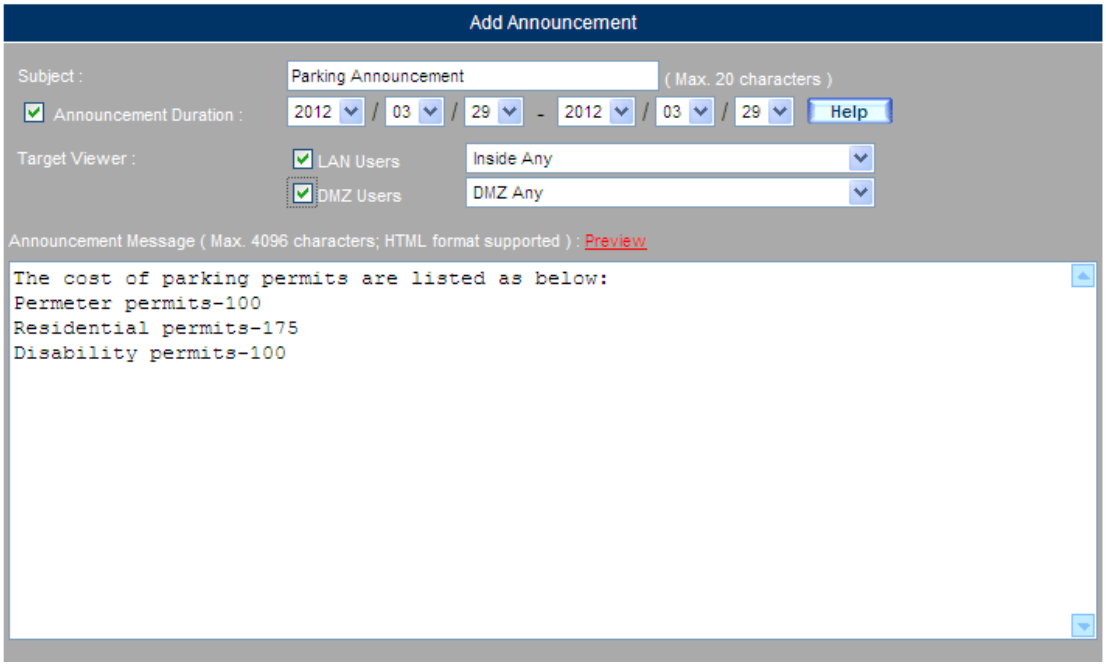


Figure 2-37 Configuring the Announcement

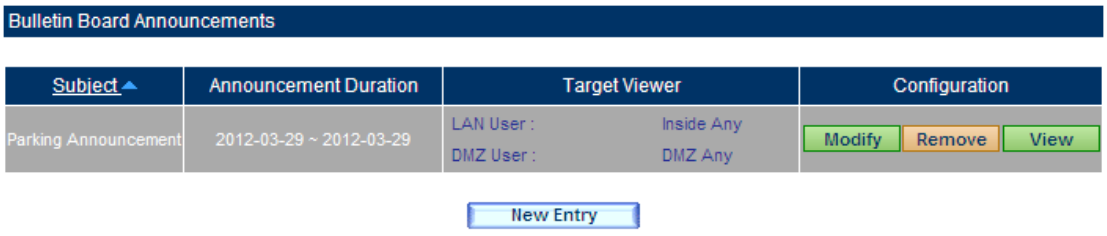


Figure 2-38 Announcement Created

Note:

1. You may configure the **Target Viewer** under **Policy Object > Address > LAN/ LAN Group/ DMZ/ DMZ Group**.

Step 3. The LAN users and DMZ users will see the announcement when they access the Internet.（**Figure 2-39, 2-40**）

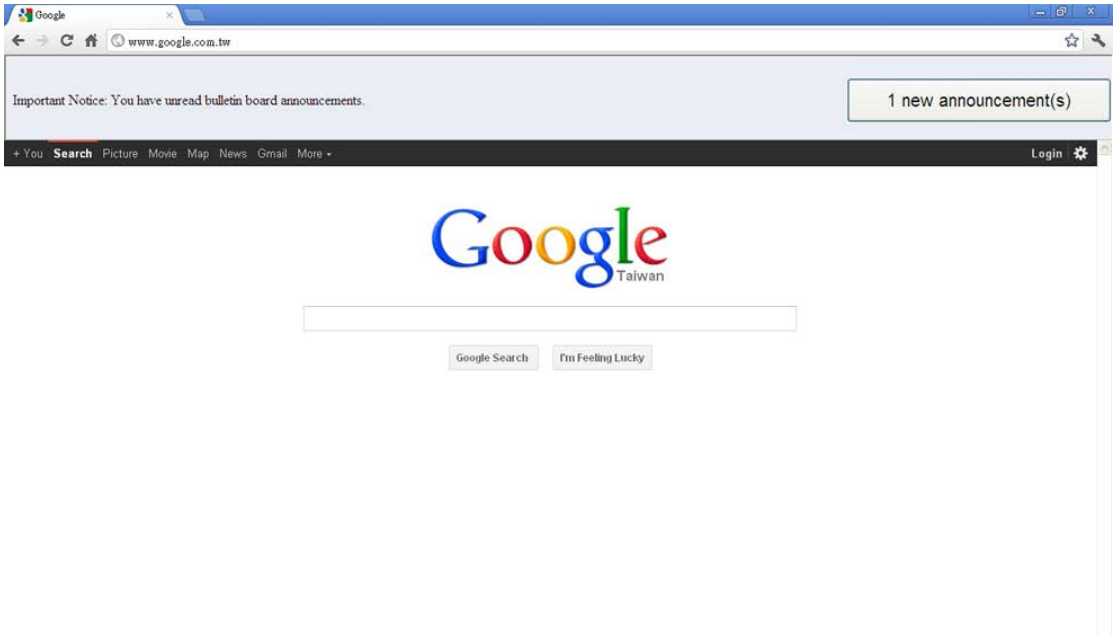


Figure 2-39 Clicking the Button to See the Announcement

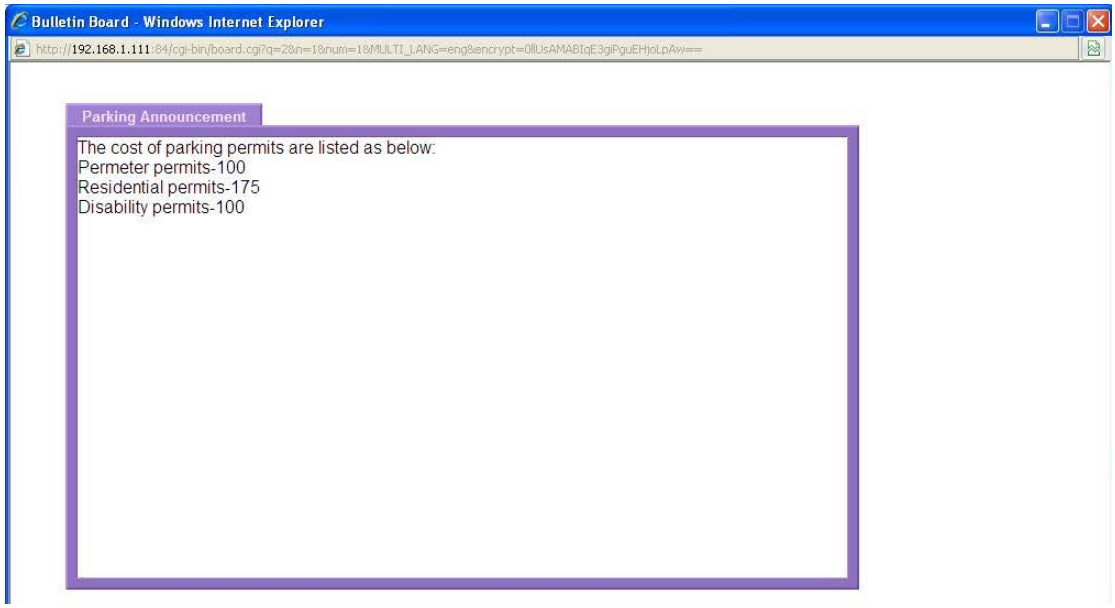


Figure 2-40 LAN / DMZ Users Seeing the Announcement

Note:

1. To know how many users have seen the announcement, you may go to **System > Configuration > Bulletin Board** and then click the **View** button of the announcement.
2. You may access the setting page to configure the announcement by enter the IP address appended with the port number. For example, if the port number is 84, the IP address is

172.19.1.254. You may enter http://172.19.1.254:84 in the web browser. **(Figure 2-41, 2-42)**

Figure 2-41 Logging in the Bulletin Board Setting Page

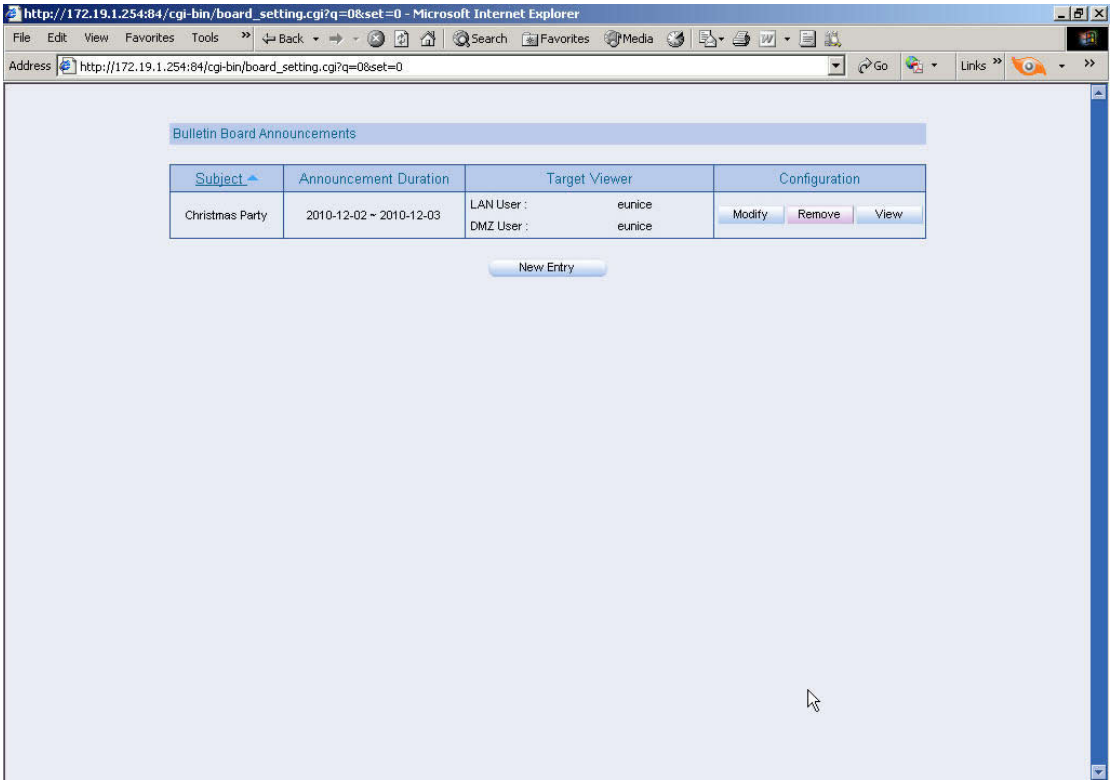


Figure 2-42 The Bulletin Board Setting Page

2.10 Language

2.10.1 Changing the Language

Step 1. Under **System** > **Configuration** > **Language**, you may change the language of the user interface.（**Figure 2-36**）

Figure 2-36 The Language Settings

Interface

Chapter 3 Interface

The *Interface* configuration allows you to configure the connection parameters separately for LAN, WAN and DMZ interfaces as well as to assign multiple network interfaces into a group based on your topology plan.

In this chapter, it will be covering the functionality and application of *Settings*, *Interface* and *Interface Group*.

Terms in Settings

DNS Settings

- The DNS servers used for resolving domain names to IP addresses.

MTU Setting

- The Maximum Transmission Unit (MTU) controls the maximum buffer size used for inter-node communication in bytes. By default, it is 1500 bytes.

Incoming Packet Header Logging

- When enabled, packets destined to or originated from CS-2001 are logged in details, which are available under **Monitoring > Logs > Traffic.**

Link Speed / Duplex Mode Settings

- Specifies the speed and duplex mode of a physical port.

Terms in Interface

Load Balancing Mode

- **Auto**: Distributes the outward sessions by the usage status of each WAN port. (For multiple Internet connections at different speeds)
- **Round-Robin**: Evenly distributes the downloading sessions to each WAN port. (For multiple Internet connections at the same speed)
- **By Traffic**: Distributes the downloading sessions by traffic.
- **By Session**: Distributes the outward sessions by the setting of Saturated Connections.
- **By Packet**: Distributes the downloading sessions by the amount of packet.
- **By Source IP:** For services that require using the same IP address throughout the process, such as online game and banking, CS-2001 helps user retain the same WAN port (i.e. IP address) over which the session was created to avoid disconnection caused by the variation of the user's IP address.
- **By Destination IP:** Once a session is created between the CS-2001 and a specific host, then the following sessions linking to that host will be automatically distributed to the same WAN port.

Port

- The sequential number of a physical port.

Interface Designation

- The system-assigned name based on the network interface type selected.

Interface Type

- The network interface is categorized into three types:
  - Local Area Network (LAN)
  - Wide Area Network (WAN)
  - Demilitarized Zone (DMZ)

Connection Type (As Interface Type set to LAN)

- It has three connection types, namely:
  - **NAT Routing**: Allows private IP addresses (not-in-use ones) to be translated into public addresses based on network policy.
  - **Transparent Bridging**: Allows internal users to access a specific networking device in a different network based on network policy through the default gateway. Note: This mode requires configuring **Interface Group** settings under **Network**.
  - **Transparent Routing**: Provides internal users with direct access to the Internet due to being in the same subnet range.

IPv4 Settings

- Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and it is by far the most widely deployed Internet Layer protocol.
- IPv4 addresses are written in dot-decimal notation, which consists of the four octets of the address expressed in decimal and separated by periods, such as 192.168.1.1.
- Please configure the **IPv4 Address**, **Netmask** and **MAC Address** fields according to your network topology.

IPv6 Settings

- Internet Protocol version 6 (IPv6) is called the “IP Next Generation” (IPng), which is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. It is backward compatible and thus expected to slowly replace IPv4, with the two existing side by side for many years.

- IPv6 address represent itself as text string using the following three conventional forms:
  - **Colon-hexadecimal form:** This is the preferred form n:n:n:n:n:n:n:n. Each n represents the hexadecimal value of one of the eight 16-bit elements of the address. For example: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
  - **Compressed form:** This is to simplify writing addresses that contains a long string of zeros, use the compressed form, in which a single contiguous sequence of 0 blocks are represented by a double-colon symbol (::). This symbol can appear only once in an address. For example, the unicast address FE80:0:0:0:2AA: FF: FE9A:4CA2 in compressed form is FE80:: 2AA:FF:FE9A:4CA2.
  - **Mixed form:**
    - **IPv4-compatible addresses:** The IPv4-compatible address, 0:0:0:0:0:0:*w.x.y.z* or ::*w.x.y.z* (where *w.x.y.z* is the dotted decimal representation of a public IPv4 address), is used by IPv6/IPv4 nodes that are communicating with IPv6 over an IPv4 infrastructure. When the IPv4-compatible address is used as an IPv6 destination, the IPv6 traffic is automatically encapsulated with an IPv4 header and sent to the destination using the IPv4 infrastructure.
    - **IPv4-mapped addresses:** The IPv4-mapped address, 0:0:0:0:0:FFFF:*w.x.y.z* or ::FFFF:*w.x.y.z*, is used to represent an IPv4-only node to an IPv6 node, for example, ::ffff:192.0.2.128 is the IPv4-mapped IPv6 address for IPv4 address 192.0.2.128.
- The leading bits in the address define the specific IPv6 address type. The variable-length field containing these leading bits is called a Format Prefix (FP). An IPv6 unicast address is divided into two parts. The first part contains the address prefix (also known as subnet prefix such as 21DA:D3:0:2F3B::/64), and the second part contains the interface identifier (MAC address).
  - A concise way to express an IPv6 address/prefix combination is as follows: ipv6-address/prefix-length. For example, an IPv6 address with a 64-bit prefix is represented as 3FFE:FFFF:0:CD30:0:0:0:0/64 or 3FFE:FFFF:0:CD30::/64.

- The IPv6 prefix is the part of the address that indicates the bits that have fixed values. If it happens not to be a multiple of four such as 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/***59***, then the third 16 bits (i.e., 2F3B) have to be modified (to 2F20) to become a multiple of four.

- IPv6 addresses are classified into three types:
  - **Unicast address:**
    - **Link-local addresses:** These addresses are used on a single link and have the following format: FE80::InterfaceID. A link-local address is used primarily at startup for address autoconfiguration. It is analogous to IPv4's RFC 3927 address (169.254.0.0/16).
    - **Site-local addresses:** These addresses are used on a single site and have the following format: FEC0::SubnetID:InterfaceID. The site-local addresses are used for addressing inside a site without the need for a global prefix. They are analogous to IPv4's RFC1918 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
    - **Global IPv6 unicast addresses:** These addresses can be used across the Internet and have the following format: 010 (FP, 3 bits) TLA ID (13 bits) Reserved (8 bits) NLA ID (24 bits) SLA ID (16 bits) InterfaceID (64 bits).
  - **Multicast address:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to this address is delivered to all the interfaces identified by the address. The multicast address types supersede the IPv4 broadcast addresses. They are prefixed with FF (that is, the first bits are 11111111) such as FF02::1 for all nodes address, FF02::2 for all routers address, etc.
  - **Anycast address:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to this address is delivered to only one interface identified by the address. This is the nearest interface as identified by routing metrics.

Note：

1. Converting an Ethernet MAC address (00-AA-00-3F-2A-1C) to EUI-64 format:
   - FF-FE is inserted between the third and fourth bytes. This yields 00-AA-00-FF-FE-3F-2A-1C.
   - The U/L bit, which is the seventh bit in the first byte, is complemented. The first byte in binary form is 00000000. When the seventh bit is complemented, it becomes 00000010 (0x02).

- The result, 02-AA-00-FF-FE-3F-2A-1C, is converted to colon-hexadecimal notation, yielding the interface identifier 2AA:FF:FE3F:2A1C. Thus, in this example, the link-local address that corresponds to the network adapter with the MAC address of 00-AA-00-3F-2A-1C is FE80::2AA:FF:FE3F:2A1C.

Any IP Routing

- For hoteliers (hotel, guest house, inn, hostel, motel, etc.) to provide customers with Internet service.
- Internet access is made easy by saving both the customers and the IT technician at the hotel (or a non-IT staff) from the hassle of network configuration, i.e., IP address, netmask, default gateway, etc. Simply hardwire user's laptop to the LAN network and the Internet is ready to go.

Note：

1. This feature is not intended for an office scenario.
2. There could be an IP conflict issue due to the same LAN IP used.

MAC Address

- Configure the MAC address accordingly.

Ping

- When ticked, the network can be detected by ping command.

HTTP

- When ticked, the management interface is available for access via HTTP protocol.

HTTPS

- When ticked, the management interface is available for access via HTTPS protocol.

Telnet

- When ticked, the management interface is available for access via Telnet protocol.

SSH

- When ticked, the management interface is available for access via SSH protocol.

Connection Type (As Interface Type set to WAN)

- It has three connection types, namely:
  - Static IP Address (Leased Line User)
  - Dynamic IP Address (Cable Modem User)
  - PPPoE (ADSL Dial-Up User)

Service Detection

- The test for the validity of Internet connection. As listed below are the test methods:
  - **ICMP**: Uses ping command to test the validity of Internet connection.
  - **DNS**: Tests the validity of Internet connection by requesting the domain name.

NAT Redirection

- Translates private IP addresses into public addresses.
  - **Auto-configuration**: The public address is automatically designated by the system.
  - **A designated IP**: The public address is manually designated by the IT administrator.

Max. Downstream & Upstream Bandwidth

- The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating.

Disconnect if idle for…minutes

- The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection. The time unit is minute; enter a number from 1 to 99,999 inclusive as the basis of disconnection, or “0” to stay connected.

Connection Type (As Interface Type set to DMZ)

- Please refer to “**Connection Type (As Interface Type set to LAN)**”.

Bonding

- Network Bonding allows you to aggregate the bandwidth of multiple interfaces into a single connection.

Bonding Interface

- Configuring the interface. (LAN, WAN or DMZ)

Bonding Mode

- The three available modes are as follows:
  - Round-Robin: Transmits packets in sequential order from the first available slave port through the last. (Prerequisite: A switch that supports port trunking.)
  - Active-Backup: Only one slave port in the bond is active; a different slave port becomes active only if the active one fails.
  - IEEE 802.3 ad Link Aggregation: Transmits and receives packets using all slave ports inone active aggregator. (Prerequisite: A switch that supports IEEE 802.3ad Dynamic link aggregation.)

Detection Mode

- When Round-Robin or Active-Backup is selected for Bonding Mode, ARP detect can be selected to detect the connection.

Saturated Connections

- Determines the amount of sessions each WAN port can process at a time under **By Traffic**, **By Session** or **By Packet** mode. New sessions will be distributed to other WAN ports when the number of sessions has reached the maximum specified.

Priority

- The priority of a WAN port.

Terms in Interface Group

Interface Group

- Allows you to group network interface while each group is isolated from one another. Note: This requires at least a WAN port with a static IP and a LAN or DMZ running Transparent Bridging mode.
- Allows your LAN or DMZ network traffic to be routed to an external network by modifying address contents in the IP header to be valid in the address realm into which the traffic is routed to.

3.1 Example

No.	Scenario	Page
3.1.1	Modifying the LAN Interface (NAT / Routing)	**85**
3.1.2	Configuring the WAN Interface	**87**
3.1.3	Using CS-2001 as a Gateway for Users on Two Subnets to Access the Internet (NAT/Routing)	**93**
3.1.4	Using CS-2001 as a Gateway for the Internal Users to Access the Internet and Configure the DMZ for the External Users to Access the Network Resource	**97**
3.1.5	Deploying the CS-2001 between the Gateway and LAN (configuring two subnets, one using Transparent Routing, the other one using NAT/Routing) for the LAN users to access the Internet	**101**
3.1.6	Deploying the CS-2001 between the Gateway and the LAN (LAN1 and DMZ1), connecting LAN1 to the user's PC (using NAT/Routing mode) and then connecting DMZ1 to user's PC (using Transparent Bridging mode)	**105**
3.1.7	Deploying CS-2001 between the Gateway and LAN (LAN1 and DMZ1) for LAN Users and DMZ Users to Access the Internet	**112**
3.1.8	Using the CS-2001 Device as the Gateway and Connecting it to the LAN (There are Two LAN Interface, One Use NAT/Routing, the Other One Use Transparent Bridging Mode) for the LAN Users to Access the Internet	**118**

3.1.1 Modifying the LAN Interface (NAT / Routing)

Prerequisite Setup (Note: IP addresses used as examples only)

Port1 is configured as LAN1 by default. (IP address: 192.168.1.1, NAT/ Routing)

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-1**）

- Click Port1's **Modify** button.
- Select LAN for **Interface Type**.
- Select NAT Routing for **Connection Type**.
- Enter the **IPv4 Address** and **Netmask**.
- Tick **Ping**, **HTTP** and **HTTPS**.
- Click **OK**.

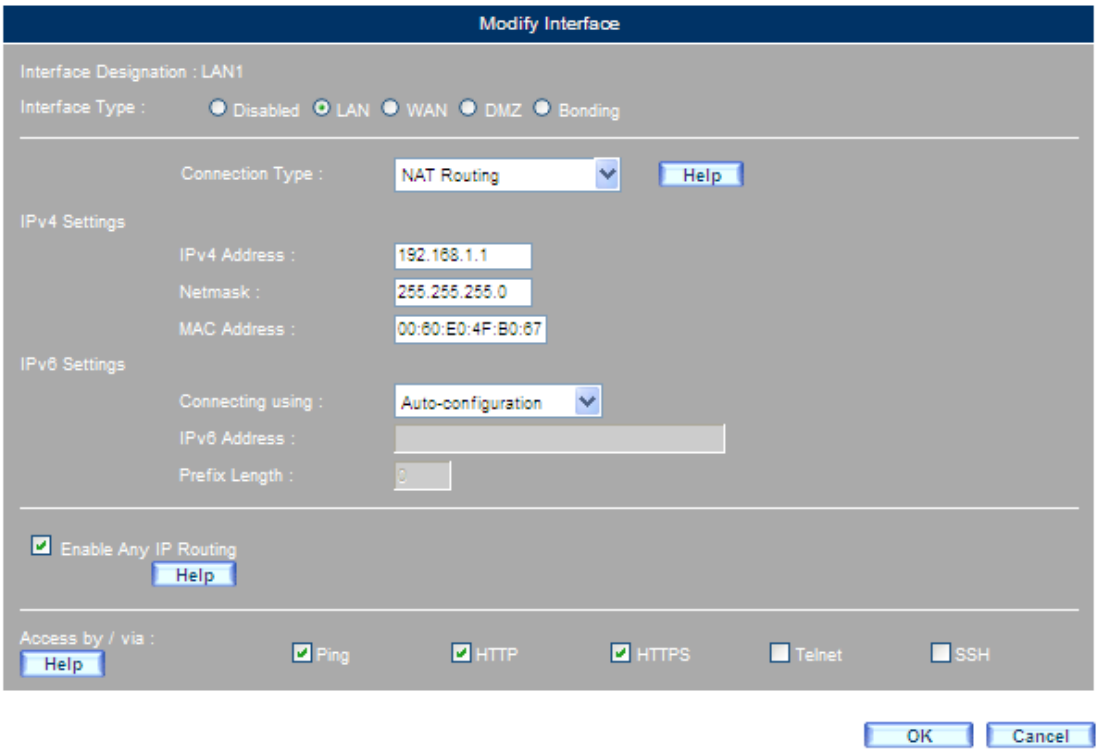


Figure 3-1 Modifying the LAN Interface

Note：

1. The LAN subnet is configured as 192.168.1.x/24 by default. After modifying the LAN subnet, LAN PCs' subnet must be modified as well for the LAN users to access the Web UI.

2. Do not disable HTTP and HTTPS before configuring the settings under **System > Administration > Permitted IPs**, or the IT administrator may be unable to access the Web UI from LAN.

3.1.2 Configuring the WAN Interface

Step 1. Go to **Network** > **Interface** and then click Port2's **Modify** button. Select WAN for **Interface Type.**

Step 2. Configure the **Service Detection** (ICMP & DNS):

- If ICMP is selected, enter the **Alive Indicator Site IP.**（**Figure 3-2**）
- If DNS is selected, enter the **DNS IP Address** and the **Domain Name.**（**Figure 3-3**）
- Enter the **Minimum Interval**.

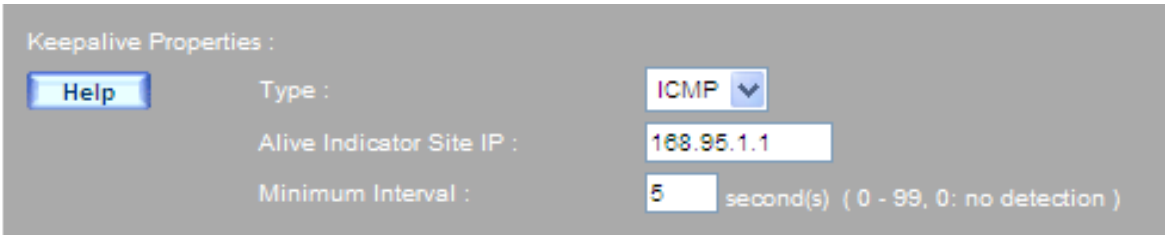


Figure 3-2 ICMP Detection

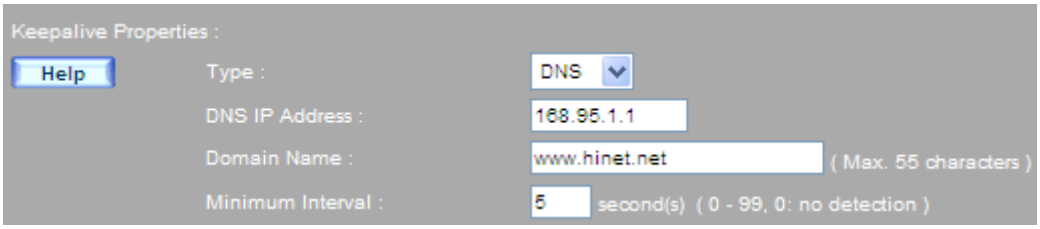


Figure 3-3 DNS Detection

⚠ Important：

1. **Keepalive Properties** is used for detecting the WAN connection. Thus, the **Alive Indicator Site IP**, the **DNS IP Address** and the **Domain Name** should be available to maintain the accuracy of detection.

Step 3. Select WAN for **Interface Type:**

- **Static IP Address:**（**Figure 3-4**）
  - Enter the **IP Address**, **Netmask** and **Default Gateway.**
  - Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth.**
  - Tick **Ping**, **HTTP** and **HTTPS.**
  - Click OK.（**Figure 3-5**）
- **Dynamic IP Address (Cable Modem User)**:（**Figure 3-6**）
  - Click the **Renew** button to get the IP Address automatically.
  - Click the **Clone MAC Address** button to get the MAC Address if required.
  - Enter the **Username** if required.
  - Enter the **Domain Name** if required.
  - Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth.**
  - Tick the **Ping**, **HTTP** and **HTTPS.**
  - Click **OK**.（**Figure 3-7**）
- **PPPoE (ADSL Dial-Up User)**:（**Figure 3-8**）
  - Enter the **Account Name.**
  - Enter the **Password.**
  - **IP Address Obtained from ISP Via**: select Dynamic.
  - Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth.**
  - Tick **Ping**, **HTTP** and **HTTPS.**
  - Click **OK**.（**Figure 3-9**）

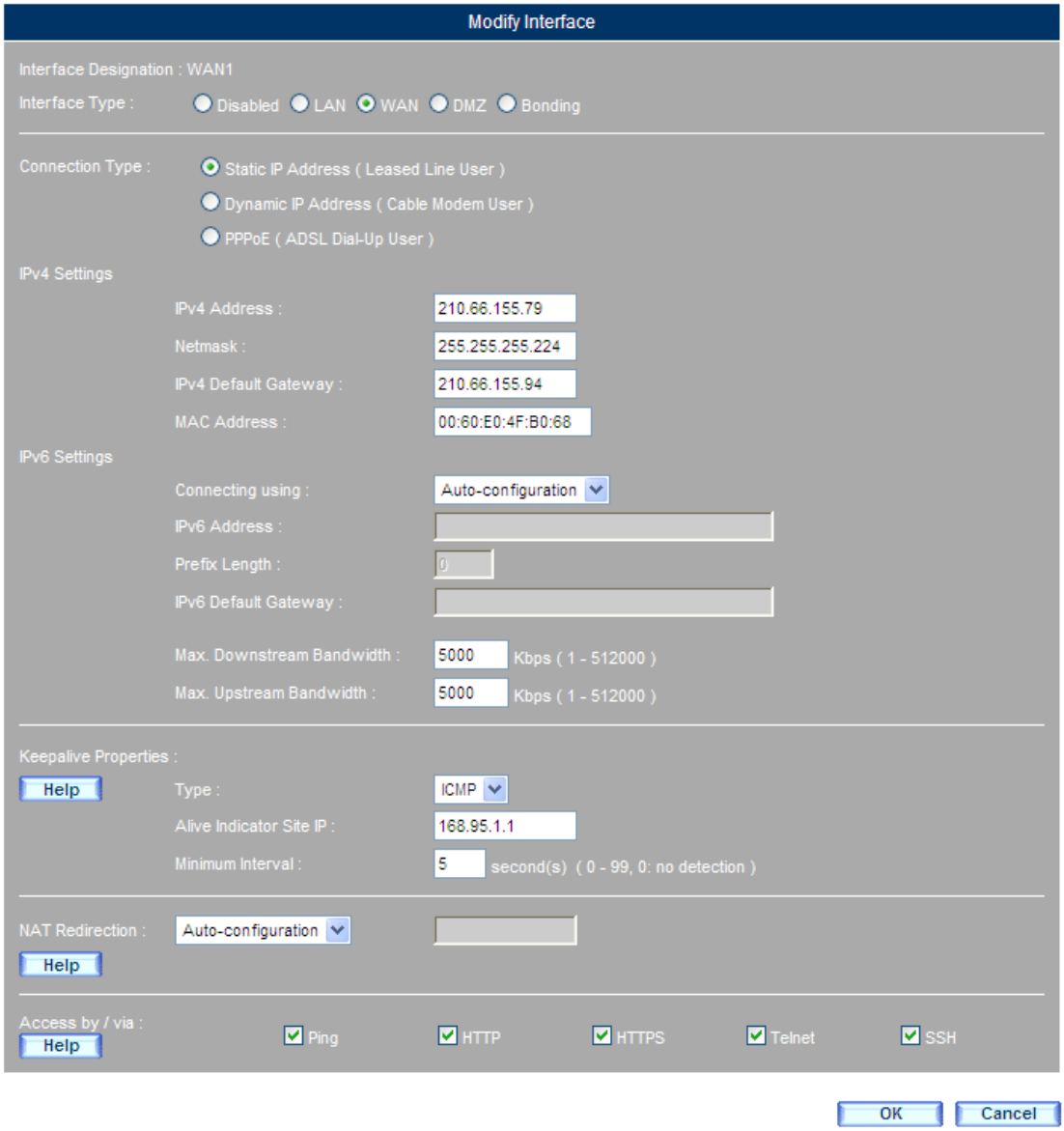


Figure 3-4 Configuring the Static IP Address

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.10.1 / 255.255.255.0	---	Modify	---
2	DMZ1	NAT Routing	192.168.2.1 / 255.255.255.0	---	Modify	---
3	WAN2	Static IP	61.62.236.15 / 255.255.255.0	---	Modify	1
4	WAN1	PPPoE	203.73.55.229 / 255.255.255.255	---	Modify	2

Figure 3-5 Setting Completed

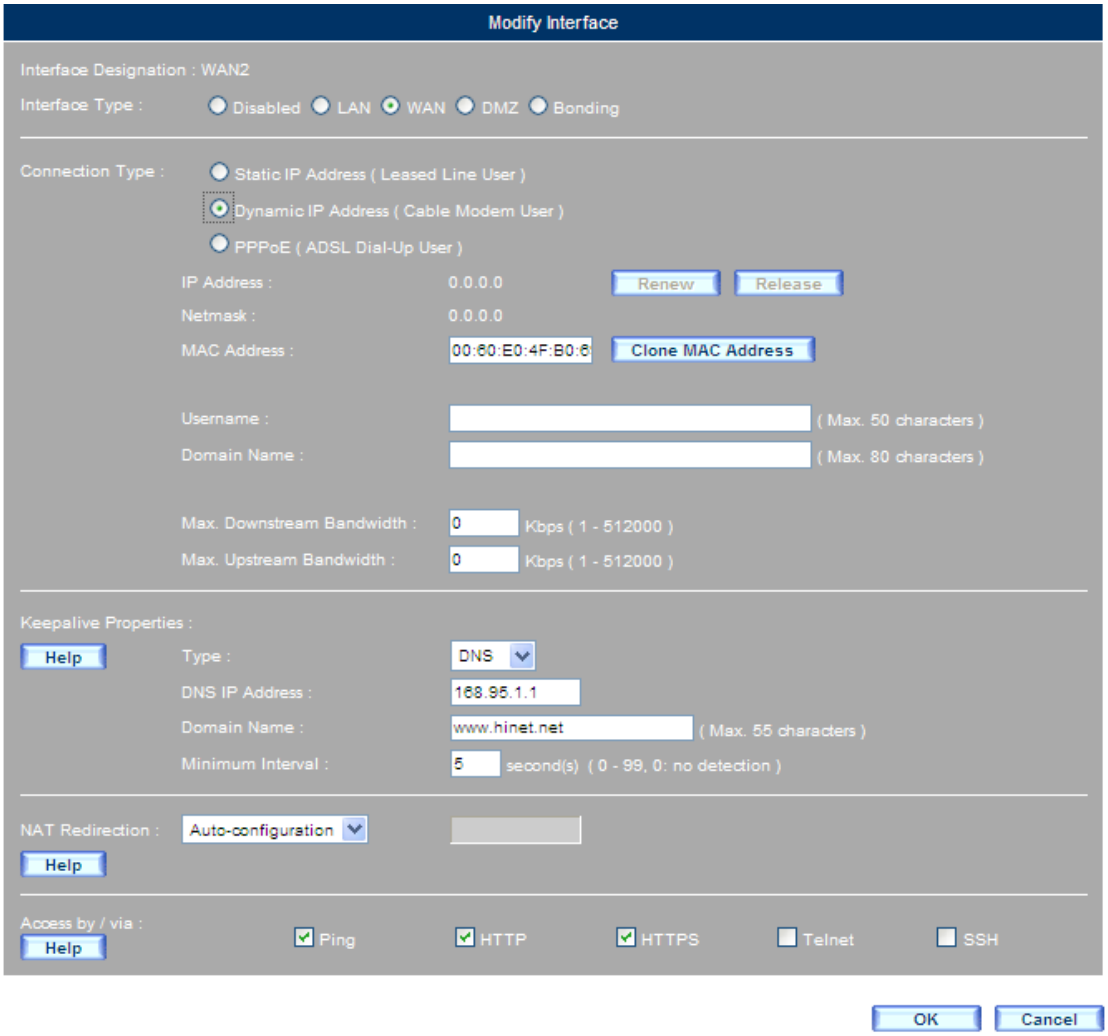


Figure 3-6 Configuring the Dynamic IP Address

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.10.1 / 255.255.255.0	---	Modify	---
2	DMZ1	NAT Routing	192.168.2.1 / 255.255.255.0	---	Modify	---
3	WAN2	Static IP	61.62.236.15 / 255.255.255.0	---	Modify	1
4	WAN1	Dynamic IP	203.73.66.63 / 255.255.255.255	---	Modify	2

Figure 3-7 Setting Completed

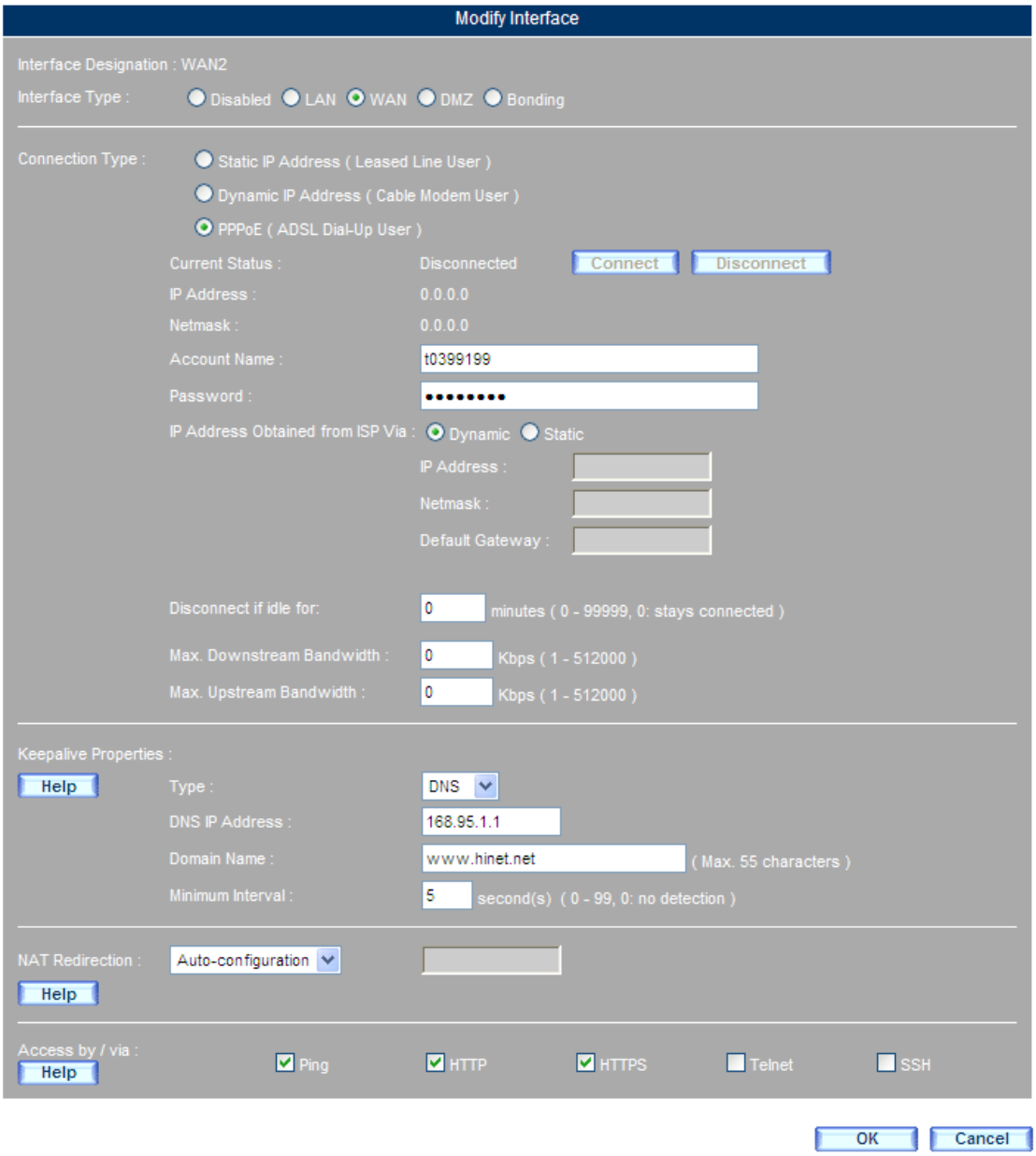


Figure 3-8 Configuring the PPPoE

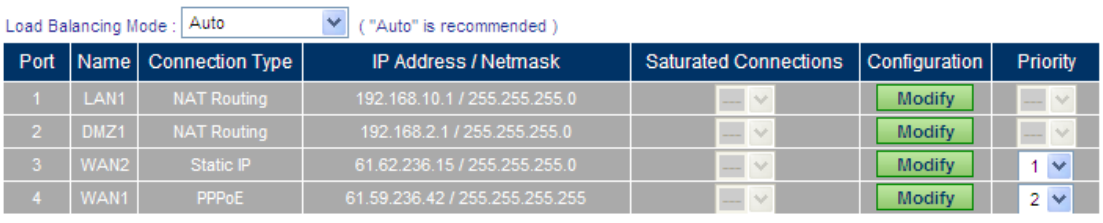


Figure 3-9 Setting Completed

Note：

1. The DNS Settings may be configured under **Network > Settings.**
2. When **Ping**, **HTTP** and **HTTPS** are enabled, the users may access the CS-2001 Web UI from external network. The access from the external network might affect the network security, thus it is suggested to disable **Ping**, **HTTP** and **HTTPS** after the configuration. If the IT administrator needs to access the Web UI from the external network, he or she may configure a Permitted IP under **System > Administration > Permitted IPs.**

3.1.3 Using CS-2001 as a Gateway for Users on Two Subnets to Access the Internet (NAT/Routing)

Prerequisite Setup (Note: IP Addresses used as examples only)
Configure Port1 as WAN1 (61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Configure Port2 as LAN1 (192.168.1.1, NAT/Routing) IP address range:192.168.20.x/24. User's PCs will connect to WAN1(61.11.11.11) to access the Internet.

Configure Port3 as LAN2 (192.168.2.1, NAT/Routing) IP address range:192.168.2.x/24. User's PCs will connect to WAN1(61.11.11.11) to access the Internet.

You may create the policy to establish the connection between LAN1 and LAN2.

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-10**）

- Click Port2's **Modify** button.
- Select LAN for **Interface Type.**
- Select NAT Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

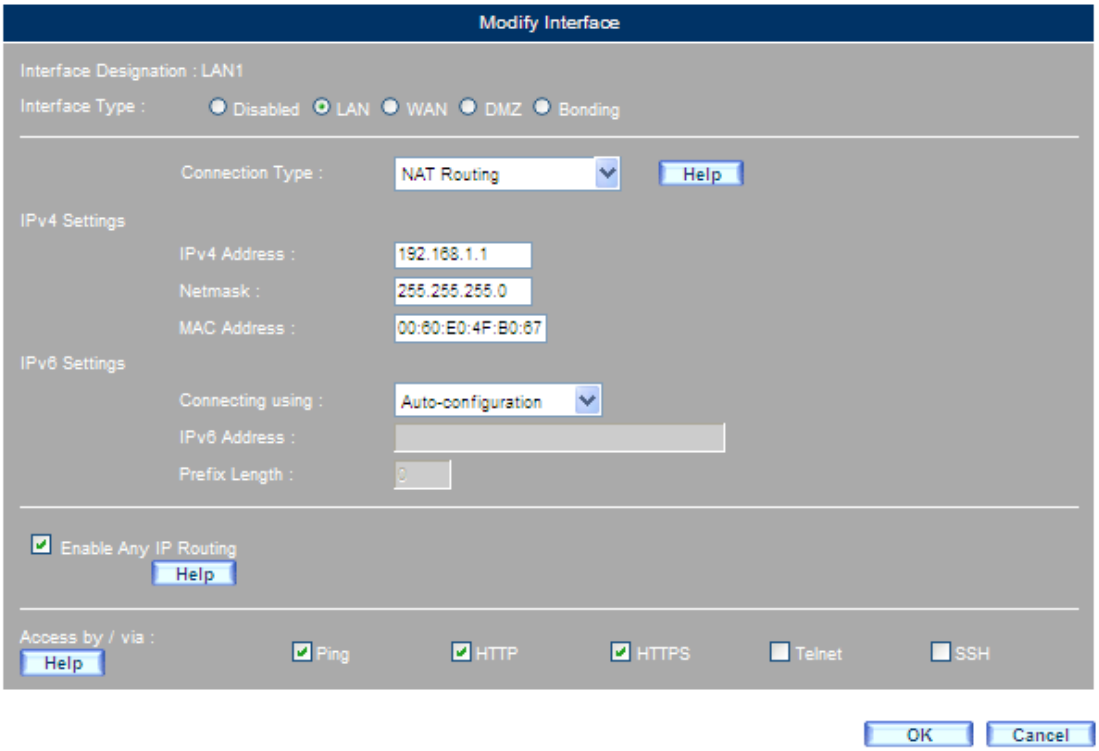


Figure 3-10 Configuring the LAN Interface

Step 2. Go to **Network** > **Interface** and then set as below:（**Figure 3-11**）

- Click Port3's **Modify** button.
- Select LAN for **Interface Type.**
- Select NAT Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

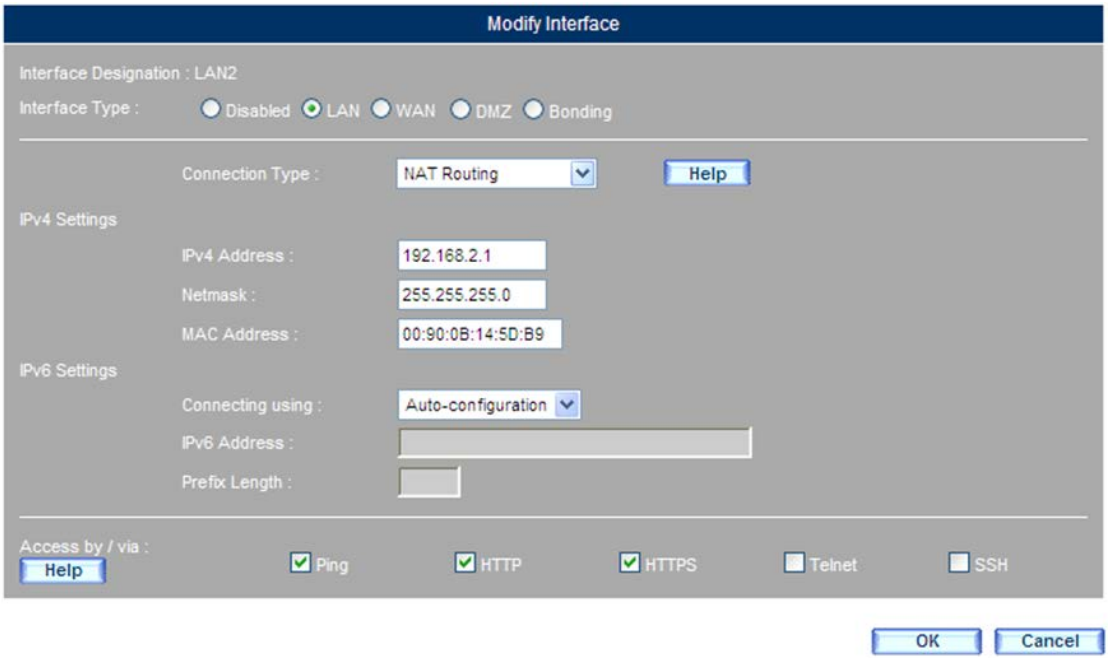


Figure 3-11 Configuring the LAN Interface

Step 3. LAN1 and LAN2 users will connect to WAN1(61.11.11.11) and use WAN1's IP address to access the Internet. You may create the policy to establish the connection between LAN1 and LAN2.（**Figure 3-12**）

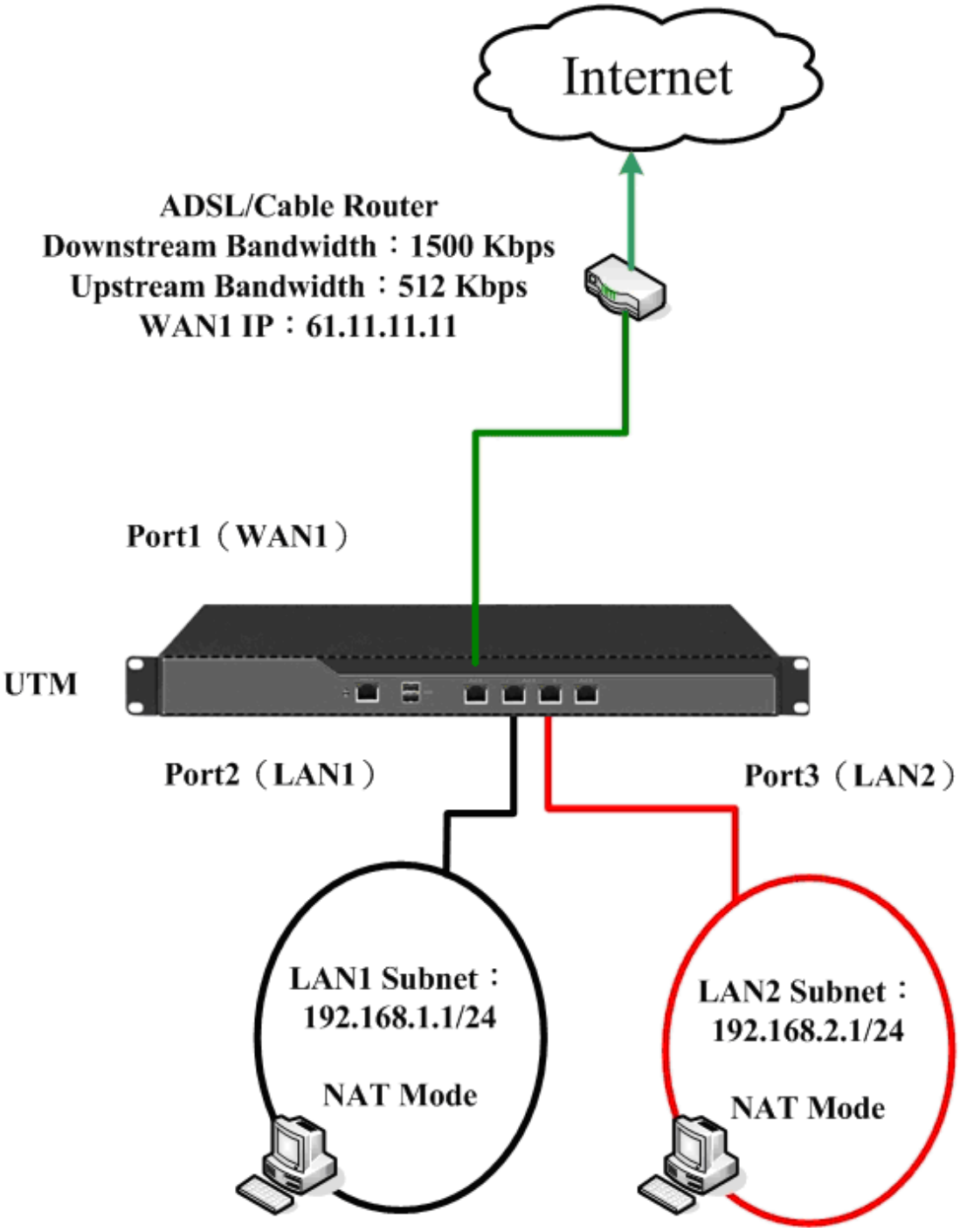


Figure 3-12 The Deployment of LAN using NAT / Routing Mode

3.1.4 Using CS-2001 as a Gateway for the Internal Users to Access the Internet and Configure the DMZ for the External Users to Access the Network Resource

Prerequisite Setup (Note: IP addresses used as examples only)

Configure Port1 as LAN1(192.168.1.1, NAT/Routing) and connect to the LAN. IP address range:192.168.1.x/24.

Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

LAN users (192.168.1.100) will connect to WAN1(61.11.11.11) and use WAN1's IP address to access the Internet.

Configure Port3 as DMZ1 (Transparent Routing) to connect to the web server. (Using WAN1's IP address: 61.11.11.12)

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-13**）

- Click Port1's **Modify** button.
- Select LAN for **Internet Type.**
- Select NAT Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK.**

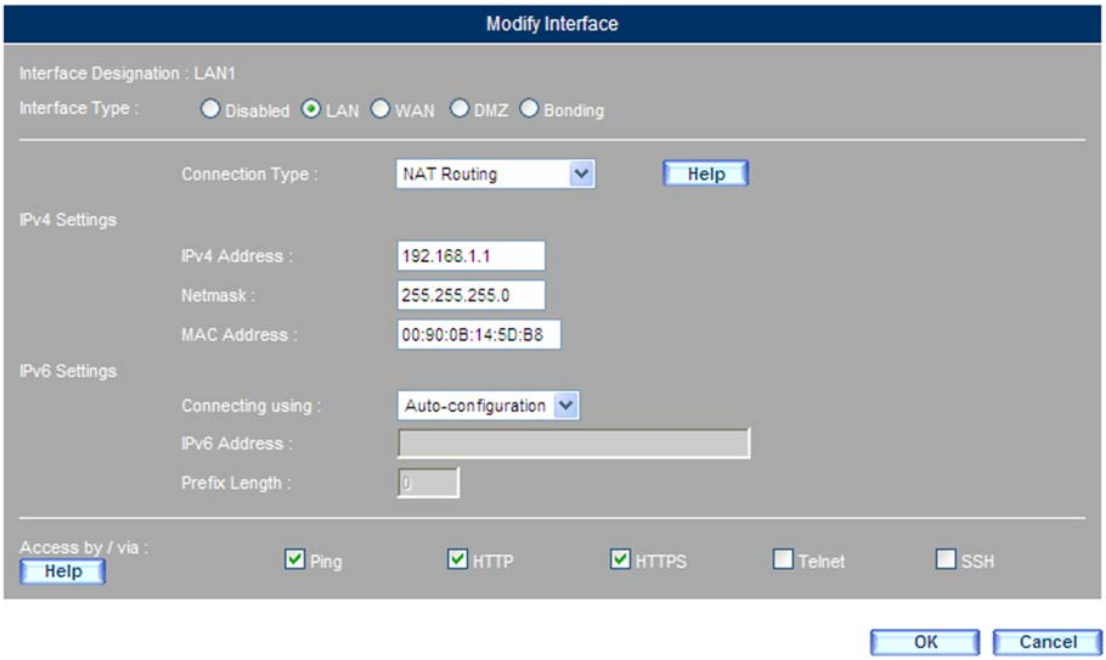


Figure 3-13 Configuring the LAN Interface

Step 2. Go to **Network** > **Interface** and then set as below:（**Figure 3-14**）

- Click Port3's **Modify** button.
- Select DMZ for **Interface Type.**
- Select Transparent Routing for **Connection Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

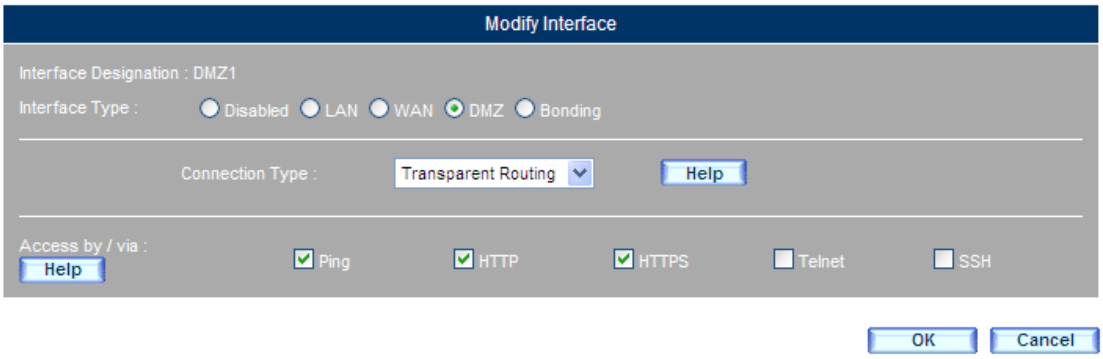


Figure 3-14 DMZ Interface Settings

Note：

1. WAN Interface must uses the static IP, then Transparent Routing can be selected for DMZ Interface settings.

Step 3. The external users may connect to the web server (61.11.11.12) to access the network resource. The LAN users may connect to WAN1 (61.11.11.11) and use WAN1's IP address to access the Internet.（Figure 3-15）

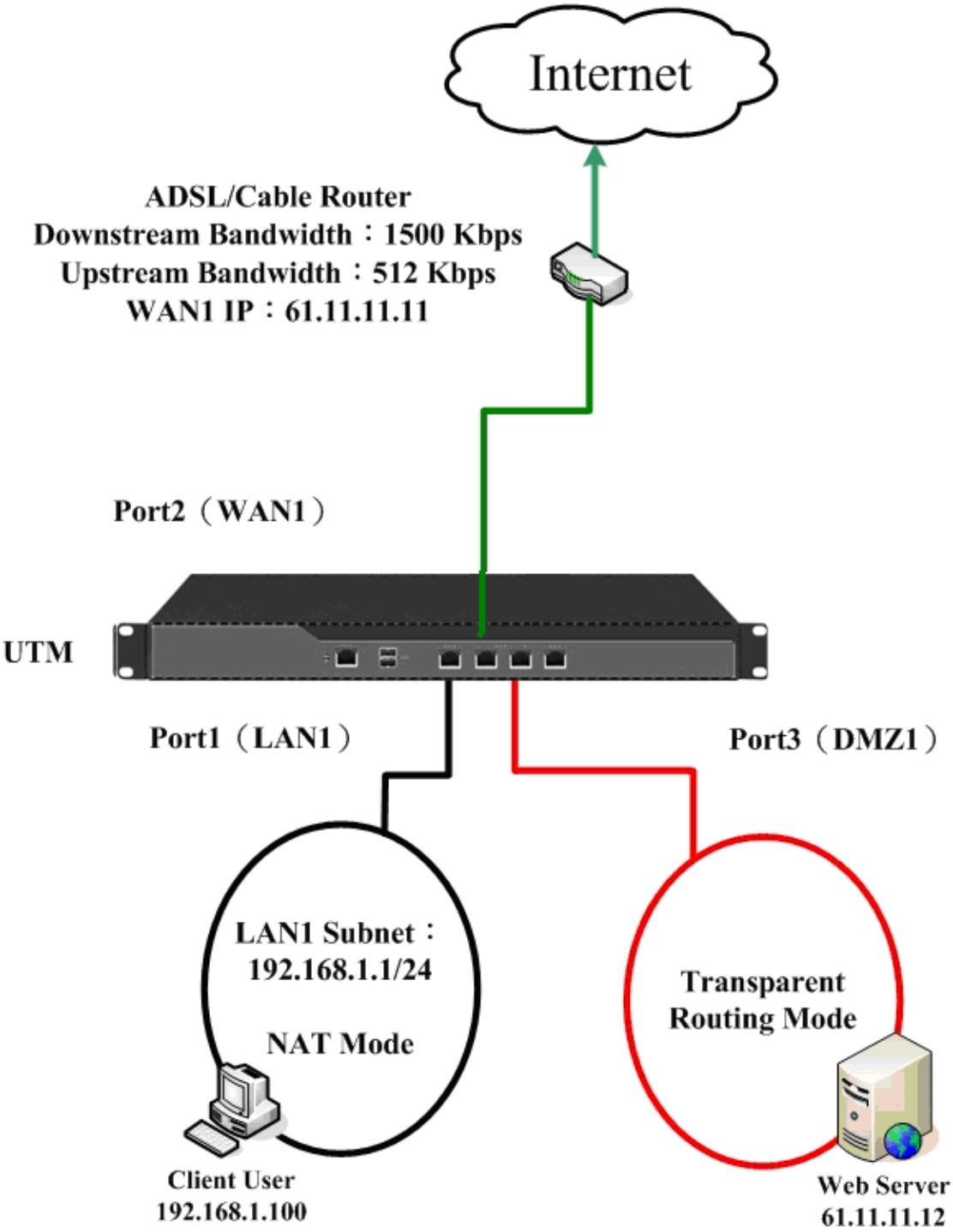


Figure 3-15 The Deployment of DMZ Using Transparent Routing Mode

3.1.5 Deploying the CS-2001 between the Gateway and LAN (configuring two subnets, one using Transparent Routing, the other one using NAT/Routing) for the LAN users to access the Internet

Prerequisite Setup (Note: IP addresses used as examples only)

Gateway's LAN IP addresses are 192.168.1.1 (192.168.1.x/24) and 192.168.2.1 (192.168.2.x/24).

Configure Port1 as WAN1(192.168.1.2) and connect it to the gateway's LAN.

Specify a static route, then packets that sent to 192.168.2.x/24 will be sent to WAN1.

Configure Port2 as LAN1 (Transparent Routing) and connect it to the LAN PCs (IP range:192.168.1.x/24, default gateway: 192.168.1.1) LAN PCs may use the original IP to access the Internet.

Configure Port3 as LAN2 (192.168.2.1, NAT/ Routng, IP range: 192.168.2.x/24) and connect it to the user's PC (default gateway: 192.168.2.1). LAN PCs may use the original IP to access the Internet.

You may create the policy to establish the connection between LAN1 and LAN2.

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-16**）

- Click Port2's **Modify** button.
- Select LAN for **Interface Type.**
- Select Transparent Routing for **Connection Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

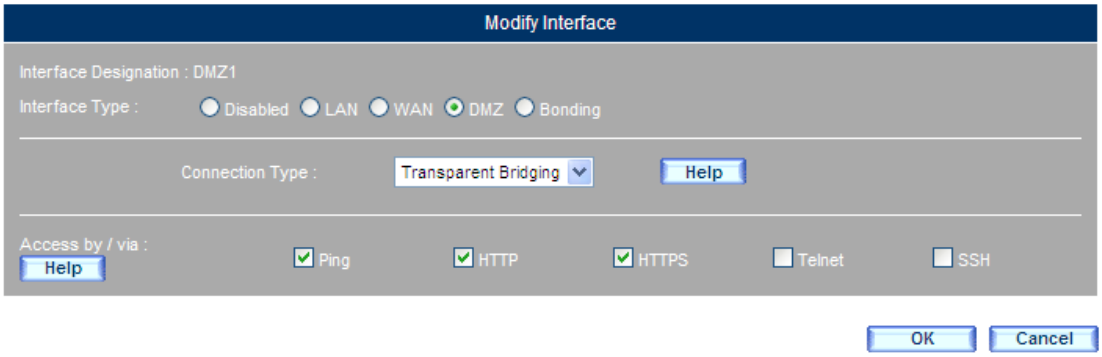


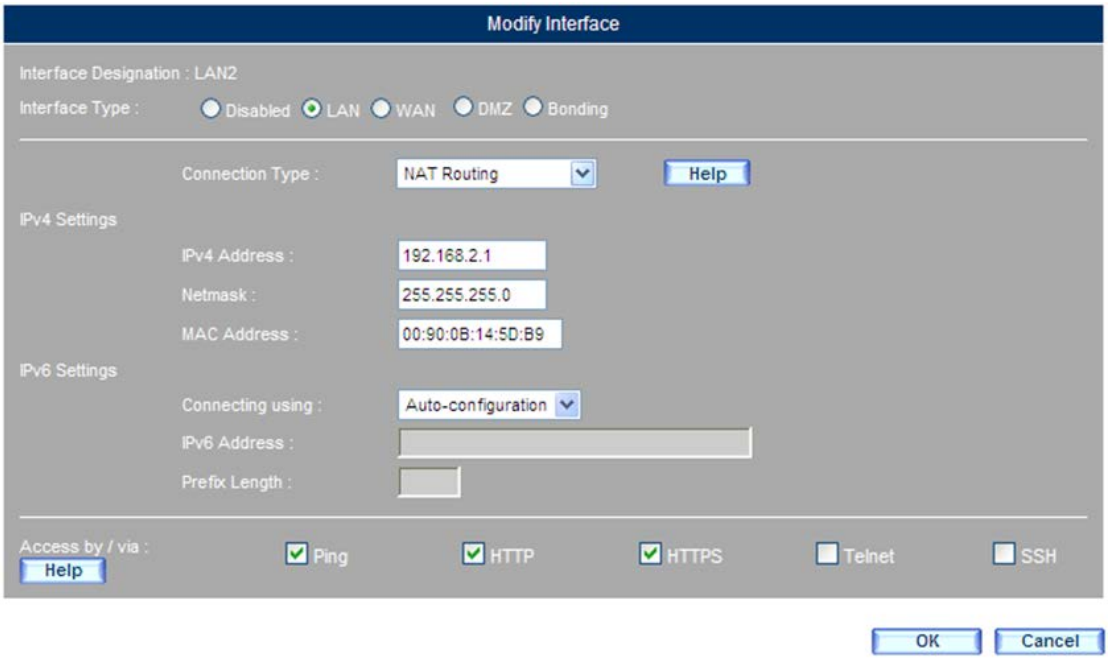
Figure 3-16 Configuring the LAN Interface

Step 2. Go to **Network** > **Interface** and then set as below:（**Figure 3-17**）

- Click Port3's **Modify** button.
- Select LAN for **Interface Type.**
- Select NAT Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

Figure 3-17 LAN

I



nterface Settings

Step 3. LAN1 users (192.168.1.x/24) and LAN2 users (192.168.2.x/24) may use their original IP addresses to access the Internet via the CS-2001. You may create the policy to establish the connection between LAN1 and LAN2. **（Figure 3-18）**

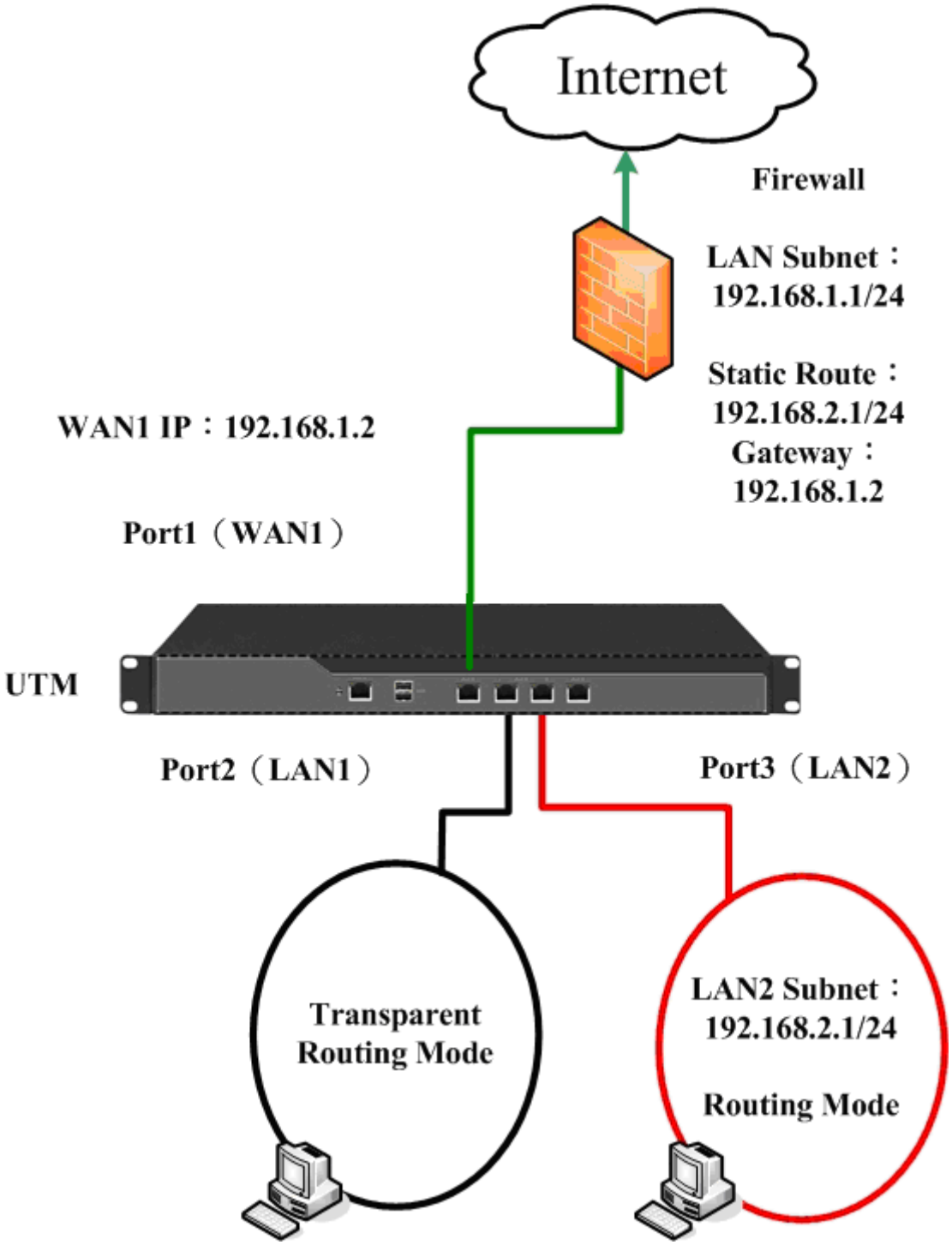


Figure 3-18 The deployment of LAN Using Transparent Routing and NAT/ Routing

3.1.6 Deploying the CS-2001 between the Gateway and the LAN (LAN1 and DMZ1), connecting LAN1 to the user's PC (using NAT/Routing mode) and then connecting DMZ1 to user's PC (using Transparent Bridging mode)

Prerequisite Setup (Note: IP addresses used as examples only)
Gateway's LAN (172.16.1.1). IP range: 172.16.x.x/16.

Configure Port1 as LAN1(192.168.1.1, NAT/Routing, IP range:192.168.1.x/24) and connect it to the user's PC (default gateway: 192.168.1.1). PCs will connect to WAN1(172.16.1.12) and use WAN1's IP address to access the Internet.

Configure Port2 as WAN1(172.16.1.12) and connect it to gateway's LAN.

Configure Port3 as DMZ1(using Transparent Bridging mode) and connect it to PCs (IP range:172.16.x.x/16, default gateway: 172.16.1.1). PCs will use the original addresses to access the Internet.

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-19**）

- Click Port1's **Modify** button.
- Select LAN for **Interface Type.**
- Select NAT Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

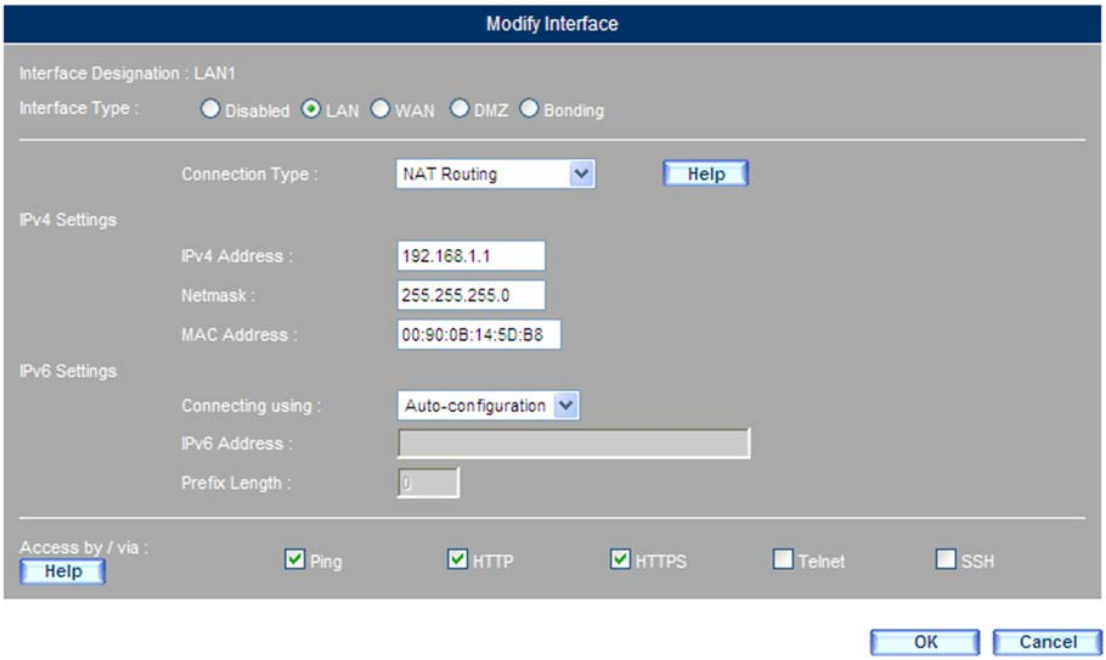


Figure 3-19 LAN Interface Settings

Step 2. Under **Network** > **Interface**, set as below:（**Figure 3-20**）

- Click Port3's **Modify** button.
- Select DMZ for **Interface Type.**
- Select Transparent Bridging for **Connecion Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK.**

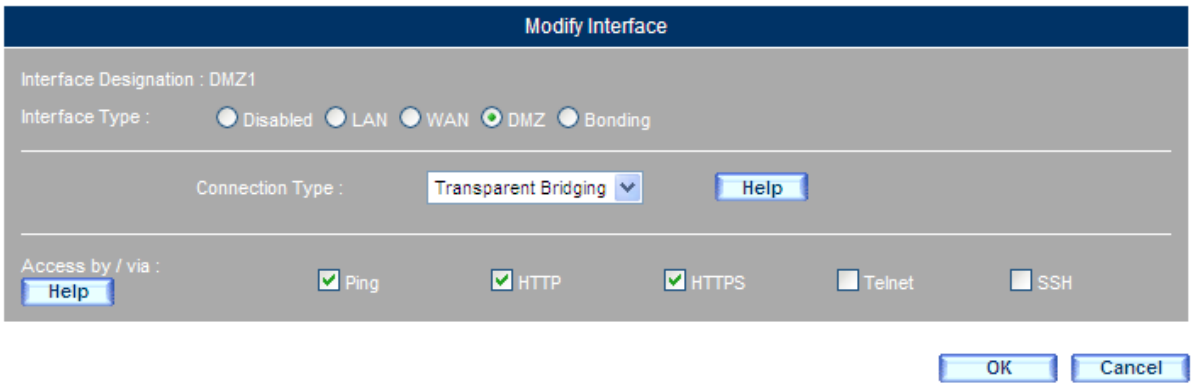


Figure 3-20 DMZ Interface Settings

Step 3. Go to **Network** > **Interface Group** and then set as below:（**Figure 3-21**）

- Configure **Port2(WAN1)** and **Port3(WAN2)** as Group1.
- Click **OK.**

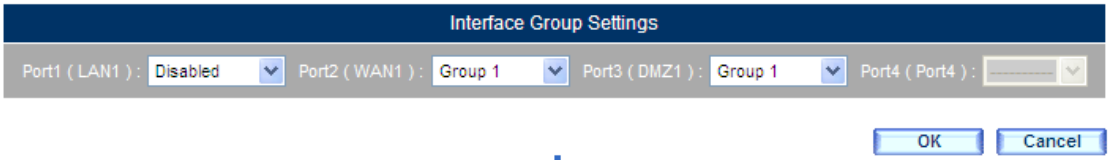


Figure 3-21 Configuring the Interface Group

Step 4. PCs (IP range: 172.16.x.x/16) on DMZ may use the original address to access the Internet through CS-2001. PCs on LAN will connect to WAN1 (172.16.1.12) and use WAN1's IP address to access the Internet.(**Figure 3-22**)

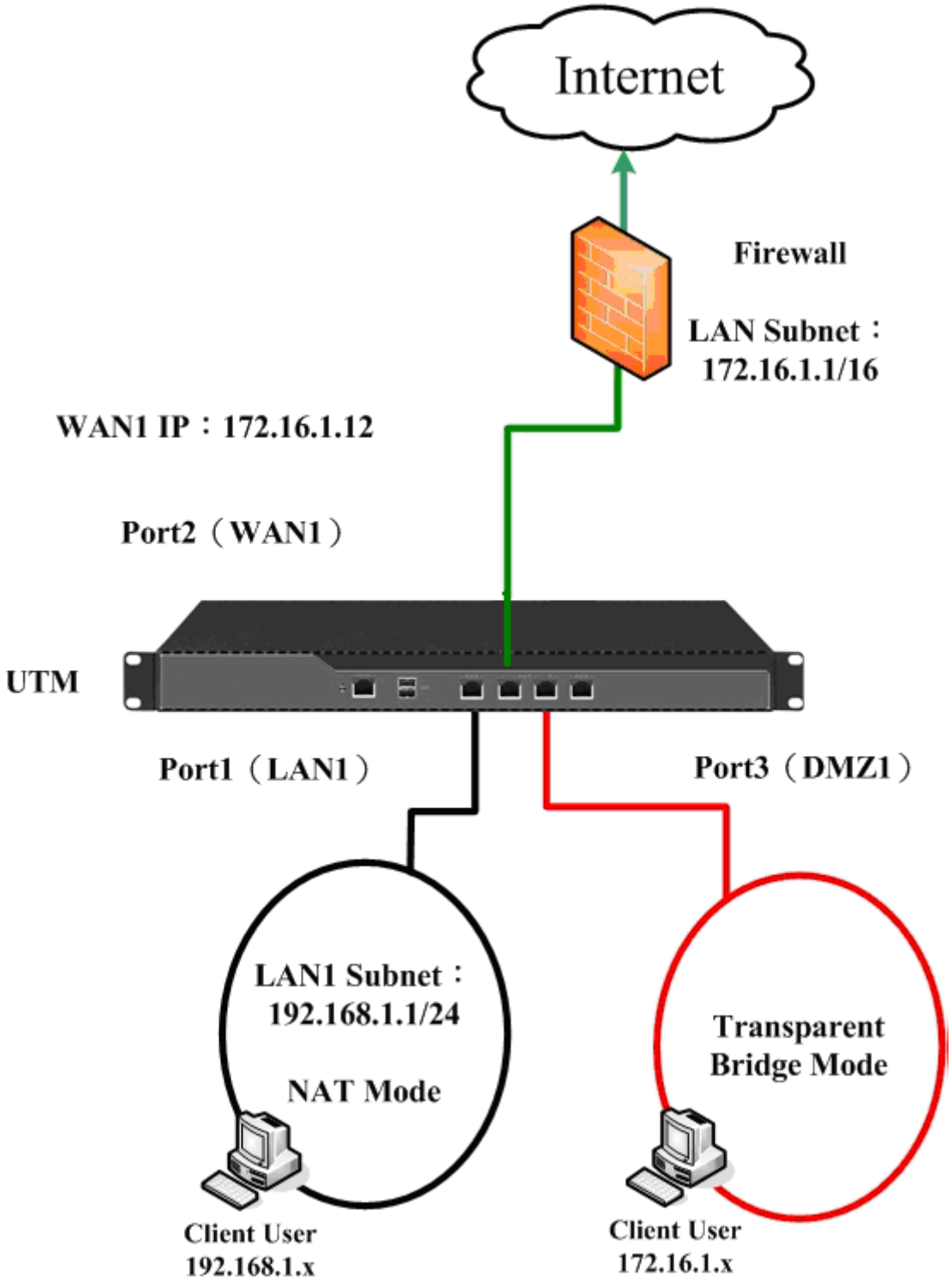


Figure 3-22 The Deployment of DMZ Using Transparent Bridging Mode

Note：

1. PCs in DMZ will access the Internet via the original firewall.
2. If Port4 is configured as WAN2 (211.22.22.22) and connected to the ADSL Termination Unit Remote (ATUR) to access the Internet.（**Figure 3-23**）
   - PCs in DMZ (172.16.x.x/16):
     - The LAN PCs (default gateway:172.16.1.1) will access the Internet through CS-2001's WAN1.
     - Configure the default gateway as CS-2001's WAN1 (172.16.1.12). Packets pass through the CS-2001 will use WAN1(172.16.1.12) or WAN2(211.22.22.22) to access the Internet. (Load Balancing)
   - PCs in LAN (192.168.1.x/24):
     - Configure the default gateway as CS-2001's LAN1 (192.168.1.1). Packets pass through CS-2001 will use WAN1(172.16.1.12) or WAN2(211.22.22.22) to access the Internet. (Load Balancing)

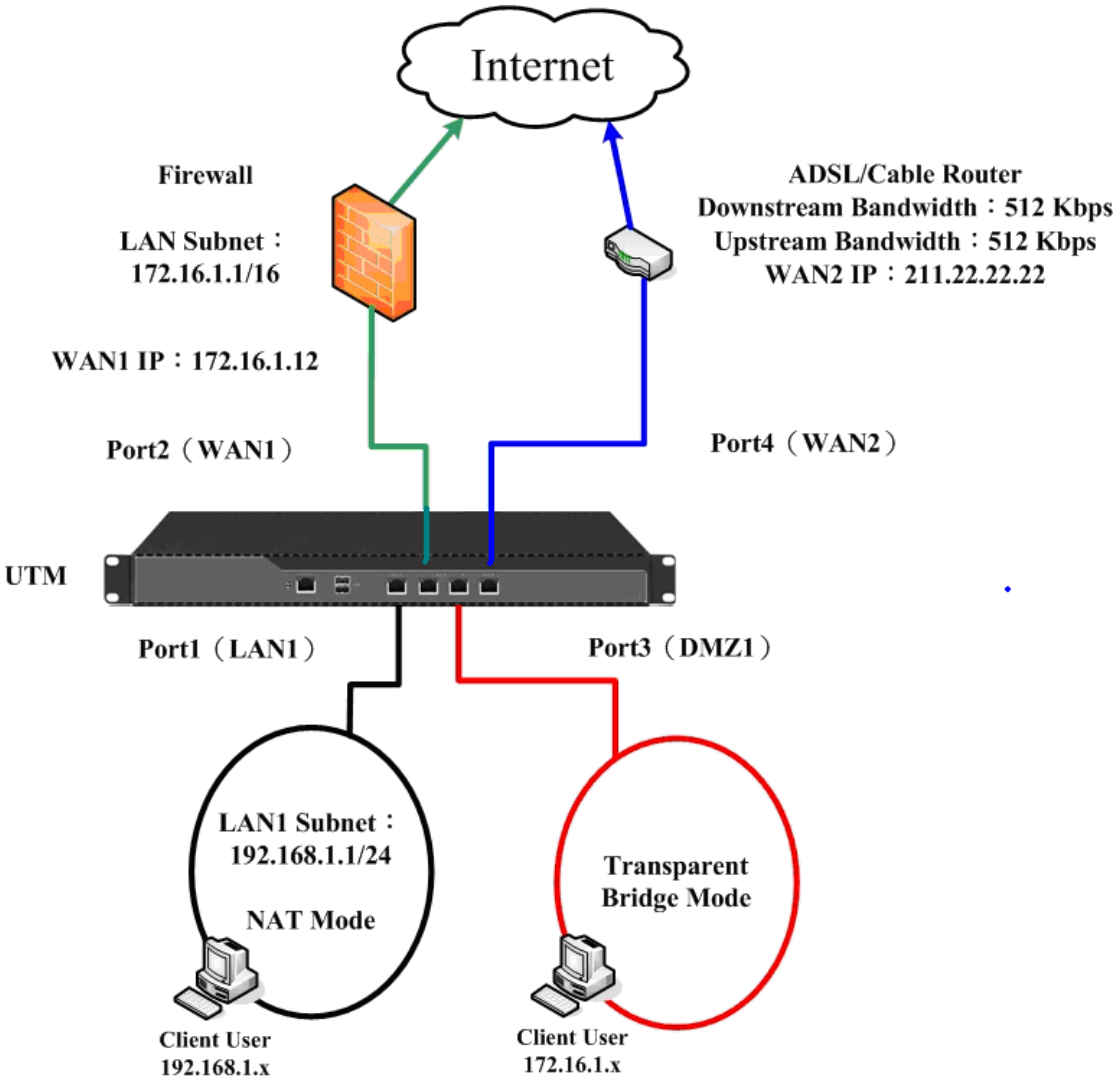


Figure 3-23 The Deployment of DMZ Using Transparent Bridging Mode 02

3. Configure a router to connect different subnets in LAN for the PCs to access the Internet through the original firewall. PCs in DMZ may using the original IP address to access the Internet through CS-2001's WAN1.（**Figure 3-24**）

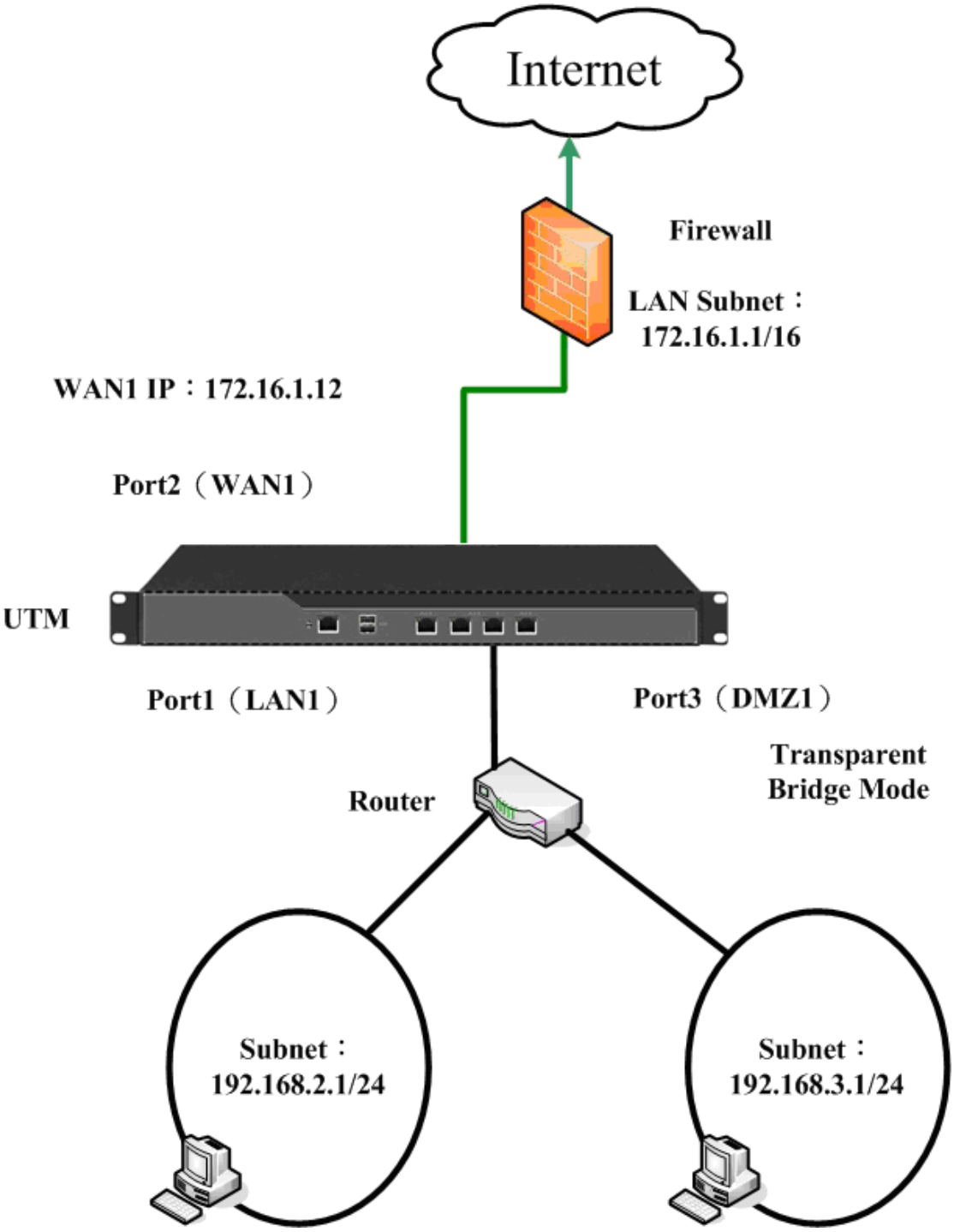


Figure 3-24 The Deployment of DMZ Using Transparent Bridging 03

4. Configure two Firewall to connect the Internet and the CS-2001 and then configure a router to connect the CS-2001 and DMZ (192.168.2.1/24 and 192.168.3.1/24). Connect the two subnets to WAN1's firewall and WAN2's firewall individually. Then, the packets from the two subnets will be sent to WAN1 or WAN2 according to the default gateway settings.（**Figure 3-25**）

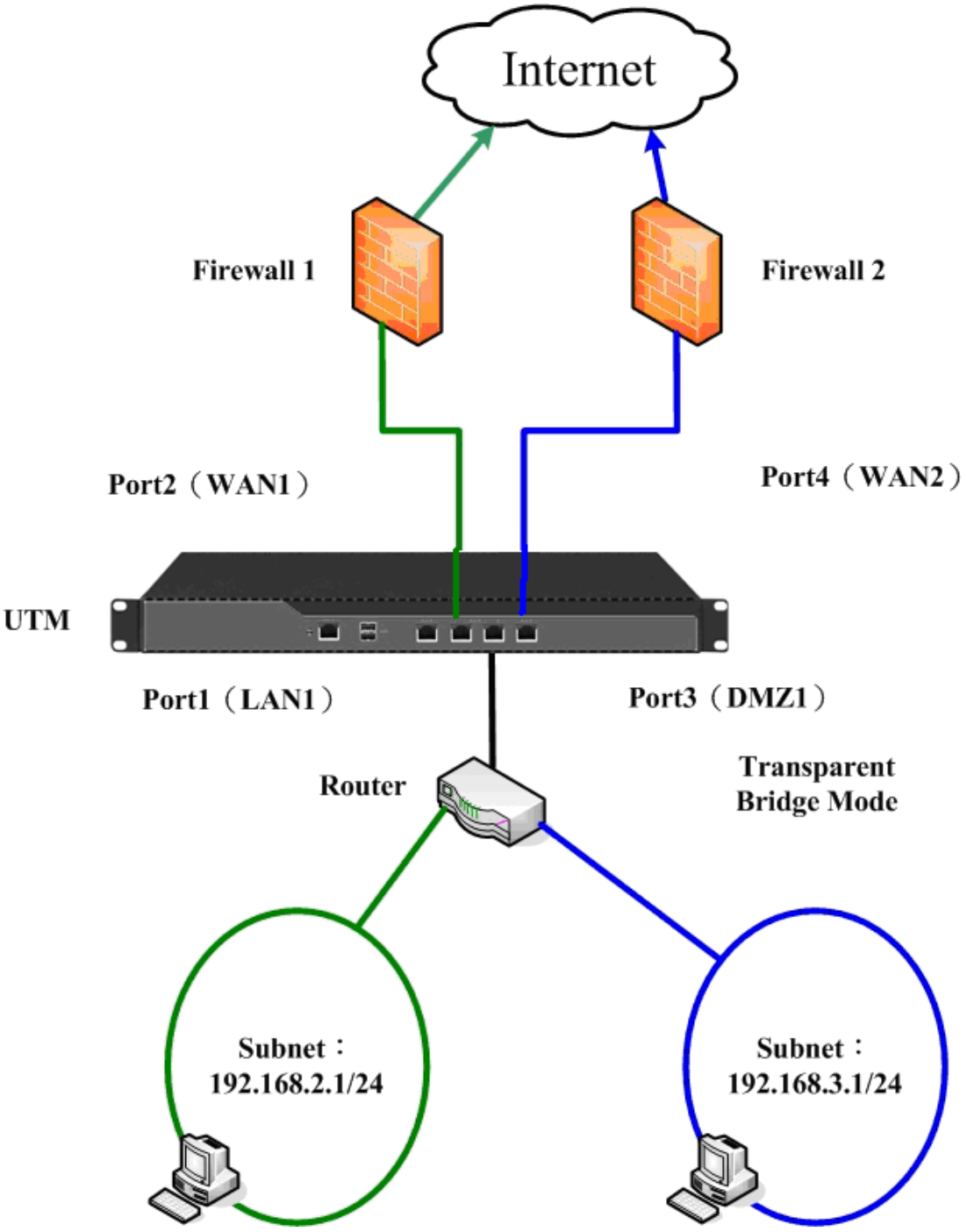


Figure 3-25 The Deployment of DMZ Using Transparent Bridging Mode 04

3.1.7 Deploying CS-2001 between the Gateway and LAN (LAN1 and DMZ1) for LAN Users and DMZ Users to Access the Internet

Prerequisite Setup (Note: IP addresses used as examples only)

Gateway: LAN(192.168.1.1), IP range:192.168.1.x/24
WAN(61.11.11.11) connects to the ADSL Termination Unit Remote to access the Internet.
DMZ (Transparent mode)

Configure Port1 as WAN1 (192.168.1.2) and connect it to the gateway's LAN.

Configure Port2 as LAN1(Transparent Bridging mode) and connect to the LAN PCs (IP range: 192.168.1.x/24, default gateway: 192.168.1.1). LAN PCs may uses the original IP address to access the Internet.

Configure Port3 as WAN2 (61.11.11.12) and connect to the gateway's DMZ.

Configure Port4 as DMZ1 (Transparent Bridging mode) and connect it to the server in DMZ (using WAN2's IP address). PCs may use the original IP addresses to access the Internet.

Step 1. Go to **Network** > **Interface** and then set as below:（**Figure 3-26**）

- Click Port1's **Modify** button.
- Select WAN for **Interface Type.**
- Select the **Connection Type.**
- Configure the connection settings.
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

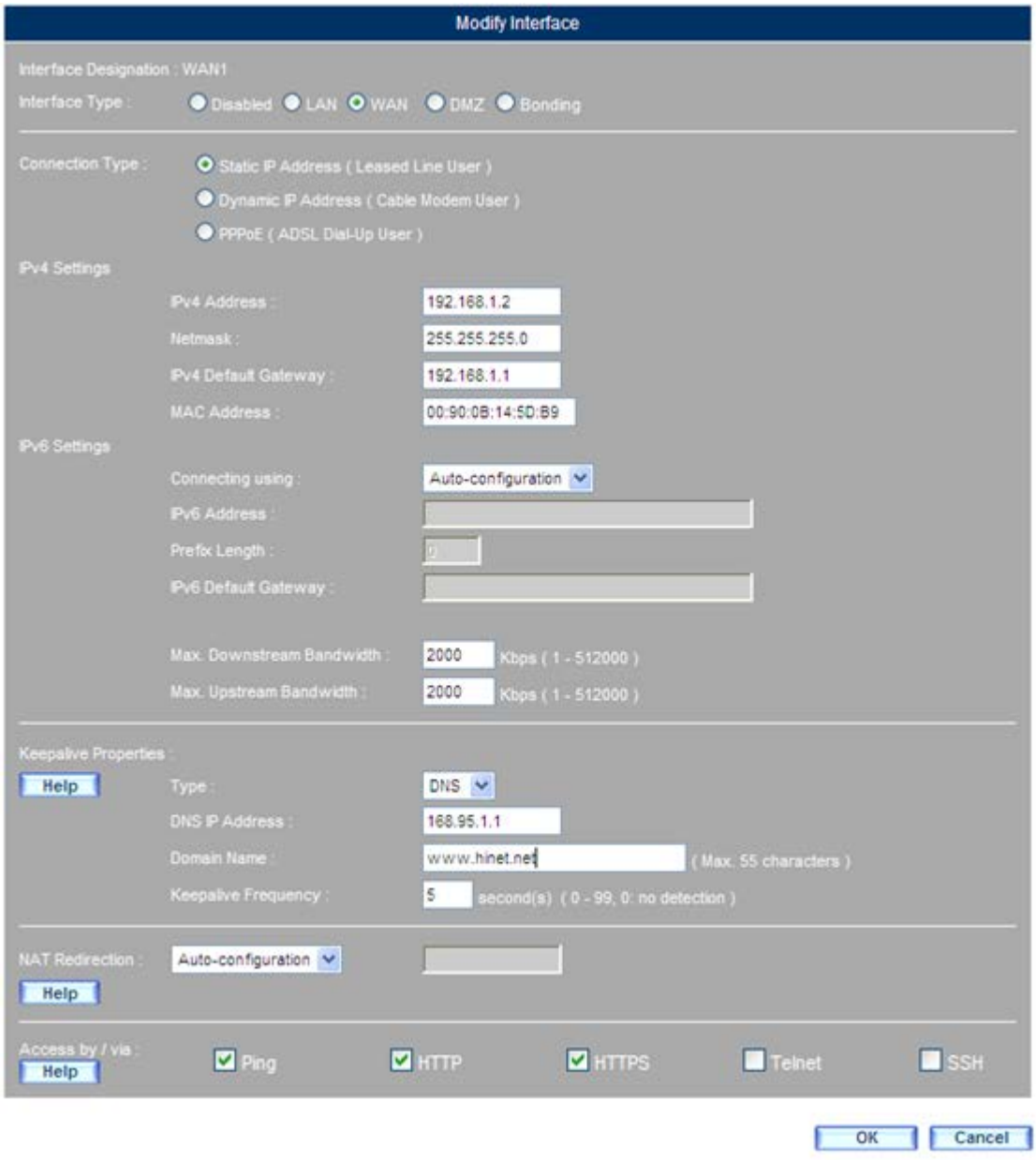


Figure 3-26 Configuring the WAN Interface

Step 2. Under **Network** > **Interface**, set as below: (**Figure 3-27**)

- Click Port2's **Modify** button.
- Select LAN for **Interface Type.**
- Select Transparent Bridging for **Connection Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

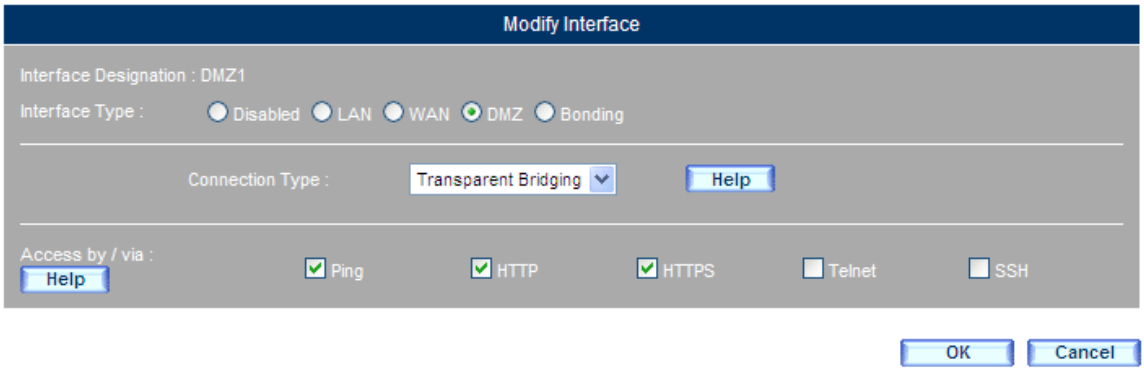


Figure 3-27 LAN Settings Using Transparent Bridging Mode

Step 3. Under **Network** > **Interface** and then set as below: (**Figure 3-28**)

- Click Port3's **Modify** button.
- Select WAN for **Interface Type.**
- Select the **Connection Type.**
- Configure the connection settings.
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK.**

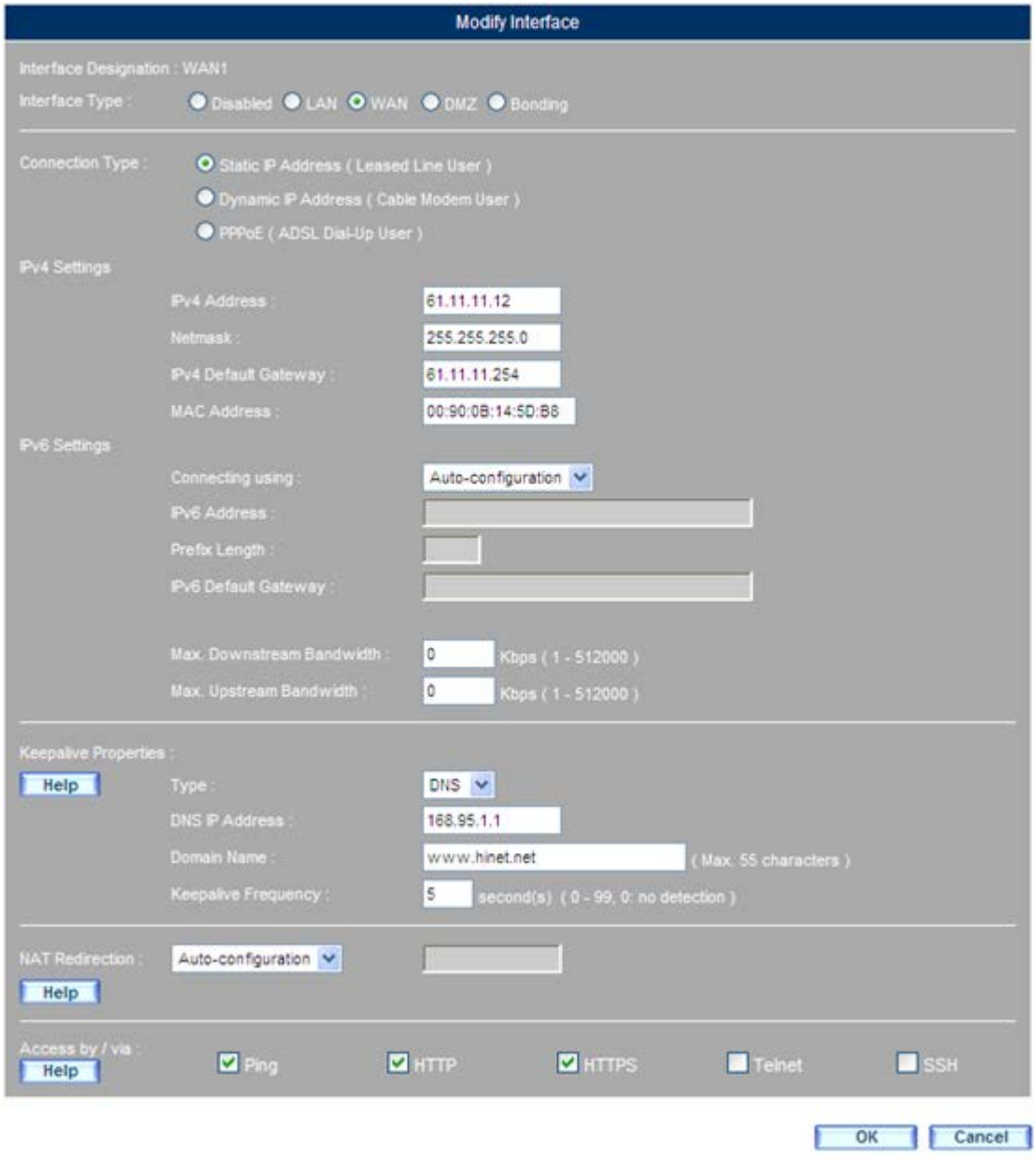


Figure 3-28 Configuring the WAN Interface

Step 4. Under **Network** > **Interface**, set as below:（**Figure 3-29**）

- Click Port4's **Modify** button.
- Select DMZ for **Interface Type.**
- Select Transparent Bridging for **Connection Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

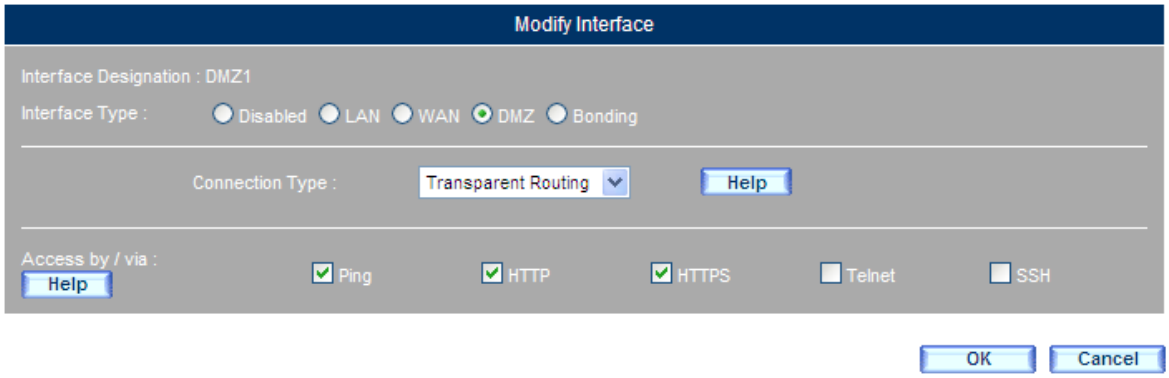


Figure 3-29 DMZ Interface Using Transparent Bridging

Step 5. Go to **Network** > **Interface Group** and then set as below:（**Figure 3-30**）

- Configure **Port1(WAN1)** and **Port2(LAN1)** as Group 1.
- Configure **Port3(WAN2)** and **Port4(DMZ1)** as Group2.
- Click OK.

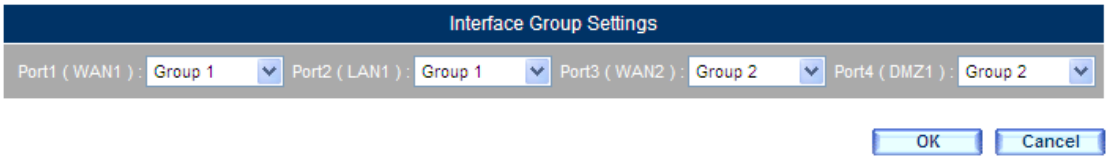


Figure 3-30 Interface Group Settings

Important：

1. Then, the CS-2001 may operate as two individual switches. Port1(WAN1) and Port2 (LAN1) connect to the LAN, Port3(WAN2) and Port4(DMZ1) connect to the DMZ. The PCs under two different switches may not connect to each other.

Step 6. Users connecting to Port2(LAN1) will use 192.168.1.x/24 to access the Internet. Users on Port4(DMZ1) will use the IP address that distributed by the ISP to access the Internet.（Figure 3-31）

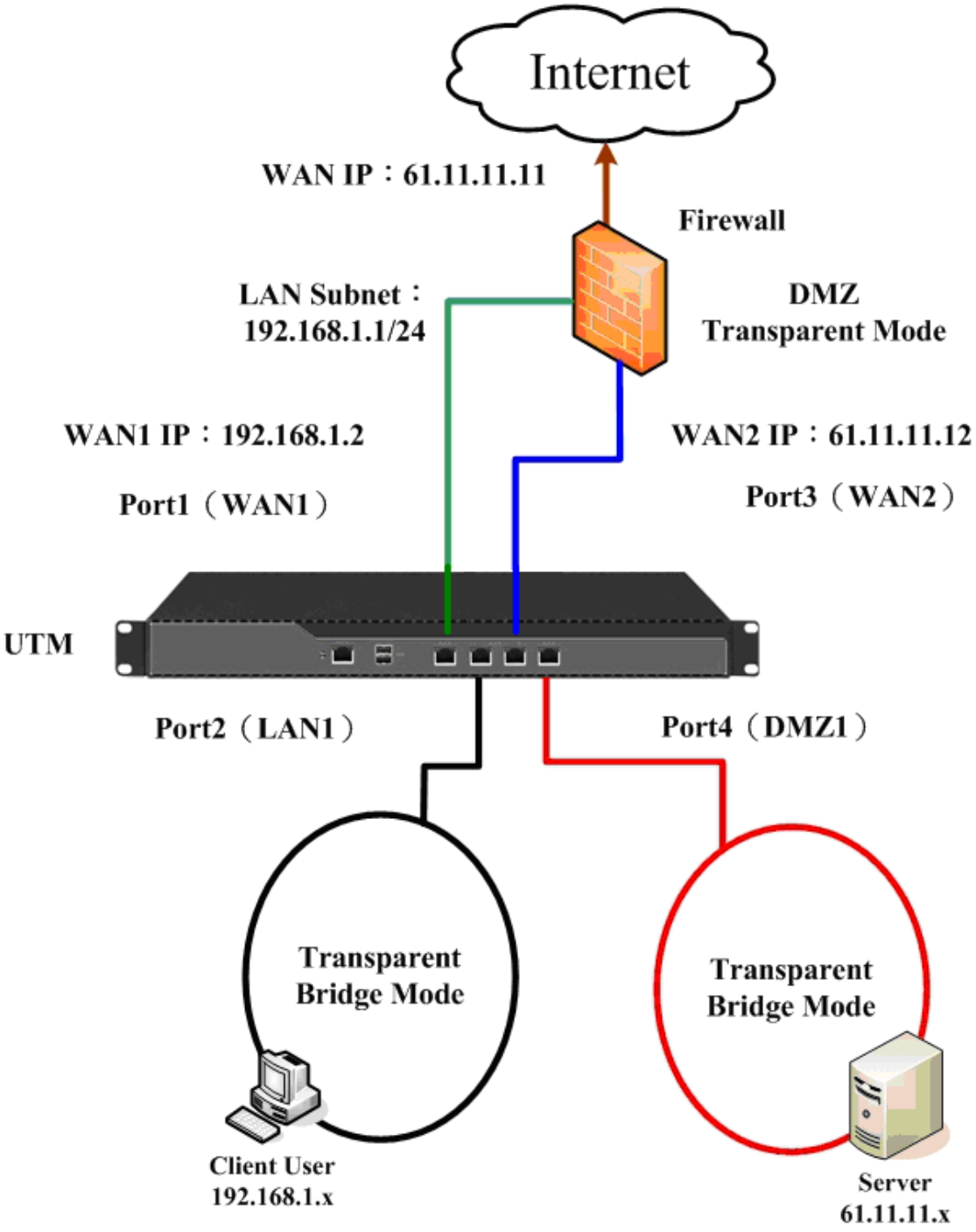


Figure 3-31 Interface Group Deployment

3.1.8 Using the CS-2001 Device as the Gateway and Connecting it to the LAN (There are Two LAN Interface, One Use NAT/Routing, the Other One Use Transparent Bridging Mode) for the LAN Users to Access the Internet

Prerequisite Setup (Note: IP Addresses used as examples only)

Configure Port1 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Configure Port2 as LAN1 (192.168.1.1, NAT/Routing, IP range: 192.168.1.x/24) and connect it to the PCs under sales department (default gateway: 192.168.1.1). PCs will connect to WAN1 (61.11.11.11) and use WAN1's IP address to access the Internet.

Configure Port3 as LAN2 (Transparent Bridging, IP range: 192.168.1.x/24) and connect it to the PCs under support department (default gateway: 192.168.1.1). PCs will connect to WAN1(61.11.11.11) and use WAN1's IP address to access the Internet.

You may create the policy to establish the connection between LAN1 and LAN2.

Step 1. Go to **Network** > **Interface** and set as below: (**Figure 3-32**)

- Click Port1's **Modify** button.
- Select WAN for **Interface Type.**
- Select the **Connection Type.**
- Configure the connection settings.
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

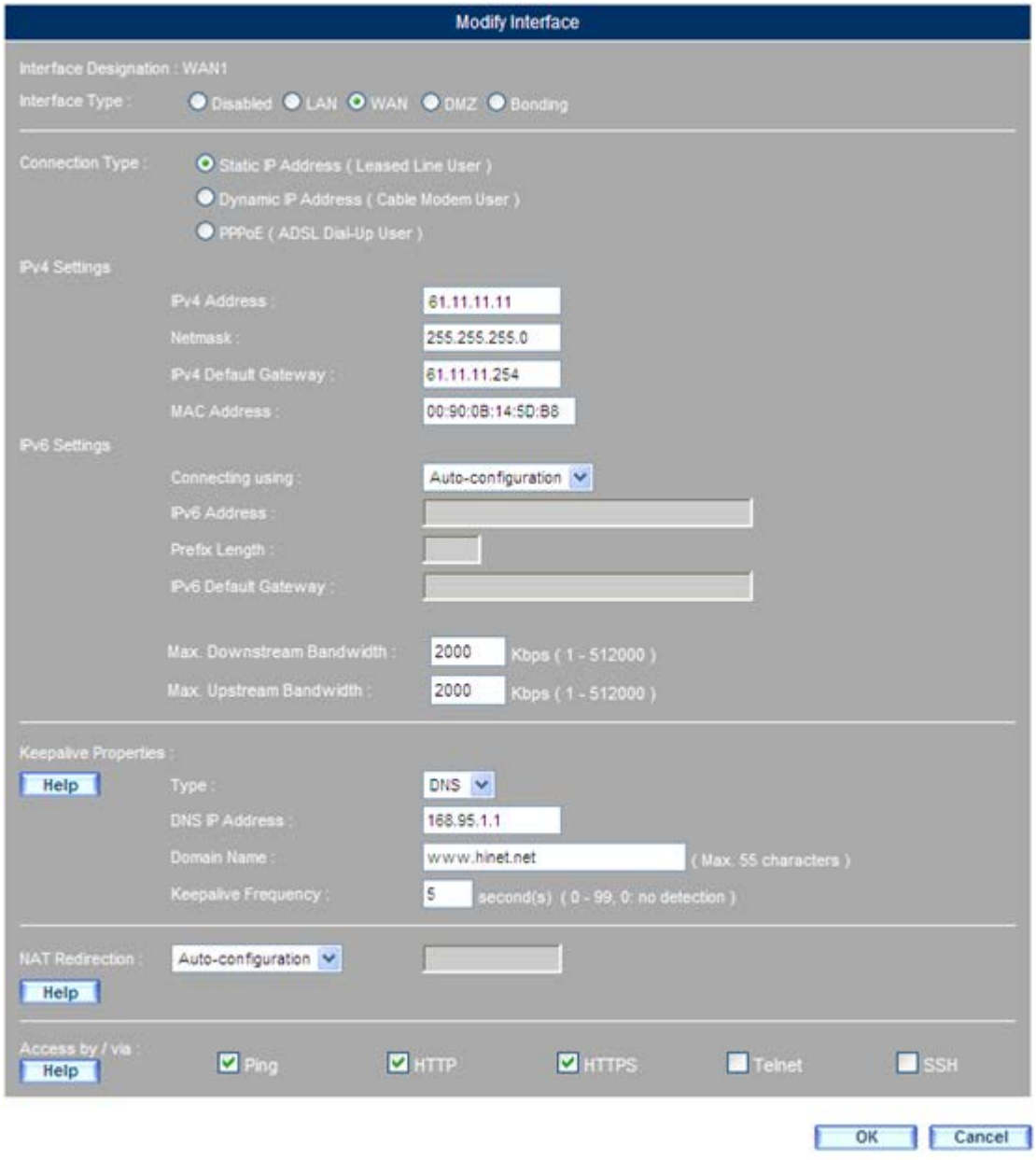


Figure 3-32 WAN Interface Settings

Step 2. Go to **Network** > **Interface** and then set as below:（**Figure 3-33**）

- Click Port2's **Modify** button.
- Select LAN for **Interface Type.**
- Select NAT/Routing for **Connection Type.**
- Enter the **IPv4 Address** and the **Netmask.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK.**

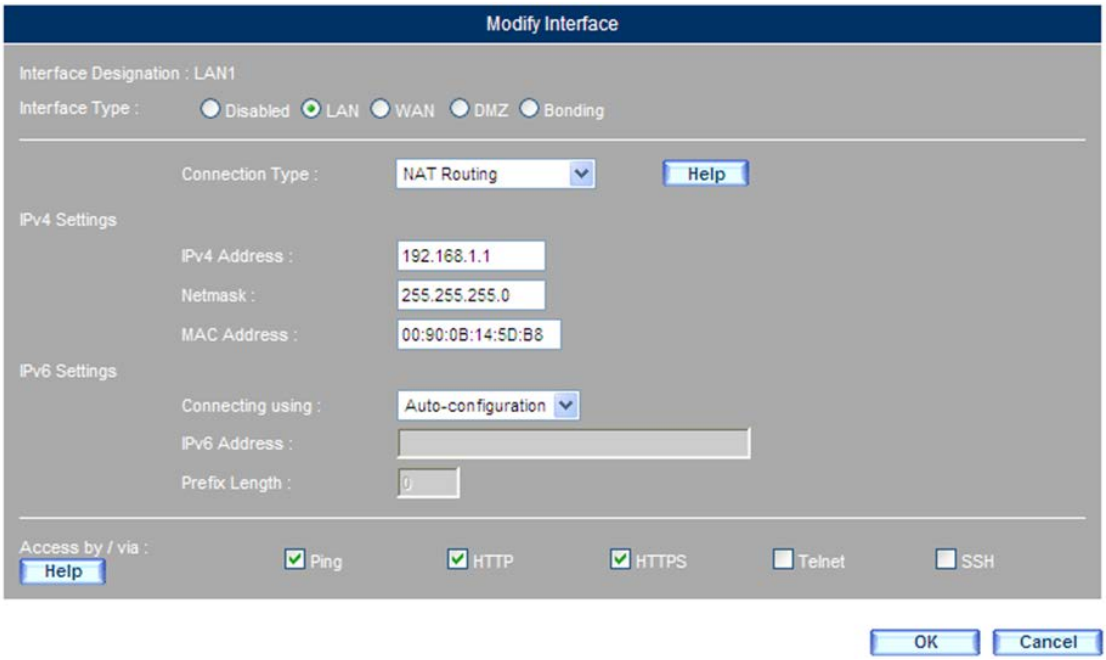


Figure 3-33 LAN Interface Settings

Step 3. Go to **Network** > **Interface** and set as below:（**Figure 3-34**）

- Click Port3's **Modify** button.
- Select LAN for **Interface Type.**
- Select Transparent Bridging for **Connection Type.**
- Tick **Ping**, **HTTP** and **HTTPS.**
- Click **OK**.

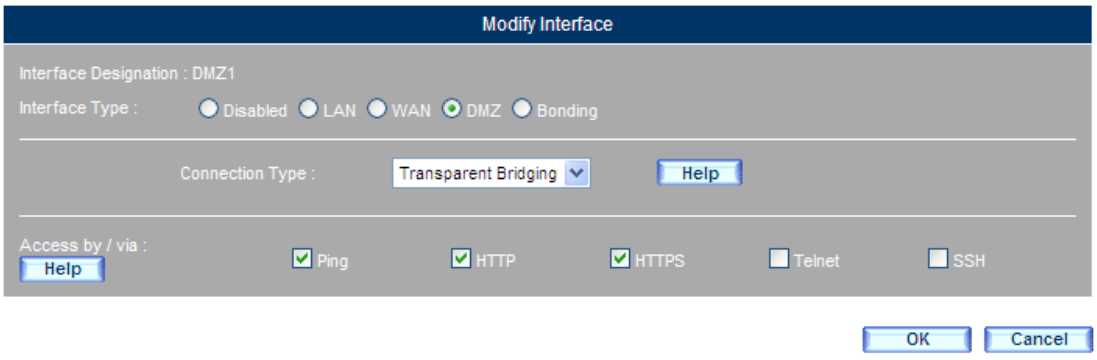


Figure 3-34 LAN Interface Settings

Step 4. Go to **Network** > **Interface Group** and then set as below:（**Figure 3-35**）

- Configure **Port1(WAN1)**, **Port2(LAN1)** and **Port3(LAN2)** as Group 1.
- Click **OK.**

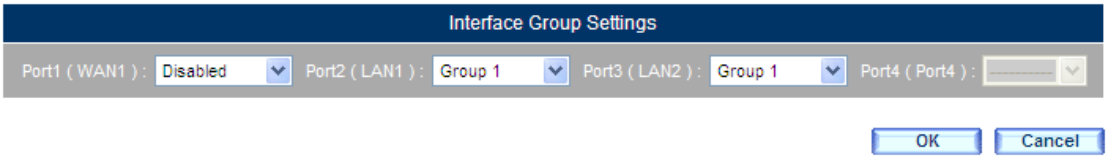


Figure 3-35 Interface Group Settings

Note：

1. Then, users on the same subnet may be divided into different interface according to their departments. For example, Port2(LAN1) connects to PCs under sales department, and Port3(LAN2) connects to PCs under support department.

Step 5. PCs under sales department (LAN1) and PCs under support department (LAN2) are on 192.168.1.x/24. They will connect to WAN1 and use WAN1's IP address (61.11.11.11) to access the Internet. You may create the policy to establish the connection between LAN1 and LAN2.（**Figure 3-36**）

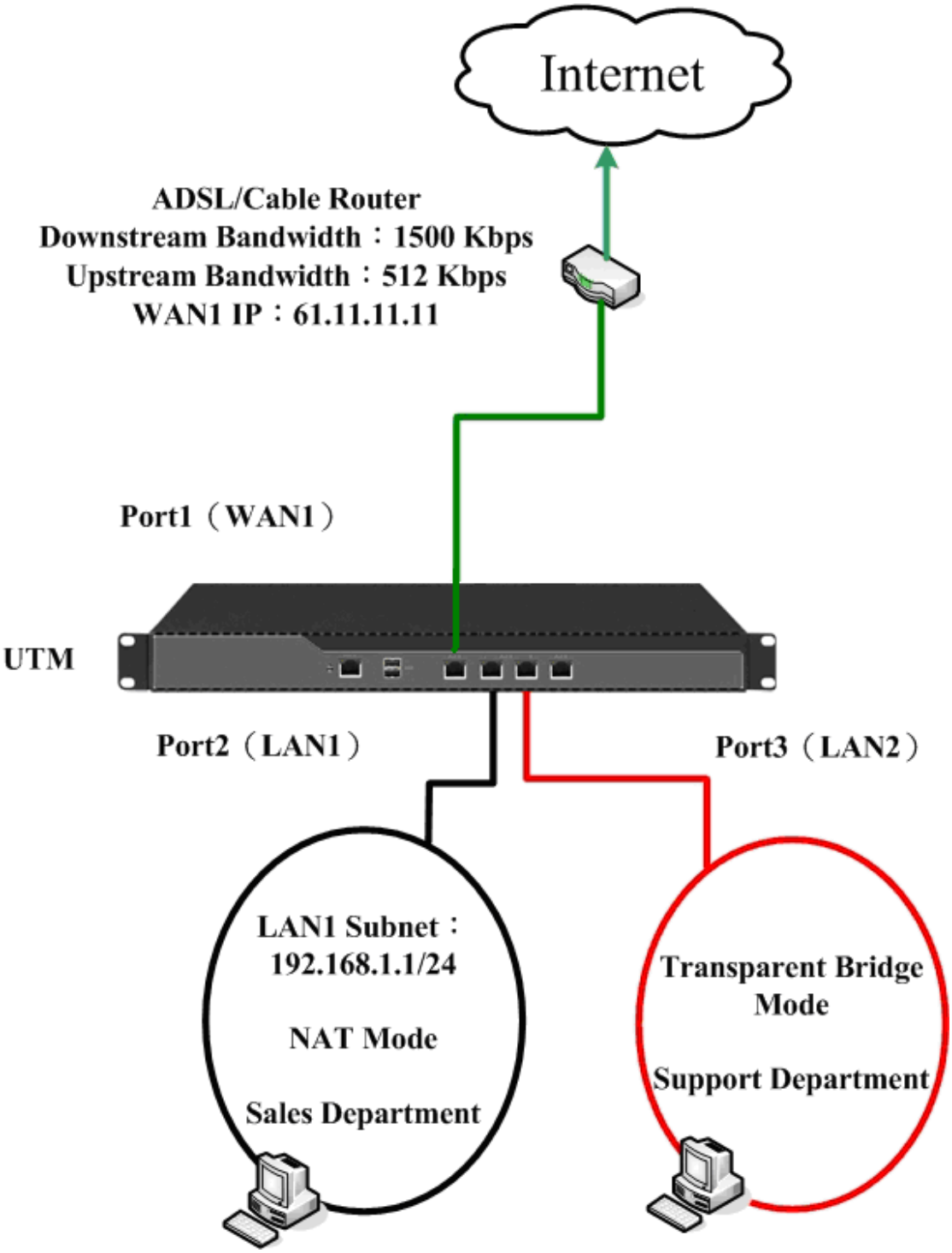


Figure 3-36 The Deployment of LAN Using NAT/Routing Mode

Policy Object

Chapter 4 Address

In *Address*, the IT administrator may configure network settings of LAN, WAN and DMZ, as well as designate specific addresses in a network as a group.

An IP address might represent a host or a subnet, in either case, the IT administrator may give it an easily identifiable name for better management. According to the network in which an IP address resides, it can be categorized into three kinds, namely, a LAN IP address, WAN IP address or DMZ IP address. Each of the three can be organized into an address group comprising several addresses. Simply by applying the address group to a policy, the IT administrator may easily manage a group of users with merely one policy.

Note:

1. It is recommended to configure some desirable address names within **Address** first so that they are ready to use for the **Source Address** or **Destination Address** setting of a policy.

Terms in Address

Name

- An easily identifiable name to represent the IP address or addresses.

Address type

- Used to designate the IP range and IPv6 address / prefix length or IP / netmask IP.

IP Version

- IPv4 or IPv6 can be selected.

IP Address

- Represents a host or subnet; and can be categorized into three kinds, i.e. LAN IP address, WAN IP address and DMZ IP address.

Netmask

- Enter 255.255.255.255 to represent the single IPv4 address that you entered in **IP Address**.
- As an example, to represent the subnet from a class C IPv4 address such as 192.168.100.1, enter 255.255.255.0 into the **Netmask** field.

Prefix Length

- Enter 128 to represent a single IPv6 address.
- To represent an IPv6 subnet (for example 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A with a prefix of 1DA:D3:0:2F3B) then **Prefix length** should be set to 64.

MAC Address

- Specifying a MAC address for the specified host helps to prevent unauthorized access.

Interface

- Specifys the interface that the IP address or addresses belongs to.

FQDN（Fully Qualified Domain Name）

- The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN may be www.planet.com.tw. The hostname is www, and the domain name is planet.com.tw.
- To regulate the access to the specified web site, the IT administrator only needs to configure an FQDN setting.

Note:

1. FQDN settings helps IT administrator to block all the IP addresses that are mapped to the site. Normally, the site has more than one IP address, thus, block an IP address does not block the site reliably. For example, facebook has the IP addresses like 69.171.228.14、69.171.224.39、69.171.229.14, etc. To block facebook, the IT administrator may block the site by its FQDN instead of its IP addresses.
2. Instead of type the whole address such as http://www.facebook.com/#!/profile.php?id=105520583884516, you merely need to type "hostname + domain name" such as www.facebook.com. to complete the FQDN settings.
3. FQDN settings may regulate the protocol like HTTP, HTTPS and FTP, while the black-/whitelist may regulate HTTP protocol only. To configure the FQDN setting, you may add an FQDN under **Policy Object > Address > WAN** first, and then apply it to the policy.
4. Under **Policy Object > Address > WAN Group**, the newly added *CHINA_TELECOM and *CNC selections represent two major ISPs in China. During an outward session, in order to take advantage of policy-based routing (PBR), the device will designate the most appropriate route based upon the destination address.
5. To quickly create the settings under **Policy Object > Address > LAN / DMZ**, you may click **Assist Me** to automatically obtain data from **Monitor > Status > ARP Table / Sessions Info**

4.1 Example

No.	Settings	Scenario	Page
4.1.1	**LAN**	Using DHCP to Grant Only FTP Access to a LAN User with Specific IP Address	**129**
4.1.2	**LAN/ WAN Group**	Creating a Policy for Certain Users to Connect to a Specific IP Address	**132**

4.1.1 Using DHCP to Assign an IP to a Specific User and only

Permitting FTP Access

Step 1. Under **Policy Object** > **Address** > **LAN**, set as below:（**Figure 4-1**）

- Click **New Entry.** Type the name of the user in the **Name** field. (e.g., Alex).
- **Address type:** Select either **IP / Netmask** or **IP Range.**
- **IP Version**: Select **IPv4** or **IPv6**.
- Type the IP address of the user in the **IP Address** field. (e.g., 192.168.3.2)
- **Netmask**: Type “255.255.255.255” (denotes a single IP address as specified in the **IP Address** field).
- Type the MAC address of the user in the **MAC Address** field. (e.g., 00:B0:18:25:F5:89)
- Select the Interface from the **Interface** drop-down list.
- Click **OK.**（**Figure 4-2**）

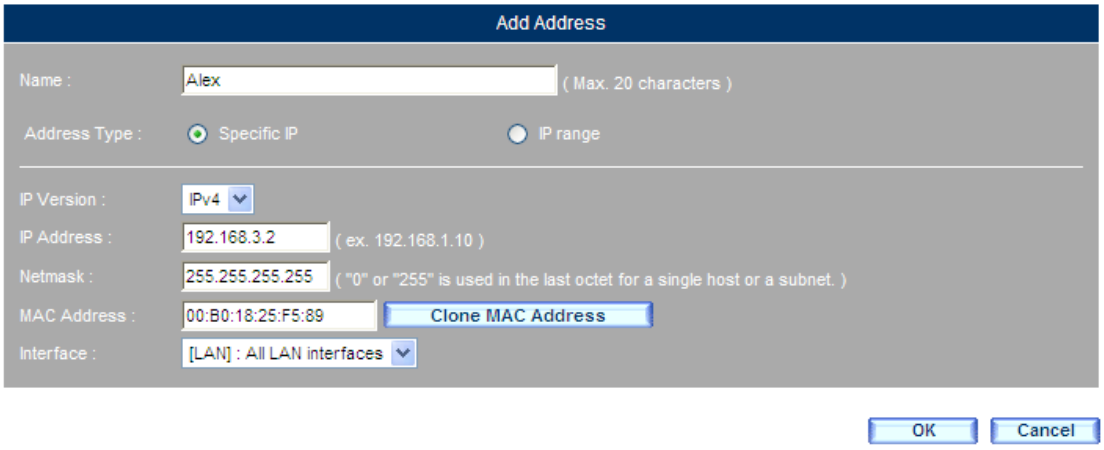


Figure 4-1 Adding a LAN Address

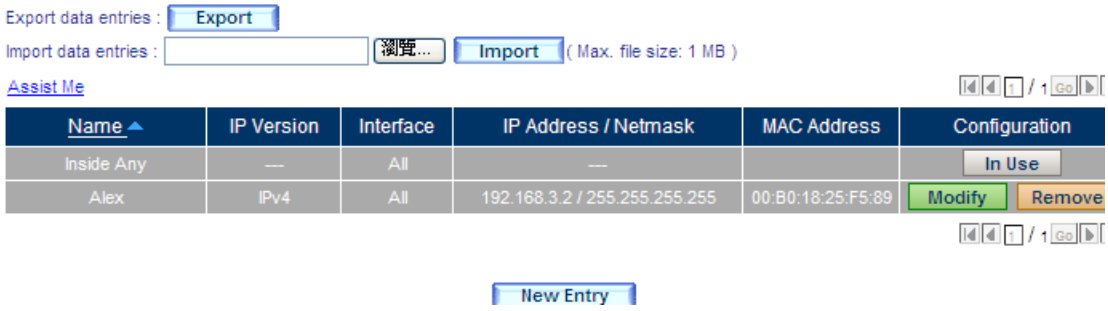


Figure 4-2 The Added LAN Address

Note:

1. To save the configured data from **Policy Object > Address > WAN / LAN / DMZ** as a file for storage or modification, use **Export data entries**. If the list needs to be restored due to accidential modifications etc., use **Import data entries.**
2. To assist with the configuration, you may click on the **Clone MAC Address** button Clone MAC Address to automatically obtain the user's MAC address.
3. To assign the IP address to the MAC, go to **System > Configuration > DHCP** and configure the settings under the **Assign a Static IP Address** section.
4. By default, three address settings, namely Inside_Any, Outside_Any and DMZ_Any, appear separately under **Policy Object > Address > LAN / WAN / DMZ**. Each of the settings represents all the IP addresses from its network.
5. Configuring **Policy Object > Address > WAN / DMZ** is the same as **Policy Object > Address > LAN.** However, **Policy Object > Address > WAN** does not require setting a **MAC Address** or **Interface**.

Step 2. Go to **Policy** > **Outgoing** and configure as below: (**Figure 4-3**)

- **Source Address:** Select the source address.
- **Service** : Select FTP**.**
- Click **OK.** (**Figure 4-4**)

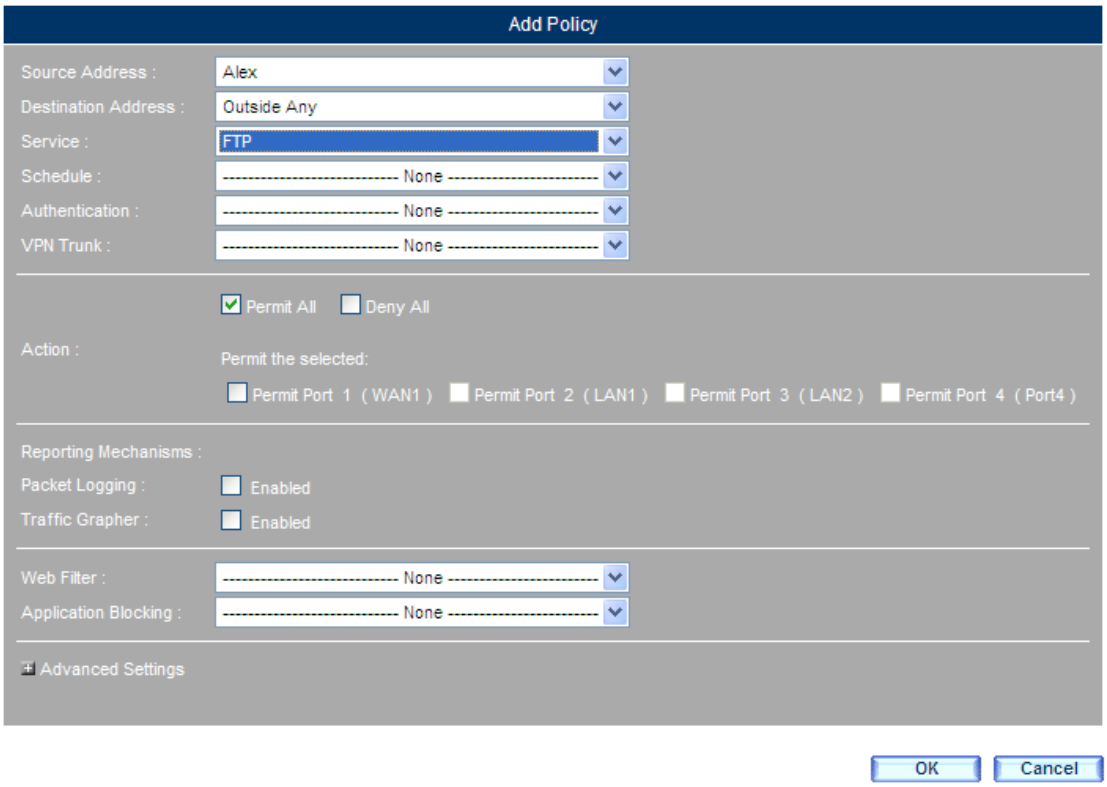


Figure 4-3 The Outgoing Policy Settings

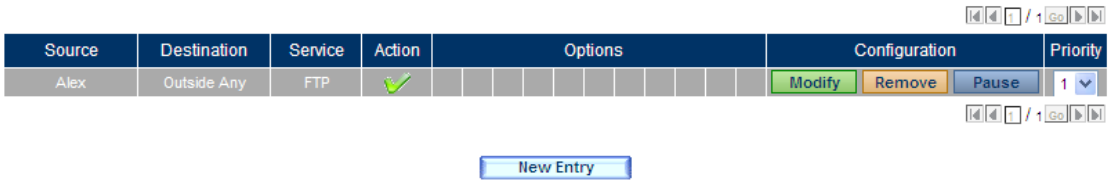


Figure 4-4 Policy Completed

4.1.2 Creating a Policy for Certain Users to Connect to a Specific IP Address

Step 1. Create several addresses under **Policy Object > Address > LAN.** (**Figure 4-5**)

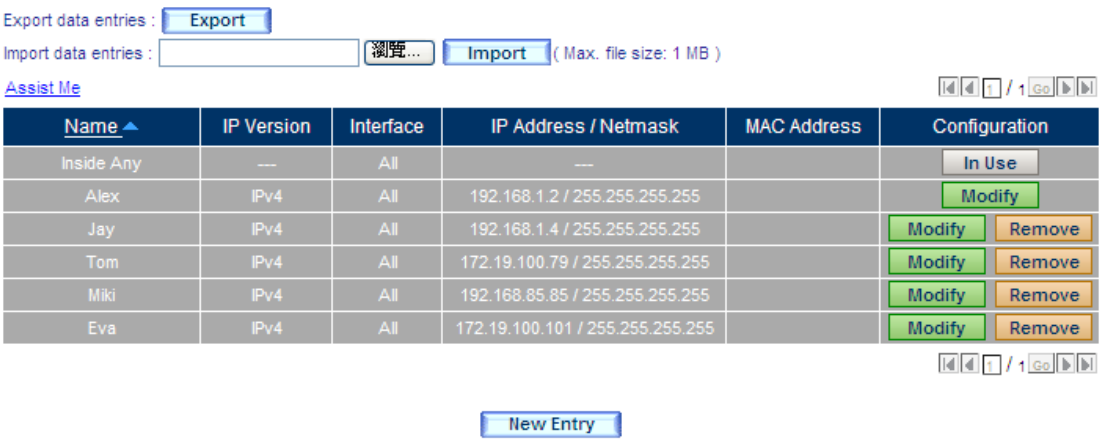


Figure 4-5 The Creation of Several LAN Addresses

Step 2. Under **Policy Object > Address > LAN Group**, set as below: (**Figure 4-6**)

- Click **New Entry**.
- **Name:** Designate a name for the group.
- Select group members from the **Available address** column on the left, and then click **Add**.
- Click **OK.** (**Figure 4-7**)

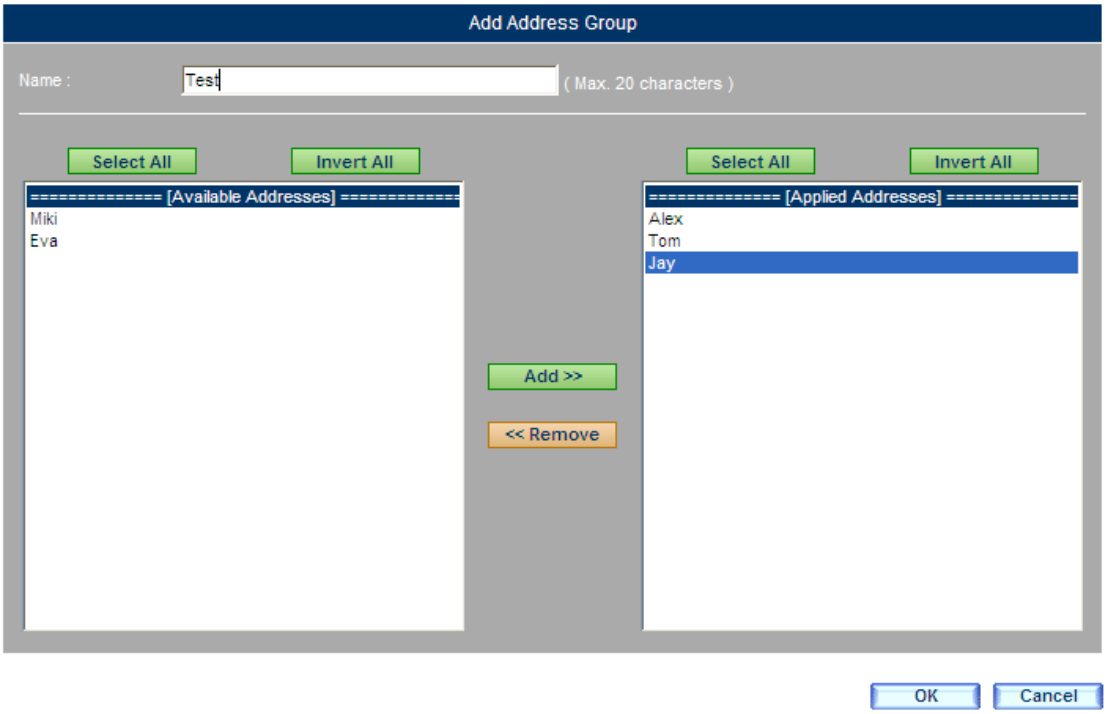


Figure 4-6 Grouping LAN Addresses

Figure 4-7 An Added LAN Group

Note:

1. Configuring **Policy Object > Address > WAN Group / DMZ Group** can be done in a similar manner to **Policy Object > Address > LAN Group.**

Step 3. Go to **Policy Object** > **Address** > **WAN** and configure as below:（**Figure 4-8**）

- Click **New Entry.**
- **Name:** Designate a name for the group.
- **Address Type:** Select IP / Netmask.
- **IP Version**: Select IPv4.
- **IP Address :** Input the WAN IP address.
- Click **OK.**（**Figure 4-9**）

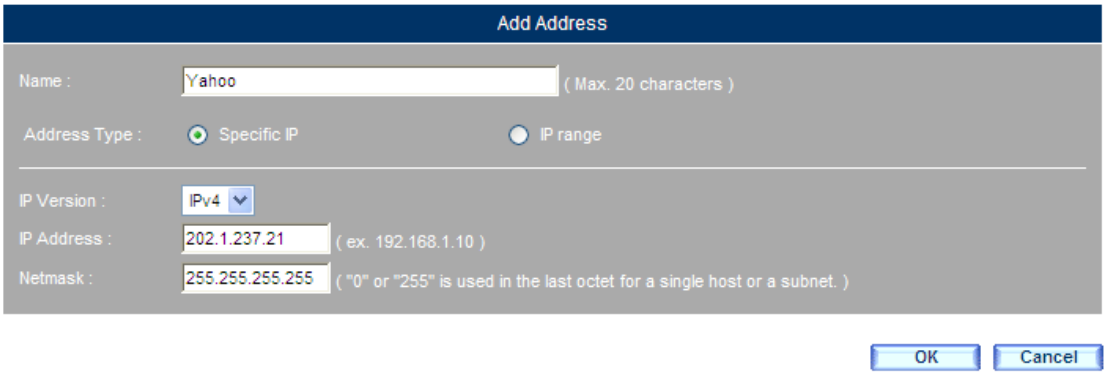


Figure 4-8 Configuring the WAN Address

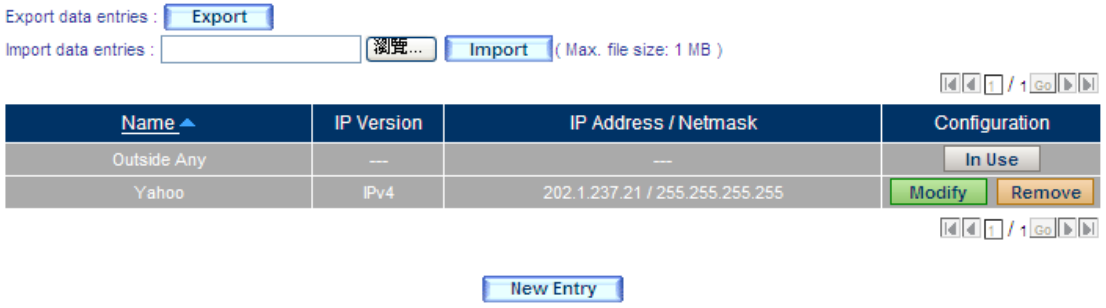


Figure 4-9 Settings Completed

Step 4. Go to **Policy** > **Outgoing** and configure as below:（**Figure 4-10**）

- **Source Address:** Select the LAN address group.
- **Destination Address:** Select the WAN destination address.
- Click **OK.**（**Figure 4-11**）

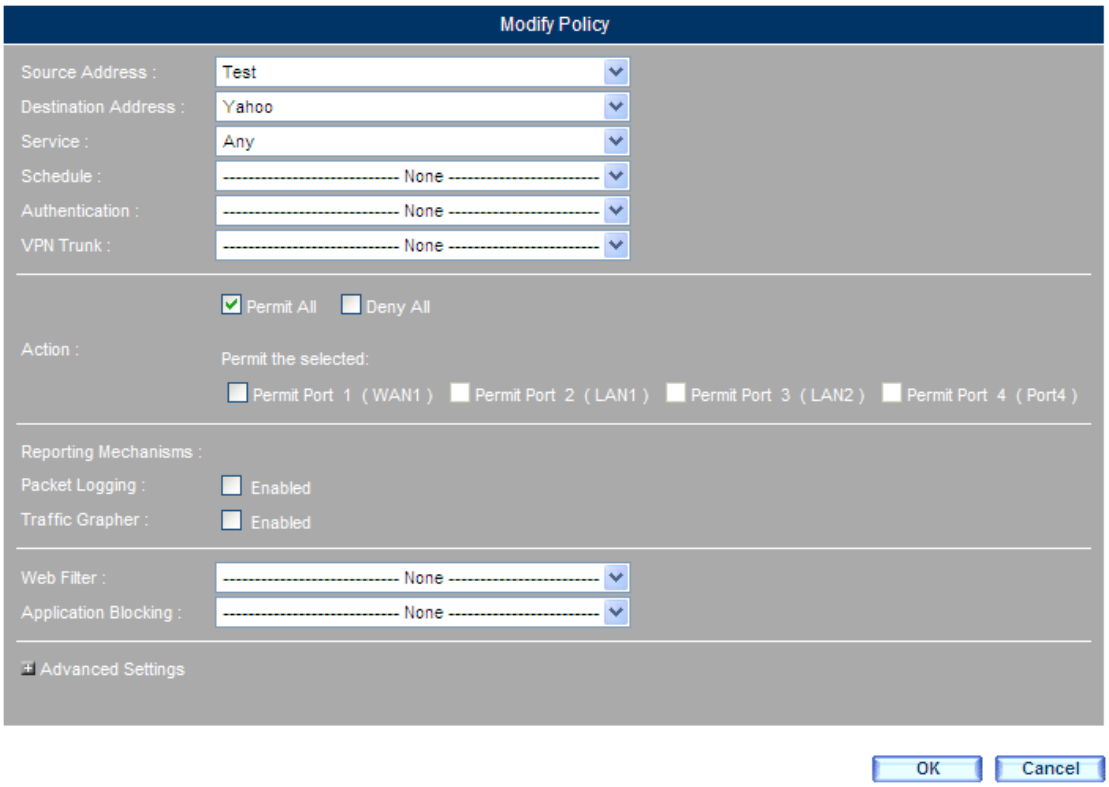


Figure 4-10 The Policy Settings

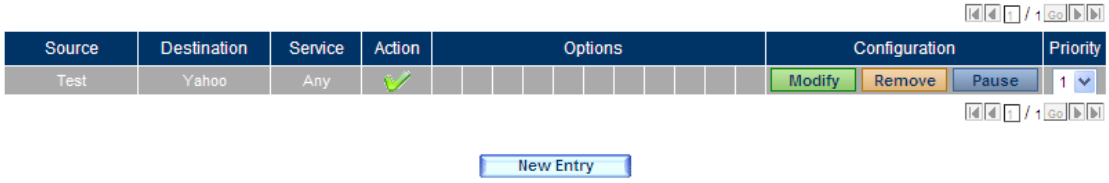


Figure 4-11 The Completed Policy Settings

Note:

1. Address must be applied to a policy to take effect.

Chapter 5 Service

TCP and UDP protocols provide different services. These services have an associated port number, for example Telnet = 23, FTP = 21, SMTP = 25, POP3 = 110, etc. The CS-2001 provides control over access to these services using **Pre-defined** and **Custom** settings.

- **Pre-defined:** Provides the most common TCP and UDP services.
- **Custom:** Allows customization of the port numbers and their associated TCP and UDP services.

Note:

1. **Policy Object > Service > Group** provides a convient means to manage a group of different services. For example, a single IP address may access five different services from a server (e.g. HTTP, FTP, SMTP, POP3 and Telnet). If the services are not grouped into one under **Policy Object > Service > Group,** then five individual policies for each of the five services will need to be created under **Policy**.

Terms of Service

Pre-Defined

Symbol	Description
ANY	Any service
TCP	Services using the TCP protocol: AFPoverTCP, AOL, BGP, FINGER, FTP, GOPHER, HTTP, HTTPS, InterLocator, IRC, L2TP, LDAP, MSN, NetMeeting, NNTP, POP3, PPTP, Real-Media, RLOGIN, SMTP, SSH, TCP-Any, TELNET, Traceroute, VDO-Live, WAIS, WINFRAME, X-Windows, etc.
UDP	Services using the UDP protocol: DNS, IKE, IMAP, NFS, NTP, PC-Anywhere, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-Any, UUCP, etc.

Name

- The name for the customized service.

Protocol

- The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.

Client Port

- The port number of the client user's PC which is used for connecting to the CS-2001. It is recommended using the default range (0 to 65535).

Server Port

- The port number for the customized service.

5.1 Example of Pre-defined

5.1.1 Creating a Policy to Permit WAN Users Using VoIP

Technology to Communicate with LAN Users (Using VoIP Port

Numbers of TCP 1720, TCP 15328-15333 and UDP

15328-15333)

Step 1. Go to **Policy Object** > **Address** > **LAN Group** and configure the following settings.（**Figure 5-1, 5-2**）

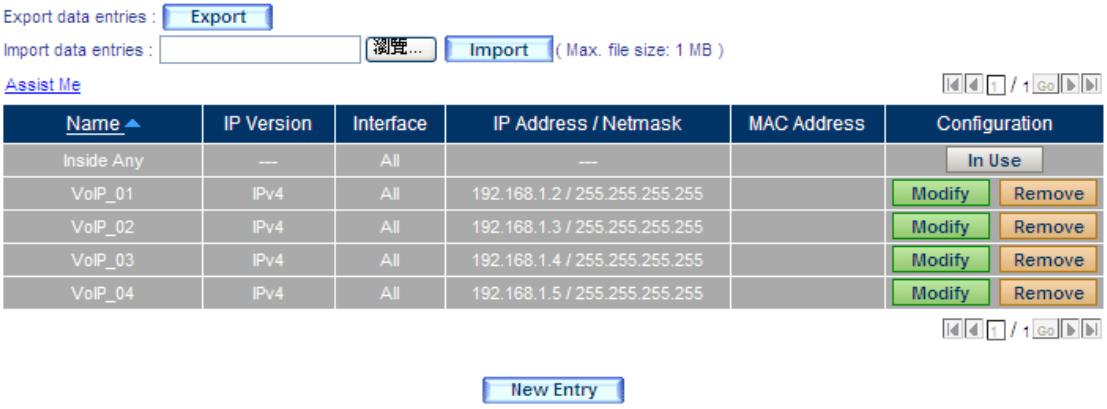


Figure 5-1 Address Settings for the LAN

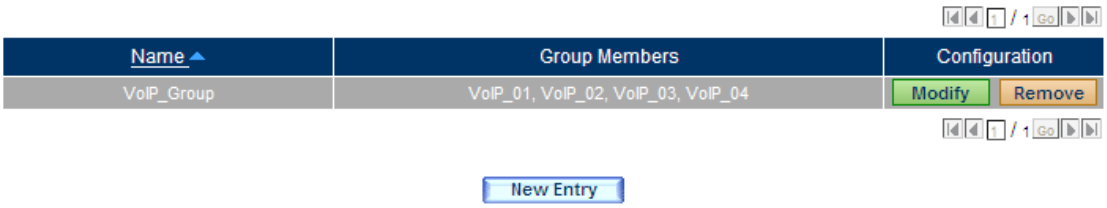


Figure 5-2 An Added LAN Group

Step 2. Go to **Policy Object** > **Service** > **Custom** and then configure as below: （**Figure 5-3**）

- Name: Type in a name for the service.
- In row number 1 select **TCP** for the protocol. Leave the **Client Port** on the default setting. **Server Port:** set as 1720 – 1720.
- In row number 2 select **TCP** for the protocol. Leave the **Client Port** on the default setting. **Server Port:** set as 15328 – 15333.
- In row number 3 select **TCP** for the protocol. Leave the **Client Port** on the default setting. **Server Port:** set as 15328 – 15333.
- Click **OK.**（**Figure 5-4**）

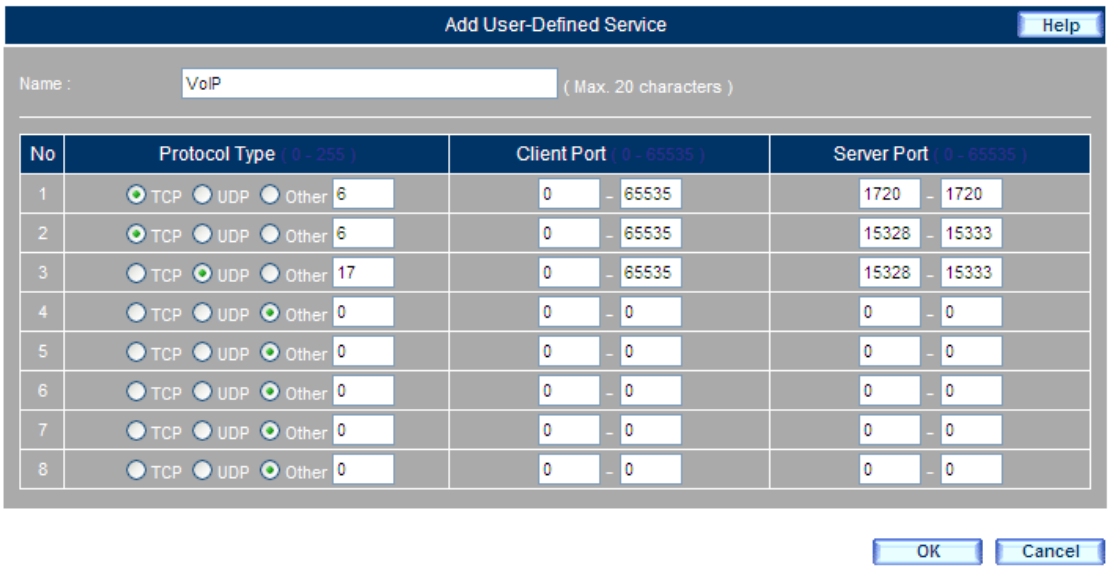


Figure 5-3 Adding a Custom Service

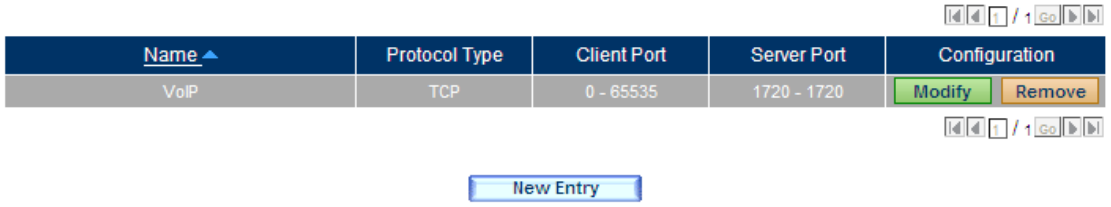


Figure 5-4 The Added Custom Service

Note:

1. Normally, the port number setting for the client port falls between 0 and 65535. It is recommended to adhere to the range mentioned above when configuring the client port number.
2. Both the **Client Port** and **Server Port** contain two fields. You may use the two fields to specify a range (e.g. 15328 : 15333) or to specify a single port number e.g (1720 : 1720).

Step 3. Go to **Policy Object** > **Virtual Server** > **Port Mapping** and use settings you created in **Policy Object** > **Service** > **Custom.** (Figure 5-5)

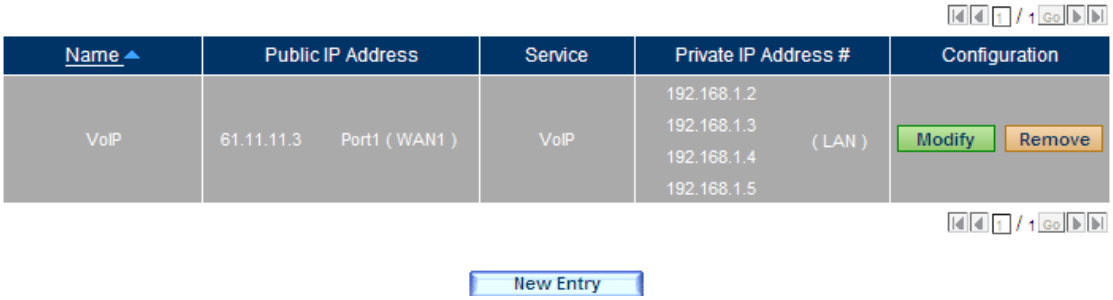


Figure 5-5 Using the Pre-defined Service Settings

Step 4. Go to **Policy** > **Incoming** and configure as below:（**Figure 5-6**）

- **Destination Address:** Select the virtual server setting configured in the previous step.
- **Service**: Select the pre-defined service.
- Click **OK.**（**Figure 5-7**）

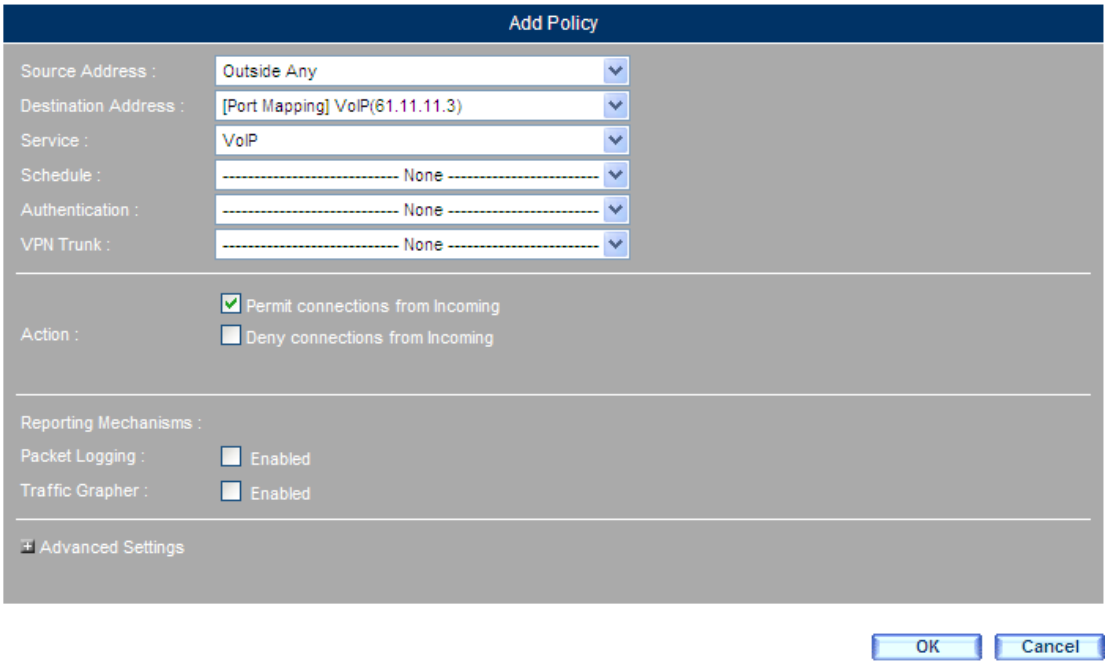


Figure 5-6 Configuring an Incoming Policy

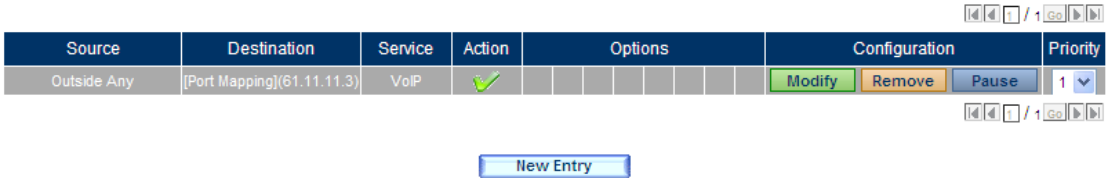


Figure 5-7 The Completed Settings

Step 5. Go to **Policy** > **Outgoing** and configure as below:（**Figure 5-8**）

- **Source Address:** Select the LAN group.
- **Service**: Select the custom service.
- **Action**: Select Port1 (WAN1).
- Click **OK.**（**Figure 5-9**）

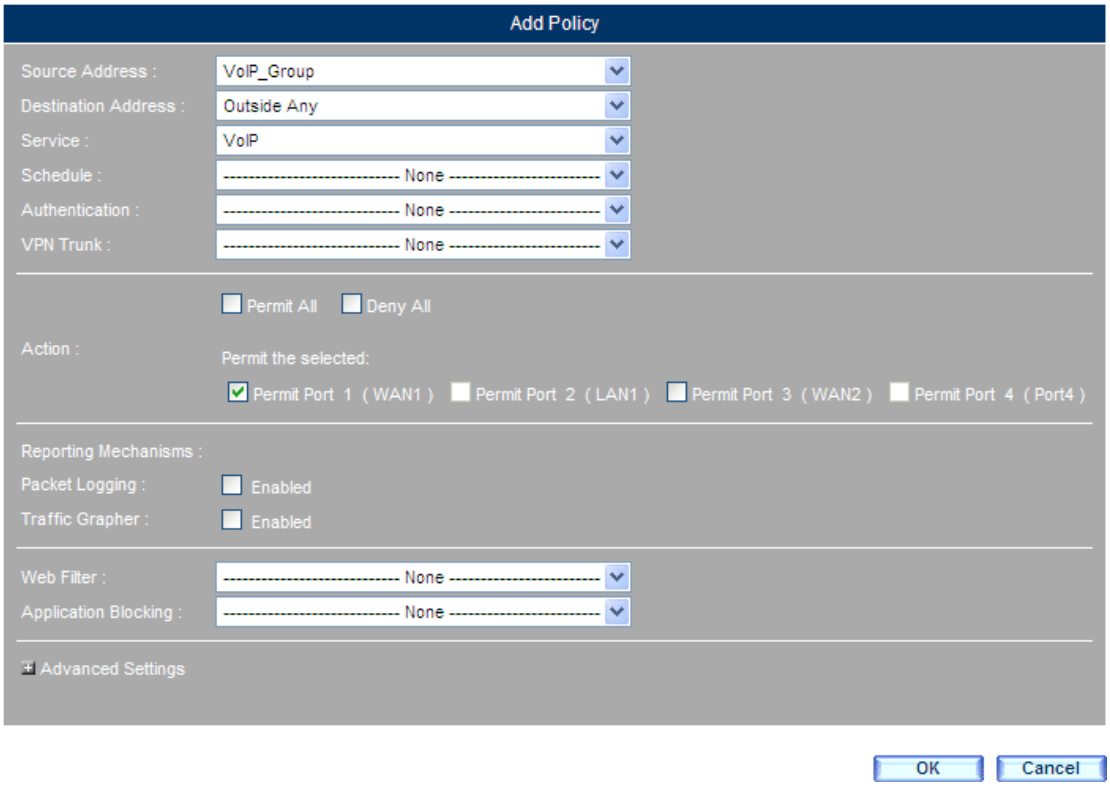


Figure 5-8 The Outgoing Policy for VoIP

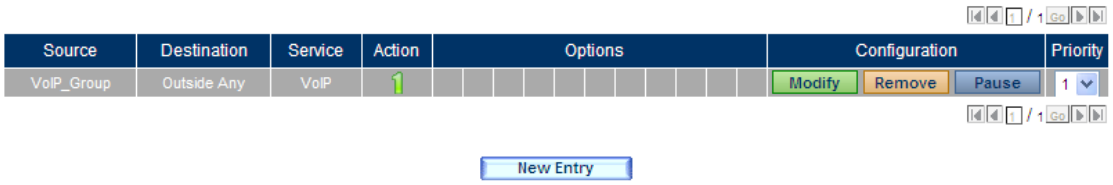


Figure 5-9 The Completed Settings

Note:

1. **Service** needs to be applied to a **Virtual Server** setting and then a **Policy** to take effect.

5.2 Example of Service Group

5.2.1 Creating a Policy with a Service Group to Limit Specific LAN Users to Access Only Certain Internet Services (HTTP, POP3, SMTP and DNS)

Step 1. Go to **Policy Object** > **Service** > **Group**, and set as below: (**Figure 5-10**)

- **Group Name:** Type a name for the service group.
- Select HTTP, POP3, SMTP and DNS services from the **Available Services** column on the left, and then click **Add.**
- Click **OK.** (**Figure 5-11**)

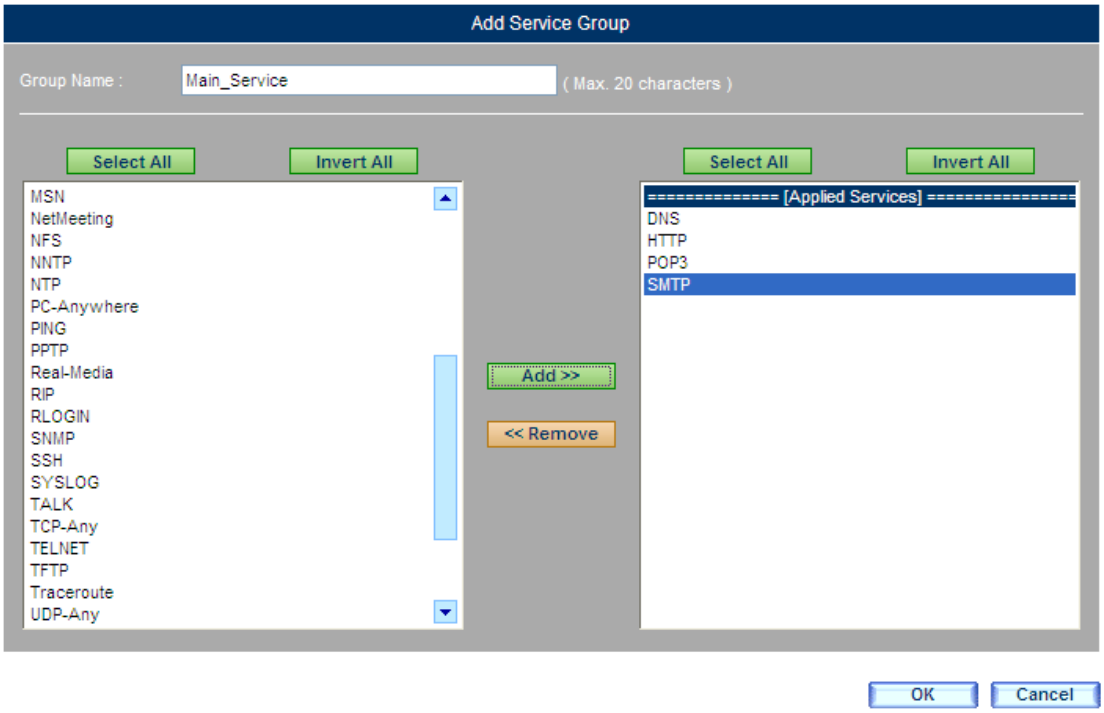


Figure 5-10 The Settings for Service Group

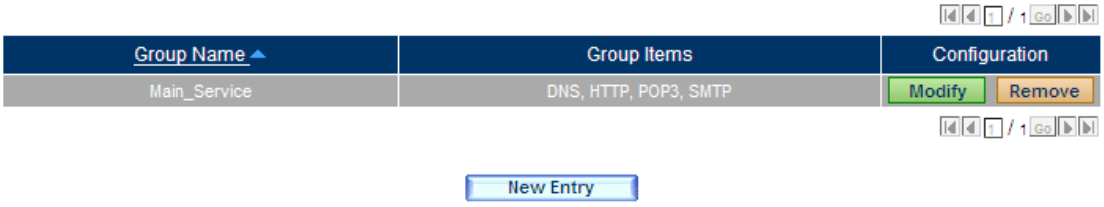


Figure 5-11 The Added Service Group

Step 2. Go to **Policy Object > Address > LAN Group** and create a **LAN Group** of specific LAN users that are only permitted to access certain services.（**Figure 5-12**）

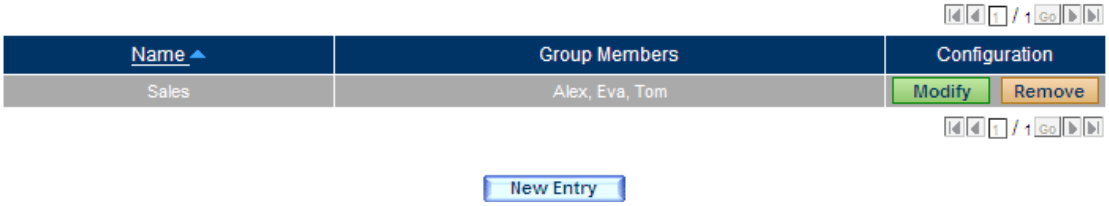


Figure 5-12 The Added LAN Group

Step 3. Under **Policy > Outgoing**, set as below:（**Figure 5-13**）

- Select the defined LAN group for **Source Address.**
- Select the defined service for **Service.**
- Click **OK.**（**Figure 5-14**）

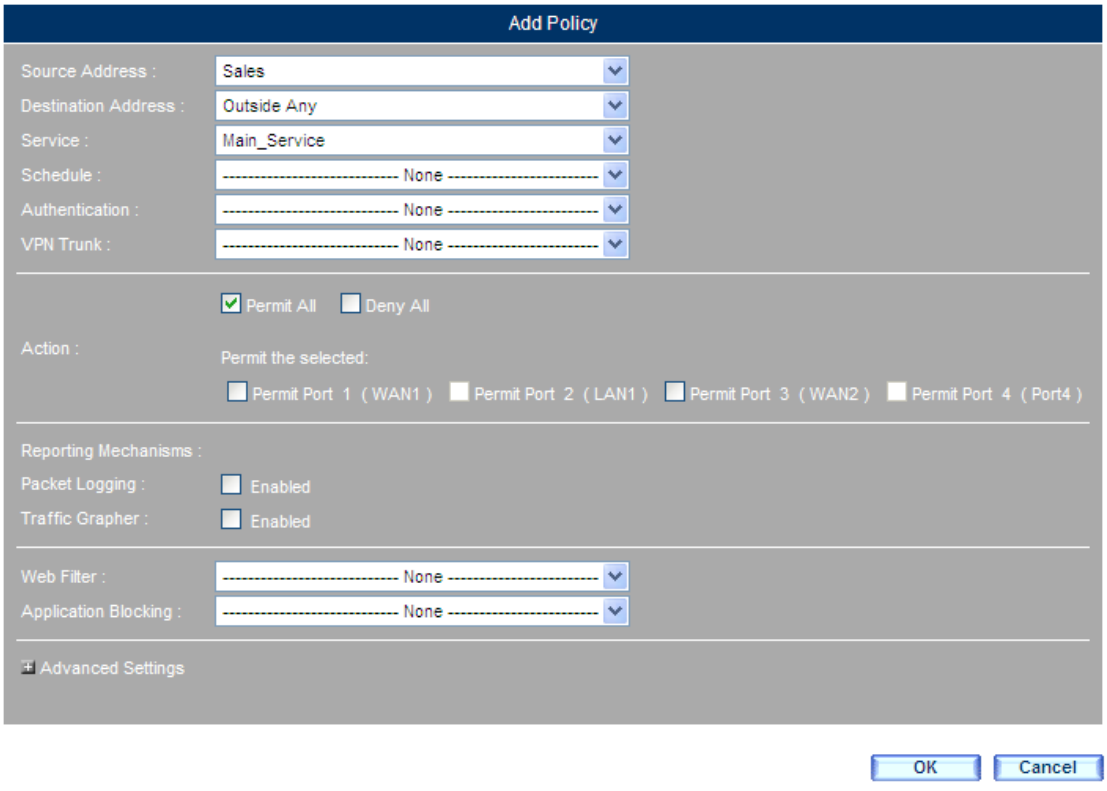


Figure 5-13 Applying the Group Service to a Policy

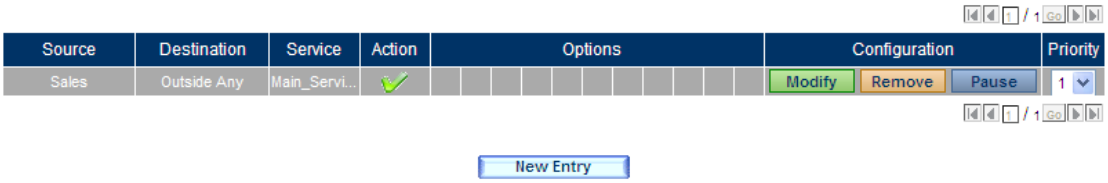


Figure 5-14 The Completed Policy Settings

Chapter 6 Schedule

Schedule is used for regulating the activation time of policies. With its help, the IT administrator may determine a specific period of time for each policy to take effect, saving time on system administration.

Terms in Schedule

Name

- Designates the name of the schedule.

Type

- Two modes are provided:
  - **Recurring**: Based upon a weekly schedule, with configurable start and end periods for each of the seven days in a week.
  - **One-Time**: Provides a start and stop time for a single specific date based upon the year, month, day, hour and minute.

6.1 Example

6.1.1 Assigning Daily Internet Access Time Slots for LAN

Users

Step 1. Under **Policy Object** > **Schedule** > **Settings**, set as below: (**Figure 6-1**)

- Type the name.
- **Mode:** Select either **Recurring** or **One-Time.**
- Use the drop-down menus to select the required start and end time for each day of the week.
- Click **OK**. (**Figure 6-2**)

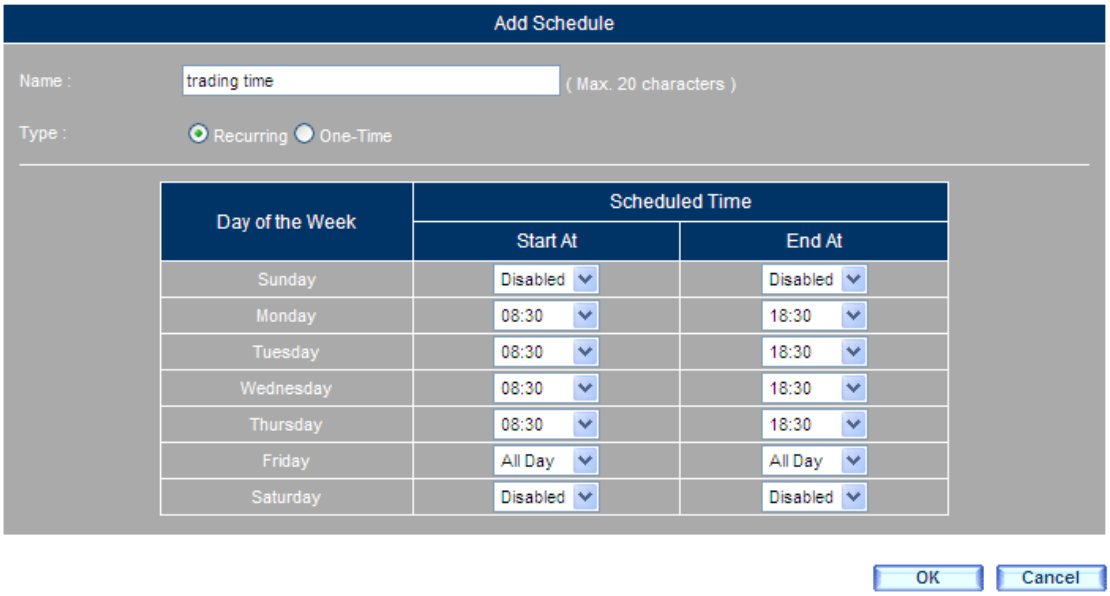


Figure 6-1 Schedule Settings

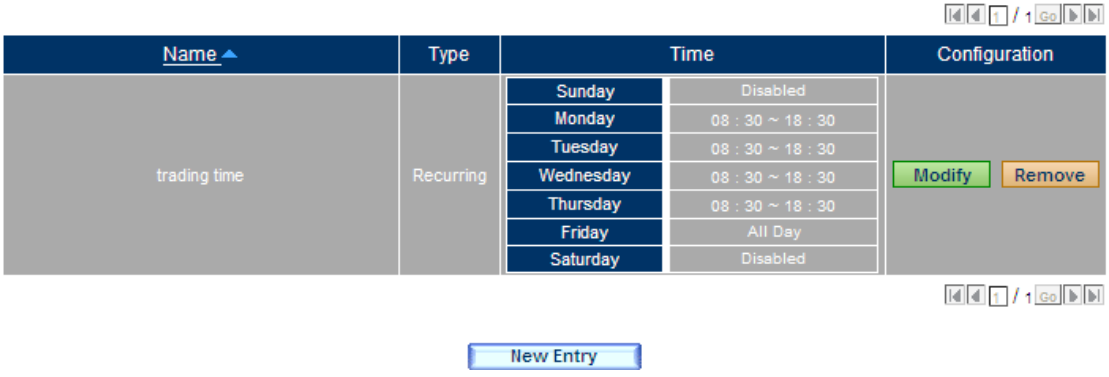


Figure 6-2 The Completed Schedule Settings

Step 2. Under **Policy** > **Outgoing**, set as below:（**Figure 6-3**）

- Select the pre-defined schedule for **Schedule.**
- Click **OK**.（**Figure 6-4**）

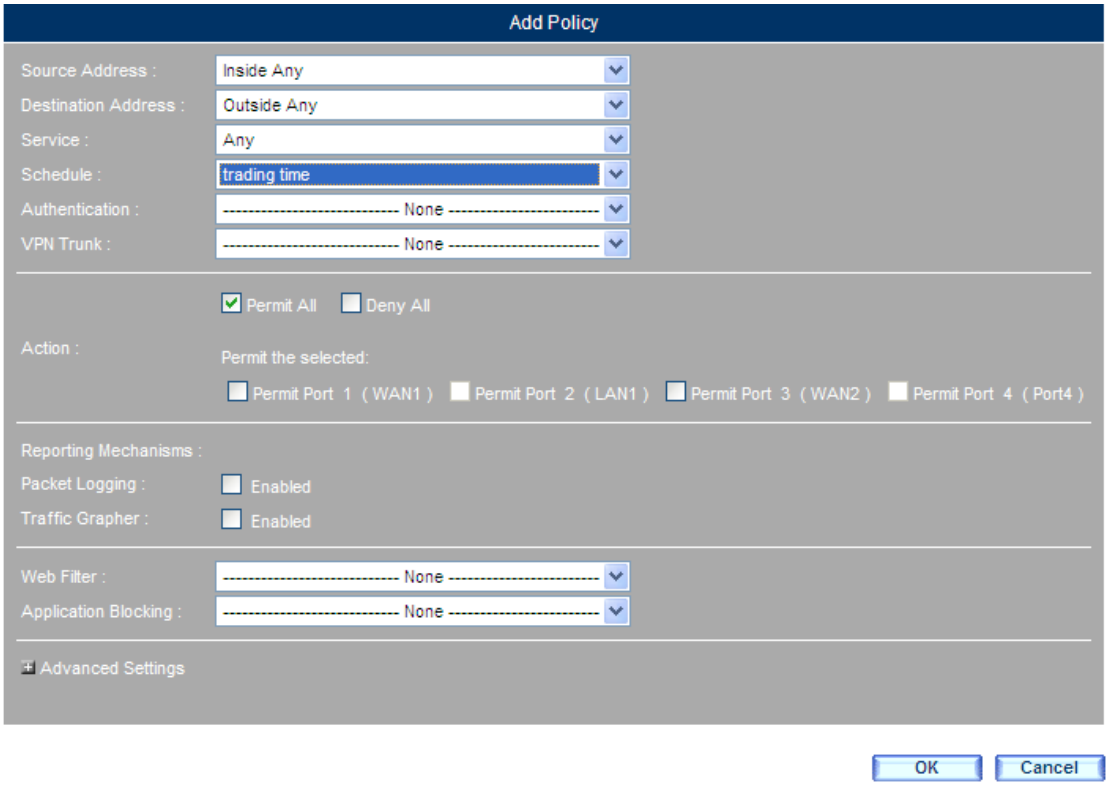


Figure 6-3 Applying the Schedule to the Policy

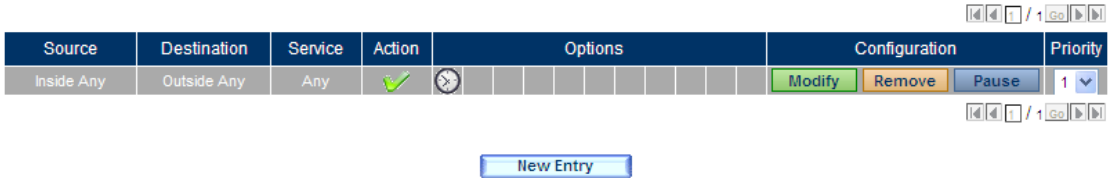


Figure 6-4 The Completed Policy Settings

Chapter 7 QoS

QoS provides bandwidth management for LAN users accessing the Internet via the CS-2001. When applied with a **Policy**, it ensures users are allocated suitable amounts of bandwidth.（**Figure 7-1, 7-2**）

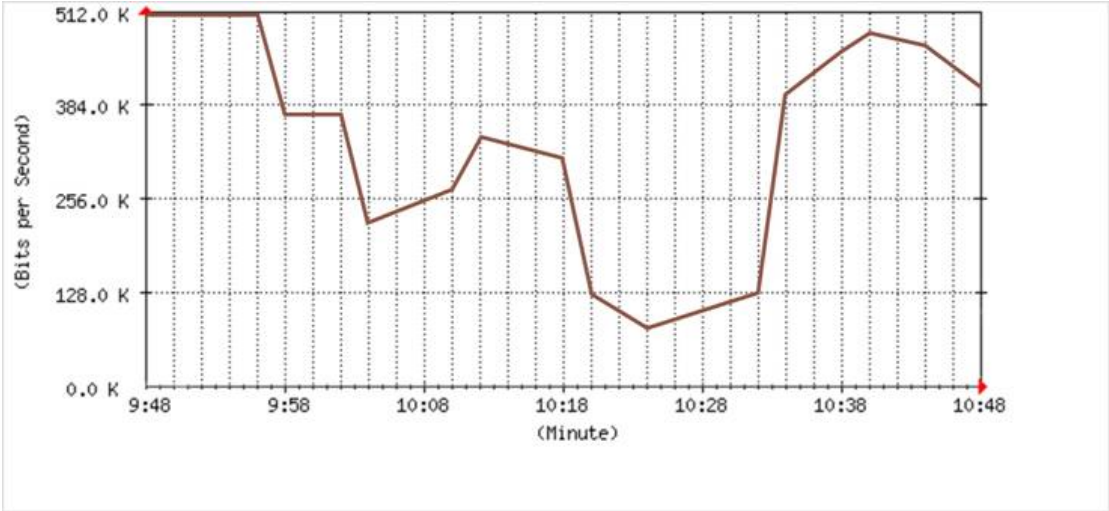


Figure 7-1 The Network with no QoS

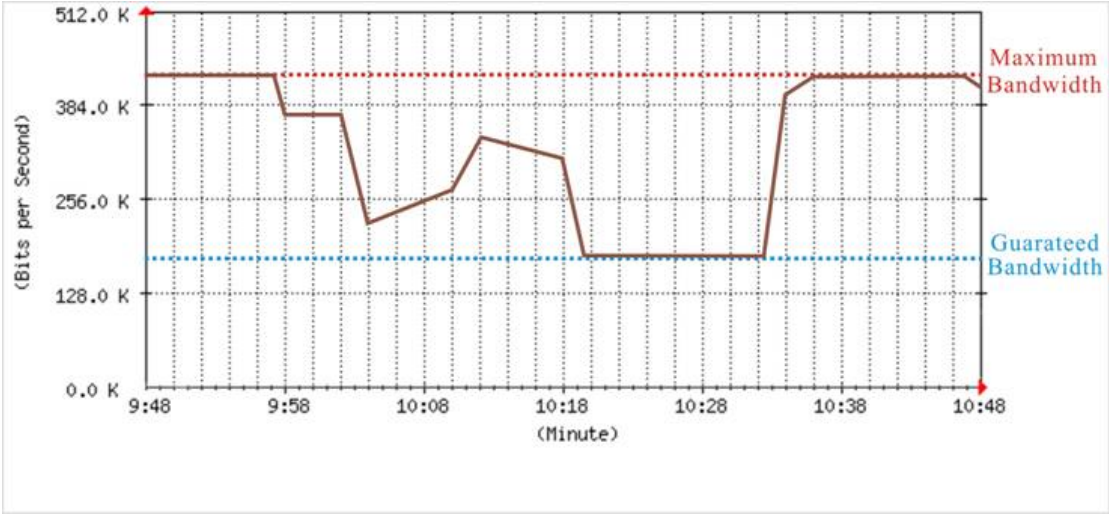


Figure 7-2 Applying QoS to the Network (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

Terms in Settings

Name

- The name of the QoS setting.

Port

- The WAN port to apply QoS.

Downstream Bandwidth

- Determines the guaranteed bandwidth and maximum bandwidth of the total downstream bandwidth.

Upstream Bandwidth：

- Determines the guaranteed bandwidth and maximum bandwidth of the total upstream bandwidth.

Priority

- Specifies the priority that upstream and downstream bandwidth gets allocated.

G.Bandwidth

- Specifies the minimum (guaranteed) amount of bandwidth.

M.Bandwidth

- Specifies the maximum amount of bandwidth.

7.1 Example

7.1.1 Creating a Policy to Limit Upload and Download

Bandwidth

Step 1. Under **Policy Object** > **QoS** > **Settings**, set as below: (**Figure 7-3**)

- Click **New Entry**. Type the **Name** accordingly.
- Configure the bandwidth of Port 2 (WAN1) and Port 3 (WAN2).
- Select the priority for this QoS setting.
- Click **OK**. (**Figure 7-4**)

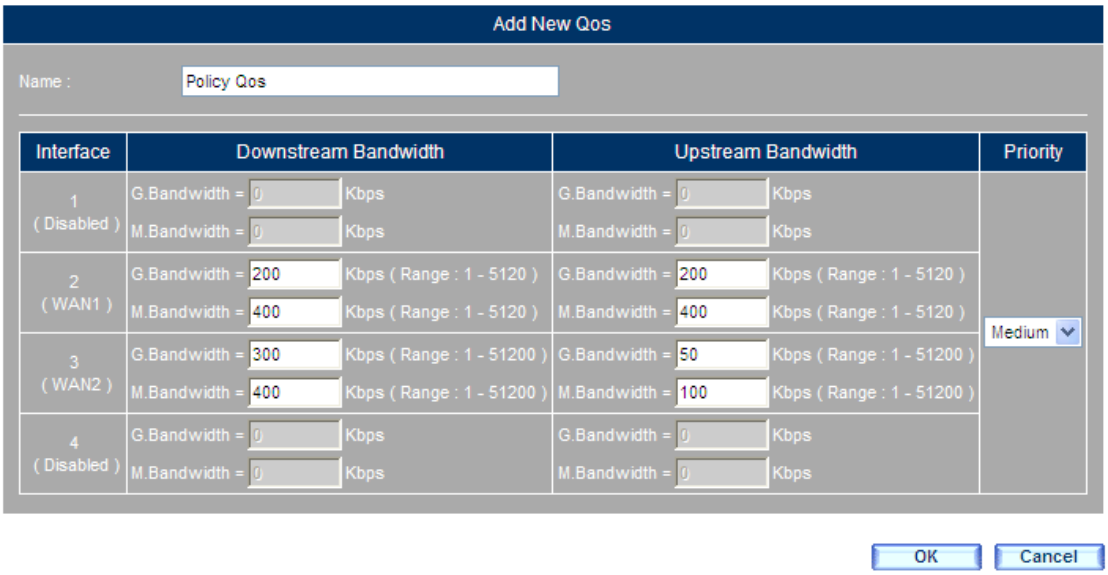
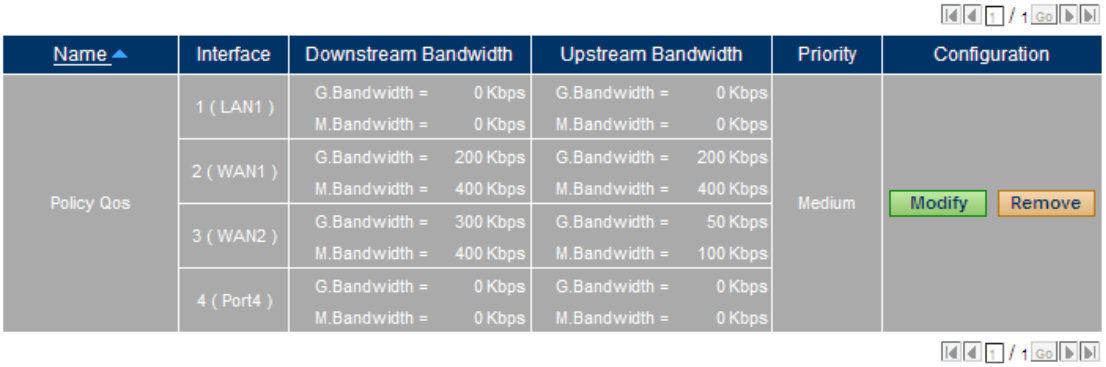


Figure 7-3 Configuring the QoS Settings



Name	Interface	Downstream Bandwidth		Upstream Bandwidth		Priority	Configuration
Policy Qos	1 (LAN1)	G.Bandwidth =	0 Kbps	G.Bandwidth =	0 Kbps	Medium	Modify Remove
		M.Bandwidth =	0 Kbps	M.Bandwidth =	0 Kbps		
	2 (WAN1)	G.Bandwidth =	200 Kbps	G.Bandwidth =	200 Kbps		
		M.Bandwidth =	400 Kbps	M.Bandwidth =	400 Kbps		
	3 (WAN2)	G.Bandwidth =	300 Kbps	G.Bandwidth =	50 Kbps		
		M.Bandwidth =	400 Kbps	M.Bandwidth =	100 Kbps		
	4 (Port4)	G.Bandwidth =	0 Kbps	G.Bandwidth =	0 Kbps		
		M.Bandwidth =	0 Kbps	M.Bandwidth =	0 Kbps		

Figure 7-4 The Completed QoS Settings

Step 2. Under **Policy** > **Outgoing**, set as below: (**Figure 7-5**)

- Select the pre-configured QoS setting.
- Click **OK**. (**Figure 7-6**)

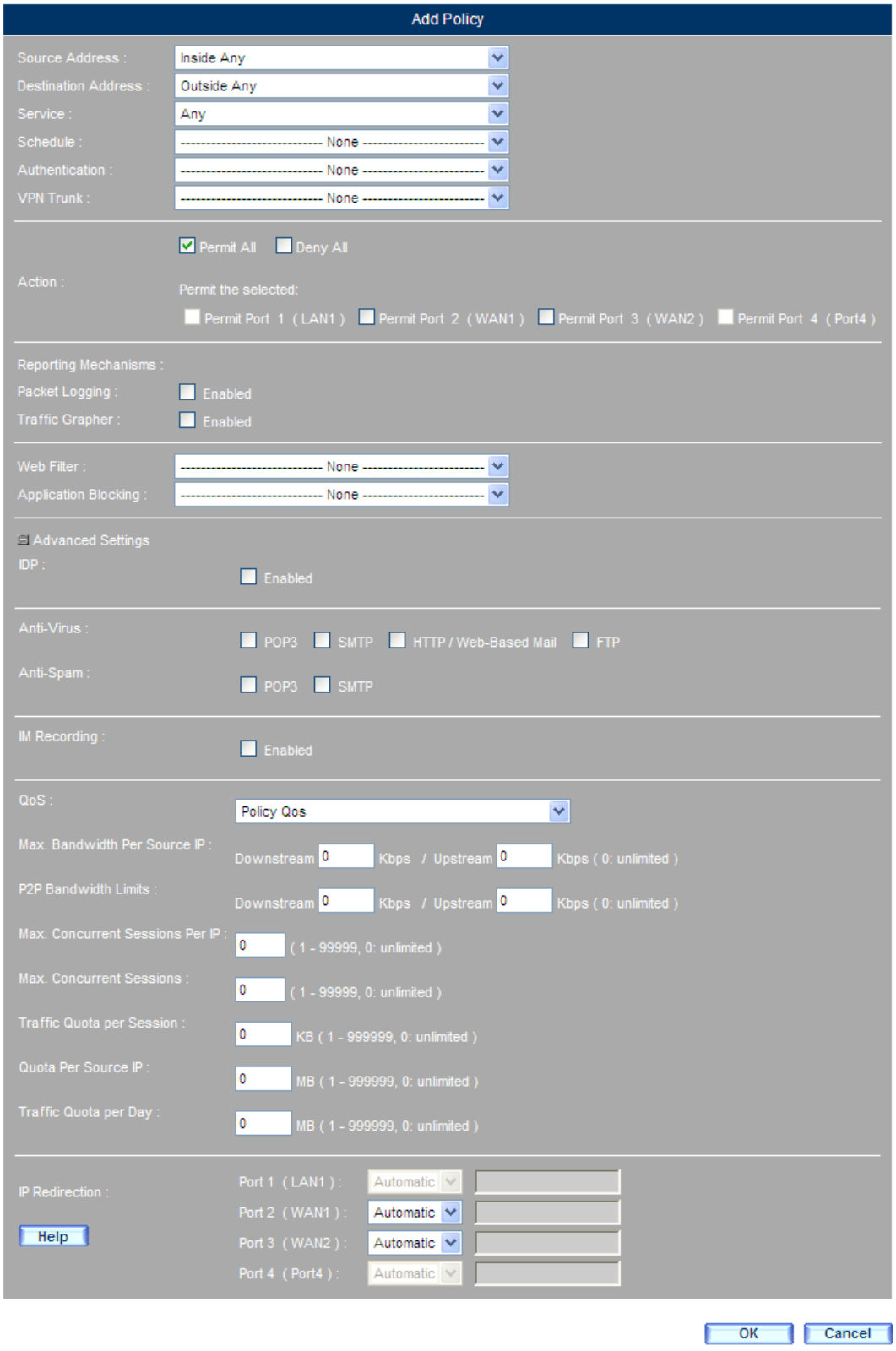


Figure 7-5 Applying QoS to a Policy

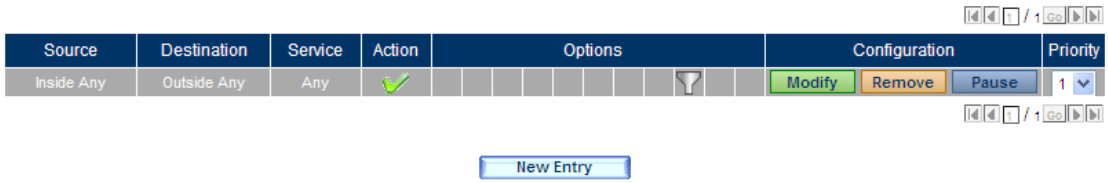


Figure 7-6 The Completed Policy Setting

Note：

1. Under **Policy Object > QoS > Settings**, the available bandwidth range, such as **G. Bandwidth** and **M. Bandwidth**, is predefined under **Interface > WAN**. Thus, an appropriate value of **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** should be configured under **Interface > WAN** first.

Chapter 8 Authentication

Authentication regulates users access to the Internet. CS-2001 offers five authentication modes, namely **User, Group, RADIUS, POP3** and **LDAP**, adding flexibility to your choice of authentication method.

Terms in Authentication

Authentication Management

- Provides basic settings for managing authentication:
  - **Authentication Port Number:** The port number designated for authentication. By default, it is 82.
  - **Authentcation Idle Timeout:** If an authenticated connection has been idle for a period of time, it will expire. The default is 30 minutes.
  - **Log off users that have logged in for:** Determines the valid time for the authenticated connection. Authentication expires on the due time.
  - **Allow password modification:** The authenticated users may change the password by themselves.
  - **Deny multi-login if auth user has login:** When enabled, once a user has logged in with his / her own authentication account no other user is permitted to log in to the same account.
  - **Successful Authentication Redirect URL:** Authenticated user can be redirected to the designated web site by assigning its address to this field. Leaving it blank means the user will just go directly to their desired web site.
  - **Login Display Message:** The message shown (HTML supported) in the login screen. Leaving it blank will result in no message be shown.
    - Go to **Policy Object > Authentication > Settings** and configure as below:（**Figure 8-1**）

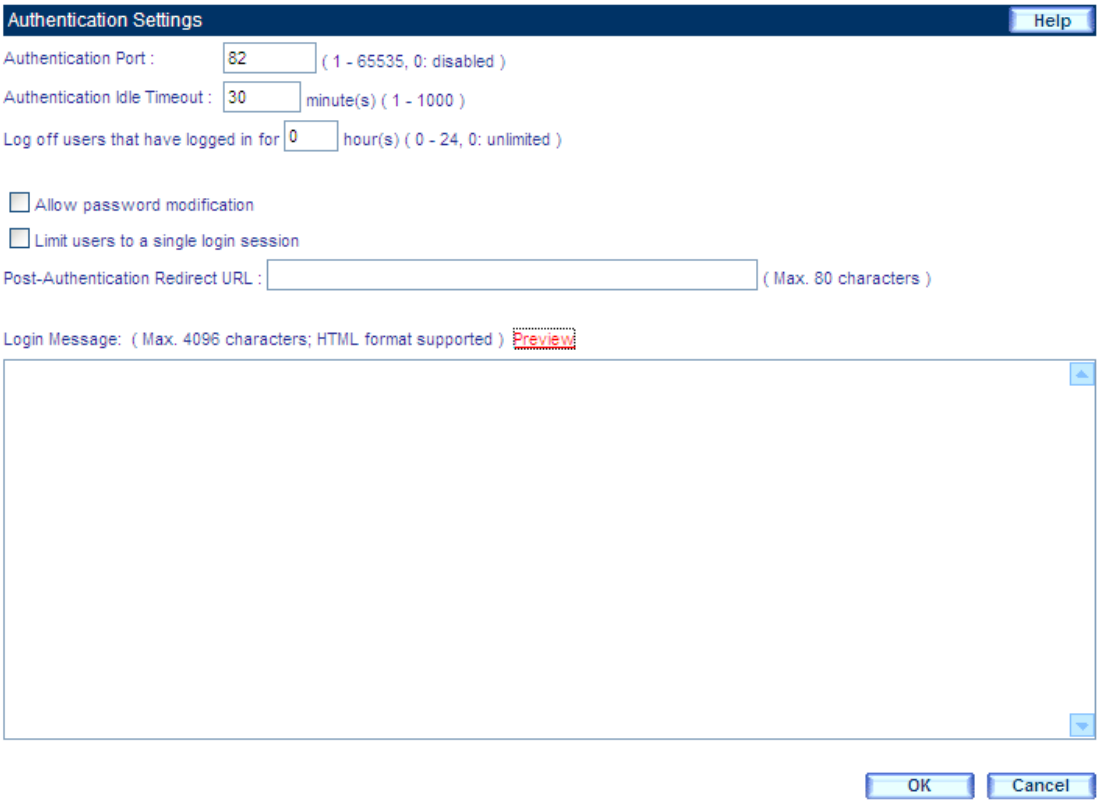


Figure 8-1 Authentication Management Settings

- The authentication login screen appears after a user attempts to access a web site:（**Figure 8-2**）

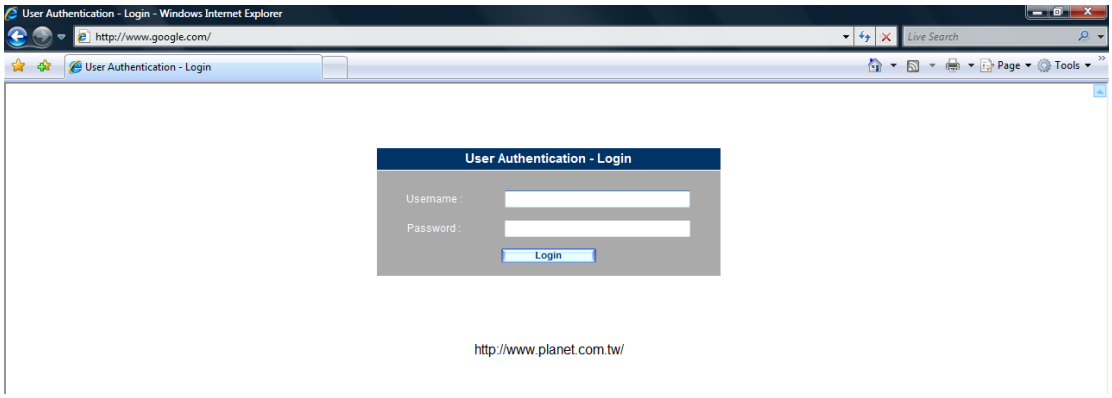


Figure 8-2 The Authentication Login Screen

- An authenticated user will be redirected to the designated web site:（**Figure 8-3**）

Figure 8-3 The User Being Redirected to a Website

Note：

1. The **Allow password modification** mechanism is only applicable to authenticated users.
2. The authentication login screen appears after either trying to access a web site or by typing the management address together with its authentication port number in the address field of a web browser.
3. the user authentication windows may block by the browsers pop-up feature.

Authentication User Name

- The user name for authentication.

Password

- The password for authentication.

Confirm Password

- The confirmation of password.

Force the user to change their password at their next login

- The authenticated users must change their password at their next login.

The account’s authentication is valid through

- The time of the account’s authentication.

RADIUS Server Shared Secret

- The password used for authentication using a RADIUS server.

Enable 802.1x RADIUS Server Authentication

- When enabled, the device supports the wireless authentication of a wireless-capable RADIUS server.

LDAP Base DN

- The distinguished name for LDAP server.

LDAP Bind DN

Used for searching entries with a specific key wor

Name:

- The user name required by a LDAP server.

LDAP User Name

Lists the LDAP User Name from LDAP server. The user name may be grouped for authentication.

8.1 User / Group Authentication

8.1.1 Regulating Internet Access with a Policy

Step 1. Go to **Policy Object** > **Authentication** > **Account**, and then create some users who require to be authenticated.（**Figure 8-4**）

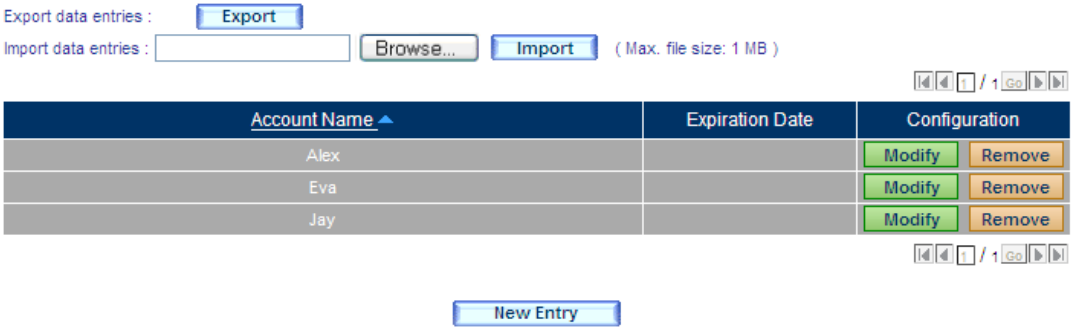


Figure 8-4 Authenticated Users Created

Note：

1. The IT administrator may export the Authentication user list for safe keeping, and restore the list if needed.
2. To use authentication, LAN users must configure their **Preferred DNS server** in **Internet Protocol (TCP/IP) Properties** to be the same as the LAN interface address of CS-2001.

Step 2. Under **Policy Object** > **Authentication** > **Group**, set as below:（**Figure 8-5**）

- Click **New Entry**.
- **Group Name**: Type a name for the group.
- Select group members from the **Available Authentication User** column on the left, and then click **Add**.
- Settings completed.

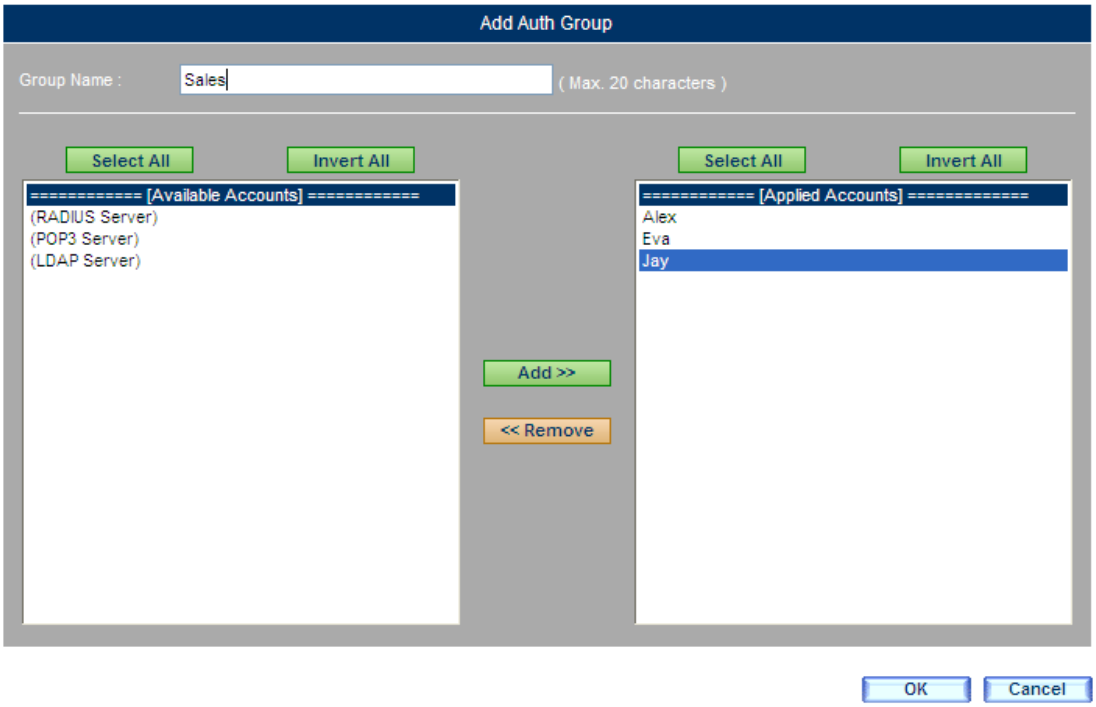


Figure 8-5 Configuring the Authenticated User Group

Step 3. Go to **Policy** > **Outgoing** and configure as below:（**Figure 8-6**）

- **Authentication:** Select the group name that was configured in the previous step.
- Click **OK**.（**Figure 8-7**）

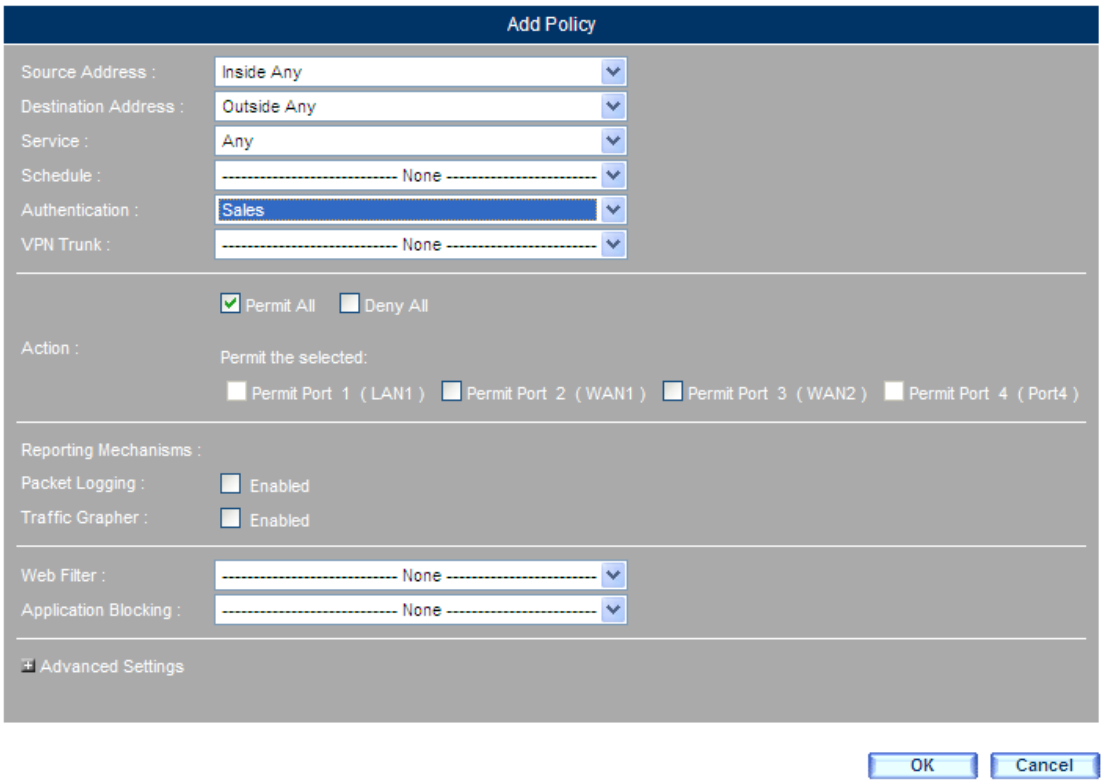


Figure 8-6 Apply the Authentication to a Policy

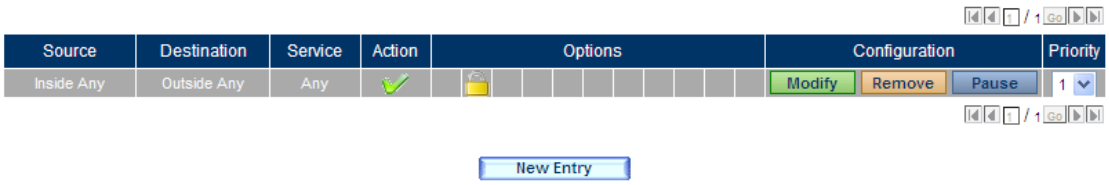


Figure 8-7 The Completed Policy Settings

Step 4. The authentication login screen is displayed in the web browser when a LAN user tries to access the Internet. Internet access will be available after applying the valid user name and password to the corresponding fields in the login screen.（**Figure 8-8**）

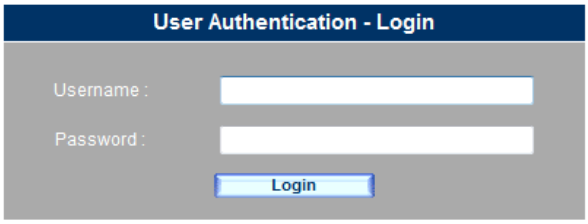


Figure 8-8 The Authentication Login Screen

Step 5. To end an authenticated session, you may click on the **Login** button in the window that popped up after authentication. Or, simply log onto **http://Management Address**: **Authentication Port Number/ logout.html** to logout.（**Figure 8-9**）

Figure 8-9 The Authentication Logout Screen

8.2 RADIUS Authentication

8.2.1 Regulating Internet Access with a Policy – An Example using the RADIUS Server from Windows Server 2003

※ The Configuration of Windows Server 2003 Built-in RADIUS Server

Step 1. Go to **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**, and then click **Add/Remove Windows Components** on the left.

Step 2. In the **Windows Components Wizard** window, select **Networking Services** and then double-click on it. (**Figure 8-10**)

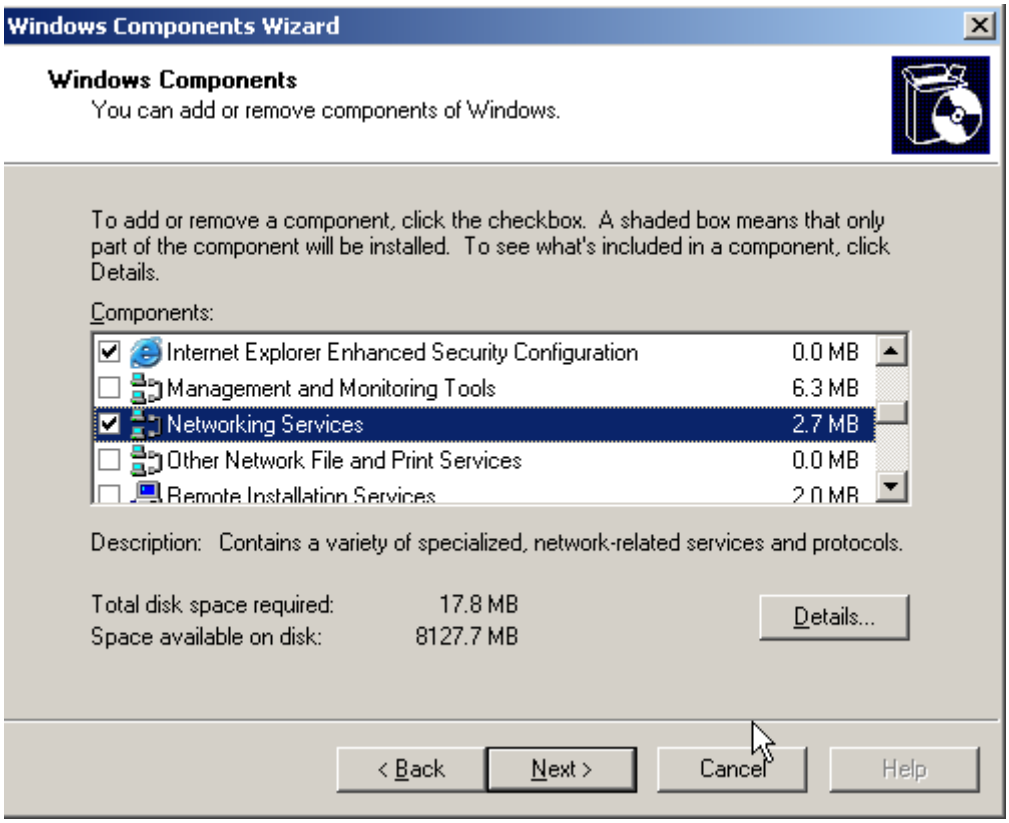


Figure 8-10 The Windows Components Screen

Step 3. The **Internet Authentication Service**. (**Figure 8-11**)

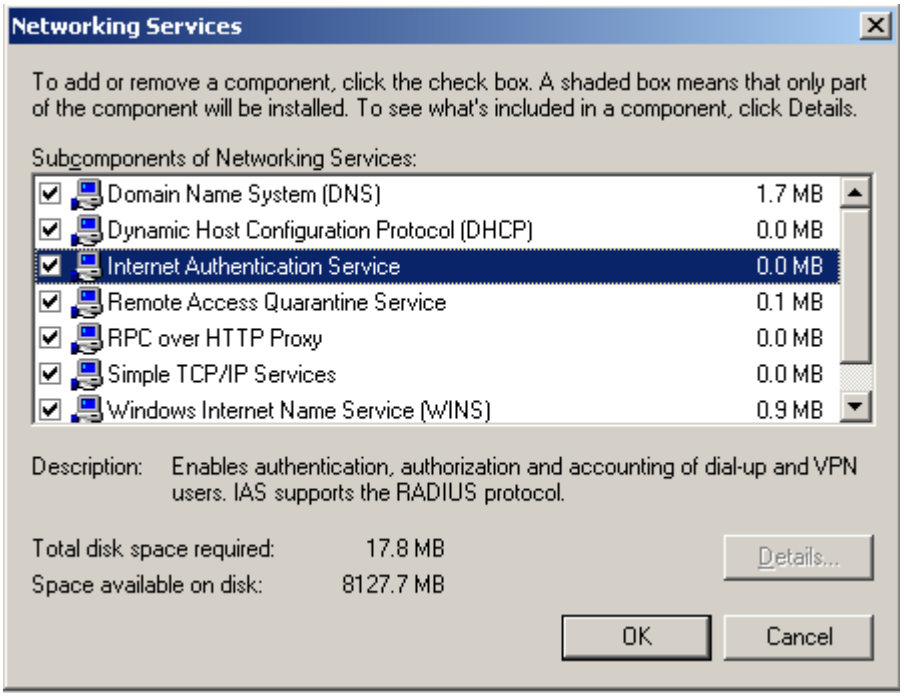


Figure 8-11 Selecting the Internet Authentication Service

Step 4. Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Internet Authentication Service,** and then click it. (**Figure 8-12**)

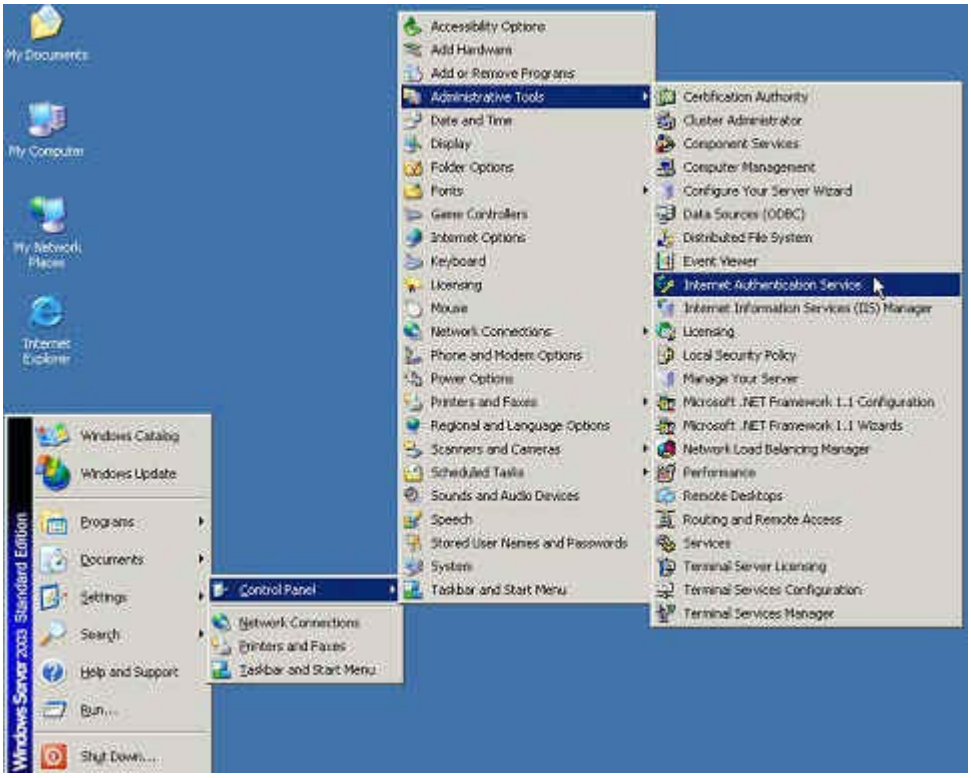


Figure 8-12 The Path of Internet Authentication Service on the Start Menu

Step 5. Right-click **RADIUS Clients** and then click **New RADIUS Client.**（**Figure 8-13**）

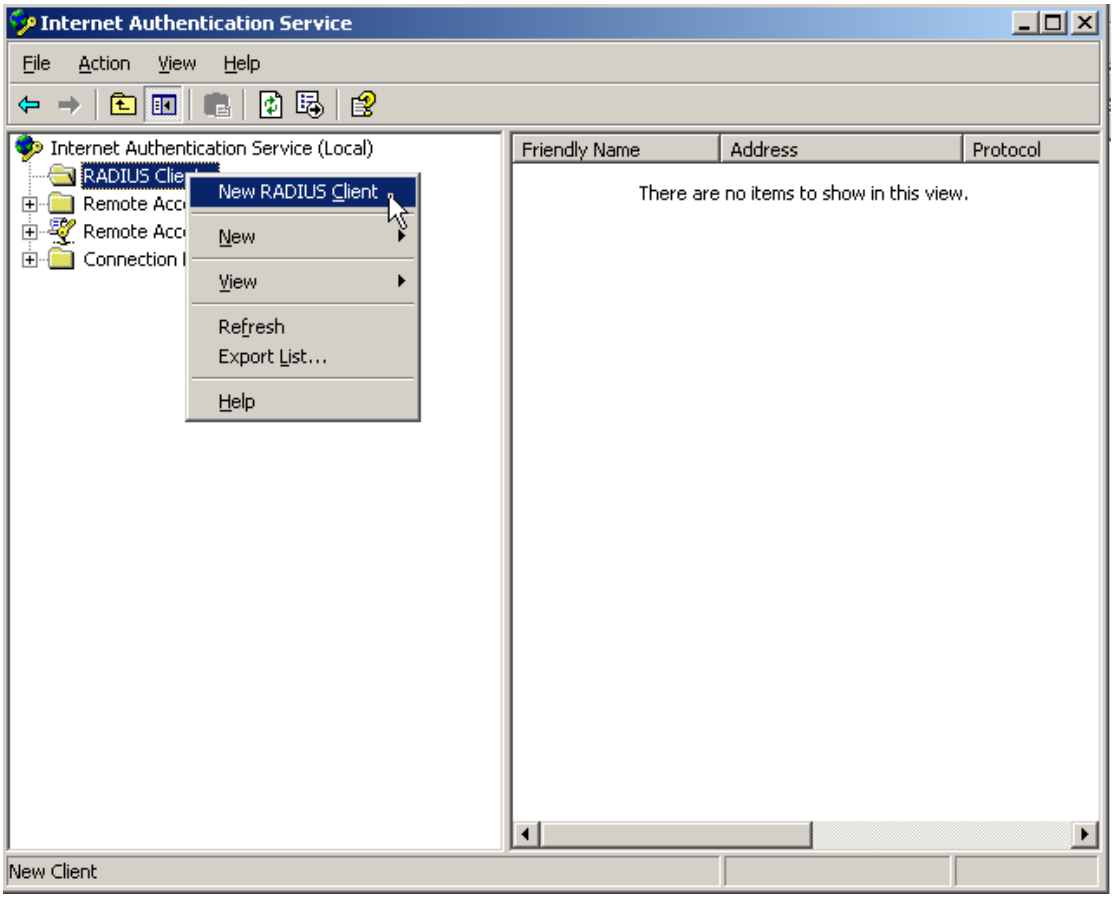


Figure 8-13 Adding a RADIUS Client

Step 6. Type a name and the client address, namely the management address of CS-2001.（**Figure 8-14**）

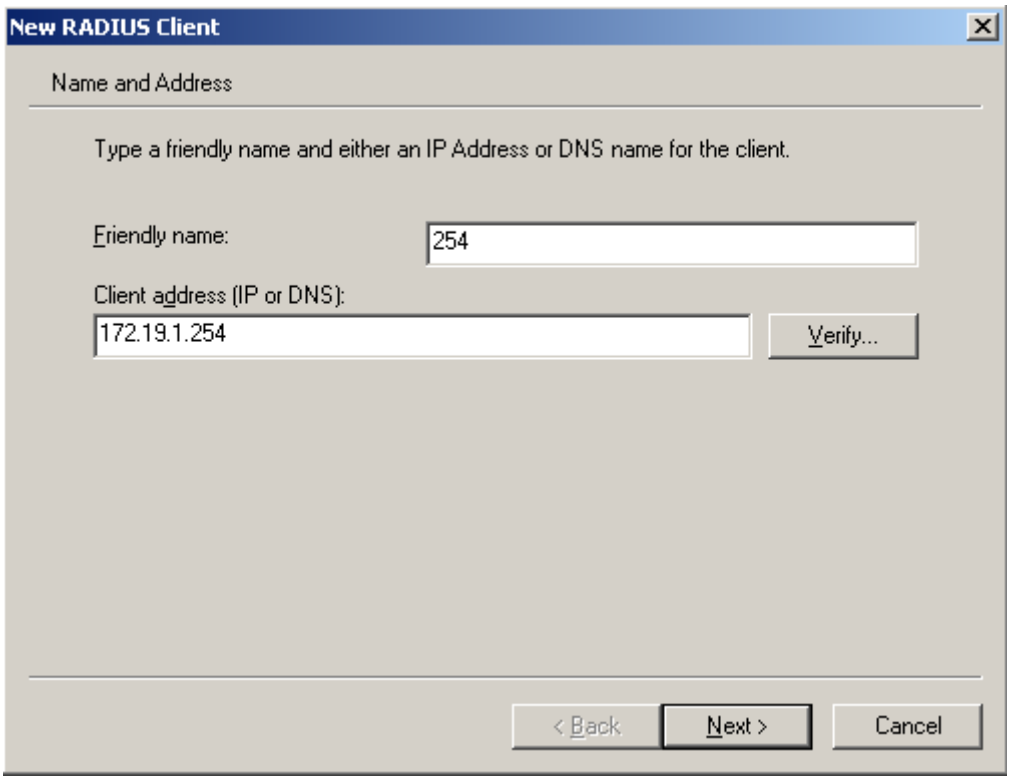


Figure 8-14 Typing a Friendly Name and the Management Address

Step 7. Select **RADIUS Standard** from the **Client-Vendor** dorp-down list, and then configure the **Shared secret** and **Confirm shared secret** as same as that of the CS-2001 under **Policy Object > Authentication > RADIUS**. （**Figure 8-15**）

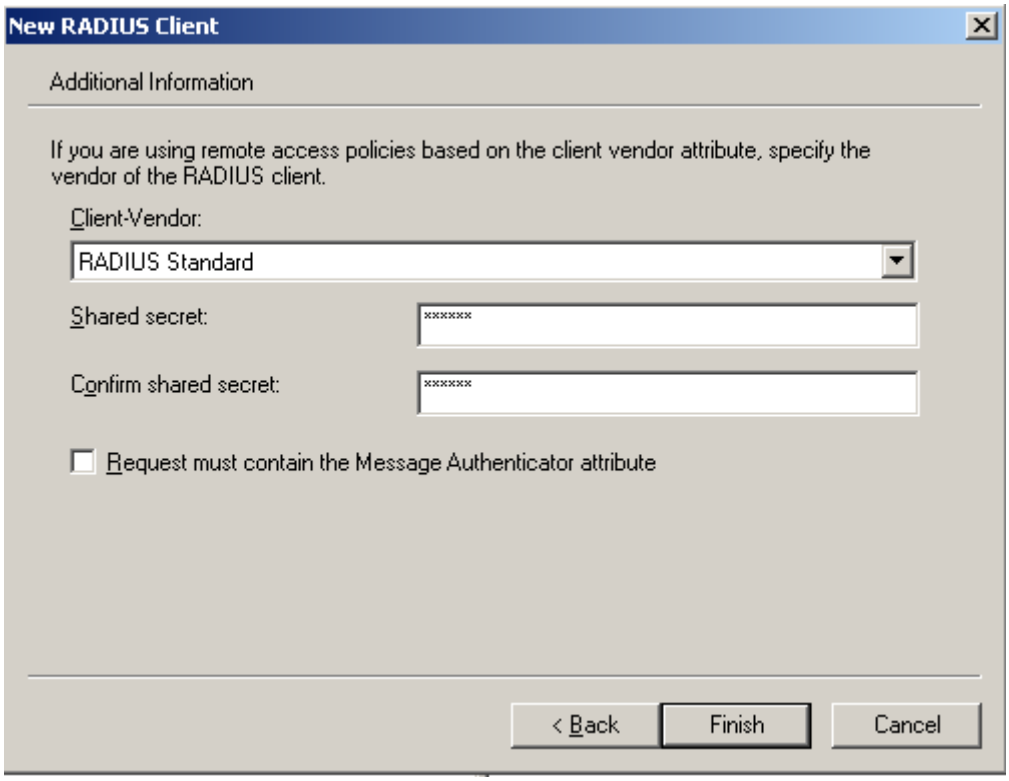


Figure 8-15 Selecting the Client Vendor and Entering the Password

Step 8. Right-click **Remote Access Policies** and then click **New Remote Access Policy**.（**Figure 8-16**）

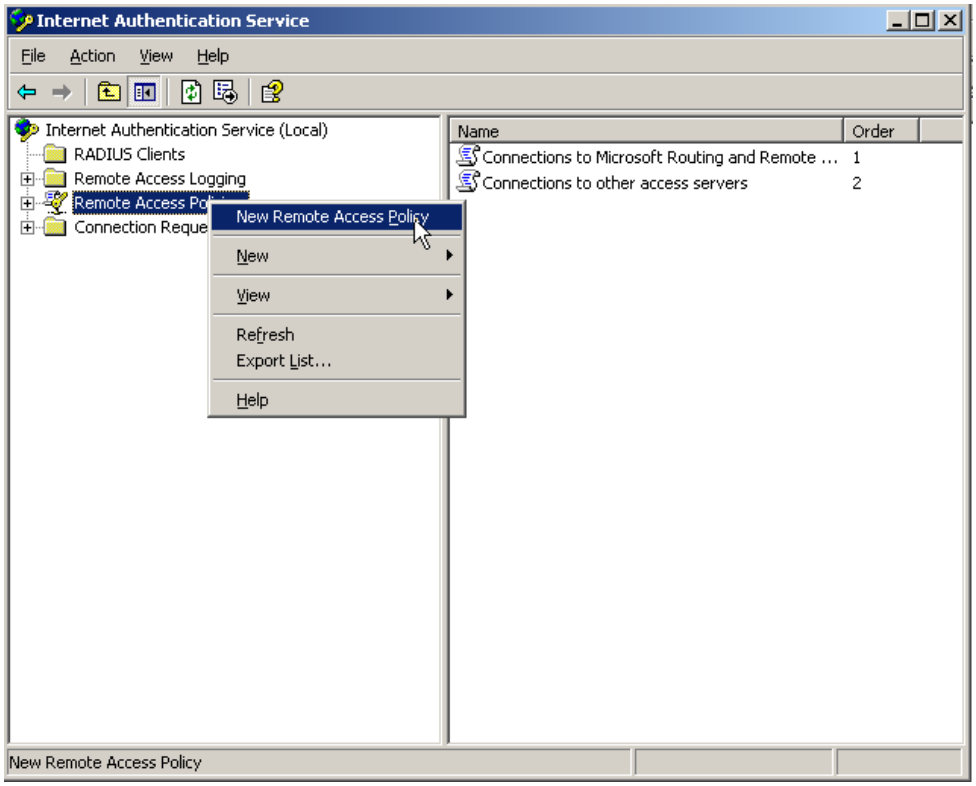


Figure 8-16 Adding a Remote Access Policy

Step 9. Select **Use the wizard to set up a typical policy for a common scenario** and then type a name in the **Policy name** field. (**Figure 8-17**)

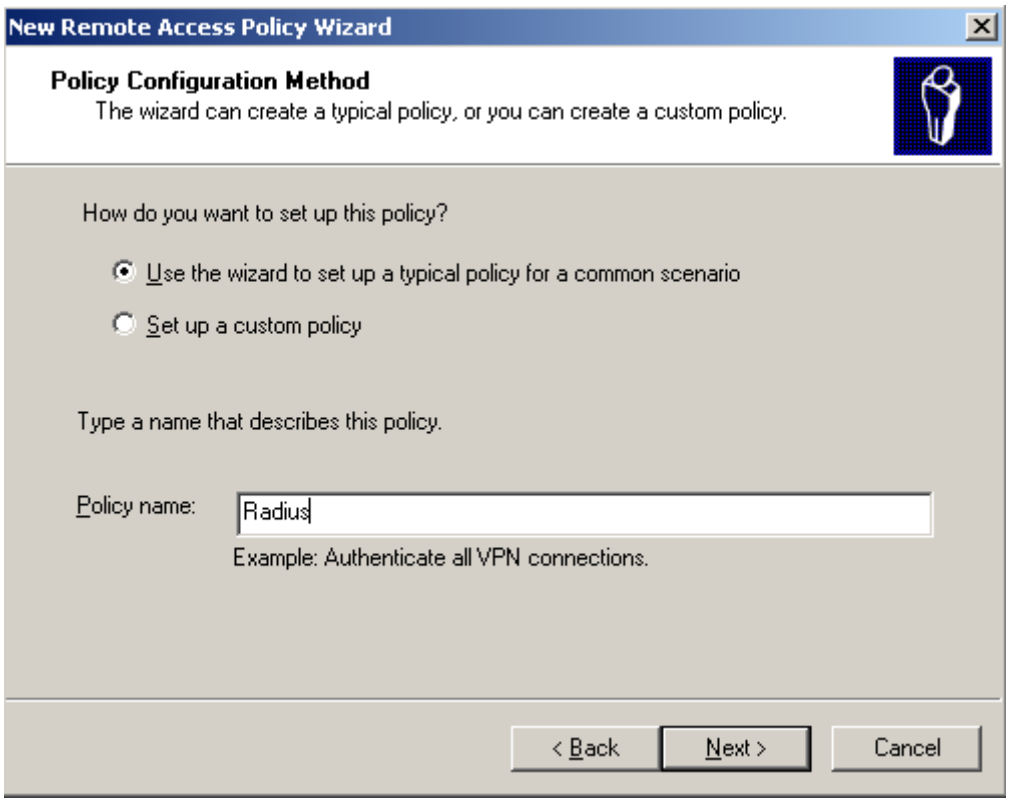


Figure 8-17 Configuring and Naming the Policy

Step 10. Select **Ethernet**.（Figure 8-18）

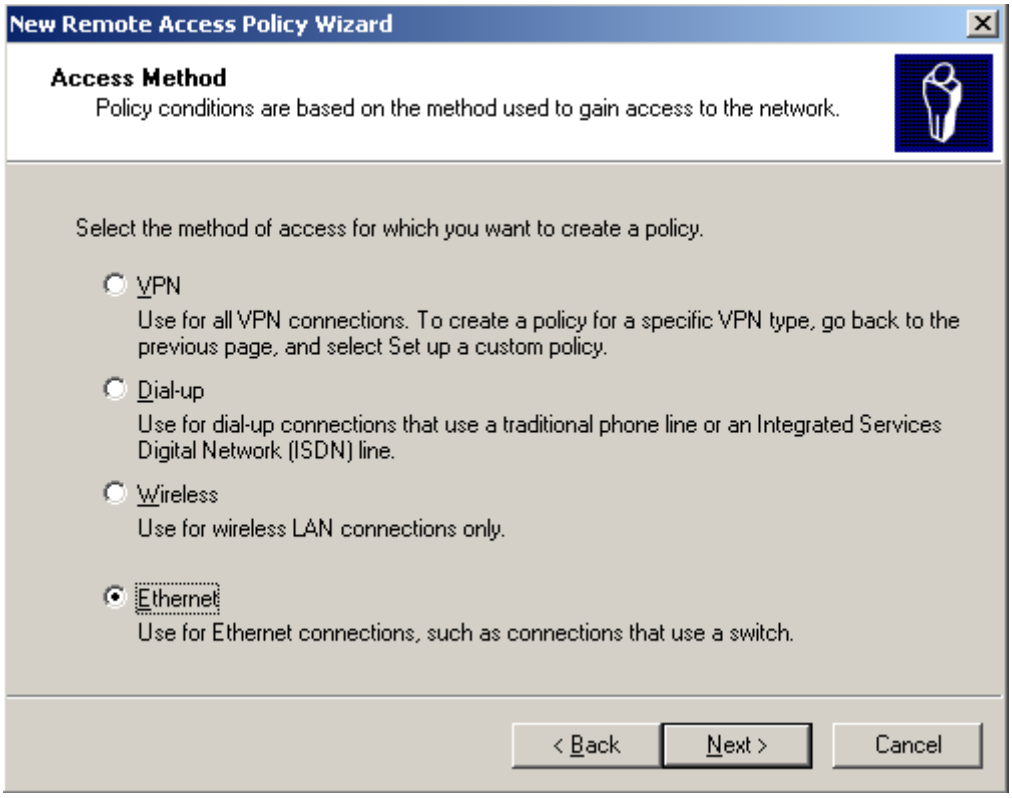


Figure 8-18 Selecting the Access Method

Step 11. Select **User**. (**Figure 8-19**)

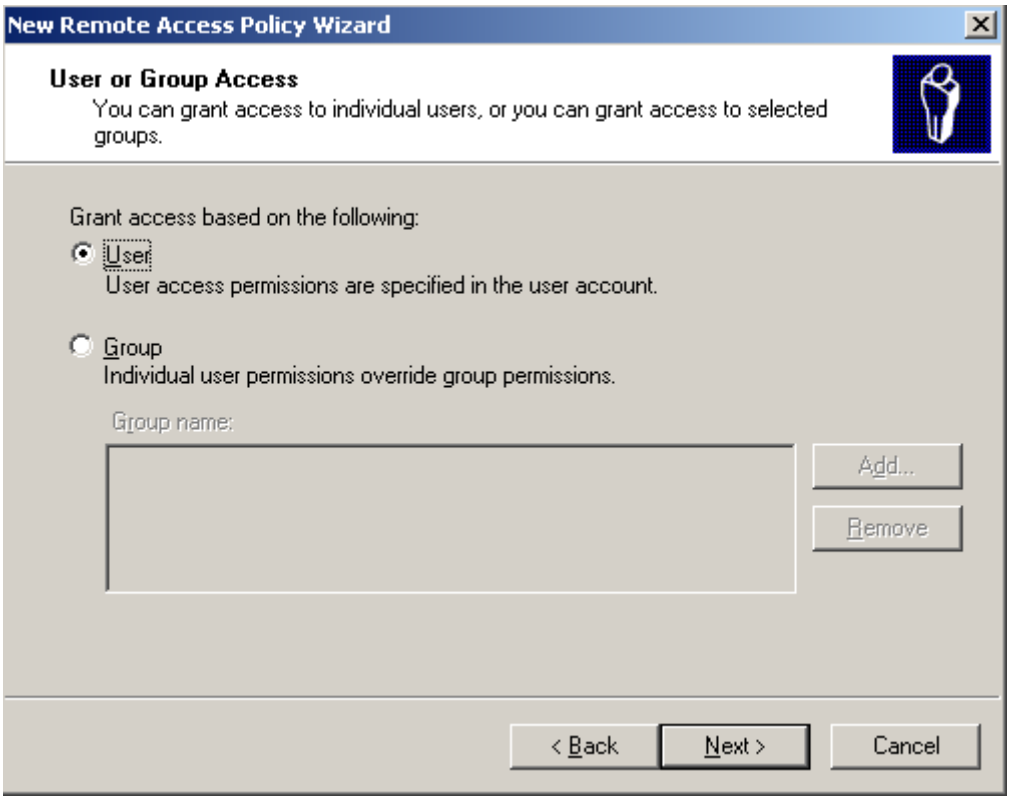


Figure 8-19 Selecting User or Group Access

Step 12. Select **MD5-Challenge** from the drop-down list. (**Figure 8-20**)

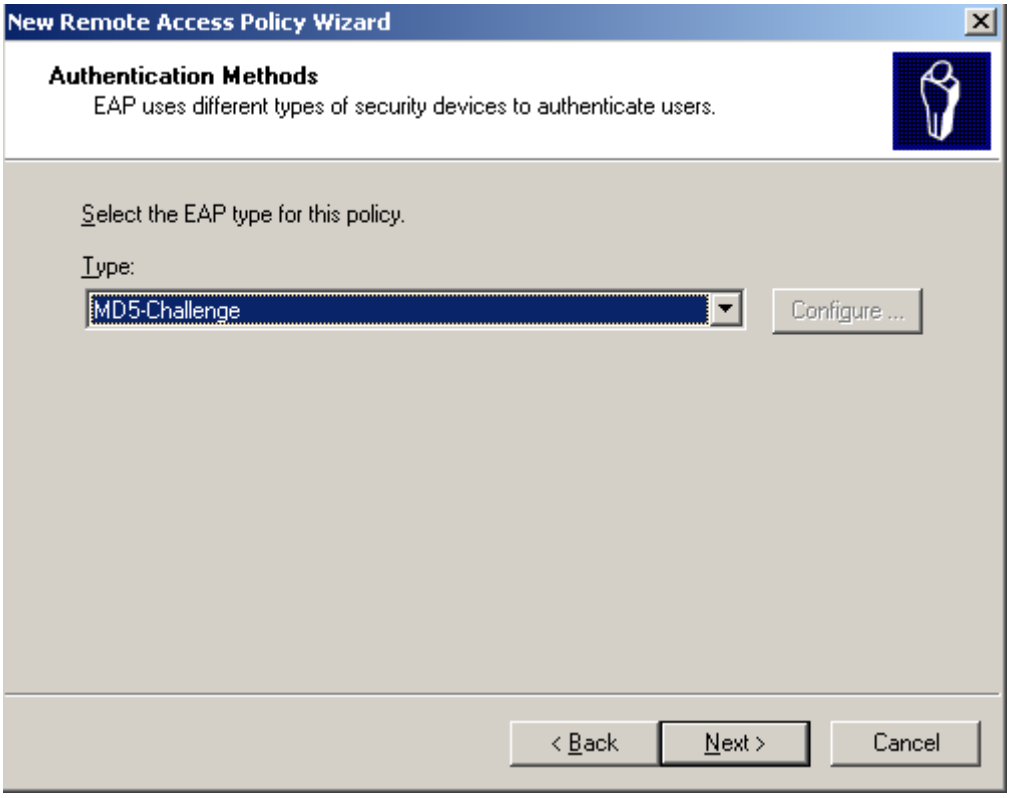


Figure 8-20 Selecting an Authentication Method

Step 13. Right-click the newly added policy name and then click **Properties.** （**Figure 8-21**）

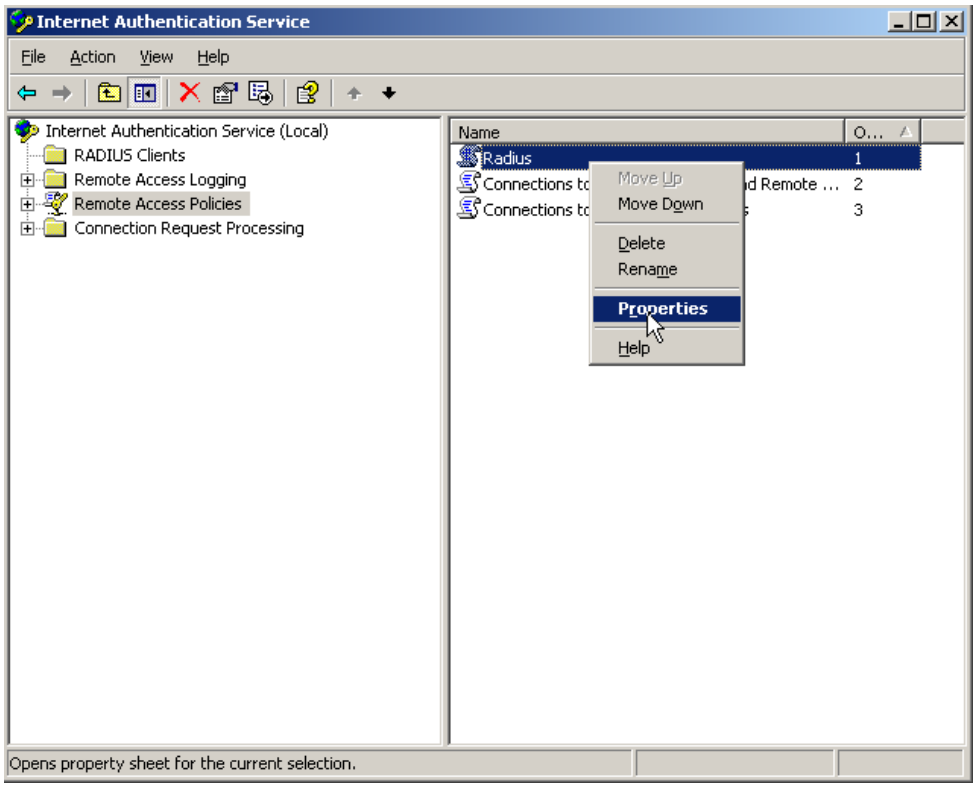


Figure 8-21 Configuring the Properties of a Policy

Step 14. Select **Grant remote access permission** and then remove the existing settings. Next, click **Add…**. (**Figure 8-22**)

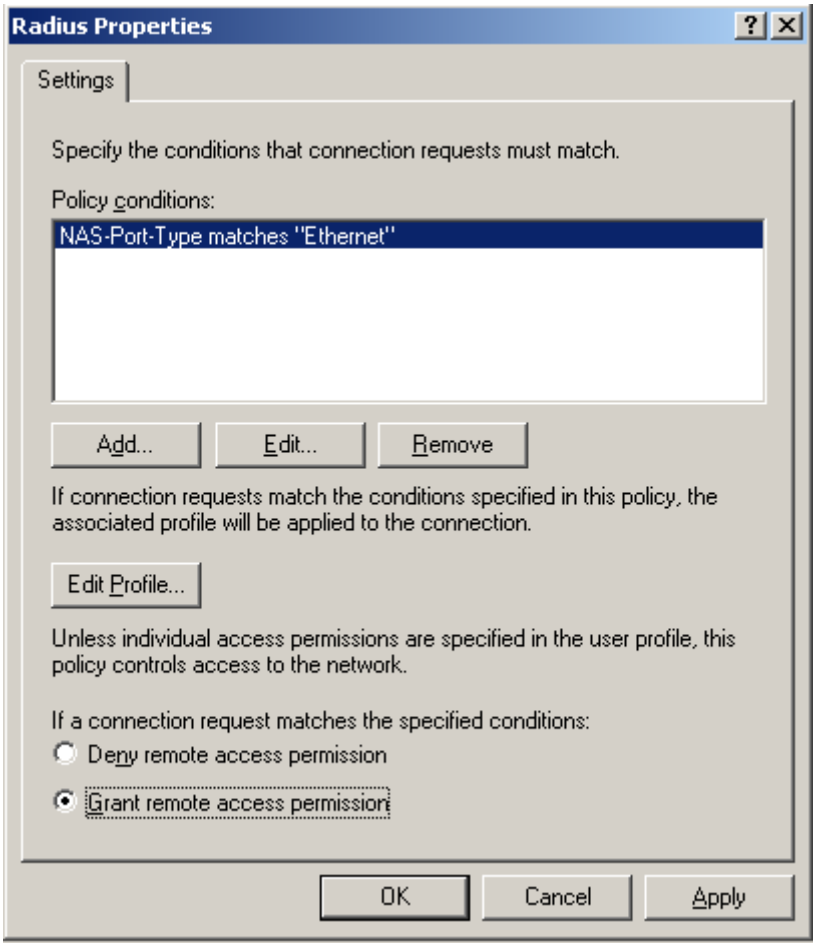


Figure 8-22 Configuring the RADIUS Properties

Step 15. Select **Service-Type** to add. (**Figure 8-23**)

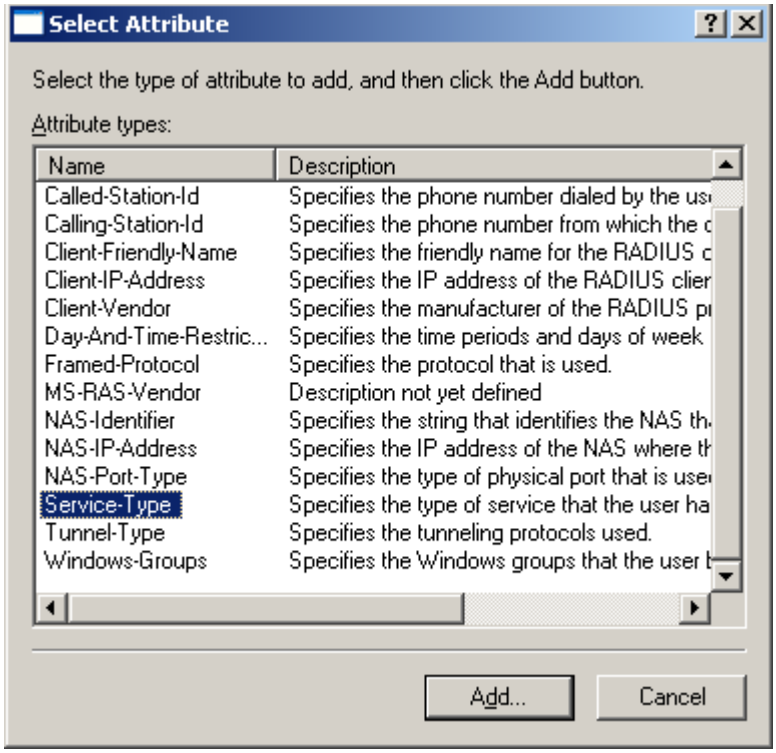


Figure 8-23 Select the Attribute Type

Step 16. Select **Authenticate Only** and **Framed** from the **Available types** and then click **Add**. (**Figure 8-24**)

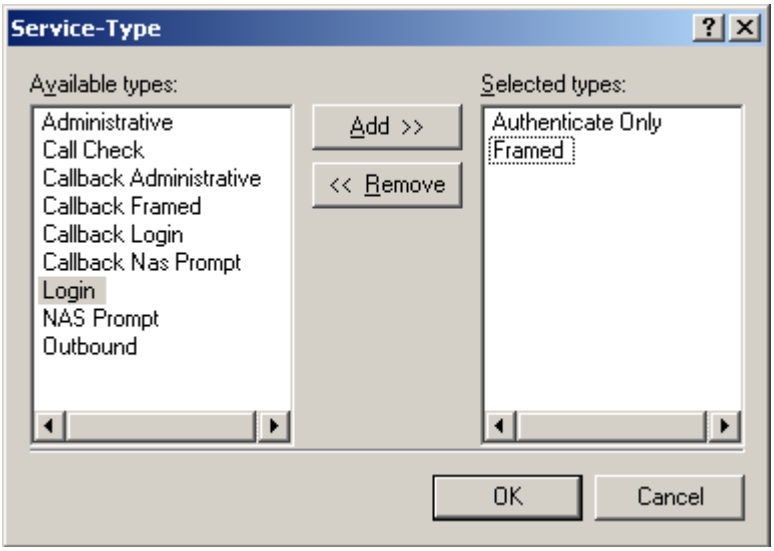


Figure 8-24 Adding the Service Type

Step 17. Click on the **Edit Profile**…, then click the **IP** tab and then tick **Server settings determine IP address assignment**.（Figure 8-25）

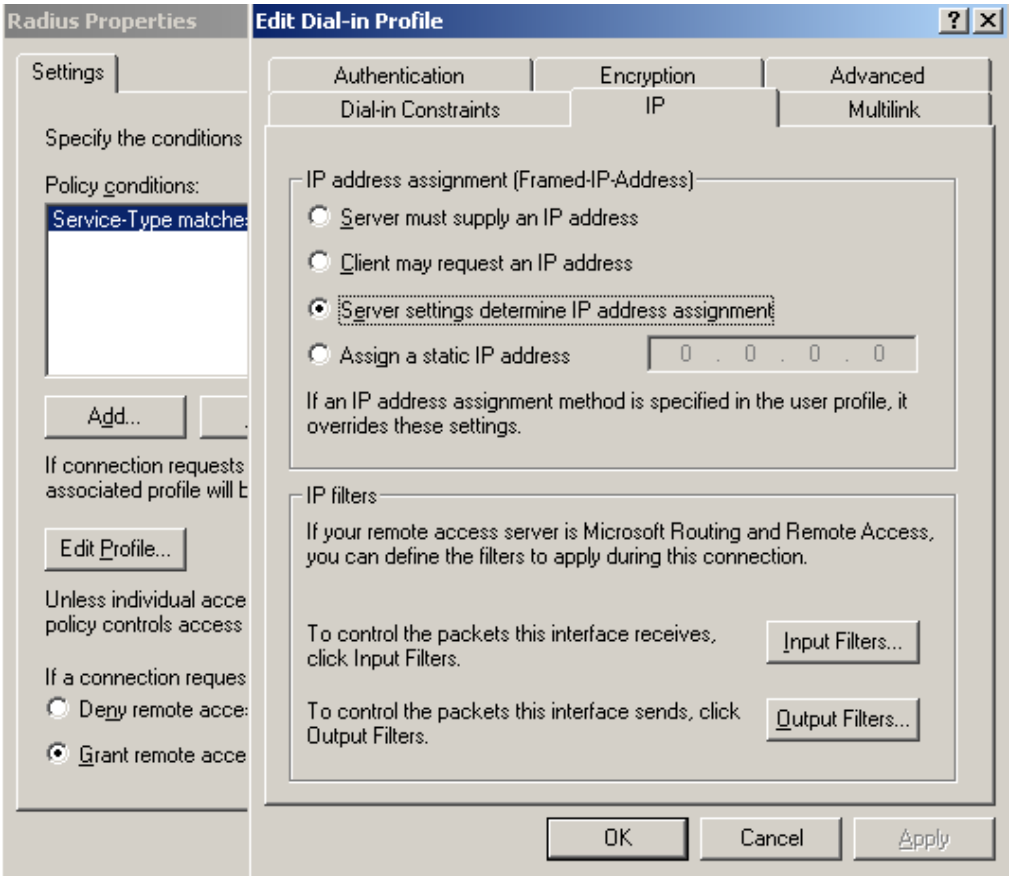


Figure 8-25 Configuring the IP Setting

Step 18. Click on the **Edit Profile…** button then click on the **Authentication** tab. Tick **Microsoft Encrypted Authentication version 2 (MS-CHAP v2), Microsoft Encrypted Authentication (MS-CHAP), Encrypted authentication (CHAP)** and **Unencrypted authentication [PAP, SPAP].** （**Figure 8-26**）

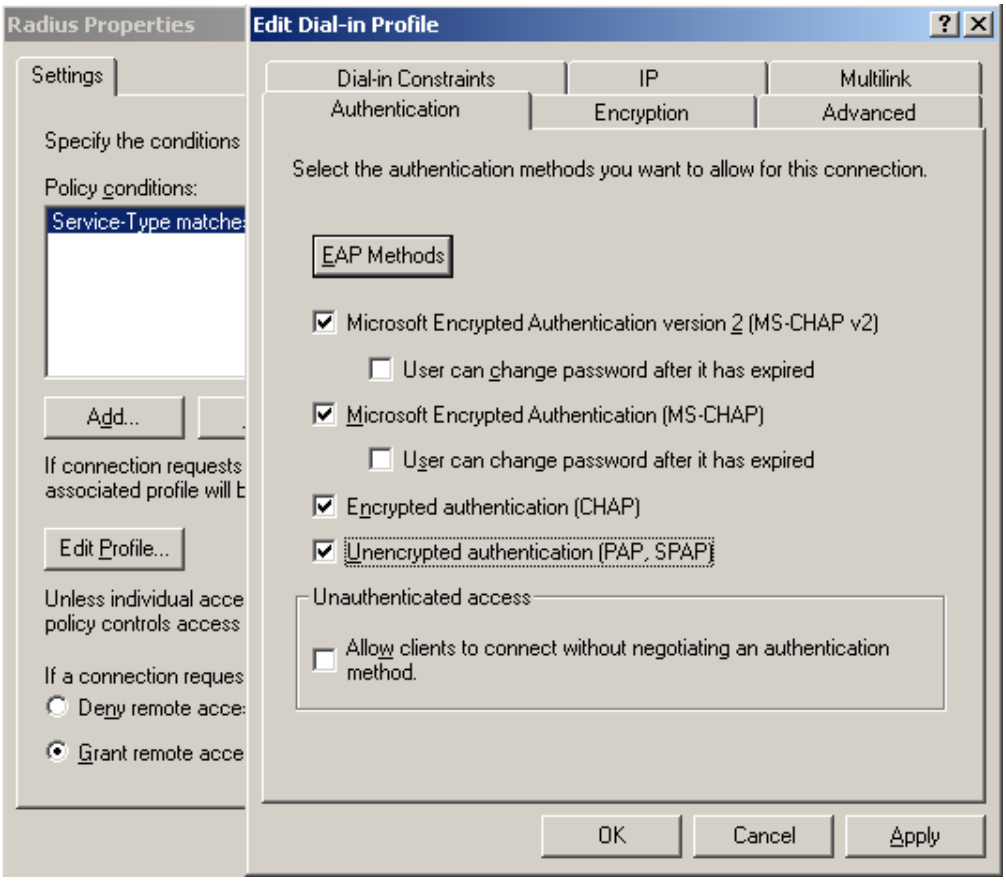


Figure 8-26 Configuring the Authentication Settings

Step 19. Click on the **Edit Profile…**, click the **Advanced** tab and then click **Add….**（**Figure 8-27**）

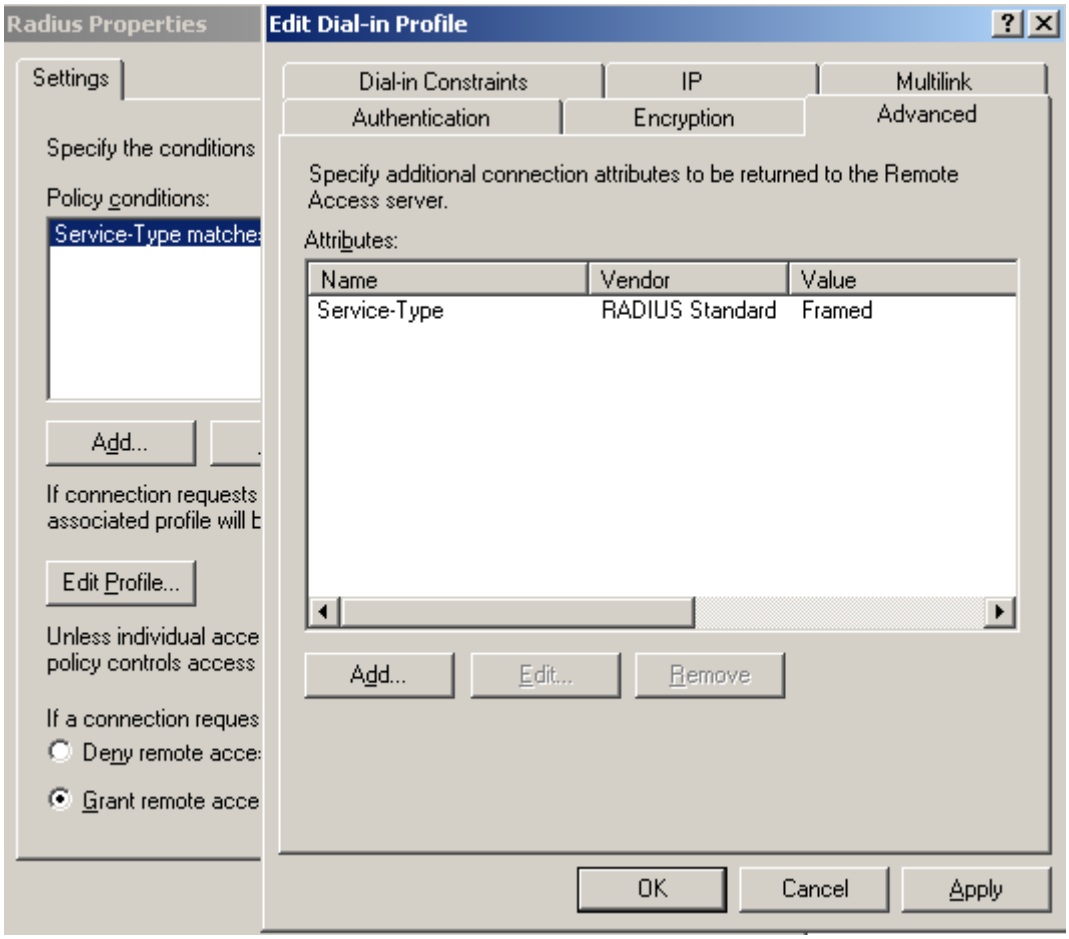


Figure 8-27 Configuring the Advanced Settings

Step 20. Select **Framed-Protocol** and click **Add**. (**Figure 8-28**)

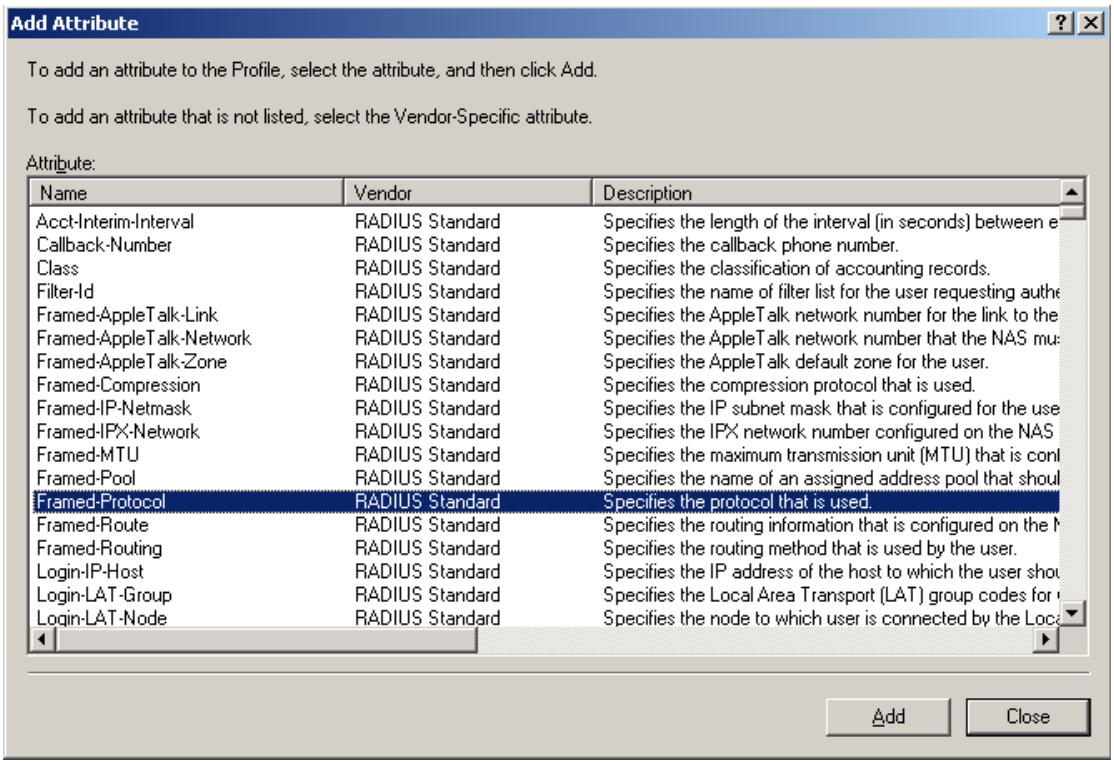


Figure 8-28 Adding the Attribute

Step 21. For **Framed-Protocol**, select **PPP** from the **Attribute value** drop-down list.（**Figure 8-29**）

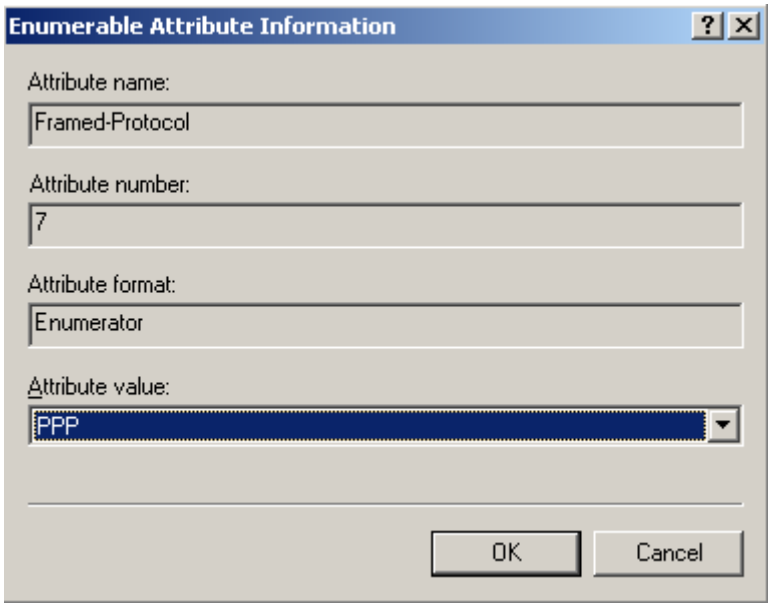


Figure 8-29 Attribute Setting 1

Step 22. For **Service-Type**, select Framed from the **Attribute value** drop-down list.（**Figure 8-30**）

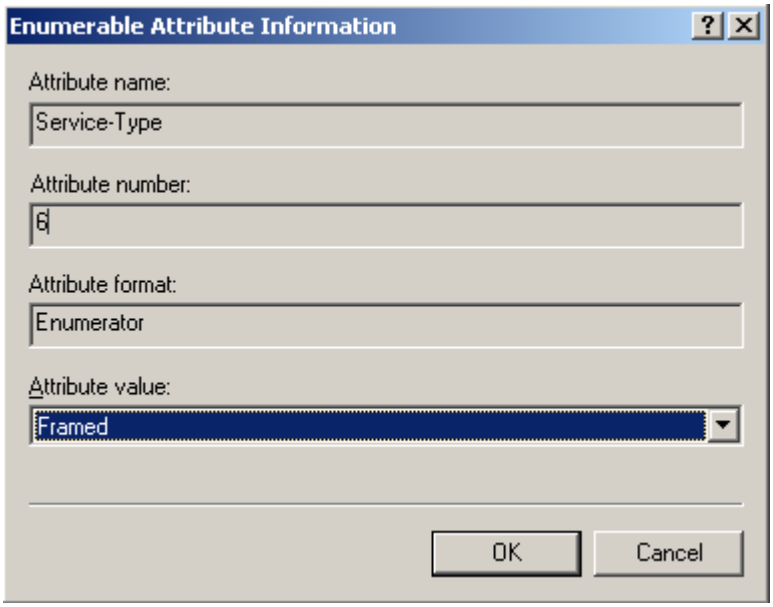


Figure 8-30 Attribute Setting 2

Step 23. Go to **Start > Settings > Control Panel > Administrative Tools,** then select **Computer Management**.（**Figure 8-31**）

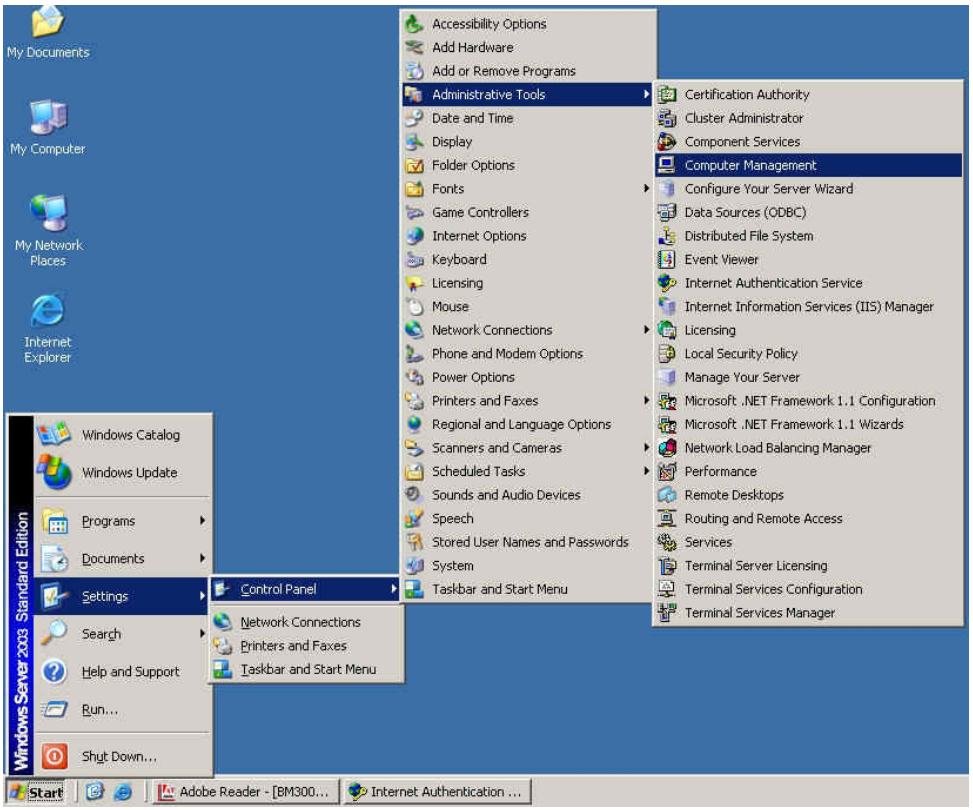


Figure 8-31 Selecting "Computer Management" on the Start Menu

Step 24. In the left column, go to **Computer Management (Local) > System Tools > Local Users and Groups > Users** and then right-click it. After that, click **New User….**（**Figure 8-32**）

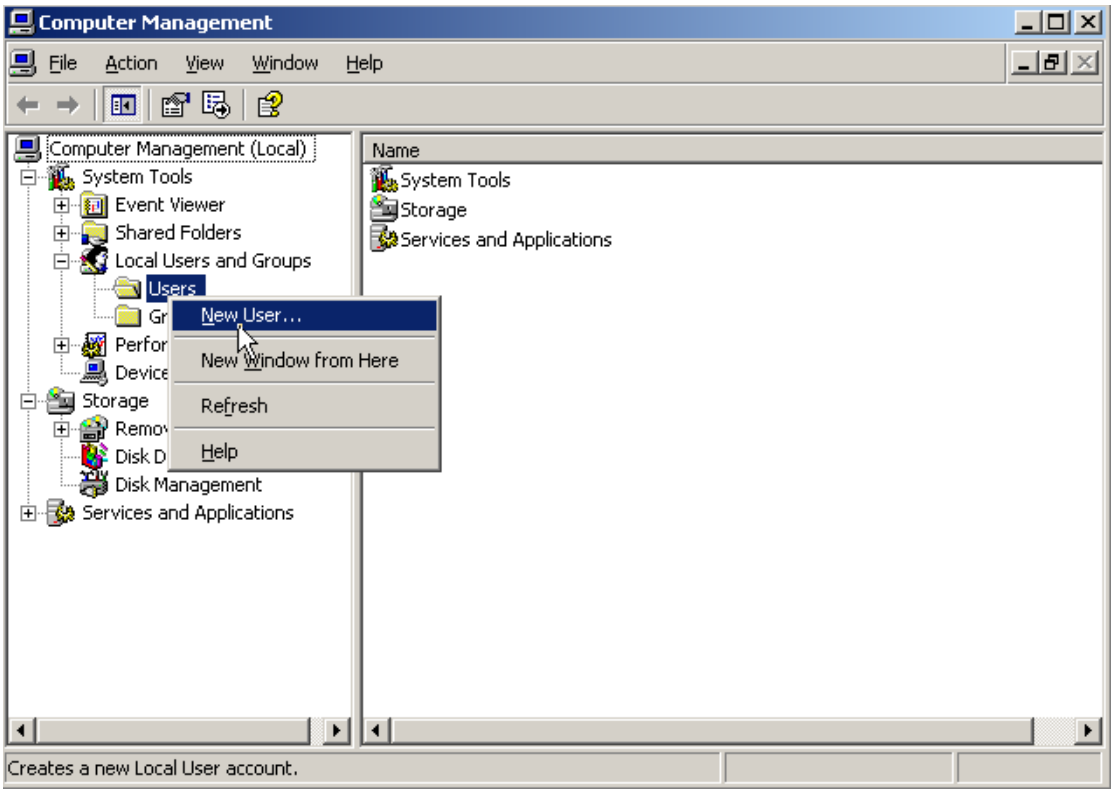


Figure 8-32 Adding a User

Step 25. Settings completed.

Step 26. Under **Policy Object** > **Authentication** > **RADIUS**, configure each field to be the same as the settings of Windows Server 2003 built-in RADIUS server:（**Figure 8-33**）

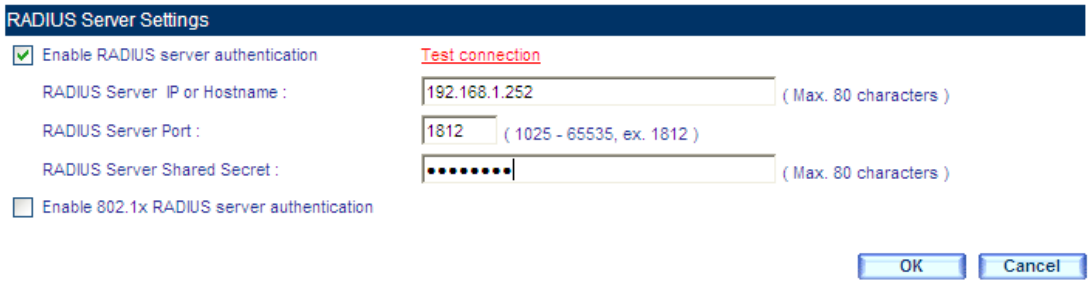


Figure 8-33 The RADIUS Server Settings

Note：

1. You may click **Test Connection** to detect the connection between CS-2001 and RADIUS server.

Step 27. Under **Policy Object** > **Authentication** > **Group**, select **RADIUS Server** from the **Available Authentication User** column and then click **Add**.（**Figure 8-34**）

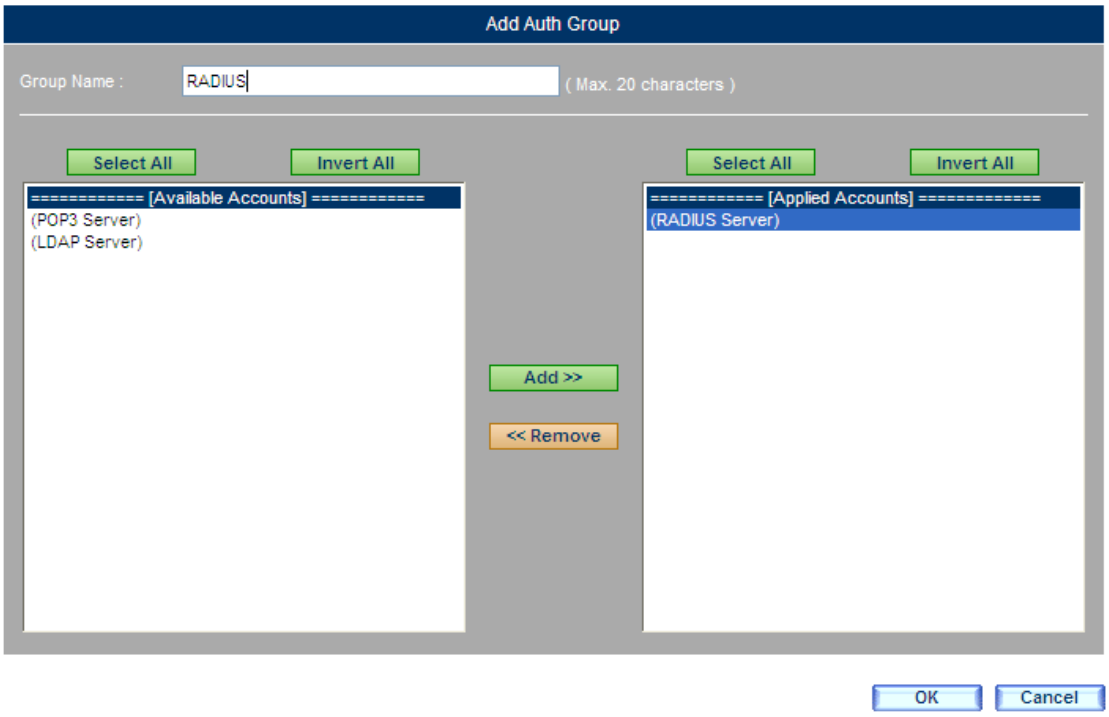


Figure 8-34 Adding RADIUS User to an Authenticated Group

Step 28. Under **Policy** > **Outgoing**, set as below:（**Figure 8-35**）

- Select the defined user group for **Authentication User**.
- Click **OK**.（**Figure 8-36**）

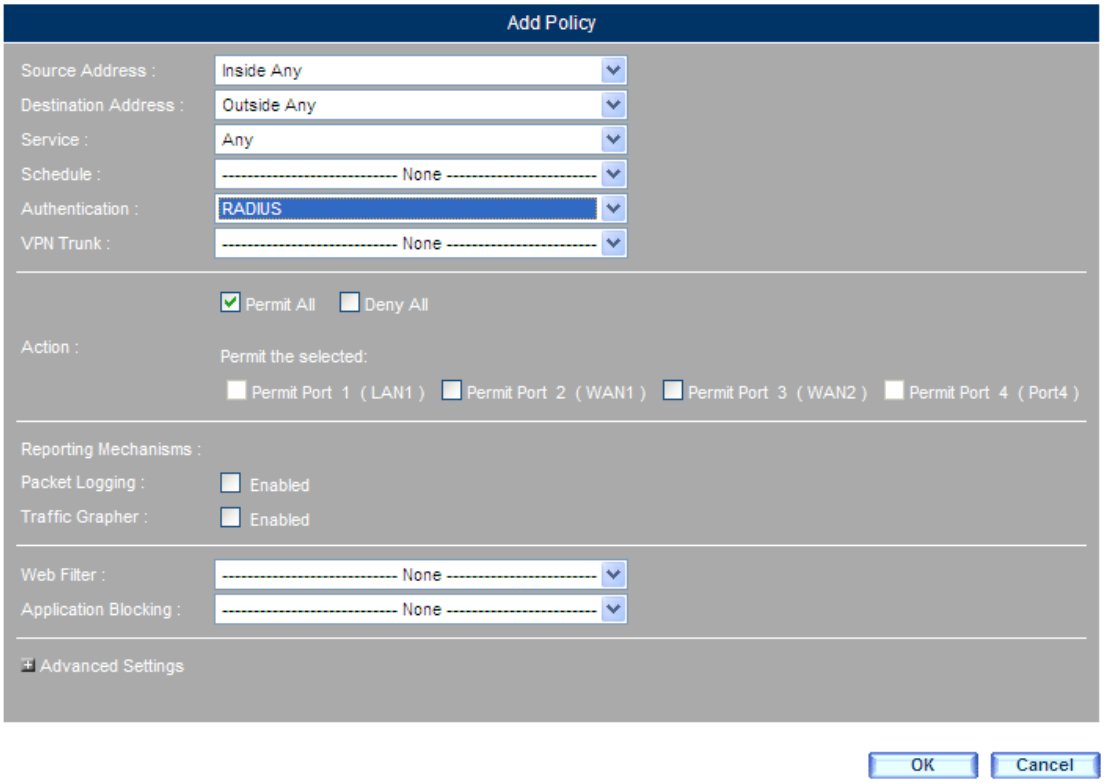


Figure 8-35 Applying the Authentication to a Policy

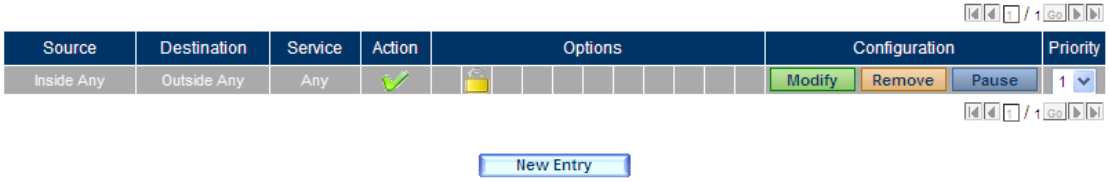


Figure 8-36 The Completed Policy Settings

Step 29. The authentication login screen will appear in the web browser with which a LAN user tries to surf the Internet. Internet access will be available after applying the valid user name and password to the corresponding fields in the login screen.（**Figure 8-37**）

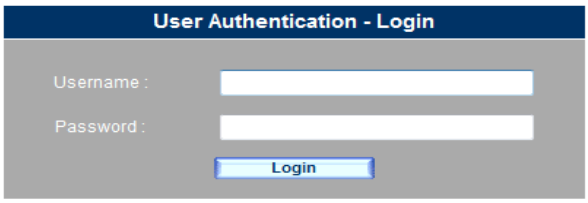


Figure 8-37 The Authentication Login Screen

8.3 POP3 Authentication

8.3.1 Regulating Internet Access with a Policy – An Example of POP3

Step 1. Under **Policy Object** > **Authentication** > **POP3**, set as below: (**Figure 8-38**)

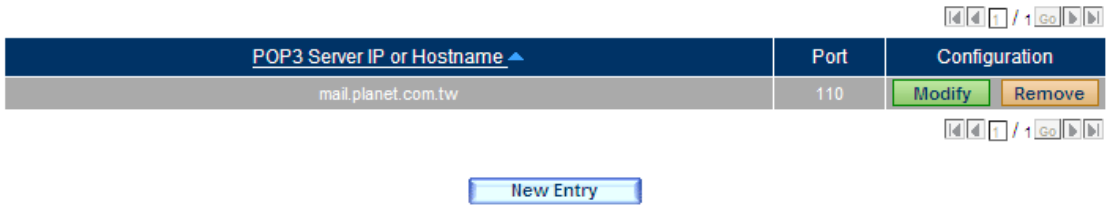


Figure 8-38 The POP3 Server Settings

Note：

1. You may click **Test Connection** to test the connection between CS-2001 and the POP3 server.

Step 2. From **Policy Object** > **Authentication** > **Group**, select **POP3 User** from the **Available Addresses** column and then click **Add**. (**Figure 8-39**)

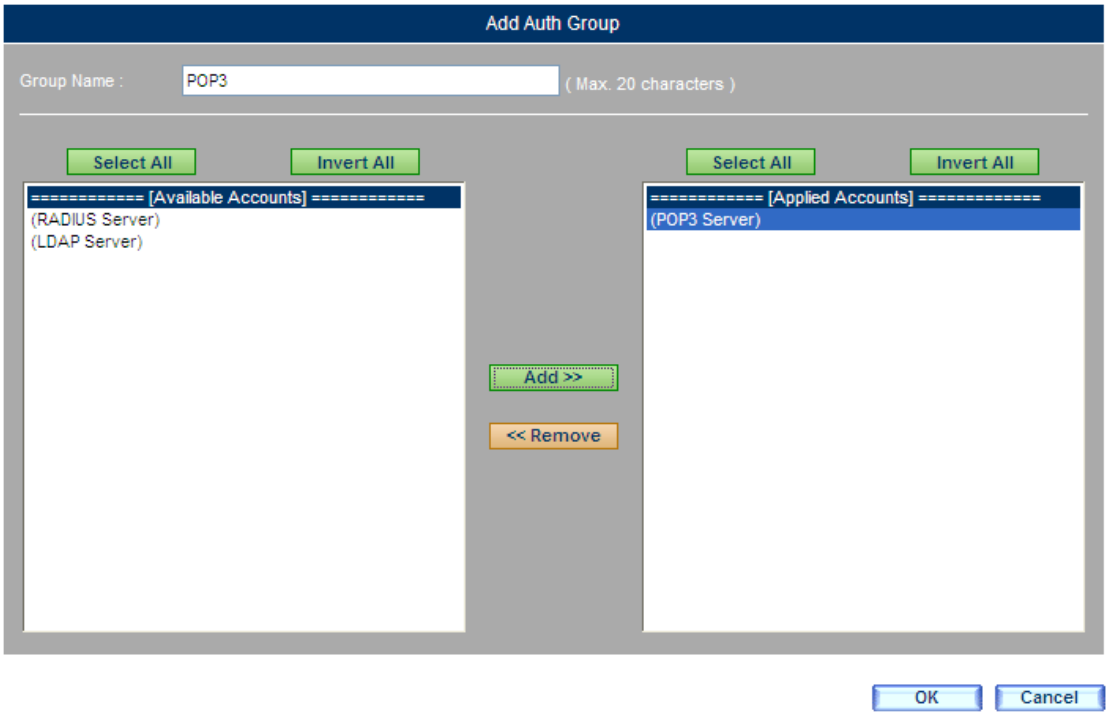


Figure 8-39 Adding POP3 User to an Authenticated Group

Step 3. Under **Policy** > **Outgoing**, set as below: (**Figure 8-40**)

- **Authentication**: Select the user group.
- Click **OK**. (**Figure 8-41**)

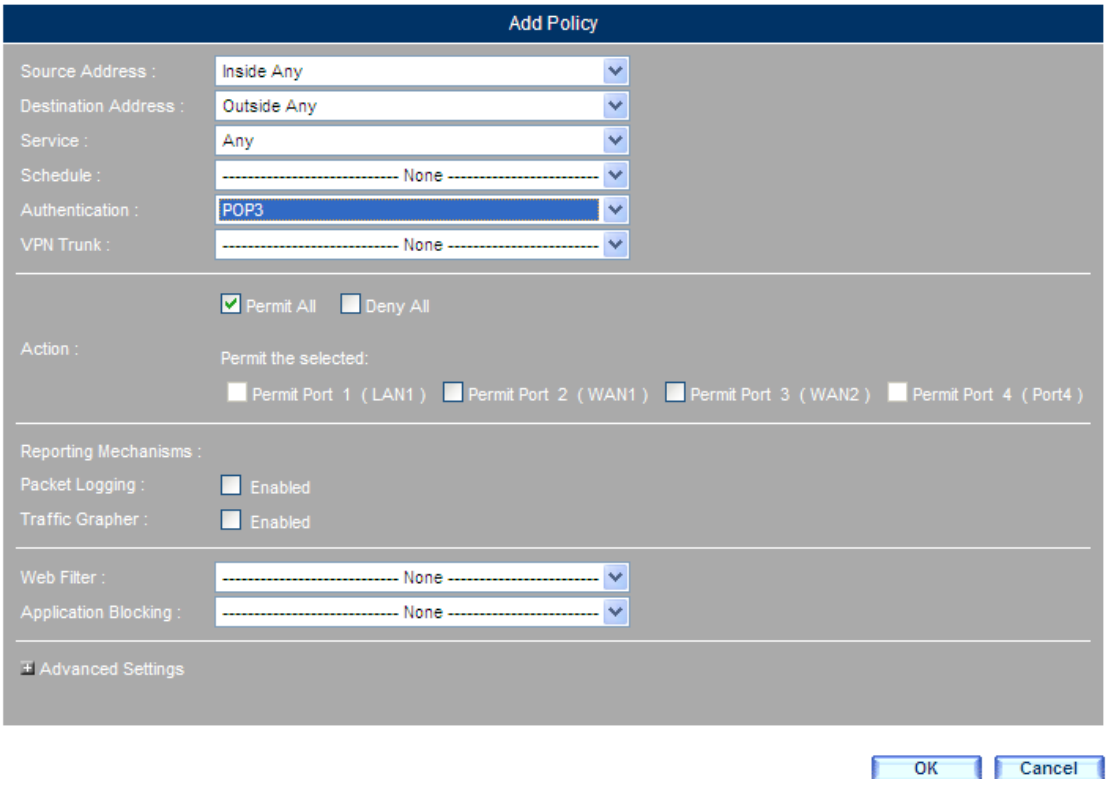


Figure 8-40 Using POP3 Authentication in a Policy

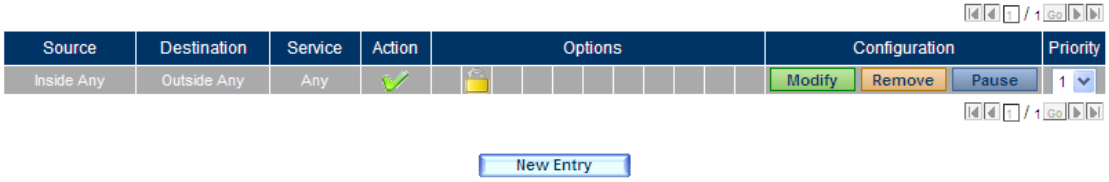


Figure 8-41 A Policy with POP3 Authentication

Step 4. The authentication login screen appears in the web browser when a LAN user tries to access the Internet. Internet access will be available after applying the valid user name and password to the corresponding fields in the login screen. (**Figure 8-42**)

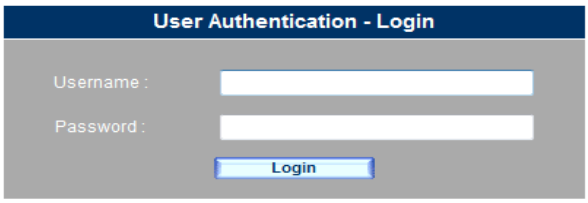


Figure 8-42 The Authentication Login Screen

8.4 LDAP Authentication

8.4.1 Regulating Internet Access with a Policy — An Example of Windows Server 2003 Built-in LDAP Server

※ The Configuration of the LDAP Server from Windows Server 2003

Step 1. Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Manage Your Server.**

Step 2. In the **Manage Your Server** window, click "**Add or remove a role**".（**Figure 8-43**）

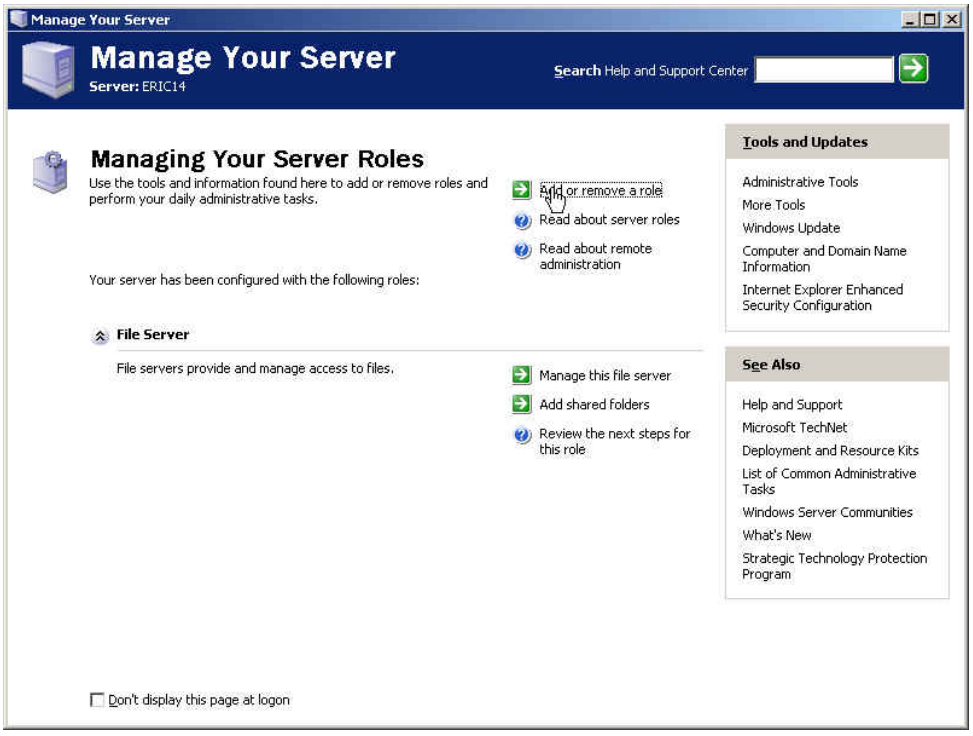


Figure 8-43 Managing Your Server

Step 3. In the **Preliminary Steps** window, click **Next**. (Figure 8-44)

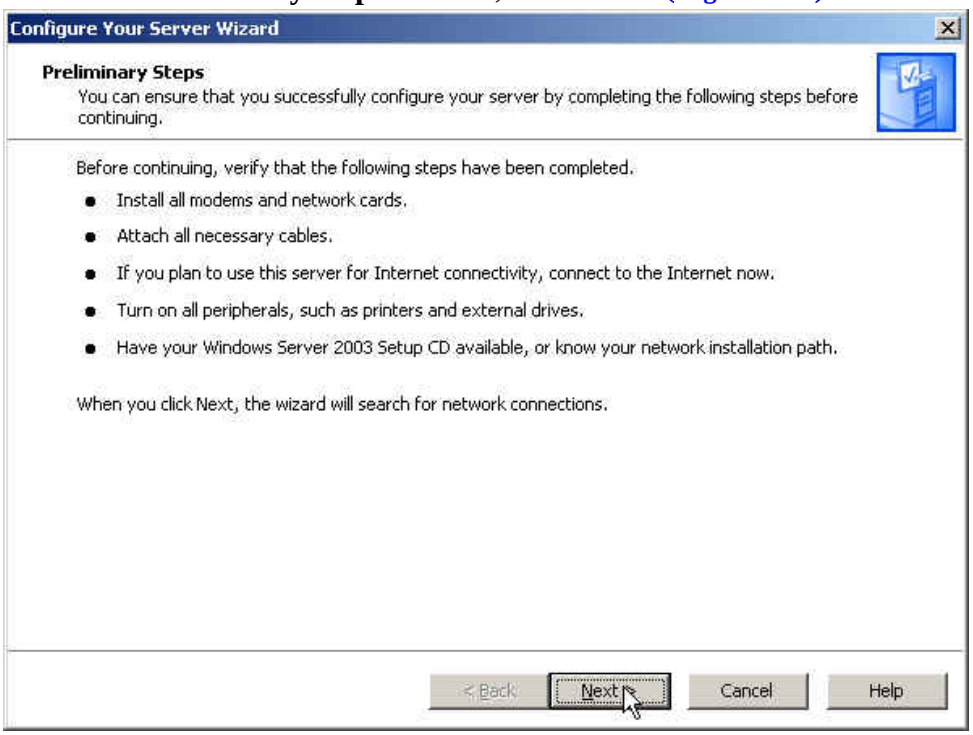


Figure 8-44 Preliminary Steps

Step 4. In the **Server Role** window, select **Domain Controller (Active Directory)** and click **Next**. (Figure 8-45)

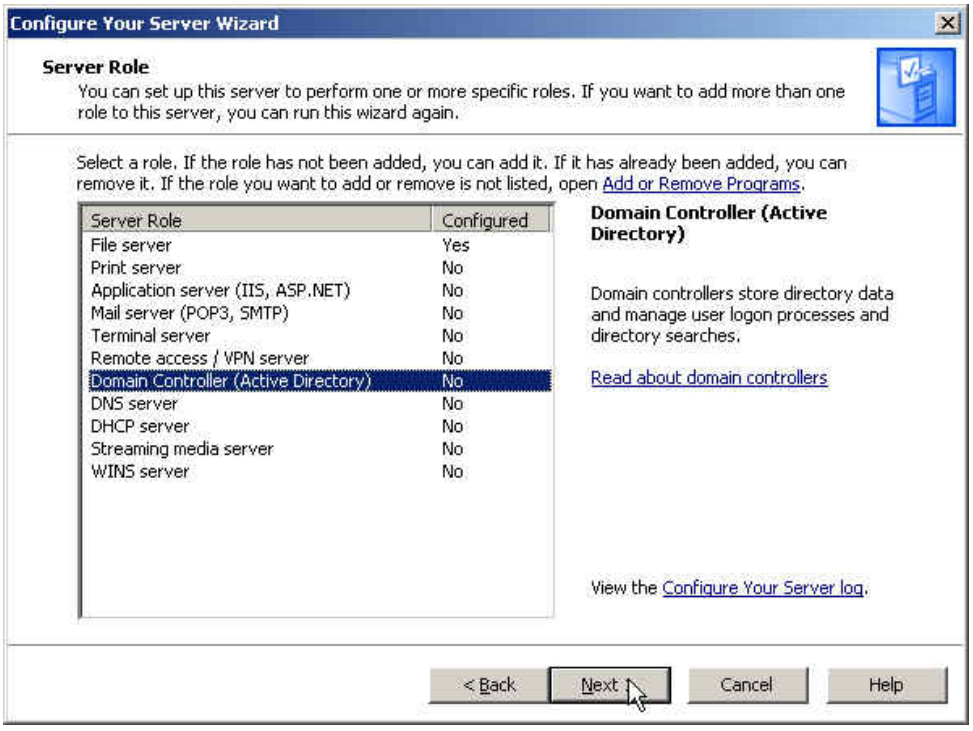


Figure 8-45 Server Role

Step 5. In the **Summary of Selections** window, click **Next**.（**Figure 8-46**）

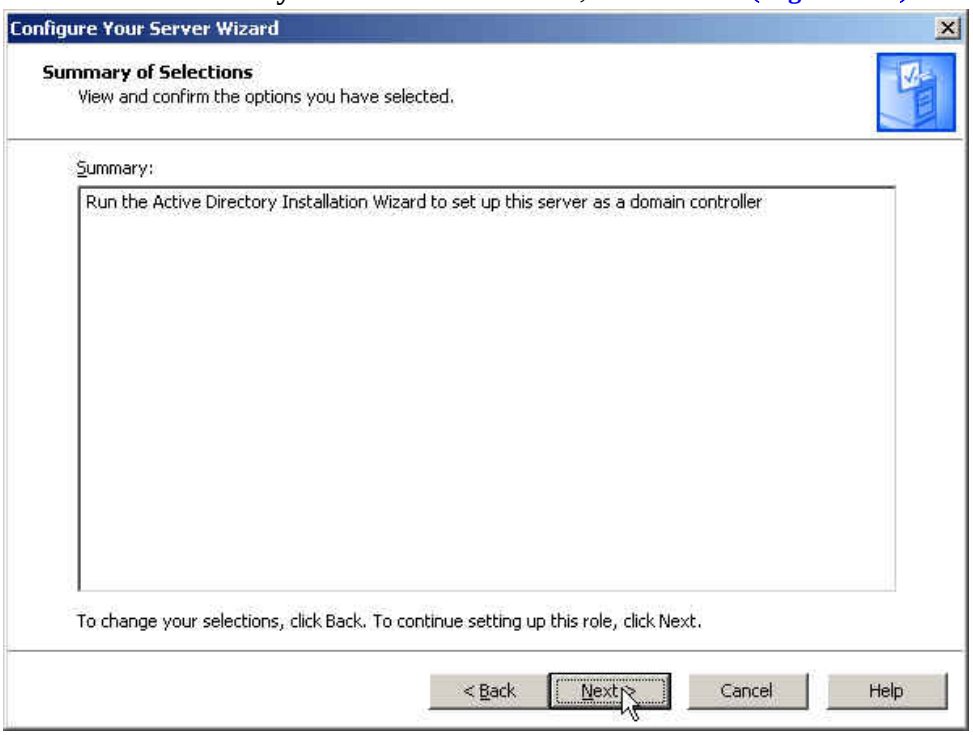


Figure 8-46 Summary of Selections

Step 6. In the **Active Directory Installation Wizard** window, click **Next**.（**Figure 8-47**）

Figure 8-47 Active Directory Installation Wizard

Step 7. In the **Operating System Compatibility** window, click **Next**. (**Figure 8-48**)

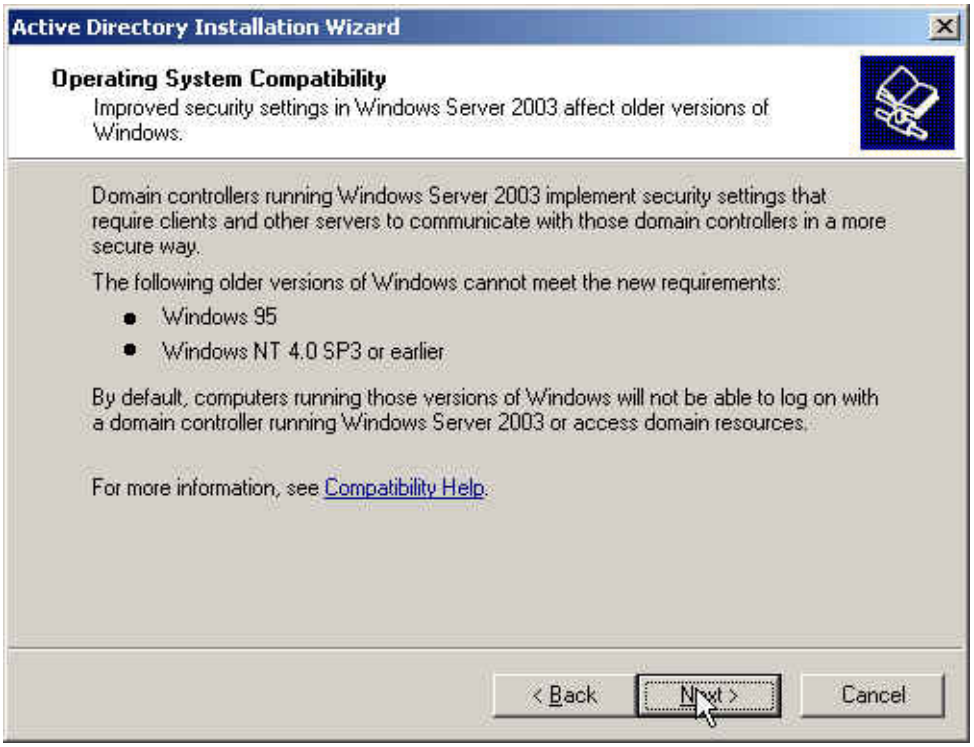


Figure 8-48 Operating System Compatibility

Step 8. In the **Domain Controller Type** window, select **Domain controller for a new domain**, then click **Next**. (**Figure 8-49**)

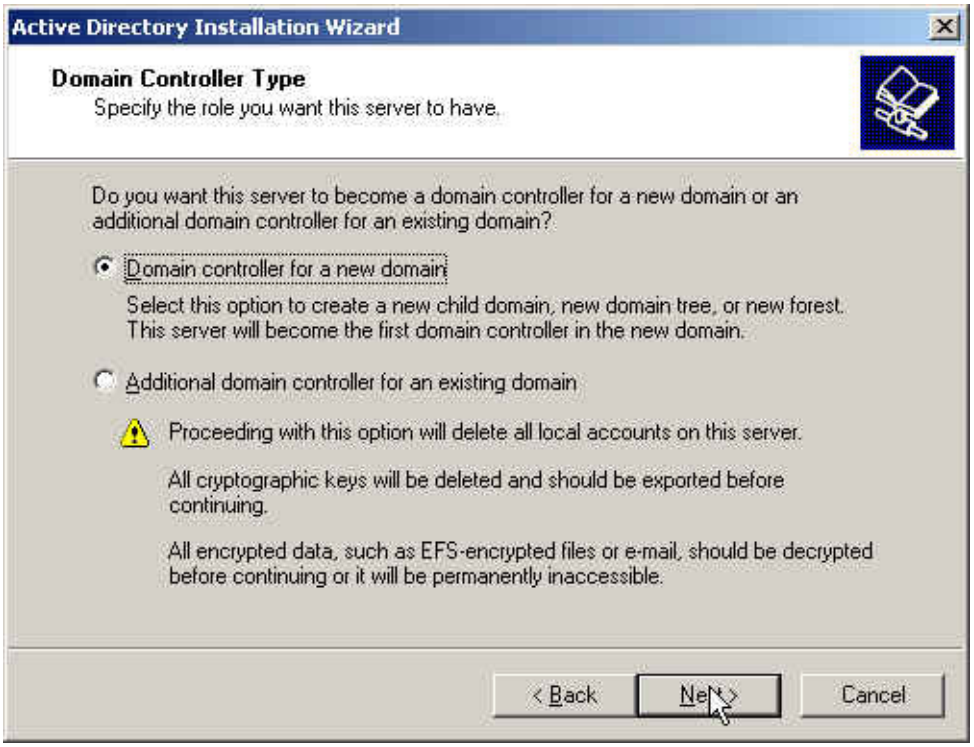


Figure 8-49 Domain Controller Type

Step 9. In the **Create New Domain** window, select **Domain in a new forest** and click **Next**.（Figure 8-50）

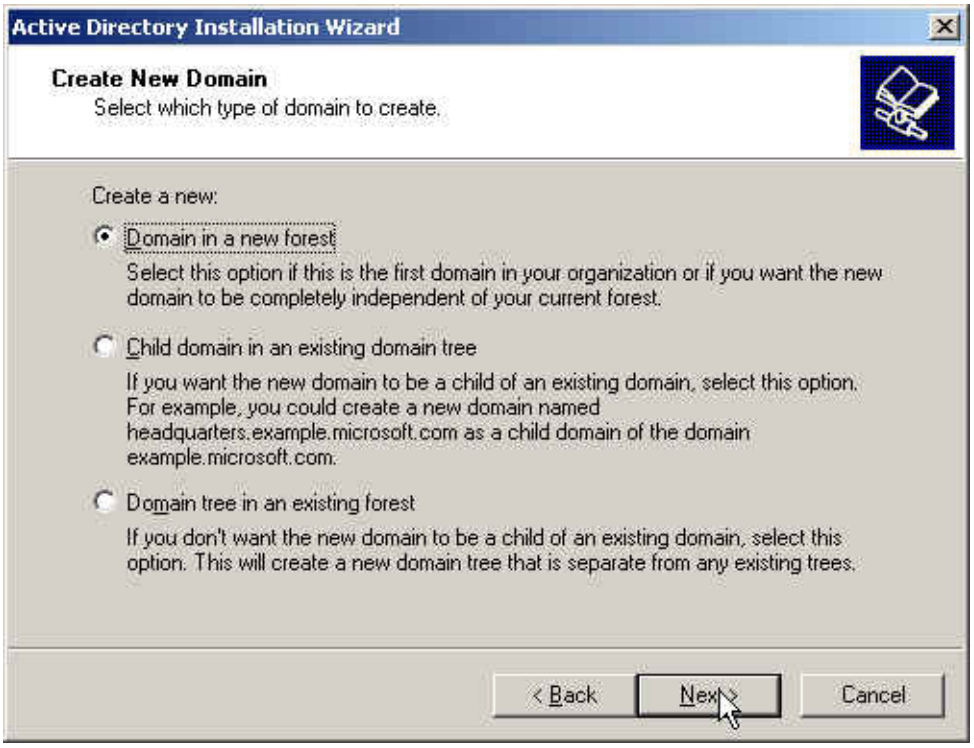


Figure 8-50 Creating a New Domain

Step 10. In the **New Domain Name** window, enter the **Full DNS name for new domain** and then click **Next.**（Figure 8-51）

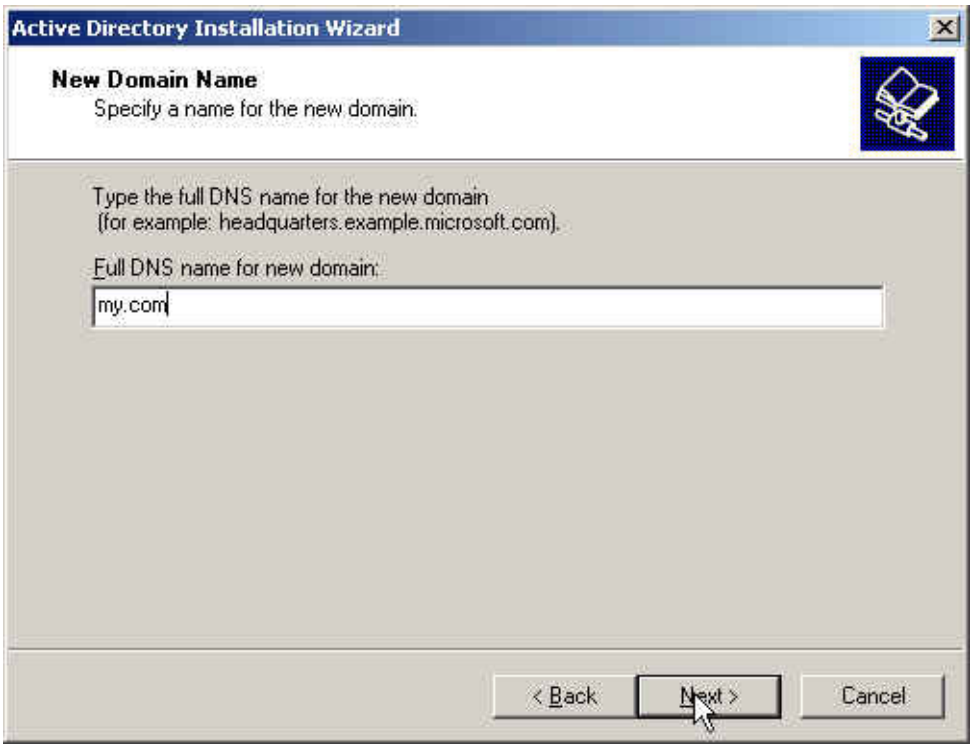


Figure 8-51 Specifying the New Domain Name

Step 11. In the **NetBIOS Domain Name** window, type a **Domain NetBIOS name** and then click **Next**.（Figure 8-52）

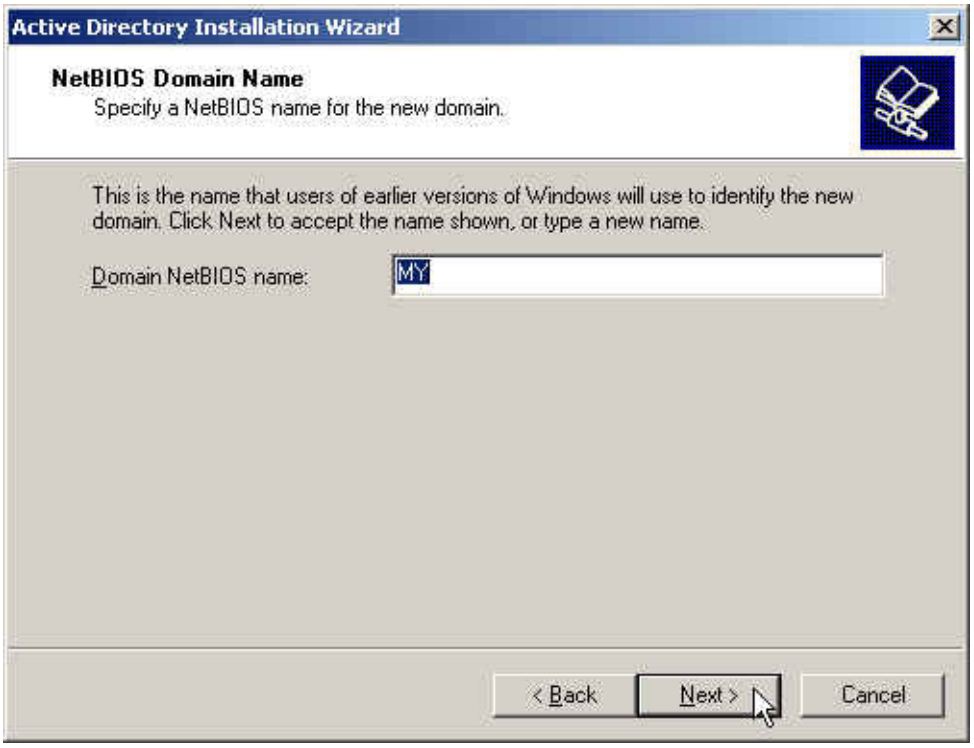


Figure 8-52 The NetBIOS Domain Name

Step 12. In the **Database and Log Folders** window, specify the pathname of the **Database folder** and the **Log folder** and then click **Next**.（Figure 8-53）

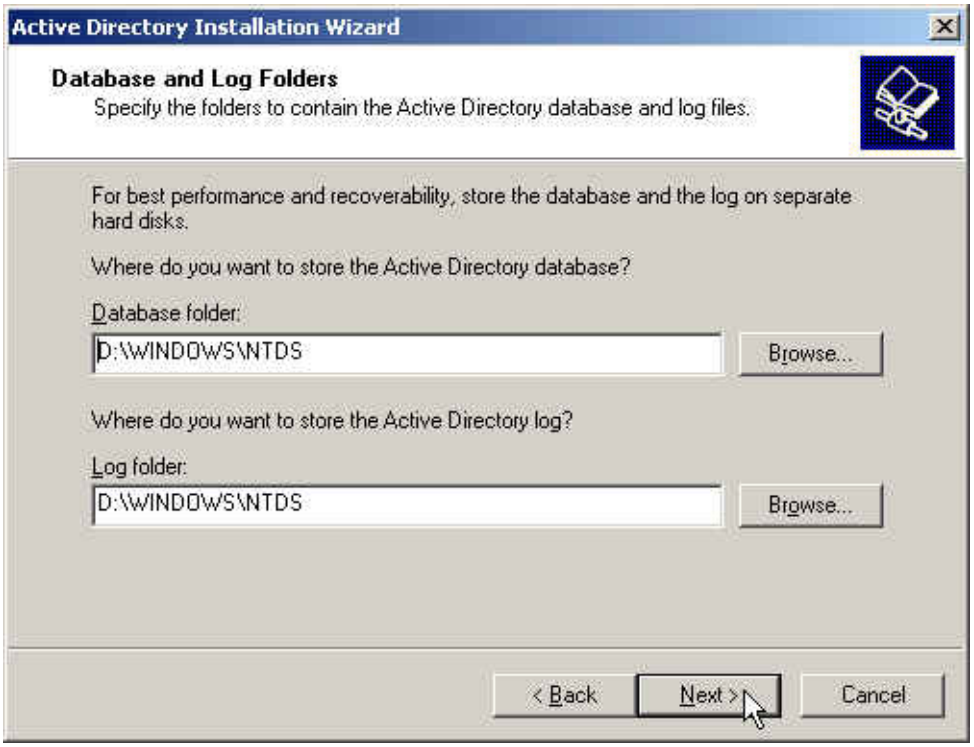


Figure 8-53 The Database and Log Folders

Step 13. In the **Shared System Volume** window, specify the **Folder location** and then click **Next.**（Figure 8-54）

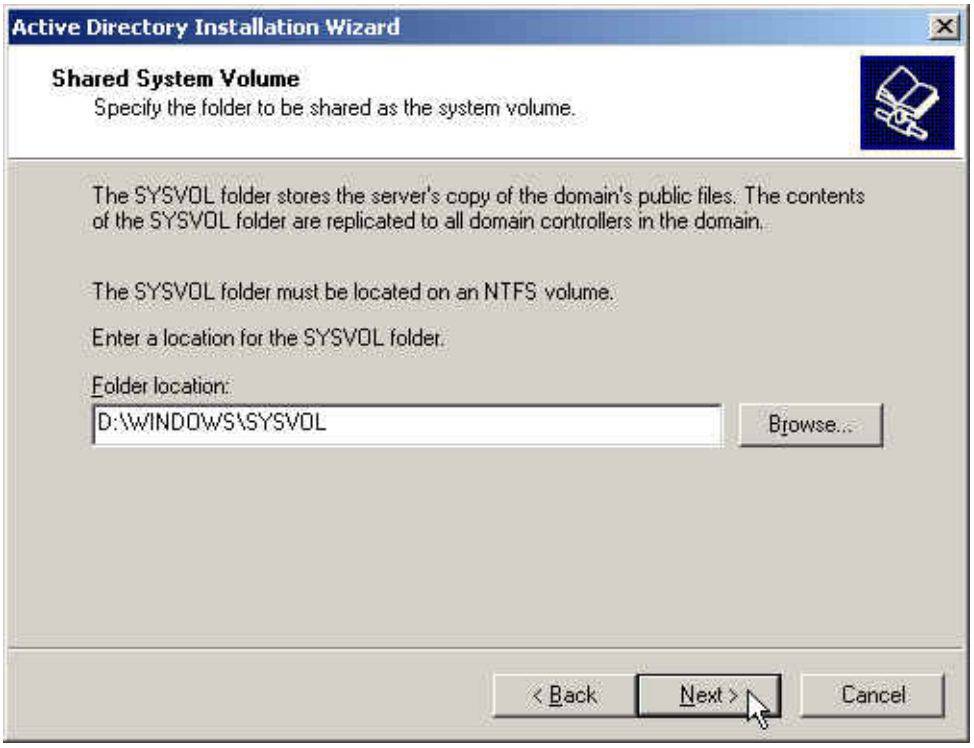


Figure 8-54 The Shared System Volume

Step 14. In the **DNS Registration Diagnostics** window, select **I will correct the problem later by configuring DNS manually (Advanced)** and then click **Next.**（Figure 8-55）

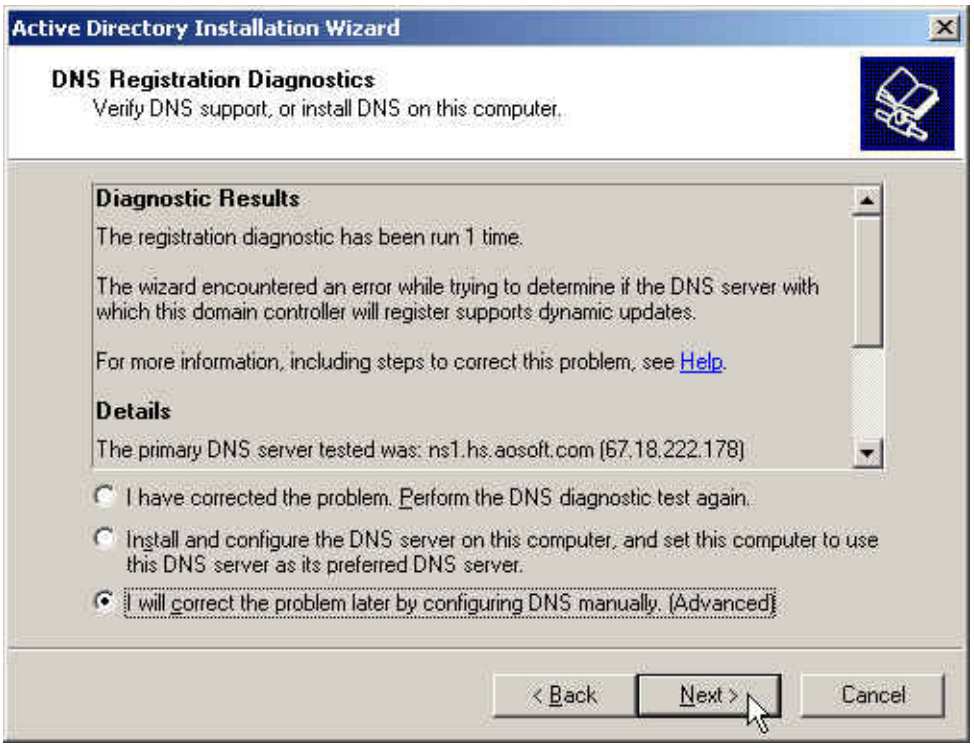


Figure 8-55 DNS Registration Diagnostics

Step 15. In the **Permissions** window, select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** and then click **Next.**（**Figure 8-56**）

Figure 8-56 Permissions

Step 16. In the **Directory Services Restore Mode Administrator Password** window, enter the **Restore Mode Password** and **Confirm password**, and then click **Next.**（**Figure 8-57**）

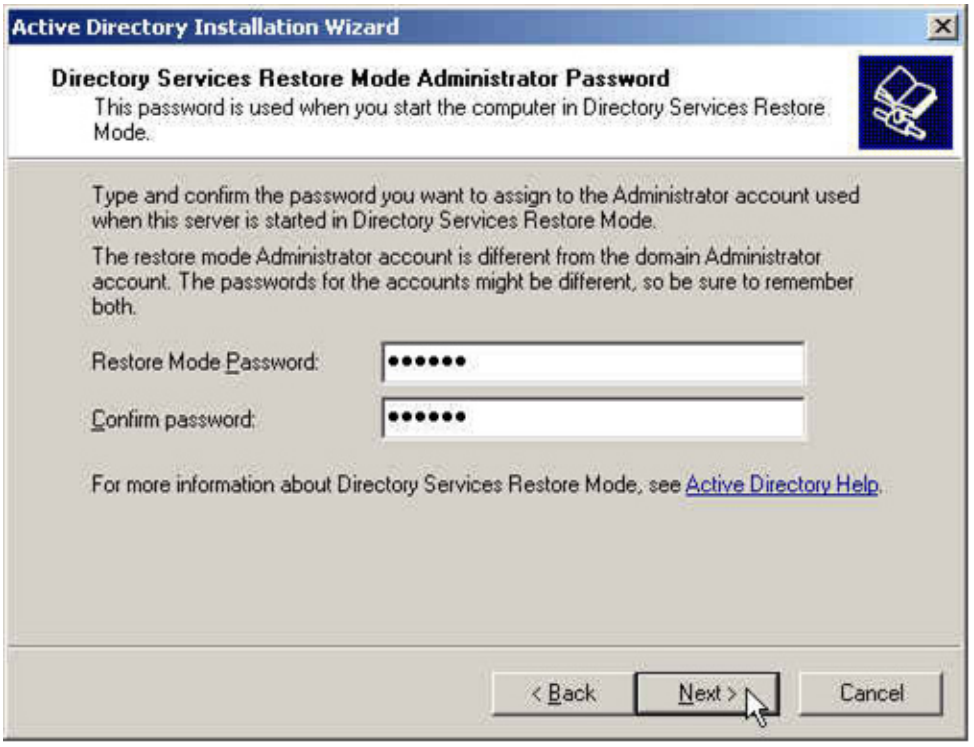


Figure 8-57 The Directory Services Restore Mode Administrator Password

Step 17. In the **Summary** window, click **Next**. **(Figure 8-58)**

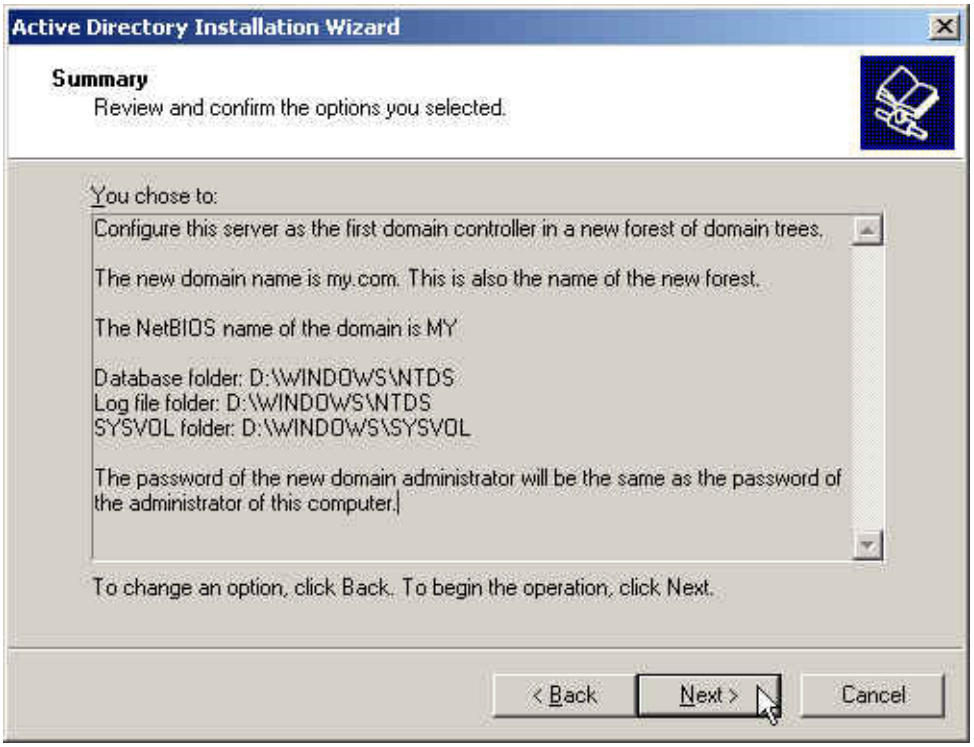


Figure 8-58 The Summary

Step 18. Settings completed.（**Figure 8-59**）

Figure 8-59 Settings Completed

Step 19. Go to **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.（**Figure 8-60**）

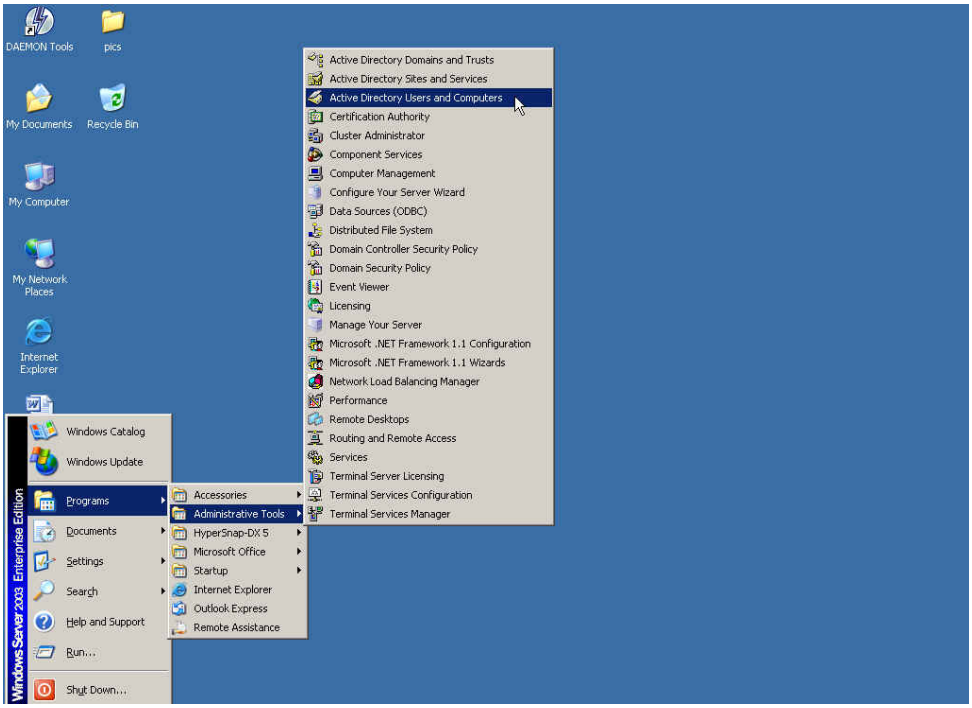


Figure 8-60 Navigating to "Active Directory Users and Computers" on the Menu

Step 20. In the **Active Directory Users and Computers** window, right-click **Users**, and then go to **New** > **User.**（**Figure 8-61**）

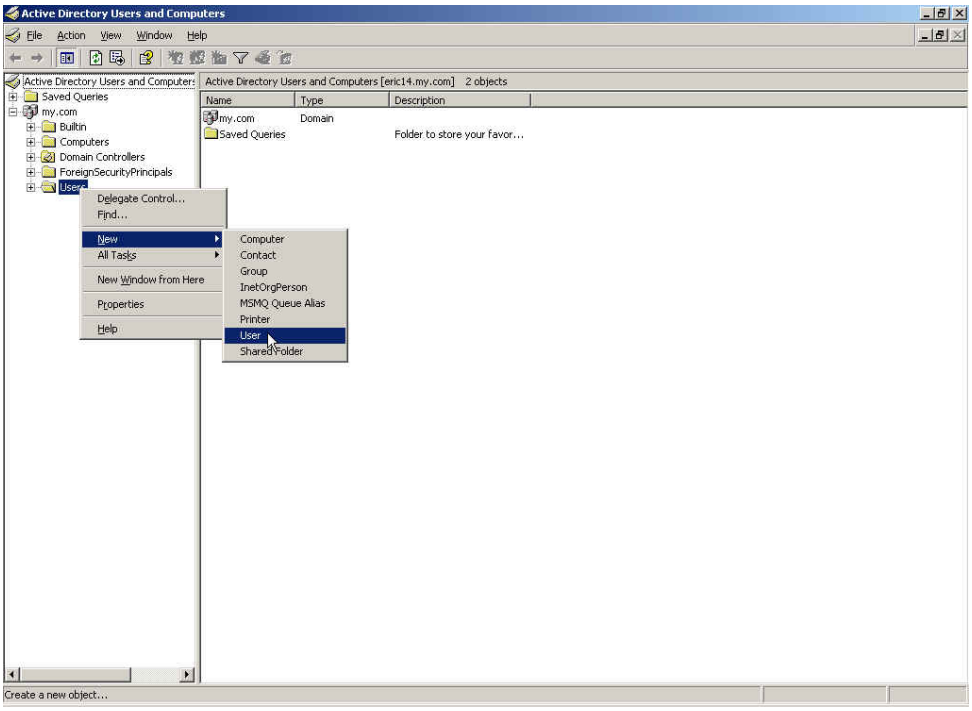


Figure 8-61 Adding an Active Directory User

Step 21. In the **New Object–User** window, apply your information to the fields, and then click **Next**.（Figure 8-62）

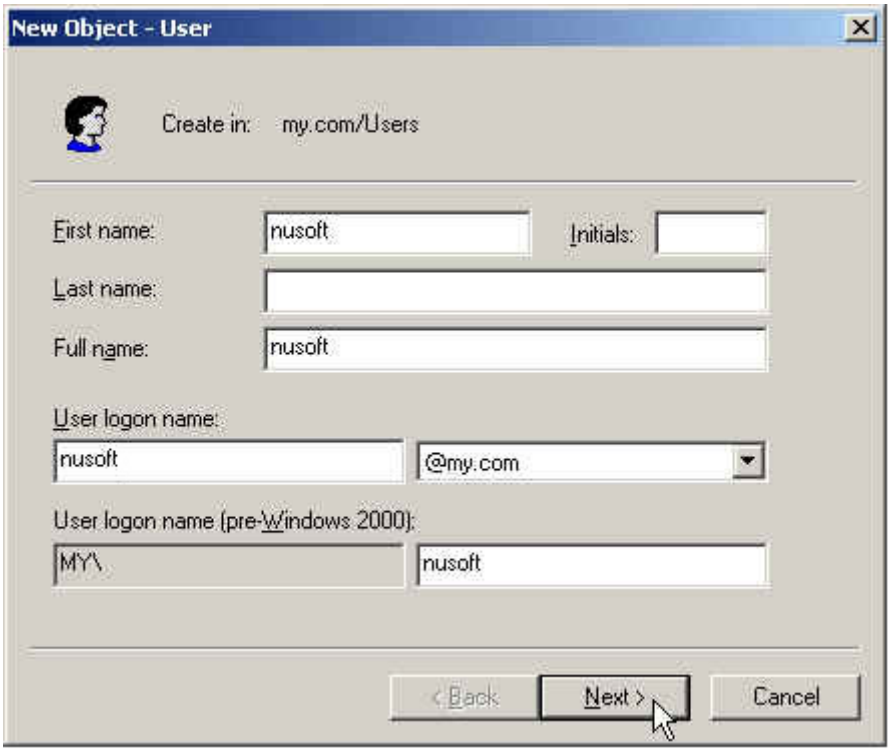


Figure 8-62 New Object – User Settings

Step 22. In the **New Object – User** window, enter the password, and then click **Next.**（Figure 8-63）

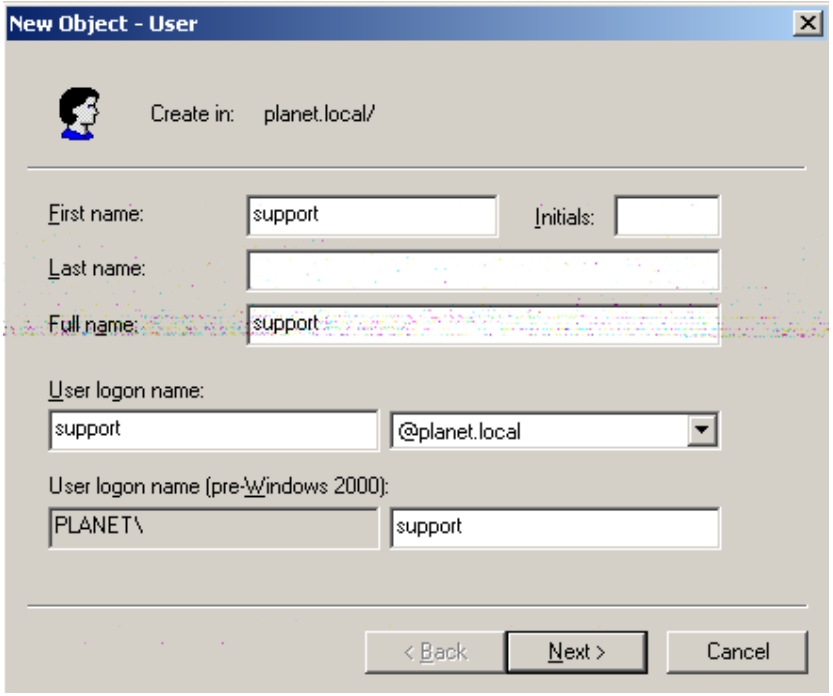


Figure 8-63 New Object – User Settings

Step 23. User has been successfully created. (Figure 8-64)

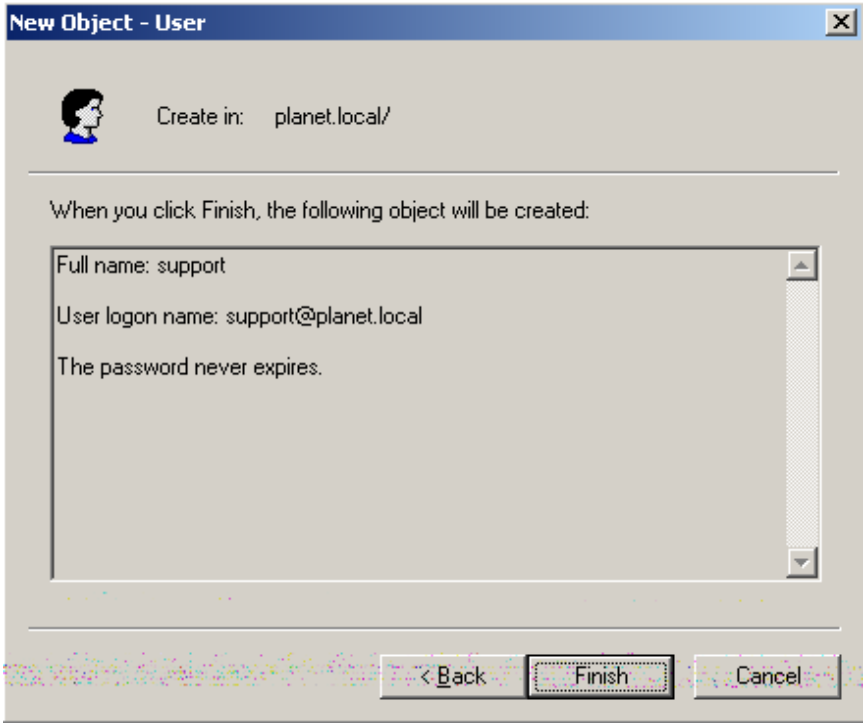


Figure 8-64 User Successfully Created

Step 24. Go to **Policy Object** > **Authentication** > **LDAP**, and then refer to figure below to configure: (Figure 8-65)

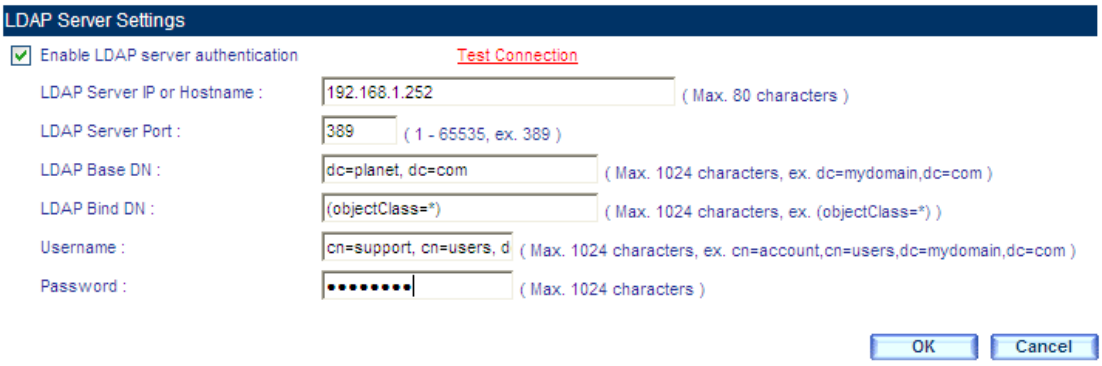


Figure 8-65 LDAP Server Settings

Note :

1. You may click **Test Connection** to detect the connection between CS-2001 and LDAP server.
2. Lists the LDAP User Name from LDAP server. The user name may be grouped for authentication.

Step 25. Go to **Policy Object > Authentication > Group**, then add **LDAP User**. （**Figure 8-66**）

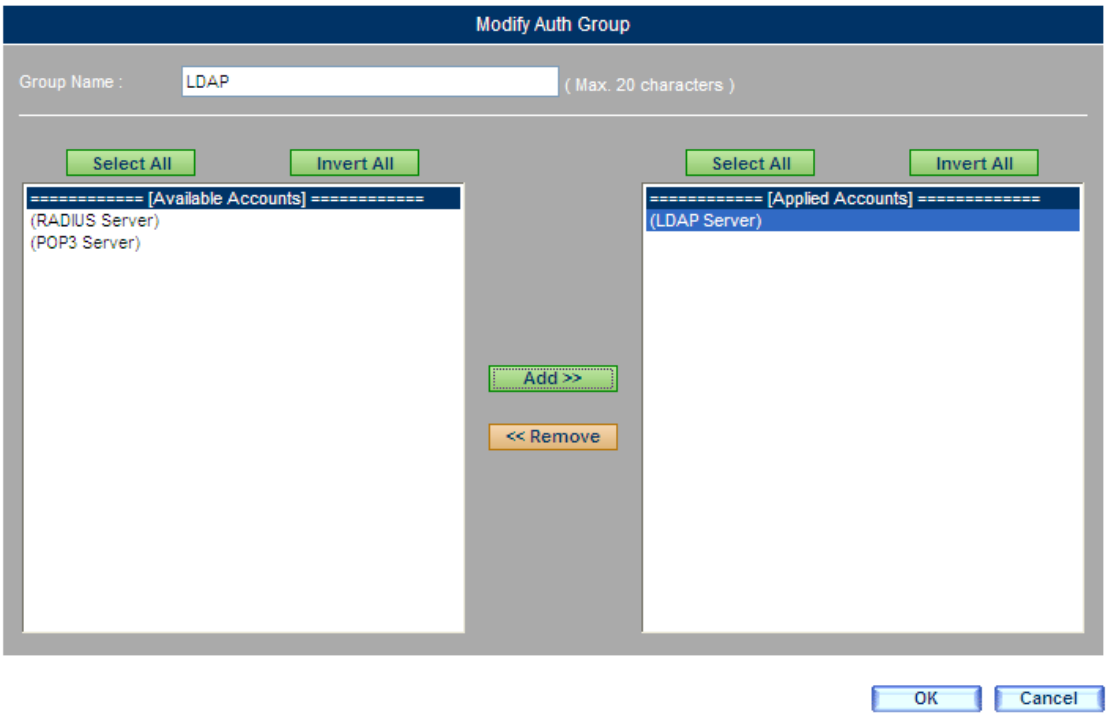


Figure 8-66 Adding the LDAP User

Step 26. Under **Policy** > **Outgoing**, set as below:（**Figure 8-67**）

- Select the defined user group for **Authentication User.**
- Click **OK**.（**Figure 8-68**）

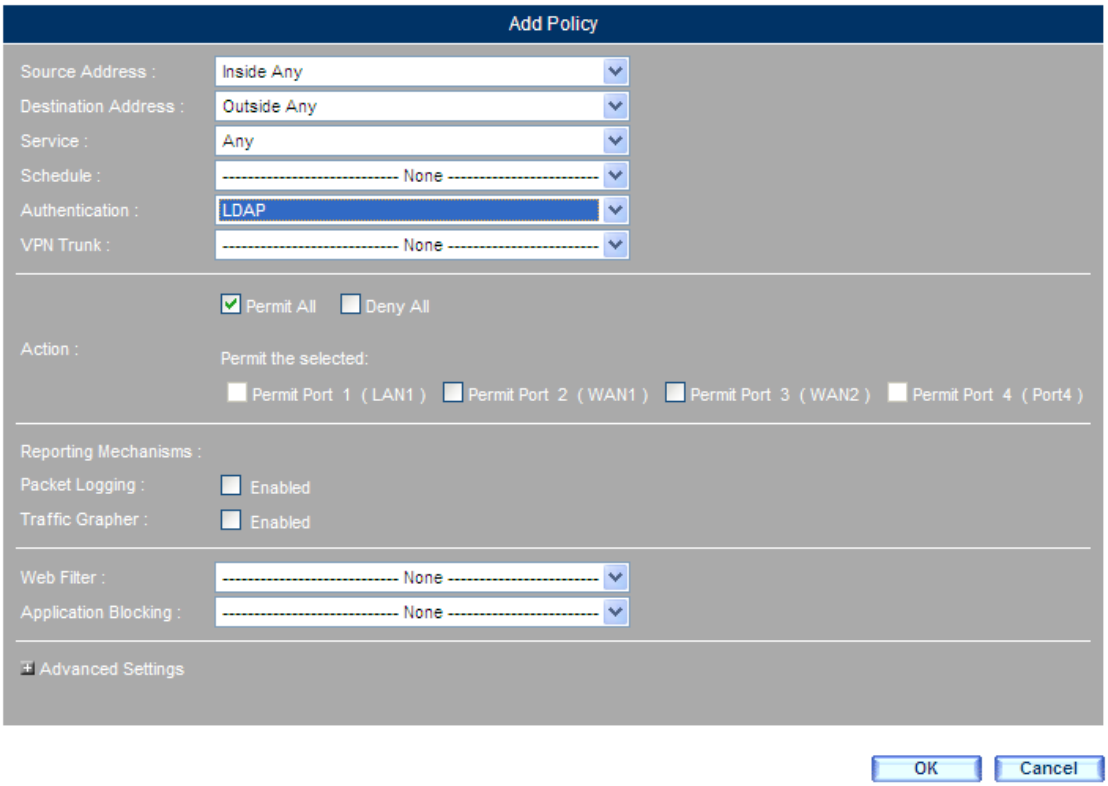


Figure 8-67 Using LDAP Authentication in a Policy

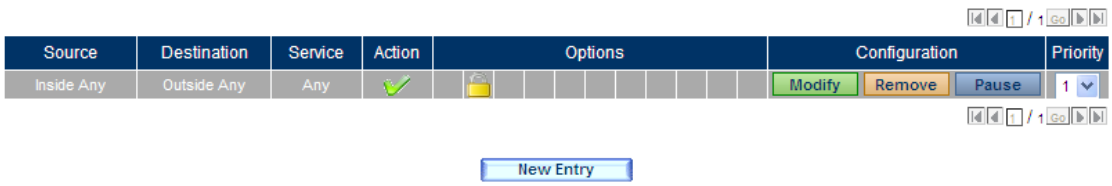


Figure 8-68 A Policy with LDAP Authentication

Step 27. The authentication login screen appears in the web browser when a LAN user tries to access the Internet. Internet access will be available after applying the valid user name and password to the corresponding fields in the login screen.（**Figure 8-69**）

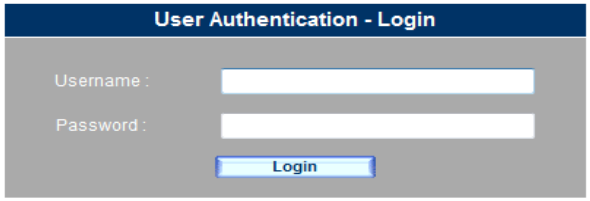


Figure 8-69 The Authentication Login

Chapter 9 Application Blocking

Application Blocking regulates the control of Instant Messenger Login, File Transfer over IM, Peer-to-Peer Sharing, Multimedia Streaming, Web-Based Mail, Online Gaming, VPN Tunneling, Remote Controlling and Other Applications.

Terms in Application Blocking

Application Signatures Settings

- The application signatures are updated hourly. Alternatively, they can be manualy updated instantly. The most recent update time is displayed together with the version number.

Note:

1. Once the Proxy Server is deployed, the proxy settings under **System** > **Configuration** > **Settings** must be configured for the CS-2001 to access the Internet.

Instant Messenger Login

- Regulates the use of MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, Rediff, WebIM, Alisoft, BaiduHi, SinaUC, Fetion, Facebook Chat, Comfrog.

File Transfer over IM

- Regulates file transfers for MSN, Yahoo, ICQ/AIM, QQ, Google Talk, and Gadu-Gadu.

Peer-to-Peer Sharing

- Regulates the online usage of eDonkey, eMule, BitTorrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, GoGoBox, QQDownload, Ares, Shareaza, BearShare, Morpheus, Limewire and Kazaa.

Multimedia Streaming

- Regulates logins for PPLive, PPStream, UUSee, QQLive/QQGame, ezPeer, qvodplayer, Funshion and PPMate.

Web-Based Mail

- Regulates logins for Gmail, Hotmail, Yahoo, Hinet, PChome, URL, Yam, Seednet, 163/126/Yeah, Tom, Sina and Sohu.

Online Gaming

- Restricts logins for GLWorld and QQGame.

VPN Tunneling

- Regulates the online usage of VNN Client, Ultra-Surf, Tor, Hamachi, HotSpot Shield and FreeGate.

Remote Controlling

- Regulates the online usage of TeamViewer, VNC and Remote Desktop.

9.1 Example

No.	Example	Scenario	Page
9.1.1	**IM**	Regulating the Use of IM Software — Messaging and File Transferring	**208**
9.1.2	**P2P**	Regulating the Use of P2P Software — Downloading and Uploading	**211**

9.1.1 Regulating the Use of IM Software — Messaging and File Transferring

Step 1. Go to **Policy Object** > **Application Blocking** > **Settings** and set as below: **(Figure 9-1)**

- Click **New Entry**.
- Type a name in the **Name** field.
- Select **Instant Messaging Login** and **File Transfer over IM** then tick **Select All** for both.
- Click **OK**.（**Figure 9-2**）

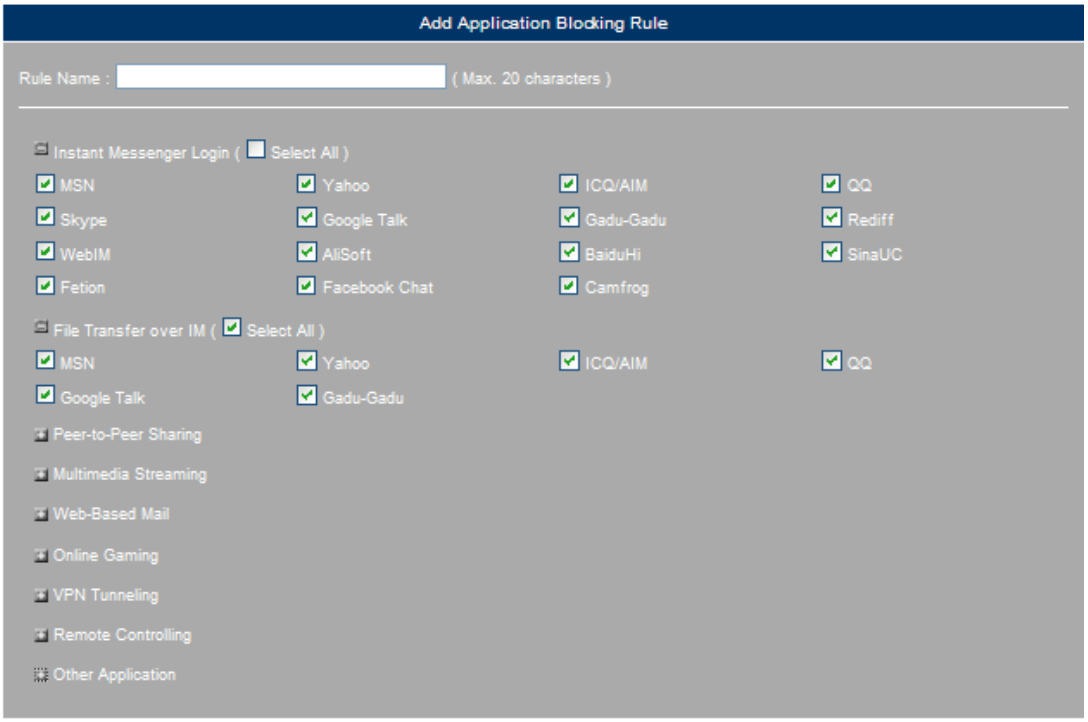


Figure 9-1 Regulating the Use of IM Software

Figure 9-2 Settings Completed

Step 1. Under **Policy** > **Outgoing**, set as below: (**Figure 9-3**)

- **Application Blocking:** Select the name of the Application Blocking setting.
- Click OK. (**Figure 9-4**)

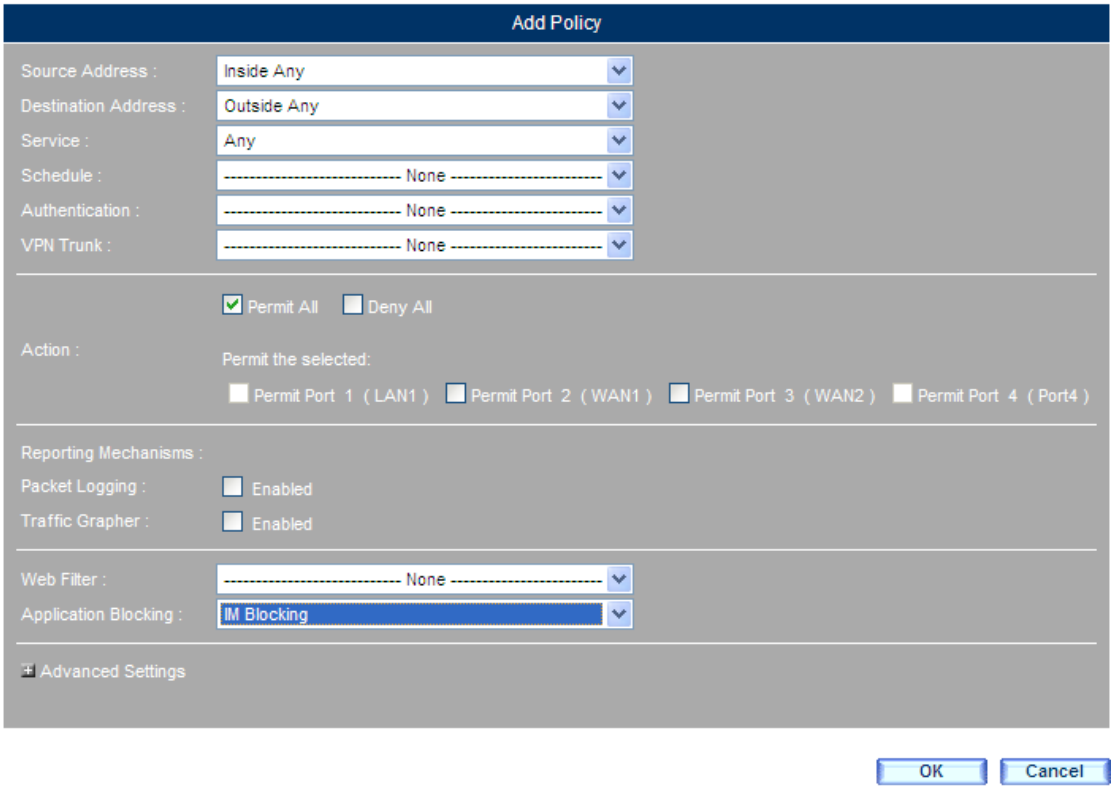


Figure 9-3 Applying IM Blocking to a Policy

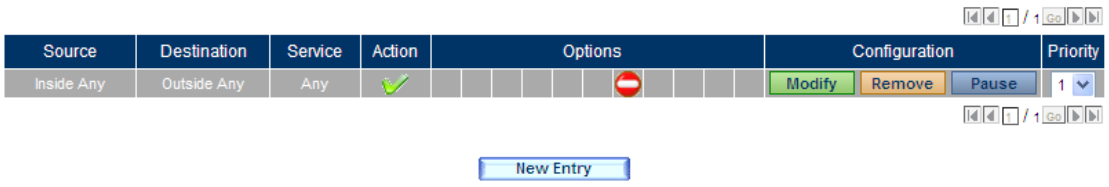


Figure 9-4 A Policy with IM Blocking

9.1.2 Regulating the Use of P2P Software — Downloading and Uploading

Step 1. Under **Policy Object** > **Application Blocking** > **Settings**, set as below: **(Figure 9-5)**

- Click **New Entry**.
- Type a name in the **Name** field.
- Select **Peer-to-Peer Sharing** and tick **Select All**.
- Click **OK**.（**Figure 9-6**）

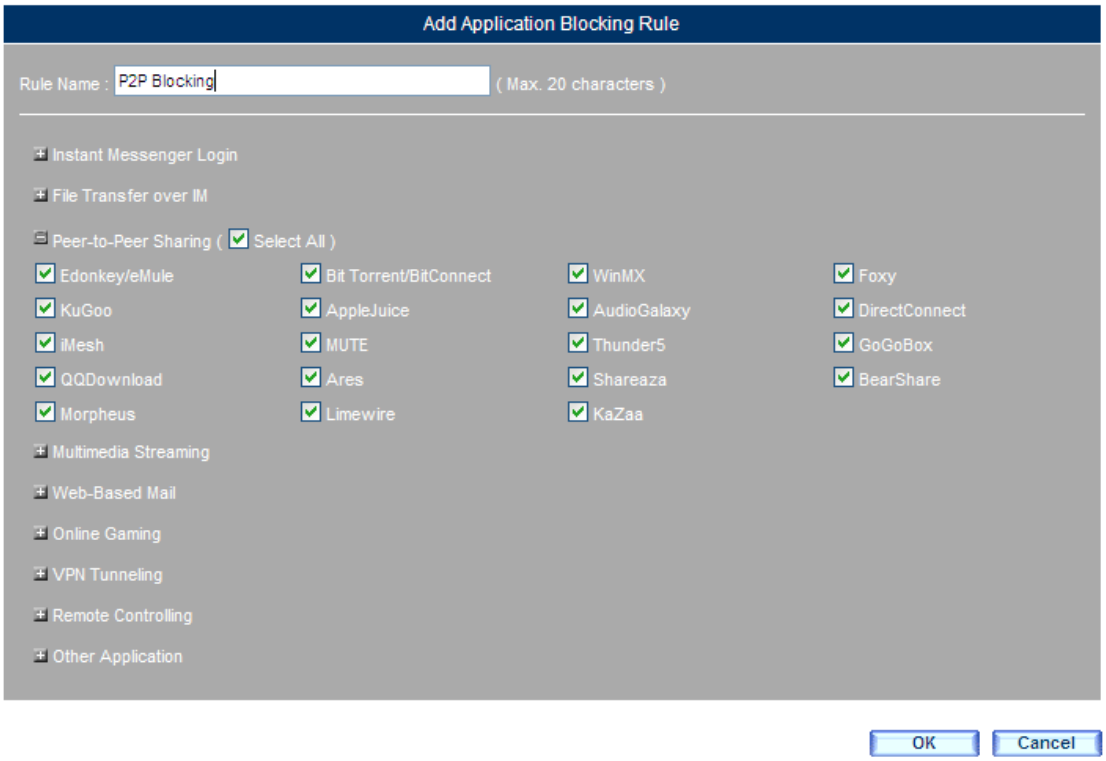


Figure 9-5 Regulating the Use of P2P Software

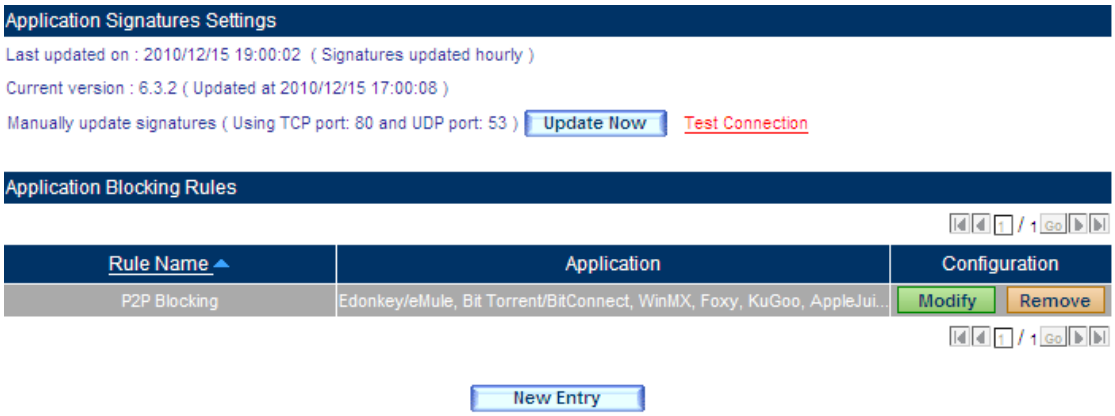


Figure 9-6 Settings Completed

Step 2. Under **Policy > Outgoing**, set as below: (**Figure 9-7**)

- **Application Blocking:** Select the name of the Application Blocking Setting.
- Click **OK**. (**Figure 9-8**)

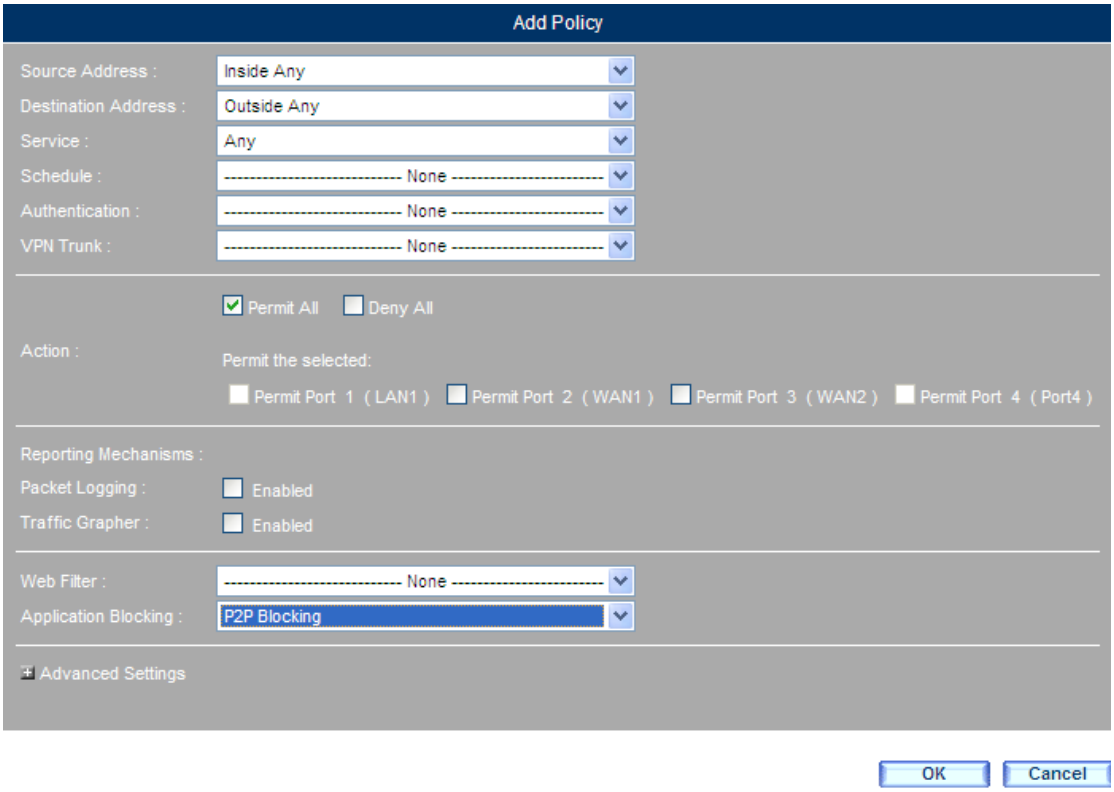


Figure 9-7 Enabling the P2P Blocking in a Policy

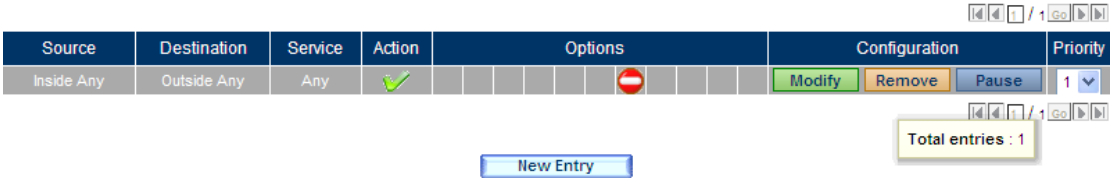


Figure 9-8 A Policy with P2P Blocking

Note:

1. P2P software occupies significant network bandwidth resources, adversly affecting other users. **Policy Object > Service** can block the port number that P2P software uses, however this port number is variable and can be modified by users. Therefore, the IT administrator must use the **Peer to Peer Application** settings located under **Policy Object > Application Blocking > Setting** to successfully block users from using P2P software.

Chapter 10 Virtual Server

Virtual server provides services to external users by mapping a real IP address from a WAN port on the CS-2001 to a private IP address within the LAN.

- **Mapped IPs:** Uses Network Address Translation (NAT) to map a real IP address to a private IP address (one-to-one mapping) to provide any service (ports 0-65535).
- **Port Mapping:** Uses Port Address Translation (PAT) to map different services (ports) of a real IP address to the private IP addresses of internal servers. Services may also be shared amongst multiple internal servers to provide load balancing ensuring external service requests with an efficient and uninterrupted service.
- **Virtual IP Group:** Provides groupings of **Mapped IPs** and **Port Mapping** settings for convenient application in a policy.

Terms in Virtual Server

WAN IP

- The real IP address of the WAN.

Map to Virtual IP

- The private network address of a server in the LAN.

Server Real IP

- The real IP address used by the virtual server.

Service

- The name of the service that the virtual server is providing.

External Service Port

- The port number that the service will be using. If the service is just using one port, then it can be modified. For example, supposing the HTTP port has been changed into 8080, then ":8080" must be appended to a web site / page address, such as http://www.yahoo.com: 8080.

Load Balancing

- **Round-Robin**: In this mode, sessions are allocated to the internal servers by means of a round-robin cycle. This improves overall efficiency and prevents the entire load being placed on just a single server.
- **Backup Mode**: When the main server ceases to function, the sessions will then be allocated to the backup servers according to their number on the list.
- **Source IP Hash**: Allocate the sessions according to the source IP.

Interface

- Designates the interface of the server's private IP address.

Private IP Address

- The private network address to be mapped.

10.1 Example

No.	Settings	Scenario	Page
10.1.1	**Mapped IPs**	Using a Server to Provide FTP, Web and Mail Services through the Regulation of a Policy	**217**
10.1.2	**Port Mapping**	Using Multiple Virtual Servers to Host a Web Site through the Regulation of a Policy	**221**
10.1.3	**Port Mapping**	A VoIP Session Between an External and Internal User (VoIP Ports: TCP 1720, TCP 15321-15333 and UDP 15321-15333)	**225**
10.1.4	**Port Mapping**	Using Multiple Virtual Servers to Provide HTTP, POP3, SMTP and DNS Services through the Regulation of a Policy	**230**

Prerequisite Setup (Note: IP address used as example only)

Apply to a local ISP for two ADSL lines with static IP addresses.

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing Mode) and connect to the LAN (192.168.1.x/24)
Configure Port2 as WAN1 with the fixed IP address range from 61.11.11.10 to 61.11.11.14.
Configure Port3 as WAN2 with the fixed IP address range from 211.22.22.18 to 211.22.22.30.

10.1.1 Using a Server to Provide FTP, Web and Mail Services through the Regulation of a Policy

Step 1. Setup a server in the LAN which provides FTP, web and mail services; configure its IP address as 192.168.1.100 and its **Preferred DNS server** address as that of the external DNS server.

Step 2. Under **Policy Object** > **Address** > **LAN**, set as below: (**Figure 10-1**)

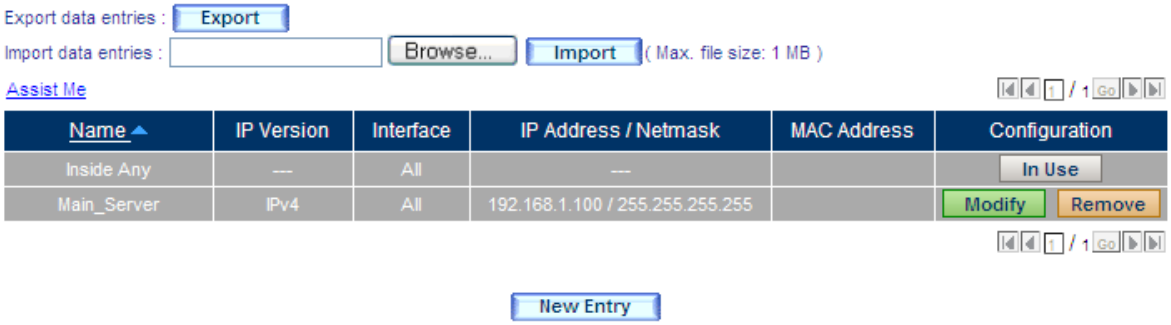


Figure 10-1 Configuring the Address Settings

Step 3. Under **Policy Object** > **Virtual Server** > **Mapped IPs**, set as below:

- Click **New Entry**.
- Enter a name for the Mapped IP address in the **Name** field.
- **WAN IP:** Select Port2(WAN1) then type 61.11.11.12 in the field, or click **Assist Me** to select an IP address.
- **Mapped IPs :** Select **Port1(LAN1)** and type 192.168.1.100 in the field, or click **Assist Me** to select an IP address.
- Click OK. (**Figure 10-2**)

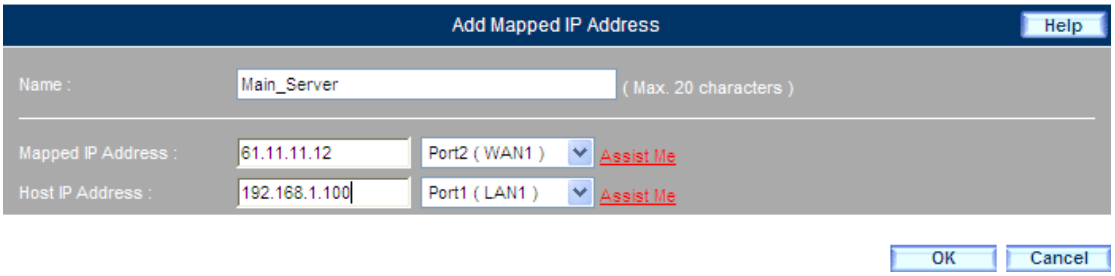


Figure 10-2 Configuring the Mapped IPs

Step 4. Go to **Policy Object** > **Service** > **Group**, and create a group called Main_Service containing all of the server's services e.g. DNS, FTP, HTTP, POP3, SMTP, etc. Create another group called Mail_Service comprising the services for enabling the server to send emails.（**Figure 10-3**）

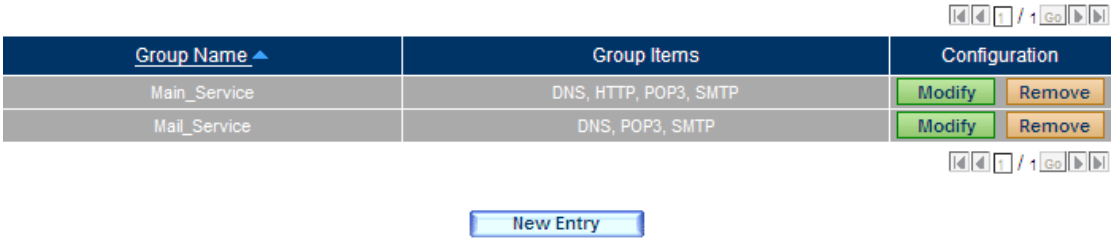


Figure 10-3 Group Settings

Step 5. Under **Policy** > **Incoming**, set as below: **(Figure 10-4)**

- Select the defined mapped IP for **Destination IP**.
- Select Mail_Service for **Service**.
- Click **OK**.（**Figure 10-5**）

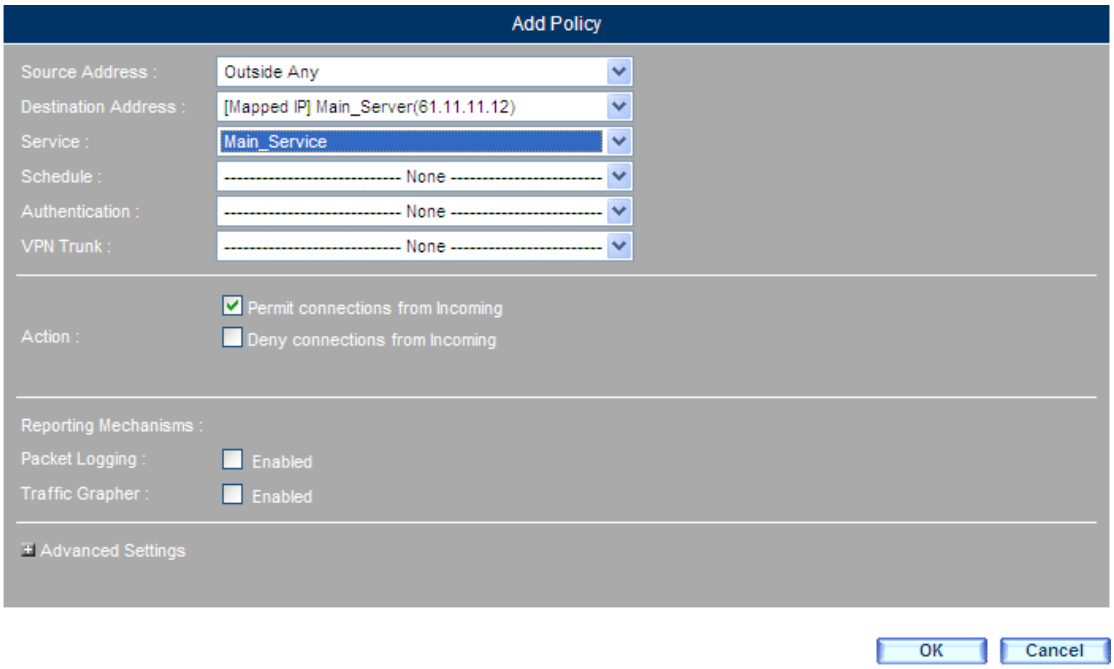


Figure 10-4 Configuring the Incoming Policy

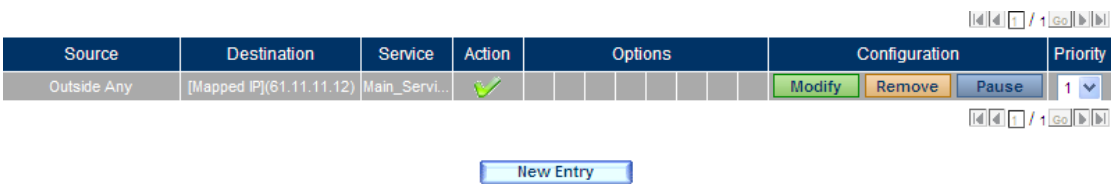


Figure 10-5 The Completed Policy Settings

Step 6. Under **Policy > Outgoing**, set as below: **(Figure 10-6)**

- **Source Address**: Select the LAN address.
- **Service**: Select Mail_Service.
- Click **OK**.（**Figure 10-7**）

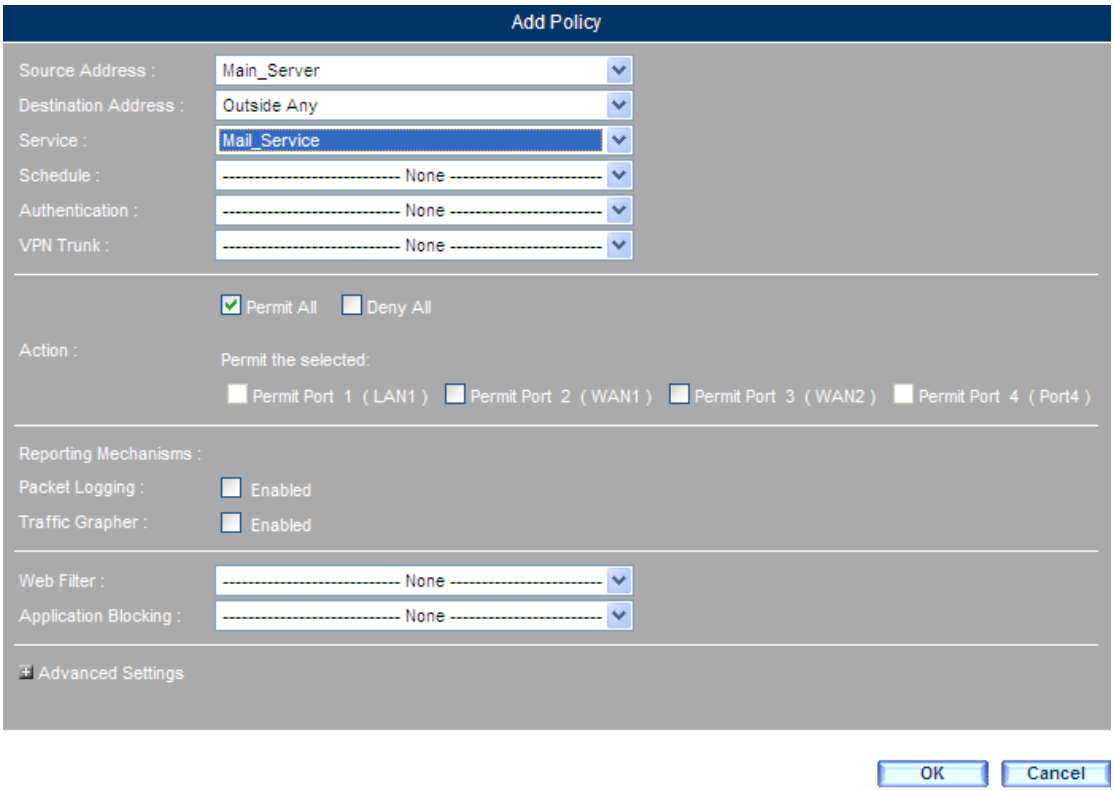


Figure 10-6 Configuring an Outgoing Policy

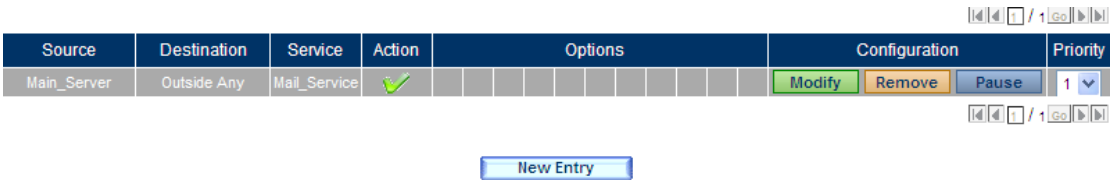


Figure 10-7 The Completed Policy Settings

Important:

1. To enable the LAN to LAN connection, go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**). To enable the DMZ to DMZ connection, go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address)**.

Step 7. The completed settings. (Figure 10-8)

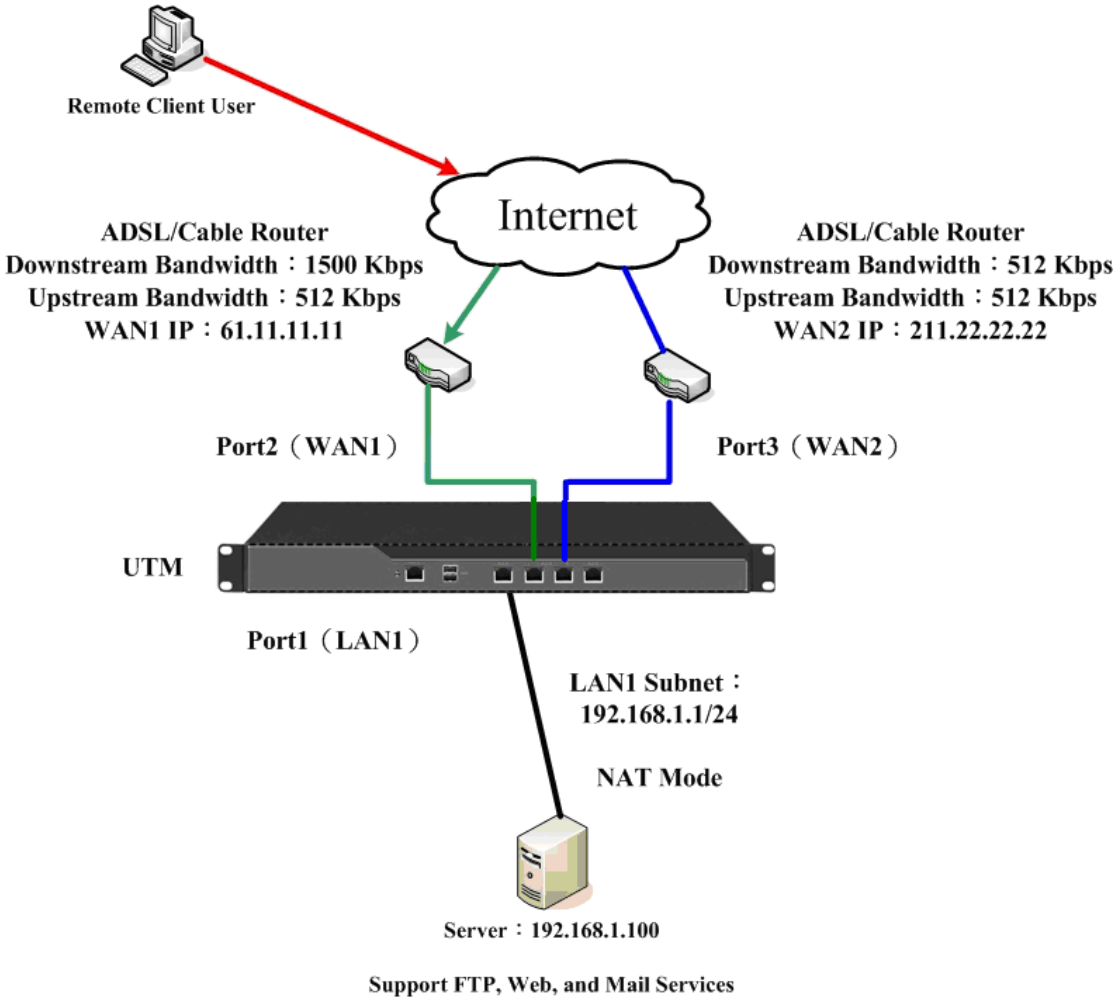


Figure 10-8 The Server Providing Multiple Services

Note:

1. It is strongly recommended not to select **ANY** for **Service** when configuring a policy, especially when using a Mapped IP. This is because of the possibility of hackers being able to use some of the services as a means to hack into server.

10.1.2 Using Multiple Virtual Servers to Host a Web Site through the Regulation of a Policy

Step 1. Set up multiple web servers in the LAN using the IP addresses: 192.168.1.101, 192.168.1.102, 192.168.1.103 and 192.168.1.104.

Step 2. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below: （**Figure 10-9**）

- **Name**：Type a name for the Virtual IP setting.
- **Server Real IP**: Select Port3 (WAN2) and type 211.74.99.122 into the field or click **Assist Me** to select an IP address.
- **Service**: select HTTP(80).
- **WAN Port**: Change “80” into “8080”.
- **Scheduling Algorithm:** Select “Round-Robin”.
- **Interface**: Select Port1 (LAN1).
- **IP of Virtual Server 1**: Enter 192.168.1.101 (or you may click on **Assist Me**)
- **IP of Virtual Server 2**: Enter 192.168.1.102 (or you may click on **Assist Me**)
- **IP of Virtual Server 3**: Enter 192.168.1.103 (or you may click on **Assist Me**)
- **IP of Virtual Server 4**: Enter 192.168.1.104 (or you may click on **Assist Me**)
- Click **OK**.（**Figure 10-10**）

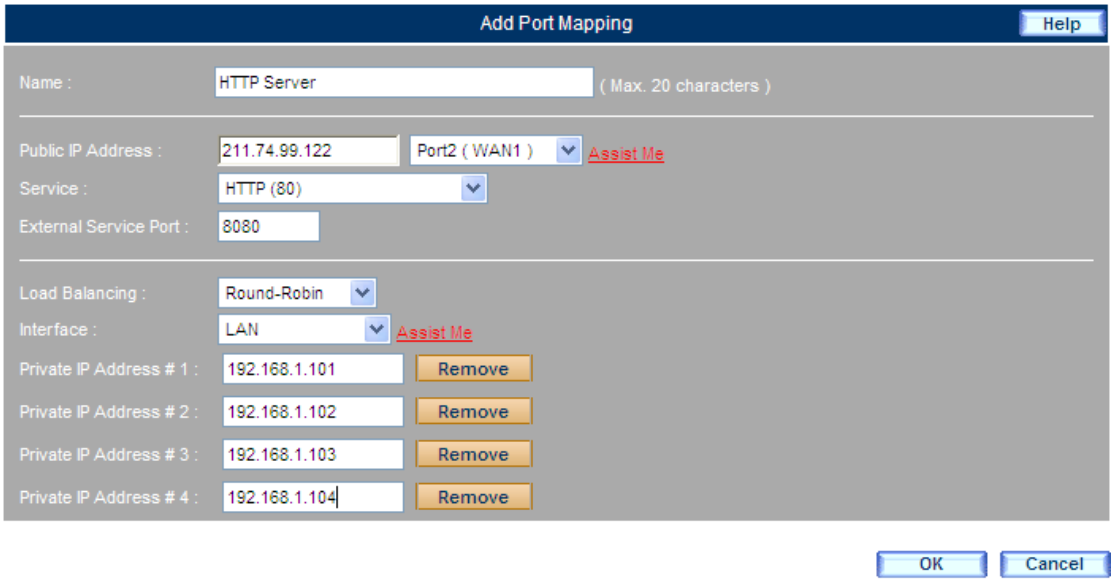


Figure 10-9 Setting Virtual IP

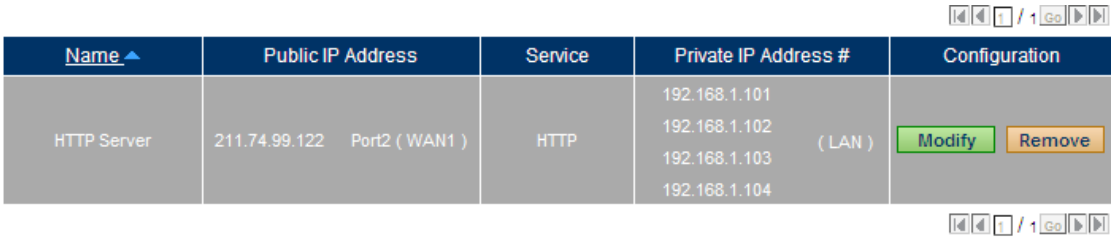


Figure 10-10 The Completed Virtual IP Settings

Step 3. Under **Policy > Incoming**, set as below: (**Figure 10-11**)

- **Destination IP**: Select the Virtual IP setting.
- **Service**: Select HTTP(8080)
- Click OK. (**Figure 10-12**)

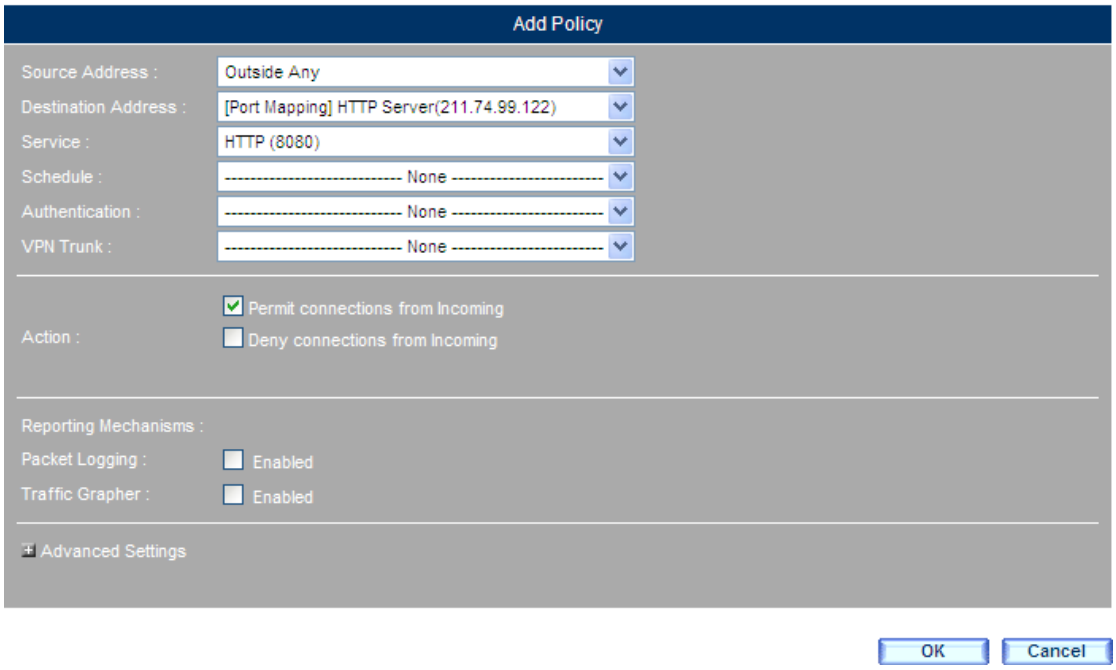


Figure 10-11 Applying the Service to Policy

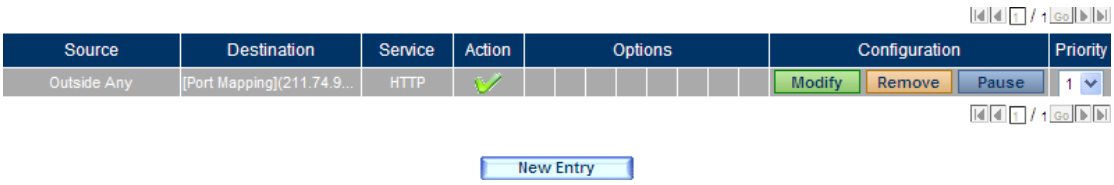


Figure 10-12 The Completed Policy Setting

Note：

1. Since the HTTP port number has been changed into 8080 in this example, then ":8080" must be appended to the web page address, such as http://www.yahoo.com: 8080.

Important:

1. To enable the LAN to LAN connection, go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**). To enable the DMZ to DMZ connection, go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**).

Step 4. Settings completed.（Figure 10-13）

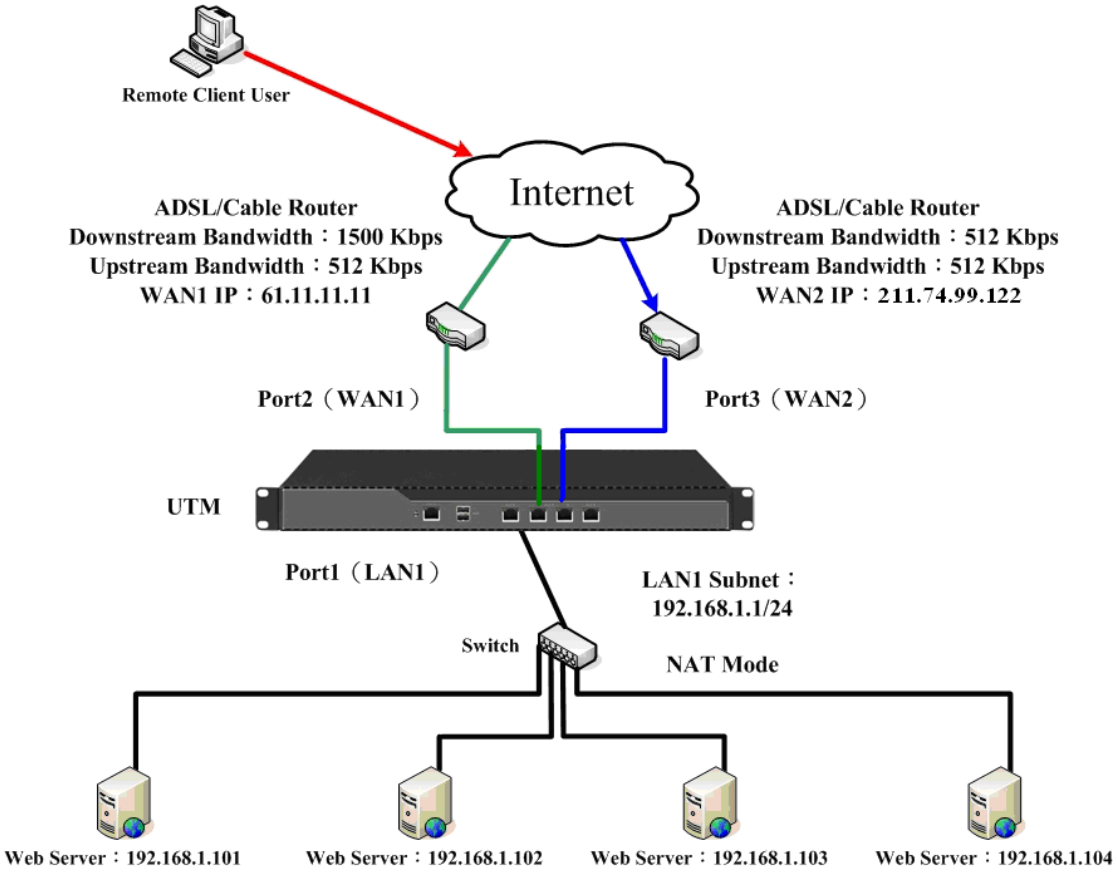


Figure 10-13 Multiple Servers Hosting a Single Website

10.1.3 A VoIP Session Between an External and Internal User (VoIP Ports: TCP 1720, TCP 15321-15333 and UDP 15321-15333)

Step 1. Configure internal VoIP user with the IP address: 192.168.1.100.

Step 2. Under **Policy Object** > **Address** > **LAN**, set as below: (**Figure 10-14**)

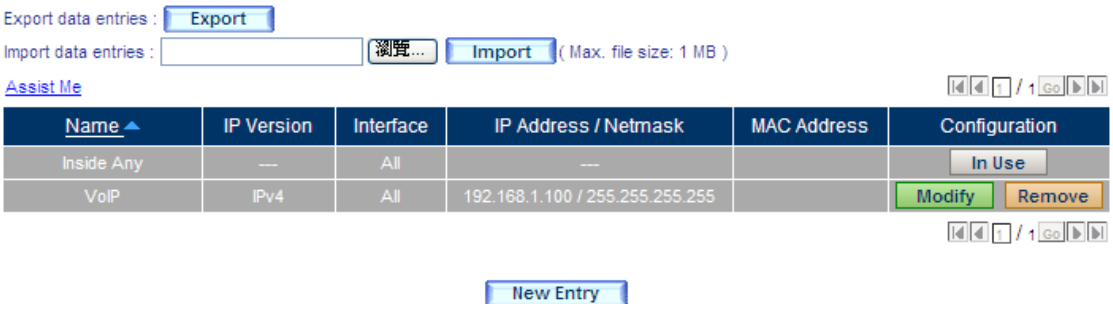


Figure 10-14 The Address Settings

Step 3. Create a VoIP service under **Policy Object** > **Service** > **Custom**. **(Figure 10-15)**

Figure 10-15 The Completed Custom Service

Step 4. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below: （**Figure 10-16**）

- **Name :** Enter the name for the Virtual IP setting.
- **Server Real IP :** Select Port 2 (WAN1) and type 61.11.11.12 in the field, or click **Assist Me** to select an IP addresss.
- **Service**: Select the custom service setting.
- **External Port No:** Will be automatically set to the customized service.
- **Scheduling Algorithm:** Select **Round-Robin.**
- **Interface**: Select Port1 (LAN1).
- **IP of Virtual Server 1**: Enter 192.168.1.100, or click **Assist Me** to select an IP addresss)
- Click **OK**.（**Figure 10-17**）

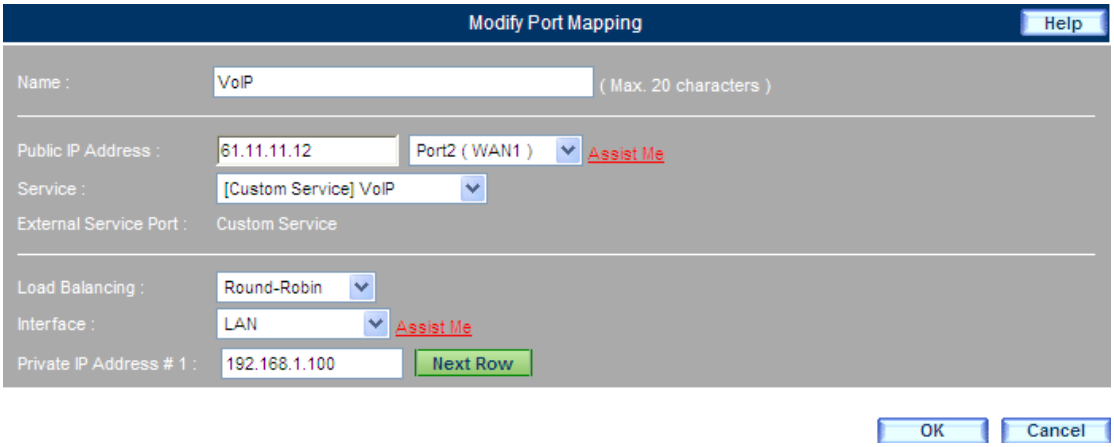


Figure 10-16 Setting Virtual IP

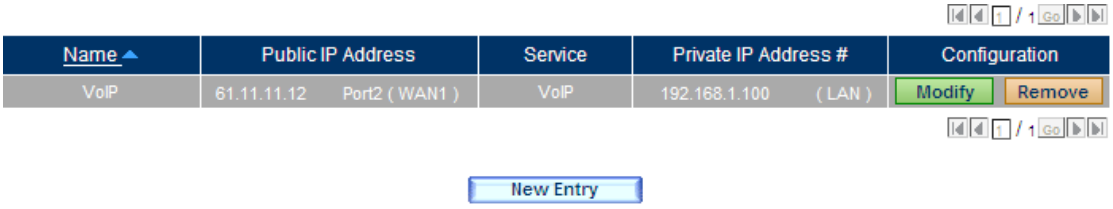


Figure 10-17 The Completed Virtual IP Settings

Note：

1. The **External Port No.** can only be modified for single port numbers and not for ranges.

Step 5. Under **Policy** > **Incoming**, set as below:（**Figure 10-18**）

- **Destination IP**: Select the vitual server setting.
- **Service**: Select the custom service setting.
- Click **OK**.（**Figure 10-19**）

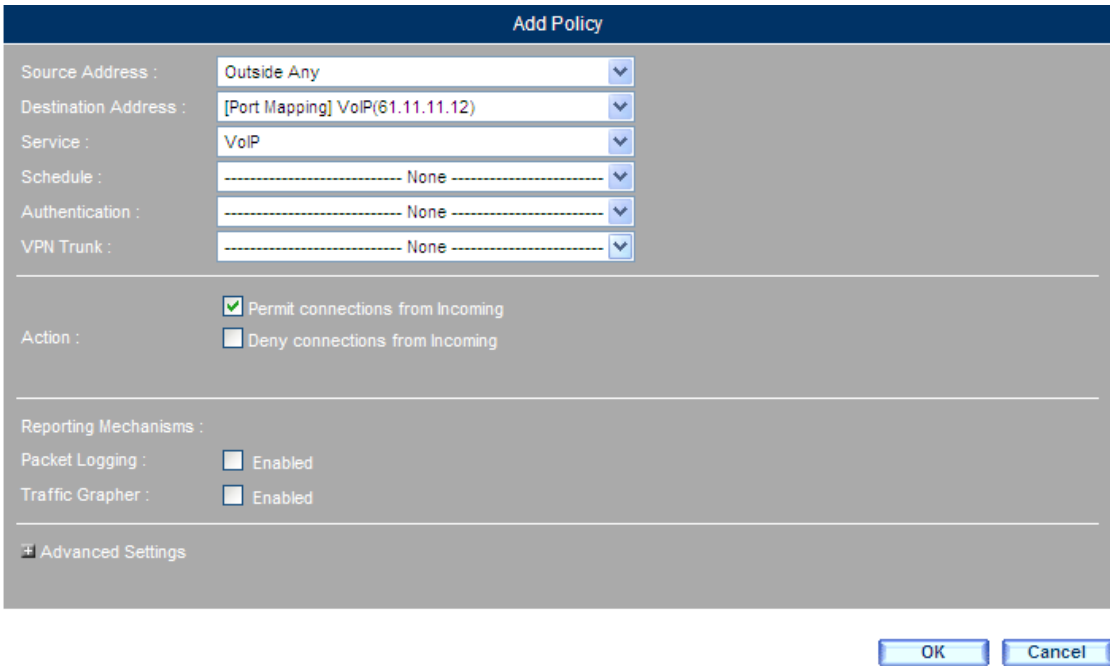


Figure 10-18 Applying the Service to the Policy

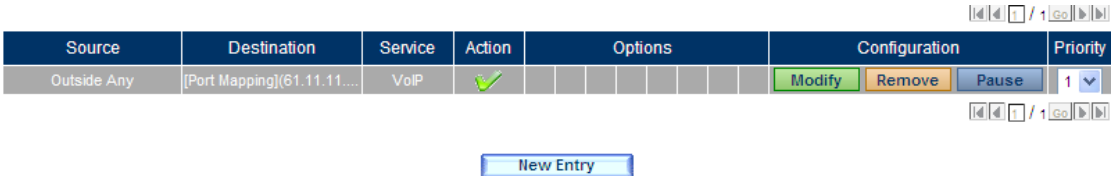


Figure 10-19 The Completed Policy Setting

Step 6. Under **Policy > Outgoing**, set as below: (**Figure 10-20**)

- **Source IP:** Select the address setting.
- **Service**: Select the service setting.
- **Action**: Select Port2 (WAN1)
- Click **OK**. (**Figure 10-21**)

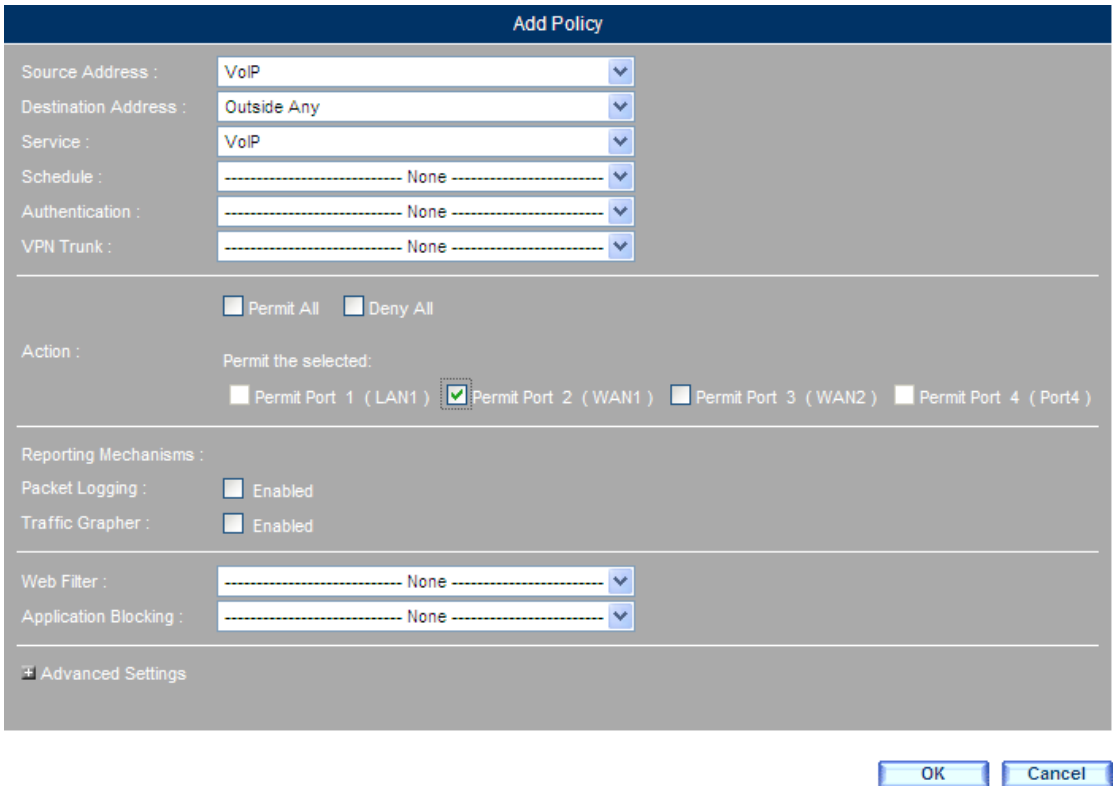


Figure 10-20 Setting an Outgoing Policy

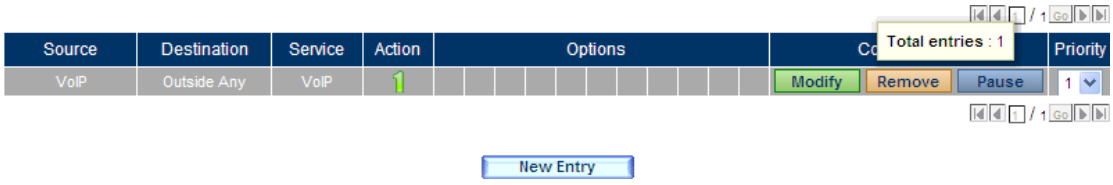


Figure 10-21 The Completed Settings

Important：

1. To enable the LAN to LAN connection, go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**). To enable the DMZ to DMZ connection, go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**).

Step 7. A VoIP session created between an internal and external user.（Figure 10-22）

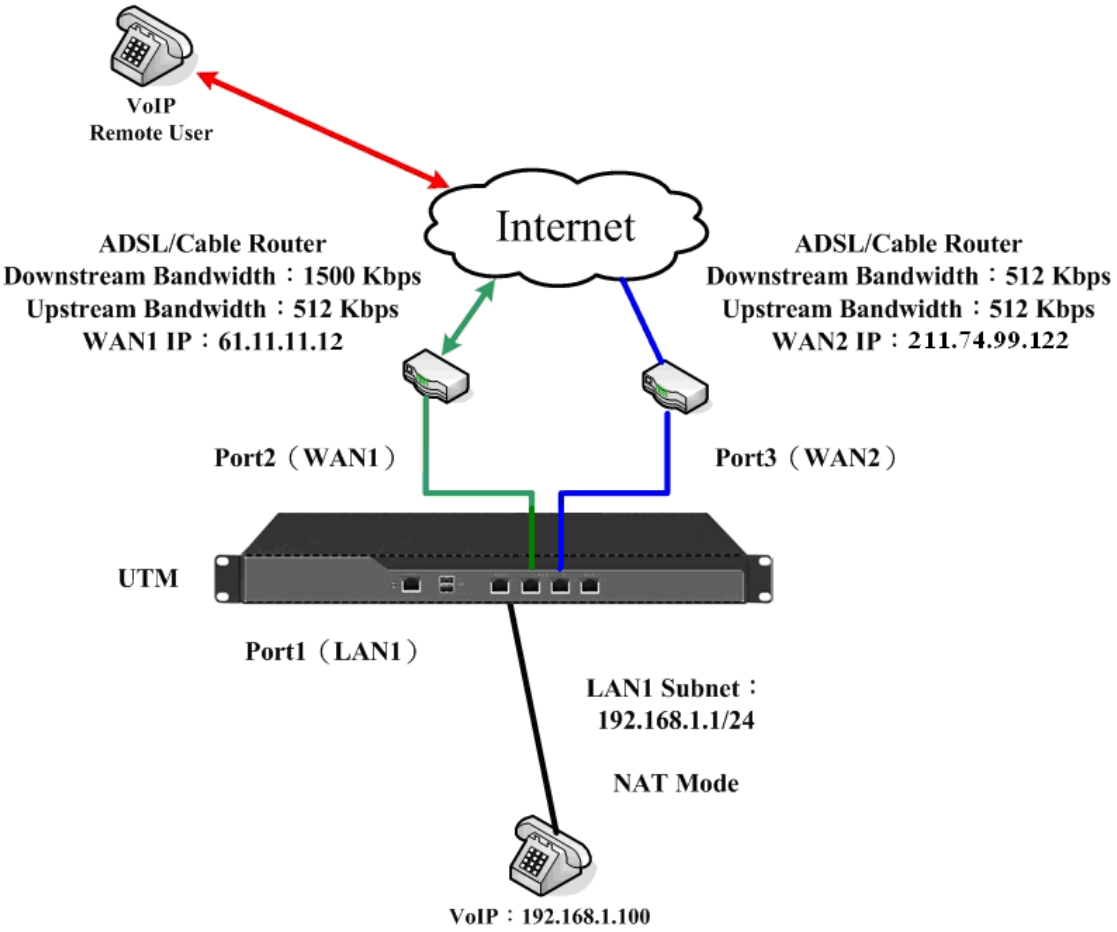


Figure 10-22 The Completed VoIP Setup

10.1.4 Using Multiple Virtual Servers to Provide HTTP, POP3, SMTP and DNS Services through the Regulation of a Policy

Step 1. Set up multiple service servers of which IP addresses respectively are 192.168.1.101, 192.168.1.102, 192.168.1.103 and 192.168.1.104 in the LAN. And then, configure their preferred DNS server addresses as that of the external DNS server.

Step 2. Under **Policy Object** > **Address** > **LAN / LAN Group**, set as below: （**Figure 10-23, 10-24**）

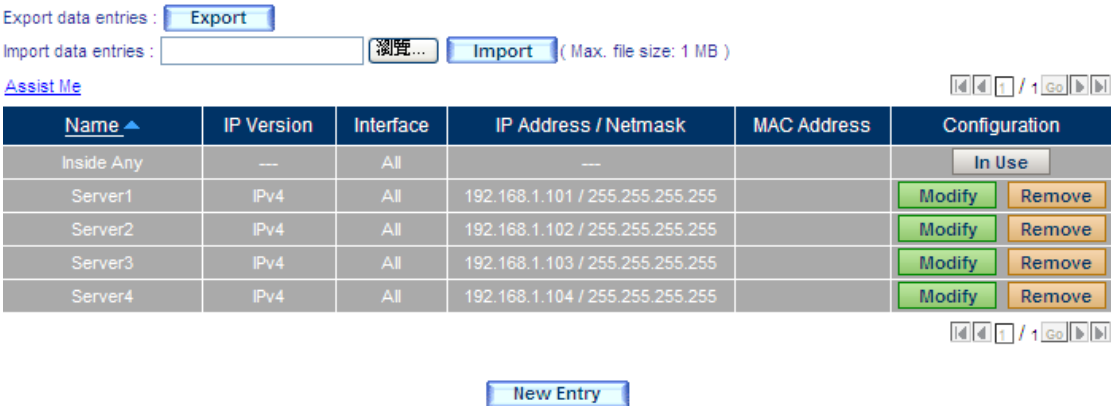


Figure 10-23 Address Settings

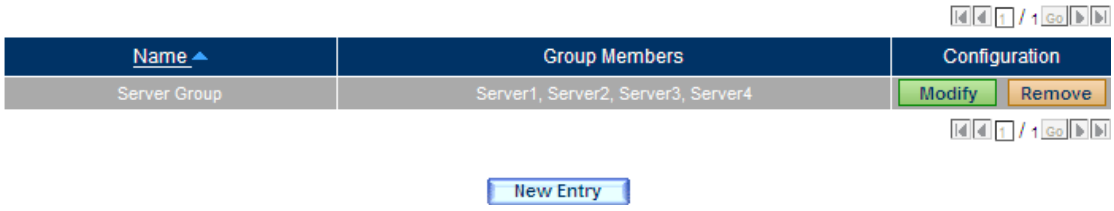


Figure 10-24 A Created Group Address

Step 3. In **Policy Object** > **Service** > **Group**, group the necessary services of providing HTTP, POP3, SMTP and DNS services. And then, create a group containing the necessary services for the server to send emails.（**Figure 10-25**）

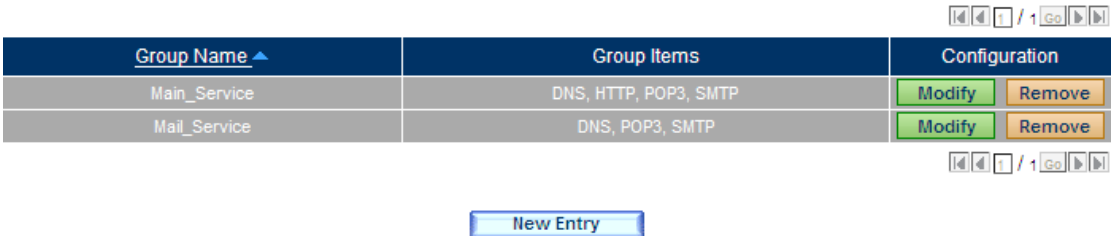


Figure 10-25 A Created Group Service

Step 4. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below: （**Figure 10-26**）

- Name: Enter the name for the setting.
- **Server Real IP**: Select Port3 (WAN2) and type “211.22.22.23” in the field, or click **Assist Me** to select an IP address.
- Select the defined service from the **Service** drop-down list.
- **External Port No:** Will be automatically set to the customized service.
- **Scheduling Algorithm**: Select Round-Robin.
- **Interface**: Select Port1(LAN1).
- IP of Virtual Server 1: Enter 192.168.1.101 (or you may click on **Assist Me**)
- IP of Virtual Server 2: Enter 192.168.1.102 (or you may click on **Assist Me**)
- IP of Virtual Server 3: Enter 192.168.1.103 (or you may click on **Assist Me**)
- IP of Virtual Server 4: Enter 192.168.1.104 (or you may click on **Assist Me**)
- Click **OK**.（**Figure 10-27**）

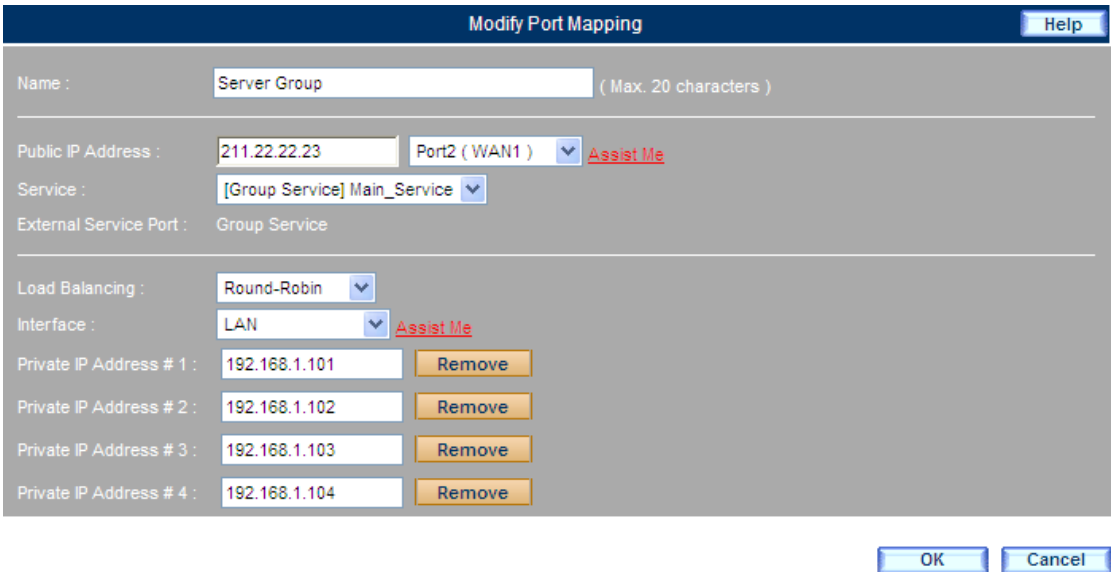


Figure 10-26 Port Mapping Settings

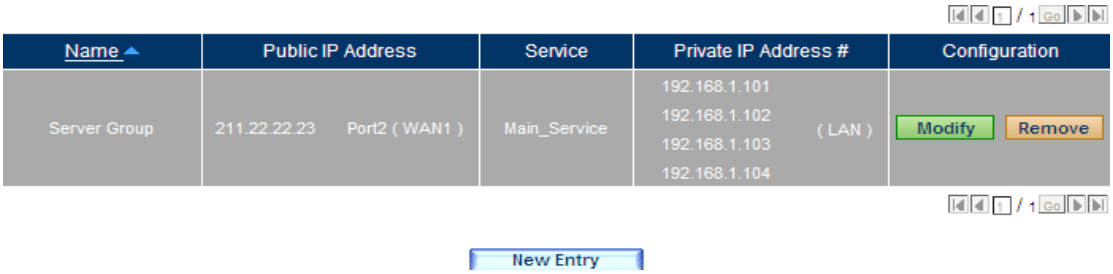


Figure 10-27 Settings Completed

Step 5. Go to **Policy** > **Incoming** and then set as below:（**Figure 10-28**）

- Select the virtual server setting for **Destination IP**.
- Select Main_Service for **Service**.
- Click **OK**.（**Figure 10-29**）

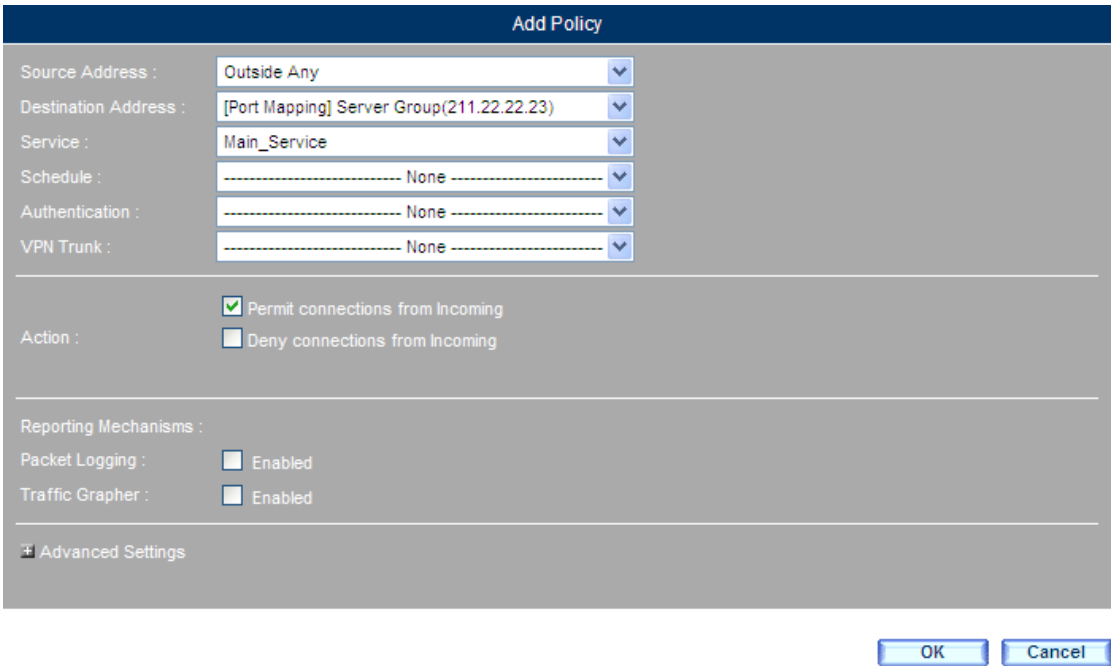


Figure 10-28 Configuring an Incoming Policy

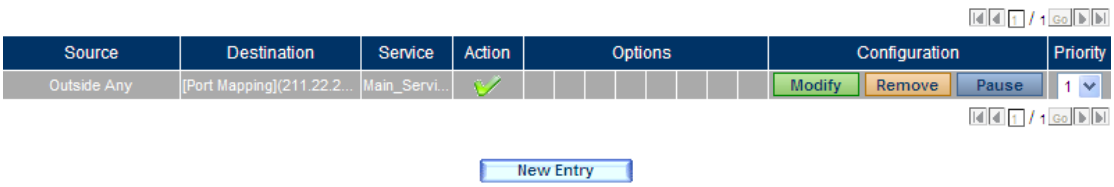


Figure 10-29 Policy Completed

Step 6. Go to **Policy > Outgoing** and set as below: (**Figure 10-30**)

- Select the defined rule from the **Source Address** drop-down list.
- Select Mail_Service from the **Service** drop-down list.
- Click **OK**. (**Figure 10-31**)

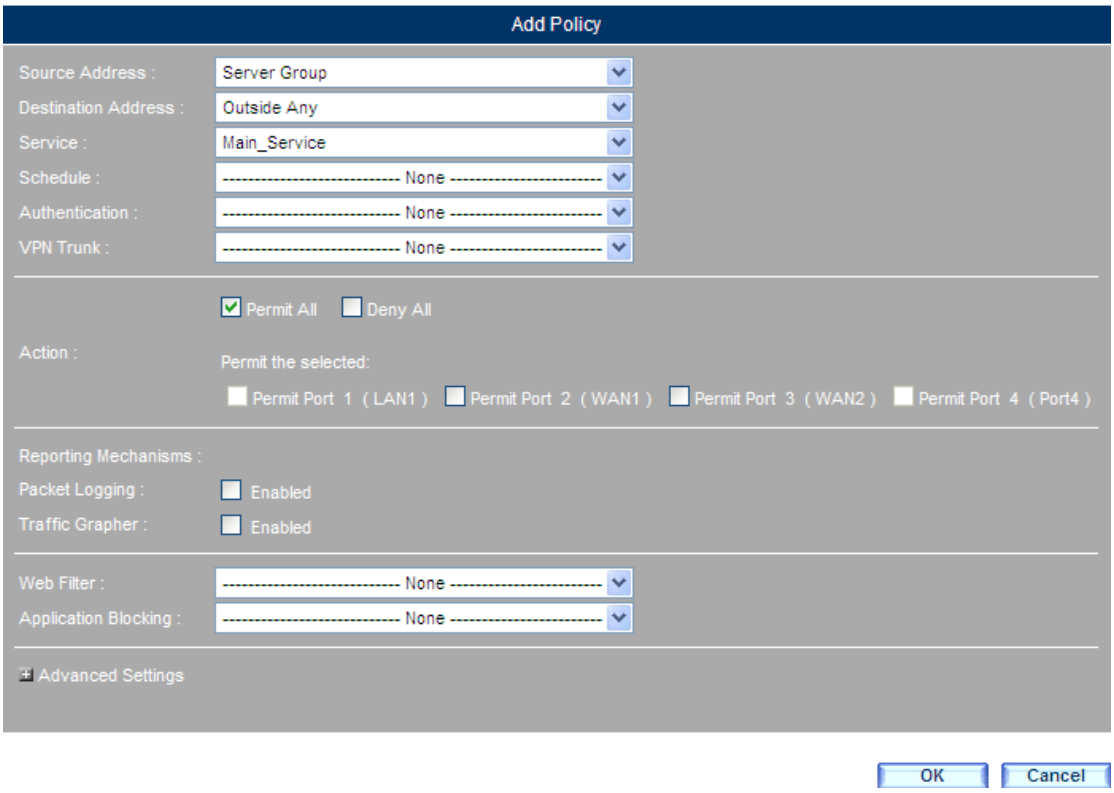


Figure 10-30 Configuring an Outgoing Policy

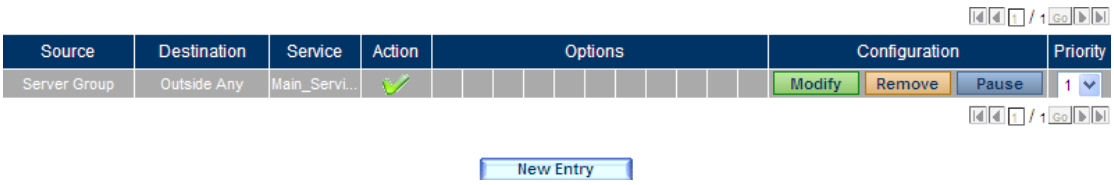


Figure 10-31 Policy Completed

Important：

1. To enable the LAN to LAN connection, go to **Policy > LAN to LAN** and create a policy (select Inside Any for both **Source Address** and **Destination Address**). To enable the DMZ to DMZ connection, go to **Policy > DMZ to DMZ** and create a policy (select DMZ Any for both **Source Address** and **Destination Address**).

Step 7. Settings completed.（Figure 10-32）

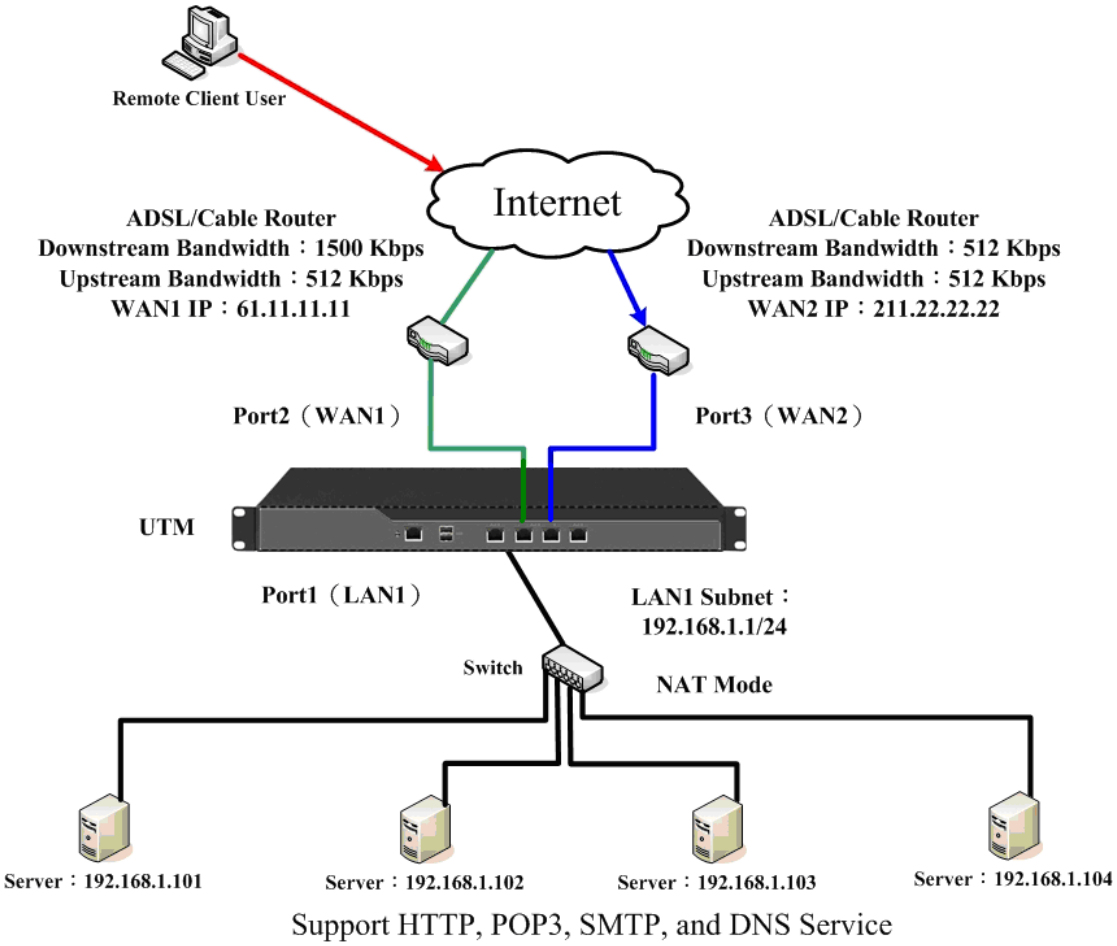


Figure 10-32 Settings Completed

Chapter 11 VPN

To obtain a private and secure network link, the CS-2001 is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secure options for enterprises to adopt in comparison to other methods.

Note：

1. To create a secure VPN connection, the settings of **IPSec Autokey**, **PPTP Server** or **PPTP Client** must be applied to the **Trunk** settings. Then, apply the **Trunk** settings to correlative policies.

Terms in VPN

Diffie-Hellman

- A cryptographic protocol that allows two parties that have no perior knowledge of each other to establish a shared secret key over an insecure communications channel.

RSA

- The RSA is a kind of asymmetric cryptography. It involves a public and private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Pre-Shared Key String

- A Pre-Shared Key String is a string of Unicode characters used to authenticate Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPSec) connections.

ISAKMP (Internet Security Association Key Management Protocol)

- 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 IT administrator can assign of which key size or Pre-Shared Key String and algorithm to use. The SA comes in many connection ways, for instance, use the ISAKMP SA between two PCs, and assign an ENC algorithm (DES, triple DES, 40-bit DES or not using any) and an authentication method to use.

Main mode

- When associating IKE certificates, the device offers main mode and aggressive mode to choose from. The main mode requests sending 6 messages mutually before starting the data exchange, it is to confirm the identity of both parties, ensuring the data transferring security.

Aggressive mode

- The aggressive mode requests sending 3 messages mutually before starting the data exchange, it is to confirm the identity of both parties, ensuring the data transferring security.

AH (Authentication Header)

- The Authentication Header guarantees connectionless integrity and data origin authentication of IP datagrams.

ESP (Encapsulating Security Payload)

- The Encapsulated Security Payload provides confidentiality and integrity protection to IP datagrams.

DES (Data Encryption Standard)

- The Data Encryption Standard is a NIST standard encryption using 56-bit key.

3DES (Triple-DES)

- Triple DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times. It can achieve an algorithm up to 168 bits.

AES (Advanced Encryption Standard)

- The Advanced Encryption Standard (AES) is a symmetric key encryption technique, usually using a 126-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.

NULL Algorithm

- The NULL Algorithm is an instant and convenient alternative for connection. It is merely a simple replacement for ESP (Encapsulating Security Payload) without any cryptograph protection.

SHA1 (Secure Hash Algorithm-1)

- The SHA1 is a revision of SHA (Secure Hash Algorithm). It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.

MD5 Algorithm

- MD5 (Message Digest Algorithm 5) processes a variable-length message into a fixed–length output of 128 bits.

GRE/ IPSec

- The GRE (Generic Routing Encapsulation) comes in packet packing function without any encryption against monitoring and attacking. Normally, the GRE needs to cooperate with IPSec so as to provide a secure connection.

Extended Authentication (XAuth)

- XAuth provides an additional level of authentication. It uses a Request/ Reply mechanism to provide the extended authentication. XAuth is also referred to as two factor authentication.

Note:

1. The **Account Name** under **Extended Authentication (XAuth)** are the accounts listed under **Poliy > Authentication > Account**.

Terms in One-Step IPSec

One-Step IPSec

- *One-Step IPSec* merely takes one step to complete settings
  - Go to **Policy Object > VPN > One-Step IPSec**, and then refer to the following to configure:
    - Type a name for the connection in the **Name** field.（**Figure 11-1**）
    - Select a WAN port for **WAN Interface**.
    - Select **LAN** and then select the **Subnet / Mask** addresses.
    - Specify the IP address or domain name of the destination gateway in **Remote Gateway – Fixed IP or Domain Name**.
    - Specify the subnet and mask addresses in the **Subnet / Mask** fields.
    - Type a word string as Pre-Shared Key String in the **Pre-Shared Key String** field.
    - Click **OK.**
    - The device will automatically finish other related but necessary settings and create a corresponding policy for the connection.（**Figure 11-2, 11-3, 11-4, 11-5**）

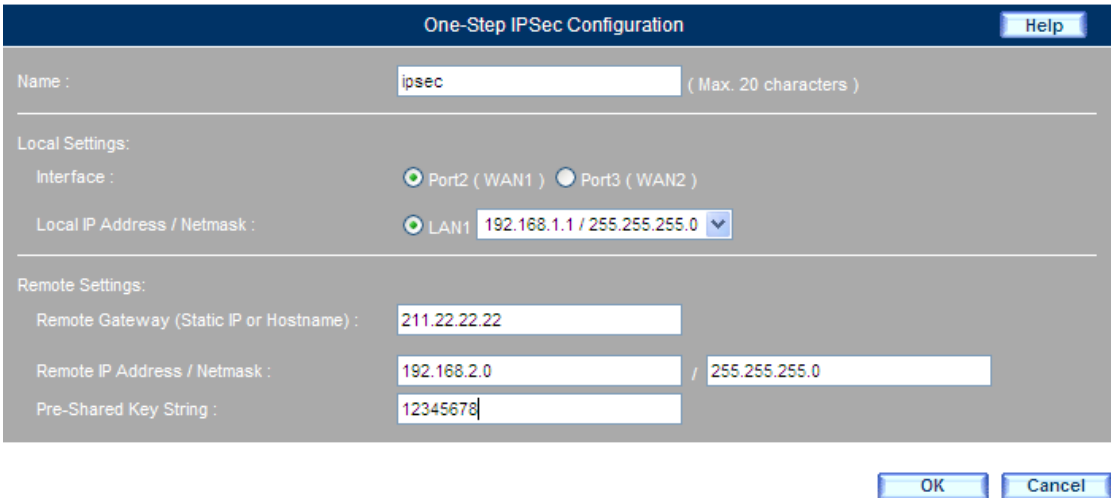


Figure 11-1 One-Step IPSec Settings

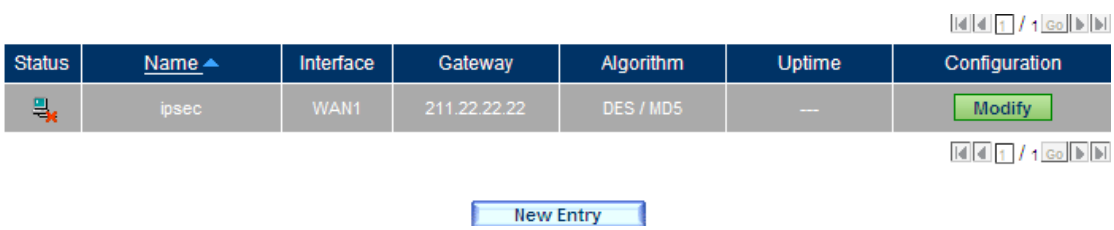


Figure 11-2 Setting Completed

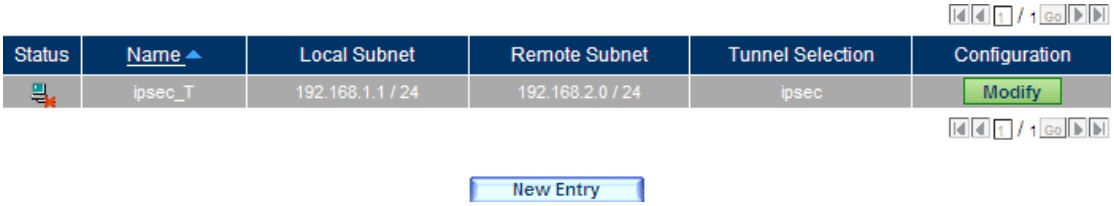


Figure 11-3 The Automatically Created IPSec Policy

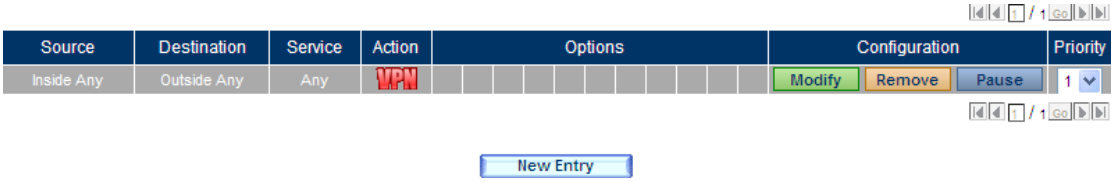


Figure 11-4 The Corresponding Outgoing Policy

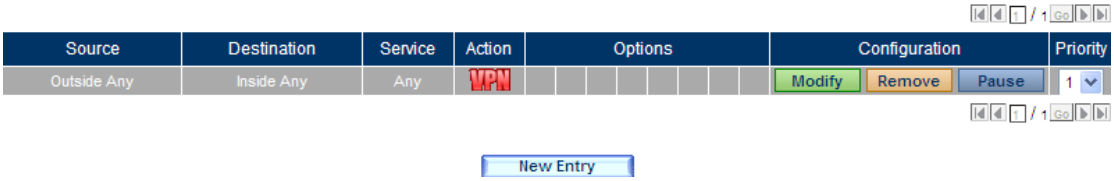


Figure 11-5 The Corresponding Incoming Policy

Note：

1. **One-Step IPSec** uses default settings (listed below) on most configurations to simplify the procedure of creating a VPN connection with IPSec encryption:
   - Mode: Main mode
   - Authentication Method: Pre-Shared Key
   - ISAKMP Algorithm: DES + MD5 + Group1
   - IPSec Algorithm: DES + MD5
   - The corresponding policies for the VPN connection will be created accordingly.

Terms in VPN Wizard：

VPN Wizard

- It simplifies the settings of a VPN connection.
  - Under **Policy Object > VPN > VPN Wizard**, set as below:
    - Select a connection method and then click **Next**.（**Figure 11-6**）
    - Create a policy for VPN connection. Click **Next** when finished.（**Figure 11-7**）
    - Create a VPN Trunk. Click **Next** when finished.（**Figure 11-8**）
    - Select the VPN.（**Figure 11-9**）
    - Click **Finish**.（**Figure 11-10**）
    - Setting completed.（**Figure 11-11, 11-12**）

Figure 11-6 Selecting a Connection Method

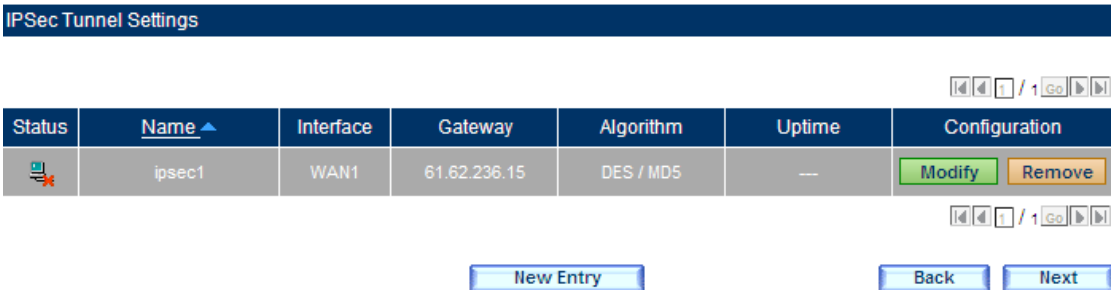


Figure 11-7 A Policy for VPN Connection

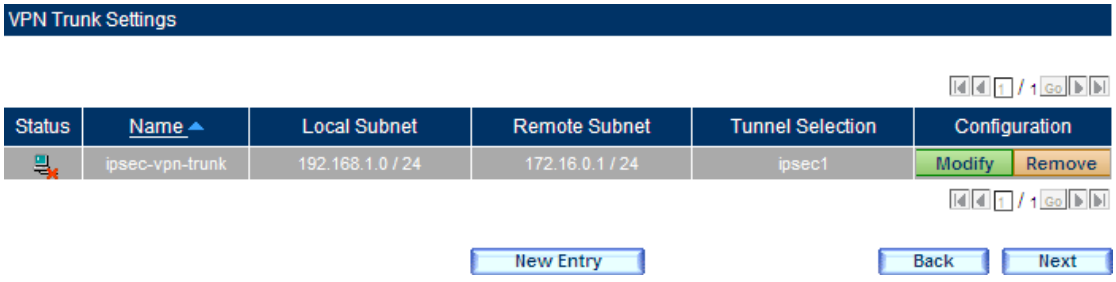


Figure 11-8 A VPN Trunk Setting

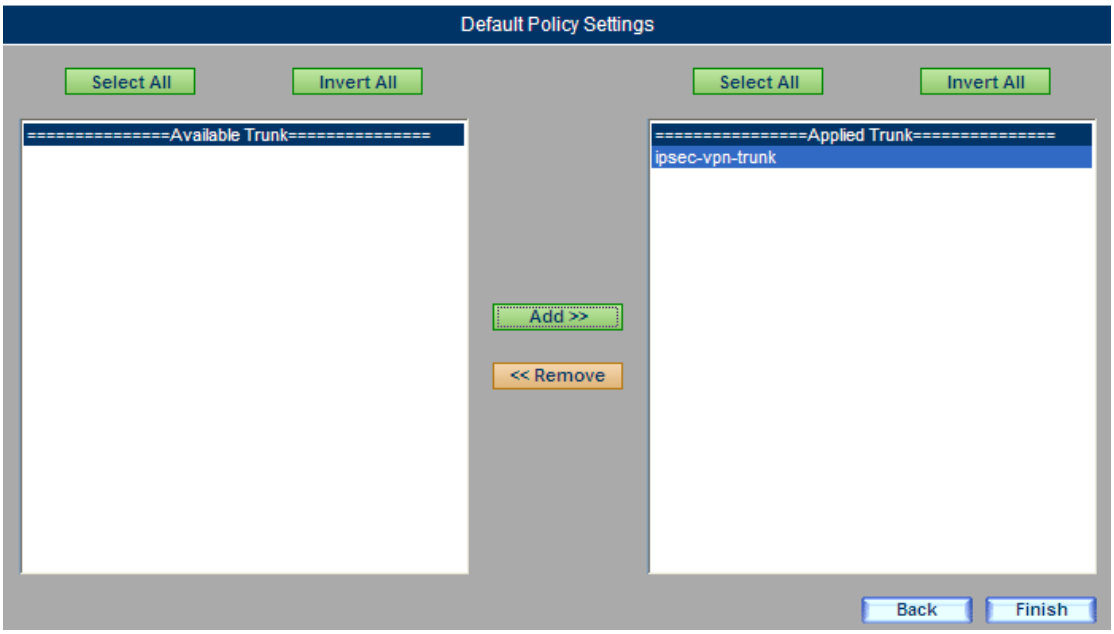


Figure 11-9 Applying Available VPN Trunk to the Policy

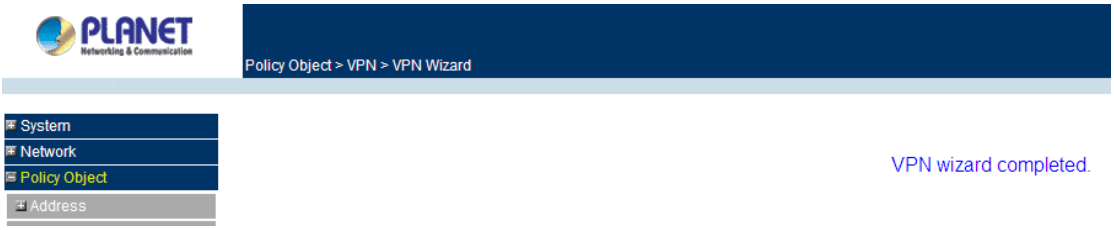


Figure 11-10 Setting Completed

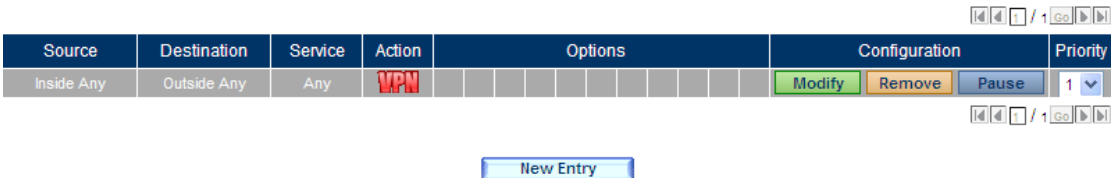


Figure 11-11 An Outgoing Policy Completed

Figure 11-12 An Incoming policy Completed

Terms in IPSec Autokey

Status

- The symbol and its description used in the VPN connection status.

Symbol		
Description	Disconnected	Connecting

Name

- The description for IPSec Autokey. Note: the name has to be unique.

Interface

- The WAN interface of the local gateway.

Gateway IP

- The WAN interface address of the remote gateway.

IPSec Algorithm

- It displays the algorithm that the VPN connection currently employed.

Uptime

- Signified the time elapsed since the connection was established.

Configuration

- Click **Modify** to modify the setting, or click **Remove** to remove the setting.

（**Figure 11-13**）

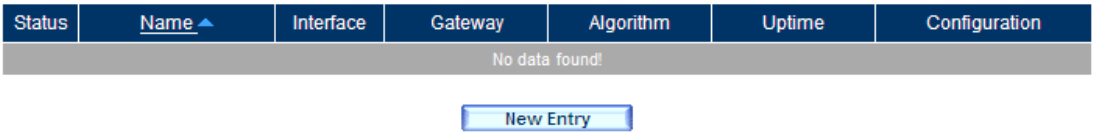


Figure 11-13 IPSec Autokey Screen

Note：

1. By default, CS-2001 will create an IPSec VPN connection using **Dead Peer Detection**. If **Remote Gateway – Fixed IP or Domain Name** has been specified, then the IT administrator may manually create an IPSec VPN connection.

Terms in PPTP Server

PPTP Server

- The status of PPTP server that shows enable or disable.
- The range of IP address, DNS server, WINS servers for clients using PPTP connection.

Status

- The symbol and its description used in the VPN connection status.

Symbol		
Description	Disconnected	Connecting

User Name

- It displays the name of logged-in PPTP client user.

Client IP

- It displays the IP address of clients using PPTP connection to log in to PPTP server.

Uptime

- It displays the duration of the connection between client and server.

Configuration

- Click **Modify** to modify the settings, or click **Remove** to remove the settings. **（Figure 11-14）**

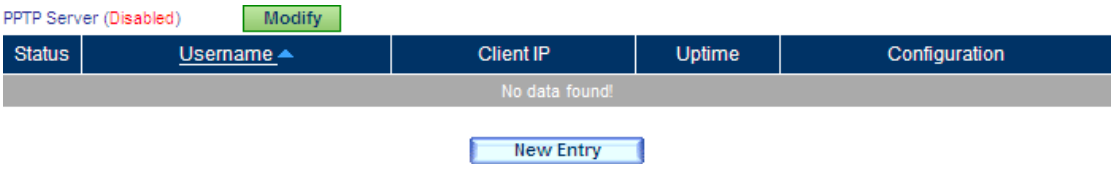


Figure 11-14 PPTP Server Screen

Note：

1. By default, CS-2001 will create a PPTP VPN connection using **Echo-Request**. If **Manual Disconnect** is ticked, then the IT administrator shall be able to disconnect the connection manually.

Terms in PPTP Client

Status

- The symbol and its description used in the VPN connection status.

Symbol		
Description	Disconnected	Connecting

User Name

- It displays the name of clients using PPTP to log in to PPTP server.

Server IP or Domain Name

- It displays the IP address or the domain name of clients using PPTP to log in to PPTP server.

Encryption

- It determines whether to use encryption on the connection between client and server.

Uptime

- It displays the duration of the connection between client and server.

Configuration

- Click **Modify** to modify the setting, or click **Remove** to remove the setting. （**Figure 11-15**）

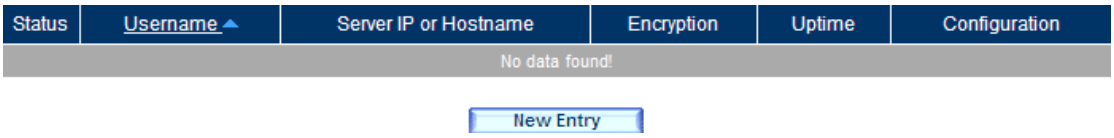


Figure 11-15 PPTP Client Screen

Note：

1. By default, CS-2001 will create a PPTP VPN connection using **Echo-Request**. If **Manual Connection** is ticked, then the IT administrator shall be able to create a connection manually.

Terms in Trunk

Status

- The symbol and its description used in the VPN connection status.

Symbol		
Description	Disconnected	Connecting

Name

- The description for VPN trunk. Note: the name has to be exclusive from any other.

Source Subnet

- The IP address of source subnet.

Destination Subnet

- The IP address of destination subnet.

Tunnel

- It displays of which VPN trunk it includes, such as IPSec, PPTP Server or PPTP client.

Configuration

- Click **Modify** to change the configuration of VPN trunk; click **Remove** to remove the setting; click **Pause** to suspend the setting; click **Enable** to resume the setting.（**Figure 11-16**）

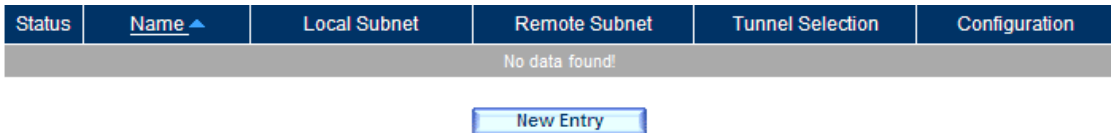


Figure 11-16 VPN Trunk Screen

Note:

1. Enabling the trunk load balancing feature will allow the packets of a session to be load-balanced through a VPN trunk to increase the link speed. The load balancing algorithm specifed under **Network > Interface > Load Balancing Mode** will be adapted to load balance between two CS-2001 units.

Terms in Trunk

Name

- The description for VPN trunk. Note: the name has to be exclusive from any other.

Group Member

- The groups that are subject to the VPN Trunk rule.

Configuration

- Click **Modify** to change the configuration of VPN trunk; click **Remove** to remove the setting.（**Figure 11-17**）

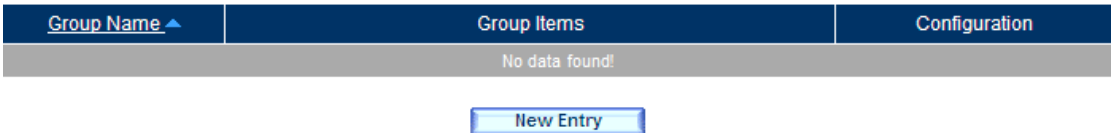


Figure 11-17 VPN Trunk Screen

11.1 Example

No.	Settings	Scenario	Page
11.1.1	**IPSec Autokey**	Using Two CS-2001 Devices to Mutually Access the Resources of Two Subnets via an IPSec VPN Connection	**256**
11.1.2	**IPSec Autokey**	Creating an IPSec VPN Connection under Windows 2000 by a CS-2001 Device	**269**
11.1.3	**IPSec Autokey**	Creating an IPSec VPN Connection between Two CS-2001 Devices (An Aggressive Mode Example)	**319**
11.1.4	**IPSec Autokey**	Using Two CS-2001 Devices to Connect Outbound Load Balance with IPSec VPN (Using GRE/IPSec Package Algorithm)	**334**
11.1.5	**IPSec Autokey**	Establishing an IPSec VPN Connection by Three CS-2001 Devices	**352**
11.1.6	**PPTP**	Using Two CS-2001 Devices to Establish PPTP VPN Connection (Outbound Load Balancing)	**374**
11.1.7	**PPTP**	Using Two CS-2001 Devices to Establish PPTP VPN Connection	**389**
11.1.8	**PPTP**	Establishing PPTP VPN Connection by One CS-2001 Device and One PC Running Windows 2000	**396**

11.1.1 Using Two CS-2001 Devices to Mutually Access the Resources of Two Subnets via an IPSec VPN Connection

Prerequisite Setup (Note: IP addresses used as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP address range: 192.168.10.x/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1 (192.168.20.1). IP address range 192.168.20.x/24.
Configure Port2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Multiple subnet: 192.168.85.1. IP address range: 192.168.85.x/24

This example uses two CS-2001 devices to establish VPN connection between A Company and B Company.

For A Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **IPSec Autokey**, and then click **New Entry.** （**Figure 11-18**）

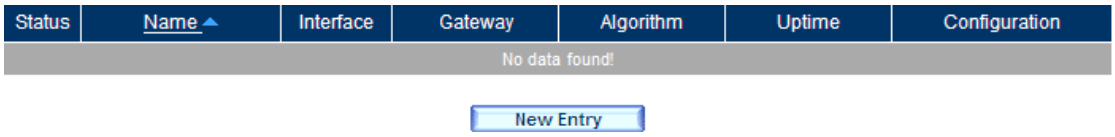


Figure 11-18 IPSec Autokey Screen

Step 2. Enter IPSec tunnel in the **Name** field. Select Port2 (WAN1) for **WAN Interface.**（**Figure 11-19**）

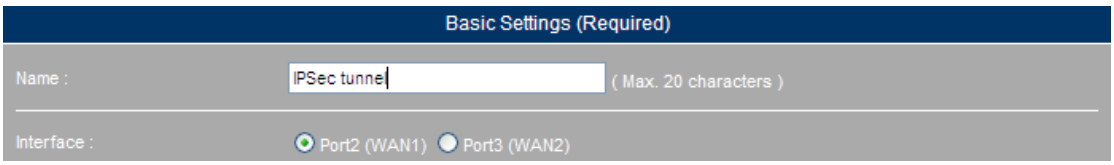


Figure 11-19 Name and WAN Interface Settings

Step 3. Select **Remote Gateway (Static IP or Hostname)** for **Remote Settings**, and enter the management address of B Company.（**Figure 11-20**）

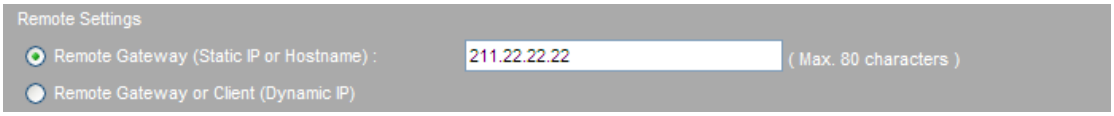


Figure 11-20 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of Pre-Shared Key String is 103 characters.) （**Figure 11-21**）

Figure 11-21 Authentication Method Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “Group 1” for **Group**. （**Figure 11-22**）

Figure 11-22 Encryption and Data Integrity Algorithms Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**. （**Figure 11-23**）

Figure 11-23 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**. （**Figure 11-24**）

Figure 11-24 Advanced Settings of IPSec Autokey

Step 8. Settings completed.（Figure 11-25）

Figure 11-25 IPSec Autokey Settings Completed

Step 9. Under **Policy Object** > **VPN** > **Trunk**, set as below:（Figure 11-26）

- **Name**:Type a name.
- **Local Settings** : Select "LAN**". Local IP / Netmask** : Type "192.168.10.0" as A Company's subnet address and 255.255.255.0 as **Mask**.
- **Remote Settings**: Tick "**Remote IP / Netmask**". **Remote IP / Netmask**: Type "192.168.85.0" as B Company's subnet address and 255.255.255.0 as **Mask**.
- **Tunnel**: Select "IPSec tunnel" and then add it to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（Figure 11-27）

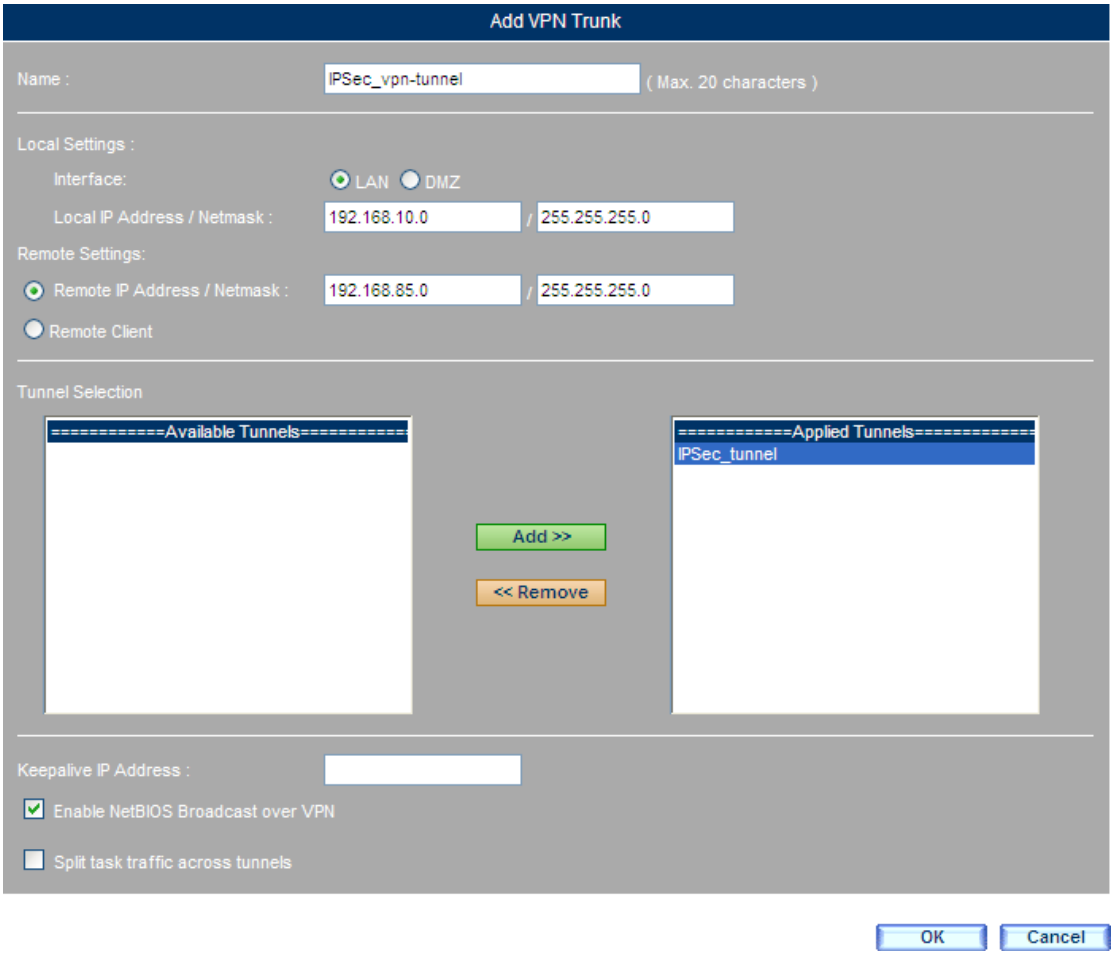


Figure 11-26 VPN Trunk Settings

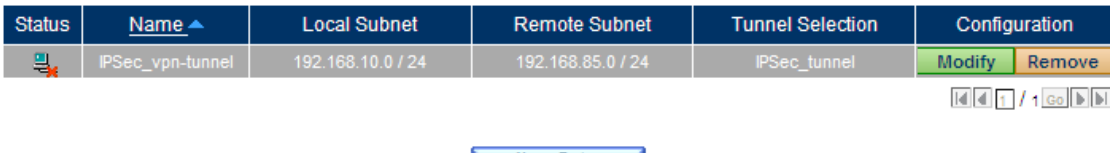


Figure 11-27 VPN Trunk Created

Step 10. Under **Policy** > **Outgoing**, set as below:（Figure 11-28）

- Select the defined trunk for VPN Trunk.
- Click **OK**.（Figure 11-29）

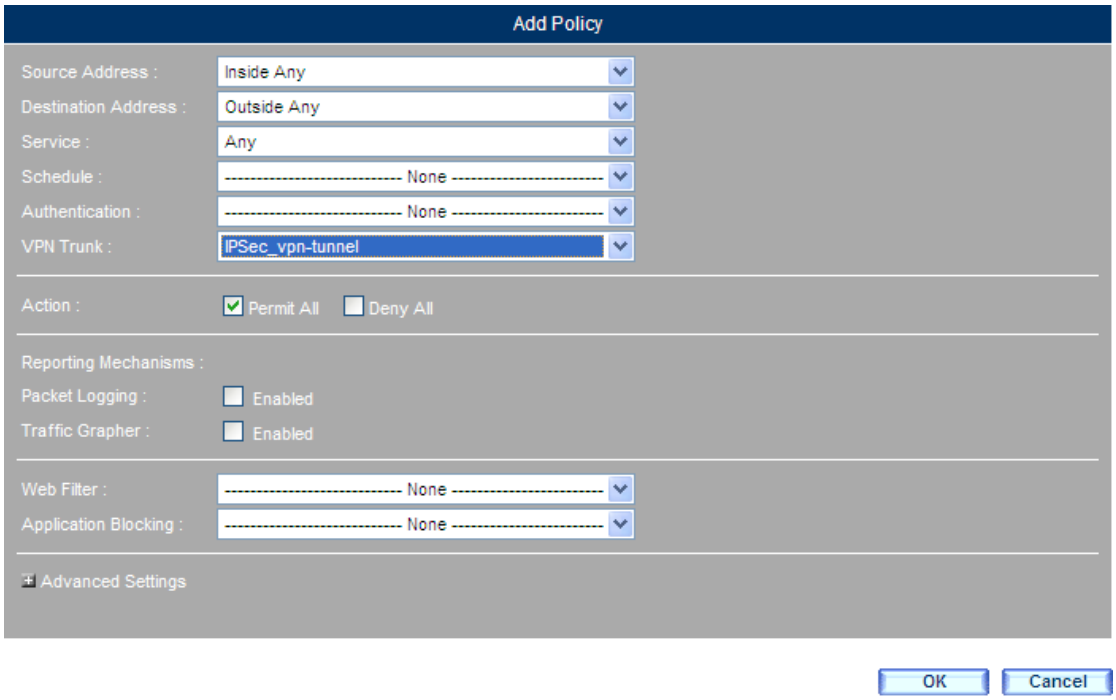


Figure 11-28 Configuring a Policy with VPN Trunk

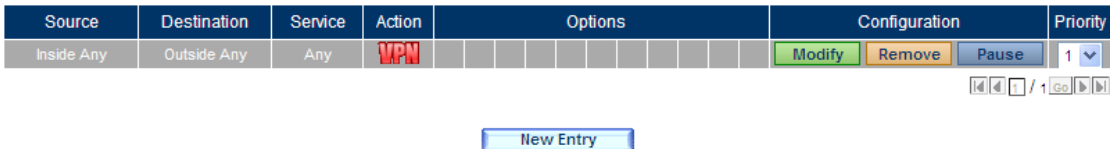


Figure 11-29 Policy Created

Step 11. Under **Policy > Incoming**, set as below: (**Figure 11-30**)

- Select the defined trunk for **VPN Trunk**.
- Click **OK**. (**Figure 11-31**)

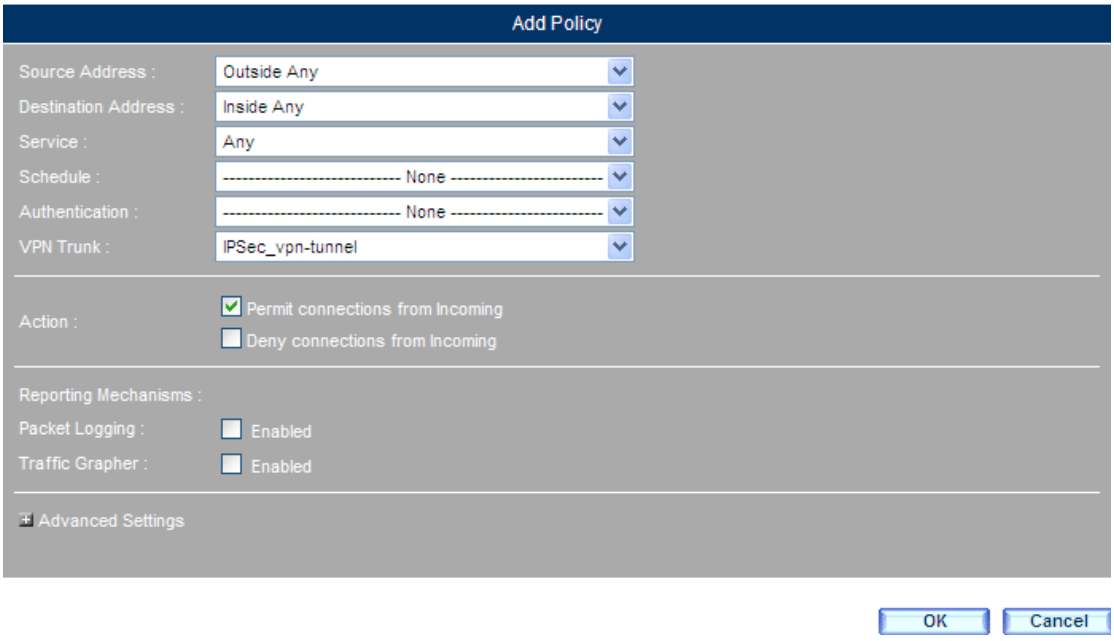


Figure 11-30 Creating an Incoming Policy with VPN Trunk

Figure 11-31 An Incoming Policy with VPN Trunk

Note：

1. Under **Policy Object > VPN > IPSec Autokey**, if **Remote Gateway or Client (Dynamic IP)** is selected under **Remote Settings**, then **Aggressive Mode** must be selected for **IKE Negotiation** and the **Local ID** field and the **Peer ID** field must be completed for the connection.

For B Company, set as below:

Step 1. Under **System** > **Configuration** > **Multiple Subnets**, set as below: (**Figure 11-32**)

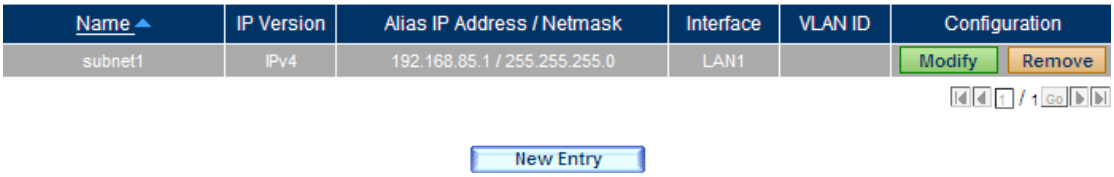


Figure 11-32 Multiple Subnet Settings

Step 2. Go to **Policy Object** > **VPN** > **IPSec Autokey**, and then click **New Entry.** (**Figure 11-33**)

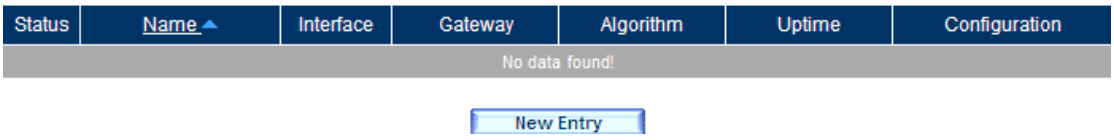


Figure 11-33 IPSec Autokey Screen

Step 3. Type IPSec_tunnel2 in the **Name** field and then select Port2 (WAN1) for **WAN Interface**. (**Figure 11-34**)

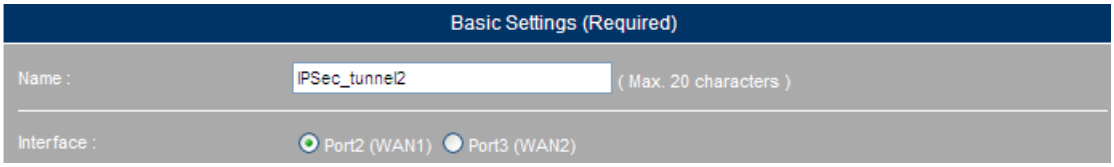


Figure 11-34 Name and WAN Interface Settings

Step 4. Select **Remote Gateway (Static IP or Hostname)** for **Remote Settings**, and enter the management address of A Company. (**Figure 11-35**)

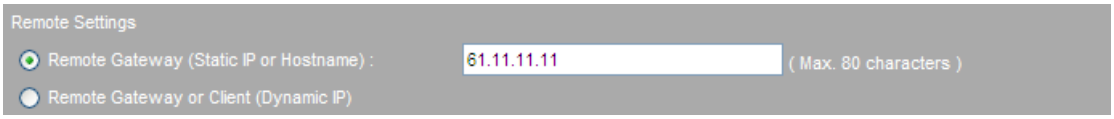


Figure 11-35 Remote Settings

Step 5. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of Pre-Shared Key String is 103 characters.) （**Figure 11-36**）

Figure 11-36 Authentication Method Settings

Step 6. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.（**Figure 11-37**）

Figure 11-37 Encryption and Data Integrity Algorithms Settings

Step 7. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm.**（**Figure 11-38**）

Figure 11-38 IPSec Algorithm Settings

Step 8. Under the **Advanced Settings (optional)** section, select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.
（**Figure 11-39**）

Figure 11-39 Advanced Settings of IPSec Autokey

Step 9. Settings completed.（**Figure 11-40**）

Figure 11-40 IPSec Autokey Settings Completed

Step 10. Under **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-41**）

- **Name**: Type a name.
- **Local Settings**: Check “LAN”. **Local IP / Netmask**: Type “192.168.85.0” as B Company’s subnet address and “255.255.255.0” as **Mask**.
- **Remote Settings**: Select “**Remote IP / Netmask**”. **Remote IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask.**
- **Tunnel**: Select “IPSec_tunnel2” and then add it to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-42**）

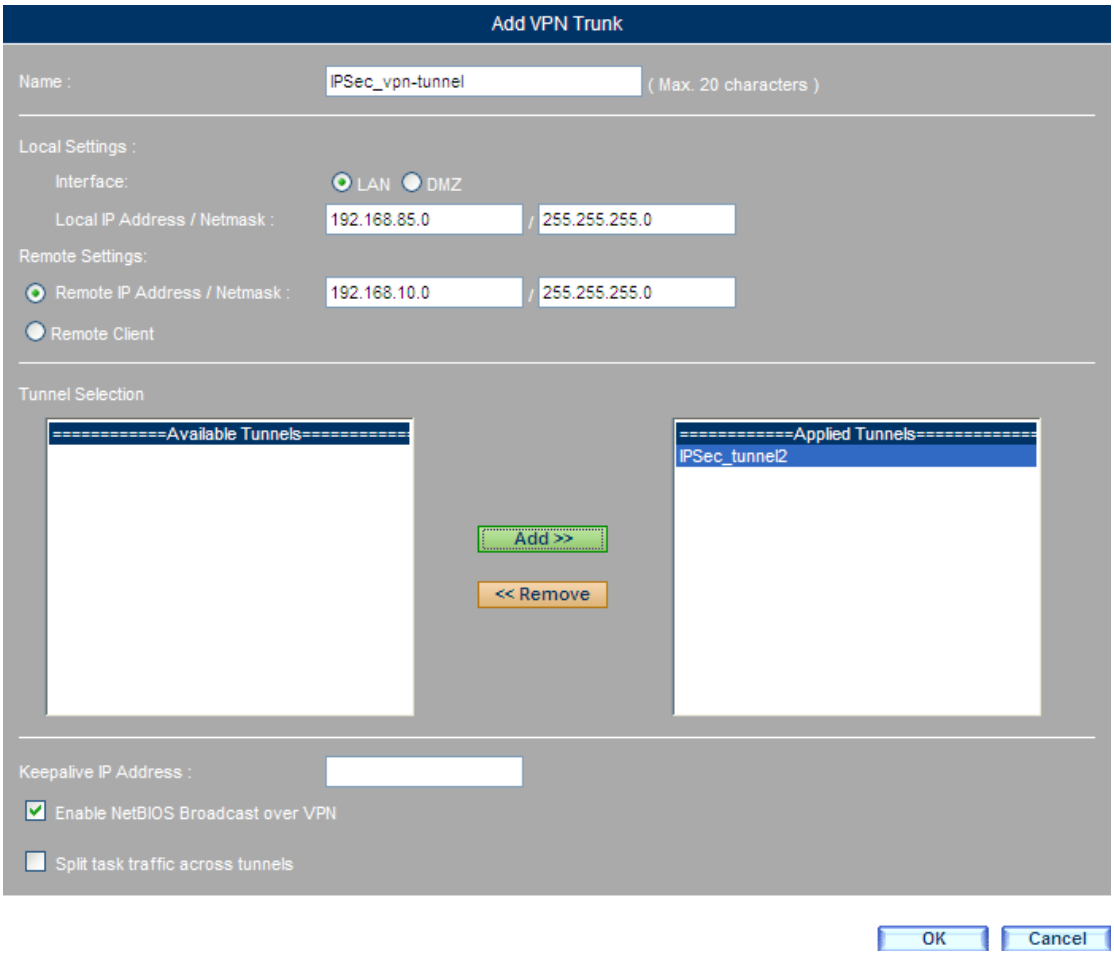


Figure 11-41 VPN Trunk Settings

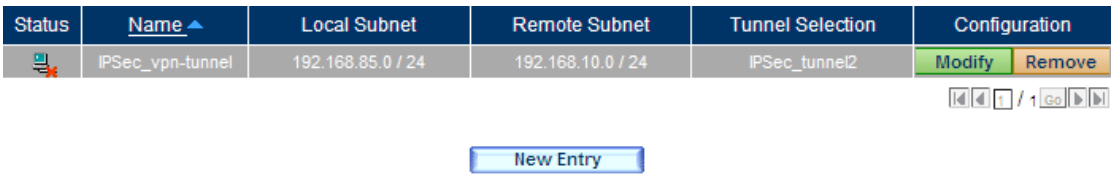


Figure 11-42 VPN Trunk Created

Step 11. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-43**）

- Select the defined Trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-44**）

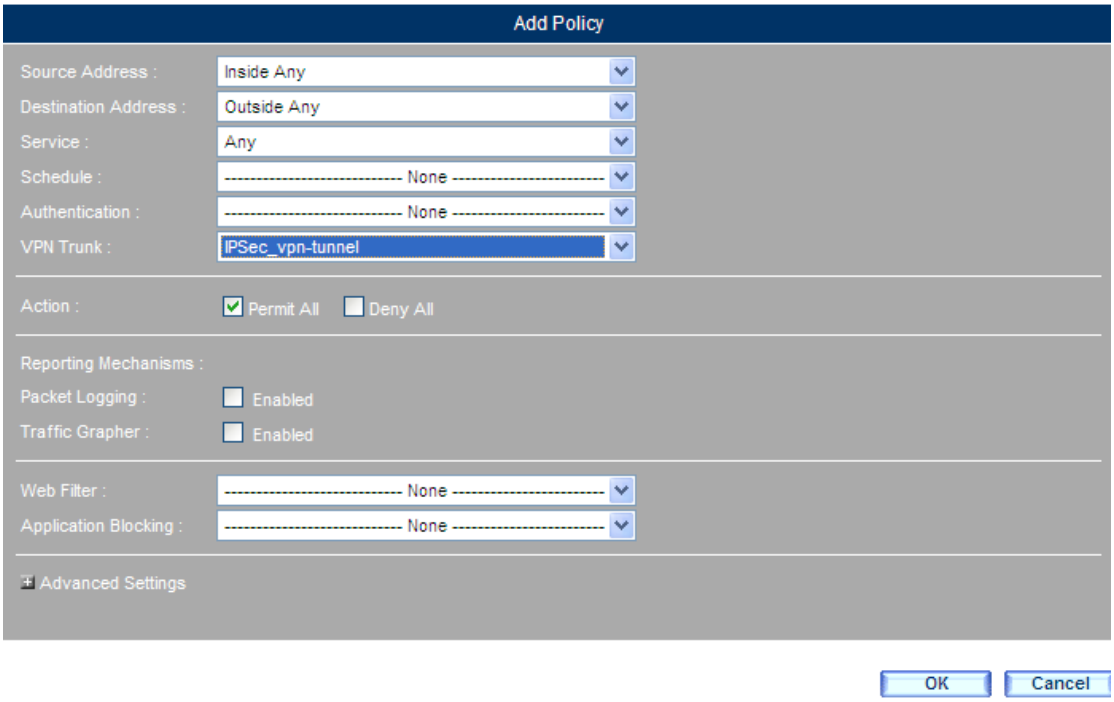


Figure 11-43 Using VPN Trunk in an Outgoing Policy

Figure 11-44 An Outgoing Policy with VPN Trunk

Step 12. Under **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-45**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-46**）

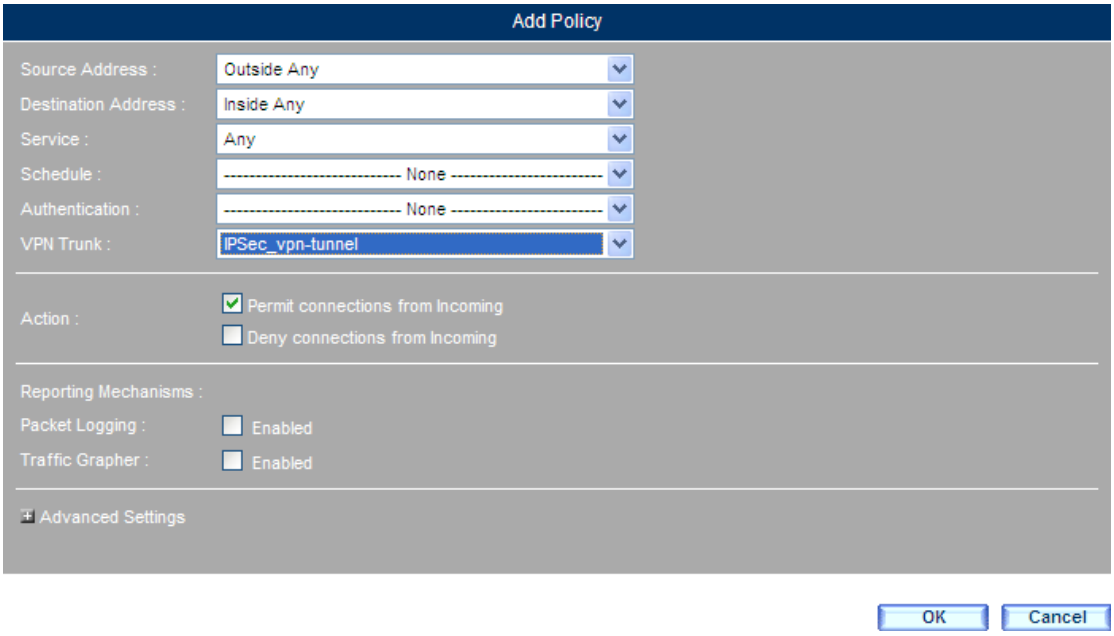


Figure 11-45 Creating an Incoming Policy with VPN Trunk

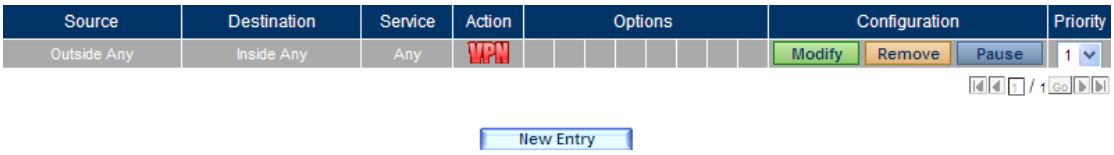


Figure 11-46 An Incoming Policy with VPN Trunk

Step 13. Settings completed.（Figure 11-47）

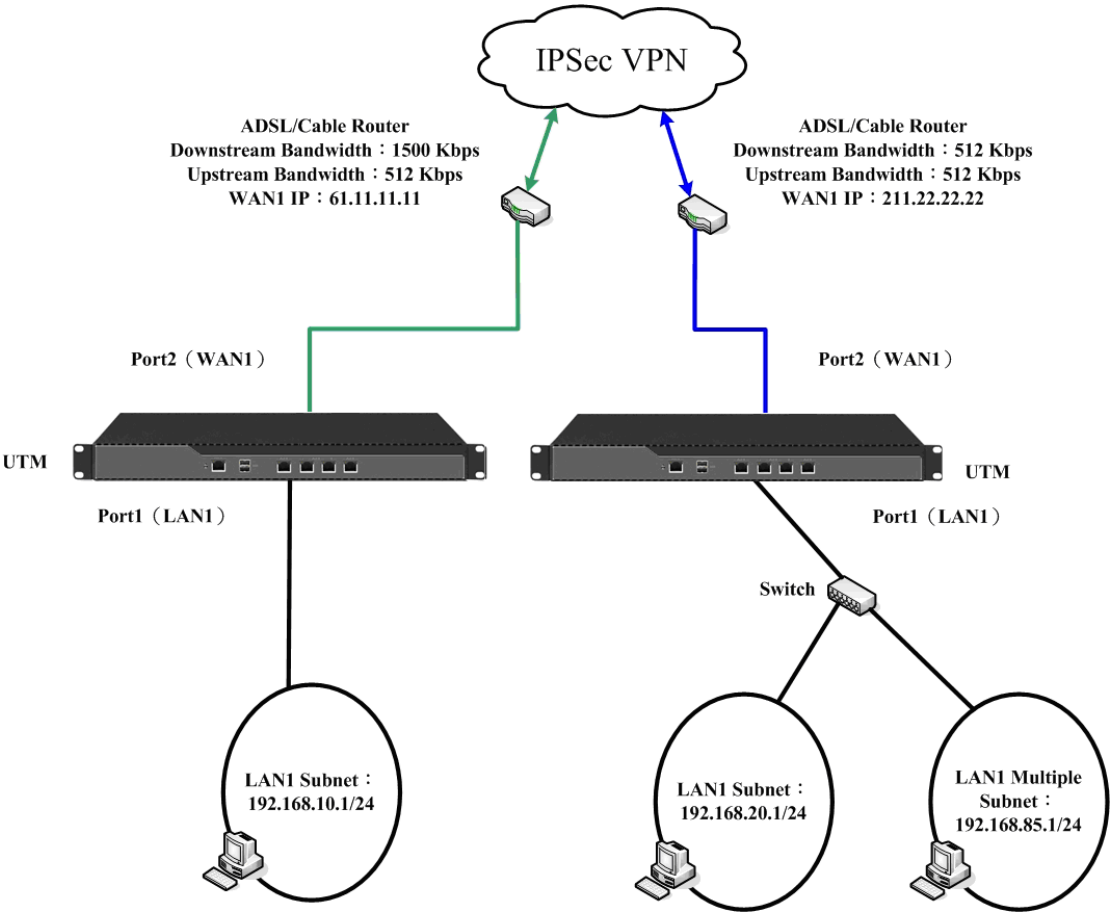


Figure 11-47 Deployment of IPSec VPN

11.1.2 Creating an IPSec VPN Connection under Windows

2000 by a CS-2001 Device

Prerequisite Setup (Note: IP addresses used as examples only)

A Company uses a CS-2001 device:
Configure Port1 as LAN1(192.168.10.1). IP address range:192.168.10.x/24
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote to access the Internet.

B Company uses a PC running Windows 2000:
IP address: 211.22.22.22.

This example is to establish VPN connection between A Company and B Company.

For A Company, set as below:

Step 1. Under **Policy Object** > **VPN** > **IPSec Autokey**, click **New Entry**.（**Figure 11-48**）

Figure 11-48 IPSec Autokey Screen

Step 2. Enter ipsec1 in the **Name** field and then select Port2 (WAN1) for **WAN Interface**.（**Figure 11-49**）

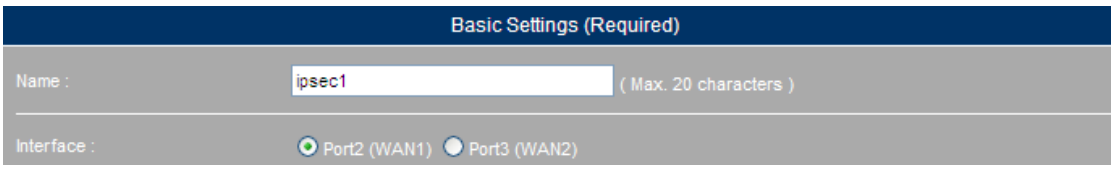


Figure 11-49 Configuring the Name and the WAN Interface for the IPSec

Step 3. For Remote, select **Remote Gateway or Client—Dynamic IP**.（**Figure**

11-50）

Figure 11-50 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of Pre-Shared Key String is 103 characters.)（Figure 11-51）

Figure 11-51 Authentication Method Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “Group 2” for **Group**.（Figure 11-52）

Figure 11-52 ISAKMP Algorithm Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm.**（Figure 11-53）

Figure 11-53 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.（Figure 11-54）

Figure 11-54 Advanced Settings of IPSec Autokey

Step 8. Settings completed.（**Figure 11-55**）

Figure 11-55 IPSec Autokey Settings Completed

Step 9. Under **Policy Object** > **VPN** > **Trunk**, set as below:（**Figure 11-56**）

- **Name**: Type a name.
- **Local Settings**: Select “LAN”. **Local IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask**.
- **Remote Settings**: Select **Remote Client**.
- **Tunnel**: Select “ipsec1” and then add it to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click OK.（**Figure 11-57**）

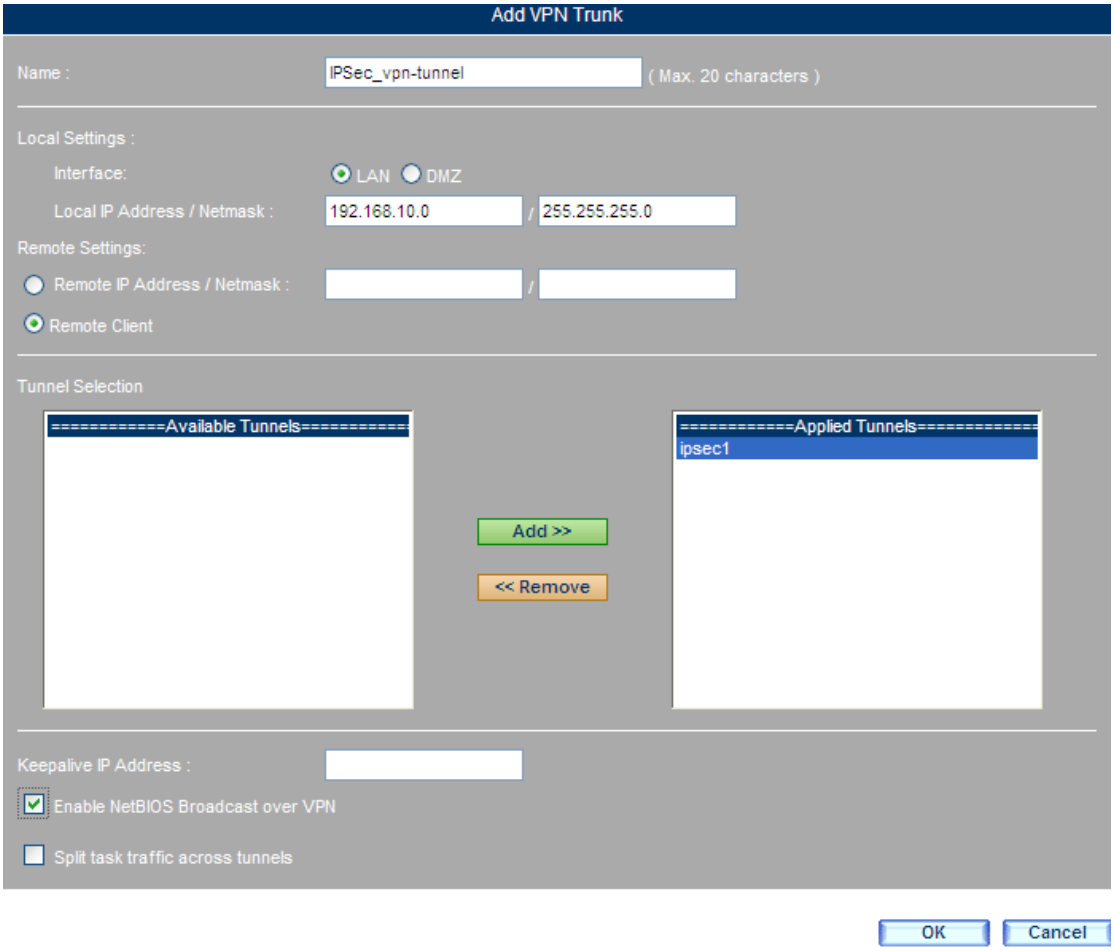


Figure 11-56 VPN Trunk Settings

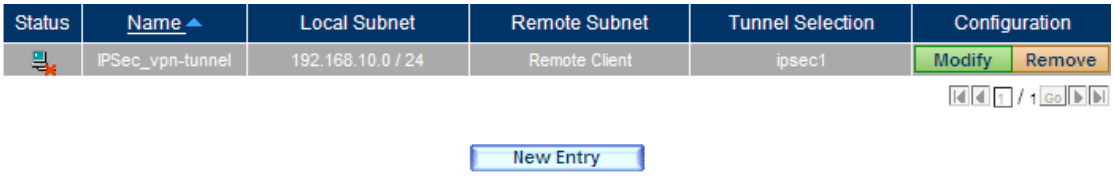


Figure 11-57 VPN Trunk Created

Step 10. Under **Policy** > **Outgoing**, set as below:（**Figure 11-58**）

- Select the defined trunk for **VPN Trunk**.
- Click **OK**.（**Figure 11-59**）

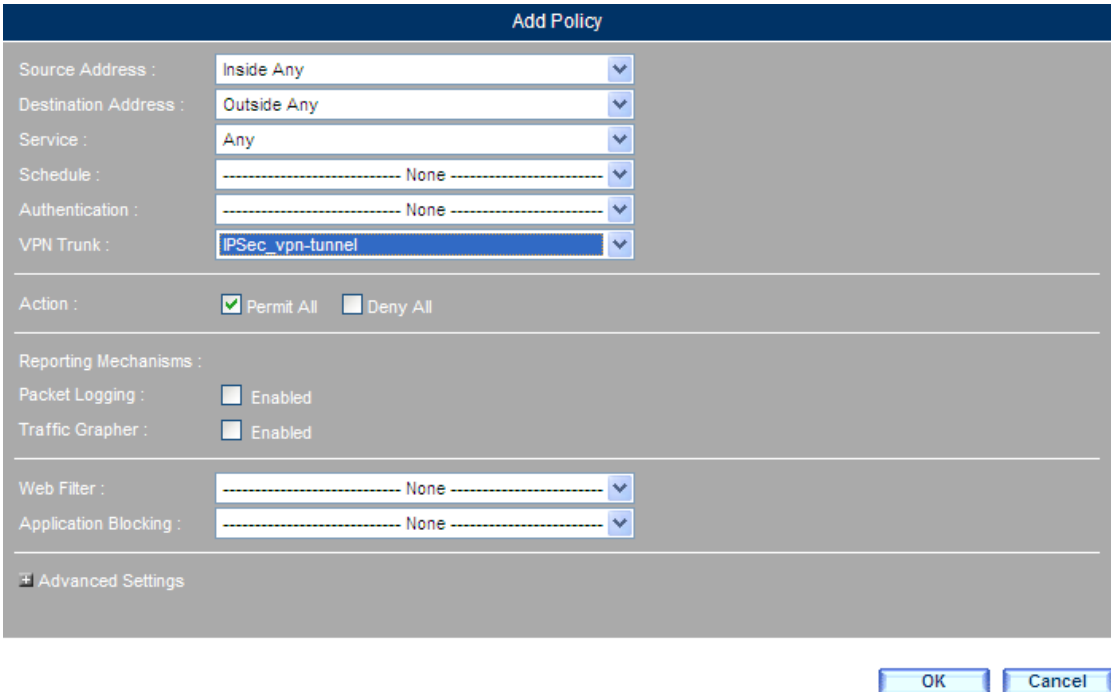


Figure 11-58 Creating an Outgoing Policy with VPN Trunk

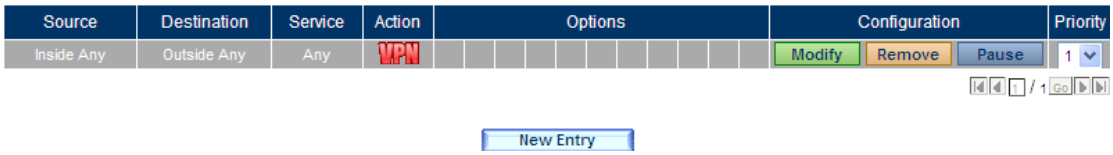


Figure 11-59 Policy Completed

Step 11. Under **Policy** > **Incoming**, set as below:（**Figure 11-60**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-61**）

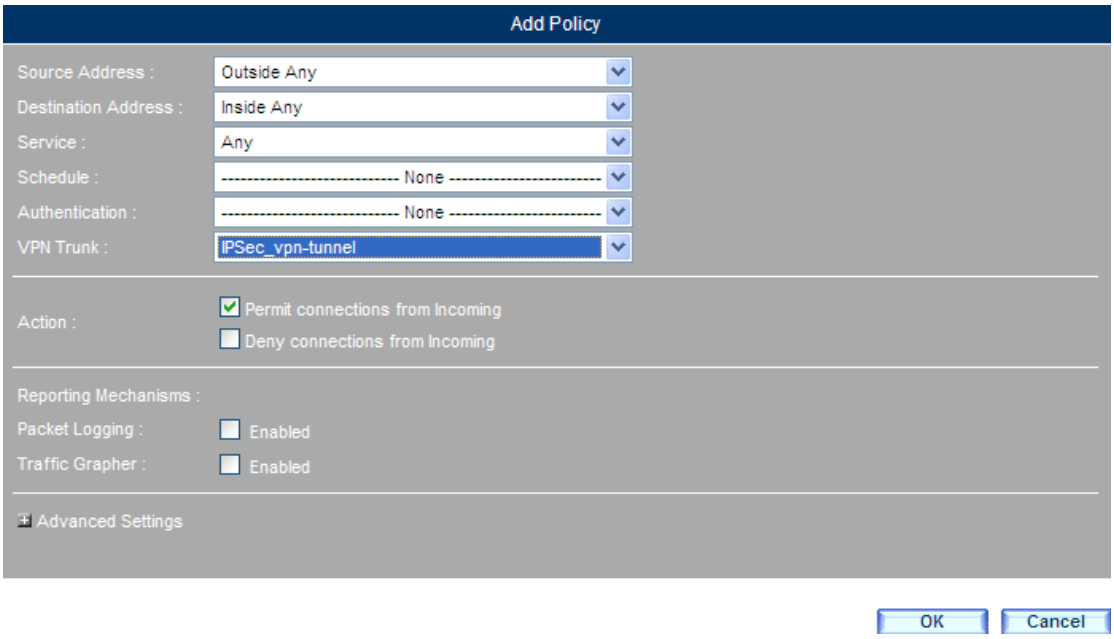


Figure 11-60 Creating an Incoming Policy with VPN Trunk

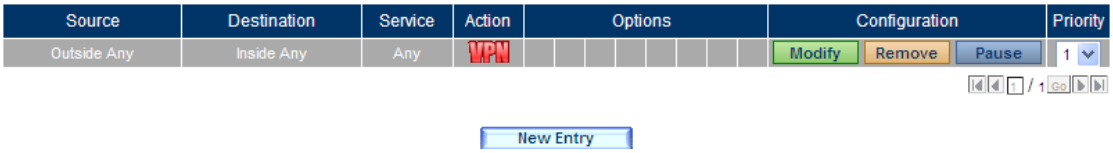


Figure 11-61 Policy Completed

For B Company, set as below:

Step 1. Select **Start** > **Run** on the **Start** menu in Windows 2000.（**Figure 11-62**）

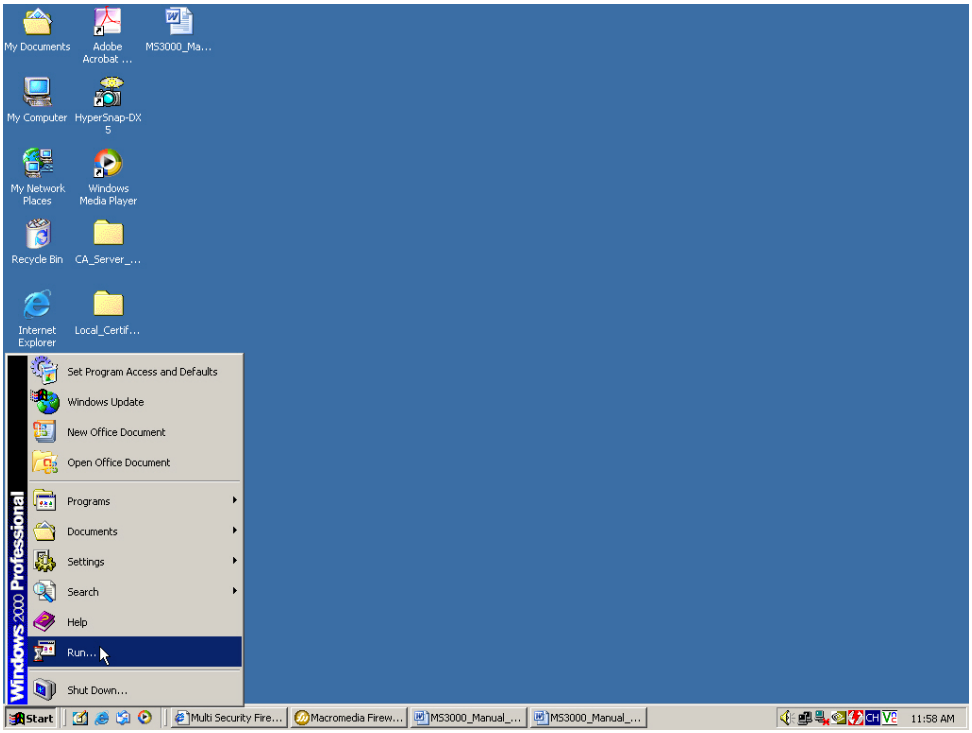


Figure 11-62 Selecting "Run…" on the Start Menu

Step 2. In the **Open** field of the **Run** window, type "mmc".（**Figure 11-63**）

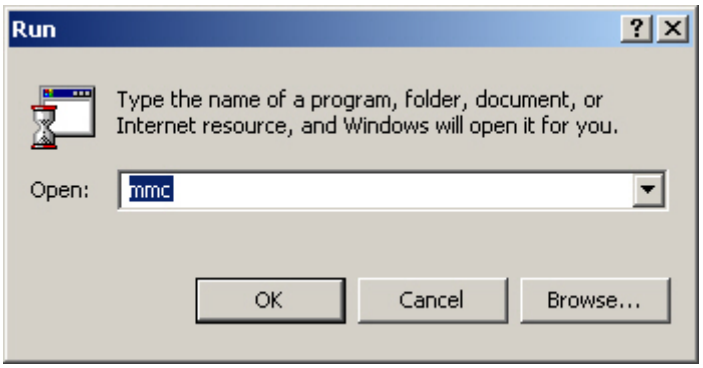


Figure 11-63 Typing "mmc" to Lunch the Microsoft Management Console Application

Step 3. In the **Console 1** window, click **Console** on the menu bar, and then click **Add/Remove Snap-in.**（**Figure 11-64**）

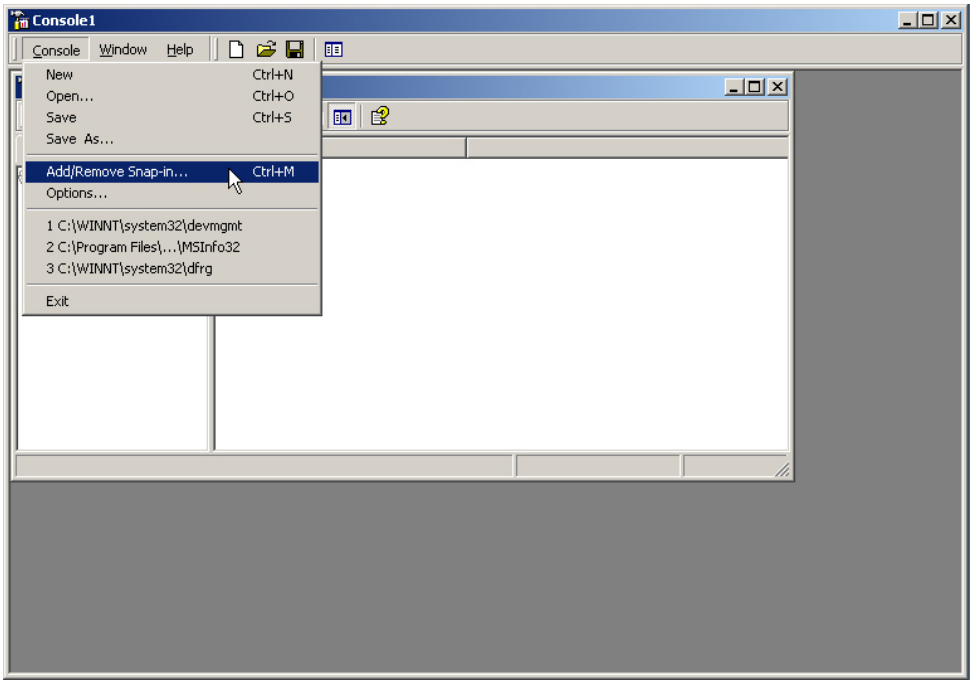


Figure 11-64 Selecting "Add / Remove Snap-in" on the Console Menu

Step 4. In the **Add / Remove Snap-in** window, click **Add**. Then, in the **Add Standalone Snap-ins** window, select **IP Security Policy Management** and add it.（**Figure 11-65**）

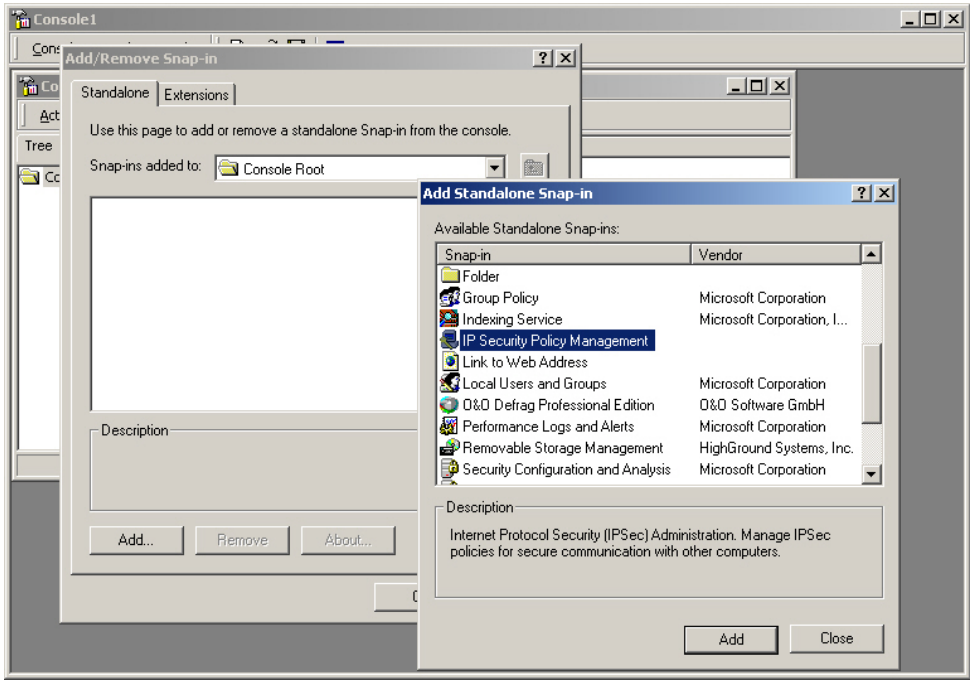


Figure 11-65 Adding the "IP Security Policy Management"

Step 5. Select **Local Computer**, and then click **Finish**.（**Figure 11-66**）

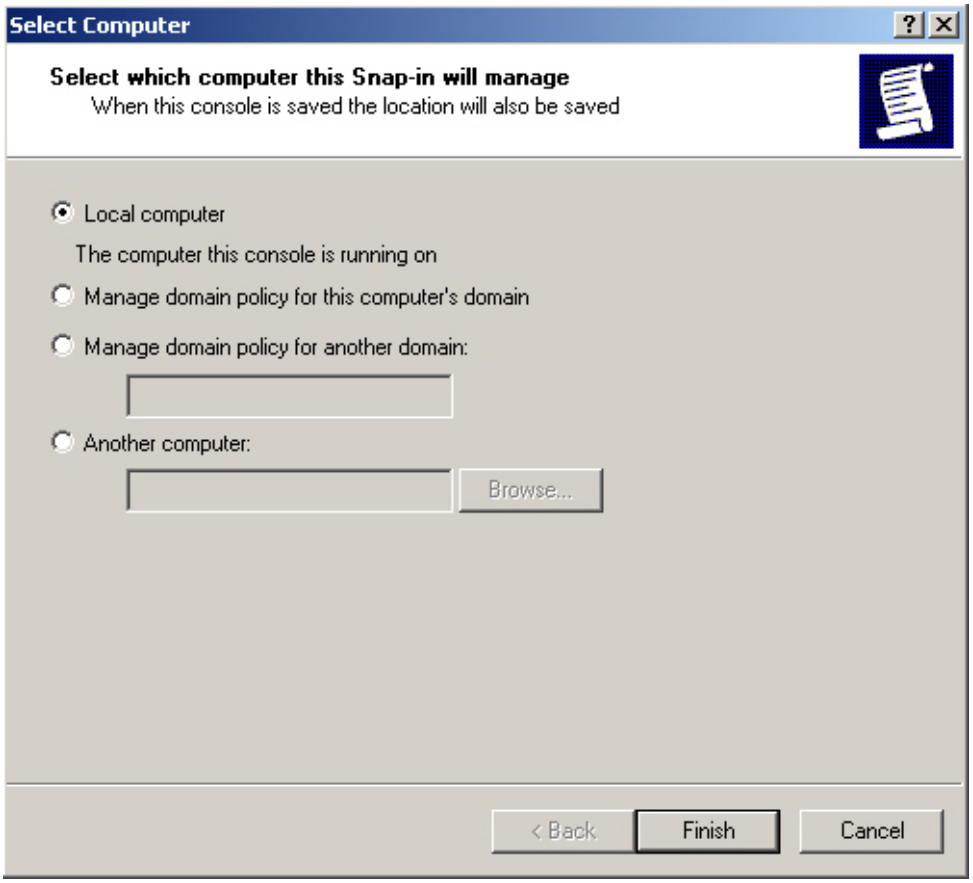


Figure 11-66 Selecting Local Computer

Step 6. Settings completed.（**Figure 11-67**）

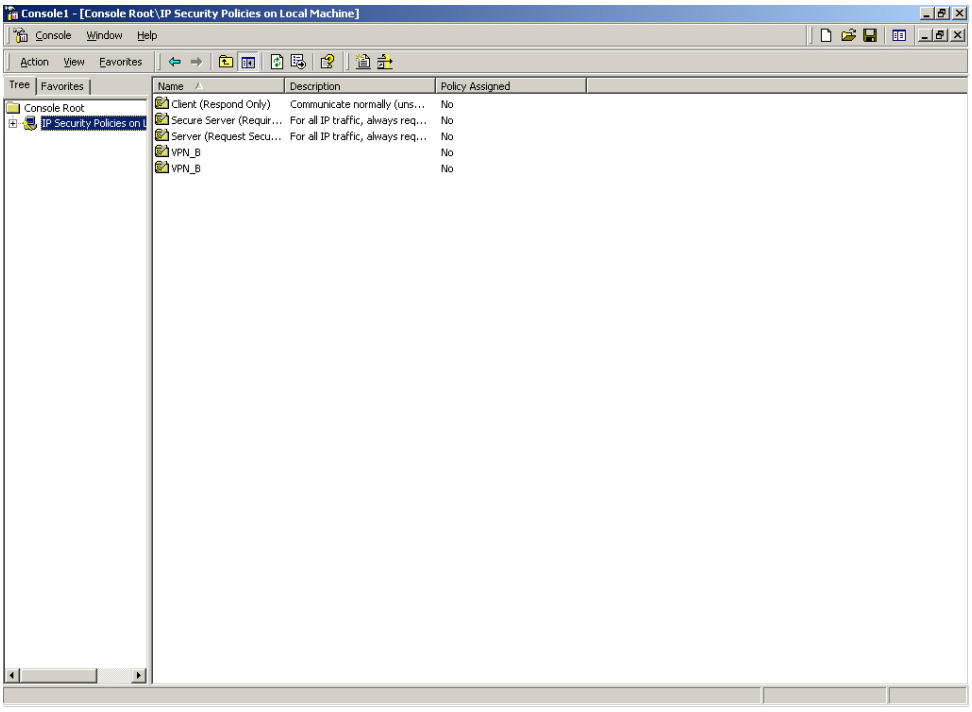


Figure 11-67 Settings Completed

Step 7. Right-click the **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**.（Figure 11-68）

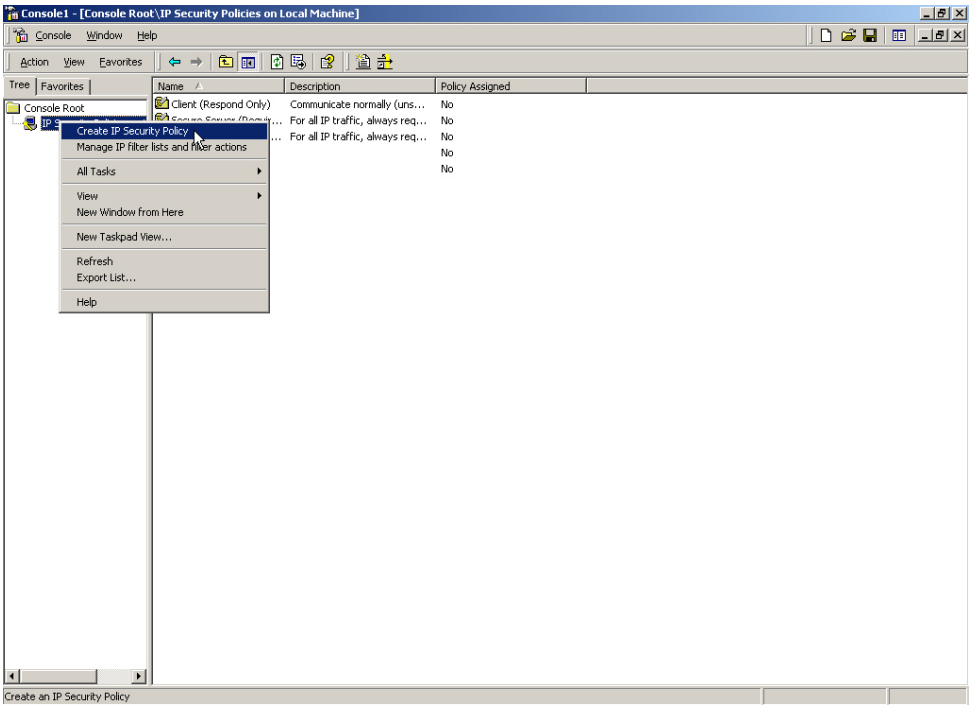


Figure 11-68 Creating an IP Security Policy

Step 8. Click **Next**.（Figure 11-69）

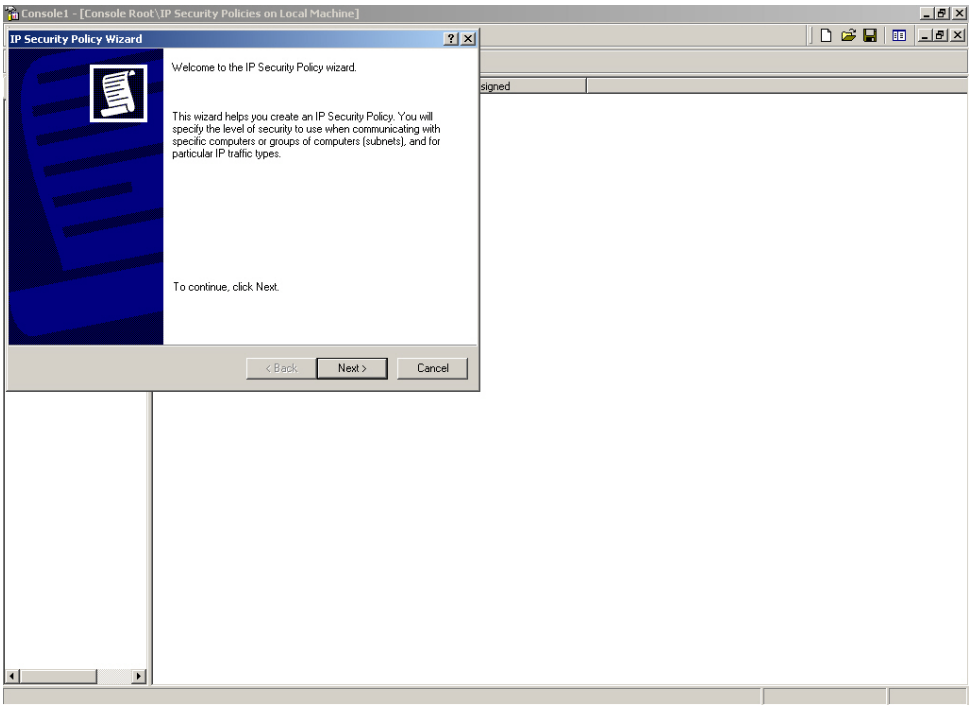


Figure 11-69 Security Policy Wizard

Step 9. Type the **Name** and **Description** and then click **Next**. (Figure 11-70)

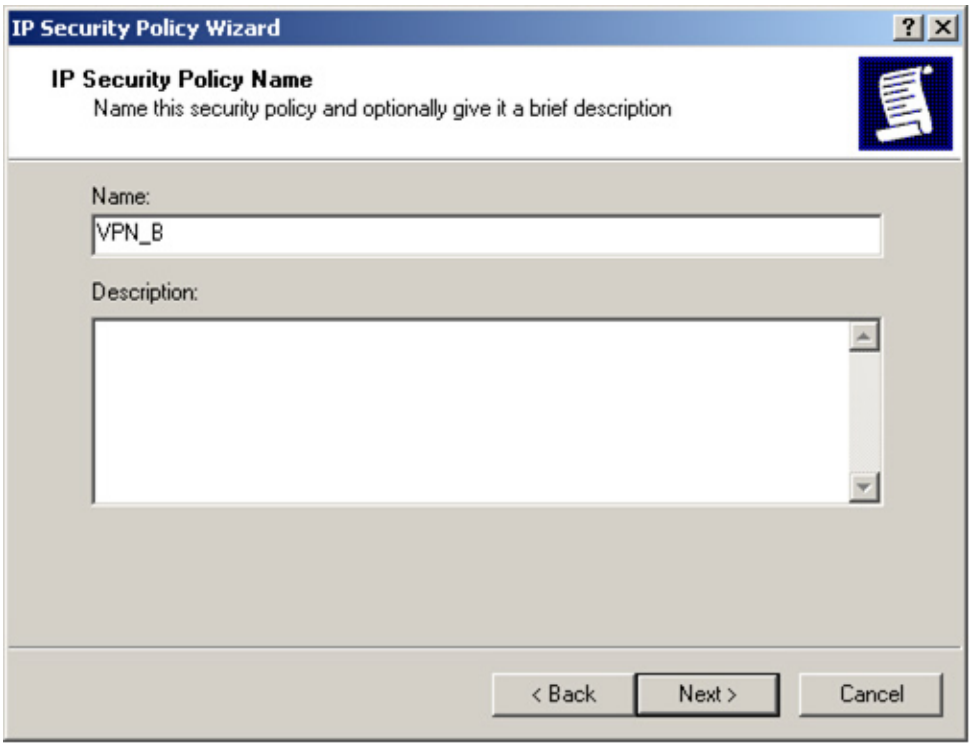


Figure 11-70 Name and Description Settings

Step 10. Disable **Activate the default response rule** and then click **Next.** (Figure 11-71)

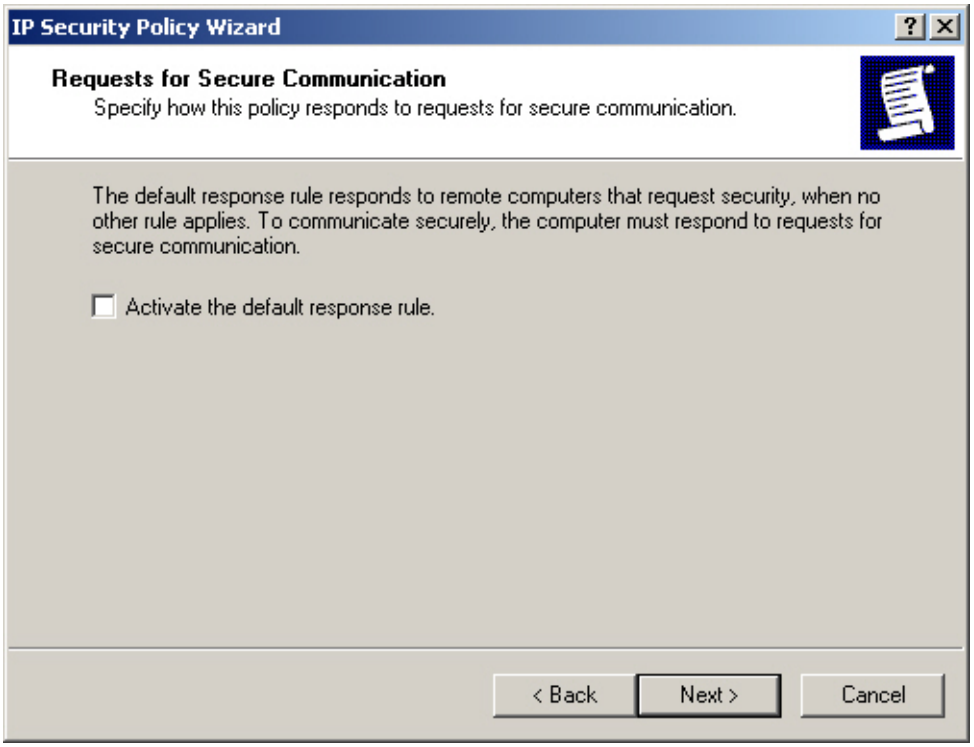


Figure 11-71 Disable the "Activate the Default Response Rule"

Step 11. In the **IP Security Policy Wizard** window, tick **Edit properties** and click **Finish**. (**Figure 11-72**)

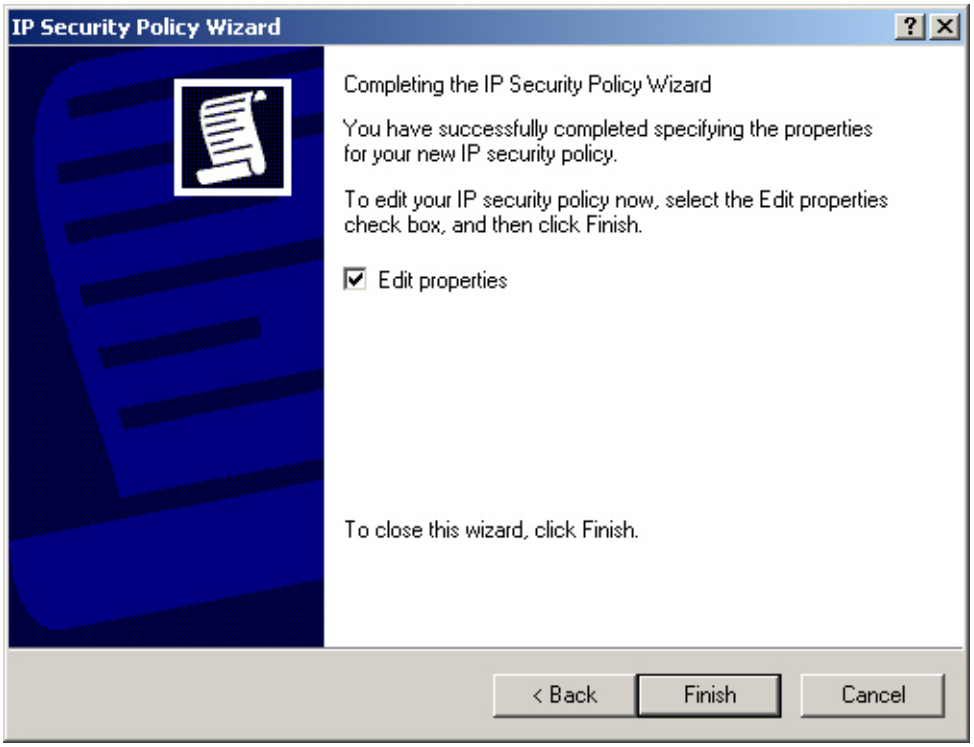


Figure 11-72 Settings Completed

Step 12. In the **VPN_B Properties** window, disable **Use Add Wizard** and then click **Add**. (**Figure 11-73**)

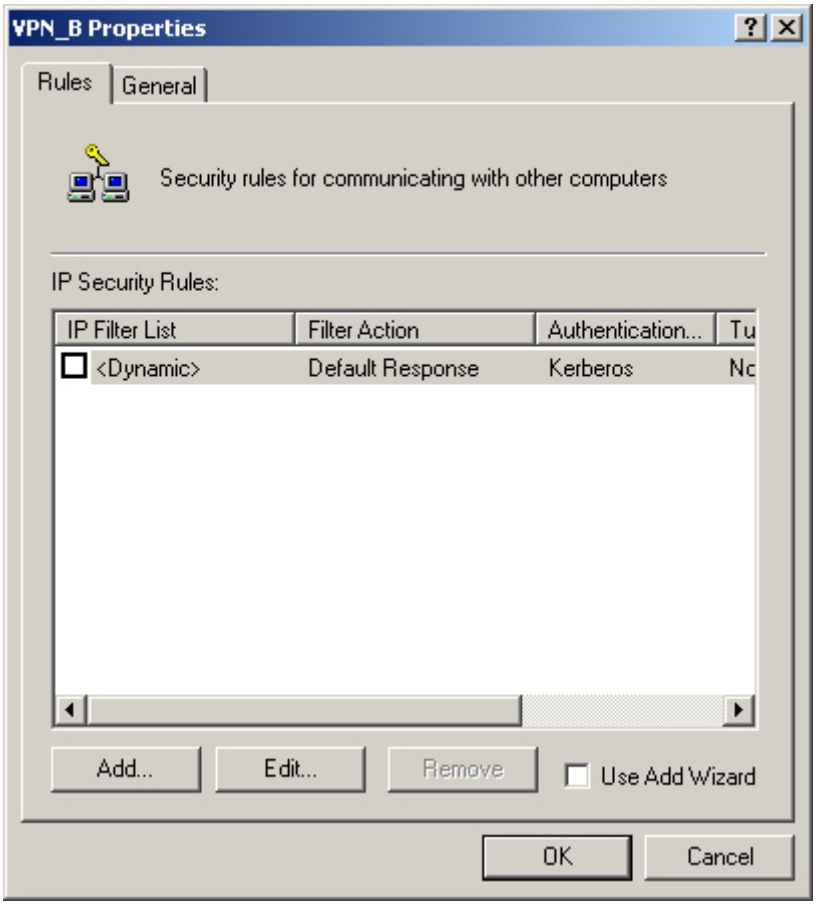


Figure 11-73 VPN_B Properties

Step 13. In the **New Rule Properties** window, click **Add.**（**Figure 11-74**）

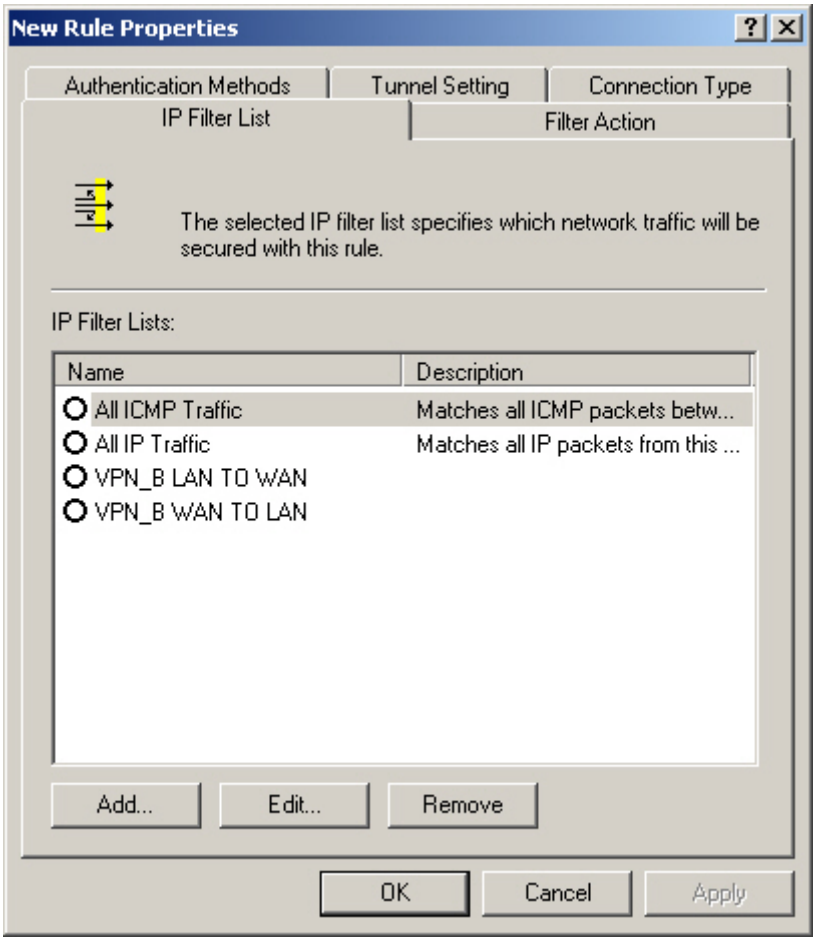


Figure 11-74 New Rule Properties

Step 14. In the **IP Filter List** window, disable **Use Add Wizard**. Change the **Name** into “VPN_B WAN TO LAN” and then click **Add**.（**Figure 11-75**）

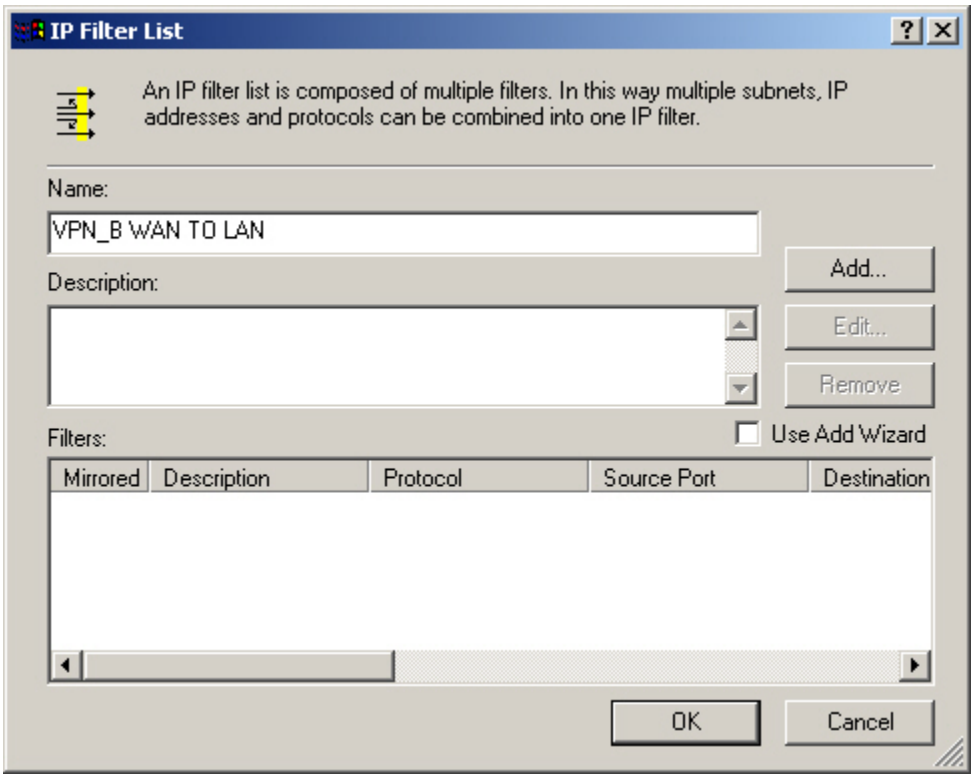


Figure 11-75 Adding an IP Filter

Step 15. In the **Filter Properties** window, select “A specific IP Address” for **Source address**, and then apply B Company’s WAN IP address “211.22.22.22” and subnet mask “255.255.255.255” to the fields. After that, select “A specific IP Subnet” for **Destination address**, and then type “192.168.10.0” as A Company‘s subnet address, and “255.255.255.0” as subnet mask. Note: Do not tick “Mirrored. Also match packets with the exact opposite source and destination addresses”.（**Figure 11-76**）

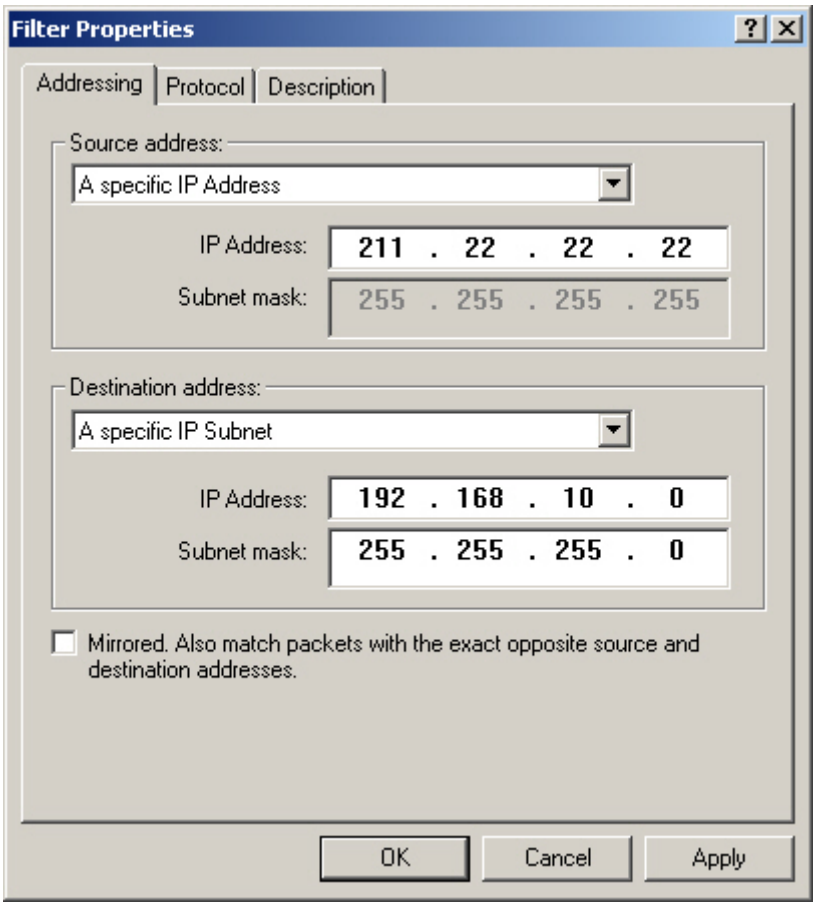


Figure 11-76 Filter Properties Settings

Step 16. Settings completed.（**Figure 11-77**）

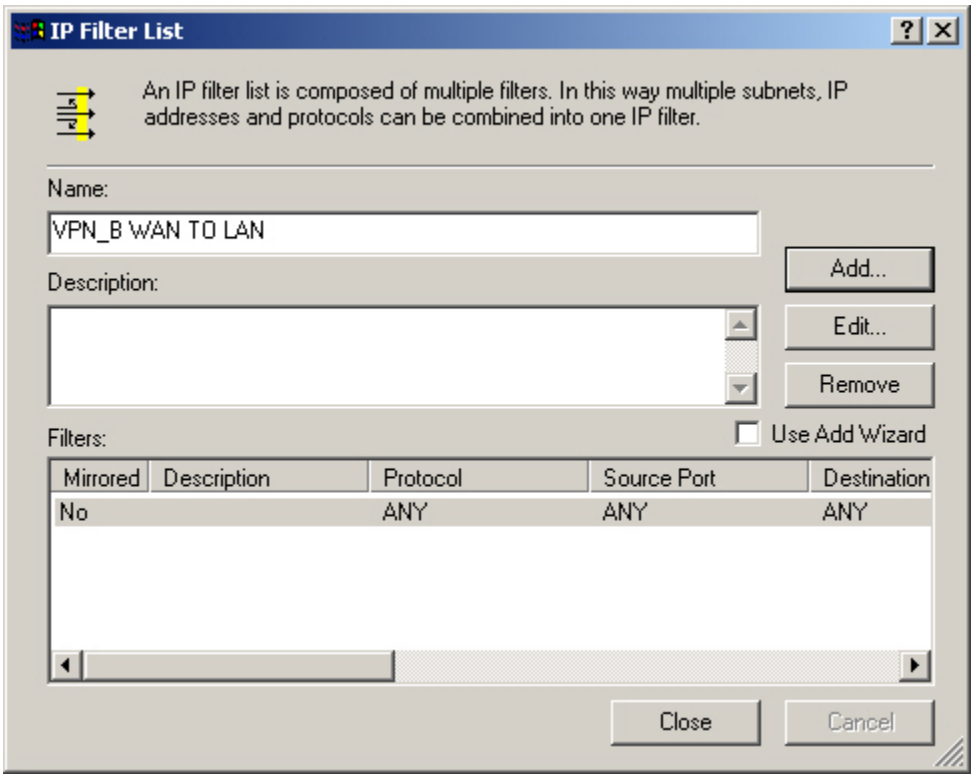


Figure 11-77 IP Filter Added

Step 17. In the **New Rule Properties** window, click **Filter Action** tab and then tick **Require Security**. Next, click **Edit**.（**Figure 11-78**）

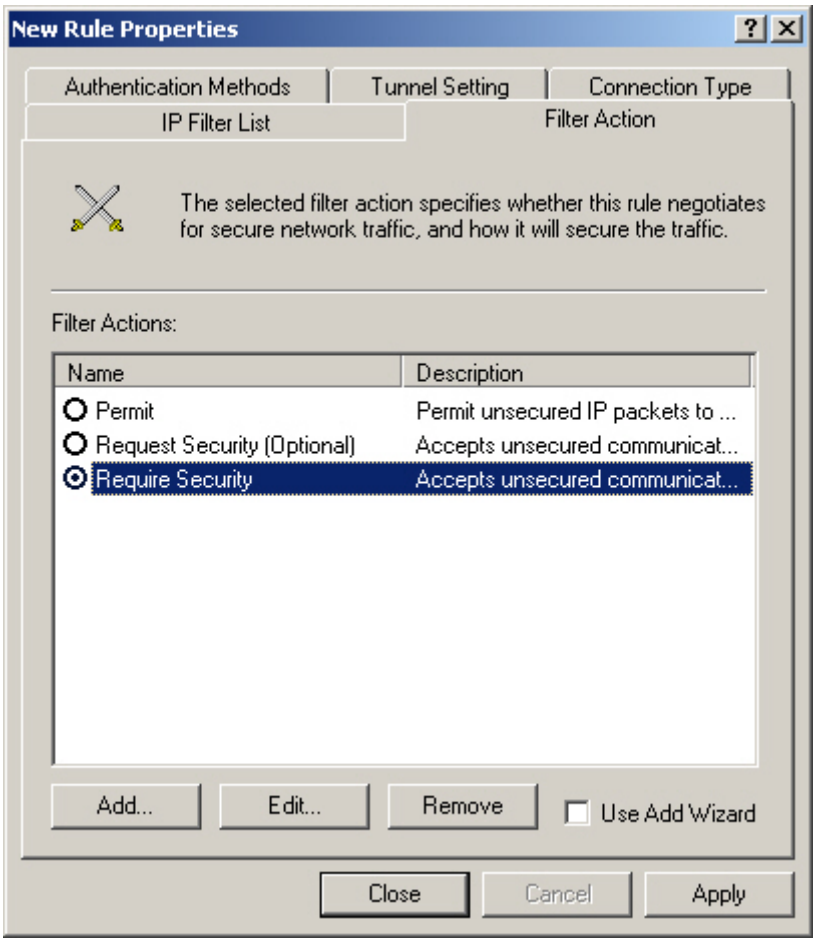


Figure 11-78 Selecting Filter Action

Step 18. In the **Require Security Properties** window, tick “Session Key Perfect Forward Secrecy” on the bottom.（**Figure 11-79**）

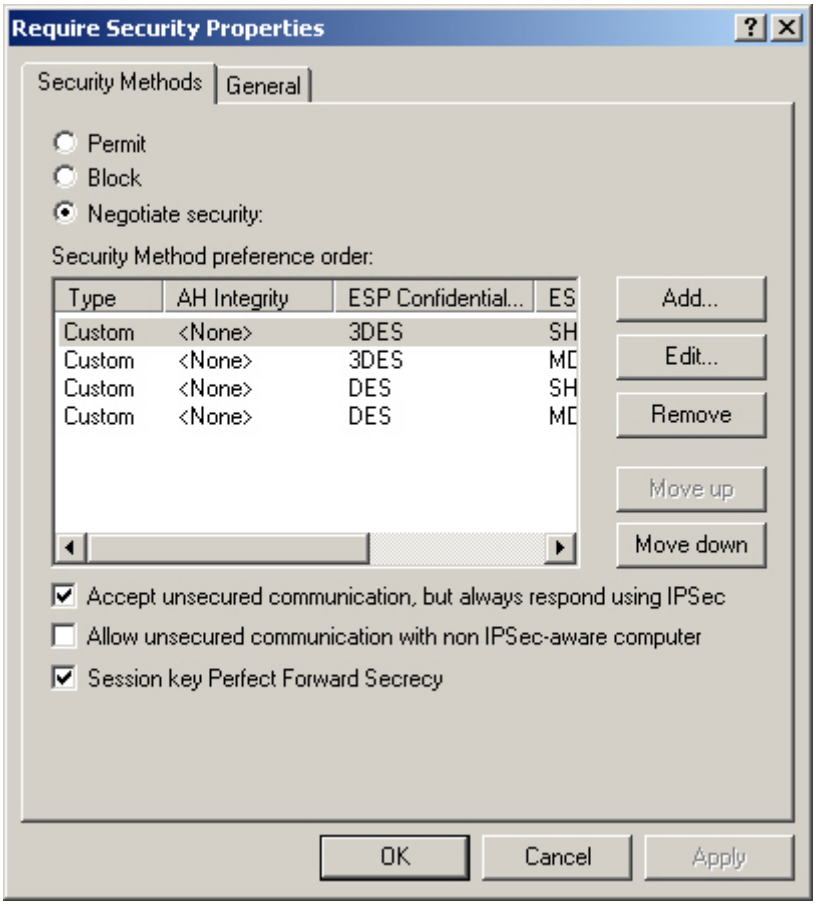


Figure 11-79 Ticking the "Session Key Perfect Forward Secrecy"

Step 19. Select the security method (**Custom / None / 3DES / MD5**), and then click **Edit**. (**Figure 11-80**)

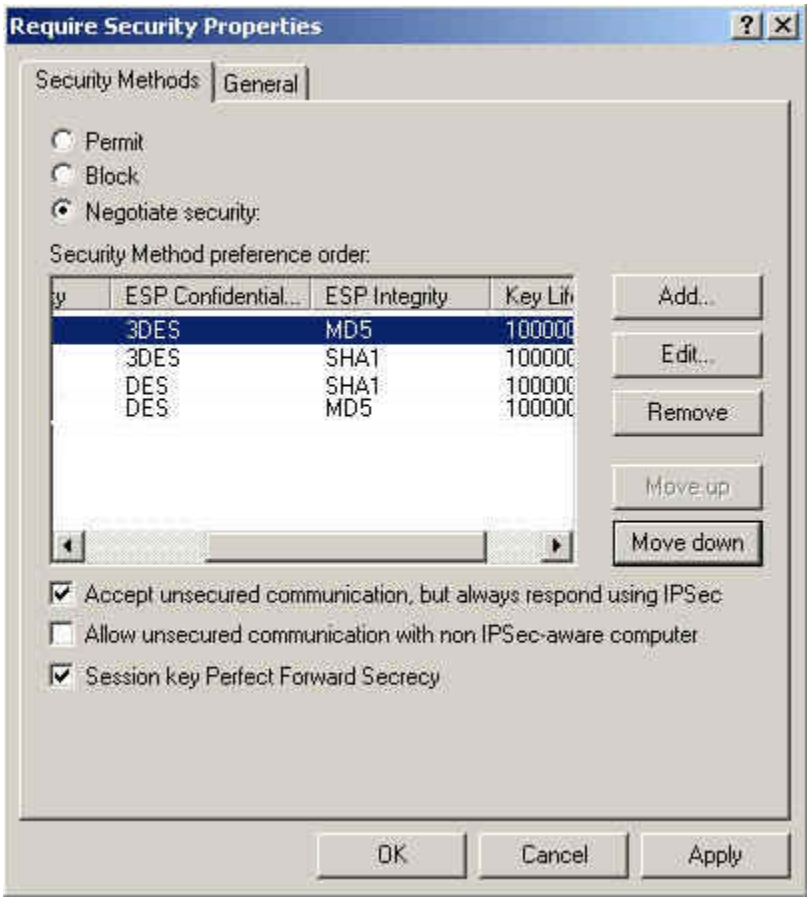


Figure 11-80 Selecting a Security Method to Edit

Step 20. Select **Custom (for expert users)**, and then click **Settings**. (**Figure 11-81**)

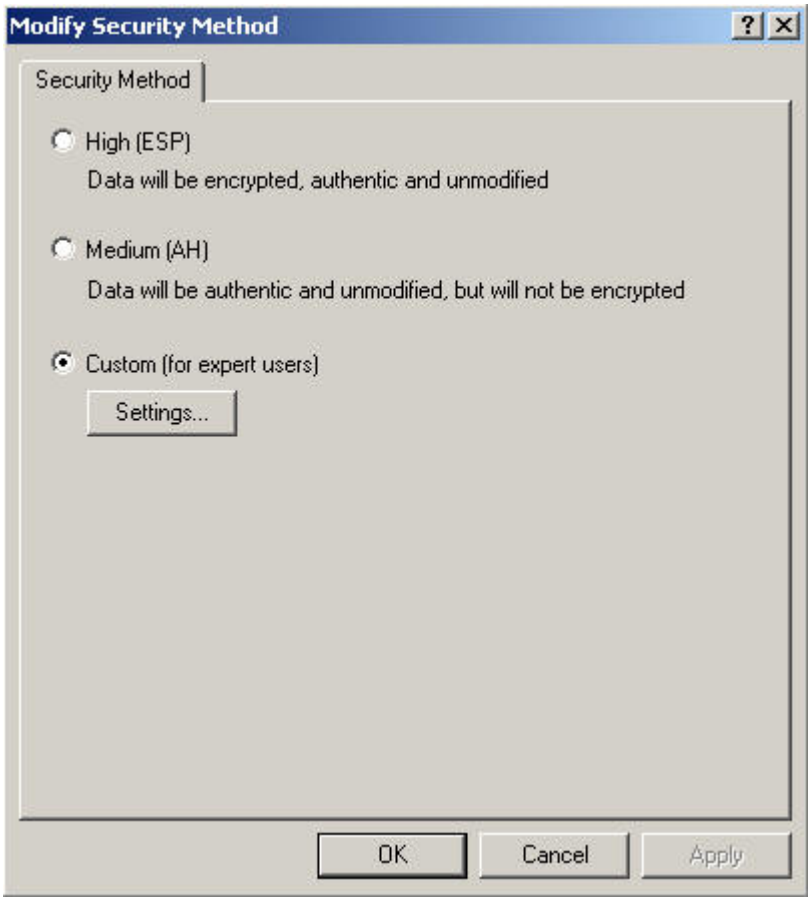


Figure 11-81 Modifying Security Method

Step 21. Tick **Data integrity and encryption**, and select “MD5” for **Integrity algorithm** and “3DES” for **Encryption algorithm**. Tick **Generate a new key every**, and enter “28800” in the seconds field, and then click **OK** to return to the **New Rule Properties** window.（**Figure 11-82**）

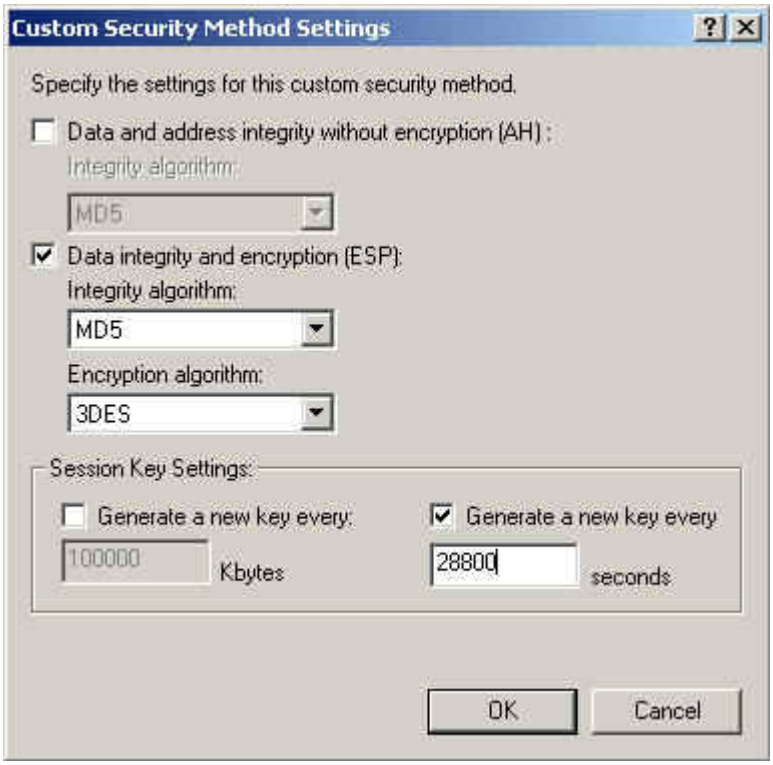


Figure 11-82 Customizing Security Method

Step 22. In the **New Rule Properties** window, click **Connection Type** tab and tick **All network connections**.（**Figure 11-83**）

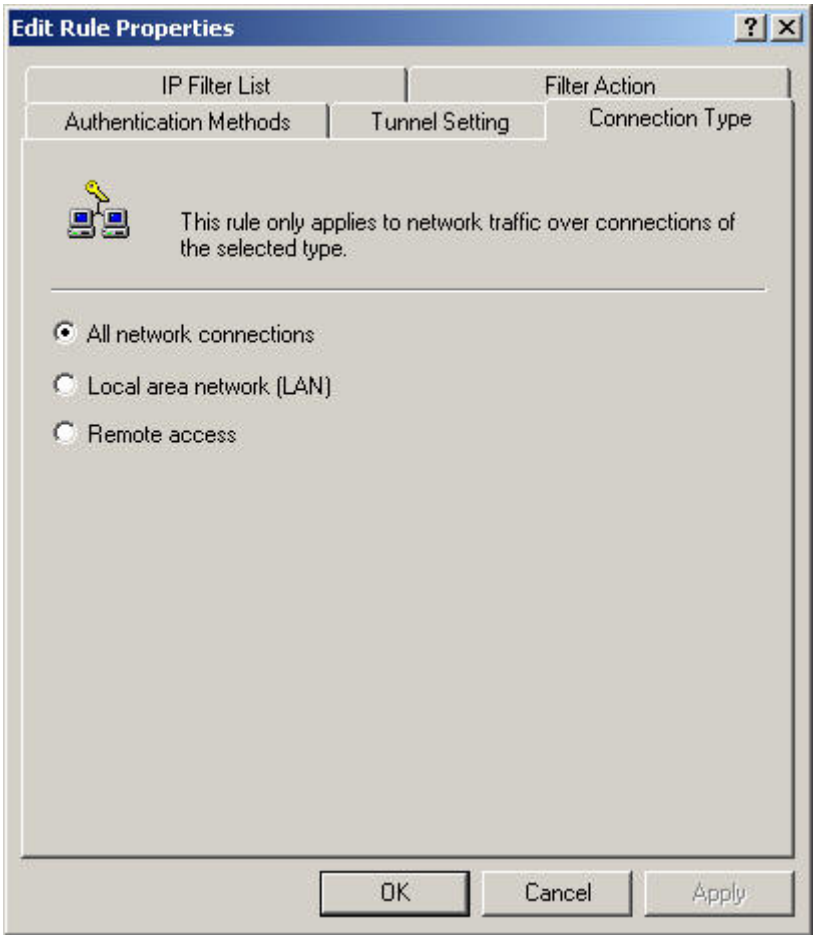


Figure 11-83 Selecting the Connection Type

Step 23. In the **New Rule Properties** window, click **Tunnel Setting tab**. After that, tick **The tunnel endpoint is specified by this IP Address**, and then enter “61.11.11.11” as the WAN IP address of A Company. （**Figure 11-84**）

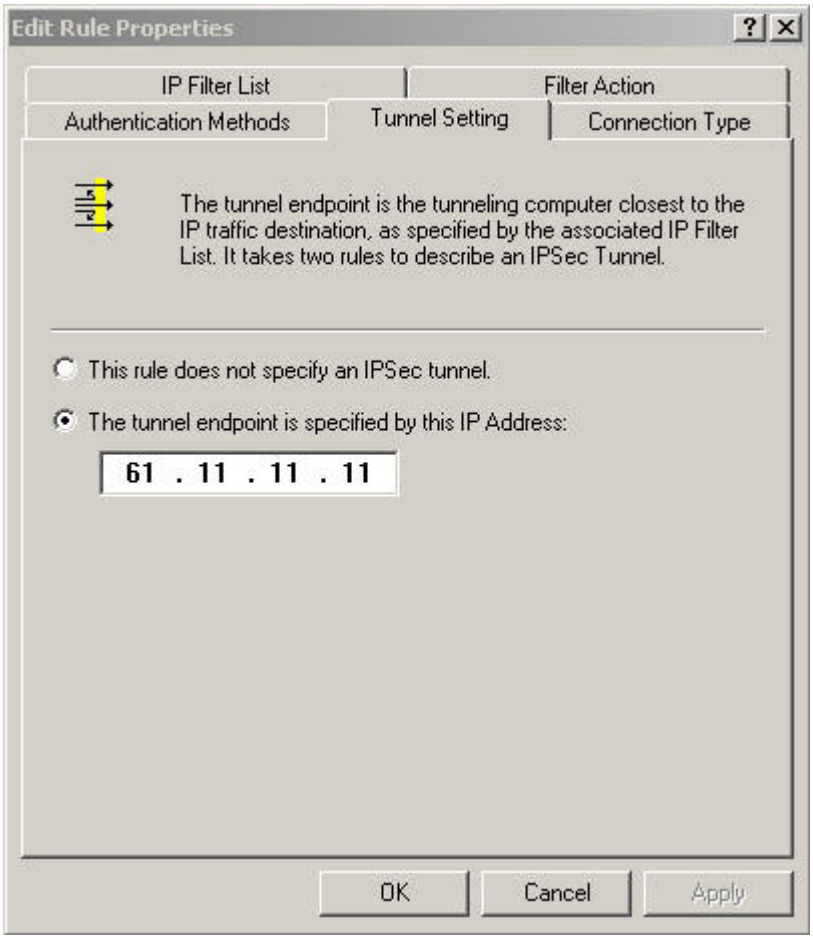


Figure 11-84 Tunnel Setting

Step 24. In the **New Rule Properties** window**,** click **Authentication Methods** tab. Next, select the method “Kerberos” and then click **Edit** on the right. （**Figure 11-85**）

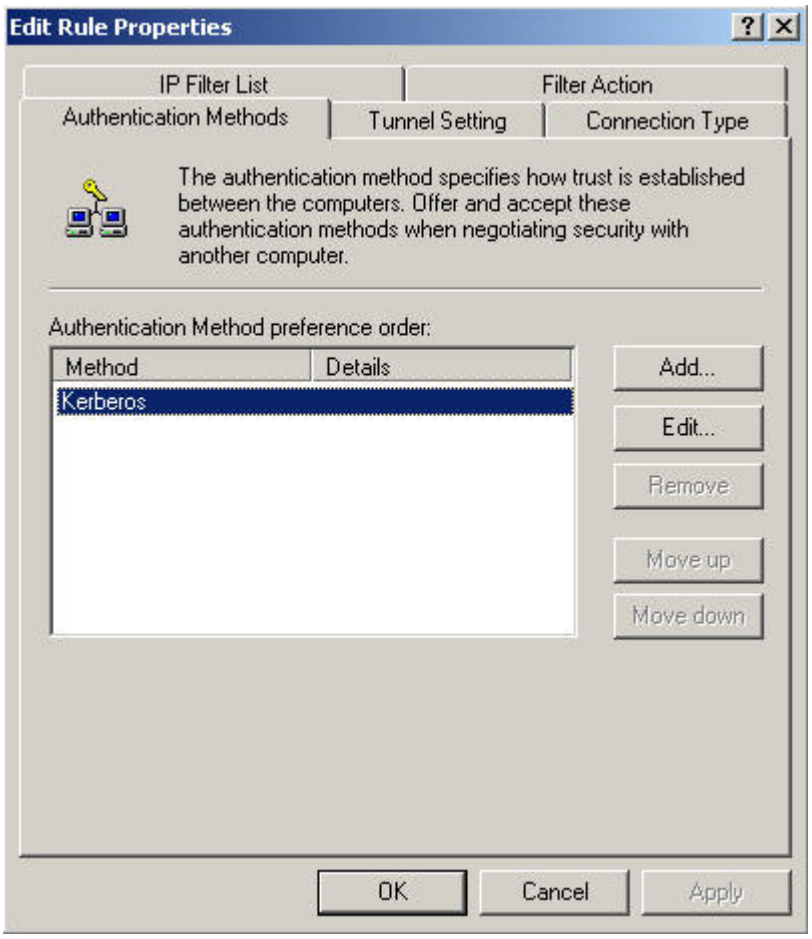


Figure 11-85 Authentication Methods Settings

Step 25. Select **Use this string to protect the key exchange (preshared key)**, and then enter the preshared key “123456789” in the field.（**Figure 11-86**）

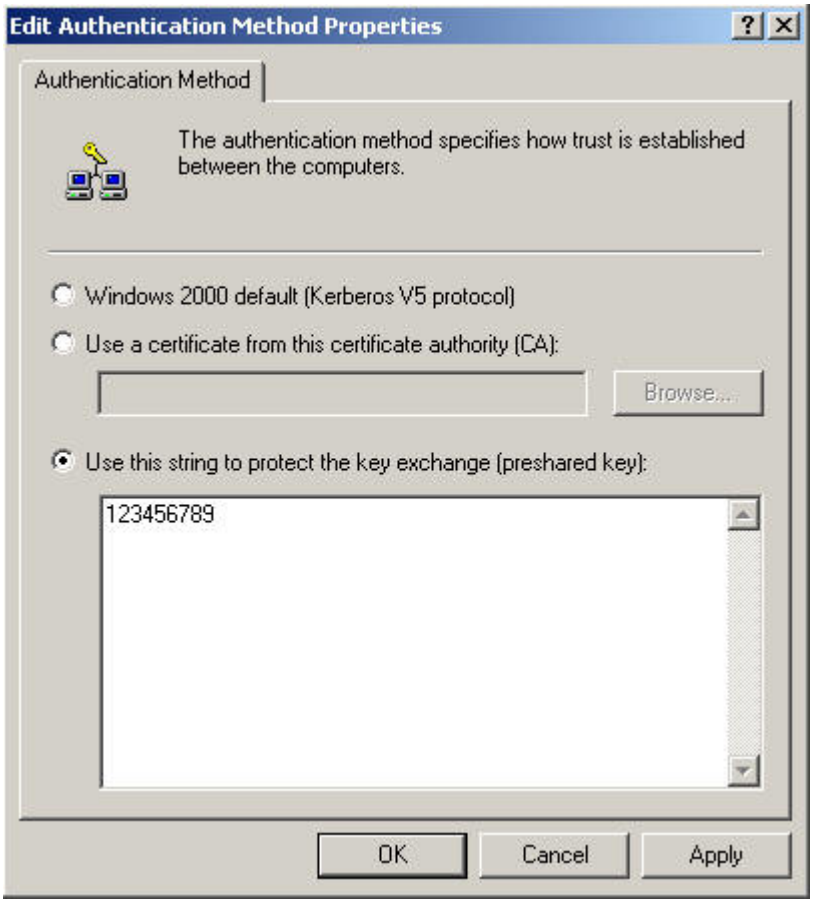


Figure 11-86 Preshared Key Settings

Step 26. Click **Apply**, and then click **Close** to close the window.（**Figure 11-87**）

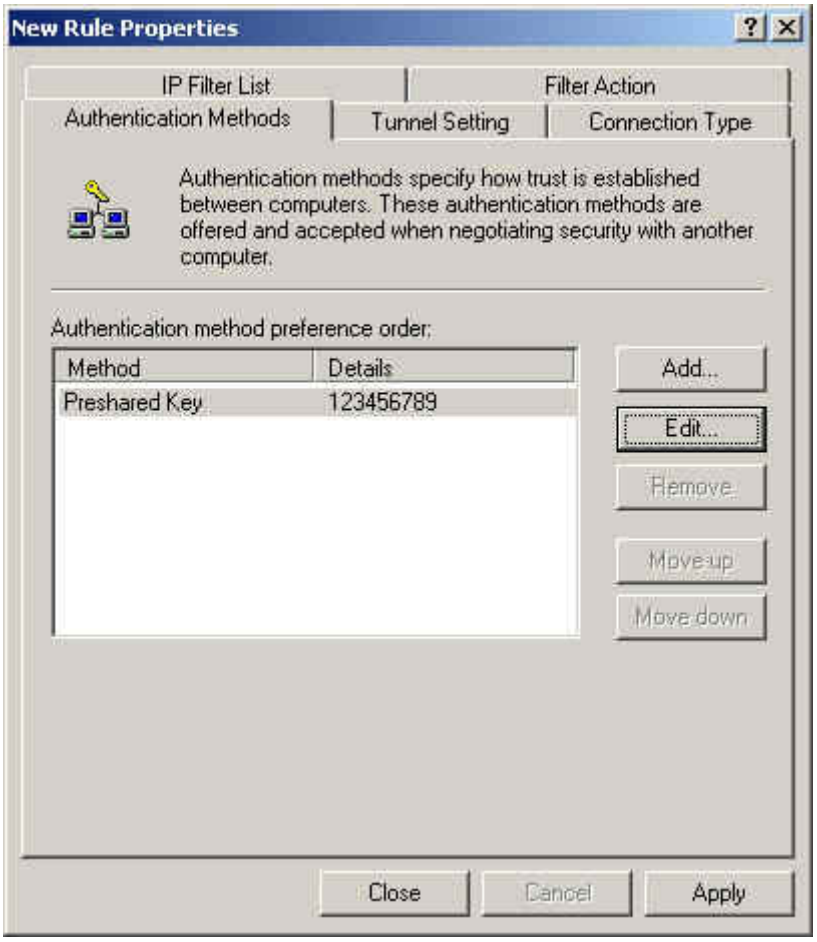


Figure 11-87 Authentication Methods Settings

Step 27. Settings completed. (**Figure 11-88**)

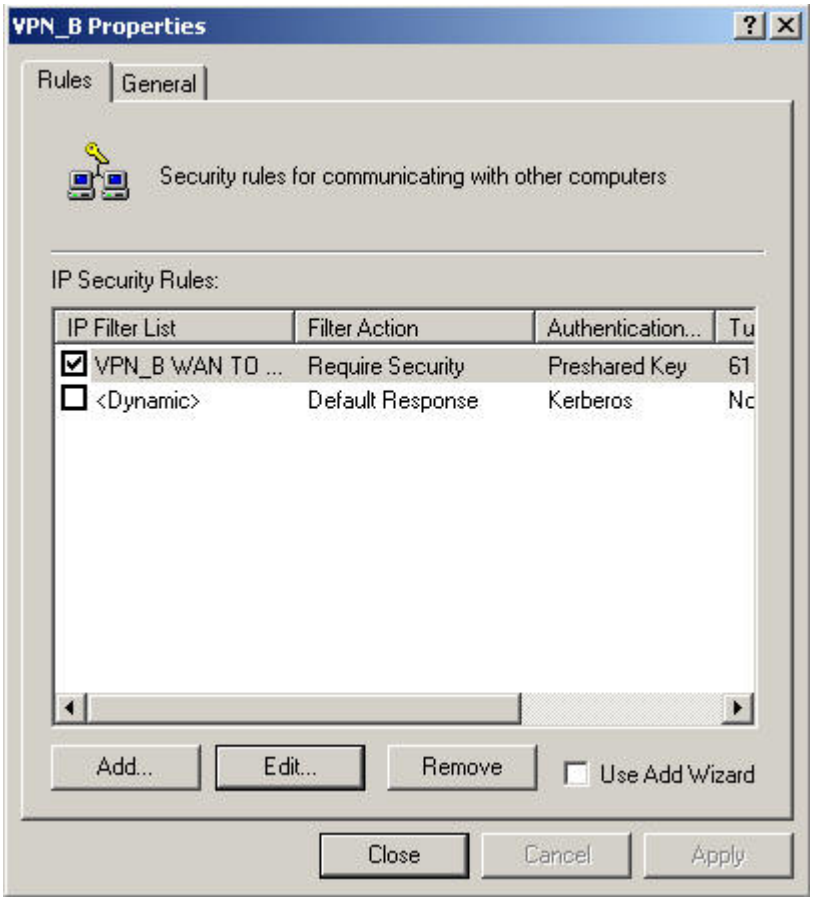


Figure 11-88 Settings Completed

Step 28. In the **VPN_B Properties** window, disable **Use Add Wizard**; click **Add** to create the second IP security rule.（**Figure 11-89**）

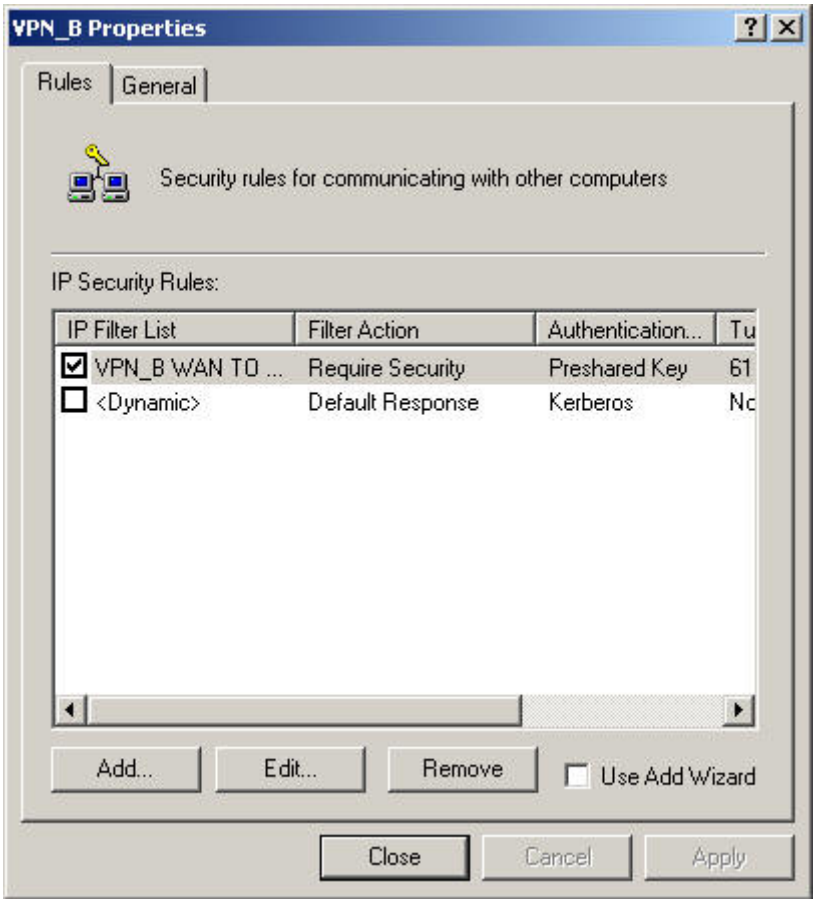


Figure 11-89 VPN_B Properties Settings

Step 29. In the **New Rule Properties** window, click **Add**.（**Figure 11-90**）

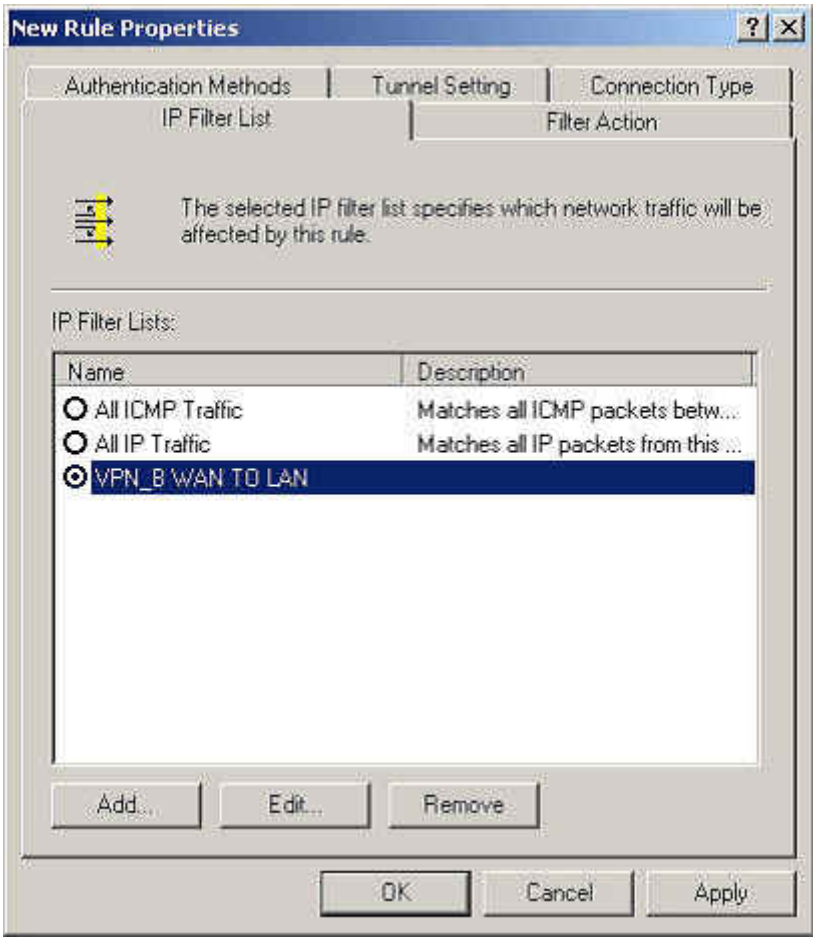


Figure 11-90 Clicking "Add…" to Add an IP Filter

Step 30. In the **IP Filter List** window, disable **Use Add Wizard**. Change the **Name** into “VPN_B LAN TO WAN”, and then click **Add.**（**Figure 11-91**）

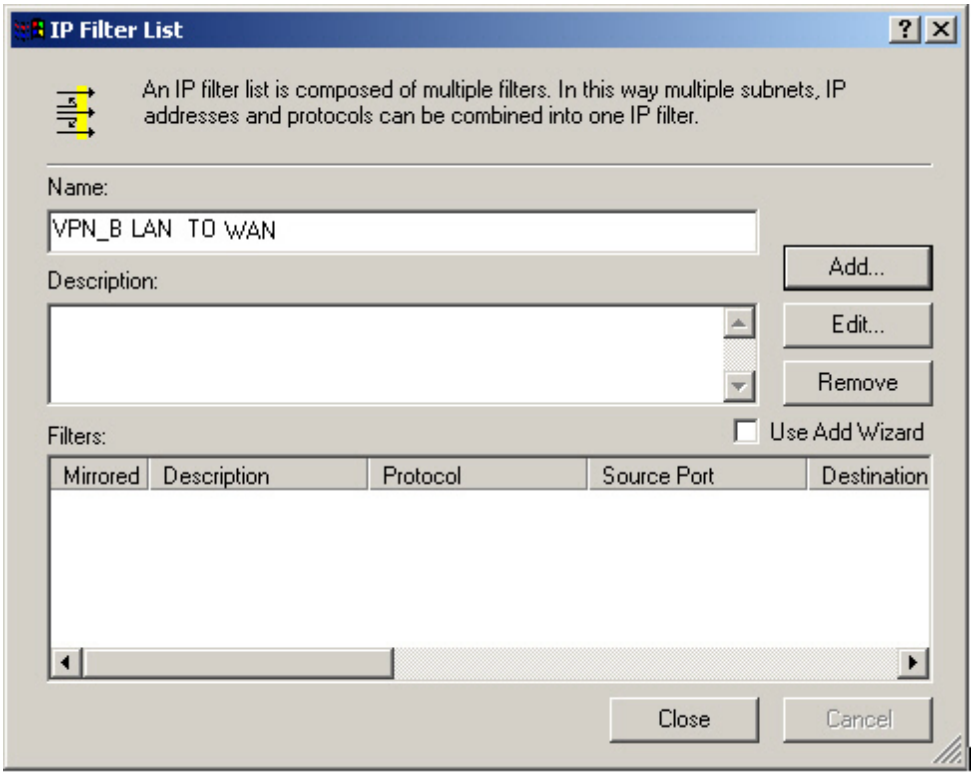


Figure 11-91 Adding an IP Filter

Step 31. In the **Filter Properties** window, select “A specific IP Subnet” for **Source address**, and then type “192.168.10.0” as A Company‘s subnet address and “255.255.255.0” as subnet mask. After that, select “A specific IP Address” for **Destination address**, and then type “211.22.22.22” as B Company‘s WAN IP address and “255.255.255.255” as subnet mask. Note: Do not enable “Mirrored. Also match packets with the exact opposite source and destination addresses”.（**Figure 11-92**）

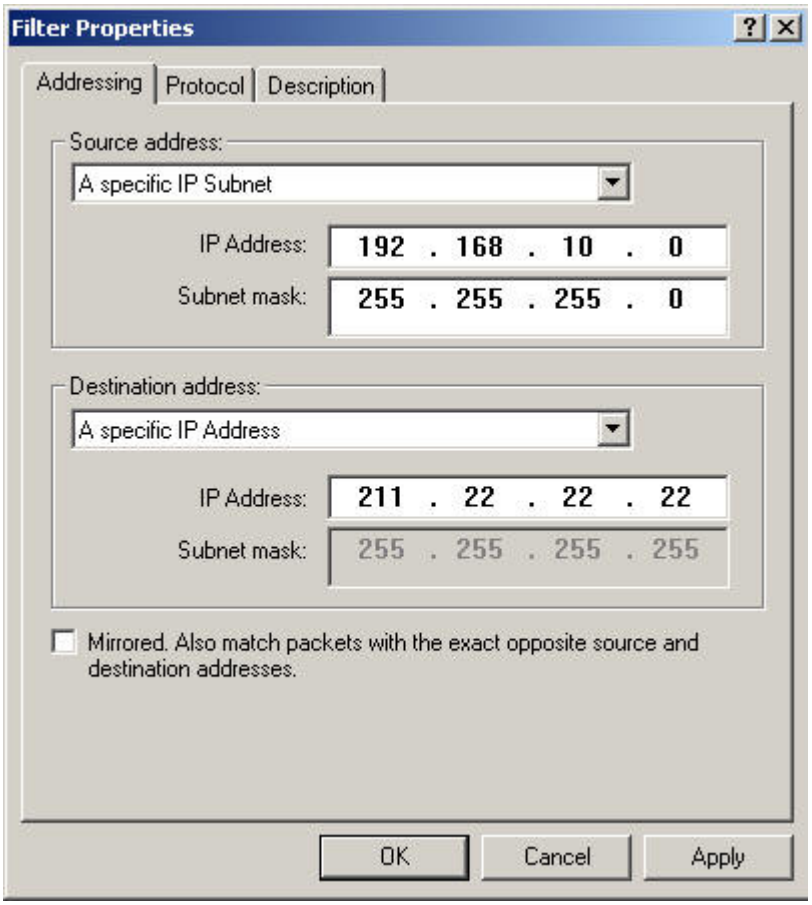


Figure 11-92 Filter Properties Settings

Step 32. Settings completed. (**Figure 11-93**)

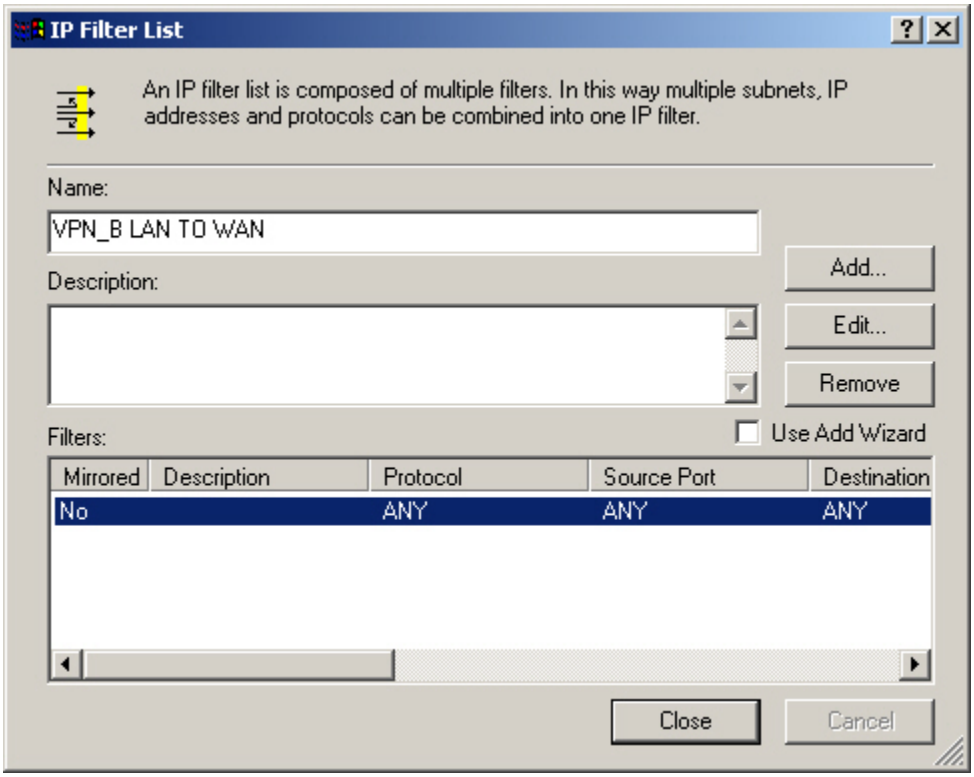


Figure 11-93 IP Filter Added

Step 33. In the **New Rule Properties** window, click **Filter Action** tab; tick **Required Security** and then click **Edit**. (**Figure 11-94**)

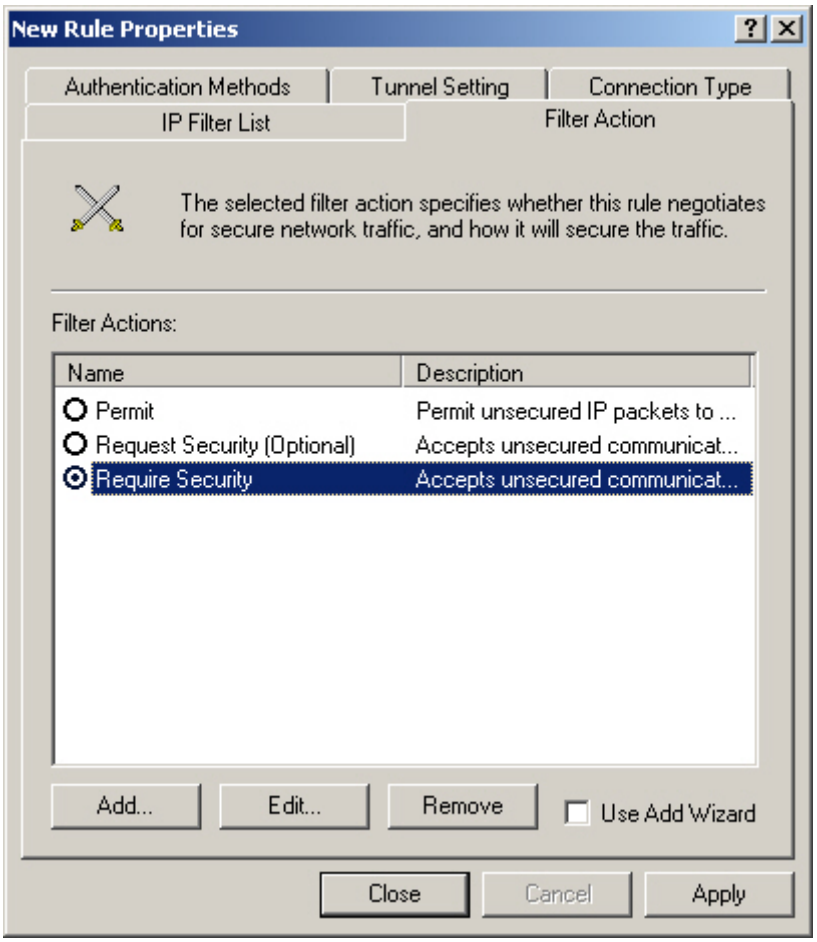


Figure 11-94 Filter Action Settings

Step 34. In the **Require Security Properties** window, tick **Session key Perfect Forward Secrecy** on the bottom. (**Figure 11-95**)

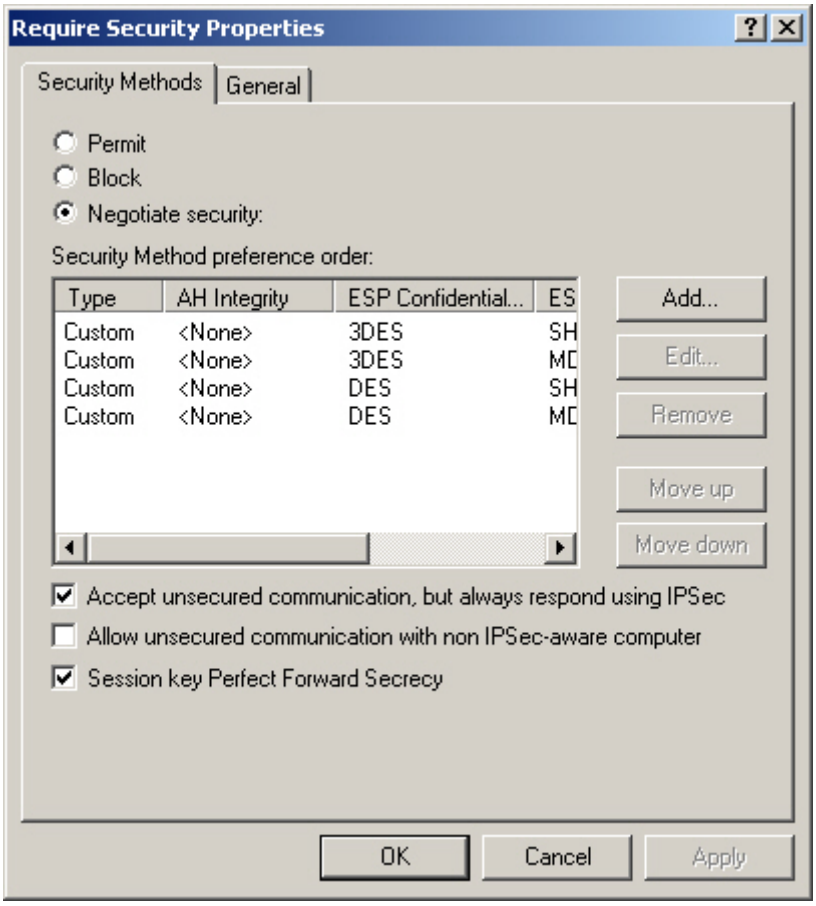


Figure 11-95 Ticking the "Session Key Perfect Forward Secrecy"

Step 35. Select the security method (**Custom / None / 3DES / MD5**), and then click **Edit**. (**Figure 11-96**)

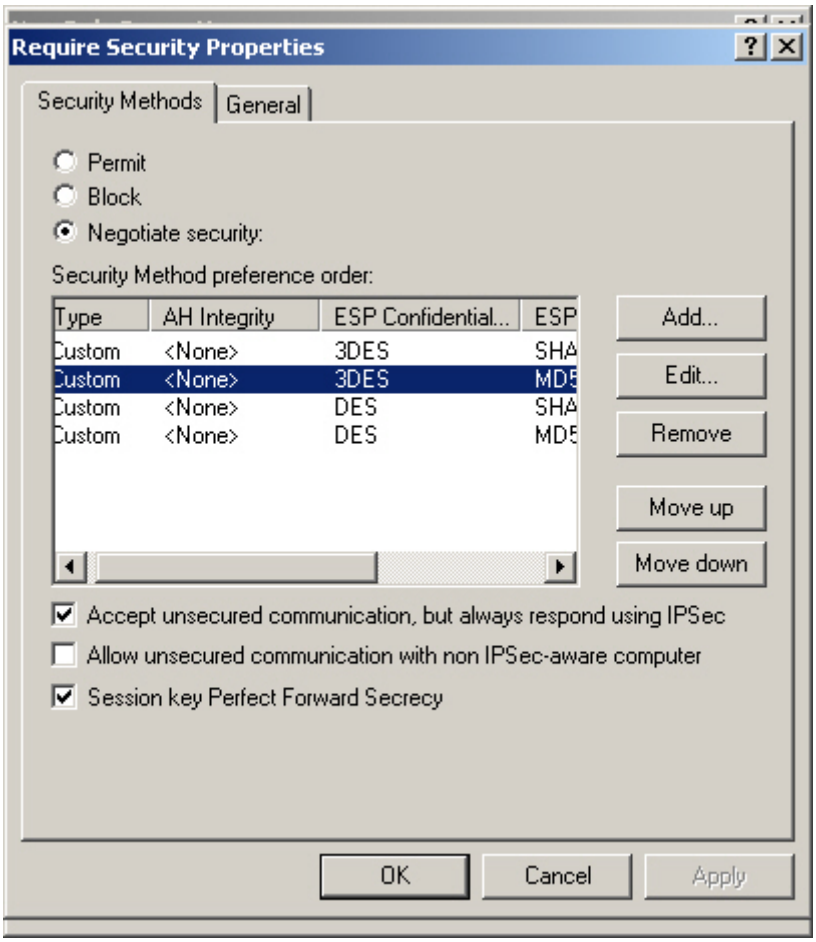


Figure 11-96 Security Methods Settings

Step 36. Select "Custom (for expert users)", and then click **Settings**. (**Figure 11-97**)

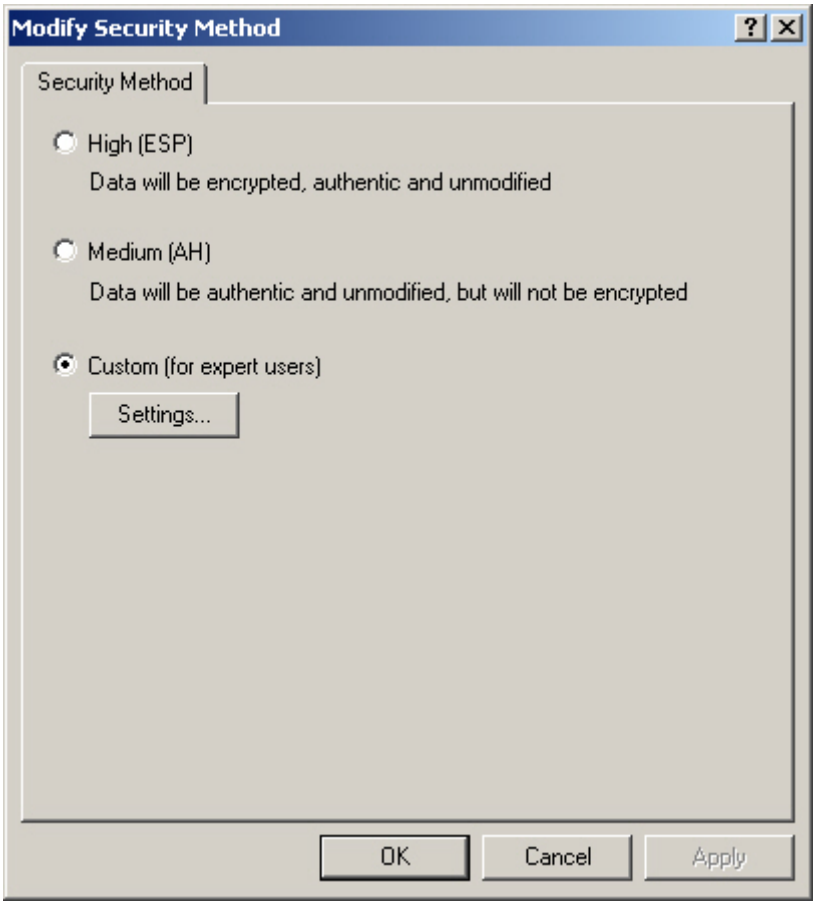


Figure 11-97 Modifying Security Method

Step 37. Check **Data integrity and encryption**, and select “MD5” for **Integrity algorithm** and “3DES” for **Encryption algorithm**. Tick **Generate a new key every**, and type “28800” in the **seconds** field, and then click **OK** to return to the **New Rule Properties** window（**Figure 11-98**）

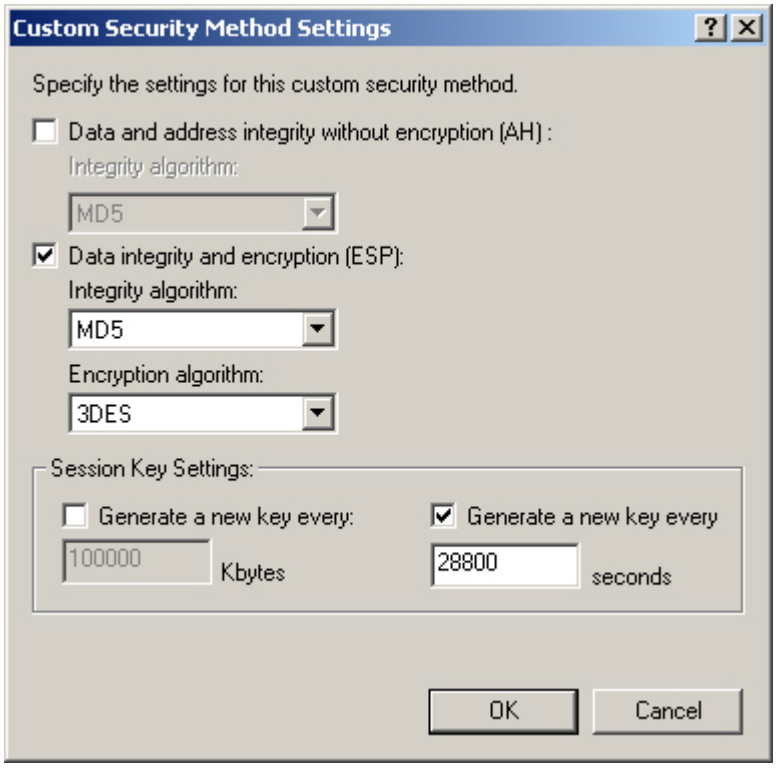


Figure 11-98 Customizing Security Method

Step 38. In the **New Rule Properties** window, click **Connection Type** tab and tick **All network connections**.（**Figure 11-99**）

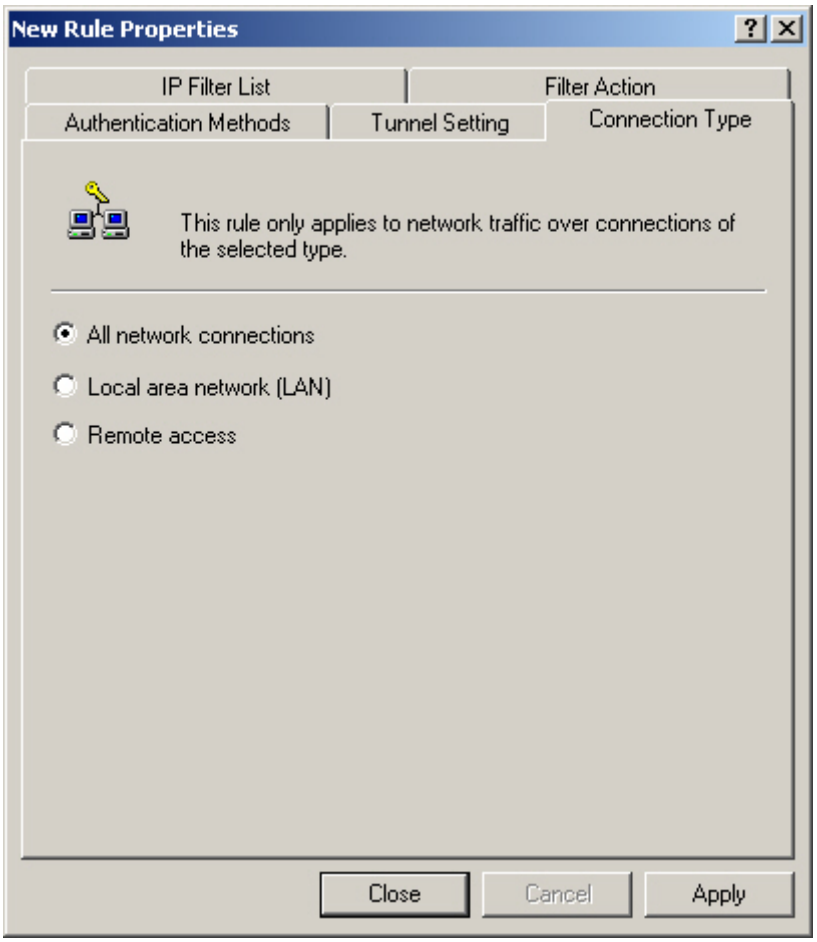


Figure 11-99 Selecting the Connection Type

Step 39. In the **New Rule Properties** window, click **Tunnel Setting** tab. After that, tick **The tunnel endpoint is specified by this IP Address**, and then type “211.22.22.22” as the WAN IP address of B Company.（**Figure 11-100**）

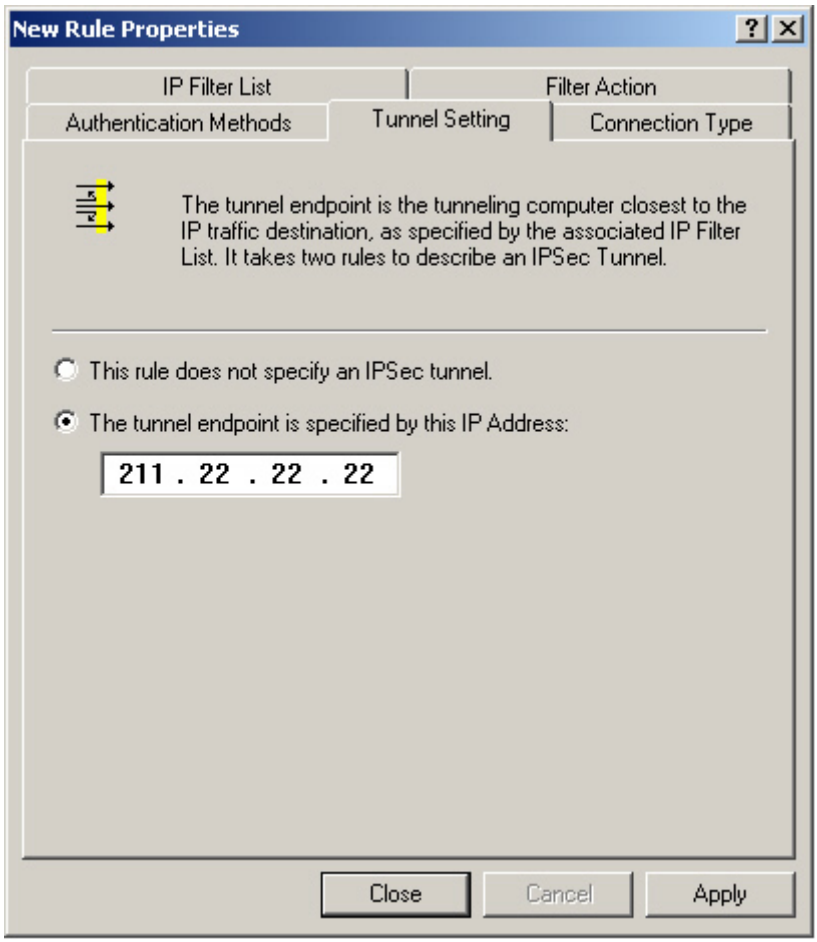


Figure 11-100 Tunnel Settings

Step 40. In the **New Rule Properties** window, click **Authentication Methods** tab. Next, select the method “Kerberos” and then click **Edit** on the right. （**Figure 11-101**）

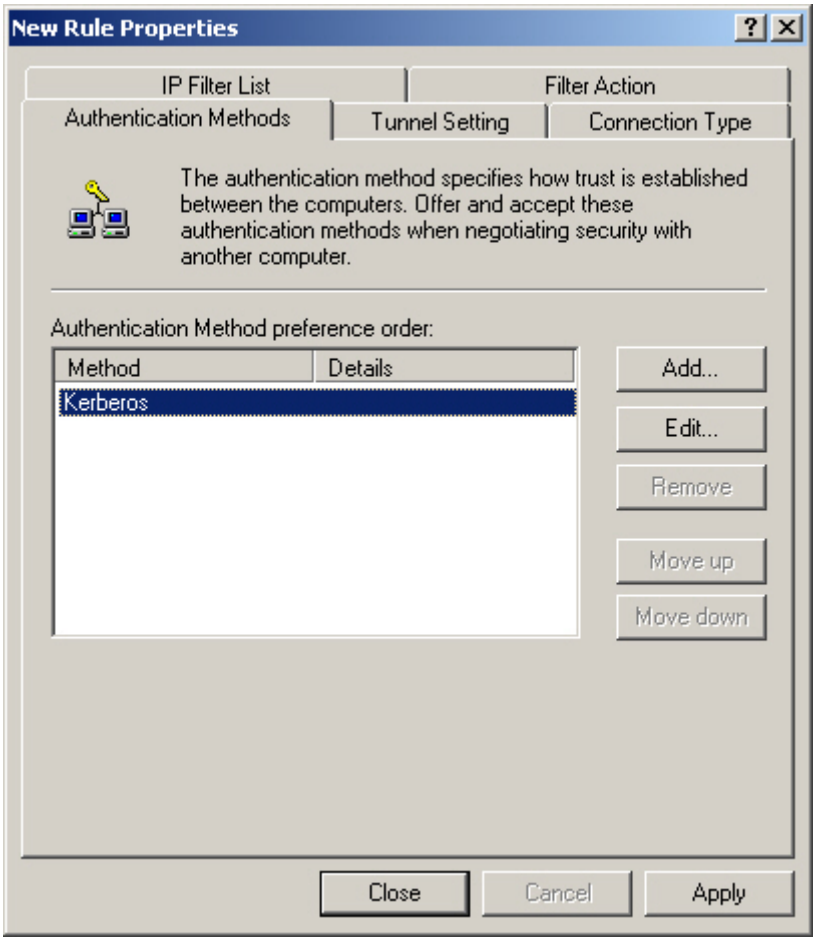


Figure 11-101 Authentication Methods Settings

Step 41. Select **Use this string to protect the key exchange (preshared key)**, and then enter the preshared key “123456789” in the field. （**Figure 11-102**）

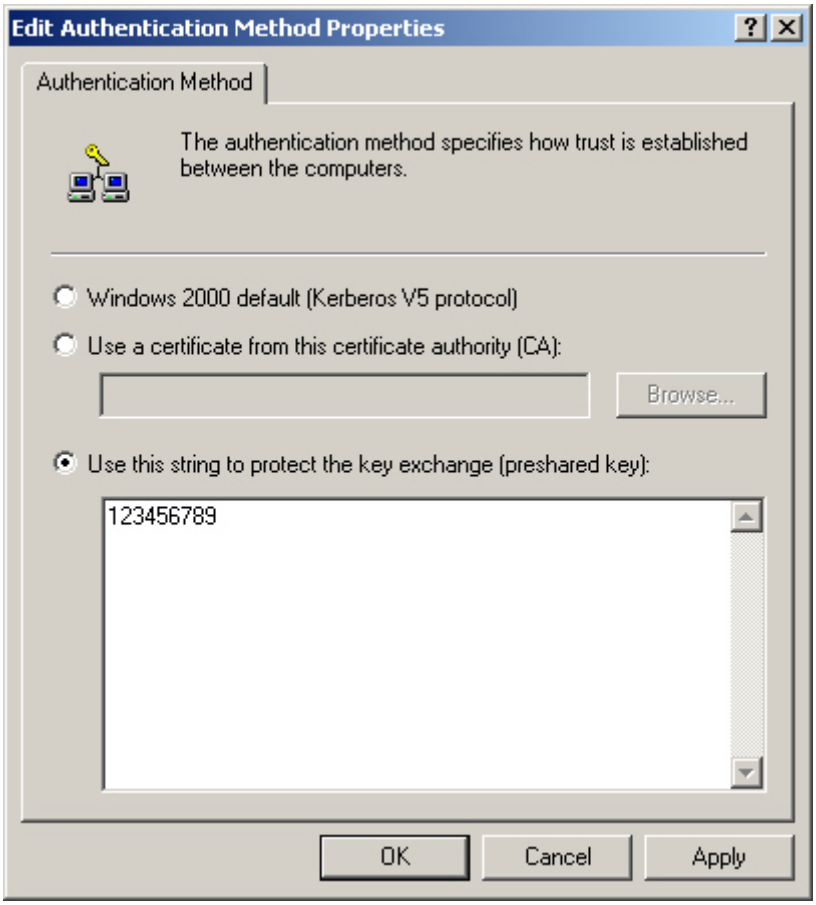


Figure 11-102 Preshared Key Settings

Step 42. Click **Apply**, and then click **Close** to close the window.（**Figure 11-103**）

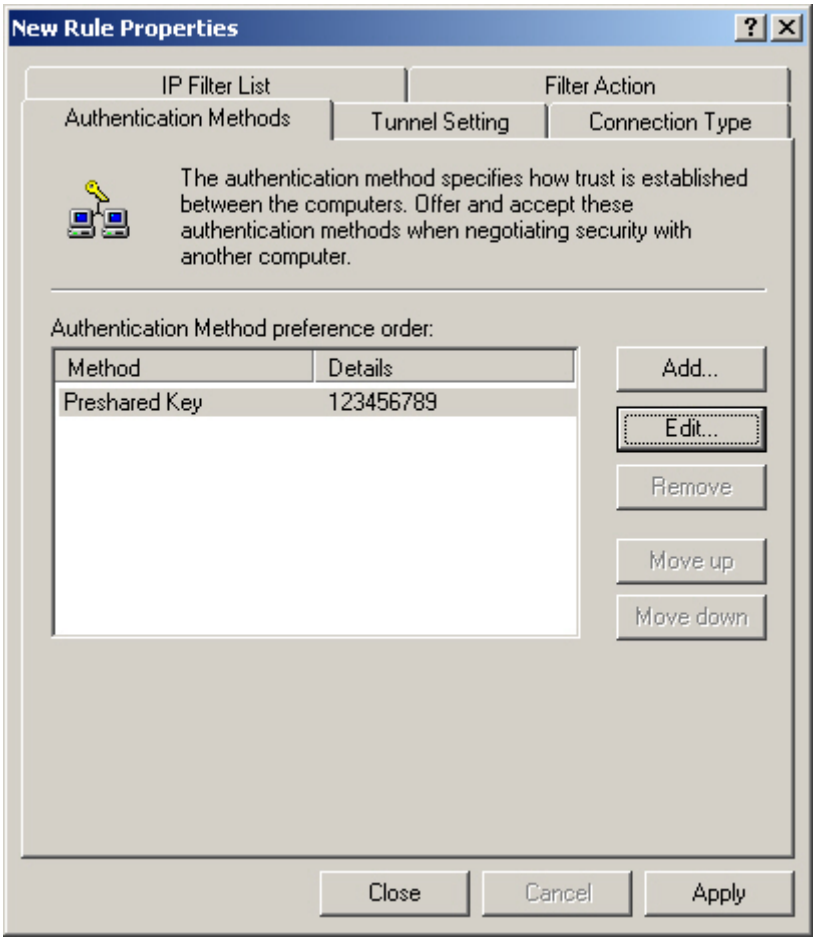


Figure 11-103 New Authentication Method Created

Step 43. Settings completed.（Figure 11-104）

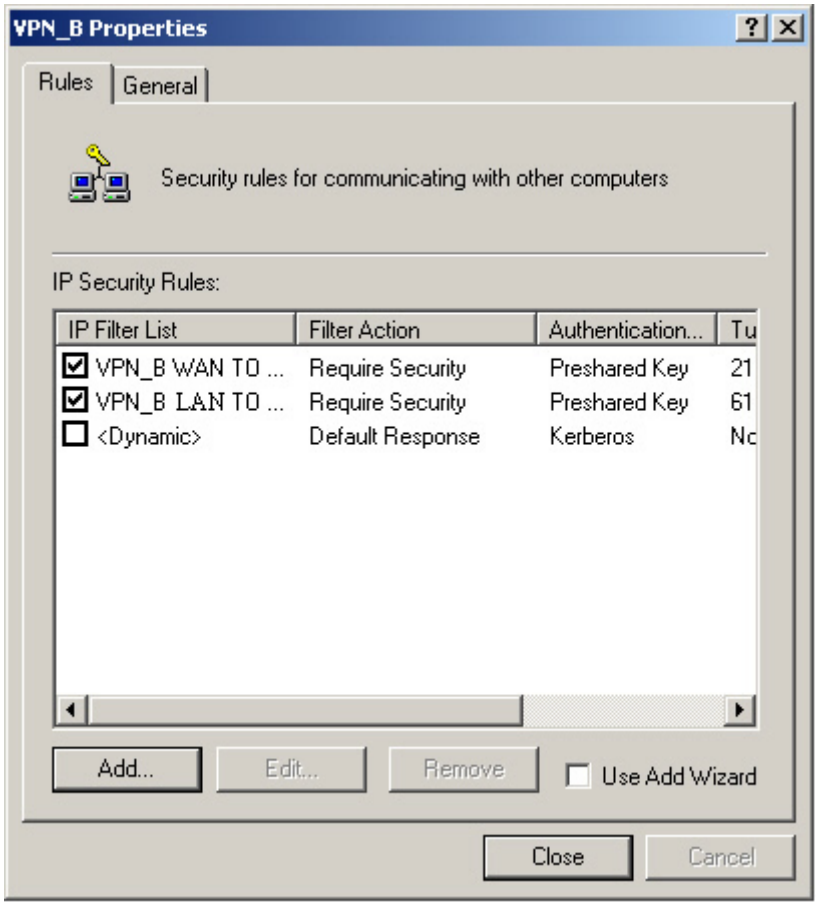


Figure 11-104 Settings Completed

Step 44. In the **VPN_B Properties** window, click **General** tab and then click **Advanced**.（**Figure 11-105**）

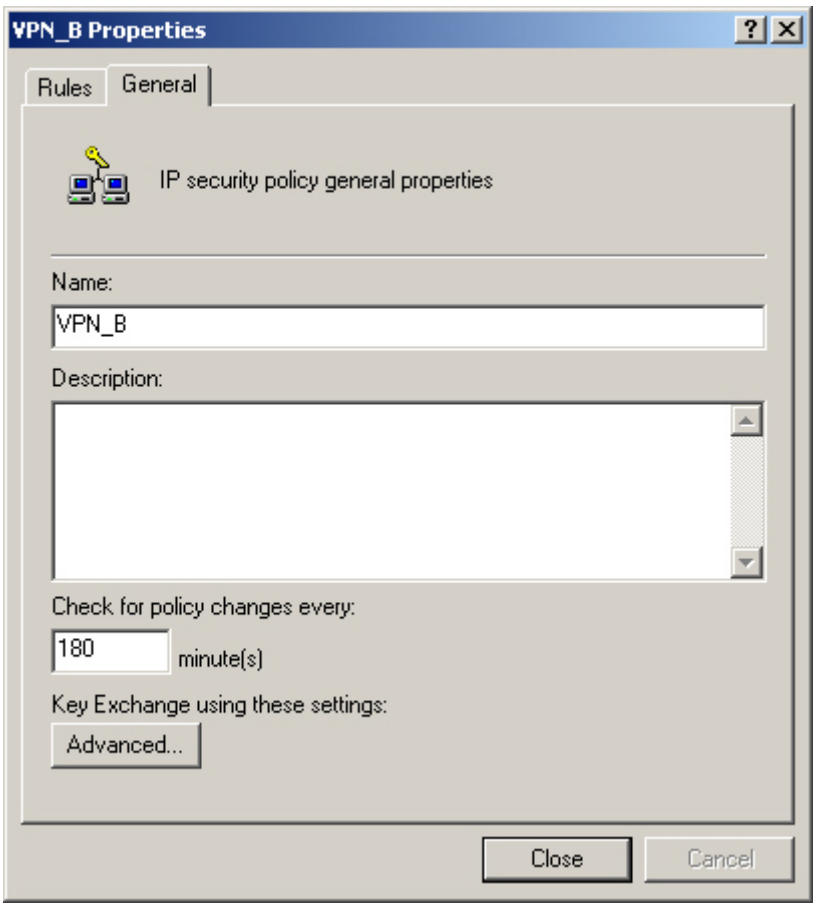


Figure 11-105 General Settings of VPN_B Properties

Step 45. Tick **Master Key Perfect Forward Secrecy** and then click **Methods.** （**Figure 11-106**）

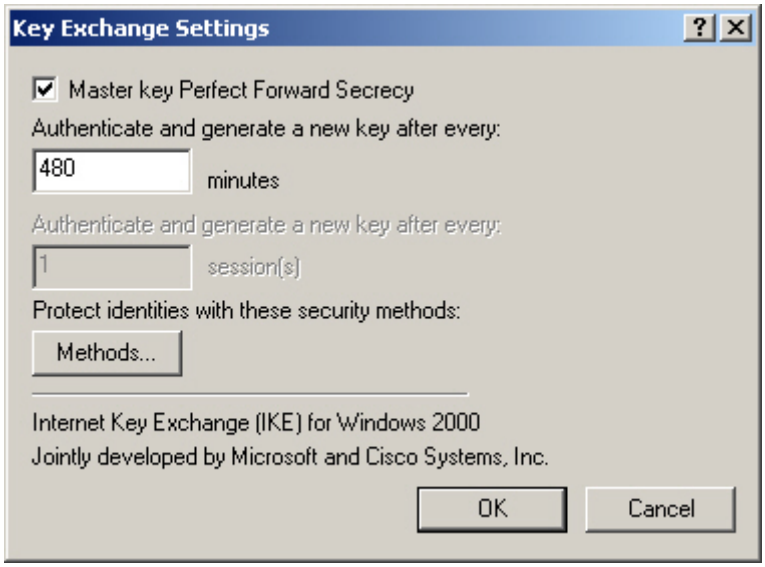


Figure 11-106 Key Exchange Settings

Step 46. Click **Move up** or **Move down** to arrange the order of selected item. Move the item “IKE / 3DES / MD5” to the top, and then click **OK**. （**Figure 11-107**）

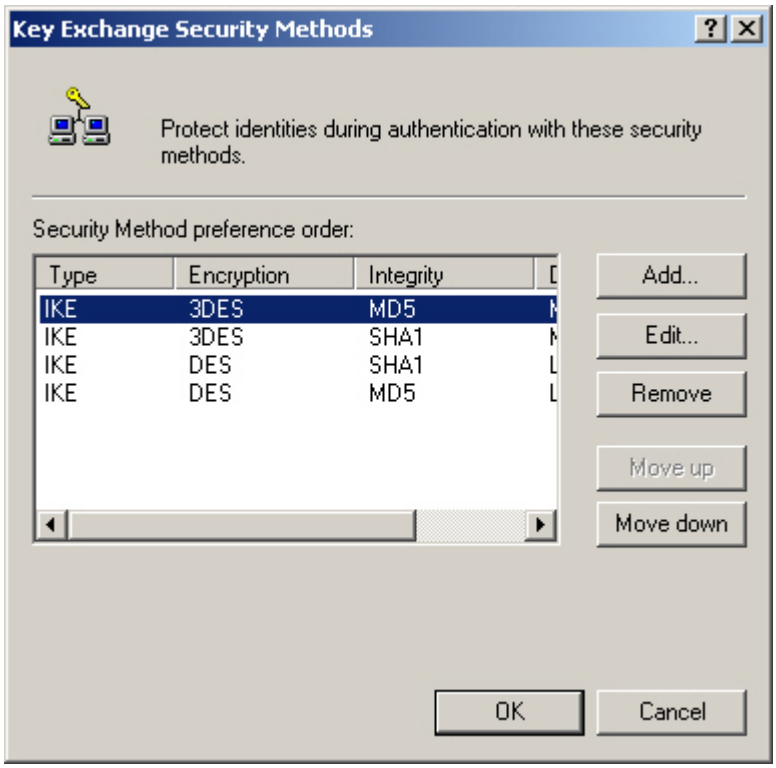


Figure 11-107 Rearranging the Order of Security Methods

Step 47. Settings completed.（**Figure 11-108**）

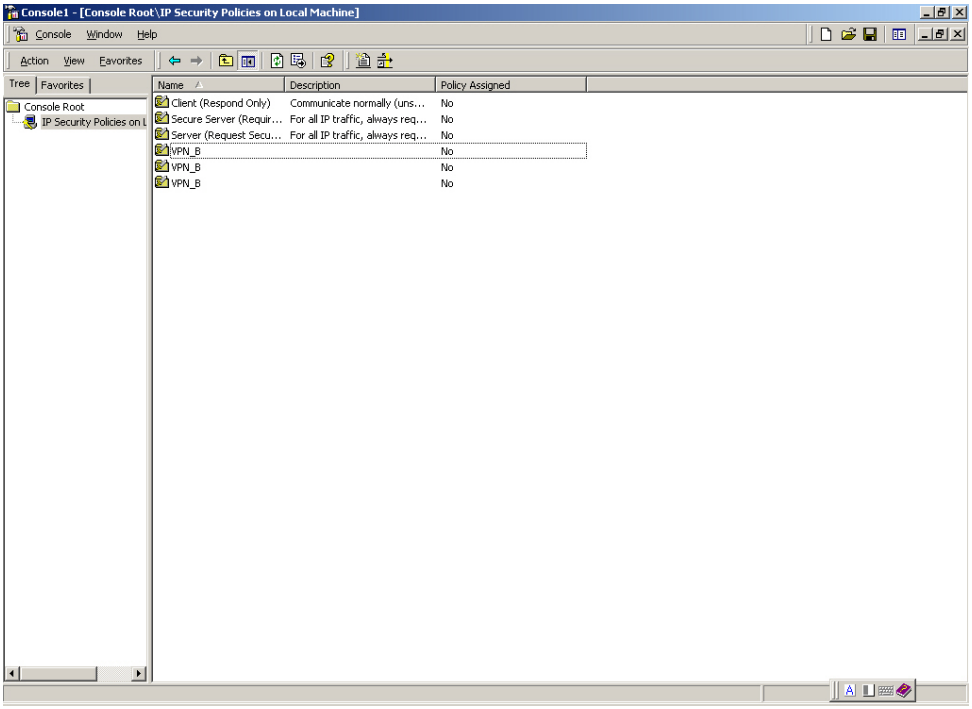


Figure 11-108 IPSec VPN Settings Completed

Step 48. Right-click **VPN_B** and move to **Assign**, and then click it.（**Figure 11-109**）

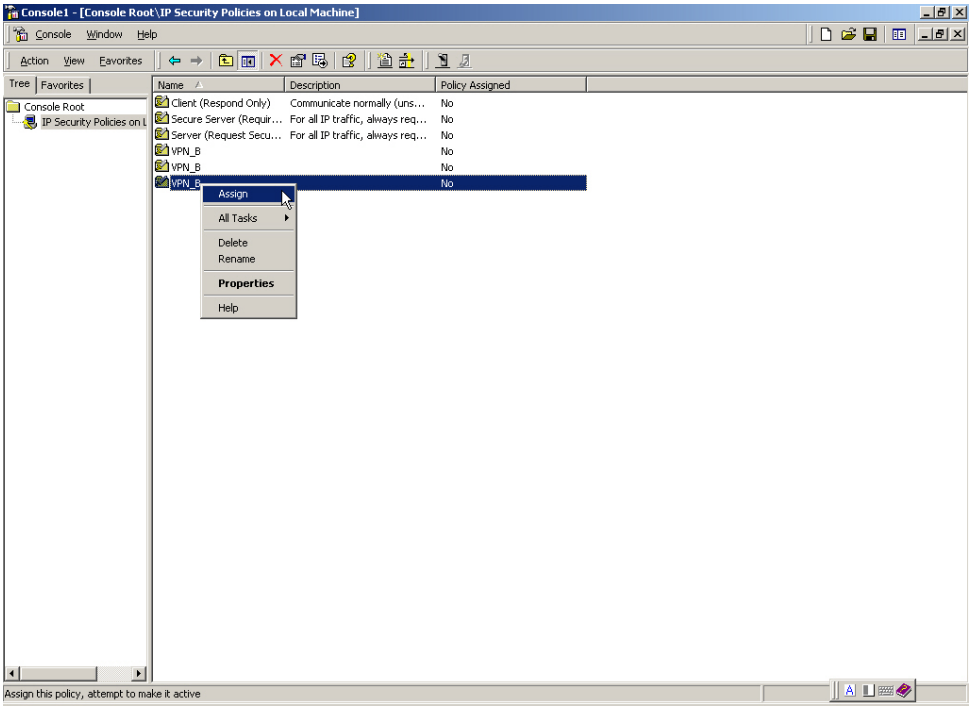


Figure 11-109 Assigning a Security Rule to VPN_B

Step 49. Select **Start** > **Settings** > **Control Panel** on the **Start** menu, and then click it. （**Figure 11-110**）

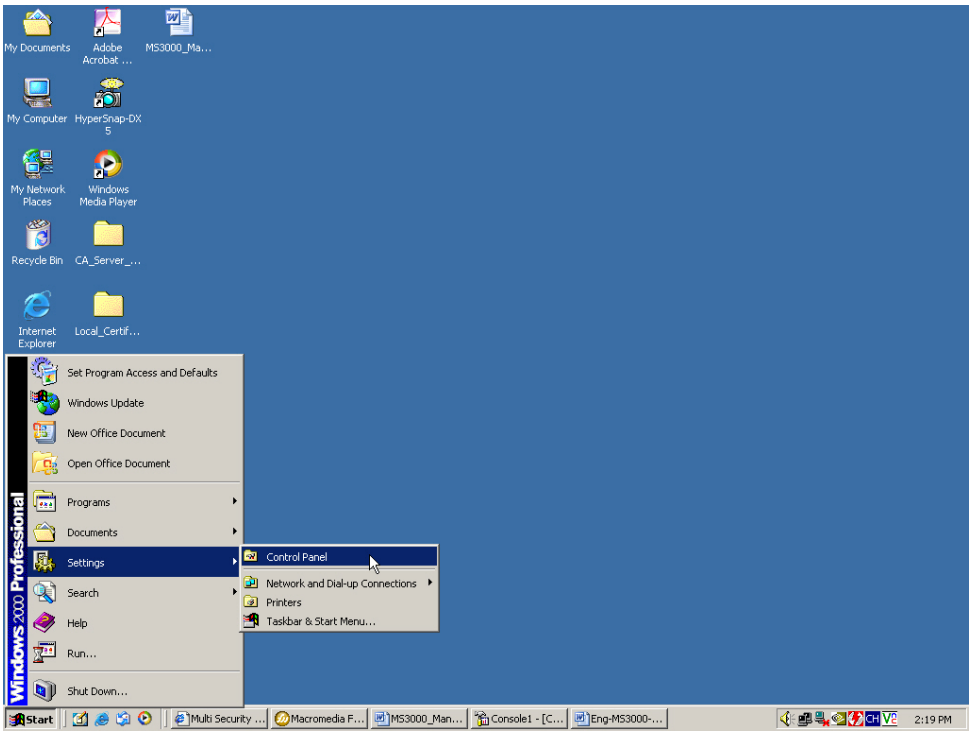


Figure 11-110 Selecting “Control Panel” on the Start Menu

Step 50. In the **Control Panel** window, double-click **Administrative Tools.** （**Figure 11-111**）

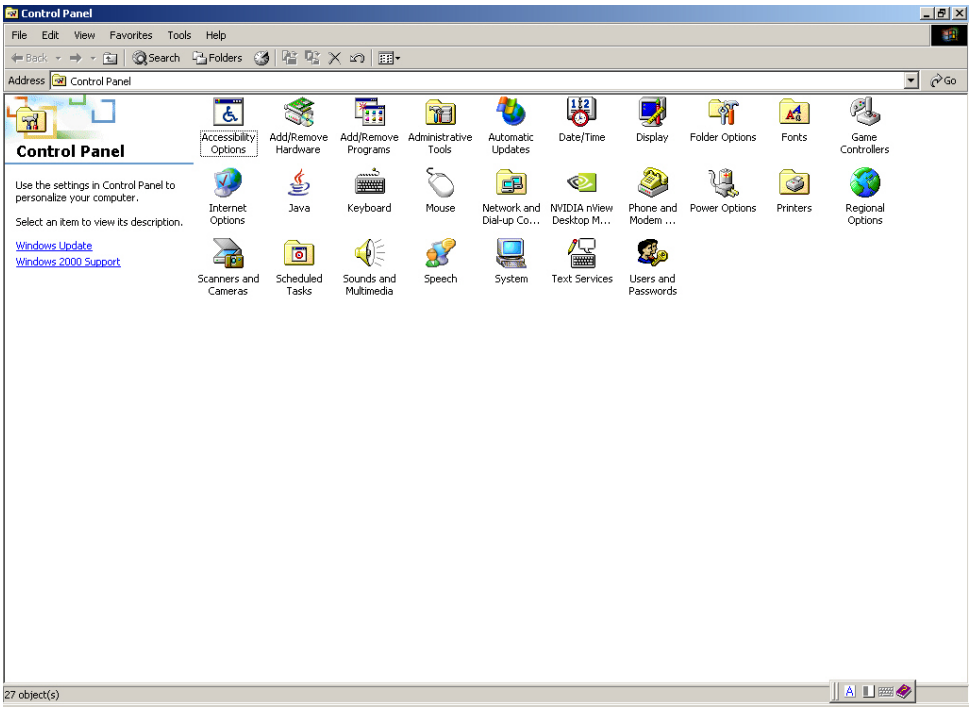


Figure 11-111 Double-Clicking “Administrative Tools”

Step 51. In the **Administrative Tools** window, double-click **Services**.（**Figure 11-112**）

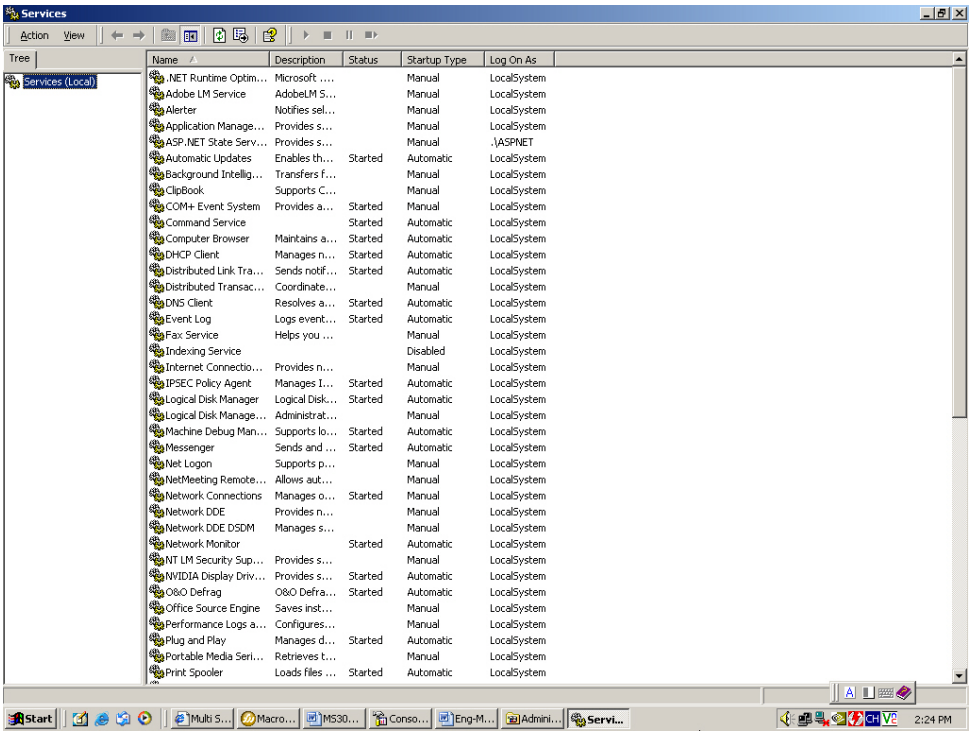


Figure 11-112 The Services Window

Step 52. In the **Services** window, right-click **IPSec Policy Agent** and move to **Restart**, and then click it.（**Figure 11-113**）

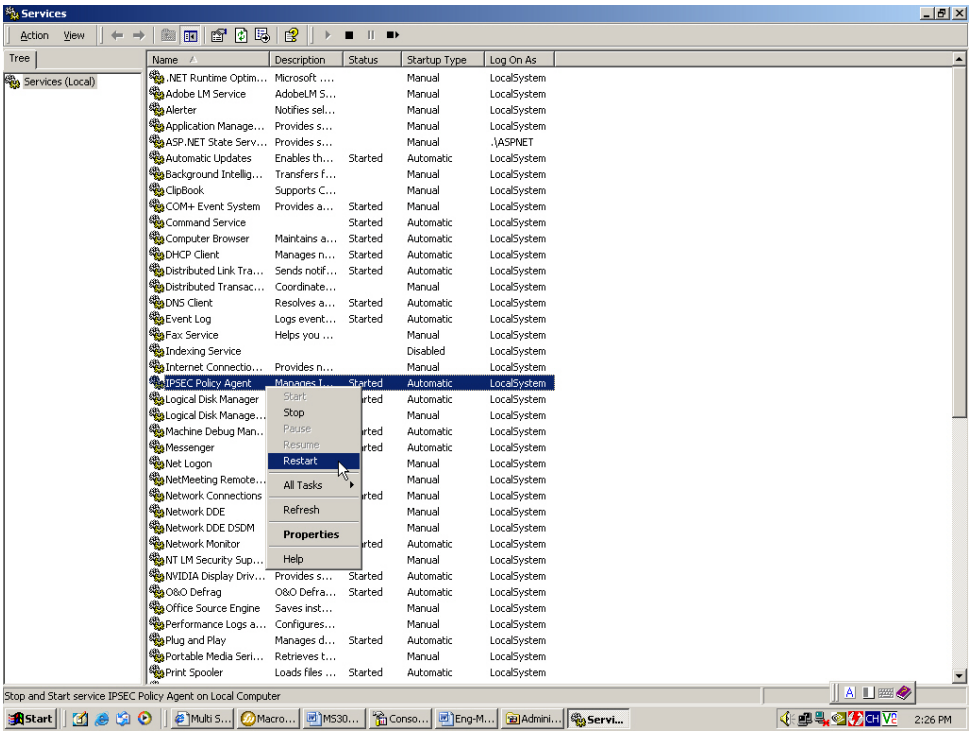


Figure 11-113 Restarting IPSec Policy Agent

Step 53. Settings completed.（Figure 11-114）

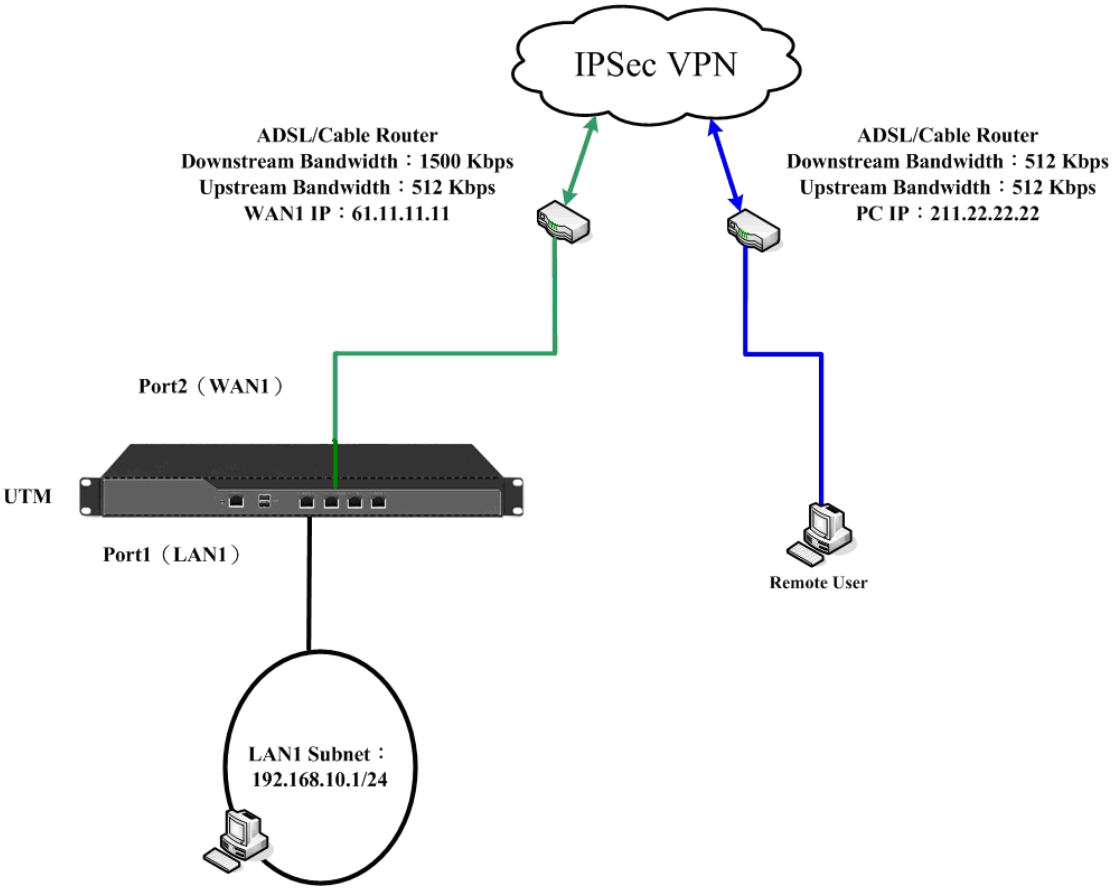


Figure 11-114 Deployment of IPSec VPN Using CS-2001 and Windows 2000

11.1.3 Creating an IPSec VPN Connection between Two CS-2001

Devices (An Aggressive Mode Example)

Prerequisite Setup (Note: IP addresses used as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP range: 192.168.10.x/24. Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1(192.168.20.1). IP range: 192.168.20.x/24. Configure Port2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

This example uses two CS-2001 devices to establish VPN connection between A Company and B Company. (using aggressive mode)

For A Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **IPSec Autokey**, and then click **New Entry**. （**Figure 11-115**）

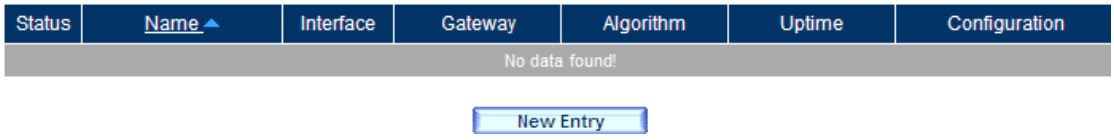


Figure 11-115 IPSec Autokey Screen

Step 2. Type ipsec1 in the **Name** field and then select Port2 (WAN1) for **WAN Interface**.（**Figure 11-116**）

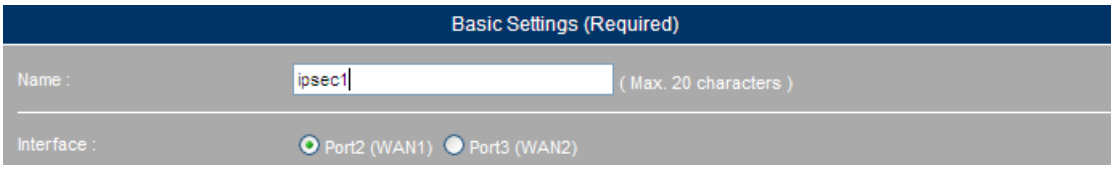


Figure 11-116 Name and WAN Interface Settings

Step 3. Select **Remote Gateway (Static IP or Hostname)** for **Remote Settings**,

and enter the management address of B Company.（**Figure 11-117**）

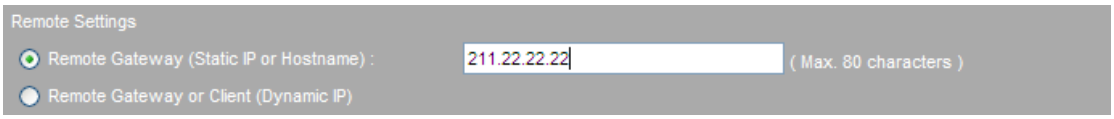


Figure 11-117 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of Pre-Shared Key String is 103 characters.（**Figure 11-118**）

Figure 11-118 Authentication Method Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “SHA1” for **Authentication Algorithm**; select “DH 2” for **Key Group**.（**Figure 11-119**）

Figure 11-119 Encryption and Data Integrity Algorithms Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.（**Figure 11-120**）

Figure 11-120 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field.（**Figure 11-121**）

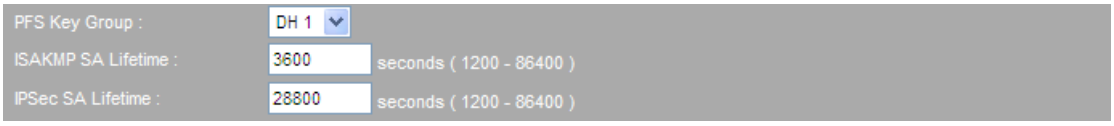


Figure 11-121 Advanced Settings of IPSec Autokey

Step 8. Select “Aggressive mode” for Mode. Enter 11.11.11.11 in the **My ID** field and then enter @abc123 in the **Peer ID** field.（**Figure 11-122**）

Figure 11-122 Mode Settings

Note：

1. MY ID / Peer ID Settings:

- The ID will be the same as the WAN IP if you leave the field blank.
- MY ID and Peer ID should be different and be choosen from an IP address not currently being used by something else, such as, 11.11.11.11, 22.22.22.22.
- The symbol @ should be added before the ID, such as, @123a, @abcd1.

Step 9. Settings completed.（**Figure 11-123**）

Figure 11-123 IPSec Autokey Settings Completed

Step 10. Under **Policy Object** > **VPN** > **Trunk**, set as below:（**Figure 11-124**）

- **Name**: Type a name.
- **Local Settings**: Select “LAN”. **Local IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask**.
- **Remote Settings**: Select **Remote IP / Netmask**. **Remote IP / Mask**: Type “192.168.20.0” as B Company’s subnet address and “255.255.255.0” as **Mask**.
- **Tunnel**: Select “ipsec1” and then add it to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-125**）

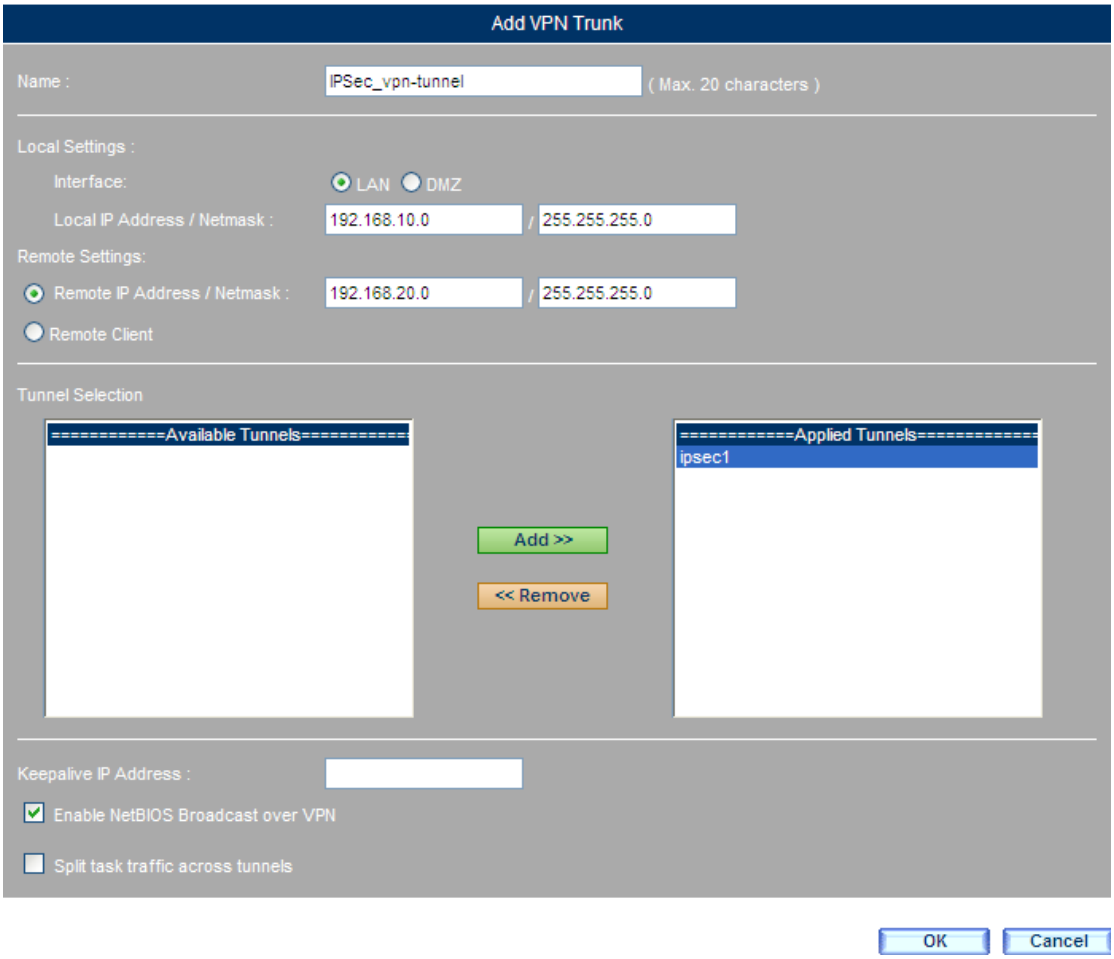


Figure 11-124 VPN Trunk Settings

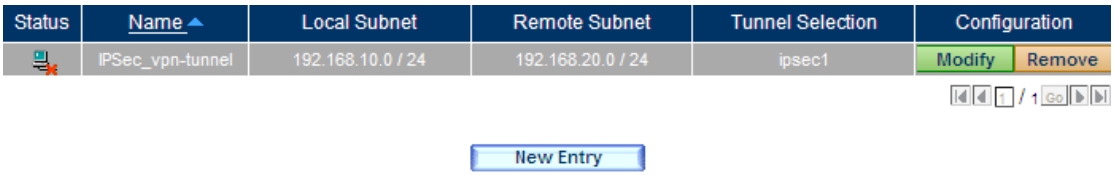


Figure 11-125 VPN Trunk Created

Step 11. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-126**）

- Select the defined trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-127**）

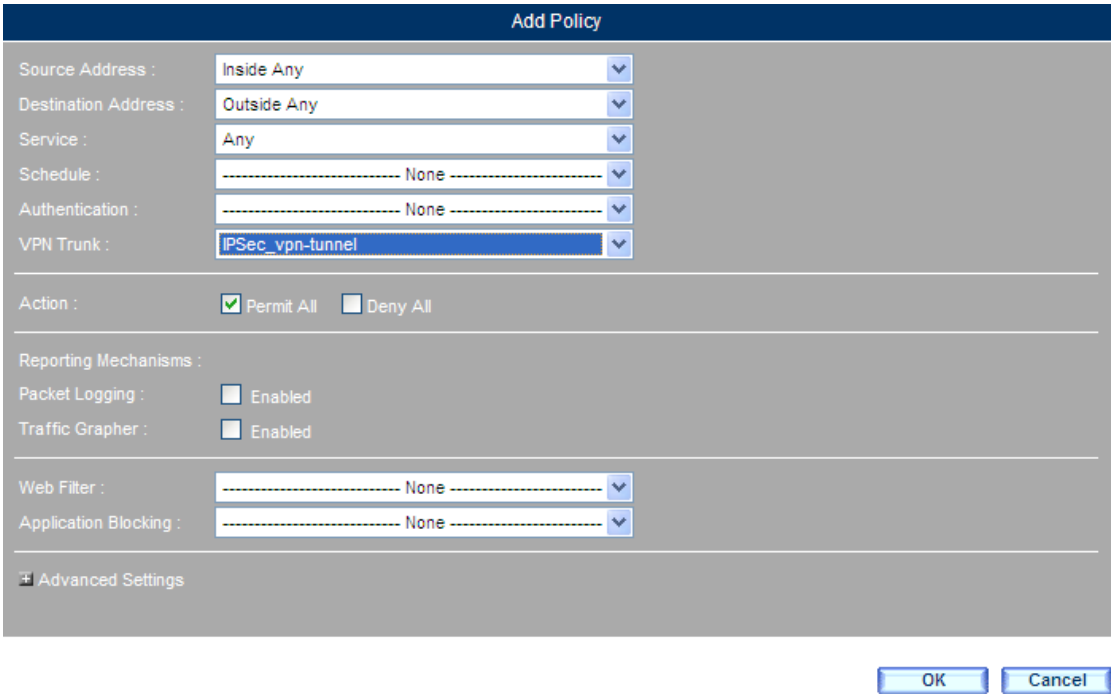


Figure 11-126 Configuring an Outgoing Policy with VPN Trunk

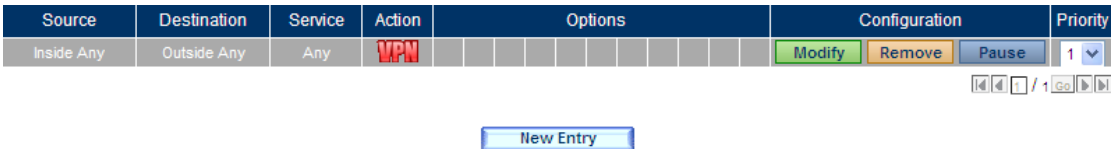


Figure 11-127 An Outgoing Policy with VPN Trunk

Step 12. Under **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-128**）

- Select the defined trunk from the **VPN Trunk** drop-down list.
- Click OK.（**Figure 11-129**）

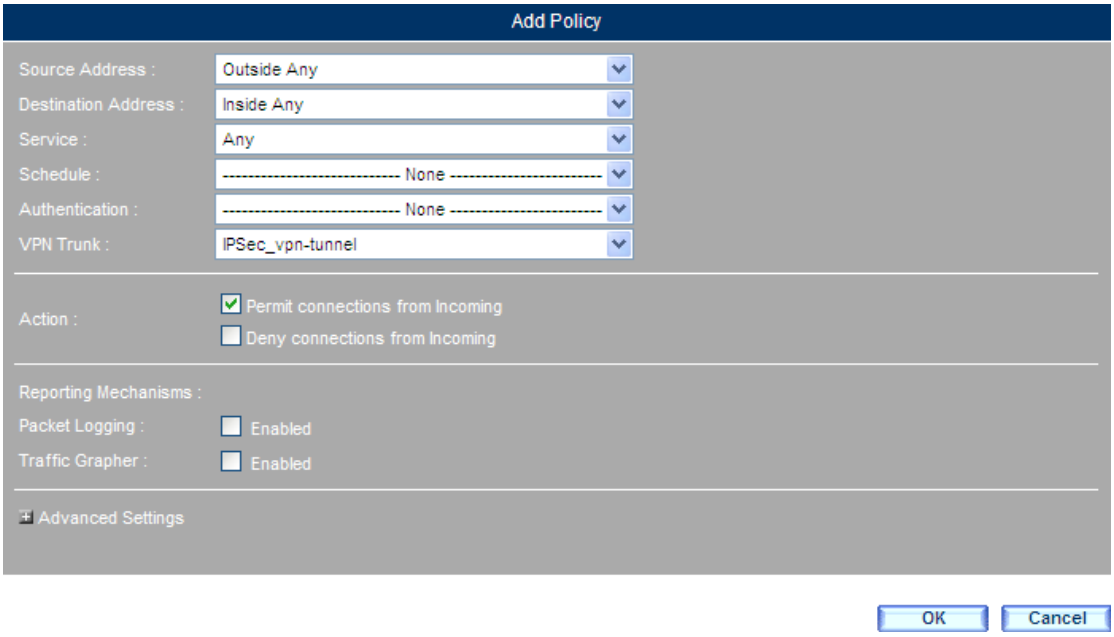


Figure 11-128 Configuring an Incoming Policy with VPN Trunk

Figure 11-129 An Incoming Policy with VPN Trunk

For B Company, set as below:

Step 1. Under **Policy Object** > **VPN** > **IPSec Autokey**, click **New Entry** and then set as below:（**Figure 11-130**）

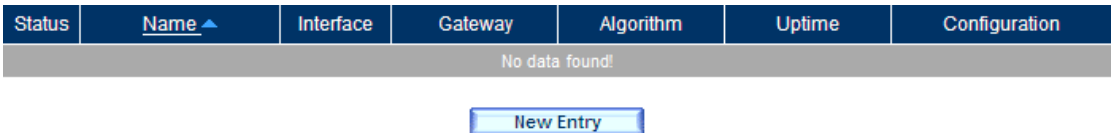


Figure 11-130 IPSec Autokey Screen

Step 2. Enter ipsec2 in the **Name** field and then select Port2 (WAN1) for **WAN Interface**.（**Figure 11-131**）

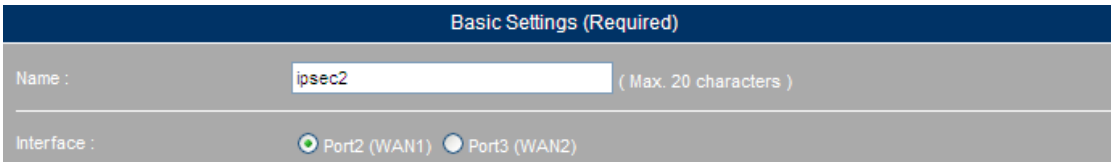


Figure 11-131 Name and WAN Interface Settings

Step 3. **Remote Settings** : Select **Remote Gateway (Static IP or Hostname)**, and then enter the management address of A Company.（**Figure 11-132**）

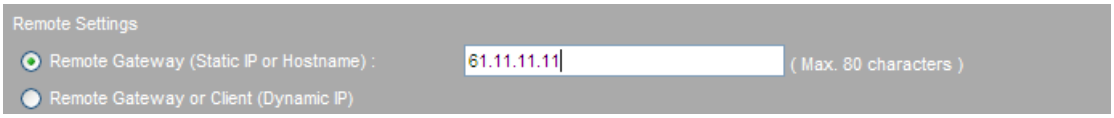


Figure 11-132 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of Pre-Shared Key String is 103 characters)（**Figure 11-133**）

Figure 11-133 Authentication Method Settings

Step 5. Below **Encryption and Data Integrity Algorithms,** select “3DES” for **Encryption Algorithm**; select “SHA1” for **Authentication Algorithm**; select “DH 2” for **Key Group**.（**Figure 11-134**）

Figure 11-134 ISAKMP Algorithm Settings

Step 6. Configure the settings under **IPSec Algorithm.** Select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.（**Figure 11-135**）

Figure 11-135 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field.（**Figure 11-136**）

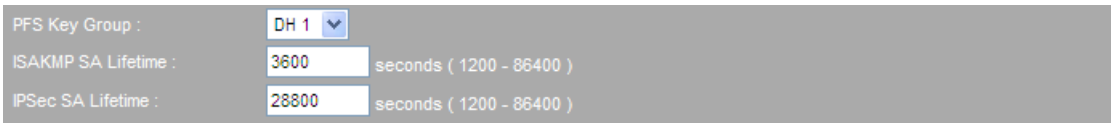


Figure11-136 Advanced Settings of IPSec Autokey

Step 8. Select “Aggressive mode” for **Mode**, enter @abc123 in the **My ID** field and then enter 11.11.11.11 in the **Peer ID** field.（**Figure 11-137**）

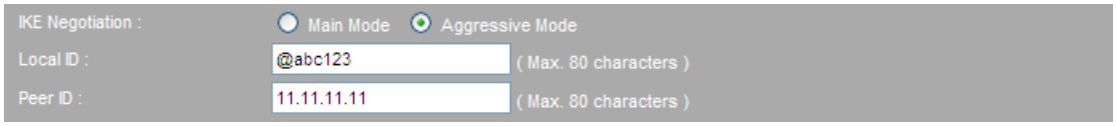


Figure 11-137 Mode Settings

Step 9. Settings completed.（**Figure 11-138**）

Figure 11-138 IPSec Autokey Settings Completed

Step 10. Select **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-139**）

- **Name**: Type a name.
- **Local Settings**: Select “LAN”. **Local IP / Netmask**: Type “192.168.20.0” as B Company’s subnet address and “255.255.255.0” as **Mask.**
- **Remote Settings**: Select **Remote IP / Netmask. Remote IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask**.
- **Tunnel**: Select “ipsec2”and then add it to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-140**）

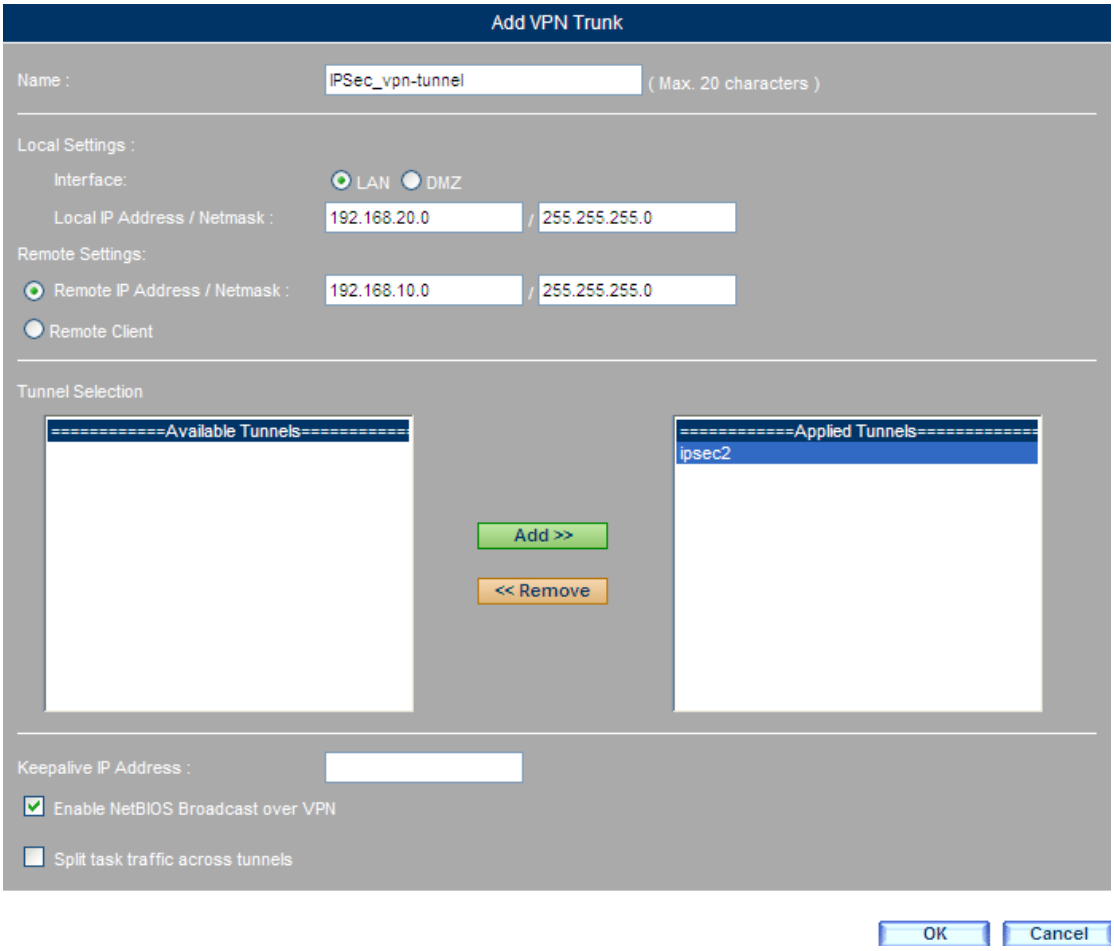


Figure 11-139 VPN Trunk Settings

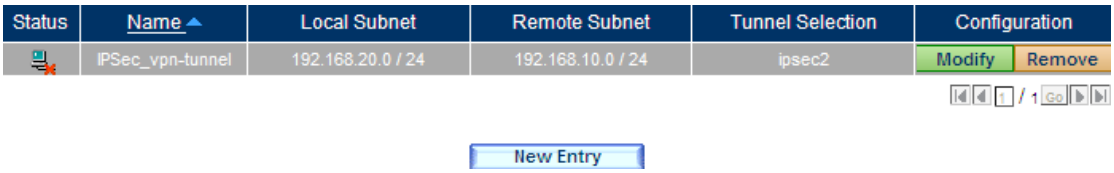


Figure 11-140 VPN Trunk Created

Step 11. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-141**）

- Select the defined trunk for **VPN Trunk**.
- Click **OK**.（**Figure 11-142**）

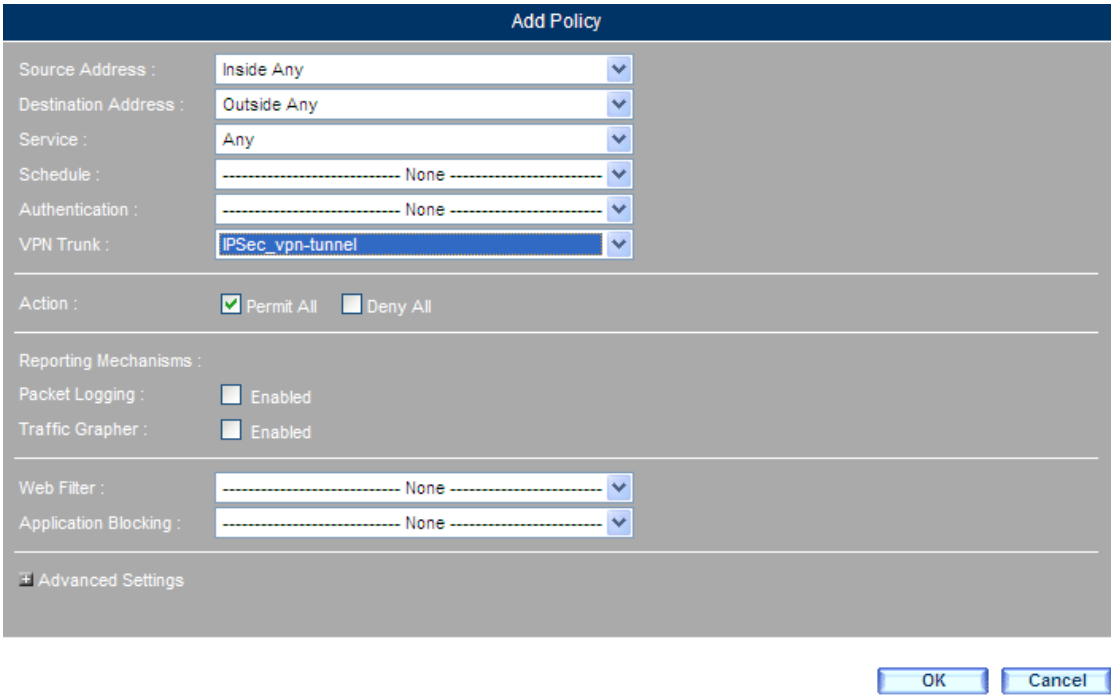


Figure 11-141 Configuring an Outgoing Policy with VPN Trunk

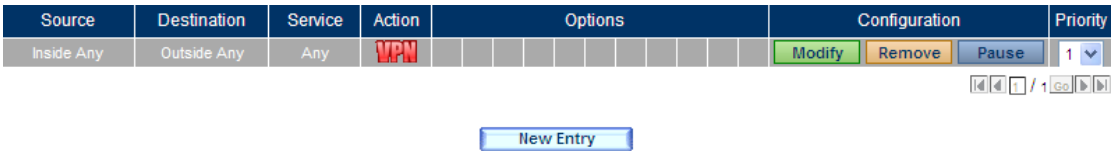


Figure 11-142 Policy Completed

Step 12. Under **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-143**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-144**）

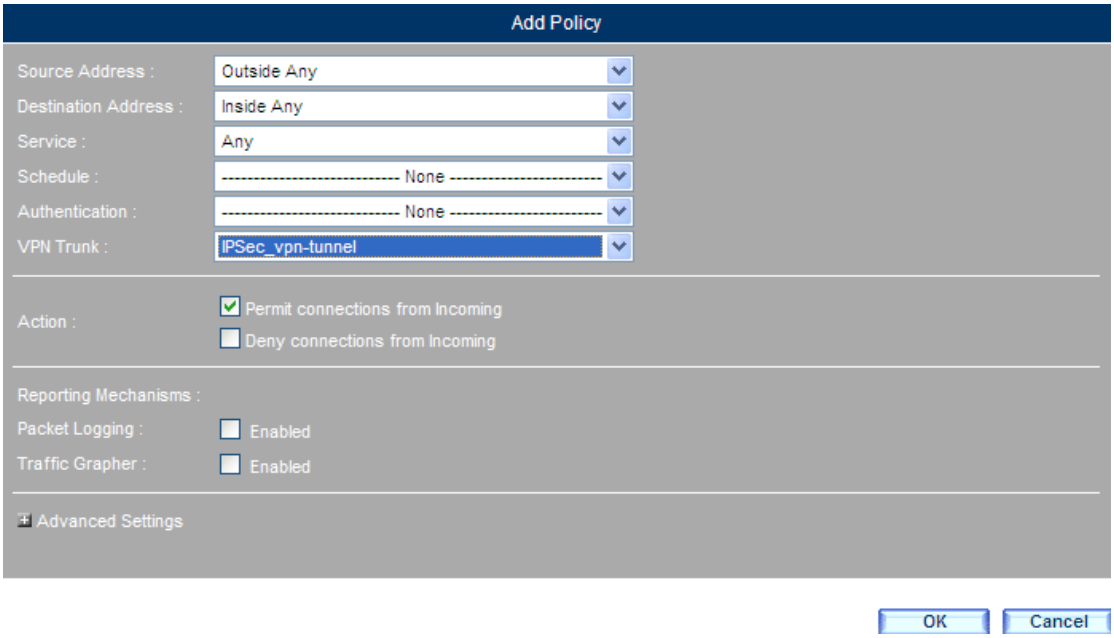


Figure 11-143 Configuring an Incoming Policy with VPN Trunk

Figure 11-144 Policy Completed

Step 13. Settings completed.（Figure 11-145）

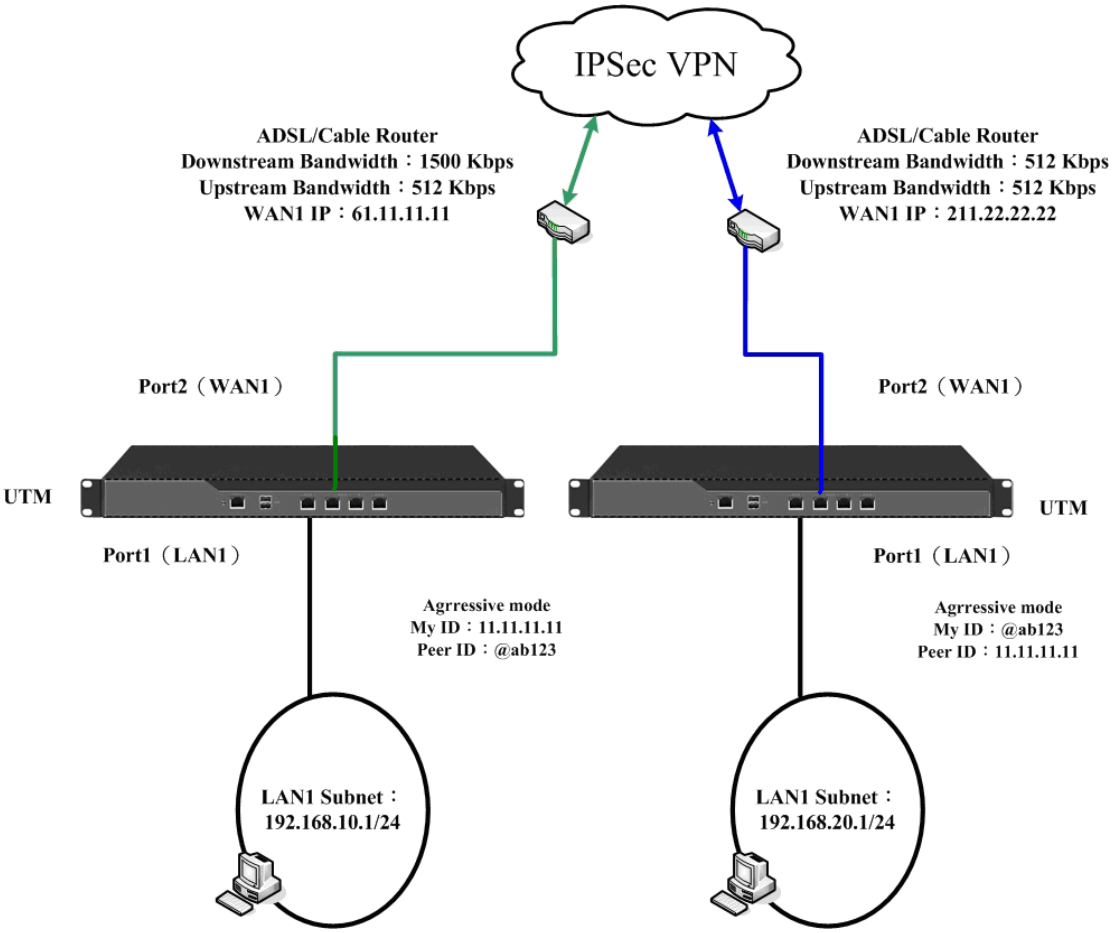


Figure 11-145 Deployment of IPSec VPN Using Aggressive Mode

11.1.4 Using Two CS-2001 Devices to Connect Outbound Load

Balance with IPSec VPN (Using GRE/IPSec Package Algorithm)

Prerequisite Setup (Note: IP Addresses uses as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP range: 192.168.10.x/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Configure Port3 as WAN2(61.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1(192.168.20.1). IP range:192.168.20.x/24.
Configure Port2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Configure Port3 as WAN2(211.33.33.33) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Two IPSec VPN connections are created between:
A Company's WAN port 1 and B Company's WAN port 1;
A Company's WAN port 2 and B Company's WAN port 2.

This example uses two CS-2001 devices. Assume that A Company wants to create a VPN connection with B Company in order to access files. (GRE / IPSec package algorithm is adopted.)

For A Company, set as below:

Step 1. Go to **Policy Object > VPN > IPSec Autokey**, and then click **New Entry**. （**Figure 11-146**）

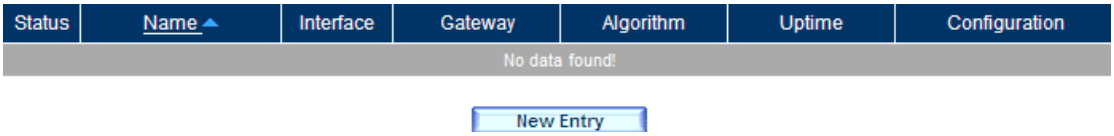


Figure 11-146 IPSec Autokey Screen

Step 2. Enter VPN_01 in the **Name** field and then select Port2 (WAN1) for the **WAN Interface**.（**Figure 11-147**）

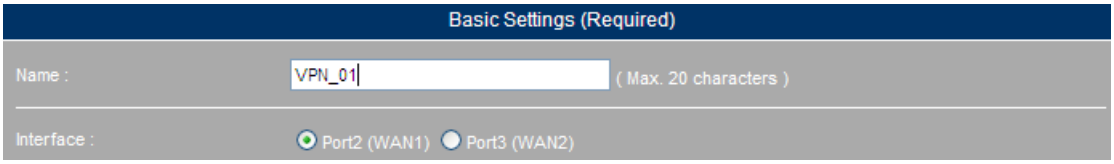


Figure 11-147 Remote Settings

Step 3. For **Remote Settings**: Select **Remote Gateway (Static IP or Hostname)**, and enter the management address of B Company (WAN port 1).（**Figure 11-148**）

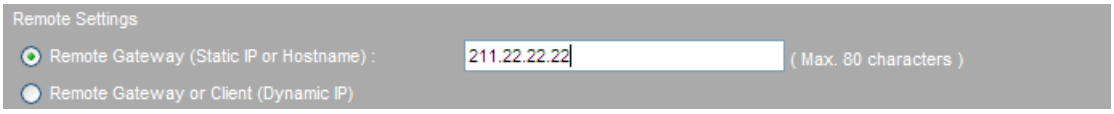


Figure 11-148 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method** and enter the **Pre-Shared Key String.**（**Figure 11-149**）

Figure 11-149 Authentication Method Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.（**Figure 11-150**）

Figure 11-150 ISAKMP Algorithm Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.（**Figure 11-151**）

Figure 11-151 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.（**Figure 11-152**）

Figure 11-152 Advanced Settings of IPSec Autokey

Step 8. For **GRE Tunnel Settings**, type “192.168.50.100” in the **Local Endpoint Address** field and “192.168.50.200” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)（**Figure 11-153**）

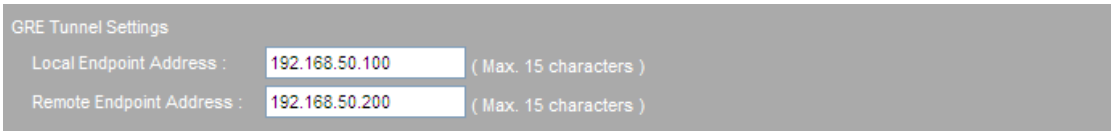


Figure 11-153 GRE / IPSec Settings

Note：

1. The IP addresses for **Local Endpoint Address** and **Remote Endpoint Address** should be on the same Class C subnet but must not already be in use.

Step 9. Setting completed.（Figure 11-154）

Figure 11-154 IPSec Autokey Settings Completed

Step 10. Select **Policy Object > VPN > IPSec Autokey**, and then click **New Entry**.

Step 11. Type VPN_02 in the **Name** field and then select Port3(WAN2) for the **WAN Interface**.（Figure 11-156）

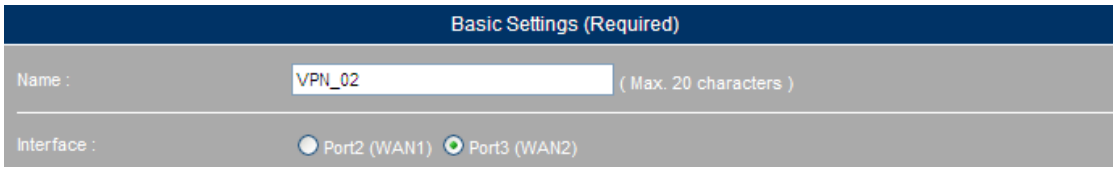


Figure 11-156 Name and WAN Interface Settings

Step 12. **Remote Settings**: Select **Remote Gateway (Static IP or Hostname)** and then type B Company's IP address in the field.（Figure 11-157）

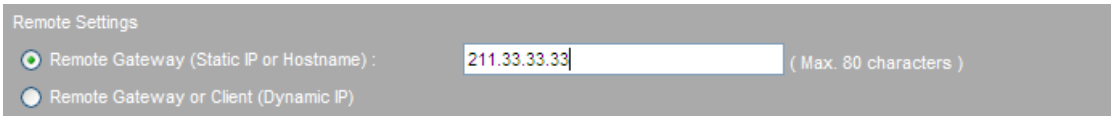


Figure 11-157 Remote Settings

Step 13. Select "Pre-Shared Key" for **Authentication Method** and enter the **Pre-Shared Key String**.（Figure 11-158）

Figure 11-158 Authentication Method Settings

Step 14. Under the **ISAKMP Algorithm** section, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.（**Figure 11-159**）

Figure 11-159 ISAKMP Algorithm Settings

Step 15. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.（**Figure 11-160**）

Figure 11-160 IPSec Algorithm Settings

Step 16. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.（**Figure 11-161**）

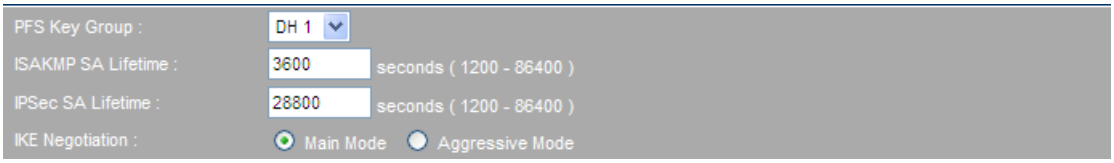


Figure 11-161 Advanced Settings of IPSec Autokey

Step 17. For **GRE Tunnel Settings**, type “192.168.60.100” in the **Local Endpoint Address** field and “192.168.60.200” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)（**Figure 11-162**）

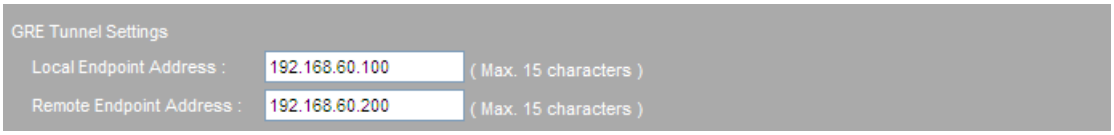


Figure 11-162 GRE/ IPSec Settings

Step 18. Settings completed.（Figure 11-163）

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	---	Modify Remove
	VPN_02	WAN2	211.33.33.33	3DES / MD5	---	Modify Remove

/ 1 Go

New Entry

Figure 11-163 IPSec Autokey Settings Completed

Step 19. Under **Policy Object > VPN > Trunk**, set as below: （Figure 11-164）

- **Name**: Type a name.
- **Local Settings**: Select “LAN”. **Local IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask.**
- **Remote Settings**: Select **Remote IP / Netmask**. **Remote IP / Netmask**: Type “192.168.20.0” as B Company’s subnet address and “255.255.255.0” as **Mask.**
- **Tunnel**: Select “VPN_01” and “VPN_02” and then add them to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（Figure 11-165）

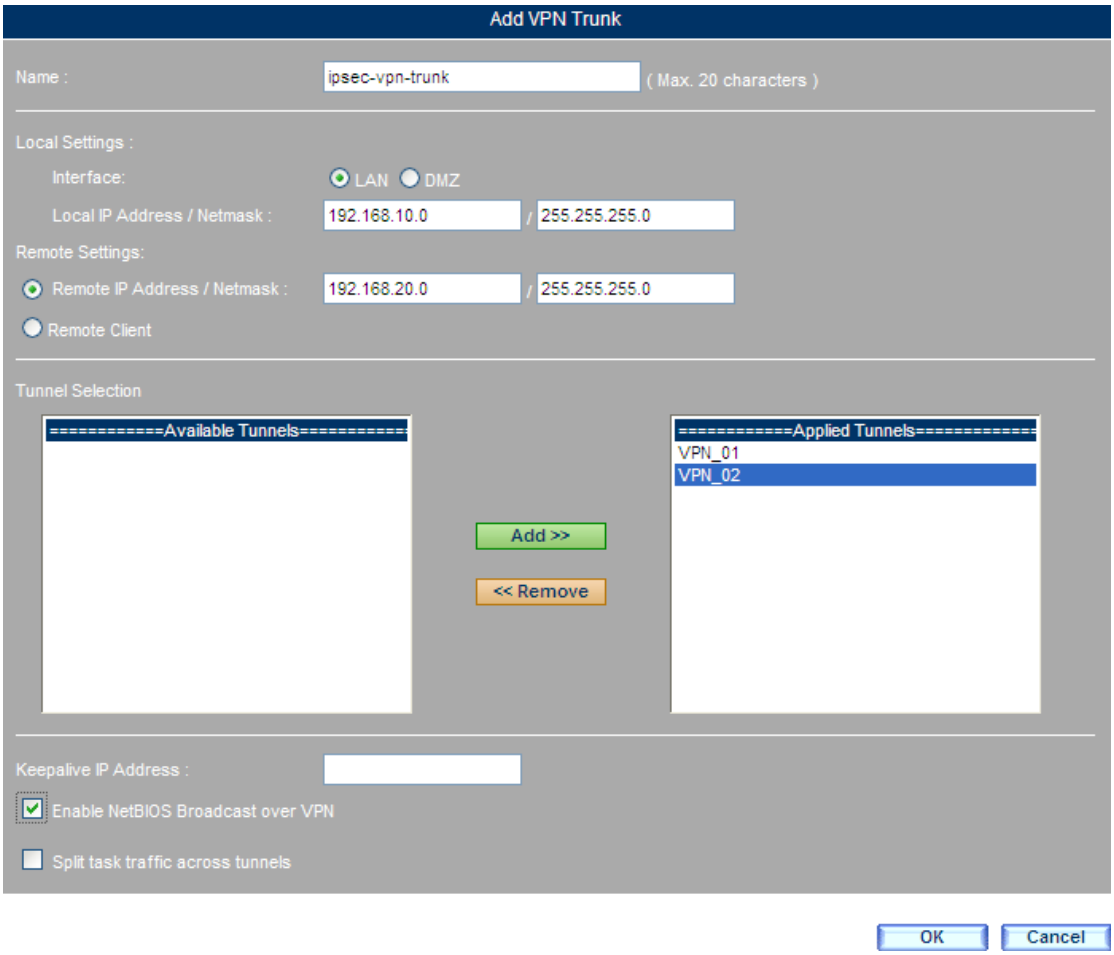


Figure 11-164 VPN Trunk Settings

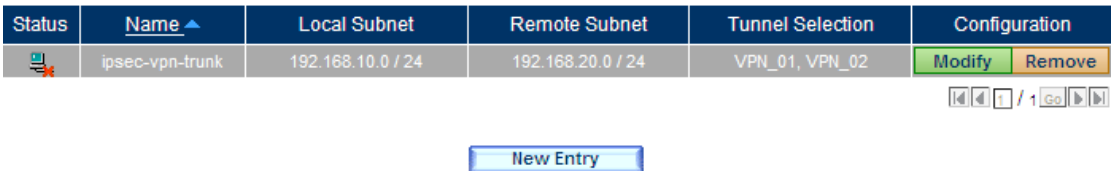


Figure 11-165 VPN Trunk Created

Step 20. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-166**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-167**）

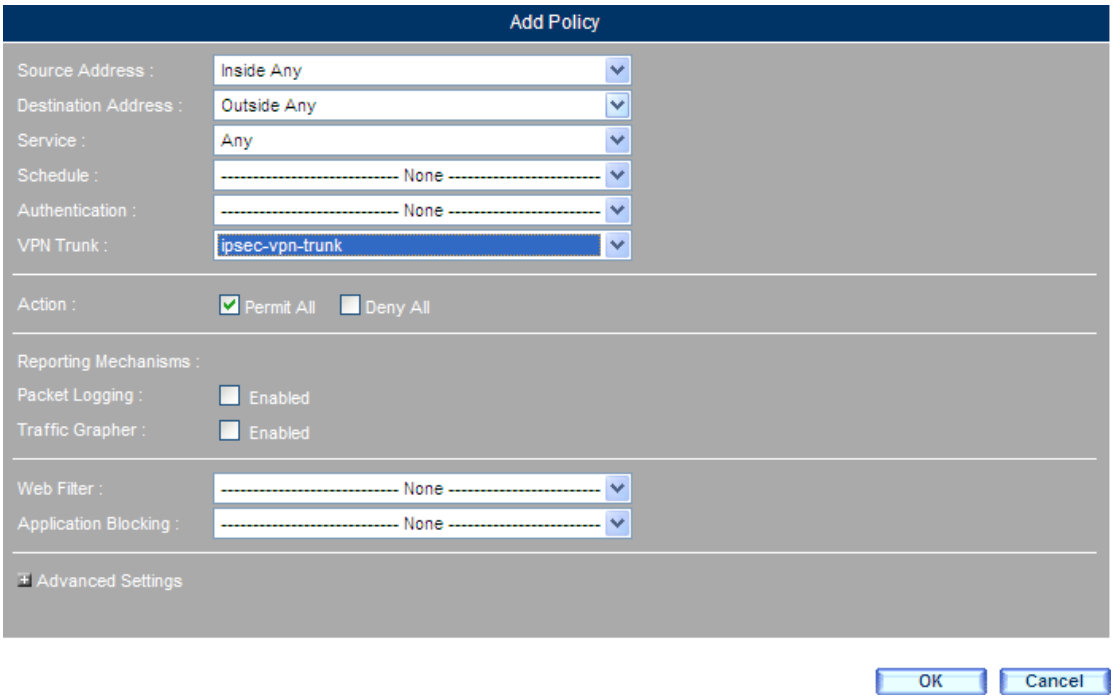


Figure 11-166 Configuring an Outgoing Policy with VPN Trunk

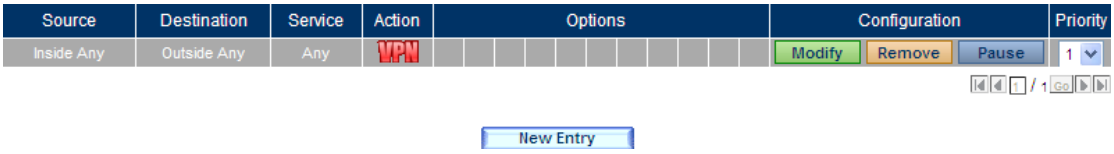


Figure 11-167 Policy Completed

Step 21. Under **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure11-168**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-169**）

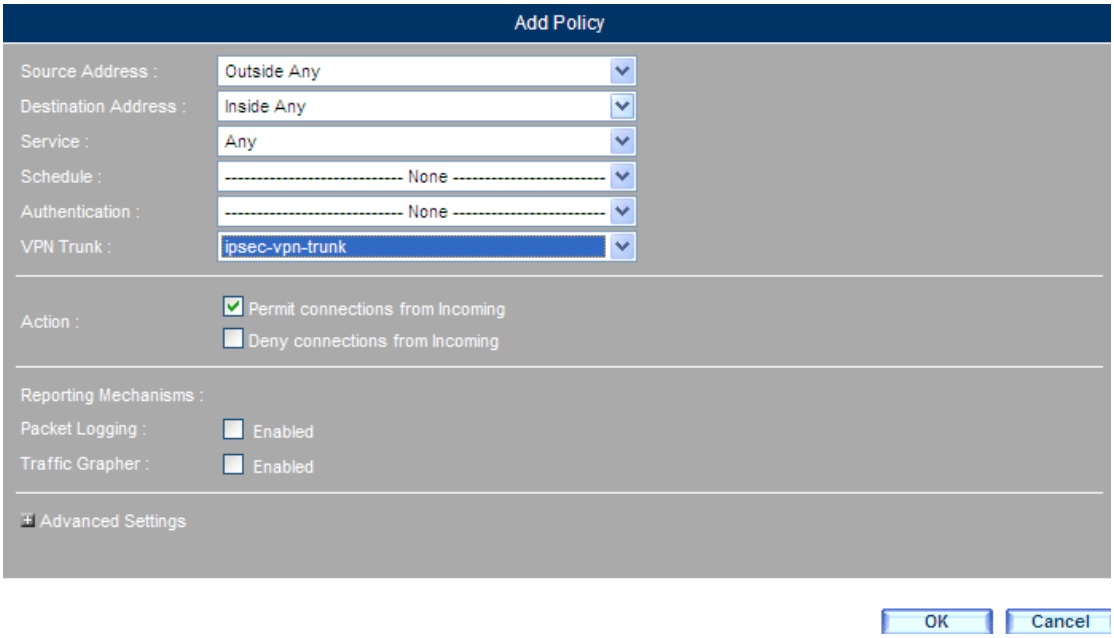


Figure 11-168 Configuring an Incoming Policy with VPN Trunk

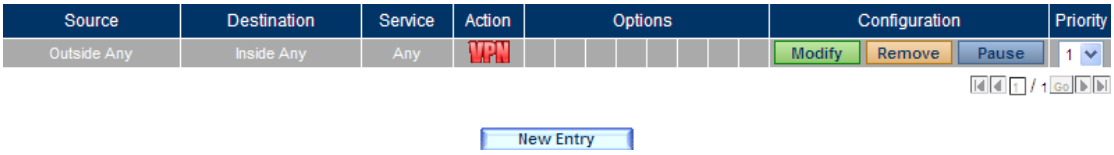


Figure 11-169 An Incoming Policy with VPN Trunk Completed

For B Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **IPSec Autokey**, and then click **New Entry**. （**Figure 11-170**）

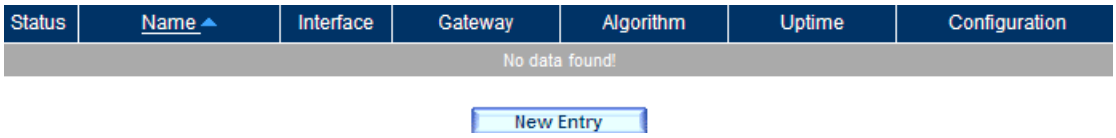


Figure 11-170 IPSec Autokey Screen

Step 2. Type VPN_01 in the **Name** field and then select **Port2(WAN1)** for WAN Interface.（**Figure 11-171**）

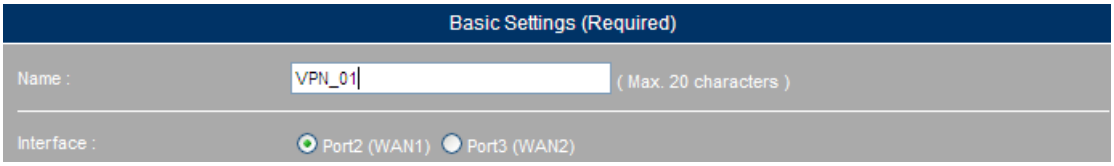


Figure 11-171 Name and WAN Interface Settings

Step 3. For **Remote Settings**, select **Remote Gateway (Static IP or Hostname)**, and enter the management address of A Company (WAN pot 1).（**Figure 11-172**）

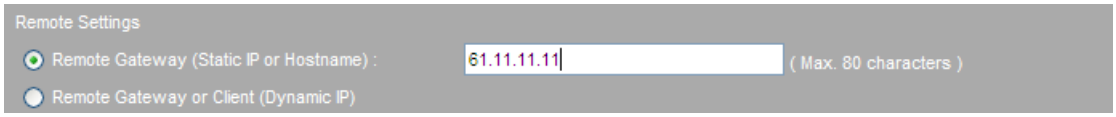


Figure 11-172 Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method** and enter the **Pre-Shared Key String**.（**Figure 11-173**）

Figure 11-173 IPSec Algorithm Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.（**Figure 11-174**）

Figure 11-174 ISAKMP Algorithm Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.（**Figure 11-175**）

Figure 11-175 IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.（**Figure 11-176**）

Figure 11-176 Advanced Settigs of IPSec Autokey

Step 8. For **GRE Tunnel Settings**, type “192.168.50.200” in the **Local Endpoint Address** field and “192.168.50.100” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)（**Figure 11-177**）

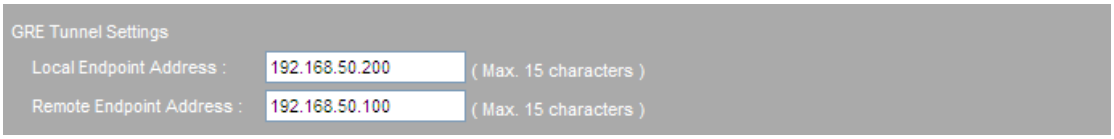


Figure 11-177 GRE Tunnel Settings

Step 9. Settings completed.（**Figure 11-178**）

Figure 11-178 IPSec Autokey Settings Completed

Step 10. Under **Policy Object > VPN > IPSec Autokey**, click **New Entry** again.

Step 11. Type VPN_02 in the **Name** field and then select Port3 (WAN2) for **Interface**.（**Figure 11-180**）

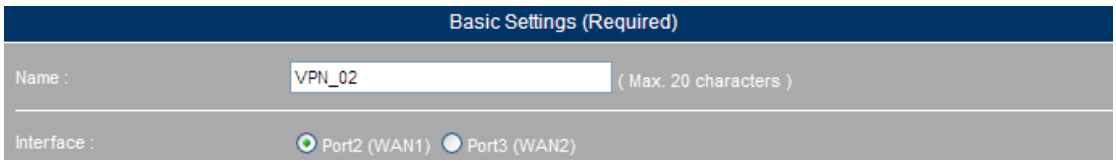


Figure 11-180 Name and Interface Settings

Step 12. Select **Remote Gateway (Static IP or Hostname)** for **Remote Settings**, and enter the management address of A Company (WAN port 2).（**Figure 11-181**）

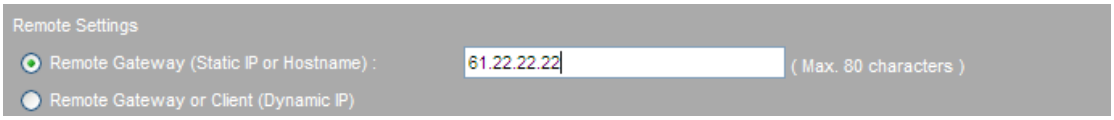


Figure 11-181 Remote Settings

Step 13. Select “Pre-Shared Key” for **Authentication Method** and enter the **Pre-Shared Key String**.（**Figure 11-182**）

Figure 11-182 Authentication Method Settings

Step 14. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.（**Figure 11-183**）

Figure 11-183 ISAKMP Algorithm Settings

Step 15. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication**

Algorithm.（Figure 11-184）

Figure 11-184 IPSec Algorithm Settings

Step 16. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.（Figure 11-185）

Figure 11-185 Advanced Settings of IPSec Autokey

Step 17. For **GRE Tunnel Settings**, type “192.168.60.200” in the **Local Endpoint Address** field and “192.168.60.100” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)（Figure 11-186）

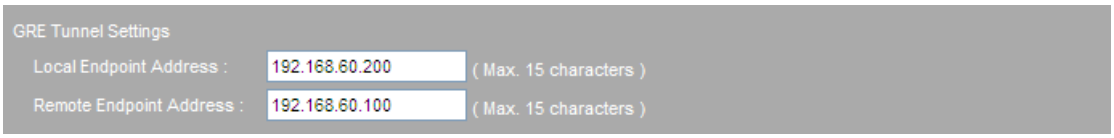


Figure 11-186 GRE Tunnel Settings

Step 18. Settings completed.（Figure 11-187）

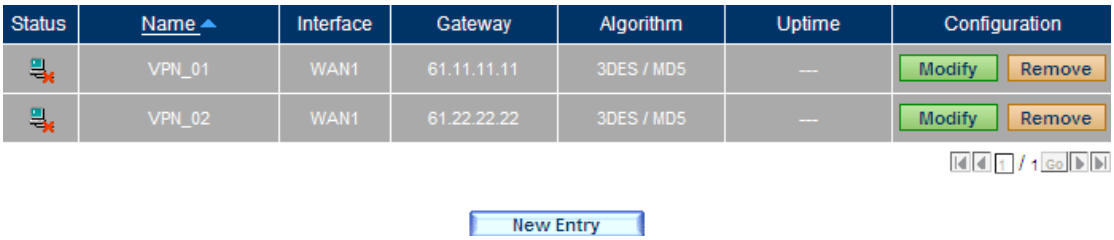


Figure 11-187 IPSec Autokey Settings Completed

Step 19. Under **Policy Object > VPN > Trunk**, set as below: （**Figure 11-188**）

- **Name**: Type a name.
- **Local Settings**: Select “LAN”. **Local IP / Netmask**: Type “192.168.20.0” as B Company’s subnet address and “255.255.255.0” as **Mask.**
- **Remote Settings**: Select **Remote IP / Netmask**. **Remote IP / Netmask**: Type “192.168.10.0” as A Company’s subnet address and “255.255.255.0” as **Mask**.
- **Tunnel**: Select “VPN_01” and “VPN_02” and then add them to the right column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-189**）

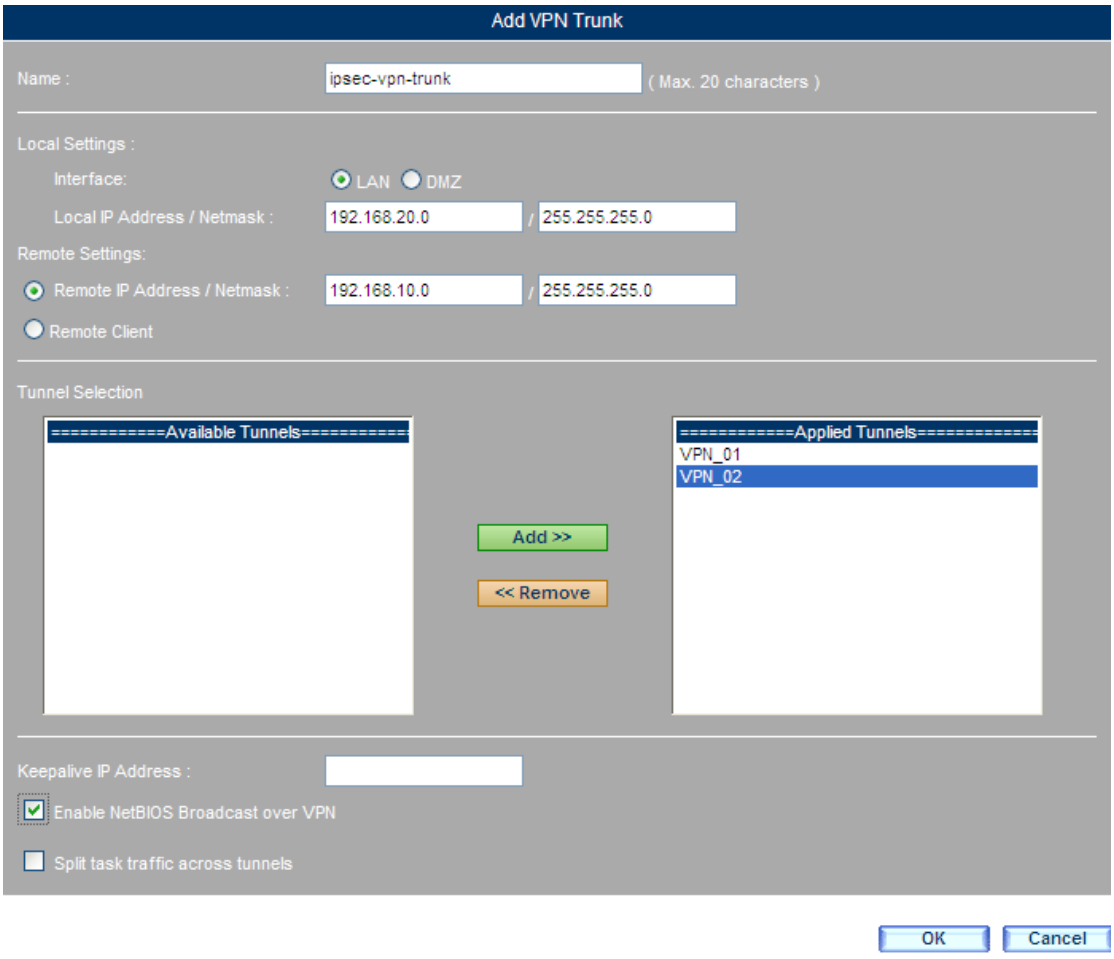


Figure 11-188 VPN Trunk Settings

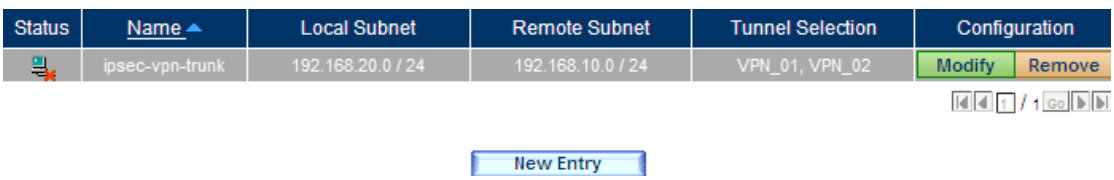


Figure 11-189 VPN Trunk Created

Step 20. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-190**）

- Select the defined trunk for **VPN Trunk**.
- Click OK.（**Figure 11-191**）

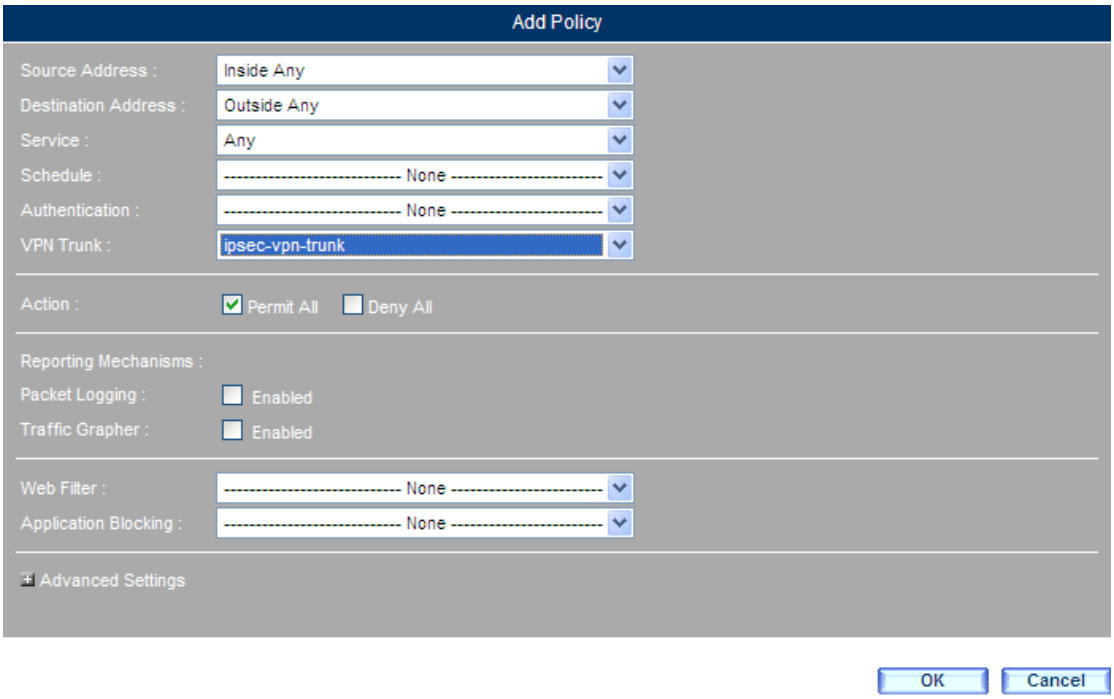


Figure 11-190 Using VPN Trunk in an Outgoing Policy

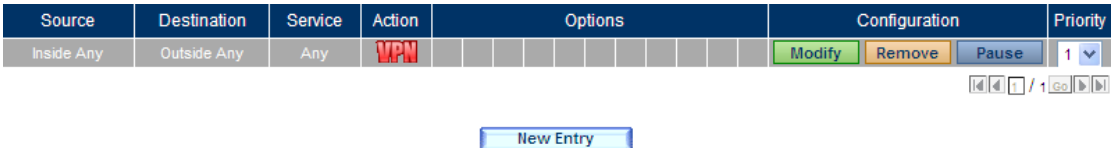


Figure 11-191 An Outgoing Policy with VPN Trunk

Step 21. Select **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-192**）

- Select the defined trunk for **VPN Trunk.**
- Click **OK**.（**Figure 11-193**）

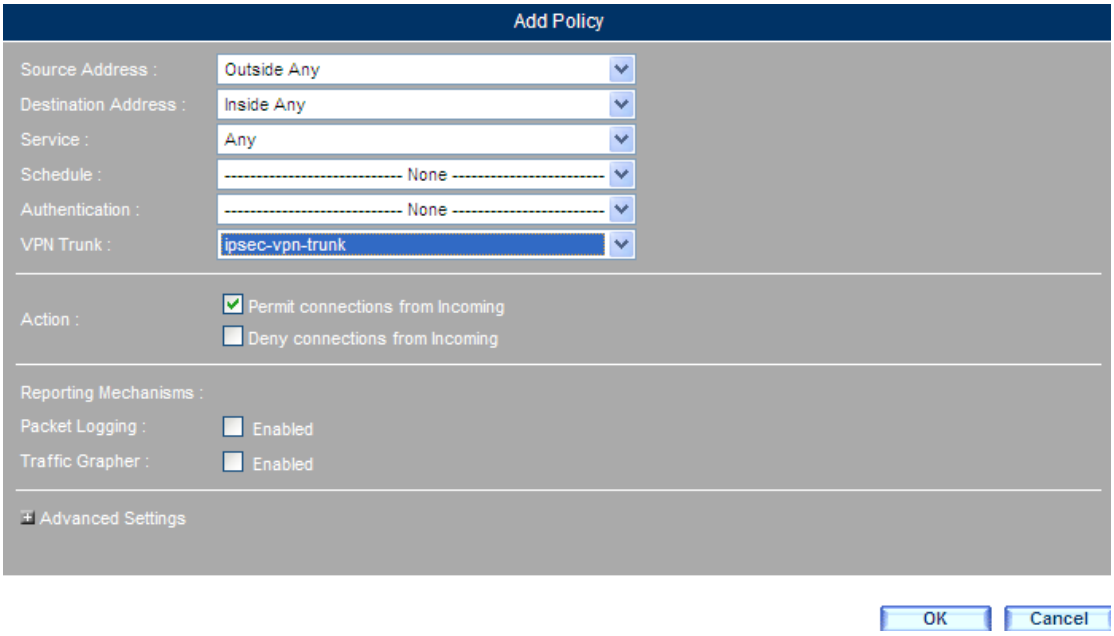


Figure 11-192 Using VPN Trunk in an Incoming Policy

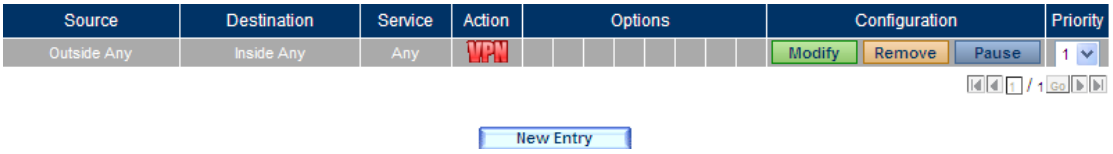


Figure11-193 An Incoming Policy with VPN Trunk

Step 22. Settings completed.（Figure 11-194）

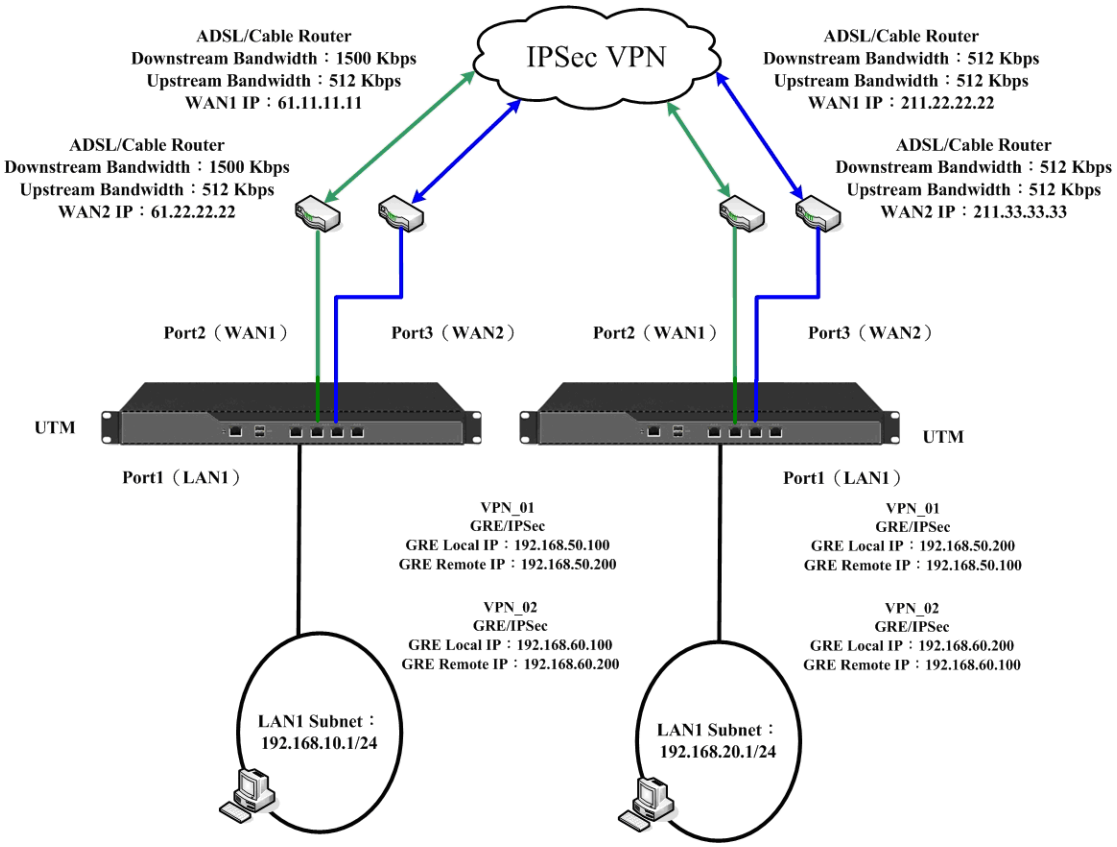


Figure 11-194 Deployment of IPSec VPN Using GRE/IPSec

11.1.5 Establishing an IPSec VPN Connection by Three

CS-2001 Devices

Prerequisite Setup (Note: IP addresses used as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP range: 192.168.10.x/24. Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1(192.168.20.1). IP range: 192.168.20.x/24. Configure Port2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

C Company: Configure Port1 as LAN1(192.168.30.1). IP range:192.168.30.x/24. Configure Port2 as WAN1(121.33.33.33) and connect it to the ADSL Termination Unit Remote to access the Internet.

This example is to use three CS-2001 devices to establish VPN connection among A Company, B Company and C Company.

For A Company, set as below:

Step1. Go to **Policy Object** > **VPN** > **IPSec Autokey** and then click **New Entry**. （**Figure 11-195**）

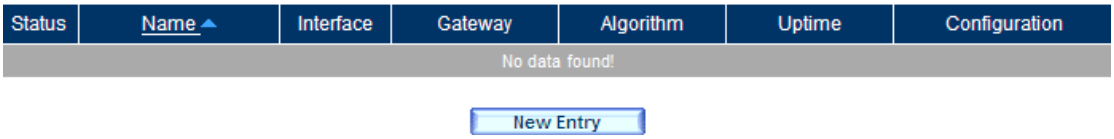


Figure 11-195 IPSec Autokey

Step2. Type VPN_01 in the **Name** field and then select Port2(WAN1) for **Interface**.（**Figure 11-196**）

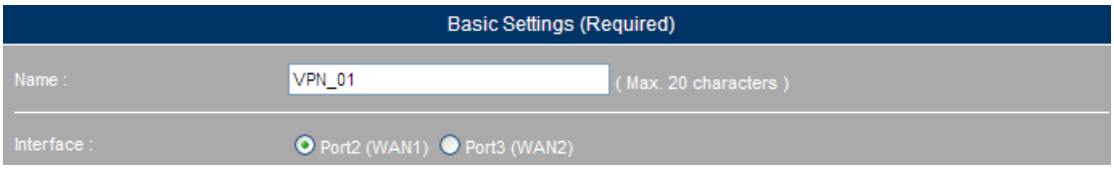


Figure 11-196 Configuring the Name and the Interface

Step3. Under the **Remote Settings** section, select the **Remote Gateway (Static IP or Hostname)** and then fill the blank.（**Figure 11-197**）

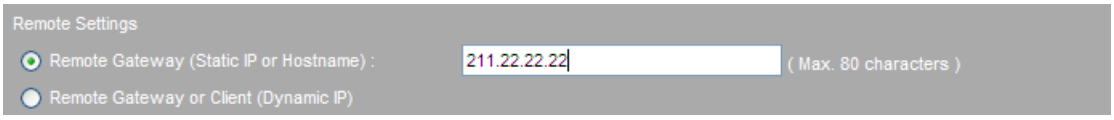


Figure 11-197 Configuring the Static IP or Hostname

Step4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**. （**Figure 11-198**）

Figure 11-198 Configuring the Authentication Method

Step5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH 1 for Key **Group**.（**Figure 11-199**）

Figure 11-199 Configuring the IPSec Algorithm

Step6. Under the **IPSec Algorithm** section, select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.（**Figure 11-200**）

Figure 11-200 Configuring the IPSec Algorithm

Step7. Under the **Advanced Settings (optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPSec SA Lifetime** field and then select Main mode for **Mode**.（**Figure 11-201**）

Figure 11-201 Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step8. Policy Created.（Figure 11-202）

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	---	Modify Remove

1 / 1 Go

New Entry

Figure 11-202 Policy Created

Step9. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（Figure 11-203）

- Type the name in the **Name** field.
- **Local Settings**: select LAN. Enter the local subnet and the mask.
- Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the local subnet and the mask.
- Move the VPN_01 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（Figure 11-204）

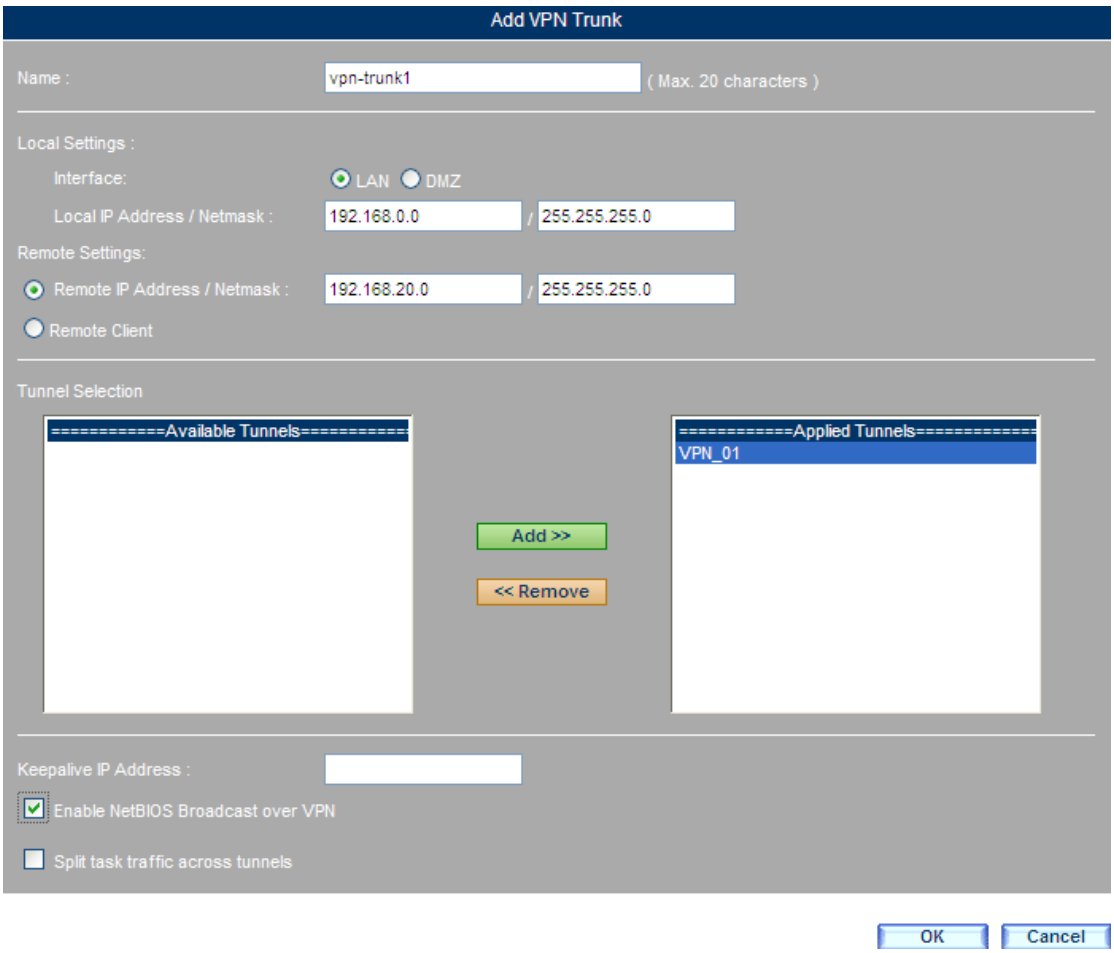


Figure 11-203 Configuring the First Trunk

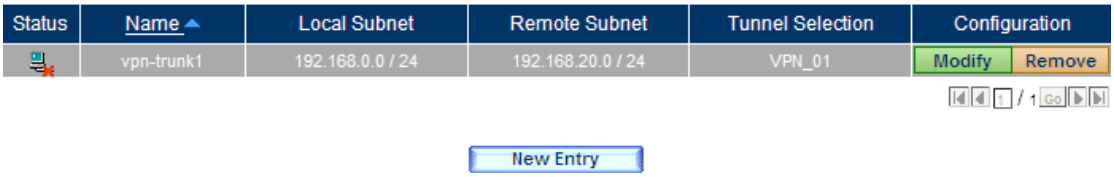


Figure 11-204 First Trunk Completed

Step10. Go to **Policy Object** > **VPN** > **IPSec Autokey** and then click the **New Entry** button again.（**Figure 11-205**）

Figure 11-205 The IPSec Autokey Page

Step11. Type VPN_02 in the **Name** field and then select Port2(WAN1) for the **Interface**.（**Figure 11-206**）

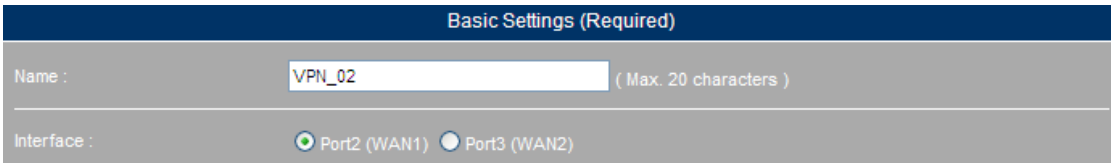


Figure 11-206 Configuring the Name and the Interface

Step12. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then fill the field.（**Figure 11-207**）

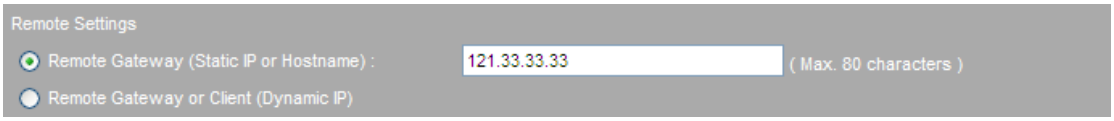


Figure 11-207 Configuring the Remote Gateway –Fixed IP or Domain Name

Step13. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.（**Figure 11-208**）

Figure 11-208 Configuring the Authentication Method

Step14. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH

1 for **Key Group**.（**Figure 11-209**）

Figure 11-209 Configuring ISAKMP Algorithm

Step15. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and MD5 for **Authentication Algorithm**.（**Figure 11-210**）

Figure 11-210 Configuring IPSec Algorithm

Step16. Under the **Advanced Settings (Optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPSec SA Lifetime** field and then select Main mode for **Mode**.（**Figure 11-211**）

Figure 11-211 Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step17. Policy created.（**Figure 11-212**）

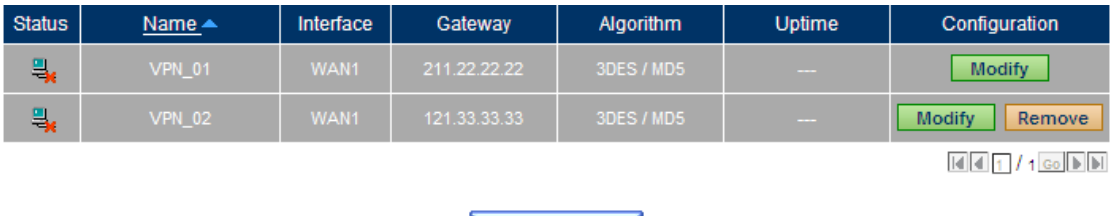


Figure 11-212 Policy Created

Step18. Go to **Policy Object** > **VPN** > **Trunk**, click **New Entry** and then set as below:（**Figure 11-213**）

- Type the name in the **Name** field.
- **Local Settings**: select LAN. Enter the IP address and the Mask in the **Local IP / Netmask** field.
- Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the subnet and the mask.
- Move the **VPN_02** from the **Available Tunnels** to the **Selected Tunnels**.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-214**）

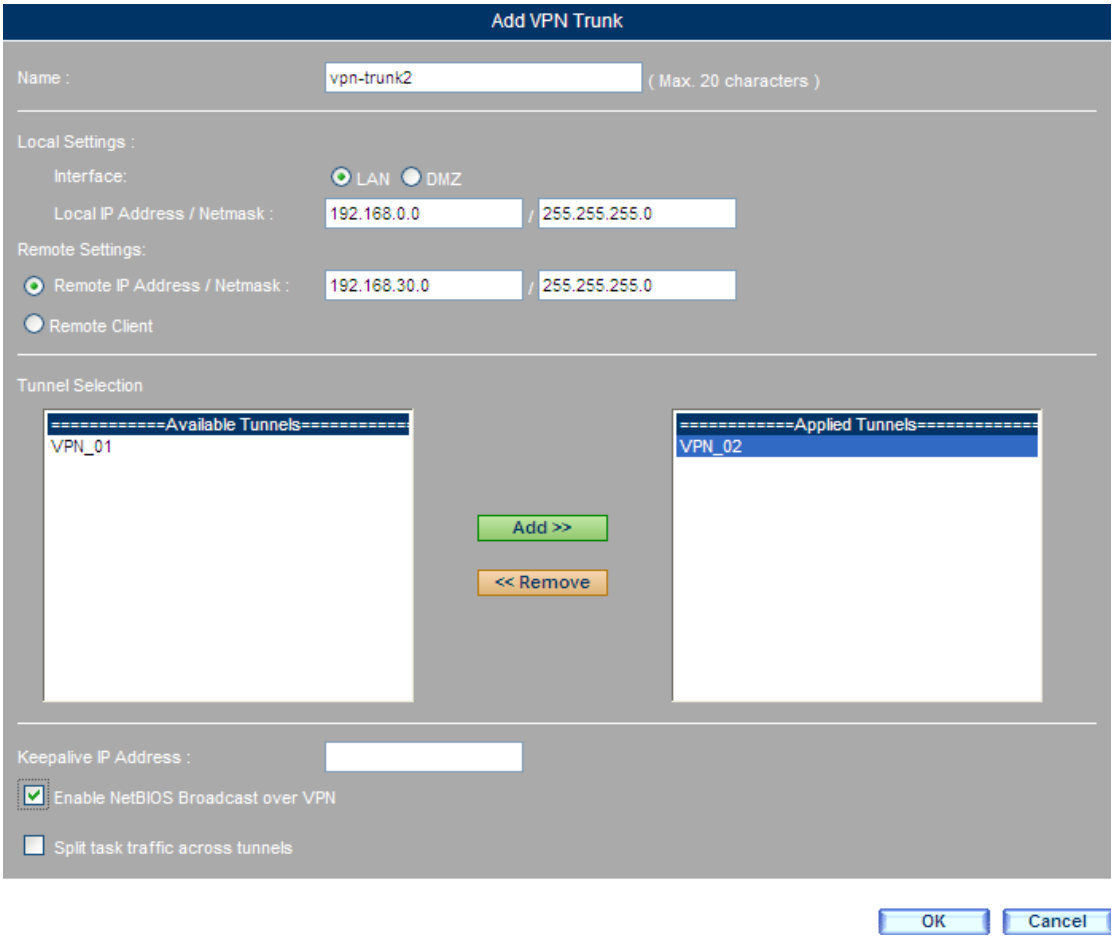


Figure 11-213 Configuring the Second Trunk

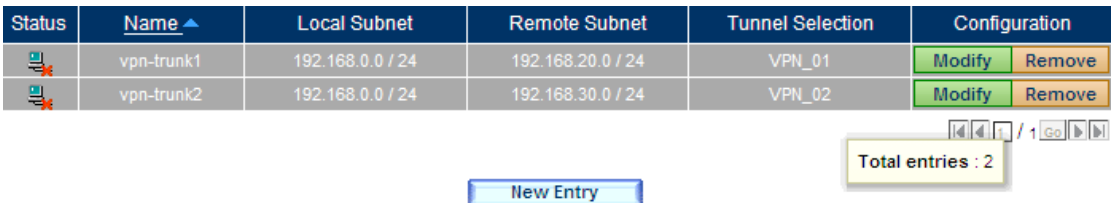


Figure 11-214 The Second Trunk Created

Step19. Go to **Policy Object** > **VPN** > **Trunk Group**, click **New Entry** and then set as below:（**Figure 11-215**）

- Type the name in the **Name** field.
- Move the IPSec_VPN_Trunk_01(LAN) and IPSec_VPN_Trunk_02(LAN) from the **Available Trunks** column to the **Selected Trunks** column.
- Click **OK**.（**Figure 11-216**）

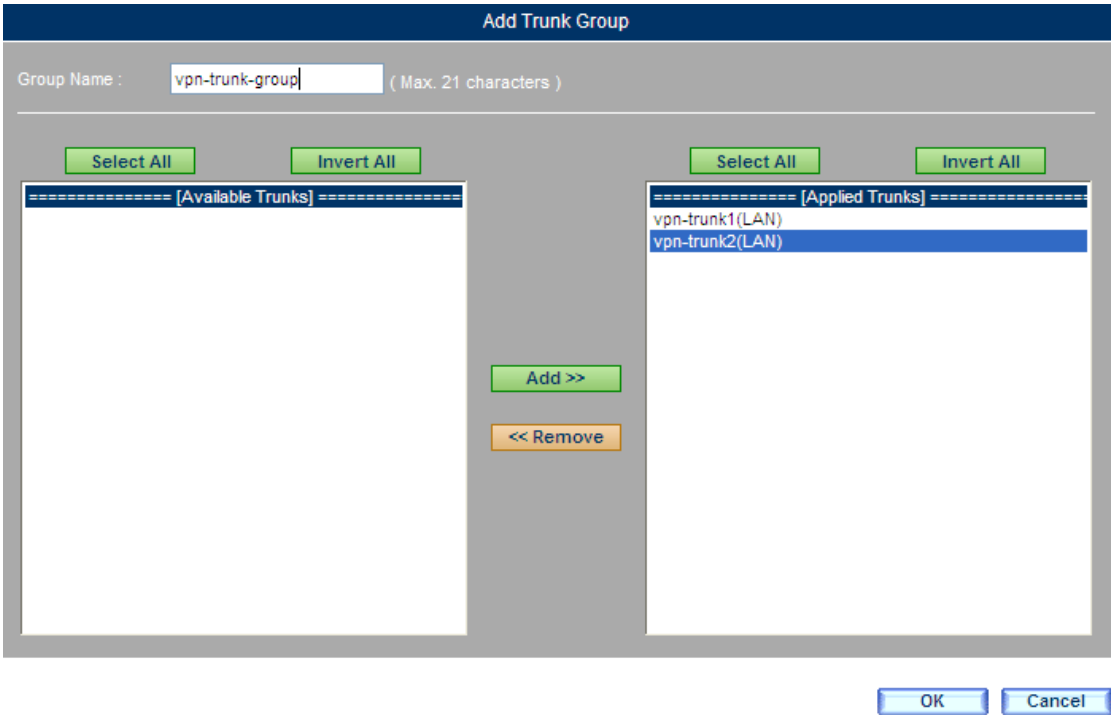


Figure 11-215 Configuring the Trunk Group

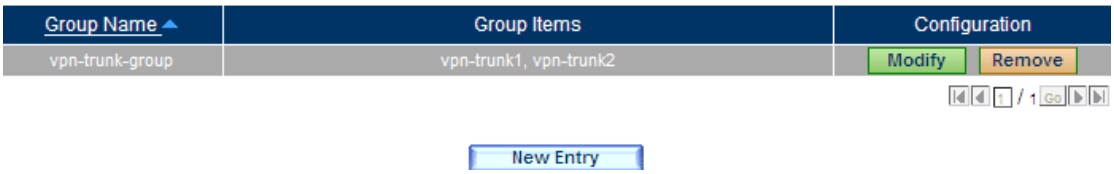


Figure 11-216 Trunk Group Created

Important：

1. Under **Policy Object** > **VPN** > **Trunk**, B Company and C Company's subnet should be on A Company's subnet.

Step20. Under **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-217**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-218**）

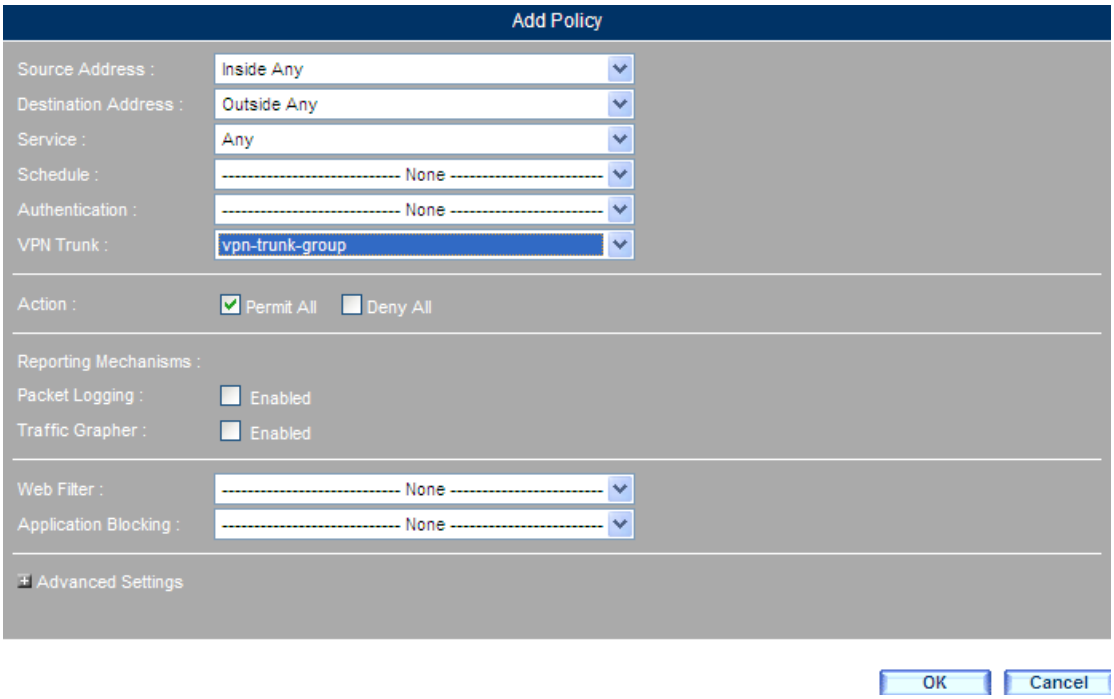


Figure 11-217 Configuring the Outgoing Policy with VPN Trunk

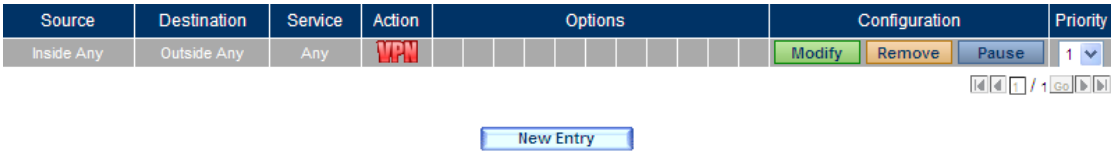


Figure 11-218 Policy Created

Step21. Go to **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-219**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-220**）

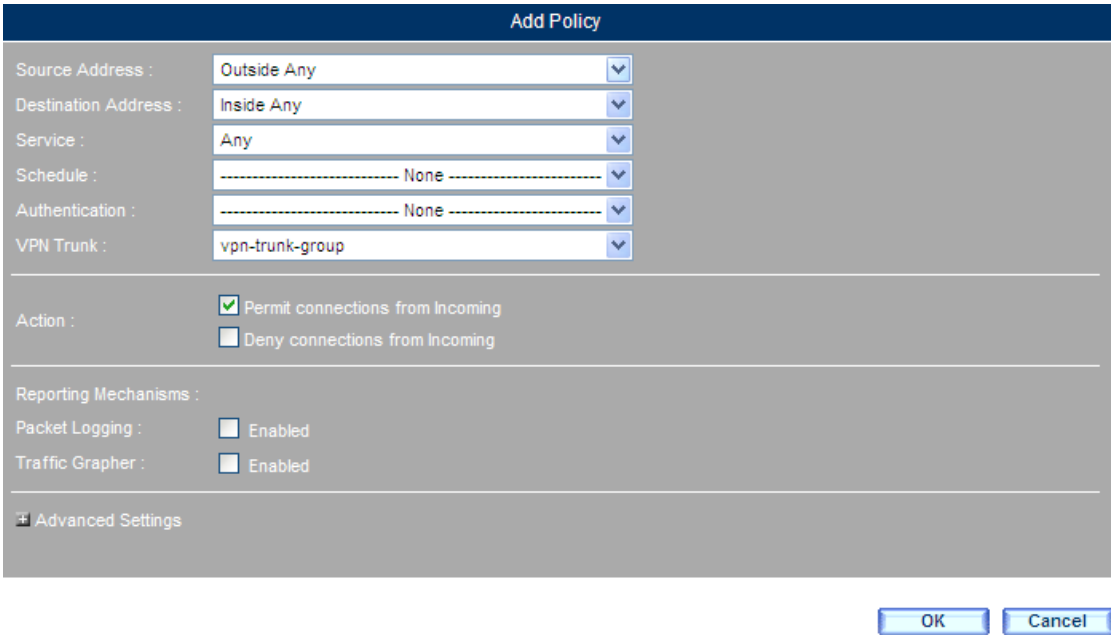


Figure 11-219 Configuring an Incoming Policy with VPN Trunk

Figure 11-220 Policy Created

For B Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **IPSec Autokey** and then click the **New Entry** button.（**Figure 11-221**）

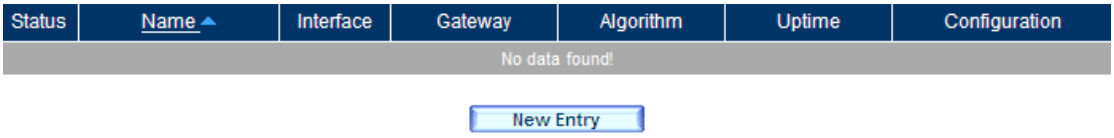


Figure 11-221 The IPSec Autokey Page

Step 2. Type VPN_01 in the **Name** field and then select Port2(WAN1) for **Interface**.（**Figure 11-222**）

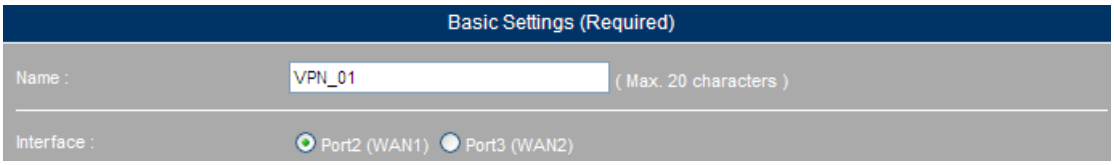


Figure 11-222 Configuring the Name and the Interface

Step 3. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then enter A Company's IP.（**Figure 11-223**）

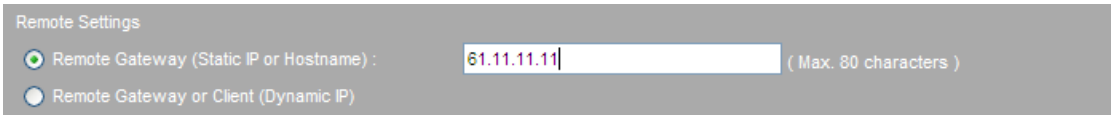


Figure 11-223 Configuring the Remote Settings

Step 4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.（**Figure 11-224**）

Figure 11-224 Configuring the Authentication Method

Step 5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH for **Key Group**.（**Figure 11-225**）

Figure 11-225 Configuring the ISAKMP Algorithm

Step 6. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.（**Figure 11-226**）

Figure 11-226 Configuring the IPSec Algorithm

Step 7. Under the **Advanced Settings (optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPSec SA Lifetime** field and then select Main mode for **Mode**. （**Figure 11-227**）

Figure 11-227 Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step 8. Setting completed.（**Figure 11-228**）

Figure 11-228 IPSec Setting Completed

Step 9. Under **Policy Object** > **VPN** > **Trunk**, click the **New Entry** button and then set as below:（**Figure 11-229**）

- Type the name in the **Name** field.
- **Local Settings**: Select LAN. **Local IP / Netmask**: Enter the subnet and the mask.
- Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the subnet and mask.
- Move VPN_01 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-230**）

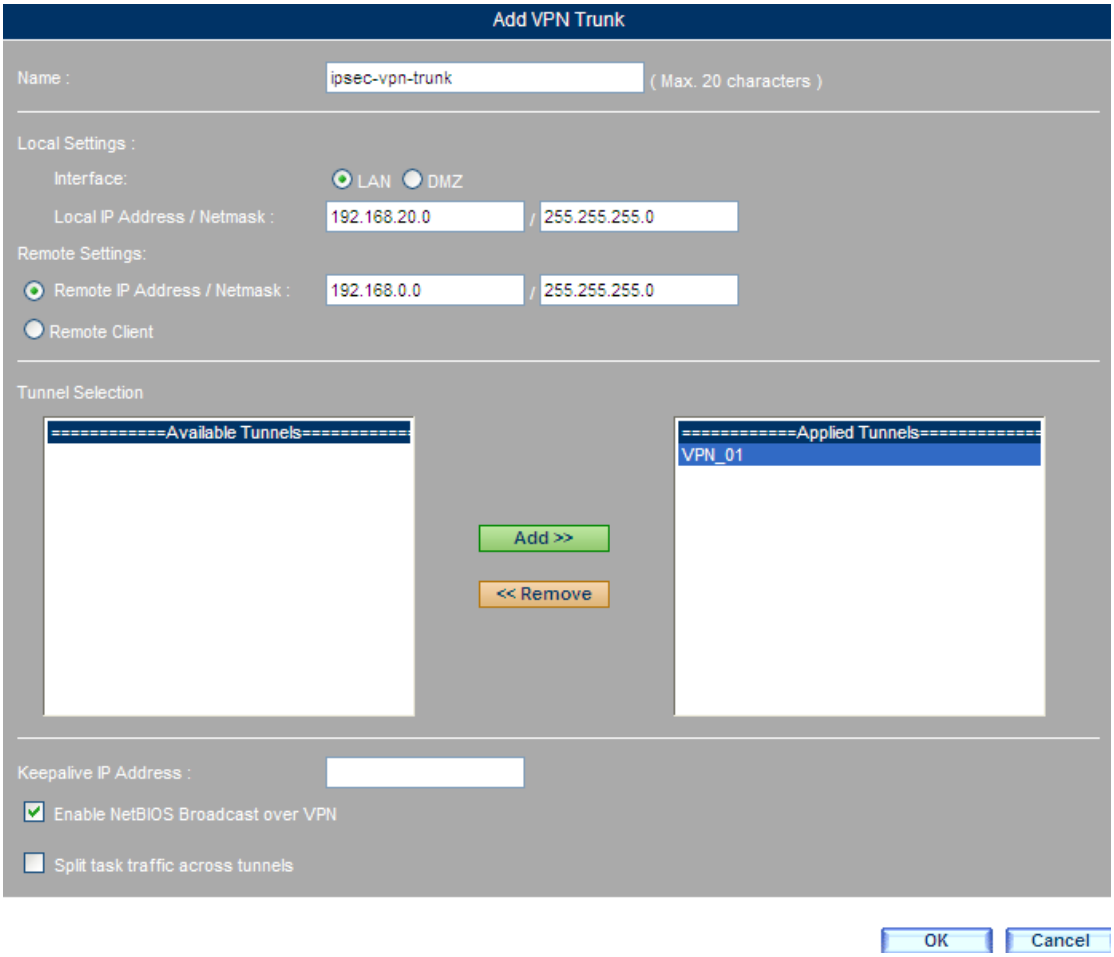


Figure 11-229 Configuring the Trunk

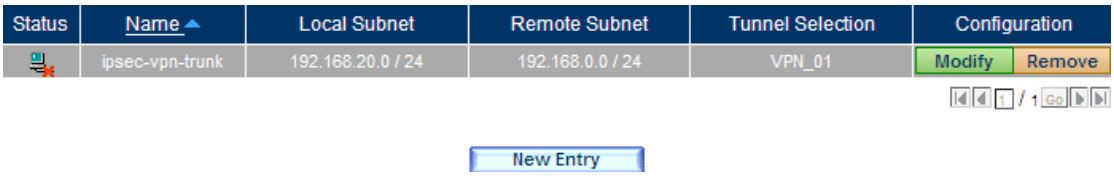


Figure 11-230 Setting Completed

Step 10. Go to **Policy Outgoing**, click the **New Entry** button and then set as below:（**Figure 11-231**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-232**）

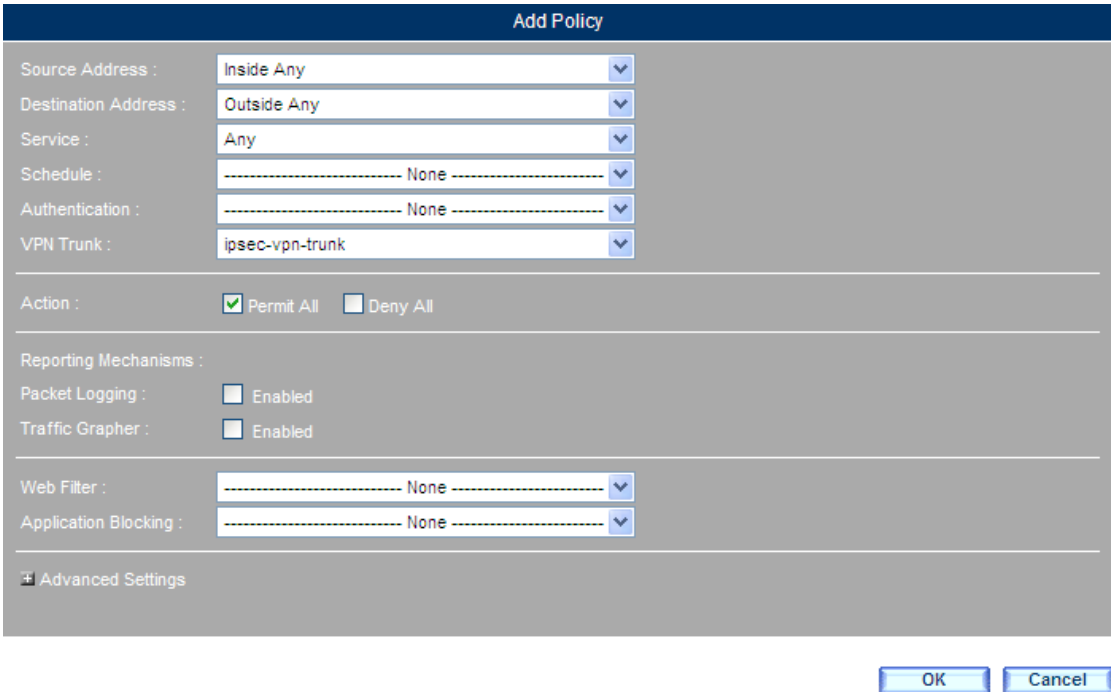


Figure 11-231 Configuring an Outgoing Policy with VPN Trunk

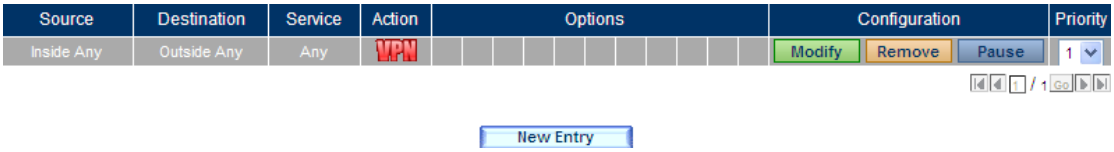


Figure 11-232 A Policy with VPN Trunk Created

Step 11. Go to **Policy** > **Incoming**, click the **New Entry** button and then set as below:（**Figure 11-233**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-234**）

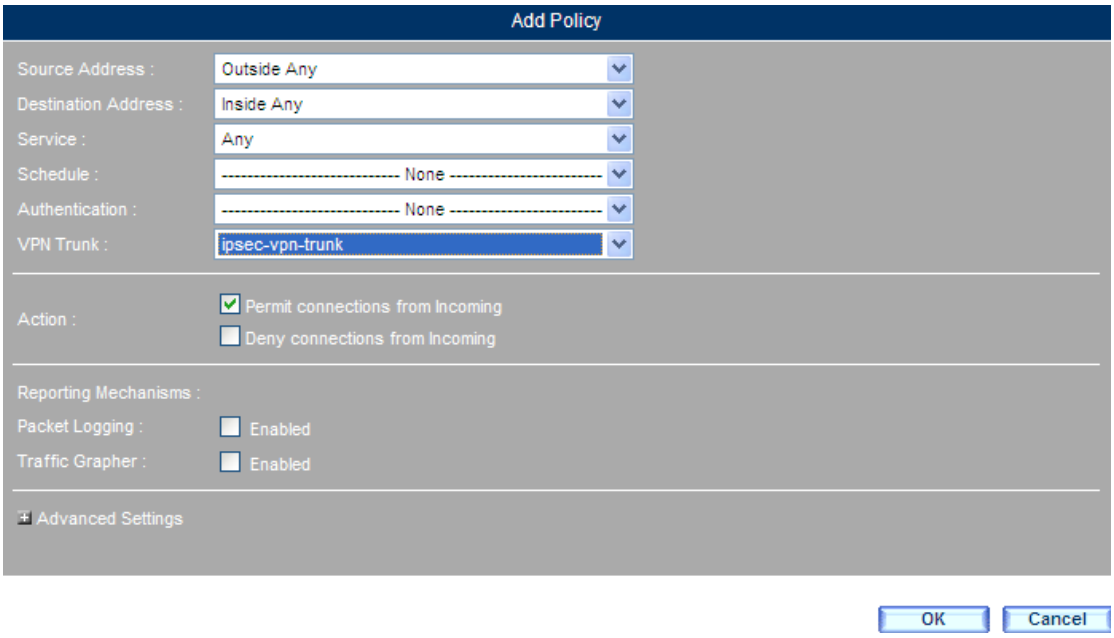


Figure 11-233 Configuring an Incoming Policy with VPN Trunk

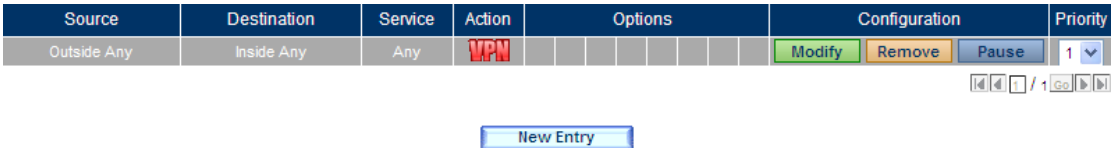


Figure 11-234 A Policy with VPN Trunk Created

For C Company, set as below:

Step 1. Under **Policy Object > VPN > IPSec Autokey**, click the **New Entry** button and then set as below:（**Figure 11-235**）

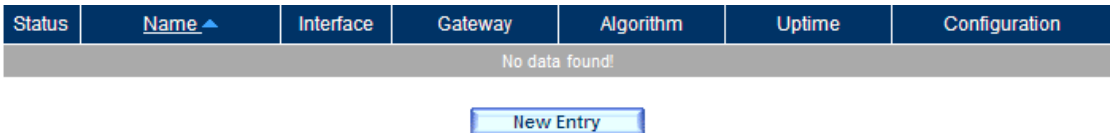


Figure 11-235 The IPSec Autokey Page

Step 2. Enter the name in the **Name** field and then select Port2(WAN1) for **Interface**.（**Figure 11-236**）

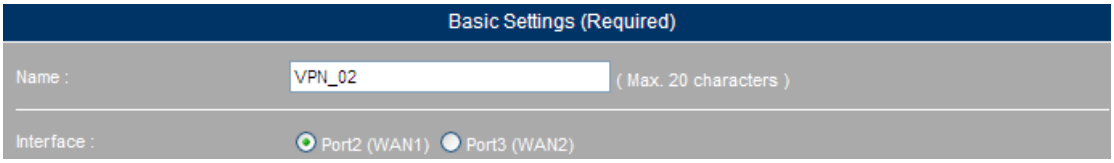


Figure 11-236 Configuring the Name and the Interface

Step 3. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then enter A Company's IP in the field.（**Figure 11-237**）

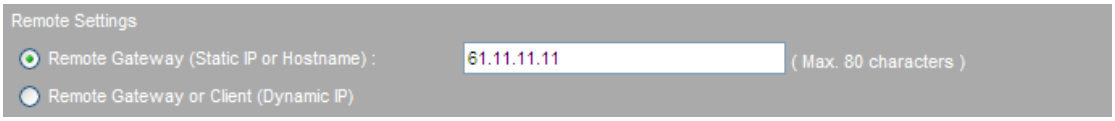


Figure 11-237 Configuring the Remote Settings

Step 4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.（**Figure 11-238**）

Figure 11-238 Configuring the Authentication Method

Step 5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH for **Key Group**.（**Figure 11-239**）

Figure 11-239 Configuring the ISAKMP Algorithm

Step 6. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.（**Figure 11-240**）

Figure 11-240 Configuring the IPSec Algorithm

Step 7. Under the **Advanced Settings (optional)** section, select GROUP 1 from the **PFS Key Group** drop-down list. Enter 3600 in the **ISAKMP SA Lifetime** field and then enter 28800 in the **IPSec SA Lifetime** field.（**Figure 11-241**）

Figure 11-241 Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step 8. Setting completed.（**Figure 11-242**）

Figure 11-242 Setting Completed

Step 9. Go to **Policy Object > VPN > Trunk**, click the **New Entry** button and then set as below:（**Figure 11-243**）

- Type the name in the **Name** field.
- **Local Settings** : Select LAN. Enter C Company's subnet / mask 192.168.30.3 / 255.255.255.0 in the field.
- Under the **Remote Settings** section, type A Company's subnet / mask 192.168.0.0 / 255.255.255.0 in the field.
- Move VPN_02 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click OK.（**Figure 11-244**）

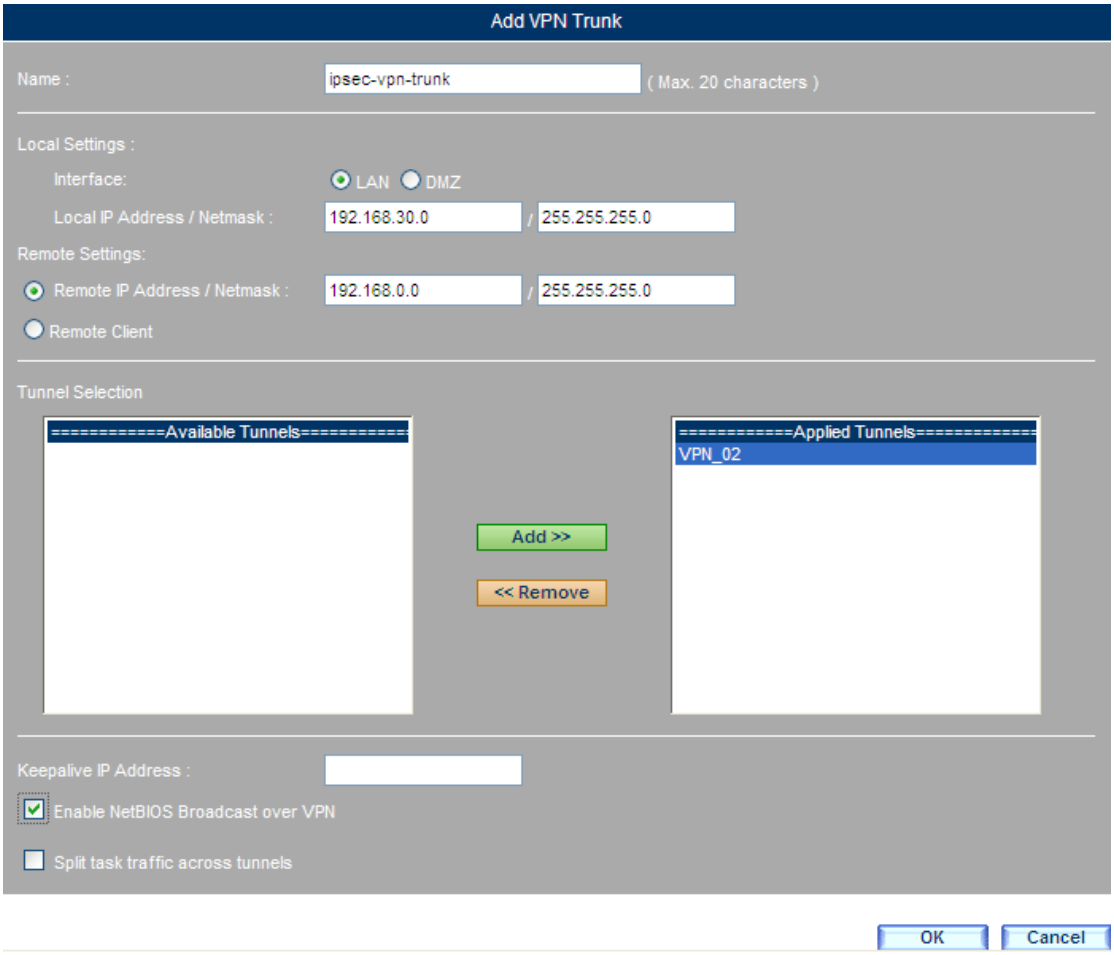


Figure 11-243 Configuring the Trunk

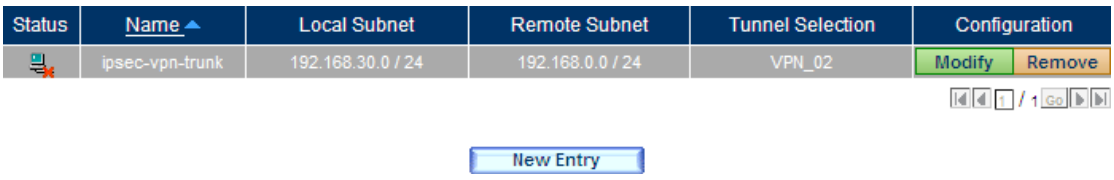


Figure 11-244 Setting Completed

Step 10. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below: （**Figure 11-245**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-246**）

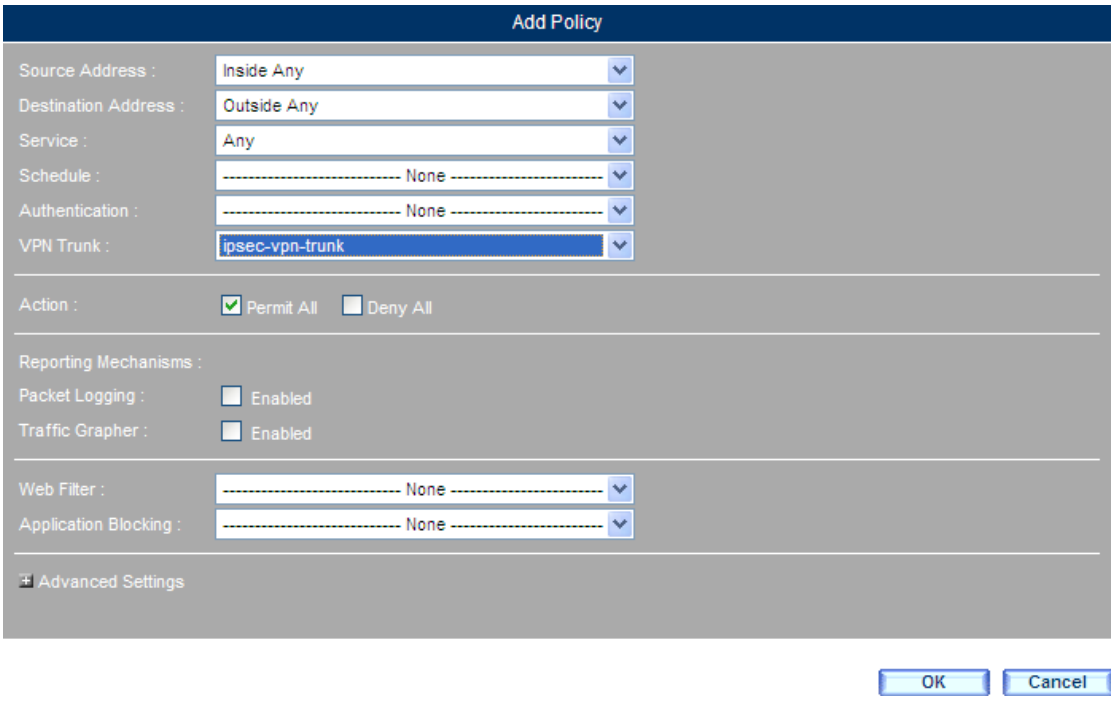


Figure 11-245 Configuring an Outgoing Policy

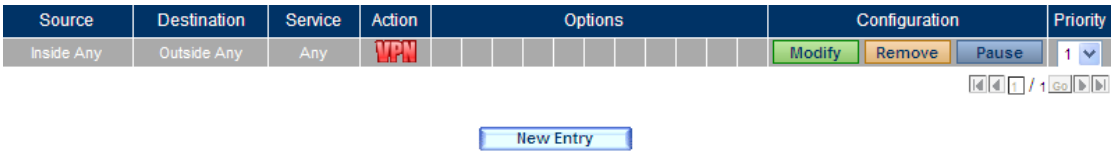


Figure 11-246 Policy Completed

Step 11. Go to **Policy** > **Incoming**, click **New Entry** and then set as below: （**Figure 11-247**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-248**）

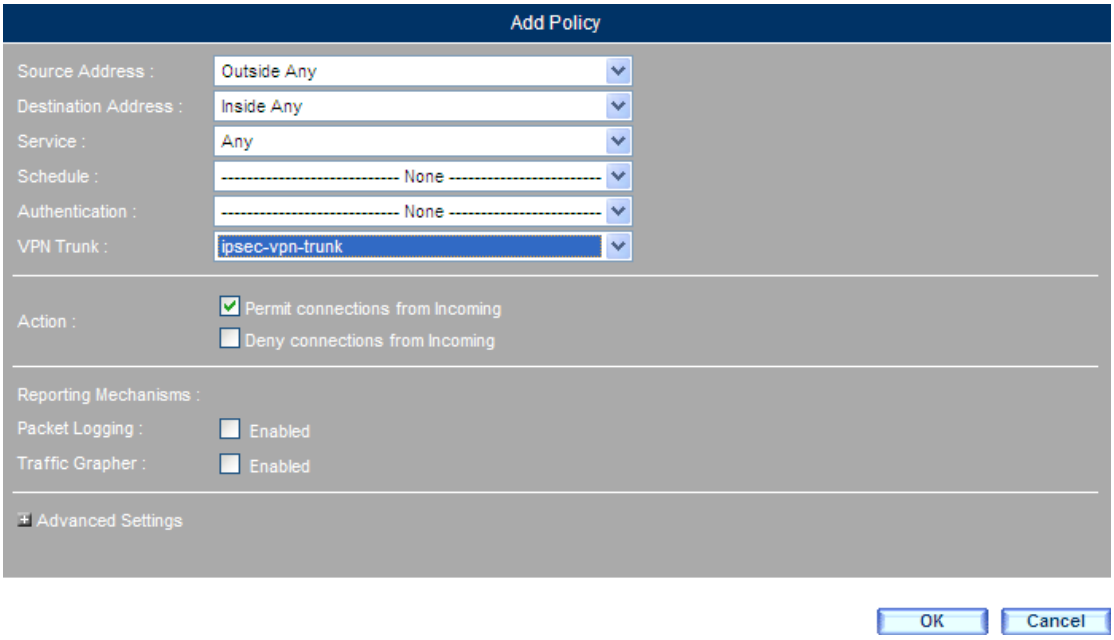


Figure 11-247 Configuring an Incoming Policy

Figure 11-248 Setting Completed

Step 12. Setting completed.（**Figure 11-249**）

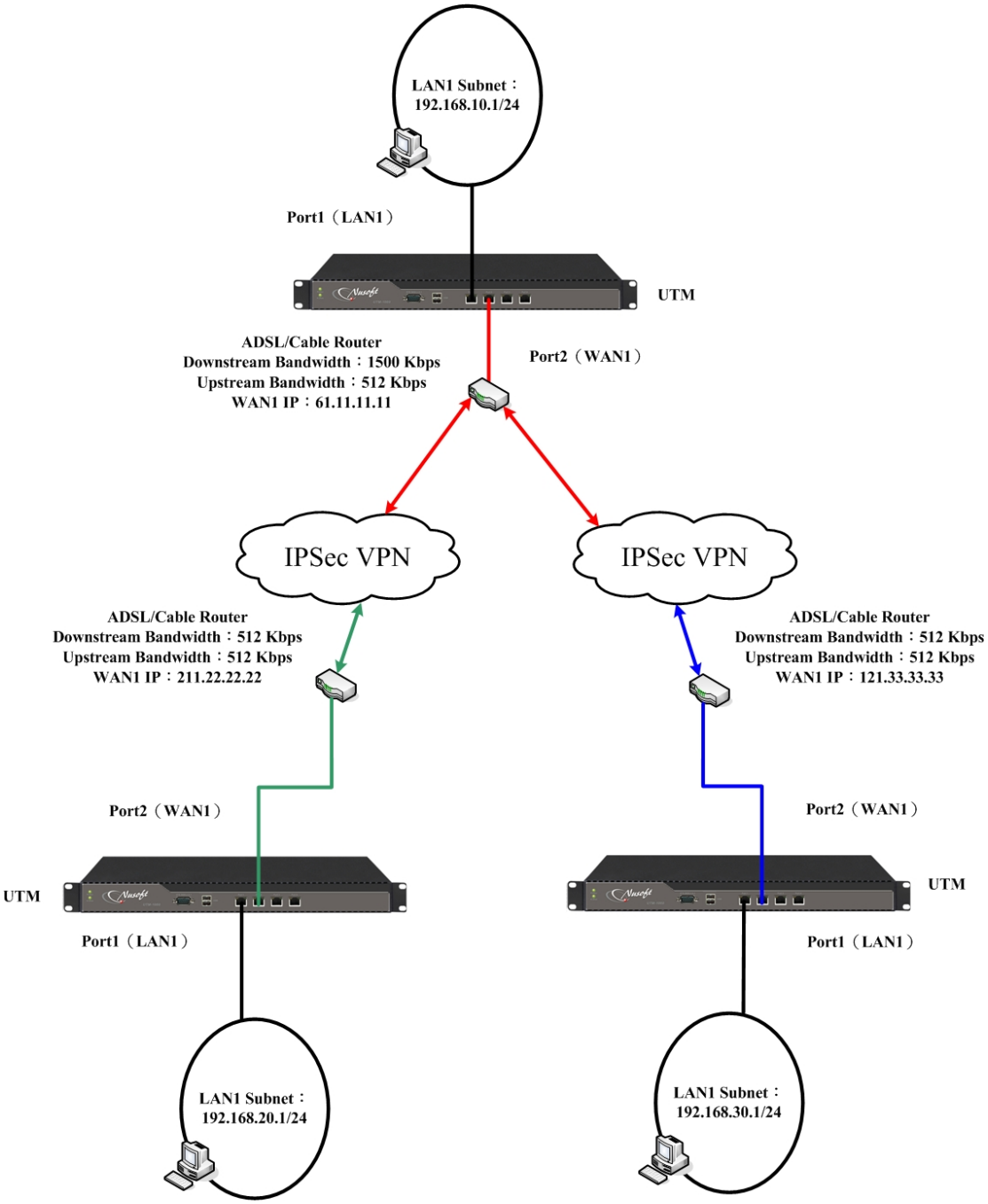


Figure 11-249 The Deployment of IPSec VPN

11.1.6 Using Two CS-2001 Devices to Establish PPTP VPN

Connection (Outbound Load Balancing)

Prerequisite Setup (Note: IP address used as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP range: 192.168.10.x/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Configure Port3 as WAN2(61.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1(192.168.20.1). IP range:192.168.20.x/24.
Configure Port2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Configure Port3 as WAN2(211.33.33.33) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

A Company's WAN port 1 and B Company's WAN port 1;
A Company's WAN port 2 and B Company's WAN port 2.

This example is to use two CS-2001 devices to establish VPN connection between A Company and B Company.

For A Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **PPTP Server** and then set as below: (**Figure 11-250**)

- Click the **Modify** button.
- Tick **Enable PPTP.**
- Tick **Encryption.**
- Tick **Allow Internet access via** and then select the port.
- **Auto-disconnect if idle for**: type 0.
- Enter the **Client IP – IP Range**.
- Click **OK**.

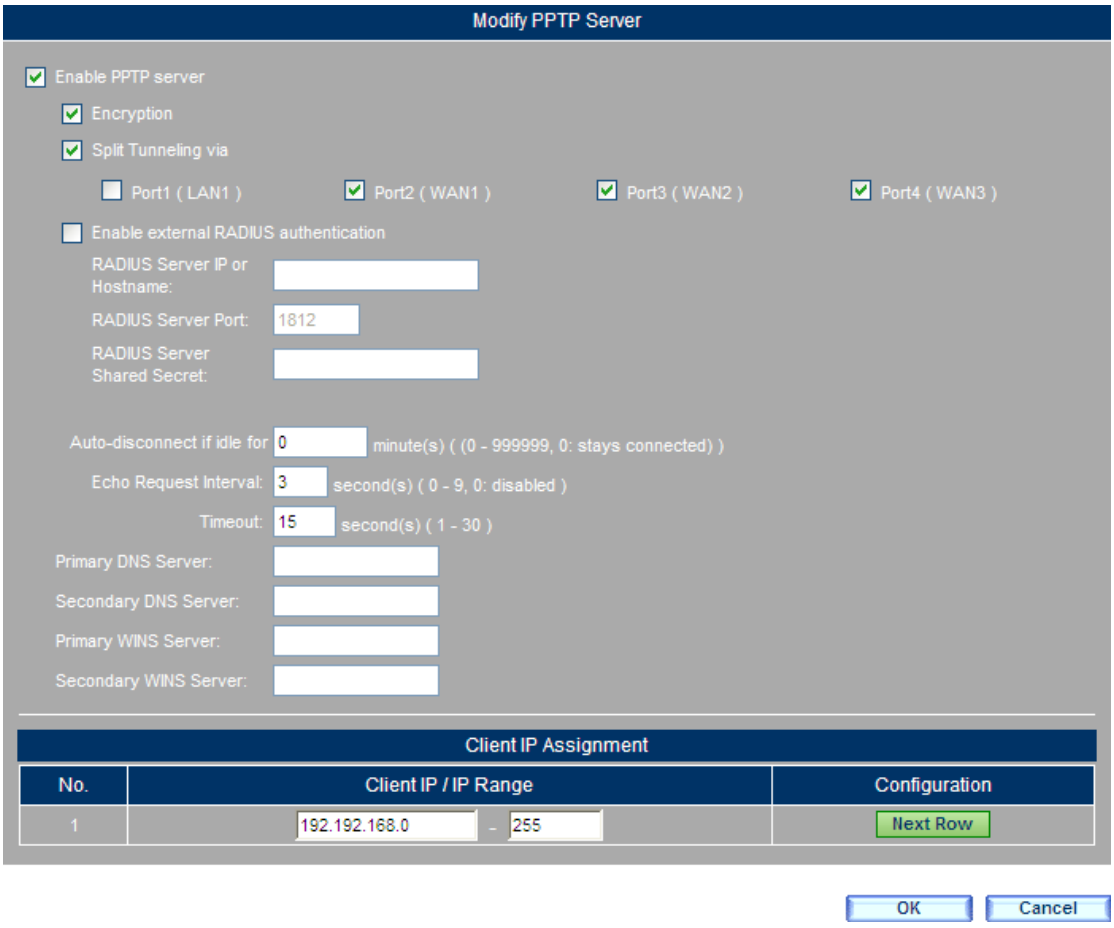


Figure 11-250 Enabling the PPTP Server

Note：

1. The IT administrator may enable or disable the external users to access the Internet via the CS-2001 device when they establish a VPN connection with the CS-2001 device.
2. **Auto-disconnect if idle for**: if the VPN connection is idle for the defined times, it will be disconnected automatically.

3. Using RADIUS Server (refer to chapter 8 for RADIUS authentication) to establish PPTP VPN connection, go to **Policy Object > VPN > PPTP Server** and create a PPTP Server setting of which **User Name** is"*" and the **Password** is "@radius" for RADIUS authentication.

Step 2. Go to **Policy Object > VPN > PPTP Server** and then set as below:

- Click the **New Entry** button.（**Figure 11-251**）
- Type PPTP_01 in the **Username** field.
- Type 123456789 in the **Password** field.
- Select **IP Range** under **Client IP(s) assigned from**.
- Click **OK**.（**Figure 11-252**）
- Click the **New Entry** again.（**Figure 11-253**）
- Type PPTP_02 in the **Username** field.
- Type 987654321 in the **Password** field.
- Tick **IP Range** under **Client IP(s) assigned from.**
- Click **OK**.（**Figure 11-254**）

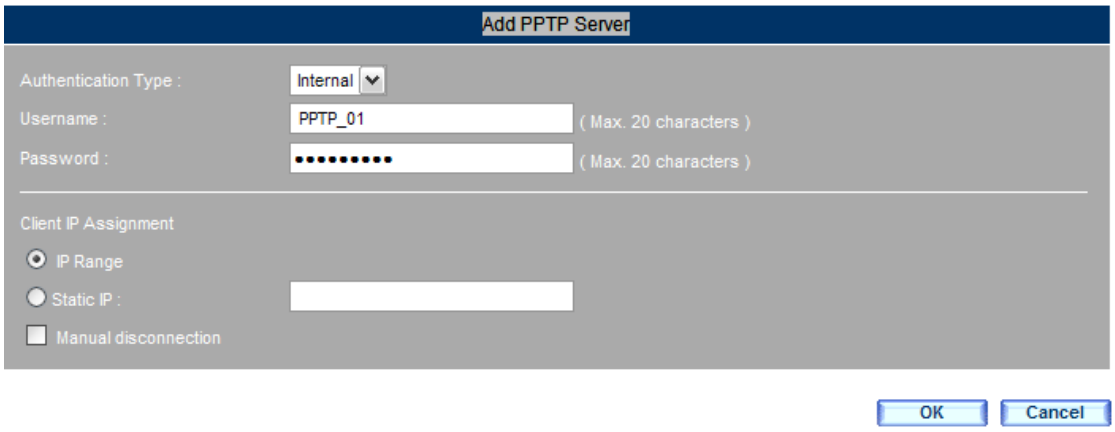


Figure 11-251 Configuring the First PPTP Server

Figure 11-252 First PPTP Server Completed

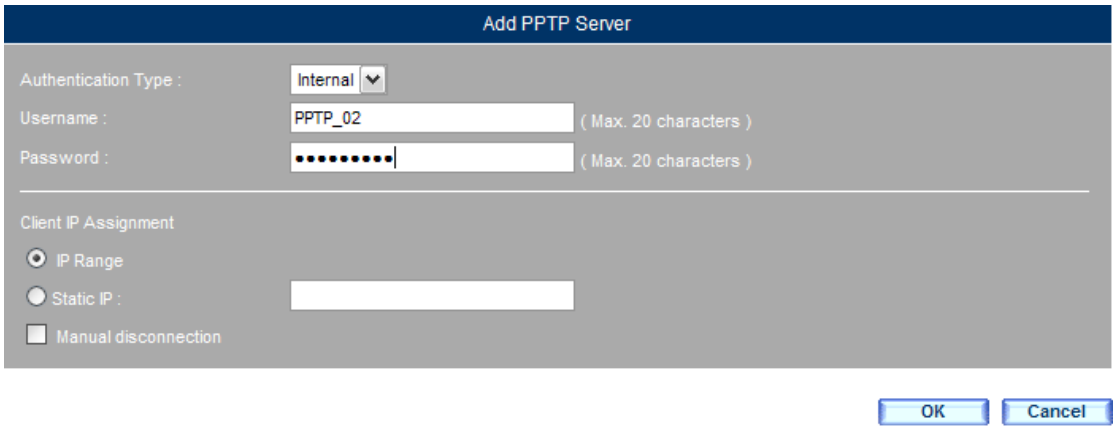


Figure 11-253 Configuring the Second PPTP Server

Figure 11-254 Second PPTP Server Completed

Step 3. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-255**）

- Type the name in the **Name** field.
- **Local Settings**: Select LAN. Type A Company's subnet / mask 192.168.10.0 / 255.255.255.0 in the field.
- Under the **Remote Settings** section, type B Company's subnet / mask 192.168.20.0 / 255.255.255.0 in the field.
- Move PPTP_Server_PPTP_01 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-256**）

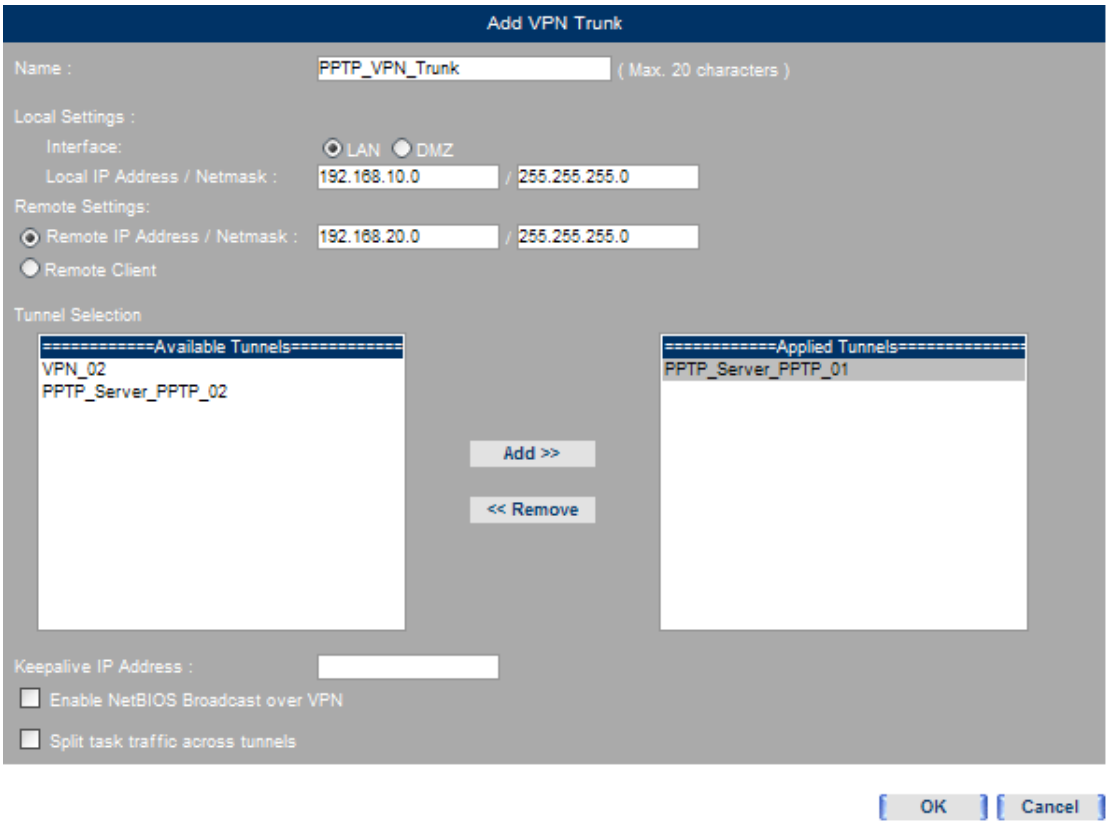


Figure 11-255 Configuring the Trunk

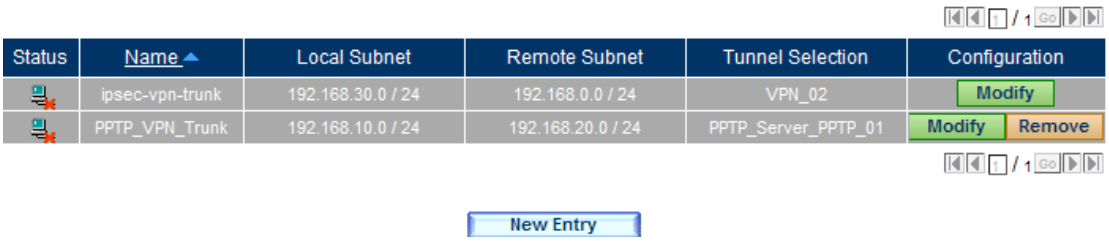


Figure 11-256 Setting Completed

Note：

1. When **Remote IP / Netmask** is selected for **Remote Settings**, you may select only one tunnel to establish the PPTP VPN connection.

Step 4. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below:（**Figure 11-257**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-258**）

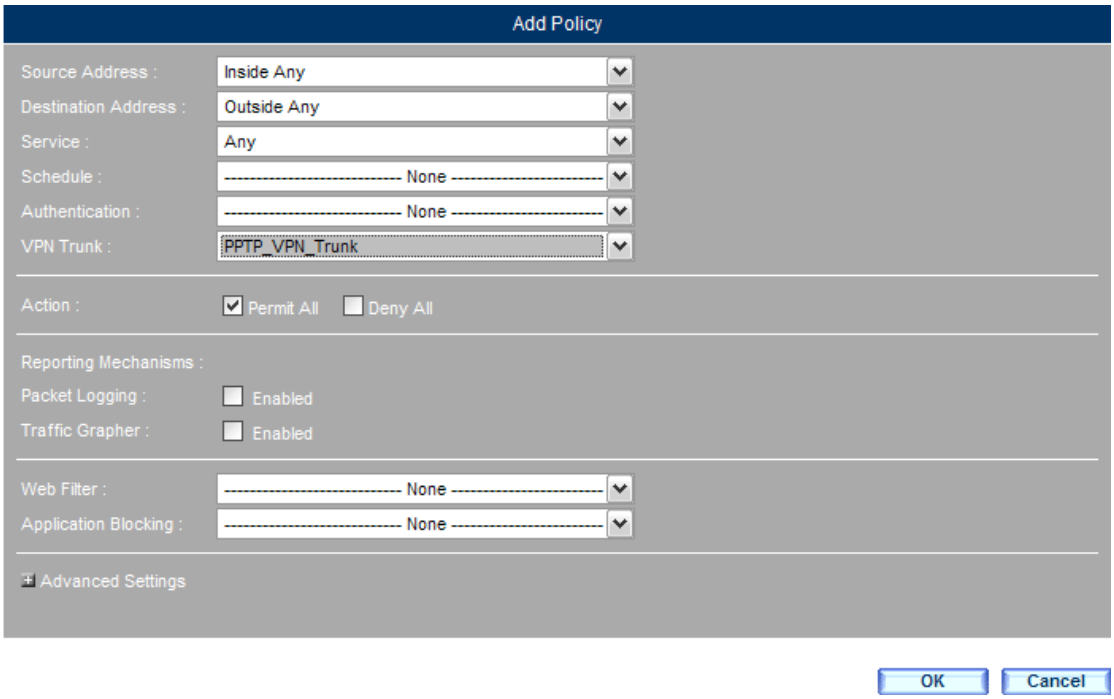


Figure 11-257 Configuring an Outgoing Policy with VPN Trunk

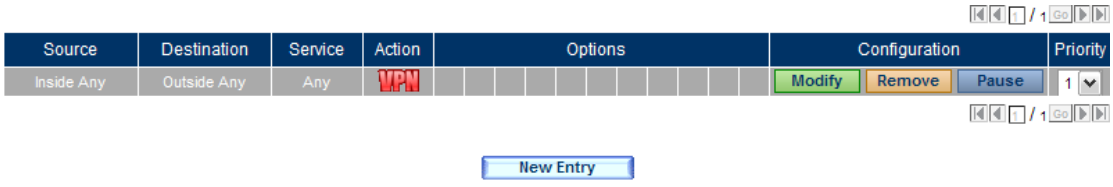


Figure 11-258 Settings Completed

Step 5. Go to **Policy** > **Incoming**, click **New Entry** and then set as below:（**Figure 11-259**）

- Select the defined VPN from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-260**）

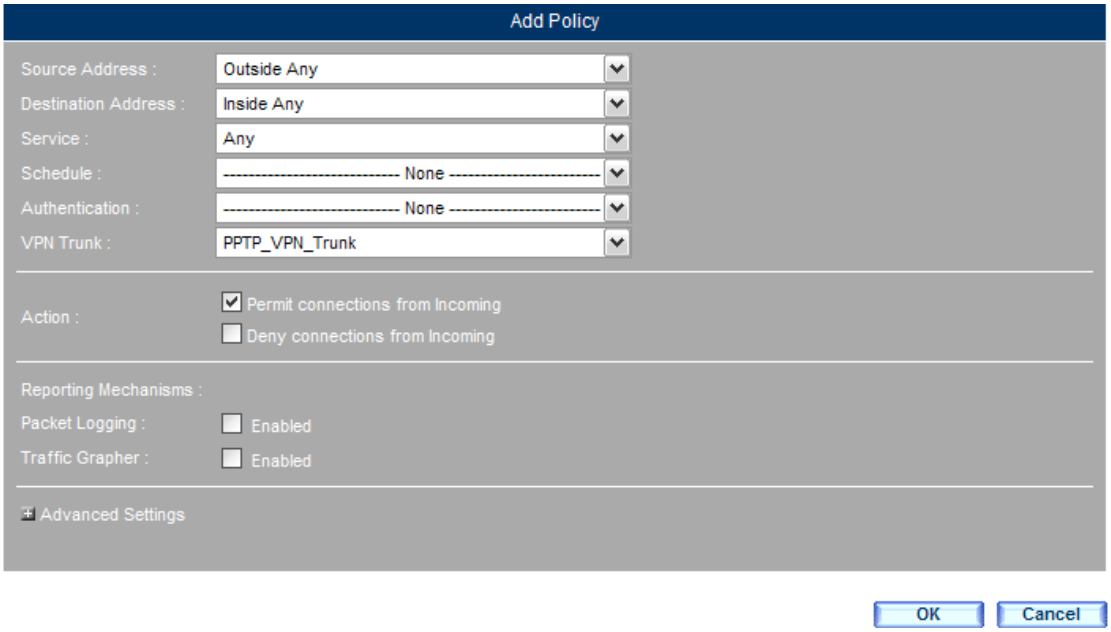


Figure 11-259 Configuring an Incoming Policy with VPN Trunk

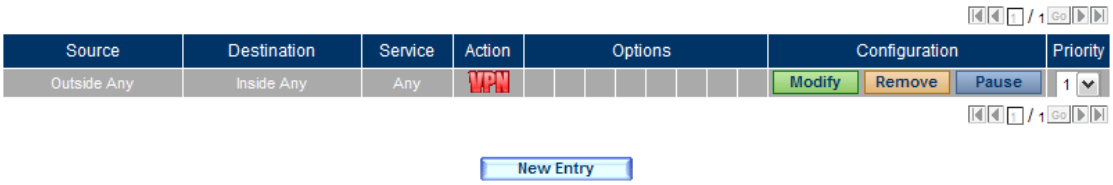


Figure 11-260 Settings Completed

For B Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **PPTP Client** and then set as below:

- Click New Entry.（**Figure 11-261**）
- Type PPTP_01 in the **Username** field.
- Enter 123456789 in the **Password** field.
- Enter A Company's WAN1 IP address in the **Server IP or Hostname** field.
- Click **Encryption.**
- Select Port2(WAN1) for **Interface.**
- Click **OK**.（**Figure 11-262**）
- Click **OK** again.（**Figure 11-263**）
- Enter PPTP_02 in the User Name field.
- Enter 987654321 in the **Password** field.
- Enter A Company's WAN2 IP address in the **Server IP or Hostname** field.
- Click **Encryption.**
- Select Port3(WAN2) for **Interface.**
- Click **OK**.（**Figure 11-264**）

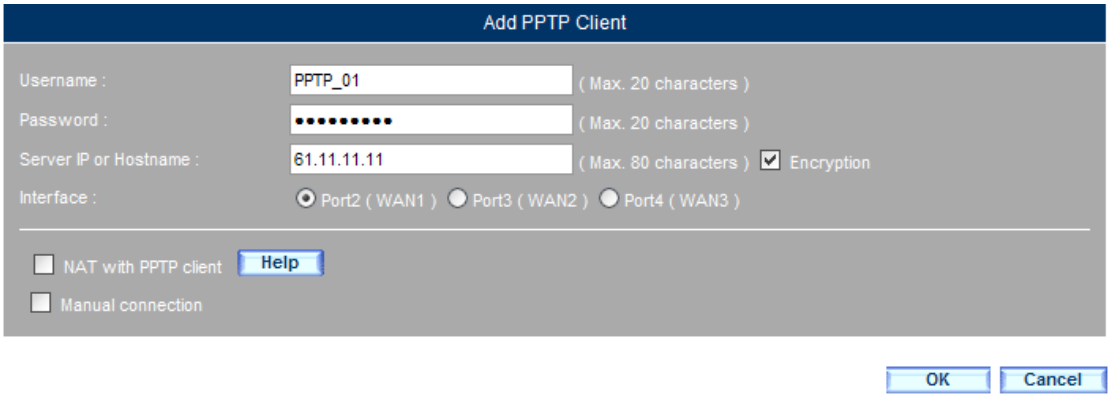


Figure 11-261 Configuring the First PPTP Client

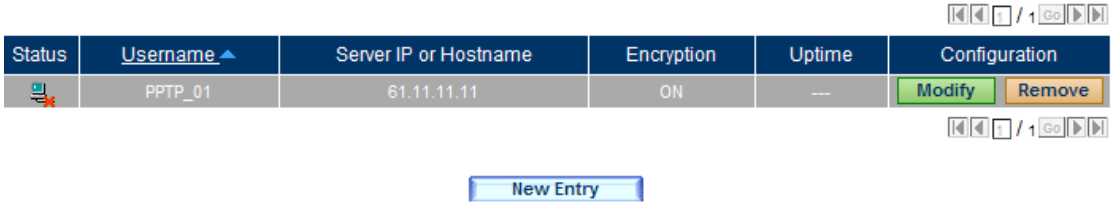


Figure 11-262 First PPTP Client Settings Completed

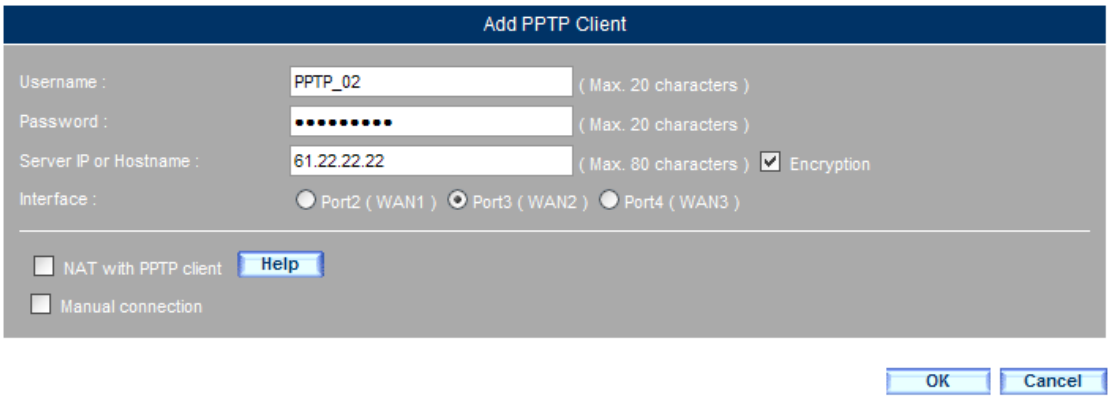


Figure 11-263 Second PPTP Client Setting Completed

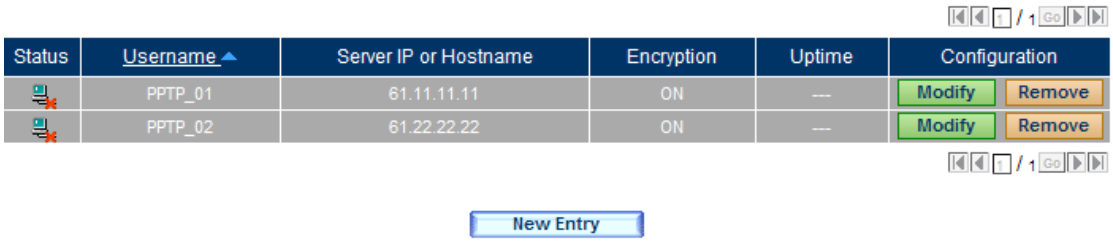


Figure 11-264 Second PPTP Client Setting Completed

Note：

1. When CS-2001 PPTP Client establish VPN connection with Windows PPTP Server, **NAT with PPTP Client** must be selected for the PCs under CS-2001 to access to Windows PPTP server.

Step 2. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-265**）

- Enter the name in the **Name** field.
- **Local Settings**: select LAN. Enter B Company's local subnet / mask 192.168.20.0/ 255.255.255.0 in the **Local IP / Netmask** field.
- Under the **Remote Settings** section, select **Remote IP/ Netmask** and then enter A Company's subnet/ mask 192.168.10.0 / 255.255.255.0.
- Move PPTP_Client_PPTP_01(61.11.11.11) and PPTP_Client_PPTP_02 (61.22.22.22) from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-266**）

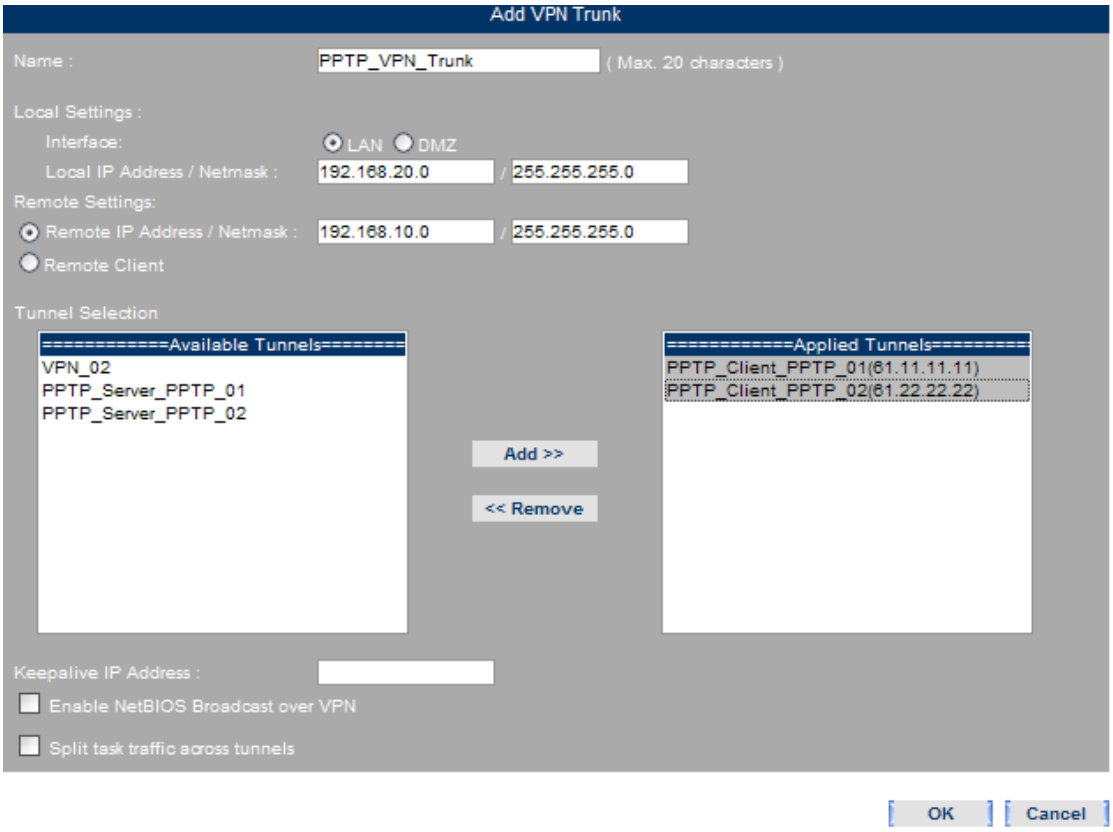


Figure 11-265 Configuring the Trunk

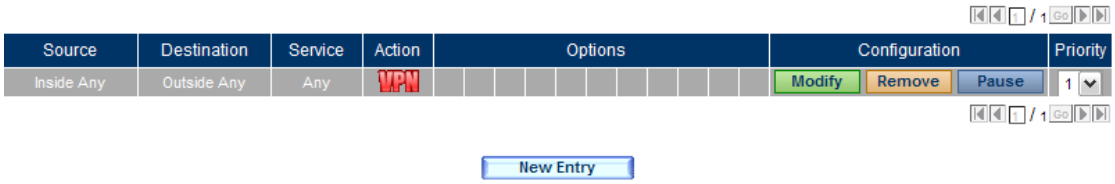


Figure 11-266 Settings Completed

Note:

1. When **Remote IP / Netmask** is selected for **Remote Settings**, the number of the PPTP_Client tunnel should be configured according to the number of WAN.

Step 3. Go to **Policy** > **Outgoing** and then set as below:（**Figure 11-267**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-268**）

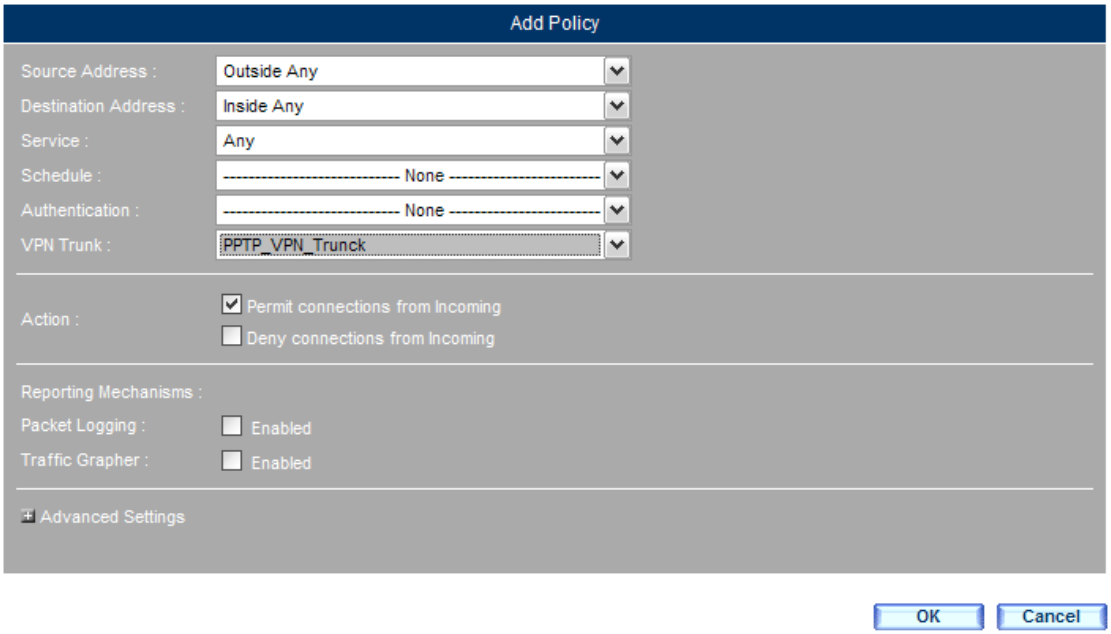


Figure 11-267 Configuring an Outgoing Policy

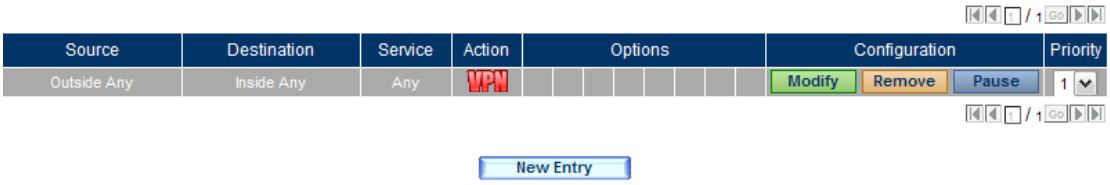


Figure 11-268 Setting Completed

Step 4. Go to **Policy** > **Incoming**, click **New Entry** and then set as below:（**Figure 11-269**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-270**）

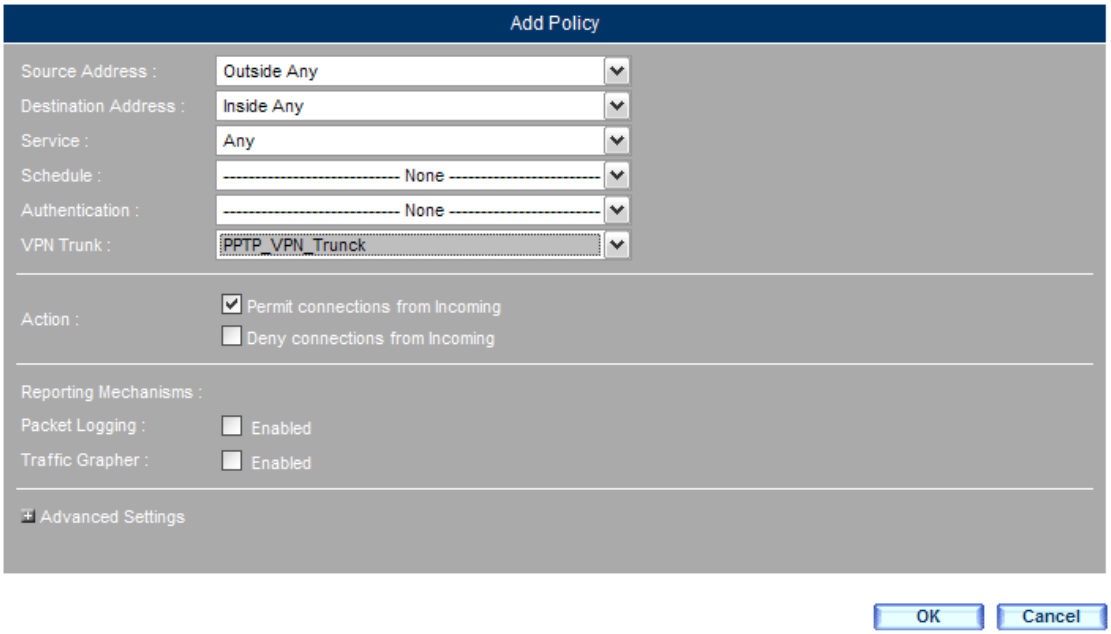


Figure 11-269 Configuring an Incoming Policy

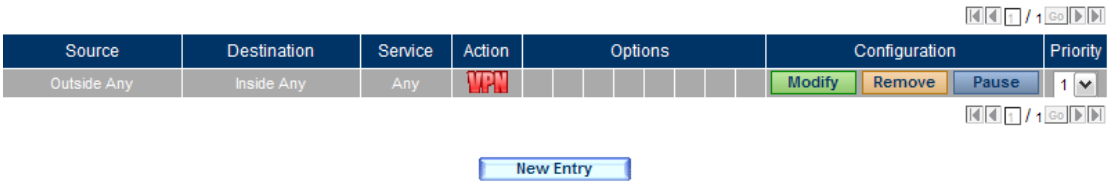


Figure 11-270 Settings Completed

Step 5. Settings completed.（Figure 11-271）

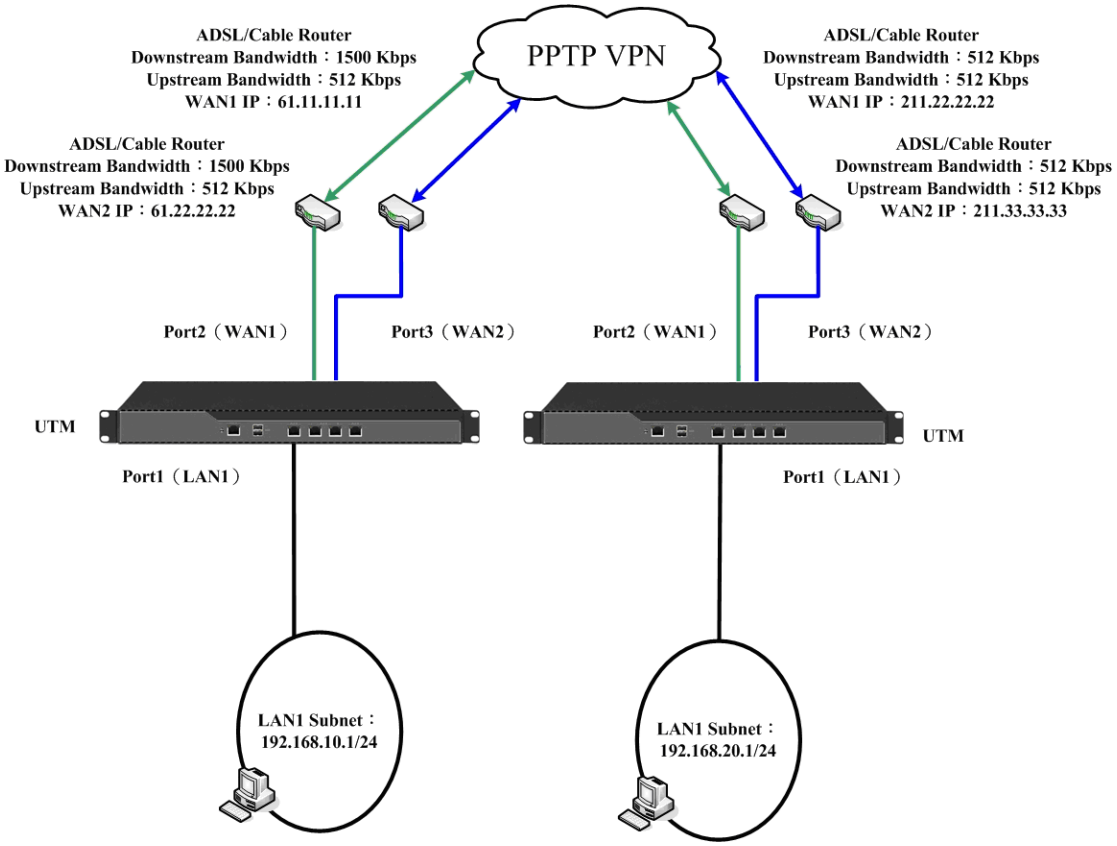


Figure 11-271 The Deployment of PPTP VPN

11.1.7 Using Two CS-2001 Devices to Establish PPTP VPN

Connection

Prerequisite Setup (Note: IP addresses used as examples only)

A Company: Configure Port1 as LAN1(192.168.10.1). IP range: 192.168.10.x/24. Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company: Configure Port1 as LAN1(192.168.20.1). IP range: 192.168.20.x/24. Configure Port 2 as WAN1(211.22.22.22) and connect it to the ADSL Termination Unit Remote(ATUR) to access the Internet.

This example is to use two CS-2001 devices to establish VPN connection between A Company and B Company.

For A Company, set as below:

Step 1. Go to **Policy Object >VPN > PPTP Server** and then set as below: (**Figure 11-272**)

- Click **Modify.**
- Click **Enable PPTP.**
- Click **Encryption.**
- Tick **Allow Internet access via** and then select the port.
- **Auto-disconnect if idle for**: type 0.
- Enter the **Client IP- IP Range.**
- Click **OK**.

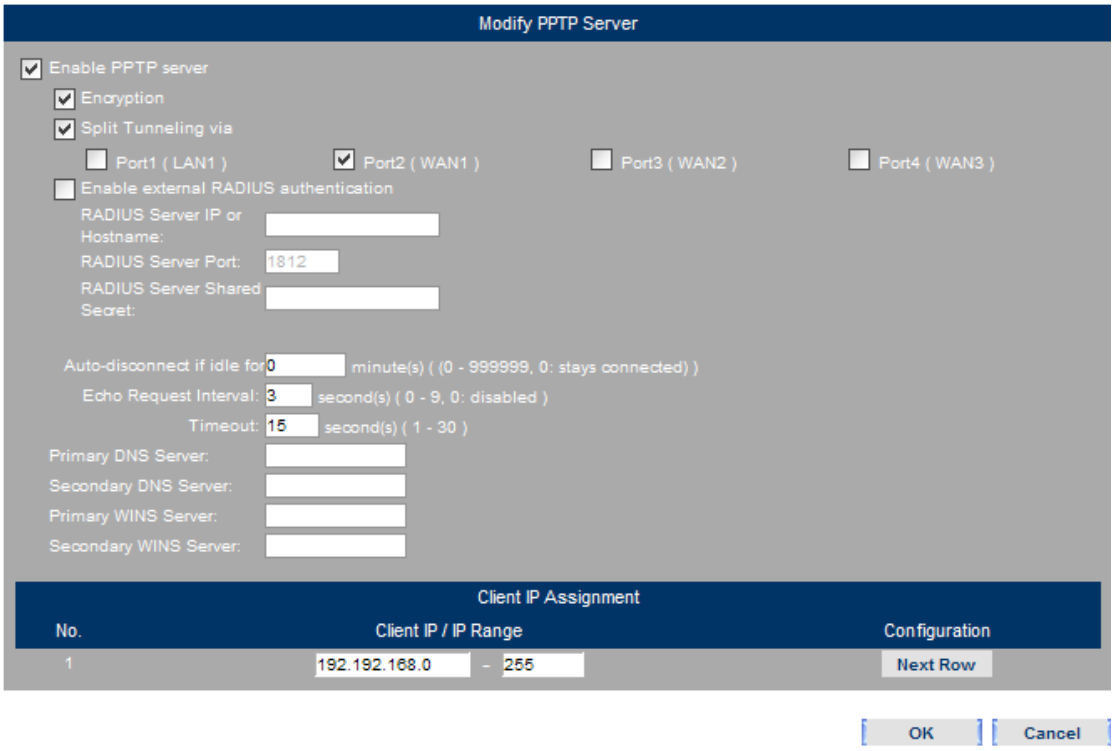


Figure 11-272 Enabling the PPTP Server

Step 2. Go to **Policy Object** > **VPN** > **PPTP Server**, click **New Entry** and then set as below:（**Figure 11-273**）

- Type PPTP_Connection in the **Username** field.
- Type 123456789 in the **Password** field.
- Under **Client IP(s) assigned from**, click **IP Range**.
- Click **OK**.（**Figure 11-274**）

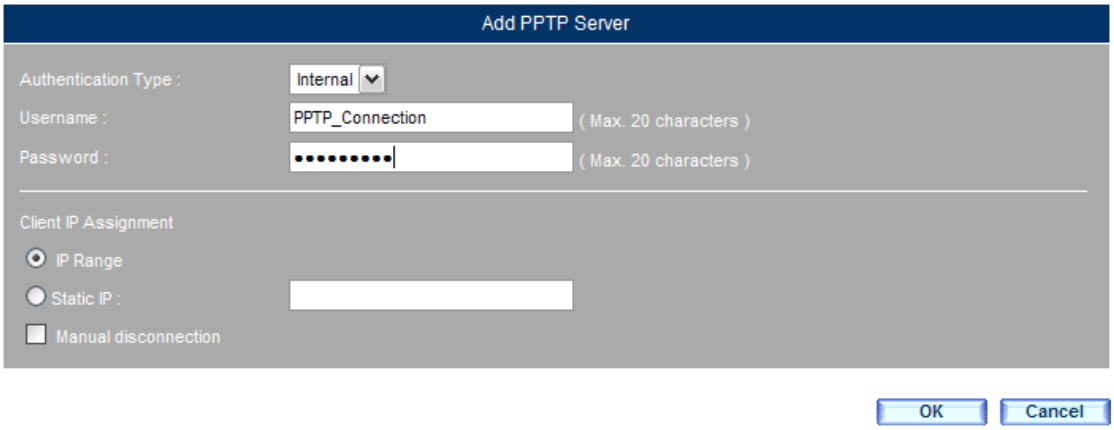


Figure 11-273 Configuring the PPTP Server Connection

Figure 11-274 Setting Completed

For B Company, set as below;

Step 1. Go to **Policy Object** > **VPN** > **PPTP Client**, click **New Entry** and then set as below:（**Figure 11-275**）

- Type PPTP_Connection in the **Username** field.
- Enter 123456789 in the Password field.
- Enter A Company's WAN1 IP address in the **Server IP or Hostname** field.
- Click **Encryption.**
- Select Port2 (WAN1) for **Interface.**
- Tick **NAT with PPTP Client.**
- Click **OK**.（**Figure 11-276**）

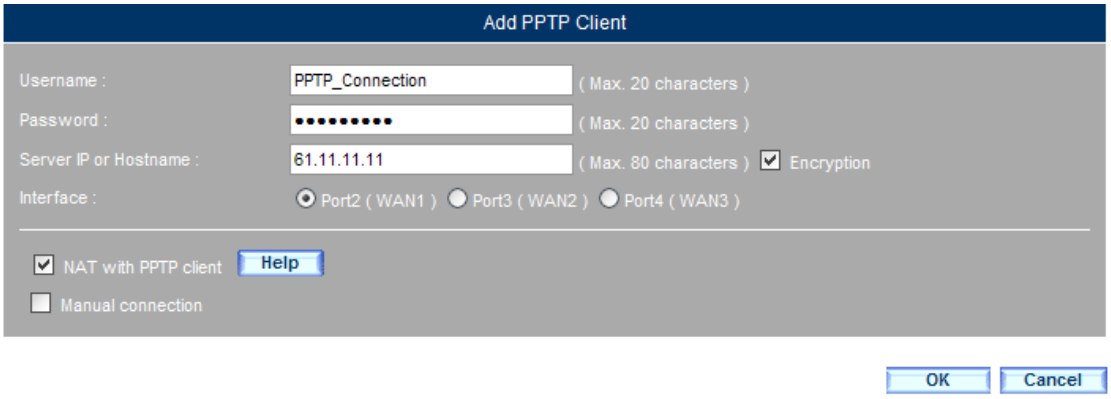


Figure 11-275 Configuring PPTP Connection

Figure 11-276 Setting Completed

Note:

1. When CS-2001 PPTP Client establish VPN connection wih the CS-2001 PPTP Server, **NAT with PPTP Client** must be selected for CS-2001 PPTP Client users to access the Internet via PPTP Server.

Step 2. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-277**）

- Enter the name in the **Name** field.
- **Local Settings**: select **LAN**. Type B Company's subnet/ mask 192.168.20.0 / 255.255.255.0 in the **Local IP / Netmask** field.
- Under **Remote Settings**, select **Remote IP / Netmask** and then enter A Company 's subnet / mask.
- Move PPTP_Client_PPTP_Connection(61.11.11.11) from the **Available Tunnels** column to the **Selected Tunnels** column.
- Click **OK**.（**Figure 11-278**）

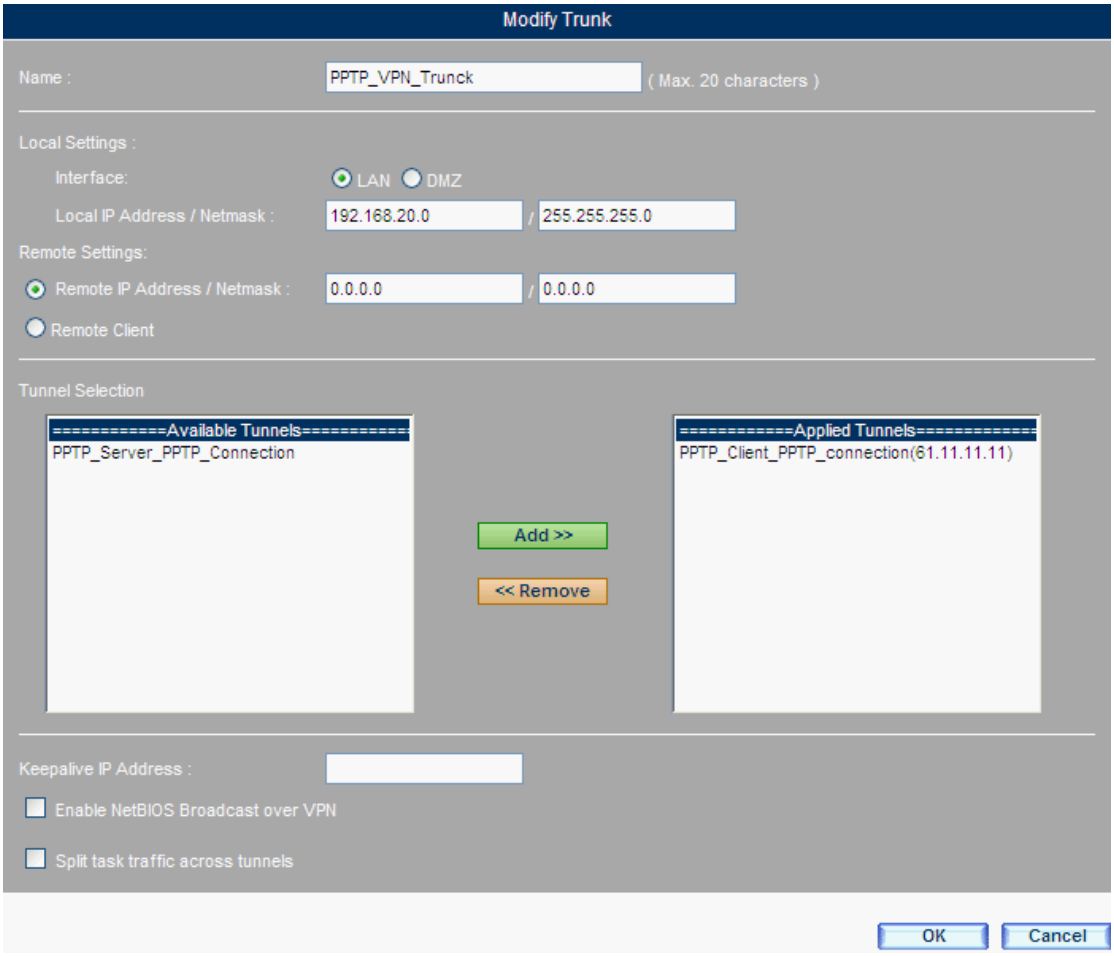


Figure 11-277 Configuring theTrunk

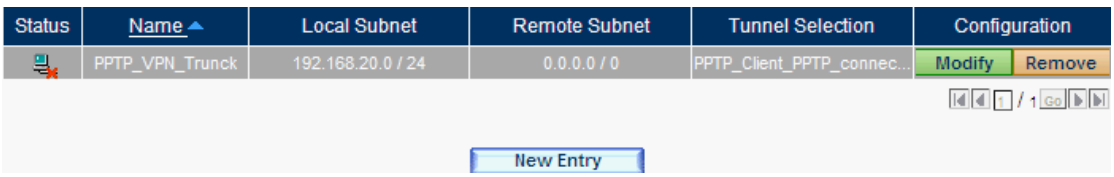


Figure 11-278 Setting Completed

Step 3. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below:（**Figure 11-279**）

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-280**）

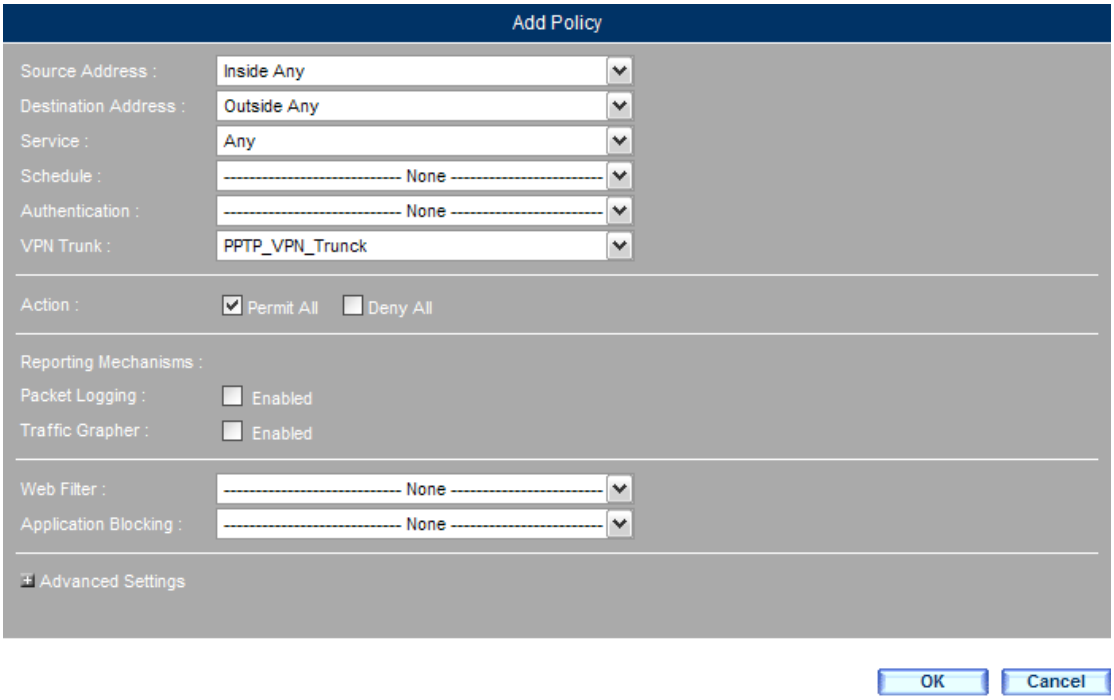


Figure 11-279 Configuring an Outgoing Policy

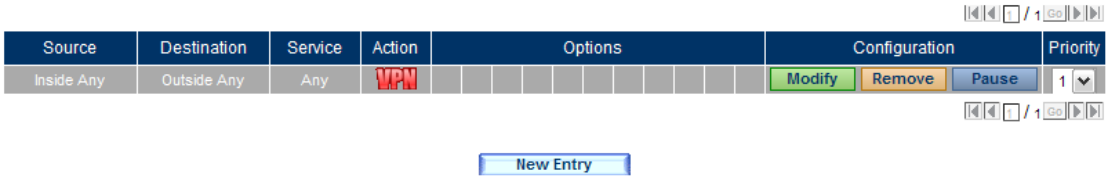


Figure 11-280 Setting Completed

Note：

1. In this example, B company's Trunk settings only need to be applied to **Policy** > **Outgoing**.

Step 4. Setting Completed.（Figure 11-281）

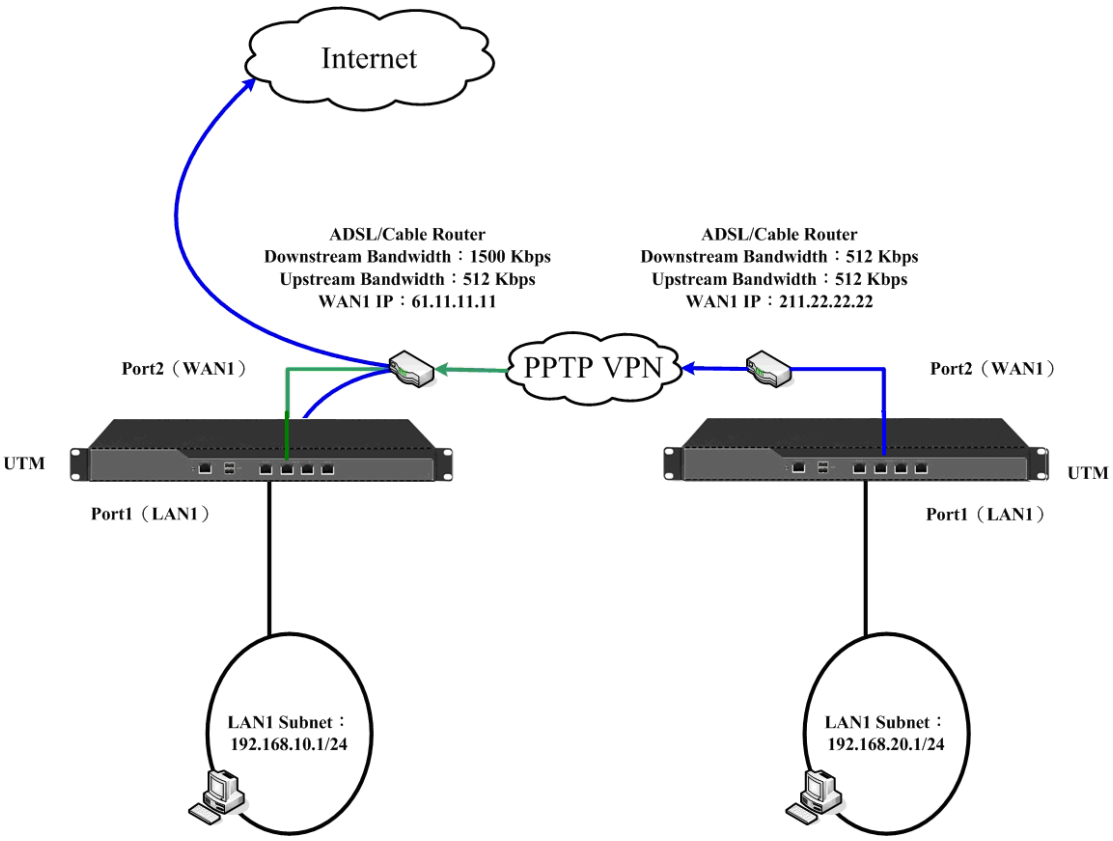


Figure 11-281 Deployment of PPTP VPN Connection

11.1.8 Establishing PPTP VPN Connection by One CS-2001

Device and One PC Running Windows 2000

Prerequisite Setup (Note: IP addresses used as examples only)

A Company uses CS-2001.
Configure Port1 as LAN1(192.168.10.1) IP range:192.168.10.x/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

B Company uses a PC running Windows 2000. IP address: 211.22.22.22

This example is to establish VPN connection by one CS-2001 device and one PC running Windows 2000.

For A Company, set as below:

Step 1. Go to **Policy Object** > **VPN** > **PPTP Server** and then set as below: (**Figure 11-282**)

- Click **Modify.**
- Click **Enable PPTP.**
- Click **Encryption.**
- Tick **Allow Internet access via** and then select the port.
- **Auto-disconnect if idle for**: enter 0.
- Enter the **Client IP – IP Range.**
- Click **OK**.

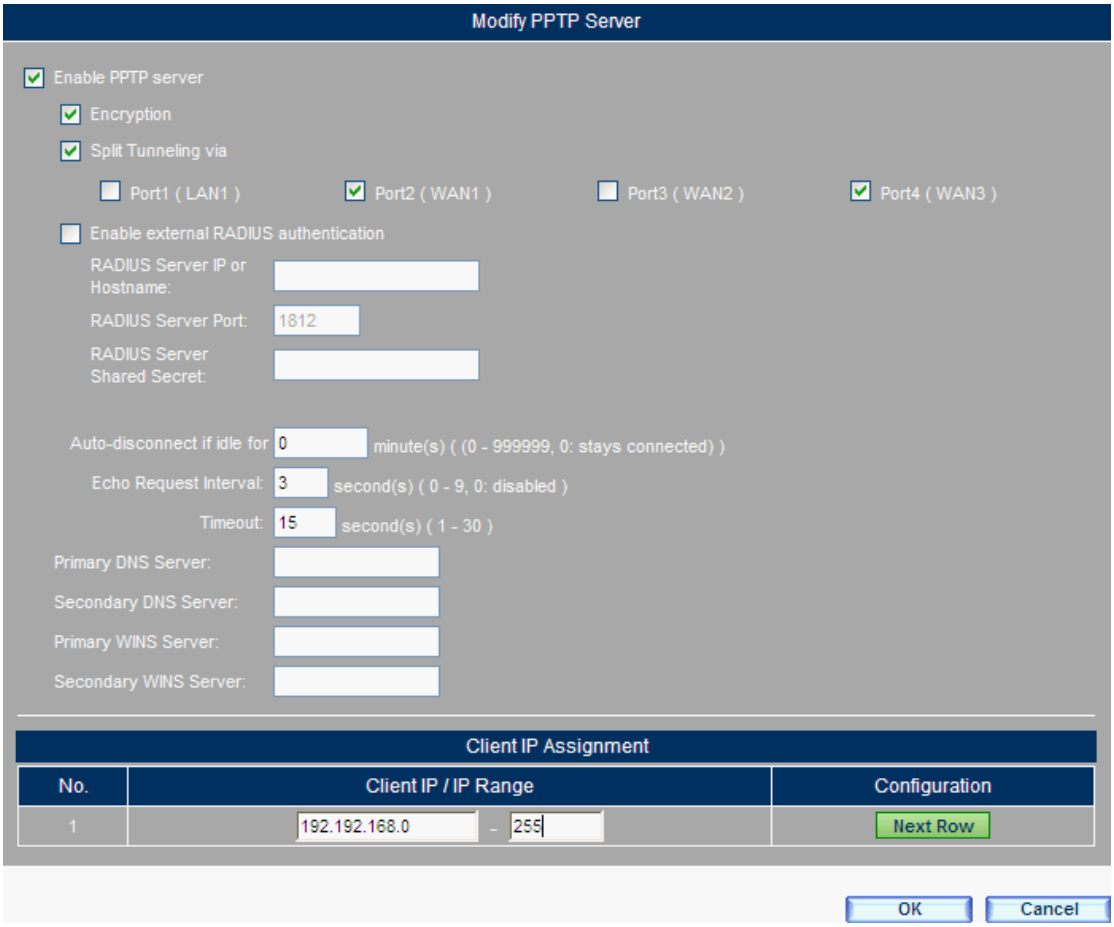


Figure 11-282 Enabling the PPTP Server

Note:

1. The IT administrator may enable or disable the external users to access the Internet via the CS-2001 device when they establish a VPN connection to the CS-2001 PPTP Server.
2. **Auto-disconnect if idle for**: if the VPN connection is idle for the specified minutes, it will be disconnected automatically.

3. If the external user wants to connect to IPSec VPN subnet via PPTP VPN connection, the **Client IP Allocation/ IP Range** must be on the LAN1 (192.168.10.x/24) which must not already be in use. In addition, the external user must establish the PPTP VPN connection to the CS-2001 via IPSec VPN.

Step 2. Go to **Policy Object** > **VPN** > **PPTP Server**, click **New Entry** and then set as below:（**Figure 11-283**）

- Type PPTP_Connection in the **Username** field.
- Type 123456789 in the **Password** field.
- Select **IP Range** under **Client IP(s) assigned from.**
- Click **OK**.（**Figure 11-284**）

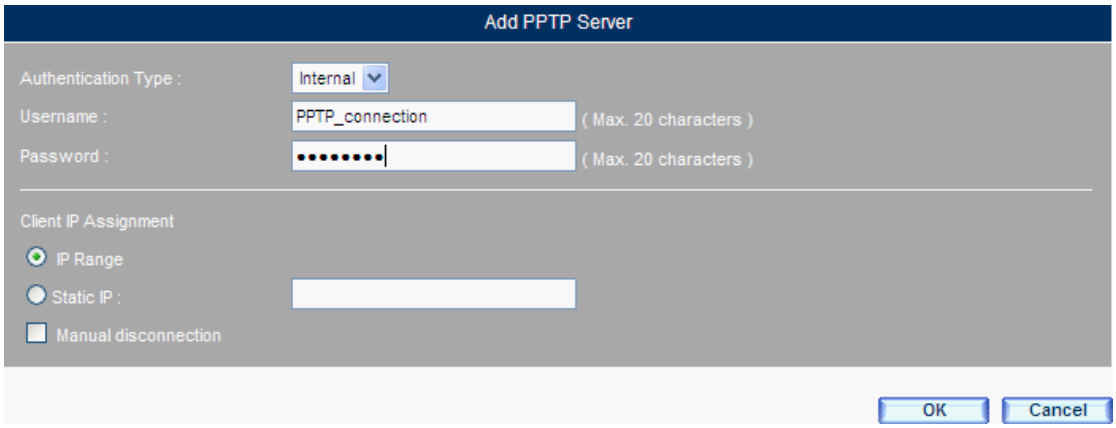


Figure 11-283 Configuring the PPTP Server Connection

Figure 11-284 Setting Completed

Step 3. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as below:（**Figure 11-285**）

- Type the name in the **Name** field.
- **Local Settings**: select LAN. Type A Company's subnet / mask 192.168.10.0 / 255.255.255.0 in the **Local IP/ Netmask** field**.**
- Under **Remote Settings**, select **Remote Client.**
- Move PPTP_Server_PPTP_Connection from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.（**Figure 11-286**）

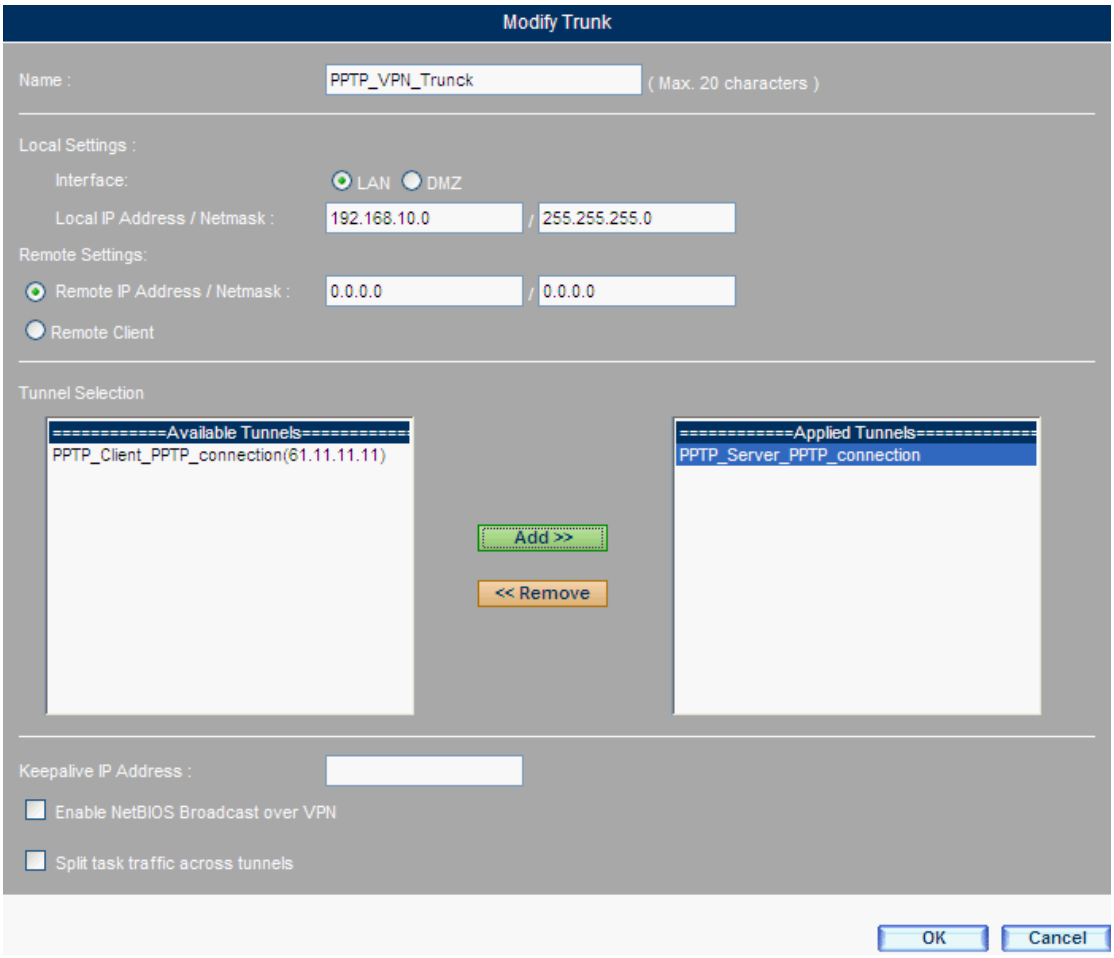


Figure 11-285 Configuring the Trunk

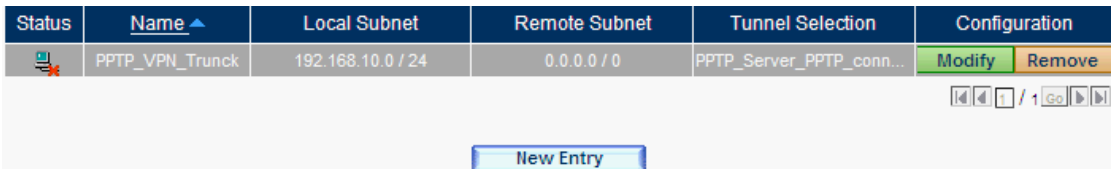


Figure 11-286 Setting Completed

Note：

1. If the external users want to connect to the IPSec VPN subnet, the **Local IP/ Netmask** must be configured as the IPSec VPN subnet.

Step 4. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below:（**Figure 11-287**）

- Select the defined trunk from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 11-288**）

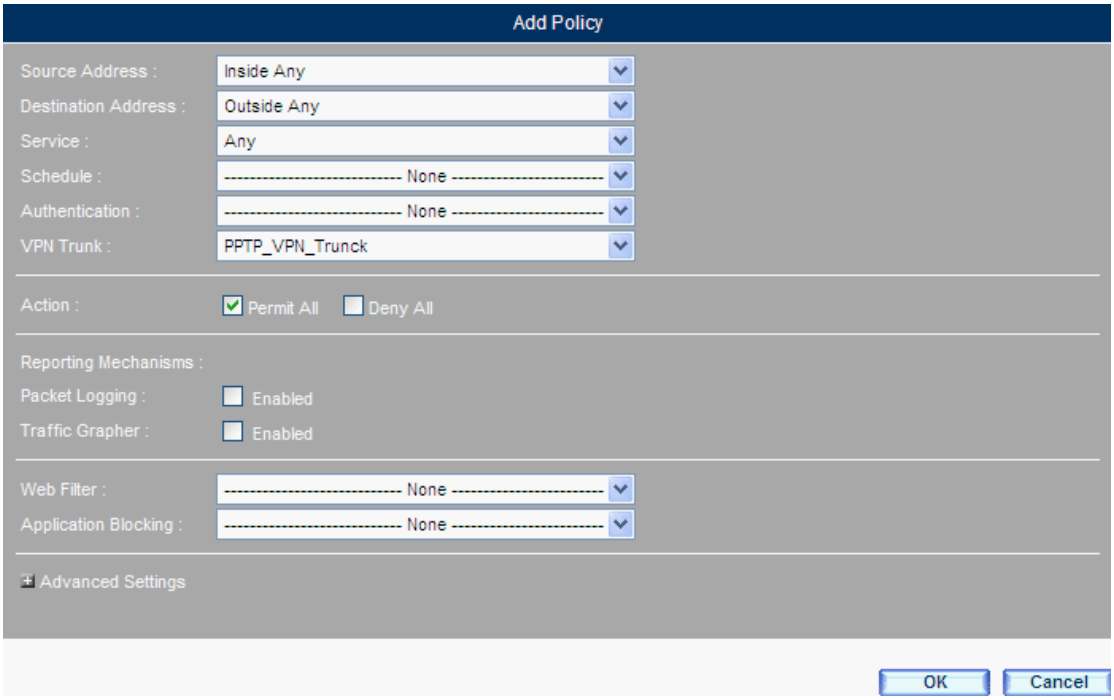


Figure11-287 Configuring an Outgoing Policy

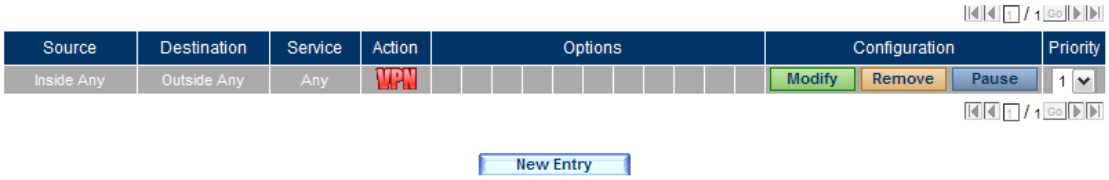


Figure 11-288 Setting Completed

Step 5. Go to **Policy** > **Incoming**, click **New Entry** and then set as below: (**Figure 11-289**)

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**. (**Figure 11-290**)

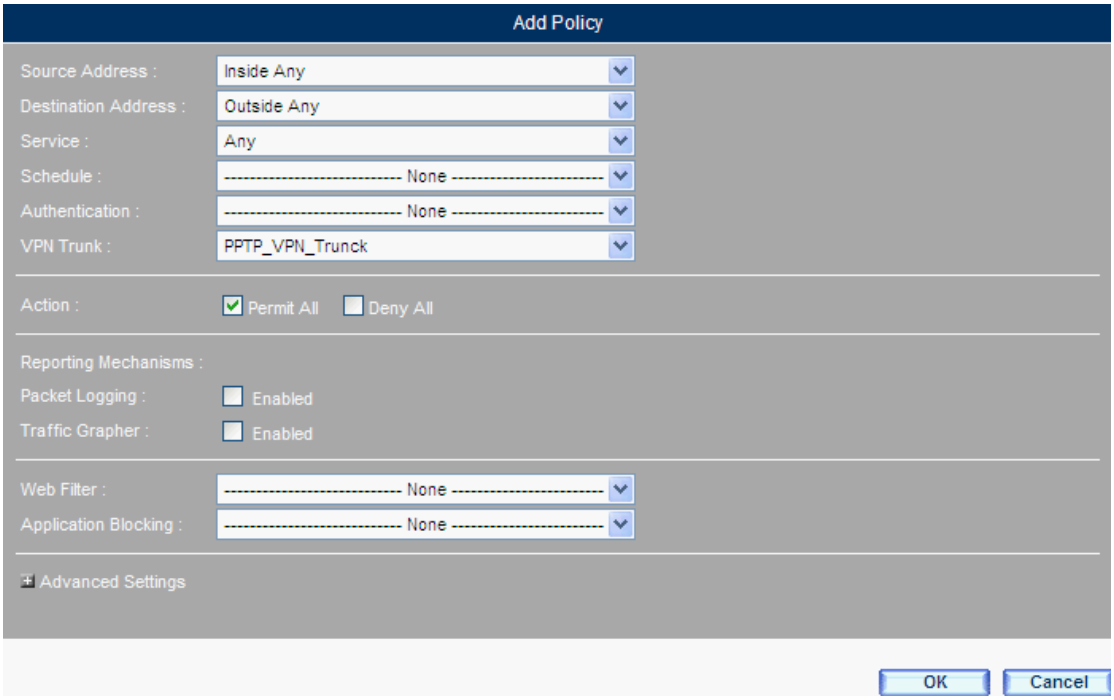


Figure 11-289 Configuring an Incoming Policy with VPN Trunk

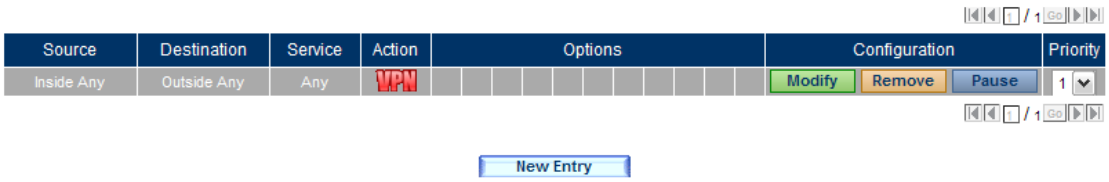


Figure 11-290 Setting Completed

For B Company, set as below:

Step 1. Right-click on **My Network Places** and then click **Properties**. (**Figure 11-291**)

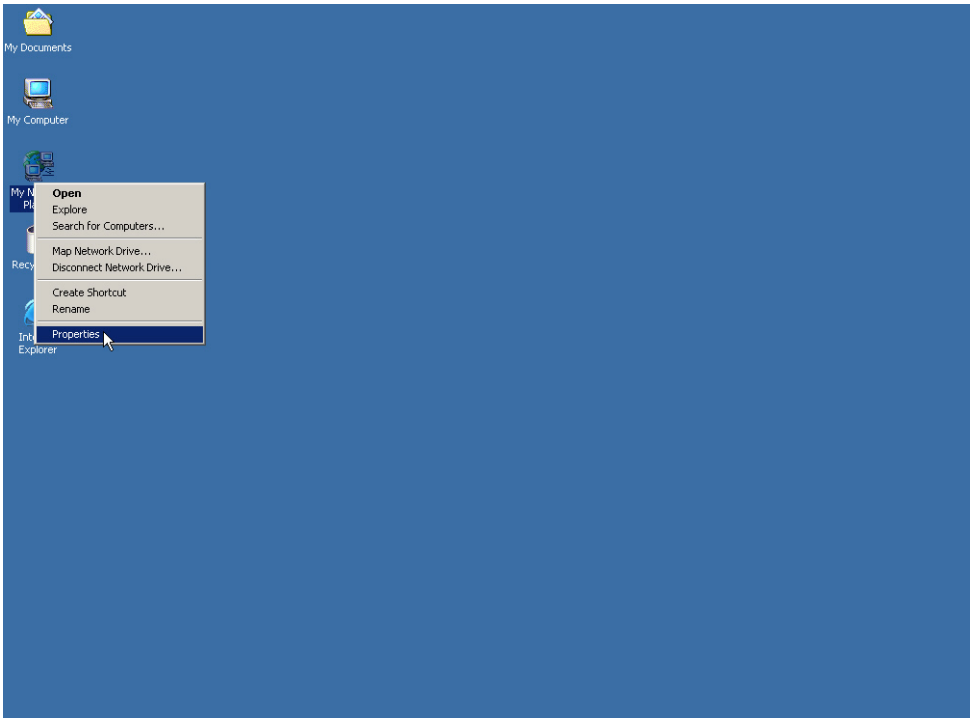


Figure 11-291 Selecting "Properties" on the Shortcut Menu of "My Network Places"

Step 2. In the **Network and Dial-up Connections** window, double-click "Make New Connection". (**Figure 11-292**)

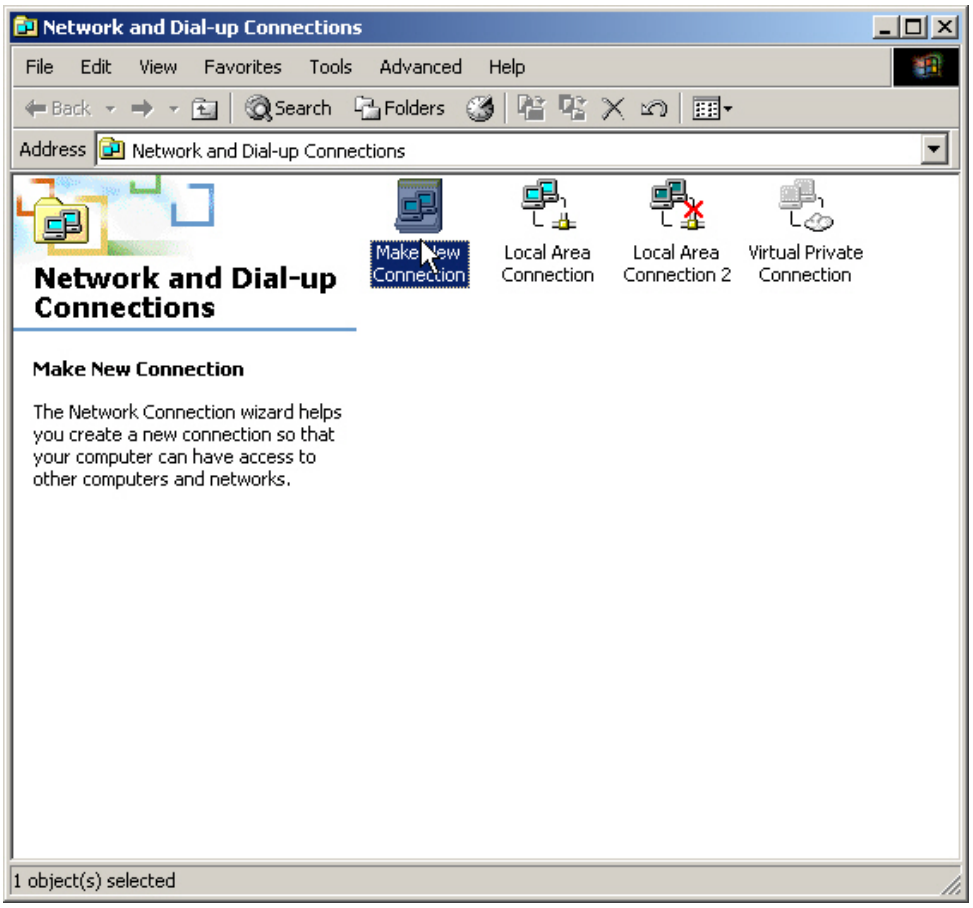


Figure 11-292 Double-Clicking on "Make New Connection"

Step 3. In the **Location Information** window, specify the country / region, area code and phone system accordingly, and then click **OK**.（**Figure 11-293**）

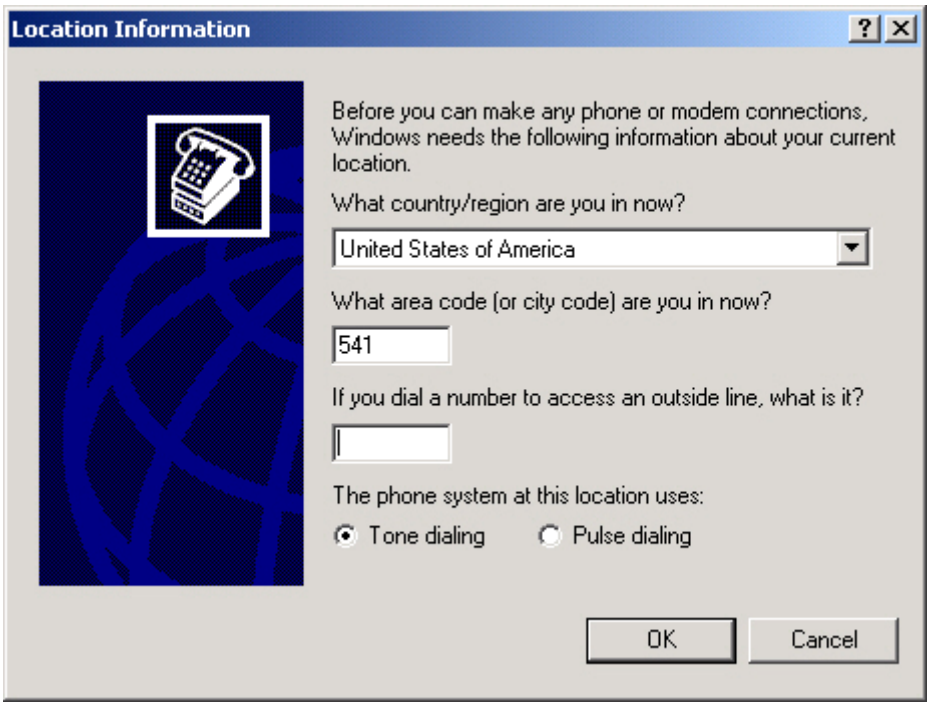


Figure 11-293 Local Information Settings

Step 4. In the **Phone And Modem Options** window, click **OK**.（**Figure 11-294**）

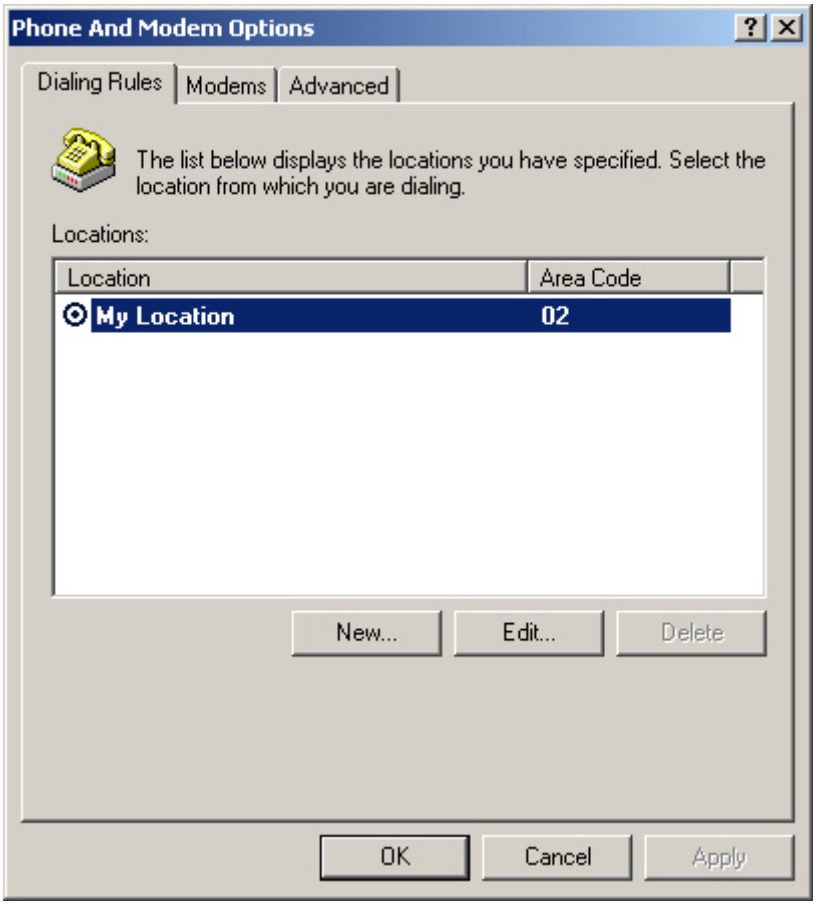


Figure 11-294 Phone and Modem Options

Step 5. In the **Network Connection Wizard** window, click **Next**. (**Figure 11-295**)

Figure 11-295 Network Connection Wizard

Step 6. In the **Network Connection Type** window, select **Connect to a private network through the Network** and then click **Next**. (**Figure 11-296**)

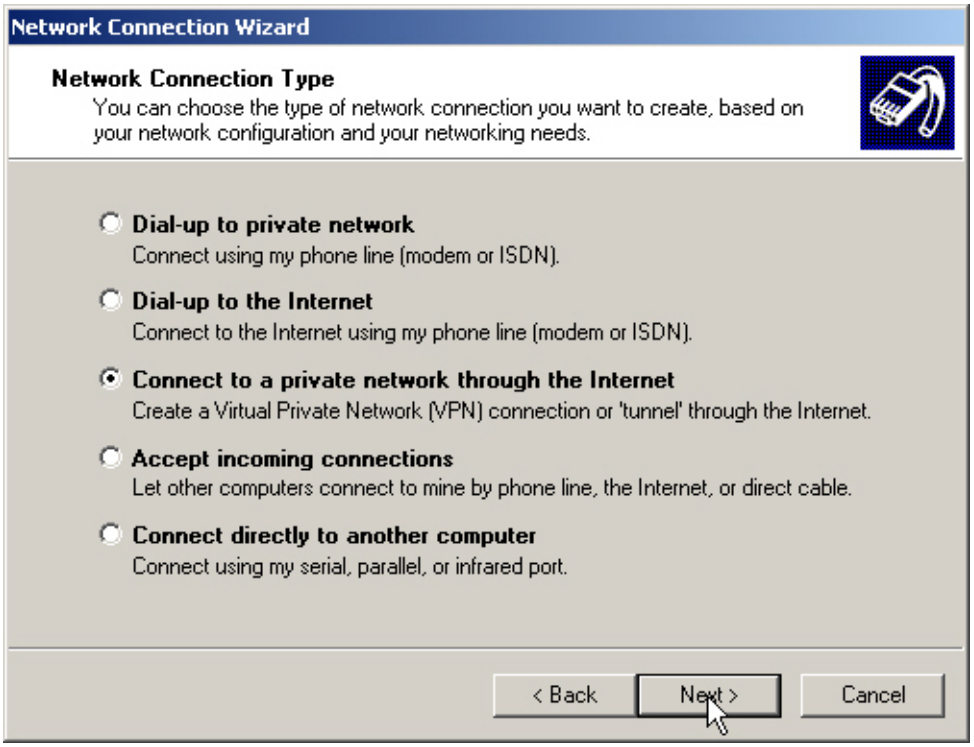


Figure 11-296 Select the "Connect to a private network through the Internet"

Step 7. In the **Destination Address** window, type the host name or IP address in the blank field and then click **Next**. (**Figure 11-297**)

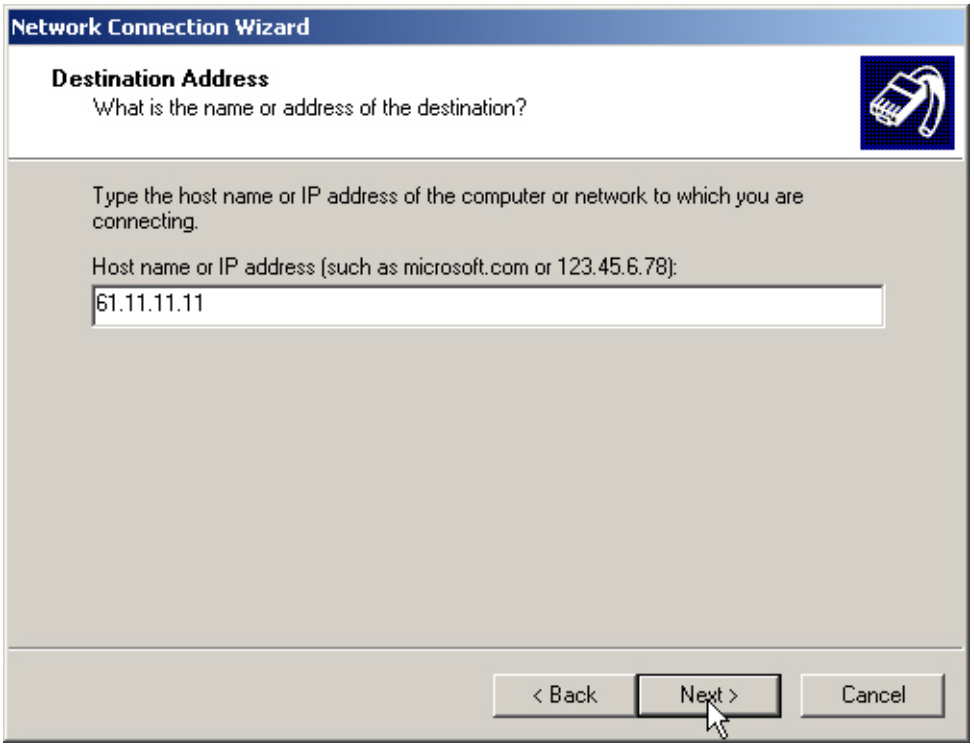


Figure 11-297 Destination Address Settings

Step 8. In the **Connection Availability** window, select **For all users** and then click **Next**. (**Figure 11-298**)

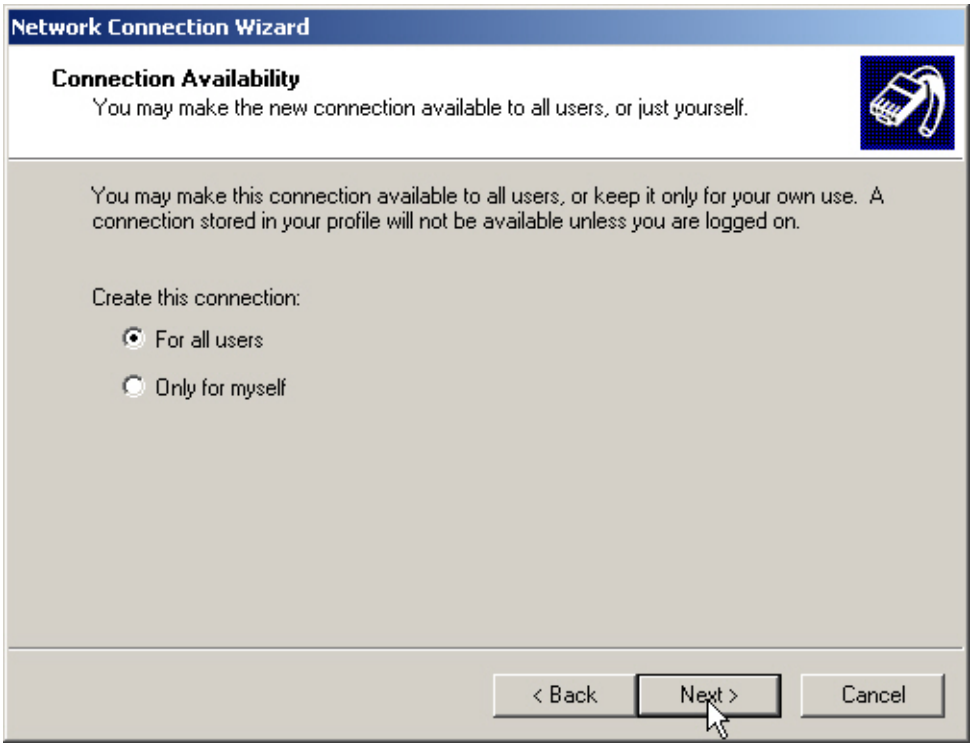


Figure 11-298Connection Availability Settings

Step 9. In the **Completing the New Connection Wizard** window, type a **Connection Name** and then click **Finish**.（**Figure 11-299**）

Figure 11-299 New Connection Created

Step 10. In the **Connect Virtual Private Connection** window, set as below: （**Figure 11-300**）

- **User Name**: Type “PPTP_Connection”.
- **Password**: Enter 123456789.
- Tick **Save Password.**
- Click **Connect.**
- The “Connecting Virtual Private Connection…” dialogue box appears. （**Figure 11-301**）
- Connection created.（**Figure 11-302**）

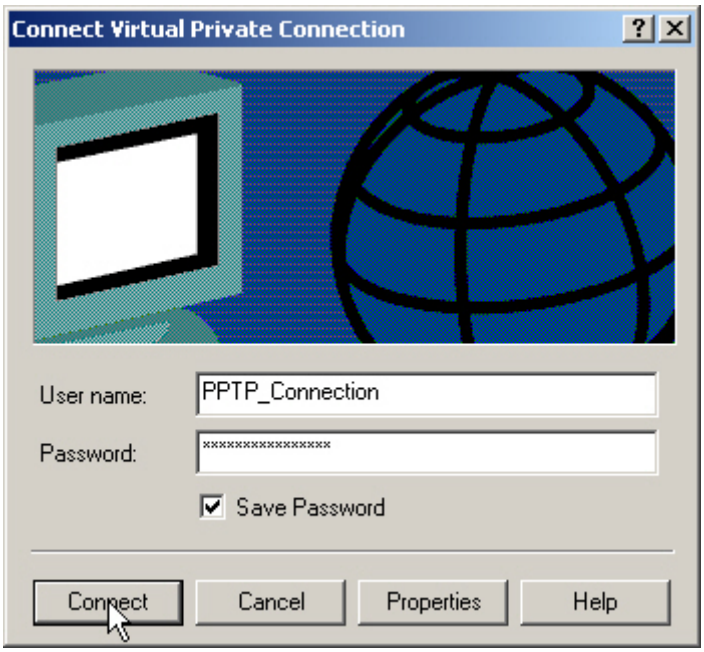


Figure 11-300 Virtual Private Connection Window

Figure 11-301 Creating a PPTP VPN Connection

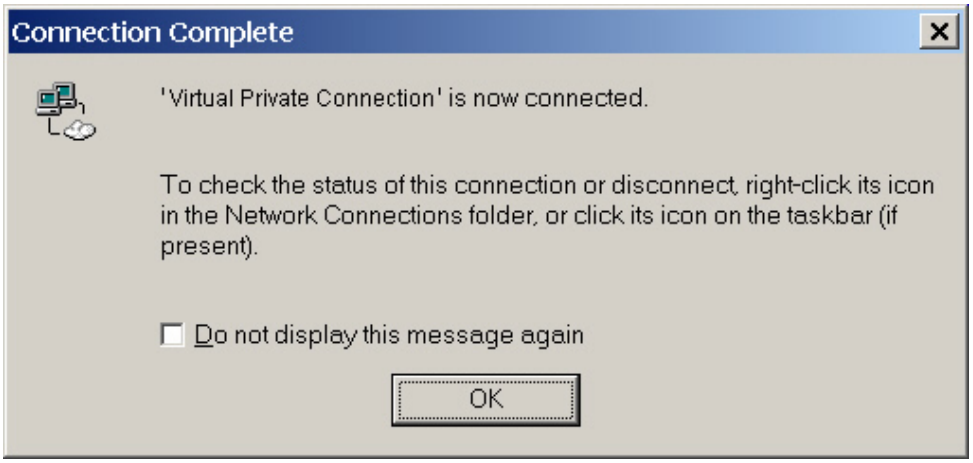


Figure 11-302 PPTP VPN Connection Successfully Connected

Step 11. Settings completed.（Figure 11-303）

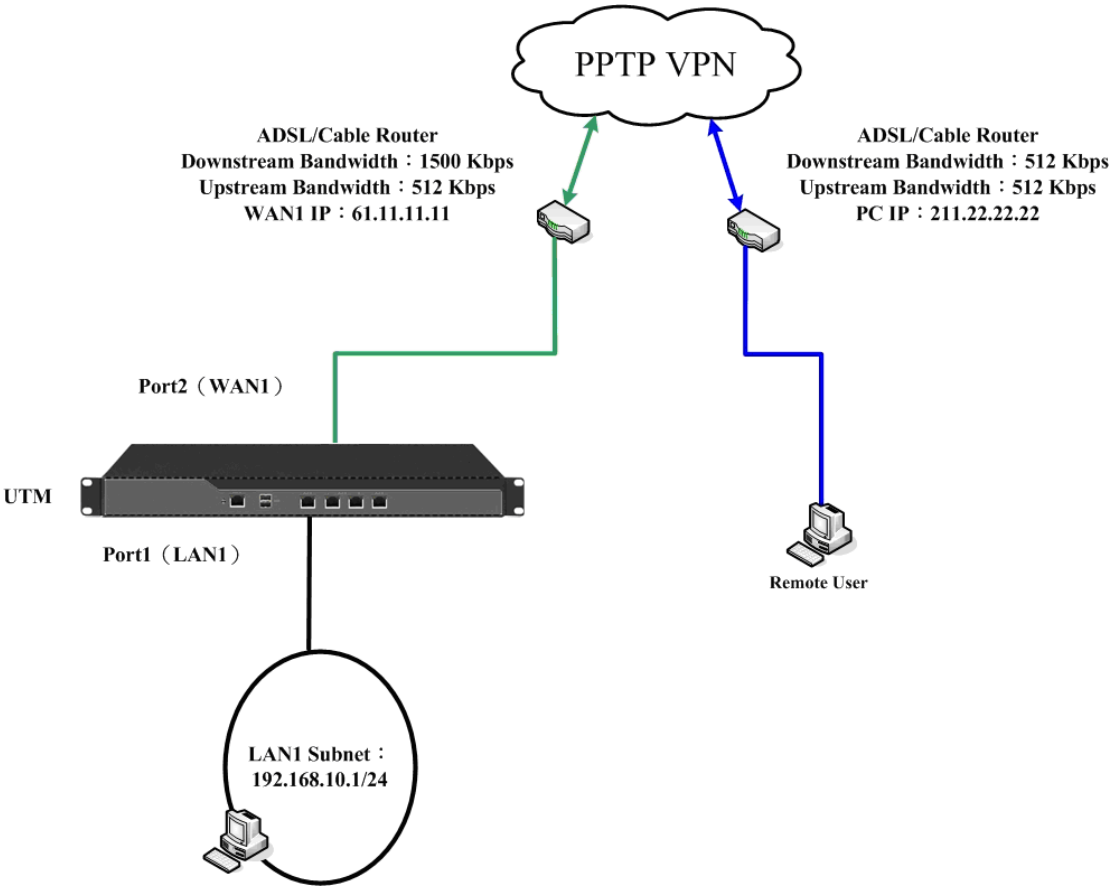


Figure 11-303 Deployment of PPTP VPN

Mail Security

Chapter 12 Configuration

Mail configuration refers to the processing basis of mail services. In this chapter, it will be covering the functionality and application of *Settings, Mail Domains, Account Manager, Mail Relay, Mail Notice, Queued Mail* and *Mail Signatures*.

Terms in Settings

Log Storage Time

- Quarantined spam / virus emails can be designate a storage time and deleted when due.
- You may also decide whether a quarantined email can be repeatedly retrieved or not.

Personal Email Viewer / Email Notification Settings

- This is to enable the Personal Email Viewer and configure the port and public IP address/ Hostname for email notification.
- Configures the Login Authentication.

Email Settings

- Configure the maximum number of sessions per IP per minute and the maximum number of concurrent sessions per IP.
- Set the storage time of queued mail.

Mail Scanning Settings

- It determines of which size an email is to be scanned for viruses and spam.
- It allows you to highlight unscanned emails by adding a warning message.
- It allows you to tag spam email's subject or virus-infected emails with warning message.

The Subject and Content of the Mail Notice

- The IT administrator may configure the subject and content of the mail notice. The system will send the mail notice by default if this part is left blank.
  - Go to **Mail Security > Configuration > Settings** and then set as below:
    - **Storage Time of Quarantined Logs**: enter 14.
    - Tick **Enable Web Mail**. Type 8080 in the **HTTP** field. Type 1443 in the **HTTPS** field. Type 59.124.36.162 in the **Public IP Address/ Domain Name** field.
    - **Max. No. of Sessions per IP per Minute**: enter 20.
    - **Max. No. of Concurrent Sessions per IP**: enter 100.
    - **Max. Lifetime of Queued Mail**: enter 4 hours
    - **Max. Spam Mail Scanning Size**: 128 KBytes.
    - **Max. Virus Mail Scanning Size**: 512 KBytes.
    - **Tag an unscanned email's subject with**: --Unscanned--.

- **Tag spam email's subject with**: --Spam--.
- **Tag virus-infected emails with**: --Virus--.
- Type the subject and the content of the mail notice.
- Click **OK**.（**Figure 12-1**）

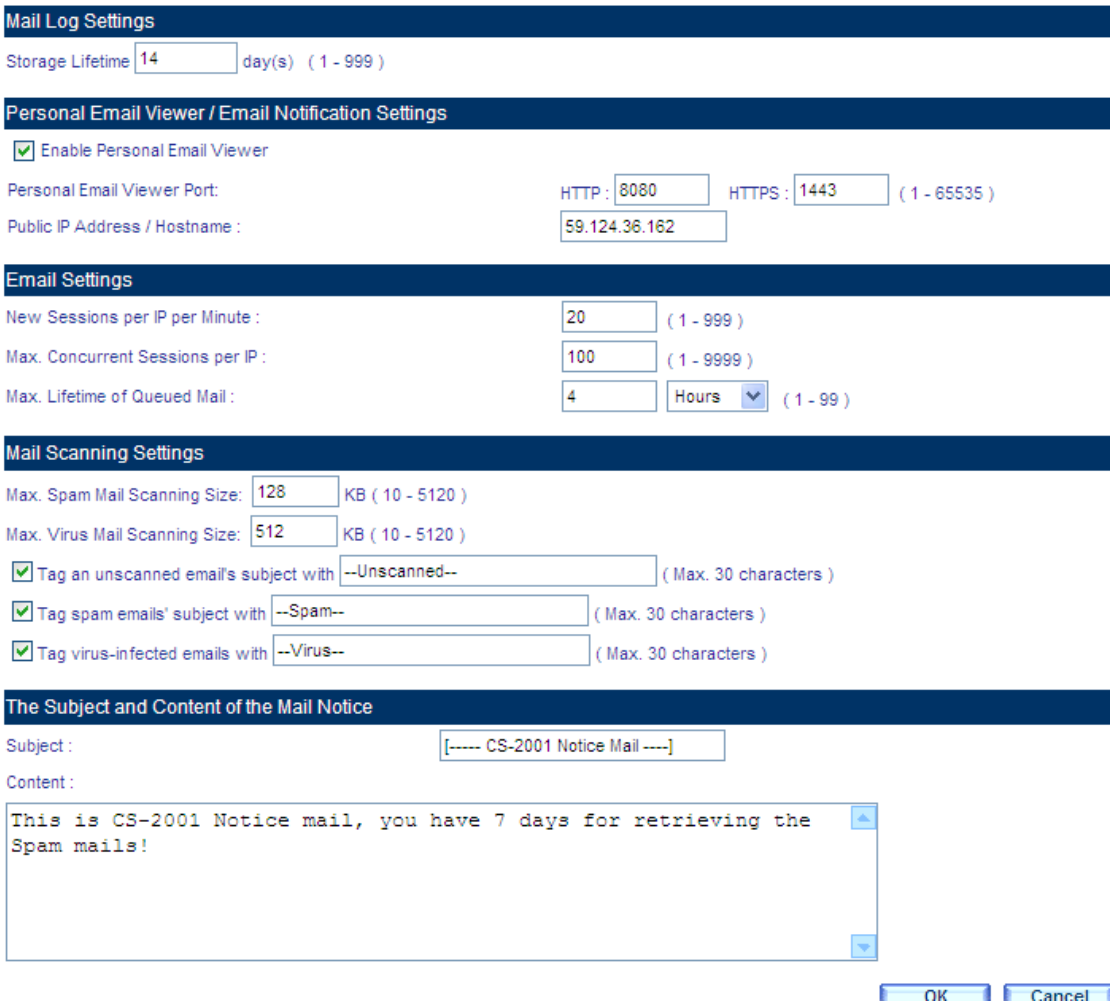


Figure 12-1 Configuring the Settings of Mail Security

- A notice with customized subject and message.（**Figure 12-2**）

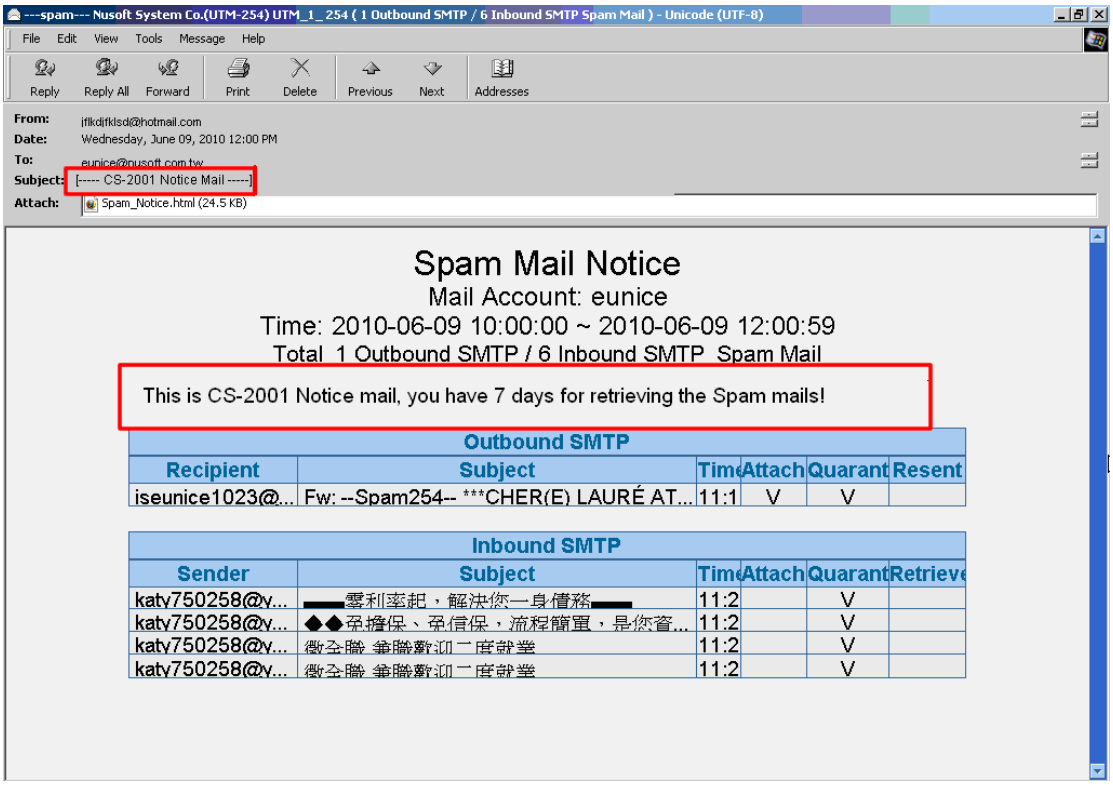


Figure 12-2 A Notice Shows Customized Subject and Message

- An unscanned email is highlighted with a warning message“---Unscanned---”.（**Figure 12-3**）

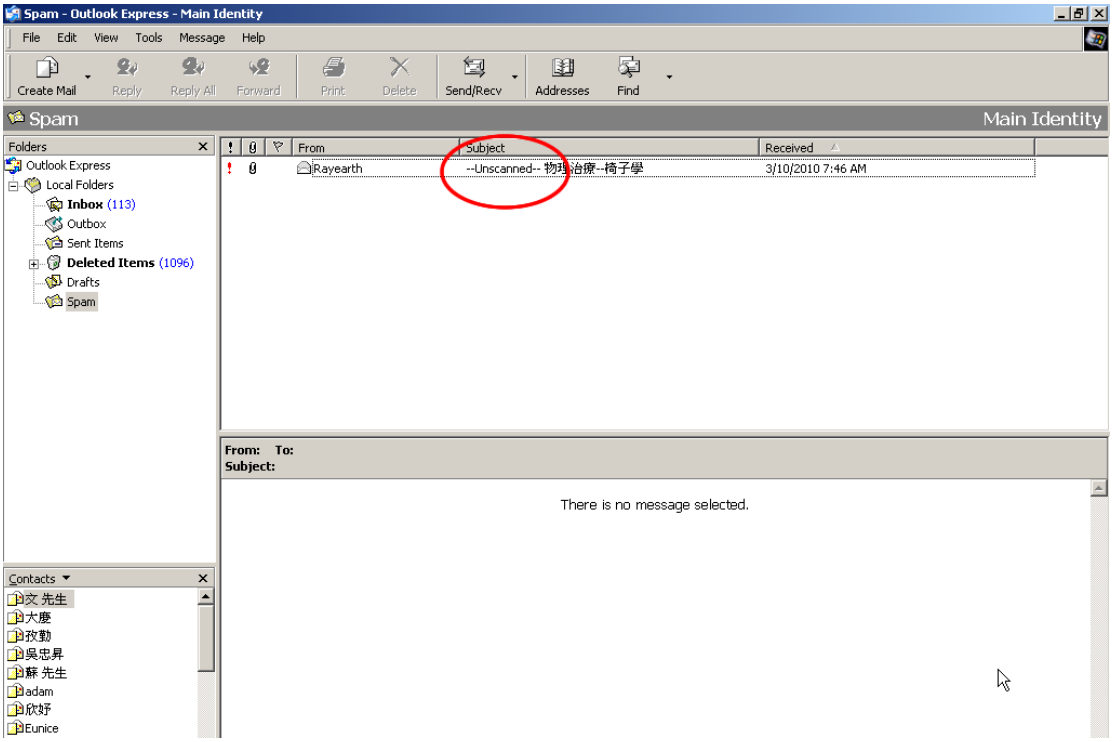


Figure 12-3 An Unscanned Email Shows a Warning Message

- The spam mail's subject tagged with warning message.（**Figure 12-4**）

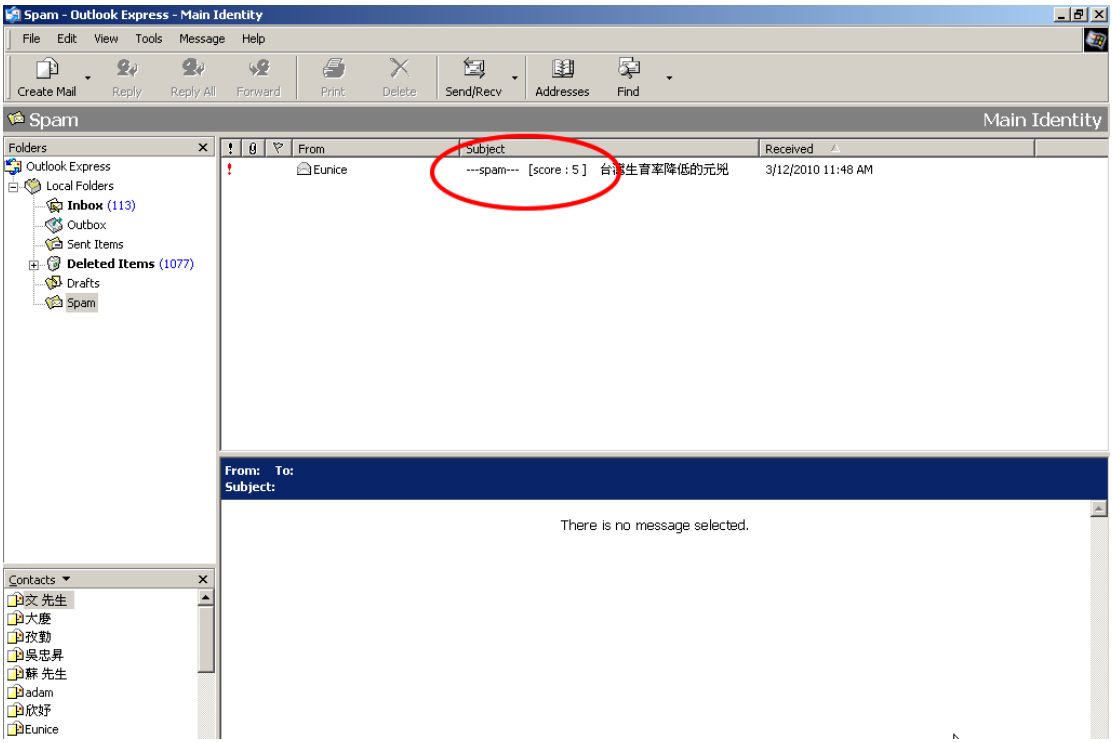


Figure 12-4 The Spam Mail's Subject Tagged with "Spam"

- The virus mail's subject tagged with warning message.（**Figure 12-5**）

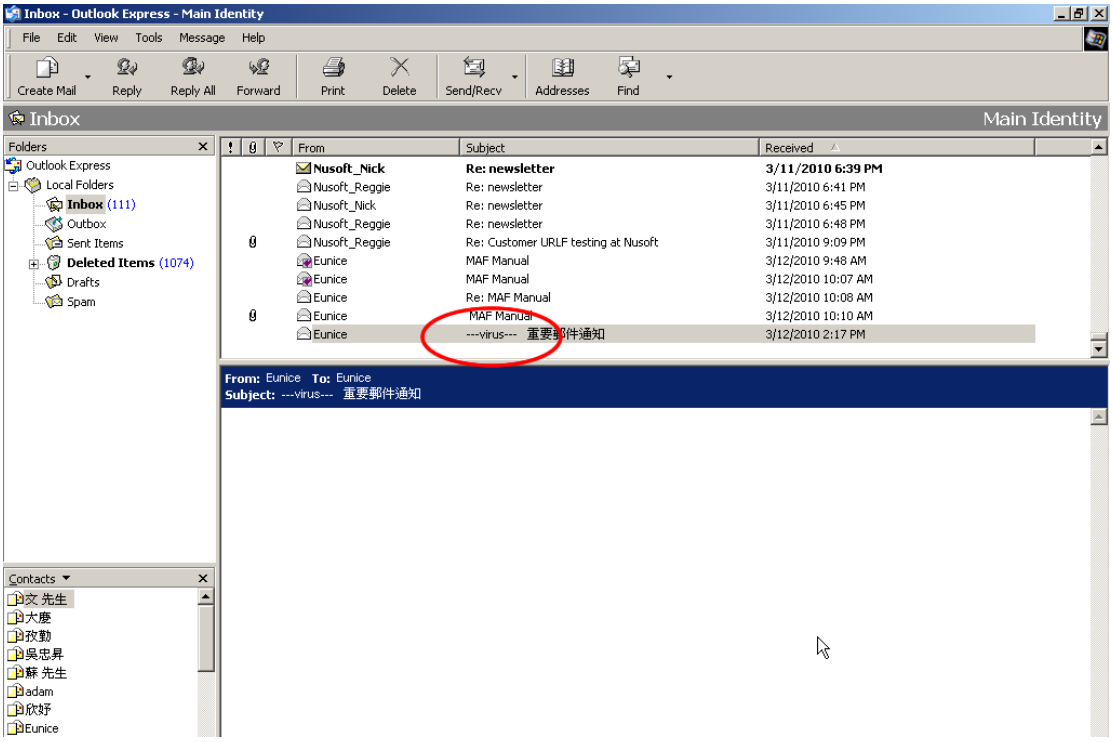


Figure 12-5 The Virus Mail's Subject Tagged with "Virus"

Terms in Account Manager

Account Learning Settings

- Disabled: Accounts added manually.
- Accounts added automatically: the email account will be added in the local mail server automatically once it is proved valid by the mail server.
- Synchronized with LDAP server: The accounts can be imported from LDAP server.

Terms in Queued Mail

Queued Mail

- Shows the status of queued mail.

12.1 Mail Domains

12.1.1 Using Mail Domains to Filter Emails

Step 1. Apply to a local ISP for several domain names, “planet.com.tw”, “supportplanet.com.tw”, “testplanet.com.tw” and “virtualplanet.com.tw” for instance, to provide mail service. The mapped IP address is 172.19.100.164.

Step 2. Under **Mail Management** > **Configuration** > **Mail Domains**, set as below:

- Click the **New Entry** button to create the first entry.
- Type **planet.com.tw** in the **Domain Name** field.
- Enter the mapped IP address.
- Click **OK** and then modify the domain.（**Figure 12-6, 12-7**）
- Click the **New Entry** button and then add a domain alias.
- Type **supportplanet.com.tw** in the **Domain Name** field.（**Figure 12-8**）
- Click **OK** to complete the first entry.（**Figure 12-9, 12-10**）
- Click the **New Entry** button again to create the second entry.
- Type **testplanet.com.tw** in the **Domain Name** field.
- Enter the mapped IP address.
- Click **OK** and then modify the domain.（**Figure 12-11, 12-12**）
- Click the **New Entry** button and then add a domain alias.
- Type **virtualplanet.com.tw** in the **Domain Name** field.（**Figure 12-13**）
- Click **OK** to complete the second entry.（**Figure 12-14, 12-15**）

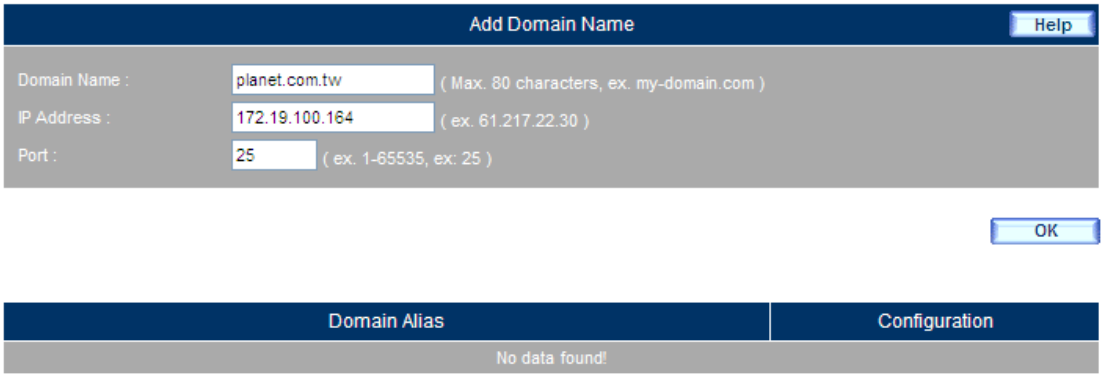


Figure 12-6 Creating the First Domain Name

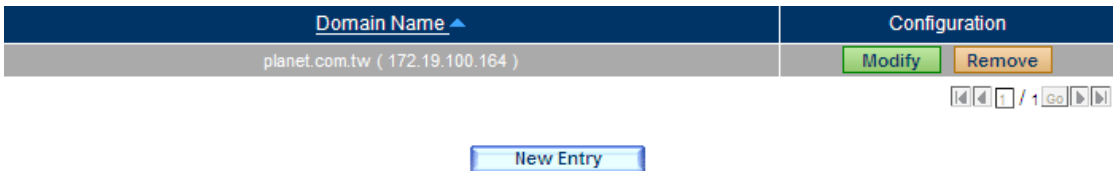


Figure 12-7 The First Entry Created

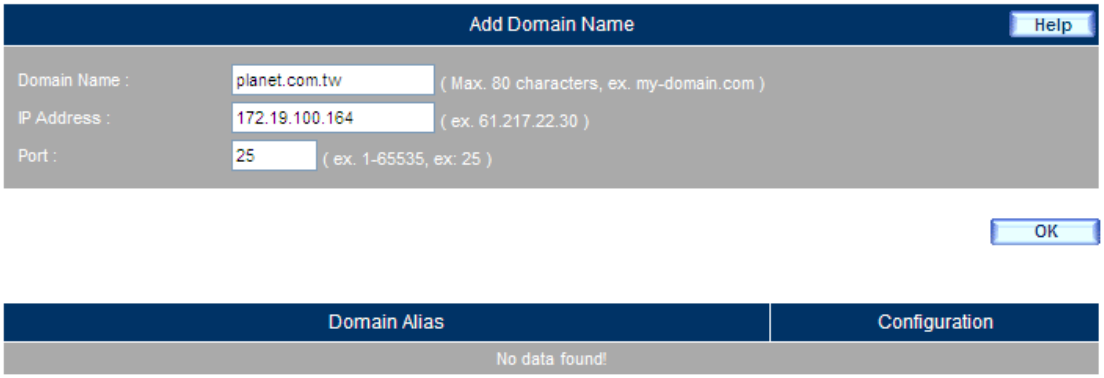


Figure 12-8 Modifying the First Entry

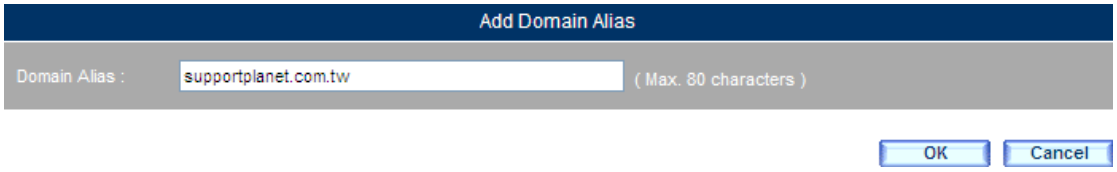


Figure 12-9 Typing the Domain Alias

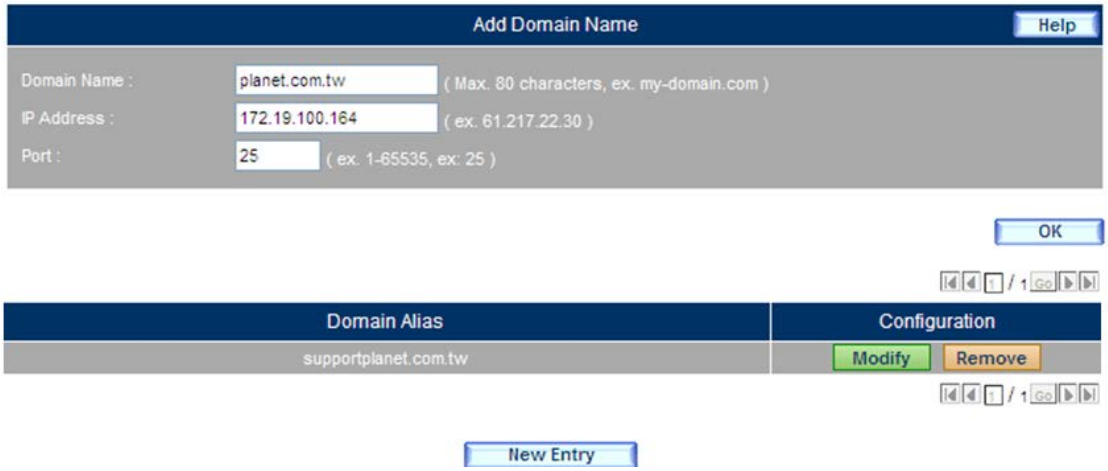


Figure 12-10 Settings Completed

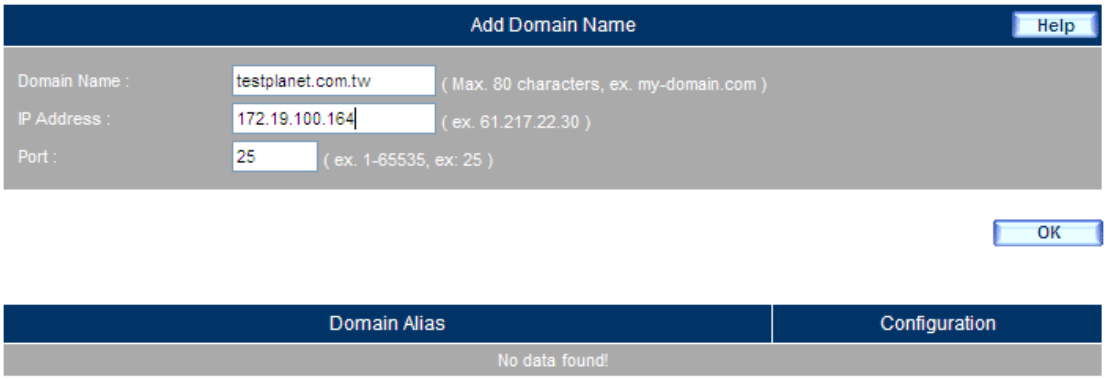


Figure 12-11 Creating the Second Entry

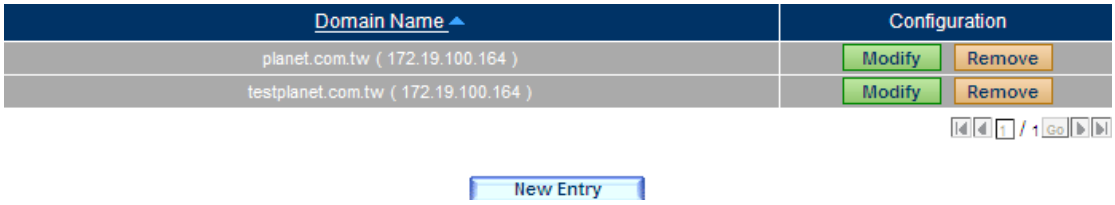


Figure 12-12 The Second Entry Completed

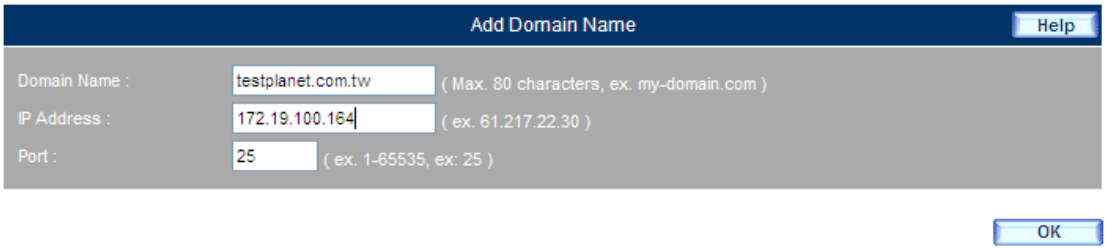


Figure 12-13 Modifying the Second Entry

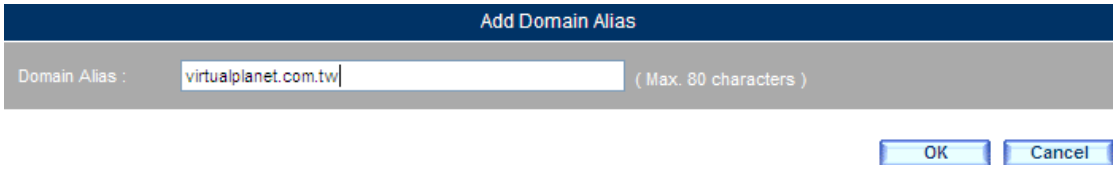


Figure 12-14 Typing the Domain Alias

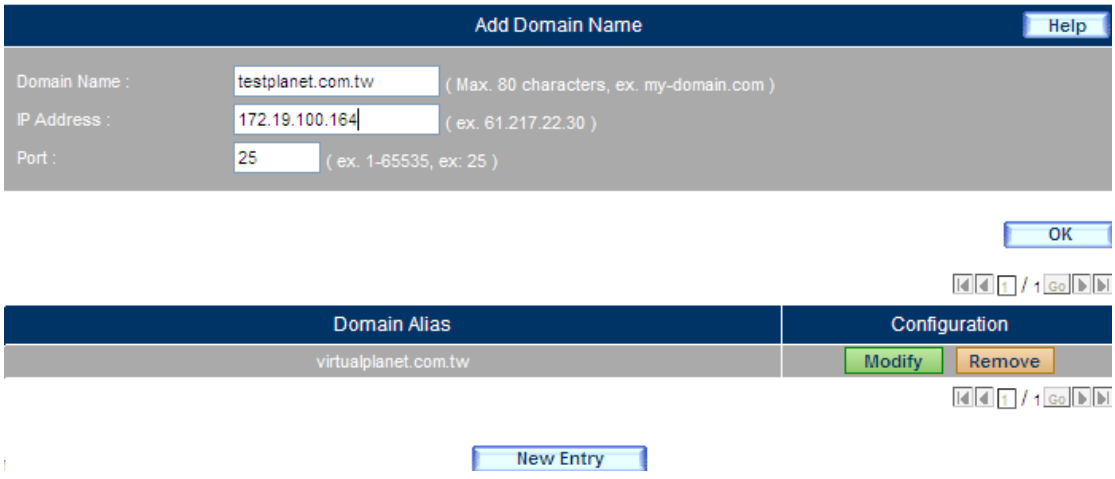


Figure 12-15 Settings Completed

Step 3. Emails sent to the internal account “alex”, depending on the domain name, will be handled as follows:

- Emails that go to alex@planet.com.tw or its alias alex@supportplanet.com.tw will be stored in the same storage location, the internal account “joe” will be able to retrieve them by logging in to either account.
- The user logs in alex@planet.com.tw or alex@supportplanet.com.tw is able to receive this mail.
- Emails that go to alex@testplanet.com.tw or alex@virtualplanet.com.tw will be stored in the same storage location, the internal account “joe” will be able to retrieve them by logging in to either account.
- The user logs in alex@testplanet.com.tw or alex@virtualplanet.com.tw is able to receive this mail.
- It can be concluded that however many aliases a domain has, whether emails are sent to the domain itself or any of the aliases, the recipient will be able to retrieve them anyhow.

Note：

1. The CS-2001 device will filter the emails according to the settings under **Mail Security > Configuration > Mail Domains.** If there is no **Mail Domains** settings, the filtered emails will be recorded under **Mail Security > Mail Reports > Logs > Outbound SMTP**.
2. The mail server port (SMTP) is 25 by default. If it is changed, you should enter the new one or mail server may not be able to deliver emails normally.

12.2 Account Manager

12.2.1 Using CS-2001 to Filter Mail Accounts

Step1. Go to **Mail Security** > **Configuration** > **Account Manager** and then configure the settings under the **Account Learning Settings** section:

- Select **Accounts added automatically**.
- Click **OK**.
- The CS-2001 filters any emails passing through by verifying with the mail server that the recipients account exists.
- Select **Import from LDAP server** and configure the settings.
- Click **OK**.
- The CS-2001 device will firstly require the account lists from the LDAP server.

Step2. Go to **Mail Security** > **Configuration** > **Account Manager**, export the account list and save the file:

- Click the **Export** button.

Click **Save** in the **File Download** dialog box. Specify the location and then click **Save**.

Step3. Go to **Mail Security > Configuration > Account Manager**, import the accounts into the system:

- Click the **Browse...** button. In the **Choose file** window, locate the file and then click the **Open** button.（**Figure 12-16**）
- Click the **Import** button. In the **Import Mail Account** window, select the file type and then click the **OK** button.
- In the confirmation window, click **OK** to complete the import.（**Figure 12-17**）

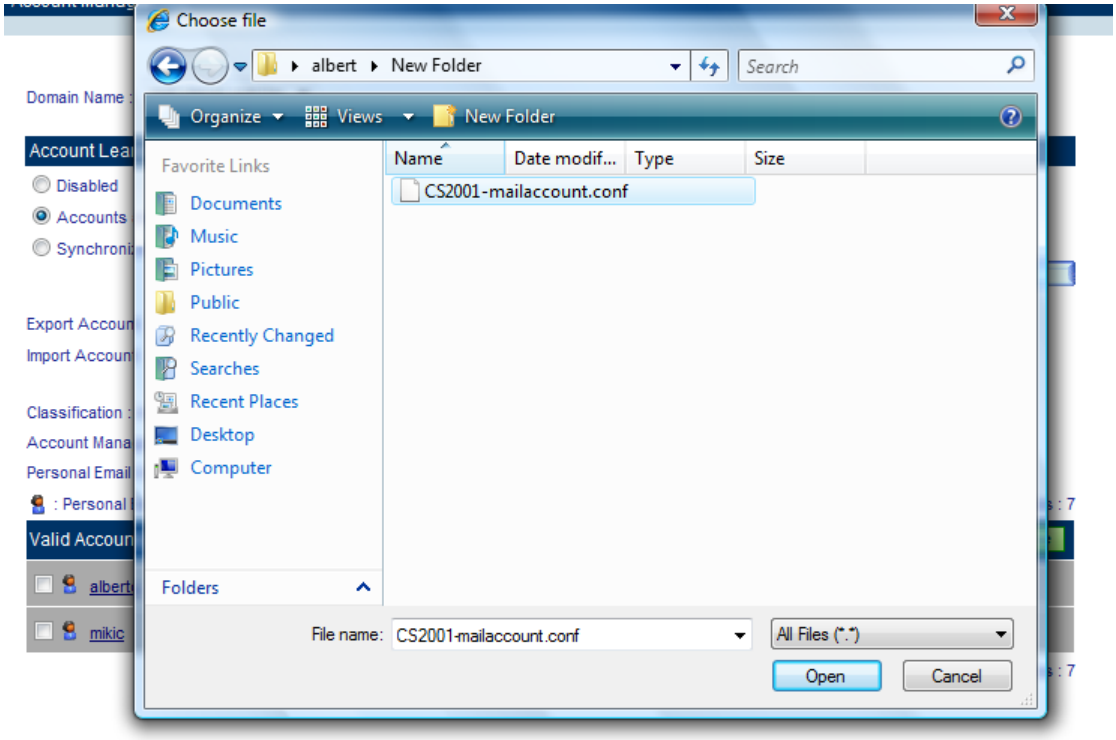


Figure 12-16 Selecting the File to be Imported

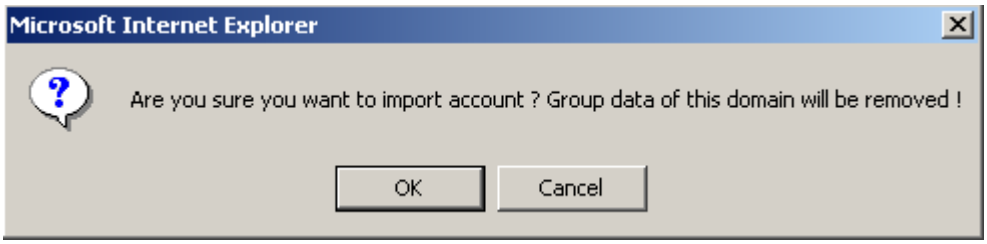


Figure 12-17 The Confirmation Window

Step4. Go to **Mail Security** > **Configuration** > **Account Manager**, add or remove the accounts.

- Click the **Add** button.
- Enter the account information.（**Figure 12-18**）
- Click the **OK** button.（**Figure 12-19**）
- To remove the account, select the account and then click the **Remove** button.
- Click the **OK** button in the confirmation window.（**Figure 12-20**）

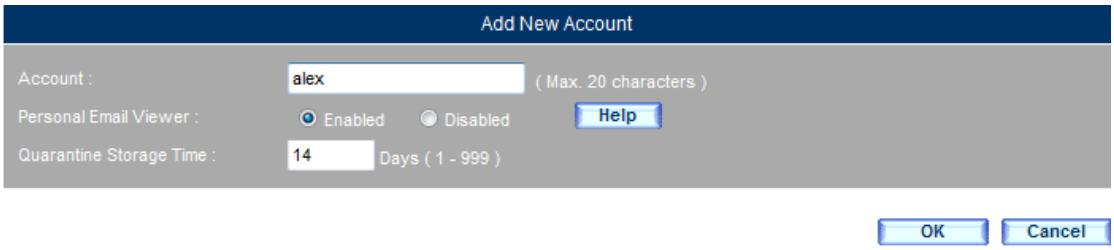


Figure 12-18 Adding an Account

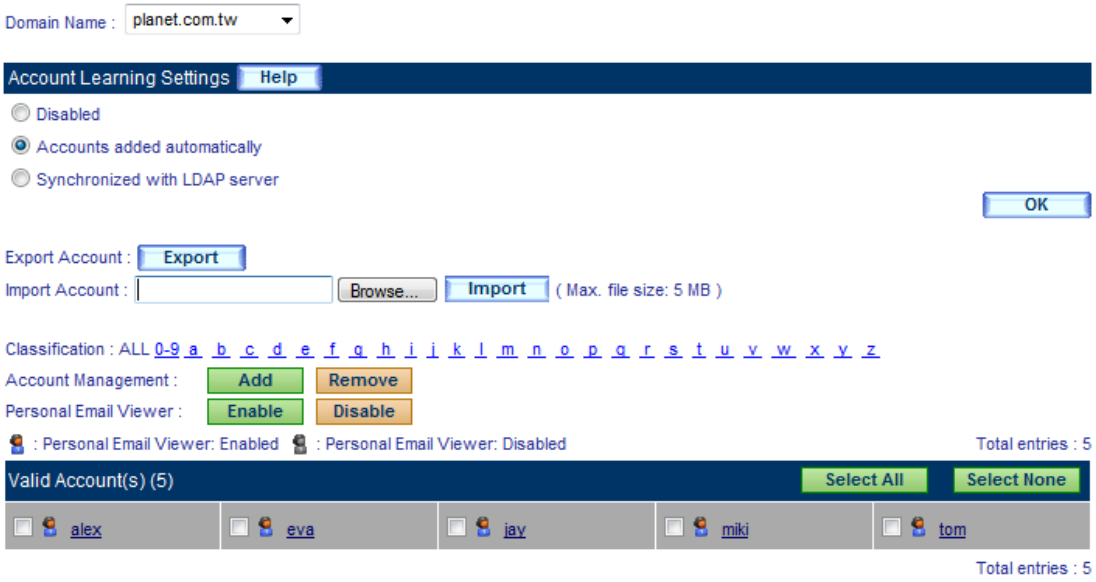


Figure 12-19 Account Added

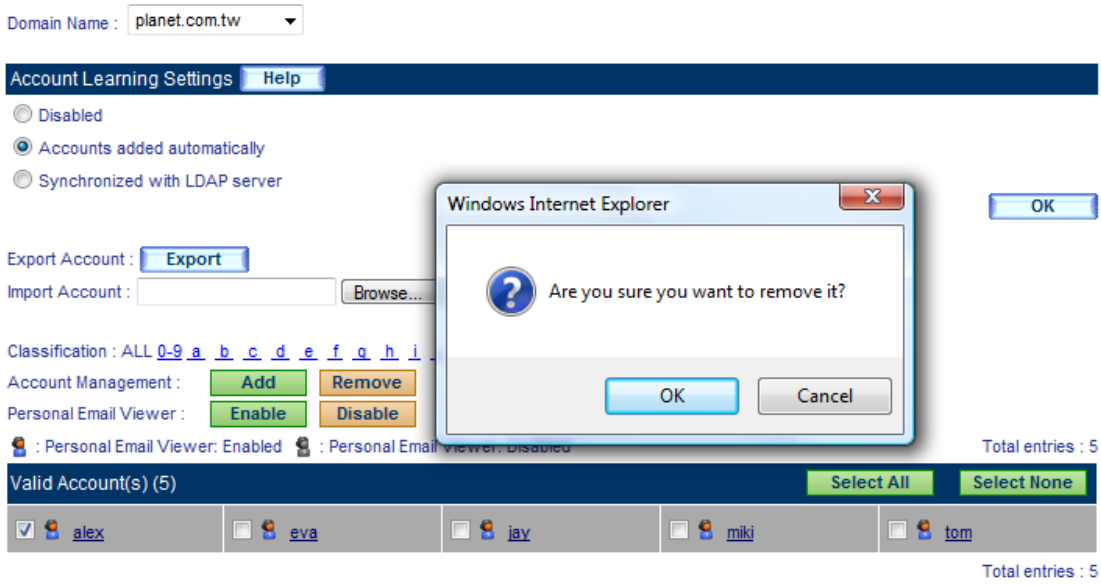


Figure 12-20 Removing the Account

Note：

1. Once **Accounts added automatically** is selected, the CS-2001 will varify the existence of the account with the mail server before relaying the mail.
2. When **Imported from LDAP server** is selected, the CS-2001 will determine whether to relay the email by varifying the account with the LDAP accounts list. (The MAF-1000 queries the LDAP server for the list every 30 minutes.)
3. The **Quarantine Storage Time** field under the **Add New Account** section is the storage time of the scanned incoming / outgoing emails. Under **Mail Security > Configuration > Settings**, the **Storage Time of Quarantined Logs** under the **Log Storage Time** section is the storage time of the scanned emails under **Mail Security > Mail Reports > Log**.

Step5. Users may be given permission to access Personal Email Viewer under **Mail Security > Configuration > Account Manager**.

- To permit a user to access Personal Email Viewer, select the account(s) and then click **Enable Personal Email Viewer**.
- Click **OK** in the confirmation window.（**Figure 12-21**）
- If you do not permit the user to access the Personal Email Viewer, select the account(s) and then click **Disable Personal Email Viewer**.
- Click **OK** in the confirmation window.（**Figure 12-22**）

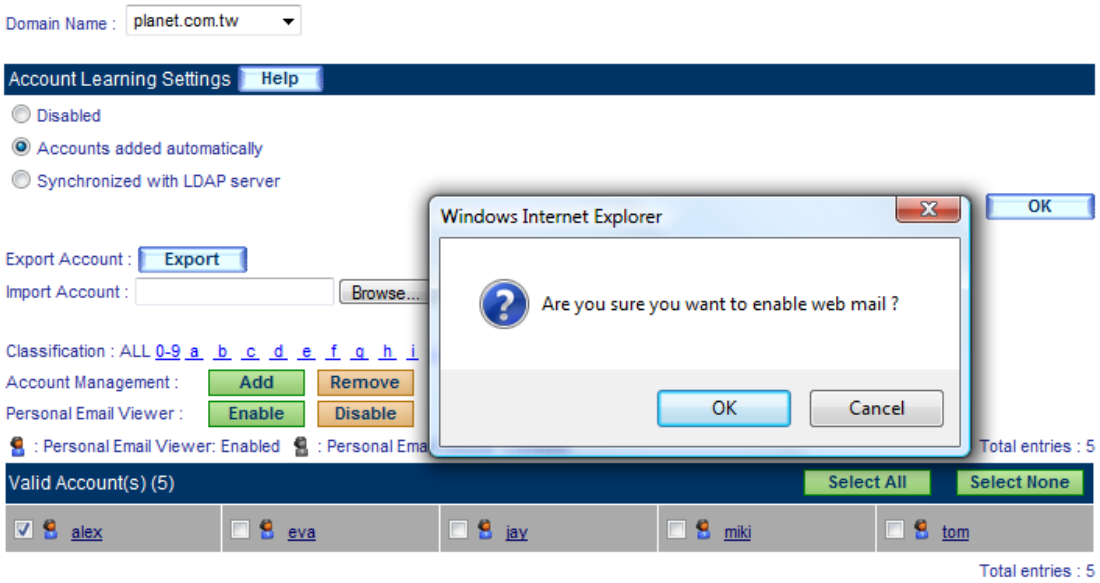


Figure 12-21 Giving a User the Permission to Access Web Mail

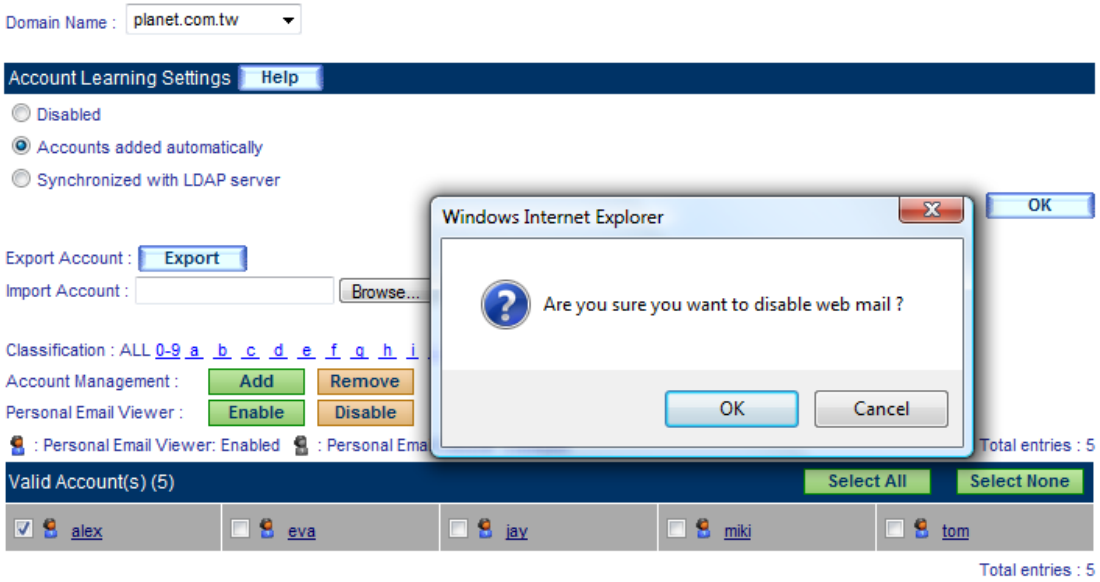


Figure 12-22 Disabling a User from Accessing Web Mail

12.2.2 Accessing Personal Email Viewer

Step 1. Type the management address together with the HTTP port (8080) or HTTPS port (1443) in the address field of a Web browser.（**Figure 12-23**）

- Type the account name and the password.
- Select the mail domain from the drop-down list.
- Click the **Login** button.
- The account will be authenticated with the designated mail server.

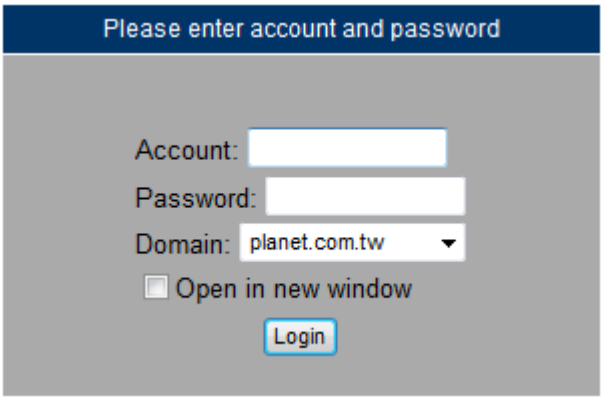


Figure 12-23 The Webmail Login Page

Step 2. Users will be requested to configure user preferences during their first login.

- Click **Continue.**（**Figure 12-24**）
- Configure the **User Preferences** accordingly.（**Figure 12-25**）
- Click **Save.**
- Settings completed.（**Figure 12-26**）
- Click **Continue.**

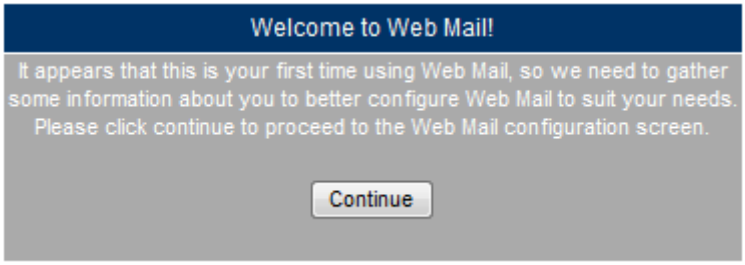


Figure 12-24 The Greeting Message Shown upon First Login

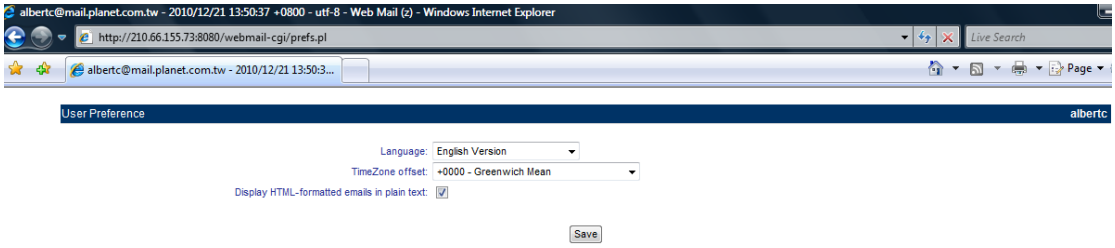


Figure 12-25 The User Preferences Settings

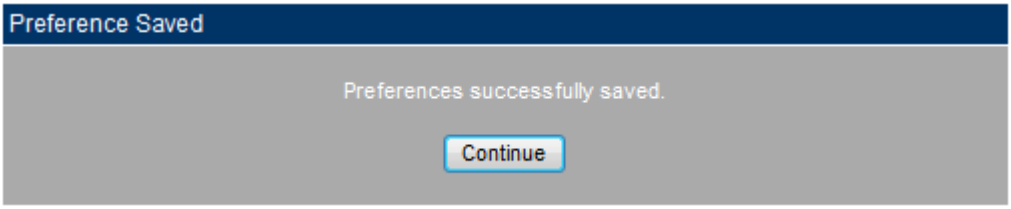


Figure 12-26 User Preferences Settings Completed

Step 3. Below shows the CS-2001's user-friendly, web-based mailbox.(**Figure 12-27**)

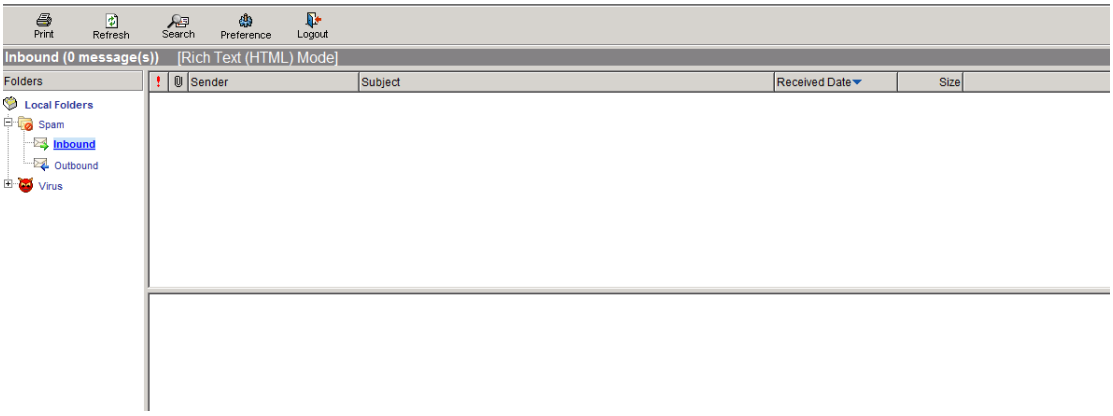


Figure 12-27 The Web Mail User Interface

12.2.3 Using Whitelist and Blacklist to Filter Emails

Supposed the domain name “planet.com.tw” is registered to your organization, and you are using the account “joe” to log in to Personal Email Viewer, then:

Step 1. Click **Preference** in the Web Mail main screen and then a pop-up window appears. Click the **Whitelist** button under the **User Preference** section:

- Click the **New** button.
- Enter share2k01@yahoo.com.tw in the **Email Address/ Domain Name** field.
- Select **From** form the **Direction** drop-down list.
- Click the **OK** button.（**Figure 12-28**）
- Click the **New Entry** button again.
- Enter share2k01@yahoo.com.tw in the **Email Address/ Domain Name** field.
- Select **To** from the **Direction** drop-down list.
- Click the **OK** button.（**Figure 12-29**）
- Settings completed.（**Figure 12-30**）

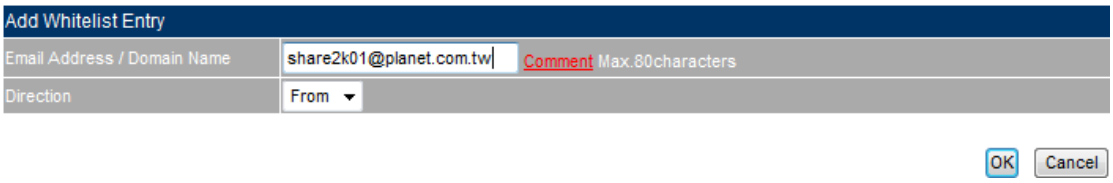


Figure 12-28 Creating the First Entry of Whitelist

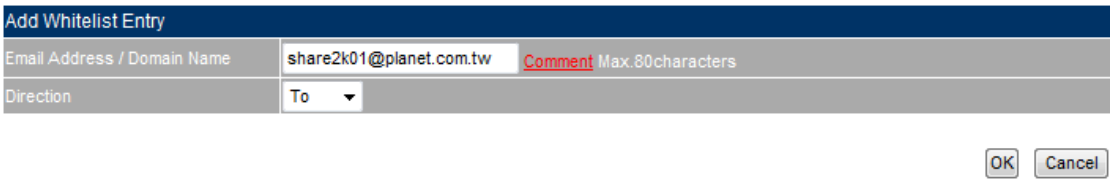


Figure 12-29 Creating the Second Entry of Whitelist

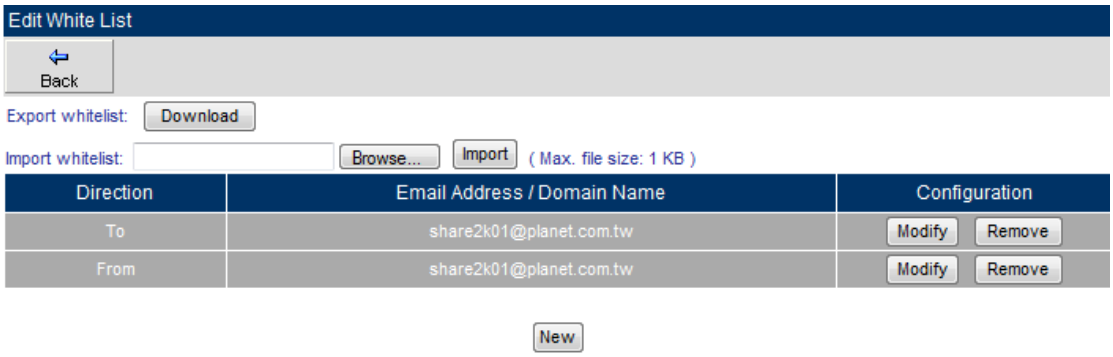


Figure 12-30 Settings Completed

Step 2. Click **Preference** in the Personal Email Viewer main screen and then a pop-up window appears. Click the **Blacklist** button under the **User Preference** section.

- Click the **New** button.
- Type ***yahoo*** in the **Email Address/ Domain Name** field.
- Select **From** from the **Direction** drop-down list.
- Click the **OK** button.（**Figure 12-31**）
- Click the **New** button again.
- Enter ***yahoo*** in the **Email Address/ Domain Name** field.
- Select **To** from the **Direction** drop-down list.
- Click the **OK** button.（**Figure 12-32**）
- Settings completed.（**Figure 12-33**）

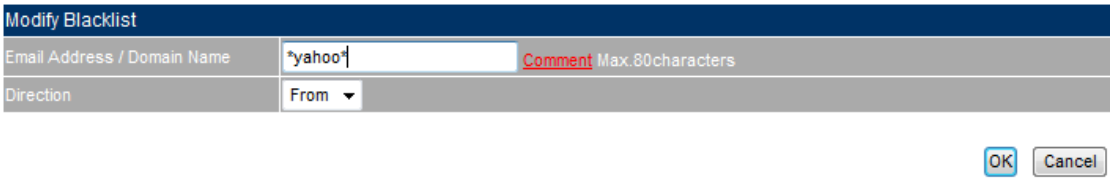


Figure 12-31 Creating the First Entry of Blacklist

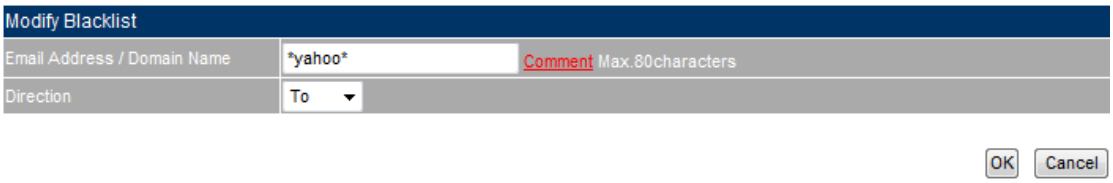


Figure 12-32 Creating the Second Entry of Blacklist

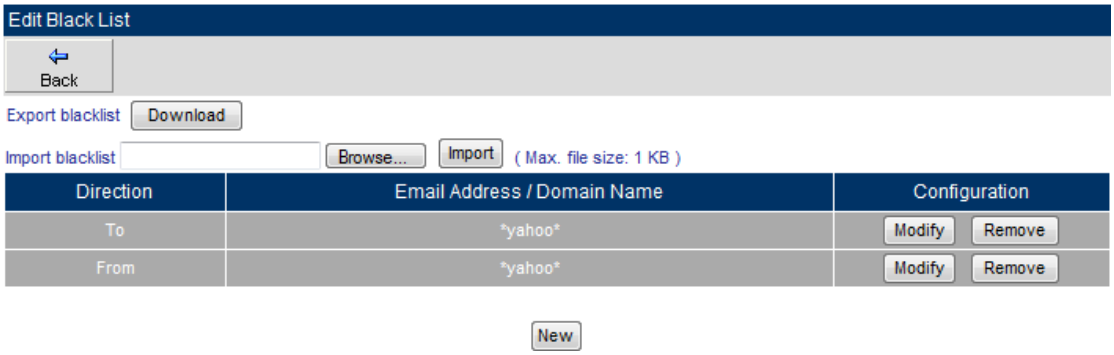


Figure 12-33 Blacklist Created

Step 3. When joe@planet.com.tw receives an email from a yahoo account:

- If the mail is from share2k01@yahoo.com.tw, then joe@planet.com.tw will receive it.
- If the mail is from another yahoo account, such as share2k003@yahoo.com.tw, then it will be rated as a spam mail.

Step 4. When joe@planet.com.tw sends emails to both share2k01@yahoo.com.tw and share2k003@yahoo.com.tw:

- share2k01@yahoo.com.tw will receive the emails from joe@planet.com.tw.
- Emails sent to share2k003@yahoo.com.tw will be rated as spam mail.
- Only share2k01@yahoo.com.tw will receive emails from joe@planet.com.tw, whereas share2k003@yahoo.com.tw receives none as a result of emails sent to it are classified as spam.

12.3 Mail Relay

12.3.1 Using CS-2001 as a Gateway (Set the Mail Server in DMZ under Transparent Mode)

Prerequisite Setup

Configure Port1 as LAN1 (192.168.1.1, NAT/Routing Mode) and connect it to the LAN which is using the IP range 192.168.1.X/24.
Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.
Configure Port3 as DMZ1 (Transparent Routing) and connect it to the mail server. IP address: 61.11.11.12.

Map the registered domain name “supportplanet.com.tw” (used here only as an example) to the mail server IP address by creating a MX record.

In order to relay emails to recipients in supportplanet.com.tw, refer to the steps below to configure:

Step 1. Go to **Mail Security** > **Configuration** > **Mail Domains** and then set as below:（**Figure 12-34**）

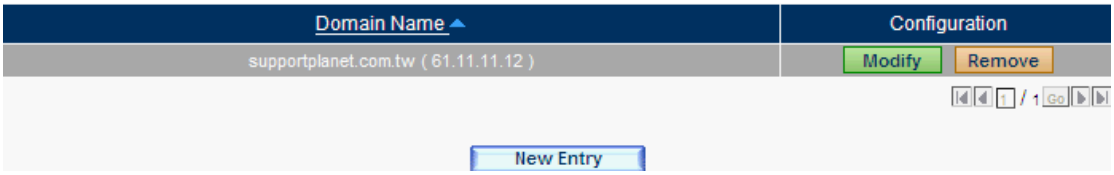


Figure 12-34 Mail Domain Settings

Step 2. Go to **Mail Security** > **Configuration** > **Mail Relay** and then set as below: （**Figure 12-35**）

- Select **Sender's IP Address**.
- Type the **IP Address** and the **Netmask**.
- Click **OK**.

Figure 12-35 Mail Relay Settings

Note：

1. In this example, the **Mail Relay** setting is used for determining the emails sent from the mail server under DMZ1.
   - If the recipient is an internal user (supportplanet.com.tw), the email will be recorded under **Mail Security** > **Mail Reports** > **Logs** > **Inbound SMTP** after filtering.
   - If the recipient is an external user, the email will be recorded under **Mail Security** > **Mail Reports** > **Logs** > **Outbound SMTP** after filtering.
2. Given that a valid internal account sends an email to the extenal recipient upon the activation of SMTP authentication, then there is no need to configure the **Sender's IP Address** under **Mail Security** > **Configuration** > **Mail Relay**.

12.3.2 Deploying the CS-2001 Device between the Gateway and Mail Server (Mail Server is in DMZ under Transparent Mode)

Prerequisite Setup

LAN Segment: 172.16.x.x/16
Configure Port1 as WAN1(172.16.1.12) and connect it to the LAN.
Configure Port2 as DMZ1 (Transparent Routing mode) and connect it to the mail server. (LAN IP 172.16.1.13 mapping to the WAN IP 61.11.11.11)

Map the registered domain name “supportplanet.com.tw” (used here as an example only) to the mail server IP address by creating a MX record.

In order to relay emails to third party recipients, refer to the steps below to configure:

Step 1. Go to **Mail Security** > **Configuration** > **Mail Domains** and then set as below:（**Figure 12-36**）

Figure 12-36 Configuring the Mail Domains

Step 2. Go to **Mail Security** > **Configuration** > **Mail Relay** and then set as below:

- Click **New Entry**.（**Figure 12-37**）
- Select **Sender's IP Address**.
- Type the IP Address and the Netmask.
- Click **OK**.
- Click **New Entry** again.（**Figure 12-38**）
- Select **Sender's IP Address**.
- Enter the IP Address and the Netmask.
- Click **OK**.

Figure 12-37 The First Entry of Mail Relay

Figure 12-38 The Second Entry of Mail Relay

12.3.3 Using CS-2001 as Gateway to Enable Branch's Employees to Send Emails via Headquarters' Mail Server (Set the Mail Server under DMZ Transparent Routing Mode)

Prerequisite Setup

Configure Port1 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Configure Port2 as DMZ1 (Transparent Routing mode) and connect it to the mail server. IP address: 61.11.11.12

Branch's WAN Interface: 211.22.22.22

Map the registered domain name "supportplanet.com.tw" (used here as an example only) to the mail server IP address by creating a MX record.

In order to relay emails from branch's employees to third party recipients via headquarters' mail server, refer to the steps below to configure:

Step 1. Go to **Mail** > **Configuration** > **Mail Domains** and then set as below: (**Figure 12-39**)

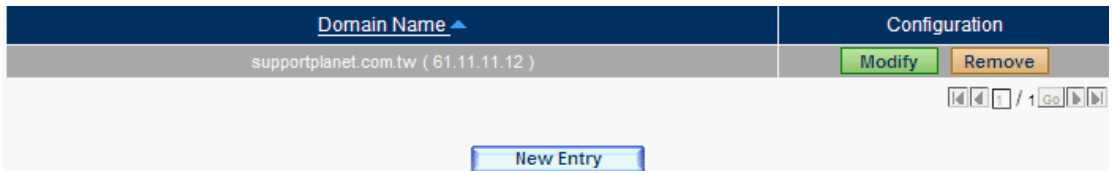


Figure 12-39 Configuring the Mail Domains

Step 2. Go to **Mail Security** > **Configuration** > **Mail Relay** and then set as below: （**Figure 12-40**）

- Select **Sender's IP Address**.
- Enter the IP Address and the Netmask.
- Click **OK**.

Figure 12-40 Mail Relay Settings

12.4 Mail Notice

12.4.1 Retrieving Spam or Virus Emails from the Mail Notice

(An Outlook Exparess Example)

Step 1. All the accounts are listed under **Mail Security** > **Configuration** > **Mail Notice** but only accounts in the **Selected Accounts** column will be notified: （**Figure 12-41**）

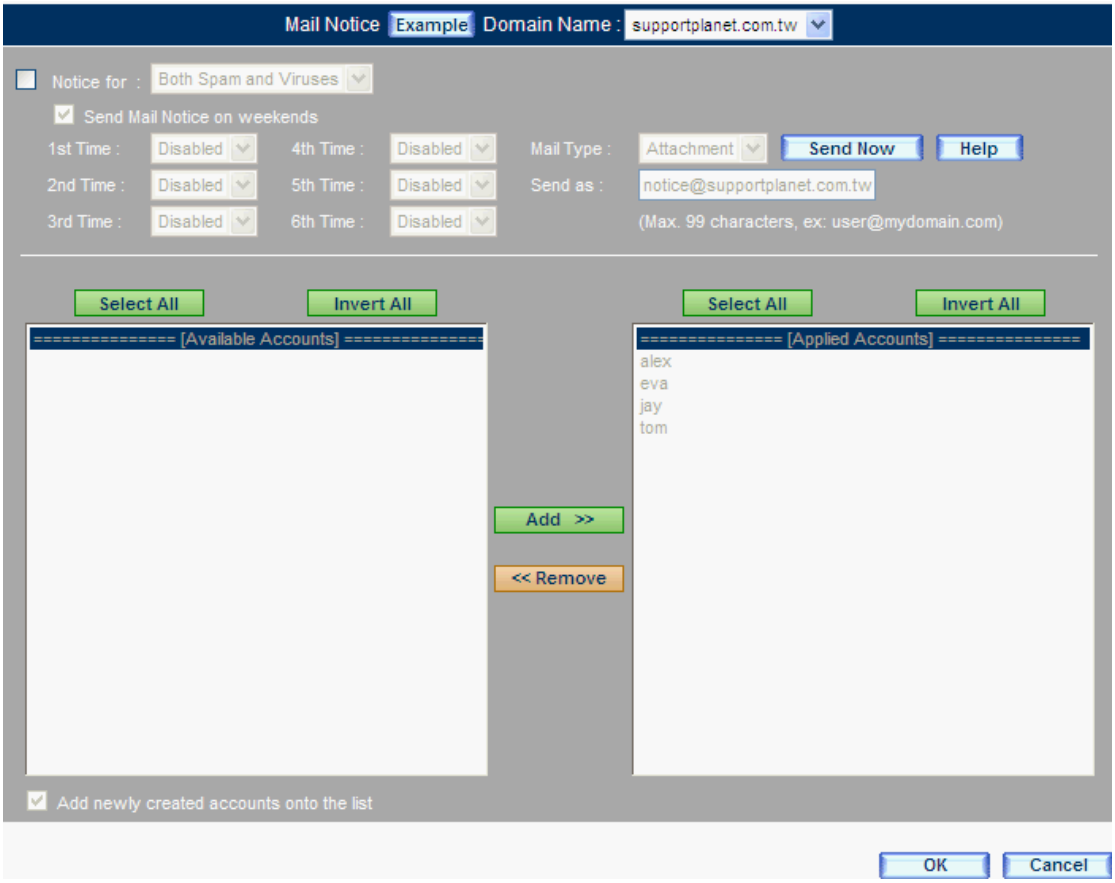


Figure 12-41 Selecting Accounts to be Notified

Step 2. Go to **Mail Security > Configuration > Mail Notice** and then set as below:

- Tick **Notice for**, then select “Both Spam and Viruses” from the drop-down list.
- Tick **Send Mail Notice on weedends**.
- Select “00 : 00” for **1st Time.**
- Select “04 : 00” for **2nd Time.**
- Select “08 : 00” for **3rd Time.**
- Select “12 : 00” for **4th Time.**
- Select “16 : 00” for **5th Time.**
- Select “20 : 00” for **6th Time.**
- Select “HTML” for **Mail Type.**
- In the **Send as** field, type an email address to appear as the notification sender.
- To cancel the email notification for certain users, choose the users from **Selected Accounts** and then click **Remove.**
- To ensure new accounts are automatically added to the **Selected Accounts** column, tick **Add newly created accounts onto the list.**

（Figure 12-42）

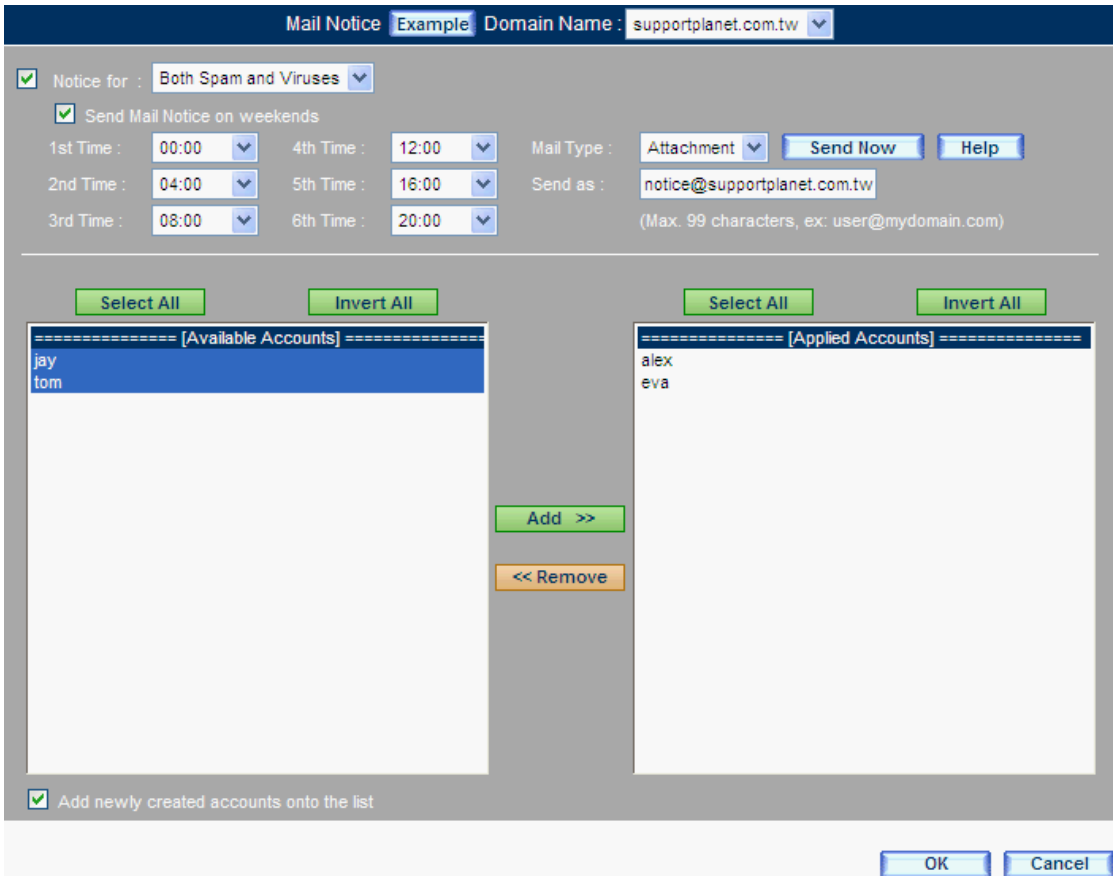


Figure 12-42 Mail Notice Settings

Note：

1. Accounts in the **Selected Accounts** column will receive a mail notice based upon schedules when emails sent from or to them are classified as spam or virus emails.
2. Up to six email notifications can be sent based upon the time order, starting from the earliest time set.
3. If there are no spam or virus emails, the designated accounts won't receive any notifications.
4. IT administrators can use the **Select All** button or the **Invert All** button to select accounts from the list, and then click **Add** or **Remove** to either allow or disallow them from receiving mail notices.
5. If **Send Mail Notice on weekends** is disabled, mail notices will not be issued on weekends but will be issued according to the first scheduled time on the upcoming Monday.
6. If **Add newly created accounts on the list** is disabled, newly created accounts will not receive mail notices.

12.5 Queued Mail

12.5.1 Monitoring Email Delivery Status

Step 1. Go to **Mail Security** > **Configuration** > **Settings** and then set as below:

- **Max. Lifetime of Queued Mail**: 4 hour.
- When the delivery has failed, the system will keep trying to resend the email to the recipient periodically within the storage time.（**Figure 12-43**）

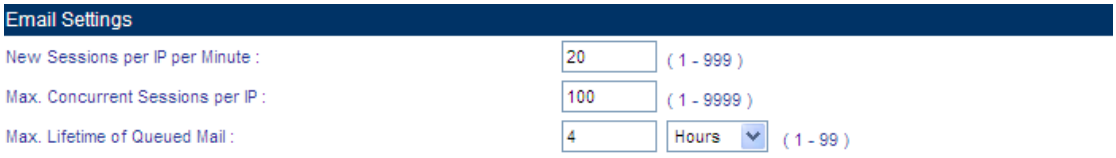


Figure 12-43 Specifying the Storage Time of an Email

Step 2. Go to **Mail Security** > **Configuration** > **Queued Mail** to obtain the delivery status.

- A symbol, under the **Reason** column, indicates an email is being processed (delivered).（**Figure 12-44 Figure 12-45**）
- Factors that caused failed deliveries are obtainable and the email can be resent by clicking **Resend**.
- Emails in the queue will be periodically resent until the delivery is successful or the **Max. lifetime of Queued Mail** has been exceeded.
- To stop queued emails from delivery, tick the corresponding checkboxes then click Clear (or click Clear All simply to remove them all).

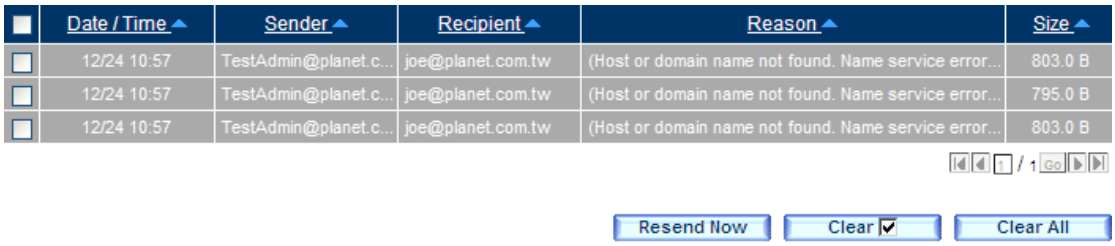


Figure 12-44 Emails Being Processed

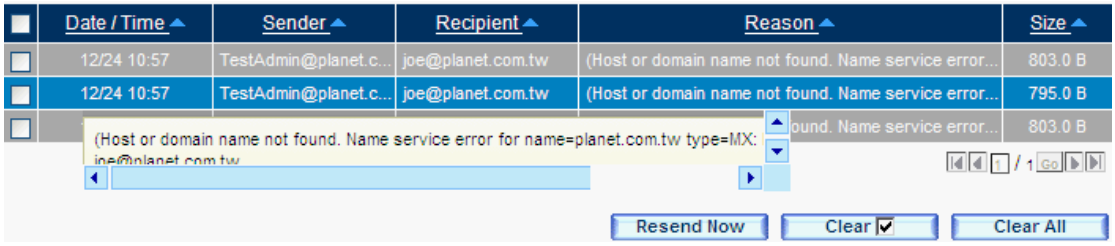


Figure 12-45 A Failed Delivery

12.6 Mail Signatures

Step 1. Go to **Mail Security** > **Configuration** > **Mail Signatures** and then set as below:

- Tick **Add signatures to all outgoing messages**.
- Type the message to be shown in the text field.
- Click **OK** to complete the settings.（**Figure 12-46**）

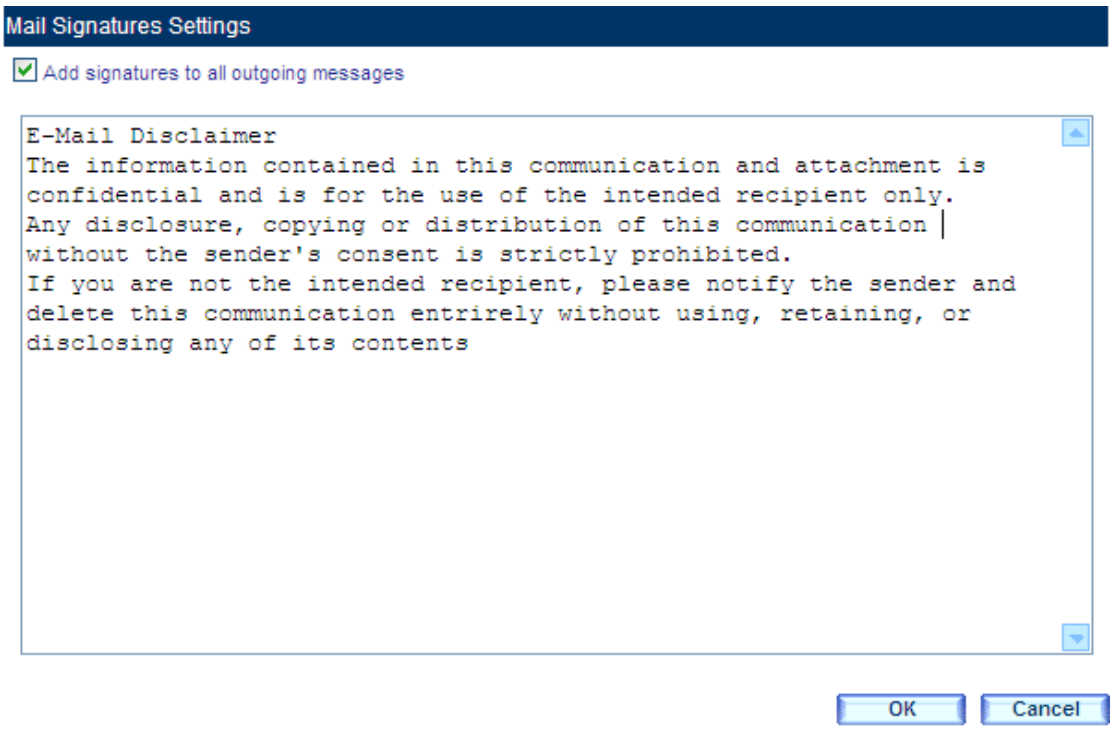


Figure 12-46 Mail Signature Settings

Step 2. Any email sent from the CS-2001 will now have the signature message appended to the body of the email for the recipient to view.（**Figure 12-47**）

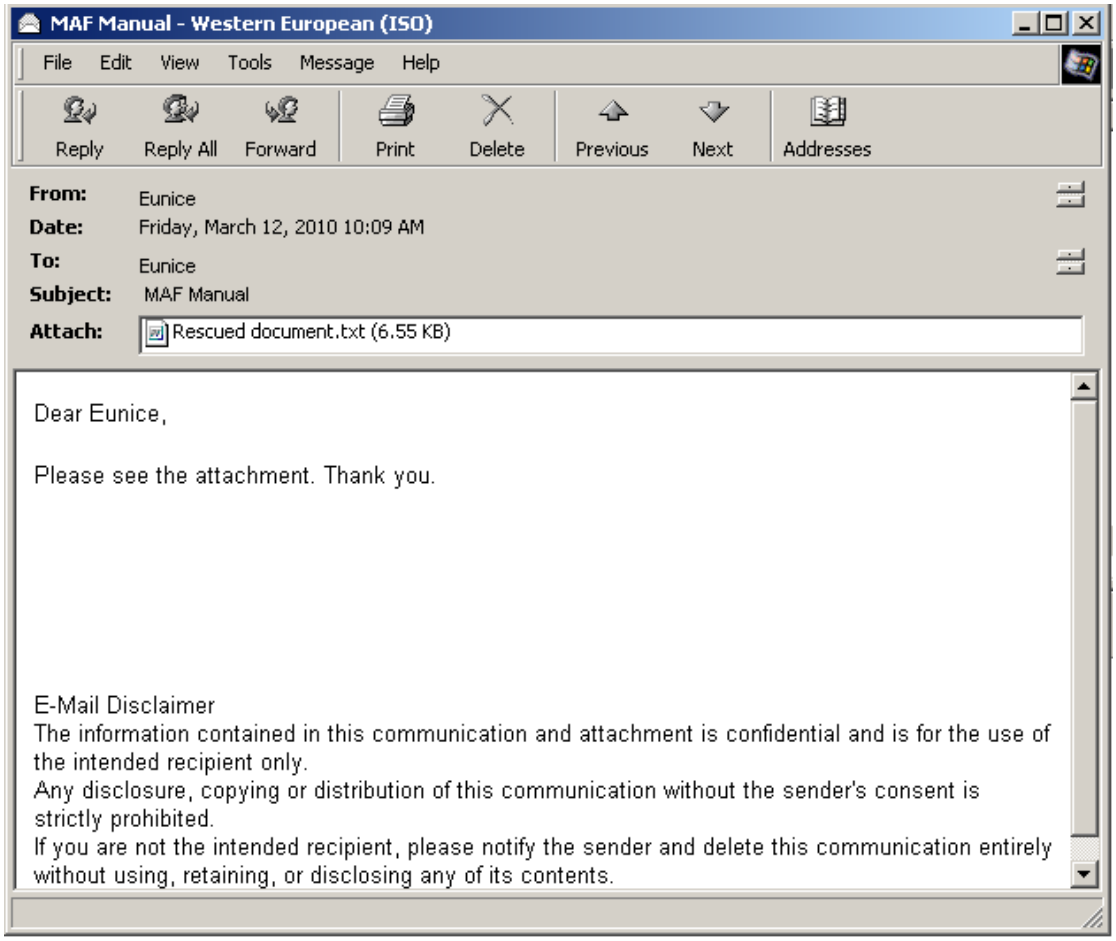


Figure 12-47 Email with the Mail Signatures

Chapter 13 Anti-Spam

Users will no longer be disturbed by large influxes of spam. The Anti-Spam mechanism prevents the users from wasting their time on searching for business emails amongst the spam. It also lowers the risk of accidentally deleting business emails when deleting spam.

Terms in Settings

Anti-Spam Filter Settings

- Incoming and outgoing emails can be inspected.
- Emails exceeding the threshold score can have a warning message added and a score tag appended to the subject, whereas others below the threshold score can only have a score tag appended in the subject line.
- The inspection methods utilized:
  - **Verify with spam fingerprint database**: Generates an ID number by analyzing the email with algorithms, and then makes a comparison with the spam ID list on the server.
  - **Enable spam signature push update**: Generates a value by analyzing the email with algorithms, and then compares it to the spam signatures on the database.
  - **Greylist Filtering**: Rejects the session requests from new senders for the first time.
  - **Verify sender's IP with Real-Time Block List**: Compares the sender's IP address to the blacklist on the server.
  - **Enable Bayesian filtering**: Compares the email header to the Bayesian database.
  - **Enable Sender Policy Framework(SPF)**: Checks whether the sender's IP address is identical with the one specified in the DNS SPF record.
  - **Enable DomainKey**: Verifies the domain of an email sender and the message integrity.
- Configuring the filtering priority of Personal rules and Global rules.

Note：

1. Once the Proxy Server is deployed, the proxy settings under **System > Configuration > Settings** must be configured for the CS-2001 to access the Internet.
2. The CS-2001 will apply its default spam filtering settings if no method has been selected.
3. Bayesian filtering is not effective unless at least 200 messages have been classified for spam and ham individually.（**Figure 13-1**）

Figure 13-1 The Amount of Spam and Ham in the Database

Spam Actions (Sending)

- The action of outbound spam mail can be set to delete, deliver as normal or store the quarantine.

Spam Actions (Receiving)

- The action of inbound spam mail is deliver. In addition, you may also store the spam in the quarantine.
  - Go to **Mail Security > Anti-Spam > Settings** and then set as below:
    - **The threshold score to classify mail as spam is**: select 5.
    - Tick **Add score tag to the subject line**.
    - Tick **Deliver the email as normal** under the **Spam Actions (Sending)** section.
    - Click OK.（**Figure 13-2**）

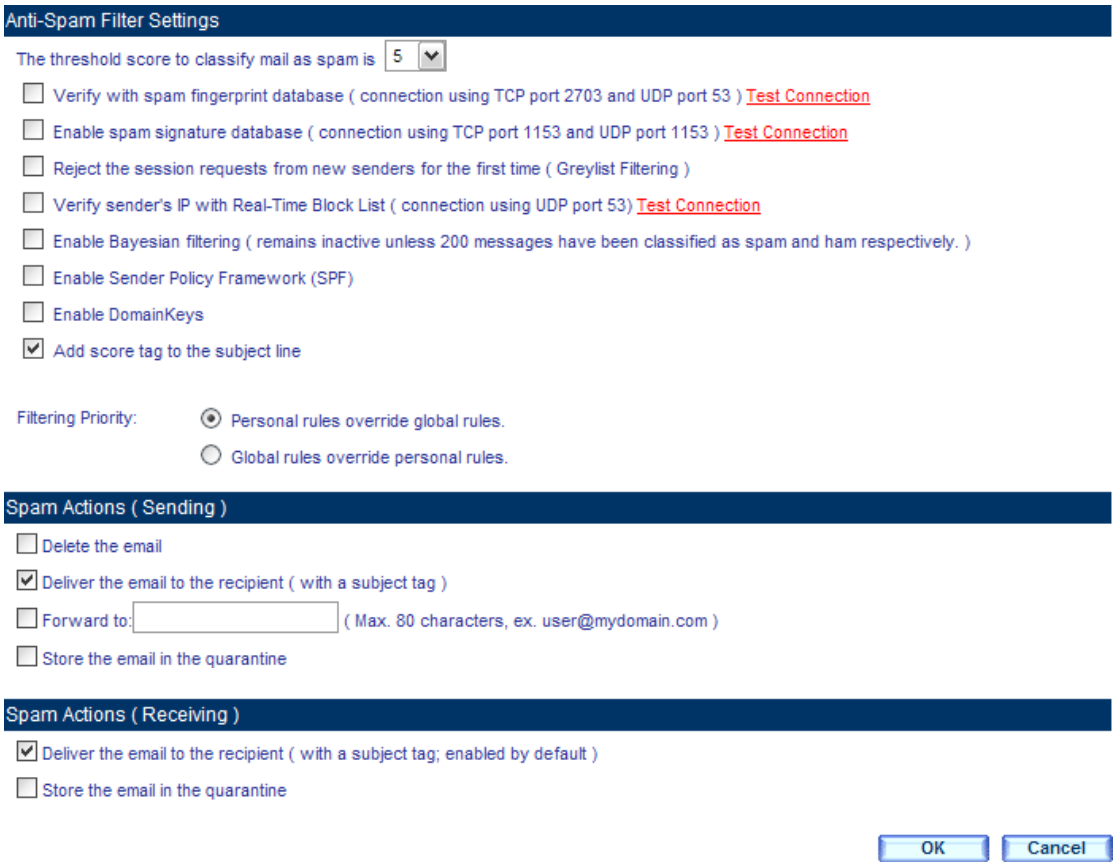


Figure 13-2 Anti-Spam Settings

- The figure below shows that an email's subject is tagged with the score (optional).（**Figure 13-3**）

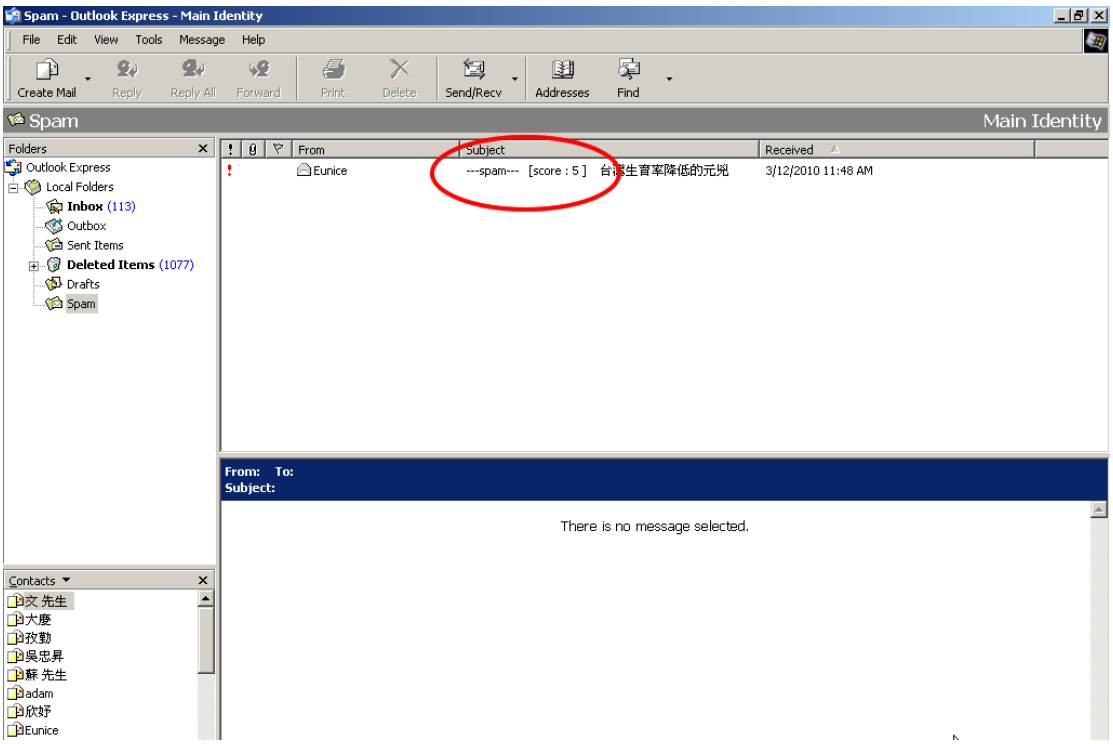


Figure 13-3 An Email's Subject Tagged with the Score

Terms in Personal Rule

Search

- Used for searching for individual emails.
- Used for retrieving quarantined emails.

Whitelist

- Specifies permitted email addresses.

Blacklist

- Specifies prohibited email addresses.

Terms in Global Rule

Rule Name

- The name for an inspection rule.

Comment

- The description of the rule's name.

Classification

- When **Spam** is selected, emails that meet the inspection criteria will be classified as spam.
- When **Ham (Non-Spam)** is selected, emails that meet the inspection criteria will be classified as ham.

Action

- This only functions when **Classification** is set to spam as there is no need for it if there are no emails being classified as spam.
- Spam can be deleted, quarantined, or delivered to the recipient.

Combination

- And: Only emails that meet all the criteria will be classified as spam or ham.
- Or: An email just has to satisfy one of the specified criterion to be regarded as spam or ham.

Item

- Uses email attributes, such as header, body, attachment name, size, mailcommand-From and mailcommand-To to examine whether an email is spam or not.
- The email header can be subdivided into received, envelope-to, from, to, Cc, Bcc, subject, sender, reply-to, errors-to, message-ID, date and header for spam inspection.

Condition

- When **item** is set to header, body, attachment name, mailcommand-From or mailcommand-To, the corresponding conditions are contains, does not contain, is equal to, is not equal to, starts with, ends with, exists and does not exist.
- When **item** is set to size, the corresponding conditions are larger than, is equal to, is not equal to and less than.

Pattern

- Rates an email as spam or ham according to the settings of item and condition. For example, when **item** is set to from, condition is set to contains along with

“joe” typed as a pattern, it means emails from whosever email account contained the word “joe” will be considered as spam or ham.

Terms in Whitelist

Email Address/ Domain Name

- Used to designate specific email addresses as ham.

Direction

- From: Inspects emails sent from a specific sender address.
- To: Inspects emails sent to a specific recipient address.

Terms in Blacklist

Email Address/ Domain Name

- Used to designate specific email address as spam.

Terms in Training

Bayesian Database Management

- Enables the IT administrator to import, export or reset the training database.

Spam Training Using Importing

- Spam emails can be imported onto the device for training purposes to increase the inspection accuracy.

Ham Training Using Importing

- Ham emails can be imported onto the device for training purposes to increase the inspection accuracy.

Spam Training Using Forwarded Mail

- IT administrator may designate a separate email account for reporting spam emails. Through the help of users, spam emails can be reported to CS-2001 to raise filtering accuracy.

Ham Training Using Forwarded Mail

- IT administrator may designate an email account for reporting ham emails. Through the help of users, ham emails can be reported to CS-2001 to raise filtering accuracy.

Training Schedule

- CS-2001 can be scheduled a daily time for spam or ham training.
- CS-2001 can be set to immediately train.

An Overview on Email Transmission

A mail server acts as an intermediary among users during mail delivery or retrieval. The format of an email address looks like “account@server.name”. Information on the left side of an “at” sign (@) indicates an account name while the other side denotes the host name or domain name.

For instance, when sending an email from an email application, a DNS query will be made to retrieve the MX record from the domain name. This will return a list of host names of mail exchange servers. The email will be sent to the host name with the highest preference number. If no MX records could be retrieved, the email will be sent to the A record of the domain name. The account name will then be used to send the email to the specified email account.

The Three Key Elements of Email Transmission

An email transmission is achieved by using an MUA, MTA and MDA.

- **MUA（Mail User Agent）**：Whether sending or receiving email, the end-user client must rely on an MUA which came along with the OS, as without it they are unable to obtain email access. Outlook Express, for example, serves as a mail deliverer and recipient, as well as enables user to view and compose emails.
- **MTA（Mail Transfer Agent）**：Email delivery and retrieval are done by a MTA. It allows users to:
  - Receive emails from other hosts. As long as user has an account on the MTA, then the user will be able to receive emails.
  - Sent out emails. If the user is authorized, he or she will be able to send out emails.
  - Retrieve emails from the mail server.
- **MDA（Mail Delivery Agent）**：It distributes incoming emails from the MTA to local email accounts based on the account names or passes them on to the next MTA.

Note：

1. Usually, MTA refers to an mail server.

How an Email is Processed

Composing and sending an email:

- Email delivery from an MUA to an MTA: Run a MUA client (email program) and follow the instructions below:
  - Apply the sender address and the domain name of outgoing mail server (sender MTA), to the corresponding fields.
  - Apply the recipient address and the domain name of incoming mail server (recipient MTA), to the corresponding fields.

After finished composing the email with a MUA application, such as Outlook Express, the user can deliver it to the specified MTA by clicking “Send”.

- If a MTA receives emails dedicated to internal accounts, the local MDA will distribute the received emails to accounts based on account names.
- If a MTA receives emails dedicated to external accounts, it will automatically forward them to the destination address. This functionality is called “Relay”.
- If a remote MTA receives emails sent from the local MTA, its MDA will distribute them by the account names.

Receiving emails:

User uses MTA and MDA to check emails. If there is a new email, it will be moved to the inbox of the user’s MUA application on the local computer. Meanwhile, the MTA will clean up the remaining emails according to the MUA application settings. If the configuration is set to keep the retrieved emails, then the read emails will still be available when the recipient logs on to check emails.

Note：

1. Email protocols: SMTP & POP3

- Email delivery: signifies emails transferred from MUA to MTA and from MTA to MTA. Nowadays, most mail servers use SMTP (Simple Mail Transfer Protocol) for outgoing emails. By default, port 25 is assigned to the SMTP protocol.

- Email retrieval: signifies MUA is using POP (Post Office Protocol) to communicate with the MTA by which users may have the access to emails. Currently, POP3 (Post Office Protocol version 3) is the most popular protocol for incoming emails. By default, port 110 is assigned to the POP3 protocol.

2. MTA needs at least two protocols, namely SMTP and POP3, to receive and send emails. As long as both your MUA and MTA support SMTP and POP3 protocols, you will be able to have email access.

3. Relay, a function that MTA transfers emails to another MTA, functions when MTA has received emails intended for external recipients, it will pass them onto the destination MTA.

4. When a mail server can be used for sending emails by anyone, it is called “Open Relay”. To avoid this, nowadays most mail servers preserve the “Relay” functionality to the local MTA. Only the local MTA can utilize relay to receive emails that were specified for its internal accounts. Nevertheless, there is a drawback in using relay. Since relay normally only allows email from certain trusted mail servers with specified IPs or segments, emails from other unspecified mail servers will be rejected. SMTP authentication, therefore, is the solution to this situation.

5. SMTP authentication, a mechanism whereby the MTA inspects the sender’s address and password on the MUA, takes place when emails transfer from the MUA to the MTA. It has a benefit of enabling relay only to the authorized accounts rather than just certain trusted domain names or IP addresses. Whenever SMTP authentication is employed, the MTA will neither accept incoming emails nor provide email delivery services unless the sender is authenticated.

13.1 Example

No.	Scenario	Page
13.1.1	Detecting Whether Emails are Spam	**459**
13.1.2	Using CS-2001 in Accordance with Whitelist and Blacklist to Filter Spam (Mail Server Is Deployed in DMZ under Transparent Mode)	**471**
13.1.3	Deploying CS-2001 in between Gateway and Mail Server and Filtering Spam with Global Rule (Mail Server Is Deployed in DMZ under Transparent Mode)	**483**
13.1.4	Improving Bayesian Filtering Accuracy by Training Spam Filtering / Ham-Filtering (An Outlook Express Example)	**497**
13.1.5	Improving Bayesian Filtering Accuracy by Training Spam Filtering / Ham-Filtering	**518**

13.1.1 Detecting Whether Emails are Spam

Prerequisite Setup

Configure Port1 as LAN1(192.168.1.1, NAT/ Routing mode) and connect it to the LAN which is using 192.168.1.x/24.

Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range: 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2(211.22.22.22) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range: 211.22.22.18 to 211.22.22.30.

Configure Port4 as DMZ1 (Transparent Routing mode) and connect to the mail server. IP address: 61.11.11.12.

Step 1. To enable internal users to receive emails from an external mail server, configure the setting of **Preferred DNS Server** in **Internet Protocol (TCP/IP) Properties** on local computer. (Note: the DNS server can be any external DNS server, please decide which to use on your own.)

Step 2. To enable external users to receive emails from internal mail server, set as below:

1. Deploy the mail server in DMZ.
2. Type “61.11.11.12” in the **IP Address** field of **Internet Protocol (TCP/IP) Properties.**
3. Configure the **Preferred DNS Server** field in **Internet Protocol (TCP/IP) Properties**. (Use an external DNS server to resolve domain names)
4. Name the server as “supportplanet.com.tw”.

Step 3. Under **Policy Object** > **Address** > **DMZ**, set as below:（**Figure 13-4**）

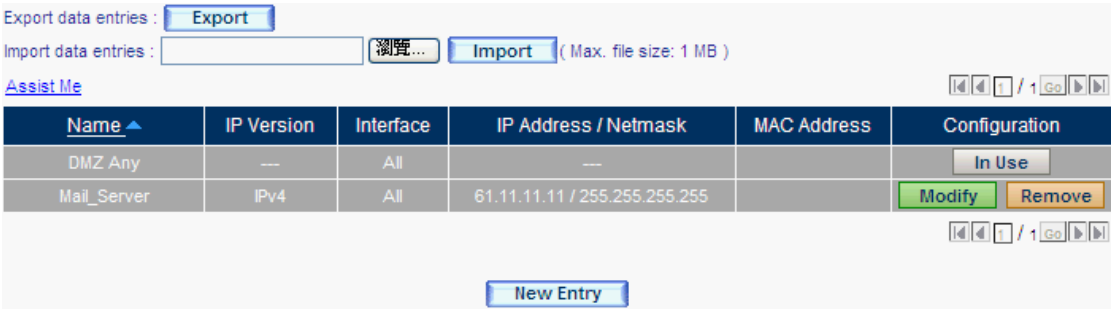


Figure 13-4 Creating an Address Setting Corresponding to the Mail Server

Step 4. Under **Policy Object** > **Service** > **Group**, set as below:（**Figure 13-5**）

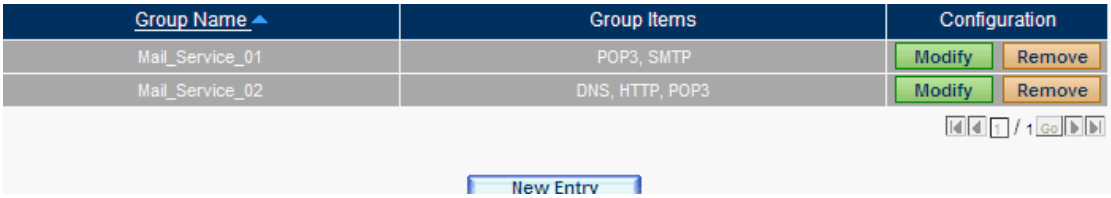


Figure 13-5 Creating Service Groups to Include the POP3, SMTP or DNS Services

Step 5. Go to **Policy** > **Outgoing** and then set as below: （**Figure 13-6**）

- Select the defined group (Mail_Service_02) from the **Service** drop-down list.
- Tick POP3 for **Anti-Spam**.
- Click **OK**.（**Figure 13-7**）

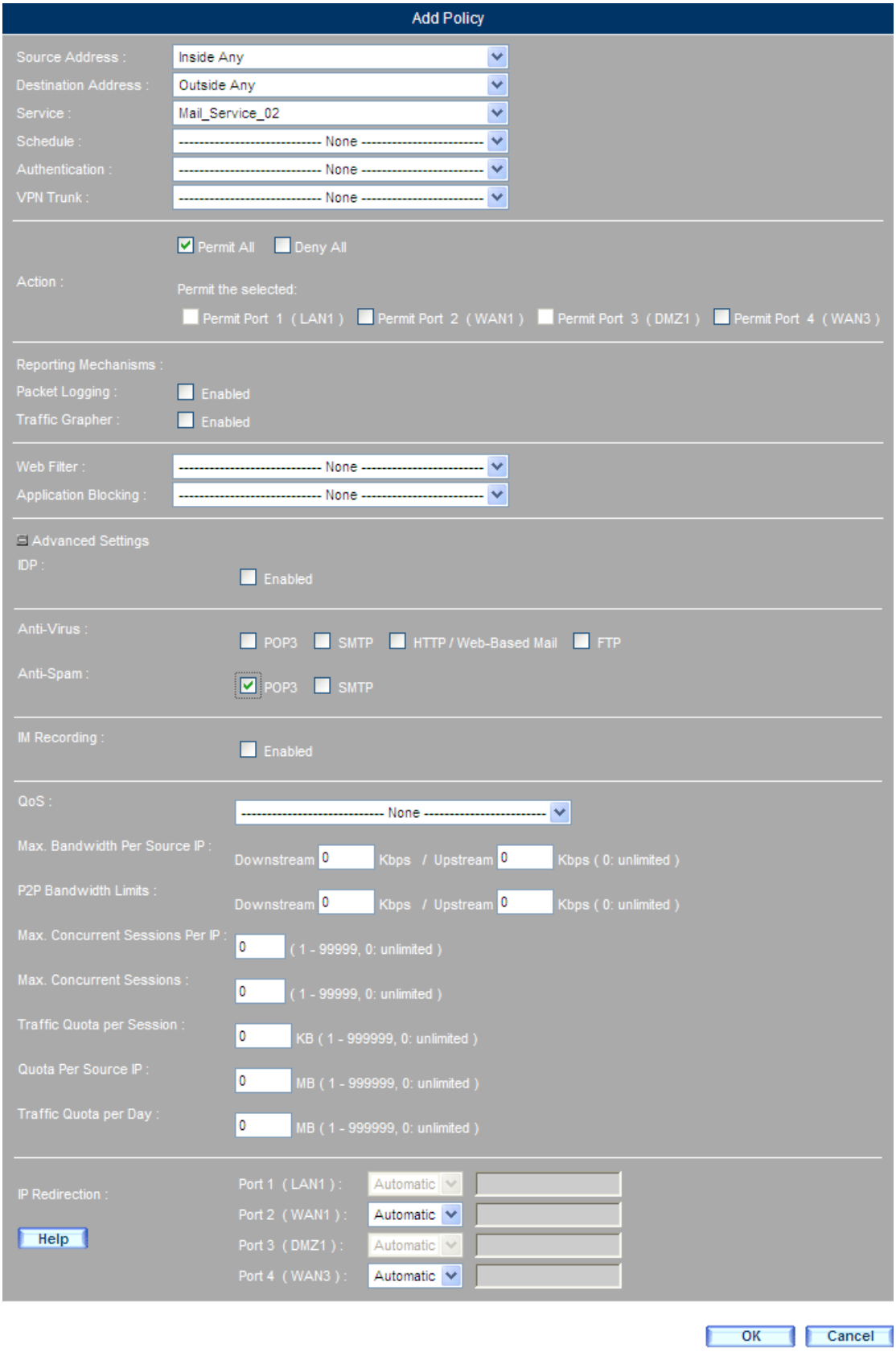


Figure 13-6 Configuring an Outgoing Policy with Group Service and POP3 Anti-Spam

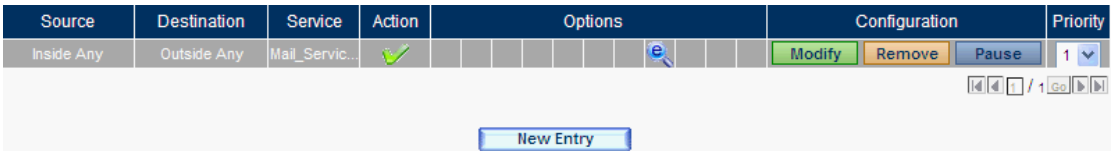


Figure 13-7 Policy Created

Step 6. Under **Policy** > **WAN to DMZ**, set as below:（**Figure 13-8**）

- Select the defined rule from the **Destination Address** drop-down list.
- Select the defined service group (Mail_Service_01) from the **Service** drop-down list.
- Tick POP3 for **Anti-Spam**.
- Click **OK**.（**Figure 13-9**）

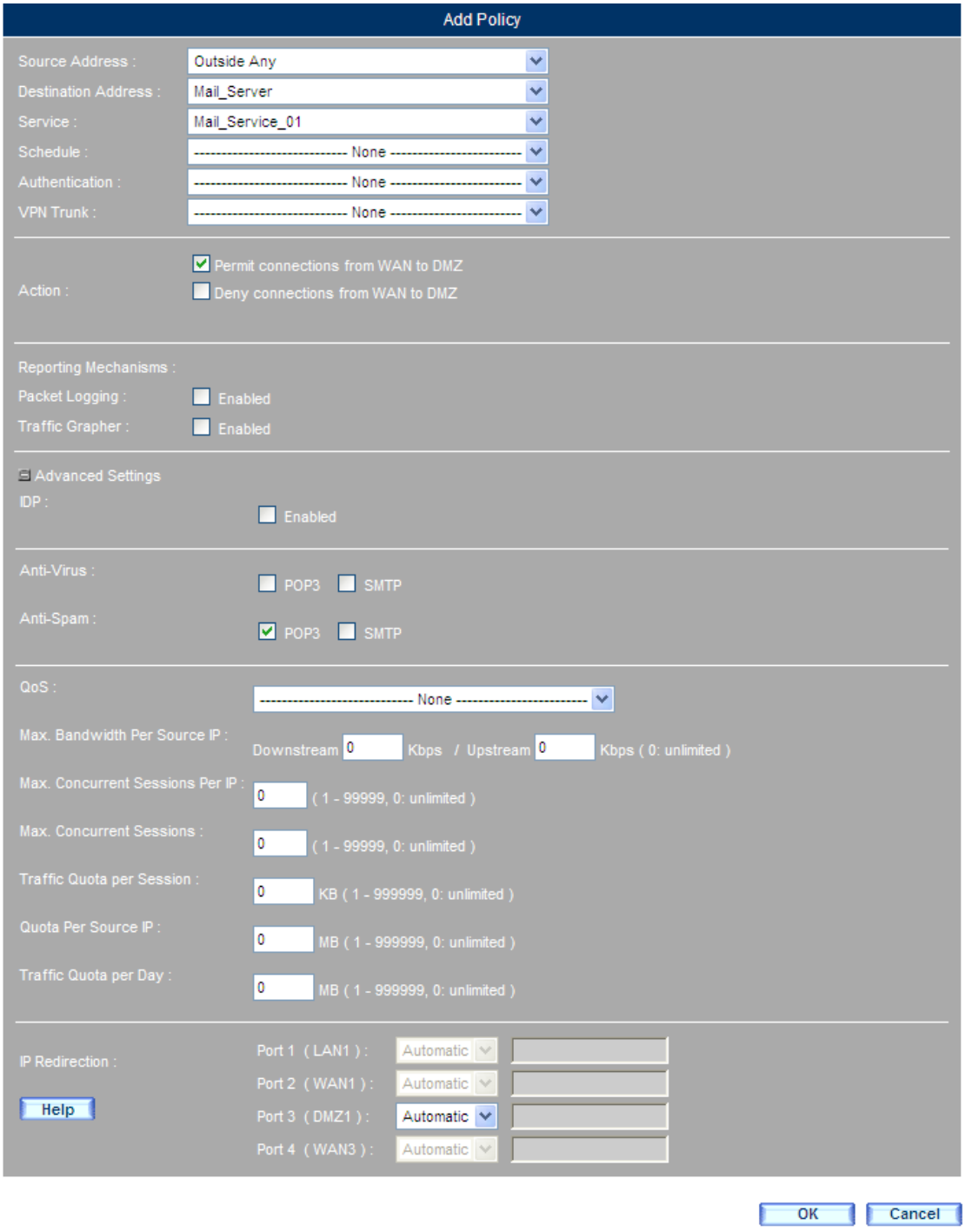


Figure 13-8 Creating a WAN To DMZ Policy with Service and POP3 Anti-Spam

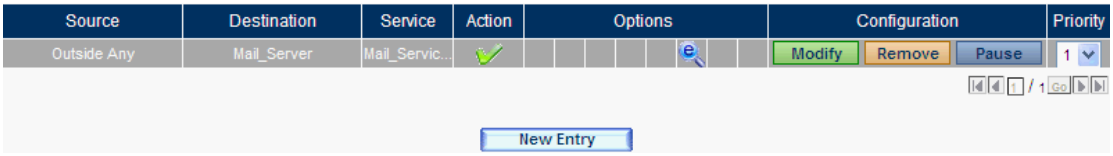


Figure 13-9 Policy Created

Step 7. Go to **Policy** > **DMZ to WAN** and then set as below: (**Figure 13-10**)

- Select the defined group from the **Source Address** drop-down list.
- Select the defined service group (Mail_Service_02) from the **Service** drop-down list.
- Tick POP3 for **Anti-Spam**.
- Click **OK**. (**Figure 13-11**)

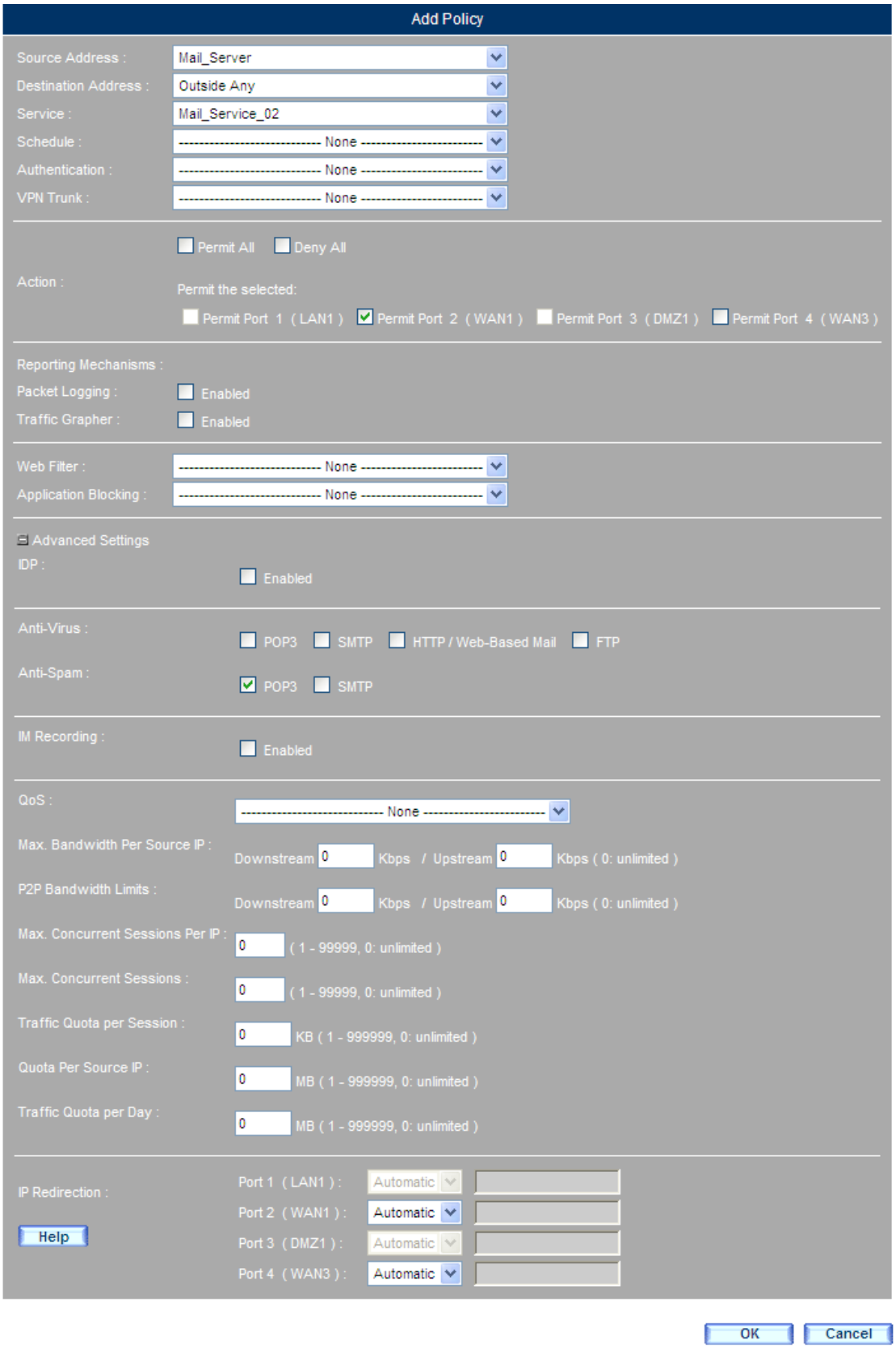


Figure 13-10 Creating a DMZ to WAN Policy with Group Service and POP3 Anti-Spam

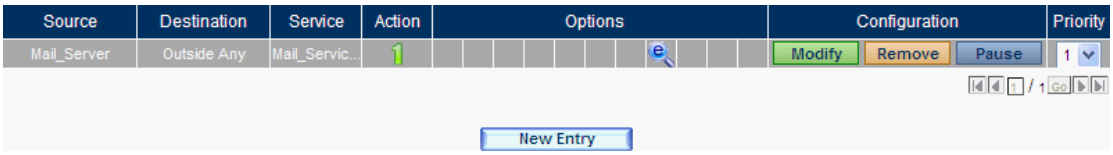


Figure 13-11 Policy Created

Step 8. Under **Mail Security** > **Anti-Spam** > **Settings**, set as below: (**Figure 13-12**)

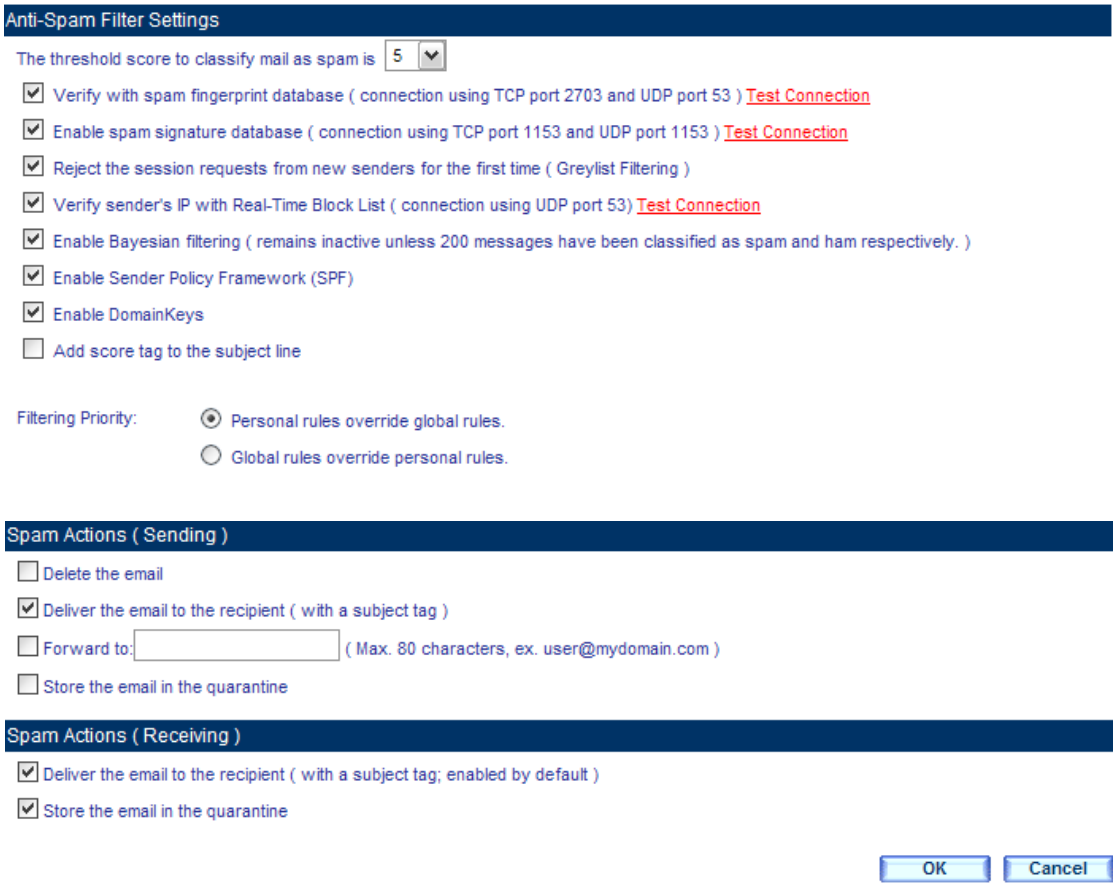


Figure 13-12 Anti-Spam Filter Settings and Action Settings

Note：

1. By default, Anti-Spam is enabled. Therefore, the IT administrator merely has to configure the settings under **Mail Security > Configuration > Mail Domains** to filter all the incoming and outgoing spam emails.（**Figure 13-13**）

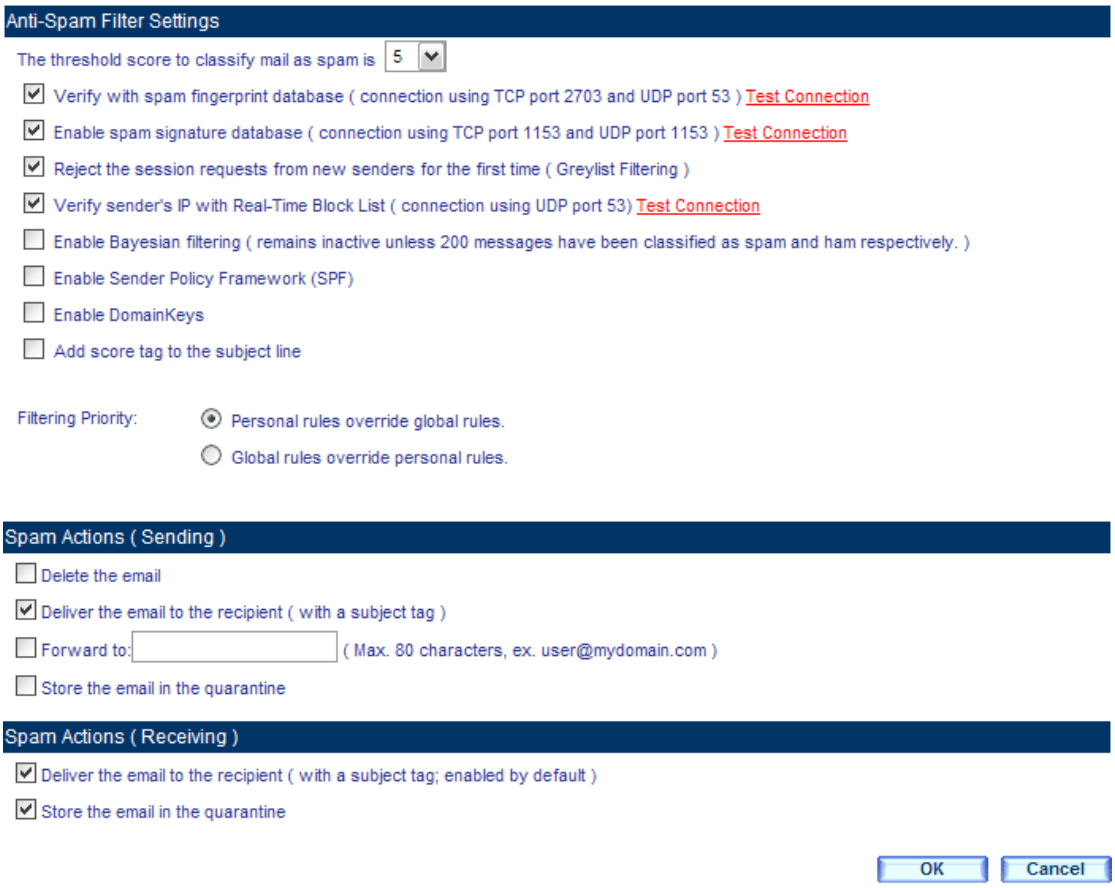


Figure 13-13 Anti-Spam Settings

2. When filtering incoming emails for spam:
   - The functionality **Deliver the email as normal** under the **Spam Actions (Receiving)** section is selected by default and can not be disabled. In addition, you may tick **Store the email in the quarantine** to store the email in the quarantine.
   - **Global Rule**, **Whitelist** or **Blacklist** can be used as criteria to filter spam.
   - The list of filtered spam cannot be obtained by means of Mail Notice.

Step 9. When receiving an email from an external mail account js1720@ms21.pchome.com.tw, CS-2001 will filter the email for spam.

Step 10. When receiving an email from an internal mail account joe@supportplanet.com.tw. CS-2001 will filter the email for spam.

13.1.2 Using CS-2001 in Accordance with Whitelist and Blacklist to Filter Spam (Mail Server Is Deployed in DMZ under Transparent Mode)

Prerequisite Setup

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing mode) and connect it to the LAN which is using 192.168.1.x/24.

Configure Port2 as WAN1 (61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet. IP range: 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet. IP range: 211.22.22.18 to 211.22.22.30.

Configure Port4 as DMZ1 (Transparent Routing mode) and connect it to the mail server. (IP address: 61.11.11.12)

Step 1. Set up a mail server in **DMZ**, name it as "supportplanet.com.tw", configure its IP address as 61.11.11.12 and then use an external DNS server to resolve domain names.

Step 2. Go to **Policy Object** > **Address** > **DMZ** and then set as below: （**Figure 13-14**）

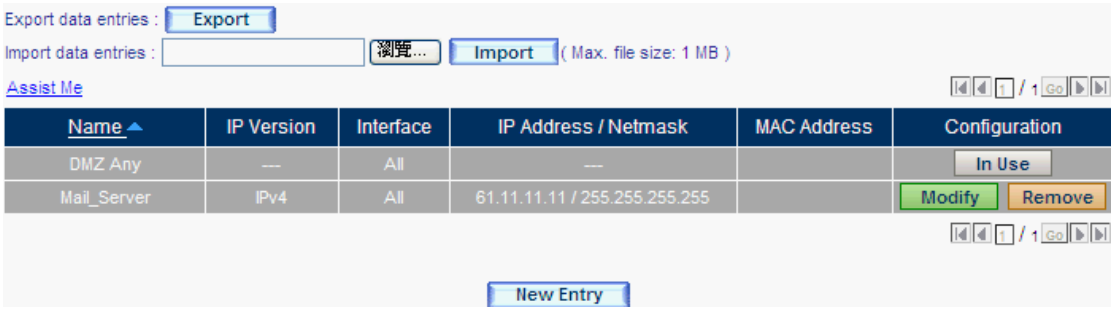


Figure 13-14 Address Settings for the Mail Server

Step 3. Go to **Policy Object** > **Service** > **Group** and then set as below: (**Figure 13-15**)

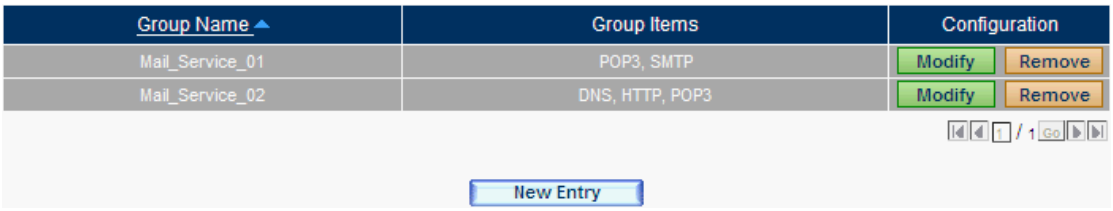


Figure 13-15 Creating Service Groups to Include POP3, SMTP and DNS Service

Step 4. Go to **Policy** > **WAN to DMZ** and then set as below: (**Figure 13-16**)

- Select the defined rule from the **Destination Address** drop-down list.
- Select the defined rule (Mail_Service_01) from the **Service** drop-down list.
- Select SMTP for **Anti-Spam**.
- Click **OK**. (**Figure 13-17**)

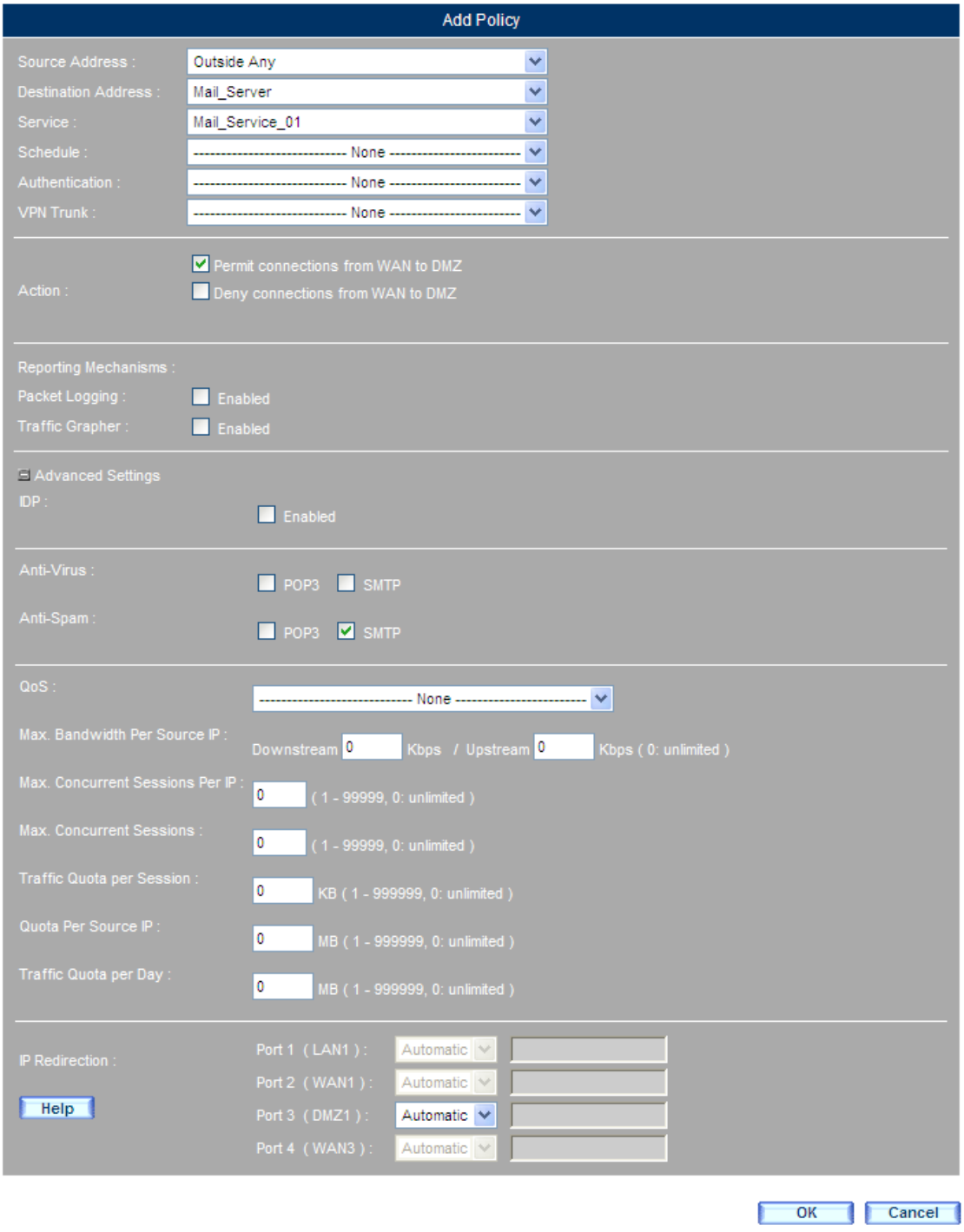


Figure 13-16 Creating a WAN to DMZ Policy

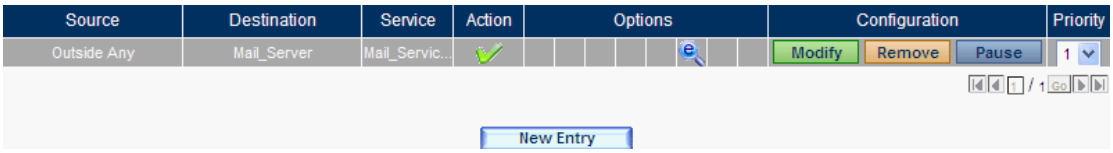


Figure 13-17 Policy Created

Step 5. Under **Policy** > **DMZ To WAN**, set as below: (**Figure 13-18**)

- Select the defined rule for **Source Address**.
- Select the defined service (Mail_Service_02) for **Service**.
- Select SMTP for **Anti-Spam**.
- Click **OK**. (**Figure 13-19**)

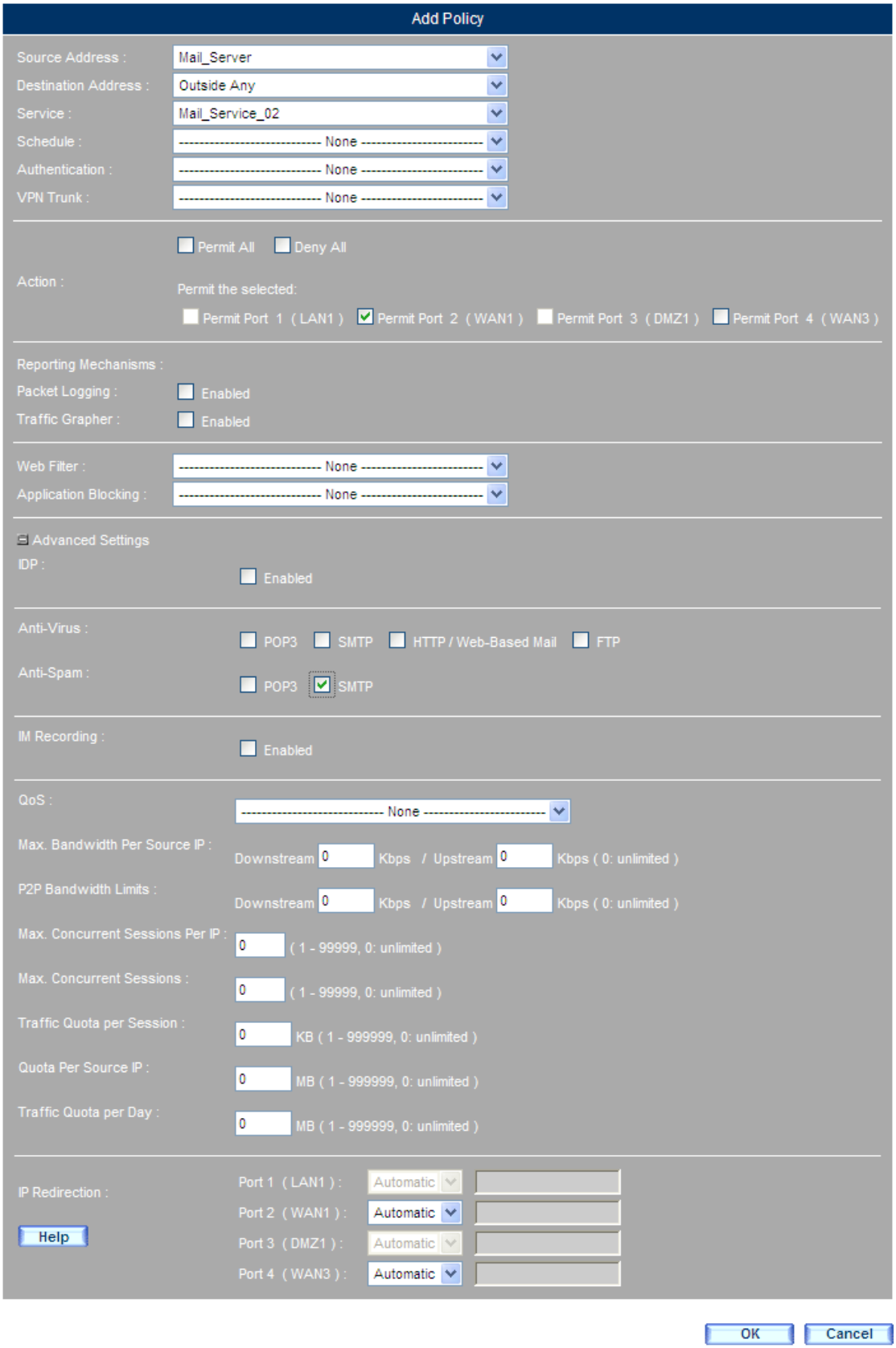


Figure 13-18 Creating a DMZ to WAN Policy

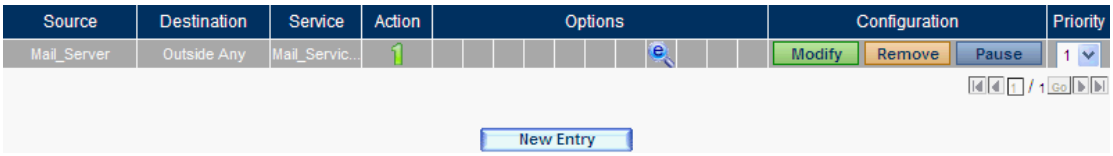


Figure 13-19 Policy Created

Step 6. Go to **Mail Security** > **Configuration** > **Mail Domains** and then set as below:（**Figure 13-20**）

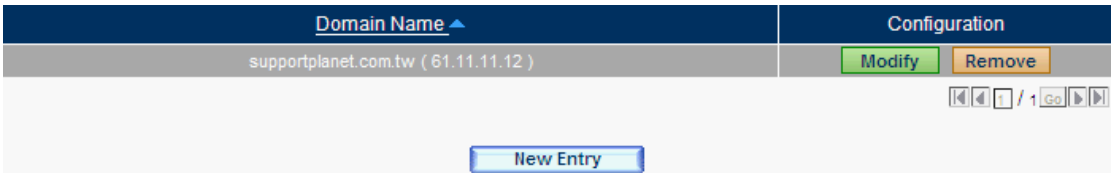


Figure 13-20 Mail Domain Settings

Step 7. Go to **Mail Security** > **Anti-Spam** > **Settings** and then set as below: （**Figure 13-21**）

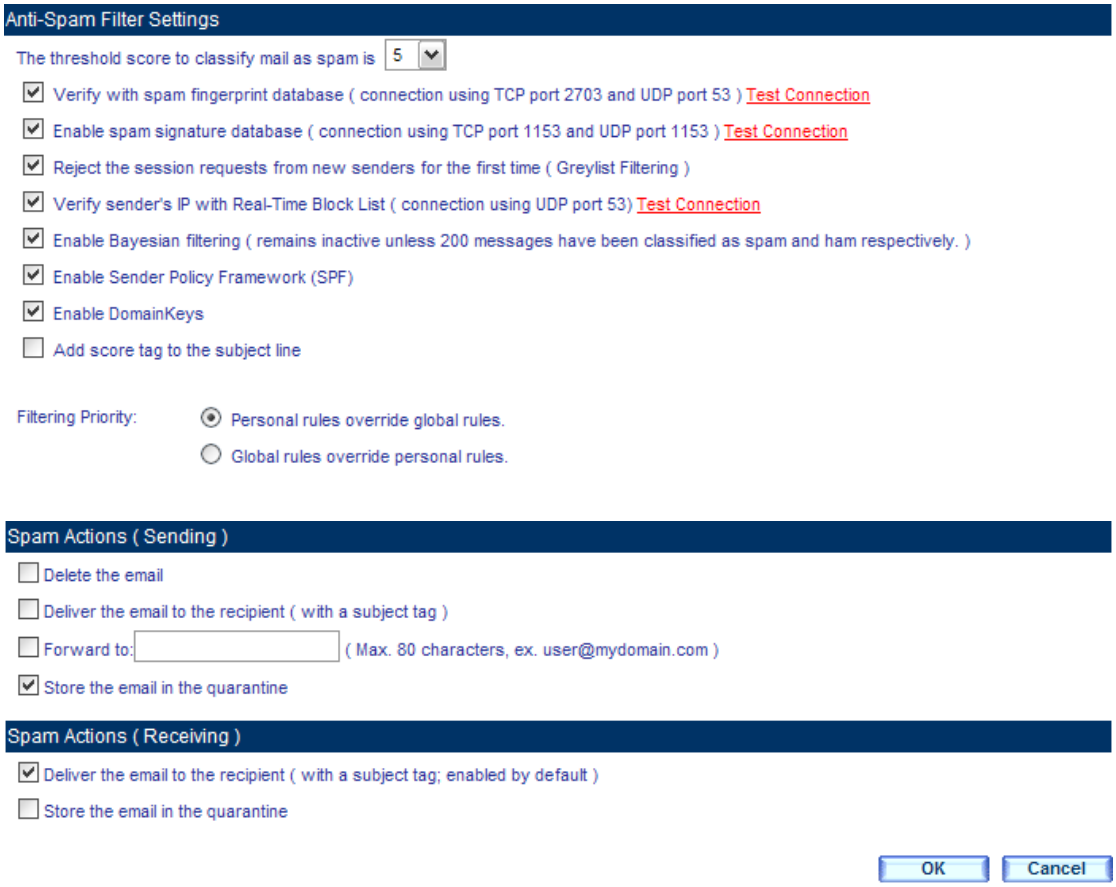


Figure 13-21 Anti-Spam Settings

Note:

1. When **Delete the email** is selected, **Deliver the email as normal** and **Store the email in the quarantine** will be disabled. Any spam mail will be be deleted directly. The logs are shown under **Mail Security** > **Mail Reports** > **Logs**.

Step 8. Go to **Mail Security** > **Anti-Spam** > **Whitelist** and then set as below:

- Click **New Entry**.
- Type share2k01@yahoo.com.tw in the **Mail Account** field.
- Select From for **Direction**.
- Click **OK**.（**Figure 13-22**）
- Click **New Entry** again.
- Type share2k01@yahoo.com.tw in the **Mail Account** field.
- Select To for **Direction**.
- Click **OK**.（**Figure 13-23**）
- Click **New Entry**.
- Type joe@supportplanet.com.tw in the **Mail Account** field.
- Select From for **Direction**.
- Click **OK**.（**Figure 13-24**）
- Click **New Entry**.
- Type joe@supportplanet.com.tw in the **Mail Account** field.
- Select To for **Direction**.
- Click **OK**.（**Figure 13-25, 13-26**）

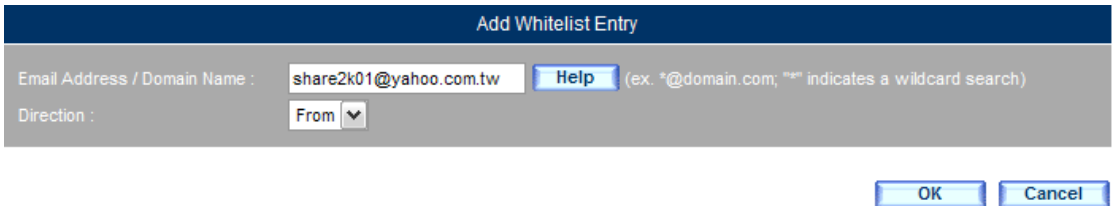


Figure 13-22 Creating the First Entry on Whitelist

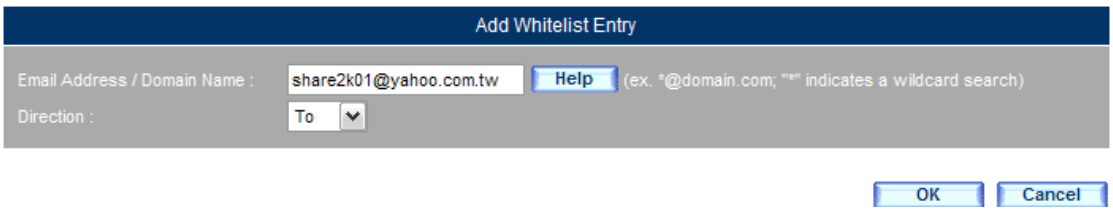


Figure 13-23 Creating the Second Entry on Whitelist

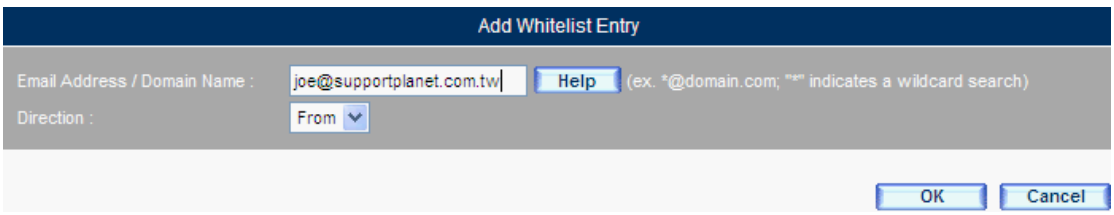


Figure 13-24 Creating the Third Entry on Whitelist

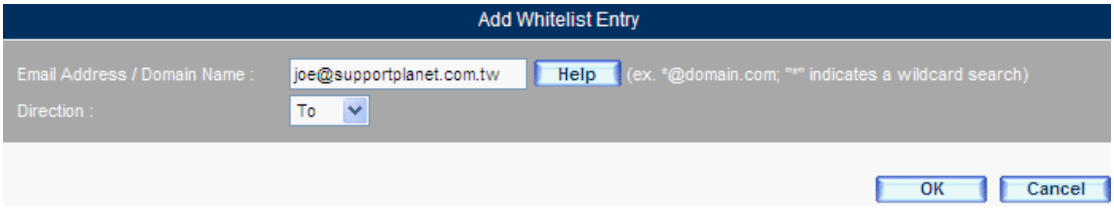


Figure 13-25 Creating the Fourth Entry on Whitelist

Figure 13-26 Whitelist Setting Completed

Note:

1. **Whitelist** can be exported as a file for archive and editing purpose, which can be used for restoring the list later on.

Step 9. Go to **Mail Security** > **Anti-Spam** > **Blacklist** and then set as below:

- Click **New Entry**.
- Type *yahoo* in the **Mail Account** field.
- Select From for **Direction**.
- Click **OK**.（**Figure 13-27**）
- Click **New Entry** again.
- Type *yahoo* in the **Mail Account** field.
- Select To for **Direction**.
- Click **OK**.（**Figure 13-28, 13-29**）

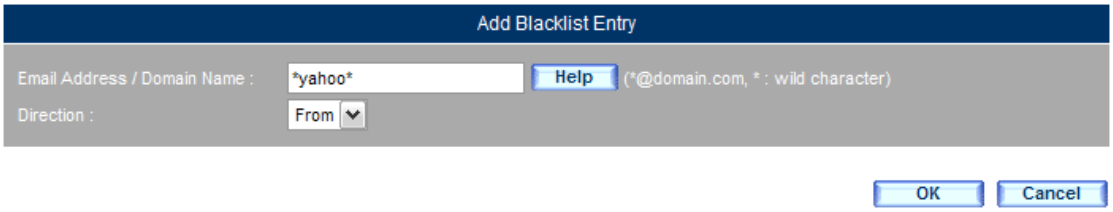


Figure 13-27 Creating the First Entry on Blacklist

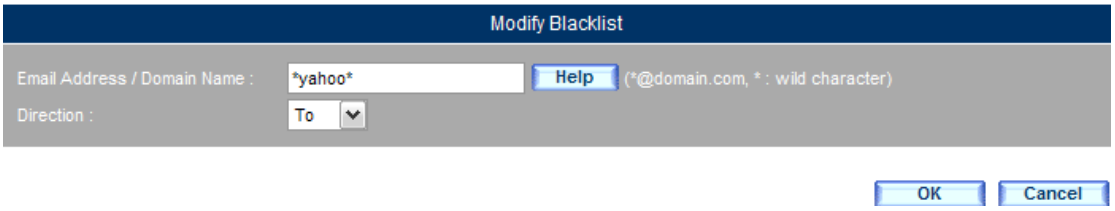


Figure 13-28 Creating the Second Entry on Blacklist

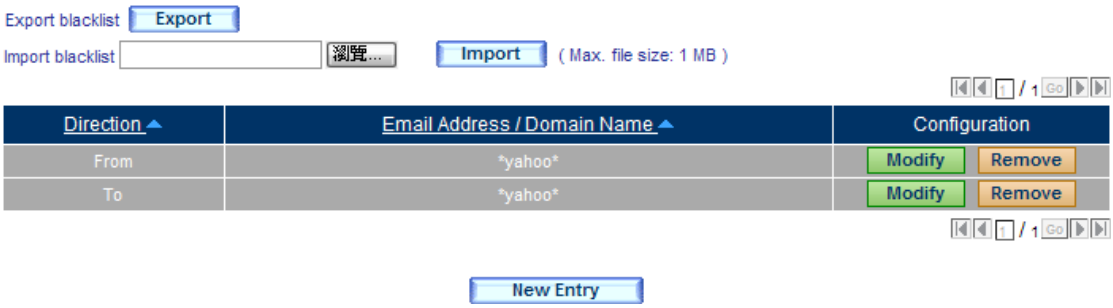


Figure 13-29 Blacklist Setting Completed

Note:

1. **Blacklist** can be exported as a file for archive and editing purpose, which can be used for restoring the list later on.
2. The **Mail Account** field of both **Whitelist** or **Blacklist** can be a complete email address or a word string containing wildcard characters (*). For example, "*yahoo*" means email address that contains "yahoo".

3. **Whitelist** overrides **Blacklist**, thus, email inspection will firstly act on **Whitelist** and then **Blacklist**.

Step 10. Provided that joe@supportplanet.com.tw and steve@supportplanet.com.tw both receive an email from a Yahoo account:

- If the sender's account is share2k01@yahoo.com.tw, then both Joe and Steve will receive it.
- But if the sender's account is share2k003@yahoo.com.tw, only Joe will receive it. Emails that sent to Steve will be classified as spam and quarantined.

Step 11. When an internal account at **supportplanet.com.tw** sends an email to both share2k01@yahoo.com.tw and share2k003@yahoo.com.tw:

- If the sender is joe@supportplanet.com.tw, then both of them will be receiving the email from Joe.
- But if the sender is someone other than Joe, steve@supportplanet.com.tw for instance, then only share2k01 will receive the email from Steve. Emails that sent to share2k003 will be classified as spam and quarantined.

13.1.3 Deploying CS-2001 in between Gateway and Mail

Server and Filtering Spam with Global Rule (Mail Server Is

Deployed in DMZ under Transparent Mode)

Prerequisite Setup

Gateway: 172.16.x.x/16
Configure Port1 as LAN1.
Configure Port2 as WAN1 (172.16.1.12) and connect it to the gateway.
Configure Port3 as WAN2.

Configure Port4 as DMZ1(Transparet Routing mode) and connect it to the mail server (LAN IP: 172.16.1.13, WAN IP: 61.11.11.11)

Step 1. Setup a mail server in **DMZ**, name it as “supportplanet.com.tw”, configure its IP address as 172.16.1.13, and then use an external DNS server to resolve domain names.

Step 2. Under **Policy Object** > **Address** > **DMZ**, set as below:（**Figure 13-30**）

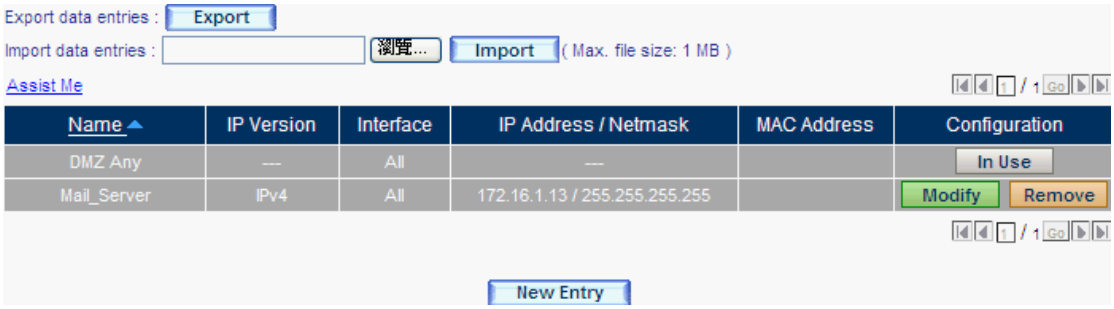


Figure 13-30 Address Setting for Mail Server

Step 3. Under **Policy Object** > **Service** > **Group**, set as below:（**Figure 13-31**）

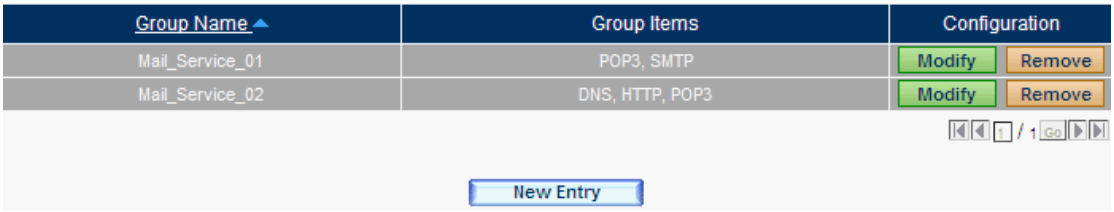


Figure 13-31 Creating Service Groups

Step 4. Under **Policy** > **WAN To DMZ**, set as below: (**Figure 13-32**)

- Select the defined DMZ for **Destination Address**.
- Select the defined service (Mail_Service_01) for **Service**.
- Select SMTP for **Anti-Spam**.
- Click **OK**. (**Figure 13-33**)

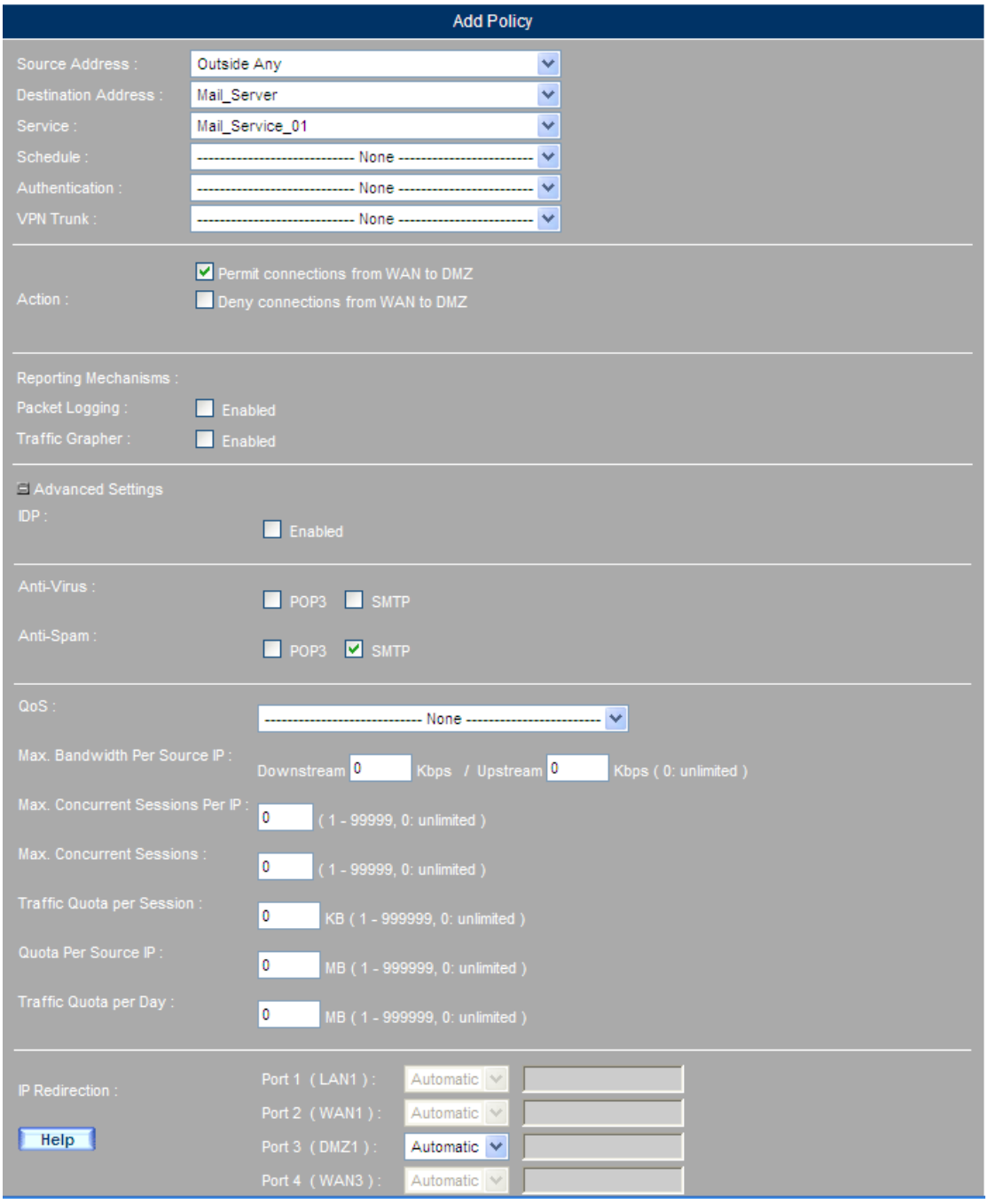


Figure 13-32 Creating a WAN to DMZ Policy with Service and SMTP Anti-Spam

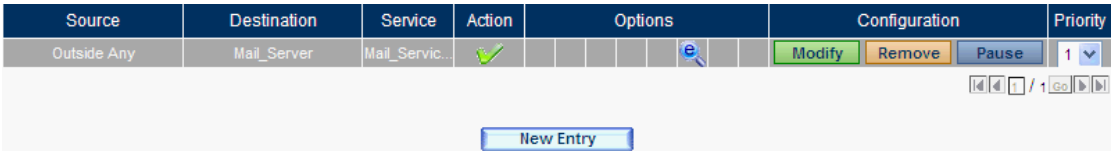


Figure 13-33 Policy Completed

Step 5. Under **Policy** > **DMZ To WAN**, set as below: (**Figure 13-34**)

- Select the defined DMZ for **Source Address**.
- Select the defined service (Mail_Service_02) for **Service**.
- Select SMTP for **Anti-Spam**.
- Click **OK**. (**Figure 13-35**)

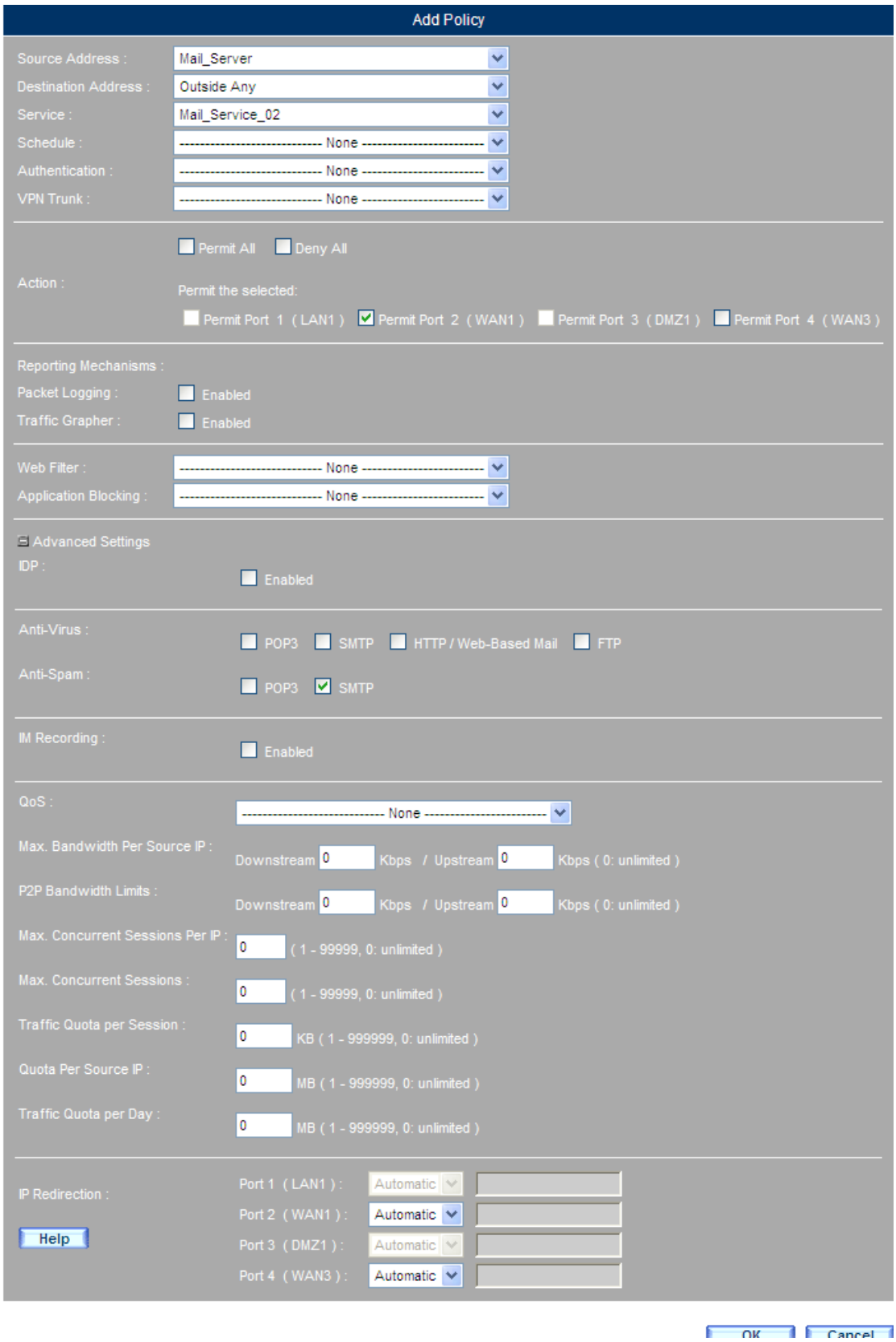


Figure 13-34 Creating a DMZ to WAN Policy with Service and SMTP Anti-Spam

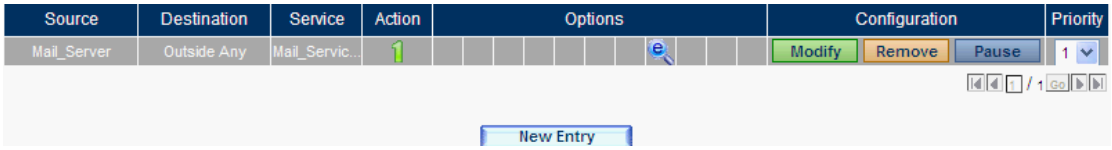


Figure 13-35 Policy Created

Step 6. Under **Mail Security** > **Configuration** > **Mail Domains**, set as below: （**Figure 13-36**）

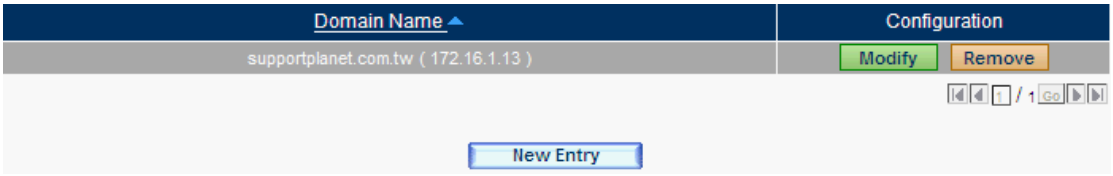


Figure 13-36 Mail Domain Settings

Step 7. Under **Mail Security** > **Configuration** > **Mail Relay**, set as below:（**Figure 13-37**）

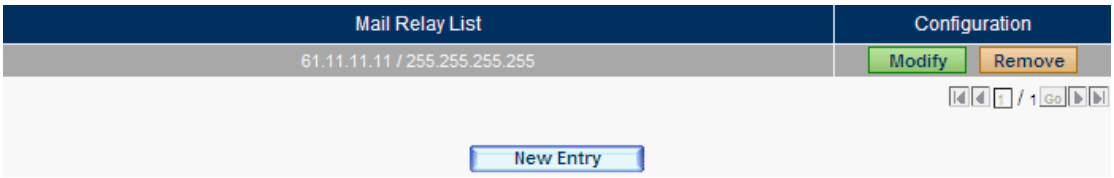


Figure 13-37 Mail Relay Settings

Note:

1. **Mail Relay** relays emails that sent to a specific domain to the destination mail server. It also allows external users to send emails via internal email accounts.

Step 8. Under **Mail Security** > **Anti-Spam** > **Settings**, set as below: (**Figure 13-38**)

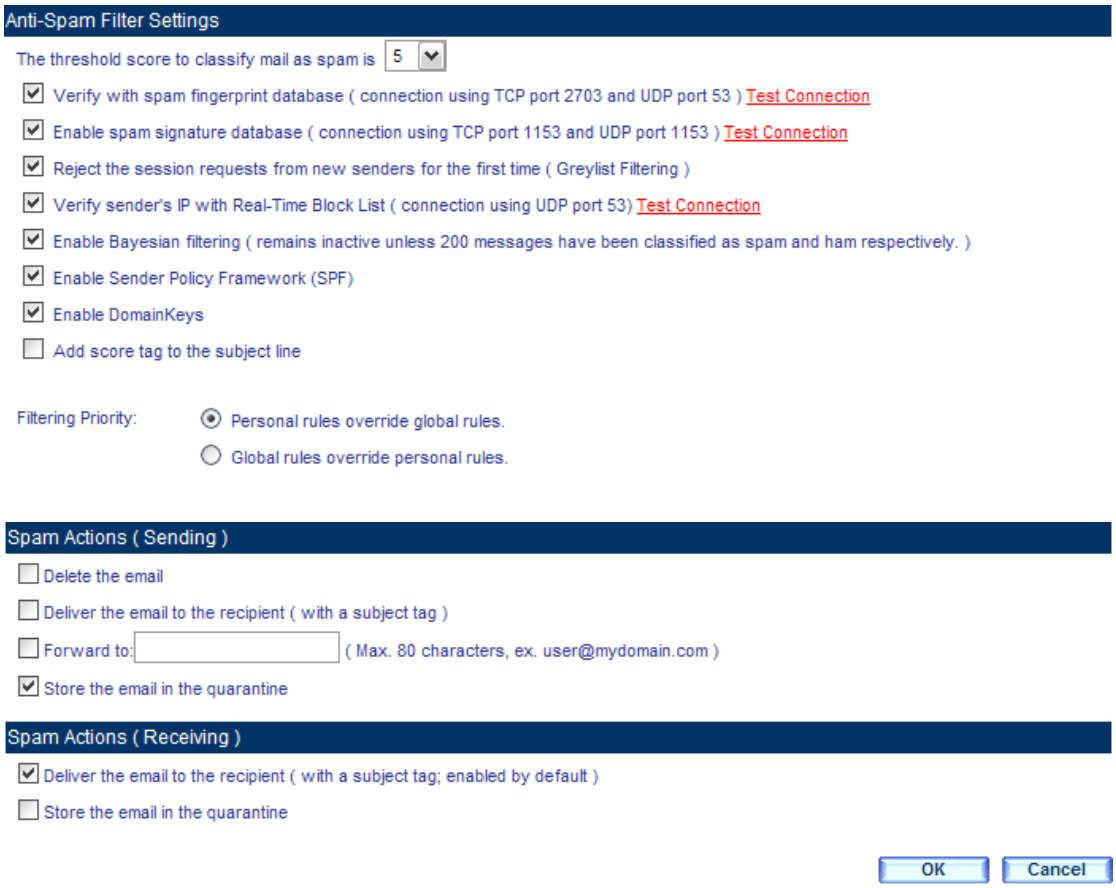


Figure 13-38 Anti-Spam Settings

Note:

1. An email that meets a **Global Rule** will be processed based on the corresponding **Action** setting of the **Global Rule**.

Step 9. Go to **Mail Security > Anti-Spam > Global Rule** and then set as below:

- Click **New Entry**.
- Type HamMail in the **Rule Name** field.
- Type Ham Mail in the **Comment** field.
- Select Ham (Non-Spam) for **Classification**.
- Select Or for **Combination**.
- Select From for **Item**, select Contains for **Condition** and then type share2k01 in the **Pattern** field.
- Click **Next**.
- In the second row, select To for **Item**, select Contains for **Condition** and then type share2k01 in the **Pattern** field.
- Click **Next**.
- In the Third row, select From for **Item**, select Contains for **Condition** and then type joe in the **Pattern** field.
- Click **Next**.
- In the fourth row, select To for **Item**, select Contains for **Condition** and then type joe in the **Pattern** field.（**Figure 13-39**）
- Click **OK**.（**Figure 13-40**）

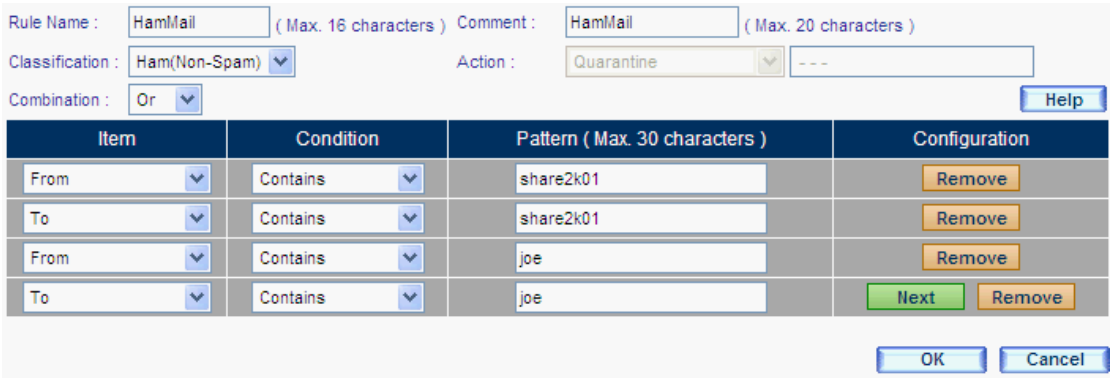


Figure 13-39 Configuring the First Global Rule

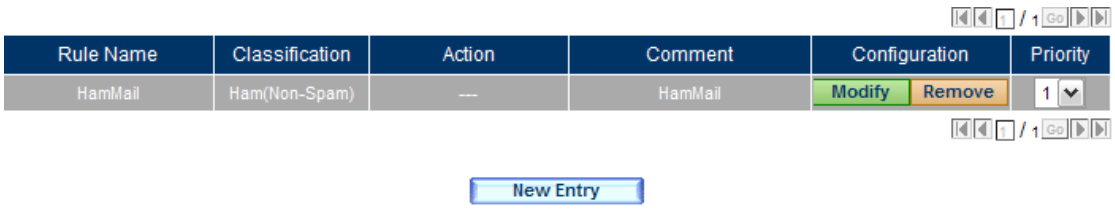


Figure 13-40 The First Global Rule Created

Note:

1. The **Action** setting of a **Global Rule** will be unavailable if **Classification** selected as **Ham (Non-Spam)**. It is because normal emails do not need any additional process before sending to the recipient.

Step 10. Go to **Mail Security** > **Anti-Spam** > **Global Rule** and then set as below:

- Click **New Entry**.
- Type SpamMail in the **Rule Name** field.
- Type Spam Mail in the **Comment** field.
- Select Spam for **Classification**.
- Select Quarantine for **Action**.
- Select Or for **Combination**.
- Select From for **Item**, Contains for **Condition** and then type yahoo in the **Pattern** field.
- Click **Next**.
- In the second row, select To for **Item**, Contains for **Condition** and then type yahoo in the **Pattern** field. (**Figure 13-41**)
- Click **OK**. (**Figure 13-42**)

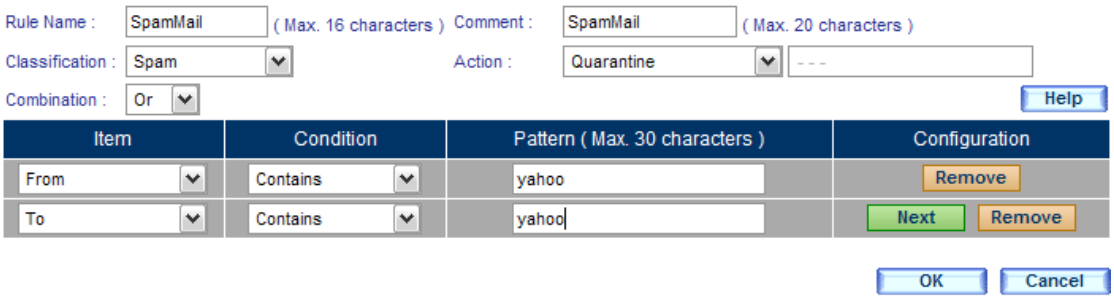


Figure 13-41 Configuring the Second Global Rule

Figure 13-42 Second Global Rule Completed

Note：

1. When **Classification** is set to Spam, one of the following associated actions must be selected: **Quarantine**, **Delete**, **Deliver** or **Same as spam settings**.
2. The priority of spam filtering criteria from high to low is Greylist > Whitelist in Personal Rule > Blacklist in Personal Rule > Global Rule > Whitelist > Blacklist > Default Filtering Rules, Spam Fingerprint Database, Spam Signature, Verify sender's IP with Real-Time Block List, Bayesian Filtering, Sender Policy Framework(SPF), DomainKey. Note: For filtering using Global Rule, it acts on the order of each **Priority** settings.

Email header can be used as a reference when configuring **Condition** and **Item** of **Global Rule**. Figure 13-43 shows the header of an email. To view header, click to select any email in your Outlook Express, then right-click it and move to **Properties** on the shortcut menu. After a window appeared, click the **Details** tab for header information.（**Figure 13-43**）

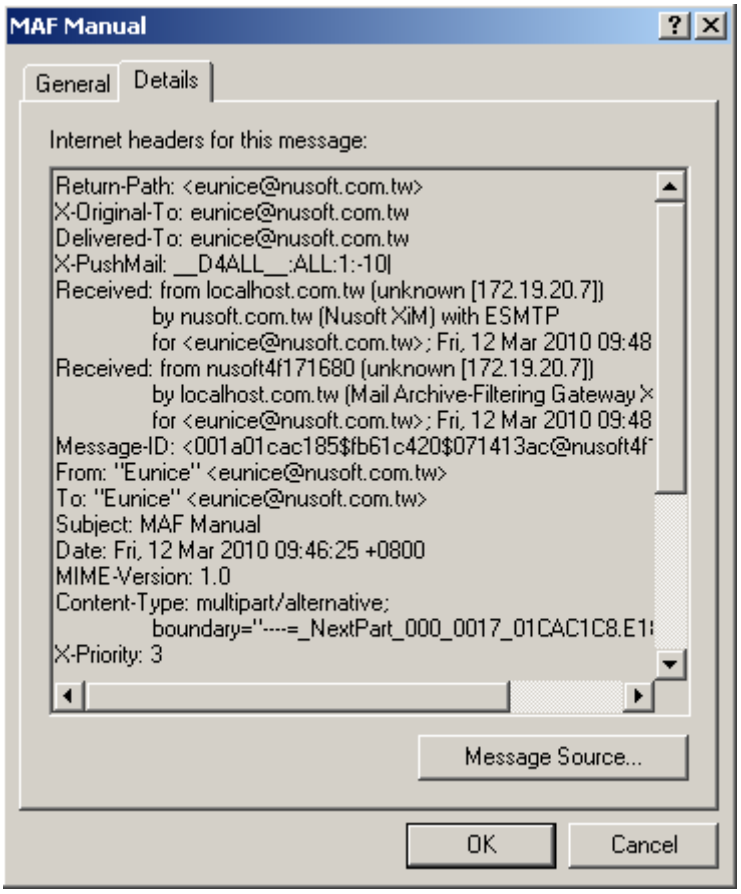


Figure 13-43 Detailed Information of an Email

Step 11. Provided that joe@supportplanet.com.tw and steve@supportplanet.com.tw both receive an email from a Yahoo account:

- If the sender's account is share2k01@yahoo.com.tw, then both Joe and Steve will receive it.
- But if the sender's account is share2k003@yahoo.com.tw, only Joe will receive it. Emails that sent to Steve will be classified as spam and quarantined.

Step 12. When an internal account at **supportplanet.com.tw** sends an email to both share2k01@yahoo.com.tw and share2k003@yahoo.com.tw:

- If the sender is joe@supportplanet.com.tw, then both of them will receive the email from Joe.
- But if the sender is someone other than Joe, steve@supportplanet.com.tw for instance, then only share2k01 will receive the email from Steve. Emails sent to share2k003 will be classified as spam and quarantined.

13.1.4 Improving Bayesian Filtering Accuracy by Training

Spam Filtering / Ham-Filtering (An Outlook Express Example)

To train spam filtering:

Step 1. In **Outlook Express**, create a new folder named “Spam Mail”:

- Right-click **Local Folders**, and then select **New Folder.**（**Figure 13-44**）
- In the **Create Folder** window, type “Spam Mail” in the **Folder name** field, and then click **OK.**（**Figure 13-45**）

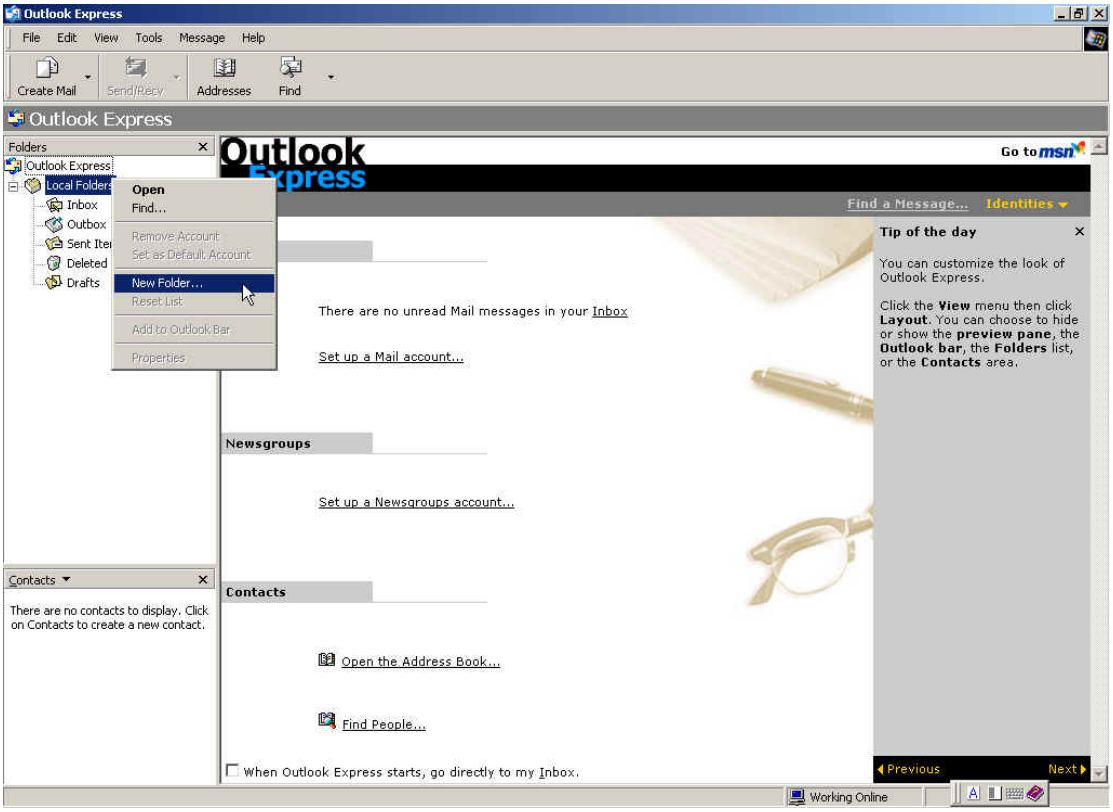


Figure 13-44 Creating a New Folder

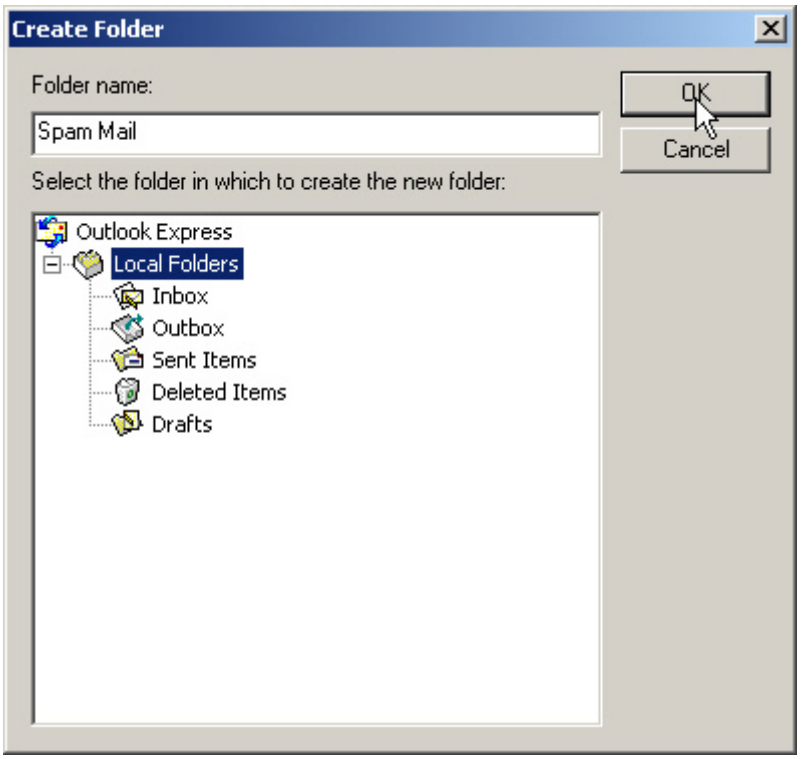


Figure 13-45 Naming the Folder as Spam Mail

Step 2. Click **Inbox** in **Outlook Express**, and then move the spam to the **Spam Mail** folder:

- In **Inbox**, select all the spam, right-click them, and then move to **Move to Folder** on shortcut menu.（**Figure 13-46**）
- Select **Spam Mail** folder in the **Move** window, and then click **OK.**（**Figure 13-47**）

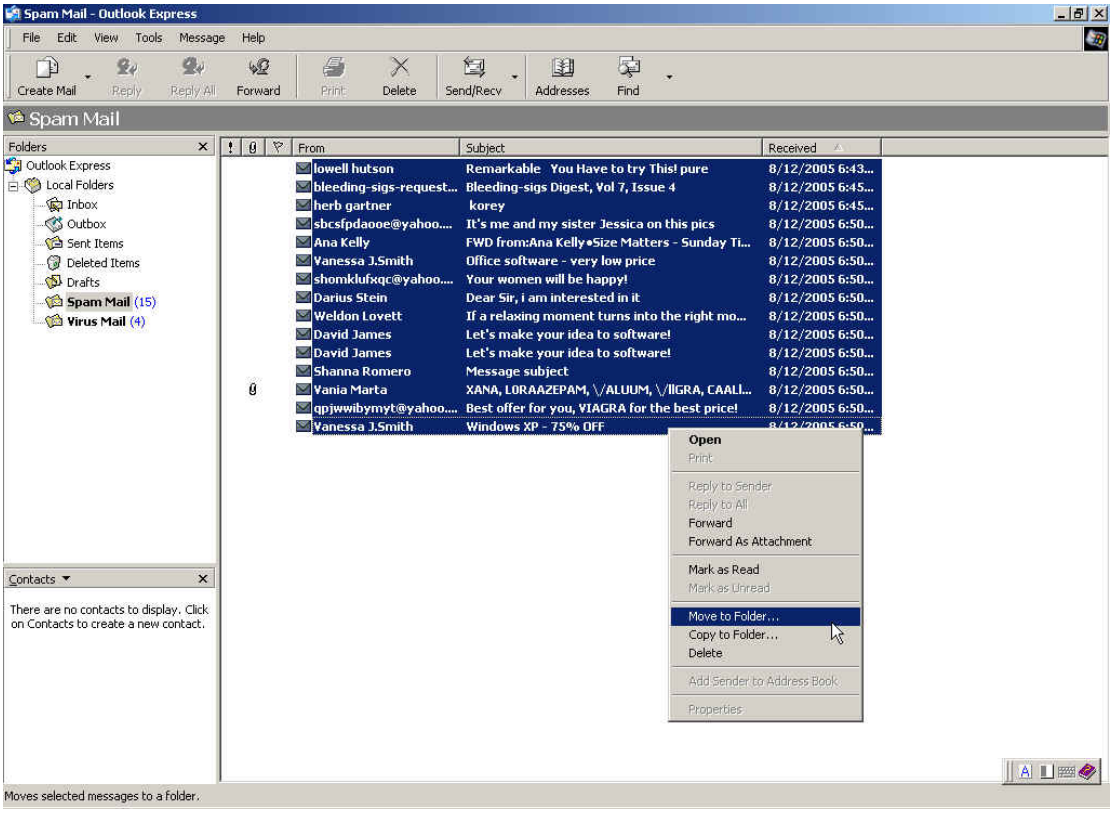


Figure 13-46 Moving Spam Emails

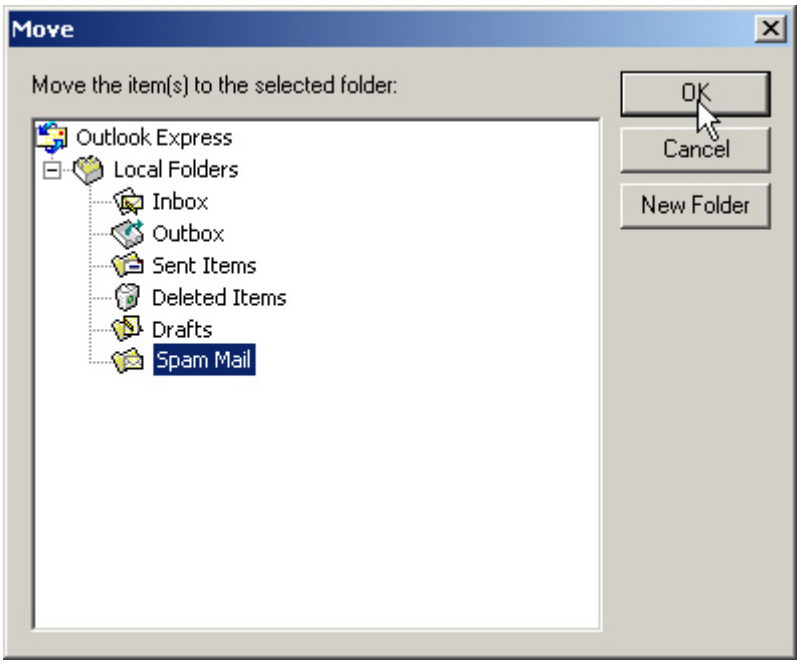


Figure 13-47 Selecting the “Spam Mail” Folder

Step 3. Compact the **Spam Mail** folder to make it easier importing spam messages onto CS-2001 for spam filtering training:

- Click the **Spam Mail** folder.（**Figure 13-48**）
- In the upper left corner, click **File**, point to **Folder**, and then click **Compact**.（**Figure 13-49**）

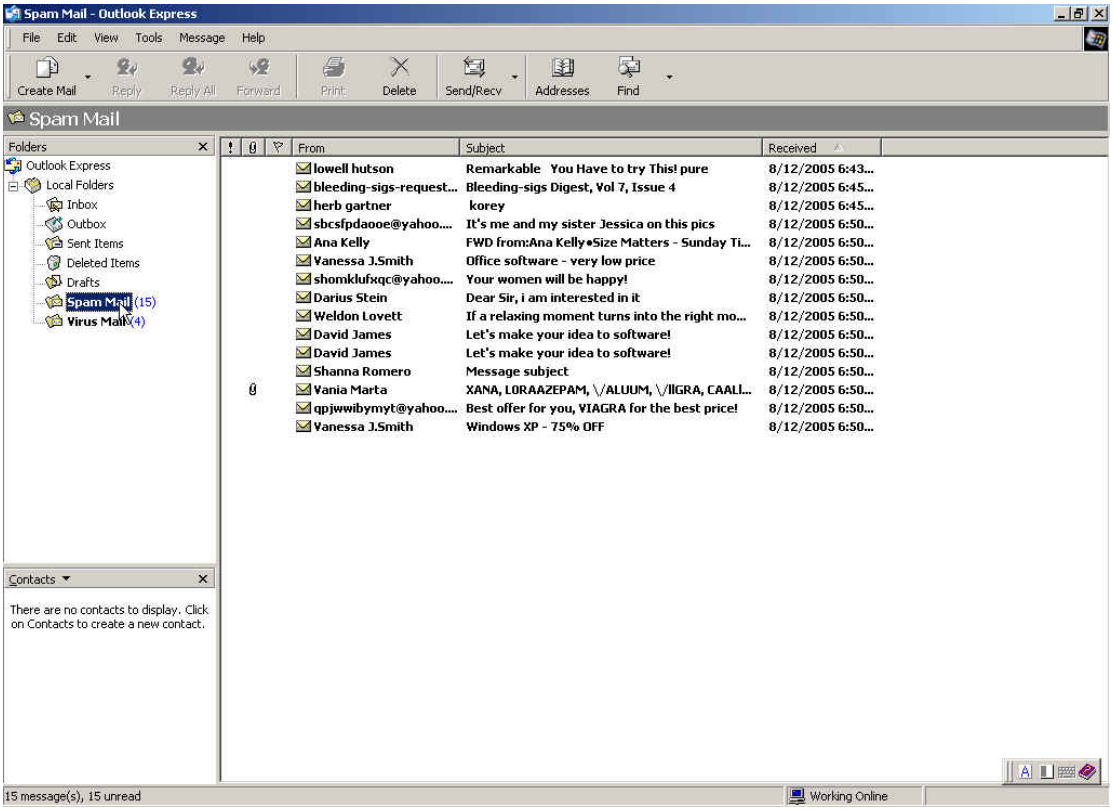


Figure 13-48 Selecting the Spam Mail Folder

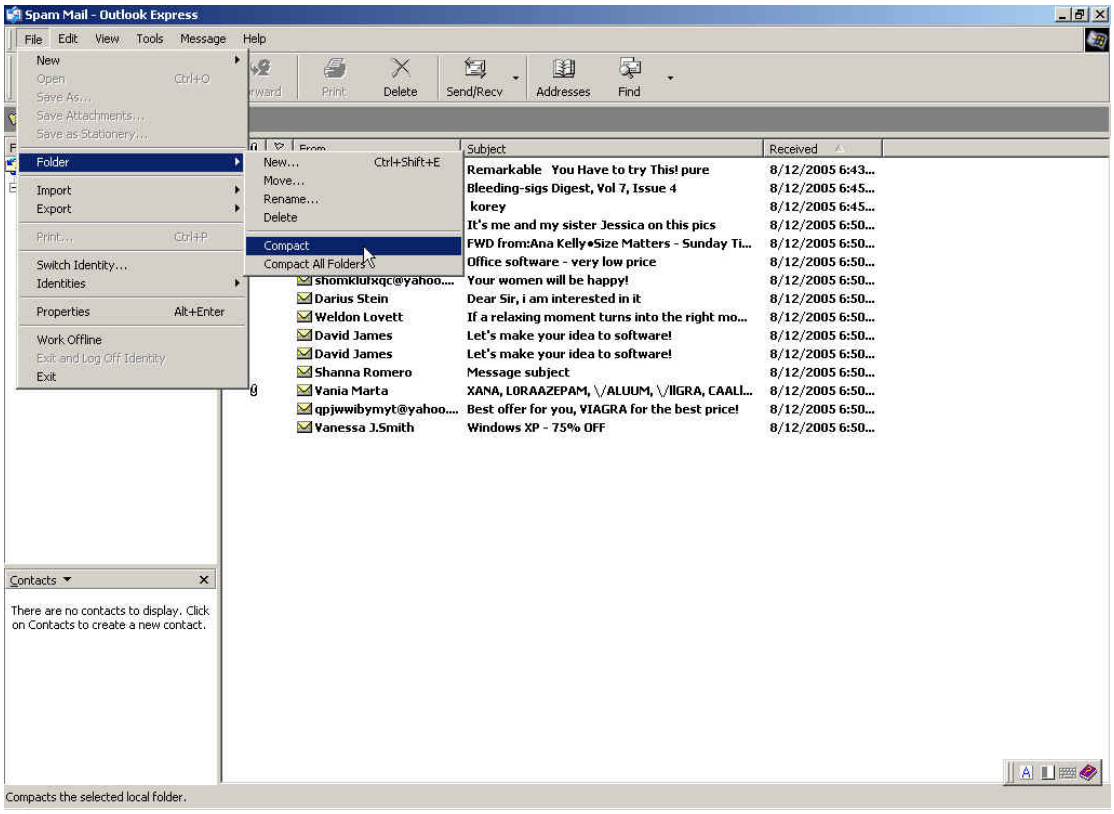


Figure 13-49 Compacting the Spam Mail Folder

Step 4. Copy the pathname of the **Spam Mail** folder to CS-2001 device for training use:

- Right-click **Spam Mail** folder, and then click **Properties** on shortcut menu.（**Figure 13-50**）
- In the **Spam Mail Properties** window, copy the pathname.（**Figure 13-51**）

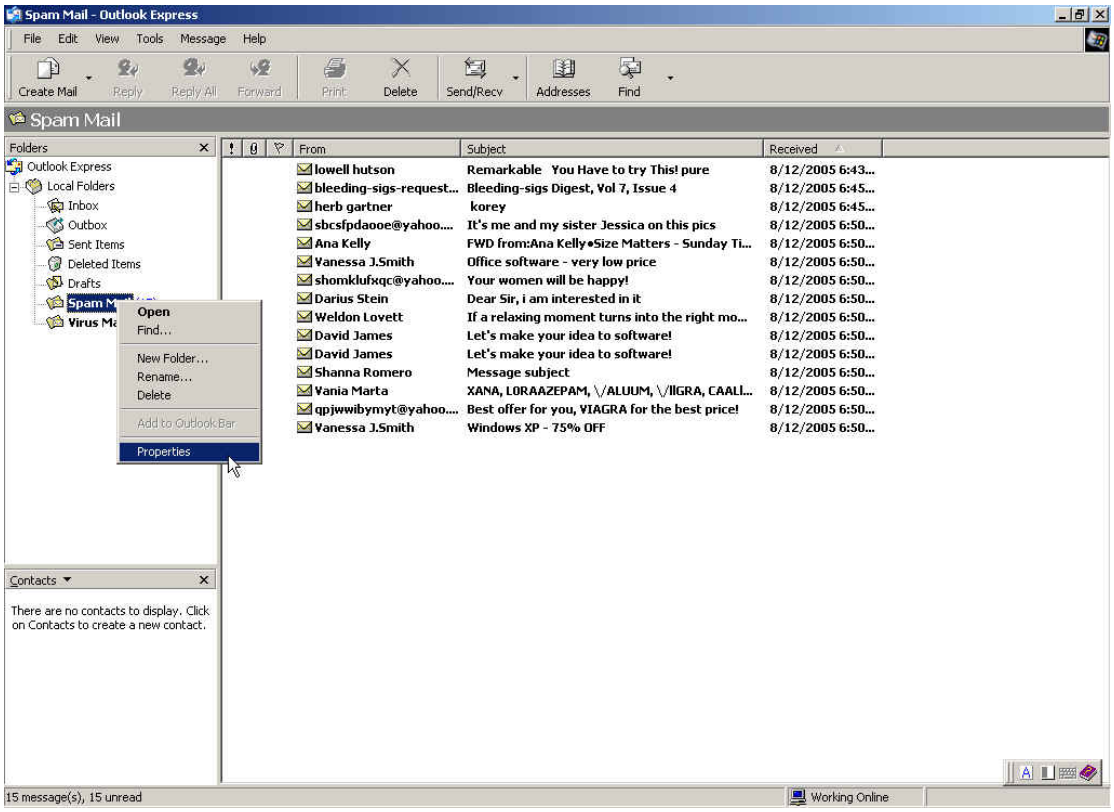


Figure 13-50 Selecting the Properties of the Spam Mail Folder

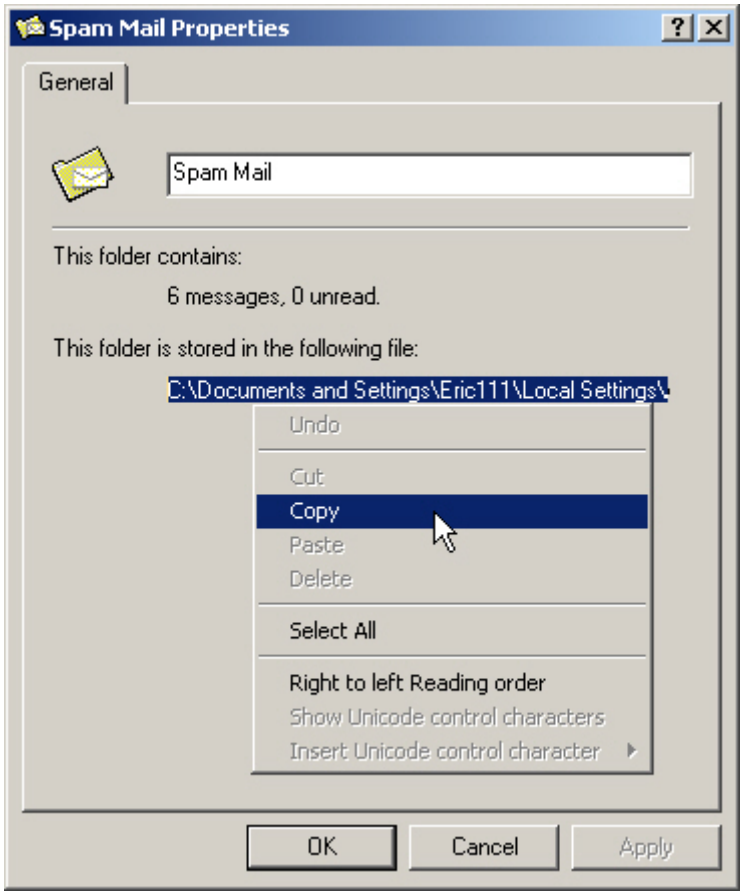


Figure 13-51 Copying the Pathname of the Spam Mail Folder

Step 5. Go to **Mail Security** > **Anti-Spam** > **Training** and then configure the settings under the **Spam Training Using Importing** section:

- Paste the pathname of the **Spam Mail folder** in the **Import Spam Mail from** field.
- Click the lower right **OK** to import the folder; the spam filtering will be trained on schedules.（**Figure 13-52**）

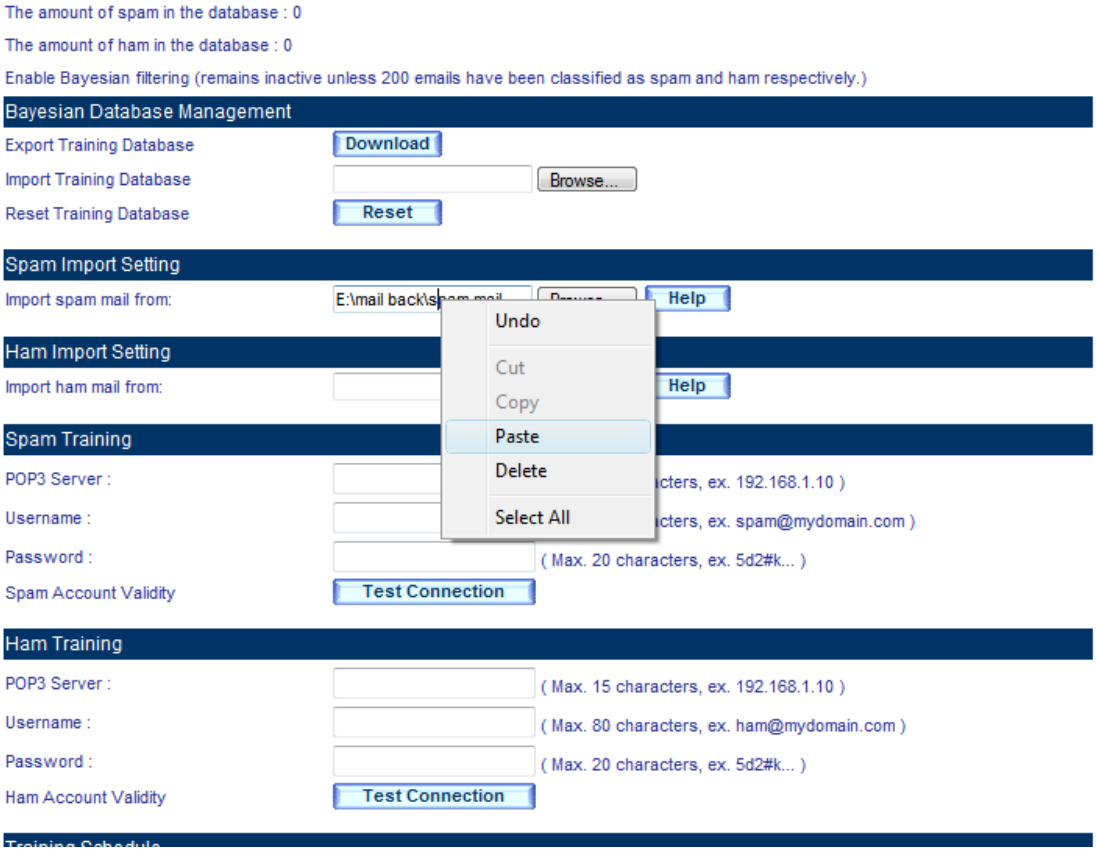


Figure 13-52 Importing Spam Emails for Spam Filtering Training

---

⚠ Important:

1. The file for spam filtering training can be any database file. It has no limitation in file extension, yet it has to be in ASCII format.
2. When importing a ".pst" file, Outlook must be closed before proceeding.

Step 6. Delete all spam emails in the **Spam Mail** folder; since they have been compressed and uploaded to CS-2001, they are of no use any longer:

- In the **Spam Mail** folder, select all emails, right-click them, and then click **Delete** on shortcut menu.（**Figure 13-53**）
- All spam emails have been deleted.（**Figure 13-54**）

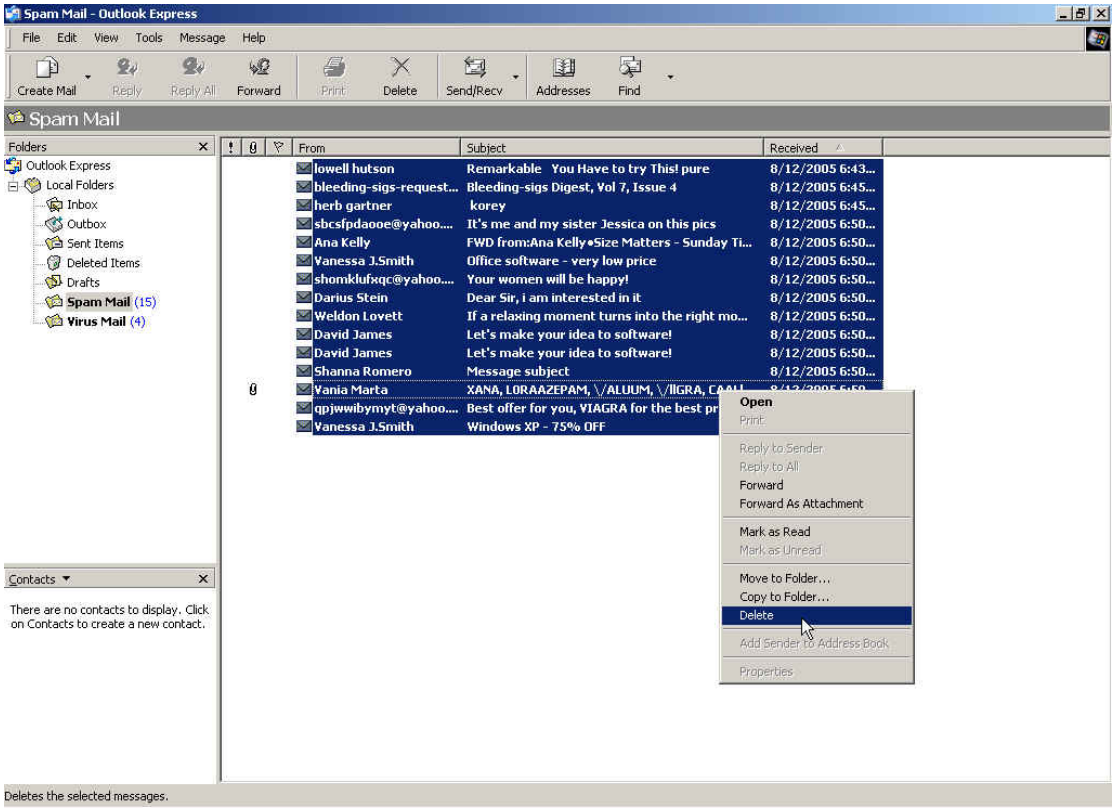


Figure 13-53 Selecting All Spam Emails to Delete

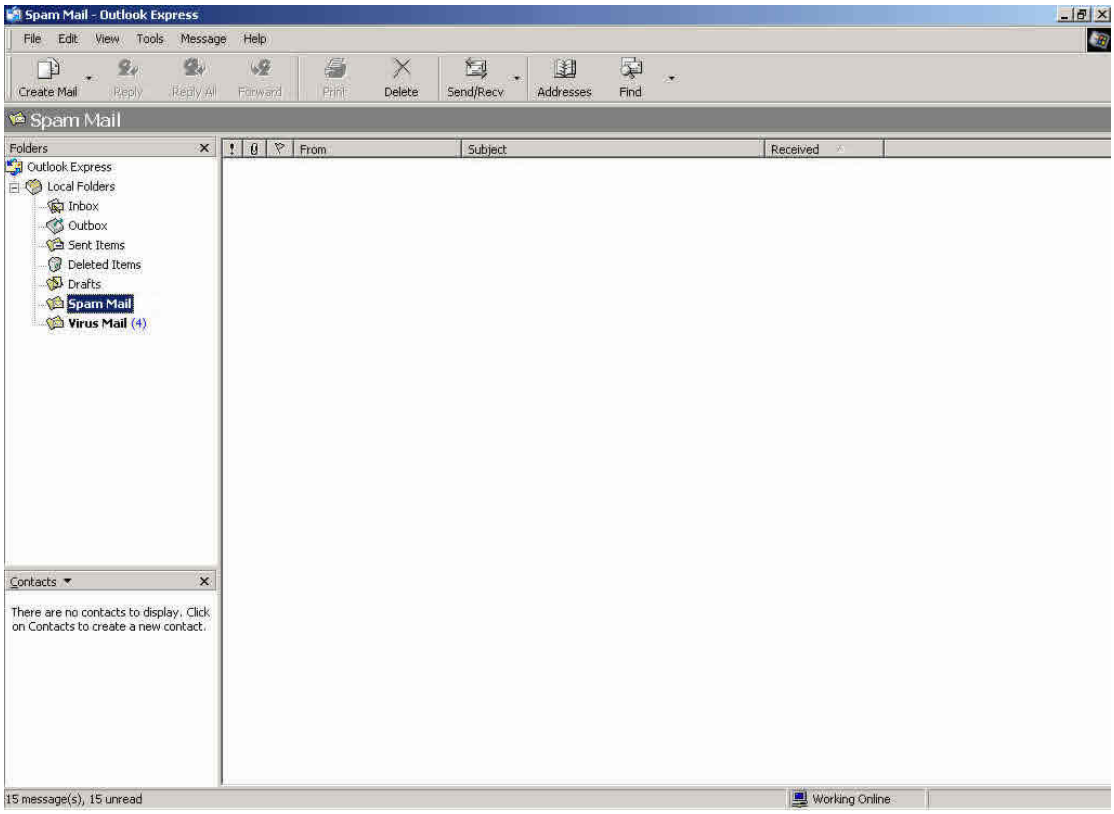


Figure 13-54 All Spam Emails Have Been Deleted

To train ham filtering:

Step 7. In **Outlook Express**, create a new folder called “Ham Mail”:

- Right-click **Local Folders**, and then select **New Folder**.（**Figure 13-55**）
- In the **Create Folder** window, type “Ham Mail” in the **Folder name** field, and then click **OK**.（**Figure 13-56**）

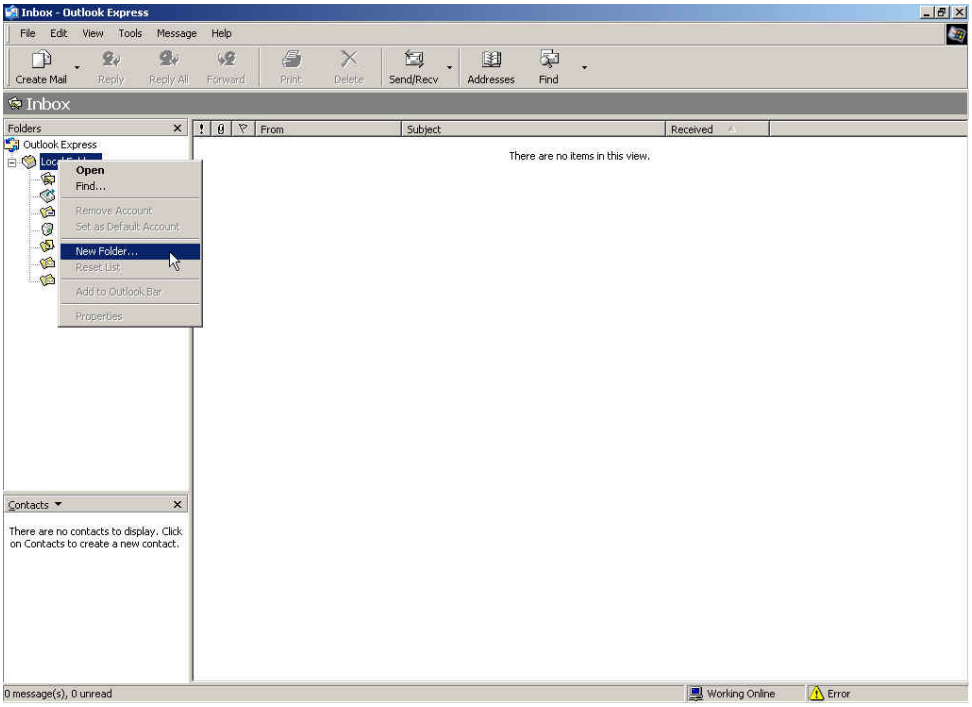


Figure 13-55 Creating a New Folder

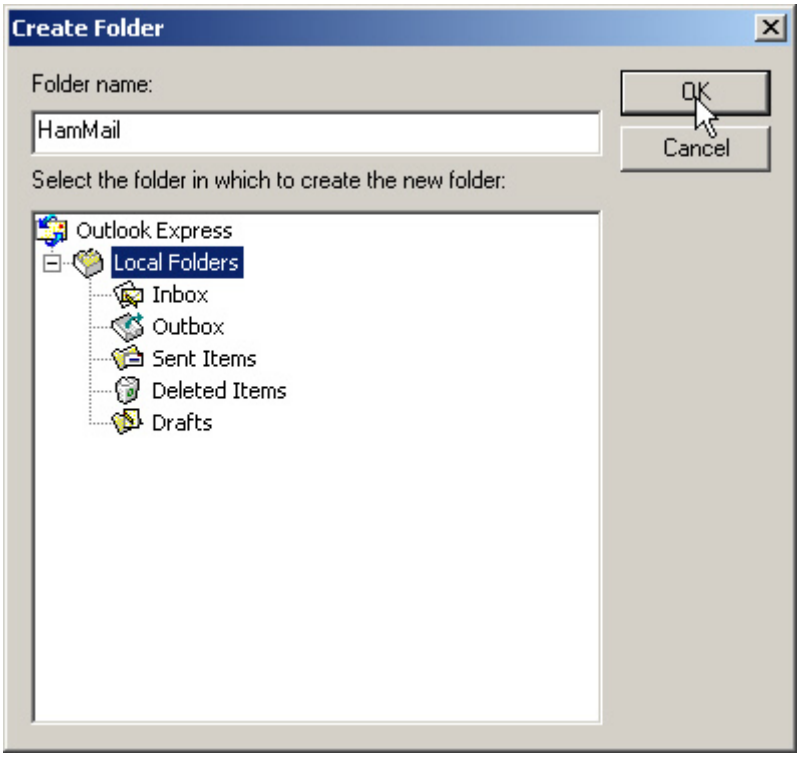


Figure 13-56 Naming the Folder as Ham Mail

Step 8. Click **Inbox** in **Outlook Express**, and then move normal emails to the **Ham Mail** folder:

- In **Inbox**, select all the hams, right-click them, and then move to **Move to Folder** on shortcut menu.（**Figure 13-57**）
- Select **Ham Mail** folder in the **Move** window, and then click **OK.**（**Figure 13-58**）

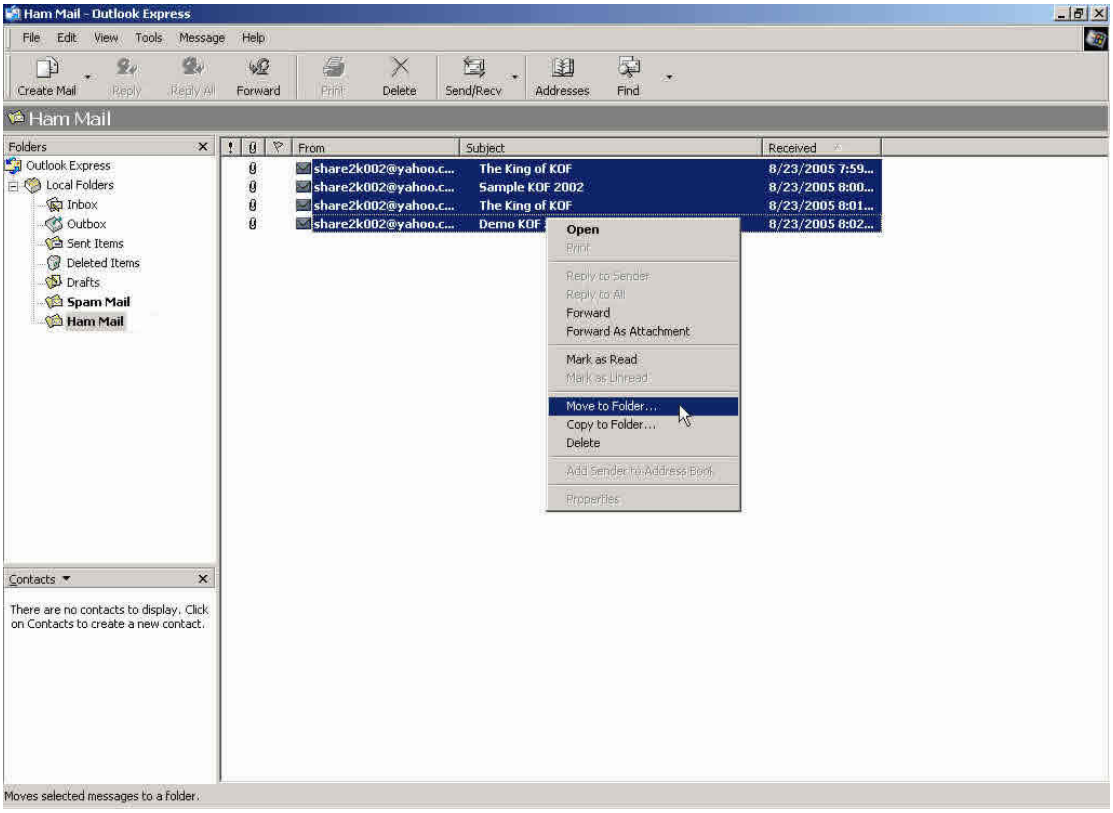


Figure 13-57 Moving Normal Emails

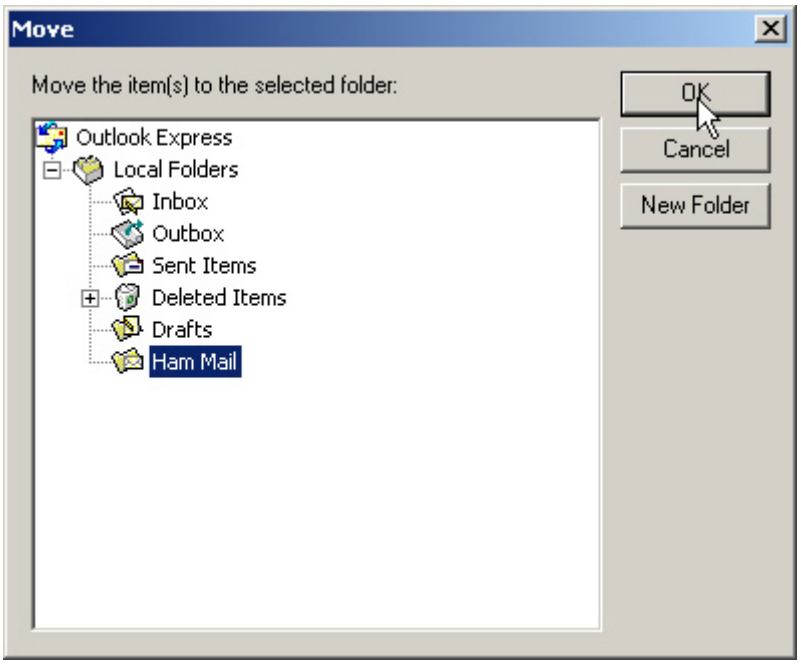


Figure 13-58 Selecting the Ham Mail Folder

Step 9. Compact the **Ham Mail** folder for the easy of importing normal email messages onto CS-2001 for ham filtering training:

- Click the **Ham Mail** folder.（**Figure 13-59**）
- In the upper left corner, click **File**, point to **Folder**, and then click **Compact**.（**Figure 13-60**）

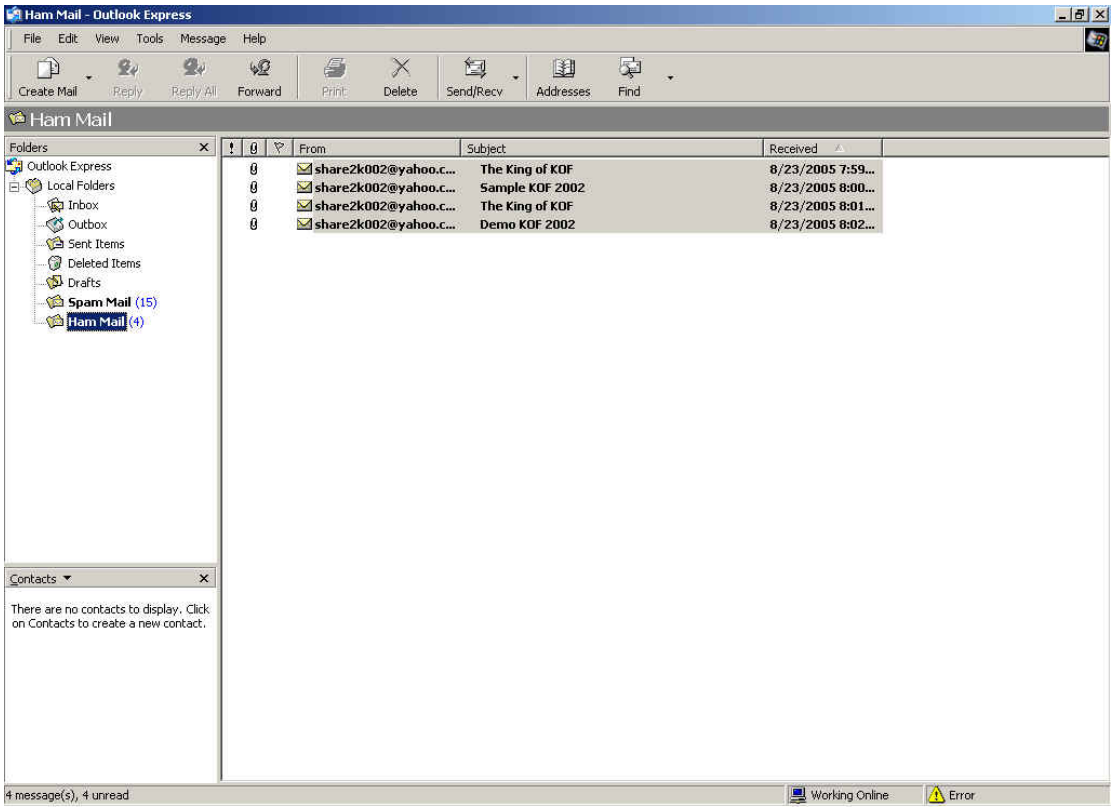


Figure 13-59 Selecting the Ham Mail Folder

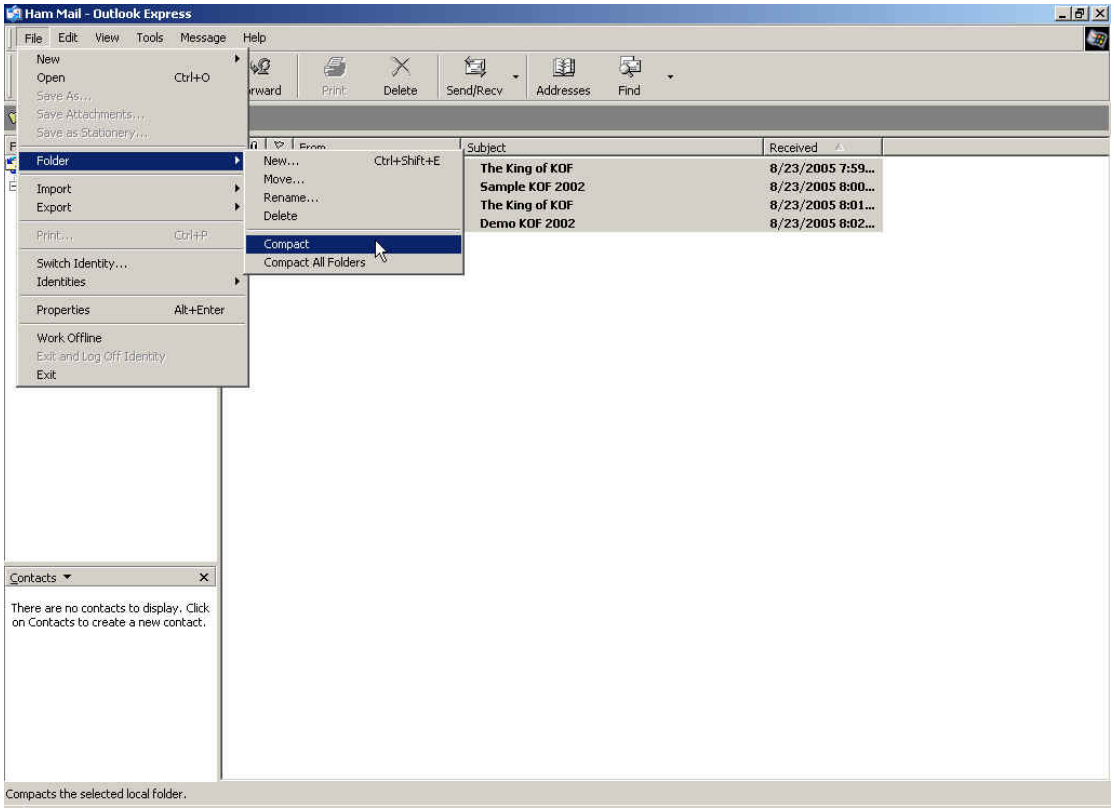


Figure 13-60 Compacting the Ham Mail Folder

Step 10. Copy the pathname of the **Ham Mail** folder to CS-2001 device for training use:

- Right-click the **Ham Mail** folder, and then click **Properties** on shortcut menu.（**Figure 13-61**）
- In the **Ham Mail Properties** window, copy the pathname.（**Figure 13-62**）

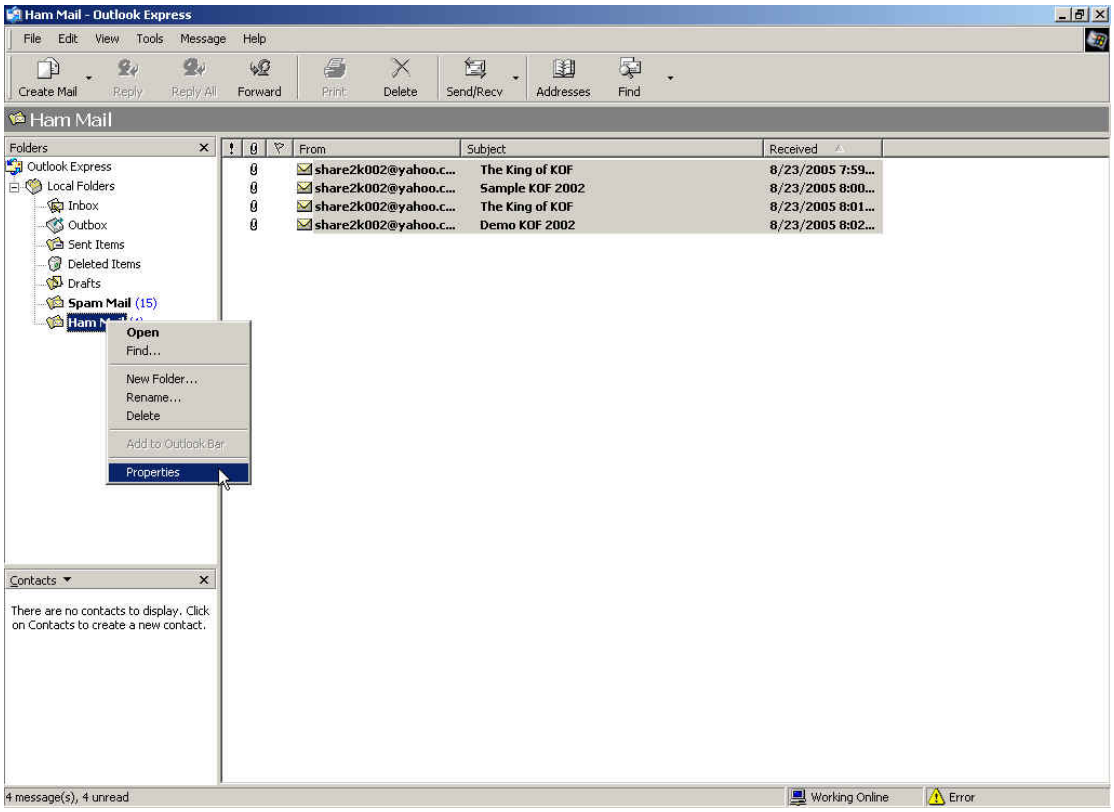


Figure 13-61 Selecting the Properties of the Ham Mail Folder

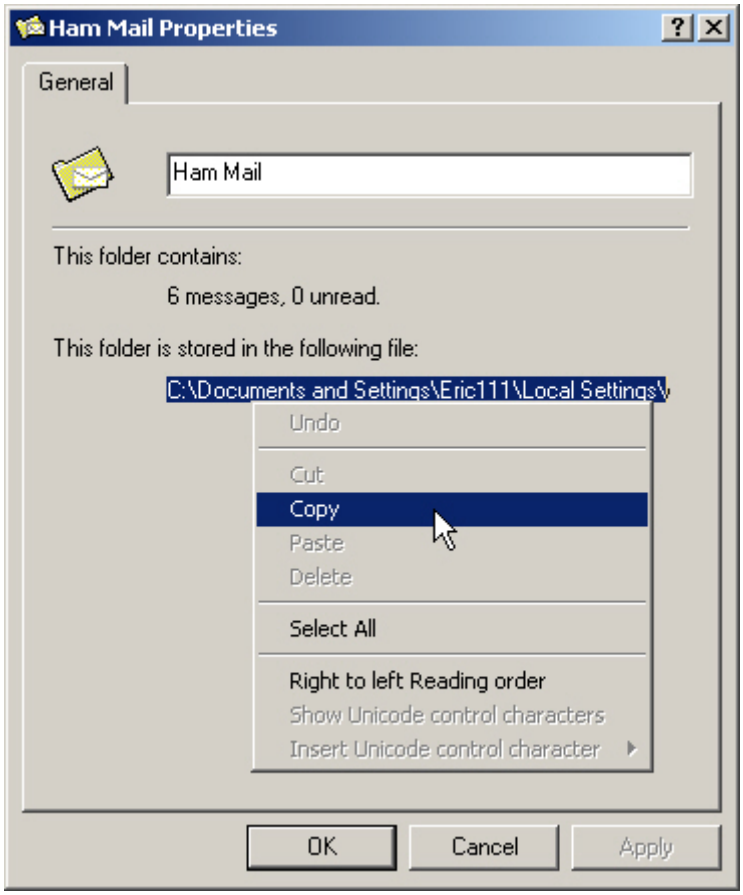


Figure 13-62 Copying the Pathname of the Ham Mail Folder

Step 11. Go to **Mail Security> Anti-Spam > Training**, configure the settings under the **Ham Training Using Importing** section.

- Paste the pathname of the **Ham Mail folder** to the **Import ham mail from** field.
- Click lower right **OK** to import the folder; the ham filtering will be trained on schedules.（**Figure 13-63**）

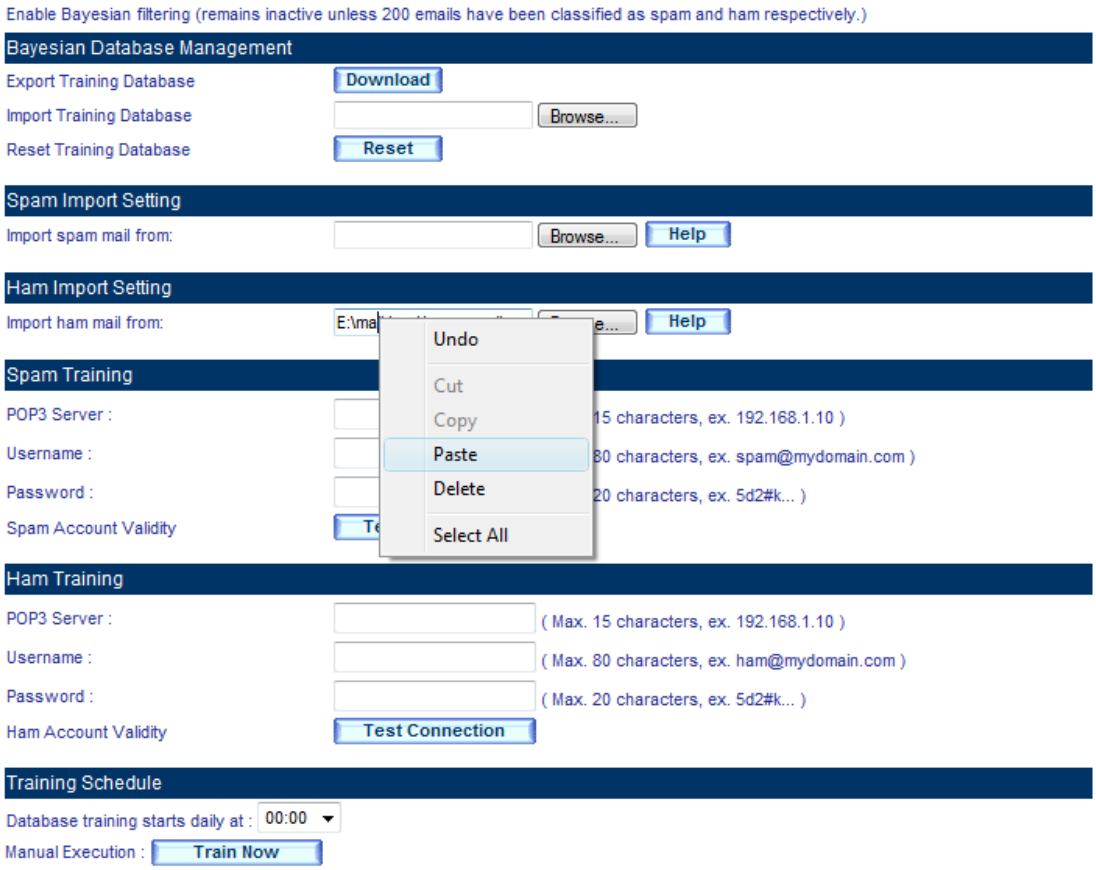


Figure 13-63 Importing Normal Emails for Ham-Filtering Training

Step 12. Delete all emails in the **Ham Mail** folder; since they have been compressed and uploaded to CS-2001, they are of no use any longer:

- In the **Ham Mail** folder, select all normal emails, right-click them, and then click **Delete** on shortcut menu.（**Figure 13-64**）
- All normal emails have been deleted.（**Figure 13-65**）

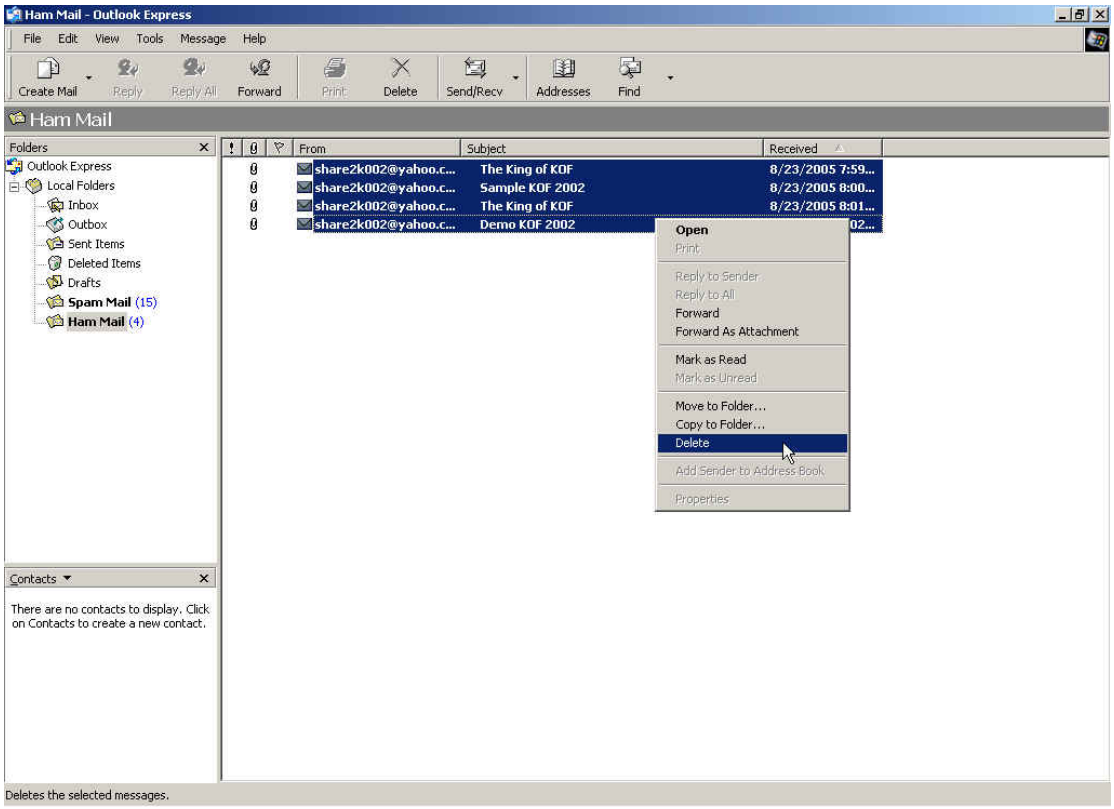


Figure 13-64 Selecting All Normal Emails to Delete

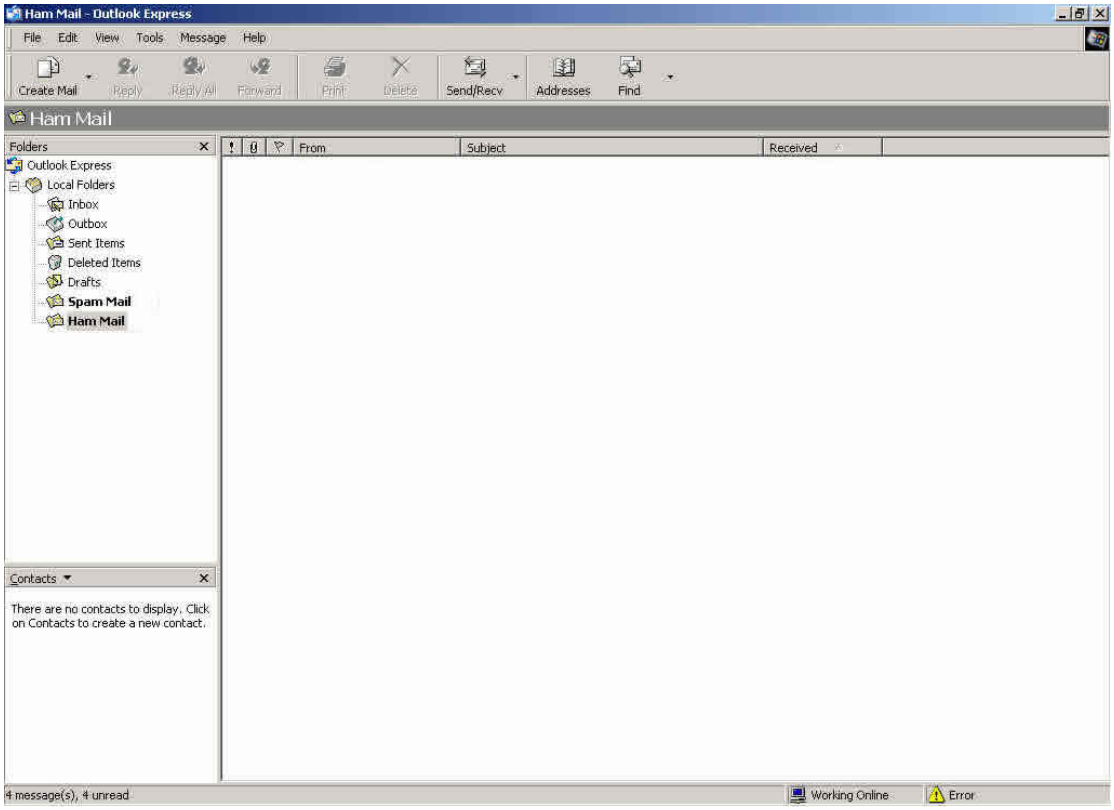


Figure 13-65 All Normal Emails Have Been Deleted

13.1.5 Improving Bayesian Filtering Accuracy by Training

Spam Filtering / Ham-Filtering

Step 1. On you mail server, create an email account, such as spam@supportplanet.com.tw, for gathering spam emails.

Step 2. On you mail server, create an email account, such as ham@supportplanet.com.tw, for gathering normal emails.

Step 3. In **Mail Security** > **Anti-Spam > Training**, configure the **Spam Training Using Forwarded Mail** setting according to the relevant information of spam@supportplanet.com.tw:

- **POP3 Server**: Type “supportplanet.com.tw”.
- Enter the user name and the password.
- Click **OK**.

Step 4. In **Mail Security** > **Anti-Spam** > **Training**, configure the **Ham Training Using Forwarded Mail** setting according to the relevant information of ham@supportplanet.com.tw:

- **POP3 Server**
- Enter the user name and the password.
- Click **OK**.（**Figure 13-66**）

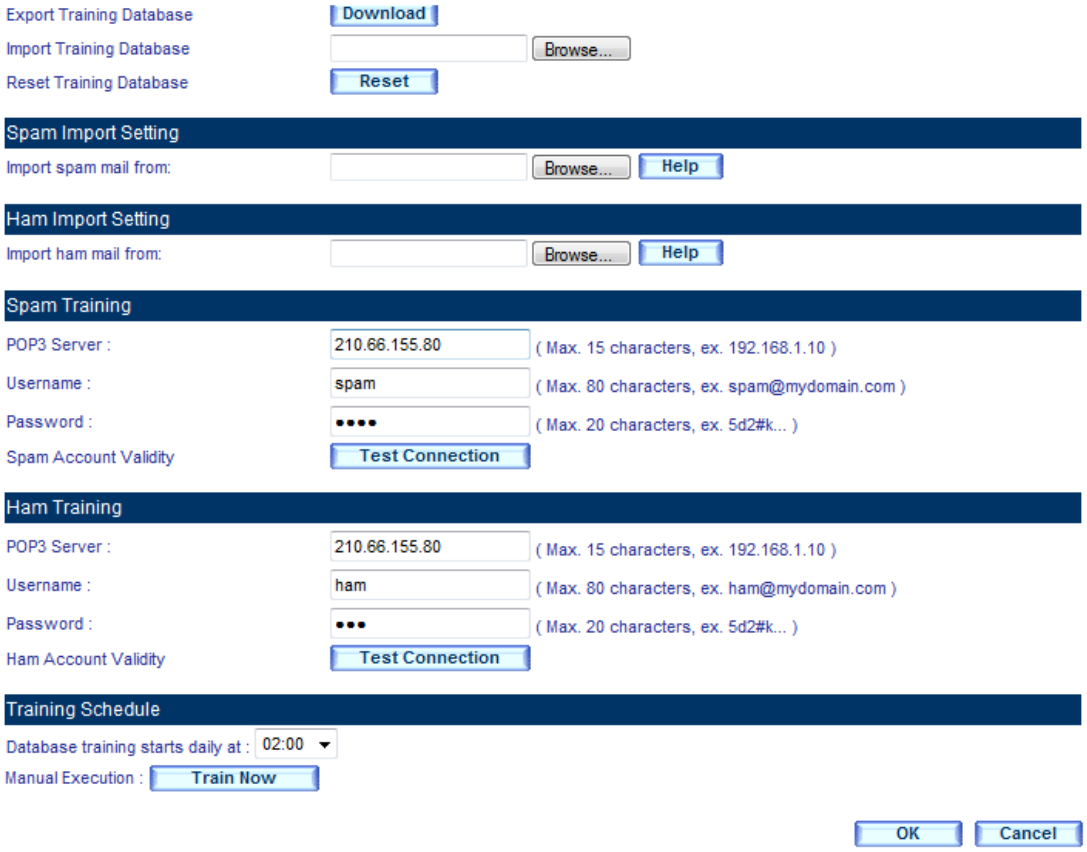


Figure 13-66 Email Accounts Used for Gathering Normal/ Spam Messages and Training

To train spam filtering:

Step 5. In **Outlook Express**, forward all spam emails in the **Inbox** as attachment to spam@supportplanet.com.tw:

- In **Inbox**, select all spam emails, right-click any of the selected emails, and then click **Forward As Attachment** on shortcut menu.（**Figure 13-67**）
- In the **New Message** window, type spam@supportplanet.com.tw in the **To** field, type “Spam” in the **Subject** field, leave out the message content, and then click **Send**.（**Figure 13-68**）

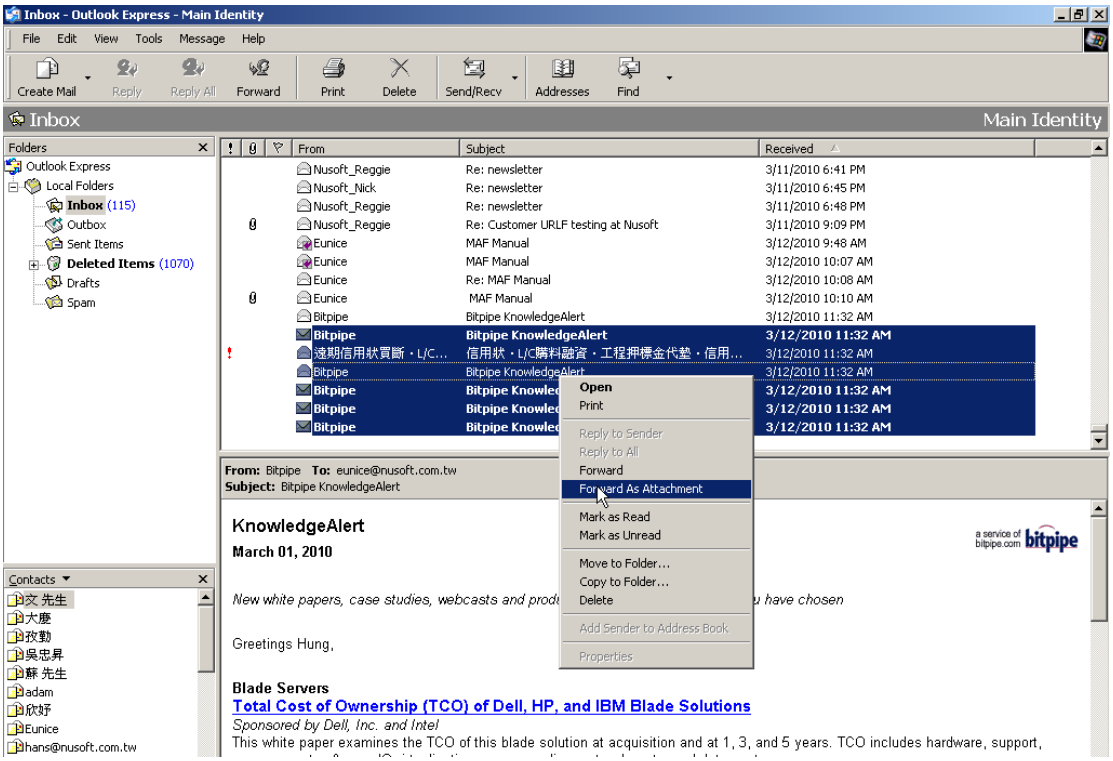


Figure 13-67 Selecting All the Spam Emails

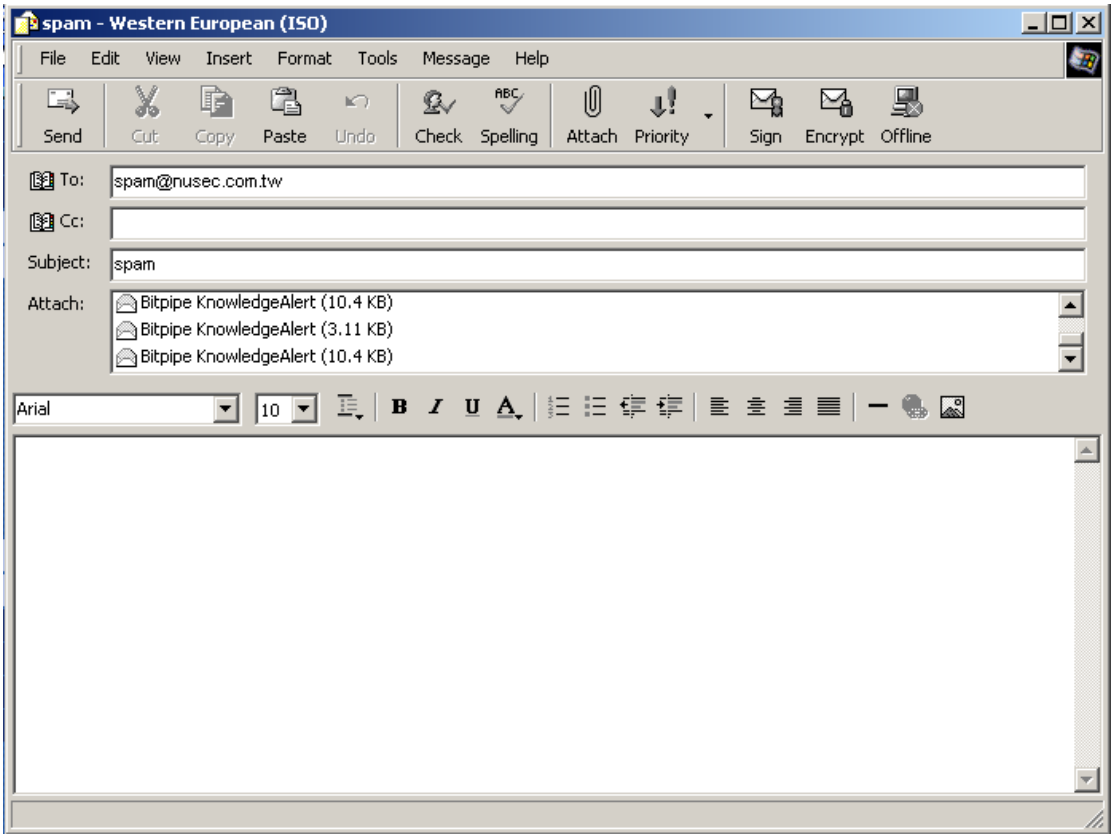


Figure 13-68 Forwarding the Selected Spam Emails as Attachment

To train ham filtering:

Step 6. In **Outlook Express**, forward all normal emails in the **Inbox** as attachment to ham@supportplanet.com.tw:

- In **Inbox**, select all normal emails, right-click any of the selected emails, and then click **Forward As Attachment** on shortcut menu. （**Figure 13-69**）
- In the **New Message** window, type ham@supportplanet.com.tw in the **To** field, type “Ham” in the **Subject** field, leave out the message content, and then click **Send**.（**Figure 13-70**）

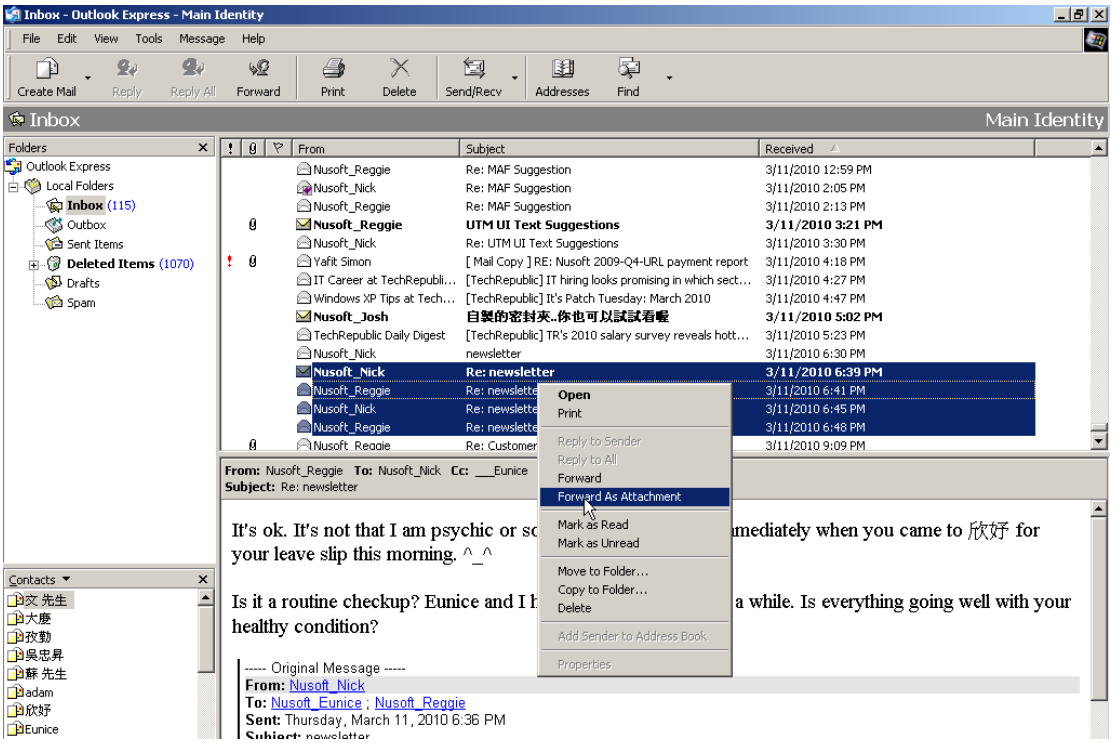


Figure 13-69 Selecting All the Normal Emails

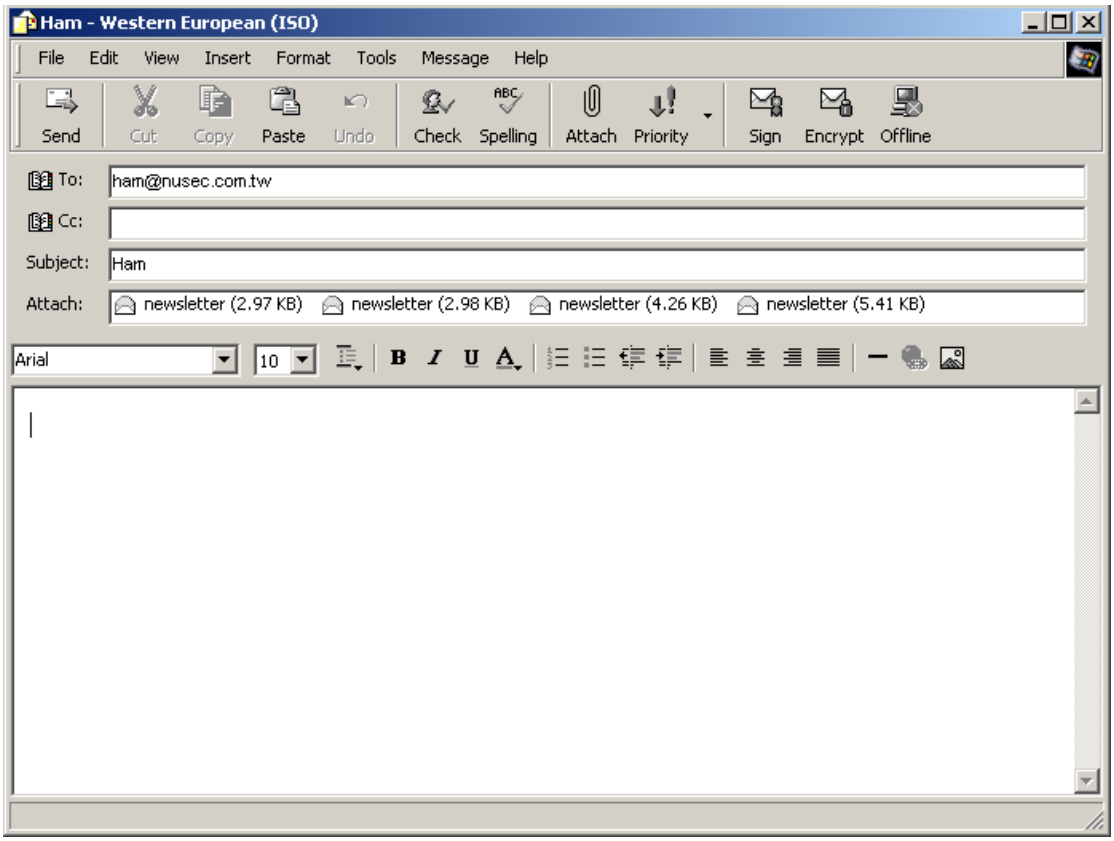


Figure 13-70 Forwarding the Selected Normal Emails as Attachment

Step 7. CS-2001 will retrieve emails in spam@supportplanet.com.tw and ham@supportplanet.com.tw periodically and use them for training on schedules.（**Figure 13-71**）

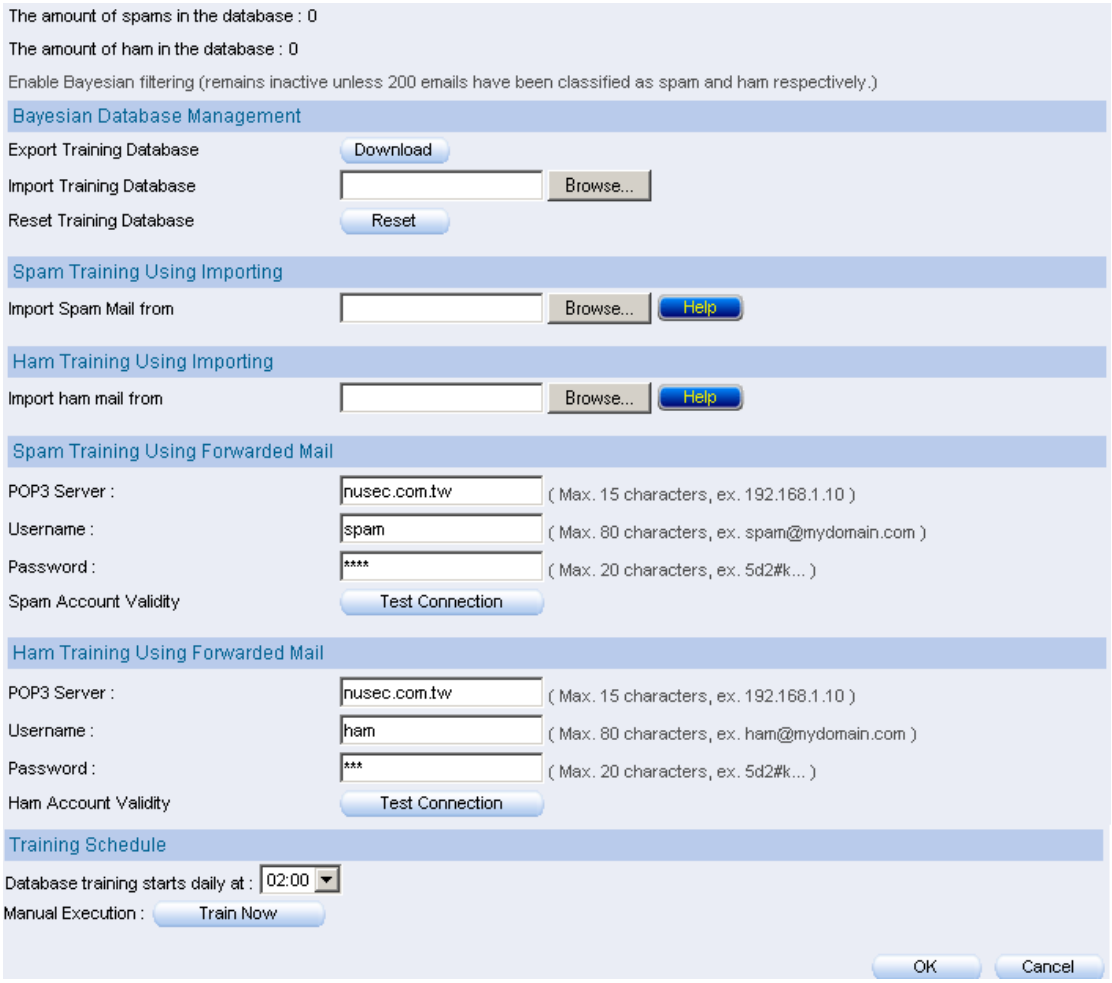


Figure 13-71 Training Schedule Settings

Chapter 14 Anti-Virus

Due to its inbound and outbound email anti-virus scanning capabilities, CS-2001 guards against the extensive damage that virus infections can inflict on your business.

Terms in Setting

Anti-Virus Settings

- Scans inbound and outbound emails for viruses.
- Virus definitions can be updated periodically or can be instantly updated manually. After each update, it will show the definition version and updated time
- Available virus-scanning engines are:
  - ClamAV—The default and free of charge virus-scanning engine.
  - Sophos—The purchase of an end-user license is required for legal use.

Note:

1. To assure the CS-2001 is updated successfully, click **Test Connection** to check whether the connection to the virus definition server works before running the update.
2. Once the Proxy Server is deployed, the proxy settings under **System > Configuration > Settings** must be configured for the CS-2001 to access the Internet.

SMTP Options (For a virus infected email sent from a user)

- Virus emails sent from an external user to the internal mail server or sent from internal user to external user can be deleted, delivered to the recipient (deliver an email notification istead) or stored in the quarantine.

POP3 Options (For a virus infected email sent to a user)

- Virus emails from external mail server to an internal user or from internal mail server to an external user can be delivered to the recipient (or deliver an email notification istead) or stored in the quarantine.
  - Go to **Mail Security > Anti-Virus > Settings** and then set as below:
    - Select ClamAV for **Scanning Engine**.
    - Under the **SMTP Options** section, tick **Deliver the email to the recipient** and select **Deliver an email notification instead**.
    - Click **OK**.（**Figure 14-1**）

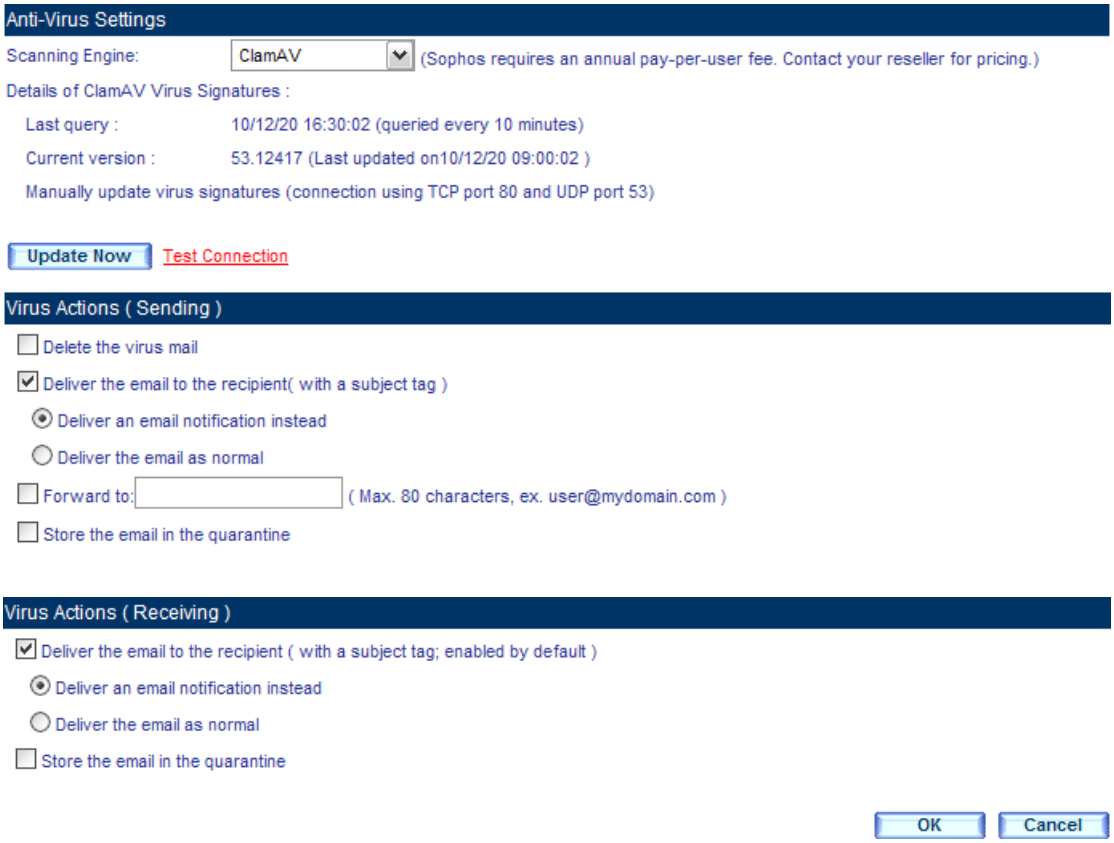


Figure 14-1 Anti-Virus Settings

Note:

1. Three virus-scanning modes available for users are **ClamAV**, **Sophos** and **ClamAV+Sophos**.

14.1 Example

No.	Scenario	Page
14.1.1	Filtering Out the Virus Emails on Mail Server the Virus Emails on Mail Server	**530**
14.1.2	Using CS-2001 as a Gateway to Filter Out Virus Emails (Mail Server Is Deployed in LAN under NAT Mode)	**541**

14.1.1 Filtering Out the Virus Emails on Mail Server

Prerequisite Setup

Configure Port1 as LAN1 (192.168.1.1, NAT/ Transparent Routing mode) and connect it to the LAN which is using 192.168.1.x/24.

Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range: 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range: 211.22.22.18 to 211.22.22.30.

Configure Port4 as DMZ1(Transparent Routing mode) and connect it to the mail server. IP address:61.11.11.12.

Step 1. To enable internal users to receive emails from external mail server, use an external DNS server to resolve domain names. (Please decide which external DNS server to use on your own.)

Step 2. To enable external users to receive emails from internal mail server, configure as below:

1. Deploy the mail server in DMZ.
2. Type “61.11.11.12” in the **IP Address** field of **Internet Protocol (TCP/IP) Properties.**
3. Configure the **Preferred DNS Server** field in **Internet Protocol (TCP/IP) Properties**. (Use an external DNS server to resolve domain names)
4. Name the server as “supportplanet.com.tw”.

Step 3. Go to **Policy Object** > **Address** > **DMZ**, set as below: **(Figure 14-2)**

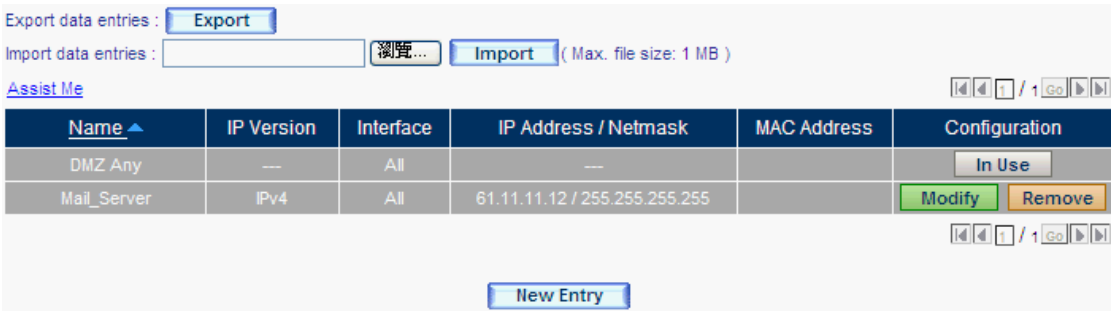


Figure 14-2 Creating an Address Setting Corresponding to the Mail Server

Step 4. Go to **Policy Object** > **Service** > **Group**, set as below:（**Figure 14-3**）

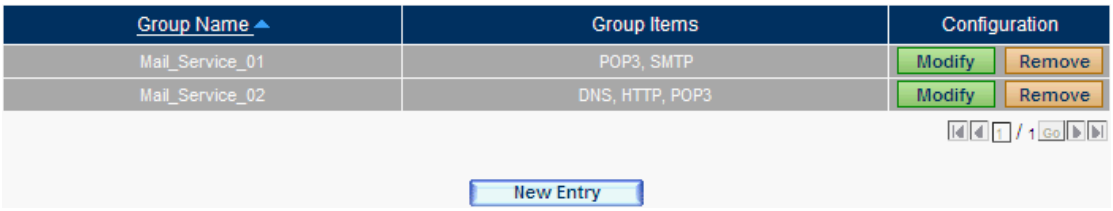


Figure 14-3 Creating Service Groups to Include the POP3, SMTP and DNS Services

Step 5. Under **Policy** > **Outgoing**, set as below: (**Figure 14-4**)

- Select the defined service (Mail_Service_02) for **Service**.
- Select POP3 for **Anti-Virus**.
- Click **OK**. (**Figure 14-5**)

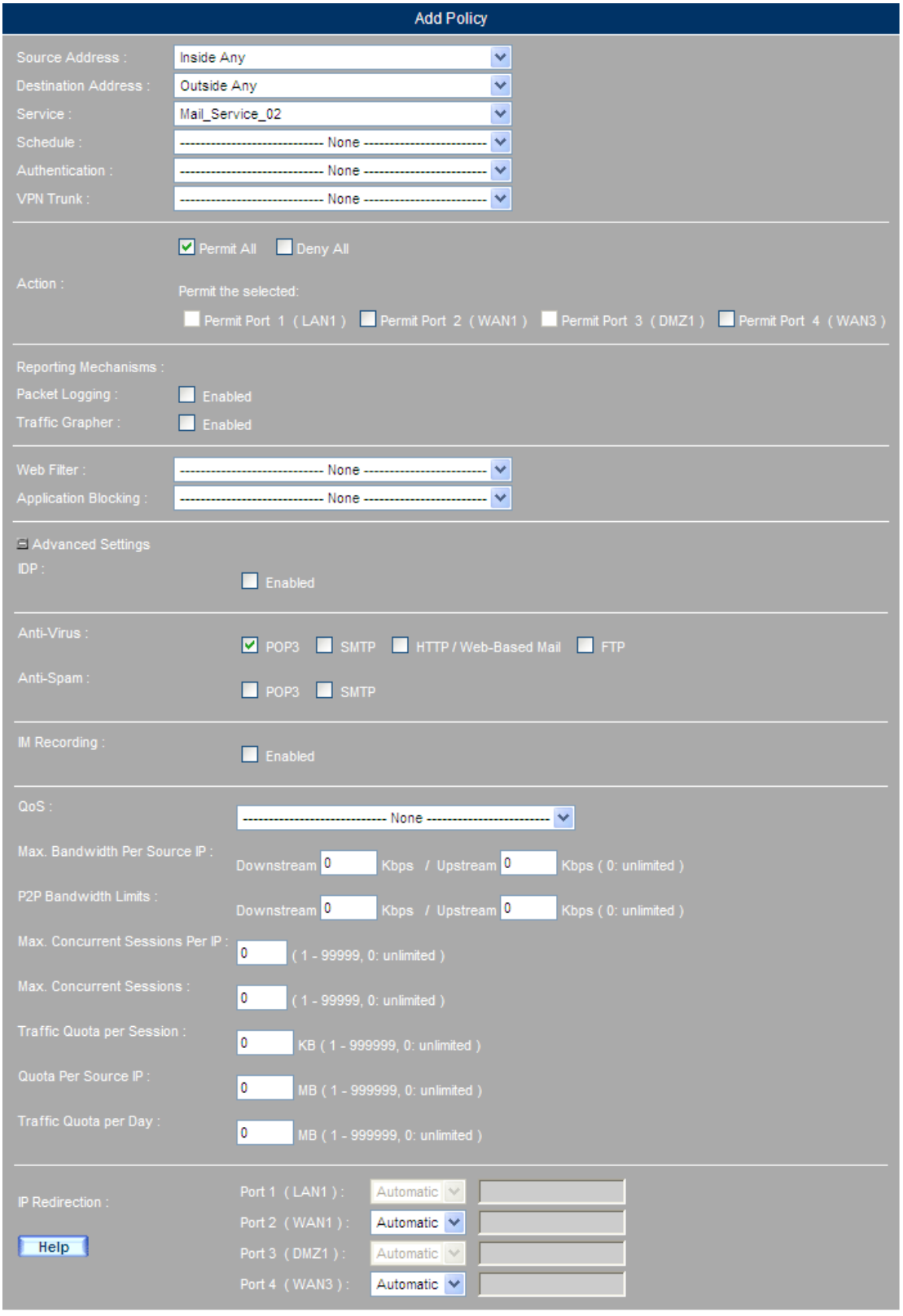


Figure 14-4 Creating an Outgoing Policy with Service and POP3 Anti-Virus

Figure 14-5 Policy Created

Step 6. Under **Policy** > **WAN To DMZ**, set as below: (**Figure 14-6**)

- Select the defined DMZ for **Destination Address.**
- Select the defined service (Mail_Service_01) for **Service.**
- Select POP3 for **Anti-Virus**.
- Click **OK**. (**Figure 14-7**)

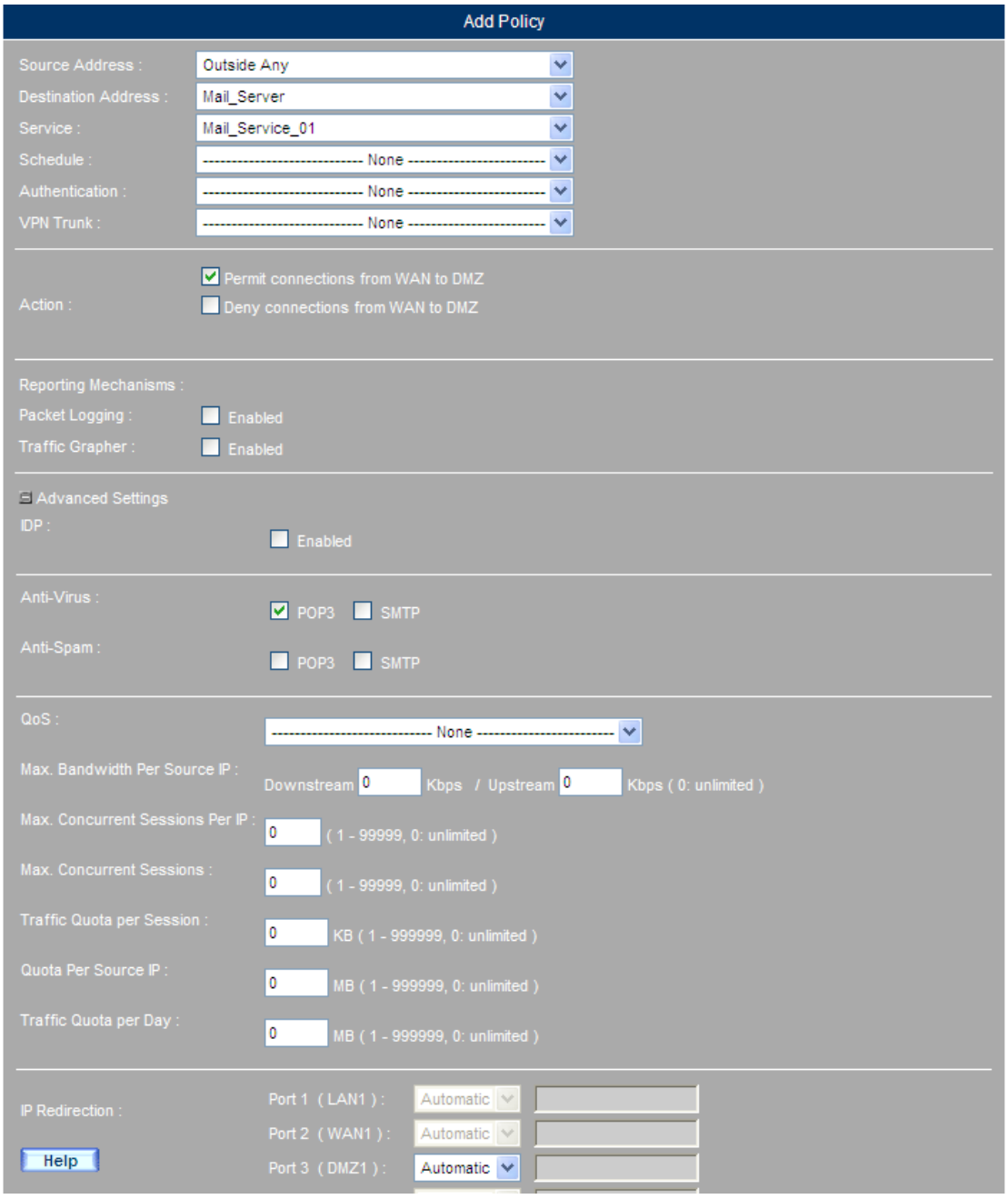


Figure 14-6 Creating a WAN to DMZ Policy with Service and POP3 Anti-Virus

Figure 14-7 Policy Created

Step 7. Under **Policy** > **DMZ To WAN**, set as below:（**Figure 14-8**）

- Select the defined DMZ for **Source Address.**
- Select the defined service (Mail_Service_02) for **Service.**
- Select POP3 for **Anti-Virus**.
- Click **OK**.（**Figure 14-9**）

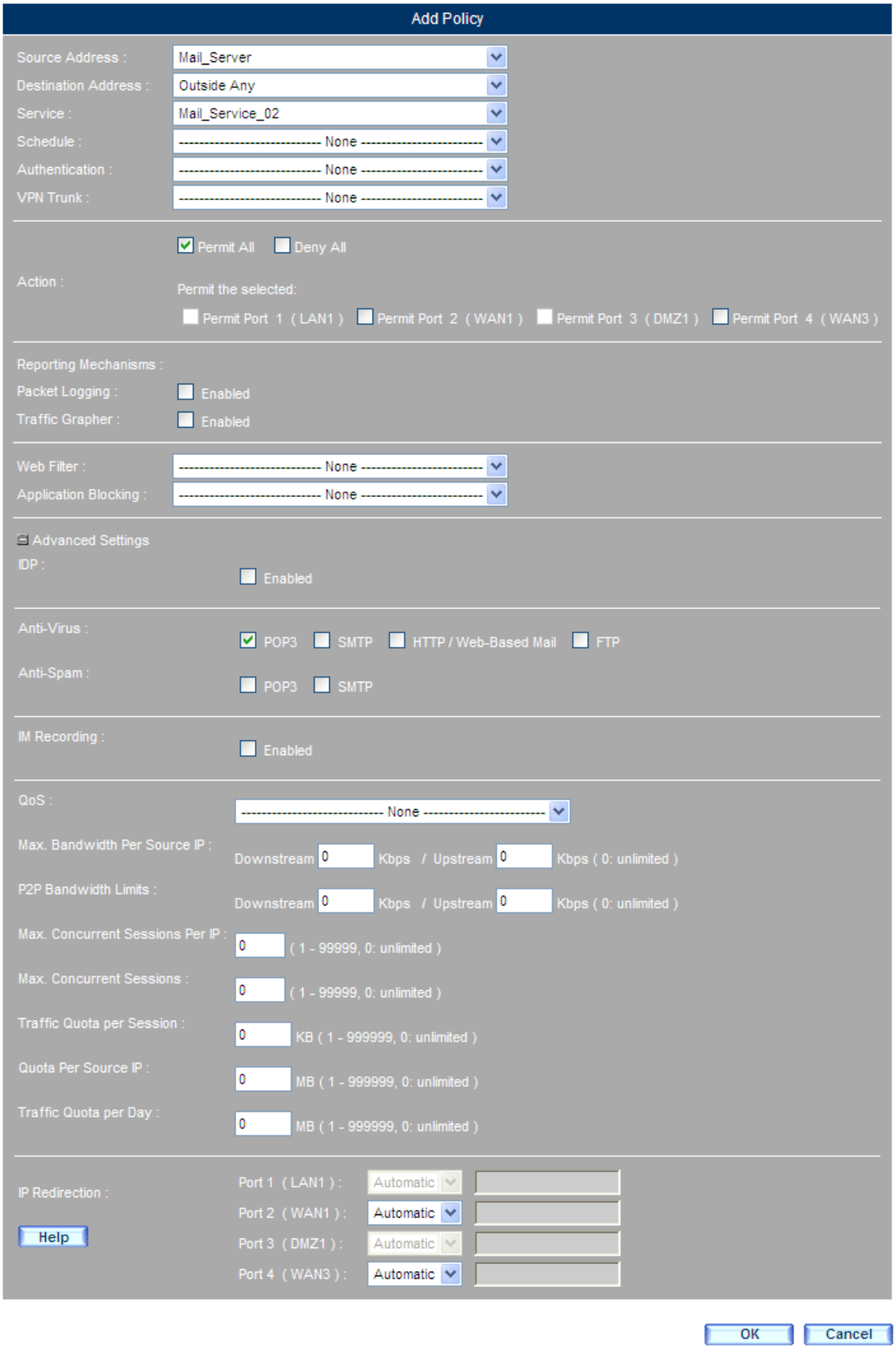


Figure 14-8 Creating a DMZ to WAN Policy with Service and POP3 Anti-Virus

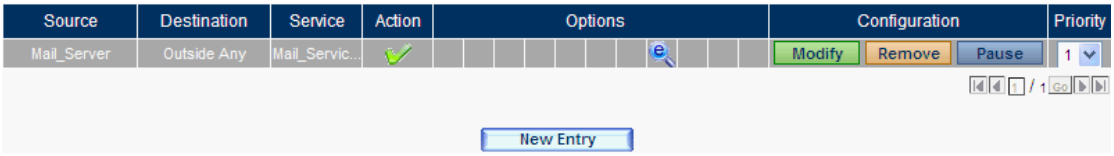


Figure 14-9 Policy Created

Step 8. Go to **Mail Security** > **Anti-Virus** > **Settings** and then set as below: (**Figure 14-10**)

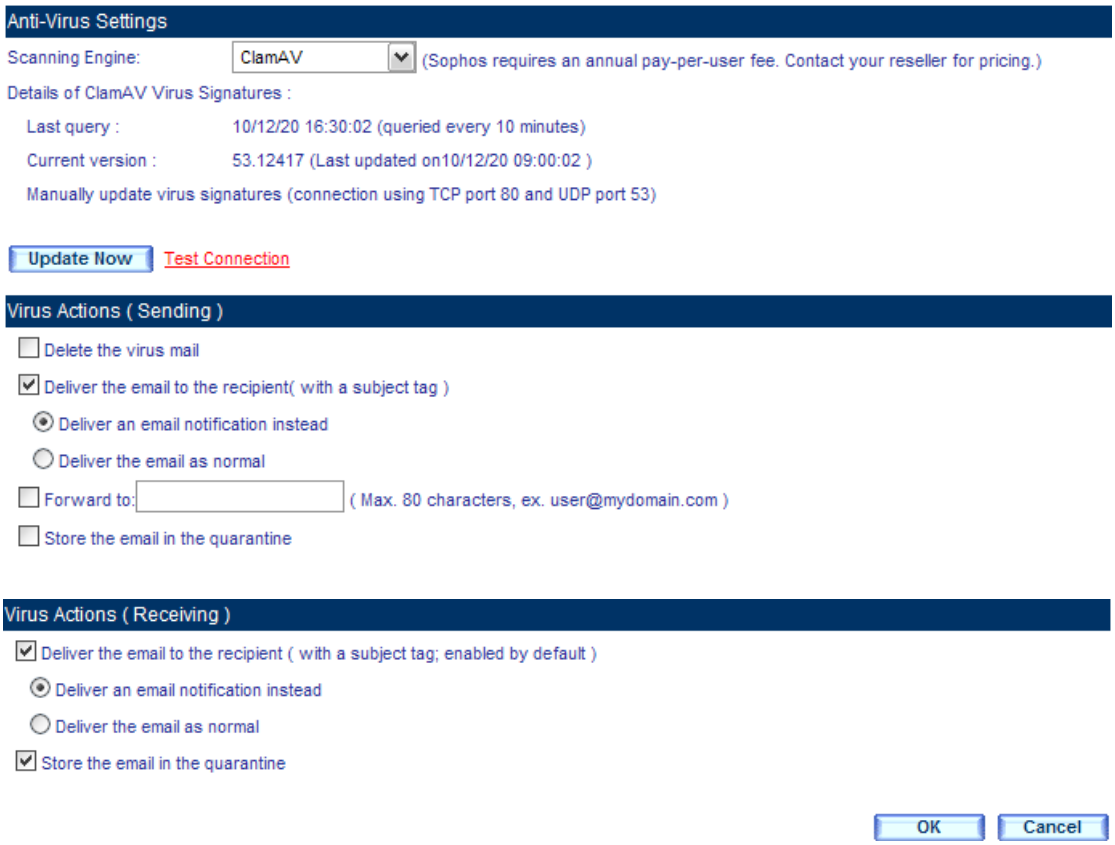


Figure 14-10 Anti-Virus Settings

Note：

1. By default, **Anti-Virus** is enabled. Therefore, the IT administrator merely has to configure the **Mail Domains** to scan all the incoming and outgoing emails for virus.（**Figure 14-11**）

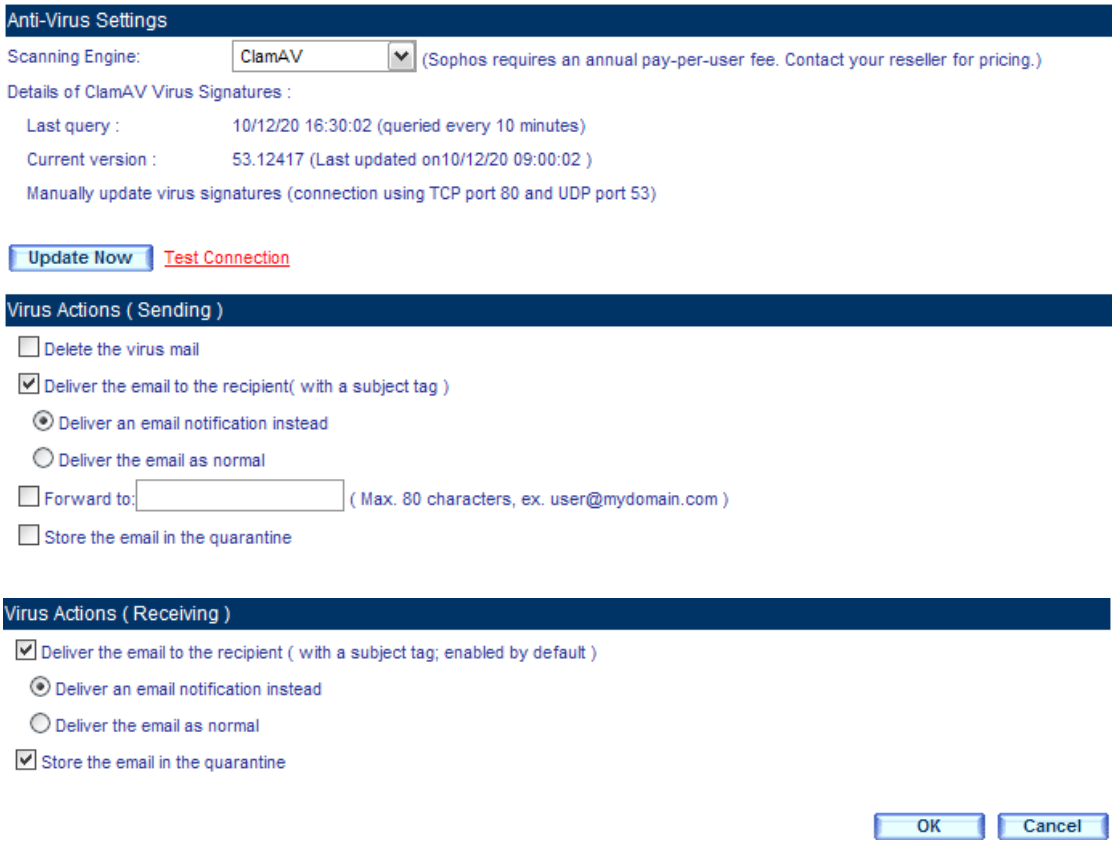


Figure 14-11 Anti-Virus Settings by Default

2. When scanning incoming emails for virus:
   - Under the **POP3 Options** section, the functionality **Deliver the email to the recipient** is enabled by default and can not be disabled; Another alternative handling method is "**Store the email in the quarantine**".

Step 9. When receiving emails from an external mail account, such as js1720@ms21.pchome.com.tw, CS-2001 will scan emails for viruses.

Step 10. When an external user receiving emails from an internal account, such as joe@supportplanet.com.tw, CS-2001 will scan emails for viruses.

14.1.2 Using CS-2001 as a Gateway to Filter Out Virus Emails

(Mail Server Is Deployed in LAN under NAT Mode)

Prerequisite Setup

Configure Port1 as LAN1(192.168.2.1, NAT/Routing mode) and connect it to the LAN which is using 192.168.2.x/24.
Mail Server: using LAN1 IP address (192.168.2.12) mapping to WAN1 IP address(61.11.11.12).

Configure Port2 as WAN1(61.11.11.12) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet. IP range: 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet. IP range:211.22.22.18 to 211.22.22.30.

Configure Port4 as DMZ1.

Step 1. Setup a mail server in LAN, name it as “supportplanet.com.tw”, configure its IP address as 192.168.2.12, and then use an external DNS server to resolve domain names.

Step 2. Under **Policy Object** > **Address** > **LAN**, set as below:（**Figure 14-12**）

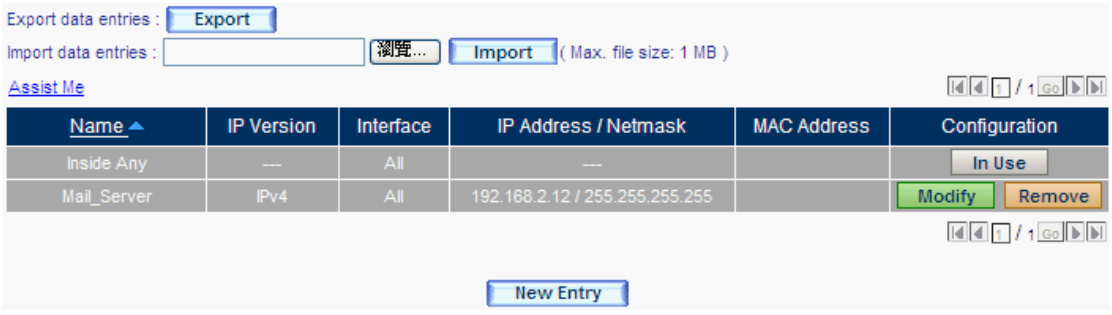


Figure 14-12 Address Setting for the Mail Server

Step 3. Under **Policy Object** > **Service** > **Group**, set as below:（**Figure 14-13**）

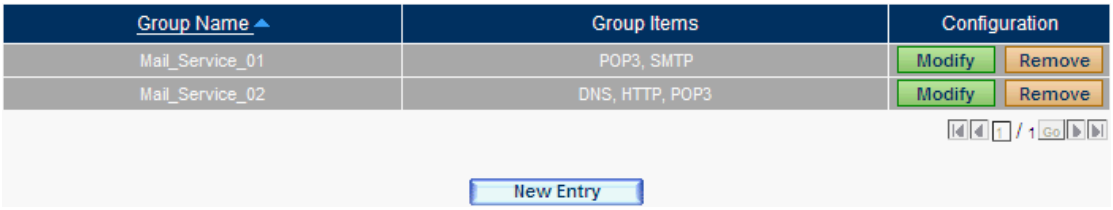


Figure 14-13 Creating Service Groups to Include POP3, SMTP and DNS Service

Step 4. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below:

（**Figure 14-14**）

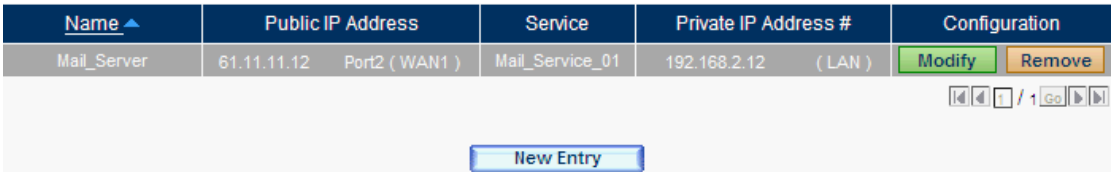


Figure 14-14 Port Mapping Settings

Step 5. Under **Policy** > **Incoming**, set as below: (**Figure 14-15**)

- Select the defined virtual server for **Destination Address.**
- Select the defined service (Mail_Service_01) for **Service.**
- Select SMTP for **Anti-Virus**.
- Click **OK**. (**Figure 14-16**)

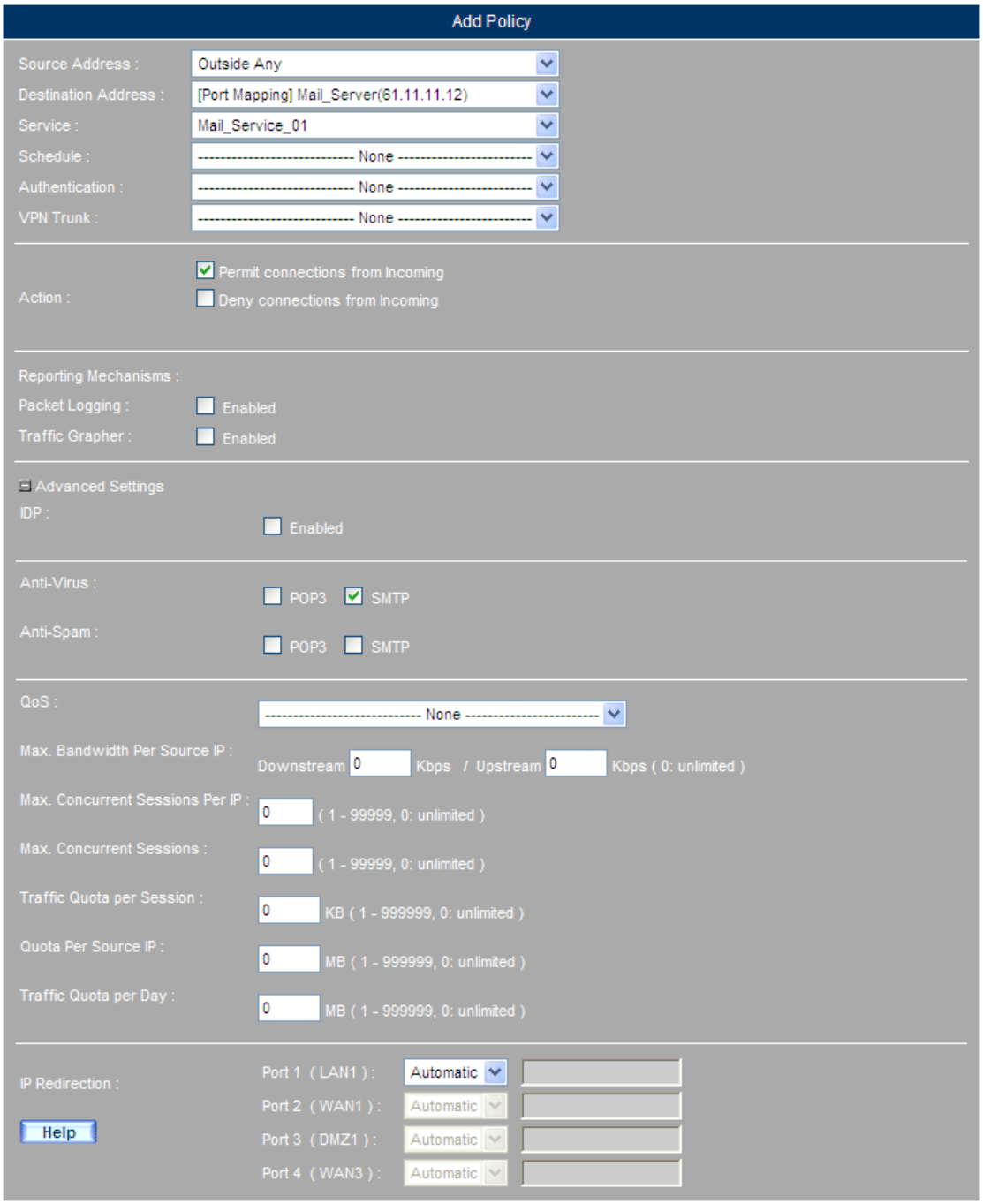


Figure 14-15 Creating an Incoming Policy with Service and SMTP Anti-Virus

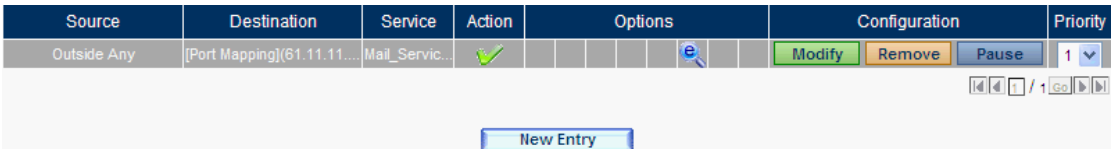


Figure 14-16 Policy Completed

Step 6. Under **Policy** > **Outgoing**, set as below: (**Figure 14-17**)

- Select the defined LAN address for **Source Address.**
- Select the defined service (Mail_Service_02) for **Service.**
- Select SMTP for **Anti-Virus**.
- Click **OK**. (**Figure 14-18**)

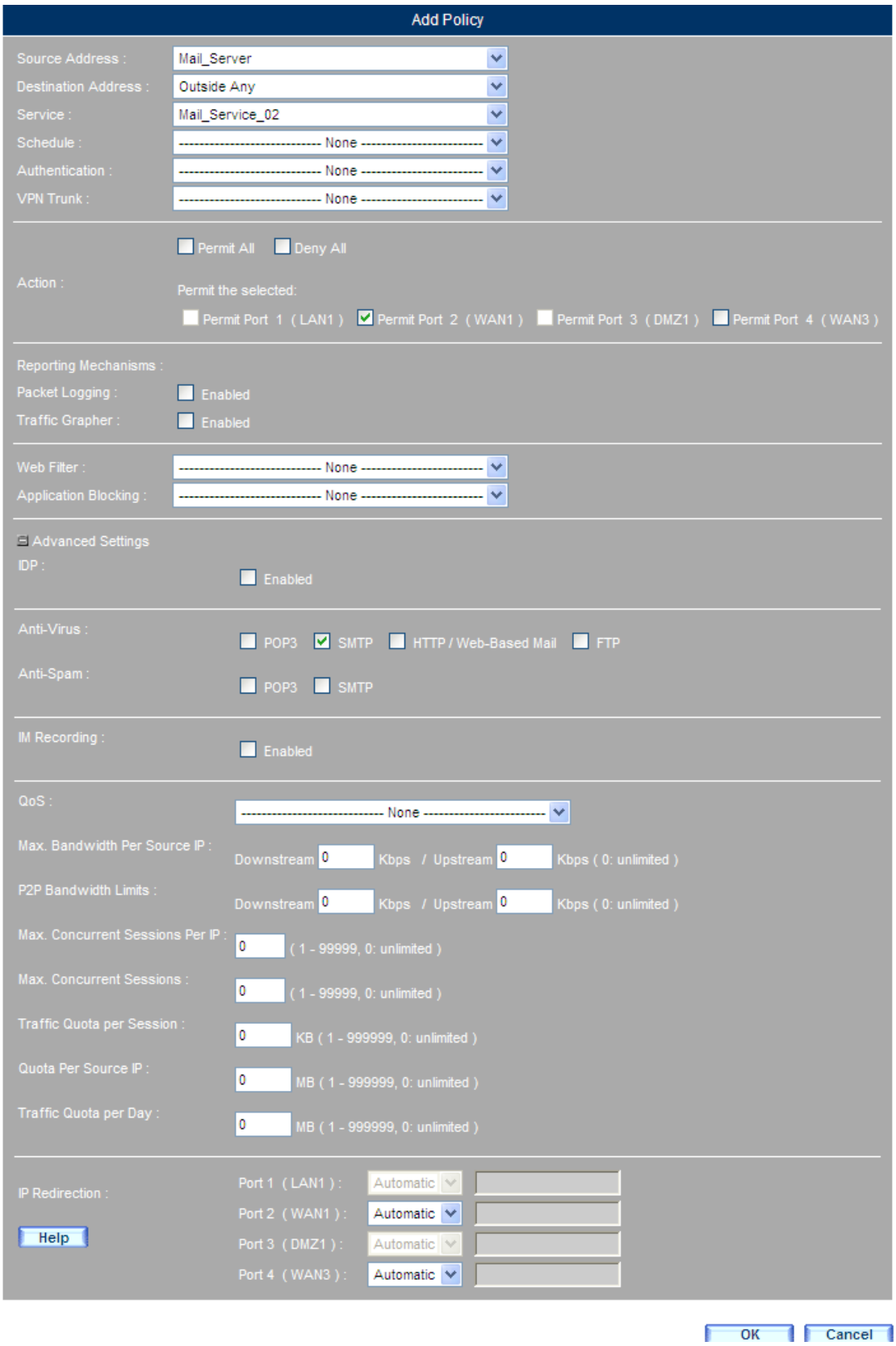


Figure 14-17 Creating an Outgoing Policy with Service and SMTP Anti-Virus

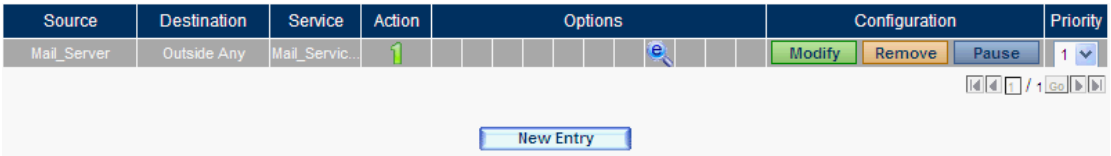


Figure 14-18 Settings Completed

Step 7. Go to **Mail Security** > **Configuration** > **Mail Domains** and then set as below:（**Figure 14-19**）

Figure 14-19 Mail Domain Settings

Step 8. Go to **Mail Security** > **Anti-Virus** > **Settings** and then set as below:（**Figure 14-20**）

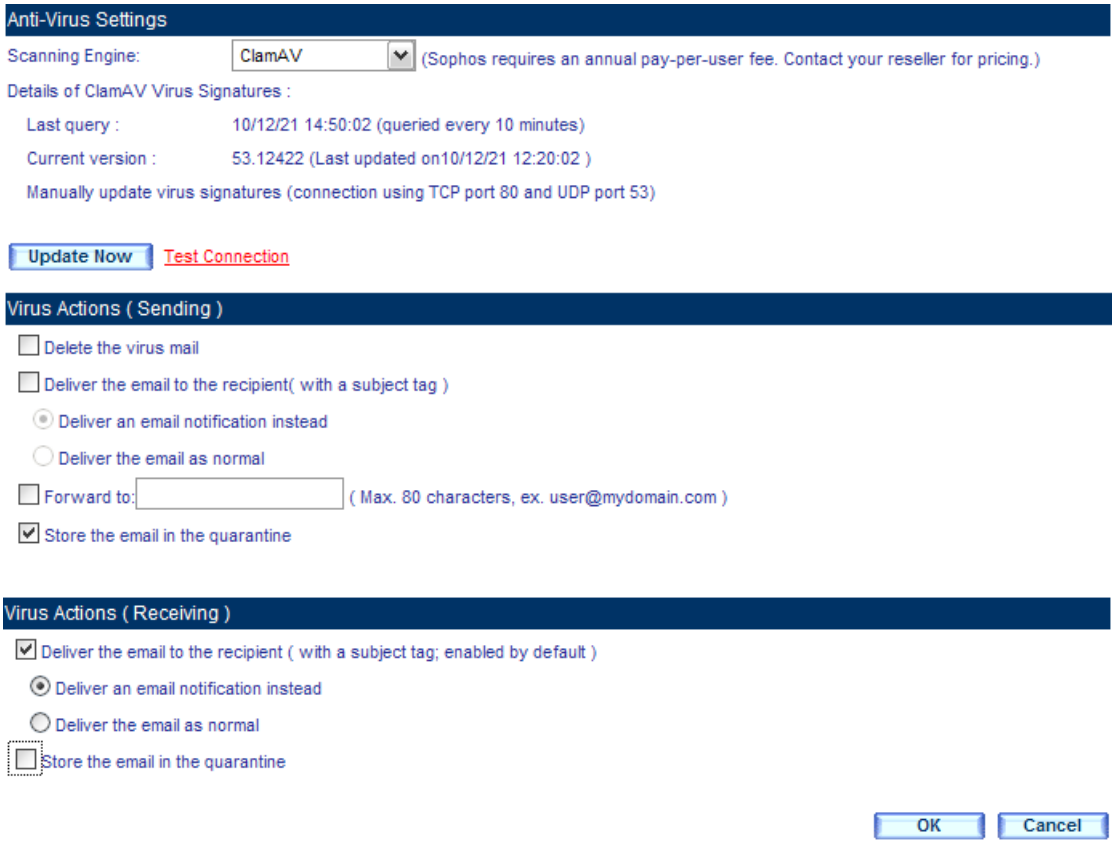


Figure 14-20 Anti-Virus Settings

Note：

1. When **Delete the virus mail** is selected, virus-infected emails will be deleted immediately upon detection. Other options, **Deliver the email to the recipient** and **Store the email in the quarantine** will be disabled to be selected. Logs are shown under **Mail Security** > **Mail Reports** > **Logs**.

Step 9. When “Joe”, an internal user at supportplanet.com.tw, receives emails from external mail accounts at yahoo.com.tw:

- The virus mail from share2k01@yahoo.com.tw will be stored in the quarantine.
- The regular mail from share2k003@yahoo.com.tw will be sent to joe@supportplanet.com.tw.

Step 10. When “Joe”, an internal user at supportplanet.com.tw, sends emails to the recipients at yahoo.com.tw:

- The virus mail sent to share2k01@yahoo.com.tw will be stored in the quarantine.
- The regular mail sent to share2k003@yahoo.com.tw will be sent to the recipient.

Chapter 15 Mail Reports

CS-2001 provides you with email reports in the form of statistics and logs, presenting you with a thorough insight into the email activities of the business.

Terms in Setting

Periodic Report Scheduling Settings

- It can generate and send out the periodic report to the designated recipient(s) on schedules.

History Report Scheduling Settings

- It can generate and send the history report to the designated recipient(s) on schedules.
  - Go to **System > Configuration > Settings**, configure the **Email Notification Settings**. Then, go to **Mail Security > Mail Reports > Settings**, set as below:
    - Under the **Periodic Report Scheduling Settings** section, tick **Enable the mailing of Periodic Report** and then select **Yearly report, Monthly report**, **Weekly report** and **Daily report**.
    - Click **OK**.（**Figure 15-1**）
    - The designated recipient will receive the reports on schedules.（**Figure 15-2**）
    - Under the **History Report Shceduling Settings**, tick a desired period and specify a date for it.
    - Click **Mail Report**.
    - The designated recipients will receive reports on schedules.

Note：

1. Periodic report schedule:

- Yearly Report: Creates the report at 00.10 on January 1.
- Monthly Report: Creates the report at 00.10 on the first day of the month.
- Weekly Report: Creates the report at 00.10 on the first day of the week.
- Daily Report: Creates the report at 00.10 everyday.

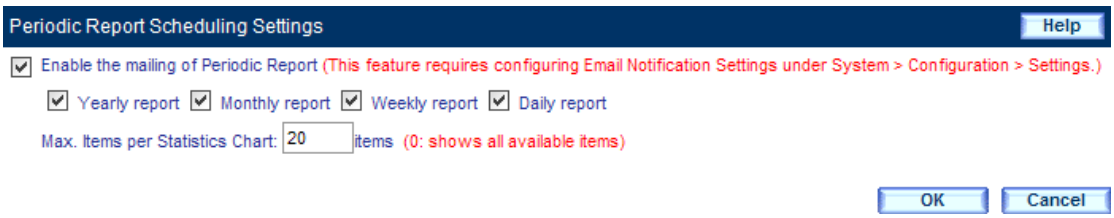


Figure 15-1 Periodical Report Settings

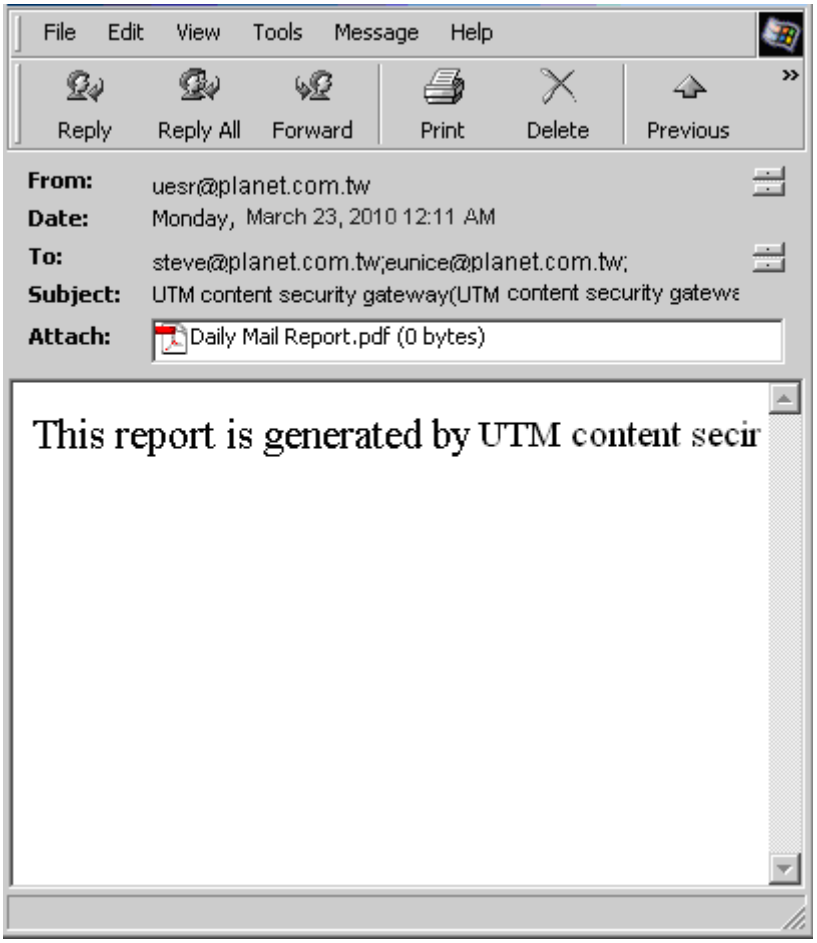


Figure 15-2 Periodical Report Sent as an Attachment

Terms in Logs

Search

- Available searching criteria are: date, sender, sender IP, recipient, attachment, subject, attribute and process.
  - Go **to Mail Security > Mail Reports > Logs**, click the **Search** icon and then set as below:
    - Enable the searching duration and then specify a period of time.
    - Type the keyword in the **Recipient** field.
    - Select All for **Attachment**.
    - Select All for **Attribute**.
    - Select All processes for **Process**.
    - Click **Search**.（**Figure 15-3**）
    - To store the searching results in the local computer, click the **Download Report** button.
    - To export the searched emails, click the **Export Mail** button.

Figure 15-3 Searching for a Specific Log

Note：

1. How to open an ".mbx" file (exported from quarantined or archived emails) on your local computer:

- Convert the ".mbx" file into an ".eml" file with an mbx2eml application (e.g., IMAPSize) and then run Outlook Express to open the ".eml" file.

- Run IMAPSize, go to **Tools > mbox2eml** on the menu bar, and then click it.（**Figure 15-26**）
- In the **mbox2eml** window, click the **Select mbox files to convert** button, locate the ".mbx" file, click **Open**, and then click **Convert** to start converting the file into an ".eml" file.（**Figure 15-27, 15-28, 15-29**）
- Run Outlook Express to open the ".eml" file.（**Figure 15-30**）

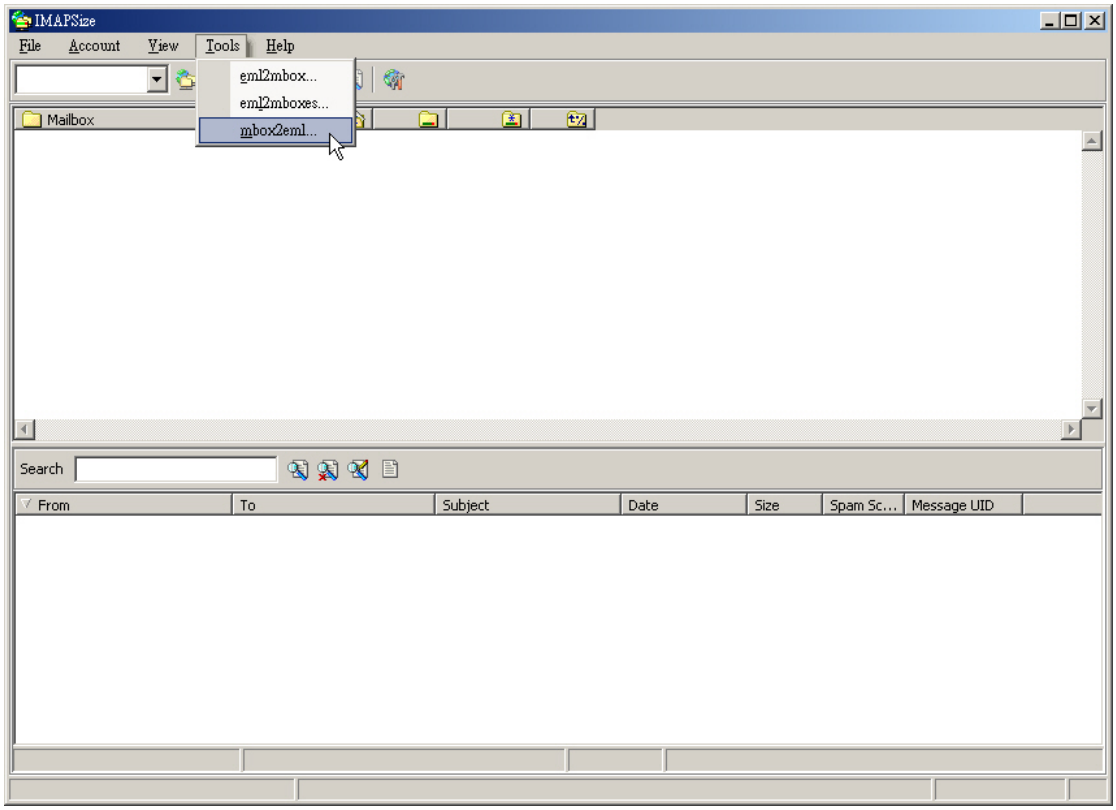


Figure 15-26 Navigating to Tools > Mbox2eml on the Menu Bar

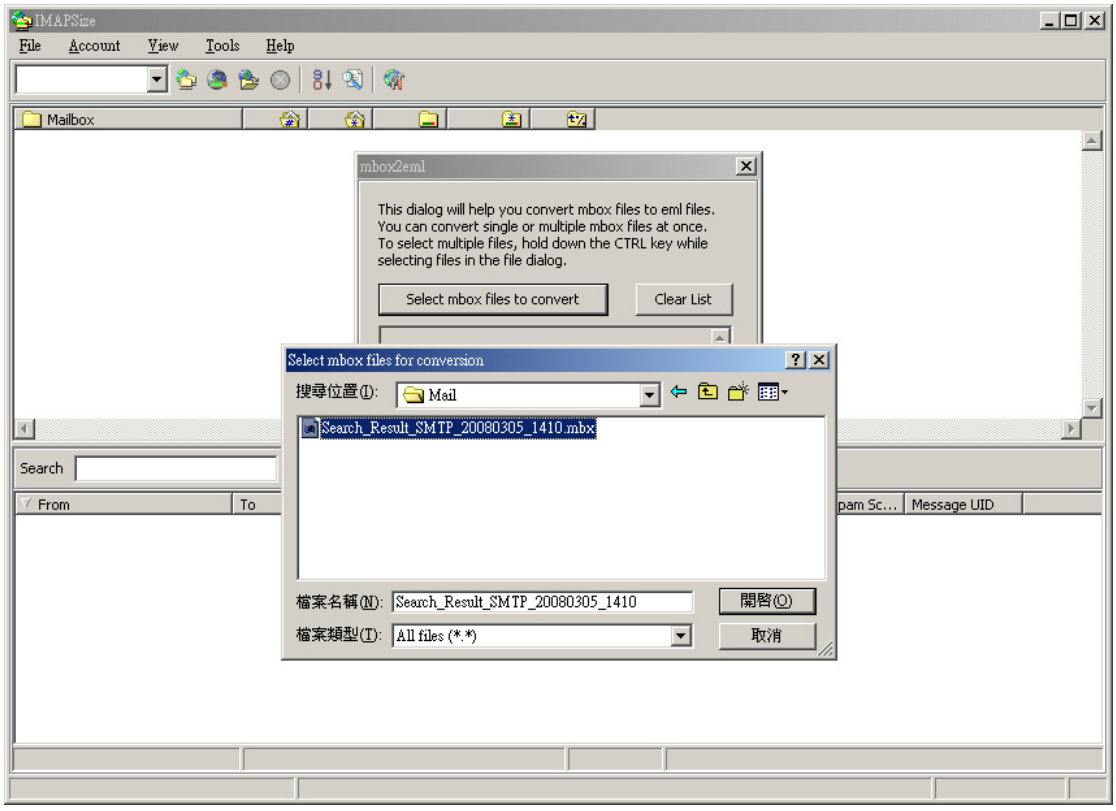


Figure 15-27 Locating the ".mbx" File to be Converted

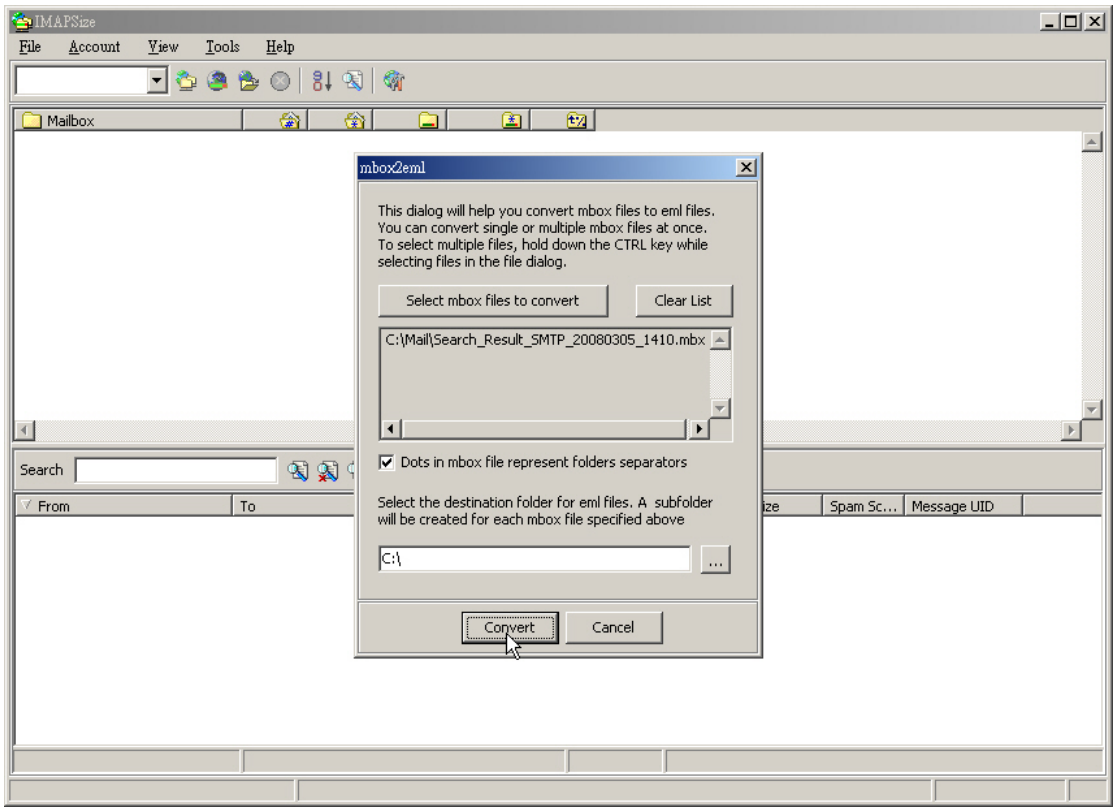


Figure 15-28 Converting the ".mbx" File into an ".eml" File

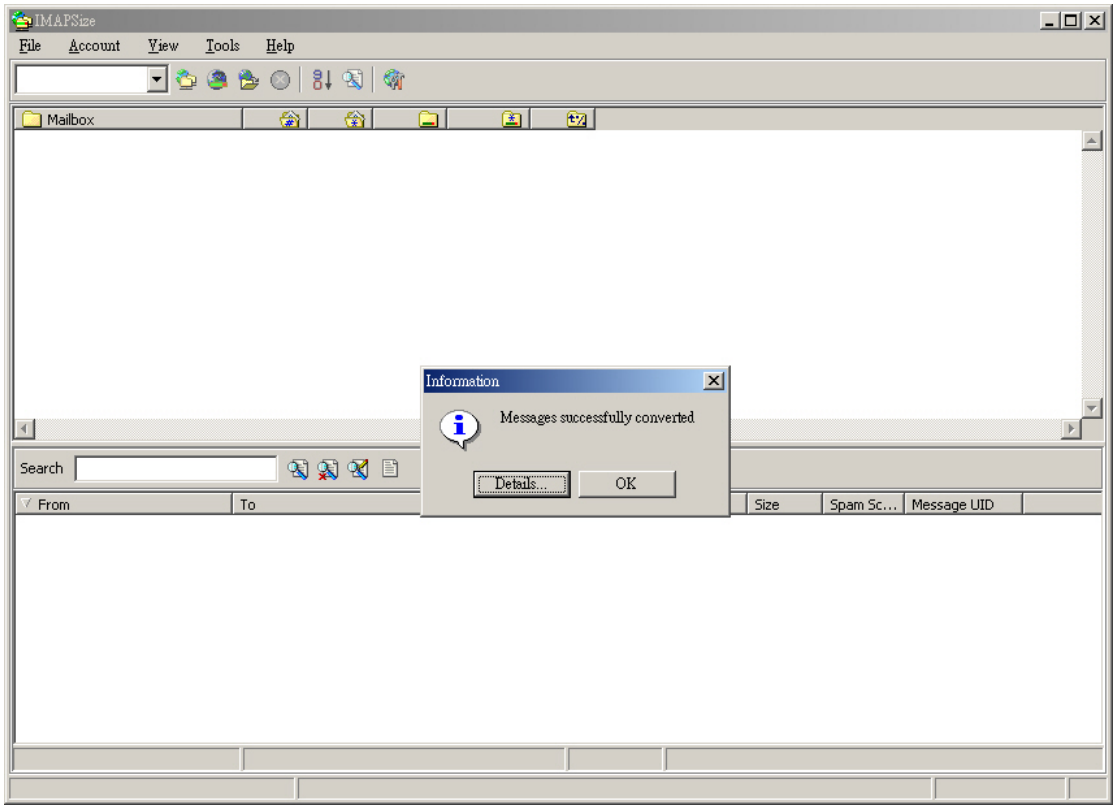


Figure 15-29 File Conversion Completed

Figure 15-30 Clicking and Dragging the ".eml" File into Outlook Express to Open It

15.1 Statistics

Step 1. **Mail Security** > **Mail Reports** > **Statistics** shows a comprehensive statistical report.

Step 2. In the upper left corner, click **Day** for a daily statistics report; click **Week** for a weekly statistics report; click **Month** for a monthly statistics report; click **Year** for an annual statistics report.

15.2 Logs

Step 1. Under **Mail Security** > **Mail Reports** > **Logs**, it shows how emails are processed.

The symbols used in **Logs**:

- Attribute：

Symbol				
Description	Regular	Spam	Virus	Unscanned

- Process:

Symbol					
Description	Deleted	Notified	Delivered	Stored	Retrieved

- Attachment:

Web Filter

Chapter 16 Configuration

Regulating the websites that employees may access improves profuctivity, and protects the network from the damage caused by malicious software or code.

- Whitelist : To permit access to specific websites, the IT administrator may enter the complete URL, or a URL in combination with a wildcard (*).
- Blacklist : To block access to specific websites, the IT administrator may enter the complete URL, or a URL in combination with a wildcard (*).
- Category: The IT administrator may block websites based upon their classification. (This feature requires activation; please contact your distributor for pricing details)
- File Extensions: To block the specific file extensions downloaded or uploaded via HTTP or FTP.
- MIME/Scritp: To block the access to Window Popup, Microsoft Active X, Java Applet, Web Cookie, etc.
- Group: A group can be formed from a combination of any Whitelist, Blacklist, Category, File Extensions, MIME/ Script or Group settings.

Terms in Setting

URL Blocking License

- To activate the **Category** feature for URL Blocking, the license key must be imported into the device here.
- Each license key is unique to the device it was purchased for, thus the key is invalid if used on other devices. To obtain a key, or if your current license has expired, please contact your distributor.

Alert Message Settings

- Once a user attempts to access a blocked website, their browser can display a customizable notification message.

Storage Lifetime of Logs

- Provides a setting to specify the storage time required to keep the **URL Blocking** logs.
- The logs may be stored in the designated remote storage device.

HTTP/ FTP Virus Scanning

- The HTTP/FTP file size that is less than the defined value will be scanned.
  - Go to **Web Filter** > **Configuration** > **Settings** and then set as below:
    - Browse the location path of the license key.
    - Click **Enable message alerts for website blocking** and then enter the alert message to be displayed.
    - Enter 60 in the **Storage Lifetime** field.
    - **Max. File Scanning Size**: enter 512.
    - Click **OK**.（**Figure 16-1**）

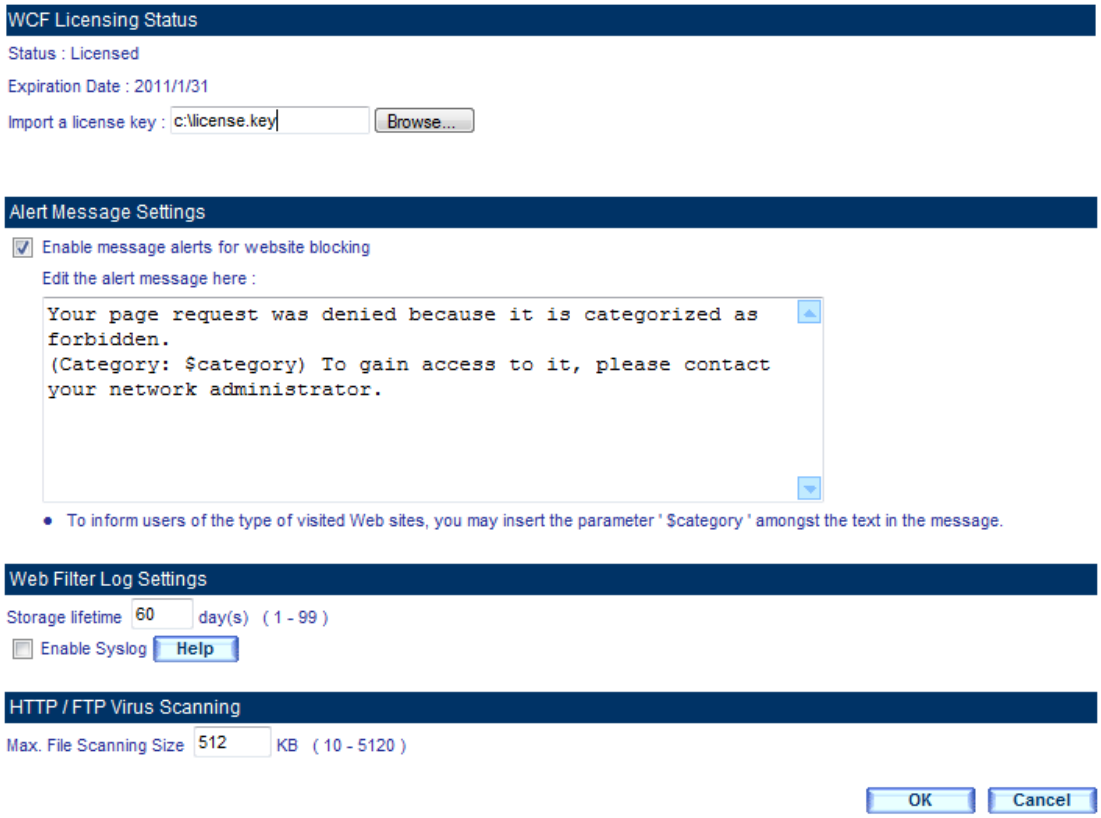


Figure 16-1 Web Filter Settings

Note：

1. Before enabling syslog, please configure the syslog setting under **System > Configuration > Settings**.

- The alert message displays when an internal user tries to access the blocked web page.（**Figure 16-2**）

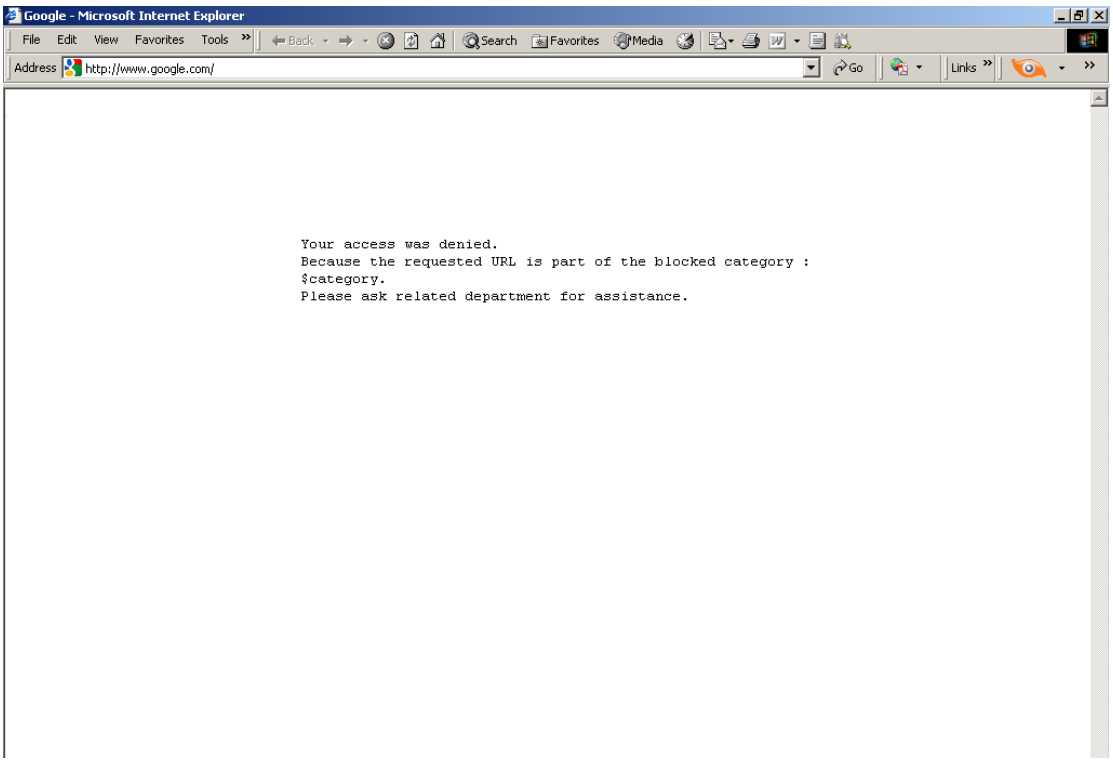


Figure 16-2 The Alert Message

Terms in Whitelist

Name

- The name of the Whitelist.

URL

- Specifies permitted URLs.
- The asterisk character (“*”) allows any website.

Terms in Blacklist

Name

- The name of the Blacklist.

URL

- Specifies any URLs required to be blocked.
- The asterisk character (“*”) blocks any websites.

Terms in Category

Name

- The name for the Category.

Member

- Provides the following categories: Anti-Social and Illegal, Pornographic and Abusive, Gaming and Gambling, Society and Commerce, Communication and Technology, Leisure, Information and Education, and Other. Each category contains further subcategories available for selection.
- Provides various URL category for configuring specific management.

Note：

1. The checking procedure performed on each website is in the following order: Whitelist → Blacklist → Category → Group.

Terms in Extension

Name

- The name of the Extension.

Predefined File Extensions (Select All)

- Blocking the file with the default extension of attachment transferred via HTTP or FTP protocol.

Custom File Extensions (Select All)

- Blocking the file with the defined extension of attachment transferred via HTTP or FTP protocol.

Any file extensions used by download manager software

- Blocking any file extensions used by download manager software.

All Types of file extensions

- Blocking the thansferring of file extensions via HTTP or FTP.

Terms in MIME/Script

Name

- The name of MIME/Script.

Script

- Window Popup：Blocking the popup window.
- Microsoft ActiveX：Disallowing the execution of ActiveX.
- Java Applet：Disallowing the execution of Java.
- Web Cookie：Blocking Web Cookie.

MIME Type

- MIME (Multipurpose Internet Mail Extensions) is an Inernet standard that extends the format of e-mail. It supports the binary content and text in character sets other than ASCII. In addition, it is also be used for communication protocols like HTTP.
- MIME defines the format of e-mail.
- Content-Type, the header indicates the type of the message content, consisting of type and subtype.
  - Type:
    - Text: Format the text message.
    - Multipart: Combine different type messages into one.
    - Application：Transfer application or binary content.
    - Message：Construct message.
    - Image：Transfer image.
    - Audio：Transfer audio.
    - Video：Transfer video.
  - Subtype:
    - text/plain
    - text/html
    - application/xhtml+xml
    - image/gif
    - image/jpeg
    - image/png

- video/mpeg
- application/octet-stream
- application/pdf
- application/msword

Important:

1. To apply the Whitelist, Blacklist, Category, File Extensions and MIME/Script to the Policy, those rules need to be added in the Group first.

16.1 Example

No.	Settings	Scenario	Page
16.1.1	**Whitelist** **Blacklist** **Group**	Regulating User’s Access to Specific Websites Using Blacklist and Whitelist	**571**
16.1.2	**Category** **File Extensions** **MIME/Script** **Group**	Regulating User’s access to Specific Website, Downloading or Uploading Specific File Extension via HTTP or FTP or the Access to Specific MIME Types/ Script Types	**577**

16.1.1 Regulating User's Access to Specific Websites Using

Blacklist and Whitelist

Step 1. Go to **Web Filter** > **Configuration** > **Whitelist** and then set as below:

- Click **New Entry**.
- Type the name in the **Name** field.
- In the **URL** field, type the keyword of the URL, such as yahoo.
- Click **OK.**（**Figure 16-3**）
- Click **New Entry** again.
- Type the name in the **Name** field.
- In the **URL** fIield, type the keyword of URL, such as google.
- Click **OK**.（**Figure 16-4, 16-5**）

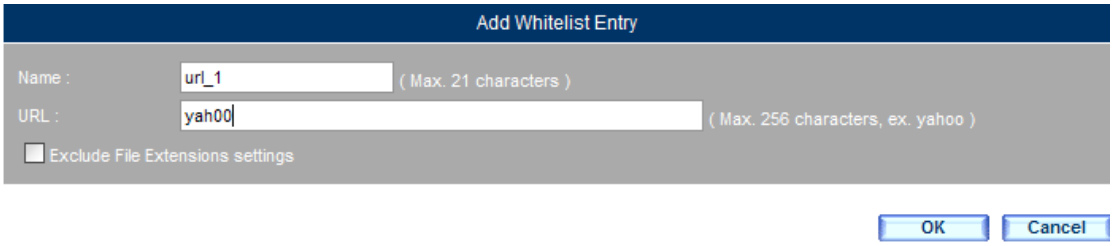


Figure 16-3 Configuring the First Rule of Whitelist

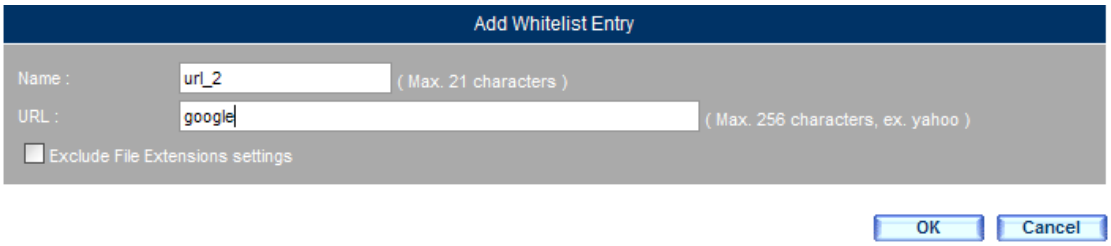


Figure 16-4 Configuring the Second Rule of Whitelist

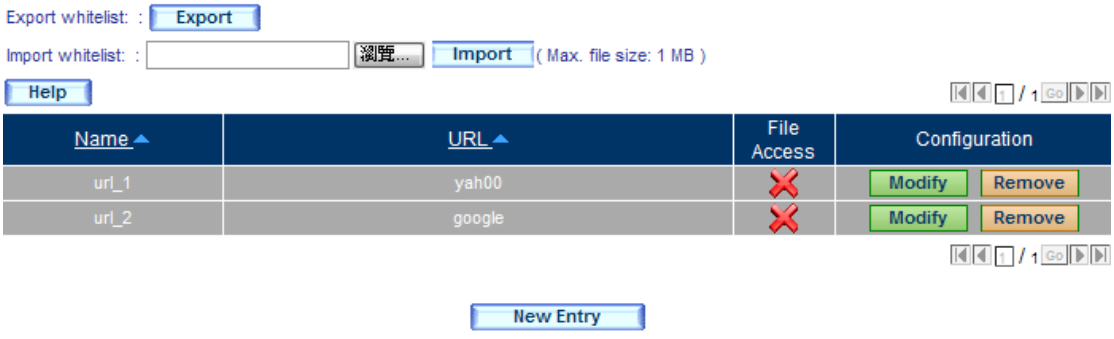


Figure 16-5 The Whitelist Completed

Note：

1. **Whitelist** can be exported as a file for storage, which can be used for restoring the list later on.

Step 2. Go to **Web Filter** > **Configuration** > **Blacklist** and then set as below:（**Figure 16-6**）

- Type the name in the **Name** field.
- In the **URL** field, enter *.
- Click **OK**.（**Figure 16-7**）

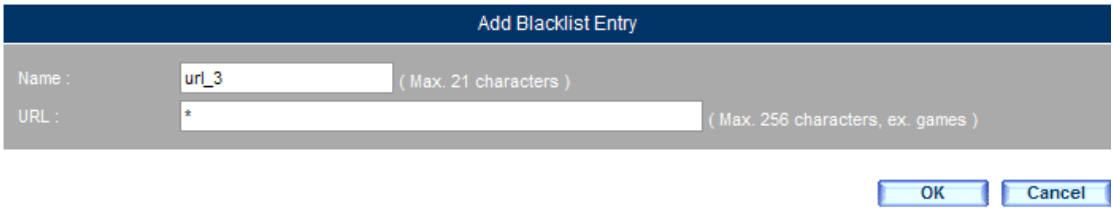


Figure 16-6 Configuring Blacklist

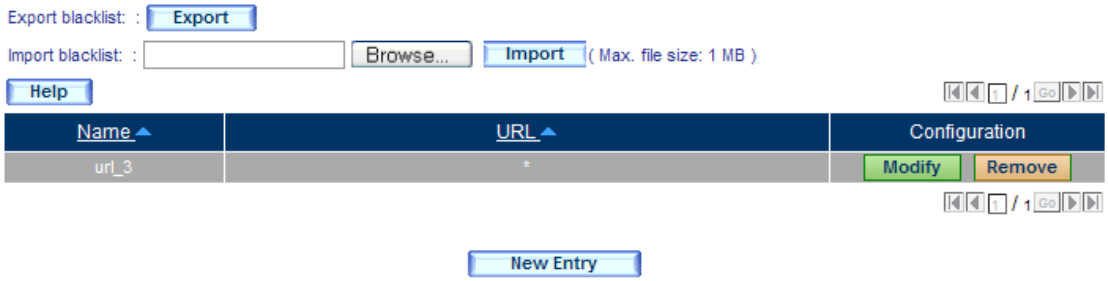


Figure 16-7 The Blacklist Completed

Note：

1. **Blacklist** can be exported as a file for storage, which can be used for restoring the list later on

Step 3. Go to **Web Filter** > **Configuration** > **Group**, click **New Entry** and then set as below:（**Figure 16-8**）

- Type the name in the **Name** field.
- Move the Whitelist from the **Available Whitelists** column to the **Selected Whitelists** column.
- Move the Blacklist from the **Available Blacklists** column to the **Selected Blacklists** column.
- Click **OK**.（**Figure 16-9**）

Figure 16-8 Group Settings for URL Blocking

Figure 16-9 The Completed Group Settings

Step 4. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below: (**Figure 16-10**)

- Select the defined group from the **Web Filter** drop-down list.
- Click **OK**. (**Figure 16-11**)
- By applying this policy, only websites containing “yahoo” or “google” in the domain name will be permitted.

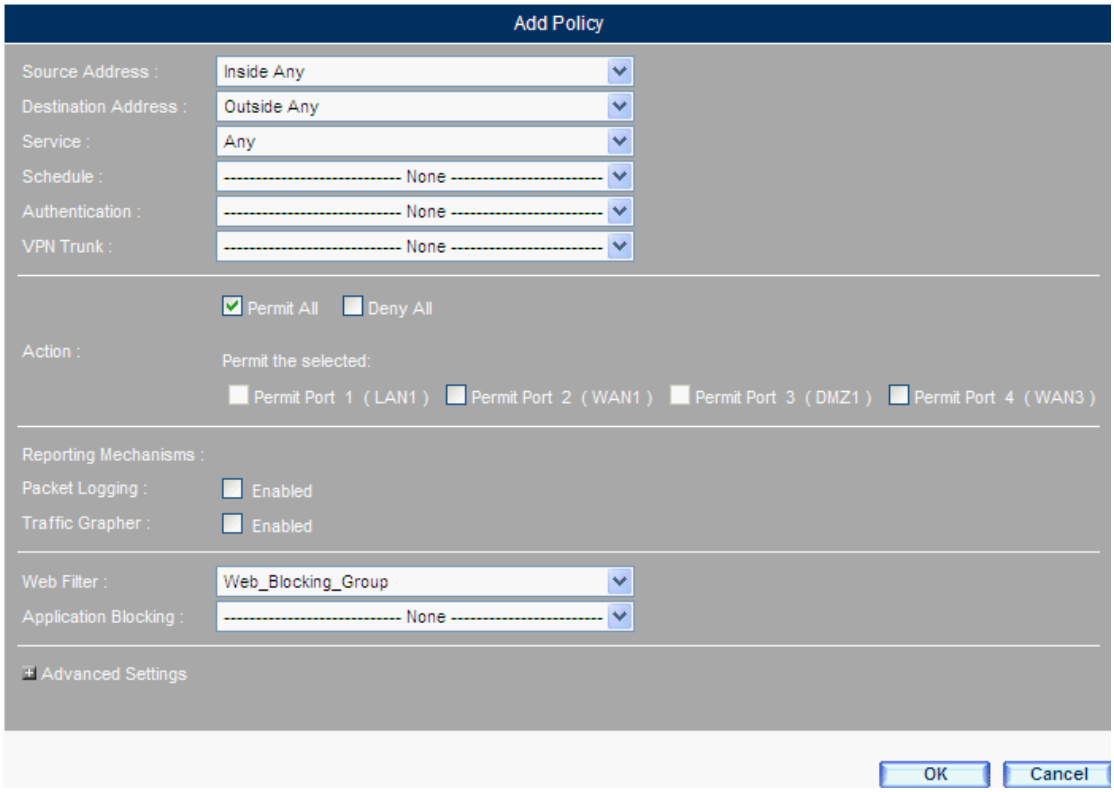


Figure 16-10 Policy Setting for URL Blocking

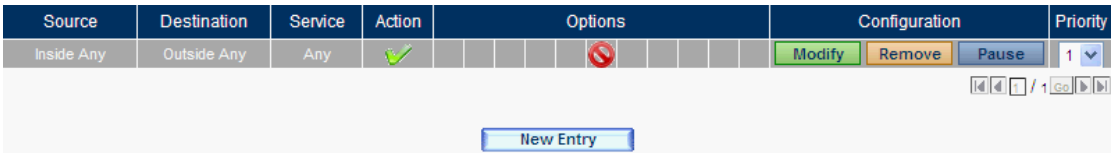


Figure 16-11 Policy Created

16.1.2 Regulating User's access to Specific Website, Downloading or Uploading Specific File Extension via HTTP or FTP or the Access to Specific MIME Types/ Script Types

Step 1. Go to **Web Filter** > **Configuration** > **Category**, click **New Entry** and then set as below: (**Figure 16-12**)

- Type the name in the **Name** field.
- Select the category, such as **Anti-Social and Illegal**, **Pornographic and Abusive**, **Gaming and Gambling.**
- Click **OK**. (**Figure 16-13**)

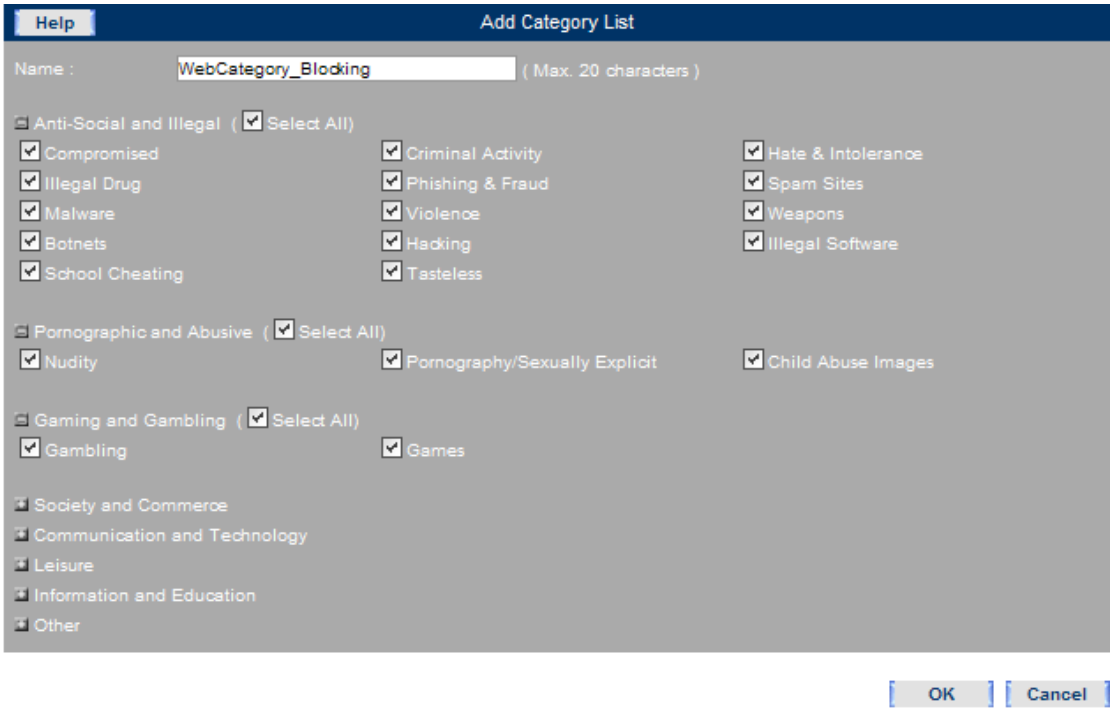


Figure 16-12 Category Blocking Settings

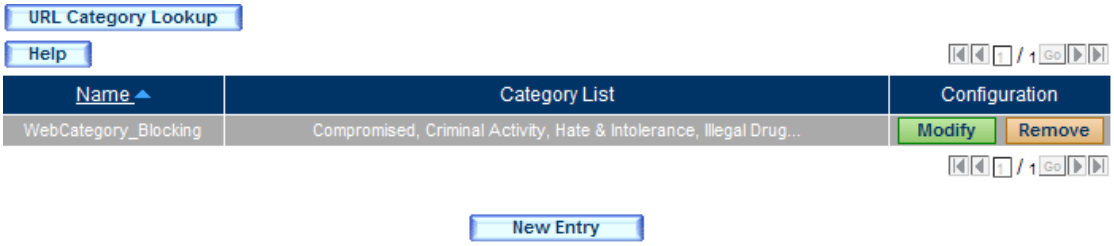


Figure 16-13 The Completed Category Settings

Step 2. Go to **Web Filter > Configuration > File Extensions**, click **New Entry** and then set as below:（**Figure 16-14**）

- Type the name in the **Name** field.
- Select **All types of file extensions.**
- Click **OK**.（**Figure 16-15**）

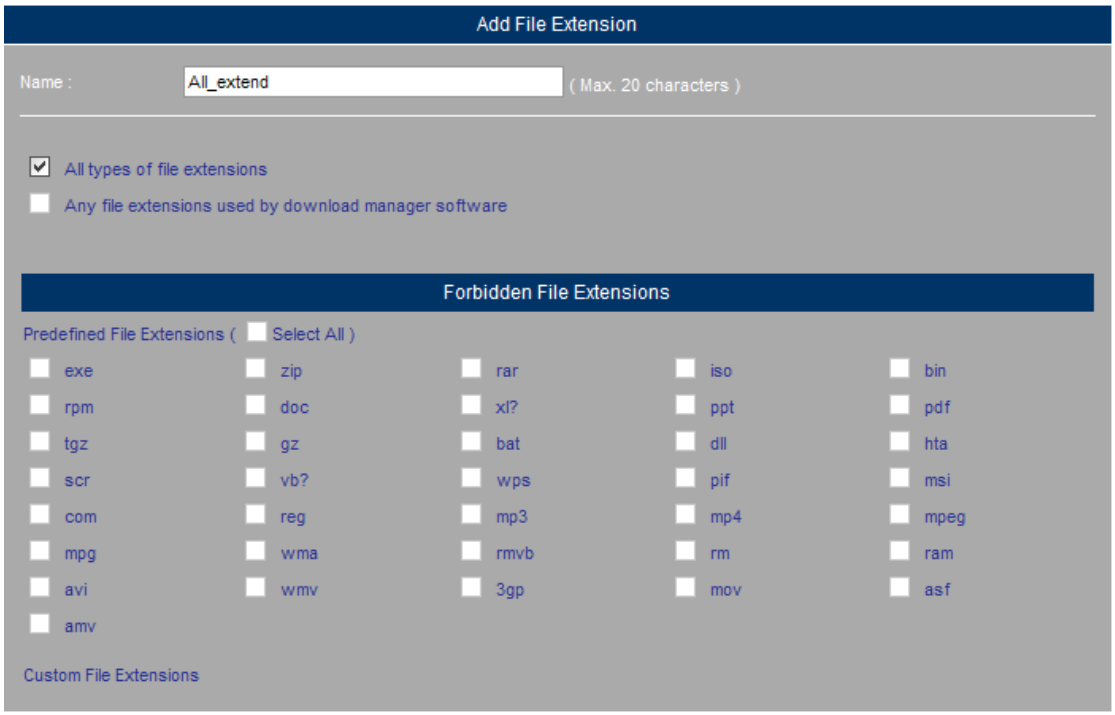


Figure 16-14 Blocking the Specific File Extension

Figure 16-15 Setting Completed

Note：

1. Under **Web Filter > Configuration > File Extensions**, the user may add the extension to be blocked:
   - Click **Modify** and then click **New Entry.**（**Figure 16-16**）
   - Type the extenstion in the field.
   - Click **OK**.（**Figure 16-17, 16-18**）

Figure 16-16 Adding a New Extension

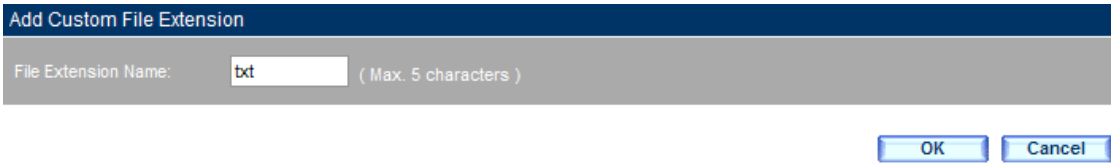


Figure 16-17 Typing a New Extension

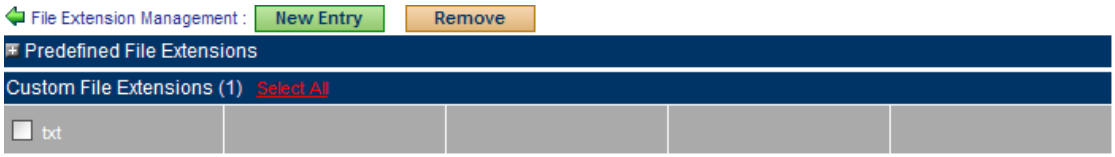


Figure 16-18 File Extension Added

Step 3. Go to **Web Filter > Configuration > MIME/Script**, click **New Entry** and then set as below:（**Figure 16-19**）

- Type the name in the **Name** field.
- Under the **Forbidden File Extensions** section, tick **Window Popup**, **Microsoft ActiveX**, **Java Applet** and **Web Cookie.**
- Move the MIME type from the **Available MIME Types** column to the **Selected MIME Types** column.
- Click **OK.**（**Figure 16-20**）

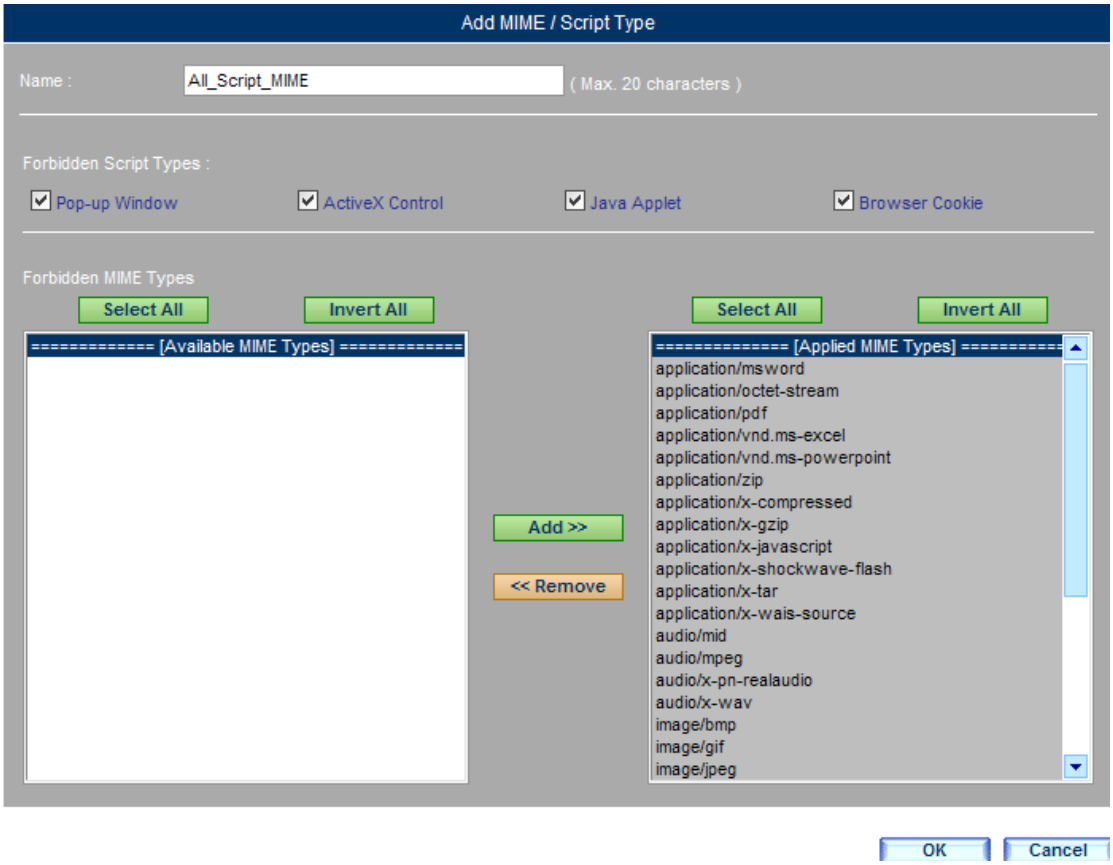


Figure 16-19 Configuring the MIME/Script

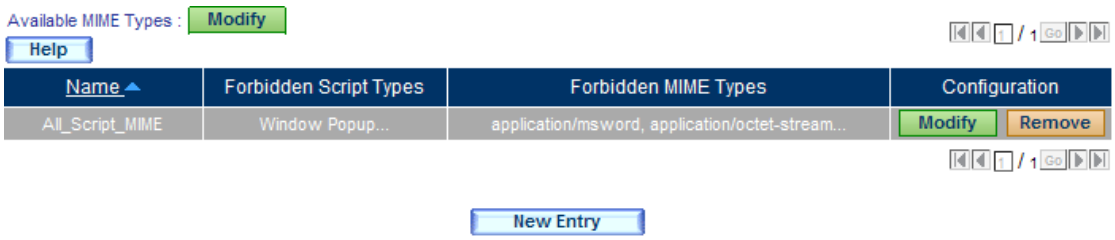


Figure 16-20 MIME/Script Setting Completed

Note：

1. Under **Web Filter > Configuration > MIME/ Script**, users may configure the MIME Type to be blocked:

- Click **Modify** and then click **Add.**（**Figure 16-21**）
- Enter the **MIME Types** in the field.
- Click **OK.**（**Figure 16-22, 16-23**）

Figure 16-21 Configuring the MIME Type

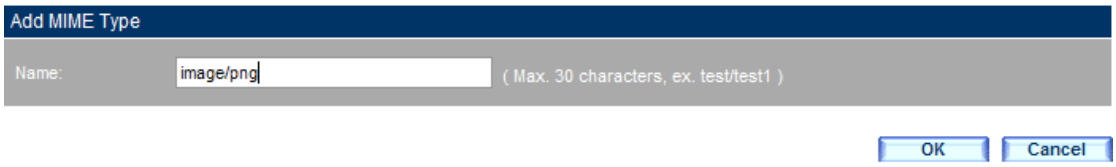


Figure 16-22 Adding the MIME Types

Figure 16-23 MIME Type Added

Step 4. Go to **Web Filter** > **Configuration** > **Group**, click **New Entry** and then set as below:（**Figure 16-24**）

- Type the name in the **Name** field.
- Select the defined category from the **Category** drop-down list.
- Select the defined rule from the **Upload Blocking** drop-down list and the **Download Blocking** drop-down list.
- Select the defined rule from the **MIME/Script** drop-down list.
- Click **OK**.（**Figure 16-25**）

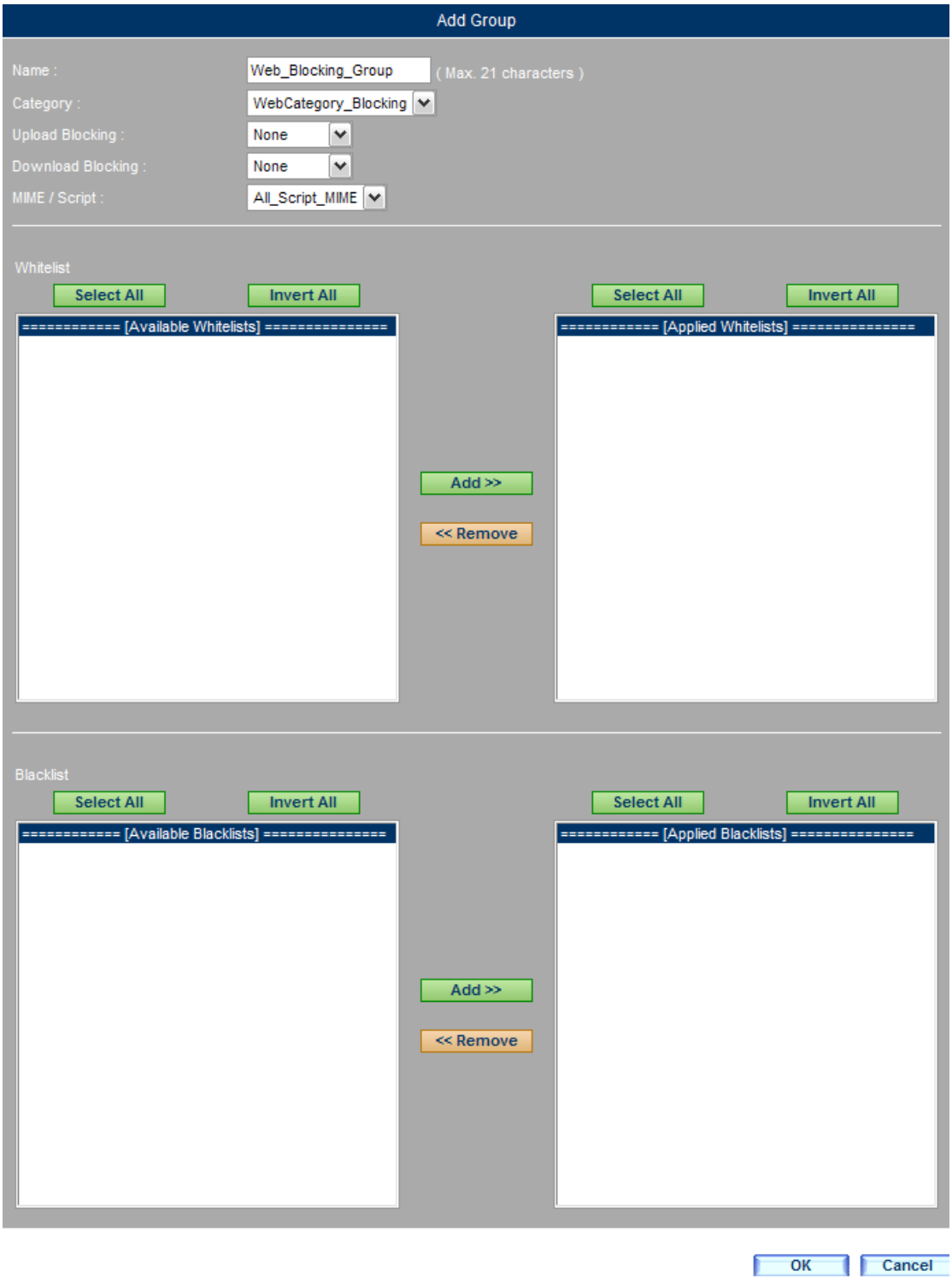


Figure 16-24 Configuring the URL Group

Figure 16-25 Setting Completed

Step 5. Go to **Policy** > **Outgoing**, click **New Entry** and then set as below: (**Figure 16-26**)

- Select the defined group from the **Web Filter** drop-down list.
- Click **OK.** (**Figure 16-27**)

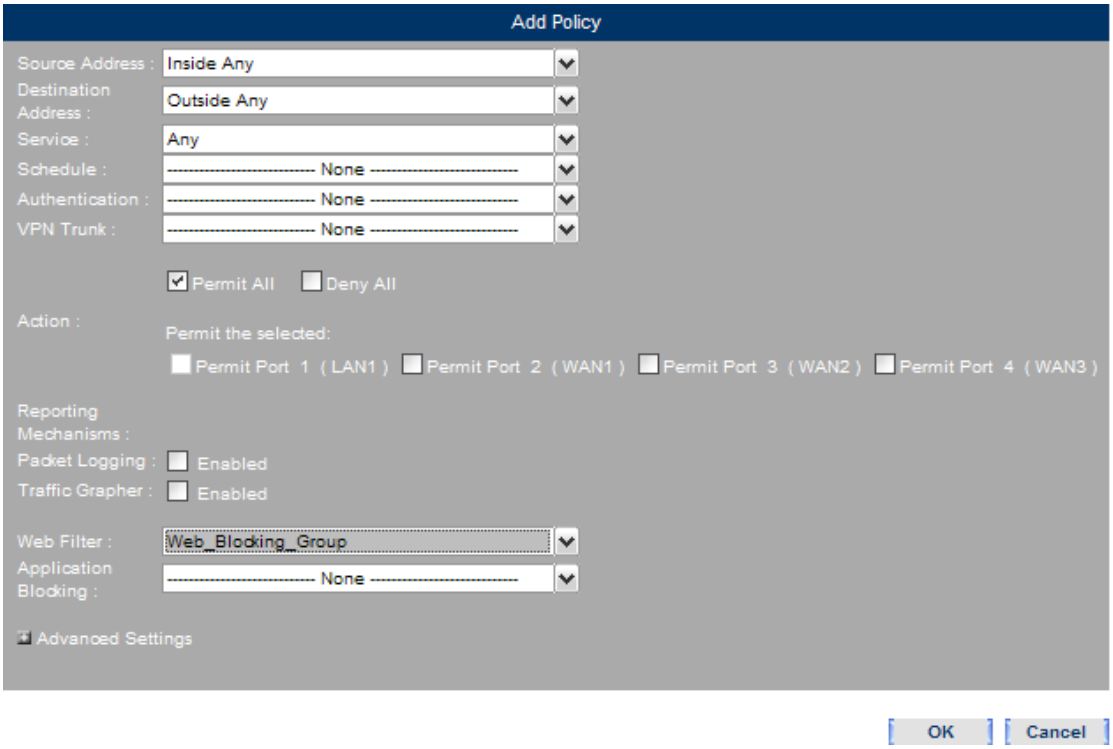


Figure 16-26 Configuring the Policy

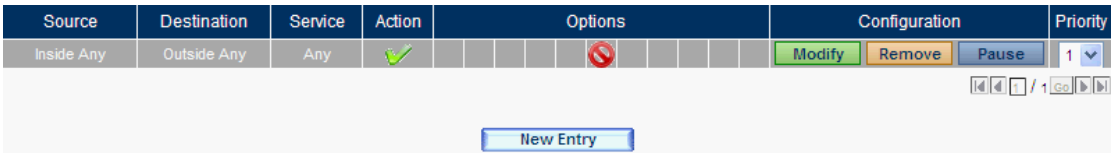


Figure 16-27 Policy Completed

Chapter 17 Reports

Reports delivers the IT administrator with detailed statistics and logs regarding the access of websites made by users.

Terms in Setting

Periodic Report Scheduling Settings

- Generates and sends out a periodic report to the designated recipient(s) based on a schedule.

History Report Retrieving Settings

- Generates the report of a specific date and instantly sends it to the designated recipient(s).
  - Go to **Syetem > Configuration > Settings** to enable **email notification** and configure its related settings. And then refer to the following to adjust settings under **Web Filter > Reports > Settings:**
    - Under the **Periodic Report** section, tick **Enable the mailing of Periodic Report** and then select **Yearly report**, **Monthly report**, **Weekly report** and **Daily report.**
    - Click **OK**.（**Figure 17-1**）
    - The recipient will receive the reports based upon the schedule.（**Figure 17-2**）

Note:

1. Schedule for periodic report:

- **Yearly report** is produced at 00:00 hours on January 1st of every year.
- **Monthly report** is produced at 00:00 hours on the first day of every month.
- **Weekly report** is produced at 00:00 hours on the first day of every week.
- **Daily report** is produced at 00:00 hours every day.

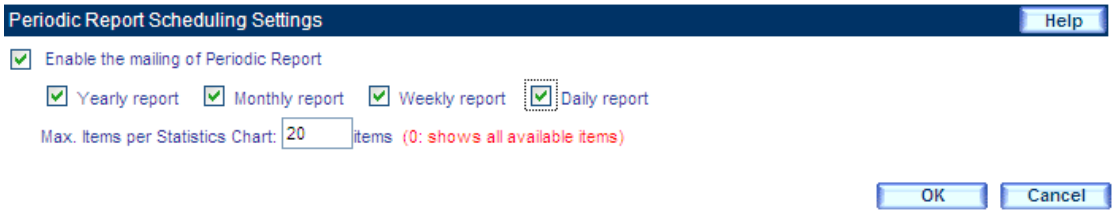


Figure 17-1 Periodic Report Settings

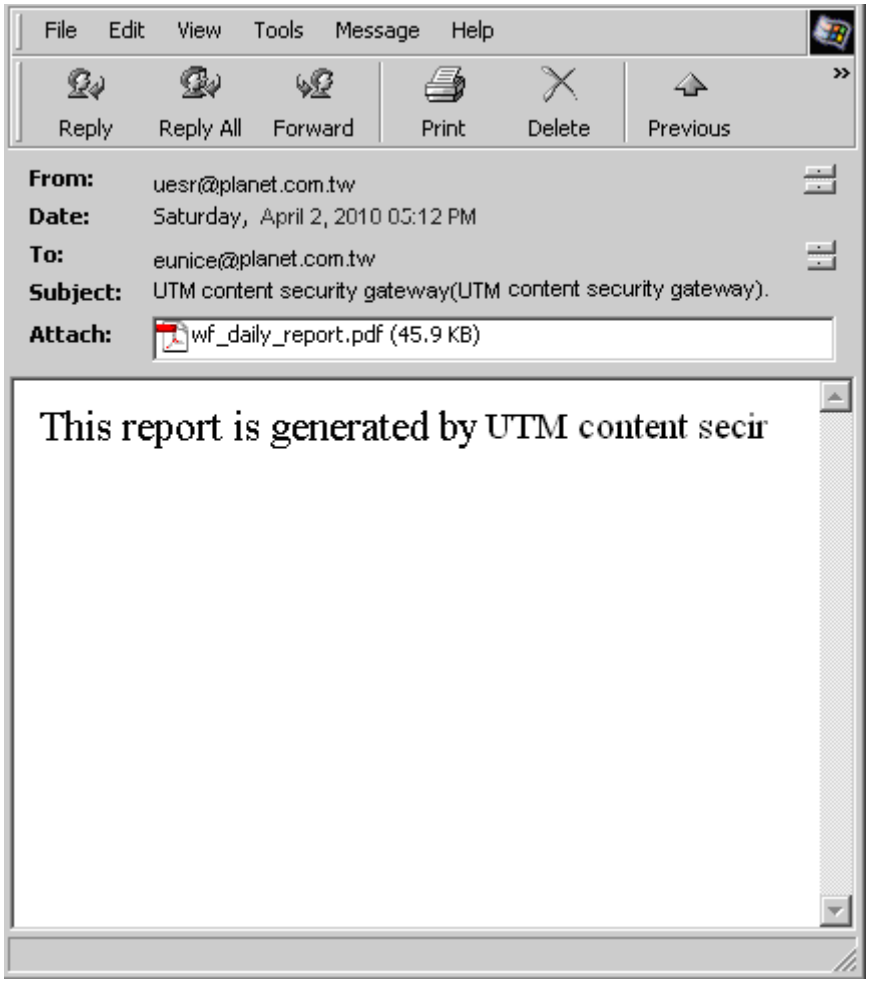


Figure 17-2 A Daily Report Sent through an Email Message

Terms in Logs

Search

- Category: Available searching criteria are time, souce IP address, website, classification and action.
- Upload: Available searching criteria are time, source IP addrss, website, file, rule and action.
- Download: Available searching criteria are time, source IP address, website, file, rule and action.
- MIME/Script: Available searching criteria are time, source IP address, website, rule and action.
  - Go to **Web Filter > Reports > Logs**, click the **Search** icon to start a search:
    - Enable the searching duration and specify a period of time to search within.
    - Select All for **Category**.
    - Select All for **Status**.
    - Click **Search**.（**Figure 17-3**）
    - Click **Download** to store the result.

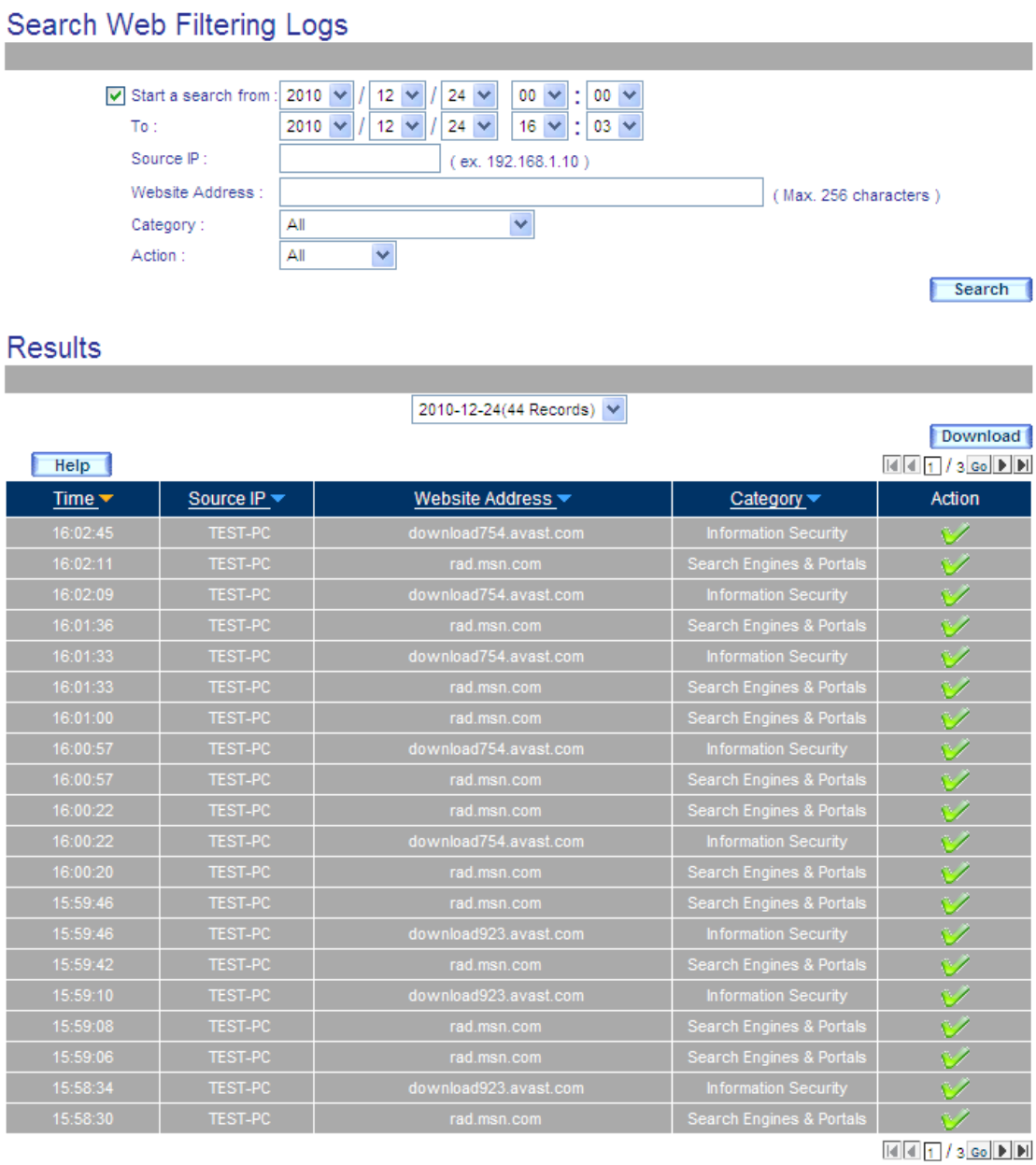


Figure 17-13 Searching for the Specific Logs

Note:

1. Under **Web Filter > Reports > Logs**, the Category reports can be sorted by the time, source IP, website, class or action.
2. Under **Web Filter > Reports > Logs**, the download and the upload report can be sorted by the time, source IP, website, class and action.
3. Under **Web Filter > Reports > Logs**, the MIME/Script report can be sorted by time, source IP, website, rule and action.

17.1 Statistics

Step 1. Under **Web Filter** > **Reports** > **Statistics**, bar charts shows the report of URL blocking.

Step 2. In the upper left corner, click on a time reference from which to display the bar charts. Click on **Day** for bar charts derived from daily statistics; click on **Week** for bar charts derived from weekly statistics; click on **Month** for bar charts derived from monthly statistics; click on **Year** for bar charts derived from yearly statistics.

Step 3. You can see the reports of the specific date by select the date from the **Date** drop-down list or you can see the reports organized by the specific type by select the type from the **Type** drop-down list.

Step 4. Below it shows the statistics report. (**Figure 17-15**)

- Y-axis indicates the amount of scanned URL.
- X-axis indicates the time.

Year | Month | Week | Day Date : 2010-12-24 Chart : Website Category

Website Category Top Chart Blocked Allowed Download 1 / 1

No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Information Security	0	40	40	40
2	Unknown	0	17	17	17
3	Search Engines & Portals	0	16	16	16
4	General	0	1	1	1
5	Computers & Technology	0	1	1	1
6	Web-based Email	0	1	1	1

Duration: **2010/12/24 00:00 ~ 2010/12/24 16:21** Total: **76** Average: **4.47 URLs/Hour**

1 / 1

Website Address Top Chart Blocked Allowed Download 1 / 2

No.	Website Address	Blocked	Allowed	Total	Access Indicator
1	rad.msn.com	0	15	15	15
2	ll002.avast.com	0	6	6	6
3	download789.avast.com	0	5	5	5
4	download754.avast.com	0	5	5	5
5	download662.avast.com	0	5	5	5
6	download728.avast.com	0	5	5	5
7	download923.avast.com	0	5	5	5
8	download516.avast.com	0	5	5	5
9	download667.avast.com	0	5	5	5
10	www.msftncsi.com	0	2	2	2
11	tw.news.yahoo.com	0	2	2	2
12	l.yimg.com	0	2	2	2
13	tools.google.com	0	1	1	1
14	sup.live.com	0	1	1	1
15	byfiles.storage.msn.com	0	1	1	1
16	207.46.125.52	0	1	1	1
17	207.46.124.166	0	1	1	1
18	www.google.com.tw	0	1	1	1
19	tw.yahoo.com	0	1	1	1
20	login.live.com	0	1	1	1

Duration: **2010/12/24 00:00 ~ 2010/12/24 16:21** Total: **76** Average: **4.47 URLs/Hour**

1 / 2

NetBIOS Name / IP Address Top Chart Blocked Allowed Download 1 / 1

No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
1	TEST-PC	0	69	69	69
2	ENMLAB-PC	0	7	7	7

Duration: **2010/12/24 00:00 ~ 2010/12/24 16:21** Total: **76** Average: **4.47 URLs/Hour**

1 / 1

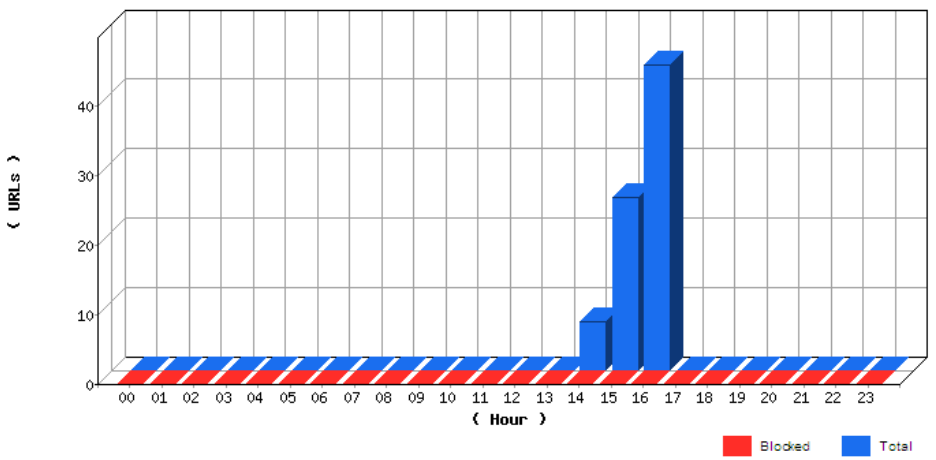


Figure 17-15 Statistics Report

17.2 Logs

Step 1. Under **Web Filter** > **Reports** > **Logs**, there it shows the URL blocking logs. （**Figure 17-16**）

Figure 17-16 URL Blocking Logs

IDP

Chapter 18 Configuration

In order to protect your network from various security threats, the device produces timely alerts and blocking mechanisms based upon anomaly flows and the inspection of packet contents.

Terms in Settings

IDP Settings

- IDP signature definitions update automatically everyday or updated by the IT administrator manually. After each update, it shows the latest updated time and current version number.
- IDP mechanism can perform a virus scanning on compressed and unencrypted files.
- Scanning engine:
  - ClamAV: The default and free of charge virus scanning engine.
- The device can perform a complete scanning on every single packet.
- The device can be configured
- Security is divided into 3 levels : High Risk, Medium Risk and Low Risk. Action taken to each level can be: Pass, Drop, Log or Alert.

Note:

1. To ensure signature definitions can be updated successfully, click on Test Connection to check the connection to the designated IDP definition server.
2. Once the Proxy Server is deployed, the proxy settings under **System > Configuration > Settings** must be configured for the CS-2001 to access the Internet.

IDP Logging Setting

- Configures the storage time of the IDP logs and deletes the logs when the time is expired.
- Store the IDP logs in the remote server.
  - Go to **System > Configuration > Settings**, configure the settings under the **Email Notification Settings** section and then go to **IDP > Configuration > Settings** and set as below:
    - Tick **Enable virus scanning.**
    - Tick **Enable Deep Packet Inspection (IDP).**
    - Tick **Enable NetBIOS Notification** and then type the **Administrator's IP Address.**
    - In the **High Risk** row, select **Drop** and tick **Log** and **Alert.**
    - In the **Medium Risk** row, select **Drop** and tick **Log** and **Alert.**
    - In the **Low Risk** row, select **Pass** and tick **Log** and **Alert.**

- Type 60 in the **Storage Lifetime** field.
- Click **OK**.（**Figure 18-1**）

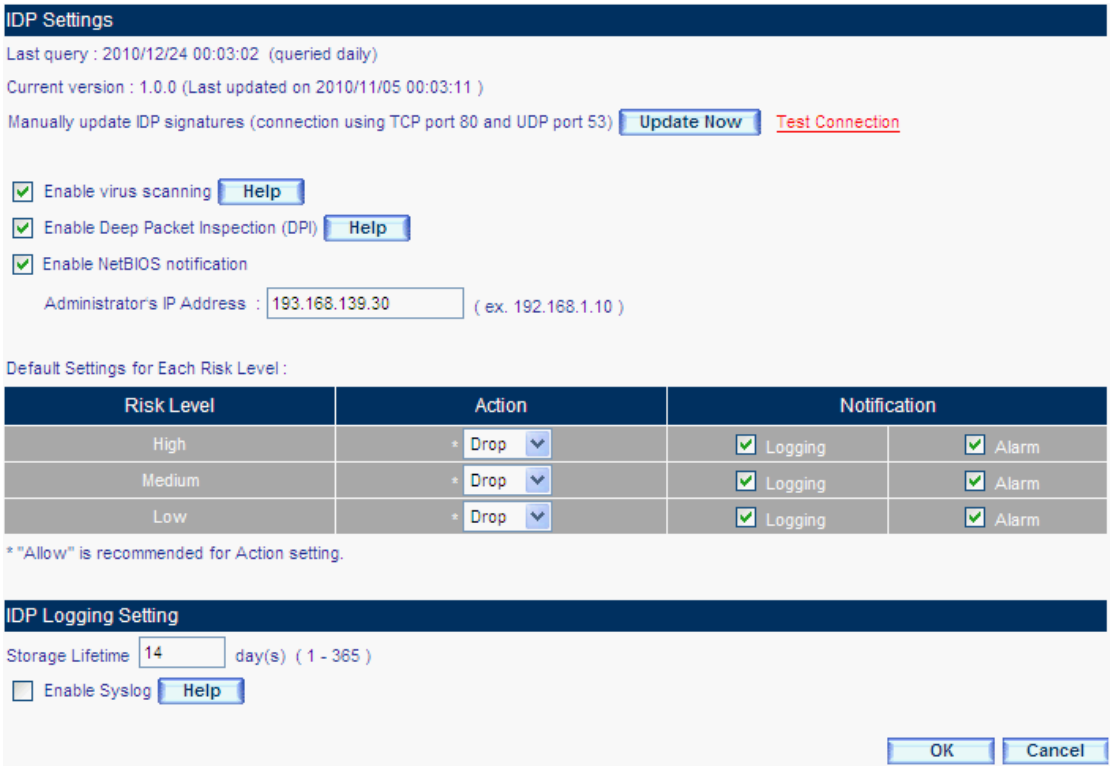


Figure 18-1 IDP Settings

Note:

1. To enable Syslog, the IT administrator must configure the **Syslog Message Settings** under **System > Configuration > Settings** first.

- When detecting attacks, the IT administrator will receive both an email notification and a NetBIOS Notification, Also, a corresponding log will be available under **IDP > IDP Reports > Logs**.（**Figure 18-2, 18-3**）

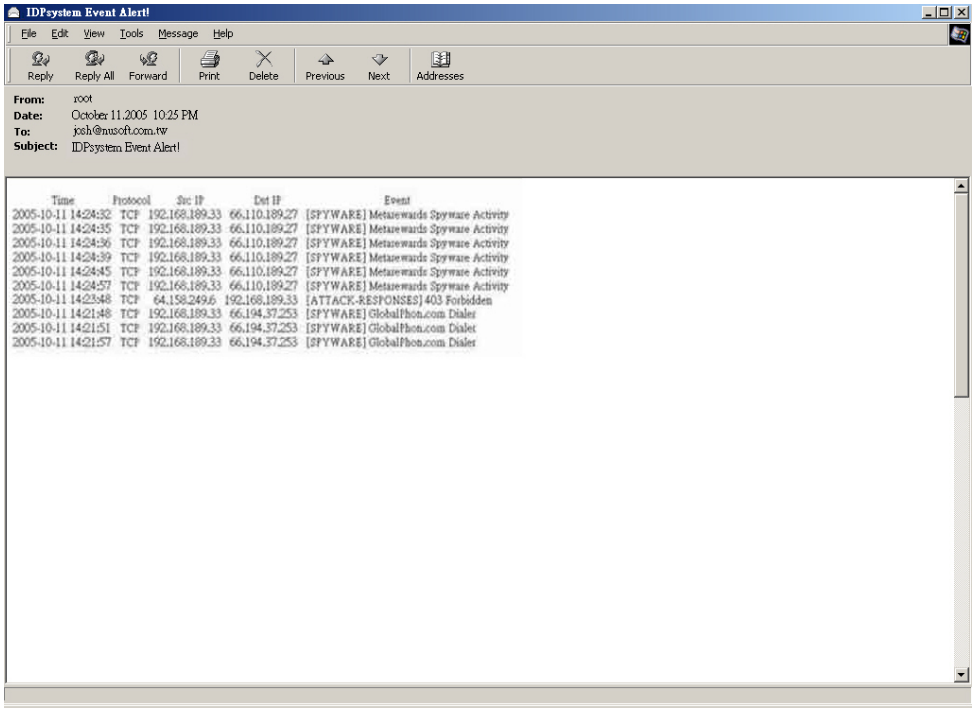


Figure 18-2 An Email Notification

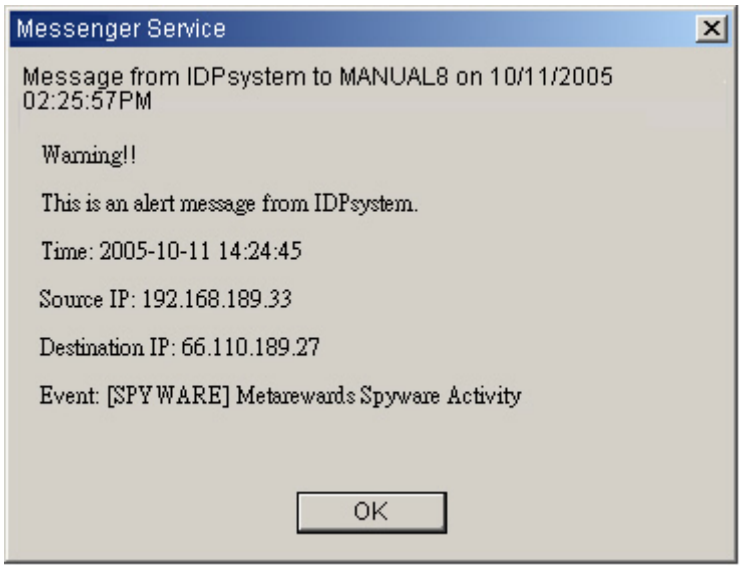


Figure 18-3 A NetBIOS Notification

Note:

1. The IDP log is generated upon the “Log”setting under **IDP** > **Signatures** > **Anomaly** / **Pre-defined** / **Custom**.

Chapter 19 Signatures

To protect your company's network from malicious intrusions and attacks, the CS-2001 provides alerts and blocking mechanisms based upon the inspection of packets and the detection of anomaly traffic flows. Regardless of whether the attack originated internally or externally, the device ensures that legitimate network traffic remains secure and undisturbed.

To deal with different forms of attacks, three types of signatures are provided:

- Anomaly: Detects suspicious packets and anomaly flows based upon definitions from the latest signature file version.
- Pre-defined: Detects suspicious packets and anomaly flows based upon pre-defined definitions from the latest signature file version.
- Custom: Allows the IT administrator to define signatures based on specific customizable criteria.

Terms in Signatures

Anomaly

- Available signatures are syn flood, udp flood, icmp flood, portscan and http insptct.（**Figure 19-1**）
- You may specify the action taken upon the detection of an anomaly flow. Available actions are **Pass**, **Drop** and **Reject**. Available Alert are **Log** and **Alert.**

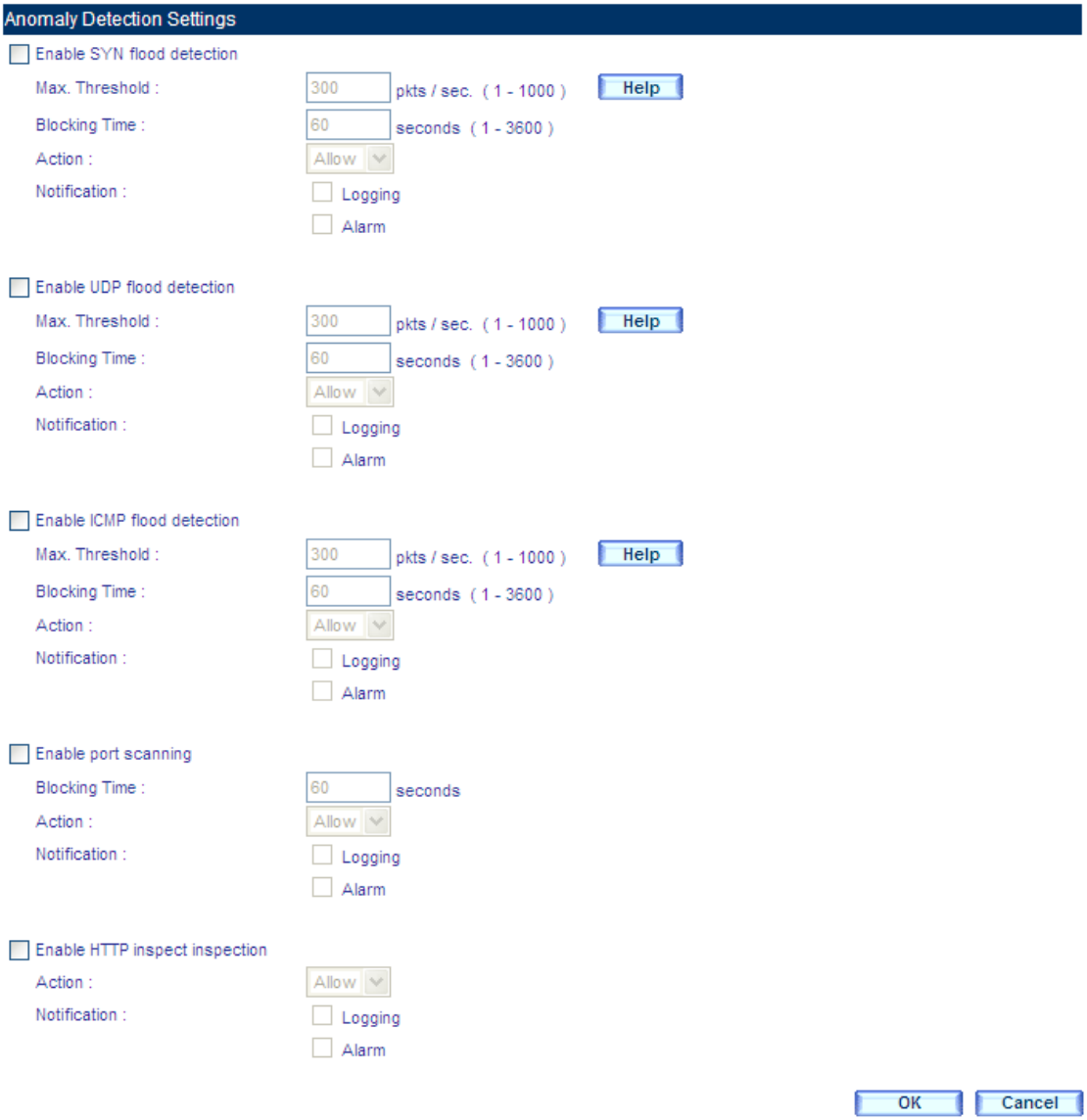


Figure 19-1 Anomaly Settings

Pre-defined

- Available signatures are Attack Responses, Backdoor, Bad Traffic, Chat, DDoS, DNS, DoS, Exploit, Finger, FTP, ICMP, IMAP, Info, Misc, MySQL, NetBIOS, NNTP, Oracle, Policy, POP2, POP3, Porn, RPC, Rservices, Scan, Shellcode, SMTP, SNMP, Spyware, SQL, Telnet, TFTP, Web CGI, Web Client, Web Coldfusion, Web Frontpage, Web IIS, Web Misc, Web PHP, X11 and other. **（Figure 19-2）**
- You may specify the action taken upon the detection of an anomaly flow. Available actions are **Pass**, **Drop**, **Reject**, **Log** and **Alert.**

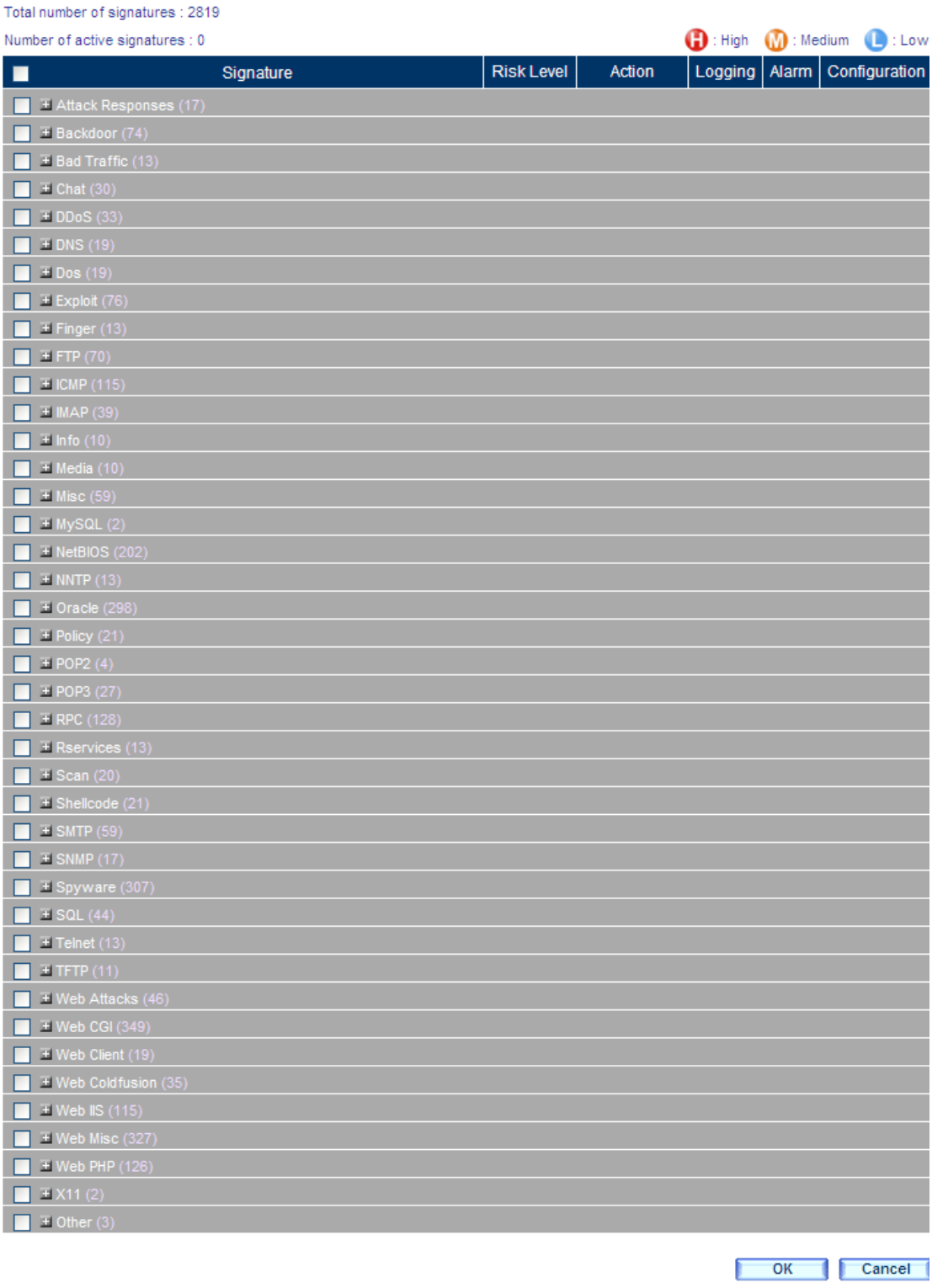


Figure 19-2 Pre-Defined Settings

Note:

1. All the signatures under the **IDP > Signatures > Pre-defined** are processed according to the **Default Settings for Each Risk Level** settings under **IDP > Configuration > Settings**. However, after the settings under **IDP > Configuration > Settings**, the user may go to **IDP > Signatures > Pre-defined** to modify the process of each signature individually.

Name

- The name of the signature.

Protocol

- Determine of which IP Version (IPv4, IPv6) and Communication Protocol to detect and protect.

Source IP / Netmask

- The IP address/ netmask where the attack is from.

Source Port

- The port number where the attack is from. (range : 0-65535)

Destination IP / Netmask

- The IP address of the victim.

Destination Port

- The port number of the victim. (Range 0-65535)

Risk Level

- Define the risk level.

Process

- Determines the action to take against hostile packets.

Action

- Generates the logs and sends the alert to the IT administrator.

Option

- Determines the detection according to the packet’s direction.
- Determines the detection according to the packet’s text case.

Content

- Specifies the contents of packets deemed to be hostile.

19.1 Example

19.1.1 Adopting Packets Inspection along with Custom and

Pre-Defined Signatures to Detect and Prevent the Intrusion

Step 1. Under **IDP > Configuration > Settings**, set as below: (**Figure 19-3**)

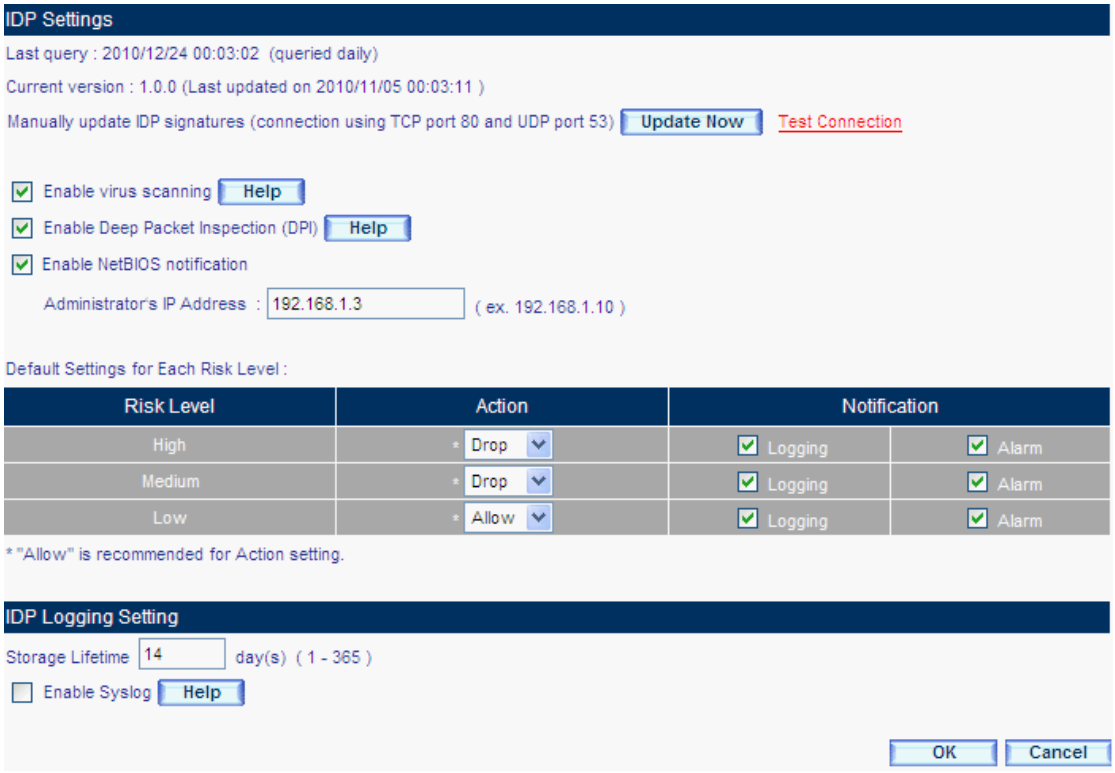


Figure 19-3 IDP Settings

Step 2. Go to **IDP > Signatures > Anomaly** and then set as below:（**Figure 19-4**）

- Enable the signatures and configure the settings.
- Click **OK.**

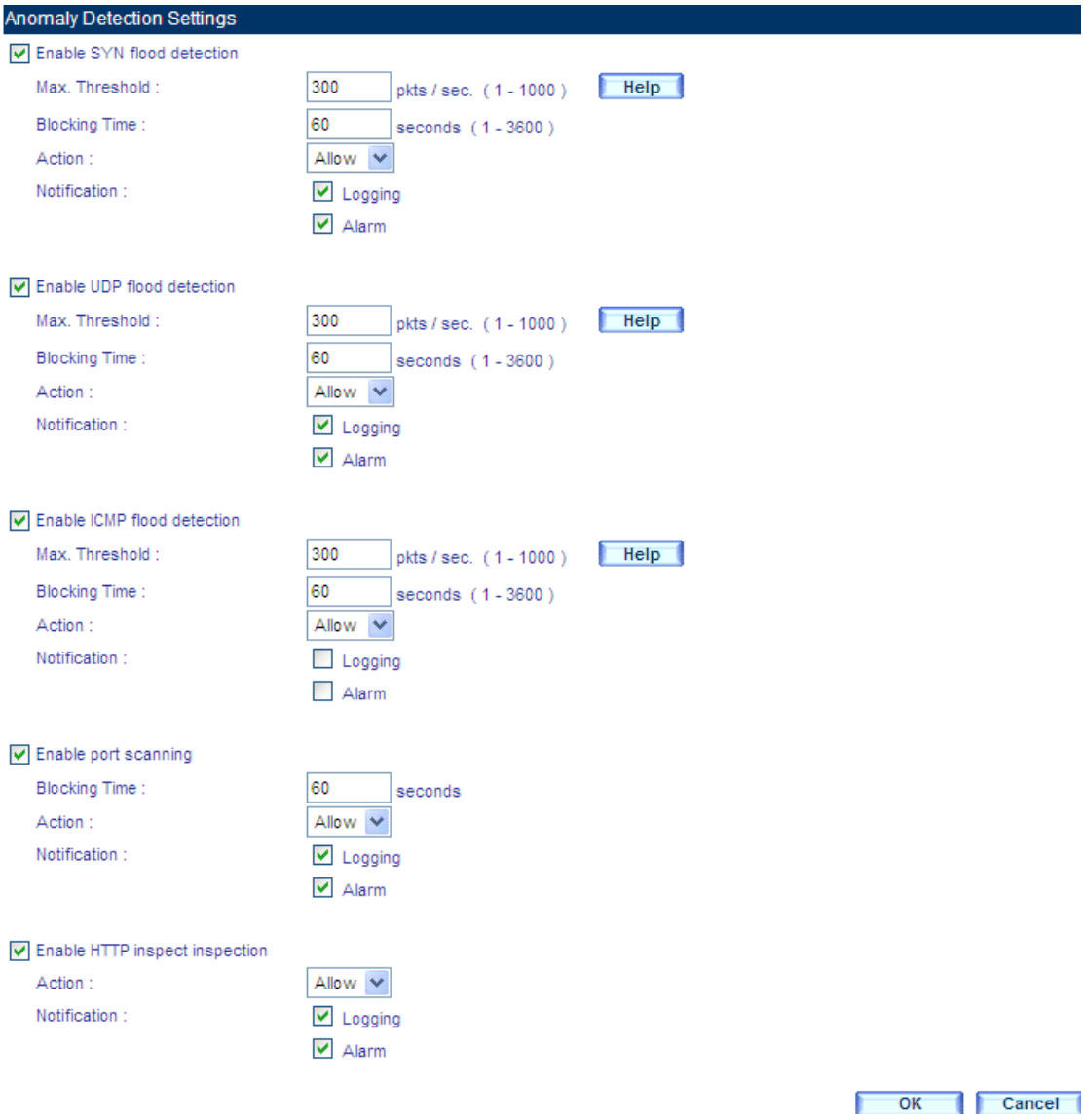


Figure 19-4 Anomaly Settings

Step 3. Under **IDP > Signatures > Pre-defined**, set as below: (**Figure 19-5**)

- Select the signatures.
- Click **OK.**

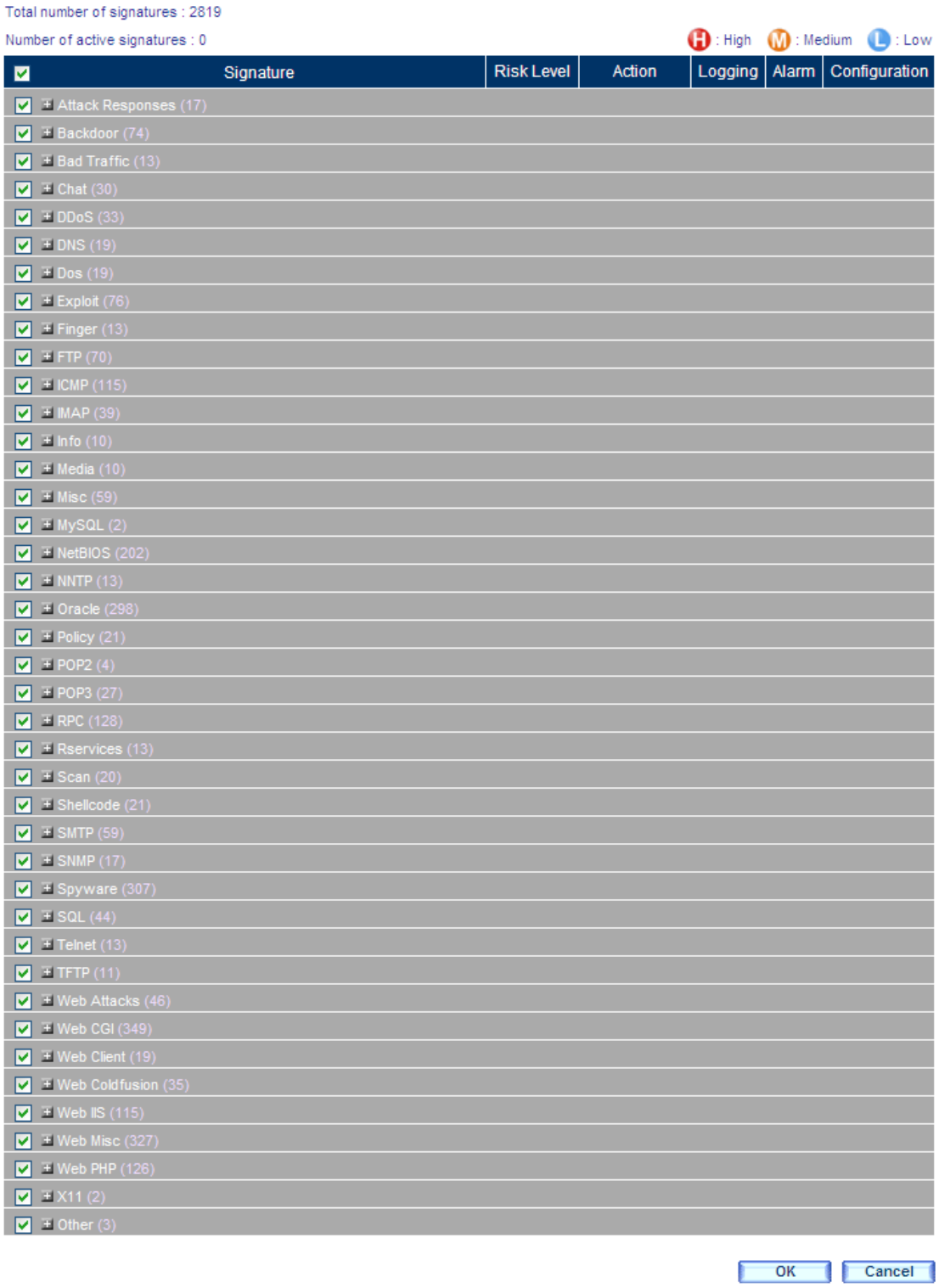


Figure 19-5 Pre-Defined Settings

Step 4. Go to **IDP** > **Signatures** > **Custom** and set as below:（**Figure 19-6**）

- Type the name in the **Name** field.
- Select IPv4 for **IP Version** and TCP for **Communication Protocol**.
- Type the **Source Port No**.
- Type the **Destination Port No**.
- Select High for **Risk Level**.
- Select Drop for **Process**.
- Tick Log and Alert for **Action**.
- Tick **Ignore Packet direction** and **Ignore letter case** for **Advanced Options**.
- Type the content pattern in the field.
- Click **OK**.（**Figure 19-7**）

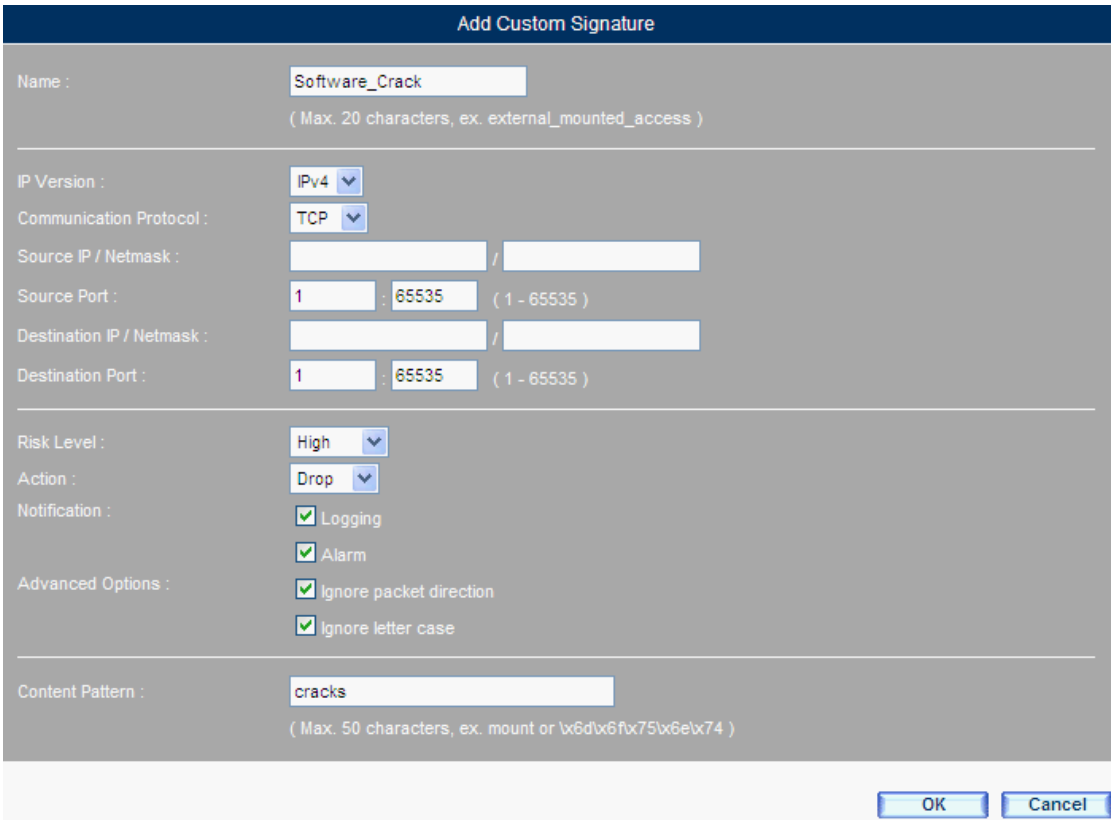


Figure 19-6 Custom Signature Settings

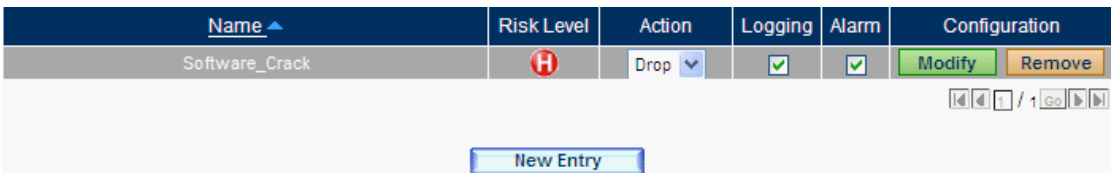


Figure 19-7 Custom Signature Completed

Note:

1. You may type a word string in the **Content Pattern** field; or convert it to hexadecimal ASCII code and then paste it into the field. (E.g., the word “cracks” can also be converted to |63 72 61 63 6b 73|)

Step 5. Go to **Policy** > **Outgoing** and set as below: (**Figure 19-8**)

- Select Enabled for **IDP**.
- Click **OK**. (**Figure 19-9**)

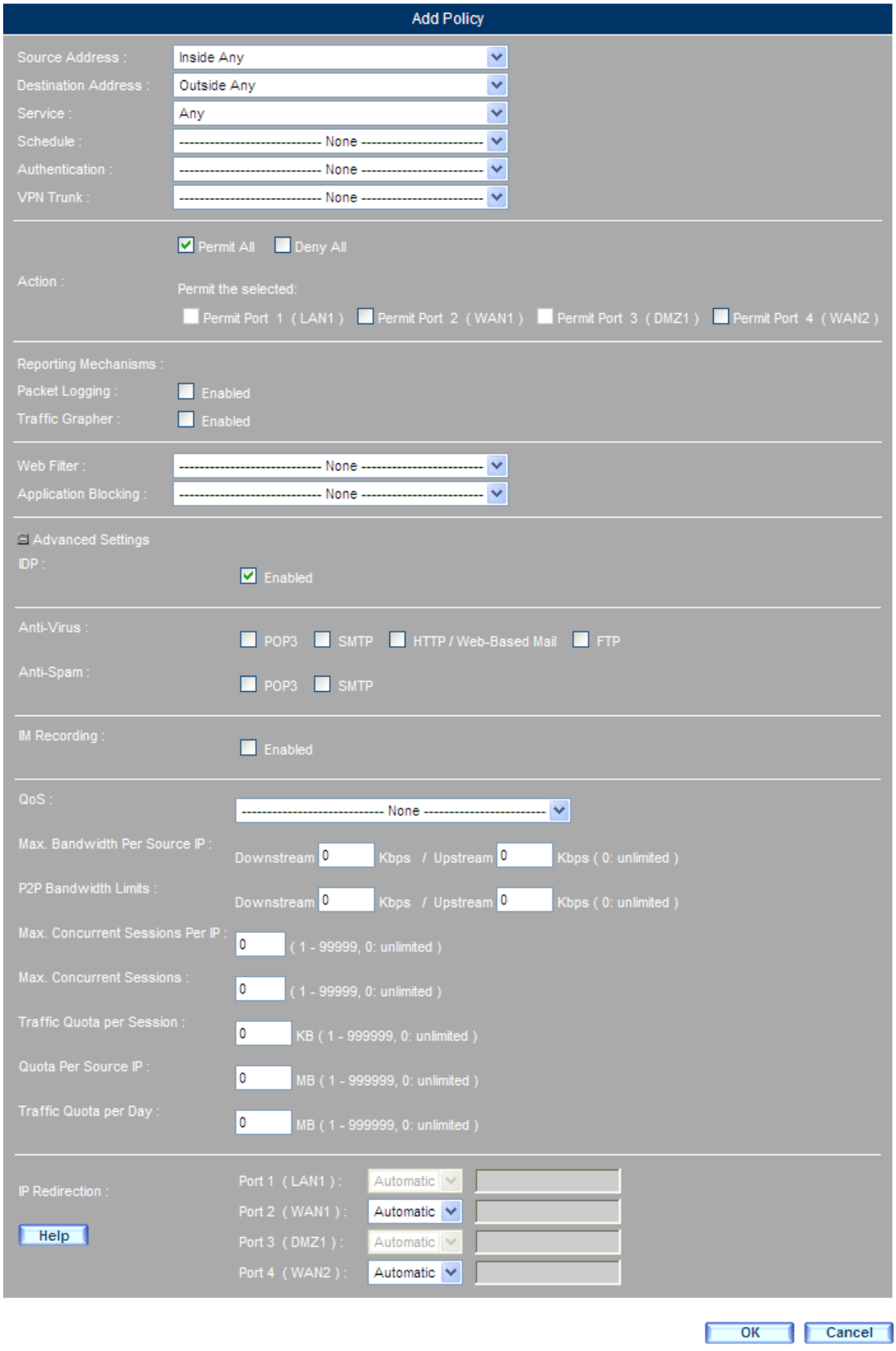


Figure 19-8 Applying the IDP to the Policy

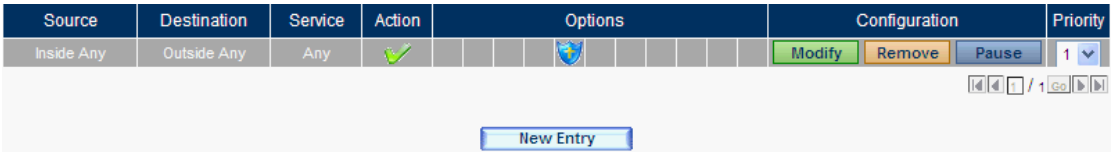


Figure 19-9 Policy Created

Chapter 20 IDP Report

CS-2001 provides you with a comprehensive IDP report in both statistics and logs. With the help of them, you could have a clear view of network security status.

Terms in Settings

Periodic Report Scheduling Settings

- It can generates and send out the periodic report to the designated recipient(s) on schedules.

History Report Scheduling Settings

- It can generates the report of a specific date and instantly send it to the designated recipient(s).
  - Go to **System > Configuration > Settings** to enable the **Email Notification** and configure its correlative settings. And then configure the settings under **IDP > IDP Report > Settings** as below:
    - Tick **Enable the mailing of Periodic Report** and then select **Yearly report**, **Monthly report**, **Weekly report** and **Daily Report**.
    - Click **OK**.（**Figure 20-1**）
    - The recipient will receive the reports based on the schedule.（**Figure 20-2**）

Note:

1. Schedule for periodic report:

- **Yearly report** is produced once a year at 00:00 hours on January 1.
- **Monthly report** is produced at 00:00 hours on the first day of every month.
- **Weekly report** is produced at 00:00 hours on the first day of every week.
- **Daily report** is produced at 00:00 hours of every day.

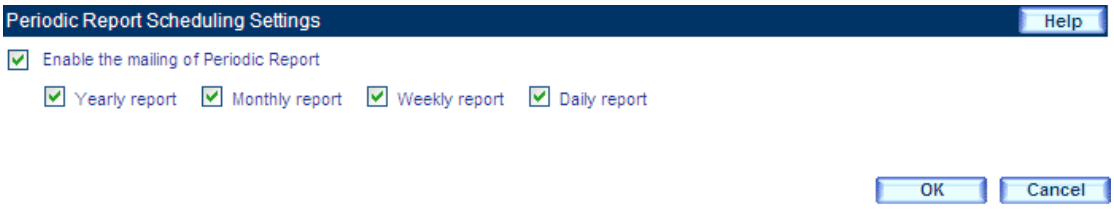


Figure 20-1 Periodic Report Settings

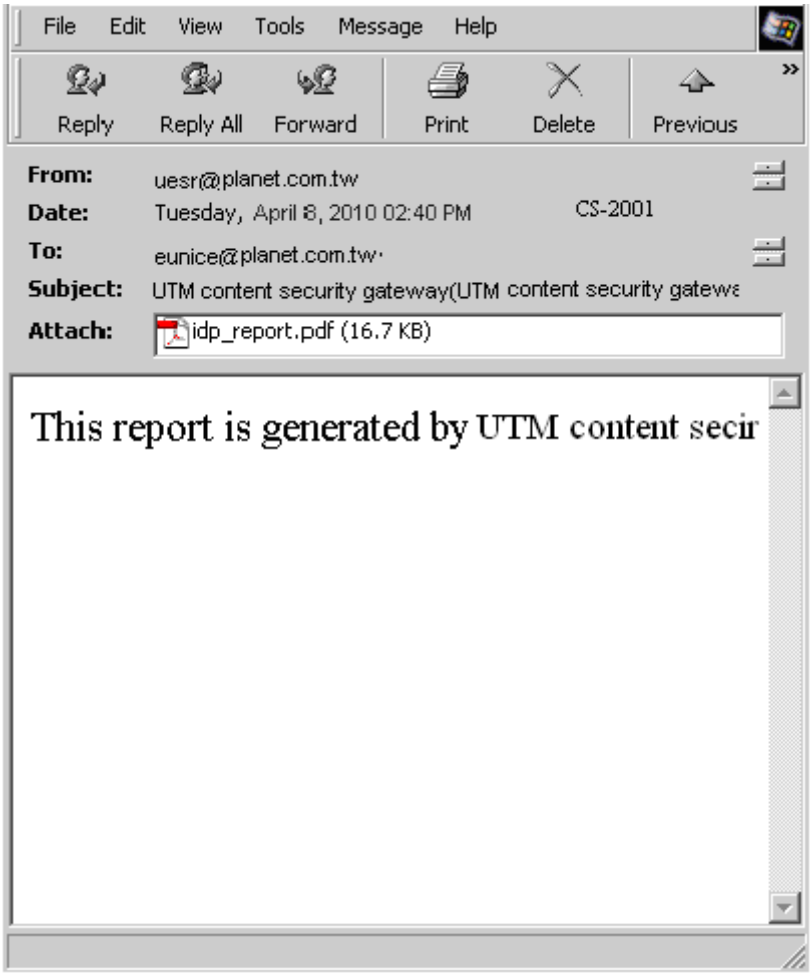


Figure 20-2 Periodic Report Received

Terms in Logs

Search

- Available search criteria are date, event, signature category, attacker IP, victim IP, interface and risk level.
  - Go to **IDP > IDP Reprots > Logs**, click the **Search** icon and then set as below:
    - Enable searching duration and specify a period of time.
    - Type a keyword from the attack event in the **Event** field.
    - Select All for **Interface.**
    - Select All for **Risk Level.**
    - Click **Search**.

Note:

1. Logs (**IDP > IDP Reports > Logs**) can be sorted by Time, Event, Interface, Aattacker IP, Victim IP or Action.

20.1 Statistics

Step 1. Go to **IDP** > **IDP Reports** > **Statistics**, to view a full-scale IDP report in statistics.

Step 2. In the upper left corner, click **Day** to see the daily statistics report, click **Week** to see the weekly statistics report, click **Month** to see the monthly statistics report, click **Year** to see the yearly statistics report.

20.2 Logs

Under **IDP > IDP Reports > Logs**, it shows the IDP status.

Note:

1. The symbol used in **Logs:**

- Process:

Symbol		
Description	Allow	Drop, Reject

- Risk Level:

Symbol			
Description	High Risk	Medium Risk	Low Risk

Web VPN / SSL VPN

Chapter 21 Web VPN / SSL VPN

Since the Internet is in widespread use these days, the demand for secure remote connections is increasing. To meet this demand, SSL VPN provides the best solution. By using SSL VPN from a standard browser, clients can transfer data securely through its SSL security protocol without the need to install any software or hardware.

Terms in VPN

DES

- DES, an acronym for Data Encryption Standard, is a cipher that was selected by NIST (National Institute of Standard and Technology), using a 56-bit key for encryption.

3DES

- 3DES, an acronym for Triple Data Encryption Standard, providing significantly enhanced security by executing the core DES algorithm three times in a row, is more difficult to break than DES, using a 168-bit key size.

AES

- AES, an acronym for Advanced Encryption Standard, is more difficult to break than DES. The DES encryption key is 56 bits long; on the contrary, AES keys can be 128, 192 or 256 bits long.

Terms in Settings

Web VPN / SSL VPN Client Configuration

- Configures the Protocol, Client IP address range, Encryption algorithm, Server port. Assigns DNS server addresses to clients or WINS server addresses to client.
- Set subnet of server that can be accessed by the client user.

Note：

1. The SSL VPN IP address range cannot overlap with the address range from any of the following internal network subnets or servers: LAN, DMZ, WAN, Multiple. Subnet, etc.

Name

- The name of the SSL VPN authentication.

Authentication Account / Group

- The authentication group and user under **Policy Object > Authentication > User / Group.**

Hardware Auth.

- The IT administrator may enable the PCs listed under **Web VPN/ SSL VPN > Hardware Auth** by adding them to the **Selected Hardware** column under **Web VPN / SSL VPN / Settings**.

Terms in Hardware Auth

Hardware Authentication Users

- The list of the devices that have been established SSL VPN connection to the CS-2001 device.

Note：

1. Hardware authentication prevents the need for users to enter a username and password every time they wish to establish a SSL VPN connection with the CS-2001. However, if it is the first time that a user tries to establish a SSL VPN connection, they will be requested to enter a username and password. Once the IT administrator has moved the user to the Accepted User list (located under **Web VPN / SSL VPN > Hardware Auth**) any subsequent SSL VPN connection attempts will authenticate the user based on their hardware and not by a username and password.

Terms in Status

Auth Name

- The authentication name of the client user.

Computer Name

- The computer name of the client user.

Real IP

- The real IP of the client user.

VPN IP

- The client IP allocated by the CS-2001.

Uptime

- The connection duration between the client and CS-2001.

Configuration

- To stop the connection between the CS-2001 and SSL VPN.（**Figure 21-1**）

Auth Name	Computer Name	Real IP	Web VPN IP	Connection Uptime	Configuration
No data found!					

Figure 21-1 SSL VPN Connection Status

21.1 Example

21.1.1 Configuring Web / SSL VPN Connection settings for

External Clients

Step 1. Go to **Interface** > **WAN**, activate the HTTPS function.（**Figure 21-2**）

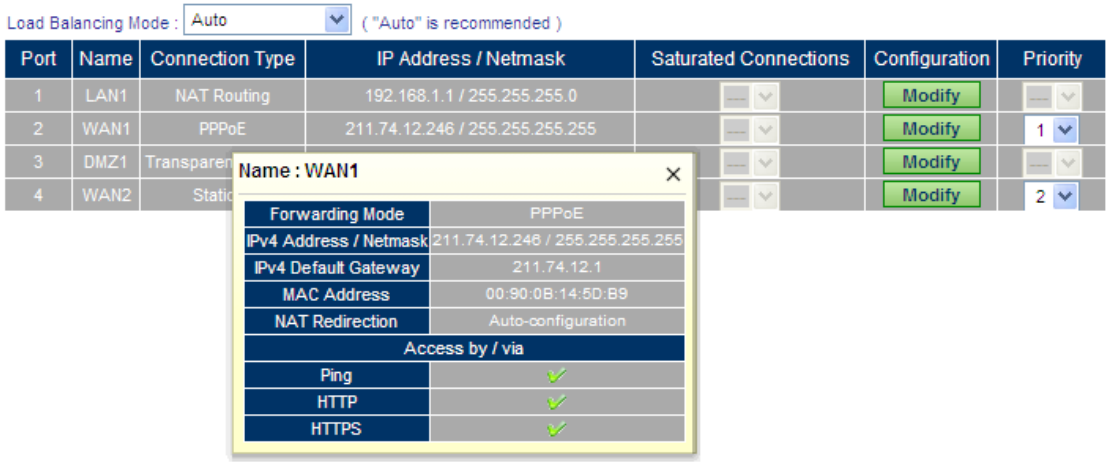


Figure 21-2 WAN Interface

Step 2. Go to **Policy Object** > **Authentication** > **Account / Group** and then set as below:（**Figure 21-3, 21-4**）

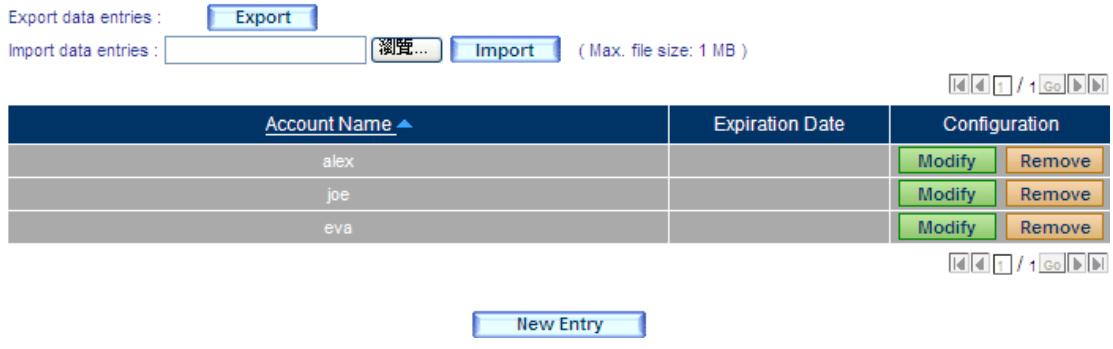


Figure 21-3 User Entries

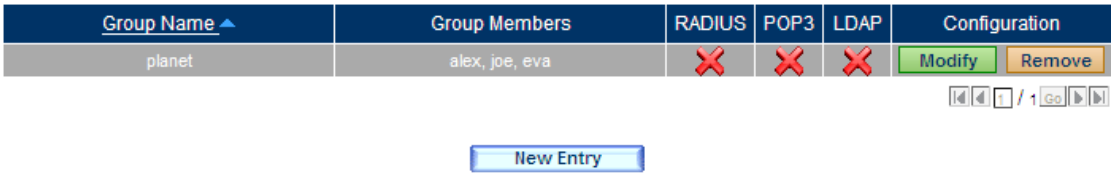


Figure 21-4 User Group Entries

Step 3. Go to **Web VPN / SSL VPN > Settings** and then set as below:

- Click **Modify**. (**Figure 21-5**)
- Tick **Enable Web VPN / SSL VPN.**
- Select the **IP Version**.
- Enter the **Client IP address / netmask**.
- Select the **Encryption Algorithm** and the **Communication Protocol**.
- Enter the **Server Port No**.
- Configure the **Available Subnets.**
- Click **OK**. (**Figure 21-6**)
- Click **New Entry**. (**Figure 21-7**)
- Type the name in the **Name** field.
- Select the authentication account / group from the drop-down list.
- Click **OK**. (**Figure 21-8**)

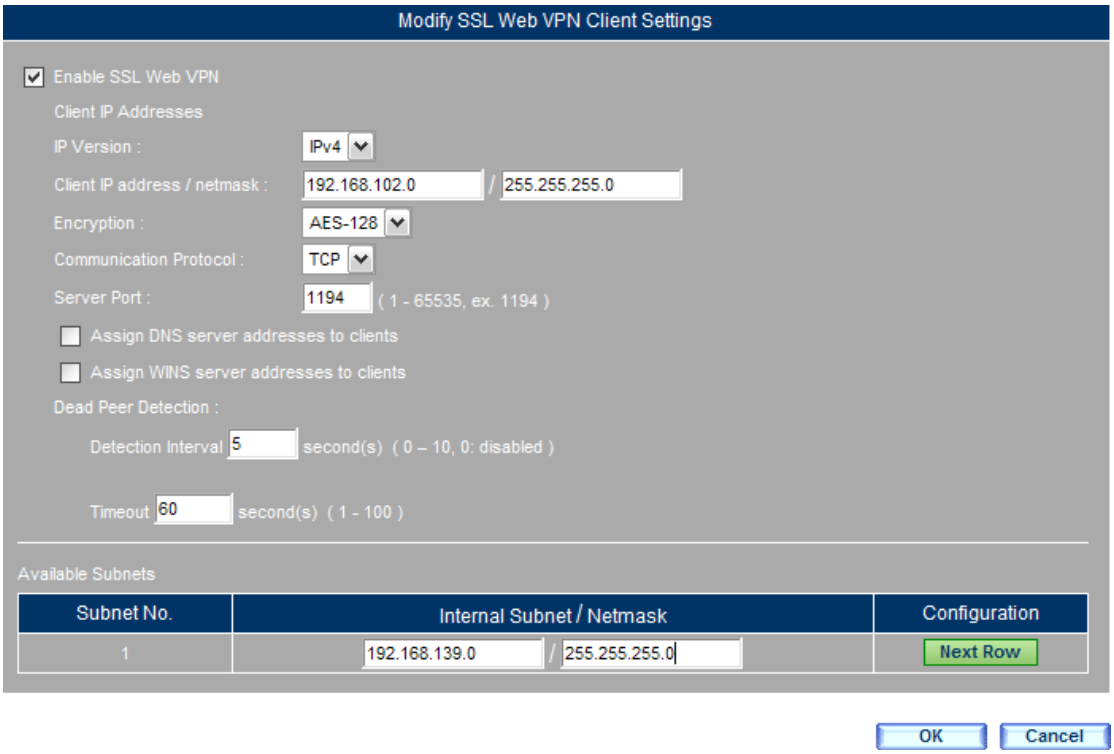


Figure 21-5 Web VPN / SSL VPN Settings

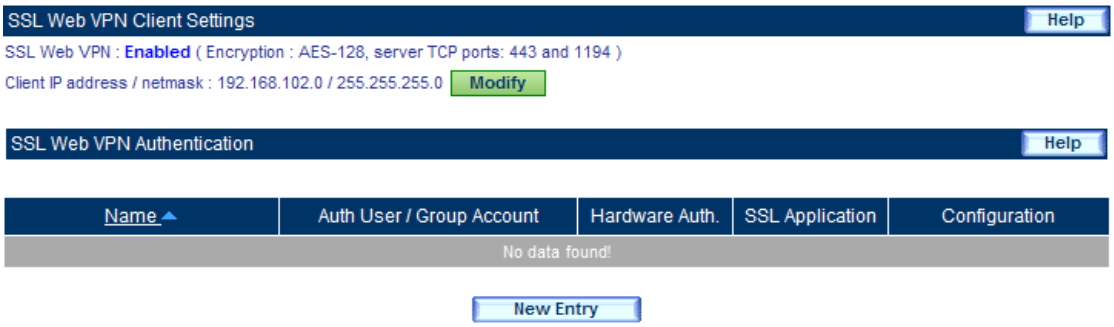


Figure 21-6 Web VPN / SSL VPN Setting Completed

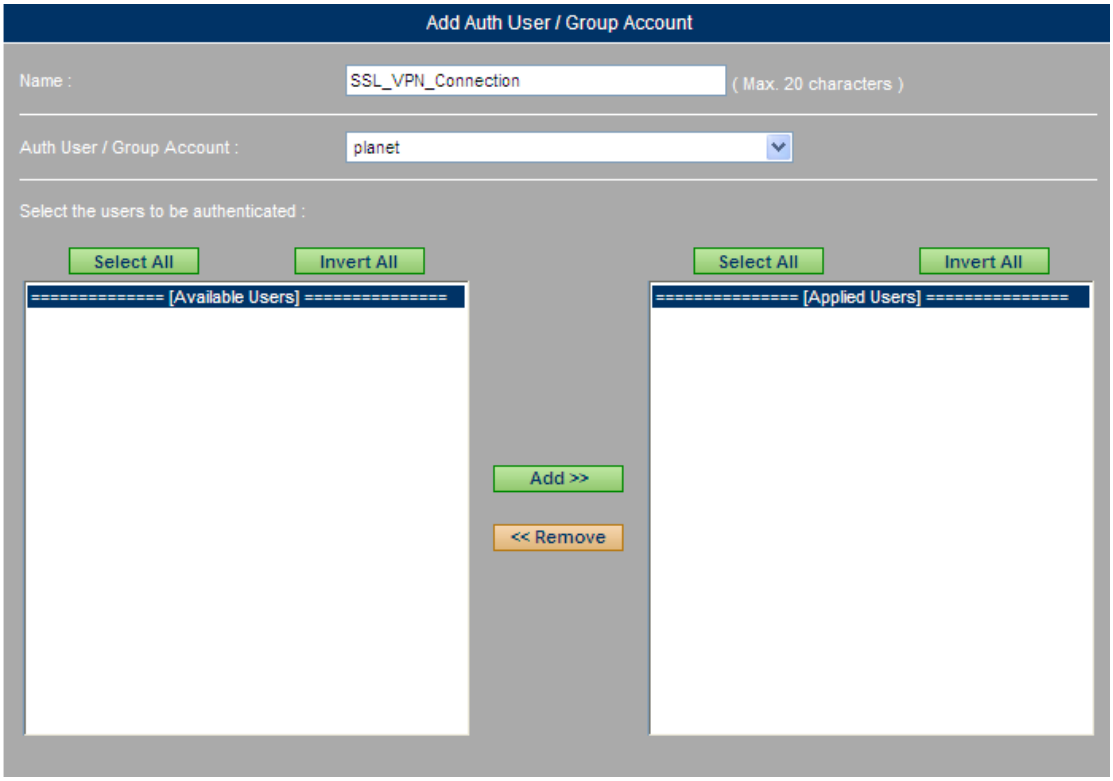


Figure 21-7 Web VPN / SSL VPN Authentication Settings

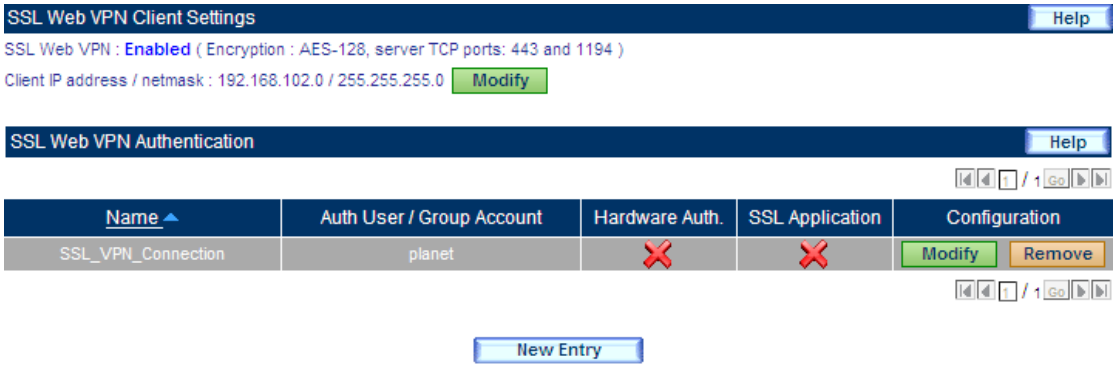


Figure 21-8 Web VPN / SSL VPN Authentication Completed

Step 4. Go to **Policy** > **Incoming** and then set as below:（**Figure 21-9**）

- Select the defined Web VPN / SSL VPN from the **VPN Trunk** drop-down list.
- Click **OK**.（**Figure 21-10**）

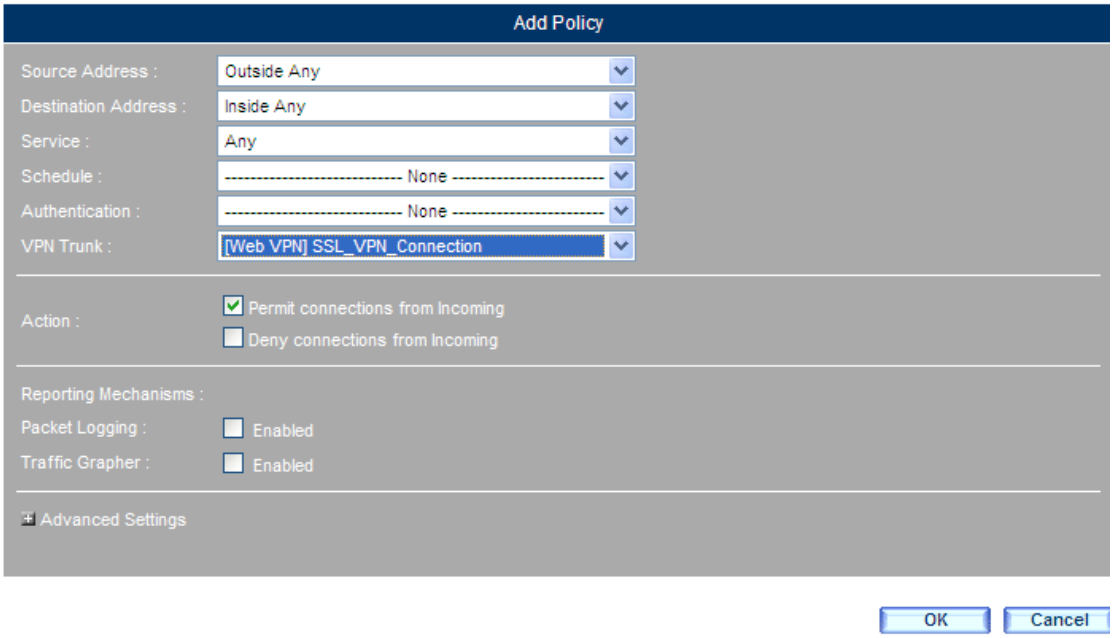


Figure 21-9 Configuring an Incoming Policy with Web VPN / SSL VPN

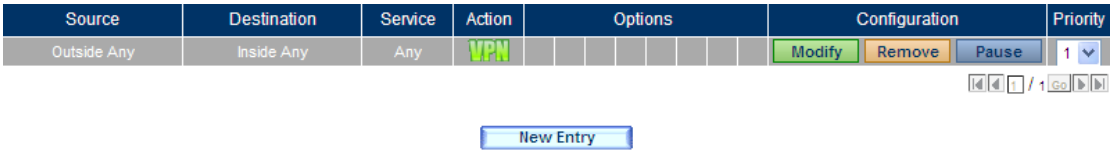


Figure 21-10 Policy Created

Step 5. Configure the setting from a browser:

- In the **URL** field, type the CS-2001 interface address plus sslvpn or webvpn. For example, https://61.11.11.11/sslvpn or https://61.11.11.11/webvpn.
- Click **Yes** in the Security Alert window.（**Figure 21-11**）
- Click **Yes** in the Warning – Security window.（**Figure 21-12**）
- Click **Yes** in the Warning-Security window again.（**Figure 21-13**）
- Select the language and then enter the username and the password.（**Figure 21-14**）
- Click **OK**.（**Figure 21-15, 21-16**）

Figure 21-11 Security Alert Window

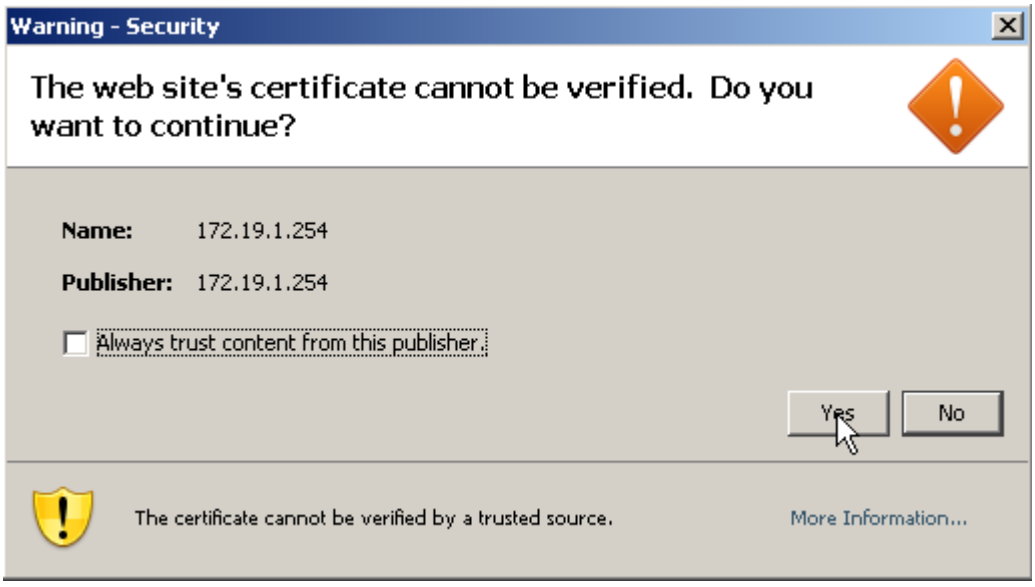


Figure 21-12 Warning-Security Window

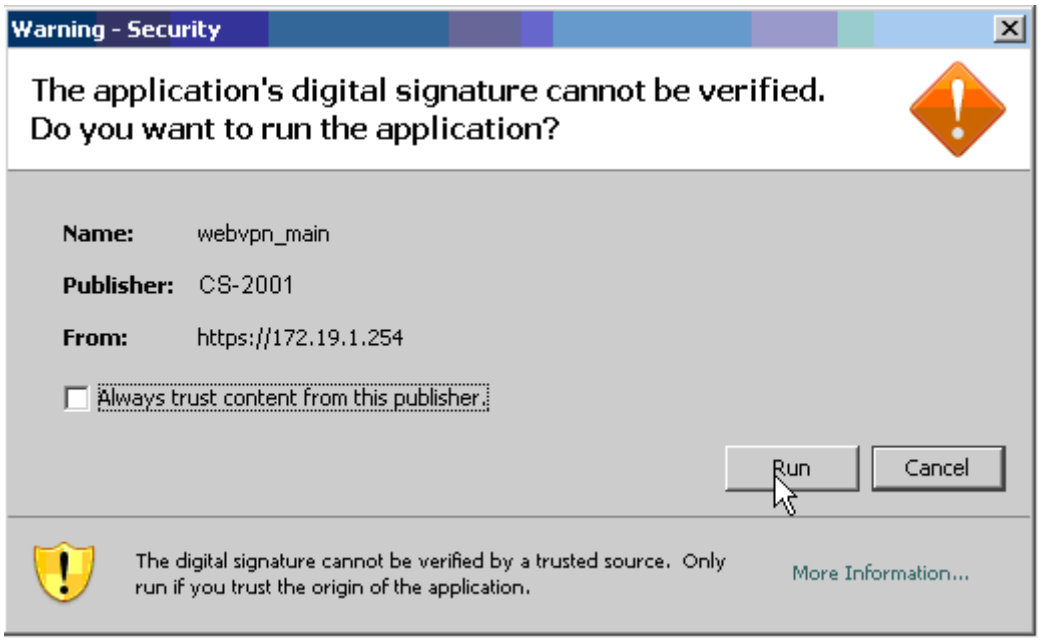


Figure 21-13 Warning-Security Window

Figure 21-14 The Authentication Window

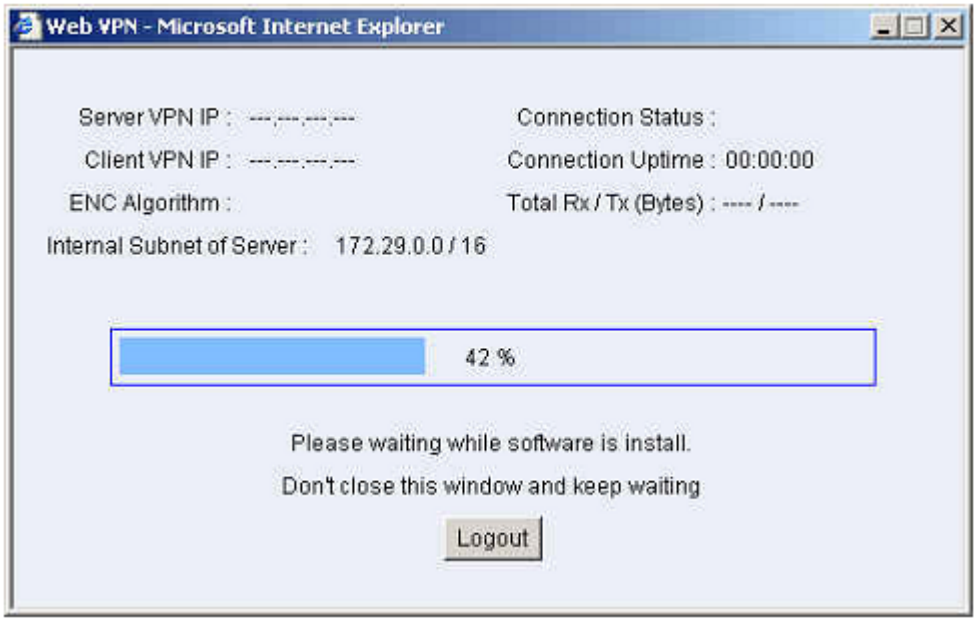


Figure 21-15 Web VPN / SSL VPN Connection

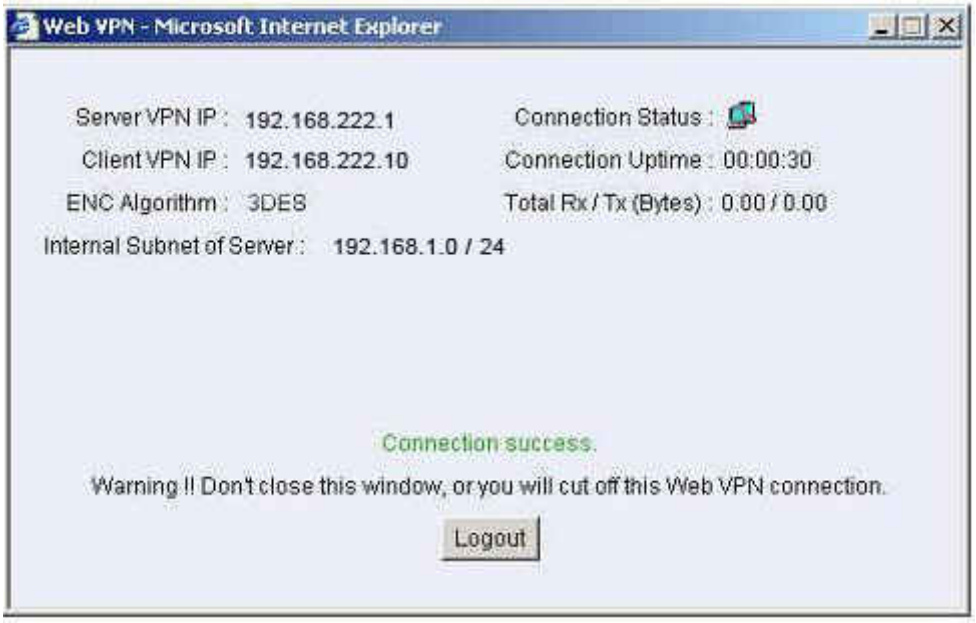


Figure 21-16 Web VPN / SSL VPN Connection Established

Step 6. Under **Web VPN/ SSL VPN > Status**, it shows the connection status: **(Figure 21-17)**

Auth Name	Computer Name	Real IP	Web VPN IP	Connection Uptime	Configuration
joe	ENM-ALBERT	211.75.117.114	192.168.102.6	00:00:25	Disconnect

Figure 21-17 Web VPN / SSL VPN Connection Status

Step 7. Under **Web VPN / SSL VPN > Hardware Auth**, it displays the connection status between the CS-2001 and the users.（**Figure 21-18**）

Figure 21-18 The Authentication User List

Step 8. Go to **Web VPN / SSL VPN > Settings** and then set as below: (**Figure 21-19**)

- Click **Modify.**
- Move the hardware from the **Available Hardware** column to the **Selected Hardware** column.
- Click **OK**. (**Figure 21-20**)

Figure 21-19 Configuring Authentication User / Group

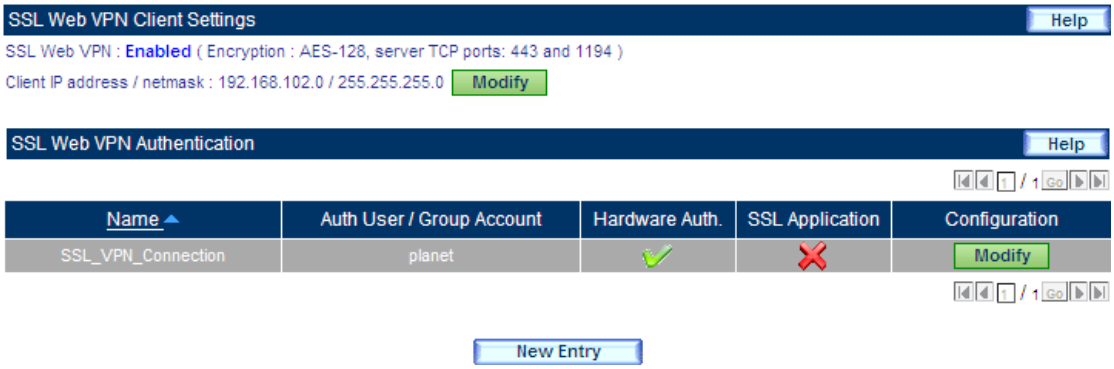


Figure 21-20 Setting Completed

Step 9. When a user establishes an SSL VPN connection through the CS-2001, their hardware can be directly authenticated without the need for a username and password.

Note：

1. When hardware authentication and user/group authentication are both enabled, the device will first try to authenticate by hardware authentication and will perform the following:
   - If the user's PC hardware information is under **Web VPN / SSL VPN > Settings**, then the user is permitted to establish a Web VPN connection.
   - If the user's PC hardware information is not under **Web VPN / SSL VPN > Settings**, then the user needs to be authenticated by username and password to establish a Web VPN connection.
   - The user needs to be authenticated by username and password for the first time to establish a Web VPN connection.
2. When only hardware authentication is enabled the device will perform the following:
   - If the user's hardware information is added under **Web VPN / SSL VPN > Settings**, the user will be able to establish a SSL VPN connection.
   - If the user's hardware information is not added under **Web VPN / SSL VPN > Settings**, then the user will not be able to establish a SSL VPN connection.
3. If hardware authentication is disabled, then the user will need to authenticate using a username / password to establish a Web VPN connection.
   - The device will authenticate the user's authentication name and password, then decide whether to establish a SSL VPN connection or not.
4. If the client user's PC does not have SUN JAVA Runtime Environment software installed then it will automatically be downloaded and installed during the SSL VPN connection login phase. **（Figure 21-21, 21-22）**

Figure 21-21 Java Runtime Environment Plug-in CA Installer Screen

Figure 21-22 Installing Java Runtime Environment Plug-in

IM Recording

Chapter 22 Configuration

IM Recording can help you record and monitor the use of MSN and QQ messenger. This can prevent productivity losses from personal use and confidentiality breaches from information leaks.

Terms in QQ Account Manager

IM Logging Setting

- Configures the storage lifetime of IM logging.

Enable Block QQ access with an invalid password

- The QQ messenger uses encryption. Thus, the CS-2001 device can only record the content of users whose account and password have been verified or authenticated by the device. If **Block QQ access with an invalid password** is not selected, the unauthenticated users may log into the QQ messenger but not be monitored by the CS-2001 device.

QQ Account Manager

- Manages the use of QQ messenger. To log into the QQ messenger, users must add their accounts to the QQ user list. Users may log into the Web interface to add their own account. (The management IP address appended with qq, e.g., http://192.168.1.1/qq)

Note:

1. The meaning of symbols under **IM Recording > Configuration > QQ Account Manager**:

Symbol	Meaning	Description
	Valid Password	The user's account and password is valid. The CS-2001 device may record the user's use of QQ messenger.
	Unauthenticated Password	The user's password has not been authenticated yet.
	Invalid Password	The user's password is invalid. The CS-2001 device may not be able to record the user's use of QQ messenger.

2. The CS-2001 wll authenticate the user's account and password when the user attempts to log into the QQ messenger.

22.1 Example

22.1.1 Recording the Use of MSN / QQ Messenger

Step 1. Users may log into the Web User Interface to add their own account. (Enter the management IP address appended with qq, e.g., http://192.168.1.1/qq) **（Figure 22-1, 22-2）**

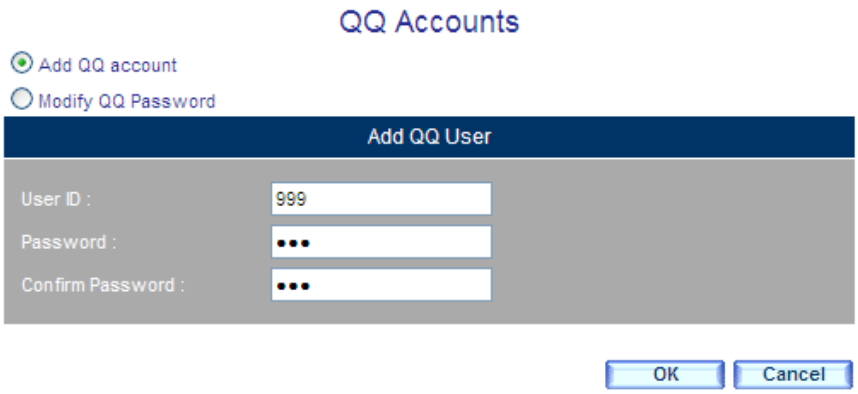


Figure 22-1 Entering the QQ Account and Password

Figure 22-2 Account Added

Note:

1. IT administrator may add new users under **IM Recording > Configuration > QQ Account Manager**.

Step 2. The added user is listed under **IM Recording** > **Configuration** > **QQ Account Manager**:

- Tick **Block QQ access with an invalid password**.
- Click **OK**.
- The newly added user has not yet been authenticated.（**Figure 22-3**）
- The user is authenticated when log into the QQ messenger.（**Figure 22-4**）

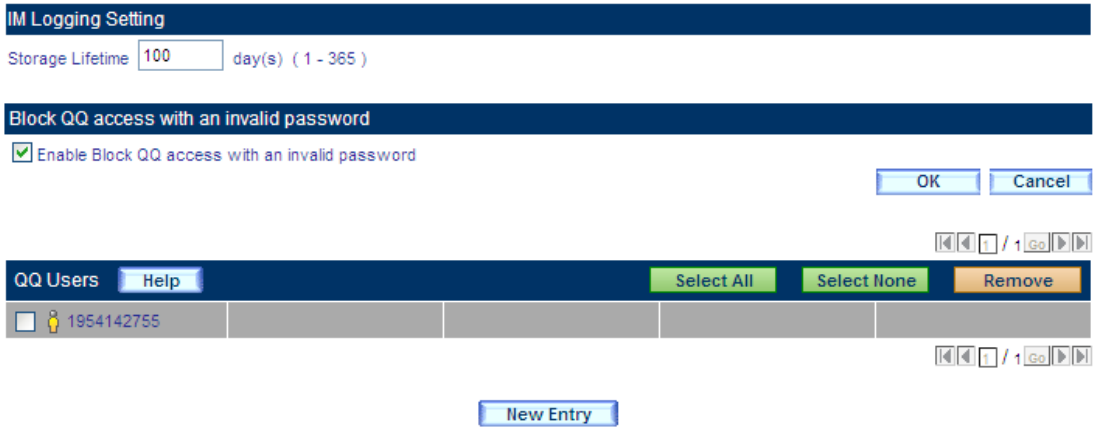


Figure 22-3 The Unauthenticated Account

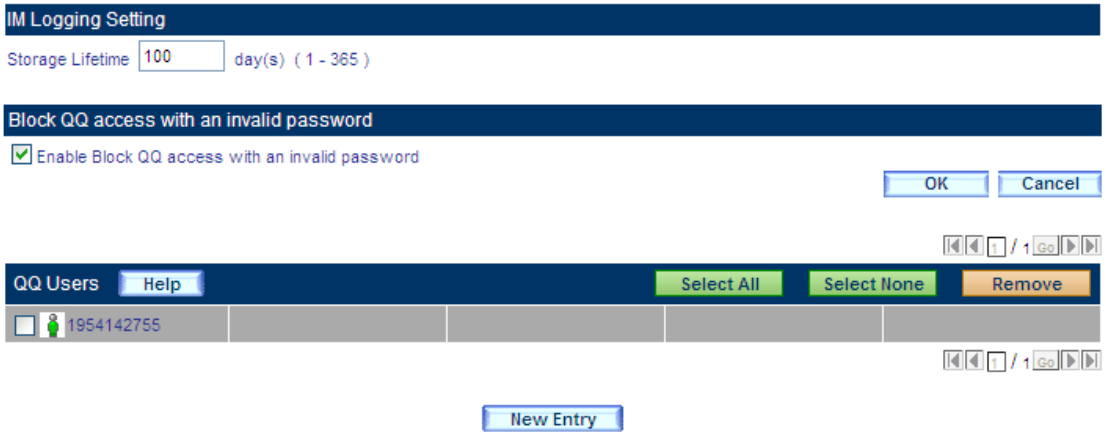


Figure 22-4 The Authenticated Account

Note:

1. Users may go to the Web user interface to change their password on their own. (Enter the management IP address appended with qq. E.g., http://192.168.1.1/qq)（**Figure 22-5**）

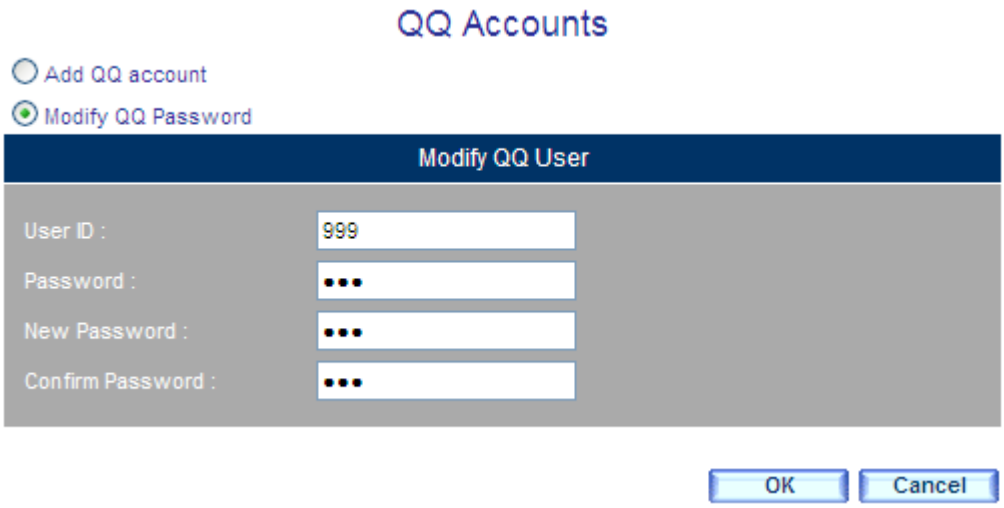


Figure 22-5 Modifying the Password

Step 3. Go to **Policy** > **Outgoing** and set as below:（**Figure 22-6**）

- Enable IM Recording.
- Click **OK**.（**Figure 22-7**）

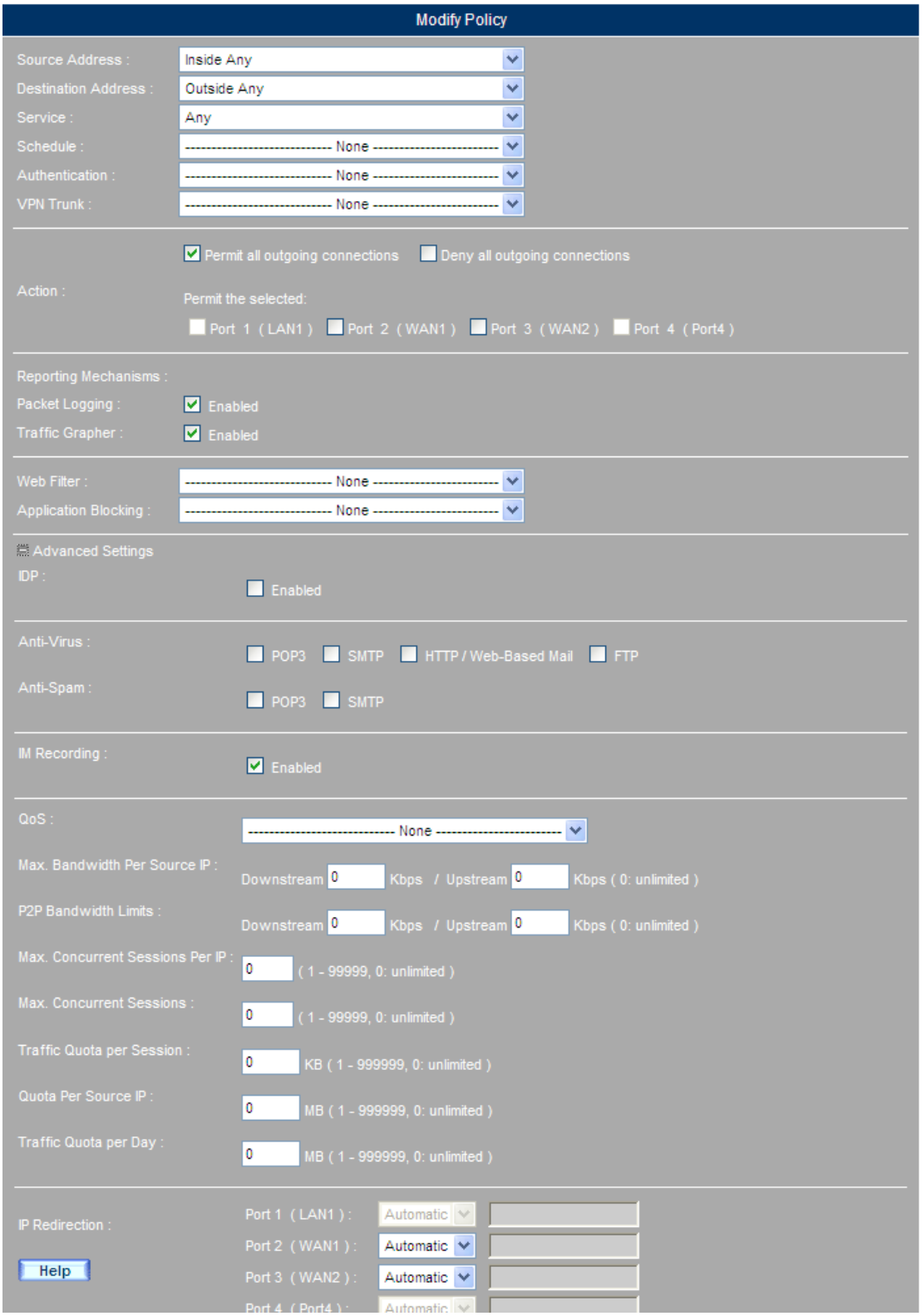


Figure 22-6 Creating an Outgoing Policy with IM Recording

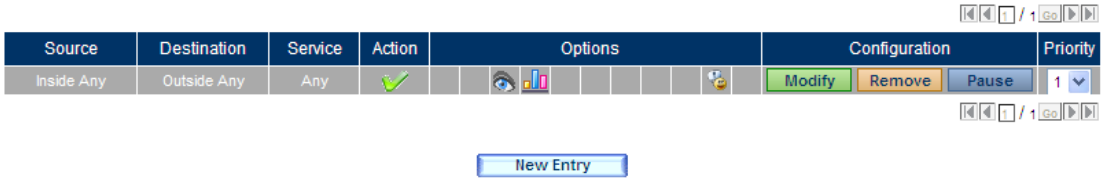


Figure 22-7 Policy Created

Chapter 23 Reports

The records of MSN and QQ messengers are shown in the form of easy-to-read log and statistics.

Terms in Settings

Periodic Report Scheduling Settings

- It can generate and send out the periodic report to the designated recipient(s) on schedules.
- You may configure the max. number of items per statistic chart.

Historical Report Scheduling Settings

- It can generate and send the history report to the designated recipient(s) on schedules.
  - Go to **System** > **Configuration** > **Settings**, configure the **Email Notification Settings**. Then, go to **IM Recording** > **Reports** > **Settings** and set as below:
    - In the **Periodic Report Scheduling Settings** section, tick **Enable the mailing of Periodic Report** and then select **Yearly report, Monthly report**, **Weekly report** and **Daily report.**
    - **Max. items per Statistics Chart**: enter 0. (0 : shows all available items)
    - Click **OK**.（**Figure 23-1**）
    - The designated recipient will receive the reports on schedules.（**Figure 23-2, 23-3**）
    - In the **Historical Report Scheduling Settings** section, tick a desired period and specify a date for it.（**Figure 23-4**）
    - Click **Send Report**.
    - The designated recipients will receive reports on schedules.（**Figure 23-5, 23-6**）

Note:

1. Periodic report schedule:

- Yearly Report: Creates the report at 00.35 on January 1.
- Monthly Report: Creates the report at 00.35 on the first day of the month.
- Weekly Report: Creates the report at 00.35 on the first day of the week.
- Daily Report: Creates the report at 00.35 everyday.

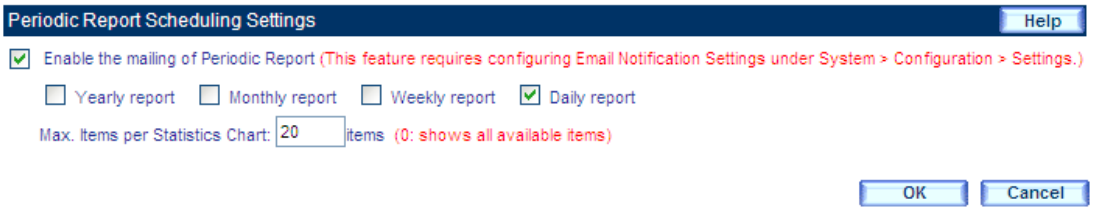


Figure 23-1 Periodic Report Settings

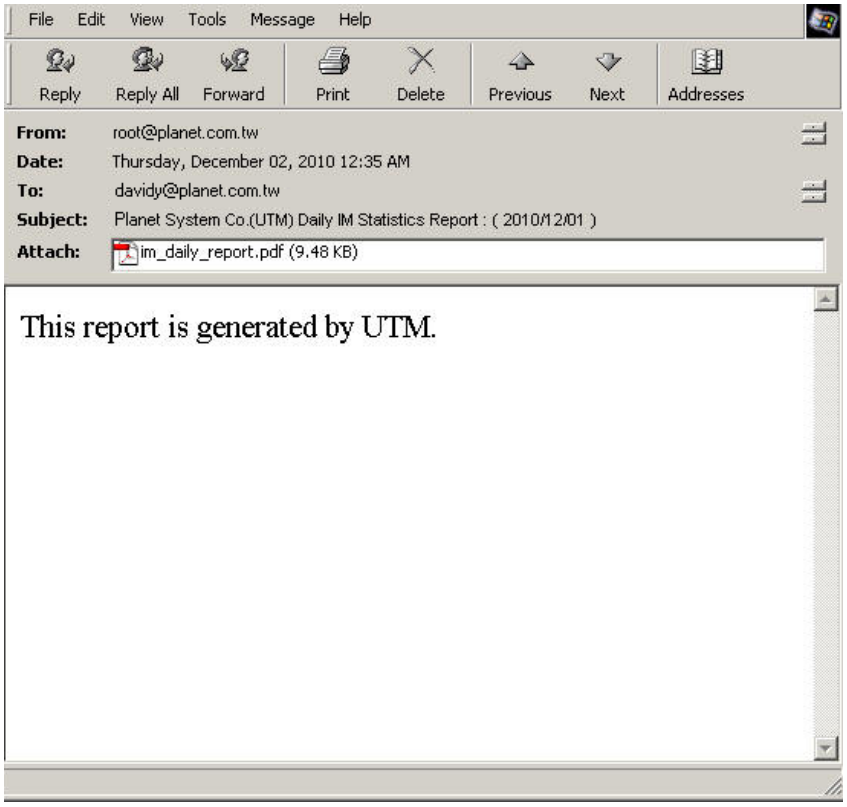


Figure 23-2 Daily IM Statistics Report

Planet System Co.

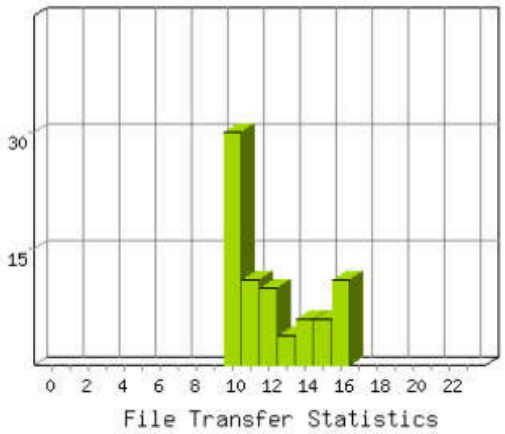
Daily IM Report

Top IM Users by IP File Transferred Message Sent

No.	IP Address	File Transferred	Message Sent	Total IM Events	Event Indicator
1	172.19.104.105	78	0	78	78
2	172.19.20.12	0	34	34	34
3	172.19.20.17	0	7	7	7
Duration : **2010-12-01 00:00 ~ 2010-12-01 23:59** Total IM Events : **119** Average : **4.96 IM events/Hour**					

Top IM Users by Account File Transferred Message Sent

No.	IM Account	File Transferred	Message Sent	Total IM Events	Event Indicator
1	sukent300@hotmail.com.tw	78	0	78	78
2	support@hotmail.com.tw	0	34	34	34
3	faith@hotmail.com.tw	0	7	7	7
Duration : **2010-12-01 00:00 ~ 2010-12-01 23:59** Total IM Events : **119** Average : **4.96 IM events/Hour**					



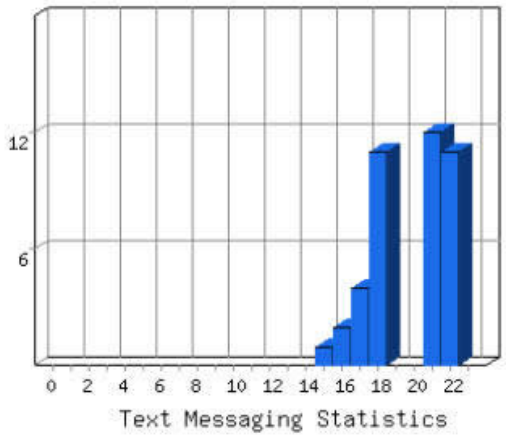


Figure 23-3 Daily IM Statistics Report

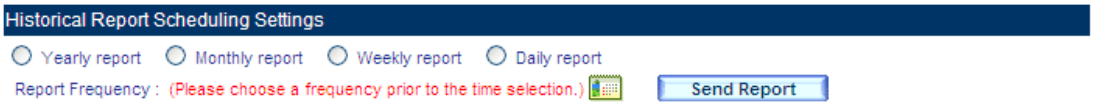


Figure 23-4 Historical Report Scheduling Settings

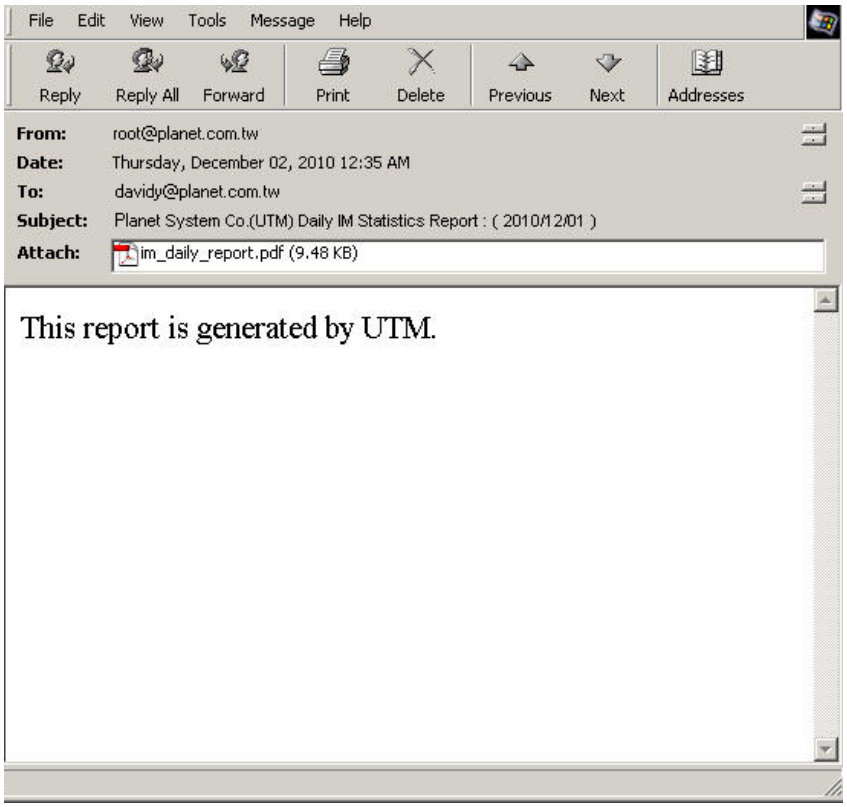


Figure 23-5 Historical Report Received

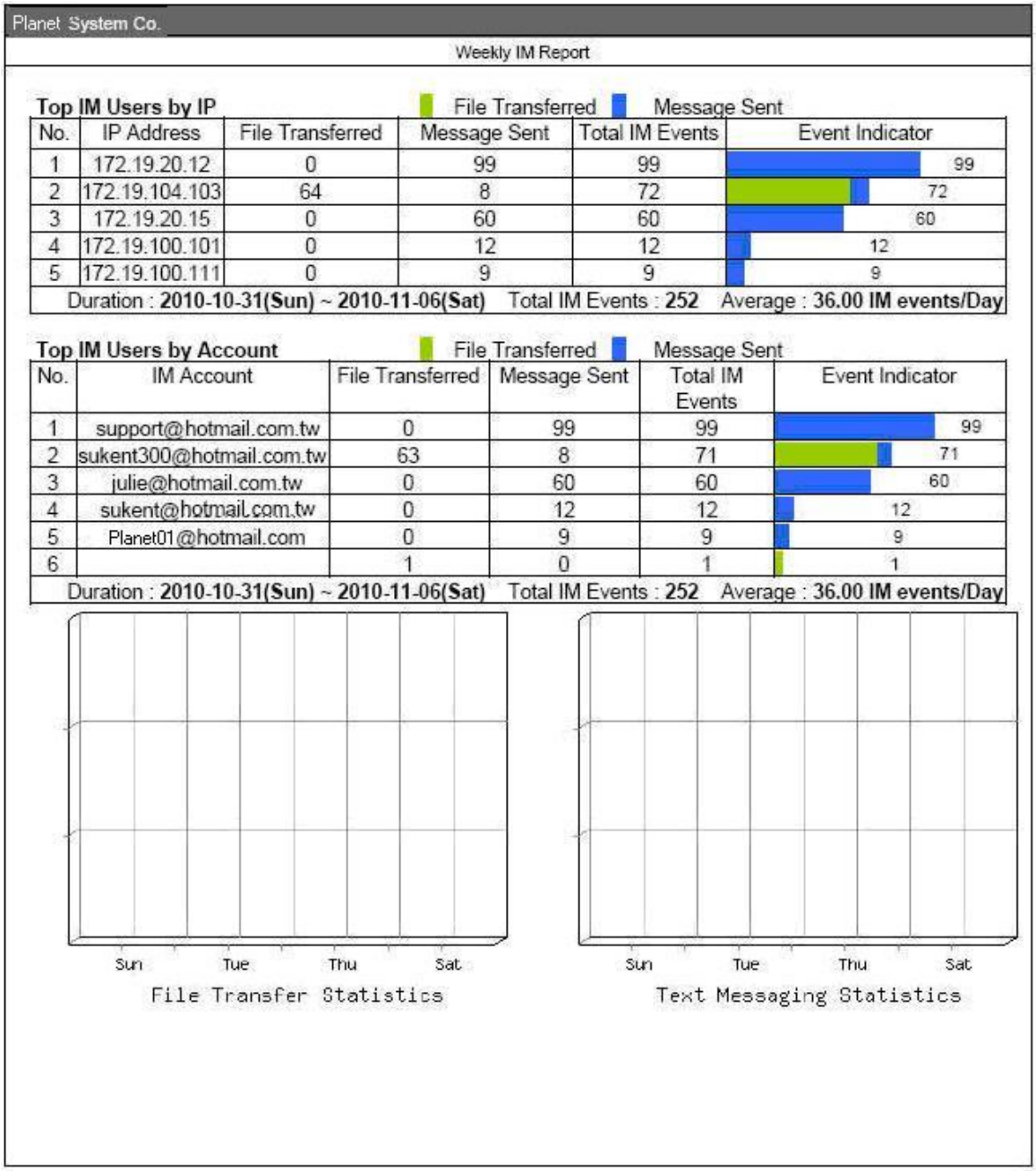


Figure 23-6 Weekly IM Statistics Report

Terms in Message History

Search

- Available search criteria are date, time range, IM type, username, account, participants, message content and transferred file name.
  - Configure the **Email Notification Settings** under **System > Configuration > Settings** and then go to **IM Recording > Reports > Message History** and set as below:
    - Specify the time duration.
    - Type the keyword of the **IM Account**.

- Click **Search**.（**Figure 23-7**）
- Click **Send Report**.
- The report is sent to the designated recipient(s). （**Figure 23-8, 23-9**）
- To store the search results in the local computer, click the **Download Report** button.（**Figure 23-10**）

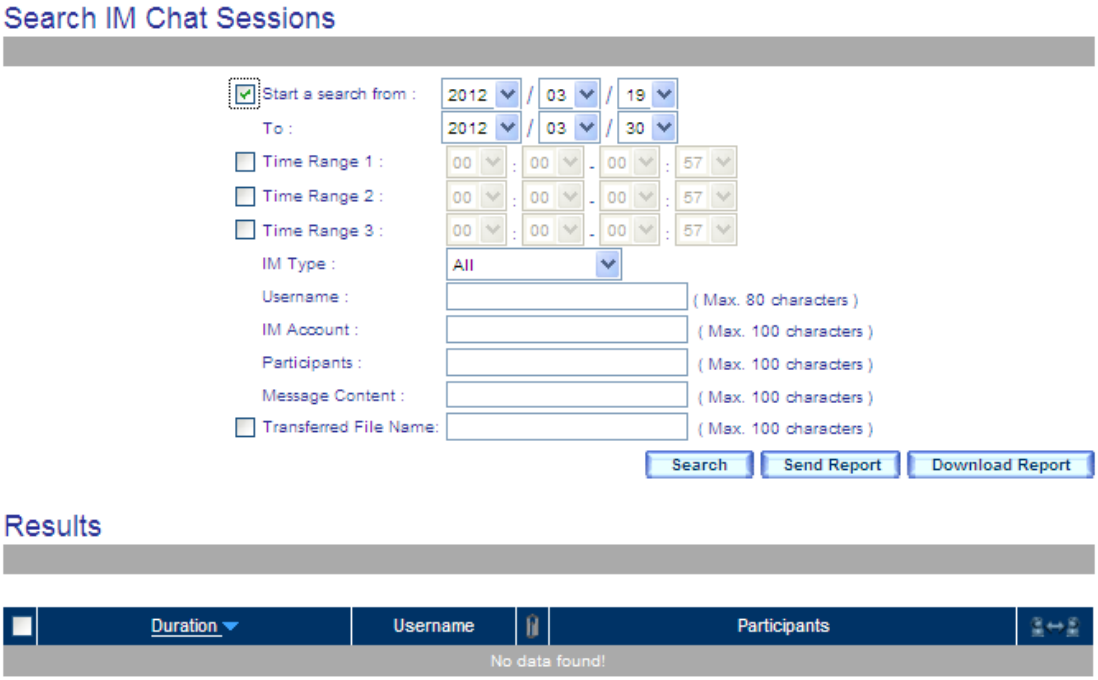


Figure 23-7 Searching the Specific Logs

Note:

The logs under **IM Recording > Reports > Message History** can be sorted by **Duration**.

UTM content security gateway(UTM content security gateway) Search IM Chat Sessions
sender@mydomain.com

To: Frank.T / ENM Dept.
Attach: Search IM Chat Sessions.html (6 KB)

UTM content security gateway

Duration	Username	Attached	Participants	Freq.
11:44:17 - 12:02:59 (18.42 min)	PC	V	(MSN) antonyseed@hotmail.com <-> anthon...	8

Figure 23-8 Receiving the Search Results

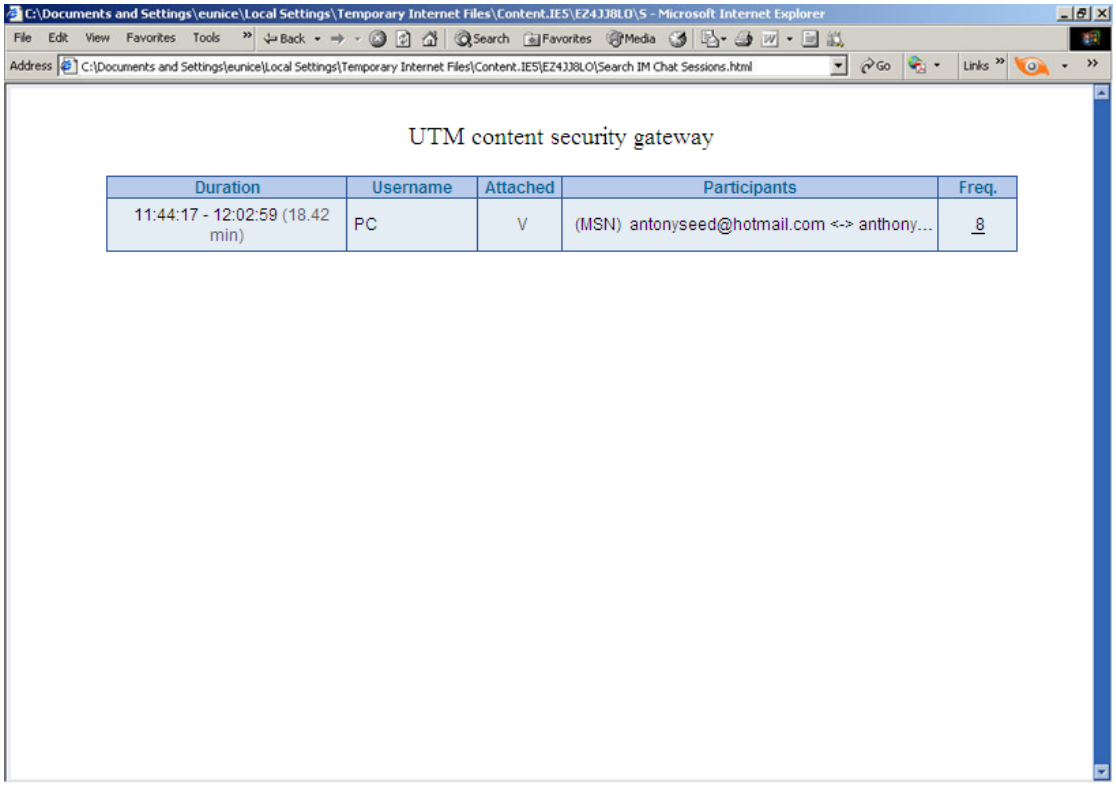


Figure 23-9 The Searching Results

Note:

You may click the number under the icon to see the sent messages of the participants.

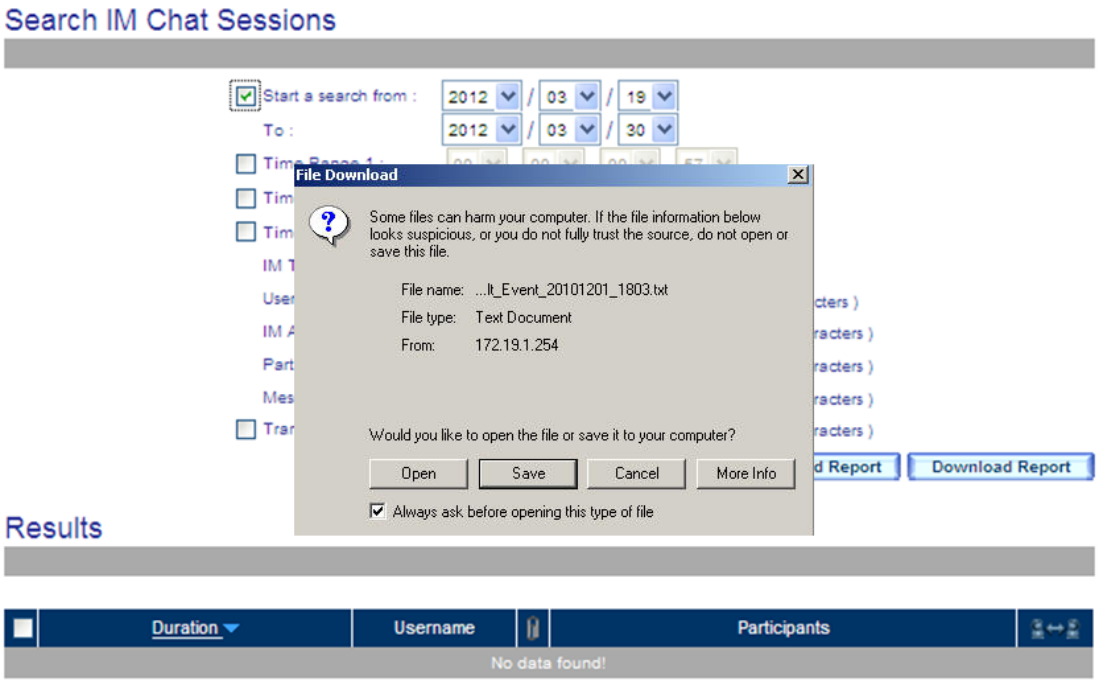


Figure 23-10 Downloading the Searching Results

23.1 Statistics

Step 1. **IM Recording** > **Reports** > **Statistics** shows a comprehensive statistical report.

Step 2. In the upper left corner, click **Day** to see the daily report; click **Week** to see the weekly report; click **Month** to see the monthly report; click **Year** to see the yearly report.

Step 3. How to read the statistics report: (**Figure 23-11**)

- Y-axis indicates the number of the sent messages and transferred files.

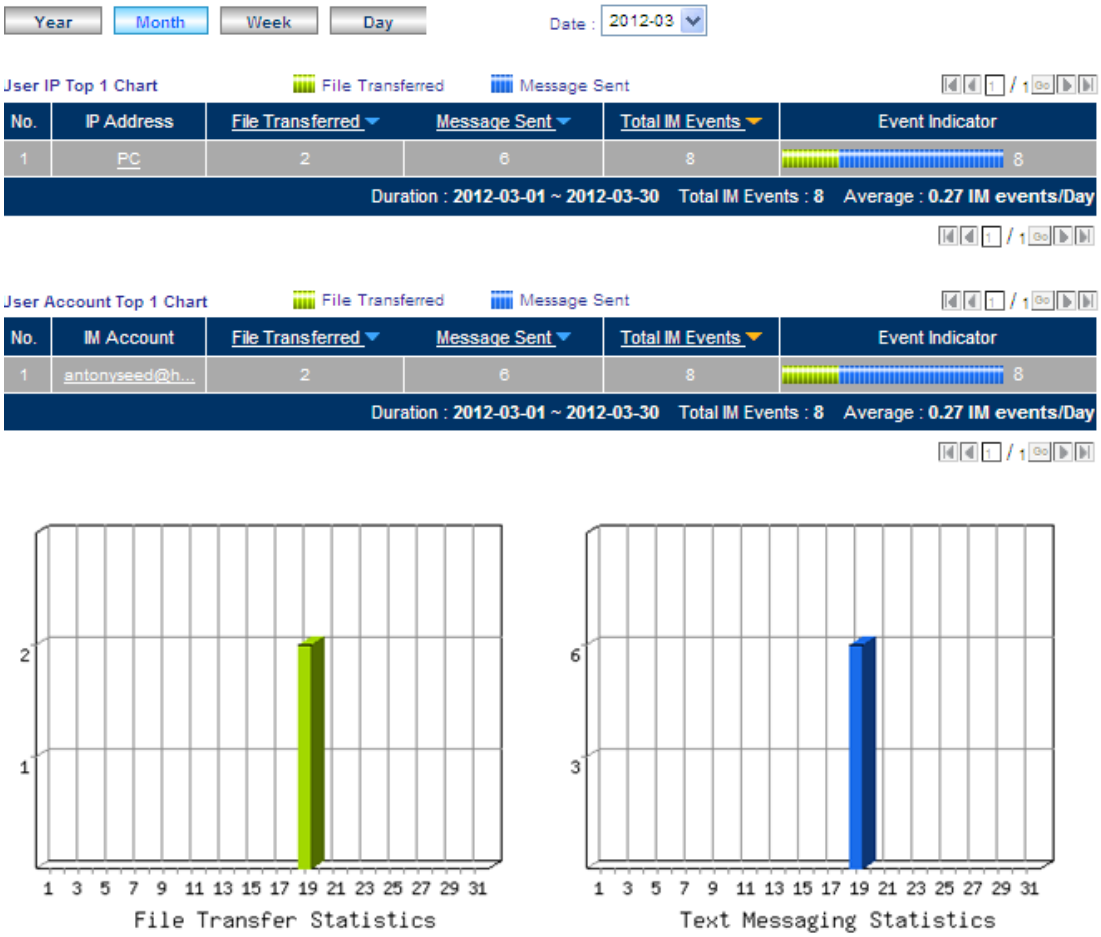


Figure 23-11 IM Recording Statistical Report

23.2 Message History

Step 1. **IM Recording** > **Reports** > **Message History** shows the logs of users' conversation.（**Figure 23-12**）

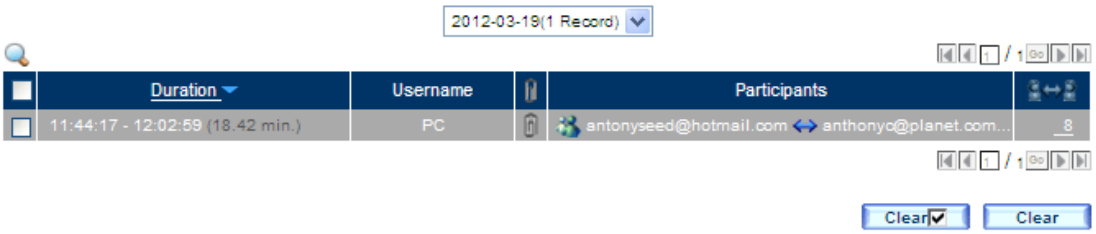


Figure 23-12 IM Conversation Logs

Policy

Chapter 24 Policy

CS-2001 inspects each packet passing through the device to see if it meets the criteria of any policy. Every packet is processed according to the designated policy, consequently any packets that do not meet the criteria will not be permitted to pass.

The items of a policy include Source Address, Destination Address, Service, Schedule, Authentication, VPN Trunk, Action, Log, Statistics, Web Filter, Application Blocking, IDP, Anti-Virus, Anti-Spam, Mail Archive/ Audit, QoS, MAX. Bandwidth Per Source IP, MAX. Concurrent Sessions Per IP, MAX. Concurrent Sessions, Quota Per Session, Quota Per Source IP, Quota Per Day, Forwarding Mode, etc. The IT administrator could determine the outgoing and incoming service or application of which data packets should be blocked or processed by configuring these items.

The IT administrator can customize the policy based on the source address, source port, destination address and destination port of a packet. According to the attribute of a packet, the policy setting is categorized into:

- **Outgoing**: The packet is from the LAN and heading to the WAN. The IT administrator can customize the policy for outgoing packets.
- **Incoming**: The packet is from the WAN and heading to the LAN (e.g., when using IP mapping or virtual server). IT administrators can customize the policy for incoming packets.
- **WAN to DMZ**: The packet is from the WAN and is heading to the DMZ (e.g., when using IP mapping or virtual server). IT administrators can customize the policy for WAN-to-DMZ packets.
- **LAN to DMZ** : The packet is from LAN and heading to the DMZ. IT administrators can customize the policy for LAN-to-DMZ packets.
- **DMZ to WAN** : The packet is from the DMZ and heading to the WAN. IT administrators can customize the policy for DMZ-to-WAN packets.

- **DMZ to LAN** : The packet is from the DMZ and heading to the LAN. IT administrators can customize the policy for DMZ-to-LAN packets.
- **LAN to LAN** : The packet is from the LAN and heading to the LAN. IT administrators can customize the policy for LAN-to-LAN packets.
- **DMZ to DMZ**: The packet is from the DMZ and heading to the DMZ. IT administrators can customize the policy for DMZ-to-DMZ packets.

Note：

1. CS-2001 only processes packets accepted from the policy. Therefore, wherever the connection is made — regardless of the network type (LAN, WAN or DMZ) — there must be policies respectively configured for these networks.

2. CS-2001 adopts VPN trunk in policy to manage the packet transmission and reception of VPN connections.

Terms in Policy

Source Address & Destination Address

- Source address and Destination address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.

Service

- The service to be regulated. Available options are the system default services and the customized services.

Option

- It shows the function that had been activated. When a function is activated, the symbol corresponding to it will appear. (see the table below)

Symbol	Meaning	Description
	Schedule	Activated as per the configured scheduled time.
	Authentication	Authentication user activated.
	Packet Logging	Packet Logging activated.
	Traffic Grapher	Traffic Grapher activated.
	IDP	IDP activated.
	Web Filter	Web Filter activated.
	Application Blocking	Application blocking activated.
	Anti-Virus, Anti-Spam, Mail Archiving/ Auditing	Anti-Virus, Anti-Spam, Mail Archiving/ Auditing activated.
	QoS	QoS activated.
	Web App Firewall	Web App Firewall activated.
	IM Recording	IM Recording activated.
	IP Redirection	Three types can be selected, Automatic, Routing and NAT.

Schedule

- The time by which a policy executes.

Authentication

- This requires users to be authenticated to create a connection.

VPN Trunk

- This is where you apply the policy to regulate the session packets of IPSec or PPTP VPN.

Action

- It determines over which WAN interface/s packets are permitted to pass through (see the table below).

Symbol	Meaning	Description
	WAN access is granted to all interfaces	Packets are granted to pass through all interfaces once approved by the configurd policy.
	WAN1 granted	Policy approved packets may access WAN1.
	WAN2 granted	Policy approved packets may access WAN2.
	VPN Trunk granted	Approved VPN session packet access.
	Access denied	Packet access denied.
	Pause	Policy suspended.

Logs

- Records the packet transmissions managed by the policy, such as Protocol, Port, Source IP, Destination IP, etc. To see the logs, click the Log icon .

Statistics

- When enabled, there will be a chart drawn from the statistics of traffic flow.

Web Filter

- It can restrict the use of HTTP or FTP protocol.

Application Blocking

- It can block the use of Instant Messenger, Peer-to-Peer Sharing, Video / Audio Application, Webmail, Game Application, Tunnel Application, Remote Control Application and other Application.

IDP

- It can identify intrusion packets and react to them in a timely manner.

Web App Firewall

- It can regulate and filter all the web application.

Anti-Virus

- It filters viruses contained within files transferred over HTTP / Web-Based Mail / FTP / SMTP / POP3 protocol.

Anti-Spam

- It filters emails transferred over POP3 and SMTP.

Mail Archiving / Auditing

- It determines whether to archive or audit the incoming or outgoing emails that pass through the policies.

QoS

- The guaranteed and maximum bandwidth settings. (The bandwidth is distributed to users who meet the criteria of the policy).

Max. Bandwidth per Source IP

- It can limit the bandwidth of each IP address respectively.

Note:

1. When the total sum of **Max. Bandwidth per Source IP** has reached the maximum bandwidth of QoS, there will be no spare bandwidth available for new sessions.
2. The **Max. Bandwidth per Source IP** can ensure that every LAN user accesses bandwidth fairly.

Max. Concurrent Sessions Per IP

- It determines the maximum number of concurrent sessions of each IP address. If the amount of sessions exceeds the set value, new sessions will not be created。

P2P Bandwidth Limits

- It determines the maximum bandwidth of P2P application.

Max. Concurrent Sessions

- It determines the maximum number of concurrent sessions of a policy. If the amount of sessions exceeds the set value, new sessions will not be created.

Note:

1. **Max. Concurrent Sessions** overrides **Max. Concurrent Sessions per IP** in a policy. When the setting value of **Max. Concurrent Sessions** exceeds the one of **Max. Concurrent Sessions per IP**, the policy will adhere to the set value of **Max. Concurrent Sessions.**

Traffic Quota per Session

- It determines the total traffic amount of a session.

Quota per Source IP

- It determines the quota of per source IP of a policy.

Traffic Quota per Day

- It determines the total traffic amount of a session per day.

IP Redirection Mode

- There are three Forwarding Mode for WAN, LAN and DMZ:
  - Automatic: Automatically Transferring the source IP address to the default IP addres of CS-2001 device.
  - Routing: Delivering the packets using its original source IP and Destination IP.
  - NAT: Transferring the Source IP address to the designated IP address on the CS-2001 interface's subnet.

Note:

1. Under **Network > Interface**, the NAT selection for **Connection Type** is used for transferring all the WAN packets's IP address. The NAT selection for **Connection Type** under **Policy** is used for transferring the IP on the specific subnet.

Pause

- When modifications are required on existing settings, such as *Address* and *QoS*, you may temporarily disable the policy so as to modify the policy.

Priority

- When accessing packets, CS-2001 will inspect the packet to see if it is identical with the criteria of existing policies. The packet-to-policy inspection is performed by the priority of policies. Therefore, in order to optimize the process, you may rearrange the priority of policies accordingly by changing the figure in the pull-down menu of each policy.

24.1 Example

No.	Settings	Scenario	Page
24.1.1	**Outgoing**	Creating a Policy to Monitor the Internet Access of LAN User	**667**
24.1.2	**Outgoing**	Creating a Policy to Restrict the Access to Specific Web Sites	**673**
24.1.3	**Outgoing**	Creating a Policy to Grant Internet Access to Only Authenticated Users on Schedule	**680**
24.1.4	**Incoming**	Creating a Policy to Enable a Remote User to Control a LAN PC with Remote Control Software (pcAnywhere)	**682**
24.1.5	**WAN to DMZ**	Creating a Policy to Limit the Bandwidth, Daily Total Traffic Amount and Maximum Concurrent Sessions of an Incoming Session to a FTP Server (A NAT Mode Example)	**684**
24.1.6	**WAN to DMZ** **DMZ to WAN** **LAN to DMZ**	Creating a Policy to Enable LAN / WAN Users to Have Email Access (A Transparent Mode Example)	**687**

Prerequisite Setup

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing mode) and connect it to the LAN which is using 192.168.1.x/24.

Configure Port2 as WAN1 (61.11.11.11) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Configure Port3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Configure Port4 as DMZ1.

24.1.1 Creating a Policy to Monitor the Internet Access of LAN Users

Step 1. Go to **Policy** > **Outgoing** and then set as below: (**Figure 22-1**)

- Enable the **Packet Logging**.
- Enable the **Traffic Grapher**.
- Click **OK**. (**Figure 22-2**)

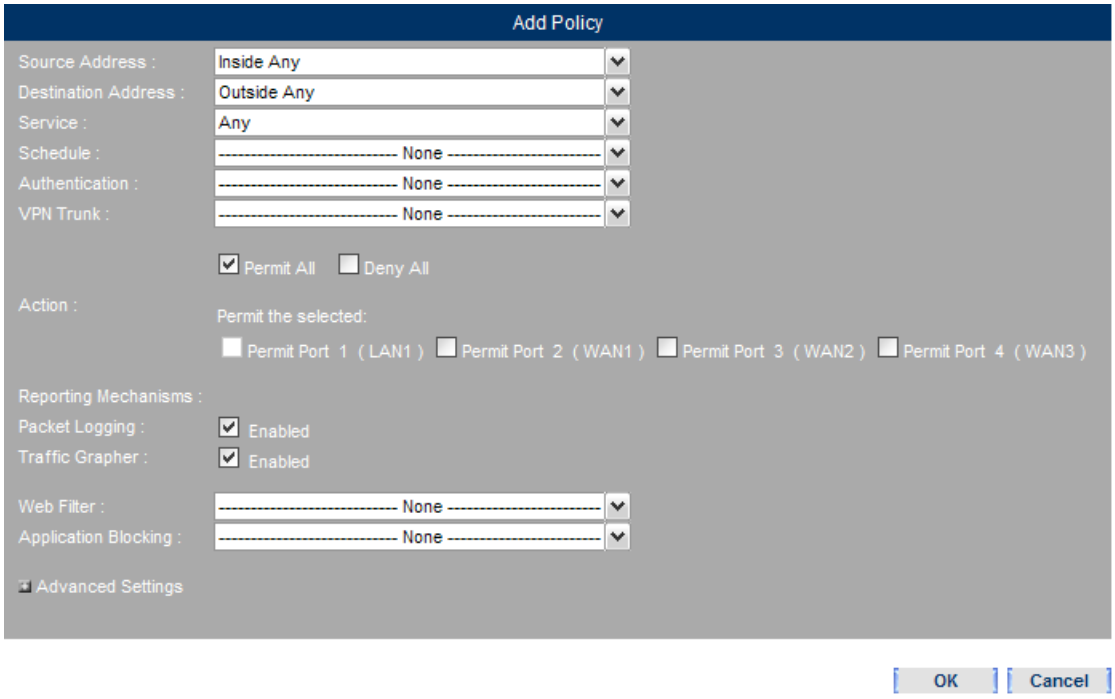


Figure 22-1 Enabling Packet Logging and Traffic Grapher

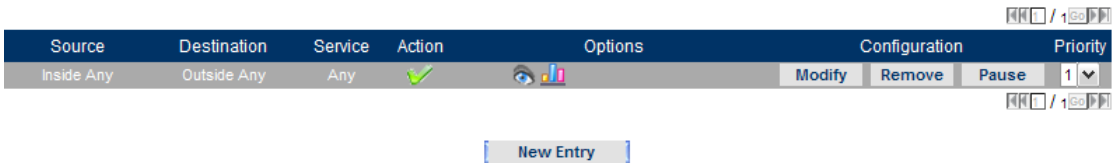


Figure 22-2 Setting Completed

Step 2. Click the Log icon of a policy to see the log. (**Figure 22-3**)

- In the upper-left corner, click the Refresh button or select a refresh interval from the drop-down list to obtain the up-to-date session information.
- Click any **Source IP** or **Destination IP** for sessions accessed through the IP address that you click on.
- For details of all sessions accessed through CS-2001, go to **Monitoring > Logs > Traffic** on the main menu. (**Figure 22-4**)

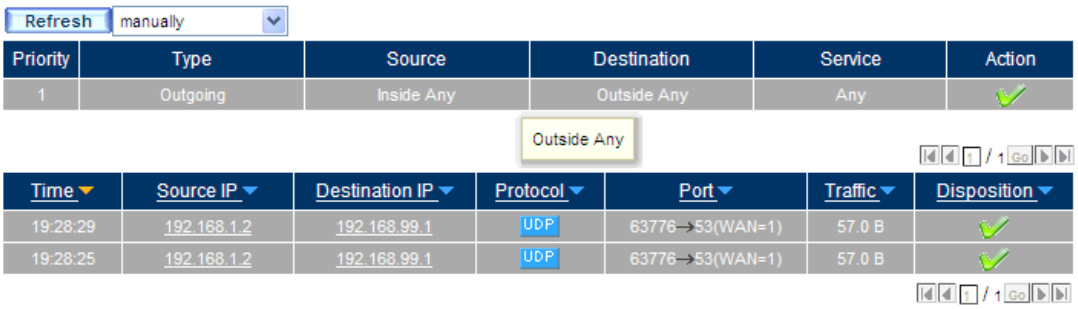


Figure 22-3 Traffic Log Filtered Screen

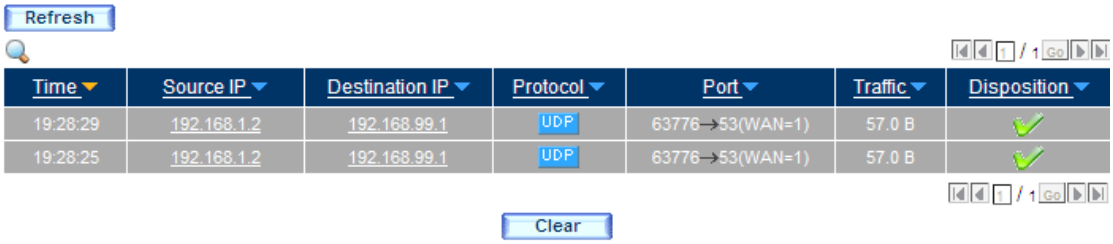


Figure 22-4 Traffic Shown in Log Screen

Step 3. Under **Monitoring** > **Traffic Grapher** > **Policy-Based Traffic**, the traffic flow is displayed in graphics, giving you an instant insight of traffic status. （**Figure 22-5**）

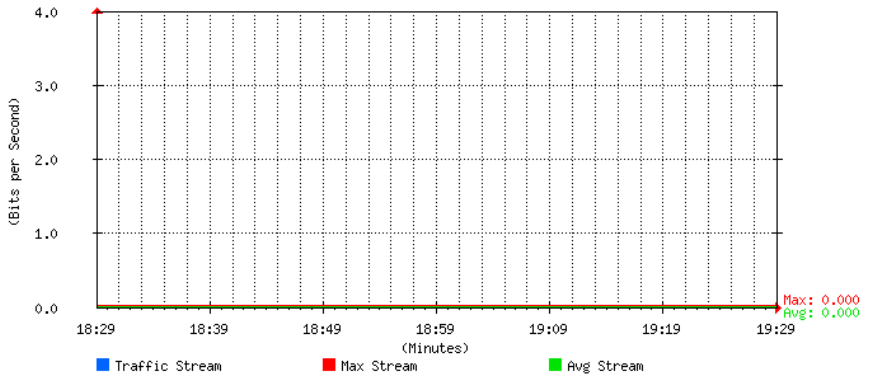
Years | Months | Weeks | Days | Hours | Minutes

Bits/sec | Bytes/sec | Utilization | Total

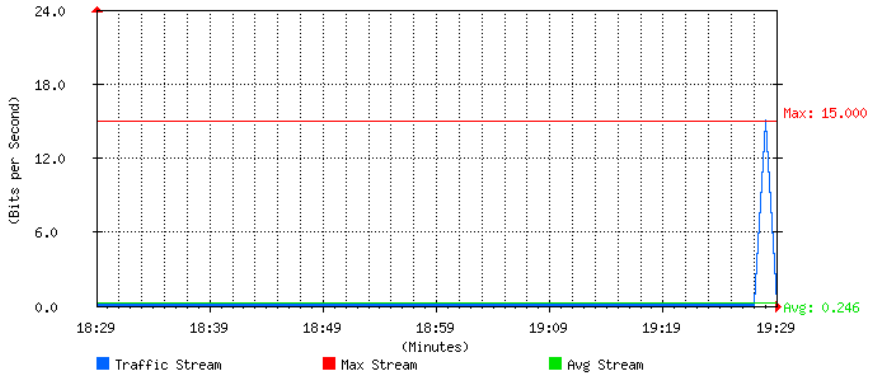
2010 / 12 / 24 19 : -- Search

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

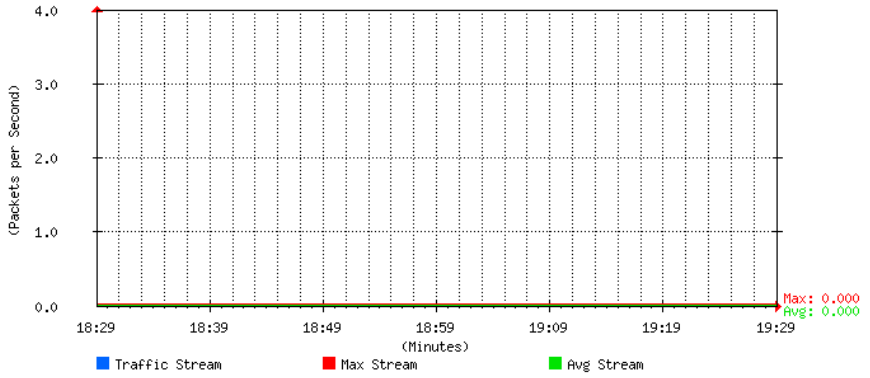
Downstream



Upstream



Received Packets



Transmitted Packets

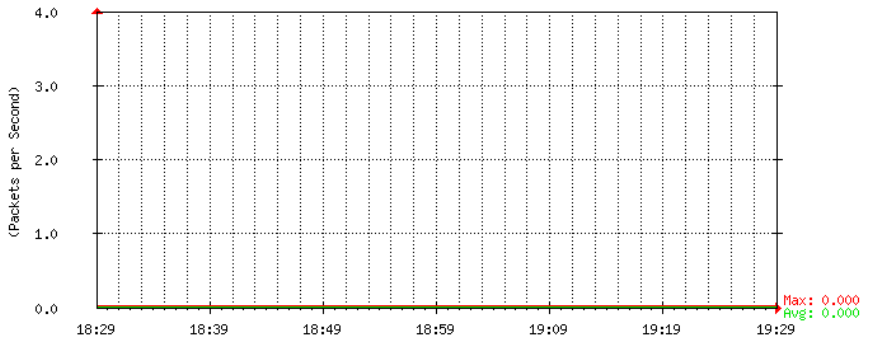


Figure 22-5 Statistics Screen

24.1.2 Creating a Policy to Restrict the Access to Specific Web Sites

Step 1. Go to **Web Filter** > **Configuration** > **Whitelist/ Blacklist/ File Extensions/ MIME/ Scritp/ Group** and then set as below: (**Figure 22-6, 22-7, 22-8, 22-9, 22-10**)

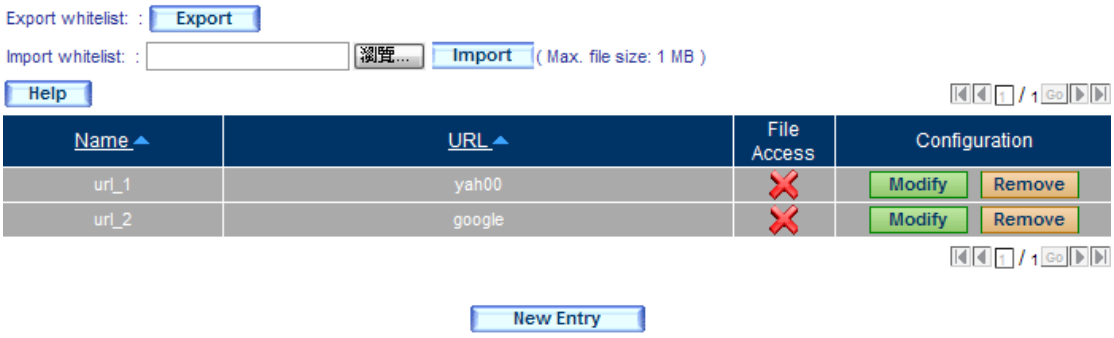


Figure 22-6 Whitelist Settings

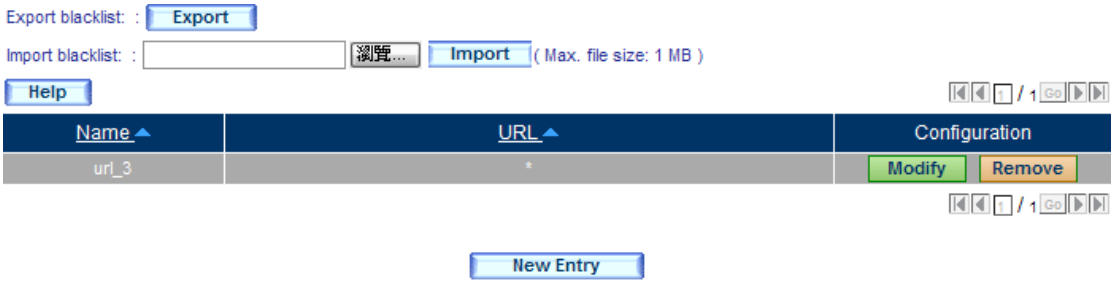


Figure 22-7 Blacklist Settings

Figure 22-8 File Extensions Settings

Figure 22-9 MIME / Script Settings

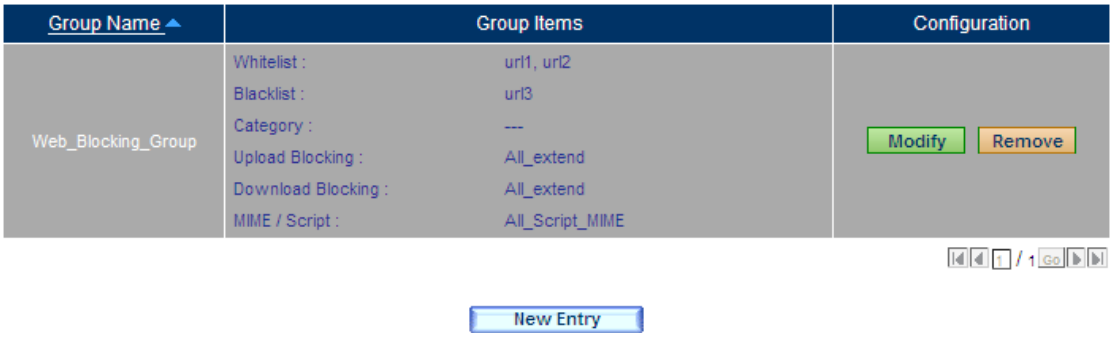


Figure 22-10 Group Settings

Step 2. Go to **Policy Object** > **Application Blocking** > **Settings** and then set as below:（**Figure 22-11, 22-12**）

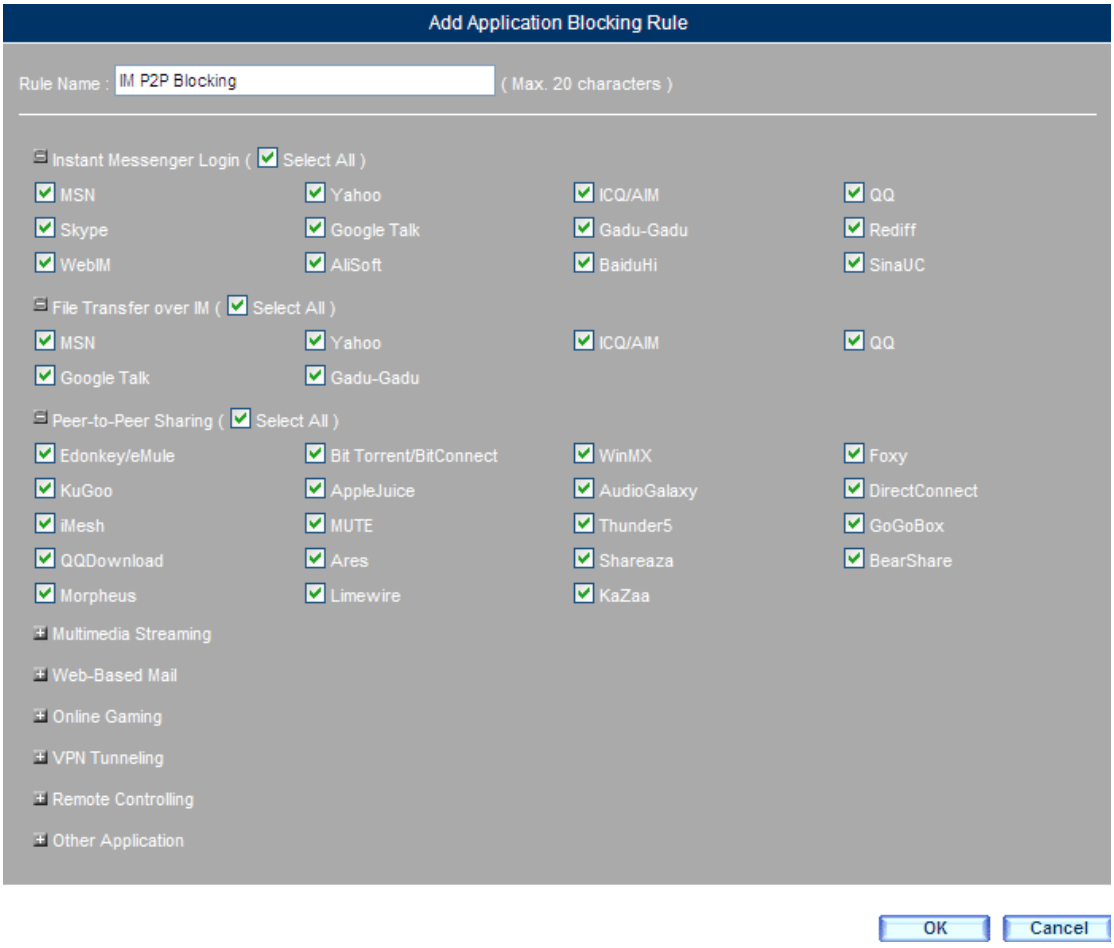


Figure 22-11 Application Blocking Settings

Figure 22-12 Setting Completed

Note:

1. Script blocking is used for blocking certain functional features of a web site, such as Java, cookie, and so on. One of the examples using these is stock exchange web sites.

2. Application Blocking is used for blocking Instant Messenger, Peer-to-Peer Application, Video/ Audio Application, Webmail, Game Application, Tunnel Application, Remote Control Application and other application.

Step 3. Go to **Policy Object > Address > WAN / WAN Group** and then set as below:（**Figure 22-13, 22-14**）

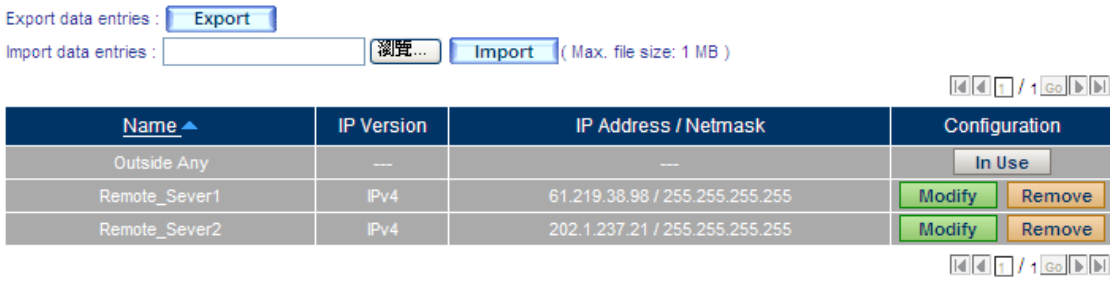


Figure 22-13 WAN Interface Setting

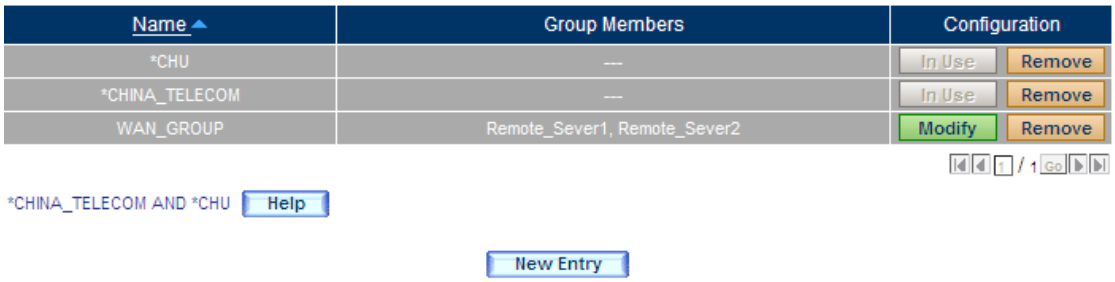


Figure 22-14 WAN Group Setting

Step 4. Go to **Policy** > **Outgoing** and then set as below: (**Figure 22-15**)

- Select the defined group from the **Destination Address** field.
- Select **Deny All** for **Action**.
- Click **OK**.

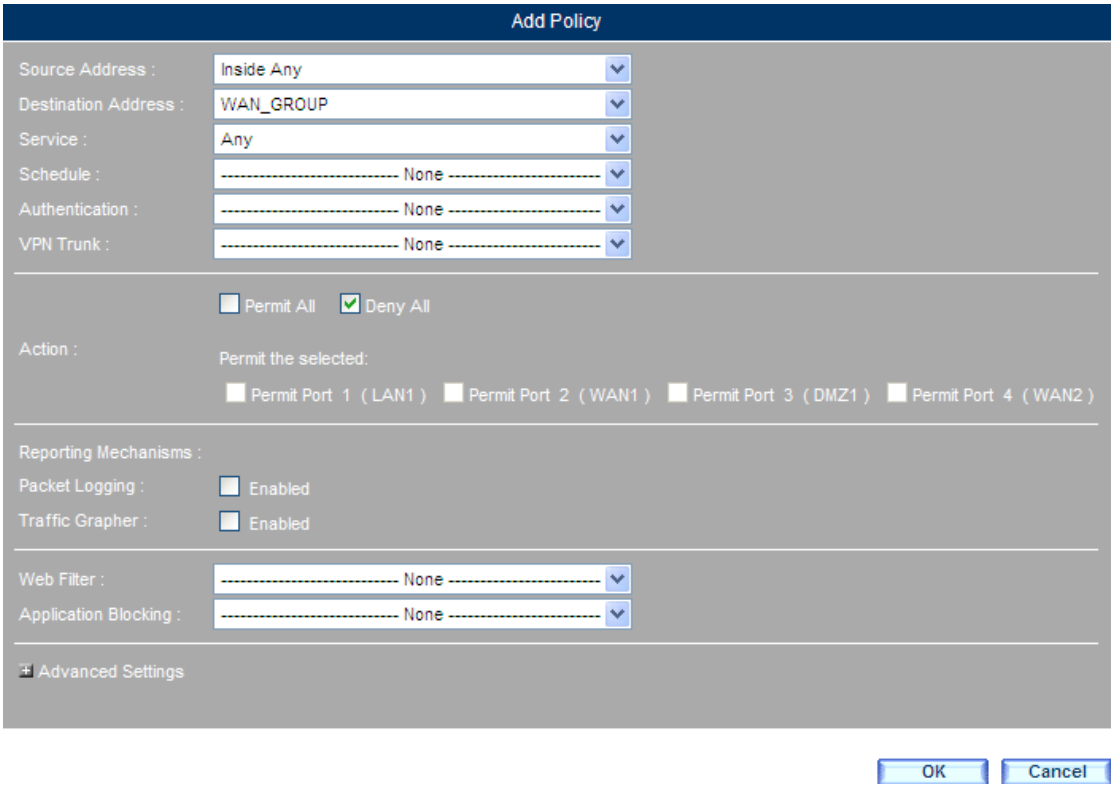


Figure 22-15 Creating an Outgoing Policy to Deny Access

Step 5. Go to **Policy** > **Outgoing** and then set as below: (**Figure 22-16**)

- Select the defined group from the **Web Filter** drop-down list.
- Select the defined rule from the **Application Blocking** drop-down list.
- Click **OK**. (**Figure 22-17**)

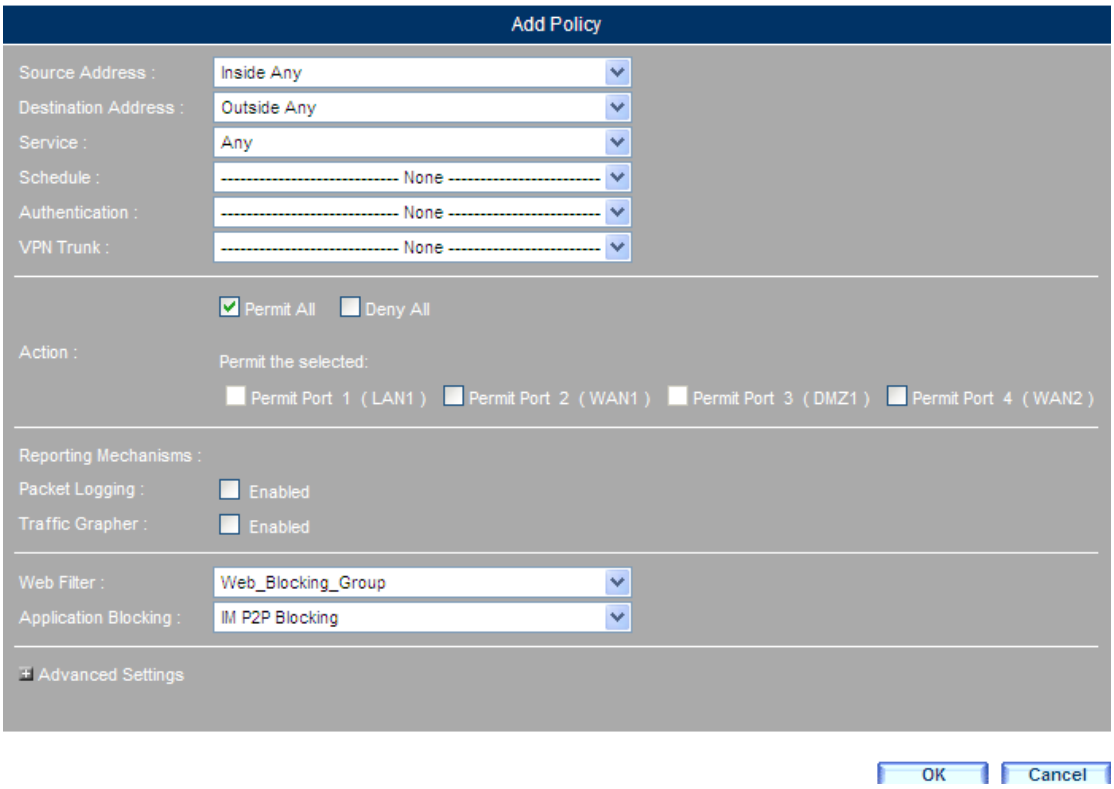


Figure 22-16 Applying Application Blocking to the Policy

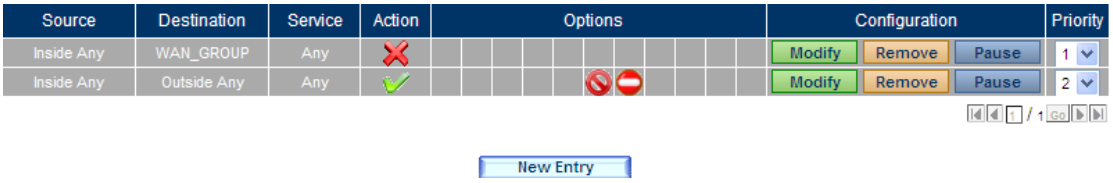


Figure 22-17 Policy Created

Note:

1. The **Deny ALL** feature of a policy can block the packets that meet the criteria. The IT administrator can adjust the order of this policy to the first rank so as to stop LAN users from accessing specific IP address.

24.1.3 Creating a Policy to Grant Internet Access to Only Authenticated Users on Schedule

Step 1. Go to **Policy Object** > **Schedule** > **Settings** and then set as below: (**Figure 22-18**)

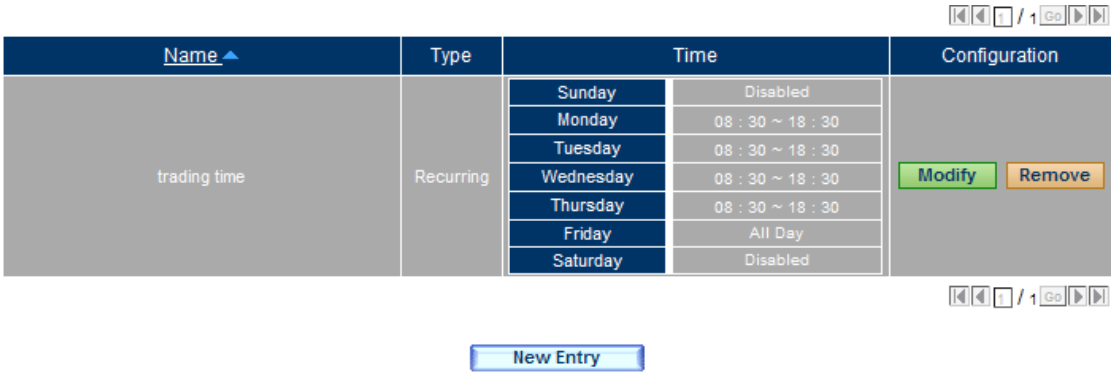


Figure 22-18 Shcedule Settings

Step 2. Go to **Policy Object** > **Authentication** > **Account / Group** and then set as below: (**Figure 22-19**)

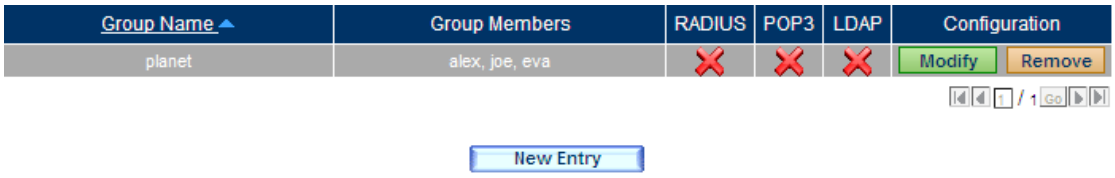


Figure 22-19 Authentication Setting

Step 3. Go to **Policy** > **Outgoing** and then set as below: (**Figure 22-20**)

- Select the defined group from the **Authentication** drop-down list.
- Select the defined rule from the **Schedule** drop-down list.
- Click **OK**. (**Figure 22-21**)

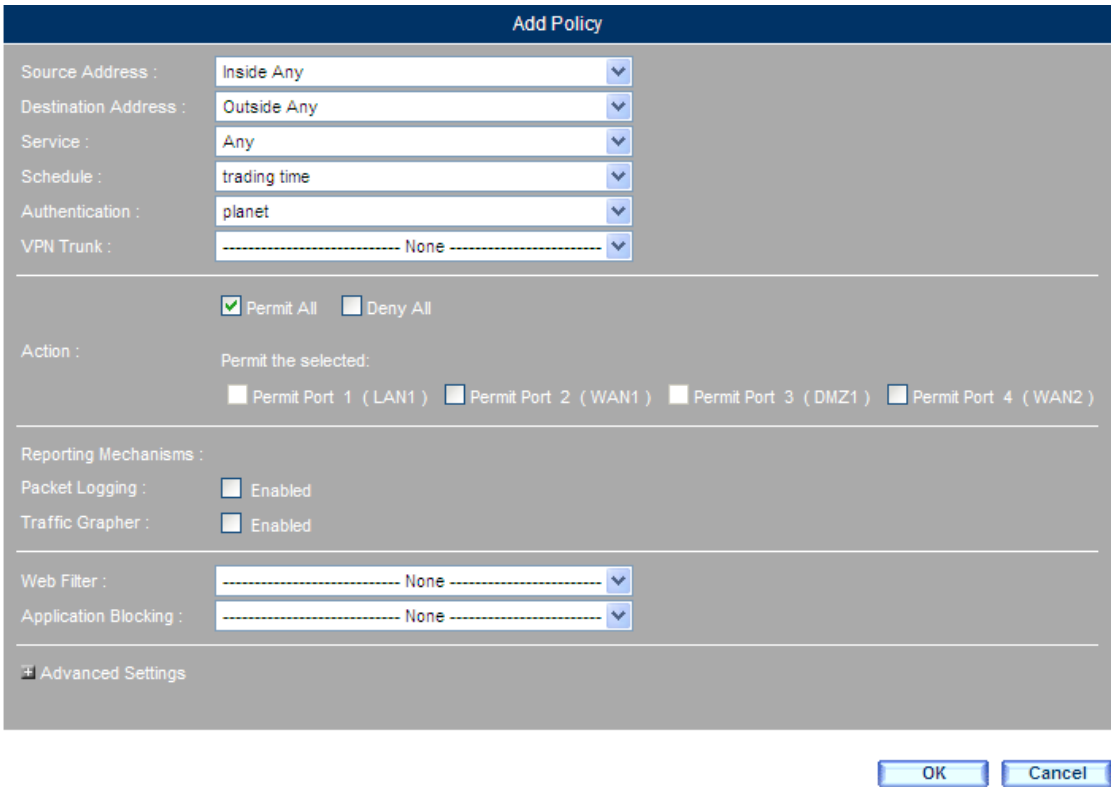


Figure 22-20 Applying the Schedule and Authentication to the Policy

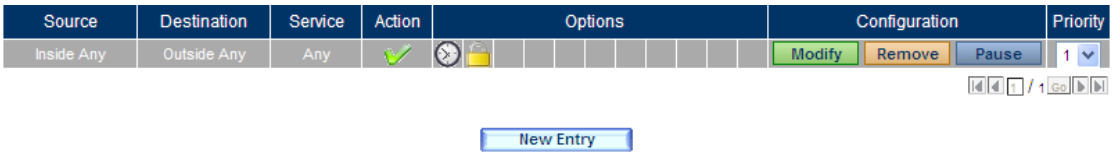


Figure 22-21 Policy Completed

24.1.4 Creating a Policy to Enable a Remote User to Control a LAN PC with Remote Control Software (pcAnywhere)

Step 1. Set up a computer to be remotely controlled; its IP address is 192.168.1.2.

Step 2. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below:

（**Figure 22-22**）

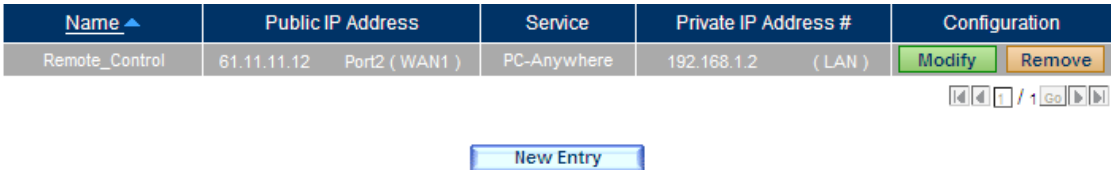


Figure 22-22 Virtual Server Settings

Step 3. Under **Policy** > **Incoming**, set as below: (**Figure 22-23**)

- Select the defined Virtual Server for **Destination Address.**
- Select PC-Anywhere(5629-5632) for **Service.**
- Click **OK**. (**Figure 22-24**)

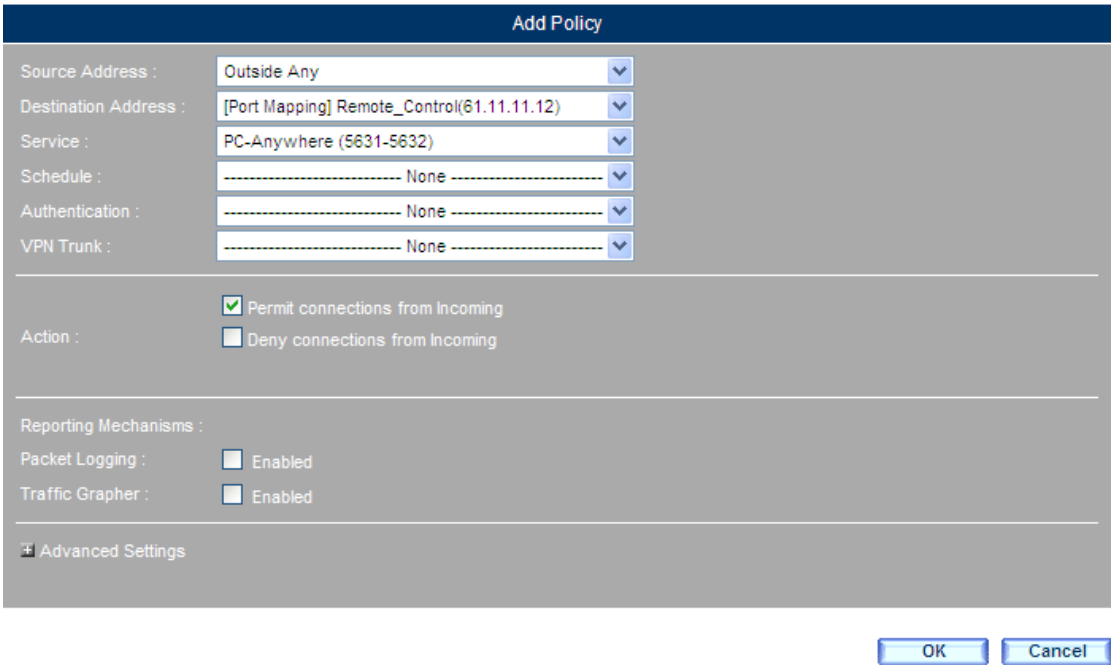


Figure 22-23 Creating an Incoming Policy to Enable LAN PC to be Remotely Controlled

Figure 22-24 Policy Completed

24.1.5 Creating a Policy to Limit the Bandwidth, Daily Total Traffic Amount and Maximum Concurrent Sessions of an Incoming Session to a FTP Server (A NAT Mode Example)

Step 1. Set up a FTP server in DMZ; the server IP address is 192.168.3.2. (The DMZ subnet addresses range from 192.168.3.1/24)

Step 2. Under **Policy Object** > **Virtual Server** > **Port Mapping**, set as below: （**Figure 22-25**）

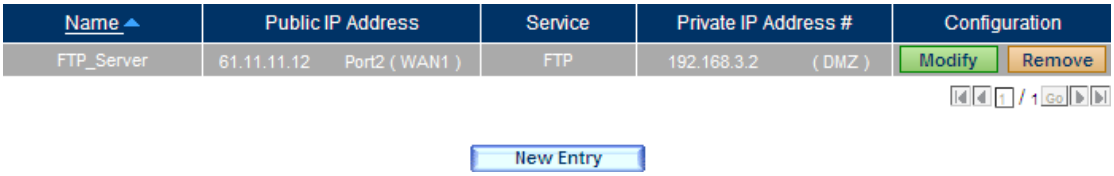


Figure 22-25 Virtual Server Settings

Note:

1. To avoid exposing your networks to hackers, it is strongly recommended not to select “ANY” for **Service** when configuring an incoming policy or WAN-to-DMZ policy.

Step 3. Go to **Policy Object** > **QoS** > **Settings** and then set as below: （**Figure 22-26**）

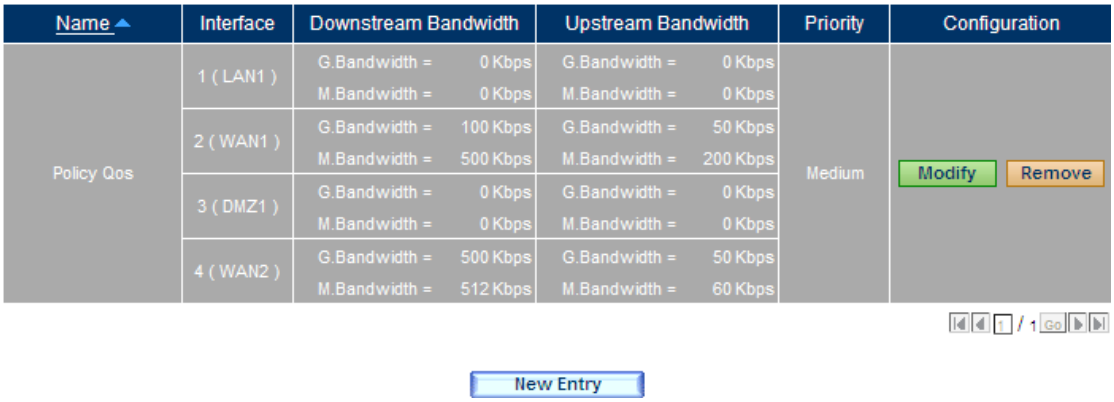


Figure 22-26 QoS Settings

Step 4. Go to **Policy > WAN to DMZ** and then set as below（**Figure 22-27**）

- Select the defined rule from the **Destination Address** drop-down list.
- Select FTP(18-21) from the **Service** drop-down list.
- Select the defined rule from the **QoS** drop-down list.
- Enter 100 in the **Max. Concurrent Sessions** field.
- Type 100000 in the **Traffic Quota Per Day** field.
- Click **OK**.（**Figure 22-28**）

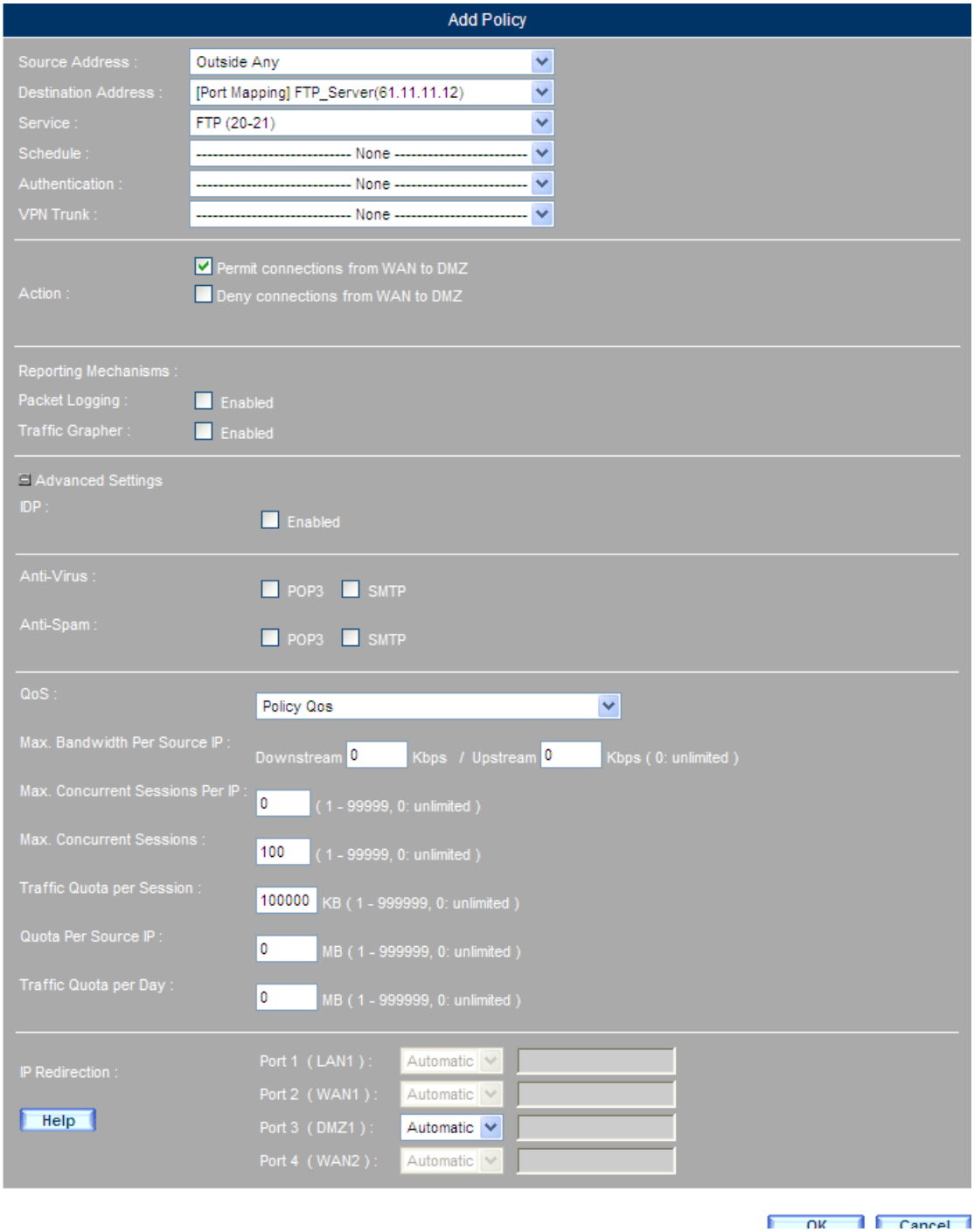


Figure 22-27 Creating a WAN-to-DMZ Policy

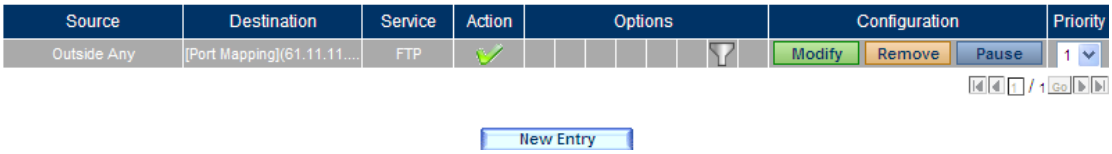


Figure 22-28 A WAN-to-DMZ Policy Created

24.1.6 Creating a Policy to Enable LAN / WAN Users to Have Email Access (A Transparent Mode Example)

Step 1. Set up a mail server in DMZ. Next, point it to the external DNS server and then set its IP address to 61.11.11.12.

Step 2. Under **Policy Object** > **Address** > **DMZ**, set as below:（**Figure 22-29**）

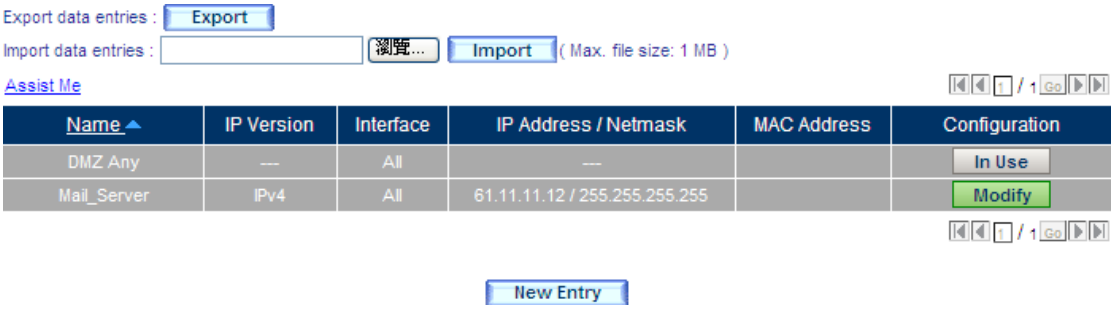


Figure 22-29 Mail Server Settings in Address

Step 3. Under **Policy Object** > **Service** > **Group**, set as below:（**Figure 22-30**）

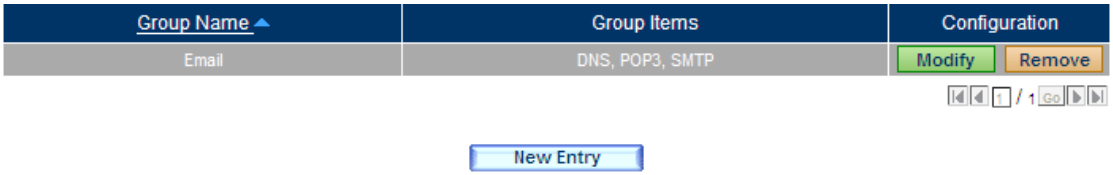


Figure 22-30 A Group Service with DNS, POP3 and SMTP Services

Step 4. Under **Policy** > **WAN To DMZ**, set as below: (**Figure 22-31**)

- Select the defined DMZ rule for **Destination Address.**
- Select the defined service for **Service.**
- Click **OK**. (**Figure 22-32**)

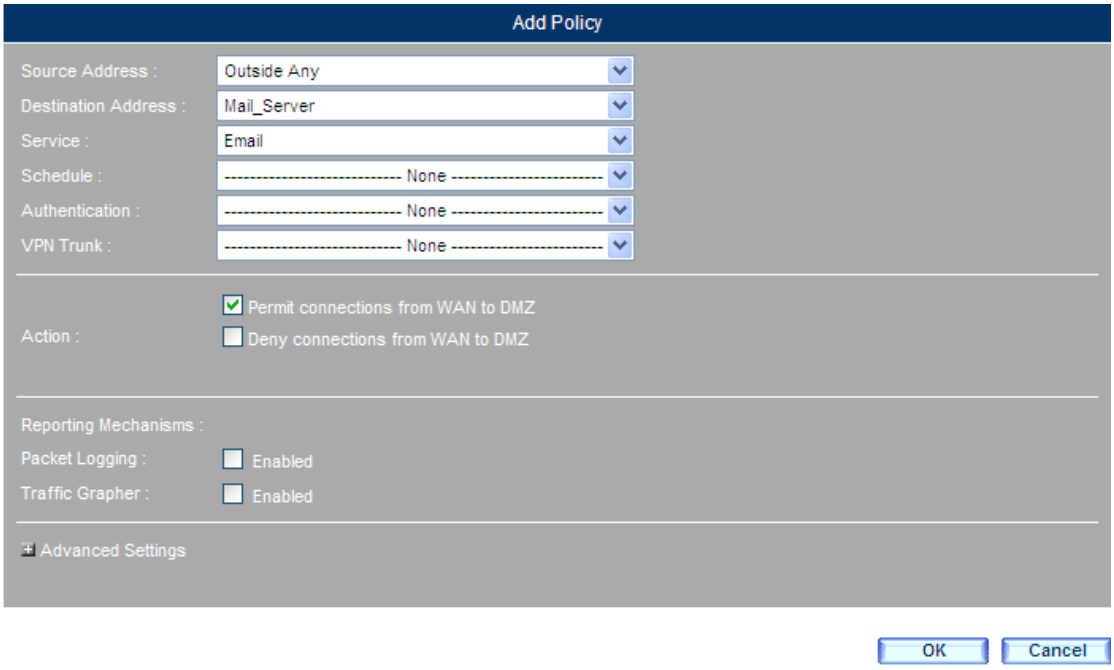


Figure 22-31 A WAN-to-DMZ Policy for Granting Email Access to WAN Users

Figure 22-32 A WAN-to-DMZ Policy for Granting Email Access to WAN Users Completed

Step 5. Under **Policy** > **LAN To DMZ**, set as below:（**Figure 22-33**）

- Select the defined DMZ entry for **Destination Address.**
- Select the defined service for **Service.**
- Click **OK**.（**Figure 22-34**）

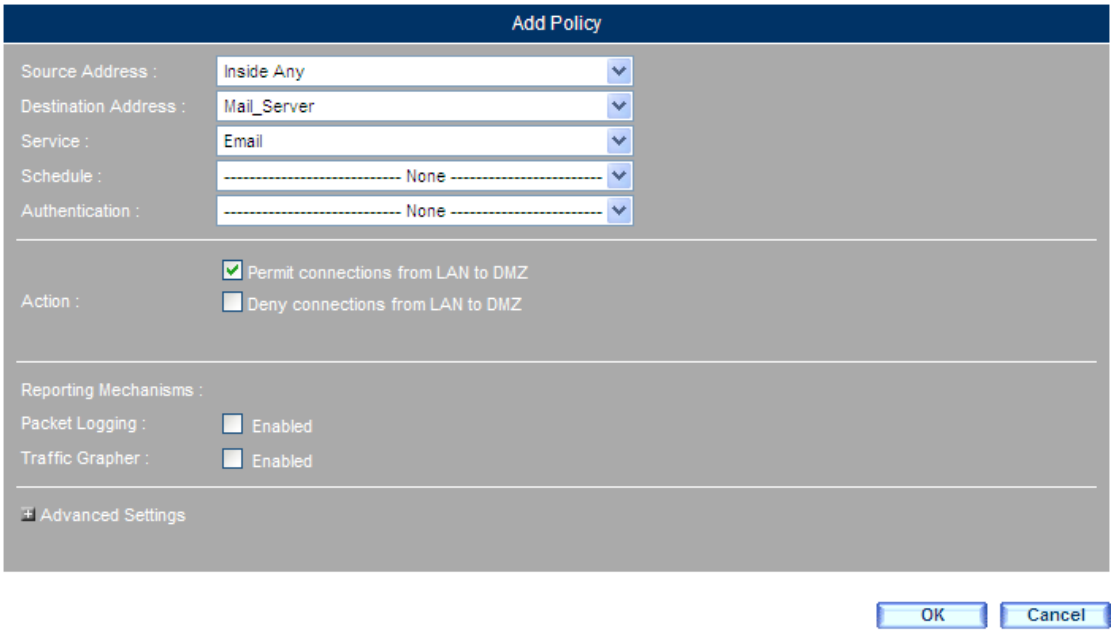


Figure 22-33 A LAN-to-DMZ Policy for Granting Email Access to LAN User

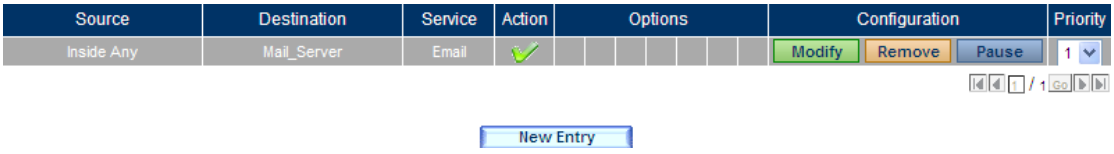


Figure 22-34 A LAN-to-DMZ Policy for Granting Email Access to LAN User Completed

Step 6. Under **Policy** > **DMZ To WAN**, set as below: (**Figure 22-35**)

- Select the defined rule for **Source Address.**
- Select the defined rule for **Service.**
- Click **OK**. (**Figure 22-36**)

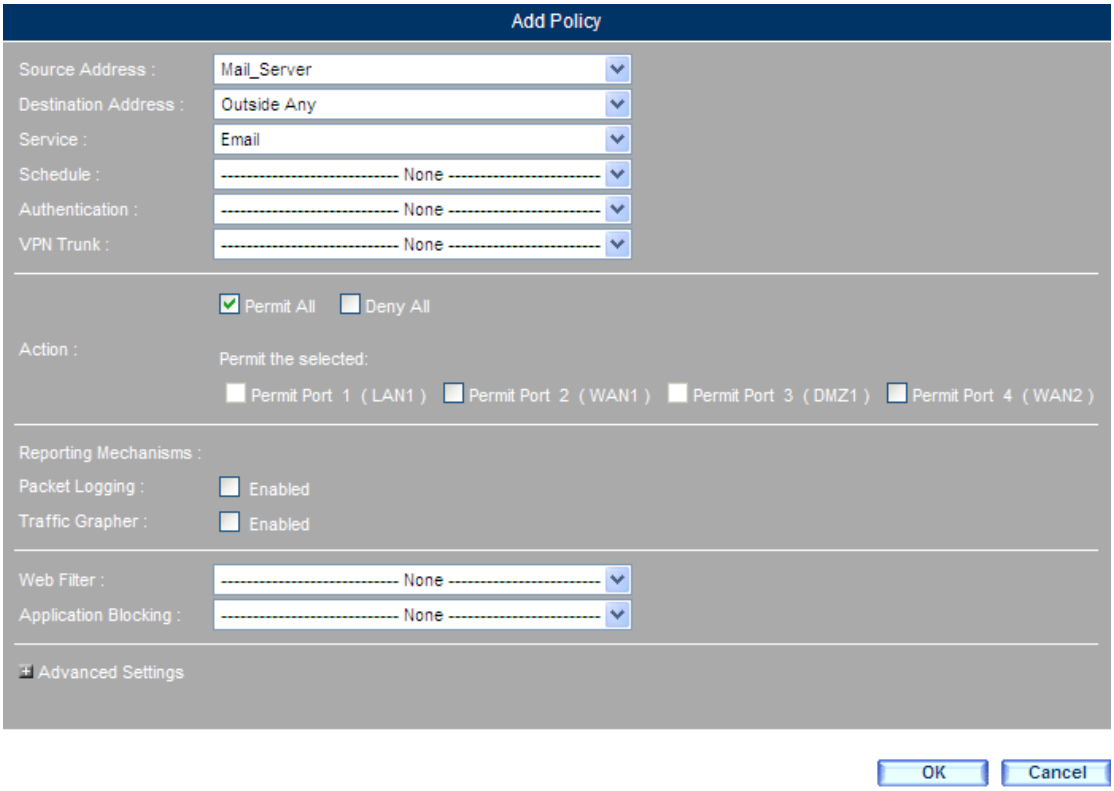


Figure 22-35 A DMZ-to-WAN Policy for Granting Email Access to WAN User

Figure 22-36 A DMZ-to-WAN Policy for Granting Email Access to WAN User Completed

Anomaly Flow IP

Chapter 25 Anomaly Flow IP

Once an anomaly traffic flow is detected, CS-2001 will take action to block the flow of packets. This protection ensures that the network remains operational, and consequently the business’s revenue generating opportunities are left undisturbed.

25.1 Example

25.1.1 Configuration for Alerts and the Blocking of Internal

DDoS Attacks

Step 1. Go to **System** > **Configuration** > **Settings** and then configure the settings under the **Email Notification Settings** section.

Step 2. Go to **System** > **Configuration** > **SNMP** and then configure the settings under the **SNMP Trap Settings** section.（**Figure 23-1**）

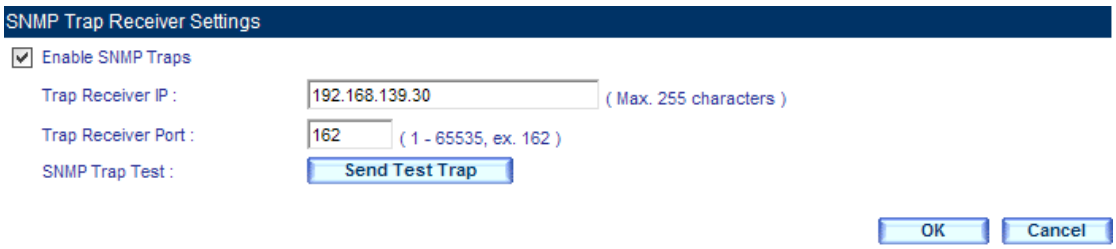


Figure 23-1 SNMP Trap Settings

Step 3. Go to **Anomaly Flow IP > Settings** and then set as below: (**Figure 23-2**)

- Enter the **Traffic Threshold per IP**. (The default value is 100)
- Tick **Enable Anomaly Flow IP Blocking** and then type the **Blocking Time**. (The default value is 60)
- Tick **Enable E-Mail Alert Notification.**
- Tick **Enable SNMP trap alerts.**
- Tick **Enable NetBIOS notification** and then type the **Administrator's IP Address.**
- Click **OK**.

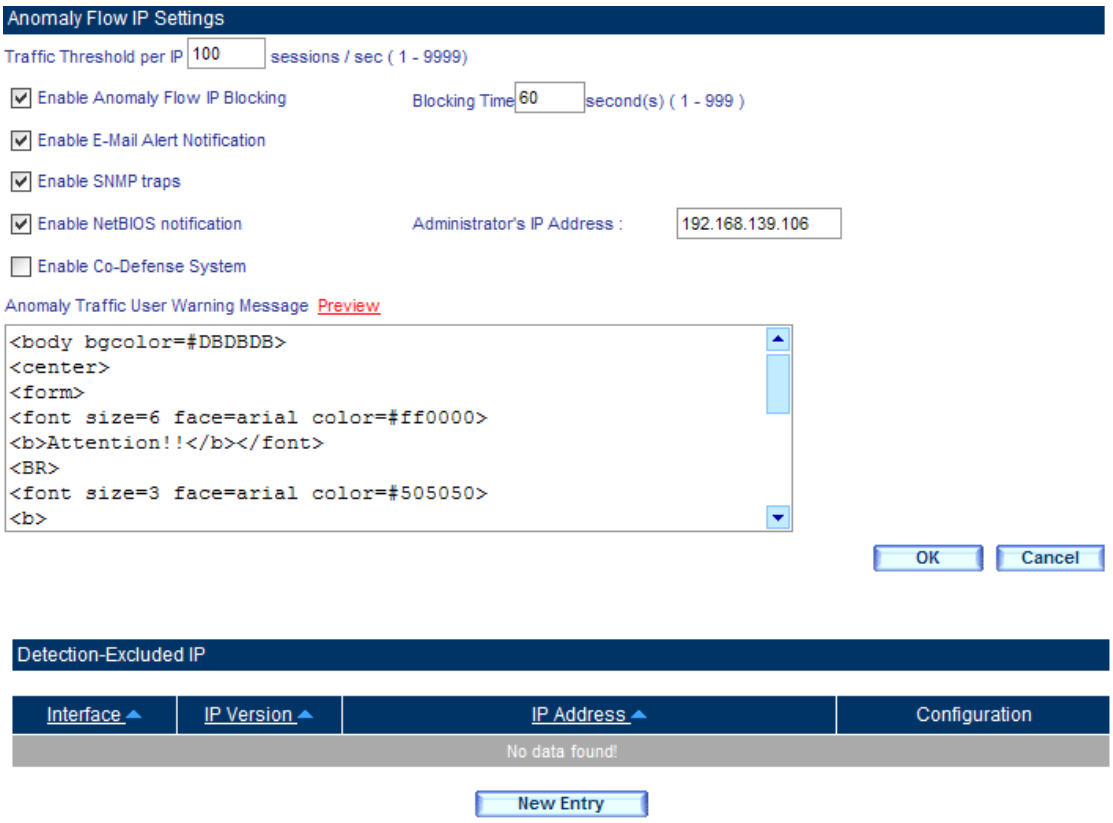


Figure 23-2 Anomaly Flow IP Setting

Note:

1. **Detection-Excluded IP** can be used for excluding specific IPs from detection.
2. Users whose PCs emit anomaly traffic flows can receive a customizable message in their browser to alert them about the incident.

Step 4. When a DDoS attack occurs, CS-2001 generates a corresponding log under **Anomaly Flow IP > Virus-infected IP**, and if **NetBIOS Notification** is enabled, sends a NetBIOS broadcast to both the victim user and IT administrator to warn about the attack.（**Figure 23-3**）

Traffic Threshold per IP : 100 sessions / sec

1 / 10 Go

Interface	Protocol	Virus-Infected IP	MAC Address	Alarm Time
LAN	IPv4	UMG	00:73:07:20:e6:5c	2010-12-09 19:05:59
LAN	IPv4	TEST-PC	00:50:bf:12:26:61	2010-10-11 15:17:27
LAN	IPv4	192.168.0.20	00:d0:89:06:b1:c3	2010-10-11 15:19:54
LAN	IPv4	192.168.0.210	00:30:4f:6c:19:8b	2010-10-11 15:01:58
LAN	IPv4	192.168.0.210	00:30:4f:6c:19:8b	2010-10-11 15:07:30
LAN	IPv4	192.168.0.250	00:d0:89:06:b1:c3	2010-10-11 14:59:16
LAN	IPv4	MYPC-1	00:18:de:28:7b:f0	2010-10-11 14:32:39
LAN	IPv4	169.254.132.91	00:18:de:28:7b:f0	2010-10-11 13:55:31
LAN	IPv4	QUAD-PC	00:30:4f:7f:ec:2e	2010-10-11 13:15:45
LAN	IPv4	ENM10FLAB01	00:1f:e1:23:f6:08	2010-10-11 13:26:42
LAN	IPv4	888TIGER-BCD55E	00:1a:73:27:03:92	2010-10-11 12:43:28
LAN	IPv4	169.254.78.175	00:1a:73:27:03:92	2010-10-11 12:40:56
LAN	IPv4	0.0.0.0	00:1a:73:27:03:92	2010-10-11 11:39:29
LAN	IPv4	ENMLAB-PC	00:1a:73:27:03:92	2010-10-11 11:39:29
LAN	IPv4	YOUR-0886792B95	00:13:ce:05:43:06	2010-10-11 15:05:17
LAN	IPv4	0.0.0.0	00:13:ce:05:43:06	2010-10-11 10:46:07
LAN	IPv4	NASD800504D	00:04:29:01:77:ff	2010-10-11 15:20:00
LAN	IPv4	192.168.0.131	00:30:4f:83:82:e4	2010-10-11 15:19:31
LAN	IPv4	140.117.176.222	00:03:c9:e7:ef:ff	2010-10-08 23:09:16
LAN	IPv4	ENM-EVAN	00:22:4e:e0:00:0c	2010-10-08 10:20:42

1 / 10 Go

Clear Download

Figure 23-3 Virus-Infected IP Addresses

Step 5. If running SNMP Trap Watcher, you will be informed of an anomaly flow (or attack), if any, as long as **SNMP trap alerts** is enabled in **System > Configuration > SNMP.** **(Figure 23-7)**

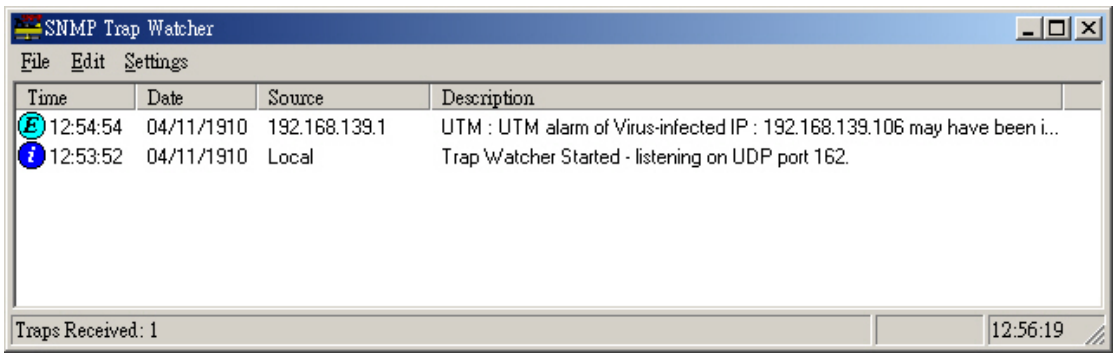


Figure 23-7 Alerts Received by the SNMP Client Software

Step 6. Internal users will see an alert message upon opening a web browser after being infected by a computer virus. CS-2001 limits virus-infected users' bandwidth to a minimum in order to oblige users to take action to remove virus. Note: The alert message merely appears to virus-infected users at the very first time to open a web browser after the infection.（**Figure 23-8**）

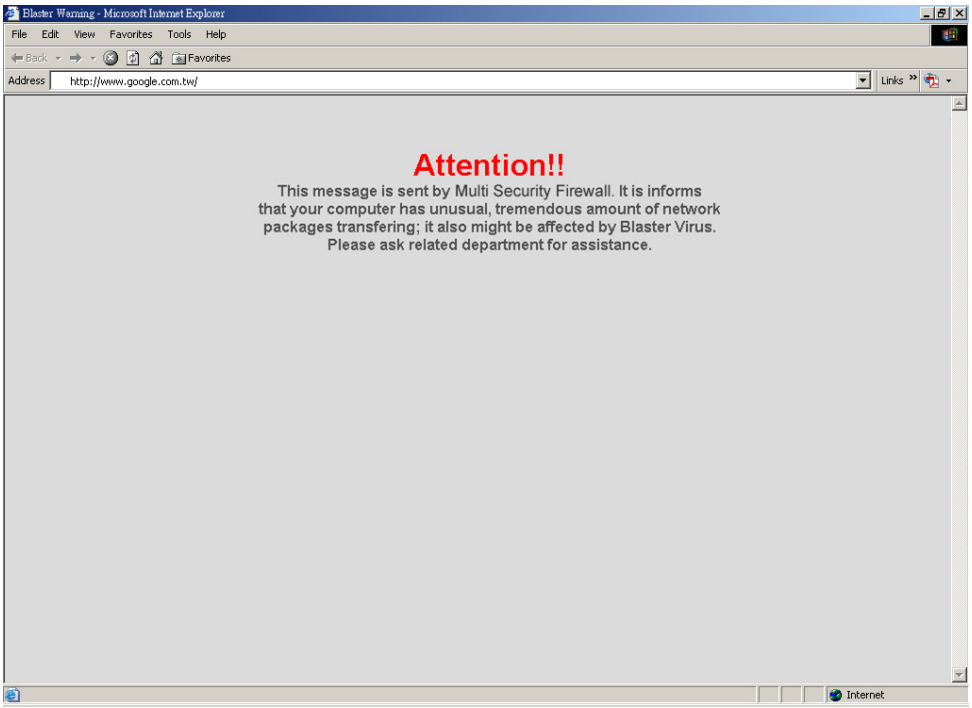


Figure 23-8 An Alert Message Shown to a Virus-Infected User

Advance

Chapter 26 Inbound Balancing

The CS-2001 provides enterprises with Inbound Load Balancing. It ensures uninterrupted access for external users to the company's servers. If one WAN link fails, incoming traffic will be redirected to another WAN link. In addition, inbound flows can be distributed to each port according to the regulated weighting and priority of each port, ensuring the quality of the connection.

Terms in Inbound Balancing

Domain Name

- Refers to an address that is registered at an ISP. An IP address like 198.68.20.78 is not easy to memorize, therefore, domain names intend to represent IP addresses with meaningful and more easily readable English hostnames, such as ccu.edu.tw, planet.com.tw.
- We are all familiar with website addresses. For example if we want to browse yahoo's website we just type in www.yahoo.com into a browser to see the website. In reality, yahoo's website address is the IP address 66.218.71.84. But with the help of a DNS server acting as an intermediary, the website address is mapped to the IP address.

Enable DNS Zone

- Allows users to activate DNS for inbound balancing.（**Figure 24-1**）

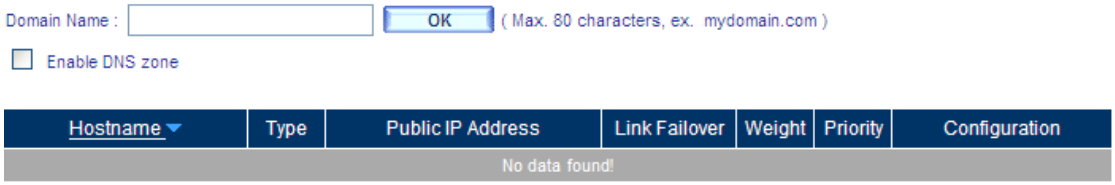


Figure 24-1 Inbound Balancing DNS Settings

DNS Zone Configuration

- Register nu.net.tw (used here as an example only) as the domain name.
- Supposing the following IP address range were applied for:
  - 61.11.11.10 ~ 61.11.11.14。
  - 211.22.22.18 ~ 211.22.22.30。
- Configure the primary server as:
  - Host Name：dns1.nu.net.tw。
  - IP Address：61.11.11.11。
- Configure the secondary server as:
  - Host Name：dns2.nu.net.tw。
  - IP Address：211.22.22.22。

DNS Record Type

- **Address (A)**
  - This is used for mapping up IP addresses and domain names.（**Table 24-1**）

Domain Name	Type	IP Address
host1.nu.net.tw	A	61.11.11.12
host2.nu.net.tw	A	61.11.11.13
host2.nu.net.tw	A	211.22.22.23

Table 24-1 Domain Name and IP Address Mapping Table

- Domain names can be mapped to more than one IP address. The table above indicates that host2 is mapped to two IP addresses, so it lists out two entries corresponding to host2. Each DNS query can return a different address if there is more than one address record. The returned result can be chosen according to an address-sorting or a round-robin list. ("**A**" represents IP address.)

■ **Canonical NAME (CNAME)**

- Type CNAME is used for mapping aliases to domain names.（**Table 24-2**）

Domain Name	Type	IP Address
host23.nu.net.tw	A	61.11.11.14
host5.nu.net.tw	CNAME	host23.nu.net.tw

Table 24-2 Domain Name CNAME Mapping Table

- The table above indicates that host5.nu.net.tw (alias) is mapping to host23.nu.net.tw (domain name). Thus, ping host5.nu.net.tw and then you'll get the result of 61.11.11.14.

■ **Mail eXchanger(MX)**

- MX, also known as "Mail eXchanger", is a type of DNS record especially designed for mail services. （**Table 24-3**）

Domain Name	Type	IP Address
host25.nu.net.tw	A	211.22.22.24
mail.nu.net.tw	MX	host25.nu.net.tw

Table 24-3 Domain Name and Mail eXchanger Mapping Table

- Under DOS mode, type **nslookup -type=MX mail.nu.net.tw**, you will find that mail.nu.net.tw is mapping to host25.nu.net.tw (the mail eXchanger) and its IP address is 211.22.22.24.

"nslookup" is the command for locating DNS records on a DNS server.

"-type" defines the DNS type.

"mail.nu.net.tw" is the inquired DNS name

- Supposing a user wants to send an email to mary@mail.nu.net.tw. The user is using test.com.tw as its SMTP server. The DNS records will be queried on this server to determine where to send the email destined for mail.nu.net.tw. The following table shows the MX record resulted from the query:（**Table 24-4**）

Domain Name	Type	IP Address
host3.nu.net.tw	A	61.11.11.10
mail.nu.net.tw	MX	host3.nu.net.tw

Table 24-4 MX Record of Querying mail.nu.net.tw

- It can be inferred from the table above that emails will be transferred to host3.nu.net.tw via the SMTP protocol.

- **Sender Policy Framework(SPF)** : SPF, serves as an authentication mechanism, rejects forged addresses in the SMTP MAIL FROM (Return-Path). It uses DNS TXT records to identify the identity of a sender, efficiently preventing spam emails and phishing.
  - MX shoulders the responsibility for directing emails depending on the DNS record. If a mail server is required to be replaced, then simply by changing the DNS MX record will allow the mail service to remain in operation. When an email is received from a different domain, the mail server will check if the sender's mail server IP is on the SPF list or not.
- (AAAA) IPv6 : Like IPv4 A(Address), (AAAA) IPv6 is used for mapping up IP addresses and domain names.
  - IPv6 is designed to succeed IPv4. It has a larger address space than IPv4. IPv6 uses 128 bits whereas IPv4 uses only 32 bits.（**Table 24-5**）

Domain Name	Type	IP Address
host33.nu.net.tw	AAAA	FEC0::2AA:FF:FE3F:2A1C

Table 24-5 Domain Name and IP Address Mapping Table

Reverse

- It reverses a DNS lookup by using its IP address. DNS lookup is distinguished into forward DNS lookup and reverse DNS lookup. Forward DNS lookup serves as a translator to transform a hostname address (e.g. www.yahoo.com) into a IP address. On the other hand, reverse DNS lookup does the reverse.
- For IPv4, the process of reverse resolving an IP address uses the pointer DNS Record type(PTR record). For example, an address(A) record for host1.nu.net.tw points to the IP address 61.11.11.12. In

pointer records of the reverse database, this IP address is stored as the domain name 12.11.11.61.in-addr.arpa pointing back to its designated hostname.

- IPv6 uses PTR record as well. For example, host33.nu.net.tw points to FEC0::2AA:FF:FE3F:2A1C (FEC0:0000:0000:0000:02AA:00FF:FE3F:2A1C), in pointer records of the reverse database, this IP address is stored as the domain name C.1.A.2.F.3.E.F.F.F.0.0.A.A.2.0.0.0.0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.INT. pointing back to its designated hostname.

- For example, using the **nslookup** command to verify whether DNS lookup functions normally. The process is as follows:

C:\>nslookup host1.nu.net.tw ---------->forward DNS lookup
Server: dns.hinet.net
Address: 168.95.1.1

Name：host1.nu.net.tw
Address：61.11.11.12

C:\>nslookup 61.11.11.12 ---------->reverse DNS lookup
Server: dns.hinet.net
Address: 168.95.1.1

Name：host1.nu.net.tw
Address：61.11.11.12

The result points out that 61.11.11.12 points to host1.nu.net.tw

Load Balancing Mode

- **Round-Robin**: According to the set weight and priority, the access is distributed in a cyclic fashion over the available links.
- **Redundancy**: This mode only functions when one of the links gets disconnected.

Further Description

DNS pointers are used to indicate which DNS server holds all the associated DNS records for a domain. Any specific information can be obtained from the DNS server, such as the physical address of a website or mail server. Thus, the DNS server must be reliably connected to the internet and accurate DNS records must be maintained.

According to international practice, a DNS system is consisted of at least two DNS servers. This ensures that DNS queries are still obtainable if one of the servers goes down. Thereby it ensures that your domain name and all the associated services remain accessible for global Internet users.

Requirements for setting up a name server are as follows:

- Register nu.net.tw as a domain name.
- Set the primary name server as 61.11.11.11 and domain name as dns1.nu.net.tw.
- Set the secondary name server as 211.22.22.22 and domain name as dns2.nu.net.tw.
- Apply to a local ISP for two fixed T1 or ADSL connections.
- Servers required for address resolution:
  - Web Server: www.nu.net.tw
  - Mail Server: mail.nu.net.tw

Apply to local ISP for two ADSL or leased line connections with fixed IPs:

- Allocated IP addresses are as followed: (used here as an example only):
  - 61.11.11.10 ~ 61.11.11.14。
  - 211.22.22.18 ~ 211.22.22.30。

Use the IP addresses within the range mentioned above when registering a desired domain name at a local ISP:

- Primary Name Server:
  - Host Name：dns1.nu.net.tw。
  - IP Address：61.11.11.11。
- Secondary Name Server:
  - Host Name：dns2.nu.net.tw。
  - IP Address：211.22.22.22。

Note:

1. The DNS must point to the fixed IPs.

Under **Advance > Inbound Balancing > Settings**, configure DNS settings as listed below:（**Table 24-6**）

Domain Name	Type	IP Address	Reverse	Weight	Priority
nu.net.tw	A	61.11.11.11	O	1	1
nu.net.tw	A	211.22.22.22	O	1	2

Table 24-6 Domain Name and IP Address Mapping Table

The Secondary DNS server can act as a substitute if the primary DNS server develops a fault by allowing the domain name to remain functioning.

According to table 24-6, use nslookup command to verify the result of forward DNS lookup and reverse DNS lookup:

C:\>nslookup nu.net.tw
Server: dns.hinet.net
Address: 168.95.1.1

Name: nu.net.tw
Addresses: 61.11.11.11, 211.22.22.22 ---------->look up for Address (Forward DNS lookup)

C:\>nslookup 61.11.11.11
Server: dns.hinet.net
Address: 168.95.1.1

Name: nu.net.tw ------------------------------>look up for real domain name(forward DNS lookup)
Address: 61.11.11.11

Configure DNS settings as listed below:（**Table 24-7**）

Domain Name	Type	IP Address	Weighting	Priority
web.nu.net.tw	A	61.11.11.11	1	1
web.nu.net.tw	A	211.22.22.22	2	2
www.nu.net.tw	CNAME	web.nu.net.tw	--	--

Table 24-7 CNAME Record of www.nu.net.tw

According to table 24-7, use nslookup command to verify the result of forward DNS lookup and reverse DNS lookup:
C:\>nslookup
Default Server：dns.hinet.net
Address：168.95.1.1

> server 61.11.11.11 ---------->switch to your DNS server
Default Server：web.nu.net.tw
Address：61.11.11.11

> www.nu.net.tw ---------->look up for real domain name
(forward DNS lookup)
Server：web.nu.net.tw
Address：61.11.11.11

Name：web.nu.net.tw ------>the real domain name that www.nu.net.tw corresponds to
Addresses：61.11.11.11, 211.22.22.20---->corresponding IP addresses of web.nu.net.tw
Aliases：www.nu.net.tw ----------> CNAME of web.nu.net.tw

From the above we can conclude that web.nu.net.tw is the real domain name mapping to the IP addresses. On the other hand, www.nu.net.tw, a CNAME of web.nu.net.tw, offers a query function and redirection to web.nu.net.tw.

As seen from table 24-7, it can be inferred that when browsing www.nu.net.tw, visitors are directed to different servers according to their browsing sequence.
The 1st user accesses the server via 61.11.11.11.
The 2nd user accesses the server via 211.22.22.22.
The 3rd user accesses the server via 211.22.22.22.
(Round-Robin priority distribution cycle finished)
The 4th user accesses the server via 61.11.11.11.
(Round-Robin priority distribution cycle has restarted)
The 5th user accesses the server via 211.22.22.22.
The 6th user accesses the server via 211.22.22.22.

When the 3rd user enters www.nu.net.tw and the weight priority of server 61.11.11.11 exceeds the original setting "1", then the Inbound Load Balance will distribute the 3rd user to the server 211.22.22.22 with weight priority of 2. When finished all the weight priority allocation, the system will restart the weight priority distribution again. This is how the load balancing mechanism can allocate the visitors to the web server www.nu.net.tw in a round robin fashion according to the weighted and priority values.

As seen from table 24-8, the lower the priority value, the higher priority it gets. For example, the user A wants to send an email to mary@mail.nu.net.tw, a mail server (hinet.net.tw) served as a SMTP server decides where and how to send the email by inquiring the target DNS server. The MX record obtain from querying email.nu.net.tw is shown below:（**Table 24-8**）

Domain Name	Type	Address	Reverse	Weight	Priority
mail.nu.net.tw	MX	smtp1.nu.net.tw	X	--	1
mail.nu.net.tw	MX	smtp2.nu.net.tw	X	--	2

Table 24-8 MX Record of mail.nu.net.tw

A priority number of "1" represents the highest level of priority, therefore the server will first try to deliver emails to smtp1.nu.net.tw. If the delivery fails, then the emails will be directed to smtp2.nu.net.tw as it is the next highest priority.

26.1 Example

No.	Application Environment	Page
26.1.1	Creating an A Record to Load Balance a Web Server Using the Backup Mode	**710**
26.1.2	Creating an A Record to Load Balance a Web Server Using the Round-Robin Mode	**717**
26.1.3	Creating a CNAME Record to Load Balance a Web Server Using the Round-Robin Mode	**724**
26.1.4	Creating a MX Record to Load Balance a Mail Server Using the Round-Robin Mode	**732**

Requirements
The DNS domain name has to correspond to the static IP.

Apply for two static IP ADSL lines.

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing mode) and connect it to the LAN which is using 192.168.1.x/24.

Configure Port2 as WAN1 (61.11.11.11). IP range: 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 (211.22.22.22). IP range:211.22.22.18 to 211.22.22.30.

Apply for a domain name e.g. supportplanet.com.tw (select your own domain name) from an ISP.
Set the DNS settings as below for the domain name:

The Primary Name Server
Host Name : dns1.supportplanet.com.tw
IP address : 61.11.11.11

The Secondary Name Server
Host Name : dns2.supportplanet.com.tw
IP address : 211.22.22.22

26.1.1 Creating an A Record to Load Balance a Web Server

Using the Backup Mode

Step 1. Go to **Advance** > **Inbound Balancing** > **Settings** and proceed with the following settings:

- Click **New Entry**.（**Figure 24-2**）
- Type the domain name.
- Tick **Enable DNS zone.**
- Click **New Entry**.（**Figure 24-3**）
- Select **A (Address)** for **DNS Record Type.**
- Type www in the **Host Name** field.
- **Real IP Address**, select **WAN1** and then enter 61.11.11.11 in the field.
- Select Round-Robin for **Load Balancing Mode**.
- Click **OK.**
- Click **New Entry** again.（**Figure 24-4**）
- Select **A(Address)** for **DNS Record Type.**
- Type www in the **Host Name** field.
- For **Real IP Address**, select WAN2 and then type 211.22.22.22.
- For **Load Balancing Mode**, select Backup and then select WAN1 from the drop-down list.
- Click **OK**.（**Figure 24-5**）

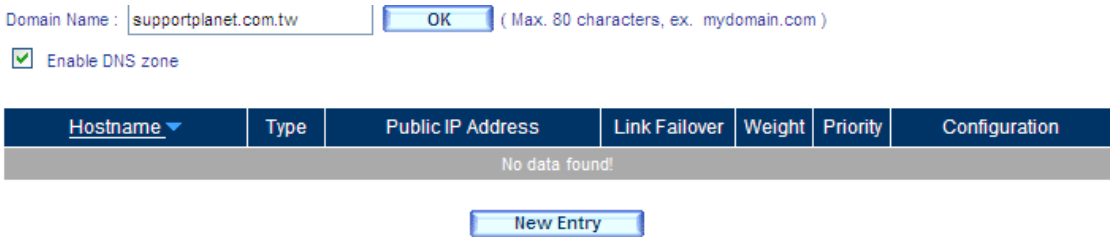


Figure 24-2 Adding a New Domain Name

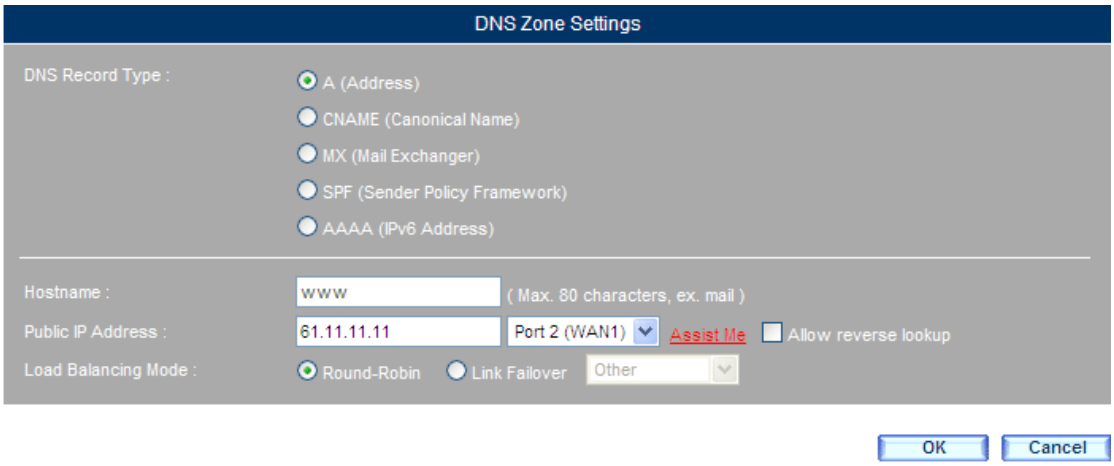


Figure 24-3 The First Inbound Balance Configuration

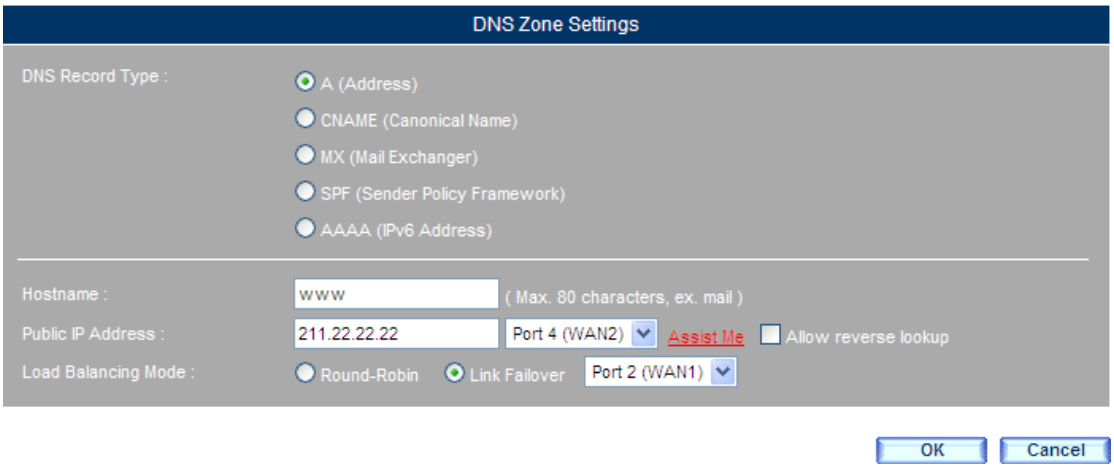


Figure 24-4 The Second Inbound Balance Configuration

Figure 24-5 The Completed Settings

Note:

1. If @ is entered in the **Hostname** field, then it will be the defined domain name. In this example, it is supportplanet.com.tw.
2. "." indicates fully qualified domain name (FQDN). For example, if www is entered in the **Hostname** field, then it will be www.supportplanet.com.tw. If www.supportplanet.com.tw is entered and plus a "." in the end, then it will be www.supportplanet.com.tw.supportplanet.com.tw.
3. Before enabling reverse lookup, make sure the IP class is Class A, Class B or Class C. If not, please apply to the ISP for the reverse lookup service.

Step 2. Go to **Policy Object** > **Virtual Server** > **Port Mapping** and then set as below:（**Figure 24-6, 24-7**）

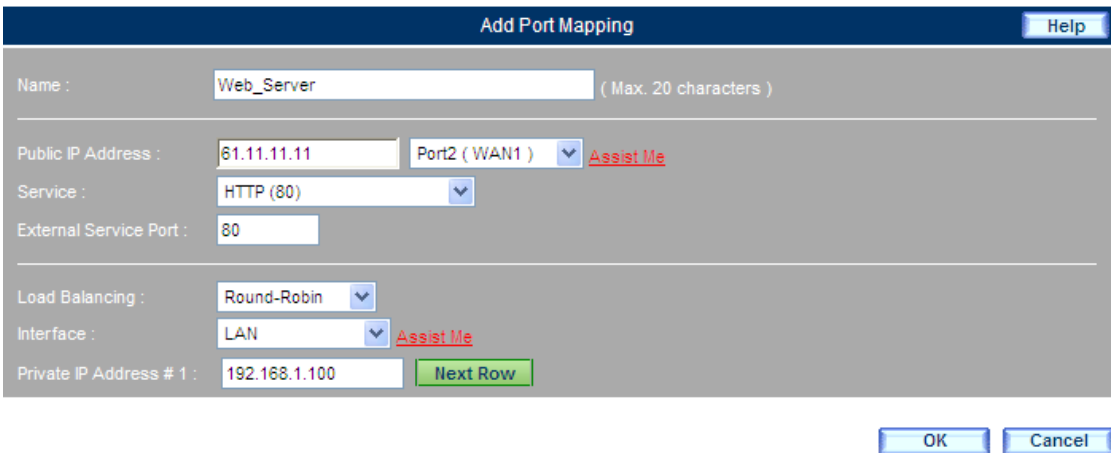


Figure 24-6 Server 1 Settings

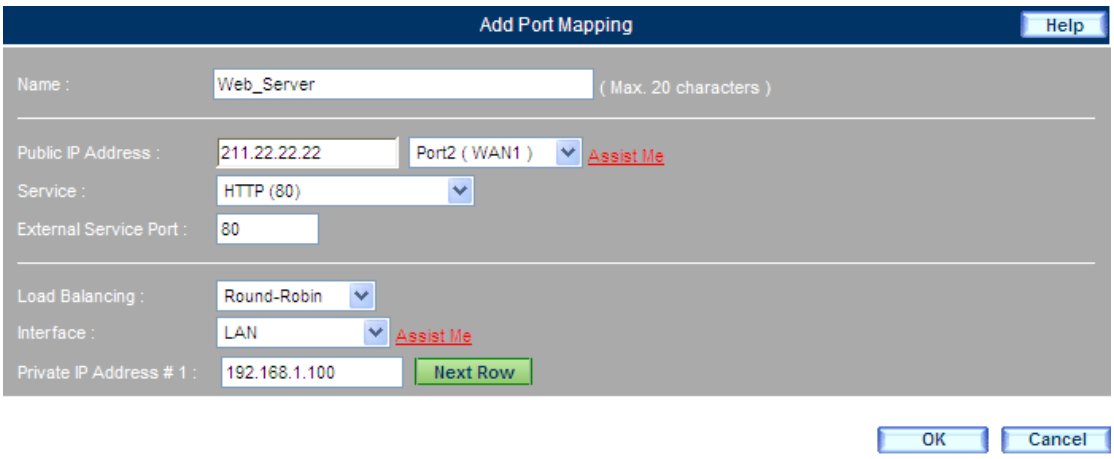


Figure 24-7 Server 2 Settings

Step 3. Go to **Policy** > **Incoming** and then set as below:

- Click **New Entry**.（**Figure 24-8**）
- For **Destination Address** select [Virtual Server IP] Web_Server(61.11.11.11).
- For **Service** select HTTP(80).
- Click **OK.**
- Click **New Entry**.（**Figure 24-9**）
- For **Destination Address** select [Virtual IP] Web_Server(211.22.22.22).
- For **Service** select HTTP(80)。
- Click **OK**.（**Figure 24-10**）

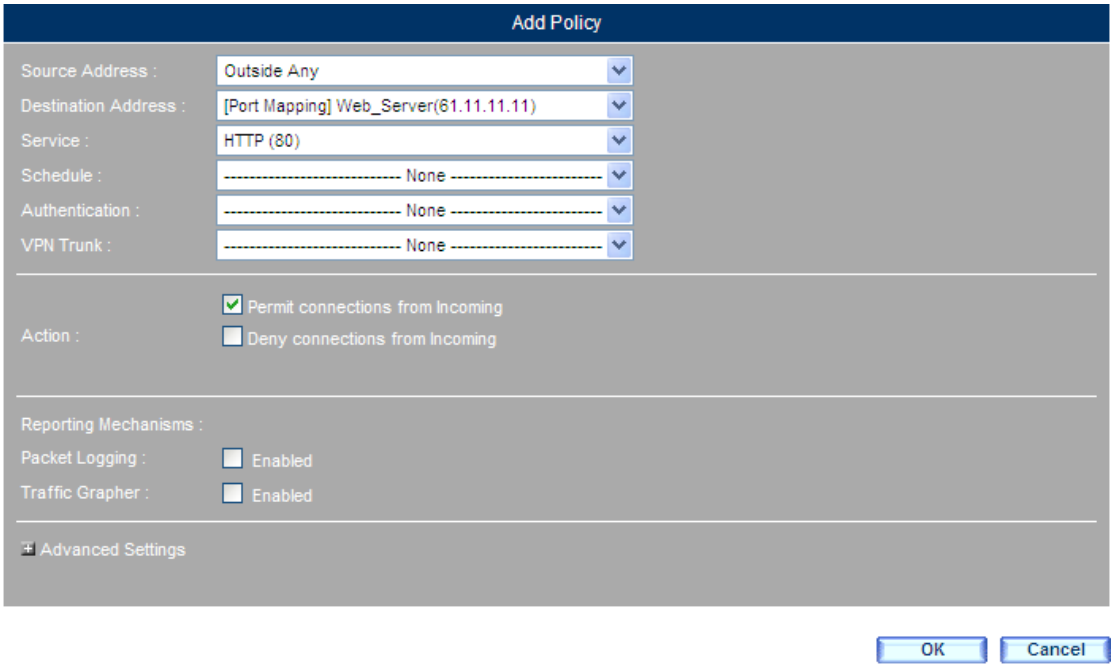


Figure 24-8 Configuring the First Settings of an Incoming Policy Settngs

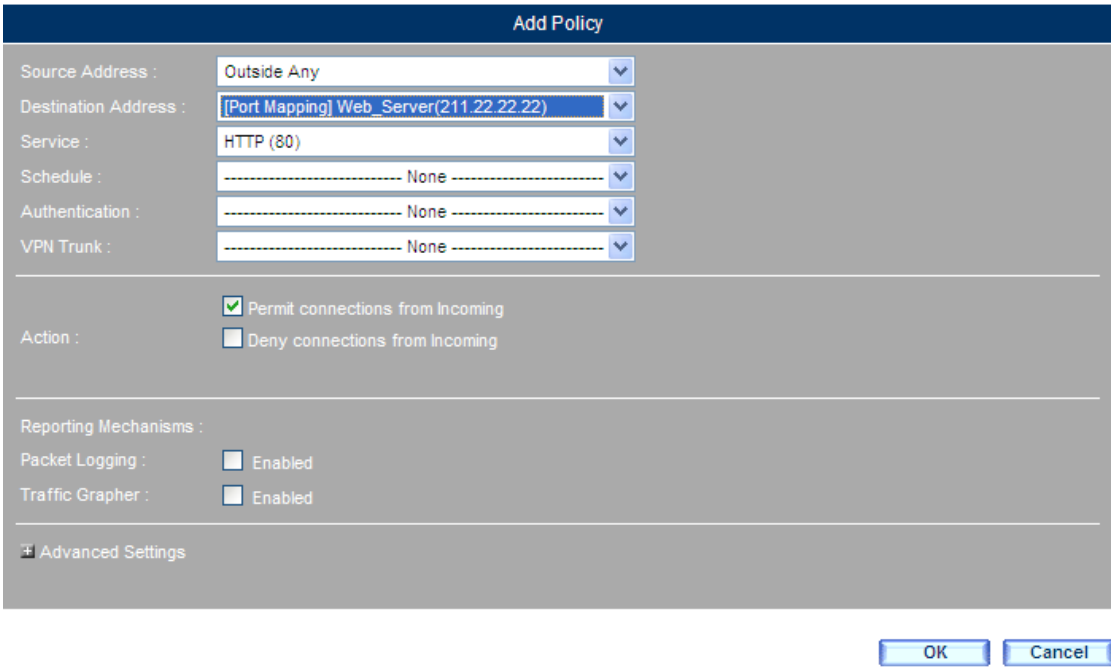


Figure 24-9 Configuring the First Settings of an Incoming Policy Settings

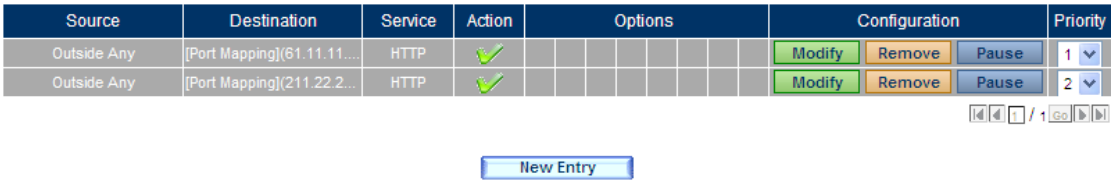


Figure 24-10 The Completed Policy Settings

Step 4. Settings complete. If WAN 1 goes down, WAN 2 ensures user's access to the web server remains uninterrupted.（Figure 24-11）

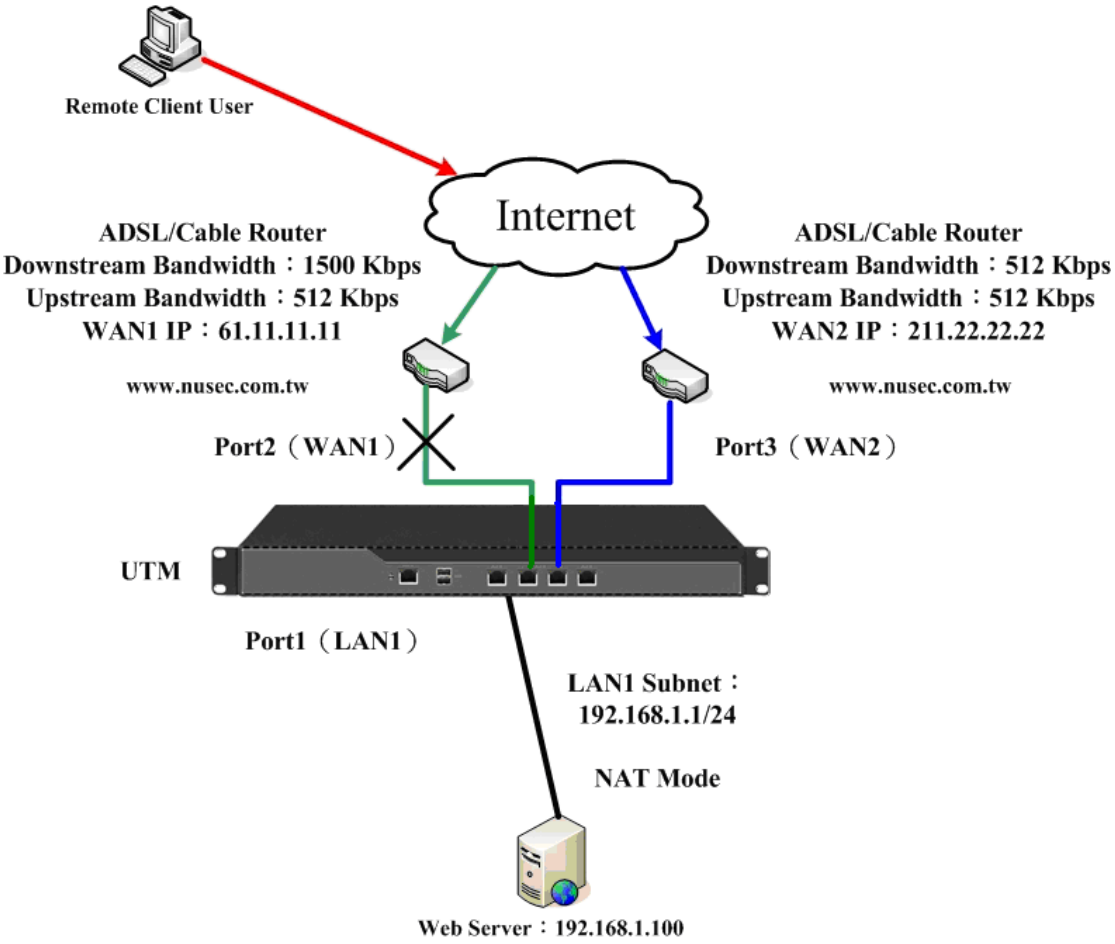


Figure 24-11 Web Server Backup Deployment

26.1.2 Creating an A Record to Load Balance a Web Server

Using the Round-Robin Mode

Step 1. Go to **Advance** > **Inbound Balancing** > **Settings** and proceed with the following settings:

- Click **New Entry**.（**Figure 24-12**）
- In the **Domain Name** field, enter the domain that you obtained from your ISP.
- Tick **Enable DNS zone.**
- Click **New Entry**.（**Figure 24-13**）
- Select A(Address) for **DNS Record Type.**
- Type www in the **Host Name** field.
- For **Real IP Address**, type 61.11.11.11 and select WAN1 from the drop-down list.
- For **Load Balancing Mode**, select **Round-Robin.**
- Click **OK**. Select 1 for **Weight** and 1 for **Priority.**
- Click **New Entry**.（**Figure 24-14**）
- Select A(Address) for **DNS Record Type.**
- Type www in the **Host Name** field.
- For **Real IP Address**, type 211.22.22.22 and select WAN2 from the drop-down list.
- Select Round-Robin for **Load Balancing Mode.**
- Click OK. Select 2 for **Weight** and select 2 for **Priority**.（**Figure 24-15**）

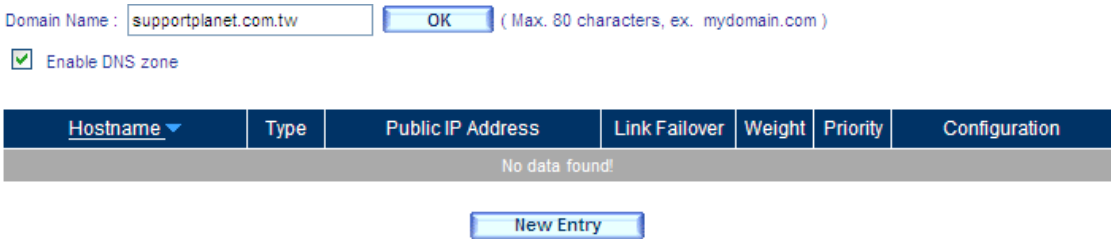


Figure 24-12 Adding New Domain Name

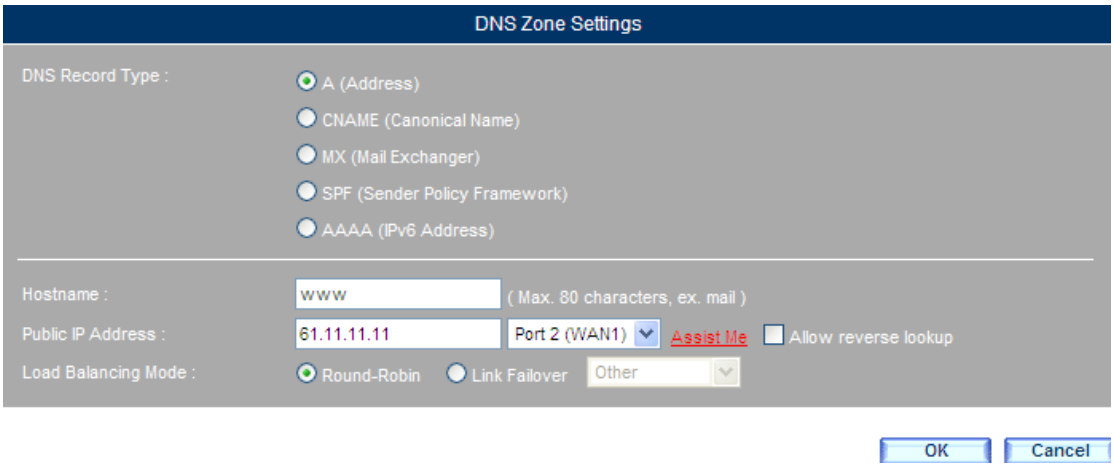


Figure 24-13 The First Inbound Balance Settings

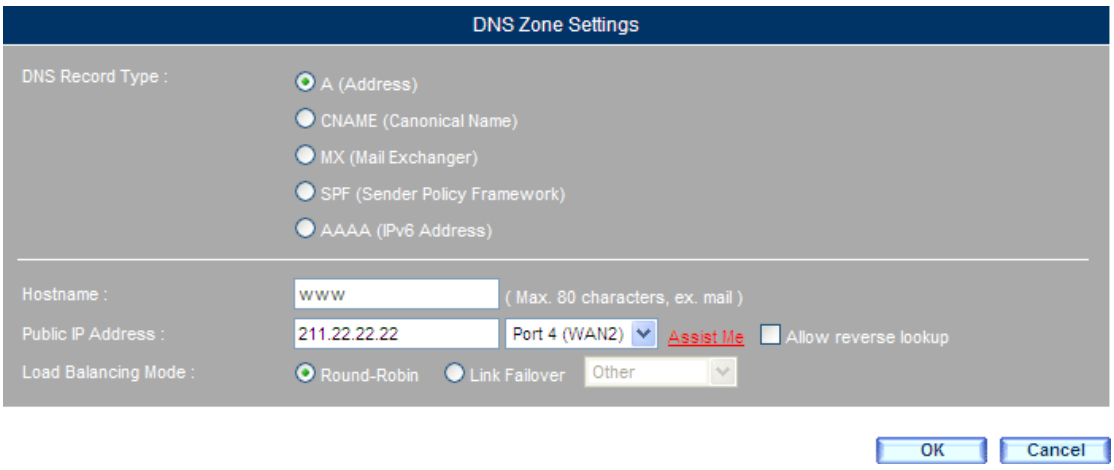


Figure 24-14 The Second Inbound Balance Configuration

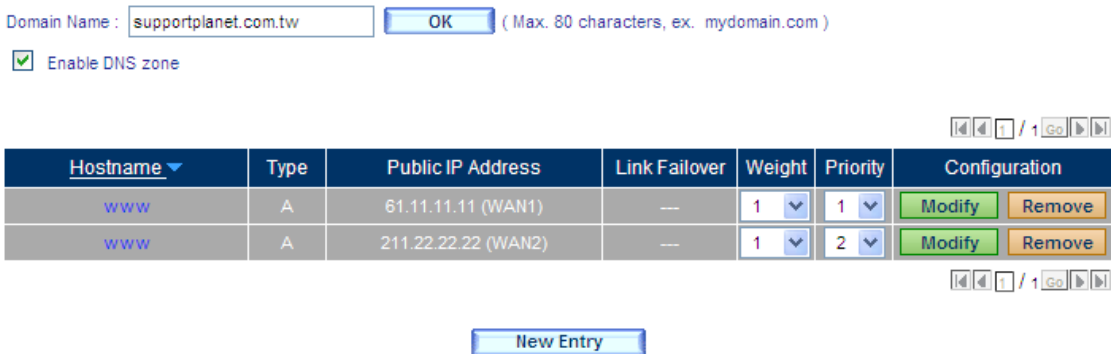


Figure 24-15 Setting Completed

Step 2. Go to **Policy Object** > **Virtual Server** > **Port Mapping** and then set as below:（**Figure 24-16, 24-17**）

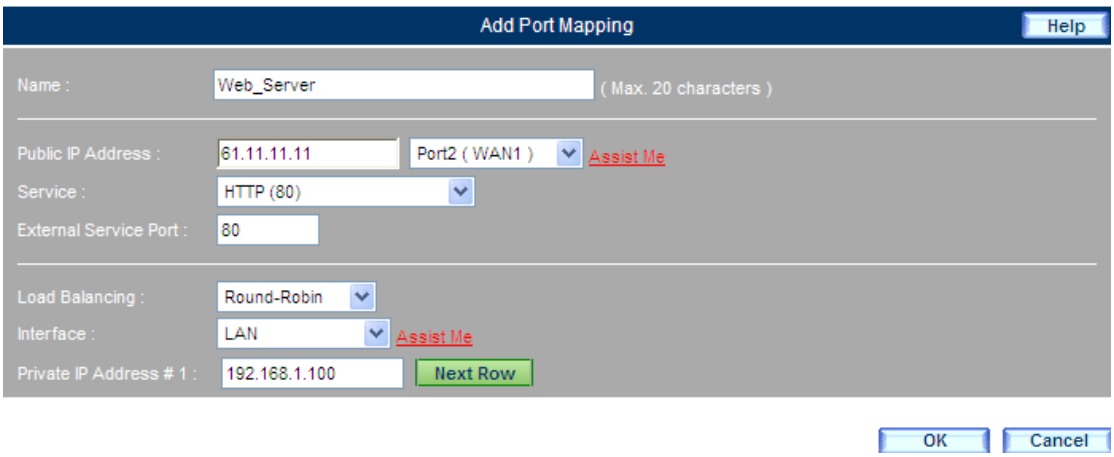


Figure 24-16 Server 1 Settings

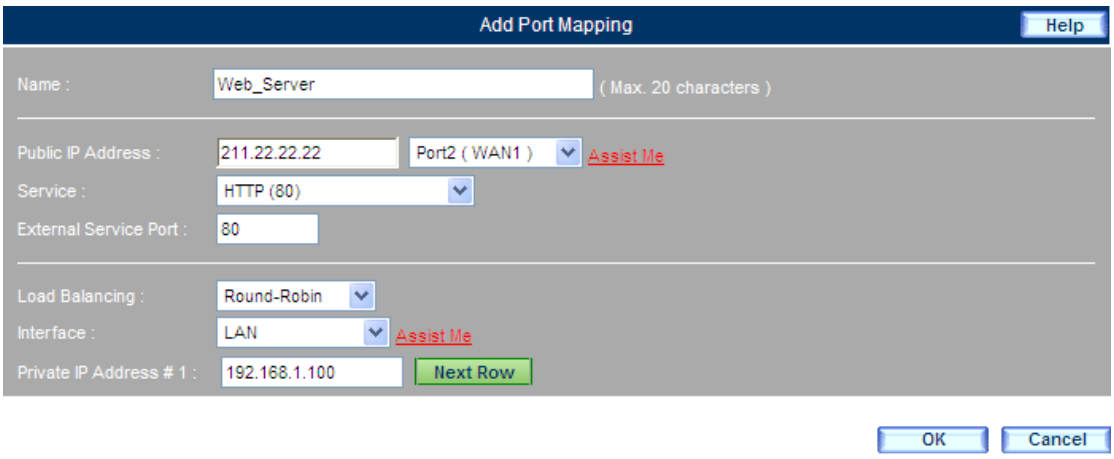


Figure 24-17 Server 2 Settings

Step 3. Go to **Policy** > **Incoming** and proceed with the following settings:

- Click **New Entry**.（**Figure 24-18**）
- Select the defined rule ([Virtual IP]Web_Server(61.11.11.11)) for **Destination Address.**
- Select HTTP(80) for **Service.**
- Click **OK**.
- Click **New Entry**.（**Figure 24-19**）
- Select the defined rule ([Virtual IP]Web_Server(211.22.22.22)) for **Destination Address.**
- Select HTTP(80) for **Service.**
- Click **OK**.（**Figure 24-20**）

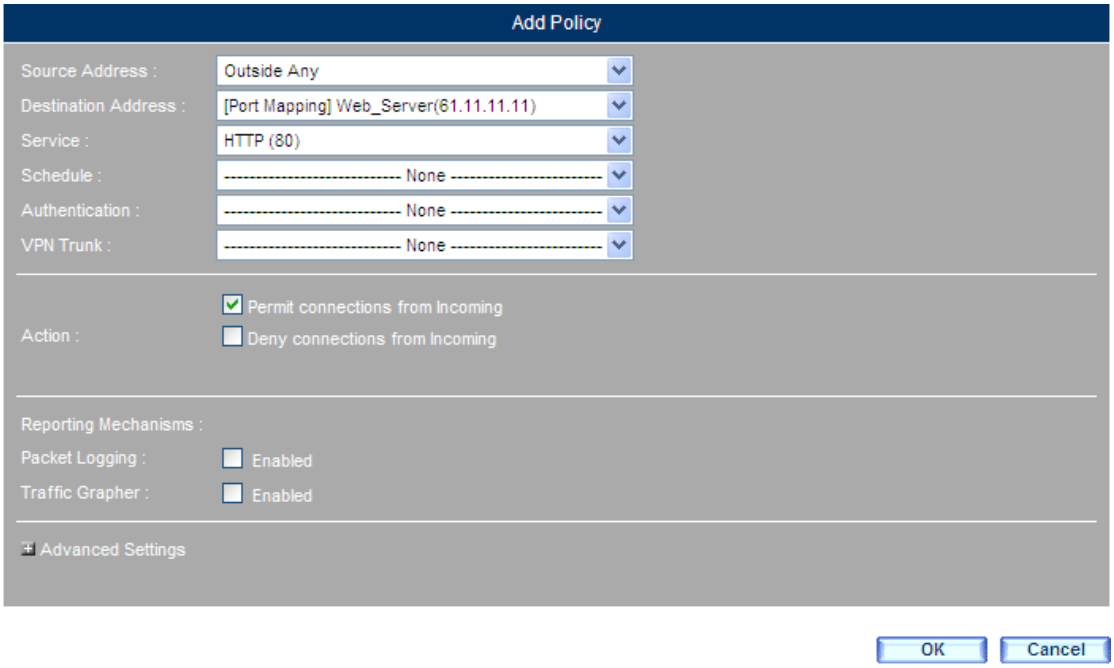


Figure 24-18 Configuring the First Policy Settings

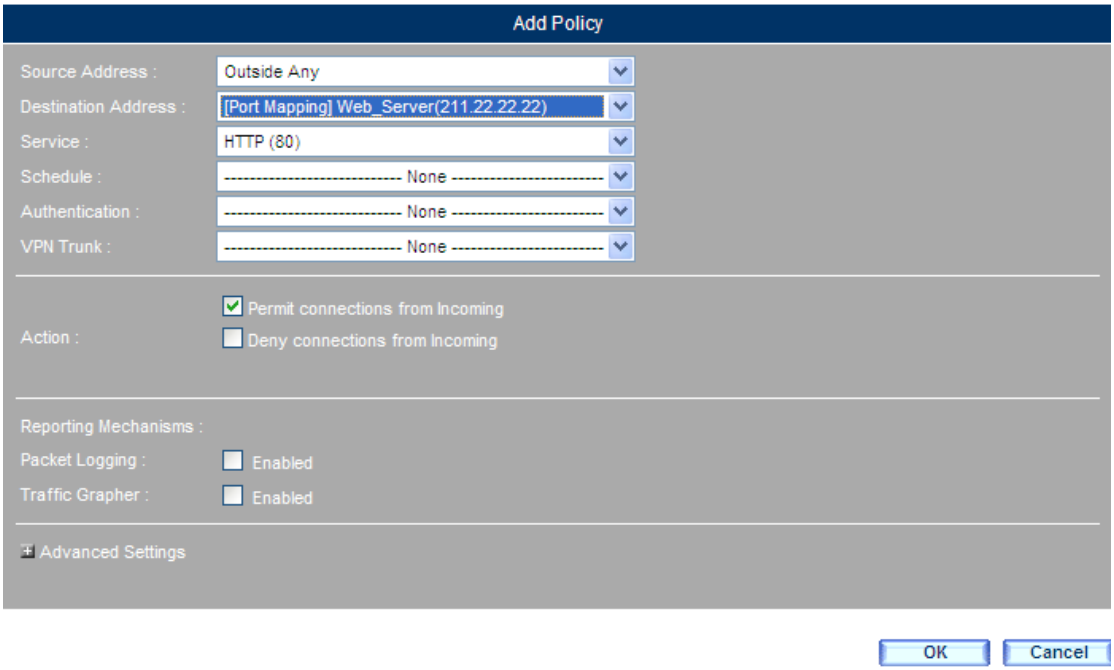


Figure 24-19 Configuring the Second Policy Settings

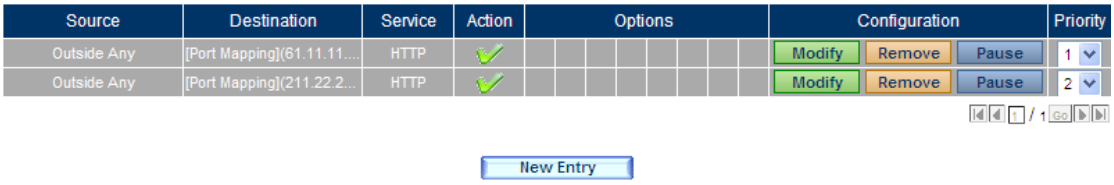


Figure 24-20 Policy Completed

Step 4. Setting completed.（Figure 24-21）

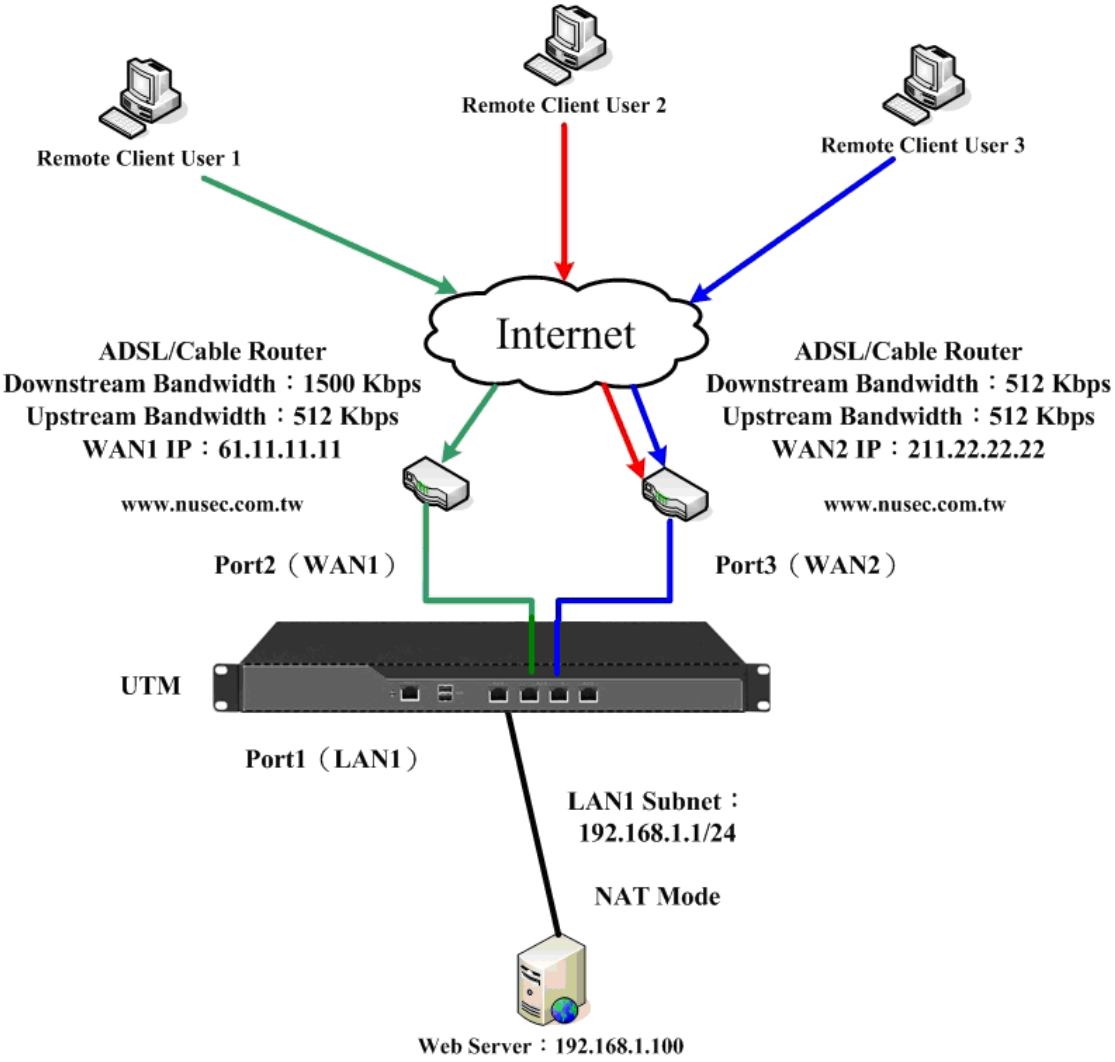


Figure 24-21 The Round-Robin Deployment

Note:

1. Inbound Balance Settings:（Table 24-9）

Name	Type	Address	Weight	Priority
www.supportplanet.com.tw	A	61.11.11.11	1	1
www.supportplanet.com.tw	A	211.22.22.22	2	2

Table 24-9 Web Server Weight and Priority Settings

- The weight and priority values will distribute their access as below:
  - The 1st user accesses the server via 61.11.11.11.
  - The 2nd user accesses the server via 211.22.22.22.
  - The 3rd user accesses the server via 211.22.22.22 (Round-Robin priority distribution cycle finished)
  - The 4th user accesses the server via 61.11.11.11 (Round-Robin priority distribution

cycle restarted)

- The 5th user accesses the server via 211.22.22.22.
- The 6th user accesses the server via 211.22.22.22.

26.1.3 Creating a CNAME Record to Load Balance a Web

Server Using the Round-Robin Mode

Step 1. Go to **Advance** > **Inbound Balancing** > **Settings** and then set as below:

- Click **New Entry**.（**Figure 24-22**）
- In the **Domain Name** field, enter the domain name you applied for from your ISP.
- Tick **Enable DNS zone.**
- Click **New Entry**.（**Figure 24-23**）
- Select **A(Address)** for **DNS Record Type.**
- Type web in the **Host Name** field.
- For **Real IP Address**, type 61.11.11.11 in the field and then select WAN1 from the drop-down list.
- For **Load Balancing Mode**, select **Round-Robin.**
- Click **OK**. Select 1 for **Weight** and select 1 for **Priority.**
- Click **OK**.（**Figure 24-24**）
- Select A(Address) for **DNS Record Type.**
- Type web in the **Host Name** field.
- For **Real IP Address**, type 211.22.22.22 in the field and then select WAN2 from the drop-down list.
- Select Round-Robin for **Load Balancing Mode.**
- Click OK. Select 2 for **Weight** and 2 for **Priority.**
- Click **New Entry**.（**Figure 24-25**）
- Select **CNAME (Canonical NAME)** for **DNS Record Type**.
- Type www in the **Alias Name** field.
- Type web.supportplanet.com.tw in the **Real Name** field.
- Click **OK**.（**Figure 24-26**）

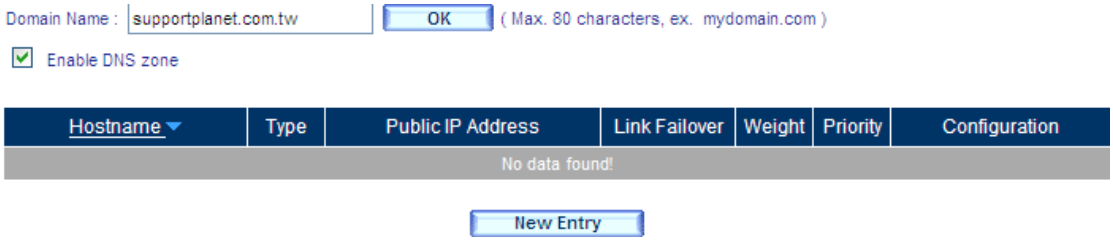


Figure 24-22 Adding a New Domain Name

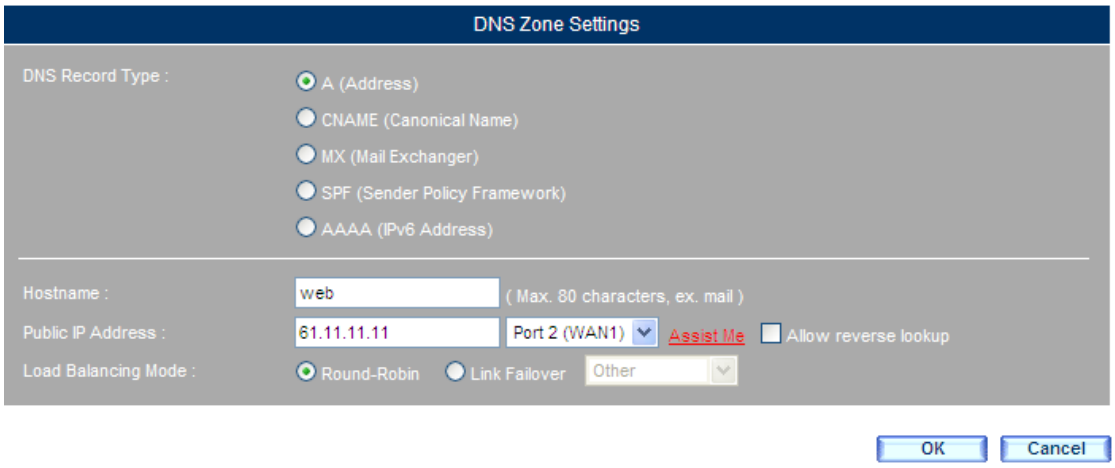


Figure 24-23 The First Inbound Balance Settings

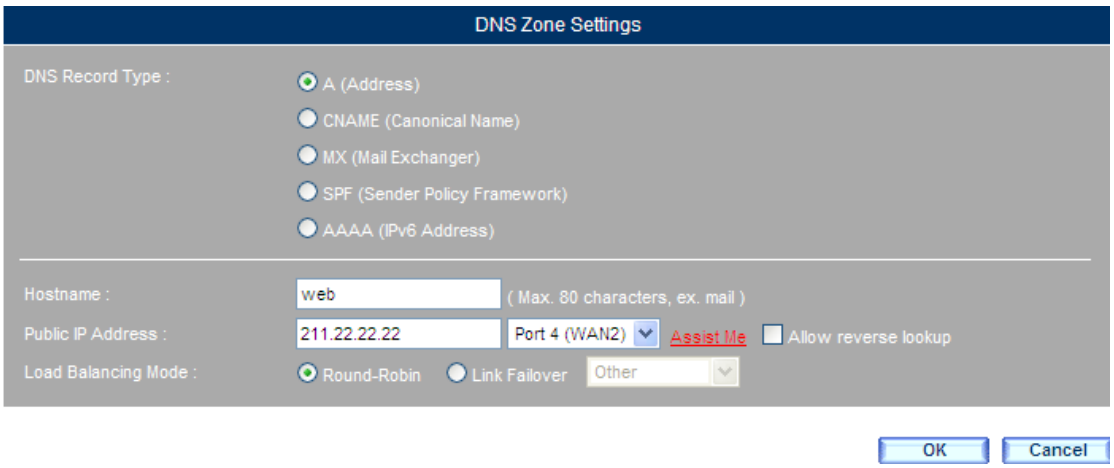


Figure 24-24 The Second Inbound Balance Settings

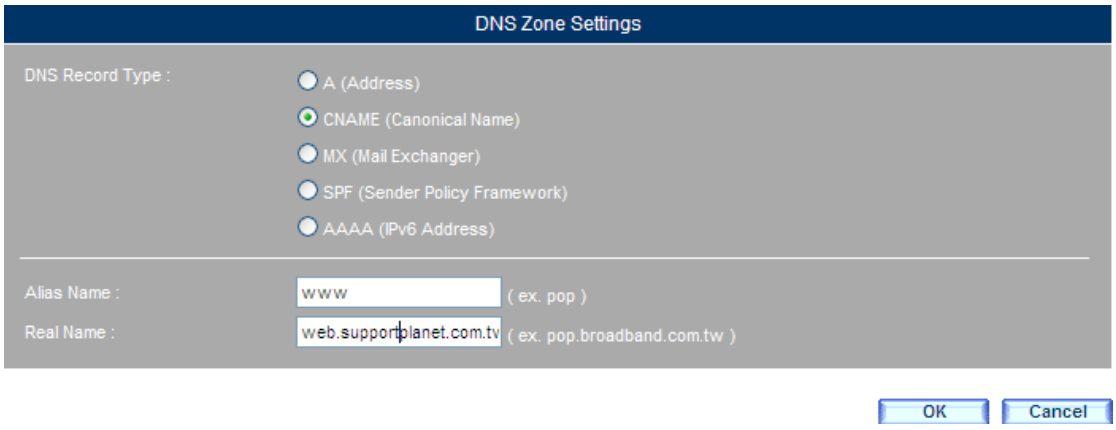


Figure 24-25 CNAME(Alias) Settings

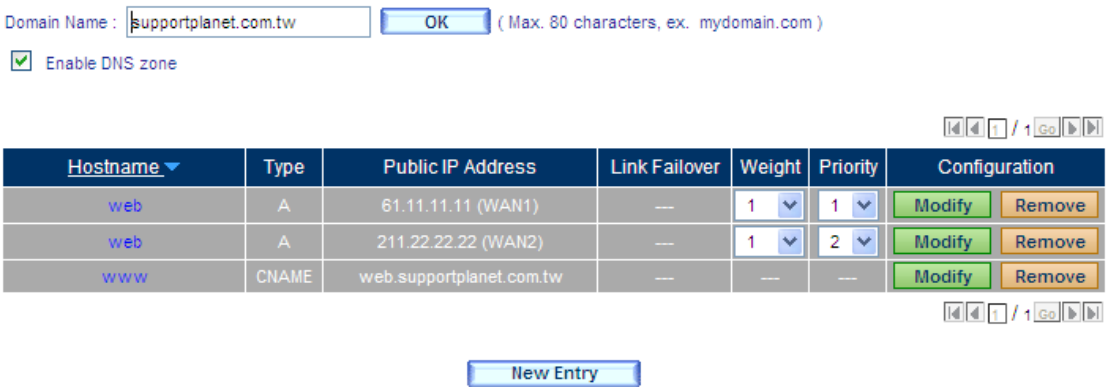


Figure 24-26 Completed CNAME(Alias) Settings

Step 2. Go to **Policy Object** > **Virtual Server** > **Port Mapping** and then set as below:（**Figure 24-27, 24-28**）

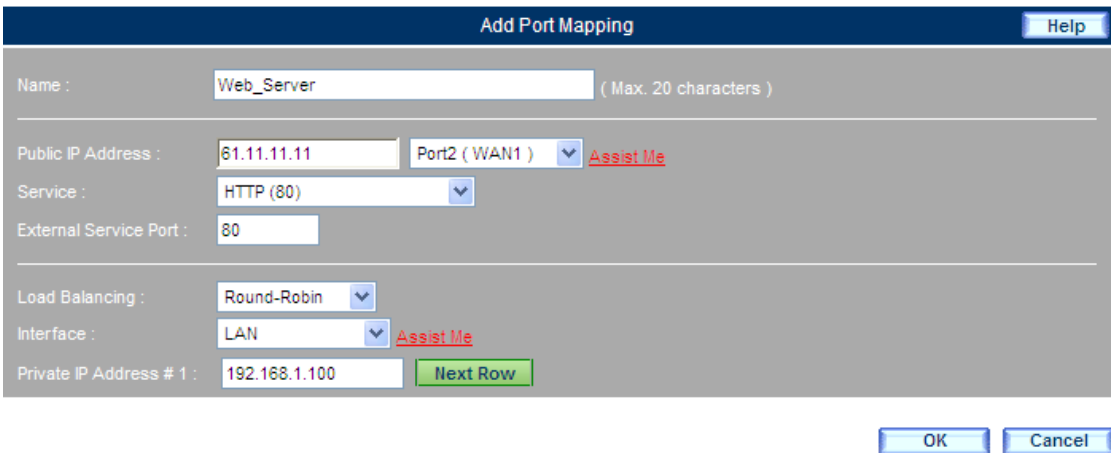


Figure 24-27 Server 1 Settings

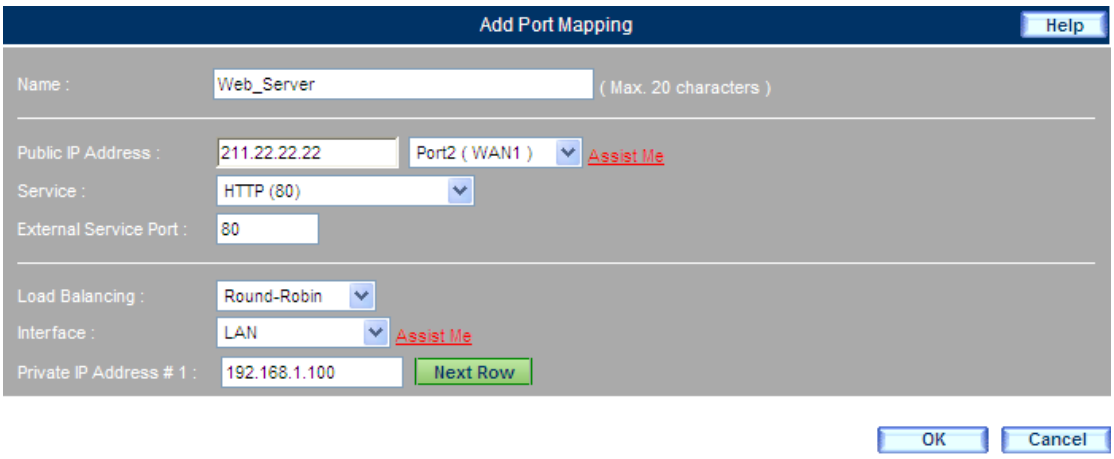


Figure 24-28 Server 2 Settings

Step 3. Go to **Policy** > **Incoming** and then set as below:

- Click **New Entry**.（**Figure 24-29**）
- Select the defined rule ([Virtual IP]Web_Server(61.11.11.11)) for **Destination Address.**
- Select HTTP(80) for **Service.**
- Click **OK.**
- Click **New Entry**.（**Figure 24-30**）
- Select the defined rule ([Virtual IP]Web_Server(211.22.22.22)) for **Destination Address**）
- Select HTTP(80) for **Service.**
- Click **OK**.（**Figure 24-31**）

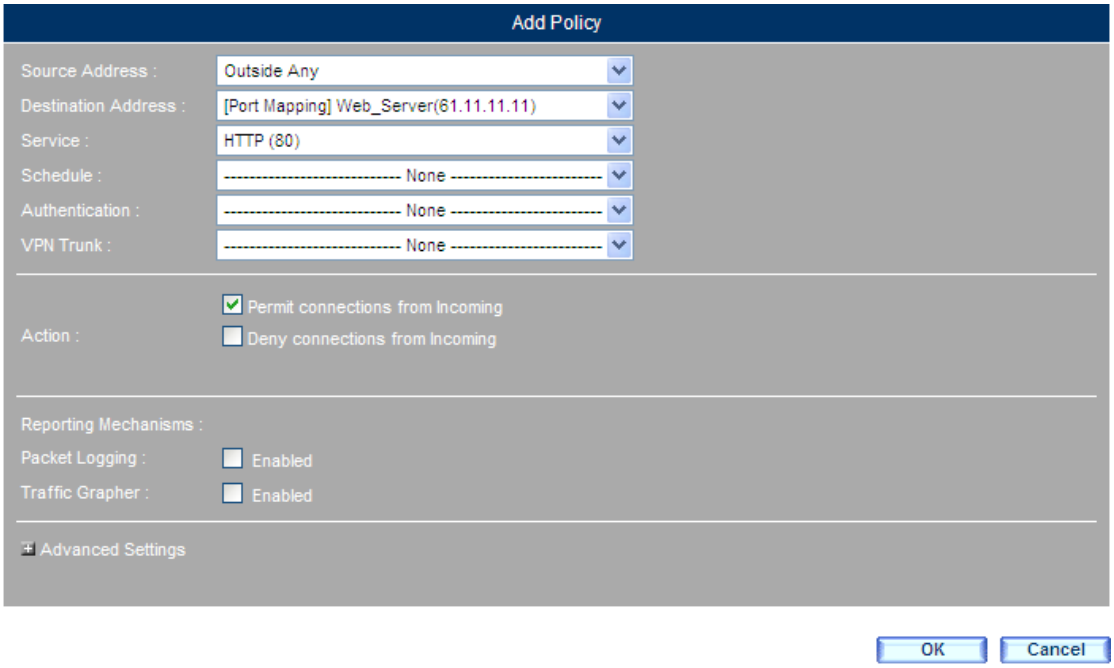


Figure 24-29 Incoming Policy Settings

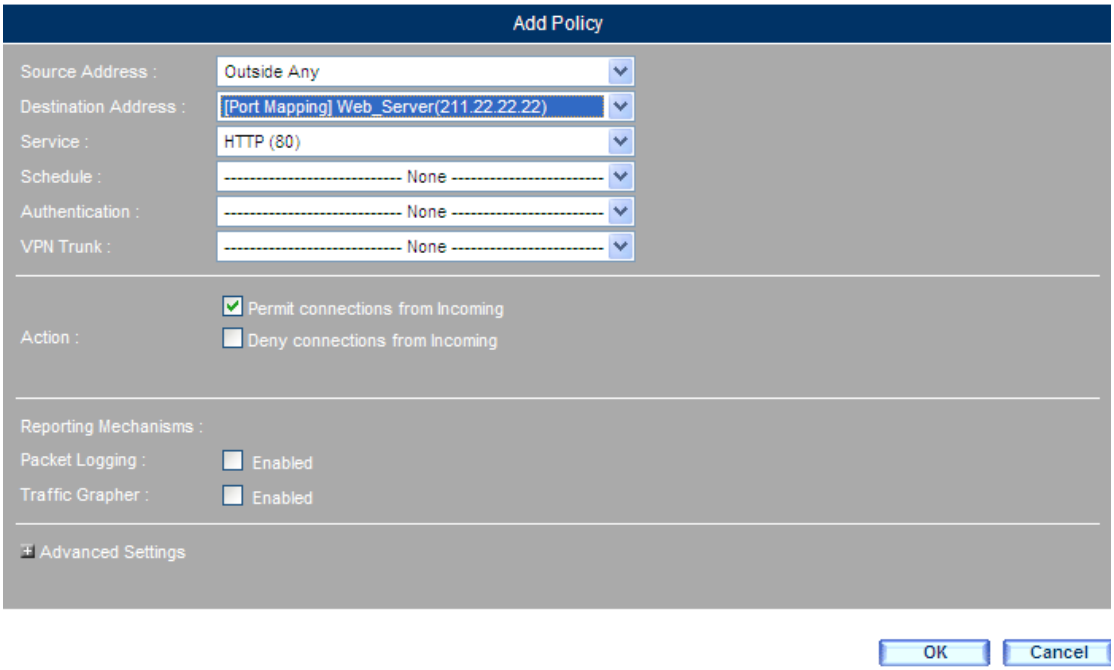


Figure 24-30 Configuring the Second Policy Settings

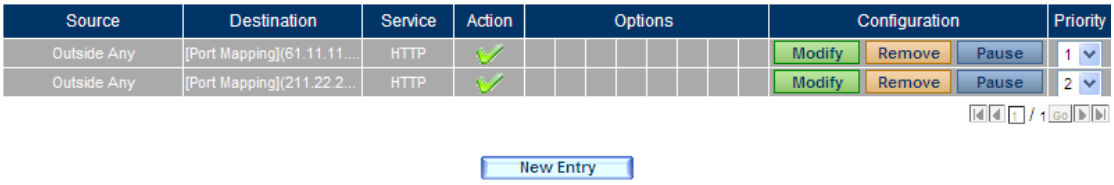


Figure 24-31 Adding the Second Policy

Step 4. Setup completed.（Figure 24-32）

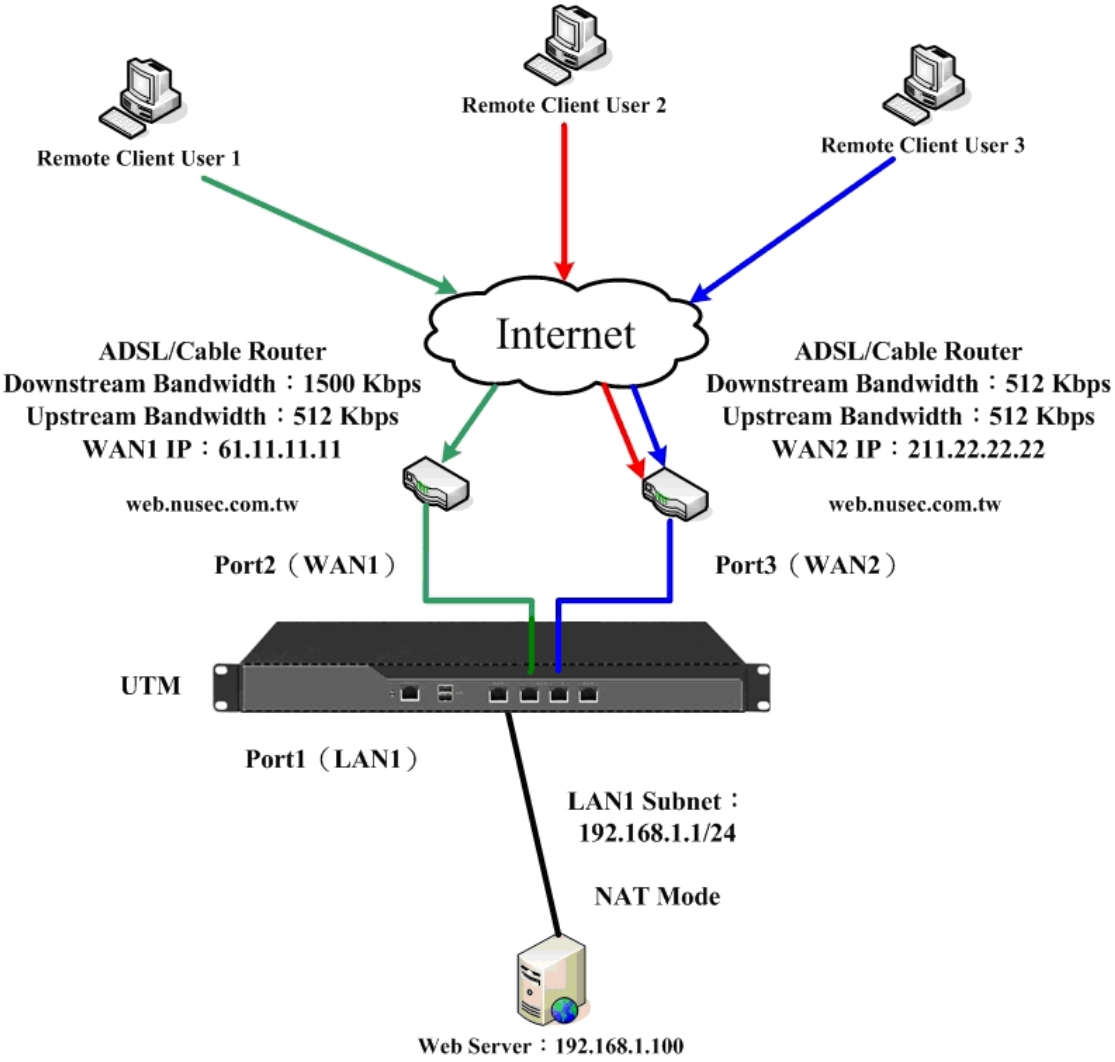


Figure 24-32 Web Server Deployment Using CNAME

Note:

1. The settings for Inbound Balancing:（**Table 24-10**）

Name	Type	Address	Weight	Priority
web.supportplanet.com.tw	A	61.11.11.11	1	1
web.supportplanet.com.tw	A	211.22.22.22	2	2
www.supportplanet.com.tw	CNAME	web.supportplanet.com.tw	--	--

Table 24-10 The Web Servers Weight, Priority and CNAME Settings

- Based on the weight and priority, the WAN distribution will be as follows:
  - The 1st user accesses the server via 61.11.11.11.
  - The 2nd user accesses the server via 211.22.22.22.
  - The 3rd user accesses the server via 211.22.22.22 (Round-Robin priority distribution cycle finished)

- The 4th user accesses the server via 61.11.11.11 (Round-Robin priority distribution cycle has restarted)
- The 5th user accesses the server via 211.22.22.22.
- The 6th user accesses the server via 211.22.22.22.

26.1.4 Creating a MX Record to Load Balance a Mail Server

Using the Round-Robin Mode

Step 1. Go to **Advance** > **Inbound Balancing** > **Settings** and then set as below:

- Click **New Entry**.（**Figure 24-33**）
- Enter the Domain Name.
- Tick **Enable DNS zone.**
- Click **New Entry**.（**Figure 24-34**）
- Select A(Address) for **DNS Record Type.**
- Type main in the **Host Name** field.
- For **Real IP Address**, type 61.11.11.11 and then select WAN1.
- Select Round-Robin for **Load Balancing Mode.**
- Click **OK**. Select 1 for **Weight** and select 1 for **Prioirty.**
- Click **New Entry**.（**Figure 24-35**）
- Select A(Address) for **DNS Record Type.**
- Type main in the **Host Name** field.
- For **Real IP Address**, type 211.22.22.22 in the field and select WAN2 from the drop-down list.
- Select Round-Robin for **Load Balancing Mode.**
- Click **OK**. Select 2 for **Weight** and select 2 for **Priority.**
- Click **New Entry** again.（**Figure 24-36**）
- Select **MX(Mail eXchanger)** for **DNS Record Type.**
- Type mail in the **Host Name** field.
- Type main.supportplanet.com.tw in the **Mail Server** field.
- Click **OK**.（**Figure 24-37**）

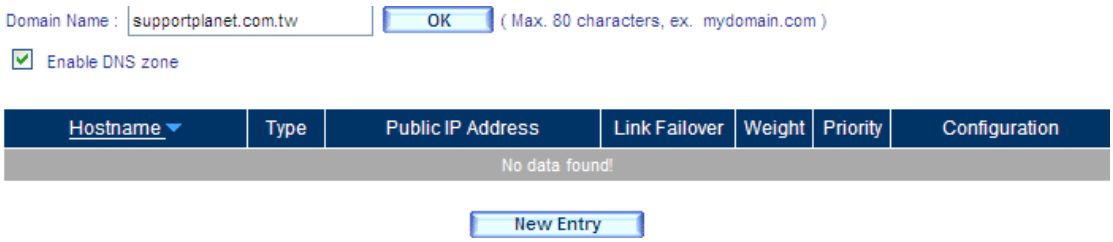


Figure 24-33 Adding a New Domain Name

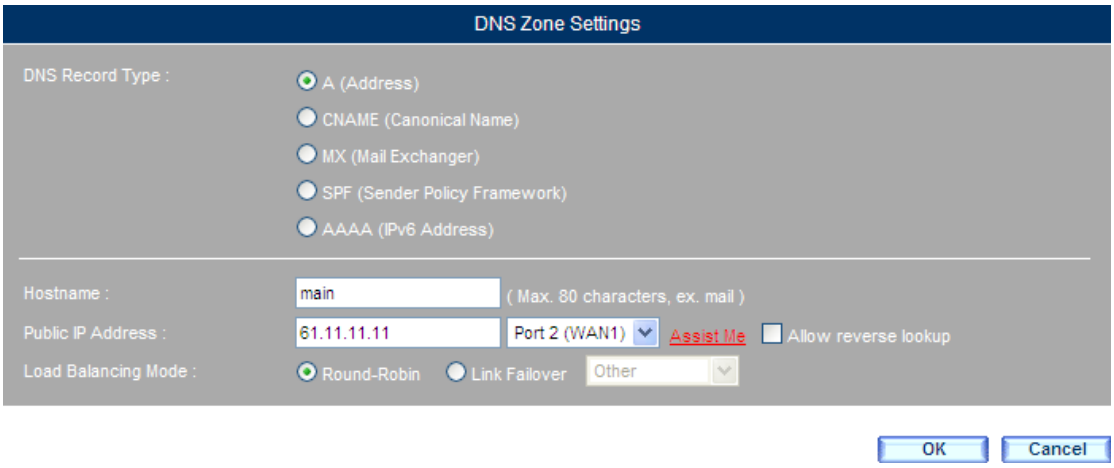


Figure 24-34 The First Inbound Balance Settings

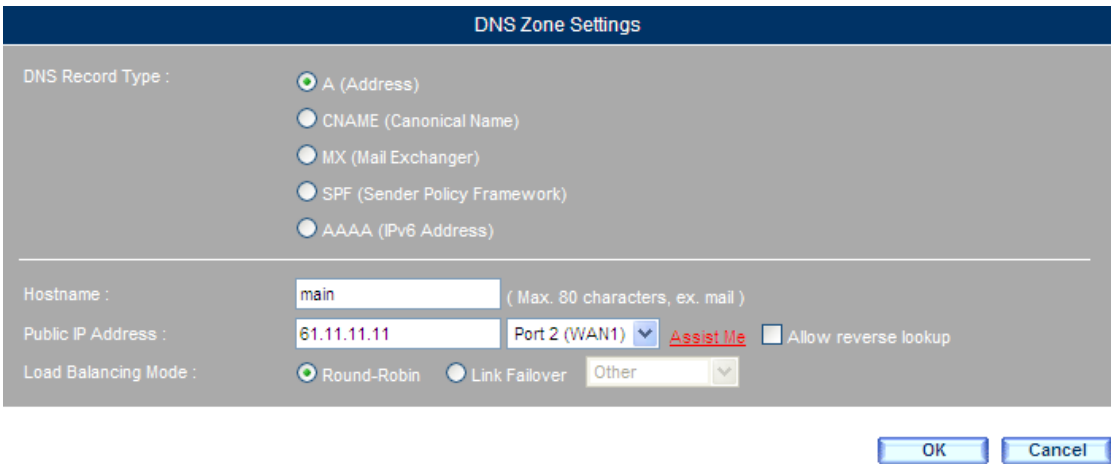


Figure 24-35 The Second Inbound Balance Settings

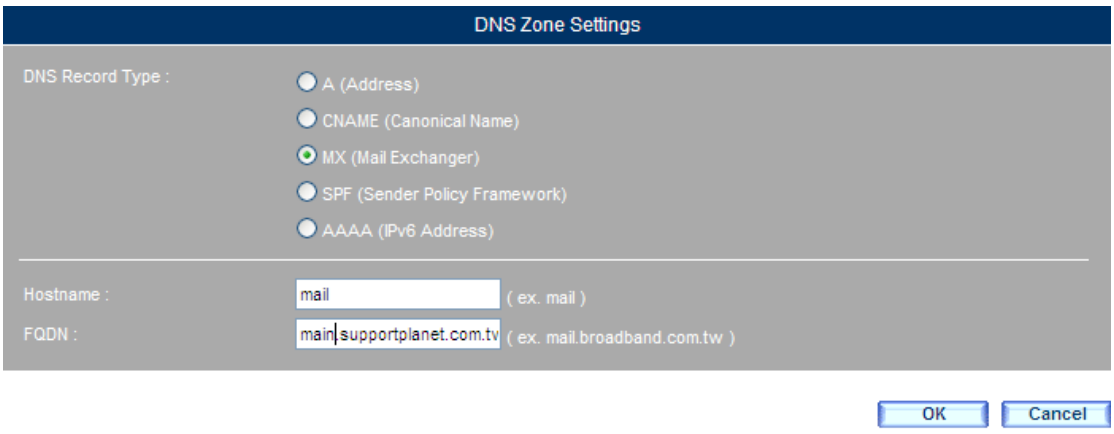


Figure 24-36 The MX(Mail eXchanger) Settings

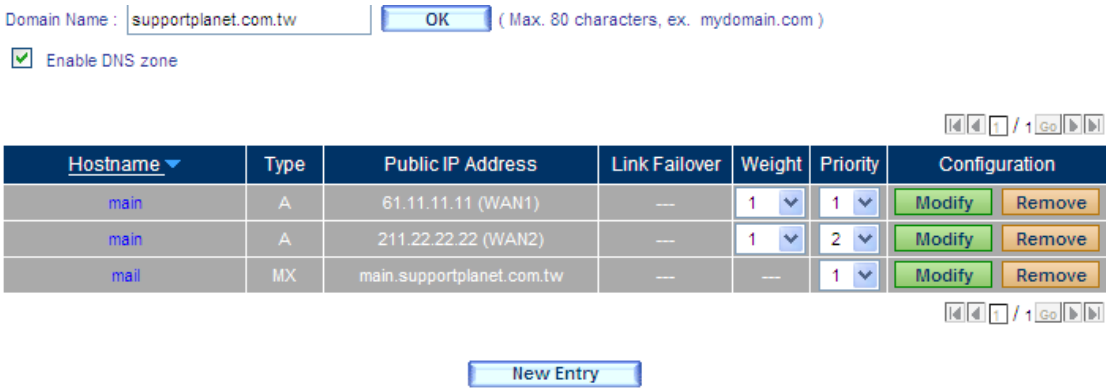


Figure 24-37 MX(Mail eXchanger) Settings Completed

Step 2. Go to **Policy Object** > **Virtual Server** > **Port Mapping** and then set as below:（**Figure 24-38, 24-39, 24-40, 24-41**）

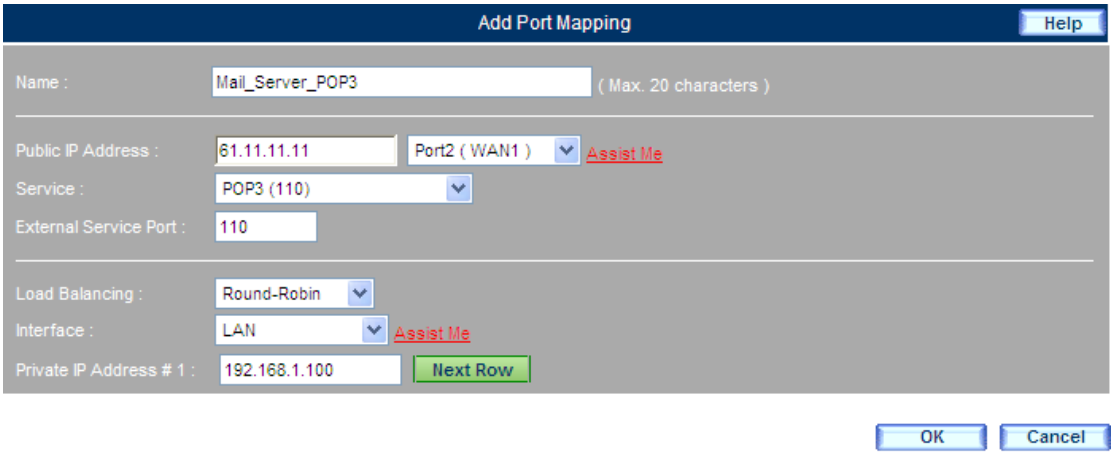


Figure 24-38 The First Setting of Server

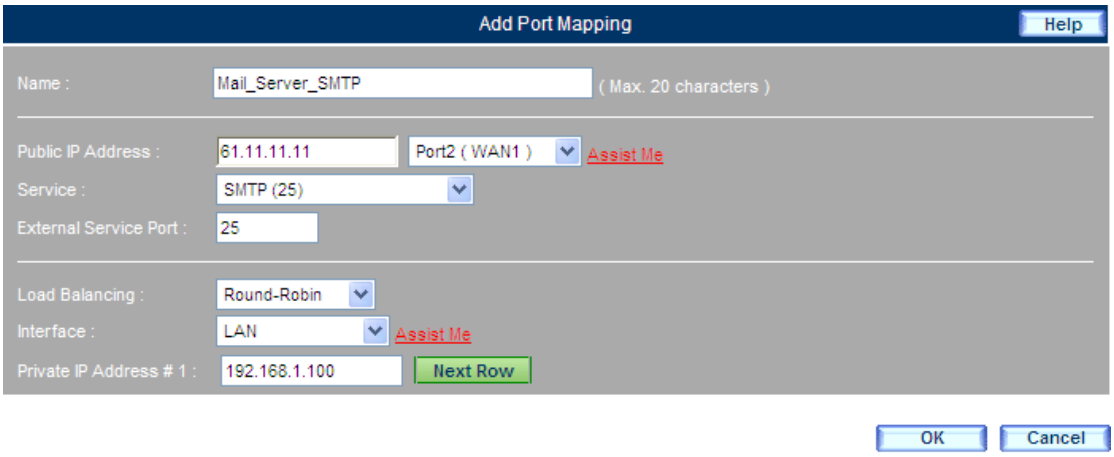


Figure 24-39 The Second Setting of Server

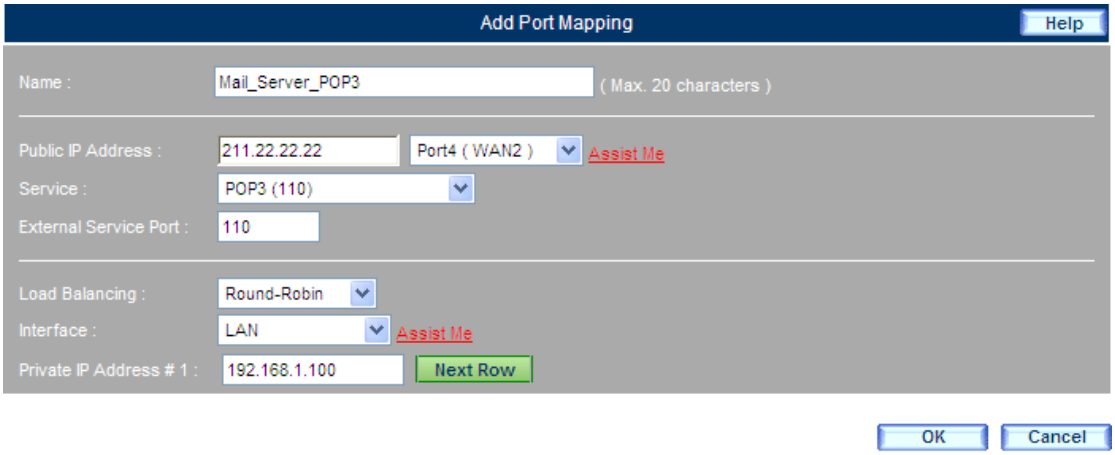


Figure 24-40 The Third Setting of Server

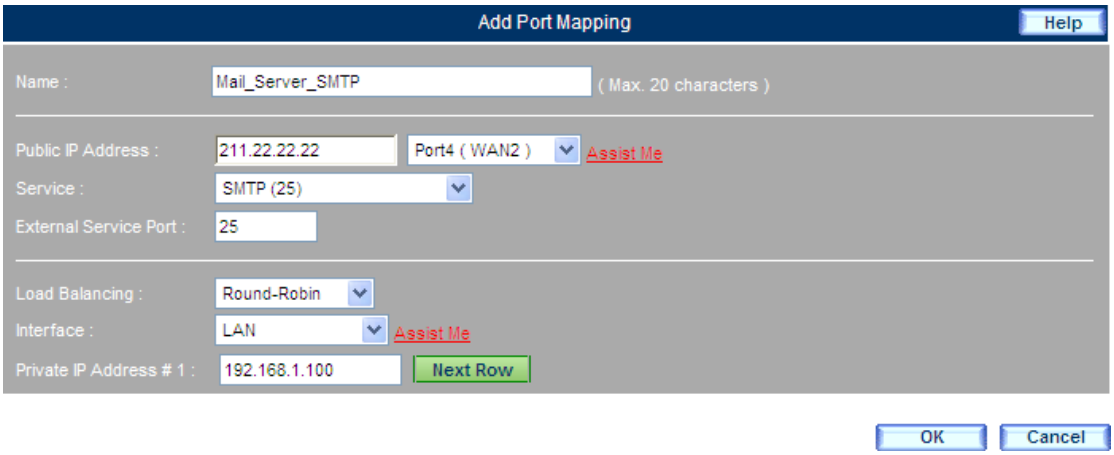


Figure 24-41 The Fourth Setting of Server

Step 3. Go to **Policy** > **Incoming** and then set as below:

- Click **New Entry**.（**Figure 24-42**）
- Select the defined rule ([Virtual IP]Mail_Server_POP3(61.11.11.11)) for **Destination Address.**
- Select POP3(110) for **Service.**
- Click **OK.**
- Click **New Entry**.（**Figure 24-43**）
- Select the defined rule ([Virtual IP]Mail_Server_SMTP(61.11.11.11)) for **Destination Address.**
- Select SMTP(25) for **Service.**
- Click **OK.**
- Click **New Entry**.（**Figure 24-44**）
- Select the defined rule ([Virtual IP]Mail_Server_POP3(211.22.22.22)) for **Destination Address.**
- Select POP3(110) for **Service.**
- Click **OK.**
- Click **New Entry**.（**Figure 24-45**）
- Select the defined rule ([Virtual IP]Mail_Server_SMTP(211.22.22.22)) from the **Destination Address.**
- Select SMTP(25) for **Service.**
- Click **OK**.（**Figure 24-46**）

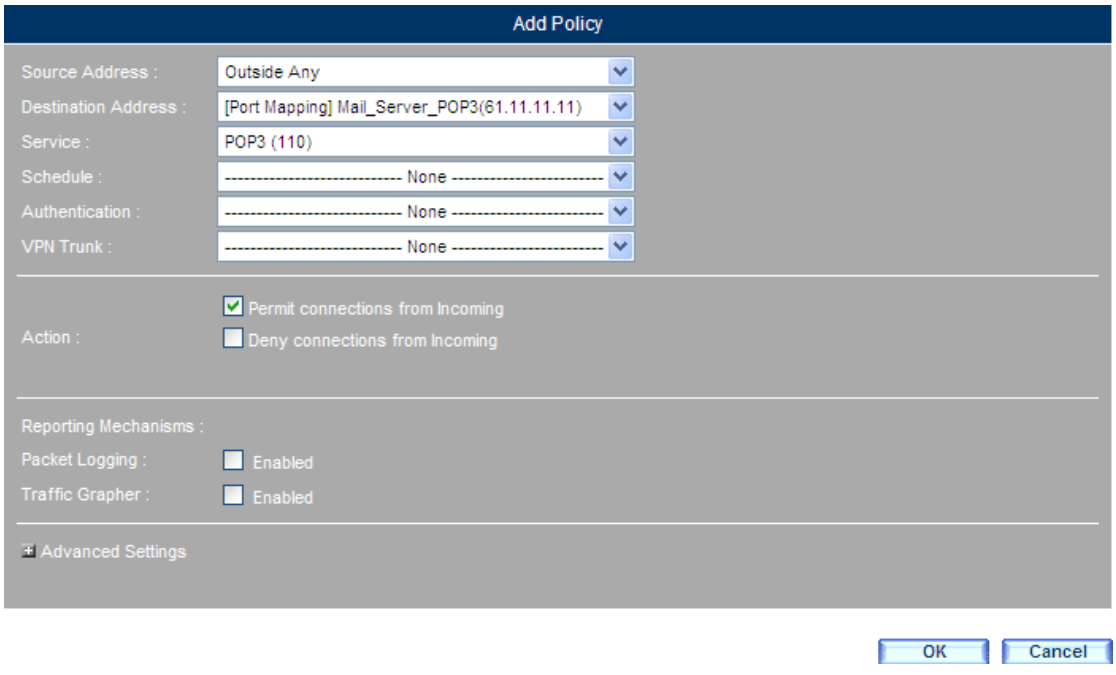


Figure 24-42 The First Policy Settings

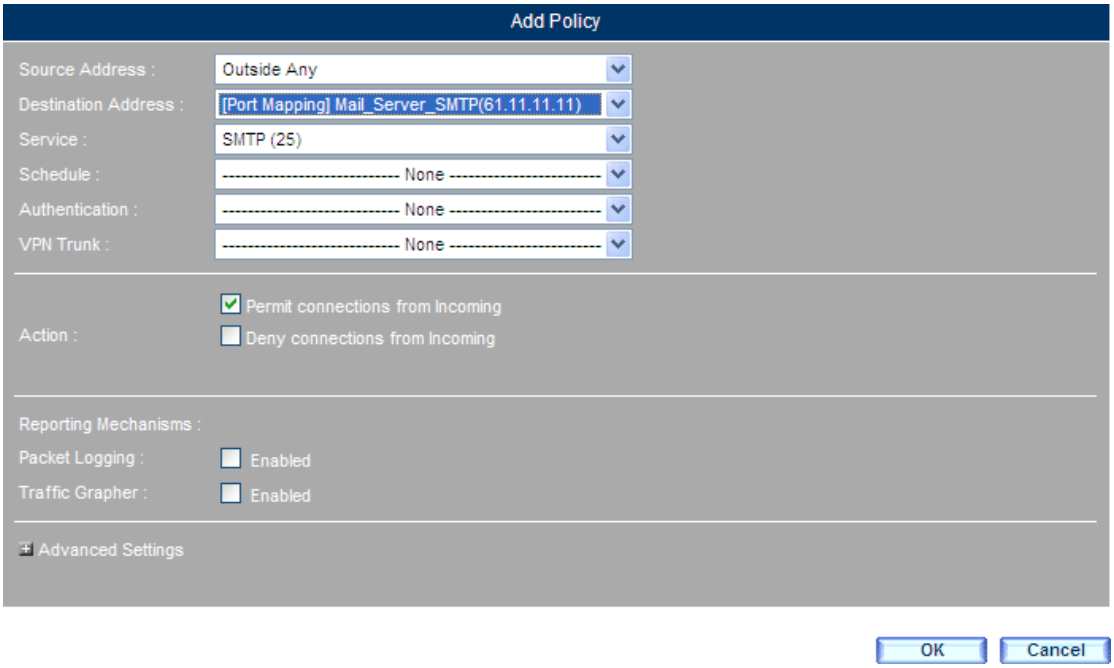


Figure 24-43 The Second Policy Settings

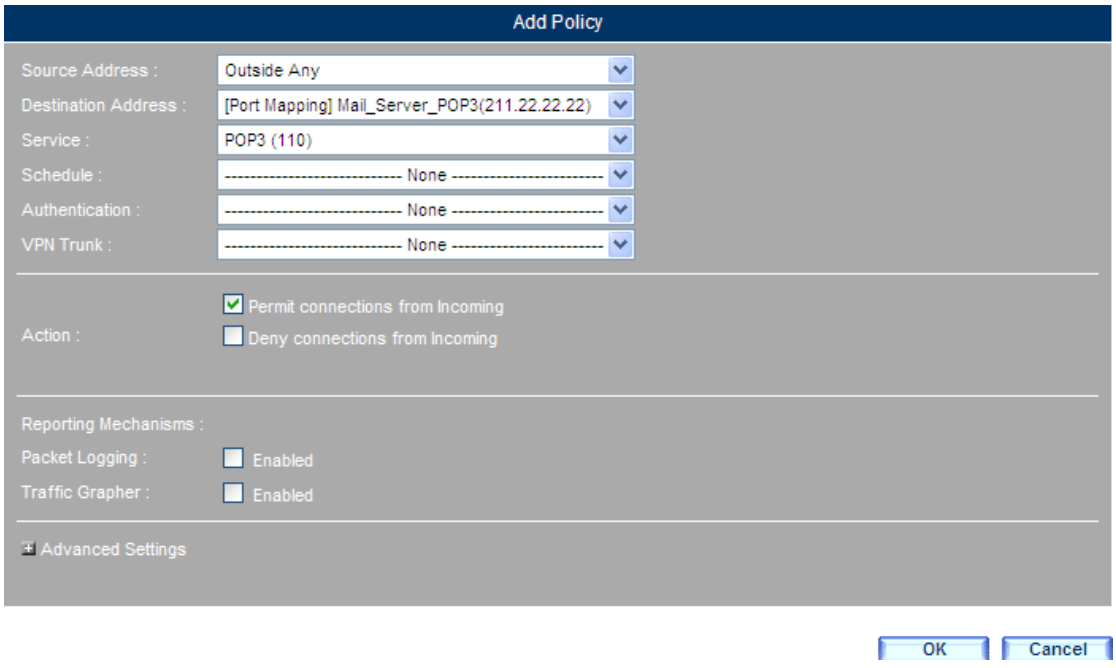


Figure 24-44 The Third Policy Settings

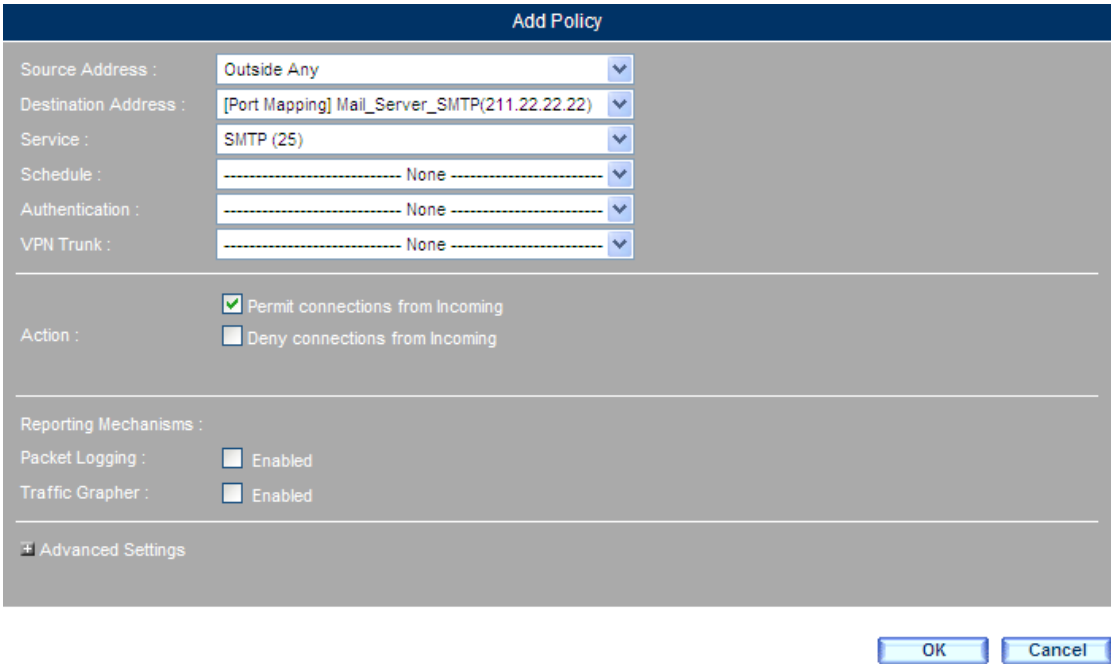


Figure 24-45 The Fourth Policy Settings

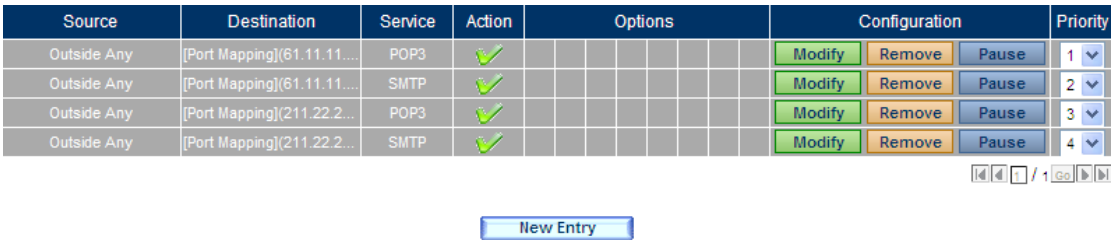


Figure 24-46 Policy Completed

Step 4. Setup Completed.（Figure 24-47）

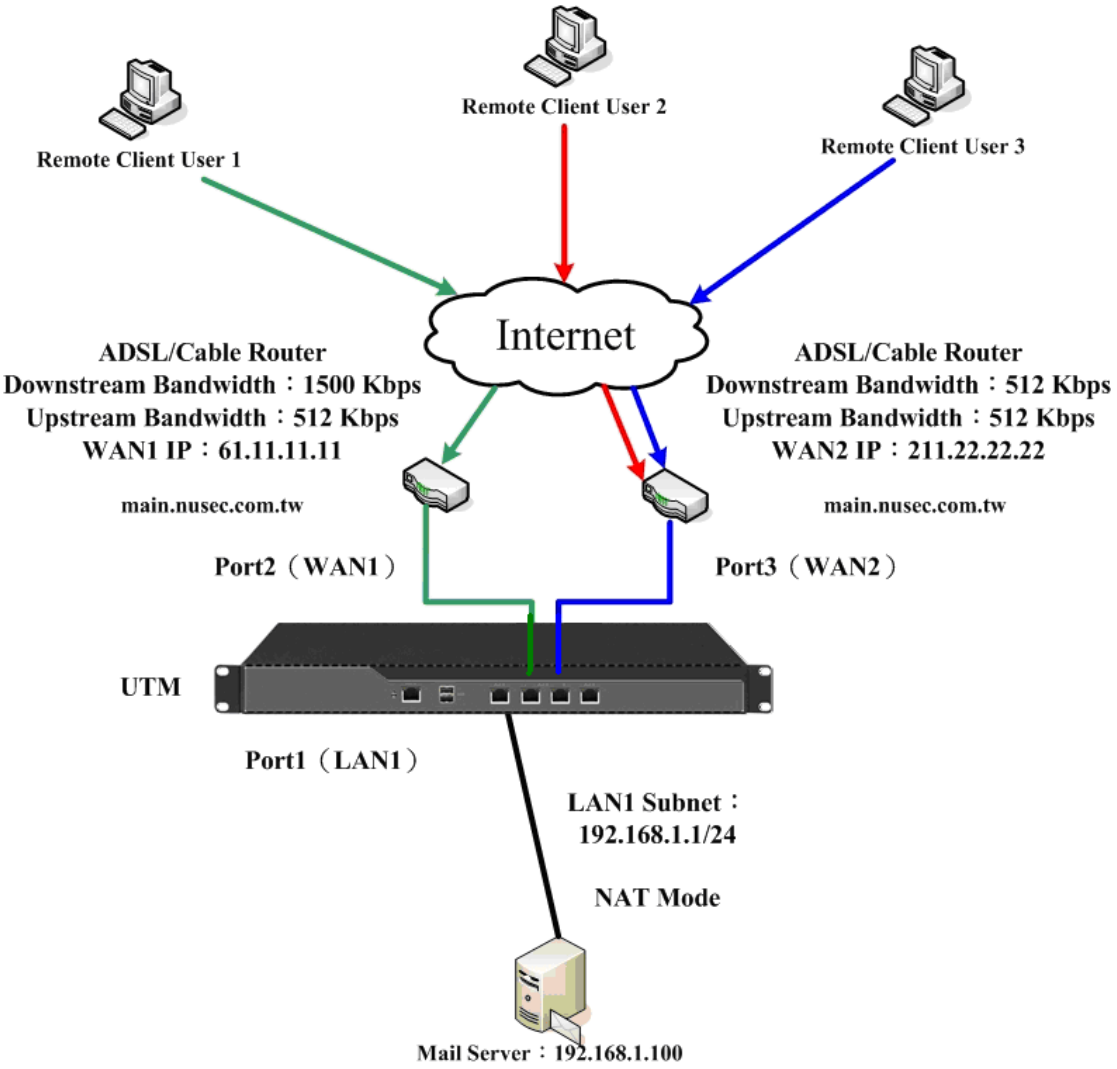


Figure 24-47 The Mail Server Deployment

Note:

1. Settings for Inbound Balancing: （Table 24-11）

Name	Type	Address	Weight	Priority
main.supportplanet.com.tw	A	61.11.11.11	1	1
main.supportplanet.com.tw	A	211.22.22.22	2	2
mail.supportplanet.com.tw.	MX	main.supportplanet.com.tw	--	--

Table 24-11 The MX Server's Weight and Priority Settings

- When a user connects to mail.supportplanet.com.tw, they will be directed to the real mail server named main.supportplanet.com.tw. As per the weight and priority values, they will be distributed to the following WAN links in the order below:
  - The 1st user accesses the server via 61.11.11.11.

- The 2nd user accesses the server via 211.22.22.22.
- The 3rd user accesses the server via 211.22.22.22 (**Round-Robin priority distribution cycle finished).**
- The 4th user accesses the server via 61.11.11.11(**Round-Robin priority distribution cycle has restarted).**
- The 5th user accesses the server via 211.22.22.22.
- The 6th user accesses the server via 211.22.22.22.

Chapter 27 High Availability

When two CS-2001 devices are deployed in the network, the two devices can operate in active / standby mode. The master device (active device) maintains a synchronization with the backup device (standby device). Once the master device fails, the backup device will seamlessly take over the operations. The High Availability mechanism effectively prevents any loss of data to your business.

Terms in High Availability

HA Mode

- This mode is used to determine if the device will serve as the master or backup.

Data Transmission Port / Management IP Address

- Configures the IP address and port for executing the synchronization between the master device and the backup device.

Backup Status

- Displays the status of the master device and the backup device.

27.1 Example

27.1.1 High Availability Deployment

Preparation

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing mode) and connect it to the LAN using 192.168.1.x/24.

Configure Port2 as WAN1(61.11.11.11) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range:61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote to access the Internet. IP range: 211.22.22.18 to 211.22.22.30.

Configure Port4 as DMZ1 (Transparent Routing mode)

Step 1. Assign one CS-2001 device as the master and connect it to the same switch that the LAN is connected to.（Figure 25-1）

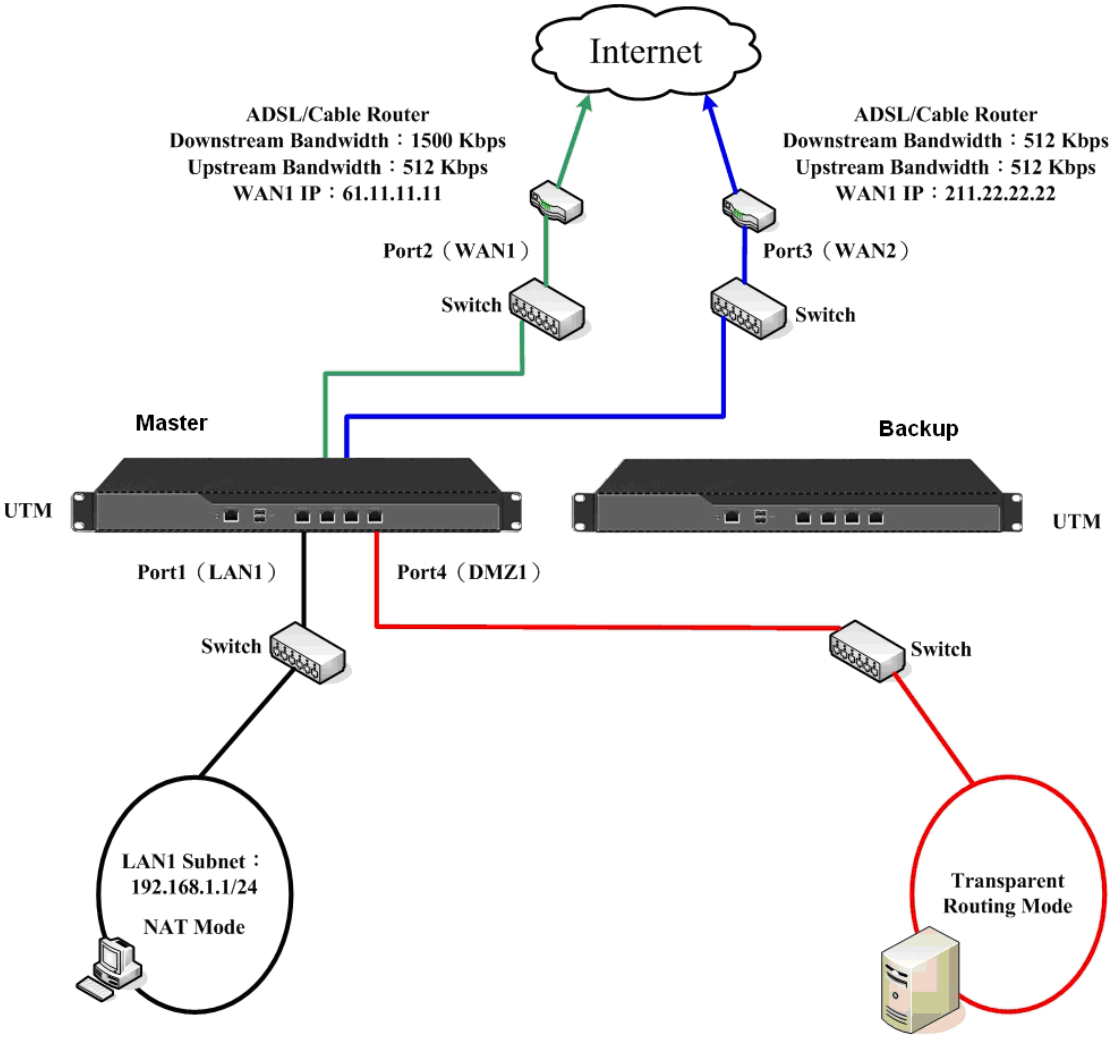


Figure 25-1 The Deployment of the Master Device under High Availability Mode

Step 2. Using the master device, configure the following High Availability settings under **Network > Interface**.（**Figure 25-2**）

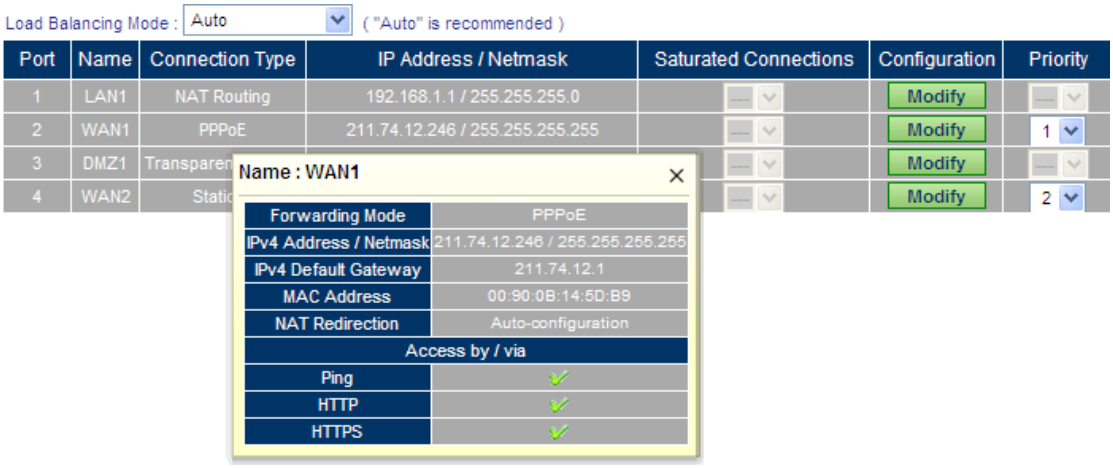


Figure 25-2 The IP Address for the LAN Interface

Step 3. Using the master device, configure the following High Availability settings under **Advance > High Availability > Settings:**

- Tick **Enable High Availability(HA).**
- For **HA Mode**, select **Active** from the drop-down list.
- For **HA Port**, select **Port1** from the drop-down list.
- Type the IP address in the **Management IP Address** field.
- Click **OK**.（**Figure 25-3**）

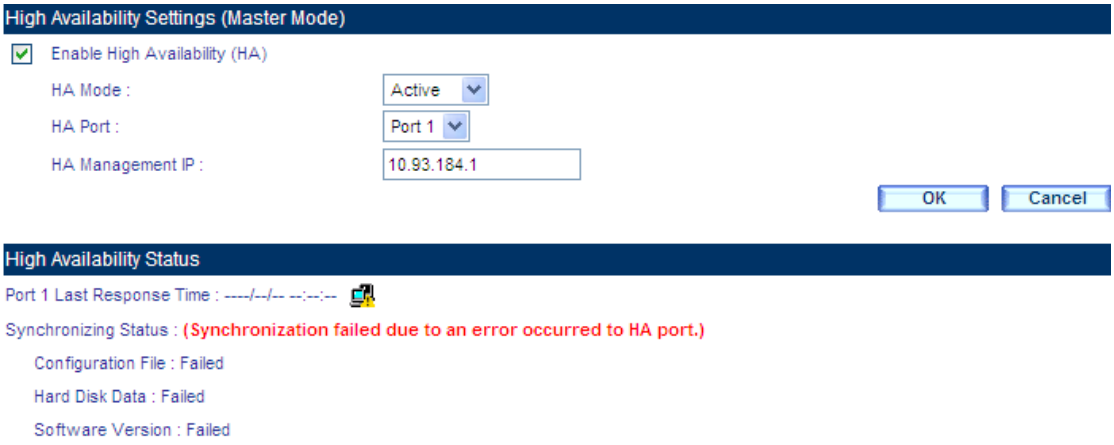


Figure 25-3 The Master Device Settings

Step 4. To set up the backup device, be sure the backup device is turned off and then configure the interface. Backup device's LAN port, WAN port and DMZ port must be different from Master device's. After the configuration, turn on the device.（**Figure 25-4**）

- The master device will daily synchronize itself with the backup device.
- The Backup device's **Management IP Address** will be assigned according to the Master device's setting while synchronization.

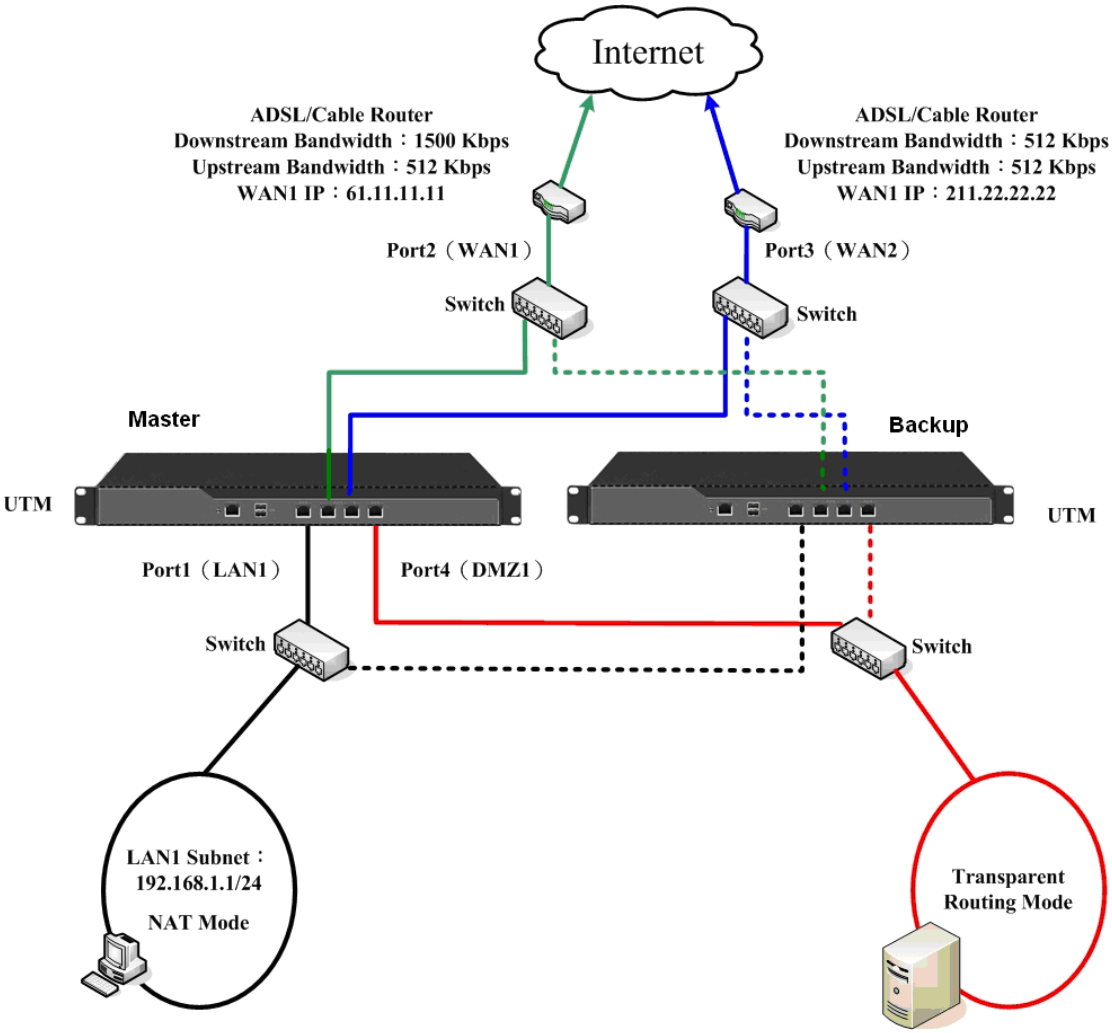


Figure 25-4 The High Availability Deployment

Important:

1. After the high availability deployment, if the first time synchronization between the master device and backup device is interrupted, please disable the high availability mode and then format hard disk and reset system to factory setting. After that, configure the synchronization according to the steps above again.

Note:

1. When deploying a high availability between two devices, the Master device must be turned on to avoid synchronization errors.
2. The built-in disk of the CS-2001 device can be changed. The capacity of the new disk should be larger than or equal to the capacity of the original one to avoid synchronization errors. (To synchronize the data of Backup device and Master device. It is recommended to change the disk of the Backup device first, and then change the disk of the Master device after synchronization.)
3. After deployment, the master device will operate. Once the master device fails, the backup device will take over the operations seamlessly.
4. The high availability mode will automatically synchronize firmware versions and configurations of both devices.
5. If the master device ceases to operate, the backup device will take over the operation.（**Figure 25-6**）

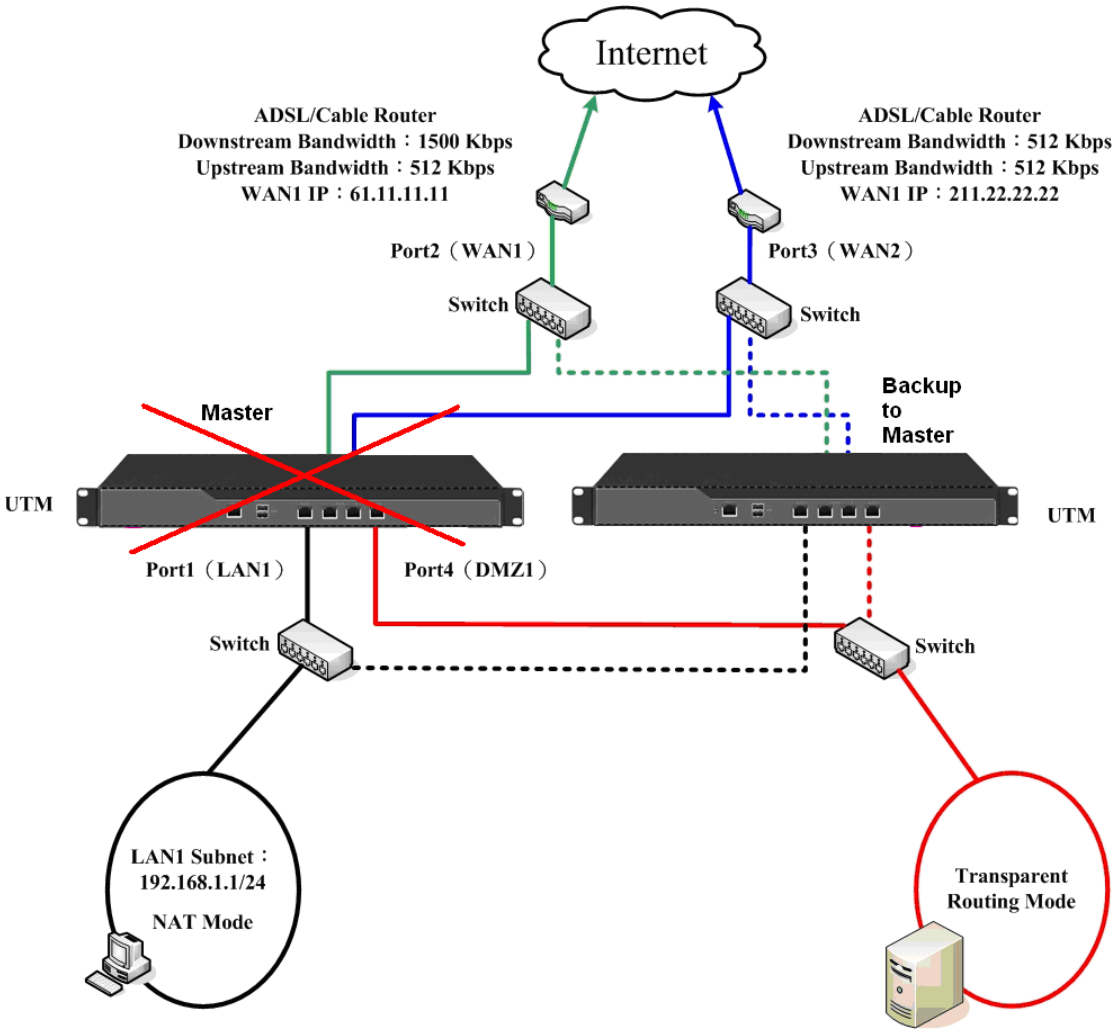


Figure 25-6 Backup Device Taking Over Operations When Master Device Fails

6. Note:

- During backup, if the WAN port is using a dynamic IP address and it is in the process of being renewed, the session will disconnect.
- IPSec VPN Connections: the IT administrator needs to set the **Keepalive IP Address** under **Policy Object > VPN > Trunk** so that a VPN session can be re-established without delay druing backup.
- PPTP VPN Connections: during backup, the connection will disconnect and the remote user will need to re-establish the connection.

Chapter 28 Co-Defense System

The CS-2001 can work in cooperation with the network's switch, to provide instant monitoring of the internal network's status. When the device detects an anomaly traffic flow, it will block the flow and provide information to help the IT administrator to resolve the problem before it slow down the entire network.

Terms in Core Switch

Name

- The name used to identify the switch.

Switch Model

- The switch model can be selected or it can be customized.

IP Version

- The Internet protocol that the system can use to telnet into the switch. There are IPv4 and IPv6.

IP Address

- The switch's IP address.

Port

- The port number that the system can use to telnet into the switch.

Username

- The username that the system can use to telnet into the switch.

Password

- The password that the system can use to telnet into the switch.

MAC Address Format

- The MAC address pattern that can be recognized by a switch. Listed below are four commonly seen patterns:
  - XX : XX : XX : XX : XX : XX
  - XX – XX – XX – XX – XX – XX
  - XXXXXXXXXXXX
  - XXXXXX - XXXXXX

Blocking Command

- This is the command the system uses to instruct the core switch to block an IP/MAC address.

Remove Blocking Command

- This command instructs the core switch to discontinue blocking an IP/MAC address.

Show Blocking Commands

- This command is used to view the IP/MAC addresses that the switch is blocking.

Note:

1. When the system detects the internal anomaly flow, the switch will use the following variables to block IP/MAC address, unblock already blocked IP/MAC addresses and view IP/MAC addresses.

- _ip_: indicates a blocked IP address.
- _mac_: indicates a blocked MAC address.
- _port_: indicates one of the switch ports.

28.1 Example

28.1.1 Quickly Isolating Any Anomaly Flow in the Internal

Network by Utilizing the Core and Edge Switch

Step 1. Go to **Anomaly Flow IP > Settings** and set as below: (**Figure 26-2**)

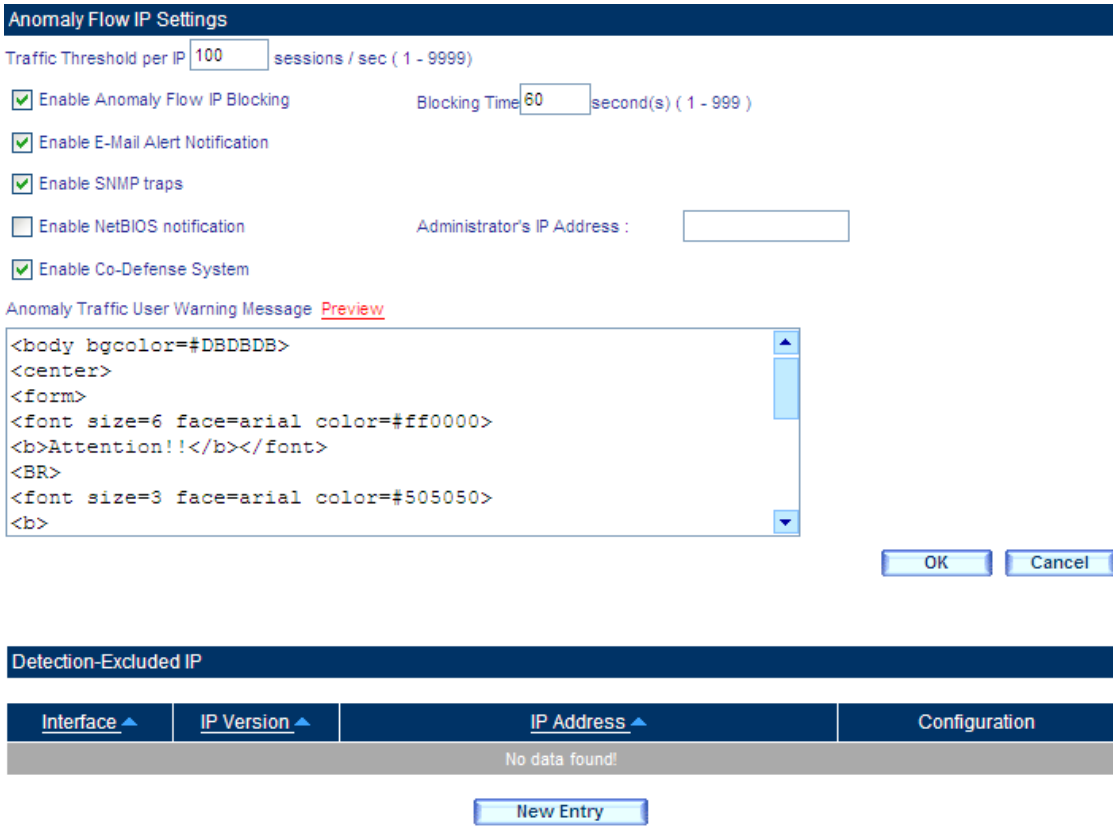


Figure 26-2 Anomaly Flow IP Settings

Step 2. Under **Advance** > **Co-Defense System** > **Core Switch**, set as below:（**Figure 26-3**）

- Enter the name to identify the switch.
- Select the model of the switch from the **Switch Model** drop-down list.
- Select **IPv4** from the **IP Version** drop-down list。
- Enter the switch's IP address in the **IP Address** field.
- Enter the port number, username and password to establish a telnet connection with the switch.
- Click **OK**.（**Figure 26-4**）
  - Click the **View** button to view the core switches blocking commands.
  - Click the **Modify** button to modify the core switches connection settings.
  - Click the **Remove** button to delete the core switches connection settings.
  - Clicking on the **Remove Blocked Address** link to remove a IP or MAC address which is blocked by the core switch.

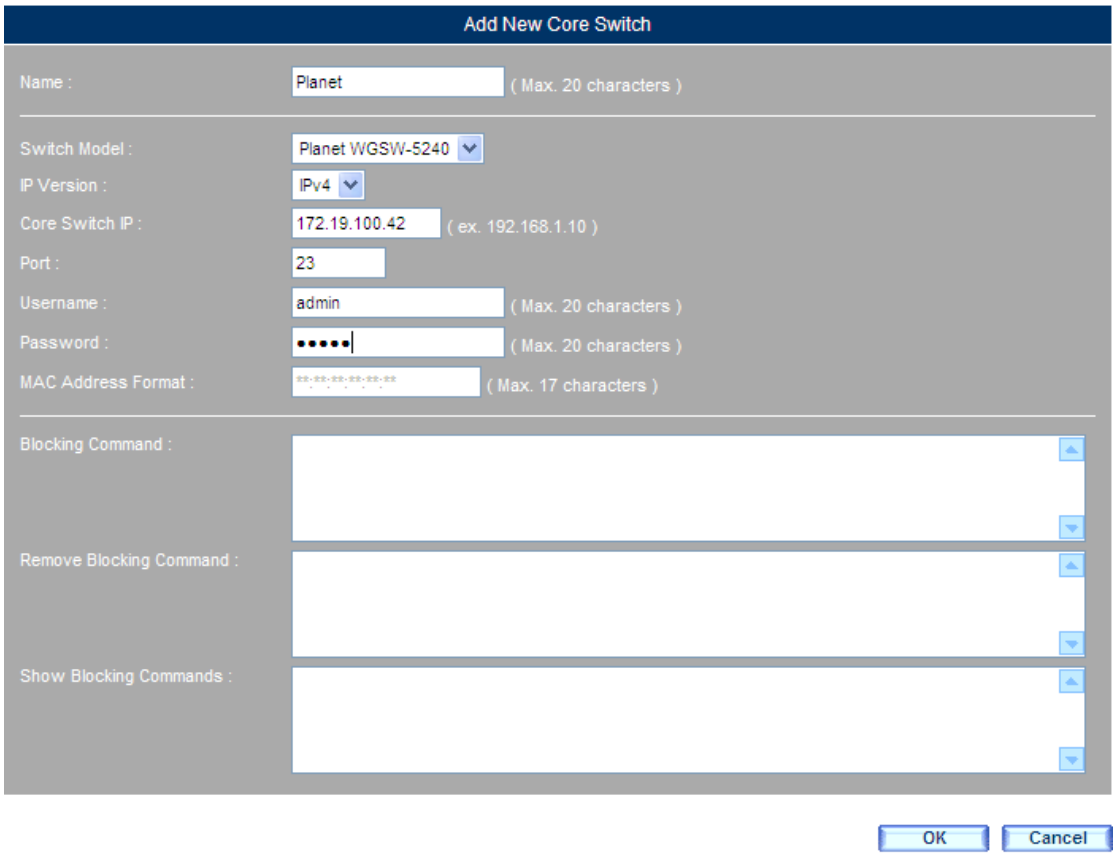


Figure 26-3 Configuring the Core Switch Connection

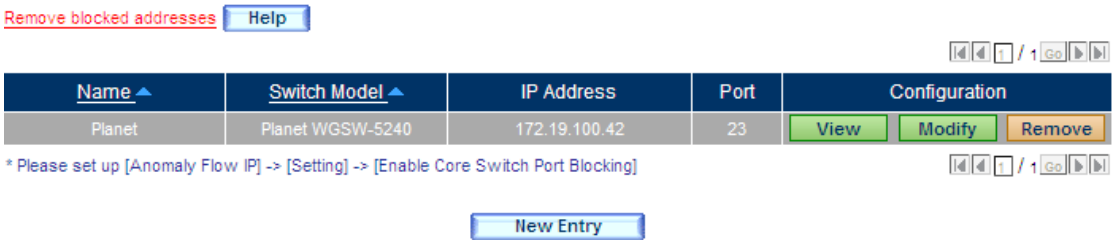


Figure 26-4 Core Switch Settings Completed

Step 3. Under **Advance > Co-Defense System > Edge Switch**, click **New Entry** and then set as below:（**Figure 26-9**）

- Type the name in the **Name** field.
- Select IPv4 from the **IP Version** drop-down list.
- Fill the **IP Address** field and the **Community String** field.
- Click **OK**.（**Figure 26-10**）

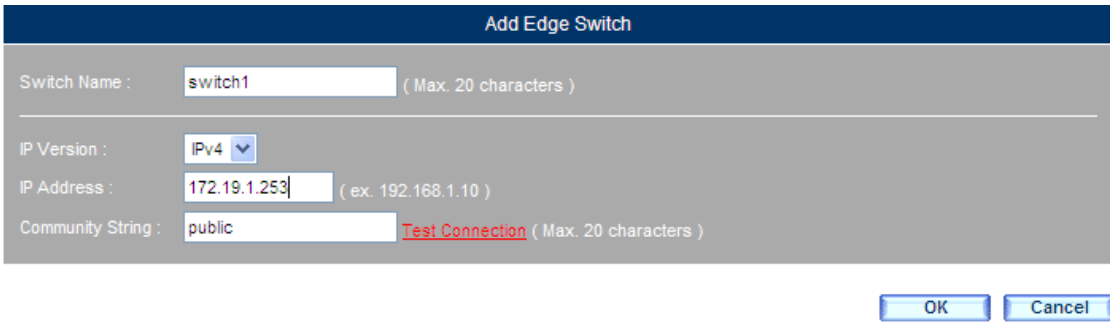


Figure 26-9 Connection Settings for the Core Switch

Figure 26-10 Completed Connection Settings for the Core Switch

Step 4. Go to **Advance > Co-Defense System > MAC ADDR Table.** Using SNMP, the CS-2001 can obtain the MAC addresses of any packets that pass through the edge switch.

Note:

1. Under **Advance > Co-Defense System > Edge Switch**, every port number from on the edge switch can be assigned with a description by clicking on **Details**.

Monitoring

Chapter 29 Logs

Log comprises logs of Traffic, Events, Connections, Viruses, Application Blocking, Concurrent Sessions and Quota. The system may send the logs to the IT administrator automatically or back up the logs to a remote device.

- Traffic Logs can be enabled under **Policy**, the sessions of the Policy will be recorded in detail.
- Event Logs have the records of any system configurations made. Each log denotes who, when, what and where that a configuration is being modified.
- Connection Logs comprehensively record all connection related data, such as VPN, PPPoE, SMTP, POP3, etc., providing the IT administrator with an instant insight when any connection issues arise.
- Virus Logs show the detected viruses from your HTTP, Webmail and FTP packets processed through the CS-2001.
- Application Blocking Logs provide details of all the applications that have been blocked by the CS-2001.
- Concurrent Sessions Logs provide details of the Max. Concurrent Sessions of each policy.
- Quota Logs provide details of the quota of each policy.

Terms in Settings

Logging Settings

- Logs are sent to the designated recipient once the file size reaches 300 KB.
- Logs can be backed up onto the remote device and SNMP Trap.
- The log setting of traffic, events, connections, viruses, application blocking, concurrent sessions and quota:
  - All logs on the built-in hard disk drive can be assigned a period of time for storing or deleting when expired.
  - You may enable email log, syslog message SNMP Trap alerts accordingly.

Terms in Traffic

Search

- Available search criteria are date, policy, priority, source IP, destination IP and port number.
  - Under **Monitoring > Logs > Traffic**, click **Search** and then set as below:
    - Enable the searching duration and then specify a period of time to search within.
    - Select All for **Policy.**
    - For **Priority**, it is set to **All** by default.
    - Click **Search**.（**Figure 27-1**）
    - Click **Download** to backup the searched results onto the local PC.（**Figure 27-2**）

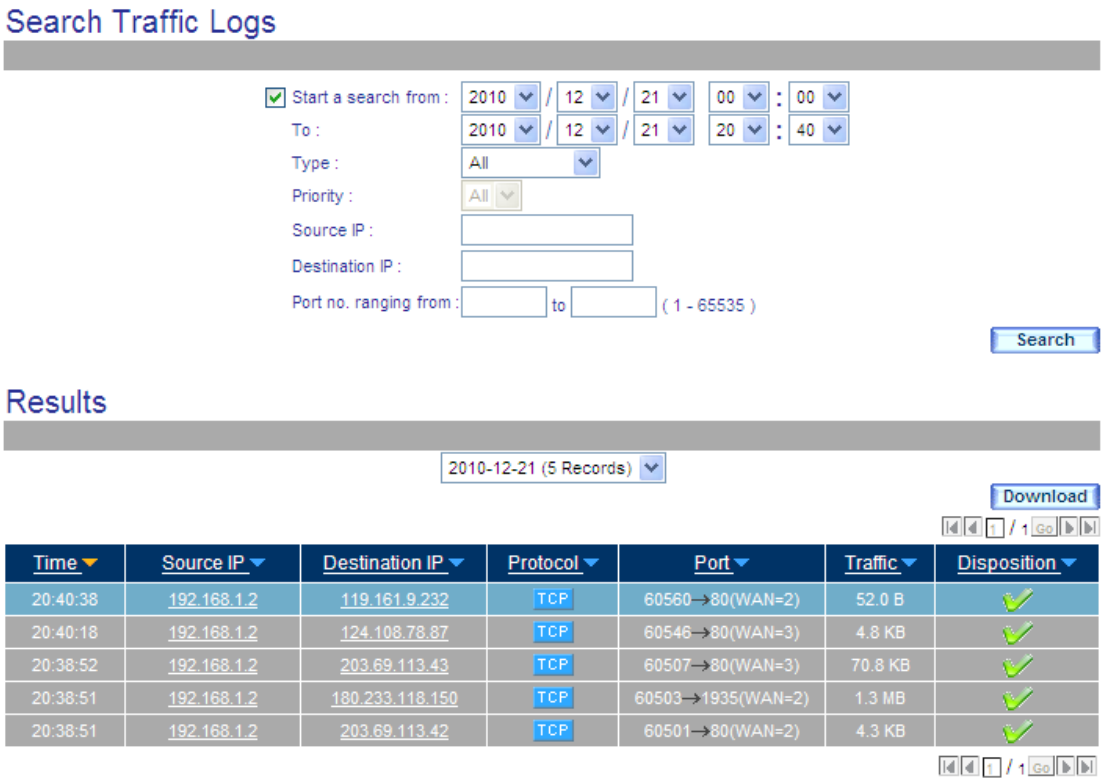


Figure 27-1 Searching for a Specific Log

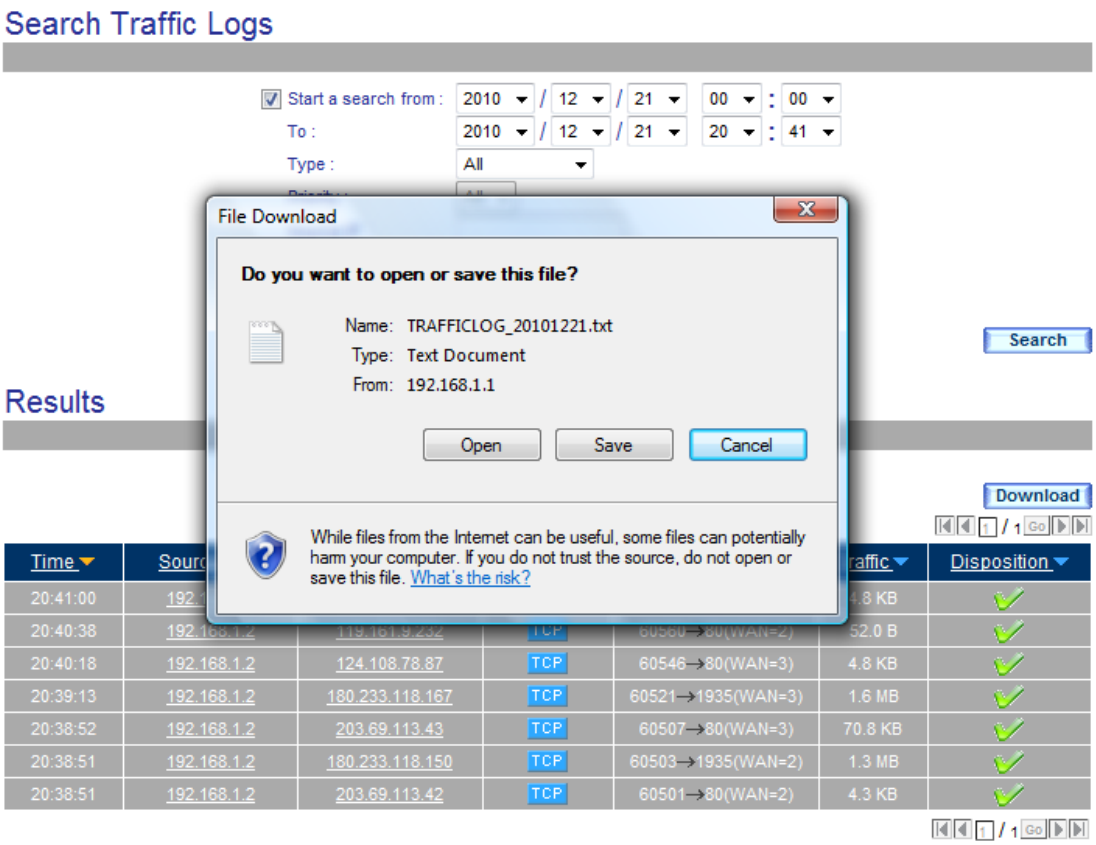


Figure 27-2 Downloading the Search Results

Terms in Events

Search

- Available search criteria are date, admin name, IP address, event type and event log with detailed content.
  - Under **Monitoring > Logs > Events**, click **Search** and then set as below:
    - Enable the search duration and then specify a period of time to search within.
    - Click **Search**.（**Figure 27-3**）

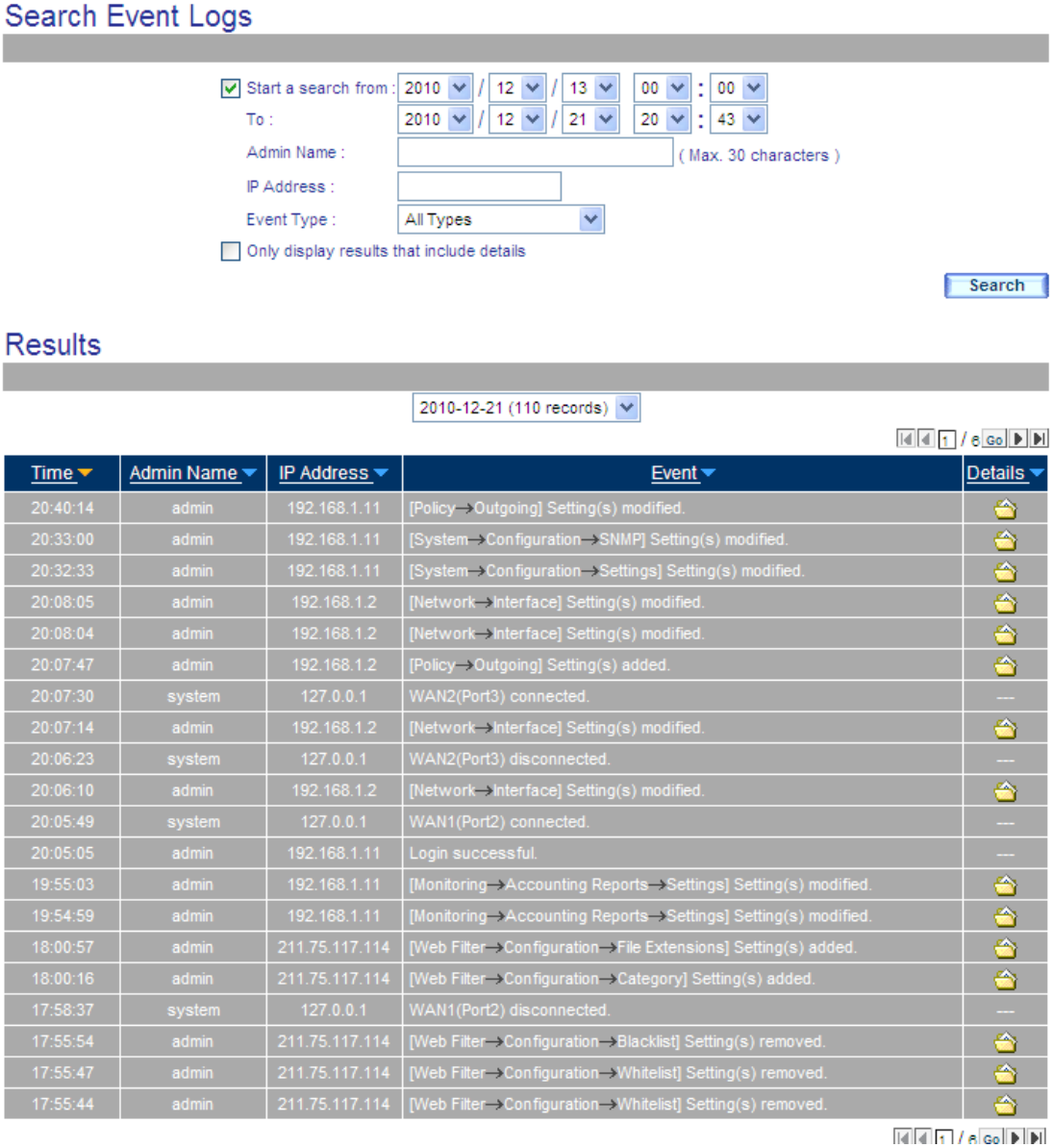


Figure 27-3 Searching for a Specific Log

Terms in Connection

Search

- PPPoE : Available search criteria are date and keyword.
- Dynamic IP Address: Available search criteria are date and keyword.
- DHCP: Available search criteria are date and keyword.
- PPTP Server : Available search criteria are date and keyword.
- PPTP Client : Available search criteria are date and keyword.
- IPSec : Available search criteria are date and keyword.
- Web VPN: Available search criteria are date and keyword.
- SMTP Inbound: Available search criteria are date, IP address, sender, recipient, status and detail.
- SMTP Outbound: Available search criteria are date, IP address, sender, recipient, status and detail.
- POP3 : Available search criteria are date, IP address, user name, status and detail.
  - Under **Monitoring > Logs > Connections**, click **Search** and then set as below:
    - Enable the search duration and then specify a period of time.
    - Click **Search**.（**Figure 27-4**）

Search Connection Logs

Start a search from : 2010 / 12 / 14 00 : 00

To : 2010 / 12 / 21 20 : 45

Search

Results

2010-12-21(3011 recorders)

1 / 151 Go

Time	Connection
20:05:48	Script /usr/sbin/ip-up.WAN1 started (pid 15125)
20:05:48	remote IP address 203.73.10.1
20:05:48	local IP address 203.73.10.36
20:05:48	kernel does not support PPP filtering
20:05:48	peer from calling number 00:30:88:01:23:C4 authorized
20:05:48	PAP authentication succeeded
20:05:48	Warning - secret file /etc/ppp/pap-secrets.WAN1 has world and/or group access
20:05:48	Warning - secret file /etc/ppp/pap-secrets.WAN1 has world and/or group access
20:05:48	Connect: WAN1_ppp <--> WAN1
20:05:48	Using interface ppp0
20:05:48	using channel 7
20:05:48	PPP session is 1383
20:05:48	PADS: Service-Name: ''
20:05:42	pppd 2.4.4 started by root, uid 0
20:05:42	RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
20:05:42	Plugin /usr/lib/pppd/2.4.4/rp-pppoe.so loaded.
20:05:16	Exit.
20:05:16	Unable to complete PPPoE Discovery
20:05:16	Timeout waiting for PADO packets
20:04:41	pppd 2.4.4 started by root, uid 0

1 / 151 Go

Figure 27-4 Searching for a Specific Log

Terms in Virus

Search

- Available search criteria are date, source IP, destination IP, application, infected file and virus name.
  - Under **Monitoring > Logs > Viruses**, click **Search** and then set as below:

Terms in Application Blocking

Search

- Available search criteria are date, source IP and keyword.
  - Under **Monitoring > Logs > Application Blocking**, click **Search** and then set as below:

Terms in Concurrent Sessions

Search

- Available search criteria are date and IP address.
  - Under **Monitoring > Logs > Concurrent Sessions**, click **Search** and then set as below:

Terms in Quota

Search

- Available search criteria are date and source IP.
  - Under **Monitoring > Logs > Quota**, click **Search** and then set as below:

29.1 Traffic

29.1.1 Viewing the Protocols and Port Numbers Used during an Access to CS-2001

Step 1. Go to **Policy> DMZ To WAN** and set as below:（**Figure 27-5**）

- Enable the **Packet Logging**.
- Click **OK**.（**Figure 27-6**）

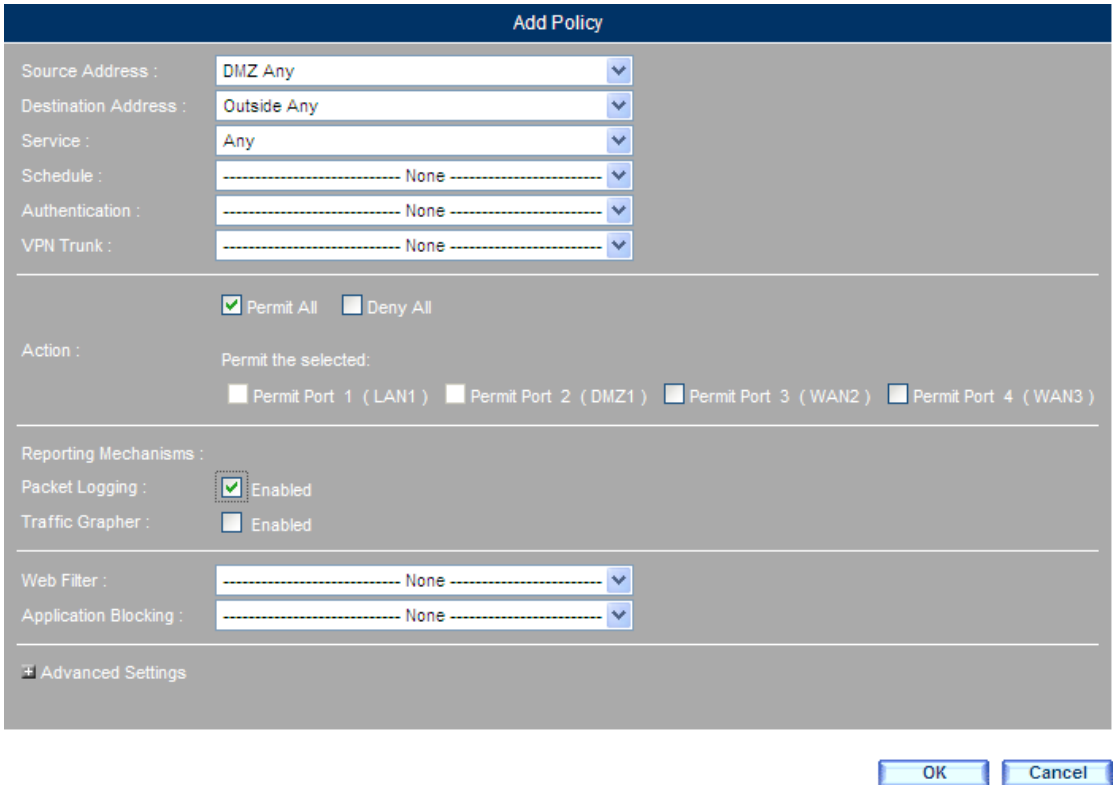


Figure 27-5 A Policy with Traffic Log

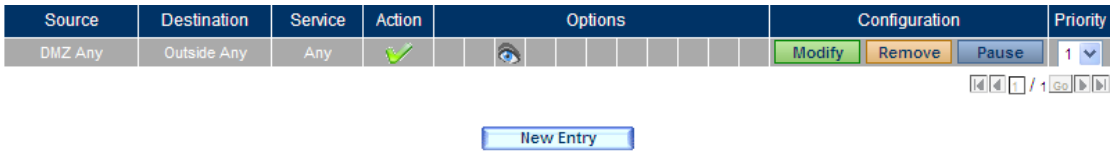


Figure 27-6 A Policy with Traffic Log Completed

Step 2. Under **Monitoring** > **Logs** > **Traffic**, it shows the traffic status of a policy. （**Figure 27-7**）

Refresh

1 / 31 Go

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
18:53:14	192.168.1.2	119.161.9.232	TCP	50590→80(WAN=3)	1.5 KB	✓
18:53:12	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:53:10	192.168.2.22	218.61.6.152	UDP	5041→8007(WAN=3)	135.0 B	✓
18:53:09	192.168.1.2	180.233.118.157	TCP	50589→1935(WAN=2)	231.2 KB	✓
18:53:08	192.168.1.2	67.195.133.149	TCP	50587→80(WAN=2)	2.8 KB	✓
18:53:08	192.168.1.2	119.161.9.232	TCP	50588→80(WAN=2)	1.5 KB	✓
18:53:02	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:52:52	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:52:50	192.168.2.22	119.167.215.53	UDP	5041→8003(WAN=3)	135.0 B	✓
18:52:48	192.168.1.2	203.84.204.124	TCP	50586→80(WAN=3)	1.5 KB	✓
18:52:48	192.168.1.2	119.160.246.14	TCP	50585→80(WAN=3)	30.9 KB	✓
18:52:46	192.168.1.2	61.213.183.97	TCP	50584→80(WAN=3)	4.3 KB	✓
18:52:45	192.168.1.2	72.30.14.127	TCP	50582→80(WAN=2)	1.6 KB	✓
18:52:45	192.168.1.2	203.84.196.149	TCP	50583→80(WAN=2)	3.0 MB	✓
18:52:44	192.168.1.2	67.195.160.33	TCP	50580→80(WAN=3)	1.5 KB	✓
18:52:44	192.168.1.2	203.69.138.19	TCP	50581→80(WAN=3)	42.9 KB	✓
18:52:43	192.168.1.2	203.84.204.124	TCP	50577→80(WAN=3)	1.7 KB	✓
18:52:43	192.168.1.2	124.108.78.87	TCP	50574→80(WAN=2)	4.8 KB	✓
18:52:43	192.168.1.2	124.108.103.68	TCP	50579→80(WAN=3)	5.5 KB	✓
18:52:43	192.168.1.2	124.108.103.68	TCP	50576→80(WAN=3)	8.1 KB	✓

1 / 31 Go

Clear

Figure 27-7 Traffic Log

Step 3. Click any Source IP or Destination IP, you will see of which protocols and ports it used and its traffic.（**Figure 27-8**）

Figure 27-8Monitoring the Traffic Flow of Each IP Address

Step 4. To clear the logs, click the **Clear** button and then click **OK** in the confirmation window.（**Figure 27-9**）

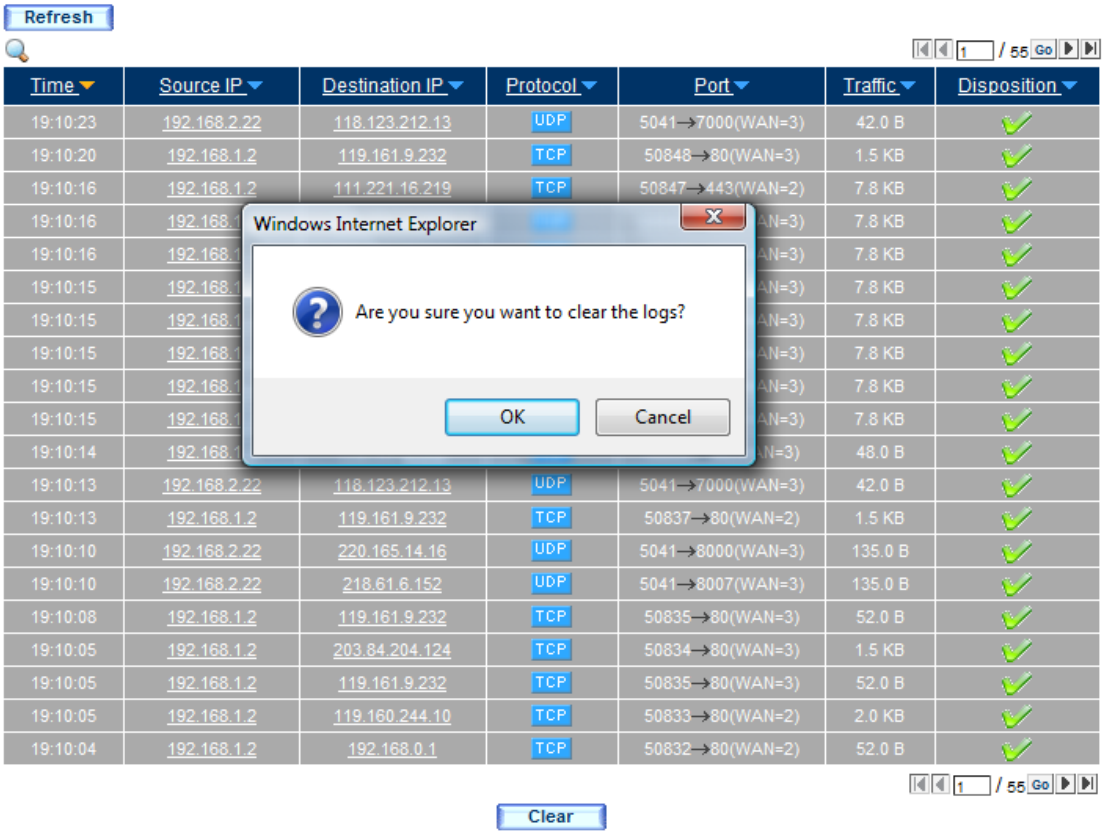


Figure 27-9 Deleting all the Traffic Log

29.2 Event

29.2.1 Viewing System History Access and the Status of WAN

Step 1. Under **Monitoring** > **Logs** > **Events**, there it shows the system history access and the status of WAN. (**Figure 27-10**)

- Click the icon for details. (**Figure 27-11**)

Time	Admin Name	IP Address	Event	Details
19:10:14	admin	192.168.1.2	Login successful.	---
18:40:17	admin	211.75.117.114	[Policy→DMZ to WAN] Setting(s) added.	
18:38:48	admin	211.75.117.114	[Network→Interface] Setting(s) modified.	
18:38:30	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	
18:38:26	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	
18:37:51	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	
18:37:47	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	
18:36:29	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	
18:22:04	admin	211.75.117.114	[Policy→Outgoing] Setting(s) modified.	
18:04:38	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	
18:04:25	admin	211.75.117.114	Login successful.	---
18:04:25	admin	211.75.117.114	[Policy→Incoming] Setting(s) added.	
18:04:07	admin	211.75.117.114	[Policy→Incoming] Setting(s) added.	
17:56:05	admin	211.75.117.114	Login successful.	---
17:56:03	admin	211.75.117.114	Login successful.	---
17:56:02	admin	211.75.117.114	Login successful.	---
17:55:51	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) added.	
17:54:02	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) added.	
16:45:27	admin	211.75.117.114	[Policy Object→Application Blocking→Settings] Setting(s) added.	
16:33:46	admin	211.75.117.114	[Policy Object→Application Blocking→Settings] Setting(s) added.	

1 / 2 Go

Figure 27-10 Event Logs

Date / Time	Admin Name	IP Address	Event
12/22 18:04	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.

Details

Before the Setting(s) Being Removed

1 / 1 Go

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1
Outside Any	[Port Mapping](211.22.2...	HTTP	✓		Modify Remove Pause	2
Outside Any	[Port Mapping](61.11.11....	HTTP	✓		Modify Remove Pause	3

1 / 1 Go

After the Setting(s) Being Removed

1 / 1 Go

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](211.22.2...	HTTP	✓		Modify Remove Pause	1
Outside Any	[Port Mapping](61.11.11....	HTTP	✓		Modify Remove Pause	2

1 / 1 Go

Figure 27-11 Specific Details of a History Event

29.3 Connection

29.3.1 Viewing the Connection Logs of WAN Interface

Step 1. Under **Monitoring** > **Logs** > **Connections**, it shows the logs of PPPoE, Dynamic IP Address, DHCP, PPTP Server, PPTP Client, IPSec, Web VPN, SMTP Inbound, SMTP Outbound and POP3.（**Figure 27-12**）

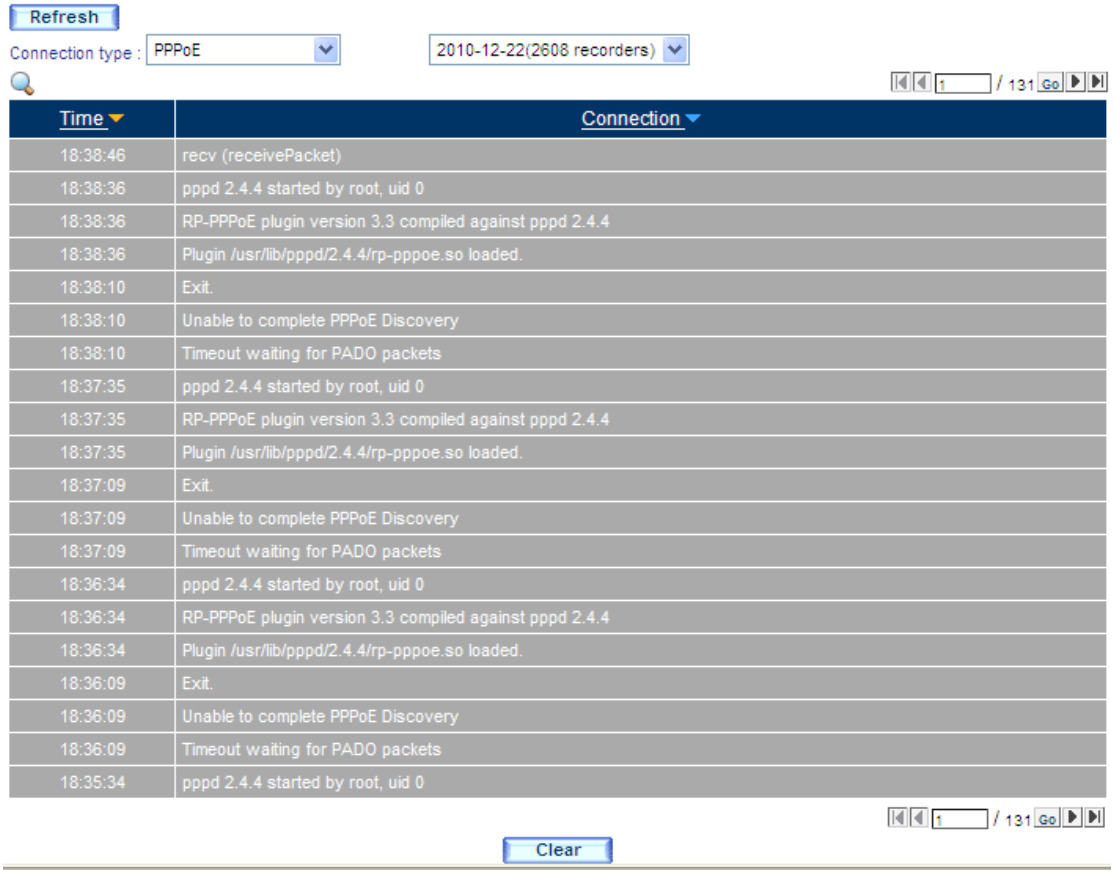


Figure 27-12 Connection Logs

Step 2. To delete the logs, click the **Clear** button and then click **OK** in the confirmation window.（**Figure 27-13**）

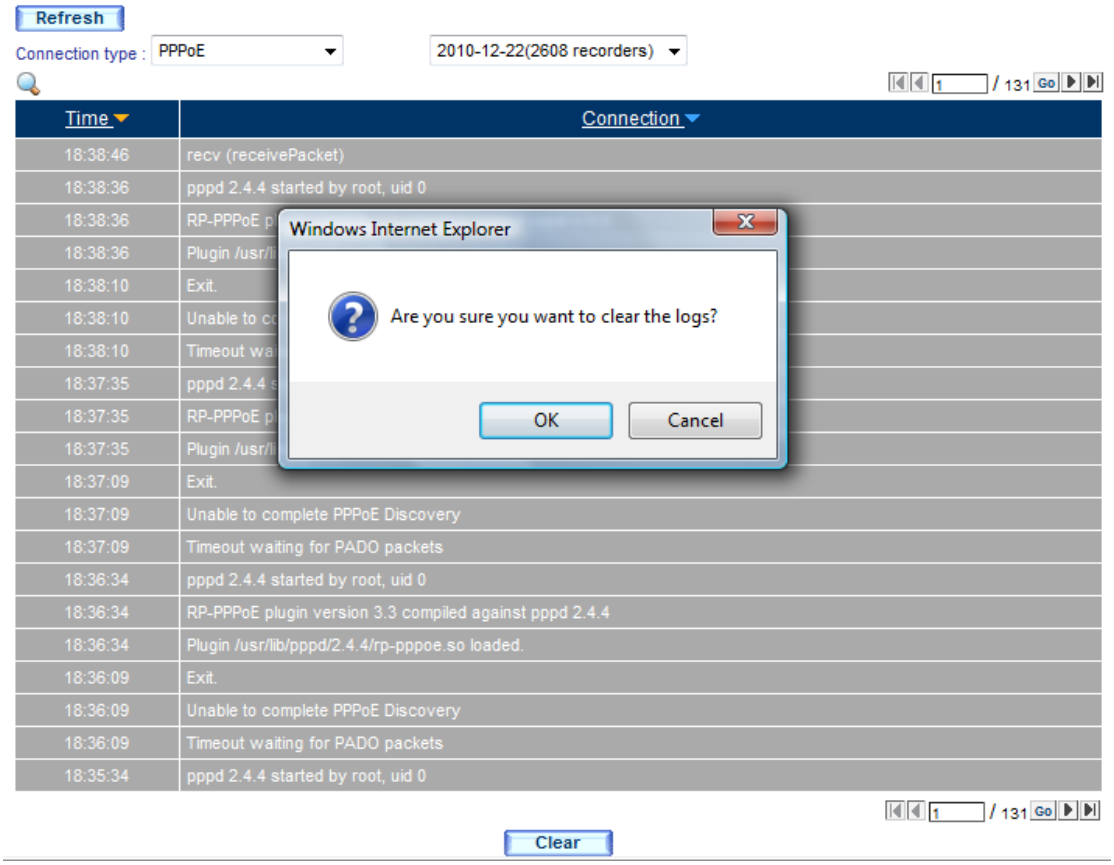


Figure 27-13 Deleting all the Connection Logs

29.4 Viruses

29.4.1 Viewing the Detected Viruses from Internal Users Using

HTTP / Web Mail / FTP Protocol to Transfer Files

Step 1. Go to **Policy** > **Outgoing** and then set as below: (**Figure 27-14**)

- For **Anti-Virus**, tick **HTTP/Webmail** and **FTP.**
- Click **OK**. (**Figure 27-15**)

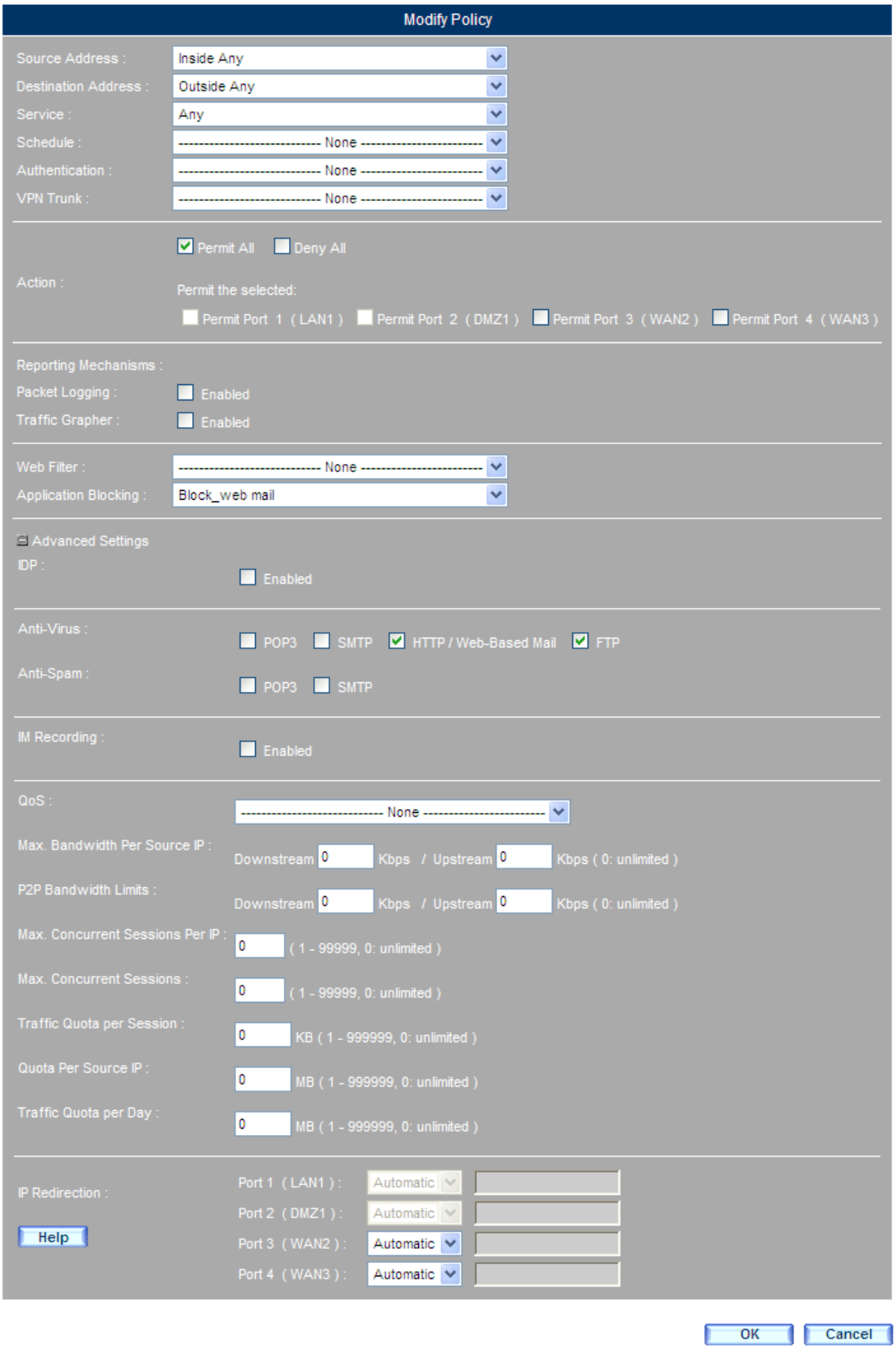


Figure 27-14 A Policy with HTTP/ WebMail and FTP

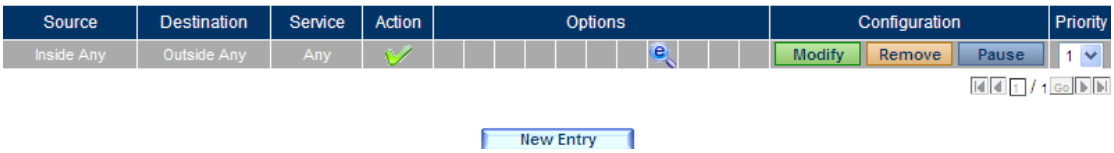


Figure 27-15 Policy Completed

Step 2. Under **Monitoring** > **Logs** > **Viruses**, it shows the logs of detected virus from the Internal users using HTTP/ WebMail and FTP protocol to transfer files.

Step 3. To delete the logs, click the Clear button and then click **OK**.

29.5 Application Blocking

29.5.1 Viewing the Logs

Step 1. Under **Policy** > **Outgoing**, set as below: （**Figure 27-16**）

- Select the defined application blocking.
- Click **OK**.（**Figure 27-17**）

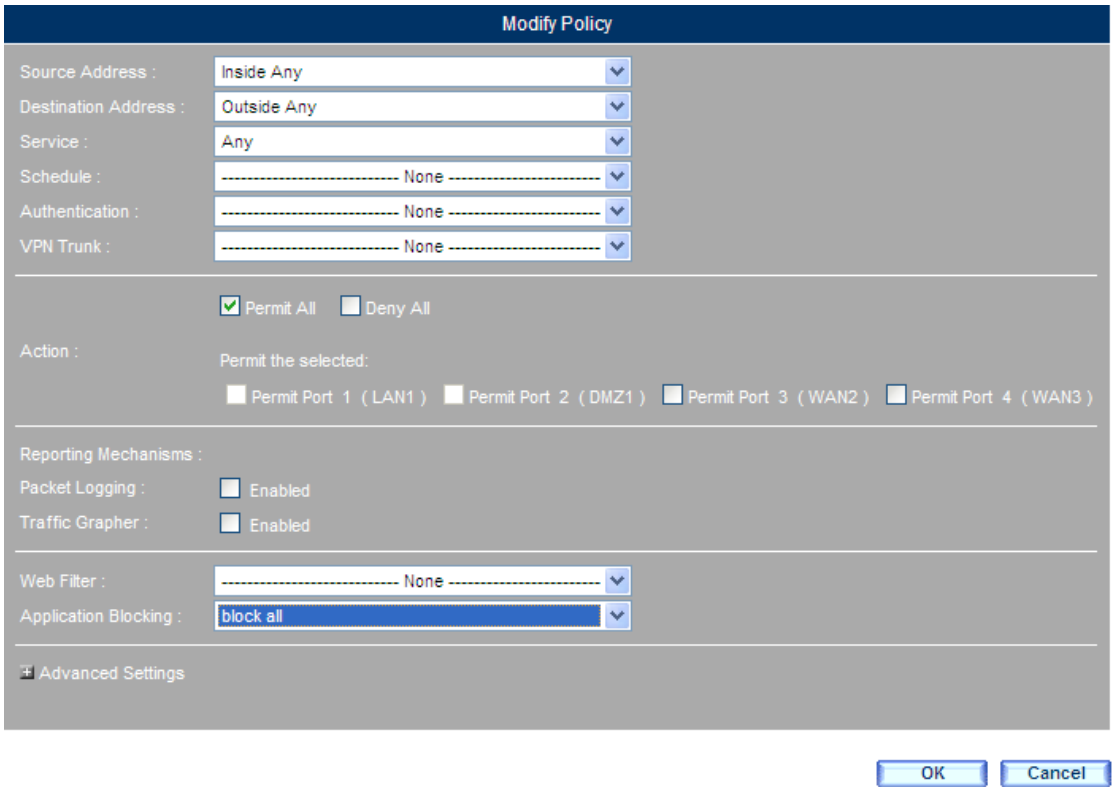


Figure 27-16 A Policy with Application Blocking

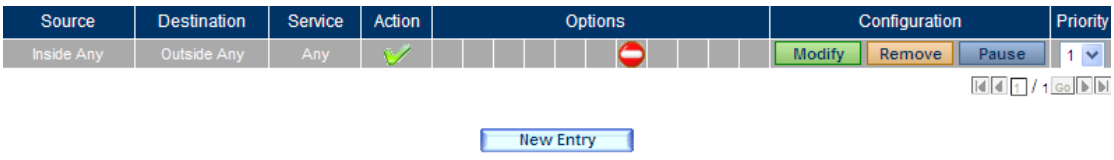


Figure 27-17 Policy Completed

Step 2. Under **Monitoring** > **Logs** > **Application Blocking**, it shows the logs of applicatons that have been blocked.（**Figure 27-18**）

Figure 27-18 Application Blocking Logs

Step 3. To delete the logs, click the **Clear** button and then click **OK** from the confirmation window.（**Figure 27-19**）

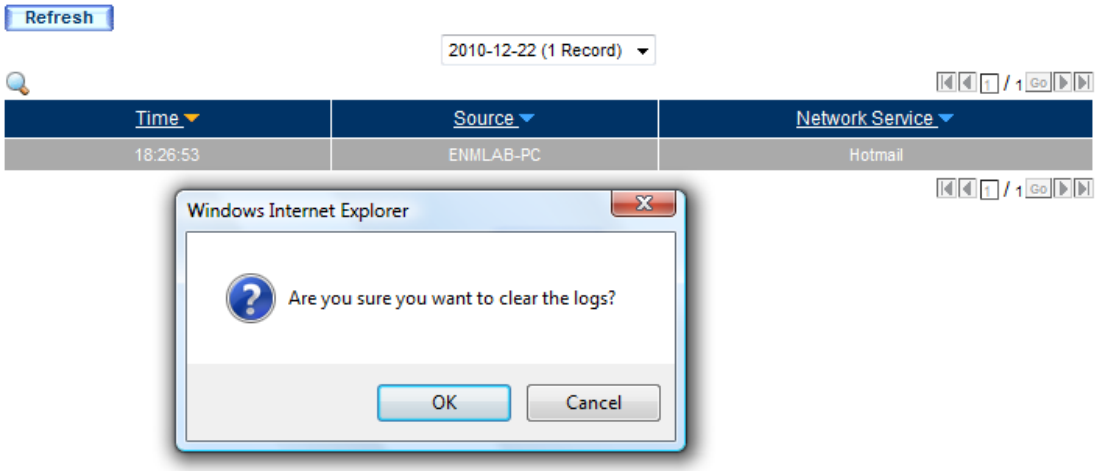


Figure 27-19 Deleting the Application Blocking Logs

29.6 Concurrent Sessions

29.6.1 Viewing the Logs of Concurrent Sessions that have been Exceeded the Configured Value

Step 1. Go to **Policy** > **Outgoing** and then set as below: (**Figure 27-20**)

- Enter a value in the **Max. Concurrent Sessions per IP** field
- Click **OK**. (**Figure 27-21**)

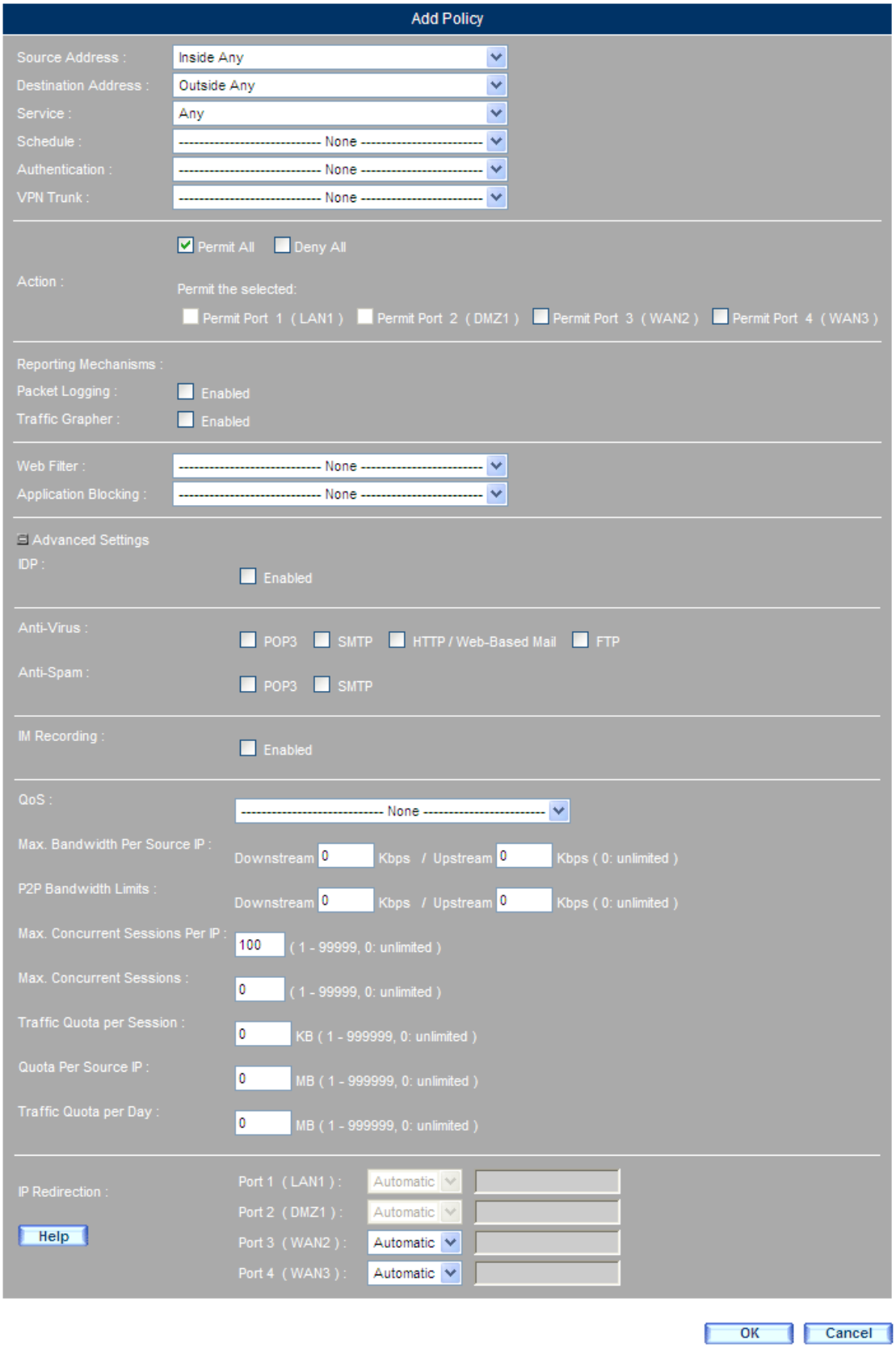


Figure 27-20 A Policy with Limitation of Concurrent Sessions

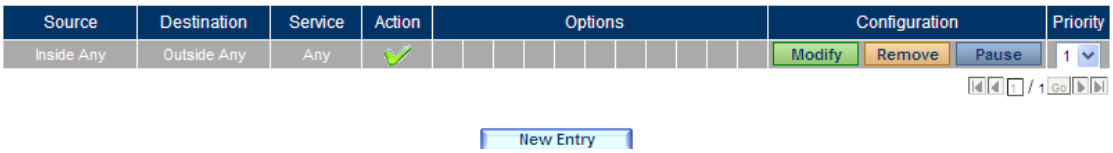


Figure 27-21 Policy Completed

Step 2. Under **Monitoring** > **Logs** > **Concurrent Sessions**, it shows the logs of the concurrent sessions that have exceeded the configured value.

Step 3. To delete the logs, click the **Clear** button and then click **OK** in the confirmation window.

29.7 Quota

29.7.1 Viewing the Logs of Quota that Has Been Reached

Step 1. Go to **Policy** > **Outgoing** and then set as below:（**Figure 27-22**）

- Type a value in the **Quota per Source IP** field.
- Click **OK**.（**Figure 27-23**）

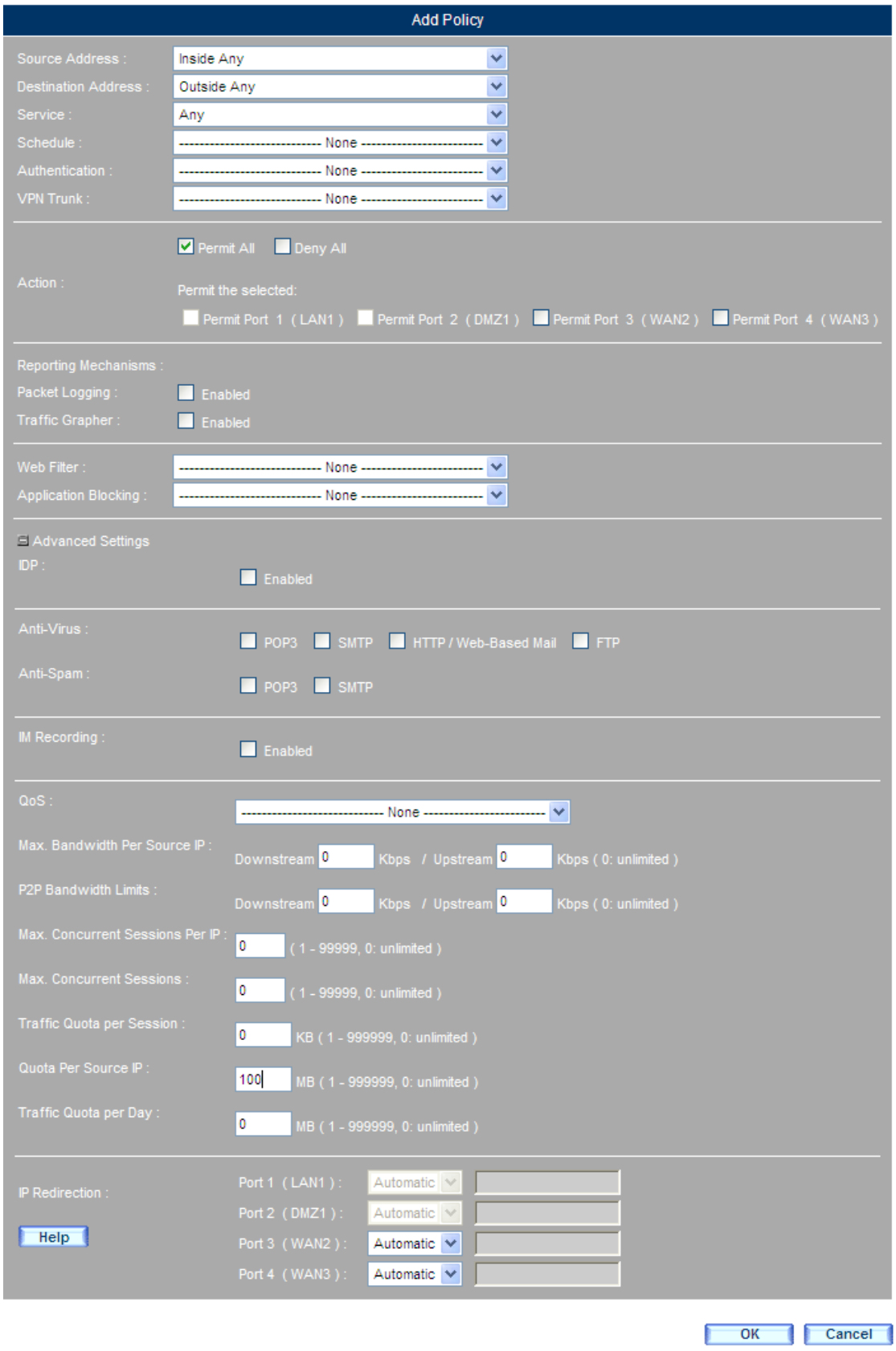


Figure 27-22 A Policy with Limitation of Quota per Source IP

Figure 27-23 Policy Completed

Step 2. Under **Monitoring** > **Logs** > **Quota**, it shows the logs of the quota that have reached the configured value.

Step 3. To delete the logs, click the **Clear** button and then click **OK** in the confirmation window.

29.8 Log Backup

29.8.1 Archiving or Retrieving Logs Generated by CS-2001

Step 1. Go to **System** > **Configuration** > **Settings** and then set as below:

- Tick **Enable email notifications** and then configure the related settings.（**Figure 27-24**）
- Tick **Enable syslog messages** and then configure the related settings.（**Figure 27-25**）

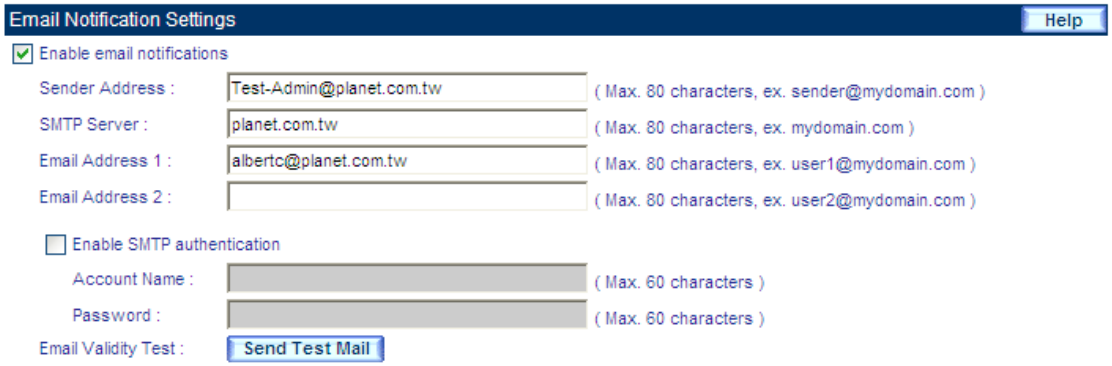


Figure 27-24 Enabling Email Notifications

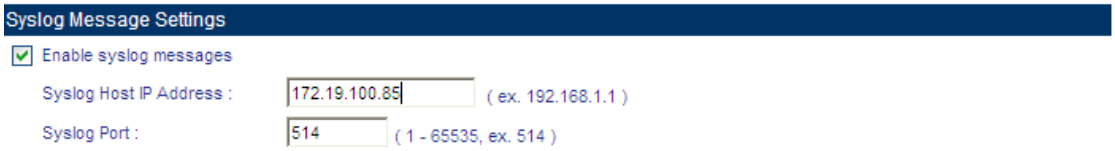


Figure 27-25 Enabling Syslog Messages

Step 2. Go to **System** > **Configuration** > **SNMP** and then set as below:（**Figure 27-26**）

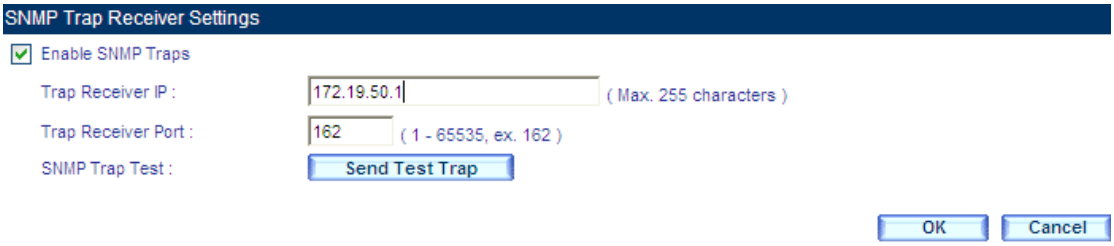


Figure 27-26 SNMP Trap Settings

Step 3. Go to **Monitor** > **Log** > **Settings** and then set as below: (**Figure 27-27**)

Figure 27-27 Monitoring Settings

Note:

1. Once **Email Notification** is enabled, the logs will be sent to the IT administrator when the files size reaches 300KB.
2. When syslog message is enabled, the logs will be delivered to the designated remote device.
3. When SNMP trap alerts is enabled, the logs can be delivered to a PC installed with SNMP Trap software.（**Figure 27-29**）

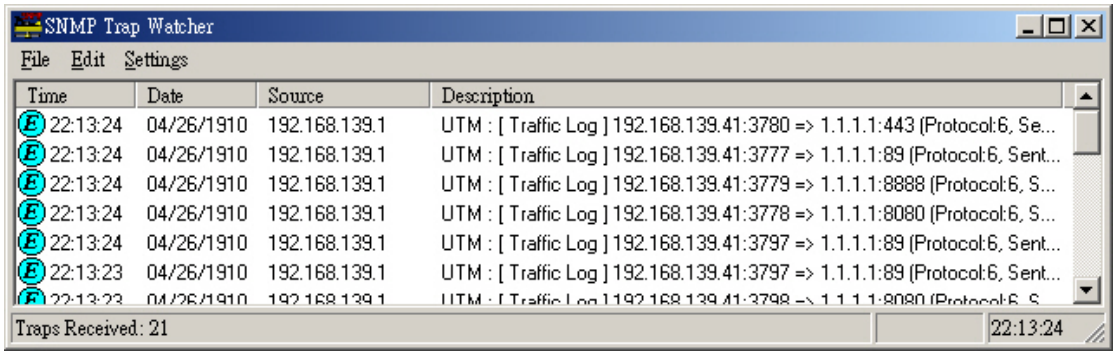


Figure 27-29 Sending SNMP Trap Alert

Chapter 30 Accounting Reports

Accounting report gives the IT administrator an insight into the various session of users that pass through the device, providing the IT administrator with detailed statistical reports and charts.

- Flow Analysis: displays the real-time traffic from the source IP and the traffic of each service.
- Today Top-N: displays the traffic from the source IP, destination IP, and service in the day.
- History Top-N: displays the certain duration of historic traffic from the source IP, destination IP and service.

Terms in Setting

Accounting Report Settings

- The configuration to enable or disable the recording of inbound and outbound data access and configure the storage period of the records.
  - Under **Monitoring > Accounting Reports > Settings**, set as below:
    - Tick **Enable outbound traffic recording** and then enter 14 in the **Storage period** field.
    - Tick **Enable inbound traffic recording** and then enter 14 in the **Storage period** field.
    - Click **OK**.（**Figure 28-1**）

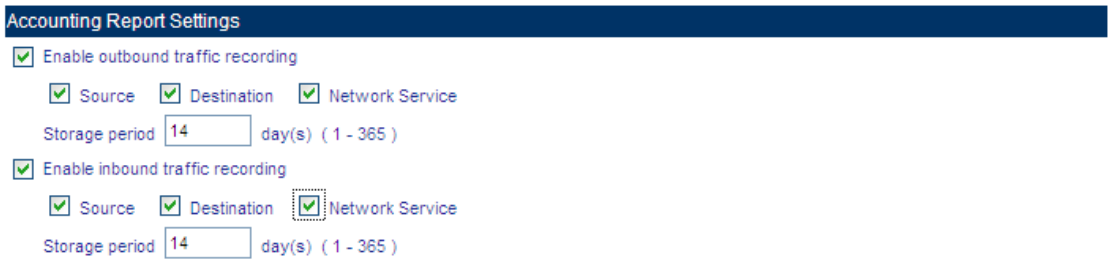


Figure 28-1 Accounting Report Settings

Terms in Flow Analysis

Source IP

- Displays the real-time traffic from the source IP.
- Source IP: indicates the source IP of the traffic.
- Traffic: indicates the traffic from the source IP.
- Provides the total traffic of all source IP and the traffic of individual source IP.

Service

- Displays the real-time traffic of services.
- Service: indicates the protocol and the port number of the traffic.
- Traffic: indicates the traffic of the service.
- Provides the total traffic of all services and the traffic of individual service.

Terms in Today Top-N

Time Slider

- Drag the two sliders to adjust the statistics' time interval (represented by the red portion.)

Source IP

- Indicates certain period of traffic of the source IP in the day.
- Source IP: indicates the source IP of the packets.
- Traffic Indicator: indicates the upload and download traffic of the source IP.
- Provides the total traffic of all source IP and the traffic of individual source IP.

Destination IP

- Indicates certain period of traffic of the destination IP in the day.
- Destination IP: indicates the destination IP of the packets.
- Traffic Indicator: indicates the upload and download traffic of the destination IP.
- Provides the total traffic of all destination IP and the traffic of the individual destination IP.

Service

- Indicates the certain period of traffic of the services in the day.
- Service: indicates the protocol and port number of the services.
- Traffic Indicator: indicates the upload and download traffic.
- Provides the total traffic of all services and the traffic of individual service.

Historical Top Chart

Refresh

- Available search criteria are date, source IP, destination IP and service.
  - Under **Monitoring > Accounting Reports > Historical Top Chart**, set as below:
    - Click **Source IP.**
    - Specify the time duration.
    - Click **Refresh**.（**Figure 28-2**）
    - Click **Download** to download the accounting report onto your local PC.（**Figure 28-3**）
    - To delete the accounting report, click **Clear All** on the upper-right corner and then click OK in the confirmation window.（**Figure 28-4**）

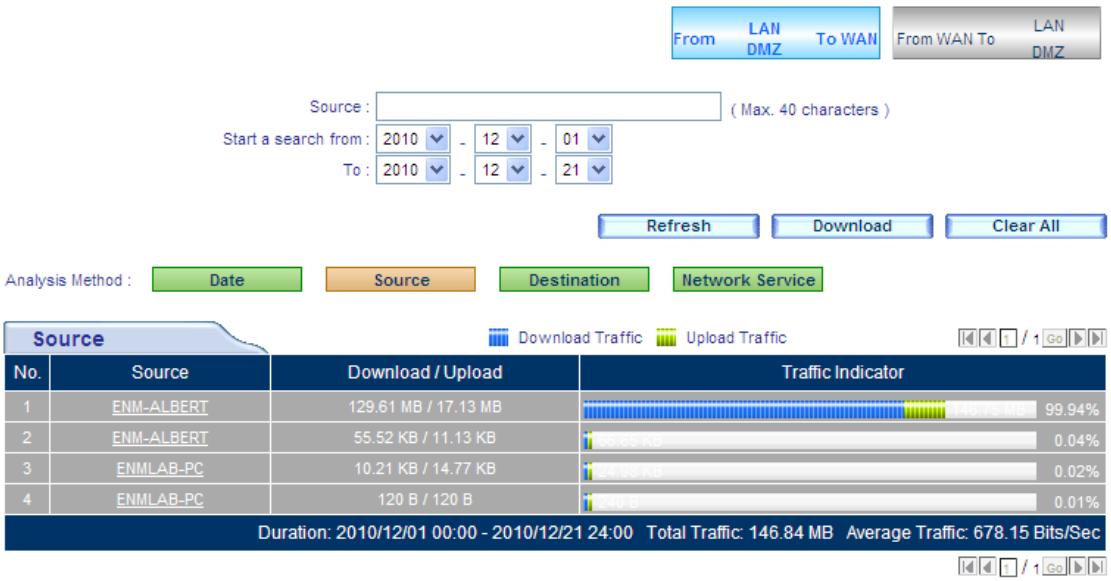


Figure 28-2 Searching for the Specific Log

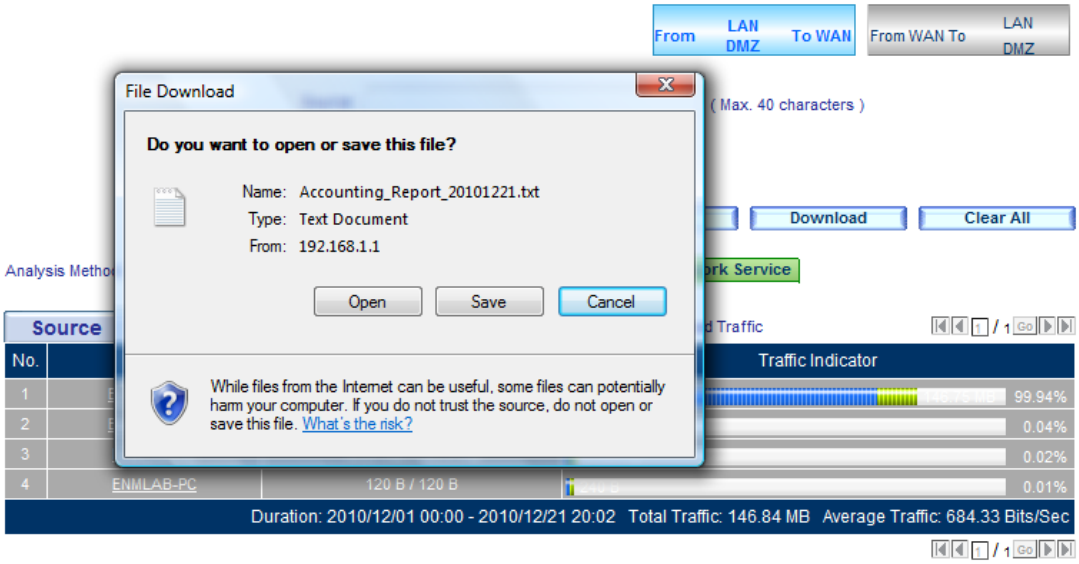


Figure 28-3 Downloading the Accounting Reports

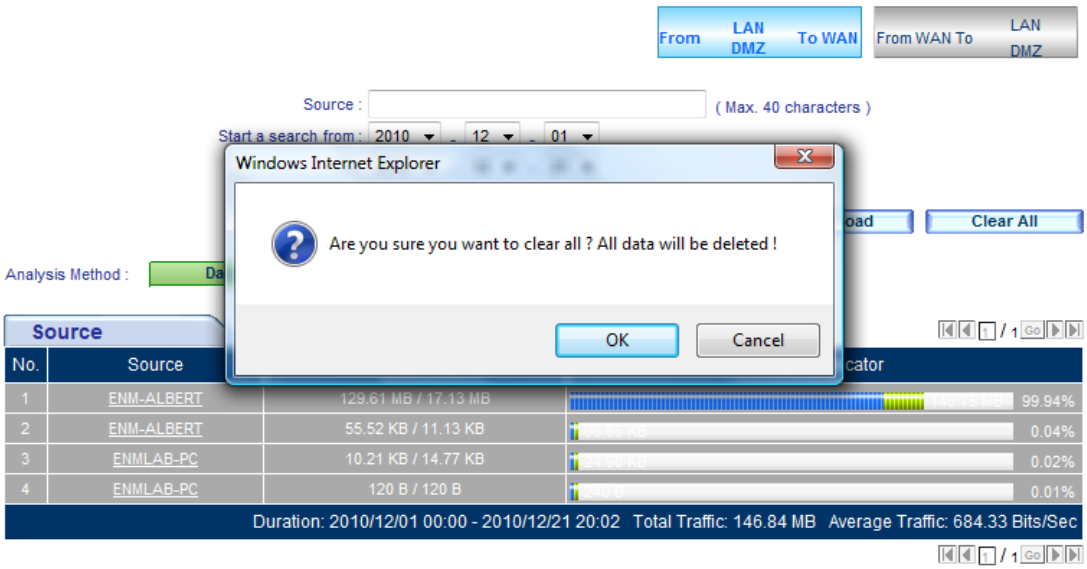


Figure 28-4 Deleting the Accounting Reprots

30.1 Flow Analysis

Step 1. Under **Monitoring** > **Accounting Reports** > **Flow Analysis**, it shows the traffic of source IP and service through CS-2001.（**Figure 28-5**）

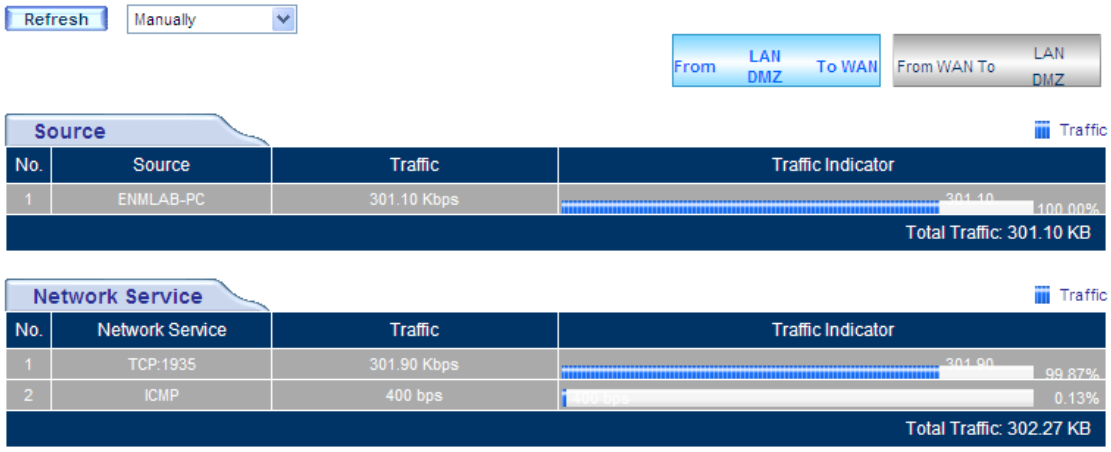
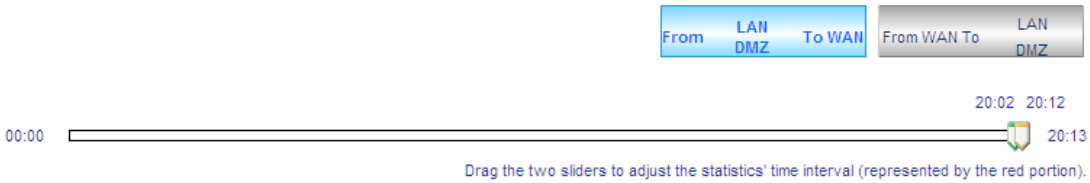


Figure 28-5 Flow Analysis

30.2 Today's Top Chart

Step 1. Under **Monitoring** > **Accounting Reports** > **Today's Top Chart**, it shows the traffic from the source IP, destination IP and the traffic of service through CS-2001 in the day.（**Figure 28-6**）



Source

Download Traffic Upload Traffic

No.	Source	Download / Upload	Traffic Indicator
1	ENMLAB-PC	6.79 MB / 292.87 KB	100.00%

Duration: 20:02 - 20:12 Total Traffic: 7.06 MB Average Traffic: 96.41 KBits/Sec

Destination

Download Traffic Upload Traffic

No.	Destination	Download / Upload	Traffic Indicator
1	c-2d45b2b821d322457734e...	1.91 MB / 36.04 KB	27.29%
2	c-17eaba26057c4c5233cb8...	1.51 MB / 28.80 KB	21.67%
3	c-f6350f9f76ae47ef0ece8ef...	1.17 MB / 23.78 KB	16.86%
4	c-9264f2d171e7f9d01bf9b5...	993.50 KB / 20.07 KB	14.02%
5	d.yimg.com	490.08 KB / 32.94 KB	7.23%
6	ts4.mm.bing.net	264.45 KB / 30.56 KB	4.08%
7	ts4.mm.bing.net	169.84 KB / 26.43 KB	2.71%
8	b.scorecardresearch.com	77.71 KB / 6.74 KB	1.17%
9	tw.yahoo.com	75.06 KB / 4.93 KB	1.11%
10	tw.video.news.yahoo.com	60.09 KB / 4.71 KB	0.90%
11	static.vap.yahoo.net	26.13 KB / 6.46 KB	0.45%
12	ad.yieldmanager.com	19.90 KB / 7.72 KB	0.38%
13	geo.yahoo.com	10.11 KB / 15.80 KB	0.36%
14	us.bc.yahoo.com	6.68 KB / 15.21 KB	0.30%
15	tw.news.yahoo.com	17.20 KB / 899 B	0.25%
16	cosmos.bcst.yahoo.com	12.32 KB / 4.38 KB	0.23%
17	urs.microsoft.com	12.64 KB / 3.41 KB	0.22%
18	tw.adserver.yahoo.com	8.38 KB / 6.69 KB	0.21%
19	b.scorecardresearch.com	4.17 KB / 4.48 KB	0.12%
20	cmk.tw.yahoo.overture.com	5.88 KB / 1.76 KB	0.11%

Duration: 20:02 - 20:12 Total Traffic: 7.06 MB Average Traffic: 96.41 KBits/Sec

Network Service

Download Traffic Upload Traffic

No.	Network Service	Download / Upload	Traffic Indicator
1	TCP:1935	5.54 MB / 108.66 KB	79.83%
2	HTTP	1.23 MB / 180.83 KB	19.90%
3	HTTPS	12.64 KB / 3.41 KB	0.22%
4	ICMP	3.29 KB / 0 B	0.05%

Duration: 20:02 - 20:12 Total Traffic: 7.06 MB Average Traffic: 96.41 KBits/Sec

Figure 28-6 Today Top-N

Step 2. You may drag the two sliders to adjust the statistics' time interval. The left one is the start time slider, the right one is the end time slider. Once you adjust the time interval, the Service IP accounting report, the Destination IP accounting report and the Service accounting report will be refreshed according to the new time interval.（**Figure 28-7**）

Source

Download Traffic Upload Traffic

No.	Source	Download / Upload	Traffic Indicator
1	ENMLAB-PC	15.03 MB / 529.13 KB	100.00%

Duration: 13:10 - 20:17 Total Traffic: 15.56 MB Average Traffic: 4.99 KBits/Sec

Destination

Download Traffic Upload Traffic

No.	Destination	Download / Upload	Traffic Indicator
1	c-9dc9cdc3dc5ebd79ea4ec...	3.82 MB / 69.92 KB	24.87%
2	c-0cbf2dde0b6ea00342913...	2.88 MB / 56.81 KB	18.76%
3	c-dce38372c89064d8fb4bd...	2.43 MB / 41.75 KB	15.83%
4	c-9264f2d171e7f9d01bf9b5...	1.98 MB / 36.29 KB	12.84%
5	c-17eaba26057c4c5233cb8...	1.51 MB / 28.80 KB	9.84%
6	c-2c341d7c97e1f85ee4d9b...	1.00 MB / 20.09 KB	6.58%
7	d.yimg.com	528.98 KB / 34.04 KB	3.54%
8	ts4.mm.bing.net	264.45 KB / 30.56 KB	1.85%
9	ts4.mm.bing.net	169.84 KB / 26.43 KB	1.23%
10	b.scorecardresearch.com	156.59 KB / 13.12 KB	1.07%
11	geo.yahoo.com	39.36 KB / 62.00 KB	0.64%
12	tw.video.news.yahoo.com	75.20 KB / 12.20 KB	0.55%
13	tw.yahoo.com	75.06 KB / 4.93 KB	0.50%
14	ad.yieldmanager.com	48.65 KB / 17.62 KB	0.42%
15	cosmos.bcst.yahoo.com	40.39 KB / 11.44 KB	0.33%
16	static.vap.yahoo.net	42.42 KB / 9.22 KB	0.32%
17	us.bc.yahoo.com	7.21 KB / 16.08 KB	0.15%
18	tw.news.yahoo.com	17.20 KB / 899 B	0.11%
19	b.scorecardresearch.com	8.34 KB / 8.89 KB	0.11%
20	tw.adserver.yahoo.com	9.51 KB / 7.46 KB	0.11%

Duration: 13:10 - 20:17 Total Traffic: 15.56 MB Average Traffic: 4.99 KBits/Sec

Network Service

Download Traffic Upload Traffic

No.	Network Service	Download / Upload	Traffic Indicator
1	TCP:1935	13.56 MB / 253.58 KB	88.73%
2	HTTP	1.48 MB / 272.16 KB	11.14%
3	HTTPS	12.64 KB / 3.41 KB	0.10%
4	ICMP	4.82 KB / 0 B	0.03%

Duration: 13:10 - 20:17 Total Traffic: 15.56 MB Average Traffic: 4.99 KBits/Sec

Figure 28-7 Today Top-N Report according to the Time Interval

Step 3. By clicking any source IP, a pop-up window will show its destination IP and service.（**Figure 28-8**）

Source : ENMLAB-PC

Destination

Download Traffic Upload Traffic 1 / 2 Go

No.	Destination	Download / Upload	Traffic Indicator
1	c-9dc9cdc3dc5ebd79ea4ec...	3.82 MB / 69.92 KB	24.82%
2	c-0cbf2dde0b6ea00342913...	2.88 MB / 56.81 KB	18.72%
3	c-fcf65db126a89f6a16f2e2...	2.43 MB / 41.75 KB	15.79%
4	c-9264f2d171e7f9d01bf9b5...	1.98 MB / 36.29 KB	12.81%
5	c-17eaba26057c4c5233cb8...	1.51 MB / 28.80 KB	9.82%
6	c-2c341d7c97e1f85ee4d9b...	1.00 MB / 20.09 KB	6.57%
7	d.yimg.com	528.98 KB / 34.04 KB	3.53%
8	ts4.mm.bing.net	264.45 KB / 30.56 KB	1.85%
9	ts4.mm.bing.net	169.84 KB / 26.43 KB	1.23%
10	b.scorecardresearch.com	156.59 KB / 13.12 KB	1.06%
11	geo.yahoo.com	51.17 KB / 80.79 KB	0.83%
12	tw.video.news.yahoo.com	82.85 KB / 15.96 KB	0.62%
13	tw.yahoo.com	75.06 KB / 4.93 KB	0.50%
14	ad.yieldmanager.com	58.26 KB / 20.92 KB	0.50%
15	cosmos.bcst.yahoo.com	48.53 KB / 13.86 KB	0.39%
16	static.vap.yahoo.net	42.42 KB / 9.22 KB	0.32%
17	us.bc.yahoo.com	11.50 KB / 23.06 KB	0.22%
18	tw.adserver.yahoo.com	18.50 KB / 13.70 KB	0.20%
19	tw.news.yahoo.com	17.20 KB / 899 B	0.11%
20	b.scorecardresearch.com	8.34 KB / 8.89 KB	0.11%

Duration: 13:10 - 20:17 Total Traffic: 15.60 MB Average Traffic: 4.10 KBits/Sec

1 / 2 Go

Network Service

Download Traffic Upload Traffic 1 / 1 Go

No.	Network Service	Download / Upload	Traffic Indicator
1	TCP:1935	13.56 MB / 253.58 KB	88.20%
2	HTTP	1.53 MB / 315.83 KB	11.67%
3	HTTPS	12.64 KB / 3.41 KB	0.10%
4	ICMP	4.82 KB / 0 B	0.03%

Duration: 13:10 - 20:17 Total Traffic: 15.65 MB Average Traffic: 5.00 KBits/Sec

1 / 1 Go

Figure 28-8 The Destination IP and Service

Step 4. By clicking any Destination IP, a pop-up window will show its source IP and service.（**Figure 28-9**）

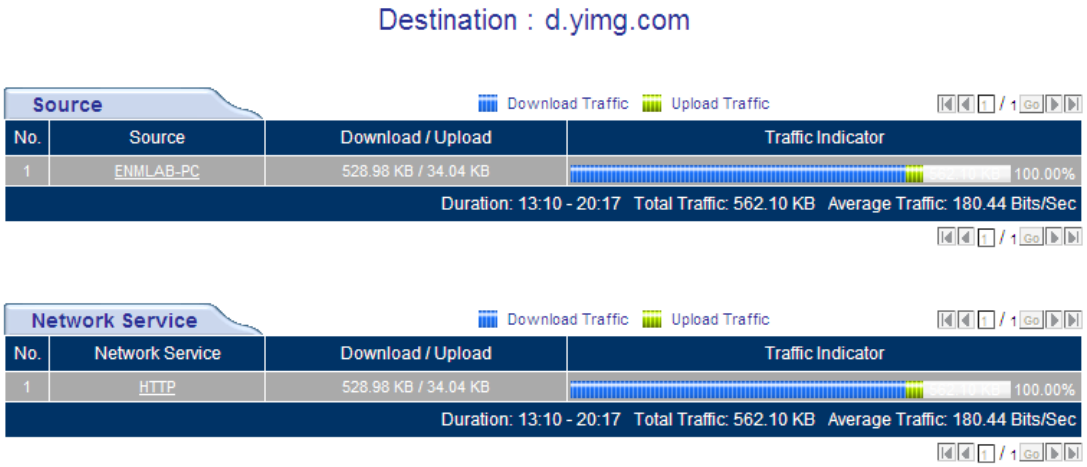


Figure 28-9 The Source IP and Service

Step 5. By clicking any service, it will show its source IP and destination IP.
（**Figure 28-10**）

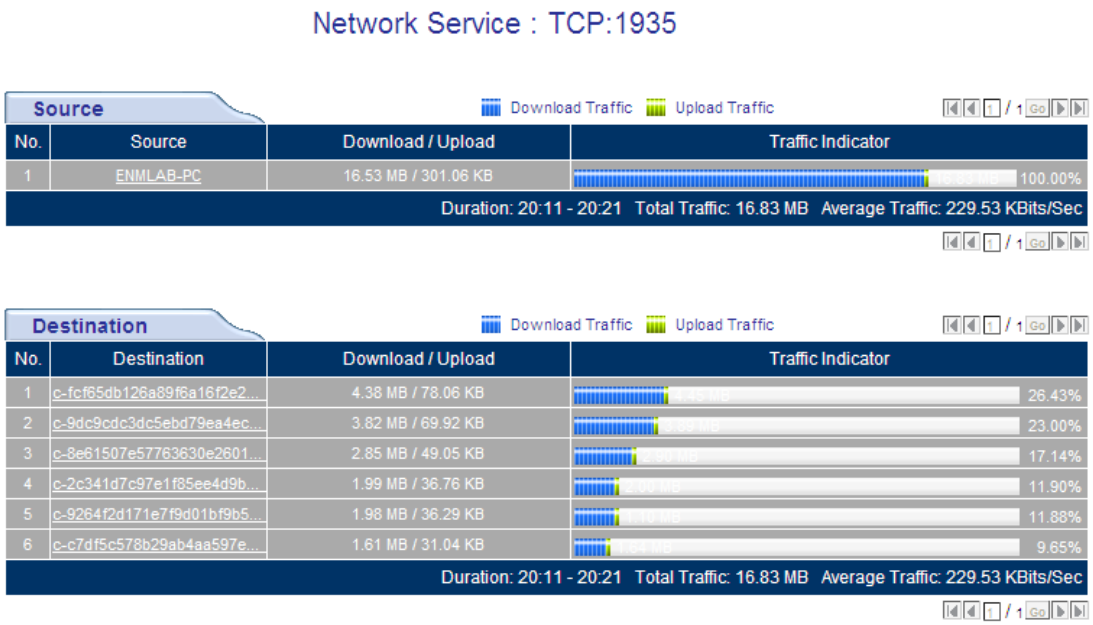


Figure 28-10 The Source IP and Destination IP

30.3 Historical Top Chart

Step 1. Under **Monitoring > Accounting Reports > Historical Top Chart**, you may see the traffic of the source IP, destination IP and service of the certain duration by specifying the date.（**Figure 28-11**）

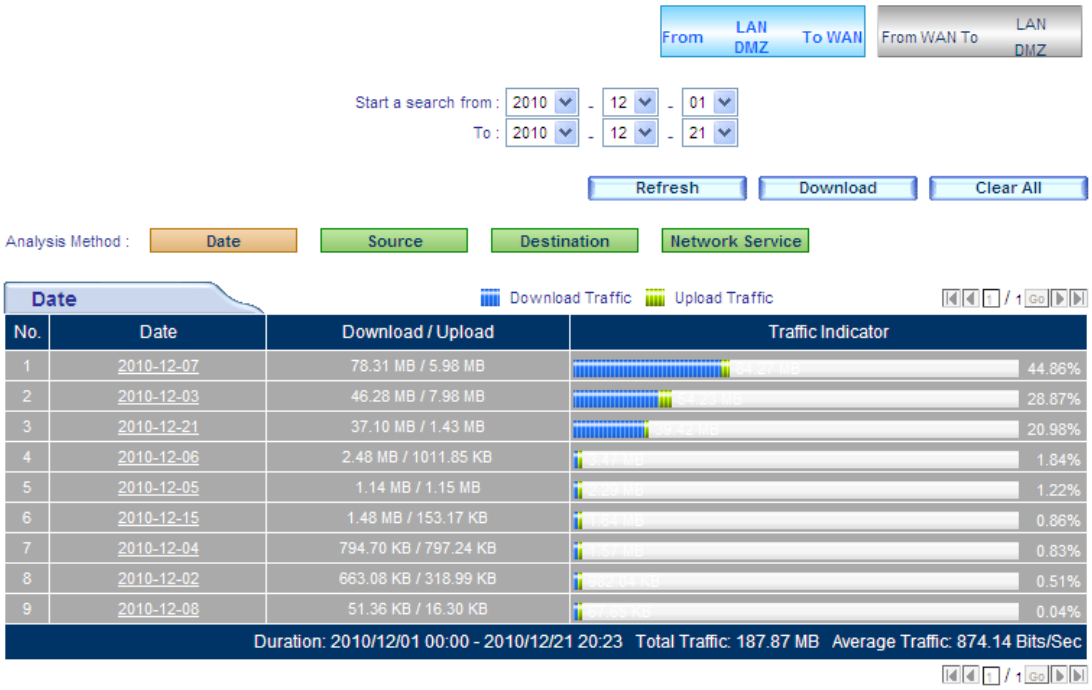


Figure 28-11 History Top-N

Chapter 31 Traffic Grapher

Statistics delivers comprehensive information regarding network traffic, enabling the IT administrator to gain a thorough understanding of traffic flow across the WAN interfaces and packets managed by policies.

- *WAN Traffic* provides upstream and downstream traffic flow statistics of all packets passing through the WAN interfaces based on their corresponding policies.
- *Policy-Based Traffic* provides upstream and downstream traffic flow statistics of all packets passing through the WAN interfaces based on their corresponding policies.

Traffic Grapher

Charts

- Vertical axis indicates the network traffic.
- Horizontal axis indicates time.

Type/ Source/ Destination/ Service/ Action

- The Items infer what **Policy** is used.

Time

- The statistics are available in time units of per minute, hour, day, week, month and year.

Note:

1. The displayed frequency of each time unit:

- Minutes：Statistics charts are presented based data collected every minute.
- Hours：Statistics charts are presented based on data collected hourly.
- Days：Statistics charts are presented based on data collected daily.
- Weeks：Statistics charts are presented based on data collected weekly.
- Months：Statistics charts are presented based on data collected monthly.
- Years：Statistics charts are presented based on data collected every year.

Bits/sec, Bytes/sec, Utilization, Total

- The IT administrator can modify the unit display from the chart's vertical axis.
  - Bits/ sec: indictes the bits per second.
  - Bytes/ sec: indicates the bytes per second.
  - Utilization: Shows the proportion relative to the Max. Downstream / Upstream Bandwidth set in the policy.
  - Accumulated: The vertical axis is drawn based on the total traffic accumulated.

31.1 WAN Traffic

Step 1. In **Monitoring** > **Traffic Grapher** > **WAN Traffic,** it shows the statistics of upstream / downstream packets over the WAN interface. The statistic charts are available in the time unit of minute, hour, day, week, month and year. Click **Minutes** for statistic charts in the time unit of minute；Click **Hours** for statistic charts in the time unit of hour；Click **Days** for statistic charts in the time unit of day；Click **Weeks** for statistic charts in the time unit of week；Click **Months** for statistic charts in the time unit of month；Click **Years** for statistic charts in the time unit of year. （**Figure 29-1**）

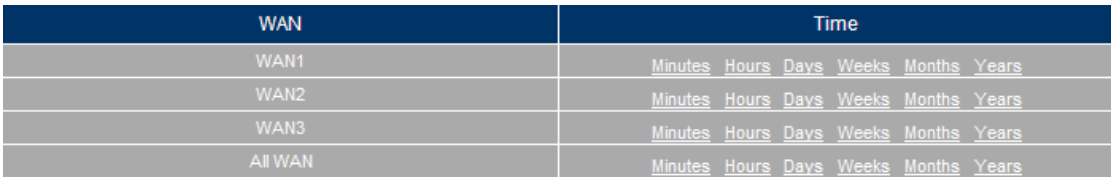


Figure 29-1 Different Time Units for Statistics

Note:

1. The **WAN statistics** is a subordinate function of **WAN interface**. Thus, it is activated when WAN **interface** is enabled.

Step 2. Statistic charts（**Figure 29-2**）

- Vertical axis indicates network stream.
- Horizontal axis indicates time.

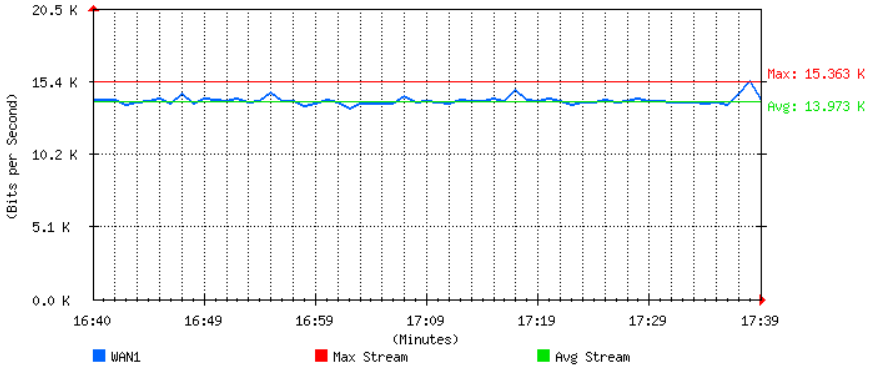
Years | Months | Weeks | Days | Hours | Minutes

Bits/sec | Bytes/sec | Utilization | Accumulated

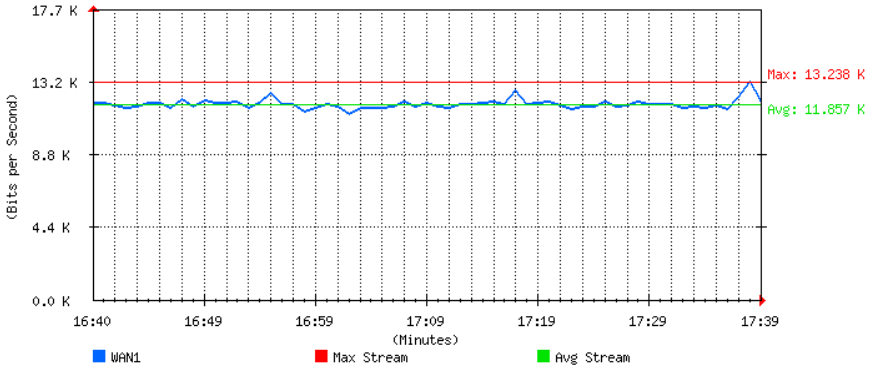
2010 / 12 / 21 17 : -- Refresh

Real-time: Down 6.51 KBits/sec Up 11.13 KBits/sec

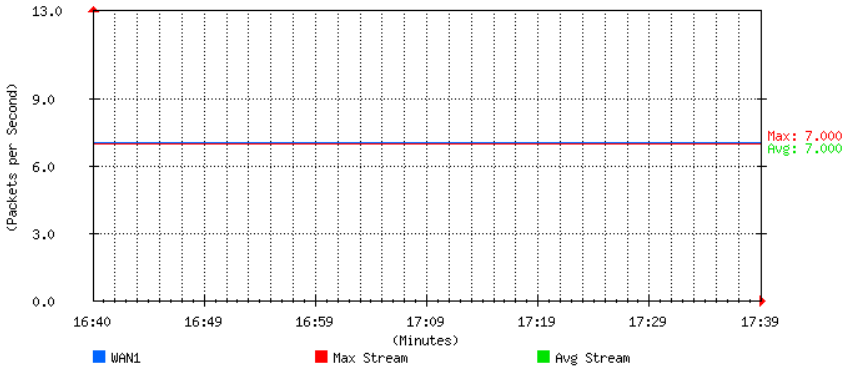
WAN1 Downstream



WAN1 Upstream



WAN1 Received Packets



WAN1 Transmitted Packets

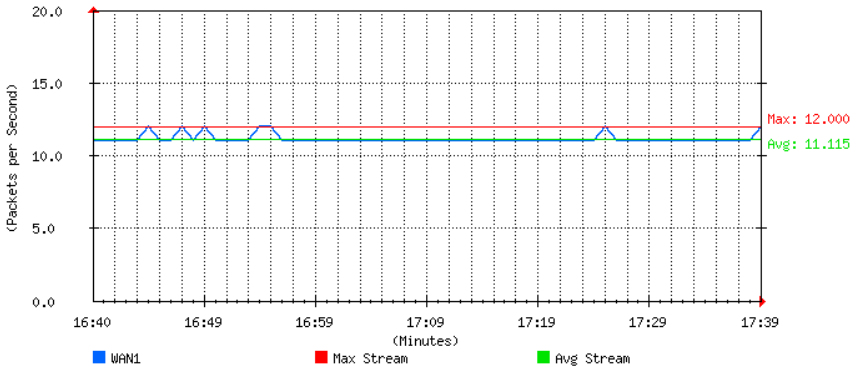


Figure 29-2 The Network Stream Chart

Note:

1. You may configure the time duration to search for the statistics in a certain period of time.

31.2 Policy-Based Traffic

Step 1. When creating a new policy, if the **Statistics** is enabled, the **Policy statistics charts** in the path of **Monitoring > Traffic Grapher > Policy-Based Traffic** corresponding to the policy will start recording**.** Under **Monitoring > Traffic Grapher** > **Policy-Based Traffic,** the statistics charts corresponding to a policy are available in the time unit of minute, hour, day, week, month, and year. Click **Minutes** for statistic charts in the time unit of minute；Click **Hours** for statistic charts in the time unit of hour；Click **Days** for statistic charts in the time unit of day；Click **Weeks** for statistic charts in the time unit of week； Click **Months** for statistic charts in the time unit of month；Click **Years** for statistic charts in the time unit of year.（**Figure 29-3**）

Figure 29-3 The Policy Statistics List

Note:

1. If the policy statistics is required, the IT administrator needs to enable the **Statistics** when creating a new policy.
2. The direction of policy are **Outgoing**, **Incoming**, **WAN to DMZ**, **LAN to DMZ**, **DMZ to WAN**, **DMZ to LAN**, **LAN to LAN**, **DMZ to DMZ.**

Step 2. Statistics charts.（**Figure 29-4**）

- Vertical axis indicates network traffic.
- Horizontal axis indicates time.

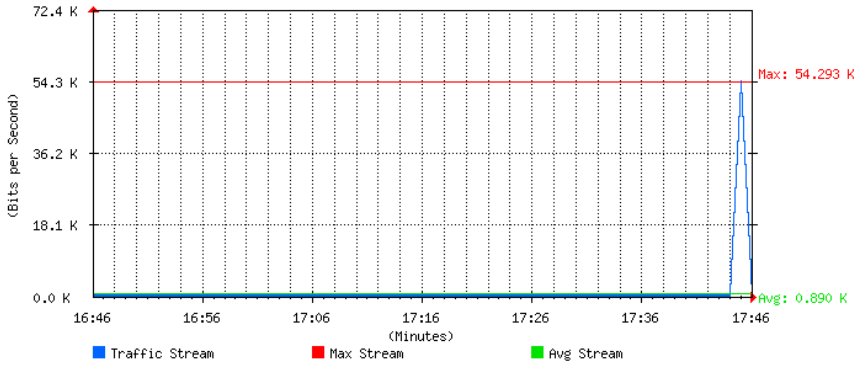
Years | Months | Weeks | Days | Hours | Minutes

Bits/sec | Bytes/sec | Utilization | Total

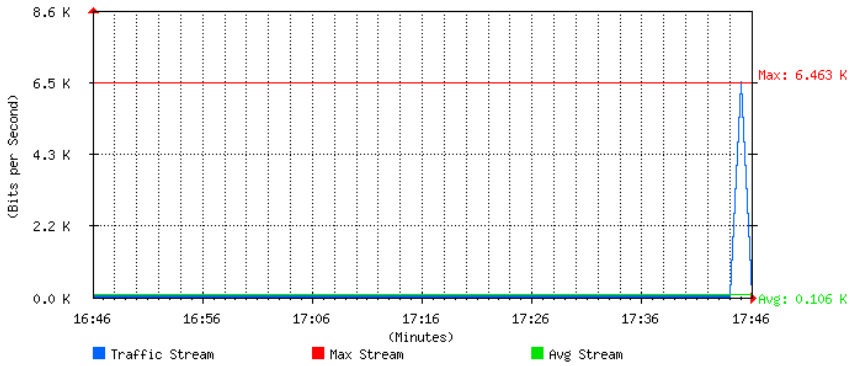
2010 / 12 / 21 17 : -- Search

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

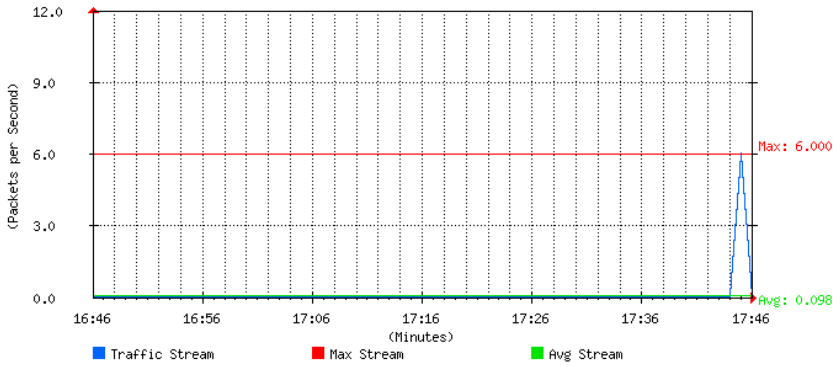
Downstream



Upstream



Received Packets



Transmitted Packets

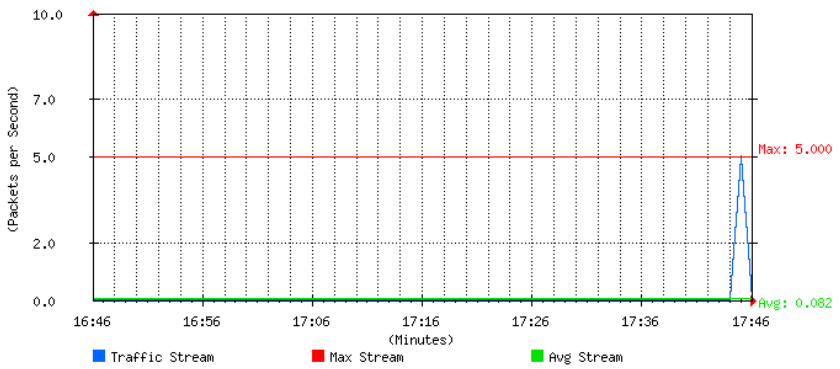


Figure 29-4 Viewing the Policy Statistics Chart

Note:

1. You may see the statistics of a certain time by using the time searching.

Chapter 32 Diagnostic Tools

The device provides ping and traceroute utilities to help diagnose network issues with particular external nodes.

32.1 Ping

Step 1. To test whether a host is reachable across an IP network, go to **Monitoring > Diagnostic Tools > Ping** and then configure as below:（**Figure 30-1**）

- Type the Destination IP or Domain name in the **Destination IP / Domain name** field.
- In **Packet size** configure the size of each packet. (32 Bytes by default)
- In **Count**, configure the quantity of packets to send out. (4 by default)
- In **Wait time**, specify the duration to wait between successive pings. (1 second by default)
- Select the interface from the **Interface** drop-down list.
- Click **OK**.（**Figure 30-2**）

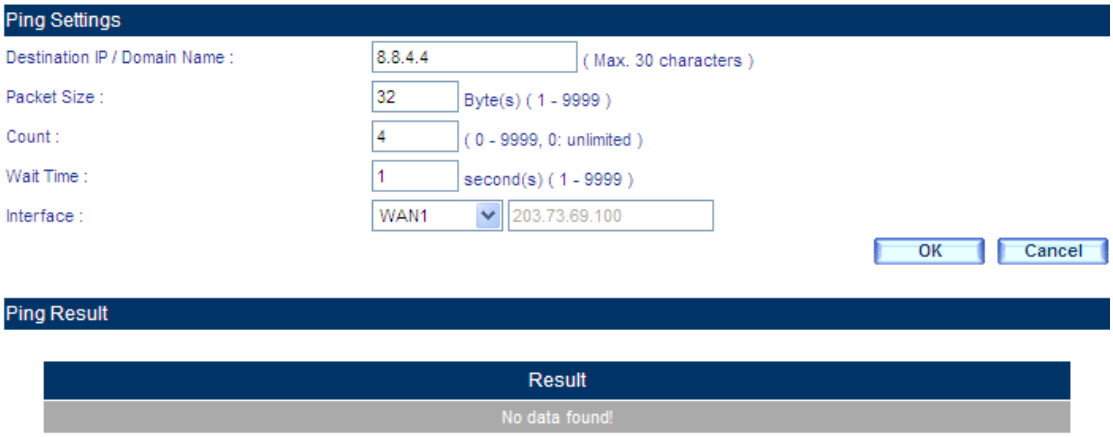


Figure 30-1 Ping Settings

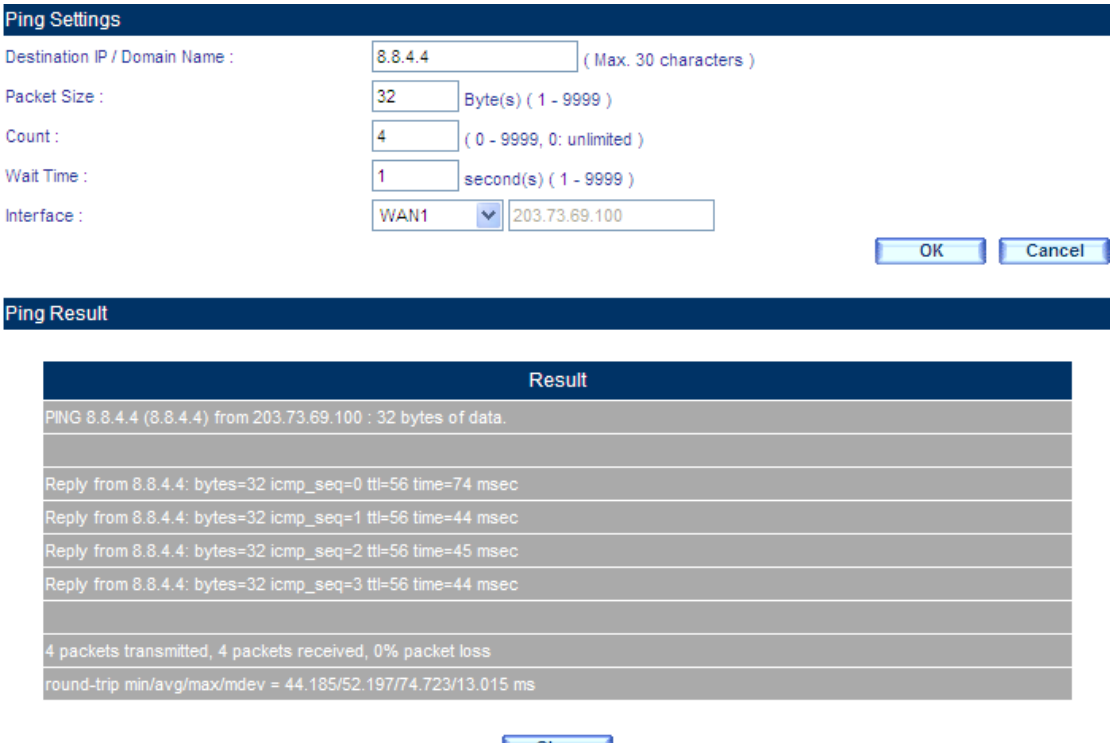


Figure 30-2 Ping Result

Note:

1. If VPN is selected from the **Interface** drop-down list, the user must enter the local LAN IP address in the **Interface** field. Enter the IP address that is under the same subnet range in the **Destination IP / Domain name** field.
   - When the VPN connection is established between the local subnet and remote subnet, the following method can be employed to test the packet transfer between the two subnets. （**Figure 30-3**）

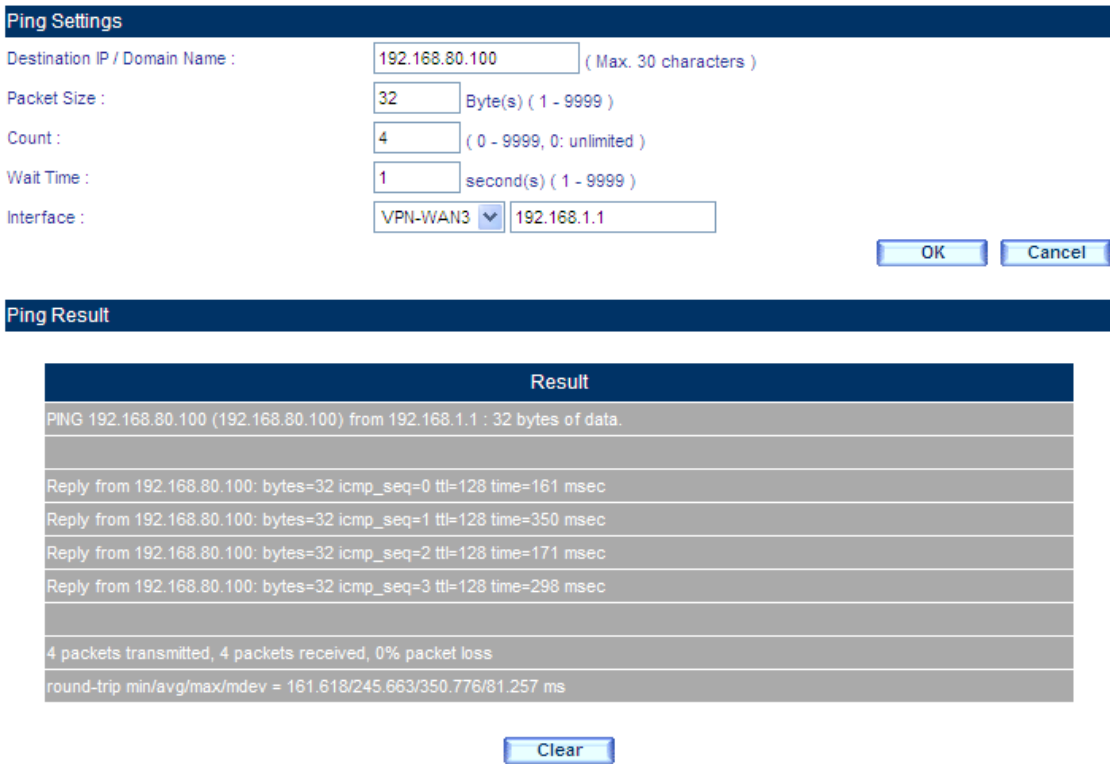


Figure 30-3 Ping Results for a VPN Connection

32.2 Traceroute

Step 1. Under **Monitoring** > **Diagnostic Tools**> **Traceroute** the Traceroute command can be used by the CS-2001 to send out packets to a specific address to diagnose the quality of the traversed network.（**Figure 30-4**）

- In **Destination IP / Domain name** enter the destination address for the packets.
- In **Packet size** configure the size of each packet. (40 Bytes by default)
- In **Max Time-to-Live**, enter the maximum number of hops. (30 by default)
- In **Wait time**, specify the duration to wait between successive pings. (2 seconds by default)
- In **Interface** select the interface that the packets will originate from.
- Click **OK**.（**Figure 30-5**）

Figure 30-4 Traceroute Settings

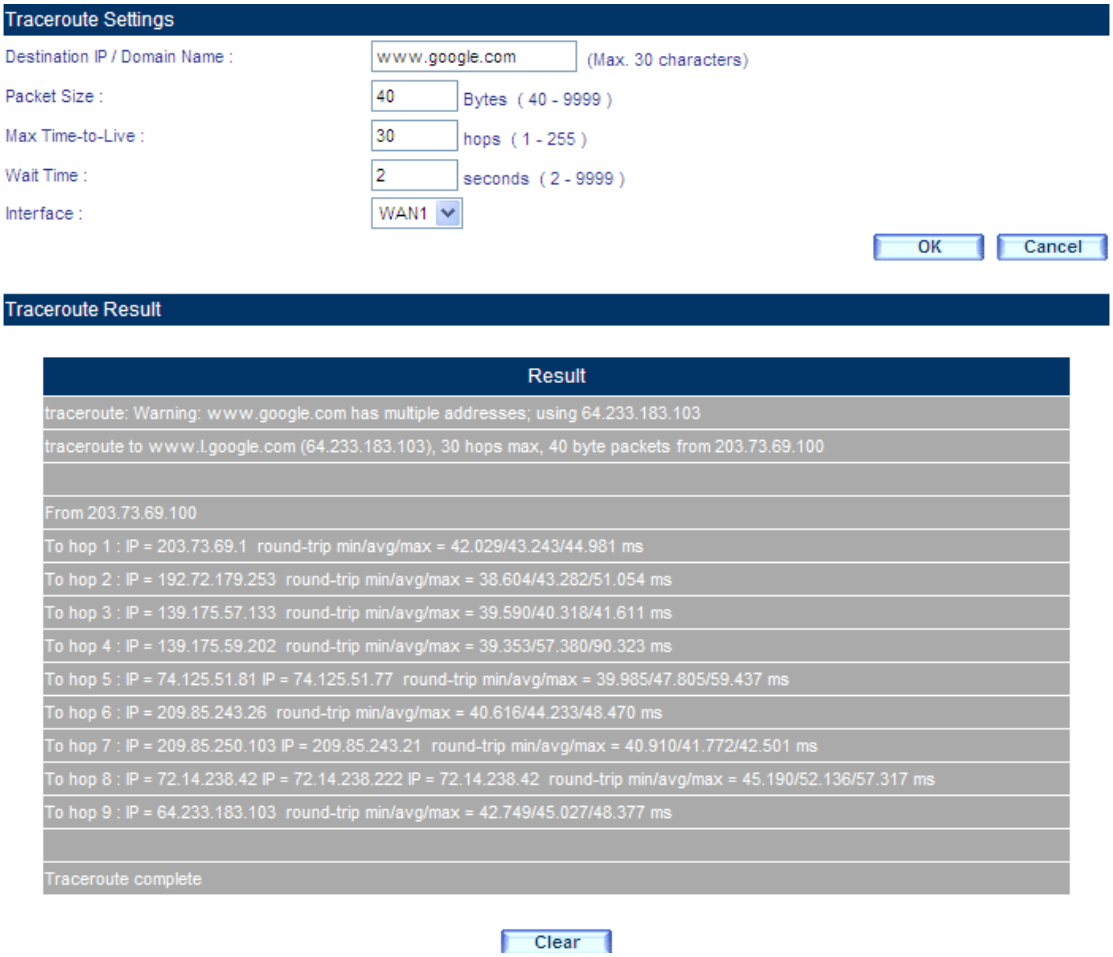


Figure 30-5 Traceroute Results

32.3 Packet Capture

Capture packetfor debugging

Step 1. Under **Monitoring** > **Diagnostic Tools**> **Packet Capture** the packet capture can help to debug and capture the packet content for debugging. **(figure 30-6)**

- In **interface** drop list selects which one of interface is going to capture the packet.
- In **capture time** list, choose hong long will be the captured time.
- Filll in the **Host IP** and **Netmask** you would like to filter.
- Configure the filtering rule
- Click **Start** then wait for the captured period, the result will display on the filed.
-

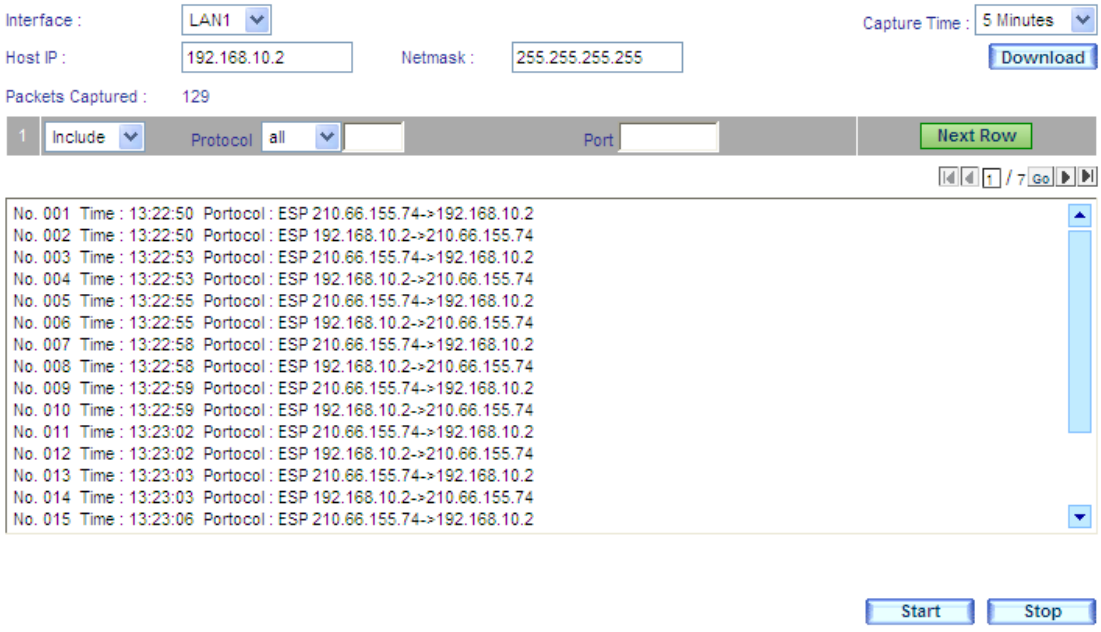


Figure 30-6 Packet Caputre Results

Chapter 33 Wake-On-LAN

Any wake-on-LAN supported PC can be remotely turned on by a “wake-up” packet sent from the CS-2001. By utilizing remote control software such as VNC, Terminal Service or PC Anywhere, a remote user may remotely wake up a computer and access it.

33.1 Example

33.1.1 Remote Controlling a PC

Step 1. Supposing the MAC address of the PC that is desired to be remotely controlled is 00:0C:76:B7:96:3B.

Step 2. Under **Monitoring** > **Wake-On-LAN** > **Settings**, click **New Entry** and then set as below:

- Enter the name in the field.
- Enter 00:0C:76:B7:96:3B in the **MAC Address** field.
- Click **OK**.（**Figure 31-1**）

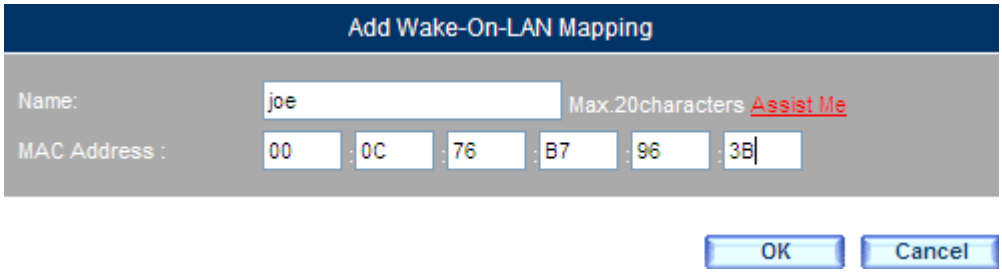


Figure 31-1 Wake on LAN Setting

Step 3. Click **WakeUp** to start up the PC.（**Figure 31-2**）

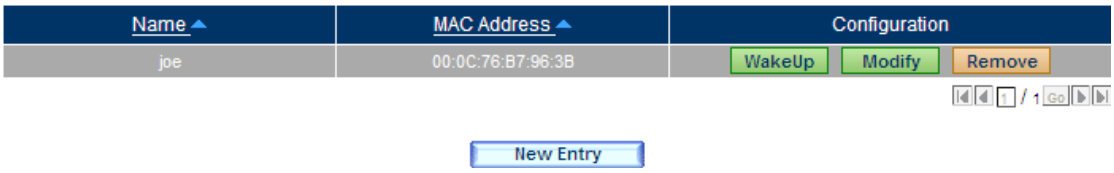


Figure 31-2 Clicking "WakeUp" to Start up the PC

Chapter 34 Status

Status provides current information about the device and the network including Interface, System Info, Authentication, ARP Table, Sessions Info, DHCP Clients, etc. as well as current network connection states and various other information.

- **Interface**: shows the status of each interface.
- **System Info**: shows the utilization of CPU, hard disk and memory.
- **Authentication**: records the use of any authentication usage for the CS-2001.
- **ARP Table**: records all the ARP tables of host PCs that have connected to CS-2001.
- **Sessions Info**: It records all the sessions sending or receiving packets over CS-2001.
- **DHCP Clients**: It records the status of IP addresses distributed by CS-2001 built-in DHCP server.

34.1 Interface

Step 1. Under **Monitoring** > **Status** > **Interface**, it shows the status of all interface. （**Figure 32-2**）

No. of Active Sessions : 166 System Uptime : 0 day(s) 7 hour(s) 28 min(s) 57 sec(s)

Physical Port No	1	2	3	4
Interface Designation	LAN1	WAN1	WAN2	WAN3
Connection Type	NAT	PPPoE	Dynamic IP	Static IP
Connection Status				
Link Speed	100Mb/s	100Mb/s	100Mb/s	10Mb/s
Duplex Mode	Full	Full	Full	Half
Up-/Downstream BW (kbps)		5120 / 5120	51200 / 51200	51200 / 51200
Downstream BW %		40%	10%	50%
Upstream BW %		5%	46%	49%
Connection Uptime		0:01:58	0:05:17	
MAC Address	00:90:0B:14:5D:B8	00:90:0B:14:5D:B9	00:90:0B:14:5D:BA	00:90:0B:14:5D:BB
IPv4 Address	192.168.1.1	203.73.69.100	192.168.99.5	210.66.155.73
Netmask	255.255.255.0	255.255.255.255	255.255.255.0	255.255.255.224
IPv4 Default Gateway		203.73.69.1	192.168.99.1	210.66.155.94
IPv6 Address				
Prefix Length				
IPv6 Default Gateway				
DNS Server 1		168.95.1.1	168.95.1.1	168.95.1.1
DNS Server 2		168.95.192.1	168.95.192.1	168.95.192.1
Rx Packets / Errors	20375,0	249,0	228,0	137993,0
Tx Packets / Errors	33037,0	264,0	237,0	48501,0
Ping	✔	✔	✔	✔
HTTP	✔	✔	✔	✔
HTTPS	✔	✔	✔	✔

Figure 32-2 Status Interface

Note:

1. **System Uptime**: the operating uptime of the CS-2001.
2. **Active Sessions Number**: shows the current number of sessions connected to the device.
3. **Forwarding Mode**: displays the interface connection mode.
4. **WAN Connection**: shows the WAN interface connection status.
5. **DnS / UpS kbps**: shows the maximum downstream / upstream bandwidth set for the WAN interface (can be configured under **Network** > **Interface** > **WAN**).
6. **Downstream Traffic**: the percentage of downstream traffic to each WAN interface.
7. **Upstream Traffic**: the percentage of upstream traffic to each WAN interface.

8. **PPPoE / Dynamic IP Uptime**: when the interface is connected using PPPoE, it displays the connection uptime.
9. **MAC Address**: displays the MAC address of the interface.
10. **IP Address / Netmask**: the interface's IP address and netmask.
11. **Default Gateway**: shows the WAN gateway address.
12. **DNS 1**: the DNS 1 server address from the ISP.
13. **DNS 2**: the DNS 2 server address from the ISP.
14. **Rx Packets / Errors**: shows the quantity of received packets and the amount of error packets for each interface。
15. **Tx Packets / Errors**: shows the quantity of sent packets and the amount of error packets for each interface.
16. **Ping / HTTP / HTTPS**: shows whether the user can ping the device's interface, or access the Web UI through HTTP and HTTPS.

34.2 System Info

Step 1. Under **Monitoring** > **Status** > **System Info**, it shows the current system information, such as CPU utilization, hard disk utilization and memory utilization.（**Figure 32-3**）

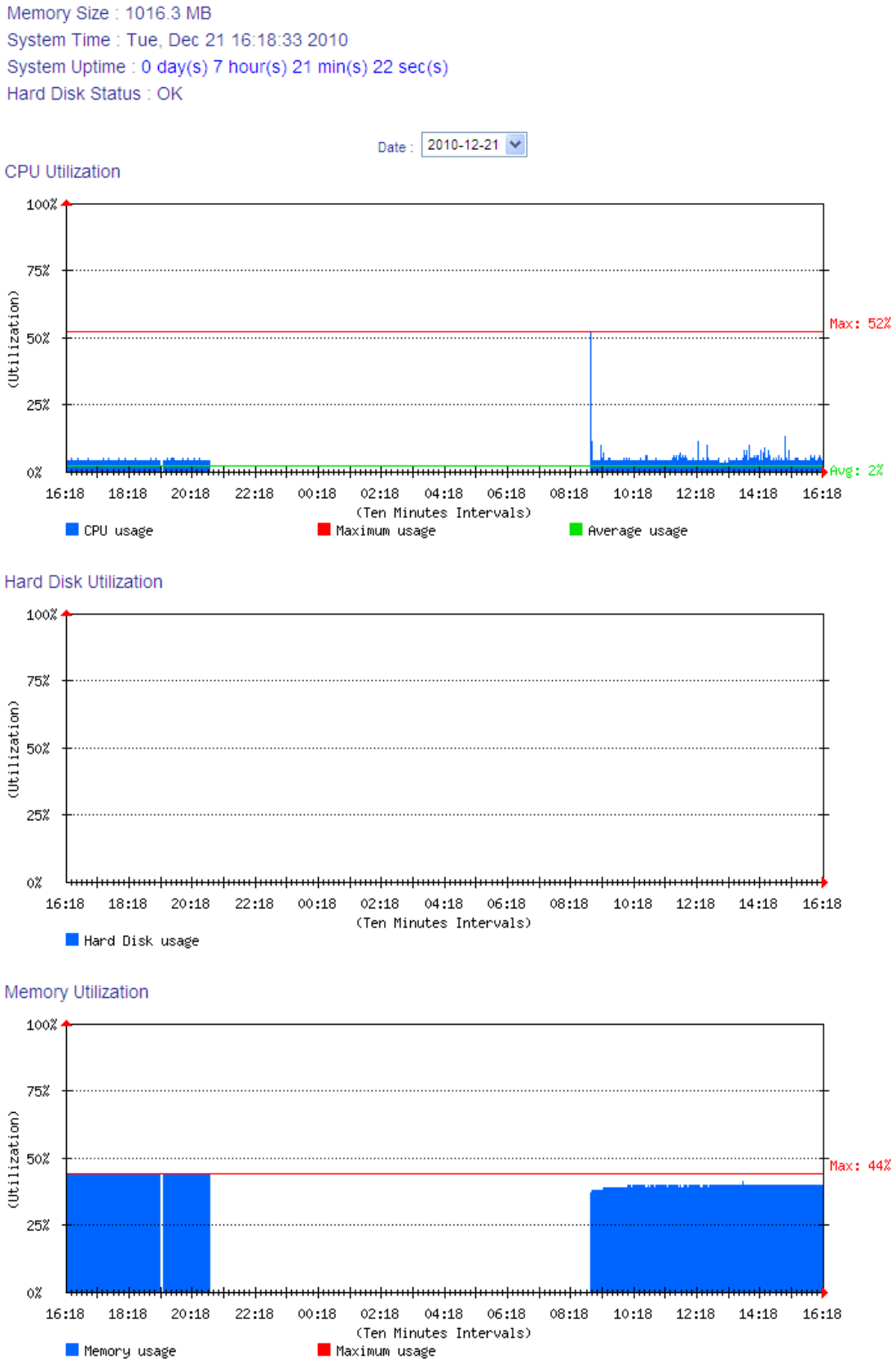
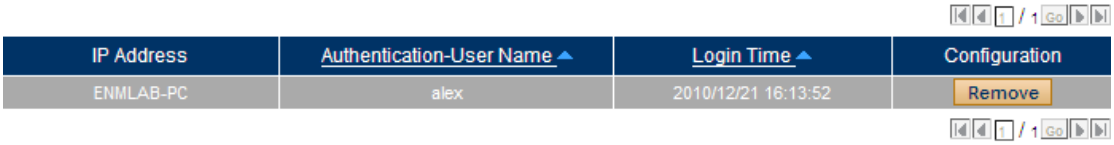


Figure 32-3 System Information

34.3 Authentication

Step 1. Under **Monitoring** > **Status** > **Authentication**, it shows the authentication status of the device.（**Figure 32-4**）



IP Address	Authentication-User Name	Login Time	Configuration
ENMLAB-PC	alex	2010/12/21 16:13:52	Remove

Figure 32-4 The Authentication Status

Note:

1. **IP Address**: displays the authenticated user's IP address.
2. **Authentication – User Name**: the user's authenticated login name.
3. **Login Time**: the user's login time (year/ month/ day/ hour/ minute/ second)

34.4 ARP Table

Step 1. Under **Monitoring** > **Status** > **ARP Table**, it shows **NetBIOS Name**, **IP Address**, **MAC Address** and **Interface** of any computer that has connected to the device.（**Figure 32-5**）

Figure 32-5 ARP Table

Note:

1. **NetBIOS Name**: the computer's network identification name.
2. **IP Address**: the computer's IP address.
3. MAC Address: the computer's network adapter identification number.
4. **Interface**: the interface that the computer is connected to.
5. To prevent any network packet errors, the **Static ARP Table** must coordinate with the **Anti-ARP virus software**. When these two function together, they provide a fixed mapping between the IP address and the MAC address.
6. The **Anti-ARP virus software** can be downloaded by clicking on the **Download** button. Once downloaded proceed with the following:（**Figure 32-6**）
   - The program can be executed immediately to start taking effect against ARP viruses.（**Figure 32-7**）
   - Copy the execution file to the computer's hard disk: \Documents and Settings\All Users\Start\Programs\Startup, after that, it will be executed every time when the system starts up.（**Figure 32-8**）

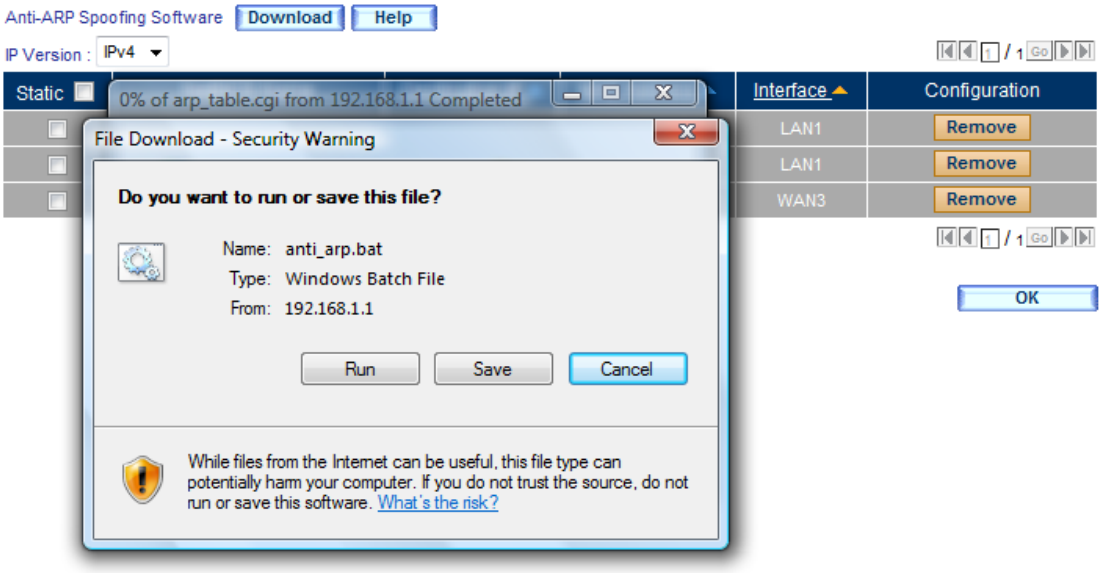


Figure 32-6 Downloading the Anti-ARP Virus Software

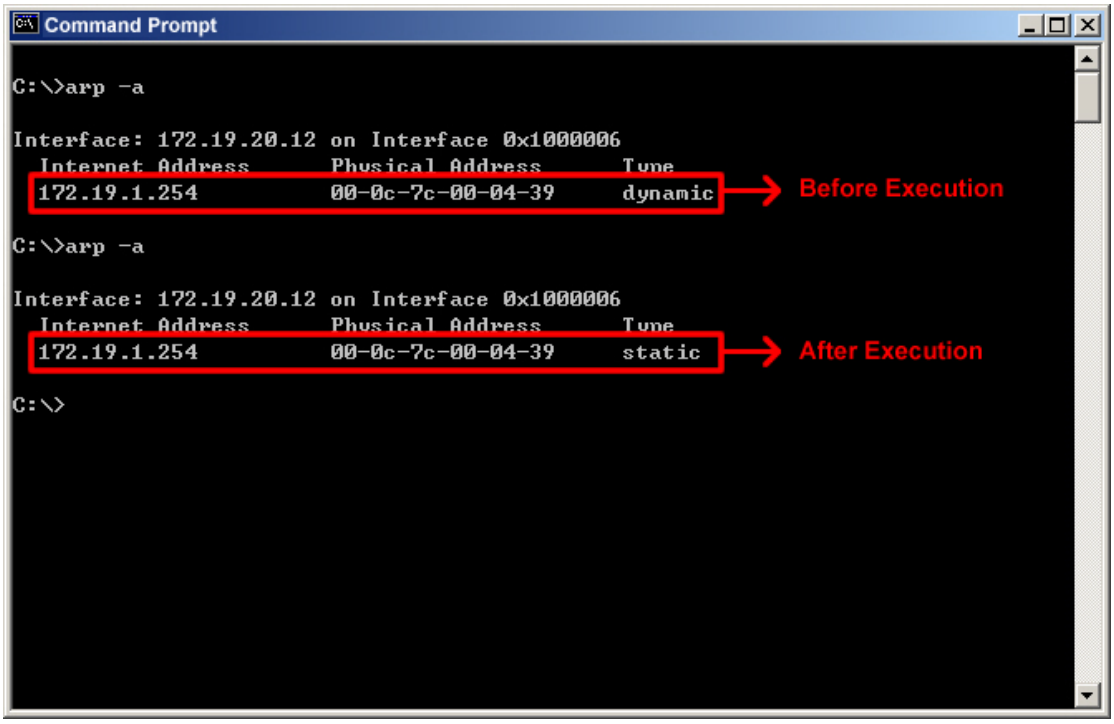


Figure 32-7 The Result of Executng the Anti-ARP Virus Software

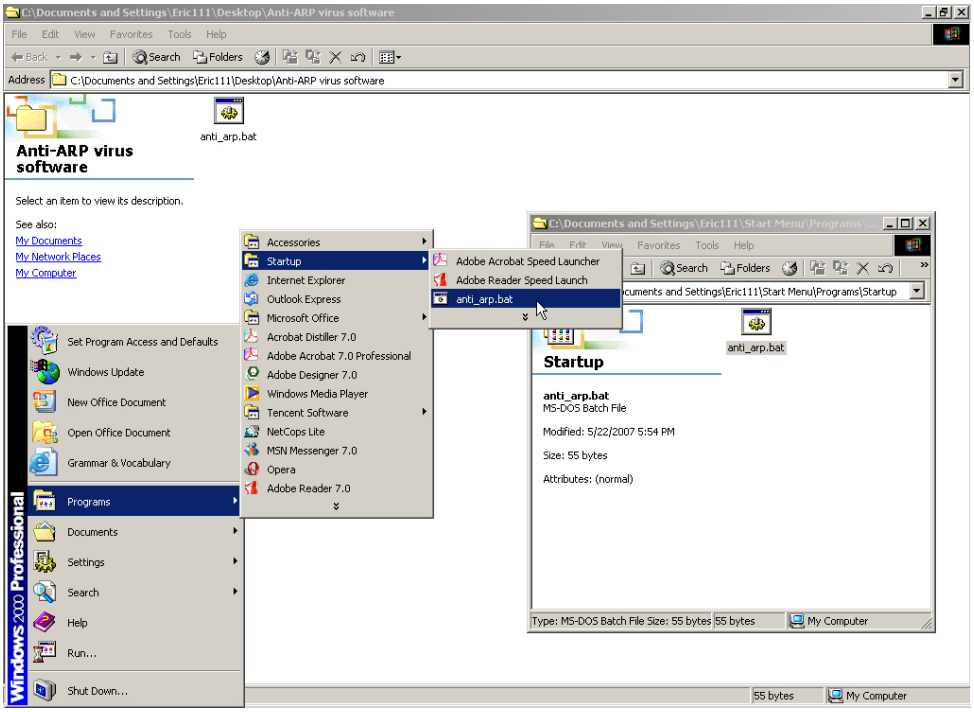


Figure 32-8 The Anti-ARP Virus Software will Automatically Run when the System Startups

34.5 Sessions Info

Step 1. Under **Monitoring** > **Status** > **Sessions Info**, it provides a list of all the sessions that have connected to the device.（**Figure 32-9**）

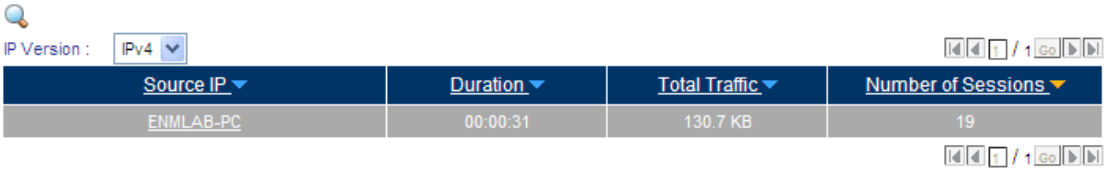
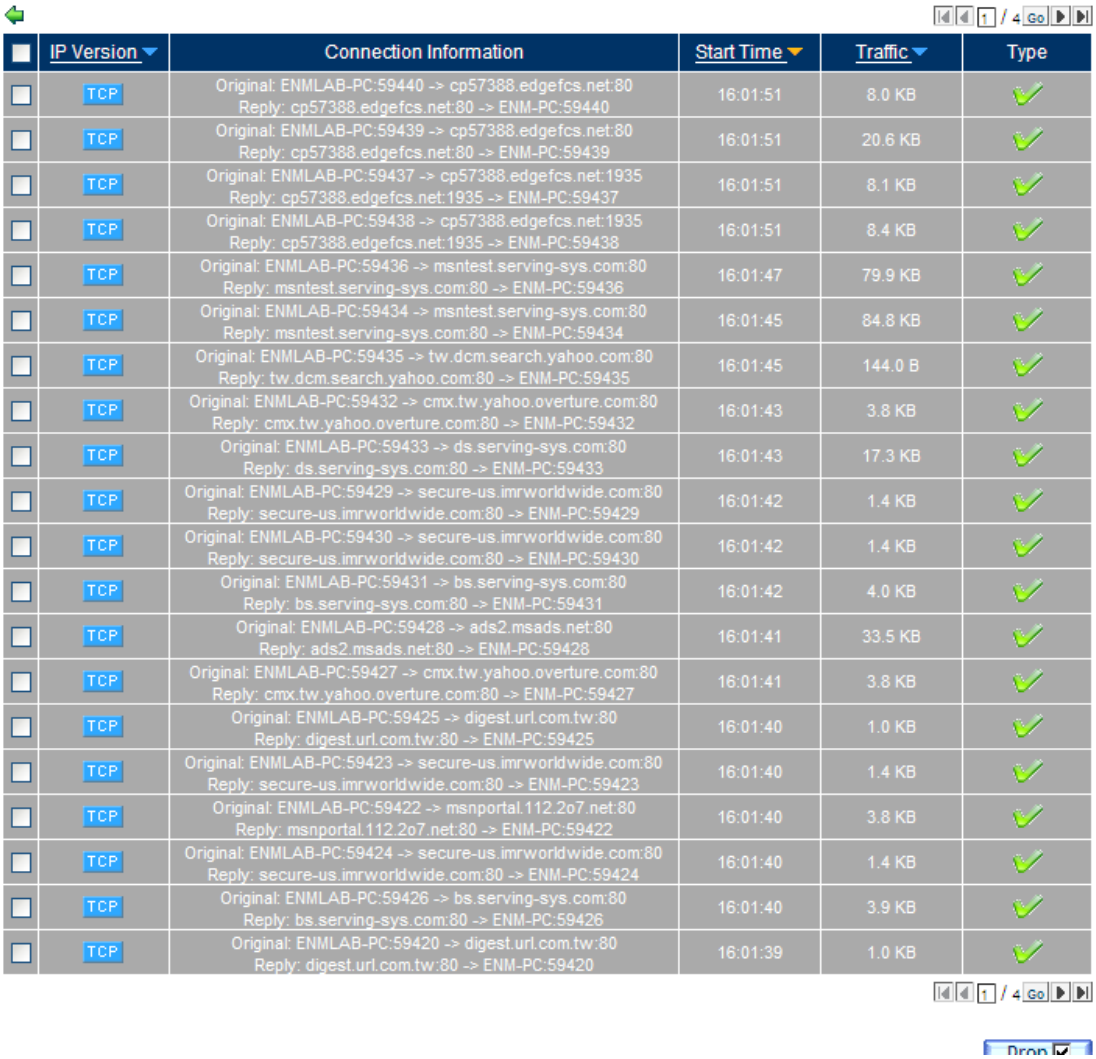


Figure 32-9 System Sessions

Step 2. By clicking on any source IP, it shows the port number and the traffic.

（Figure 32-10）



	IP Version	Connection Information	Start Time	Traffic	Type
	TCP	Original: ENMLAB-PC:59440 -> cp57388.edgefcs.net:80 Reply: cp57388.edgefcs.net:80 -> ENM-PC:59440	16:01:51	8.0 KB	
	TCP	Original: ENMLAB-PC:59439 -> cp57388.edgefcs.net:80 Reply: cp57388.edgefcs.net:80 -> ENM-PC:59439	16:01:51	20.6 KB	
	TCP	Original: ENMLAB-PC:59437 -> cp57388.edgefcs.net:1935 Reply: cp57388.edgefcs.net:1935 -> ENM-PC:59437	16:01:51	8.1 KB	
	TCP	Original: ENMLAB-PC:59438 -> cp57388.edgefcs.net:1935 Reply: cp57388.edgefcs.net:1935 -> ENM-PC:59438	16:01:51	8.4 KB	
	TCP	Original: ENMLAB-PC:59436 -> msntest.serving-sys.com:80 Reply: msntest.serving-sys.com:80 -> ENM-PC:59436	16:01:47	79.9 KB	
	TCP	Original: ENMLAB-PC:59434 -> msntest.serving-sys.com:80 Reply: msntest.serving-sys.com:80 -> ENM-PC:59434	16:01:45	84.8 KB	
	TCP	Original: ENMLAB-PC:59435 -> tw.dcm.search.yahoo.com:80 Reply: tw.dcm.search.yahoo.com:80 -> ENM-PC:59435	16:01:45	144.0 B	
	TCP	Original: ENMLAB-PC:59432 -> cmx.tw.yahoo.overture.com:80 Reply: cmx.tw.yahoo.overture.com:80 -> ENM-PC:59432	16:01:43	3.8 KB	
	TCP	Original: ENMLAB-PC:59433 -> ds.serving-sys.com:80 Reply: ds.serving-sys.com:80 -> ENM-PC:59433	16:01:43	17.3 KB	
	TCP	Original: ENMLAB-PC:59429 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59429	16:01:42	1.4 KB	
	TCP	Original: ENMLAB-PC:59430 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59430	16:01:42	1.4 KB	
	TCP	Original: ENMLAB-PC:59431 -> bs.serving-sys.com:80 Reply: bs.serving-sys.com:80 -> ENM-PC:59431	16:01:42	4.0 KB	
	TCP	Original: ENMLAB-PC:59428 -> ads2.msads.net:80 Reply: ads2.msads.net:80 -> ENM-PC:59428	16:01:41	33.5 KB	
	TCP	Original: ENMLAB-PC:59427 -> cmx.tw.yahoo.overture.com:80 Reply: cmx.tw.yahoo.overture.com:80 -> ENM-PC:59427	16:01:41	3.8 KB	
	TCP	Original: ENMLAB-PC:59425 -> digest.url.com.tw:80 Reply: digest.url.com.tw:80 -> ENM-PC:59425	16:01:40	1.0 KB	
	TCP	Original: ENMLAB-PC:59423 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59423	16:01:40	1.4 KB	
	TCP	Original: ENMLAB-PC:59422 -> msnportal.112.2o7.net:80 Reply: msnportal.112.2o7.net:80 -> ENM-PC:59422	16:01:40	3.8 KB	
	TCP	Original: ENMLAB-PC:59424 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59424	16:01:40	1.4 KB	
	TCP	Original: ENMLAB-PC:59426 -> bs.serving-sys.com:80 Reply: bs.serving-sys.com:80 -> ENM-PC:59426	16:01:40	3.9 KB	
	TCP	Original: ENMLAB-PC:59420 -> digest.url.com.tw:80 Reply: digest.url.com.tw:80 -> ENM-PC:59420	16:01:39	1.0 KB	

Figure 32-10 The System Info

34.6 DHCP Clients

Step 1. Under **Monitoring** > **Status** > **DHCP Clients**, it shows the status of IP address distributed by the device's DHCP server. （**Figure 32-11**）

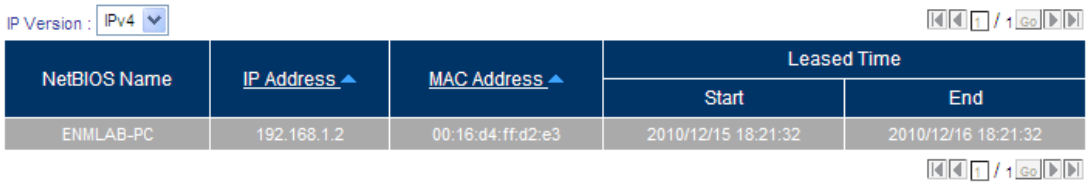


Figure 32-11 The DHCP Clients

Note:

1. **NetBIOS Name**: the computer's network identification name.
2. **IP Address**: the computer's IP address.
3. **MAC Address**: the MAC address that the dynamic IP maps to.
4. **Leased Time**: the start time and the end time of the dynamic IP. (year, month, day, hour, minute, second)

34.7 Host Info

Step1. Under **Monitoring** > **Status** > **Host Info**, the IT administrator may view the list of NetBIOS and DNS.（**Figure 34-12, 34-13**）

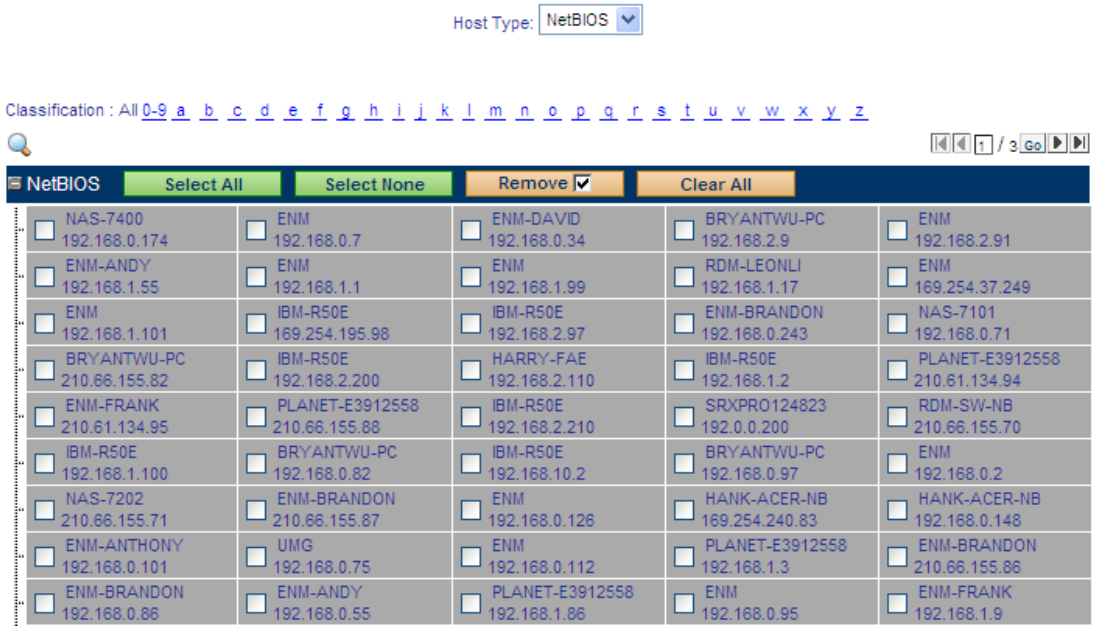


Figure 34-12 The List of NetBIOS

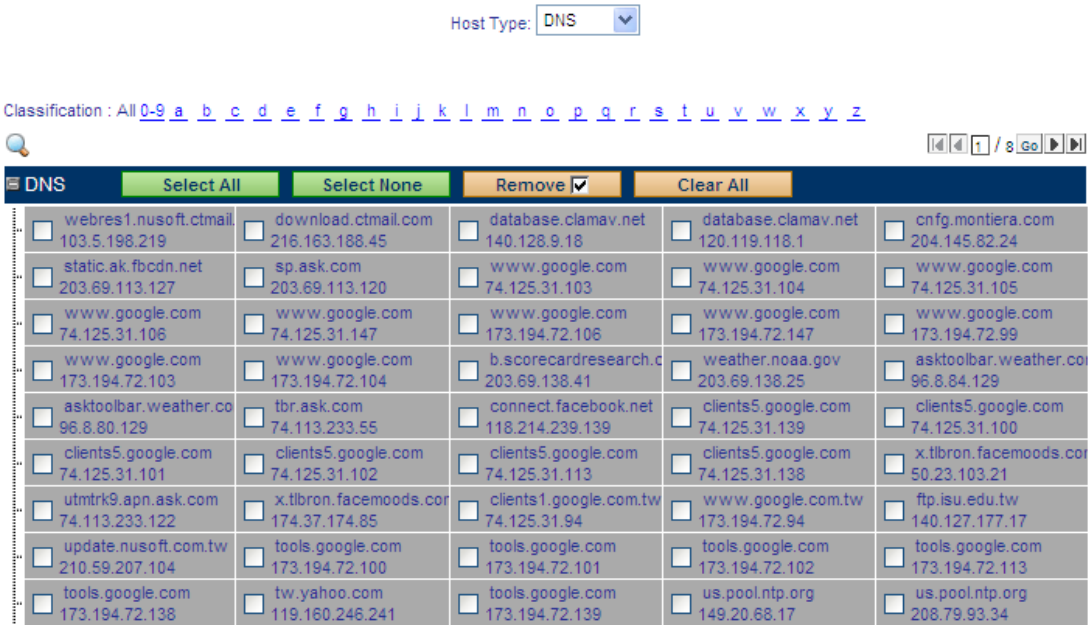


Figure 34-13 The List of DNS