

D-Link DFL-900/1500

VPN/Firewall Router

User Manual

D-Link

Building Networks for People

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

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

DFL-900/1500 User Manual

Version 2.103

August 8, 2007

Trademarks

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

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

Table of Contents

| | | |
|------------------|---|-----------|
| Part I | Overview | 2 |
| | About this user manual | 3 |
| | What's New in Version 2.103? | 4 |
| Chapter 1 | Quick Start | 5 |
| 1.1 | Check Your Package Contents | 5 |
| 1.1.1 | DFL-900 | 5 |
| 1.1.2 | DFL-1500 | 5 |
| 1.2 | Hardware | 6 |
| 1.3 | Software Specifications | 8 |
| 1.4 | Five steps to configure DFL-900/1500 quickly | 10 |
| 1.5 | Wiring the DFL-900/1500 | 12 |
| 1.6 | Default Settings and architecture of DFL-900/1500 | 13 |
| 1.7 | Using the Setup Wizard | 15 |
| 1.8 | Internet Connectivity | 19 |
| 1.8.1 | LAN1-to-WAN1 Connectivity | 19 |
| 1.8.2 | WAN1-to-DMZ1 Connectivity | 21 |
| 1.9 | NAT/Router Mode and Transparent Mode | 23 |
| 1.9.1 | NAT/Router Mode | 23 |
| 1.9.2 | Transparent Mode | 23 |
| Chapter 2 | System Overview | 25 |
| 2.1 | Typical Example Topology | 25 |
| 2.2 | Changing the LAN1 IP Address | 26 |
| 2.2.1 | From LAN1 to configure DFL-1500 LAN1 network settings | 26 |
| 2.2.2 | From CLI (command line interface) to configure DFL-1500 LAN1 network settings | 27 |
| 2.3 | The design principle | 28 |
| 2.3.1 | Web GUI design principle | 28 |
| 2.3.2 | Rule principle | 28 |
| Part II | Basic Configuration | 32 |
| Chapter 3 | Basic Setup | 34 |
| 3.1 | Demands | 34 |
| 3.2 | Objectives | 34 |
| 3.3 | Methods | 34 |
| 3.4 | Steps | 35 |
| 3.4.1 | Setup WAN1 IP | 35 |
| 3.4.2 | Setup DMZ1, LAN1 Status | 36 |
| 3.4.3 | Setup WAN1 IP alias | 38 |
| Chapter 4 | System Tools | 41 |
| 4.1 | Demands | 41 |
| 4.2 | Objectives | 41 |
| 4.3 | Methods | 41 |
| 4.4 | Steps | 45 |
| 4.4.1 | General settings | 45 |

| | | |
|--|---|-----------|
| 4.4.2 | DDNS setting | 47 |
| 4.4.3 | DNS Proxy setting..... | 48 |
| 4.4.4 | DHCP Relay setting | 48 |
| 4.4.5 | SNMP Control..... | 49 |
| 4.4.6 | Change DFL-1500 interface..... | 50 |
| Chapter 5 Remote Management | | 51 |
| 5.1 | Demands | 51 |
| 5.2 | Methods | 51 |
| 5.3 | Remote Management Access Methods | 51 |
| 5.4 | Steps..... | 53 |
| 5.4.1 | Telnet..... | 53 |
| 5.4.2 | SSH | 53 |
| 5.4.3 | WWW | 53 |
| 5.4.4 | HTTPS..... | 54 |
| 5.4.5 | SNMP | 54 |
| 5.4.6 | ICMP..... | 54 |
| Chapter 6 Authentication | | 55 |
| 6.1 | Demands | 55 |
| 6.2 | Methods | 55 |
| 6.3 | Steps..... | 55 |
| 6.3.1 | Local Setting | 55 |
| 6.3.2 | Pop3(s) Setting | 56 |
| 6.3.3 | Imap(s) Setting | 57 |
| 6.3.4 | Radius Setting | 58 |
| 6.3.5 | LDAP Setting | 58 |
| 6.3.6 | Exempt Host..... | 59 |
| Part III NAT & Routing..... | | 60 |
| Chapter 7 NAT..... | | 61 |
| 7.1 | Demands | 61 |
| 7.2 | Objectives | 62 |
| 7.3 | Methods | 62 |
| 7.4 | Steps..... | 63 |
| 7.4.1 | Setup Many-to-one NAT rules | 63 |
| 7.4.2 | Setup Virtual Server for the FtpServer1 | 66 |
| 7.5 | NAT modes introduction | 69 |
| 7.5.1 | Many-to-One type | 69 |
| 7.5.2 | Many-to-Many type..... | 70 |
| 7.5.3 | One-to-One type..... | 70 |
| 7.5.4 | One-to-One (bidirectional) type | 71 |
| 7.5.5 | NAT modes & types..... | 71 |
| Chapter 8 Routing..... | | 73 |
| 8.1 | Demands | 73 |
| 8.2 | Objectives | 74 |
| 8.3 | Methods | 74 |
| 8.4 | Steps..... | 74 |
| 8.4.1 | Add a static routing entry | 74 |

| | | |
|-------------------|---|------------|
| 8.4.2 | Add a policy routing entry..... | 76 |
| 8.5 | The priority of the routing..... | 79 |
| Part IV | Firewall & IP/MAC Binding | 82 |
| Chapter 9 | IP/Services grouping..... | 83 |
| 9.1 | Demands | 83 |
| 9.2 | Objectives | 83 |
| 9.3 | Methods | 83 |
| 9.4 | Steps..... | 83 |
| 9.4.1 | Setup Address..... | 83 |
| 9.4.2 | Setup Service..... | 86 |
| 9.4.3 | Setup Schedule | 88 |
| Chapter 10 | Firewall | 91 |
| 10.1 | Demands | 91 |
| 10.2 | Objectives | 91 |
| 10.3 | Methods | 91 |
| 10.4 | Steps..... | 92 |
| 10.4.1 | Block internal PC session (LAN → WAN)..... | 92 |
| 10.4.2 | Setup Anti-DoS | 95 |
| Chapter 11 | IP/MAC Binding..... | 97 |
| 11.1 | Demands | 97 |
| 11.2 | Objectives | 97 |
| 11.3 | Methods | 97 |
| 11.4 | Steps..... | 97 |
| Part V | Virtual Private Network..... | 101 |
| Chapter 12 | VPN Technical Introduction | 102 |
| 12.1 | VPN benefit | 102 |
| 12.2 | Related Terminology Explanation | 102 |
| 12.2.1 | VPN..... | 102 |
| 12.2.2 | IPSec | 102 |
| 12.2.3 | Security Association..... | 102 |
| 12.2.4 | IPSec Algorithms | 102 |
| 12.2.5 | Key Management | 103 |
| 12.2.6 | Encapsulation | 104 |
| 12.2.7 | IPSec Protocols | 104 |
| 12.3 | Make VPN packets pass through DFL-1500 | 105 |
| Chapter 13 | Virtual Private Network – IPSec | 107 |
| 13.1 | Demands | 107 |
| 13.2 | Objectives | 107 |
| 13.3 | Methods | 107 |
| 13.4 | Steps..... | 108 |
| 13.4.1 | DES/MD5 IPSec tunnel: the IKE way | 108 |
| 13.4.2 | DES/MD5 IPSec tunnel: the Manual-Key way | 117 |
| Chapter 14 | Virtual Private Network –Dynamic IPSec | 125 |
| 14.1 | Demands | 125 |
| 14.2 | Objectives | 125 |

| | | |
|-------------------|---|------------|
| 14.3 | Methods | 125 |
| 14.4 | Steps..... | 125 |
| Chapter 15 | Virtual Private Network – Hub and Spoke VPN..... | 131 |
| 15.1 | Demands | 131 |
| 15.2 | Objectives | 131 |
| 15.3 | Methods | 131 |
| 15.4 | Steps..... | 131 |
| Chapter 16 | PPTP Client with PPTP Server | 137 |
| 16.1 | Demands | 137 |
| 16.2 | Objectives | 137 |
| 16.3 | Methods | 137 |
| 16.4 | Steps..... | 138 |
| Chapter 17 | Remote Access VPN – PPTP | 141 |
| 17.1 | Demands | 141 |
| 17.2 | Objectives | 141 |
| 17.3 | Methods | 141 |
| 17.4 | Steps..... | 142 |
| Chapter 18 | Remote Access VPN – L2TP | 145 |
| 18.1 | Demands | 145 |
| 18.2 | Objectives | 145 |
| 18.3 | Methods | 145 |
| 18.4 | Steps..... | 146 |
| 18.4.1 | Setup L2TP Network Server | 146 |
| Chapter 19 | Remote Access VPN – DS-601 VPN client..... | 149 |
| 19.1 | Demands | 149 |
| 19.2 | Objectives | 149 |
| 19.3 | Methods | 149 |
| 19.4 | Steps..... | 149 |
| Chapter 20 | Remote Access VPN – Windows client | 161 |
| 20.1 | Demands | 161 |
| 20.2 | Objects | 161 |
| 20.3 | Methods | 161 |
| 20.4 | Steps..... | 162 |
| 20.4.1 | DFL-1500 Setup | 162 |
| 20.4.2 | Create a custom MMC console..... | 164 |
| 20.4.3 | Create an IPSec policy..... | 167 |
| 20.4.4 | Add a filter rule from WinXP to DFL-1500 | 169 |
| 20.4.5 | Add a filter rule from DFL-1500 to WinXP | 172 |
| 20.4.6 | Configure a rule for WinXP client to DFL-1500..... | 174 |
| 20.4.7 | Configure a rule for DFL-1500 to WinXP client | 178 |
| 20.4.8 | Enable the security settings..... | 180 |
| Part VI | Content Filters | 181 |
| Chapter 21 | Content Filtering – Web Filters..... | 183 |
| 21.1 | Demands | 183 |
| 21.2 | Objectives | 184 |

| | | |
|-------------------|--|------------|
| 21.3 | Methods | 184 |
| 21.4 | Steps..... | 185 |
| 21.5 | Priority of web filter functions..... | 190 |
| Chapter 22 | Content Filtering – Mail Filters | 193 |
| 22.1 | Demands | 193 |
| 22.2 | Objectives | 193 |
| 22.3 | Methods | 193 |
| 22.4 | Steps..... | 194 |
| 22.4.1 | SMTP Filters | 194 |
| 22.4.2 | POP3 Filters | 195 |
| Chapter 23 | Content Filtering – FTP Filtering..... | 197 |
| 23.1 | Demands | 197 |
| 23.2 | Objectives | 197 |
| 23.3 | Methods | 197 |
| 23.4 | Steps..... | 198 |
| Part VII | Intrusion Detection System..... | 202 |
| Chapter 24 | Intrusion Detection Systems | 203 |
| 24.1 | Demands | 203 |
| 24.2 | Objectives | 203 |
| 24.3 | Methods | 203 |
| 24.4 | Steps..... | 204 |
| Part VIII | Load Balancer 、Bandwidth Management 、High Availability..... | 206 |
| Chapter 25 | Load Balancer | 207 |
| 25.1 | Demands | 207 |
| 25.2 | Objectives | 207 |
| 25.3 | Methods | 207 |
| 25.4 | Steps..... | 208 |
| 25.4.1 | Outbound Load Balancer..... | 208 |
| Chapter 26 | Bandwidth Management | 209 |
| 26.1 | Demands | 209 |
| 26.2 | Objectives | 210 |
| 26.3 | Methods | 211 |
| 26.4 | Steps..... | 212 |
| 26.4.1 | Inbound Traffic Management..... | 212 |
| 26.4.2 | Outbound Traffic Management | 217 |
| Chapter 27 | High Availability | 219 |
| 27.1 | Demands | 219 |
| 27.2 | Objectives | 219 |
| 27.3 | Methods | 220 |
| 27.4 | Steps..... | 220 |
| 27.4.1 | Setup High Availability..... | 220 |
| Part IX | System Maintenance..... | 222 |
| Chapter 28 | System Status | 223 |
| 28.1 | Demands | 223 |
| 28.2 | Objectives | 223 |

| | | |
|-------------------|---|------------|
| 28.3 | Methods | 223 |
| 28.4 | Steps..... | 223 |
| Chapter 29 | Log System | 227 |
| 29.1 | Demands | 227 |
| 29.2 | Objectives | 227 |
| 29.3 | Methods | 227 |
| 29.4 | Steps..... | 227 |
| 29.4.1 | System Logs | 227 |
| 29.4.2 | Syslog & Mail log | 228 |
| Chapter 30 | System Maintenance | 231 |
| 30.1 | Demands | 231 |
| 30.2 | Firmware upgrade from TFTP..... | 231 |
| 30.3 | Firmware upgrade from Web GUI..... | 232 |
| 30.4 | Database Update from Web GUI..... | 233 |
| 30.5 | Factory Reset | 234 |
| 30.5.1 | Factory reset under web GUI | 234 |
| 30.5.2 | NORMAL factory reset..... | 235 |
| 30.5.3 | EMERGENT factory reset | 235 |
| 30.6 | Save the current configuration..... | 236 |
| 30.7 | Backup / Restore Configurations | 236 |
| 30.8 | Reset password | 237 |
| Appendix | | 238 |
| Appendix A | Command Line Interface (CLI) | 239 |
| A.1 | Enable the port of DFL-1500..... | 239 |
| A.2 | CLI commands list (Normal Mode) | 239 |
| A.3 | CLI commands list (Rescue Mode) | 241 |
| Appendix B | Trouble Shooting..... | 243 |
| Appendix C | Rule entry limitation | 249 |
| Appendix D | System Log Syntax..... | 251 |
| Appendix E | Glossary of Terms | 257 |
| Appendix F | Index | 259 |
| Appendix G | Customer Support..... | 261 |

Part I

Overview

About this user manual

This user manual provides information about installing and configuring your DFL-900/1500 VPN/Firewall Router using its built-in web browser interface (WBI) and command line interface (CLI). This guide is primarily for network and security personnel who configure the VPN/Firewall Router and monitor networks for evidence of intrusion attempts and inappropriate transmission of regulated information. The WBI is a versatile, configurable monitoring platform. For you to understand and use its functionality, you must understand the WBI and its capabilities.

All the examples after Chapter 2 in this manual, which instruct you how to configure the VPN/Firewall Router, are taken from DFL-1500. The hardware and software specification of the DFL-900 and DFL-1500 will be introduced in Chapter 1. You can refer the examples to configure your VPN/Firewall Router. Before you start to configure your VPN/Firewall Router, please view the specification in Section 1.3 and default settings in Section 1.6 first. That will help you to quick your configuration and save you time.

What's New in Version 2.103?

This section describes the enhancements that were made to DFL-900/1500 as compared to the previous version. It includes changes to the way that the DFL-900/1500 operates, some of which are reflected by changes to the WBI and others that were made to the DFL-900/1500 engine to improve performance and accuracy. As compared to the previous version, version 2.103 provides the following additional improvements:

- **WAN Load Balancer**

The WAN load balancer module consists of outbound load balancing and inbound load balancing. Users may want to subscribe multiple WAN links and make their outbound traffic load-balanced among the WAN links. DFL-1500 now supports outbound WAN load balancing. Inbound load balancing will be supported in a very near future.

Chapter 1

Quick Start

This chapter introduces how to quick setup the DFL-900/1500.

DFL-900/1500 VPN/Firewall Router is an integrated all-in-one solution that can facilitate the maximum security and the best resource utilization for the enterprises. It contains a high-performance stateful packet inspection (SPI) **Firewall**, policy-based **NAT**, ASIC-based wire-speed **VPN**, upgradeable **Intrusion Detection System**, **Dynamic Routing**, **Content Filtering**, **Bandwidth Management**, **High Availability** and other solutions in a single box. It is one of the most cost-effective all-in-one solutions for enterprises.

1.1 Check Your Package Contents

1.1.1 DFL-900

These are the items included with your DFL-900 purchase as Figure 1-2. They are the following items

1. DFL-900 Device * 1
2. Ethernet cable (RJ-45) * 2
3. RS-232 console * 1
4. CD (include User's manual and Quick Guide) * 1
5. Power cord * 1



Figure 1-1 All items in the DFL-900 package

1.1.2 DFL-1500

These are the items included with your DFL-1500 purchase as Figure 1-2. They are the following items

1. DFL-1500 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 cord * 1



Figure 1-2 All items in the DFL-1500 package

1.2 Hardware

| Feature | DFL-900 | DFL-1500 |
|------------------------------|---|--|
| Chassis | | |
| Dimensions | <ul style="list-style-type: none"> • Rack mount 1U size • 146 mm (H) x 275 mm (D) x 203 mm (W)(8"*5.75"*10") | <ul style="list-style-type: none"> • Rack mount 1U size • 146 mm (H) x 275 mm (D) x 203 mm (W)(8"*5.75"*10") |
| Look & feel | D-Link style | D-Link style |
| Key Components | | |
| CPU | Intel Celeron 850 MHZ | Intel Celeron 1.2G |
| Memory | 256MB 168-P SDRAM | 256MB 168-P SDRAM |
| 10/100M Ethernet MAC and PHY | RTL 8139C+ | Intel I82559 |
| PCI bridge | Intel 815E | Intel FW82801BA |
| FLASH memory | 32MB (San Disk) | 32MB (San Disk) |
| Memory control HUB | -- | FW82815EP |
| Hardware monitor | -- | Super I/O hardware monitor IT8712F-A |
| Security processor | -- | Safenet 1141 (VPN accelerator board) |
| Port functions | | |
| WAN port | <ul style="list-style-type: none"> • 1 port for connecting to outbound WAN • RJ-45 connector • IEEE 802.3 compliance • IEEE 802.3u compliance • Support Half/Full-Duplex operations • Support backpressure at Half-Duplex operation. • IEEE 802.3x Flow Control support for Full-Duplex mode | <ul style="list-style-type: none"> • 2 ports for connecting to outbound WAN • RJ-45 connector • IEEE 802.3 compliance • IEEE 802.3u compliance • Support Half/Full-Duplex operations • Support backpressure at Half-Duplex operation. • IEEE 802.3x Flow Control support for Full-Duplex mode |

| | | |
|-------------------------------------|---|--|
| LAN port | <ul style="list-style-type: none"> ● 1 port for connecting inbound LAN ● RJ-45 connector ● IEEE 802.3 compliance ● IEEE 802.3u compliance ● Support Half/Full-Duplex operations ● Support backpressure at Half-Duplex operation. ● IEEE 802.3x Flow Control support for Full-Duplex mode | <ul style="list-style-type: none"> ● 2 ports for connecting inbound LAN ● RJ-45 connector ● IEEE 802.3 compliance ● IEEE 802.3u compliance ● Support Half/Full-Duplex operations ● Support backpressure at Half-Duplex operation. ● IEEE 802.3x Flow Control support for Full-Duplex mode |
| DMZ port | <ul style="list-style-type: none"> ● 1 port for connecting to server. ● RJ-45 connector ● IEEE 802.3 compliance ● IEEE 802.3u compliance ● Support Half/Full-Duplex operations ● Support backpressure at Half-Duplex operation. ● IEEE 802.3x Flow Control support for Full-Duplex mode | <ul style="list-style-type: none"> ● 1 port for connecting to server. ● RJ-45 connector ● IEEE 802.3 compliance ● IEEE 802.3u compliance ● Support Half/Full-Duplex operations ● Support backpressure at Half-Duplex operation. ● IEEE 802.3x Flow Control support for Full-Duplex mode |
| Console port | <ul style="list-style-type: none"> ● DB-9 male connector ● Asynchronous serial DTE with full modem controls ● No hardware handshaking such as RTS/CTS | <ul style="list-style-type: none"> ● DB-9 male connector ● Asynchronous serial DTE with full modem controls |
| LED indication | <ul style="list-style-type: none"> ● Power, Solid Orange – System ready ● Blinking Green – System under power-on self test <p>Ethernet 10/100M Per ports:</p> <ul style="list-style-type: none"> ● Link/ACT LED Off – No Link Solid Green – Link Blinking Green – Activity | <ul style="list-style-type: none"> ● Power, Solid Orange – System ready ● Blinking Green – System under power-on self test <p>Ethernet 10/100M Per ports:</p> <ul style="list-style-type: none"> ● Link/ACT LED Off – No Link Solid Green – Link Blinking Green – Activity |
| Power | | |
| Power supply | AT PS, AC 90~230 V full range @ 45~63 Hz | AT PS, AC 90~230 V full range @ 45~63 Hz |
| Power dissipation | 180 W | 180 W |
| Environmental Specifications | | |
| Operating Temperature | 0 ~ 60°C | 0 ~ 60°C |
| Storage Temperature | -25~70°C | -25~70°C |
| Operating Humidity | 5% - 95% non-condensing | 5% - 95% non-condensing |
| EMC and Safety Certification | | |
| EMC Approval | FCC class A VCCI class A CE class A C-Tick class A | FCC class A VCCI class A CE class A C-Tick class A |
| Safety Approval | UL | UL |

| | | |
|--|-------------------------|-------------------------|
| | CSA TUV/GS T-mark | CSA TUV/GS T-mark |
|--|-------------------------|-------------------------|

Table 1-1 DFL-900/1500 Hardware

1.3 Software Specifications

| Product | | DFL VPN/Firewall Router | |
|--------------------------|-----------------|-------------------------|----------|
| Model | | DFL-900 | DFL-1500 |
| Features | | | |
| Basic Setup | | | |
| Wizard | | ✓ | ✓ |
| Transparent Mode | | ✓ | ✓ |
| WAN Settings | WAN1 IP | ✓ (no default WAN Link) | ✓ |
| | WAN2 IP | ✗ | ✓ |
| | IP Alias | ✓ | ✓ |
| LAN Settings | LAN1 Status | ✓ | ✓ |
| | LAN2 Status | ✗ | ✓ |
| | IP Alias | ✓ | ✓ |
| DMZ Settings | DMZ1 Status | ✓ | ✓ |
| | IP Alias | ✓ | ✓ |
| Books | Address | ✓ | ✓ |
| | Service | ✓ | ✓ |
| | Schedule | ✓ | ✓ |
| Authentication | Local | ✓ | ✓ |
| | POP3 | ✓ | ✓ |
| | IMAPs | ✓ | ✓ |
| | Radius | ✓ | ✓ |
| | LDAP | ✓ | ✓ |
| Advanced Settings | | ✓ | ✓ |
| VPN Settings | IPSec | ✓ | ✓ |
| | VPN Hub | ✓ | ✓ |
| | VPN Spoke | ✓ | ✓ |
| | PPTP | ✓ | ✓ |
| | L2TP | ✓ | ✓ |
| | Pass Through | ✓ | ✓ |
| NAT | NAT Rule | ✓ | ✓ |
| | Virtual Servers | ✓ | ✓ |
| Routing | Static Route | ✓ | ✓ |
| | Policy Route | ✓ | ✓ |
| Firewall | Firewall Rule | ✓ | ✓ |

| | | | |
|----------------------|----------------------------|---|---|
| | Anti-DoS | ✓ | ✓ |
| Content Filters | Web Filter | ✓ | ✓ |
| | Mail Filter | ✓ | ✓ |
| | FTP Filter | ✓ | ✓ |
| IDS | IDS | ✓ | ✓ |
| Bandwidth Management | Edit Actions | ✓ | ✓ |
| IP/MAC Binding | Binding | ✓ | ✓ |
| | Allow Range | ✓ | ✓ |
| Load Balancer | Outbound Wan Load Balancer | ✗ | ✓ |
| High Availability | High Availability | ✗ | ✓ |
| System Tools | | ✓ | ✓ |
| Admin Settings | General | ✓ | ✓ |
| | DDNS | ✓ | ✓ |
| | DNS Proxy | ✓ | ✓ |
| | DHCP Relay | ✓ | ✓ |
| | Password | ✓ | ✓ |
| | Time/Date | ✓ | ✓ |
| | Timeout | ✓ | ✓ |
| | Interface | ✗ | ✓ |
| System Utilities | Save Configuration | ✓ | ✓ |
| | Backup Configuration | ✓ | ✓ |
| | Restore Configuration | ✓ | ✓ |
| | Factory Reset | ✓ | ✓ |
| Firmware Upgrade | Firmware Upgrade | ✓ | ✓ |
| Remote Management | TELNET | ✓ | ✓ |
| | SSH | ✓ | ✓ |
| | WWW | ✓ | ✓ |
| | HTTPS | ✓ | ✓ |
| | SNMP | ✓ | ✓ |
| | MISC (ICMP) | ✓ | ✓ |
| SNMP Control | SNMP Control | ✓ | ✓ |
| Database Update | Database Update | ✓ | ✓ |
| Device Status | | ✓ | ✓ |
| System Status | System Status | ✓ | ✓ |
| | Network Status | ✓ | ✓ |
| | CPU & Memory | ✓ | ✓ |
| | DHCP Table | ✓ | ✓ |
| | Routing Table | ✓ | ✓ |
| | Active Sessions | ✓ | ✓ |
| | Top 20 Sessions | ✓ | ✓ |
| | IPSec Sessions | ✓ | ✓ |
| Log Config | Syslog Server | ✓ | ✓ |
| | Mail Logs | ✓ | ✓ |

Part I Overview

| | | | |
|---------------------|-------------------------|---|---|
| System Logs | System Access logs | ✓ | ✓ |
| | Firewall Logs | ✓ | ✓ |
| | Anti-DoS Logs | ✓ | ✓ |
| IDS Logs | IDS Logs | ✓ | ✓ |
| Content Filter Logs | Web Filter Logs | ✓ | ✓ |
| | Mail Filter Logs | ✓ | ✓ |
| | FTP Filter Logs | ✓ | ✓ |
| VPN Logs | IPSec Logs - IKE | ✓ | ✓ |
| | IPSec Logs - Manual Key | ✓ | ✓ |
| | PPTP Logs - Server | ✓ | ✓ |
| | PPTP Logs - Client | ✓ | ✓ |
| | L2TP Logs | ✓ | ✓ |

Table 1-2 The specification comparison of the DFL-900/1500

1.4 Five steps to configure DFL-900/1500 quickly

Let's look at the common network topology without DFL-900/1500 applying like Figure 1-3. This is a topology which is almost used by all the small/medium business or SOHO use as their internet connectivity. Although that your topology is not necessarily the same diagram below, but it still can give you a guideline to configure DFL-900/1500 quickly.

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

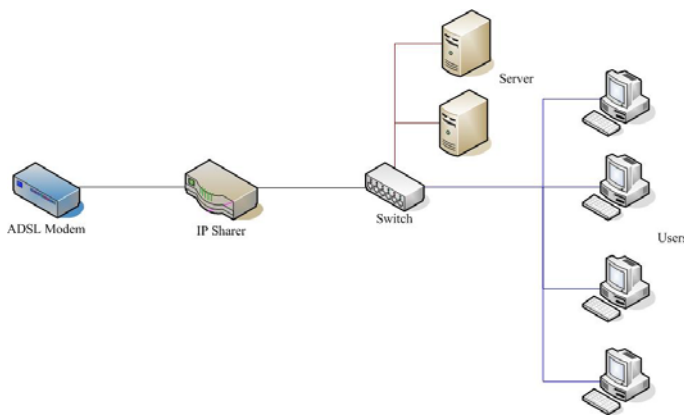


Figure 1-3 The example before DFL-900/1500 applies on it

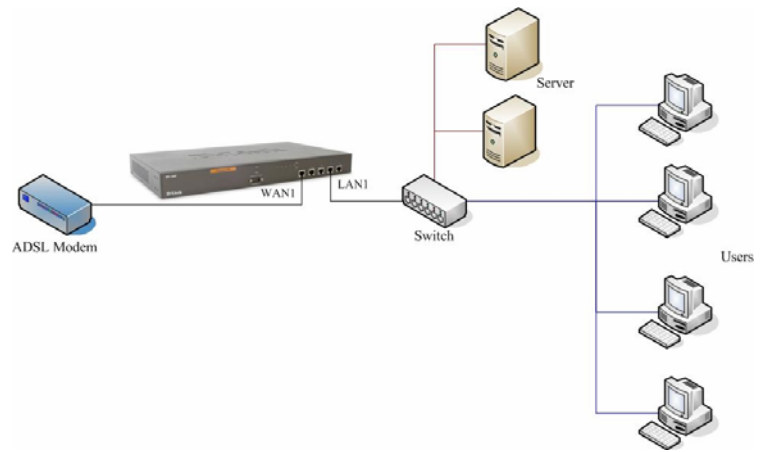


Figure 1-4 The example after DFL-900/1500 applies on it

Here we would like to alter the original IP Sharer with the DFL-900/1500 like Figure 1-4. If we hope to have DFL-900/1500 to replace the IP Sharer, we just need to simply execute the following five steps as Figure 1-5 showed. By these steps, we hope to build an image to tell you how to let DFL-900/1500 work basically.

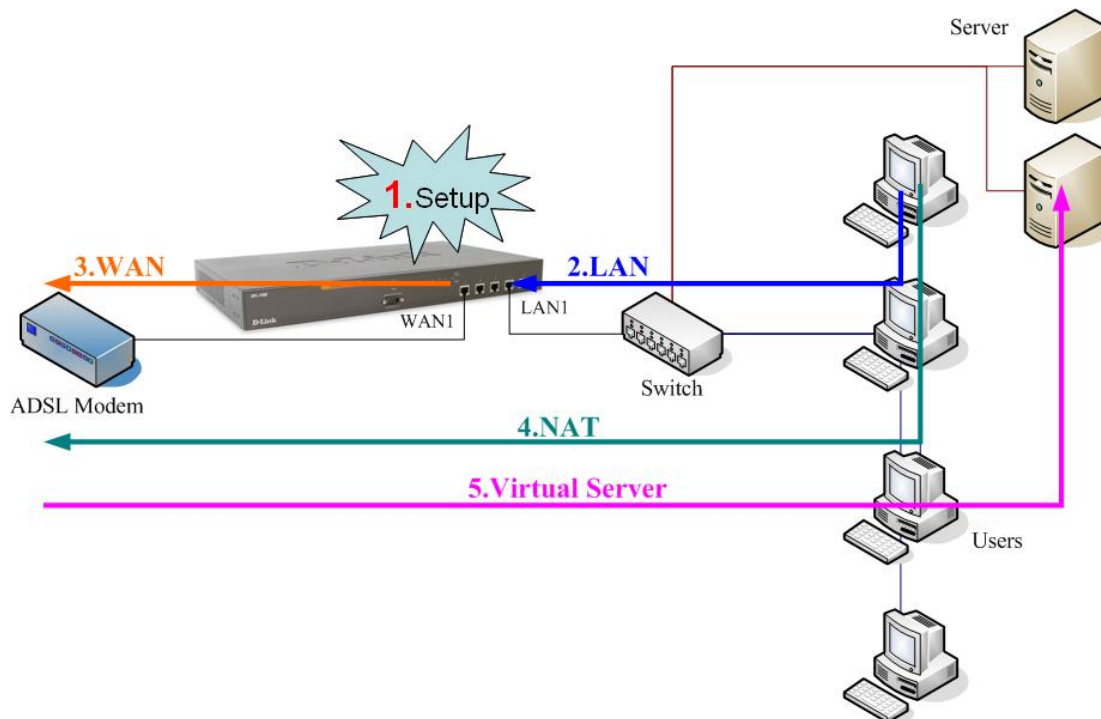


Figure 1-5 Five steps to configure DFL-900/1500

As the Figure 1-5 illustrated, with the five-step configurations, DFL-900/1500 will have the same functions with the original IP Sharer. Please see the following description of the five-step configurations.

Step 1. Setup:

Install three physical lines inclusive of the power cord, outbound link (connected WAN1 port) and inbound direction (connected LAN1 port). For the details, please refer section 1.5.

Continually, we will connect to the web GUI of DFL-900/1500. So you must make sure that you have a PC which is located in the same subnet with DFL-900/1500 before this step. Note: The default LAN1 port is (192.168.1.254 / 255.255.255.0). Refer to Table 1-3 for the default settings and section 1.7 for more information.

Step 2. LAN:

Configure the LAN1 port of DFL-900/1500. You can refer to section 1.6 for the default network configurations of DFL-900/1500. Note: If you were connected from LAN1 port and changed the LAN1 IP address settings of DFL-900/1500. The network will be disconnected since the IP address is different between your pc and DFL-900/1500 LAN1 port.

Step 3. WAN:

Configure the WAN1 port of DFL-900/1500. You can refer to section 1.6 for the default network configurations of DFL-900/1500.

Step 4. NAT:

Configure the connection of LAN to WAN direction. It will make all the client pc access the internet through DFL-900/1500. For more information, please refer to section 1.8.1.

Step 5. Virtual Server:

If there is any server located inside the DFL-900/1500. You may hope these servers can provide services outside. So you should configure the Virtual Server which provides connections of WAN to LAN direction. For more information, please refer to section 1.8.2.

After you completely finished the above steps, the connectivity function of DFL-900/1500 is probably well-done.

1.5 Wiring the DFL-900/1500

- A.** First, connect the power cord to the socket at the back panel of the DFL-900/1500 as in Figure 1-6, Figure 1-7 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 1-6 Back panel of the DFL-900



Figure 1-7 Back panel of the DFL-1500

- B.** Using an Ethernet cable, insert one end of the cable to the WAN port on the front panel of the DFL-900/1500 and the other end of the cable to a DSL or Cable modem, as in Figure 1-8, Figure 1-9.
- 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 1-8, Figure 1-9.
- D.** Computers that act as servers to provide Internet services should be connected to the DMZ port using an Ethernet Cable, as in Figure 1-8, Figure 1-9.

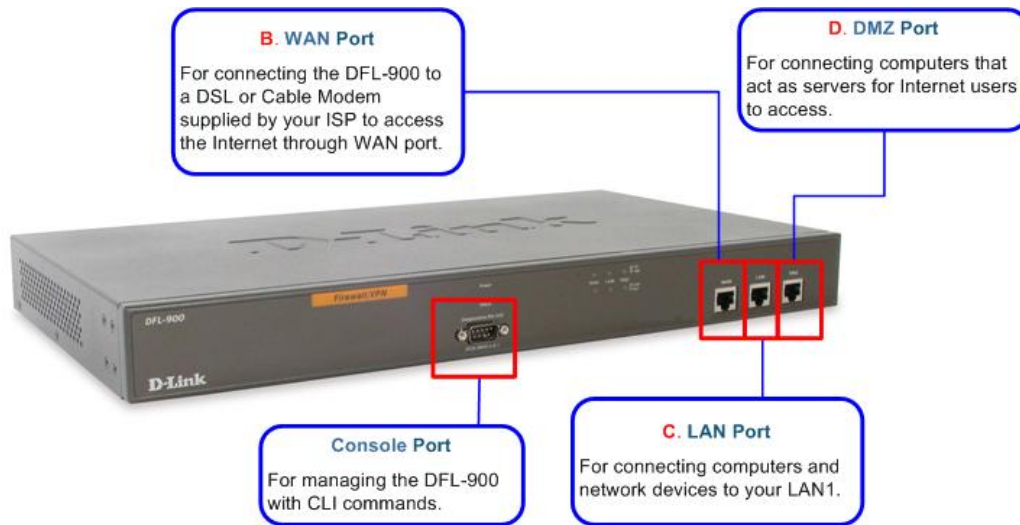


Figure 1-8 Front end of the DFL-900

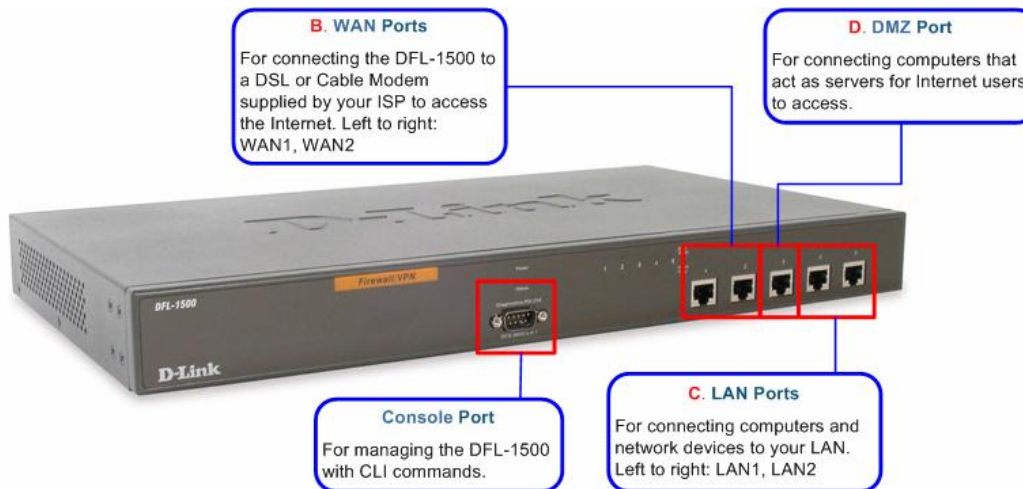


Figure 1-9 Front end of the DFL-1500

1.6 Default Settings and architecture of DFL-900/1500

You should have an Internet account already set up and have been given most of the following information as Table 1-3. Fill out this table when you edit the web configuration of DFL-900/1500. DFL-900 has three ports inclusive of the WAN1 (port1), LAN1 (port2) and DMZ1 (port3) while DFL-1500 has five ports inclusive of the WAN1 (port1), WAN2 (port2), DMZ1 (port3), LAN1 (port4), and LAN2 (port5).

| Items | | | DFL-900 | | DFL-1500 | |
|------------------|----------|-------------|-----------------|-----------|-----------------|-----------|
| | | | Default value | New value | Default value | New value |
| Password: | | | admin | | admin | |
| WAN1 | Fixed IP | IP Address | Not initialized | _____ | Not initialized | _____ |
| | | Subnet Mask | | _____ | | _____ |
| | | Gateway IP | | _____ | | _____ |

Part I
Overview

| | | | | | | |
|------|----------------|----------------|-------|-----------------|-------|-------|
| | | Primary DNS | | _____ | | _____ |
| | | Secondary DNS | | _____ | | _____ |
| | PPPoE | PPPoE Username | | _____ | | _____ |
| | | PPPoE Password | | _____ | | _____ |
| | DHCP | | | | | |
| WAN2 | Fixed IP | IP Address | N/A | Not initialized | _____ | |
| | | Subnet Mask | | | _____ | |
| | | Gateway IP | | | _____ | |
| | | Primary DNS | | | _____ | |
| | | Secondary DNS | | | _____ | |
| | PPPoE | PPPoE Username | | | _____ | |
| | | PPPoE Password | | | _____ | |
| | DHCP | | | | | |
| DMZ1 | IP Address | 10.1.1.254 | _____ | 10.1.1.254 | _____ | |
| | IP Subnet Mask | 255.255.255.0 | _____ | 255.255.255.0 | _____ | |
| LAN1 | IP Address | 192.168.1.254 | _____ | 192.168.1.254 | _____ | |
| | IP Subnet Mask | 255.255.255.0 | _____ | 255.255.255.0 | _____ | |
| LAN2 | IP Address | N/A | | 192.168.2.254 | _____ | |
| | IP Subnet Mask | | | 255.255.255.0 | _____ | |

Table 1-3 DFL-900/1500 related network settings

Organization_1

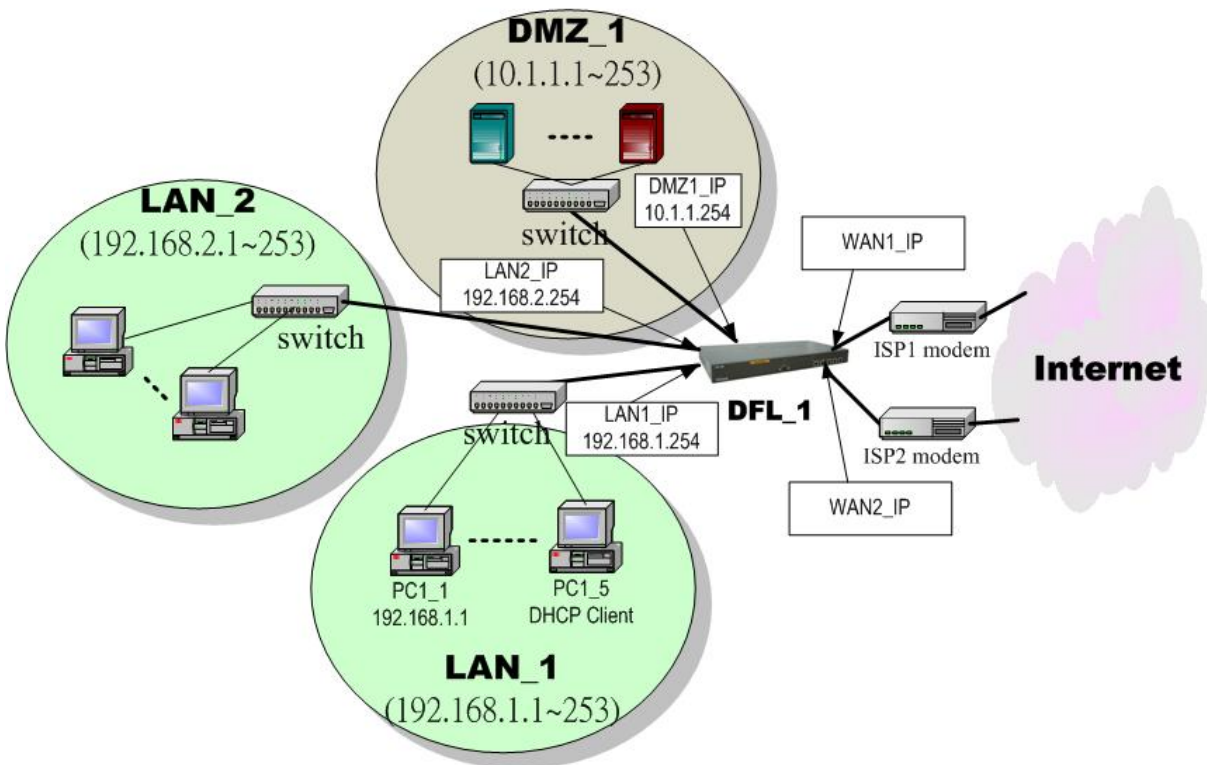

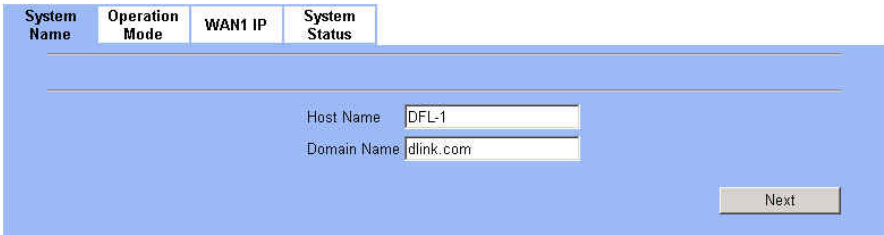
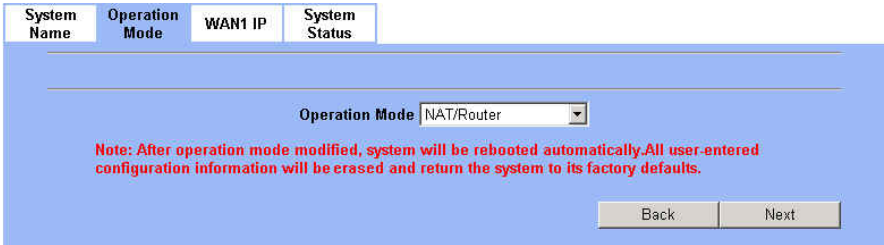


Figure 1-10 The default settings of DFL-1500

As the above diagram Figure 1-10 illustrated, this diagram shows the default topology of DFL-1500. And you can configure the DFL-1500 by connecting to the LAN1_IP (192.168.1.254) from the PC1_1 (192.168.1.1). In the following sections, we will teach you how to quickly setup the DFL-1500 in the basic appliances. We are going to introduce you how to configure the VPN/Firewall Router by the example of the DFL-1500 in this document. It is the same way to configure the DFL-900. For the related software specification, please refer to Table 1-2.

1.7 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-900/1500 in order to be able to make an HTTPS connection using a web browser. The DFL-900/1500 is assigned an IP address of 192.168.1.254 with a Subnet Mask of 255.255.255.0 by default. The computer that will be used to configure the DFL-900/1500 must be assigned an IP address between 192.168.1.1 and 192.168.1.253 with a Subnet Mask of 255.255.255.0 to be able to connect to the DFL-900/1500. This address range can be changed later. There are instructions in the DFL-900/1500 Quick Installation 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>Note: Please do not access web UI through proxy, or the login may be locked by others or the original user.</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>BASIC SETUP > Wizard</p> <p>Welcome to the DFL-1500 Web-Based Configuration !</p> <p>Basic Setup Connect to the Internet and configure your Intranet with the Setup Wizard (WAN, LAN and DMZ settings, routing protocol and DHCP server settings).</p> <p>Advanced Settings Access advanced features, including IPSec/L2TP/PPTP VPNs, VPN pass through, NAT, virtual servers, static/policy route, firewall, attack alert, web/mail/ftp filters, intrusion detection, and bandwidth management.</p> <p>System Tools Setup DDNS, DNS proxy, DHCP relay, system password/time/date/timeouts, protocol services, interface types, perform firmware upgrade, save running configurations, backup/restore configurations, reset to factory defaults, customize remote management and SNMP, schedule database update.</p> <p>Device Status Display system name, firmware version, interface IP settings, network status, CPU/memory utilization, DHCP/Routing table, active/top20/IPSec sessions. Setup logging systems, including system/firewall/IDS/content-filter/VPN logs.</p> <p>Help Get help about your VPN/Firewall Router.</p> <p>Setup Wizard A step-by-step setup wizard will guide you to configure your VPN/Firewall Router to connect to your ISP (Internet Service Provider).</p> <p>Run 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>  |
| <p>Step 4. Operation Mode</p> <p>DFL-1500 VPN/Firewall Router can operate in NAT/Router mode or Transparent mode. Choose which operation Mode for this device to use.</p> | <p>BASIC SETUP > Wizard > Next</p>  |

| | |
|-----------------------|--|
| <p>NAT/Route mode</p> | <p>In NAT/Route mode, you can create NAT mode rules and Route mode rules. For the related information, please refer to Chapter 7 and Chapter 8.</p> <ul style="list-style-type: none"> NAT mode rules use network address translation to hide the addresses in a more secure network from users in a less secure network. Route mode rules accept or deny connections between networks without performing address translation. |
|-----------------------|--|

| | |
|-------------------------|--|
| <p>Transparent mode</p> | <p>Transparent mode provides the same basic protection as NAT mode. Packets received by the DFL-900/1500 are intelligently forwarded or blocked according to firewall rules. The DFL-900/1500 can be inserted in your network at any point without the need to make any changes to your network or any of its components. However, VPN, NAT, Routing and some advanced firewall features (such as Authentication, IP/MAC Binding) are only available in NAT/Route mode.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. You cannot connect the LAN1/LAN2/DMZ interfaces to the same Hub while using Transparent mode, otherwise the traffic from the PCs under LAN1/LAN2/DMZ interfaces may be blocked. 2. If you would like to change the operation mode from NAT/Route mode to Transparent mode, you have to backup the configuration file and then do the factory reset first. 3. If the DFL-900/1500 is regarded as a proxy server when you enable content filter, etc. in the transparent mode, you should assign a public IP (WAN IP) and the gateway IP to it in order for the device to access the internet. |
|-------------------------|--|

Table 1-4 The operation mode

| | |
|---|--|
| <p>Step 5. WAN Connectivity</p> <p>Choose the type of IP Address Assignment provided by your ISP to access the Internet. Here we have four types to select. This will determine how the IP address of WAN1 is obtained. Click Next to proceed.</p> <p>Note that some features of the DFL-1500 (such as Virtual Server, VPN, Content Filter, and IDS) can only be available while using Default WAN link.</p> | <p>BASIC SETUP > Wizard > Next > WAN1 IP</p> |
| <p>Step 5.a — DHCP client</p> <p>If Get IP Automatically (DHCP) is selected, DFL-1500 will request for IP address, netmask, and DNS servers from your ISP. You can use your preferred DNS by clicking the DNS IP Address and then completing the Primary DNS and Secondary DNS server IP addresses. Click Next to proceed.</p> | <p>BASIC SETUP > Wizard > Next > DHCP</p> |

Step 5.b — Fixed IP

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

BASIC SETUP > Wizard > Next > Fixed IP

| System Name | Operation Mode | WAN1 IP | System Status |
|---|----------------|---------|---------------|
| <p>IP Address Assignment: Fixed IP Address</p> <p><input checked="" type="checkbox"/> Default WAN link (Gateway/DNS)</p> <p>IP Address: 61.2.1.1 Subnet Mask: 255.255.255.248</p> <p>Gateway IP: 61.2.1.6</p> <p><input type="radio"/> DNS IP Address</p> <p>Primary DNS: 168.95.1.1</p> <p>Secondary DNS: 0.0.0.0</p> <p>Routing Protocol: None</p> <p>OSPF Area ID: </p> <p>Back Next</p> | | | |

Step 5.c — PPPoE client

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

BASIC SETUP > Wizard > Next > PPPoE

| System Name | Operation Mode | WAN1 IP | System Status |
|---|----------------|---------|---------------|
| <p>IP Address Assignment: PPP over Ethernet</p> <p><input checked="" type="checkbox"/> Default WAN link (Gateway/DNS)</p> <p>Service Name: (Optional)</p> <p>User Name: Hey</p> <p>Password: *****</p> <p><input type="radio"/> Get DNS Automatically</p> <p><input checked="" type="radio"/> DNS IP Address</p> <p>Primary DNS: 168.95.192.1</p> <p>Secondary DNS: 168.95.1.1</p> <p>Disconnected</p> <p>Back Next</p> | | | |



✓ **Warning Message**

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

Step 6. System Status

Here we select **Fixed IP** method in WAN1 port. Then the DFL-1500 provides a short summary of the system. Please check if anything mentioned above is properly set into the system. Click **Finish** to close the wizard.

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

| System Name | Operation Mode | WAN1 IP | System Status |
|---|----------------------------------|-------------------------------------|---------------|
| System Name: DFL-1500.dlink.com | | | |
| Firmware Version: NetOS Ver2.001 (WALL) #5: Thu Sep 23 15:26:41 CST 2004 | | | |
| Software Serial Number: 60623576436830003320 | | | |
| Operation Mode: NAT/Router | | | |
| Default gateway: 61.2.1.6 | | | |
| Primary DNS: 168.95.1.1 | | | |
| Secondary DNS: | | | |
| Port1: WAN1 (Static IP)[Default] | IP Address: 61.2.1.1 | Subnet Mask: 255.255.255.248 | |
| Port2: WAN2 (Not initialized) | IP Address: not set | | |
| Port3: DMZ1 | IP Address: 10.1.1.254 | Subnet Mask: 255.255.255.0 | |
| Port4: LAN1 | IP Address: 192.168.1.254 | Subnet Mask: 255.255.255.0 | |
| Port5: LAN2 | IP Address: 192.168.2.254 | Subnet Mask: 255.255.255.0 | |

Back **Finish**

1.8 Internet Connectivity

After setting up DFL-1500 with the wizard, DFL-1500 can connect to the ISP. In this chapter, we introduce **LAN1-to-WAN1** Connectivity to explain how the computers under LAN1 can access the Internet at WAN1 through DFL-1500. Subsequently, we introduce **WAN1-to-DMZ1** Connectivity to explain how the servers under DMZ1 can be accessed by the LAN1 users and other Internet users on the WAN1 side.

You MUST press Apply to proceed to the next page. Go to System Tools > System Utilities > Save Configuration to save the configuration. Once applying any changes, the settings are immediately updated into the flash memory.

1.8.1 LAN1-to-WAN1 Connectivity

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

Step 1. Device IP Address
Setup the IP Address and IP Subnet Mask for the DFL-1500.

Step 2. Client IP Range
Enable the DHCP server if you want to use DFL-1500 to lease IP addresses to LAN PCs. Specify the Pool Starting Address, Pool Size, Primary DNS, and Secondary DNS that will be assigned to them.
Example: in the figure, the DFL-1500 will assign one IP address from 192.168.1.100 ~ 192.168.1.119, together with the DNS server 192.168.1.254, to the LAN1 PC that requests for an IP address.

Step 3. Apply the Changes
Click Apply to save. Now you can enable the DHCP clients on your LAN1 PCs to get an IP.

Step 4. Check NAT Status
The default setting of NAT is in Basic Mode. After completing Step 3, the NAT is automatically configured related rules to let all private-IP LAN/DMZ-to-WAN requests to be translated with the public IP assigned by the ISP.

Step 5. Check NAT Rules
The DFL-1500 has added the NAT rules as the right diagram. The rule Basic-LAN1 means that, when matching the condition (requests of LAN/DMZ-to-WAN direction with its source IP falling in the range of 192.168.1.254 / 255.255.255.0), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.

BASIC SETUP > LAN Settings > LAN1 Status

LAN1 Status **LAN2 Status** IP Alias

LAN1 TCP/IP
IP Address: 192.168.1.254 IP Subnet Mask: 255.255.255.0

DHCP Setup

Enable DHCP Server

IP Pool Starting Address: 192.168.1.100
Pool Size(max size: 253): 20
Primary DNS Server: 192.168.1.254
Secondary DNS Server: 0.0.0.0
Lease time(sec): 7200

Routing Protocol: None
OSPF Area ID:

Apply

Note: The IP Pool Starting Address must be on the same subnet specified in the IP Address and the IP Subnet Mask field. For example, the addresses given by the 192.168.1.100 with a pool size of 20 (192.168.1.100 ~ 192.168.1.119) are all within the same range of 192.168.1.254 / 255.255.255.0

ADVANCED SETTINGS > NAT > Status

Status **NAT Rules** Virtual Servers

Network Address Translation Mode: Basic

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

- Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports.
Reset NAT rules
- External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports.
Reset Server rules

Modes:

- None: The DFL-1500 is in routing mode without performing any address translation.
- Basic: The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
- Full Feature: The DFL-1500 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

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

Apply

ADVANCED SETTINGS > NAT > NAT Rules

Status **NAT Rules** Virtual Servers

NAT->Edit Rules

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

1.8.2 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-1500 of the DMZ1 interface.</p> | <p>BASIC SETUP > DMZ Settings > DMZ1 Status</p> <p>DMZ1 Status IP Alias</p> <p>DMZ1 TCP/IP</p> <p>IP Address: 10.1.1.254 IP Subnet Mask: 255.255.255.0</p> <p>DHCP Setup</p> <p><input checked="" type="checkbox"/> Enable DHCP Server</p> <p>IP Pool Starting Address: 10.1.1.1</p> <p>Pool Size(max size: 253): 20</p> <p>Primary DNS Server: 10.1.1.254</p> <p>Secondary DNS Server: 0.0.0.0</p> <p>Lease time(sec): 7200</p> <p>Routing Protocol: None</p> <p>OSPF Area ID:</p> <p>Apply</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|------------|----------------|-----------------------------|-----------------------|------|--------|--|--------|------|-----------|-------------------|-----------------------|------|---|---|------------|----------------|--------------------------|----------------------|-----|---|---|------------|----------------|-----------------------------|----------------------|-----|---|---|------------|----------------|-----------------------------|----------------------|-----|
| <p>Step 2. Client IP Range Enable the DHCP server if you want to use DFL-1500 to assign IP addresses to the computers under DMZ1.</p> | <p>ADVANCED SETTINGS > NAT > Status</p> <p>Status NAT Rules Virtual Servers</p> <p>Network Address Translation Mode: Basic</p> <p>Network Address Translation (NAT) translates the IP/port for</p> <p>1. Internal-to-External traffic: map the conditioned internal IPs/ports into the specified external IPs/ports. Reset NAT rules</p> <p>2. External-to-Internal traffic: map the conditioned external IPs/ports into the specified internal IPs/ports. Reset Server rules</p> <p>Modes:</p> <p>1. None: The DFL-1500 is in routing mode without performing any address translation.</p> <p>2. Basic: The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.</p> <p>3. Full Feature: The DFL-1500 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.</p> <p>Total Configured NAT Rules: 3 Vacant NAT Rules: 197</p> <p>Total Configured Server Rules: 0 Vacant Server Rules: 200</p> <p>Apply</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Step 3. Apply the Changes Click Apply to save your settings.</p> | <p>ADVANCED SETTINGS > NAT > NAT Rules</p> <p>Status NAT Rules Virtual Servers</p> <p>NAT->Edit Rules</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th rowspan="2">Item #</th> <th colspan="2">Status</th> <th colspan="2">Condition</th> <th colspan="2">Action</th> </tr> <tr> <th>Active</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/DMZ to WAN</td> <td>10.1.1.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Basic-LAN2</td> <td>LAN/DMZ to WAN</td> <td>192.168.2.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> <tr> <td>3</td> <td>Y</td> <td>Basic-LAN1</td> <td>LAN/DMZ to WAN</td> <td>192.168.1.254/255.255.255.0</td> <td>Auto (device WAN IP)</td> <td>M-1</td> </tr> </tbody> </table> <p>Page 1/1</p> <p>Prev. Page Next Page Move Page 1</p> <p>Insert Edit Delete Move Before: 1</p> | Item # | Status | | Condition | | Action | | Active | Name | Direction | Source IP Address | Translate Src IP into | Type | 1 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 | 2 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) | M-1 | 3 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 |
| Item # | Status | | Condition | | Action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Active | Name | Direction | Source IP Address | Translate Src IP into | Type | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) | M-1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Step 5. Check NAT Rules The DFL-1500 has added the NAT rules as the right diagram. The rule Basic-DMZ1 (number 1) means that, when matching the condition (requests of LAN/DMZ-to-WAN direction with its source IP falling in the range of 10.1.1.254 / 255.255.255.0), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.</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 to the well-known port (21).

N/A

Step 7. Setup Server Rules
Insert a virtual server rule by clicking the Insert button.

ADVANCED SETTINGS > NAT > Virtual Servers

Virtual Server->Edit Rules

Packets are top-down matched by the rules.

| Item | Status | Name | Direction | Condition | Action | | |
|----------|--------|------|-----------|------------------|---------|-------------|---------|
| # | Active | | | Dest. IP Address | Service | Redirect to | through |
| Page 1/1 | | | | | | | |

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: ▾

Step 8. Customize the Rule
Customize the rule name as the ftpServer. For any packets with its destination IP address equaling to the WAN1 IP (61.2.1.1) and destination port equaling to 44444. DFL-1500 will translate the packet's destination IP/port into 10.1.1.5/21. Check the Passive FTP client to maximize the compatibility of the FTP protocol. This is useful if you want to provide connectivity to passive FTP clients. For passive FTP clients, the server at DMZ will return them the private IP address (10.1.1.5) and the port number for the clients to connect back for data transmissions. Since the FTP clients at the WAN side cannot connect to a private-IP (ex.10.1.1.5) through the internet. The data connections would be fail. After enabling this feature, the DFL-1500 will translate the private IP/port into an IP/port of its own. Thus the problem is gracefully solved.

ADVANCED SETTINGS > NAT > Virtual Servers > Insert

Virtual Server->Edit Rules->Insert

Insert a new Virtual Server rule

Status

Activate this rule

Rule name: ftpServer

Condition

Sessions from Internet connecting to WAN1

External IP: 61.2.1.1

Service: TCP

Type: Single Range

Dest. Port: 44444 Passive FTP client?

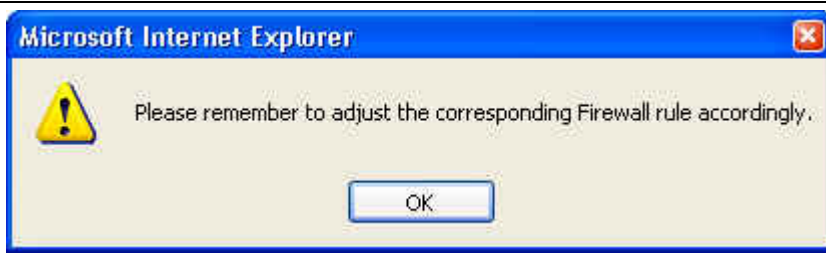
to 0

Action

Redirect to internal server under DMZ1

Internal IP: 10.1.1.5 Port: 21

Back Apply



✓ Warning message

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

Step 9. View the Result

Now any request towards the DFL-1500's WAN1 IP (61.2.1.1) with dest. port 44444 will be translated into a request towards 10.1.1.5 with port 21, and then be forwarded to the 10.1.1.5. The FTP server listening at port 21 in 10.1.1.5 will pick up the request.

ADVANCED SETTINGS > NAT > Virtual Servers

Virtual Server->Edit Rules

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

1.9 NAT/Router Mode and Transparent Mode

1.9.1 NAT/Router Mode

When the DFL-1500 is running in NAT/Router mode, you can connect a private network to the internal interface, a DMZ network to the DMZ interface, and a public network, such as the Internet, to the external interface. Each of these networks must have a different subnet address. You create security policies to control how the firewall routes packets between DFL-1500 interfaces, and therefore between the networks connected to the interface. When you switch the DFL-1500 operation mode from NAT/Router mode to Transparent mode, you have to backup your configuration first, otherwise the original configuration will be deleted inclusive of all rules, policies, addresses, etc. After system reboots, DFL-1500 will return to the factory default.

In this document, we will introduce you how to setup NAT/Router Mode firewall in the most examples. You can learn the settings of each feature by them. For more information of how to choose NAT or Route mode in the DFL-1500, please refer Section 7.5.5.

1.9.2 Transparent Mode

When the DFL-1500 is running in Transparent mode, it can be inserted in your network at any point without changing your network or any of its components. In Transparent mode, you can add Transparent mode rules/policies to accept or deny connections between interfaces. The firewall will apply those rules/policies to control traffic without modifying the packets in any way. Please make sure not to connect the LAN1/LAN2/DMZ interfaces to the same Hub while using Transparent mode, otherwise the traffic from the PCs under LAN1/LAN2/DMZ interfaces may be blocked.

For the DFL-1500 Transparent mode connections, please refer to the following Figure 1-11.

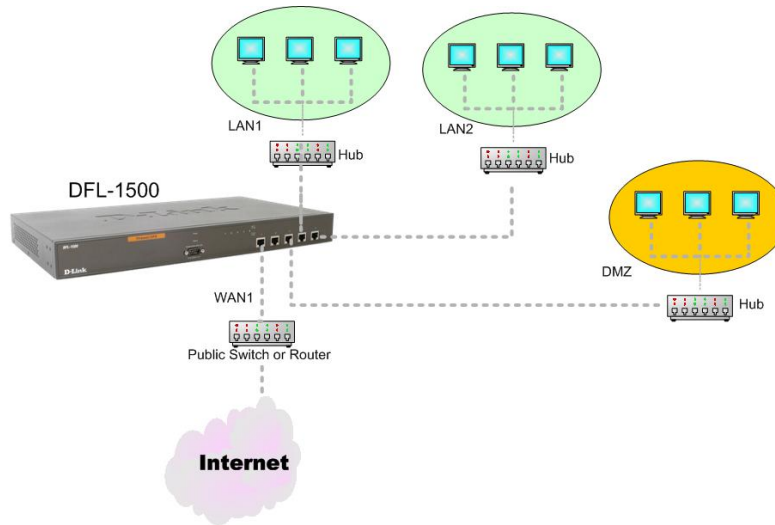


Figure 1-11 DFL-1500 Transparent mode connections

Basically, transparent mode provides the same firewall protection as NAT mode. Packets received by the DFL-1500 are intelligently forwarded or blocked according to the firewall rules. However, some advanced firewall features are only available in NAT/Route mode.

Transparent mode will not support the following features currently:

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

Chapter 2

System Overview

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

2.1 Typical Example Topology

In this chapter, we introduce a typical network topology for the DFL-1500. In Figure 2-1, the left half side is a DFL-1500 with one LAN, one DMZ, and one WAN link. We will demonstrate the administration procedure in the later chapters by using the below Figure 2-1.

The right half side contains another DFL-1500 connected with one LAN, one DMZ, and one WAN. You can imagine this is a branch office of Organization_1. In this architecture, all the users under Organization can access sever reside in the Internet or DMZ region smoothly. Besides, Organization_1 communicates with Organization_2 with a VPN tunnel established by the two DFL-1500 VPN/Firewall routers. The VPN tunnel secures communications between Organizations more safely.

We will focus on how to build up the topology using the DFL-1500 as the following Figure 2-1. In order to achieve this purpose, we need to know all the administration procedure.

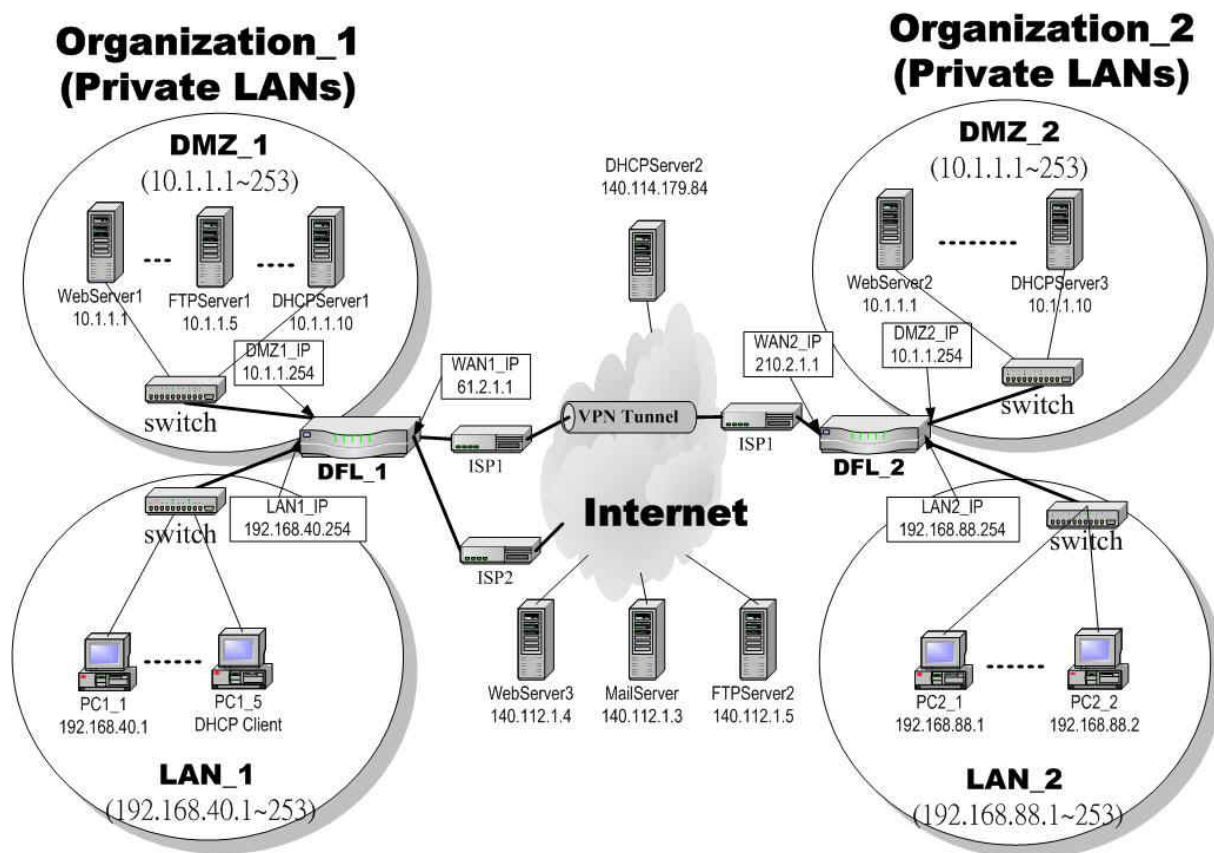


Figure 2-1 Typical topology for deploying DFL-1500

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

Part I

Overview

1. **Part II Basic Configuration**
How to configure the WAN/DMZ/LAN port settings and user authentication.
2. **Part III NAT & Routing**
Introducing the NAT, Routing features.
3. **Part IV Firewall & IP/MAC Binding**
Introducing the Firewall and IP/MAC Binding features.
4. **Part V Virtual Private Network**
If you need to build a secure channel with your branch office, or wish to access the inside company resource as usual while outside your company, the Virtual Private Network (VPN) function can satisfy you.
5. **Part VI Content Filters**
If you hope to restrict the web contents, mail attachments, downloaded ftp file from intranet region, try this feature to fit your requirement.
6. **Part VII Intrusion Detection System**
Use the Intrusion Detection System (IDS) to detect all the potential DoS attacks, worms, hackers from Internet.
7. **Part VIII Load Balancer · Bandwidth Management · High Availability**
If you wish to make your inbound/outbound bandwidth utilized more efficiently, you may use the Bandwidth Management feature to manage your bandwidth. High Availability makes your company operate smoothly.
8. **Part IX System Maintenance**
In this part, we provide some useful skills to help you to justify DFL-1500 more securely and steadily.

2.2 Changing the LAN1 IP Address

The default settings of DFL-1500 are listing in Table 1-3. However, the original LAN1 setting is 192.168.1.254/255.255.255.0 instead of 192.168.40.254/255.255.255.0 as in Figure 2-1. We will change the LAN1 IP of the DFL-1500 to 192.168.40.254.

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

2.2.1 From LAN1 to configure DFL-1500 LAN1 network settings

| | |
|---|---|
| Step 1. Connect to the DFL-1500 | Use an IE at 192.168.1.1 to connect to https://192.168.1.254 |
| Using a network line to connect DFL-1500 with LAN1 port. The PC which connected to DFL-1500 must be assigned 192.168.1.X address (LAN1 default IP address is 192.168.1.254/24). Type https://192.168.1.254 or http://192.168.1.254:8080 to configure the DFL-1500 in the web browser. | |

Step 2. Setup LAN1 IP information

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

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

BASIC SETUP > LAN Settings > LAN1 Status

LAN1 Status LAN2 Status IP Alias

LAN1 TCP/IP

IP Address 192.168.40.254 IP Subnet Mask 255.255.255.0

DHCP Setup

Enable DHCP Server

IP Pool Starting Address 192.168.40.1

Pool Size(max size: 253) 20

Primary DNS Server 192.168.40.254

Secondary DNS Server 0.0.0.0

Lease time(sec) 7200

Routing Protocol None

OSPF Area ID

Apply

2.2.2 From CLI (command line interface) to configure DFL-1500 LAN1 network settings**Step 1. Use Console port to configure DFL-1500**

Use the supplied console line to connect the PC to the Diagnostic RS-232 socket of the DFL-1500. Start a new connection using the HyperTerminal with parameters: No Parity, 8 Data bits, 1 stop bit, and baud rate 9600. Enter admin for user name and admin for password to login. After logging into DFL-1500, enter the commands "en" to enter the privileged mode. Enter the command "ip ifconfig INTF3 192.168.40.254 255.255.255.0" to change the IP of the LAN1 interface.

```
DFL-1500> en
DFL-1500#
DFL-1500# ip ifconfig INTF3 192.168.40.254 255.255.255.0
```

```
DFL-1500#
DFL-1500# ip ifconfig INTF3
```

```
====
Port Interface IP Address Netmask Status Type
====
4 LAN1 192.168.40.254 255.255.255.0 DOWN
====
```

```
DFL-1500#
DFL-1500#
```

2.3 The design principle

2.3.1 Web GUI design principle

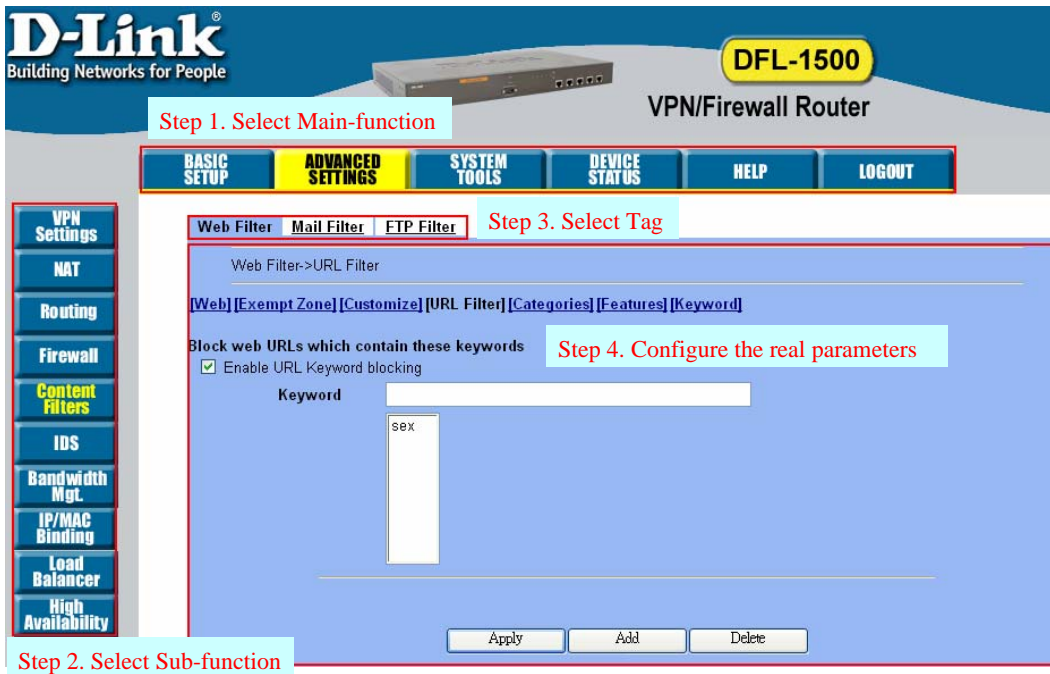


Figure 2-2 You can select the functional area by the sequence in Web GUI

If we want to configure DFL-1500, we can follow the sequence as the Figure 2-2 illustrated.

Step1. Select Main-function

Step2. Select Sub-function

Step3. Select Tag

Step4. Configure the real parameters

2.3.2 Rule principle

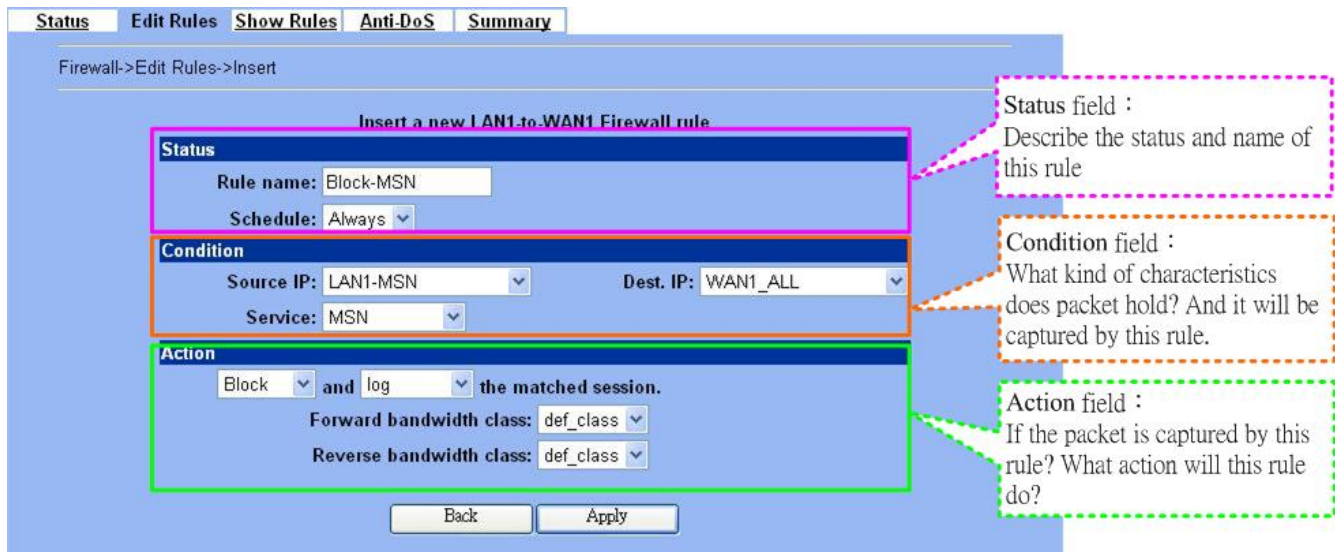


Figure 2-3 The rule configuration is divided into three parts

You may find many rules configuration in the DFL-1500. They are distributed in the respective feature. These rules include

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

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

1. **Status:** Describe the status and name of this rule.
2. **Condition:** What kind of characteristics does packet hold? And it will be captured by this rule.
3. **Action:** If the packet is captured by this rule? What action will this rule do?

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

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

The screenshot shows a firewall rule configuration interface. At the top, there are tabs for 'Status', 'Edit Rule', 'Flow Rules', 'Anti-DoS', and 'Summary'. Below these, there are dropdown menus for 'Edit LAN1' and 'WAN1', and a 'rules' button. A 'Default action for this packet direction:' section shows 'Forward' and a 'Log' checkbox. Below this is a table of rules with columns for 'Item', 'Status', 'Condition', and 'Action'. The table contains two rules: 'Block-MSN' and 'Default'. At the bottom, there are navigation buttons: 'Prev. Page', 'Next Page', 'Move Page', '1', 'Insert', 'Edit', 'Delete', and 'Move Before: 1'. Three callout boxes provide explanations: a pink box for the 'Status field', an orange box for the 'Condition field', and a green box for the 'Action field'. A brown box points to the 'Move Before' button.

Status field :
Describe the status and name of this rule

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

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

| Item # | Status | | Condition | | | | Action | |
|--------|-----------|----------|-----------|----------|-------------|---------|--------|--|
| | Name | Schedule | Source IP | Dest. IP | Service | Action | Log | |
| 1 | Block-MSN | ALWAYS | LAN1-MSN | WAN1_ALL | MSN | Block | Y | |
| 2 | Default | ALWAYS | LAN1_ALL | WAN1_ALL | ALL_SERVICE | Forward | N | |

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

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

Part II

Basic Configuration

Chapter 3 Basic Setup

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

3.1 Demands

1. For the external network, suppose your company uses DSL to connect Internet via fixed-IP. By this way, you should setup WAN port of the DFL-1500 in advance.
2. There are some adjustment within your company, so the original network structure has been changed. Now, you should modify the configuration between the internal network (DMZ, LAN).
3. Your company needs more network bandwidth if it is insufficient for your company to connect to the external network. Suppose there are many public IPs in your company. You would like to specify a unique public IP to a local server.

3.2 Objectives

1. Configure the network settings of the DFL-1500 WAN1 port.
2. Configure the network settings of the DFL-1500 DMZ1 and LAN1 ports.
3. We hope to assign another IP address to the same WAN port we have configured an existed IP address before.

3.3 Methods

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

The features of the Virtual Server, VPN, Content Filter, and IDS can only be available while DFL-1500 connects to the internet via DEFAULT WAN Link.

3.4 Steps

3.4.1 Setup WAN1 IP

Step 1. Setup WAN1 port

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

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

The screenshot shows the configuration interface for WAN1 IP Fixed IP Address. It includes tabs for WAN1 IP, WAN2 IP, and IP Alias. The IP Address Assignment is set to Fixed IP Address. The Default WAN link (Gateway/DNS) is checked. The IP Address is 61.2.1.1, Subnet Mask is 255.255.255.248, and Gateway IP is 61.2.1.6. The DNS IP Address section is selected with a radio button, showing Primary DNS as 168.95.1.1 and Secondary DNS as 0.0.0.0. The Routing Protocol is set to None, and the OSPF Area ID field is empty. An Apply button is located at the bottom right.

| IP Address Assignment | FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------------------------|--|---|---|-----------------------|
| Get IP Automatically (DHCP) | Default WAN link (Gateway/DNS) | When Default WAN link is enabled, all packets sent out from DFL-1500 will be via this interface. | Enable/Disable | Enabled |
| | Get DNS Automatically / DNS IP Address | Get DNS Automatically → Get DNS related information from DHCP Server DNS IP Address → manually specify these Primary and Secondary DNS Server information. | Get DNS Automatically / DNS IP Address | Get DNS Automatically |
| | Routing Protocol | Determine to enable the dynamic routing protocol, to receive RIP message, and to send out the RIP message if the RIP message is received. | None, RIPv1/In, RIPv1/In+Out, RIPv2/In, RIPv2/In+Out, OSPF | None |
| | OSPF Area ID | Specify OSPF area ID number. | IPv4 format or digit string (Max 9 bits) | N/A |
| Fixed IP Address | Default WAN link (Gateway/DNS) | When Default WAN link is enabled, all packets sent out from DFL-1500 will be via this interface. | Enable/Disable | Enabled |
| | IP Address | Specified WAN IP address. | IPv4 format | 61.2.1.1 |
| | Subnet Mask | Specified subnet mask | IPv4 format | 255.255.255.248 |
| | Gateway IP | Default gateway IP address. | IPv4 format | 61.2.1.6 |

Part II

Basic Configuration

| | | | | |
|-------------------|---|--|---|---|
| | DNS IP Address: Primary DNS Secondary DNS | Specified Primary and Secondary DNS Server address. | IPv4 format | Primary DNS: 168.95.1.1 Secondary DNS: 0.0.0.0 |
| | Routing Protocol | Determine to enable the dynamic routing protocol, to receive RIP message, to send out the RIP message if the RIP message is received. | None, RIPv1/In, RIPv1/In+Out, RIPv2/In, RIPv2/In+Out, OSPF | None |
| | OSPF Area ID | Specify OSPF area ID number. | IPv4 format or digit string (Max 9 bits) | N/A |
| PPP over Ethernet | Default WAN link (Gateway/DNS) | When Default WAN link is enabled, all packets sent out from DFL-1500 will be via this port. | Enable/Disable | Enabled |
| | Service Name | ISP vendor (Optional). | text string | So-Net |
| | User Name | The user name of PPPoE account. | text string | Hey |
| | Password | The password of PPPoE account. | text string | G54688 |
| | Get DNS Automatically / DNS IP Address | Get DNS Automatically → Get DNS related information from PPPoE ISP DNS IP Address → manually specify these Primary and Secondary DNS Server information | Get DNS Automatically / DNS IP Address | Get DNS Automatically |
| | Disconnect button | Disconnect PPPoE link by clicking Disconnect button. | Disconnect | Click Disconnect |

Table 3-1 Detailed information of setup WAN port configuration

3.4.2 Setup DMZ1, LAN1 Status

Step 1. Setup DMZ port

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

BASIC SETUP > DMZ Settings > DMZ1 Status

DMZ1 Status **IP Alias**

DMZ1 TCP/IP

IP Address: 10.1.1.254 IP Subnet Mask: 255.255.255.0

DHCP Setup

Enable DHCP Server

IP Pool Starting Address: 10.1.1.1

Pool Size(max size: 253): 20

Primary DNS Server: 10.1.1.254

Secondary DNS Server: 0.0.0.0

Lease time(sec): 7200

Routing Protocol: None

OSPF Area ID:

Apply

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

Table 3-2 Configure DMZ network settings

Step 2. Setup LAN port

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

Note, when changing the LAN IP, your configuration may be disconnected. You may need to reconfigure the Firewall, such as Firewall objects, IP/MAC Binding, Authentication Exempt Host, Virtual Server rules, IPSec/L2TP/PPTP VPN rules, and Remote Mgmt settings.

BASIC SETUP > LAN Settings > LAN1 Status

LAN1 Status LAN2 Status IP Alias

LAN1 TCP/IP

IP Address: 192.168.40.254 IP Subnet Mask: 255.255.255.0

DHCP Setup

Enable DHCP Server

IP Pool Starting Address: 192.168.40.100

Pool Size(max size: 253): 20

Primary DNS Server: 192.168.40.254

Secondary DNS Server: 0.0.0.0

Lease time(sec): 7200

Routing Protocol: None

OSPF Area ID:

Apply

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------------|-------------------------------------|----------------|----------------|
| IP Address | LAN1 port IP address. | IPv4 format | 192.168.40.254 |
| IP Subnet Mask | LAN1 port IP subnet mask. | netmask format | 255.255.255.0 |
| Enable DHCP Server | Enable LAN1 port of the DHCP Sever. | Enable/Disable | Enabled |

Part II

Basic Configuration

| | | | |
|--------------------------|---|---|----------------|
| IP Pool Starting Address | Specify the starting address of the DHCP IP address. | IPv4 format in the LAN1 address range | 192.168.40.100 |
| Pool Size(max size: 253) | Specify the numbers of the DHCP IP address. | 1 ~253 | 20 |
| Primary DNS Server | Specify the Primary DNS Server IP address of the DHCP information. | IPv4 format | 192.168.40.254 |
| Secondary DNS Server | Specify the Secondary DNS Server IP address of the DHCP information. | IPv4 format | 0.0.0.0 |
| Lease time(sec) | Specify DHCP information lease time. | greater than 0 | 7200 |
| Routing Protocol | Determine to enable the dynamic routing protocol (RIP), to receive RIP message, to send out RIP message if the message is received. | None / RIPv1In / RIPv1In+out / RIPv2In / RIPv2In+out / OSPF | None |
| OSPF Area ID | Specify OSPF area ID number. | IPv4 format or digit string (Max 9 bits) | N/A |

Table 3-3 Configure LAN network settings

➤ What is the difference between LAN and DMZ area in the DFL-1500?

| Area | LAN | DMZ |
|-----------------------|--------------------------------|------------------------------|
| Feature | | |
| usage method | Placing the client PCs. | Placing the server PCs. |
| firewall rule | LAN to DMZ default is forward. | DMZ to LAN default is block. |
| Authentication | Have restriction | No restriction |
| Web filter | Have restriction | No restriction |
| SMTP/ POP3/FTP filter | Have restriction | No restriction |
| IP/MAC binding | Have restriction | No restriction |

Table 3-4 The differences between LAN and DMZ area

3.4.3 Setup WAN1 IP alias

Step 1. Add WAN1 IP alias

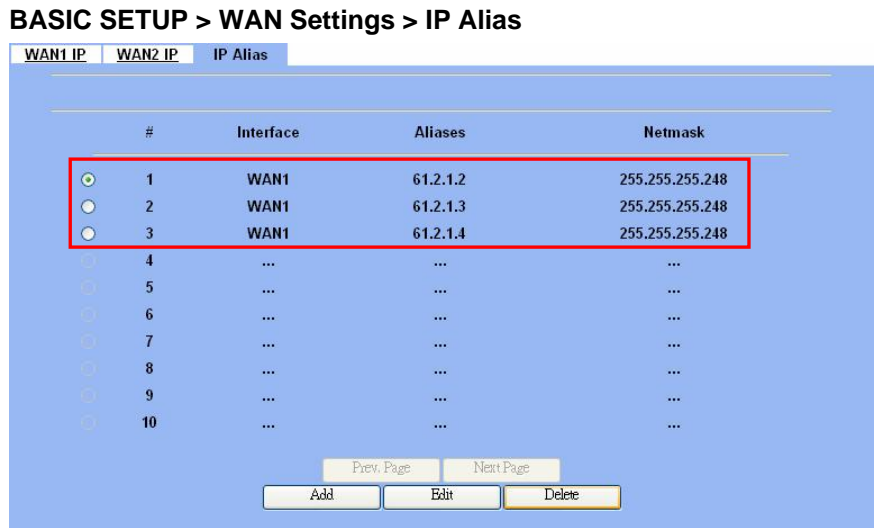
Suppose you apply 8 IP addresses from ISP. The range of the ISP-given IP address is from 61.2.1.0 to 61.2.1.7. Now you would like to add three WAN1 IP aliases. Select WAN1 in the Interface field. Enter the IP alias and Netmask with 61.2.1.2/255.255.255.248. Key in 3 into the Alias size field. And then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

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

BASIC SETUP > WAN Settings > IP Alias > Add

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

Table 3-5 Add a IP alias record

| | |
|--|---|
| <p>Step 2. Edit, Delete IP alias record</p> <p>You can easily add, edit, or delete IP alias records by the Add, Edit, or Delete button.</p> | <p>BASIC SETUP > WAN Settings > IP Alias</p>  |
|--|---|

| FIELD | DESCRIPTION | EXAMPLE |
|------------|---|---------|
| Prev. Page | If there are more than one IP alias pages, you can press Prev. Page to back to the previous page. | N/A |
| Add | Insert a new IP alias record. | N/A |
| Edit | Edit the properties of the existent record. | N/A |
| Delete | Delete the indicated record. | N/A |
| Next Page | If there are more than one action records, you can press Next Page to go to the next page. | N/A |

Table 3-6 Show the entered IP alias records

Part II

Basic Configuration

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

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

Warning: If you select Fixed IP Address as your WAN link type and set any IP alias, the previous set IP aliases will disappear when you try to exchange the WAN link type to other type such as DHCP or PPPoE.

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

WAN1 IP | **WAN2 IP** | IP Alias

IP Address Assignment: Fixed IP Address

Default WAN link (Gateway/DNS)

IP Address: 61.2.1.1 Subnet Mask: 255.255.255.248

Gateway IP: 61.2.1.6

IP Aliased: 61.2.1.2/255.255.255.248

IP Aliased: 61.2.1.3/255.255.255.248

IP Aliased: 61.2.1.4/255.255.255.248

DNS IP Address

Primary DNS: 168.95.1.1

Secondary DNS: 0.0.0.0

Routing Protocol: None

OSPF Area ID:

Apply

Chapter 4

System Tools

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

4.1 Demands

1. Basic configurations for domain name, password, system time, timeout and services.
2. DDNS: Suppose the DFL-1500's WAN uses dynamic IP but needs a fixed host name. When the IP is changed, it is necessary to have the DNS record updated accordingly. To use this service, one has to register the account, password, and the wanted host name with the service provider.
3. DNS Proxy: Shorten the time of DNS lookup performed by applications.
4. DHCP Relay: It is to solve the problem that when the DHCP client is not in the same domain with the DHCP server, the DHCP broadcast will not be received by the server. If the client is in the LAN (192.168.40.X) while the server is located in the DMZ (10.1.1.4), the server will not receive any broadcast packet from the client.
5. The System Administrator would like to monitor the device from remote side efficiently.
6. Suppose our company applies three ISPs, but there are just two default WAN ports in the DFL-1500. You hope to connect the whole ISP links to the DFL-1500. Note this capability is only valid in the DFL-1500 model.

4.2 Objectives

1. Configure the general properties, such as domain name, password, system time, and connection timeout correctly. Besides, we can configure the preferred service name as the service name/numeric mapping list.
2. DDNS: By using the DDNS (Dynamic DNS), the DFL-1500 will send the request for modification of the corresponding DNS record to the DDNS server after the IP is changed.
3. DNS Proxy: Reduce the number of DNS requests and the time for DNS lookup.
4. DHCP Relay: Enable the DHCP client to contact with the DHCP server located in different domain and get the required IP.
5. Through the SNMP manager, we can easily monitor the device status.
6. We hope to customize the interface of DFL-1500 to fit our requests.

4.3 Methods

1. Configure the domain name, password, system time, connection timeout and service name.
2. DDNS: Configure the DFL-1500 so that whenever the IP of the DFL-1500 is changed, it will send requests to the DDNS server to refresh the DNS record. As the following Figure 4-1 demonstrated, the original DFL-1 has registered WAN1 IP address "61.2.1.1" on the DDNS server (www.dyndns.org). Its domain name address is "me.dyndns.org". If the WAN1 IP address is reassigned by the ISP, DFL-1 will update the registered IP address "61.2.1.1" as the assigned one. This is the base mechanism of the DDNS.

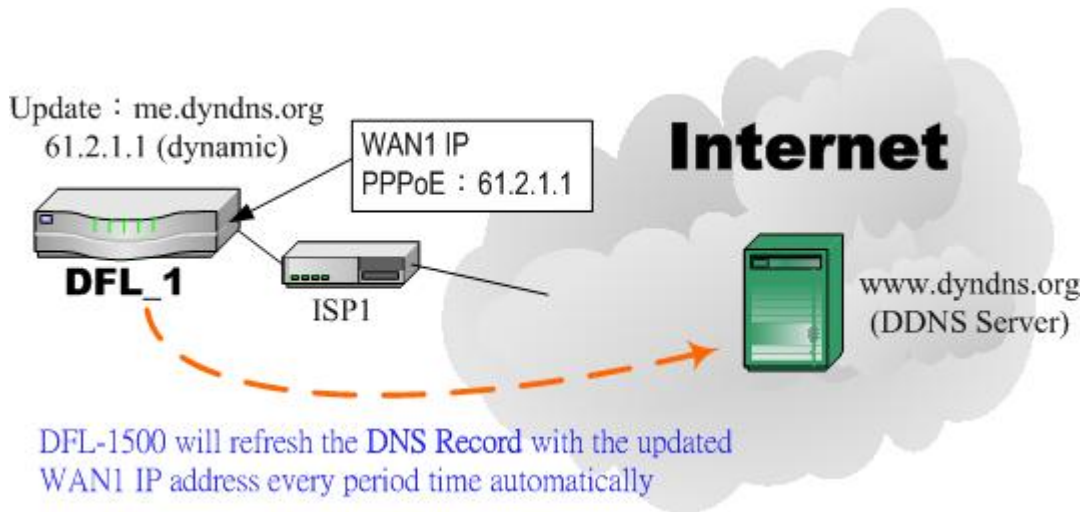


Figure 4-1 DDNS mechanism chart

3. DNS Proxy: After activating the DNS proxy mode, the client can set its DNS server to the DFL-1500 (that is, send the DNS requests to the DFL-1500). The DFL-1500 will then make the enquiry to the DNS server and return the result to the client. Besides, the caching mechanism performed by the DNS proxy can also help reduce possible duplicate DNS lookups. As the following Figure 4-2 described. DFL-1 redirects the DNS request from PC1_1 to the real DNS server (140.113.1.1).

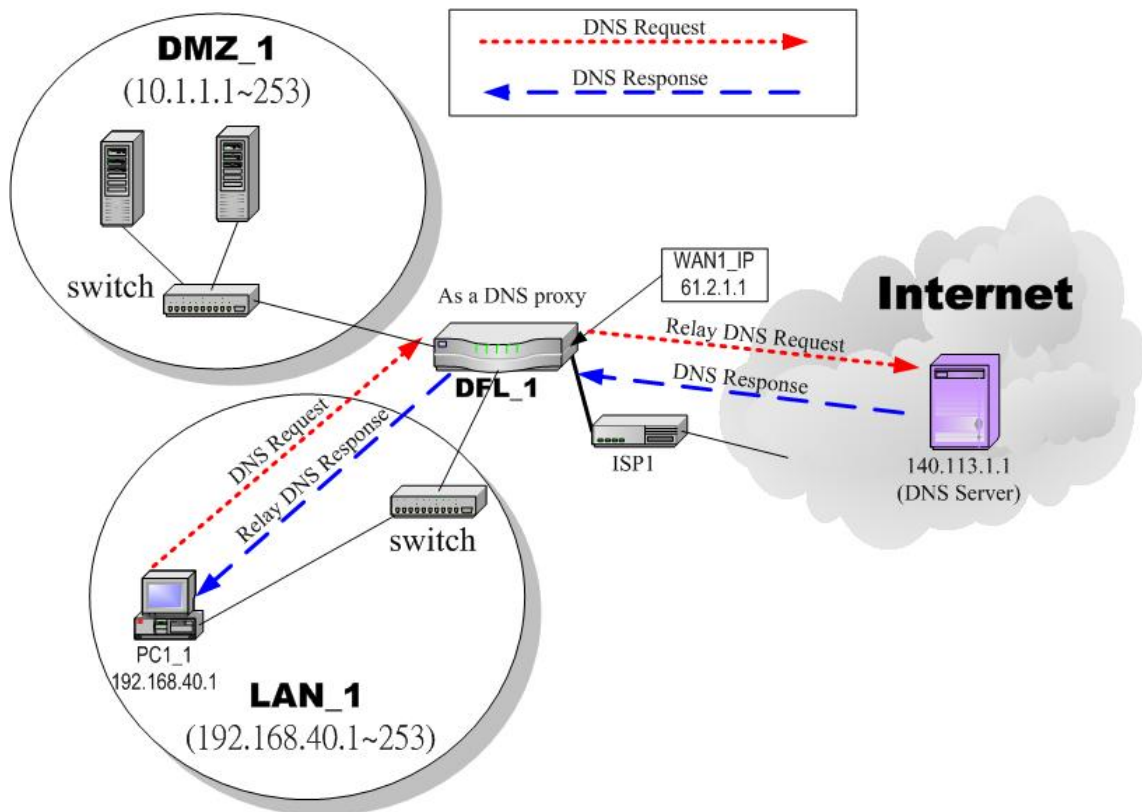


Figure 4-2 DNS Proxy mechanism chart

4. DHCP Relay: Activate the DHCP relay mode of DFL-1500 so that the DFL-1500 will become the relay agent and relay the DHCP broadcast to the configured DHCP server. As the following Figure 4-3 described, DFL-1 redirects the DHCP

request from the preconfigured port (LAN1) to the real DHCP server (10.1.1.4). Besides, in this diagram, we can find that the PC of DMZ region communicated with the DHCP server directly.

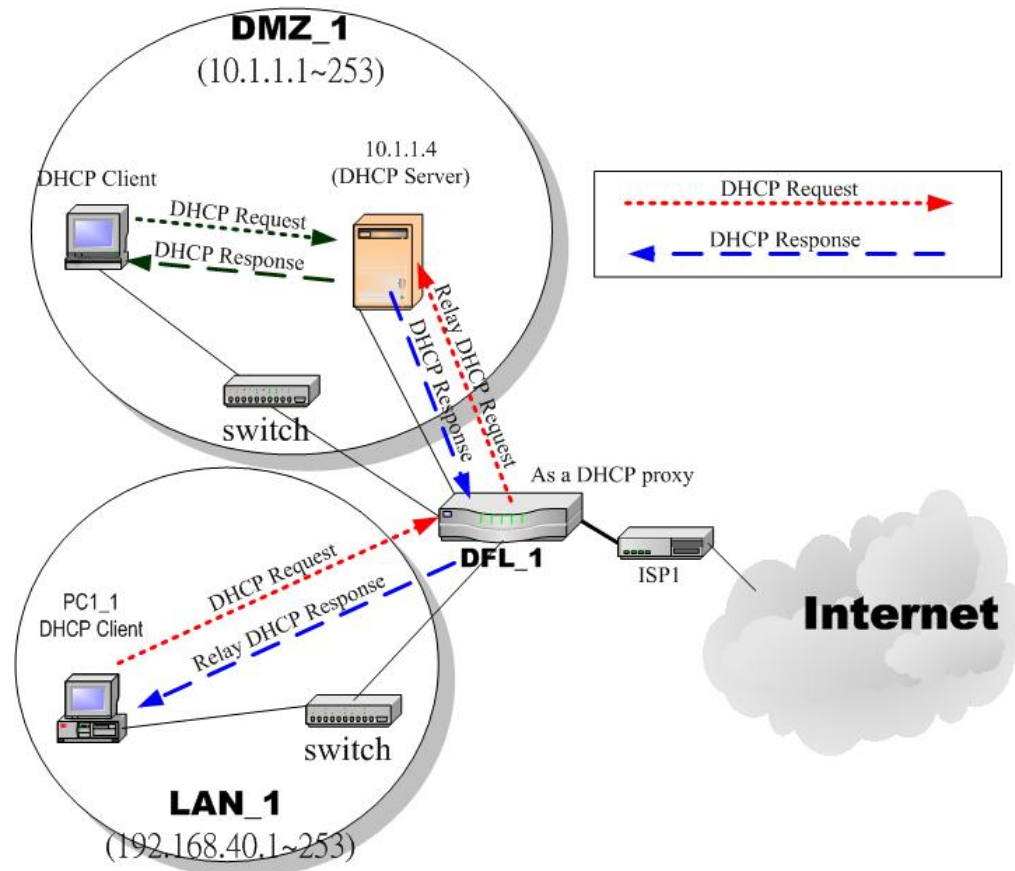


Figure 4-3 DHCP Relay mechanism chart

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

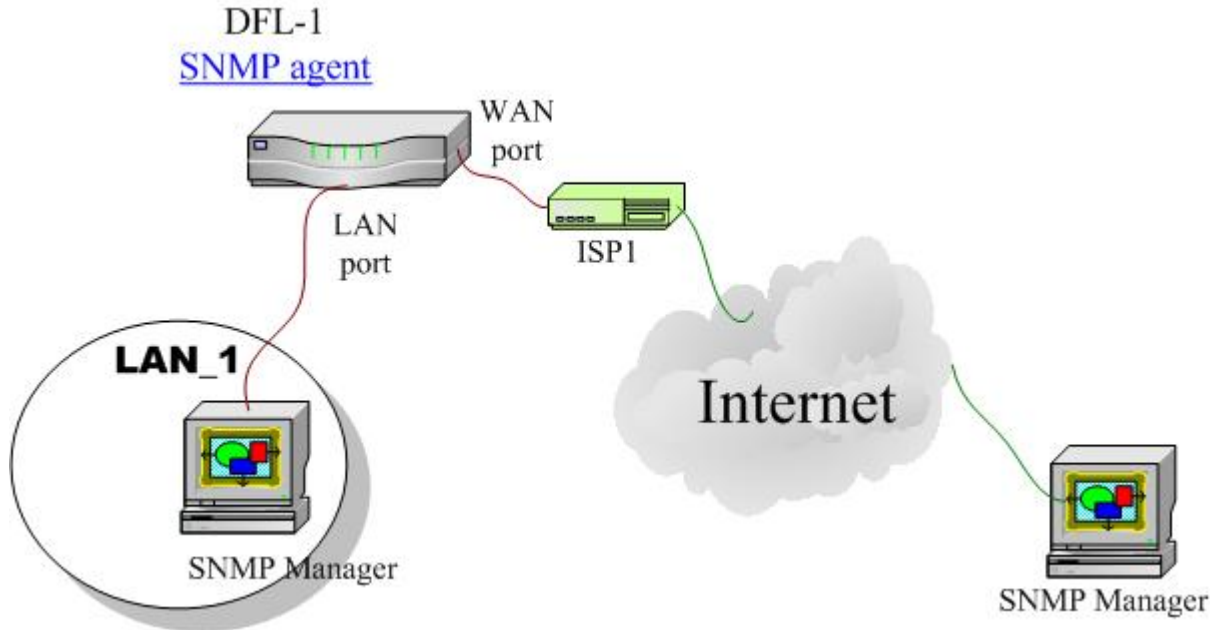


Figure 4-4 It is efficient to use SNMP Manager to monitor DFL-1500 device

6. We can adjust the DFL-1500 interface in the SYSTEM TOOLS > Admin Settings > Interface in according to our preference and requirement (3 WAN, 1 DMZ, 1 LAN). As the following Figure 4-5 demonstrated, there are three ISP connected onto DFL-1500. So we must adjust the interface up to 3 WAN ports to fit the current condition.

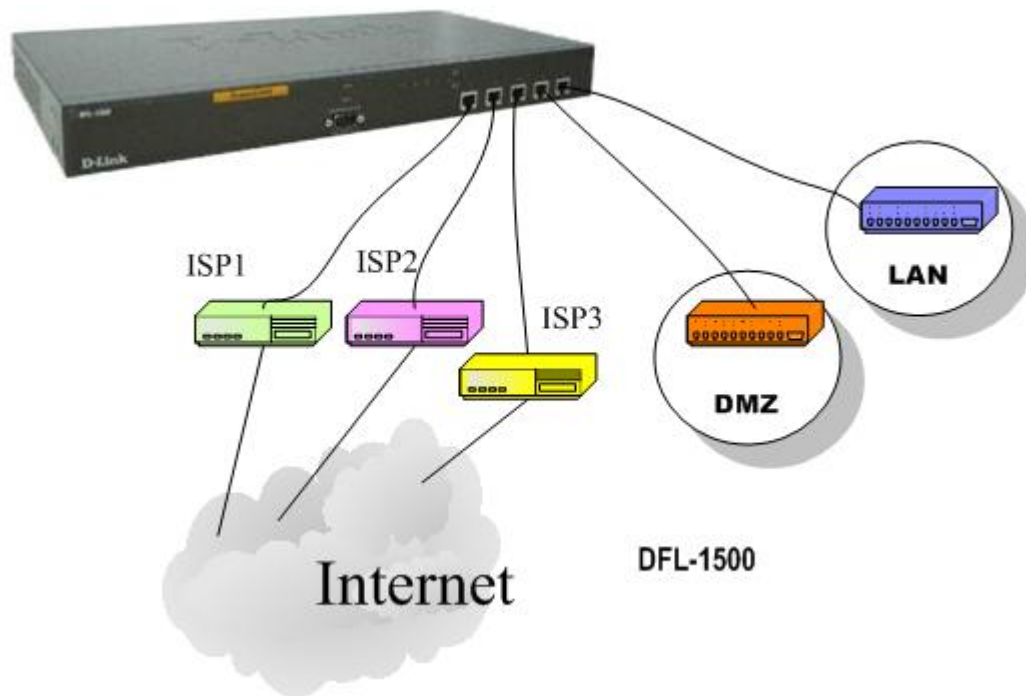


Figure 4-5 Adjust DFL-1500 interface to fit present situation

4.4 Steps

4.4.1 General settings

Step 1. General Setup

Enter the Host Name as DFL-1, Domain Name as the domain name of your company. Click Apply.

SYSTEM TOOLS > Admin Settings > General

General DDNS DNS Proxy DHCP Relay Password Time/Date Timeout Interface

Host Name DFL-1

Domain Name dlink.com

Apply

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

Table 4-1 System Tools - General Setup menu

Step 2. Change Password

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

SYSTEM TOOLS > Admin Settings > Password

General DDNS DNS Proxy DHCP Relay Password Time/Date Timeout Interface

Old Password *****

New Password *****

Confirm Password *****

Apply

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

Table 4-2 Enter new password

Part II

Basic Configuration

Step 3. Setup Time/Date

Select the Time Zone where you are located. Enter the nearest NTP time server in the NTP time server address. Note that your DNS must be set if the entered address requires domain name lookup. You can also enter an IP address instead. Check the Continuously (every 3 min) update system clock and click Apply. The DFL-1500 will immediately update the system time and will periodically update it. Check the Update system clock using the time server at boot time and click Apply if you want to update the clock at each boot. If you want to manually change the system time, uncheck the Continuously (every 3 min) update system clock and proceed by entering the target date.

SYSTEM TOOLS > Admin Settings > Time/Date

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

Table 4-3 System Tools – Time Data menu

Step 4. Setup Timeout

Select the target timeout (e.g. 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.

SYSTEM TOOLS > Admin Settings > Timeout

| 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 logout automatically. | 10 |

Table 4-4 System Tools – Timeout menu

4.4.2 DDNS setting

Step 1. Setup DDNS

If the IP address of DFL-1500 WAN port is dynamic allocated, you may want to have the Dynamic DNS mechanism to make your partner always use the same domain name (like xxx.com) to connect to you. Select a WAN interface to update the DDNS record. Here we supply some DDNS Service Providers. Fill in the Host Name, Username, Password supplied by the DDNS web site. Please refer to the DDNS web site for the detailed information. Click Apply to activate the settings.

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

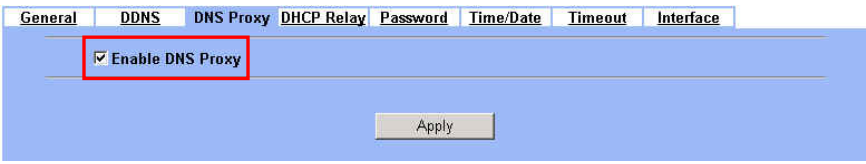
Note: If you choose "WWW.ORAY.NET" as your DDNS service provider, a default port number 5050 will be shown on the Port field. It means that if you use this port to connect to WWW.ORAY.NET, it will be free charge.

SYSTEM TOOLS > Admin Settings > DDNS

| FIELD | DESCRIPTION | EXAMPLE |
|----------------------|---|--------------|
| Enable DDNS for WAN1 | Enable DDNS feature of DFL-1500. | Enabled |
| Interface | Assign which public IP address of interface to the DDNS server. | WAN1 |
| Service Provider | The domain address of DDNS server. In the DFL-1500, we provide WWW.DYNDNS.ORG, WWW.DHS.ORG, WWW.ORAY.NET, WWW.CHANGEIP.COM, WWW.ADSLDNS.NET, WWW.NO-IP.COM, WWW.DNS2GO.COM, WWW.3322.ORG, WWW.88IP.NET, and WWW.HN.ORG websites for your choice. If you choose WWW.ORAY.NET as DDNS service provider, it would register the source IP address which is connected to the DDNS server. It means that the WAN1 IP address must be public address. | WWW.ORAY.NET |
| Hostname | The registered Hostname in the DDNS server. | abc.vicp.net |
| Username | The registered username in the DDNS server. | john |
| Password | The registered password in the DDNS server. | 123456 |
| ORAY Server | The domain of the ORAY server. | ns1.oray.net |
| Port | The default port number to connect to WWW.ORAY.NET for free charge | 5050 |

Table 4-5 System Tools – DDNS setting page

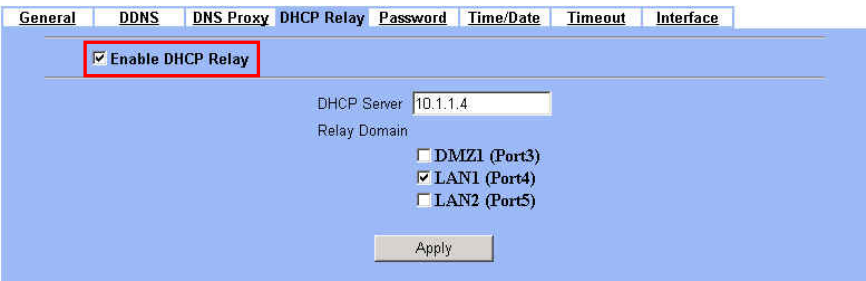
4.4.3 DNS Proxy setting

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

| FIELD | DESCRIPTION | EXAMPLE |
|------------------|---|---------|
| Enable DNS Proxy | When the host which resides at the LAN/DMZ region sends a DNS Request to the DNS server (DFL-1500), DFL-1500 will request for forwarding it to the assigned DNS server. When there is a response from assigned DNS server, then DFL-1500 will forward it back to the host of the LAN/DMZ. | Enabled |

Table 4-6 System Tools – DNS Proxy menu

4.4.4 DHCP Relay setting

| | |
|--|--|
| <p>Step 1. Setup DHCP Relay</p> <p>Check the <code>Enable DHCP Relay</code>. Enter the IP address of your DHCP server. Here we enter the DHCP Server address 10.1.1.4. Check the relay domain of DFL-1500 that needs to be relayed. Namely, check the one where the DHCP clients are located. And click the <code>Apply</code> button finally.</p> <p>Notice, the DHCP Server can not be located with the subnet range of Relay Domain.</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-1500 internal network sends a DHCP request, DFL-1500 will forward it automatically to the specified DHCP server (different subnet from the network segment of the DHCP client). | Enabled |
| DHCP Server | Current location of the DHCP server. | 10.1.1.4 |
| Relay Domain | The locations of the DHCP clients. | Enable LAN1 |

Table 4-7 System Tools – DHCP Relay menu

4.4.5 SNMP Control

Step 1. Setup SNMP Control

Through setting the related information in this page, we can use SNMP manager to monitor the system status, network status of DFL-1500.

SYSTEM TOOLS > SNMP Control

| FIELD | DESCRIPTION | EXAMPLE |
|------------------|--|-----------------|
| Enable SNMP | Enable the SNMP function. | Enabled |
| System Name | The device name of DFL-1500. | DFL-1.dlink.com |
| System Location | The settled location of DFL-1500. | Office |
| Contact Info | The person who takes charge of the DFL-1500. | mis |
| Get community | The community which can get the SNMP information. Here “community” is something like password. | public-ro |
| Set community | The community which can set the SNMP information. Here “community” is something like password. | private-rw |
| Trusted hosts | The IP address which can get or set community from the DFL-1500. | 192.168.1.5 |
| Trap community | The community which will send SNMP trap. Here “community” is something like password. | trap-comm |
| Trap destination | The IP address which will send SNMP trap from the DFL-1500. | 192.168.1.5 |

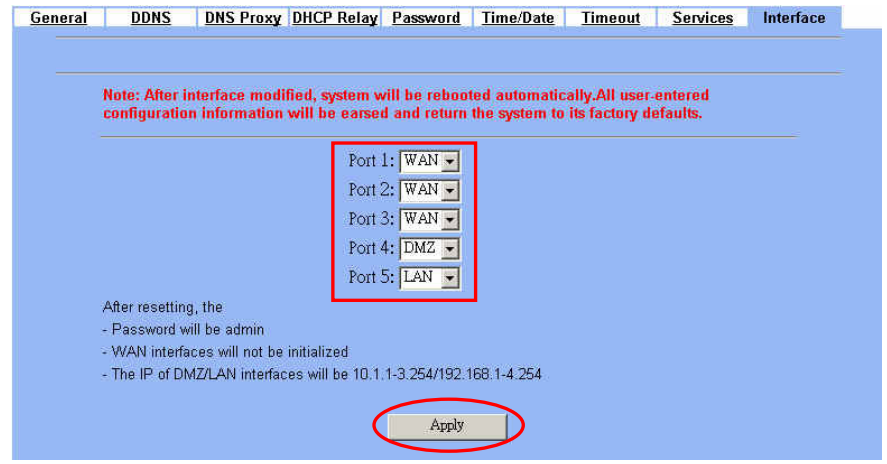
Table 4-8 SNMP Settings

4.4.6 Change DFL-1500 interface

Step 1. Change Interface definition

DFL-1500 interfaces by default are 2 WAN ports, 1 DMZ port and 2 LAN ports. In order to fit our requirement, we change the interfaces to 3 WANs (port1~3), 1 DMZ (port4), 1 LAN (port5). And then Click Apply button to reboot DFL-1500. Note that the DMZ and LAN port IP addresses are going to be 10.1.1.254 and 192.168.1.254 after device reboots. Besides, there should be at least one WAN port and one LAN port existing in the DFL-1500. You are not allowed to casually change the interface to the state which has no LAN port or WAN port.

SYSTEM TOOLS > Admin Settings > Interface



| FIELD | DESCRIPTION | EXAMPLE |
|---------------|--|---|
| Port1 ~ Port5 | You can specify WAN / LAN / DMZ for each port by your preference. However, there must be one WAN and one LAN interface existing in the DFL-1500. | Port1 : WAN Port2 : WAN Port3 : WAN Port4 : DMZ Port5 : LAN |

Table 4-9 Change the DFL-1500 interface setting

Chapter 5

Remote Management

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

5.1 Demands

Administrators may want to manage the DFL-1500 remotely from any PC in LAN_1 with HTTP at port 8080, and from WAN_PC with TELNET. In addition, the DFL-1500 may be more secure if monitored by a trusted host (PC1_1). What is more, the DFL-1500 should not respond to ping to hide itself. The remote management function in DFL-1500 devices is implemented by hidden Firewall rules.

5.2 Methods

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

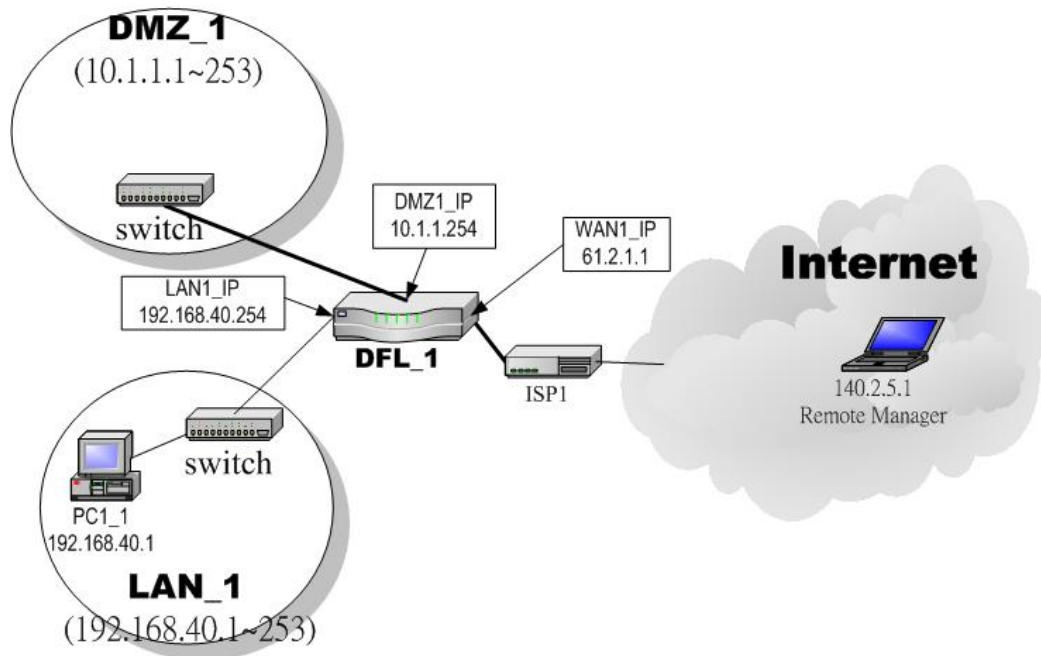


Figure 5-1 Some management methods of DFL-1500

5.3 Remote Management Access Methods

Configuring management access for an interface connected to the Internet allows remote administration of the DFL-1500 unit from any location on the Internet. Allowing management access from the Internet could compromise the security of your DFL-1500 unit. You should avoid allowing management access for an interface connected to the Internet unless this is required for your configuration. To improve the security of a DFL-1500 unit that allows remote management from the Internet, add secure administrative user passwords, change these passwords regularly, and only enable secure management access using HTTPS or SSH.

| Remote Management | Definition |
|-------------------|------------|
|-------------------|------------|

Part II

Basic Configuration

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

Table 5-1 Definition of the Remote Management Methods

The priority of the login methods to configure the DFL-1500 is described as the following Table 5-2..

| Priority | Login Method | Description |
|----------|---------------|---|
| 1 | Console | If you login using console method, then anyone else won't configure DFL-1500 afterward. For the CLI commands of console, please refer Appendix A. |
| 2 | SSH Telnet | You can login DFL-1500 using SSH or telnet method multiple times remotely. This is useful while you are trying to debug the network problem using the CLI commands "tcpdump". The priority of SSH is equal with telnet method. For the CLI commands of SSH/Telnet, please refer Appendix A. |
| 3 | HTTPS HTTP | The priority of HTTPS is equal with HTTP. |

Table 5-2 Priorities of login method

5.4 Steps

5.4.1 Telnet

Step 1. Setup Telnet

Enter 23 instead of the default 2323 in the Server Port field. Check the WAN1 checkbox. Click the Selected of Secure Client IP Address, and then enter the specified IP address (140.2.5.1) for accessing DFL-1500. And click the Apply.

SYSTEM TOOLS > Remote Mgt. > TELNET

5.4.2 SSH

Step 1. Setup SSH

Enter 22 in the Server Port field. Check the LAN1/LAN2 checkbox. Click the ALL of Secure Client IP Address for accessing DFL-1500. And click the Apply.

SYSTEM TOOLS > Remote Mgt. > SSH

5.4.3 WWW

Step 1. Setup WWW

Check the LAN1 checkbox, and enter the new Server Port 8080 that will be accessed by the user's browser (http://192.168.40.254:8080). In the Secure Client IP Address field, we select the specified IP address "192.168.40.2". And click the Apply button.

Note that the Secure Client IP Address is the IP address which can be used to configure DFL-1500.

SYSTEM TOOLS > Remote Mgt. > WWW



✓ Warning message

If you click the Selected of Secure Client IP Address and then enter the specified IP address which is not the same as current login IP address, a warning message will appear to notice you that "Warning! If you are connecting to this Firewall with WWW, this action may disconnect your session. Please remember the settings and reconnect to the firewall again." after applying the settings.

5.4.4 HTTPS

Step 1. Setup HTTPS

Check the WAN1/LAN1/LAN2 checkbox, and enter the new Server Port 443 that will be accessed by the user's browser (https://192.168.40.254). Here we click All for all no IP range limitation of clients. And click the Apply button.

SYSTEM TOOLS > Remote Mgt. > HTTPS

Server Port: 443
Allow Access to IP on port: WAN1 WAN2 DMZ1 LAN1 LAN2
Secure Client IP Address: All Selected 0.0.0.0
Apply

5.4.5 SNMP

Step 1. Setup SNMP

Check the LAN1/LAN2 checkbox. In the Secure Client Address field. If you prefer indicated specified IP address. Just click the Selected, and enter the valid IP address for reading the SNMP MIBs at the DFL-1500. Finally click the Apply button.

SYSTEM TOOLS > Remote Mgt. > SNMP

Server Port: 161
Allow Access to IP on port: WAN1 WAN2 DMZ1 LAN1 LAN2
Secure Client IP Address: All Selected 0.0.0.0
Apply

5.4.6 ICMP

Step 1. Setup ICMP

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

SYSTEM TOOLS > Remote Mgt. > MISC

Respond to Ping on: WAN1 WAN2 DMZ1 LAN1 LAN2
Apply

Chapter 6

Authentication

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

6.1 Demands

DFL-1500 VPN/Firewall Router supports user authentication against the internal user database, a RADIUS server or a LDAP server. You can create a user account by adding username and password to the internal database to grant the user an access to Internet, etc. Alternatively, you may input the IP address of a Radius server to let users to be authenticated using the server database.

6.2 Methods

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

1. If PCs under LAN interfaces cannot pass the authentication, they will not be allowed to access WAN, LAN and DMZ resources.
2. If PCs like servers are located under DMZ, the authentication is not necessary.
3. If you put a server under LAN, you have to add its IP address to the Exempt Host list in order to access its resources.

There are four steps to configure the authentication:

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

6.3 Steps

6.3.1 Local Setting

Step 1. Enable Authentication

Check the `Enable Authentication` checkbox. Set Authentication timeout to control how long authenticated firewall connections are valid. Select the Authentication Type.

Basic Setup > Authentication > Authentication

Authentication Exempt Host

Enable Authentication

Timeout(min)

60

Authentication Type

Local Pop3(s) Imap(s) Radius LDAP

LOCAL Setting

Username: susan

Password: ****

tom

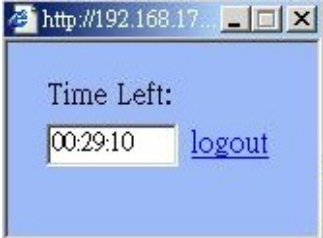
Add

Delete

Apply

Part II

Basic Configuration

| | |
|--|---|
| <p>Step 2. Configure Local Settings</p> <p>Enter the Username and Password, and then click Add to add it to user's list. If you would like to delete a user, just click that username and then click Delete to remove it. Click Apply to finish the settings.</p> | <p>Basic Setup > Authentication > Authentication > Local</p> <p>Authentication Exempt Host</p> <p><input checked="" type="checkbox"/> Enable Authentication</p> <p>Timeout(min) <input type="text" value="60"/></p> <p>Authentication Type <input checked="" type="radio"/> Local <input type="radio"/> Pop3(s) <input type="radio"/> Imap(s) <input type="radio"/> Radius <input type="radio"/> LDAP</p> <p>LOCAL Setting</p> <p>Username: <input type="text" value="susan"/></p> <p>Password: <input type="password" value="****"/></p> <p><input type="text" value="tom"/> <input type="button" value="Add"/></p> <p><input type="button" value="Delete"/></p> <p><input type="button" value="Apply"/></p> |
| <p>Step 3. Show the Authentication</p> <p>After applying Local setting, there will be an Authentication dialog to ask you to enter the Username and Password when you would like to connect to the internet. And then click Login.</p> | <p>Authentication</p> <p>Username: <input type="text" value="tom"/></p> <p>Password: <input type="password" value="●●●●"/></p> <p><input type="button" value="Login"/></p> |
| <p>Step 4. Show the time left</p> <p>When you pass the authentication, a message box will appear to tell you how long the connection will remain.</p> |  |

6.3.2 Pop3(s) Setting

| | |
|--|--|
| <p>Step 1. Configure Pop3(s) Settings</p> <p>Click Authentication Type as Pop3(s). Enter Server IP and Server Port. Check the Encryption as SSL if the server port is 995 (Pop3s). Click Apply to store the settings.</p> | <p>Basic Setup > Authentication > Authentication > Pop3(s)</p> <p>Authentication Exempt Host</p> <p><input checked="" type="checkbox"/> Enable Authentication</p> <p>Timeout(min) <input type="text" value="60"/></p> <p>Authentication Type <input type="radio"/> Local <input checked="" type="radio"/> Pop3(s) <input type="radio"/> Imap(s) <input type="radio"/> Radius <input type="radio"/> LDAP</p> <p>POP3(s) Setting</p> <p>Server IP <input type="text" value="10.1.1.1"/></p> <p>Server Port <input type="text" value="110"/></p> <p>Encryption <input type="checkbox"/> SSL</p> <p><input type="button" value="Apply"/></p> |
|--|--|

| FIELD | DESCRIPTION | EXAMPLE |
|-----------|---------------------------------------|----------|
| Server IP | The IP address of the POP3(s) server. | 10.1.1.1 |

| | | |
|-------------|--|----------|
| Server Port | The port which the data goes into or out of the POP3(s) server. For instance, POP3 service uses port 110 and POP3s service uses port 995. | 110 |
| Encryption | Encryption is the process of changing data into a form that can be read only by the intended receiver. Secured Sockets Layer is a protocol that transmits your communications over the Internet in an encrypted form. It ensures that the information is sent, unchanged, only to the server you intended to send it to. Therefore, if you use port 995 (POP3s) as your server port, you have to check SSL checkbox. | Disabled |

Table 6-1 POP3(s) Settings

6.3.3 Imap(s) Setting

| | |
|--|--|
| <p>Step 1. Configure Imap(s) Settings</p> <p>Click Authentication Type as Imap(s). Enter Server IP and Server Port. Check the Encryption as SSL. Click Apply to store the settings. Note, if you enter server port as 143 (IMAP), don't check the SSL checkbox.</p> | <p>Basic Setup > Authentication > Authentication > Imap(s)</p> <p>Authentication Exempt Host</p> <p><input checked="" type="checkbox"/> Enable Authentication</p> <p>Timeout(min) <input type="text" value="60"/></p> <p>Authentication Type <input type="radio"/> Local <input type="radio"/> Pop3(s) <input checked="" type="radio"/> Imap(s) <input type="radio"/> Radius <input type="radio"/> LDAP</p> <p>IMAP Setting</p> <p>Server IP <input type="text" value="10.1.1.1"/></p> <p>Server Port <input type="text" value="993"/></p> <p>Encryption <input checked="" type="checkbox"/> SSL</p> <p><input type="button" value="Apply"/></p> |
|--|--|

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

Table 6-2 IMAP(s) Settings

6.3.4 Radius Setting

Step 1. Configure Radius Settings

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the DFL-1500 then will contact the RADIUS server for authentication.

Click Authentication Type as Radius. Enter Server IP/Server Port and enter the RADIUS Server Secret. Click Apply to store the settings.

Basic Setup > Authentication > Authentication > Radius

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

Table 6-3 RADIUS Settings

6.3.5 LDAP Setting

Step 1. Configure LDAP Settings

If you have configured LDAP support and a user is required to authenticate using a LDAP server, the DFL-1500 will then contact the LDAP server for authentication. To authenticate with the DFL-1500, the user enters a username and password. The DFL-1500 sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the DFL-1500.

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

Basic Setup > Authentication > Authentication > LDAP

| FIELD | DESCRIPTION | EXAMPLE |
|-----------|---|--|
| Server IP | The IP address of the LDAP server. | 192.168.40.66 |
| Base DN | The distinguished name used to look up entries on the LDAP server. For example: | ou=people, dc=yourcompany, dc=com, dc=tw |

| | | |
|------------|--|------------|
| | <p>In OpenLDAP: entry1: uid=mary,ou=people,dc= yourcompay,dc=com entry2: uid=jack,ou=people,dc= yourcompay,dc=com Base DN: ou=people,dc=yourcompany,dc=com UID : uid</p> <p>In Windows AD (special case): entry1: cn=mary,dc= yourcompay,dc=com entry2: cn=jack ,dc= yourcompay,dc=com Base DN: cn=Users,dc=yourcompany,dc=com UID: cn</p> | |
| <p>UID</p> | <p>UID is the field name and used to look up entries on LDAP server. Please refer to the above description.</p> | <p>uid</p> |

Table 6-4 LDAP Settings

6.3.6 Exempt Host

| | |
|--|---|
| <p>Step 1. Configuring the Exempt Host Enter the exempt host IP Address, and click Add to add an IP address. When enabling authentication, the chosen PC IP address will pass the authentication.</p> | <p>Basic Setup > Authentication > Exempt Host</p> <p><u>Authentication Exempt Host</u></p> <p>When enable Authentication, it will pass Authentication with following IP hosts:</p> <p>IP Address: <input type="text" value="10.1.1.1"/> (Ex: 127.0.0.1) <input type="text" value="192.168.17.1"/> <input type="button" value="Add"/> <input type="button" value="Delete"/></p> |
|--|---|

Part III

NAT & Routing

Chapter 7

NAT

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

To facilitate the explanation on how DFL-1500 implements NAT and how to use it, we zoom in the left part of Figure 1-10 into Figure 7-1.

7.1 Demands

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

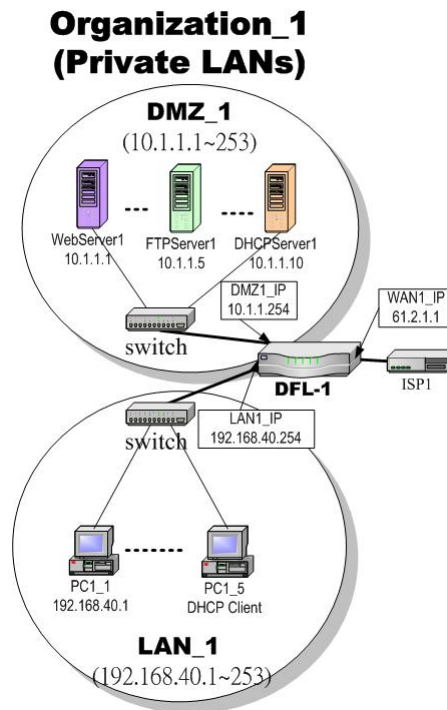


Figure 7-1 All the internal PCs can connect internet through limited WAN IP address by using NAT technology

2. Internet servers provided by your company may open many ports by default that may be dangerous if exposed to the public Internet. As the Figure 7-2 illustrated, we make the real servers hide behind the DFL-1500. And all the internet clients can still access the service of servers.

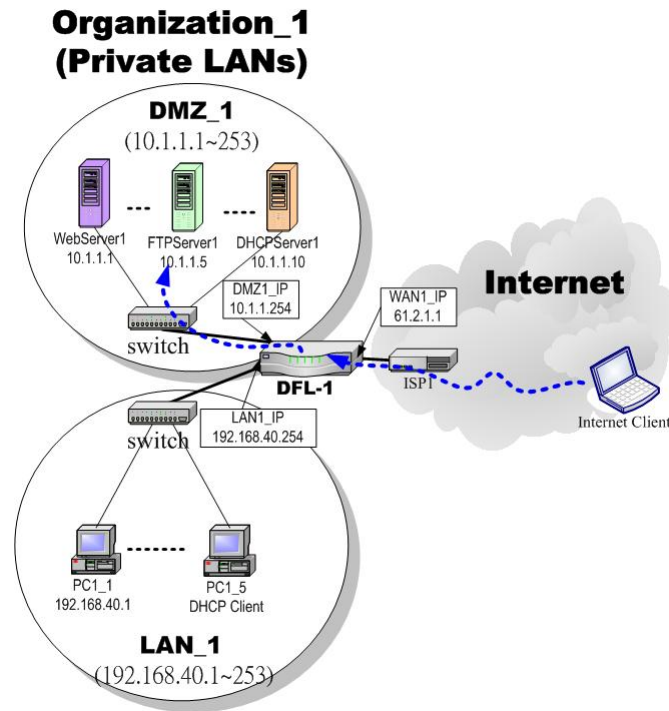


Figure 7-2 Internet clients can access the server behind the DFL-1500

7.2 Objectives

1. Let PC1_1~PC1_5 connect to the Internet.
2. As the Figure 7-2 illustrated, the clients will connect to the DFL-1500. Then DFL-1500 will forward the packet to the real server. So FTPServer1 (10.1.1.5) will be accessed by other Internet users.

7.3 Methods

1. Assign private IP addresses to the PC1_1~PC1_5. Setup NAT at DFL-1500 to map those assigned private hosts under LAN1 to the public IP address WAN1_IP at the WAN1 side.
2. Assign a private IP address to the FTPServer1. Setup Virtual Server at DFL-1500 to redirect “any connections towards some port of WAN1” to the port 21 at the FTPServer1.

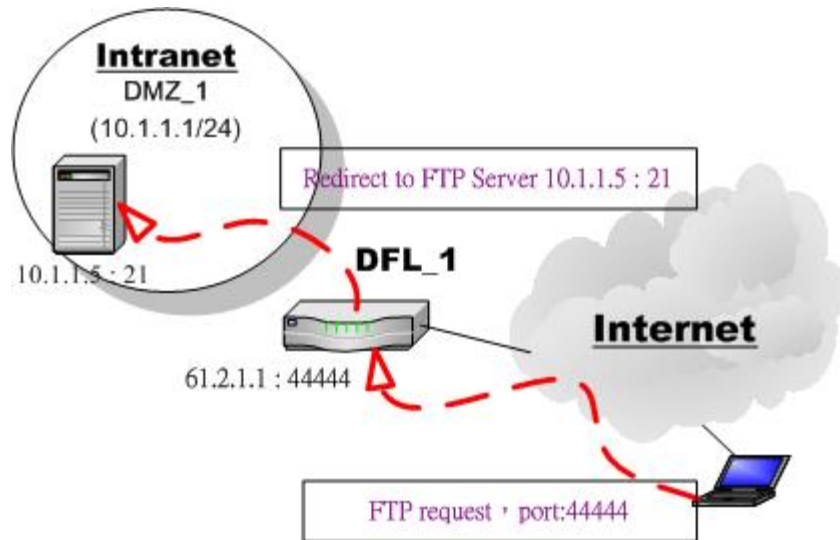


Figure 7-3 DFL-1500 plays the role as Virtual Server

As the above Figure 7-3 illustrates, the server 10.1.1.5 provides FTP service. But it is located at the DMZ region behind DFL-1500. And DFL-1500 will act as a Virtual Server role which redirects the packets to the real server 10.1.1.5. And you can announce to the internet users that there exists a ftp server IP/port is 61.2.1.1/44444. So, all the internet users will just connect the 61.2.1.1/44444 to get ftp service.

The feature of Virtual Server can only be available while DFL-1500 connects to the internet via DEFAULT WAN link.

7.4 Steps

7.4.1 Setup Many-to-one NAT rules

Step 1. Enable NAT

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

ADVANCED SETTINGS > NAT > Status

Status **NAT Rules** **Virtual Servers**

Network Address Translation Mode: Basic

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

- Internal-to-External traffic:** map the conditioned internal IPs/ports into the specified external IPs/ports.
Reset NAT rules
- External-to-Internal traffic:** map the conditioned external IPs/ports into the specified internal IPs/ports.
Reset Server rules

Modes:

- None: The DFL-1500 is in routing mode without performing any address translation.
- Basic: The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnet IP ranges.
- Full Feature: The DFL-1500 performs routing and NAT simultaneously. It performs several kinds of NAT on the conditioned IP subnet, while performing routing on other IP subnets.

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

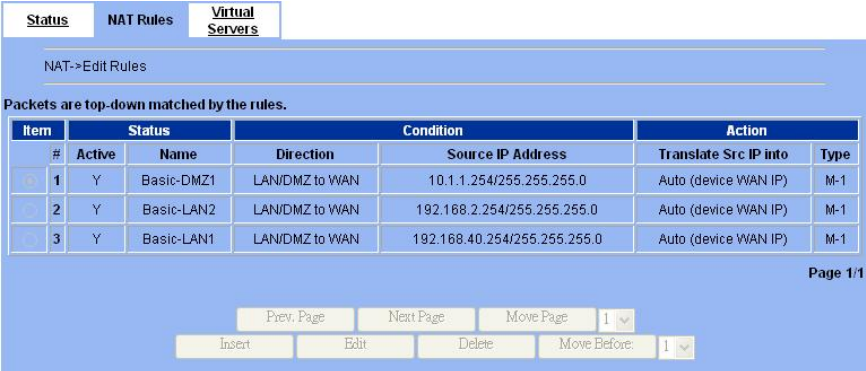
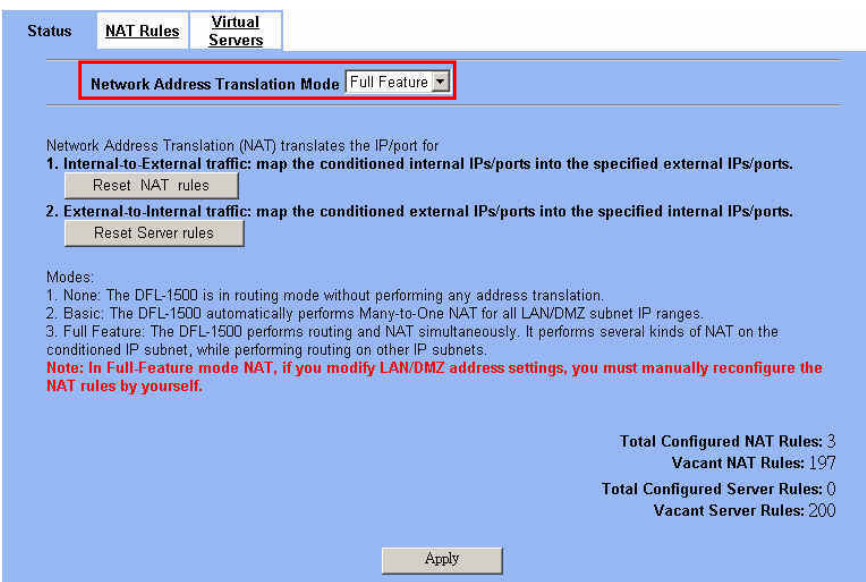
Apply

Part III

NAT & Routing

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|----------------------------------|---|-----------------------------------|---------|
| Network Address Translation Mode | Determine what NAT type you are using in your network topology. Refer more information in the section 7.5.5. | None / Basic / Full Feature | Basic |
| BUTTON | DESCRIPTION | | |
| Reset NAT Rules | Reset NAT rules to the default status | | |
| Reset Server Rules | Clear all the Virtual Server rules. | | |
| Apply | Apply the settings which have been configured. | | |

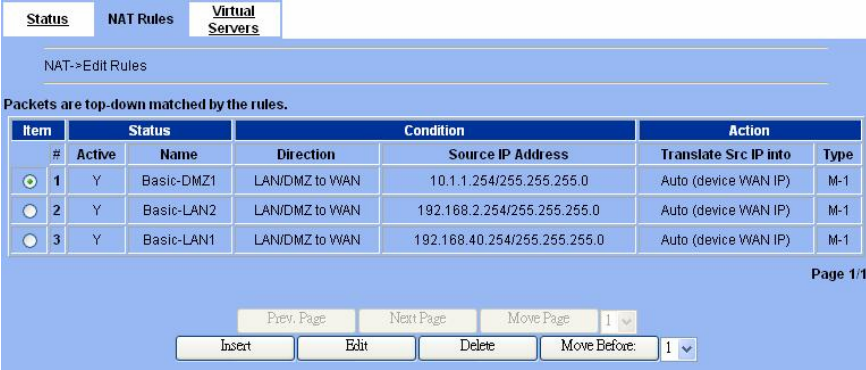
Table 7-1 Determine Network Address Translation Mode

| | |
|---|---|
| <p>Step 2. Check NAT Rules</p> <p>As described in the previous sections, the DFL-1500 has set the rules for the LAN/DMZ zones. They all belong to the Many-to-One (M-1) type that will map many private addresses to the automatically chosen public IP address. When the WAN interfaces change the IP, these rules do not require any manual modifications for the changed public IP addresses. The rules will reload the new settings automatically. Besides, you cannot insert/edit any rules under the Basic mode.</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-1500. If you change the LAN/DMZ IP settings, you have to manually update related rules by yourself. Otherwise, hosts in your LAN/DMZ cannot establish connections to the hosts in the WAN side.</p> | <p>ADVANCED SETTINGS > NAT > Status</p>  |

Step 4. Customize NAT Rules

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

ADVANCED SETTINGS > NAT > NAT Rules



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

| Item # | Status | Name | Direction | Source IP Address | Translate Src IP into | Type |
|--------|--------|------------|----------------|------------------------------|-----------------------|------|
| 1 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 |
| 2 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) | M-1 |
| 3 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.40.254/255.255.255.0 | Auto (device WAN IP) | M-1 |

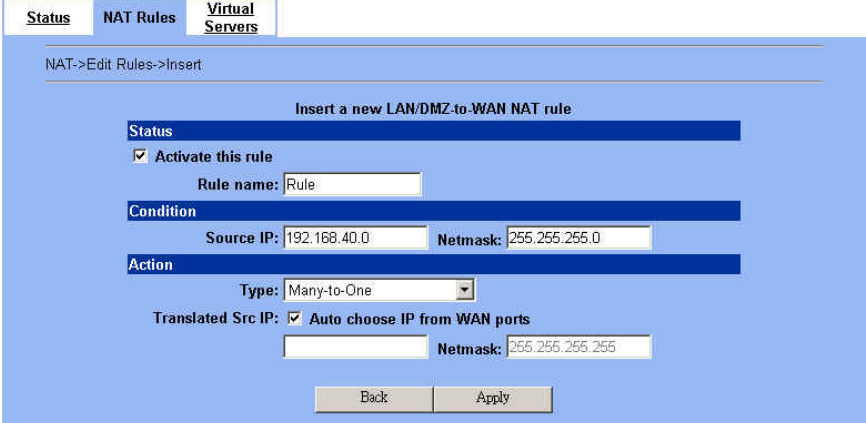
At the bottom of the table, there are navigation buttons: 'Prev. Page', 'Next Page', 'Move Page', and a dropdown menu showing '1'. Below the table, there are buttons for 'Insert', 'Edit', 'Delete', and 'Move Before:' with a dropdown menu showing '1'.

Step 5. Insert NAT Rule

Step 5.a — Insert an Many-to-One Rule

As described in the above, Many-to-One NAT is the default NAT rule type in the Basic mode. If you have other alias LAN/DMZ subnets, you can manually add a Many-to-One NAT rule for them. First select the Type as Many-to-One, check the Activate this rule, enter a Rule name for this rule, enter the private-IP subnet (an IP address with a netmask) to be translated, and enter the public IP address for being translated into. You can check the Auto choose IP from WAN ports. The DFL-1500 will automatically determine which WAN IP is to be translated into.

ADVANCED SETTINGS > NAT > NAT Rules > Insert



The screenshot shows the 'Insert' configuration page for a Many-to-One NAT rule. The page title is 'NAT->Edit Rules->Insert'. The main heading is 'Insert a new LAN/DMZ-to-WAN NAT rule'. The configuration is divided into three sections:

- Status:** Includes a checked checkbox for 'Activate this rule' and a text input field for 'Rule name' containing 'Rule'.
- Condition:** Includes input fields for 'Source IP' (192.168.40.0) and 'Netmask' (255.255.255.0).
- Action:** Includes a dropdown menu for 'Type' set to 'Many-to-One', a checked checkbox for 'Translated Src IP: Auto choose IP from WAN ports', and input fields for 'Netmask' (255.255.255.255).

At the bottom, there are 'Back' and 'Apply' buttons.

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

Table 7-2 Add a NAT rule

Step 5.b — Insert an Many-to-Many Rule

If your ISP has assigned a range of public IP to your company, you can tell DFL-1500 to translate the private IP addresses into the pool of public IP addresses. The DFL-1500 will use the first public IP until DFL-1500 uses up all source ports for the public IP. DFL-1500 will then choose the second public IP from the address pool. Select Many-to-Many from the Type. Enter the subnet with an IP address and a netmask. Other fields are the same with those of Many-to-One rules. However, the DFL-1500 will no longer choose the device IP for you. It will choose the IP from the address pool you have entered.

ADVANCED SETTINGS > NAT > NAT Rules > Insert

The screenshot shows the 'NAT Rules > Insert' configuration page. It has three tabs: 'Status', 'NAT Rules', and 'Virtual Servers'. The 'NAT Rules' tab is active. The page title is 'NAT->Edit Rules->Insert'. Below the title, it says 'Insert a new LAN/DMZ-to-WAN NAT rule'. There are three main sections: 'Status', 'Condition', and 'Action'. In the 'Status' section, 'Activate this rule' is checked. The 'Rule name' field contains 'Rule'. In the 'Condition' section, 'Source IP' is '192.168.40.0' and 'Netmask' is '255.255.255.0'. In the 'Action' section, 'Type' is set to 'Many-to-Many'. There is an unchecked checkbox for 'Auto choose IP from WAN ports'. Below it, 'Translated Src IP' is '61.2.1.1' and 'Netmask' is '255.255.255.252'. At the bottom, there are 'Back' and 'Apply' buttons.

Step 5.c — Insert an One-to-One Rule

Though you may have many public IP address for translation, you may want to make some private IP to always use a public IP. In this case, you can select One-to-One from the Type, and enter the private-public IP address pair in the Source IP and the Translated Source IP fields.

ADVANCED SETTINGS > NAT > NAT Rules > Insert

The screenshot shows the 'NAT Rules > Insert' configuration page. It has three tabs: 'Status', 'NAT Rules', and 'Virtual Servers'. The 'NAT Rules' tab is active. The page title is 'NAT->Edit Rules->Insert'. Below the title, it says 'Insert a new LAN/DMZ-to-WAN NAT rule'. There are three main sections: 'Status', 'Condition', and 'Action'. In the 'Status' section, 'Activate this rule' is checked. The 'Rule name' field contains 'Rule'. In the 'Condition' section, 'Source IP' is '192.168.40.0' and 'Netmask' is '255.255.255.255'. In the 'Action' section, 'Type' is set to 'One-to-One'. There is an unchecked checkbox for 'Auto choose IP from WAN ports'. Below it, 'Translated Src IP' is '61.2.1.1' and 'Netmask' is '255.255.255.255'. At the bottom, there are 'Back' and 'Apply' buttons.

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

The above three modes allow LAN/DMZ-to-WAN sessions establishment but do not allow WAN-to-LAN/DMZ sessions. WAN-to-LAN/DMZ sessions are allowed by Virtual Server rules. You can make the One-to-One NAT in the above to incorporate the WAN-to-LAN/DMZ feature by selecting the One-to-One (Bidirectional) from the Type. Note that WAN-to-LAN/DMZ traffic will be blocked by the Firewall by default. You have to add a Firewall rule to allow such traffic. If you expect a LAN/DMZ host to be fully accessed by public Internet users, use this mode. Note that this mode is extremely dangerous because the host is fully exposed to the Internet and may be cracked. Always use Virtual Server rules first.

ADVANCED SETTINGS > NAT > NAT Rules > Insert

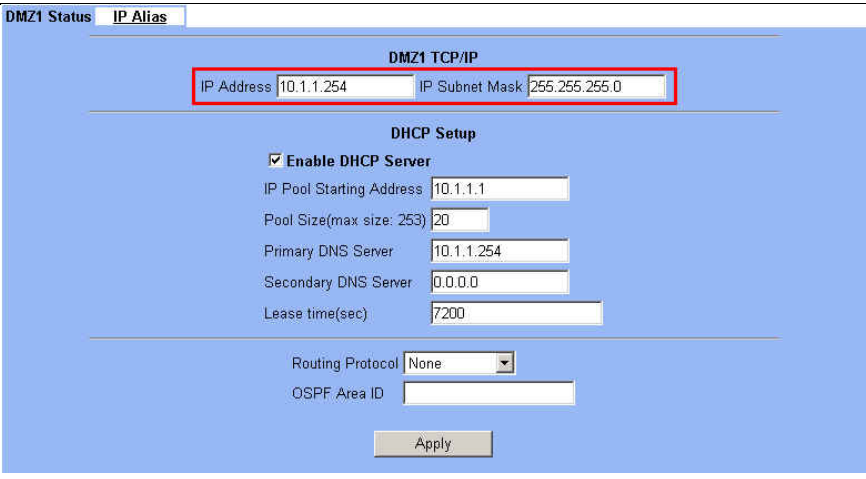
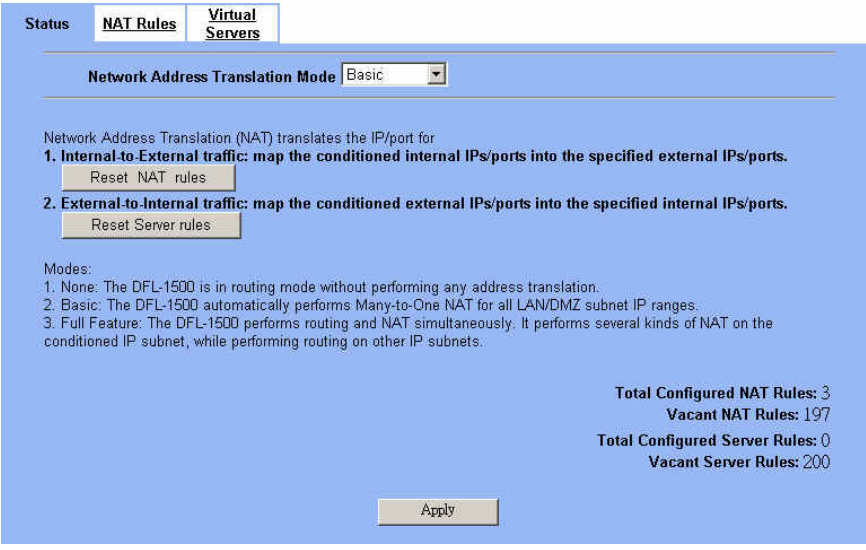
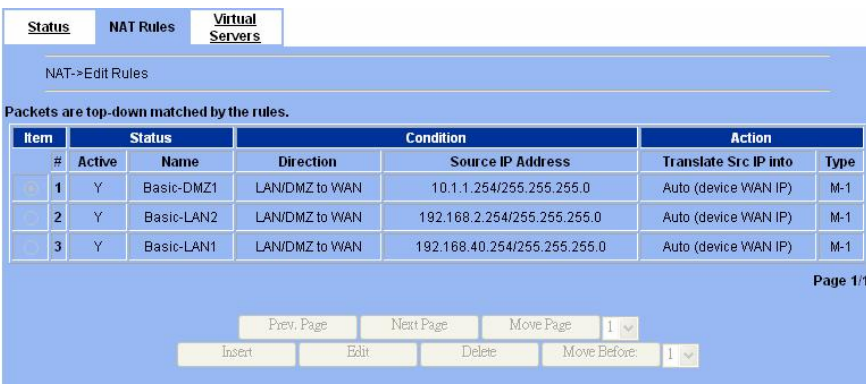
The screenshot shows the 'NAT Rules > Insert' configuration page. It has three tabs: 'Status', 'NAT Rules', and 'Virtual Servers'. The 'NAT Rules' tab is active. The page title is 'NAT->Edit Rules->Insert'. Below the title, it says 'Insert a new LAN/DMZ-to-WAN NAT rule'. There are three main sections: 'Status', 'Condition', and 'Action'. In the 'Status' section, 'Activate this rule' is checked. The 'Rule name' field contains 'Rule'. In the 'Condition' section, 'Source IP' is '192.168.40.0' and 'Netmask' is '255.255.255.255'. In the 'Action' section, 'Type' is set to 'One-to-One (bidirectional)'. There is an unchecked checkbox for 'Auto choose IP from WAN ports'. Below it, 'Translated Src IP' is '61.2.1.1' and 'Netmask' is '255.255.255.255'. At the bottom, there are 'Back' and 'Apply' buttons.

7.4.2 Setup Virtual Server for the FtpServer1

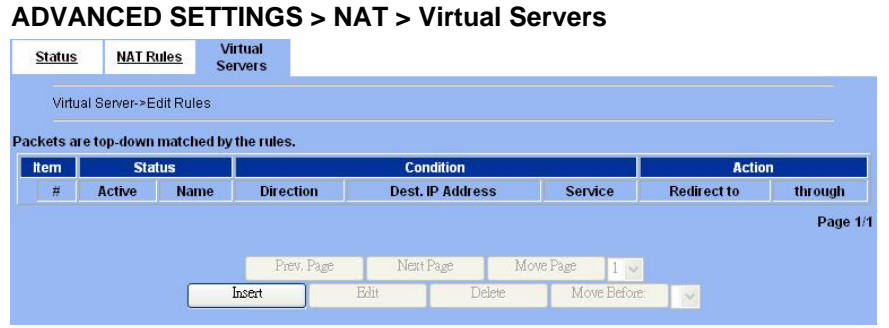
Step 1. Device IP Address

Setup the IP Address and IP Subnet Mask for the DFL-1500 of the DMZ1 interface.

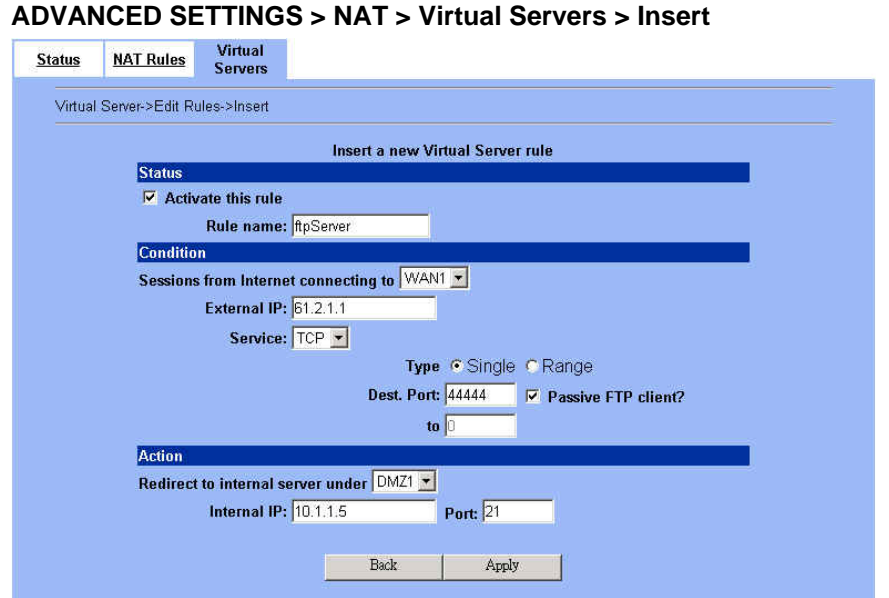
BASIC SETUP > DMZ Settings > DMZ1 Status

| <p>Step 2. Client IP Range Enable the DHCP server if you want to use DFL-1500 to assign IP addresses to the computers under DMZ1. Here we make the DHCP feature enabled.</p> |  | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|--|----------------|------------------------------|--------------------------|-----------|--------|---|---|------------|----------------|--------------------------|--------------------------|---|---|------------|----------------|-----------------------------|--------------------------|---|---|------------|----------------|------------------------------|--------------------------|
| <p>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 the rules to let all private-IP LAN/DMZ-to-WAN 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-1500 has added the NAT rules automatically as right diagram described. The rule Basic-DMZ1 (number 1) means that, when matching the condition (requests of LAN/DMZ-to-WAN direction with its source IP falling in the range of 10.1.1.254/255.255.255.0), the request will be translated into a public-source-IP requests, and then be forwarded to the destinations.</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> </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) M-1</td> </tr> <tr> <td>2</td> <td>Y</td> <td>Basic-LAN2</td> <td>LAN/DMZ to WAN</td> <td>192.168.2.254/255.255.255.0</td> <td>Auto (device WAN IP) M-1</td> </tr> <tr> <td>3</td> <td>Y</td> <td>Basic-LAN1</td> <td>LAN/DMZ to WAN</td> <td>192.168.40.254/255.255.255.0</td> <td>Auto (device WAN IP) M-1</td> </tr> </tbody> </table> | Item | Status | Name | Direction | Condition | Action | 1 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) M-1 | 2 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) M-1 | 3 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.40.254/255.255.255.0 | Auto (device WAN IP) M-1 |
| Item | Status | Name | Direction | Condition | Action | | | | | | | | | | | | | | | | | | | | |
| 1 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) M-1 | | | | | | | | | | | | | | | | | | | | |
| 2 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) M-1 | | | | | | | | | | | | | | | | | | | | |
| 3 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.40.254/255.255.255.0 | Auto (device WAN IP) M-1 | | | | | | | | | | | | | | | | | | | | |
| <p>Step 6. Setup IP for the FTP Server Assign an IP of 10.1.1.1/255.255.255.0 to the FTP server under DMZ1. Assume the FTP Server is at 10.1.1.5. And it is listening on the well-known port (21).</p> | <p>N/A</p> | | | | | | | | | | | | | | | | | | | | | | | | |

Step 7. Setup Server Rules
Insert a virtual server rule by clicking the Insert button.



Step 8. Customize the Rule
Customize the rule name as the ftpServer. For any packets with its destination IP equaling to the WAN1 IP (61.2.1.1) and destination port equaling to 44444, ask DFL-1500 to translate the packet's destination IP/port into 10.1.1.5/21. Check the Passive FTP client? to maximize the compatibility of the FTP protocol. This is useful if you want to provide connectivity to passive FTP clients. For passive FTP clients, the server will return them the private IP address and the port number for them to connect back to do data transmissions. Since the private IP from them cannot be routed to our zone, the data connections will fail. After enabling this feature, the DFL-1500 will translate the private IP/port into an IP/port of its own. Thus the problem is gracefully solved. Click Apply to proceed.



Note after setting the Virtual Server rule, please adjust your corresponding firewall/NAT rules manually. Or the virtual server will work improperly.

| | FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------|--------------------------------------|--|--------------------|-----------|
| Status | Activate this rule | Activate the Virtual Server rule. | Enabled / Disabled | Enabled |
| | Rule name | The Virtual Server rule name | text string | ftpServer |
| Condition | Sessions from Internet connecting to | Which interface does the connected session come from? | WAN interfaces | WAN1 |
| | External IP | The public IP address of the Virtual Server. | IPv4 format | 61.2.1.1 |
| | Service | The service which is provided by the real server. | TCP / UDP | TCP |
| | Type | Port is Single or Range | Single / Range | Single |
| | Dest Port | The TCP/UDP port number which is provided by the real server. | 1 ~65534 | 44444 |
| | Passive FTP client | If the Passive FTP client is checked, it will connect to the internal DMZ FTP server of DFL-1500 when FTP client uses passive mode. Otherwise, it will not work. | Enabled / Disabled | Enabled |

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

Table 7-3 Add a Virtual Server rule

Step 9. View the Result

Now any request towards the DFL-1500's WAN1 IP (61.2.1.1) with port 44444 will be translated into a request towards 10.1.1.5 with port 21, and then be forwarded to the 10.1.1.5. The FTP server listening at port 21 in 10.1.1.5 will pick up the request.

ADVANCED SETTINGS > NAT > Virtual Servers

Status NAT Rules **Virtual Servers**

Virtual Server->Edit Rules

Packets are top-down matched by the rules.

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

Page 1/1

1

7.5 NAT modes introduction

7.5.1 Many-to-One type

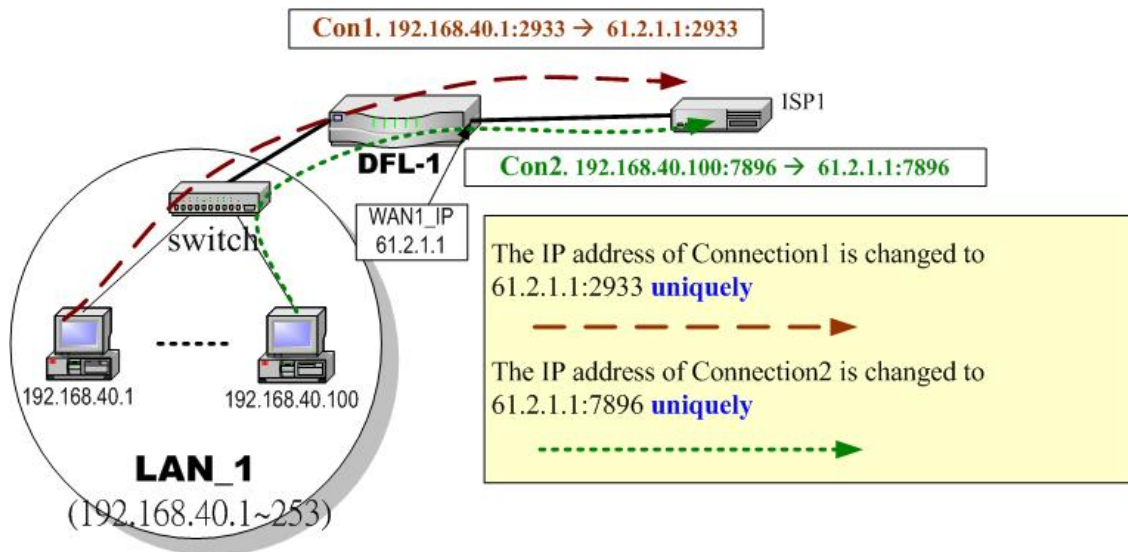


Figure 7-4 NAT Many-to-One type

As the above Figure 7-4 illustrated, NAT Many-to-One type means that many local PCs are translated into only one public IP address when the packets are forwarded out through the DFL-1500. Take Connection1 for example. Its IP address and port are

translated from 192.168.40.1:2933 to 61.2.1.1:2933. In the same way, when the packets of Connection2 are forwarded out, its IP address is still translated to the same public IP address (61.2.1.1:7896).

7.5.2 Many-to-Many type

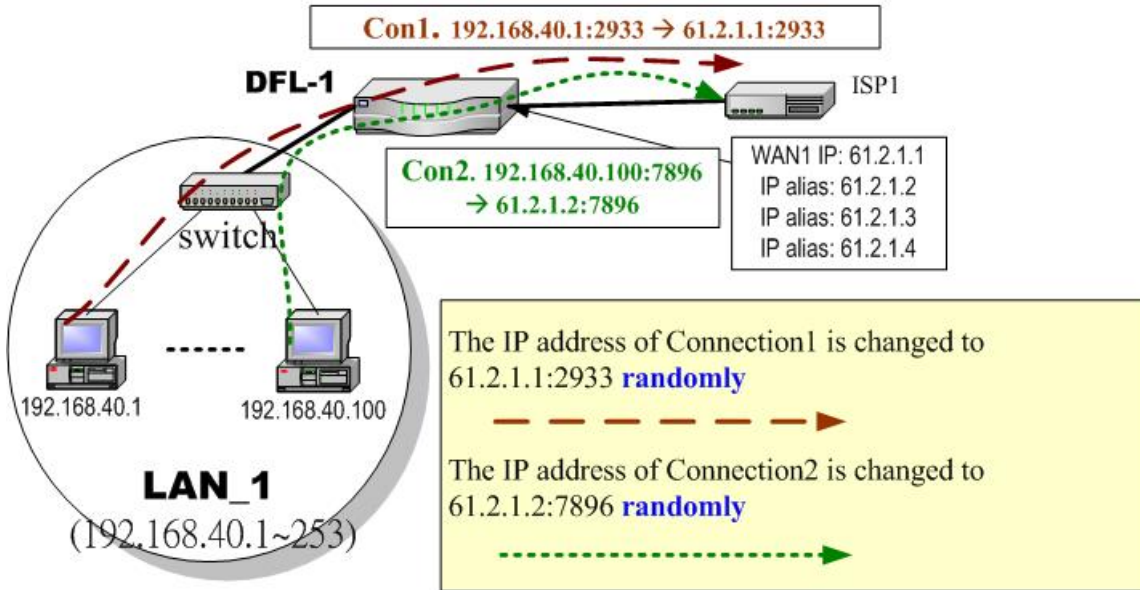


Figure 7-5 NAT Many-to-Many type

As the above Figure 7-5 illustrated, NAT Many-to-Many type means that many local PCs are translated into multiple public IP addresses when the packets are forwarded out through the DFL-1500. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933. Until DFL-1500 uses out of all source ports of the public (61.2.1.1), DFL-1500 will then choose the second public IP (such as 61.2.1.2) from the address pool. For example, Connection2 are forwarded out, the source IP address will be translated into the second public IP address (61.2.1.2) from the public IP address pools. So the translated IP address (61.2.1.2:7896) is different from Connection1 one (61.2.1.1:2933).

7.5.3 One-to-One type

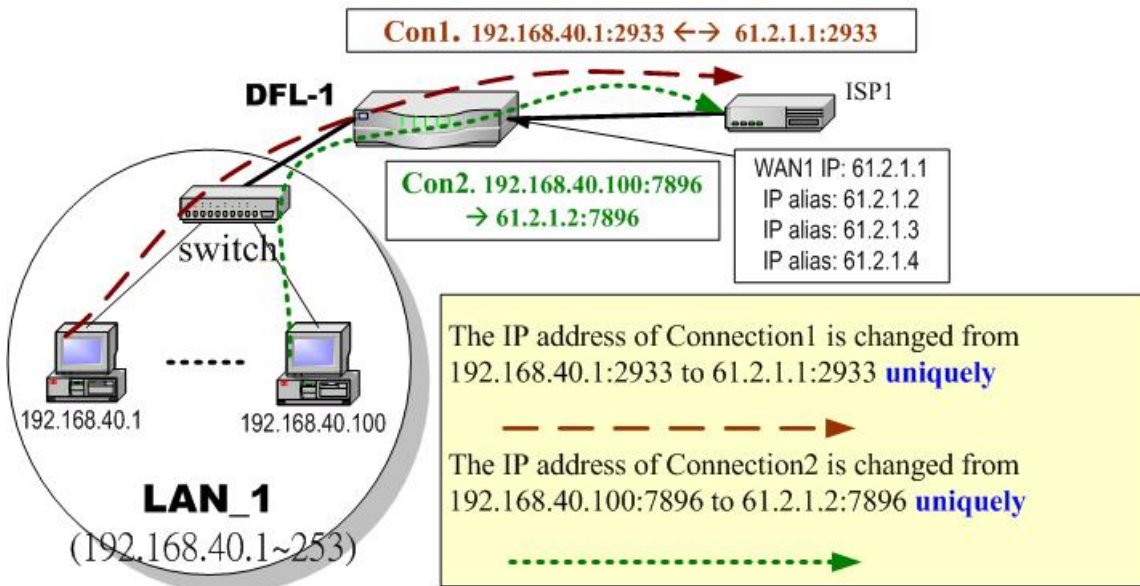


Figure 7-6 NAT One-to-One type

As the above Figure 7-6 illustrated, NAT One-to-One type means that each local PC is translated into a unique public IP address when the packets are forwarded out through the DFL-1500. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933. But, when the packets of Connection2 are forwards out, the source IP address is translated to another dedicated public IP address(61.2.1.2:7896).

7.5.4 One-to-One (bidirectional) type

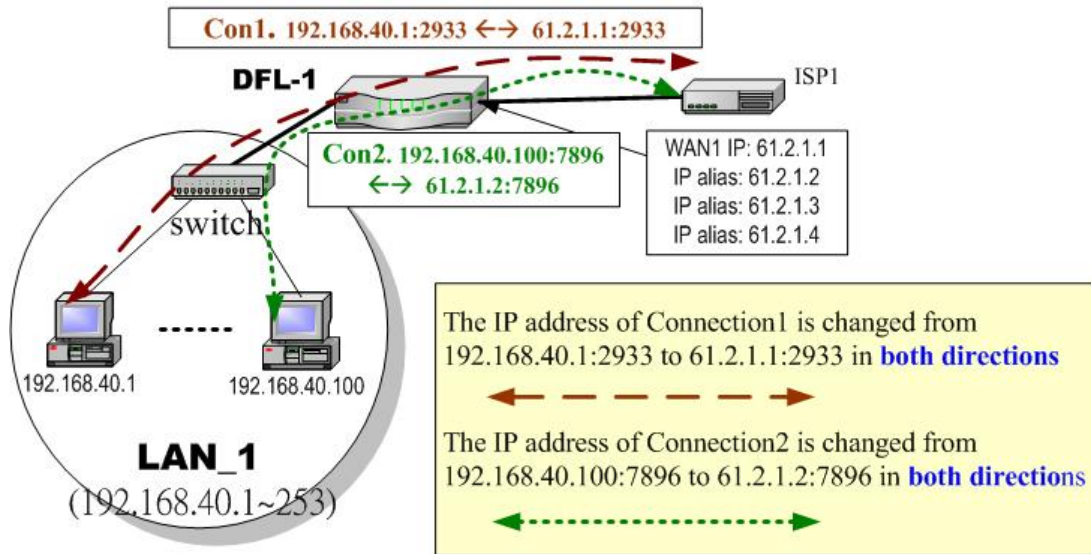


Figure 7-7 NAT One-to-One (bidirectional) type

As the above Figure 7-7 illustrated, NAT One-to-One (bidirectional) type means that each local PC is translated into a unique public IP address when the packets are forwarded out through the DFL-1500. Besides, when packets came from internet to LAN, they were translated to the same private IP address too. Take Connection1 for example. Its IP address and port are translated from 192.168.40.1:2933 to 61.2.1.1:2933 in both ways. Accordingly, the source IP address and port of the Connection2 are translated from 192.168.40.100:7896 to 61.2.1.2:7896 in both ways.

7.5.5 NAT modes & types

The following three NAT modes are supported by DFL-1500 now as the following Table 7-4.

| NAT mode | Description |
|--------------|--|
| None | If you choose this mode, the DFL-1500 will act as a pure router without performing any address translation. |
| Basic | The DFL-1500 automatically performs Many-to-One NAT for all LAN/DMZ subnets. All IP addresses with outgoing packets will be translated to the IP address of default WAN link automatically. |
| Full Feature | The DFL-1500 can be manually configured with Many-to-One, and Many-to-Many, One-to-One, and bidirectional One-to-One rules to do policy-based NAT. Here policy-based NAT means that you can fully decide which zone (LAN, DMZ) will do the IP NAT and which zone (LAN, DMZ) will just do the pure IP routing without IP translation. |

Table 7-4 NAT modes overview

Part III

NAT & Routing

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

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

Table 7-5 The NAT type comparison

Chapter 8

Routing

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

To facilitate the explanation on how DFL-1500 implements routing and how to use it. We zoom in the left part of Figure 2-1 into Figure 8-1 and increase some devices for description.

8.1 Demands

1. There is only one local area (192.168.40.0/24) inside the LAN1 port. Now there is a new financial area (192.168.50.0/24) in the Figure 8-1. The financial area is connected with a router which is inside the LAN1 port of DFL-1500. So we need to add the configurations for the financial department.
2. Refer to the Figure 8-1 description. The bandwidth subscribed from ISP1 is insufficient so that some important traffic, say the traffic from PCs belonging to the General-Manager-Room department (192.168.40.192/255.255.255.192), is blocked by the other traffic. We hope that the employees of General-Manager-Room can have a dedicated bandwidth to improve the quality of connecting internet.

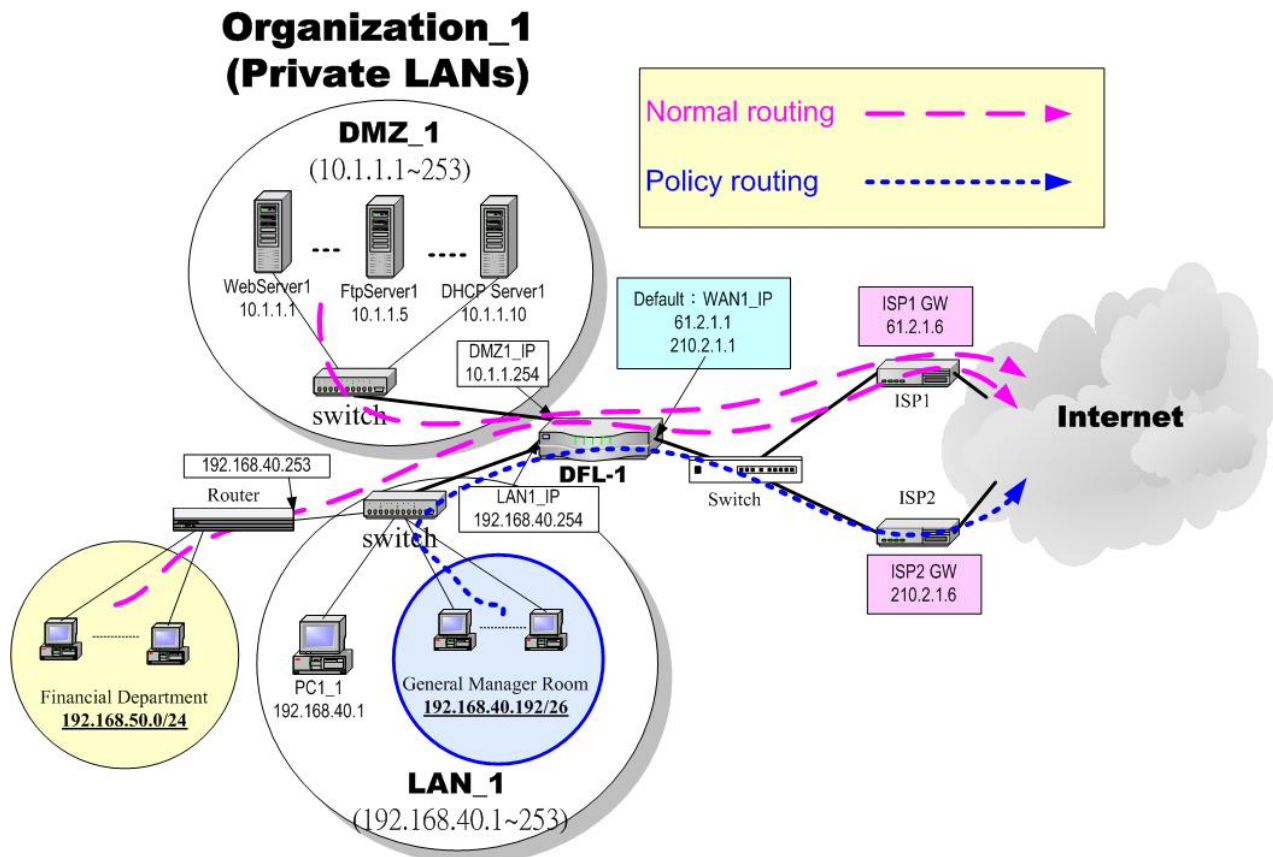


Figure 8-1 Add policy routing entry for the General-Manager-Room department

8.2 Objectives

1. We need to let DFL-1500 know how to forward the packets which is bound for financial department (192.168.50.0/24).
2. The network administrator plans to solve the problem by subscribing the second link (ISP2). He hopes that all the packets from the General-Manager-Room (192.168.40.192/26) will pass through the ISP2 link instead of the default ISP1 link.

8.3 Methods

1. Add a static routing entry to direct the packets towards 192.168.50.0/24 through the router (192.168.40.253).
2. Add a policy routing entry for the packets coming from General-Manager-Room department (192.168.40.192 / 255.255.255.192) through the ISP2 link.

Two restrictions of the default WAN Policy Route: 1) As long as the subnet is directly connected to the DFL-900/1500, it will be routed with the routing table as the priority 1. 2) For the subnet indirectly connected to the DFL-900/1500, it will be routed to the policy route only when it comes to the default route.

8.4 Steps

8.4.1 Add a static routing entry

Step 1. Add a static routing rule

Click the Add button to the next process.

Advanced Settings > Routing > Static Route

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

Step 2. Fill out the related field

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

Advanced Settings > Routing > Static Route > Add

Static Route->Add Entry

Type:

Destination:

Netmask:

Gateway:

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-------------|--|----------------|----------------|
| Type | Determine this static routing entry record is multiple hosts (Net) or a single host (Host) ° | Net / Host | Net |
| Destination | The destination IP address of this static routing entry record. | IPv4 format | 192.168.50.0 |
| Netmask | The destination IP Netmask of this static routing entry record. | IPv4 format | 255.255.255.0 |
| Gateway | The default gateway of this static routing entry record. | IPv4 format | 192.168.40.253 |

Table 8-1 Add a static routing entry

| <p>Step 3. View the result</p> <p>The static route has been stored. After filling data completely, view the static routing entries which have been set.</p> | <p>Advanced Settings > Routing > Static Route</p> <p>Static Route <u>Policy Route</u></p> <table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Destination/Netmask</th> <th>Gateway</th> <th>Activated</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Net</td> <td>192.168.50.0/255.255.255.0</td> <td>192.168.40.253</td> <td>Yes</td> </tr> <tr> <td>2</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>3</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>4</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>5</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>6</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>7</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>8</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>9</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>10</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <p>Prev. Page Next Page</p> <p>Add Edit Delete</p> | # | Type | Destination/Netmask | Gateway | Activated | 1 | Net | 192.168.50.0/255.255.255.0 | 192.168.40.253 | Yes | 2 | - | - | - | - | 3 | - | - | - | - | 4 | - | - | - | - | 5 | - | - | - | - | 6 | - | - | - | - | 7 | - | - | - | - | 8 | - | - | - | - | 9 | - | - | - | - | 10 | - | - | - | - | | | | | | | | | |
|---|--|----------------------------|----------------|---------------------|-----------------|----------------|-----------------|----------------|----------------------------|----------------|------|---------------------|---------|-----------|---|---|---|---|----------------|-----------------|----------|------|---|---|---|---|-----|------------------------|------------|------|---|---|---|---|-----|--------------------------|----------|------|---|---|---|---|-----|---------------------------|---------------|------|---|---|---|---|-----|----------------------------|----------------|------|---|---|--|---|------------|----------------------------|----------------|------|--|--|--|
| # | Type | Destination/Netmask | Gateway | Activated | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Net | 192.168.50.0/255.255.255.0 | 192.168.40.253 | Yes | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10 | - | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>Step 4. View the routing table</p> <p>You can notice there is an extra routing entry in the routing table. The indicated routing entry as right diagram is produced by static routing rule.</p> | <p>Device Status > System Status > Routing Table</p> <table border="1"> <thead> <tr> <th>System Status</th> <th>Network Status</th> <th>CPU & Memory</th> <th>DHCP Table</th> <th>Routing Table</th> <th>Active Sessions</th> <th>Top20 Sessions</th> <th>IPSec Sessions</th> </tr> </thead> <tbody> <tr> <td>#</td> <td>Type</td> <td>Destination/Netmask</td> <td>Gateway</td> <td>Interface</td> <td></td> <td></td> <td></td> </tr> <tr> <td>1</td> <td>Default/Static</td> <td>0.0.0.0/0.0.0.0</td> <td>61.2.1.6</td> <td>WAN1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>2</td> <td>Net</td> <td>10.1.1.0/255.255.255.0</td> <td>10.1.1.254</td> <td>DMZ1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>3</td> <td>Net</td> <td>61.2.1.0/255.255.255.248</td> <td>61.2.1.1</td> <td>WAN1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>4</td> <td>Net</td> <td>192.168.2.0/255.255.255.0</td> <td>192.168.2.254</td> <td>LAN2</td> <td></td> <td></td> <td></td> </tr> <tr> <td>5</td> <td>Net</td> <td>192.168.40.0/255.255.255.0</td> <td>192.168.40.254</td> <td>LAN1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>6</td> <td>Net/Static</td> <td>192.168.50.0/255.255.255.0</td> <td>192.168.40.253</td> <td>WAN1</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Refresh</p> | System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions | # | Type | Destination/Netmask | Gateway | Interface | | | | 1 | Default/Static | 0.0.0.0/0.0.0.0 | 61.2.1.6 | WAN1 | | | | 2 | Net | 10.1.1.0/255.255.255.0 | 10.1.1.254 | DMZ1 | | | | 3 | Net | 61.2.1.0/255.255.255.248 | 61.2.1.1 | WAN1 | | | | 4 | Net | 192.168.2.0/255.255.255.0 | 192.168.2.254 | LAN2 | | | | 5 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.254 | LAN1 | | | | 6 | Net/Static | 192.168.50.0/255.255.255.0 | 192.168.40.253 | WAN1 | | | |
| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| # | Type | Destination/Netmask | Gateway | Interface | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Default/Static | 0.0.0.0/0.0.0.0 | 61.2.1.6 | WAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Net | 10.1.1.0/255.255.255.0 | 10.1.1.254 | DMZ1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Net | 61.2.1.0/255.255.255.248 | 61.2.1.1 | WAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Net | 192.168.2.0/255.255.255.0 | 192.168.2.254 | LAN2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.254 | LAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Net/Static | 192.168.50.0/255.255.255.0 | 192.168.40.253 | WAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

8.4.2 Add a policy routing entry

Step 1. Setup the ISP2 link

We must add an IP alias record to the WAN1 port because a new ISP link has been applied. So. See section 3.4.3 for the full procedures. Here we add an IP alias of WAN1 as 210.2.1.1/255.255.255.248.

Basic Setup > WAN Settings > IP Alias

| # | Interface | Aliases | Netmask |
|----|-----------|-----------|-----------------|
| 1 | WAN1 | 210.2.1.1 | 255.255.255.248 |
| 2 | ... | ... | ... |
| 3 | ... | ... | ... |
| 4 | ... | ... | ... |
| 5 | ... | ... | ... |
| 6 | ... | ... | ... |
| 7 | ... | ... | ... |
| 8 | ... | ... | ... |
| 9 | ... | ... | ... |
| 10 | ... | ... | ... |

Step 2. Insert a policy routing entry

Click Insert button to add a policy routing entry.

Advanced Settings > Routing > Policy Route

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

Step 3. Fill out the related field

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

Advanced Settings > Routing > Policy Route > Insert

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

Table 8-2 Add a policy routing entry

Step 4. View the result

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

Advanced Settings > Routing > Policy Route

Static Route Policy Route

Policy Routing->Edit Rules

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Step 5. Add a NAT rule

If you would like to use policy route to accomplish static load balance as Figure 8-1 illustrated, you must add an extra NAT rule (Many-to-1) manually. It will let all the packets coming from the specified addresses (192.168.40.192/26) be translated into the second IP address (210.2.1.1). Then the NAT rules will be shown as right diagram. For the detailed description of the NAT rule, please refer section 7.4.1.

Advanced Settings > NAT > NAT Rules

Status NAT Rules Virtual Servers

NAT->Edit Rules

Packets are top-down matched by the rules.

| Item | Status | | Condition | | Action | |
|------|--------|------------|----------------|--------------------------------|---------------------------|------|
| # | Active | Name | Direction | Source IP Address | Translate Src IP into | Type |
| 1 | Y | PolicyRule | LAN/DMZ to WAN | 192.168.40.192/255.255.255.192 | 210.2.1.1/255.255.255.255 | M-1 |
| 2 | Y | Basic-DMZ1 | LAN/DMZ to WAN | 10.1.1.254/255.255.255.0 | Auto (device WAN IP) | M-1 |
| 3 | Y | Basic-LAN2 | LAN/DMZ to WAN | 192.168.2.254/255.255.255.0 | Auto (device WAN IP) | M-1 |
| 4 | Y | Basic-LAN1 | LAN/DMZ to WAN | 192.168.40.254/255.255.255.0 | Auto (device WAN IP) | M-1 |

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Step 6. View the routing table

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

Note that the information of the policy routing entries will not be shown in this screen. It will just appear in the policy routing page as the previous step.

Device Status > System Status > Routing Table

System Status Network Status CPU & Memory DHCP Table Routing Table Active Sessions Top20 Sessions IPsec Sessions

| # | Type | Destination/Netmask | Gateway | Interface |
|---|----------------|----------------------------|----------------|-----------|
| 1 | Default/Static | 0.0.0.0/0.0.0.0 | 61.2.1.6 | WAN1 |
| 2 | Net | 10.1.1.0/255.255.255.0 | 10.1.1.254 | DMZ1 |
| 3 | Net | 61.2.1.0/255.255.255.248 | 61.2.1.1 | WAN1 |
| 4 | Net | 192.168.2.0/255.255.255.0 | 192.168.2.254 | LAN2 |
| 5 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.254 | LAN1 |
| 6 | Net/Static | 192.168.50.0/255.255.255.0 | 192.168.40.253 | WAN1 |
| 7 | Net | 210.2.1.0/255.255.255.0 | 210.2.1.1 | WAN1 |

Refresh

8.5 The priority of the routing

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

| Priority sequence | Routing Method | Description |
|-------------------|--|--|
| 1. | a · LAN/DMZ/WAN local bound network b · Static/RIP routing entry of LAN/DMZ | Method a means the network which is attached to the interface. There is an example as the Line-2 at the Figure 8-2. Method b means the network which is defined by the static route (please refer section 8.4.1) or learned from RIP method. Please notice the method b is only for LAN/DMZ. Please refer the Line-1 at the Figure 8-2. The priority between RIP route and static route depends on its prefix. Whose prefix is shortest, it will have the high priority. Ex. The 210.10.1.0/24 has the higher priority then 210.10.1.1.0/16. |
| 2. | WAN policy route | The defined policy routing as section 8.4.2 indicated. There is an example as the Line-3 at the Figure 8-2. Please notice that policy route can only work at the default WAN link. |
| 3. | Static/RIP routing entry of WAN | It is the same as method b's Priority. But this priority is only designated for WAN ports. |
| 4. | Default Route | Basically, if no other routing policy has been set, the traffic will go through the default route. Please refer the Line-4 in the Figure 8-2. |

Table 8-3 The priority of the routing

The number of each routing direction is indicated the example which is described in the above Table 8-3.

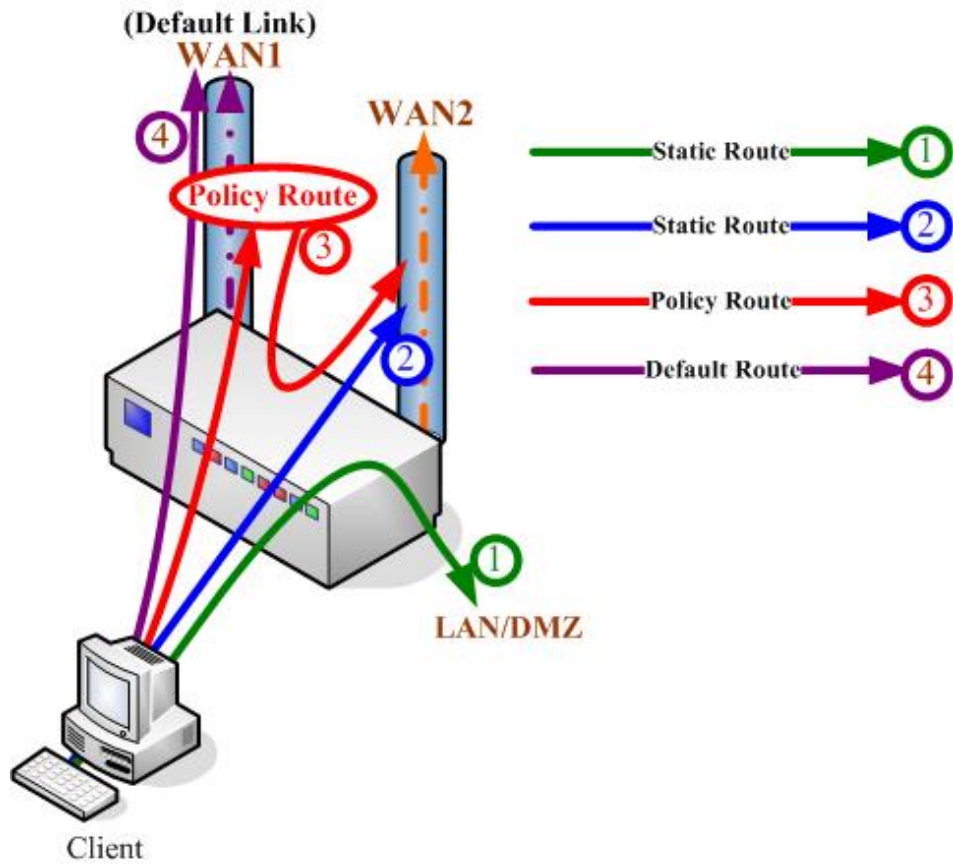


Figure 8-2 The routing decision of DFL-900/DFL-1500

Part IV

Firewall & IP/MAC Binding

Chapter 9

IP/Services grouping

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

9.1 Demands

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

9.2 Objectives

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

9.3 Methods

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

9.4 Steps

9.4.1 Setup Address

Step 1. Address Settings

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

Click the [Objects](#) hyperlink and then select the [Define Objects on LAN1](#). Click [Insert](#) to add a new address object.

BASIC SETUP > Books > Address > Object

| Item | Name | Type | Value |
|------|----------|--------|-----------------|
| # | Name | Type | Value |
| 1 | LAN1_ALL | Subnet | 0.0.0.0/0.0.0.0 |

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

Table 9-1 Define the address objects

Step 2. Insert a new Address object

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

BASIC SETUP > Books > Address > Object > Insert

Address Service Schedule

[Objects] [Groups]

Address -> Objects -> Add

Insert a new Address object

Name

Value

Address Type:

Subnet IP: Mask:

Range Start IP: End IP:

Host IP:

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

Table 9-2 The field of the Address object

Step 3. View the Address object settings

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

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

BASIC SETUP > Books > Address > Objects

Address Service Schedule

[Objects] [Groups]

Address -> Objects

Define Objects on

| Item | # | Name | Type | Value |
|----------------------------------|---|----------|--------|-----------------|
| <input checked="" type="radio"/> | 1 | PC1_3 | Host | 192.168.40.3 |
| <input type="radio"/> | 2 | PC1_2 | Host | 192.168.40.2 |
| <input type="radio"/> | 3 | PC1_1 | Host | 192.168.40.1 |
| <input type="radio"/> | 4 | LAN1_ALL | Subnet | 0.0.0.0/0.0.0.0 |

Step 4. Address Group Settings

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

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

BASIC SETUP > Books > Address > Group

Address Service Schedule

[Objects] [Groups]

Address -> Groups

Define Address Groups on

| Group | Name | Content |
|-------|------|---------|
| # | Name | Content |

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

Table 9-3 Define the addresses group

| | |
|--|--|
| <p>Step 5. Add an address group</p> <p>Enter a Group Name to identify the address group. Select the addresses from the available address list and click right arrow to add them to the Members list. To remove addresses from address group, please select addresses from the Members list and then click left arrow.</p> <p>You can add address groups to any interface. The address group can only contain addresses from that interface. Address group cannot have the same names as individual addresses. If an address group is included in a firewall rule, it cannot be deleted unless it is first removed by the firewall rule.</p> | <p>BASIC SETUP > Books > Address > Group > Insert</p> |
|--|--|

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

Table 9-4 Define the addresses group

| | |
|---|--|
| <p>Step 6. view the address group result</p> <p>According to our setting as previous steps, the address group is shown as right diagram.</p> | <p>BASIC SETUP > Books > Address > Group</p> |
|---|--|

9.4.2 Setup Service

Step 1. Service Settings

The DFL-1500 predefined firewall services are listed as right diagram. You can add these services to any firewall rule or you can add a service if you need to create a firewall rule for a service that is not in the predefined service list.

Select **Insert** to add a new service.

BASIC SETUP > Books > Service > Objects

Address Service Schedule

[Objects] [Groups]

Service -> Objects

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

Insert Edit Delete

Step 2. Insert a new service object

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

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

BASIC SETUP > Books > Service > Insert

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

Table 9-5 The field of the Service objects

Step 3. Add a service group

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

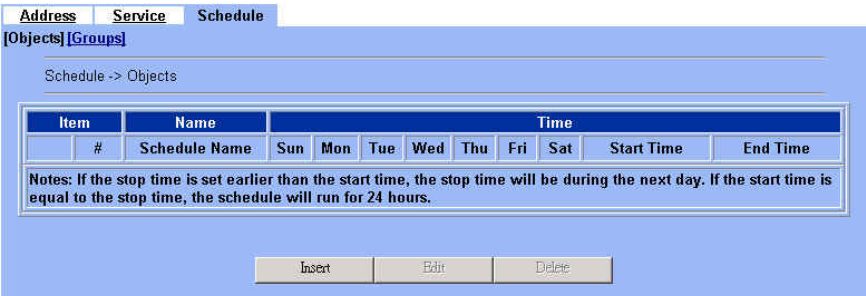
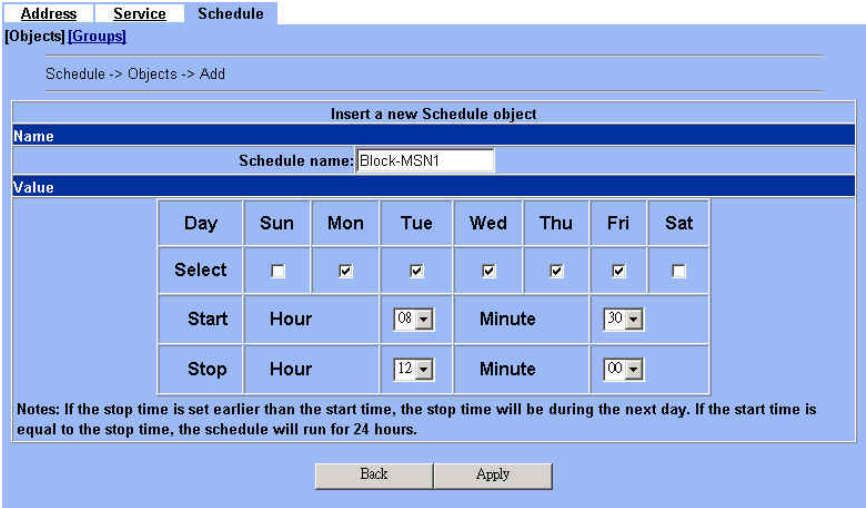
Click **Groups** hyperlink, and then click **Insert** to add a new service group. Enter a Group Name to identify the group. Select the services from the available services list and click right arrow to copy them to the Members list. If you would like to remove the services from the members list, just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

BASIC SETUP > Books > Service > Groups > Insert

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

Table 9-6 Define the services group

9.4.3 Setup Schedule

| | |
|--|--|
| <p>Step 1. Schedule Settings</p> <p>Use scheduling to control when rules are active or inactive.</p> <p>Select Insert to add a new service.</p> | <p>BASIC SETUP > Books > Schedule > Objects</p>  |
| <p>Step 2. Insert a new schedule object</p> <p>Enter the Schedule name. Select the Day you would like to active or inactive a firewall rule, and then select the Start/Stop time. Click Apply to add the schedule object.</p> <p>Suppose using MSN is forbidden in your company from 08:30~12:00, 13:00~17:30 during Monday to Friday, you have to add two schedule ranges (08:30~12:00 and 13:00~17:30) and then group them together in order for your company to make a firewall rule to block the MSN service.</p> <p>Note that schedule name should be an alphanumeric value (including dash '-' and underscore '_'), can start with a letter only and, please note, it is case-sensitive! Spaces and other special characters are not allowed.</p> | <p>BASIC SETUP > Books > Address > Schedule > Insert</p>  |

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|---------------|---|----------------|------------|
| Schedule name | The name of the schedule object. | text string | Block-MSN1 |
| Day | The days to active or inactive a firewall rule. | Sun ~ Sat | Mon ~ Fri |

| | | | |
|------------|--|----------------|-------|
| Start time | The start time of the schedule object. | 24-hour format | 08:30 |
| Stop time | The stop time of the schedule object. | 24-hour format | 12:00 |

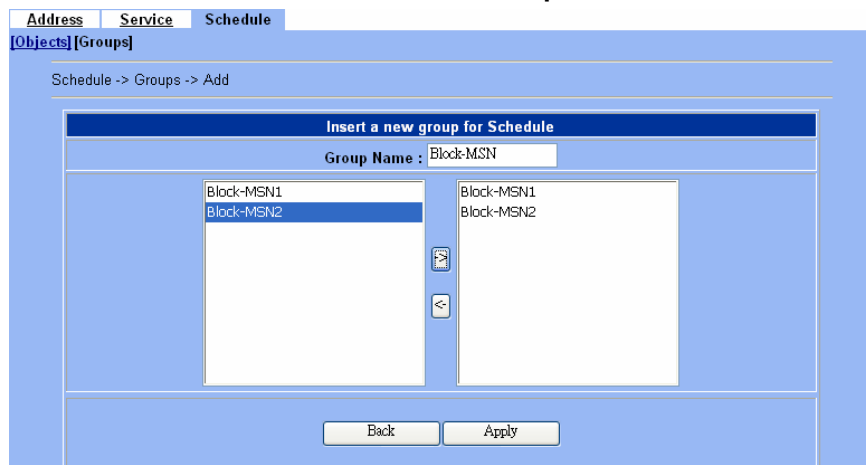
Table 9-7 The field of the Schedule object

Step 3. Add a Schedule group

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

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

BASIC SETUP > Books > Schedule > Groups > Insert



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

Table 9-8 Define the schedule group

Chapter 10 Firewall

This chapter introduces firewall and explains how to implement it.

10.1 Demands

1. Administrators detect that PC1_1 in LAN_1 is doing something that may hurt our company and should instantly block his traffic towards the Internet.
2. On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money. Now, suppose a DMZ server was attacked by SYN-Flooding attack and requires the DFL-1500 to protect it.

10.2 Objectives

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

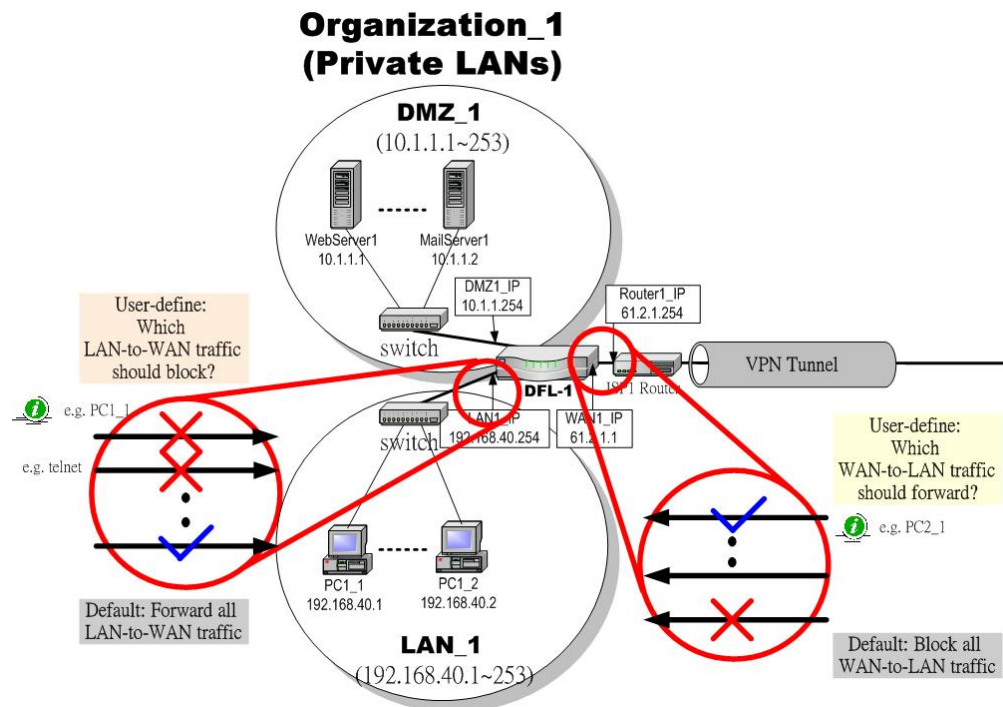


Figure 10-1 Setting up the firewall rule

10.3 Methods

1. Configure the Address/Service/Schedule first.
2. Add a LAN1-to-WAN1 Firewall rule to block PC1_1.
3. Start the SYN-Flooding protection by detecting statistical half-open TCP connections.

10.4 Steps

10.4.1 Block internal PC session (LAN → WAN)

| | |
|---|---|
| <p>Step 1. Setup NAT</p> <p>Check the Enable Stateful Inspection Firewall checkbox, and click the Apply.</p> | <p>ADVANCED SETTINGS > Firewall > Status</p> <p>Status Edit Rules Show Rules Anti-DoS Summary</p> <p><input checked="" type="checkbox"/> Enable Stateful Packet Inspection Firewall</p> <p>The Stateful Packet Inspection (SPI) firewall defines access control rules for traffic running across the interfaces.</p> <p>Reset Rules</p> <p style="text-align: right;">Total Configured Rules: 49 Vacant Rules: 2951</p> <p style="text-align: center;">Apply</p> |
|---|---|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--|--|--------------------|---------|
| Enable Stateful Packet Inspection Firewall | Enable Firewall feature of DFL-1500 | Enabled / Disabled | Enabled |
| BUTTON | DESCRIPTION | | |
| Reset Rules | Clean all the user defined rules and restore firewall rules to the default settings. | | |
| Apply | Apply the settings which have been configured. | | |

Table 10-1 Configure Firewall status

| <p>Step 2. Add a Firewall Rule</p> <p>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>Status Edit Rules Show Rules Anti-DoS Summary</p> <p>Firewall->Edit Rules</p> <p>Edit LAN1 to WAN1 rules</p> <p>Default action for this packet direction: Forward <input type="checkbox"/> Log Apply</p> <p>Packets are top-down matched by the rules.</p> <table border="1"> <thead> <tr> <th>Item</th> <th>Status</th> <th colspan="4">Condition</th> <th>Action</th> <th></th> </tr> <tr> <th>#</th> <th>Name</th> <th>Schedule</th> <th>Source IP</th> <th>Dest. IP</th> <th>Service</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Default</td> <td>ALWAYS</td> <td>LAN1_ALL</td> <td>WAN1_ALL</td> <td>ALL_SERVICE</td> <td>Forward</td> <td>N</td> </tr> </tbody> </table> <p style="text-align: right;">Page 1/1</p> <p style="text-align: center;">Prev. Page Next Page Move Page 1</p> <p style="text-align: center;">Insert Edit Delete Move Before: 1</p> | Item | Status | Condition | | | | Action | | # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log | 1 | Default | ALWAYS | LAN1_ALL | WAN1_ALL | ALL_SERVICE | Forward | N |
|---|---|-----------|-----------|-----------|-------------|---------|-----|--------|--|---|------|----------|-----------|----------|---------|--------|-----|---|---------|--------|----------|----------|-------------|---------|---|
| Item | Status | Condition | | | | Action | | | | | | | | | | | | | | | | | | | |
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log | | | | | | | | | | | | | | | | | | |
| 1 | Default | ALWAYS | LAN1_ALL | WAN1_ALL | ALL_SERVICE | Forward | N | | | | | | | | | | | | | | | | | | |

| FIELD | DESCRIPTION | Range/Format | EXAMPLE |
|--|---|----------------------------|-------------------------|
| Edit __ to __ rules | Select the rule direction of rule which you are going to configure. | WAN/LAN/DMZ to WAN/LAN/DMZ | Edit LAN1 to WAN1 rules |
| Default action for this packet direction | Decide the default policy of firewall rule. | Forward / Block | Forward |
| Log | Decide the default log policy of firewall rule. | Log / Don't log | Don't log |
| BUTTON | DESCRIPTION | | |

| | |
|-----------------|---|
| Prev. Page | If there are more than one rule pages, you can press Prev. Page to back to the previous page. |
| Next Page | If there are more than one action rules, you can press Next Page to go to the next page. |
| Move Page ___ | Move to the indicated page. |
| Insert | Insert a new rule. |
| Edit | Edit the properties of the existent rule. |
| Delete | Delete the indicated rule. |
| Move Before ___ | Move the selected rule to the front of the indicated rule number. |

Table 10-2 Add a firewall rule

Step 3. Customize the rule

Before adding a new firewall, you have to set the Books in the Basic Setup > Books > Addresses/Services/Schedules first. After configuring the settings, you can then add a new firewall rule.

Enter the rule name as PC1_1, and select Schedule. Select Source IP as PC1_1 (192.168.40.1 / 255.255.255.255), and select Dest. IP as WAN1_ALL. Select Service as ANY (TCP, UDP and ICMP). Select Block and Log to the matched session. And choose the Forward bandwidth class or Reverse bandwidth class if any. Click the Apply to apply the changes.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

The screenshot shows the 'Insert a new LAN1-to-WAN1 Firewall rule' configuration page. The fields are as follows:

- Status:** Rule name: PC1_1, Schedule: Always
- Condition:** Source IP: PC1_1, Dest. IP: WAN1_ALL, Service: ANY
- Action:** Block and log the matched session. Forward bandwidth class: def_class, Reverse bandwidth class: def_class

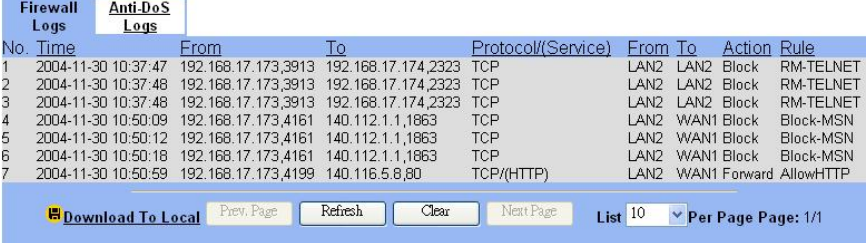
Buttons: Back, Apply

| | FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------|-------------------------------------|---|---|----------|
| Status | Rule name | The name of the Firewall rule. Note that rule name should begin with alphabet, followed by alphabet/digits/dashes. | text string | PC1_1 |
| | Schedule | When does this firewall rule take effect? | All the defined schedule objects and groups | Always |
| Condition | Source IP | Compared with the incoming packets, whether Source IP is matched. | All the defined address objects and groups | PC1_1 |
| | Dest IP | Compared with the incoming packets, whether Dest IP is matched. | All the defined address objects and groups | WAN1_ALL |
| | Service | Verified the service of incoming packet is belonging to each TCP、UDP、ICMP. | All the defined service objects and groups | ANY |
| Action | Forward / Block the matched session | If packet is matched the rule condition, Forward or Block this matched packet? | Forward / Block | Block |

Part IV
Firewall & IP/MAC Binding

| | | | | |
|--|--------------------------------------|---|------------------|-----------|
| | do not log / log the matched session | If packet is matched the rule condition, Log or Don't log this matched packet? | log / do not log | log |
| | Forward bandwidth class | About this field description, please refer Table 26-6 Add a new Bandwidth Management rule for more information. | | def_class |
| | Reverse bandwidth class | The same as above field. | | def_class |

Table 10-3 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>  <p>The screenshot shows a web interface for viewing firewall logs. At the top, there are tabs for 'Firewall Logs' and 'Anti-DoS Logs'. Below the tabs is a table with columns: No., Time, From, To, Protocol/(Service), From, To, Action, and Rule. The table contains 7 rows of log entries. At the bottom of the interface, there are several buttons: 'Download To Local', 'Prev. Page', 'Refresh', 'Clear', 'Next Page', and a dropdown menu for 'List' set to '10'. To the right of the dropdown, it says 'Per Page Page: 1/1'.</p> |
|---|---|

| FIELD | DESCRIPTION |
|--------------------|--|
| No | The indicated firewall log sequence number. |
| Time | The record time of indicated firewall log. |
| From | The source IP address (include port) which the indicated log event is come from. |
| To | The destination IP address (include port) which the indicated log event is bound for. |
| Protocol/(Service) | The record log is TCP, UDP or ICMP / (which service it will be). |
| From | The interface which the indicated log event come from. |
| To | The interface which the indicated log event is bound for. |
| Action | The status of indicated firewall log is Block or Forward. |
| Rule | The log is produced by which firewall rule. "Default" means the default rule of the selected firewall direction. "RM-<method>" means the log is produced by remote management function (Almost it is the illegal user who wants to use the Non-Opened remote management functions). "Rule-Name" The log is produced by which firewall rule. |

Table 10-4 Firewall log field description

| Firewall Logs | | Anti-DoS Logs | | | | | |
|---------------|---------------------|---------------------|---------------------|--------------------|-----------|---------|-----------|
| No. | Time | From | To | Protocol/(Service) | From To | Action | Rule |
| 1 | 2004-11-30 10:37:47 | 192.168.17.173,3913 | 192.168.17.174,2323 | TCP | LAN2 LAN2 | Block | RM-TELNET |
| 2 | 2004-11-30 10:37:48 | 192.168.17.173,3913 | 192.168.17.174,2323 | TCP | LAN2 LAN2 | Block | RM-TELNET |
| 3 | 2004-11-30 10:37:48 | 192.168.17.173,3913 | 192.168.17.174,2323 | TCP | LAN2 LAN2 | Block | RM-TELNET |
| 4 | 2004-11-30 10:50:09 | 192.168.17.173,4161 | 140.112.1.1,1863 | TCP | LAN2 WAN1 | Block | Block-MSN |
| 5 | 2004-11-30 10:50:12 | 192.168.17.173,4161 | 140.112.1.1,1863 | TCP | LAN2 WAN1 | Block | Block-MSN |
| 6 | 2004-11-30 10:50:18 | 192.168.17.173,4161 | 140.112.1.1,1863 | TCP | LAN2 WAN1 | Block | Block-MSN |
| 7 | 2004-11-30 10:50:59 | 192.168.17.173,4199 | 140.116.5.8,80 | TCP/(HTTP) | LAN2 WAN1 | Forward | AllowHTTP |

Download To Local

 List Per Page Page: 1/1

| Log Message | Description |
|--|--|
| 6 2004-11-30 10:50:18 192.168.17.173,4161 140.112.1.1,1863 TCP LAN2 WAN1 BLOCK Block-MSN | The firewall log is number 6. At the specified time (2004-11-30 10:50:18), the firewall blocked the packet which came from source IP address/port (192.168.17.173:4161) to the destination IP address/port (140.112.1.1:1863) using TCP protocol. The direction of packet flow is from LAN2 to WAN1 in this log. The packet matched the firewall rule (Block-MSN) and then blocked it out according to the rule's configuration. |
| 7 2004-11-30 10:50:59 192.168.17.173:4199 140.116.5.8:80 TCP/(HTTP) LAN2 WAN1 Forward AllowHTTP | The firewall log is number 7. At the specified time (2004-11-30 10:50:59), the firewall forwarded the packet which came from source IP address/port (192.168.17.173:4199) to the destination IP address/port (140.116.5.8:80) using TCP(HTTP) protocol. The direction of packet flow is from LAN2 to WAN1 in this log. The packet matched the firewall rule (AllowHTTP) and then forwarded it out according to the rule's configuration. |

Table 10-5 Firewall Log examples

10.4.2 Setup Anti-DoS

Step 1. Setup Anti-DoS

With the Anti-DoS attacks protection enabled, the DFL-1500 will be equipped with the built-in Anti-DoS engine. Normal DoS attacks will show up in the log when detecting and blocking such traffic. However, Flooding attacks require extra parameters to recognize. Check the Enable DoS attacks protection checkbox. And change the value of flooding thresholds as your preference.

ADVANCED SETTINGS > Firewall > Anti-DoS

| Status | Edit Rules | Show Rules | Anti-DoS | Summary |
|---|----------------------------------|------------|----------|---------|
| <input checked="" type="checkbox"/> Enable DoS attacks protection | | | | |
| The DoS protection can block well-known denial-of-service attacks such as WinNuke and LAND attacks. Thresholds for Flooding types of DoS can be defined in this page. | | | | |
| Denial of Service Thresholds: | | | | |
| TCP SYN Flooding | <input type="text" value="800"/> | pkt/sec | | |
| UDP Flooding | <input type="text" value="500"/> | pkt/sec | | |
| ICMP Flooding | <input type="text" value="10"/> | pkt/sec | | |
| Block all fragments | <input type="checkbox"/> | | | |
| <input type="button" value="Apply"/> | | | | |

| FIELD | DESCRIPTION | EXAMPLE |
|-------------------------------|---|---------|
| Enable DoS attacks protection | Enable the Denial of Service (DoS) attack protection. You should enable this to activate any further settings. Notice, the Anti-DoS feature can detect the TCP/UDP/ICMP flooding on each interface of the firewall device. | Enabled |

Part IV Firewall & IP/MAC Binding

| Denial of Service Thresholds | | |
|------------------------------|--|----------|
| TCP SYN Flooding | The number of TCP SYN packets that arrive at the same interface will block the further TCP connection attempts. | 800 |
| UDP Flooding | The number of UDP packets that arrive at the same interface will block the further arriving UDP packets. | 500 |
| ICMP Flooding | The number of ICMP packets that arrive at the same interface will block the further arriving ICMP packets. | 10 |
| Block all fragmented packets | When enabled, the firewall will drop any packets that have the fragment bit set in the IP header. This will protect the internal network from fragmented packet attacks. Note that this may cause some applications failure. | Disabled |

Table 10-6 Setup the thresholds of Anti-DoS

| <p>Step 2. View Anti-DoS Logs</p> <p>While there are any DoS attacks through DFL Firewall, it will block the attacked packets and log it as right diagram.</p> | <p>DEVICE Status > Firewall Logs > Anti-DoS Logs</p> <table border="1"> <thead> <tr> <th colspan="2">Firewall Logs</th> <th>Anti-DoS Logs</th> </tr> <tr> <th>No.</th> <th>Time</th> <th>Information</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2004-11-29 21:42:41</td> <td>ICMP-Flooding DoS Attack from 192.168.131.254 blocked</td> </tr> <tr> <td>2</td> <td>2004-11-30 02:55:11</td> <td>UDP-Flooding DoS Attack from 192.168.18.87 blocked</td> </tr> <tr> <td>3</td> <td>2004-11-30 05:00:11</td> <td>UDP-Flooding DoS Attack from 192.168.18.87 blocked</td> </tr> <tr> <td>4</td> <td>2004-11-30 06:01:13</td> <td>UDP-Flooding DoS Attack from 192.168.18.87 blocked</td> </tr> </tbody> </table> <p> <input type="button" value="Download To Local"/> <input type="button" value="Prev. Page"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/> <input type="button" value="Next Page"/> List 10 Per Page Page: 1/1 </p> | Firewall Logs | | Anti-DoS Logs | No. | Time | Information | 1 | 2004-11-29 21:42:41 | ICMP-Flooding DoS Attack from 192.168.131.254 blocked | 2 | 2004-11-30 02:55:11 | UDP-Flooding DoS Attack from 192.168.18.87 blocked | 3 | 2004-11-30 05:00:11 | UDP-Flooding DoS Attack from 192.168.18.87 blocked | 4 | 2004-11-30 06:01:13 | UDP-Flooding DoS Attack from 192.168.18.87 blocked |
|---|--|---|--|---------------|-----|------|-------------|---|---------------------|---|---|---------------------|--|---|---------------------|--|---|---------------------|--|
| Firewall Logs | | Anti-DoS Logs | | | | | | | | | | | | | | | | | |
| No. | Time | Information | | | | | | | | | | | | | | | | | |
| 1 | 2004-11-29 21:42:41 | ICMP-Flooding DoS Attack from 192.168.131.254 blocked | | | | | | | | | | | | | | | | | |
| 2 | 2004-11-30 02:55:11 | UDP-Flooding DoS Attack from 192.168.18.87 blocked | | | | | | | | | | | | | | | | | |
| 3 | 2004-11-30 05:00:11 | UDP-Flooding DoS Attack from 192.168.18.87 blocked | | | | | | | | | | | | | | | | | |
| 4 | 2004-11-30 06:01:13 | UDP-Flooding DoS Attack from 192.168.18.87 blocked | | | | | | | | | | | | | | | | | |

Chapter 11

IP/MAC Binding

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

11.1 Demands

Your company would like to protect some servers or users avoid their IP address snatched by others, and control the computers to let them accepted or denied by the IP/MAC rules. IP/MAC binding protects the DFL-1500 unit and avoid your network from IP spoofing attacks.

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

- a、 IP spoofing:
IP spoofing attempts to use the IP address of a trusted computer to connect to or through the DFL-1500 unit from a different computer. The IP address of a computer can easily be changed to a trusted address, but MAC addresses are added to Ethernet cards at the factory and cannot easily be changed.
- b、 Unregistered user accessing:
Through the MAC addresses registering, administrator can prohibit those unregistered addresses passing through DFL-1500.

11.2 Objectives

Use this mechanism to permit some specified MAC address passing through DFL-1500. Other MAC addresses without permission will be blocked by DFL-1500.

11.3 Methods

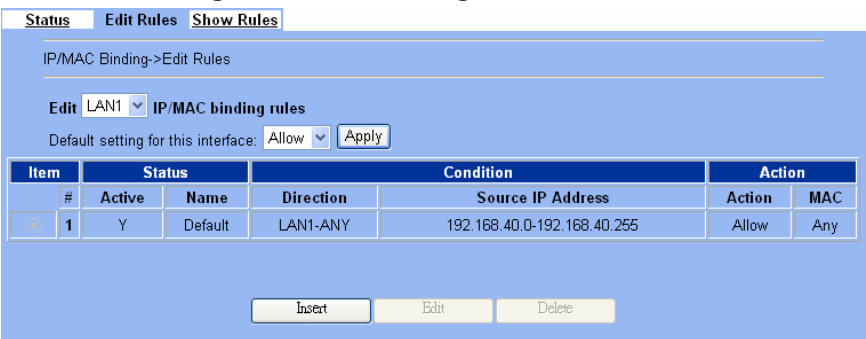
Binding the specified IP address and MAC address together. And permit the legal one to pass through the DFL-1500.

11.4 Steps

| | |
|--|---|
| <p>Step 1. Enable IP/MAC binding</p> <p>Check the <code>Enable IP/MAC Binding</code> checkbox, and then click <code>Apply</code> to apply the setting.</p> <p>Note that the IP/MAC binding locks IP address for specific MACs. It achieves the purpose by the steps as right diagram described.</p> | <p>Advanced Settings > IP/MAC Binding > Status</p> |
|--|---|

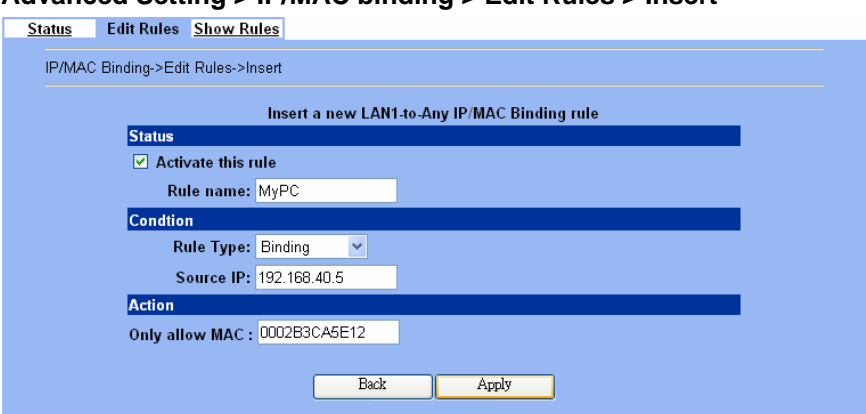
| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------------------|--|--------------------|---------|
| Enable IP/MAC Binding | Enable IP/MAC Binding feature of DFL-1500 | Enabled / Disabled | Enabled |
| BUTTON | DESCRIPTION | | |
| Reset | Clear all the predefined IP/MAC binding rules. | | |

Table 11-1 Enable IP/MAC Binding feature

| | |
|---|--|
| <p>Step 2. Leave IP/MAC binding “Allow” state</p> <p>Select LAN1 as the interface to edit the IP/MAC binding rules. Because we do not add current MAC address of our PC, do not change the Default IP/MAC settings to Block. Please keep this state with Allow at this moment. And click Insert to add a rule.</p> <p>Note that you have to add an IP/MAC binding rule as Allow for your computer to pass the firewall rule before you block the LAN1-ANY direction, otherwise you will be blocked by that rule.</p> | <p>Advanced Settings > IP/MAC Binding > Edit Rules</p>  |
|---|--|

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

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

| | |
|--|---|
| <p>Step 3. Add a new IP/MAC binding rule</p> <p>Add an IP/MAC binding rule to allow our PC passing through the DFL-1500. Otherwise our PC will be blocked by DFL-1500 in the further steps.</p> <p>Here the IP address “192.168.40.5” is the MAC address of our login PC.</p> | <p>Advanced Setting > IP/MAC binding > Edit Rules > Insert</p>  |
|--|---|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------------|---|---------------------|---------|
| Activate this rule | Activate the IP/MAC binding rule. | Enabled/Disabled | Enabled |
| Rule name | The name of the IP/MAC binding rule. Note that rule name should begin with alphabet, followed by alphabet/digits/dashes. | text string | MyPC |
| Rule Type | The type of IP/MAC “Binding” is combined IP address with MAC address together to decide packet is passed or blocked by the DFL-1500. Another type of IP/MAC “Allow range” depends on the IP range to permit whether packets can pass or not. For this type, please refer Table 11-4 description. | Binding/Allow Range | Binding |

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

Table 11-3 Add an IP/MAC Binding rule

| | |
|--|--|
| <p>Step 4. View the results</p> <p>Through the previous step, you can see the configured result as the right diagram.</p> | <p>Advanced Setting > IP/MAC binding > Edit Rules</p> |
| <p>Step 5. Add a another new IP/MAC rule</p> <p>Add another IP/MAC rule to allow an IP address range to pass through DFL-1500. This rule type is useful for local PC using DHCP feature specially. Suppose DHCP IP range of LAN1 interface is 192.168.40.100 to 192.168.40.119.</p> <p>Check Activate this rule checkbox. Enter Rule name as LAN1_DHCP. Select Allow Range in the Rule Type field, and enter the Start IP as 192.168.40.100 and End IP as 192.168.40.119. Click Apply to store this setting.</p> | <p>Advanced Setting > IP/MAC binding > Edit Rules > Insert</p> |

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

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

Part IV

Firewall & IP/MAC Binding

Step 6. Change the IP/MAC binding to “Block”

Through the previous steps, we have configured two IP/MAC rules for allowing passing through DFL-1500. In this step, we will change the IP/MAC binding status to “Block” to prohibit invalid IP address to pass through DFL-1500.

Advanced Settings > IP/MAC Binding > Edit Rules

IP/MAC Binding->Edit Rules

Edit LAN1 IP/MAC binding rules

Default setting for this interface: Allow Apply

| Item | Status | Condition | Action | | | |
|------|--------|-----------|-----------|-------------------------------|--------|--------------|
| # | Active | Name | Direction | Source IP Address | Action | MAC |
| 1 | Y | LAN1_DHCP | LAN1-ANY | 192.168.40.100-192.168.40.119 | Allow | Any |
| 2 | Y | MyPC | LAN1-ANY | 192.168.40.5 | Allow | 0002B3CA5E12 |
| 3 | Y | Default | LAN1-ANY | 192.168.40.0-192.168.40.255 | Allow | Any |

Insert Edit Delete

Step 7. Show the IP/MAC binding rule

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

Advanced Setting > IP/MAC binding > Show Rules

IP/MAC Binding->Edit Rules

Edit LAN1 IP/MAC binding rules

Default setting for this interface: Block Apply

| Item | Status | Condition | Action | | | |
|------|--------|-----------|-----------|-------------------------------|--------|--------------|
| # | Active | Name | Direction | Source IP Address | Action | MAC |
| 1 | Y | LAN1_DHCP | LAN1-ANY | 192.168.40.100-192.168.40.119 | Allow | Any |
| 2 | Y | MyPC | LAN1-ANY | 192.168.40.5 | Allow | 0002B3CA5E12 |
| 3 | Y | Default | LAN1-ANY | 192.168.40.0-192.168.40.255 | Block | Any |

Insert Edit Delete

Part V

Virtual Private Network

Chapter 12

VPN Technical Introduction

This chapter introduces VPN related technology

12.1 VPN benefit

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

1. Authentication

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

2. Integrity

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

3. Confidentiality

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

4. Non-repudiation

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

12.2 Related Terminology Explanation

12.2.1 VPN

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

12.2.2 IPsec

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

12.2.3 Security Association

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

12.2.4 IPsec Algorithms

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

12.2.5 Key Management

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

➤ IKE Phases

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

In phase 1 you must :

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

In phase 2 you must :

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

➤ Negotiation Mode

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

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

➤ Pre-Shared Key

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

➤ Diffie-Hellman (DH) Key Groups

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

➤ Perfect Forward Secrecy (PFS)

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

This may be unnecessary for data that does not require such security, so PFS is disabled (None) by default in the DFL-1500. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

12.2.6 Encapsulation

➤ Transport Mode

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

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

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

➤ Tunnel Mode

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

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

12.2.7 IPsec Protocols

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

➤ AH (Authentication Header) Protocol

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

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

➤ ESP (Encapsulating Security Payload) Protocol

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

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

12.3 Make VPN packets pass through DFL-1500

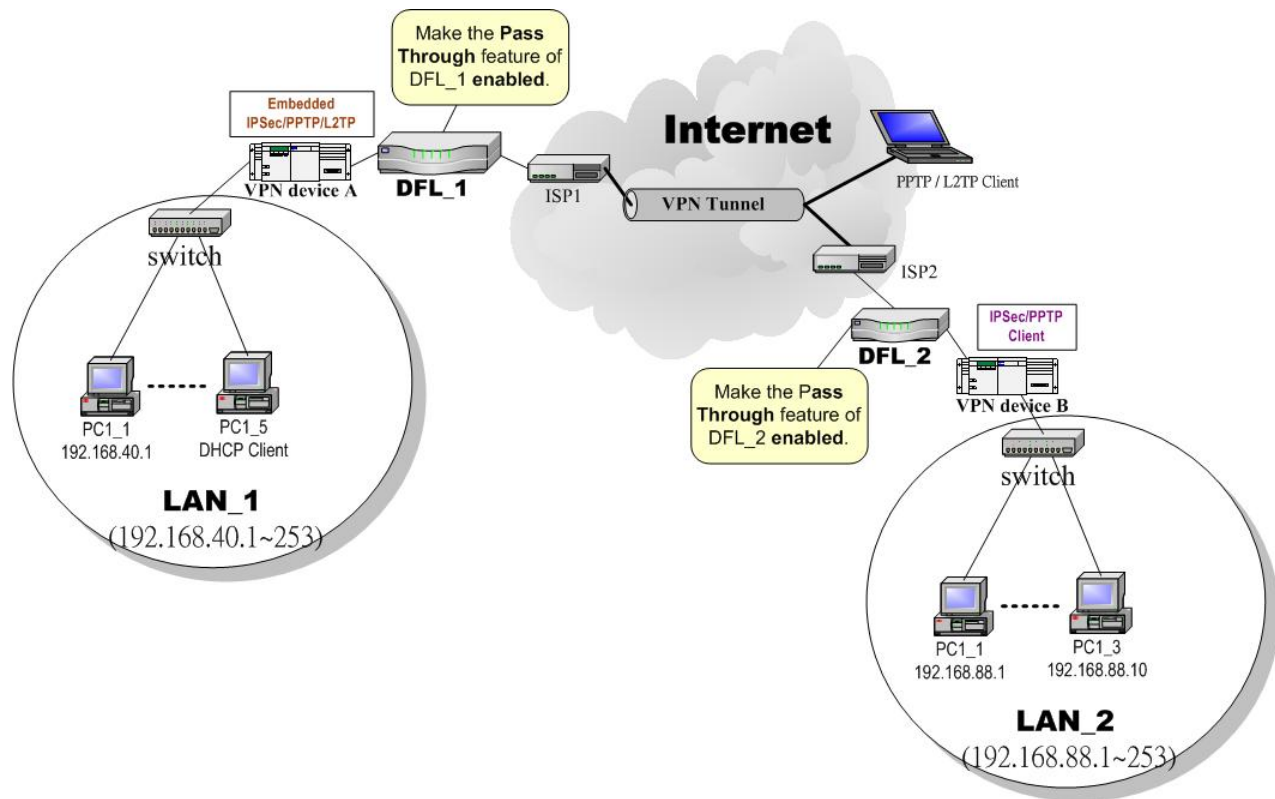


Figure 12-1 Enable the Pass Through feature of DFL-1500

Sometimes there are some VPN devices existing in your network topology. As Figure 12-1 illustrated, you are using the VPN device A under LAN_1 to establish IPsec/PPTP/L2TP with others (ex. VPN device B, PPTP/L2TP client). And you want to place the DFL-1500 into this topology, but you would like to remain the original VPN device to establish the VPN connections. Thus you can make the “Pass Through” feature enabled to make sure the IPsec/PPTP/L2TP traffic will not be blocked by the DFL-1500 device.

Step 1. Enable IPsec

If we need to setup DFL-1500 between the existed IPsec / PPTP / L2TP connections. We need to open up the Firewall blocking port of DFL-1500 in advance. Here we provide a simple way. You can through enable the IPsec / PPTP / L2TP pass through checkbox on this page. Then the VPN connections of IPsec / PPTP / L2TP will pass through DFL-1500. As well as DFL-1500 will play the middle forwarding device role.

ADVANCED SETTINGS > VPN Settings > Pass Through

| IPsec | VPN Hub | VPN Spoke | PPTP | L2TP | Pass Through |
|---|---------|-----------|------|------|---|
| | | | | | <input checked="" type="checkbox"/> Enable IPsec pass through <input checked="" type="checkbox"/> Enable PPTP pass through <input checked="" type="checkbox"/> Enable L2TP pass through |
| IPsec/PPTP/L2TP pass through make the DFL-1500 device as a middle forwarding device between. <ol style="list-style-type: none"> Two IPsec devices. Two PPTP devices. Two L2TP devices. | | | | | |
| <input type="button" value="Apply"/> | | | | | |

For the IPsec/PPTP/L2TP description, please refer the later individual chapter discussion.

The feature of the VPN can only be available while DFL-1500 connects to the internet via Default WAN Link.

Chapter 13

Virtual Private Network – IPsec

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

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

13.1 Demands

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

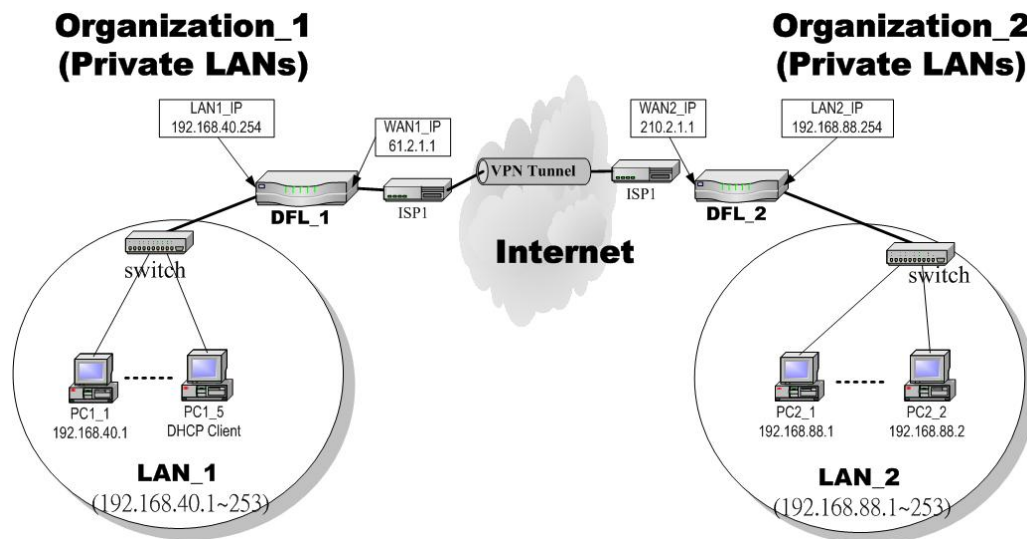


Figure 13-1 Organization_1 LAN_1 is making VPN tunnel with Organization_2 LAN_2

13.2 Objectives

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

13.3 Methods

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

| | IKE | Manual Key |
|------|--|------------|
| Same | “Local Address” means the local LAN subnet; “Remote Address” means the remote LAN subnet; “My IP Address” means the WAN IP address of the local VPN gateway while the “Peer’s IP Address” means the WAN IP address of the other VPN gateway. | |

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

Table 13-1 Compared IKE and Manual Key methods

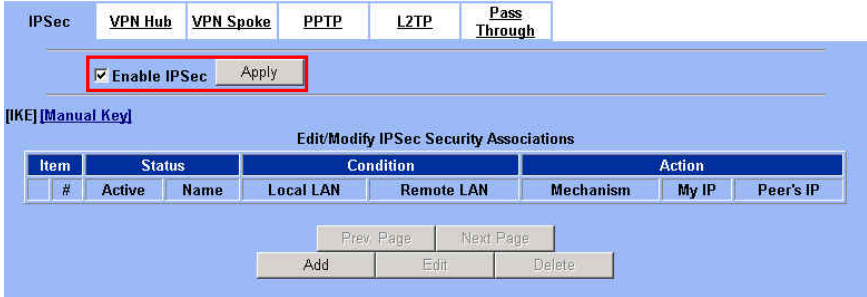
13.4 Steps

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

13.4.1 DES/MD5 IPsec tunnel: the IKE way

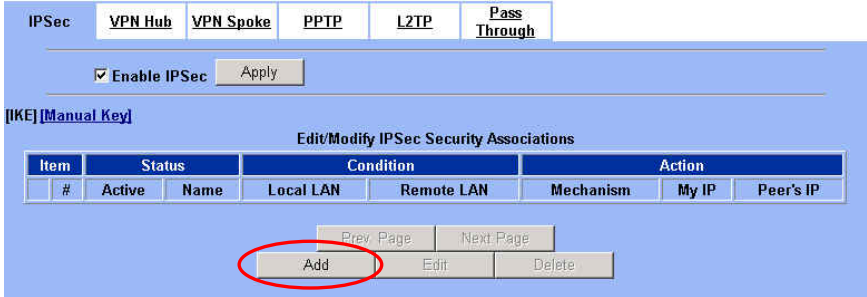
At DFL-1:

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

| | |
|---|--|
| <p>Step 1. Enable IPsec Check the <code>Enable IPsec</code> checkbox and click <code>Apply</code>.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec</p>  |
|---|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------|----------------------------------|----------------|---------|
| Enable IPsec | Enable IPsec feature of DFL-1500 | Enable/Disable | Enabled |

Table 13-2 Enable the IPsec feature

| | |
|---|--|
| <p>Step 2. Add an IKE rule 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>  |
|---|--|

| FIELD | DESCRIPTION | EXAMPLE |
|------------|--|--------------|
| IKE | Use the IKE (Internet Key Exchange) method to negotiate the key used in building IPsec tunnel. | Selected |
| Manual Key | Use the key which you have been designated to build IPsec tunnel in peer VPN device. | Non selected |

| BUTTON | DESCRIPTION |
|------------|---|
| Prev. Page | If there are more than one action pages, you can press Prev. Page to back to the previous page. |
| Next Page | If there are more than one action pages, you can press Next Page to go to the next page. |
| Add | Insert a new IPsec rule. |
| Edit | Edit the properties of the indicated IPsec rule. |
| Delete | Delete the indicated IPsec rule. |

Table 13-3 Add an IPsec policy rule

Step 3. Customize the rule

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

ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add

Self local IP Address

The opposite side IP Address

| | FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------|------------------------|---|---------------------------------|----------------|
| Status | Active | This field will activate this IPsec policy rule | Enable/Disable | Enabled |
| | IKE Rule Name | The name of this IPsec policy | text string | IKErule |
| Condition | Local Address Type | Determine the method to connect to the remote side of VPN by using the local subnet or the local single host. | Subnet Address / Single Address | Subnet Address |
| | IP Address | The local IP address | IPv4 format | 192.168.40.0 |
| | Prefix Len/Subnet Mask | The local IP Netmask | IPv4 format | 255.255.255.0 |

Part V
Virtual Private Network

| | | | | |
|--------|------------------------|--|--|---------------------|
| | Remote Address Type | Determine the method to connect to the local side of VPN by using the remote subnet or the remote single host. | Subnet Address / Single Address | Subnet Address |
| | IP Address | The remote IP address | IPv4 format | 192.168.88.0 |
| | Prefix Len/Subnet Mask | The remote IP Netmask | IPv4 format | 255.255.255.0 |
| Action | Negotiation Mode | Choose Main or Aggressive mode, see Chapter 12 for details. | Main / Aggressive | Main |
| | Encapsulation Mode | Choose Tunnel or Transport mode, see Chapter 12 for details. | Tunnel / Transport | Tunnel |
| | Outgoing Interface | The WAN interface you are going to build IPsec tunnel with. | WAN interfaces | WAN1 |
| | Peer's IP Address | The IP address of remote VPN device. The IP address may be fixed (Static) or dynamic. | Static IP / Dynamic IP | Static IP 210.2.1.1 |
| | My Identifier | Fill your information in this field. The filled information will be provided for the IPsec tunnel establishment. | IP Address / FQDN (domain name) / User FQDN (mail box) | IP Address |
| | Peer's Identifier | Fill the information of peer VPN device in this field. The filled information will be provided for the IPsec tunnel establishment. | IP Address / FQDN (domain name) / User FQDN (mail box) | IP Address |

| | | | | |
|--|----------------|---|--|-------------------------------------|
| | ESP Algorithm | <p>ESP Algorithm may be grouped by the items of the Encryption and Authentication Algorithms or execute separately.</p> <p>We can select below items, the Encryption and Authentication Algorithm combination or the below item Authentication Algorithm singly.</p> <p>Here Encryption Algorithms include DES(64 bits), 3DES(192 bits) and AES(128/192/256 bits)</p> <p>Authentication Algorithms include MD5(128 bits) and SHA1(160 bits)</p> | <p>Encrypt and Authenticate (DES, MD5) /</p> <p>Encrypt and Authenticate (DES, SHA1) /</p> <p>Encrypt and Authenticate (3DES, MD5) /</p> <p>Encrypt and Authenticate (3DES, SHA1) /</p> <p>Encrypt and Authenticate (AES, MD5) /</p> <p>Encrypt and Authenticate (AES, SHA1) /</p> <p>Encrypt only (DES) /</p> <p>Encrypt only (3DES) /</p> <p>Encrypt only (AES) /</p> <p>Authenticate only (MD5) /</p> <p>Authenticate only (SHA1)</p> | Encrypt and Authenticate (DES, MD5) |
| | AH Algorithm | Select Authentication Algorithm | <p>Authenticate (MD5) /</p> <p>Authenticate (SHA1)</p> | Disabled |
| | Pre-Shared Key | The key which is pre-shared with remote side. | text string | 1234567890 |

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

Step 4. Detail settings of IPSec IKE

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

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

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

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

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

Step 5. Remind to add a Firewall rule

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

ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add

IPsec **VPN Hub** VPN Spoke PPTP L2TP Pass Through

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

OK

Step 6. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Step 7. Customize the Firewall rule

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

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNA Dest. IP: LAN1_VPNA

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Back Apply

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through DFL-1500. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

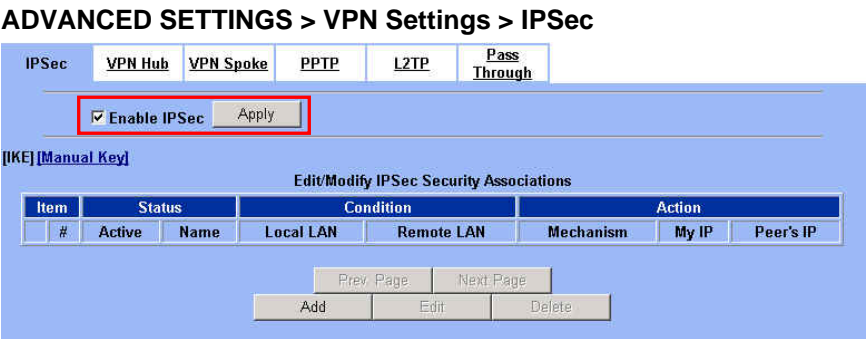
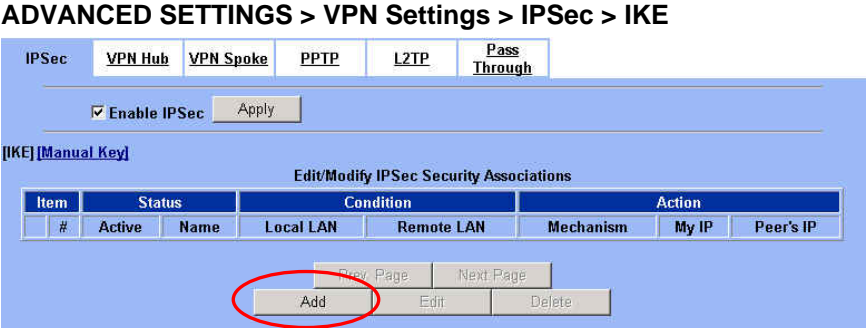
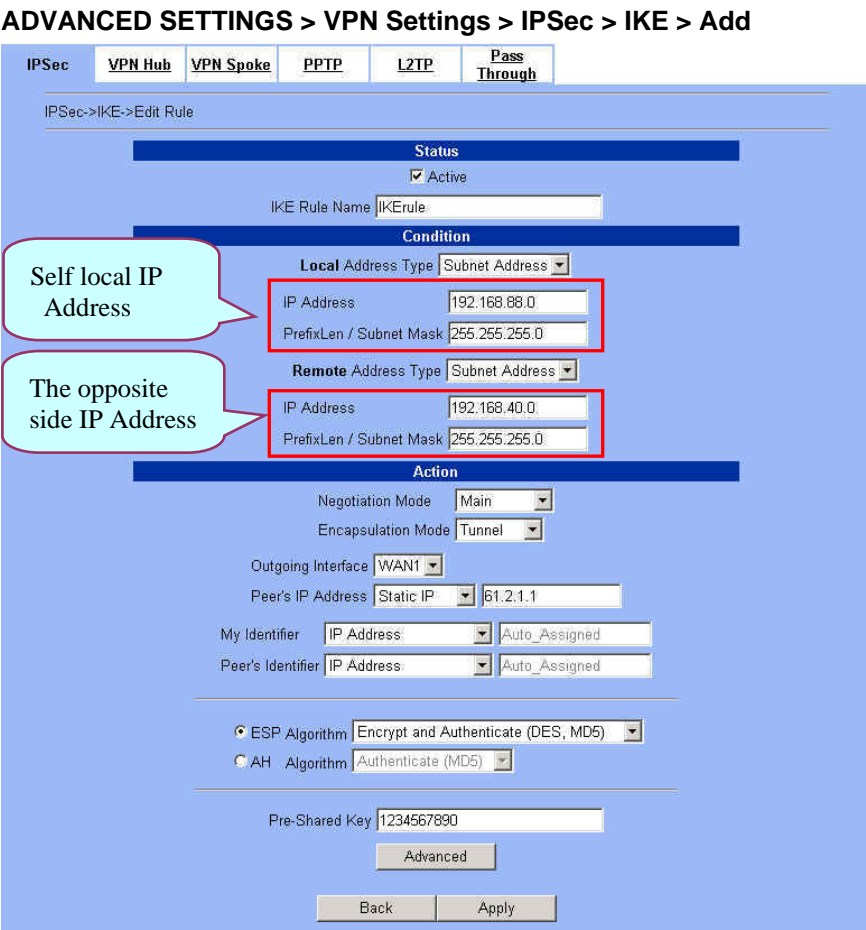
Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

At DFL-2:

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

| | |
|--|--|
| <p>Step 1. Enable IPsec</p> <p>Check the Enable IPsec checkbox and click Apply.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec</p>  |
| <p>Step 2. Add an IKE rule</p> <p>Click the IKE hyperlink and click Add to add a new IPsec VPN tunnel endpoint.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec > IKE</p>  |
| <p>Step 3. Customize the rule</p> <p>Check the Active checkbox. Enter a name for this rule like IKerule. Enter the Local IP Address (192.168.88.0/255.255.255.0) and the Remote IP Address (192.168.40.0/255.255.255.0). Select the Outgoing interface of this VPN/Firewall Router. Enter the public IP of the opposite-side VPN gateway (61.2.1.1) in the Peer's IP Address. Click the ESP Algorithm and select Encrypt and Authenticate (DES, MD5). Enter the Pre-Shared Key as 1234567890. Click the Apply button to store the settings. Note, in the Action region, you should choose either ESP Algorithm or AH Algorithm, or system will show error message.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add</p>  |

Step 4. Remind to add a Firewall rule

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

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add

Step 5. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

Step 6. Customize the Firewall rule

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

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from 192.168.40.0/24 to 192.168.88.0/24 will be allowed to pass through the DFL-1500 and successfully access the 192.168.88.0/24 through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

| Item | Status | Condition | Action | | | | |
|------|-----------|-----------|-----------|-----------|-------------|---------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | Allow/VPN | ALWAYS | WAN1_VPNB | LAN1_VPNB | ANY | Forward | N |
| 2 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

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

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

At DFL-1:

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

Step 1. Enable IPsec

Check the Enable IPsec checkbox and click Apply.

ADVANCED SETTINGS > VPN Settings > IPsec

IPsec VPN Hub VPN Spoke PPTP L2TP Pass Through

Enable IPsec Apply

[IKE] [Manual Key]

Edit/Modify IPsec Security Associations

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

Prev. Page Next Page

Add Edit Delete

Step 2. Add a Manual Key rule

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

ADVANCED SETTINGS > VPN Settings > IPsec > Manual Key

IPsec VPN Hub VPN Spoke PPTP L2TP Pass Through

Enable IPsec Apply

[IKE] [Manual Key]

Edit/Modify IPsec Security Associations

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

Prev. Page Next Page

Add Edit Delete

Step 3. Customize the rule

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

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

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

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

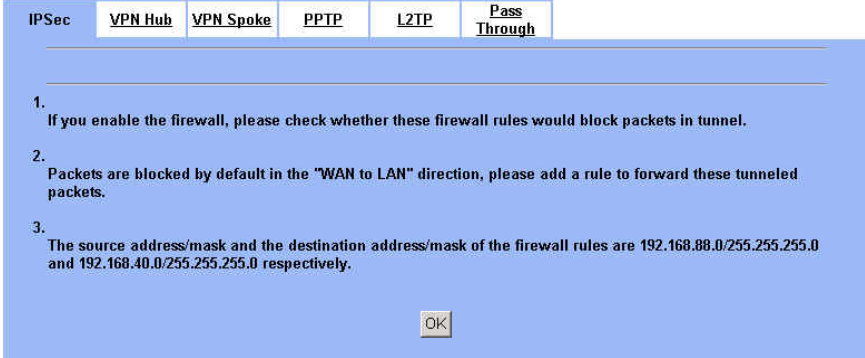
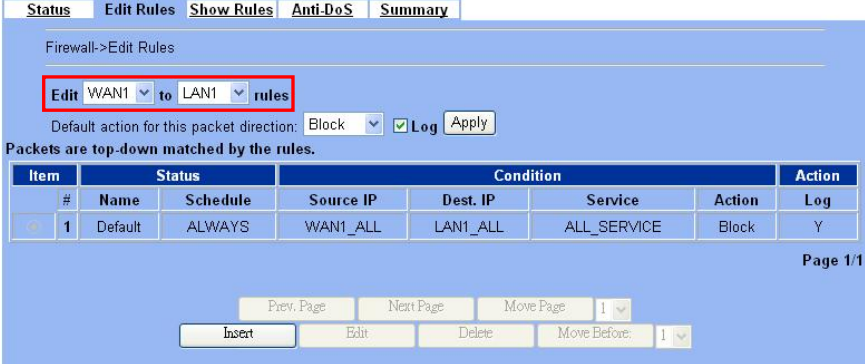
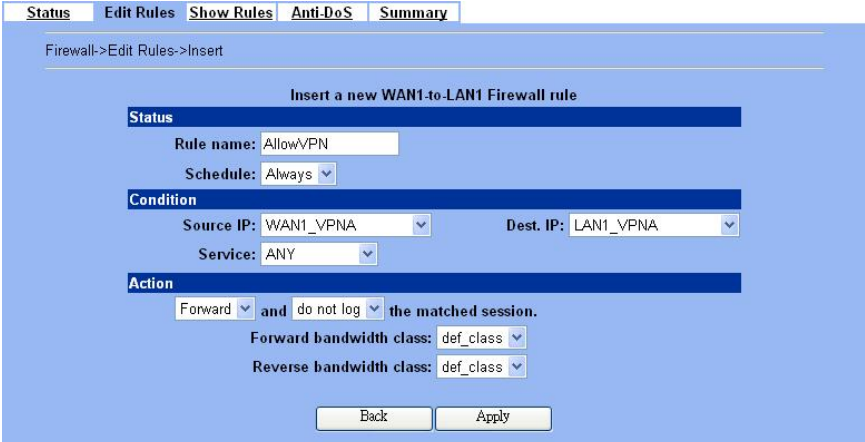
Table 13-6 Add a IPsec Manual Key rule

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

| | | | | |
|--------|-------------------------|---|----------|----|
| Action | Enable Replay Detection | Whether is the "Replay Detection" enabled ? | NO / YES | NO |
|--------|-------------------------|---|----------|----|

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

| <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. Just press the OK button to add a firewall rule.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec > Manual Key > Add</p>  | | | | | | | | | | | | | | | | |
|---|---|----------|-----------|----------|-------------|----------|---------|--------|-----|---|---------|--------|----------|----------|-------------|-------|---|
| <p>Step 6. Add a Firewall rule Same as that in IKE method. Please make sure that the Firewall is enabled. Select WAN1-to-LAN1 to display the rules of this direction. The default action of this direction is Block with Logs. We have to allow the VPN traffic from the WAN1 side to enter our LAN1 side. So we click the Insert button to add a Firewall rule before the default rule.</p> | <p>ADVANCED SETTINGS > Firewall > Edit Rules</p>  <table border="1"> <thead> <tr> <th>Item</th> <th>Name</th> <th>Schedule</th> <th>Source IP</th> <th>Dest. IP</th> <th>Service</th> <th>Action</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Default</td> <td>ALWAYS</td> <td>WAN1_ALL</td> <td>LAN1_ALL</td> <td>ALL_SERVICE</td> <td>Block</td> <td>Y</td> </tr> </tbody> </table> | Item | Name | Schedule | Source IP | Dest. IP | Service | Action | Log | 1 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |
| Item | Name | Schedule | Source IP | Dest. IP | Service | Action | Log | | | | | | | | | | |
| 1 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y | | | | | | | | | | |
| <p>Step 7. Customize the Firewall rule Enter the Rule Name as AllowVPN, Source IP as WAN1_VPN (192.168.88.0), and Dest. IP as LAN1_VPN (192.168.40.0). Click Apply to store this rule.</p> | <p>ADVANCED SETTINGS > Firewall > Edit Rules > Insert</p>  | | | | | | | | | | | | | | | | |

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through DFL-1500. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit **WANI** to **LAN1** rules

Default action for this packet direction: **Block** **Log**

Packets are top-down matched by the rules.

| Item | Status | Condition | Action | | | | |
|------|-----------|-----------|-----------|----------|-------------|---------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | Allow/VPN | ALWAYS | WANI_VPN | LAN1_VPN | ANY | Forward | N |
| 2 | Default | ALWAYS | WANI_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

Prev. Page Next Page Move Page 1

Move Before: 1

At DFL-2:

Second, we will use the Manual-Key way to install the IPsec properties of DFL-2.

Step 1. Enable IPsec

Check the **Enable IPsec** checkbox and click **Apply**.

ADVANCED SETTINGS > VPN Settings > IPsec

IPsec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

Enable IPsec

[IKE] [Manual Key]

Edit/Modify IPsec Security Associations

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

Prev. Page Next Page

Step 2. Add a Manual Key rule

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

ADVANCED SETTINGS > VPN Settings > IPsec > Manual Key

IPsec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

Enable IPsec

[IKE] [Manual Key]

Edit/Modify IPsec Security Associations

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

Prev. Page Next Page

Step 3. Customize the rule

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

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

Step 4. Remind to add a Firewall rule

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

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

Step 5. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Default action for this packet direction: Block Log

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Move Before: 1

Step 6. Customize the Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNB Dest. IP: LAN1_VPNB

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from 192.168.40.0/24 to 192.168.88.0/24 will be allowed to pass through the DFL-1500 and successfully access the 192.168.88.0/24 through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Default action for this packet direction: Block Log

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Move Before: 1

Chapter 14

Virtual Private Network –Dynamic IPsec

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

In the previous chapter, we have introduced static address method of IPsec. In this chapter, we will extend to explain how to make a dynamic VPN link between LAN_1 and LAN_2. The following Figure 14-1 is the real structure in our implemented process.

14.1 Demands

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

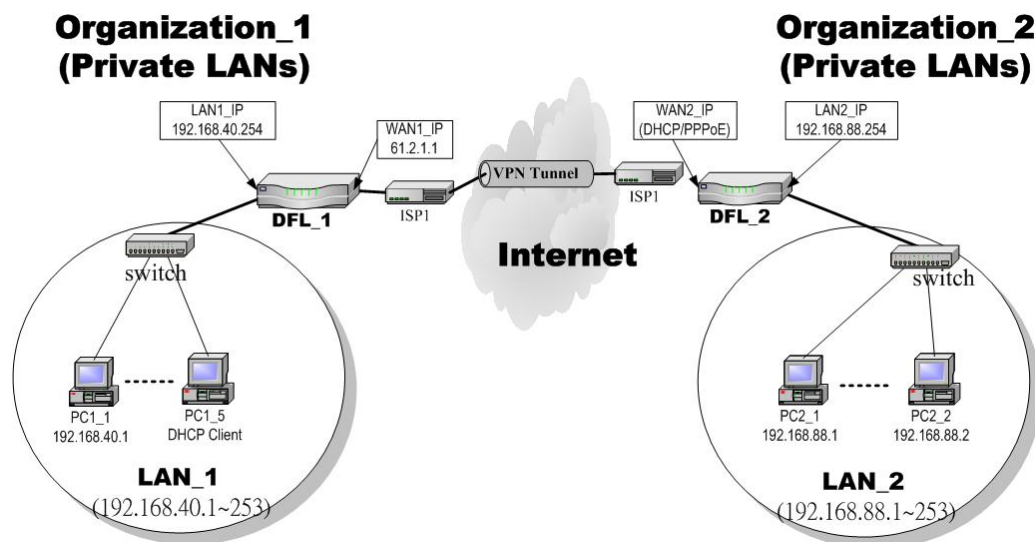


Figure 14-1 Organization_1 LAN_1 is making dynamic VPN tunnel with Organization_2 LAN_2

14.2 Objectives

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

14.3 Methods

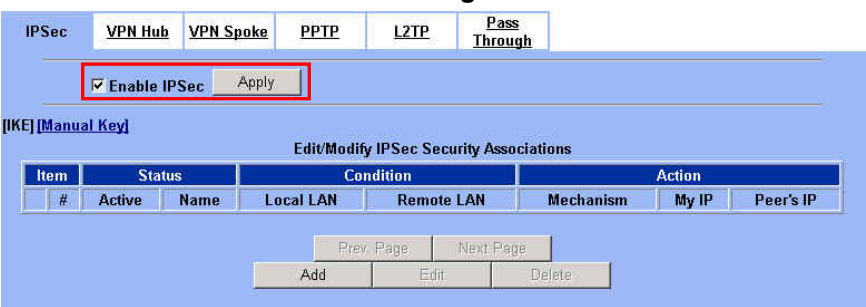
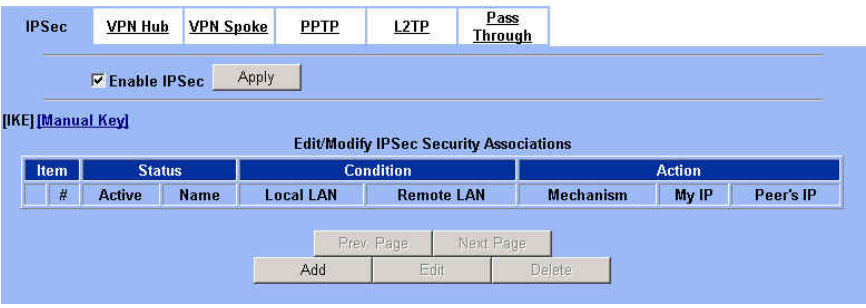
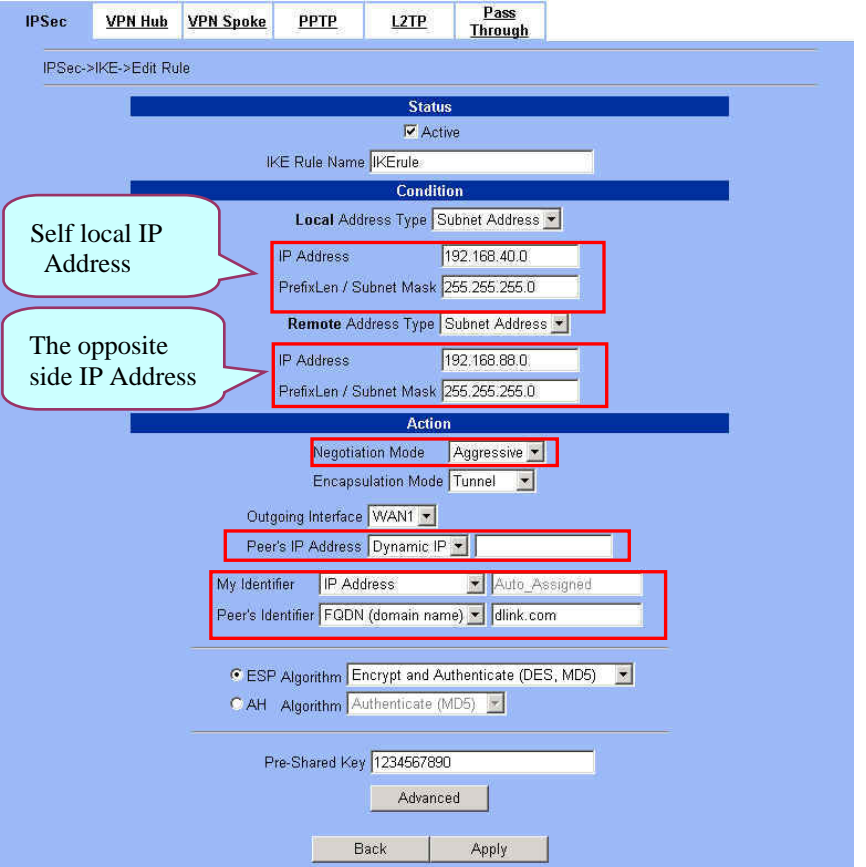
- Separately configure DFL-1 and DFL-2 which are the edge gateways of LAN_1 and LAN_2 respectively.

14.4 Steps

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

At DFL-1:

At the first, we will install the IPSec properties of DFL-1. For the related explanation, please refer to Chapter 12 and Chapter 13.

| | |
|---|--|
| <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>  |
| <p>Step 3. Customize the rule</p> <p>Check the <code>Active</code> checkbox. Enter a name for this rule like <code>IKERule</code>. Enter the <code>Local IP Address (192.168.40.0/255.255.255.0)</code> and the <code>Remote IP Address (192.168.88.0/255.255.255.0)</code>. Select the <code>Outgoing Interface</code> of this VPN/Firewall Router. Select <code>Dynamic IP</code> in the <code>Peer's IP Address</code>. Be sure to select <code>Aggressive mode</code> for the dynamic remote gateway address type. Click the <code>ESP Algorithm</code> and select <code>Encrypt and Authenticate (DES, MD5)</code>. Enter the <code>Pre-Shared Key</code> as <code>1234567890</code>. Click the <code>Apply</code> button to store the settings. Note, in the <code>Action</code> region. It should choose either <code>ESP Algorithm</code> or <code>AH Algorithm</code>, or system will show error message. If you hope to set the detailed item of <code>IKE</code> parameter. Click the <code>Advanced</code> button in this page. Otherwise it is ok to just leave the value default.</p> <p>Note that <code>Peers Identifier</code> must NOT be <code>IP Address</code> type in the <code>Dynamic IP</code> type. So, you have to select <code>FQDN (domain name)</code> or user <code>FQDN (mailbox)</code> as the <code>Peer's Identifier</code>.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add</p>  <p>Self local IP Address</p> <p>The opposite side IP Address</p> |

Step 4. Detail settings of IPSec IKE

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

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

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

IPSec->IKE->Edit Rule->Advanced

Condition
Transport Layer Protocol ANY

Action
Enable Replay Detection NO

Phase 1
Negotiation Mode Aggressive
Pre-Shared Key 1234567890
Encryption Algorithm Encrypt and Authenticate (DES, MD5)
SA Life Time 28800 sec min hour
Key Group DH2

Phase 2
Encapsulation Tunnel
Active Protocol ESP
Encryption Algorithm Encrypt and Authenticate (DES, MD5)
SA Life Time 28800 sec min hour
Perfect Forward Secrecy(PFS) DH1

Back Apply

Step 5. Remind to add a Firewall rule

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

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add

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

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

OK

Step 6. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

Status **Edit Rules** Show Rules Anti-DoS Summary

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Part V Virtual Private Network

Step 7. Customize the Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNA Dest. IP: LAN1_VPNA

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Back Apply

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from 192.168.88.0 / 255.255.255.0 pass through DFL-1500. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

At DFL-2:

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

Step 1. Enable IPSec

Check the Enable IPSec checkbox and click Apply.

ADVANCED SETTINGS > VPN Settings > IPSec

IPSec VPN Hub VPN Spoke PPTP L2TP Pass Through

Enable IPSec Apply

[IKE] [Manual Key]

Edit/Modify IPSec Security Associations

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

Prev. Page Next Page

Add Edit Delete

Step 2. Add an IKE rule
Click the **IKE** hyperlink and click **Add** to add a new IPsec VPN tunnel endpoint.

ADVANCED SETTINGS > VPN Settings > IPsec > IKE

IPsec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

Enable IPsec **Apply**

[IKE] [Manual Key]

Edit/Modify IPsec Security Associations

| Item # | Status | Name | Local LAN | Remote LAN | Mechanism | My IP | Peer's IP |
|--------|--------|------|-----------|------------|-----------|-------|-----------|
| | | | | | | | |

Prev Page Next Page
Add Edit Delete

Step 3. Customize the rule
Check the **Active** checkbox. Enter a name for this rule like **IKERule**. Enter the **Local IP Address** (192.168.88.0/255.255.255.0) and the **Remote IP Address** (192.168.40.0/255.255.255.0). Be sure to select **Aggressive** mode to match the DFL-1 settings. Select the **Outgoing interface** of this VPN/Firewall Router. Enter the public IP of the opposite-side VPN gateway (61.2.1.1) in the **Peer's IP Address**. Click the **ESP Algorithm** and select **Encrypt and Authenticate** (DES, MD5). Enter the **Pre-Shared Key** as 1234567890. Select **FQDN**(domain name) and enter **dlink.com** in **My Identifier** field. Click the **Apply** button to store the settings. Note, in the **Action** region, you should choose either **ESP Algorithm** or **AH Algorithm**, or system will show error message.

ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add

IPsec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

IPsec>IKE->Edit Rule

Status
 Active

Condition
IKE Rule Name: IKERule

Local Address Type: Subnet Address
 IP Address: 192.168.88.0
 PrefixLen / Subnet Mask: 255.255.255.0

Remote Address Type: Subnet Address
 IP Address: 192.168.40.0
 PrefixLen / Subnet Mask: 255.255.255.0

Action
 Negotiation Mode: Aggressive
 Encapsulation Mode: Tunnel

Outgoing Interface: WAN1
 Peer's IP Address: Static IP 61.2.1.1

My Identifier: FQDN (domain name) dlink.com
 Peer's Identifier: IP Address Auto_Assigned

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

Pre-Shared Key: 1234567890

Advanced
Back Apply

Self local IP Address

The opposite side IP Address

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

Step 4. Remind to add a Firewall rule
After finishing IPsec rule settings, we need to add a firewall rule. Here system shows a window message to remind you of adding a firewall rule. Just press the **OK** button to add a firewall rule.

ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add

IPsec **VPN Hub** **VPN Spoke** **PPTP** **L2TP** **Pass Through**

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

OK

Step 5. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Step 6. Customize the Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowVPN

Schedule: Always

Condition

Source IP: WAN1_VPNB Dest. IP: LAN1_VPNB

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: def_class

Reverse bandwidth class: def_class

Back Apply

Step 7. View the result

Now we have inserted a new rule before the default firewall rule. Any packets from 192.168.40.0/24 to 192.168.88.0/24 will be allowed to pass through the DFL-1500 and successfully access the 192.168.88.0/24 through the VPN tunnel.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Chapter 15

Virtual Private Network – Hub and Spoke VPN

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

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

15.1 Demands

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

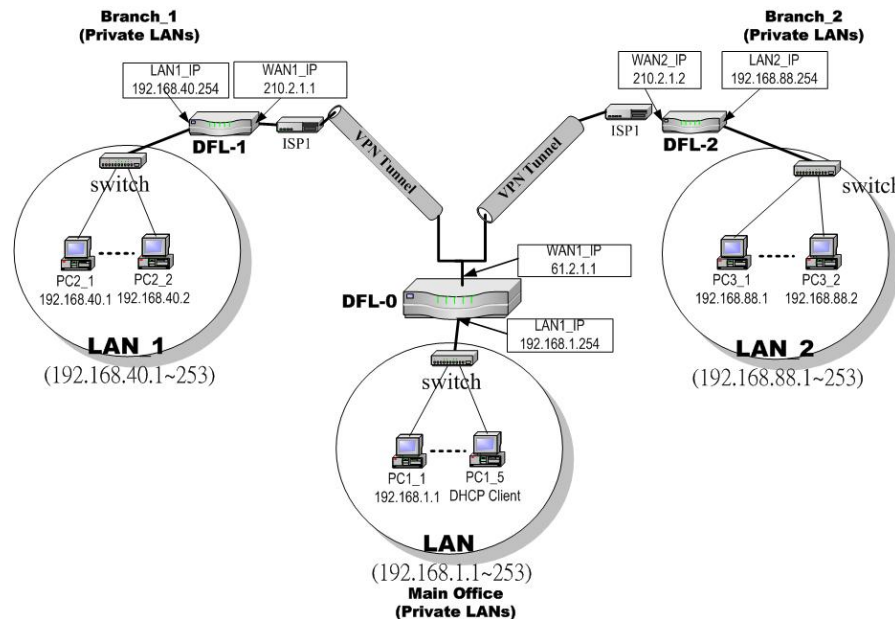


Figure 15-1 The Topology of the VPN Hub (Main Office) and VPN Spoke (Branch offices)

15.2 Objectives

- Using the VPN hub we can create a hub and spoke VPN configuration to direct traffic through a central DFL-1500 from one VPN tunnel to another VPN tunnel. Each VPN tunnel provides connectivity to a different remote VPN gateway. All of the VPN Hub member tunnels can establish VPN connections with any of the other member VPN tunnels.

15.3 Methods

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

15.4 Steps

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

Configuring the IPSec IKE tunnels

For the main office (the hub), we have to create the IKE tunnels, and then create VPN hub and add tunnels to it as members. For the VPN settings, please refer to Chapter 13 for details. Use the information in the following Table 15-1 to configure IKE tunnels. After finishing the IPSec VPN setting, please remember to add a WAN-to-LAN firewall rule.

| Field Name | Main Office Information | | Branch_1 Information | Branch_2 Information |
|-----------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Status | | | | |
| Active | Enable | Enable | Enable | Enable |
| IKE Rule Name | IKEVpnA | IKEVpnB | IKEMainVPN | IKEMainVPN |
| Condition | | | | |
| Local Address Type | Subnet Address | Subnet Address | Subnet Address | Subnet Address |
| IP Address | 192.168.1.0 | 192.168.1.0 | 192.168.40.0 | 192.168.88.0 |
| PrefixLen/Subnet Mask | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| Remote Address Type | Subnet Address | Subnet Address | Subnet Address | Subnet Address |
| IP Address | 192.168.40.0 | 192.168.88.0 | 192.168.1.0 | 192.168.1.0 |
| PrefixLen/Subnet Mask | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| Action | | | | |
| Negotiation Mode | Main | Main | Main | Main |
| Encapsulation Mode | Tunnel | Tunnel | Tunnel | Tunnel |
| Outgoing Interface | WAN1 | WAN1 | WAN1 | WAN1 |
| Peer's IP Address | 210.2.1.1 | 210.2.1.2 | 61.2.1.1 | 61.2.1.1 |
| My Identifier | IP Address | IP Address | IP Address | IP Address |
| Peer's Identifier | IP Address | IP Address | IP Address | IP Address |
| ESP Algorithm | Encrypt and Authenticate (DES, MD5) | Encrypt and Authenticate (DES, MD5) | Encrypt and Authenticate (DES, MD5) | Encrypt and Authenticate (DES, MD5) |
| AH Algorithm | Not selected | Not selected | Not selected | Not selected |
| Pre-Shared Key | 1234567890 | 1234567890 | 1234567890 | 1234567890 |

Table 15-1 The IKE tunnel configuration

Configuring the VPN Hub for Main Office**Step 1. Add a Firewall rule**

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

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

ADVANCED SETTINGS > Firewall > Edit Rules

The screenshot shows the 'ADVANCED SETTINGS > Firewall > Edit Rules' page. At the top, there are tabs for 'Status', 'Edit Rules', 'Show Rules', 'Anti-DoS', and 'Summary'. Below the tabs, it says 'Firewall->Edit Rules:'. There is a dropdown menu for 'Edit WAN1 to WAN1 rules'. Below that, it says 'Default action for this packet direction: Block' with a 'Log' checkbox checked and an 'Apply' button. A note states 'Packets are top-down matched by the rules.' Below this is a table with columns: Item, Status, Name, Schedule, Source IP, Dest. IP, Service, Action, and Log. The table contains one row: Item 1, Status Default, Name Default, Schedule ALWAYS, Source IP WAN1_ALL, Dest. IP WAN1_ALL, Service ALL_SERVICE, Action Block, and Log Y. At the bottom right, it says 'Page 1/1'. At the bottom, there are navigation buttons: 'First Page', 'Next Page', 'More Page: 1', 'Insert', 'Edit', 'Delete', and 'More Before: 1'.

Step 2. Customize a Firewall rule from Spoke1 to Spoke2

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

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

The screenshot shows the 'ADVANCED SETTINGS > Firewall > Edit Rules > Insert' page. At the top, there are tabs for 'Status', 'Edit Rules', 'Show Rules', 'Anti-DoS', and 'Summary'. Below the tabs, it says 'Firewall->Edit Rules->Insert'. The main heading is 'Insert a new WAN1-to-WAN1 Firewall rule'. Below this, there are sections for 'Status', 'Condition', and 'Action'. In the 'Status' section, 'Rule name' is 'AllowVPNA' and 'Schedule' is 'Always'. In the 'Condition' section, 'Source IP' is 'Spoke_1' and 'Dest. IP' is 'Spoke_2'. In the 'Action' section, 'Forward' is selected and 'do not log' is checked. Below the action section, there are 'Forward bandwidth class' and 'Reverse bandwidth class' both set to 'def_class'. At the bottom, there are 'Back' and 'Apply' buttons.

Step 3. Customize a Firewall rule from Spoke 2 to Spoke 1

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

The screenshot shows the 'ADVANCED SETTINGS > Firewall > Edit Rules > Insert' page. At the top, there are tabs for 'Status', 'Edit Rules', 'Show Rules', 'Anti-DoS', and 'Summary'. Below the tabs, it says 'Firewall->Edit Rules->Insert'. The main heading is 'Insert a new WAN1-to-WAN1 Firewall rule'. Below this, there are sections for 'Status', 'Condition', and 'Action'. In the 'Status' section, 'Rule name' is 'AllowVPNB' and 'Schedule' is 'Always'. In the 'Condition' section, 'Source IP' is 'Spoke_2' and 'Dest. IP' is 'Spoke_1'. In the 'Action' section, 'Forward' is selected and 'do not log' is checked. Below the action section, there are 'Forward bandwidth class' and 'Reverse bandwidth class' both set to 'def_class'. At the bottom, there are 'Back' and 'Apply' buttons.

Step 4. Add a VPN Hub

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

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

ADVANCED SETTINGS > VPN Settings > VPN Hub > Add

Configuring the VPN Spoke for the Branch_1

Step 1. Add a Firewall rule

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

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

ADVANCED SETTINGS > Firewall > Edit Rules

| Item | Status | Schedule | Source IP | Dest. IP | Service | Action | Log |
|------|---------|----------|-----------|----------|-------------|--------|-----|
| 1 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Step 2. Customize a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Step 3. Add a VPN Spoke in Branch_1

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

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

ADVANCED SETTINGS > VPN Settings > VPN Spoke > Add

Step 4. View the added VPN Spoke

You can view the added VPN spoke here.

ADVANCED SETTINGS > VPN Settings > VPN Spoke

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

Configuring the VPN Spoke for the Branch_2

Step 1. Add a Firewall rule

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

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

ADVANCED SETTINGS > Firewall > Edit Rules

| Item | Name | Status | Schedule | Source IP | Dest. IP | Service | Action | Log |
|------|---------|--------|----------|-----------|----------|-------------|--------|-----|
| 1 | Default | ALWAYS | | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Step 2. Customize a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Step 3. Add a VPN Spoke in Branch_2

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

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

ADVANCED SETTINGS > VPN Settings > VPN Spoke > Add

Step 4. View the added VPN Spoke

You can view the added VPN spoke here.

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

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

Chapter 16

PPTP Client with PPTP Server

This chapter introduces how to build a site to site VPN using PPTP client and PPTP server.

16.1 Demands

- In our branch office, we need to provide secure connection methods to connect back to headquarter for the internal company employees. As the following Figure 16-1 illustrated, The employees of LAN_2 area would like to access the resources of LAN_1 area with a security way.

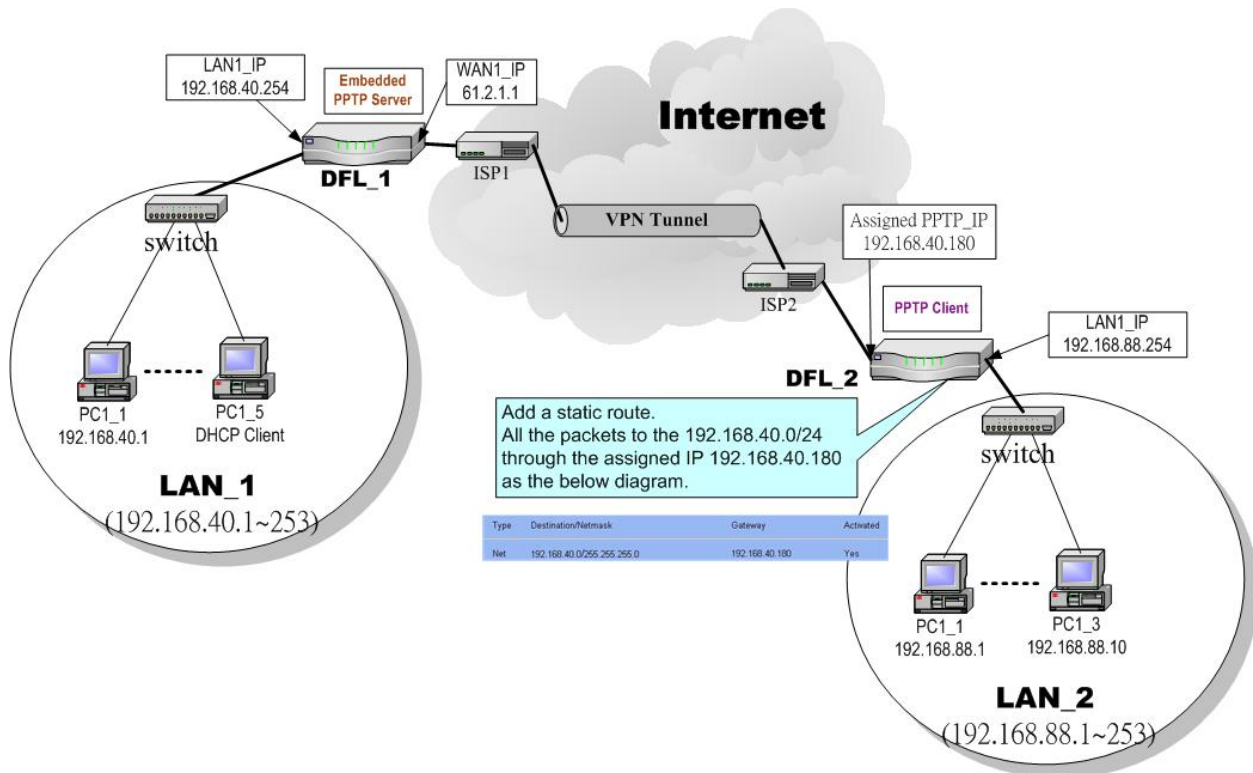


Figure 16-1 PPTP client with PPTP server

16.2 Objectives

- Make sure each employee in the branch office can use the network resource in the headquarter. After the VPN tunnel is established, the employees of LAN_2 seem to work in the same internal network of LAN_1, and keep the communication security.

16.3 Methods

- Setup the DFL-1500 of LAN_1 as PPTP Server. Then Setup the DFL-1500 of LAN_2 as the PPTP client. Besides we must add a static routing rule at the DFL-1500 of LAN_2.

16.4 Steps

➤ The DFL-1500 of LAN_1

| | |
|---|---|
| <p>Step 1. Enable PPTP server</p> <p>Fill the related field in this page. For the field description of this page, please refer section 17.4.</p> | <p>ADVANCED SETTINGS > VPN Settings > PPTP</p> |
|---|---|

➤ The DFL-1500 of LAN_2

| | |
|---|---|
| <p>Step 1. Enable PPTP Client</p> <p>Enter the IP address of PPTP Server and Username/Password. When connecting to the PPTP Server successfully, it will appear the allocated IP address for the PPTP client in the "Assigned IP" field.</p> | <p>ADVANCED SETTINGS > VPN Settings > PPTP > Client</p> |
|---|---|

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

Table 16-1 Setup PPTP Client settings

Step 2. Add a static routing entry

Add a static routing entry. For all the packets which are leaving for the 192.168.40.0/255.255.255.0, route these packets through the assigned IP address (192.168.40.180). For the field description and the procedure of adding a static route, please refer section 8.4.1.

ADVANCED SETTINGS > Routing > Static RouteStatic Route Policy Route

| # | Type | Destination/Netmask | Gateway | Activated |
|------------------------------------|------|----------------------------|----------------|-----------|
| <input checked="" type="radio"/> 1 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.180 | Yes |
| <input type="radio"/> 2 | - | - | - | - |
| <input type="radio"/> 3 | - | - | - | - |
| <input type="radio"/> 4 | - | - | - | - |
| <input type="radio"/> 5 | - | - | - | - |
| <input type="radio"/> 6 | - | - | - | - |
| <input type="radio"/> 7 | - | - | - | - |
| <input type="radio"/> 8 | - | - | - | - |
| <input type="radio"/> 9 | - | - | - | - |
| <input type="radio"/> 10 | - | - | - | - |

Prev. Page

Next Page

Add

Edit

Delete

Chapter 17

Remote Access VPN – PPTP

This chapter introduces PPTP and explains how to implement it.

17.1 Demands

1. One employee in our company may sometimes want to connect back to our corporate network to work on something. His PC is PC1_1 in LAN_1 instead of DMZ_1 so he cannot directly access the host by simply with virtual server settings. This causes inconvenience for the employee to work remotely.

17.2 Objectives

1. With PPTP tunneling, emulate the mobile employee as a member in LAN1 after he dials in the corporate network. Then he can access all computers in LAN_1 just as if he stays in the office covered by LAN1.

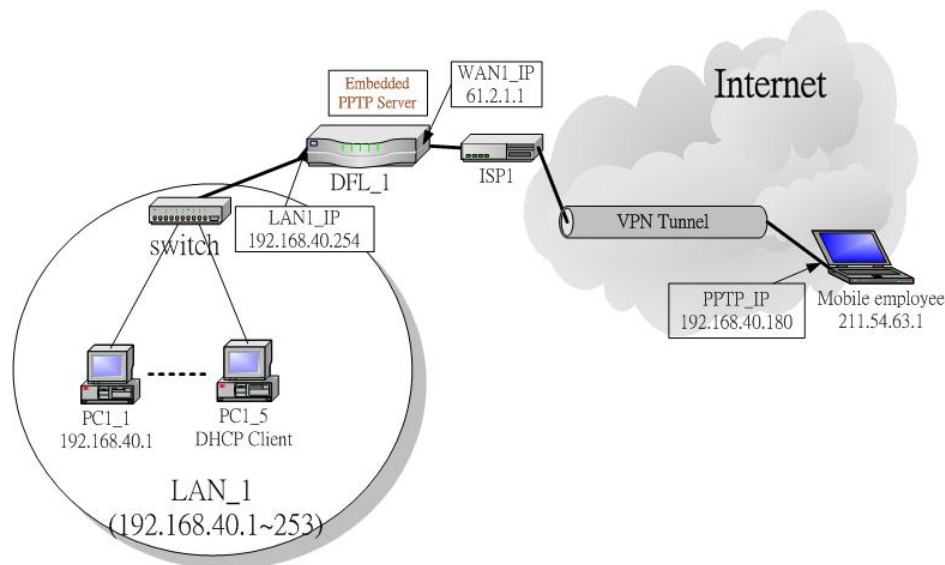


Figure 17-1 PPTP method connection

17.3 Methods

1. Setup the PPTP server at DFL-1500. Setup the remote PC as the PPTP client. After dialing up to DFL-1, DFL-1 will assign a private IP which falls in the range of the settings in the PPTP server at DFL-1. Suppose the range is defined as 192.168.40.180 ~ 192.168.40.199, the remote host may get an IP of 192.168.40.180 and logically become a member in LAN1.

17.4 Steps

Step 1. Enable PPTP Server

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. Click the `Apply` to finish configurations.

ADVANCED SETTINGS > VPN Settings > PPTP

The screenshot shows the 'ADVANCED SETTINGS > VPN Settings > PPTP' configuration window. It has tabs for 'IPSec', 'PPTP', 'L2TP', and 'Pass Through'. The 'PPTP' tab is selected. A checkbox labeled 'Enable PPTP Server' is checked. Below this, there are two radio buttons: '[Server]' and '[Client]', with '[Client]' selected. The configuration fields are: 'Local IP' with the value '192.168.40.254'; 'Assigned IP Range' with 'Start' at '192.168.40.180' and 'End' at '192.168.40.199'; 'Username' with the value 'PptUsers'; and 'Password' with a masked value '*****'. An 'Apply' button is at the bottom.

| FIELD | | DESCRIPTION | EXAMPLE |
|--------------------|-------|--|----------------|
| Enable PPTP Server | | Enable PPTP feature of the DFL-1500 | Enabled |
| Local IP | | The Local IP is the allocated IP address in the internal Network after PPTP client dials in the DFL-1500. | 192.168.40.254 |
| Assigned IP Range | Start | The Start IP is the allocated starting IP address in the internal network after PPTP client dials in the DFL-1500. | 192.168.40.180 |
| | End | The End IP is the allocated ending IP address in the internal network after PPTP client dials in the DFL-1500. | 192.168.40.199 |
| Username | | The account which allow PPTP client user to dial in DFL-1500. | PptUsers |
| Password | | The password which allow PPTP client user to dial in DFL-1500. | Dif3wk |

Table 17-1 Setup PPTP Server

Step 2. Setup Windows XP/2000 PPTP clients

Note that in the DFL-1500 release II version, both PPTP and L2TP can support MPPE. In other words, you can choose "Require data encryption" while a client computer running Windows XP/2000. However, this release II version will not support MS-CHAP, you have to check MS-CHAPv2 checkbox if you would like to require data encryption.

Configuring A PPTP Dial-Up Connection

1. Configuring a PPTP dial-up connection
2. Go to `Start > Control Panel > Network and Internet Connections > Make new connection`.
3. Select `Create a connection to the network of your workplace and select Next`.
4. Select `Virtual Private Network Connection and select Next`.
5. Give a Name the connection and select `Next`.
6. If the `Public Network dialog box` appears, choose the `Don't dial up initial connection and select Next`.
7. In the `VPN Server Selection dialog`, enter the public IP or hostname of the DFL-1500 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 <code>Properties > Security > Advanced > Settings</code>.3. Select <code>No Encryption</code> from the <code>Data Encryption</code> and click <code>Apply</code>.4. Select the <code>Properties > Networking</code> tab.5. Select <code>PPTP VPN</code> from the <code>VPN Type</code>. Make sure the following are selected: TCP/IP QoS Packet Scheduler6. Select <code>Apply</code>. <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 <code>User Name</code> and <code>Password</code>.4. Select <code>Connect</code>. |
|--|--|

Chapter 18

Remote Access VPN – L2TP

This chapter introduces L2TP and explains how to implement it.

18.1 Demands

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

18.2 Objectives

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

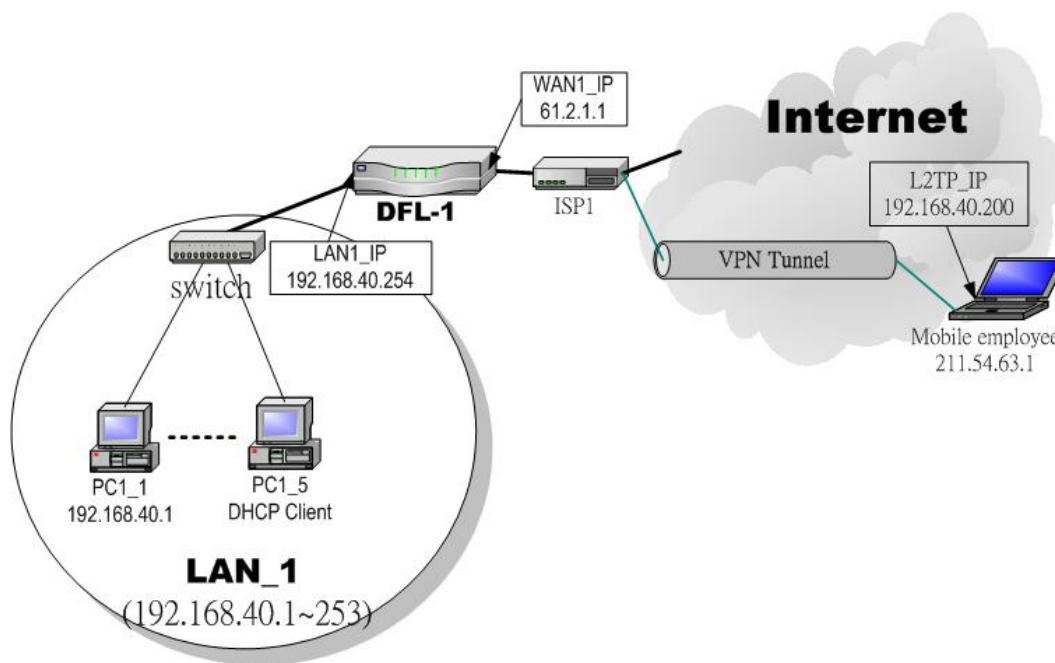


Figure 18-1 L2TP method connection

18.3 Methods

1. Setup the L2TP server at DFL-1500 (LNS: L2TP Network Server). After dialing up to DFL-1500, DFL-1500 will assign a private IP which falls in the range of the settings in the L2TP server at DFL-1500. Suppose the range is defined as 192.168.40.200 ~ 192.168.40.253, the remote host may get an IP of 192.168.40.200 and logically become a member in LAN_1.

18.4 Steps

18.4.1 Setup L2TP Network Server

Step 1. Enable L2TP LNS

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

ADVANCED SETTINGS > VPN Settings > L2TP

The screenshot shows the configuration page for L2TP. At the top, there are tabs for IPsec, PPTP, L2TP, and Pass Through. The L2TP tab is selected. Below the tabs, there is a checkbox labeled 'Enable L2TP LNS' which is checked. Underneath, there are several input fields: 'Local IP' with the value '192.168.40.254', 'Assigned IP Range' with 'Start' at '192.168.40.200' and 'End' at '192.168.40.253', 'Secure Client IP Range' with 'Start' at '211.54.63.1' and 'End' at '211.54.63.5', 'Username' with the value 'L2tpUsers', and 'Password' with the value '*****'. An 'Apply' button is located at the bottom of the form.

| FIELD | DESCRIPTION | EXAMPLE |
|------------------------|--|----------------|
| Enable L2TP LNS | Enable L2TP LNS feature of DFL-1500 | Enabled |
| Local IP | The Local IP is the allocated IP address in the internal network after default gateway of L2TP client dials in the DFL-1500. | 192.168.40.254 |
| Assigned IP Range | Start The Start IP is the allocated starting IP address in the internal network after L2TP client dials in the DFL-1500. | 192.168.40.200 |
| | End The End IP is the allocated ending IP address in the internal network after L2TP client dials in the DFL-1500. | 192.168.40.253 |
| Secure Client IP Range | Start The IP address starting range which is allowed user to dial in LNS server by using L2TP protocol. | 211.54.63.1 |
| | End The IP address ending range which is allowed user to dial in LNS server by using L2TP protocol. | 211.54.63.5 |
| Username | The account which allows L2TP client user to dial in DFL-1500. | L2tpUsers |
| Password | The password which allows L2TP client user to dial in DFL-1500. | Dif3wk |

Table 18-1 Setup L2TP LNS Server settings

Step 2. Setup Windows XP/2000 L2TP clients

Note that in the DFL-1500 release II version, both PPTP and L2TP can support MPPE. In other words, you can choose “Require data encryption” while a client computer running Windows XP/2000. However, this release II version will not support MS-CHAP, you have to check MS-CHAPv2 checkbox if you would like to require data encryption.

Configuring A L2TP Dial-Up Connection

1. Configure a L2TP dial-up connection
2. Go to Start > Control Panel > Network and Internet Connections > Make new connection.
3. Select Create a connection to the network of your workplace and select Next.
4. Select Virtual Private Network Connection and select Next.
5. Give a Name the connection and select Next.
6. If the Public Network dialog box appears, choose the Don't dial up initial connection and select Next.
7. In the VPN Server Selection dialog, enter the public IP or hostname of the DFL-1500 to connect to and select Next.
8. Set Connection Availability to Only for myself and select Next.
9. Select Finish.

Customize the VPN Connection

1. Right-click the icon that you have created.
2. Select Properties > Security > Advanced > Settings.
3. Select No Encryption from the Data Encryption and click Apply.
4. Select the Properties > Networking tab.
5. Select L2TP VPN from the VPN Type.

Make sure the following are selected:

 - TCP/IP
 - QoS Packet Scheduler
6. Select Apply.

Editing Windows Registry

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

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

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

Connecting to the L2TP VPN

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

Chapter 19

Remote Access VPN – DS-601 VPN client

This chapter introduces Remote Access VPN using DS-601 VPN client and explains how to implement it.

As described in the Figure 2-1, we will extend to explain how to make a VPN link between LAN_1 and a remote client in this chapter. The following Figure 19-1 is the real structure in our implemented process.

19.1 Demands

1. When someone is on a business trip and need to connect back to the company by using VPN function, he uses the DS-601 VPN client to make IPSec VPN tunnel with Organization_1 LAN_1. See the following diagram for the details.

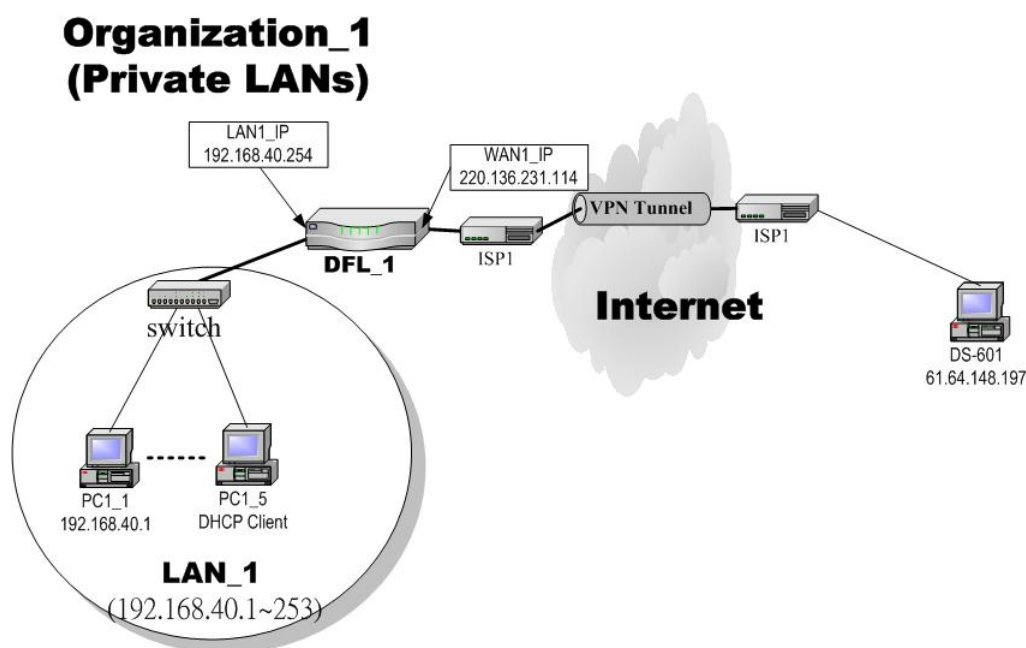


Figure 19-1 The client DS-601 is making IPSec VPN tunnel with Organization_1 LAN_1

19.2 Objectives

1. Let the users in LAN_1 and the client DS-601 share the resources through a secure channel established using the IPSec.

19.3 Methods

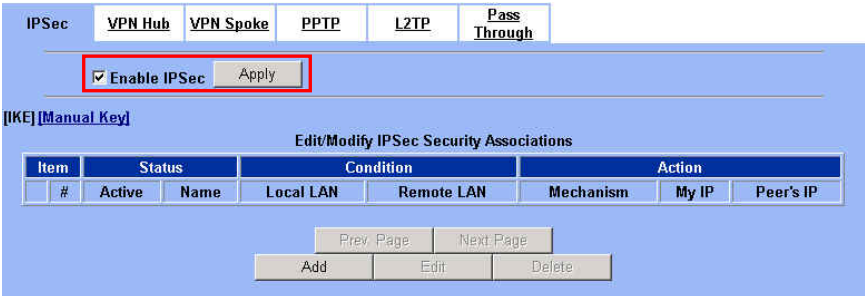
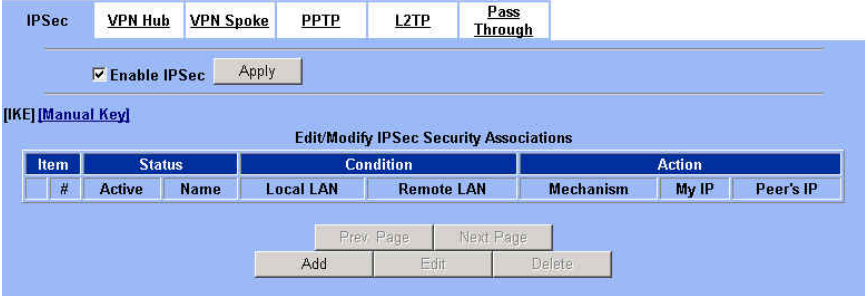
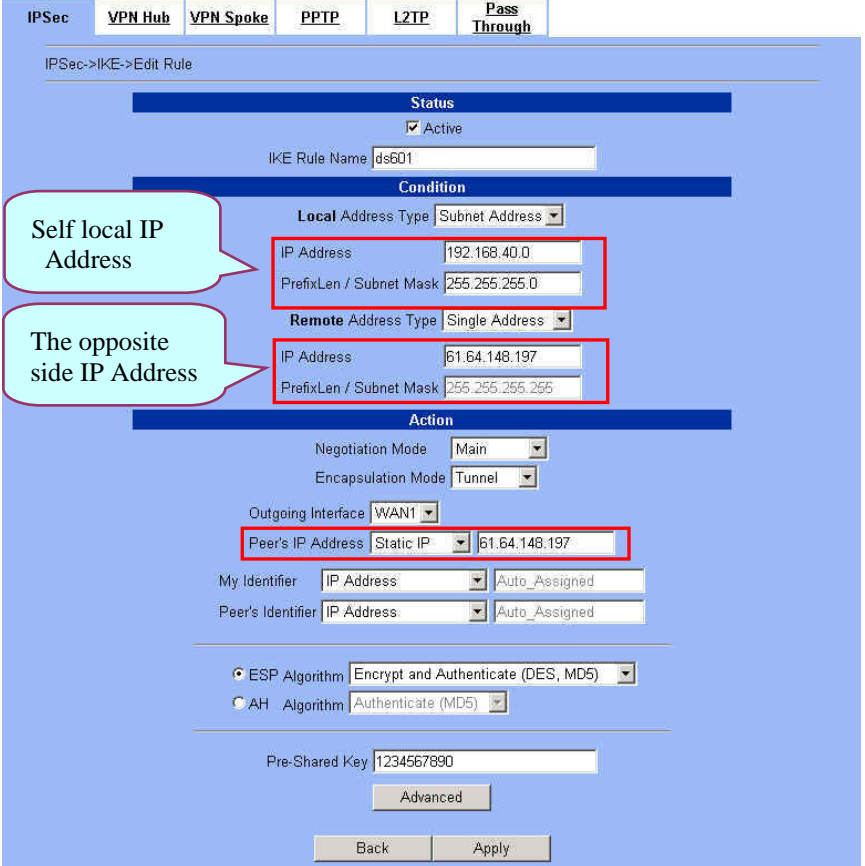
1. Separately configure DFL-1 and DS-601 VPN client to make IPSec VPN tunnel..

19.4 Steps

In the following, we will introduce you how to setup the IPSec between Organization_1 LAN_1 and DS-601 VPN client.

At DFL-1:

At the first, we will install the IPSec properties of 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>  |
| <p>Step 3. Customize the rule</p> <p>Check the <code>Active</code> checkbox. Enter a name for this rule like <code>ds601</code>. Enter the <code>Local IP Address</code> (<code>192.168.40.0/255.255.255.0</code>) and the <code>Remote IP Address</code> (<code>61.64.148.197/255.255.255.255</code>). Select the <code>Outgoing Interface</code> of this VPN/Firewall Router. Enter the public IP of the opposite-side VPN gateway (<code>61.64.148.197</code>) in the <code>Peer's IP Address</code>. Click the <code>ESP Algorithm</code> and select <code>Encrypt and Authenticate (DES, MD5)</code>. Enter the <code>Pre-Shared Key</code> as <code>1234567890</code>. Click the <code>Apply</code> button to store the settings. Note, In the <code>Action</code> region. It should choose either <code>ESP Algorithm</code> or <code>AH Algorithm</code>, or system will show error message. If you hope to set the detailed item of IKE parameter. Click the <code>Advanced</code> button in this page. Otherwise it is ok to just leave the value default.</p> | <p>ADVANCED SETTINGS > VPN Settings > IPsec > IKE > Add</p>  |

Step 4. Detailed settings of IPSec IKE

In this page, we will set the detailed value of IKE parameter.

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

Step 5. Remind to add a Firewall rule

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

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add

Step 6. Add a Firewall rule

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

ADVANCED SETTINGS > Firewall > Edit Rules

| Item | Name | Status | Schedule | Source IP | Dest. IP | Service | Action | Log |
|------|---------|--------|----------|-----------|----------|-------------|--------|-----|
| 1 | Default | ALWAYS | | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Step 7. Customize the Firewall rule

Enter the Rule Name as AllowDS-601, Source IP as WAN1_ds601 (61.64.148.197), and Dest. IP as LAN1_VPNA (192.168.40.0). Click Apply to store this rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: AllowDS-601
Schedule: Always

Condition

Source IP: WAN1_ds601 Dest. IP: LAN1_VPNA
Service: ANY

Action

Forward and do not log the matched session.
Forward bandwidth class: def_class
Reverse bandwidth class: def_class

Back Apply

Step 8. View the result

Here we have a new rule before the default firewall rule. This rule will allow packets from WAN1_ds601 (61.64.148.197 / 255.255.255.255) pass through DFL-1500. And accomplish the VPN tunnel establishment.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules
Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

| Item | Status | Condition | Action | |
|------|-------------|-----------|---|-----------------|
| # | Name | Schedule | Source IP Dest. IP Service | Action Log |
| 1 | AllowDS-601 | ALWAYS | WAN1_ds601 LAN1_VPNA ANY | Forward N |
| 2 | Default | ALWAYS | WAN1_ALL LAN1_ALL ALL_SERVICE | Block Y |



Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

At DS-601 VPN client:

Here we will introduce you how to setup DS-601 VPN client properties. Before that, please install the DS-601 VPN client into the remote client first.

| | |
|--|--|
| <p>Step 1. Enter a Connection Name</p> <p>Enter DFL-1500 in the Name of the connection field and click Next to proceed.</p> | <p>Configuration > Profile Settings > New Entry</p>  <p>The screenshot shows a window titled "Destination Assistant" with the D-Link logo. The main heading is "Connection Name" with the instruction "Enter the name of the connection". Below this, a text box contains "DFL-1500". At the bottom are buttons for "< Back", "Next >", and "Cancel".</p> |
| <p>Step 2. Select Link Type</p> <p>Select LAN (over IP) in the Communication media field and the click Next to proceed.</p> | <p>Configuration > Profile Settings > New Entry</p>  <p>The screenshot shows a window titled "Destination Assistant" with the D-Link logo. The main heading is "Link type (Dial up configuration)" with the instruction "Select the media type of the connection". Below this, a dropdown menu labeled "Communication media:" is set to "LAN (over IP)". At the bottom are buttons for "< Back", "Next >", and "Cancel".</p> |

Step 3. Setup VPN gateway

Enter the VPN gateway IP (220.136.231.114) which is also the DFL-1's WAN1 IP. Click Next to proceed.

Configuration > Profile Settings > New Entry

The screenshot shows the 'Destination Assistant' window with the title 'VPN gateway parameters'. The subtitle is 'To which VPN gateway should the connection be established?'. The D-Link logo is in the top right. Below the subtitle, there is a text box with the instruction: 'Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.' The 'Gateway' field contains '220.136.231.114'. There is an unchecked checkbox for 'Use extended authentication (XAUTH)'. The 'Username' and 'Password' fields are empty. The 'Password (Confirm)' field is also empty. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Step 4. Pre-share Key

Enter 1234567890 in the Shared secret field and retype it in the Confirm secret field. Select IP Address and enter 61.64.148.197 as the Type and ID in the Local identity area.

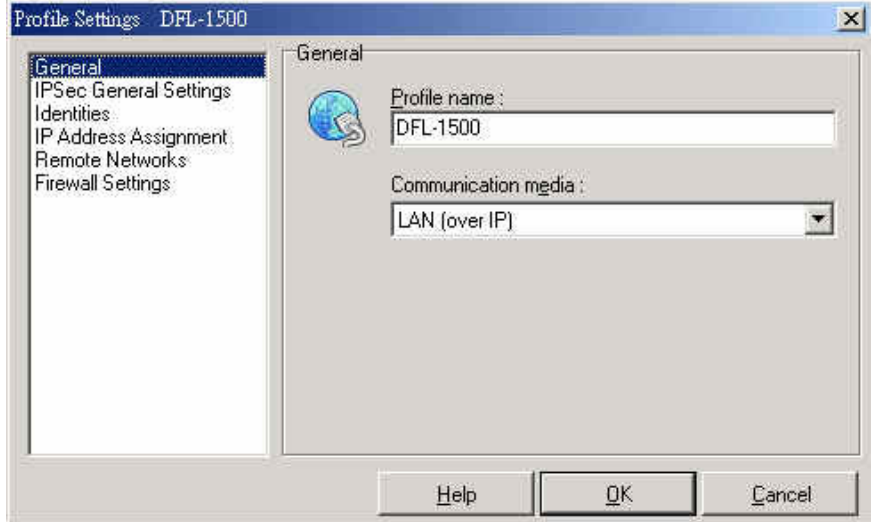
Configuration > Profile Settings > New Entry

The screenshot shows the 'Destination Assistant' window with the title 'Pre-shared key'. The subtitle is 'Common secret for data encryption'. The D-Link logo is in the top right. Below the subtitle, there is a text box with the instruction: 'A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically on both sides (VPN client and VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type.' The 'Pre-shared key' section has two fields: 'Shared secret' and 'Confirm secret', both containing 'XXXXXXXXXX'. The 'Local identity' section has a 'Type' dropdown menu set to 'IP Address' and an 'ID' field containing '61.64.148.197'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Step 5. General information

After finishing the previous setting, we can view the general information here.

Configuration > Profile Settings > Configure > General



Step 6. IPsec General Settings

Check if the Gateway IP is correct, and then click the Policy editor to edit IKE and IPsec policy.

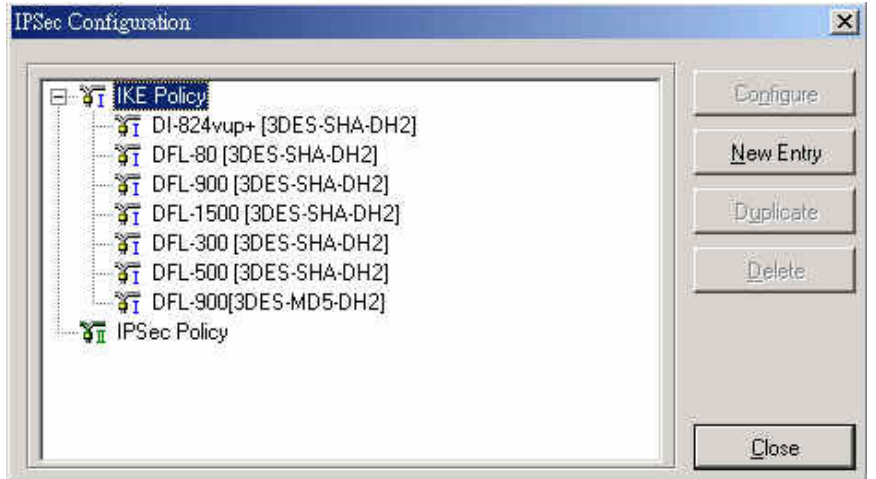
Configuration > Profile Settings > Configure > IPsec General Settings



Step 7. Policy editor

Click IKE Policy to edit the IKE policy.

Configuration > Profile Settings > Configure > IPsec General Settings > Policy editor



Step 8. Setup IKE Policy

Enter DFL-1500[DES-MD5] as the IKE Policy name. Select DES/MD5/DH-Group 2 [1024 Bit] in the Encryption/Hash/DH Group field. Click OK to finish the settings.

Configuration > Profile Settings > Configure > IPSec General Settings > Policy editor > IKE Policy

IKE Proposals

Policy name : DFL-1500 [DES, MD5]

| Authentication | Encryption | Hash | DH Group |
|----------------|------------|------|-----------------------|
| Preshared Key | DES | MD5 | DH-Group 2 (1024 Bit) |

Authentication : Preshared Key Add

Encryption : DES Remove

Hash : MD5

DH Group : DH-Group 2 (1024 Bit)

Help OK Cancel

Step 9. Setup IPSec Policy

Enter DFL-1500[DES-MD5] as the IPSec Policy name. Select DES and MD5 in the Transform and Authentication field. Click OK to finish the settings.

Configuration > Profile Settings > Configure > IPSec General Settings > Policy editor > IPSec Policy

IPSec Proposals

Policy name : DFL-1500 [DES-MD5]

| Protocol | Transform | None |
|----------|-----------|------|
| ESP | DES | MD5 |

Protocol : ESP Add

Transform : DES Remove

Authentication : MD5

Help OK Cancel

Step 10. IPSec advanced options

In the Advanced options area, please select Main Mode in the Exch. mode and DH-Group 1 [768 Bit] in the PFS group.

Configuration > Profile Settings > Configure > IPSec General Settings > Advanced Options

Profile Settings DFL-1500

General
IPSec General Settings
 Identities
 IP Address Assignment
 Remote Networks
 Firewall Settings

IPSec General Settings:

Gateway : 220.136.231.114

Policies:

IKE policy : DFL-1500 [DES, MD5]

IPSec policy : DFL-1500 [DES-MD5]

Policy lifetimes ... Policy editor ...

Advanced options:

Exch. mode : Main Mode

PFS group : DH-Group 1 (768 Bit)

Use IP compression (LZS)

Disable DPD (Dead Peer Detection)

Help OK Cancel

Step 11. View Identities

Check if the Local Identity and the Pre-shared key are correct or not. If yes, click OK to finish the settings.

Configuration > Profile Settings > Configure > Identities

Profile Settings DFL-1500

General
 IPSec General Settings
Identities
 IP Address Assignment
 Remote Networks
 Firewall Settings

Identities:

Local identity:

Type : IP Address

ID : 61.64.148.197

Pre-shared key:

Shared secret : *****

Confirm secret : *****

Use extended authentication (XAUTH)

Username : _____

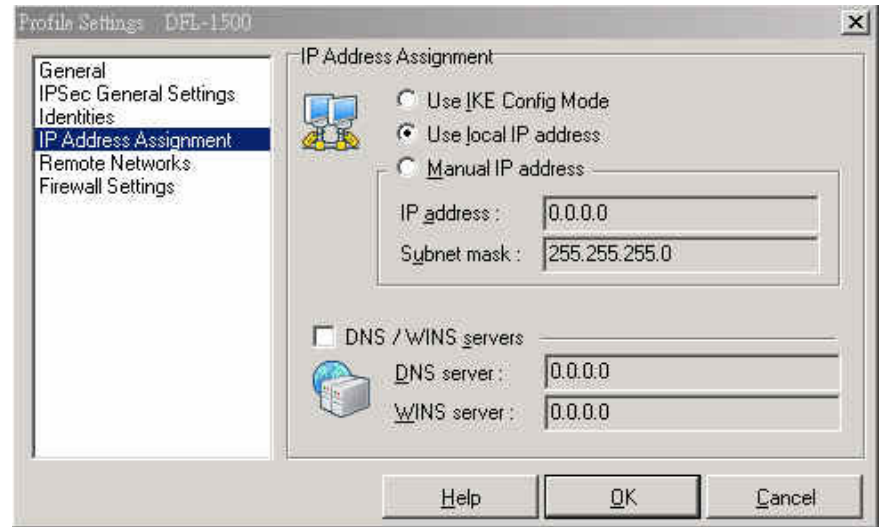
Password : _____

Help OK Cancel

Step 12. IP Address Assignment

Select Use local IP address and then click OK to finish this settings.

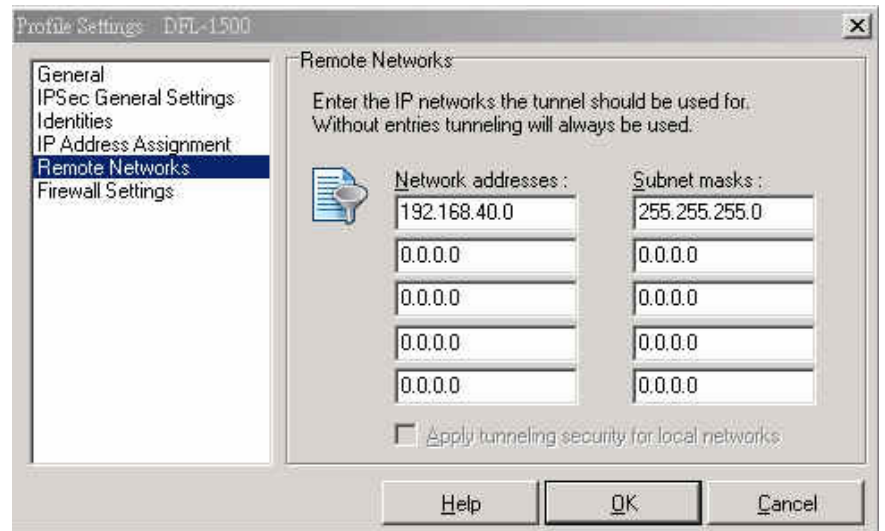
Configuration > Profile Settings > Configure > IP Address Assignment



Step 13. Setup Remote Networks

Enter the IP network address 192.168.40.0 and subnet masks 255.255.255.0, and then click OK to finish the settings.

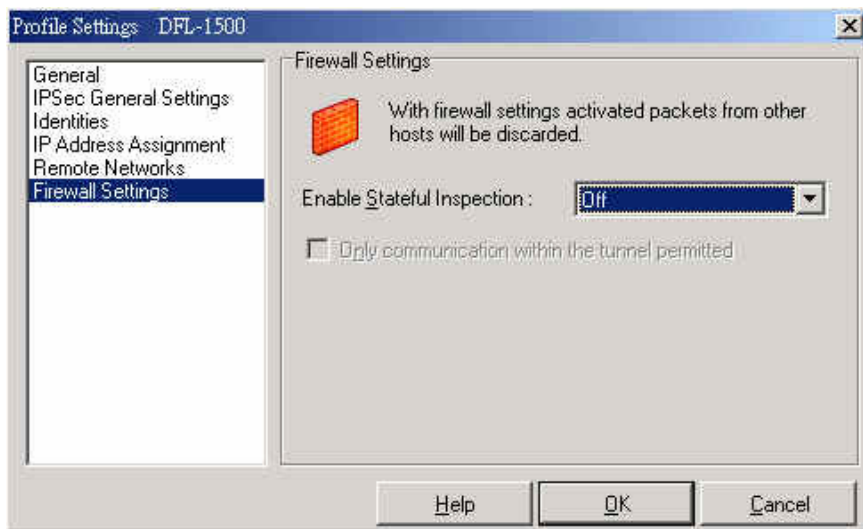
Configuration > Profile Settings > Configure > Remote Networks



Step 14. Firewall Settings

In order to avoid any conflict, we recommend you to disable the Stateful Inspection.

'Configuration > Profile Settings > Configure > Firewall Settings



Step 15. Connect the IPSec VPN

Click Connect to establish the IPSec VPN tunnel with Organization_1 LAN_1. If connection is established, you can view it like right diagram.

Connection > Connect



Chapter 20

Remote Access VPN – Windows client

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

20.1 Demands

Suppose an employee often works at home, he will have the requirement to access the resource inside the company. The topology is illustrated in the Figure 20-1.

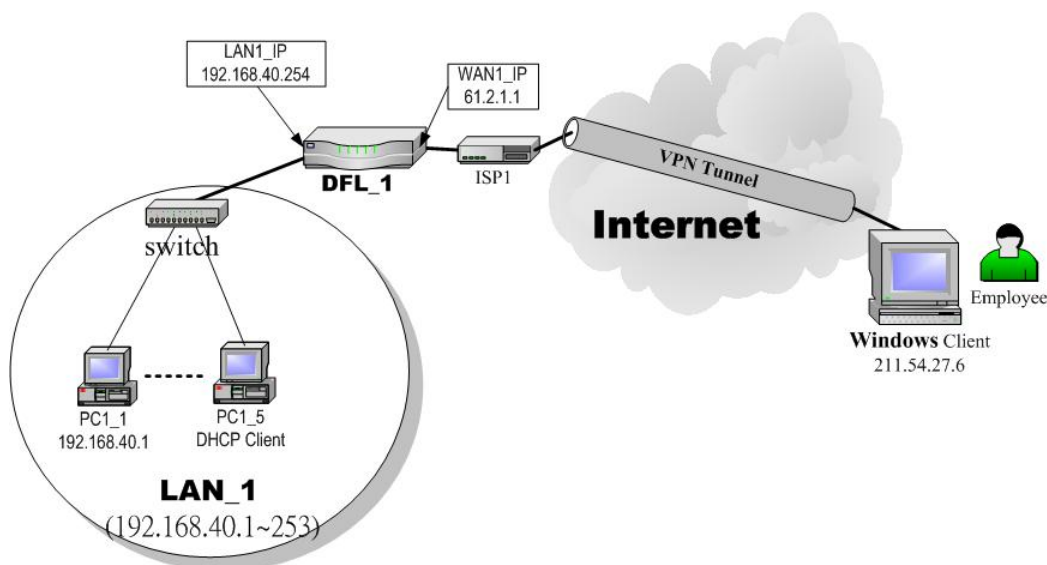


Figure 20-1 Using Windows client to connect DFL-1500 IPSec Server

20.2 Objects

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

20.3 Methods

As the Figure 20-1 illustrated, we need to setup the IPSec feature of the DFL-1500 at company first. On the other hand, we have to setup the related IPSec setting in the Windows client at employee's side so that the employee can establish the IPSec tunnel through windows client to access the resource of the company.

For the procedure to setup the DFL-1500, please refer 20.4.1 description.

In the following steps, we would propose the example using windows XP to introduce the setup process.

And the setup procedures will be divided into several parts.

1. Create a custom MMC console, please refer 20.4.2 description.
2. Create an IPSec policy, please refer 20.4.3 description.
3. Add a filter rule from WinXP to DFL-1500, please refer 20.4.4 description.

4. Add a filter rule from DFL-1500 to WinXP, please refer 20.4.5 description.
5. Configure a rule for WinXP client to DFL-1500, please refer 20.4.6 description.
6. Configure a rule for DFL-1500 to WinXP client, please refer 20.4.7 description.
7. Enable the security settings, please refer 20.4.8 description.

20.4 Steps

20.4.1 DFL-1500 Setup

Step 1. Add an IPSec rule

At the DFL-1500 side, we need to add an IPSec policy to establish IPSec tunnel with WinXP client. Enter the related IPSec parameter in the suitable field. For the field description, please refer Table 13-4 for the details. Note that because the remote client is just a single WinXP machine, so we select Single Address in the Remote Address Type field.

ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add

The screenshot shows the configuration page for adding an IKE rule. The breadcrumb path is 'ADVANCED SETTINGS > VPN Settings > IPSec > IKE > Add'. The page has several tabs: 'IPSec', 'VPN Hub', 'VPN Spoke', 'PPTP', 'L2TP', and 'Pass Through'. The current page is titled 'IPSec->IKE->Edit Rule'. The configuration is divided into three sections: Status, Condition, and Action.

- Status:** A checkbox for 'Active' is checked.
- Condition:**
 - Local Address Type:** Subnet Address
 - IP Address:** 192.168.40.0
 - PrefixLen / Subnet Mask:** 255.255.255.0
 - Remote Address Type:** Single Address (highlighted with a red box)
 - IP Address:** 211.54.27.6
 - PrefixLen / Subnet Mask:** 255.255.255.255
- Action:**
 - Negotiation Mode:** Main
 - Encapsulation Mode:** Tunnel
 - Outgoing Interface:** WAN1
 - Peer's IP Address:** Static IP, 211.54.27.6
 - My Identifier:** IP Address, Auto_Assigned
 - Peer's Identifier:** IP Address, Auto_Assigned

Below the Action section, there are radio buttons for 'ESP Algorithm' (selected) and 'AH Algorithm'. The ESP Algorithm is set to 'Encrypt and Authenticate (DES, MD5)'. The AH Algorithm is set to 'Authenticate (MD5)'. A 'Pre-Shared Key' field contains the value '1234567890'. At the bottom, there are 'Advanced', 'Back', and 'Apply' buttons.

Step 2. Edit the detailed settings of IPSec rule

Fill the detailed settings as the diagram of right side. And then click **Apply** to finish the IPSec rule edition. For the field description, please refer Table 13-5 for more information.

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

Step 3. Warning message

Here appears a warning message to remind you to add a firewall rule which can allow IPSec traffic into the DFL-1500, because the WAN-to-LAN traffic of the DFL-1500 by default is blocked. For the detailed procedure to add a firewall rule, please refer Section 13.4.

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

Step 4. Finish adding an IPSec rule

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

ADVANCED SETTINGS > VPN Settings > IPSec > IKE

| Item # | Active | Name | Local LAN | Remote LAN | Mechanism | My IP | Peer's IP |
|--------|--------|--------------|-----------------|----------------|--------------------------|----------------|-------------|
| 1 | Y | WindowClient | 192.168.40.0/24 | 211.54.27.6/32 | Tunnel - ESP (DES MD5) | 192.168.17.174 | 211.54.27.6 |

Step 5. Add Firewall rule settings

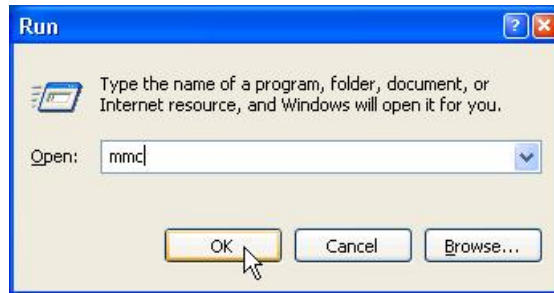
Additionally, because the traffic of WAN to LAN default is blocked. So we must add a firewall rule to allow the local area of remote side to pass through the DFL firewall. Please refer the section 13.4.1 for the full description and examples.

N/A

20.4.2 Create a custom MMC console

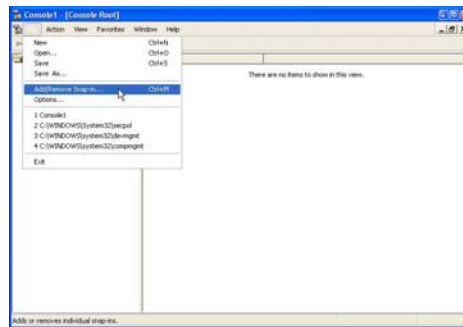
Step 1. Run mmc

From Windows desktop, go to Start > Run, and in the Open textbox type mmc, click OK.



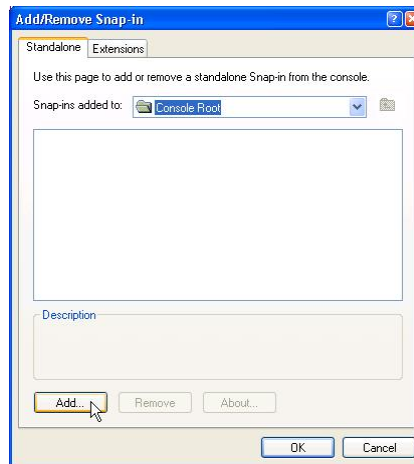
Step 2. Add Snap-in

On the Console window, click Add/Remove Snap-In.



Step 3. Add a Standalone Snap-in

In the Add/Remove Snap-In dialog box, click Add.

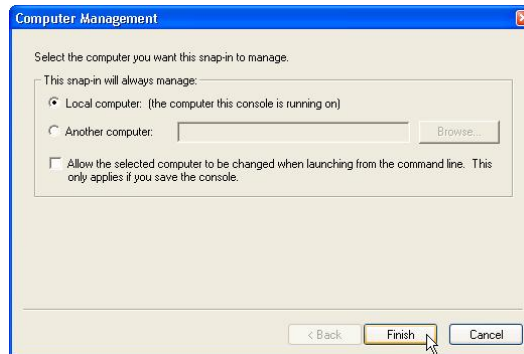


Step 4. Add “Computer Management” snap-in

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

**Step 5. Verify the Local Computer is selected**

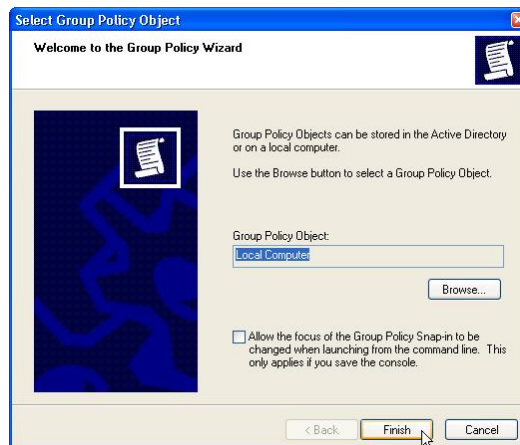
Verify that Local Computer (default setting) is selected, and click Finish.

**Step 6. Add “Group Policy” snap-in**

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

**Step 7. Verify the Local Computer is selected**

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



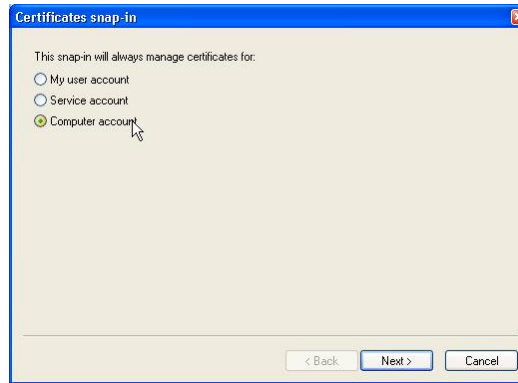
Step 8. Add “Certificates” snap-in

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



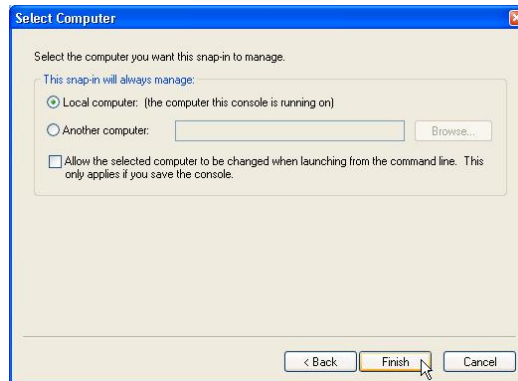
Step 9. Select Computer account

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



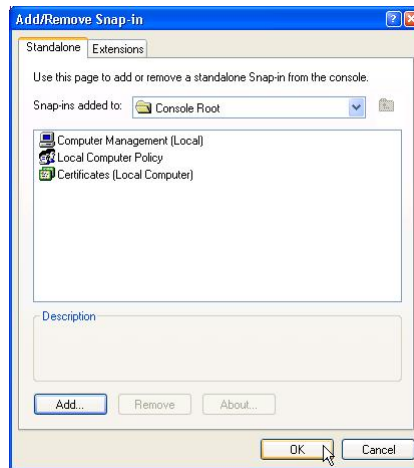
Step 10. Verify the Local Computer is selected

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



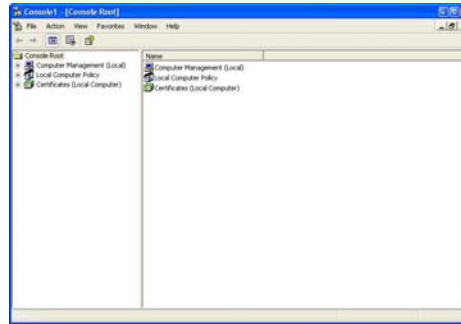
Step 11. Close the Add/Remove Snap-in windows

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

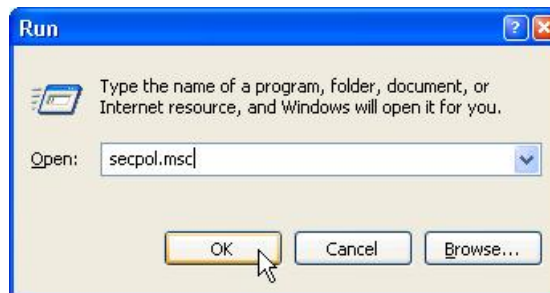


Step 12. Finish the mmc console creation

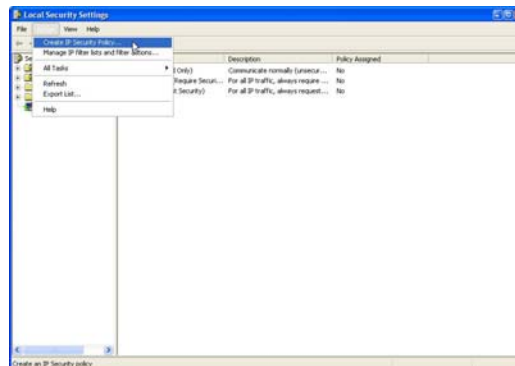
After finishing the previous steps, we have selected three snap-in components in the mmc console.

**20.4.3 Create an IPSec policy****Step 1. Run secpol.msc**

From Windows desktop, go to Start > Run, and in the Open textbox, type `secpol.msc`. And then click OK.

**Step 2. Create IP Security policy**

Select Action > Create IP Security policy to add security policy.

**Step 3. Enter policy name**

Click Next, and type a name for your policy. For example, winXP to DFL-1500 tunnel.



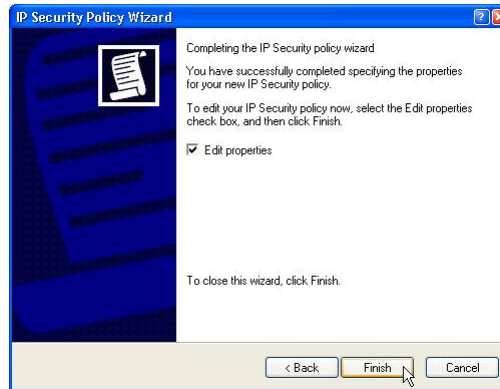
Step 4. Uncheck the item

Uncheck Active the default response rule checkbox, and click Next



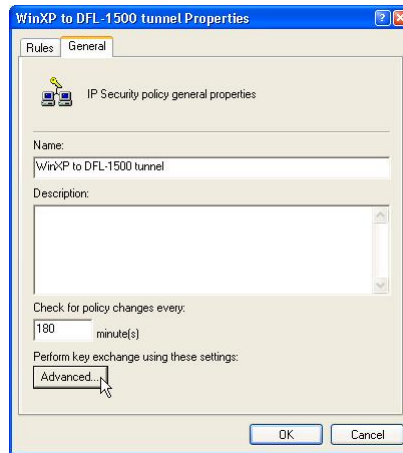
Step 5. Finish the IP Security policy creation

Keep the Edit properties check box selected and click Finish.



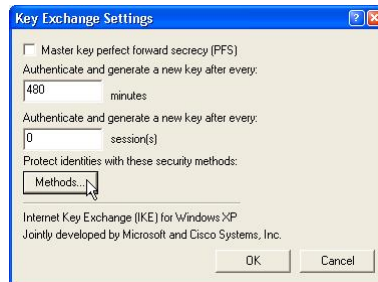
Step 6. Edit policy properties

A dialog window will bring up for you to configure two filter rules for this policy. Click General tab and click Advanced button to setup IPsec phase1 parameters.



Step 7. Key Exchange Settings

Click Methods to proceed.



Step 8. Delete the extra items

In this diagram, we are going to specify the phase1 parameter of IPSec rule at the WinXP. We setup DFL-1500 IPSec phase1 with DES-MD5-DH1 (please refer Section 20.4.1), therefore we delete the extra 3 items, and only remain the item that matches our IPSec settings of the DFL-1500.



Step 9. Remain the corresponding item

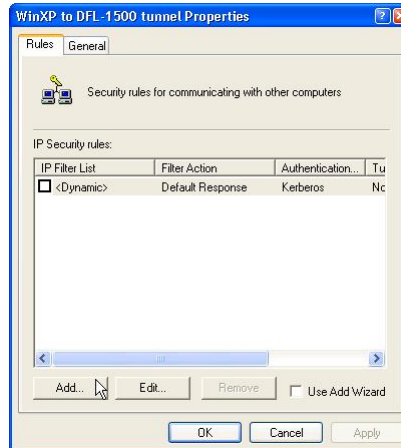
For this example, we remain the item of DES, MD5 and DH1 combinations.



20.4.4 Add a filter rule from WinXP to DFL-1500

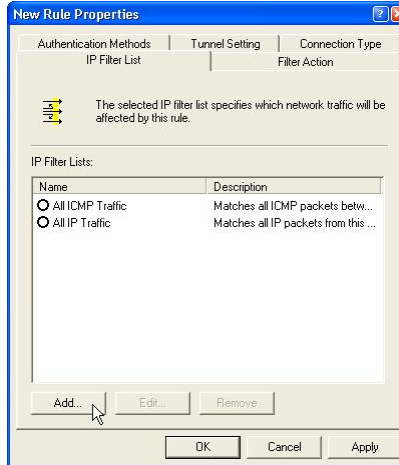
Step 1. Add a new filter rule

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



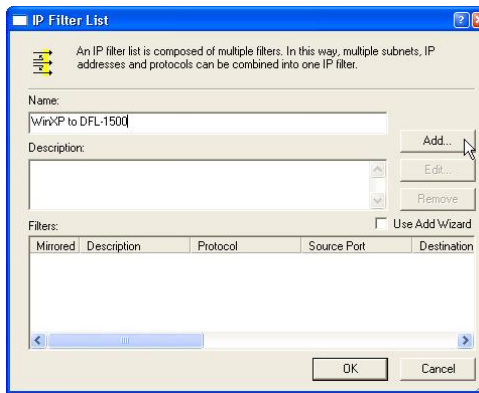
Step 2. Add an IP Filter List

On the IP Filter List tab, click Add to add an IP Filter List.



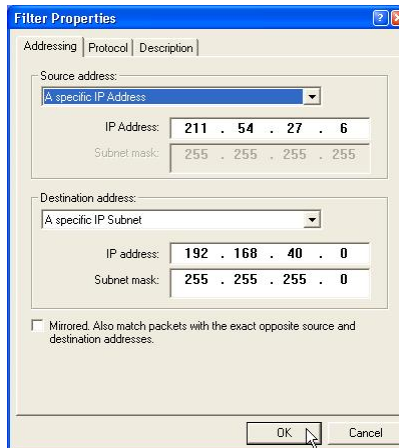
Step 3. Edit IP filter list

Type a name for the filter list (e.g., WinXP to DFL-1500), uncheck Use Add Wizard check box, and click Add.



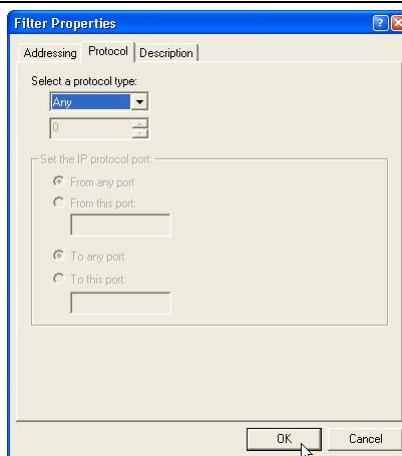
Step 4. Edit the address of filter properties

In the Source address, choose A specific IP Address, and enter the IP address of WinXP (ex. 211.54.27.6). In the Destination address, choose A specific IP Subnet, and enter the IP address and Subnet mask of the local subnet (ex. 192.168.40.0/255.255.255.0). Uncheck Mirrored check box. Click OK to next.

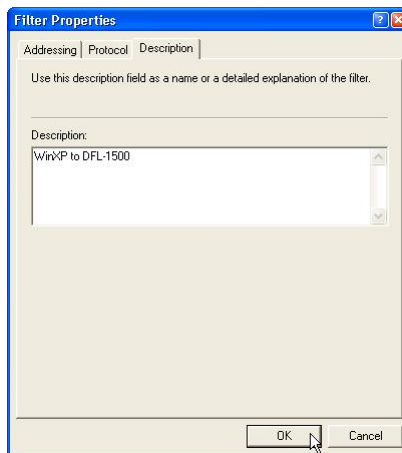


Step 5. Edit the protocol of filter properties

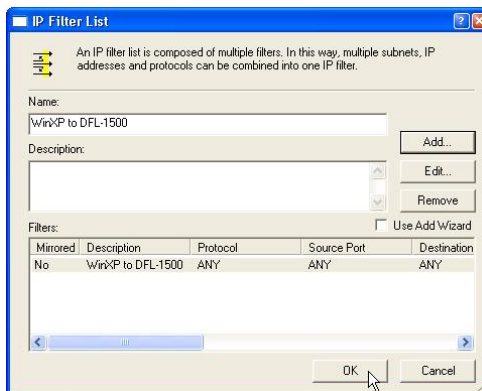
Click the **Protocol** tab. Leave the protocol type to Any.

**Step 6. Edit the description of filter properties**

Click the **Description** tab. You can give a name for this filter list. The filter name is displayed in the IPsec monitor when the tunnel is active.

**Step 7. Finish the creation of IP filter list**

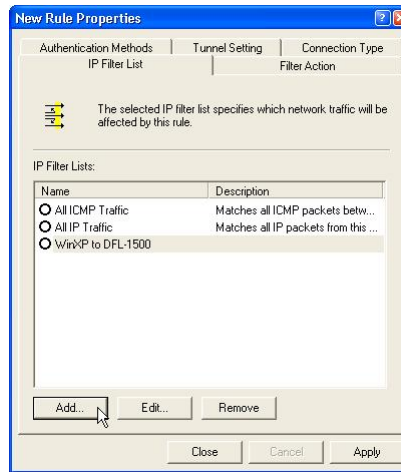
Click **OK** and **Close** these windows.



20.4.5 Add a filter rule from DFL-1500 to WinXP

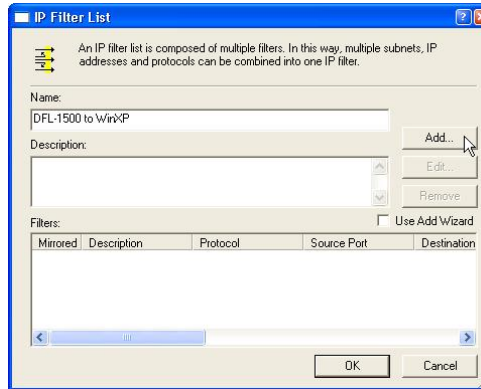
Step 1. Add a new filter rule

Click the IP Filter List tab, and then click Add to add an IP Filter List.



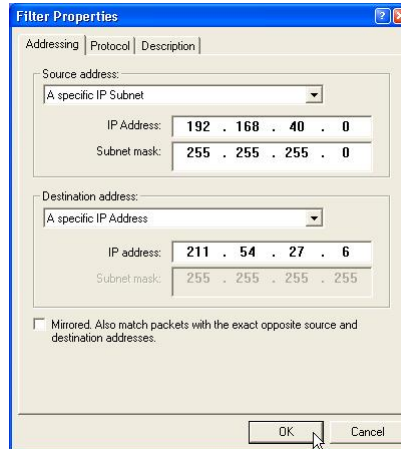
Step 2. Edit IP filter list

Type a name for the filter list (e.g., DFL-1500 to WinXP), uncheck Use Add Wizard check box, and click Add.



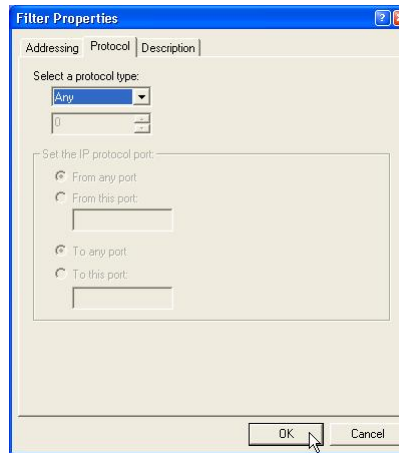
Step 3. Edit the address of filter properties

In the Source address, choose A specific IP Subnet, and enter the IP address and Subnet mask of the local subnet (ex. 192.168.40.0/255.255.255.0). In the Destination address, choose A specific IP Address, and enter the IP address of WinXP (ex. 211.54.27.6). Uncheck Mirror check box. Click OK to next.

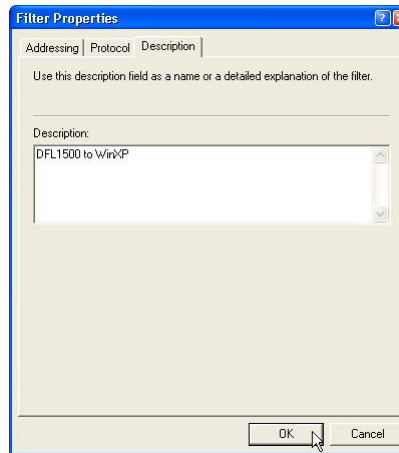


Step 4. Edit the protocol of filter properties

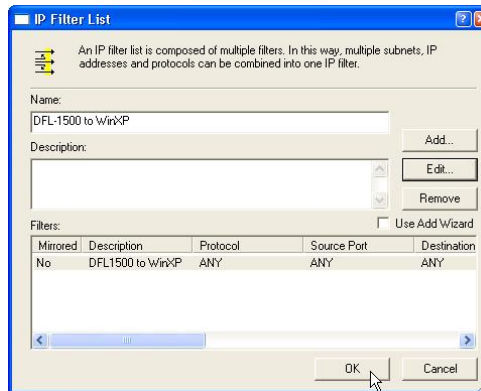
Click the **Protocol** tab. Leave the protocol type to Any.

**Step 5. Edit the description of filter properties**

Click the **Description** tab. You can give a name for this filter list. The filter name is displayed in the IPsec monitor when the tunnel is active.

**Step 6. Finish the creation of IP filter list**

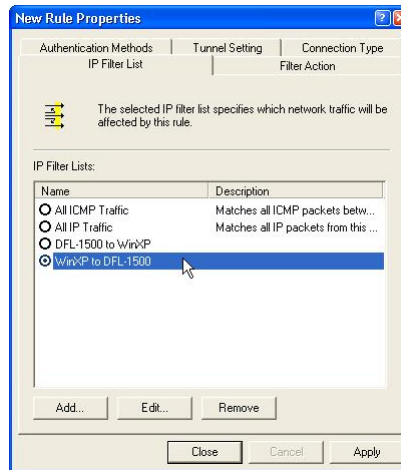
Click **OK** to close the window.



20.4.6 Configure a rule for WinXP client to DFL-1500

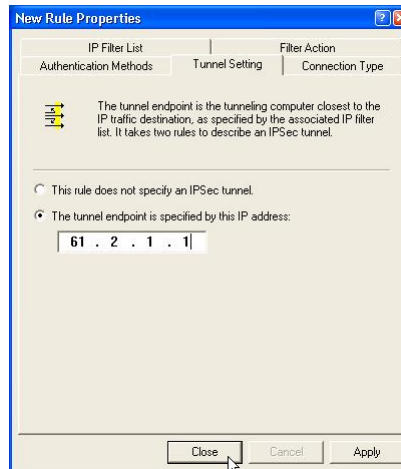
Step 1. Select the first IP filter list

Now there are two IP filter lists for the WinXP IPsec use. Select the first filter list you have created above from the IP Filter List, such as WinXP to DFL-1500.



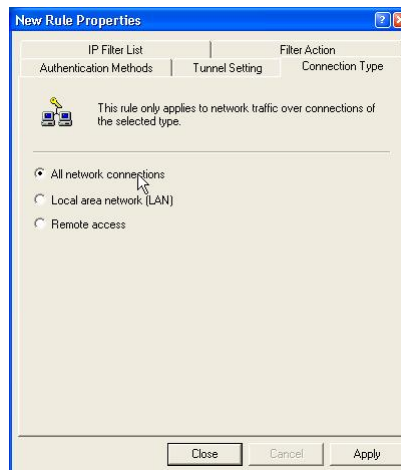
Step 2. Tunnel Settings

Click Tunnel Setting tab, enter the remote endpoint. For this filter list, the remote IPsec endpoint is DFL-1500 (61.2.1.1).



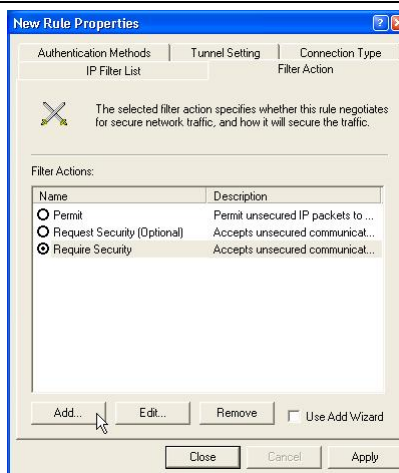
Step 3. Connection Type

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



Step 4. Edit filter action of WinXP to DFL-1500 IP filter list

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



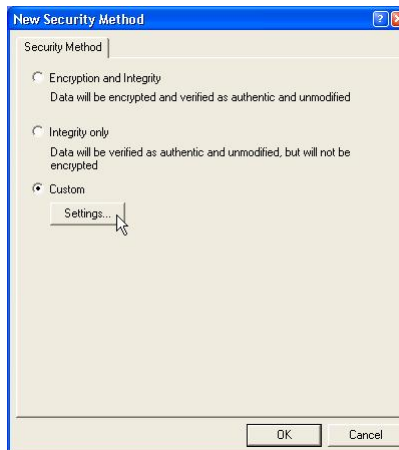
Step 5. Set the properties of Security Methods

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



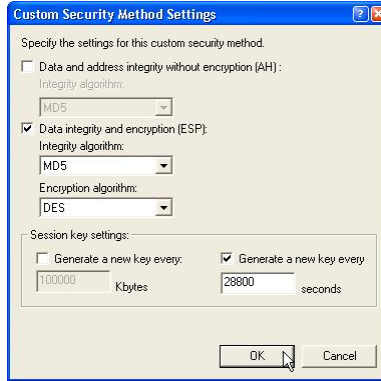
Step 6. Setting the Security Method

Select **Custom** (for expert users) if you want to define specific algorithms and session key lifetimes). Please make sure the settings match whatever we had configured in DFL-1500 before



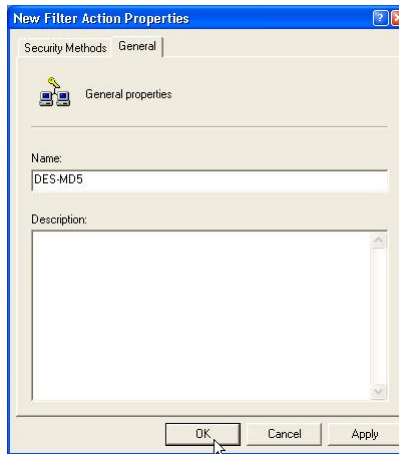
Step 7. Custom security method settings

Select the Data integrity encryption (ESP). Select MD5 integrity algorithms and DES encryption algorithm. Fill the new key generation rate (ex. 28800 sec). Note that the settings of this page must match the settings of IPSec phase2 at DFL-1500.



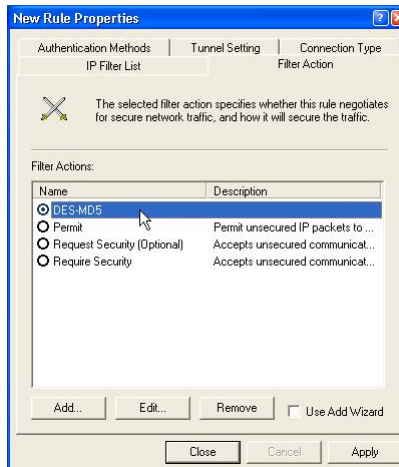
Step 8. New Filter Action Properties

Click the General tab. Give a name to the filter action. For example, DES-MD5, and click OK.



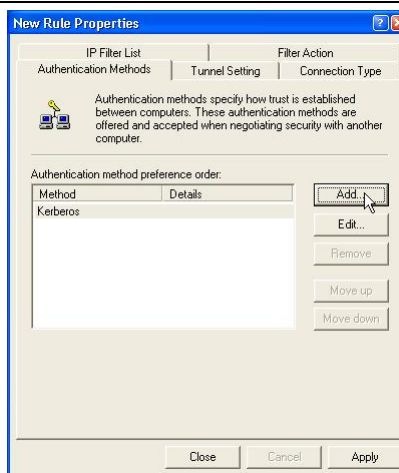
Step 9. Filter Action

Select the filter action (DES-MD5) you just created.

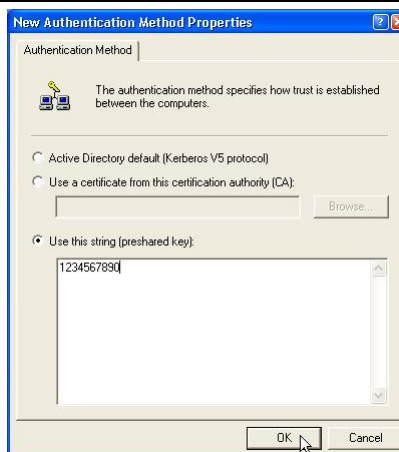


Step 10. Authentication Methods

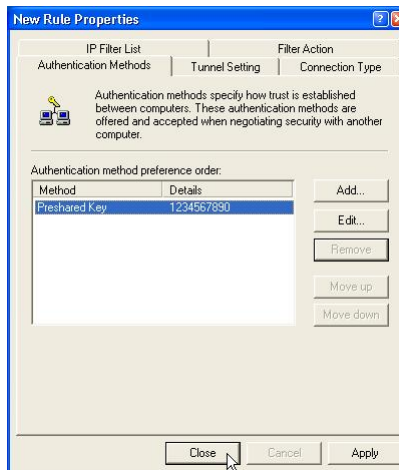
Click the Authentication Methods tab, and then click Add.

**Step 11. Select the authentication methods**

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

**Step 12. Delete Kerberos method**

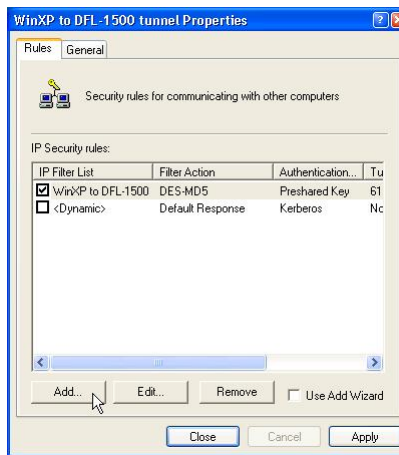
Delete the original Kerberos method. Just select the Preshared Key we defined before. Click Close to finish the WinXP to DFL-1500 Rule settings.



20.4.7 Configure a rule for DFL-1500 to WinXP client

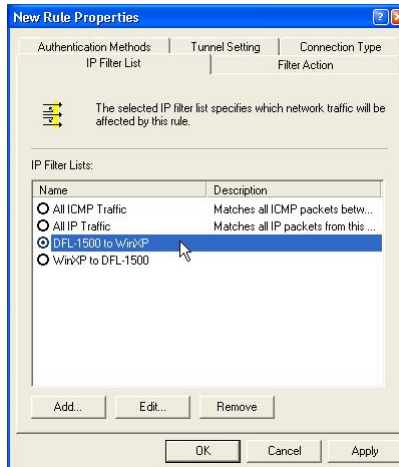
Step 1. Add a new IP filter rule

Now we are going to configure the rule of DFL-1500 to WinXP client. Click Add to add a new IP filter rule.



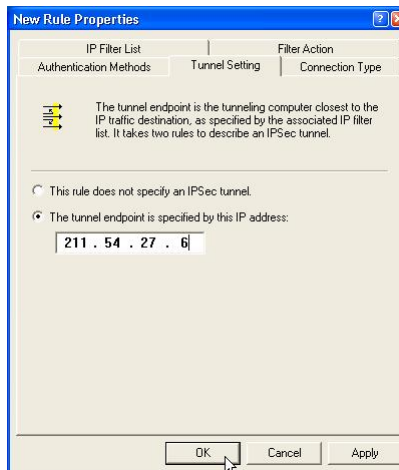
Step 2. Select IP filter list

Click the IP Filter List tab. Select the filter list you created above from the IP Filter List (DFL-1500 to WinXP).



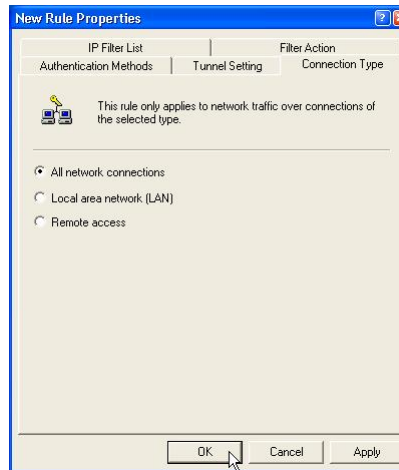
Step 3. Tunnel Settings

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

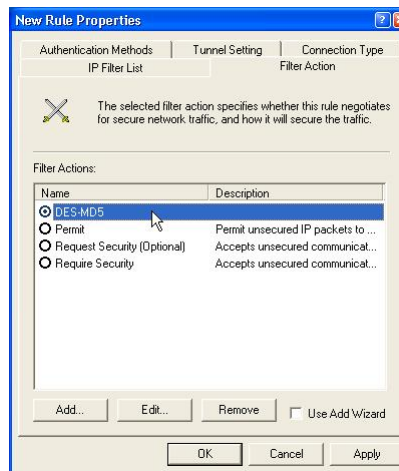


Step 4. Connection Type

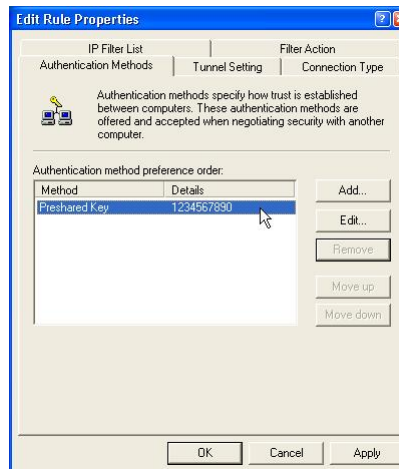
Click **Connection Type** tab, and then click **All network connections**.

**Step 5. Filter Action**

Click **Filter Action** tab, and then select the filter action (**DES-MD5**) you just created.

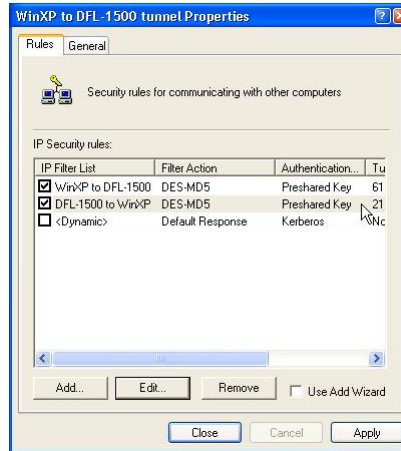
**Step 6. Authentication Methods**

Click **Authentication Methods** tab, select the **Preshared Key** we defined before. Click **OK** to finish the rule creation.



Step 7. Finish the rules edition

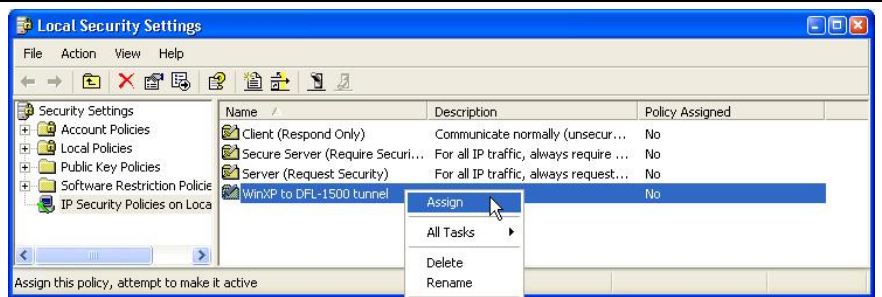
The IP Security rule of DFL-1500 to WinXP is configured completely as the figure listing. Click Close to finish the settings.



20.4.8 Enable the security settings

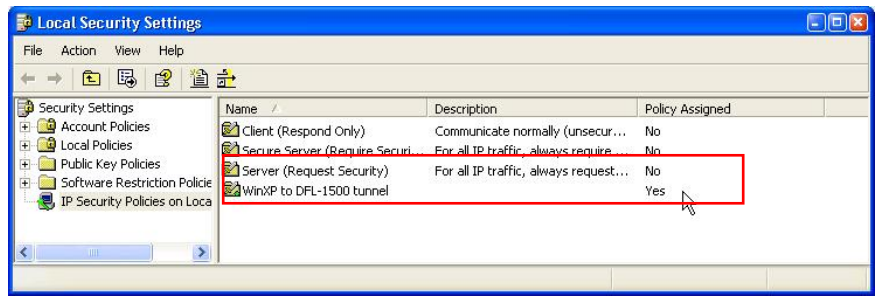
Step 1. Assign the security policy

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



Step 2. Finish all the settings of WinXP

After the above configurations, now you can use WinXP to connect back to the local company behind the DFL-1500 device.



Part VI

Content Filters

Chapter 21

Content Filtering – Web Filters

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

21.1 Demands

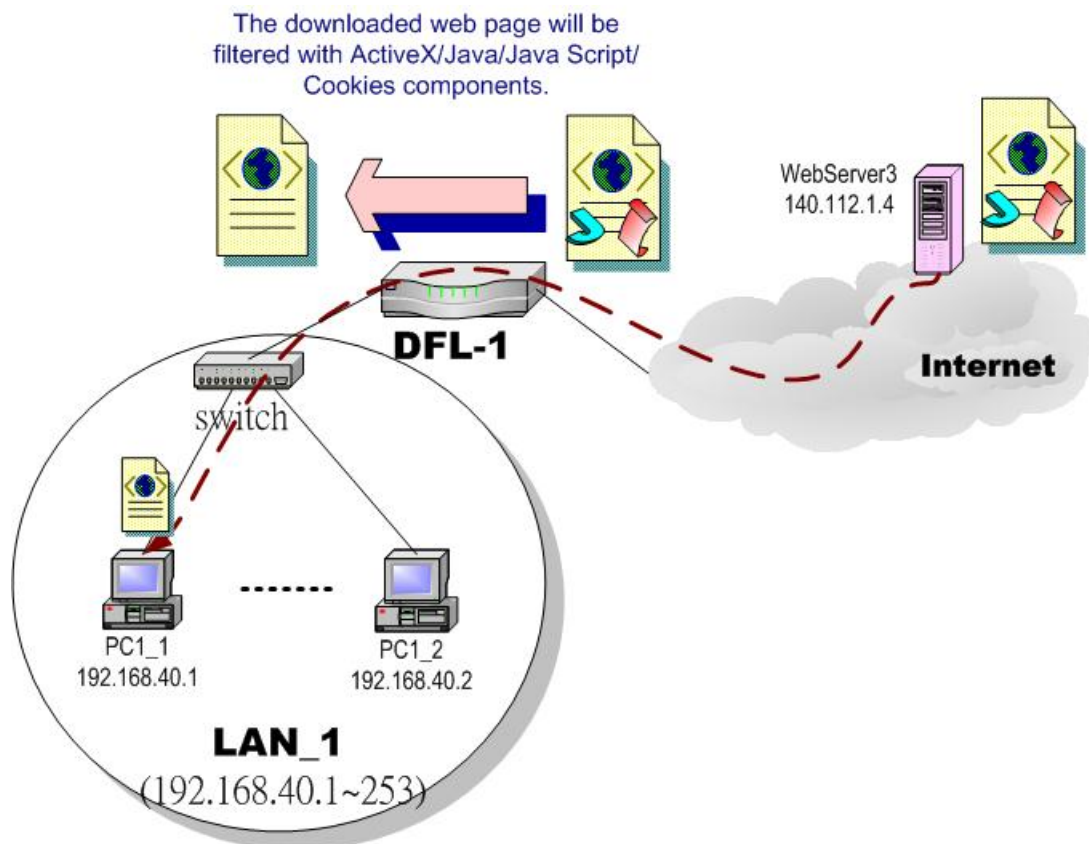


Figure 21-1 Use web filter functionality to avoid users browsing the forbidden web site

1. As the above Figure 21-1 illustrates, someone (PC1_1) is browsing the web pages at the WebServer3. The contents of the web pages may include cookies, Java applets, Java scripts or ActiveX objects that may contain malicious program of users' information. So, we wish to prohibit the user (PC1_1) from downloading the forbidden components.

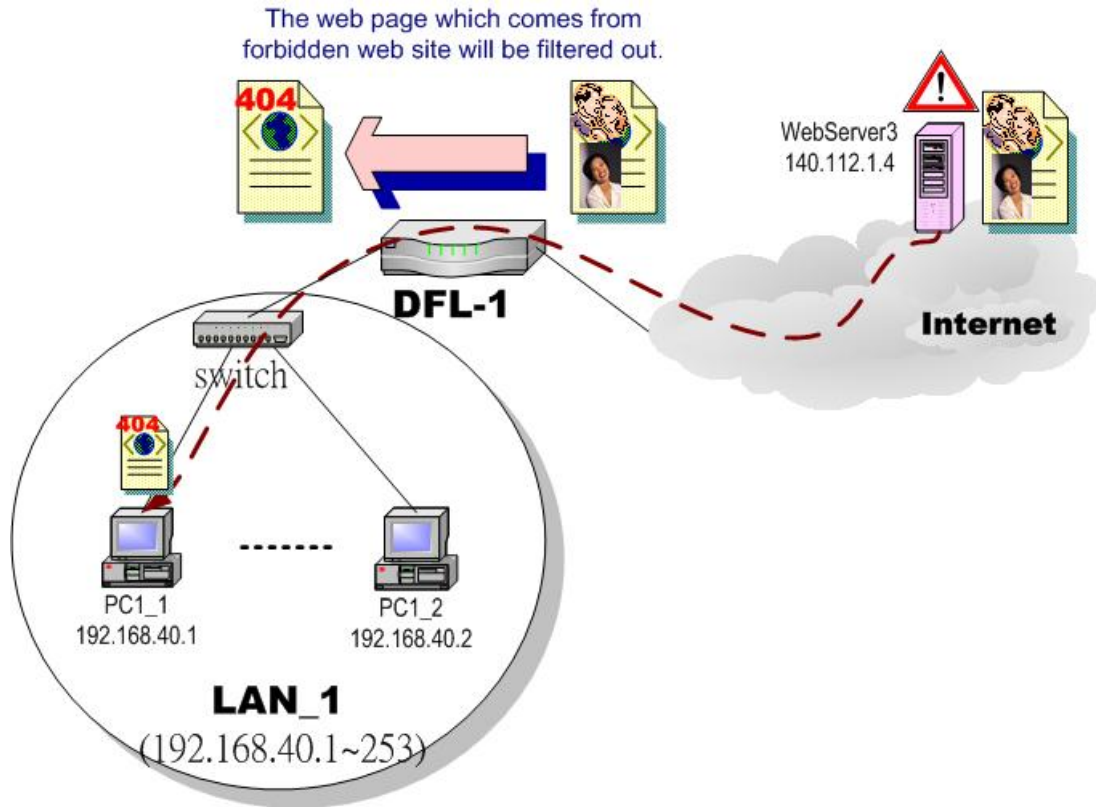


Figure 21-2 Use web filter functionality to avoid users view the forbidden web site

2. As the above Figure 21-2 illustrates, someone (PC1_1) is browsing forbidden web pages on office hours. The contents of the web pages may include stock markets, violence, or sex that will waste the bandwidth of the Internet access link while degrading the efficiency of normal working hours. So, we wish to prohibit the user (PC1_1) from viewing the page on the forbidden web site.

21.2 Objectives

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

21.3 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.

The feature of the Web Filter can only be available while DFL-1500 connects to the Internet via Default WAN Link.

21.4 Steps

Step 1. Enable Web Filter

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

ADVANCED SETTINGS > Content Filters > Web Filter > Web

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|----------------------------|--|----------------|----------|
| Enable Web Filter | Enable Web Filter feature of DFL-1500 | Enable/Disable | Enabled |
| Enable Web Proxy Filtering | If enabling this feature, all the web pages pass through proxy (Only port 3128) will also be verified by DFL-1500. If disabling the “Web Proxy”, all the web pages through will bypass the verification. | Enable/Disable | Disabled |

Table 21-1 Enable Web Filter



✓ Warning message

While enabling the web filter feature, it will show the warning message saying that if you block any web traffic from LAN-to-WAN in Firewall, the access control is shifted 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>Step 2. 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> |
|---|---|

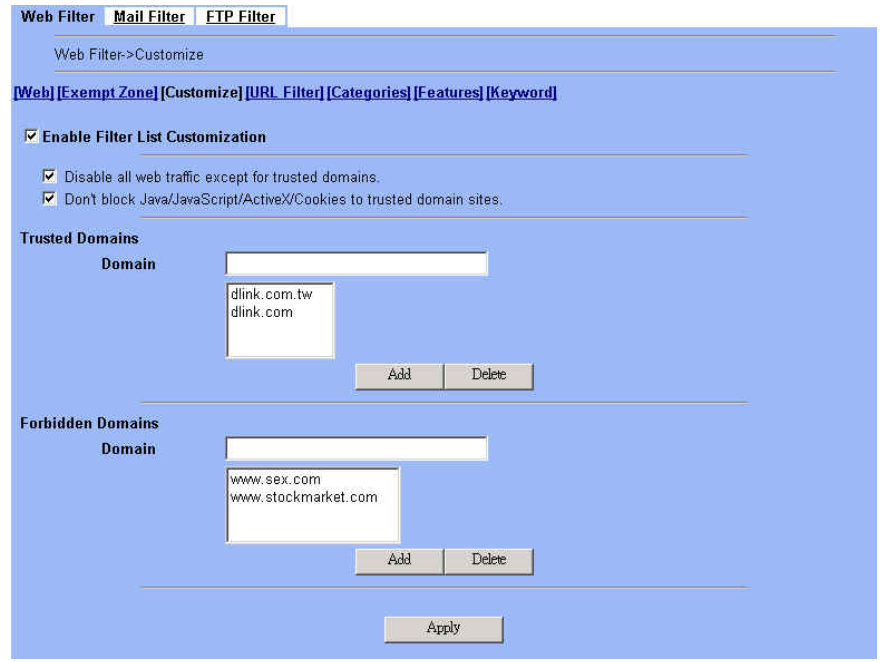
| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--|---|-------------------------|--|
| Exempt Computers | Determine which IP range will exempt the verification by the web filter | | |
| Enforce web filter policies for all computers | Web filter is activated at all the computers, not limit range of the IP addresses | Enable/Disable | disabled |
| Include specified address ranges in the web filter enforcement | Web filter will only be activated at below specified computers. | Enable/Disable | Enabled |
| Exclude specified address ranges from the web filter enforcement | Except below specified IP address ranges. All the other IP address range, web filter will active totally. | Enable/Disable | disabled |
| Range From ____ To ____ | Here we can setup the IP address range, for the above Exempt Computers to use. | IPv4 format IPv4 format | 10.1.1.1 – 10.1.1.254 192.168.40.100 – 192.168.40.130 |
| BUTTON | DESCRIPTION | | |
| Apply | Apply the above selected “Exempt Computers” radius button. | | |
| Add | Add the specified IP range which filled in the above “Range From” field. | | |
| Delete | Delete the specified IP range which filled in the above “Range From” field. | | |

Table 21-2 Web Filter Exempt Zone setting page

Step 3. Customize the specified sites

Check the Enable Filter List Customization to allow all accesses to the Trusted Domains while disallowing all accesses to the Forbidden Domains. Check the Disable all web traffic except for trusted domains if you want to only allow the access to the Trusted Domains. However, if the web objects are set to be blocked by the DFL-1500 in step 3, these allowed accesses will never be able to retrieve these objects. Check the “Don’t block ...” to allow the objects for these trusted domains. The domains are maintained by enter the address in the Domain field with a click of the Add button. To delete a domain, click the domain with a click of the Delete button.

ADVANCED SETTINGS > Content Filters > Web Filter > Customize

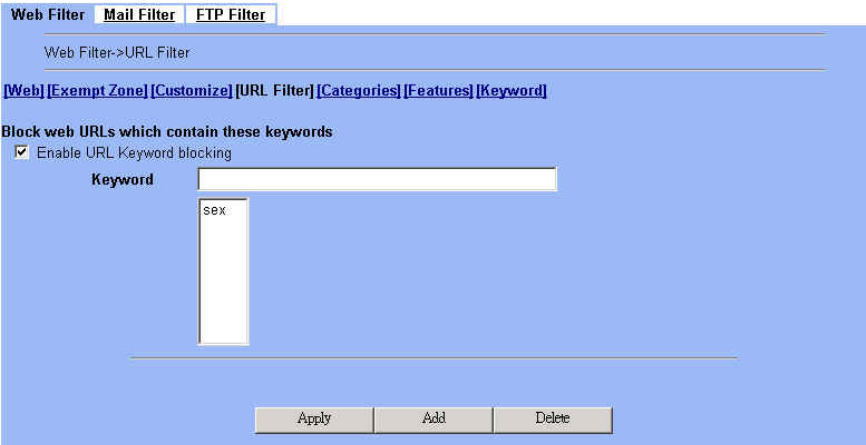


| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|---|---|--------------------------------------|------------------------------------|
| Enable Filter List Customization | Enable the Filter List Customization feature of web filter. If you only enable it, all the domains in the Trusted Domains will be allowed to pass through DFL-1500. Contrarily, all the domains in the Forbidden Domain will be blocked by the DFL-1500. | Enable/Disable | Enabled |
| Disable all web traffic except for trusted domains | All the other URL domain IP addresses are blocked except the following specified domain range specified by the trusted domain. | Enable/Disable | Enabled |
| Don't block Java/JavaScript/ActiveX/Cookies to trusted domain sites | In the following domain range of the trusted domains. If there are include Java/ JavaScript/ActiveX/Cookies components in the web page, the action is setting not to block. | Enable/Disable | Enabled |
| Trusted Domains Domain | You can enter either domain name or IP address for the trusted domains. Note: if the domain name can not be distinguished by the DNS server, the domain name entry will be ignored. Another issue is that if there are a lot of domain names in customized area, name resolving will take longer time on Web Filter starting up. | IPv4 format / resolvable domain name | www.dlink.com.tw www.dlink.com |
| Forbidden Domains Domain | You can enter either domain name or IP address for the forbidden domains. Note: if the domain name can not be distinguished by the DNS server, the domain name entry will be ignored. Another issue is that if there are a lot of domain names in customized area, name resolving will take longer time on Web Filter starting up. | IPv4 format / resolvable domain name | www.sex.com www.stockmarket.com |
| BUTTON | DESCRIPTION | | |

Part VI Content Filters

| | |
|--------|--|
| Add | Add the Trusted/Forbidden Domains IP range to the list. |
| Delete | Delete the Trusted/Forbidden Domains IP range from the list. |
| Apply | Apply the setting which configured on the checkbox. |

Table 21-3 Web Filter Customize setting page

| | |
|--|---|
| <p>Step 4. 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 > URL Filter</p>  |
|--|---|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|-----------------------------|---|----------------|---------|
| Enable URL Keyword blocking | Enable URL keyword blocking feature of web filter | Enable/Disable | Enabled |
| Keyword | If the Keyword appears in the URL when connect to the Internet using browser. The contents about the URL will be block. | text string | sex |
| BUTTON | DESCRIPTION | | |
| Apply | Apply the setting which configured on the checkbox. | | |
| Add | Add the Keyword to the list. | | |
| Delete | Delete the selected keyword from the list. | | |

Table 21-4 Web Filter Domain Name setting page

| | |
|--|--|
| <p>Step 5. Customize Categories</p> <p>With the built-in URL database, DFL-1500 can block web sessions towards several pre-defined Categories of URLs. Check the items that you want to block or log. If you click Block all categories checkbox, it will be applied to 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 | Range / Format | EXAMPLE |
|--|---|----------------|-------------------------|
| Use URL Database | Determine how to deal with the URL types in this page (Log & Block Access, Log Only, Block Only). | Enable/Disable | Log & Block Access |
| Block all categories | Make all categories below enabled. | Enable/Disable | disabled |
| Violence/Profanity, Gross Depictions, Militant/Extremist ,etc. items | Check the categories you would like to enable. | Enable/Disable | Enable the checked ones |
| Time of Day | The time which was set for Web Filter. | Enable/Disable | 9:30 ~ 17:30 |

Table 21-5 Web Filter Categories setting page

| | |
|--|--|
| <p>Step 6. Customize Objects</p> <p>Check the objects of Restricted Features to block the objects. Click the Apply button at the bottom of this page.</p> | <p>ADVANCED SETTINGS > Content Filters > Web Filter > Features</p> |
|--|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|---------------------|---|----------------|----------|
| Restricted Features | Select the below items that will verified by Web Filter feature. | | |
| ActiveX | Filter the web page that includes ActiveX. | Enable/Disable | Enabled |
| Java | Filter the web page that includes Java applet. | Enable/Disable | Enabled |
| Java Script | Filter the web page that includes Java Script. | Enable/Disable | .Enabled |
| Cookies | Filter the web page that includes Cookies. | Enable/Disable | Enabled |
| MSN over HTTP | Filter MSN application which is through http proxy. Note this feature supports MSN under version 6.0 (include) currently. | Enable/Disable | Disabled |

Table 21-6 Web Filter setting page

✓ **Note**

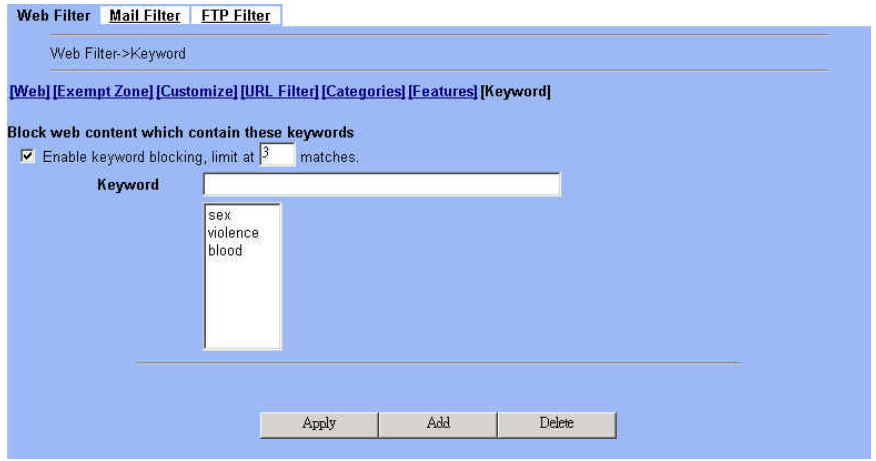
After finishing the above feature settings, you can use PC1_1 to browse the web page to see if the objects are blocked. If the objects are still shown on web pages, they may be cached by the browser. Please clear the cache in the web browser, and then close the browser. Reopen the browser, and reconnect to the web page.

Step 7. Setup contents keyword blocking

Check the **Enable Keyword Blocking** to block any Web pages that contain the entered keywords. Add a key word by entering a word in the **Keyword** field and then click **Add** to proceed.

Note that you can add the keywords as many as you like.

ADVANCED SETTINGS > Content Filters > Web Filter > Keyword



| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--|---|----------------|--------------------------|
| Enable keyword blocking, limit at __ matches | Check Enable keyword blocking checkbox, and then the web pages may be blocked if they contain those added keywords. "Limit at 3 matches" means that the webpages will be blocked as long as any of the added keywords appear equal or more than three times. | Enable/Disable | Enabled 3 matches |
| Keyword | Insert the keyword that you want to block. It is supported only in English currently. | Text string | sex violence blood |
| BUTTON | DESCRIPTION | | |
| Apply | Apply the settings which have been configured. | | |
| Add | Add the Keyword to the list. | | |
| Delete | Delete the Keyword from the list. | | |

Table 21-7 Web Filter Content Keywords setting page

21.5 Priority of web filter functions

The priority of web filter functions are shown as the following Figure 21-3 illustrated. From the left feature (Exempt Zone) to the right feature (Keyword). Their priority is high to low.

Notice: The Restricted features of /Web Filter/Web page is lowest priority, but it is located at the most left side.



Figure 21-3 web filter features priority (from High to Low)

According to the priorities of web filter, we have the guiding principle to setup the web filter now. As we know, there are many choices according to your requirement for the web filter settings. Here we list the setting priorities for your reference. As the following Table 21-8 indicates, the smaller priority sequence would be executed first when running web filter.

| Priority sequence | Selected item | Description | Restricted Region |
|-------------------|---|---|---------------------|
| 1. | Web Filter > Exempt zone | Select which LAN region will apply the web filter settings. There are three options: 1) enforce all computers, 2) include specified computers, and 3) exclude specified computers. | LAN |
| 2. | Web Filter > Customize | Use the Customize domain to indicate the Trusted/Forbidden destination. Two options for your choice. We can specify which URL domain names are trusted, and which ones are forbidden separately. Warning: Customize will not work on the proxy connections. | Internet web server |
| 3. | Web Filter > URL_Filter | When an URL contains any keywords listed in the domain name, it will be blocked. | Internet web server |
| 4. | Web Filter > Categories | We can use Database Update to update the latest URL database and then the Categories will be updated at the same time. The URL which user request will be blocked if it matches the categories in the URL Database. | Internet web server |
| 5. | Web Filter > Features Web Filter > Keyword | If the web page contains the components included activex/java/javascript/cookie which indicated in “Web Filter > Features”, or the keywords indicated in “Web Filter > Keyword”. The forbidden components will be taken off from the web page by web filter. | Web page contents |

Table 21-8 web filter features priority

Chapter 22

Content Filtering – Mail Filters

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

22.1 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.

22.2 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.

22.3 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.

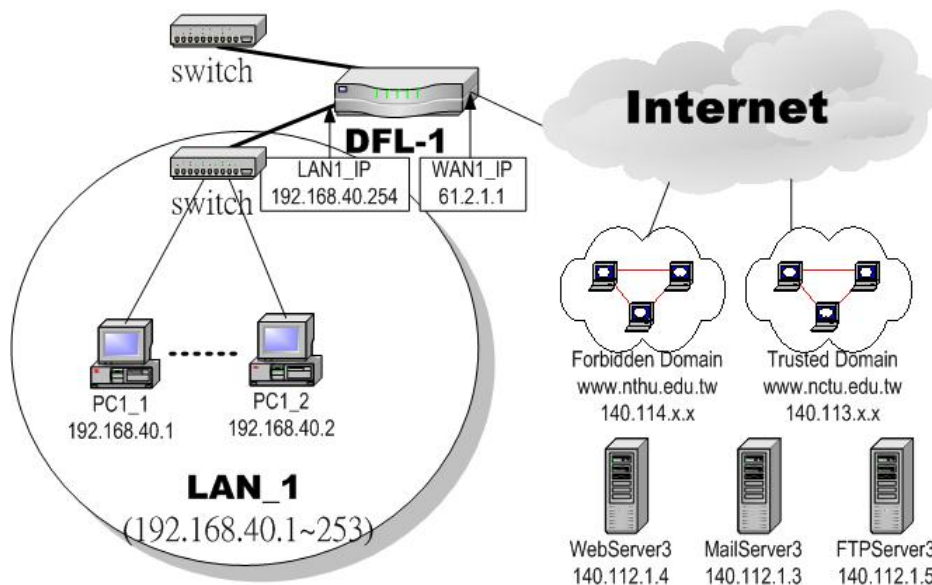


Figure 22-1 Use SMTP / POP3 filter functionality to avoid some sensitive e-mail directly opened

The feature of the Mail Filter can only be available while DFL-1500 connects to the Internet via Default WAN Link.

22.4 Steps

22.4.1 SMTP Filters

Step 1 – Enable SMTP Filters

Check the `Enable SMTP Proxy` checkbox and click `Apply`.

While enabling the SMTP filter feature. All the configured firewall rules (LAN → WAN SMTP) will be disabled immediately. Subsequently the LAN user to access internet mail will take over by the “SMTP filter”.

ADVANCED SETTINGS > Content Filters > Mail Filters > SMTP

The screenshot shows the configuration page for SMTP filters. At the top, there are tabs for 'Web Filter', 'Mail Filter', and 'FTP Filter'. Below the tabs, the 'Enable SMTP Proxy' checkbox is checked and highlighted with a red box, with an 'Apply' button next to it. Below this, there are links for '[SMTP]', '[SMTP Exempt Zone]', '[POP3]', and '[POP3 Exempt Zone]'. A section titled 'Append ".bin" to E-mail attachments whose filename extension' has a dropdown menu set to 'filename extension' and an empty text input field. Below that is a 'Blocking list' table with columns '#', 'Original Name', 'Type', and 'Mapped Name'. The table currently shows 'No mapping defined'. At the bottom, there are 'Add' and 'Delete' buttons.

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|---|--|-------------------------------------|--------------------|
| Enable SMTP Proxy | Enable SMTP Proxy feature of DFL-1500 | text string | 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 / exact filename | Filename extension |

Table 22-1 Enable SMTP feature

Step 2 – Add a SMTP Filter

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

Note that the filename to block cannot contain the marks such as “/ , \ , * , ? , ; , < , > , |”.

ADVANCED SETTINGS > Content Filters > Mail Filters > SMTP

The screenshot shows the same configuration page as in Step 1, but now a rule has been added to the 'Blocking list' table. The rule is highlighted with a red box and has the following details: # 1, Original Name vbs, Type EXT, and Mapped Name vbs.bin. The 'Enable SMTP Proxy' checkbox remains checked.

| | |
|---|--|
| <p>Step 3 – 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 SMTP 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 > Mail Filters > SMTP Exempt Zone</p> |
|---|--|

22.4.2 POP3 Filters

| | |
|---|--|
| <p>Step 1 – Enable POP3 Filters</p> <p>Check the Enable POP3 Proxy checkbox and click Apply.</p> <p>While enabling the POP3 filter feature. All the configured firewall rules (LAN → WAN POP3) will be disabled immediately. Subsequently the LAN user access internet mail will take over by the “POP3 filter”.</p> | <p>ADVANCED SETTINGS > Content Filters > Mail Filters > POP3</p> |
|---|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|---|--|-------------------------------------|--------------------|
| Enable POP3 Proxy | Enable POP3 Proxy feature of DFL-1500 | text string | 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 / exact filename | Filename extension |

Table 22-2 Enable POP3 feature

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.

Note that the filename to block cannot contain the marks such as “/, \, *, ?, “, <, >, |”.

ADVANCED SETTINGS > Content Filters > Mail Filters > POP3

Web Filter Mail Filter FTP Filter

Enable POP3 Proxy

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

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

Blocking list

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

Step 3 – Customize the local zones

You can configure to what range the filters will apply to the local zones. By default, the web filters apply to all computers so the “Enforce POP3 filter policies for all computers” is selected, and the range is 0.0.0.0 – 255.255.255.255. Delete the default range by clicking the range item and the Delete button. Enter the IP range in the Range fields followed by a click of the Add button to add one address range to the web filter. Click “Include.....” and Apply if you want web filters to only apply to the specified ranges. Click “Exclude.....” and Apply if you want web filters to apply to all computers except those specified ranges.

ADVANCED SETTINGS > Content Filters > Mail Filters > POP3 Exempt Zone

Web Filter Mail Filter FTP Filter

Mail Filter->POP3 Proxy Exempt Zone

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

POP3 Exempt Computers

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

Range From To

192.168.40.100 -- 192.168.40.130
 10.1.1.1 -- 10.1.1.254

Chapter 23

Content Filtering – FTP Filtering

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

23.1 Demands

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

23.2 Objectives

1. Forbid PC1_1 from downloading MP3 files with FTP.

23.3 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.

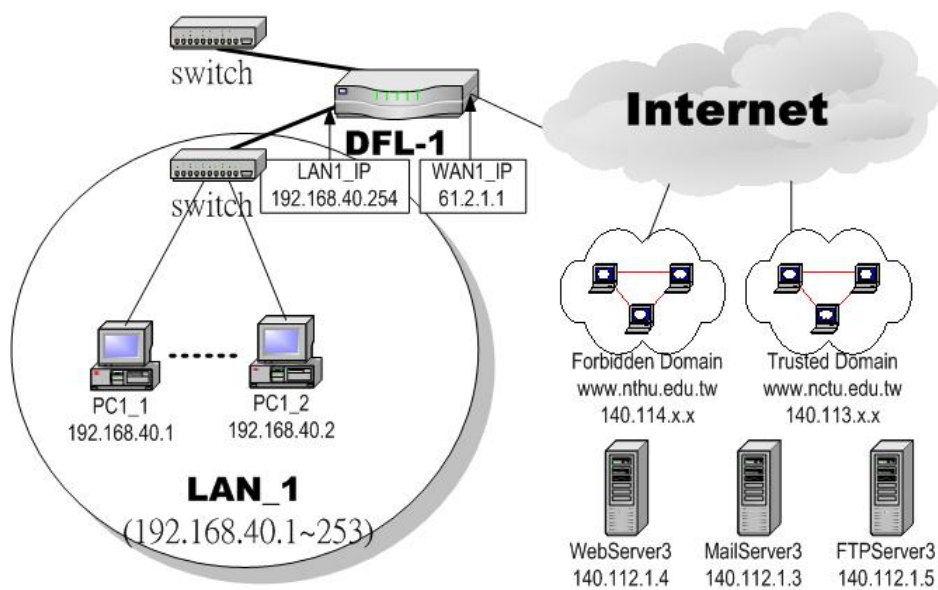


Figure 23-1 Use FTP filter functionality to avoid user download forbidden file type

The feature of the FTP Filter can only be available while DFL-1500 connects to the Internet via Default WAN Link.

23.4 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 | Range / Format | EXAMPLE |
|-------------------|---------------------------------------|----------------|---------|
| Enable FTP Filter | Enable FTP Filter feature of DFL-1500 | Enable/Disable | Enabled |

Table 23-1 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>Note that the filename to block cannot contain the marks such as “/, \, *, ?, “, <, >, ”.</p> | <p>ADVANCED SETTINGS > Content Filters > FTP Filter > FTP > Add</p> |
|---|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------|---|----------------------------|----------------|
| Name | Fill in the file extension or exact filename. | Text string | mp3 |
| Blocked Type | <ul style="list-style-type: none"> ➤ Extension Name When the extension filename of download file is matching the rule, the download action will be blocked by FTP filter. ➤ Full Name When the exact filename of download file is matching the rule, the download action will be blocked by FTP filter. | Extension Name / Full Name | Extension Name |

Table 23-2 FTP Filter FTP adding filter entry

Step 3. View the result

We can see the specified record in this page.
The

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP

Web Filter | Mail Filter | FTP Filter

Enable FTP Filter

[FTP] [FTP Exempt Zone]

| # | Type | Blocked Name |
|-------------------------|-----------|--------------|
| <input type="radio"/> 1 | Extension | mp3 |
| <input type="radio"/> 2 | ... | ... |
| <input type="radio"/> 3 | ... | ... |
| <input type="radio"/> 4 | ... | ... |
| <input type="radio"/> 5 | ... | ... |
| <input type="radio"/> 6 | ... | ... |
| <input type="radio"/> 7 | ... | ... |
| <input type="radio"/> 8 | ... | ... |

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------|--|----------------|---------------|
| From Address | Exempt zone record IP address from. | Ipv4 format | 192.168.40.10 |
| To Address | Exempt zone record IP address to. | Ipv4 format | 192.168.40.30 |
| BUTTON | DESCRIPTION | | |
| Prev. Page | If there is more than one page, you can press Prev. Page to back to the previous page. | | |
| Next Page | If there is more than one page, you can press Next Page to go to the next page. | | |
| Add | Create an address range. | | |
| Delete | Delete the indicated address range. | | |

Table 23-3 FTP Filter add an exempt zone entry

Step 4. Add an Exempt Zone

Add a new Exempt Zone record. It's IP address range is between 192.168.40.10 to 192.168.40.30.

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP Exempt Zone > Add

Web Filter | Mail Filter | FTP Filter

FTP Filter->FTP Exempt Zone

[FTP] [FTP Exempt Zone]

Add Address Range

From Address:

To Address:

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------|------------------------------------|----------------|---------------|
| From Address | Exempt zone record IP address from | Ipv4 format | 192.168.40.10 |
| To Address | Exempt zone record IP address to | Ipv4 format | 192.168.40.30 |

Table 23-4 FTP Filter add an exempt zone entry

Step 5. Show the Exempt Zones

Here we can discover that new added Exempt Zone record is appeared.

ADVANCED SETTINGS > Content Filters > FTP Filter > FTP Exempt Zone

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--|---|----------------|----------|
| FTP Exempt Computers | Determine which IP range will exempt the verification by the FTP filter | | |
| Enforce FTP filter policies for all computers | FTP filter will be applied to all computers, and no exceptions. | Enable/Disable | Disabled |
| Include specified address ranges in the FTP filter enforcement | FTP filter will only be applied to the specified computers. | Enable/Disable | Enabled |
| Exclude specified address ranges from the FTP filter enforcement | FTP filter will be applied to all other IP address ranges, except the specified ones. | Enable/Disable | Disabled |
| BUTTON | DESCRIPTION | | |
| Prev. Page | If there is more than one page, press Prev. Page to back to the previous page. | | |
| Next Page | If there is more than one page, press Next Page to go to the next page. | | |
| Apply | Apply the configured settings. | | |
| Add | Create an exempt zone. | | |
| Delete | Delete the indicated exempt zone. | | |

Table 23-5 Add FTP filter exempt zone

Part VII

Intrusion Detection System

Chapter 24

Intrusion Detection Systems

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

24.1 Demands

Even though we have already configured the firewall rules, it is still not enough. Crackers may 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.

24.2 Objectives

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

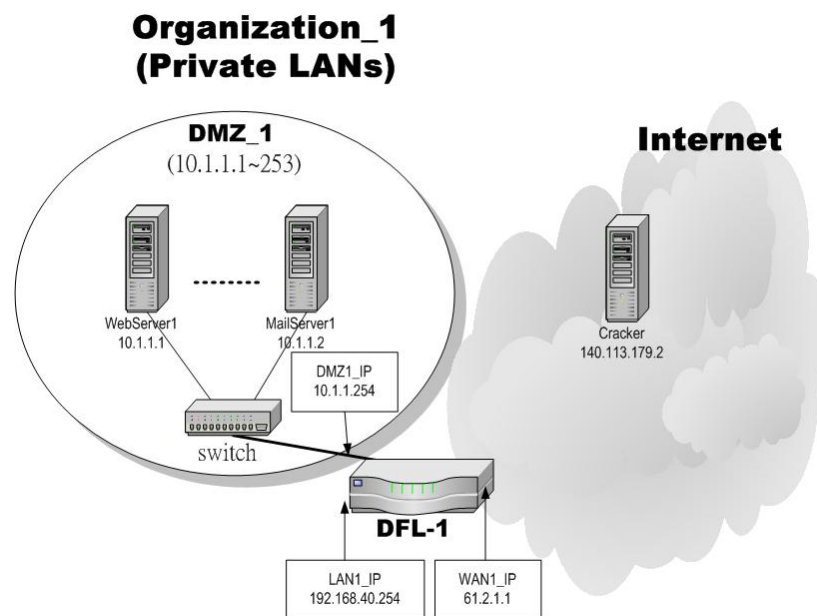


Figure 24-1 Some cracker in the Internet would try to hack our company

24.3 Methods

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

The feature of the IDS can only be available while DFL-1500 connects to the Internet via Default WAN Link.

24.4 Steps

| | |
|--|--|
| <p>Step 1 – Enable IDS</p> <p>Check the <code>Enable IDS</code> checkbox, and click the <code>Apply</code> button.</p> <p>Notice, the IDS can just detect default WAN interfaces currently.</p> | <p>ADVANCED SETTINGS > IDS > IDS Status</p> <p>IDS Status</p> <p><input checked="" type="checkbox"/> <code>Enable IDS</code></p> <hr/> <p>When enabled, the built-in IDS will detect more than 2000 application-level attacks from the default WAN link. The attack signatures can be periodically updated.</p> <p style="text-align: center;"><code>Apply</code></p> |
|--|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|------------|---|----------------|---------|
| Enable IDS | Enable IDS feature of DFL-1500. When enabled, the built-in IDS will detect more than 2000 application-level attacks from the default WAN link. The attack signatures can be periodically updated. | Enable/Disable | Enabled |

Table 24-1 IDS option 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>Syslog Server Mail Logs</p> <p><input checked="" type="checkbox"/> <code>Enable Mail Logs</code></p> <p>Logs will be generated and can be sent via e-mail configuration the mail server and e-mail address(es) here. You can also specify how frequently you want to receive logs.</p> <p>Mail Server: <input type="text" value="10.1.1.1"/></p> <p>Mail Subject: <input type="text" value="IDS"/></p> <p>E-mail Logs To: <input type="text" value="mis@dlink.com"/> (E-mail address)</p> <p>Log Schedule: <input type="text" value="Hourly"/></p> <p>Day for Sending Logs: <input type="text" value="Monday"/></p> <p style="text-align: center;"><code>Apply</code> <code>Test</code></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>IDS Logs</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Time</th> <th>Pri</th> <th>Access-Info</th> <th>Classification</th> <th>Protocol</th> <th>From</th> <th>To</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2004-01-07 11:36:18</td> <td>3</td> <td>ICMP PING (Undefined Code)</td> <td>Misc activity</td> <td>ICMP</td> <td>192.168.17.150</td> <td>192.168.17.175</td> </tr> <tr> <td>2</td> <td>2004-01-07 11:36:19</td> <td>3</td> <td>ICMP Echo Reply (Undefined Code)</td> <td>Misc activity</td> <td>ICMP</td> <td>192.168.17.175</td> <td>192.168.17.150</td> </tr> <tr> <td>3</td> <td>2004-01-07 11:36:20</td> <td>2</td> <td>SCAN SOCKS Proxy attempt</td> <td>Attempted Information Leak</td> <td>TCP</td> <td>192.168.17.150:48968</td> <td>192.168.17.175:1080</td> </tr> <tr> <td>4</td> <td>2004-01-07 11:36:21</td> <td>2</td> <td>SNMP AgentX/tcp request</td> <td>Attempted Information Leak</td> <td>TCP</td> <td>192.168.17.150:48968</td> <td>192.168.17.175:705</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Download To Local"/> <input type="button" value="Prev. Page"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/> <input type="button" value="Next Page"/> List <input type="text" value="10"/> Per Page Page: 1/1 </p> | No. | Time | Pri | Access-Info | Classification | Protocol | From | To | 1 | 2004-01-07 11:36:18 | 3 | ICMP PING (Undefined Code) | Misc activity | ICMP | 192.168.17.150 | 192.168.17.175 | 2 | 2004-01-07 11:36:19 | 3 | ICMP Echo Reply (Undefined Code) | Misc activity | ICMP | 192.168.17.175 | 192.168.17.150 | 3 | 2004-01-07 11:36:20 | 2 | SCAN SOCKS Proxy attempt | Attempted Information Leak | TCP | 192.168.17.150:48968 | 192.168.17.175:1080 | 4 | 2004-01-07 11:36:21 | 2 | SNMP AgentX/tcp request | Attempted Information Leak | TCP | 192.168.17.150:48968 | 192.168.17.175:705 |
| No. | Time | Pri | Access-Info | Classification | Protocol | From | To | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 2004-01-07 11:36:18 | 3 | ICMP PING (Undefined Code) | Misc activity | ICMP | 192.168.17.150 | 192.168.17.175 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 2004-01-07 11:36:19 | 3 | ICMP Echo Reply (Undefined Code) | Misc activity | ICMP | 192.168.17.175 | 192.168.17.150 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 2004-01-07 11:36:20 | 2 | SCAN SOCKS Proxy attempt | Attempted Information Leak | TCP | 192.168.17.150:48968 | 192.168.17.175:1080 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 2004-01-07 11:36:21 | 2 | SNMP AgentX/tcp request | Attempted Information Leak | TCP | 192.168.17.150:48968 | 192.168.17.175:705 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Step 4 – Update Attack Patterns

IDS attack patterns require frequent updates because there are many new attacks every week. Please go to System Tools > Database Update > update to update IDS attack patterns. The DFL-1500 will connect to fwupdate.dlinktw.com.tw to fetch any new signatures.

System Tools > Database Update > Update

Update

Status :

URL database : v1.40808 [2004/08/09 16:17]

IDS signatures: v1.40809 [2004/08/09 16:17]

Auto Update :

Update Center

Update Schedule On

Auto URL update

Auto IDS update

Part VIII

Load Balancer、 Bandwidth

Management、 High Availability

Chapter 25

Load Balancer

This chapter introduces Load Balancer and explains how to implement it.

25.1 Demands

Organization_1

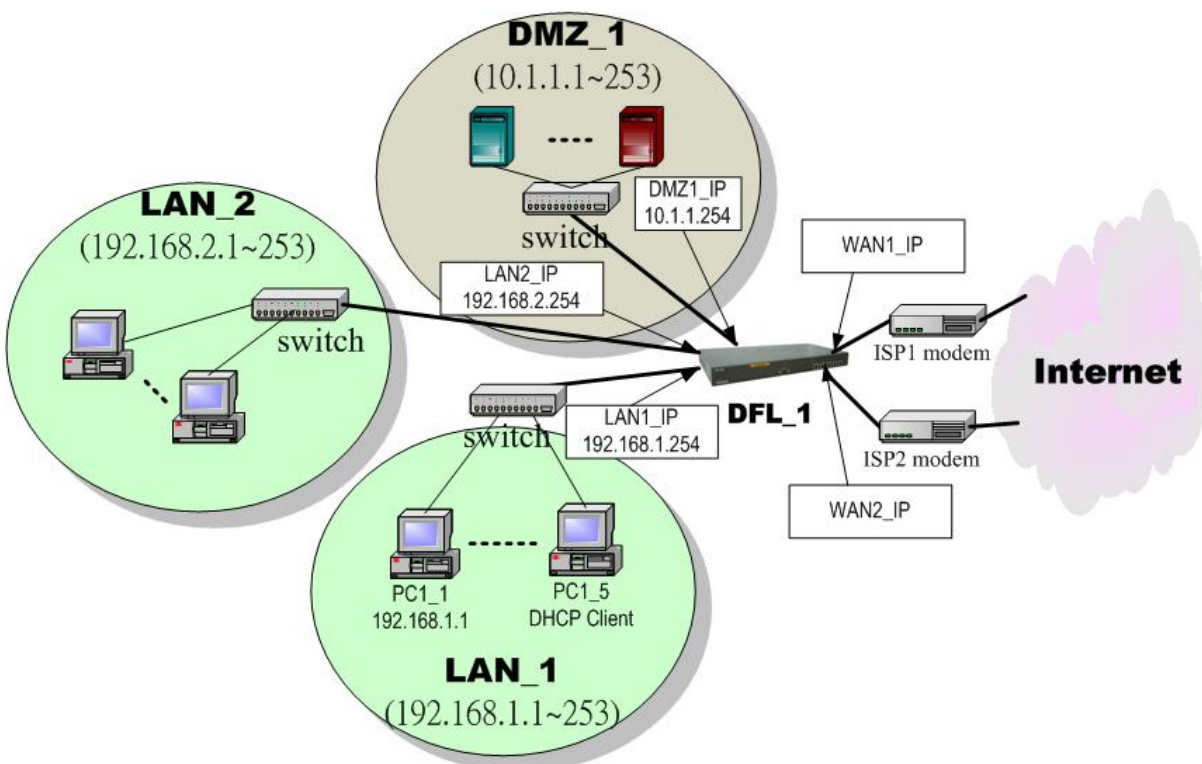


Figure 25-1 Multiple WAN settings of DFL-1500

The WAN load balancer module consists of outbound load balancing and inbound load balancing. Users may want to subscribe multiple WAN links and make their outbound traffic load-balanced among the WAN links. DFL-1500 now supports outbound WAN load balancing. Inbound load balancing will be supported in a very near future.

The WAN load balancer module currently supports

25.2 Objectives

The traffic from LAN_1 and LAN_2 towards the Internet are intelligently outbound load-balanced between the WAN links. However, traffic from DMZ_1 towards the Internet will be decided by the inbound load balancing module.

25.3 Methods

The outbound WAN load balancer module will intelligently decide whether the new connection will be directed to which WAN link. It has a built-in fuzzy intelligence that will measure the round-trip delay of the traffic and make the best route selection.

25.4 Steps

25.4.1 Outbound Load Balancer

Step 1. Make Firewall rules the same

Since the traffic will be intelligently load-balanced among the WAN links, the Firewall settings for all WAN links should be set to the same settings. For example, you have to make sure that all LAN1-to-WAN1 Firewall rules are the same as those in LAN1-to-WAN2, LAN2-to-WAN1, and LAN2-to-WAN2 rules. Otherwise, the traffic may be blocked by the firewall rules accidentally due to the load balancing decision.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Default action for this packet direction: Forward Log

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Move Before: 1

Step 2. Enable outbound WAN load balancer

Check the Enable Outbound WAN Load Balancer checkbox, click the Apply.

ADVANCED SETTINGS > Load Balancer > Outbound

Outbound

Enable Outbound WAN Load Balancer

When enabled, LAN-to-WAN traffic will be intelligently load-balanced among the following WAN links:

Port1: WAN1 (Static IP)
 IP Address: 61.2.1.1/255.255.255.248
 Gateway: 61.2.1.6

Port2: WAN2 (Static IP) [Default]
 IP Address: 61.71.105.4/255.255.255.248
 Gateway: 61.71.105.6

Routing priority: Policy Route > Static/Default Route > WAN Load Balancer

Note that the priority among the policy route, static route, and WAN load balancer are explicitly shown as Policy Route > Static/Default Route > WAN Load Balancer. If there are conflicted settings among these three settings, the route will be chosen according to the priority.

Chapter 26

Bandwidth Management

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

26.1 Demands

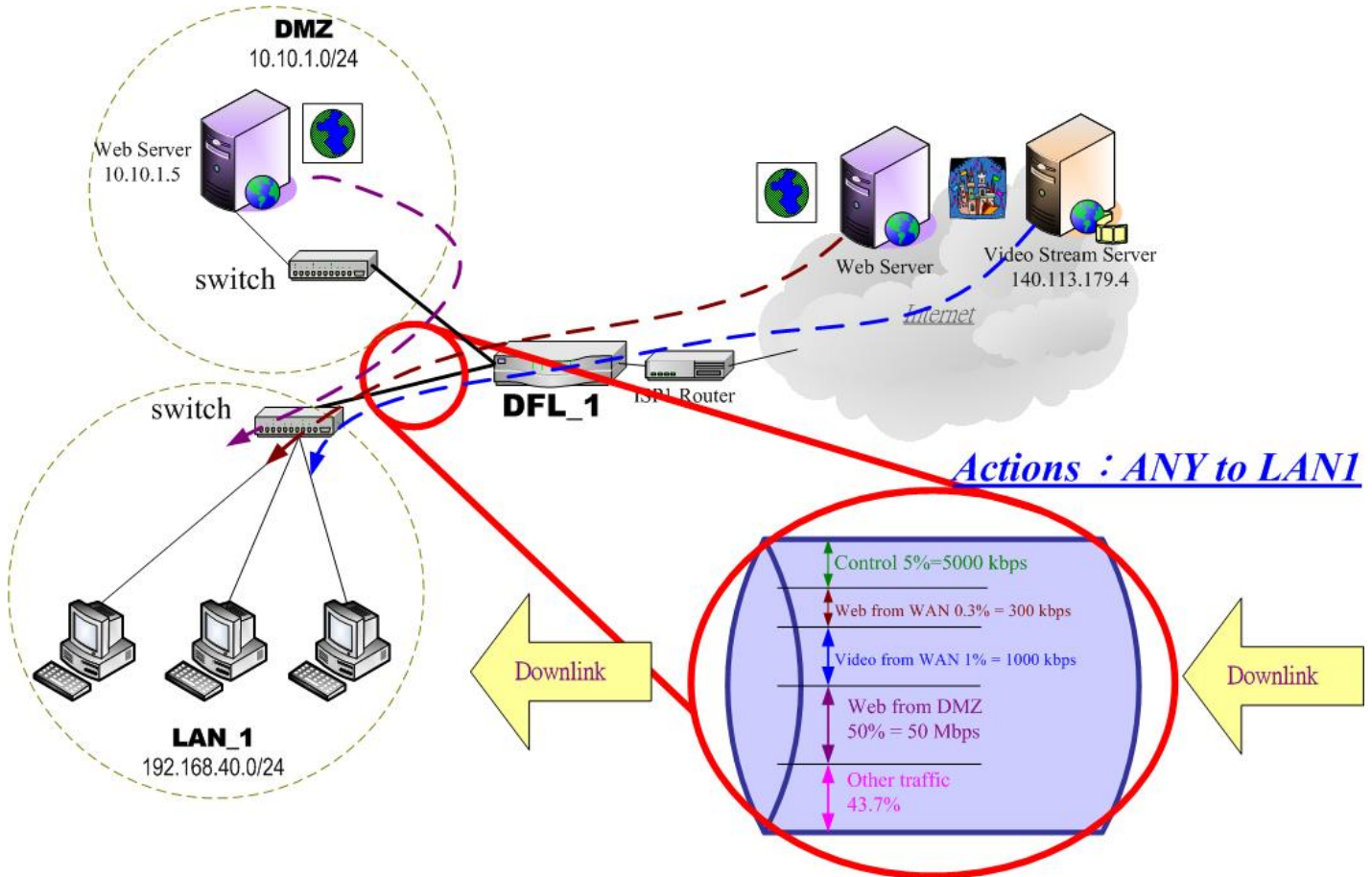


Figure 26-1 Use bandwidth management mechanism to shape the data flow on the downlink direction

- As the above Figure 26-1 illustrated, we hope LAN_1 users can watch the Video Stream Server smoothly. Besides, we hope LAN_1 users can access the web server located at DMZ region more faster

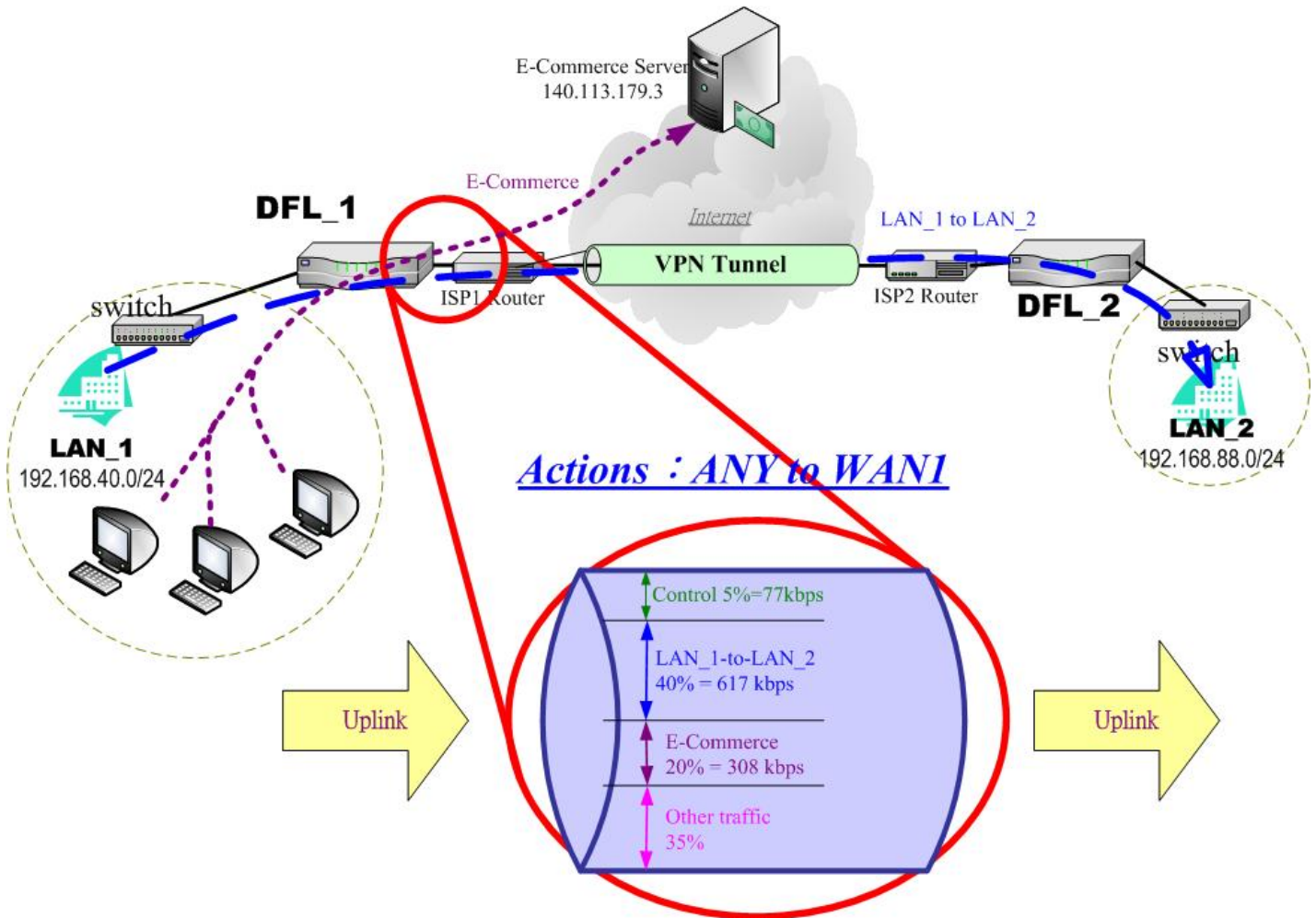


Figure 26-2 Use bandwidth management mechanism to shape the data flow on the uplink direction

- As the above Figure 26-2 illustrated, LAN_1 PCs are using the E-Commerce service from the E-Commerce Server (140.113.79.3), causing the blocking of the VPN transfer from LAN_1 to LAN_2. So we want to make sure that the VPN tunnel links is reserved at least 600 kbps speed rate. And the free bandwidth will raise the transmission bandwidth of LAN_1 PCs access the E-Commerce service.

26.2 Objectives

- As the above diagram Figure 26-1 illustrates, LAN_1 PCs are browsing the web pages from the Web Server of Internet. This occupies the bandwidth of PCs who are watching the video provided by the Video Stream Server (140.113.179.4), causing the video to be blocked and to have poor quality. So we hope to guarantee the video quality of the LAN_1 PCs which are accessing Video Stream Server.

The total bandwidth of ANY to LAN1 direction is 100 Mbps (The bandwidth of LAN1 interface is 100 Mbps). Here we will make sure that PCs of LAN_1 have the smooth stream quality that must have at least 1% of LAN1 total bandwidth (1000 kbps) speed rate.

Besides, we have another web server located at DMZ region. Because the web server is located at local area, so we can assign larger bandwidth for this direction (web traffic from DMZ → LAN).

The remaining bandwidths are named Other traffic. They are reserved for other ANY to LAN1 data transmission which don't list in the above Figure 26-1 diagram.

- Reserve at least 600kbps for the LAN_1 to LAN_2 transfer. The LAN_1 PCs can share about 20% (308kbps) for using E-Commerce Services. However, when the LAN_1 to LAN_2 traffic less than 40% (617kbps), the E-Commerce service can occupy the free bandwidth from LAN_1-toLAN_2 and the remaining bandwidth from default class.

26.3 Methods

- As the following Table 26-1 listed, partition the inbound bandwidth (total 100Mbps) into three classes, web_from_WAN, video_from_WAN and web_from_DMZ class. The remaining bandwidth is assigned to other services which are not listed here.

| Service | Goal | Assigned bandwidth | Borrow bit status |
|----------------|---|--------------------|-------------------|
| Web from WAN | limited bandwidth (MAX. 300kbps) | 0.3% = 300kbps | Disabled |
| Video from WAN | guaranteed bandwidth (At least 1000kbps) | 1% = 1000kbps | Enabled |
| Web from DMZ | guaranteed bandwidth (At least 50Mbps) | 50% = 50Mbps | Enabled |

Table 26-1 Bandwidth management action assignment from ANY to LAN1

- As the following Table 26-2 listed. Partition the outbound bandwidth (total 1.544Mbps) into two classes, the LAN_1-to-LAN_2 (40% 617 kbps) and the E-commerce (20% 308kbps) classes. Besides, set the E-Commerce to be able to borrow from other bandwidth if any bandwidth is available.

| Service | Goal | Assigned bandwidth | Borrow bit status |
|----------------|--|--------------------|-------------------|
| LAN_1 to LAN_2 | limited bandwidth (MAX. 617kbps) | 40% = 617kbps | Disabled |
| E-Commerce | guaranteed bandwidth (At least 308kbps) | 20% = 308kbps | Enabled |

Table 26-2 Bandwidth management action assignment from ANY to WAN1

26.4 Steps

26.4.1 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 | Range/Format | EXAMPLE |
|-----------------------------|---|----------------|---------|
| Enable Bandwidth Management | Enable Bandwidth Management feature of DFL-1500 | Enable/Disable | Enabled |
| BUTTON | DESCRIPTION | | |
| Reset Bandwidth Management | Reset all the bandwidth management rules to default status. | | |
| Apply | Apply the settings which have been configured. | | |

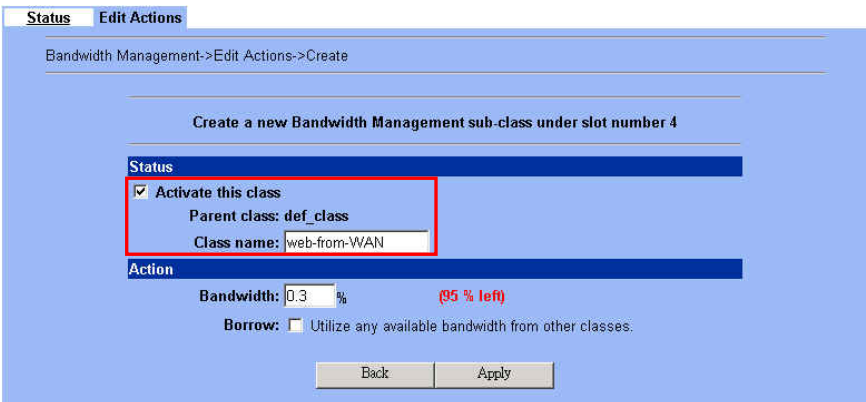
Table 26-3 Setup status page of Bandwidth Management

| | |
|---|---|
| <p>Step 2. Setup the LAN1 Link</p> <p>Select ANY to LAN1 to setup traffic that will be transmitted by the LAN1 interface. Enter the LAN1 interface bandwidth as 100000kbps (100Mbps). Click the Apply button to enforce the LAN1 link bandwidth to be specified bandwidth. In the table, the root class represents the whole bandwidth of the link. By default the link is partitioned into two classes: control class (ctl_class) and default class (def_class). The control class reserves bandwidth for control protocols such as ICMP, TCP ACKs. The default class is the default action of non-matched packets. The default class can be recursively partitioned into more classes. The classes are organized as a tree. Click Create Sub-Class to partition the default class.</p> | <p>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions</p> |
|---|---|

| FIELD | DESCRIPTION | Range/Format | EXAMPLE |
|----------------------------------|--|--------------------|--------------------------|
| Edit __ to __ classes | Select the direction of action which you are going to configure one. | ANY to WAN/LAN/DMZ | Edit ANY to LAN1 classes |
| LAN1 Interface Bandwidth __ kbps | Fill the real bandwidth which is located in the upper direction. | 10 to 100000 kbps | 100000 kbps |

| BUTTON | DESCRIPTION |
|------------------|---|
| Prev. Page | If there are more than one action pages, you can press Prev. Page to back to the previous page. |
| Next Page | If there are more than one action pages, you can press Next Page to go to the next page. |
| Create-Sub-class | Create a sub class from the indicated class. |
| Edit | Edit the properties of the existent class. |
| Delete | Delete the indicated class. |

Table 26-4 Setup edit actions page of Bandwidth Management

| | |
|---|---|
| <p>Step 3. Add new classes</p> <p>Create a sub-class named <code>web-from-WAN</code> from the default class. Enter 0.3% in the bandwidth field. Make sure that <code>Borrow</code> button is unchecked and then <code>web-from-WAN</code> class will not enlarge the bandwidth from borrowing other unused bandwidth. Finally, click <code>Apply</code> button. See the steps in the right diagram.</p> <p>Subsequently, we will continue to setup another two classes, such as <code>video-from-WAN</code> class and <code>web-from-DMZ</code> class. Select the default class and click the <code>Create Sub-Class</code> to create these two classes. The setting procedure is the same as the <code>web-from-WAN</code> class described.</p> | <p>ADVANCED SETTINGS > Bandwidth Mgt. > Edit Actions > Create Sub-class</p>  |
|---|---|

| FIELD | DESCRIPTION | Range/Format | EXAMPLE |
|---------------------|---|---|--------------|
| Activate this class | Enable the bandwidth management class for later use. | Enable/Disable | Enabled |
| Class name | Bandwidth management class name. | text string | web-from-WAN |
| Bandwidth | How many percentage does this class occupy the parent class? | 0.1 ~ Max Value (as red text described) | 0.3 |
| Borrow | When enabled, this class will borrow the idle bandwidth from other classes temporarily if needed. | Enable/Disable | Disabled |
| BUTTON | DESCRIPTION | | |
| Back | Back to previous configuration page. | | |
| Apply | Apply the settings which have been configured. | | |

Table 26-5 Add new class in the bandwidth management feature

Step 4. Partition into Classes

Now there are three actions under the default action.

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

Bandwidth Management->Edit Actions

Edit ANY to LAN1 classes

LAN1 Interface Bandwidth: 100000 kbps

| Item | # | Active | Name | Borrow | Bandwidth |
|------|---|--------|---------------------|--------|-------------|
| | 1 | Y | LAN1 Interface | | 100000 kbps |
| | 2 | Y | (100%) root_class | N | 100000 kbps |
| | 3 | Y | (5%) ct1_class | Y | 5000 kbps |
| | 4 | Y | (95%) def_class | Y | 95000 kbps |
| | 5 | Y | (50%) web-from-DMZ | Y | 50000 kbps |
| | 6 | Y | (1%) video-from-WAN | Y | 1000 kbps |
| | 7 | Y | (0.3%) web-from-WAN | N | 300 kbps |

Page 1/1

Step 5. Setup WAN1-to-LAN1 Rules

Select WAN1 to LAN1 to display the rules. There is a pre-defined rule that matches all traffic into the default class. Click Insert to insert a rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log

Packets are top-down matched by the rules.

| Item | # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
|------|---|---------|----------|-----------|----------|-------------|--------|-----|
| | 1 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

1

1

✓ **Note**

Regarding the above field description, please refer to Table 10-2 Add a firewall rule for details.

Step 6. Customize the Rule
Enter a rule name such as web-from-WAN, select the Source IP as WAN1_ALL and Dest. IP as LAN1_ALL Besides, make sure the service is HTTP (port 80) because of this is web service. Select the action to be web-from-WAN. In this way, all inbound web traffic from WAN1 will be put into the web-from-WAN queue and scheduled out at 300kbps bandwidth. Click Apply to store the changes.

Repeat the same procedure for the video-from-WAN class.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Status Edit Rules Show Rules Anti-DoS Summary

Firewall->Edit Rules->Insert

Insert a new WAN1-to-LAN1 Firewall rule

Status

Rule name: web-from-WAN
Schedule: Always

Condition

Source IP: WAN1_ALL Dest. IP: LAN1_ALL
Service: HTTP

Action

Forward and do not log the matched session.
Forward bandwidth class: web-from-WAN
Reverse bandwidth class: def_class

Back Apply

| | FIELD | DESCRIPTION | Range/Format | EXAMPLE |
|--------|-------------------------|--|--------------------------------------|--------------|
| Action | Forward bandwidth class | Select the forward bandwidth class which will be assigned to this rule. The forward bandwidth class is defined in the previous action of forward direction. In this case, it will be the actions of "ANY to LAN1". | All the actions of forward direction | web-from-WAN |
| | Reverse bandwidth class | Select the reverse bandwidth class which will be assigned to this rule. The reverse bandwidth class is defined in the previous action of reverse direction. In this case, it will be the actions of "ANY to WAN1". | All the actions of reverse direction | def_class |

Table 26-6 Add a new Bandwidth Management rule

✓ **Note**

For the other field description above, please refer Table 10-3 Insert a Firewall rule for details.

Step 7. View the rules
Now we can see that there are existed two customized rules in the queue of WAN1 to LAN1 direction.
In the No. 1 rule. The DFL-1500 is configured to direct video-from-WAN packets into the video-from-WAN queue (300kbps).
In the No. 2 rule. The DFL-1500 will direct web-from-WAN packets into the web-from-WAN queue (1000kbps).
In the No. 3 rule. The other traffic will be put into the def_class queue (any available bandwidth).

ADVANCED SETTINGS > Firewall > Edit Rules

Status Edit Rules Show Rules Anti-DoS Summary

Firewall->Edit Rules

Edit WAN1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

| Item | Status | | Condition | | | Action | |
|------|----------------|----------|------------|----------|-------------|---------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | video-from-WAN | ALWAYS | WAN1_video | LAN1_ALL | ANY | Forward | N |
| 2 | web-from-WAN | ALWAYS | WAN1_ALL | LAN1_ALL | HTTP | Forward | N |
| 3 | Default | ALWAYS | WAN1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

Prev. Page Next Page Move Page 1

Insert Edit Delete Move Before: 1

Step 8. Add DMZ to LAN1 rule

Here we will add another rule (web from DMZ). Select DMZ1 to LAN1 direction.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit DMZ1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

| Item | Status | | Condition | | | Action | |
|------|---------|----------|-----------|----------|-------------|--------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | Default | ALWAYS | DMZ1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

Step 9. Customize the rule

Setup the web-from-DMZ rule. Here we select DMZ1_ALL / LAN1_ALL in the Source IP / Dest. IP field. It means that if the packets come from DMZ and targeted LAN1 region, we do not need to care about its source / dest IP. If the packets request for web traffic (source port HTTP 80), it will be put into the web-from-DMZ queue by DFL-1500 bandwidth management feature.

Note: In the Action region, the web-from-DMZ class was edited in the previous Step 4 before.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new DMZ1-to-LAN1 Firewall rule

Status

Rule name: web-from-DMZ

Schedule: Always

Condition

Source IP: DMZ1_ALL Dest. IP: LAN1_ALL

Service: HTTP

Action

Forward and do not log the matched session.

Forward bandwidth class: web-from-DMZ

Reverse bandwidth class: def_class

Back Apply

Step 10. View the results

We can see the result of our settings at the DMZ-to-LAN rule direction.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit DMZ1 to LAN1 rules

Default action for this packet direction: Block Log Apply

Packets are top-down matched by the rules.

| Item | Status | | Condition | | | Action | |
|------|--------------|----------|-----------|----------|-------------|---------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | web-from-DMZ | ALWAYS | DMZ1_ALL | LAN1_ALL | HTTP | Forward | N |
| 2 | Default | ALWAYS | DMZ1_ALL | LAN1_ALL | ALL_SERVICE | Block | Y |

Page 1/1

26.4.2 Outbound Traffic Management

Step 1. Enable Bandwidth Management

Check the **Enable Bandwidth Management** checkbox, click the **Apply**.

ADVANCED SETTINGS > Bandwidth Mgt. > StatusStatus **Edit Actions** **Enable Bandwidth Management**

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

Step 1. Enable the bandwidth management system.

Step 2. Edit actions to be imposed on each link.

Step 3. Choose the preferred action during editing firewall rules.

[Reset Bandwidth Management](#)

[Apply](#)**Step 2. Setup the WAN1 Link**

Select **ANY** to **WAN1** to setup traffic that will be transmitted by the WAN1 interface. Enter the WAN1 interface bandwidth as 1544kbps. Click the **Apply** button to enforce the WAN1 link bandwidth to be 1544kbps. Then click **Create Sub-Class** to partition the default class.

ADVANCED SETTINGS > Bandwidth Mgt. > Edit ActionsStatus **Edit Actions**

Bandwidth Management->Edit Actions

Edit **ANY** to **WAN1** classesWAN1 Interface Bandwidth: 1544 kbps [Apply](#)

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

Page 1/1

[Prev. Page](#)[Next Page](#)[Create Sub-class](#)[Edit](#)[Delete](#)**Step 3. Partition into Classes**

Create a sub-class named **LAN_1-to-LAN_2** from the default class. Enter 40% in the bandwidth field, uncheck the **Borrow** button, and click **Apply**. Select the default class and click the **Create Sub-Class** to create another sub-class named **E-Commerce** from the default class. Enter 20% in the bandwidth field, check the **Borrow** button and click **Apply**. Now there are two actions under the default action. They are separately **LAN_1-to-LAN_2** and **E-Commerce** class as the right diagram.

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

Bandwidth Management->Edit Actions

Edit **ANY** to **WAN1** classesWAN1 Interface Bandwidth: 1544 kbps [Apply](#)

| Item | # | Active | Defined Actions | Borrow | Bandwidth |
|------|---|--------|----------------------|--------|-----------|
| | 1 | Y | WAN1 Interface | | 1544 kbps |
| | 2 | Y | (100%) root_class | N | 1544 kbps |
| | 3 | Y | (5%) cti_class | Y | 77 kbps |
| | 4 | Y | (95%) def_class | Y | 1466 kbps |
| | 5 | Y | (20%) E-Commerce | Y | 308 kbps |
| | 6 | Y | (40%) LAN_1-to-LAN_2 | N | 617 kbps |

Page 1/1

[Prev. Page](#)[Next Page](#)[Create Sub-class](#)[Edit](#)[Delete](#)

Step 4. Setup LAN1-to-WAN1 Rules

Select LAN1 to WAN1 to display the rules. There is a pre-defined rule that matches all traffic into the default class. Click Insert to insert a rule before the default rule.

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward Log

Packets are top-down matched by the rules.

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

Page 1/1

Prev. Page Next Page Move Page 1

Step 5. Customize the Rules

Enter a rule name such as outVPN, select the Source IP as LAN1_outVPN (192.168.40.0) and Dest. IP as WAN1_outVPN (192.168.88.0). Select the action to be LAN_1-to-LAN_2. In this way, all outbound packets to the LAN_2 area will be put into the LAN_1-to-LAN_2 queue and scheduled out at 617 kbps bandwidth. Click Apply to store the changes.

Repeat the same procedure for the outE-Commerce rule.

ADVANCED SETTINGS > Firewall > Edit Rules > Insert

Firewall->Edit Rules->Insert

Insert a new LAN1-to-WAN1 Firewall rule

Status

Rule name: outVPN

Schedule: Always

Condition

Source IP: LAN1_outVPN Dest. IP: WAN1_outVPN

Service: ANY

Action

Forward and do not log the matched session.

Forward bandwidth class: LAN_1-to-LAN_2

Reverse bandwidth class: def_class

Step 6. View the rules

The DFL-1500 is configured to direct outE-Commerce matched packets into the E-Commerce queue (308 kbps), outVPN matched packets into the LAN_1-to-LAN_2 queue (617 kbps). Here we reserve 40% WAN1 bandwidth for the LAN_1 to LAN_2 VPN data, to guarantee the data communication between VPN. The other traffic will be put into the def_class queue (any available bandwidth).

ADVANCED SETTINGS > Firewall > Edit Rules

Firewall->Edit Rules

Edit LAN1 to WAN1 rules

Default action for this packet direction: Forward Log

Packets are top-down matched by the rules.

| Item | Status | | Condition | | | Action | |
|------|---------------|----------|-------------|----------------|-------------|---------|-----|
| # | Name | Schedule | Source IP | Dest. IP | Service | Action | Log |
| 1 | outE-Commerce | ALWAYS | LAN1_ALL | WAN1_Ecommerce | ANY | Forward | N |
| 2 | outVPN | ALWAYS | LAN1_outVPN | WAN1_outVPN | ANY | Forward | N |
| 3 | Default | ALWAYS | LAN1_ALL | WAN1_ALL | ALL_SERVICE | Forward | N |

Page 1/1

Prev. Page Next Page Move Page 1

Chapter 27

High Availability

This chapter introduces High Availability and explains how to implement it.

27.1 Demands

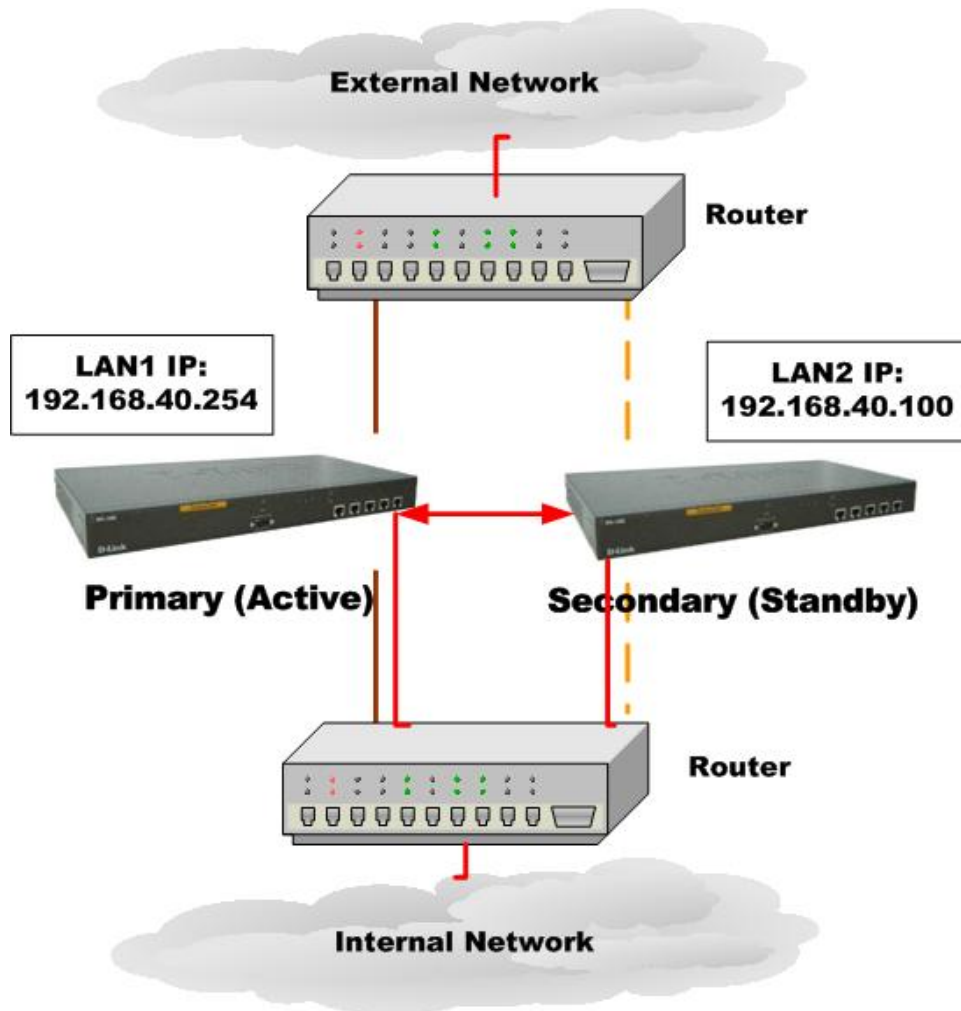


Figure 27-1 Use High Availability mechanism to let network connection continually

1. As the above Figure 22-1 illustrates, your company is afraid that the firewall may crash someday, so it needs a backup system to let the network connection continually. High Availability makes it possible to let the network in your company operate smoothly.

27.2 Objectives

1. Prepare two DFL-1500 devices, and then let one as a primary firewall and the other as a secondary one. While the primary firewall is crashed, you can replace it with secondary firewall.

27.3 Methods

There are five steps to configure High Availability feature.

- Step 1. Set two DFL-1500 devices first. Remember to set the Action Mode for primary device as Active mode and secondary device as Standby mode.
- Step 2. When the primary device crashes, the secondary one will replace it within 30 seconds while detecting by “ping” command.
- Step 3. The secondary device will immediately load the configuration from primary device, and then change its action mode to Active mode.
- Step 4. After rebooting, the primary device will automatically change its action mode to Standby mode if it detects the secondary device in active mode already.
- Step 5. If both of primary and secondary devices crash simultaneously, the one which reboots faster will action as Active mode, and the other will be in Standby mode.

27.4 Steps

27.4.1 Setup High Availability

| | |
|---|--|
| <p>Step 1. Enable High Availability</p> <p>Check the Enable High Availability checkbox. Select the Action Mode as Active if it is the primary device and Standby for the secondary device. And then configure the other HA device. Select which interface to connect to. Enter IP Address and Login Password.</p> <p>Note that you have to configure the Secondary device as Standby mode and the IP address/Login Password of the Primary device, so High Availability can work then.</p> | <div style="border: 1px solid black; padding: 5px;"> <p>ADVANCED SETTINGS > High Availability > Status</p> <p>Status</p> <p><input checked="" type="checkbox"/> Enable High Availability</p> <hr/> <p>Action Mode Active ▾</p> <p>The settings for the other HA device:</p> <p>Connect to interface LAN1 ▾</p> <p>IP Address 192.168.40.100</p> <p>Login Password ****</p> <p style="text-align: center;"><input type="button" value="Apply"/></p> </div> |
|---|--|

| FIELD | DESCRIPTION | Range/Format | EXAMPLE |
|--------------------------|---|----------------|----------------|
| Enable High Availability | Activate the High Availability feature. | Enable/Disable | Enabled |
| Action Mode | Specify which device is Active or Standby. | Active/Standby | Active |
| Connect to interface | The interface zone where the HA devices is set. | LAN1/LAN2/DMZ | LAN1 |
| IP Address | The IP address of the other HA device. | Ipv4 format | 192.168.40.100 |
| BUTTON | DESCRIPTION | | |
| Apply | Apply the settings which have been configured. | | |

Table 27-1 Setup status page of High Availability

Step 2. Show the result in Web

After you apply the High Availability feature, the Primary device will show the message to tell you that “Sync configuration file successfully, the device will rebooting now and stay in standby mode.”

ADVANCED SETTINGS > High Availability > Status

Step 3. Show the message in Console

When Primary device crashed, the messages like the right diagram will appear to tell you that this device will be in Standby mode after rebooting.

```
login: syncing disks... done
rebooting...

>> NetOS Loader (i386), V1.5 (Mon Jul 19 18:54:37 CST 2004)
Press <TAB> to prompt - starting in 0
1453120+10792452+2439344 [159+113696+989881=0xe27a8c
NetOS Ver2.000 (WALL) #0: Thu Sep 9 05:46:41 CST 2004
total memory = 255 MB
avail memory = 235 MB
cpu0: Intel Celeron (686-class), 1202.79 MHz, id 0x6b4
ASIC IPsec Enabled
Ethernet address 00:80:c8:50:fb:87
Ethernet address 00:80:c8:50:fb:88
Ethernet address 00:80:c8:50:fb:89
Ethernet address 00:80:c8:50:fb:8a
Ethernet address 00:80:c8:50:fb:8b
IPsec: Initialized Security Association Processing.
Software Serial Number: [39686122395656264007]
Installing Modules ... done.
Startup High Availability : Standby mode.

NetOS/i386 (HA: Standby mode) (tty00)

login:
```

Step 4. Check the Device status

You can see the status of the device in Standby mode here.

```
Welcome to DFL-1500 VPN/Firewall Router

DFL-1500> en
DFL-1500# sys st
=====
System Name:
Firmware Version: NetOS Ver2.000 (WALL) #0: Thu Sep 9 05:46:41 CST 2004
Software Serial Number: 39686122395656264007
=====
Operation Mode: NAT/Router
Default Gateway:
Primary DNS:      Secondary DNS:
=====
Port Interface IP Address      Netmask      Status Type
-----
1
2
3
4
5
=====
11:24AM up 1 min, 0 users, load averages: 1.10, 0.37, 0.14
DFL-1500# _
```

Part IX

System Maintenance

Chapter 28

System Status

28.1 Demands

1. Since DFL-1500 has been set and installed, you may want to gather the device information, so you can overview the system status quickly.

28.2 Objectives

1. To know the current situation easily through an integrated web user interface.

28.3 Methods

1. Get the needed information from the DEVICE STATUS pages.

28.4 Steps

Step 1. System Status

Here we can see the system information (including system name, firmware version), and the full list of each port settings.

DEVICE STATUS > System Status > System Status

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions |
|--|----------------|--------------|------------|---------------|-----------------|----------------|----------------|
| System Name: DFL-1500.dlink.com Firmware Version: NetOS Ver2.001 (WALL) #5: Thu Sep 23 15:26:41 CST 2004 Software Serial Number: 60623576436830003320 | | | | | | | |
| Operation Mode: NAT/Router Default gateway: 61.2.1.6 Primary DNS: 168.95.1.1 Secondary DNS: | | | | | | | |
| Port1: WAN1 (Static IP)[Default] IP Address: 61.2.1.1 Subnet Mask: 255.255.255.248 | | | | | | | |
| Port2: WAN2 (Not initialized) IP Address: not set | | | | | | | |
| Port3: DMZ1 IP Address: 10.1.1.254 Subnet Mask: 255.255.255.0 | | | | | | | |
| Port4: LAN1 IP Address: 192.168.40.254 Subnet Mask: 255.255.255.0 | | | | | | | |
| Port5: LAN2 IP Address: 192.168.2.254 Subnet Mask: 255.255.255.0 | | | | | | | |

Step 2. Network Status

We can know the port status here, whether the port is up or down, and view the amount of the transmitted packets or received packets in each port.

DEVICE STATUS > System Status > Network Status

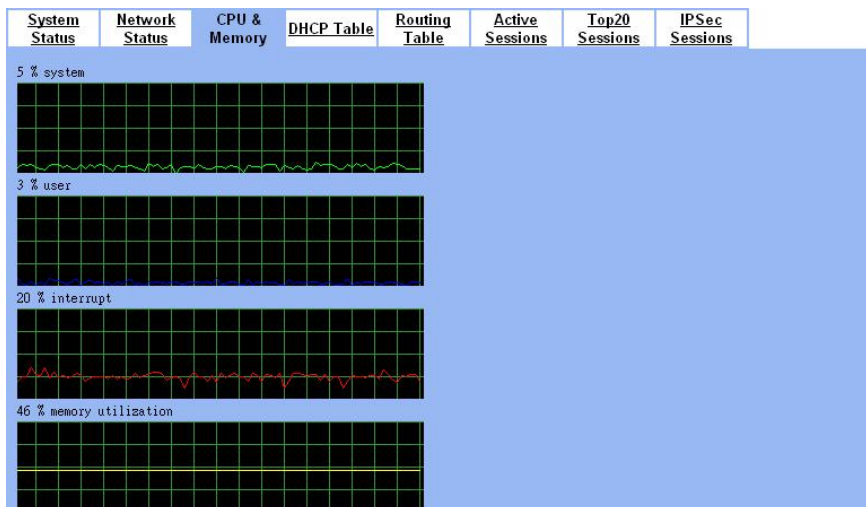
| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions |
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|
| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | |
| 1. WAN1 | UP | 1 | 108 | 0 | 0 | 55 | |
| 2. WAN2 | DOWN | 0 | 0 | 0 | 0 | 0 | |
| 3. DMZ1 | UP | 1 | 10 | 0 | 0 | 0 | |
| 4. LAN1 | UP | 1270 | 1317 | 0 | 2150 | 349 | |
| 5. LAN2 | UP | 1 | 10 | 0 | 0 | 0 | |

| FIELD | DESCRIPTION |
|-------|----------------------------|
| Port | The interface of DFL-1500. |

Part IX System Maintenance

| | |
|------------|--|
| Status | The interface status of DFL-1500. The possible value is either “UP” or “DOWN”. |
| TxPkts | The amount of packets which are transferred from this interface in bytes. |
| RxPkts | The amount of packets which are received from this interface in bytes |
| Collisions | The amount of packets which have collisions in this interface. |
| Tx B/s | The transmitted speed of packets which are in the indicated interface. |
| Rx B/s | The receipted speed of packets which are in the indicated interface. |

Table 28-1 field description of network status

| | |
|--|---|
| <p>Step 3. CPU & Memory</p> <p>We can know the device information (including system, user, interrupt and memory utilization) through the graphic interface. For example, CPU states: 3.0% user, 0% nice, 5% system, 20% interrupt, and 72% idle. CPU Utilization= user + nice + system + interrupt + idle= 100%</p> <p>Note: If you can not view the graphic correctly, the situation may result from that you don't install the java virtual machine (JVM) onto your browser. Simply go to the following link, http://java.sun.com/j2se/1.4.2/download.html. And then, download the Java 2 Platform, Standard Edition (JRE) to your platform (ex. Windows). After installing JRE properly, you will see the CPU & Memory graphic as right side.</p> | <p>DEVICE STATUS > System Status > CPU & Memory</p>  <p>The screenshot shows a web interface with a navigation menu at the top containing: System Status, Network Status, CPU & Memory (selected), DHCP Table, Routing Table, Active Sessions, Top20 Sessions, and IPSec Sessions. Below the menu are four line graphs on a grid background. The first graph is titled '5 % system' and shows a green line fluctuating near the bottom. The second is '3 % user' with a blue line. The third is '20 % interrupt' with a red line showing more activity. The fourth is '46 % memory utilization' with a purple line.</p> |
|--|---|

| FIELD | DISCRIPTION |
|----------------------|---|
| % system | The percentage of the CPU utilization to perform kernel functions, I/O and other hardware interaction. |
| % user | The percentage of the CPU utilization to perform high-level functions, data movement, math, etc. such as the running of the Anti-Virus, Anti-Spam, Content Filter, etc. |
| % interrupt | The percentage of the CPU utilization for the network traffic to trigger the CPU running. The VPN/Firewall Router uses interrupts to signal the CPU when there is work for it to do. For example, when a packet comes to the device, it will trigger the CPU to work. A large number of packets come concurrently (such as attacks), they will raise the CPU's loading. The percentage of the interrupt will then be quite high to tell you that the device has many jobs to do. Watching the count of each interrupt can give you a rough idea of how much load the VPN/Firewall Router is handling. |
| % memory utilization | The percentage of the memory utilization. When many processes are running and using up available memory, the system will slow down as processes get paged or swapped out to make room for other processes to run. When the time slice is exhausted, that task may have to be written out to the paging device to make way for the next process. Memory-utilization graphs help point out memory problems. |

Table 28-2 Explanation of the CPU & Memory Page

Step 4. DHCP Table

Through the DHCP Table, we can recognize which IP has been allocated by the DHCP server. And know which pc (MAC address) has been leased this IP address.

DEVICE STATUS > System Status > DHCP Table

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions | | | | | | | | | | | | | | | |
|--|----------------|--------------|-------------------|---------------------|-----------------|----------------|----------------|---|------------|----------|-------------|----------------|---|---------------|----------|-------------------|---------------------|---|---------------|----------|-------------------|---------------------|
| <table border="1"> <thead> <tr> <th>#</th> <th>IP Address</th> <th>Hostname</th> <th>MAC Address</th> <th>Leases Expires</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>192.168.17.20</td> <td>04033nb1</td> <td>00:0D:60:80:43:90</td> <td>2004-10-04 12:21:29</td> </tr> <tr> <td>2</td> <td>192.168.17.14</td> <td>04033nb1</td> <td>00:0D:C9:92:11:40</td> <td>2004-10-04 13:35:57</td> </tr> </tbody> </table> | | | | | | | | # | IP Address | Hostname | MAC Address | Leases Expires | 1 | 192.168.17.20 | 04033nb1 | 00:0D:60:80:43:90 | 2004-10-04 12:21:29 | 2 | 192.168.17.14 | 04033nb1 | 00:0D:C9:92:11:40 | 2004-10-04 13:35:57 |
| # | IP Address | Hostname | MAC Address | Leases Expires | | | | | | | | | | | | | | | | | | |
| 1 | 192.168.17.20 | 04033nb1 | 00:0D:60:80:43:90 | 2004-10-04 12:21:29 | | | | | | | | | | | | | | | | | | |
| 2 | 192.168.17.14 | 04033nb1 | 00:0D:C9:92:11:40 | 2004-10-04 13:35:57 | | | | | | | | | | | | | | | | | | |
| Refresh | | | | | | | | | | | | | | | | | | | | | | |

| FIELD | DESCRIPTION |
|----------------|---|
| IP Address | The IP address which is assigned by the DHCP server of DFL-1500. |
| Hostname | The hostname of the specified host which gets the IP address by DHCP. |
| MAC Address | The MAC address of the specified host which gets the IP address by DHCP. |
| Leases Expires | The expired lease time of the specified host which gets the IP address by DHCP. |

Table 28-3 field description of DHCP table

Step 5. Routing Table

Click the Routing Table to see the routing table information of DFL-1500.

DEVICE STATUS > System Status > Routing Table

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|----------------|----------------------------|----------------|---------------|-----------------|----------------|----------------|---|------|---------------------|---------|-----------|---|----------------|-----------------|----------|------|---|-----|------------------------|------------|------|---|-----|--------------------------|----------|------|---|-----|---------------------------|---------------|------|---|-----|----------------------------|----------------|------|
| <table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Destination/Netmask</th> <th>Gateway</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Default/Static</td> <td>0.0.0.0/0.0.0.0</td> <td>61.2.1.6</td> <td>WAN1</td> </tr> <tr> <td>2</td> <td>Net</td> <td>10.1.1.0/255.255.255.0</td> <td>10.1.1.254</td> <td>DMZ1</td> </tr> <tr> <td>3</td> <td>Net</td> <td>61.2.1.0/255.255.255.248</td> <td>61.2.1.1</td> <td>WAN1</td> </tr> <tr> <td>4</td> <td>Net</td> <td>192.168.2.0/255.255.255.0</td> <td>192.168.2.254</td> <td>LAN2</td> </tr> <tr> <td>5</td> <td>Net</td> <td>192.168.40.0/255.255.255.0</td> <td>192.168.40.254</td> <td>LAN1</td> </tr> </tbody> </table> | | | | | | | | # | Type | Destination/Netmask | Gateway | Interface | 1 | Default/Static | 0.0.0.0/0.0.0.0 | 61.2.1.6 | WAN1 | 2 | Net | 10.1.1.0/255.255.255.0 | 10.1.1.254 | DMZ1 | 3 | Net | 61.2.1.0/255.255.255.248 | 61.2.1.1 | WAN1 | 4 | Net | 192.168.2.0/255.255.255.0 | 192.168.2.254 | LAN2 | 5 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.254 | LAN1 |
| # | Type | Destination/Netmask | Gateway | Interface | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Default/Static | 0.0.0.0/0.0.0.0 | 61.2.1.6 | WAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Net | 10.1.1.0/255.255.255.0 | 10.1.1.254 | DMZ1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Net | 61.2.1.0/255.255.255.248 | 61.2.1.1 | WAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Net | 192.168.2.0/255.255.255.0 | 192.168.2.254 | LAN2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Net | 192.168.40.0/255.255.255.0 | 192.168.40.254 | LAN1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Prev. Page Refresh Next. Page | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| FIELD | DESCRIPTION |
|---------------------|--|
| Type | The type of this specified routing entry. "Net" means that the routing entry is generated by the direct-connected interface. "Net/Static" means that the routing is generated by the static routing, please refer to section 8.4.1. "Default Static" is generated by the default gateway of default WAN link. |
| Destination/Netmask | The destination address of this specified routing entry. |
| Gateway | The target gateway of this specified routing entry. |
| Interface | The outgoing interface when the passing through traffic matches this routing entry. |

Table 28-4 field description of routing table

Step 6. Active Sessions

Click the Active Sessions to see all the current sessions of DFL-1500. The Active Sessions include all the outbound and inbound sessions.

DEVICE STATUS > System Status > Active Sessions

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions |
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|

Refresh Clear

Current Sessions: 1 Page 1/1

| Item | Source | Destination | Traffic Statistics | | |
|------|---------------|-------------|--------------------|------|-------|
| # | IP Address | Port | IP Address | Port | Bytes |
| 1 | 192.168.17.78 | 3612 | 192.168.17.176 | 443 | 1937 |

Current Sessions: 1 Page 1/1

Prev. Page Next Page Move Page 1

Step 7. Top20 Sessions

Click the Top20 Sessions to see the front-20 sessions of transmitted bytes amount. These front-20 sessions were sorted by the amount of current transmitted bytes.

Note: Here Traffic Statistics are calculated by the transmitted bytes from the Source IP Address/Port to the Destination IP Address/Port.

DEVICE STATUS > System Status > Top20 Sessions

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions |
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|

Refresh Clear

Current Sessions: 1 Page 1/1

| Item | Source | Destination | Traffic Statistics | | |
|------|---------------|-------------|--------------------|------|-------|
| # | IP Address | Port | IP Address | Port | Bytes |
| 1 | 192.168.17.78 | 3631 | 192.168.17.176 | 443 | 1929 |

Current Sessions: 1 Page 1/1

Prev. Page Next Page Move Page 1

Step 8. IPSec Sessions

If we use the IPSec to establish VPN with other device, then we can view the IPSec tunnel information in this page.

DEVICE STATUS > System Status > IPSec Sessions

| System Status | Network Status | CPU & Memory | DHCP Table | Routing Table | Active Sessions | Top20 Sessions | IPSec Sessions |
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|
|---------------|----------------|--------------|------------|---------------|-----------------|----------------|----------------|

Refresh Delete Item Delete All

Current Sessions: 1 Page 1/1

| Item | End Points | | Created Date | Traffic Statistics (Bytes) | |
|------|---------------|-------------------|----------------------|----------------------------|----------|
| # | My IP Address | Peer's IP Address | Day/Time/Year | Transmitted | Received |
| 1 | 140.113.1.1 | 140.113.1.200 | May 29 15:38:02 2004 | 10154848 | 29186080 |

Current Sessions: 1 Page 1/1

Prev. Page Next Page Move Page 1

Chapter 29

Log System

29.1 Demands

1. The System Administrator wants to know all the actions of administration in the past. So it can avoid illegal system administration.
2. The System Administrator needs to check the logs of VPN, IDS, Firewall, and Content Filter everyday. But he / she feels inconvenient to verify the DFL-1500 logs. He / She hopes to decrease the checking procedure.

29.2 Objectives

1. The System Administrator wants to know all actions of administration in the past.
2. The System administrator would like to view the daily log report of DFL-1500.

29.3 Methods

1. Through tracking the system logs, you can distinguish which administrated action is valid or not.
2. Use the syslog server to receive mail, or edit the “Mail Logs” page of DFL-1500. Make the log mailed out automatically every periodic time.

29.4 Steps

29.4.1 System Logs

Step 1. View System Logs

All the system administrated actions will be log in this page.

For the detailed information of System Logs, please refer Appendix D.

DEVICE STATUS > System Logs


| System Access Logs | | | |
|--------------------|---------------------|---------------|--|
| No. | Time | Source-IP | Access-Info |
| 1 | 2004-04-27 16:23:23 | DFL-1500 | Firewall: Reload all rules at startup |
| 2 | 2004-04-27 16:23:23 | DFL-1500 | NAT: rule for Basic-LAN1 added |
| 3 | 2004-04-27 16:23:24 | DFL-1500 | NAT: rule for Basic-LAN2 added |
| 4 | 2004-04-27 16:23:24 | DFL-1500 | NAT: rule for Basic-DMZ1 added |
| 5 | 2004-04-27 16:23:27 | DFL-1500 | SYSTEM: [S5] HTTP started. |
| 6 | 2004-04-27 16:23:28 | DFL-1500 | SYSTEM: [S6] HTTPS started. |
| 7 | 2004-04-27 16:53:18 | 192.168.2.170 | AUTH: [A1] admin login success (192.168.2.254:443) |
| 8 | 2004-04-27 16:53:35 | 192.168.2.170 | SYSTEM: [S8] WAN1: IP address: 61.2.1.1/255.255.255.248. EventID:3 |
| 9 | 2004-04-27 16:53:35 | 192.168.2.170 | SYSTEM: [S3] WAN1: Gateway IP: 61.2.1.6. EventID:3 |
| 10 | 2004-04-27 16:53:35 | 192.168.2.170 | SYSTEM: [S3] WAN1: Set default WAN link from WAN1 to WAN1 |

List 10 Per Page Page: 1/12

| FIELD | DESCRIPTION |
|--------------|---|
| NO | system logs sequence number |
| Time | The time which is occurred by the specified system event. |
| Source-IP | A type of the specified system events. |
| Access--Info | The description of the system log. Include Component Type, Log ID, Log Description and Event ID (optional). |


Table 29-1 System log description

29.4.2 Syslog & Mail log

| | |
|---|---|
| <p>Step 1. Setup Syslog Server</p> <p>Setup Syslog Server by checking the Enable Syslog Server. It will let DFL-1500 send logs to the Syslog Server specified in the "Syslog Server IP Address" field.</p> <p>Notice: If the logs were sent out to the syslog server, they will still keep a copy in the DFL-1500.</p> | <p>DEVICE STATUS > Log Config > Syslog Server</p>  |
|---|---|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|--------------------------|--|----------------|-----------|
| Enable Syslog Server | Enable the Syslog Server feature of DFL-1500 | Enable/Disable | Enabled |
| Syslog Server IP Address | The IP Address which Syslog Server located. | IPv4 format | 10.1.1.20 |

Table 29-2 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>Notice:</p> <ol style="list-style-type: none"> If the logs were sent out to the mail server, they will be deleted by the DFL-1500. The mail server of the email to receive the log reports should be the same as the mail server sending logs out. | <p>DEVICE STATUS > Log Config > Mail Logs</p>  |
|---|--|

| FIELD | DESCRIPTION | Range / Format | EXAMPLE |
|----------------------|---|--|----------------------|
| Enable Mail Logs | Enable the Mail Logs Server feature of DFL-1500 | Enable / Disable | Enabled |
| Mail Server | The IP Address of Mail Server which will send out the logs. | IPv4 format | 10.1.1.1 |
| Mail Subject | The subject of log mail | text string | Log Report |
| E-mail Logs To | E-Mail address of receiver | valid mail address format | <u>mis@dlink.com</u> |
| Log Schedule | The schedule which the mail logs will be sent out. Note if you choose "Immediately", it will increase the load of the DFL-1500 device, especially, many logs will be producing. | When Log is Full / Immediately / Hourly / Daily / Weekly | 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 ~ Sunday | Monday |
| BUTTON | DESCRIPTION | | |

| | |
|------|---|
| Test | Test the mail logs configuration in this page |
|------|---|

Table 29-3 Setup the Mail Logs

Chapter 30

System Maintenance

This chapter introduces how to do system maintenance.

30.1 Demands

1. DFL-1500 is designed to provide upgradeable firmware and database to meet the upcoming dynamics of the Internet. New features, new attack signatures and new forbidden URLs require timely updates to the DFL-1500. This chapter introduces how to upgrade your system with TFTP and Web UI respectively.
2. Sometimes one may want to reset the firmware to factory default due to loss of password, firmware corrupted, configuration corrupted. Since DFL-1500 does not have a reset button to prevent careless pressing of it, factory default has to be set with web GUI or console terminal. Of course, when you lose the password, you have to use CLI only because you can never enter the web GUI with the lost password.
3. Another issue is that after setup the DFL-1500 properly, we might want to keep the current configuration to avoid the unknown accident. Then we can recover the original state from the previous reserved configuration.

30.2 Firmware upgrade from TFTP

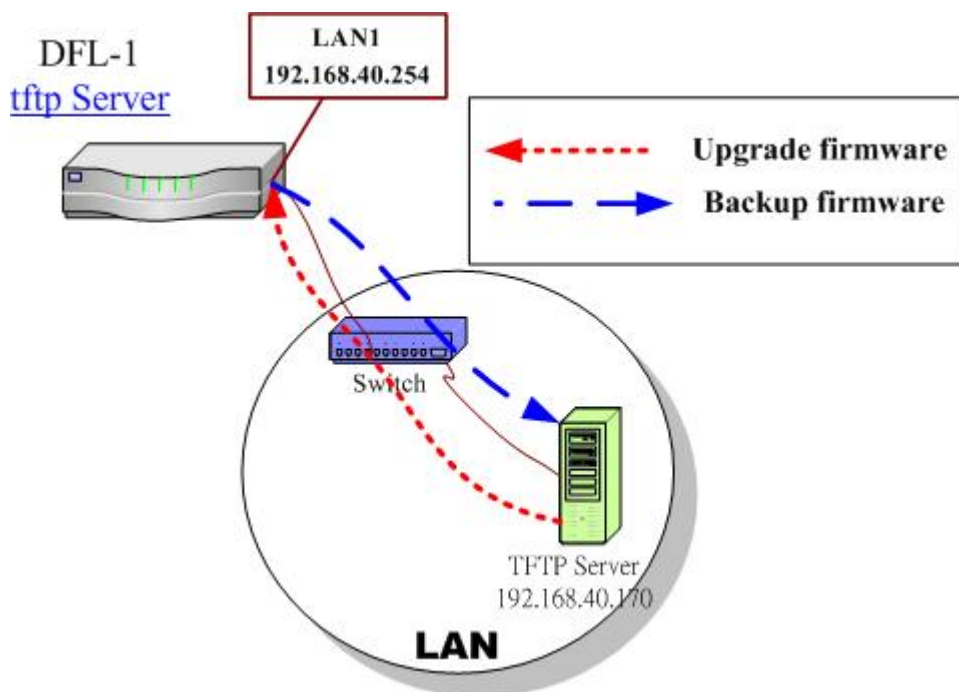


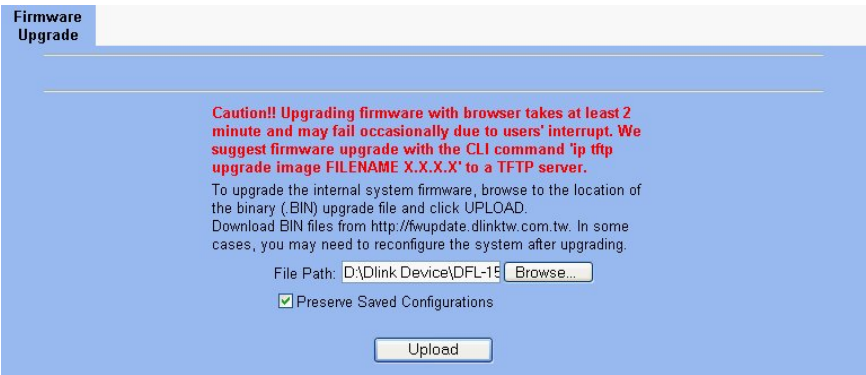
Figure 30-1 Upgrade/Backup firmware from TFTP server

Part IX System Maintenance

| | |
|--|---|
| <p>Step 1. Setup TFTP server</p> <p>Place the TFTP server <code>TftpServer</code> in the <code>c:\</code> directory and double click to run it. Place all <code>bin</code> files in the <code>c:\</code> as well. Set the PC to be 192.168.40.x to be in the same subnet with the DFL-1500's LAN1. Login to DFL-1500's console. Enter <code>en</code> to enter privileged mode. Configure the LAN1 address so that the DFL-1500 can connect to the TFTP server. The CLI command to configure LAN1 interface is <code>ip ifconfig INTF3 192.168.40.254 255.255.255.0</code>.</p> | <pre>NetOS/i386 (DFL-1500) (tty00) login: admin Password: Welcome to DFL-1500 VPN/Firewall Router! DFL-1500> en DFL-1500# ip ifconfig INTF3 192.168.40.254 255.255.255.0 DFL-1500#</pre> |
| <p>Step 2. Upgrade firmware</p> <p>Enter <code>IP tftp upgrade image 192.168.40.x DFL-1500-<ver>.bin</code>. After this procedure, DFL-1500 device will reboot automatically.</p> <p>Notice: if you want to preserve the previous configuration, add the "preserve" keyword to the end.</p> <p>Refer Appendix A for the details.</p> | <pre>DFL-1500# ip tftp upgrade image DFL-1500-2.001-ALL.bin 192.168.40.170 preserve Fetching from 192.168.40.170 for DFL-1500-2.001-ALL.bin tftp> tftp> Verbose mode on. tftp> getting from 192.168.40.170:DFL-1500-2.001-ALL.bin to DFL-1500-2.001-ALL.bin [octet]</pre> |
| <p>Step 3. Check if OK</p> <p>Check whether the system status is working properly or not.</p> | <pre>DFL-1500> sys st ===== System Name: Firmware Version: NetOS Ver2.001 (WALL) #5: Thu Sep 23 15:26:41 CST 2004 Software Serial Number: 60623576436830003320 ===== Operation Mode: NAT/Router Default Gateway: 61.2.1.6 Primary DNS: 168.95.1.1 Secondary DNS: Default WAN Link (Gateway/DNS): WAN1 ===== Port Interface IP Address Netmask Status Type ----- 1 WAN1 61.2.1.1 255.255.255.248 DOWN (Static IP) 2 WAN2 DOWN (Not initialized) 3 DMZ1 10.1.1.254 255.255.255.0 DOWN 4 LAN1 192.168.40.254 255.255.255.0 DOWN 5 LAN2 192.168.2.254 255.255.255.0 UP ===== 1:18PM up 19:57, 0 users, load averages: 1.11, 1.11, 1.08 DFL-1500></pre> |

30.3 Firmware upgrade from Web GUI

| | |
|--|--|
| <p>Step 1. Download the newest firmware from web site</p> <p>If a new firmware issued, we can download it from the web site (fwupdate.dlinktw.com.tw) to the local computer.</p> | <p>Firmware upgrade site : http://fwupdate.dlinktw.com.tw/</p> |
|--|--|

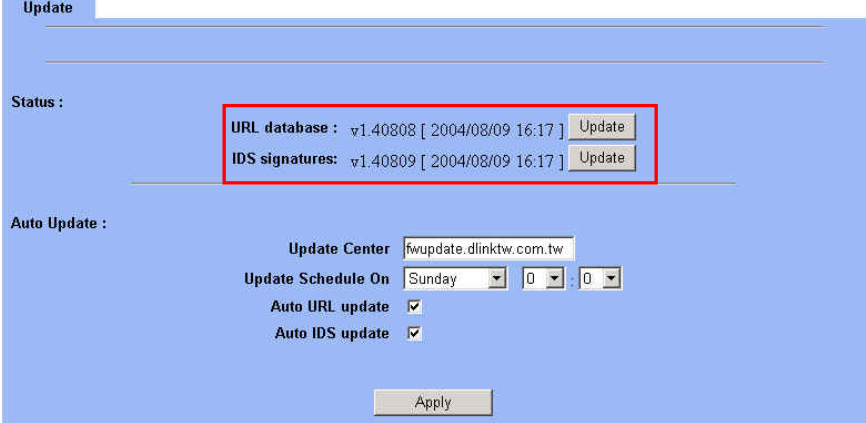
| | |
|--|---|
| <p>Step 2. Upgrade firmware</p> <p>In the System Tools / Firmware Upgrade page. Select the path of firmware through Browse button, and check the Preserve Saved Configurations to reserve original settings. Click the Upload button to upgrade firmware.</p> | <p>SYSTEM TOOLS > Firmware Upgrade > Firmware Upgrade</p>  |
|--|---|

What will it happen, if there is an accident during the process as the following list while upgrading firmware?

| Accident | What will it happen? |
|---------------------------------------|---|
| The network line is broken. | The process of the new firmware upgrade will fail. After rebooting the DFL-1500, it will remain the original firmware and configuration. No firmware is upgraded. |
| The DFL-1500 powered off or rebooted. | Generally, after rebooting the DFL-1500, it will remain the original firmware and configuration. But, sometimes the DFL-1500 may fail to remain the original firmware and reboot correctly. In this circumstance, you should use the rescue mode to do the factory reset. For the details, please refer section 30.5.3. |

Table 30-1 The result while an accident happens during the firmware upgrade.

30.4 Database Update from Web GUI

| | |
|---|--|
| <p>Step 1. Update database manually</p> <p>If a new firmware issued, we can download it by clicking the Update button. Then we will see the database version shown on the left side.</p> |  |
|---|--|

Step 2. Auto Update

We can also update database automatically. Fill the database server in the Update Center field. Choose what date/time we would like to update the database, and then check which databases we would like to update. Click Apply button to finish the settings.

SYSTEM TOOLS > Firmware Upgrade > Firmware Upgrade

Update

Status :

URL database : v1.40808 [2004/08/09 16:17] Update

IDS signatures: v1.40809 [2004/08/09 16:17] Update

Auto Update :

Update Center fwupdate.dlinktw.com.tw

Update Schedule On Sunday 0 0

Auto URL update

Auto IDS update

Apply

30.5 Factory Reset

30.5.1 Factory reset under web GUI

Step 1. Factory reset

In the Web GUI mode. Follow the path of right side. We can make DFL-1500 configuration restored to the factory defaults with simply clicking the Apply button.

Warning: Be careful to use this function. It will clear all current configurations. And the configuration will be back to the factory default.

SYSTEM TOOLS > System Utilities > Factory Reset

Save Configuration Backup Configuration Restore Configuration Factory Reset

Back to Factory Defaults

Reset to clear all user-entered configuration information and return the system to its factory defaults. After resetting, the

- Password will be admin
- WAN1 will not be initialized
- WAN2 will not be initialized
- DMZ1 IP will be 10.1.1.254
- LAN1 IP will be 192.168.1.254
- LAN2 IP will be 192.168.2.254
- DHCP will be reset to server

To erase the router's configuration information and restore factory default settings, system will be rebooted automatically

Apply

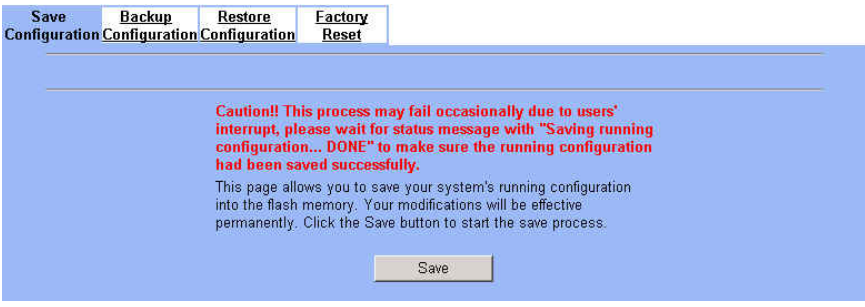
30.5.2 NORMAL factory reset

| | |
|---|--|
| <p>Step 1. Factory reset</p> <p>In the CLI mode. Enter <code>sys resetconf</code> now to reset the firmware to factory default. Then the system will reboot automatically.</p> | <pre>NetOS/i386 (DFL-1500) (tty00) login: admin Password: Welcome to DFL-1500 VPN/Firewall Router DFL-1500> en DFL-1500# sys resetconf now Resetting Configuration to default... DONE System will reboot now syncing disks... done rebooting...</pre> |
|---|--|


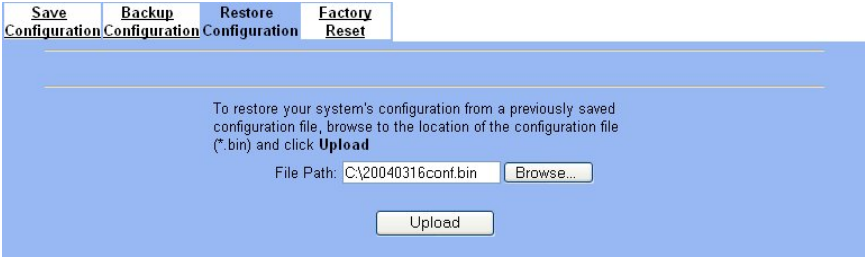
30.5.3 EMERGENT factory reset

| | |
|---|--|
| <p>Step 1. Enter the boot loader</p> <p>If the original firmware is damaged, you may need to recover the firmware with the factory default. Press <tab> or <space> during the 2-second countdown process.</p> | <pre>>> NetOS Loader (i386), V1.5 (Fri Feb 20 10:25:11 CST 2004) Press <TAB> to prompt - starting in 0 Type "boot rescue" to load safe-mode kernel to (1) rescue corrupted firmware (2) reset password for admin type "?" or "help" for help. ></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>fttp</code> to fetch another firmware to install, or reset the configuration to default even though you lost the password.</p> | <pre>> boot rescue 651354+7888404+127584=0x84528c NetOS Ver1.529 (RESCUE) #1: Wed Apr 7 00:54:55 CST 2004 cpu0: Intel (null) Celeron (686-class), 1202.85 MHz total memory = 255 MB avail memory = 228 MB Ethernet address 00:90:0b:02:eb:ac, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:ad, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:ae, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:af, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:b0, 10/100 Mb/s wd0: drive supports PIO mode 4 Software Serial Number: I60623576436828722320I Tips: Type "?" anytime when you need helps. Tips: To recover from corrupted fi rmware, setup IP address and use ftftp to install the new firmware. DFL-1500> _</pre> |
| <p>Step 3. Factory reset</p> <p>Enter <code>sys resetconf</code> now to reset the firmware to factory default. Then system will reboot automatically.</p> | <pre>DFL-1500> en DFL-1500# sys resetconf now System will reboot now syncing disks... done rebooting...</pre> |

30.6 Save the current configuration

| | |
|---|---|
| <p>Step 1. Backup the current configuration</p> <p>After finishing the settings of DFL-1500, be sure to Press the Save button in this page to keep the running configuration.</p> | <p>SYSTEM TOOLS > System Utilities > Save Configuration</p>  |
|---|---|

30.7 Backup / Restore Configurations

| | |
|--|--|
| <p>Step 1. Backup the current configuration</p> <p>Before backup your current configuration, make sure you have saved your current configurations as described in Section 30.6. Then select page in the page of / System Tools / System Utilities / Backup Configurations, 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 page of System Tools / System Utilities / Restore Configuration, click the Browse button to select configuration file path first, and then click Upload button to restore configuration.</p> | <p>SYSTEM TOOLS > System Utilities > Restore Configuration</p>  |

What will it happen if there is an accident during the process as the following list while restoring configuration?

| Accident | What will it happen? |
|---------------------------------------|---|
| The network line is broken. | The configuration restoring will fail. After rebooting the DFL-1500, it will remain the original configuration. No configuration is restored. |
| The DFL-1500 powered off or rebooted. | The configuration restoring will fail. After rebooting the DFL-1500, it will remain the original configuration. No configuration is restored. |

Table 30-2 The result while an accident happens during the configuration restoring.

30.8 Reset password

| | |
|---|---|
| <p>Step 1. Enter the boot loader</p> <p>If you forget the password, you can use the following way to reset the password. Press <tab> or <space> during the 2-second countdown process.</p> | <pre>>> NetOS Loader (i386), V1.5 (Fri Feb 20 10:25:11 CST 2004) Press <TAB> to prompt - starting in 0 Type "boot rescue" to load safe-mode kernel to (1) rescue corrupted firmware (2) reset password for admin type "?" or "help" for help. ></pre> |
| <p>Step 2. Get the Initial Key</p> <p>Enter <code>boot -I</code> command as right side. When screen shows "Enter Initial Key", you can consult with your local technical supporter to get the Initial Key. You will need to tell the local technical supporter all the MAC address value. Then you will get the Initial Key. To reset admin password.</p> | <pre>> boot -I 998681+10753736+329772 [74+85936+645241=0xbaba08 NetOS Ver1.529 (DLINK) #0: Wed Apr 7 00:38:02 CST 2004 cpu0: Intel (null) Celeron (686-class), 1202.84 MHz total memory = 255 MB avail memory = 224 MB Ethernet address 00:90:0b:02:eb:ac, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:ad, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:ae, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:af, 10/100 Mb/s Ethernet address 00:90:0b:02:eb:b0, 10/100 Mb/s wd0: drive supports PIO mode 4 IPSec: Initialized Security Association Processing. Enter Initial Key:</pre> |

Appendix


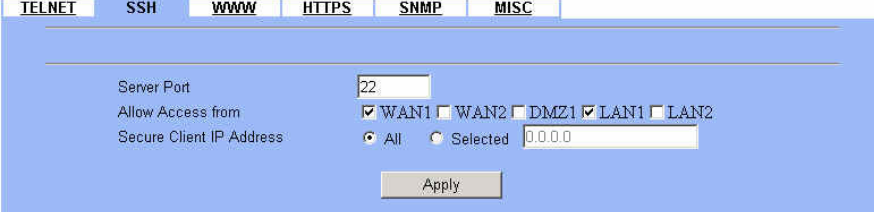
Appendix A

Command Line Interface (CLI)

You can configure the DFL-1500 through the web interface (http/https) for the most time. Besides you can use another method, console/ssh/telnet method to configure the DFL-1500 in the emergency. This is known as the Command Line Interface (CLI). By the way of CLI commands, you can effectively set the IP addresses, restore factory reset, reboot/shutdown system etc. Here we will give you a complete list to configure the DFL-1500 using the CLI commands.

A.1 Enable the port of DFL-1500

If you prefer to use CLI commands, you can use it through console/ssh/telnet methods. For using ssh/telnet feature, you must enable the remote management first. Enable the specified port, so that you can login from the configured port.

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

A.2 CLI commands list (Normal Mode)

Subsequently, we can use the console/ssh/telnet to connect the DFL-1500. After logging the system successfully, we can use the CLI commands to configure DFL-1500. The complete CLI commands are described as follows.

Non-privileged mode

| Main commands | Sub commands | Example | Command description |
|---------------|--------------|-------------------------|--|
| ? | | ? | Show the help menu |
| enable (en) | | enable | Turn on privileged mode command |
| exit (ex) | | exit | Exit command shell |
| ip | | | Configure IP related settings |
| | ping | ip ping 202.11.22.33 | Send ICMP echo request messages |
| | tracert | ip tracert 202.11.22.33 | Trace route to destination address or hostname |
| sys | | | Configure system parameters |

| | | | |
|--|---------------|-------------|--------------------------------|
| | status (st) | sys status | Show system and network status |
| | version (ver) | sys version | Show DFL-1500 firmware version |

Table A-1 Non-privileged mode of normal mode

Note: If you don't know what parameter is followed by the commands, just type "?" following the command. Ex "ip ?". It will show all the valid suffix parameters from "ip".

Privileged mode

| Main commands | Sub commands | Example | Command description |
|----------------------|------------------------|--|---|
| ? | | ? | Show the help menu |
| disable (dis) | | disable | Turn off privileged mode command |
| exit (ex) | | exit | Exit command shell |
| ip | | | Configure IP related settings |
| | arp | ip arp status | Show the ip/MAC mapping table |
| | dns | ip dns query www.yam.com.tw | Show the IP address of the www.yam.com.tw. |
| | ifconfig | ip ifconfig INTF1 192.168.1.100 255.255.255.0 | Configure the ip address of each port |
| | ping | ip ping 202.11.22.33 | Send ICMP echo request messages |
| | tftp upgrade/backup | ip tftp upgrade image <FILENAME> 192.168.1.170. | Upgrade/Backup firmware/configuration from/to tftp server. About the full description, please refer to Section A-3. |
| | traceroute | ip traceroute 202.11.22.33 | Trace route to destination address or hostname. |
| sys | | | Configure system parameters |
| | halt | sys halt now | Shutdown system |
| | password | sys password | Change administrator password |
| | reboot | sys reboot now | Reboot system |
| | resetconf | sys resetconf now | Reset system configuration to default settings |
| | saveconf (sa) | sys saveconf | Save running configuration |
| | status (st) | sys status | Show system and network status |
| | tcpdump (tc) | sys tcpdump INTF0 host 10.1.1.1 | Capture the information of specified packets which pass through the indicated interface. |
| | version (ver) | sys version | Show DFL-1500 firmware version |

Table A-2 Privileged mode of normal mode

The Full tftp commands are described in the following Table A-3.

| Prefix command | 2th command | 3th command | Postfix command | Example | Command description |
|----------------|-------------|-------------|-----------------------------|---|---|
| ip tftp | upgrade | config | FILENAME WORD | ip tftp upgrade config conf-0101 192.168.1.170 | Upgrade configuration file image from tftp server. |
| | | image | FILENAME WORD (preserve) | ip tftp upgrade image <FILENAME> 192.168.1.170 preserve | Upgrade system image from tftp server. |
| | backup | config | WORD | ip tftp backup config 192.168.1.170 | Backup configuration file image to tftp server. |
| | | image | WORD | ip tftp backup image 192.168.1.170 | Backup system image to tftp server. |

Table A-3 ip tftp commands description

In the Postfix command, the meanings of keywords are listed here.

WORD: tftp server IP address

FILENAME: Upgrade configuration file image name

(preserve): string “preserve”, this is optional

A.3 CLI commands list (Rescue Mode)

If the original firmware was damaged by some accidents, you may need to recover it with the factory reset process in the rescue mode. Boot the DFL-1500 and press <tab> or <space> during the 2-second countdown process. You may refer Section 30.5.3 for details.

Non-privileged mode

| Main commands | Sub commands | Example | Command description |
|--------------------|---------------|----------------------|--|
| ? | | ? | Show the help menu |
| enable (en) | | enable | Turn on privileged mode command |
| exit (ex) | | exit | Exit command shell |
| ip | | | Configure IP related settings |
| | ping | ip ping 202.11.22.33 | Send ICMP messages |
| sys | | | Configure system parameters |
| | status (st) | sys status | Show the mode name and firmware version. |
| | version (ver) | sys version | Show the firmware version |

Table A-4 Non-privileged mode of rescue mode

Note: If you don't know what parameter is followed by the commands, just type “?” following the command. Ex “ip?”. It will show all the valid suffix parameters from “ip”.

Privileged mode

| Main commands | Sub commands | Example | Command description |
|----------------------|---------------|--|--|
| ? | | ? | Show the help menu |
| disable (dis) | | disable | Turn off privileged mode command |
| exit (ex) | | exit | Exit command shell |
| ip | | | Configure IP related settings |
| | arp | ip arp status | Show the ip/MAC mapping table |
| | dns | ip dns query www.yam.com.tw | Show the IP address of the www.yam.com.tw. |
| | ifconfig | ip ifconfig INTF1 192.168.1.100 255.255.255.0 | Configure the ip address of each port |
| | ping | ip ping 202.11.22.33 | Send ICMP echo request messages |
| | tftp | ip tftp upgrade image <FILENAME> 192.168.1.170. | Upgrade firmware from tftp server. |
| sys | | | Configure system parameters |
| | halt | sys halt now | Shutdown system |
| | reboot | sys reboot now | Reboot system |
| | resetconf | sys resetconf now | Reset system configuration to default settings |
| | status (st) | sys status | Show the mode name and firmware version. |
| | version (ver) | sys version | Show the firmware version |

Table A-5 Privileged mode CLI commands

Appendix B

Trouble Shooting

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

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

2. How can I configure the DFL-1500 if I forget the admin password of the DFL-1500 ?

Ans : You can gather all the MAC addresses values of DFL-1500, and contact the local technical supporter. Then we will give you an initial key. Please refer to the Section 30.8 described to reset the admin password.

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

Ans : Check the console line and make sure it is connected between your computer serial port and DFL-1500 Diagnostic RS-232 port. Notice whether the terminal software parameter setting as follows. No parity, 8 data bits, 1 stop bit, baud rate 9600 bps. The terminal type is VT100.

4. I can't ping DFL-1500 WAN1 interface successfully ? Why ?

Ans : Follow below items to check if ready or not

- a. Check Basic Setup > WAN Settings > WAN1 status fields. Verify whether any data is correctly.
 - b. Check Device Status > System Status > Network Status WAN1 status is "UP". If the status is "DOWN", check if the network line is connectionless ?
 - c. Check System Tools > Remote Mgt. > MISC > WAN1. Verify if WAN1 port checkbox is enabled. The default enabled port is only LAN port.
 - d. Check whether virtual server rule (Dest. IP : WAN1 IP address, port : 1~65535) exists or not. If existing any virtual server rule like this type, it will make all the connections from WAN1 port outside relay to another server. Actually what you have pinged is another server, not DFL-1500.
 - e. Check whether NAT One-to-One(bidirectional) rule (Translated Src IP : WAN1 IP address, port : 1~65535) exists or not. If existing any virtual server rule like this type, it will make all the connections from WAN1 port outside relay to another server. Actually what you have pinged is another server, not DFL-1500.
 - f. If all the above items have checked, try to change a new network line. This is almost resulting from the network line problem. Please neglect the LED status, because it will confuse your judgment sometimes.
5. I have already set the WAN1 ip address of DFL-1500 the same subnet with my pc, but I can't use https to login DFL-1500 via WAN1 port from my pc all the time, why ?

Ans :

- a. Be sure that you can ping the WAN1 port, please check the procedure as question 4 description.
 - b. Make sure that the WAN1 IP address of DFL-1500 is not duplicated with other existent IP address. You can take off the network line connected on the WAN1 port. Then try to ping the IP address which setup on the WAN1 port. If it is still successful, the IP address which setup on the WAN1 port is duplicated with the existent IP address.
 - c. Notice that you must check System Tools > Remote Mgt. > HTTPS > WAN1. The default enabled port is only LAN port.
6. I can't build the VPN – IPSec connection with another device at the another side all the time, why ?

Ans : Please make sure if you follow the setting method as follows.

- a. Check your IPSec Setting. Please refer to the settings in the Section 13.4- Step 3.
- b. Make sure if you have already added a WAN to LAN policy in the Advanced Settings/Firewall to let the IPSec packets pass through the DFL-1500. (The default value from WAN to LAN is block.).

When you add a Firewall rule, the Source IP and Netmask are the IP address , PrefixLen/Subnet Mask in the pages of the Remote Address Type. And the Dest IP and Netmask are the IP Address , PrefixLen/Subnet Mask in the pages of the Local Address Type.

The following Figure B-1, Figure B-2 indicated the DFL_A IPSec and Firewall setting. The Figure B-3, Figure B-4 indicated the opposite side DFL_B IPSec and Firewall setting. When you configure an IPSec policy, please be sure to add a rule to let the packets of the IPSec pass from WAN to LAN. For the IP address of firewall rules, please refer to the Figure B-2, Figure B-4.

IPSec **PPTP** **L2TP** **Pass Through**

IPSec->IKE->Edit Rule

Status
 Active
 IKE Rule Name: IKEruleA

Condition
 Local Address Type: Subnet Address
 IP Address: 192.168.40.0
 PrefixLen / Subnet Mask: 255.255.255.0
 Remote Address Type: Subnet Address
 IP Address: 192.168.88.0
 PrefixLen / Subnet Mask: 255.255.255.0

The Local Address of DFL B

Figure B-1 DFL_A - Inset a new IPSec policy

Firewall->Edit Rules->Edit

Edit WAN1-to-LAN1 Firewall rule number 1

Status
 Rule name: AllowIPSecPktA
 Schedule: Always

Condition
 Source IP: WAN1_VPNA
 Dest. IP: LAN1_VPNA
 Service: ANY

Action
 Forward and do not log the matched session
 Forward bandwidth class: def_class
 Reverse bandwidth class: def_class

Back Apply

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

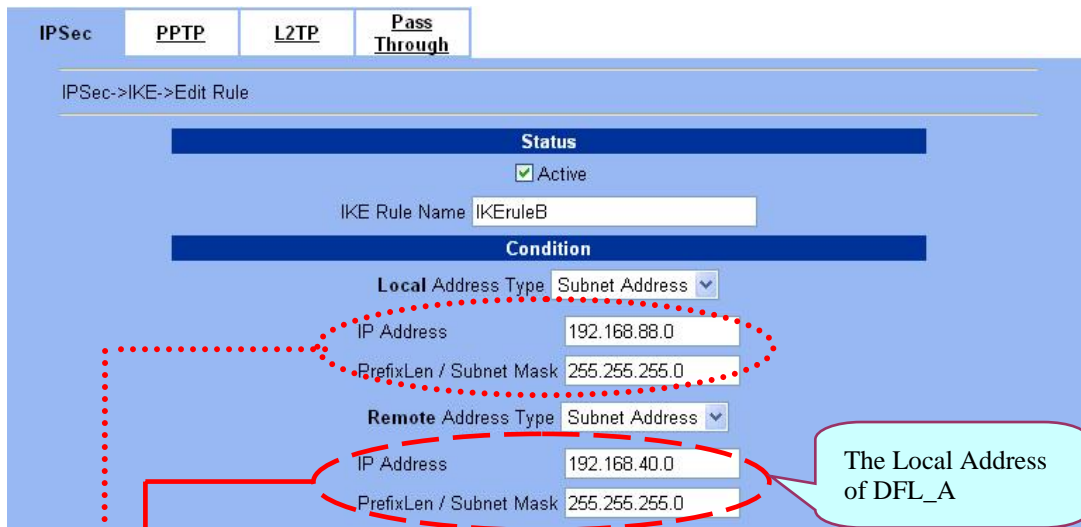


Figure B-3 DFL_B - Inset a new IPsec policy

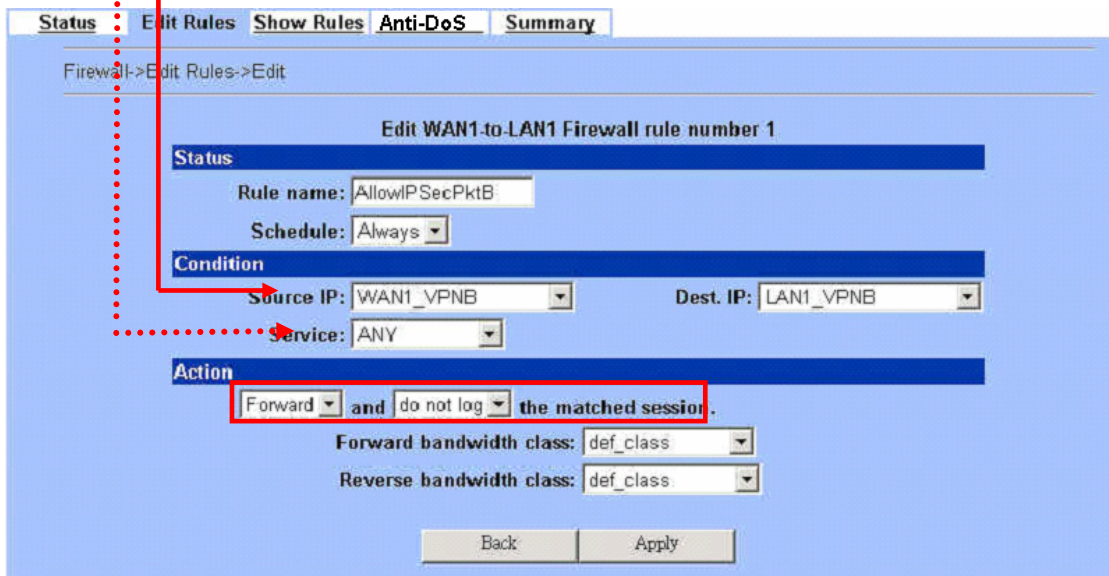


Figure B-4 DFL_B - Insert a new firewall rule in WAN to LAN

7. Why the Source-IP field of System Logs is blank?

Ans : One reason is that you may enter Host Name and following by a space like “DFL-1500 “. And enter the Domain Name string like “dlink.com” in the firmware version 1.391B. Then the System Name will present as “DFL-1500 .dlink.com”. After upgrading firmware to upper version (ex. 1.50R). It will appear blank in the Source-IP field of System Logs.

8. When I ping the internet host from LAN/DMZ. I can't always finish the ping successfully. Sometimes it is work. But sometimes it fails to ping the outside host.

Ans : This may cause there are more than one host in the LAN/DMZ pinging the same host at the same time. If one host (Lan-A) is pinging internet host A(ex. 140.106.100.1), and at the same time, Lan-B is also pinging 140.106.100.1. Then the pinging action of the Lan-A and Lan-B may fail. But when each host (Lan-A or Lan-B) is finish pinging, the other host can continue the pinging action.

9. While I am upgrading firmware from local disk, the download is not complete but the network has been disconnected. What will it happen in such situation?

Ans : Under this circumstance, the DFL-1500 will automatically reboot and all configurations will still remain as before.

10. While I am upgrading firmware from local disk, the download is complete. After md5 checks, the screen appears “Upgrading kernel image”. What will it happen if the power is off suddenly?

Ans : Almost all the cases will not cause firmware fail. The DFL-1500 will automatically reboot and all configurations will still remain as before. But sometimes it will make firmware fail. If the firmware fails, DFL-1500 will automatically enter rescue mode when it reboots. You may need to do the factory reset, and then restore your original configuration to DFL-1500. Refer to the factory reset procedure of DFL-1500 as Section 30.5. About restoring configuration procedure, please refer to Section 30.7.

11. While finishing the Content Filters > Web Filter settings, if I try to use browser to test, why does not the web page result match with the web filter configuration?

Ans : Be sure that you have cleaned all the file cache in the browser, and try to connect the internet web server. If the web page result still does not match with the web filter configuration, you may close your browser and reopen it.

12. While finishing the edition of DFL-1500 settings and pressing apply button, the LAN/DMZ to WAN network connection (telnet, ssh, ftp, msn..) fails, why?

Ans : This is a normal situation. When you finish the following settings, all the active network connection will be disconnected. So, you must reconnect it again.

- a. SYSTEM TOOLS > Remote Mgt.
- b. ADVANCED SETTINGS > VPN Settings > IPSec
- c. ADVANCED SETTINGS > VPN Settings > PPTP > Client
- d. ADVANCED SETTINGS > VPN Settings > Pass Through
- e. ADVANCED SETTINGS > NAT

Appendix C

Rule entry limitation

For the DFL-1500 web configuration, there is a limitation of permitted maximum entering rule. Here we provide a list for your reference.

| Classification | Item | Permitted Maximum rule entry | Refer section |
|------------------|---|------------------------------|----------------|
| Basic Setup | IP alias records of WAN port | 60 | Section 3.4.3 |
| | IP alias records of DMZ port | 10 | Section 3.4.3 |
| | IP alias records of LAN port | 10 | Section 3.4.3 |
| Authentication | Local type of authentication, account entries | 2000 | Section 6.3.1 |
| | Authentication exempt host entries | unlimited | Section 6.3.6 |
| NAT | NAT rule entries | 200 | Section 7.4.1 |
| Virtual Server | Virtual Server rule entries | 200 | Section 7.4.2 |
| Routing | static routing entries | 30 | Section 8.4.1 |
| | policy routing entries | 200 | Section 8.4.2 |
| Grouping | address object | 1000 | Section 9.4.1 |
| | address group | 1000 | Section 9.4.1 |
| | service object | 1000 | Section 9.4.2 |
| | service group | 1000 | Section 9.4.2 |
| | schedule object | 256 | Section 9.4.3 |
| | schedule group | 256 | Section 9.4.3 |
| Firewall | Firewall rule entries | 3000 | Section 10.4.1 |
| IP/MAC binding | IP/MAC binding rule entries | 1000 | Section 11.4 |
| VPN | IPSec IKE rule entries | 2000 | Section 13.4.1 |
| | IPSec Manual-Key rule entries | 2000 | Section 13.4.2 |
| | IPSec Hub entries | 100 | Section 15.4 |
| | IPSec Spoke entries | 100 | Section 15.4 |
| Web filter | Web filter exempt zone entries | 256 | Section 21.4 |
| | Customize trusted domain entries | 256 | Section 21.4 |
| | Customize Forbidden domain entries | 256 | Section 21.4 |
| | URL filter keyword entries | 256 | Section 21.4 |
| | Content keyword entries | 256 | Section 21.4 |
| SMTP/POP3 filter | SMTP blocking list entries | 256 | Section 22.4.1 |
| | SMTP exempt zone entries | 256 | Section 22.4.1 |
| | POP3 blocking list entries | 256 | Section 22.4.2 |

| | | | |
|----------------------|-------------------------------------|-----|----------------|
| | POP3 exempt zone entries | 256 | Section 22.4.2 |
| FTP filter | FTP blocking list entries | 40 | Section 23.4 |
| | FTP exempt zone entries | 20 | Section 23.4 |
| Bandwidth Management | Bandwidth Management Action entries | 200 | Section 26.4 |
| Log | System Access Logs | 256 | Section 29.4.1 |
| | Firewall Logs | 256 | Section 10.4.1 |
| | Anti-DoS Logs | 256 | N/A |
| | IDS Logs | 256 | Section 24.4 |
| | Web Filter Logs | 256 | N/A |
| | Mail Filter Logs | 256 | N/A |
| | POP3 Filter Logs | 256 | N/A |
| | IPSec Logs – IKE | 256 | N/A |
| | IPSec Logs – Manual Key | 256 | N/A |
| | PPTP Logs – Server | 256 | N/A |
| | PPTP Logs – Client | 256 | N/A |
| | L2TP Logs | 256 | N/A |

Table C-1 Rule entries limitation

Appendix D

System Log Syntax

In the DFL-1500, all the administration action will be logged by the system. You can refer all your management process through System log (DEVICE STATUS > System Logs > System Access Logs). Besides, all the system log descriptions are following the same syntax format.

In the below diagram, you can view the example of system log. The amplified system log example can be divided into 4 parts. The first part is **Component type**, second part is **Log ID**, third part is **log description** and final part is **Event ID**. When you applied each setting in the DFL-1500, you had been issued an Event. So the same Event ID may have many different Log IDs because you may change different settings in the same apply action. The Event ID is a sequence number. It means that the same Log ID would not be assigned the same Event ID every time.

So if you apply any button while setting DFL-1500 every time, an “Event” will occur immediately. And the “Event” will be displayed in the System log.

The screenshot shows the 'System Access Logs' interface. A table lists log entries with columns for No., Time, Source-IP, and Access-Info. The entry at row 8 is highlighted with a red box: '8 2004-05-14 11:08:47 192.168.17.170 ROUTING : [R3] LAN1: Routing Protocol: None. EventID:247'. Below the table, a green box contains the breakdown of this log entry: 'ROUTING : [R3] LAN1: Routing Protocol: None. EventID:247' and 'Component type : Log ID : Log description : Event ID'.

Figure D-1 All the system log descriptions are following the same format as above

In the following table, we list all the system logs for reference.

| Component type | Log ID | Log description | Example |
|----------------|--------|-----------------|---|
| AUTH | A01 | User Login | AUTH: [A01] admin login success (192.168.17.102:443). |
| | | | AUTH: [A01] admin login fail, miss password (192.168.17.102:443). |
| | | | AUTH: [A01] admin login fail, configuration is locked by administrator from Console (192.168.17.102:443). |
| | | | AUTH: [A01] admin login fail, configuration is locked by another user from 192.168.17.100 (192.168.17.102:443). |
| | A02 | User Logout | AUTH: [A02] admin logout (192.168.17.102:443). |

Appendix D

| | | | |
|-----------|-----|---|---|
| | A03 | Change Password | AUTH: [A03] admin change system password (192.168.17.100:443). |
| BANDWIDTH | B01 | Enable/Disable Bandwidth Management | BANDWIDTH: [B01] Enable bandwidth management by admin (192.168.17.100:443). |
| | | | BANDWIDTH: [B01] Disable bandwidth management by admin (192.168.17.100:443). |
| CONTENT | C01 | Web filter categories configuration updated | CONTENT: [C01] Web filter categories configuration update by admin (192.168.17.100:443). EID=6 |
| | C02 | Web filter added trusted host | CONTENT: [C02] Web filter add trusted host by admin (192.168.17.100:443). EID=6 |
| | C03 | Web filter deleted trust host | CONTENT: [C03] Web filter deleted trust host by admin (192.168.17.100:443). EID=6 |
| | C04 | Web filter added forbidden domain | CONTENT: [C04] Web filter added forbidden domain by admin (192.168.17.100:443). EID=7 |
| | C05 | Web filter deleted forbidden domain | CONTENT: [C05] Web filter deleted forbidden domain by admin (192.168.17.100:443). EID=8 |
| | C06 | Enable web-filter access control | CONTENT: [C06] Enable web-filter access control by admin (192.168.17.100:443). EID=9 |
| | C07 | Disable web-filter access control | CONTENT: [C07] Disable web-filter access control by admin (192.168.17.100:443). EID=10 |
| | C08 | Web filter URL keyword added | CONTENT: [C08] Web filter URL keyword added by admin (192.168.17.100:443). EID=11 |
| | C09 | Web filter URL keyword deleted | CONTENT: [C09] Web filter URL keyword deleted by admin (192.168.17.100:443). EID=12 |
| | C10 | Enable web filter url matching | CONTENT: [C10] Enable web filter url matching by admin (192.168.17.100:443). EID=13 |
| | C11 | Disable web filter url matching | CONTENT: [C11] Disable web filter url matching by admin (192.168.17.100:443). EID=14 |
| | C12 | Updated web filter exempt zone configuration | CONTENT: [C12] Updated web filter exempt zone configuration by admin (192.168.17.100:443). EID=15 |
| | C13 | Web filter exempt zone added range | CONTENT: [C13] web filter exempt zone added range from 140.126.1.1 to 140.126.100.255 by admin (192.168.17.100:443). EID=16 |
| | C14 | Updated ftp filter exempt zone configuration | CONTENT: [C14] Updated ftp filter exempt zone configuration by admin (192.168.17.100:443). EID=17 |
| | C15 | FTP filter exempt zone added range | CONTENT: [C15] FTP filter exempt zone added range from 140.126.1.1 to 140.126.255.255 by admin (192.168.17.100:443). EID=18 |
| | C16 | Updated ftp filter blocked file configuration | CONTENT: [C16] Updated ftp filter blocked file configuration by admin (192.168.17.100:443). EID=19 |
| | C17 | FTP Filter blocking list updated | CONTENT: [C17] FTP Filter blocking list updated by admin (192.168.17.100:443). EID=20 |
| | C18 | Web filter keyword added | CONTENT: [C18] Web filter keyword added by admin (192.168.17.100:443). EID=21 |

| | | | |
|----------|-----|---|---|
| | C19 | Web filter keyword deleted | CONTENT: [C19] Web filter keyword deleted by admin (192.168.17.100:443). EID=22 |
| | C20 | Enable web filter keyword matching | CONTENT: [C20] Enable web filter keyword matching by admin (192.168.17.100:443). EID=23 |
| | C21 | Disable web filter keyword matching | CONTENT: [C21] Disable web filter keyword matching by admin (192.168.17.100:443). EID=24 |
| | C22 | Updated POP3 filter exempt zone configuration | CONTENT: [C22] Updated POP3 filter exempt zone configuration by admin (192.168.17.100:443). EID=25 |
| | C23 | POP3 filter exempt zone added range | CONTENT: [C23] POP3 filter exempt zone added range from 140.126.1.1 to 140.126.1.255 by admin (192.168.17.100:443). EID=26 |
| | C24 | Enable POP3 filter | CONTENT: [C24] Enable POP3 filter by admin (192.168.17.100:443). EID=27 |
| | C25 | Disable POP3 filter | CONTENT: [C25] Disable POP3 filter by admin (192.168.17.100:443). EID=28 |
| | C26 | POP3 Filter blocking list updated | CONTENT: [C26] POP3 Filter blocking list updated by admin (192.168.17.100:443). EID=29 |
| | C27 | Updated SMTP exempt zone configuration | CONTENT: [C27] Updated SMTP exempt zone configuration by admin (192.168.17.100:443). EID=30 |
| | C28 | SMTP filter exempt zone added range from | CONTENT: [C28] SMTP filter exempt zone added range from by admin (192.168.17.100:443). EID=31 |
| | C29 | Enable SMTP filter | CONTENT: [C29] Enable SMTP filter by admin (192.168.17.100:443). EID=32 |
| | C30 | Disable SMTP filter | CONTENT: [C30] Disable SMTP filter by admin (192.168.17.100:443). EID=33 |
| | C31 | SMTP Filter blocking list updated | CONTENT: [C31] SMTP Filter blocking list updated by admin (192.168.17.100:443). EID=34 |
| | C36 | Enable WEB filter | CONTENT: [C36] Enable WEB filter by admin (192.168.17.100:443). EID=39 |
| | C37 | Disable WEB filter | CONTENT: [C37] Disable WEB filter by admin (192.168.17.100:443). EID=40 |
| FIREWALL | F01 | Enable/Disable Firewall | FIREWALL: [F01] Activated firewall by admin (192.168.17.102:443). FIREWALL: [F01] Deactivated firewall by admin (192.168.17.102:443). |
| | F02 | Edit Firewall Rules | |
| | F03 | Anti-DoS Setup | FIREWALL: [F03] Enable Anti-DoS when attack detected by admin (192.168.17.102:443). FIREWALL: [F03] Disable Anti-DoS when attack detected by admin (192.168.17.102:443). |
| | F04 | Reload Firewall Rules | FIREWALL: [F04] WAN1 Reload all NAT/Firewall rules for new WAN IP |
| LOG | L01 | Logfile is Full | LOG: [L01] logfile is full. |
| | L02 | Mail Log | LOG: [L02] mail logfile to tom@hotmail.com. |
| | L03 | Remote Syslog Server offline | |

Appendix D

| | | | |
|------------------------|-----|--|---|
| | L04 | Enable/Disable Syslog Forward to Remote Syslog Server | LOG: [L04] Enable syslog server at 192.168.17.100 by admin (192.168.17.102:443). LOG: [L04] Disable syslog server by admin (192.168.17.102:443). |
| | L05 | Enable/Disable Mail Log | LOG: [L05] Enable mail logs to tom@hotmail.com by admin (192.168.17.102:443). LOG: [L05] Disable mail logs by admin (192.168.17.102:443). |
| | L06 | Send Mail Log | LOG: [L06] mail logfile to tom@hotmail.com |
| | L07 | Log Cleanup | LOG: [L07] logfile is cleanup. |
| | L08 | Mail Log Configuration Update | LOG: [L08] Mail configuration updated by admin (192.168.17.102:443). |
| | L09 | Log Half-Clean | LOG: [L09] logfile half-clean. |
| NAT | N01 | Set NAT Mode | NAT: [N01] Disable WAN NAT feature. |
| | N02 | NAT Rules | NAT: [N02] |
| | N03 | Virtual Server | |
| ROUTING | R01 | Static Route | |
| | R02 | Policy Route | |
| | R03 | Changing Routing Protocol | ROUTING: [R03] |
| | | OSPF Area ID | ROUTING: [R3] WAN1: OSPF Area ID = 15. EventID:15 |
| | | Routing Protocol: OSPF | ROUTING: [R3] WAN1: Routing Protocol: OSPF. EventID:15 |
| | | Routing Protocol: RIPv2/In+Out | ROUTING: [R3] WAN1: Routing Protocol: RIPv2/In+Out. EventID:15 |
| | | Routing Protocol: RIPv1/In+Out | ROUTING: [R3] WAN1: Routing Protocol: RIPv1/In+Out. EventID:15 |
| | | Routing Protocol: RIPv2/In | ROUTING: [R3] WAN1: Routing Protocol: RIPv2/In. EventID:15 |
| | | Routing Protocol: RIPv1/In | ROUTING: [R3] WAN1: Routing Protocol: RIPv1/In. EventID:15 |
| Routing Protocol: None | | ROUTING: [R3] WAN1: Routing Protocol: None. EventID:15 | |
| SYSTEM | S01 | Wall Startup | SYSTEM: [S01] Wall Startup. |
| | S02 | Wall Shutdown | SYSTEM: [S02] Wall Shutdown. |
| | S03 | Interface Configuration | SYSTEM: [S03] WAN1: IP Address Assignment = Get IP Automatically by admin (192.168.17.102:443). SYSTEM: [S03] WAN1: IP Address Assignment = Fixed IP Address by admin (192.168.17.102:443). SYSTEM: [S03] WAN1: Got PPPoE IP Address F63/255.255.255.0. |
| | S04 | Startup/Shutdown DHCP Server | SYSTEM: [S04] Enable DHCP server on LAN1 by admin (192.168.17.102:443) SYSTEM: [S04] Disable DHCP server on LAN1. |
| | S05 | Startup/Shutdown HTTP Server | SYSTEM: [S05] HTTP started. SYSTEM: [S05] HTTP stopped. |

| | | |
|-----|---|--|
| S06 | Startup/Shutdown HTTPS Server | SYSTEM: [S06] HTTPS started. |
| S07 | Startup TELNET Server | |
| S08 | Set Interface IP Address | SYSTEM: [S08] WAN1: IP Address: 192.168.17.102/255.255.255.0. (192.168.17.102:443). |
| S09 | IP Alias | SYSTEM: [S09] LAN1: Add IP address alias 192.168.1.2/255.255.255.0 by admin (192.168.17.102:443). SYSTEM: [S09] LAN1: Delete IP address alias 192.168.1.2/255.255.255.0 by admin (192.168.17.102:443). SYSTEM: [S09] LAN1: Change IP address alias 192.168.1.2/255.255.255.0 to 192.168.1.3/255.255.255.0 by admin (192.168.17.102:443). |
| S10 | Set Host Name | SYSTEM: [S10] HostName:DFL-1500, set by admin (192.168.17.102:443). |
| S11 | Set Domain Name | SYSTEM: [S11] Domain Name: dlink.com, set by admin (192.168.17.102:443). |
| S12 | Enable/Disable DDNS | SYSTEM: [S12] Enable Dynamic DNS with hostname wall.adslDNS.org on WAN1 by admin (192.168.17.102:443). SYSTEM: [S12] Disable Dynamic DNS on WAN1 by admin (192.168.17.102:443). |
| S13 | Enable/Disable DNS Proxy | SYSTEM: [S13] Enable DNS proxy by admin (192.168.17.102:443). SYSTEM: [S13] Disable DNS proxy by admin (192.168.17.102:443). |
| S14 | Enable/Disable DHCP Relay | SYSTEM: [S14] Enable DHCP relay by admin (192.168.17.102:443). SYSTEM: [S14] Disable DHCP relay by admin (192.168.17.102:443). |
| S15 | Set Date/Time | SYSTEM: [S15] System time update with NTP server tock.usno.navy.mil, set by admin (192.168.17.102:443). SYSTEM: [S15] System time update to 2003-10-10 13:33:25, set by admin (192.168.17.102:443). |
| S16 | Set System Auto Timeout Lifetime | SYSTEM: [S16] System auto timeout changed to 45 minutes by admin (192.168.17.102:443). |
| S17 | Interface PORTS Configuration (WAN/LAN/DMZ) | |
| S18 | Backup Configuration | SYSTEM: [S18] Backup configuration file by admin (192.168.17.102:443). |
| S19 | Restore Configuration | SYSTEM: [S19] Restore configuration file by admin (192.168.17.102:443). |
| S20 | Factory Reset | SYSTEM: [S20] Factory Reset to default settings by admin (192.168.17.102:443) |
| S21 | Firmware Upgrade | SYSTEM: [S21] Firmware upgraded by admin (192.168.17.102:443) |
| S22 | Setup TELNET Server | |

| | | | |
|---|-----|---------------------------------------|--|
| | S23 | Setup SSH Server | |
| | S24 | Setup WWW Server | |
| | S25 | Setup HTTPS Server | |
| | S26 | Setup SNMP Server | |
| | S27 | MISC Setup | |
| | S28 | Enable/Disable SNMP | SYSTEM: [S28] Enable SNMP by admin (192.168.17.104:443) SYSTEM: [S28] System Location: Building-A. SYSTEM: [S28] Contact Info: +886-2-28826262. SYSTEM: [S28] Disable SNMP. |
| | S29 | Configure SNMP server | |
| | S30 | File System Full | |
| | S31 | Update remote management settings. | SYSTEM: [S31] Update remote management TELNET Server settings by admin (192.168.17.102:443). |
| | S32 | Set Gateway | SYSTEM: [S32] WAN1: Gateway IP: 192.167.17.254 SYSTEM: [S32] WAN1: Got PPPoE Gateway IP 210.58.28.91. |
| | S33 | Set DNS IP Address | SYSTEM: [S33] WAN1: Clear DNS IP Address. SYSTEM: [S33] WAN1: DNS IP Address: 168.95.1.1. SYSTEM: [S33] WAN1: Get DNS Automatically. |
| | S34 | Syslog Reload | SYSTEM: [S34] Syslogd stop. SYSTEM: [S34] Syslogd start. SYSTEM: [S34] Syslogd restart. |
| | S35 | Enable/Disable Ipmon | SYSTEM: [S35] Enable Ipmon. SYSTEM: [S35] Disable Ipmon. |
| | S36 | System Checksum Update | |
| | S37 | Disable Multicast Update Multicast | SYSTEM: [S37] Disable Multicast on interface WAN1 |
| SYSTEM: [S37] Update Multicast on interface WAN1 to xxx | | | |
| SYSTEM: [S37] Update Multicast on interface WAN1 to xxx | | | |
| | S38 | Update WAN NAT settings | SYSTEM: [S38] Update WAN NAT settings to FULL feature |
| | | Update WAN NAT settings | SYSTEM: [S38] Update WAN NAT settings to Basic operation |
| | | Disable WAN NAT feature | SYSTEM: [S38] Disable WAN NAT feature |
| VPN | V1 | Update pass-through settings | VPN: [V1] Update pass-through settings |
| | V2 | Deactivated IPSec | VPN: [V2] Deactivated IPSec |
| | | Activated IPSec | |

Table D-2 All the System Log descriptions

Appendix E

Glossary of Terms

CF (Content Filter) –

A content filter is one or more pieces of software that work together to prevent users from viewing material found on the Internet. This process has two components.

DHCP (Dynamic Host Configuration Protocol) –

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on BOOTP, adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents, and DHCP participants can interoperate with BOOTP participants.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts.

DMZ (Demilitarized Zone) –

From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.

Firewall –

A device that protects and controls the connection of one network to another, for traffic both entering and leaving. Firewalls are used by companies that want to protect any network-connected server from damage (intentional or otherwise) by those who log in to it. This could be a dedicated computer equipped with security measures or it could be a software-based protection.

IPSec (IP Security) –

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers").

L2TP (Layer 2 Tunneling Protocol) –

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet Service Provider (ISP) to enable the operation of a Virtual Private Network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

NAT (Network Address Translation) –

By the network address translation skill, we can transfer the internal network private address of DFL-1500 to the public address for the Internet usage. By this method, we can use a large amount of private addresses in the enterprise.

POP3 (Post Office Protocol 3) –

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail.

PPTP (Point-to-Point Tunneling Protocol) –

PPTP extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking. PPTP operates at Layer 2 of the OSI model.

OSPF (Open Shortest Path First) –

Open Shortest Path First (OSPF), is a routing protocol used to determine the correct route for packets within IP networks. It was designed by the Internet Engineering Task Force to serve as an Interior Gateway Protocol replacing RIP.

SMTP (Simple Mail Transfer Protocol) –

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol, that let the user save messages in a server mailbox and download them periodically from the server.

VPN (Virtual Private Network) –

The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technologies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.

Appendix F

Index

B

| | |
|----------------------------|------------|
| backup configuration | 236 |
| Bandwidth Management | 209, 219 |
| bidirectional | 65, 66, 71 |

C

| | |
|----------------------|-----|
| Content Filter | 181 |
| FTP Filter | 197 |
| Mail Filter | 193 |
| Web Filter | 183 |

D

| | |
|------------------|----------------|
| DDNS | 41 |
| DHCP | 17, 20, 35, 37 |
| DHCP Relay | 41 |
| DNS Proxy | 41 |

F

| | |
|------------------------|----------|
| factory reset | 234 |
| Firewall | 91 |
| firmware upgrade | 232, 233 |

I

| | |
|--------------------------------------|-----|
| IDS (Intrusion Dection System) | 203 |
|--------------------------------------|-----|

M

| | |
|----------------|-----|
| mail log | 228 |
|----------------|-----|

N

| | |
|-----------|----|
| NAT | 61 |
|-----------|----|

P

| | |
|------------|----------|
| POP3 | 193, 195 |
|------------|----------|

R

| | |
|-----------------------------|-----|
| restore configuration | 236 |
| Routing | 73 |
| policy routing | 73 |
| static routing | 73 |

S

| | |
|--------------|----------|
| SMTP | 193, 194 |
| syslog | 227, 228 |

T

| | |
|--------------------|-----|
| tftp upgrade | 231 |
|--------------------|-----|

V

| | |
|--------------------------------|-------------------------|
| Virtual Server | 22, 62, 66, 68 |
| VPN | 102 |
| AH | 104 |
| DH | 103 |
| Encapsulation | 104 |
| ESP | 104 |
| IKE | 107 |
| IPSec | 102, 107, 125, 131, 149 |
| Key Management | 103 |
| L2TP | 145 |
| Manual Key | 107 |
| PFS | 103 |
| PPTP | 141 |
| SA(Security Association) | 102 |
| VPN | 102 |

Appendix G

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. Edifício 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 Street, Fountain Valley, CA 92708, USA
TEL: 1-714-885-6000 FAX: 1-866-743-4905
INFO: 1-877-453-5465 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com