Multi-Homing
UTM Security Gateway

MH-5001

User's Manual

Copyright

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

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

WEEE Warning

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

Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Customer Service

For information on customer service and support for the Multi-Homing Security Gateway, please refer to the following Website URL:

http://www.planet.com.tw and email: Suppor_router@planet.com.tw

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

- Multi-Homing Security Gateway serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User's Manual for PLANET Multi-Homing Security Gateway
Model: MH-5001
Rev: 4.0 (July, 2006)
Part No. EM-MH5Kv4 (2081-B90070-000)

Table of Contents

About this user manual

This user manual provides information about installing and configuring your MH-5001 Multi-Homing Security Gateway using its built-in web browser interface (WBI) and command line interface (CLI). This guide is primarily for network and security personnel who configure the Multi-Homing Security Gateway and monitor networks for evidence of intrusion attempts and inappropriate transmission of regulated information. The WBI is a versatile, configurable monitoring platform. For you to understand and use its functionality, you must understand the WBI and its capabilities.

All the examples after Chapter 2 in this manual, which instruct you how to configure the Multi-Homing Security Gateway, are taken from MH-5001. The hardware and software specification of the MH-5001 will be introduced in Chapter 1. You can refer the examples to configure your MH-5001. That will help you to quick your configuration and save you time.

What's New in Version 4?

This section describes the enhancements that were made to MH-5001 as compared to the previous version. It includes changes to the way that the MH-5001 operates, some of which are reflected by changes to the WBI and others that were made to the MH-5001 engine to improve performance and accuracy. As compared to the previous version, version 2.000 provides the following additional improvements:

Anti-DoS

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In order to avoid the loss of the particular network services such as e-mail or even security loss, MH-5001 provide Anti-DoS function to help users to block the well-known Denial-of-Service attacks such as WinNuke and LAN attacks.

- TCP SYN Flooding
- UDP Flooding
- ICMP Flooding

Please refer to Section 10.4.2 for details.

Authentication

The MH-5001 supports user authentication to the user database or to a RADIUS server. Users can be allowed to access internal database after passing the authentication. In this version, we provide the following authentication types, such as Local, POP3(s), IMAP(s), RADIUS, LDAP, etc. See Chapter 6 Authentication for details.

Books (Address/Service/Schedule)

Address: All rules require source and destination addresses. You have to add the addresses to each interface while inserting a new firewall rule. These addresses must be valid addresses for the network connected to that interface. You can also organize related addresses into address groups to make it easier to add rules. See Section 9.4.1 for details.

Service: Use service to control the types of communication accepted or denied by the firewall. In this version, we provide you with the predefined services. You can also create your own custom services and add services to service group. See Section 9.4.2 for details.

Schedule: Use scheduling to control when the rules are activated or deactivate. You can also organize the related schedules into schedule groups. See Section 9.4.3 for details.

High Availability

Suppose your company is afraid that the firewall may be crashed someday, High Availability will meet the requirement to backup the original system and let the network connection continually. It makes it possible to let the network in your company operate smoothly. See Chapter 26 High Availability for details.

IP/MAC Binding

IP/MAC binding protects MH-5001 and your network from IP spoofing attacks. IP spoofing attempts to use the IP address of a trusted computer to or through the MH-5001 from a different computer. There are two IP/MAC Binding type for your choice. You can choose binding to bind the IP address with MAC address to allow the legal traffic passing through MH-5001. You can also select range to allow a range of the IP addresses such as DHCP IP range passing through MH-5001. See Chapter 11 IP/MAC Binding for Details.

IPSec VPN improvements

Hub and Spoke VPN: Suppose that your company has a main office and two branch offices or more which communicates using a hub and spoke VPN configuration. The main office is the hub where the VPN tunnels terminate, while Branch_1 and Branch_2 are the spokes. The Main office has a VPN tunnel to each branch office. Both Branch_1 and Branch_2 have their own VPN tunnel to the hub. The VPN Spoke allows VPN traffic to pass from one tunnel to the other through a central MH-5001 hub. See Chapter 15 Virtual Private Network – Hub and Spoke VPN for details.

MPPE Support: In MH-5001 release II version, both PPTP and L2TP can support MPPE. In other words, you can choose “Require data encryption” while a client computer running Windows XP/2000. However, this release II version will not support MS-CHAP, you have to check MS-CHAPv2 checkbox if you would like to require data encryption.

Transparent Mode

Transparent mode provides the same basic firewall protection as NAT mode. Packets received by the MH-5001 are intelligently forwarded or blocked according to the firewall rules. The MH-5001 can be inserted into your network without changing your network or any of its components. See Section 1.7.2 for details.

WAN Backup

When WAN Backup is enabled, the system will start to ping the public Internet Server IP addresses with a sequence of every specified Timeout to check the connection of the current default WAN link. When the current default WAN link is disconnected, MH-5001 will try to make the ping action to the first Public Internet Server IP address within the specified Timeout. When all of them are timeout, the default route/link will be switched to another WAN link to continue the ping action within the specified Detection Interval until the system is successful to ping the specified public IP address. See Section 3.4.4 for details.

Layer 7 Application Layer Firewall

When L7 Firewall enabled, the MH-5001 can instant block the application layer services such as MSN, Yahoo, SIP, H.323, etc services. The information can be found at Chapter 22.

Chapter 1
Quick Start

This chapter introduces how to quick setup the MH-5001.

MH-5001 is an integrated all-in-one solution that can facilitate the maximum security and the best resource utilization for the enterprises. It contains a high-performance stateful packet inspection (SPI) **Firewall**, policy-based **NAT**, ASIC-based wire-speed **VPN**, upgradeable **Intrusion Detection System**, **Dynamic Routing**, **Content Filtering**, **Bandwidth Management**, **WAN Load Balancer**, and other solutions in a single box. It is one of the most cost-effective all-in-one solutions for enterprises.

1.1 Check Your Package Contents

These are the items included with your MH-5001 purchase. They are the following items

1. MH-5001 x 1
2. Quick Installation Guide x 1
3. CD-ROM Manual / Installation Guide x 1
4. Power Cord x 1
5. Rack mount x 1
6. RS-232 cable x 1

1.2 Five steps to configure MH-5001 quickly

Let’s look at the common network topology without MH-5001 applying like Figure 1-. This is a topology which is almost used by all the small/medium business or SOHO use as their Internet connectivity. Although that your topology is not necessarily the same diagram below, but it still can give you a guideline to configure MH-5001 quickly.

Now you can pay attention at the IP Sharer in the diagram. The IP Sharer can provide you with NAT (Network Address Translation), PAT (Port Address Translation) and other functions.

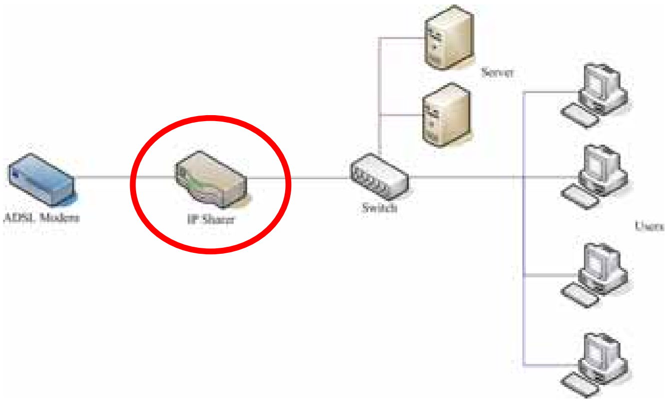


Figure 1-1 The example before MH-5001 applies on it

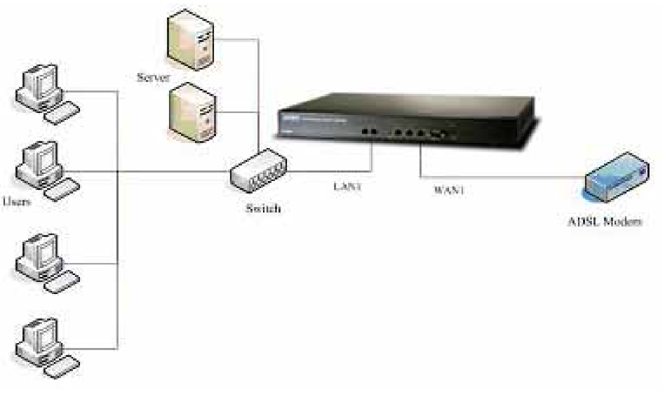


Figure 1-2 The example after MH-5001 applies on it

Here we would like to alter the original IP Sharer with the MH-5001 like Figure 1-. If we hope to have MH-5001 to replace the IP Sharer, we just need to simply execute the following five steps as Figure 1- showed. By these steps, we hope to build an image to tell you how to let MH-5001 work basically.

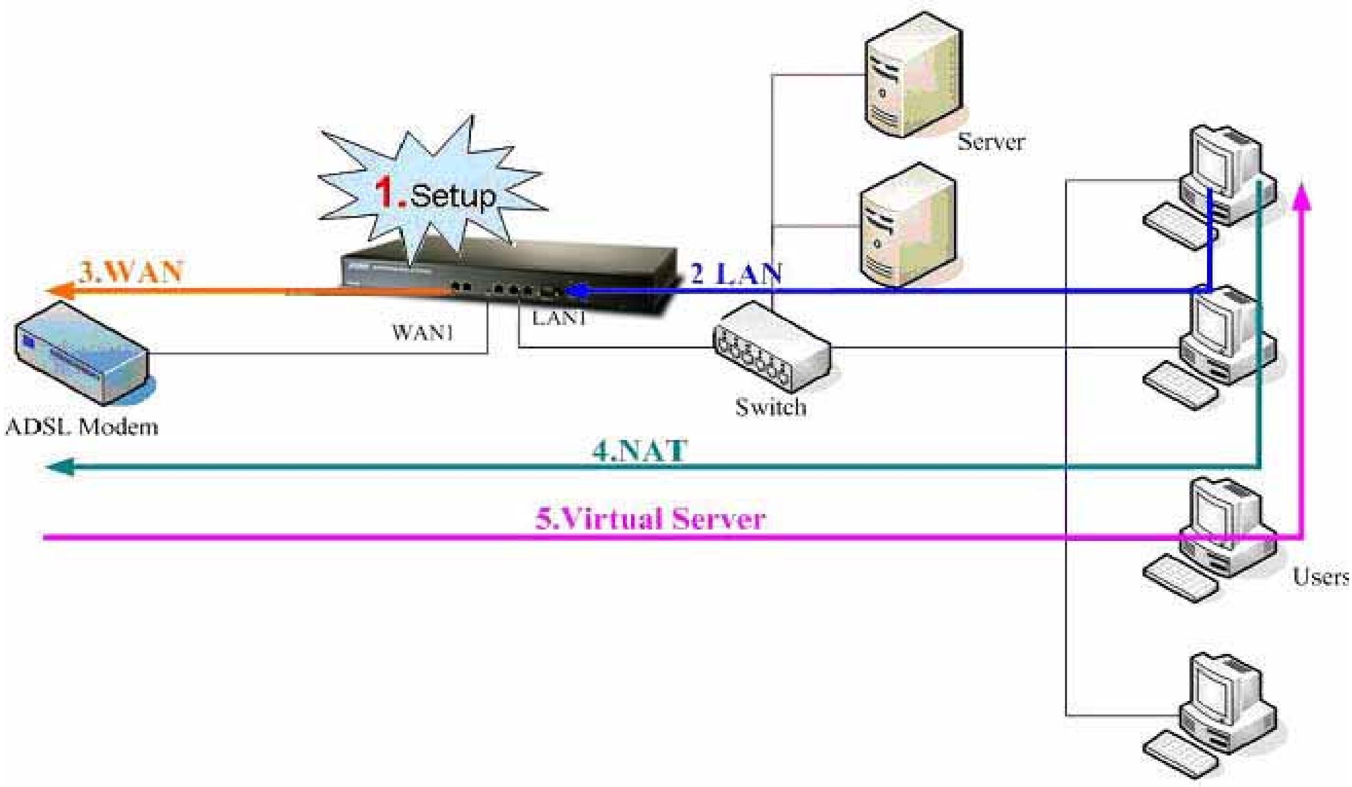


Figure 1-3 Five steps to configure MH-5001

As the Figure 1- illustrated, with the five-step configurations, MH-5001 will have the same functions with the original IP Sharer. Please see the following description of the five-step configurations.

1. Setup:
   Install three physical lines inclusive of the power cord, outbound link (connected WAN1 port) and inbound direction (connected LAN1 port). For the details, please refer section 1.3.
   Continually, we will connect to the web GUI of MH-5001. So you must make sure that you have a PC which is located in the same subnet with MH-5001 before this step. Note: The default LAN1 port is (192.168.1.254 / 255.255.255.0). Refer to section 1.5 for more information.
2. LAN:
   Configure the LAN1 port of MH-5001. You can refer to section 1.4 for the default network configurations of MH-5001. Note: If you were connected from LAN1 port and changed the LAN1 IP address settings of MH-5001. The network will be disconnected since the IP address is different between your pc and MH-5001 LAN1 port.

3. WAN:
   Configure the WAN1 port of MH-5001. You can refer to section 1.4 for the default network configurations of MH-5001.

4. NAT:
   Configure the connection of LAN to WAN direction. It will make all the client pc access the Internet through MH-5001. For more information, please refer to section 1.6.1.
5. Virtual Server:
   If there is any server located inside the MH-5001. You may hope these servers can provide services outside. So you should configure the Virtual Server which provides connections of WAN to LAN direction. For more information, please refer to section 1.6.2.

After you completely finished the above steps, the connectivity function of MH-5001 is probably well-done.

1.3 Wiring the MH-5001

A. First, connect the power cord to the socket at the back panel of the MH-5001 as in Figure 1- and then plug the other end of the power adapter to a wall outlet or power strip. The Power LED will turn **ON** to indicate proper operation.

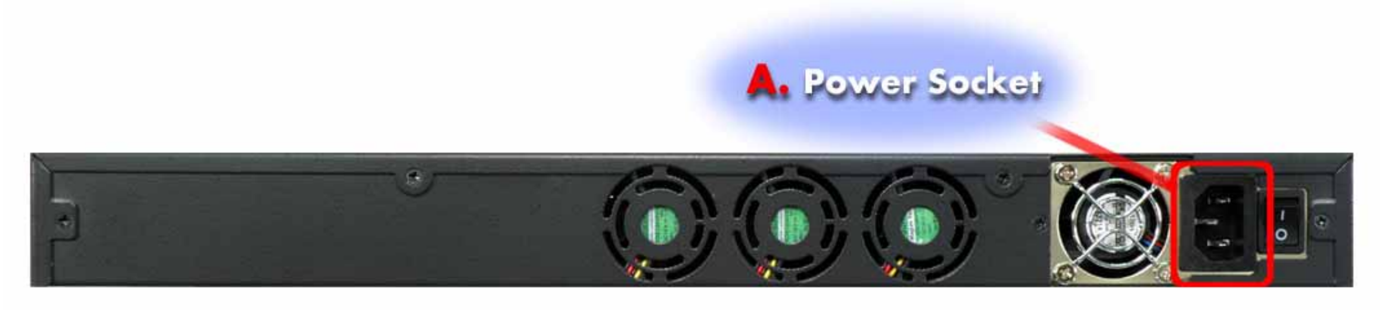


Figure 1-4 Back panel of the MH-5001

B. Using an Ethernet cable, insert one end of the cable to the WAN port on the front panel of the MH-5001 and the other end of the cable to a DSL or Cable modem, as in Figure 1-.

C. Computers with an Ethernet adapter can be directly connected to any of the LAN ports using a cross-over Ethernet cable, as in Figure 1-.

D. Computers that act as servers to provide Internet services should be connected to the DMZ port using an Ethernet Cable, as in Figure 1-.

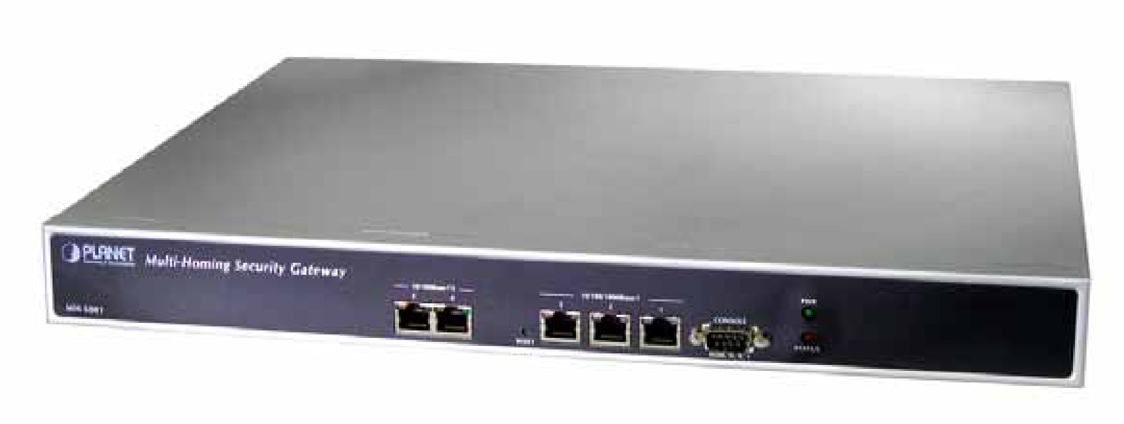


Figure 1-5 Front end of the MH-5001

1.4 Default Settings and architecture of MH-5001

You should have an Internet account already set up and have been given most of the following information as Table 1-1. Fill out this table when you edit the web configuration of MH-5001.

Items			Default value	New value
Password:			admin	
WAN1 (Port 1)	Fixed IP	IP Address	Not initialized	____.____.____.____
		Subnet Mask		____.____.____.____
		Gateway IP		____.____.____.____
		Primary DNS		____.____.____.____
		Secondary DNS		____.____.____.____
	PPPoE	PPPoE Username		____.____.____.____
		PPPoE Password		____.____.____.____
	DHCP			
WAN2 (Port 2)	Fixed IP	IP Address	Not initialized	____.____.____.____
		Subnet Mask		____.____.____.____
		Gateway IP		____.____.____.____
		Primary DNS		____.____.____.____
		Secondary DNS		____.____.____.____
	PPPoE	PPPoE Username		____.____.____.____
		PPPoE Password		____.____.____.____
	DHCP			
DMZ1(Port 3)		IP Address	10.1.1.254	____.____.____.____
		IP Subnet Mask	255.255.255.0	____.____.____.____
LAN1(Port 4)		IP Address	192.168.1.254	____.____.____.____
		IP Subnet Mask	255.255.255.0	____.____.____.____
LAN2(Port 5)		IP Address	192.168.2.254	____.____.____.____
		IP Subnet Mask	255.255.255.0	____.____.____.____

Table 1-1 MH-5001 related network settings

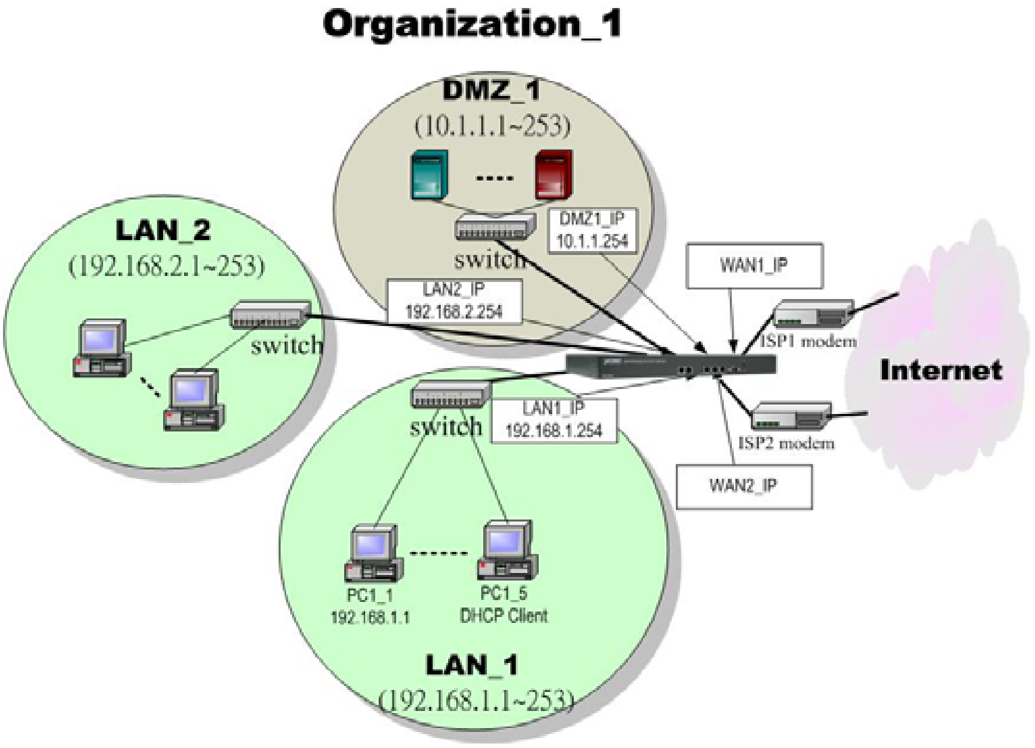
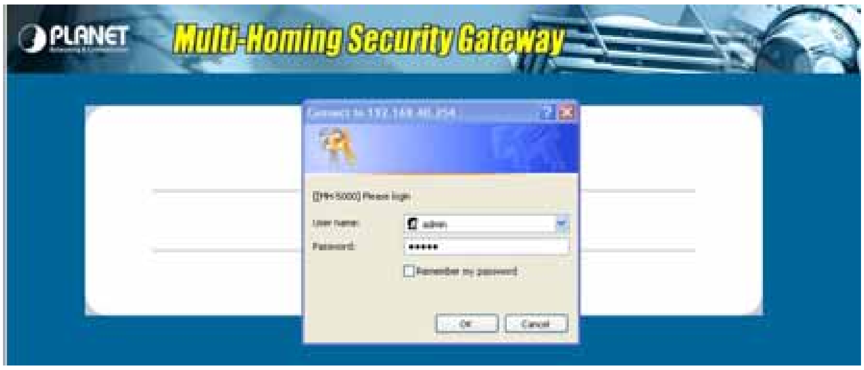
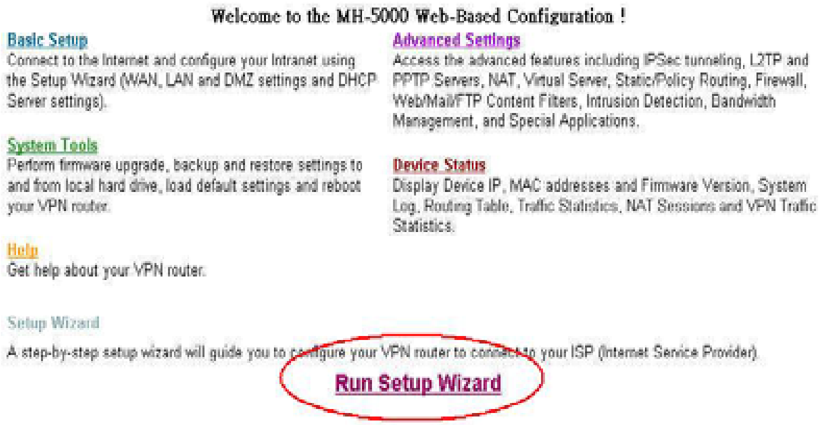
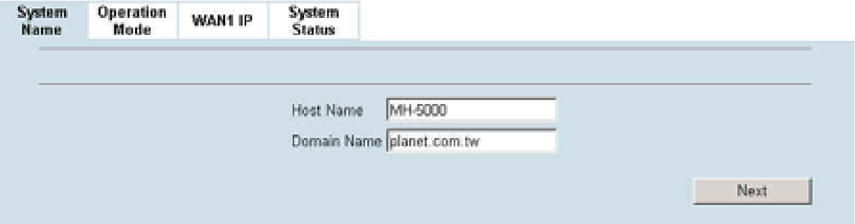
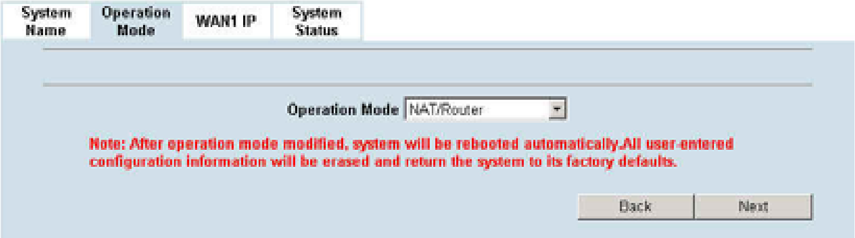


Figure 1-6 The default settings of MH-5001

As the above diagram Figure 1- illustrated, this diagram shows the default topology of MH-5001. And you can configure the MH-5001 by connecting to the LAN1_IP (192.168.1.254) from the PC1_1 (192.168.1.1). In the following sections, we will teach you how to quickly setup the MH-5001 in the basic appliances.

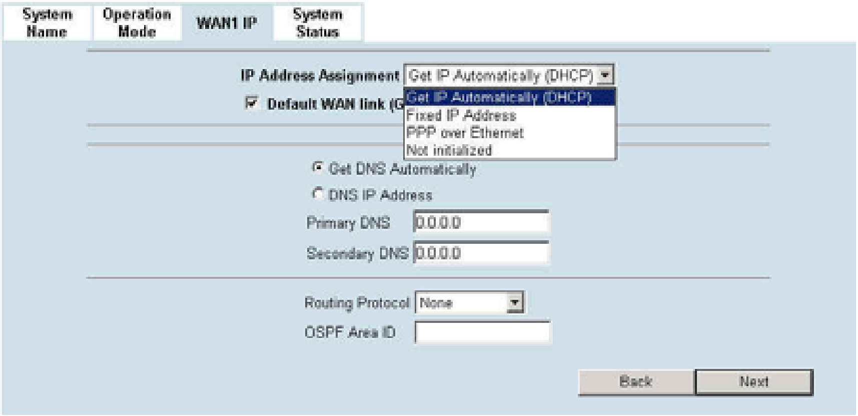
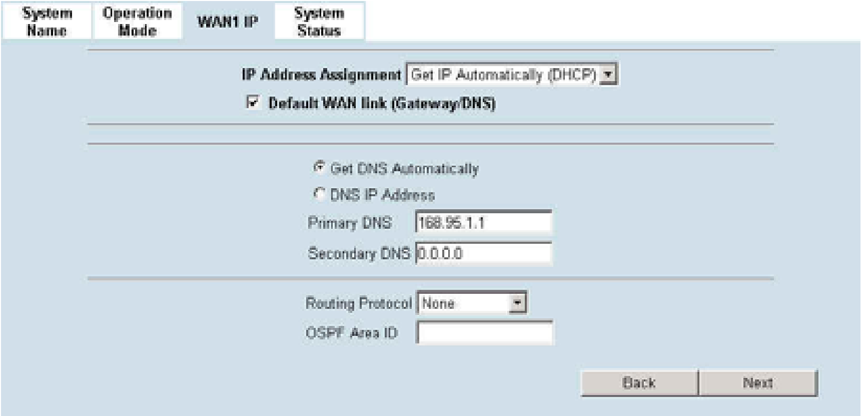
1.5 Using the Setup Wizard

A computer on your LAN1 must be assigned an IP address and Subnet Mask from the same range as the IP address and Subnet Mask assigned to the MH-5001 in order to be able to make an HTTPS connection using a web browser. The MH-5001 is assigned an IP address of 192.168.1.254 with a Subnet Mask of 255.255.255.0 by default. The computer that will be used to configure the MH-5001 must be assigned an IP address between 192.168.1.1 and 192.168.1.253 with a Subnet Mask of 255.255.255.0 to be able to connect to the MH-5001. This address range can be changed later. There are instructions in the MH-5001 Quick Installation Guide, if you do not know how to set the IP address and Subnet Mask for your computer.

Step 1. Login Type “**admin**” in the account field, “**admin**” in the Password field and click Login. Note: Please do not access web UI through proxy, or the login may be locked by others or the original user.	**Connect to https://192.168.1.254**  Connect to 192.168.40.254 [MH-5000] Please login User name: admin Password: •••••• □ Remember my password OK Cancel
Step 2. Run Setup Wizard Click the Run Setup Wizard.	**After login to https://192.168.1.254** **BASIC SETUP > Wizard**  Welcome to the MH-5000 Web-Based Configuration ! Basic Setup Connect to the Internet and configure your Intranet using the Setup Wizard (WAN, LAN and DMZ settings and DHCP Server settings). Advanced Settings Access the advanced features including IPSec tunneling, L2TP and PPTP Servers, NAT, Virtual Server, Static/Policy Routing, Firewall, Web/Mail/FTP Content Filters, Intrusion Detection, Bandwidth Management, and Special Applications. System Tools Perform firmware upgrade, backup and restore settings to and from local hard drive, load default settings and reboot your VPN router. Device Status Display Device IP, MAC addresses and Firmware Version, System Log, Routing Table, Traffic Statistics, NAT Sessions and VPN Traffic Statistics. Help Get help about your VPN router. Setup Wizard A step-by-step setup wizard will guide you to configure your VPN router to connect to your ISP (Internet Service Provider). Run Setup Wizard
Step 3. System Name Enter the Host Name and the Domain Name, followed by clicking the Next.	**BASIC SETUP > Wizard**  System Name | Operation Mode | WAN1 IP | System Status Host Name: MH-5000 Domain Name: planet.com.tw Next
Step 4. Operation Mode MH-5001 Multi-Homing Security Gateway can operate in NAT/Router mode or Transparent mode. Choose which operation Mode for this device to use.	**BASIC SETUP > Wizard > Next**  System Name | Operation Mode | WAN1 IP | System Status Operation Mode: NAT/Router Note: After operation mode modified, system will be rebooted automatically.All user-entered configuration information will be erased and return the system to its factory defaults. Back Next
NAT/Route mode	In NAT/Route mode, you can create NAT mode rules and Route mode rules. For the related information, please refer to Chapter 7 and Chapter 8. • NAT mode rules use network address translation to hide the addresses in a more secure network from users in a less secure network. • Route mode rules accept or deny connections between networks without performing address translation.

Transparent mode	Transparent mode provides the same basic protection as NAT mode. Packets received by the MH-5001 are intelligently forwarded or blocked according to firewall rules. MH-5001 can be inserted in your network at any point without the need to make any changes to your network or any of its components. However, VPN, NAT, Routing and some advanced firewall features (such as Authentication, IP/MAC Binding) are only available in NAT/Route mode. Note: 1. You cannot connect the LAN1/LAN2/DMZ interfaces to the same Hub while using Transparent mode, otherwise the traffic from the PCs under LAN1/LAN2/DMZ interfaces may be blocked. 2. If you would like to change the operation mode from NAT/Route mode to Transparent mode, you have to backup the configuration file and then do the factory reset first.

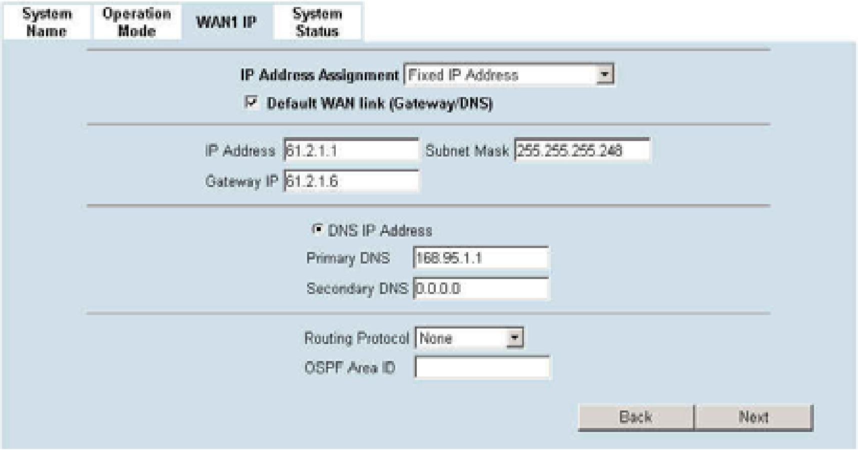
Table 1-2 The operation mode

Step 5. WAN Connectivity Choose the type of `IP Address Assignment` provided by your ISP to access the Internet. Here we have four types to select. This will determine how the IP address of WAN1 is obtained. Click `Next` to proceed.	**BASIC SETUP > Wizard > Next**  System Name Operation Mode WAN1 IP System Status Back Next IP Address Assignment: Get IP Automatically (DHCP) ▾ Get IP Automatically (DHCP) Fixed IP Address PPP over Ethernet Not initialized ☑ Default WAN link (G ● Get DNS Automatically ○ DNS IP Address Primary DNS: 0.0.0.0 Secondary DNS: 0.0.0.0 Routing Protocol: None ▾ OSPF Area ID:
Step 5.a — DHCP client If `Get IP Automatically (DHCP)` is selected, MH-5001 will request for IP address, netmask, and DNS servers from your ISP. You can use your preferred DNS by clicking the `DNS IP Address` and then completing the `Primary DNS` and `Secondary DNS` server IP addresses. Click `Next` to proceed.	**BASIC SETUP > Wizard > Next > DHCP**  System Name Operation Mode WAN1 IP System Status Back Next IP Address Assignment: Get IP Automatically (DHCP) ▾ ☑ Default WAN link (Gateway/DNS) ● Get DNS Automatically ○ DNS IP Address Primary DNS: 168.95.1.1 Secondary DNS: 0.0.0.0 Routing Protocol: None ▾ OSPF Area ID:

Step 5.b — **Fixed IP**

If Fixed IP Address is selected, enter the ISP-given IP Address, Subnet Mask, Gateway IP, Primary DNS and Secondary DNS IP. Click Next to proceed.

BASIC SETUP > Wizard > Next > Fixed IP



IP Address Assignment: Fixed IP Address

☑ Default WAN link (Gateway/DNS)

IP Address: 61.2.1.1
Subnet Mask: 255.255.255.248
Gateway IP: 61.2.1.6

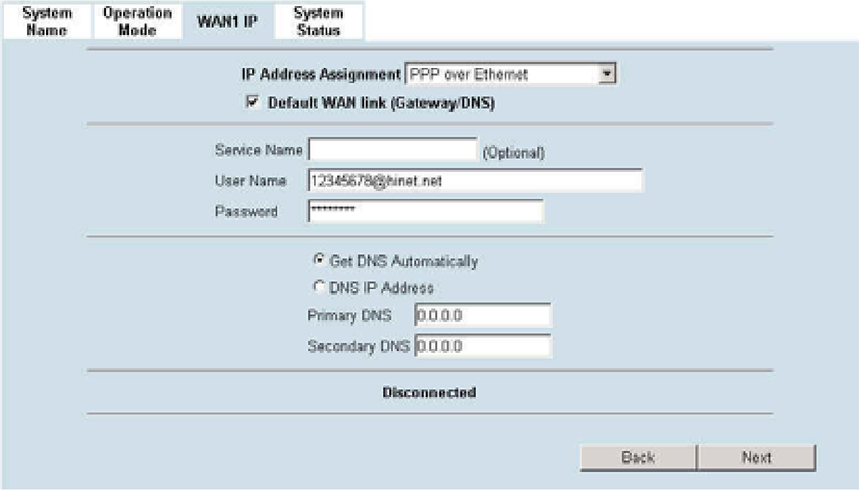
● DNS IP Address
Primary DNS: 168.95.1.1
Secondary DNS: 0.0.0.0

Routing Protocol: None
OSPF Area ID:

Step 5.c — **PPPoE client**

If PPP over Ethernet is selected, enter the ISP-given User Name, Password and the optional Service Name. Click Next to proceed.

BASIC SETUP > Wizard > Next > PPPoE



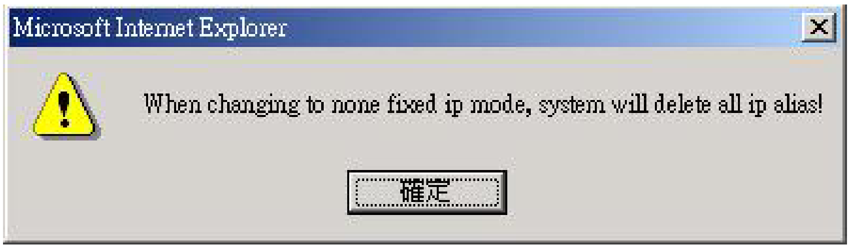
IP Address Assignment: PPP over Ethernet

☑ Default WAN link (Gateway/DNS)

Service Name: (Optional)
User Name: 12345678@hinet.net
Password: ********

● Get DNS Automatically
○ DNS IP Address
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0

Disconnected



When changing to none fixed ip mode, system will delete all ip alias!

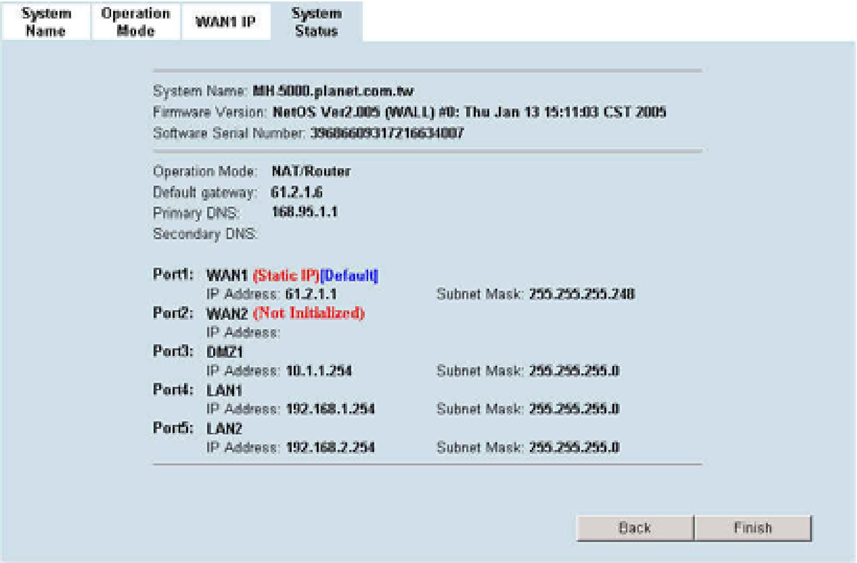
✓ Warning Message

Please Note that an alert message box “`When changing to none fixed ip mode, system will delete all ip alias!`” will appear while you change Get IP Automatically (DHCP) or PPP over Ethernet but not Fixed IP Address as your WAN link.

Step 6. System Status

Here we select `Fixed IP` method in WAN1 port. Then the MH-5001 provides a short summary of the system. Please check if anything mentioned above is properly set into the system. Click `Finish` to close the wizard.

BASIC SETUP > Wizard > Run Setup Wizard > Next > Next



```
System Name: MH 5000.planet.com.tw
Firmware Version: NetOS Ver2.005 (WALL) #0: Thu Jan 13 15:11:03 CST 2005
Software Serial Number: 39606609317216634007

Operation Mode:    NAT/Router
Default gateway:   61.2.1.6
Primary DNS:       168.95.1.1
Secondary DNS:

Port1:  WAN1 (Static IP)[Default]
        IP Address: 61.2.1.1          Subnet Mask: 255.255.255.240
Port2:  WAN2 (Not Initialized)
        IP Address:
Port3:  DMZ1
        IP Address: 10.1.1.254        Subnet Mask: 255.255.255.0
Port4:  LAN1
        IP Address: 192.168.1.254     Subnet Mask: 255.255.255.0
Port5:  LAN2
        IP Address: 192.168.2.254     Subnet Mask: 255.255.255.0
```

1.6 Internet Connectivity

After setting up MH-5001 with the wizard, MH-5001 can connect to the ISP. In this chapter, we introduce **LAN1-to-WAN1** Connectivity to explain how the computers under LAN1 can access the Internet at WAN1 through MH-5001. Subsequently, we introduce **WAN1-to-DMZ1** Connectivity to explain how the servers under DMZ1 can be accessed by the LAN1 users and other Internet users on the WAN1 side.

You MUST press Apply to proceed to the next page. Once applying any changes, the settings are immediately updated into the flash memory.

1.6.1 LAN1-to-WAN1 Connectivity

The LAN Settings page allows you to modify the IP address and Subnet Mask that will identify the MH-5001 on your LAN. This is the IP address you will enter in the URL field of your web browser to connect to the MH-5001. It is also the IP address that all of the computers and devices on your LAN will use as their Default Gateway.

Step 1. Device IP Address

Setup the IP Address and IP Subnet Mask for the MH-5001.

BASIC SETUP > LAN Settings > LAN1 Status

Step 2. Client IP Range

Enable the DHCP server if you want to use MH-5001 to assign IP addresses to the computers under LAN1. Specify the Pool Starting Address, Pool Size, Primary DNS, and Secondary DNS that will be assigned to them.

Example: in the figure, the MH-5001 will assign one IP address from 192.168.1.100 ~ 192.168.1.119, together with the DNS server 192.168.1.254, to the LAN1 PC that requests for an IP address.

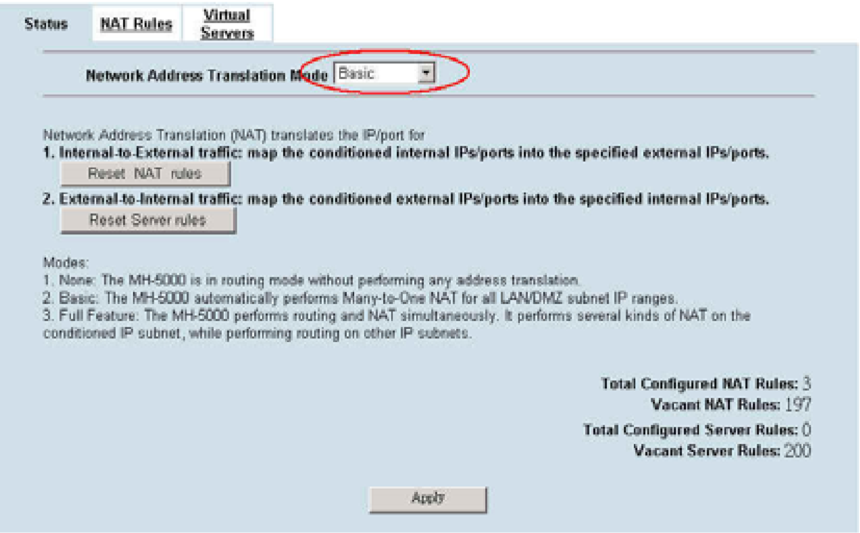
Step 3. Apply the Changes

Click `Apply` to save. Now you can enable the DHCP clients on your LAN1 PCs to get an IP.

Step 4. Check NAT Status

The default setting of NAT is in `Basic` Mode. After completing Step 3, the NAT is automatically configured related rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.

ADVANCED SETTINGS > NAT > Status



Network Address Translation Mode: Basic

Network Address Translation (NAT) translates the IP/port for
1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.

2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.

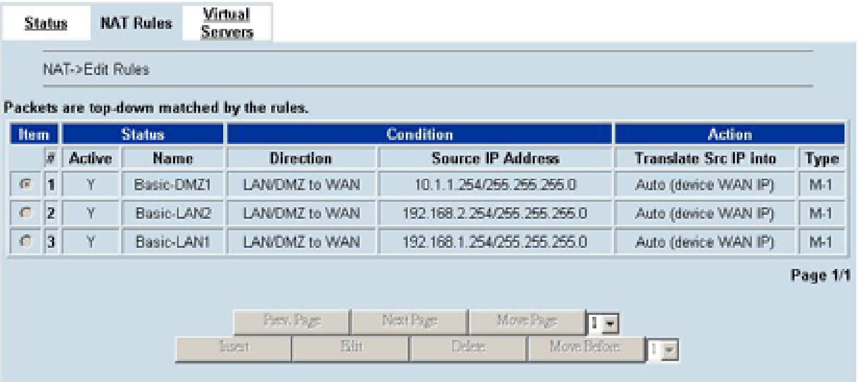
Modes:
1. None: The MH-5000 is in routing mode without performing any address translation.
2. Basic: The MH-5000 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
3. Full Feature: The MH-5000 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

Total Configured NAT Rules: 3
Vacant NAT Rules: 197
Total Configured Server Rules: 0
Vacant Server Rules: 200

Step 5. Check NAT Rules

The MH-5001 has added the NAT rules as the right diagram. The rule `Basic-LAN1` means that, when matching the condition (requests of `LAN/DMZ-to-WAN` direction with its source IP falling in the range of `192.168.1.254 / 255.255.255.0`), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.

ADVANCED SETTINGS > NAT > NAT Rules



NAT->Edit Rules

Packets are top-down matched by the rules.

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Translate Src IP Into	Type
●	1	Y	Basic-DMZ1	LAN/DMZ to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1
○	2	Y	Basic-LAN2	LAN/DMZ to WAN	192.168.2.254/255.255.255.0	Auto (device WAN IP)	M-1
○	3	Y	Basic-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M-1

Page 1/1

1.6.2 WAN1-to-DMZ1 Connectivity

This section tells you how to provide an FTP service with a server installed under your DMZ1 to the public Internet users. After following the steps, users at the WAN side can connect to the FTP server at the DMZ1 side.

Step 1. Device IP Address

Setup the IP Address and IP Subnet Mask for the MH-5001 of the DMZ1 interface.

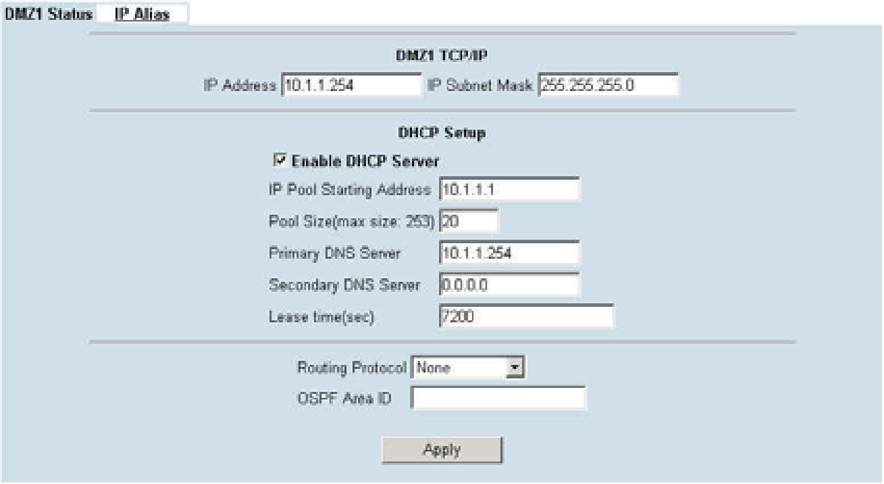
Step 2. Client IP Range

Enable the `DHCP server` if you want to use MH-5001 to assign IP addresses to the computers under DMZ1.

Step 3. Apply the Changes

Click `Apply` to save your settings.

BASIC SETUP > DMZ Settings > DMZ1 Status



DMZ1 TCP/IP

IP Address 10.1.1.254 IP Subnet Mask 255.255.255.0

DHCP Setup

☑ **Enable DHCP Server**

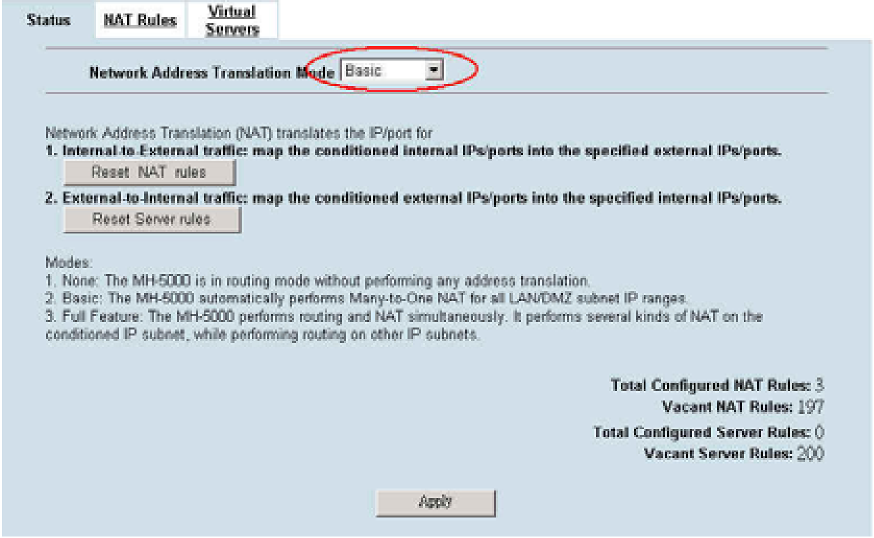
IP Pool Starting Address	10.1.1.1
Pool Size(max size: 253)	20
Primary DNS Server	10.1.1.254
Secondary DNS Server	0.0.0.0
Lease time(sec)	7200

Routing Protocol	None
OSPF Area ID	

Step 4. Check NAT Status

The default setting of NAT is in `Basic` Mode. After applying the Step 3, the NAT is automatically configured related rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.

ADVANCED SETTINGS > NAT > Status



Network Address Translation Mode Basic

Network Address Translation (NAT) translates the IP/port for

1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.

2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.

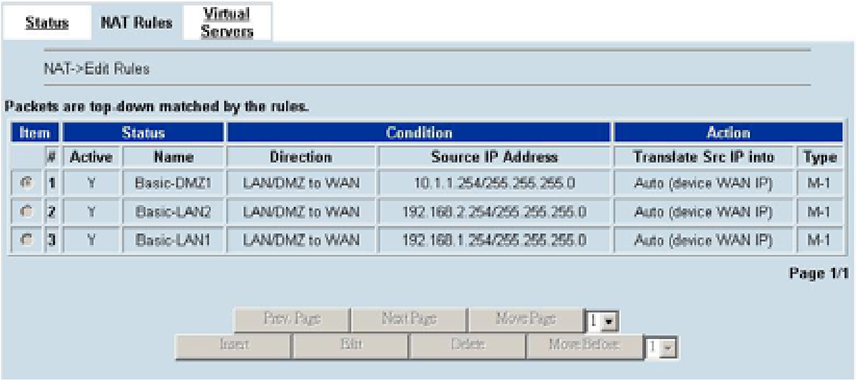
Modes:
1. None: The MH-5000 is in routing mode without performing any address translation.
2. Basic: The MH-5000 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
3. Full Feature: The MH-5000 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

Total Configured NAT Rules: 3
Vacant NAT Rules: 197
Total Configured Server Rules: 0
Vacant Server Rules: 200

Step 5. Check NAT Rules

The MH-5001 has added the NAT rules as the right diagram. The rule `Basic-DMZ1` (number 1) means that, when matching the condition (requests of `LAN/DMZ-to-WAN` direction with its source IP falling in the range of `10.1.1.254 / 255.255.255.0`), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.

ADVANCED SETTINGS > NAT > NAT Rules



NAT->Edit Rules

Packets are top-down matched by the rules.

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Translate Src IP into	Type
●	1	Y	Basic-DMZ1	LAN/DMZ to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1
○	2	Y	Basic-LAN2	LAN/DMZ to WAN	192.168.2.254/255.255.255.0	Auto (device WAN IP)	M-1
○	3	Y	Basic-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M-1

Page 1/1

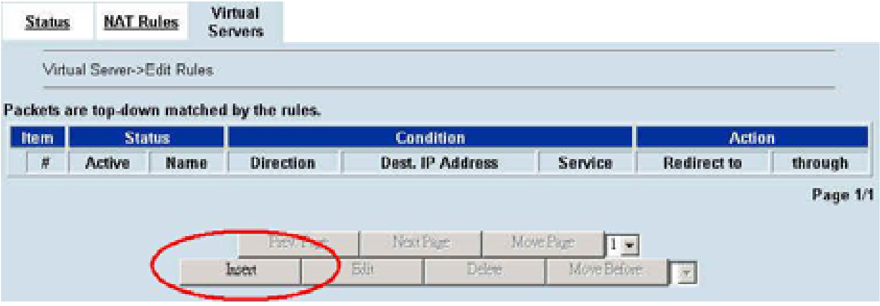
Step 6. Setup IP for the FTP Server

Assign an IP of 10.1.1.5/255.255.255.0 to the FTP server under DMZ1. Assume the FTP Server is at 10.1.1.5. And it is listening on the well-known port (21).

Step 7. Setup Server Rules

Insert a virtual server rule by clicking the `Insert` button.

ADVANCED SETTINGS > NAT > Virtual Servers



Virtual Server->Edit Rules

Packets are top-down matched by the rules.

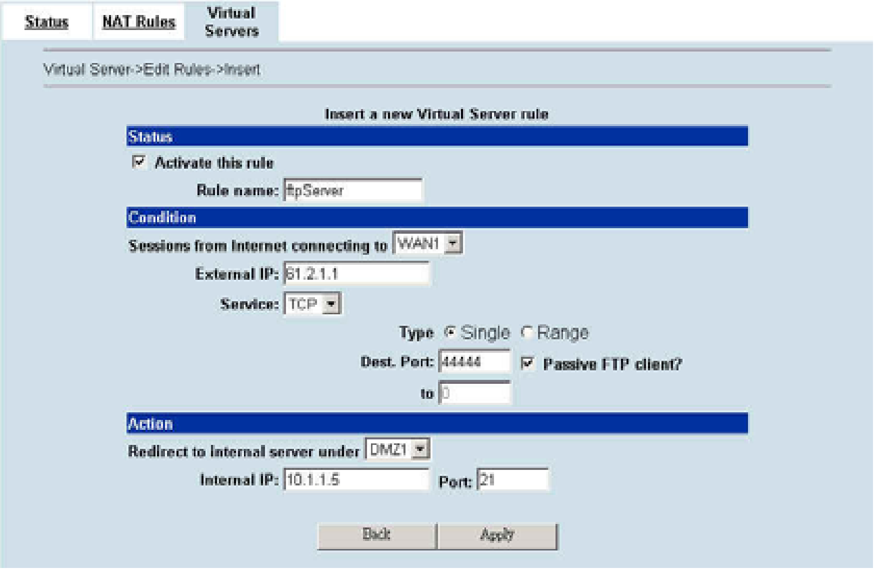
Item	Status		Condition			Action	
#	Active	Name	Direction	Dest. IP Address	Service	Redirect to	through

Page 1/1

Step 8. Customize the Rule

Customize the rule name as the `ftpServer`. For any packets with its destination IP address equaling to the WAN1 IP (`61.2.1.1`) and destination port equaling to `44444`. MH-5001 will translate the packet's destination IP/port into `10.1.1.5/21`. Check the `Passive FTP client` to maximize the compatibility of the FTP protocol. This is useful if you want to provide connectivity to passive FTP clients. For passive FTP clients, the server at DMZ will return them the private IP address (10.1.1.5) and the port number for the clients to connect back for data transmissions. Since the FTP clients at the WAN side cannot connect to a private-IP (ex.10.1.1.5) through the Internet. The data connections would be fail. After enabling this feature, the MH-5001 will translate the private IP/port into an IP/port of its own. Thus the problem is gracefully solved. Click `Apply` to proceed.

ADVANCED SETTINGS > NAT > Virtual Servers > Insert



Virtual Server->Edit Rules->Insert

Insert a new Virtual Server rule

Status

☑ Activate this rule

Rule name: ftpServer

Condition

Sessions from Internet connecting to WAN1

External IP: 61.2.1.1

Service: TCP

Type ● Single ○ Range

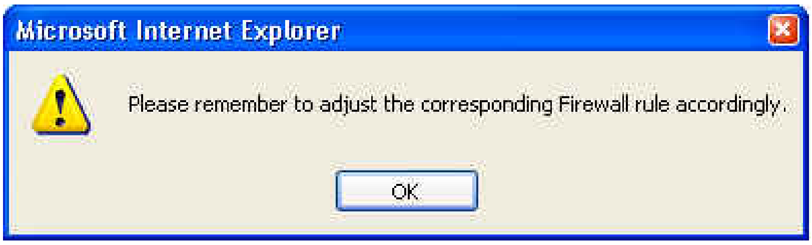
Dest. Port: 44444 ☑ Passive FTP client?

to 0

Action

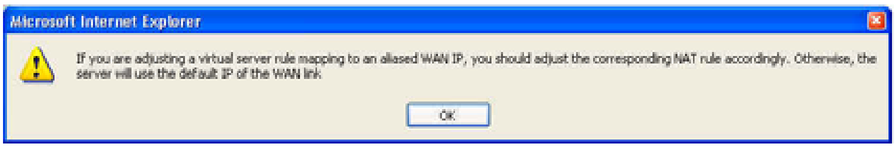
Redirect to Internal server under DMZ1

Internal IP: 10.1.1.5 Port: 21



Microsoft Internet Explorer

Please remember to adjust the corresponding Firewall rule accordingly.



Microsoft Internet Explorer

If you are adjusting a virtual server rule mapping to an aliased WAN IP, you should adjust the corresponding NAT rule accordingly. Otherwise, the server will use the default IP of the WAN link

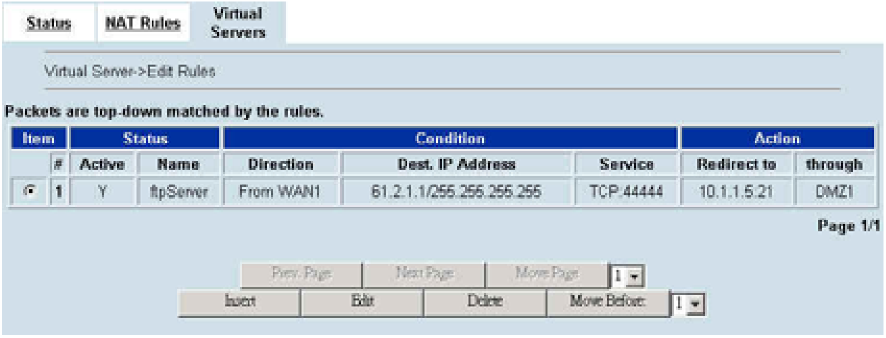
✓ Warning message

After applying the virtual server rule, there will appear two messages as above diagrams. The purpose of the above two message boxes are trying to remind you to add firewall/NAT rules manually while you add a virtual server rule for your existing server.

Step 9. View the Result

Now any request towards the MH-5001's WAN1 IP (`61.2.1.1`) with dest. port `44444` will be translated into a request towards `10.1.1.5` with port `21`, and then be forwarded to the `10.1.1.5`. The FTP server listening at port `21` in `10.1.1.5` will pick up the request.

ADVANCED SETTINGS > NAT > Virtual Servers



Virtual Server->Edit Rules

Packets are top-down matched by the rules.

Item	Status		Condition			Action	
#	Active	Name	Direction	Dest. IP Address	Service	Redirect to	through
● 1	Y	ftpServer	From WAN1	61.2.1.1/255.255.255.255	TCP:44444	10.1.1.5:21	DMZ1

Page 1/1

1.7 NAT/Router Mode and Transparent Mode

1.7.1 NAT/Router Mode

When the MH-5001 is running in NAT/Router mode, you can connect a private network to the internal interface, a DMZ network to the DMZ interface, and a public network, such as the Internet, to the external interface. Each of these networks must have a different subnet address. You create security policies to control how the firewall routes packets between MH-5001 interfaces, and therefore between the networks connected to the interface. When you switch the MH-5001 operation mode from NAT/Router mode to Transparent mode, you have to backup your configuration first, otherwise the original configuration will be deleted inclusive of all rules, policies, addresses, etc. After system reboots, MH-5001 will return to the factory default.

In this document, we will introduce you how to setup NAT/Router Mode firewall in the most examples. You can learn the settings of each feature by them. For more information of how to choose NAT or Route mode in the MH-5001, please refer Section 7.5.4.

1.7.2 Transparent Mode

When the MH-5001 is running in Transparent mode, it can be inserted in your network at any point without changing your network or any of its components. In Transparent mode, you can add Transparent mode rules/policies to accept or deny connections between interfaces. The firewall will apply those rules/policies to control traffic without modifying the packets in any way. Please make sure not to connect the LAN1/LAN2/DMZ interfaces to the same Hub while using Transparent mode, otherwise the traffic from the PCs under LAN1/LAN2/DMZ interfaces may be blocked.

For the MH-5001 Transparent mode connections, please refer to the following Figure 1-.

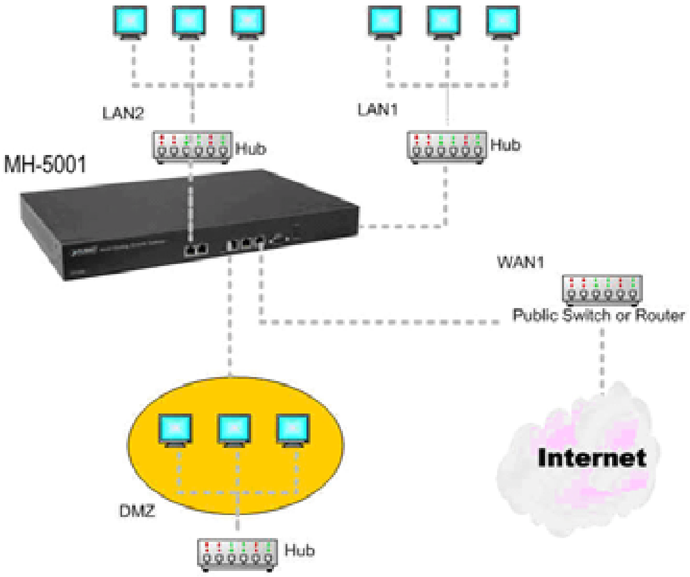


Figure 1-7 MH-5001 Transparent mode connections

Basically, transparent mode provides the same firewall protection as NAT mode. Packets received by the MH-5001 are intelligently forwarded or blocked according to the firewall rules. However, some advanced firewall features are only available in NAT/Route mode.

Transparent mode will not support the following features currently:

1. WAN PPPoE link
2. Authentication
3. VPN (IPSec / PPTP / L2TP)
4. NAT
5. Routing
6. IP/MAC Binding
7. DDNS / DNS Proxy / DHCP Relay
8. Interface change
9. Show IPSec sessions
10. VPN Logs

Chapter 2
System Overview

In this chapter, we will introduce the network topology for use with later chapters.

2.1 Typical Example Topology

In this chapter, we introduce a typical network topology for the MH-5001. In Figure 2-1, the left half side is a MH-5001 with one LAN, one DMZ, and one WAN link. We will demonstrate the administration procedure in the later chapters by using the below Figure 2-1.

The right half side contains another MH-5001 connected with one LAN, one DMZ, and one WAN. You can imagine this is a branch office of Organization_1. In this architecture, all the users under Organization can access sever reside in the Internet or DMZ region smoothly. Besides, Organization_1 communicates with Organization_2 with a VPN tunnel established by the two MH-5001 Multi-Homing Security Gateways. The VPN tunnel secures communications between Organizations more safely.

We will focus on how to build up the topology using the MH-5001 as the following Figure 2-1. In order to achieve this purpose, we need to know all the administration procedure.

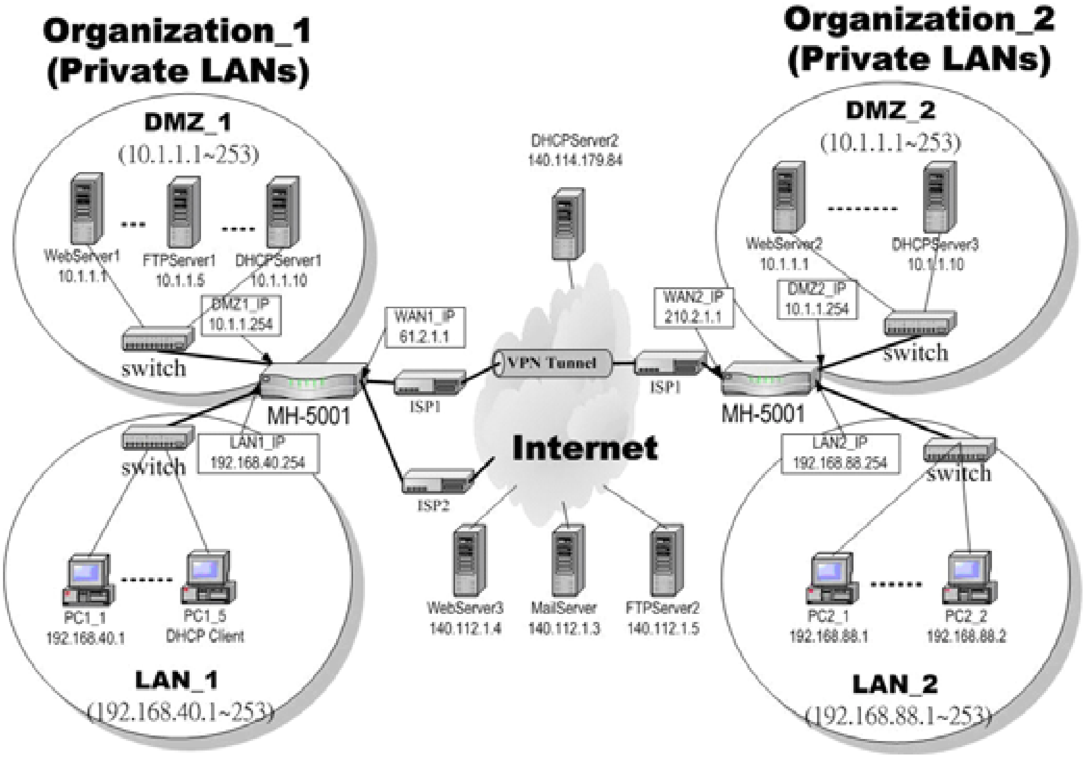


Figure 2-1 Typical topology for deploying MH-5001

Continually, we will introduce all the needed administration procedure in the following section.

1. **Chapter 3 Basic Setup**
   How to configure the WAN/DMZ/LAN port settings.

2. **Chapter 7 ~ Chapter 12 NAT, Routing and Firewall**
   Introducing the NAT, Routing, Firewall features.

3. **Chapter 13 ~ Chapter18 VPN Technology Introduction**
   If you need to build a secure channel with your branch office, or wish to access the inside company resource as usual while outside your company, the Virtual Private Network (VPN) function can satisfy you.

4. **Chapter19 ~ Chapter 21 Content Filtering**
   If you hope to restrict the web contents, mail attachments, or downloaded ftp file from intranet region, try this feature to fit your requirement.

5. **Chapter 23 Intrusion Prevention System**
   Use the Intrusion Detection System (IPS) to detect all the potential DoS attacks, worms, hackers from Internet.

6. **Chapter 24 Bandwidth Management**
   If you wish to make your inbound/outbound bandwidth utilized more efficiently, you may use the Bandwidth Management feature to manage your bandwidth.

7. **Chapter23 Load Balancer**
   The WAN load balancer module consists of outbound load balancing and inbound load balancing. Users may want to subscribe multiple WAN links and make their outbound traffic load-balanced among the WAN links. MH-5001 now supports outbound WAN load balancing. Inbound load balancing will be supported in a very near future.

8. **Chapter 24 ~ Chapter 29 System Maintenance**
   In this part, we provide some useful skills to help you to justify MH-5001 more securely and steadily.

2.2 Changing the LAN1 IP Address

The default settings of MH-5001 are listing in Table 1-1. However, the original LAN1 setting is 192.168.1.254/255.255.255.0 instead of 192.168.40.254/255.255.255.0 as in Figure 2-1. We will change the LAN1 IP of the MH-5001 to 192.168.40.254.

We provide two normal ways to configure the LAN1 IP address. One is to configure the LAN1 IP from LAN1 port. The other way is to configure the LAN1 IP through console.

2.2.1 From LAN1 to configure MH-5001 LAN1 network settings

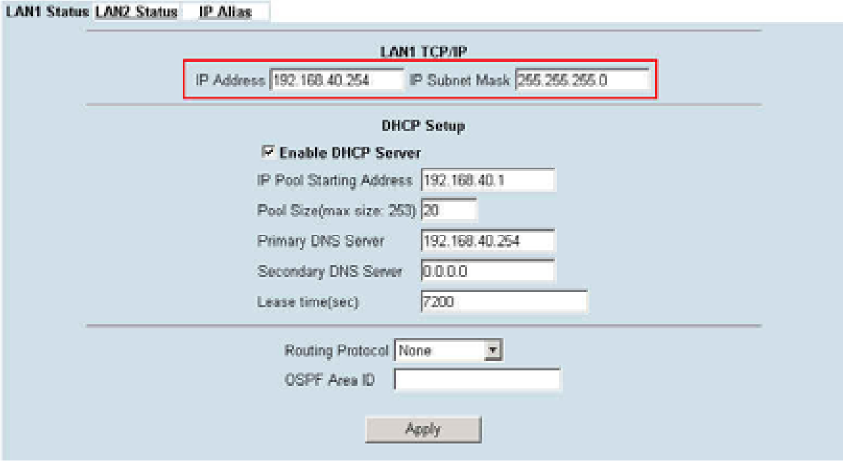
Step 1. Connect to the MH-5001 Using a network line to connect MH-5001 with LAN1 port. The PC which connected to MH-5001 must be assigned 192.168.1.X address (LAN1 default IP address is 192.168.1.254/24). Type https://192.168.1.254 or http://192.168.1.254:8080 to configure the MH-5001 in the web browser.	**Use an IE at 192.168.1.1 to connect to** https://192.168.1.254

Step 2. Setup LAN1 IP information

Enter the IP Address and IP Subnet Mask with 192.168.40.254 / 255.255.255.0 and click Apply.

Warning: After you apply the changed settings, the network will be disconnected instantly since the network IP address you are logining is changed.

BASIC SETUP > LAN Settings > LAN1 Status



IP Address 192.168.40.254 IP Subnet Mask 255.255.255.0

☑ Enable DHCP Server

IP Pool Starting Address 192.168.40.1

Pool Size(max size: 253) 20

Primary DNS Server 192.168.40.254

Secondary DNS Server 0.0.0.0

Lease time(sec) 7200

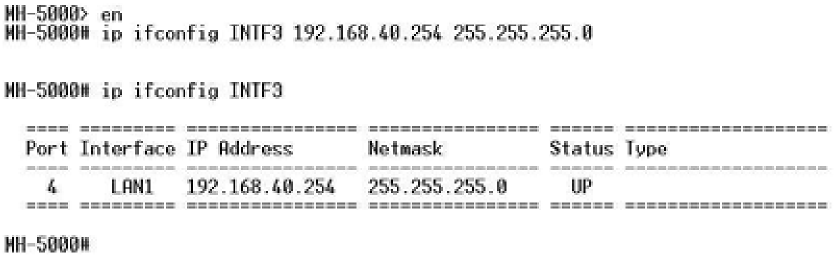
Routing Protocol None

OSPF Area ID

2.2.2 From CLI (command line interface) to configure MH-5001 LAN1 network settings

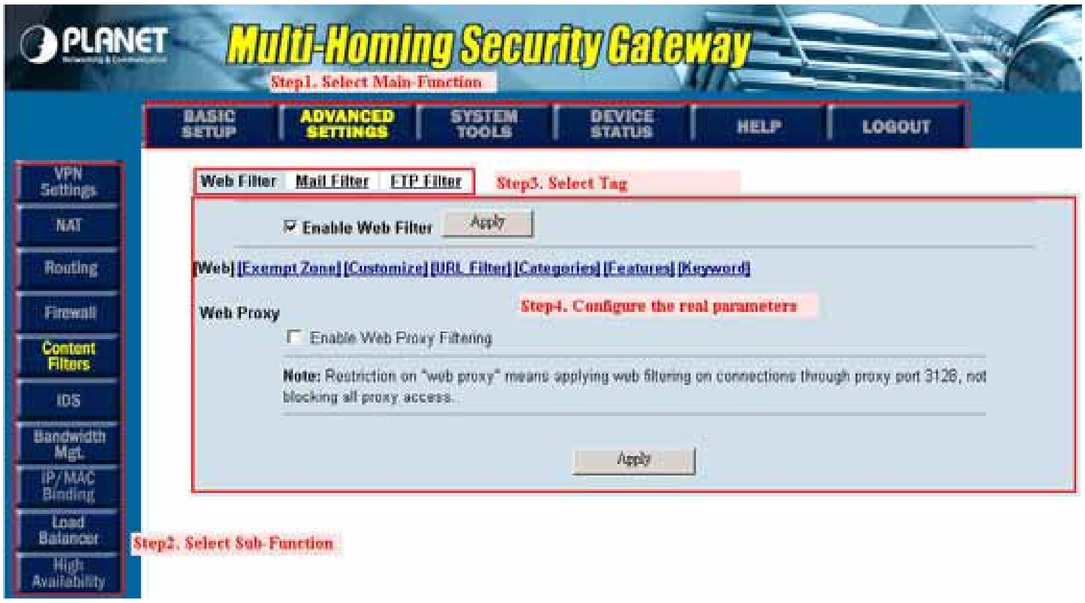
Step 1. Use Console port to configure MH-5001

Use the supplied console line to connect the PC to the Diagnostic RS-232 socket of the MH-5001. Start a new connection using the HyperTerminal with parameters: No Parity, 8 Data bits, 1 stop bit, and baud rate 9600. Enter admin for user name and admin for password to login. After logging into MH-5001, enter the commands “en“ to enter the privileged mode. Enter the command “ip ifconfig INTF3 192.168.40.254 255.255.255.0” to change the IP of the LAN1 interface.



```
MH-5000> en
MH-5000# ip ifconfig INTF3 192.168.40.254 255.255.255.0

MH-5000# ip ifconfig INTF3

  ==== ========= ================ ================ ====== ===================
  Port Interface IP Address       Netmask          Status Type
  ---- --------- ---------------- ---------------- ------ -------------------
   4     LAN1    192.168.40.254   255.255.255.0     UP
  ==== ========= ================ ================ ====== ===================

MH-5000#
```

2.2.3 Web GUI design principle



Step1. Select Main-Function

Step2. Select Sub-Function

Step3. Select Tag

Step4. Configure the real parameters

☑ Enable Web Filter

Web Proxy

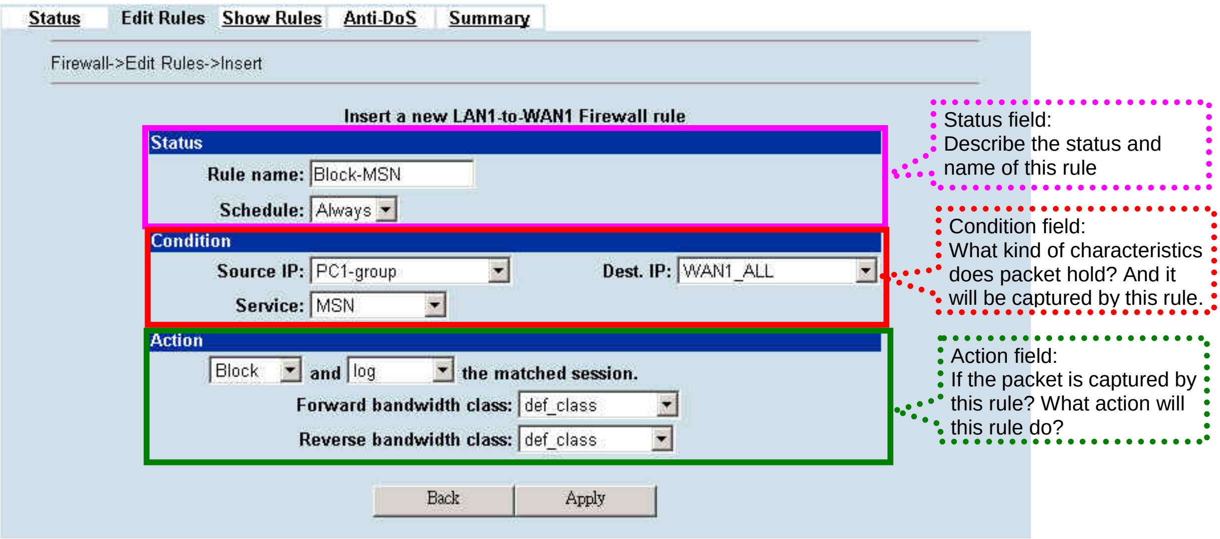
□ Enable Web Proxy Filtering

Note: Restriction on "web proxy" means applying web filtering on connections through proxy port 3128, not blocking all proxy access.

Figure 2-2 You can select the functional area by the sequence in Web GUI

If we want to configure MH-5001, we can follow the sequence as the Figure 2-2 illustrated.
Step1. Select Main-function
Step2. Select Sub-function
Step3. Select Tag
Step4. Configure the real parameters

2.2.4 Rule principle



Firewall->Edit Rules->Insert

Insert a new LAN1-to-WAN1 Firewall rule

Status
Rule name: Block-MSN
Schedule: Always

Condition
Source IP: PC1-group
Dest. IP: WAN1_ALL
Service: MSN

Action
Block and log the matched session.
Forward bandwidth class: def_class
Reverse bandwidth class: def_class

Status field:
Describe the status and name of this rule

Condition field:
What kind of characteristics does packet hold? And it will be captured by this rule.

Action field:
If the packet is captured by this rule? What action will this rule do?

Figure 2-3 The rule configuration is divided into three parts

You may find many rules configuration in the MH-5001. They are distributed in the respective feature. These rules include

1. NAT rule
2. Virtual Server rule
3. Firewall rule
4. Policy route rule
5. Bandwidth management rule

The behavior of each rule is different, and so are their configuration parameters. But the designed principle of each rule is the same. The configuration is divided into three parts as Figure 2-3 illustrated. You just need to enter the necessary information onto each part according to your requirement. As for the definitions of the three-part configuration, please refer to the following description.

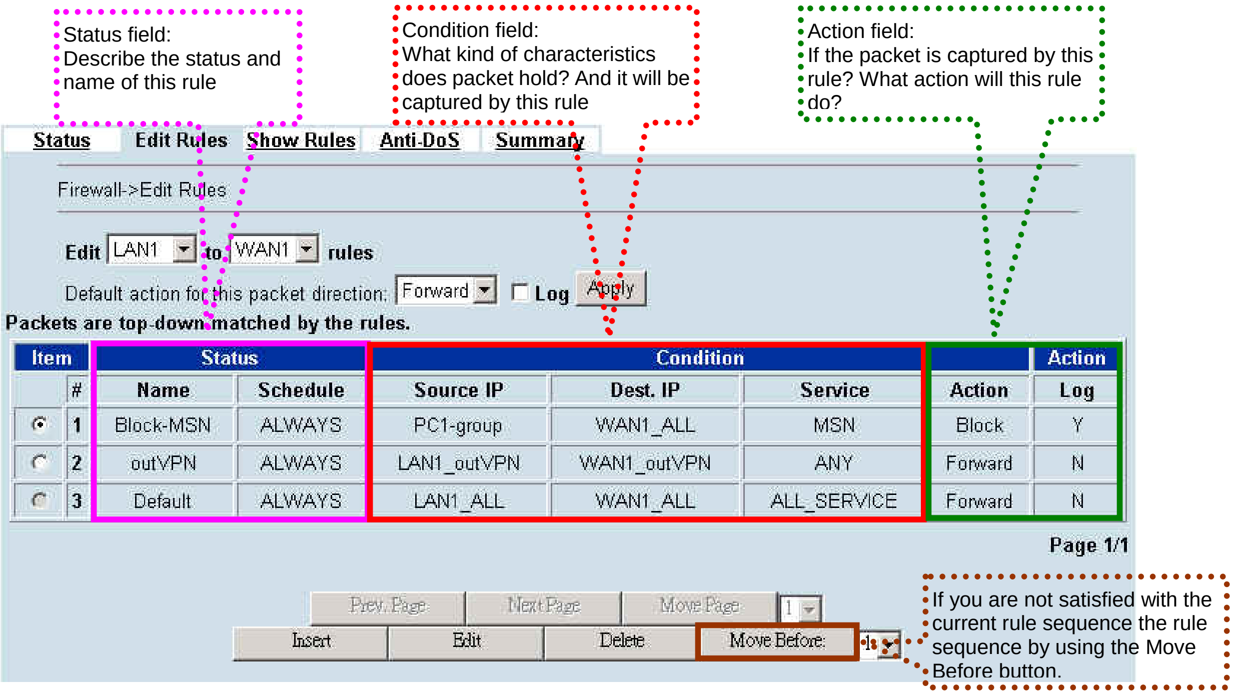
1. Status: Describe the status and name of this rule.

2. Condition: What kind of characteristics does packet hold? And it will be captured by this rule.

3. Action: If the packet is captured by this rule? What action will this rule do?

As the Figure 2-4 illustrated, the page of the rule edition is also divided into three parts. Their definitions are also the same as we have discussed in Figure 2-3.

Additionally, please note that there is a button named “Move Before” in the Figure 2-4. If you are not satisfied with the current rule sequence, you can adjust the rule sequence by using the “Move Before” button.



Status field:
Describe the status and name of this rule

Condition field:
What kind of characteristics does packet hold? And it will be captured by this rule

Action field:
If the packet is captured by this rule? What action will this rule do?

Firewall->Edit Rules

Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward □ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition			Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Block-MSN	ALWAYS	PC1-group	WAN1_ALL	MSN	Block	Y
○	2	outVPN	ALWAYS	LAN1_outVPN	WAN1_outVPN	ANY	Forward	N
○	3	Default	ALWAYS	LAN1_ALL	WAN1_ALL	ALL_SERVICE	Forward	N

Page 1/1

If you are not satisfied with the current rule sequence the rule sequence by using the Move Before button.

Figure 2-4 The rules in the page of the rule edition are also divided into three parts

.

Chapter 3
Basic Setup

In this chapter, we will introduce how to setup network settings for each port separately

3.1 Demands

1. For the external network, suppose your company uses DSL to connect Internet via fixed-IP. By this way, you should setup WAN port of the MH-5001 in advance.
2. There are some adjustment within your company, so the original network stucture has been changed. Now, you should modify the configuration between the internal network (DMZ, LAN).
3. Your company needs more network bandwidth if it is insufficent for your company to connect to the external network. Suppose there are many public IPs in your commpany, you would like to specify an unique public IP to a local server.
4. When the default WAN link is disconnected, you need a backup solution to keep the Internet connection working.

3.2 Objectives

1. Configure the network settings of the MH-5001 WAN1 port.
2. Configure the network settings of the MH-5001 DMZ1 and LAN1 ports.
3. We hope to assign another IP address to the same WAN port that we have configured before.
4. Ping the public Internet Server IP addresses with a sequence of every specified Timeout to check the connection of the current default WAN link. When the specified WAN link is disconnected, MH-5001 will try to make the ping action to the first Public Internet Server IP address within the specified Timeout. When all of them are timeout, the default route/link will be switched to another WAN link to continue the ping action within the specified Detection Interval.

3.3 Methods

1. Select the Fixed IP Address method in the MH-5001 Basic Setup/WAN settings/WAN1 IP, and then configure the related account and password in order to connet to the Internet.
2. Configure the related network settings in the pages of the MH-5001 Basic Setup / DMZ settings / DMZ1 Status、Basic Setup / LAN settings / LAN1 Status.
3. Configure the IP alias in WAN1 port.
4. Configure the public Internet Server IP addresses, set the time to continue the ping action per IP address and then set the detection interval for the next WAN link check.

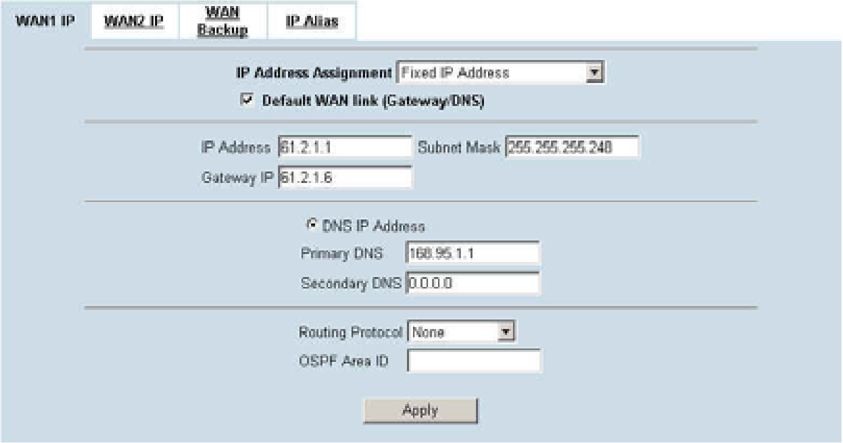
3.4 Steps

3.4.1 Setup WAN1 IP

Step 1. Setup WAN1 port

Here we select `Fixed IP Address` method in WAN1 port. Fill in the `IP Address, Subnet Mask, Gateway IP`. And then enter the other `DNS IP Address`, `Routing Protocol` fields. Click `Apply` to finish this setting.

BASIC SETUP > WAN Settings > WAN1 IP > Fixed IP Address



IP Address Assignment: Fixed IP Address

☑ Default WAN link (Gateway/DNS)

IP Address: 61.2.1.1 Subnet Mask: 255.255.255.248

Gateway IP: 61.2.1.6

● DNS IP Address

Primary DNS: 168.95.1.1

Secondary DNS: 0.0.0.0

Routing Protocol: None

OSPF Area ID:

IP Address Assignment	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Get IP Automatically (DHCP)	Default WAN link (Gateway/DNS)	When Default WAN link is enabled, all the packets sent out from MH-5001 will be via this port.	Enable/Disable	Enabled
	Get DNS Automatically / DNS IP Address	Get DNS Automatically → Get DNS related information from DHCP Server DNS IP Address → manually specify these Primary and Secondary DNS Server information	Get DNS Automatically / DNS IP Address	Get DNS Automatically
	Routing Protocol	Determine to enable the dynamic routing protocol, to receive RIP message, to send out the RIP message if the RIP message is received or not.	None, RIPv1/In, RIPv1/In+Out, RIPv2/In, RIPv2/In+Out, OSPF	None
	OSPF Area ID	Specify OSPF area ID number	IPv4 format or digit string (Max 9 bits)	
Fixed IP Address	Default WAN link (Gateway/DNS)	When Default WAN link is enabled. All the packets sent out from MH-5001 will be via this port.	Enable/Disable	Enabled
	IP Address	Specified IP address	IPv4 format	61.2.1.1
	Subnet Mask	Specified subnet mask	IPv4 format	255.255.255.248
	Gateway IP	Default gateway IP address	IPv4 format	61.2.1.6

	DNS IP Address: Primary DNS Secondary DNS	Specified Primary and Secondary DNS Server address	IPv4 format	Primary DNS: 168.95.1.1 Secondary DNS: 0.0.0.0
	Routing Protocol	Determine to enable the dynamic routing protocol, to receive RIP message, to send out the RIP message if the RIP message is received or not.	None, RIPv1/In, RIPv1/In+Out, RIPv2/In, RIPv2/In+Out, OSPF	None
	OSPF Area ID	Specify OSPF area ID number	IPv4 format or digit string (Max 9 bits)	
PPP over Ethernet	Default WAN link (Gateway/DNS)	When Default WAN link is enabled. All the packets sent out from MH-5001 will be via this port.	Enable/Disable	Enabled
	Service Name	ISP vendor (Optional)	text string	So-Net
	User Name	The user name of PPPoE account	text string	Hey
	Password	The password of PPPoE account	text string	G54688
	Get DNS Automatically / DNS IP Address	Get DNS Automatically → Get DNS related information from PPPoE ISP DNS IP Address → manually specify these Primary and Secondary DNS Server information	Get DNS Automatically / DNS IP Address	Get DNS Automatically

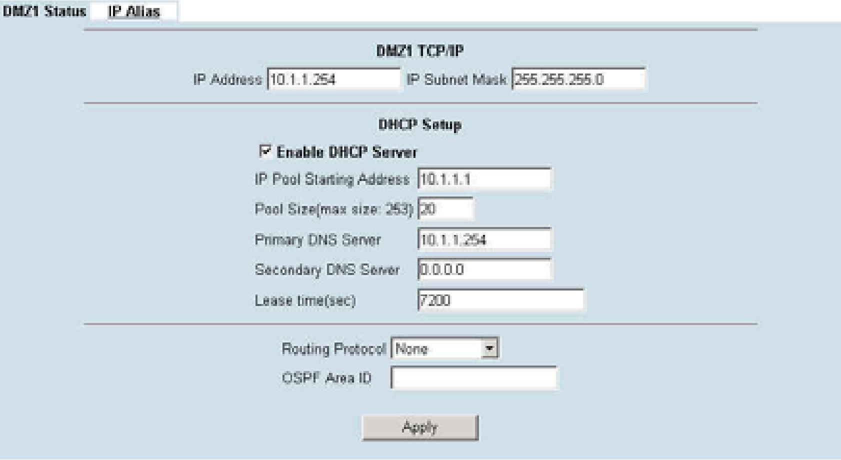
Table 3-1 Detailed information of setup WAN port configuration

3.4.2 Setup DMZ1, LAN1 Status

Step 1. Setup DMZ port

Here we are going to configure the DMZ1 settings. Setup `IP Address` and `IP Subnet Mask`, and determine if you would like to `enable the DHCP Server`. And then select Routing Protocol. Click `Apply` to finish this setting.

BASIC SETUP > DMZ Settings > DMZ1 Status



DMZ1 TCP/IP

IP Address 10.1.1.254 IP Subnet Mask 255.255.255.0

DHCP Setup

☑ Enable DHCP Server

IP Pool Starting Address 10.1.1.1

Pool Size(max size: 253) 20

Primary DNS Server 10.1.1.254

Secondary DNS Server 0.0.0.0

Lease time(sec) 7200

Routing Protocol None

OSPF Area ID

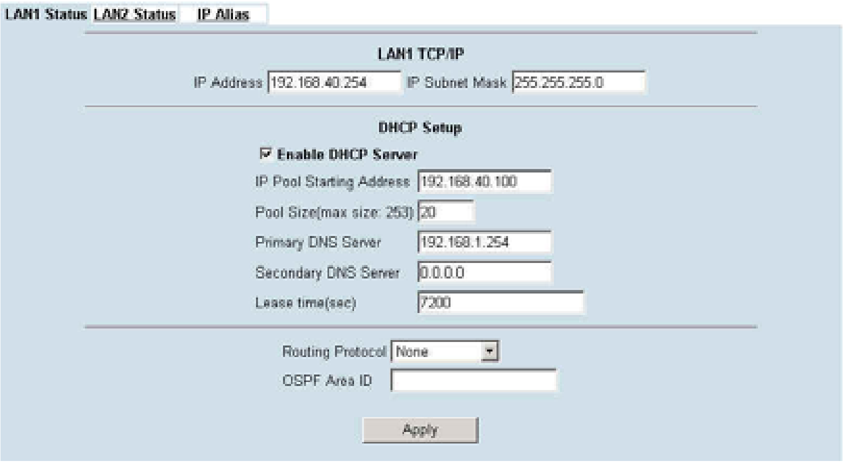
FIELD	DESCRIPTION	Range / Format	EXAMPLE
IP Address	DMZ port IP address	IPv4 format	10.1.1.254
IP Subnet Mask	DMZ port IP subnet mask	netmask format	255.255.255.0
Enable DHCP Server	Enable DMZ port of the DHCP Sever or not	Enable/Disable	Enabled
IP Pool Starting Address	Specify the starting address of the DHCP IP address.	IPv4 format in the DMZ address range	10.1.1.1
Pool Size(max size: 253)	Specify the numbers of the DHCP IP address.	1 ~253	20
Primary DNS Server	Specify the Primary DNS Server IP address of the DHCP information.	IPv4 format	10.1.1.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP information.	IPv4 format	0.0.0.0
Lease time(sec)	Specify DHCP information lease time	greater than 0	7200
Routing Protocol	Determine to enable the dynamic routing protocol (RIP), to receive RIP message, to send out RIP message if the message is received or not.	None / RIPv1In / RIPv1In+out / RIPv2In / RIPv2In+out / OSPF	None
OSPF Area ID	Specify OSPF area ID number	IPv4 format or digit string (Max 9 bits)	N/A

Table 3-2 Configure DMZ network settings

Step 2. Setup LAN port

Here we are going to configure the LAN1 settings. Setup IP Address and IP Subnet Mask, and determine if you would like to enable the DHCP Server. And then select Routing Protocol. Click `Apply` to finish this setting.

BASIC SETUP > LAN Settings > LAN1 Status



LAN1 TCP/IP

IP Address 192.168.40.254 IP Subnet Mask 255.255.255.0

DHCP Setup

☑ Enable DHCP Server

IP Pool Starting Address 192.168.40.100

Pool Size(max size: 253) 20

Primary DNS Server 192.168.1.254

Secondary DNS Server 0.0.0.0

Lease time(sec) 7200

Routing Protocol None

OSPF Area ID

FIELD	DESCRIPTION	Range / Format	EXAMPLE
IP Address	LAN1 port IP address	IPv4 format	192.168.40.254
IP Subnet Mask	LAN1 port IP subnet mask	netmask format	255.255.255.0
Enable DHCP Server	Enable LAN1 port of the DHCP Sever or not	Enable/Disable	Enabled

IP Pool Starting Address	Specify the starting address of the DHCP IP address.	IPv4 format in the LAN1 address range	192.168.40.100
Pool Size(max size: 253)	Specify the numbers of the DHCP IP address.	1 ~253	20
Primary DNS Server	Specify the Primary DNS Server IP address of the DHCP information.	IPv4 format	192.168.40.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP information.	IPv4 format	0.0.0.0
Lease time(sec)	Specify DHCP information lease time	greater than 0	7200
Routing Protocol	Determine to enable the dynamic routing protocol (RIP), to receive RIP message, to send out RIP message if the message is received or not.	None / RIPv1In / RIPv1In+out / RIPv2In / RIPv2In+out / OSPF	None
OSPF Area ID	Specify OSPF area ID number	IPv4 format or digit string (Max 9 bits)	N/A

Table 3-3 Configure LAN network settings

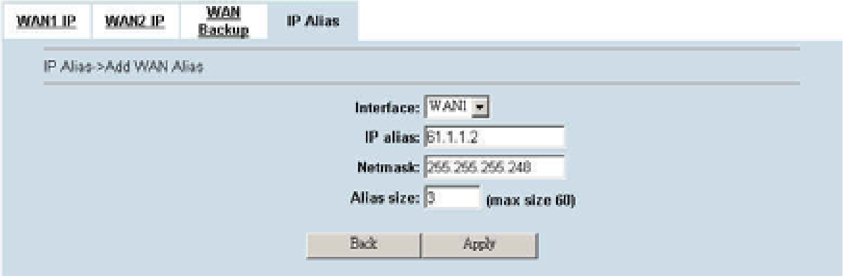
3.4.3 Setup WAN1 IP alias

Step 1. Add WAN1 IP alias

Suppose you apply 8 IP addresses from ISP. The range of the ISP-given IP address is from 61.2.1.0 to 61.2.1.7. Now you would like to add three WAN1 IP aliases. Select WAN1 in the Interface field. Enter the IP alias and Netmask with 61.2.1.2/255.255.255.248. Key in 3 into the Alias size field. And then click Apply.

Notice : It's the same way to set IP alias in DMZ or LAN.

BASIC SETUP > WAN Settings > IP Alias > Add



IP Alias->Add WAN Alias

Interface: WAN1

IP alias: 61.1.1.2

Netmask: 255.255.255.248

Alias size: 3 (max size 60)

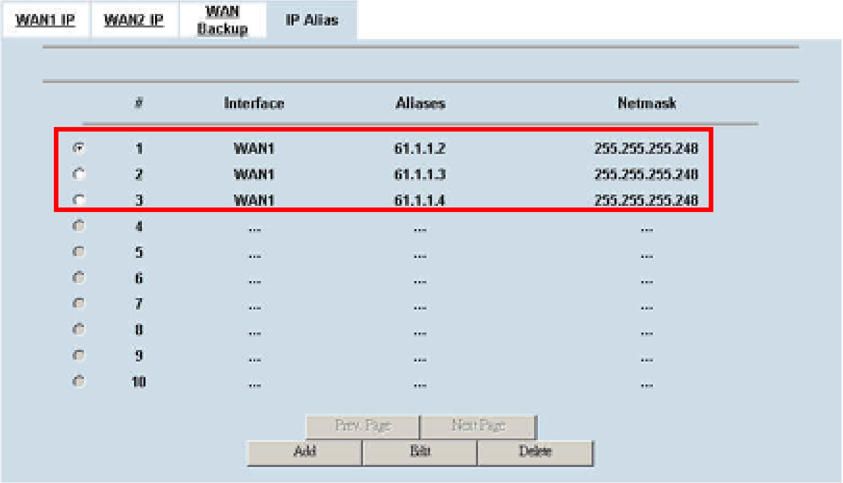
FIELD	DESCRIPTION	Range / Format	EXAMPLE
Interface	The interface which we set for the IP alias	WAN interfaces	WAN1
IP alias	The alias IP address	IPv4 format	61.2.1.2
Netmask	The netmask of the IP alias	netmask format	255.255.255.248
Alias size	The size of IP alias address	Max 60	3

Table 3-4 Add a IP alias record

Step 2. Edit, Delete IP alias record

You can easily add, edit, or delete IP alias records by the Add, Edit, or Delete button.

BASIC SETUP > WAN Settings > IP Alias



	#	Interface	Aliases	Netmask
●	1	WAN1	61.1.1.2	255.255.255.248
○	2	WAN1	61.1.1.3	255.255.255.248
○	3	WAN1	61.1.1.4	255.255.255.248
○	4	...	...	...
○	5	...	...	...
○	6	...	...	...
○	7	...	...	...
○	8	...	...	...
○	9	...	...	...
○	10	...	...	...

Maximize IP alias records of MH-5001	WAN port	60 records
	DMZ port	10 records
	LAN port	10 records

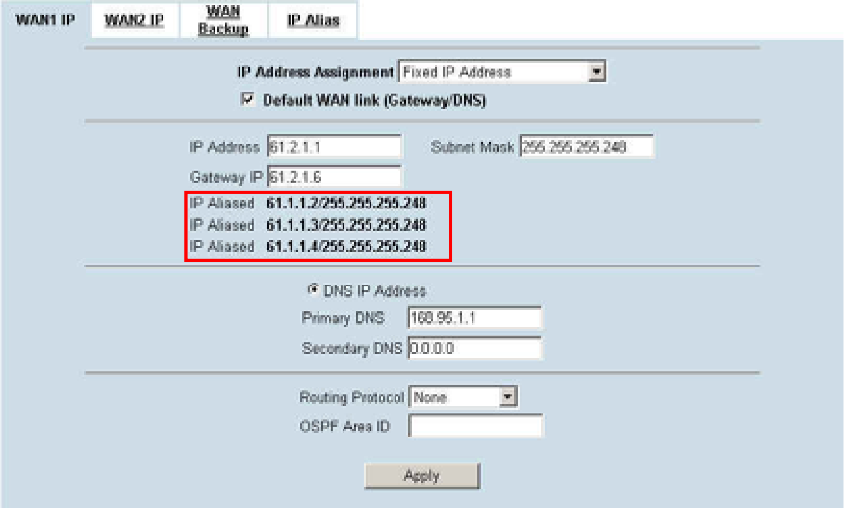
Table 3-5 IP alias limitation of each port

Step 3. See the IP alias setting in the "WAN1 IP" page

After entering the IP alias address, it will show the result in the "WAN1 IP" page.

Warning: If you select Fixed IP Address as your WAN link type and set any IP alias. When you try to exchange the WAN link type to other type such as DHCP, PPPoE. The previous setting IP aliases will disappear after you apply the new WAN link setting.

BASIC SETUP > WAN Settings > WAN1 IP > Fixed IP Address



IP Address Assignment: Fixed IP Address

☑ Default WAN link (Gateway/DNS)

IP Address: 61.2.1.1   Subnet Mask: 255.255.255.248

Gateway IP: 61.2.1.6

IP Aliased 61.1.1.2/255.255.255.248

IP Aliased 61.1.1.3/255.255.255.248

IP Aliased 61.1.1.4/255.255.255.248

● DNS IP Address

Primary DNS: 168.95.1.1

Secondary DNS: 0.0.0.0

Routing Protocol: None

OSPF Area ID:

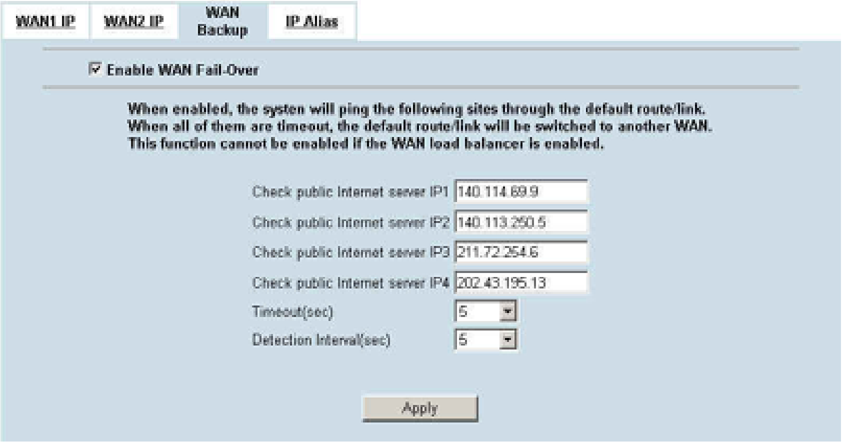
3.4.4 Setup WAN Backup

Step 4. Set public Internet server IP

Specify public Internet server IPs for system to ping in order for you to make sure the connection of the default WAN link. Setup the time to ping per IP address and to the detection Interval. If the first specified IP address fails to ping, the system will jump to the second specified IP to continue the ping action after the specified time. When all of them are timeout, the default route/link will be switched to another WAN link to continue the ping action within the specified Detection Interval.

Note that WAN Backup cannot be enabled with WAN Load Balancer at the same time. You can only enable either WAN Backup or WAN Load Balancer per time.

BASIC SETUP > WAN Settings > WAN Backup



☑ Enable WAN Fail-Over

When enabled, the systen will ping the following sites through the default route/link.
When all of them are timeout, the default route/link will be switched to another WAN.
This function cannot be enabled if the WAN load balancer is enabled.

Check public Internet server IP1 140.114.69.9
Check public Internet server IP2 140.113.250.5
Check public Internet server IP3 211.72.254.6
Check public Internet server IP4 202.43.195.13
Timeout(sec) 5
Detection Interval(sec) 5

FIELD	DESCRIPTION	RANGE/FORMAT	EXAMPLE
Enable WAN Fail-Over	When enabled, the system will ping the specified public server IP addresses through the default route/link.	Enable/Disable	Enable
Check public Internet server IP1	The first Internet public IP address used to check the connection of the current default WAN link.	IPv4 Format	140.114.69.9
Check public Internet server IP2	The second Internet public IP address used to check the connection of the current default WAN link.	IPv4 Format	140.113.250.5
Check public Internet server IP3	The third Internet public IP address used to check the connection of the current default WAN link.	IPv4 Format	211.72.254.6
Check public Internet server IP4	The fourth Internet public IP address used to check the connection of the current default WAN link.	IPv4 Format	202.43.195.13
Timeout (sec)	The time to ping the current public Internet Server IP.	Sec: 5,10,30,60,300,600	5
Detection Interval (sec)	The time to switch to detect the next WAN link when the default WAN link is disconnected.	Sec: 5,10,20,30,60	5

Table 3-6 WAN Backup Example

Chapter 4
System Tools

This chapter introduces System Management and explains how to implement it.

4.1 Demands

1. Basic configurations for domain name, password, system time, timeout and services.
2. DDNS: Suppose the MH-5001's WAN uses dynamic IP but needs a fixed host name. When the IP is changed, it is necessary to have the DNS record updated accordingly. To use this service, one has to register the account, password, and the wanted host name with the service provider.
3. DNS Proxy: Shorten the time of DNS lookup performed by applications.
4. DHCP Relay: It is to solve the problem that when the DHCP client is not in the same domain with the DHCP server, the DHCP broadcast will not be received by the server. If the client is in the LAN (192.168.40.X) while the server is located in the DMZ (10.1.1.4), the server will not receive any broadcast packet from the client.
5. The System Administrator would like to monitor the device from remote side efficiently.
6. Suppose our company applies three ISPs, but there are just two default WAN ports in the MH-5001. You hope to connect the whole ISP links to the MH-5001.

4.2 Objectives

1. Configure the general properties, such as domain name, password, system time, and connection timeout correctly. Besides, we can configure the prefered service name as the service name/numeric mapping list.
2. DDNS: By using the DDNS (Dynamic DNS), the MH-5001 will send the request for modification of the corresponding DNS record to the DDNS server after the IP is changed.
3. DNS Proxy: Reduce the number of DNS requests and the time for DNS lookup.
4. DHCP Relay: Enable the DHCP client to contact with the DHCP server located in different domain and get the required IP.
5. Through the SNMP manager, we can easily monitor the device status.
6. We hope to customize the interface of MH-5001 to fit our requests.

4.3 Methods

1. Configure the domain name, password, system time, connection timeout and service name.
2. DDNS: Configure the MH-5001 so that whenever the IP of the MH-5001 is changed, it will send requests to the DDNS server to refresh the DNS record. As the following Figure 4-1 demonstrated, the original WALL-1 has registered WAN1 IP address "61.2.1.1" on the DDNS server (www.dyndns.org). It's domain name address is "me.dyndns.org". If the WAN1 IP address is reassigned by the ISP. WALL-1 will update the registered IP address "61.2.1.1" as the assigned one. This is the base mechanism of the DDNS.

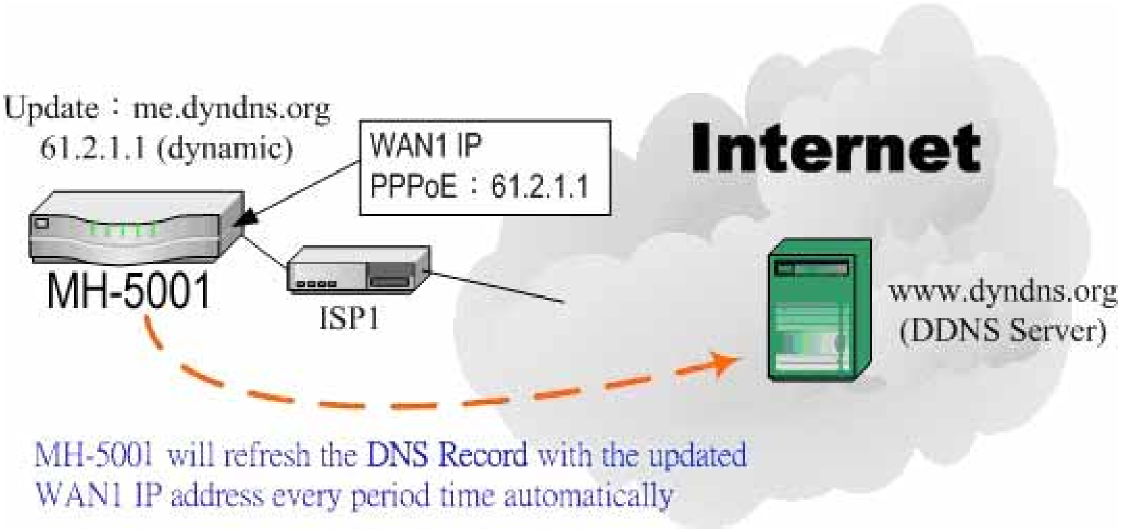


Figure 4-1 DDNS mechanism chart

3. DNS Proxy: After activating the DNS proxy mode, the client can set its DNS server to the MH-5001 (that is, send the DNS requests to the MH-5001). The MH-5001 will then make the enquiry to the DNS server and return the result to the client. Besides, the caching mechanism performed by the DNS proxy can also help reduce possible duplicate DNS lookups. As the following Figure 4-2 described. WALL-1 redirects the DNS request from PC1_1 to the real DNS server (140.113.1.1).

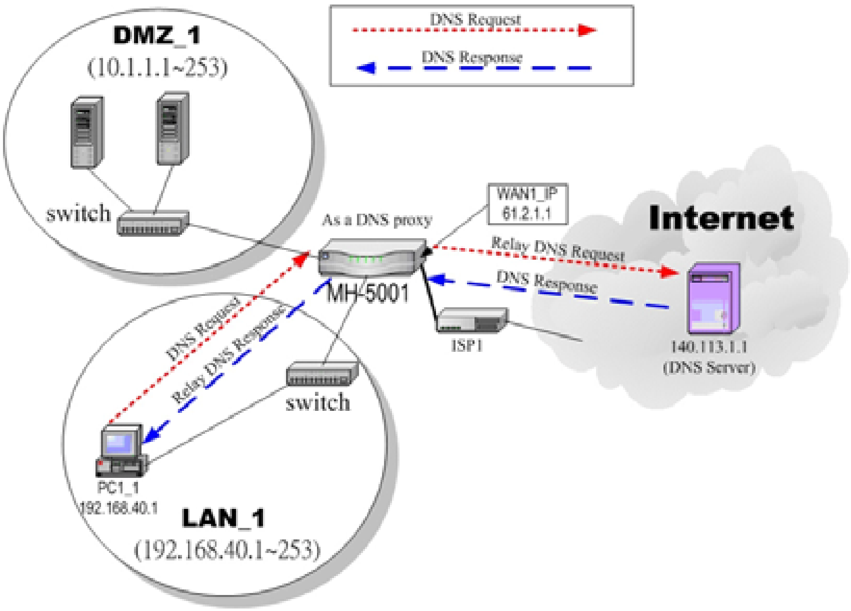


Figure 4-2 DNS Proxy mechanism chart

4. DHCP Relay: Activate the DHCP relay mode of MH-5001 so that the MH-5001 will become the relay agent and relay the DHCP broadcast to the configured DHCP server. As the following Figure 4-3 described, MH-5001 redirects the DHCP request from the preconfigured port (LAN1) to the real DHCP server (10.1.1.4). Besides, in this diagram, we can find that the PC of DMZ region communicated with the DHCP server directly.

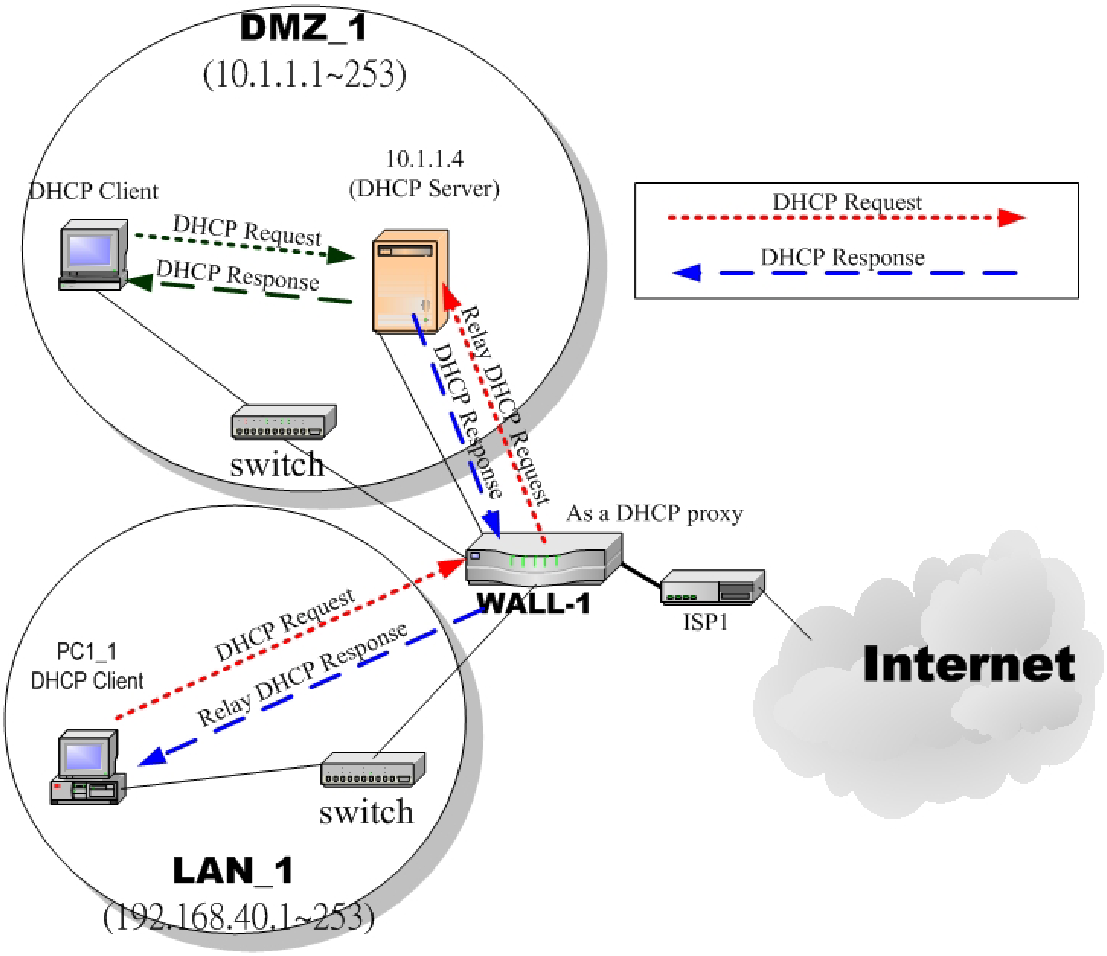


Figure 4-3 DHCP Relay mechanism chart

5. As the following Figure 4-4 demonstrated, there is an embedded snmp agent in the MH-5001. So you can use SNMP manager to monitor the MH-5001 system status, network status ,etc. from either LAN or Internet.

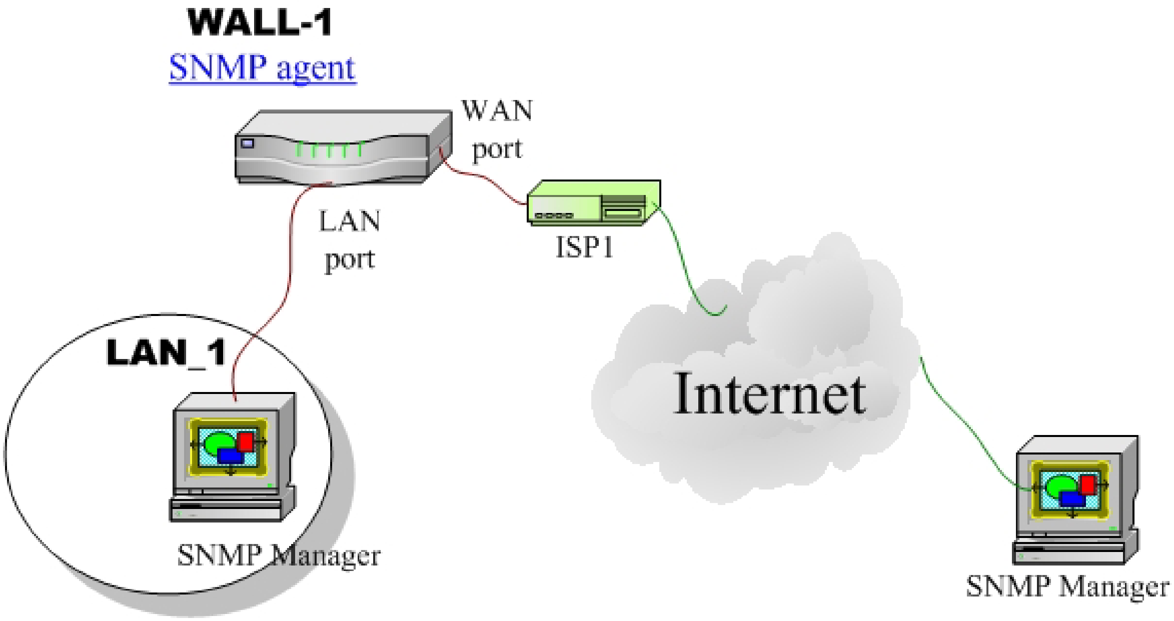


Figure 4-4 It is efficient to use SNMP Manager to monitor MH-5001 device

6. We can adjust the MH-5001 interface in the SYSTEM TOOLS > Admin Settings > Interface in according to our preference and requirement (3 WAN, 1 DMZ, 1 LAN). As the following Figure 4-5 demonstrated, there are three ISP connected onto MH-5001. So we must adjust the interface up to 3 WAN ports to fit the current condition.

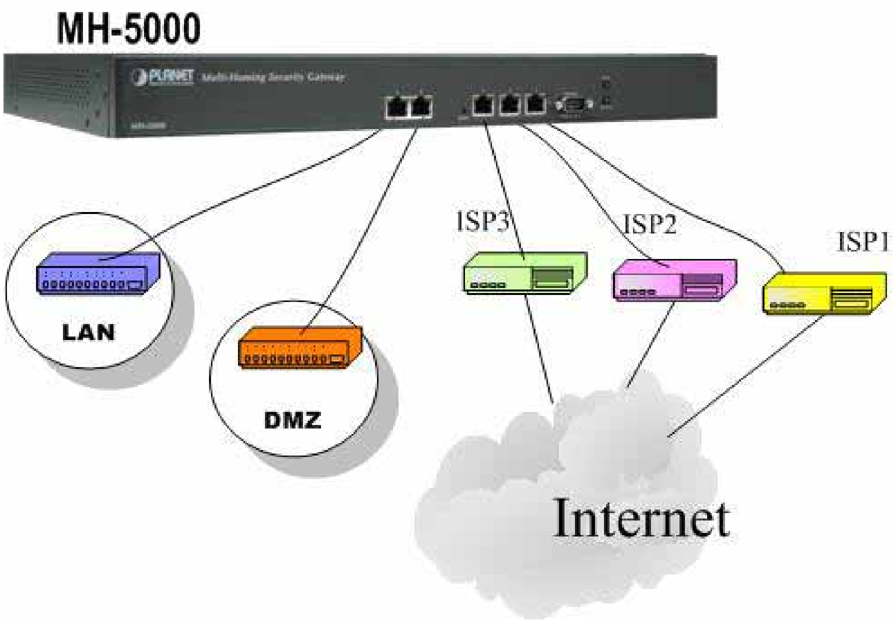


Figure 4-5 Adjust MH-5001 interface to fit current condition

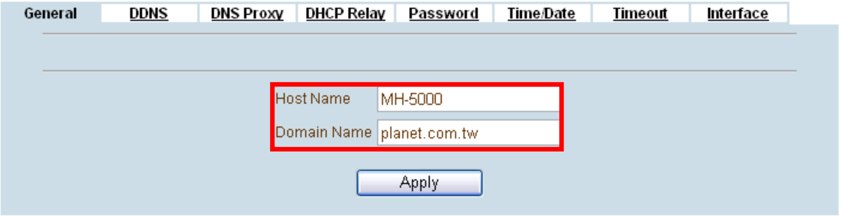
4.4 Steps

4.4.1 General settings

Step 1. General Setup

Enter the `Host Name` as `MH-5000`, `Domain Name` as the domain name of your company Click `Apply`.

SYSTEM TOOLS > Admin Settings > General



Host Name: MH-5000

Domain Name: planet.com.tw

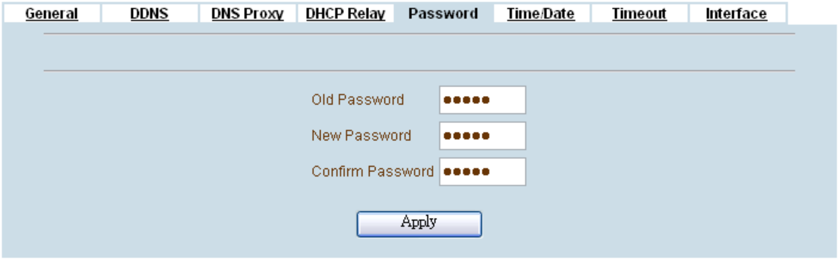
FIELD	DESCRIPTION	EXAMPLE
Host Name	The host name of the MH-5001 device	MH-5001
Domain Name	Fill in the domain name of company	planet.com.tw

Table 4-1 System Tools - General Setup menu

Step 2. Change Password

Enter the current password in the `Old Password` field. Enter the new password in the `New Password` and retype it in the `Confirm Password` field. Click `Apply`.

SYSTEM TOOLS > Admin Settings > Password



Old Password: ●●●●●

New Password: ●●●●●

Confirm Password: ●●●●●

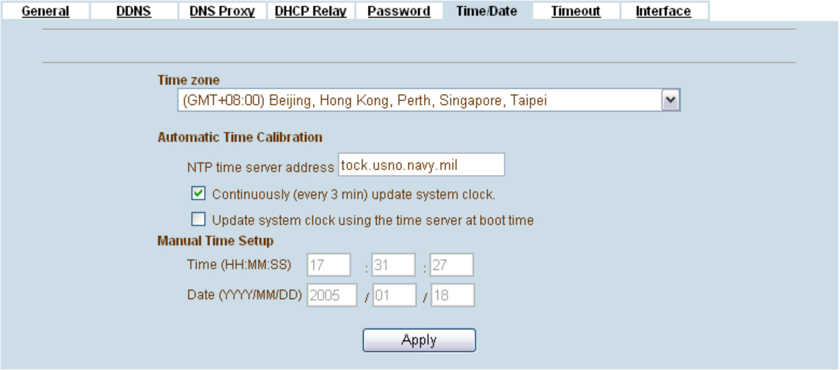
FIELD	DESCRIPTION	EXAMPLE
Old Password	The original password of administrator	admin
New Password	The new selected password	12345
Confirm Password	Double confirm the new selected password	12345

Table 4-2 Enter new password

Step 3. Setup Time/Date

Select the Time Zone where you are located. Enter the nearest NTP time server in the NTP time server address. Note that your DNS must be set if the entered address requires domain name lookup. You can also enter an IP address instead. Check the Continuously (every 3 min) update system clock and click Apply. The MH-5001 will immediately update the system time and will periodically update it. Check the Update system clock using the time server at boot time and click Apply if you want to update the clock at each boot. If you want to manually change the system time, uncheck the Continuously (every 3 min) update system clock and proceed by entering the target date.

SYSTEM TOOLS > Admin Settings > Time/Date



Time zone
(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

Automatic Time Calibration

NTP time server address: tock.usno.navy.mil

☑ Continuously (every 3 min) update system clock.

☐ Update system clock using the time server at boot time

Manual Time Setup

Time (HH:MM:SS) 17 : 31 : 27

Date (YYYY/MM/DD) 2005 / 01 / 18

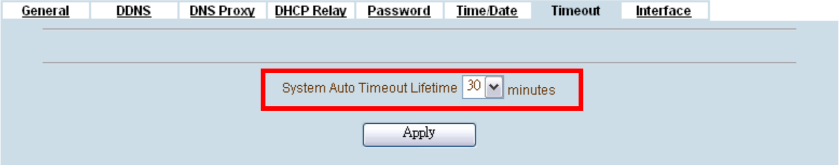
FIELD	DESCRIPTION	EXAMPLE
Time zone	the time zone of your area	N/A
NTP time server address	Use NTP time server to auto update date/time value	tock.usno.navy.mil
Continuously (every 3 min) update system clock	System will update system date/time value every 3 minutes to NTP time sever.	Enabled
Update system clock using the time server at boot time	System will update system date/time value to the NTP time server at boot time.	disabled
Manual Time Setup	Manual setting Time & Date value.	N/A

Table 4-3 System Tools – Time Data menu

Step 4. Setup Timeout

Select the target timeout (e.g. 30 min) from the System Auto Timeout Lifetime. Click the Apply button. Now the browser will not timeout for the following 10 minutes after your last touching of it.

SYSTEM TOOLS > Admin Settings > Timeout



System Auto Timeout Lifetime 30 minutes

FIELD	DESCRIPTION	EXAMPLE
System Auto Timeout Lifetime	When system is idle for a specified time, system will force the people who logins into the system will logout automatically.	30

Table 4-4 System Tools – Timeout menu

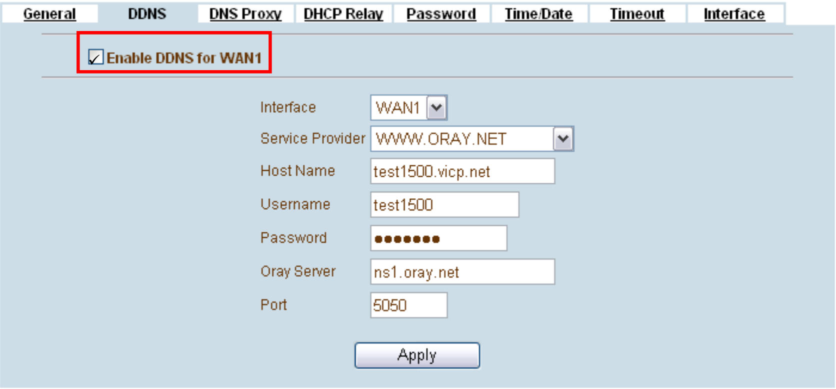
4.4.2 DDNS setting

Step 1. Setup DDNS

If the IP address of MH-5001 WAN port is dynamic allocated, you may want to have the Dynamic DNS mechanism to make your partner always use the same domain name (like xxx.com) to connect to you. Select a WAN `interface` to update the DDNS record. Here we supply three DDNS `Service Providers`. Fill in the `Host Name`, `Username`, `Password` supplied by the DDNS web site. Please refer to the DDNS web site for the detailed information. Click `Apply` to activate the settings.

Before setting the DDNS information in this page. Make sure that you have registered an account in the indicated Service Provider. Then you can enter the related information in the DDNS page.

SYSTEM TOOLS > Admin Settings > DDNS



☑ Enable DDNS for WAN1

Interface: WAN1
Service Provider: WWW.ORAY.NET
Host Name: test1500.vicp.net
Username: test1500
Password: ●●●●●●●
Oray Server: ns1.oray.net
Port: 5050

FIELD	DESCRIPTION	EXAMPLE
Enable DDNS for WAN1	Enable DDNS feature of MH-5001	Enabled
Interface	Assign which public IP address of interface to the DDNS server.	WAN1
Service Provide	The domain address of DDNS server. In the MH-5001, we provide some websites for your choice. If you choose WWW.ORAY.NET as DDNS service provider. It would register the source IP address which is connected to the DDNS server. It means that the WAN1 IP address must be public address.	WWW.ORAY.NET
Hostname	The registered Hostname in the DDNS server.	Test1500.vicp.net
Username	The registered username in the DDNS server.	Test1500
Password	The registered password in the DDNS server.	Wall500
Oray Server	The server which users can access its resources.	ns1.oray.net
Port	The default port number to connect to WWW.ORAY.NET for free charge.	5050

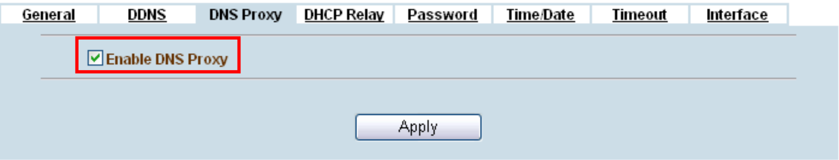
Table 4-5 System Tools – DDNS setting page

4.4.3 DNS Proxy setting

Step 1. Setup DNS Proxy

Check the `Enable DNS Proxy` and click the `Apply` to store the settings. From now on, your LAN/DMZ PCs can use MH-5001 as their DNS server, as long as the DNS server for MH-5001 has been set in its WAN settings.

SYSTEM TOOLS > Admin Settings > DNS Proxy



☑ Enable DNS Proxy

FIELD	DESCRIPTION	EXAMPLE
Enable DNS Proxy	When the host which resides at the LAN/DMZ region sends a DNS Request to the DNS server (MH-5001). MH-5001 will request for forwarding it to the assigned DNS server. When there is a response from assigned DNS server, then MH-5001 will forward it back to the host of the LAN/DMZ.	Enabled

Table 4-6 System Tools – DNS Proxy menu

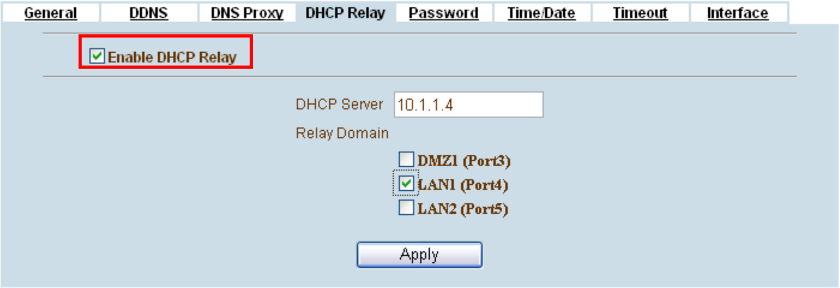
4.4.4 DHCP Relay setting

Step 1. Setup DHCP Relay

Check the `Enable DHCP Relay.` Enter the IP address of your `DHCP server`. Here we enter the DHCP Server address 10.1.1.4. Check the `relay domain` of MH-5001 that needs to be relayed. Namely, check the one where the DHCP clients are located. And click the `Apply` button finally.

Notice, the DHCP Server can not be located with the subnet range of `Relay Domain`.

SYSTEM TOOLS > Admin Settings > DHCP Relay



☑ Enable DHCP Relay

DHCP Server 10.1.1.4

Relay Domain

☐ DMZ1 (Port3)
☑ LAN1 (Port4)
☐ LAN2 (Port5)

FIELD	DESCRIPTION	EXAMPLE
Enable DHCP Relay	When the host of the LAN/DMZ in the MH-5001 internal network sends a DHCP request, MH-5001 will forward it automatically to the specified DHCP server (different subnet from the network segment of the DHCP client).	Enabled
DHCP Server	Current location of the DHCP server.	10.1.1.4
Relay Domain	The locations of the DHCP clients.	Enable LAN1

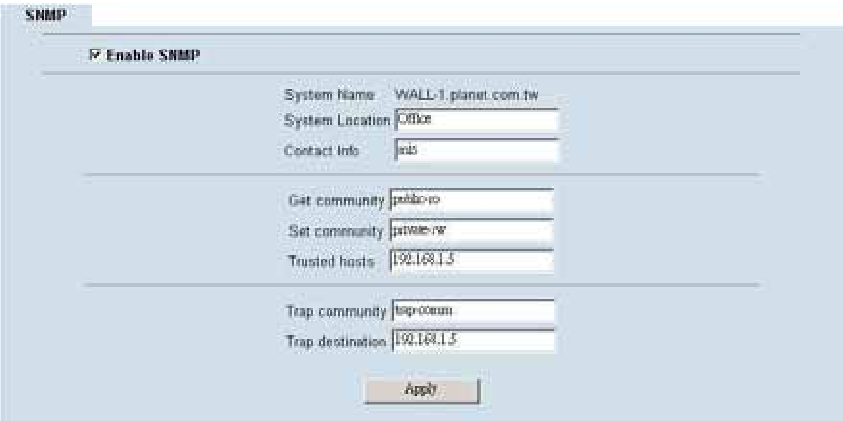
Table 4-7 System Tools – DHCP Relay menu

4.4.5 SNMP Control

Step 1. Setup SNMP Control

Through setting the related information in this page, we can use SNMP manager to monitor the system status, network status of MH-5001. Before that, please remember to enable the Remote management SNMP (SYSTEM TOOLS > Remote Mgt. > SNMP) first.

SYSTEM TOOLS > SNMP Control



☑ Enable SNMP

System Name WALL-1.planet.com.tw
System Location Office
Contact Info info

Get community public-ro
Set community private-rw
Trusted hosts 192.168.1.5

Trap community trap-comm
Trap destination 192.168.1.5

FIELD	DESCRIPTION	EXAMPLE
Enable SNMP	Enable the SNMP function or not.	Enabled
System Name	The device name of MH-5001.	MH-5001.planet.com.tw
System Location	The settled location of MH-5001.	Office
Contact Info	The person who takes charge of the MH-5001.	mis
Get community	The community which can get the SNMP information. Here “community” is something like password.	public-ro
Set Community	The community which can get the SNMP information. Here “community” is something like password.	private-rw
Trusted hosts	The IP address which can get or set community from the MH-5001.	192.168.1.5
Trap community	The community which will send SNMP trap. Here “community” is something like password.	trap-comm
Trap destination	The IP address which will send SNMP trap from the MH-5001.	192.168.1.5

Table 4-8 SNMP Settings

Step 2. MH-5001 traps

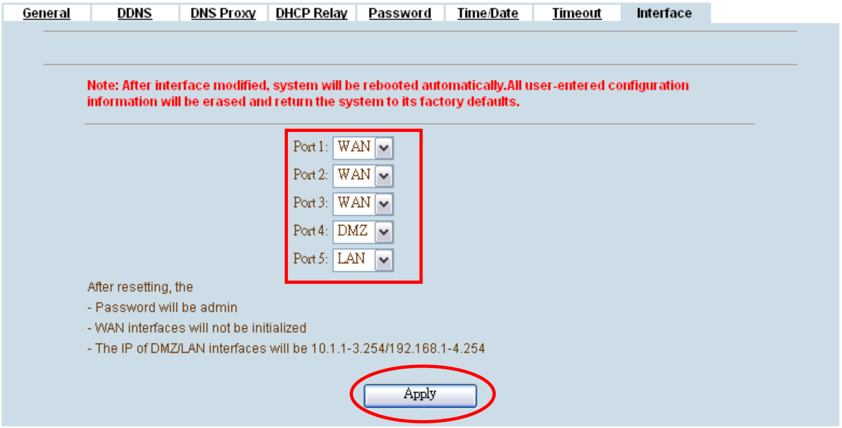
The MH-5001 agent can send traps to the SNMP trap receivers on your network that are configured to receive traps from the MH-5001 when rebooting. The MH-5001 agent sends traps in response to the events listed in SNMP traps.

4.4.6 Change MH-5001 interface

Step 1. Change Interface definition

The default port settings are 2 WAN ports, 1 DMZ port and 2 LAN ports. But in order to fit our requirement. Here we select 3 WAN (port1~3), 1 DMZ (port4), 1 LAN (port5). And then press apply button to reboot MH-5001. Note that the DMZ and LAN port IP addresses are going to be 10.1.1.254 and 192.168.1.254 after device finishes reboot. Besides, there should be at least one WAN port and one LAN port existing in the MH-5001. You are not allowed to casually change the interface to the state which has no LAN port or WAN port.

SYSTEM TOOLS > Admin Settings > Interface



Note: After interface modified, system will be rebooted automatically.All user-entered configuration information will be erased and return the system to its factory defaults.

Port 1: WAN
Port 2: WAN
Port 3: WAN
Port 4: DMZ
Port 5: LAN

After resetting, the
- Password will be admin
- WAN interfaces will not be initialized
- The IP of DMZ/LAN interfaces will be 10.1.1-3.254/192.168.1-4.254

FIELD	DESCRIPTION	EXAMPLE
Port1 ~ Port5	You can specify WAN / LAN / DMZ for each port by your preference. However, there must be one WAN and one LAN interface existing in the MH-5001.	Port1 : WAN Port2 : WAN Port3 : WAN Port4 : DMZ Port5 : LAN

Table 4-9 Change the MH-5001 interface setting

Chapter 5
Remote Management

This chapter introduces remote management and explains how to implement it.

5.1 Demands

Administrators may want to manage the MH-5001 remotely from any PC in LAN_1 with HTTP at port 8080, and from WAN_PC with TELNET. In addition, the MH-5001 may be more secure if monitored by a trusted host (PC1_1). What is more, the MH-5001 should not respond to ping to hide itself. The remote management function in MH-5001 devices is implemented by hidden Firewall rules.

5.2 Methods

1. Only allow management by WAN_PC (140.2.5.1) at the WAN1 side.
2. Administrators can use browsers to connect to http://192.168.40.254:8080 for management.
3. Allow SNMP monitoring by PC1_1 (192.168.40.1) at the LAN1 side.
4. Do not respond to ICMP ECHO packets at the WAN1 side.

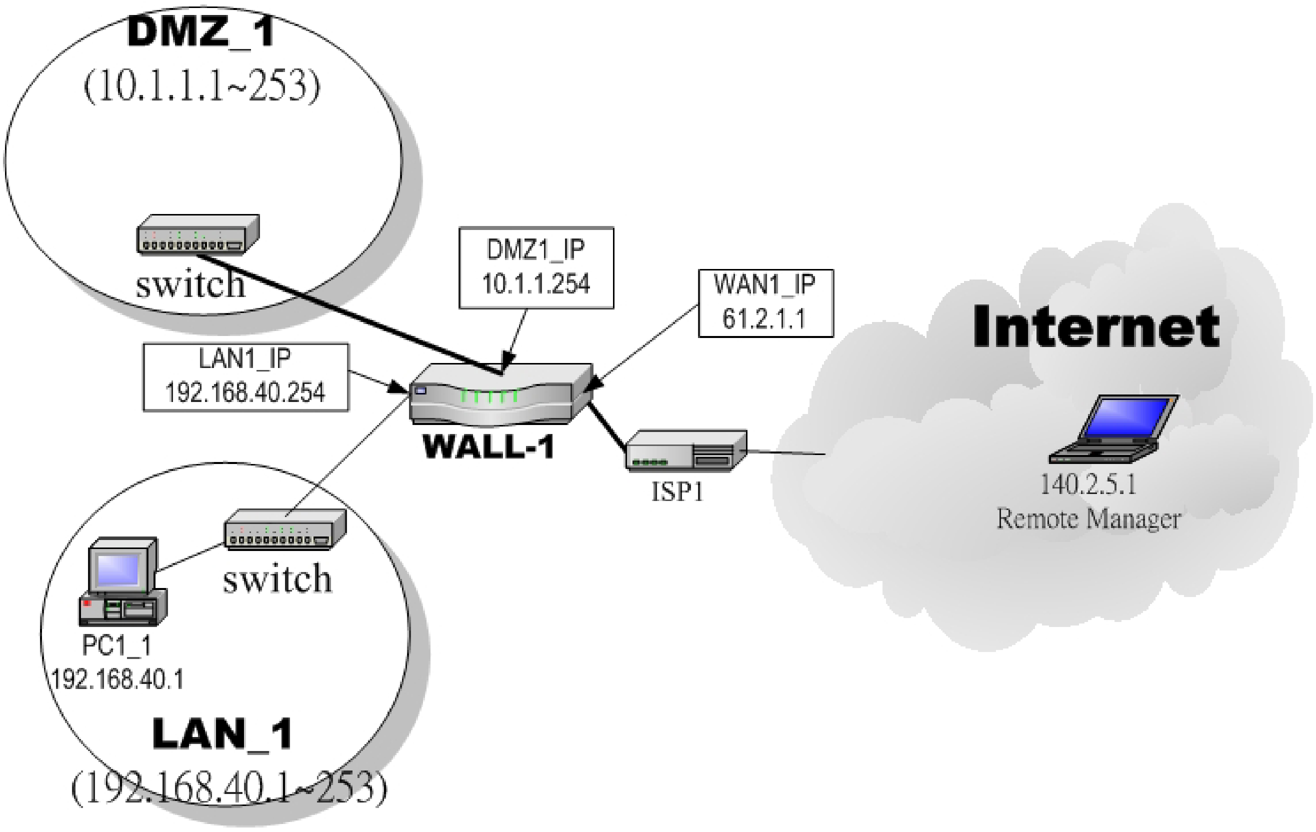


Figure 5-1 Some management methods of MH-5001

5.3 Remote Management Access Methods

Configuring management access for an interface connected to the Internet allows remote administration of the MH-5001 unit from any location on the Internet. Allowing management access from the Internet could compromise the security of your MH-5001 unit.

You should avoid allowing management access for an interface connected to the Internet unless this is required for your configuration. To improve the security of a MH-5001 unit that allows remote management from the Internet, add secure administrative user passwords, change these passwords regularly, and only enable secure management access using HTTPS or SSH.

Remote Management Access methods	Definition
Telnet	Telnet is a protocol for remote computing on the Internet. It allows a computer to act as a remote terminal on another machine, anywhere on the Internet. This means that when you telnet to a particular host and port, the remote computer (which must have a telnet server) accepts input directly from your computer (which must have a telnet client) and output for your session is directed to your screen. There are many library and information resources that are accessible through telnet.
SSH	Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. SSH uses RSA public key cryptography for both connection and authentication. Encryption algorithms include Blowfish, DES, and IDEA. IDEA is the default.
WWW	World Wide Web. Two meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers) which are the servers that allow text, graphics, sound files, etc. to be mixed together. WWW allows HTTP connections to the web-based manager through the selected interface. HTTP connections are not secure and can be intercepted by a third party.
HTTPS	HyperText Transfer Protocol Secure. A secure protocol for sending information back and forth over the Internet. The HTTPS protocol most frequently relies on the SSL (Secure Socket Layer) encryption system but others such as TLS (Transport layer security) are also available.
SNMP	Simple Network Management Protocol; a standard for gathering statistical data about network traffic and the behavior of network components; SNMP uses management information bases (MIBs), which define what information is available from any manageable network device
MISC	ICMP is an acronym for Internet Control Message Protocol. An ICMP is the standard error and control message protocol for Internet systems. The most well known use of ICMP messages is the Echo Request, Echo Reply sequence used by ping.

Table 5-1 Definition of the Remote Management Methods

The priority of the remote management methods to configure the MH-5001 is like the following order.

Console > SSH > Telnet > HTTPs > HTTP

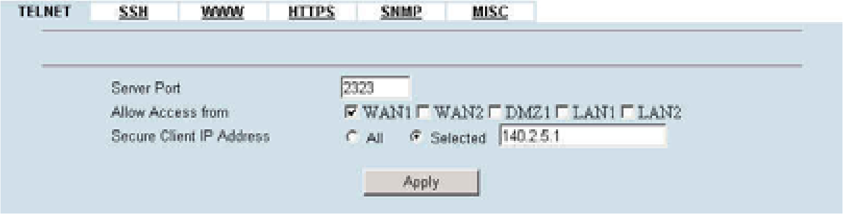
5.4 Steps

5.4.1 Telnet

Step 1. Setup Telnet

Enter 23 instead of the default 2323 in the `Server Port` field. Check the `WAN1` checkbox. Click the `Selected` of `Secure Client IP Address`, and then enter the specified `IP address` (`140.2.5.1`) for accessing MH-5001. And click the `Apply`.

SYSTEM TOOLS > Remote Mgt. > TELNET



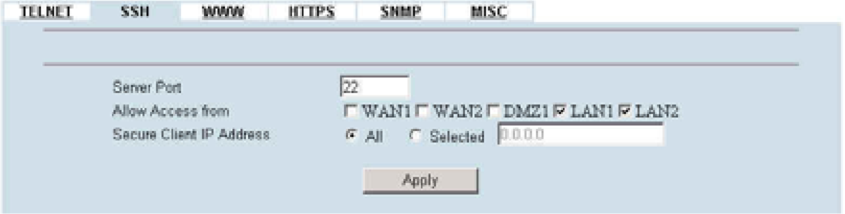
Server Port 2323
Allow Access from ☑ WAN1 □ WAN2 □ DMZ1 □ LAN1 □ LAN2
Secure Client IP Address ○ All ● Selected 140.2.5.1

5.4.2 SSH

Step 2. Setup SSH

Enter 22 in the `Server Port` field. Check the `LAN1/LAN2` checkbox. Click the `ALL` of `Secure Client IP Address` for accessing MH-5001. And click the `Apply`.

SYSTEM TOOLS > Remote Mgt. > SSH



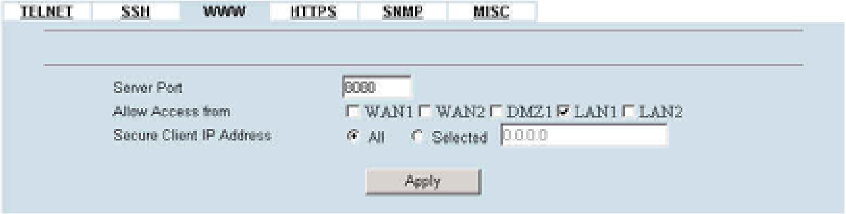
Server Port 22
Allow Access from □ WAN1 □ WAN2 □ DMZ1 ☑ LAN1 ☑ LAN2
Secure Client IP Address ● All ○ Selected 0.0.0.0

5.4.3 WWW

Step 1. Setup WWW

Check the `LAN1` checkbox, and enter the new `Server Port 8080` that will be accessed by the user's browser (http://192.168.40.254:8080). Here we click `All` for all no IP range limitation of clients. And click the `Apply` button.

SYSTEM TOOLS > Remote Mgt. > WWW



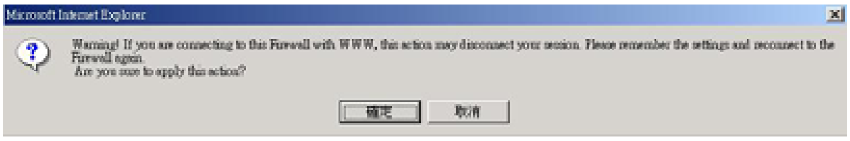
Server Port 8080
Allow Access from □ WAN1 □ WAN2 □ DMZ1 ☑ LAN1 □ LAN2
Secure Client IP Address ● All ○ Selected 0.0.0.0

Step 2. Message alert

If you select "Selected" and enter the IP address in the `Secure Client IP Address` field. After you apply the WWW, there will be a message to alert you that "`Warning! If you are connecting to this Firewall with WWW, this action may disconnect your session. Please remember the settings and reconnect to the Firewall again. Are you sure to apply this action?`"

Note, the `Secure Client IP Address` is the IP address which can be used to configure the MH-5001.

SYSTEM TOOLS > Remote Mgt. > WWW > Apply



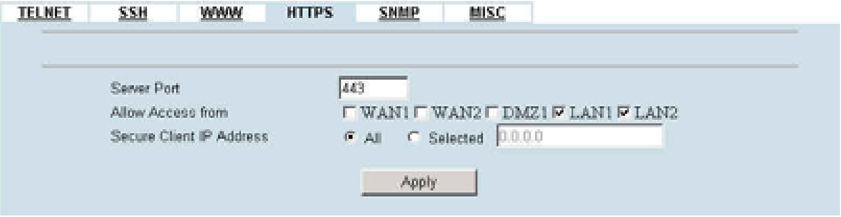
Warning! If you are connecting to this Firewall with WWW, this action may disconnect your session. Please remember the settings and reconnect to the Firewall again.
Are you sure to apply this action?

5.4.4 HTTPS

Step 3. Setup HTTPS

Check the LAN1/LAN2 checkbox, and enter the new Server Port 443 that will be accessed by the user's browser (https://192.168.40.254). Here we click All for all no IP range limitation of clients. And click the Apply button.

SYSTEM TOOLS > Remote Mgt. > HTTPS



Server Port 443

Allow Access from ☐ WAN1 ☐ WAN2 ☐ DMZ1 ☑ LAN1 ☑ LAN2

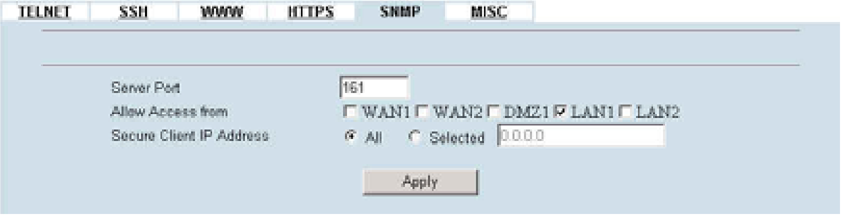
Secure Client IP Address ● All ○ Selected 0.0.0.0

5.4.5 SNMP

Step 1. Setup SNMP

Check the LAN1 checkbox. In the Secure Client Address field. If you prefer indicated specified IP address. Just click the Selected, and enter the valid IP address for reading the SNMP MIBs at the MH-5001. Finally click the Apply button.

SYSTEM TOOLS > Remote Mgt. > SNMP



Server Port 161

Allow Access from ☐ WAN1 ☐ WAN2 ☐ DMZ1 ☑ LAN1 ☐ LAN2

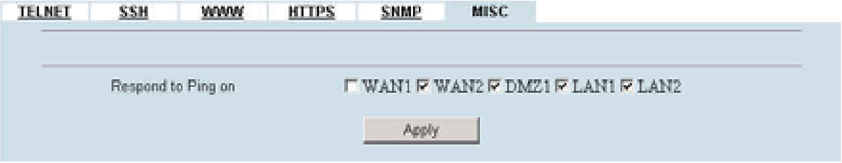
Secure Client IP Address ● All ○ Selected 0.0.0.0

5.4.6 ICMP

Step 1. Setup ICMP

Uncheck the WAN1 checkbox and make others checked. Then click the Apply button. For example, WAN1 IP is 61.2.1.1. When you make a command "ping 61.2.1.1", WAN1 will not respond to ICMP ECHO packets since you deactivate its ICMP function.

SYSTEM TOOLS > Remote Mgt. > MISC



Respond to Ping on ☐ WAN1 ☑ WAN2 ☑ DMZ1 ☑ LAN1 ☑ LAN2

Chapter 6
Authentication

This chapter introduces user authentication and explains how to implement it.

6.1 Demands

MH-5001 Multi-Homing Security Gateway supports user authentication against the internal user database, a RADIUS server or a LDAP server. You can create a user account by adding username and password to the internal database to grant the user an access to Internet, etc. Alternatively, you may input the IP address of a Radius server to let users to be authenticated using the server database.

6.2 Methods

To pass any of these authentications the user must use a browser. An authentication fail results to the complete inability to access both WAN and LAN resources. To avoid the authentication, there are two options: a) to route a service through DMZ interface, which is designed for this; or b) to add a chosen PC IP address to the Exempt Host list. For instance,

i. If PCs under LAN interfaces cannot pass the authentication, they will not be allowed to access WAN, LAN and DMZ resources.

ii. If PCs like servers are located under DMZ, the authentication is not necessary.

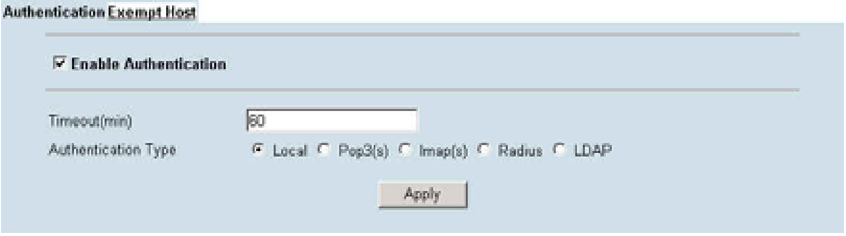
iii. If you put a server under LAN, you have to add its IP address to the Exempt Host list in order to access its resources.

There are four steps to configure the authentication:

1. Setting authentication timeout.
2. Configuring the Authentication Type.
3. Configuring the Authentication Setting.
4. Configuring the Exempt Host.

6.3 Steps

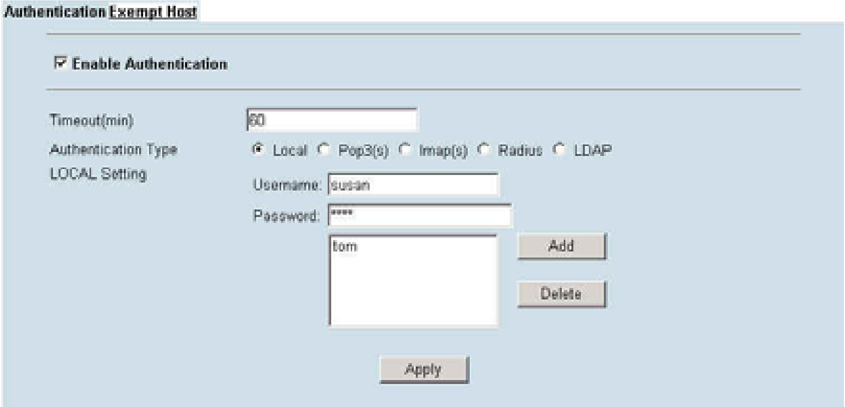
6.3.1 Local Setting

Step 2. Enable Authentication Check the `Enable Authentication` checkbox. Set Authentication timeout to control how long authenticated firewall connections are valid. Select the `Authentication Type`.	**Basic Setup > Authentication > Authentication**  ☑ Enable Authentication Timeout(min) 60 Authentication Type ● Local ○ Pop3(s) ○ Imap(s) ○ Radius ○ LDAP

Step 3. Configure Local Settings

Enter the `Username` and `Password`, and then click Add to add it to user's list. If you would like to delete a user, just click that username and then click Delete to remove it. Click `Apply` to finish the settings.

Basic Setup > Authentication > Authentication > Local



☑ Enable Authentication

Timeout(min): 60

Authentication Type: ● Local ○ Pop3(s) ○ Imap(s) ○ Radius ○ LDAP

LOCAL Setting

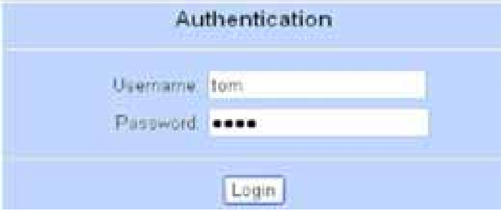
Username: susan

Password: ****

tom

Step 4. Show the Authentication

After applying Local setting, there will be an Authentication dialog to ask you to enter the `Username` and `Password` when you would like to connect to the Internet. And then click `Login`.

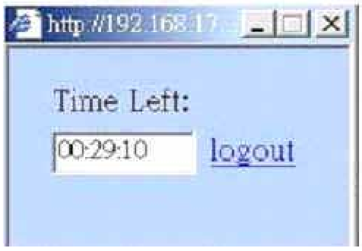


Username: tom

Password: ●●●●

Step 5. Show the time left

When you pass the authentication, a message box will appear to tell you how long the connection will remain.



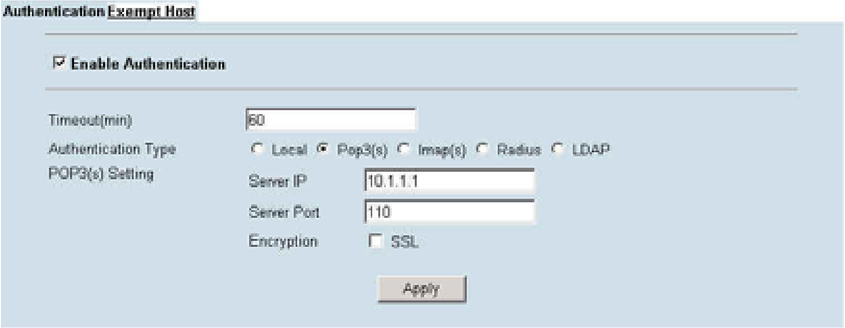
Time Left: 00:29:10

6.3.2 Pop3(s) Setting

Step 6. Configure Pop3(s) Settings

Click `Authentication Type` as `Pop3(s)`. Enter Server IP and Server Port. Check the Encryption as SSL if the server port is 995 (PoP3s). Click `Apply` to store the settings.

Basic Setup > Authentication > Authentication > Pop3(s)



☑ Enable Authentication

Timeout(min): 60

Authentication Type: ○ Local ● Pop3(s) ○ Imap(s) ○ Radius ○ LDAP

POP3(s) Setting

Server IP: 10.1.1.1

Server Port: 110

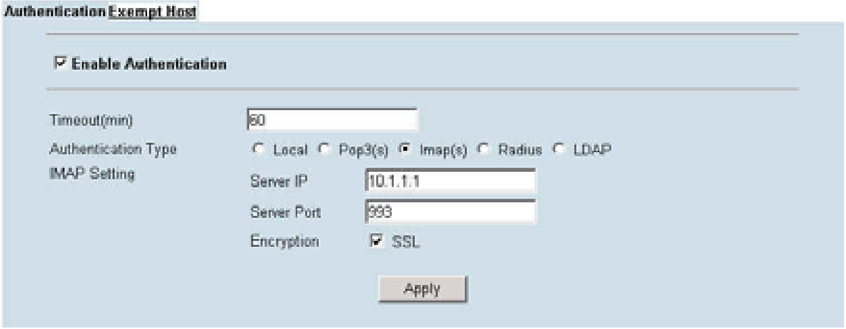
Encryption: □ SSL

FIELD	DESCRIPTION	EXAMPLE
Server IP	The IP address of the POP3(s) server.	10.1.1.1
Server Port	The port which the data goes into or out of the POP3(s) server. For instance, POP3 service uses port 110 and POP3s service uses port 995.	110

Encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. Secured Sockets Layer is a protocol that transmits your communications over the Internet in an encrypted form. It ensures that the information is sent, unchanged, only to the server you intended to send it to. Therefore, if you use port 995 (POP3s) as your server port, you have to check SSL checkbox.	

Table 6-1 POP3(s) Settings

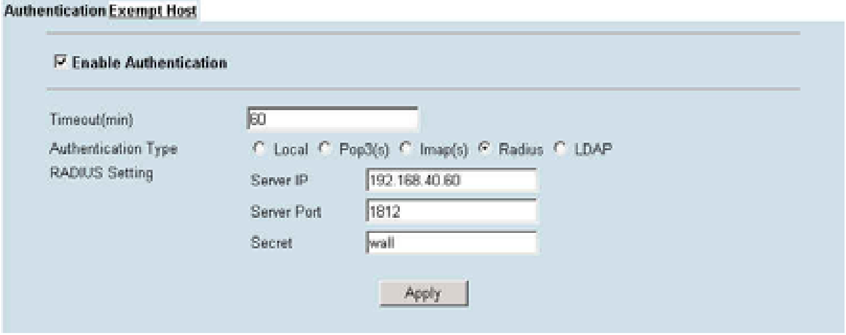
6.3.3 Imap(s) Setting

Step 7. Configure Imap(s) Settings	**Basic Setup > Authentication > Authentication > Imap(s)**
Click `Authentication Type` as `Imap(s)`. Enter Server IP and Server Port. Check the Encryption as `SSL.` Click `Apply` to store the settings. Note, if you enter server port as `143 (IMAP)`, don't check the SSL checkbox.	 Authentication Exempt Host ☑ Enable Authentication Timeout(min) 60 Authentication Type ○ Local ○ Pop3(s) ● Imap(s) ○ Radius ○ LDAP IMAP Setting Server IP 10.1.1.1 Server Port 993 Encryption ☑ SSL Apply

FIELD	DESCRIPTION	EXAMPLE
Server IP	The IP address of the IMAP(s) server.	10.1.1.1
Server Port	The port which the data goes into or out of the IMAP(s) server. For instance, IMAP service uses port 143 and IMAPs service uses port 993.	993
Encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. Secured Sockets Layer (SSL) is a protocol that transmits your communications over the Internet in an encrypted form. It ensures that the information is sent, unchanged, only to the server you intended to send it to. Therefore, if you use port 993 (IMAPs) as your server port, you have to check SSL checkbox.	SSL

Table 6-2 IMAP(s) Settings

6.3.4 Radius Setting

Step 8. Configure Radius Settings	**Basic Setup > Authentication > Authentication > Radius**
If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the MH-5001 then will contact the RADIUS server for authentication. Click `Authentication Type` as `Radius`. Enter `Server IP/Server Port` and enter the RADIUS Server `Secret`. Click `Apply` to store the settings.	 Authentication Exempt Host ☑ Enable Authentication Timeout(min) 60 Authentication Type ○ Local ○ Pop3(s) ○ Imap(s) ● Radius ○ LDAP RADIUS Setting Server IP 192.168.40.60 Server Port 1812 Secret wall Apply

FIELD	DESCRIPTION	EXAMPLE
Server IP	The IP address of the RADIUS server.	192.168.40.60
Server Port	The port which the data goes into or out of the RADIUS server.	1812
Secret	Secret is the encryption key used by RADIUS to send authentication information over a network.	wall

Table 6-3 RADIUS Settings

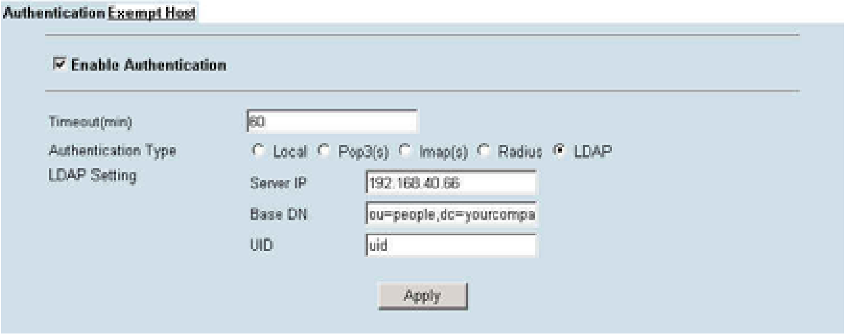
6.3.5 LDAP Setting

Step 9. Configure LDAP Settings

If you have configured LDAP support and a user is required to authenticate using a LDAP server, the MH-5001 will then contact the LDAP server for authentication. To authenticate with the MH-5001, the user enters a username and password. The MH-5001 sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the MH-5001.

Click `Authentication Type` as `LDAP`. Enter `LDAP Server IP` and then enter the distinguished name (`Base DN`) used to look up entries on the LDAP server. For example, you can use the Base DN like `ou=people, dc=yourcompany,dc=com`,`dc=tw` where ou is organization unit and dc is domain component. Enter the common name identifier in the `UID` field. Note that UID (it may be named as `cn`) is the field name in LDAP server. Please refer to Table 6-4 for details.

Basic Setup > Authentication > Authentication > LDAP



☑ Enable Authentication

Timeout(min) 60

Authentication Type ○ Local ○ Pop3(s) ○ Imap(s) ○ Radius ● LDAP

LDAP Setting
Server IP 192.168.40.66
Base DN ou=people,dc=yourcompa
UID uid

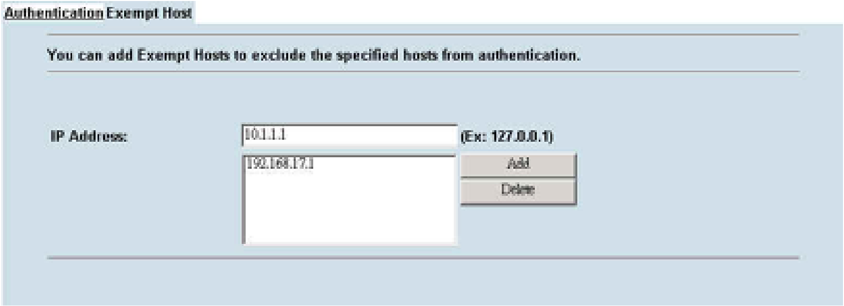
FIELD	DESCRIPTION	EXAMPLE
Server IP	The IP address of the LDAP server.	192.168.40.66

Base DN	The distinguished name used to look up entries on the LDAP server. For example:
	In OpenLDAP:
	entry1: uid=mary,ou=people,dc= yourcompay,dc=com
	entry2: uid=jack,ou=people,dc= yourcompay,dc=com
	Base DN: ou=people,dc=yourcompany,dc=com
	UID : uid
	In Windows AD (special case):
	entry1: cn=mary,dc= yourcompay,dc=com
	entry2: cn=jack ,dc= yourcompay,dc=com
	Base DN: cn=Users,dc=yourcompany,dc=com
	UID: cn
		ou=people,dc=yourcompany,
		dc=com,dc=tw

UID	UID is the field name and used to look up entries on LDAP server. Please refer to the above description.	uid

Table 6-4 LDAP Settings

6.3.6 Exempt Host

Step 10. Configuring the Exempt Host	**Basic Setup > Authentication > Exempt Host**
Enter the exempt host `IP Address`, and click `Add` to add an IP address. When enabling authentication, the chosen PC IP address will pass the authentication.	 Authentication Exempt Host You can add Exempt Hosts to exclude the specified hosts from authentication. IP Address: 10.1.1.1 (Ex: 127.0.0.1) 192.168.17.1 Add Delete

Chapter 7
NAT

This chapter introduces NAT and explains how to implement it in MH-5001.

To facilitate the explanation on how MH-5001 implements NAT and how to use it, we zoom in the left part of Figure 1- into Figure 7-1.

7.1 Demands

1. The number of public IP address allocated to each Internet subscribers is often very limited compared to the number of PCs in the LAN1. Additionally, public-IP hosts are directly exposed to the Internet and have more chances to be cracked by intruders. As the Figure 7-1 illustrated, you hope all the pcs located at LAN1 and DMZ1 can connect Internet through limited IP address (61.2.1.1).

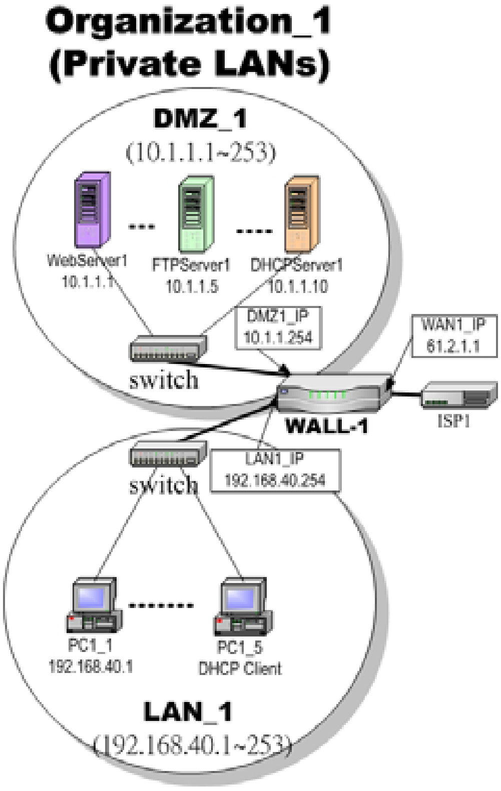


Figure 7-1 All the internal PCs can connect Internet through limited WAN IP address by using NAT technology

2. Internet servers provided by your company may open many ports in default that may be dangerous if exposed to the public Internet. As the Figure 7-2 illustrated, we make the real servers hide behind the Wall-1 - MH-5001. And all the Internet clients can still access the service of servers.

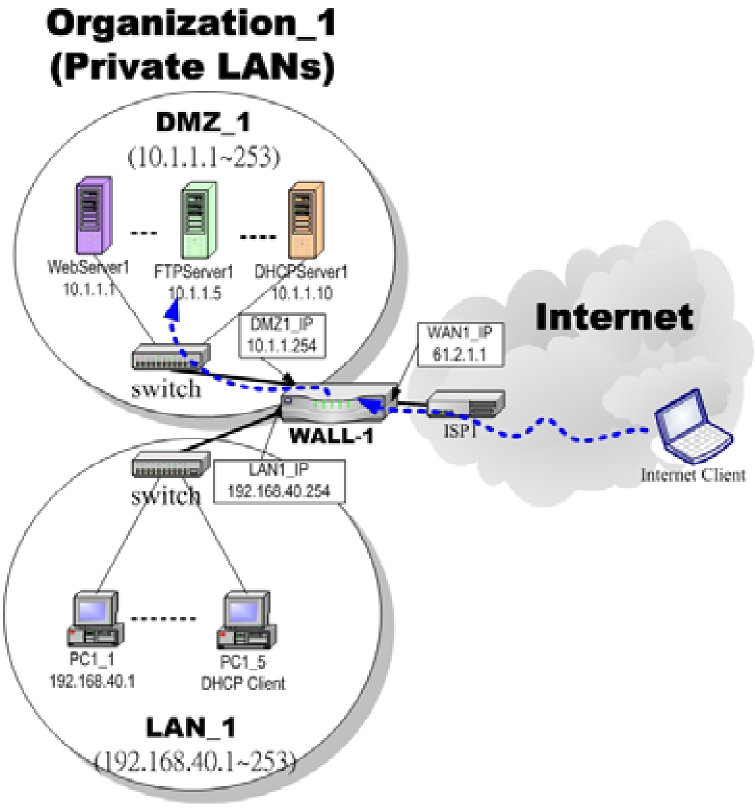


Figure 7-2 Internet clients can access the server behind the MH-5001

7.2 Objectives

1. Let PC1_1~PC1_5 connect to the Internet.
2. As the Figure 7-2 illustrated, the clients will connect to the MH-5001. Then MH-5001 will forward the packet to the real server. So FTPServer1 (10.1.1.5) will be accessed by other Internet users.

7.3 Methods

1. Assign private IP addresses to the PC1_1~PC1_5. Setup NAT at MH-5001 to map those assigned private hosts under LAN1 to the public IP address WAN_IP at the WAN1 side.
2. Assign a private IP address to the FTPServer1. Setup Virtual Server at MH-5001 to redirect “any connections towards some port of WAN1” to the port 21 at the FTPServer1.

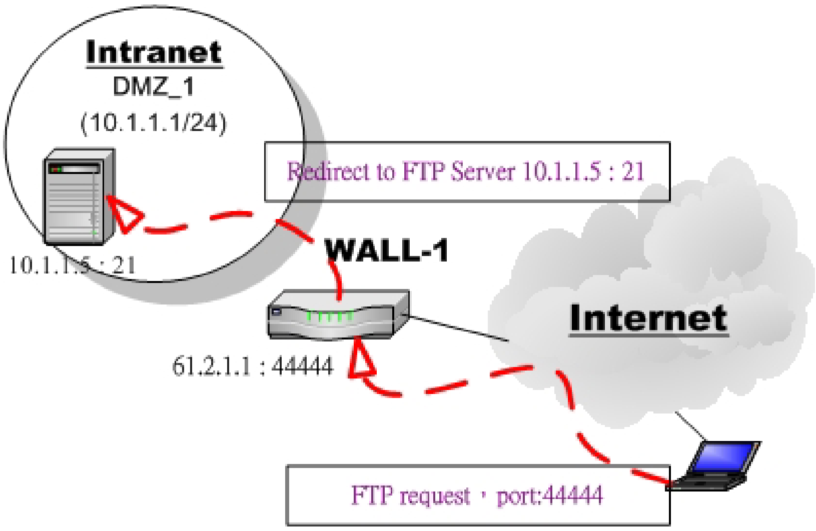


Figure 7-3 MH-5001 plays the role as Virtual Server

As the above Figure 7-3 illustrates, the server 10.1.1.5 provides FTP service. But it is located on the DMZ region behind WALL-1 - MH-5001. And MH-5001 will act as a Virtual Server role which redirects the packets to the real server 10.1.1.5. And you can announce to the Internet users that there exists a ftp server IP/port is 61.2.1.1/44444. So, all the Internet users will just connect the 61.2.1.1/44444 to get ftp service.

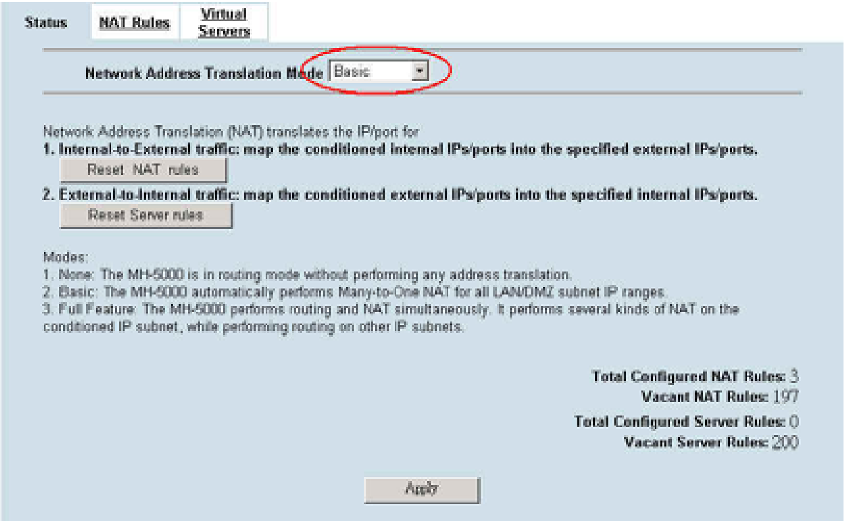
7.4 Steps

7.4.1 Setup Many-to-one NAT rules

Step 1. Enable NAT

Select the `Basic` from the list of `Network Address Translation Mode`. Click `Apply`. Now the MH-5001 will automatically set the NAT rules for LAN/DMZ zones. Namely, all internal networks can establish connections to the outside world if the WAN settings are correct.

ADVANCED SETTINGS > NAT > Status



Network Address Translation Mode: Basic

Network Address Translation (NAT) translates the IP/port for
1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.
2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.

Modes:
1. None: The MH-5000 is in routing mode without performing any address translation.
2. Basic: The MH-5000 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
3. Full Feature: The MH-5000 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

Total Configured NAT Rules: 3
Vacant NAT Rules: 197
Total Configured Server Rules: 0
Vacant Server Rules: 200

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Network Address Translation Mode	Determine what NAT type you are using in your network topology. Refer more information in the section 7.5.4.	None / Basic / Full Feature	Basic

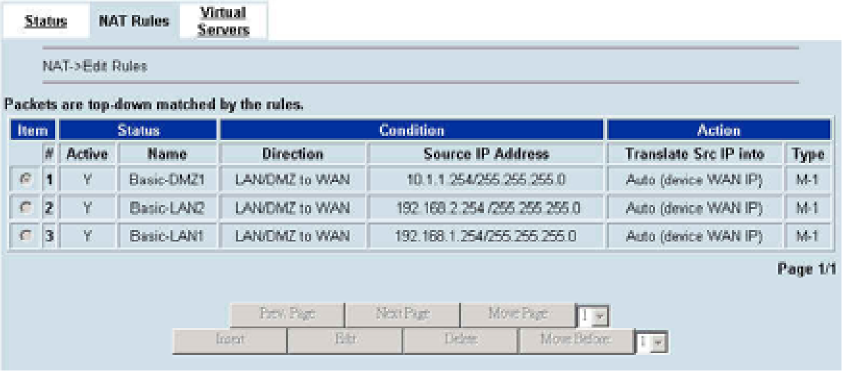
BUTTON	DESCRIPTION
Reset NAT Rules	Reset NAT rules to the default status
Reset Server Rules	Clear all the Virtual Server rules.
Clear active NAT/Server sessions	Clear all the active NAT/Virtual Server sessions.
Apply	Apply the settings which have been configured.

Table 7-1 Determine Network Address Translation Mode

Step 2. Check NAT Rules

As described in the above, the MH-5001 has set the rules for the `LAN/DMZ` zones. They all belong to the `Many-to-One` (`M-1`) type that will map many private addresses to the automatically chosen public IP address. When the WAN interfaces change the IP, these rules do not require any manual modifications for the changed public IP addresses. The rules will reload the new settings automatically. Besides, you cannot insert/edit any rules under the Basic mode.

ADVANCED SETTINGS > NAT > NAT Rules



NAT->Edit Rules

Packets are top-down matched by the rules.

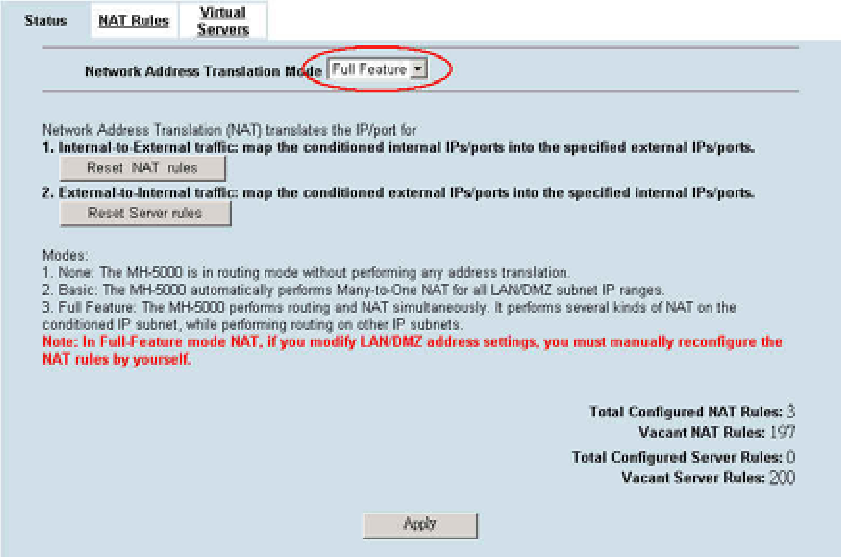
Item	Status			Condition		Action	
	#	Active	Name	Direction	Source IP Address	Translate Src IP into	Type
●	1	Y	Basic-DMZ1	LAN/DMZ to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1
○	2	Y	Basic-LAN2	LAN/DMZ to WAN	192.168.2.254 /255.255.255.0	Auto (device WAN IP)	M-1
○	3	Y	Basic-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M-1

Page 1/1

Step 3. Switch the NAT Mode

Select the `Full Feature` from the list of `Network Address Translation Mode`. Click `Apply`. After applying the setting, the page will highlight a warning saying that the rules are no more automatically maintained by the MH-5001. If you change the LAN/DMZ IP settings, you have to manually update related rules by yourself. Otherwise, hosts in your LAN/DMZ cannot establish connections to the hosts in the WAN side.

ADVANCED SETTINGS > NAT > Status



Network Address Translation Mode: Full Feature

Network Address Translation (NAT) translates the IP/port for

1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.

2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.

Modes:
1. None: The MH-5000 is in routing mode without performing any address translation.
2. Basic: The MH-5000 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
3. Full Feature: The MH-5000 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

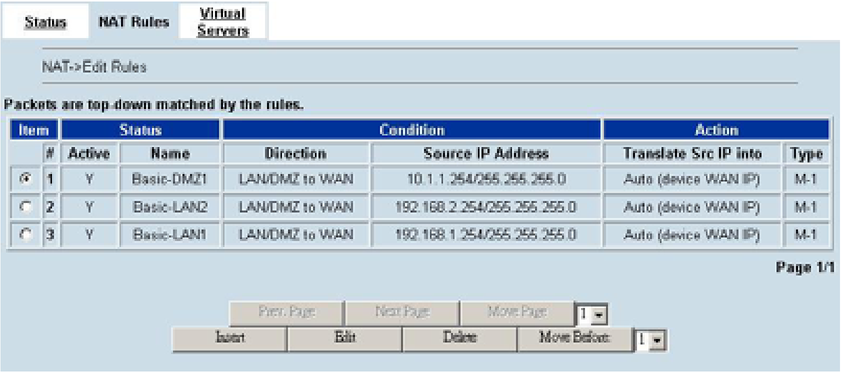
Note: In Full-Feature mode NAT, if you modify LAN/DMZ address settings, you must manually reconfigure the NAT rules by yourself.

Total Configured NAT Rules: 3
Vacant NAT Rules: 197
Total Configured Server Rules: 0
Vacant Server Rules: 200

Step 4. Customize NAT Rules

In the full-feature mode, the rules can be further customized. Incoming packets from LAN/DMZ zones are top-down matched by the NAT rules. Namely, NAT implements first match. Select the rule item that you want to do with: `insert` a new rule before it; `delete` it; `move` it `before` the list-box chosen item.

ADVANCED SETTINGS > NAT > NAT Rules



NAT->Edit Rules

Packets are top-down matched by the rules.

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Translate Src IP into	Type
●	1	Y	Basic-DMZ1	LAN/DMZ to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1
○	2	Y	Basic-LAN2	LAN/DMZ to WAN	192.168.2.254/255.255.255.0	Auto (device WAN IP)	M-1
○	3	Y	Basic-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M-1

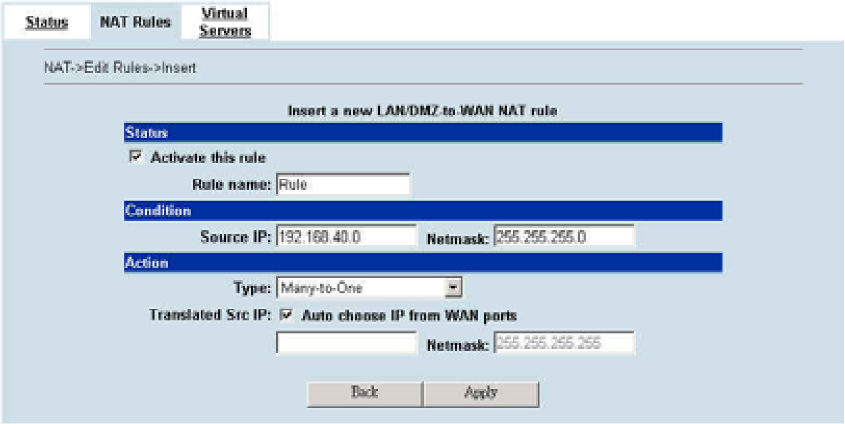
Page 1/1

Step 5. Insert NAT Rule

Step 5.a — Insert an Many-to-One Rule

As described in the above, `Many-to-One` NAT is the default NAT rule type in the `Basic` mode. If you have other alias LAN/DMZ subnets, you can manually add a Many-to-One NAT rule for them. First select the `Type` as Many-to-One, check the `Activate this rule`, enter a `Rule` name for this rule, enter the private-IP subnet (an `IP address` with a `netmask`) to be translated, and enter the public `IP address` for being translated into. You can check the `Auto choose IP from WAN ports`. The MH-5001 will automatically determine which WAN IP is to be translated into.

ADVANCED SETTINGS > NAT > NAT Rules > Insert



NAT->Edit Rules->Insert

Insert a new LAN/DMZ-to-WAN NAT rule

Status

☑ Activate this rule

Rule name: Rule

Condition

Source IP: 192.168.40.0 Netmask: 255.255.255.0

Action

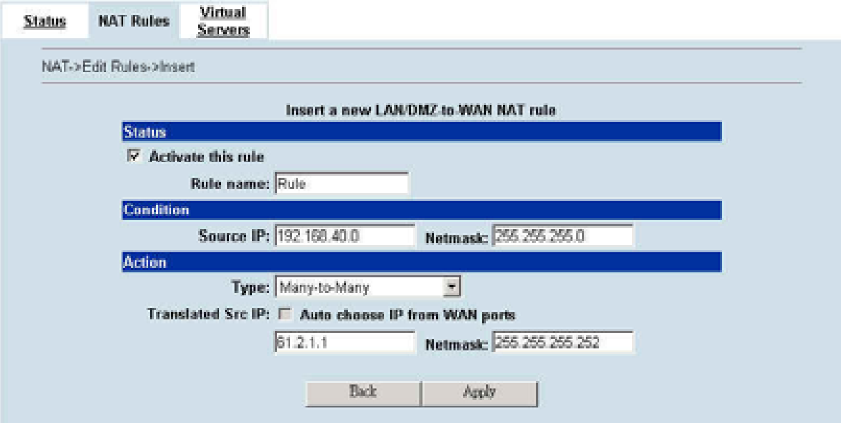
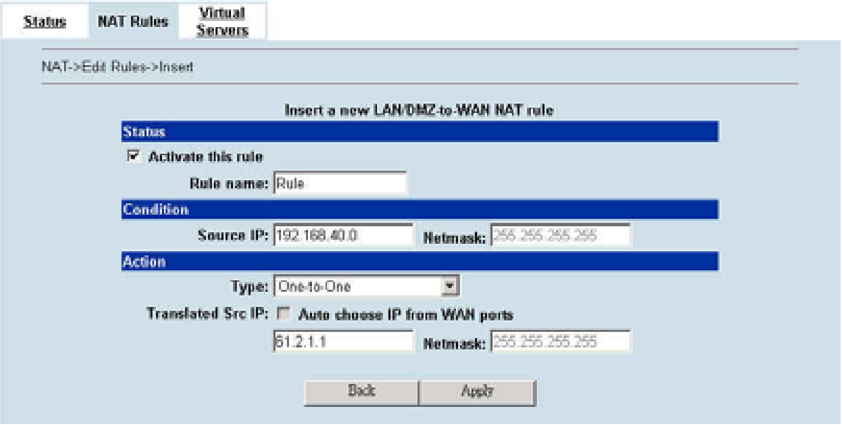
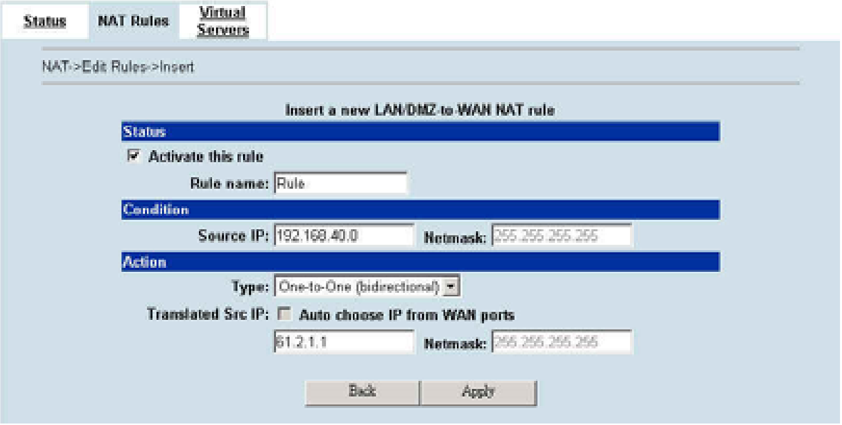
Type: Many-to-One

Translated Src IP: ☑ Auto choose IP from WAN ports

Netmask: 255.255.255.255

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Activate this rule	The NAT rule is enabled or not	Enabled / Disabled	Enabled
	Rule name	The NAT rule name	text string (Max: 200 entries)	Rule
Condition	Source IP / Netmask	Compared with the incoming packets, whether Source IP/Netmask is matched or not.	IPv4 format	192.168.40.0 / 255.255.255.0
Action	Type	Determine what NAT method you are using in the specified NAT rule. Refer more information in the section 7.5.	Many-to-One / Many-to-Many / One-to-One / One-to-One (bidirectional)	Many-to-One
	Translated Src IP (Auto choose IP from WAN ports)	Only work in Many-to-One type, the public IP address will be assigned by the default wan link.	Enabled / Disabled	Enabled
	Space / Netmask	When NAT type is not Many-to-One, we must specify IP address / Netmask directly.	IPv4 format	N/A

Table 7-2 Add a NAT rule

Step 5.b — Insert an Many-to-Many Rule If your ISP has assigned a range of public IP to your company, you can tell MH-5001 to translate the private IP addresses into the pool of public IP addresses. The MH-5001 will use the first public IP until MH-5001 uses up all source ports for the public IP. MH-5001 will then choose the second public IP from the address pool. Select `Many-to-Many` from the `Type`. Enter the subnet with an `IP address` and a `netmask`. Other fields are the same with those of Many-to-One rules. However, the MH-5001 will no longer choose the device IP for you. It will choose the IP from the address pool you have entered.	**ADVANCED SETTINGS > NAT > NAT Rules > Insert**  NAT->Edit Rules->Insert Insert a new LAN/DMZ-to-WAN NAT rule Status ☑ Activate this rule Rule name: Rule Condition Source IP: 192.168.40.0 Netmask: 255.255.255.0 Action Type: Many-to-Many Translated Src IP: □ Auto choose IP from WAN ports 61.2.1.1 Netmask: 255.255.255.252
Step 5.c — Insert an One-to-One Rule Though you may have many public IP address for translation, you may want to make some private IP to always use a public IP. In this case, you can select `One-to-One` from the `Type`, and enter the private-public IP address pair in the `Source IP` and the `Translated Source IP` fields.	**ADVANCED SETTINGS > NAT > NAT Rules > Insert**  NAT->Edit Rules->Insert Insert a new LAN/DMZ-to-WAN NAT rule Status ☑ Activate this rule Rule name: Rule Condition Source IP: 192.168.40.0 Netmask: 255.255.255.255 Action Type: One-to-One Translated Src IP: □ Auto choose IP from WAN ports 61.2.1.1 Netmask: 255.255.255.255
Step 5.d — Insert a One-to-One (Bidirectional) Rule The above three modes allow LAN/DMZ-to-WAN sessions establishment but do not allow WAN-to-LAN/DMZ sessions. WAN-to-LAN/DMZ sessions are allowed by Virtual Server rules. You can make the One-to-One NAT in the above to incorporate the WAN-to-LAN/DMZ feature by selecting the `One-to-One (Bidirectional)` from the Type. Note that WAN-to-LAN/DMZ traffic will be blocked by the Firewall in default. You have to add a Firewall rule to allow such traffic. If you expect a LAN/DMZ host to be fully accessed by public Internet users, use this mode. Note that this mode is extremely dangerous because the host is fully exposed to the Internet and may be cracked. Always use Virtual Server rules first.	**ADVANCED SETTINGS > NAT > NAT Rules > Insert**  NAT->Edit Rules->Insert Insert a new LAN/DMZ-to-WAN NAT rule Status ☑ Activate this rule Rule name: Rule Condition Source IP: 192.168.40.0 Netmask: 255.255.255.255 Action Type: One-to-One (bidirectional) Translated Src IP: □ Auto choose IP from WAN ports 61.2.1.1 Netmask: 255.255.255.255

7.4.2 Setup Virtual Server for the FtpServer1

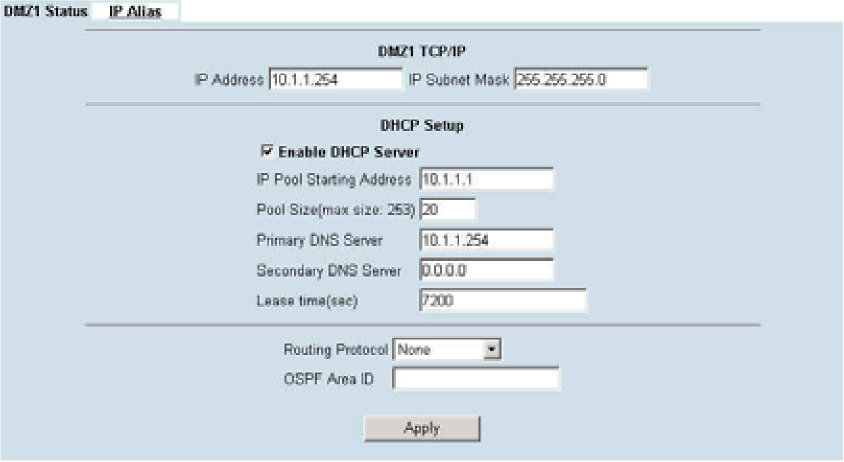
Step 1. Device IP Address Setup the `IP Address` and `IP Subnet Mask` for the MH-5001 of the DMZ1 interface.	**BASIC SETUP > DMZ Settings > DMZ1 Status**

Step 2. Client IP Range

Enable the `DHCP server` if you want to use MH-5001 to assign IP addresses to the computers under DMZ1. Here we make the DHCP feature enabled.

Step 3. Apply the Changes

Click `Apply` to save your settings.



DMZ1 Status | IP Alias

DMZ1 TCP/IP

IP Address: 10.1.1.254
IP Subnet Mask: 255.255.255.0

DHCP Setup

☑ Enable DHCP Server

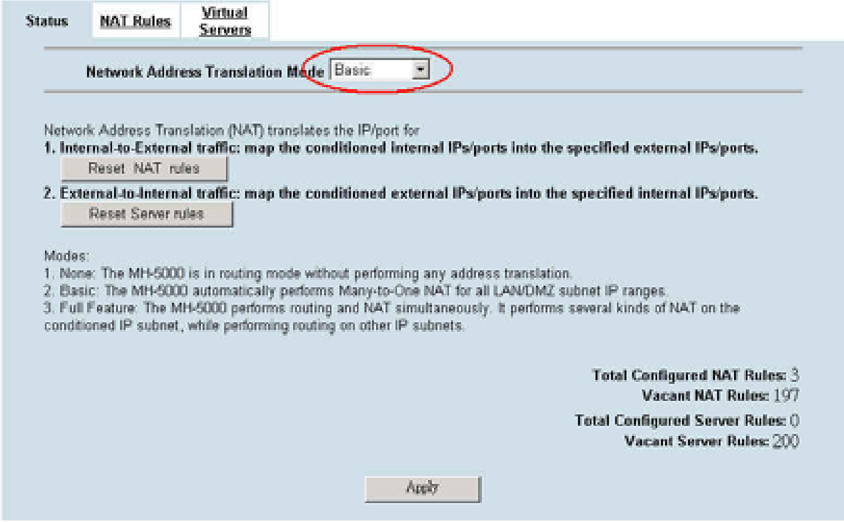
IP Pool Starting Address: 10.1.1.1
Pool Size(max size: 253): 20
Primary DNS Server: 10.1.1.254
Secondary DNS Server: 0.0.0.0
Lease time(sec): 7200

Routing Protocol: None
OSPF Area ID:

Step 4. Check NAT Status

The default setting of NAT is in `Basic` Mode. After applying the **Step 3**, the NAT is automatically configured with the rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.

ADVANCED SETTINGS > NAT > Status



Status | NAT Rules | Virtual Servers

Network Address Translation Mode: Basic

Network Address Translation (NAT) translates the IP/port for
1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.

2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.

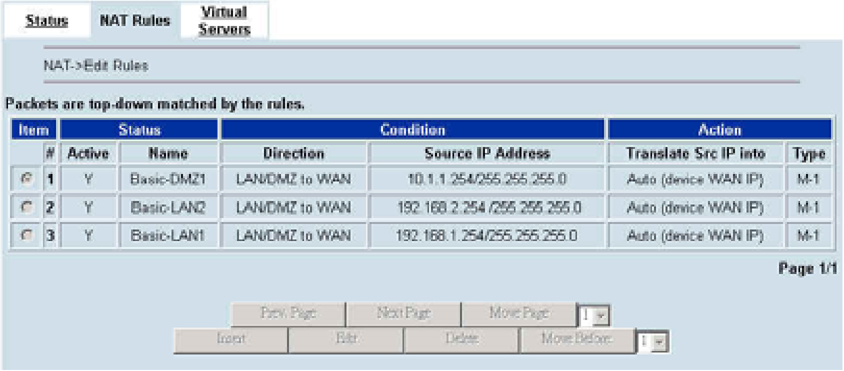
Modes:
1. None: The MH-5000 is in routing mode without performing any address translation.
2. Basic: The MH-5000 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
3. Full Feature: The MH-5000 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

Total Configured NAT Rules: 3
Vacant NAT Rules: 197
Total Configured Server Rules: 0
Vacant Server Rules: 200

Step 5. Check NAT Rules

The MH-5001 has added the NAT rules automatically as right diagram described. The rule `Basic-DMZ1` (number 1) means that, when matching the condition (requests of `LAN/DMZ-to-WAN` direction with its source IP falling in the range of `10.1.1.254 /255.255.255.0`), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.

ADVANCED SETTINGS > NAT > NAT Rules



Status | NAT Rules | Virtual Servers

NAT->Edit Rules

Packets are top-down matched by the rules.

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Translate Src IP into	Type
●	1	Y	Basic-DMZ1	LAN/DMZ to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1
○	2	Y	Basic-LAN2	LAN/DMZ to WAN	192.168.2.254 /255.255.255.0	Auto (device WAN IP)	M-1
○	3	Y	Basic-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M-1

Page 1/1

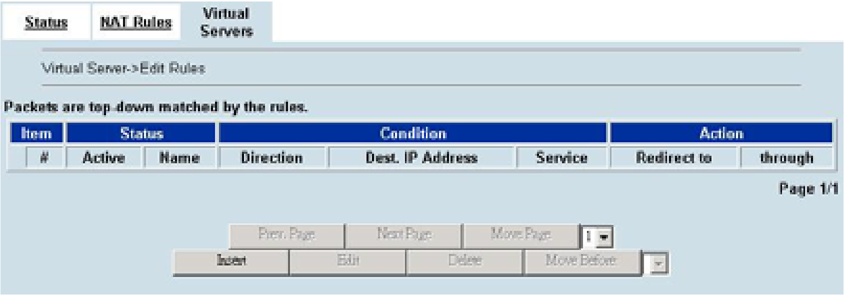
Step 6. Setup IP for the FTP Server

Assign an IP of 10.1.1.1/255.255.255.0 to the FTP server under DMZ1. Assume the FTP Server is at 10.1.1.5. And it is listening on the well-known port (21).

Step 7. Setup Server Rules

Insert a virtual server rule by clicking the `Insert` button.

ADVANCED SETTINGS > NAT > Virtual Servers



Virtual Server->Edit Rules

Packets are top-down matched by the rules.

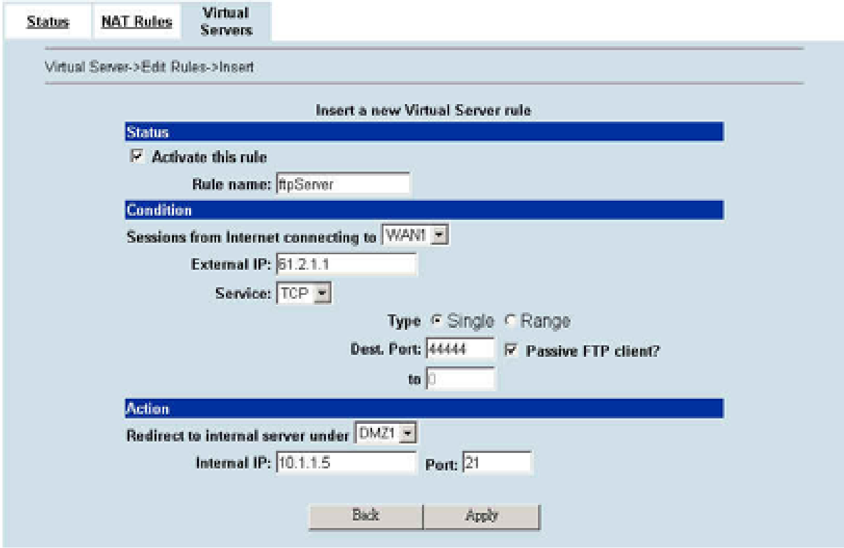
Item	Status		Condition			Action	
#	Active	Name	Direction	Dest. IP Address	Service	Redirect to	through

Page 1/1

Step 8. Customize the Rule

Customize the rule name as the `ftpServer`. For any packets with its destination IP equaling to the WAN1 IP (`61.2.1.1`) and destination port equaling to `44444`, ask MH-5001 to translate the packet's destination IP/port into `10.1.1.5/21`. Check the `Passive FTP client?` to maximize the compatibility of the FTP protocol. This is useful if you want to provide connectivity to passive FTP clients. For passive FTP clients, the server will return them the private IP address and the port number for them to connect back to do data transmissions. Since the private IP from them cannot be routed to our zone, the data connections would fail. After enabling this feature, the MH-5001 will translate the private IP/port into an IP/port of its own. Thus the problem is gracefully solved. Click `Apply` to proceed.

ADVANCED SETTINGS > NAT > Virtual Servers > Insert



Virtual Server->Edit Rules->Insert

Insert a new Virtual Server rule

Status

☑ Activate this rule

Rule name: ftpServer

Condition

Sessions from Internet connecting to WAN1

External IP: 61.2.1.1

Service: TCP

Type ● Single ○ Range

Dest. Port: 44444 ☑ Passive FTP client?

to 0

Action

Redirect to internal server under DMZ1

Internal IP: 10.1.1.5 Port: 21

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Activate this rule	The Virtual Server rule is enabled or not	Enabled / Disabled	Enabled
	Rule name	The Virtual Server rule name	text string (Max: 200 entries)	ftpServer
Condition	Sessions from Internet connecting to	Which interface does the connected session come from?	WAN interfaces	WAN1
	External IP	The public IP address of the Virtual Server.	IPv4 format	61.2.1.1
	Service	The service which is provided by the real server.	TCP / UDP	TCP
	Type	Port is Single or Range	Single / Range	Single
	Dest Port	The TCP/UDP port number which is provided by the real server.	1 ~65534	44444
	Passive FTP client	If the Passive FTP client is checked, it will connect to the internal DMZ FTP server of MH-5001 when FTP client uses passive mode. Otherwise, it will not work.	Enabled / Disabled	Enabled

Action	Redirect to internal server under	The subnet which is located the virtual server.	LAN / DMZ regions	DMZ1
	Internal IP	The IP address which is actually transferred to the internal DMZ	IPv4 format	10.1.1.5
	Port	The port number which is actually transferred to the internal DMZ. If you filled 0 in this field, it means that the real connected port is the same as the translated destination port.	0 ~ 65534	21

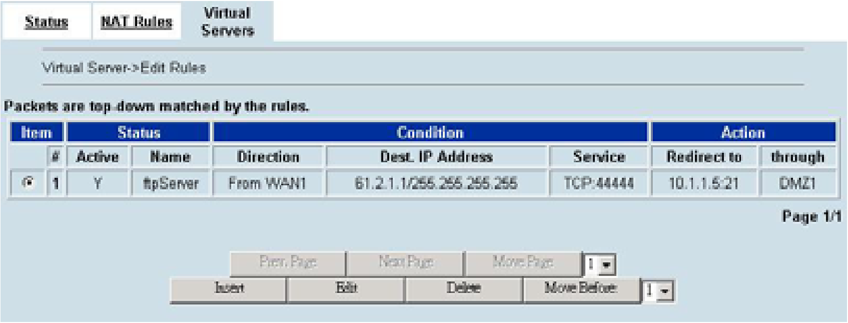
Table 7-3 Add a Virtual Server rule

Step 9. View the Result

Now any request towards the MH-5001's WAN1 IP (`61.2.1.1`) with port `44444` will be translated into a request towards `10.1.1.5` with port `21`, and then be forwarded to the `10.1.1.5`. The FTP server listening at port `21` in `10.1.1.5` will pick up the request.

After adding a virtual server's rule, make sure to add a NAT and Firewall rule.

ADVANCED SETTINGS > NAT > Virtual Servers



Virtual Server->Edit Rules

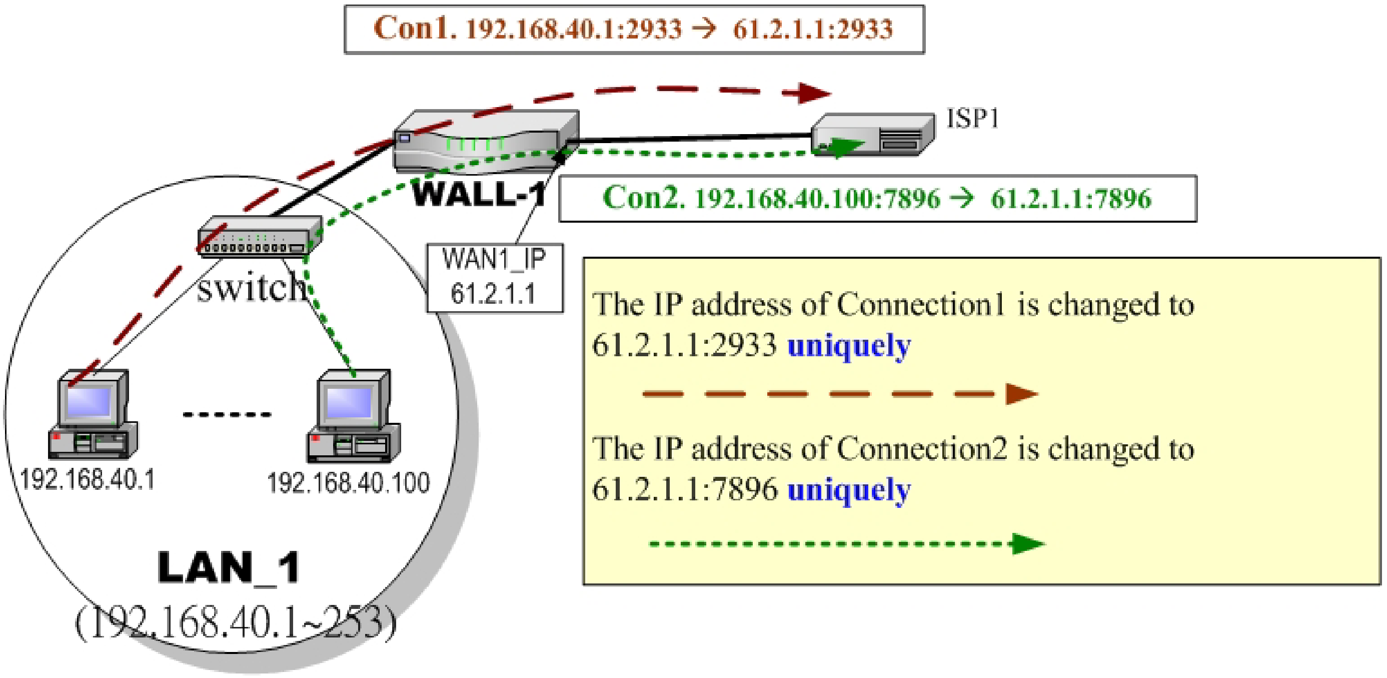
Packets are top-down matched by the rules.

Item		Status		Condition			Action	
	#	Active	Name	Direction	Dest. IP Address	Service	Redirect to	through
●	1	Y	ftpServer	From WAN1	61.2.1.1/255.255.255.255	TCP:44444	10.1.1.5:21	DMZ1

Page 1/1

7.5 NAT modes introduction

7.5.1 Many-to-One type

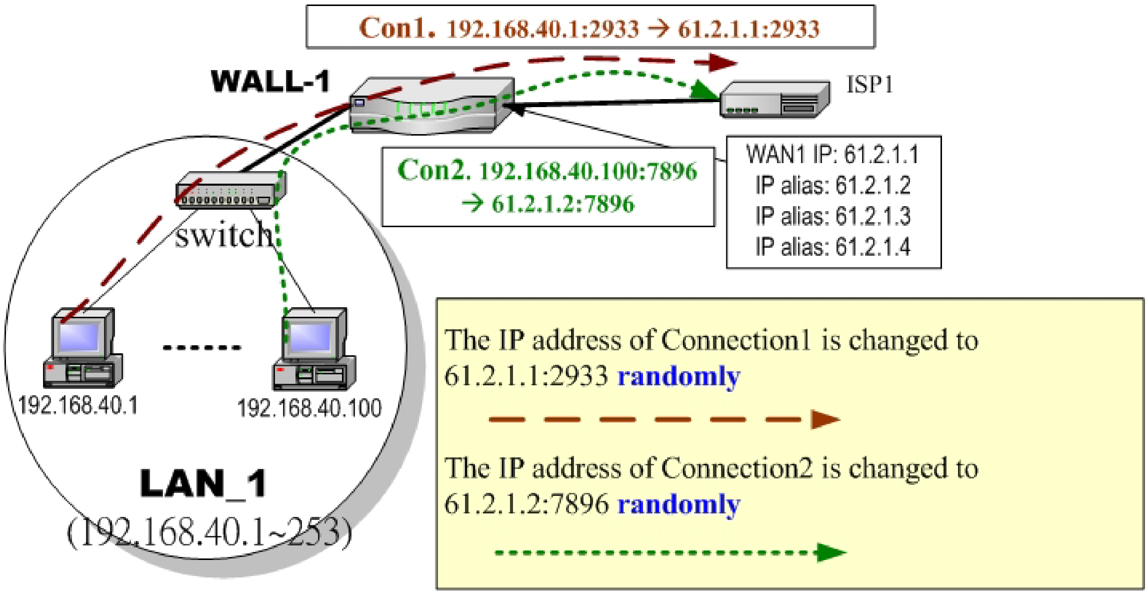

Con1. 192.168.40.1:2933 → 61.2.1.1:2933
ISP1
WALL-1
Con2. 192.168.40.100:7896 → 61.2.1.1:7896
switch
WAN1_IP
61.2.1.1
The IP address of Connection1 is changed to 61.2.1.1:2933 uniquely
The IP address of Connection2 is changed to 61.2.1.1:7896 uniquely
192.168.40.1

192.168.40.100
LAN_1
(192.168.40.1~253)

Figure 7-4 NAT Many-to-One type

As the above Figure 7-4 illustrated, NAT Many-to-One type means that many local PCs are translated into only one public IP address when the packets are forwarded out through the WALL-1 - MH-5001. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933. In the same way, when the packets of Connection2 are forwarded out, its IP address is still translated to the same public IP address (61.2.1.1:7896).

7.5.2 Many-to-Many type



The IP address of Connection1 is changed to 61.2.1.1:2933 **randomly**

The IP address of Connection2 is changed to 61.2.1.2:7896 **randomly**

Figure 7-5 NAT Many-to-Many type

As the above Figure 7-5 illustrated, NAT Many-to-Many type means that many local PCs are translated into multiple public IP addresses when the packets are forwarded out through the MH-5001. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933. Until MH-5001 uses out of all source ports of the public (61.2.1.1), MH-5001 will then choose the second public IP (such as 61.2.1.2) from the address pool. For example, Connection2 are forwarded out, the source IP address will be translated into the second public IP address (61.2.1.2) from the public IP address pools. So the translated IP address (61.2.1.2:7896) is different from Connection1 one (61.2.1.1:2933).

7.5.3 One-to-One type

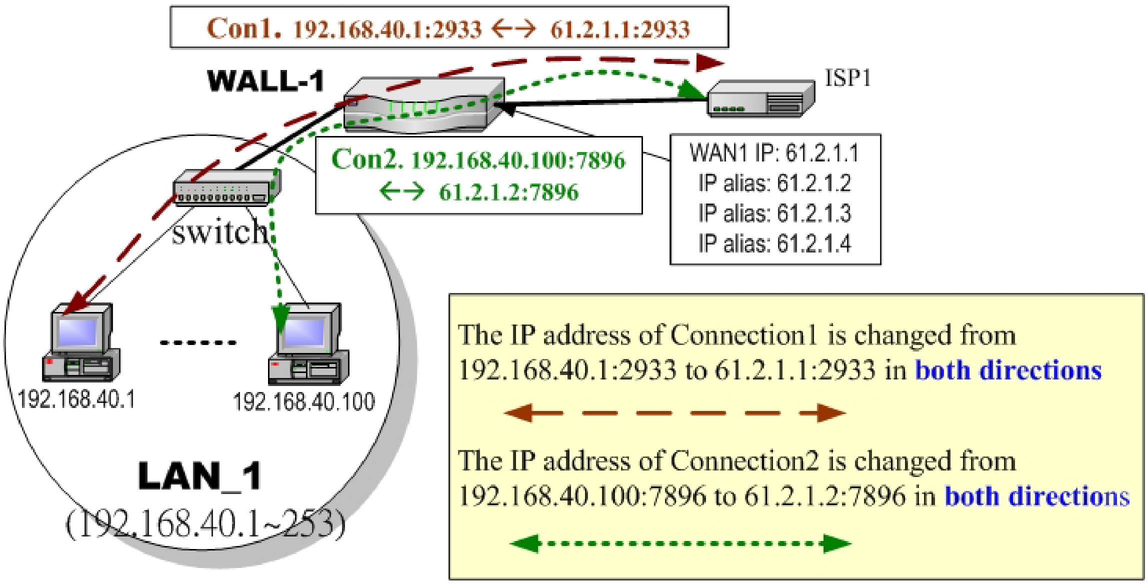

Con1. 192.168.40.1:2933 <-> 61.2.1.1:2933
WALL-1
ISP1
Con2. 192.168.40.100:7896
<-> 61.2.1.2:7896
WAN1 IP: 61.2.1.1
IP alias: 61.2.1.2
IP alias: 61.2.1.3
IP alias: 61.2.1.4
switch
192.168.40.1
192.168.40.100
LAN_1
(192.168.40.1~253)
The IP address of Connection1 is changed from 192.168.40.1:2933 to 61.2.1.1:2933 in both directions
The IP address of Connection2 is changed from 192.168.40.100:7896 to 61.2.1.2:7896 in both directions

Figure 7-6 NAT One-to-One type

As the above Figure 7-6 illustrated. NAT One to One type means that each local PC is translated into a unique public IP address when the packets are forwarded out through the MH-5001. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933. But, when the packets of Connection2 are forwards out, the source IP address is translated to another dedicated public IP address(61.2.1.2:7896).

7.5.4 NAT modes & types

The following three NAT modes are supported by MH-5001 now as the following Table 7-4.

NAT mode	Description
None	The MH-5001 is in routing mode without performing any address translation.
Basic	The MH-5001 automatically performs Many-to-One NAT for all LAN/DMZ subnets.
Full Feature	The MH-5001 can be manually configured with Many-to-One, and Many-to-Many, One-to-One, and bidirectional. One-to-One rules to do policy-based NAT.

Table 7-4 NAT modes overview

If you choose Full Feature mode of NAT at Table 7-4, you may need to edit the rule by yourself. Then you must determine the NAT type in the NAT rule. What meaning does each NAT type represent? How to determine which NAT type is best choice for you. You can lookup the explainations and suggestions at Table 7-5.

Type	Description	Usage moment
Many-to-One	Map a pool of private IP addresses to a single public IP address chosen from the WAN ports.	If the public IP addresses of your company is insufficient, and you prefer to increase the node which can connect to the Internet. You can just choose the Many-to-One type to fit your request.

Many-to-Many	Map a pool of private IP addresses to a subnet range of public IP addresses chosen from the WAN ports. Only when all ports of the first public IP are used, it will then use the next public IP address for transferring by all private IPs.	If the public IP address of your company is not only one node (ex. you have applied extra-one ISP). You may use the Many-to-Many type to make the multiple public addresses sharing the outbound bandwidth. So your inbound and outbound traffic will be more flexible.
One-to-One	Map a single private IP address to a single public IP address chosen from the WAN ports. This was useful when you have multiple public IPs in the WAN ports. And you intended to map each local server to a unique public IP on the WAN port.	If you wish to specify a unique internal IP address to transfer a fixed external IP address. You can specify the One-to-One type.
One-to-One (bidirectional)	An internal host is fully mapped to a WAN IP address. Notice that you must add a firewall rule to forward WAN to LAN/DMZ traffic.	If you wish to expose the local pc onto the Internet, and open all Internet services outside. You can specify the One-to-One (bidirectional) type. This will make the local pc you specified fully exposed to the Internet. Additionally you must add a firewall rule to allow WAN to LAN (or DMZ) traffic forward. Then you can finish the settings. Be careful to use this type, or it will endanger your network security.

Table 7-5 The NAT type comparison

Chapter 8 Routing

This chapter introduces how to add static routing and policy routing entries

To facilitate the explanation on how MH-5001 implements routing and how to use it. We zoom in the left part of Figure 2-1 into Figure 8-1 and increase some devices for description.

8.1 Demands

1. There is only one local area (192.168.40.0/24) inside the LAN1 port. Now there is a new financial area (192.168.50.0/24) in the Figure 8-1. The financial area is connected with a router which is inside the LAN1 port of MH-5001. So we need to add the configurations for the financial department.

2. Refer to the Figure 8-1 description. The bandwidth subscribed from ISP1 is insufficient so that some important traffic, say the traffic from PCs belonging to the General-Manager-Room department (192.168.40.192/255.255.255.192), is blocked by the other traffic. We hope that the employees of General-Manager-Room can have a dedicated bandwidth to improve the quality of connecting Internet.

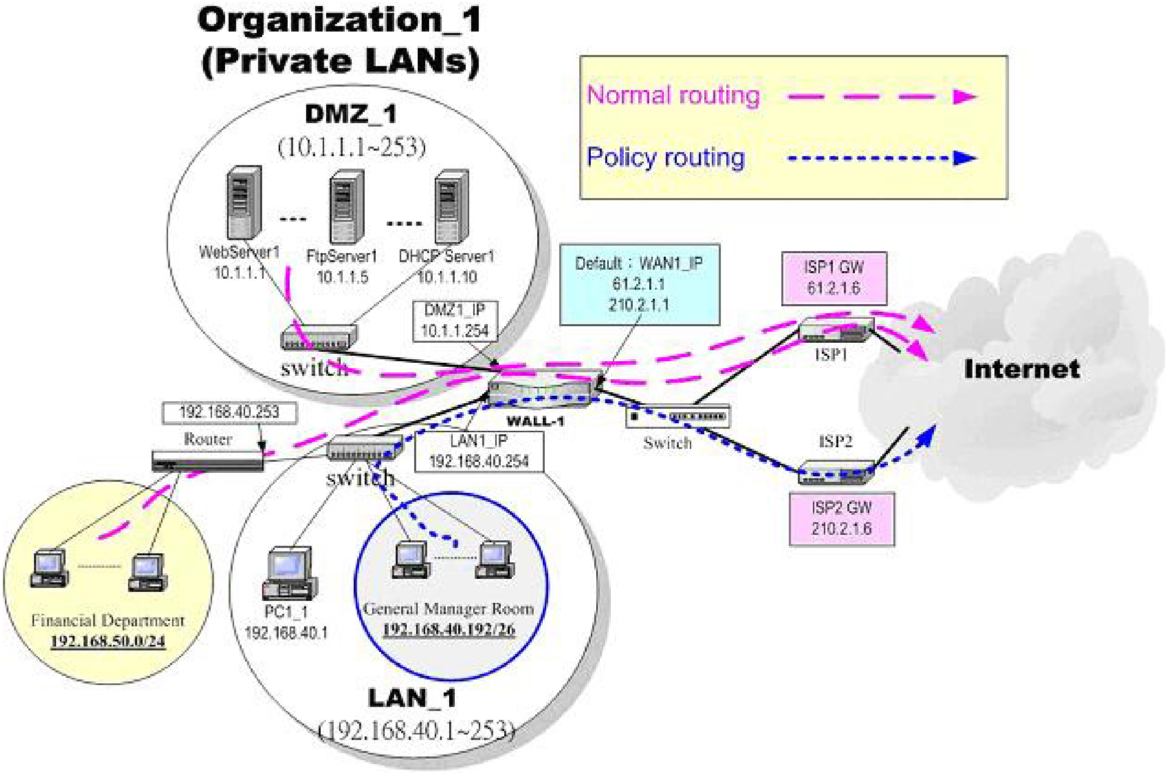


Figure 8-1 Add policy routing entry for the General-Manager-Room department

8.2 Objectives

1. We need to let WALL-1, the MH-5001 knows how to forward the packets which is destinated financial department (192.168.50.0/24).

2. The network administrator plans to solve the problem by subscribing the second link (ISP2). He hopes that all the packets from the General-Manager-Room (192.168.40.192/26) will pass through the ISP2 link instead of the default ISP1 link.

8.3 Methods

1. Add a static routing entry to direct the packets towards 192.168.50.0/24 through the router (192.168.40.253).

2. Add a policy routing entry for the packets coming from General-Manager-Room department (192.168.40.192 / 255.255.255.192) through the ISP2 link.

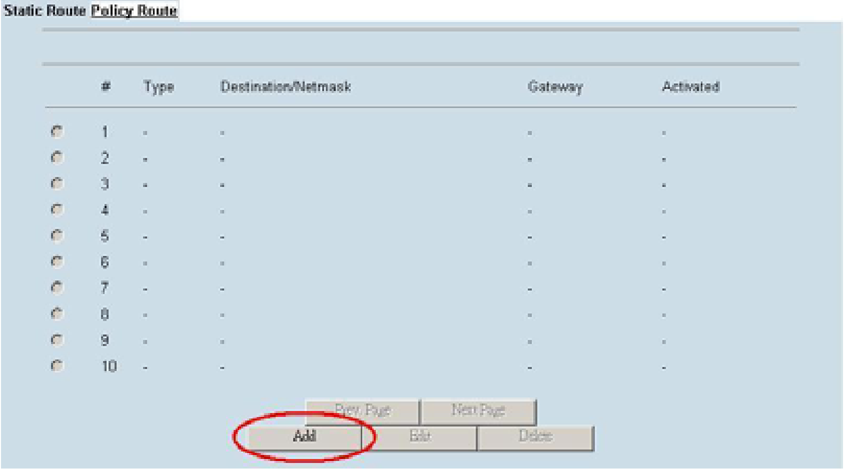
8.4 Steps

8.4.1 Add a static routing entry

Step 1. Add a static routing rule

Click the Add button to the next process.

Advanced Settings > Routing > Static Route

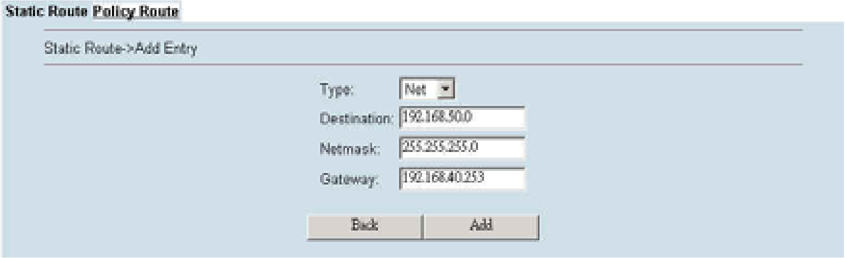


	#	Type	Destination/Netmask	Gateway	Activated
○	1	-	-	-	-
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-	-	-
○	6	-	-	-	-
○	7	-	-	-	-
○	8	-	-	-	-
○	9	-	-	-	-
○	10	-	-	-	-

Step 2. Fill out the related field

Fill in the `Destination` and the `Netmask` field with `192.168.50.0` and `255.255.255.0`. Assign the next hop `Gateway` as `192.168.40.253` (Router IP address). Click Add to proceed. (Max: 30 entries)

Advanced Settings > Routing > Static Route > Add



Static Route->Add Entry

Type: Net
Destination: 192.168.50.0
Netmask: 255.255.255.0
Gateway: 192.168.40.253

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Type	Determine this static routing entry record is multiple hosts (Net) or a single host (Host)。	Net / Host	Net
Destination	The destination IP address of this static routing entry record.	IPv4 format	192.168.50.0

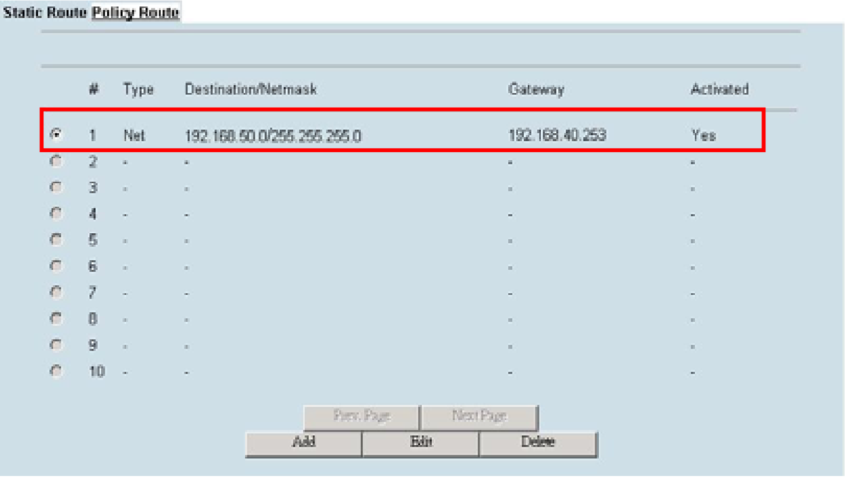
Netmask	The destination IP Netmask of this static routing entry record.	IPv4 format	255.255.255.0
Gateway	The default gateway of this static routing entry record.	IPv4 format	192.168.40.253

Table 8-1Add a static routing entry

Step 3. View the result

The static route has been stored. After filling data completely, view the static routing entries which have been set.

Advanced Settings > Routing > Static Route

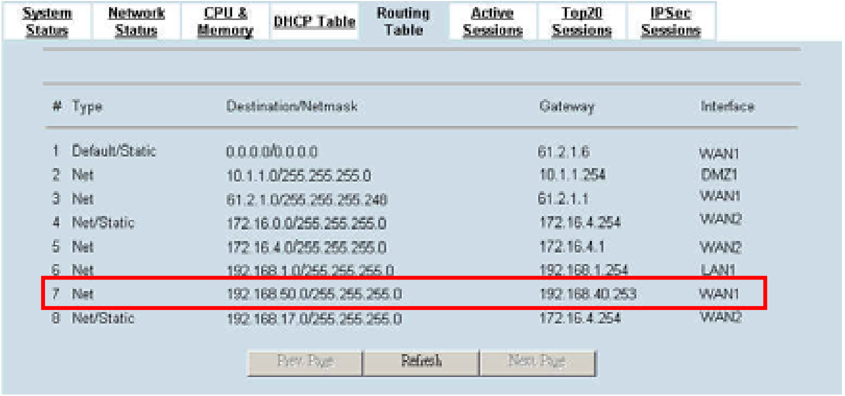


	#	Type	Destination/Netmask	Gateway	Activated
●	1	Net	192.168.50.0/255.255.255.0	192.168.40.253	Yes
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-	-	-
○	6	-	-	-	-
○	7	-	-	-	-
○	8	-	-	-	-
○	9	-	-	-	-
○	10	-	-	-	-

Step 4. View the routing table

You can notice there is an extra routing entry in the routing table. The indicated routing entry as right diagram is produced by static routing rule.

Device Status > System Status > Routing Table



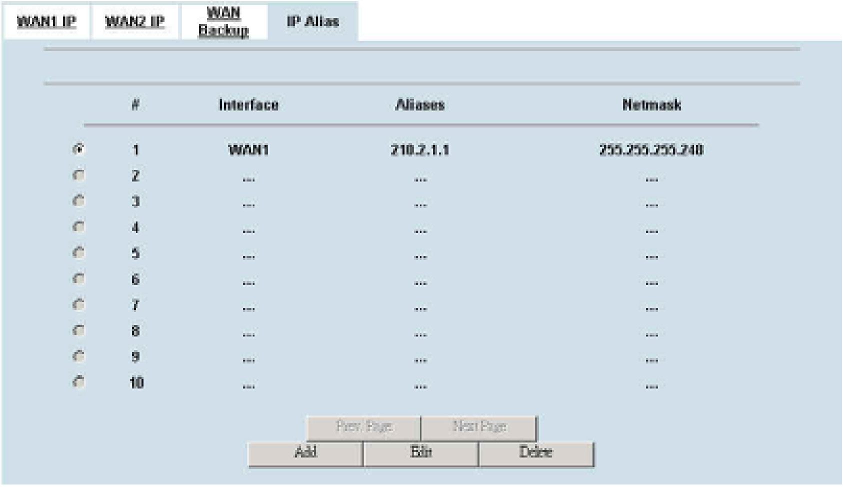
#	Type	Destination/Netmask	Gateway	Interface
1	Default/Static	0.0.0.0/0.0.0.0	61.2.1.6	WAN1
2	Net	10.1.1.0/255.255.255.0	10.1.1.254	DMZ1
3	Net	61.2.1.0/255.255.255.240	61.2.1.1	WAN1
4	Net/Static	172.16.0.0/255.255.255.0	172.16.4.254	WAN2
5	Net	172.16.4.0/255.255.255.0	172.16.4.1	WAN2
6	Net	192.168.1.0/255.255.255.0	192.168.1.254	LAN1
7	Net	192.168.50.0/255.255.255.0	192.168.40.253	WAN1
8	Net/Static	192.168.17.0/255.255.255.0	172.16.4.254	WAN2

8.4.2 Add a policy routing entry

Step 5. Setup the ISP2 link

We must add an IP alias record to the WAN1 port, because a new ISP link has been applied. See section 3.4.3 for the full procedures.

Basic Setup > WAN Settings > IP Alias

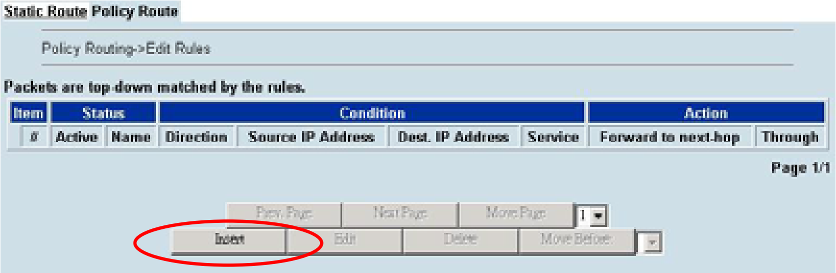


	#	Interface	Aliases	Netmask
●	1	WAN1	210.2.1.1	255.255.255.240
○	2	...	...	...
○	3	...	...	...
○	4	...	...	...
○	5	...	...	...
○	6	...	...	...
○	7	...	...	...
○	8	...	...	...
○	9	...	...	...
○	10	...	...	...

Step 6. Insert a policy routing entry

Click `Insert` button to add a policy routing entry.

Advanced Settings > Routing > Policy Route



Policy Routing->Edit Rules

Packets are top-down matched by the rules.

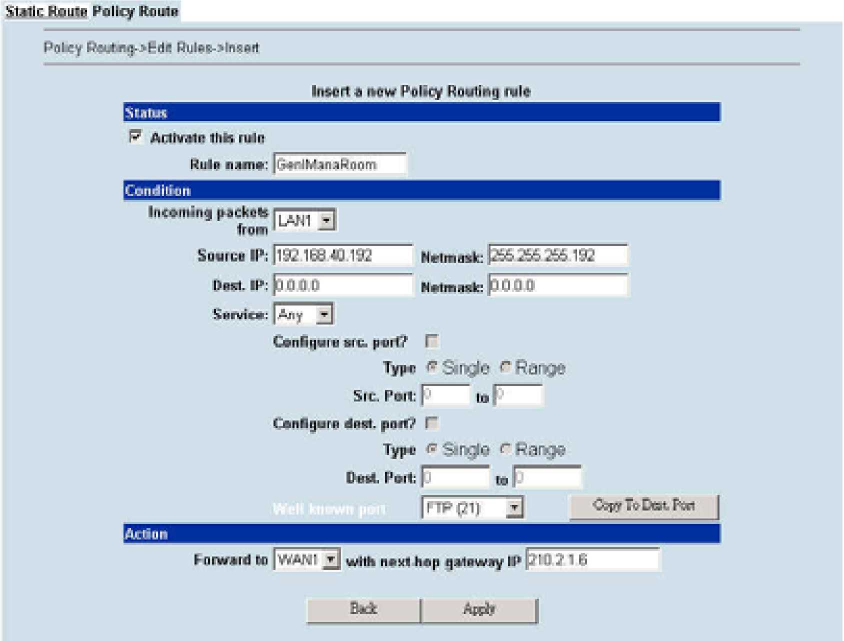
Item	Status		Condition				Action	
#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Forward to next-hop	Through

Page 1/1

Step 7. Fill out the related field

For the General-Manager-Room department, we need to set an extra policy routing entry for them. So in the `Status` region, make sure the `Activate this rule` is enabled, and then fill in `GenlManaRoom` in the `Rule name` field. In the `Condition` region, we fill `192.168.40.192` in `Source IP` field. Fill `255.255.255.192` in the `Netmask` field. In the `Action` region, fill forward to `WAN1` with next-hop gateway `210.2.1.6`. After setting as above, the packets which match the condition, they will follow the predefined action to forward to the next hop.

Advanced Settings > Routing > Policy Route > Insert



Policy Routing->Edit Rules->Insert

Insert a new Policy Routing rule

Status

☑ Activate this rule

Rule name: GenlManaRoom

Condition

Incoming packets from: LAN1

Source IP: 192.168.40.192 Netmask: 255.255.255.192

Dest. IP: 0.0.0.0 Netmask: 0.0.0.0

Service: Any

Configure src. port? □

Type ● Single ○ Range

Src. Port: 0 to 0

Configure dest. port? □

Type ● Single ○ Range

Dest. Port: 0 to 0

Well known port FTP (21) Copy To Dest. Port

Action

Forward to WAN1 with next-hop gateway IP 210.2.1.6

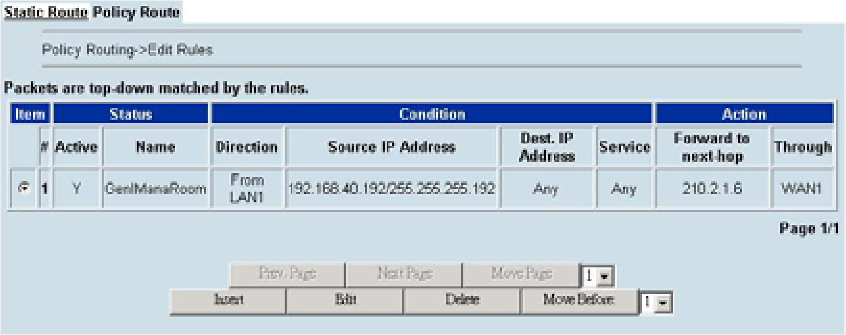
	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Activate this rule	The policy routing rule is enabled or not.	Enabled / Disabled	Enabled
	Rule name	The policy routing rule name.	text string (Max: 200 entries)	GenlManaRoom
Condition	Incoming packets from	Packets comes from which interface	LAN / DMZ regions	LAN1
	Source IP & Netmask	Verify if the incoming packets belong to the range of the Source IP/Netmask in the policy routing rule.	IPv4 format / IPv4 format	192.168.40.192 / 255.255.255.192
	Dest IP & Netmask	Verify if the incoming packets belong to the range of the Dest IP/Netmask in the policy routing rule.	IPv4 format / IPv4 format	0.0.0.0 / 0.0.0.0
	Service	Verify what is the service of this packet?	ANY / TCP / UDP / ICMP	Any
	Configure src. port? Type Src. port	If the service is TCP or UDP, we can choose to configure or not to configure source port.	Enabled / Disabled	No
	Type	If we decide to configure source port, we must choose the port to be single or range.	Single / Range	N/A
	Src. Port	If we select single at above field, we just have to fill a port in the first blank space. If we select range at above field, we need to fill the range of the ports.	1 ~ 65534	N/A
	Configure dest. port? Type Dest. port	If the service is TCP or UDP, we can choose to configure or not to configure destination port.	Enabled / Disabled	No
	Type	If we decide to configure destination port, we must choose the port to be single or range.	Single / Range	N/A
	Dest. Port	If we select single at above field, we just have to fill a port in the first blank space. If we select range at above field, we need to fill the range of the ports.	1 ~ 65534	N/A
Action	Forward to	If the packet is matched to this rule, which interface does this packet sent out to?	WAN interfaces	WAN1
	Nexthop gateway IP	The next gateway IP address of forwarding interface.	IPv4 format	210.2.1.6

Table 8-2 Add a policy routing entry

Step 8. View the result

After filling data completely, view the policy routing entries which have been set.

Advanced Settings > Routing > Policy Route



Policy Routing->Edit Rules

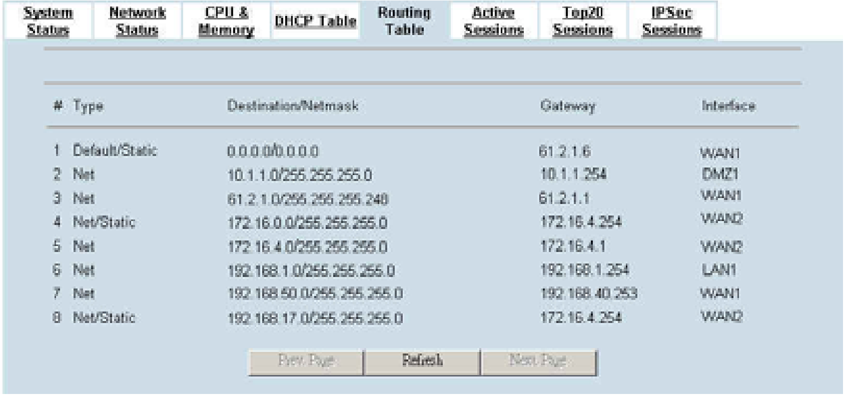
Packets are top-down matched by the rules.

Item		Status		Condition				Action	
	#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Forward to next-hop	Through
○	1	Y	GenManaRoom	From LAN1	192.168.40.192/255.255.255.192	Any	Any	210.2.1.6	WAN1

Step 9. View the routing table

Finally click the "Routing Table" to see all the current routing table information.

Device Status > System Status > Routing Table



#	Type	Destination/Netmask	Gateway	Interface
1	Default/Static	0.0.0.0/0.0.0.0	61.2.1.6	WAN1
2	Net	10.1.1.0/255.255.255.0	10.1.1.254	DMZ1
3	Net	61.2.1.0/255.255.255.240	61.2.1.1	WAN1
4	Net/Static	172.16.0.0/255.255.255.0	172.16.4.254	WAN2
5	Net	172.16.4.0/255.255.255.0	172.16.4.1	WAN2
6	Net	192.168.1.0/255.255.255.0	192.168.1.254	LAN1
7	Net	192.168.50.0/255.255.255.0	192.168.40.253	WAN1
8	Net/Static	192.168.17.0/255.255.255.0	172.16.4.254	WAN2

8.4.3 The priority of the routing

As we know, there are many choices according to your requirement in the routing settings. As the following Table 8-3 indicates, the smaller priority sequence would be executed first when running routing.

Priority sequence	Routing Method	Description	Restricted Region
1.	WAN policy route > WAN Static/RIP route	WAN policy route will redirect the traffic to the specific WAN interface if the traffic matches the policy.	WAN
2.	WAN static/RIP route > Default route	Static route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols. Routing information protocol (RIP) teaches routers on a wide area network which routers have access to which addresses. This information is kept in a routing table on each router. As routers communicate with each other, they all update their routing tables to include each others' routing table information. The priority between RIP route and static route depends on its prefix. Whose prefix is shortest, it will have the high priority. If the traffic is not from the WAN interface, the priority will be static/RIP route > default route.	WAN
3.	Default Route	A routing table entry which is used to direct packets addressed to networks not explicitly listed in the routing table. Basically, if no other routing has been set, the traffic will go through the default route.	WAN

Table 8-3 The priority of the routing

Chapter 9
IP / Services grouping

This chapter introduces group functions and explains how to edit it.

9.1 Demands

1. You hope to group some similar IP addresses to make it easier for editing the firewall rule.
2. You hope to group some similar services to make it easier for editing the firewall rule.
3. You hope to make your firewall rule taken effect by the pre-scheduled time.

9.2 Objectives

1. Through the IP addresses grouping, we can group the multiple IP addresses and make it easier to configure the firewall rule.
2. Suppose you would like to use services to control the types of communication accepted or denied by the firewall, you can add any of the predefined services or create a service group to edit the firewall rule manually.
3. Suppose the MSN policy cannot be used in your company from Monday to Friday 9:00~12:00, 13:00~17:30, but user can use it any time after work. The administrator needs to create the schedules to meet the policy requirement.

9.3 Methods

1. You can configure the function under Basic Setup > Books > Address to group mutiple IP addresses into the an unigue group.
2. You can configure the function under Basic Setup > Books > Services to group mutiple services into an unique group.
3. In the Basic Setup > Books > Schedule, define the schedule which will deny MSN service.

9.4 Steps

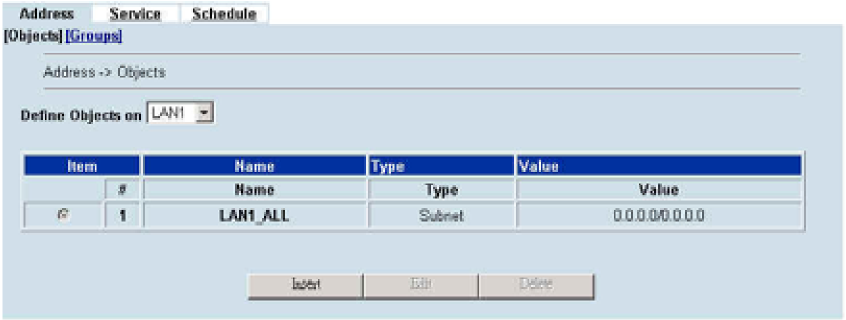
9.4.1 Setup Address

Step 10. Address Settings

Suppose you would like to configure a firewall rule, you must define addresses to the addresses list for each interface first. These addresses should be valid, that is installed.

Click the `Objects` hyperlink and then select the `Define Objects` on `LAN1`. Click `Insert` to add a new address object.

BASIC SETUP > Books > Address > Object



Define Objects on LAN1

Item		Name	Type	Value
	#	Name	Type	Value
○	1	LAN1_ALL	Subnet	0.0.0.0/0.0.0.0

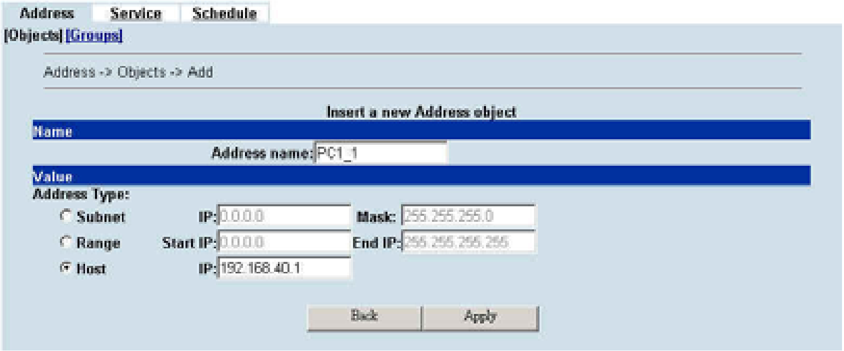
FIELD	DESCRIPTION	Range / Format	EXAMPLE
Define Objects on __	Select the interface which you are going to define address object.	All the interfaces	LAN1

Table 9-1 Define the address objects

Step 11. Insert a new Address object

Enter the `Address name`. Select which address type the address object will be. And then enter the IP address.

BASIC SETUP > Books > Address > Object > Insert



Insert a new Address object

Name

Address name: PC1_1

Value

Address Type:

○ Subnet	IP:	0.0.0.0	Mask:	255.255.255.0
○ Range	Start IP:	0.0.0.0	End IP:	255.255.255.255
● Host	IP:	192.168.40.1		

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Address name	The name of the address object. Note that address name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.	text string	PC1_1
Address Type	The address type of the object.	Subnet / Range / Host	Host 192.168.40.1

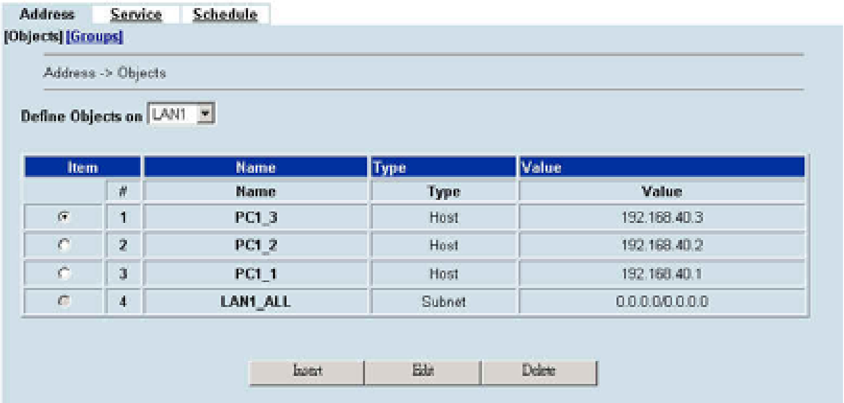
Table 9-2 The field of the Address object

Step 12. View the Address object settings

After entering the new Address object, subsequently we add the other two address objects. The result is shown in the "Object" page.

Note: It is the same way to setup address objects in the other interfaces.

BASIC SETUP > Books > Address > Objects



Define Objects on LAN1

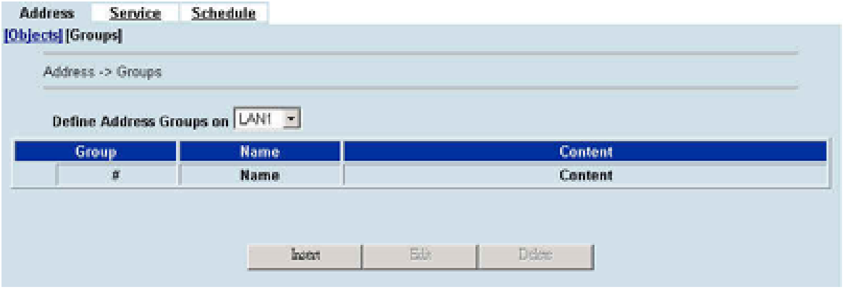
Item		Name	Type	Value
	#	Name	Type	Value
●	1	PC1_3	Host	192.168.40.3
○	2	PC1_2	Host	192.168.40.2
○	3	PC1_1	Host	192.168.40.1
○	4	LAN1_ALL	Subnet	0.0.0.0/0.0.0.0

Step 13. Address Group Settings

You can add, edit, and delete all other addresses definition as required. You can also organize related addresses into address group to simplify firewall rule creation.

Click the `Groups` hyperlink. Select `LAN1` to define Address Groups, and then click `Insert` to proceed.

BASIC SETUP > Books > Address > Group



Define Address Groups on LAN1

Group	Name	Content
#	Name	Content

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Define Addresses Groups on __	Select the interface which you are going to define addresses group.	All the interfaces	LAN1

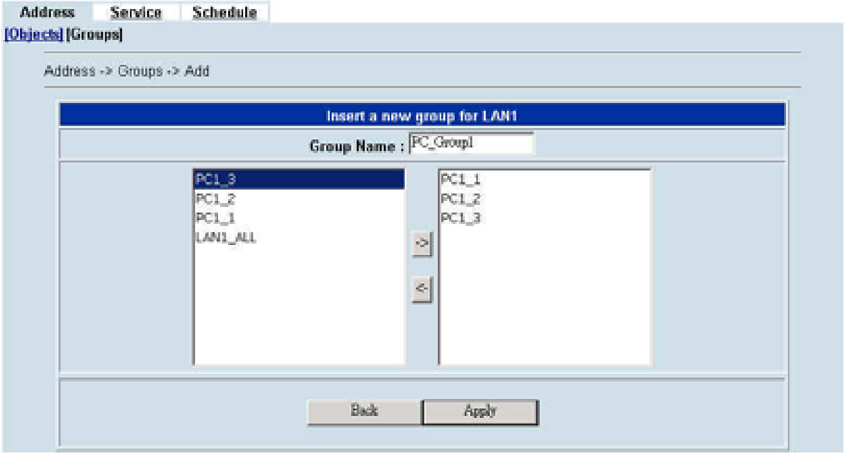
Table 9-3 Define the addresses group

Step 14. Add an address group

Enter a `Group Name` to identify the address group. Select the addresses from the available address list and click right arrow to add them to the Members list. To remove addresses from address group, please select addresses from the Members list and then click left arrow.

You can add address groups to any interface. The address group can only contain addresses from that interface. Address group cannot have the same names as individual addresses. If an address group is included in a firewall rule, it cannot be deleted unless it is first removed by the firewall rule.

BASIC SETUP > Books > Address > Group > Insert



Insert a new group for LAN1

Group Name : PC_Group1

PC1_3
PC1_2
PC1_1
LAN1_ALL

PC1_1
PC1_2
PC1_3

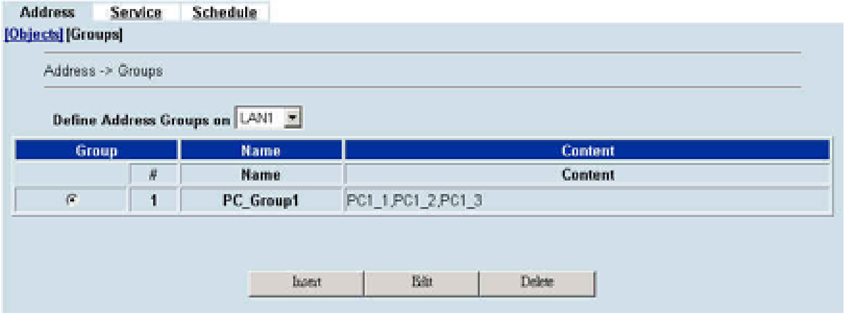
FIELD	DESCRIPTION	Range / Format	EXAMPLE
Group Name	The address group name. Note that group name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.	text string	PC_Group1
BUTTON	DESCRIPTION		
->	Add the selected address object to the address group.		
<-	Remove the selected address object from address group.		

Table 9-4 Define the addresses group

Step 15. view the address group result

According to our setting as previous steps, the address group is shown as right diagram.

BASIC SETUP > Books > Address > Group



Define Address Groups on LAN1

Group		Name	Content
	#	Name	Content
●	1	PC_Group1	PC1_1,PC1_2,PC1_3

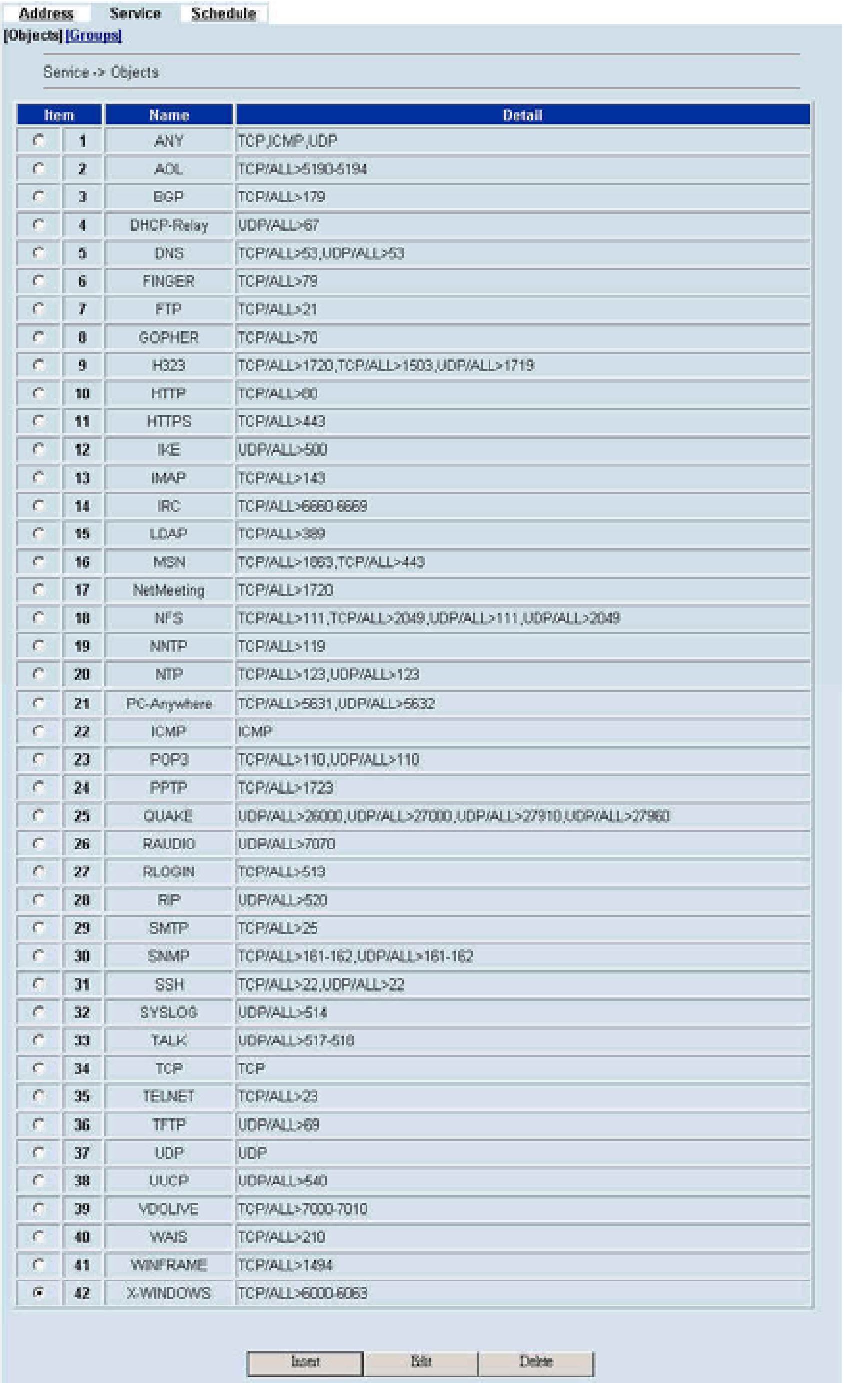
9.4.2 Setup Service

Step 16. Service Settings

The MH-5001 predefined firewall services are listed as right diagram. You can add these services to any firewall rule or you can add a service if you need to create a firewall rule for a service that is not in the predefined service list.

Select `Insert` to add a new service.

BASIC SETUP > Books > Service > Objects



Service -> Objects

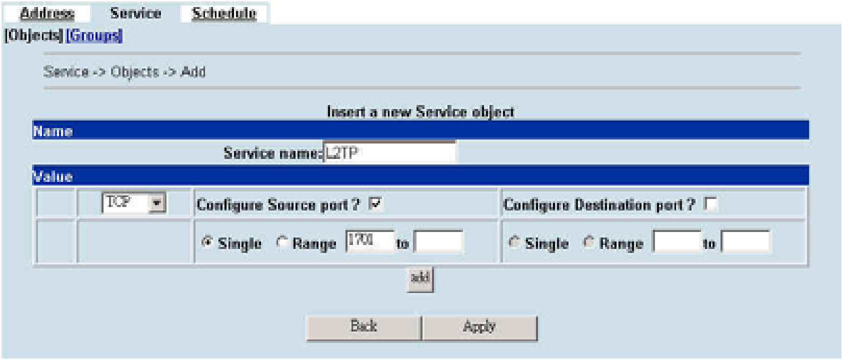
Item		Name	Detail
○	1	ANY	TCP,ICMP,UDP
○	2	AOL	TCP/ALL>5190-5194
○	3	BGP	TCP/ALL>179
○	4	DHCP-Relay	UDP/ALL>67
○	5	DNS	TCP/ALL>53,UDP/ALL>53
○	6	FINGER	TCP/ALL>79
○	7	FTP	TCP/ALL>21
○	8	GOPHER	TCP/ALL>70
○	9	H323	TCP/ALL>1720,TCP/ALL>1503,UDP/ALL>1719
○	10	HTTP	TCP/ALL>80
○	11	HTTPS	TCP/ALL>443
○	12	IKE	UDP/ALL>500
○	13	IMAP	TCP/ALL>143
○	14	IRC	TCP/ALL>6660-6669
○	15	LDAP	TCP/ALL>389
○	16	MSN	TCP/ALL>1863,TCP/ALL>443
○	17	NetMeeting	TCP/ALL>1720
○	18	NFS	TCP/ALL>111,TCP/ALL>2049,UDP/ALL>111,UDP/ALL>2049
○	19	NNTP	TCP/ALL>119
○	20	NTP	TCP/ALL>123,UDP/ALL>123
○	21	PC-Anywhere	TCP/ALL>5631,UDP/ALL>5632
○	22	ICMP	ICMP
○	23	POP3	TCP/ALL>110,UDP/ALL>110
○	24	PPTP	TCP/ALL>1723
○	25	QUAKE	UDP/ALL>26000,UDP/ALL>27000,UDP/ALL>27910,UDP/ALL>27960
○	26	RAUDIO	UDP/ALL>7070
○	27	RLOGIN	TCP/ALL>513
○	28	RIP	UDP/ALL>520
○	29	SMTP	TCP/ALL>25
○	30	SNMP	TCP/ALL>161-162,UDP/ALL>161-162
○	31	SSH	TCP/ALL>22,UDP/ALL>22
○	32	SYSLOG	UDP/ALL>514
○	33	TALK	UDP/ALL>517-518
○	34	TCP	TCP
○	35	TELNET	TCP/ALL>23
○	36	TFTP	UDP/ALL>69
○	37	UDP	UDP
○	38	UUCP	UDP/ALL>540
○	39	VDOLIVE	TCP/ALL>7000-7010
○	40	WAIS	TCP/ALL>210
○	41	WINFRAME	TCP/ALL>1494
●	42	X-WINDOWS	TCP/ALL>6000-6063

Step 17. Insert a new service object

Enter the Service name. Select which protocol type (TCP, UDP, ICMP) used by this service. Specify a Source and Destination Port number range for the service. If this service uses single port, enter the number in the first blank. If the service has more than one port range, select `add` to specify additional protocols and port range. Select `Apply` to add a new service object.

Note that service name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.

BASIC SETUP > Books > Service > Insert



Service name: L2TP

TCP

Configure Source port ? ☑

Configure Destination port ? □

● Single ○ Range 1701 to

○ Single ○ Range to

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Service name	The name of the service object.	text string	L2TP
Protocol Type	The protocol type of the service object.	TCP/UDP/ICMP	TCP
Configure Source Port?	Configure the source port if yes.	Enable/Disable	Enable
Port type	The service port type.	Single/Range	Single
Port number	The service port number.	text sting	1701
Configure Destination port	Configure the destination port if any.	Enable/Disable	N/A

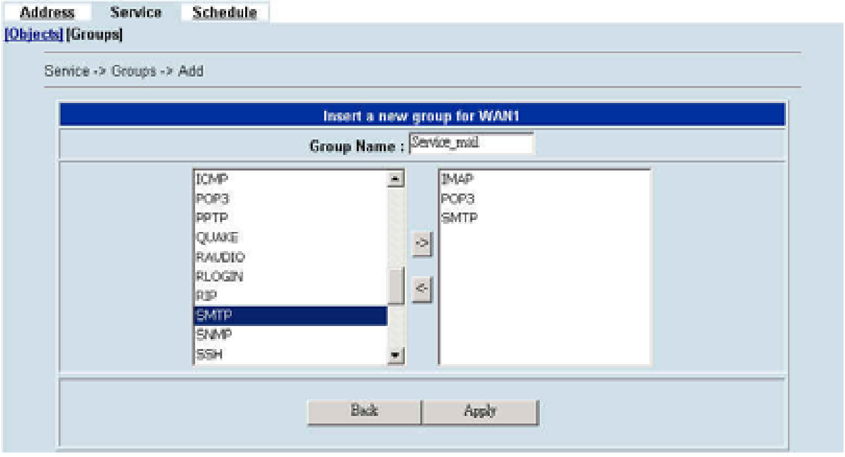
Table 9-5 The field of the Service objects

Step 18. Add a service group

You can create groups of services to make it easier to add rules. A service group can contain predefined services and custom services in any combination. You cannot add service groups to another service group.

Click `Groups` hyperlink, and then click `Insert` to add a new service group. Enter a Group Name to identify the group. Select the services from the available services list and click right arrow to copy them to the Members list. If you would like to remove the services from the members list, just select the services and then click left arrow to remove them.

BASIC SETUP > Books > Service > Groups > Insert



Group Name : Service_mail

ICMP
POP3
PPTP
QUAKE
RAUDIO
RLOGIN
RIP
SMTP
SNMP
SSH

IMAP
POP3
SMTP

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Group Name	The service group name. Note that group name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.	text string	Service_mail
BUTTON	DESCRIPTION		
->	Add the selected address object to the service group.		
<-	Remove the selected address object from service group.		

Table 9-6 Define the services group

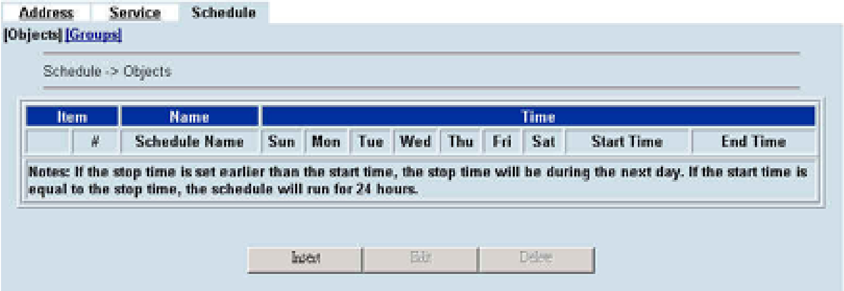
9.4.3 Setup Schedule

Step 19. Schedule Settings

Use scheduling to control when rules are active or inactive.

Select `Insert` to add a new service.

BASIC SETUP > Books > Schedule > Objects



Item		Name	Time								
	#	Schedule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.

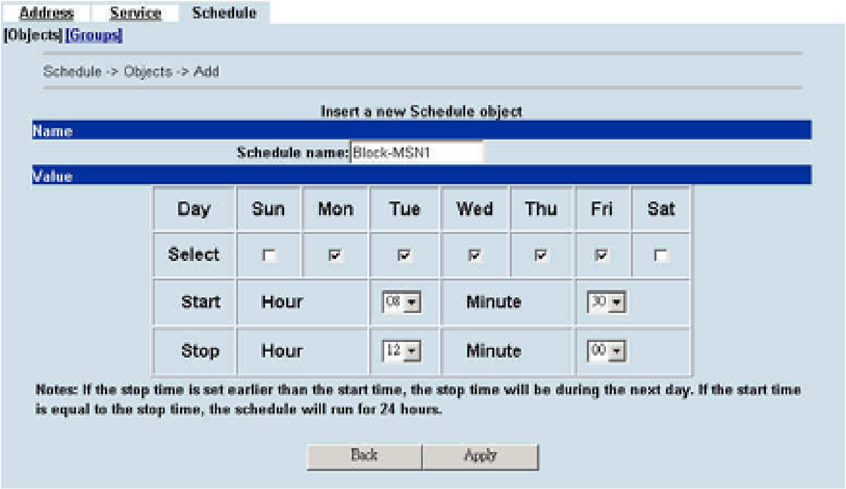
Step 20. Insert a new schedule object

Enter the `Schedule name`. Select the Day you would like to active or inactive a firewall rule, and then select the Start/Stop time. Click `Apply` to add the schedule object.

Suppose using MSN is forbidden in your company from 08:30~12:00, 13:00~17:30 during Monday to Friday, you have to add two schedule ranges (08:30~12:00 and 13:00~17:30) and then group them together in order for your company to make a firewall rule to block the MSN service.

Note that schedule name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.

BASIC SETUP > Books > Address > Schedule > Insert



Insert a new Schedule object

Name

Schedule name: Block-MSN1

Value

Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Select	☐	☑	☑	☑	☑	☑	☐
Start	Hour	08	Minute	30			
Stop	Hour	12	Minute	00			

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Schedule name	The name of the schedule object.	text string	Block-MSN1
Day	The days to active or inactive a firewall rule.	Sun ~ Sat	Mon ~ Fri
Start time	The start time of the schedule object.	24-hour format	08:30

Stop time	The stop time of the schedule object.	24-hour format	12:00

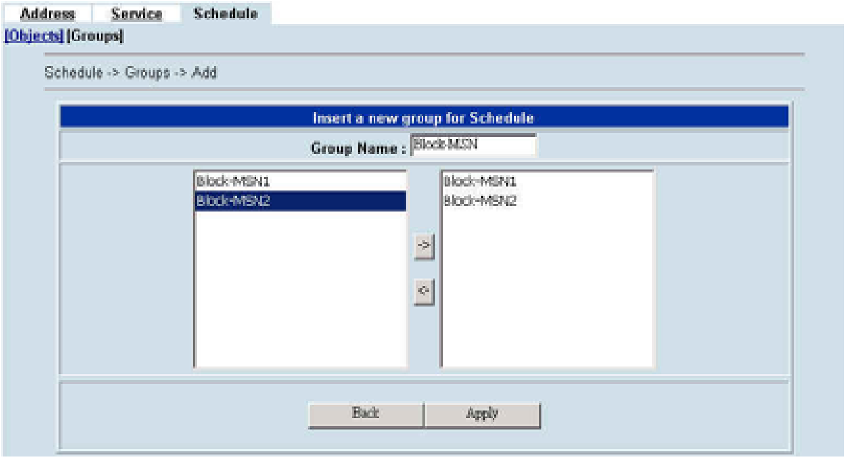
Table 9-7 The field of the Schedule object

Step 21. Add a Schedule group

As Step 2 indicated, you have already created two schedule objects to block the MSN service. You can group them to make it easier to block the MSN service while you would like to make a firewall rule.

Click `Groups` hyperlink, and then click `Insert` to add a new schedule group. Enter a Group Name to identify the group. Select the schedules from the available schedules list and click right arrow to copy them to the Members list. If you would like to remove the schedules from the members list, just select the schedules and then click left arrow to remove them.

BASIC SETUP > Books > Schedule > Groups > Insert



Insert a new group for Schedule

Group Name : Block-MSN

Block-MSN1
Block-MSN2

Block-MSN1
Block-MSN2

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Group Name	The schedule group name. Note that group name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.	text string	Block-MSN
BUTTON	DESCRIPTION		
->	Add the selected address object to the schedule group.		
<-	Remove the selected address object from schedule group.		

Table 9-8 Define the schedule group

Chapter 10
Firewall

This chapter introduces firewall and explains how to implement it.

10.1 Demands

4. Administrators detect that PC1_1 in LAN_1 is doing something that may hurt our company and should instantly block his traffic towards the Internet.
5. A DMZ server was attacked by SYN-Flooding attack and requires the MH-5001 to protect it.

10.2 Objectives

1. Block the traffic from PC1_1 in LAN1 to the Internet in WAN1.
2. Start the SYN-Flooding protection.

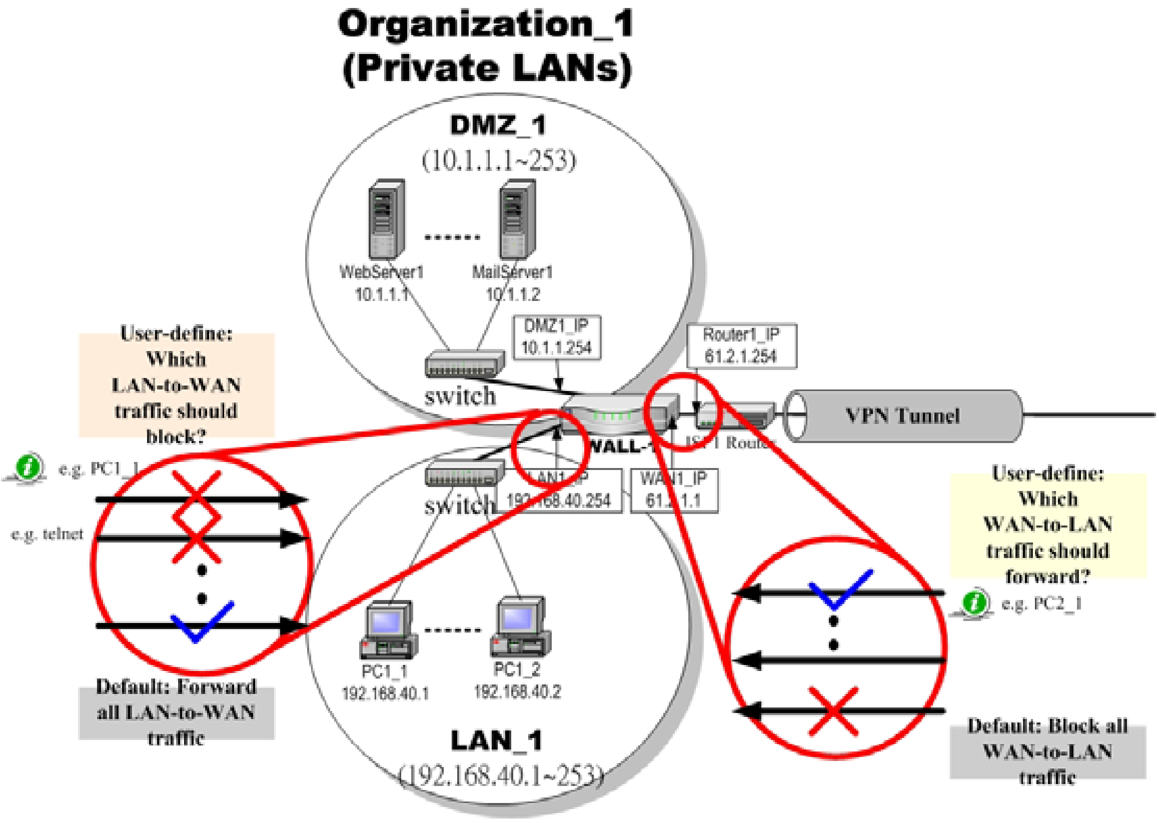


Figure 10-1 Setting up the firewall rule

10.3 Methods

1. Add a LAN1-to-WAN1 Firewall rule to block PC1_1.
2. Start the SYN-Flooding protection by detecting statistical half-open TCP connections.

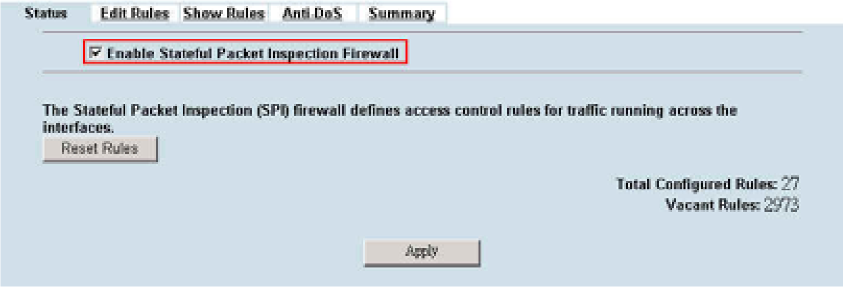
10.4 Steps

10.4.1 Block internal PC session (LAN → WAN)

Step 1. Setup Firewall

Check the `Enable Stateful Inspection Firewall` checkbox, and click the `Apply`.

ADVANCED SETTINGS > Firewall > Status



☑ Enable Stateful Packet Inspection Firewall

The Stateful Packet Inspection (SPI) firewall defines access control rules for traffic running across the interfaces.

Total Configured Rules: 27
Vacant Rules: 2973

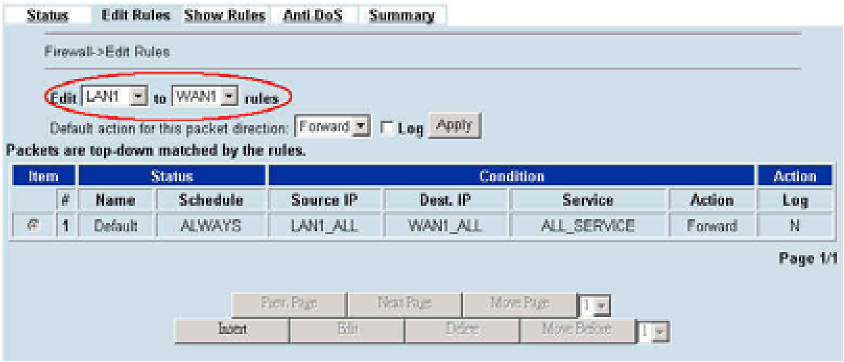
FIELD	DESCRIPTION	Range / Format	EXAMPLE
Enable Stateful Inspection Firewall	Enable Firewall feature of MH-5001	Enabled / Disabled	Enabled
Block all fragment packets	Enable this feature will block the fragmented packets by the firewall of MH-5001. Warning: Enable this feature will cause problem in some applications.	Enabled / Disabled	Disabled
BUTTON	DESCRIPTION		
Reset Rules	Reset Firewall rules to the default status		
Apply	Apply the settings which have been configured.		

Table 10-1 Configure Firewall status

Step 2. Add a Firewall Rule

Select LAN1 to WAN1 traffic direction. The default action of this direction is to forward all traffic without logging anything. Click Insert to add a Firewall block rule before the default rule to stop the bad traffic.

ADVANCED SETTINGS > Firewall > Edit Rules



Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward □ Log

Packets are top-down matched by the rules.

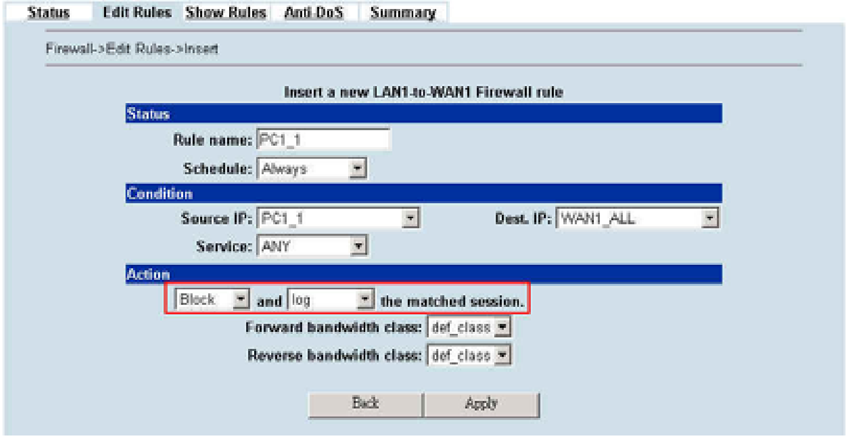
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
◉	1	Default	ALWAYS	LAN1_ALL	WAN1_ALL	ALL_SERVICE	Forward	N

Page 1/1

Step 3. Customize the rule

Check the `Activate this rule` checkbox. Enter the rule name as `PC1_1`, and enter the `IP address` of `PC1_1` (`192.168.40.1 / 255.255.255.255`). Select `Block` and `Log` to block and log the matched traffic. Click the `Apply` to apply the changes.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Insert a new LAN1-to-WAN1 Firewall rule

Status

Rule name: PC1_1

Schedule: Always

Condition

Source IP: PC1_1 Dest. IP: WAN1_ALL

Service: ANY

Action

Block and log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

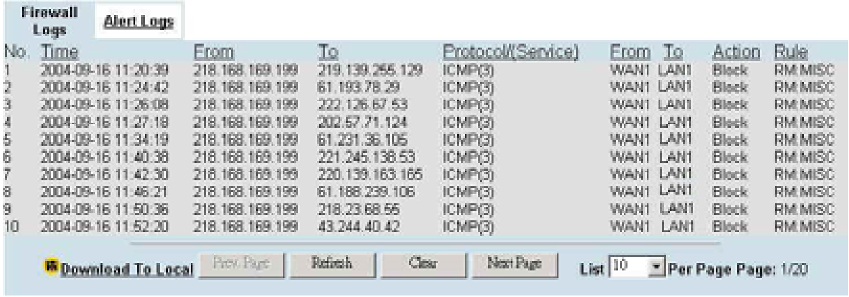
	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Rule name	The name of the Firewall rule. Note that rule name should begin with alphabet, followed by alphabet/digits/dashes.	text string	PC1_1
	Schedule	When does this firewall rule take effect?	All the defined schedule objects and groups	Always
Condition	Source IP	Compared with the incoming packets, whether Source IP is matched or not.	All the defined address objects and groups	PC1_1
	Dest IP	Compared with the incoming packets, whether Dest IP is matched or not.	All the defined address objects and groups	WAN1_ALL
	Service	Verified the service of incoming packet is belong to each TCP、UDP、ICMP.	All the defined service objects and groups	ANY
Action	Forward / Block the matched session	If packet is matched the rule condition, Forward or Block this matched packet?	Forward / Block	Block
	do not log / log the matched session	If packet is matched the rule condition, Log or Don’t log this matched packet?	log / do not log	log
	Forward bandwidth class	About this field description, please refer Table 24-6 Add a new Bandwidth Management rule for more information.		def_class
	Reverse bandwidth class	The same as above field.		def_class

Table 10-2 Insert a Firewall rule

Step 4. View the Firewall Log

You can go to DEVICE Status>Firewall Logs >Firewall Logs to view the firewall logs. If you prefer to download these logs, please click the “Download To Local” button to save the logs to localhost.

DEVICE Status > Firewall Logs > Firewall Logs



No.	Time	From	To	Protocol/(Service)	From	To	Action	Rule
1	2004-09-16 11:20:39	218.168.169.199	219.139.255.129	ICMP(3)	WAN1	LAN1	Block	RM:MISC
2	2004-09-16 11:24:42	218.168.169.199	61.193.78.29	ICMP(3)	WAN1	LAN1	Block	RM:MISC
3	2004-09-16 11:26:08	218.168.169.199	222.126.67.53	ICMP(3)	WAN1	LAN1	Block	RM:MISC
4	2004-09-16 11:27:18	218.168.169.199	202.57.71.124	ICMP(3)	WAN1	LAN1	Block	RM:MISC
5	2004-09-16 11:34:19	218.168.169.199	61.231.36.105	ICMP(3)	WAN1	LAN1	Block	RM:MISC
6	2004-09-16 11:40:38	218.168.169.199	221.245.138.53	ICMP(3)	WAN1	LAN1	Block	RM:MISC
7	2004-09-16 11:42:30	218.168.169.199	220.139.163.165	ICMP(3)	WAN1	LAN1	Block	RM:MISC
8	2004-09-16 11:46:21	218.168.169.199	61.188.239.106	ICMP(3)	WAN1	LAN1	Block	RM:MISC
9	2004-09-16 11:50:36	218.168.169.199	218.23.68.55	ICMP(3)	WAN1	LAN1	Block	RM:MISC
10	2004-09-16 11:52:20	218.168.169.199	43.244.40.42	ICMP(3)	WAN1	LAN1	Block	RM:MISC

List 10 Per Page Page: 1/20

FIELD	DESCRIPTION
No	The indicated firewall log sequence number.
Time	The record time of indicated firewall log.
From	The source IP address which the indicated log event come from.
To	The destination IP address which the indicated log event is bound for.
Protocol/Service	The record log is TCP, UDP or ICMP, and which service it will be.
From	The interface which the indicated log event come from.
To	The interface which the indicated log event is bound for.
Action	The status of indicated firewall log is Block or Forward.
Rule	The log is produced by which firewall rule. “Default” means the default rule of the selected firewall direction. “RM XXX” means the log is produced by remote management function (Almost it is the illegal user who wants to use the Non-Opened remote management functions. Other condition, it will be marked at the rule number (ex. Rule0, Rule1…).

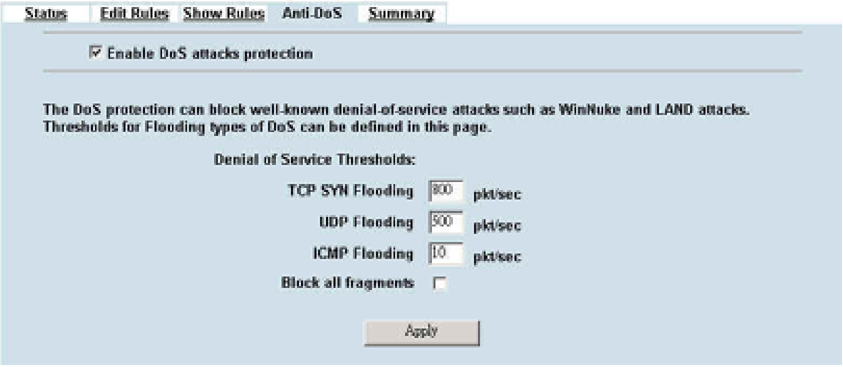
Table 10-3 Firewall log field description

10.4.2 Setup Anti-DoS

Step 5. Setup Anti-DoS

With the `Anti-DoS attacks protection` enabled, the MH-5001 will be equipped with the built-in Anti-DoS engine. Normal DoS attacks will show up in the log when detecting and blocking such traffic. However, Flooding attacks require extra parameters to recognize. Check the `Enable DoS attacks protection` checkbox. And change the value of flooding thresholds as your preference.

ADVANCED SETTINGS > Firewall > Anti-DoS



☑ Enable DoS attacks protection

The DoS protection can block well-known denial-of-service attacks such as WinNuke and LAND attacks. Thresholds for Flooding types of DoS can be defined in this page.

Denial of Service Thresholds:

TCP SYN Flooding 800 pkt/sec

UDP Flooding 500 pkt/sec

ICMP Flooding 10 pkt/sec

Block all fragments ☐

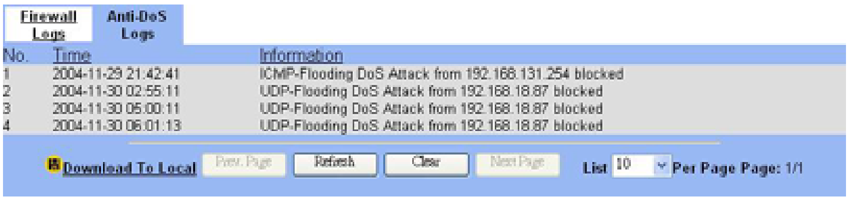
FIELD	DESCRIPTION	EXAMPLE
Enable DoS attacks protection	Enable the Denial of Service (DoS) attack protection. You should enable this to activate any further settings. Notice, the Anti-DoS feature can detect the TCP/UDP/ICMP flooding on each interface of the firewall device.	Enabled
Denial of Service Thresholds		
TCP SYN Flooding	The number of TCP SYN packets that arrive at the same interface will block the further TCP connection attempts.	800
UDP Flooding	The number of UDP packets that arrive at the same interface will block the further arriving UDP packets.	500
ICMP Flooding	The number of ICMP packets that arrive at the same interface will block the further arriving ICMP packets.	10
Block all fragmented packets	When enabled, the firewall will drop any packets that have the fragment bit set in the IP header. This will protect the internal network from fragmented packet attacks. Note that this may cause some applications failure.	disabled

Table 10-4 Setup the thresholds of Anti-DoS

Step 6. View Anti-DoS Logs

While there are any DoS attackts through MH-5001 Firewall, it will block the attacked packets and log it as right diagram.

DEVICE Status > Firewall Logs > Anti-DoS Logs



```
No.  Time                 Information
1    2004-11-29 21:42:41  ICMP-Flooding DoS Attack from 192.168.131.254 blocked
2    2004-11-30 02:55:11  UDP-Flooding DoS Attack from 192.168.18.87 blocked
3    2004-11-30 05:00:11  UDP-Flooding DoS Attack from 192.168.18.87 blocked
4    2004-11-30 06:01:13  UDP-Flooding DoS Attack from 192.168.18.87 blocked
```

Chapter 11
IP / MAC Binding

This chapter introduces how to restrict local pc accessing according to their MAC address

11.1 Demands

Your company would like to protect some servers or users avoid their IP address snatched by others, and control the computers to let them accepted or denied by the IP/MAC rules. IP/MAC binding protects the MH-5001 unit and avoid your network from IP spoofing attacks.

Generally, the IP/MAC Binding will prevent the following usage.

a、 IP spoofing:
IP spoofing attempts to use the IP address of a trusted computer to connect to or through the MH-5001 unit from a different computer. The IP address of a computer can easily be changed to a trusted address, but MAC addresses are added to Ethernet cards at the factory and cannot easily be changed.

b、 Unregistered user accessing:
Through the MAC addresses registering, administrator can prohibit those unregistered addresses passing through MH-5001.

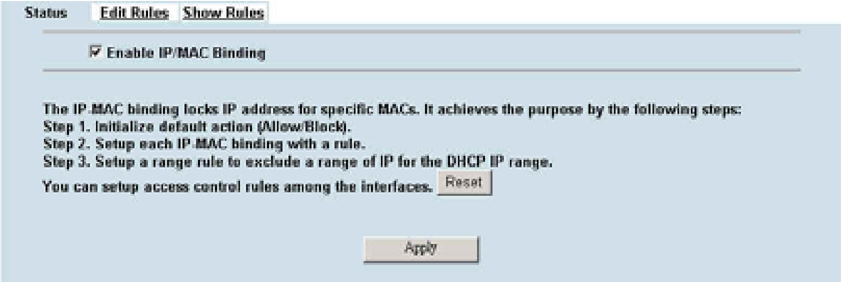
11.2 Objectives

Use this mechanism to permit some specified MAC address passing through MH-5001. Other MAC addresses without permission will be blocked by MH-5001.

11.3 Methods

Binding the specified IP address and MAC address together. And permit the legal one to pass through the MH-5001.

11.4 Steps

Step 7. Enable IP/MAC binding Check the `Enable IP/MAC Binding` checkbox, and then click `Apply` to apply the setting. Note that the IP/MAC binding locks IP address for specific MACs. It achieves the purpose by the steps as right diagram described.	**Advanced Settings > IP/MAC Binding > Status**  ☑ Enable IP/MAC Binding The IP/MAC binding locks IP address for specific MACs. It achieves the purpose by the following steps: Step 1. Initialize default action (Allow/Block). Step 2. Setup each IP/MAC binding with a rule. Step 3. Setup a range rule to exclude a range of IP for the DHCP IP range. You can setup access control rules among the interfaces.

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Enable IP/MAC Binding	Enable IP/MAC Binding feature of MH-5001	Enabled / Disabled	Enabled
BUTTON	**DESCRIPTION**		
Reset	Clear all the predefined IP/MAC binding rules.		

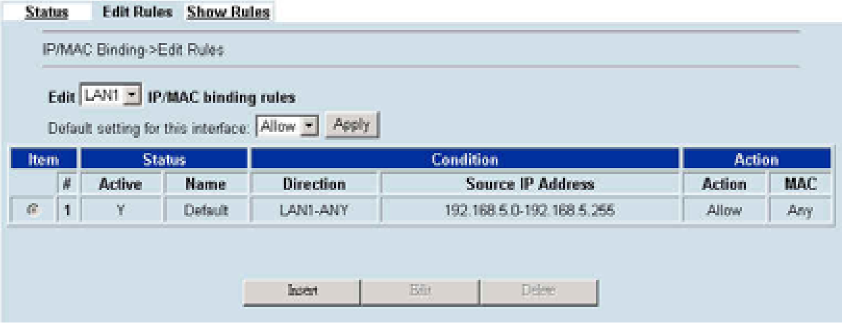
Table 11-1 Enable IP/MAC Binding feature

Step 8. Leave IP/MAC binding “Allow” state

Select `LAN1` as the interface to edit the IP/MAC binding rules. Because we do not add current MAC address of our PC, do not change the Default IP/MAC settings to `Block`. Please keep this state with `Allow` at this moment. And click `Insert` to add a rule.

Note that you have to add an IP/MAC binding rule as `Allow` for your computer to pass the firewall rule before you block the LAN1-ANY direction, otherwise you will be blocked by that rule.

Advanced Settings > IP/MAC Binding > Edit Rules



IP/MAC Binding->Edit Rules

Edit LAN1 IP/MAC binding rules

Default setting for this interface: Allow

Item	Status			Condition		Action	
	#	Active	Name	Direction	Source IP Address	Action	MAC
●	1	Y	Default	LAN1-ANY	192.168.5.0-192.168.5.255	Allow	Any

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Edit __ IP/MAC binding rules	Select the local interface which you are going to configure.	LAN interfaces	LAN1

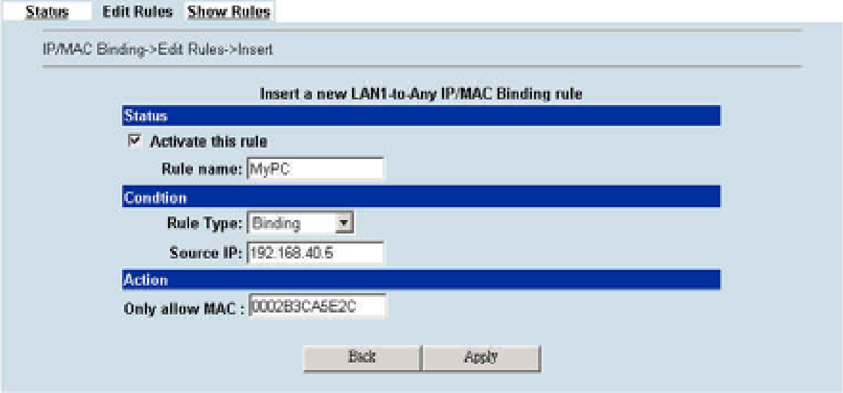
Table 11-2 Select the IP/MAC Binding configured interface

Step 9. Add a new IP/MAC binding rule

Add an IP/MAC binding rule to allow our PC passing through the MH-5001. Otherwise our PC will be blocked by MH-5001 in the further steps.

Here the IP address “192.168.40.5” is the MAC address of our login PC.

Advanced Setting > IP/MAC binding > Edit Rules > Insert



IP/MAC Binding->Edit Rules->Insert

Insert a new LAN1-to-Any IP/MAC Binding rule

Status

☑ Activate this rule

Rule name: MyPC

Condtion

Rule Type: Binding

Source IP: 192.168.40.5

Action

Only allow MAC : 0002B3CA5E2C

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Activate this rule	Activate the IP/MAC binding rule.	Enabled/Disabled	Enabled
Rule name	The name of the IP/MAC binding rule. Note that rule name should begin with alphabet, followed by alphabet/digits/dashes.	text string	MyPC
Rule Type	The type of IP/MAC “Binding” is combined IP address with MAC address together to decide packet is passed or blocked by the MH-5001. Another type of IP/MAC “Allow range” depends on the IP range to permit whether packets can pass or not. For this type, please refer Table 11-4 description.	Binding/Allow Range	Binding

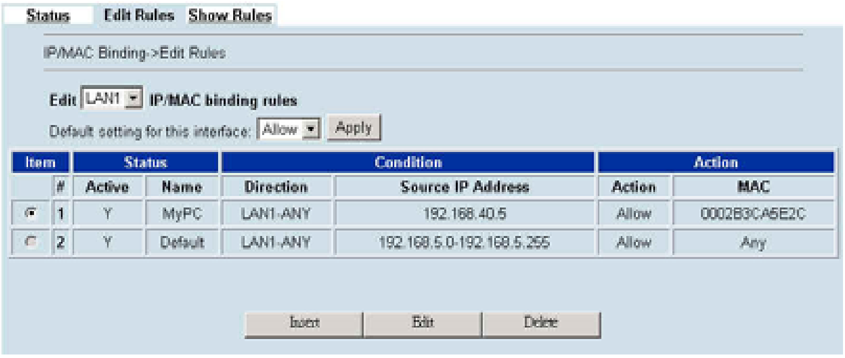
Source IP	The Source IP address which will bound the below MAC address	IPv4 format	192.168.40.5
Only allow MAC	The MAC address which is bound the above IP address.	12 hex characters (valid MAC format)	0002B3CA5E2C

Table 11-3 Add an IP/MAC Binding rule

Step 10. View the results

Through the previous step, you can see the configured result as the right diagram.

Advanced Setting > IP/MAC binding > Edit Rules



IP/MAC Binding->Edit Rules

Edit [LAN1 ▾] IP/MAC binding rules

Default setting for this interface: [Allow ▾] Apply

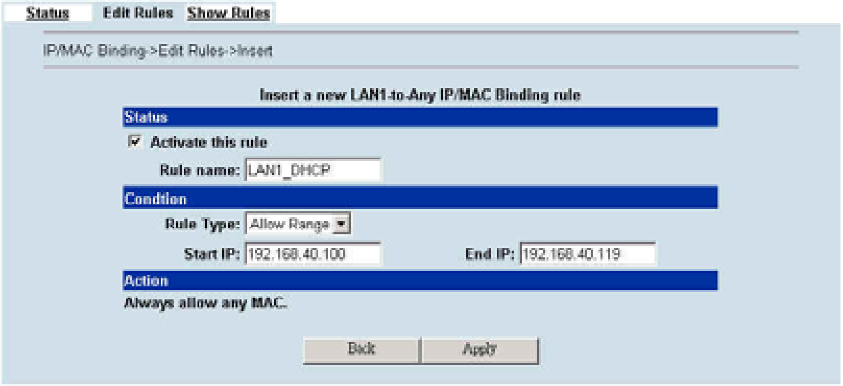
Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Action	MAC
●	1	Y	MyPC	LAN1-ANY	192.168.40.5	Allow	0002B3CA5E2C
○	2	Y	Default	LAN1-ANY	192.168.5.0-192.168.5.255	Allow	Any

Step 11. Add a another new IP/MAC rule

Add another IP/MAC rule to allow an IP address range to pass through MH-5001. This rule type is useful for local PC using DHCP feature specially. Suppose DHCP IP range of LAN1 interface is `192.168.40.100` to `192.168.40.119`.

Check `Activate this rule` checkbox. Enter Rule name as `LAN1_DHCP`. Select `Allow Range` in the Rule Type field, and enter the `Start IP` as `192.168.40.100` and `End IP` as `192.168.40.119`. Click `Apply` to store this setting.

Advanced Setting > IP/MAC binding > Edit Rules > Insert



IP/MAC Binding->Edit Rules->Insert

Insert a new LAN1-to-Any IP/MAC Binding rule

Status

☑ Activate this rule

Rule name: LAN1_DHCP

Condition

Rule Type: [Allow Range ▾]

Start IP: 192.168.40.100 End IP: 192.168.40.119

Action

Always allow any MAC.

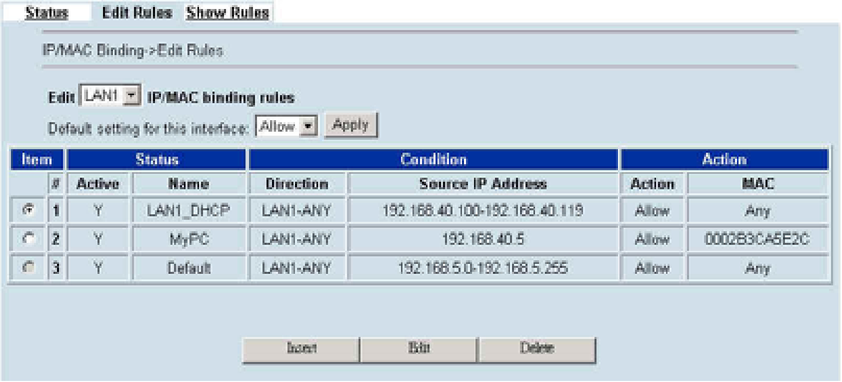
	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Condition	Rule Type	Refer to Table 11-3 for this field description.	Binding/Allow Range	Allow Range
	Source IP	The starting IP address of "IP allowed range".	IPv4 format	192.168.40.100
	End IP	The final IP address of "IP allowed range".	IPv4 format	192.168.40.119

Table 11-4 Add an IP/MAC allow range rule

Step 12. Change the IP/MAC binding to "Block"

Through the previous steps, we have configured two IP/MAC rules for allowing passing through MH-5001. In this step, we will change the IP/MAC binding status to "Block" to prohibit invalid IP address to pass through MH-5001.

Advanced Settings > IP/MAC Binding > Edit Rules



IP/MAC Binding->Edit Rules

Edit LAN1 IP/MAC binding rules

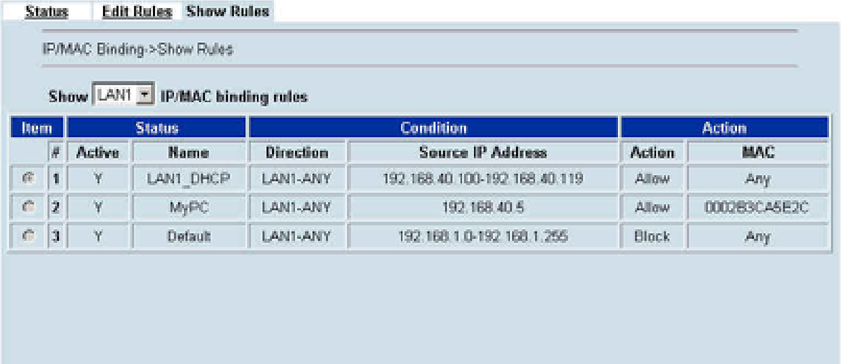
Default setting for this interface: Allow Apply

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Action	MAC
●	1	Y	LAN1_DHCP	LAN1-ANY	192.168.40.100-192.168.40.119	Allow	Any
○	2	Y	MyPC	LAN1-ANY	192.168.40.5	Allow	0002B3CA5E2C
○	3	Y	Default	LAN1-ANY	192.168.5.0-192.168.5.255	Allow	Any

Step 13. Show the IP/MAC binding rule

After finishing the setting, you can view the result as the right diagram shown.

Advanced Setting > IP/MAC binding > Show Rules



IP/MAC Binding->Show Rules

Show LAN1 IP/MAC binding rules

Item		Status		Condition		Action	
	#	Active	Name	Direction	Source IP Address	Action	MAC
●	1	Y	LAN1_DHCP	LAN1-ANY	192.168.40.100-192.168.40.119	Allow	Any
○	2	Y	MyPC	LAN1-ANY	192.168.40.5	Allow	0002B3CA5E2C
○	3	Y	Default	LAN1-ANY	192.168.1.0-192.168.1.255	Block	Any

Chapter 12
VPN Technical Introduction

This chapter introduces VPN related technology

12.1 VPN benefit

If you choose to implement VPN technology in your enterprise, then it may bring the following benefits to your company.

1. Authentication

Ensure the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender.

2. Integrity

Ensure that data is transmitted from source to destination without undetected alteration.

3. Confidentiality

Guarantee the intended recipients know what was being sent but unintended parties cannot determine what was sent. This is almost provided by data encryption.

4. Non-repudiation

The receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data.

12.2 Related Terminology Explanation

12.2.1 VPN

A VPN (Virtual Private Network) logically provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of encryption, tunneling, authentication, and access control used to transport traffic over the Internet or any insecure TCP/IP networks.

12.2.2 IPSec

Internet Protocol Security (IPSec) is a standard-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

12.2.3 Security Association

A Security Association (SA) is an agreement between two parties indicating what security parameters, such as keys and algorithms they will use.

12.2.4 IPSec Algorithms

There are two types of the algorithms in the IPSec, including (1) Encryption Algorithms such as DES (Data Encryption Standard), and 3DES (Triple DES) algorithms, and (2) Authentication Algorithms such as HMAC-MD5 (RFC 2403), and HMAC-SHA1 (RFC 2404).

12.2.5 Key Management

Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to setup a VPN.

➢ IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange established an IKE SA and the second one uses that SA to negotiate SAa for IPSec.

In phase 1 you must：

- Choose a negotiation mode
- Authenticate the connection by entering a pre-shared key
- Choose an encryption algorithm
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group (DH1 or DH2).
- Set the IKE SA lifetime. This field allows you to determine how long IKE SA negotiation should proceed before it times out. A value of 0 means IKE SA negotiation never times out. If IKE SA negotiation times out, then both IKE SA and IPSec SA must be renegotiated.

In phase 2 you must：

- Choose which protocol to use (ESP or AH) for the IKE key exchange
- Choose an encryption algorithm
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Security (PFS) using Diffie-Hellman public-key cryptography
- Choose Tunnel mode or Transport mode
- Set the IPSec SA lifetime. This field allows you to determine how long IPSec SA setup should proceed before it times out. A value of 0 means IPSec SA never times out. If IPSec SA negotiation times out, then the IPSec SA must be renegotiated (but not the IKE SA).

➢ Negotiation Mode

The phase 1 Negotiation Mode you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- Main Mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips (SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number)). This mode features identity protection (your identity is not revealed in the negotiation).
- Aggressive Mode is quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that fast speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situation where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

➢ Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

➢ Diffie-Hellman (DH) Key Groups.

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 – DH1) and 1024-bit (Group 2 – DH2) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

- Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (None) by default in the MH-5001. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

12.2.6 Encapsulation

- Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packets. In Transport mode, the IP packets contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contains in the packet (such as TCP and UDP).

With ESP, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of AH as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

- Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A Tunnel mode is required for gateway services to provide access to internal system. Tunnel mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. Tunnel mode is required for gateway to gateway and host to gateway communications. Tunnel mode communication have two sets of IP headers：

- Outside header： The outside IP header contains the destination IP address of the VPN gateway.
- Inside header： The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

12.2.7 IPSec Protocols

The ESP and AH protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by AH and ESP protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

- AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed.

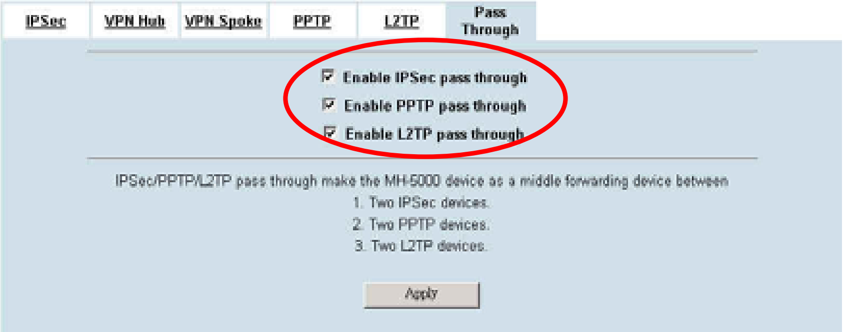
In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an AH can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

- ESP (Encapsulating Security Payload) Protocol

The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. ESP authenticating properties are limited compared to the AH due to the non-inclusion of the IP header information during the authentication process. However, ESP is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the ESP is payload padding, which further protects communications by concealing the size of the packet being transmitted.

12.3 Make VPN packets pass through MH-5001

Step 1. Enable IPSec If we need to setup MH-5001 between the existed IPSec / PPTP / L2TP connections. We need to open up the Firewall blocking port of MH-5001 in advance. Here we provide a simple way. You can through enable the `IPSec / PPTP / L2TP pass through` checkbox on this page. Then the VPN connections of IPSec / PPTP / L2TP will pass through MH-5001. As well as MH-5001 will play the middle forwarding device role.	**ADVANCED SETTINGS > VPN Settings > Pass Through**  ☑ Enable IPSec pass through ☑ Enable PPTP pass through ☑ Enable L2TP pass through IPSec/PPTP/L2TP pass through make the MH-5000 device as a middle forwarding device between 1. Two IPSec devices. 2. Two PPTP devices. 3. Two L2TP devices. IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through Apply

Chapter 13
Virtual Private Network – IPSec

This chapter introduces IPSec VPN and explains how to implement it.

As described in the Figure 2-1, we will extend to explain how to make a VPN link between LAN_1 and LAN_2 in this chapter. The following Figure 13-1 is the real structure in our implemented process.

13.1 Demands

1. When a branch office subnet LAN_1 wants to connect with another branch office subnet LAN_2 through the public Internet instead of the expensive private leased lines, VPN can provide encryption and authentication to secure the tunnel that connects these two LANs.

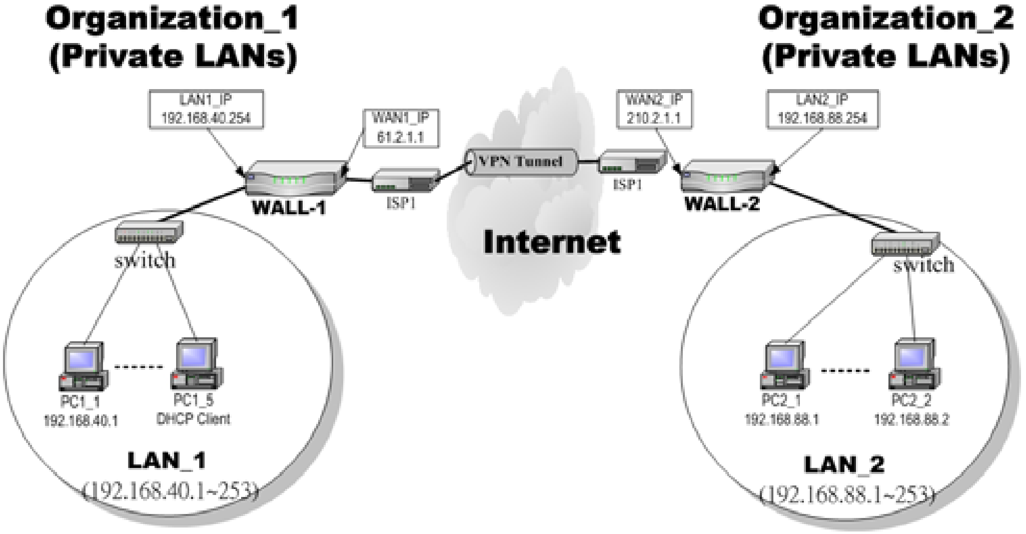


Figure 13-1 Organization_1 LAN_1 is making VPN tunnel with Organization_2 LAN_2

13.2 Objectives

1. Let the users in LAN_1 and LAN_2 share the resources through a secure channel established using the public Internet.

13.3 Methods

1. Separately configure WALL-1 and WALL-2, the two MH-5001, which are the edge gateways of LAN_1 and LAN_2 respectively. You have to determine a key management method between IKE (Internet Key Exchange) and Manual Key. The following table compares the settings between IKE and Manual Key. In the following, we will describe them separately.

	IKE	Manual Key

Same	"Local Address" means the local LAN subnet; "Remote Address" means the remote LAN subnet; "My IP Address" means the WAN IP address of the local VPN gateway while the "Peer's IP Address" means the WAN IP address of the other VPN gateway.	
Difference	The "Pre-Shared Key" must be the same at both MH-5001s.	The types and keys of "Encryption" and "Authenticate" must be set the same on both MH-5001s. However, the "Outgoing SPI" at WALL-1 must equal to "Incoming SPI" at WALL-2, and the "Outgoing SPI" at WALL-2 must equal to "Incoming SPI" at WALL-1.

Table 13-1 Compared IKE and Manual Key methods

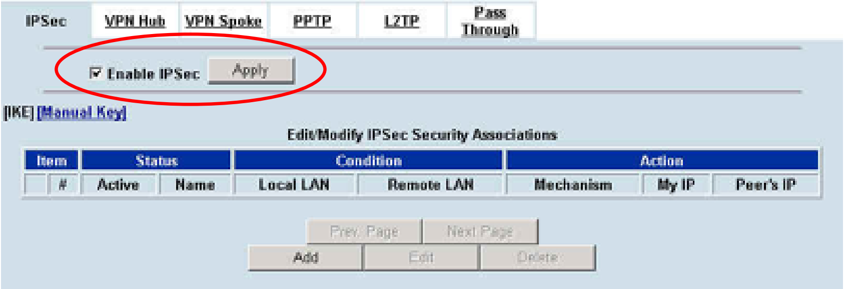
13.4 Steps

In the following we will separately explain the ways to set up a secure DES/MD5 tunnel with IKE and Manual key.

➢ DES/MD5 IPSec tunnel: the IKE way

At WALL-1:

At the first, we will install the IPSec properties of WALL-1.

Step 1. Enable IPSec Check the `Enable IPSec` checkbox and click `Apply`.	**ADVANCED SETTINGS > VPN Settings > IPSec** 

Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

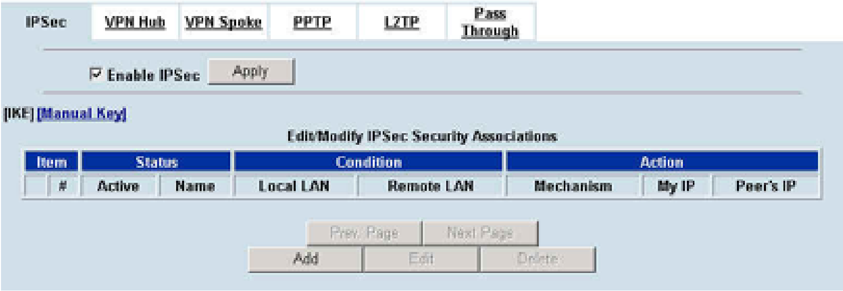
FIELD	DESCRIPTION	EXAMPLE
Enable IPSec	Enable IPSec feature of MH-5001	Enabled
BUTTON	DESCRIPTION	
Apply	Apply the settings which have been configured.	

Table 13-2 Enable the IPSec feature

Step 2. Add an IKE rule

Click the IKE hyperlink and click Add to add a new IPSec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE



☑ Enable IPSec

Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

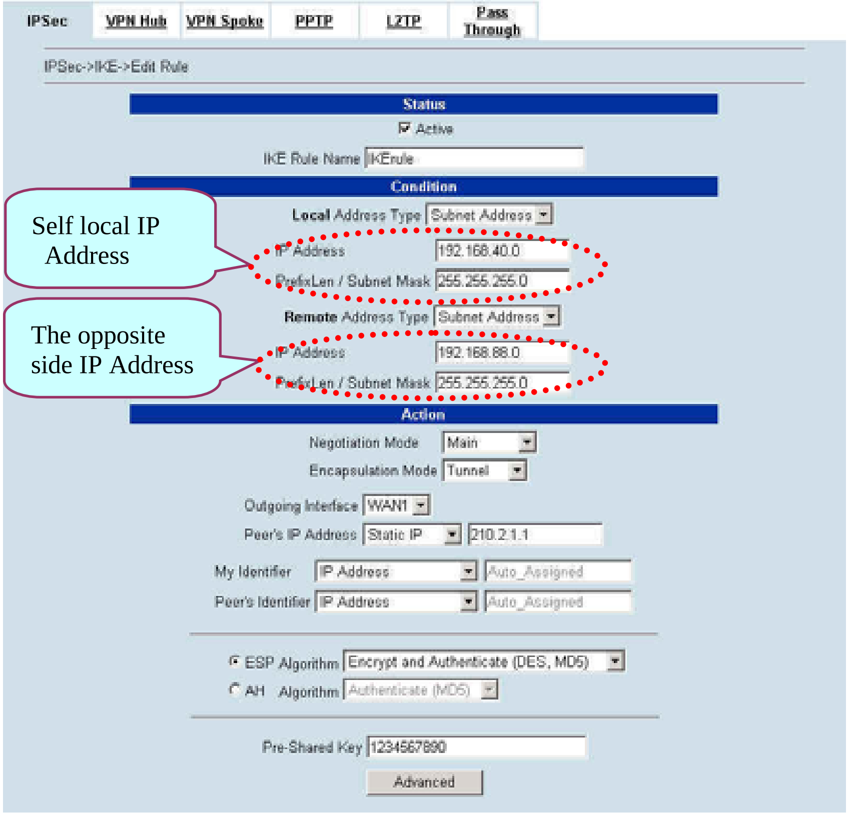
FIELD	DESCRIPTION	EXAMPLE
IKE	Use the IKE (Internet Key Exchange) method to negotiate the key used in building IPSec tunnel.	Selected
Manual Key	Use the key which you have been designated to build IPSec tunnel in peer VPN device.	Non selected
BUTTON	DESCRIPTION	
Prev. Page	If there are more than one action pages, you can press Prev. Page to back to the previous page.	
Next Page	If there are more than one action pages, you can press Next Page to go to the next page.	
Add	Insert a new IPSec rule.	
Edit	Edit the properties of the indicated IPSec rule.	
Delete	Delete the indicated IPSec rule.	

Table 13-3 Add an IPSec policy rule

Step 3. Customize the rule

Check the Active checkbox. Enter a name for this rule like IKErule. Enter the Local IP Address (192.168.40.0/255.255.255.0) and the Remote IP Address (192.168.88.0/255.255.255.0). Select the Outgoing Interface of this Multi-Homing Security Gateway. Enter the public IP of the opposite-side VPN gateway (210.2.1.1) in the Peer’s IP Address. Click the ESP Algorithm and select Encrypt and Authenticate (DES, MD5). Enter the Pre-Shared Key as 1234567890. Click the Apply button to store the settings. Note, In the Action region. It should choose either ESP Algorithm or AH Algorithm, or system will show error message. If you hope to set the detailed item of IKE parameter. Click the Advanced button in this page. Otherwise it is ok to just leave the value default.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



☑ Active

IKE Rule Name: IKErule

Local Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Negotiation Mode: Main

Encapsulation Mode: Tunnel

Outgoing Interface: WAN1

Peer's IP Address: Static IP 210.2.1.1

My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890

Self local IP Address

The opposite side IP Address

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Active	This field will activate this IPSec policy rule	Enable/Disable	Enabled
	IKE Rule Name	The name of this IPSec policy	text string (Max: 256 entries)	IKErule
Condition	Local Address Type	Determine the method to connect to the remote side of VPN by using the local subnet or the local single host.	Subnet Address / Single Address	Subnet Address
	IP Address	The local IP address	IPv4 format	192.168.40.0
	Prefix Len/Subnet Mask	The local IP Netmask	IPv4 format	255.255.255.0
	Remote Address Type	Determine the method to connect to the local side of VPN by using the remote subnet or the remote single host.	Subnet Address / Single Address	Subnet Address
	IP Address	The remote IP address	IPv4 format	192.168.88.0
	Prefix Len/Subnet Mask	The remote IP Netmask	IPv4 format	255.255.255.0
Action	Negotiation Mode	Choose Main or Aggressive mode, see Chapter 12 for details.	Main / Aggressive	Main
	Encapsulation Mode	Choose Tunnel or Transport mode, see Chapter 12 for details.	Tunnel / Transport	Tunnel

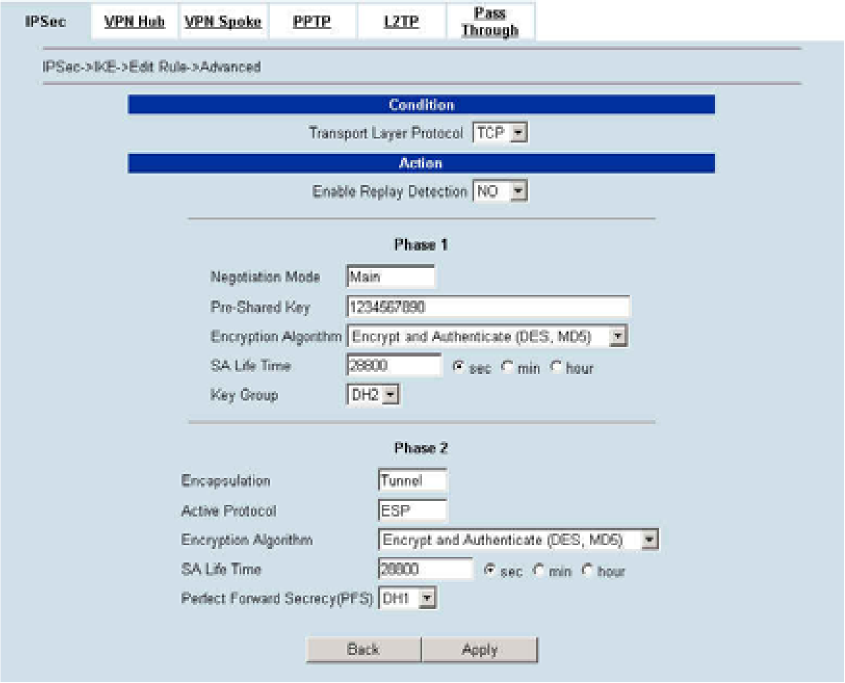
	Outgoing Interface	The WAN interface you are going to build IPSec tunnel with.	WAN interfaces	WAN1
	Peer’s IP Address	The IP address of remote VPN device. The IP address may be fixed (Static) or dynamic.	Static IP / Dynamic IP	Static IP 210.2.1.1
	My Identifier	Fill your information in this field. The filled information will be provided for the IPSec tunnel establishment.	IP Address / FQDN (domain name) / User FQDN (mail box)	IP Address
	Peer’s Identifier	Fill the information of peer VPN device in this field. The filled information will be provided for the IPSec tunnel establishment.	IP Address / FQDN (domain name) / User FQDN (mail box)	IP Address
	ESP Algorithm	ESP Algorithm may be grouped by the items of the Encryption and Authentication Algorithms or execute separately. We can select below items, the Encryption and Authentication Algorithm combination or the below item Authentication Algorithm singly. Here Encryption Algorithms include DES(64 bits), 3DES(192 bits) and AES(128/192/256 bits) Authentication Algorithms include MD5(128 bits) and SHA1(160 bits)	Encrypt and Authenticate (DES, MD5) / Encrypt and Authenticate (DES, SHA1) / Encrypt and Authenticate (3DES, MD5) / Encrypt and Authenticate (3DES, SHA1) / Encrypt and Authenticate (AES, MD5) / Encrypt and Authenticate (AES, SHA1) / Encrypt only (DES) / Encrypt only (3DES) / Encrypt only (AES) / Authenticate only (MD5) / Authenticate only (SHA1)	Encrypt and Authenticate (DES, MD5)
	AH Algorithm	Select Authentication Algorithm	Authenticate (MD5) / Authenticate (SHA1)	Disabled
	Pre-Shared Key	The key which is pre-shared with remote side.	text string	1234567890

Table 13-4 Related field explanation of adding an IPSec policy rule

Step 4. Detail settings of IPSec IKE

In this page, we will set the detailed value of IKE parameter. Fill in the related field as Table 13-5 indicated to finish these settings.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add > Advanced



IPSec->IKE->Edit Rule->Advanced

Condition

Transport Layer Protocol: TCP

Action

Enable Replay Detection: NO

Phase 1

Negotiation Mode: Main

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Key Group: DH2

Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Perfect Forward Secrecy(PFS): DH1

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Condition	Transport Layer Protocol	Utilize this field to select some packets which are specified protocol (ANY, TCP, UDP). If the packets are not the specified protocol will not be allowed to pass through IPSec tunnels.	ANY / TCP / UDP	TCP
Action	Enable Replay Detection	Whether is the “Replay Detection” enabled?	NO / YES	NO
	Phase1			
	Negotiation Mode	View only, it is set previously and can not be edited again.	Can not be edited	Main
	Pre-Shared Key	View only, it is set previously and can not be edited again.	Can not be edited	1234567890
	Encryption Algorithm	Choose a type of encryption and authentication algorithm combination.	Encrypt and Authenticate (DES, MD5) / Encrypt and Authenticate (DES, SHA1) / Encrypt and Authenticate (3DES, MD5) / Encrypt and Authenticate (3DES, SHA1)	Encrypt and Authenticate (DES、MD5)
	SA Life Time	Set the IKE SA lifetime. A value of 0 means IKE SA negotiation never times out. See Chapter 12 for details.	0~86400000 sec 0~1440000 min 0~24000 hour	28800 sec

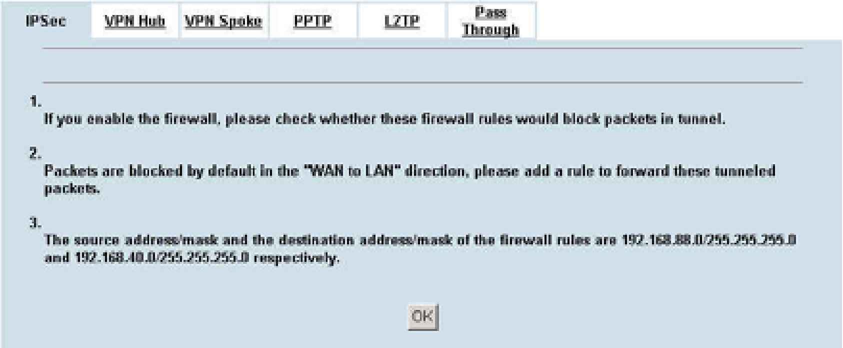
	Key Group	Choose a Diffie-Hellman public-key cryptography key group	DH1 / DH2 / DH5	DH2
	Phase2			
	Encapsulation	View only, it is set previously and can not be edited again.	Can not be edited	Tunnel
	Active Protocol	View only, it is set previously and can not be edited again.	Can not be edited	ESP
	Encryption Algorithm	Choose a type of encryption and authentication algorithm combination or singly.	Encrypt and Authenticate (DES, MD5) / Encrypt and Authenticate (DES, SHA1) / Encrypt and Authenticate (3DES, MD5) / Encrypt and Authenticate (3DES, SHA1) / Encrypt and Authenticate (AES, MD5) / Encrypt and Authenticate (AES, SHA1) / Encrypt only (DES) / Encrypt only (3DES) / Encrypt only (AES) / Authenticate only (MD5) / Authenticate only (SHA1)	Encrypt and Authenticate (DES、MD5)
	SA Life Time	Set the IPSec SA lifetime. A value of 0 means IKE SA negotiation never times out. See Chapter 12 for details.	0~86400000 sec 0~1440000 min 0~24000 hour	28800 sec
	Perfect Forward Secrecy(PFS)	Enabling PFS means that the key is transient. This extra setting will cause more security.	None / DH1 / DH2 / DH5	DH1

Table 13-5 Setup Advanced feature in the IPSec IKE rule

Step 5. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the OK button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



1. If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

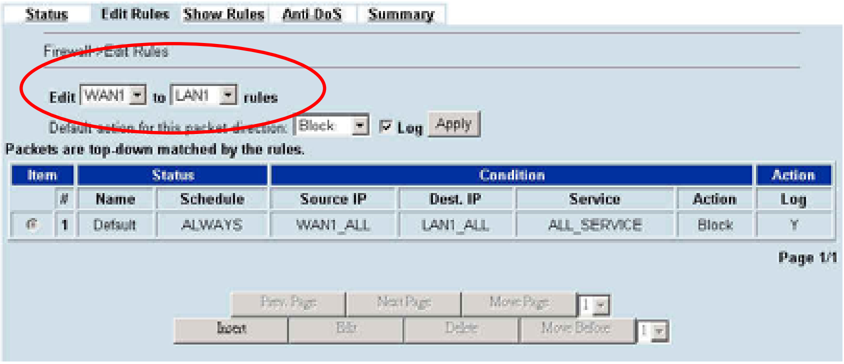
2. Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

3. The source address/mask and the destination address/mask of the firewall rules are 192.168.88.0/255.255.255.0 and 192.168.40.0/255.255.255.0 respectively.

Step 6. Add a Firewall rule

Beforehand, please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log

Packets are top-down matched by the rules.

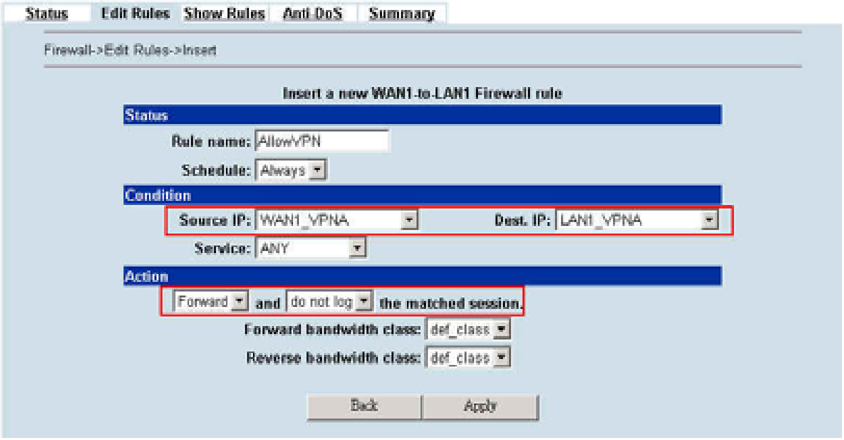
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 7. Customize the Firewall rule

Check the Activate this rule. Enter the Rule Name as AllowVPN, Source IP as WAN1_VPNA (192.168.88.0), and Dest. IP as LAN1_VPNA (192.168.40.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNA Dest. IP: LAN1_VPNA

Service: ANY

Action

Forward and do not log the matched session.

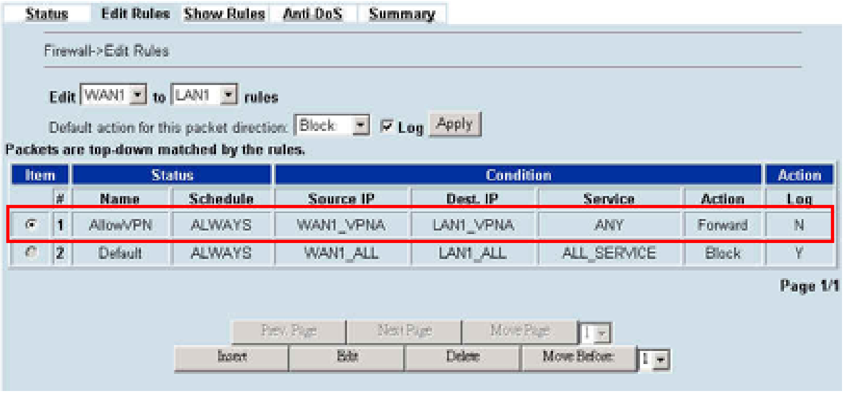
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through MH-5001. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNA	LAN1_VPNA	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

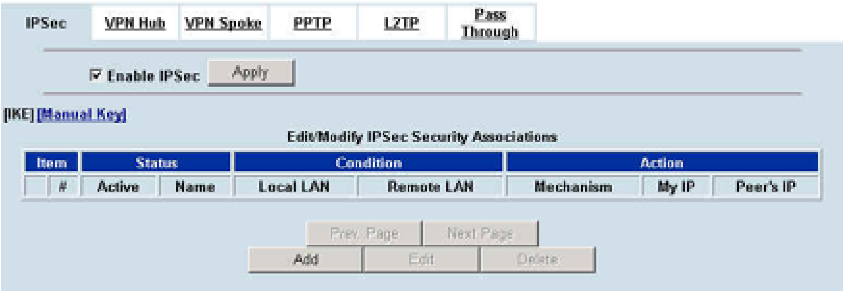
At WALL-2:

Here we will install the IPSec properties of WALL-2. Note that the “Local Address” and “Remote address” field are opposite to the WALL-1, and so are “My IP Address” and “Peer’s IP Address” field.

Step 1. Enable IPSec

Check the `Enable IPSec` checkbox and click `Apply`.

ADVANCED SETTINGS > VPN Settings > IPSec

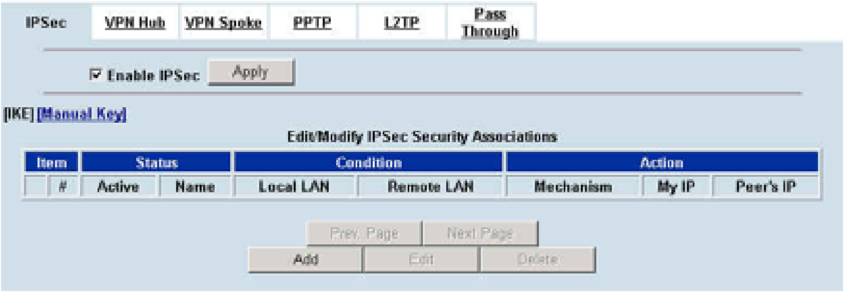


☑ Enable IPSec

Step 2. Add an IKE rule

Click the `IKE` hyperlink and click Add to add a new IPSec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE

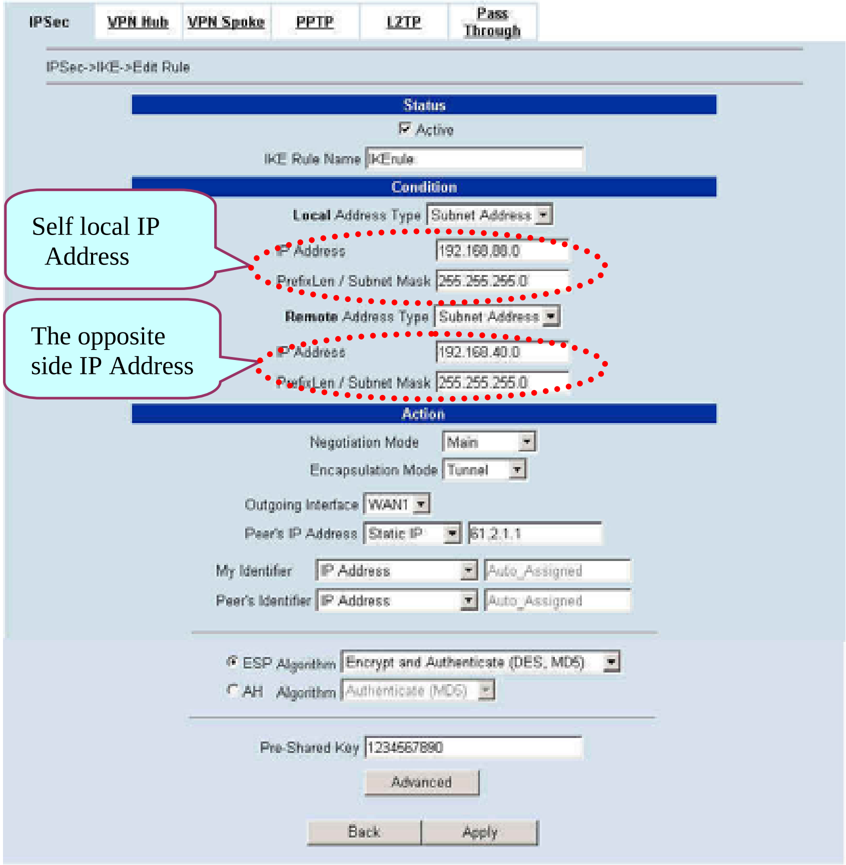


☑ Enable IPSec

Step 3. Customize the rule

Check the `Active` checkbox. Enter a name for this rule like `IKErule`. Enter the `Local IP Address` (`192.168.88.0/255.255.255.0`) and the `Remote IP Address` (`192.168.40.0/255.255.255.0`). Select the `Outgoing interface` of this Multi-Homing Security Gateway. Enter the public IP of the opposite-side VPN gateway (`61.2.1.1`) in the `Peer's IP Address`. Click the ESP `Algorithm` and select `Encrypt and Authenticate (DES, MD5)`. Enter the `Pre-Shared Key` as `1234567890`. Click the `Apply` button to store the settings. Note, in the Action region, you should choose either ESP Algorithm or AH Algorithm, or system will show error message.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



IPSec->IKE->Edit Rule

☑ Active

IKE Rule Name: IKErule

Local Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Negotiation Mode: Main

Encapsulation Mode: Tunnel

Outgoing Interface: WAN1

Peer's IP Address: Static IP 61.2.1.1

My Identifier: IP Address Auto_Assigned

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890

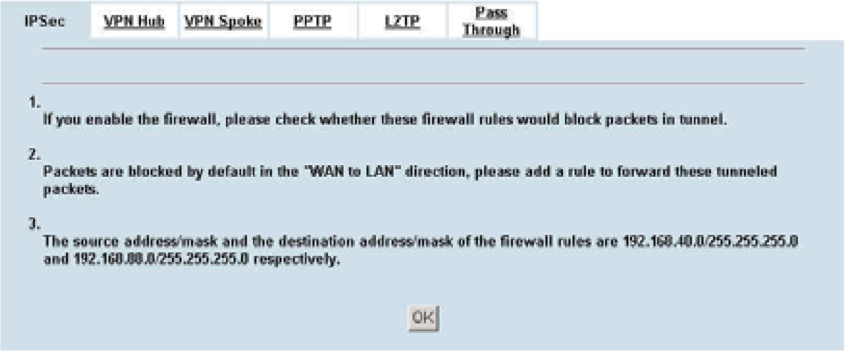
Self local IP Address

The opposite side IP Address

Step 4. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the OK button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



1. If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

2. Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

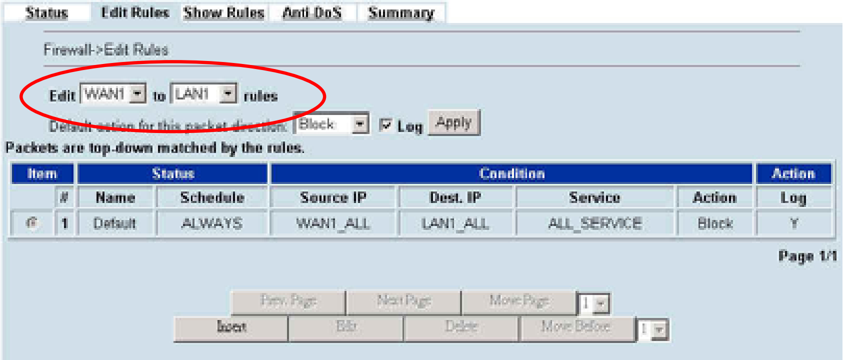
3. The source address/mask and the destination address/mask of the firewall rules are 192.168.40.0/255.255.255.0 and 192.168.88.0/255.255.255.0 respectively.

OK

Step 5. Add a Firewall rule

Same as at WALL-1. We need to add an extra firewall rule to allow IPSec packets to come from Internet. So here we select `WAN1-to-LAN1` direction, and click `Insert` button.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

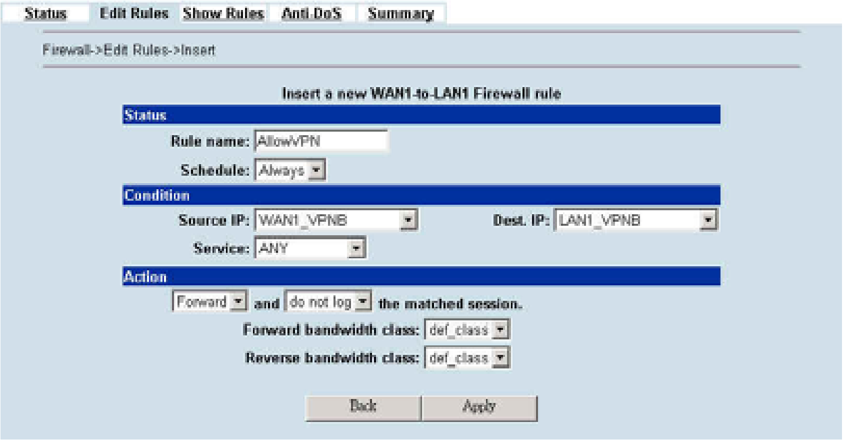
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
◉	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 6. Customize the Firewall rule

Check the `Activate this rule`. Enter the `Rule Name` as `AllowVPN`, `Source IP` as `WAN1_VPNB (192.168.40.0)`, and `Dest. IP` as `LAN1_VPNB (192.168.88.0)`. Click `Apply` to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNB Dest. IP: LAN1_VPNB

Service: ANY

Action

Forward and do not log the matched session.

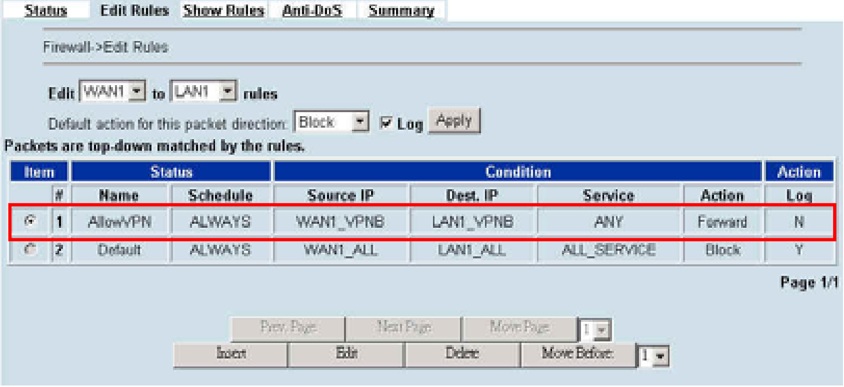
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from `192.168.40.0/24` to `192.168.88.0/24` will be allowed to pass through the MH-5001 and successfully access the `192.168.88.0/24` through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNB	LAN1_VPNB	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

➢ DES/MD5 IPSec tunnel: the Manual-Key way

In the previous section, we have introduced IKE method. Here we will introduce another method using Manual-Key way instead of IKE to install WALL-1.

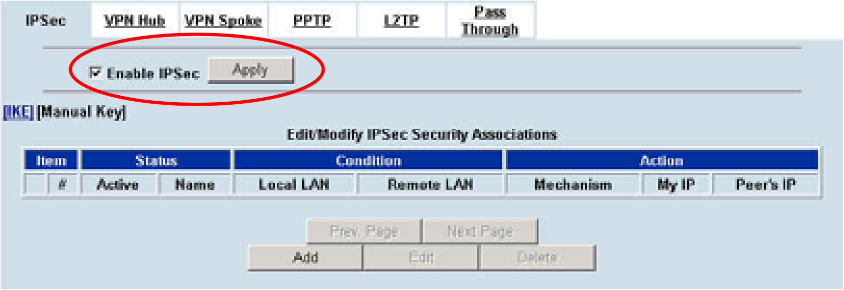
At WALL-1:

At the first, we will use the Manual-Key way to install the IPSec properties of WALL-1.

Step 1. Enable IPSec

Check the `Enable IPSec` checkbox and click `Apply`.

ADVANCED SETTINGS > VPN Settings > IPSec



☑ Enable IPSec Apply

[IKE] [Manual Key]

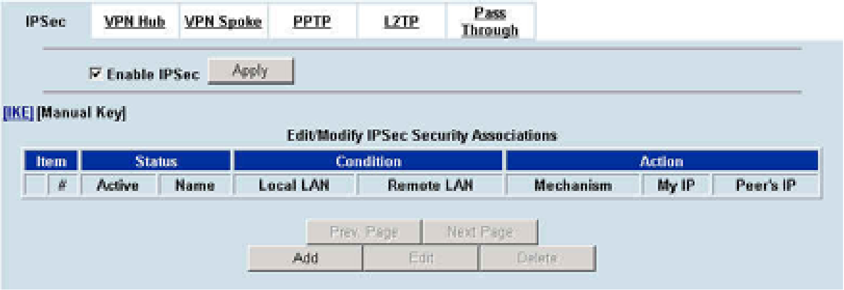
Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 2. Add a Manual Key rule

Click the `Manual Key` hyperlink and click Add to add a new IPSec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key



☑ Enable IPSec Apply

[IKE] [Manual Key]

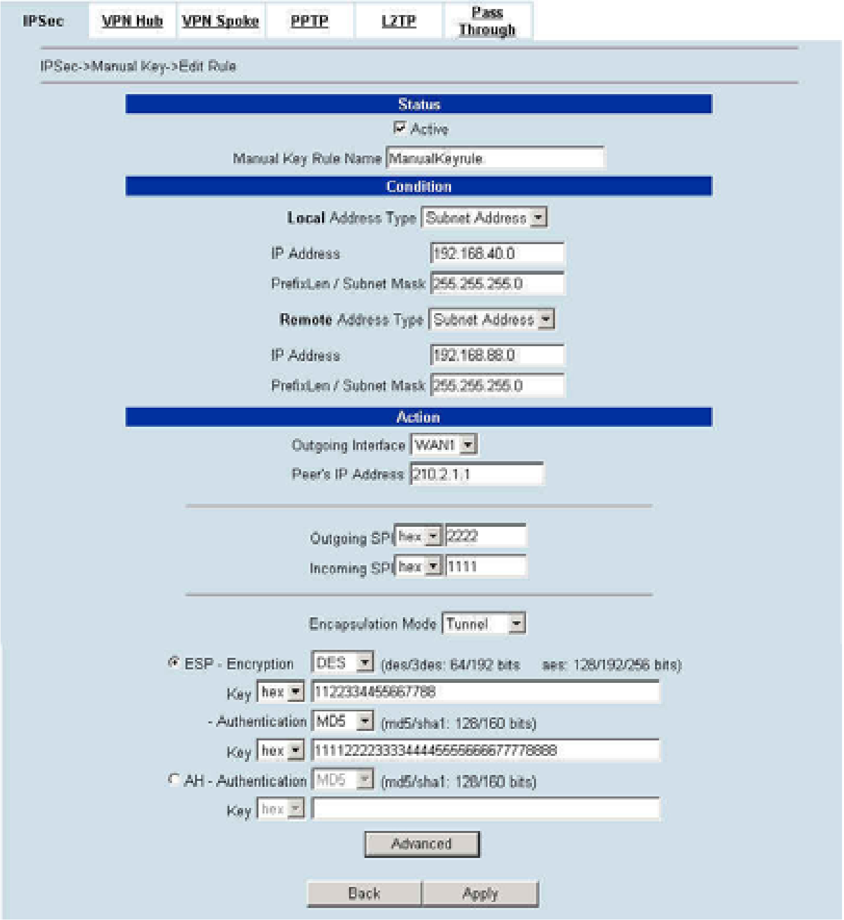
Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 3. Customize the rule

Same as those in IKE. But there is no pre-shared key in the manual-key mode. Enter the `Key` for encryption, such as `1122334455667788`. Enter the `Key` for authentication, such as `11112222333344445555666677778888`. Additionally, the `Outgoing SPI` and `Incoming SPI` have to be manually specified. Enter `2222` and `1111` respectively to the `Outgoing SPI` and the `Incoming SPI`. Click `Apply` to store the rule.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add



IPSec->Manual Key->Edit Rule

Status

☑ Active

Manual Key Rule Name: ManualKeyrule

Condition

Local Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Action

Outgoing Interface: WAN1

Peer's IP Address: 210.2.1.1

Outgoing SPI: hex 2222

Incoming SPI: hex 1111

Encapsulation Mode: Tunnel

● ESP - Encryption: DES (des/3des: 64/192 bits aes: 128/192/256 bits)

Key: hex 1122334455667788

- Authentication: MD5 (md5/sha1: 128/160 bits)

Key: hex 11112222333344445555666677778888

○ AH - Authentication: MD5 (md5/sha1: 128/160 bits)

Key: hex

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Status	Active	This field will activate this IPSec policy rule	Enable / Disable	Enabled
	Manual Key Rule Name	The name of this IPSec policy	text string (Max: 2000 entries)	ManualKeyrule
Condition	Local Address Type	Determine the method to connect to the remote side of VPN by using the local subnet or the local single host.	Subnet Address / Single Address	Subnet Address
	IP Address	The local IP address	IPv4 format	192.168.40.0
	PrefixLen / Subnet Mask	The local IP Netmask	IPv4 format	255.255.255.0
	Remote Address Type	Determine the method to connect to the local side of VPN by using the remote subnet or the remote single host.	Subnet Address / Single Address	Subnet Address
	IP Address	The remote IP address	IPv4 format	192.168.88.0
	PrefixLen / Subnet Mask	The remote IP Netmask	IPv4 format	255.255.255.0

Action	Outgoing Interface	The WAN interface you are going to build IPSec tunnel with.	WAN interfaces	WAN1
	Peer's IP Address	The IP address of remote site device, like MH-5001 Multi-Homing Security Gateway.	IPv4 format	210.2.1.1
	Outgoing SPI	The Outgoing SPI (Security Parameter Index) value.	hex (600 ~ 600000) / dec(1500 ~ 6300000)	hex: 2222
	Incoming SPI	The Incoming SPI (Security Parameter Index) value.	hex(600 ~ 600000) / dec(1500 ~ 6300000)	hex: 1111
	Encapsulation Mode	Choose Tunnel or Transport mode, see Chapter 12 for details.	Transport / Tunnel	Tunnel
	ESP – Encryption / Authentication	Select the Encryption (DES, 3DES, AES or Null) and Authentication (MD5, SHA1 or NULL) Algorithm combination. And enter the key either hex or string form separately. Notice: You can not select both Encryption and Authentication "NULL" type.	Encryption: DES(64bits) / 3DES(192bits) / AES(128, 192, 256bits) / NULL Authentication: MD5(128bits) / SHA1(160bits) / NULL Input format: hex{0-9,a-f,A-F}/ str{text string}	ESP – Encryption (DES) / Authentication (MD5)

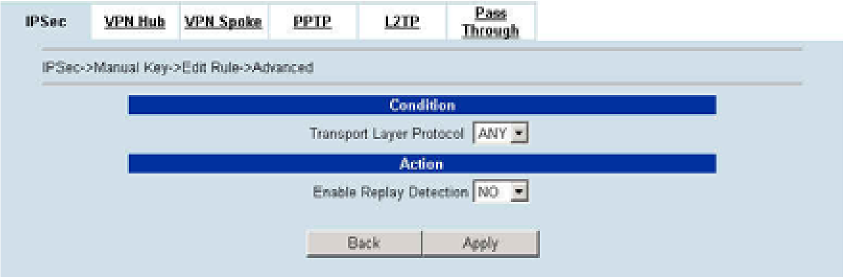
	AH - Authentication	Use the Authentication method only. And enter the key either hex or string form.	MD5(128bits) / SHA1(160bits)
			Input format:
			hex{0-9,a-f,A-F}/ str{text string}
				Disabled

Table 13-6 Add a IPSec Manual Key rule

Step 4. Detail settings of IPSec Manual Key

For the detailed setting in the Manual Key. We can press the Advanced button in the previous page. Then set the parameter separately.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add > Advanced



IPSec->Manual Key->Edit Rule->Advanced

Condition

Transport Layer Protocol: ANY

Action

Enable Replay Detection: NO

	FIELD	DESCRIPTION	Range / Format	EXAMPLE
Condition	Transport Layer Protocol	Utilize this field to select some packets which are specified protocol (ANY, TCP, UDP). If the packets are not the specified protocol will not be allowed to pass through IPSec tunnels.	ANY / TCP / UDP	ANY

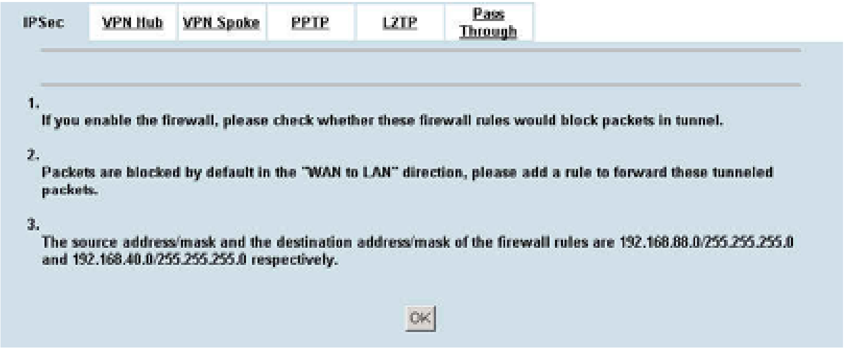
Action	Enable Replay Detection	Whether is the “Replay Detection” enabled？	NO / YES	NO

Table 13-7 Setup Advanced feature in the IPSec Manual Key rule

Step 5. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the OK button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add

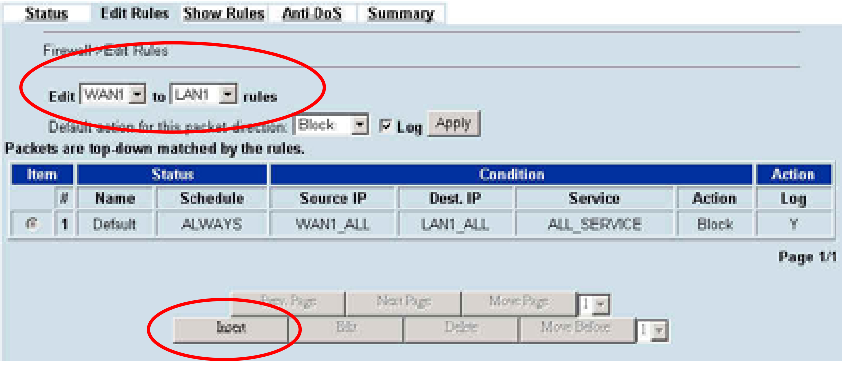


1. If you enable the firewall, please check whether these firewall rules would block packets in tunnel.
2. Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.
3. The source address/mask and the destination address/mask of the firewall rules are 192.168.88.0/255.255.255.0 and 192.168.40.0/255.255.255.0 respectively.

Step 6. Add a Firewall rule

Same as that in IKE method. Please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

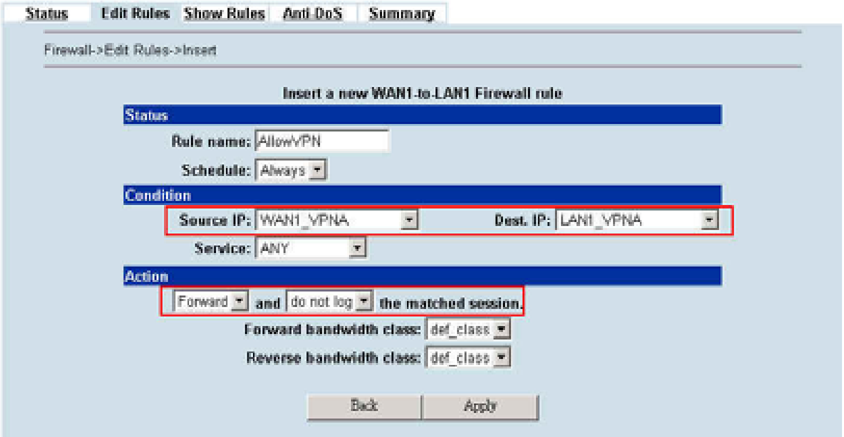
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 7. Customize the Firewall rule

Check the Activate this rule. Enter the Rule Name as AllowVPN, Source IP as WAN1_VPNA (192.168.88.0), and Dest. IP as LAN1_VPNA (192.168.40.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNA Dest. IP: LAN1_VPNA

Service: ANY

Action

Forward and do not log the matched session.

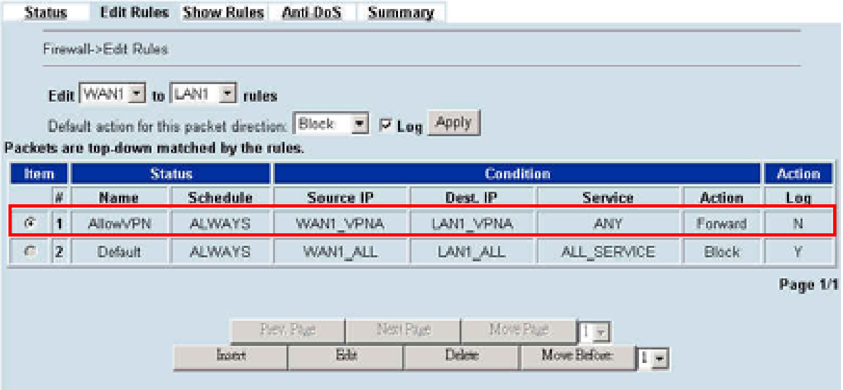
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through MH-5001. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit [WAN1] to [LAN1] rules

Default action for this packet direction: [Block] ☑ Log [Apply]

Packets are top-down matched by the rules.

Item		Status		Condition				Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNA	LAN1_VPNA	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

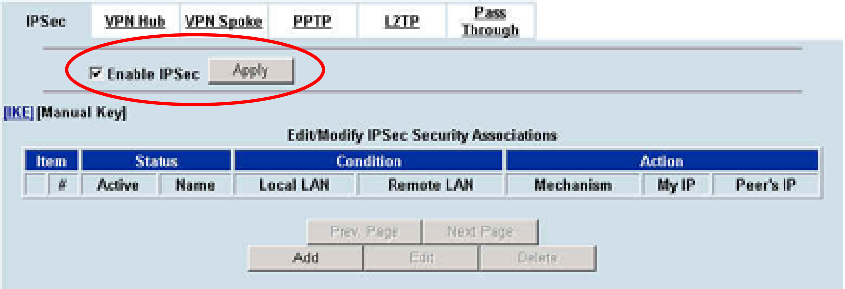
At WALL-2:

Second, we will use the Manual-Key way to install the IPSec properties of WALL-1.

Step 1. Enable IPSec

Check the `Enable IPSec` checkbox and click `Apply`.

ADVANCED SETTINGS > VPN Settings > IPSec



☑ Enable IPSec [Apply]

[IKE] [Manual Key]

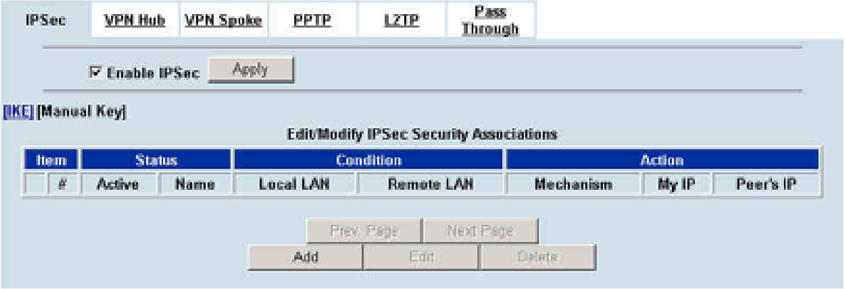
Edit/Modify IPSec Security Associations

Item	Status		Condition		Action		
#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 2. Add a Manual Key rule

Click the `Manual Key` hyperlink and click Add to add a new IPSec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key



☑ Enable IPSec [Apply]

[IKE] [Manual Key]

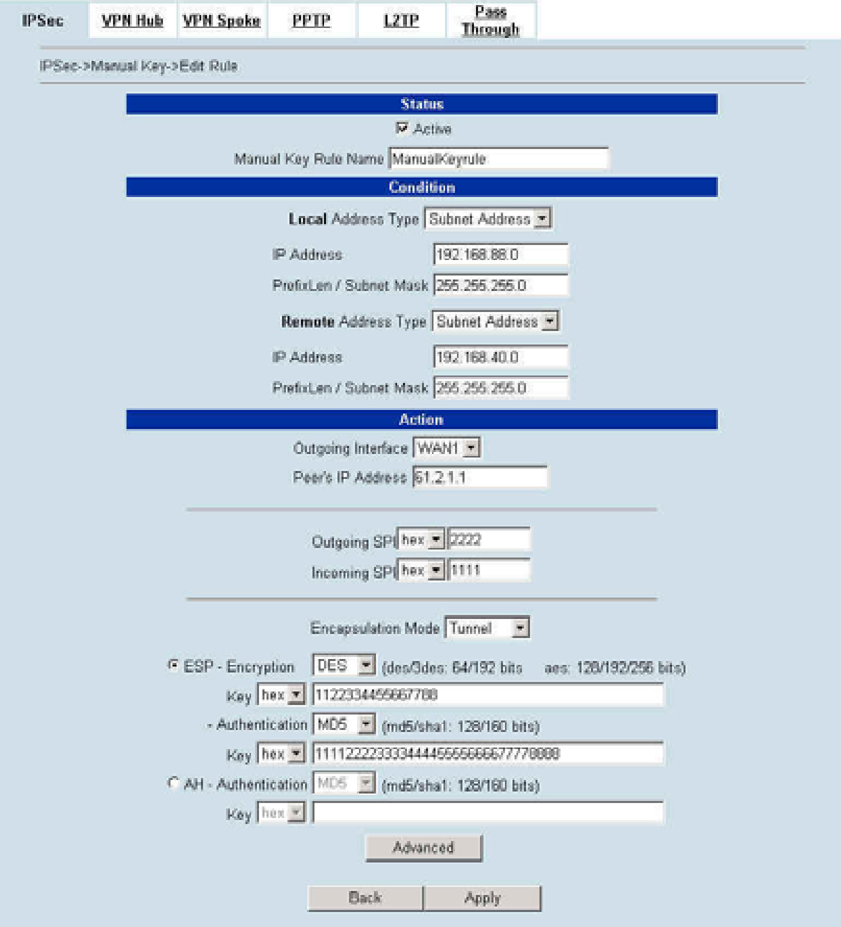
Edit/Modify IPSec Security Associations

Item	Status		Condition		Action		
#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 3. Customize the rule

Similar to those in WALL-1, except that you should interchange the `Local IP Address` with `Remote IP Address` in the `Condition` part and the `Outgoing SPI` with the `Incoming SPI` in the `Action part.` Besides, set the `Peer's IP Address` with the WAN1 IP address of WALL-1.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add



IPSec->Manual Key->Edit Rule

Status

☑ Active

Manual Key Rule Name: ManualKeyrule

Condition

Local Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Action

Outgoing Interface: WAN1

Peer's IP Address: 61.2.1.1

Outgoing SPI: hex 2222

Incoming SPI: hex 1111

Encapsulation Mode: Tunnel

● ESP - Encryption: DES (des/3des: 64/192 bits aes: 128/192/256 bits)

Key: hex 1122334455667788

- Authentication: MD5 (md5/sha1: 128/160 bits)

Key: hex 11112222333344445555666677778888

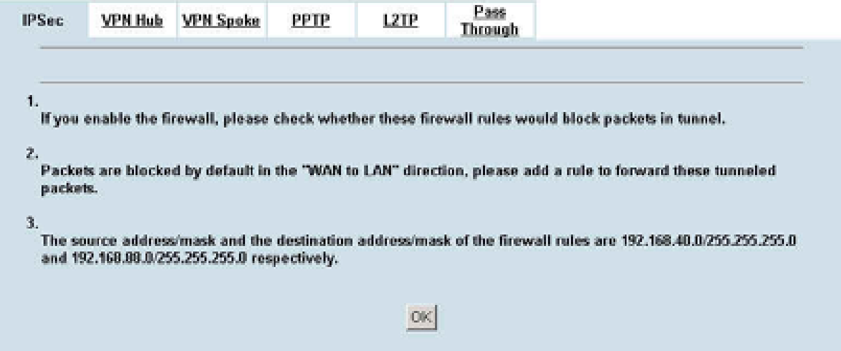
○ AH - Authentication: MD5 (md5/sha1: 128/160 bits)

Key: hex

Step 4. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the `OK` button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add



1.
If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

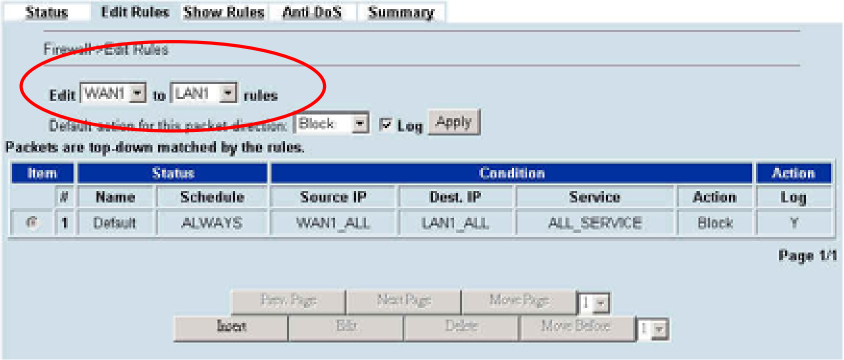
2.
Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

3.
The source address/mask and the destination address/mask of the firewall rules are 192.168.40.0/255.255.255.0 and 192.168.88.0/255.255.255.0 respectively.

Step 5. Add a Firewall rule

Same as that in IKE method. Please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

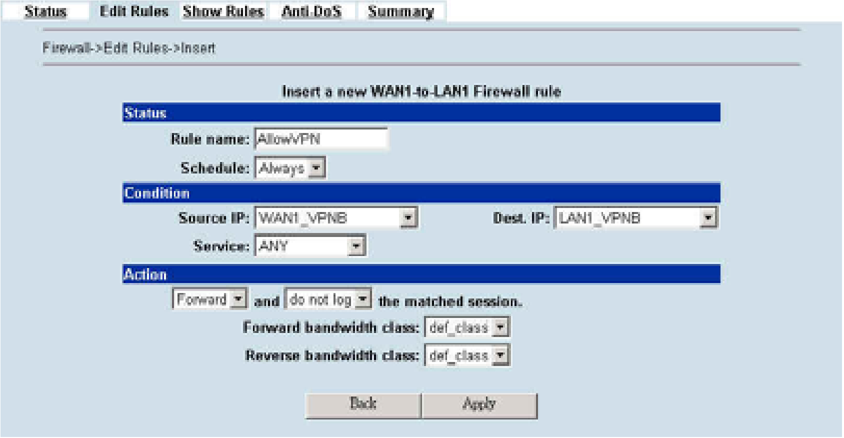
Item	Status		Condition				Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 6. Customize the Firewall rule

Check the Activate this rule. Enter the Rule Name as AllowVPN, Source IP as WAN1_VPNB (192.168.40.0), and Dest. IP as LAN1_VPNB (192.168.88.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNB Dest. IP: LAN1_VPNB

Service: ANY

Action

Forward and do not log the matched session.

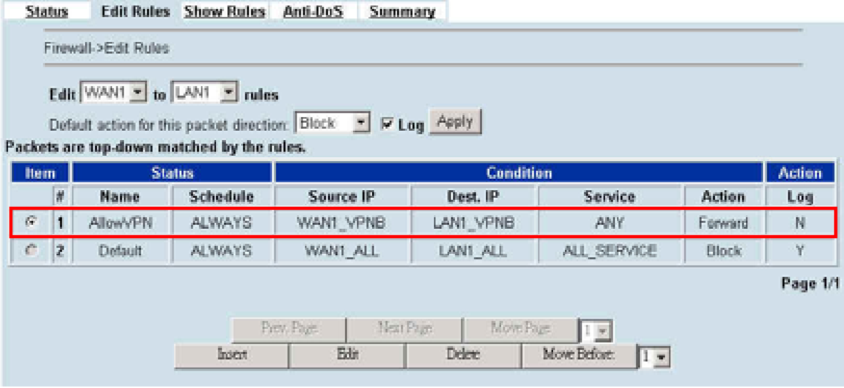
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from 192.168.40.0/24 to 192.168.88.0/24 will be allowed to pass through the MH-5001 and successfully access the 192.168.88.0/24 through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item	Status		Condition				Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNB	LAN1_VPNB	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Chapter 14
Virtual Private Network –Dynamic IPSec

This chapter introduces Dynamic IPSec VPN and explains how to implement it.

As described in the Figure 2-1, we will extend to explain how to make a dynamic VPN link between LAN_1 and LAN_2 in this chapter. The following Figure 14-1 is the real structure in our implemented process.

14.1 Demands

1. When a branch office subnet LAN_1 wants to connect with another branch office subnet LAN_2 through the public Internet instead of the expensive private leased lines, VPN can provide encryption and authentication to secure the tunnel that connects these two LANs. If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE) like Organization_2, we have to use the Dynamic IPSec for the tunnel connection.

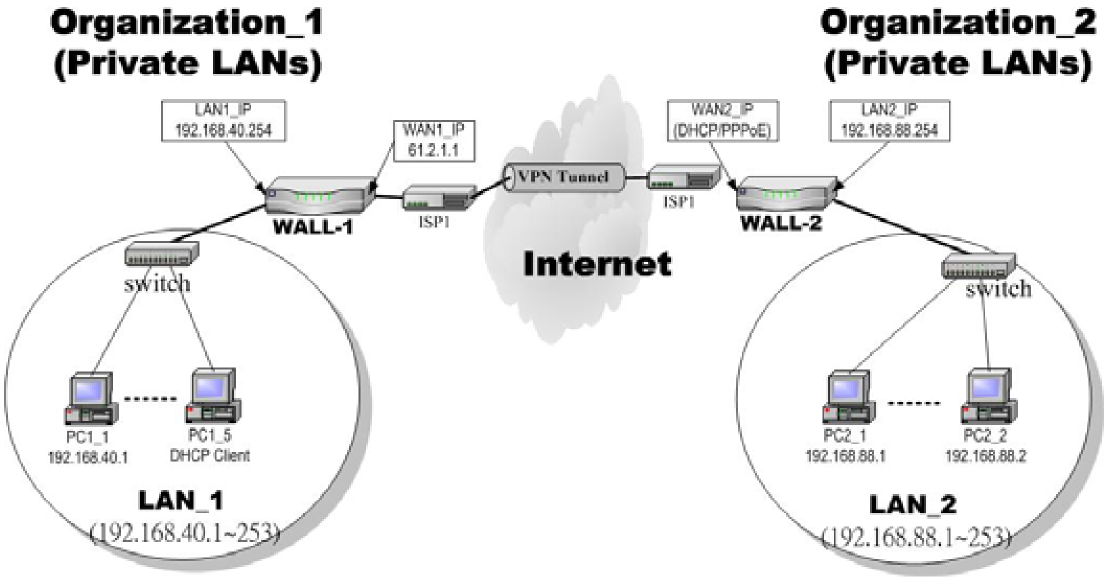


Figure 14-1 Organization_1 LAN_1 is making dynamic VPN tunnel with Organization_2 LAN_2

14.2 Objectives

1. Let the users in LAN_1 and LAN_2 share the resources through a secure channel established using the dynamic IPSec VPN.

14.3 Methods

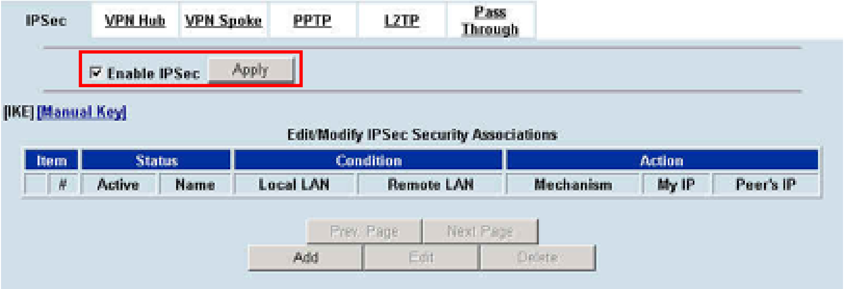
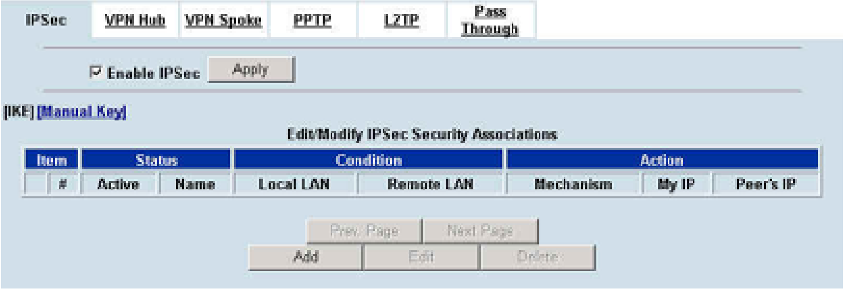
1. Separately configure WALL-1 and WALL-2 which are the edge gateways of LAN_1 and LAN_2 respectively.

14.4 Steps

In the following we will separately explain how to set up a secure DES/MD5 tunnel with the dynamic remote gateway IP address type.

At WALL-1:

At the first, we will install the IPSec properties of WALL-1. For the related explanation, please refer to Chapter 12 and Chapter 10.

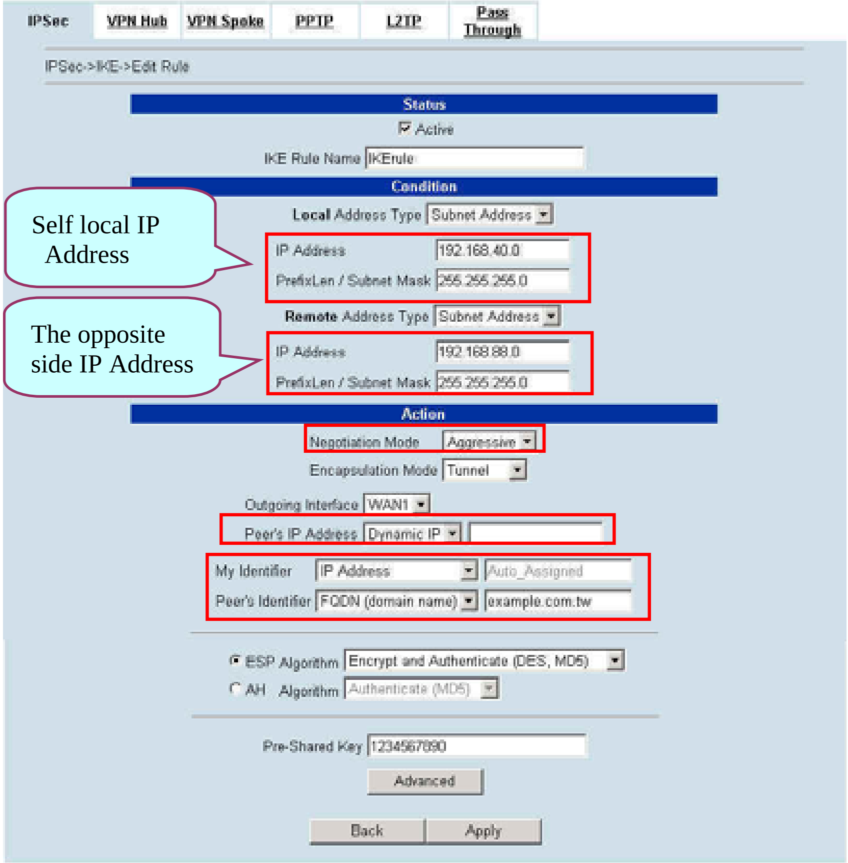
Step 1. Enable IPSec Check the `Enable IPSec` checkbox and click `Apply`.	**ADVANCED SETTINGS > VPN Settings > IPSec**  IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through ☑ Enable IPSec Apply [IKE] [Manual Key] Edit/Modify IPSec Security Associations Item Status Condition Action # Active Name Local LAN Remote LAN Mechanism My IP Peer's IP Prev. Page Next Page Add Edit Delete
Step 2. Add an IKE rule Click the `IKE` hyperlink and click Add to add a new IPSec VPN tunnel endpoint.	**ADVANCED SETTINGS > VPN Settings > IPSec > IKE**  IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through ☑ Enable IPSec Apply [IKE] [Manual Key] Edit/Modify IPSec Security Associations Item Status Condition Action # Active Name Local LAN Remote LAN Mechanism My IP Peer's IP Prev. Page Next Page Add Edit Delete

Step 3. Customize the rule

Check the Active checkbox. Enter a name for this rule like IKErule. Enter the Local IP Address (192.168.40.0/255.255.255.0) and the Remote IP Address (192.168.88.0/255.255.255.0). Select the Outgoing Interface of this Device. Select Dynamic IP in the Peer's IP Address. Be sure to select Aggressive mode for the dynamic remote gateway address type. Click the ESP Algorithm and select Encrypt and Authenticate (DES, MD5). Enter the Pre-Shared Key as 1234567890. Click the Apply button to store the settings. Note, In the Action region. It should choose either ESP Algorithm or AH Algorithm, or system will show error message. If you hope to set the detailed item of IKE parameter. Click the Advanced button in this page. Otherwise it is ok to just leave the value default.

Note that Peers Identifier must NOT be IP Address type in the Dynamic IP type. So, you have to select FQDN (domain name) or user FQDN (mailbox) as the Peer's Identifier.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: IKErule

Condition

Local Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Action

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Outgoing Interface: WAN1

Peer's IP Address: Dynamic IP

My Identifier: IP Address | Auto_Assigned

Peer's Identifier: FQDN (domain name) | example.com.tw

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

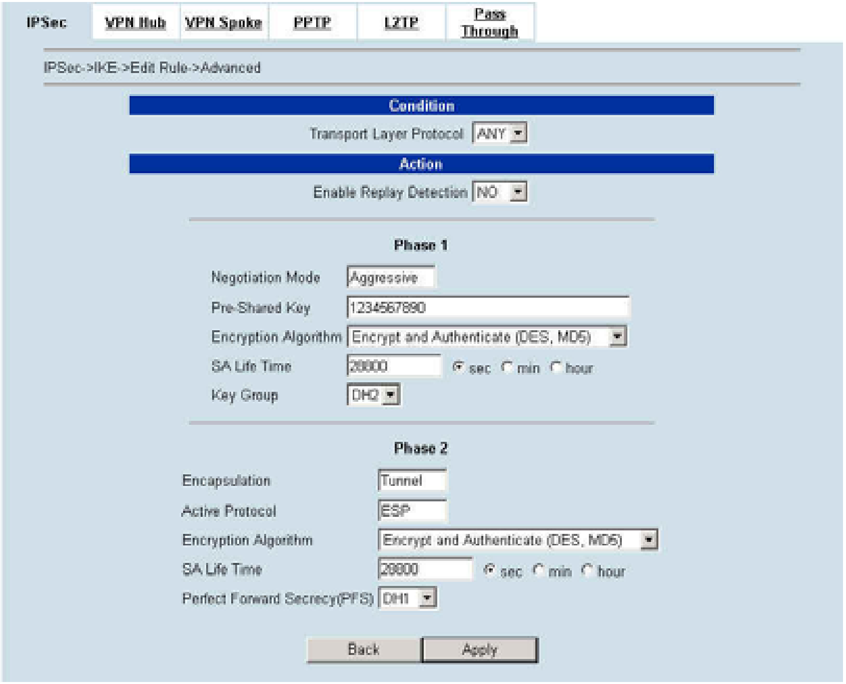
○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890

Step 4. Detail settings of IPSec IKE

In this page, we will set the detailed value of IKE parameter. For the related field, please refer to Table 13-5 indicated.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add > Advanced



IPSec->IKE->Edit Rule->Advanced

Condition

Transport Layer Protocol: ANY

Action

Enable Replay Detection: NO

Phase 1

Negotiation Mode: Aggressive

Pre-Shared Key: 1234567890

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

SA Life Time: 28800 ● sec ○ min ○ hour

Key Group: DH2

Phase 2

Encapsulation: Tunnel

Active Protocol: ESP

Encryption Algorithm: Encrypt and Authenticate (DES, MD5)

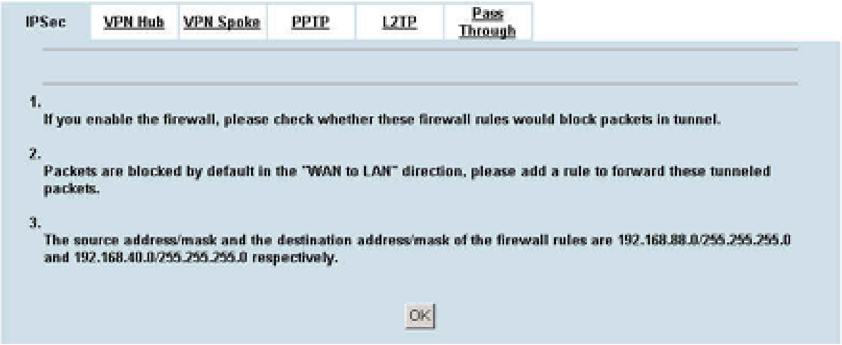
SA Life Time: 28800 ● sec ○ min ○ hour

Perfect Forward Secrecy(PFS): DH1

Step 5. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the OK button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



1\.
If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

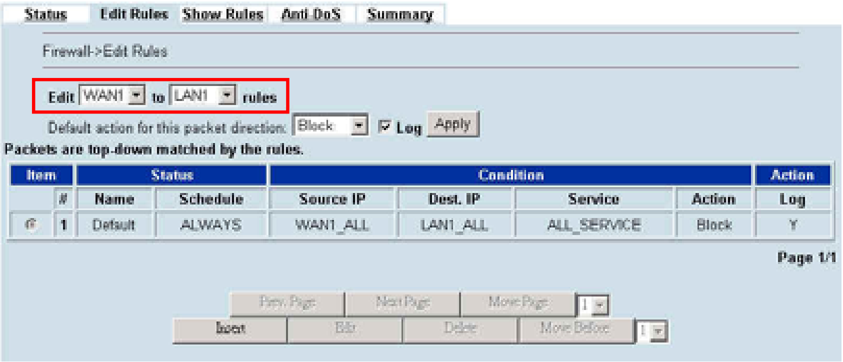
2\.
Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

3\.
The source address/mask and the destination address/mask of the firewall rules are 192.168.88.0/255.255.255.0 and 192.168.40.0/255.255.255.0 respectively.

Step 6. Add a Firewall rule

Beforehand, please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

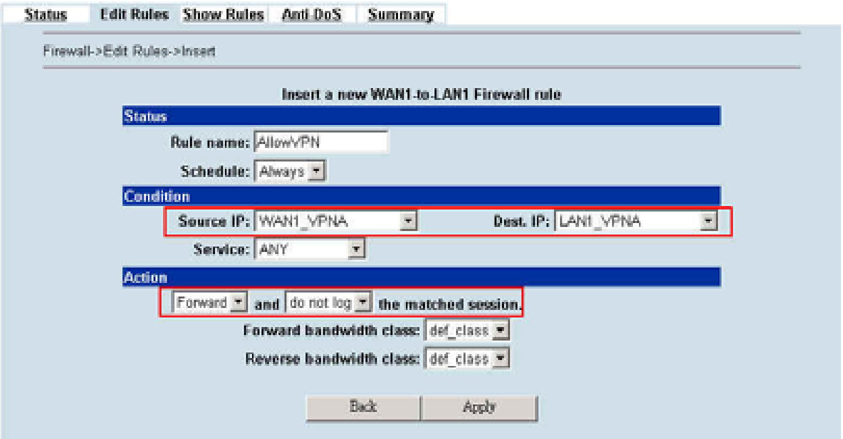
Item		Status		Condition			Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 7. Customize the Firewall rule

Check the Activate this rule. Enter the Rule Name as AllowVPN, Source IP as WAN1_VPNA (192.168.88.0), and Dest. IP as LAN1_VPNA (192.168.40.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNA Dest. IP: LAN1_VPNA

Service: ANY

Action

Forward and do not log the matched session.

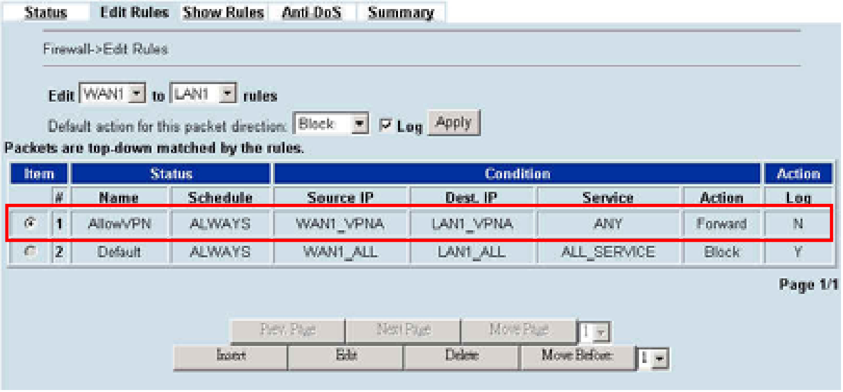
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through MH-5001. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition			Action	Log
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNA	LAN1_VPNA	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

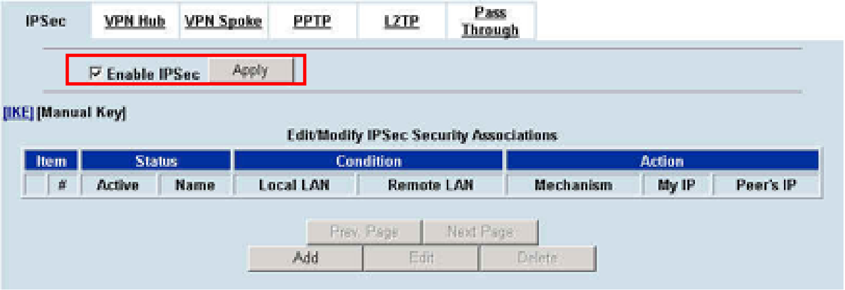
At WALL-2:

Here we will install the IPSec properties of WALL-2. Note that the “Local Address” and “Remote address” field are opposite to the WALL-1, and so are “My IP Address” and “Peer’s IP Address” field.

Step 1. Enable IPSec

Check the `Enable IPSec` checkbox and click `Apply`.

ADVANCED SETTINGS > VPN Settings > IPSec



☑ Enable IPSec Apply

[IKE] [Manual Key]

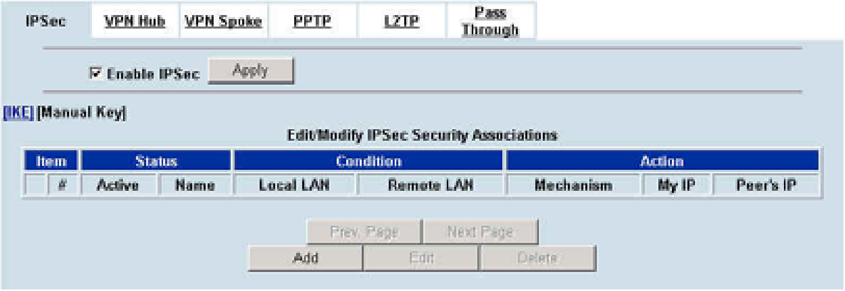
Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 2. Add an IKE rule

Click the `IKE` hyperlink and click `Add` to add a new IPSec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE



☑ Enable IPSec Apply

[IKE] [Manual Key]

Edit/Modify IPSec Security Associations

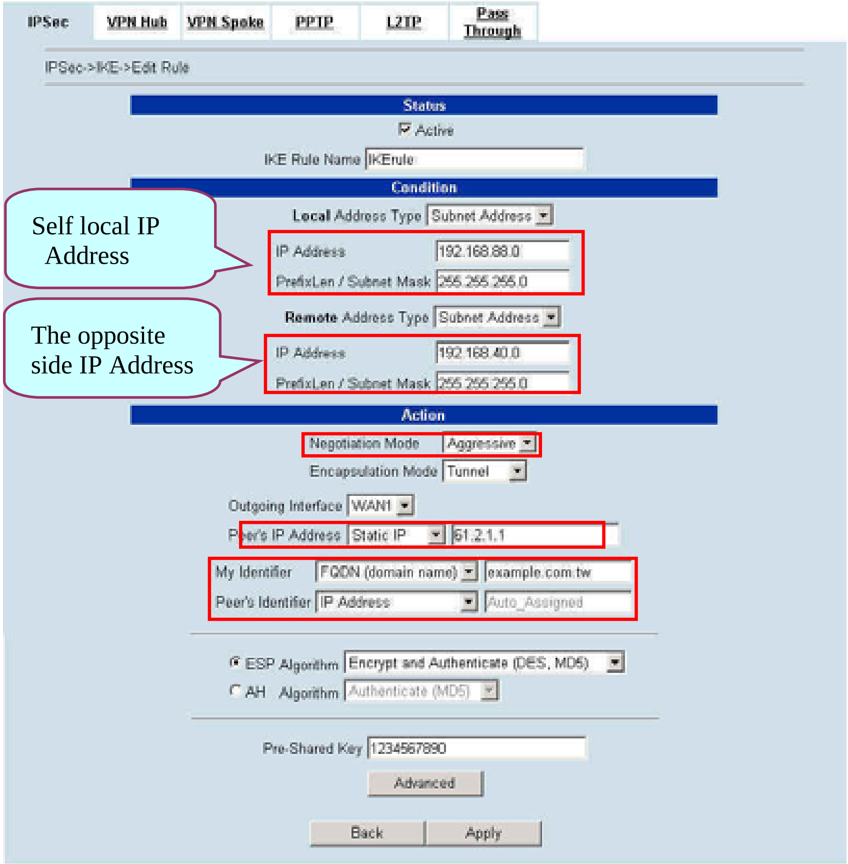
Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP

Step 3. Customize the rule

Check the `Active` checkbox. Enter a name for this rule like `IKErule`. Enter the `Local IP Address (192.168.88.0/255.255.255.0)` and the `Remote IP Address (192.168.40.0/255.255.255.0)`. Be sure to select `Aggressive` mode to match the WALL-1 settings. Select the `Outgoing interface` of this Device. Enter the public IP of the opposite-side VPN gateway (`61.2.1.1`) in the `Peer's IP Address`. Click the `ESP Algorithm` and select `Encrypt` and `Authenticate (DES, MD5)`. Enter the `Pre-Shared Key` as `1234567890`. Select `User FQDN (mailbox)` and enter `planet.com.tw` in My Identifier field. Click the `Apply` button to store the settings. Note, in the Action region, you should choose either ESP Algorithm or AH Algorithm, or system will show error message.

Note that one of the Peer's IP Addresses is `Static IP`, and the other must be the `Dynamic IP` while using Dynamic IPSec VPN type to establish the VPN tunnel.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: IKErule

Condition

Local Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Action

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Outgoing Interface: WAN1

Peer's IP Address: Static IP 61.2.1.1

My Identifier: FQDN (domain name) example.com.tw

Peer's Identifier: IP Address Auto_Assigned

● ESP Algorithm: Encrypt and Authenticate (DES, MD5)

○ AH Algorithm: Authenticate (MD5)

Pre-Shared Key: 1234567890

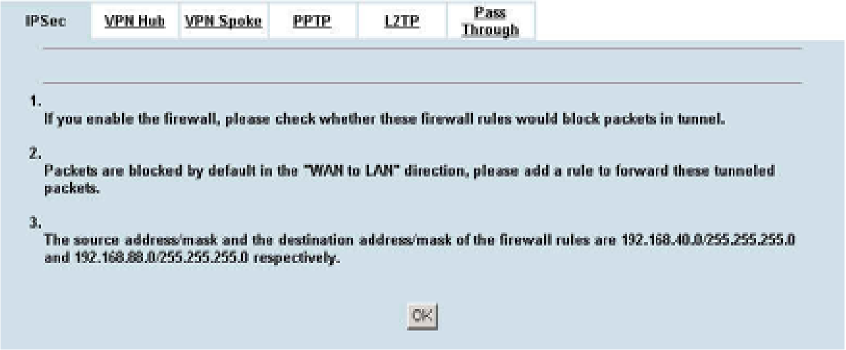
Self local IP Address

The opposite side IP Address

Step 4. Remind to add a Firewall rule

After finishing IPSec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the `OK` button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add



1. If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

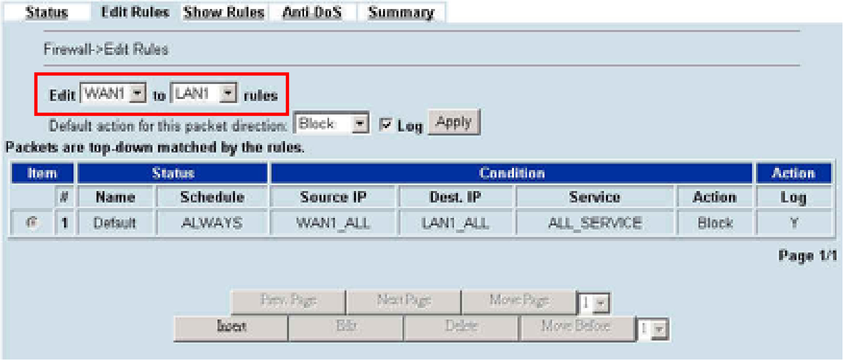
2. Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

3. The source address/mask and the destination address/mask of the firewall rules are 192.168.40.0/255.255.255.0 and 192.168.88.0/255.255.255.0 respectively.

Step 5. Add a Firewall rule

Same as at WALL-1. We need to add an extra firewall rule to allow IPSec packets to come from Internet. So here we select `WAN1-to-LAN1` direction, and click `Insert` button.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

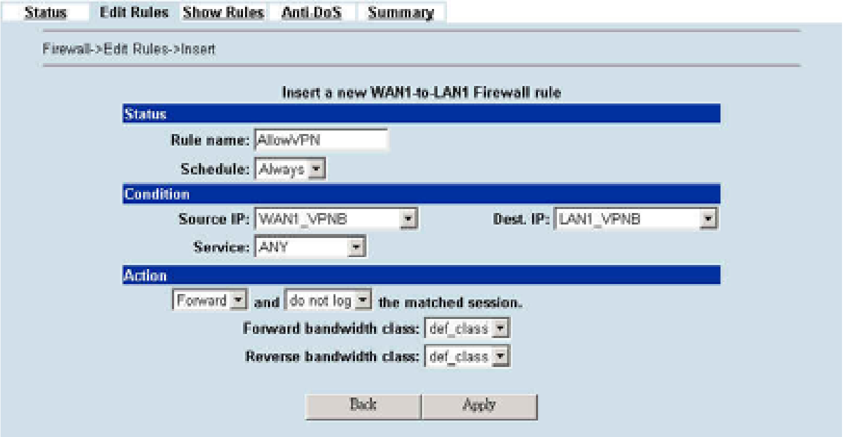
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 6. Customize the Firewall rule

Check the `Activate this rule`. Enter the `Rule Name` as `AllowVPN`, `Source IP` as `WAN1_VPNB (192.168.40.0)`, and `Dest. IP` as `LAN1_VPNB (192.168.88.0)`. Click `Apply` to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNB Dest. IP: LAN1_VPNB

Service: ANY

Action

Forward and do not log the matched session.

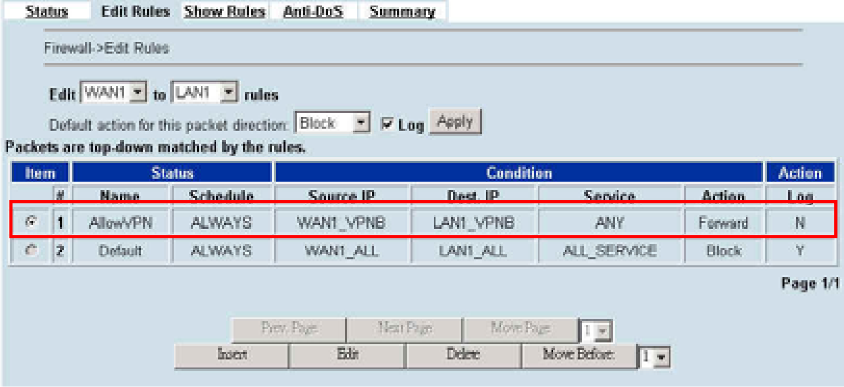
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from `192.168.40.0/24` to `192.168.88.0/24` will be allowed to pass through the MH-5001 and successfully access the `192.168.88.0/24` through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	AllowVPN	ALWAYS	WAN1_VPNB	LAN1_VPNB	ANY	Forward	N
○	2	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Chapter 15
Virtual Private Network – Hub and Spoke VPN

This chapter introduces Hub and Spoke VPN and explains how to implement it.

As described in the Figure 2-1, we will extend to explain how to make a VPN link between Main Office (the hub) and the branches in this chapter. The following Figure 15-1 is the real structure in our implemented process.

15.1 Demands

1. Suppose that your company has a main office and two branch offices which communicates using a hub and spoke VPN configuration. The main office is the hub where the VPN tunnels terminate, while Branch_1 and Branch_2 are the spokes. The Main office has a VPN tunnel to each branch office. Branch_1 and Branch_2 has its own VPN tunnel to the hub.

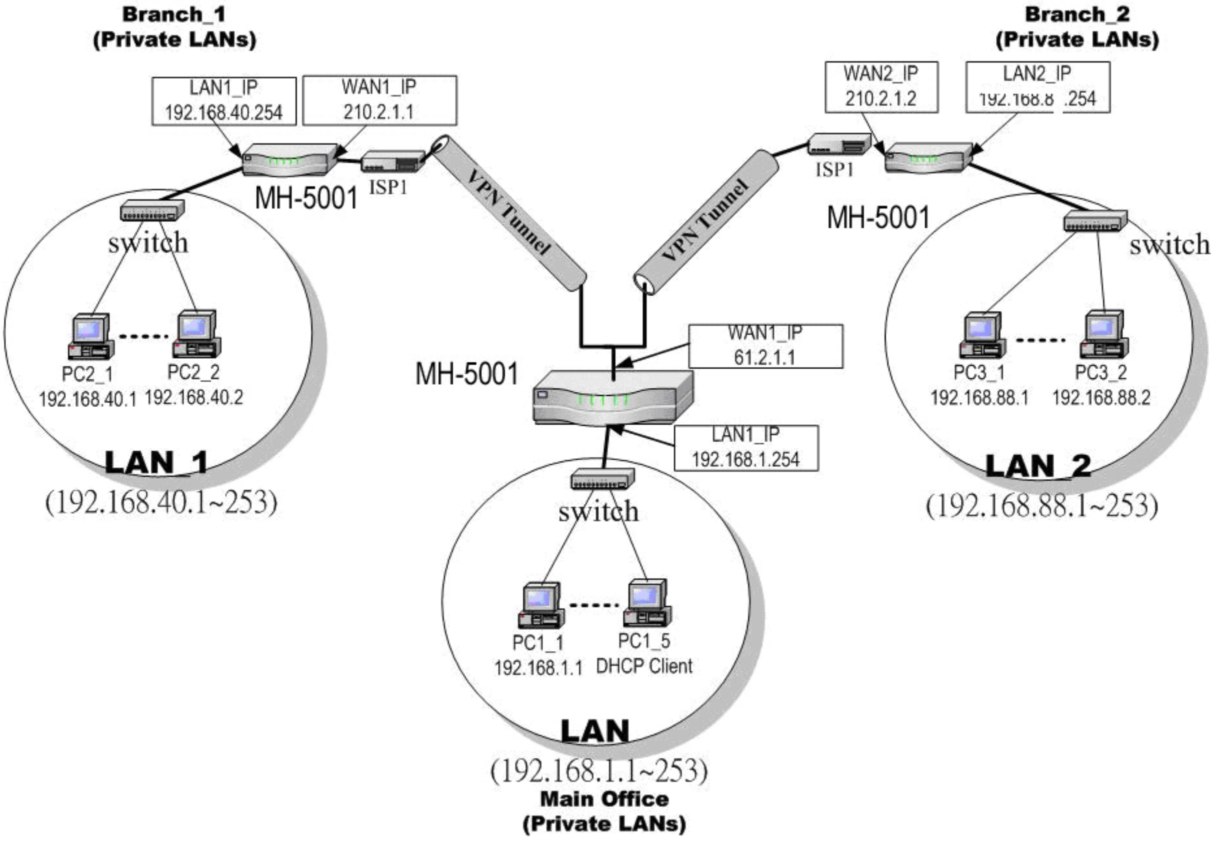


Figure 15-1 The Topology of the VPN Hub (Main Office) and VPN Spoke (Branch offices)

15.2 Objectives

1. Using the VPN hub we can create a hub and spoke VPN configuration to direct traffic through a central MH-5001 from one VPN tunnel to another VPN tunnel. Each VPN tunnel provides connectivity to a different remote VPN gateway. All of the VPN Hub member tunnels can establish VPN connections with any of the other member VPN tunnels.

15.3 Methods

1. Configuring the IKE tunnels.
2. Configuring the WAN1-to-LAN1 Firewall Rule.
3. Configuring the VPN Hub for the Main Office.
4. Configuring the VPN spoke for the Branch Offices.

15.4 Steps

In the following, we will introduce you how to setup the Hub and Spoke VPN between main office and two branch offices.

Configuring the IPSec IKE tunnels

For the main office (the hub), we have to create the IKE tunnels, and then create VPN hub and add tunnels to it as members. Use the information in the following Table 15-1 to configure IKE tunnels. After finishing the IPSec VPN setting, please remember to add a WAN-to-LAN firewall rule.

Field Name	Main Office Information		Branch_1 Information	Branch_2 Information
Status				
Active	Enable	Enable	Enable	Enable
IKE Rule Name	IKEVpnA	IKEVpnB	IKEMainVPN	IKEMainVPN
Condition				
Local Address Type	Subnet Address	Subnet Address	Subnet Address	Subnet Address
IP Address	192.168.1.0	192.168.1.0	192.168.40.0	192.168.88.0
PrefixLen/Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Remote Address Type	Subnet Address	Subnet Address	Subnet Address	Subnet Address
IP Address	192.168.40.0	192.168.88.0	192.168.1.0	192.168.1.0
PrefixLen/Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Action				
Negotiation Mode	Main	Main	Main	Main
Encapsulation Mode	Tunnel	Tunnel	Tunnel	Tunnel
Outgoing Interface	WAN1	WAN1	WAN1	WAN1
Peer’s IP Address	210.2.1.1	210.2.1.2	61.2.1.1	61.2.1.1
My Identifier	IP Address	IP Address	IP Address	IP Address
Peer’s Identifier	IP Address	IP Address	IP Address	IP Address
ESP Algorithm	Encrypt and Authenticate (DES,	Encrypt and Authenticate (DES,	Encrypt and Authenticate (DES,	Encrypt and Authenticate (DES,

	MD5)	MD5)	MD5)	MD5)
AH Algorithm	Not selected	Not selected	Not selected	Not selected
Pre-Shared Key	1234567890	1234567890	1234567890	1234567890

Table 15-1 The IKE tunnel configuration

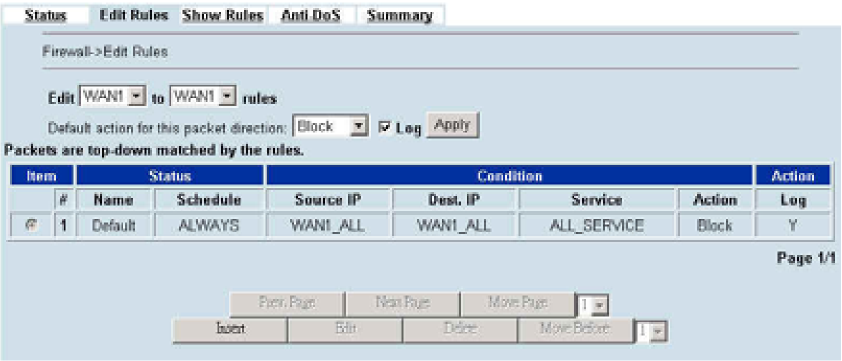
Configuring the VPN Hub for Main Office

Step 8. Add a Firewall rule

Suppose Main Office has already added two VPN tunnels to communicate with two branch offices. Now, the Main Office has to add a firewall rule to allow IPSec packets to come from Internet. Before adding a firewall rule, please make sure to add the addresses first.

Please make sure that the Firewall is enabled. Select `WAN1`-to-`WAN1` to display the rules of this direction. The default action of this direction is `Block` with `Logs`. We have to allow the VPN traffic from the WAN1 side to enter another WAN1 side. So we click the `Insert` button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to WAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item	Status			Condition			Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
○	1	Default	ALWAYS	WAN1_ALL	WAN1_ALL	ALL_SERVICE	Block	Y

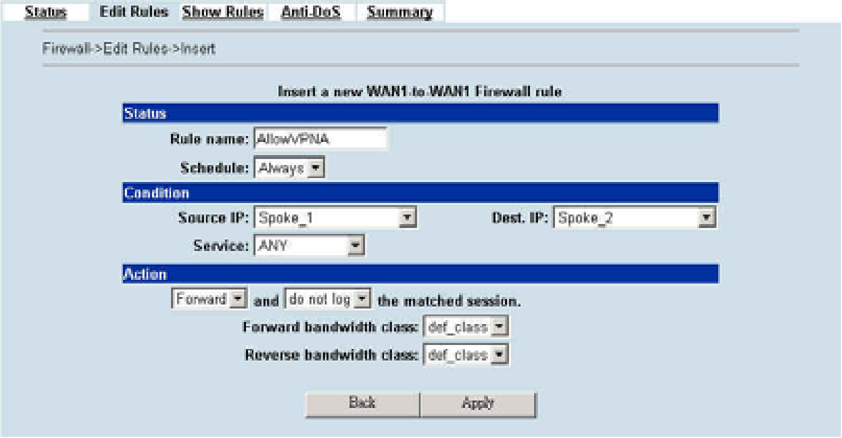
Page 1/1

Step 9. Customize a Firewall rule from Spoke1 to Spoke2

Enter the `Rule Name` as `AllowVPNA`, Source IP as `Spoke_1 (192.168.40.0)`, and Dest. IP as `Spoke_2(192.168.88.0)`. Click `Apply` to store this rule.

If you have not yet configured the Source IP, Dest IP or Service objects. Please refer Chapter 9 for the setting information first.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-WAN1 Firewall rule

Status

Rule name: AllowVPNA

Schedule: Always

Condition

Source IP: Spoke_1 Dest. IP: Spoke_2

Service: ANY

Action

Forward and do not log the matched session.

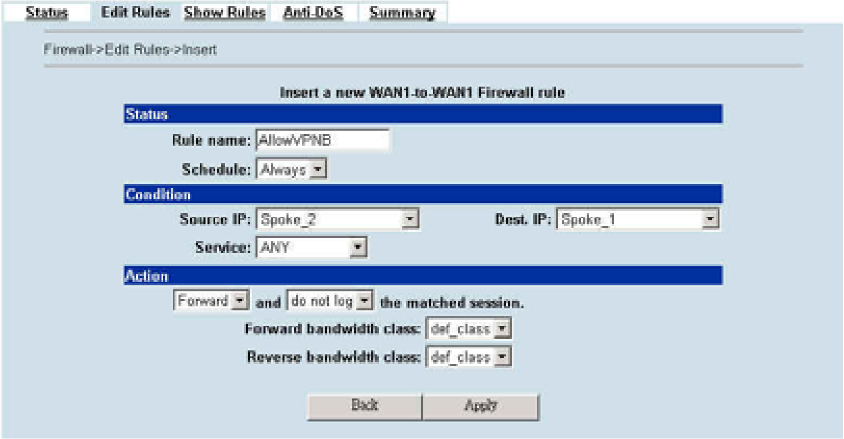
Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 10. Customize a Firewall rule from Spoke 2 to Spoke 1

Enter the Rule Name as `AllowVPNB`, Source IP as `Spoke_2 (192.168.88.0)`, and Dest. IP **as** `Spoke_1 (192.168.40.0)`. Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-WAN1 Firewall rule

Status

Rule name: AllowVPNB

Schedule: Always

Condition

Source IP: Spoke_2 Dest. IP: Spoke_1

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

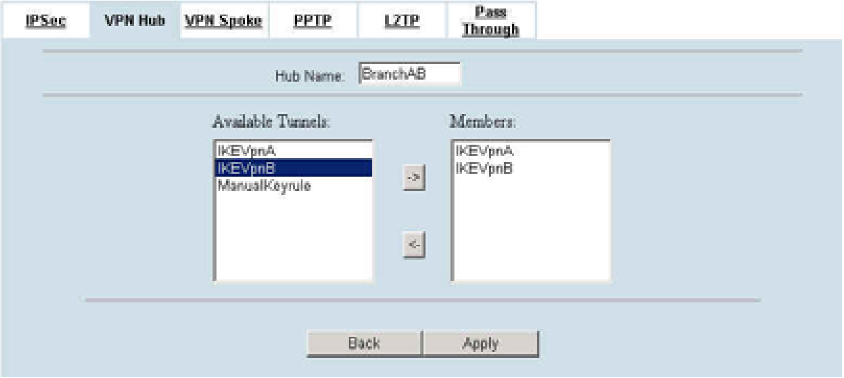
Reverse bandwidth class: def_class

Step 11. Add a VPN Hub

Select Add to add a VPN Hub. Enter a name in the `Hub Name` field. To add tunnels to the VPN Hub, select a VPN tunnel from the `Available Tunnels` list and select the right arrow. To remove tunnels from the Members list, select the tunnels and select the left arrow. Select `Apply` to add the VPN Hub.

Note the Available Tunnel is the IPSec tunnel which you have finished setting before. Please refer the Table 15-1 IPSec tunnel information.

ADVANCED SETTINGS > VPN Settings > VPN Hub > Add



Hub Name: BranchAB

Available Tunnels: IKEVpnA, IKEVpnB, ManualKeyrule

Members: IKEVpnA, IKEVpnB

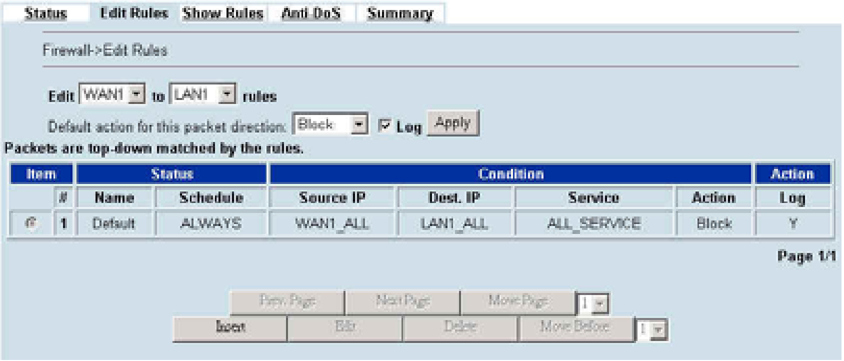
Configuring the VPN Spoke for the Branch_1

Step 12. Add a Firewall rule

Suppose Brach_1 Office has already added a VPN tunnel to communicate with the Main Office. Now, the Branch_1 has to add a firewall rule to allow IPSec packets to come from Main Office and Branch_2. Before adding the firewall rules, please make sure to add the addresses first.

Please make sure that the Firewall is enabled. Select `WAN1-to-LAN1` to display the rules of this direction. The default action of this direction is `Block` with `Logs`. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the `Insert` button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log

Packets are top-down matched by the rules.

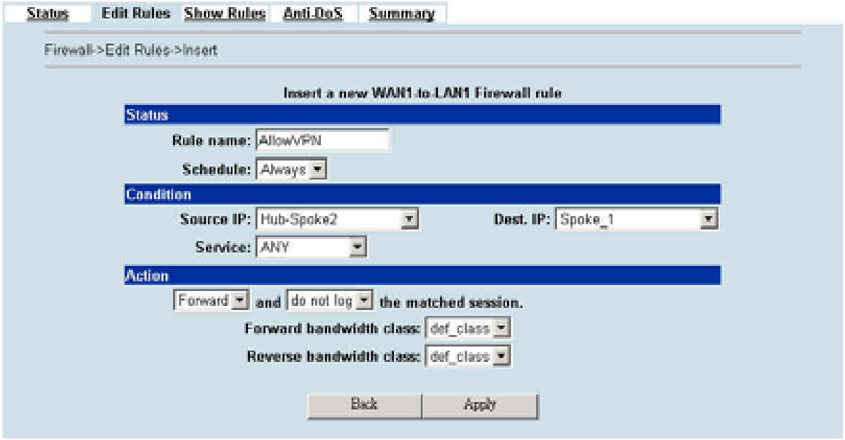
Item	Status			Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 13. Customize a Firewall rule

Enter the `Rule` Name as `AllowVPN`, Source IP as `Hub-Spoke2 [Hub (192.168.1.0), Spoke_2 (192.168.88.0)]`, and Dest. IP as `Spoke_1 (192.168.40.0)`. Click `Apply` to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: Hub-Spoke2 Dest. IP: Spoke_1

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

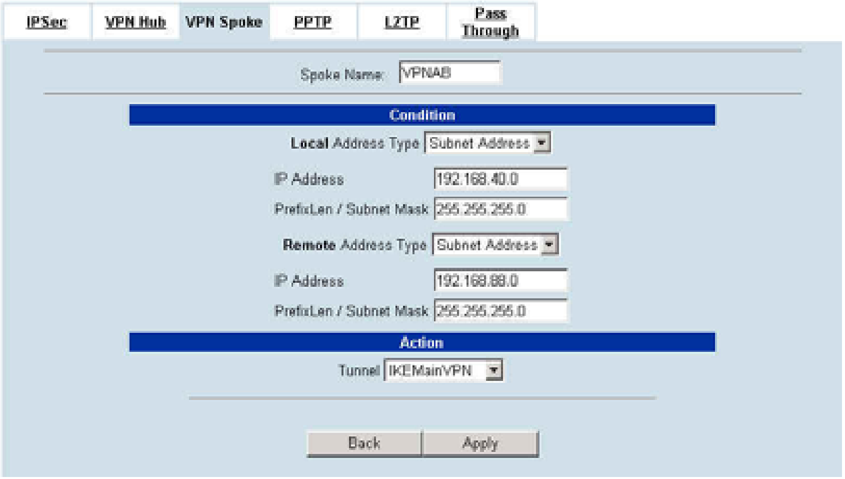
Reverse bandwidth class: def_class

Step 14. Add a VPN Spoke in Branch_1

Select Add to add a `VPN Spoke`. Enter a name in the `Spoke Name` field. Enter the Local IP Address/Subnet Mask and Remote Address IP Address/Subnet Mask. Select the VPN tunnel which is established to connect Branch_1 and Main Office.

Note the Tunnel of Action is the IPSec tunnel which you have finished setting before. Please refer the Table 15-1 IPSec tunnel information.

ADVANCED SETTINGS > VPN Settings > VPN Spoke > Add



Spoke Name: VPNAB

Condition

Local Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

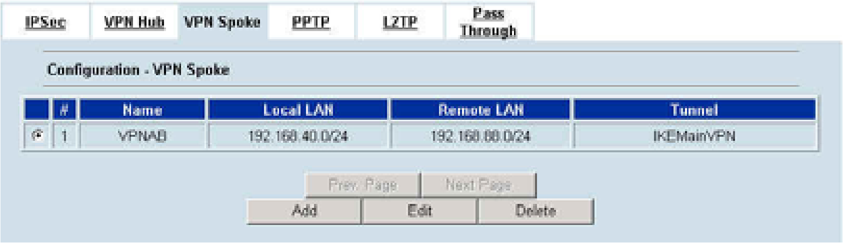
Action

Tunnel: IKEMainVPN

Step 15. View the added VPN Spoke

You can view the added VPN spoke here.

ADVANCED SETTINGS > VPN Settings > VPN Spoke



Configuration - VPN Spoke

	#	Name	Local LAN	Remote LAN	Tunnel
●	1	VPNAB	192.168.40.0/24	192.168.88.0/24	IKEMainVPN

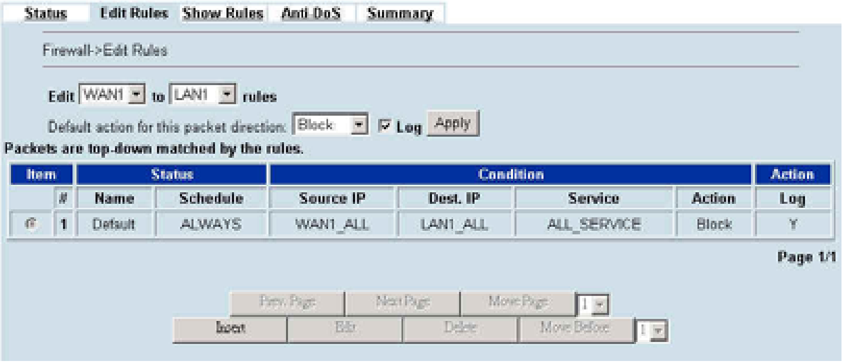
Configuring the VPN Spoke for the Branch_2

Step 16. Add a Firewall rule

Suppose Brach_2 Office has already added a VPN tunnel to communicate with the Main Office. Now, the Branch_2 has to add a firewall rule to allow IPSec packets to come from Main office and Branch_1. Before adding a firewall rule, please make sure to add the addresses first.

Please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Status | Edit Rules | Show Rules | Anti DoS | Summary

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

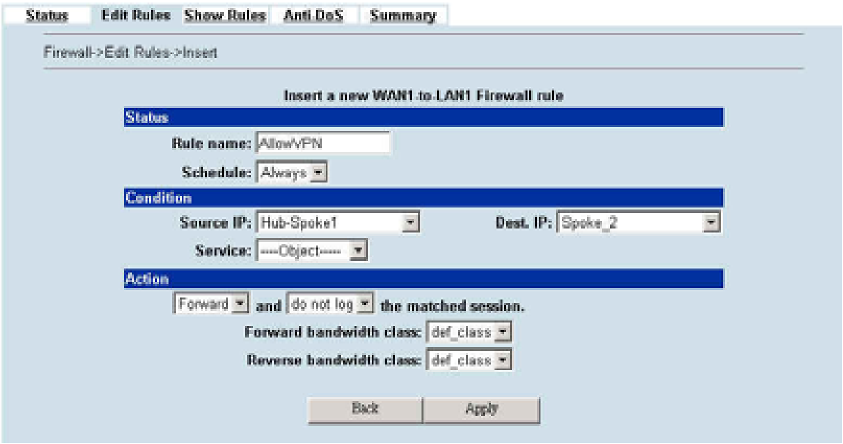
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
◉	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 17. Customize a Firewall rule

Enter the Rule Name as AllowVPN, Source IP as Hub-Spoke1 [Hub (192.168.1.0), Spoke_1 (192.168.40.0)], and Dest. IP as Spoke_2 (192.168.88.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Status | Edit Rules | Show Rules | Anti DoS | Summary

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: Hub-Spoke1   Dest. IP: Spoke_2

Service: ----Object-----

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

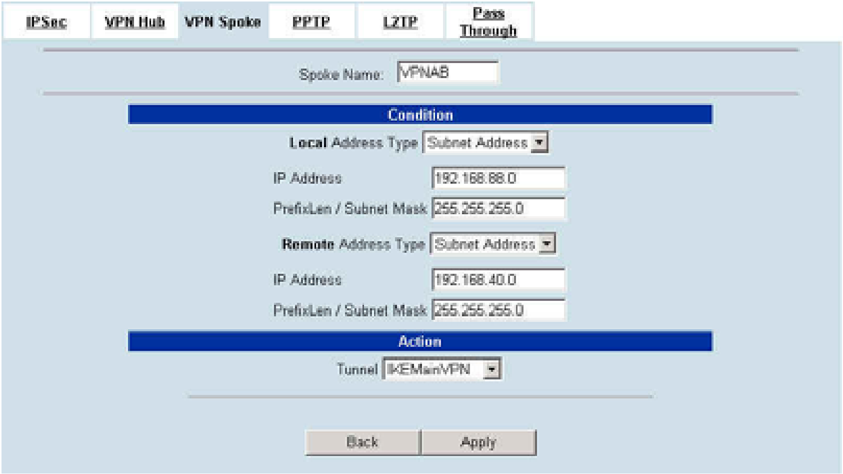
Reverse bandwidth class: def_class

Step 18. Add a VPN Spoke in Branch_2

Select Add to add a VPN Spoke. Enter a name in the Spoke Name field. Enter the Local IP Address/Subnet Mask and Remote Address IP Address/Subnet Mask. Select the VPN tunnel which is established to connect Branch_2 and Main Office.

Note the Tunnel of Action is the IPSec tunnel which you have finished setting before. Please refer the Table 15-1 IPSec tunnel information.

ADVANCED SETTINGS > VPN Settings > VPN Spoke > Add



IPSec | VPN Hub | VPN Spoke | PPTP | L2TP | Pass Through

Spoke Name: VPNAB

Condition

Local Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

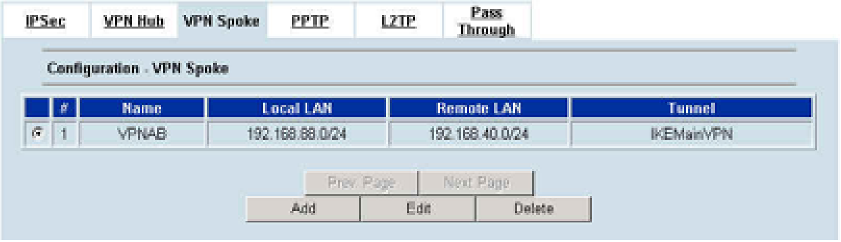
Action

Tunnel: IKEMainVPN

Step 19. View the added VPN Spoke

You can view the added VPN spoke here.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add > Advanced



Configuration - VPN Spoke

	#	Name	Local LAN	Remote LAN	Tunnel
●	1	VPNAB	192.168.88.0/24	192.168.40.0/24	IKEMainVPN

Chapter 16
Remote Access VPN – PPTP

This chapter introduces PPTP and explains how to implement it.

16.1 Demands

1. One employee in our company may sometimes want to connect back to our coporate network to work on something. His PC is PC1_1 in LAN_1 instead of DMZ_1 so he cannot directly access the host by simply with virtual server settings. This causes inconvenience for the employee to work remotely.
2. In our branch office, we need to provide PPTP connection methods to connect back to headquater for the internal company employees.

16.2 Objectives

1. With PPTP tunneling, emulate the mobile employee as a member in LAN1 after he dials in the corporate network. Then he can access all computers in LAN_1 just as if he stays in the office covered by LAN1.
2. Make sure every employee in the branch office can use the network resource in the headquater. Suppose they are in the same internal network, and keep the communication security.

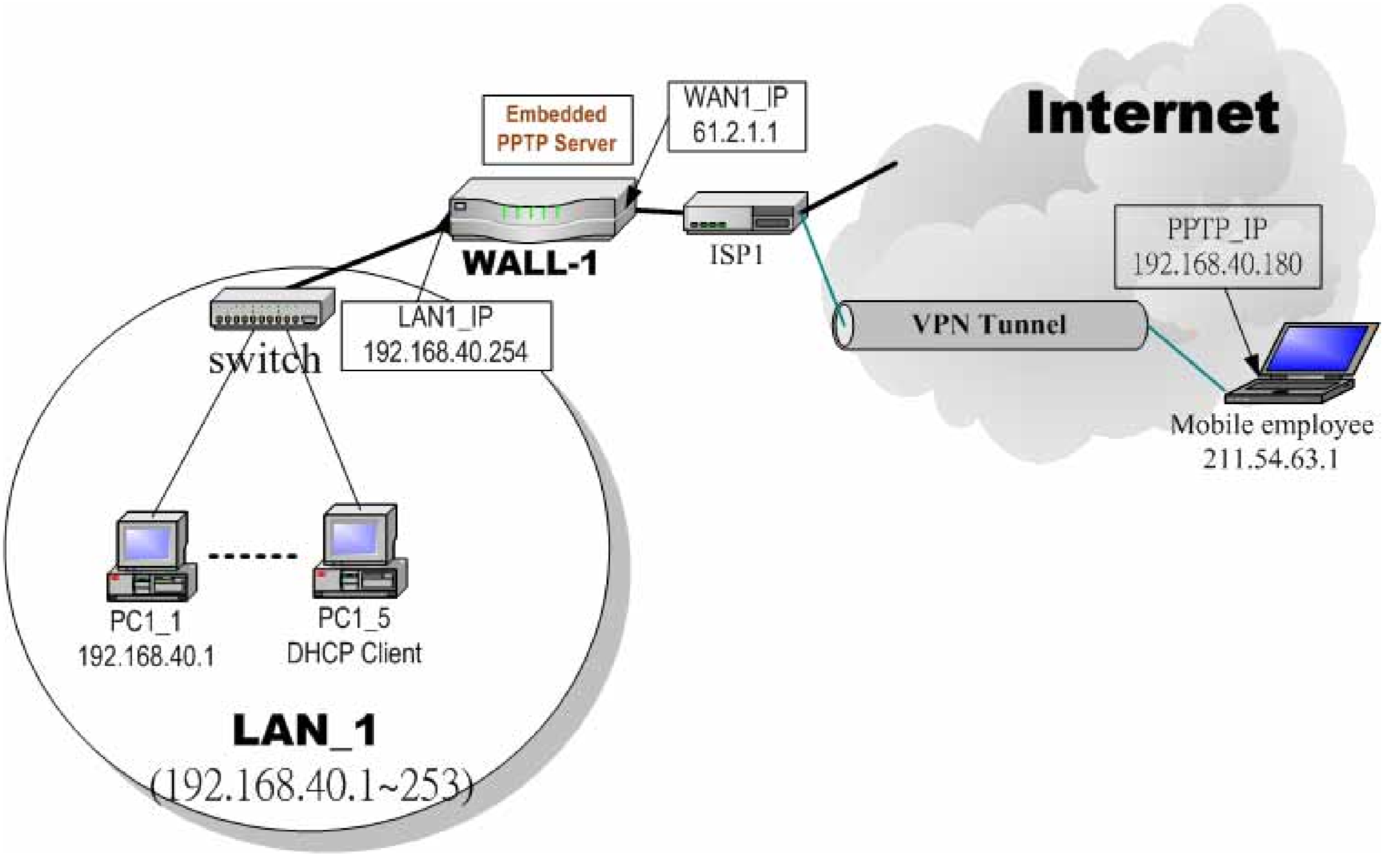


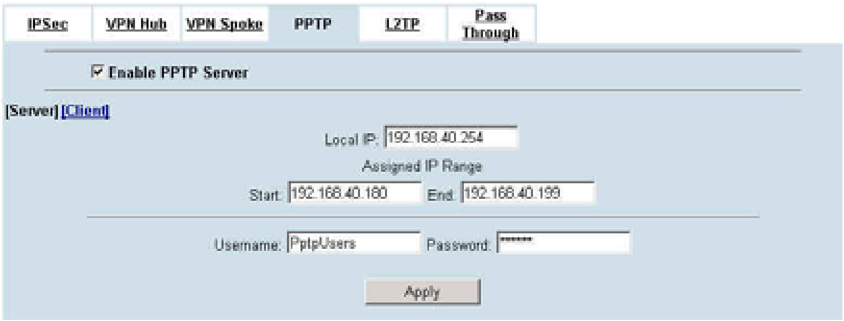
Figure 16-1 PPTP method connection

16.3 Methods

1. Setup the PPTP server at WALL-1, the MH-5001. Setup the remote PC as the PPTP client. After dialing up to WALL-1, WALL-1 will assign a private IP which falls in the range of the settings in the PPTP server at WALL-1. Suppose the range is defined as 192.168.40.180 ~ 192.168.40.199, the remote host may get an IP of 192.168.40.180 and logically become a member in LAN1.
2. Setup the MH-5001 as the PPTP client. Let all the client PCs behind the MH-5001. They can connect to the network behind PPTP Server by passing through MH-5001. It sounds like no Internet exists but can connect with each other.

16.4 Steps

16.4.1 Setup PPTP Network Server

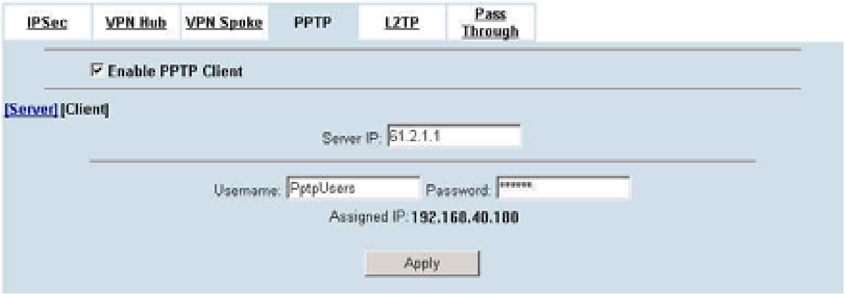
Step 1 – Enable PPTP Server	**ADVANCED SETTINGS > VPN Settings > PPTP**
Check the Enable PPTP checkbox, enter the LAN1_IP of the WALL-1(192.168.40.254) in the Local IP, and enter the IP range that will be assigned to the PPTP clients in the Start IP and the End IP fields. Enter the Username and Password that will be used by the employees during dial-up. Click the Apply to finish configurations.	 IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through [Server] [Client] Assigned IP Range Apply ☑ Enable PPTP Server Local IP: 192.168.40.254 Start: 192.168.40.180 End: 192.168.40.199 Username: PptpUsers Password: ******

FIELD	DESCRIPTION	EXAMPLE
Enable PPTP Server	Enable PPTP feature of the MH-5001	Enabled
Local IP	The Local IP is the allocated IP address in the internal Network after PPTP client dials in the MH-5001.	192.168.40.254
Start IP	The Start IP is the allocated starting IP address in the internal network after PPTP client dials in the MH-5001.	192.168.40.180
End IP	The End IP is the allocated ending IP address in the internal network after PPTP client dials in the MH-5001.	192.168.40.199
Username	The account which allow PPTP client user to dial in MH-5001.	PptpUsers
Password	The password which allow PPTP client user to dial in MH-5001.	Dif3wk

Table 16-1 Setup PPTP Server

Step 2 – Setup Windows XP/2000 PPTP clients Note that in the MH-5001 release II version, both PPTP and L2TP can support MPPE. In other words, you can choose “Require data encryption” while a client computer running Windows XP/2000. However, this release II version will not support MS-CHAP, you have to check MS-CHAPv2 checkbox if you would like to require data encryption.	**Configuring A PPTP Dial-Up Connection** 1. Configuring a PPTP dial-up connection 2. Go to Start > Control Panel > Network and Internet Connections > Make new connection. 3. Select Create a connection to the network of your workplace and select Next. 4. Select Virtual Private Network Connection and select Next. 5. Give a Name the connection and select Next. 6. If the Public Network dialog box appears, choose the Don’t dial up initial connection and select Next. 7. In the VPN Server Selection dialog, enter the public IP or hostname of the MH-5001 to connect to and select Next. 8. Set Connection Availability to Only for myself and select Next. 9. Select Finish.
	Customize the VPN Connection 1. Right-click the icon that you have created. 2. Select Properties > Security > Advanced > Settings. 3. Select No Encryption from the Data Encryption and click Apply. 4. Select the Properties > Networking tab. 5. Select PPTP VPN from the VPN Type. Make sure the following are selected: TCP/IP QoS Packet Scheduler 6. Select Apply.
	Connecting to the PPTP VPN 1. Connect to your ISP. 2. Start the dial-up connection configured in the previous procedure. 3. Enter your PPTP VPN User Name and Password. 4. Select Connect.

16.4.2 Setup PPTP Network Client

Step 1 – Enable PPTP Client Fill in the IP address of PPTP Server and allocates Username/Password. When connecting to the PPTP Server successfully, it will appear the allocated IP address for the PPTP client in the “Assigned IP” field.	**ADVANCED SETTINGS > VPN Settings > PPTP > Client**  IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through [Server] [Client] Apply ☑ Enable PPTP Client Server IP: 61.2.1.1 Username: PptpUsers Password: ****** Assigned IP: 192.168.40.100

FIELD	DESCRIPTION	EXAMPLE
Enable PPTP Client	Enable PPTP Client feature of MH-5001	Enabled
Server IP	The IP address of PPTP server.	61.2.1.1
Username	The designed account which allows PPTP client to dial in.	PptpUsers
Password	The designed password which allows PPTP client to dial in.	Dif3wk
Assigned IP	The allocated IP address when PPTP client connects to the PPTP server.	192.168.40.180

Table 16-2 Setup PPTP Client settings

Chapter 17
Remote Access VPN – L2TP

This chapter introduces L2TP and explains how to implement it.

17.1 Demands

1. One employee in our company may sometimes want to connect back to our coporate network to work on something. His PC is PC1_1 in LAN1 instead of DMZ1 so he cannot directly access the host by simply with virtual server settings. This causes inconvenience for the employee to work remotely.

17.2 Objectives

1. With L2TP tunneling, emulate the mobile employee as a member in LAN_1 after he dials in the corporate network. Then he can access all computers in LAN_1 just as if he stays in the office covered by LAN_1.

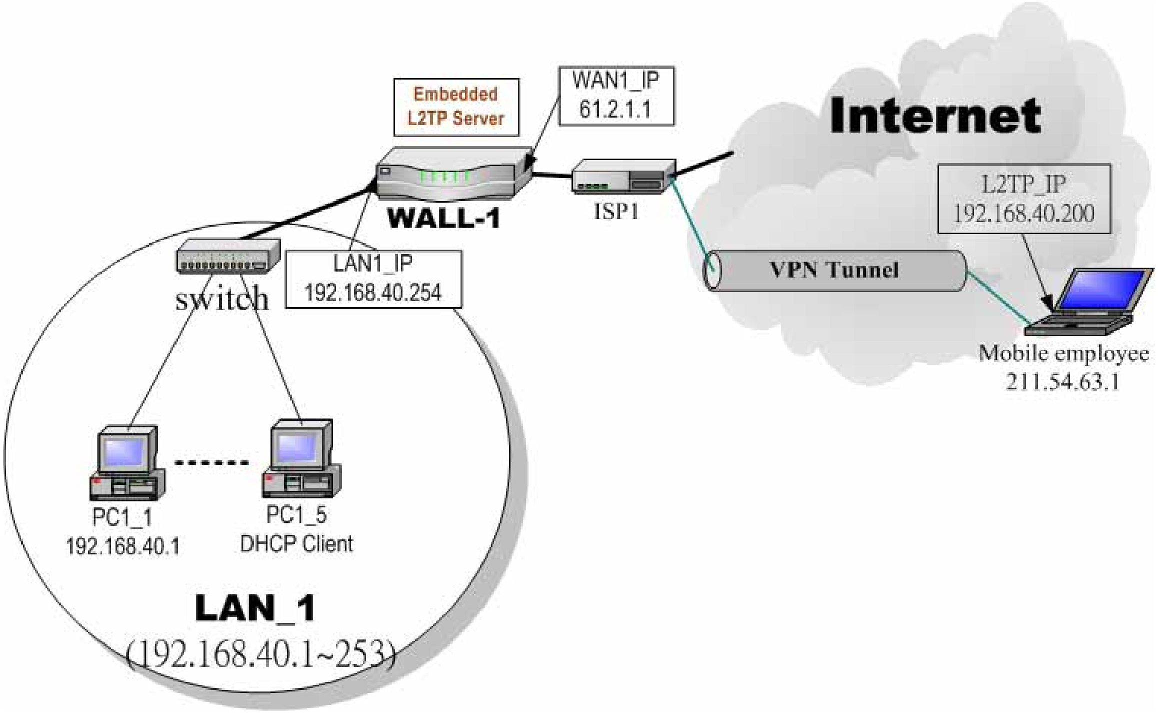


Figure 17-1 L2TP method connection

17.3 Methods

1. Setup the L2TP server at WALL-1, the MH-5001 (LNS: L2TP Network Server). After dialing up to MH-5001, MH-5001 will assign a private IP which falls in the range of the settings in the L2TP server at MH-5001. Suppose the range is defined as 192.168.40.200 ~ 192.168.40.253, the remote host may get an IP of 192.168.40.200 and logically become a member in LAN_1.

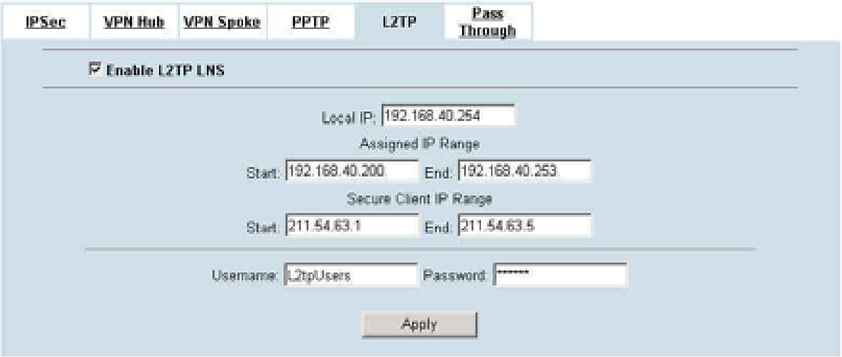
17.4 Steps

17.4.1 Setup L2TP Network Server

Step 1 – Enable L2TP LNS

Check the `Enable L2TP LNS` checkbox, enter the `LAN1_IP` of the `WALL-1` (`192.168.40.254`) in the `Local IP`, and enter the IP range that will be assigned to the L2TP clients in the `Start IP` and the `End IP` fields. Enter the IP range in the `LAC Start IP` and the `LAC End IP` that will cover the real IP of the remote users. In our case, since the employee uses `211.54.63.1` so we can fill `211.54.63.1~211.54.63.5` to cover `211.54.63.1`. Enter the `Username` and `Password` that will be used by the employees during dial-up. Click the `Apply` to finish configurations.

ADVANCED SETTINGS > VPN Settings > L2TP > LNS



☑ Enable L2TP LNS

Local IP: 192.168.40.254

Assigned IP Range
Start: 192.168.40.200 End: 192.168.40.253

Secure Client IP Range
Start: 211.54.63.1 End: 211.54.63.5

Username: L2tpUsers Password: *******

FIELD	DESCRIPTION	EXAMPLE
Enable L2TP LNS	Enable L2TP LNS feature of MH-5001	Enabled
Local IP	The Local IP is the allocated IP address in the internal network after default gateway of L2TP client dials in the MH-5001.	192.168.40.254
Start IP	The Start IP is the allocated starting IP address in the internal network after L2TP client dials in the MH-5001.	192.168.40.200
End IP	The End IP is the allocated ending IP address in the internal network after L2TP client dials in the MH-5001.	192.168.40.253
LAC Start IP	The IP address starting range which is allowed user to dial in LNS server by using L2TP protocol.	211.54.63.1
LAC End IP	The IP address ending range which is allowed user to dial in LNS server by using L2TP protocol.	211.54.63.5
Username	The account which allows L2TP client user to dial in MH-5001.	L2tpUsers
Password	The password which allows L2TP client user to dial in MH-5001.	Dif3wk

Table 17-1 Setup L2TP LNS Server settings

Step 2 – Setup Windows XP/2000 L2TP clients Note that in the MH-5001 release II version, both PPTP and L2TP can support MPPE. In other words, you can choose “Require data encryption” while a client computer running Windows XP/2000. However, this release II version will not support MS-CHAP, you have to check MS-CHAPv2 checkbox if you would like to require data encryption.	**Configuring A L2TP Dial-Up Connection** 1. Configure a L2TP dial-up connection 2. Go to Start > Control Panel > Network and Internet Connections > Make new connection. 3. Select Create a connection to the network of your workplace and select Next. 4. Select Virtual Private Network Connection and select Next. 5. Give a Name the connection and select Next. 6. If the Public Network dialog box appears, choose the Don’t dial up initial connection and select Next. 7. In the VPN Server Selection dialog, enter the public IP or hostname of the MH-5001 to connect to and select Next. 8. Set Connection Availability to Only for myself and select Next. 9. Select Finish.
	Customize the VPN Connection 1. Right-click the icon that you have created. 2. Select Properties > Security > Advanced > Settings. 3. Select No Encryption from the Data Encryption and click Apply. 4. Select the Properties > Networking tab. 5. Select L2TP VPN from the VPN Type. Make sure the following are selected: TCP/IP QoS Packet Scheduler 6. Select Apply.
	Editing Windows Registry The default Windows 2000 L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows 2000 Registry as described in the following steps. Please refer to the Microsoft documentation for editing the Windows Registry. 1. Use the registry editor (regedit) to locate the following key in the registry: HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Rasman \ Parameters 2. Add the following registry value to this key: • Value Name: ProhibitIpSec • Data Type: REG_DWORD • Value: 1 3. Save your changes and restart the computer. You must add the ProhibitIpSec registry value to each Windows 2000-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the ProhibitIpSec registry value is set to 1, your Windows 2000-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy.

	Connecting to the L2TP VPN 1. Connect to your ISP. 2. Start the dial-up connection configured in the previous procedure. 3. Enter your L2TP VPN `User Name` and `Password`. 4. Select `Connect`.

Chapter 18
Remote Access VPN – Windows client

This chapter introduces Remote Access VPN using Windows client and explains how to implement it.

18.1 Demands

Suppose an employee often works at home, he will have the requirement to access the resource inside the company. See Figure 18-1 for this kind of the remote access VPN topology.

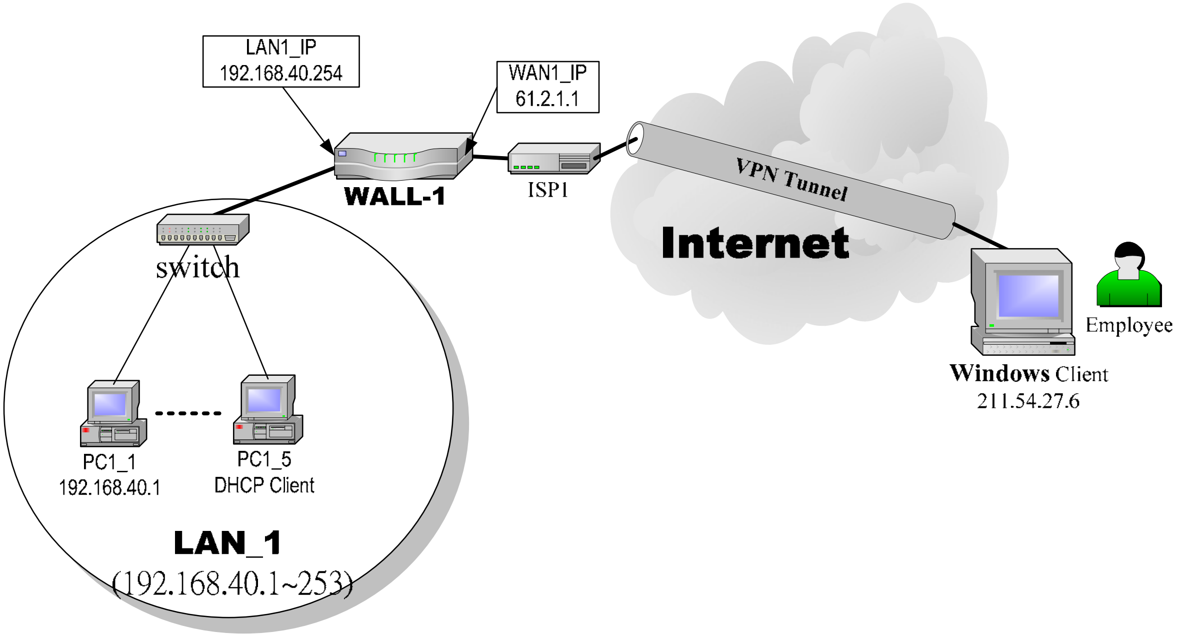


Figure 18-1 Using Windows client to connect MH-5001 IPSec Server

18.2 Objects

Under this circumstance, the employee can use the IPSec VPN method to achieve this target. In the previous chapter, we have introduced the DS-601 client method. In this chapter, we will provide another method to use Windows client solution.

18.3 Methods

As the Figure 18-1 illustrated, we need to setup the IPSec feature of WALL-1, the MH-5001 at company first. On the other hand, we have to setup the related IPSec setting in the Windows client at employee’s side so that the employee can establish the IPSec tunnel through windows client to access the resource of the company.

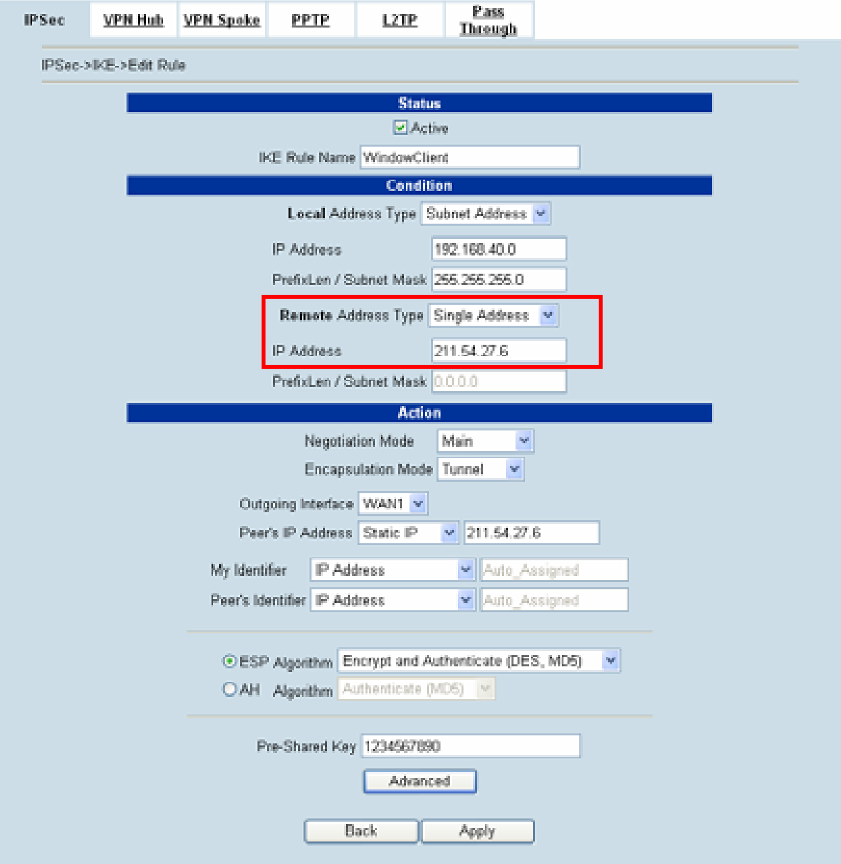
For the procedure to setup the MH-5001, please refer 18.4.1 description.

In the following steps, we would propose the example using windows XP to introduce the setup process.
And the setup procedures will be divided into several parts.

1. Create a custom MMC console, please refer 18.4.2 description.
2. Create an IPSec policy, please refer 18.4.3 description.
3. Add a filter rule from WinXP to MH-5001, please refer 18.4.4 description.
4. Add a filter rule from MH-5001 to WinXP, please refer 18.4.5 description.
5. Configure a rule for WinXP client to MH-5001, please refer 18.4.6 description.
6. Configure a rule for MH-5001 to WinXP client, please refer 18.4.7 description.
7. Enable the security settings, please refer 18.4.8 description.

18.4 Steps

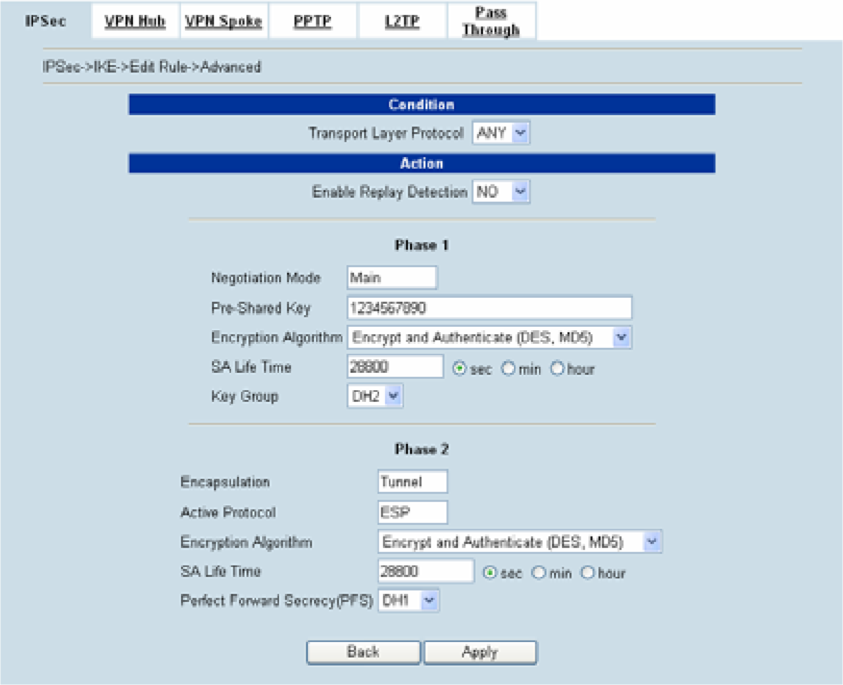
18.4.1 MH-5001 Setup

Step 20. Add an IPSec rule	**ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add**
At the MH-5001 side, we need to add an IPSec policy to establish IPSec tunnel with WinXP client. Enter the related IPSec parameter in the suitable field. Note that because the remote client is just a single WinXP machine, so we select `Single Address` in the `Remote Address Type` field.	 IPSec->IKE->Edit Rule Status ☑ Active IKE Rule Name: WindowClient Condition Local Address Type: Subnet Address IP Address: 192.168.40.0 PrefixLen / Subnet Mask: 255.255.255.0 Remote Address Type: Single Address IP Address: 211.54.27.6 PrefixLen / Subnet Mask: 0.0.0.0 Action Negotiation Mode: Main Encapsulation Mode: Tunnel Outgoing Interface: WAN1 Peer's IP Address: Static IP 211.54.27.6 My Identifier: IP Address Auto_Assigned Peer's Identifier: IP Address Auto_Assigned ● ESP Algorithm: Encrypt and Authenticate (DES, MD5) ○ AH Algorithm: Authenticate (MD5) Pre-Shared Key: 1234567890 IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through Advanced Back Apply

Step 21. Edit the detailed settings of IPSec rule

Fill the detailed settings as the diagram of right side. And then click `Apply` to finish the IPSec rule edition.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add > Advanced



IPSec->IKE->Edit Rule->Advanced

Condition

Transport Layer Protocol: ANY

Action

Enable Replay Detection: NO

Phase 1

Negotiation Mode	Main
Pre-Shared Key	1234567890
Encryption Algorithm	Encrypt and Authenticate (DES, MD5)
SA Life Time	28800 ● sec ○ min ○ hour
Key Group	DH2

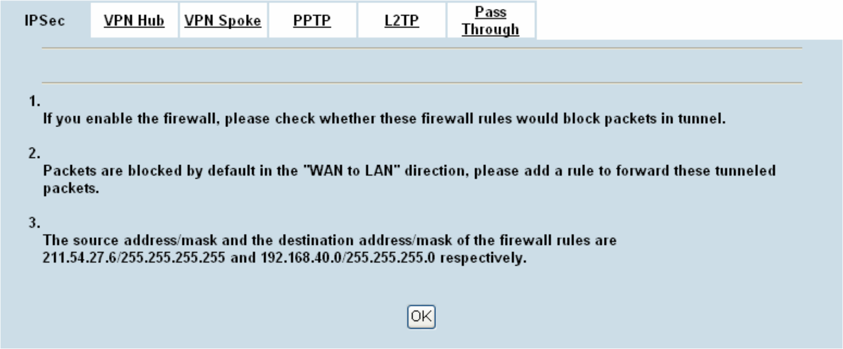
Phase 2

Encapsulation	Tunnel
Active Protocol	ESP
Encryption Algorithm	Encrypt and Authenticate (DES, MD5)
SA Life Time	28800 ● sec ○ min ○ hour
Perfect Forward Secrecy(PFS)	DH1

Step 22. Warning message

Here appears a warning message to remind you to add a firewall rule which can allow IPSec traffic into the MH-5001, because the WAN-to-LAN traffic of the MH-5001 by default is blocked.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add > Apply



1. If you enable the firewall, please check whether these firewall rules would block packets in tunnel.

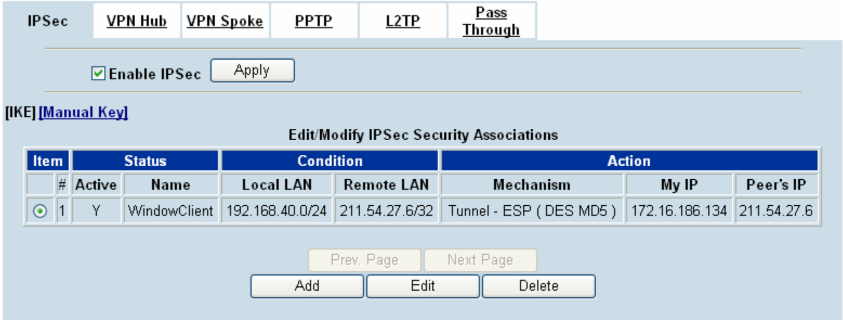
2. Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.

3. The source address/mask and the destination address/mask of the firewall rules are 211.54.27.6/255.255.255.255 and 192.168.40.0/255.255.255.0 respectively.

Step 23. Finish adding an IPSec rule

Finally we have added an IPSec rule shown as the right diagram.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE



☑ Enable IPSec

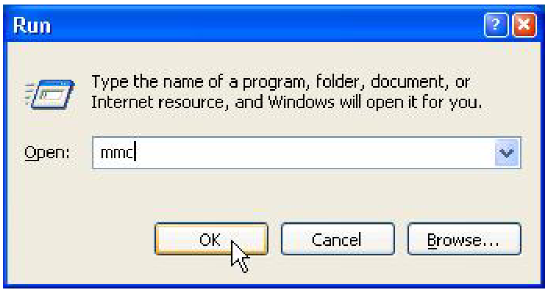
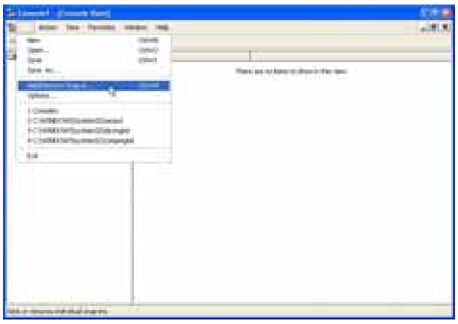
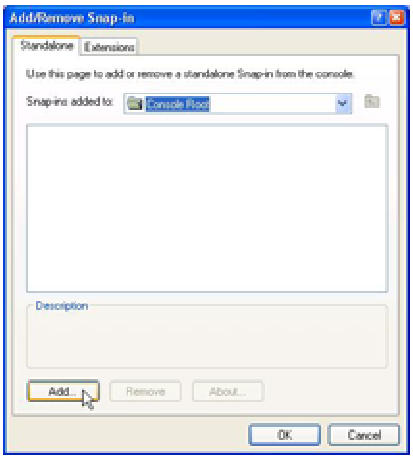
[IKE] [Manual Key]

Edit/Modify IPSec Security Associations

Item		Status		Condition		Action		
	#	Active	Name	Local LAN	Remote LAN	Mechanism	My IP	Peer's IP
●	1	Y	WindowClient	192.168.40.0/24	211.54.27.6/32	Tunnel - ESP (DES MD5)	172.16.186.134	211.54.27.6

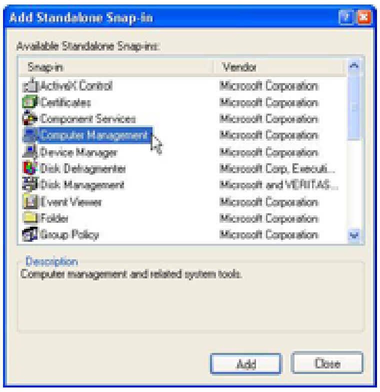
Step 24. Add Firewall rule settings Additionally, because the traffic of WAN to LAN default is blocked. So we must add a firewall rule to allow the local area of remote side to pass through the device. Please refer **錯誤! 找不到參照來源。** for the full description and examples.	N/A

18.4.2 Create a custom MMC console

Step 25. Run mmc From Windows desktop, go to `Start` > Run, and in the `Open` textbox type `mmc`, click `OK.`	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: mmc
Step 26. Add Snap-in On the Console window, click `Add/Remove Snap-In`.	
Step 27. Add a Standalone Snap-in In the `Add/Remove Snap-In` dialog box, click `Add`.	 Add/Remove Snap-in Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Description Standalone Extensions Add... Remove About... OK Cancel

Step 28. Add “Computer Management” snap-in

In the Add Standalone Snap-in dialog box, click Computer Management, and then click Add.



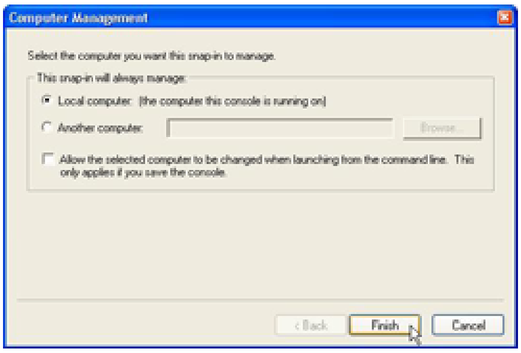
Available Standalone Snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy	Microsoft Corporation

Description
Computer management and related system tools.

Step 29. Verify the Local Computer is selected

Verify that Local Computer (default setting) is selected, and click Finish.



Select the computer you want this snap-in to manage.

This snap-in will always manage:

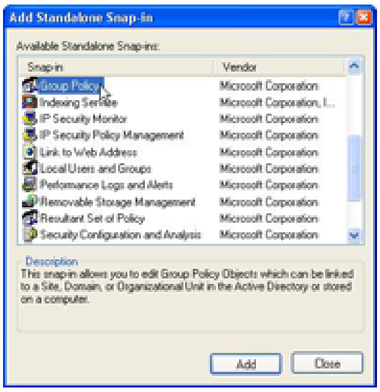
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Step 30. Add “Group Policy” snap-in

In the Add Standalone Snap-in dialog box, click Group Policy, and then click Add.



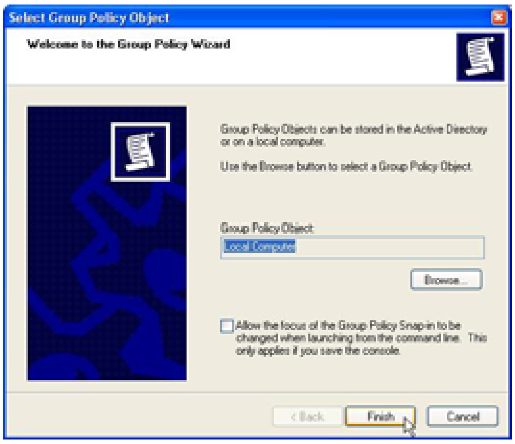
Available Standalone Snap-ins:

Snap-in	Vendor
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	Microsoft Corporation
Resultant Set of Policy	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation

Description
This snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

Step 31. Verify the Local Computer is selected

Verify that Local Computer (default setting) is selected in the Group Policy Object dialog box, and then click Finish.



Welcome to the Group Policy Wizard

Group Policy Objects can be stored in the Active Directory or on a local computer.

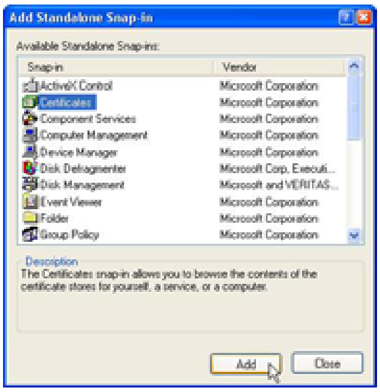
Use the Browse button to select a Group Policy Object.

Group Policy Object:
Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

Step 32. Add “Certificates” snap-in

In the Add Standalone Snap-in dialog box, click Certificates, and then click Add.



Add Standalone Snap-in

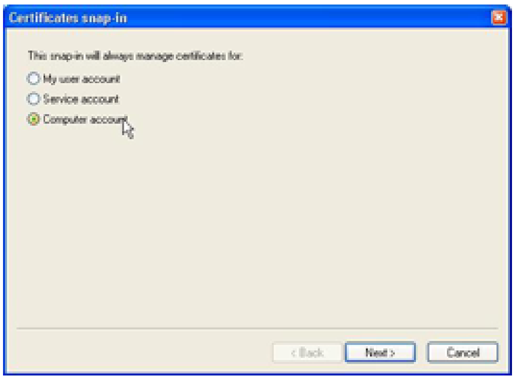
Available Standalone Snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy	Microsoft Corporation

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Step 33. Select Computer account

In the Certificates snap-in dialog box, select Computer account, and click Next.



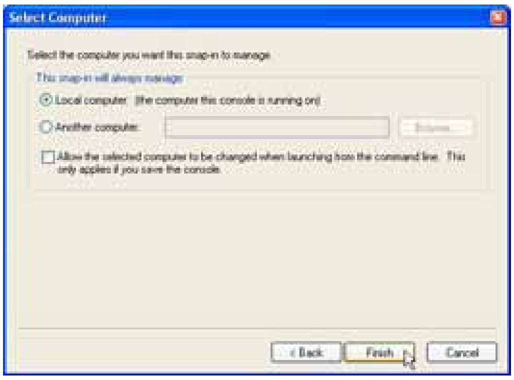
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Step 34. Verify the Local Computer is selected

Verify that Local Computer (default setting) is selected, and click Finish.



Select Computer

Select the computer you want this snap-in to manage.

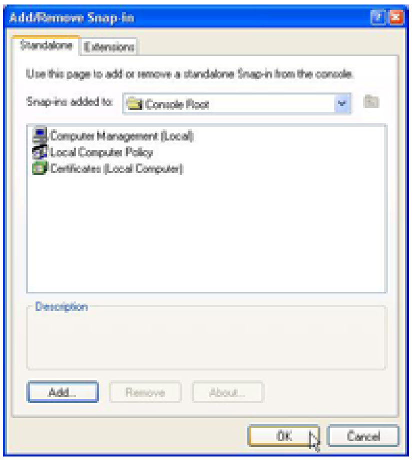
This snap-in will always manage:

● Local computer: (the computer this console is running on)
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Step 35. Close the Add/Remove Snap-in windows

Close the Add Standalone Snap-in dialog box. And then close the Add/Remove Snap-in dialog box.



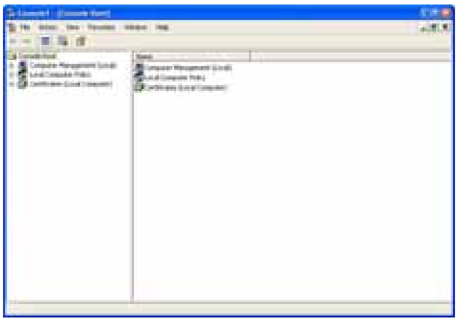
Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

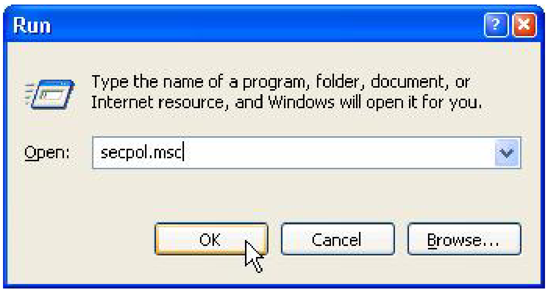
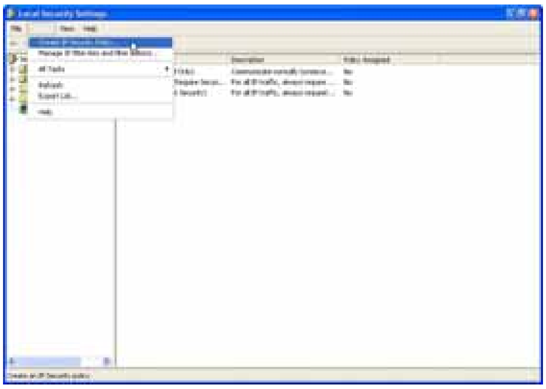
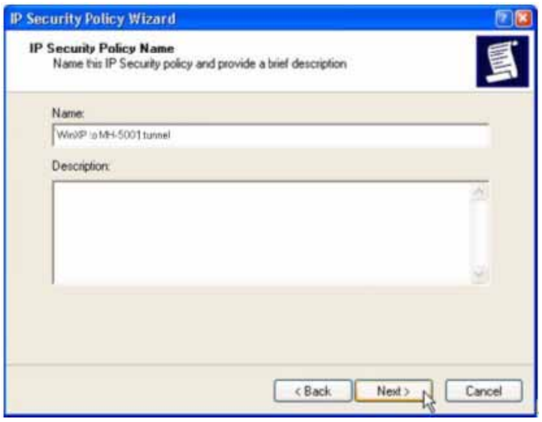
Snap-ins added to: Console Root

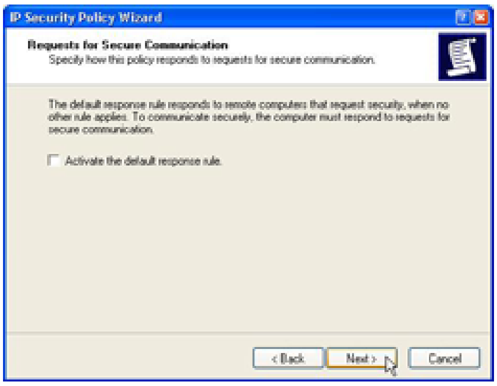
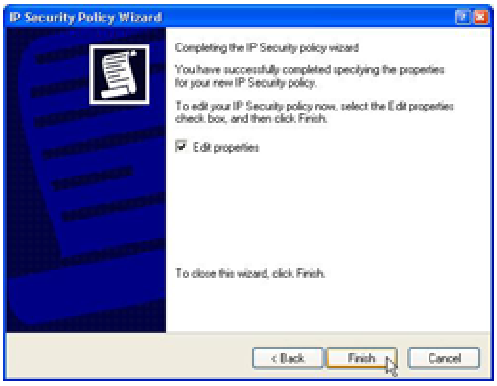
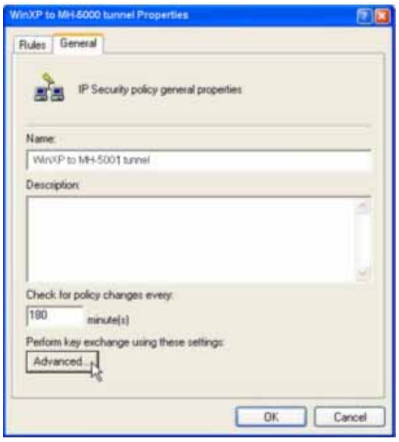
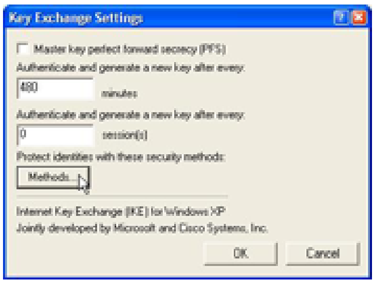
Computer Management (Local)
Local Computer Policy
Certificates (Local Computer)

Description

Step 36. Finish the mmc console creation After finishing the previous steps, we have selected three snap-in components in the mmc console.	

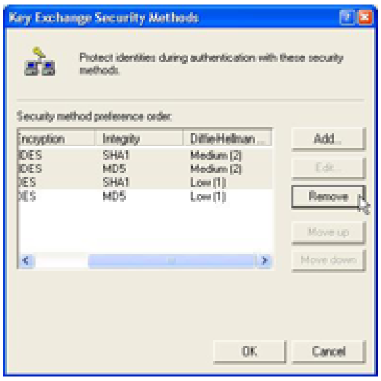
18.4.3 Create an IPSec policy

Step 37. Run secpol.msc From Windows desktop, go to `Start` > `Run`, and in the `Open` textbox, type `secpol.msc`. And then click `OK`.	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: secpol.msc
Step 38. Create IP Security policy Select `Action` > `Create IP Security policy` to add security policy.	
Step 39. Enter policy name Click `Next`, and type a name for your policy. For example, `WinXP to MH-5001 tunnel`.	 IP Security Policy Wizard IP Security Policy Name Name this IP Security policy and provide a brief description Name: WinXP to MH-5001 tunnel Description:

Step 40. Uncheck the item Uncheck `Active the default response rule` checkbox, and click `Next`	 IP Security Policy Wizard Requests for Secure Communication Specify how this policy responds to requests for secure communication. The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication. □ Activate the default response rule.
Step 41. Finish the IP Security policy creation Keep the `Edit properties` check box selected and click `Finish.`	 IP Security Policy Wizard Completing the IP Security policy wizard You have successfully completed specifying the properties for your new IP Security policy. To edit your IP Security policy now, select the Edit properties check box, and then click Finish. ☑ Edit properties To close this wizard, click Finish.
Step 42. Edit policy properties A dialog window will bring up for you to configure two filter rules for this policy. Click `General tab` and click `Advanced` button to setup IPSec phase1 parameters.	 WinXP to MH-5000 tunnel Properties IP Security policy general properties Name: WinXP to MH-5001 tunnel Description: Check for policy changes every: 180 minute(s) Perform key exchange using these settings:
Step 43. Key Exchange Settings Click `Methods` to proceed.	 Key Exchange Settings □ Master key perfect forward secrecy (PFS) Authenticate and generate a new key after every: 480 minutes Authenticate and generate a new key after every: 0 session(s) Protect identities with these security methods: Internet Key Exchange (IKE) for Windows XP Jointly developed by Microsoft and Cisco Systems, Inc.

Step 44. Delete the extra items

In this diagram, we are going to specify the phase1 parameter of IPSec rule at the WinXP. We setup MH-5001 IPSec phase1 with DES-MD5-DH1 (please refer Section 18.4.1), therefore we delete the extra 3 items, and only remain the item that matches our IPSec settings of the MH-5001.



Key Exchange Security Methods

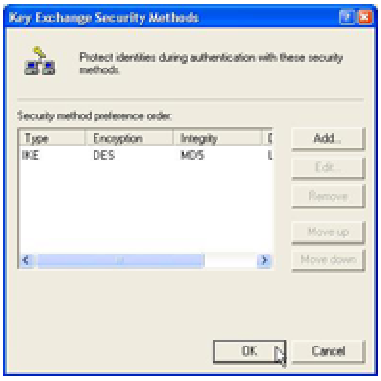
Protect identities during authentication with these security methods.

Security method preference order:

ncryption	Integrity	Diffie-Hellman ...
DES	SHA1	Medium (2)
DES	MD5	Medium (2)
ES	SHA1	Low (1)
ES	MD5	Low (1)

Step 45. Remain the corresponding item

For this example, we remain the item of `DES, MD5 and DH1` combinations.



Key Exchange Security Methods

Protect identities during authentication with these security methods.

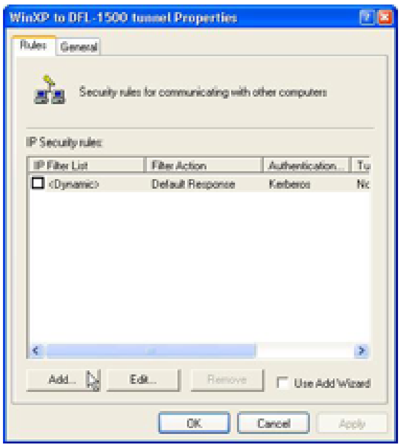
Security method preference order:

Type	Encryption	Integrity	D
IKE	DES	MD5	L

18.4.4 Add a filter rule from WinXP to MH-5001

Step 46. Add a new filter rule

In the tunnel properties, uncheck `Use Add Wizard` check box, and click `Add` to create a new rule. And click `Add` to create a new IP Security Rule.



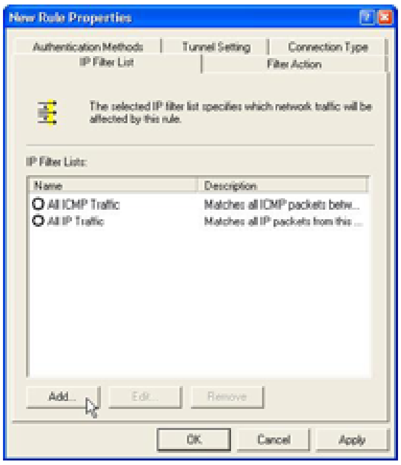
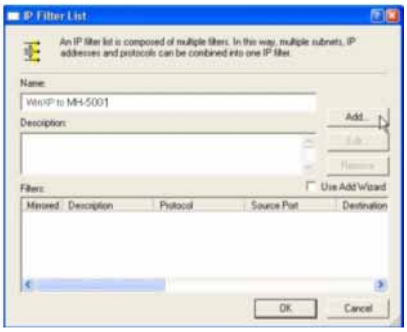
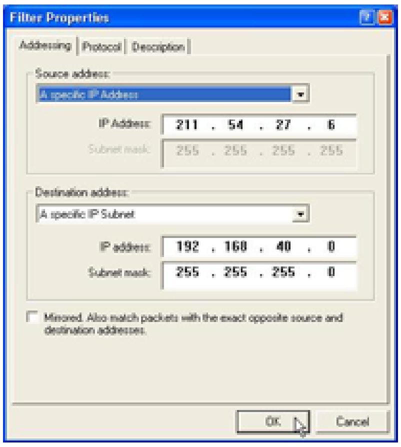
WinXP to DFL-1500 tunnel Properties

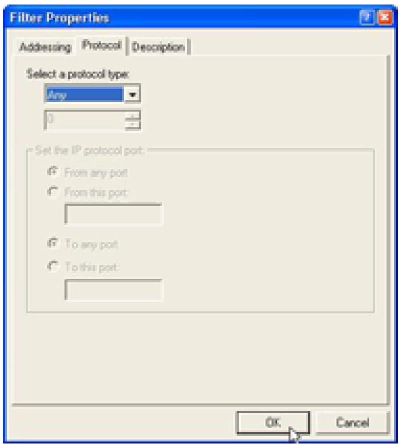
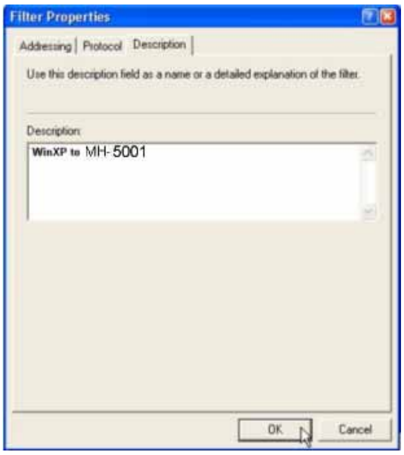
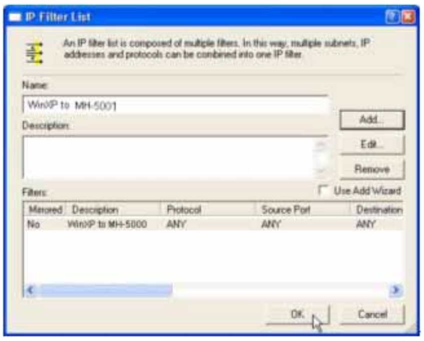
Security rules for communicating with other computers

IP Security rules:

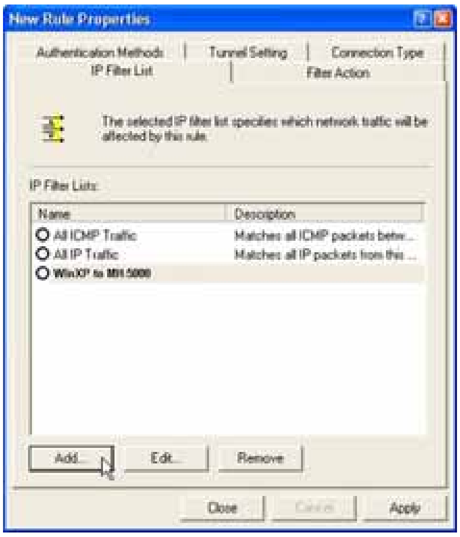
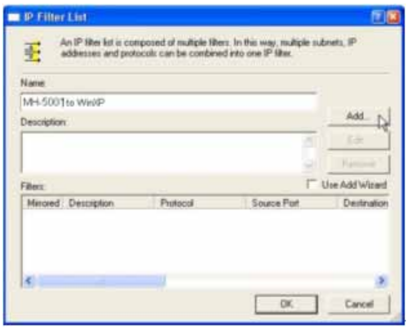
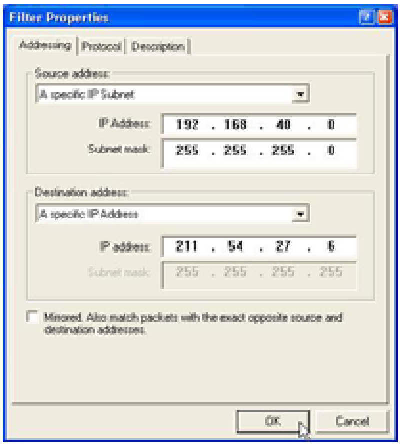
IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	Nc

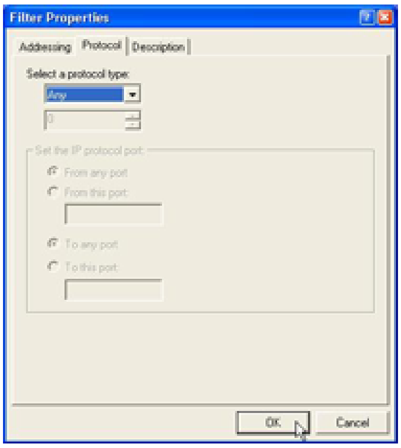
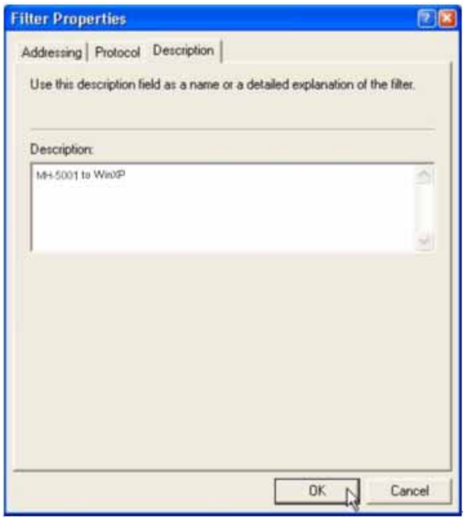
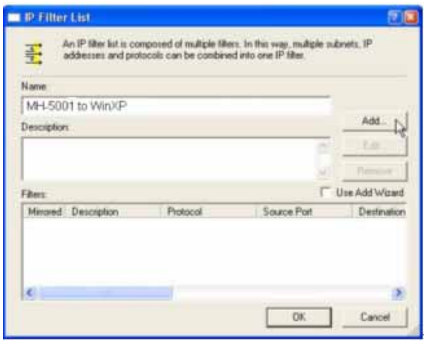
□ Use Add Wizard

Step 47. Add an IP Filter List On the `IP Filter List` tab, click Add to add an `IP Filter List`.	 New Rule Properties Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action The selected IP filter list specifies which network traffic will be affected by this rule. IP Filter Lists: Name: ○ All ICMP Traffic; Description: Matches all ICMP packets betw... Name: ○ All IP Traffic; Description: Matches all IP packets from this ... Add... | Edit... | Remove OK | Cancel | Apply
Step 48. Edit IP filter list Type a name for the filter list (e.g., WinXP to MH-5001), uncheck `Use Add Wizard` check box, and click `Add`.	 IP Filter List An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter. Name: WinXP to MH-5001 Description: Add... | Edit... | Remove Filters: ☐ Use Add Wizard Mirrored | Description | Protocol | Source Port | Destination OK | Cancel
Step 49. Edit the address of filter properties In the `Source address`, choose `A specific IP Address`, and enter the `IP address` of WinXP (ex. 211.54.27.6). In the `Destination address`, choose `A specific IP Subnet`, and enter the `IP address` and `Subnet mask` of the local subnet (ex. 192.168.40.0/255.255.255.0). Uncheck `Mirror check` box. Click `OK` to next.	 Filter Properties Addressing | Protocol | Description Source address: A specific IP Address IP Address: 211 . 54 . 27 . 6 Subnet mask: 255 . 255 . 255 . 255 Destination address: A specific IP Subnet IP address: 192 . 168 . 40 . 0 Subnet mask: 255 . 255 . 255 . 0 ☐ Mirrored. Also match packets with the exact opposite source and destination addresses. OK | Cancel

Step 50. Edit the protocol of filter properties Click the `Protocol` tab. Leave the `protocol type` to `Any`.	 Filter Properties Select a protocol type: Any 0 Set the IP protocol port: ● From any port ○ From this port: ● To any port ○ To this port:
Step 51. Edit the description of filter properties Click the `Description` tab. You can give a name for this filter list. The filter name is displayed in the IPSec monitor when the tunnel is active.	 Filter Properties Use this description field as a name or a detailed explanation of the filter. Description: WinXP to MH-5001
Step 52. Finish the creation of IP filter list Click `OK` and `Close` these windows.	 IP Filter List An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter. Name: WinXP to MH-5001 Description: Filters: Mirrored / Description / Protocol / Source Port / Destination No / WinXP to MH-5000 / ANY / ANY / ANY □ Use Add Wizard

18.4.5 Add a filter rule from MH-5001 to WinXP

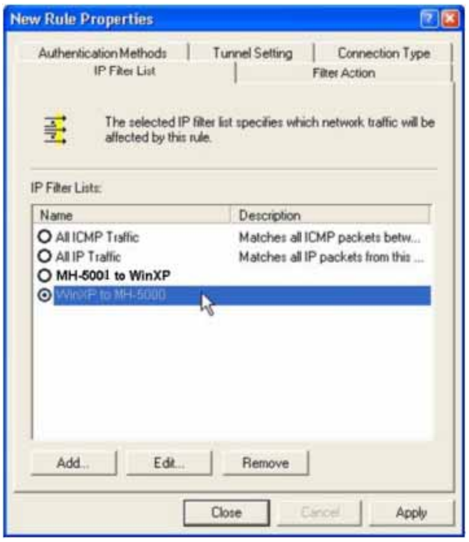
Step 53. Add a new filter rule Click the `IP Filter List` tab, and then click `Add` to add an `IP Filter List`.	 New Rule Properties Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action Add... Edit... Remove Close Cancel Apply The selected IP filter list specifies which network traffic will be affected by this rule. IP Filter Lists: Name / Description ○ All ICMP Traffic — Matches all ICMP packets betw... ○ All IP Traffic — Matches all IP packets from this ... ○ WinXP to MH 5000
Step 54. Edit IP filter list Type a name for the filter list (e.g., MH-5001 to WinXP), uncheck `Use Add Wizard` check box, and click `Add`.	 IP Filter List Add... Edit... Remove Mirrored Description Protocol Source Port Destination OK Cancel An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter. Name: MH-5001 to WinXP Description: Filters: □ Use Add Wizard
Step 55. Edit the address of filter properties In the `Source address`, choose `A specific IP Subnet`, and enter the `IP address` and `Subnet mask` of the local subnet (ex. 192.168.40.0/255.255.255.0). In the `Destination address`, choose `A specific IP Address`, and enter the `IP address` of WinXP (ex. 211.54.27.6). Uncheck `Mirror check` box. Click `OK` to next.	 Filter Properties Addressing Protocol Description OK Cancel Source address: A specific IP Subnet IP Address: 192 . 168 . 40 . 0 Subnet mask: 255 . 255 . 255 . 0 Destination address: A specific IP Address IP address: 211 . 54 . 27 . 6 Subnet mask: 255 . 255 . 255 . 255 □ Mirrored. Also match packets with the exact opposite source and destination addresses.

Step 56. Edit the protocol of filter properties Click the `Protocol` tab. Leave the `protocol type` to `Any`.	 Filter Properties Addressing | Protocol | Description Select a protocol type: Any 0 Set the IP protocol port: ● From any port ○ From this port ● To any port ○ To this port OK Cancel
Step 57. Edit the description of filter properties Click the `Description` tab. You can give a name for this filter list. The filter name is displayed in the IPSec monitor when the tunnel is active.	 Filter Properties Addressing | Protocol | Description Use this description field as a name or a detailed explanation of the filter. Description: MH-5001 to WinXP OK Cancel
Step 58. Finish the creation of IP filter list Click `OK` to close the window.	 IP Filter List An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter. Name: MH-5001 to WinXP Description: Add... Edit... Remove Filters: □ Use Add Wizard Mirrored | Description | Protocol | Source Port | Destination OK Cancel

18.4.6 Configure a rule for WinXP client to MH-5001

Step 59. Select the first IP filter list

Now there are two IP filter lists for the WinXP IPSec use. Select the first filter list you have created above from the `IP Filter List`, such as `WinXP to MH-5001.`



New Rule Properties

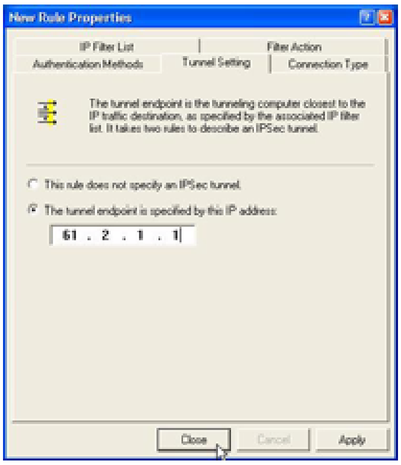
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ MH-5001 to WinXP	
● WinXP to MH-5000	

Step 60. Tunnel Settings

Click `Tunnel Setting` tab, enter the remote endpoint. For this filter list, the remote IPSec endpoint is MH-5001 (`61.2.1.1`).



New Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

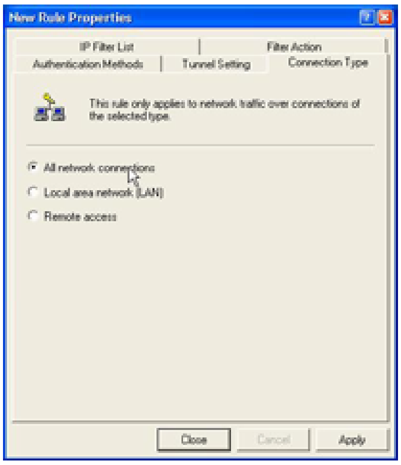
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

61 . 2 . 1 . 1

Step 61. Connection Type

Click `Connection Type` tab, and then click `All network connections.`



New Rule Properties

This rule only applies to network traffic over connections of the selected type.

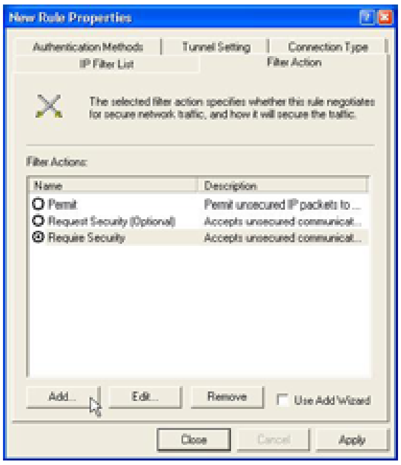
● All network connections

○ Local area network (LAN)

○ Remote access

Step 62. Edit filter action of WinXP to MH-5001 IP filter list

Click `Filter Action` tab, click Add to add a new `Filter Action`.



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

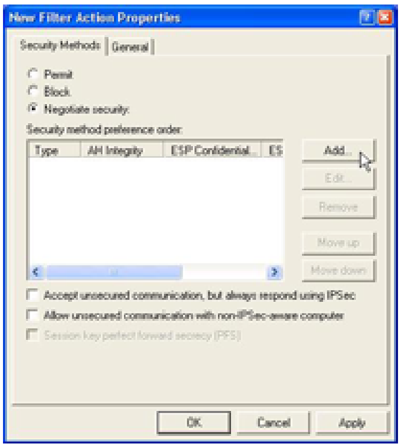
Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

☐ Use Add Wizard

Step 63. Set the properties of Security Methods

Leave `Negotiate security` as checked, and uncheck `Accept unsecured communication, but always respond using IPSec` check box. You must do this to ensure secure connections. Click `Add` to proceed.



○ Permit
○ Block
● Negotiate security:

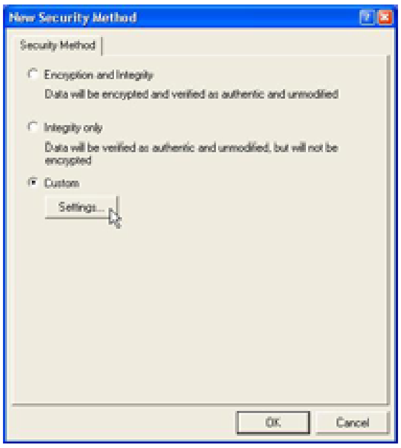
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES

☐ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non-IPSec-aware computer
☐ Session key perfect forward secrecy (PFS)

Step 64. Setting the Security Method

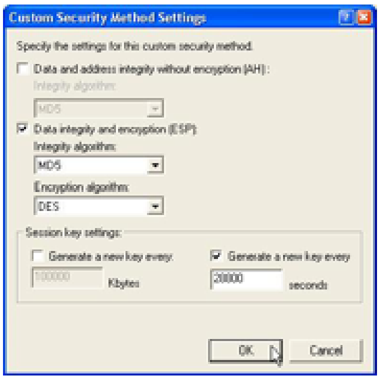
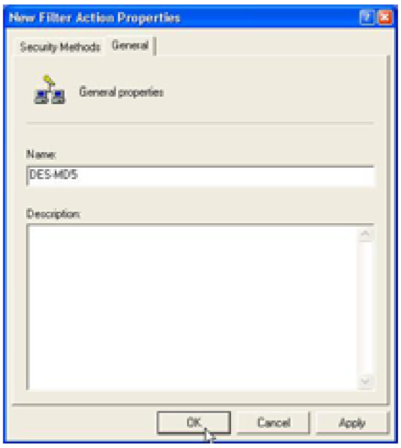
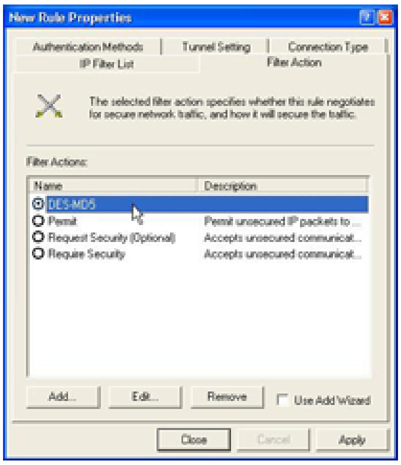
Select `Custom` (for expert users) if you want to define specific algorithms and session key lifetimes). Please make sure the settings match whatever we had configured in MH-5001 before



○ Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified

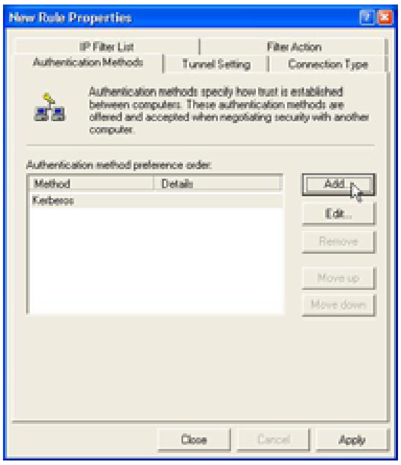
○ Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted

● Custom

Step 65. Custom security method settings Select the `Data integrity encryption (ESP)`. Select `MD5` integrity algorithms and `DES` encryption algorithm. Fill the new key generation rate (ex. 28800 sec). Note that the settings of this page must match the settings of IPSec phase2 at MH-5001.	 Custom Security Method Settings Specify the settings for this custom security method. ☐ Data and address integrity without encryption (AH): Integrity algorithm: MD5 ☑ Data integrity and encryption (ESP): Integrity algorithm: MD5 Encryption algorithm: DES Session key settings: ☐ Generate a new key every: 100000 Kbytes ☑ Generate a new key every 28800 seconds OK Cancel
Step 66. New Filter Action Properties Click the `General` tab. Give a name to the filter action. For example, `DES-MD5`, and click `OK.`	 New Filter Action Properties Security Methods General General properties Name: DES-MD5 Description: OK Cancel Apply
Step 67. Filter Action Select the filter action (`DES-MD5`) you just created.	 New Rule Properties Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic. Filter Actions: Name — Description ● DES-MD5 ○ Permit — Permit unsecured IP packets to ... ○ Request Security (Optional) — Accepts unsecured communicat... ○ Require Security — Accepts unsecured communicat... Add... Edit... Remove ☐ Use Add Wizard Close Cancel Apply

Step 68. Authentication Methods

Click the `Authentication Methods` tab, and then click Add.



New Rule Properties

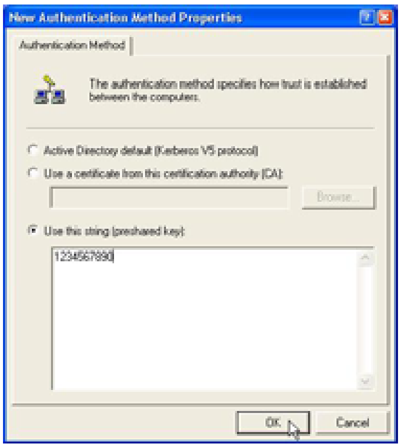
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

Step 69. Select the authentication methods

Select `Use this string (pre-shared key)` option. And enter the string `1234567890` in the text box.



New Authentication Method Properties

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

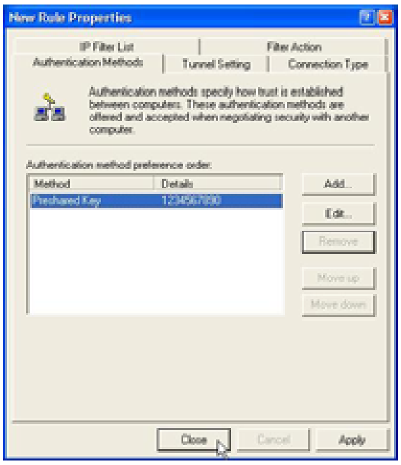
○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

1234567890

Step 70. Delete Kerberos method

Delete the original `Kerberos` method. Just select the `Preshared Key` we defined before. Click `Close` to finish the WinXP to MH-5001 Rule settings.



New Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

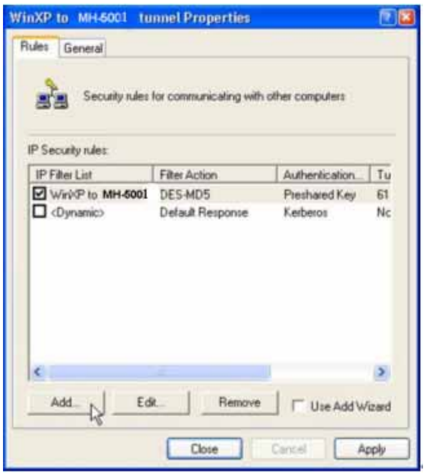
Authentication method preference order:

Method	Details
Preshared Key	1234567890

18.4.7 Configure a rule for MH-5001 to WinXP client

Step 71. Add a new IP filter rule

Now we are going to configure the rule of MH-5001 to WinXP client. Click Add to add a new IP filter rule.



Security rules for communicating with other computers

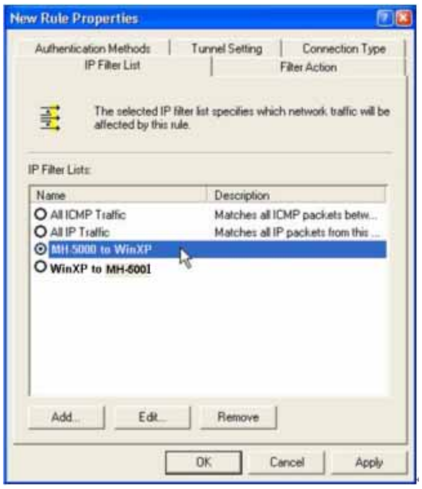
IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ WinXP to **MH-5001**	DES-MD5	Preshared Key	61
□ <Dynamic>	Default Response	Kerberos	Nc

□ Use Add Wizard

Step 72. Select IP filter list

Click the `IP Filter List` tab. Select the filter list you created above from the `IP Filter List` (`MH-5001 to WinXP).`



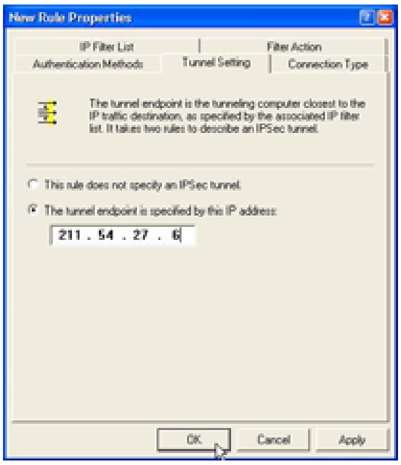
The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● MH-5000 to WinXP	
○ **WinXP to MH-6001**	

Step 73. Tunnel Settings

Click `Tunnel Setting` tab, and then enter the remote endpoint. For this filter list, the remote IPSec endpoint is WinXP (`211.54.27.6`).

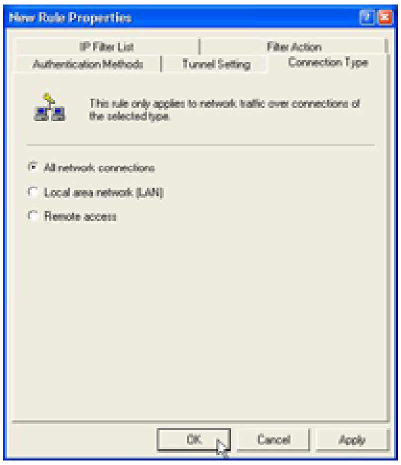
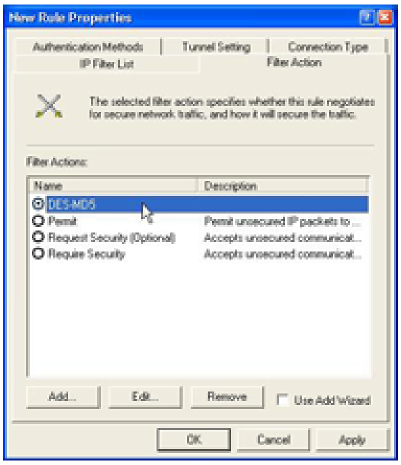
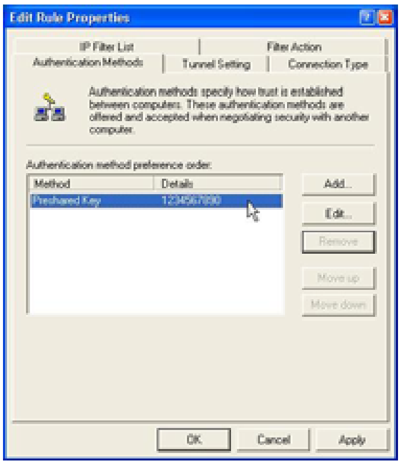


The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

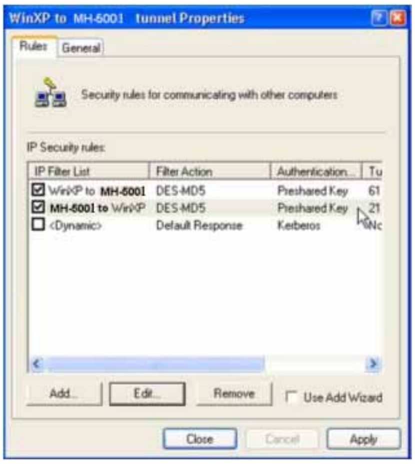
● The tunnel endpoint is specified by this IP address:

211 . 54 . 27 . 6

Step 74. Connection Type Click `Connection Type` tab, and then click `All network connections`.	 New Rule Properties This rule only applies to network traffic over connections of the selected type. ● All network connections ○ Local area network (LAN) ○ Remote access
Step 75. Filter Action Click `Filter Action` tab, and then select the filter action (`DES-MD5`) you just created.	 New Rule Properties The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic. Filter Actions: Name — Description ● DES-MD5 ○ Permit — Permit unsecured IP packets to ... ○ Request Security (Optional) — Accepts unsecured communicat... ○ Require Security — Accepts unsecured communicat... □ Use Add Wizard
Step 76. Authentication Methods Click `Authentication Methods` tab, select the `Preshared Key` we defined before. Click `OK` to finish the rule creation.	 Edit Rule Properties Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer. Authentication method preference order: Method — Details Preshared Key — 1234567890

Step 77. Finish the rules edition

The `IP Security rule` of `MH-5001 to WinXP` is configured completely as the figure listing. Click `Close` to finish the settings.

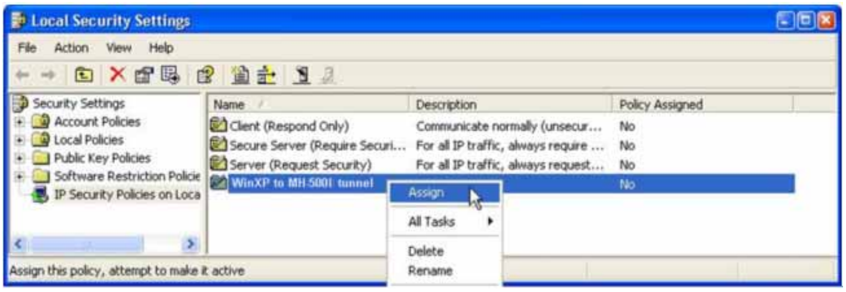

WinXP to MH-5001 tunnel Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

	IP Filter List	Filter Action	Authentication...	Tu
☑	WinXP to **MH-5001**	DES-MD5	Preshared Key	61
☑	**MH-5001 to** WinXP	DES-MD5	Preshared Key	21
□	<Dynamic>	Default Response	Kerberos	Nc

18.4.8 Enable the security settings

Step 78. Assign the security policy

Use the pop-up menu to assign the security rule which we have configured.

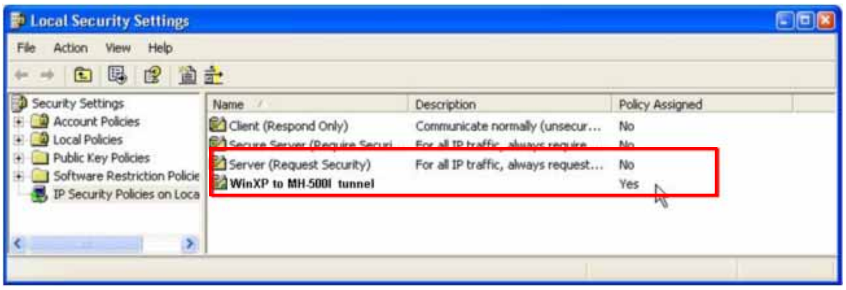


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecur...	No
Secure Server (Require Securi...	For all IP traffic, always require ...	No
Server (Request Security)	For all IP traffic, always request...	No
WinXP to MH-5001 tunnel		No

Assign this policy, attempt to make it active

Step 79. Finish all the settings of WinXP

After the above configurations, now you can use WinXP to connect back to the local company behind the MH-5001 device.



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecur...	No
Secure Server (Require Securi	For all IP traffic, always require	No
Server (Request Security)	For all IP traffic, always request...	No
WinXP to MH-5001 tunnel		Yes

Chapter 19
Content Filtering – Web Filters

This chapter introduces web content filters and explains how to implement it.

19.1 Demands

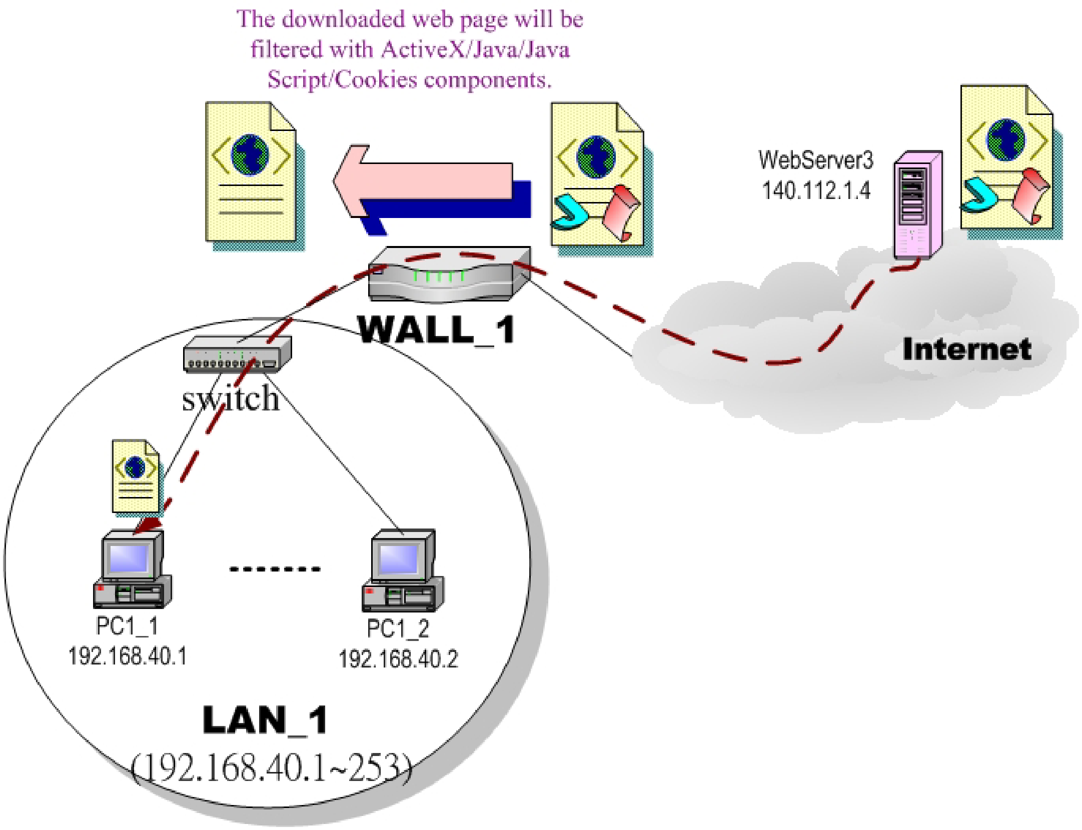


Figure 19-1 Use web filter functionality to avoid users browsing the forbidden web site

1. As the above Figure 19-1 illustrates, someone (PC1_1) is browsing the web pages at the WebServer3. The contents of the web pages may include cookies, Java applets, Java scripts or ActiveX objects that may contain malicious program of users' information. So, we wish to prohibit the user (PC1_1) from downloading the forbidden components.

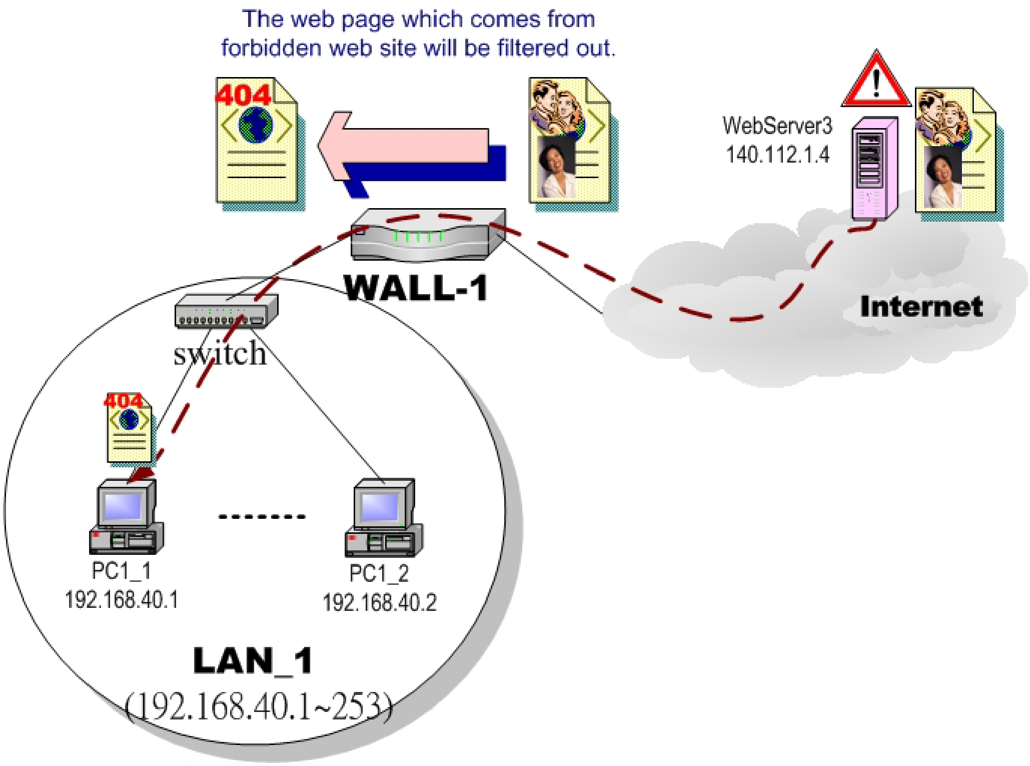


Figure 19-2 Use web filter functionality to avoid users view the forbidden web site

2. As the above Figure 19-2 illustrates, someone (PC1_1) is browsing forbidden web pages on office hours. The contents of the web pages may include stock markets, violence, or sex that will waste the bandwidth of the Internet access link while degrading the efficiency of normal working hours. So, we wish to prohibit the user (PC1_1) from viewing the page on the forbidden web site.

19.2 Objectives

1. Remove the cookies, Java applet, Java scripts, ActiveX objects from the web pages.
2. Prevent users from connecting to the forbidden sites.

19.3 Methods

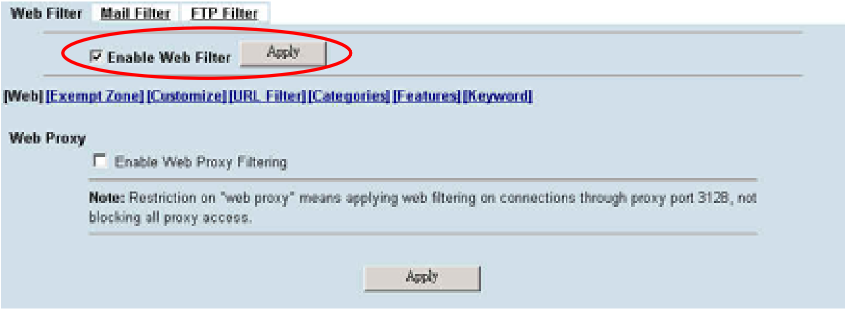
1. Setup content filtering for web objects such as cookies and Java applets.
2. Setup content filtering for URL requests. For each URL, check the pre-defined upgradeable URL database, self-entered forbidden domains, and self-entered keywords to check if the URL is allowed.

19.4 Steps

Step 1. Enable Web Filter

Check the `Enable Web Filter` checkbox and click the `Apply` right on the right side.

ADVANCED SETTINGS > Content Filters > Web Filter > Web



Web Filter
Mail Filter
FTP Filter
[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]
Apply
Apply

☑ Enable Web Filter

Web Proxy

□ Enable Web Proxy Filtering

Note: Restriction on "web proxy" means applying web filtering on connections through proxy port 3128, not blocking all proxy access.

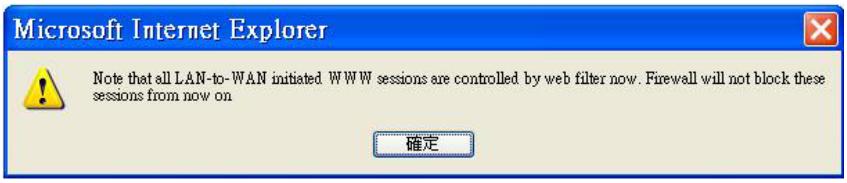
FIELD	DESCRIPTION	EXAMPLE
Enable Web Filter	Enable Web Filter feature of MH-5001	Enabled
Enable Web Proxy Filtering	If enabling this feature, all the web pages pass through proxy (**Only** port 3128) will also be verified by MH-5001. If disabling the "Web Proxy", all the web pages through will bypass the verification.	Disabled
BUTTON	DESCRIPTION	
Apply	Apply the settings which have been configured.	

Table 19-1 Enable Web Filter

Step 2. Warning of Firewall

This is a warning saying that if you block any web traffic from LAN-to-WAN in Firewall, the access control is shift to the Web Filter. Namely, if you block someone to access the web at the WAN side, after enabling the web filter, he can resume accessing the web until you set a content filter rule to block it.

ADVANCED SETTINGS > Content Filters > Web Filter > Web



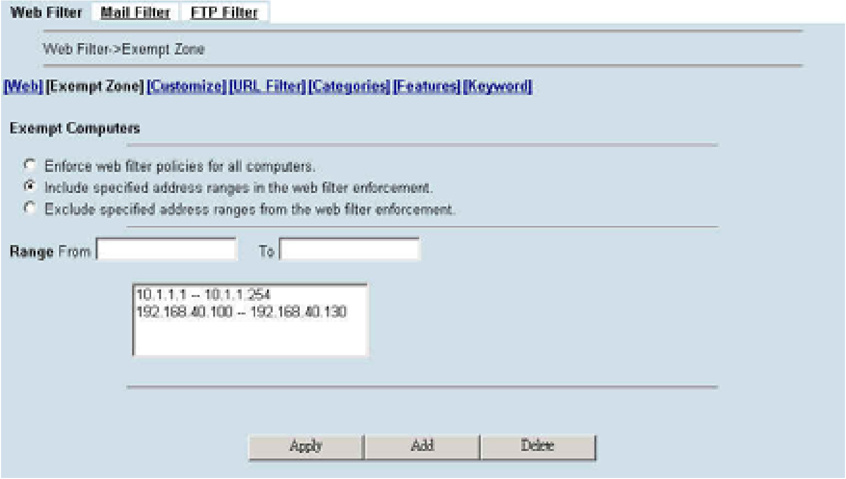
Microsoft Internet Explorer

Note that all LAN-to-WAN initiated WWW sessions are controlled by web filter now. Firewall will not block these sessions from now on

Step 3. Further Customize the local zones

You can configure to what range the filters will apply to the local zones. By default, the web filters apply to all computers so the "`Enforce web filter policies for all computers`" is selected, and the range is `0.0.0.0` – `255.255.255.255`. Delete the default range by clicking the range item and the `Delete` button. Enter the IP range in the `Range` fields followed by a click of the `Add` button to add one address range to the web filter. Click "`Include`…… " and `Apply` if you want web filters to only apply to the specified ranges. Click "`Exclude`……" and `Apply` if you want web filters to apply to all computers except those specified ranges.

ADVANCED SETTINGS > Content Filters > Web Filter > Exempt Zone



Web Filter
Mail Filter
FTP Filter
[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]
Apply
Add
Delete

Web Filter->Exempt Zone

Exempt Computers

○ Enforce web filter policies for all computers.
● Include specified address ranges in the web filter enforcement.
○ Exclude specified address ranges from the web filter enforcement.

Range From ____ To ____

10.1.1.1 -- 10.1.1.254
192.168.40.100 -- 192.168.40.130

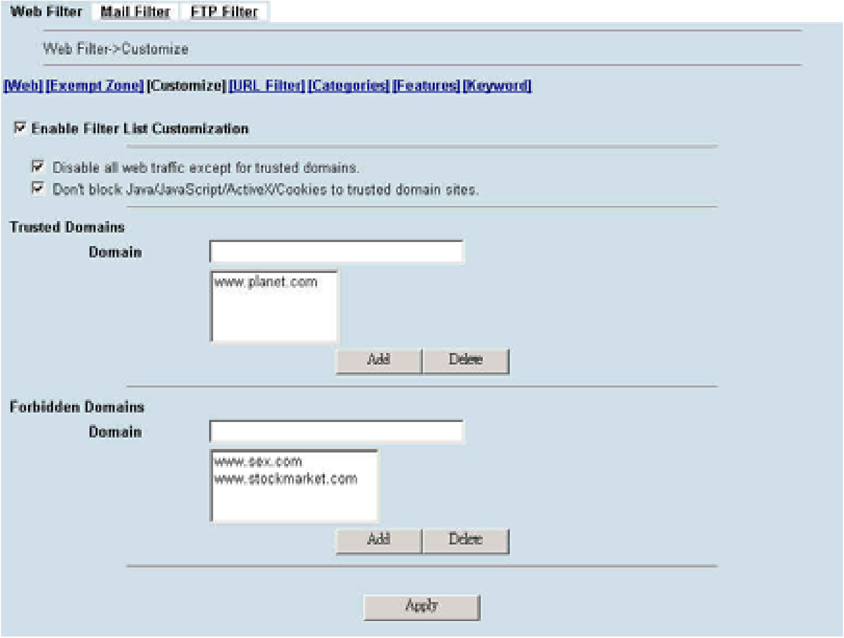
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Exempt Computers	Determine which IP range will exempt the verification by the web filter		
Enforce web filter policies for all computers	Web filter actives at all the computers, not limit range of the IP addresses	Enable/Disable	disabled
Include specified address ranges in the web filter enforcement	Web filter will only active at below specified computers.	Enable/Disable	Enabled
Exclude specified address ranges from the web filter enforcement	Except below specified IP address ranges. All the other IP address range, Web filter will active totally.	Enable/Disable	disabled
Range From	Here we can setup the IP address range, for the above Exempt Computers to use.	IPv4 format (Max: 256 entries)	10.1.1.1 – 10.1.1.254 192.168.40.100 – 192.168.40.130
BUTTON	DESCRIPTION		
Apply	Apply the above selected “Exempt Computers” radius button.		
Add	Add the specified IP range which filled in the above “Range From” field.		
Reset	Clean the filled data and restore the original one.		
Delete	Delete the specified IP range which filled in the above “Range From” field.		

Table 19-2 Web Filter Exempt Zone setting page

Step 4. Customize the specified sites

Check the `Enable Filter List Customization` to allow all accesses to the `Trusted Domains` while disallowing all accesses to the `Forbidden Domains`. Check the `Disable all web traffic except for trusted domains` if you want to only allow the access to the Trusted Domains. However, if the web objects are set to be blocked by the MH-5001 in step 3, these allowed accesses will never be able to retrieve these objects. Check the “`Don’t block …`” to allow the objects for these trusted domains. The domains are maintained by enter the address in the `Domain` field with a click of the `Add` button. To delete a domain, click the domain with a click of the `Delete` button.

ADVANCED SETTINGS > Content Filters > Web Filter > Customize


Web Filter
Mail Filter
FTP Filter
Web Filter->Customize
[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]
Add
Delete
Add
Delete
Apply

☑ Enable Filter List Customization

☑ Disable all web traffic except for trusted domains.

☑ Don't block Java/JavaScript/ActiveX/Cookies to trusted domain sites.

Trusted Domains

Domain: www.planet.com

Forbidden Domains

Domain: www.sex.com
www.stockmarket.com

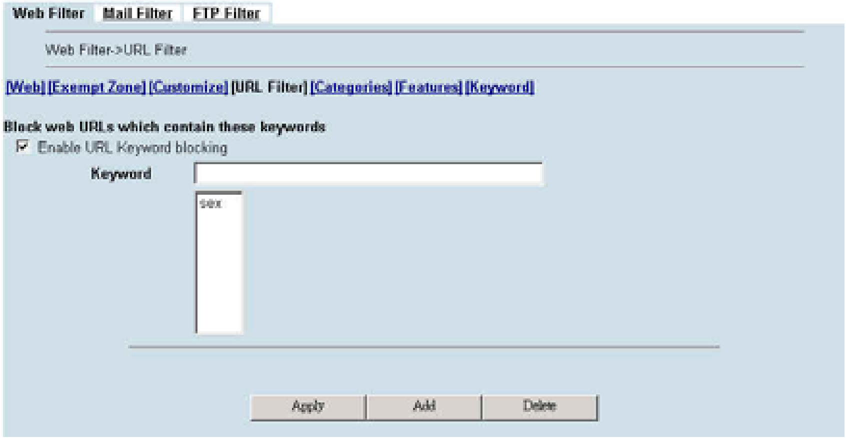
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Enable Filter List Customization	Enable the Filter List Customization feature of web filter. If you only enable it, all the domains in the `Trusted Domains` will be allowed to pass through MH-5001. Contrarily, all the domains in the `Forbidden Domain` will be blocked by the MH-5001.	Enable/Disable	Enabled
Disable all web traffic except for trusted domains	Except the following specified domain range specified by the trusted domain. All the other URL domain IP addresses are all blocked access.	Enable/Disable	Enabled
Don't block Java/Java Script/ActiveX/Cookies to trusted domain sites	In the following domain range of the trusted domains. If there are include Java/ Java Script/ActiveX/Cookies components in the web page, the action is setting not to block.	Enable/Disable	Enabled
Trusted Domains Domain	Here we can specify the Trusted Domains for the above item using. You can enter either domain name or IP address. Note: if the domain name can not be resolved by the DNS server, the domain name entry will be ignored. Another issue is that if there are a lot of domain names in Customize area, name resolving will take longer time on Web Filter starting up.	Max: 256 entries	www.planet.com.tw
Forbidden Domains Domain	Here we can specify the Forbidden Domains for the above item using. You can enter either domain name or IP address. Note: if the domain name can not be resolved by the DNS server, the domain name entry will be ignored. Another issue is that if there are a lot of domain names in Customize area, name resolving will take longer time on Web Filter starting up.	Max: 256 entries	www.stockmarket.com www.sex.com
BUTTON	DESCRIPTION		
Add	Add the Trusted/Forbidden Domains IP range to the list.		
Delete	Delete the Trusted/Forbidden Domains IP range from the list.		
Apply	Apply the setting which configured on the checkbox.		

Table 19-3 Web Filter Customize setting page

Step 5. Setup URL keyword blocking

Check the `Enable Keyword Blocking` to block any URLs that contains the entered keywords. Add a key word by entering a word in the `keyword` field followed by a click of `Add`.

ADVANCED SETTINGS > Content Filters > Web Filter > URL Filter



Web Filter | Mail Filter | FTP Filter

Web Filter->URL Filter

[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]

Block web URLs which contain these keywords

☑ Enable URL Keyword blocking

Keyword:

sex

Apply | Add | Delete

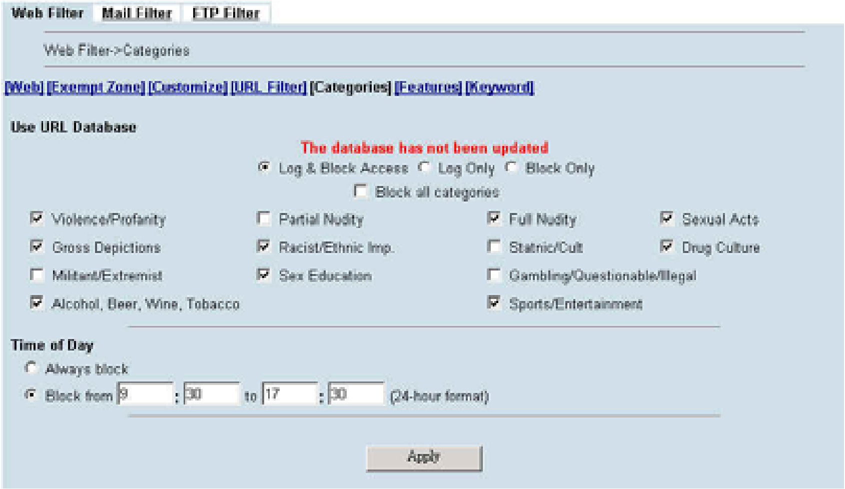
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Enable Keyword blocking	Enable URL keyword blocking feature of web filter	Enable/Disable	Enabled
Keyword	If the Keyword appears in the URL when connect to the Internet using browser. The contents about the URL will be block.	text string (Max: 256 entries)	sex
BUTTON	**DESCRIPTION**		
Apply	Apply the setting which configured on the checkbox.		
Add	Add the Keyword to the list.		
Delete	Delete the selected keyword from the list.		

Table 19-4 Web Filter URL Filter setting page

Step 6. Customize Categories

With the built-in URL database, MH-5001 can block web sessions towards several pre-defined `Categories` of URLs. Check the items that you want to block or log. Simply click the `Block all categories` will apply all categories. Click `Log & Block Access` if you want to block and log any matched traffic. You can customize the `Time of Day` to allow such traffic after the office hours, such as `9:30` to `17:30`.

ADVANCED SETTINGS > Content Filters > Web Filter > Categories



Web Filter | Mail Filter | FTP Filter

Web Filter->Categories

[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]

Use URL Database

The database has not been updated

● Log & Block Access ○ Log Only ○ Block Only

☐ Block all categories

☑ Violence/Profanity ☐ Partial Nudity ☑ Full Nudity ☑ Sexual Acts

☑ Gross Depictions ☑ Racist/Ethnic Imp. ☐ Statnic/Cult ☑ Drug Culture

☐ Militant/Extremist ☑ Sex Education ☐ Gambling/Questionable/Illegal

☑ Alcohol, Beer, Wine, Tobacco ☑ Sports/Entertainment

Time of Day

○ Always block

● Block from 9 : 30 to 17 : 30 (24-hour format)

Apply

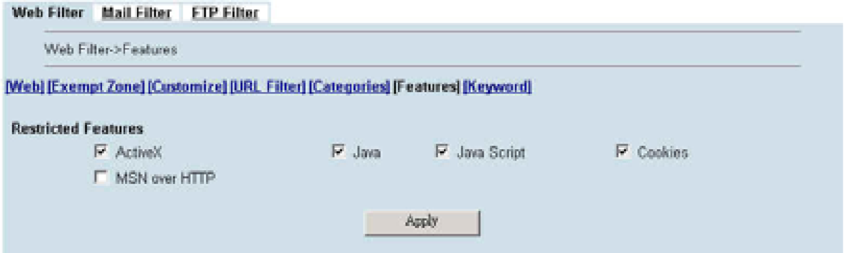
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Use URL Database	Determine how to deal with the URL types in this page.	Log & Block Access / Log Only / Block Only	Log & Block Access
Block all categories	Make all categories below enabled	Enable/Disable	disabled
Violence/Profanity, Gross Depictions, Militant/Extremist ,etc. items	Check the categories you would like to enable	Enable/Disable	Enable the checked ones
Time of Day	The time which was set for Web Filter.	24-hour format	9:30 ~ 17:30
BUTTON	DESCRIPTION		
Apply	Apply the settings which have been configured.		

Table 19-5 Web Filter Categories setting page

Step 7. Customize Objects

Check the objects of `Restricted Features` to block the objects. Click the `Apply` button at the bottom of this page. Use PC1_1 to browse the web page to see if the objects are blocked. If the objects still exist, the objects may be cached by the browser. Please clear the cache in the web browser, close the browser, reopen the browser, and connect to the web page again.

ADVANCED SETTINGS > Content Filters > Web Filter > Features



Web Filter
Mail Filter
FTP Filter
Web Filter->Features
[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]
Apply

Restricted Features

☑ ActiveX ☑ Java ☑ Java Script ☑ Cookies
☐ MSN over HTTP

FIELD	DESCRIPTION	EXAMPLE
Restricted Features	Select the below items that will verified by Web Filter of MH-5001.	
ActiveX	filter the web page that includes ActiveX	Enabled
Java	filter the web page that includes Java applet	Enabled
Java Script	filter the web page that includes Java Script	Enabled
Cookies	filter the web page that includes Cookies	Enabled
MSN over HTTP	filter MSN application which is through http proxy	Disabled
BUTTON	DESCRIPTION	
Apply	Apply the settings which have been configured.	

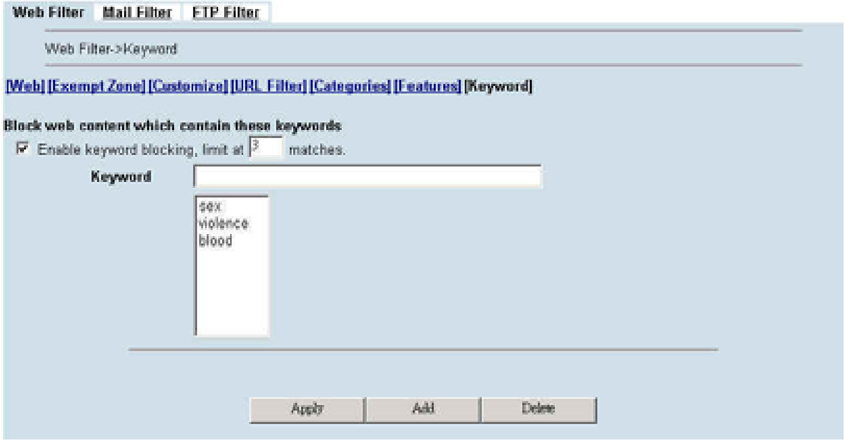
Table 19-6 Web Filter Features

Step 8. Setup contents keyword blocking

Check the `Enable Keyword Blocking` to block any Web pages that contain the entered keywords. Add a key word by entering a word in the `Keyword` field and then click Add to proceed.

Note that you can add the keywords as many as you like.

ADVANCED SETTINGS > Content Filters > Web Filter > Keyword



Web Filter->Keyword

[Web] [Exempt Zone] [Customize] [URL Filter] [Categories] [Features] [Keyword]

Block web content which contain these keywords

☑ Enable keyword blocking, limit at 3 matches.

Keyword

sex
violence
blood

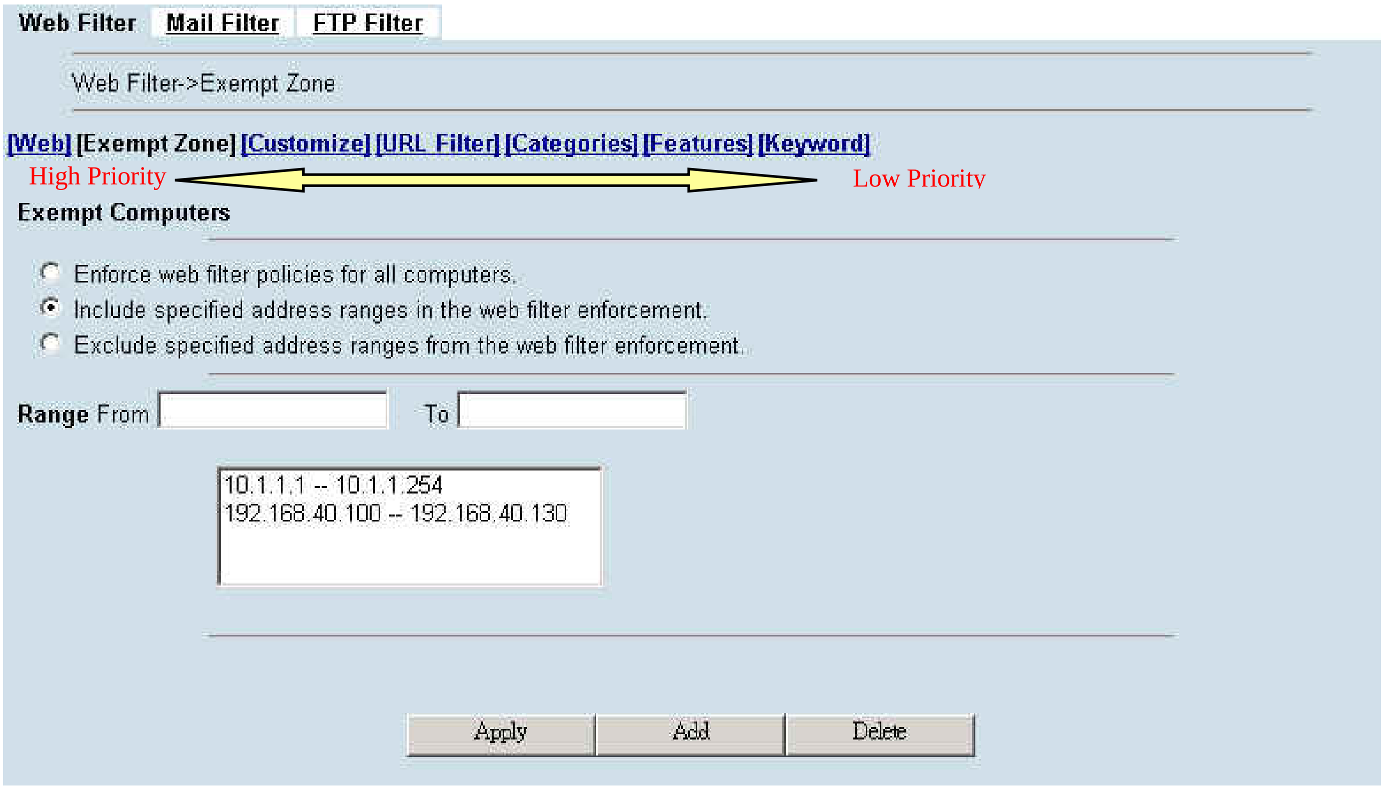
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Enable keyword blocking, limit at __ matches	Check Enable keyword blocking, and then the web pages will be blocked if the keywords below you have added are appeared in the pages. "Limit at 3 matches" means that the webpages will be blocked as long as any of the added keywords appear equal or more than three times.	Enable/Disable Integer	Enabled 3 matches
Keyword	Specify the keyword that you want to block.	test string (Max: 256 entries)	sex violence blood
BUTTON	DESCRIPTION		
Apply	Apply the settings which have been configured.		
Add	Add the Keyword to the list.		
Delete	Delete the Keyword from the list.		

Table 19-7 Web Filter Content Keywords setting page

19.5 Setting priorities

The function priority of web filter is shown as the following Figure 19-3 illustrated. From the left feature (Exempt Zone) to the right feature (Keyword). Their priority is high to low.

Notice: The Restricted features of /Web Filter/Web page is lowest priority, but it is located at the leftest side.



Exempt Computers

○ Enforce web filter policies for all computers.

● Include specified address ranges in the web filter enforcement.

○ Exclude specified address ranges from the web filter enforcement.

Range From ______ To ______

10.1.1.1 -- 10.1.1.254
192.168.40.100 -- 192.168.40.130

Figure 19-3 web filter features priority (from High to Low)

According to the priorities of web filter, we have the guiding principle to setup the web filter now. As we know, there are many choices according to your requirement in the web filter settings. Here we list the setting priorities for your reference. As the following Table 19-8 indicates, the smaller priority sequence would be executed first when running web filter.

Priority sequence	Selected item	Description	Restricted Region
4.	Web Filter > Exempt zone	Select which LAN region will apply the web filter settings. There are three items to choose (enforce all computers, include specified computers, and exclude specified computers)	LAN
5.	Web Filter > Customize	We can use the Customize domain to indicate the Trusted/Forbidden destination. There are two items for your choice. We can specify which URL domain names are trusted, and which ones are forbidden separately. Warning: Customize will not work on the proxy connections.	Internet web server
6.	Web Filter > URL Filter	When an URL contains any keywords listed in the domain name, it will be blocked.	Internet web server
7.	Web Filter > Categories	We can use Database Update in the page of the System Tools > Database Update > Update to update the latest URL database and then the Categories will be updated at the same time. The URL which user request will be blocked if it matches the categories in the URL Database.	Internet web server

8.	Web Filter > Features Web Filter > Keyword	If the web page contains the components included activex/java/javascript/cookie which indicated in "`Web Filter > Web`", or the keywords indicated in "`Web Filter > Keyword`". The forbidden components will be taken off from the web page by web filter.	Web page contents

Table 19-8 web filter features priority

Chapter 20
Content Filtering – Mail Filters

This chapter introduces SMTP proxies and explains how to implement it.

20.1 Demands

1. Sometimes there are malicious scripts like *.vbs that may be attached in the email. If the users accidentally open such files, their computers may be infectious with virus.
2. You may receive some commercial mails which always persecute you and waste your time to deal with.

20.2 Objectives

1. Modify the filename extension of the suspicious email attachments so that email receivers may notice that the file cannot be directly opened by the operating system because of the unrecognized filename extension.
2. Restrict the commercial mails to send or to be received and append "[SPAM]" to email subject if recognized as SPAM email so that email receivers may easily judge what he should do next step while receiving such mails.

20.3 Methods

1. Setup SMTP filters for outgoing emails from PC_1 (in LAN1) towards the mail server (in DMZ1 or in WAN1) to block the suspicious attachments like vbs, exe, etc. extension files.

2. Setup POP3 filters for incoming emails from a mail server (in WAN1 or in DMZ1) to PC_1 (in LAN1) to append a ".bin" to all suspicious attachments like vbs, exe, etc. extension files.

3. Setup IMAP filters for incoming emails from a mail server (in WAN1 or in DMZ1) to PC_1 (in LAN1) to append a ".bin" to all suspicious attachments like vbs, exe, etc. extension files.

4. Setup SMTP filters for outgoing emails from PC_1 (in LAN1) towards the mail server (in DMZ1 or in WAN1) to block the mails by the black list and let the trusted mails passing through and append "[SPAM]" to email subject if recognized as SPAM emails.

5. Setup POP3 filters for incoming emails from a mail server (in WAN1 or in DMZ1) to PC_1 (in LAN1) to block the mails by the black list and let the trusted mails passing through and append "[SPAM]" to email subject if recognized as SPAM email.

6. Setup IMAP filters for incoming emails from a mail server (in WAN1 or in DMZ1) to PC_1 (in LAN1) to block the mails by the black list and let the trusted mails passing through and append "[SPAM]" to email subject if recognized as SPAM email.

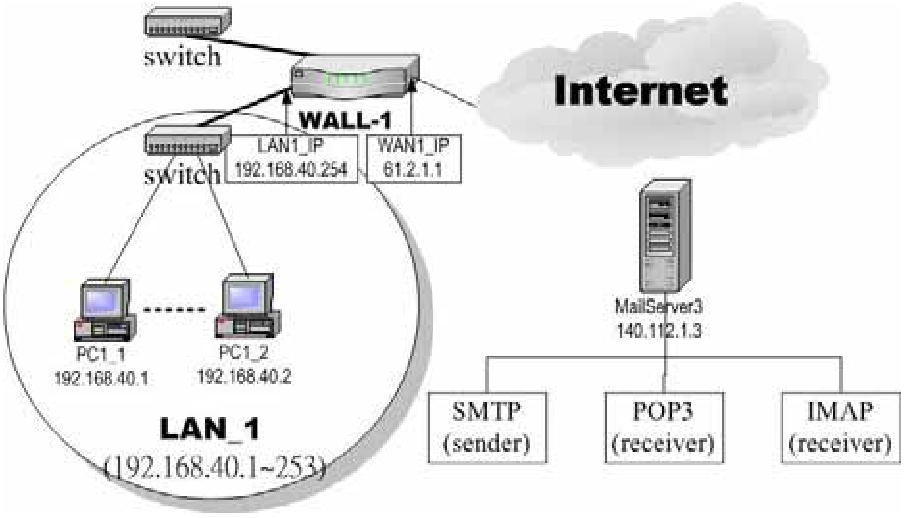
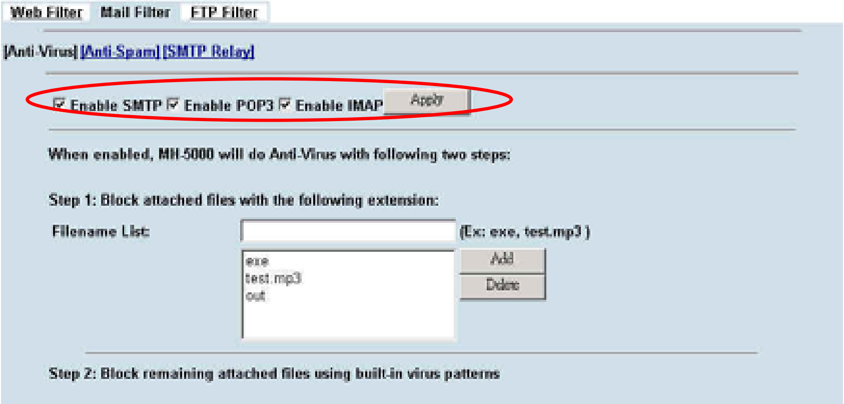
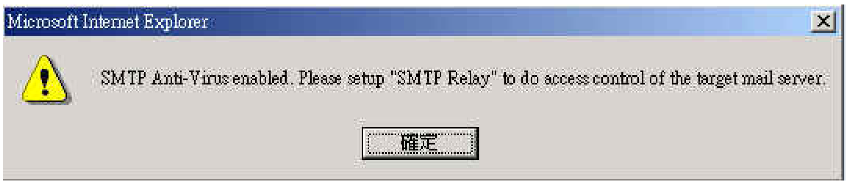
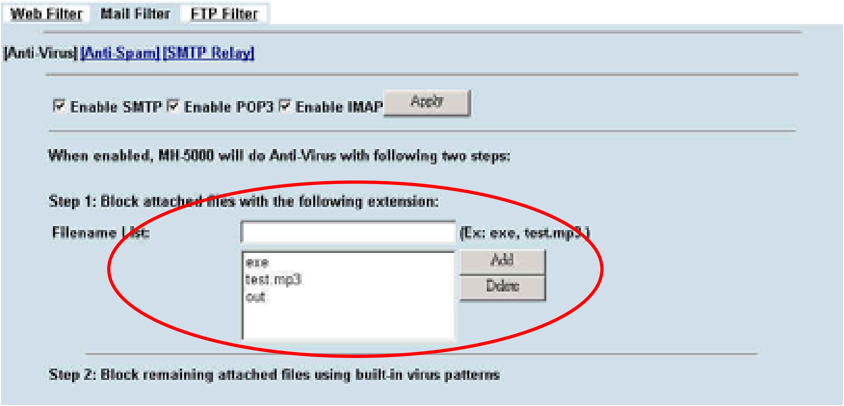


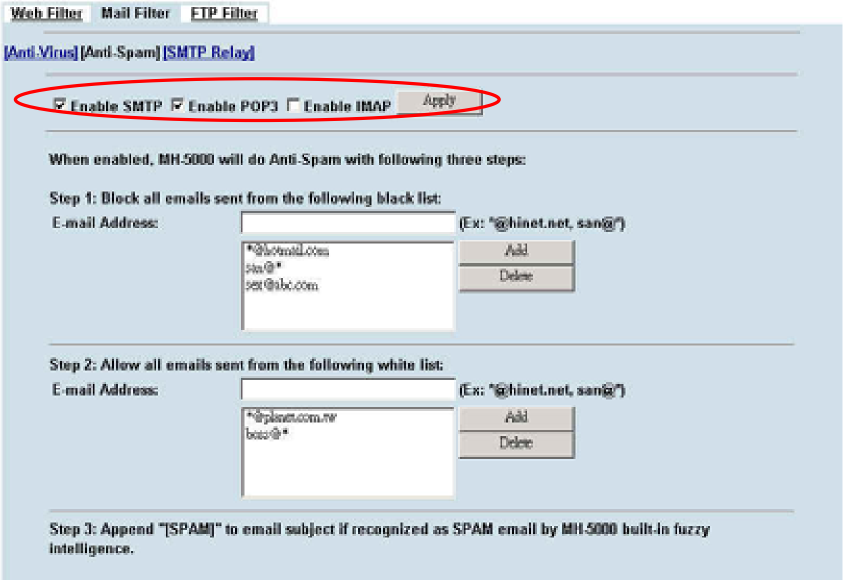
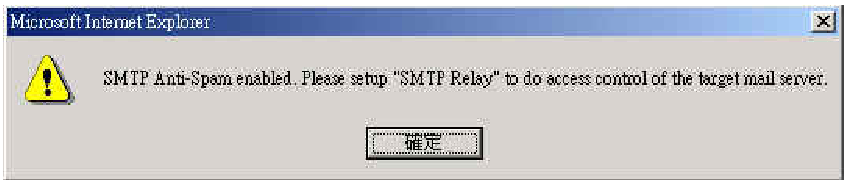
Figure 20-1 Use SMTP / POP3 filter functionality to avoid some sensitive e-mail directly opened

20.4 Steps for Anti-Virus

Step 1 – Enable Anti-Virus Click the `Anti-Virus` hyperlink. Check `Enable SMTP/POP3/IMAP` checkbox, and then click `Apply` button.	**ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Virus**  [Anti-Virus] [Anti-Spam] [SMTP Relay] ☑ Enable SMTP ☑ Enable POP3 ☑ Enable IMAP Apply When enabled, MH-5000 will do Anti-Virus with following two steps: Step 1: Block attached files with the following extension: Filename List: (Ex: exe, test.mp3) exe test.mp3 out Add Delete Step 2: Block remaining attached files using built-in virus patterns
Step 2 – Message alert After applying Anti-Virus, there will be a message "`SMTP Anti-Virus enabled. Please setup "SMTP Relay" to do access control of the target mail server.`" to notify you to setup SMTP Relay.	**ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Virus**  Microsoft Internet Explorer SMTP Anti-Virus enabled. Please setup "SMTP Relay" to do access control of the target mail server. 確定

Step 3 – Block attached files When enabled `SMTP/POP3/IMAP` filter function, MH-5001 will do Anti-Virus with two steps. Step 1, add the extensions which you would like to block. (Max: 32 items) You can add/delete the items by clicking `Add/Delete` button. Step 2, block remaining attached files using built-in virus patterns. Note that the filename to block cannot contain the marks such as " /, \, *, ?, ", <, >, | ".	 Web Filter Mail Filter FTP Filter [Anti-Virus] [Anti-Spam] [SMTP Relay] ☑ Enable SMTP ☑ Enable POP3 ☑ Enable IMAP Apply When enabled, MH-5000 will do Anti-Virus with following two steps: Step 1: Block attached files with the following extension: Filename List: (Ex: exe, test.mp3) exe test.mp3 out Add Delete Step 2: Block remaining attached files using built-in virus patterns

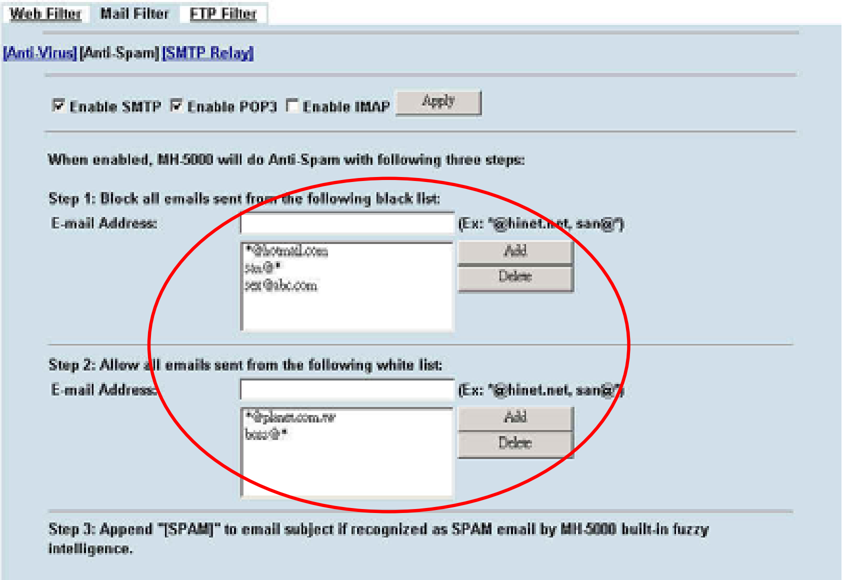
20.5 Steps for Anti-Spam

Step 1 – Enable Anti-Spam Click the `Anti-Spam` hyperlink. Check `Enable SMTP/POP3/IMAP` checkbox, and then click `Apply` button.	**ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Spam**  Web Filter Mail Filter FTP Filter [Anti-Virus] [Anti-Spam] [SMTP Relay] ☑ Enable SMTP ☑ Enable POP3 □ Enable IMAP Apply When enabled, MH-5000 will do Anti-Spam with following three steps: Step 1: Block all emails sent from the following black list: E-mail Address: (Ex: *@hinet.net, san@*) *@hotmail.com sta@* sex@abc.com Add Delete Step 2: Allow all emails sent from the following white list: E-mail Address: (Ex: *@hinet.net, san@*) *@planet.com.tw boss@* Add Delete Step 3: Append "[SPAM]" to email subject if recognized as SPAM email by MH-5000 built-in fuzzy intelligence.
Step 2 – Message alert After applying Anti-Spam, there will be a message "`SMTP Anti-Spam enabled. Please setup "SMTP Relay" to do access control of the target mail server.`" to notify you to setup SMTP Relay.	**ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Spam**  Microsoft Internet Explorer SMTP Anti-Spam enabled. Please setup "SMTP Relay" to do access control of the target mail server.

Step 3 – Add the black list

When enabled SMTP/POP3/IMAP filter function, MH-5001 will do Anti-Spam with three steps. Step 1, add the emails which you would like to block. You can add/delete the block list by clicking Add/Delete button. (Max: 256 items) Step 2, add the e-mails which you always trust. You also can add/delete the white list by clicking Add/Delete button. (Max: 256 items) Step 3, Append "[Spam]" to email subject if recognized as SPAM email by MH-5001 built-in fuzzy intelligence.

Note that you cannot duplicate the email addresses in the black list or white list. For example, if you have already added the email "sex@abc.com" in the black list, you can repeat it neither in the black list nor in the white list.



☑ Enable SMTP ☑ Enable POP3 □ Enable IMAP

When enabled, MH-5000 will do Anti-Spam with following three steps:

Step 1: Block all emails sent from the following black list:

E-mail Address: (Ex: "@hinet.net, san@")

*@hotmail.com
sta@*
sex@abc.com

Step 2: Allow all emails sent from the following white list:

E-mail Address: (Ex: "@hinet.net, san@")

*@planet.com.tw
boss@*

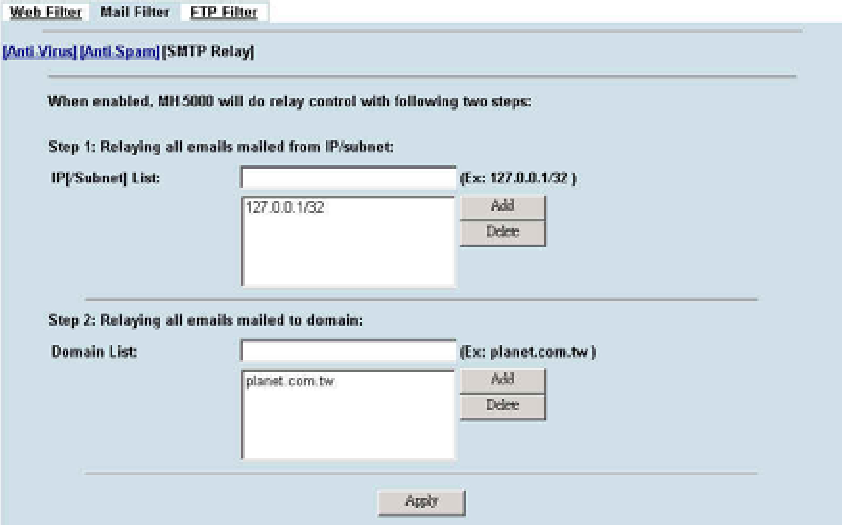
Step 3: Append "[SPAM]" to email subject if recognized as SPAM email by MH-5000 built-in fuzzy intelligence.

20.6 Steps for SMTP Relay

Step 1 – SMTP Relay

When enabled SMTP Relay function, MH-5001 will do relay with the following two steps. Step 1, Relaying all emails mailed from IP/subnet which you are adding to the IP[/Subnet] List. You can add/delete the list by clicking Add/Delete button. Step 2, Relaying all emails mailed to domain which you are adding to the Domain List. You also can add/delete the list by clicking Add/Delete button.

ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Spam



When enabled, MH-5000 will do relay control with following two steps:

Step 1: Relaying all emails mailed from IP/subnet:

IP[/Subnet] List: (Ex: 127.0.0.1/32)

127.0.0.1/32

Step 2: Relaying all emails mailed to domain:

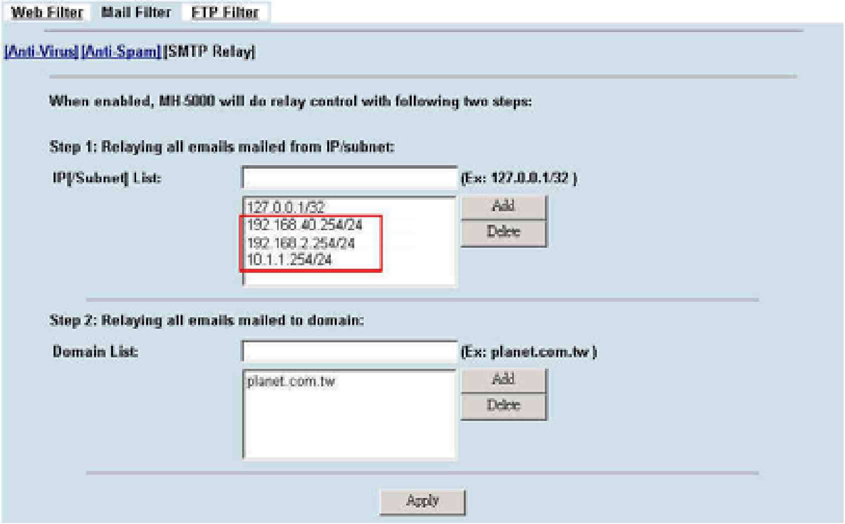
Domain List: (Ex: planet.com.tw)

planet.com.tw

Step 2 – Apply SMTP Relay

When you apply the SMTP Relay, the IP addresses of the LAN and DMZ interfaces will be shown on the `IP/[Subnet] List` automatically.

ADVANCED SETTINGS > Content Filters > Mail Filters > Anti-Spam



When enabled, MH-5000 will do relay control with following two steps:

Step 1: Relaying all emails mailed from IP/subnet:

IP[/Subnet] List: (Ex: 127.0.0.1/32)

127.0.0.1/32
192.168.40.254/24
192.168.2.254/24
10.1.1.254/24

Step 2: Relaying all emails mailed to domain:

Domain List: (Ex: planet.com.tw)

planet.com.tw

Chapter 21
Content Filtering – FTP Filtering

This chapter introduces FTP proxies and explains how to implement it.

21.1 Demands

1. Some users in LAN1 use FTP to download big MP3 files and cause waste of bandwidth.

21.2 Objectives

1. Forbid PC1_1 from downloading MP3 files with FTP.

21.3 Methods

1. Setup the filename extension of the forbidden types of file that are not allowed to be transmitted using standard FTP port.

2. Let PC1_1 download a MP3 file from the FTPServer3 to see if the session is blocked.

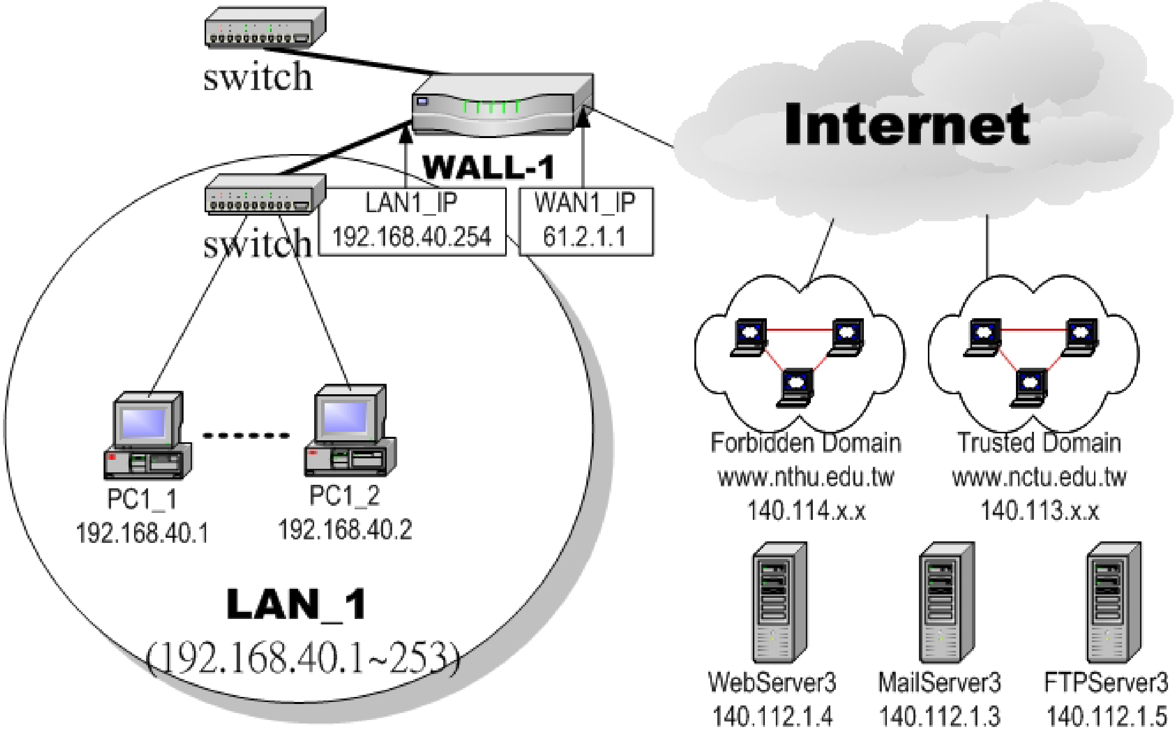


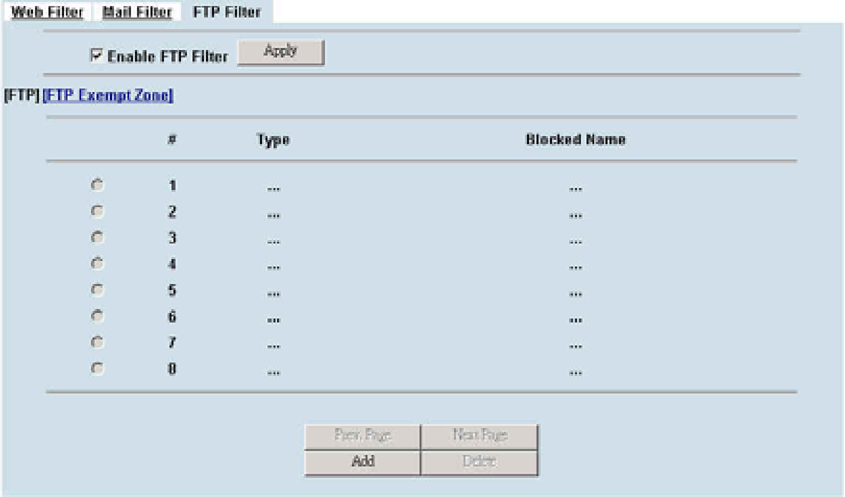
Figure 21-1 Use FTP filter functionality to avoid user download forbidden file type

21.4 Steps

Step 1. Enable FTP Filter

Check the `Enable FTP Filter` checkbox and click the nearby `Apply` button to enable this feature. Click the `Add` button to add a new FTP filter.

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP



☑ Enable FTP Filter

[FTP] [FTP Exempt Zone]

	#	Type	Blocked Name
○	1	...	...
○	2	...	...
○	3	...	...
○	4	...	...
○	5	...	...
○	6	...	...
○	7	...	...
○	8	...	...

FIELD	DESCRIPTION	EXAMPLE
Enable FTP Filter	Enable FTP Filter feature of MH-5001	Enabled

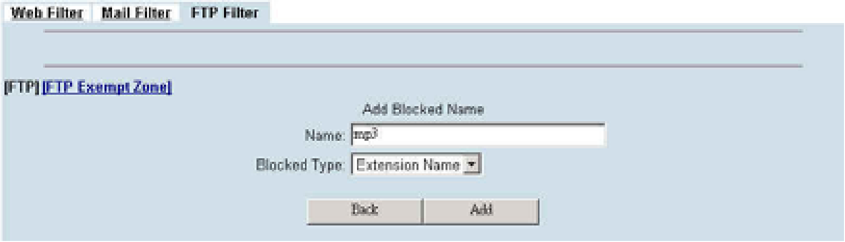
Table 21-1 FTP Filter FTP setting page

Step 2. Add an FTP Filter

Enter `mp3` in the `Name` field and select `Extension Name` in the `Blocked Type` field. Click the `Add` button to apply the change. Now users in LANs can never download any mp3 files.

Note that the filename to block cannot contain the marks such as " /, \, *, ?, ", <, >, | ".

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP > Add



[FTP] [FTP Exempt Zone]

Add Blocked Name

Name: mp3

Blocked Type: Extension Name

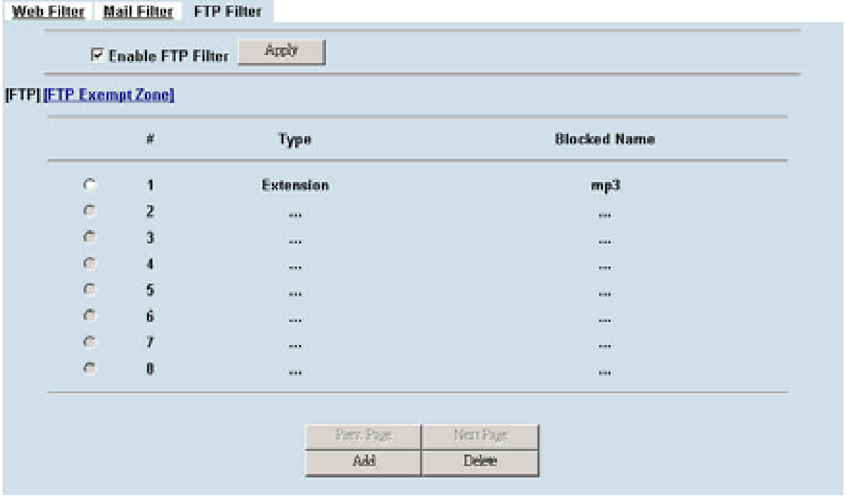
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Name	Fill in the file extension or exact filename.	text string (Max: 40 entries)	mp3
Blocked Type	➢ Extension Name When the extension filename of download file is matching, the action is blocked download from FTP server. ➢ Full Name When the exact filename of download file is matching, the action is blocked download from FTP server.	Extension Name Full name	Extension Name

Table 21-2 FTP Filter FTP adding filter entry

Step 3. View the result

We can see the specified record in this page.

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP



☑ Enable FTP Filter

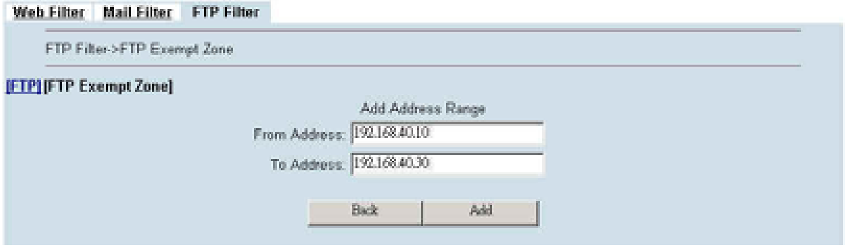
[FTP] [FTP Exempt Zone]

	#	Type	Blocked Name
○	1	Extension	mp3
○	2	...	...
○	3	...	...
○	4	...	...
○	5	...	...
○	6	...	...
○	7	...	...
○	8	...	...

Step 4. Add an Exempt Zone

Add a new Exempt Zone record. It's IP address range is between 192.168.40.10 to 192.168.40.30.

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP Exempt Zone > Add



FTP Filter->FTP Exempt Zone

[FTP] [FTP Exempt Zone]

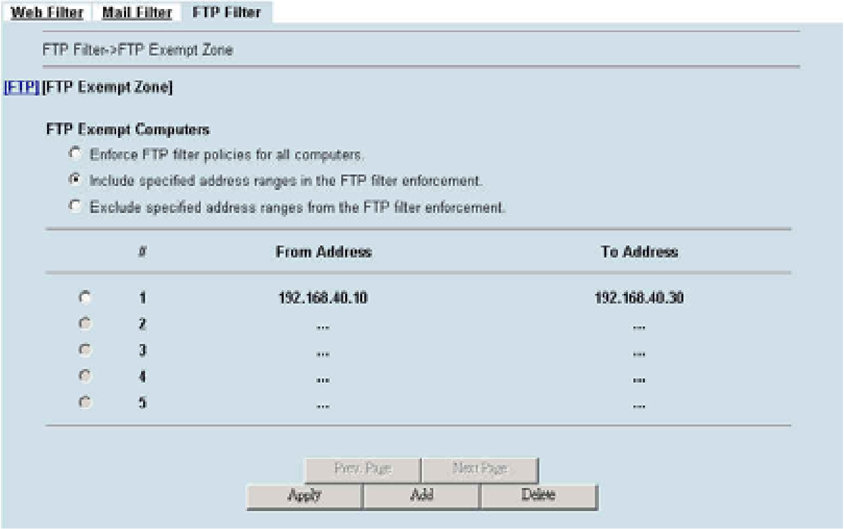
Add Address Range

From Address: 192.168.40.10

To Address: 192.168.40.30

FIELD	DESCRIPTION	Range/Format	EXAMPLE
From Address	Exempt zone record IP address from	Max: 20 entries	192.168.40.10
To Address	Exempt zone record IP address to	Max: 20 entries	192.168.40.30

Table 21-3 FTP Filter add an exempt zone entry

Step 5. Show the Exempt Zones Here we can discover that new added Exempt Zone record is appeared.	**ADVANCED SETTINGS > Content Filters > FTP Filter > FTP Exempt Zone**  FTP Filter->FTP Exempt Zone [FTP] [FTP Exempt Zone] FTP Exempt Computers ○ Enforce FTP filter policies for all computers. ● Include specified address ranges in the FTP filter enforcement. ○ Exclude specified address ranges from the FTP filter enforcement. # / From Address / To Address ○ 1 192.168.40.10 192.168.40.30 ○ 2 ... ... ○ 3 ... ... ○ 4 ... ... ○ 5 ... ...

Chapter 22
Content Filters – L7 Firewall

This chapter introduces Layer 7 Application Layer Firewall and explains how to implement it.

22.1 Demands

Instant messaging (IM) and peer-to-peer (P2P) are the fastest growing communications medium of all time. The proliferation of IM/P2P has created a network security threat and consumed significant amount of bandwidth. The key factor in the popularity of these protocols is their ability to work across almost all practical firewall deployments. However, it is exactly this same ability that has created the security threat, as these protocols are able to transfer information and files across the security infrastructure relatively unchecked. Therefore, your company needs a tool to manage those IM/P2P applications.

22.2 Objectives

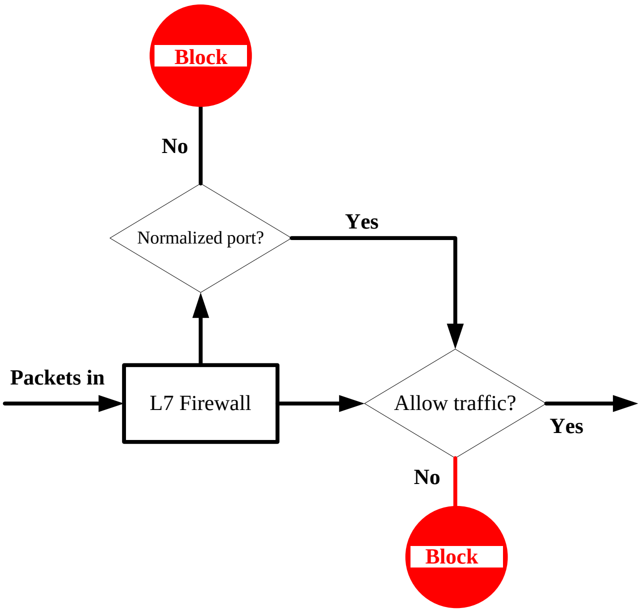


Figure 22-1 IM Management design principle

As Figure 22-1 illustrates, L7 Firewall is designed to manage IM/P2P/Remote Access applications. Whatever the TCP protocol or a proxy server (such as HTTP/SOCKS) may be used by a certain application to attempt to deceive administrator, it will be recognized by MH-5001.

22.3 Methods

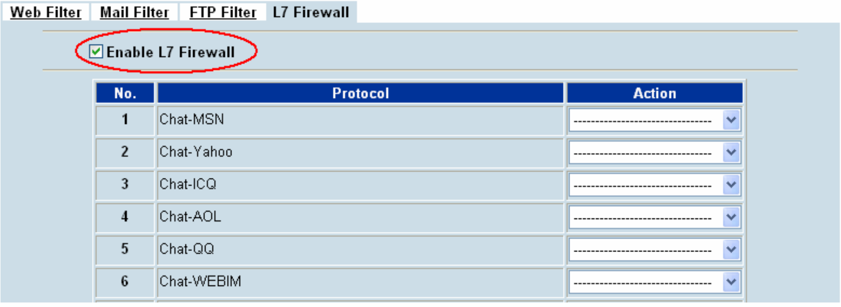
The L7 firewall can be enabled by clicking the “`Enable L7 Firewall`” checkbox. When enabled, any IM/P2P sessions which have been set to block will be stopped. For example, if you choose to block MSN, any MSN requests no matter it runs over HTTP/ SOCKS4/ SOCKS5 with random ports or the default well-known port 1863, it will be blocked. For the traffic to be allowed, select “Allow” in the Action field. For those applications restricted to go out via the well-known port, select the “Allow only at port ( )” in the Action field. All traffic will be normalized to go out via the well-known port. If you will not manage a certain applications, select “--------------“ to tell MH-5001 to skip it. That will make MH-5001 keep its good performance.

22.4 Steps

Step 6. Enable L7 Firewall

Check `Enable L7 Firewall` checkbox.

ADVANCED SETTINGS > L7 Firewall > Status



☑ Enable L7 Firewall

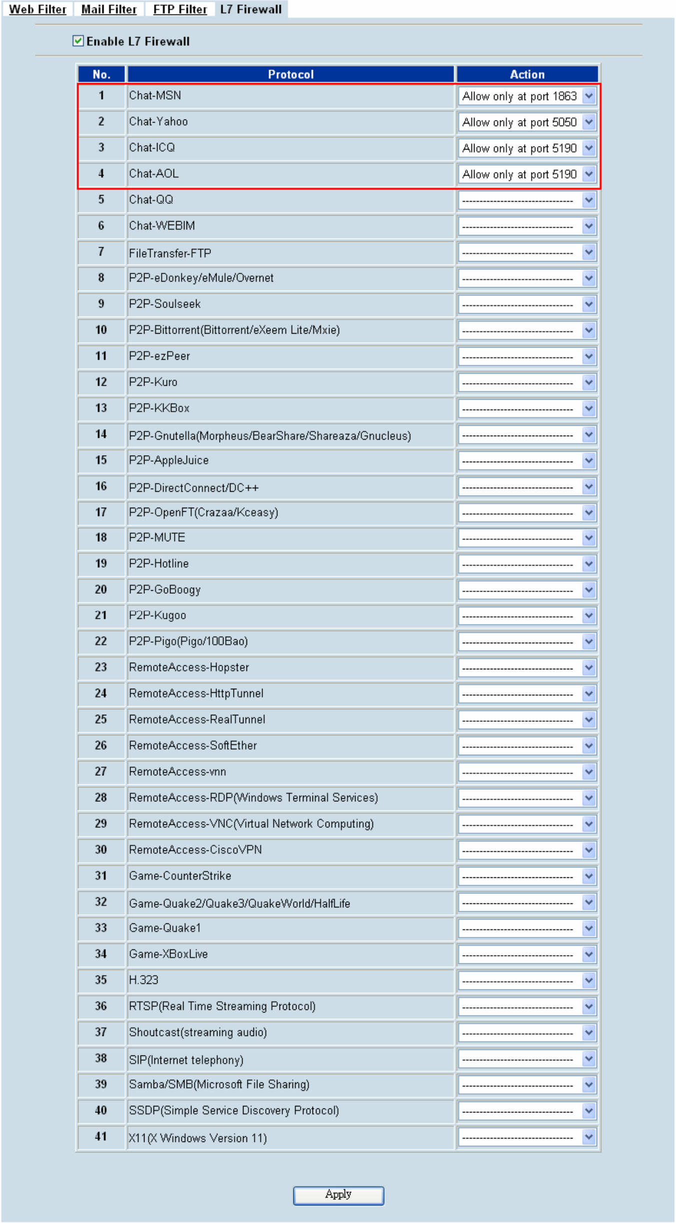
No.	Protocol	Action
1	Chat-MSN	--------------------------------
2	Chat-Yahoo	--------------------------------
3	Chat-ICQ	--------------------------------
4	Chat-AOL	--------------------------------
5	Chat-QQ	--------------------------------
6	Chat-WEBIM	--------------------------------

Step 7. Manage the L7 Firewall

Select `Allow/Block/Allow` only at `port ( )` in the `Action` field for the applications. If you will not manage a certain application, please select or leave it as "`--------------`". That will make MH-5001 keep its good performance. Click `Apply` button to apply the settings.

Note, the MH-5001 screen displays the manageable applications according to the updatable database frequently.

ADVANCED SETTINGS > L7 Firewall > Status



☑ Enable L7 Firewall

No.	Protocol	Action
1	Chat-MSN	Allow only at port 1863
2	Chat-Yahoo	Allow only at port 5050
3	Chat-ICQ	Allow only at port 5190
4	Chat-AOL	Allow only at port 5190
5	Chat-QQ	-------------------------------
6	Chat-WEBIM	-------------------------------
7	FileTransfer-FTP	-------------------------------
8	P2P-eDonkey/eMule/Overnet	-------------------------------
9	P2P-Soulseek	-------------------------------
10	P2P-Bittorrent(Bittorrent/eXeem Lite/Mxie)	-------------------------------
11	P2P-ezPeer	-------------------------------
12	P2P-Kuro	-------------------------------
13	P2P-KKBox	-------------------------------
14	P2P-Gnutella(Morpheus/BearShare/Shareaza/Gnucleus)	-------------------------------
15	P2P-AppleJuice	-------------------------------
16	P2P-DirectConnect/DC++	-------------------------------
17	P2P-OpenFT(Crazaa/Kceasy)	-------------------------------
18	P2P-MUTE	-------------------------------
19	P2P-Hotline	-------------------------------
20	P2P-GoBoogy	-------------------------------
21	P2P-Kugoo	-------------------------------
22	P2P-Pigo(Pigo/100Bao)	-------------------------------
23	RemoteAccess-Hopster	-------------------------------
24	RemoteAccess-HttpTunnel	-------------------------------
25	RemoteAccess-RealTunnel	-------------------------------
26	RemoteAccess-SoftEther	-------------------------------
27	RemoteAccess-vnn	-------------------------------
28	RemoteAccess-RDP(Windows Terminal Services)	-------------------------------
29	RemoteAccess-VNC(Virtual Network Computing)	-------------------------------
30	RemoteAccess-CiscoVPN	-------------------------------
31	Game-CounterStrike	-------------------------------
32	Game-Quake2/Quake3/QuakeWorld/HalfLife	-------------------------------
33	Game-Quake1	-------------------------------
34	Game-XBoxLive	-------------------------------
35	H.323	-------------------------------
36	RTSP(Real Time Streaming Protocol)	-------------------------------
37	Shoutcast(streaming audio)	-------------------------------
38	SIP(Internet telephony)	-------------------------------
39	Samba/SMB(Microsoft File Sharing)	-------------------------------
40	SSDP(Simple Service Discovery Protocol)	-------------------------------
41	X11(X Windows Version 11)	-------------------------------

FIELD	DESCRIPTION	Range / Format	EXAMPLE
Enable L7 Firewall	Activate or deactivate the L7 Firewall feature.	Enable/disable	Enabled
No.	The sequence number of the applications (protocols).	numeric	1
Protocol	The applications (protocols) (such as IM, P2P, Game, Remote Access, etc.) which MH-5001 can manage currently.	IM/P2P applications	Chat-MSN Chat-Yahoo Chat-ICQ Chat-AOL
Action	The action for MH-5001 to do when user implements the chosen applications. If you select "---------------", it means that MH-5001 will skip the chosen protocol.	-------------------- Allow Block Allow only at port ( )	Allow only at port 1863 Allow only at port 5050 Allow only at port 5190 Allow only at port 5190

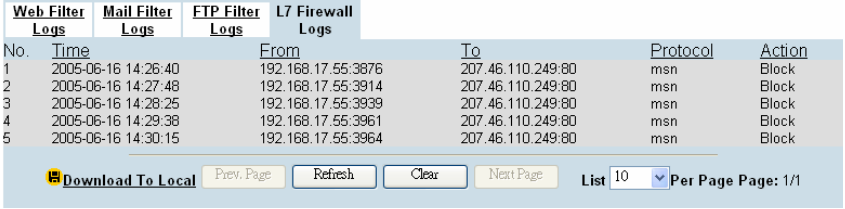
Table 22-1 The IM Users

22.4.1 View L7 Firewall Logs

Step 8. View L7 Firewall logs

View L7 Firewall Logs shown as right diagram.

ADVANCED SETTINGS > Device Status > L7 Firewall Logs > L7 Firewall Logs



No.	Time	From	To	Protocol	Action
1	2005-06-16 14:26:40	192.168.17.55:3876	207.46.110.249:80	msn	Block
2	2005-06-16 14:27:48	192.168.17.55:3914	207.46.110.249:80	msn	Block
3	2005-06-16 14:28:25	192.168.17.55:3939	207.46.110.249:80	msn	Block
4	2005-06-16 14:29:38	192.168.17.55:3961	207.46.110.249:80	msn	Block
5	2005-06-16 14:30:15	192.168.17.55:3964	207.46.110.249:80	msn	Block

Chapter 23
Intrusion Prevention Systems

This chapter introduces Intrusion Prevention System (IPS) and explains how to implement it.

23.1 Demands

Besides firewall, you still need Intrusion Prevention System to protect your networks. Crackers hack into your system through Firewall-allowed channels with sophisticated skills. Most often, they attack specific application servers such as SNMP, Web, and FTP services in your DMZ.

23.2 Objectives

1. Detect any attacks towards your DMZ servers.

2. Instantly notify your network administrators what attacks have been detected.

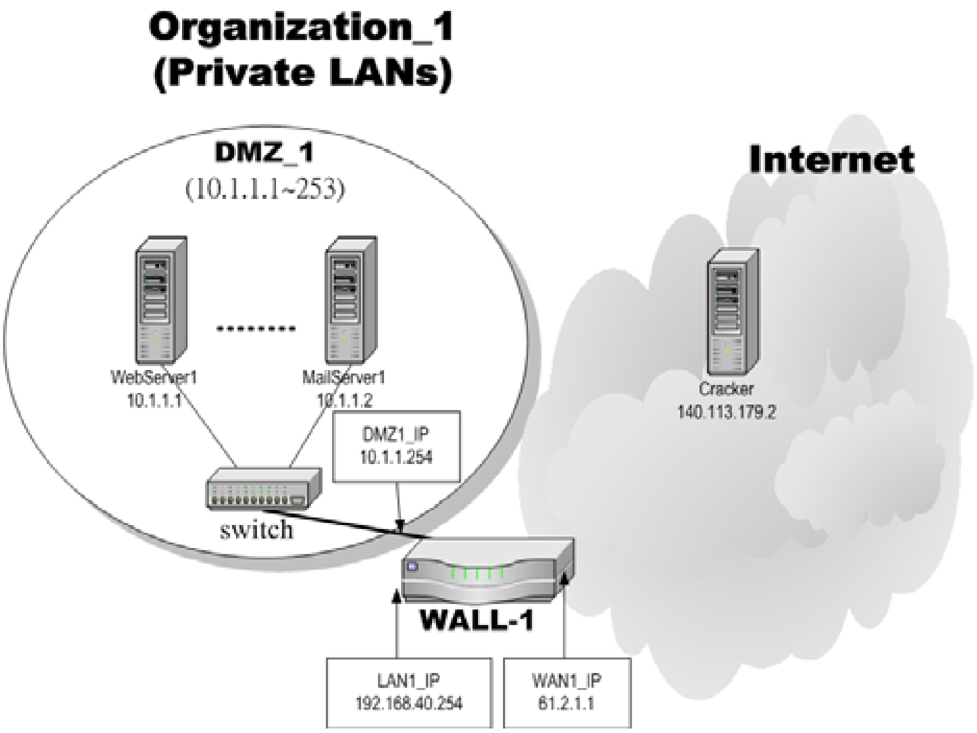


Figure 23-1 Some crackers in the Internet would try to hack your company

23.3 Methods

1. Specify where to put Web server and let the IPS on the MH-5001 prevent the network from the attacks.
2. Setup logs to send mails to the specified email address during the defined time. You can set daily/weekly to receive mails and periodically monitor the IPS logs.

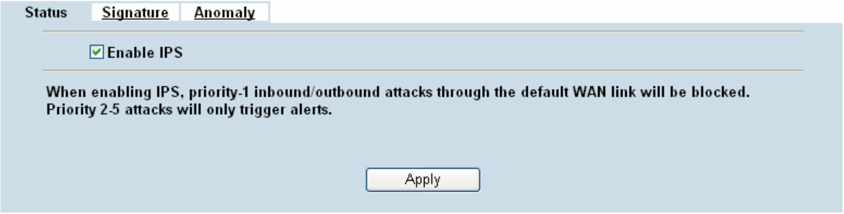
The feature of the IPS can only be available while MH-5001 connects to the Internet via Default WAN Link.

23.4 Steps

Step 1 – Enable IPS

Check the `Enable IPS` checkbox, and then click the `Apply` button. When IPS enabled, priority-1 inbound/outbound attacks through the default WAN link will be blocked. Priority 2-5 attacks will only trigger alerts.

ADVANCED SETTINGS > IPS > IPS Status



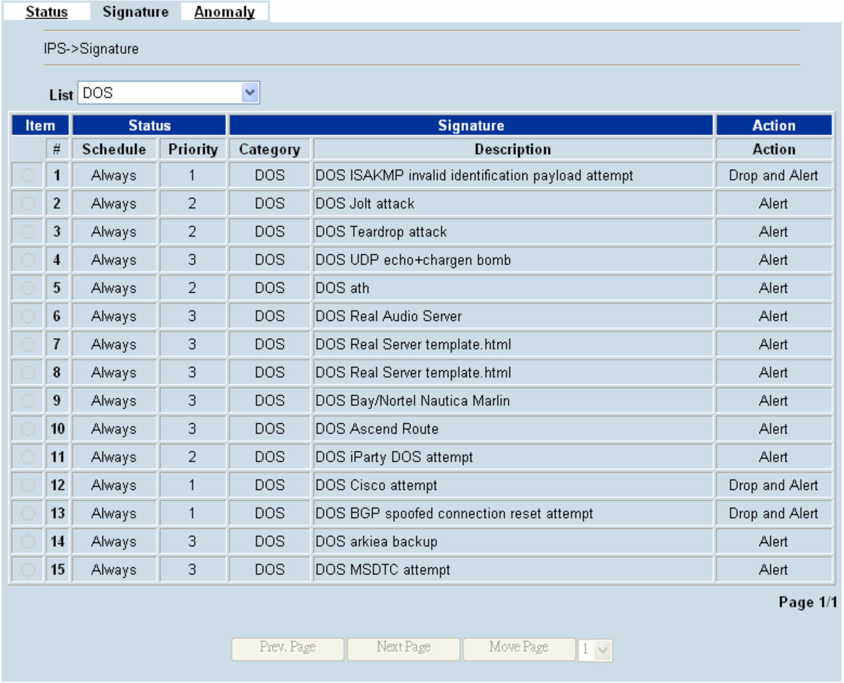
☑ Enable IPS

When enabling IPS, priority-1 inbound/outbound attacks through the default WAN link will be blocked. Priority 2-5 attacks will only trigger alerts.

Step 3 – Consult Signature-based IPS

You can consult signature-based attack shown as right diagram. The signature-based IPS can be sorted by groups. Select `DOS` to list all DOS category attacks. See Table 23-1 for the details.

ADVANCED SETTINGS > IPS > Signature



IPS->Signature

List DOS

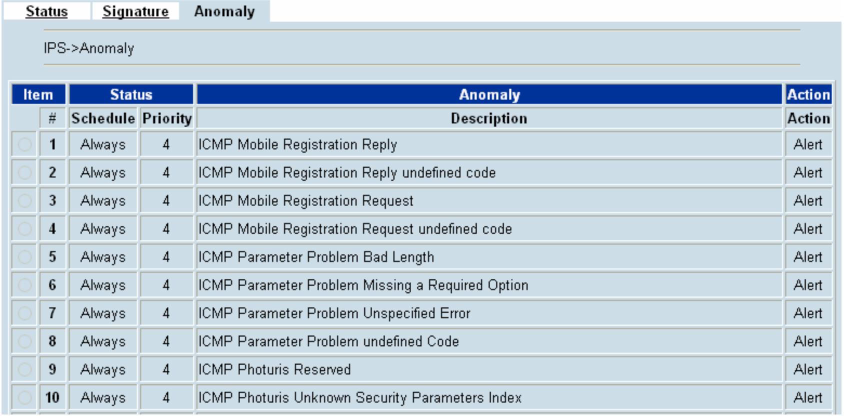
Item		Status		Signature		Action
	#	Schedule	Priority	Category	Description	Action
○	1	Always	1	DOS	DOS ISAKMP invalid identification payload attempt	Drop and Alert
○	2	Always	2	DOS	DOS Jolt attack	Alert
○	3	Always	2	DOS	DOS Teardrop attack	Alert
○	4	Always	3	DOS	DOS UDP echo+chargen bomb	Alert
○	5	Always	2	DOS	DOS ath	Alert
○	6	Always	3	DOS	DOS Real Audio Server	Alert
○	7	Always	3	DOS	DOS Real Server template.html	Alert
○	8	Always	3	DOS	DOS Real Server template.html	Alert
○	9	Always	3	DOS	DOS Bay/Nortel Nautica Marlin	Alert
○	10	Always	3	DOS	DOS Ascend Route	Alert
○	11	Always	2	DOS	DOS iParty DOS attempt	Alert
○	12	Always	1	DOS	DOS Cisco attempt	Drop and Alert
○	13	Always	1	DOS	DOS BGP spoofed connection reset attempt	Drop and Alert
○	14	Always	3	DOS	DOS arkiea backup	Alert
○	15	Always	3	DOS	DOS MSDTC attempt	Alert

Page 1/1

Step 4 - Consult Anomaly-based IPS

You can consult anomaly-based attacks shown as right diagram. See Table 23-1 for the details.

ADVANCED SETTINGS > IPS > IPS Status



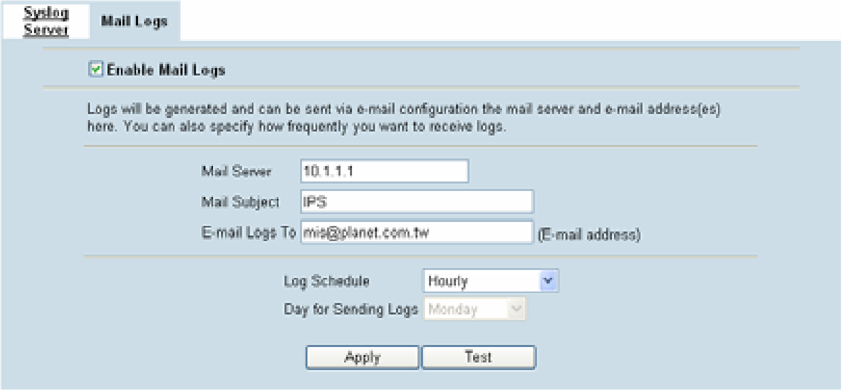
IPS->Anomaly

Item		Status		Anomaly	Action
	#	Schedule	Priority	Description	Action
○	1	Always	4	ICMP Mobile Registration Reply	Alert
○	2	Always	4	ICMP Mobile Registration Reply undefined code	Alert
○	3	Always	4	ICMP Mobile Registration Request	Alert
○	4	Always	4	ICMP Mobile Registration Request undefined code	Alert
○	5	Always	4	ICMP Parameter Problem Bad Length	Alert
○	6	Always	4	ICMP Parameter Problem Missing a Required Option	Alert
○	7	Always	4	ICMP Parameter Problem Unspecified Error	Alert
○	8	Always	4	ICMP Parameter Problem undefined Code	Alert
○	9	Always	4	ICMP Photuris Reserved	Alert
○	10	Always	4	ICMP Photuris Unknown Security Parameters Index	Alert

Step 2 – Setup Logs

Enter the `Mail Server IP Address`, `Mail Subject`, and the `email address` that you want to receive from. Select the `Log Schedule` of emailing the logs to your email server.

DEVICE STATUS > Log Config > Mail Logs



☑ Enable Mail Logs

Logs will be generated and can be sent via e-mail configuration the mail server and e-mail address(es) here. You can also specify how frequently you want to receive logs.

Mail Server: 10.1.1.1

Mail Subject: IPS

E-mail Logs To: mis@planet.com.tw (E-mail address)

Log Schedule: Hourly

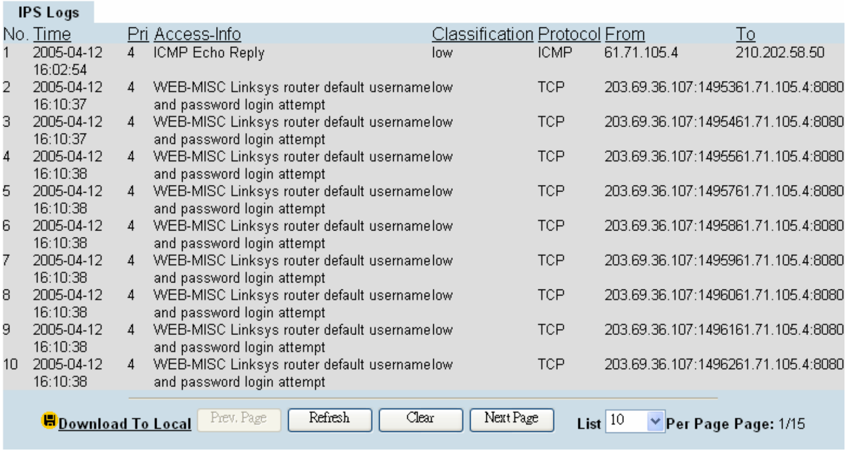
Day for Sending Logs: Monday

Step 3 – View logs

Attacks towards the WAN port from the public Internet will be logs to tell the details.

Notice, the IPS can only detect WAN interfaces currently.

DEVICE STATUS > IPS Logs



No.	Time	Pri	Access-Info	Classification	Protocol	From	To
1	2005-04-12 16:02:54	4	ICMP Echo Reply	low	ICMP	61.71.105.4	210.202.58.50
2	2005-04-12 16:10:37	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14953	61.71.105.4:8080
3	2005-04-12 16:10:37	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14954	61.71.105.4:8080
4	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14955	61.71.105.4:8080
5	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14957	61.71.105.4:8080
6	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14958	61.71.105.4:8080
7	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14959	61.71.105.4:8080
8	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14960	61.71.105.4:8080
9	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14961	61.71.105.4:8080
10	2005-04-12 16:10:38	4	WEB-MISC Linksys router default username and password login attempt	low	TCP	203.69.36.107:14962	61.71.105.4:8080

List 10 Per Page Page: 1/15

Signature-based IPS	**Signature-based IPS** detects intrusions by observing events and identifying patterns which match the signatures of known attacks. An attack signature defines the essential events required to perform the attack, and the order in which they must be performed. Different ID systems represent signatures in different ways. It uses a database table to store the state of the finite state machines representing possible attacks in progress. MH-5001 has a complete attack database to provide you a corporate-wide real-time protection.
Anomaly-based IPS	**Anomaly-based IPS** captures all the headers of the IP packets running towards the network. From this, it filters out all known and legal traffic, including Web traffic to the organization's Web server, mail traffic to and from its mail server, outgoing Web traffic from company employees and DNS traffic to and from its DNS server. The anomaly method detects any traffic that is new or unusual. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks. And, the more targeted the probes and scans, the more likely that the hacker is serious about attacking your network.

Table 23-1 Signature-based IPS vs. Anomaly-based IPS

Chapter 24
Bandwidth Management

This chapter introduces bandwidth management and explains how to implement it.

24.1 Demands

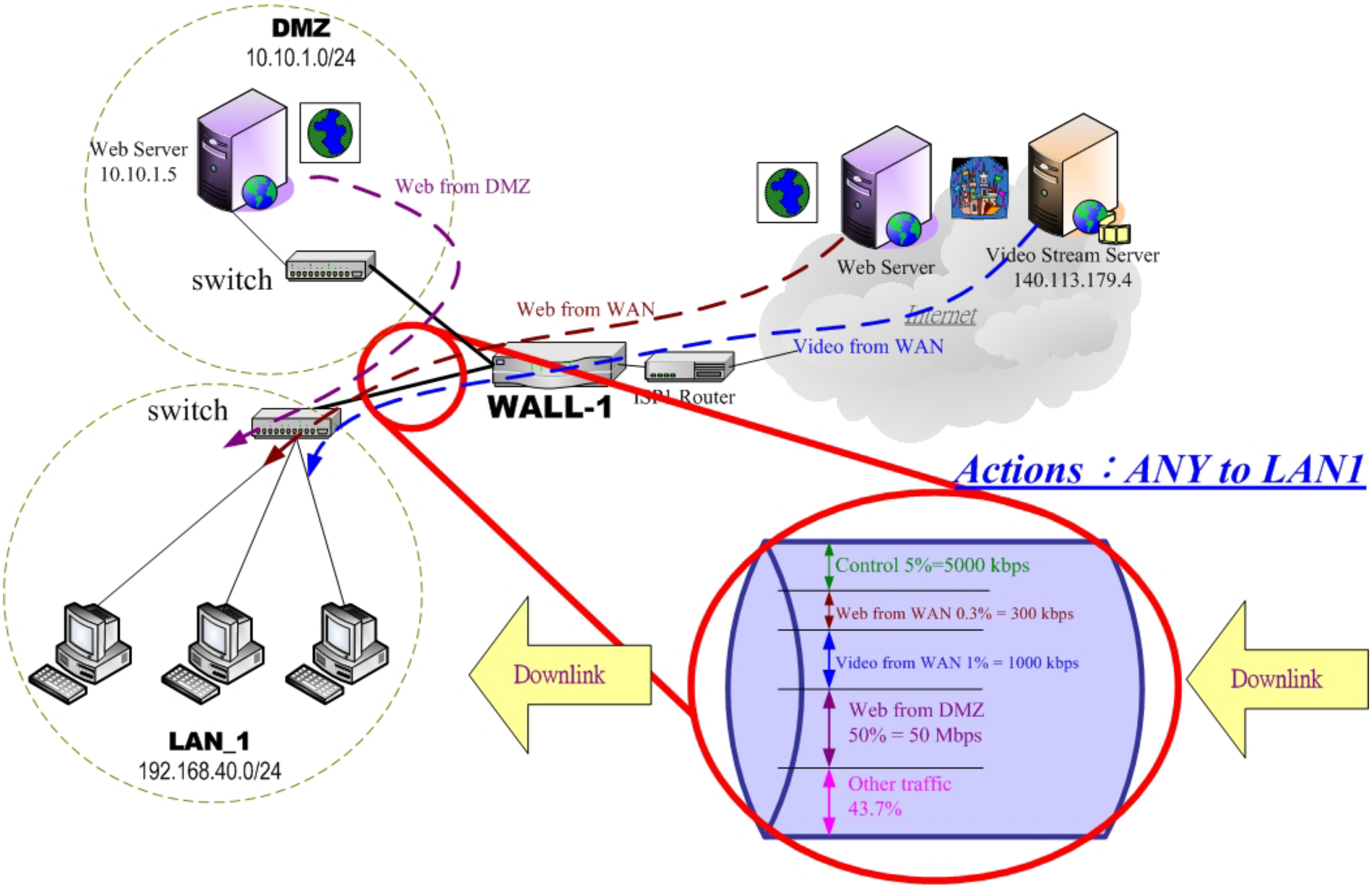


Figure 24-1 Use bandwidth management mechanism to shape the data flow on the downlink direction

1. As the above Figure 24-1 illustrated, we hope LAN_1 users can watch the Video Stream Server smoothly. Besides, we hope LAN_1 users can access the web server located at DMZ region more faster

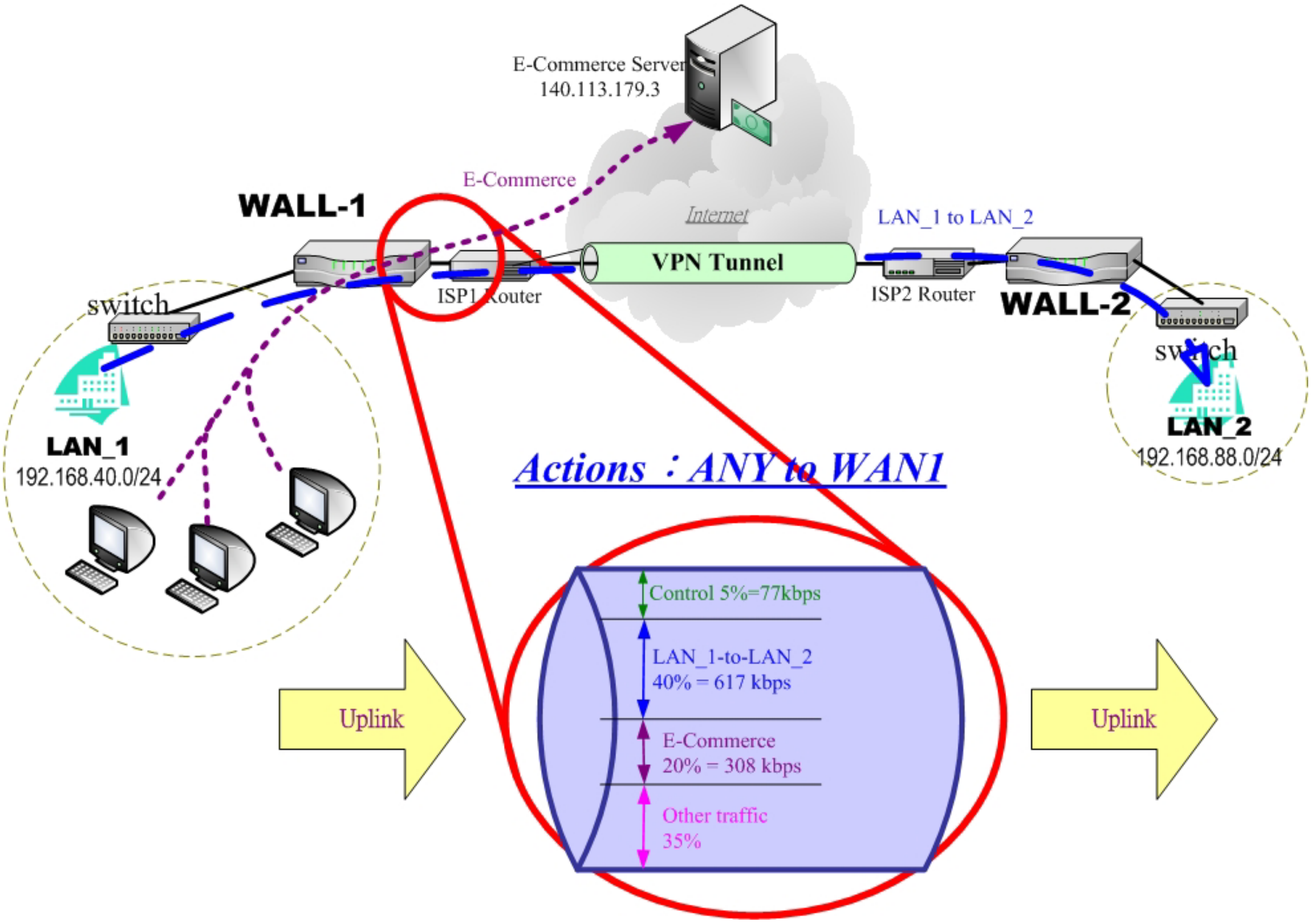


Figure 24-2 Use bandwidth management mechanism to shape the data flow on the uplink direction

2. As the above Figure 24-2 illustrated, LAN_1 PCs are using the E-Commerce service from the E-Commerce Server (140.113.79.3), causing the blocking of the VPN transfer from LAN_1 to LAN_2. So we want to make sure that the VPN tunnel links is reserved at least 600 kbps speed rate. And the free bandwidth will raise the transmission bandwidth of LAN_1 PCs access the E-Commerce service.

24.2 Objectives

1. As the above diagram Figure 24-1 illustrates, LAN_1 PCs are browsing the web pages from the Web Server of Internet. This occupies the bandwidth of PCs who are watching the video provided by the Video Stream Server (140.113.179.4), causing the video to be blocked and to have poor quality. So we hope to guarantee the video quality of the LAN_1 PCs which are accessing Video Stream Server.

   The total bandwidth of ANY to LAN1 direction is 100 Mbps (The bandwidth of LAN1 interface is 100 Mbps). Here we will make sure that PCs of LAN_1 have the smooth stream quality that must have at least 1% of LAN1 total bandwidth (1000 kbps) speed rate.

   Besides, we have another web server located at DMZ region. Because the web server is located at local area, so we can assign larger bandwidth for this direction (web traffic from DMZ → LAN).

   The remaining bandwidths are named Other traffic. They are reserved for other ANY to LAN1 data transmission which don’t list in the above Figure 24-1 diagram.

2. Reserve at least 600kbps for the LAN_1 to LAN_2 transfer. The LAN_1 PCs can share about 20% (308kbps) for using E-Commerce Services. However, when the LAN_1 to LAN_2 traffic less then 40% (617kbps), the E-Commerce service can occupy the free bandwidth from LAN_1-toLAN_2 and the remaining bandwidth from default class.

24.3 Methods

1. As the following table Table 24-1 listed, we partition the inbound bandwidth (total 100Mbps) into three classes, web_from_WAN, video_from_WAN and web_from_DMZ class. The remaining bandwidth is assigned to other services which are not listed here.

Service	Goal	Assigned bandwidth	Borrow bit status
Web from WAN	limited bandwidth (MAX. 300kbps)	0.3% = 300kbps	Disabled
Video from WAN	guaranteed bandwidth (At least 1000kbps)	1% = 1000kbps	Enabled
Web from DMZ	guaranteed bandwidth (At least 50Mbps)	50% = 50Mbps	Enabled

Table 24-1 Bandwidth management action assignment from ANY to LAN1

2. As the following Table 24-2 listed. Partition the outbound bandwidth (total 1.544Mbps) into two classes, the LAN_1-to-LAN_2 (40% 617 kbps) and the E-commerce (20% 308kbps) classes. Besides, set the E-Commerce to be able to borrow from other bandwidth if any bandwidth is available.

Service	Goal	Assigned bandwidth	Borrow bit status
LAN_1 to LAN_2	limited bandwidth (MAX. 617kbps)	40% = 617kbps	Disabled
E-Commerce	guaranteed bandwidth (At least 308kbps)	20% = 308kbps	Enabled

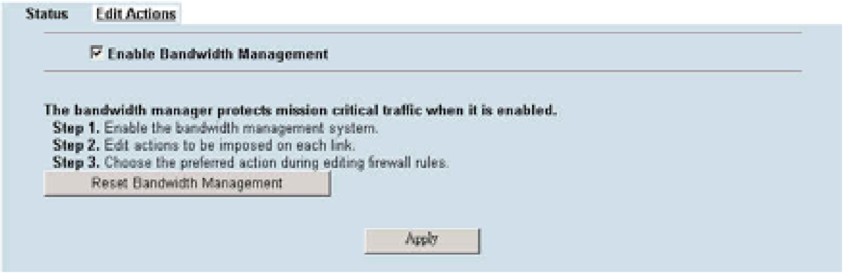
Table 24-2 Bandwidth management action assignment from ANY to WAN1

24.4 Steps

Step 1. Enable Bandwidth Management

Check the `Enable Bandwidth Management` checkbox, and click the `Apply` button.

ADVANCED SETTINGS > Bandwidth Mgt. > Status



☑ Enable Bandwidth Management

The bandwidth manager protects mission critical traffic when it is enabled.

Step 1. Enable the bandwidth management system.
Step 2. Edit actions to be imposed on each link.
Step 3. Choose the preferred action during editing firewall rules.

FIELD	DESCRIPTION	Range/Format	EXAMPLE
Enable Bandwidth Management	Enable Bandwidth Management feature of MH-5001	Enable/Disable	Enabled

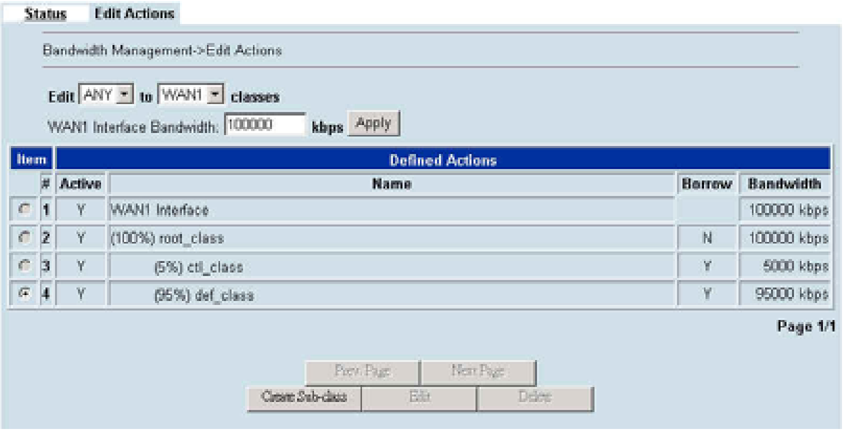
BUTTON	DESCRIPTION
Reset Bandwidth Management	Reset all the bandwidth management rules to default status.
Apply	Apply the settings which have been configured.
Reset	Clean the filled data and restore the original one.

Table 24-3 Setup status page of Bandwidth Management

Step 2. Setup the Actions Link

Select ANY to LAN1 to setup traffic that will be transmitted by the LAN1 interface. Enter the LAN1 interface bandwidth as 100000kbps (100Mbps). Click the Apply button to enforce the LAN1 link bandwidth to be specified bandwidth. In the table, the root class represents the whole bandwidth of the link. By default the link is partitioned into two classes: control class (ctl_class) and default class (def_class). The control class reserves bandwidth for control protocols such as ICMP, TCP ACKs. The default class is the default action of non-matched packets. The default class can be recursively partitioned into more classes. The classes are organized as a tree. Click Create Sub-Class to partition the default class.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions



Bandwidth Management->Edit Actions

Edit ANY to WAN1 classes

WAN1 Interface Bandwidth: 100000 kbps Apply

Item	Defined Actions				
	#	Active	Name	Borrow	Bandwidth
○	1	Y	WAN1 Interface		100000 kbps
○	2	Y	(100%) root_class	N	100000 kbps
○	3	Y	(5%) ctl_class	Y	5000 kbps
●	4	Y	(95%) def_class	Y	95000 kbps

Page 1/1

FIELD	DESCRIPTION	Range/Format	EXAMPLE
Edit __ to __ classes	Select the direction of action which you are going to configure one.	ANY to WAN/LAN/DMZ	Edit ANY to LAN1 classes
LAN1 Interface Bandwidth __ kbps	Fill the real bandwidth which is located in the upper direction.	10 to 100000 kbps	100000 kbps
BUTTON	DESCRIPTION		
Prev. Page	If there are more than one action pages, you can press Prev. Page to back to the previous page.		
Next Page	If there are more than one action pages, you can press Next Page to go to the next page.		
Create-Sub-class	Create a sub class from the indicated class.		
Edit	Edit the properties of the existent class.		
Delete	Delete the indicated class.		

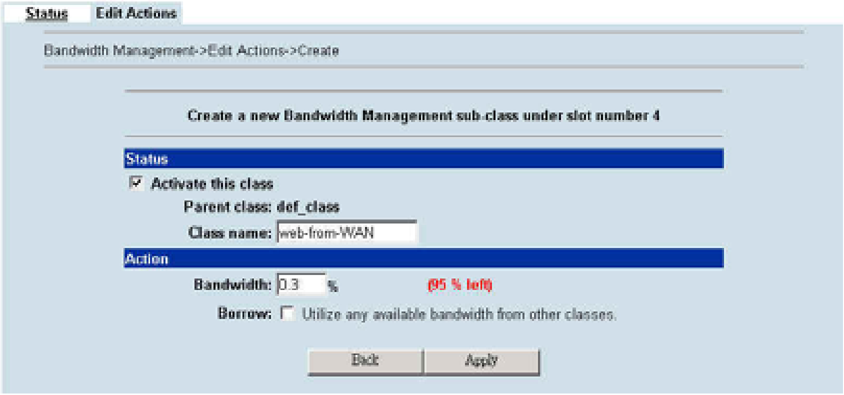
Table 24-4 Setup edit actions page of Bandwidth Management

Step 3. Add new classes

Create a sub-class named `web-from-WAN` from the default class. Enter `0.3%` in the `bandwidth` field. Make sure that `Borrow` button is unchecked and then web-from-WAN class will not enlarge the bandwidth from borrowing other unused bandwidth. Finally, click `Apply` button. See the steps in the right diagram.

Subsequently, we will continue to setup another two classes, such as video-from-WAN class and web-from-DMZ class. Select the default class and click the `Create Sub-Class` to create these two classes. The setting procedure is the same as the web-from-WAN class described.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-class



Status | Edit Actions

Bandwidth Management->Edit Actions->Create

Create a new Bandwidth Management sub-class under slot number 4

Status

☑ Activate this class

Parent class: def_class

Class name: web-from-WAN

Action

Bandwidth: 0.3 % (95 % left)

Borrow: □ Utilize any available bandwidth from other classes.

Back | Apply

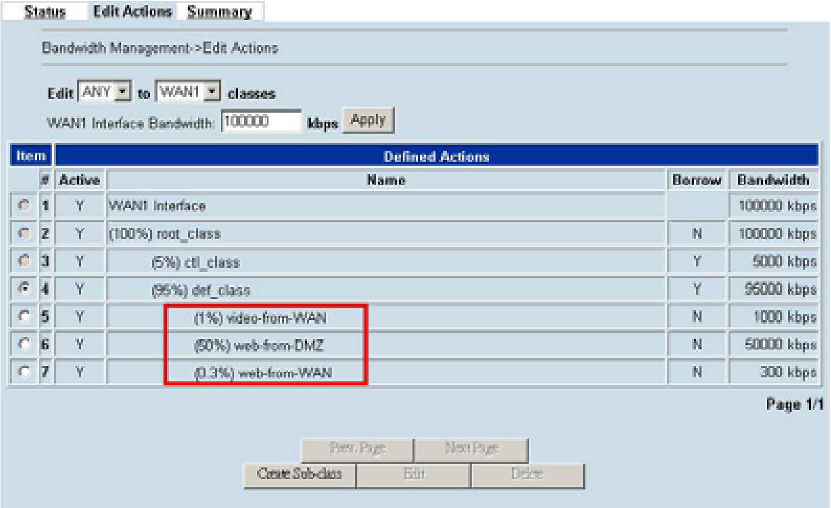
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Activate this class	Enable the bandwidth management class for later using	Enable/Disable	Enabled
Class name	Bandwidth management class name	text string	web-from-WAN
Bandwidth	How many percentage does this class occupy higher class?	0.1 ~ Max Value (as red text described)	0.3
Borrow	When the bandwidth of other class is idle, it will use the bandwidth of other class to increase bandwidth temporarily.	Enable/Disable	Disabled
BUTTON	DESCRIPTION		
Back	back to previous configuration page.		
Apply	Apply the settings which have been configured.		
Reset	Clean the filled data and restore the original one.		

Table 24-5 Add new class in the bandwidth management feature

Step 4. Partition into Classes

Now there are three actions under the default action.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-Class



Status | Edit Actions | Summary

Bandwidth Management->Edit Actions

Edit ANY to WAN1 classes

WAN1 Interface Bandwidth: 100000 kbps Apply

Item		Defined Actions			
	#	Active	Name	Borrow	Bandwidth
○	1	Y	WAN1 Interface		100000 kbps
○	2	Y	(100%) root_class	N	100000 kbps
○	3	Y	(5%) ctl_class	Y	5000 kbps
●	4	Y	(95%) def_class	Y	95000 kbps
○	5	Y	(1%) video-from-WAN	N	1000 kbps
○	6	Y	(50%) web-from-DMZ	N	50000 kbps
○	7	Y	(0.3%) web-from-WAN	N	300 kbps

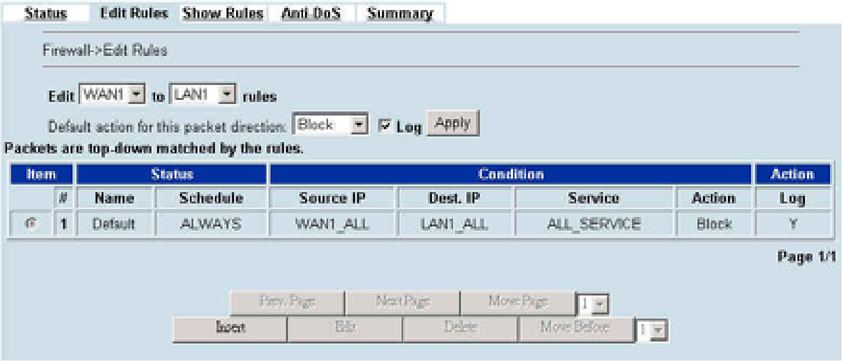
Page 1/1

Prev. Page | Next Page
Create Sub-class | Edit | Delete

Step 5. Setup WAN1-to-LAN1 Rules

Select `WAN1 to LAN1` to display the rules. There is a pre-defined rule that matches all traffic into the default class. Click `Insert` to insert a rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

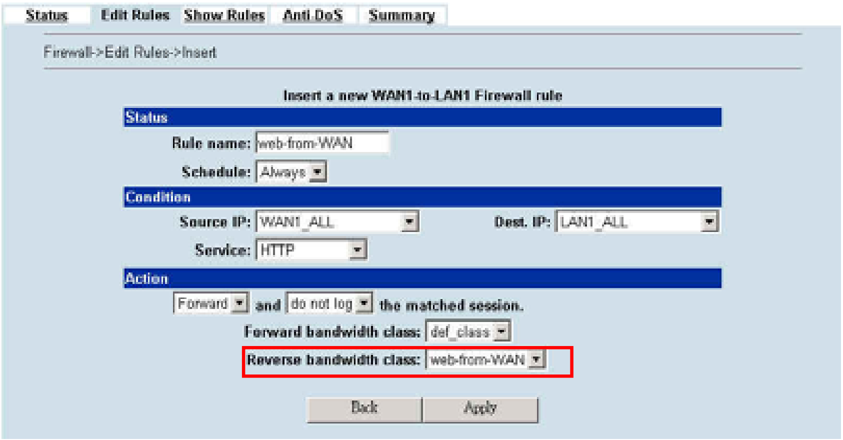
Page 1/1

Step 6. Customize the Rule

Enter a rule name such as `web-from-WAN`, select `Source IP` as `WAN1_ALL` and `Dest. IP` as `LAN1_ALL`. Besides, make sure the Service is `HTTP` port 80 because of that this is web service. Select the action to be `web-from-WAN`. In this way. All inbound web traffic from WAN1 will be put into the `web-from-WAN` queue and scheduled out at 300kbps bandwidth. Click `Apply` to store the changes.

Repeat the same procedure for the `video-from-WAN` class.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: web-from-WAN

Schedule: Always

Condition

Source IP: WAN1_ALL Dest. IP: LAN1_ALL

Service: HTTP

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: web-from-WAN

Action	Forward / Block the matched session	If packet is matched the rule condition, Forward or Block this matched packet?	Forward / Block	Forward
	Don’t log / Log the matched session	If packet is matched the rule condition, Log or Don’t log this matched packet?	log / don’t log	do not log
	Forward bandwidth class	Forward the bandwidth class if any.	def_class E-Commerce LAN_1-to-LAN_2	def_class
	Reverse bandwidth class	Reverse the bandwidth class if any.	def_class web-from-DMZ video-from-WAN web-from-WAN	web-from-WAN

Table 24-6 Add a new Bandwidth Management rule

✓ Note

For the other field description above, please refer 錯誤! 找不到參照來源。 for details.

Step 7. View the rules

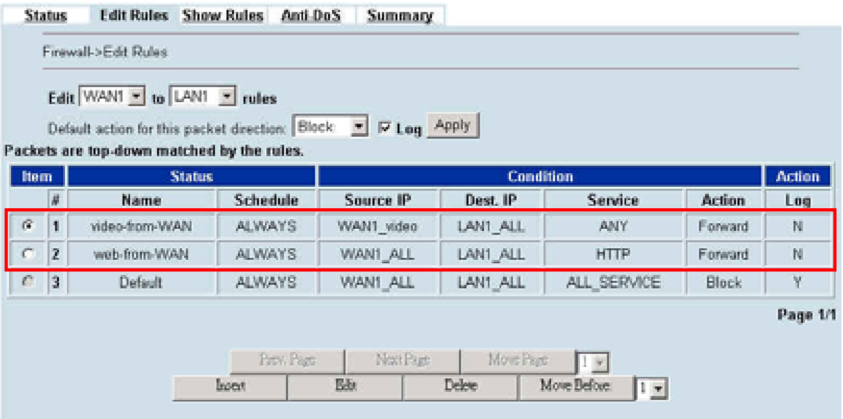
Now we can see that there are existed two customized rules in the queue of WAN1 to LAN1 direction.

In the No. 1 rule. The MH-5001 is configured to direct video-from-WAN packets into the video-from-WAN queue (300kbps).

In the No. 2 rule. The MH-5001 will direct web-from-WAN packets into the web-from-WAN queue (1000kbps).

In the No. 3 rule. The other traffic will be put into the def_class queue (any available bandwidth).

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

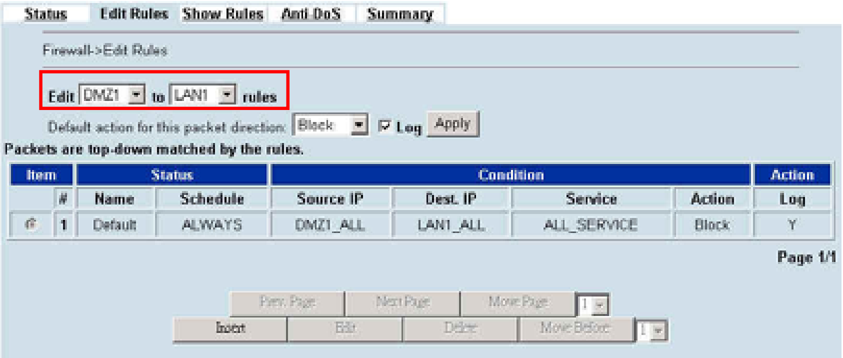
Item		Status		Condition			Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	video-from-WAN	ALWAYS	WAN1_video	LAN1_ALL	ANY	Forward	N
○	2	web-from-WAN	ALWAYS	WAN1_ALL	LAN1_ALL	HTTP	Forward	N
○	3	Default	ALWAYS	WAN1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

Page 1/1

Step 8. Add DMZ to LAN1 rule

Here we will add another rule (web from DMZ). Select DMZ1 to LAN1 direction.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit DMZ1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition			Action	
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	DMZ1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

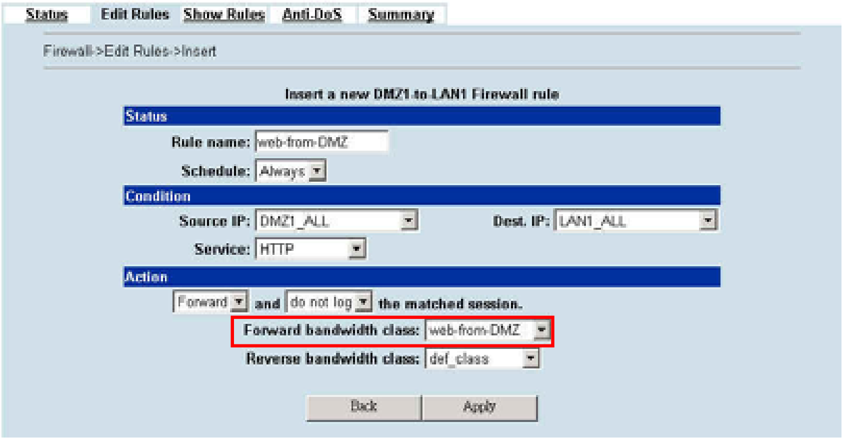
Page 1/1

Step 9. Customize the rule

Setup the web-from-DMZ rule. Select the defined `Source IP / Dest. IP`. It means that if the packets come from DMZ and targeted LAN1 region, we do not need to care about its source / dest IP. If the packets request for web traffic (source port 80), it will be put into the `web-from-DMZ` queue by MH-5001 bandwidth management feature.

Not: In the `Action` region, the `web-from-DMZ` class was edited in the previous Step 4 before.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new DMZ1-to-LAN1 Firewall rule

Status

Rule name: web-from-DMZ

Schedule: Always

Condition

Source IP: DMZ1_ALL Dest. IP: LAN1_ALL

Service: HTTP

Action

Forward and do not log the matched session.

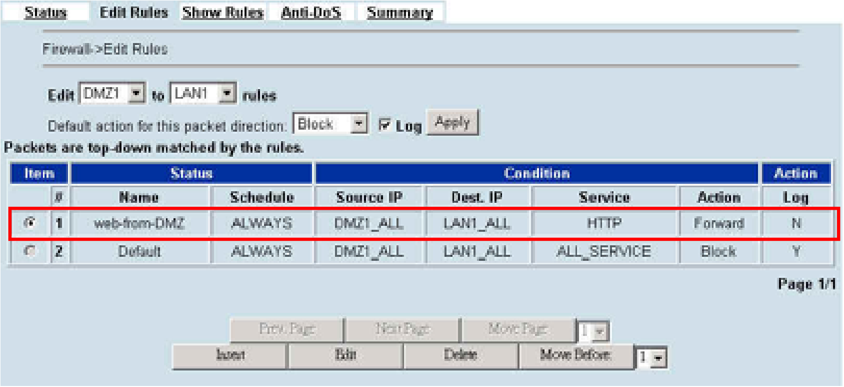
Forward bandwidth class: web-from-DMZ

Reverse bandwidth class: def_class

Step 10. View the results

We can see the result of our settings at the DMZ-to-LAN rule direction.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit DMZ1 to LAN1 rules

Default action for this packet direction: Block ☑ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	web-from-DMZ	ALWAYS	DMZ1_ALL	LAN1_ALL	HTTP	Forward	N
○	2	Default	ALWAYS	DMZ1_ALL	LAN1_ALL	ALL_SERVICE	Block	Y

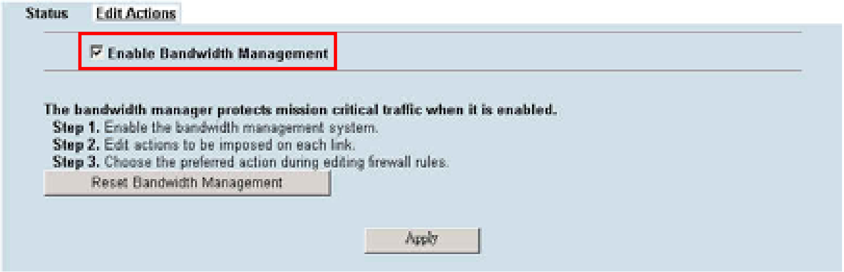
Page 1/1

24.4.1 Outbound Traffic Management

Step 1. Enable Bandwidth Management

Check the `Enable Bandwidth Management` checkbox, click the `Apply`.

ADVANCED SETTINGS > Bandwidth Mgt. > Status



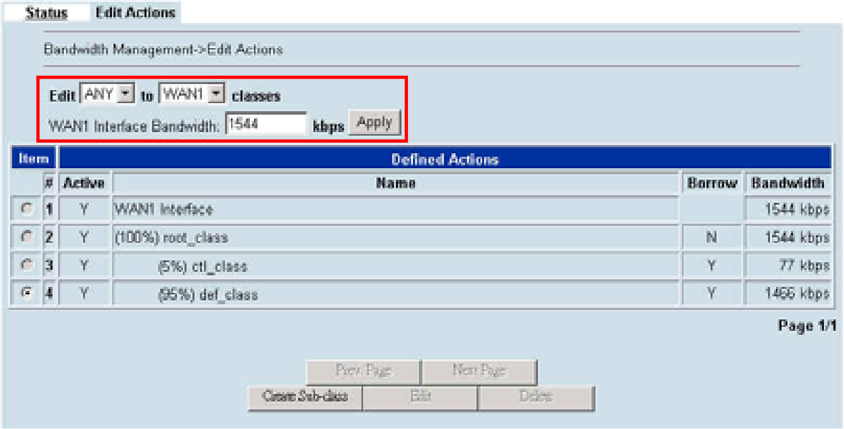
☑ Enable Bandwidth Management

The bandwidth manager protects mission critical traffic when it is enabled.
Step 1. Enable the bandwidth management system.
Step 2. Edit actions to be imposed on each link.
Step 3. Choose the preferred action during editing firewall rules.

Step 2. Setup the WAN1 Link

Select ANY to WAN1 to setup traffic that will be transmitted by the WAN1 interface. Enter the WAN1 interface bandwidth as 1544kbps. Click the `Apply` button to enforce the WAN1 link bandwidth to be 1544kbps. Then click `Create Sub-Class` to partition the default class.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions



Bandwidth Management->Edit Actions

Edit ANY to WAN1 classes

WAN1 Interface Bandwidth: 1544 kbps Apply

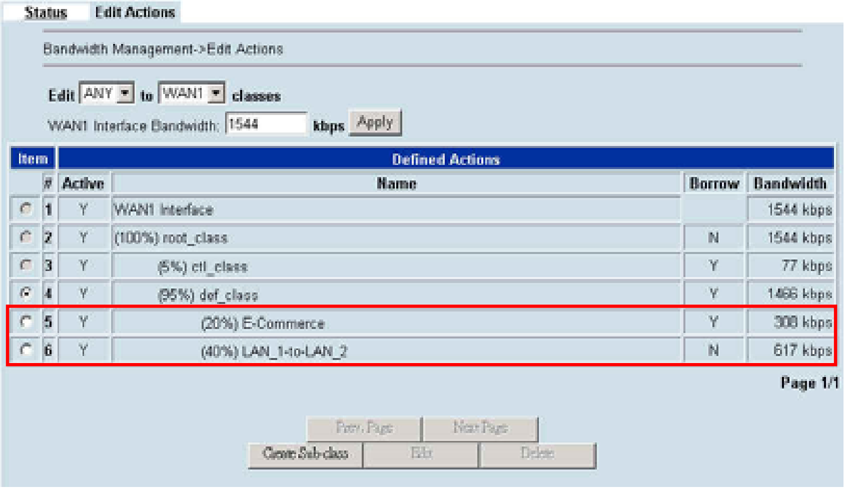
Item	Defined Actions			
#	Active	Name	Borrow	Bandwidth
○ 1	Y	WAN1 Interface		1544 kbps
○ 2	Y	(100%) root_class	N	1544 kbps
○ 3	Y	(5%) ctl_class	Y	77 kbps
● 4	Y	(95%) def_class	Y	1466 kbps

Page 1/1

Step 3. Partition into Classes

Create a sub-class named LAN_1-to-LAN_2 from the default class. Enter 40% in the bandwidth field, uncheck the Borrow button, and click Apply. Select the default class and click the Create Sub-Class to create another sub-class named E-Commerce from the default class. Enter 20% in the bandwidth field, check the Borrow button and click Apply. Now there are two actions under the default action. They are separately LAN_1-to-LAN_2 and E-Commerce class as the right diagram.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-Class



Bandwidth Management->Edit Actions

Edit ANY to WAN1 classes

WAN1 Interface Bandwidth: 1544 kbps Apply

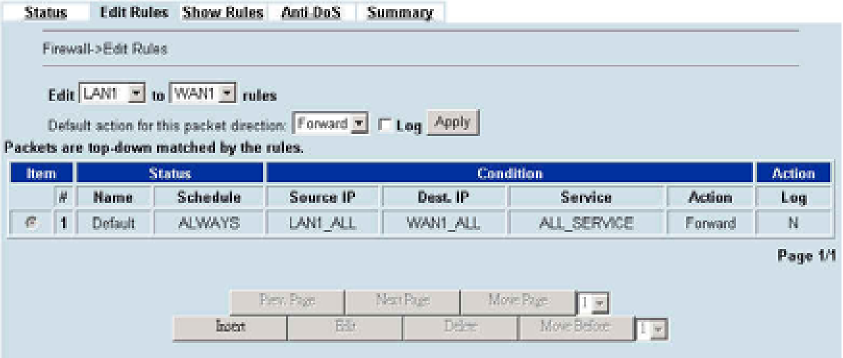
Item		Defined Actions			
	#	Active	Name	Borrow	Bandwidth
○	1	Y	WAN1 Interface		1544 kbps
○	2	Y	(100%) root_class	N	1544 kbps
○	3	Y	(5%) ctl_class	Y	77 kbps
●	4	Y	(95%) def_class	Y	1466 kbps
○	5	Y	(20%) E-Commerce	Y	308 kbps
○	6	Y	(40%) LAN_1-to-LAN_2	N	617 kbps

Page 1/1

Step 4. Setup LAN1-to-WAN1 Rules

Select LAN1 to WAN1 to display the rules. There is a pre-defined rule that matches all traffic into the default class. Click Insert to insert a rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward □ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	LAN1_ALL	WAN1_ALL	ALL_SERVICE	Forward	N

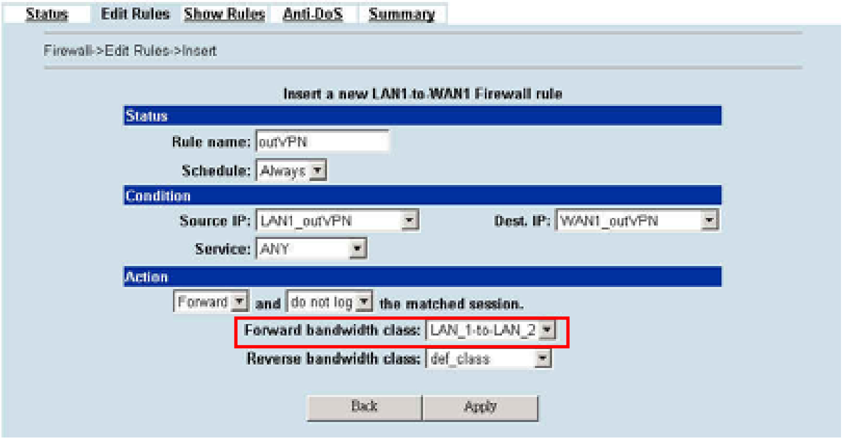
Page 1/1

Step 5. Customize the Rules

Enter a rule name such as outVPN, select the defined Source IP as LAN1_outVPN and Dest. IP as WAN1_outVPN. Select the action to be LAN_1-to-LAN_2. In this way, all outbound packets to the LAN_2 area will be put into the LAN_1-to-LAN_2 queue and scheduled out at 617 kbps bandwidth. Click Apply to store the changes.

Repeat the same procedure for the outE-Commerce rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert



Firewall->Edit Rules->Insert

Insert a new LAN1 to WAN1 Firewall rule

Status

Rule name: outVPN

Schedule: Always

Condition

Source IP: LAN1_outVPN Dest. IP: WAN1_outVPN

Service: ANY

Action

Forward and do not log the matched session.

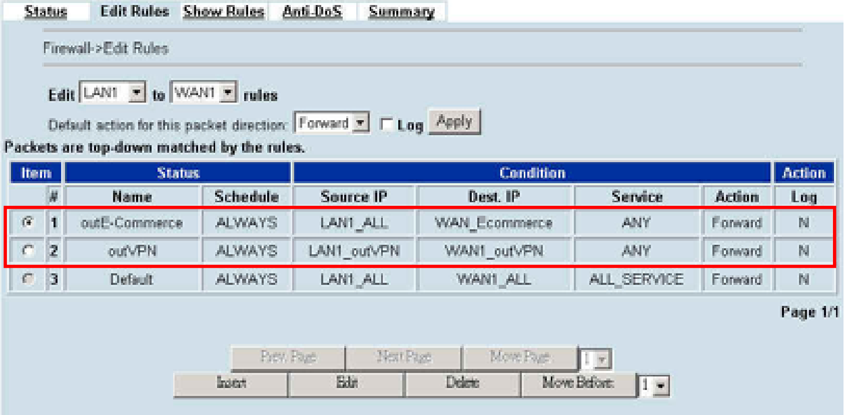
Forward bandwidth class: LAN_1-to-LAN_2

Reverse bandwidth class: def_class

Step 6. View the rules

The MH-5001 is configured to direct outE-Commerce matched packets into the E-Commerce queue (308 kbps), outVPN matched packets into the LAN_1-to-LAN_2 queue (617 kbps). Here we reserve 40% WAN1 bandwidth for the LAN_1 to LAN_2 VPN data, to guarantee the data communication between VPN. The other traffic will be put into the def_class queue (any available bandwidth).

ADVANCED SETTINGS > Firewall > Edit Rules



Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward □ Log Apply

Packets are top-down matched by the rules.

Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	outE-Commerce	ALWAYS	LAN1_ALL	WAN_Ecommerce	ANY	Forward	N
○	2	outVPN	ALWAYS	LAN1_outVPN	WAN1_outVPN	ANY	Forward	N
○	3	Default	ALWAYS	LAN1_ALL	WAN1_ALL	ALL_SERVICE	Forward	N

Page 1/1

Chapter 25
Load Balancer

This chapter introduces Load Balancer and explains how to implement it.

25.1 Demands

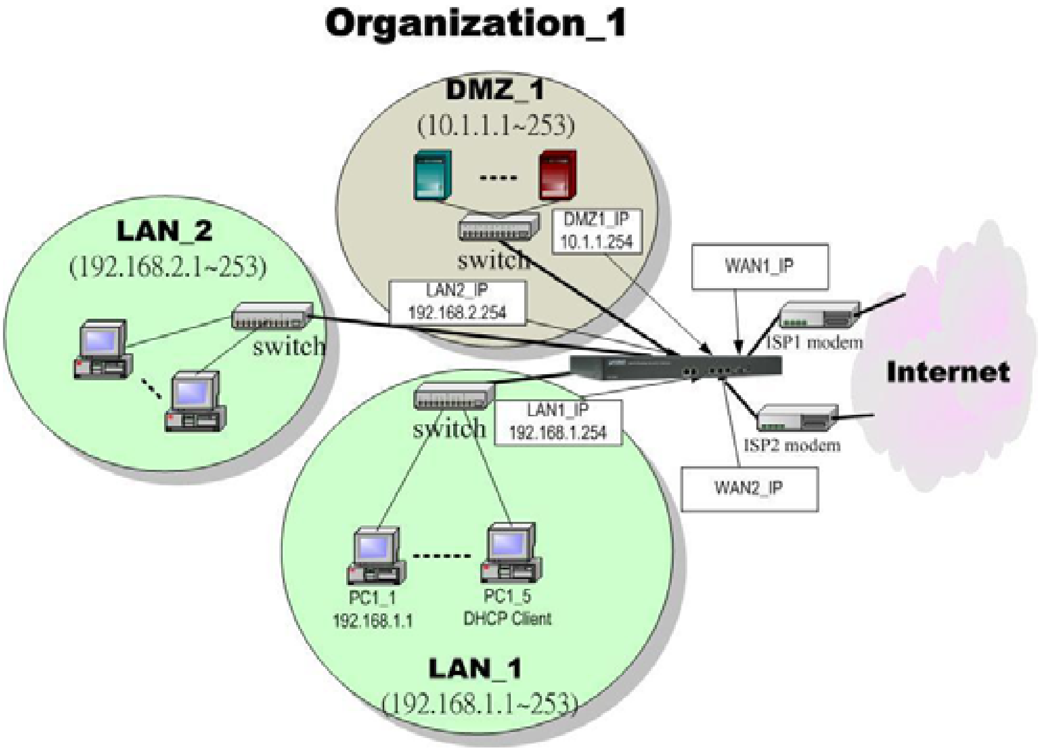


Figure 25-1 Multiple WAN settings of MH-5001

The WAN load balancer module consists of outbound load balancing and inbound load balancing. Users may want to subscribe multiple WAN links and make their outbound traffic load-balanced among the WAN links. MH-5001 now supports outbound WAN load balancing. Inbound load balancing will be supported in a very near future.

25.2 Objectives

The traffic from LAN_1 and LAN_2 towards the Internet are intelligently outbound load-balanced between the WAN links. However, traffic from DMZ_1 towards the Internet will be decided by the inbound load balancing module.

25.3 Methods

The outbound WAN load balancer module will intelligently decide whether the new connection will be directed to which WAN link. It has a built-in fuzzy intelligence that will measure the round-trip delay of the traffic and make the best route selection.

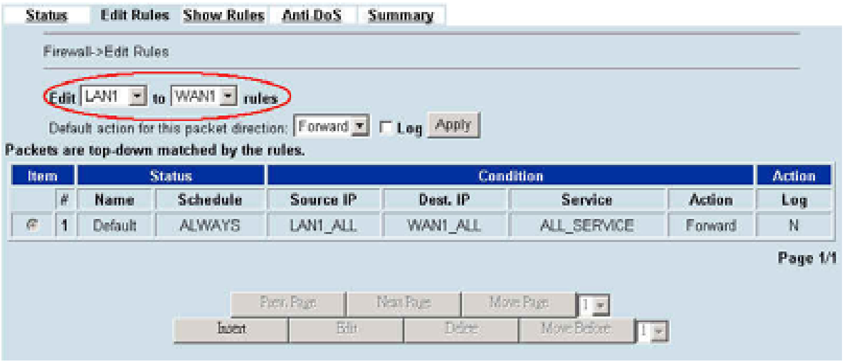
25.4 Steps

25.4.1 Outbound Load Balancer

Step 1. Make Firewall rules the same

Since the traffic will be intelligently load-balanced among the WAN links, the Firewall settings for all WAN links should be set to the same settings. For example, you have to make sure that all LAN1-to-WAN1 Firewall rules are the same as those in LAN1-to-WAN2, LAN2-to-WAN1, and LAN2-to-WAN2 rules. Otherwise, the traffic may be blocked by the firewall rules accidentally due to the load balancing decision.

ADVANCED SETTINGS > Firewall > Edit Rules



Firewall->Edit Rules

Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward □ Log Apply

Packets are top-down matched by the rules.

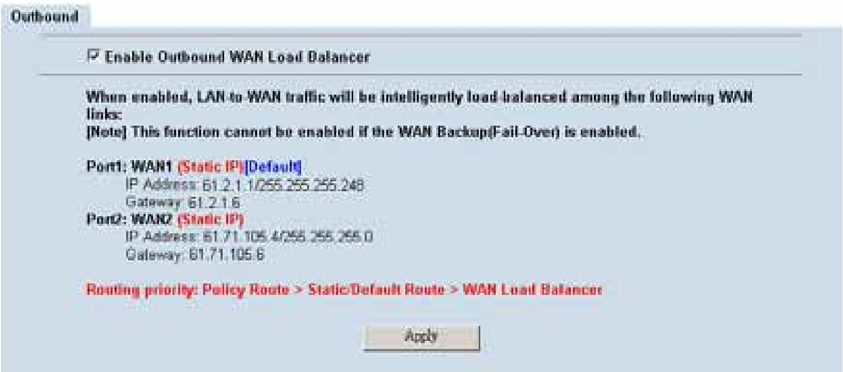
Item		Status		Condition				Action
	#	Name	Schedule	Source IP	Dest. IP	Service	Action	Log
●	1	Default	ALWAYS	LAN1_ALL	WAN1_ALL	ALL_SERVICE	Forward	N

Page 1/1

Step 2. Enable outbound WAN load balancer

Check the `Enable Outbound WAN Load Balancer` checkbox, click the `Apply`.

ADVANCED SETTINGS > Load Balancer > Outbound



☑ Enable Outbound WAN Load Balancer

When enabled, LAN-to-WAN traffic will be intelligently load-balanced among the following WAN links:
[Note] This function cannot be enabled if the WAN Backup(Fail-Over) is enabled.

Port1: WAN1 (Static IP)[Default]
IP Address: 61.2.1.1/255.255.255.248
Gateway: 61.2.1.6
Port2: WAN2 (Static IP)
IP Address: 61.71.105.4/255.255.255.0
Gateway: 61.71.105.6

Routing priority: Policy Route > Static/Default Route > WAN Load Balancer

Note that the priority among the policy route, static route, and WAN load balancer are explicitly shown as Policy Route > Static/Default Route > WAN Load Balancer. If there are conflicted settings among these three settings, the route will be chosen according to the priority.

Chapter 26
High Availability

This chapter introduces High Availability and explains how to implement it.

26.1 Demands

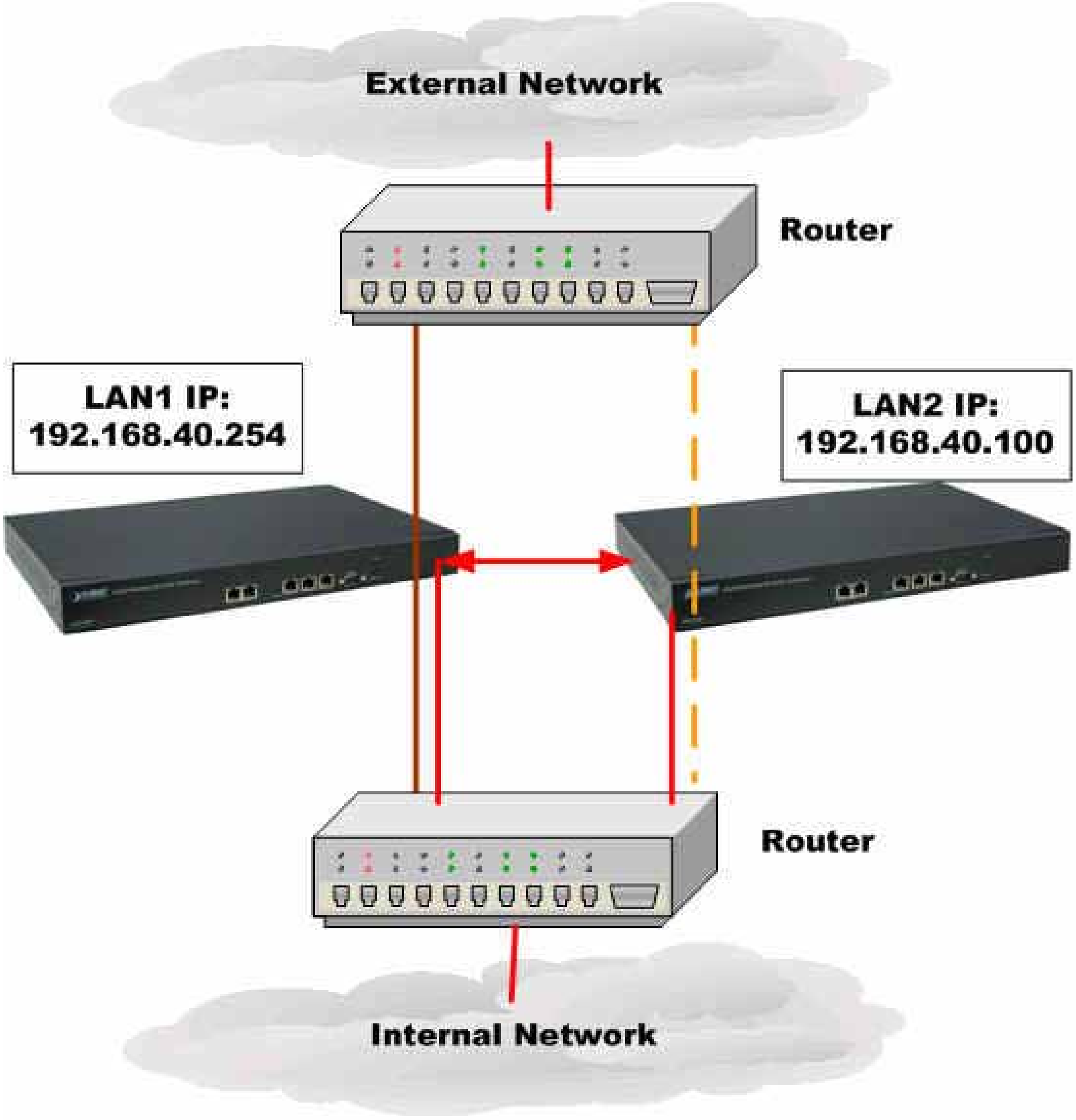


Figure 26-1 Use High Availability mechanism to let network connection continually

1. As the above Figure 22-1 illustrates, your company is afraid that the firewall may be crashed someday, so it needs a backup system to let the network connection continually. High Availability makes it possible to let the network in your company operate smoothly.

26.2 Objectives

1. Prepare two MH-5001 devices, and then let one as a primary firewall and the other as a secondary firewall. While the primary firewall is crashed, you can replace it with secondary firewall.

26.3 Methods

There are five steps to configure High Availability feature.

Step 1. You have to setup two MH-5001 devices first. Remember to set the Action Mode for primary device as `Active mode` and secondary device as `Standby mode`.

Step 2. When the primary device crashed, the secondary device will replace it within 30 seconds while detecting by "ping" command.

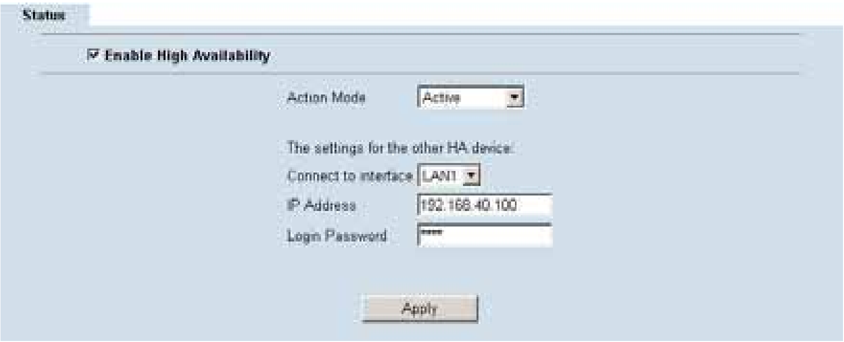
Step 3. The secondary device will immediately load the configuration under primary device, and then change its action mode to `Active mode.`

Step 4. After rebooting, the primary device will automatically change its action mode to `Standby mode` if it detects the secondary device in `active mode already`.

Step 5. If both of primary and secondary devices crashed simultaneously, the one which reboots faster will action as `Active mode`, and the other will be `in Standby mode`.

26.4 Steps

26.4.1 Setup High Availability

Step 1. Enable High Availability	**ADVANCED SETTINGS > High Availability > Status**
Check the `Enable High Availability` checkbox. Select the Action Mode as `Active` if it is the primary device and `Standby` for the secondary device. And then configure the other HA device. Select which interface to connect to. Enter `IP Address` and `Login Password`. Note that you have to configure the Secondary device as `Standby mode` and the IP address/ Login Password of the Primary device, so High Availability can work then.	 Status ☑ Enable High Availability Action Mode: Active The settings for the other HA device: Connect to interface: LAN1 IP Address: 192.168.40.100 Login Password: **** Apply

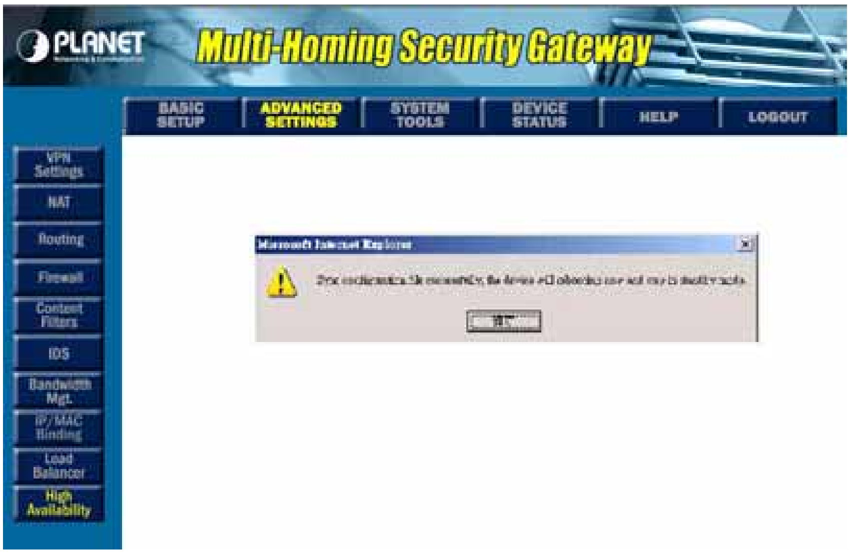
FIELD	DESCRIPTION	Range/Format	EXAMPLE
Enable High Availability	Enable High Availability feature of MH-5001	Enable/Disable	Enabled
Action Mode	Specify which device is Active or Standby.	Active/Standby	Active
Connect to interface	The interface which the HA devices will connect to.	LAN1/LAN2/DMZ	LAN1
IP Address	The IP address of the other HA device.	IPv4 format	192.168.40.100
BUTTON	DESCRIPTION		
Apply	Apply the settings which have been configured.		

Table 26-1 Setup status page of High Availability

Step 2. Show the result in Web

After you apply the High Availability feature, the secondary device will show the message to tell you that "`Sync configuration file successfully, the device will rebooting` now and `stay` in `standby` `mode.`"

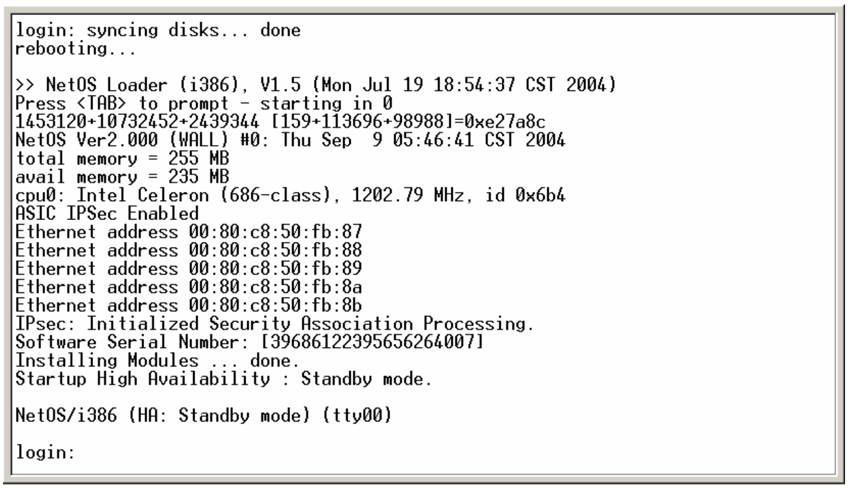
ADVANCED SETTINGS > High Availability > Status



Sync configuration file successfully, the device will rebooting now and stay in standby mode.

Step 3. Show the message in Console

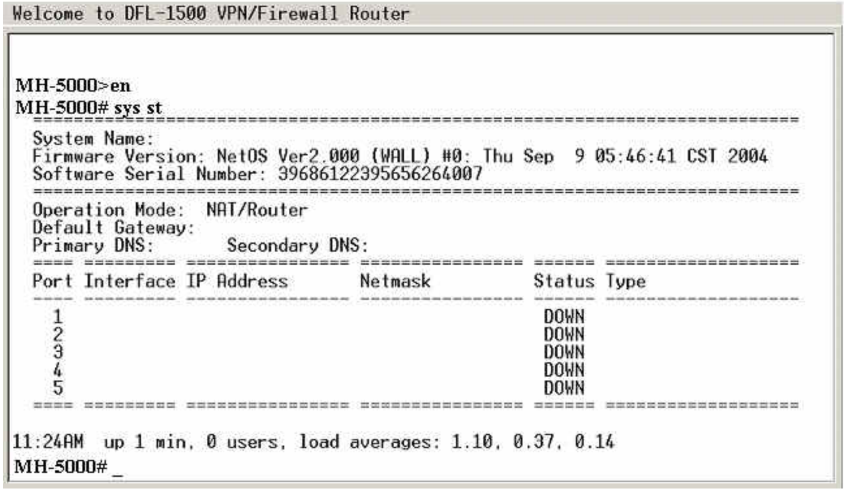
When Primary device crashed, the messages like the right diagram will appear to tell you that this device will be in Standby mode after rebooting.



```
login: syncing disks... done
rebooting...

>> NetOS Loader (i386), V1.5 (Mon Jul 19 18:54:37 CST 2004)
Press <TAB> to prompt - starting in 0
1453120+10732452+2439344 [159+113696+98988]=0xe27a8c
NetOS Ver2.000 (WALL) #0: Thu Sep  9 05:46:41 CST 2004
total memory = 255 MB
avail memory = 235 MB
cpu0: Intel Celeron (686-class), 1202.79 MHz, id 0x6b4
ASIC IPSec Enabled
Ethernet address 00:80:c8:50:fb:87
Ethernet address 00:80:c8:50:fb:88
Ethernet address 00:80:c8:50:fb:89
Ethernet address 00:80:c8:50:fb:8a
Ethernet address 00:80:c8:50:fb:8b
IPsec: Initialized Security Association Processing.
Software Serial Number: [3968612239565626400 7]
Installing Modules ... done.
Startup High Availability : Standby mode.

NetOS/i386 (HA: Standby mode) (tty00)

login:
```

Step 4. Check the Device status

You can see the status of the device in Standby mode here.



```
Welcome to DFL-1500 VPN/Firewall Router


MH-5000>en
MH-5000# sys st
  ======================================================================
  System Name:
  Firmware Version: NetOS Ver2.000 (WALL) #0: Thu Sep  9 05:46:41 CST 2004
  Software Serial Number: 39686122395656264007
  ======================================================================
  Operation Mode:  NAT/Router
  Default Gateway:
  Primary DNS:       Secondary DNS:
  ==== ========= =============== =============== ====== ==================
  Port Interface IP Address      Netmask         Status Type
  ---- --------- --------------- --------------- ------ ------------------
    1                                             DOWN
    2                                             DOWN
    3                                             DOWN
    4                                             DOWN
    5                                             DOWN
  ==== ========= =============== =============== ====== ==================

11:24AM  up 1 min, 0 users, load averages: 1.10, 0.37, 0.14
MH-5000# _
```

Chapter 27
System Status

27.1 Demands

1. Since we have finished the settings of MH-5001, we need to gather the device information quickly. Then we can have a overview of the system status.

27.2 Objectives

1. We can know the current situation easily through an integrated interface.

27.3 Methods

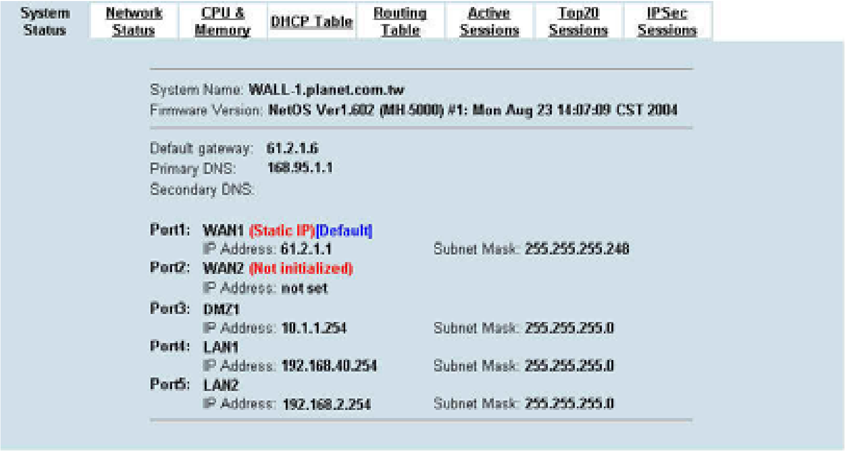
1. Through DEVICE STATUS > System Status path, we can get the needed information.

27.4 Steps

Step 1. System Status

Here we can see the system information (include system name, firmware version), and the full list of each port settings.

DEVICE STATUS > System Status > System Status



System Name: WALL-1.planet.com.tw
Firmware Version: NetOS Ver1.602 (MH-5000) #1: Mon Aug 23 14:07:09 CST 2004

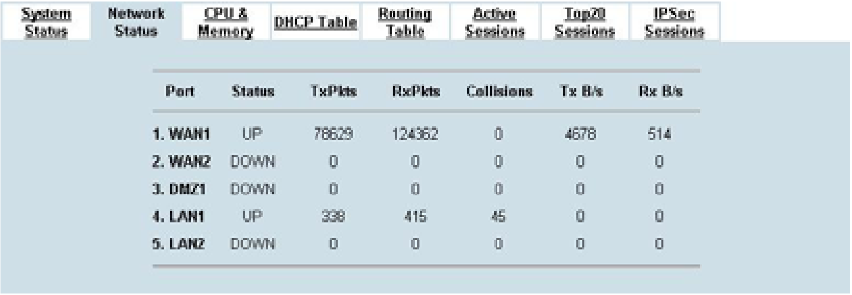
Default gateway: 61.2.1.6
Primary DNS: 168.95.1.1
Secondary DNS:

Port1: WAN1 (Static IP)[Default]
IP Address: 61.2.1.1 Subnet Mask: 255.255.255.248
Port2: WAN2 (Not initialized)
IP Address: not set
Port3: DMZ1
IP Address: 10.1.1.254 Subnet Mask: 255.255.255.0
Port4: LAN1
IP Address: 192.168.40.254 Subnet Mask: 255.255.255.0
Port5: LAN2
IP Address: 192.168.2.254 Subnet Mask: 255.255.255.0

Step 2. Network Status

We can know the port status here, whether the port is up or down, and view the amount of the transmitted packets or received packets in each port.

DEVICE STATUS > System Status > Network Status



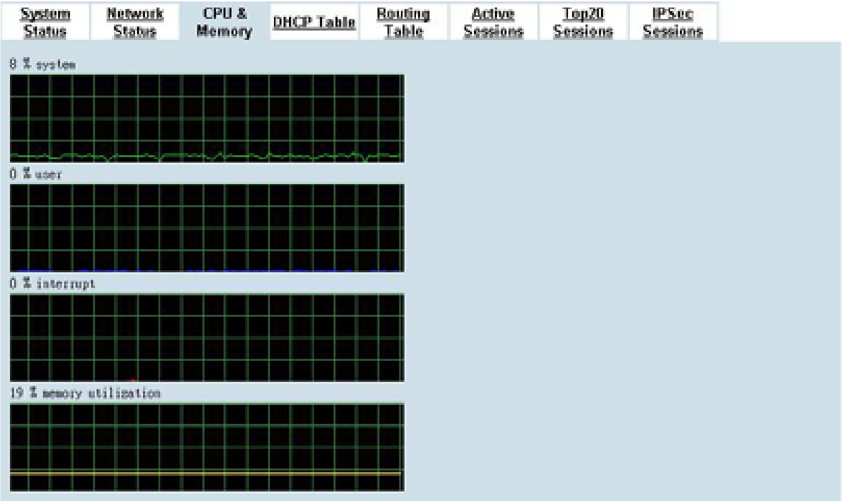
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s
1. WAN1	UP	78629	124362	0	4678	514
2. WAN2	DOWN	0	0	0	0	0
3. DMZ1	DOWN	0	0	0	0	0
4. LAN1	UP	338	415	45	0	0
5. LAN2	DOWN	0	0	0	0	0

Step 3. CPU & Memory

We can know the device information (include system, user, interrupt and memory utilization) through the graphic interface.

Note: If you can not view the graphic correctly, the situation may result from that you don’t install the java virtual machine (JVM) onto your browser. Simply go to the following link, http://java.sun.com/j2se/1.4.2/download.html. And then, download the Java 2 Platform, Standard Edition (JRE) to your platform (ex. windows). After installing JRE properly, you will see the CPU & Memory graphic as right side.

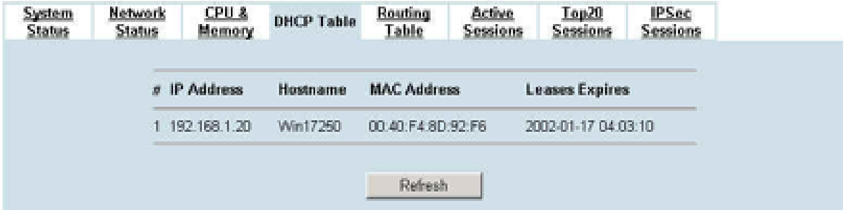
DEVICE STATUS > System Status > CPU & Memory



Step 4. DHCP Table

Through the DHCP Table, we can recognize which IP has been allocated by the DHCP server. And know which pc (MAC address) has been leased this IP address.

DEVICE STATUS > System Status > DHCP Table

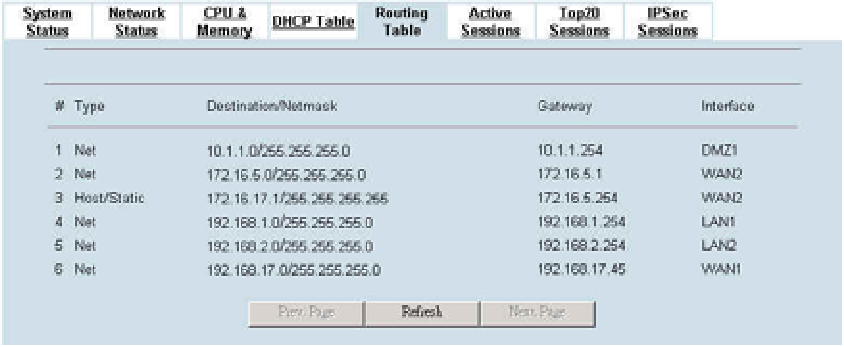


#	IP Address	Hostname	MAC Address	Leases Expires
1	192.168.1.20	Win17250	00:40:F4:8D:92:F6	2002-01-17 04:03:10

Step 5. Routing Table

Click the `Routing Table` to see the routing table information of MH-5001.

DEVICE STATUS > System Status > Routing Table

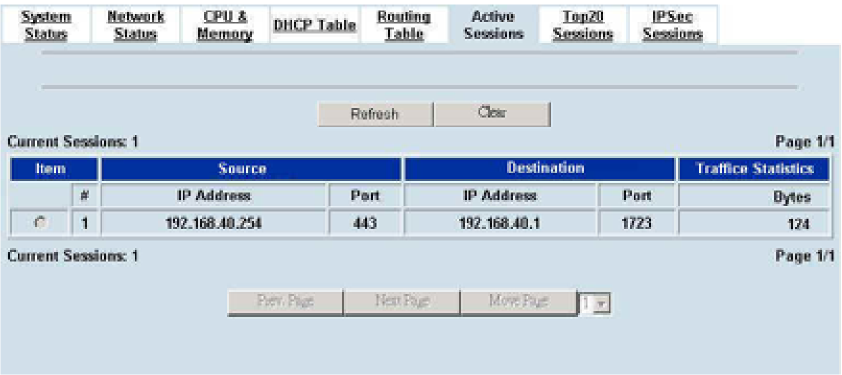


#	Type	Destination/Netmask	Gateway	Interface
1	Net	10.1.1.0/255.255.255.0	10.1.1.254	DMZ1
2	Net	172.16.5.0/255.255.255.0	172.16.5.1	WAN2
3	Host/Static	172.16.17.1/255.255.255.255	172.16.5.254	WAN2
4	Net	192.168.1.0/255.255.255.0	192.168.1.254	LAN1
5	Net	192.168.2.0/255.255.255.0	192.168.2.254	LAN2
6	Net	192.168.17.0/255.255.255.0	192.168.17.45	WAN1

Step 6. Active Sessions

Click the `Active Sessions` to see all the current sessions of MH-5001. The `Active Sessions` include all the outbound and inbound sessions.

DEVICE STATUS > System Status > Active Sessions



Current Sessions: 1 Page 1/1

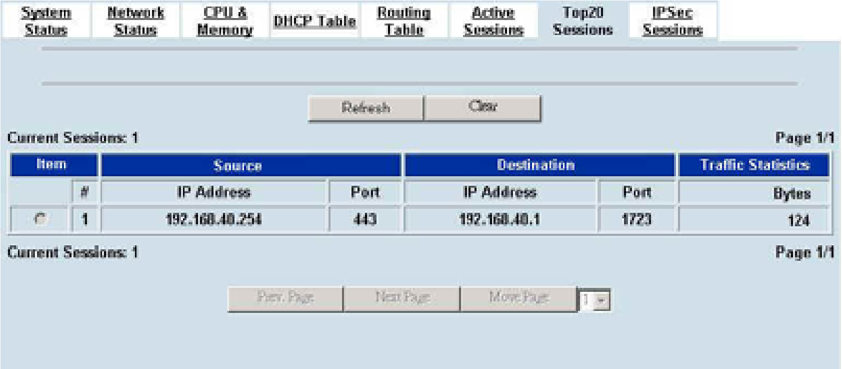
Item		Source		Destination		Traffice Statistics
	#	IP Address	Port	IP Address	Port	Bytes
○	1	192.168.40.254	443	192.168.40.1	1723	124

Current Sessions: 1 Page 1/1

Step 7. Top20 Sessions

Click the `Top20 Sessions` to see the front-20 sessions of transmitted bytes amount. These front-20 sessions were sorted by the amount of transmitted bytes.

DEVICE STATUS > System Status > Top20 Sessions



Current Sessions: 1 Page 1/1

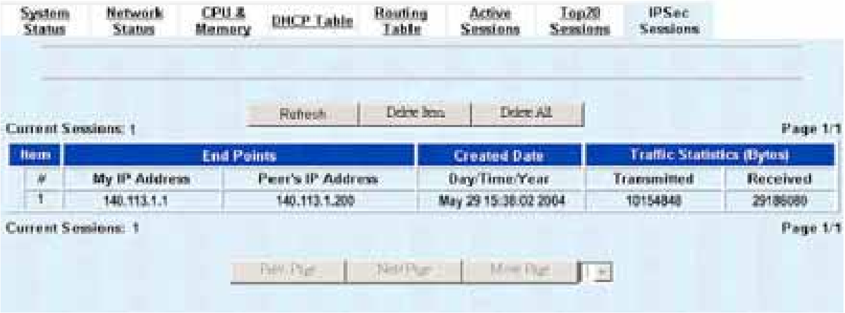
Item		Source		Destination		Traffic Statistics
	#	IP Address	Port	IP Address	Port	Bytes
○	1	192.168.40.254	443	192.168.40.1	1723	124

Current Sessions: 1 Page 1/1

Step 8. IPSec Sessions

If we use the IPSec to establish VPN with other device, then we can view the IPSec tunnel information in this page.

DEVICE STATUS > System Status > IPSec Sessions



Current Sessions: 1 Page 1/1

Item	End Points		Created Date	Traffic Statistics (Bytes)	
#	My IP Address	Peer's IP Address	Day/Time/Year	Transmitted	Received
1	140.113.1.1	140.113.1.200	May 29 15:38:02 2004	10154848	29186080

Current Sessions: 1 Page 1/1

Chapter 28
Log System

28.1 Demands

1. The System Administrator wants to know all the actions of administration in the past. So it can avoid illegal system administration.
2. The System Administrator needs to check the logs of VPN, IDS, Firewall, and Content Filter everyday. But he / she feels inconvient to verify the MH-5001 logs. He / She hopes to decrease the checking procedure.

28.2 Objectives

1. The System Administrator wants to know all actions of administration in the past.
2. The System administrator would like to view the daily log report of MH-5001.

28.3 Methods

1. Through tracking the system logs, you can distinguish which administrated action is valid or not.
2. Use the syslog server to receive mail, or edit the "Mail Logs" page of MH-5001. Make the log mailed out automatically every periodic time.

28.4 Steps

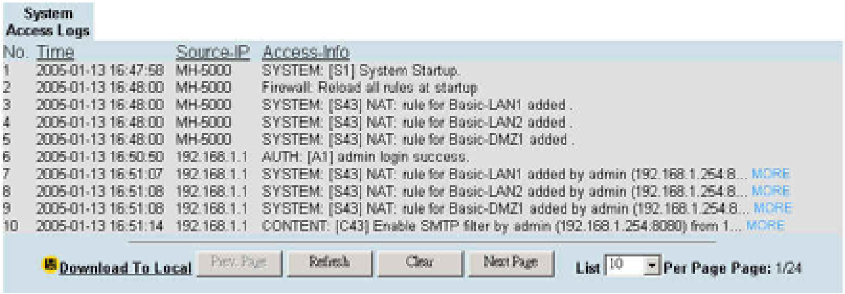
28.4.1 System Logs

Step 1. View System Logs

All the system administrated actions will be log in this page.

For the detailed information of System Logs, please refer Appendix C.

DEVICE STATUS > System Logs



No.	Time	Source-IP	Access-Info
1	2005-01-13 16:47:58	MH-5000	SYSTEM: [S1] System Startup.
2	2005-01-13 16:48:00	MH-5000	Firewall: Reload all rules at startup
3	2005-01-13 16:48:00	MH-5000	SYSTEM: [S43] NAT: rule for Basic-LAN1 added .
4	2005-01-13 16:48:00	MH-5000	SYSTEM: [S43] NAT: rule for Basic-LAN2 added .
5	2005-01-13 16:48:00	MH-5000	SYSTEM: [S43] NAT: rule for Basic-DMZ1 added .
6	2005-01-13 16:50:50	192.168.1.1	AUTH: [A1] admin login success.
7	2005-01-13 16:51:07	192.168.1.1	SYSTEM: [S43] NAT: rule for Basic-LAN1 added by admin (192.168.1.254:8... MORE
8	2005-01-13 16:51:08	192.168.1.1	SYSTEM: [S43] NAT: rule for Basic-LAN2 added by admin (192.168.1.254:8... MORE
9	2005-01-13 16:51:08	192.168.1.1	SYSTEM: [S43] NAT: rule for Basic-DMZ1 added by admin (192.168.1.254:8... MORE
10	2005-01-13 16:51:14	192.168.1.1	CONTENT: [C43] Enable SMTP filter by admin (192.168.1.254:8080) from 1... MORE

FIELD	DESCRIPTION
NO	system logs sequence number
Time	The time which is occurred by the specified system event.
Source-IP	A type of the specified system events.
Access--Info	The description of the system log. Include `Component Type`, `Log ID`, `Log Description` and `Event ID` (optional).

Table 28-1 System log description

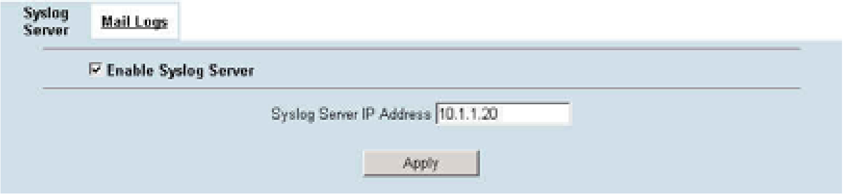
28.4.2 Syslog & Mail log

Step 1. Setup Syslog Server

Setup Syslog Server by checking the `Enable Syslog Server.` `It` will let MH-5001 send logs to the Syslog Server specified in the “`Syslog Server IP Address`” field.

Notice: If the logs were sent out to the syslog server, they will still keep a copy in the MH-5001.

DEVICE STATUS > Log Config > Syslog Server



☑ Enable Syslog Server

Syslog Server IP Address 10.1.1.20

FIELD	DESCRIPTION	EXAMPLE
Enable Syslog Server	Enable the Syslog Server feature of MH-5001	Enabled
Syslog Server IP Address	The IP Address which Syslog Server located.	10.1.1.20
BUTTON	DESCRIPTION	
Apply	Apply the configuration in this page	
Reset	Restore the original configuration in this page	

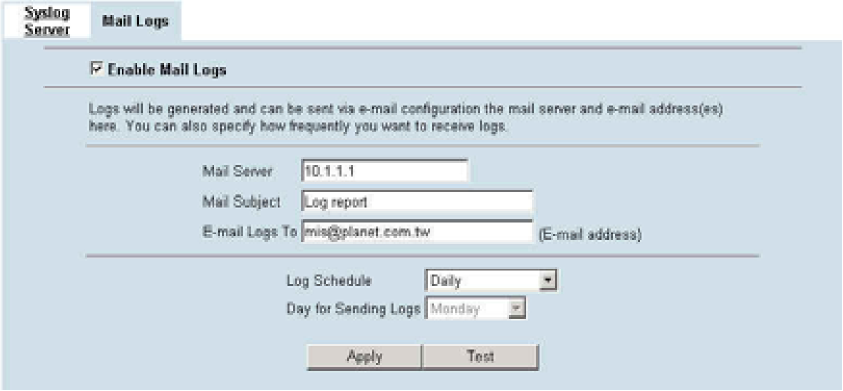
Table 28-2 Setup the Syslog Server

Step 2. Setup Mail Log method

Fill in the IP address of the `Mail Server` and `Mail Subject`. Also fill your `E-Mail address` for receiving logs. Select the preferred Log Schedule to mail out logs. Click the `Apply` button to finish the settings.

Notice: If the logs were sent out to the mail server, they will be deleted by the MH-5001.

DEVICE STATUS > Log Config > Mail Logs



☑ Enable Mail Logs

Logs will be generated and can be sent via e-mail configuration the mail server and e-mail address(es) here. You can also specify how frequently you want to receive logs.

Mail Server 10.1.1.1

Mail Subject Log report

E-mail Logs To mis@planet.com.tw (E-mail address)

Log Schedule Daily

Day for Sending Logs Monday

FIELD	DESCRIPTION	EXAMPLE
Enable Mail Logs	Enable the Mail Logs Server feature of MH-5001	Enabled
Mail Server	The IP Address of Mail Server which will send out the logs.	10.1.1.1
Mail Subject	The subject of log mail	Log Report
E-mail Logs To	E-Mail address of receiver	mis@planet.com.tw
Log Schedule	The schedule which the mail logs will be sent out.	Daily
Day for Sending Logs	When selecting Weekly in the “Log Schedule” field, we have to choose which day the mail logs will be sent out in the “Day for Sending Logs” field.	Monday
BUTTON	DESCRIPTION	
Apply	Apply the configuration in this page	

Test	test the mail logs configuration in this page

Table 28-3 Setup the Mail Logs

Chapter 29
System Maintenance

This chapter introduces how to do system maintenance.

29.1 Demands

1. MH-5001 is designed to provide upgradeable firmware and database to meet the upcoming dynamics of the Internet. New features, new attack signatures, new forbidden URLs, and new virus definitions require timely updates to the MH-5001. This chapter introduces how to upgrade your system with TFTP and Web UI respectively.

2. Sometimes one may want to reset the firmware to factory default due to loss of password, firmware corrupted, configuration corrupted. Since MH-5001 does not have a reset button to prevent careless pressing of it, factory default has to be set with web GUI or console terminal. Of course, when you loss the password, you have to use CLI only because you can never enter the web GUI with the lost password.

3. Anthoer issue is that after setup the MH-5001 properly, we might want to keep the current configuration to avoid the unknown accident. Then we can recover the original state from the previous reserved configuration.

29.2 Steps for TFTP Upgrade

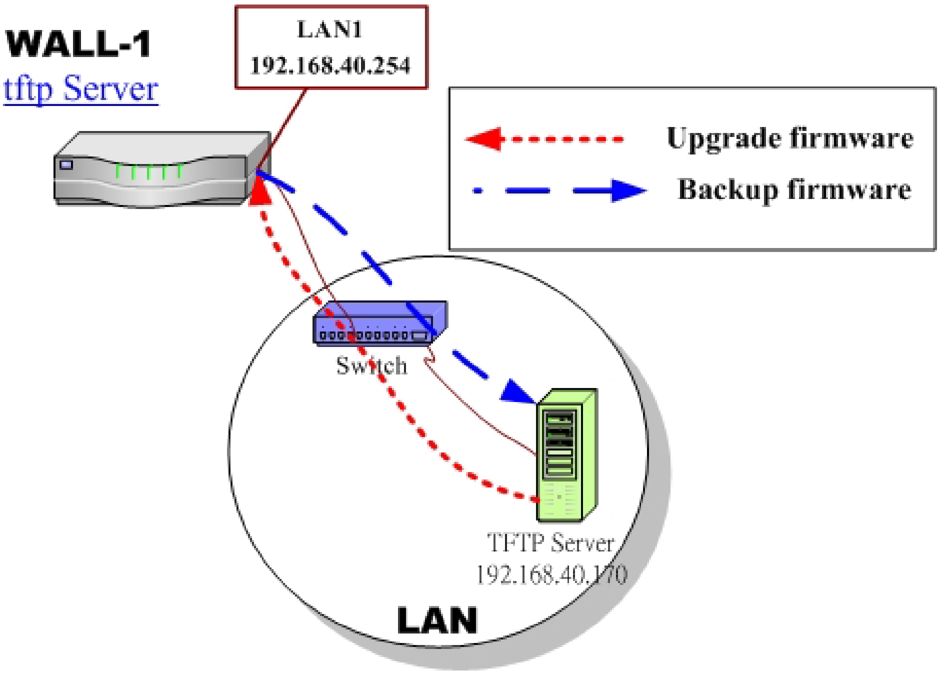
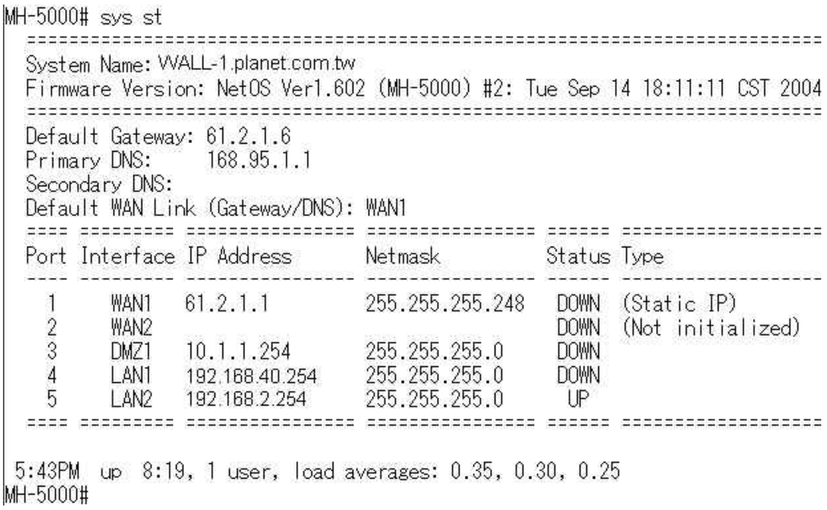


Figure 29-1 Upgrade/Backup firmware from TFTP server

Step 1. Setup TFTP server
Place the TFTP server `TftpServer` in the `c:\` directory and double click to run it. Place all `bin` files in the `c:\` as well. Set the PC to be 192.168.40.x to be in the same subnet with the MH-5001's LAN1. Login to MH-5001's console. Enter en to enter privileged mode. Configure the LAN1 address so that the MH-5001 can connect to the TFTP server. The CLI command to configure LAN1 interface is ip `ifconfig INTF3 192.168.1.254 255.255.255.0.`
	`NetOS/i386 (MH-5001) (tty00)`
	
	`login: admin`
	`Password:`
	`Welcome to MH-5001 Multi-Homing Security Gateway!`
	
	`MH-5001> en`
	`MH-5001# ip ifconfig INTF3 192.168.40.254 255.255.255.0`
	
	`MH-5001#`

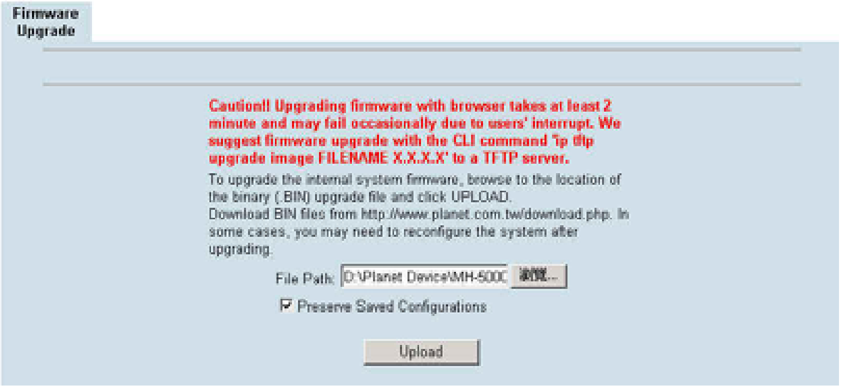
Step 2. Upgrade firmware
Enter `IP tftp upgrade image 192.168.1.x MH-5001-<ver>.bin After this procedure, MH-5001 device will reboot automatically.`
`Notice: if you want to preserve the previous configuration, add the "preserve" keyword to the end.`
`Refer Appendix A for the details.`
	`MH-5001# ip tftp upgrade image MH-5001-1.602-ALL.bin 192.168.1.170 preserve`
	
	`Fetching from 192.168.1.170 for MH-5001-1.602-ALL.bin`
	`tftp> tftp> Verbose mode on.`
	`tftp> getting from 192.168.1.170:MH-5001-1.602-ALL.bin to MH-5001-1.602-ALL.bin [octet]`

Step 3. Check if OK Check whether the system status is working properly or not.	

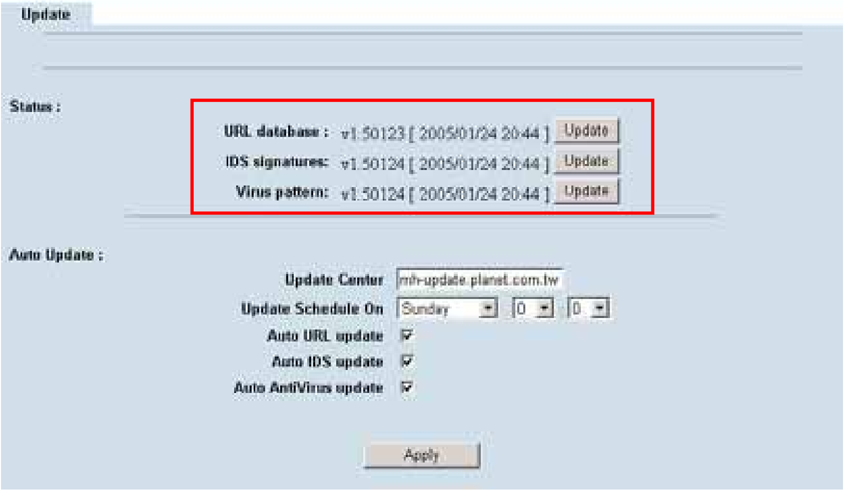
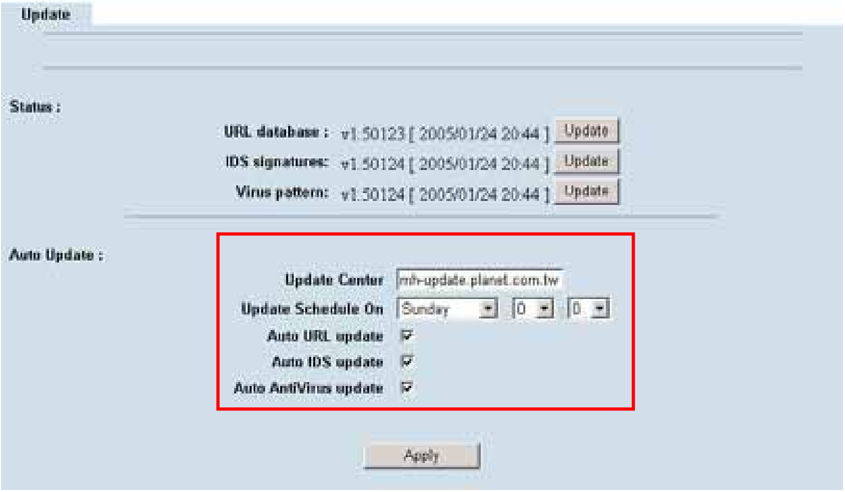
```
MH-5000# sys st
  =========================================================================
  System Name: WALL-1.planet.com.tw
  Firmware Version: NetOS Ver1.602 (MH-5000) #2: Tue Sep 14 18:11:11 CST 2004
  =========================================================================
  Default Gateway: 61.2.1.6
  Primary DNS:     168.95.1.1
  Secondary DNS:
  Default WAN Link (Gateway/DNS): WAN1
  ==== ========= =============== =============== ====== ==================
  Port Interface IP Address      Netmask         Status Type
  ---- --------- --------------- --------------- ------ ------------------
    1     WAN1   61.2.1.1        255.255.255.248  DOWN  (Static IP)
    2     WAN2                                    DOWN  (Not initialized)
    3     DMZ1   10.1.1.254      255.255.255.0    DOWN
    4     LAN1   192.168.40.254  255.255.255.0    DOWN
    5     LAN2   192.168.2.254   255.255.255.0     UP
  ==== ========= =============== =============== ====== ==================

 5:43PM  up  8:19, 1 user, load averages: 0.35, 0.30, 0.25
MH-5000#
```

29.3 Steps for Firmware upgrade from Web GUI

Step 4. Download the newest firmware from web site If a new firmware issued, we can download it from the web site (planet.com.tw/download.php) to the local computer.	Firmware upgrade site： http://www.planet.com.tw/download.php

2. **Upgrade firmware** In the System Tools / Firmware Upgrade page. Select the path of firmware through `Browse` button, and check the `Preserve Saved Configurations` to reserve original settings. Click the `Upload` button to upgrade firmware.	**SYSTEM TOOLS > Firmware Upgrade > Firmware Upgrade**  Firmware Upgrade Caution!! Upgrading firmware with browser takes at least 2 minute and may fail occasionally due to users' interrupt. We suggest firmware upgrade with the CLI command 'ip tftp upgrade image FILENAME X.X.X.X' to a TFTP server. To upgrade the internal system firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD. Download BIN files from http://www.planet.com.tw/download.php. In some cases, you may need to reconfigure the system after upgrading. File Path: D:\Planet Device\MH-500C 瀏覽... ☑ Preserve Saved Configurations Upload

29.4 Steps for Database Update from Web GUI

Step 1. Update database manually If a new firmware issued, we can download it by clicking the `Update` button. Then we will see the database version shown on the left side.	 Update Status : URL database : v1.50123 [2005/01/24 20:44] Update IDS signatures: v1.50124 [2005/01/24 20:44] Update Virus pattern: v1.50124 [2005/01/24 20:44] Update Auto Update : Update Center mh-update.planet.com.tw Update Schedule On Sunday 0 0 Auto URL update ☑ Auto IDS update ☑ Auto AntiVirus update ☑ Apply
Step 2. Auto Update We can also update database automatically. Fill the database server's IP address in the `Update Center` field. Choose what date/time we would like to update the database, and then check which databases we would like to update. Click `Apply` button to finish the settings.	**SYSTEM TOOLS > Firmware Upgrade > Firmware Upgrade**  Update Status : URL database : v1.50123 [2005/01/24 20:44] Update IDS signatures: v1.50124 [2005/01/24 20:44] Update Virus pattern: v1.50124 [2005/01/24 20:44] Update Auto Update : Update Center mh-update.planet.com.tw Update Schedule On Sunday 0 0 Auto URL update ☑ Auto IDS update ☑ Auto AntiVirus update ☑ Apply

29.5 Steps for Factory Reset

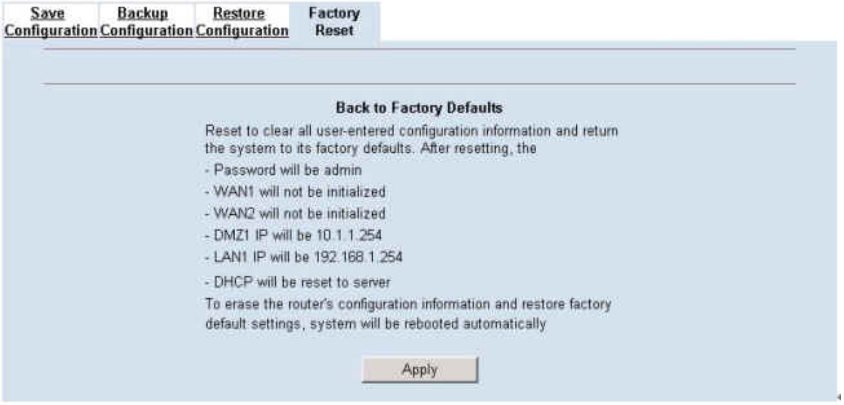
29.5.1 Step for factory reset under web GUI

Step 1. Factory reset

In the Web GUI mode. Follow the path of right side. We can make MH-5001 configuration restored to the factory defaults with simply clicking the `Apply` button.

Warning: Be careful to use this function. It will make all your present configurations disappear. And the configuration will restore to the factory default.

SYSTEM TOOLS > System Utilities > Factory Reset



Back to Factory Defaults

Reset to clear all user-entered configuration information and return the system to its factory defaults. After resetting, the

- Password will be admin
- WAN1 will not be initialized
- WAN2 will not be initialized
- DMZ1 IP will be 10.1.1.254
- LAN1 IP will be 192.168.1.254
- DHCP will be reset to server

To erase the router's configuration information and restore factory default settings, system will be rebooted automatically

29.5.2 Step for NORMAL factory reset

Step 1. Factory reset

In the CLI mode. Enter `sys resetconf now` to reset the firmware to factory default. Then the system will reboot automatically.

```
NetOS/i386 (MH-5001) (tty00)

login: admin
Password:
Welcome to MH-5001 Multi-Homing Security Gateway


MH-5001> en
MH-5001# sys resetconf now
Resetting Configuration to default... DONE
System will reboot now
syncing disks... done
rebooting...
```

29.5.3 Steps for EMERGENT factory reset

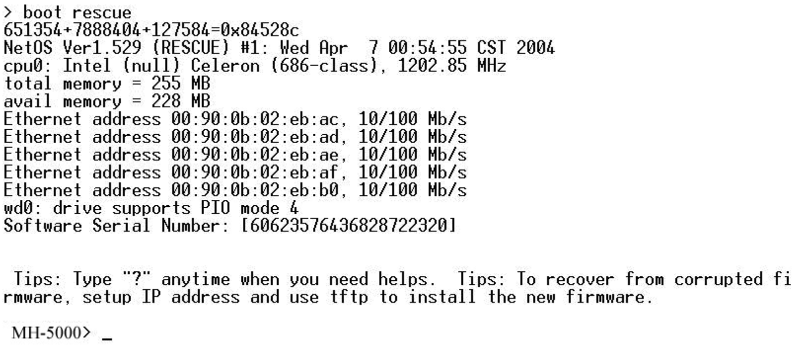
Step 1. Enter the boot loader

If the original firmware is damaged, you may need to recover the firmware with the factory default. Press <tab> or <space> during the 2-second countdown process.

```
>> NetOS Loader (i386), V1.5 (Fri Feb 20 10:25:11 CST 2004)
Press <TAB> to prompt - starting in 0
Type "boot rescue" to load safe-mode kernel to
(1) rescue corrupted firmware
(2) reset password for admin
type "?" or "help" for help.
>
```

Step 2. Enter the Safe Mode

Enter `boot rescue` to enter the emergency kernel. In this kernel, you can use tftp to fetch another firmware to install, or reset the configuration to default even though you lost the password.



```
> boot rescue
651354+7888404+127584=0x84528c
NetOS Ver1.529 (RESCUE) #1: Wed Apr  7 00:54:55 CST 2004
cpu0: Intel (null) Celeron (686-class), 1202.85 MHz
total memory = 255 MB
avail memory = 228 MB
Ethernet address 00:90:0b:02:eb:ac, 10/100 Mb/s
Ethernet address 00:90:0b:02:eb:ad, 10/100 Mb/s
Ethernet address 00:90:0b:02:eb:ae, 10/100 Mb/s
Ethernet address 00:90:0b:02:eb:af, 10/100 Mb/s
Ethernet address 00:90:0b:02:eb:b0, 10/100 Mb/s
wd0: drive supports PIO mode 4
Software Serial Number: [60623576436828722320]


 Tips: Type "?" anytime when you need helps.  Tips: To recover from corrupted fi
rmware, setup IP address and use tftp to install the new firmware.

 MH-5000> _
```

Step 3. Factory reset

Enter `sys resetconf now` to reset the firmware to factory default. Then system will reboot automatically.

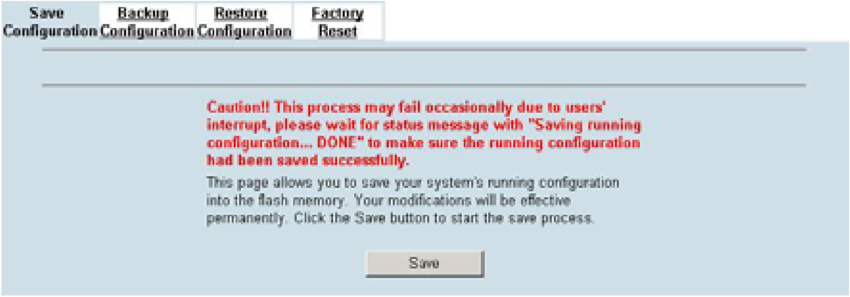
```
MH-5001> en
MH-5001# sys resetconf now
System will reboot now
syncing disks... done
rebooting...
```

29.6 Save the current configuration

Step 1. Backup the current configuration

After finishing the settings of MH-5001, be sure to Press the `Save` button in this page to keep the running configuration.

SYSTEM TOOLS > System Utilities > Save Configuration



Caution!! This process may fail occasionally due to users' interrupt, please wait for status message with "Saving running configuration... DONE" to make sure the running configuration had been saved successfully.

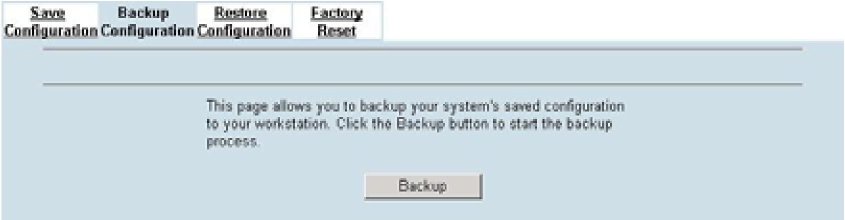
This page allows you to save your system's running configuration into the flash memory. Your modifications will be effective permanently. Click the Save button to start the save process.

29.7 Steps for Backup / Restore Configurations

Step 1. Backup the current configuration

Before backup your current configuration, make sure you have saved your current configurations as described in Section 29.6. Then select page in the page of /System Tools /System Utilities /Backup Configurations, click `Backup` button to backup configuration file to local disk.

SYSTEM TOOLS > System Utilities > Backup Configuration

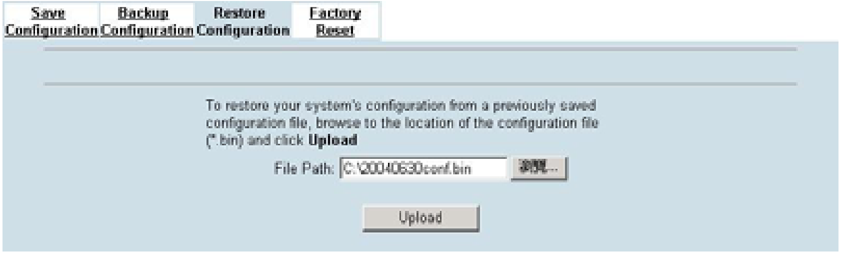


This page allows you to backup your system's saved configuration to your workstation. Click the Backup button to start the backup process.

Step 2. Restore the previous saving configuration

In the page of System Tools / System Utilities / Restore Configuration, click the `Browse` button to select configuration file path first, and then click `Upload` button to restore configuration.

SYSTEM TOOLS > System Utilities > Restore Configuration

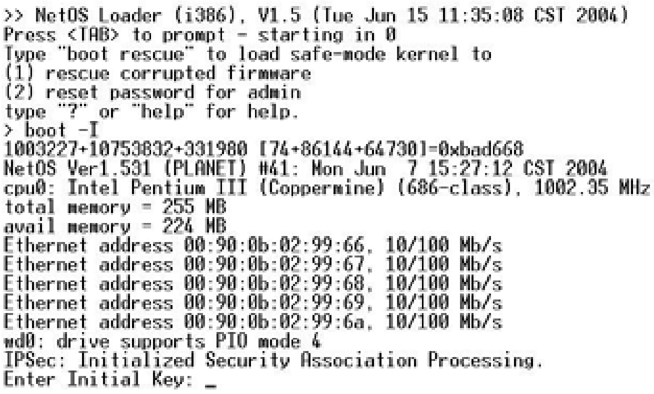


To restore your system's configuration from a previously saved configuration file, browse to the location of the configuration file (*.bin) and click **Upload**

File Path: C:\20040630conf.bin

29.8 Steps for Reset password

Step 1. Enter the boot loader
If you forget the password, you can use the following way to reset the password. Press `<tab>` or `<space>` during the 2-second countdown process.
	`>> NetOS Loader (i386), V1.5 (Fri Feb 20 10:25:11 CST 2004)`
	`Press <TAB> to prompt - starting in 0`
	`Type "boot rescue" to load safe-mode kernel to`
	`(1) rescue corrupted firmware`
	`(2) reset password for admin`
	`type "?" or "help" for help.`
	`>`

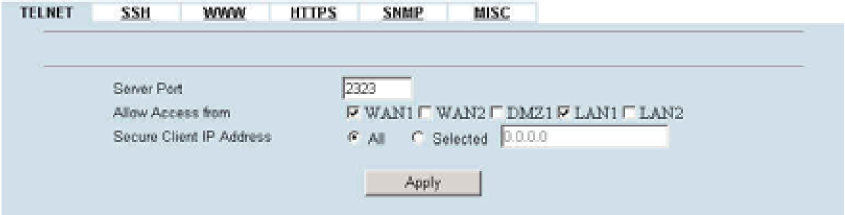
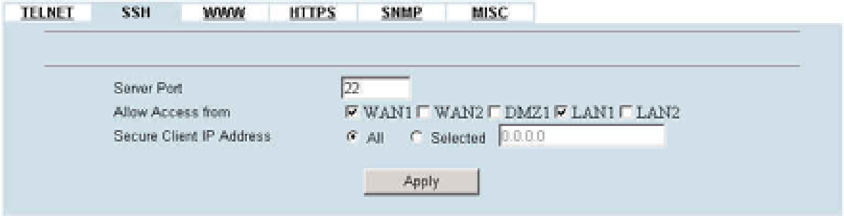
Step 2. Get the Initial Key
Enter `boot -I` command as right side. When screen shows "Enter Initial Key", you can consult with your local technical supporter to get the Initial Key. You will need to tell the local technical supporter **`all the MAC address`** value. Then you will get the Initial Key. To reset admin password.
	
	`>> NetOS Loader (i386), V1.5 (Tue Jun 15 11:35:08 CST 2004)`
	`Press <TAB> to prompt - starting in 0`
	`Type "boot rescue" to load safe-mode kernel to`
	`(1) rescue corrupted firmware`
	`(2) reset password for admin`
	`type "?" or "help" for help.`
	`> boot -I`
	`1003227+10753832+331980 [74+86144+64730]=0xbad668`
	`NetOS Ver1.531 (PLANET) #41: Mon Jun  7 15:27:12 CST 2004`
	`cpu0: Intel Pentium III (Coppermine) (686-class), 1002.35 MHz`
	`total memory = 255 MB`
	`avail memory = 224 MB`
	`Ethernet address 00:90:0b:02:99:66, 10/100 Mb/s`
	`Ethernet address 00:90:0b:02:99:67, 10/100 Mb/s`
	`Ethernet address 00:90:0b:02:99:68, 10/100 Mb/s`
	`Ethernet address 00:90:0b:02:99:69, 10/100 Mb/s`
	`Ethernet address 00:90:0b:02:99:6a, 10/100 Mb/s`
	`wd0: drive supports PIO mode 4`
	`IPSec: Initialized Security Association Processing.`
	`Enter Initial Key: _`

Appendix A
Command Line Interface (CLI)

You can configure the MH-5001 through the web interface (http/https) for the most time. Besides you can use another method, console/ssh/telnet method to configure the MH-5001 in the emergency. This is known as the Command Line Interface (CLI). By the way of CLI commands, you can effectively set the IP addresses, restore factory reset, reboot/shutdown system etc. Here we will give you a complete list to configure the MH-5001 using the CLI commands.

A.1 Enable the port of MH-5001

If you prefer to use CLI commands, you can use it through console/ssh/telnet methods. For using ssh/telnet feature, you must enable the remote management first. Enable the specified port, so that you can login from the configured port.

Step 1. Enable remote management / TELNET Check the selected port located in the telnet function. And customize the server port which is listened by telnet service.	**SYSTEM Tools > Remote Mgt. > TELNET**  TELNET SSH WWW HTTPS SNMP MISC Server Port 2323 Allow Access from ☑ WAN1 □ WAN2 □ DMZ1 ☑ LAN1 □ LAN2 Secure Client IP Address ● All ○ Selected 0.0.0.0 Apply
Step 2. Enable remote management / SSH Check the selected port located in the ssh function. And customize the server port which is listened by ssh service.	**SYSTEM Tools > Remote Mgt. > SSH**  TELNET SSH WWW HTTPS SNMP MISC Server Port 22 Allow Access from ☑ WAN1 □ WAN2 □ DMZ1 ☑ LAN1 □ LAN2 Secure Client IP Address ● All ○ Selected 0.0.0.0 Apply

A.2 CLI commands list (Normal Mode)

Subsequently, we can use the console/ssh/telnet to connect the MH-5001. After logining the system successfully, we can use the CLI commands to configure MH-5001. The complete CLI commands are described as follows.

Non-privileged mode

Main commands	Sub commands	Example	Command description
?		?	Show the help menu
enable (en)		enable	Turn on privileged mode command
exit (ex)		exit	Exit command shell
ip			Configure IP related settings
	ping	ip ping 202.11.22.33	Send ICMP echo request messages
	traceroute	ip traceroute 202.11.22.33	Trace route to destination address or hostname
sys			Configure system parameters

	status (st)	sys status	Show system and network status
	version (ver)	sys version	Show MH-5001 firmware version

Table A-1 Non-privileged mode of normal mode

Note: If you don't know what parameter is followed by the commands, just type "?" following the command. Ex "ip ?". It will show all the valid suffix parameters from "ip".

Privileged mode

Main commands	Sub commands	Example	Command description
?		?	Show the help menu
disable (dis)		disable	Turn off privileged mode command
exit (ex)		exit	Exit command shell
ip			Configure IP related settings
	arp	ip arp status	Show the IP/MAC mapping table
	dns	ip dns query www.yam.com.tw	Show the IP address of the www.yam.com.tw.
	ifconfig	ip ifconfig INTF1 192.168.1.100 255.255.255.0	Configure the IP address of each port
	ping	ip ping 202.11.22.33	Send ICMP echo request messages
	tftp upgrade/backup	ip tftp upgrade image <FILENAME> 192.168.1.170.	Upgrade/Backup firmware/configuration from/to tftp server. About the full description, please refer to Section A-3.
	traceroute	ip traceroute 202.11.22.33	Trace route to destination address or hostname.
sys			Configure system parameters
	halt	sys halt now	Shutdown system
	password	sys password	Change administrator password
	reboot	sys reboot now	Reboot system
	resetconf	sys resetconf now	Reset system configuration to default settings
	saveconf (sa)	sys saveconf	Save running configuration
	status (st)	sys status	Show system and network status
	tcpdump (tc)	sys tcpdump INTF0 host 10.1.1.1	Capture the information of specified packets which pass through the indicated interface.
	version (ver)	sys version	Show MH-5001 firmware version

Table A-2 Privileged mode of normal mode

The Full tftp commands are described in the following Table A-3.

Prefix command	2th command	3th command	Postfix command	Example	Command description
ip tftp	upgrade	config	FILENAME WORD	ip tftp upgrade config conf-0101 192.168.1.170	Upgrade configuration file image from tftp server.
		image	FILENAME WORD (preserve)	ip tftp upgrade image <FILENAME> 192.168.1.170 preserve	Upgrade system image from tftp server.
	backup	config	WORD	ip tftp backup config 192.168.1.170	Backup configuration file image to tftp server.
		image	WORD	ip tftp backup image 192.168.1.170	Backup system image to tftp server.

Table A-3 IP tftp commands description

In the Postfix command, the meanings of keywords are listed here.

WORD: tftp server IP address

FILENAME: Upgrade configuration file image name

(preserve): string “preserve”, this is optional

A.3 CLI commands list (Rescue Mode)

If the original firmware was damaged by some accidents, you may need to recover it with the factory reset process in the rescue mode. Boot the MH-5001 and press <tab> or <space> during the 2-second countdown process. You may refer Section 29.5.3 for details.

Non-privileged mode

Main commands	Sub commands	Example	Command description
?		?	Show the help menu
enable (en)		enable	Turn on privileged mode command
exit (ex)		exit	Exit command shell
ip			Configure IP related settings
	ping	ip ping 202.11.22.33	Send ICMP messages
sys			Configure system parameters
	status (st)	sys status	Show the mode name and firmware version.
	version (ver)	sys version	Show the firmware version

Table A-4 Non-privileged mode of rescue mode

Note: If you don’t know what parameter is followed by the commands, just type “?” following the command. Ex “ip ?”. It will show all the valid suffix parameters from “ip”.

Privileged mode

Main commands	Sub commands	Example	Command description
?		?	Show the help menu
disable (dis)		disable	Turn off privileged mode command
exit (ex)		exit	Exit command shell
ip			Configure IP related settings
	arp	ip arp status	Show the ip/MAC mapping table
	dns	ip dns query www.yam.com.tw	Show the IP address of the www.yam.com.tw.
	ifconfig	ip ifconfig INTF1 192.168.1.100 255.255.255.0	Configure the ip address of each port
	ping	ip ping 202.11.22.33	Send ICMP echo request messages
	tftp	ip tftp upgrade image <FILENAME> 192.168.1.170.	Upgrade firmware from tftp server.
sys			Configure system parameters
	halt	sys halt now	Shutdown system
	reboot	sys reboot now	Reboot system
	resetconf	sys resetconf now	Reset system configuration to default settings
	status (st)	sys status	Show the mode name and firmware version.
	version (ver)	sys version	Show the firmware version

Table A-5 Privileged mode CLI commands

Appendix B
Trouble Shooting

1. If the power LED of MH-5001 is off when I turn on the power?

Ans：Check the connection between the power adapter and MH-5001 power cord. If this problem still exists, contact with your sales vendor.

2. How can I configure the MH-5001 if I forget the admin password of the MH-5001？

Ans：You can gather all the MAC addresses values of MH-5001, and contact the local technical supporter. Then we will give you an initial key. Please refer to the Section 29.8 described to reset the admin password.

3. I can't access MH-5001 via the console port？

Ans：Check the console line and make sure it is connected between your computer serial port and MH-5001 Diagnostic RS-232 port. Notice whether the terminal software parameter setting as follows. No parity, 8 data bits, 1 stop bit, baud rate 9600 bps. The terminal type is VT100.

4. I can't ping MH-5001 WAN1 interface successfully？ Why？

Ans：Follow below items to check if ready or not

a. Check Basic Setup > WAN Settings > WAN1 status fields. Verify whether any data is correctly.

b. Check Device Status > System Status > Network Status WAN1 status is "UP". If the status is "DOWN", check if the network line is connectionless？

c. Check System Tools > Remote Mgt. > MISC > WAN1. Verify if WAN1 port checkbox is enabled. The default enabled port is only LAN port.

d. Check whether virtual server rule (Dest. IP : WAN1 IP address, port : 1~65535) exists or not. If existing any virtual server rule like this type, it will make all the connections from WAN1 port outside relay to another server. Actually what you have pinged is another server, not MH-5001.

e. Check whether NAT One-to-One(bidirectional) rule (Translated Src IP : WAN1 IP address, port : 1~65535) exists or not. If existing any virtual server rule like this type, it will make all the connections from WAN1 port outside relay to another server. Actually what you have pinged is another server, not MH-5001.

f. If all the above items have checked, try to change a new network line. This is almost resulting from the network line problem. Please neglect the LED status, because it will confuse your judgment sometimes.

5. I have already set the WAN1 ip address of MH-5001 the same subnet with my pc, but I can't use https to login MH-5001 via WAN1 port from my pc all the time, why？

Ans：

a. Be sure that you can ping the WAN1 port, please check the procedure as question 4 description.

b. Make sure that the WAN1 IP address of MH-5001 is not duplicated with other existed IP address. You can take off the network line connected on the WAN1 port. Then try to ping the IP address which setup on the WAN1 port. If it is still successful, the IP address which setup on the WAN1 port is duplicated with the existent IP address.

c. Notice that you must check System Tools > Remote Mgt. > HTTPS > WAN1. The default enabled port is only LAN port.

6. I can't build the VPN – IPSec connection with another device at the another side all the time, why？

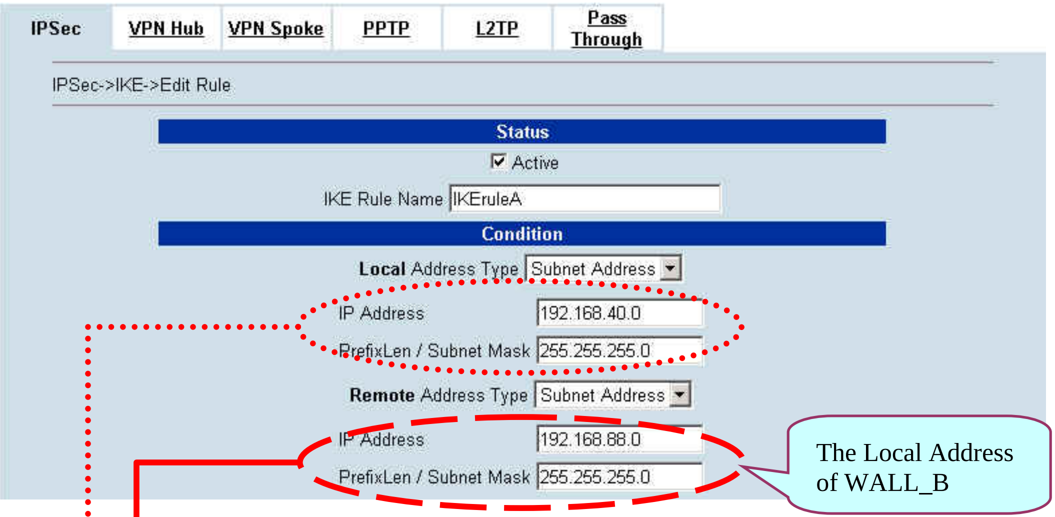
Ans：Please make sure if you follow the setting method as follows.

a. Check your IPSec Setting. Please refer to the settings in the Section 13.4- Step 3.

b. Make sure if you have already added a WAN to LAN policy in the Advanced Settings/Firewall to let the IPSec packets pass through the MH-5001. (The default value from WAN to LAN is block.).

When you add a Firewall rule, the `Source IP and Netmask` are the `IP address, PrefixLen/Subnet Mask` in the pages of the Remote Address Type. And the `Dest IP and Netmask` are the `IP Address, PrefixLen/Subnet Mask` in the pages of the Local Address Type.

The following Figure B-1, Figure B-2 indicated the WALL_A IPSec and Firewall setting. The Figure B-3, Figure B-4 indicated the opposite side WALL_B IPSec and Firewall setting. When you configure an IPSec policy, please be sure to add a rule to let the packets of the IPSec pass from WAN to LAN. For the IP address of firewall rules, please refer to the Figure B-2, Figure B-4.



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: IKEruleA

Condition

Local Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

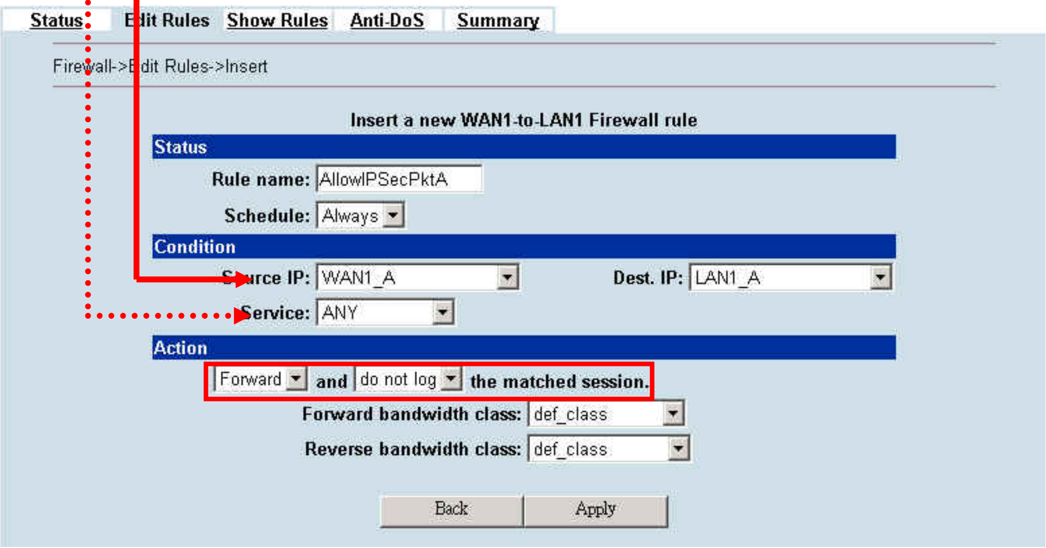
Remote Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

The Local Address of WALL_B

Figure B-1 WALL_A - Inset a new IPSec policy



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowIPSecPktA

Schedule: Always

Condition

Source IP: WAN1_A **Dest. IP:** LAN1_A

Service: ANY

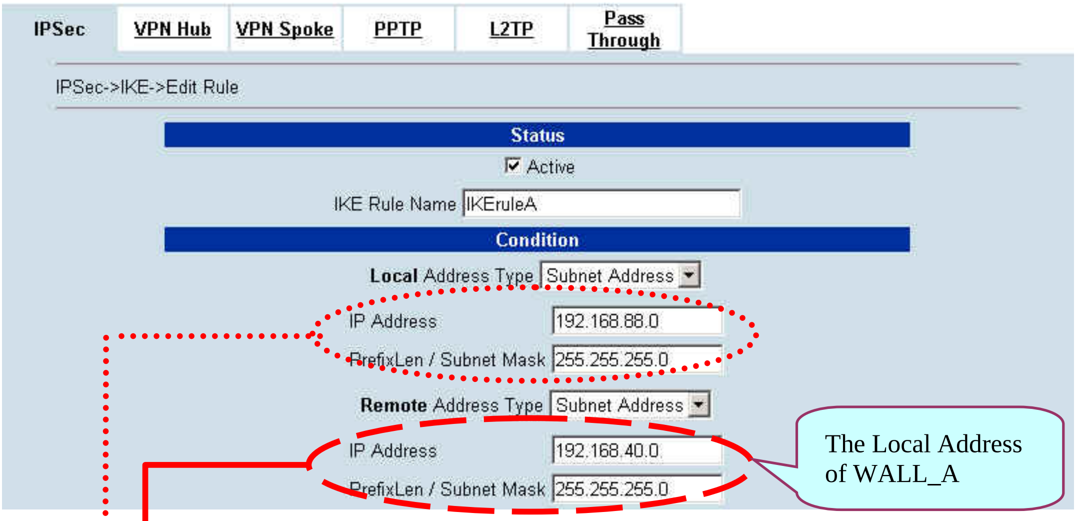
Action

Forward **and** do not log **the matched session.**

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Figure B-2 WALL_A - Insert a new firewall rule in WAN to LAN



IPSec->IKE->Edit Rule

Status

☑ Active

IKE Rule Name: IKEruleA

Condition

Local Address Type: Subnet Address

IP Address: 192.168.88.0

PrefixLen / Subnet Mask: 255.255.255.0

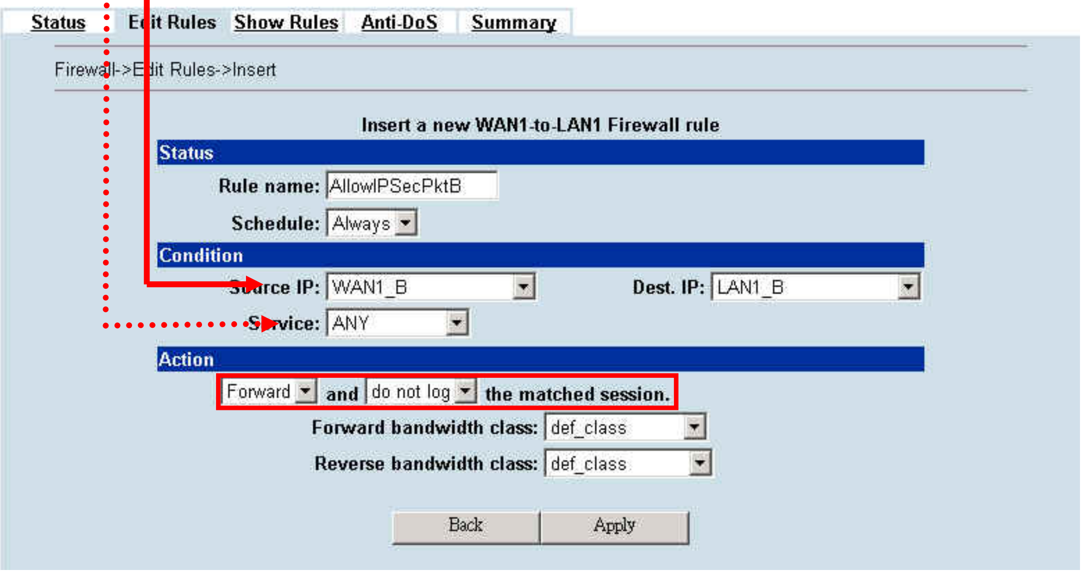
Remote Address Type: Subnet Address

IP Address: 192.168.40.0

PrefixLen / Subnet Mask: 255.255.255.0

The Local Address of WALL_A

Figure B-3 WALL_B - Inset a new IPSec policy



Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowIPSecPktB

Schedule: Always

Condition

Source IP: WAN1_B Dest. IP: LAN1_B

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Figure B-4 WALL_B - Insert a new firewall rule in WAN to LAN

7. Why the Source-IP field of System Logs is blank?

Ans：One reason is that you may enter Host Name and following by a space like “MH-5001 “. And enter the Domain Name string like “planet.com.tw” in the firmware version 1.391B. Then the System Name will present as “MH-5001 .planet.com.tw”. After upgrading firmware to upper version (ex. 1.50R). It will appear blank in the Source-IP field of System Logs.

8. When I ping the Internet host from LAN/DMZ. I can’t always finish the ping successfully. Sometimes it is work. But sometimes it fails to ping the outside host.

Ans：This may cause there are more than one host in the LAN/DMZ pinging the same host at the same time. If one host (Lan-A) is pinging Internet host A(ex. 140.106.100.1), and at the same time, Lan-B is also pinging 140.106.100.1. Then the pinging action of the Lan-A and Lan-B may fail. But when each host (Lan-A or Lan-B) is finish pinging, the other host can continue the pinging action.

9. While I am upgrading firmware from local disk, the download is not complete but the network has been disconnected. What will it happen in such situation?

Ans：Under this circumstance, the MH-5001 will automatically reboot and all configurations will still remain as before.

10. While I am upgrading firmware from local disk, the download is complete. After md5 checks, the screen appears "Upgrading kernel image". What will it happen if the power is off suddenly?

Ans：Almost all the cases will not cause firmware fail. The MH-5001 will automatically reboot and all configurations will still remain as before. But sometimes it will make firmware fail. If the firmware fails, MH-5001 will automatically enter rescue mode when it reboots. You may need to do the factory reset, and then restore your original configuration to MH-5001. Refer to the factory reset procedure of MH-5001 as Section 29.5. About restoring configuration procedure, please refer to Section 29.7.

11. While finishing the Content Filters > Web Filter settings, if I try to use browser to test, why does not the web page result match with the web filter configuration?

Ans：Be sure that you have cleaned all the file cache in the browser, and try to connect the Internet web server. If the web page result still does not match with the web filter configuration, you may close your browser and reopen it.

12. While finishing the edition of MH-5001 settings and pressing apply button, the LAN/DMZ to WAN network connection (telnet, ssh, ftp, msn..) fails, why?

Ans：This is a normal situation. When you finish the following settings, all the active network connection will be disconnected. So, you must reconnect it again.

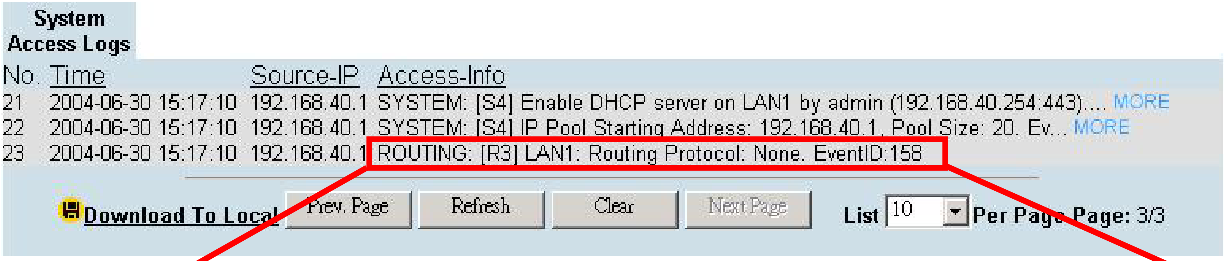
a. SYSTEM TOOLS > Remote Mgt.
b. ADVANCED SETTINGS > VPN Settings > IPSec
c. ADVANCED SETTINGS > VPN Settings > PPTP > Client
d. ADVANCED SETTINGS > VPN Settings > Pass Through
e. ADVANCED SETTINGS > NAT

Appendix C
System Log Syntax

In the MH-5001, all the administration action will be logged by the system. You can refer all your management process through System log (DEVICE STATUS > System Logs > System Access Logs). Besides, all the system log descriptions are following the same syntax format.

In the below diagram, you can view the example of system log. The amplified system log example can be divided into 4 parts. The first part is **Component type**, second part is **Log ID**, third part is **log description** and final part is **Event ID**. When you applied each setting in the MH-5001, you had been issued an Event. So the same `Event ID` may have many different Log IDs because you may change different settings in the same apply action. The `Event ID` is a sequence number. It means that the same `Log ID` would not be assigned the same `Event ID` every time.

So if you apply any button while setting MH-5001 every time, an "Event" will occur immediately. And the "Event" will be displayed in the System log.



```
No. Time                 Source-IP     Access-Info
21  2004-06-30 15:17:10  192.168.40.1  SYSTEM: [S4] Enable DHCP server on LAN1 by admin (192.168.40.254:443).... MORE
22  2004-06-30 15:17:10  192.168.40.1  SYSTEM: [S4] IP Pool Starting Address: 192.168.40.1, Pool Size: 20. Ev... MORE
23  2004-06-30 15:17:10  192.168.40.1  ROUTING: [R3] LAN1: Routing Protocol: None. EventID:158
```

Figure D-1 All the system log descriptions are following the same format as above

ROUTING	: [R3]	LAN1: Routing Protocol: None.	EventID: 158
Component type	: Log ID	: Log Description	: Event ID

In the following table, we list all the system logs for reference.

Component type	Log ID	Log description	Example
AUTH	A01	User Login	AUTH: [A01] admin login success (192.168.17.102:443).
			AUTH: [A01] admin login fail, miss password (192.168.17.102:443).
			AUTH: [A01] admin login fail, configuration is locked by administrator from Console (192.168.17.102:443).
			AUTH: [A01] admin login fail, configuration is locked by another user from 192.168.17.100 (192.168.17.102:443).
	A02	User Logout	AUTH: [A02] admin logout (192.168.17.102:443).
	A03	Change Password	AUTH: [A03] admin change system password (192.168.17.102:443).
BANDWIDTH	B01	Enable/Disable Bandwidth Management	BANDWIDTH: [B01] Enable bandwidth management by admin (192.168.17.100:443).
			BANDWIDTH: [B01] Disable bandwidth management by admin (192.168.17.100:443).

			BANDWIDTH: [B01] WAN1 Disable bandwidth management with PPPoE connection.
CONTENT	C01	Web filter categories configuration updated	CONTENT: [C01] Web filter categories configuration update by admin (192.168.17.100:443). EID=6
	C02	Web filter added trusted host	CONTENT: [C02] Web filter add trusted host by admin (192.168.17.100:443). EID=6
	C03	Web filter deleted trust host	CONTENT: [C03] Web filter deleted trust host by admin (192.168.17.100:443). EID=6
	C04	Web filter added forbidden domain	CONTENT: [C04] Web filter added forbidden domain by admin (192.168.17.100:443). EID=7
	C05	Web filter deleted forbidden domain	CONTENT: [C05] Web filter deleted forbidden domain by admin (192.168.17.100:443). EID=8
	C06	Enable web-filter access control	CONTENT: [C06] Enable web-filter access by admin (192.168.17.100:443). EID=9
	C07	Disable web-filter access control	CONTENT: [C07] Disable web-filter access control by admin (192.168.17.100:443). EID=10
	C08	Web filter URL keyword added	CONTENT: [C08] Web filter URL keyword added by adimin (192.168.17.100:443). EID=11
	C09	Web filter URL keyword deleted	CONTENT: [C09] Web filter URL keyword deleted by admin (192.168.17.100:443). EID=12
	C10	Enable web filter url matching	CONTENT: [C10] Enable web filter url matching by admin (192.168.17.100:443). EID=13
	C11	Disable web filter url matching	CONTENT: [C11] Disable web filter url matching by admin (192.168.17.100:443). EID=14
	C12	Updated web filter exempt zone configuration	CONTENT: [C12] Updated web filter exempt zone configuration by admin (192.168.17.100:443). EID=15
	C13	Web filter exempt zone added range	CONTENT: [C13] web filter exempt zone added range from 140.126.1.1 to 140.126.100.255 by admin (192.168.17.100:443). EID=16
	C14	Updated ftp filter exempt zone configuration	CONTENT: [C14] Updated ftp filter exempt zone configuration by admin (192.168.17.100:443). EID=17
	C15	FTP filter exempt zone added range	CONTENT: [C15] FTP filter exempt zone added range from 140.126.1.1 to 140.126.255.255 by admin (192.168.17.100:443). EID=18
	C16	Updated ftp filter blocked file configuration	CONTENT: [C16] Updated ftp filter blocked file configuration by admin (192.168.17.100:443). EID=19
	C17	FTP Filter blocking list updated	CONTENT: [C17] FTP Filter blocking list updated by admin (192.168.17.100:443). EID=20
	C18	Web filter keyword added	CONTENT: [C18] Web filter keyword added by admin (192.168.17.100:443). EID=21
	C19	Web filter keyword deleted	CONTENT: [C19] Web filter keyword deleted by admin (192.168.17.100:443). EID=22
	C20	Enable web filter keyword matching	CONTENT: [C20] Enable web filter keyword matching by admin (192.168.17.100:443). EID=23
	C21	Disable web filter keyword matching	CONTENT: [C21] Disable web filter keyword matching by admin (192.168.17.100:443). EID=24

	C22	Updated POP3 filter exempt zone configuration	CONTENT: [C22] Updated POP3 filter exempt zone configuration by admin (192.168.17.100:443). EID=25
	C23	POP3 filter exempt zone added range	CONTENT: [C23] POP3 filter exempt zone added range from 140.126.1.1 to 140.126.1.255 by admin (192.168.17.100:443). EID=26
	C24	Enable POP3 filter	CONTENT: [C24] Enable POP3 filter by admin (192.168.17.100:443). EID=27
	C25	Disable POP3 filter	CONTENT: [C25] Disable POP3 filter by admin (192.168.17.100:443). EID=28
	C26	POP3 Filter blocking list updated	CONTENT: [C26] POP3 Filter blocking list updated by admin (192.168.17.100:443). EID=29
	C27	Updated SMTP exempt zone configuration	CONTENT: [C27] Updated SMTP exempt zone configuration by admin (192.168.17.100:443). EID=30
	C28	SMTP filter exempt zone added range from	CONTENT: [C28] SMTP filter exempt zone added range from by admin (192.168.17.100:443). EID=31
	C29	Enable SMTP filter	CONTENT: [C29] Enable SMTP filter by admin (192.168.17.100:443). EID=32
	C30	Disable SMTP filter	CONTENT: [C30] Disable SMTP filter by admin (192.168.17.100:443). EID=33
	C31	SMTP Filter blocking list updated	CONTENT: [C31] SMTP Filter blocking list updated by admin (192.168.17.100:443). EID=34
	C32	Enable SMTP AntiVirus	CONTENT: [C32] Enable SMTP AntiVirus by admin (192.168.17.100:443). EID=35
	C33	Disable SMTP AntiVirus	CONTENT: [C33] Disable SMTP AntiVirus by admin (192.168.17.100:443). EID=36
	C34	AntiVirus module cannot download signatures	CONTENT: [C34] AntiVirus: cannot download signatures by admin (192.168.17.100:443). EID=37
	C35	AntiVirus signatures updated	CONETNT: [C35] AntiVirus signatures updated by admin (192.168.17.100:443). EID=38
	C36	Enable WEB filter	CONTENT: [C36] Enable WEB filter by admin (192.168.17.100:443). EID=39
	C37	Disable WEB filter	CONTENT: [C37] Disable WEB filter by admin (192.168.17.100:443). EID=40
FIREWALL	F01	Enable/Disable Firewall	FIREWALL: [F01] Activated firewall by admin (192.168.17.102:443). FIREWALL: [F01] Deactivated firewall by admin (192.168.17.102:443).
	F02	Edit Firewall Rules	
	F03	Attack Alert Setup	FIREWALL: [F03] Enable Alert when attack detected by admin (192.168.17.102:443). FIREWALL: [F03] Disable Alert when attack detected by admin (192.168.17.102:443).
	F04	Reload Firewall Rules	FIREWALL: [F04] WAN1 Reload all NAT/Firewall rules for new WAN IP
LOG	L01	Logfile is Full	LOG: [L01] logfile is full.

	L02	Mail Log	LOG: [L02] mail logfile to tom@hotmail.com.
	L03	Remote Syslog Server offline	
	L04	Enable/Disable Syslog Forward to Remote Syslog Server	LOG: [L04] Enable syslog server at 192.168.17.100 by admin (192.168.17.102:443). LOG: [L04] Disable syslog server by admin (192.168.17.102:443).
	L05	Enable/Disable Mail Log	LOG: [L05] Enable mail logs to tom@hotmail.com by admin (192.168.17.102:443). LOG: [L05] Disable mail logs by admin (192.168.17.102:443).
	L06	Send Mail Log	LOG: [L06] mail logfile to tom@hotmail.com
	L07	Log Cleanup	LOG: [L07] logfile is cleanup.
	L08	Mail Log Configuration Update	LOG: [L08] Mail configuration updated by admin (192.168.17.102:443).
	L09	Log Half-Clean	LOG: [L09] logfile half-clean.
NAT	N01	Set NAT Mode	NAT: [N01] Disable WAN NAT feature.
	N02	NAT Rules	NAT: [N02]
	N03	Virtual Server	
ROUTING	R01	Static Route	
	R02	Policy Route	
	R03	Changing Routing Protocol	ROUTING: [R03]
		OSPF Area ID	ROUTING: [R3] WAN1: OSPF Area ID = 15. EventID:15
		Routing Protocol: OSPF	ROUTING: [R3] WAN1: Routing Protocol: OSPF. EventID:15
		Routing Protocol: RIPv2/In+Out	ROUTING: [R3] WAN1: Routing Protocol: RIPv2/In+Out. EventID:15
		Routing Protocol: RIPv1/In+Out	ROUTING: [R3] WAN1: Routing Protocol: RIPv1/In+Out. EventID:15
		Routing Protocol: RIPv2/In	ROTUING: [R3] WAN1: Routing Protocol: RIPv2/In. EventID:15
		Routing Protocol: RIPv1/In	ROUTING: [R3] WAN1: Routing Protocol: RIPv1/In. EventID:15
		Routing Protocol: None	ROUTING: [R3] WAN1: Routing Protocol: None. EventID:15
SYSTEM	S01	Wall Startup	SYSTEM: [S01] Wall Startup.
	S02	Wall Shutdown	SYSTEM: [S02] Wall Shutdown.
	S03	Interface Configuration	SYSTEM: [S03] WAN1: IP Address Assignment = Get IP Automatically by admin (192.168.17.102:443). SYSTEM: [S03] WAN1: IP Address Assignment = Fixed IP Address by admin (192.168.17.102:443). SYSTEM: [S03] WAN1: Got PPPoE IP Address F63/255.255.255.0.
	S04	Startup/Shutdown DHCP Server	SYSTEM: [S04] Enable DHCP server on LAN1 by admin (192.168.17.102:443) SYSTEM: [S04] Disable DHCP server on LAN1.

	S05	Startup/Shutdown HTTP Server	SYSTEM: [S05] HTTP started. SYSTEM: [S05] HTTP stopped.
	S06	Startup/Shutdown HTTPS Server	SYSTEM: [S06] HTTPS started.
	S07	Startup TELNET Server	
	S08	Set Interface IP Address	SYSTEM: [S08] WAN1: IP Address: 192.168.17.102/255.255.255.0. (192.168.17.102:443).
	S09	IP Alias	SYSTEM: [S09] LAN1: Add IP address alias 192.168.1.2/255.255.255.0 by admin (192.168.17.102:443). SYSTEM: [S09] LAN1: Delete IP address alias 192.168.1.2/255.255.255.0 by admin (192.168.17.102:443). SYSTEM: [S09] LAN1: Change IP address alias 192.168.1.2/255.255.255.0 to 192.168.1.3/255.255.255.0 by admin (192.168.17.102:443).
	S10	Set Host Name	SYSTEM: [S10] HostName:MH-5001, set by admin (192.168.17.102:443).
	S11	Set Domain Name	SYSTEM: [S11] Domain Name: planet.com.tw, set by admin (192.168.17.102:443).
	S12	Enable/Disable DDNS	SYSTEM: [S12] Enable Dynamic DNS with hostname wall.adsldns.org on WAN1 by admin (192.168.17.102:443). SYSTEM: [S12] Disable Dynamic DNS on WAN1 by admin (192.168.17.102:443).
	S13	Enable/Disable DNS Proxy	SYSTEM: [S13] Enable DNS proxy by admin (192.168.17.102:443). SYSTEM: [S13] Disable DNS proxy by admin (192.168.17.102:443).
	S14	Enable/Disable DHCP Relay	SYSTEM: [S14] Enable DHCP relay by admin (192.168.17.102:443). SYSTEM: [S14] Disable DHCP relay by admin (192.168.17.102:443).
	S15	Set Date/Time	SYSTEM: [S15] System time update with NTP server tock.usno.navy.mil, set by admin (192.168.17.102:443). SYSTEM: [S15] System time update to 2003-10-10 13:33:25, set by admin (192.168.17.102:443).
	S16	Set System Auto Timeout Lifetime	SYSTEM: [S16] System auto timeout changed to 45 minutes by admin (192.168.17.102:443).
	S17	Interface PORTS Configuration (WAN/LAN/DMZ)	
	S18	Backup Configuration	SYSTEM: [S18] Backup configuration file by admin (192.168.17.102:443).
	S19	Restore Configuration	SYSTEM: [S19] Restore configuration file by admin (192.168.17.102:443).
	S20	Factory Reset	SYSTEM: [S20] Factory Reset to default settings by admin (192.168.17.102:443)
	S21	Firmware Upgrade	SYSTEM: [S21] Firmware upgraded by admin (192.168.17.102:443)

	S22	Setup TELNET Server	
	S23	Setup SSH Server	
	S24	Setup WWW Server	
	S25	Setup HTTPS Server	
	S26	Setup SNMP Server	
	S27	MISC Setup	
	S28	Enable/Disable SNMP	SYSTEM: [S28] Enable SNMP by admin (192.168.17.104:443) SYSTEM: [S28] System Location: Building-A. SYSTEM: [S28] Contact Info: +886-2-28826262. SYSTEM: [S28] Disable SNMP.
	S29	Configure SNMP server	
	S30	File System Full	
	S31	Update remote management settings.	SYSTEM: [S31] Update remote management TELNET Server settings by admin (192.168.17.102:443).
	S32	Set Gateway	SYSTEM: [S32] WAN1: Gateway IP: 192.167.17.254 SYSTEM: [S32] WAN1: Got PPPoE Gateway IP 210.58.28.91.
	S33	Set DNS IP Address	SYSTEM: [S33] WAN1: Clear DNS IP Address. SYSTEM: [S33] WAN1: DNS IP Address: 168.95.1.1. SYSTEM: [S33] WAN1: Get DNS Automatically.
	S34	Syslog Reload	SYSTEM: [S34] Syslogd stop. SYSTEM: [S34] Syslogd start. SYSTEM: [S34] Syslogd restart.
	S35	Enable/Disable Ipmon	SYSTEM: [S35] Enable Ipmon. SYSTEM: [S35] Disable Ipmon.
	S36	System Checksum Update	
	S37	Disable Multicast Update Multicast	SYSTEM: [S37] Disable Multicast on interface WAN1
			SYSTEM: [S37] Update Multicast on interface WAN1 to xxx
			SYSTEM: [S37] Update Multicast on interface WAN1 to xxx
	S38	Update WAN NAT settings	SYSTEM: [S38] Update WAN NAT settings to FULL feature
		Update WAN NAT settings	SYSTEM: [S38] Update WAN NAT settings to Basic operation
		Disable WAN NAT feature	SYSTEM: [S38] Disable WAN NAT feature
VPN	V1	Update pass-through settings	VPN: [V1] Update pass-through settings
	V2	Deactivated IPSec Activated IPSec	VPN: [V2] Deactivated IPSec

Table D-1 All the System Log descriptions

Appendix D
Glossary of Terms

CF (Content Filter) –

A content filter is one or more pieces of software that work together to prevent users from viewing material found on the Internet. This process has two components.

DHCP (Dynamic Host Configuration Protocol) –

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on BOOTP, adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents, and DHCP participants can interoperate with BOOTP participants.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts.

DMZ (Demilitarized Zone) –

From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.

Firewall –

A device that protects and controls the connection of one network to another, for traffic both entering and leaving. Firewalls are used by companies that want to protect any network-connected server from damage (intentional or otherwise) by those who log in to it. This could be a dedicated computer equipped with security measures or it could be a software-based protection.

IPSec (IP Security) –

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers").

L2TP (Layer 2 Tunneling Protocol) –

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet Service Provider (ISP) to enable the operation of a Virtual Private Network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

NAT (Network Address Translation) –

By the network address translation skill, we can transfer the internal network private address of MH-5001 to the public address for the Internet usage. By this method, we can use a large amount of private addresses in the enterprise.

POP3 (Post Office Protocol 3) –

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail.

PPTP (Point-to-Point Tunneling Protocol) –

PPTP extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking. PPTP operates at Layer 2 of the OSI model.

OSPF (Open Shortest Path First) –

Open Shortest Path First (OSPF), is a routing protocol used to determine the correct route for packets within IP networks. It was designed by the Internet Engineering Task Force to serve as an Interior Gateway Protocol replacing RIP.

SMTP (Simple Mail Transfer Protocol) –

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol, that let the user save messages in a server mailbox and download them periodically from the server.

VPN (Virtual Private Network) –

The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technologies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.