

D-Link DFL-900

Firewall/VPN 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-900 User Manual

Version 0.4

November 5, 2003

Trademarks

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

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

Version 11/4/2003 6:28 PM

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	Device default value.....	3
1.4	Wiring the DFL-900.....	4
1.5	Default Architecture of DFL-900.....	5
1.6	Using the Setup Wizard.....	6
1.7	Internet Connectivity.....	8
1.7.1	LAN1-to-WAN1 Connectivity	8
1.7.2	WAN1-to-DMZ1 Connectivity.....	9
Chapter 2	System Overview	13
2.1	Topology	13
2.2	Changing the LAN1 IP Address.....	13
2.2.1	From DMZ1 to configure DFL-900 LAN1 network settings.....	14
2.2.2	From CLI (command line interface) to configure DFL-900 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.....	18
Chapter 4	System Tools.....	21
4.1	Demand	21
4.2	Objectives.....	21
4.3	Methods.....	21
4.4	Steps	23
Chapter 5	Remote Management	27
5.1	Demands.....	27
5.2	Methods.....	27
5.3	Steps	28
Part II	NAT & Firewall.....	30
Chapter 6	NAT.....	31
6.1	Demands.....	31
6.2	Objectives.....	31
6.3	Methods.....	32
6.4	Steps	32
6.4.1	Setup Many-to-one NAT rules.....	32
6.4.2	Setup Virtual Server for the FtpServer1	35
Chapter 7	Firewall.....	39

7.1	Demands	39
7.2	Objectives	39
7.3	Methods.....	39
7.4	Steps.....	40
7.4.1	Block internal PC session (LAN → WAN).....	40
7.4.2	Setup Alert detected attack	41
Part III Virtual Private Network		44
Chapter 8 VPN Technical Introduction		45
8.1	Terminology Explanation.....	45
8.1.1	VPN.....	45
8.1.2	IPSec.....	45
8.1.3	Security Association	45
8.1.4	IPSec Algorithms.....	45
8.1.5	Key Management.....	45
8.1.6	Encapsulation	46
8.1.7	IPSec Protocols.....	47
8.2	Make VPN packets pass through DFL-900.....	47
Chapter 9 Virtual Private Network – IPSec.....		49
9.1	Demands	49
9.2	Objectives	49
9.3	Methods.....	49
9.4	Steps.....	50
9.4.1	DES/MD5 IPSec tunnel: the IKE way.....	50
9.4.2	DES/MD5 IPSec tunnel: the Manual-Key way	56
Chapter 10 Virtual Private Network – PPTP.....		61
10.1	Demands	61
10.2	Objectives	61
10.3	Methods.....	61
10.4	Steps.....	62
Chapter 11 Virtual Private Network – L2TP.....		65
11.1	Demands	65
11.2	Objectives	65
11.3	Methods.....	65
11.4	Steps.....	66
11.4.1	Setup L2TP Network Server.....	66
11.4.2	Setup L2TP Network Client	68
Part IV Content Filters		70
Chapter 12 Content Filtering – Web Filters		71
12.1	Demands	71
12.2	Objectives	71
12.3	Methods.....	71
12.4	Steps.....	72
Chapter 13 Content Filtering – Mail Filters		77
13.1	Demands	77
13.2	Objectives	77

13.3	Methods.....	77
13.4	Steps for SMTP Filters.....	78
13.5	Steps for POP3 Filters.....	79
Chapter 14 Content Filtering – FTP Filtering		81
14.1	Demands.....	81
14.2	Objectives.....	81
14.3	Methods.....	81
14.4	Steps.....	82
Part V Intrusion Detection System		84
Chapter 15 Intrusion Detection Systems		85
15.1	Demands.....	85
15.2	Objectives.....	85
15.3	Methods.....	85
15.4	Steps.....	86
Part VI Bandwidth Management.....		88
Chapter 16 Bandwidth Management.....		89
16.1	Demands.....	89
16.2	Objectives.....	89
16.3	Methods.....	89
16.4	Steps.....	90
16.4.1	Inbound Traffic Management.....	90
16.4.2	Outbound Traffic Management.....	93
Part VII System Maintenance.....		96
Chapter 17 Log System.....		97
17.1	Demands.....	97
17.2	Objectives.....	97
17.3	Methods.....	97
17.4	Steps.....	97
Chapter 18 System Maintenance.....		99
18.1	Demands.....	99
18.2	Steps for TFTP Upgrade.....	99
18.3	Steps for Firmware upgrade from Web GUI.....	100
18.4	Steps for Factory Reset.....	101
18.4.1	Steps for NORMAL factory reset.....	101
18.4.2	Steps for EMERGENT factory reset.....	101
18.5	Steps for Backup / Restore Configurations.....	101
Appendix A Trouble Shooting		103
Appendix B Glossary of Terms.....		107

Part I

Basic Configuration

Chapter 1

Quick Start

This chapter introduces how to quick setup the DFL-900.

DFL-900 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** (400Mbps at 3000 rules), policy-based **NAT**, wire-speed **VPN** (simultaneous 2000 tunnels), 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-900. The default IP address for the DFL-900 is **192.168.1.254** (LAN1, Port 2) 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-900's IP address, say 192.168.1.2, to configure the DFL-900.

1.2 Check Your Package Contents

These are the items included with your DFL-900 purchase as Figure 1-1. They are the following items

1. DFL-900 Device * 1
2. Ethernet cable (RJ-45) * 1
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-900 package

1.3 Device default value

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-900.

Items	Default value	New value	
Password:	admin		
WAN1 (Port 1)	IP Address	Not initialized	____. ____ . ____ . ____
	Subnet Mask		____. ____ . ____ . ____
	Gateway IP		____. ____ . ____ . ____
	Primary DNS		____. ____ . ____ . ____
	Secondary DNS		____. ____ . ____ . ____
	PPPoE Username		
	PPPoE Password		
LAN1 (Port 2)	IP Address	192. 168. 1. 254	____. ____ . ____ . ____
	IP Subnet Mask	255. 255. 255. 0	____. ____ . ____ . ____
DMZ1 (Port 3)	IP Address	10. 1. 1. 254	____. ____ . ____ . ____
	IP Subnet Mask	255. 255. 255. 0	____. ____ . ____ . ____

Table 1-1 DFL-900 related network settings

1.4 Wiring the DFL-900

- A.** First, connect the power cord to the socket at the back panel of the DFL-900 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-900

- B.** Using an Ethernet cable, insert one end of the cable to the WAN port on the front panel of the DFL-900 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.

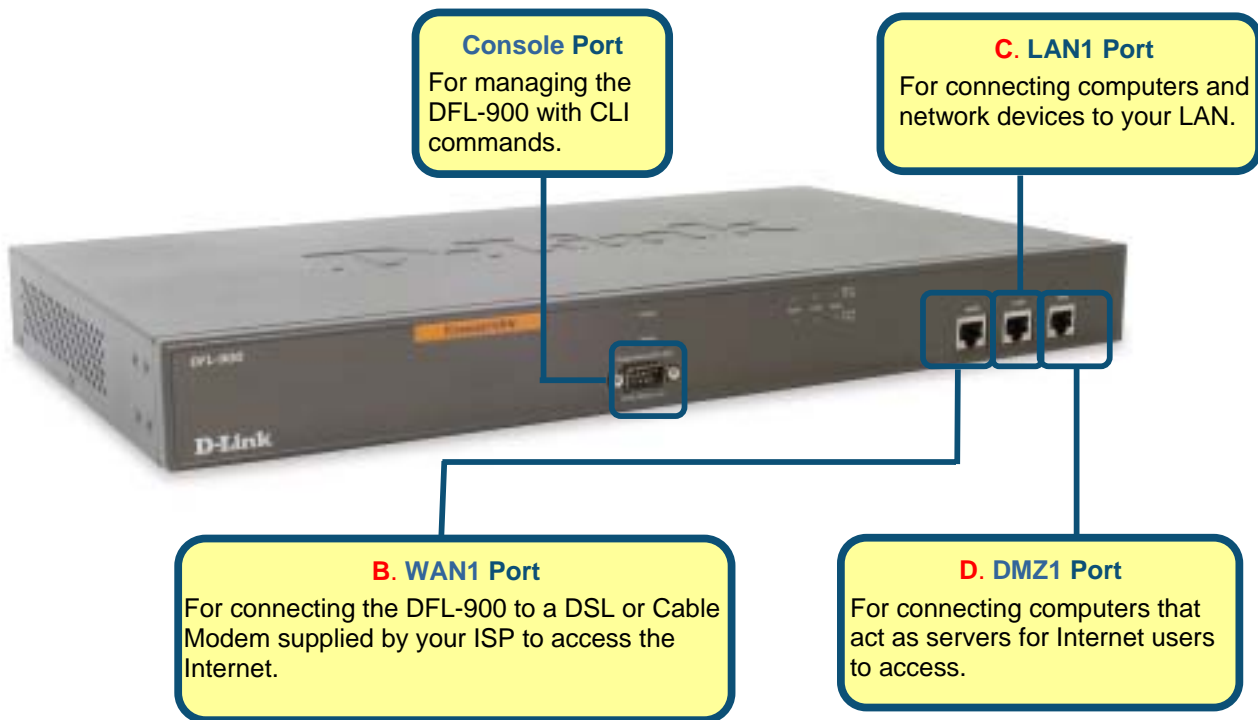


Figure 1-3 Front end of the DFL-900

1.5 Default Architecture of DFL-900

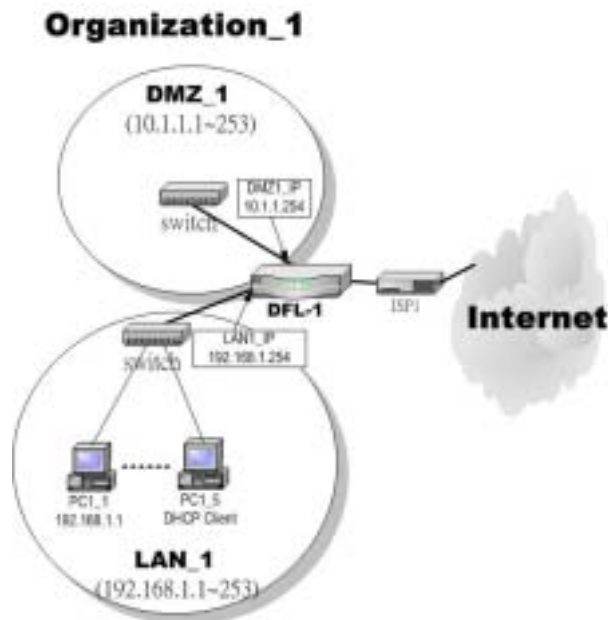

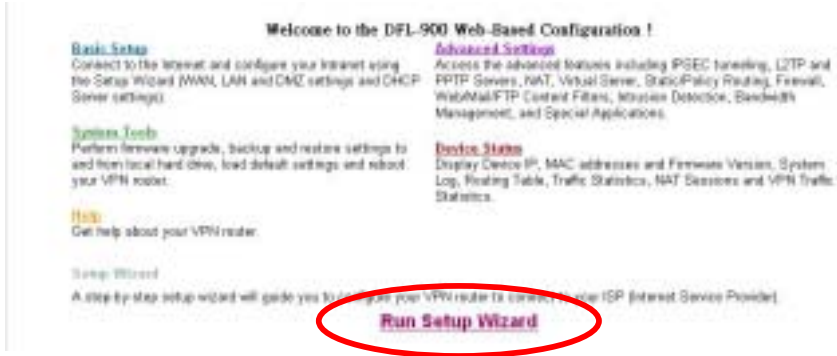



Figure 1-4 The default settings of DFL-900

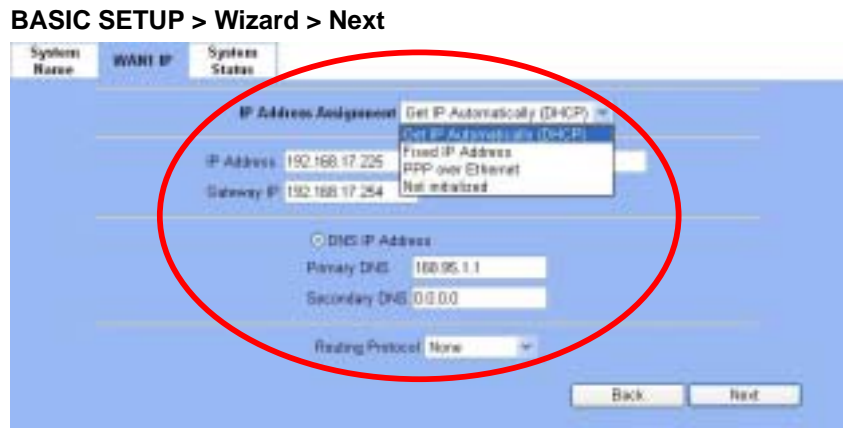
The factory default settings for the DFL-900 are in the Figure 1-4 and Table 1-1. You can configure the DFL-900 by connecting to the LAN1_IP (192.168.1.254) from the PC1_1 (192.168.1.1). The following section will teach you how to quickly setup the DFL-900 based on Figure 1-4.

1.6 Using the Setup Wizard

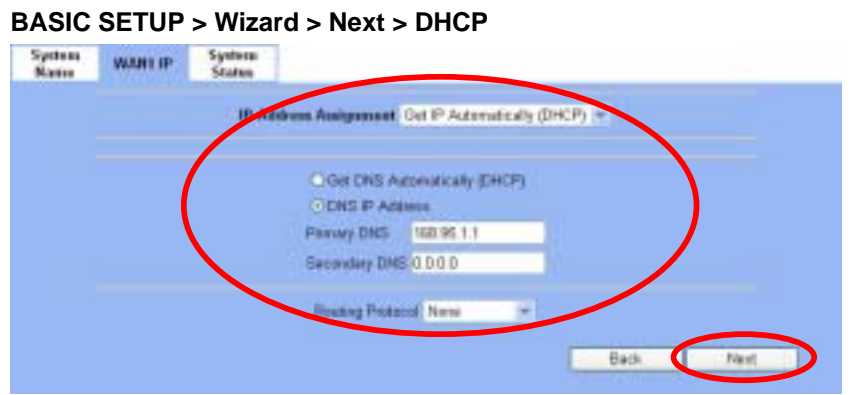
A computer on your LAN1 must be assigned an IP address and Subnet Mask from the same range as the IP address and Subnet Mask assigned to the DFL-900 in order to be able to make an HTTPS connection using a web browser. The DFL-900 is assigned an IP address of 192.168.1.254 with a Subnet Mask of 255.255.255.0 by default. The computer that will be used to configure the DFL-900 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-900. This address range can be changed later. There are instructions in the DFL-900 User's Guide, if you do not know how to set the IP address and Subnet Mask for your computer.

<p>Step 1 - Login</p> <p>Type "admin" in the account field, "admin" in the Password field and click Login.</p>	<p>Connect to https://192.168.1.254</p> 
<p>Step 2 - Run Setup Wizard</p> <p>Click the Run Setup Wizard.</p>	<p>After login to https://192.168.1.254</p> <p>BASIC SETUP > Wizard</p> 
<p>Step 3 - System Name</p> <p>Enter the Host Name and the Domain Name, followed by clicking the Next.</p>	<p>BASIC SETUP > Wizard</p> 

Step 4 - WAN Connectivity
 Choose the type of IP Address Assignment provided by your ISP to access the Internet. Here we have four types to select. This will determine how the IP address of WAN1 is obtained. Click Next to proceed.

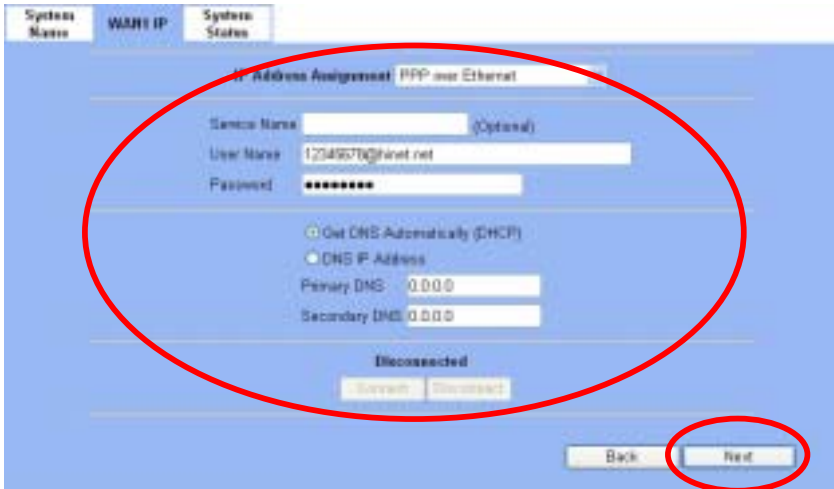



Step 4.a — DHCP client
 If Get IP Automatically (DHCP) is selected, DFL-900 will request for IP address, netmask, and DNS servers from your ISP. You can use your preferred DNS by clicking the DNS IP Address and then completing the Primary DNS and Secondary DNS server IP addresses. Click Next to proceed.



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.



<p>Step 4.c — PPPoE client</p> <p>If PPP over Ethernet is selected, enter the ISP-given User Name, Password and the optional Service Name. Click Next to proceed.</p>	<p>BASIC SETUP > Wizard > Next > PPPoE</p> 
<p>Step 5 - System Status</p> <p>Here we select PPPoE method in WAN1 port. Then the DFL-900 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.</p>	<p>BASIC SETUP > Wizard > Next > Next</p> 

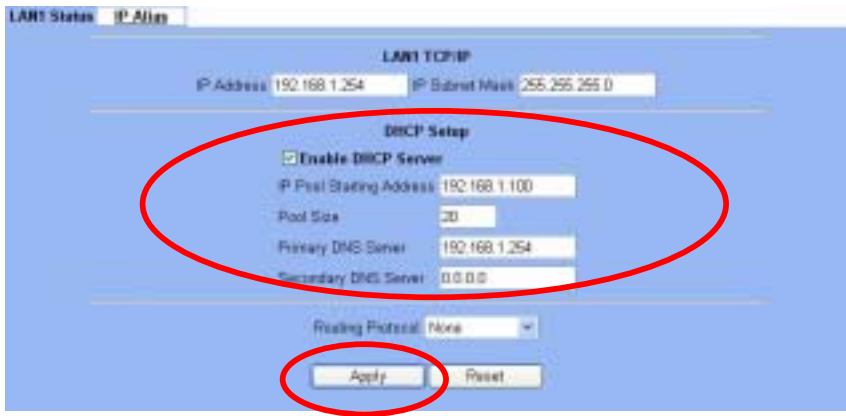
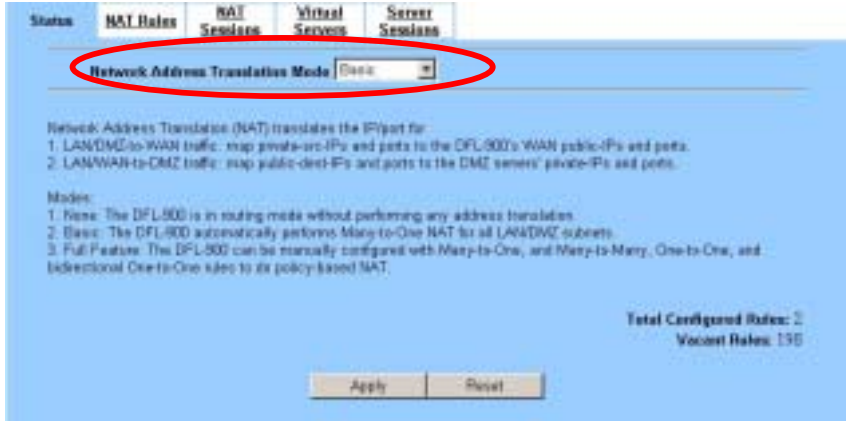

1.7 Internet Connectivity

After setting up DFL-900 with the wizard, DFL-900 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 through DFL-900. 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

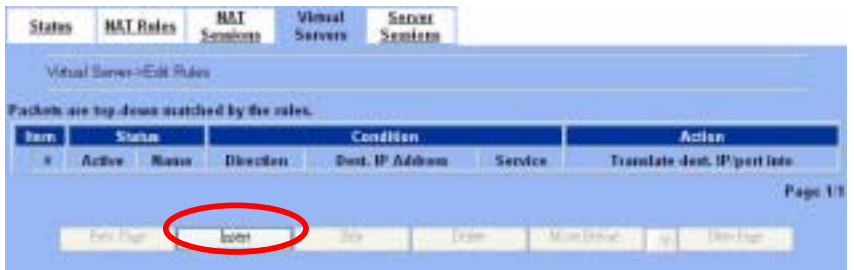
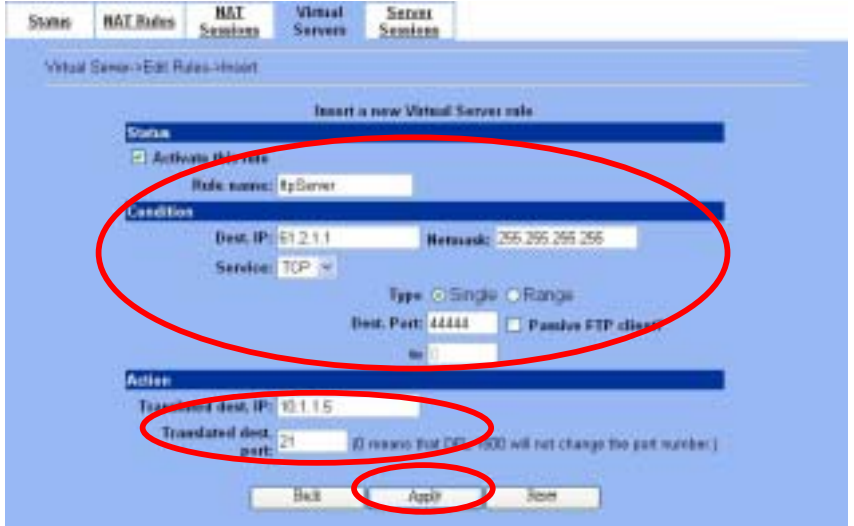

The LAN Settings page allows you to modify the IP address and Subnet Mask that will identify the DFL-900 on your LAN. This is the IP address you will enter in the URL field of your web browser to connect to the DFL-900. It is also the IP address that all of the computers and devices on your LAN will use as their Default Gateway.

<p>Step 1 - Device IP Address Setup the IP Address and IP Subnet Mask for the DFL-900.</p>	<p>BASIC SETUP > LAN Settings > LAN1 Status</p> 																					
<p>Step 2 - Client IP Range Enable the DHCP server if you want to use DFL-900 to assign IP addresses to the computers under LAN1. Specify the Pool Starting Address, Pool Size, Primary DNS, and Secondary DNS that will be assigned to them. Example: in the figure, the DFL-900 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>Note: The 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>Step 3 - Apply the Changes Click Apply to save. Now you can enable the DHCP clients on your LAN1 PCs to get an IP.</p>	<p>ADVANCED SETTINGS > NAT > Status</p>  <p>Network Address Translation (NAT) translates the IP/port for: 1. LAN/DMZ-to-WAN traffic: map private-IPs and ports to the DFL-900's WAN public-IPs and ports. 2. LAN/WAN-to-DMZ traffic: map public-dest-IPs and ports to the DMZ servers' private-IPs and ports.</p> <p>Modes: 1. None: The DFL-900 is in routing mode without performing any address translation. 2. Basic: The DFL-900 automatically performs Many-to-One NAT for all LAN/DMZ subnets. 3. Full Feature: The DFL-900 can be manually configured with Many-to-One, and Many-to-Many, One-to-One, and bidirectional One-to-One rules to its policy-based NAT.</p> <p>Total Configured Rules: 2 Vacant Rules: 158</p>																					
<p>Step 4 - Check NAT Status The default setting of NAT is in Basic Mode. After applying the Step 3, the NAT is automatically configured with two rules to let all private-IP LAN1/DMZ1-to-WAN1 requests to be translated with the public IP assigned by the ISP.</p>	<p>ADVANCED SETTINGS > NAT > NAT Rules</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-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-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-LAN1	LAN/DMZ to WAN	192.168.1.254/255.255.255.0	Auto (device WAN IP)	M:1																
<p>Step 5 - Check NAT Rules The DFL-900 has added two NAT rules. The rule Basic-LAN1 (number 2) 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>Step 1 - Device IP Address Setup the IP Address and IP Subnet Mask for the DFL-900 of the DMZ1 interface.</p>	<p>BASIC SETUP > DMZ Settings > DMZ1 Status</p> 																					
<p>Step 2 - Client IP Range Enable the DHCP server if you want to use DFL-900 to assign IP addresses to the computers under DMZ1. Here we do not want to make the DHCP feature enable.</p>																						
<p>Step 3 - Apply the Changes Click Apply to save your settings.</p>																						
<p>Step 4 - Check NAT Status The default setting of NAT is in Basic Mode. After applying the Step 3, the NAT is automatically configured with two rules to let all private-IP LAN1/DMZ1-to-WAN1 requests to be translated with the public IP assigned by the ISP.</p>	<p>ADVANCED SETTINGS > NAT > Status</p> 																					
<p>Step 5 - Check NAT Rules The DFL-900 has added two 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>ADVANCED SETTINGS > NAT > NAT Rules</p>  <table border="1" data-bbox="619 1337 1458 1449"> <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>Source IP Address: 10.1.1.254/255.255.255.0</td> <td>Translate Src IP into</td> <td>M:1</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Basic-LAN1</td> <td>LAN/DMZ to WAN</td> <td>10.1.1.1,254/255.255.255.0</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	Source IP Address: 10.1.1.254/255.255.255.0	Translate Src IP into	M:1	2	Y	Basic-LAN1	LAN/DMZ to WAN	10.1.1.1,254/255.255.255.0	Auto (Device WAN IP)	M:1
Item	Status	Name	Direction	Condition	Action	Type																
1	Y	Basic-DMZ1	LAN/DMZ to WAN	Source IP Address: 10.1.1.254/255.255.255.0	Translate Src IP into	M:1																
2	Y	Basic-LAN1	LAN/DMZ to WAN	10.1.1.1,254/255.255.255.0	Auto (Device WAN IP)	M:1																
<p>Step 6 - Setup IP for the FTP Server Assign an IP of 10.1.1.5/255.255.255.0 to the FTP server under DMZ1. Assume the FTP Server is at 10.1.1.5. And it is listening on the well-known port (21).</p>																						

<p>Step 7 - Setup Server Rules</p> <p>Insert a virtual server rule by clicking the Insert button.</p>	<p>ADVANCED SETTINGS > NAT > Virtual Servers</p>  <p>Virtual Servers -> 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>1</td> <td>Active</td> <td>ftpServer</td> <td>LAN/WAN to DMZ</td> <td>61.2.1.1</td> <td>TCP-4444</td> <td>Translate dest. IP/port into 10.1.1.5:21</td> </tr> </tbody> </table> <p>Page 1/1</p>	Item	Status	Name	Direction	Dest. IP Address	Service	Action	1	Active	ftpServer	LAN/WAN to DMZ	61.2.1.1	TCP-4444	Translate dest. IP/port into 10.1.1.5:21
Item	Status	Name	Direction	Dest. IP Address	Service	Action									
1	Active	ftpServer	LAN/WAN to DMZ	61.2.1.1	TCP-4444	Translate dest. IP/port into 10.1.1.5:21									
<p>Step 8 - Customize the Rule</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-900 to translate the packet's destination IP/port into 10.1.1.5/21. Check the Passive FTP at this port 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-900 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 > NAT > Virtual Servers > Insert</p>  <p>Virtual Servers -> Edit Rules -> Insert</p> <p>Insert a new 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 type="checkbox"/> Passive FTP client</p> <p>Action</p> <p>Translate dest. IP: 10.1.1.5</p> <p>Translated dest. port: 21 (0 means that DFL-900 will not change the port number.)</p> <p>Buttons: Back, Apply, Done</p>														
<p>Step 9 - View the Result</p> <p>Now any request towards the DFL-900'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.</p>	<p>ADVANCED SETTINGS > NAT > Virtual Servers</p>  <p>Virtual Servers -> 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>1</td> <td>Active</td> <td>ftpServer</td> <td>LAN/WAN to DMZ</td> <td>61.2.1.1/255.255.255.0</td> <td>TCP-4444</td> <td>Translate dest. IP/port into 10.1.1.5:21</td> </tr> </tbody> </table> <p>Page 1/1</p>	Item	Status	Name	Direction	Dest. IP Address	Service	Action	1	Active	ftpServer	LAN/WAN to DMZ	61.2.1.1/255.255.255.0	TCP-4444	Translate dest. IP/port into 10.1.1.5:21
Item	Status	Name	Direction	Dest. IP Address	Service	Action									
1	Active	ftpServer	LAN/WAN to DMZ	61.2.1.1/255.255.255.0	TCP-4444	Translate dest. IP/port into 10.1.1.5:21									

Chapter 2

System Overview

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

2.1 Topology

In this chapter, we introduce a typical network topology for the DFL-900. In Figure 2-1, the left half side is a DFL-900 with one LAN, one DMZ, and one WAN links. Notice there are three ports in DFL-900. In this topology, we only use one LAN.

The right half side contains a DFL-900 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-900 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 content filters and bandwidth management.

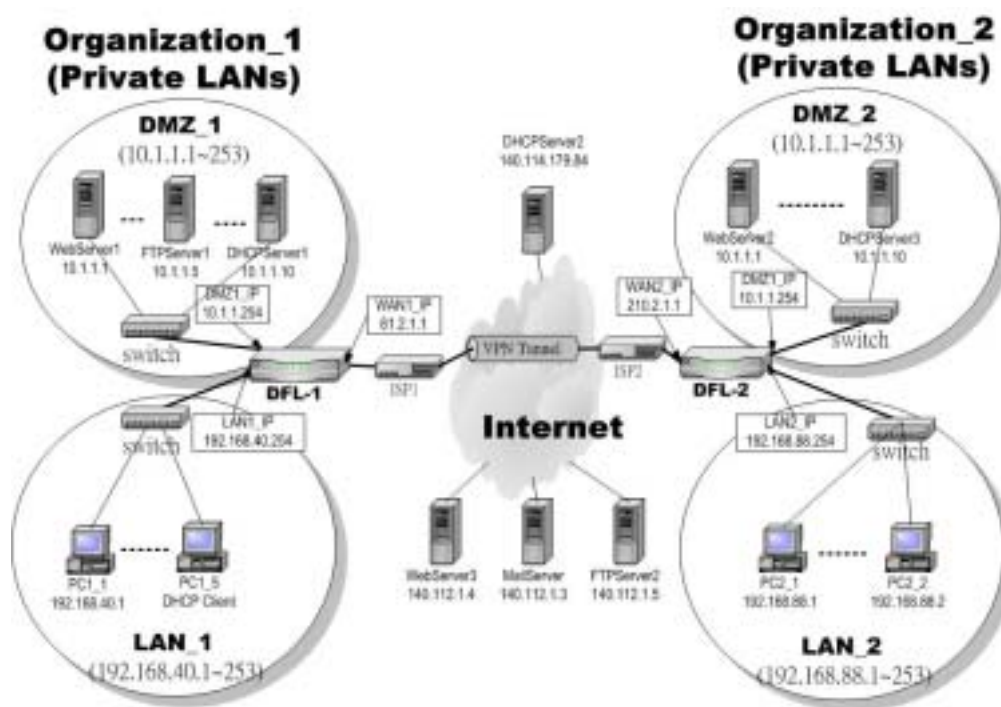


Figure 2-1 Overview of the system architecture for DFL-900


2.2 Changing the LAN1 IP Address

The default settings of DFL-900 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-900 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-900 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. 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-900 LAN1 network settings

<p>Step 1 - Check NAT Status</p> <p>In the DMZ_1 region, use a PC located 10.1.1.X to connect DFL-900 DMZ1 port (10.1.1.254). Type https://10.1.1.254 to configure the DFL-900 in the web browser.</p>	<p>Use an IE 6.0 at 10.1.1.1 to connect to https://10.1.1.254</p>
<p>Step 2 - Setup LAN1 IP information</p> <p>Enter the IP Address and IP Subnet Mask with 192.168.40.254 / 255.255.255.0 and click Apply.</p>	<p>BASIC SETUP > LAN Settings > LAN1 Status</p> 

2.2.2 From CLI (command line interface) to configure DFL-900 LAN1 network settings

<p>Step 1 - Use Console port to configure DFL-900</p> <p>Use the supplied console line to connect the PC to the Diagnostic RS-232 socket of the DFL-900. 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-900, enter the commands "en" to enter the privileged mode. Enter the command "IP ifconfig INTF1 192.168.40.254" to change the IP of the LAN1 interface.</p>	<pre>DFL-900> en DFL-900# IP ifconfig INTF1 192.168.40.254 255.255.255.0 DFL-900# IP ifconfig INTF1 LAN1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500 address: 00:50:fc:ba:db:fe media: Ethernet autoselect (100baseTX full-duplex) status: active inet 192.168.40.254 Netmask 0xfffff00 broadcast 192.168.40.255</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-900 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-900 WAN1 port.
2. Configure the network settings of the DFL-900 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-900.


3.3 Methods

1. Select the PPPoE method in the DFL-900 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-900 Basic Setup / DMZ settings / DMZ1 Status and 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>Step 1 - Setup WAN1 port</p> <p>Here we select PPP over Ethernet method in WAN1 port. Fill in the ISP-given User Name and Password and the optional Service Name. And then check the needed field. Click Apply to finish this setting.</p>	<p>BASIC SETUP > WAN Settings > WAN1 IP > PPPoE</p> 
--	--

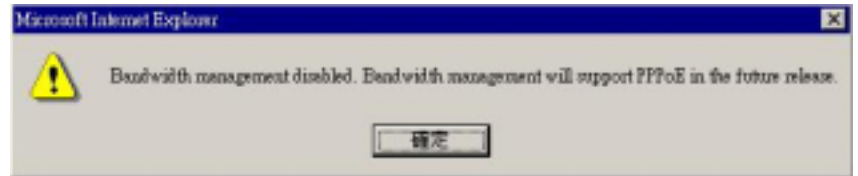
IP Address Assignment	FIELD	DESCRIPTION	EXAMPLE
PPP over Ethernet	Service Name	ISP vendor (Optional)	
	User Name	The user name of PPPoE account	12345678@hinet.net
	Password	The password of PPPoE account	G5468889
	Get DNS Automatically / DNS IP Address	Get DNS Automatically → Get DNS related information 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
Fixed IP Address	IP Address / Subnet Mask	Specified IP address and subnet mask	211.43.123.7 255.255.255.0
	Gateway IP	Default gateway IP address	211.43.123.254
	DNS IP Address	Specified Primary and Secondary DNS Server address	
	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
Get IP Automatically (DHCP)	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

Table 3-1 Detailed information of setup WAN port configuration

Step 2 - Show the Warning message

Note that if you have already enabled bandwidth management (ADVANCED SETTINGS>Bandwidth Mgt>Enable Bandwidth Management) and then select PPPoE in BASIC SETUP>WAN Settings>WAN1 IP>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.

BASIC SETUP > WAN Settings > WAN1 IP > PPPoE



3.4.2 Setup DMZ1, LAN1 Status

Step 1 - Setup DMZ port


Here we are going to configure the DMZ1 settings. Setup IP Address and IP Subnet Mask, and determine if you would like to enable the DHCP Server. If yes, please check Enable DHCP Server. And then select None for Routing Protocol. Click Apply to finish this setting.

BASIC SETUP > DMZ Settings > DMZ1 Status



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	
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.	10.1.1.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP.	
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


Table 3-2 Configure DMZ network settings

<p>Step 2 - Setup LAN port</p> <p>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.</p>	<p>BASIC SETUP > LAN Settings > LAN1 Status</p> 
--	---

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 Server 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.	192.168.40.254
Secondary DNS Server	Specify the Secondary DNS Server IP address of the DHCP.	
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

Table 3-3 Configure LAN network settings

3.4.3 Setup WAN1 IP alias

<p>Step 1 - Add WAN1 IP alias</p> <p>Suppose you apply 8 IP addresses from ISP. The range of the ISP-given IP addresses 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.</p> <p>Notice : It's the same way to set IP alias in DMZ or LAN.</p>	<p>BASIC SETUP > WAN Settings > IP Alias > Add</p> 
--	---

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	Alias	Netmask
1	WAN1	211.17.25.62	255.255.255.248
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--
9	--	--	--
10	--	--	--

First Page
Add
Edit
Delete
Last Page

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, and management timeout.
2. DDNS: Suppose the DFL-900'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.

4.2 Objectives

1. Configure the domain name, password, system time, and connection timeout.
2. DDNS: By using the DDNS (Dynamic DNS), the DFL-900 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.

4.3 Methods

1. Configure the domain name, password, system time, and connection timeout.
2. DDNS: Configure the DFL-900 so that whenever the IP of the DFL-900 is changed, it will send requests to the DDNS server to refresh the DNS record.

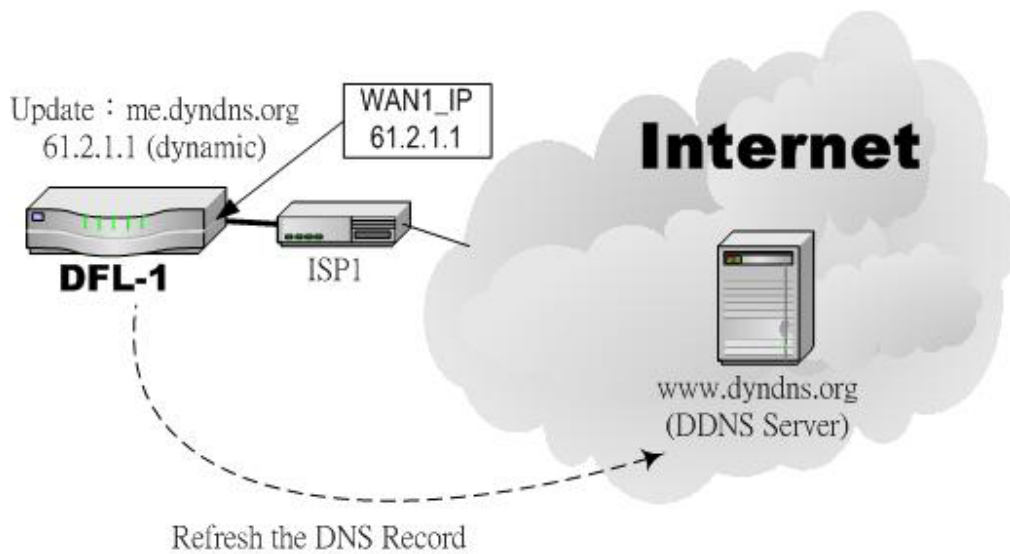


Figure 4-1 DDNS mechanism chart

3. DNS Proxy: After activating the DNS proxy mode, the client can set its DNS server to the DFL-900 (that is, send the DNS requests to the DFL-900). The DFL-900 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.

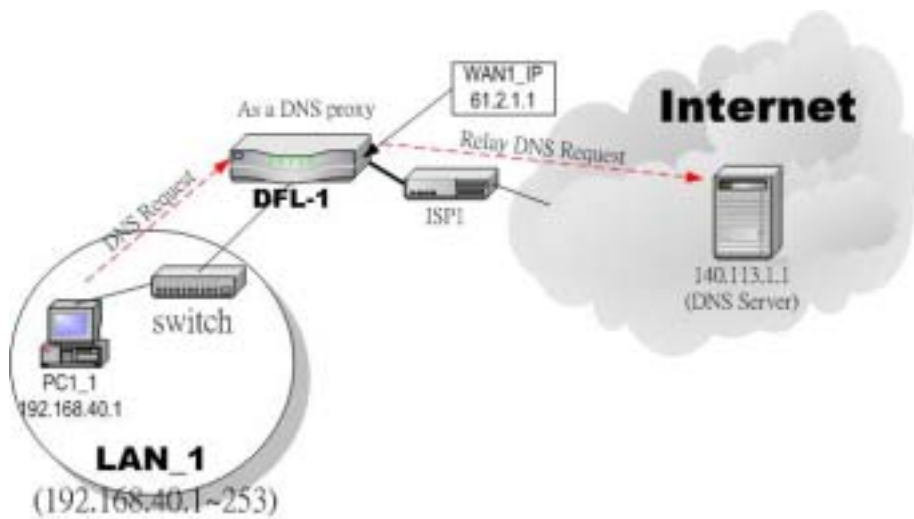


Figure 4-2 DNS Proxy mechanism chart

4. DHCP Relay: Activate the DHCP relay mode of DFL-900 so that the DFL-900 will become the relay agent and relay the DHCP broadcast to the configured DHCP server.

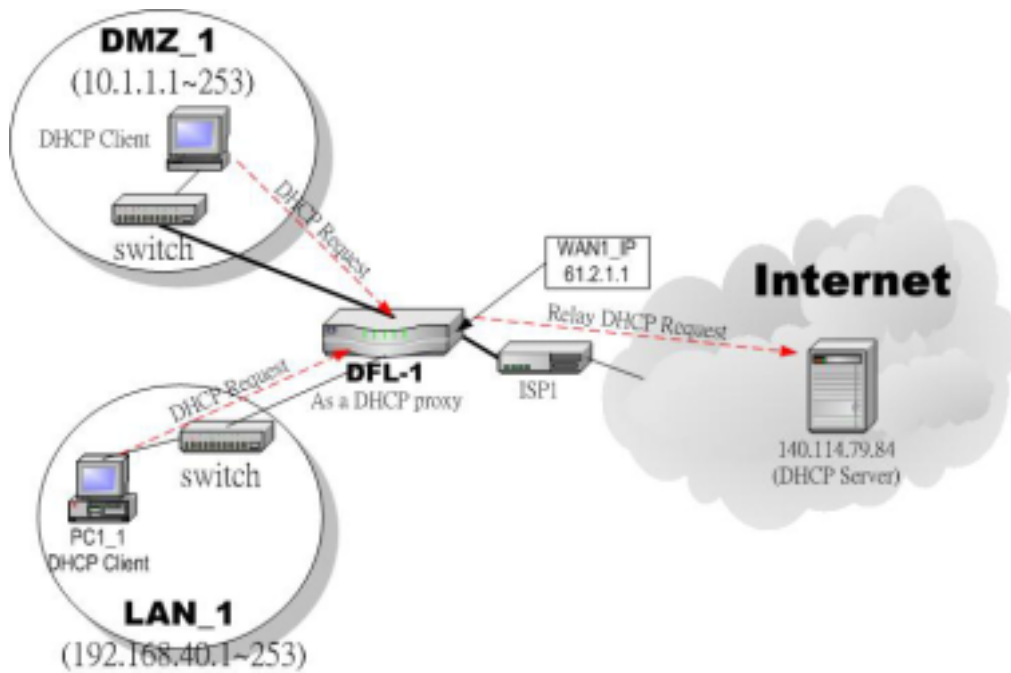


Figure 4-3 DHCP Relay mechanism chart


4.4 Steps

<p>Step 1 - General Setup</p> <p>Enter the Host Name as DFL-1, Domain Name as the domain name of your company Click Apply.</p>	<p>SYSTEM TOOLS > Admin Settings > General</p>
---	---

FIELD	DESCRIPTION	EXAMPLE
Host Name	the host name of the DFL-900 device	DFL-1
Domain Name	Fill in the domain name of company	dlink.com

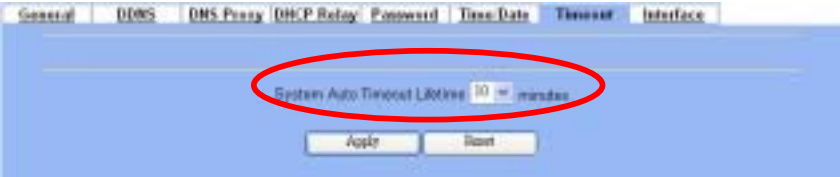
Table 4-1 System Tools - General Setup menu

<p>Step 2 - Change Password</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>SYSTEM TOOLS > Admin Settings > Password</p>
---	--

<p>Step 3 - Setup Time/Date</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-900 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>SYSTEM TOOLS > Admin Settings > Time/Date</p> 
--	--


FIELD	DESCRIPTION	EXAMPLE
Time zone	the time zone of your area	
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.	
Manual Time Setup	Manual setting Time & Date value.	

Table 4-2 System Tools – Time Data menu

<p>Step 4 - Setup Timeout</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>SYSTEM TOOLS > Admin Settings > Timeout</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 4-3 System Tools – Timeout menu

<p>Step 5 - Setup DDNS</p> <p>If the IP address of DFL-900 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.</p>	<p>SYSTEM TOOLS > Admin Settings > DDNS</p> 
--	---


FIELD	DESCRIPTION	EXAMPLE
Enable DDNS for WAN1	Enable DDNS feature of DFL-900	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-900, we provide www.DYNDNS.org and www.DHS.org two websites for choice.	WWW.DYNDNS.ORG
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 4-4 System Tools – DDNS setting page

<p>Step 6 - Setup DNS Proxy</p> <p>Check the Enable DNS Proxy and click the Apply to store the settings. From now on, your LAN/DMZ PCs can use DFL-900 as their DNS server, as long as the DNS server for DFL-900 has been set in its WAN settings.</p>	<p>SYSTEM TOOLS > Admin Settings > DNS Proxy</p> 
--	--

FIELD	DESCRIPTION	EXAMPLE
Enable DNS Proxy	When the host of the LAN/DMZ sends a DNS Request, DFL-900 will request for forwarding it to the DNS server of the WAN link. When there is a response from DNS, DFL-900 will forward it back to the host of the LAN/DMZ.	Enabled

Table 4-5 System Tools – DNS Proxy menu

<p>Step 7 - Setup DHCP Relay</p> <p>Check the Enable DHCP Relay. Enter the IP address of your DHCP server. Check the relay domain of DFL-900 that needs to be relayed. Namely, check the one where the DHCP server resides and the one where DHCP clients are located. Click the Apply button.</p>	<p>SYSTEM TOOLS > Admin Settings > DHCP Relay</p> 
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable DHCP Relay	When the host of the LAN/DMZ in the DFL-900 internal network sends a DHCP request, DFL-900 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 4-6 System Tools – DHCP Relay menu

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-900 remotely from any PC in LAN1 with HTTP at port 8080, and from WAN_PC with TELNET. In addition, the DFL-900 may be more secure if monitored by a trusted host (PC1_1). What is more, the DFL-900 should not respond to ping to hide itself. The remote management function in DFL-900 devices is implemented by hidden Firewall rules.

5.2 Methods

1. Only allow management by WAN_PC (141.2.5.1) at the WAN1 side.
2. Administrators can use browsers to connect to <http://192.168.40.254:8080> for management.
3. Allow SNMP monitoring by PC1_1 (192.168.40.1) at the LAN1 side.
4. Do not respond to ICMP ECHO packets at the WAN1 side.

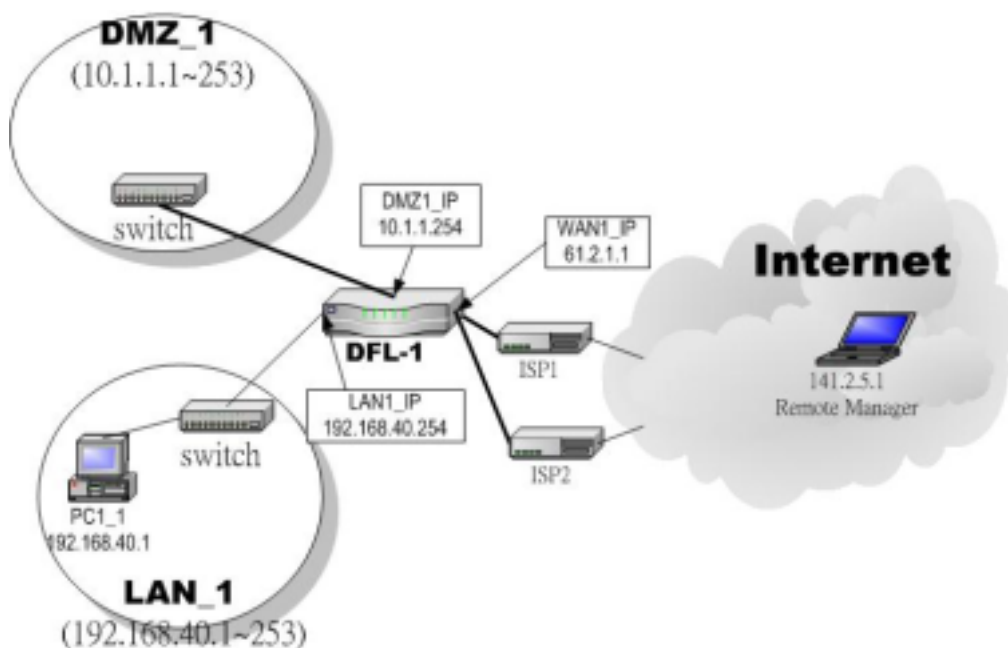
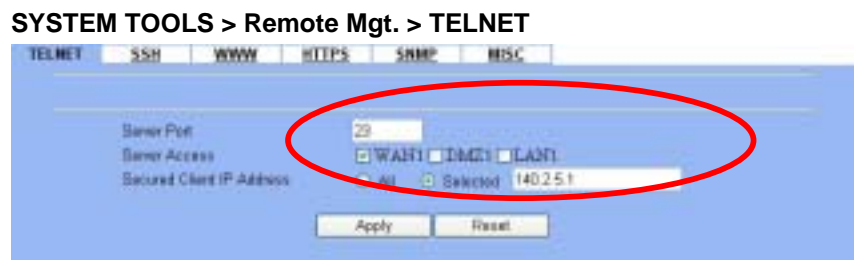
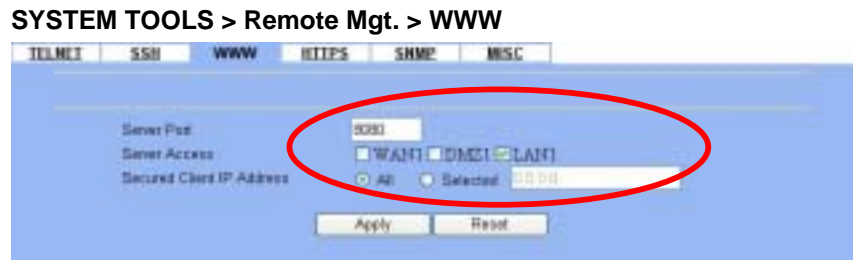
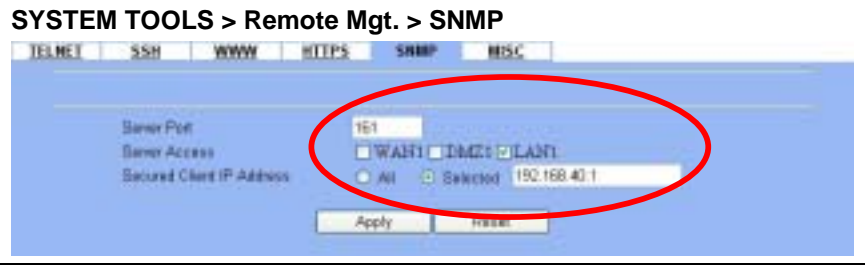
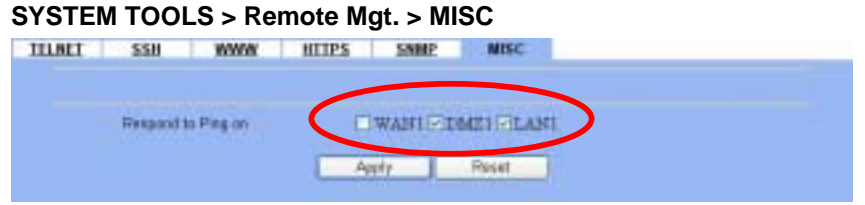


Figure 5-1 Some management method of DFL-900

5.3 Steps

<p>Setup Telnet</p> <p>Check the WAN1 checkbox, click the Selected, and enter the IP address (140.2.5.1) that will telnet to the DFL-900. And click the Apply.</p>	<p>SYSTEM TOOLS > Remote Mgt. > TELNET</p> 
<p>Setup WWW</p> <p>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-900 with HTTP, your browser will then automatically be directed to the new server port.</p>	<p>SYSTEM TOOLS > Remote Mgt. > WWW</p> 
<p>Setup SNMP</p> <p>Check the LAN1 checkbox, click the Selected, and enter the IP address (192.168.40.1) that will read the SNMP MIBs at the DFL-900. And click the Apply.</p>	<p>SYSTEM TOOLS > Remote Mgt. > SNMP</p> 
<p>Setup ICMP</p> <p>Uncheck the WAN1 checkbox and then click the Apply.</p>	<p>SYSTEM TOOLS > Remote Mgt. > MISC</p> 

Part II

NAT & Firewall

Chapter 6

NAT

This chapter introduces NAT and explains how to implement it in DFL-900.

To facilitate the explanation on how DFL-900 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.

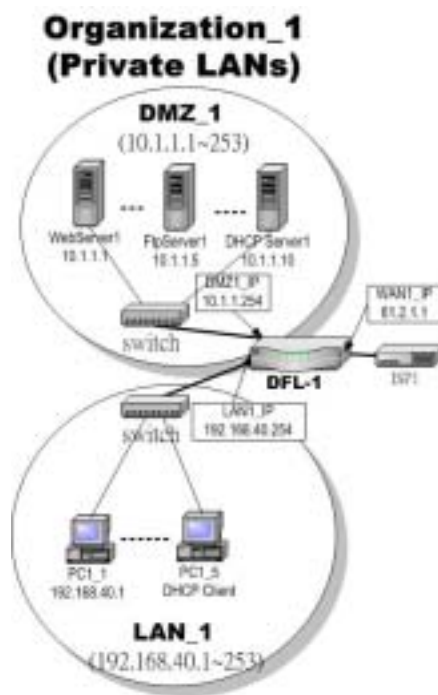


Figure 6-1 Topology for explanations of the NAT examples.

6.2 Objectives

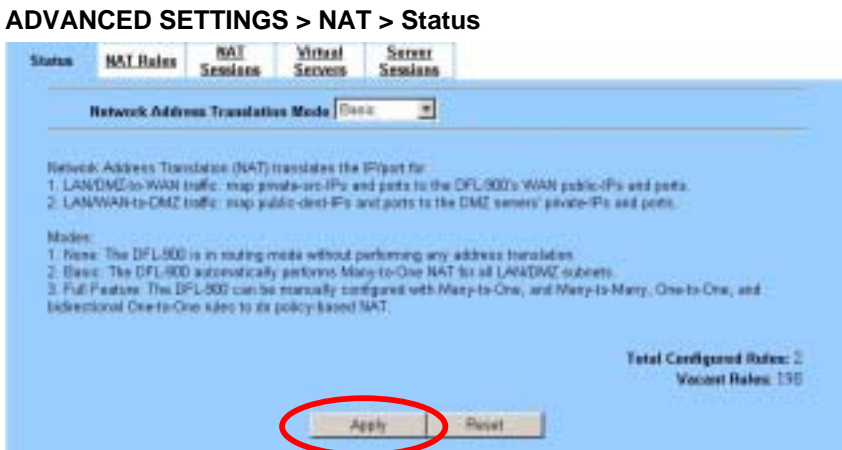
1. Let PC1_1~PC1_5 connect to the Internet.
2. Let FTPServer1 be accessed by other Internet users.

6.3 Methods

1. Assign private IP addresses to the PC1_1~PC1_5. Setup NAT at DFL-900 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-900 to redirect “any connections towards some port of WAN1” to the port 21 at the FTPServer1.


6.4 Steps


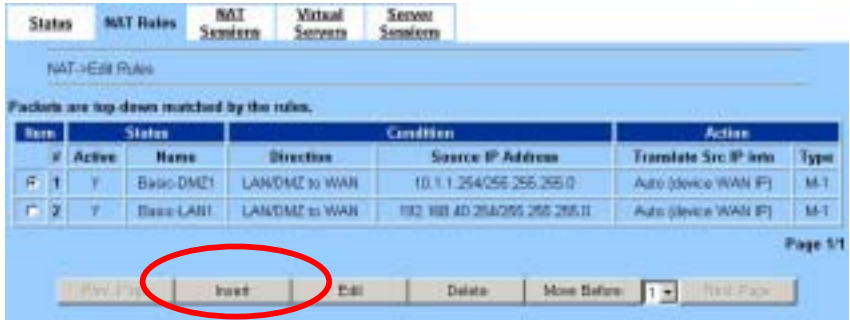

6.4.1 Setup Many-to-one NAT rules

<p>Step 1 - Enable NAT</p> <p>Select the Basic from the list of Network Address Translation Mode. Click Apply. Now the DFL-900 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.</p>	<p>ADVANCED SETTINGS > NAT > Status</p> 
---	--

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation Mode	<p>None : The DFL-900 is in routing mode without performing any address translation.</p> <p>Basic : The DFL-900 automatically performs Many-to-One NAT for all LAN/DMZ subnets.</p> <p>Full Feature : The DFL-900 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>Step 2 - Check NAT Rules</p> <p>As described in the above, the DFL-900 has set the two rules for the LAN1 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>ADVANCED SETTINGS > NAT > NAT Rules</p> 
--	--

<p>Step 3 - Switch the NAT Mode</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-900. 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>ADVANCED SETTINGS > NAT > Status</p> 
<p>Step 4 - Customize NAT Rules</p> <p>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.</p>	<p>ADVANCED SETTINGS > NAT > NAT Rules</p> 
<p>Step 5 - Insert NAT Rule</p>	
<p>Step 5.a — Insert an Many-to-One Rule</p> <p>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-900 will automatically determine which WAN IP is to be translated into.</p>	<p>ADVANCED SETTINGS > NAT > NAT Rules > Insert</p> 

	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	Type		Many-to-One
	Many-to-One	Map a pool of private IP addresses to a single public IP address chosen from the WAN ports.	
	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>Step 5.b — Insert an Many-to-Many Rule</p> <p>If your ISP has assigned a range of public IP to your company, you can tell DFL-900 to translate the private IPs into the pool of public IPs. The DFL-900 will use the first public IP until DFL-900 uses up all source ports for the public IP. DFL-900 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-900 will no longer choose the device IP for you. It will choose the IP from the address pool you have entered.</p>	<p>ADVANCED SETTINGS > NAT > NAT Rules > Insert</p>
<p>Step 5.c — Insert an One-to-One Rule</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>ADVANCED SETTINGS > NAT > NAT Rules > Insert</p>

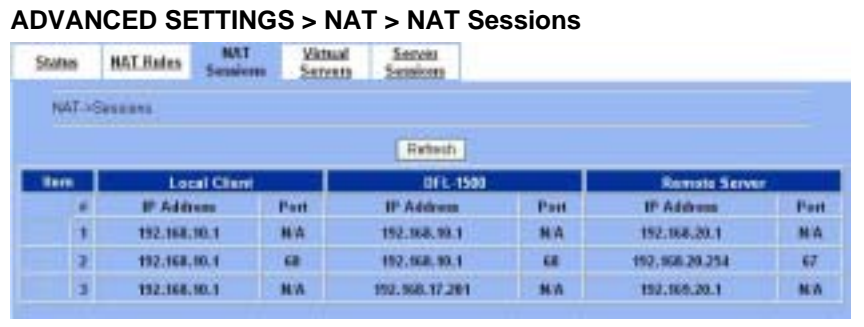
Step 5.d — Insert a One-to-One (Bidirectional) Rule

The above three modes allow LAN/DMZ-to-WAN sessions establishment but do not allow WAN-to-LAN/DMZ sessions. WAN-to-LAN/DMZ sessions are allowed by Virtual Server rules. You can make the One-to-One NAT in the above to incorporate the WAN-to-LAN/DMZ feature by selecting the One-to-One (Bidirectional) from the Type. Note that WAN-to-LAN 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 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.



Step 6 - View the LAN to WAN Sessions

Click the NAT Sessions to see the sessions between LAN to WAN.



6.4.2 Setup Virtual Server for the FtpServer1

Step 1 - Device IP Address

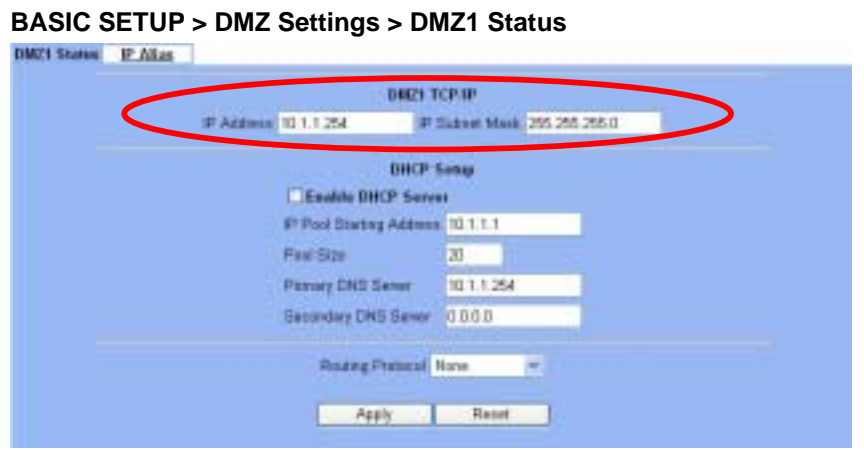
Setup the IP Address and IP Subnet Mask for the DFL-900 of the DMZ1 interface.



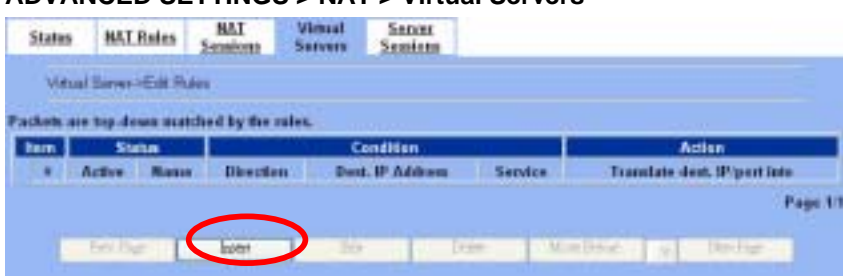
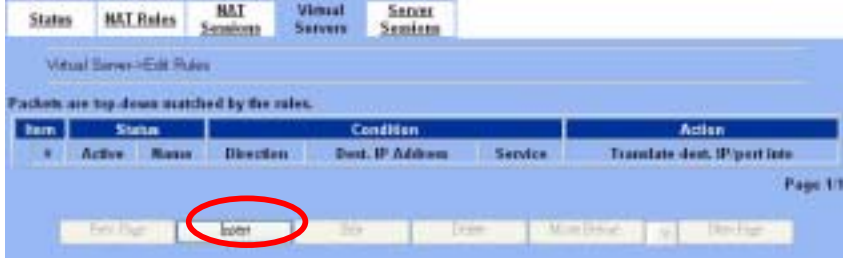
Step 2 - Client IP Range

Enable the DHCP server if you want to use DFL-900 to assign IP addresses to the computers under DMZ1. Here we do not want to make the DHCP feature enable.

Step 3 - Apply the Changes

Click **Apply** to save your settings.



<p>Step 4 - Check NAT Status</p> <p>The default setting of NAT is in Basic Mode. After applying the Step 3, the NAT is automatically configured with two rules to let all private-IP LAN1/DMZ1-to-WAN1 requests to be translated with the public IP assigned by the ISP.</p>	<p>ADVANCED SETTINGS > NAT > Status</p> 																					
<p>Step 5 - Check NAT Rules</p> <p>The DFL-900 has added two 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>ADVANCED SETTINGS > NAT > NAT Rules</p>  <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th>Name</th> <th>Direction</th> <th>Source IP Address</th> <th>Translate Src IP into</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>Basic-DMZ1</td> <td>LAN/DMZ1 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-LAN1</td> <td>LAN/DMZ1 to WAN</td> <td>192.168.0.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> </tbody> </table>	Item	Status	Name	Direction	Source IP Address	Translate Src IP into	Type	1	Y	Basic-DMZ1	LAN/DMZ1 to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1	2	Y	Basic-LAN1	LAN/DMZ1 to WAN	192.168.0.254/255.255.255.0	Auto (device WAN IP)	M-1
Item	Status	Name	Direction	Source IP Address	Translate Src IP into	Type																
1	Y	Basic-DMZ1	LAN/DMZ1 to WAN	10.1.1.254/255.255.255.0	Auto (device WAN IP)	M-1																
2	Y	Basic-LAN1	LAN/DMZ1 to WAN	192.168.0.254/255.255.255.0	Auto (device WAN IP)	M-1																
<p>Step 6 - Setup IP for the FTP Server</p> <p>Assign an IP of 10.1.1.1/255.255.255.0 to the FTP server under DMZ1. See Appendix for assistance. Assume the FTP Server is at 10.1.1.5. And it is listening on the well-known port (21).</p>																						
<p>Step 7 - Setup Server Rules</p> <p>Insert a virtual server rule by clicking the Insert button.</p>	<p>ADVANCED SETTINGS > NAT > Virtual Servers</p> 																					

<p>Step 8 - Customize the Rule</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-900 to translate the packet's destination IP/port into 10.1.1.5/21. Check the Passive FTP at this port 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-900 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 > NAT > Virtual Servers > Insert</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-900 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 6-3 Add a Virtual Server rule

Step 9 - View the Result
 Now any request towards the DFL-900'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

Virtual Server -> Edit Rules

Packets are top-down searched 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	TCP-44444	Translate dest. IP/port into 10.1.1.5:21

Page 1/1

Form: Top | Add | Edit | Delete | Move Down: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 | 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 | 192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 | 208 | 209 | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 | 224 | 225 | 226 | 227 | 228 | 229 | 230 | 231 | 232 | 233 | 234 | 235 | 236 | 237 | 238 | 239 | 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 254 | 255 | 256 | 257 | 258 | 259 | 260 | 261 | 262 | 263 | 264 | 265 | 266 | 267 | 268 | 269 | 270 | 271 | 272 | 273 | 274 | 275 | 276 | 277 | 278 | 279 | 280 | 281 | 282 | 283 | 284 | 285 | 286 | 287 | 288 | 289 | 290 | 291 | 292 | 293 | 294 | 295 | 296 | 297 | 298 | 299 | 300 | 301 | 302 | 303 | 304 | 305 | 306 | 307 | 308 | 309 | 310 | 311 | 312 | 313 | 314 | 315 | 316 | 317 | 318 | 319 | 320 | 321 | 322 | 323 | 324 | 325 | 326 | 327 | 328 | 329 | 330 | 331 | 332 | 333 | 334 | 335 | 336 | 337 | 338 | 339 | 340 | 341 | 342 | 343 | 344 | 345 | 346 | 347 | 348 | 349 | 350 | 351 | 352 | 353 | 354 | 355 | 356 | 357 | 358 | 359 | 360 | 361 | 362 | 363 | 364 | 365 | 366 | 367 | 368 | 369 | 370 | 371 | 372 | 373 | 374 | 375 | 376 | 377 | 378 | 379 | 380 | 381 | 382 | 383 | 384 | 385 | 386 | 387 | 388 | 389 | 390 | 391 | 392 | 393 | 394 | 395 | 396 | 397 | 398 | 399 | 400 | 401 | 402 | 403 | 404 | 405 | 406 | 407 | 408 | 409 | 410 | 411 | 412 | 413 | 414 | 415 | 416 | 417 | 418 | 419 | 420 | 421 | 422 | 423 | 424 | 425 | 426 | 427 | 428 | 429 | 430 | 431 | 432 | 433 | 434 | 435 | 436 | 437 | 438 | 439 | 440 | 441 | 442 | 443 | 444 | 445 | 446 | 447 | 448 | 449 | 450 | 451 | 452 | 453 | 454 | 455 | 456 | 457 | 458 | 459 | 460 | 461 | 462 | 463 | 464 | 465 | 466 | 467 | 468 | 469 | 470 | 471 | 472 | 473 | 474 | 475 | 476 | 477 | 478 | 479 | 480 | 481 | 482 | 483 | 484 | 485 | 486 | 487 | 488 | 489 | 490 | 491 | 492 | 493 | 494 | 495 | 496 | 497 | 498 | 499 | 500 | 501 | 502 | 503 | 504 | 505 | 506 | 507 | 508 | 509 | 510 | 511 | 512 | 513 | 514 | 515 | 516 | 517 | 518 | 519 | 520 | 521 | 522 | 523 | 524 | 525 | 526 | 527 | 528 | 529 | 530 | 531 | 532 | 533 | 534 | 535 | 536 | 537 | 538 | 539 | 540 | 541 | 542 | 543 | 544 | 545 | 546 | 547 | 548 | 549 | 550 | 551 | 552 | 553 | 554 | 555 | 556 | 557 | 558 | 559 | 560 | 561 | 562 | 563 | 564 | 565 | 566 | 567 | 568 | 569 | 570 | 571 | 572 | 573 | 574 | 575 | 576 | 577 | 578 | 579 | 580 | 581 | 582 | 583 | 584 | 585 | 586 | 587 | 588 | 589 | 590 | 591 | 592 | 593 | 594 | 595 | 596 | 597 | 598 | 599 | 600 | 601 | 602 | 603 | 604 | 605 | 606 | 607 | 608 | 609 | 610 | 611 | 612 | 613 | 614 | 615 | 616 | 617 | 618 | 619 | 620 | 621 | 622 | 623 | 624 | 625 | 626 | 627 | 628 | 629 | 630 | 631 | 632 | 633 | 634 | 635 | 636 | 637 | 638 | 639 | 640 | 641 | 642 | 643 | 644 | 645 | 646 | 647 | 648 | 649 | 650 | 651 | 652 | 653 | 654 | 655 | 656 | 657 | 658 | 659 | 660 | 661 | 662 | 663 | 664 | 665 | 666 | 667 | 668 | 669 | 670 | 671 | 672 | 673 | 674 | 675 | 676 | 677 | 678 | 679 | 680 | 681 | 682 | 683 | 684 | 685 | 686 | 687 | 688 | 689 | 690 | 691 | 692 | 693 | 694 | 695 | 696 | 697 | 698 | 699 | 700 | 701 | 702 | 703 | 704 | 705 | 706 | 707 | 708 | 709 | 710 | 711 | 712 | 713 | 714 | 715 | 716 | 717 | 718 | 719 | 720 | 721 | 722 | 723 | 724 | 725 | 726 | 727 | 728 | 729 | 730 | 731 | 732 | 733 | 734 | 735 | 736 | 737 | 738 | 739 | 740 | 741 | 742 | 743 | 744 | 745 | 746 | 747 | 748 | 749 | 750 | 751 | 752 | 753 | 754 | 755 | 756 | 757 | 758 | 759 | 760 | 761 | 762 | 763 | 764 | 765 | 766 | 767 | 768 | 769 | 770 | 771 | 772 | 773 | 774 | 775 | 776 | 777 | 778 | 779 | 780 | 781 | 782 | 783 | 784 | 785 | 786 | 787 | 788 | 789 | 790 | 791 | 792 | 793 | 794 | 795 | 796 | 797 | 798 | 799 | 800 | 801 | 802 | 803 | 804 | 805 | 806 | 807 | 808 | 809 | 810 | 811 | 812 | 813 | 814 | 815 | 816 | 817 | 818 | 819 | 820 | 821 | 822 | 823 | 824 | 825 | 826 | 827 | 828 | 829 | 830 | 831 | 832 | 833 | 834 | 835 | 836 | 837 | 838 | 839 | 840 | 841 | 842 | 843 | 844 | 845 | 846 | 847 | 848 | 849 | 850 | 851 | 852 | 853 | 854 | 855 | 856 | 857 | 858 | 859 | 860 | 861 | 862 | 863 | 864 | 865 | 866 | 867 | 868 | 869 | 870 | 871 | 872 | 873 | 874 | 875 | 876 | 877 | 878 | 879 | 880 | 881 | 882 | 883 | 884 | 885 | 886 | 887 | 888 | 889 | 890 | 891 | 892 | 893 | 894 | 895 | 896 | 897 | 898 | 899 | 900 | 901 | 902 | 903 | 904 | 905 | 906 | 907 | 908 | 909 | 910 | 911 | 912 | 913 | 914 | 915 | 916 | 917 | 918 | 919 | 920 | 921 | 922 | 923 | 924 | 925 | 926 | 927 | 928 | 929 | 930 | 931 | 932 | 933 | 934 | 935 | 936 | 937 | 938 | 939 | 940 | 941 | 942 | 943 | 944 | 945 | 946 | 947 | 948 | 949 | 950 | 951 | 952 | 953 | 954 | 955 | 956 | 957 | 958 | 959 | 960 | 961 | 962 | 963 | 964 | 965 | 966 | 967 | 968 | 969 | 970 | 971 | 972 | 973 | 974 | 975 | 976 | 977 | 978 | 979 | 980 | 981 | 982 | 983 | 984 | 985 | 986 | 987 | 988 | 989 | 990 | 991 | 992 | 993 | 994 | 995 | 996 | 997 | 998 | 999 | 1000

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

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	1856
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 Firewall

This chapter introduces firewall and explains how to implement it.

7.1 Demands

1. Administrators detect that PC1_1 in LAN1 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-900 to protect it.

7.2 Objectives

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

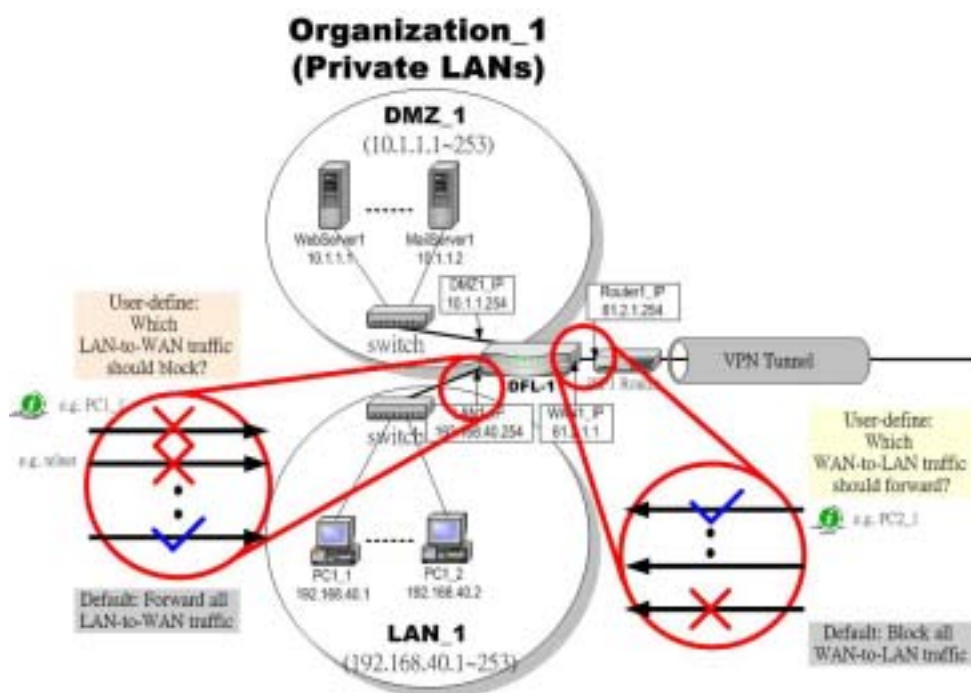



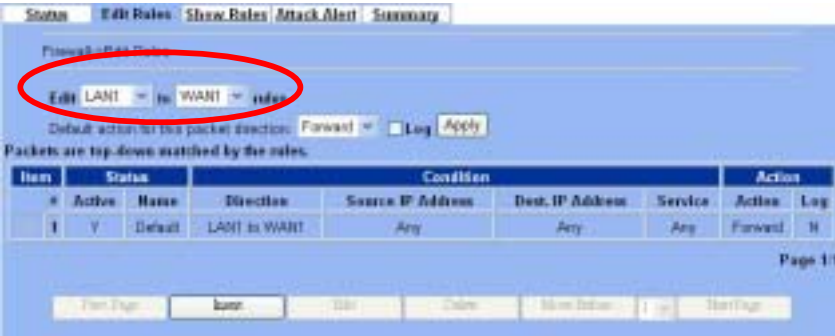
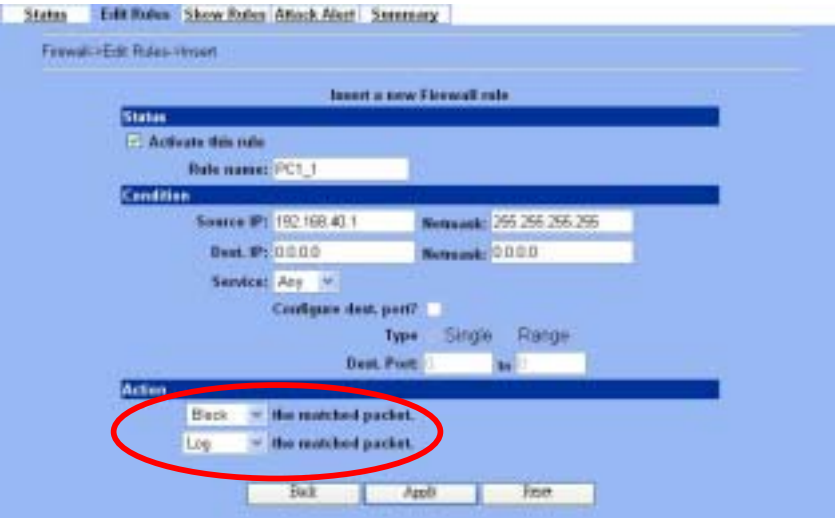
Figure 7-1 Setting up the firewall rule

7.3 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.

7.4 Steps

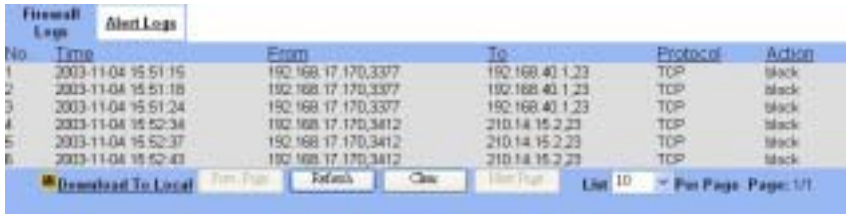
7.4.1 Block internal PC session (LAN → WAN)

<p>Step 1 - Setup NAT Check the Enable Stateful Inspection Firewall checkbox, and click the Apply.</p>	<p>ADVANCED SETTINGS > Firewall > Status</p> 
<p>Step 2 - Add a Firewall Rule Select LAN1 to WAN1 traffic direction. The default action of this direction is to forward all traffic without logging anything. Click Insert to add a Firewall block rule before the default rule to stop the bad traffic.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules</p> 
<p>Step 3 - Customize the rule Check the Activate this rule checkbox, click the Selected, and enter the IP address of PC1_1 (192.168.40.1/255.255.255.255). Select Block and Log to block and log the matched traffic. Click the Apply to apply the changes.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules > Insert</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 7-1 Insert a Firewall rule

<p>Step 4 - View the Firewall Log</p> <p>You can go to DEVICE Status>Firewall Logs >Firewall Logs to view the firewall logs. If you prefer to download these logs, please click the “Download To Local” button to save the logs to localhost.</p>	<p>DEVICE Status > Firewall Logs > Firewall Logs</p> 
--	--

7.4.2 Setup Alert detected attack

<p>Step 1 - Setup Attack Alert</p> <p>With the Firewall enabled, the DFL-900 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-900 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-900 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-900 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>ADVANCED SETTINGS > Firewall > Attack Alert</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-900 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-900 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.	
(min)	Enter the length of Blocking Time in minutes.	0

Table 7-2 Setup the Denial of Service Thresholds of attack alert

Part III

Virtual Private Network

Chapter 8

VPN Technical Introduction

This chapter introduces VPN related technology

8.1 Terminology Explanation

8.1.1 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.

8.1.2 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.

8.1.3 Security Association

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

8.1.4 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).

8.1.5 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-900. 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).

8.1.6 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.

8.1.7 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.

8.2 Make VPN packets pass through DFL-900

Step 1 - Enable IPSec

If we need to setup DFL-900 between the existed IPSec / PPTP / L2TP connections. We need to open up the Firewall blocking port of DFL-900 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-900. As well as DFL-900 will play the middle forwarding device role.

ADVANCED SETTINGS > VPN Settings > Pass Through



Chapter 9

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 tunnel between LAN_1 and LAN_2 in this chapter. The following Figure 9-1 is the real structure in our implemented process.

9.1 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.

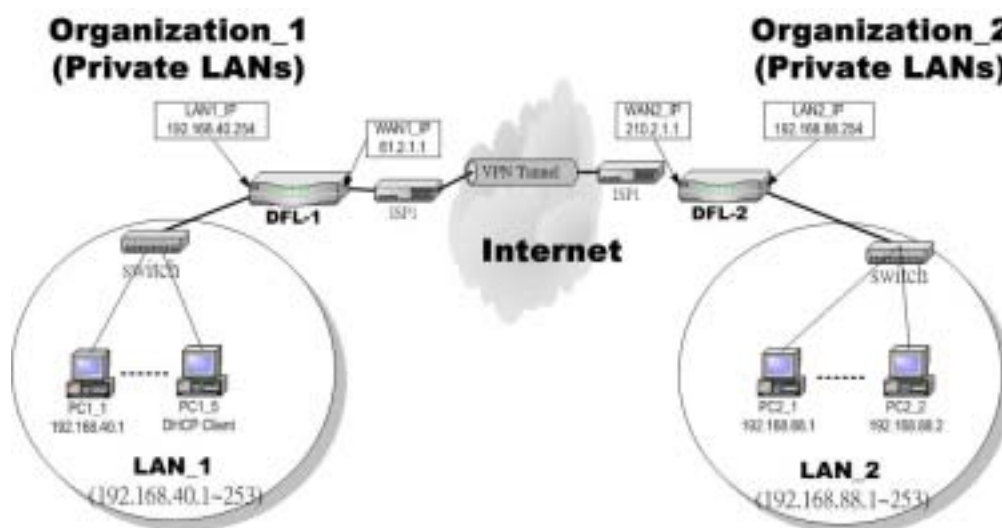


Figure 9-1 Organization_1 LAN_1 is making VPN tunnel with Organization_2 LAN_2

9.2 Objectives

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

9.3 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 IP” means the local LAN subnet; “Remote IP” 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-900s.	The types and keys of “Encryption” and “Authenticate” must be set the same on both DFL-900s. 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.
------------	---	---


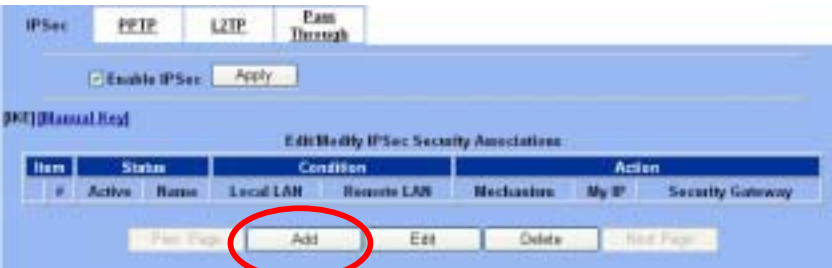
Table 9-1 Compared IKE and Manual Key methods

9.4 Steps

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

9.4.1 DES/MD5 IPSec tunnel: the IKE way

At DFL-1:

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



	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 8 for details.	Main
	Encapsulation Mode	Choose Tunnel or Transport mode, see Chapter 8 for details.	Tunnel
	My IP Address	The IP address of local site DFL-900 Firewall/VPN Router	61.2.1.1
	Security Gateway Addr	The IP address of remote site device, like DFL-900 Firewall/VPN Router.	210.2.1.1

ESP Algorithm	Select the Encryption and Authentication Algorithm combination.	Encrypt and Authenticate (DES, MD5)
AH Algorithm	Select Authentication Algorithm (MD5 or SHA1)	Authenticate (MD5)
Pre-Shared Key	The key which is pre-shared with remote side.	1234567890

Table 9-2 Related field explanation of adding a IPSec policy rule

Step 4 - Detail settings of IPSec IKE


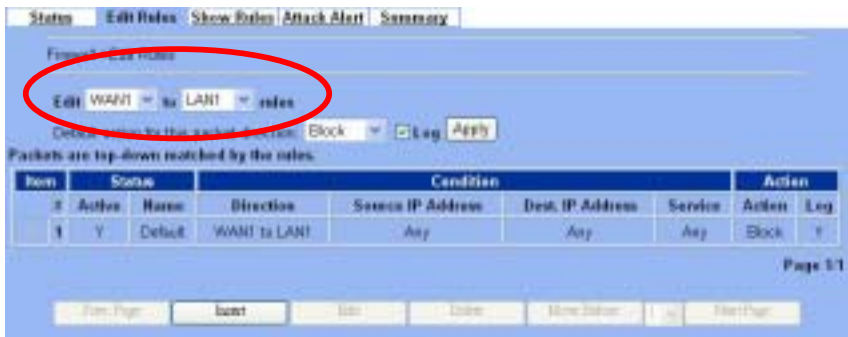
In this page, we will set the detailed value of IKE parameter. Fill the related field to finish these settings.

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

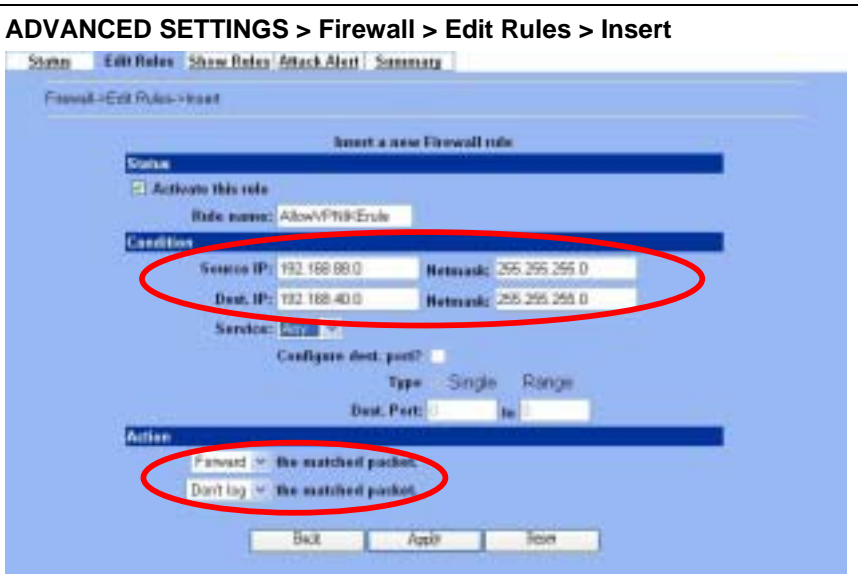
	FIELD	DESCRIPTION	EXAMPLE
Condition	Local to Remote Protocol / Src Port / Dest Port	Utilize this field to select some packets which are destined for a specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from local to remote.	TCP / 0 / 80
	Remote 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
	Phase1		
	Negotiation Mode	Choose Main or Aggressive mode, see Chapter 8 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 8 for details.	28800 sec
	Key Group	Choose a Diffie-Hellman public-key cryptography key group	DH1
Phase2			
	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 8 for details.	28800 sec
	Perfect Forward Secrecy(PFS)	Enabling PFS means that the key is transient. This extra setting will cause more security.	DH1

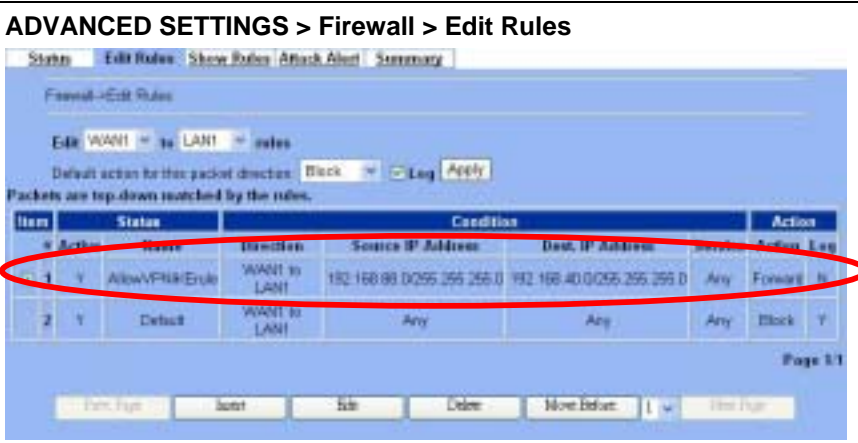
Table 9-3 Setup Advanced feature in the IPSec IKE rule

<p>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.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add</p> 																		
<p>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.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules</p>  <table border="1"> <thead> <tr> <th>Item</th> <th>Status</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>	Item	Status	Name	Direction	Source IP Address	Dest. IP Address	Service	Action	Log	1	Y	Default	WAN1 to LAN1	Any	Any	Any	Block	Y
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.

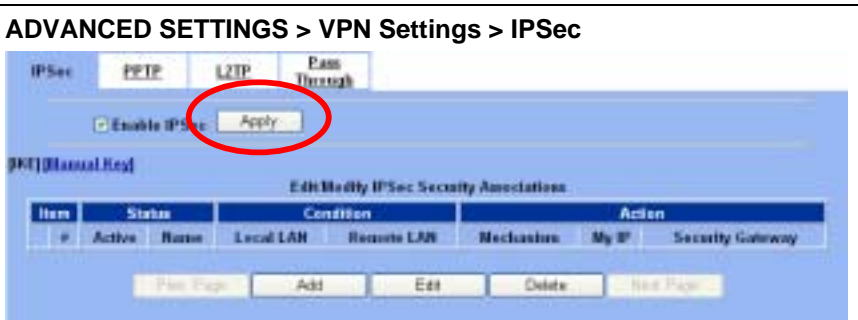


Step 8 - View the result
 Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through DFL-900. And accomplish the VPN tunnel establishment.

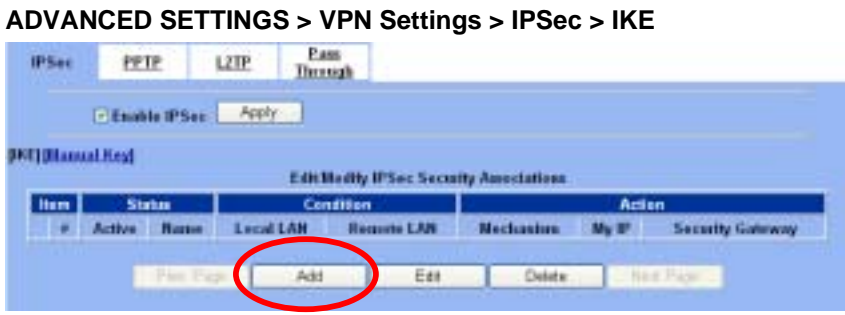


At DFL-2:

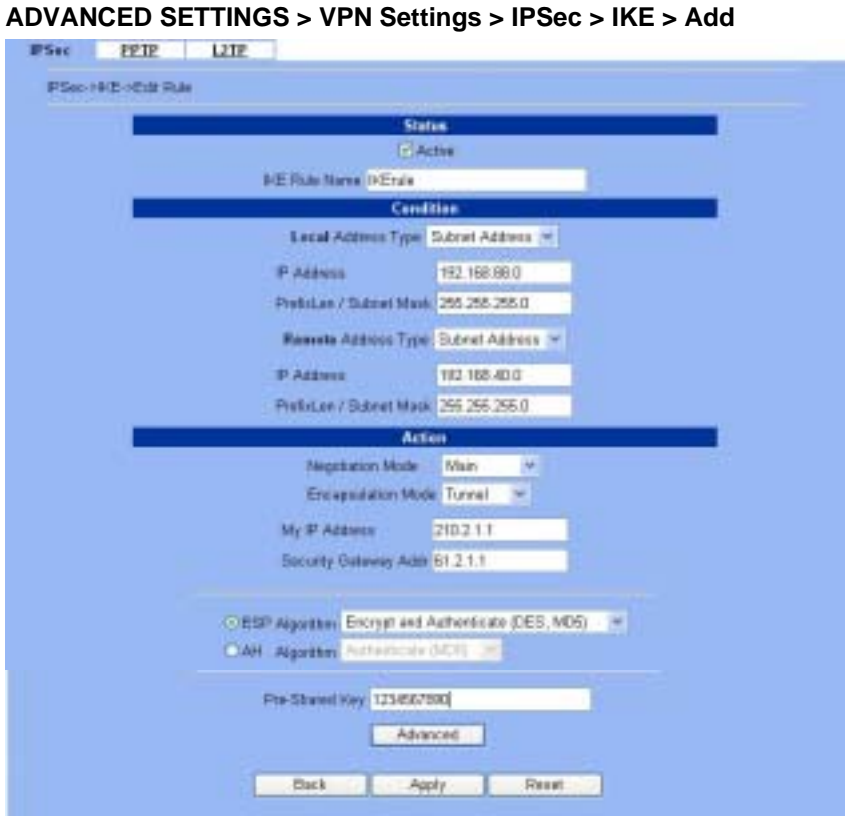
Step 1 - Enable IPSec
 Check the Enable IPSec checkbox and click Apply.



Step 2 - Add an IKE rule
 Click the [IKE](#) hyperlink and click Add to add a new IPSec VPN tunnel endpoint.





Step 3 - Customize the rule
 Check the **Active** checkbox. Enter a name for this rule like **IKERule**. Enter the **Local IP Address** (192.168.88.0/255.255.255.0) and the **Remote IP Address** (192.168.40.0/255.255.255.0). 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.



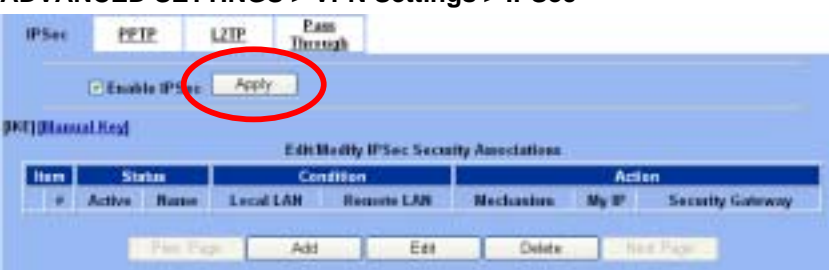
Step 4 - Add a Firewall rule
 Same as at DFL-1.

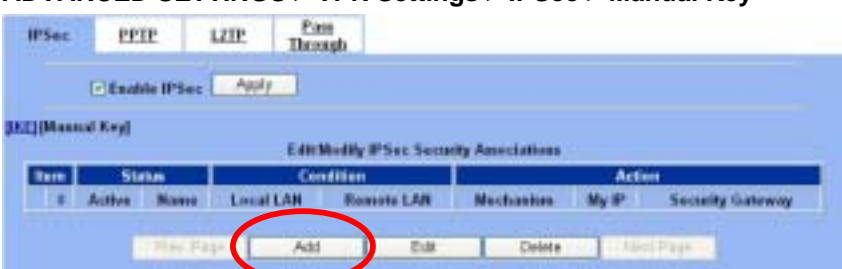

ADVANCED SETTINGS > Firewall > Edit Rules
 Just follow the above link.

<p>Step 5 - Customize the Firewall rule</p> <p>Check the Activate this rule. Enter the Rule Name as AllowVPN IKE rule, Source IP as 192.168.40.0, and Dest. IP as 192.168.88.0. Click Apply to store this rule.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules > Insert</p> 
<p>Step 6 - View the result</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-900 and successfully access the 192.168.88.0/24 through the VPN tunnel.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules</p> 

9.4.2 DES/MD5 IPsec tunnel: the Manual-Key way

Step-by-step configuration in DFL-1:


<p>Step 1 - Enable IPsec</p> <p>Check the Enable IPsec checkbox and click Apply.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPsec</p>  <table border="1" data-bbox="638 1612 1436 1680"> <thead> <tr> <th>Item</th> <th>Status</th> <th>Name</th> <th>Local LAN</th> <th>Remote LAN</th> <th>Mechanism</th> <th>My IP</th> <th>Security Gateway</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Item	Status	Name	Local LAN	Remote LAN	Mechanism	My IP	Security Gateway	1	Y						
Item	Status	Name	Local LAN	Remote LAN	Mechanism	My IP	Security Gateway										
1	Y																

<p>Step 2 - Add a Manual Key rule Click the Manual Key hyperlink and click Add to add a new IPsec VPN tunnel endpoint.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPsec > Manual Key</p> 
<p>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.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPsec > Manual Key > Add</p> 

	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-900 Firewall/VPN Router	61.2.1.1
	Security Gateway Addr	The IP address of remote site device, like DFL-900 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 8 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 9-4 Add a IPSec Manual Key rule

<p>Step 4 - Detail settings of IPSec Manual Key</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>ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key > Add > Advanced</p> 
--	--


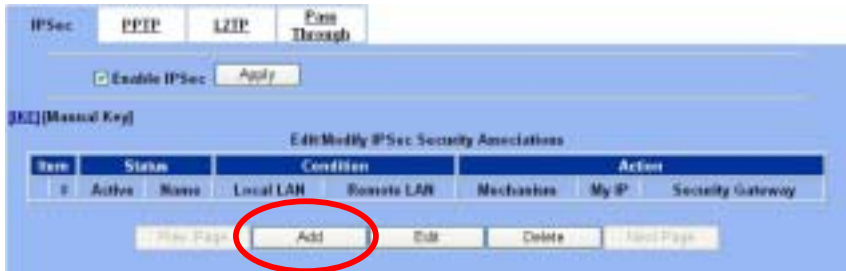
	FIELD	DESCRIPTION	EXAMPLE
Condition	Local to Remote Protocol / Src Port / Dest Port	Use this field to select some packets which are destined for specified port (Dest Port) or coming from specified port (Src Port) can use IPSec feature. The direction is from local to remote.	TCP / 0 / 80
	Remote to Local 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 9-5 Setup Advanced feature in the IPSec Manual Key rule

<p>Step 5 - Add a Firewall rule Same as that in IKE method, refer to the 9.4.1.</p>	<p>ADVANCED SETTINGS > Firewall > Edit Rules Just follow the above link.</p>
--	---

Step-by-step configuration in DFL-2:

<p>Step 1 - Enable IPSec Check the Enable IPSec checkbox and click Apply.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPSec</p> 
<p>Step 2 - Add a Manual Key rule Click the Manual Key hyperlink and click Add to add a new IPSec VPN tunnel endpoint.</p>	<p>ADVANCED SETTINGS > VPN Settings > IPSec > Manual Key</p> 

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

IPSec Manual Key Edit Rule

Status: Active

Manual Key Rule Name: ManualKeyrule

Condition

Local Address Type: Subnet Address

IP Address: 192.168.88.0

Prefix Len / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address

IP Address: 192.168.40.0

Prefix Len / Subnet Mask: 255.255.255.0

Action

My IP Address: 210.2.1.1

Security Gateway Addr.: 61.2.1.1

Outgoing SPI hex: 1111

Incoming SPI hex: 2222

Encryption Mode: Transport Tunnel

ESP - Encryption: DES (256/192 bits)

Key hex: 1122334455667788

Authentication: MD5 (128/192 bits)

Key hex: 11112222333344445555666677778888

AH - Authentication: MD5 (128/192 bits)

Key hex:

Advanced

Back Apply Reset

Step 4 - Add a Firewall rule

Same as that in IKE method, refer to the 9.4.1.

ADVANCED SETTINGS > Firewall > Edit Rules

Just follow the above link.

Chapter 10

Virtual Private Network – PPTP

This chapter introduces PPTP and explains how to implement it.

10.1 Demands

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.

10.2 Objectives

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.

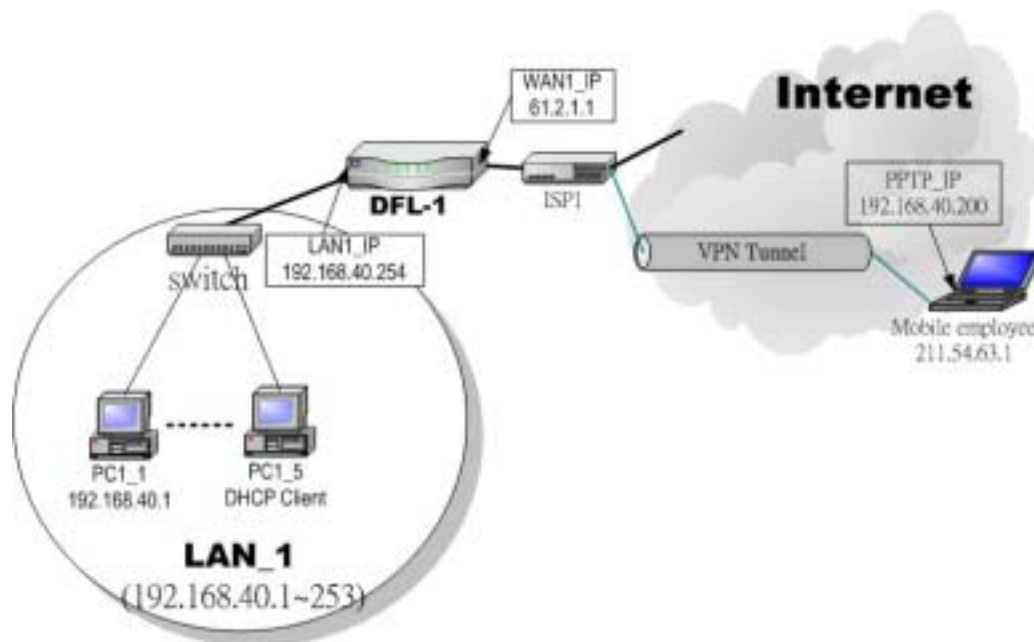


Figure 10-1 PPTP method connection

10.3 Methods

Setup the PPTP server at DFL-900. 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 192.168.40.200 ~ 192.168.40.253, the remote host may get an IP of 192.168.40.200 and logically become a member in LAN1.

10.4 Steps

Step 1 – Enable PPTP

Check the Enable PPTP 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 PPTP clients in the Start IP and the End IP fields. Enter the Username and Password that will be used by the employees during dial-up. Check the preferred Authentications and click the Apply.

ADVANCED SETTINGS > VPN Settings > PPTP

FIELD	DESCRIPTION	EXAMPLE
Enable PPTP	Enable PPTP feature of the DFL-900	enabled
Local IP	The Local IP is the allocated IP address in the internal Network after PPTP client dials in the DFL-900.	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-900.	192.168.40.200
End IP	The End IP is the allocated ending IP address in the internal network after PPTP client dials in the DFL-900.	192.168.40.253
Username	The account which allow PPTP client user to dial in DFL-900.	PptpUsers
Password	The password which allow PPTP client user to dial in DFL-900.	Dif3wk
Authentication	Determine the authentication method, chap / chapms / chapms-v2	chap

Table 10-1 Setup PPTP Server

Step 2 – Setup Windows XP/2000 PPTP clients

Configuring A PPTP Dial-Up Connection

1. Configuring a PPTP dial-up connection
2. Go to Start > Control Panel > Network and Internet Connections > Make new connection.
3. Select Create a connection to the network of your workplace and select Next.
4. Select Virtual Private Network Connection and select Next.
5. Give a Name the connection and select Next.
6. If the Public Network dialog box appears, choose the Don't dial up initial connection and select Next.
7. In the VPN Server Selection dialog, enter the public IP or hostname of the DFL-900 to connect to and select Next.
8. Set Connection Availability to Only for myself and select Next.
9. Select Finish.

	<p><u>Customize the VPN Connection</u></p> <ol style="list-style-type: none">1. Right-click the icon that you have created.2. Select Properties > Security > Advanced > Settings.3. Select No Encryption from the Data Encryption and click Apply.4. Select the Properties > Networking tab.5. Select PPTP VPN from the VPN Type. Make sure the following are selected: TCP/IP QoS Packet Scheduler6. Select Apply.
	<p><u>Connecting to the PPTP VPN</u></p> <ol style="list-style-type: none">1. Connect to your ISP.2. Start the dial-up connection configured in the previous procedure.3. Enter your PPTP VPN User Name and Password.4. Select Connect.

Chapter 11

Virtual Private Network – L2TP

This chapter introduces L2TP 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 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.
2. In our branch office, we need to provide L2TP connection methods to connect back to headquarter for the internal company employees.

11.2 Objectives

1. With L2TP 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.

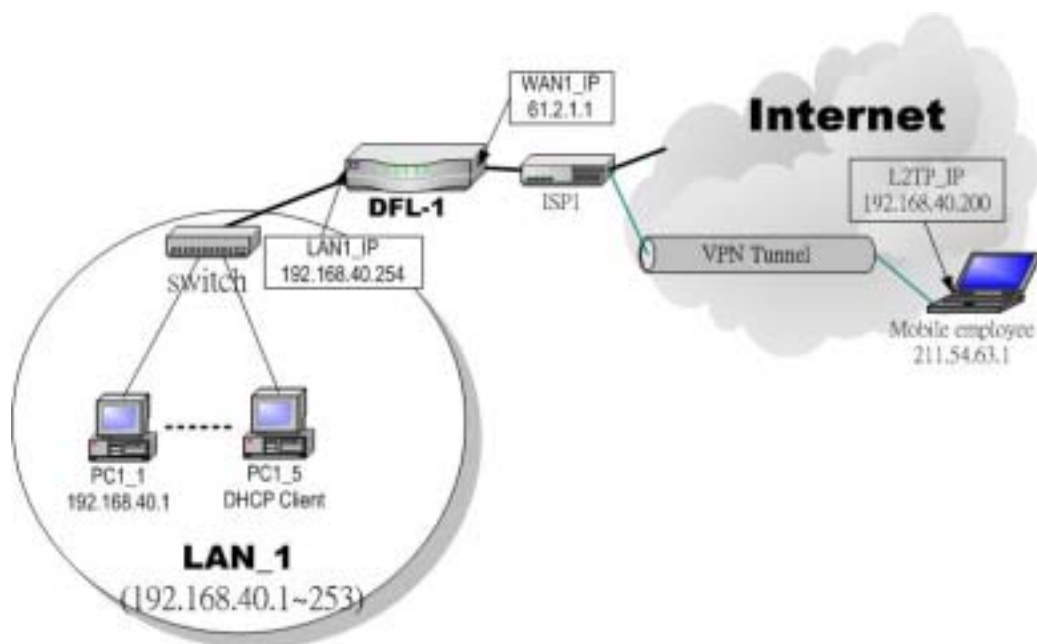


Figure 11-1 L2TP method connection

11.3 Methods

1. Setup the L2TP server at DFL-1 (LNS: L2TP Network Server). After dialing up to DFL-1, DFL-1 will assign a private IP which falls in the range of the settings in the L2TP server at DFL-1. 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 LAN1.

2. Setup the DFL-900 as the L2TP client (LAC: L2TP Access Concentrator). Let all the client PCs behind the DFL-900. They can connect to the network behind L2TP Server by passing through DFL-900. It sounds like no Internet exists but can connect with each other.

11.4 Steps

11.4.1 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. Check the preferred Authentications and click the Apply.

ADVANCED SETTINGS > VPN Settings > L2TP > LNS

The screenshot shows the configuration interface for L2TP LNS. The 'L2TP' tab is active, and the 'Enable L2TP LNS' checkbox is checked. The configuration fields are as follows:

- Local IP: 192.168.40.254
- Start IP: 192.168.40.200
- End IP: 192.168.40.253
- LAC Start IP: 211.54.63.1
- LAC End IP: 211.54.63.5
- Username: L2tpUser
- Password: *****
- Authentication: chap, chapms, chapms-v2

Buttons for 'Apply' and 'Reset' are visible at the bottom.

FIELD	DESCRIPTION	EXAMPLE
Enable L2TP LNS	Enable L2TP LNS feature of DFL-900	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-900.	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-900.	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-900.	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-900.	L2tpUser
Password	The password which allows L2TP client user to dial in DFL-900.	Dif3wk
Authentication	Determine the authentication method, chap / chapms / chapms-v2	chap

Table 11-1 Setup L2TP LNS Server settings

Step 2 – Setup Windows XP/2000 L2TP clients**Configuring A L2TP Dial-Up Connection**

1. Configuring a L2TP dial-up connection
2. Go to Start > Control Panel > Network and Internet Connections > Make new connection.
3. Select Create a connection to the network of your workplace and select Next.
4. Select Virtual Private Network Connection and select Next.
5. Give a Name the connection and select Next.
6. If the Public Network dialog box appears, choose the Don't dial up initial connection and select Next.
7. In the VPN Server Selection dialog, enter the public IP or hostname of the DFL-900 to connect to and select Next.
8. Set Connection Availability to Only for myself and select Next.
9. Select Finish.

Customize the VPN Connection

1. Right-click the icon that you have created.
2. Select Properties > Security > Advanced > Settings.
3. Select No Encryption from the Data Encryption and click Apply.
4. Select the Properties > Networking tab.
5. Select L2TP VPN from the VPN Type.
Make sure the following are selected:
 - TCP/IP
 - QoS Packet Scheduler
6. Select Apply.

Editing Windows Registry

The default Windows 2000 L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows 2000 Registry as described in the following steps. Please refer to the Microsoft documentation for editing the Windows Registry.

1. Use the registry editor (regedit) to locate the following key in the registry: HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Rasman \ Parameters
2. Add the following registry value to this key:
 - Value Name: ProhibitIpSec
 - Data Type: REG_DWORD
 - Value: 1
3. Save your changes and restart the computer.

You must add the ProhibitIpSec registry value to each Windows 2000-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the ProhibitIpSec registry value is set to 1, your Windows 2000-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy.

Connecting to the L2TP VPN

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

11.4.2 Setup L2TP Network Client**Step 1 – Enable L2TP LAC**

Fill in the IP address of LNS Server and allocates Username/Password. When connecting to the LNS Server successfully, it will appear the allocated IP address for the L2TP client in the “Assigned IP” field, and the IP address of LAC host peer host will appear in the “Remote IP” field.

ADVANCED SETTINGS > VPN Settings > L2TP > LAC

FIELD	DESCRIPTION	EXAMPLE
Enable L2TP LAC	Enable L2TP LAC feature of DFL-900	enabled
LNS IP	The IP address of LNS server.	61.2.1.1
Username	The designed account which allows LAC client to dial in.	L2tpUser
Password	The designed password which allows LAC client to dial in.	Dif3wk
Assigned IP	The allocated IP address when LAC host connects to the LNS server.	
Remote IP	The IP address in the LNS server side when LAC host connects to the LNS server.	

Table 11-2 Setup L2TP LAC settings

Part IV

Content Filters

Chapter 12

Content Filtering – Web Filters

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

12.1 Demands

1. Someone (PC1_1) is browsing the web pages at the WebServer3. The contents of the web pages may include cookies, Java applets, Javascripts, or Active-X objects that may contain malicious program of users' information.
2. 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.

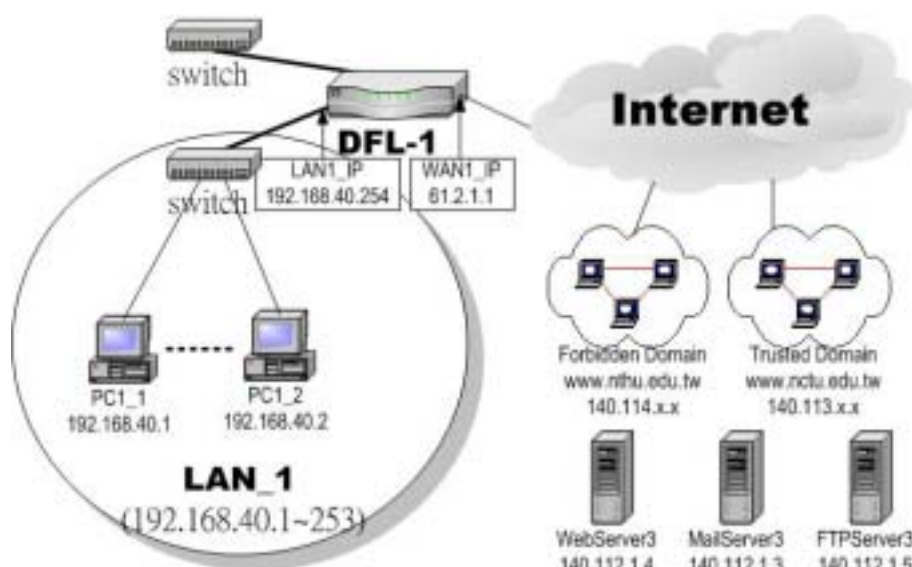


Figure 12-1 Use web filter functionality to avoid users view the forbidden pages or web site




12.2 Objectives

1. Remove the cookies, Java applet, Javascripts, Active-X objects from the web pages.
2. Prevent users from connecting to the forbidden sites.

12.3 Methods

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

12.4 Steps

<p>Step 1 - Enable Web Filter</p> <p>Check the Enable Web Filter checkbox and click the Apply right on the right side.</p>	<p>ADVANCED SETTINGS > Content Filters > Web Filter</p> 
<p>Step 2 - Warning of Firewall</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>ADVANCED SETTINGS > Content Filters > Web Filter</p> 
<p>Step 3 - Customize Objects</p> <p>Check the objects of Restricted Features to block the objects. Click the Apply button at the bottom of this page. Use PC1_1 to browse the web page to see if the objects are blocked. If the objects still exist, the objects may be cached by the browser. Please clear the cache in the web browser, close the browser, reopen the browser, and connect to the web page again.</p>	<p>ADVANCED SETTINGS > Content Filters > Web Filter</p> 

FIELD	DESCRIPTION	EXAMPLE
Enable Web Filter	Enable Web Filter feature of DFL-900	enabled
Restricted Features	Setting up the component (Include ActiveX, Java, Java Script, Cookies, Web Proxy)	

Table 12-1 Web Filter Web setting page

<p>Step 4 - Customize Categories</p> <p>With the built-in URL database, DFL-900 can block web sessions towards several pre-defined Categories of URLs. Check the items that you want to block or log. Simply click the Block all categories will apply all categories. Click Log & Block Access if you want to block and log any matched traffic. You can customize the Time of Day to allow such traffic after the office hours, such as 9:30 to 17:30.</p>	<p>ADVANCED SETTINGS > Content Filters > Web Filter > Categories</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
Time of Day	The time which was set for Web Filter.	

Table 12-2 Web Filter Categories setting page

<p>Step 5 - Update the Built-in Database</p> <p>Click the Download button to ask DFL-900 to instantly download the database from the fwupdate.dlinktw.com.tw. The DFL-900 can be set to automatically check the site for any new updates by checking the Automatic Download. You can also configure how frequently the DFL-900 checks for the updates. Click Apply to store the changes. From now on, any traffic matched with the URLs in the database will be blocked by the DFL-900.</p>	<p>ADVANCED SETTINGS > Content Filters > Web Filter > Database Update</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).	

Table 12-3 Web Filter database update

<p>Step 6 - Further Customize the local zones</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 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.</p>	<p>ADVANCED SETTINGS > Content Filters > Web Filter > Exempt Zone</p> 
---	--


FIELD	DESCRIPTION	EXAMPLE
Exempt Computers	<ul style="list-style-type: none"> ➤ Enforce web filter policies for all computers Web filter activates at all the computers, not limit range of the IP addresses ➤ Include specified address ranges in the web filter enforcement Web filter only activates at below specified computers. ➤ 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. 	Enforce web filter policies for all computers
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

Table 12-4 Web Filter Exempt Zone setting page

<p>Step 7 - Further Customize the remote sites</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-900 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>ADVANCED SETTINGS > Content Filters > Web Filter > Customize</p> 
--	--

FIELD	DESCRIPTION	EXAMPLE
Filter List Customization	<ul style="list-style-type: none"> ➤ Enable Filter List Customization Enable the Filter List Customization feature of web filter <ul style="list-style-type: none"> ➤ 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. <ul style="list-style-type: none"> ➤ 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 Enabled Enabled
Trusted Domains / Forbidden Domains	Here we can specify the Trusted Domains / Forbidden Domains for the above item using.	

Table 12-5 Web Filter Customize setting page

<p>Step 8 - Setup URL keyword blocking</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>ADVANCED SETTINGS > Content Filters > Web Filter > Domain Name</p> 
---	---

FIELD	DESCRIPTION	EXAMPLE
Enable Keyword blocking	Enable 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

Table 12-6 Web Filter Domain Name setting page

Chapter 13

Content Filtering – Mail Filters

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

13.1 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.

13.2 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.

13.3 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.

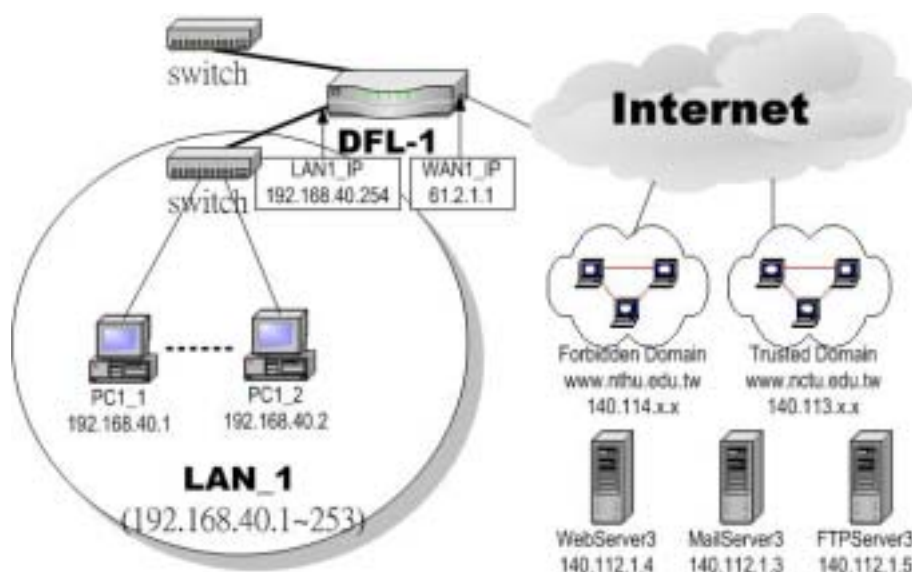




Figure 13-1 Use SMTP / POP3 filter functionality to avoid some sensitive e-mail directly opened

13.4 Steps for SMTP Filters

<p>Step 1 – Enable SMTP Filters</p> <p>Check the <code>Enable SMTP Proxy</code> checkbox and click <code>Apply</code>.</p>	<p>ADVANCED SETTINGS > Content Filters > Mail Filters > SMTP</p> 
---	---

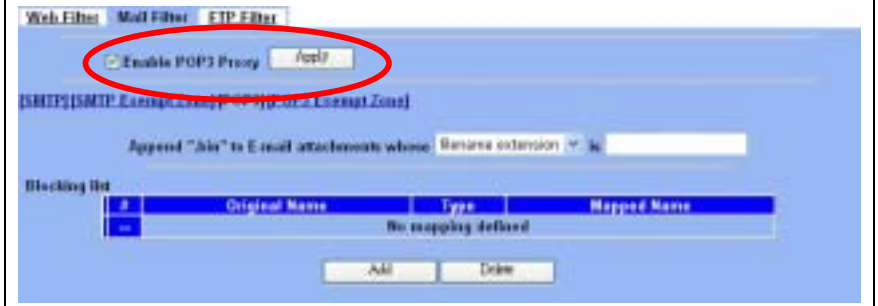
FIELD	DESCRIPTION	EXAMPLE
Enable SMTP Proxy	Enable SMTP Proxy feature of DFL-900	enabled
Append ".bin" to E-mail attachments whose	<ul style="list-style-type: none"> ➤ Filename extension When the filename extension of attachment file matches "Filename extension", add the ".bin" extension to the attachment file. ➤ Exact filename When the whole filename of attachment file matches "Exact filename", add the ".bin" extension to the attachment file. 	Filename extension

Table 13-1 Mail Filter SMTP setting page

<p>Step 2 – Add a SMTP Filter</p> <p>Select filename extension, enter <code>vbs</code>, and click <code>Add</code> 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 <code>vbs</code> to <code>vbs.bin</code>.</p>	<p>ADVANCED SETTINGS > Content Filters > Mail Filters > SMTP</p> 
--	---

<p>Step 3 – Customize the local zones Same as in setting Web Filters.</p>	<p>ADVANCED SETTINGS > Content Filters > Mail Filters > SMTP Exempt Zone</p> 
--	---

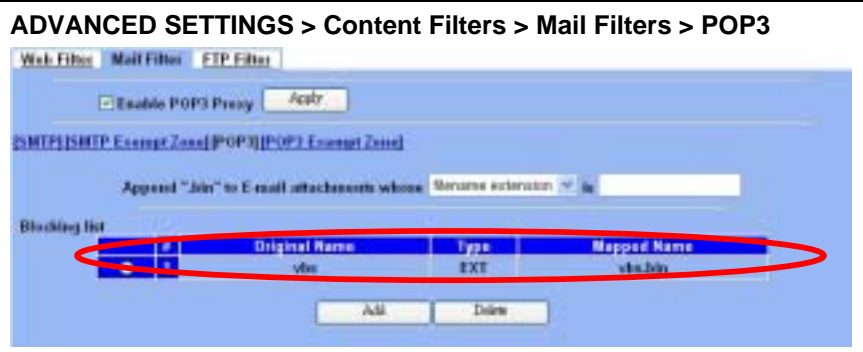
13.5 Steps for POP3 Filters

<p>Step 1 – Enable POP3 Filters Check the Enable POP3 Proxy checkbox and click Apply.</p>	<p>ADVANCED SETTINGS > Content Filters > Mail Filters > POP3</p> 
--	---

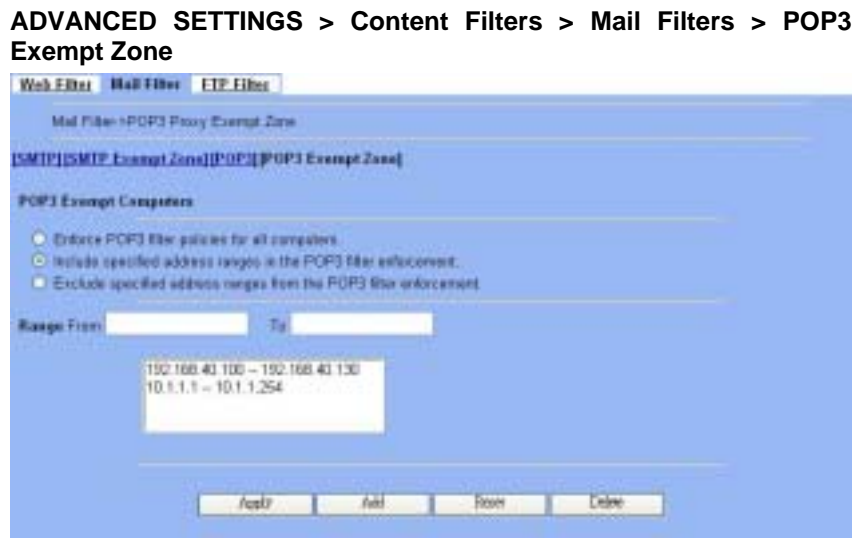
FIELD	DESCRIPTION	EXAMPLE
Enable POP3 Proxy	Enable POP3 Proxy feature of DFL-900	enabled
Append ".bin" to E-mail attachments whose	<ul style="list-style-type: none"> ➤ Filename extension When the filename extension of attachment file matches “Filename extension”, add the “.bin” extension to the attachment file. ➤ Exact filename When the whole filename of attachment file matches “Exact filename”, add the “.bin” extension to the attachment file. 	Filename extension

Table 13-2 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.



Step 3 – Customize the local zones
 Same as in setting Web Filters.



Chapter 14

Content Filtering – FTP Filtering

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

14.1 Demands

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

14.2 Objectives

1. Forbid PC1_1 from downloading MP3 files with FTP.

14.3 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.

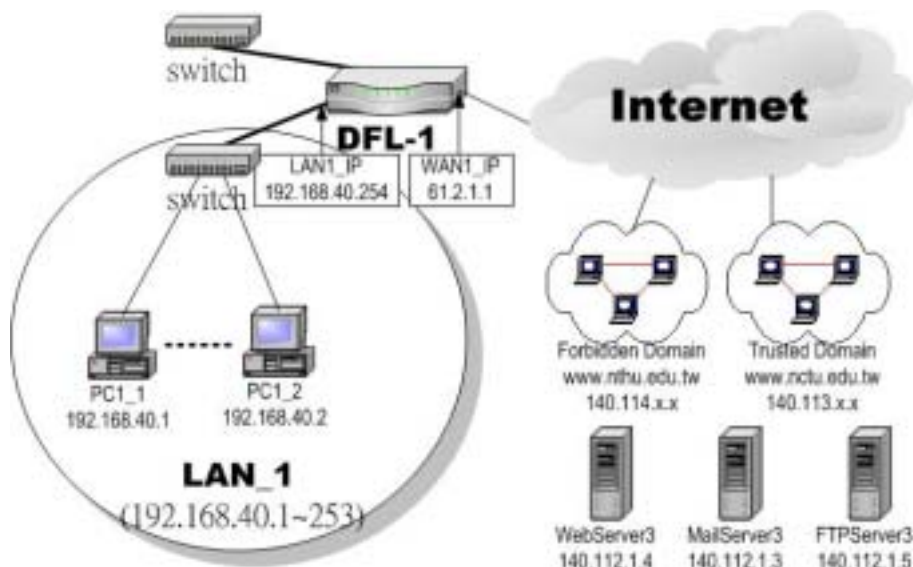



Figure 14-1 Use FTP filter functionality to avoid user download forbidden file type

14.4 Steps

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


FIELD	DESCRIPTION	EXAMPLE
Enable FTP Filter	Enable FTP Filter feature of DFL-900	enabled

Table 14-1 FTP Filter FTP setting page

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


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

Table 14-2 FTP Filter FTP adding filter entry

<p>Step 3 - Add an Exempt Zone</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>ADVANCED SETTINGS > Content Filters > FTP Filter > FTP Exempt Zone > Add</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 14-3 FTP Filter add an exempt zone entry

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

Part V

Intrusion Detection System

Chapter 15

Intrusion Detection Systems

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

15.1 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.

15.2 Objectives

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

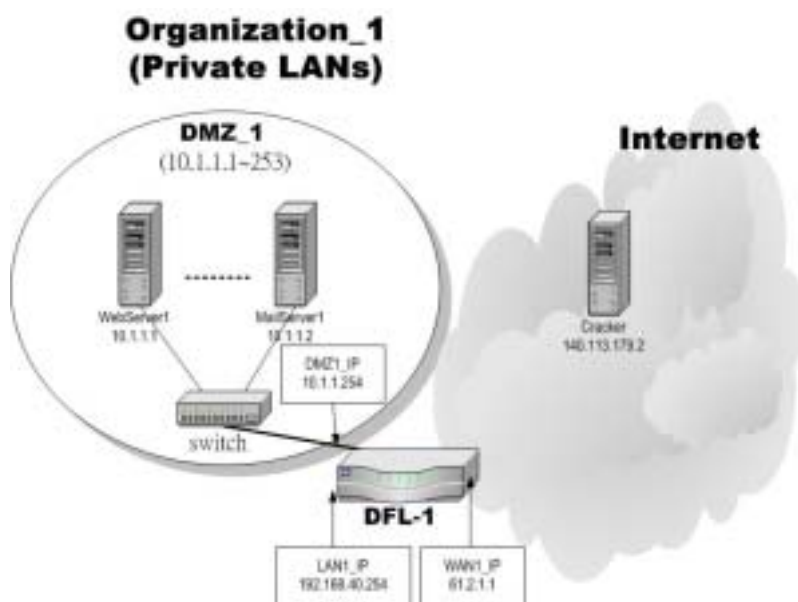


Figure 15-1 Some cracker in the Internet would try to hack our company

15.3 Methods

1. Specify where our Web server is located to let the IDS on the DFL-900 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.

15.4 Steps

Step 1 – Enable IDS




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.

ADVANCED SETTINGS > IDS > IDS Status

FIELD	DESCRIPTION	EXAMPLE
Enable IDS	Enable IDS feature of DFL-900	enabled
Detect Attacks Towards	Specified the IP address region of each DMZ/LAN, Server area.	
Options		
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 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 15-1 IDS option list explanation

<p>Step 2 – Setup Logs</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>DEVICE STATUS > Log Config > Mail Logs</p> 
<p>Step 3 – View logs</p> <p>If there are attacks towards the WAN port from the public Internet, there will be logs describing the details.</p>	<p>DEVICE STATUS > IDS Logs</p> 
<p>Step 4 – Update Attack Patterns</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-900 will connect to fwupdate.dlinktw.com.tw to fetch any new signatures.</p>	<p>ADVANCED SETTINGS > IDS > Update Rule</p> 

Part VI

Bandwidth Management

Chapter 16

Bandwidth Management

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

16.1 Demands

1. PC1_1 is downloading the MP3 files from the FTP Server. This occupies the bandwidth of PC1_2 who is watching the video provided by the Web Server, causing the video to be blocked and to have poor quality.
2. WAN_PC is downloading the files from Web Server, causing the blocking of the VPN transfer from LAN_1 to LAN_2.

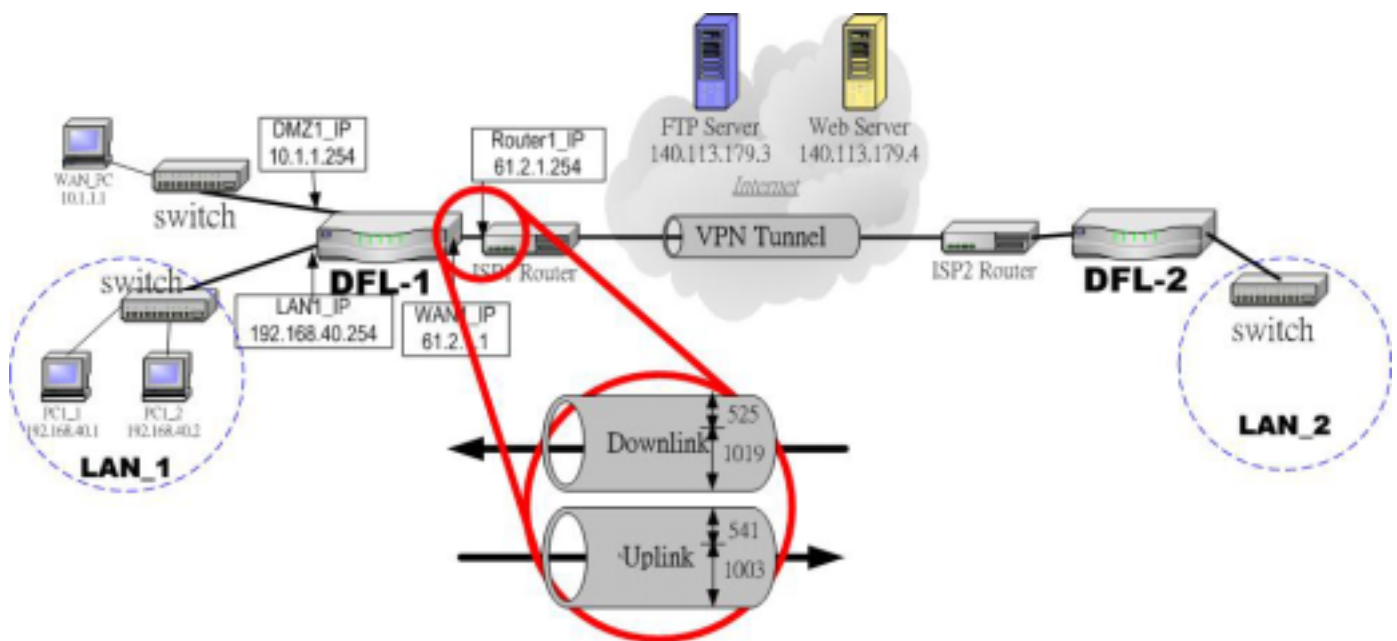


Figure 16-1 Use bandwidth management mechanism to shape the data flow

16.2 Objectives


1. 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.
2. Reserve at least 1Mbps for the LANa-to-LANb transfer. The others can share the remaining 463kbps. However, when the LANa-to-LANb traffic has only 300kbps, the others can occupy the bandwidth up to (1003kbps - 300kbps) + 463kbps.

16.3 Methods

1. Partition the inbound bandwidth (1.544Mbps) into two classes, the FTP and the Video classes. Set the Video class to obtain the 447kbps and set it to be able to be borrowed to others. Set the FTP class to obtain 1019kbps.
2. Partition the outbound bandwidth (1.544Mbps) into two classes, the LANa-to-LANb and the Others classes. Set the LANa-to-LANb to obtain 1Mbps and set it to be able to be borrowed to Others. Set the others class to obtain 463kbps.

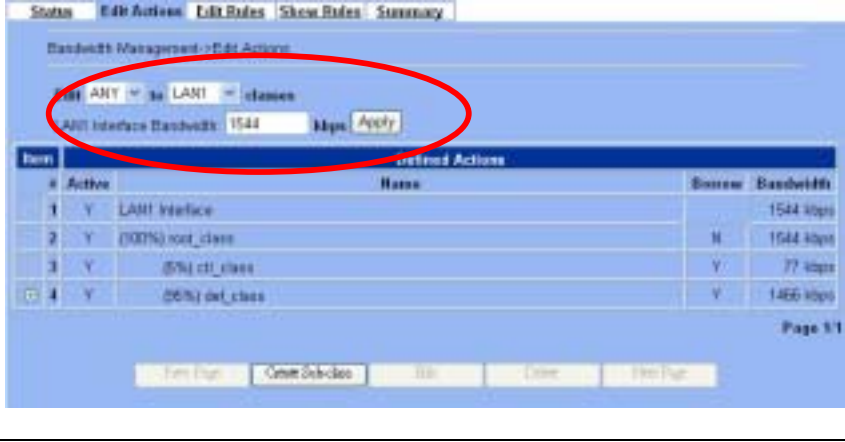
16.4 Steps


16.4.1 Inbound Traffic Management

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

FIELD	DESCRIPTION	EXAMPLE
Enable Bandwidth Management	Enable Bandwidth Management feature of DFL-900	enabled



Table 16-1 Setup Bandwidth Management status page

<p>Step 2 - Setup the LAN1 Link</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>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions</p> 
---	---

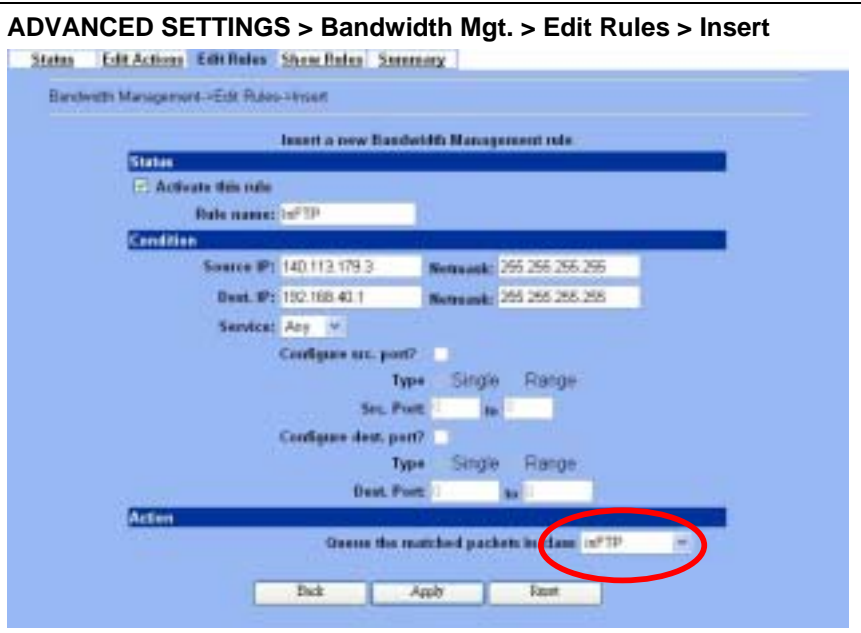
<p>Step 3 - Add new classes</p> <p>Create a sub-class named inFTP from the default class. Enter 66% in the bandwidth field and click Apply. Select the default class and click the Create Sub-Class to create another sub-class named inVideo from the default class. Enter 29% in the bandwidth field, check the Let other classes utilize any available bandwidth of this class, and click Apply.</p>	<p>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-class</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 this class is idle, it will let other class to borrow from temporarily.	Not enabled

Table 16-2 Add new class in the bandwidth management feature

<p>Step 4 - Partition into Classes Now there are two actions under the default action.</p>	<p>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-Class</p> 
<p>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.</p>	<p>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Rules</p> 

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. Click Apply to store the changes. Repeat the same procedure for the inVideo class.



	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".	140.113.79.3 255.255.255.255
	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

Table 16-3 Add a new Bandwidth Management rule

Step 7 - View the rules

The DFL-900 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

16.4.2 Outbound Traffic Management

Step 1 - Enable Bandwidth Management

Check the Enable Bandwidth Management checkbox, click the Apply.

ADVANCED SETTINGS > Bandwidth Mgt. > Status

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

Step 3 - Partition into Classes
 Create a sub-class named LANa-to-LANb from the default class. Enter 65% in the bandwidth field and click Apply. Select the default class and click the Create Sub-Class to create another sub-class named Others from the default class. Enter 30% in the bandwidth field, check the Let other classes utilize any available bandwidth of this class, and click Apply. Now there are two actions under the default action.

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

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

Step 5 - Customize the Rules
 Same as that in inbound management.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit Rules > Insert

Step 6 - View the rules

The DFL-900 is configured to direct outWebDownload-matched packets into the Others 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

Bandwidth Management -> Edit Rules

EDIT ANY to WAN1 rules
Packets are top-down matched by the rules.

Item	Status	Name	Direction	Source IP Address	Dest. IP Address	Service	Action
1	Y	outVPN	ANY to WAN1	192.168.40.0/255.255.255.0	192.168.98.0/255.255.255.0	Any	LANa-to-LANb
2	Y	outWebDownload	ANY to WAN1	10.1.1.1/255.255.255.255	140.113.170.4/255.255.255.255	Any	Others
3	Y	Default	ANY to WAN1	Any	Any	Any	def_class

Page 1/1

Part VII

System Maintenance

Chapter 17

Log System

17.1 Demands

1. 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-900 logs. He / She hopes to decrease the checking procedure.

17.2 Objectives

1. The System administrator would like to view the daily log report of DFL-900.

17.3 Methods


1. Use the syslog server to receive mail. Or edit the “Mail Logs” page of DFL-900. Make the log mailed out automatically every periodic time.

17.4 Steps

<p>Step 1 - Setup Syslog Server</p> <p>Setup Syslog Server by checking the <code>Enable Syslog Server</code>. It will let DFL-900 send logs to the Syslog Server specified in the “Syslog Server IP Address” field.</p>	<p>DEVICE STATUS > Log Config > Syslog Server</p> 
--	---

FIELD	DESCRIPTION	EXAMPLE
Syslog Server	Enable the Syslog Server feature of DFL-900	Enabled
Syslog Server IP Address	The IP Address which Syslog Server located.	10.1.1.20

Table 17-1 Setup the Syslog Server

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

FIELD	DESCRIPTION	EXAMPLE
Mail Server IP Address	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

Table 17-2 Setup the Mail Logs

Chapter 18

System Maintenance

This chapter introduces how to do system maintenance.

18.1 Demands


1. DFL-900 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-900. 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-900 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.

18.2 Steps for TFTP Upgrade

<p>Step 1 - Setup TFTP server</p> <p>Place the TFTP server <code>TftpServer.exe</code> in the <code>c:\</code> directory and double click to run it. Place all bin 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-900's LAN1. Login to DFL-900's console. Enter <code>en</code> to enter privileged mode. Configure the LAN1 address so that the DFL-900 can connect to the TFTP server. The CI command to configure LAN1 interface is <code>IP ifconfig INTF1 192.168.1.254 255.255.255.0</code>.</p>	<pre>NetOS/i386 (DFL-900) (tty00) login: admin Password: Welcome to DFL-900 Firewall/VPN Router! DFL-900> en DFL-900# ip ifconfig INTF1 192.168.1.254 255.255.255.0 DFL-900#</pre>
<p>Step 2 - Upgrade firmware</p> <p>Enter <code>IP tftp upgrade combo 192.168.1.x <date>-DFL900-<ver>.bin</code></p>	<pre>DFL-900# ip tftp upgrade combo 192.168.1.2 20030910-DFL-900-1.40B.bin Fetching from 192.168.1.2 for 20030910-DFL-900-1.40B.bin tftp> tftp> Verbose mode on. tftp> getting from 192.168.1.2:20030910-DFL-900-1.40B.bin to 20030910-DFL-900-1.40B.bin [octet]</pre>
<p>Step 3 - Reboot the system</p> <p>Enter <code>sys reboot now</code> to instantly reboot the system.</p>	<pre>DFL-900# sys reboot now Rebooting... syncing disks... done rebooting...</pre>

<p>Step 4 - Check if OK</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 wd0: drive supports PIO mode 4 IPsec: Initialized Security Association Processing. Current WAN1 IP = 192.168.17.87 Netmask = 0xffffffff00 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-900) (tty00) login: </pre>
------------------------------------	--

18.3 Steps for Firmware upgrade from Web GUI

<p>Step 1 – Download the newest firmware from web site</p>	<p>Firmware upgrade site : http://fwupdate.dlinktw.com.tw/</p>
<p>Step 2 – Upgrade firmware</p> <p>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.</p>	

18.4 Steps for Factory Reset



18.4.1 Steps for NORMAL factory reset

<p>Step 1 – Factory reset</p> <p>Enter <code>sys resetconf now</code> to reset the firmware to factory default. Then enter <code>sys reboot now</code> to instantly reboot the system.</p>	<pre>NetOS/i386 (DFL-900) (tty00) login: admin Password: Welcome to DFL-900 Firewall/VPN Router! DFL-900> en DFL-900# sys resetconf now Resetting Configuration to default... DONE Please reboot the system DFL-900# sys reboot now Rebooting... syncing disks... done rebooting...</pre>
---	--

18.4.2 Steps for EMERGENT factory reset

<p>Step 1 – Enter the boot loader</p> <p>If you forget the password, this is the only way to recover your system. Press <tab> or <space> during the 2-second countdown process.</p>	<pre>>> NetOS/i386 BIOS boot, Revision 2.7 (Wed Sep 10 05:42:33 CST 2003) booting - starting in 0 type "?" or "help" for help. ></pre>
<p>Step 2 – Enter the Safe Mode</p> <p>Enter <code>boot rescue</code> to enter the emergency kernel. In this kernel, you can use <code>tftp</code> to fetch another firmware to install, or reset the configuration to default even you lost the password.</p>	<pre>> 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 wd0: drive supports PIO mode 4 DFL-900></pre>
<p>Step 3 – Factory reset</p> <p>Enter <code>sys resetconf now</code> to reset the firmware to factory default. Then enter <code>sys reboot now</code> to instantly reboot the system.</p>	<pre>DFL-900> en DFL-900# sys resetconf now Resetting Configuration to default... DONE Please reboot the system DFL-900# sys reboot now Rebooting...</pre>

18.5 Steps for Backup / Restore Configurations

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

Appendix A

Trouble Shooting

1. If the power LED of DFL-900 is off when I turn on the power?

Ans : Check the connection between the power adapter and DFL-900 power cord. If this problem still exists, contact with your sales vendor.

2. How can I configure the DFL-900 if I loss the account/password of the DFL-900 ?

Ans : Use the Console mode (CLI) to restore the factory setting, refer to the procedure as .prior section 18.4.2.

3. I can't access DFL-900 via the console port ?

Ans : Check the console line and make sure it is connected between your computer serial port and DFL-900 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-900 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. Verify if DMZ1 port checkbox is enabled.

5. 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 9.4.1- 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-900. (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 18-1 and Figure 18-2 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 18-2.

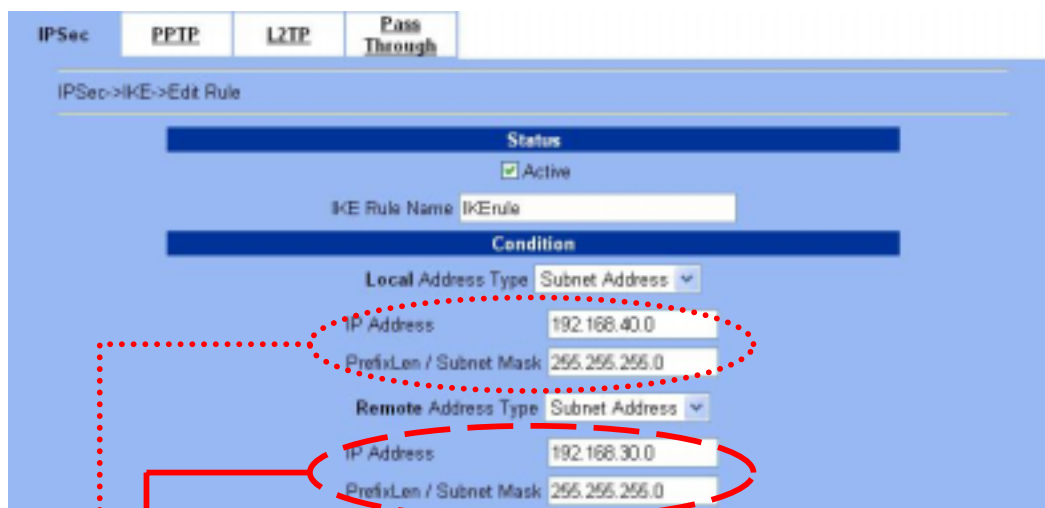


Figure 18-1 Inset a new IPsec policy

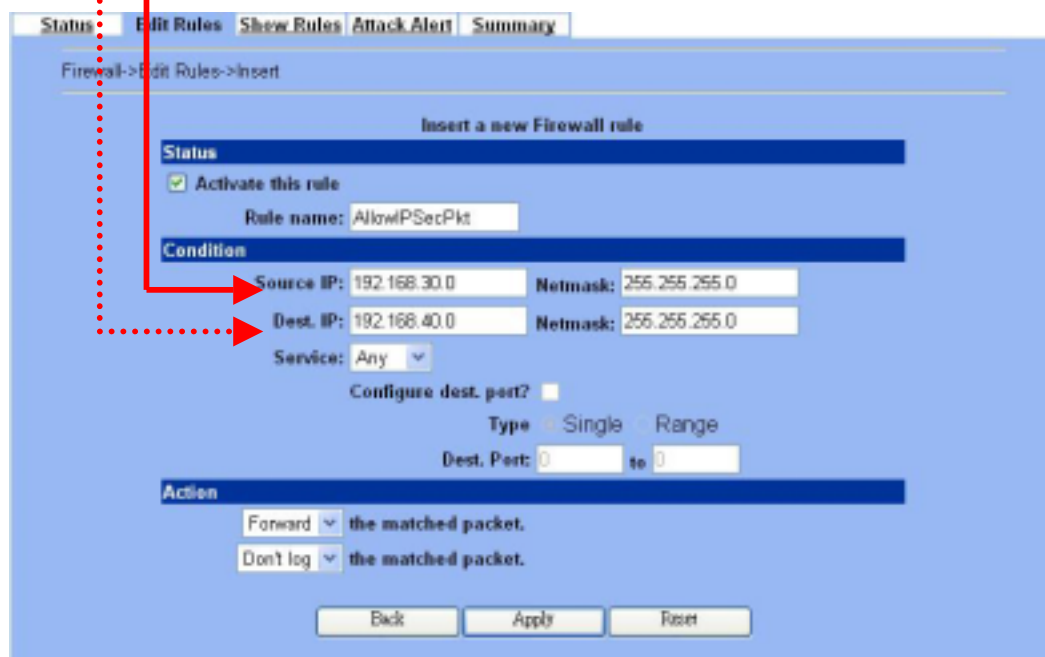


Figure 18-2 Insert a new firewall rule in WAN to LAN

6. When I try to login into the DFL-900, it showed up the following information, as the Figure 18-3 indicated, and couldn't login successfully.

Ans : It is because there is someone logging into the DFL-900 at the same time with the other IP address. Please logout the system from that IP address first and then login using your IP address again. You are definitely able to login into the DFL-900.

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-900 session timeout, and then you can login into DFL-900 again. The default timeout is 5 minutes in the System Tools/Admin Settings/Timeout. After session timeout happens, we could login DFL-900 another time.

- b. You can use supplied console to login into the DFL-900 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-900 from the same side.
- c. The final way is to power off the DFL-900, and then turn on the power. After DFL-900 reboot, you can login into DFL-900 again.

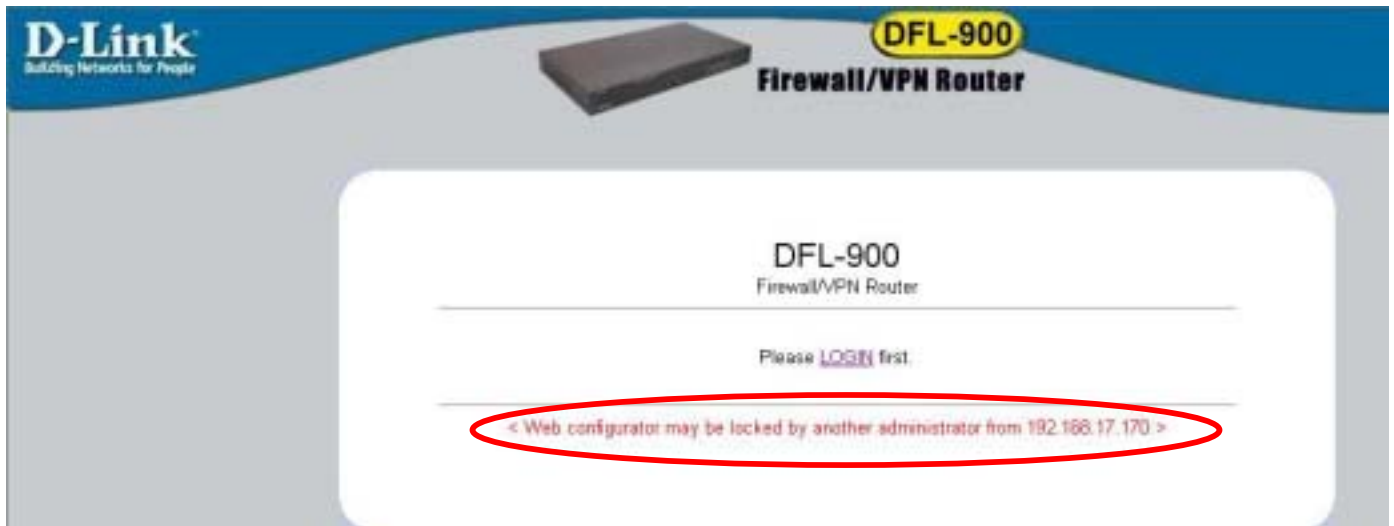


Figure 18-3 Login process is locked by the web configurator

7. Why does it always show the message as Figure 18-4 indicated when I try to enable bandwidth management feature of DFL-900?

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

Figure 18-4 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).

Appendix B

Glossary of Terms

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.

NAT (Network Address Translation) –

By the network address translation skill, we can transfer the internal network private address of DFL-900 to the public address for the Internet usage. By this method, we can use a large amount of private addresses in the enterprise.

Appendix C Customer Support

D-Link Offices

Australia	D-Link Australia 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: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au
Brazil	D-Link Brasil Ltda. 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: efreitas@dlink.cl
Canada	D-Link Canada 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: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
Chile	D-Link South America (Sudamérica) Isidora Goyenechea 2934 Of. 702, Las Condes Fono, 2323185, Santiago, Chile, S. A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl
China	D-Link China 15 th Floor, Science & Technology Tower, No. 11, Baishiqiao Road, Haidan District, 100081 Beijing, China TEL: 86-10-68467106 FAX: 86-10-68467110 URL: www.dlink.com.cn E-MAIL: liweii@digitalchina.com.cn
Denmark	D-Link Denmark Naverland Denmark, Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL: 45-43-969040 FAX: 45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk
Egypt	D-Link Middle East 7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt TEL: 202-245-6176 FAX: 202-245-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com
Finland	D-Link Finland Pakkalankuja 7A, FIN-0150 Vantaa, Finland TEL: 358-9-2707-5080 FAX: 358-9-2707-5081 URL: www.dlink-fi.com
France	D-Link France 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

E-MAIL: 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
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
- 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 & www.dlink.co.in
E-MAIL: service@dlink.india.com & 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 E-MAIL: 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 E-MAIL: 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 & www.dlink-benelux.be
E-MAIL: info@dlink-benelux.nl & 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
- 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
E-MAIL: 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 URL: 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 E-MAIL: 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 E-MAIL: 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 E-MAIL: 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**

4th 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, Fountain Valley, CA 92708-4160
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com