

# D-Link DFL-1500

VPN/Firewall Router

## User Manual

**D-Link**

Building Networks for People

© Copyright 2003 D-Link Systems, Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of D-Link Systems, Inc.

DFL-1500 User Manual

Version 0.4

January 30, 2004

### **Trademarks**

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

### **Regulatory Compliance**

FCC Class A Part 15 CSA/CUS

# Table of Contents

Part I	Basic Configuration.....	2
Chapter 1	Quick Start .....	3
1.1	Before You Begin.....	3
1.2	Check Your Package Contents .....	3
1.3	Default Settings .....	3
1.4	Wiring the DFL-1500.....	4
1.5	Default Architecture of DFL-1500.....	6
1.6	Using the Setup Wizard.....	6
1.7	Internet Connectivity.....	9
1.7.1	LAN1-to-WAN1 Connectivity .....	9
1.7.2	WAN1-to-DMZ1 Connectivity.....	10
Chapter 2	System Overview .....	13
2.1	Typical Example Topology .....	13
2.2	Changing the LAN1 IP Address.....	13
2.2.1	From DMZ1 to configure DFL-1500 LAN1 network settings.....	14
2.2.2	From CLI (command line interface) to configure DFL-1500 LAN1 network settings.....	14
Chapter 3	Basic Setup .....	15
3.1	Demand .....	15
3.2	Objectives.....	15
3.3	Methods.....	15
3.4	Steps .....	15
3.4.1	Setup WAN1 IP .....	16
3.4.2	Setup DMZ1, LAN1 Status.....	17
3.4.3	Setup WAN1 IP alias.....	19
Chapter 4	System Tools .....	21
4.1	Demand .....	21
4.2	Objectives.....	21
4.3	Methods.....	21
4.4	Steps .....	24
4.4.1	General settings.....	24
4.4.2	DDNS setting.....	26
4.4.3	DNS Proxy setting .....	27
4.4.4	DHCP Relay setting.....	27
4.4.5	Change DFL-1500 interface .....	28
4.4.6	SNMP Control .....	28
Chapter 5	Remote Management .....	31
5.1	Demands.....	31
5.2	Methods.....	31
5.3	Steps .....	32
5.3.1	Telnet .....	32
5.3.2	WWW .....	32
5.3.3	SNMP .....	32

5.3.4	ICMP .....	32
<b>Part II</b>	<b>NAT、Routing &amp; Firewall .....</b>	<b>34</b>
<b>Chapter 6</b>	<b>NAT .....</b>	<b>35</b>
6.1	Demands.....	35
6.2	Objectives.....	35
6.3	Methods.....	36
6.4	Steps .....	36
6.4.1	Setup Many-to-one NAT rules.....	36
6.4.2	Setup Virtual Server for the FtpServer1 .....	40
<b>Chapter 7</b>	<b>Routing.....</b>	<b>45</b>
7.1	Demands.....	45
7.2	Objectives.....	45
7.3	Methods.....	46
7.4	Steps .....	46
7.4.1	Add a static routing entry.....	46
7.4.2	Add a policy routing entry .....	47
<b>Chapter 8</b>	<b>Firewall.....</b>	<b>49</b>
8.1	Demands.....	49
8.2	Objectives.....	49
8.3	Methods.....	49
8.4	Steps .....	50
8.4.1	Block internal PC session (LAN → WAN).....	50
8.4.2	Setup Alert detected attack .....	51
<b>Part III</b>	<b>Virtual Private Network .....</b>	<b>54</b>
<b>Chapter 9</b>	<b>VPN Technical Introduction.....</b>	<b>55</b>
9.1	Terminology Explanation.....	55
9.1.1	VPN .....	55
9.1.2	IPSec.....	55
9.1.3	Security Association .....	55
9.1.4	IPSec Algorithms.....	55
9.1.5	Key Management.....	55
9.1.6	Encapsulation.....	56
9.1.7	IPSec Protocols.....	57
9.2	Make VPN packets pass through DFL-1500.....	57
<b>Chapter 10</b>	<b>Virtual Private Network – IPSec .....</b>	<b>59</b>
10.1	Demands.....	59
10.2	Objectives.....	59
10.3	Methods.....	59
10.4	Steps .....	60
DES/MD5 IPSec tunnel: the IKE way.....	60	
DES/MD5 IPSec tunnel: the Manual-Key way .....	67	
<b>Chapter 11</b>	<b>Virtual Private Network – PPTP.....</b>	<b>75</b>
11.1	Demands.....	75
11.2	Objectives.....	75
11.3	Methods.....	75



11.4	Steps .....	76
11.4.1	Setup PPTP Network Server .....	76
11.4.2	Setup PPTP Network Client .....	77
<b>Chapter 12</b>	<b>Virtual Private Network – L2TP .....</b>	<b>79</b>
12.1	Demands .....	79
12.2	Objectives .....	79
12.3	Methods .....	79
12.4	Steps .....	80
12.4.1	Setup L2TP Network Server .....	80
<b>Part IV</b>	<b>Content Filters .....</b>	<b>84</b>
<b>Chapter 13</b>	<b>Content Filtering – Web Filters .....</b>	<b>85</b>
13.1	Demands .....	85
13.2	Objectives .....	86
13.3	Methods .....	86
13.4	Steps .....	87
<b>Chapter 14</b>	<b>Content Filtering – Mail Filters .....</b>	<b>93</b>
14.1	Demands .....	93
14.2	Objectives .....	93
14.3	Methods .....	93
14.4	Steps for SMTP Filters .....	94
14.5	Steps for POP3 Filters .....	95
<b>Chapter 15</b>	<b>Content Filtering – FTP Filtering .....</b>	<b>97</b>
15.1	Demands .....	97
15.2	Objectives .....	97
15.3	Methods .....	97
15.4	Steps .....	98
<b>Part V</b>	<b>Intrusion Detection System .....</b>	<b>100</b>
<b>Chapter 16</b>	<b>Intrusion Detection Systems .....</b>	<b>101</b>
16.1	Demands .....	101
16.2	Objectives .....	101
16.3	Methods .....	101
16.4	Steps .....	102
<b>Part VI</b>	<b>Bandwidth Management .....</b>	<b>104</b>
<b>Chapter 17</b>	<b>Bandwidth Management .....</b>	<b>105</b>
17.1	Demands .....	105
17.2	Objectives .....	106
17.3	Methods .....	106
17.4	Steps .....	107
17.4.1	Inbound Traffic Management .....	107
17.4.2	Outbound Traffic Management .....	111
<b>Part VII</b>	<b>System Maintenance .....</b>	<b>114</b>
<b>Chapter 18</b>	<b>System Status .....</b>	<b>115</b>
18.1	Demands .....	115
18.2	Objectives .....	115
18.3	Methods .....	115

18.4	Steps .....	115
Chapter 19 Log System.....		117
19.1	Demands.....	117
19.2	Objectives.....	117
19.3	Methods.....	117
19.4	Steps .....	117
19.4.1	System Logs.....	117
19.4.2	Syslog & Mail log.....	118
Chapter 20 System Maintenance .....		119
20.1	Demands.....	119
20.2	Steps for TFTP Upgrade.....	119
20.3	Steps for Firmware upgrade from Web GUI.....	121
20.4	Steps for Factory Reset.....	121
20.4.1	Steps for NORMAL factory reset.....	121
20.4.2	Steps for EMERGENT factory reset.....	121
20.5	Steps for Backup / Restore Configurations .....	122
Appendix A Command Line Interface (CLI) .....		123
A.1	Enable the port of DFL-1500.....	123
A.2	CLI commands list.....	123
Appendix B Trouble Shooting.....		125
Appendix C Packet Flow.....		129
Appendix D Glossary of Terms .....		131
Appendix E Index .....		133
Appendix F Hardware.....		135
Appendix G Version of Software and Firmware .....		137
Appendix H Customer Support .....		139



# Part I

## Basic Configuration

# Chapter 1

## Quick Start

*This chapter introduces how to quick setup the DFL-1500.*

DFL-1500 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 Before You Begin

Prepare a computer with an Ethernet adapter for configuring the DFL-1500. The default IP address for the DFL-1500 is **192.168.1.254** (LAN1, Port 4) with a Subnet Mask of **255.255.255.0**. You will need to assign your computer a Static IP address within the same range as the DFL-1500's IP address, say 192.168.1.2, to configure the DFL-1500.

### 1.2 Check Your Package Contents

These are the items included with your DFL-1500 purchase as Figure 1-1. They are the following items

1. DFL-1500 Device \* 1
2. Ethernet cable (RJ-45)
3. RS-232 console \* 1
4. CD (include User's manual and Quick Guide) \* 1
5. Power code \* 1



Figure 1-1 All items in the DFL-1500 package

### 1.3 Default Settings

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 DFL-1500.

Items		Default value	New value
Password:		admin	
WAN1 (Port 1)	Fixed IP	IP Address	____.____.____.____
		Subnet Mask	____.____.____.____
		Gateway IP	____.____.____.____
		Primary DNS	____.____.____.____
		Secondary DNS	____.____.____.____
	PPPoE	PPPoE Username	____.____.____.____
		PPPoE Password	____.____.____.____
DHCP			
WAN2 (Port 2)	Fixed IP	IP Address	____.____.____.____
		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 DFL-1500 related network settings

### 1.4 Wiring the DFL-1500

- A. First, connect the power cord to the socket at the back panel of the DFL-1500 as in Figure 1-2 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.

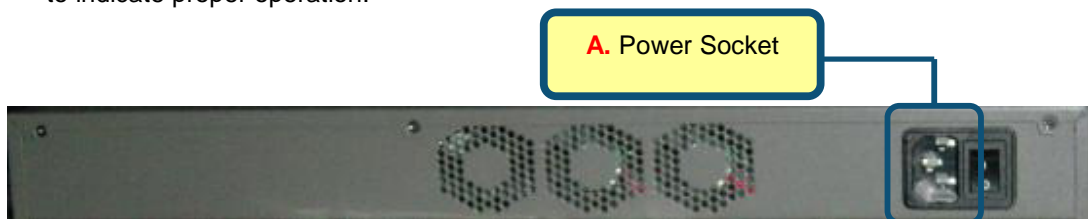


Figure 1-2 Back panel of the DFL-1500

- B.** Using an Ethernet cable, insert one end of the cable to the WAN port on the front panel of the DFL-1500 and the other end of the cable to a DSL or Cable modem, as in Figure 1-3.
- 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 1-3.
- D.** Computers that act as servers to provide Internet services should be connected to the DMZ port using an Ethernet Cable, as in Figure 1-3.

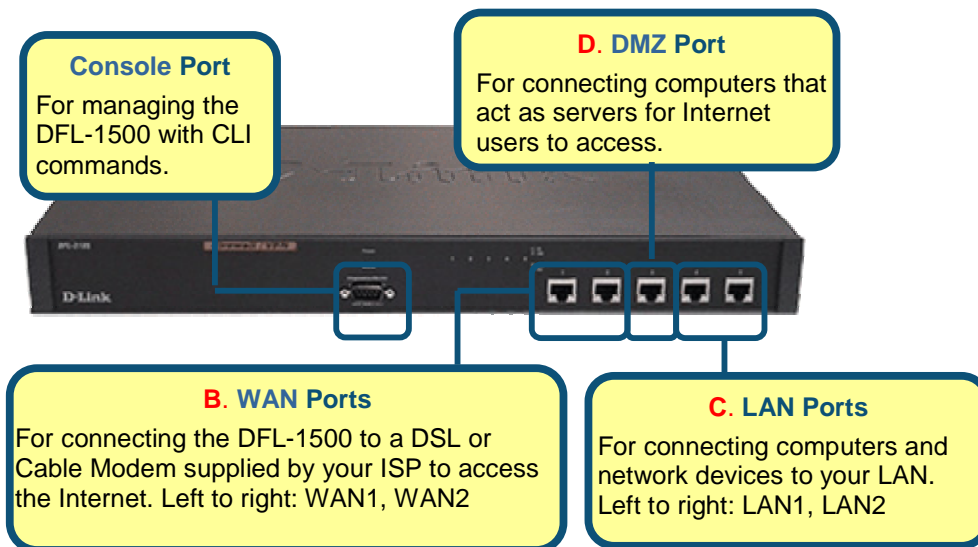


Figure 1-3 Front end of the DFL-1500

## 1.5 Default Architecture of DFL-1500

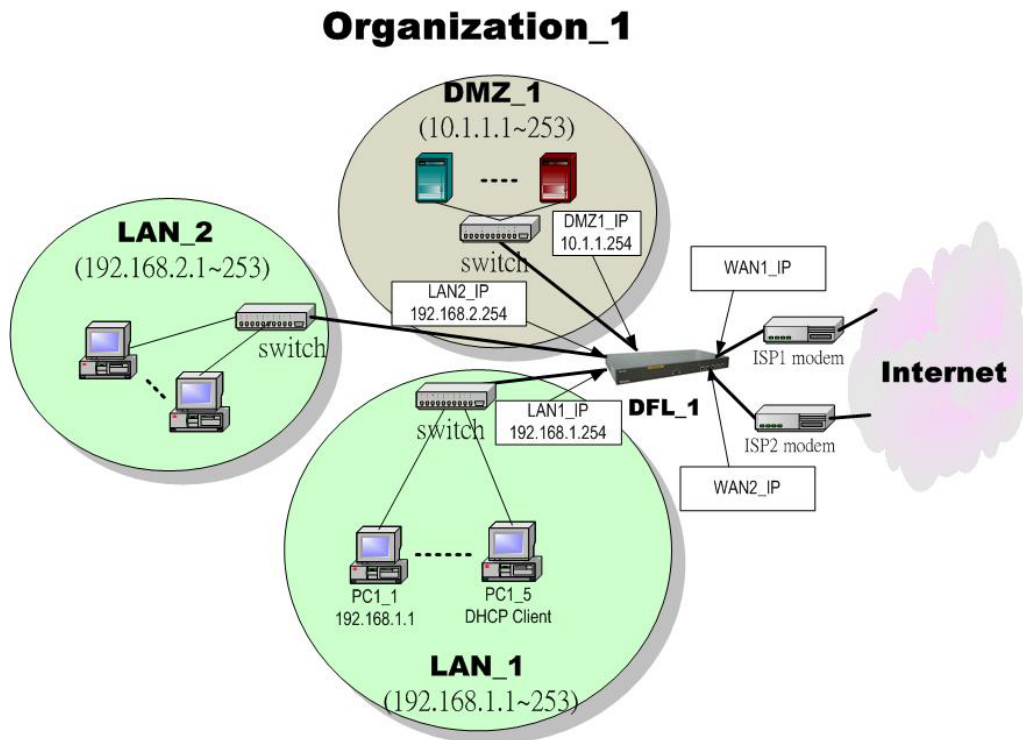




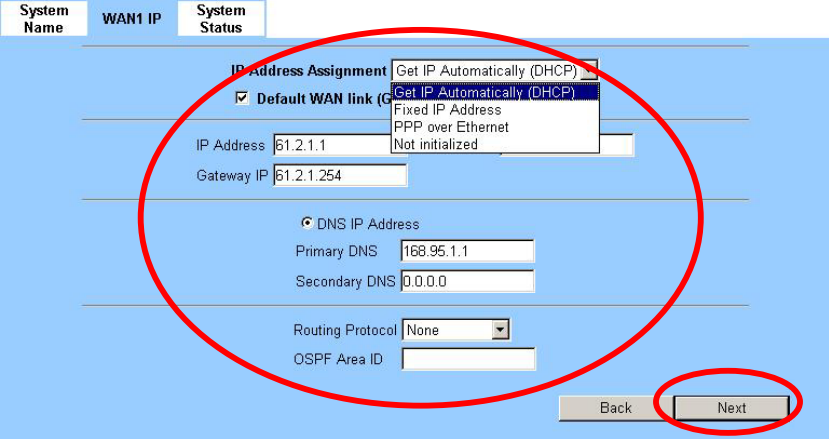
Figure 1-4 The default settings of DFL-1500

The factory default settings for the DFL-1500 are in the Figure 1-4 and Table 1-1. You can configure the DFL-1500 by connecting to the LAN1\_IP (192.168.1.254) from the PC1\_1 (192.168.1.1). The following section will teach you how to quickly setup the DFL-1500 based on Figure 1-4.

## 1.6 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 DFL-1500 in order to be able to make an HTTPS connection using a web browser. The DFL-1500 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 DFL-1500 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 DFL-1500. This address range can be changed later. There are instructions in the DFL-1500 Quick Installation Guide, if you do not know how to set the IP address and Subnet Mask for your computer.



<p><b>Step 1 - Login</b></p> <p>Type "admin" in the account field, "admin" in the Password field and click Login.</p>	<p><b>Connect to <a href="https://192.168.1.254">https://192.168.1.254</a></b></p> 
<p><b>Step 2 - Run Setup Wizard</b></p> <p>Click the Run Setup Wizard.</p>	<p><b>After login to <a href="https://192.168.1.254">https://192.168.1.254</a></b></p> <p><b>BASIC SETUP &gt; Wizard</b></p> <p>Welcome to the DFL-1500 Web-Based Configurator !</p> <p><b>Basic Setup</b> Connect to the Internet and configure your Intranet using the Setup Wizard (WAN, LAN and DMZ settings and DHCP Server settings).</p> <p><b>Advanced Settings</b> 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.</p> <p><b>System Tools</b> Perform firmware upgrade, backup and restore settings to and from local hard drive, load default settings and reboot your VPN router.</p> <p><b>Device Status</b> Display Device IP, MAC addresses and Firmware Version, System Log, Routing Table, Traffic Statistics, NAT Sessions and VPN Traffic Statistics.</p> <p><b>Help</b> Get help about your VPN router.</p> <p><b>Setup Wizard</b> A step-by-step setup wizard will guide you to configure your VPN router to connect to your ISP (Internet Service Provider).</p> <p><b>Run Setup Wizard</b></p>
<p><b>Step 3 - System Name</b></p> <p>Enter the Host Name and the Domain Name, followed by clicking the Next.</p>	<p><b>BASIC SETUP &gt; Wizard</b></p> 
<p><b>Step 4 - WAN Connectivity</b></p> <p>To setup the first WAN link, make WAN1 as the Default WAN link (Gateway/DNS). 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.</p>	<p><b>BASIC SETUP &gt; Wizard &gt; Next</b></p> 

**Step 4.a — DHCP client**

If Get IP Automatically (DHCP) is selected, DFL-1500 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**

**Step 4.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**

**Step 4.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.

Notice: On the current firmware version, if you select PPPoE method as the WAN link connection. The bandwidth management feature will not be supported.

**BASIC SETUP > Wizard > Next > PPPoE**

**Step 5 - System Status**

Here we select PPPoE method in WAN1 port. Then the DFL-1500 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 > Next > Next**

System Name	WAN1 IP	System Status
System Name: <b>DFL-1.dlink.com</b>		
Firmware Version: <b>NetOS Ver1.40B (DLINK) #0: Thu Sep 4 05:13:24 CST 2003</b>		
Default gateway: <b>61.216.123.254</b>		
Primary DNS: <b>168.95.192.1</b>		
Secondary DNS: <b>168.95.1.1</b>		
<b>Port1: WAN1 (PPPoE)[Default]</b>	IP Address: <b>61.216.123.205</b>	Subnet Mask: <b>255.0.0.0</b>
<b>Port2: WAN2 (Not initialized)</b>	IP Address: <b>not set</b>	
<b>Port3: DMZ1</b>	IP Address: <b>10.1.1.254</b>	Subnet Mask: <b>255.255.255.0</b>
<b>Port4: LAN1</b>	IP Address: <b>192.168.1.254</b>	Subnet Mask: <b>255.255.255.0</b>
<b>Port5: LAN2</b>	IP Address: <b>192.168.2.254</b>	Subnet Mask: <b>255.255.255.0</b>

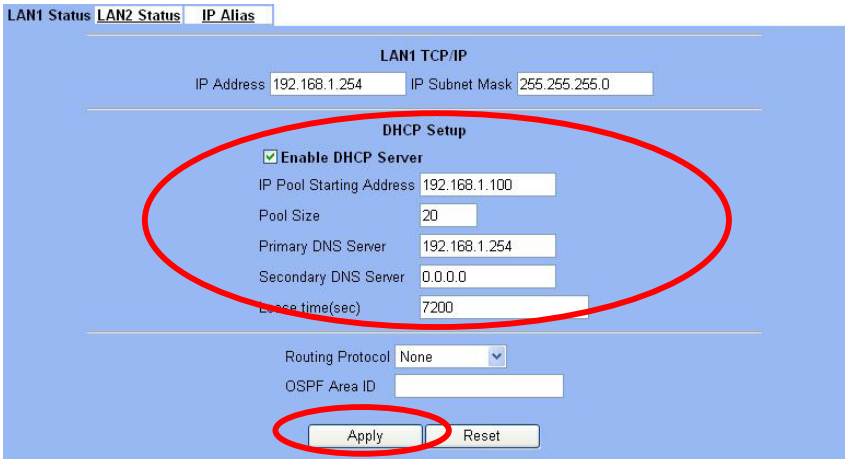
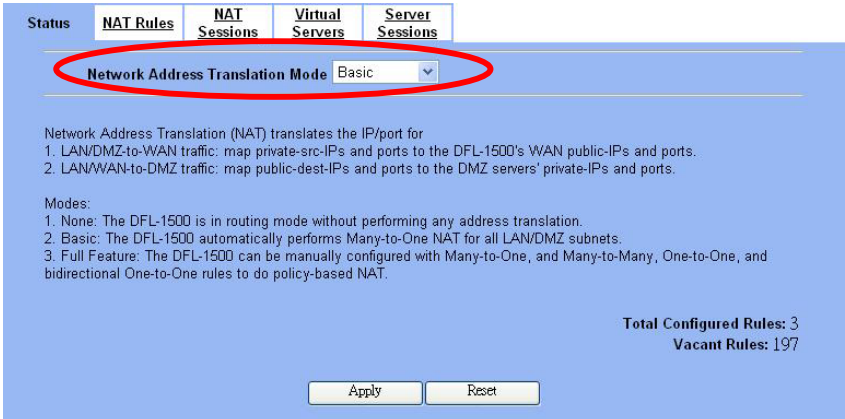
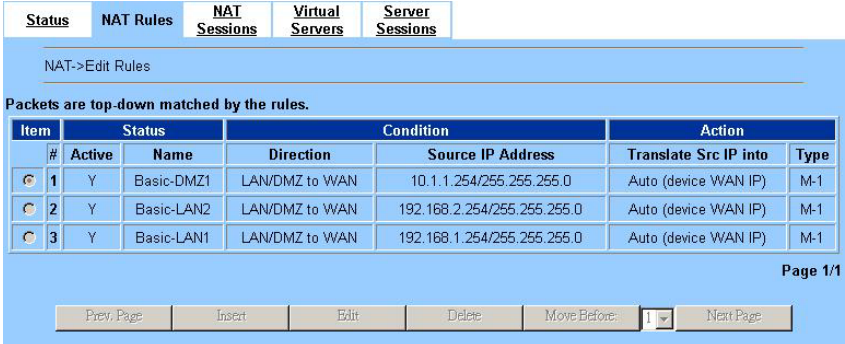
## 1.7 Internet Connectivity

After setting up DFL-1500 with the wizard, DFL-1500 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 DFL-1500. 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.**

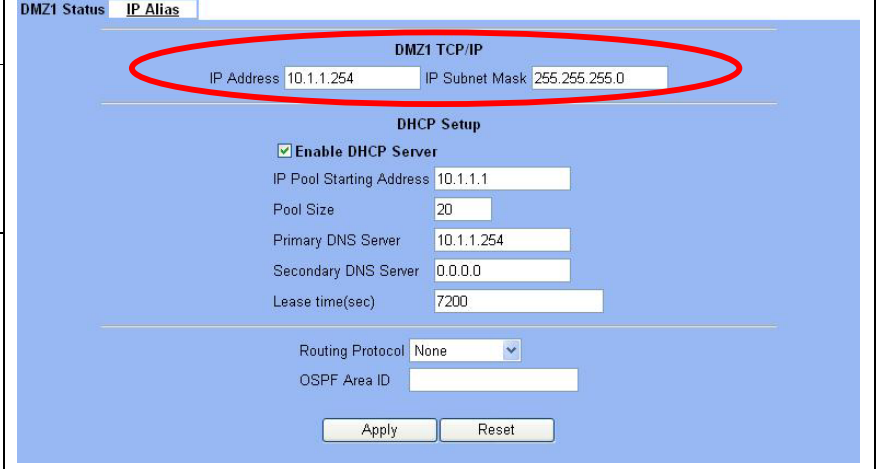
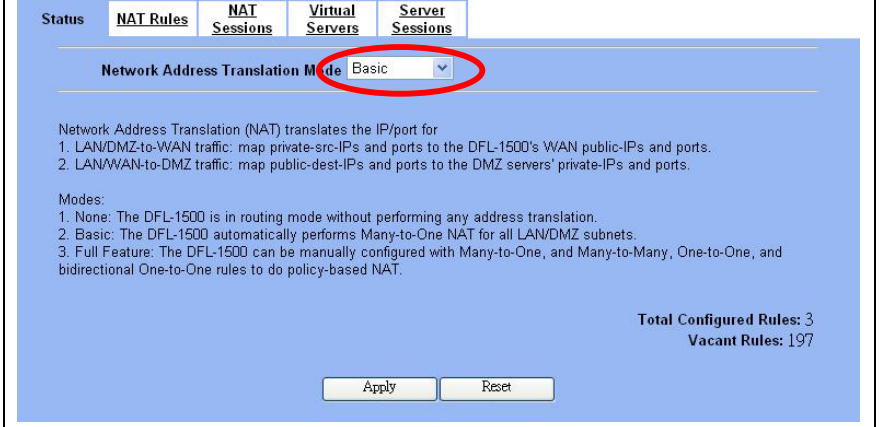
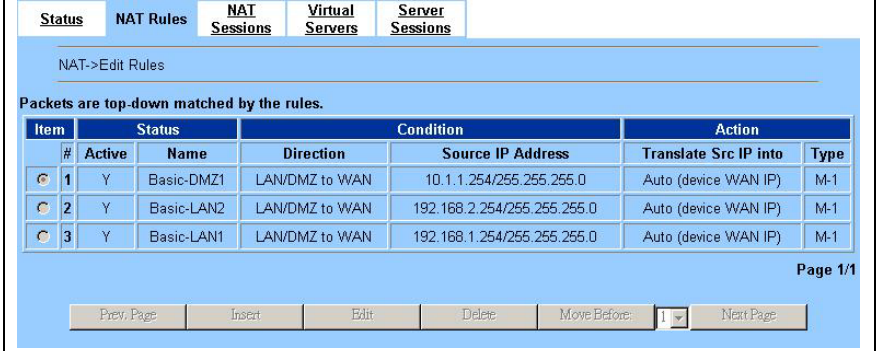
### 1.7.1 LAN1-to-WAN1 Connectivity

The LAN Settings page allows you to modify the IP address and Subnet Mask that will identify the DFL-1500 on your LAN. This is the IP address you will enter in the URL field of your web browser to connect to the DFL-1500. It is also the IP address that all of the computers and devices on your LAN will use as their Default Gateway.

<p><b>Step 1 - Device IP Address</b></p> <p>Setup the IP Address and IP Subnet Mask for the DFL-1500.</p>	<p><b>BASIC SETUP &gt; LAN Settings &gt; LAN1 Status</b></p> 																												
<p><b>Step 2 - Client IP Range</b></p> <p>Enable the DHCP server if you want to use DFL-1500 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.</p> <p>Example: in the figure, the DFL-1500 will assign one IP address from 192.168.1.100 ~ 192.168.1.120, together with the DNS server 192.168.1.254, to the LAN1 PC that requests for an IP address.</p>	<p><b>Note:</b> The IP Pool Starting Address must be on the same subnet specified in the IP Address and the IP Subnet Mask field. For example, the addresses given by the 192.168.1.100 with a pool size of 20 (192.168.1.100 ~ 192.168.1.120) are all within the same range of 192.168.1.254 / 255.255.255.0</p>																												
<p><b>Step 3 - Apply the Changes</b></p> <p>Click Apply to save. Now you can enable the DHCP clients on your LAN1 PCs to get an IP.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; Status</b></p> 																												
<p><b>Step 4 - Check NAT Status</b></p> <p>The default setting of NAT is in Basic Mode. After completing Step 3, the NAT is automatically configured with three rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules</b></p>  <table border="1" data-bbox="646 1556 1476 1691"> <thead> <tr> <th>Item</th> <th>Status</th> <th>Name</th> <th>Direction</th> <th>Condition</th> <th>Action</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>Basic-DMZ1</td> <td>LAN/DMZ to WAN</td> <td>10.1.1.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Basic-LAN2</td> <td>LAN/DMZ to WAN</td> <td>192.168.2.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>3</td> <td>Y</td> <td>Basic-LAN1</td> <td>LAN/DMZ to WAN</td> <td>192.168.1.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> </tbody> </table>	Item	Status	Name	Direction	Condition	Action	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
Item	Status	Name	Direction	Condition	Action	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																							
<p><b>Step 5 - Check NAT Rules</b></p> <p>The DFL-1500 has added three NAT rules. The rule Basic-LAN1 (number 3) 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.</p>																													

**1.7.2 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.

<p><b>Step 1 - Device IP Address</b> Setup the IP Address and IP Subnet Mask for the DFL-1500 of the DMZ1 interface.</p>	<p><b>BASIC SETUP &gt; DMZ Settings &gt; DMZ1 Status</b></p> 
<p><b>Step 2 - Client IP Range</b> Enable the DHCP server if you want to use DFL-1500 to assign IP addresses to the computers under DMZ1. Here we do not enable DHCP feature.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; Status</b></p> 
<p><b>Step 3 - Apply the Changes</b> Click Apply to save your settings.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules</b></p> 
<p><b>Step 4 - Check NAT Status</b> The default setting of NAT is in Basic Mode. After applying the Step 3, the NAT is automatically configured with three rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.</p>	<p><b>Step 6 - Setup IP for the FTP Server</b> 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).</p>



**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	Name	Direction	Dest. IP Address	Service	Action
						Translate dest. IP/port into

Page 1/1

Prev. Page **Insert** Edit Delete Move Before: Next Page

**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. DFL-1500 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 DFL-1500 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 LAN/WAN-to-DMZ Virtual Server rule

Activate this rule

Rule name: ftpServer

**Condition**

Dest. IP: 61.2.1.1 Netmask: 255.255.255.255

Service: TCP

Type:  Single  Range

Dest. Port: 44444  Passive FTP client?

to 0

Well known port: DNS (53) Copy To Dist.

**Action**

Translated dest. IP: 10.1.1.5

Translated dest. port: 21 (0 means that DFL-1500 will not change the port number.)

Back **Apply** Reset

**Step 9 - View the Result**  
 Now any request towards the DFL-1500'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	Name	Direction	Dest. IP Address	Service	Action
1	Y	ftpServer	LAN/WAN to DMZ	61.2.1.1/255.255.255.0	TCP-44444	10.1.1.5:21

Page 1/1

Prev. Page **Insert** Edit Delete Move Before: 1 Next Page

## 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 DFL-1500. In Figure 2-1, the left half side is a DFL-1500 with one LAN, one DMZ, and two WAN links. Notice there are five ports in DFL-1500. In this topology, we only use one LAN.

The right half side contains a DFL-1500 connected with one LAN, one DMZ, and one WAN. In this architecture, Organization\_1 communicates with Organization\_2 with a VPN tunnel established by the two DFL-1500 Firewall/VPN routers. The VPN tunnel secures communications between Organizations more safely.

On the Internet side, there are Web server, Mail server, DHCP server, and FTP server for testing the content filters and the bandwidth management system.

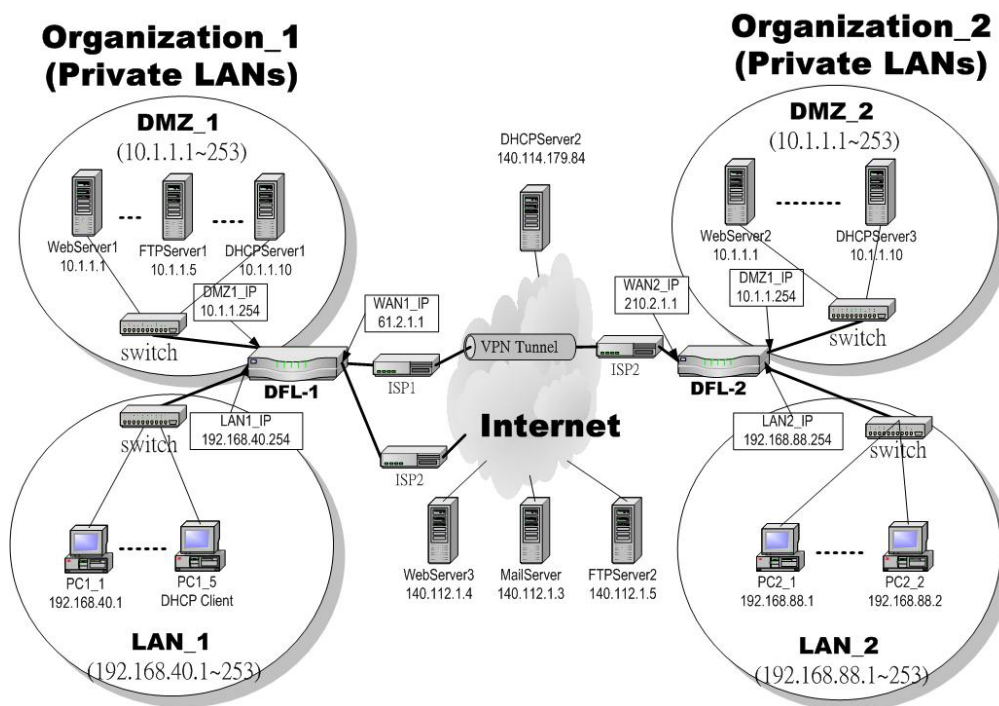


Figure 2-1 Typical topology for deploying DFL-1500

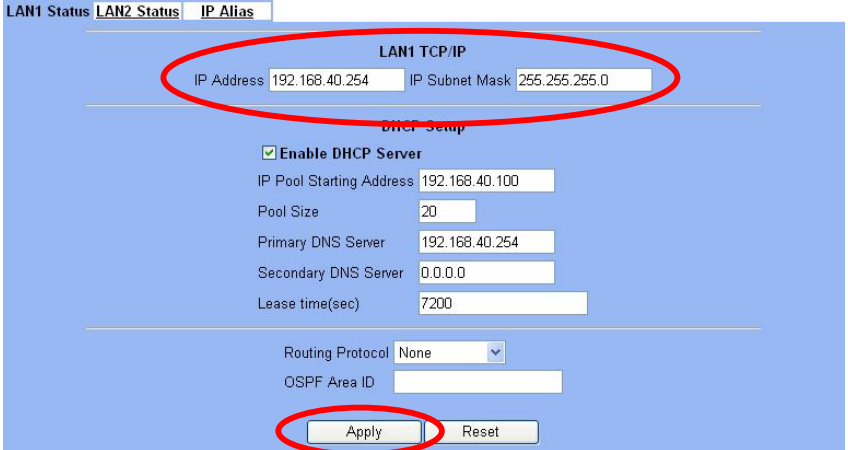
### 2.2 Changing the LAN1 IP Address

The default settings of DFL-1500 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 DFL-1500 to 192.168.40.254. Notice that you cannot change the LAN1 IP from the LAN1 interface because your configuration session to LAN1 will be terminated as long as the LAN1 IP address is changed. If you do change the IP from the LAN1 port, you will have to reboot the system, change your computer's IP to the new subnet, and reconnect to the new LAN1 IP address. You can also use console to login into the system

and then logout the system. That will clean up the zombie left in the system so you will be able to login to the DFL-1500 from the LAN1 side after your computer's IP is changed into the new subnet.

We provide two normal ways to configure the LAN1 IP address. One is to configure the LAN1 IP from another port such as DMZ1 or LAN2. The other is to configure the LAN1 IP through console. Note that when setting the IP address from console, the settings are updated into run-time system but not stored into the flash. Namely, the settings will be lost after you reboot the system. So, it is best to use the first method for setting the LAN1 IP address.

### 2.2.1 From DMZ1 to configure DFL-1500 LAN1 network settings

<p><b>Step 1 - Check NAT Status</b></p> <p>In the DMZ_1 region, use a PC located 10.1.1.X to connect DFL-1500 DMZ1 port (10.1.1.254). Type <a href="https://10.1.1.254">https://10.1.1.254</a> to configure the DFL-1500 in the web browser.</p>	<p>Use an IE 6.0 at 10.1.1.1 to connect to <a href="https://10.1.1.254">https://10.1.1.254</a></p>
<p><b>Step 2 - Setup LAN1 IP information</b></p> <p>Enter the IP Address and IP Subnet Mask with 192.168.40.254 / 255.255.255.0 and click Apply.</p>	<p><b>BASIC SETUP &gt; LAN Settings &gt; LAN1 Status</b></p>  <p>The screenshot shows the 'LAN1 Status' configuration page. The 'LAN1 TCP/IP' section has 'IP Address' set to 192.168.40.254 and 'IP Subnet Mask' set to 255.255.255.0. Below this, the 'DHCP Setup' section has 'Enable DHCP Server' checked. Other fields include 'IP Pool Starting Address' (192.168.40.100), 'Pool Size' (20), 'Primary DNS Server' (192.168.40.254), 'Secondary DNS Server' (0.0.0.0), and 'Lease time(sec)' (7200). At the bottom, 'Routing Protocol' is set to 'None' and 'OSPF Area ID' is empty. The 'Apply' button is circled in red.</p>

### 2.2.2 From CLI (command line interface) to configure DFL-1500 LAN1 network settings

<p><b>Step 1 - Use Console port to configure DFL-1500</b></p> <p>Use the supplied console line to connect the PC to the Diagnostic RS-232 socket of the DFL-1500. 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 DFL-1500, 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.</p>	<pre>DFL-1500&gt; en DFL-1500# ip ifconfig INTF3 192.168.40.254 255.255.255.0  DFL-1500# ip ifconfig INTF3  ===== Port Interface IP Address      Netmask      Status Type ----- 4    LAN1    192.168.40.254 255.255.255.0  UP =====</pre>
--	---



## Chapter 3

# Basic Setup

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

### 3.1 Demand

1. For the external network, suppose your company uses DSL to connect Internet via PPPoE. By this way, you should setup WAN port of the DFL-1500 in advance.
2. There are some adjustment within your company, so the original network structure 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 insufficient for your company to connect to the external network.

### 3.2 Objectives

1. Configure the network settings of the DFL-1500 WAN1 port.
2. Configure the network settings of the DFL-1500 DMZ1 and LAN1 ports.
3. Suppose your company applies another ISP, and hope that the applied Network IP can configure in the same WAN port of DFL-1500.

### 3.3 Methods

1. Select the PPPoE method in the DFL-1500 Basic Setup/WAN settings/WAN1 IP, and then configure the related account and password in order to connect to the internet.
2. Configure the related network settings in the pages of the DFL-1500 Basic Setup / DMZ settings / DMZ1 Status, Basic Setup / LAN settings / LAN1 Status.
3. Configure the IP alias in WAN1 port.

### 3.4 Steps

Notice : Do not try to configure the port network setting from the same port you login. Or the network will be terminated and system will be locked in the original IP address.


### 3.4.1 Setup WAN1 IP

<p><b>Step 1 - Setup WAN1 port</b></p> <p>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.</p>	<p><b>BASIC SETUP &gt; WAN Settings &gt; WAN1 IP &gt; Fixed IP Address</b></p>
---	--

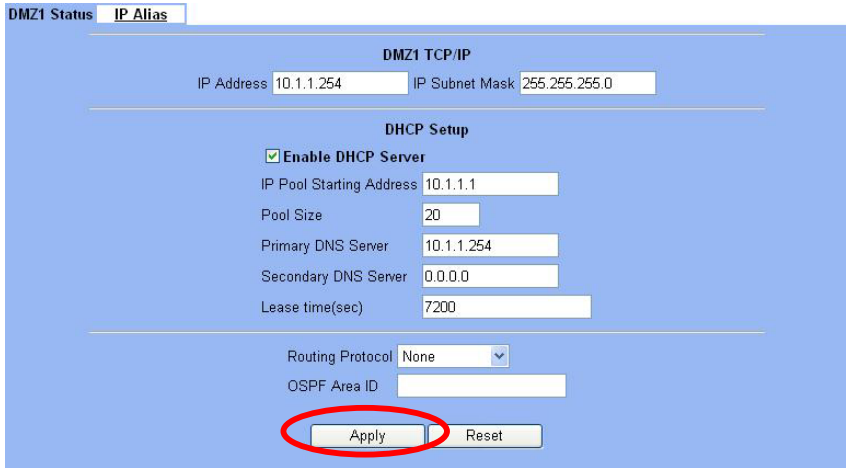
IP Address Assignment	FIELD	DESCRIPTION	EXAMPLE
Get IP Automatically (DHCP)	Default WAN link (Gateway/DNS)	When Default WAN link is enabled. All the packets sent out from DFL-1500 will be via this port.	Enabled
	Get DNS Automatically or DNS IP Address	Get DNS Automatically → Get DNS related information from DHCP Server DNS IP Address → manually specify these Primary and Secondary DNS Server information	Get DNS Automatically
	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
	OSPF Area ID	Specify OSPF area ID number	
Fixed IP Address	Default WAN link	When Default WAN link is enabled. All the packets sent out from DFL-1500 will be via this port.	Enabled
	IP Address / Subnet Mask	Specified IP address and subnet mask	61.2.1.1 255.255.255.0
	Gateway IP	Default gateway IP address	61.2.1.254
	DNS IP Address	Specified Primary and Secondary DNS Server address	168.95.1.1
	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
	OSPF Area ID	Specify OSPF area ID number	
PPP over Ethernet	Default WAN link	When Default WAN link is enabled. All the packets sent out from DFL-1500 will be via this port.	Enabled
	Service Name	ISP vendor (Optional)	So-Net
	User Name	The user name of PPPoE account	Hey
	Password	The password of PPPoE account	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
Disconnected	Through click Connect or Disconnect button to connect or disconnect PPPoE line	Click Connect

Table 3-1 Detailed information of setup WAN port configuration

<p><b>Step 2 - Show the Warning message</b></p> <p>Note that if you have already enabled bandwidth management (ADVANCED SETTINGS&gt;Bandwidth Mgt&gt;Enable Bandwidth Management) and then select PPPoE in BASIC SETUP&gt;WAN Settings&gt;WAN1 IP&gt;PPPoE as your internet connection, it will show you a message indicated as right column to tell you that Bandwidth management will not support PPPoE in this version. If you still like to use bandwidth management, please try to use another method, such as DHCP or Fixed IP, to connect Internet.</p>	<p><b>BASIC SETUP &gt; WAN Settings &gt; WAN1 IP &gt; PPPoE</b></p> 
--	--

### 3.4.2 Setup DMZ1, LAN1 Status

<p><b>Step 1 - Setup DMZ port</b></p> <p>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.</p>	<p><b>BASIC SETUP &gt; DMZ Settings &gt; DMZ1 Status</b></p> 
--	---

FIELD	DESCRIPTION	EXAMPLE
IP Address	DMZ port IP address	10.1.1.254
IP Subnet Mask	DMZ port IP subnet mask	255.255.255.0
Enable DHCP Server	Enable DMZ port of the DHCP Server or not	Enabled
IP Pool Starting Address	Specify the starting address of the DHCP IP address.	10.1.1.1
Pool Size	Specify the numbers of the DHCP IP address.	20

Primary DNS Server	Specify the Primary DNS Server IP address of the DHCP information.	10.1.1.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP information.	
Lease time(sec)	Specify DHCP information lease time	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
OSPF Area ID	Specify OSPF area ID number	

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.

FIELD	DESCRIPTION	EXAMPLE
IP Address	LAN port IP address	192.168.40.254
IP Subnet Mask	LAN port IP subnet mask	255.255.255.0
Enable DHCP Server	Enable LAN port of the DHCP Sever or not	Enabled
IP Pool Starting Address	Specify the starting address of the DHCP IP address.	192.168.40.100
Pool Size	Specify the numbers of the DHCP IP address.	20
Primary DNS Server	Specify the Primary DNS Server IP address of the DHCP information.	192.168.40.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP information.	
Lease time(sec)	Specify DHCP information lease time	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
OSPF Area ID	Specify OSPF area ID number	

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 211.17.25.56 to 211.17.25.63. Now you would like to add a WAN1 IP alias. Select WAN1 in the Interface. Enter the IP alias and Netmask with 211.17.25.62/255.255.255.248. 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**

FIELD	DESCRIPTION	EXAMPLE
Interface	The interface which we set for the IP alias	WAN1
IP alias	The alias IP address	211.17.25.62
Netmask	The netmask of the IP alias	255.255.255.248

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
<input checked="" type="radio"/> 1	WAN1	211.17.25.62	255.255.255.248
<input type="radio"/> 2	...	...	...
<input type="radio"/> 3	...	...	...
<input type="radio"/> 4	...	...	...
<input type="radio"/> 5	...	...	...
<input type="radio"/> 6	...	...	...
<input type="radio"/> 7	...	...	...
<input type="radio"/> 8	...	...	...
<input type="radio"/> 9	...	...	...
<input type="radio"/> 10	...	...	...

**Step 3 - Add a static or policy routing entry**

Refer to the Chapter 7 explanation.

In the “Advanced Settings > Routing” pages, setup the static or policy routing pages to share the outbound traffic load.



## Chapter 4

# System Tools

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

### 4.1 Demand

1. Basic configurations for domain name, password, system time, timeout and services.
2. DDNS: Suppose the DFL-1500'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 (10.1.1.10), the server will not receive any broadcast packet from the client.
5. Suppose our company applies three ISPs, but there are just two default WAN ports in the DFL-1500. You hope to connect the whole ISP links to the DFL-1500.
6. The System Administrator would like to monitor the device from remote side efficiently.

### 4.2 Objectives

1. Configure the general properties, such as domain name, password, system time, and connection timeout correctly. Besides, we can configure the preferred service name as the service name/numeric mapping list.
2. DDNS: By using the DDNS (Dynamic DNS), the DFL-1500 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. We hope to customize the interface of DFL-1500 to fit our requests.
6. Through the SNMP manager, we can easily monitor the device status.

### 4.3 Methods

1. Configure the domain name, password, system time, connection timeout and service name.
2. DDNS: Configure the DFL-1500 so that whenever the IP of the DFL-1500 is changed, it will send requests to the DDNS server to refresh the DNS record. As the following Figure 4-1 demonstrated, the original DFL-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. DFL-1 will update the registered ip address "61.2.1.1" as the assigned one. This is the base mechanism of the DDNS.

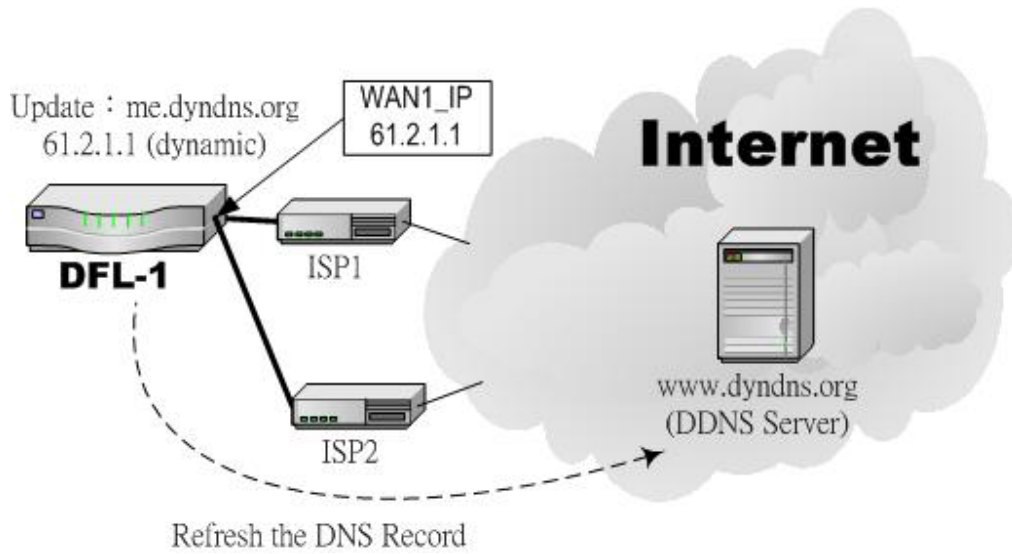


Figure 4-1 DDNS mechanism chart

3. DNS Proxy: After activating the DNS proxy mode, the client can set its DNS server to the DFL-1500 (that is, send the DNS requests to the DFL-1500). The DFL-1500 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, DFL-1 redirects the DNS request from PC1\_1 to the real DNS server (140.113.1.1).

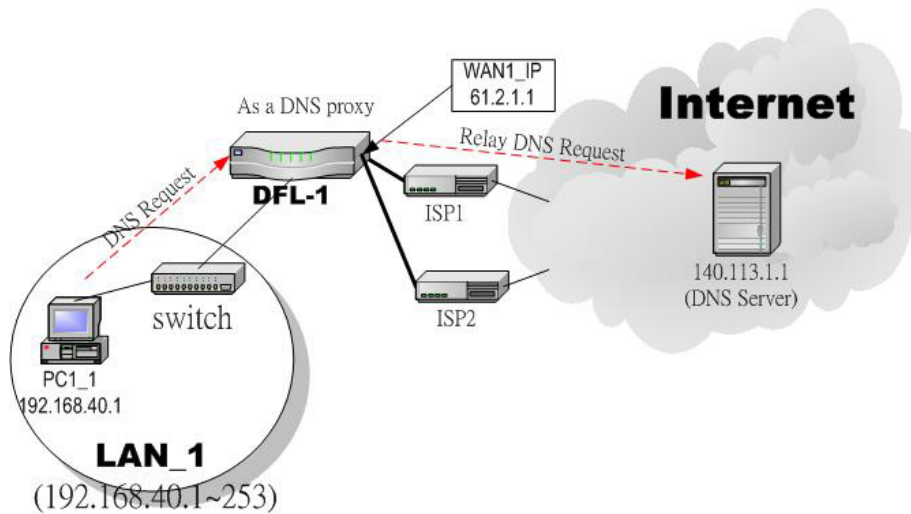


Figure 4-2 DNS Proxy mechanism chart

4. DHCP Relay: Activate the DHCP relay mode of DFL-1500 so that the DFL-1500 will become the relay agent and relay the DHCP broadcast to the configured DHCP server. As the following Figure 4-3 described, DFL-1 redirects the DHCP request from the preconfigured port (LAN1, DMZ1) to the real DHCP server (210.176.25.3).



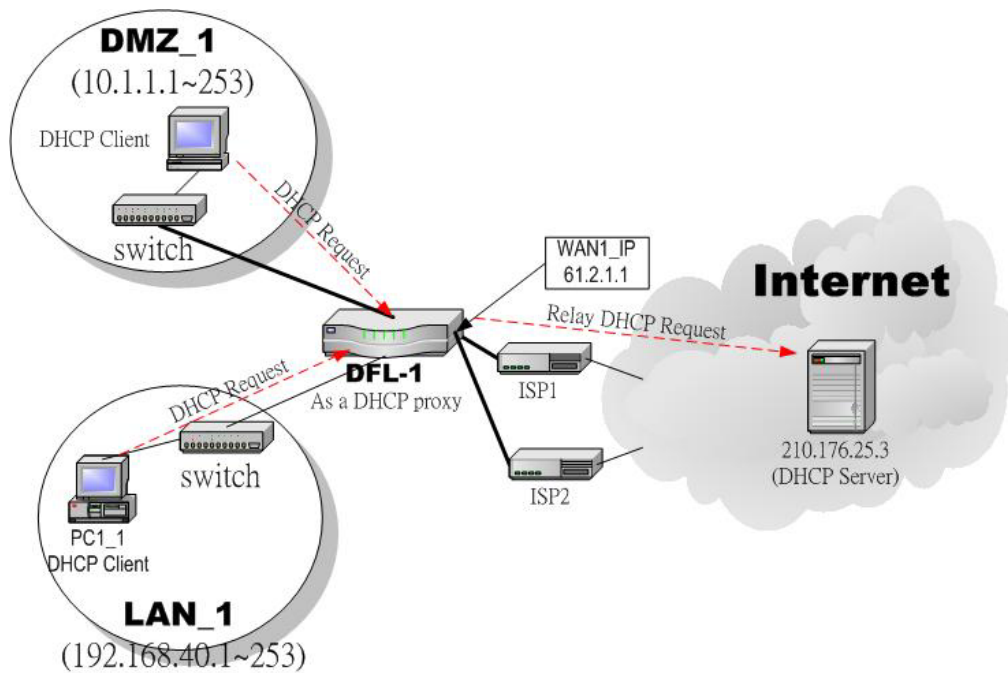


Figure 4-3 DHCP Relay mechanism chart

- We can adjust the DFL-1500 interface in the SYSTEM TOOLS > Admin Settings > Interface in according to our preference and requirement (3 WAN, 1 LAN, 1 DMZ). As the following Figure 4-4 demonstrated, there are three ISP connected onto DFL-1500. So we must adjust the interface up to 3 WAN ports to fit the current condition.

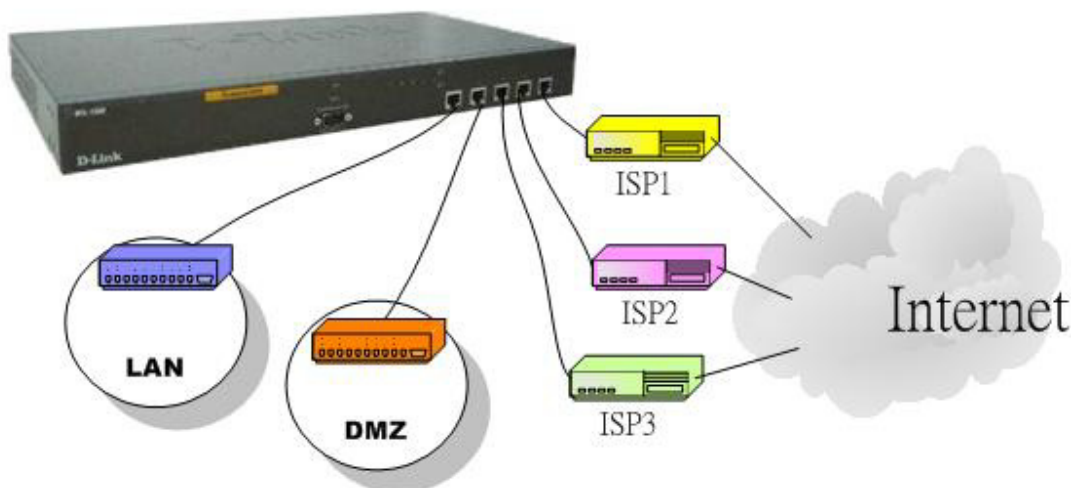


Figure 4-4 Adjust DFL-1500 interface to fit present situation

- As the following Figure 4-5 demonstrated, there is an embedded snmp agent in the DFL-1500. So you can use SNMP manager to monitor the DFL-1500 system status, network status ,etc. from either LAN or internet.

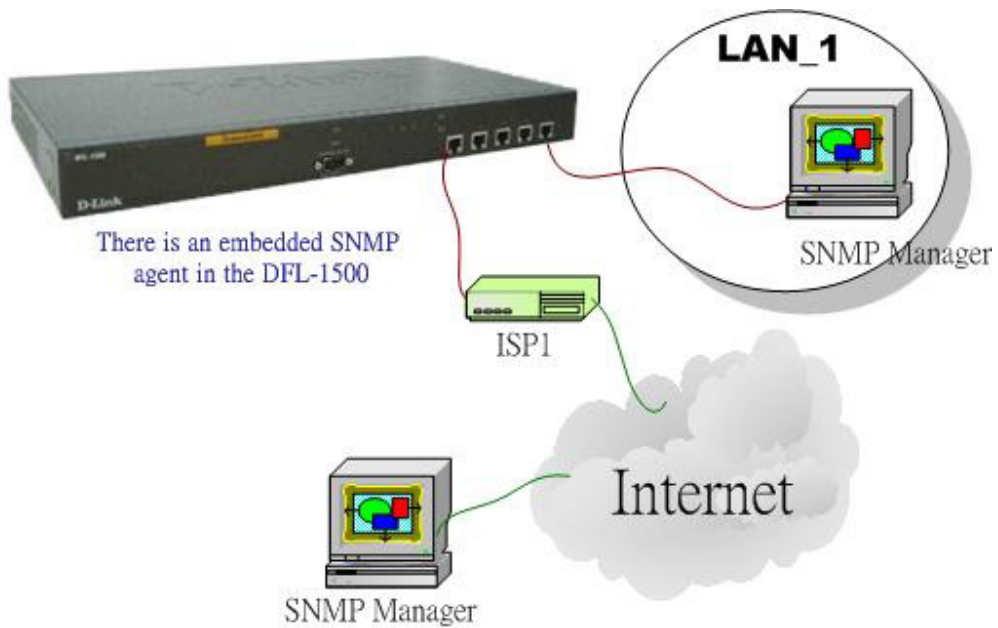


Figure 4-5 It is efficient to use SNMP Manager to monitor DFL-1500 device

## 4.4 Steps

### 4.4.1 General settings

<p><b>Step 1 - General Setup</b></p> <p>Enter the Host Name as DFL-1, Domain Name as the domain name of your company Click Apply.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; General</b></p> <p>General   DDNS   DNS Proxy   DHCP Relay   Password   Time/Date   Timeout   Services   Interface</p> <p>Host Name: DFL-1</p> <p>Domain Name: dlink.com</p> <p>Apply   Reset</p>
---	---

FIELD	DESCRIPTION	EXAMPLE
Host Name	The host name of the DFL-1500 device	DFL-1
Domain Name	Fill in the domain name of company	dlink.com

Table 4-1 System Tools - General Setup menu

<p><b>Step 2 - Change Password</b></p> <p>Enter the current password in the Old Password field. Enter the new password in the New Password and retype it in the Retype to Confirm field. Click Apply.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; Password</b></p> <p>General   DDNS   DNS Proxy   DHCP Relay   Password   Time/Date   Timeout   Services   Interface</p> <p>Old Password: [masked]</p> <p>New Password: [masked]</p> <p>Confirm Password: [masked]</p> <p>Apply   Reset</p>
---	--

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

<p><b>Step 3 - Setup Time/Date</b></p> <p>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 DFL-1500 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.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; Time/Date</b></p>
---	---

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

<p><b>Step 4 - Setup Timeout</b></p> <p>Select the target timeout (e.g. 10 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.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; Timeout</b></p>
--	---

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.	10

Table 4-4 System Tools – Timeout menu

**Step 5 - Configure Services**

We can configure the service name and numeric port number as the same group, so you can simply use the domain name for the configuration in the DFL-1500. If you want to add/edit/delete the service record, just click the below button to add/edit/delete it.

**SYSTEM TOOLS > Admin Settings > Services**

FIELD	DESCRIPTION	EXAMPLE
Add	Add a service name record	N/A
Edit	edit an existing service name record	N/A
Delete	delete an existing service name record	N/A

Table 4-5 Setup the service name record

### 4.4.2 DDNS setting

**Step 1 - Setup DDNS**


If the IP address of DFL-1500 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 two 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 detail information. Click Apply to activate the settings.

**SYSTEM TOOLS > Admin Settings > DDNS**

FIELD	DESCRIPTION	EXAMPLE
Enable DDNS for WAN1	Enable DDNS feature of DFL-1500	Enabled
Interface	Assign which public IP address of interface to the DDNS server.	WAN1
Service Provide	The domain address of DDNS server. In the DFL-1500, we provide <u>WWW.DYNDNS.ORG</u> and <u>WWW.DHS.ORG</u> two websites for choice.	<u>WWW.DYNDNS.ORG</u>
Hostname	The registered Hostname in the DDNS server.	abc.com
Username	The registered username in the DDNS server.	user
Password	The registered password in the DDNS server.	1234567

Table 4-6 System Tools – DDNS setting page

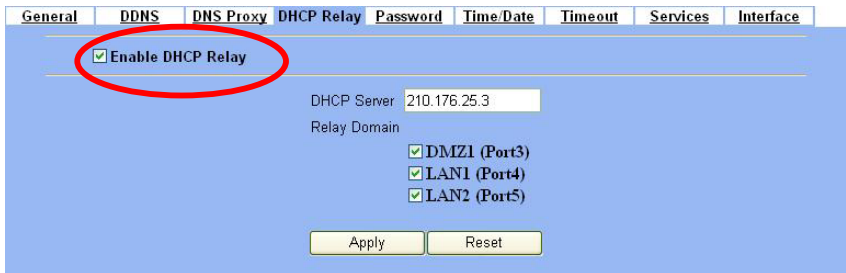
### 4.4.3 DNS Proxy setting

<p><b>Step 1 - Setup DNS Proxy</b></p> <p>Check the <b>Enable DNS Proxy</b> and click the <b>Apply</b> to store the settings. From now on, your LAN/DMZ PCs can use DFL-1500 as their DNS server, as long as the DNS server for DFL-1500 has been set in its WAN settings.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; DNS Proxy</b></p> 
--	---

FIELD	DESCRIPTION	EXAMPLE
Enable DNS Proxy	When the host of the LAN/DMZ sends a DNS Request, DFL-1500 will request for forwarding it to the DNS server of the Default WAN link. When there is a response from DNS, DFL-1500 will forward it back to the host of the LAN/DMZ.	Enabled

Table 4-7 System Tools – DNS Proxy menu

### 4.4.4 DHCP Relay setting

<p><b>Step 1 - Setup DHCP Relay</b></p> <p>Check the <b>Enable DHCP Relay</b>. Enter the IP address of your DHCP server. Check the relay domain of DFL-1500 that needs to be relayed. Namely, check the one where the DHCP server resides and the one where DHCP clients are located. Click the <b>Apply</b> button.</p>	<p><b>SYSTEM TOOLS &gt; Admin Settings &gt; DHCP Relay</b></p> 
--	---

FIELD	DESCRIPTION	EXAMPLE
Enable DHCP Relay	When the host of the LAN/DMZ in the DFL-1500 internal network sends a DHCP request, DFL-1500 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.	210.176.25.3
Relay Domain	The locations of the DHCP clients.	

Table 4-8 System Tools – DHCP Relay menu

### 4.4.5 Change DFL-1500 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 1 LAN (port1), 1 DMZ (port2) and 3 WAN (port3~5). And then press apply button to reboot DFL-1500. 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 DFL-1500. 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

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 DFL-1500.	WAN / LAN / DMZ

Table 4-9 Change the DFL-1500 interface setting

### 4.4.6 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 DFL-1500.

#### SYSTEM TOOLS > SNMP Control

---

FIELD	DESCRIPTION	EXAMPLE
Enable SNMP	Enable the SNMP function or not.	enabled
System Name	The device name of DFL-1500.	DFL-1.dlink.com
System Location	The settled location of DFL-1500.	Office
Contact Info	The person who takes charge of the DFL-1500.	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 DFL-1500.	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 DFL-1500.	192.168.1.5





# Chapter 5

## Remote Management

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

### 5.1 Demands

Administrators may want to manage the DFL-1500 remotely from any PC in LAN\_1 with HTTP at port 8080, and from WAN\_PC with TELNET. In addition, the DFL-1500 may be more secure if monitored by a trusted host (PC1\_1). What is more, the DFL-1500 should not respond to ping to hide itself. The remote management function in DFL-1500 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, WAN2 side.

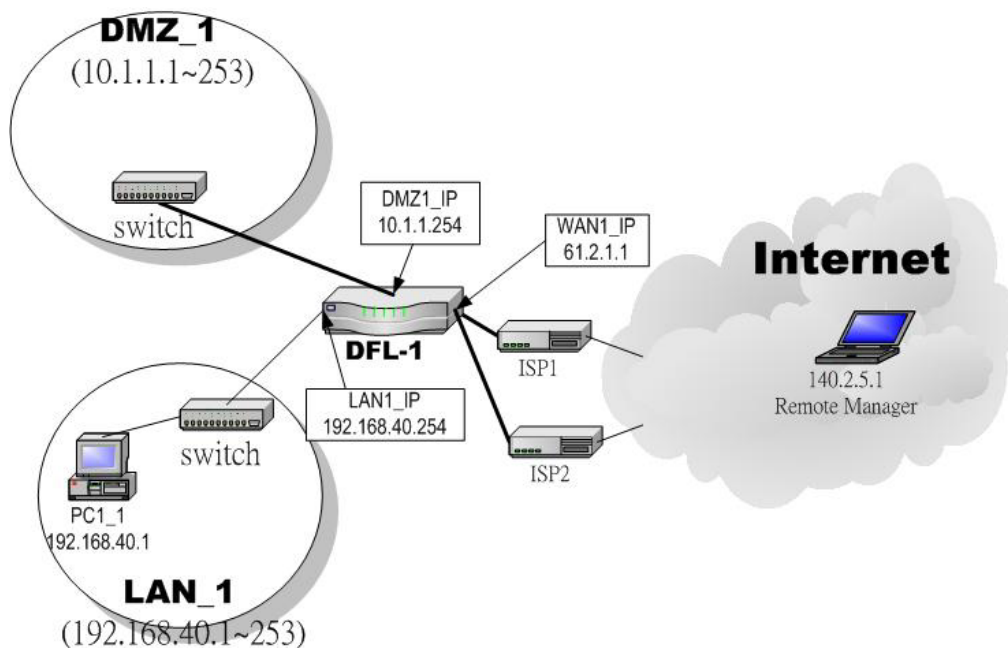


Figure 5-1 Some management method of DFL-1500

### 5.3 Steps

#### 5.3.1 Telnet

##### Step 1 - Setup Telnet

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 DFL-1500. And click the Apply.

##### SYSTEM TOOLS > Remote Mgt. > TELNET

#### 5.3.2 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). And click the Apply. If you are configuring the DFL-1500 with HTTP, your browser will then automatically be directed to the new server port.

##### SYSTEM TOOLS > Remote Mgt. > WWW

#### 5.3.3 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 DFL-1500. Here we click All for all no IP range limitation of clients. Finally click the Apply.

##### SYSTEM TOOLS > Remote Mgt. > SNMP

#### 5.3.4 ICMP

##### Step 1 - Setup ICMP

Uncheck the WAN1, WAN2 checkbox and make others checked. Then click the Apply button.

##### SYSTEM TOOLS > Remote Mgt. > MISC



# Part II

## NAT, Routing & Firewall

# Chapter 6

## NAT

*This chapter introduces NAT and explains how to implement it in DFL-1500.*

To facilitate the explanation on how DFL-1500 implements NAT and how to use it, we zoom in the left part of Figure 1-4 into Figure 6-1.

### 6.1 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.
2. Internet servers provided by your company may open many ports in default that may be dangerous if exposed to the public Internet.

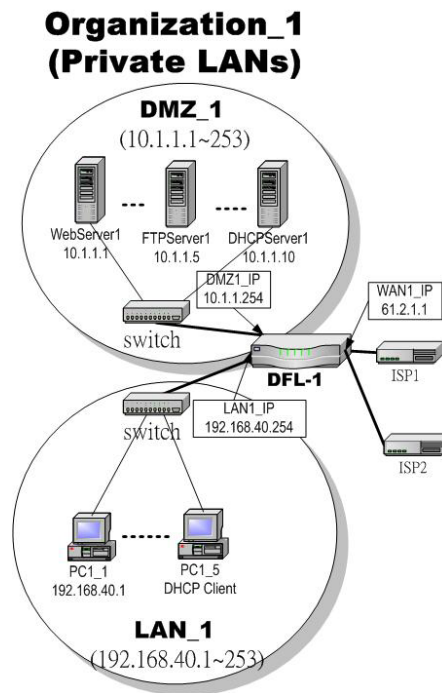


Figure 6-1 Topology for explanations of the NAT examples.

### 6.2 Objectives

1. Let PC1\_1~PC1\_5 connect to the Internet.
2. Let FTPServer1 be accessed by other Internet users.

### 6.3 Methods

1. Assign private IP addresses to the PC1\_1~PC1\_5. Setup NAT at DFL-1500 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 DFL-1500 to redirect “any connections towards some port of WAN1” to the port 21 at the FTPServer1.

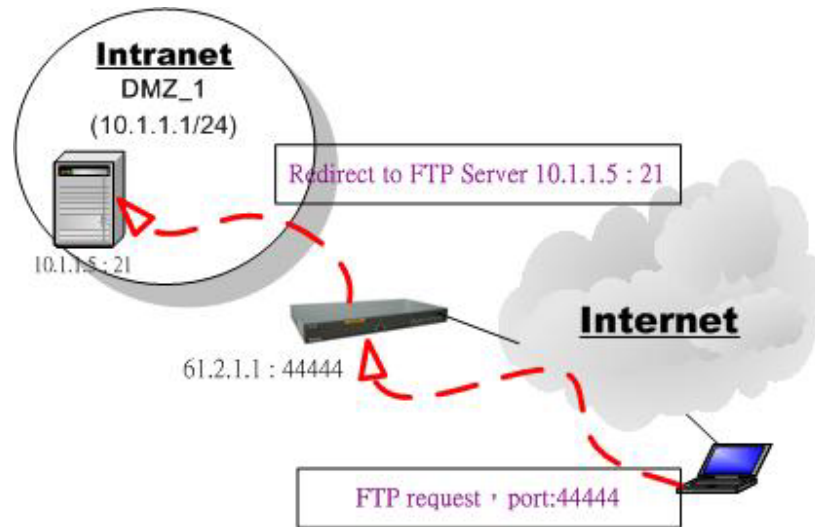


Figure 6-2 DFL-1500 plays the role as Virtual Server

As the above Figure 6-2 illustrates, the server 10.1.1.5 provides FTP service. But it is located on the DMZ region behind DFL-1500. And DFL-1500 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.

### 6.4 Steps

#### 6.4.1 Setup Many-to-one NAT rules

##### Step 1 - Enable NAT

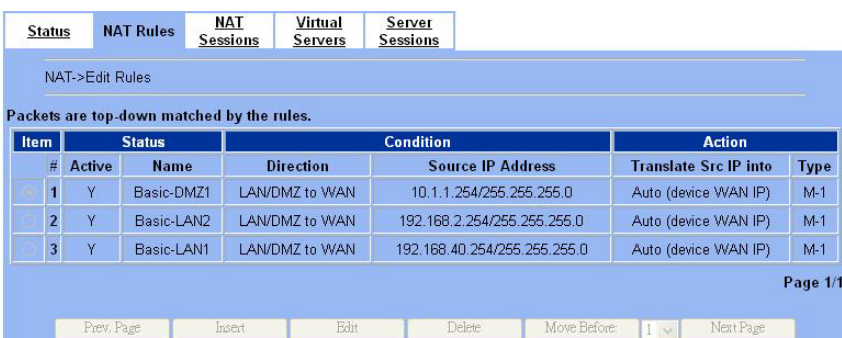
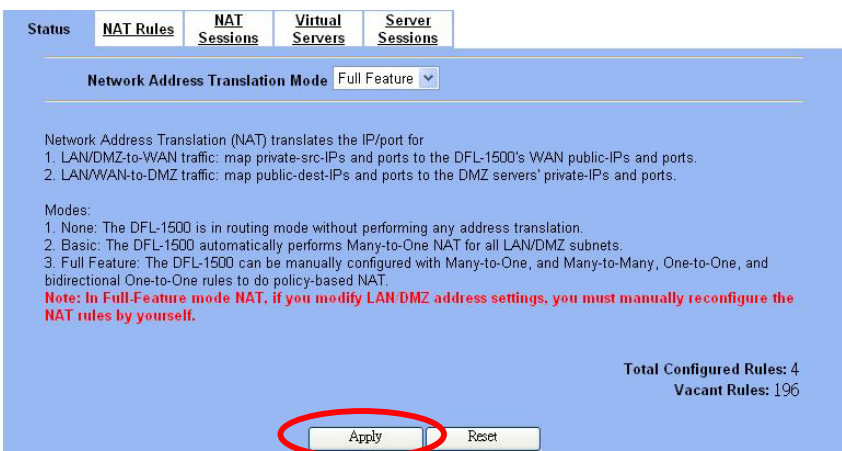
Select the Basic from the list of Network Address Translation Mode. Click Apply. Now the DFL-1500 will automatically set the NAT rules for LAN/DMZ zones. Namely, all internal networks can establish connections to the outside world if the WAN settings are correct.

##### ADVANCED SETTINGS > NAT > Status

Status	NAT Rules	NAT Sessions	Virtual Servers	Server Sessions
<p><b>Network Address Translation Mode</b> Basic</p> <p>Network Address Translation (NAT) translates the IP/port for</p> <ol style="list-style-type: none"> <li>1. LAN/DMZ-to-WAN traffic: map private-src-IPs and ports to the DFL-1500's WAN public-IPs and ports.</li> <li>2. LAN/WAN-to-DMZ traffic: map public-dest-IPs and ports to the DMZ servers' private-IPs and ports.</li> </ol> <p>Modes:</p> <ol style="list-style-type: none"> <li>1. None: The DFL-1500 is in routing mode without performing any address translation.</li> <li>2. Basic: The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnets.</li> <li>3. Full Feature: The DFL-1500 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.</li> </ol> <p style="text-align: right;"><b>Total Configured Rules: 4</b> <b>Vacant Rules: 196</b></p> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </p>				

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation Mode	<p>None : The DFL-1500 is in routing mode without performing any address translation.</p> <p>Basic : The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnets.</p> <p>Full Feature : The DFL-1500 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.</p>	Basic

Table 6-1 Determine Network Address Translation Mode

<p><b>Step 2 - Check NAT Rules</b></p> <p>As described in the above, the DFL-1500 has set the three rules for the LAN1, LAN2, and DMZ1 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 automatically reload the new settings. In the Basic mode, you cannot edit the rules in this page.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules</b></p> 
<p><b>Step 3 - Switch the NAT Mode</b></p> <p>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 DFL-1500. 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.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; Status</b></p> 

**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**

The screenshot shows the 'NAT Rules' configuration page. At the top, there are tabs for 'Status', 'NAT Rules', 'NAT Sessions', 'Virtual Servers', and 'Server Sessions'. Below the tabs, there is a breadcrumb 'NAT->Edit Rules' and a note: 'Packets are top-down matched by the rules.' A table lists three NAT rules:

Item #	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	192.168.40.254/255.255.255.0	Auto (device WAN IP)	M-1

At the bottom of the page, there are navigation buttons: 'Prev. Page', 'Insert', 'Edit', 'Delete', 'Move Before: 1', and 'Next Page'. The 'Insert' button is circled in red.

**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 DFL-1500 will automatically determine which WAN IP is to be translated into.

**ADVANCED SETTINGS > NAT > NAT Rules > Insert**

The screenshot shows the 'Insert' form for a new NAT rule. It includes the following fields and options:

- 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, 61.2.1.1, Netmask: 255.255.255.255

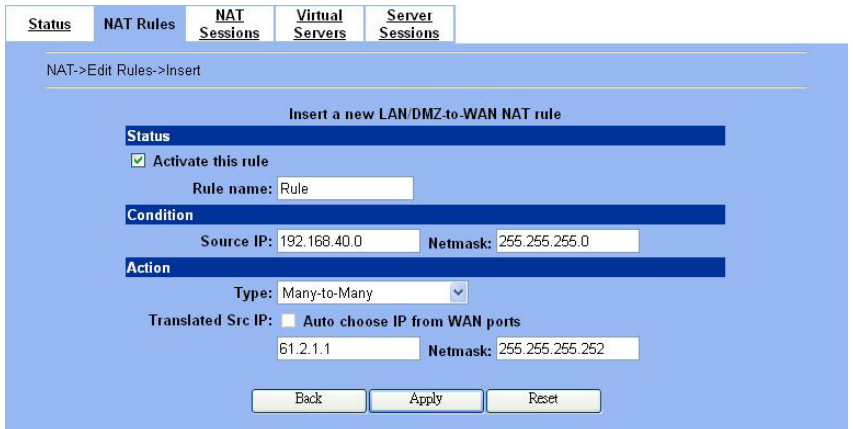

Buttons at the bottom: Back, Apply, Reset.

	FIELD	DESCRIPTION	EXAMPLE
Status	Activate this rule	The NAT rule is enabled or not	enabled
	Rule name	The NAT rule name	Rule
Condition	Source IP / Netmask	Compared with the incoming packets, whether Source IP/Netmask is matched or not.	192.168.40.0 / 255.255.255.0
Action	<b>Type</b>		
	Many-to-One	Map a pool of private IP addresses to a single public IP address chosen from the WAN ports.	Many-to-One
	Many-to-Many	Map a pool of private IP addresses to a pool of public IP addresses chosen from the WAN ports.	
	One-to-One	Map a single private IP address to a single public IP address chosen from the WAN ports.	
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.		



	Translated Src IP	Auto choose IP from WAN ports : Only work in Many-to-One type, the default WAN link is the default source interface for NAT translation. Only when all ports are used, it will use the next NAT interface. Another way is to specify IP address / Netmask by self.	Auto choose IP from WAN ports
--	-------------------	---	-------------------------------

Table 6-2 Add a NAT rule

<p><b>Step 5.b — Insert an Many-to-Many Rule</b></p> <p>If your ISP has assigned a range of public IP to your company, you can tell DFL-1500 to translate the private IP addresses into the pool of public IP addresses. The DFL-1500 will use the first public IP until DFL-1500 uses up all source ports for the public IP. DFL-1500 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 DFL-1500 will no longer choose the device IP for you. It will choose the IP from the address pool you have entered.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules &gt; Insert</b></p> 
<p><b>Step 5.c — Insert an One-to-One Rule</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules &gt; Insert</b></p> 

<p><b>Step 5.d — Insert a One-to-One (Bidirectional) Rule</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules &gt; Insert</b></p>
--	---

How to determine which NAT type is best choice for you. Here we have some suggestions as the following table description.

Type	Usage moment
Many-to-One	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	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 inbound bandwidth. So your inbound and outbound traffic will be more flexible.
One-to-One	If you just wish one local IP address to connect to the internet, and prohibit others to connect to the internet. You can specify the One-to-One type.
One-to-One (bidirectional)	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 traffic forward. Then you can finish the settings. Be careful to use this type, or it will endanger your network security.

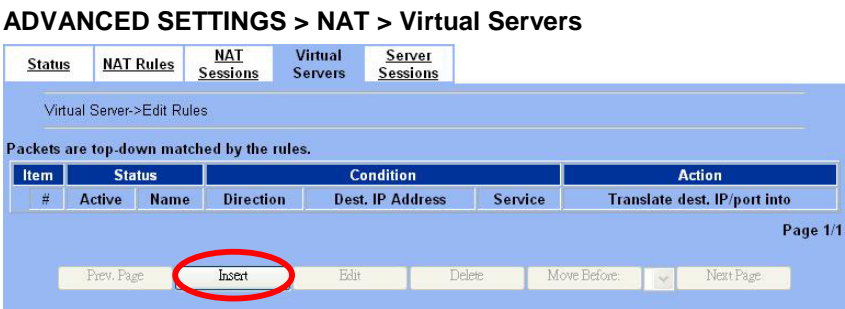
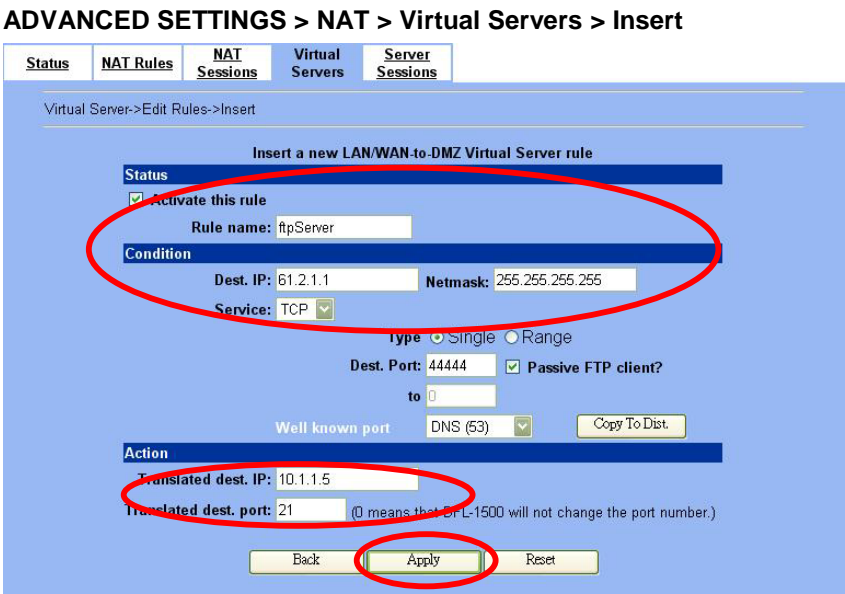
Table 6-3 The NAT type comparison

<p><b>Step 6 - View the LAN to WAN Sessions</b></p> <p>Click the NAT Sessions to see the sessions between LAN to WAN.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Sessions</b></p> <table border="1"> <thead> <tr> <th rowspan="2">Item</th> <th colspan="2">Local Client</th> <th colspan="2">DFL-1500</th> <th colspan="2">Remote Server</th> </tr> <tr> <th>IP Address</th> <th>Port</th> <th>IP Address</th> <th>Port</th> <th>IP Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>192.168.10.1</td> <td>N/A</td> <td>192.168.10.1</td> <td>N/A</td> <td>192.168.20.1</td> <td>N/A</td> </tr> <tr> <td>2</td> <td>192.168.10.1</td> <td>68</td> <td>192.168.10.1</td> <td>68</td> <td>192.168.20.254</td> <td>67</td> </tr> <tr> <td>3</td> <td>192.168.10.1</td> <td>N/A</td> <td>192.168.17.201</td> <td>N/A</td> <td>192.169.20.1</td> <td>N/A</td> </tr> </tbody> </table>	Item	Local Client		DFL-1500		Remote Server		IP Address	Port	IP Address	Port	IP Address	Port	1	192.168.10.1	N/A	192.168.10.1	N/A	192.168.20.1	N/A	2	192.168.10.1	68	192.168.10.1	68	192.168.20.254	67	3	192.168.10.1	N/A	192.168.17.201	N/A	192.169.20.1	N/A
Item	Local Client		DFL-1500		Remote Server																														
	IP Address	Port	IP Address	Port	IP Address	Port																													
1	192.168.10.1	N/A	192.168.10.1	N/A	192.168.20.1	N/A																													
2	192.168.10.1	68	192.168.10.1	68	192.168.20.254	67																													
3	192.168.10.1	N/A	192.168.17.201	N/A	192.169.20.1	N/A																													

### 6.4.2 Setup Virtual Server for the FtpServer1

<p><b>Step 1 - Device IP Address</b></p> <p>Setup the IP Address and IP Subnet Mask for the DFL-1500 of the DMZ1 interface.</p>	<p><b>BASIC SETUP &gt; DMZ Settings &gt; DMZ1 Status</b></p>
---	--

<p><b>Step 2 - Client IP Range</b></p> <p>Enable the DHCP server if you want to use DFL-1500 to assign IP addresses to the computers under DMZ1. Here we make the DHCP feature enabled.</p>																													
<p><b>Step 3 - Apply the Changes</b></p> <p>Click Apply to save your settings.</p>	<p><b>Step 4 - Check NAT Status</b></p> <p>The default setting of NAT is in Basic Mode. After applying the Step 3, the NAT is automatically configured with three rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; Status</b></p> <p>Network Address Translation (NAT) translates the IP/port for</p> <ol style="list-style-type: none"> <li>LAN/DMZ-to-WAN traffic: map private-src-IPs and ports to the DFL-1500's WAN public-IPs and ports.</li> <li>LAN/WAN-to-DMZ traffic: map public-dest-IPs and ports to the DMZ servers' private-IPs and ports.</li> </ol> <p>Modes:</p> <ol style="list-style-type: none"> <li>None: The DFL-1500 is in routing mode without performing any address translation.</li> <li>Basic: The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnets.</li> <li>Full Feature: The DFL-1500 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.</li> </ol> <p>Total Configured Rules: 3 Vacant Rules: 197</p>																											
<p><b>Step 5 - Check NAT Rules</b></p> <p>The DFL-1500 has added three NAT rules. 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.</p>	<p><b>ADVANCED SETTINGS &gt; NAT &gt; NAT Rules</b></p> <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th>Name</th> <th>Direction</th> <th>Condition</th> <th>Action</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>Basic-DMZ1</td> <td>LAN/DMZ to WAN</td> <td>10.1.1.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Basic-LAN2</td> <td>LAN/DMZ to WAN</td> <td>192.168.2.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>3</td> <td>Y</td> <td>Basic-LAN1</td> <td>LAN/DMZ to WAN</td> <td>192.168.40.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> </tbody> </table>	Item	Status	Name	Direction	Condition	Action	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	192.168.40.254/255.255.255.0	Auto (device WAN IP)	M-1
Item	Status	Name	Direction	Condition	Action	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	192.168.40.254/255.255.255.0	Auto (device WAN IP)	M-1																							
<p><b>Step 6 - Setup IP for the FTP Server</b></p> <p>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).</p>																													

<p><b>Step 7 - Setup Server Rules</b></p> <p>Insert a virtual server rule by clicking the Insert button.</p>	 <p>ADVANCED SETTINGS &gt; NAT &gt; Virtual Servers</p> <p>Virtual Server-&gt;Edit Rules</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th>Item #</th> <th>Status</th> <th>Name</th> <th>Direction</th> <th>Dest. IP Address</th> <th>Service</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Translate dest. IP/port into</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page <b>Insert</b> Edit Delete Move Before: Next Page</p>	Item #	Status	Name	Direction	Dest. IP Address	Service	Action							Translate dest. IP/port into
Item #	Status	Name	Direction	Dest. IP Address	Service	Action									
						Translate dest. IP/port into									
<p><b>Step 8 - Customize the Rule</b></p> <p>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 DFL-1500 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 DFL-1500 will translate the private IP/port into an IP/port of its own. Thus the problem is gracefully solved. Click Apply to proceed.</p>	 <p>ADVANCED SETTINGS &gt; NAT &gt; Virtual Servers &gt; Insert</p> <p>Virtual Server-&gt;Edit Rules-&gt;Insert</p> <p>Insert a new LAN/WAN-to-DMZ Virtual Server rule</p> <p><input checked="" type="checkbox"/> Activate this rule</p> <p>Rule name: ftpServer</p> <p>Condition</p> <p>Dest. IP: 61.2.1.1 Netmask: 255.255.255.255</p> <p>Service: TCP</p> <p>Type: <input checked="" type="radio"/> Single <input type="radio"/> Range</p> <p>Dest. Port: 44444 <input checked="" type="checkbox"/> Passive FTP client?</p> <p>to 0</p> <p>Well known port: DNS (53) Copy To Dist.</p> <p>Action</p> <p>Translated dest. IP: 10.1.1.5</p> <p>Translated dest. port: 21 (0 means that DFL-1500 will not change the port number.)</p> <p>Back <b>Apply</b> Reset</p>														

	FIELD	DESCRIPTION	EXAMPLE
Status	Activate this rule	The Virtual Server rule is enabled or not	enabled
	Rule name	The Virtual Server rule name	ftpServer
Condition	Dest IP / Netmask	The public IP address and IP netmask of the Virtual Server.	61.2.1.1 / 255.255.255.255
	Service	Any, TCP or UDP	TCP
	Type	Port is Single or Range	Single
	Dest Port	The port number in the internet.	44444
	Passive FTP client	If the Passive FTP client is checked, it will connect to the internal DMZ FTP server of DFL-1500 when FTP client uses passive mode. Otherwise, it will not work.	enabled
Action	Translated dest IP	The IP address which is actually transferred to the internal DMZ	10.1.1.5
	Translated dest port	The port number which is actually transferred to the internal DMZ.	21

Table 6-4 Add a Virtual Server rule

**Step 9 - View the Result**  
 Now any request towards the DFL-1500'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.

**ADVANCED SETTINGS > NAT > Virtual Servers**

Status NAT Rules NAT Sessions Virtual Servers Server Sessions

Virtual Server->Edit Rules

Packets are top-down matched by the rules.

Item	Status	Name	Direction	Condition	Action
1	Y	ftpServer	LAN/WAN to DMZ	Dest. IP Address: 61.2.1.1/255.255.255.255 Service: TCP:44444	Translate dest. IP/port into: 10.1.1.5:21

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**Step 10 - View the WAN to LAN Sessions**  
 Click the Server Sessions to see the sessions between WAN to LAN.

**ADVANCED SETTINGS > NAT > Server Sessions**

Status NAT Rules NAT Sessions Virtual Servers Server Sessions

Virtual Server->Sessions

Refresh

Item	Local Server		DFL-1500		Remote Client		
	#	IP Address	Port	IP Address	Port	IP Address	Port
1		10.1.30.1	80	192.168.17.203	80	192.168.17.170	1856
2		10.1.30.1	80	192.168.17.203	80	192.168.17.170	1855
3		10.1.30.1	80	192.168.17.203	80	192.168.17.170	1722
4		10.1.30.1	80	192.168.17.203	80	192.168.17.170	1673



# Chapter 7

## Routing

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

To facilitate the explanation on how DFL-1500 implements routing and how to use it, we zoom in the left part of Figure 2-1 into Figure 7-1

### 7.1 Demands

1. The bandwidth subscribed from ISP1 is insufficient so that some important traffic, say traffic towards the subnet 140.116.53.0/255.255.255.0, is blocked by the other traffic.
2. 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.

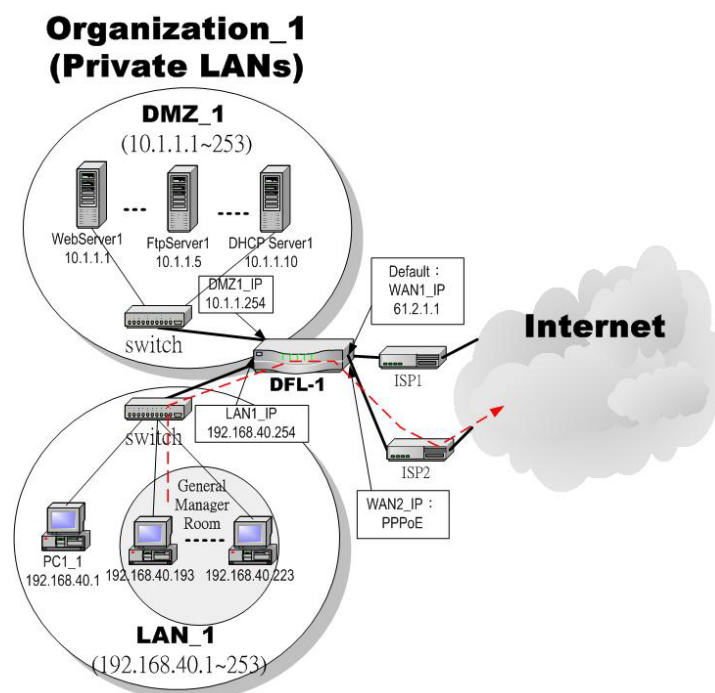


Figure 7-1 Add policy routing entry for the General-Manager-Room department

### 7.2 Objectives

1. The network administrator plans to solve the problem by subscribing the second link (ISP2). He/She wires the ISP2 to the WAN2 socket of the DFL-1. Now there are two WAN links connected to the DFL-1. He/she hopes that all the packets destined to the subnet 140.116.53.0/255.255.255.0 will pass through the WAN2 link instead of the default WAN1 link. In such a way, the WAN2 link can offload the traffic.
2. The same as the above. However, routing table can only be specified by destinations. That is, routing table can only direct some packets “destined to” somewhere through some link. It cannot direct some packets “from” somewhere through some



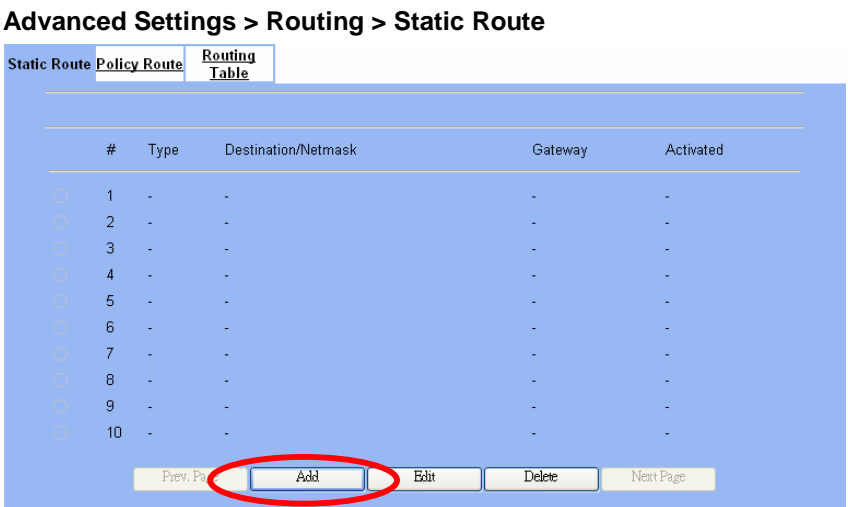
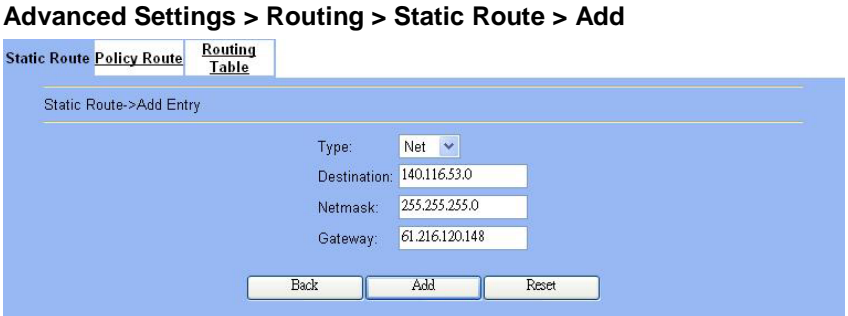
link. The policy route can solve this problem. He/she hopes that all the packets from the General-Manager-Room will pass through the WAN2 link instead of the default WAN1 link.

### 7.3 Methods

1. Add a static routing entry to direct the packets towards 140.116.53.0/255.255.255.0 through the WAN2 link.
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 WAN2 link.

### 7.4 Steps

#### 7.4.1 Add a static routing entry

<p><b>Step 1 - Add a static routing entry</b> Click the Add button to the next process.</p>	 <p>Advanced Settings &gt; Routing &gt; Static Route</p> <p>Static Route Policy Route Routing Table</p> <table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Destination/Netmask</th> <th>Gateway</th> <th>Activated</th> </tr> </thead> <tbody> <tr><td>1</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>2</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>3</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>4</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>5</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>6</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>7</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>8</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>9</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>10</td><td>-</td><td>-</td><td>-</td><td>-</td></tr> </tbody> </table> <p>Prev. Page <b>Add</b> Edit Delete Next Page</p>	#	Type	Destination/Netmask	Gateway	Activated	1	-	-	-	-	2	-	-	-	-	3	-	-	-	-	4	-	-	-	-	5	-	-	-	-	6	-	-	-	-	7	-	-	-	-	8	-	-	-	-	9	-	-	-	-	10	-	-	-	-
#	Type	Destination/Netmask	Gateway	Activated																																																				
1	-	-	-	-																																																				
2	-	-	-	-																																																				
3	-	-	-	-																																																				
4	-	-	-	-																																																				
5	-	-	-	-																																																				
6	-	-	-	-																																																				
7	-	-	-	-																																																				
8	-	-	-	-																																																				
9	-	-	-	-																																																				
10	-	-	-	-																																																				
<p><b>Step 2 - Fill out the related field</b> Fill in the destination and the netmask field with 140.116.53.0 and 255.255.255.0. Assign the next hop Gateway as 61.216.120.148 (the WAN2 IP address). Click Add to proceed.</p>	 <p>Advanced Settings &gt; Routing &gt; Static Route &gt; Add</p> <p>Static Route Policy Route Routing Table</p> <p>Static Route-&gt;Add Entry</p> <p>Type: Net</p> <p>Destination: 140.116.53.0</p> <p>Netmask: 255.255.255.0</p> <p>Gateway: 61.216.120.148</p> <p>Back Add Reset</p>																																																							

FIELD	DESCRIPTION	EXAMPLE
Type	Determine this static routing entry record is multiple hosts (Net) or a single host (Host).	Net
Destination	The destination IP address of this static routing entry record.	140.116.53.0
Netmask	The destination IP Netmask of this static routing entry record.	255.255.255.0
Gateway	The default gateway of this static routing entry record.	61.216.120.148

Table 7-1 Add 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**

Static Route Policy Route Routing Table

#	Type	Destination/Netmask	Gateway	Activated
1	Net	140.116.53.0/255.255.255.0	61.216.120.148	Yes
2	-	-	-	-
3	-	-	-	-
4	-	-	-	-
5	-	-	-	-
6	-	-	-	-
7	-	-	-	-
8	-	-	-	-
9	-	-	-	-
10	-	-	-	-

Prev. Page Add Edit Delete Next Page

**7.4.2 Add a policy routing entry**

**Step 1 - Insert a policy routing entry**

Click Insert button to add a policy routing entry.

**Advanced Settings > Routing > Policy Route**

Static Route Policy Route Routing Table

Policy Routing->Edit Rules

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page **Insert** Edit Delete Move Before: Next Page

**Step 2 - 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 the rule is enabled. Rule name field fill in GenlManaRoom. 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 WAN2 with next-hop gateway 61.216.120.148. 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**

Static Route Policy Route Routing Table

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

**Action**

Forward to WAN2 with next-hop gateway IP 61.216.120.148

Back Apply Reset

	FIELD	DESCRIPTION	EXAMPLE
Status	Activate this rule	The policy routing rule is enabled or not.	enabled
	Rule name	The policy routing rule name.	GenlManaRoom
Condition	Incoming packets from	Packets comes from which interface	LAN1
	Source IP & Netmask	Verify if the incoming packets belong to the range of the Source IP/Netmask in the policy routing rule.	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.	0.0.0.0 / 0.0.0.0
	Service	Verify what is the service of this packet?	Any
	Configure src. port? Type Src. port	Check the source port of the incoming packets. If checked, what is the range of the port?	No
	Configure dest. port? Type Dest. port	Check the dest port of the incoming packets. If checked, what is the range of the port?	No
Action	Forward to	If the packet is matched to this rule, which interface does this packet sent out to?	WAN2
	Nexthop gateway IP	The next gateway IP address of forwarding interface.	61.216.120.148

Table 7-2 Add a policy routing entry

<p><b>Step 3 - View the result</b></p> <p>After filling data completely, view the policy routing entries which have been set.</p>	<p><b>Advanced Settings &gt; Routing &gt; Policy Route</b></p> <p>Static Route Policy Route <b>Routing Table</b></p> <p>Policy Routing-&gt;Edit Rules</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th rowspan="2">#</th> <th colspan="2">Status</th> <th colspan="4">Condition</th> <th colspan="2">Action</th> </tr> <tr> <th>Active</th> <th>Name</th> <th>Direction</th> <th>Source IP Address</th> <th>Dest. IP Address</th> <th>Service</th> <th>Forward to next-hop</th> <th>Through</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>GenlManaRoom</td> <td>From LAN1</td> <td>192.168.40.192/255.255.255.192</td> <td>Any</td> <td>Any</td> <td>61.216.120.148</td> <td>WAN2</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page Insert Edit Delete Move Before: 1 Next Page</p>	#	Status		Condition				Action		Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Forward to next-hop	Through	1	Y	GenlManaRoom	From LAN1	192.168.40.192/255.255.255.192	Any	Any	61.216.120.148	WAN2														
#	Status		Condition				Action																																		
	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Forward to next-hop	Through																																	
1	Y	GenlManaRoom	From LAN1	192.168.40.192/255.255.255.192	Any	Any	61.216.120.148	WAN2																																	
<p><b>Step 4 - Show the routing table</b></p> <p>Finally click the "Routing Table" to see all the current routing table information.</p>	<p><b>Advanced Settings &gt; Routing &gt; Routing Table</b></p> <p>Static Route Policy Route <b>Routing Table</b></p> <table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Destination/Netmask</th> <th>Gateway</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Default/Static</td> <td>0.0.0.0/0.0.0.0</td> <td>192.168.17.253</td> <td>WAN1</td> </tr> <tr> <td>2</td> <td>Net</td> <td>10.1.1.0/255.255.255.0</td> <td>10.1.1.254</td> <td>DMZ1</td> </tr> <tr> <td>3</td> <td>PPP</td> <td>61.216.104.254/255.255.255.255</td> <td>61.216.104.26</td> <td>WAN2</td> </tr> <tr> <td>4</td> <td>Gateway/Static</td> <td>140.116.53.0/255.255.255.0</td> <td>61.216.120.148</td> <td>WAN1</td> </tr> <tr> <td>5</td> <td>Net</td> <td>192.168.1.0/255.255.255.0</td> <td>192.168.1.254</td> <td>LAN1</td> </tr> <tr> <td>6</td> <td>Net</td> <td>192.168.2.0/255.255.255.0</td> <td>192.168.2.254</td> <td>LAN2</td> </tr> <tr> <td>7</td> <td>Net</td> <td>192.168.17.0/255.255.255.0</td> <td>192.168.17.204</td> <td>WAN1</td> </tr> </tbody> </table> <p>Refresh</p>	#	Type	Destination/Netmask	Gateway	Interface	1	Default/Static	0.0.0.0/0.0.0.0	192.168.17.253	WAN1	2	Net	10.1.1.0/255.255.255.0	10.1.1.254	DMZ1	3	PPP	61.216.104.254/255.255.255.255	61.216.104.26	WAN2	4	Gateway/Static	140.116.53.0/255.255.255.0	61.216.120.148	WAN1	5	Net	192.168.1.0/255.255.255.0	192.168.1.254	LAN1	6	Net	192.168.2.0/255.255.255.0	192.168.2.254	LAN2	7	Net	192.168.17.0/255.255.255.0	192.168.17.204	WAN1
#	Type	Destination/Netmask	Gateway	Interface																																					
1	Default/Static	0.0.0.0/0.0.0.0	192.168.17.253	WAN1																																					
2	Net	10.1.1.0/255.255.255.0	10.1.1.254	DMZ1																																					
3	PPP	61.216.104.254/255.255.255.255	61.216.104.26	WAN2																																					
4	Gateway/Static	140.116.53.0/255.255.255.0	61.216.120.148	WAN1																																					
5	Net	192.168.1.0/255.255.255.0	192.168.1.254	LAN1																																					
6	Net	192.168.2.0/255.255.255.0	192.168.2.254	LAN2																																					
7	Net	192.168.17.0/255.255.255.0	192.168.17.204	WAN1																																					

# Chapter 8 Firewall

*This chapter introduces firewall and explains how to implement it.*

## 8.1 Demands

1. 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.
2. A DMZ server was attacked by SYN-Flooding attack and requires the DFL-1500 to protect it.

## 8.2 Objectives

1. Block the traffic from PC1\_1 in LAN1 to the Internet in WAN1.
2. Start the SYN-Flooding protection.

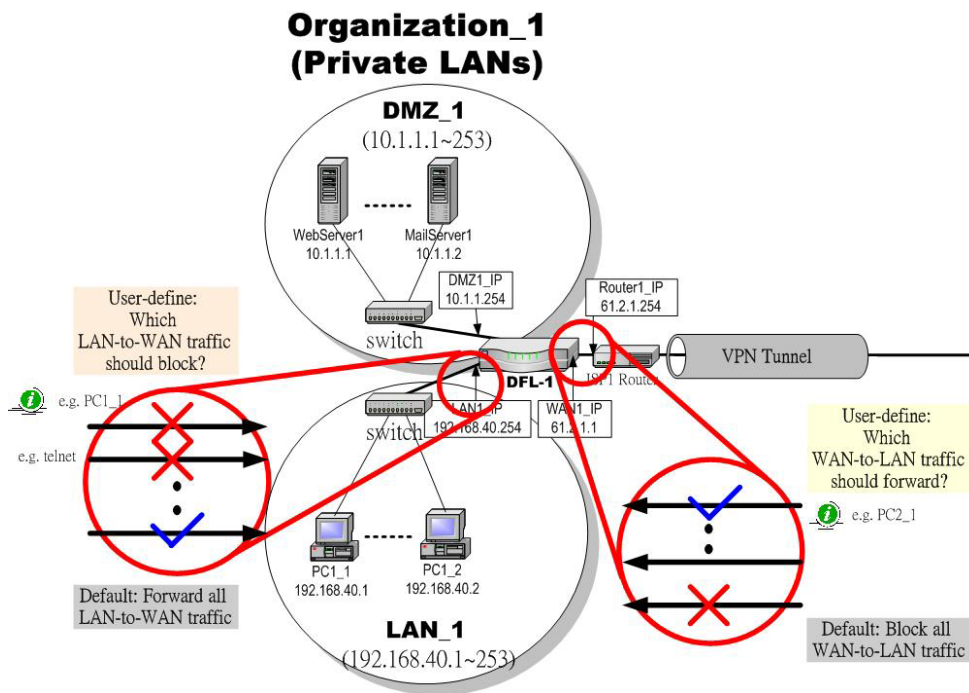


Figure 8-1 Setting up the firewall rule

## 8.3 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.

## 8.4 Steps


### 8.4.1 Block internal PC session (LAN → WAN)

<p><b>Step 1 - Setup NAT</b></p> <p>Check the <b>Enable Stateful Inspection Firewall</b> checkbox, and click the <b>Apply</b>.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Status</b></p> <p>Status   Edit Rules   Show Rules   Attack Alert   Summary</p> <p><input checked="" type="checkbox"/> <b>Enable Stateful Inspection Firewall</b></p> <p>The firewall protects against Denial of Service (DoS) attacks when it is enabled.</p> <p>Total Configured Rules: 26 Vacant Rules: 2974</p> <p>Apply   Reset</p>																											
<p><b>Step 2 - Add a Firewall Rule</b></p> <p>Select LAN1 to WAN1 traffic direction. The default action of this direction is to forward all traffic without logging anything. Click <b>Insert</b> to add a Firewall block rule before the default rule to stop the bad traffic.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Edit Rules</b></p> <p>Status   Edit Rules   Show Rules   Attack Alert   Summary</p> <p>Firewall-&gt;Edit Rules</p> <p>Edit LAN1 to WAN1 rules</p> <p>Default action for this packet direction: Forward <input type="checkbox"/> Log Apply</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th colspan="5">Condition</th> <th colspan="2">Action</th> </tr> <tr> <th>#</th> <th>Active</th> <th>Name</th> <th>Direction</th> <th>Source IP Address</th> <th>Dest. IP Address</th> <th>Service</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>Default</td> <td>LAN1 to WAN1</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Forward</td> <td>N</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page   Insert   Edit   Delete   Move Before: 1   Next Page</p>	Item	Status	Condition					Action		#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log	1	Y	Default	LAN1 to WAN1	Any	Any	Any	Forward	N
Item	Status	Condition					Action																					
#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log																				
1	Y	Default	LAN1 to WAN1	Any	Any	Any	Forward	N																				
<p><b>Step 3 - Customize the rule</b></p> <p>Check the <b>Activate this rule</b> checkbox. Enter the rule name as <b>PC1_1</b>, and enter the IP address of <b>PC1_1</b> (192.168.40.1 / 255.255.255.255). Select <b>Block</b> and <b>Log</b> to block and log the matched traffic. Click the <b>Apply</b> to apply the changes.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Edit Rules &gt; Insert</b></p> <p>Status   Edit Rules   Show Rules   Attack Alert   Summary</p> <p>Firewall-&gt;Edit Rules-&gt;Insert</p> <p>Insert a new WAN1-to-WAN1 Firewall rule</p> <p><b>Status</b></p> <p><input checked="" type="checkbox"/> <b>Activate this rule</b></p> <p>Rule name: PC1_1</p> <p><b>Condition</b></p> <p>Source IP: 192.168.40.1 Netmask: 255.255.255.255</p> <p>Dest. IP: 0.0.0.0 Netmask: 0.0.0.0</p> <p>Service: Any</p> <p>Configure dest. port? <input type="checkbox"/></p> <p>Type: Single Range</p> <p>Dest. Port: 0 to 0</p> <p>Well known port: FTP (21) Copy To Dist.</p> <p><b>Action</b></p> <p>Block the matched packet.</p> <p>Log the matched packet.</p> <p>Back   Apply   Reset</p>																											

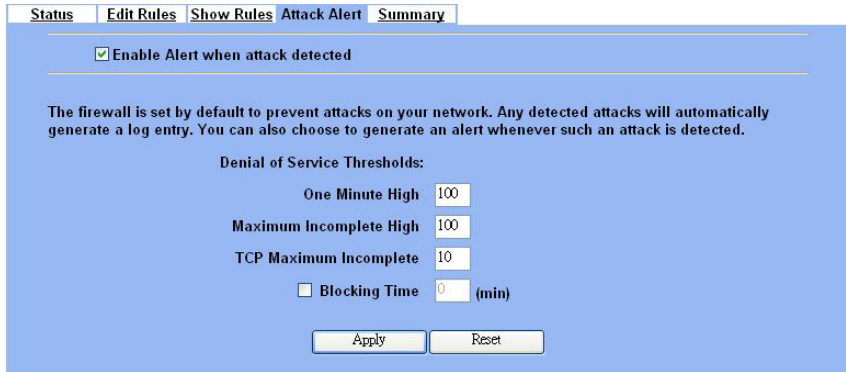
	FIELD	DESCRIPTION	EXAMPLE
Status	Activate this rule	Enable the firewall rule for later using	enabled
	Rule name	The name of the Firewall rule	PC1_1
Condition	Source IP & Netmask	Compared with the incoming packets, whether Source IP/Netmask is matched or not.	192.168.40.1 255.255.255.255

	Dest IP & Netmask	Compared with the incoming packets, whether Dest IP/Netmask is matched or not.	0.0.0.0 0.0.0.0.
	Service	Verified the service of packet is belong to each TCP、UDP、ICMP.	Any
Action	Forward / Block the matched packet	If packet is matched the rule condition, Forward or Block this matched packet?	Block
	Don't log / Log the matched packet	If packet is matched the rule condition, Log or Don't log this matched packet?	Log

Table 8-1 Insert a Firewall rule

<p><b>Step 4 - View the Firewall Log</b></p> <p>You can go to DEVICE Status&gt;Firewall Logs &gt;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.</p>	<p><b>DEVICE Status &gt; Firewall Logs &gt; Firewall Logs</b></p>  <p>The screenshot shows a web interface for viewing firewall logs. It has a title bar 'DEVICE Status &gt; Firewall Logs &gt; Firewall Logs'. Below the title are two tabs: 'Firewall Logs' (selected) and 'Alert Logs'. A table displays log entries with columns: No., Time, From, To, Protocol, Direction, and Action. The table contains 5 rows of data. Below the table are navigation buttons: 'Download To Local', 'Prev. Page', 'Refresh', 'Clear', 'Next Page', and a 'List' dropdown set to 'MAX'. At the bottom right, it says 'Per Page Page: 1/1'.</p>
--	---

**8.4.2 Setup Alert detected attack**

<p><b>Step 1 - Setup Attack Alert</b></p> <p>With the Firewall enabled, the DFL-1500 is already equipped with an Anti-DoS engine within it. 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 Alert when attack detected checkbox. Enter 100 in the One Minute High means that DFL-1500 starts to generate alerts and delete the half-open states if 100 half-open states are established in the last minute. Enter 100 in the Maximum Incomplete High means that DFL-1500 starts to generate alerts and delete half-open states if the current number of half-open states reaches 100. Enter 10 in the TCP Maximum Incomplete means that DFL-1500 starts to generate alerts and delete half-open states if the number of half-open states towards a server (SYN-Flooding attack) reaches 10. Check the Blocking time if you want to stop the traffic towards the server. During this blocking time, the server can digest the loading.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Attack Alert</b></p>  <p>The screenshot shows the 'Attack Alert' configuration page. It has a title bar 'ADVANCED SETTINGS &gt; Firewall &gt; Attack Alert'. Below the title are tabs: 'Status', 'Edit Rules', 'Show Rules', 'Attack Alert' (selected), and 'Summary'. A checkbox 'Enable Alert when attack detected' is checked. Below this is a text block: 'The firewall is set by default to prevent attacks on your network. Any detected attacks will automatically generate a log entry. You can also choose to generate an alert whenever such an attack is detected.' Underneath is a section 'Denial of Service Thresholds:' with several input fields: 'One Minute High' (100), 'Maximum Incomplete High' (100), 'TCP Maximum Incomplete' (10), and 'Blocking Time' (0 min). At the bottom are 'Apply' and 'Reset' buttons.</p>
--	---

FIELD	DESCRIPTION	EXAMPLE
Enable Alert when attack detected	Enable the firewall alert to detect Denial of Service (DoS) attack.	Enabled

Denial of Service Thresholds		
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half open sessions. When the rate of new connection attempts rises above this number, the DFL-1500 deletes half-open sessions as required to accommodate new connection attempts.	100
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the DFL-1500 deletes half-open sessions as required to accommodate new connection requests.	100
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10
Blocking Time	When TCP Maximum Incomplete is reached you can choose if the next session should be allowed or blocked. If you check Blocking Time any new sessions will be blocked for the length of time you specified in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as will give the server some time to digest the loading.	disabled
(min)	Enter the length of Blocking Time in minutes.	0

Table 8-2 Setup the Denial of Service Thresholds of attack alert



# Part III

## Virtual Private Network



# Chapter 9

## VPN Technical Introduction

*This chapter introduces VPN related technology*

### 9.1 Terminology Explanation

#### 9.1.1 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.

#### 9.1.2 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.

#### 9.1.3 Security Association

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

#### 9.1.4 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).

#### 9.1.5 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 DFL-1500. 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).

## 9.1.6 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.

### 9.1.7 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.

## 9.2 Make VPN packets pass through DFL-1500

### Step 1 - Enable IPSec

If we need to setup DFL-1500 between the existed IPSec / PPTP / L2TP connections. We need to open up the Firewall blocking port of DFL-1500 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 DFL-1500. As well as DFL-1500 will play the middle forwarding device role.

### ADVANCED SETTINGS > VPN Settings > Pass Through

IPSec	PPTP	L2TP	Pass Through
			<input checked="" type="checkbox"/> Enable IPSec pass through <input checked="" type="checkbox"/> Enable PPTP pass through <input checked="" type="checkbox"/> Enable L2TP pass through
IPSec/PPTP/L2TP pass through make the DFL-1500 device as a middle forwarding device between <ol style="list-style-type: none"> <li>1. Two IPSec devices.</li> <li>2. Two PPTP devices.</li> <li>3. Two L2TP devices.</li> </ol>			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			



# Chapter 10

## 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 10-1 is the real structure in our implemented process.

### 10.1 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.

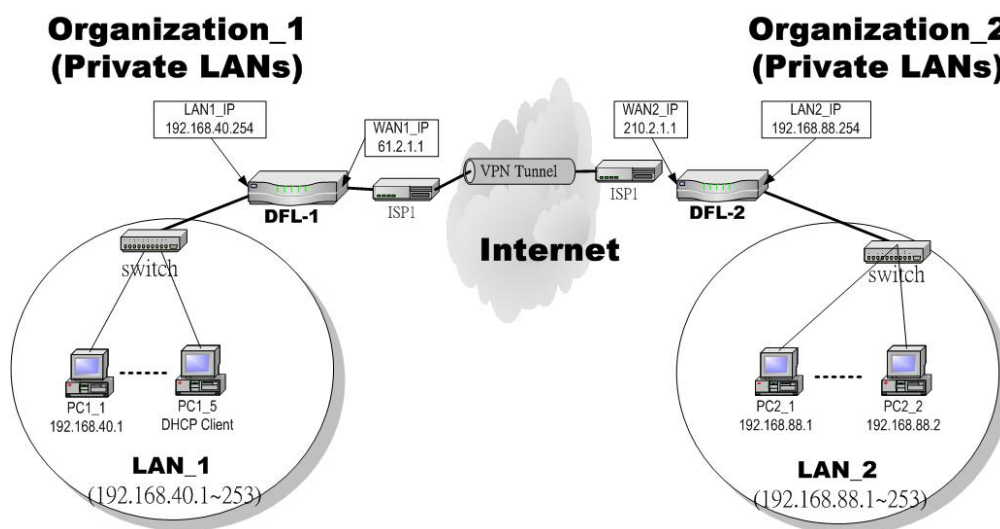


Figure 10-1 Organization\_1 LAN\_1 is making VPN tunnel with Organization\_2 LAN\_2

### 10.2 Objectives

1. Let the users in LAN\_1 and LAN\_2 share the resources through a secure channel established using the public Internet.

### 10.3 Methods

1. Separately configure DFL-1 and DFL-2 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 “Security Gateway Address” means the WAN IP address of the other VPN gateway.	

Difference	The “Pre-Shared Key” must be the same at both DFL-1500s.	The types and keys of “Encryption” and “Authenticate” must be set the same on both DFL-1500s. However, the “Outgoing SPI” at DFL-1 must equal to “Incoming SPI” at DFL-2, and the “Outgoing SPI” at DFL-2 must equal to “Incoming SPI” at DFL-1.
------------	--	--

Table 10-1 Compared IKE and Manual Key methods

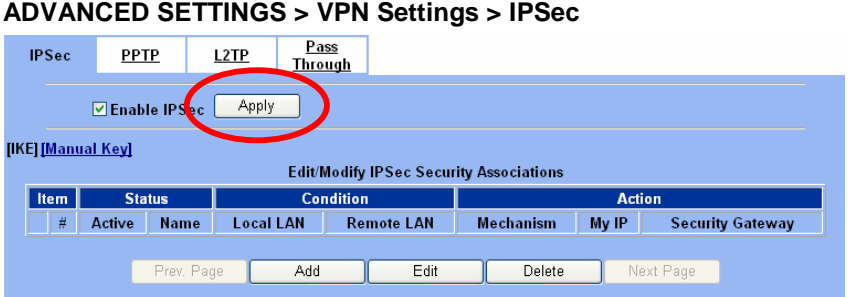
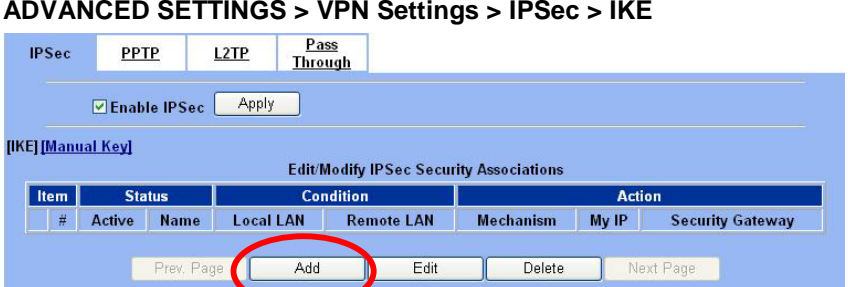
## 10.4 Steps

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 DFL-1:

At the first, we will install the IPsec properties of DFL-1.

<p><b>Step 1 - Enable IPsec</b></p> <p>Check the <code>Enable IPsec</code> checkbox and click <code>Apply</code>.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPsec</b></p> 
<p><b>Step 2 - Add an IKE rule</b></p> <p>Click the <code>IKE</code> hyperlink and click <code>Add</code> to add a new IPsec VPN tunnel endpoint.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPsec &gt; IKE</b></p> 

**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). Enter the My IP Address as the public IP address of this Firewall/VPN Router (61.2.1.1). Enter the public IP of the opposite-side VPN gateway (210.2.1.1) in the Security Gateway Addr. 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**

The screenshot shows the configuration page for an IKE rule. At the top, there are tabs for 'IPSec', 'PPTP', and 'L2TP', with 'IPSec' selected. Below the tabs, the breadcrumb path 'IPSec->IKE->Edit Rule' is visible. The main configuration area is divided into three sections: 'Status', 'Condition', and 'Action'.  
 - **Status:** Includes a checked 'Active' checkbox and an 'IKE Rule Name' field containing 'IKErule'.  
 - **Condition:** Contains 'Local Address Type' (Subnet Address), 'Local Address' (IP Address: 192.168.40.0, PrefixLen / Subnet Mask: 255.255.255.0), and 'Remote Address Type' (Subnet Address), 'Remote Address' (IP Address: 192.168.88.0, PrefixLen / Subnet Mask: 255.255.255.0).  
 - **Action:** Includes 'Negotiation Mode' (Main), 'Encapsulation Mode' (Tunnel), 'My IP Address' (61.2.1.1), and 'Security Gateway Addr' (210.2.1.1).  
 Below these sections, there are radio buttons for 'ESP Algorithm' (selected, Encrypt and Authenticate (DES, MD5)) and 'AH Algorithm' (Authenticate (MD5)). A 'Pre-Shared Key' field contains '1234567890'. At the bottom, there are 'Advanced', 'Back', 'Apply', and 'Reset' buttons.

	FIELD	DESCRIPTION	EXAMPLE
Status	Active	This field will activate this IPSec policy rule	enabled
	IKE Rule Name	The name of this IPSec policy	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
	IP Address	The local IP address	192.168.40.0
	Prefix Len/Subnet Mask	The local IP Netmask	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
	IP Address	The remote IP address	192.168.88.0
	Prefix Len/Subnet Mask	The remote IP Netmask	255.255.255.0
Action	Negotiation Mode	Choose Main or Aggressive mode, see Chapter 9 for details.	Main
	Encapsulation Mode	Choose Tunnel or Transport mode, see Chapter 9 for details.	Tunnel
	My IP Address	The IP address of local site DFL-1500 Firewall/VPN Router	61.2.1.1
	Security Gateway Addr	The IP address of remote site device, like DFL-1500 Firewall/VPN Router.	210.2.1.1

ESP Algorithm	<p>ESP Algorithm may be grouped by the items of the Encryption and Authentication Algorithms or execute separately.</p> <p>We can select below items, the Encryption and Authentication Algorithm combination or the below item Authentication Algorithm singly.</p> <p>Here Encryption Algorithms include DES, 3DES and AES Authentication Algorithms include MD5 and SHA1</p>	Encrypt and Authenticate (DES, MD5)
AH Algorithm	Select Authentication Algorithm (MD5 or SHA1)	disabled
Pre-Shared Key	The key which is pre-shared with remote side.	1234567890

Table 10-2 Related field explanation of adding a 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 10-3 indicated to finish these settings.

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

	FIELD	DESCRIPTION	EXAMPLE
Condition	Local to Remote Protocol / Src Port / Dest Port	Utilize this field to select some packets which are destined for a specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from local to remote.	TCP / 0 / 80



	Remote to Local Protocol / Src Port / Dest Port	Utilize this field to select some packets which are destined for specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from remote to local.	ANY / 0 / 0
Action	Enable Replay Detection	Whether is the “Replay Detection” enabled?	NO
	<b>Phase1</b>		
	Negotiation Mode	Choose Main or Aggressive mode, see Chapter 9 for details.	Main
	Pre-Shared Key	View only, it is set previously and can not be edited again.	ESP
	Encryption Algorithm	Choose an encryption and authentication algorithm.	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 9 for details.	28800 sec
	Key Group	Choose a Diffie-Hellman public-key cryptography key group	DH1
	<b>Phase2</b>		
	Encapsulation	View only, it is set previously and can not be edited again.	Tunnel
	Active Protocol	View only, it is set previously and can not be edited again.	ESP
	Encryption Algorithm	Choose an encryption and authentication algorithm.	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 9 for details.	28800 sec
Perfect Forward Secrecy(PFS)	Enabling PFS means that the key is transient. This extra setting will cause more security.	DH1	

Table 10-3 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**

IPSec PPTP L2TP

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.

OK

**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**

Status Edit Rules Show Rules Attack Alert 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	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log
1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**Step 7 - Customize the Firewall rule**  
 Check the Activate this rule. Enter the Rule Name as AllowVPNIKerule, Source IP as 192.168.88.0, and Dest. IP as 192.168.40.0. Click Apply to store this rule.

**ADVANCED SETTINGS > Firewall > Edit Rules > Insert**

Status Edit Rules Show Rules Attack Alert Summary

Firewall->Edit Rules->Insert

Insert a new WAN1-to-WAN1 Firewall rule

Status

Activate this rule

Rule name: AllowVPNIKerule

Condition

Source IP: 192.168.88.0 Netmask: 255.255.255.0

Dest. IP: 192.168.40.0 Netmask: 255.255.255.0

Service: Any

Configure dest. port?

Type: Single Range

Dest. Port: 0 to 0

Well known port: FTP (21) Copy To Dist.

Action

Forward the matched packet.

Don't log the matched packet.

Back Apply Reset

**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 DFL-1500. And accomplish the VPN tunnel establishment.

**ADVANCED SETTINGS > Firewall > Edit Rules**

Status Edit Rules Show Rules Attack Alert 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.

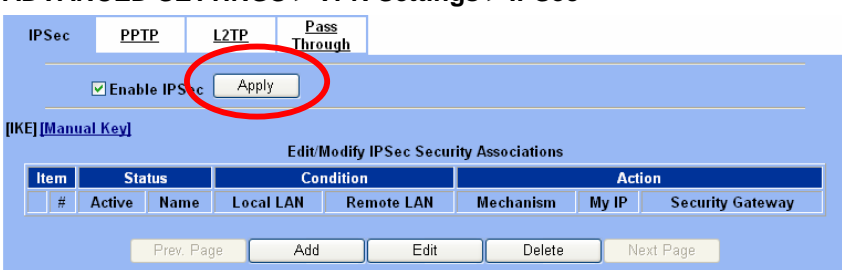
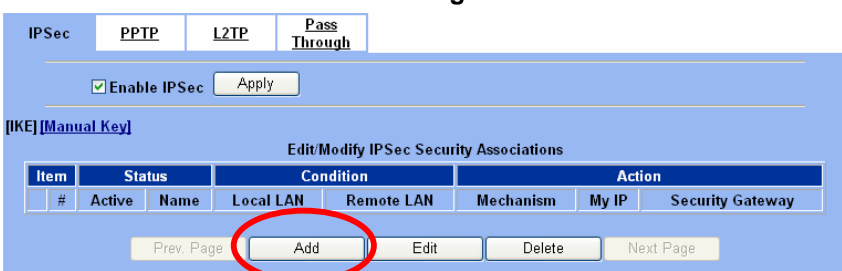
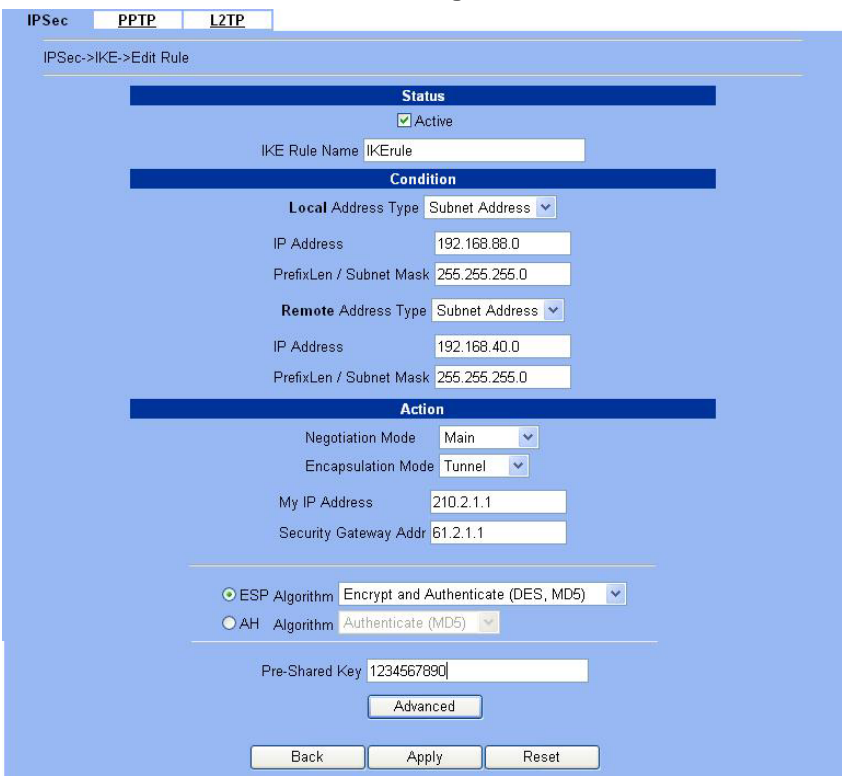
Item #	Status	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log
1	Y	AllowVPNIKerule	WAN1 to LAN1	192.168.88.0/255.255.255.0	192.168.40.0/255.255.255.0	Any	Forward	N
2	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**At DFL-2:**

Here we will install the IPSec properties of DFL-2. Note that the “Local Address” and “Remote address” field are opposite to the DFL-1, and so are “My IP Address” and “Security Gateway Addr” field.

<p><b>Step 1 - Enable IPSec</b></p> <p>Check the Enable IPSec checkbox and click Apply.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPSec</b></p> 
<p><b>Step 2 - Add an IKE rule</b></p> <p>Click the IKE hyperlink and click Add to add a new IPSec VPN tunnel endpoint.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPSec &gt; IKE</b></p> 
<p><b>Step 3 - Customize the rule</b></p> <p>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). Enter the My IP Address as the public IP address of this Firewall/VPN Router (210.2.1.1). Enter the public IP of the opposite-side VPN gateway (61.2.1.1) in the Security Gateway Addr. 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.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPSec &gt; IKE &gt; Add</b></p> 

**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**

IPSec  PPTP  L2TP

- If you enable the firewall, please check whether these firewall rules would block packets in tunnel.
- Packets are blocked by default in the "WAN to LAN" direction, please add a rule to forward these tunneled packets.
- 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.

OK

**Step 5 - Add a Firewall rule**

Same as at DFL-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**

Status Edit Rules Show Rules Attack Alert 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	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log
1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y

Page 1/1

Prev. Page **Insert** Edit Delete Move Before: 1 Next Page

**Step 6 - Customize the Firewall rule**

Check the Activate this rule. Enter the Rule Name as AllowVPNIKerule, Source IP as 192.168.40.0, and Dest. IP as 192.168.88.0. Click Apply to store this rule.

**ADVANCED SETTINGS > Firewall > Edit Rules > Insert**

Status Edit Rules Show Rules Attack Alert Summary

Firewall Edit Rules Insert

Insert a new WAN1-to-WAN1 Firewall rule

Status

Activate this rule

Rule name: AllowVPNIKerule

Condition

Source IP: 192.168.40.0 Netmask: 255.255.255.0

Dest. IP: 192.168.88.0 Netmask: 255.255.255.0

Service: Any

Configure dest. port?

Type  Single  Range

Dest. Port: 0 to 0

Well known port: FTP (21) Copy To Dist.

Action

Forward the matched packet.

Don't log the matched packet.

Back Apply Reset

**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 DFL-1500 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		
	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log	
1	Y	AllowVPN IKE rule	WAN1 to LAN1	192.168.40.0/255.255.255.0	192.168.88.0/255.255.255.0	Any	Forward	N	
2	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y	

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**➤ 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 DFL-1.

**At DFL-1:**

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

**Step 1 - Enable IPSec**

Check the Enable IPSec checkbox and click Apply.

**ADVANCED SETTINGS > VPN Settings > IPSec**

IPSec 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	Security Gateway	

Prev. Page Add Edit Delete Next Page

**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**

IPSec 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	Security Gateway	

Prev. Page Add Edit Delete Next Page

**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**

	FIELD	DESCRIPTION	EXAMPLE
Status	Active	This field will activate this IPSec policy rule	enabled
	Manual Key Rule Name	The name of this IPSec policy	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
	IP Address	The local IP address	192.168.40.0
	Prefix Len/Subnet Mask	The local IP Netmask	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
	IP Address	The remote IP address	192.168.88.0
	Prefix Len/Subnet Mask	The remote IP Netmask	255.255.255.0
Action	My IP Address	The IP address of local site DFL-1500 Firewall/VPN Router	61.2.1.1
	Security Gateway Addr	The IP address of remote site device, like DFL-1500 Firewall/VPN Router.	210.2.1.1



Outgoing SPI	The Outgoing SPI (Security Parameter Index) value. Notice : HEX SPI must be a value between 600 and 600000.Or DEC SPI must be a value between 1500 and 6300000.	2222
Incoming SPI	The Incoming SPI (Security Parameter Index) value. Notice : HEX SPI must be a value between 600 and 600000.Or DEC SPI must be a value between 1500 and 6300000.	1111
Encapsulation Mode	Choose Tunnel or Transport mode, see Chapter 9 for details.	Tunnel
ESP – Encryption / Authentication or AH - Authentication	Select the Encryption (DES or 3DES) and Authentication (MD5 or SHA1) Algorithm combination. And enter the key either hex or string format separately.	ESP – Encryption (DES) / Authentication (MD5)

Table 10-4 Add a IPSec Manual Key rule

<p><b>Step 4 - Detail settings of IPSec Manual Key</b></p> <p>For the detailed setting in the Manual Key. We can press the Advanced button in the previous page. Then set the parameter separately.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; IPSec &gt; Manual Key &gt; Add &gt; Advanced</b></p>
---	---

	FIELD	DESCRIPTION	EXAMPLE
Condition	Local to Remote Protocol / Src Port / Dest Port	Use this field to select some packets which are destined for specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from local to remote.	TCP / 0 / 80
	Remote to Local Protocol / Src Port / Dest Port	Use this field to select some packets which are destined for specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from remote to local.	ANY / 0 / 0
Action	Enable Replay Detection	Whether is the “Replay Detection” enabled ?	YES

Table 10-5 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**

**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**

Item #	Status	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log
1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y

**Step 7 - Customize the Firewall rule**

Check the Activate this rule. Enter the Rule Name as AllowVPNIKerule, Source IP as 192.168.88.0, and Dest. IP as 192.168.40.0. Click Apply to store this rule.

**ADVANCED SETTINGS > Firewall > Edit Rules > Insert**



**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 DFL-1500. 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	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log
1	Y	AllowVPN IKE rule	WAN1 to LAN1	192.168.88.0/255.255.255.0	192.168.40.0/255.255.0	Any	Forward	N
2	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**At DFL-2:**

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

**Step 1 - Enable IPSec**

Check the Enable IPSec checkbox and click Apply.

**ADVANCED SETTINGS > VPN Settings > IPSec**

IPSec PPTP L2TP Pass Through

Enable IPSec Apply

[[IKE] [Manual Key]

Edit/Modify IPSec Security Associations

Item #	Status	Name	Local LAN	Remote LAN	Mechanism	My IP	Security Gateway
--------	--------	------	-----------	------------	-----------	-------	------------------

Prev. Page Add Edit Delete Next Page

**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**

IPSec PPTP L2TP Pass Through

Enable IPSec Apply

[[IKE] [Manual Key]

Edit/Modify IPSec Security Associations

Item #	Status	Name	Local LAN	Remote LAN	Mechanism	My IP	Security Gateway
--------	--------	------	-----------	------------	-----------	-------	------------------

Prev. Page Add Edit Delete Next Page

**Step 3 - Customize the rule**

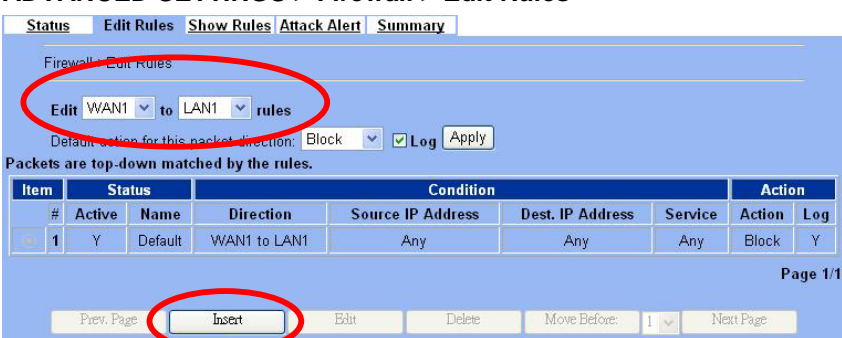
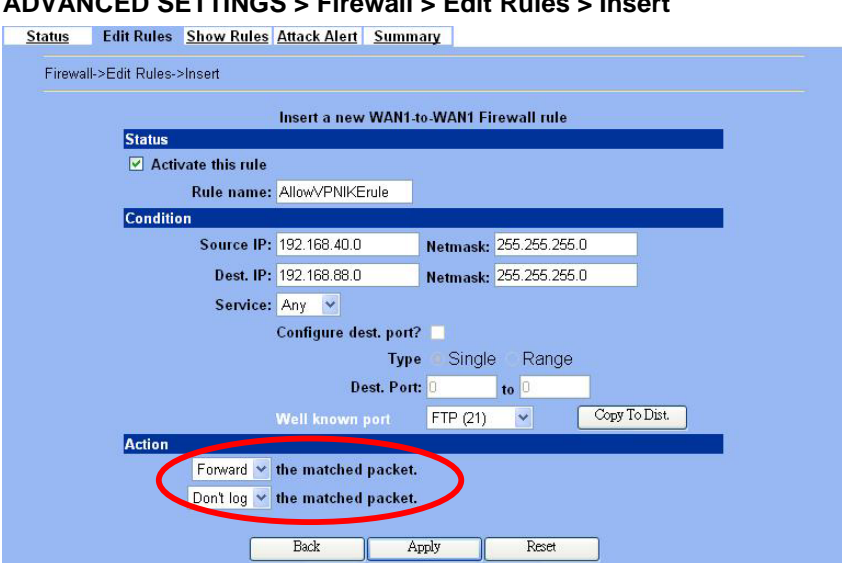

Similar to those in DFL-1, except that you should interchange the Local IP Address with the Remote IP Address, the My IP Address with the Security Gateway Addr., and the Outgoing SPI with the Incoming SPI.

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

**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**

<p><b>Step 5 - Add a Firewall rule</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Edit Rules</b></p>  <p>Firewall-&gt;Edit Rules</p> <p>Edit WAN1 to LAN1 rules</p> <p>Default action for this packet direction: Block <input checked="" type="checkbox"/> Log Apply</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th colspan="4">Condition</th> <th colspan="2">Action</th> </tr> <tr> <th>#</th> <th>Active</th> <th>Name</th> <th>Direction</th> <th>Source IP Address</th> <th>Dest. IP Address</th> <th>Service</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>Default</td> <td>WAN1 to LAN1</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Block</td> <td>Y</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page <b>Insert</b> Edit Delete Move Before: 1 Next Page</p>	Item	Status	Condition				Action		#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log	1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y									
Item	Status	Condition				Action																														
#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log																												
1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y																												
<p><b>Step 6 - Customize the Firewall rule</b></p> <p>Check the Activate this rule. Enter the Rule Name as AllowVPNIKErule, Source IP as 192.168.40.0, and Dest. IP as 192.168.88.0. Click Apply to store this rule.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Edit Rules &gt; Insert</b></p>  <p>Firewall-&gt;Edit Rules-&gt;Insert</p> <p>Insert a new WAN1-to-WAN1 Firewall rule</p> <p><b>Status</b></p> <p><input checked="" type="checkbox"/> Activate this rule</p> <p>Rule name: AllowVPNIKErule</p> <p><b>Condition</b></p> <p>Source IP: 192.168.40.0 Netmask: 255.255.255.0</p> <p>Dest. IP: 192.168.88.0 Netmask: 255.255.255.0</p> <p>Service: Any</p> <p>Configure dest. port? <input type="checkbox"/></p> <p>Type <input checked="" type="radio"/> Single <input type="radio"/> Range</p> <p>Dest. Port: 0 to 0</p> <p>Well known port: FTP (21) Copy To Dist.</p> <p><b>Action</b></p> <p><input checked="" type="checkbox"/> Forward the matched packet.</p> <p><input checked="" type="checkbox"/> Don't log the matched packet.</p> <p>Back Apply Reset</p>																																			
<p><b>Step 7 - View the result</b></p> <p>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 DFL-1500 and successfully access the 192.168.88.0/24 through the VPN tunnel.</p>	<p><b>ADVANCED SETTINGS &gt; Firewall &gt; Edit Rules</b></p>  <p>Firewall-&gt;Edit Rules</p> <p>Edit WAN1 to LAN1 rules</p> <p>Default action for this packet direction: Block <input checked="" type="checkbox"/> Log Apply</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th colspan="4">Condition</th> <th colspan="2">Action</th> </tr> <tr> <th>#</th> <th>Active</th> <th>Name</th> <th>Direction</th> <th>Source IP Address</th> <th>Dest. IP Address</th> <th>Service</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>AllowVPNIKErule</td> <td>WAN1 to LAN1</td> <td>192.168.40.0/255.255.255.0</td> <td>192.168.88.0/255.255.255.0</td> <td>Any</td> <td>Forward</td> <td>N</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Default</td> <td>WAN1 to LAN1</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Block</td> <td>Y</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page Insert Edit Delete Move Before: 1 Next Page</p>	Item	Status	Condition				Action		#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log	1	Y	AllowVPNIKErule	WAN1 to LAN1	192.168.40.0/255.255.255.0	192.168.88.0/255.255.255.0	Any	Forward	N	2	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y
Item	Status	Condition				Action																														
#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log																												
1	Y	AllowVPNIKErule	WAN1 to LAN1	192.168.40.0/255.255.255.0	192.168.88.0/255.255.255.0	Any	Forward	N																												
2	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y																												



# Chapter 11

## Virtual Private Network – PPTP

*This chapter introduces PPTP and explains how to implement it.*

### 11.1 Demands

1. One employee in our company may sometimes want to connect back to our corporate 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 headquarter for the internal company employees.

### 11.2 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 headquarter. Suppose they are in the same internal network, and keep the communication security.

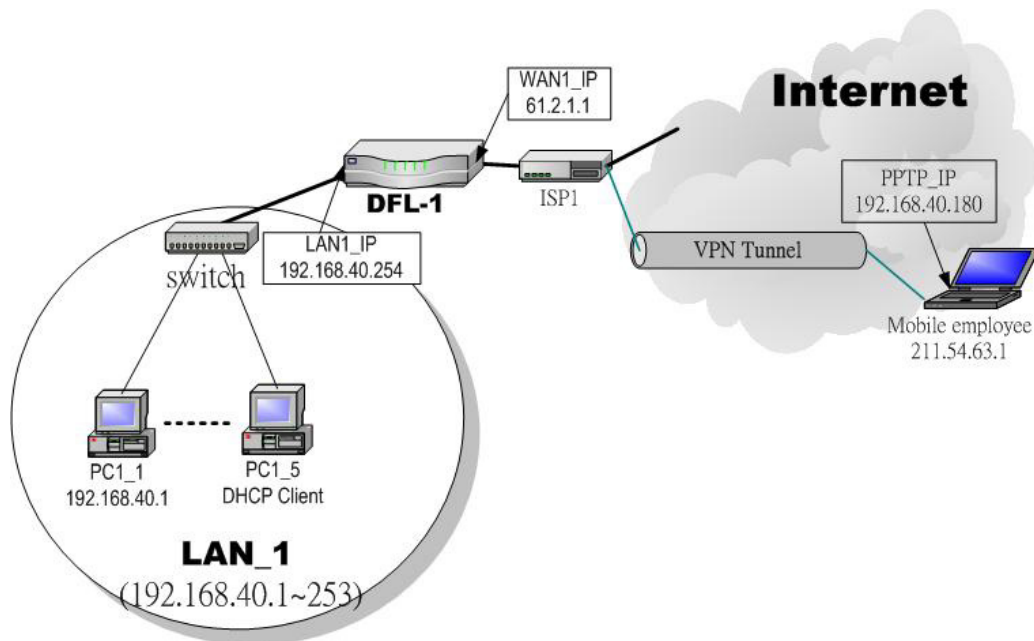


Figure 11-1 PPTP method connection

### 11.3 Methods

1. Setup the PPTP server at DFL-1500. Setup the remote PC as the PPTP client. After dialing up to DFL-1, DFL-1 will assign a private IP which falls in the range of the settings in the PPTP server at DFL-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 DFL-1500 as the PPTP client. Let all the client PCs behind the DFL-1500. They can connect to the network behind PPTP Server by passing through DFL-1500. It sounds like no Internet exists but can connect with each other.

## 11.4 Steps

### 11.4.1 Setup PPTP Network Server

<p><b>Step 1 – Enable PPTP Server</b></p> <p>Check the <b>Enable PPTP</b> checkbox, enter the <b>LAN1_IP</b> of the DFL-1(192.168.40.254) in the <b>Local IP</b>, and enter the IP range that will be assigned to the PPTP clients in the <b>Start IP</b> and the <b>End IP</b> fields. Enter the <b>Username</b> and <b>Password</b> that will be used by the employees during dial-up. Click the <b>Apply</b> to finish configurations.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; PPTP</b></p>
---	---

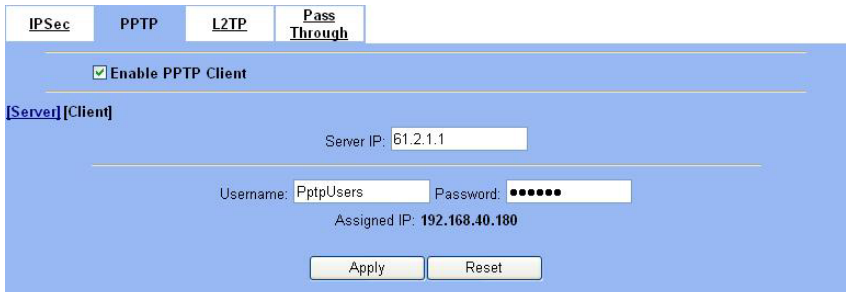
FIELD	DESCRIPTION	EXAMPLE
Enable PPTP Server	Enable PPTP feature of the DFL-1500	enabled
Local IP	The Local IP is the allocated IP address in the internal Network after PPTP client dials in the DFL-1500.	192.168.40.254
Start IP	The Start IP is the allocated starting IP address in the internal network after PPTP client dials in the DFL-1500.	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 DFL-1500.	192.168.40.199
Username	The account which allow PPTP client user to dial in DFL-1500.	PptpUsers
Password	The password which allow PPTP client user to dial in DFL-1500.	Dif3wk

Table 11-1 Setup PPTP Server

<p><b>Step 2 – Setup Windows XP/2000 PPTP clients</b></p>	<p><b><u>Configuring A PPTP Dial-Up Connection</u></b></p> <ol style="list-style-type: none"> <li>1. Configuring a PPTP dial-up connection</li> <li>2. Go to Start &gt; Control Panel &gt; Network and Internet Connections &gt; Make new connection.</li> <li>3. Select Create a connection to the network of your workplace and select Next.</li> <li>4. Select Virtual Private Network Connection and select Next.</li> <li>5. Give a Name the connection and select Next.</li> <li>6. If the Public Network dialog box appears, choose the Don't dial up initial connection and select Next.</li> <li>7. In the VPN Server Selection dialog, enter the public IP or hostname of the DFL-1500 to connect to and select Next.</li> <li>8. Set Connection Availability to Only for myself and select Next.</li> <li>9. Select Finish.</li> </ol>
---	---

	<p><b>Customize the VPN Connection</b></p> <ol style="list-style-type: none"> <li>1. Right-click the icon that you have created.</li> <li>2. Select <b>Properties &gt; Security &gt; Advanced &gt; Settings</b>.</li> <li>3. Select <b>No Encryption</b> from the <b>Data Encryption</b> and click <b>Apply</b>.</li> <li>4. Select the <b>Properties &gt; Networking</b> tab.</li> <li>5. Select <b>PPTP VPN</b> from the <b>VPN Type</b>. Make sure the following are selected: TCP/IP QoS Packet Scheduler</li> <li>6. Select <b>Apply</b>.</li> </ol>
	<p><b>Connecting to the PPTP VPN</b></p> <ol style="list-style-type: none"> <li>1. Connect to your ISP.</li> <li>2. Start the dial-up connection configured in the previous procedure.</li> <li>3. Enter your PPTP VPN <b>User Name</b> and <b>Password</b>.</li> <li>4. Select <b>Connect</b>.</li> </ol>

### 11.4.2 Setup PPTP Network Client

<p><b>Step 1 – Enable PPTP Client</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; VPN Settings &gt; PPTP &gt; Client</b></p> 
--	--

FIELD	DESCRIPTION	EXAMPLE
Enable PPTP Client	Enable PPTP Client feature of DFL-1500	enabled
Server IP	The IP address of PPTP server.	61.2.1.1
Username	The designed account which allows PPTP client to dial in.	PptUsers
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 11-2 Setup PPTP Client settings





# Chapter 12

## Virtual Private Network – L2TP

*This chapter introduces L2TP and explains how to implement it.*

### 12.1 Demands

1. One employee in our company may sometimes want to connect back to our corporate 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.

### 12.2 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.

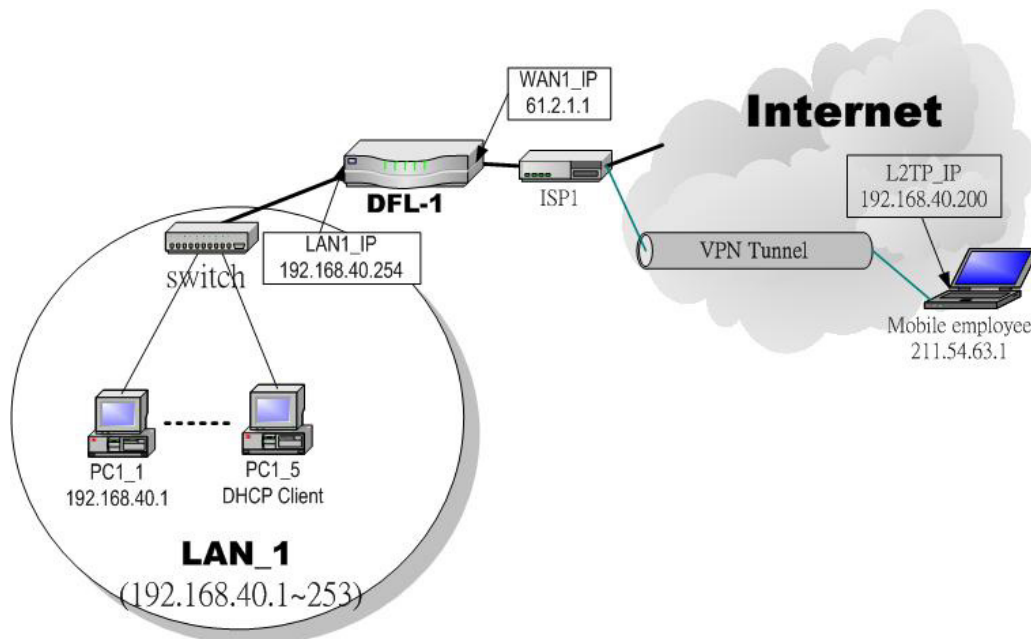


Figure 12-1 L2TP method connection

### 12.3 Methods

1. Setup the L2TP server at DFL-1500 (LNS: L2TP Network Server). After dialing up to DFL-1500, DFL-1500 will assign a private IP which falls in the range of the settings in the L2TP server at DFL-1500. 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.

## 12.4 Steps

### 12.4.1 Setup L2TP Network Server

#### Step 1 – Enable L2TP LNS

Check the **Enable L2TP LNS** checkbox, enter the LAN1\_IP of the DFL-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

FIELD	DESCRIPTION	EXAMPLE
Enable L2TP LNS	Enable L2TP LNS feature of DFL-1500	enabled
Local IP	The Local IP is the allocated IP address in the internal network after default gateway of L2TP client dials in the DFL-1500.	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 DFL-1500.	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 DFL-1500.	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 DFL-1500.	L2tpUsers
Password	The password which allows L2TP client user to dial in DFL-1500.	Dif3wk

Table 12-1 Setup L2TP LNS Server settings

<b>Step 2 – Setup Windows XP/2000 L2TP clients</b>	<p><b><u>Configuring A L2TP Dial-Up Connection</u></b></p> <ol style="list-style-type: none"> <li>1. Configure a L2TP dial-up connection</li> <li>2. Go to Start &gt; Control Panel &gt; Network and Internet Connections &gt; Make new connection.</li> <li>3. Select Create a connection to the network of your workplace and select Next.</li> <li>4. Select Virtual Private Network Connection and select Next.</li> <li>5. Give a Name the connection and select Next.</li> <li>6. If the Public Network dialog box appears, choose the Don't dial up initial connection and select Next.</li> <li>7. In the VPN Server Selection dialog, enter the public IP or hostname of the DFL-1500 to connect to and select Next.</li> <li>8. Set Connection Availability to Only for myself and select Next.</li> <li>9. Select Finish.</li> </ol>
	<p><b><u>Customize the VPN Connection</u></b></p> <ol style="list-style-type: none"> <li>1. Right-click the icon that you have created.</li> <li>2. Select Properties &gt; Security &gt; Advanced &gt; Settings.</li> <li>3. Select No Encryption from the Data Encryption and click Apply.</li> <li>4. Select the Properties &gt; Networking tab.</li> <li>5. Select L2TP VPN from the VPN Type. Make sure the following are selected: <ul style="list-style-type: none"> <li>TCP/IP</li> <li>QoS Packet Scheduler</li> </ul> </li> <li>6. Select Apply.</li> </ol>
	<p><b><u>Editing Windows Registry</u></b></p> <p>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.</p> <ol style="list-style-type: none"> <li>1. Use the registry editor (regedit) to locate the following key in the registry: HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Rasman \ Parameters</li> <li>2. Add the following registry value to this key: <ul style="list-style-type: none"> <li>• Value Name: ProhibitIpSec</li> <li>• Data Type: REG_DWORD</li> <li>• Value: 1</li> </ul> </li> <li>3. Save your changes and restart the computer.</li> </ol> <p>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.</p>

**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.



# Part IV

## Content Filters

## Chapter 13

# Content Filtering – Web Filters

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

### 13.1 Demands

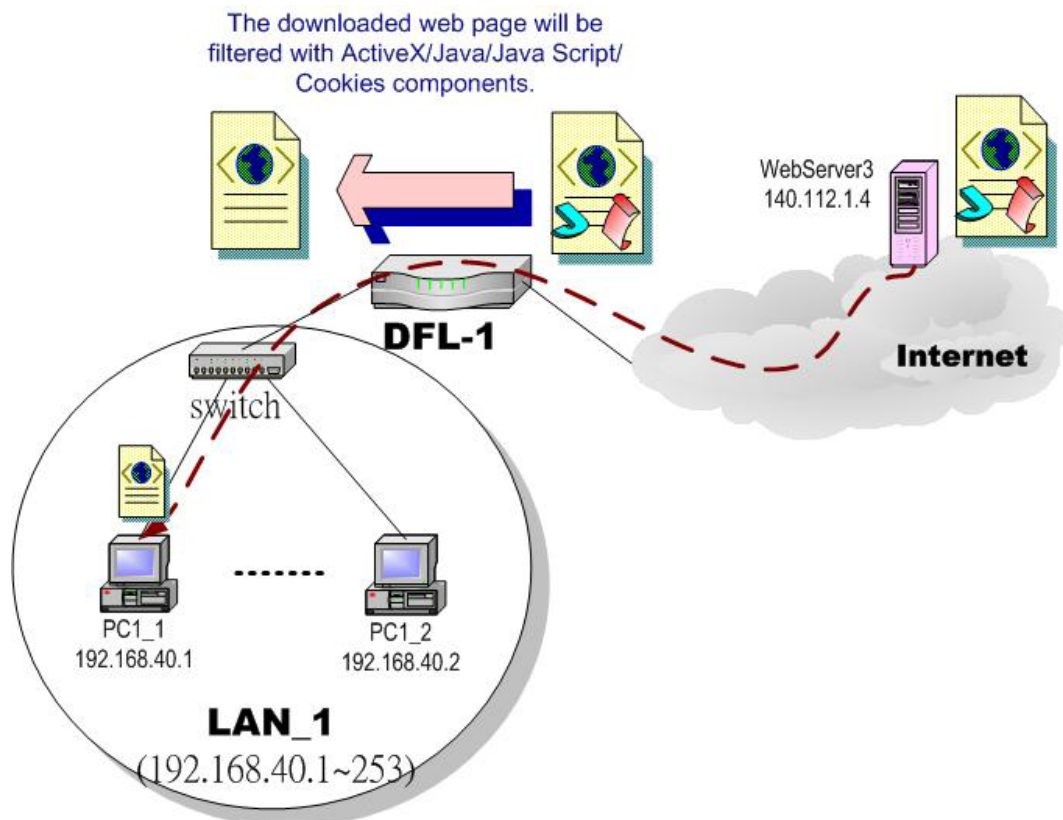


Figure 13-1 Use web filter functionality to avoid users browsing the forbidden web site

1. As the above Figure 13-1 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.

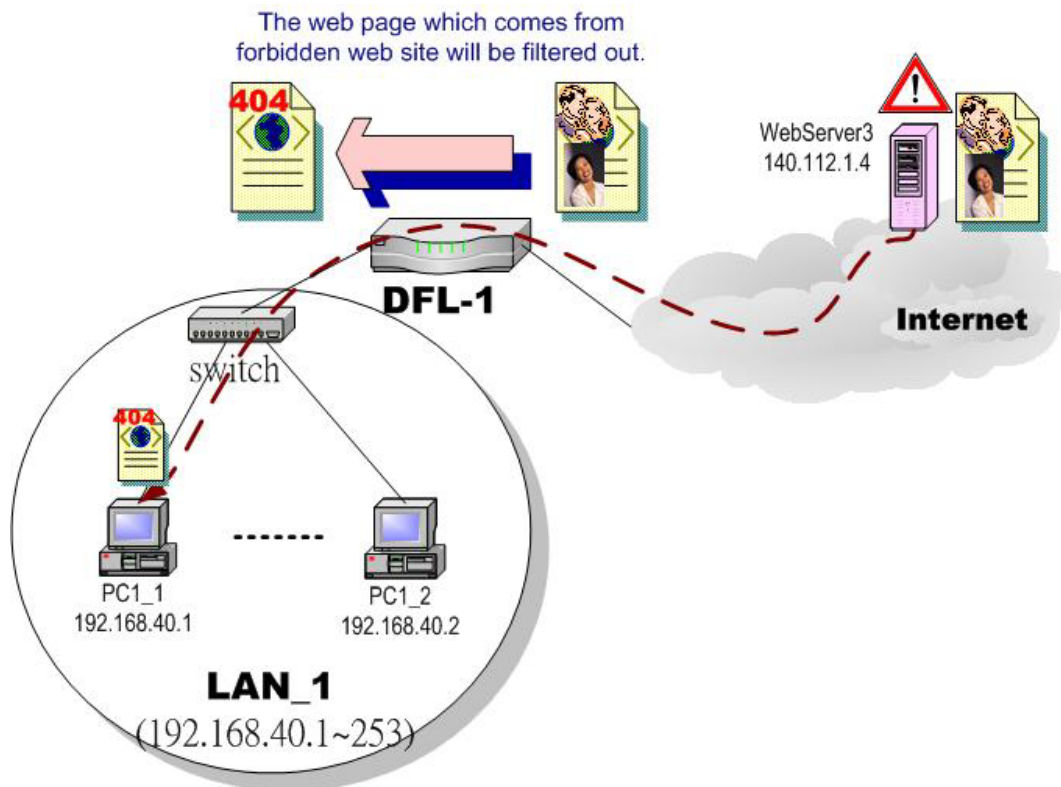


Figure 13-2 Use web filter functionality to avoid users view the forbidden web site

- As the above Figure 13-2 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.

## 13.2 Objectives

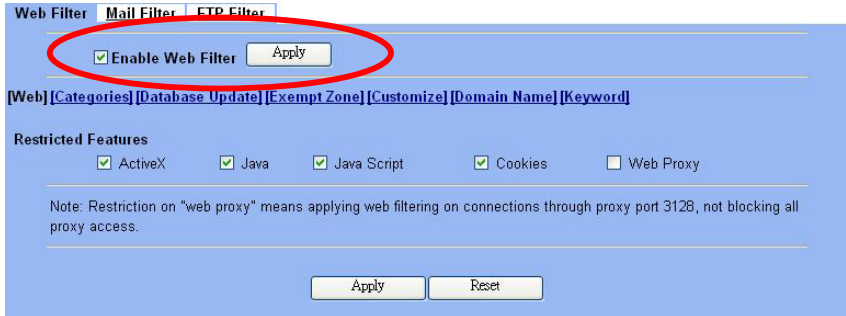
- Remove the cookies, Java applet, Java scripts, ActiveX objects from the web pages.
- Prevent users from connecting to the forbidden sites.

## 13.3 Methods

- Setup content filtering for web objects such as cookies and Java applets.
- 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.





### 13.4 Steps

<p><b>Step 1 - Enable Web Filter</b></p> <p>Check the <code>Enable Web Filter</code> checkbox and click the <code>Apply</code> right on the right side.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter</b></p> 
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable Web Filter	Enable Web Filter feature of DFL-1500	enabled

Table 13-1 Enable Web Filter

<p><b>Step 2 - Warning of Firewall</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter</b></p> 
<p><b>Step 3 - Customize Objects</b></p> <p>Check the objects of <code>Restricted Features</code> to block the objects. Click the <code>Apply</code> button at the bottom of this page. Use <code>PCI_1</code> 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.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter</b></p> 

FIELD	DESCRIPTION	EXAMPLE
Restricted Features	Select the below items that will verified by Web Filter of DFL-1500.	
ActiveX	filter the web page that includes ActiveX	enabled
Java	filter the web page that includes Java	enabled
Java Script	filter the web page that includes Java Script	enabled
Cookies	filter the web page that includes Cookies	enabled

Web Proxy	If enabling the “Web Proxy”, all the web pages pass through proxy (Only port 3128) will also be verified by DFL-1500. If disabling the “Web Proxy”, all the web pages through will bypass the verification.	enabled
Apply	Apply the settings which have been configured.	N/A
Reset	Clean the filled data and restore the original.	N/A

Table 13-2 Web Filter setting page

<p><b>Step 4 - Customize Categories</b></p> <p>With the built-in URL database, DFL-1500 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 &amp; 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.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Categories</b></p>
--	--

FIELD	DESCRIPTION	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	disabled
Violence/Profanity, Gross Depictions, Militant/Extremist ,etc. items	Check the categories you would like to enable	Enable the checked ones
Time of Day	The time which was set for Web Filter.	09:30 ~ 17:30
Apply	Apply the settings which have been configured.	N/A
Reset	Clean the filled data and restore the original one.	N/A

Table 13-3 Web Filter Categories setting page

<p><b>Step 5 - Update the Built-in Database</b></p> <p>Click the <b>Download</b> button to ask DFL-1500 to instantly download the database from the fwupdate.dlinktw.com.tw. The DFL-1500 can be set to automatically check the site for any new updates by checking the <b>Automatic Download</b>. You can also configure how frequently the DFL-1500 checks for the updates. Click <b>Apply</b> to store the changes. From now on, any traffic matched with the URLs in the database will be blocked by the DFL-1500.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Database Update</b></p>
---	---

FIELD	DESCRIPTION	EXAMPLE
List Server	Determine the URL database website to download from (default is fwupdate.dlinktw.com.tw).	fwupdate.dlinktw.com.tw
Automatic Download	download the URL database automatically or not	enabled
Update Schedule On	Setup the automatically download time (DayOfWeek).	Sunday At 03:00
Apply	Apply the settings which have been configured.	N/A
Reset	Clean the filled data and restore the original one.	N/A

Table 13-4 Web Filter database update

<p><b>Step 6 - Further Customize the local zones</b></p> <p>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 <b>Delete</b> button. Enter the IP range in the <b>Range</b> fields followed by a click of the <b>Add</b> button to add one address range to the web filter. Click “<b>Include.....</b>” and <b>Apply</b> if you want web filters to only apply to the specified ranges. Click “<b>Exclude.....</b>” and <b>Apply</b> if you want web filters to apply to all computers except those specified ranges.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Exempt Zone</b></p>
--	---

FIELD	DESCRIPTION	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	disabled

Include specified address ranges in the web filter enforcement	Web filter will only active at below specified computers.	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.	disabled
Range From	Here we can setup the IP address range, for the above Exempt Computers to use.	10.1.1.1 – 10.1.1.254 192.168.40.100 – 192.168.40.130
Apply	Apply the above selected “Exempt Computers” radius button.	N/A
Add	Add the specified IP range which filled in the above “Range From” field.	N/A
Reset	Clean the filled data and restore the original one.	N/A
Delete	Delete the specified IP range which filled in the above “Range From” field.	N/A

Table 13-5 Web Filter Exempt Zone setting page

<p><b>Step 7 - Further Customize the remote sites</b></p> <p>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 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 DFL-1500 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.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Customize</b></p> <p>Web Filter   Mail Filter   FTP Filter</p> <p>Web Filter-&gt;Customize</p> <p><a href="#">Web</a>   <a href="#">Categories</a>   <a href="#">Database Update</a>   <a href="#">Exempt Zone</a>   <a href="#">Customize</a>   <a href="#">Domain Name</a>   <a href="#">Keyword</a></p> <p><input checked="" type="checkbox"/> <b>Enable Filter List Customization</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Disable all web traffic except for trusted domains.</li> <li><input checked="" type="checkbox"/> Don't block Java/ActiveX/Cookies/Web Proxy to trusted domain sites.</li> </ul> <p><b>Trusted Domains</b></p> <p>Domain</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">www.dlink.com.tw www.dlink.com</div> <p style="text-align: right;">Add Delete</p> <hr/> <p><b>Forbidden Domains</b></p> <p>Domain</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">www.sex.com www.stockmarket.com</div> <p style="text-align: right;">Add Delete</p> <p style="text-align: center;">Apply Reset</p>
---	--

FIELD	DESCRIPTION	EXAMPLE
Enable Filter List Customization	Enable the Filter List Customization feature of web filter	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.	Enabled

Don't block Java/ActiveX/Cookies/Web Proxy to trusted domain sites	In the following domain range of the trusted domains. If there are include Java/ActiveX/Cookies/Web Proxy components in the web page, the action is setting not to block.	Enabled
Trusted Domains Domain	Here we can specify the Trusted Domains for the above item using.	www.dlink.com.tw www.dlink.com
Forbidden Domains Domain	Here we can specify the Forbidden Domains for the above item using.	www.sex.com www.stockmarket.com
Add	Add the Trusted/Forbidden Domains IP range to the list.	N/A
Delete	Delete the Trusted/Forbidden Domains IP range from the list.	N/A
Apply	Apply the setting which configured on the checkbox.	N/A
Reset	Clean the filled data and restore the original one.	N/A

Table 13-6 Web Filter Customize setting page

<p><b>Step 8 - Setup URL keyword blocking</b></p> <p>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.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Domain Name</b></p>
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable Keyword blocking	Enable URL keyword blocking feature of web filter	Enabled
Keyword	If the Keyword appears in the URL when connect to the Internet using browser. The contents about the URL will be block.	sex
Apply	Apply the setting which configured on the checkbox.	N/A
Add	Add the Keyword to the list.	N/A
Reset	Clean the filled data and restore the original one.	N/A
Delete	Delete the selected keyword from the list.	N/A

Table 13-7 Web Filter Domain Name setting page

<p><b>Step 9 - Setup contents keyword blocking</b></p> <p>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.</p> <p>Note that you can add the keywords as many as you like.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Web Filter &gt; Keyword</b></p> <p>Web Filter   Mail Filter   FTP Filter</p> <p>Web Filter-&gt;Domain Name</p> <p>[Web] [Categories] [Database Update] [Exempt Zone] [Customize] [Domain Name] [Keyword]</p> <p>Block web content which contain these keywords</p> <p><input checked="" type="checkbox"/> Enable keyword blocking, limit at 3 matches.</p> <p>Keyword <input type="text"/></p> <p>sex violence blood</p> <p>Apply Add Reset Delete</p>
--	--

FIELD	DESCRIPTION	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.	Enabled 3 matches
Keyword	Specify the keyword that you want to block.	sex violence blood
Apply	Apply the settings which have been configured.	N/A
Add	Add the Keyword to the list.	N/A
Reset	Clean the filled data and restore the original one.	N/A
Delete	Delete the Keyword from the list.	N/A

Table 13-8 Web Filter Content Keywords setting page

# Chapter 14

## Content Filtering – Mail Filters

*This chapter introduces SMTP proxies and explains how to implement it.*

### 14.1 Demands

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.

### 14.2 Objectives

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.

### 14.3 Methods

1. Setup SMTP filters for outgoing emails from PC\_1 (in LAN1) towards the mail server (in DMZ1 or in WAN1) to append a “.bin” to all vbs attachments. Use PC1\_1 to send an email with vbs attachments to test the configuration.
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 vbs attachments. Use PC1\_1 to retrieve an email with vbs attachments to test the configuration.

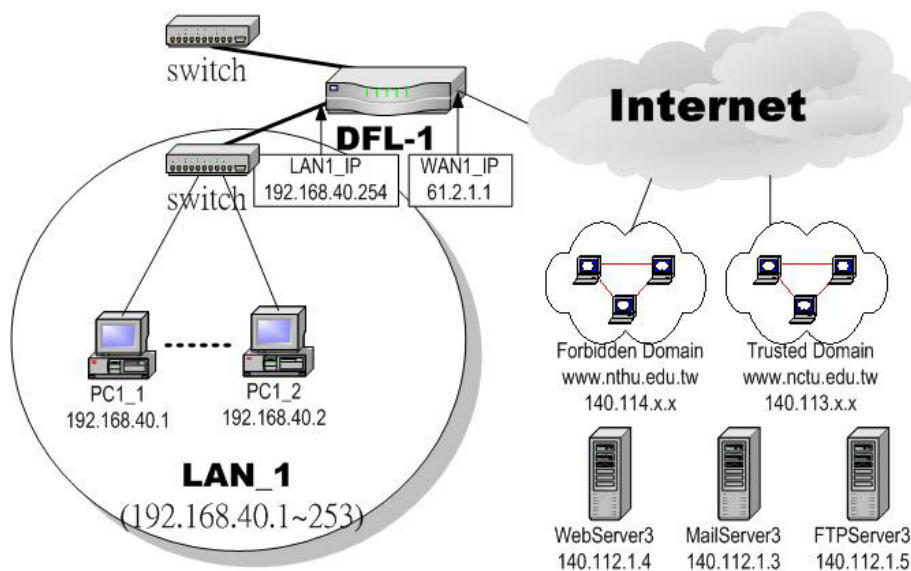
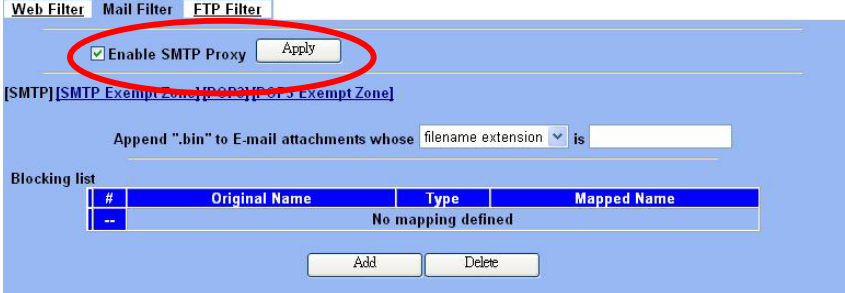


Figure 14-1 Use SMTP / POP3 filter functionality to avoid some sensitive e-mail directly opened

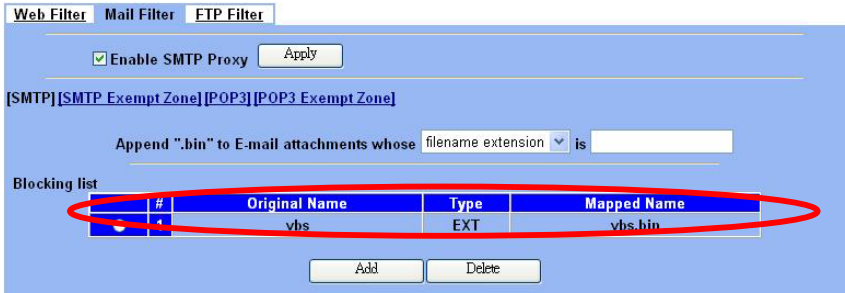


### 14.4 Steps for SMTP Filters

<p><b>Step 1 – Enable SMTP Filters</b></p> <p>Check the Enable SMTP Proxy checkbox and click Apply.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Mail Filters &gt; SMTP</b></p>  <p>The screenshot shows the 'Mail Filter' tab selected. The 'Enable SMTP Proxy' checkbox is checked and circled in red. Below it, there is a section for 'Append ".bin" to E-mail attachments whose filename extension is' with a dropdown menu set to 'filename extension' and an empty text box. A 'Blocking list' table is shown with the text 'No mapping defined'.</p>
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable SMTP Proxy	Enable SMTP Proxy feature of DFL-1500	enabled
Append ".bin" to E-mail attachments whose	<ul style="list-style-type: none"> <li>➤ Filename extension When the filename extension of attachment file matches "Filename extension", add the ".bin" extension to the attachment file.</li> <li>➤ Exact filename When the whole filename of attachment file matches "Exact filename", add the ".bin" extension to the attachment file.</li> </ul>	Filename extension

Table 14-1 Mail Filter SMTP setting page

<p><b>Step 2 – Add a SMTP Filter</b></p> <p>Select filename extension, enter vbs, and click Add to add a rule. This rule will apply to all LAN-to-DMZ/WAN SMTP connections. All such SMTP traffic will be examined to change the filename extension from vbs to vbs.bin.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; Mail Filters &gt; SMTP</b></p>  <p>The screenshot shows the same settings as Step 1, but now a rule is added to the 'Blocking list' table. The rule is circled in red and has the following details: # 1, Original Name vbs, Type EXT, and Mapped Name vbsbin.</p>
--	--



**Step 3 – 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 > Mail Filters > SMTP Exempt Zone**

**14.5 Steps for POP3 Filters**

**Step 1 – Enable POP3 Filters**

Check the Enable POP3 Proxy checkbox and click Apply.

**ADVANCED SETTINGS > Content Filters > Mail Filters > POP3**

FIELD	DESCRIPTION	EXAMPLE
Enable POP3 Proxy	Enable POP3 Proxy feature of DFL-1500	enabled
Append ".bin" to E-mail attachments whose	<ul style="list-style-type: none"> <li>➤ Filename extension When the filename extension of attachment file matches “Filename extension”, add the “.bin” extension to the attachment file.</li> <li>➤ Exact filename When the whole filename of attachment file matches “Exact filename”, add the “.bin” extension to the attachment file.</li> </ul>	Filename extension

Table 14-2 Mail Filter SMTP setting page

**Step 2 – Add a POP3 Filter**

Select filename extension, enter vbs, and click Add to add a rule. This rule will apply to all DMZ/WAN-to-LAN POP3 connections. All such POP3 traffic will be examined to change the filename extension from vbs to vbs.bin.

**ADVANCED SETTINGS > Content Filters > Mail Filters > POP3**

Web Filter Mail Filter FTP Filter

Enable POP3 Proxy

[SMTP] [SMTP Exempt Zone] [POP3] [POP3 Exempt Zone]

Append ".bin" to E-mail attachments whose filename extension is

Blocking list

#	Original Name	Type	Mapped Name
1	vbs	EXT	vbs.bin

**Step 3 – 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 > Mail Filters > POP3 Exempt Zone**

Web Filter Mail Filter FTP Filter

Mail Filter->POP3 Proxy Exempt Zone

[SMTP] [SMTP Exempt Zone] [POP3] [POP3 Exempt Zone]

POP3 Exempt Computers

Enforce POP3 filter policies for all computers.  
 Include specified address ranges in the POP3 filter enforcement.  
 Exclude specified address ranges from the POP3 filter enforcement.

Range From  To

192.168.40.100 -- 192.168.40.130  
10.1.1.1 -- 10.1.1.254

# Chapter 15

## Content Filtering – FTP Filtering

*This chapter introduces FTP proxies and explains how to implement it.*

### 15.1 Demands

1. Some users in LAN1 use FTP to download big MP3 files and cause waste of bandwidth.

### 15.2 Objectives

1. Forbid PC1\_1 from downloading MP3 files with FTP.

### 15.3 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.

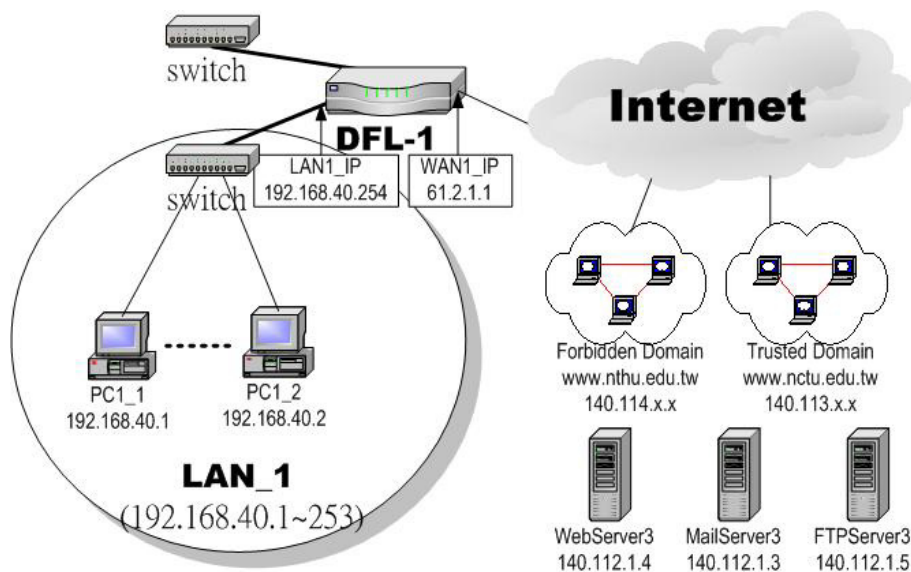



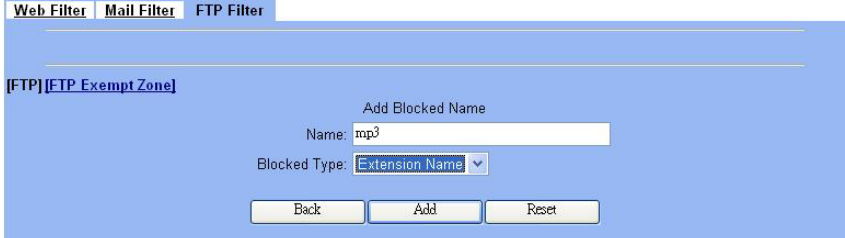
Figure 15-1 Use FTP filter functionality to avoid user download forbidden file type

## 15.4 Steps

<p><b>Step 1 - Enable FTP Filter</b></p> <p>Check the <b>Enable FTP Filter</b> checkbox and click the nearby <b>Apply</b> button to enable this feature. Click the <b>Add</b> button to add a new FTP filter.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; FTP Filter &gt; FTP</b></p> 
---	--

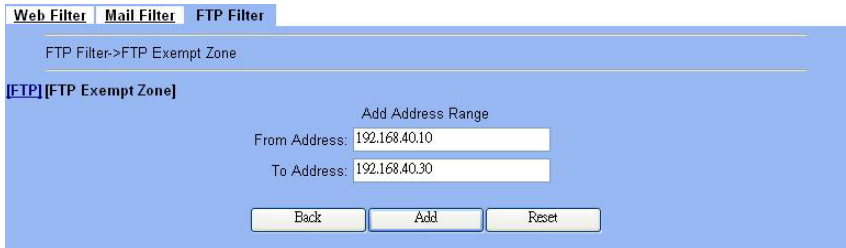
FIELD	DESCRIPTION	EXAMPLE
Enable FTP Filter	Enable FTP Filter feature of DFL-1500	enabled

Table 15-1 FTP Filter FTP setting page

<p><b>Step 2 - Add an FTP Filter</b></p> <p>Enter <b>mp3</b> in the <b>Name</b> field and select <b>Extension Name</b> in the <b>Blocked Type</b> field. Click the <b>Add</b> button to apply the change. Now users in LANs can never download any mp3 files.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; FTP Filter &gt; FTP &gt; Add</b></p> 
---	---

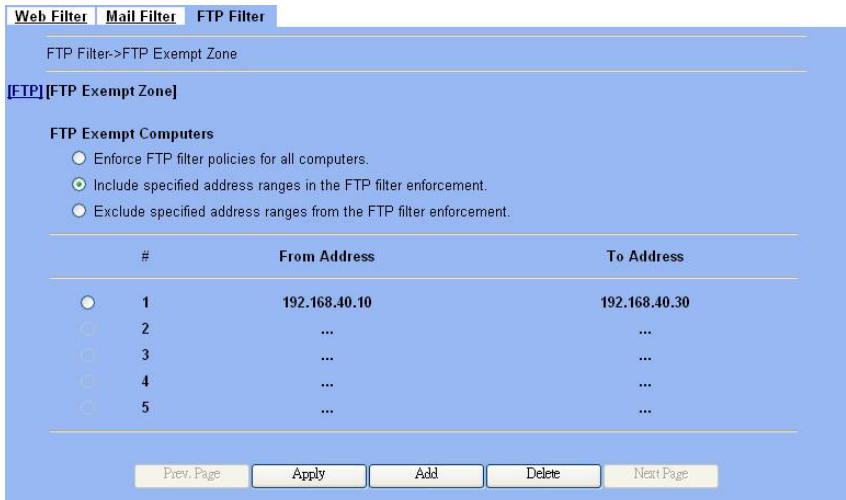
FIELD	DESCRIPTION	EXAMPLE
Name	Fill in the file extension or exact filename.	mp3
Blocked Type	<ul style="list-style-type: none"> <li>➤ Extension Name When the extension filename of download file is matching, the action is blocked download from FTP server.</li> <li>➤ Full Name When the exact filename of download file is matching, the action is blocked download from FTP server.</li> </ul>	Extension Name

Table 15-2 FTP Filter FTP adding filter entry

<p><b>Step 3 - Add an Exempt Zone</b></p> <p>Add a new Exempt Zone record. It's IP address range is between 192.168.40.10 to 192.168.40.30.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; FTP Filter &gt; FTP Exempt Zone &gt; Add</b></p> 
---	---

FIELD	DESCRIPTION	EXAMPLE
From Address	Exempt zone record IP address from	192.168.40.10
To Address	Exempt zone record IP address to	192.168.40.30

Table 15-3 FTP Filter add an exempt zone entry

<p><b>Step 4 - Show the Exempt Zones</b></p> <p>Here we can discover that new added Exempt Zone record is appeared.</p>	<p><b>ADVANCED SETTINGS &gt; Content Filters &gt; FTP Filter &gt; FTP Exempt Zone</b></p> 
---	---

# Part V

## Intrusion Detection System

# Chapter 16

## Intrusion Detection Systems

*This chapter introduces Intrusion Detection System (IDS) and explains how to implement it.*

### 16.1 Demands

Although Firewall settings are correct, there may still be some crackers intrude our system. Crackers hack into our 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.

### 16.2 Objectives

1. Detect any attacks towards our DMZ servers.
2. Instantly notify our network administrators what attacks have been detected.

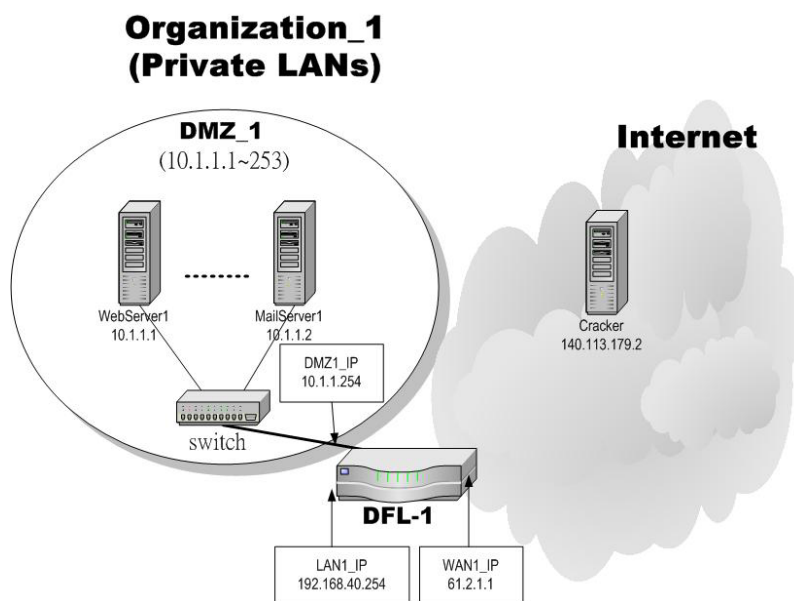


Figure 16-1 Some cracker in the Internet would try to hack our company

### 16.3 Methods

1. Specify where our Web server is located to let the IDS on the DFL-1500 focus more on the attacks.
2. Setup logs to email to the specified email address when the log is full. You can also set daily/weekly emails to periodically monitor the IDS logs.

## 16.4 Steps


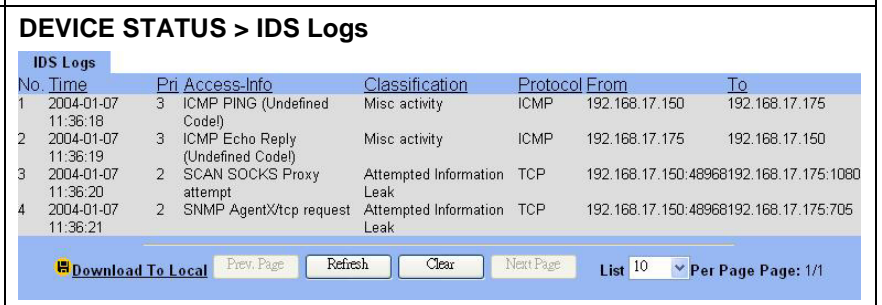

<p><b>Step 1 – Enable IDS</b></p> <p>Check the Enable IDS checkbox. Enter the DMZ IP subnet and the designated HTTP server. The subnets are specified in the types like 192.168.40.0/24 and 10.1.1.1/32. Check all options and click the Apply button.</p>	<div style="border: 1px solid black; padding: 5px;"> <p><b>ADVANCED SETTINGS &gt; IDS &gt; IDS Status</b></p> <p>IDS Status <a href="#">Update Rule</a></p> <p><input checked="" type="checkbox"/> Enable IDS</p> <hr/> <p><b>Detect Attacks Towards</b></p> <p>Example      Setting 192.168.1.0/24 will make IDS detect this network</p> <p>DMZ/LAN      <input type="text" value="192.168.40.0/24"/></p> <p>SMTP Servers      <input type="text" value="any"/></p> <p>HTTP Servers      <input type="text" value="10.1.1.1/32"/></p> <p>DNS Servers      <input type="text" value="any"/></p> <p>SQL Servers      <input type="text" value="any"/></p> <p>TELNET Servers      <input type="text" value="any"/></p> <hr/> <p><b>Options</b></p> <p><input checked="" type="checkbox"/> IP Defragment</p> <p><input checked="" type="checkbox"/> Stateful Inspection</p> <p><input checked="" type="checkbox"/> TCP Stream Reassembly(Stateful Inspection must be checked)</p> <p><input checked="" type="checkbox"/> Normalize HTTP Requests</p> <p><input checked="" type="checkbox"/> Normalize RPC Traffic</p> <p><input checked="" type="checkbox"/> Back Orifice Detector</p> <p><input checked="" type="checkbox"/> Normalize Telnet Negotiation String</p> <p><input checked="" type="checkbox"/> ARP Spoof Detection</p> <p style="text-align: right;"><input type="button" value="Apply"/> <input type="button" value="Reset"/></p> </div>
--	--

FIELD	DESCRIPTION	EXAMPLE
Enable IDS	Enable IDS feature of DFL-1500	enabled
Detect Attacks Towards	Specified the IP address region of each DMZ/LAN, Server area.	
<b>Options</b>		
IP Defragment	This option is designed to memory efficient. This has configurable memory usage and fragment timeout options. It uses the default memory limit of 4194304 bytes (4 MB) and a timeout period of 60 seconds. The timeout period is used to determine a length of time that an unassembled fragment should be discarded.	enabled
Stateful Inspection	This option provides TCP stream reassembly and stateful analysis capabilities. Robust stream reassembly capabilities ignore "stateless" attacks such as stick. It also gives large scale users the ability to track more than 256 simultaneous TCP streams. It should be able to scale to handle 32,768 simultaneous TCP connections in its default configuration.	enabled
TCP Stream Reassembly	This item is collocating "Stateful Inspection" to increase prevention ability of packet reassemble.	enabled
Normalize HTTP Requests	This option is used to process HTTP URI strings and convert their data to non-obfuscated ASCII strings. For example, HTTP defines a hex encoding method for characters such that the string 20% is interpreted as a single space ex. Webservers are designed to handle the myriad of clients available as well as being written to support many different standards. Microsoft webservers handle additional types of encodings as well as some specific bugs.	enabled
Normalize RPC Traffic	This option normalizes RPC multiple fragmented records into a single unfragmented record. It does this by normalizing the packet into the the packet buffer. If "Stateful Inspection" option is enabled, it will only process client side traffic. It defaults to running on ports 111 and 32771.	enabled
Back Orifice Detector	This option will enable the detection of "Back Orifice".	enabled



Normalize Telnet Negotiation String	This option will normalize telnet control protocol characters from the session data. It accepts a list of ports to run on as arguments. It defaults to running on ports 21, 23, 25, and 119.	enabled
ARP Spoof Detection	This option will enable the detection of “ARP Spoof”.	enabled

Table 16-1 IDS option list explanation

<p><b>Step 2 – Setup Logs</b></p> <p>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.</p>	<p><b>DEVICE STATUS &gt; Log Config &gt; Mail Logs</b></p> 																																								
<p><b>Step 3 – View logs</b></p> <p>If there are attacks towards the WAN port from the public Internet, there will be logs describing the details.</p>	<p><b>DEVICE STATUS &gt; IDS Logs</b></p>  <table border="1"> <thead> <tr> <th>No.</th> <th>Time</th> <th>Pri</th> <th>Access-Info</th> <th>Classification</th> <th>Protocol</th> <th>From</th> <th>To</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2004-01-07 11:36:18</td> <td>3</td> <td>ICMP PING (Undefined Code)</td> <td>Misc activity</td> <td>ICMP</td> <td>192.168.17.150</td> <td>192.168.17.175</td> </tr> <tr> <td>2</td> <td>2004-01-07 11:36:19</td> <td>3</td> <td>ICMP Echo Reply (Undefined Code)</td> <td>Misc activity</td> <td>ICMP</td> <td>192.168.17.175</td> <td>192.168.17.150</td> </tr> <tr> <td>3</td> <td>2004-01-07 11:36:20</td> <td>2</td> <td>SCAN SOCKS Proxy attempt</td> <td>Attempted Information Leak</td> <td>TCP</td> <td>192.168.17.150:48968</td> <td>192.168.17.175:1080</td> </tr> <tr> <td>4</td> <td>2004-01-07 11:36:21</td> <td>2</td> <td>SNMP AgentX/tcp request</td> <td>Attempted Information Leak</td> <td>TCP</td> <td>192.168.17.150:48968</td> <td>192.168.17.175:705</td> </tr> </tbody> </table>	No.	Time	Pri	Access-Info	Classification	Protocol	From	To	1	2004-01-07 11:36:18	3	ICMP PING (Undefined Code)	Misc activity	ICMP	192.168.17.150	192.168.17.175	2	2004-01-07 11:36:19	3	ICMP Echo Reply (Undefined Code)	Misc activity	ICMP	192.168.17.175	192.168.17.150	3	2004-01-07 11:36:20	2	SCAN SOCKS Proxy attempt	Attempted Information Leak	TCP	192.168.17.150:48968	192.168.17.175:1080	4	2004-01-07 11:36:21	2	SNMP AgentX/tcp request	Attempted Information Leak	TCP	192.168.17.150:48968	192.168.17.175:705
No.	Time	Pri	Access-Info	Classification	Protocol	From	To																																		
1	2004-01-07 11:36:18	3	ICMP PING (Undefined Code)	Misc activity	ICMP	192.168.17.150	192.168.17.175																																		
2	2004-01-07 11:36:19	3	ICMP Echo Reply (Undefined Code)	Misc activity	ICMP	192.168.17.175	192.168.17.150																																		
3	2004-01-07 11:36:20	2	SCAN SOCKS Proxy attempt	Attempted Information Leak	TCP	192.168.17.150:48968	192.168.17.175:1080																																		
4	2004-01-07 11:36:21	2	SNMP AgentX/tcp request	Attempted Information Leak	TCP	192.168.17.150:48968	192.168.17.175:705																																		
<p><b>Step 4 – Update Attack Patterns</b></p> <p>IDS attack patterns require frequent updates because there are many new attacks every week. Please check your DNS settings and click Apply. The DFL-1500 will connect to fwupdate.dlinktw.com.tw to fetch any new signatures.</p>	<p><b>ADVANCED SETTINGS &gt; IDS &gt; Update Rule</b></p> 																																								

# Part VI

## Bandwidth Management

# Chapter 17

## Bandwidth Management

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

### 17.1 Demands

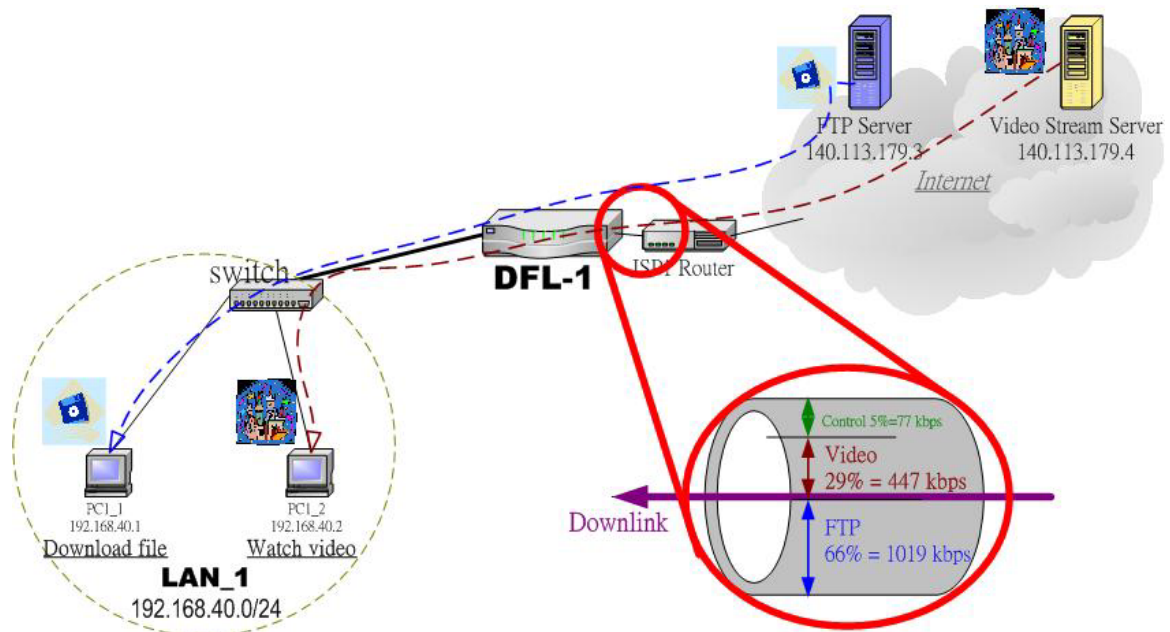


Figure 17-1 Use bandwidth management mechanism to shape the data flow on the downlink direction

- As the above diagram Figure 17-1 illustrates, PC1\_1 is downloading the MP3 files from the FTP Server (140.113.179.3). This occupies the bandwidth of PC1\_2 who is watching the video provided by the Video Stream Server (140.113.179.4), causing the video to be blocked and to have poor quality. Here we will make sure that PC1\_2 has the smooth stream quality that must have at least 400 kbps speed rate.

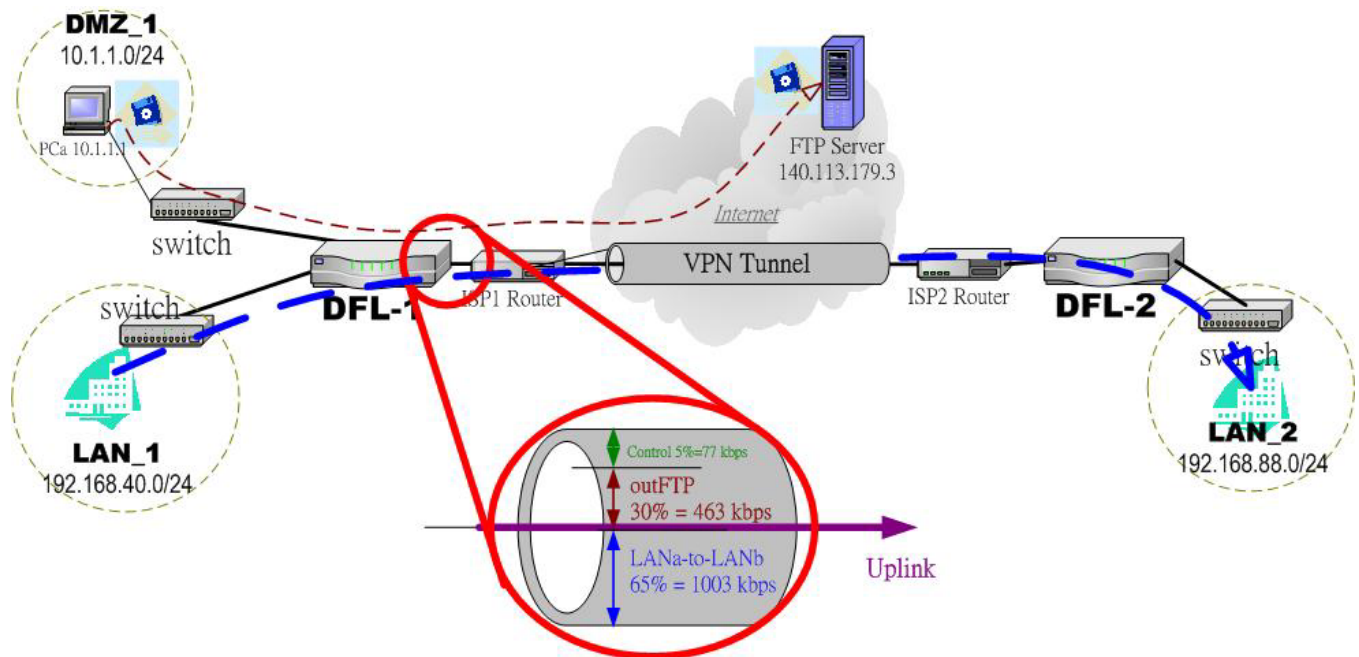


Figure 17-2 Use bandwidth management mechanism to shape the data flow on the uplink direction

- As the above Figure 17-2 illustrates, PCa (10.1.1.1) is uploading files to the FTP Server (140.113.179.3), causing the blocking of the VPN transfer from LAN\_1 to LAN\_2. We want to make sure that the VPN tunnel links is reserved at least 1000 kbps speed rate. And the nonuse bandwidth of LANa-to-LANb will raise the bandwidth of PCa uploading files

## 17.2 Objectives

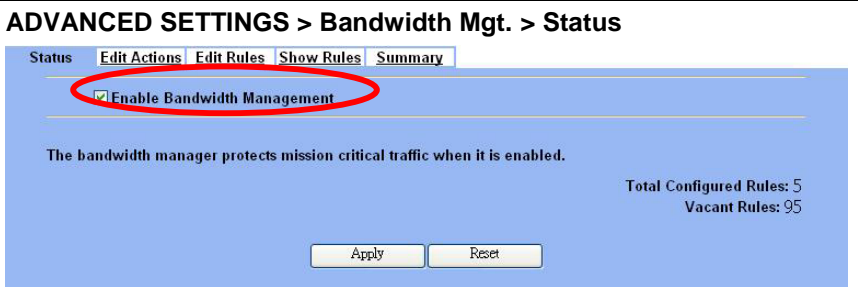
- Guarantee the video quality of the PC1\_2 (192.168.40.2). The remaining bandwidth can be utilized by the PC1\_1 (192.168.40.1) to download the mp3 files from FTP Server (140.113.179.3). However, when the movie is over, the whole bandwidth can be utilized by the PC1\_1.
- Reserve at least 1Mbps for the LANa-to-LANb transfer. The DMZ\_1 PCs can share the remaining 463kbps for uploading files. However, when the LANa-to-LANb traffic has only 300kbps, the DMZ PCs can occupy the remaining bandwidth from LANa-to-LANb (1003kbps - 300kbps), and add the original bandwidth 463kbps. So, the total bandwidth is 1166kbps [(1003kbps - 300kbps) + 463kbps].

## 17.3 Methods

- Partition the inbound bandwidth (1.544Mbps) into two classes, the FTP and the Video classes. Set the Video class to obtain 447kbps (29%). Set the FTP class to obtain 1019kbps and set it to be able to borrow any available bandwidth from others.
- Partition the outbound bandwidth (1.544Mbps) into two classes, the LANa-to-LANb (65% 1003kbps) and the outFTP (30% 463kbps) classes. Set the LANa-to-LANb to obtain 1Mbps and set it to be able to borrow from other bandwidth.

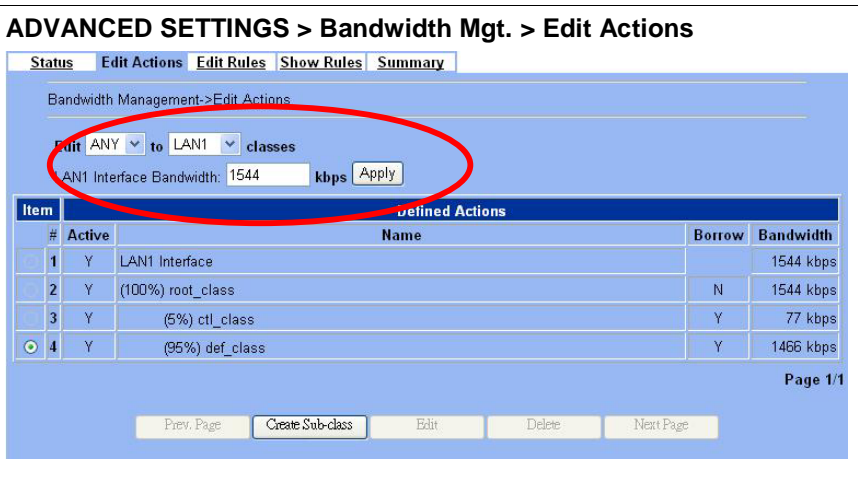
## 17.4 Steps

### 17.4.1 Inbound Traffic Management

<p><b>Step 1 - Enable Bandwidth Management</b></p> <p>Check the Enable Bandwidth Management checkbox, click the Apply.</p>	<p><b>ADVANCED SETTINGS &gt; Bandwidth Mgt. &gt; Status</b></p> 
--	--

FIELD	DESCRIPTION	EXAMPLE
Enable Bandwidth Management	Enable Bandwidth Management feature of DFL-1500	enabled
Apply	Apply the settings which have been configured.	N/A
Reset	Clean the filled data and restore the original one.	N/A

Table 17-1 Setup status page of Bandwidth Management

<p><b>Step 2 - Setup the LAN1 Link</b></p> <p>Select ANY to LAN1 to setup traffic that will transmit by the LAN1 interface. Enter the LAN1 interface bandwidth as 1544kbps. Click the Apply button to enforce the LAN1 link bandwidth to be 1544kbps. 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.</p>	<p><b>ADVANCED SETTINGS &gt; Bandwidth Mgt. &gt; Edit Actions</b></p> 
---	--

FIELD	DESCRIPTION	EXAMPLE
Edit __ to __ classes	Select the direction of action which you are going to configure one.	Edit ANY to LAN1 classes
WAN1 Interface Bandwidth __ kbps	Fill the real bandwidth which is located in the upper direction.	1544
Prev. Page	If there are more than one action pages, you can press Prev. Page to back to the previous page.	N/A
Create-Sub-class	Create a sub class from the indicated class.	N/A
Edit	Edit the properties of the existent class.	N/A

Delete	Delete the indicated class.	N/A
Next Page	If there are more than one action pages, you can press Next Page to go to the next page.	N/A

Table 17-2 Setup edit actions page of Bandwidth Management

<p><b>Step 3 - Add new classes</b></p> <p>Create a sub-class named <code>inFTP</code> from the default class. Enter 66% in the <code>bandwidth</code> field. Make sure that <code>Borrow</code> button is checked and then <code>inFTP</code> class will enlarge the bandwidth from borrowing other unused bandwidth. Finally, click <code>Apply</code> button. See the steps in the right diagram.</p> <p>Subsequently, we will continue to setup another class, such as <code>inVideo</code> class. Select the default class and click the <code>Create Sub-Class</code> to create another sub-class named <code>inVideo</code> from the default class. Enter 29% in the <code>bandwidth</code> field and click <code>Apply</code>.</p>	<p><b>ADVANCED SETTINGS &gt; Bandwidth Mgt. &gt; Edit Actions &gt; Create Sub-class</b></p>
---	---

FIELD	DESCRIPTION	EXAMPLE
Activate this class	Enable the bandwidth management class for later using	enabled
Class name	Bandwidth management class name	inFTP
Bandwidth	How many percentage does this class occupy higher class?	66
Borrow	When the bandwidth of other class is idle, it will use the bandwidth of other class to increase bandwidth temporarily.	Enabled
Back	back to previous configuration page.	N/A
Apply	Apply the settings which have been configured.	N/A
Reset	Clean the filled data and restore the original one.	N/A

Table 17-3 Add new class in the bandwidth management feature

**Step 4 - Partition into Classes**

Now there are two actions under the default action.

**ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-Class**

Bandwidth Management->Edit Actions

Edit ANY to LAN1 classes

LAN1 Interface Bandwidth: 1544 kbps Apply

Item #	Active	Name	Borrow	Bandwidth
1	Y	LAN1 Interface		1544 kbps
2	Y	(100%) root_class	N	1544 kbps
3	Y	(5%) cti_class	Y	77 kbps
4	Y	(95%) def_class	Y	1466 kbps
5	Y	(29%) inVideo	N	447 kbps
6	Y	(66%) inFTP	Y	1019 kbps

Page 1/1

Prev. Page Create Sub-class Edit Delete Next Page

**Step 5 - Setup ANY-to-LAN1 Rules**

Select ANY 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 > Bandwidth Mgt. > Edit Rules**

Bandwidth Management->Edit Rules

Edit ANY to LAN1 rules

Packets are top-down matched by the rules.

Item #	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action
1	Y	Default	ANY to LAN1	Any	Any	Any	def_class

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

FIELD	DESCRIPTION	EXAMPLE
Edit __ to __ rules	Select the rule direction of rule which you are going to configure.	Edit ANY to LAN1 rules
Prev. Page	If there are more than one rule pages, you can press Prev. Page to back to the previous page.	N/A
Insert	Insert a new rule.	N/A
Edit	Edit the properties of the existent rule.	N/A
Delete	Delete the indicated rule.	N/A
Move Before __	Move the selected rule to the front of the indicated rule number.	Move Before 1
Next Page	If there are more than one action rules, you can press Next Page to go to the next page.	N/A

Table 17-4 Setup edit rules page of Bandwidth Management



**Step 6 - Customize the Rules**

Enter a rule name such as inFTP, enter the Source IP as 140.113.179.3 and the netmask as 255.255.255.255. Enter the Dest. IP as 192.168.40.1 and the netmask as 255.255.255.255. Select the action to be inFTP. In this way, all FTP Server to PC1\_1 packets will be put into the inFTP queue and scheduled out at 1019kbps bandwidth. Click Apply to store the changes. Repeat the same procedure for the inVideo class.

**ADVANCED SETTINGS > Bandwidth Mgt. > Edit Rules > Insert**

	FIELD	DESCRIPTION	EXAMPLE
Status	Activate this rule	Enable this bandwidth management rule	Enabled
	Rule name	The bandwidth management rule name	InFTP
Condition	Source IP & Netmask	When source IP address of incoming packets conforms the "Source IP/Netmask" settings, do the "Action".	140.113.179.3 255.255.255.255
	Dest. IP & Netmask	When destination IP address of incoming packets conforms the "Dest IP/Netmask" settings, do the "Action".	192.168.40.1 255.255.255.255
	Service	Verify if the service of packet belongs to TCP, UDP, or ICMP type.	Any
	Configure src. port?	If the service is TCP or UDP, we can setup the range of the source ports. When selecting the range of source ports, it can be a single port or a range of ports.	disabled
	Configure dest. port?	If the service is TCP, UDP, we can setup the range of the destination ports. When selecting the range of the destination ports, it can be single port or a range of ports.	disabled
Action	Queue the matched packets in class	Allocate these packets which conform this rule to the classes of the previous setting.	inFTP
Back		back to previous configuration page.	N/A
Apply		Apply the settings which have been configured.	N/A
Reset		Clean the filled data and restore the original one.	N/A

Table 17-5 Add a new Bandwidth Management rule



**Step 7 - View the rules**

The DFL-1500 is configured to direct inFTP-matched packets into the inFTP queue (1019kbps), inVideo-matched packets into the inVideo queue (447kbps). The other traffic will be put into the def\_class queue (any available bandwidth).

**ADVANCED SETTINGS > Bandwidth Mgt. > Edit Rules**

Status Edit Actions Edit Rules Show Rules Summary

Bandwidth Management->Edit Rules

Edit ANY to LAN1 rules

Packets are top-down matched by the rules.

Item	Status	Condition					Action
#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action
1	Y	InVideo	ANY to LAN1	140.113.179.4/255.255.255.255	192.168.40.2/255.255.255.255	Any	InVideo
2	Y	InFTP	ANY to LAN1	140.113.179.3/255.255.255.255	192.168.40.1/255.255.255.255	Any	inFTP
3	Y	Default	ANY to LAN1	Any	Any	Any	def_class

Page 1/1

Prev. Page Insert Edit Delete Move Before: 1 Next Page

**17.4.2 Outbound Traffic Management**

**Step 1 - Enable Bandwidth Management**

Check the Enable Bandwidth Management checkbox, click the Apply.

**ADVANCED SETTINGS > Bandwidth Mgt. > Status**

Status Edit Actions Edit Rules Show Rules Summary

Enable Bandwidth Management

The bandwidth manager protects mission critical traffic when it is enabled.

Total Configured Rules: 7  
Vacant Rules: 93

Apply Reset

**Step 2 - Setup the WAN1 Link**

Select ANY to WAN1 to setup traffic that will transmit 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**

Status Edit Actions Edit Rules Show Rules Summary

Bandwidth Management->Edit Actions

Edit ANY to WAN1 classes

WAN1 Interface Bandwidth: 1544 kbps Apply

Item	Active	Defined Actions	
#		Name	Borrow Bandwidth
1	Y	WAN1 Interface	1544 kbps
2	Y	(100%) root_class	N 1544 kbps
3	Y	(5%) ctt_class	Y 77 kbps
4	Y	(95%) def_class	Y 1466 kbps

Page 1/1

Prev. Page Create Sub-class Edit Delete Next Page

**Step 3 - Partition into Classes**

Create a sub-class named LANa-to-LANb from the default class. Enter 65% in the bandwidth field, check the Borrow button, and click Apply. Select the default class and click the Create Sub-Class to create another sub-class named outFTP from the default class. Enter 30% in the bandwidth field and click Apply. Now there are two actions under the default action. They are separately LANa-to-LANb and outFTP class.

**ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-Class**

Status Edit Actions Edit Rules Show Rules Summary

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	(65%) LANa-to-LANb	Y	1003 kbps
6	Y	(30%) outFTP	N	463 kbps

Page 1/1

Prev. Page Create Sub-class Edit Delete Next Page

**Step 4 - Setup ANY-to-WAN1 Rules**

Select ANY 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 > Bandwidth Mgt. > Edit Rules**

Status Edit Actions Edit Rules Show Rules Summary

Bandwidth Management->Edit Rules

Edit ANY to WAN1 rules

Packets are top-down matched by the rules.

Item	Status		Condition				Action	
	#	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action
1	Y		Default	ANY to WAN1	Any	Any	Any	def_class

Page 1/1

Prev. Page **Insert** Edit Delete Move Before: 1 Next Page

**Step 5 - Customize the Rules**

Enter a rule name such as outVPN, enter the Source IP as 192.168.40.0 and the netmask as 255.255.255.0. Enter the Dest. IP as 192.168.88.0 and the netmask as 255.255.255.0. Select the action to be LANa-to-LANb. In this way, all outbound packets to the LAN\_2 area will be put into the LANa-to-LANb queue and scheduled out at 1003kbps bandwidth. Click Apply to store the changes. Repeat the same procedure for the outWebDownload class.

**ADVANCED SETTINGS > Bandwidth Mgt. > Edit Rules > Insert**

Status Edit Actions Edit Rules Show Rules Summary

Bandwidth Management->Edit Rules->Insert

Insert a new ANY-to-WAN1 Bandwidth Management rule

**Status**

Activate this rule

Rule name: outVPN

**Condition**

Source IP: 192.168.40.0 Netmask: 255.255.255.0

Dest. IP: 192.168.88.0 Netmask: 255.255.255.0

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)

**Action**

Queue the matched packets in class: LANa-to-LANb

Back Apply Reset

**Step 6 - View the rules**

The DFL-1500 is configured to direct outFtpUpload matched packets into the outFTP queue (463kbps), outVPN matched packets into the LANa-to-LANb queue (1003kbps). Here we reserve 65% WAN1 bandwidth for the LANa-to-LANb 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 > Bandwidth Mgt. > Edit Rules**

[Status](#) | [Edit Actions](#) | [Edit Rules](#) | [Show Rules](#) | [Summary](#)

Bandwidth Management->Edit Rules

Edit ANY to WAN1 rules

Packets are top-down matched by the rules.

Item #	Status		Condition				Action
	Active	Name	Direction	Source IP Address	Dest. IP Address	Service	Action
1	Y	outFtpUpload	ANY to WAN1	10.1.1.0/255.255.255.0	140.113.179.3/255.255.255.255	Any	outFTP
2	Y	outVPN	ANY to WAN1	192.168.40.0/255.255.255.0	192.168.88.0/255.255.255.0	Any	LANa-to-LANb
3	Y	Default	ANY to WAN1	Any	Any	Any	def_class

Page 1/1

# Part VII

## System Maintenance

# Chapter 18

## System Status

### 18.1 Demands

1. Since we have finished the settings of DFL-1500, we need to gather the device information quickly. Then we can have a overview of the system status.

### 18.2 Objectives

1. We can know the current situation easily through an integrated interface.

### 18.3 Methods

1. Through DEVICE STATUS > System Status path, we can get the needed information.

### 18.4 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 Status	Network Status	CPU & Memory	DHCP Table
System Name: <b>DFL-1.dlink.com</b>			
Firmware Version: <b>NetOS Ver1.50B (DLINK) #0: Thu Dec 4 03:44:32 CST 2003</b>			
Default gateway: <b>192.168.17.254</b>			
Primary DNS: <b>168.95.1.1</b>			
Secondary DNS:			
<b>Port1:</b>	<b>WAN1 (Static IP)[Default]</b>	IP Address: <b>192.168.17.204</b>	Subnet Mask: <b>255.255.255.0</b>
<b>Port2:</b>	<b>WAN2 (PPPoE)</b>	IP Address: <b>not set</b>	
<b>Port3:</b>	<b>DMZ1</b>	IP Address: <b>10.1.40.254</b>	Subnet Mask: <b>255.255.255.0</b>
<b>Port4:</b>	<b>LAN1</b>	IP Address: <b>192.168.40.254</b>	Subnet Mask: <b>255.255.255.0</b>
<b>Port5:</b>	<b>LAN2</b>	IP Address: <b>192.168.2.254</b>	Subnet Mask: <b>255.255.255.0</b>

#### 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

System Status	Network Status	CPU & Memory	DHCP Table			
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s
1. <b>WAN1</b>	UP	34601	15690	0	376	1912
2. <b>WAN2</b>	UP	20397	512	0	48	0
3. <b>DMZ1</b>	UP	13060	1	0	24	0
4. <b>LAN1</b>	UP	2741	2188	0	0	0
5. <b>LAN2</b>	UP	744	1	0	0	0

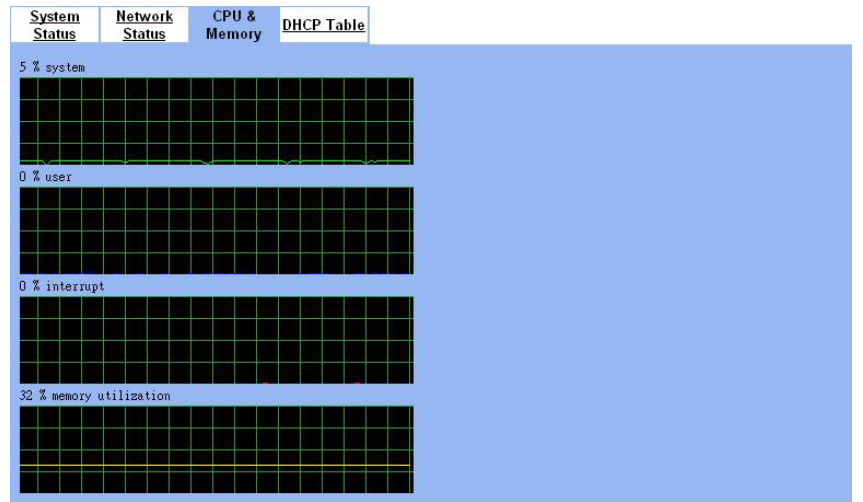
**Step 3 - CPU & Memory**

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	192.168.50.20		00:40:F4:7F:82:4B	2003-12-11 10:38:57

# Chapter 19

## Log System

### 19.1 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 inconvenient to verify the DFL-1500 logs. He / She hopes to decrease the checking procedure.

### 19.2 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 DFL-1500.

### 19.3 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 DFL-1500. Make the log mailed out automatically every periodic time.


### 19.4 Steps

#### 19.4.1 System Logs

<p><b>Step 1 - View System Logs</b></p> <p>Setup Syslog Server by checking the <b>Enable Syslog Server</b>. It will let DFL-1500 send logs to the Syslog Server specified in the "Syslog Server IP Address" field.</p>	<p><b>DEVICE STATUS &gt; System Logs</b></p> <table border="1"> <thead> <tr> <th colspan="4">System Access Logs</th> </tr> <tr> <th>No.</th> <th>Time</th> <th>Source-IP</th> <th>Access-Info</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2003-12-31 09:37:54</td> <td>DFL-1500</td> <td>SYSTEM: [S1] Wall Startup.</td> </tr> <tr> <td>2</td> <td>2003-12-31 09:37:55</td> <td>DFL-1500</td> <td>Firewall: Reload all rules at startup</td> </tr> <tr> <td>3</td> <td>2003-12-31 09:37:55</td> <td>DFL-1500</td> <td>NAT: rule for Basic-LAN2 added</td> </tr> <tr> <td>4</td> <td>2003-12-31 09:37:55</td> <td>DFL-1500</td> <td>NAT: rule for Basic-DMZ1 added</td> </tr> <tr> <td>5</td> <td>2003-12-31 09:37:57</td> <td>DFL-1500</td> <td>SYSTEM: [S5] HTTP started.</td> </tr> <tr> <td>6</td> <td>2003-12-31 09:37:58</td> <td>DFL-1500</td> <td>SYSTEM: [S6] HTTPS started.</td> </tr> <tr> <td>7</td> <td>2003-12-31 09:42:58</td> <td>192.168.17.170</td> <td>AUTH: [A1] admin login success (192.168.17.172:443).</td> </tr> <tr> <td>8</td> <td>2003-12-31 09:43:12</td> <td>192.168.17.170</td> <td>AUTH: [A2] admin logout (192.168.17.172:443).</td> </tr> <tr> <td>9</td> <td>2003-12-31 09:43:19</td> <td>CLI</td> <td>AUTH: admin login from console success.</td> </tr> <tr> <td>10</td> <td>2003-12-31 09:43:21</td> <td>CMD: CLI</td> <td>CLI:enable</td> </tr> </tbody> </table> <p> <input type="button" value="Download To Local"/> <input type="button" value="Prev Page"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/> <input type="button" value="Next Page"/> List <input type="text" value="10"/> Per Page Page: 1/3 </p>	System Access Logs				No.	Time	Source-IP	Access-Info	1	2003-12-31 09:37:54	DFL-1500	SYSTEM: [S1] Wall Startup.	2	2003-12-31 09:37:55	DFL-1500	Firewall: Reload all rules at startup	3	2003-12-31 09:37:55	DFL-1500	NAT: rule for Basic-LAN2 added	4	2003-12-31 09:37:55	DFL-1500	NAT: rule for Basic-DMZ1 added	5	2003-12-31 09:37:57	DFL-1500	SYSTEM: [S5] HTTP started.	6	2003-12-31 09:37:58	DFL-1500	SYSTEM: [S6] HTTPS started.	7	2003-12-31 09:42:58	192.168.17.170	AUTH: [A1] admin login success (192.168.17.172:443).	8	2003-12-31 09:43:12	192.168.17.170	AUTH: [A2] admin logout (192.168.17.172:443).	9	2003-12-31 09:43:19	CLI	AUTH: admin login from console success.	10	2003-12-31 09:43:21	CMD: CLI	CLI:enable
System Access Logs																																																	
No.	Time	Source-IP	Access-Info																																														
1	2003-12-31 09:37:54	DFL-1500	SYSTEM: [S1] Wall Startup.																																														
2	2003-12-31 09:37:55	DFL-1500	Firewall: Reload all rules at startup																																														
3	2003-12-31 09:37:55	DFL-1500	NAT: rule for Basic-LAN2 added																																														
4	2003-12-31 09:37:55	DFL-1500	NAT: rule for Basic-DMZ1 added																																														
5	2003-12-31 09:37:57	DFL-1500	SYSTEM: [S5] HTTP started.																																														
6	2003-12-31 09:37:58	DFL-1500	SYSTEM: [S6] HTTPS started.																																														
7	2003-12-31 09:42:58	192.168.17.170	AUTH: [A1] admin login success (192.168.17.172:443).																																														
8	2003-12-31 09:43:12	192.168.17.170	AUTH: [A2] admin logout (192.168.17.172:443).																																														
9	2003-12-31 09:43:19	CLI	AUTH: admin login from console success.																																														
10	2003-12-31 09:43:21	CMD: CLI	CLI:enable																																														


FIELD	DESCRIPTION	EXAMPLE
NO	system logs sequence number	1
Time	The time which is occurred by the specified system event.	2003-12-31 09:37:54
Source-IP	A type of the specified system events.	DFL-1500
Access--Info	The description of the system log.	SYSTEM: [S1] Wall Startup.

19.4.2 Syslog & Mail log

<p><b>Step 1 - Setup Syslog Server</b></p> <p>Setup Syslog Server by checking the <b>Enable Syslog Server</b>. It will let DFL-1500 send logs to the Syslog Server specified in the “Syslog Server IP Address” field.</p>	<p><b>DEVICE STATUS &gt; Log Config &gt; Syslog Server</b></p> 
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable Syslog Server	Enable the Syslog Server feature of DFL-1500	Enabled
Syslog Server IP Address	The IP Address which Syslog Server located.	10.1.1.20
Apply	Apply the configuration in this page	N/A
Reset	Restore the original configuration in this page	N/A

Table 19-1 Setup the Syslog Server

<p><b>Step 2 - Setup Mail Log method</b></p> <p>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 <b>Apply</b> button to finish the settings.</p>	<p><b>DEVICE STATUS &gt; Log Config &gt; Mail Logs</b></p> 
---	--

FIELD	DESCRIPTION	EXAMPLE
Enable Mail Logs	Enable the Mail Logs Server feature of DFL-1500	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	<u>mis@dlink.com</u>
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
Apply	Apply the configuration in this page	N/A
Reset	Restore the original configuration in this page	N/A
Test	test the mail logs configuration in this page	N/A

Table 19-2 Setup the Mail Logs



## Chapter 20

# System Maintenance

*This chapter introduces how to do system maintenance.*

### 20.1 Demands

1. DFL-1500 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 DFL-1500. 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 DFL-1500 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 lose the password, you have to use CLI only because you can never enter the web GUI with the lost password.

### 20.2 Steps for TFTP Upgrade

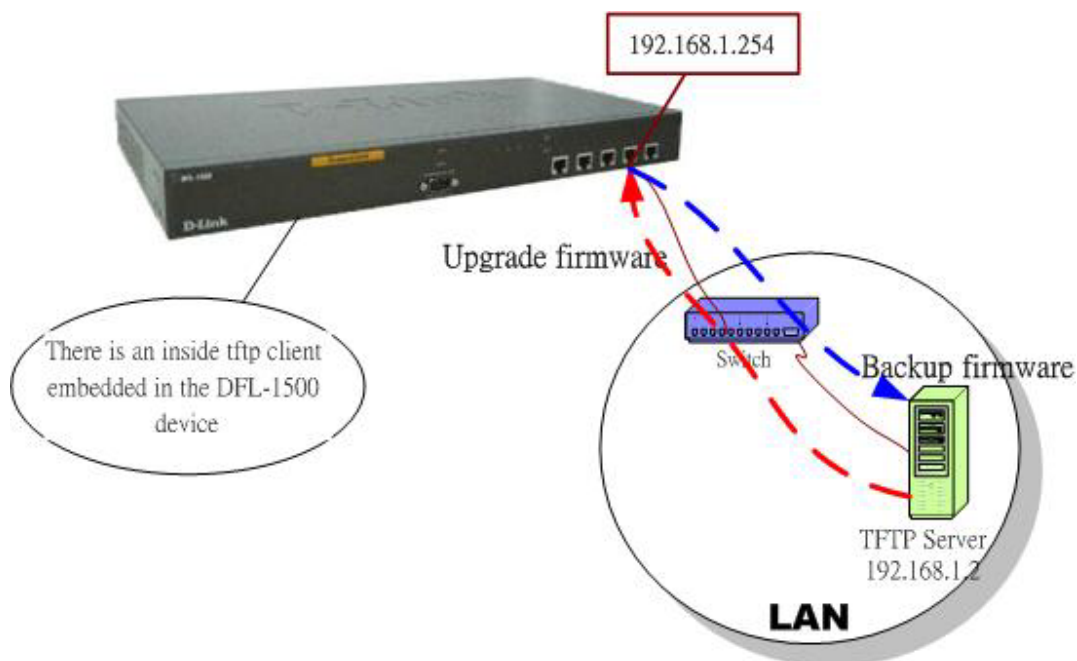
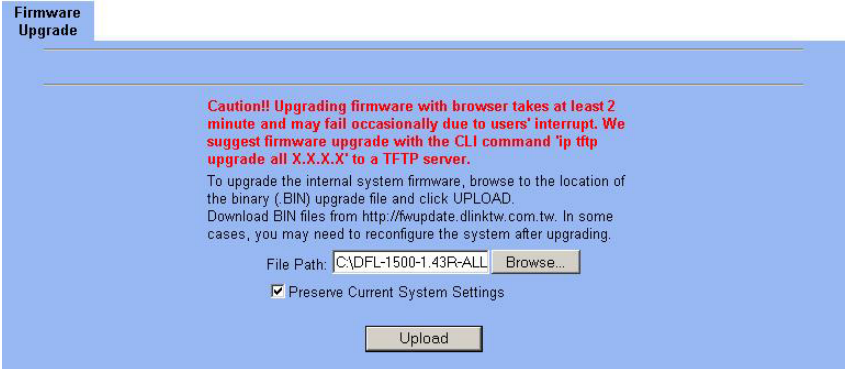


Figure 20-1 Upgrade/Backup firmware from TFTP server

<p><b>Step 1 - Setup TFTP server</b></p> <p>Place the TFTP server <code>TftpServer.exe</code> in the <code>c:\</code> directory and double click to run it. Place all <code>bin</code> files in the <code>c:\</code> as well. Set the PC to be 192.168.1.x to be in the same subnet with the DFL-1500's LAN1. Login to DFL-1500's console. Enter <code>en</code> to enter privileged mode. Configure the LAN1 address so that the DFL-1500 can connect to the TFTP server. The CLI command to configure LAN1 interface is <code>ip ifconfig INTF3 192.168.1.254 255.255.255.0</code>.</p>	<pre>NetOS/i386 (DFL-1500) (tty00) login: admin Password: Welcome to DFL-1500 Firewall/VPN Router!  DFL-1500&gt; en DFL-1500# ip ifconfig INTF3 192.168.1.254 255.255.255.0  DFL-1500#</pre>
<p><b>Step 2 - Upgrade firmware</b></p> <p>Enter <code>IP tftp upgrade combo 192.168.1.x &lt;date&gt;-DFL-1500-&lt;ver&gt;.bin</code></p> <p>Notice: if you want to preserve the previous configuration, add the "preserve" keyword to the end.</p>	<pre>DFL-1500# ip tftp upgrade combo 192.168.1.2 20030910-DFL-1500-1.50R.bin Fetching from 192.168.1.2 for 20030910-DFL-1500-1.50R.bin tftp&gt; tftp&gt; Verbose mode on. tftp&gt; getting from 192.168.1.2:20030910-DFL-1500-1.50R.bin to 20030910-DFL-1500-1.50R.bin [octet]</pre>
<p><b>Step 3 - Reboot the system</b></p> <p>Enter <code>sys reboot now</code> to instantly reboot the system.</p>	<pre>DFL-1500# sys reboot now Rebooting... syncing disks... done rebooting...</pre>
<p><b>Step 4 - Check if OK</b></p>	<pre>ASIC IPsec Enabled Ethernet address 00:80:c8:50:fa:ba, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bb, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bc, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bd, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:be, 10/100 Mb/s wd0: drive supports PIO mode 4 IPsec: Initialized Security Association Processing. Current WAN1 IP = 192.168.17.87       Netmask = 0xffffffff00 WAN2 link has not been initialized.       Gateway = 192.168.17.254       Primary DNS = 168.95.1.1       Secondary DNS = Resuming NAT/RMS/FW settings..... Starting Web-based Configurator.....       HTTP started       HTTPS started Wed Sep 10 18:13:23 2003  NetOS/i386 (DFL-1500) (tty00)  login:</pre>

## 20.3 Steps for Firmware upgrade from Web GUI

<b>Step 1 - Download the newest firmware from web site</b>	Firmware upgrade site : <a href="http://fwupdate.dlinktw.com.tw/">http://fwupdate.dlinktw.com.tw/</a>
<b>Step 2 - Upgrade firmware</b> In the System Tools / Firmware Upgrade page. Select the path of firmware through Browse button, and check the Preserve Current System Settings to reserve original settings. Click the Upload button to upgrade firmware.	

## 20.4 Steps for Factory Reset

### 20.4.1 Steps for NORMAL factory reset


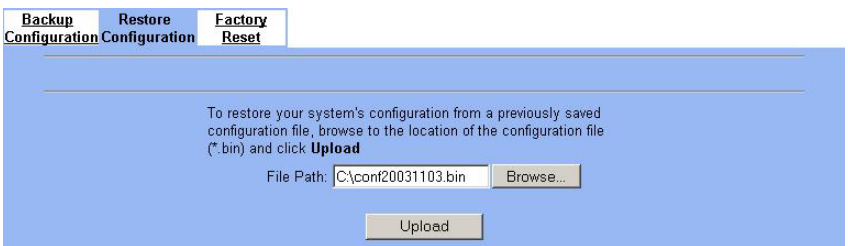
<b>Step 3 - Factory reset</b> Enter <code>sys resetconf</code> now to reset the firmware to factory default. Then enter <code>sys reboot</code> now to instantly reboot the system.	<pre> NetOS/i386 (DFL-1500) (tty00)  login: admin Password: Welcome to DFL-1500 Firewall/VPN Router!  DFL-1500&gt; en DFL-1500# sys resetconf now Resetting Configuration to default... DONE Please reboot the system DFL-1500# sys reboot now Rebooting... syncing disks... done rebooting... </pre>
--	---

### 20.4.2 Steps for EMERGENT factory reset

<b>Step 1 - Enter the boot loader</b> If you forget the password, this is the only way to recover your system. Press <tab> or <space> during the 2-second countdown process.	<pre> &gt;&gt; NetOS Loader (i386), V1.1 (Tue Dec 30 08:39:49 CST 2003) Press &lt;TAB&gt; to prompt Type "boot rescue" to load safe-mode kernel to (1) rescue corrupted firmware (2) reset password for admin - starting in 0 type "?" or "help" for help. &gt; </pre>
---	--

<p><b>Step 2 - Enter the Safe Mode</b></p> <p>Enter <code>boot rescue</code> to enter the emergency kernel. In this kernel, you can use <code>ftp</code> to fetch another firmware to install, or reset the configuration to default even you lost the password.</p>	<pre>&gt; boot rescue 651298+7888404+127552=0x84524c NetOS Ver1.40B (WALL-EMERGENCY) #3: Thu Aug 28 06:02:07 CST 2003 cpu0: Intel (null) Celeron (686-class), 1202.85 MHz total memory = 255 MB avail memory = 228 MB Ethernet address 00:80:c8:50:fa:ba, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bb, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bc, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:bd, 10/100 Mb/s Ethernet address 00:80:c8:50:fa:be, 10/100 Mb/s wd0: drive supports PIO mode 4  DFL-1500&gt;</pre>
<p><b>Step 3 - Factory reset</b></p> <p>Enter <code>sys resetconf</code> now to reset the firmware to factory default. Then enter <code>sys reboot</code> now to instantly reboot the system.</p>	<pre>DFL-1500&gt; en DFL-1500# sys resetconf now Resetting Configuration to default... DONE Please reboot the system DFL-1500# sys reboot now Rebooting...</pre>

## 20.5 Steps for Backup / Restore Configurations

<p><b>Step 1 - Backup the current configuration</b></p> <p>In the System Tools / System Utilities / Backup Configurations page, click <code>Backup</code> button to backup configuration file to local disk.</p>	<p><b>SYSTEM TOOLS &gt; System Utilities &gt; Backup Configuration</b></p> 
<p><b>Step 2 - Restore the previous saving configuration</b></p> <p>In the System Tools / System Utilities / Restore Configurations page. First click the <code>Browse</code> button to select firmware path, and then click <code>Upload</code> button to restore configuration</p>	<p><b>SYSTEM TOOLS &gt; System Utilities &gt; Restore Configuration</b></p> 

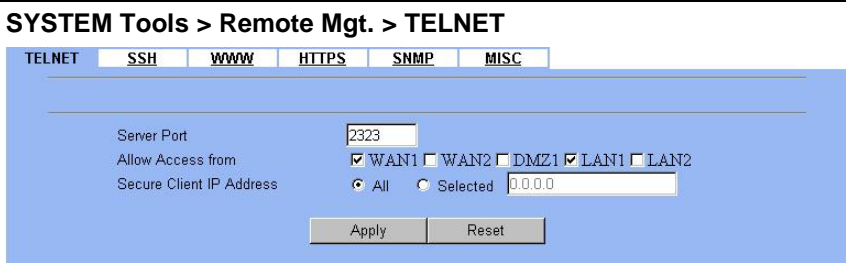
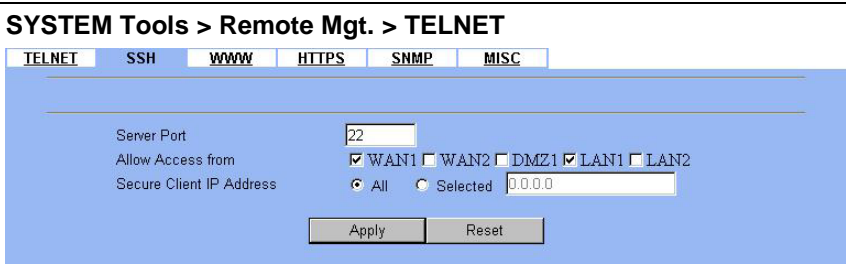
# Appendix A

## Command Line Interface (CLI)

You can configure the DFL-1500 through the web interface (http/https) for the most time. Besides you can use another method, console/ssh/telnet method to configure the DFL-1500 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 DFL-1500 using the CLI commands.

### A.1 Enable the port of DFL-1500

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.

<p><b>Step 1 - Enable remote management / TELNET</b></p> <p>Check the selected port located in the telnet function. And customize the server port which is listened by telnet service.</p>	
<p><b>Step 2 - Enable remote management / SSH</b></p> <p>Check the selected port located in the ssh function. And customize the server port which is listened by ssh service.</p>	

### A.2 CLI commands list

Subsequently, we can use the console/ssh/telnet to connect the DFL-1500. After logging the system successfully, we can use the CLI commands to configure DFL-1500. 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 messages
	tracert	ip tracert 202.11.22.33	Trace route to destination address or hostname

<b>sys</b>			Configure system parameters
	status (st)	sys status	Show system and network status
	version (ver)	sys version	Show DFL-1500 firmware version

Table A-1 Non-privileged mode CLI commands

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
<b>?</b>		?	Show the help menu
<b>disable (dis)</b>		disable	Turn off privileged mode command
<b>exit (ex)</b>		exit	Exit command shell
<b>ip</b>			Configure IP related settings
	arp	ip arp status	Show the ip/MAC mapping table
	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 messages
	tftp	ip tftp upgrade all 1.2.3.4 preserve	Upgrade/Backup from/to tftp server, refer to Section 20.2 for detailed description.
	traceroute	ip traceroute 202.11.22.33	Trace route to destination address or hostname
<b>sys</b>			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
	status (st)	sys status	Show system and network status
	version (ver)	sys version	Show DFL-1500 firmware version

Table A-2 Privileged mode CLI commands

## Appendix B

# Trouble Shooting

1. If the power LED of DFL-1500 is off when I turn on the power?

**Ans :** Check the connection between the power adapter and DFL-1500 power cord. If this problem still exists, contact with your sales vendor.

2. How can I configure the DFL-1500 if I loss the account/password of the DFL-1500 ?

**Ans :** Use the Console mode (CLI) to restore the factory setting, refer to the procedure as prior section 20.4.2.

3. I can't access DFL-1500 via the console port ?

**Ans :** Check the console line and make sure it is connected between your computer serial port and DFL-1500 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 DFL-1500 DMZ1 interface successfully ? Why ?

**Ans :** Follow below items to check if ready or not

- a. Check Basic Setup > DMZ Settings > DMZ1 status fields. Verify whether any data is correctly.
- b. Check Device Status > System Status > Network Status DMZ1 status is "UP". If the status is "DOWN", check if the network line is connectionless ?
- c. Check System Tools > Remote Mgt. > DMZ1. Verify if DMZ1 port checkbox is enabled. The default enabled port is only LAN port.

5. I have already set the WAN1 ip address the same subnet with my pc (configurator), but I can't use https to login DFL-1500 via WAN1 port all the time, why ?

**Ans :**

- a. Be sure that you can ping the WAN1 port, please check the procedure as question 4 description.
- b. 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 - 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 DFL-1500. (The default value from WAN to LAN is block.).

When you add a Firewall rule, the Source IP and Netmask are the IP address/Subnet Mask in the pages of the Remote Address Type. And the Dest IP and Netmask are the IP Address/Subnet Mask in the pages of the Local Address Type. As Figure and Figure indicated, when we 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 setting of the IP address, please refer to the Figure .

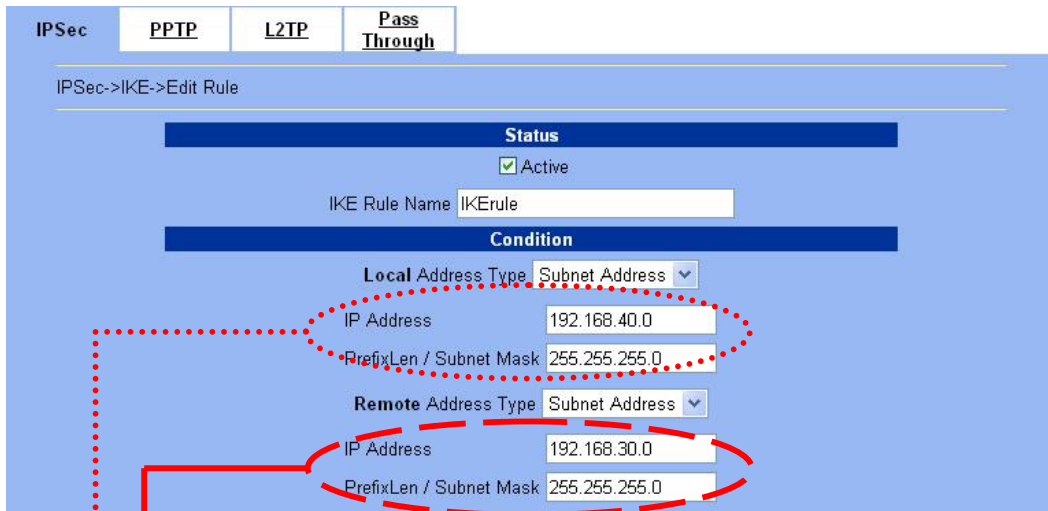


Figure B-1 Inset a new IPsec policy

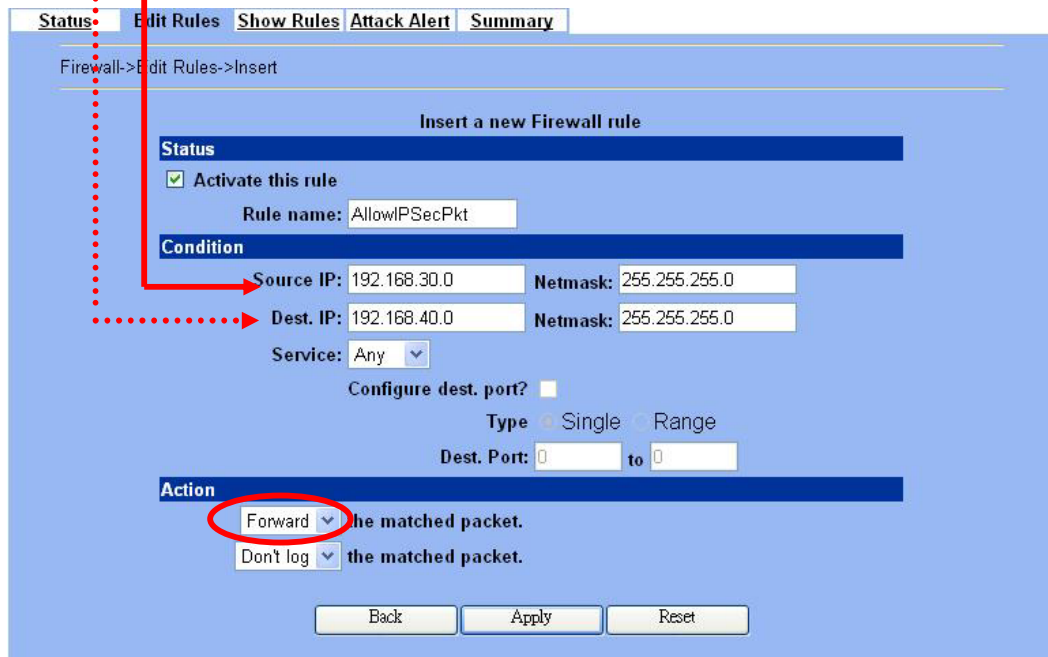


Figure B-2 Insert a new firewall rule in WAN to LAN

7. When I try to login into the DFL-1500, it showed up the following information, as the Figure indicated, and couldn't login successfully.

**Ans :** It is because there is someone logging into the DFL-1500 at the same time with the other IP address. Please logout the system from that IP address first and then login with your IP address again. You are definitely able to login into the DFL-1500.

If the disconnection happens because of the modification of the WAN/LAN/DMZ IP address (for example, you login into the system from LAN1, and then modify the LAN1 IP address), you can solve this problem by one of the following three ways.

- a. Wait for the DFL-1500 session timeout, and then you can login into DFL-1500 again. The default timeout is 5 minutes in the System Tools/Admin Settings/Timeout. After session timeout happens, we could login DFL-1500 another time.



- b. You can use supplied console to login into the DFL-1500 system and then logout the system. That will clean up the zombie left in the system so you will be able to login to the DFL-1500 from the same side.
- c. The final way is to power off the DFL-1500, and then turn on the power. After DFL-1500 reboot, you can login into DFL-1500 again.

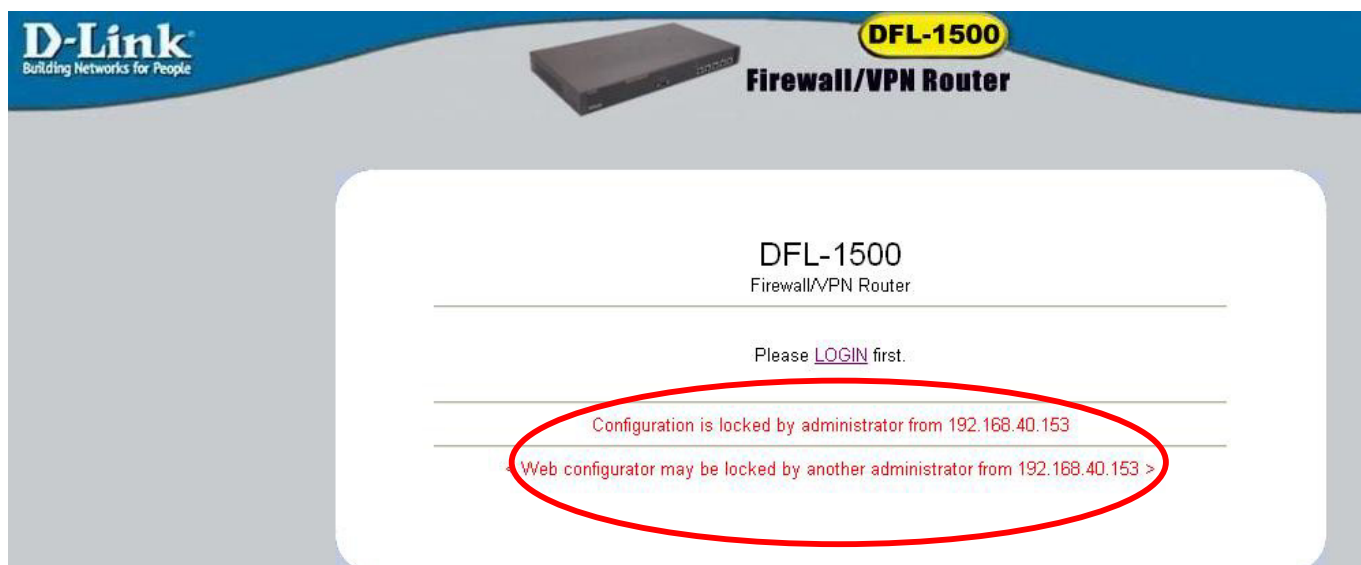


Figure B-3 Login process is locked by the web configurator

8. Why does it always show the message as Figure B-4 indicated when I try to enable bandwidth management feature of DFL-1500?

**Status: Bandwidth management will support PPPoE in the future release.**

Figure B-4 Bandwidth management feature can not cooperate with PPPoE feature

**Ans :** For the present design, you can not turn on bandwidth management in the PPPoE enabled condition. If you need to enable bandwidth management, please choose the WAN connection method (ex. DHCP, fixed IP).

9. 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 “DFL-1500 “. And enter the Domain Name string like “dlink.com” in the firmware version 1.391B. Then the System Name will present as “DFL-1500 .dlink.com”. After upgrading firmware to upper version (ex. 1.50R). It will appear blank in the Source-IP field of System Logs.



# Appendix C Packet Flow

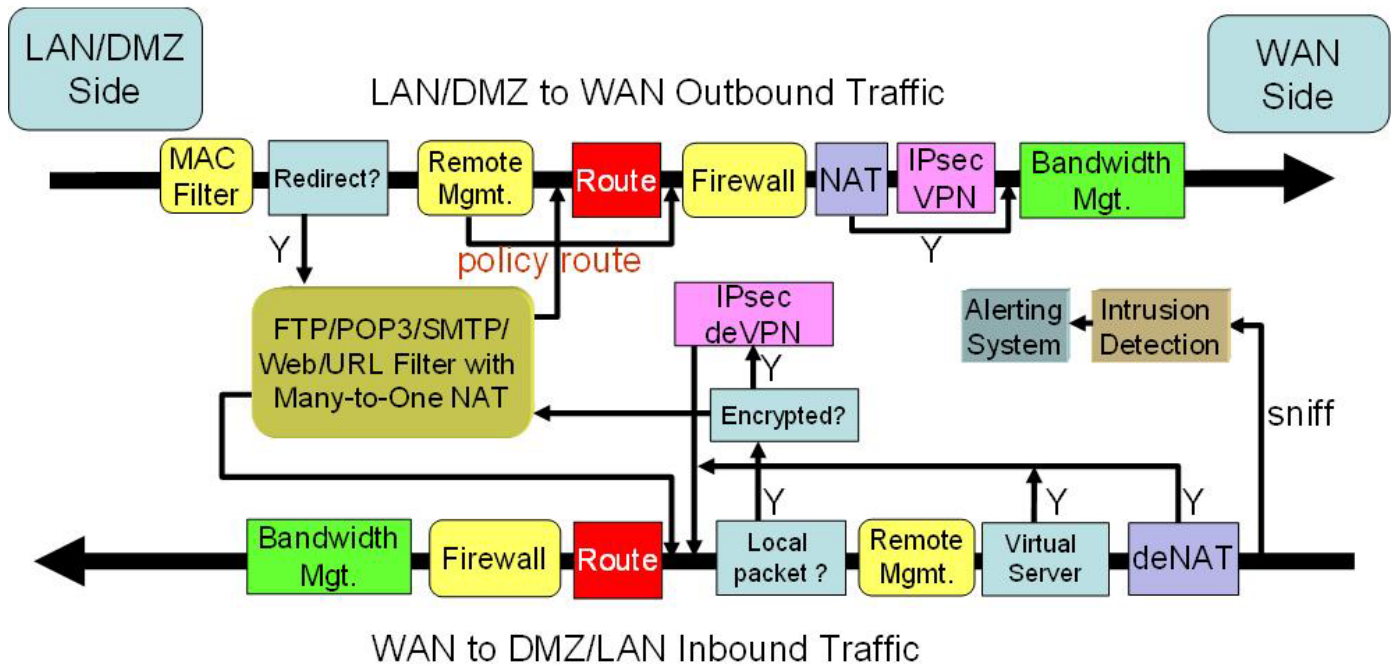


Figure C-1 Packet flow diagrams



## 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 DFL-1500 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.

## Appendix E Index

### B

backup configuration, 122  
 Bandwidth Management, 105  
 bidirectional, 37, 38, 40

### C

Content Filter  
 FTP Filter, 97  
 Mail Filter, 93  
 Web Filter, 85

### D

DDNS, 21  
 DHCP, 8, 10, 16, 17  
 DHCP Relay, 21  
 DNS Proxy, 21

### F

factory reset, 121  
 Firewall, 49  
 firmware upgrade, 121

### I

IDS (Intrusion Dection System), 101

### M

mail log, 118

### N

NAT, 35

### P

POP3, 93, 95

### R

restore configuration, 122  
 Routing, 45  
 policy routing, 45  
 static routing, 45

### S

SMTP, 93, 94  
 syslog, 117, 118

### T

tftp upgrade, 119

### V

Virtual Server, 12, 36, 40, 42  
 VPN, 55  
 AH, 57  
 DH, 56  
 Encapsulation, 56  
 ESP, 57  
 IKE, 59  
 IPSec, 55, 59  
 Key Management, 55  
 L2TP, 79  
 Manual Key, 59  
 PFS, 56  
 PPTP, 75  
 SA(Security Association), 55  
 VPN, 55





## Appendix F

### Hardware

Item	Feature	Detailed Description
<b>1. Hardware</b>		
<b>1.1.1</b>	<b>Chassis</b>	
1.1.1.1	Dimensions	Rack mount 1U size 146 mm (H) x 275 mm (D) x 203 mm (W)(8"*5.75"*10")
1.1.1.2	Look & feel	D-Link style
<b>1.1.2</b>	<b>Key Components</b>	
1.1.2.1	CPU	Intel Celeron 1.2G
1.1.2.2	Memory	256MB 168-P SDRAM
1.1.2.3	10/100M Ethernet MAC and PHY	Intel I82559
1.1.2.4	PCI bridge	Intel FW82801BA
1.1.2.5	Storage	Compact Flash 32MB (San Disk)
1.1.2.6	Memory control HUB	FW82815EP
1.1.2.7	Hardware monitor	Super I/O hardware monitor IT8712F-A
1.1.2.8	Security processor	Safenet 1141 (VPN accelerator board)
<b>1.1.3</b>	<b>Port functions</b>	
1.1.3.1	WAN port	<ul style="list-style-type: none"> <li>▪ 2 port for connecting to outbound WAN</li> <li>▪ RJ-45 connector</li> <li>▪ IEEE 802.3 compliance</li> <li>▪ IEEE 802.3u compliance</li> <li>▪ Support Half/Full-Duplex operations</li> <li>▪ Support backpressure at Half-Duplex operation.</li> <li>▪ Support Auto MDI/MDI-X</li> <li>▪ IEEE 802.3x Flow Control support for Full-Duplex mode</li> </ul>
1.1.3.2	LAN port	<ul style="list-style-type: none"> <li>▪ 2 port for connecting inbound LAN</li> <li>▪ RJ-45 connector</li> <li>▪ IEEE 802.3 compliance</li> <li>▪ IEEE 802.3u compliance</li> <li>▪ Support Half/Full-Duplex operations</li> <li>▪ Support backpressure at Half-Duplex operation.</li> <li>▪ Support Auto MDI/MDI-X</li> <li>▪ IEEE 802.3x Flow Control support for Full-Duplex mode</li> </ul>
2.2.3.3	DMZ port	<ul style="list-style-type: none"> <li>▪ 1 port for connecting to server.</li> <li>▪ RJ-45 connector</li> <li>▪ IEEE 802.3 compliance</li> <li>▪ IEEE 802.3u compliance</li> <li>▪ Support Half/Full-Duplex operations</li> <li>▪ Support backpressure at Half-Duplex operation.</li> <li>▪ Support Auto MDI/MDI-X</li> <li>▪ IEEE 802.3x Flow Control support for Full-Duplex mode</li> </ul>
1.1.3.4	Console port	<ul style="list-style-type: none"> <li>▪ DB-9 male connector</li> <li>▪ Asynchronous serial DTE with full modem controls</li> </ul>

1.1.3.5	LED indication	<p>Per Device:</p> <ol style="list-style-type: none"> <li>Power, Off – Power Off Solid Green – Power On</li> </ol> <p>Ethernet 10/100M Per ports:</p> <ol style="list-style-type: none"> <li>Link/ACT LED Off – No Link Solid Green – Link Blinking Green – Activity</li> </ol>
<b>2. Power</b>		
2.1	Power supply	AT PS, AC 90~230 V full range @ 45~63 Hz
2.2	Power dissipation	180 W
<b>3. Environmental Specifications</b>		
3.1	Operating Temperature	0 ~ 60°C
3.2	Storage Temperature	-25~70°C
3.3	Operating Humidity	5% - 95% non-condensing
<b>4. EMC &amp; Safety Certification</b>		
4.1	EMC Approval	<ul style="list-style-type: none"> <li>▪ FCC class A</li> <li>▪ VCCI class A</li> <li>▪ CE class A</li> <li>▪ C-Tick class A</li> </ul>
4.2	Safety Approval	<ul style="list-style-type: none"> <li>▪ UL</li> <li>▪ CSA</li> <li>▪ TUV/GS</li> <li>▪ T-mark</li> </ul>

## **Appendix G**

# **Version of Software and Firmware**

### **DFL-1500 VPN/Firewall Router**

#### **Version of Components:**

Firmware: v. 1.51R



## Appendix H Customer Support

### **D-Link** Offices

---

<b>Australia</b>	<b>D-Link Australia</b> 1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia TEL: 61-2-8899-1800 FAX: 61-2-8899-1868 TOLL FREE (Australia): 1800-177100 URL: <a href="http://www.dlink.com.au">www.dlink.com.au</a> E-MAIL: <a href="mailto:support@dlink.com.au">support@dlink.com.au</a> & <a href="mailto:info@dlink.com.au">info@dlink.com.au</a>
<b>Brazil</b>	<b>D-Link Brasil Ltda.</b> Edificio Manoel Tabacow Hydal, Rua Tavares Cabral 102 Sala 31, 05423-030 Pinheiros, Sao Paulo, Brasil TEL: (55 11) 3094 2910 to 2920 FAX: (55 11) 3094 2921 E-MAIL: <a href="mailto:efreitas@dlink.cl">efreitas@dlink.cl</a>
<b>Canada</b>	<b>D-Link Canada</b> 2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5095 TOLL FREE: 1-800-354-6522 URL: <a href="http://www.dlink.ca">www.dlink.ca</a> FTP: <a href="ftp:dlinknet.com">ftp.dlinknet.com</a> E-MAIL: <a href="mailto:techsup@dlink.ca">techsup@dlink.ca</a>
<b>Chile</b>	<b>D-Link South America (Sudamérica)</b> Isidora Goyenechea 2934 Of. 702, Las Condes Fono, 2323185, Santiago, Chile, S. A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: <a href="http://www.dlink.cl">www.dlink.cl</a> E-MAIL: <a href="mailto:ccasassu@dlink.cl">ccasassu@dlink.cl</a> & <a href="mailto:tsilva@dlink.cl">tsilva@dlink.cl</a>
<b>China</b>	<b>D-Link China</b> 15 <sup>th</sup> Floor, Science & Technology Tower, No.11, Baishiqiao Road, Haidan District, 100081 Beijing, China TEL: 86-10-68467106 FAX: 86-10-68467110 URL: <a href="http://www.dlink.com.cn">www.dlink.com.cn</a> E-MAIL: <a href="mailto:liweii@digitalchina.com.cn">liweii@digitalchina.com.cn</a>
<b>Denmark</b>	<b>D-Link Denmark</b> Naverland Denmark, Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL: 45-43-969040 FAX: 45-43-424347 URL: <a href="http://www.dlink.dk">www.dlink.dk</a> E-MAIL: <a href="mailto:info@dlink.dk">info@dlink.dk</a>
<b>Egypt</b>	<b>D-Link Middle East</b> 7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt TEL: 202-245-6176 FAX: 202-245-6192 URL: <a href="http://www.dlink-me.com">www.dlink-me.com</a> E-MAIL: <a href="mailto:support@dlink-me.com">support@dlink-me.com</a> & <a href="mailto:fateen@dlink-me.com">fateen@dlink-me.com</a>
<b>Finland</b>	<b>D-Link Finland</b> Pakkalankuja 7A, FIN-01500 Vantaa, Finland TEL: 358-9-2707-5080 FAX: 358-9-2707-5081 URL: <a href="http://www.dlink-fi.com">www.dlink-fi.com</a>
<b>France</b>	<b>D-Link France</b> Le Florilege, No. 2, Allée de la Fresnerie, 78330 Fontenay-le-Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689

URL: [www.dlink-france.fr](http://www.dlink-france.fr)  
E-MAIL: [info@dlink-france.fr](mailto:info@dlink-france.fr)

**Germany D-Link Central Europe (D-Link Deutschland GmbH)**

Schwalbacher Strasse 74, D-65760 Eschborn, Germany  
TEL: 49-6196-77990 FAX: 49-6196-7799300  
URL: [www.dlink.de](http://www.dlink.de)  
BBS: 49-(0) 6192-971199 (analog)  
BBS: 49-(0) 6192-971198 (ISDN)  
INFO: 00800-7250-0000 (toll free)  
HELP: 00800-7250-4000 (toll free)  
REPAIR: 00800-7250-8000 E-MAIL: [info@dlink.de](mailto:info@dlink.de)

**India D-Link India**

Plot No.5, Bandra-Kurla Complex Rd., Off Cst Rd.,  
Santacruz (East), Mumbai, 400 098 India  
TEL: 91-022-652-6696/6578/6623  
FAX: 91-022-652-8914/8476  
URL: [www.dlink-india.com](http://www.dlink-india.com) & [www.dlink.co.in](http://www.dlink.co.in)  
E-MAIL: [service@dlink.india.com](mailto:service@dlink.india.com) & [tushars@dlink-india.com](mailto:tushars@dlink-india.com)

**Italy D-Link Mediterraneo Srl/D-Link Italia**

Via Nino Bonnet n. 6/B, 20154, Milano, Italy  
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723  
URL: [www.dlink.it](http://www.dlink.it) E-MAIL: [info@dlink.it](mailto:info@dlink.it)

**Japan D-Link Japan**

10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan  
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868  
URL: [www.d-link.co.jp](http://www.d-link.co.jp) E-MAIL: [kida@d-link.co.jp](mailto:kida@d-link.co.jp)

**Netherlands D-Link Benelux**

Fellenoord 130 5611 ZB, Eindhoven, The Netherlands  
TEL: 31-40-2668713 FAX: 31-40-2668666  
URL: [www.d-link-benelux.nl](http://www.d-link-benelux.nl) & [www.dlink-benelux.be](http://www.dlink-benelux.be)  
E-MAIL: [info@dlink-benelux.nl](mailto:info@dlink-benelux.nl) & [info@dlink-benelux.be](mailto:info@dlink-benelux.be)

**Norway D-Link Norway**

Waldemar Thranesgate 77, 0175 Oslo, Norway  
TEL: 47-22-99-18-90 FAX: 47-22-20-70-39 SUPPORT: 800-10-610  
URL: [www.dlink.no](http://www.dlink.no)

**Russia D-Link Russia**

Michurinski Prospekt 49, 117607 Moscow, Russia  
TEL: 7-095-737-3389 & 7-095-737-3492  
FAX: 7-095-737-3390 URL: [www.dlink.ru](http://www.dlink.ru)  
E-MAIL: [vl@dlink.ru](mailto:vl@dlink.ru)

**Singapore D-Link International**

1 International Business Park, #03-12 The Synergy,  
Singapore 609917  
TEL: 6-6774-6233 FAX: 6-6774-6322  
E-MAIL: [info@dlink.com.sg](mailto:info@dlink.com.sg) URL: [www.dlink-intl.com](http://www.dlink-intl.com)

**South Africa D-Link South Africa**

Unit 2, Parkside, 86 Oak Avenue, Highveld Technopark,  
Centurion, Gauteng, South Africa  
TEL: 27-12-665-2165 FAX: 27-12-665-2186  
URL: [www.d-link.co.za](http://www.d-link.co.za) E-MAIL: [attie@d-link.co.za](mailto:attie@d-link.co.za)

**Spain D-Link Iberia (Spain and Portugal)**

Sabino de Arana, 56 bajos, 08028 Barcelona, Spain  
TEL: 34 93 409 0770 FAX: 34 93 491 0795  
URL: [www.dlink.es](http://www.dlink.es) E-MAIL: [info@dlink.es](mailto:info@dlink.es)

**Sweden D-Link Sweden**

P. O. Box 15036, S-167 15 Bromma, Sweden  
TEL: 46-8-564-61900 FAX: 46-8-564-61901  
URL: [www.dlink.se](http://www.dlink.se) E-MAIL: [info@dlink.se](mailto:info@dlink.se)

- Taiwan**      **D-Link Taiwan**  
2F, No. 119 Pao-chung Road, Hsin-tien, Taipei, Taiwan  
TEL: 886-2-2910-2626    FAX: 886-2-2910-1515  
URL: www.dlinktw.com.tw    E-MAIL: dssqa@tsc.dlinktw.com.tw
- Turkey**      **D-Link Middle East**  
Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5  
Mecidiyekoy, Istanbul, Turkey  
TEL: 90-212-213-3400    FAX: 90-212-213-3420  
E-MAIL: smorovati@dlink-me.com
- U.A.E.**      **D-Link Middle East**  
CHS Aptec (Dubai), P.O. Box 33550 Dubai, United Arab Emirates  
TEL: 971-4-366-885    FAX: 971-4-355-941  
E-MAIL: Wxavier@dlink-me.com
- U.K.**      **D-Link Europe (United Kingdom) Ltd**  
4<sup>th</sup> Floor, Merit House, Edgware Road, Colindale, London  
NW9 5AB United Kingdom  
TEL: 44-020-8731-5555    SALES: 44-020-8731-5550  
FAX: 44-020-8731-5511    SALES: 44-020-8731-5551  
BBS: 44 (0) 181-235-5511  
URL: www.dlink.co.uk    E-MAIL: info@dlink.co.uk
- U.S.A.**      **D-Link U.S.A.**  
17595 Mt. Herrmann Street, Fountain Valley, CA 92708, USA  
TEL: 1-714-885-6000    FAX: 1-866-743-4905  
INFO: 1-877-453-5465    URL: www.dlink.com  
E-MAIL: tech@dlink.com & support@dlink.com