

D-Link

User Manual
DFL-500

Firewall

DFL-500 V2.27

User Manual



D-Link Systems, Inc.

© Copyright 2002 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-500 User Manual

Version 2.27

31 July 2002

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

Introduction	9
Antivirus protection	9
Web content filtering	10
Firewall.....	10
NAT/Route mode	10
Transparent mode	11
Hacker prevention and network protection	11
VPN.....	11
Secure installation, configuration, and management.....	12
Web-based manager	12
Command line interface.....	12
Logging and reporting.....	12
About this document	13
For more information.....	13
Customer service and technical support.....	14
Getting started	15
Package contents	15
Mounting	15
Powering on	16
Next steps	17
NAT/Route mode installation	18
Preparing to configure NAT/Route mode.....	18
Customize NAT/Route mode settings	18
Advanced NAT/Route mode settings	19
Using the setup wizard.....	20
Connecting to the web-based manager.....	20
Starting the firewall setup wizard.....	20
Reconnecting to the web-based manager.....	21
Using the command line interface	21
Connecting to the CLI	21
Configuring the DFL-500 to run in NAT/Route mode	21
Connecting to your network	22
Configuring your internal network	23
Completing the configuration	23
Setting the date and time.....	23
Transparent mode installation	24
Preparing to configure Transparent mode	24
Customizing Transparent mode settings	24

Using the setup wizard.....	25
Connecting to the web-based manager.....	25
Changing to Transparent mode.....	25
Starting the setup wizard.....	26
Reconnecting to the web-based manager.....	26
Using the command line interface.....	26
Connecting to the CLI.....	26
Configuring the DFL-500 to run in Transparent mode.....	27
Setting the date and time.....	28
Connecting to your network.....	28

Firewall configuration..... 29

Policy modes.....	29
NAT/Route mode.....	29
Transparent mode.....	30
Changing to Transparent mode.....	30
Changing to NAT/Route mode.....	30
Changing the policy mode between interfaces.....	30
Adding policies.....	31
Adding route mode policies.....	31
Adding NAT mode policies.....	32
Editing policies.....	34
Ordering policies in policy lists.....	34
Adding addresses.....	35
Adding addresses.....	35
Editing addresses.....	36
Deleting addresses.....	36
Adding virtual IPs.....	36
Adding Virtual IPs.....	36
Services.....	37
Pre-defined services.....	37
Providing access to custom services.....	38
Grouping services.....	39
Schedules.....	40
Creating one-time schedules.....	40
Creating recurring schedules.....	41
Adding a schedule to a policy.....	42
Users and authentication.....	42
Adding user names and passwords.....	43
Setting authentication time out.....	43
Adding authentication to a policy.....	43
Port forwarding.....	44
Port forwarding example.....	44
IP/MAC binding.....	45

Adding IP/MAC binding addresses.....	46
Enabling IP/MAC binding.....	46
Traffic shaping	46
Adding traffic shaping to a policy.....	46
Example policies	48
NAT mode policy for public access to a server.....	48
Route mode policy for public access to a server	48
Transparent mode policy for public access to a server	49
Denying connections from the Internet	49
Using a schedule to deny access	50
Denying connections to the Internet	50
Adding policies that accept connections.....	51
Requiring authentication to connect to the Internet	52
IPSec VPNs	53
Compatibility with third-party VPN products	53
Autokey IPSec VPN between two networks	54
Creating the VPN tunnel.....	55
Adding source and destination addresses.....	57
Adding an IPSec VPN policy	58
Autokey IPSec VPN for remote clients	59
Configuring the network end of the VPN tunnel	60
Adding source and destination addresses.....	61
Adding an IPSec VPN policy	62
Configuring the IPSec VPN client.....	63
Dial-up VPN	63
Adding a dial-up VPN tunnel.....	64
Configuring remote IPSec VPN clients	65
Configuring remote IPSec VPN gateways.....	65
Viewing VPN tunnel status.....	66
Dial-up monitor.....	66
Manual key IPSec VPN between two networks.....	67
Configuring the manual key VPN tunnel.....	67
Manual key IPSec VPN for remote clients	68
Configuring the VPN tunnel	69
Testing a VPN	69
IPSec pass through.....	69
IPSec client to network pass through	70
IPSec network to network pass through	72
PPTP and L2TP VPNs	75
PPTP VPN configuration.....	75
Configuring the DFL-500 as a PPTP gateway.....	76
Configuring a Windows 98 client for PPTP.....	77

Configuring a Windows 2000 Client for PPTP	78
Configuring a Windows XP Client for PPTP	78
PPTP pass through.....	79
PPTP client to network pass through	80
L2TP VPN configuration	81
Configuring the DFL-500 as an L2TP gateway	81
Configuring a Windows 2000 Client for L2TP.....	82
Configuring a Windows XP Client for L2TP	83
RADIUS authentication for PPTP and L2TP VPNs	85
Adding RADIUS server addresses	85
Turning on RADIUS authentication for PPTP.....	86
Turning on RADIUS authentication for L2TP.....	86

Network Intrusion detection system (NIDS)..... 87

NIDS features.....	87
Denial of Service (DoS) attacks.....	87
Reconnaissance	87
Exploits	88
NIDS evasion.....	88
Configuring NIDS detection	88
Viewing the attack list	89
Configuring NIDS responses	89
General NIDS responses.....	89
NIDS Alerts	89

Virus protection 91

Configuring antivirus protection	91
Antivirus connection types.....	92
Configuring antivirus protection	92
Worm protection.....	93
Customize antivirus messages	94
Customizing messages added to email.....	94
Customizing messages added to web pages	94
Updating your antivirus database	95
Displaying virus and worm lists.....	95

Web content filtering 96

Block web pages that contain unwanted content.....	96
Enabling the banned word list.....	96
Changing the content block message	96
Adding words and phrases to the banned word list.....	96
Temporarily disabling the banned word list	97
Temporarily disabling individual words in the banned word list.....	97
Clearing the banned word list	98
Backing up the banned word list.....	98

Restoring the banned word list	98
Block access to Internet sites	98
Enabling the URL block list.....	99
Changing the URL block message	99
Adding URLs to the URL block list	99
Temporarily disabling the URL block list	100
Temporarily disabling individual URL blocking	100
Clearing the URL block list	100
Downloading the URL block list.....	100
Uploading a URL block list.....	101
Remove scripts from web pages	101

Logging and reporting..... 103

Configuring logging	103
Recording logs on a remote computer	103
Recording logs on a WebTrends server	103
Selecting what to log.....	104
Log message formats	104
Traffic log message format	104
Event log message format.....	105
Attack log message format	106

Administration..... 107

Logging into the web-based manager	107
System status.....	108
Upgrading the DFL-500 firmware	108
Manual antivirus database updates	111
Manual attack database updates.....	111
Displaying the DFL-500 serial number	112
Backing up system settings	112
Restoring system settings.....	112
Restoring system settings to factory defaults	113
Restarting the DFL-500	113
Shutting down the DFL-500	113
System status monitor	113
Automatic antivirus and attack database updates	114
Network configuration	115
Configuring the internal interface.....	115
Configuring the external interface.....	116
Configuring the management interface (Transparent mode)	119
Setting DNS server addresses	119
Configuring routing	119
Enabling RIP server support.....	119
Providing DHCP services to your internal network.....	120
System configuration	121

Setting system date and time	121
Changing web-based manager options	122
Adding and editing administrator accounts.....	122
Configuring SNMP	124
Alert email	126

Glossary 128

Troubleshooting FAQs 131

General administration	131
Network configuration	131
Firewall policies.....	131
Schedules	132
VPN.....	132
Virus protection	132
Web content filtering	133
Logging	133

Technical Support..... 134

Limited Warranty..... 137

Registration 140

Introduction

The DFL-500 Network Protection Gateway (NPG) supports network-based deployment of application-level services—including virus protection and full-scan content filtering. DFL-500 NPGs improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network.

Your DFL-500 NPG is a dedicated easily managed security device that delivers a full suite of capabilities that include:

- application-level services such as virus protection and content filtering
- network-level services such as firewall, intrusion detection, VPN, and traffic shaping

Your DFL-500 NPG employs D-Link's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which leverages breakthroughs in chip design, networking, security, and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks. The DFL-500 series complements existing solutions, such as host-based antivirus protection, and enables new applications and services while greatly lowering costs for equipment, administration and maintenance.

The DFL-500 NPG is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office and home office (SOHO) applications. The DFL-500 installation wizard guides users through a simple process that enables most installations to be up and running in minutes.



Antivirus protection

DFL-500 antivirus protection screens the information found in web (HTTP protocol) and email content (SMTP, POP3, and IMAP protocols) as it passes through the DFL-500. The content can be contained in normal network traffic that is allowed to pass between DFL-500 interfaces as well as in IPsec VPN traffic. Antivirus protection can scan HTTP and email files and attachments in MIME (Multipurpose Internet Mail Extensions) and Uuencode format.

Antivirus protection screens content traffic for the following types of target files that can contain viruses:

- Executable files (exe, bat, and com)
- Visual basic files (vbs)
- Compressed files (zip, gzip, tar, hta, and rar)
- Screen saver files (scr)
- Dynamic link libraries (dll)
- MS Office files that contain macros

You can configure antivirus protection to:

- Block target files

The DFL-500 removes from content protocol data streams target files and attachments that can contain viruses. You can configure antivirus protection to remove all target files or just selected target file types. You can also configure antivirus protection to remove different target file types from each content protocol.

- Scan all target files for viruses

The antivirus scanning engine performs signature and macro virus scanning on all target files. If the anti-virus scanner finds a virus, the file is deleted from the data stream.

- Identify and remove files known to be used by worms

DFL-500 virus and worm prevention is transparent to the end user. Client and server programs require no special configuration, and DFL-500 high-performance hardware and software ensure there are no noticeable download delays.

Web content filtering

DFL-500 Web content filtering can be configured to scan all HTTP content protocol streams for URLs or for web page content. If a match is found between a URL on the URL block list, or if a web page is found to contain a word or phrase in the content block list, the DFL-500 blocks the web page. The blocked web page is replaced with a message that you can edit using the DFL-500 web-based manager.

You can configure URL blocking to block all or just some of the pages on a website. Using this feature you can deny access to parts of a web site without denying access to it completely.

Content blocking can block words and word patterns using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

Web content filtering also includes a script filter feature that can be configured to block unsecure web content such as:

- Java Applets
- Cookies
- ActiveX

Firewall

The DFL-500 state-of-the-art firewall protects your computer networks from the hostile environment of the Internet. After you have performed the basic installation of the DFL-500, the firewall is configured to allow users on the protected network to access the Internet while blocking Internet access to internal networks. Using the web-based manager you can modify this firewall configuration to place controls on access to the Internet from the protected network and to allow controlled access to internal networks.

DFL-500 security policies include a complete range of options that:

- Control incoming and outgoing traffic
- Block or allow access for all policy options
- Control when individual policies are in effect
- Accept or deny traffic to and from individual addresses
- Control standard and user defined network services individually or in groups
- Require users to enter passwords before gaining access to the Internet
- Include traffic shaping to set access priorities and guarantee or limit bandwidth for each policy
- Include logging to track connections for individual policies

The DFL-500 firewall can operate in NAT/Route mode or Transparent mode.

NAT/Route mode

In NAT/Route mode, the DFL-500 is installed as a privacy barrier between the internal network and the Internet. The firewall provides network address translation (NAT) to protect the internal private network. You can also configure the firewall to provide public access to servers on your internal network.

In NAT/Route mode you can control whether firewall policies run in NAT mode or route mode. NAT mode policies route allowed connections between firewall interfaces, performing network address translation to hide

addresses on the protected internal networks. Route mode policies route allowed connections between firewall interfaces without performing network address translation.

Transparent mode

Transparent Mode is used to provide firewall protection to a pre-existing network with public addresses. The internal and external network interfaces of the DFL-500 can be in the same network; therefore, the DFL-500 can be inserted into your network at any point without the need to make any changes to your network.

The following features are not supported in Transparent mode:

- VPN
- IP/MAC binding
- Port forwarding
- DHCP and PPPoE configuration of the external network address

Hacker prevention and network protection

The DFL-500 Network Intrusion Detection System (NIDS) is a real-time network intrusion detection sensor that identifies and takes action against a wide variety of suspicious network activity. The NIDS uses intrusion signatures, stored in the attack database, to identify the most common attacks. In response to an attack, the NIDS protects the DFL-500 and the networks connected to it by:

- Dropping the connection
- Blocking packets from the location of the attack
- Blocking network ports, protocols, or services being used by an attack

To notify system administrators of the attack, the NIDS records the attack and any suspicious traffic to the attack log.

The attack database functions in a similar manner to an antivirus database. D-Link updates the attack database periodically. You can download and install attack database updates manually. You can also configure the DFL-500 to automatically check for and download IDS database updates.

VPN

Using DFL-500 virtual private networking (VPN), you can provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.

The DFL-500 VPN features include:

- Industry standard IPSec VPN including:
 - IPSec, ESP security in tunnel mode
 - DES and 3DES (triple-DES) hardware accelerated encryption
 - HMAC MD5 and HMAC SHA1 authentication and data integrity
 - AutoKey IKE and manual key exchange
- PPTP for easy connectivity with the VPN standard supported by the most popular operating systems
- L2TP for easy connectivity with a more secure VPN standard also supported by many popular operating systems
- IPSec and PPTP VPN pass through so that computers or subnets on your internal network can connect to a VPN gateway on the Internet

Secure installation, configuration, and management

Installation is quick and simple. When you initially power the DFL-500 up, it is already configured with default IP addresses and security policies. All that is required for the DFL-500 to start protecting your network is to connect to the web-based manager, set the operating mode and use the setup wizard to customize DFL-500 IP addresses for your network. From this foundation you can use the web-based manager to customize the configuration to meet your needs.

You can also create a basic configuration from the DFL-500 command line interface (CLI).

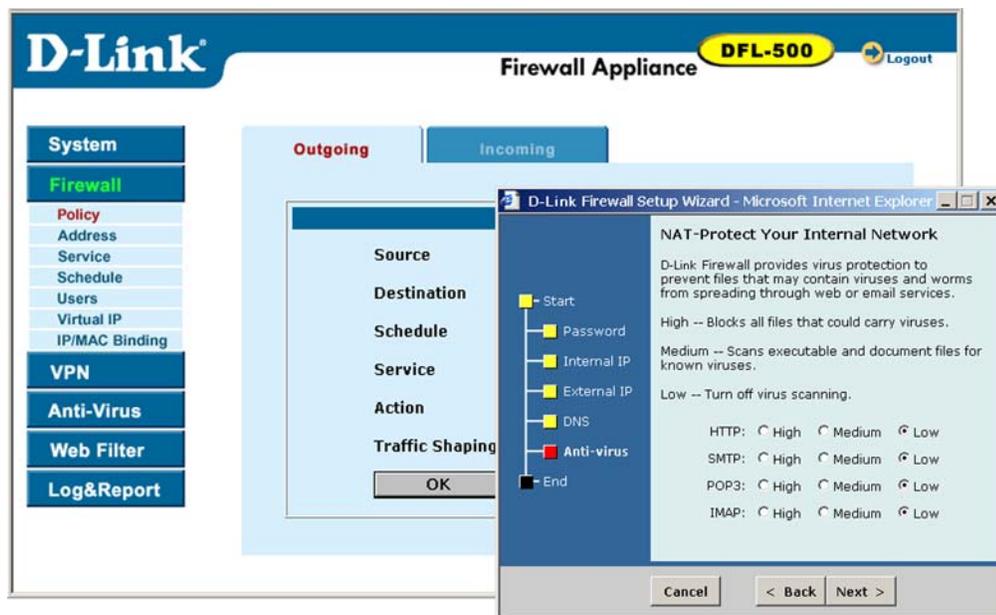
Web-based manager

Using a secure HTTPS connection from any computer running Internet Explorer, you can configure and manage the DFL-500. The web-based manager supports multiple languages. It can also be configured for secure administration from the external network (Internet).

Configuration changes made with the web-based manager are effective immediately without the need to reset the firewall or interrupt service.

Once a satisfactory configuration has been established, it can be downloaded and saved. The saved configuration can be restored at any time.

The DFL-500 web-based manager and setup wizard.



Command line interface

For troubleshooting and professional scripting, a command line interface is available by connecting a management computer to the DFL-500 RS-232 serial Console. You can also use the SSH protocol for a secure connection to the DFL-500 CLI from your internal network or the Internet. Connecting to and using the DFL-500 CLI is described in the *DFL-500 CLI Reference Guide*.

Logging and reporting

The DFL-500 supports logging of various categories of traffic and of configuration changes. You can configure logging to:

- Report traffic that connects to the firewall interfaces

- Report network services used
- Report traffic permitted by firewall policies
- Report traffic that was denied by firewall policies
- Report events such as configuration changes and other management events, IPSec tunnel negotiation, virus detection, attacks, and web page blocking

Logs can be sent to a remote syslog server or to a WebTrends server using the WebTrends enhanced log format.

About this document

This user manual describes how to install and configure the DFL-500. This document contains the following information:

- [Getting started](#) describes unpacking, mounting, and powering on the DFL-500
- [NAT/Route mode installation](#) describes how to install the DFL-500 if you are planning on running it in NAT/Route mode
- [Transparent mode installation](#) describes how to install the DFL-500 if you are planning on running it in Transparent mode
- [Firewall configuration](#) describes how to configure firewall policies to enhance firewall protection
- [Example policies](#) contains some example firewall policies
- [IPSec VPNs](#) describes how to create an IPSec VPN between two internal protected networks and between an internal network and a client
- [PPTP and L2TP VPNs](#) describes how to configure PPTP and L2TP VPNs between the DFL-500 and a windows client
- [Network Intrusion detection system \(NIDS\)](#) describes how to configure the DFL-500 to detect and prevent common network attacks
- [Virus protection](#) describes how use the DFL-500 to protect your network from viruses and worms
- [Web content filtering](#) describes how to configure web content filters to prevent unwanted Web content from passing through the DFL-500
- [Logging and reporting](#) describes how to configure logging and reporting to track activity through the DFL-500
- [Administration](#) describes DFL-500 management and administrative tasks
- The [Glossary](#) defines many of the terms used in this document
- [Troubleshooting FAQs](#) help you find the information you need if you run into problems

For more information

In addition to the *DFL-500 User Manual* , you have access to the following DFL-500 documentation:

- *DFL-500 QuickStart Guide*
- *DFL-500 CLI Reference Guide*
- DFL-500 online help

Customer service and technical support

For firmware, attack database, and antivirus database updates, updated product documentation, technical support information, and other resources, please visit our web site at <http://www.D-Link.com> and follow the link to the support page.

The D-Link automatic update center at update.D-Link.com is also available for automatically updating your antivirus and attack databases.

You can contact D-Link Technical Support at:

See [Technical Support](#)

To help us provide the support you require, please provide the following information:

- Name
- Company Name
- Location
- Email address
- Telephone Number
- Software Version
- Serial Number
- Detailed description of your problem

Getting started

This chapter describes unpacking, setting up, and powering on your DFL-500. Once you have completed the procedures in this chapter, you can proceed to one of the following:

- If you are going to run your DFL-500 in NAT/Route mode, go to [NAT/Route mode installation](#)
- If you are going to run your DFL-500 in Transparent mode, go to [Transparent mode installation](#)

This chapter includes:

- [Package contents](#)
- [Mounting](#)
- [Powering on](#)
- [Next steps](#)

Package contents

The DFL-500 package contains the following items:

- The DFL-500
- One orange cross-over ethernet cable
- One gray regular ethernet cable
- One null-modem cable
- The DFL-500 QuickStart Guide
- A CD containing this *DFL-500 User Manual* and the *DFL-500 CLI Reference Guide*
- One AC adapter
- Registration Card

DFL-500 package contents



Mounting

The DFL-500 can be installed on any stable surface. Make sure the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Dimensions

- 8.63 x 6.13 x 1.38 in. (21.9 x 15.6 x 3.5 cm)

Weight

- 1.5 lb. (0.68 kg)

Power requirements

- DC input voltage: 5 V
- DC input current: 3 A

Environmental specifications

- Operating Temperature: 32 to 104 °F (0 to 40 °C)
- Storage Temperature: -13 to 158 °F (-25 to 70 °C)
- Humidity: 5 to 95% non-condensing

Powering on

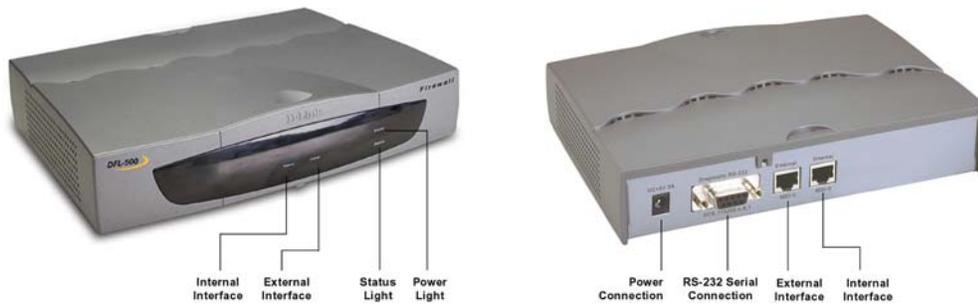
To power on the DFL-500:

- Connect the AC adapter to the power connection at the back of the DFL-500.
- Connect the AC adapter to a power outlet.

The DFL-500 starts up. The Power and Status lights light. The Status light flashes while the DFL-500 is starting up and remains lit when the system is up and running.

DFL-500 LED indicators		
LED	State	Description
Power	Green	The DFL-500 is powered on.
	Off	The DFL-500 is powered off.
Status	Flashing Green	The DFL-500 is starting up.
	Green	The DFL-500 is running normally.
	Off	The DFL-500 is powered off.
Internal External (Front)	Green	The correct cable is in use, and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
Internal External (Back)	Green	The correct cable is in use, and the connected equipment has power.
	Flashing Amber	Network activity at this interface.
	Off	No link established.

Front and back view of the DFL-500



Next steps

Now that your DFL-500 is up and running, you can proceed to configure it for operation:

- If you are going to run your DFL-500 in NAT/Route mode, go to [NAT/Route mode installation](#)
- If you are going to run your DFL-500 in Transparent mode, go to [Transparent mode installation](#)

NAT/Route mode installation

This chapter describes how to install your DFL-500 in NAT/Route mode. If you want to install the DFL-500 in Transparent mode, see [Transparent mode installation](#).

This chapter includes:

- [Preparing to configure NAT/Route mode](#)
- [Using the setup wizard](#)
- [Using the command line interface](#)
- [Connecting to your network](#)
- [Configuring your internal network](#)
- [Completing the configuration](#)

Preparing to configure NAT/Route mode

When the DFL-500 is first powered on, it is running in NAT/Route mode and has the basic configuration listed in [DFL-500 initial power on settings](#).

DFL-500 initial power on settings			
Operating Mode:			NAT/Route
Administrator Account:		User name:	admin
		Password:	(none)
Internal Interface:		IP:	192.168.1.99
		Netmask:	255.255.255.0
External Interface:	Manual:	IP:	192.168.100.99
		Netmask:	255.255.255.0
		Default Gateway:	(none)
		Primary DNS Server:	207.194.200.1
		Secondary DNS Server:	207.194.200.129

Customize NAT/Route mode settings

Use [NAT/Route mode settings](#) to gather the information you need to customize NAT/Route mode settings.

NAT/Route mode settings		
Administrator Password:		
Internal Interface:	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
External Interface:	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____

	Default Gateway:	_____ . _____ . _____ . _____	
	Primary DNS Server:	_____ . _____ . _____ . _____	
	Secondary DNS Server:	_____ . _____ . _____ . _____	
Internal Server Settings:	Web Server:	_____ . _____ . _____ . _____	
	Mail Server:	SMTP:	_____ . _____ . _____ . _____
		POP3:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____	
If you provide access from the Internet to a web server, mail server, or FTP server installed on an internal network, add the IP addresses of the servers here.			

Advanced NAT/Route mode settings

Use [Advanced DFL-500 NAT/Route mode settings](#) to gather the information you need to customize advanced DFL-500 NAT/Route mode settings.

Advanced DFL-500 NAT/Route mode settings			
External Interface:	DHCP:	If your ISP supplies you with an IP address using DHCP no further information is required.	
	PPPoE:	User name:	_____
		Password:	_____
If your ISP supplies you with an IP address using PPPoE, record your PPPoE user name and password.			
DHCP Server Settings:	Starting IP:	_____ . _____ . _____ . _____	
	Ending IP:	_____ . _____ . _____ . _____	
	Netmask:	_____ . _____ . _____ . _____	
	Default Route:	_____ . _____ . _____ . _____	
	DNS IP:	_____ . _____ . _____ . _____	
The DFL-500 contains a DHCP server that you can configure to automatically set the addresses of the computers on your internal network.			

Using the setup wizard

Use the procedures in this section to connect to the web-based manager and the setup wizard to create the initial configuration of your DFL-500.

Connecting to the web-based manager

You require:

- A computer with an ethernet connection
- Internet Explorer version 4.0 or higher
- A crossover cable or an ethernet hub and two ethernet cables

To connect to the web-based manager:

- Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
- Using the crossover cable or the ethernet hub and cables, connect the Internal interface of the DFL-500 to the computer ethernet connection.
- Start Internet Explorer and browse to the address ***https://192.168.1.99***.
- The DFL-500 login page appears.
- Type admin in the Name field and select Login.

DFL-500 login page



Starting the firewall setup wizard

To start the firewall setup wizard:

- Select the Wizard button at the upper right of the web-based manager.
- Use the information that you gathered in [NAT/Route mode settings](#) to fill in the wizard fields. Select the next button to step through the wizard pages.
- Confirm your configuration settings and then Select Finish and Close.

Reconnecting to the web-based manager

If you changed the IP address of the internal interface while using the setup wizard, you must reconnect to the web-based manager using a new IP address. Browse to <https://> followed by the new IP address of the internal interface. Otherwise, you can reconnect to the web-based manager by browsing to <https://192.168.1.99>.

You have now completed the initial configuration of your DFL-500, and you can proceed to connect the DFL-500 to your network using the information in [Connecting to your network](#).

Using the command line interface

As an alternative to the setup wizard, you can configure the DFL-500 using the Command Line Interface (CLI). To connect to the DFL-500 CLI, you require:

- A computer with an available communications port
- A null modem cable with a 9-pin connector to connect to the DFL-500 Console connection (RS-232 serial connector) (see [Front and back view of the DFL-500](#))
- Terminal emulation software such as HyperTerminal for Windows



Note: The following procedure describes how to connect to the DFL-500 CLI using Windows HyperTerminal software. You can use any terminal emulation program.

Connecting to the CLI

- Connect the null modem cable to the DFL-500 Console connector and to the available communications port on your computer.
- Make sure the DFL-500 is powered on.
- Start HyperTerminal, enter a name for the connection, and Select OK.
- Type the communications port in the Connect using field and select OK.
- Select the following port settings and select OK:

Bits per second 9600

Data bits 8

Parity None

Stop bits 1

Flow control None

- Press Enter to connect to the DFL-500 CLI.

The following prompt appears:

D-Link login:

- Type *admin* and press Enter twice.

The following prompt appears:

Type ? for a list of commands.

Configuring the DFL-500 to run in NAT/Route mode

Use the information that you gathered in [NAT/Route mode settings](#) to complete the following procedures.

Configuring NAT/Route mode IP addresses

- Login to the CLI if you are not already logged in.
- Set the IP address and netmask of the Internal interface to the Internal IP Address and Netmask that you recorded in [NAT/Route mode settings](#). Enter:

```
set system interface internal ip <IP Address> <Netmask>
```

Example

```
set system interface internal ip 192.168.1.1 255.255.255.0
```

- Set the IP address and netmask of the external interface to the External IP Address and Netmask that you recorded in [NAT/Route mode settings](#).

To set the Manual IP address and netmask, enter:

```
set system interface external manual ip <IP Address> <Netmask>
```

Example

```
set system interface external manual ip 204.23.1.5 255.255.255.0
```

To set the external interface to use DHCP enter:

```
set system interface external dhcp enable
```

To set the external interface to use PPPoE enter:

```
set system interface external pppoe enable <user name> <password>
```

Example

```
set system interface external pppoe enable username password
```

- Confirm that the addresses are correct. Enter:

```
get system interface
```

The CLI lists the IP address and netmask settings for each of the DFL-500 interfaces as well as the mode of the external interface (Manual, DHCP, or PPPoE).

Configure the NAT/Route mode default gateway

- Login to the CLI if you are not already logged in.
- Set the default route to the Default Gateway IP Address that you recorded in [NAT/Route mode settings](#). Enter:

```
set system route add 0.0.0.0 0.0.0.0 gw <IP Address> dev external
```

Example

```
set system route add 0.0.0.0 0.0.0.0 gw 204.23.1.2 dev external
```

You have now completed the initial configuration of your DFL-500 and you can proceed to connect the DFL-500 to your network using the information in [Connecting to your network](#).

Connecting to your network

Once you have completed the initial configuration, you can connect your DFL-500 between your internal network and the Internet.

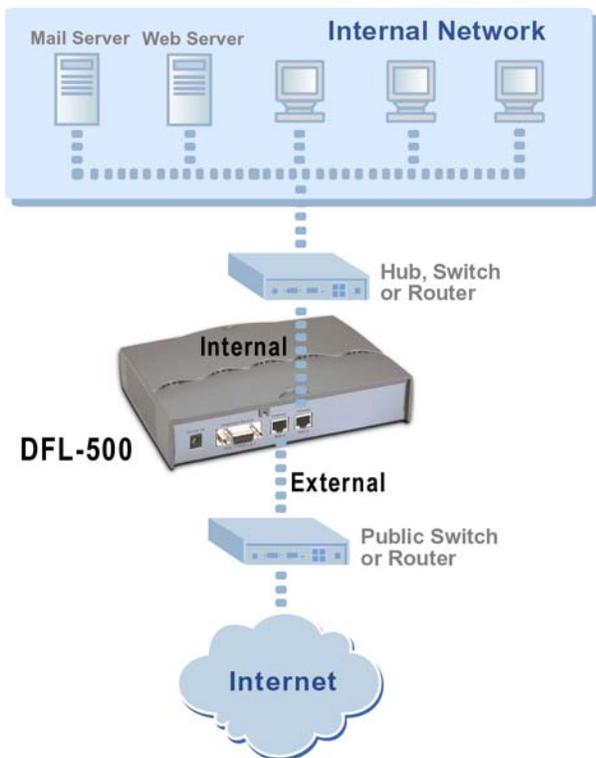
There are two 10/100 BaseTX connectors on the DFL-500:

- Internal for connecting to your internal network
- External for connecting to your public switch or router and the Internet

To connect the DFL-500:

- Connect the Internal interface to the hub or switch connected to your internal network.
- Connect the External interface to the public switch or router provided by your Internet Service Provider.

DFL-500 network connections



Configuring your internal network

If you are running the DFL-500 in NAT/Route mode, your internal network must be configured to route all internet traffic to the address of the internal interface of the DFL-500. This means changing the default gateway address of all computers and routers connected directly to the internal network.

If you are using the DFL-500 as the DHCP server for your internal network, configure the computers on your internal network for DHCP. Use the internal address of the DFL-500 as the DHCP server IP address.

Once the DFL-500 is connected, make sure it is functioning properly by connecting to the Internet from a computer on your internal network. You should be able to connect to any Internet address.

Completing the configuration

Use the information in this section to complete the initial configuration of the DFL-500.

Setting the date and time

For effective scheduling and logging, the DFL-500 date and time should be accurate. You can either manually set the DFL-500 time or you can configure the DFL-500 to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the DFL-500 date and time, see [Setting system date and time](#).

Transparent mode installation

This chapter describes how to install your DFL-500 in Transparent mode. If you want to install the DFL-500 in NAT/Route mode, see [NAT/Route mode installation](#).

This chapter includes:

- [Preparing to configure Transparent mode](#)
- [Using the setup wizard](#)
- [Using the command line interface](#)
- [Setting the date and time](#)
- [Connecting to your network](#)

Preparing to configure Transparent mode

When first switched to transparent mode, the DFL-500 has the settings listed in [DFL-500 Transparent mode settings](#).

DFL-500 Transparent mode settings		
Operating Mode:		Transparent
Administrator Account:	User name:	admin
	Password:	(none)
Management Interface: (Internal interface)	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Default Gateway:	(none)

Customizing Transparent mode settings

Use [Transparent mode settings](#) to gather the information you need to customize Transparent mode settings.

Transparent mode settings		
Administrator Password:		
Management IP:	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
The management IP address and netmask must be valid for the network from which you will manage the DFL-500. Add a default gateway if the DFL-500 must connect to a router to reach the management computer.		
DNS Settings:	Primary DNS server:	_____ . _____ . _____ . _____
	Secondary DNS server:	_____ . _____ . _____ . _____

Using the setup wizard

Use the procedures in this section to connect to the web-based manager and the setup wizard to create the initial configuration of your DFL-500.

Connecting to the web-based manager

You require:

- A computer with an ethernet connection
- Internet Explorer version 4.0 or higher
- A crossover cable or an ethernet hub and two ethernet cables

To connect to the web-based manager:

- Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
- Using the crossover cable or the ethernet hub and cables, connect the Internal interface of the DFL-500 to the computer ethernet connection.
- Start Internet Explorer and browse to the address **https://192.168.1.99** .
The DFL-500 login page appears.
- Type admin in the Name field and select Login.

DFL-500 login page



Changing to Transparent mode

The first time you connect to the DFL-500 it is configured to run in NAT/Route mode. To switch to Transparent mode using the web-based manager:

- Go to *Firewall > Mode* .
- Select Transparent.
- Select Apply.
- Select OK.

To reconnect to the web-based manager, connect to the internal interface and browse to https:// followed by the transparent mode management IP address. The default DFL-500 transparent mode Management IP address is 192.168.1.99.

Starting the setup wizard

To start the setup wizard:

- Select the Wizard button at the upper right of the web-based manager.
- Use the information that you gathered in [Transparent mode settings](#) to fill in the wizard fields. Select the next button to step through the wizard pages.
- Confirm your configuration settings and then Select Finish and Close.

Reconnecting to the web-based manager

If you changed the IP address of the management interface while using the setup wizard, you must reconnect to the web-based manager using a new IP address. Browse to `https://` followed by the new IP address of the management interface. Otherwise, you can reconnect to the web-based manager by browsing to `https://192.168.1.99`. If you connect to the management interface through a router, make sure you have added a default gateway for that router to the management IP default gateway field.

Using the command line interface

As an alternative to the setup wizard, you can configure the DFL-500 using the Command Line Interface (CLI). To connect to the DFL-500 command line interface (CLI) you require:

- A computer with an available communications port
- A null modem cable with a 9-pin connector to connect to the DFL-500 Console connection (RS-232 serial connector) (see [Front and back view of the DFL-500](#))
- Terminal emulation software such as HyperTerminal for Windows



Note: The following procedure describes how to connect to the DFL-500 CLI using Windows HyperTerminal software. You can use any terminal emulation program.

Connecting to the CLI

- Connect the null modem cable to the DFL-500 Console connector and to the available communications port on your computer.
- Make sure the DFL-500 is powered on.
- Start HyperTerminal, enter a name for the connection, and Select OK.
- Type the communications port in the Connect using field and select OK.
- Select the following port settings and select OK:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- Press Enter to connect to the DFL-500 CLI.
 - The following prompt appears:
 - `D-Link login:`

- Type `admin` and press Enter.
The following prompt appears:
Type ? for a list of commands.

Configuring the DFL-500 to run in Transparent mode

Use the information that you gathered in [Transparent mode settings](#) to complete the following procedures.

Changing to Transparent mode

- Login to the CLI if you are not already logged in.
- Switch to Transparent mode. Enter:
`set firewall opmode transparent`
After a few seconds, the following prompt appears:
D-Link login:
- Type `admin` and press Enter.
The following prompt appears:
Type ? for a list of commands.
- Confirm that the DFL-500 has switched to Transparent mode. Enter:
`get system status`
The CLI displays the status of the DFL-500. The last line shows the current operation mode.
Version:DFL-500 2.26,build041,020617
virus-db:3.1(06/13/2002 15:30)
ids-db:1.0(06/05/2002 11:33)
Serial Number:FGT-502801021075
Operation mode: Transparent

Configuring the Transparent mode management IP address

- Login to the CLI if you are not already logged in.
- Set the IP address and netmask of the Management IP to the IP address and netmask that you recorded in [Transparent mode settings](#). Enter:
`set system manageip ip <IP Address> <Netmask>`
Example
`set system manageip ip 10.10.10.2 255.255.255.0`
- Confirm that the address is correct. Enter:
`get system manageip`
The CLI lists the Management IP address and netmask.

Configure the Transparent mode default gateway

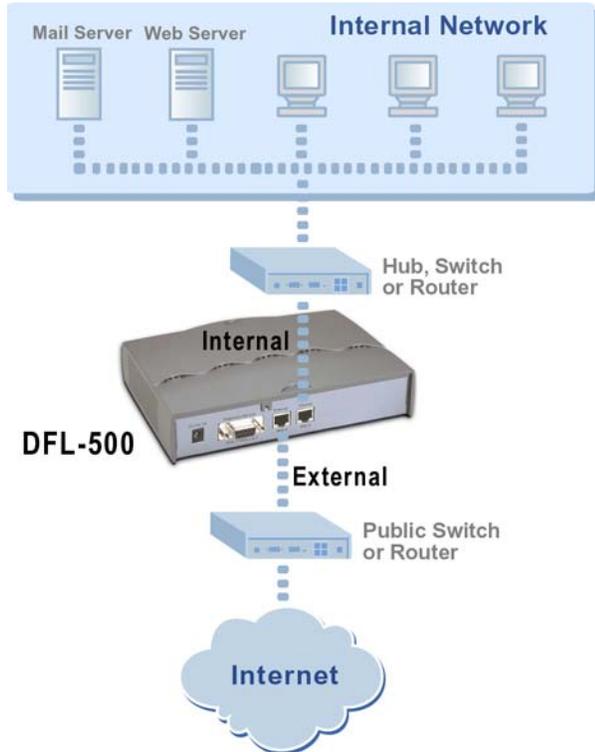
- Login to the CLI if you are not already logged in.
- Set the default route to the Default Gateway that you recorded in [Transparent mode settings](#). Enter:
`set system manageip gateway <IP Address>`
Example
`set system manageip gateway 192.168.1.20`
You have now completed the initial configuration of the DFL-500 and you can proceed to connect the DFL-500 to your network using the information in [Connecting to your network](#) that follows.

Setting the date and time

For effective scheduling and logging, the DFL-500 date and time should be accurate. You can either manually set the time or you can configure the DFL-500 to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the DFL-500 date and time, see [Setting system date and time](#).

DFL-500 network connections



Connecting to your network

Once you have completed the initial configuration, you can connect the DFL-500 between your internal network and the Internet.

There are two 10/100 BaseTX connectors on the DFL-500:

- Internal for connecting to your internal network
- External for connecting to your public switch or router and the Internet

To connect the DFL-500:

- Connect the Internal interface to the hub or switch connected to your internal network.
- Connect the External interface to the public switch or router provided by your Internet Service Provider.

Firewall configuration

By default the users on your internal network can connect through the DFL-500 to the Internet. The DFL-500 blocks all other connections. The DFL-500 is configured with a default firewall security policy that matches any connection request received from the internal network and instructs the firewall to forward the connection to the Internet.

Default security policy



Order	Source	Dest	Schedule	Service	Action
1	Internal_All	External_All	Always	ANY	ACCEPT

Security policies are instructions used by the firewall to decide what to do with a connection request. When the firewall receives a connection request in the form of a packet, it analyzes the packet to extract its source address, destination address, and service (port number).

For the packet to be connected through the DFL-500, you must have added a policy to the interface that receives the packet. The policy must match the packet's source address, destination address, and service. The policy directs the action that the firewall should perform on the packet. The action can be to allow the connection, deny the connection, or to require authentication before the connection is allowed. You can also add schedules to security policies so that the firewall can process connections differently depending on the time of day or the day of the week, month, or year.

To configure security policies:

- [Policy modes](#)
- [Adding policies](#)
- [Adding addresses](#)
- [Adding virtual IPs](#)
- [Services](#)
- [Schedules](#)
- [Users and authentication](#)
- [Port forwarding](#)
- [IP/MAC binding](#)
- [Traffic shaping](#)

Policy modes

The first step in configuring security policies is to configure the mode for the firewall. The firewall can run in NAT/Route mode or Transparent mode.

NAT/Route mode

Select NAT/Route mode to use DFL-500 network address translation to protect private networks from public networks. In NAT/Route mode, you can connect a private network to the internal interface and a public network, such as the Internet, to the external interface. Then you can create NAT mode policies to accept or deny connections between these networks. NAT mode policies hide the addresses of the internal network from users on the internet.

In NAT/Route mode you can also create route mode policies between interfaces. Route mode policies accept or deny connections between networks without performing address translation.

Transparent mode

Select Transparent Mode to provide firewall protection to a network with public addresses. There are no restrictions on the addresses of the interfaces of the DFL-500. Therefore, the DFL-500 can be inserted into your network at any point without the need to make changes to your network. In transparent mode, the DFL-500 acts like a router.

In transparent mode, you create route mode policies to accept or deny connections between the internal and external interface. You manage the DFL-500 by connecting to a transparent mode management interface through the internal interface.

Changing to Transparent mode

Use the following procedure if you want to switch the DFL-500 from NAT/Route mode to Transparent mode.



Note: Changing to Transparent mode deletes NAT/Route mode firewall policies and addresses and IPSec VPN policies.

Using the web-based manager:

- Go to *Firewall > Mode* .
- Select Transparent.
- Select Apply.
- Select OK.
- To reconnect to the web-based manager:
Connect to the internal interface and browse to <https://> followed by the transparent mode management IP address. The default transparent mode Management IP address is 192.168.1.99.

Changing to NAT/Route mode

Use the following procedure if you want to switch the DFL-500 from Transparent mode to NAT/Route mode.



Note: Changing to NAT/Route mode deletes all Transparent mode firewall policies and addresses.

Using the web-based manager:

- Go to *Firewall > Mode* .
- Select NAT/Route.
- Select Apply.
The DFL-500 changes operation mode.
- To reconnect to the web-based manager, browse to the interface that you have configured for management access using <https://> followed by the IP address of the interface.

Changing the policy mode between interfaces

If the firewall is running in NAT/Route mode, you can configure the policy mode for connections between the internal and external interface. The default policy mode is NAT.



Note: Changing policy modes between interfaces resets firewall policies and addresses and IPSec VPN policies.

To change the policy mode between the internal and external interface using the web-based manager:

- Go to *Firewall > Mode* .
- Select the mode for connections between the internal and external interface.
Select NAT to change the policy mode to NAT mode. Select Route to change the policy mode to route mode.
- Click Apply.

Adding policies

Add security policies to control connections and traffic between DFL-500 interfaces. The first step to adding a policy is to select a policy list. There are 2 policy lists:

Int to Ext Policies for connections from the internal network to the external network (the Internet).

Ext to Int Policies for connections from the external network to the internal network.

Once you have chosen the policy list, you can add policies to control connections. You must arrange policies in the policy list so that they have the results that you expect.

Use the following procedures to add policies:

- [Adding route mode policies](#)
- [Adding NAT mode policies](#)
- [Editing policies](#)
- [Ordering policies in policy lists](#)

Adding route mode policies

When the firewall is running in Transparent mode, all policies are route mode policies. When the firewall is running in NAT/Route mode, policies are route mode policies when the policy mode between two interfaces is set to route mode.

To add a route mode policy:

Go to *Firewall > Policy* .

- Select a policy list tab.
- Click New to add a new policy.

You can also select Insert Policy before  on a policy in the list to add the new policy above a specific policy.

- Configure the policy.

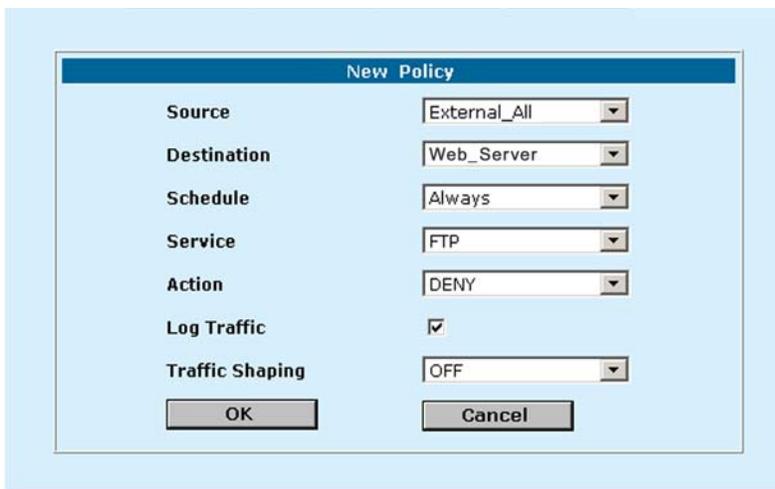
Source	An address that matches the source address of the packet. This can be a single IP address or an address range. Before you can add this address to a policy, you must add it to the source interface. This address must be a valid IP address for the network connected to the source interface. See Adding addresses .
Destination	An address that matches the destination address of the packet. This can be a single IP address or an address range. Before you can add this address to a policy, you must add it to the destination interface. This address must be a valid IP address for the network connected to the destination interface. See Adding addresses .
Schedule	A schedule that controls when this policy is active. During the time that the schedule is valid the policy is available to be matched with connections. See Schedules .

- Service** A service that matches the service (or port number) of the packet. You can select from a wide range of predefined services, or add custom services and service groups. See [Services](#).
- Action** Select how the firewall should respond when the policy matches a connection attempt. You can configure the policy to direct the firewall to accept the connection, deny the connection, or require users to authenticate with the firewall before the firewall accepts the connection. Authentication is not available in Transparent mode. See [Users and authentication](#) for more information about authentication.
- Log Traffic** Optionally select Log Traffic to add messages to the traffic log whenever the policy processes a connection.
- Traffic Shaping** Optionally select Traffic Shaping to control the bandwidth available to and set the priority of the traffic processed by the policy. See [Traffic shaping](#).

- Select OK to add the policy.

The policy is added to the selected policy list. You must arrange policies in the policy list so that they have the results that you expect. Arranging policies in a policy list is described in [Ordering policies in policy lists](#).

Sample Route mode policy (NAT/Route mode)



Adding NAT mode policies

NAT mode policies provide network address translation between interfaces. By default when the firewall is running in NAT/Route mode, it is configured for NAT mode policies between the external and internal interfaces. NAT mode policies hide IP addresses on the internal network from the Internet.

NAT mode policies for connections from the internal interface to the external interface translate the source address of packets to the address of the external interface. The firewall performs this address translation automatically because it knows the address of its external interface.

For connections from the external interface to the internal interface, NAT mode policies must translate the destination address of the packet from an Internet address to an address on the internal network. You have to add the information the firewall needs to be able to map the destination address of the packet to an address on the internal network. This mapping is referred to as a virtual IP.

A virtual IP must be added to Ext to Int NAT mode policies. For more information about virtual IPs, see [Adding virtual IPs](#).

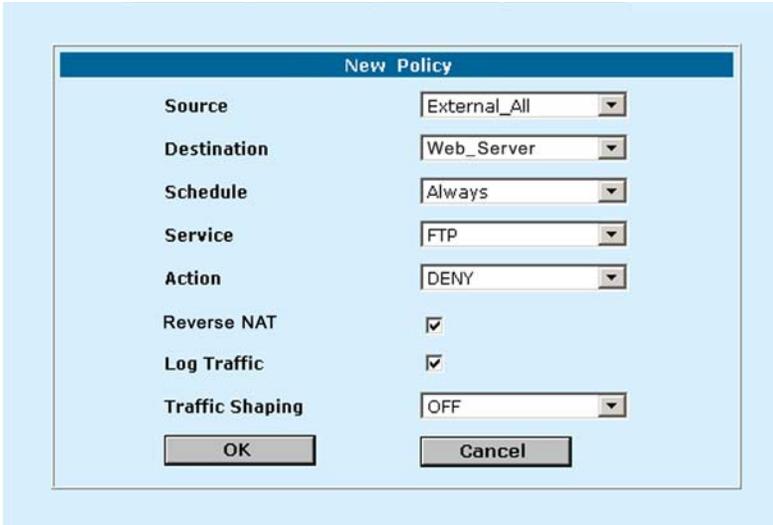
To add a NAT mode policy:

- Go to *Firewall > Policy* .
- Select a policy list tab.
- Select New to add a new policy.

You can also select Insert Policy before  on a policy in the list to add the new policy above a specific policy.

- Configure the policy.

Sample Ext to Int NAT mode policy



New Policy	
Source	External_All
Destination	Web_Server
Schedule	Always
Service	FTP
Action	DENY
Reverse NAT	<input checked="" type="checkbox"/>
Log Traffic	<input checked="" type="checkbox"/>
Traffic Shaping	OFF
OK Cancel	

- Source** An address that matches the source address of the packet. This can be a single IP address or an address range. Before you can add this address to a policy, you must add it to the source interface. This address must be a valid IP address for the network connected to the source interface. See [Adding addresses](#).
- For an Ext to Int NAT mode policy, the destination is a virtual IP that maps the destination address of the packet to a hidden destination address on the internal network.
- Destination** For Int to Ext NAT mode policies, the destination is an address that matches the destination address of the packet. This can be a single IP address or an address range. Before you can add this address to a policy, you must add it to the destination interface. This address must be a valid IP address for the network connected to the destination interface. See [Adding addresses](#).
- Schedule** A schedule that controls when this policy is active. During the time that the schedule is valid the policy is available to be matched with connections. See [Schedules](#).
- Service** A service that matches the service (or port number) of the packet. You can select from a wide range of predefined services, or add custom services and service groups. See [Services](#).
- Action** Select how the firewall should respond when the policy matches a connection attempt. You can configure the policy to accept the connection, deny the connection, or require users to authenticate with the firewall before the firewall accepts the connection. Authentication is not available in Transparent mode. See [Users and authentication](#) for more information about authentication.
- Reverse NAT** For Ext to Int policies you can select Reverse NAT to have the policy perform reverse network address translation on return packets.
- Log Traffic** Optionally select Log Traffic to add messages to the traffic log whenever the policy processes a connection.
- Traffic Shaping** Optionally select Traffic Shaping to control the bandwidth available to and set the priority of the traffic processed by the policy. See [Traffic shaping](#).

- Select OK to add the policy.

The policy is added to the selected policy list. You must arrange policies in the policy list so that they have the results that you expect. See [Ordering policies in policy lists](#) for more information.

Editing policies

To edit a policy:

- Go to *Firewall > Policy* .
- Select the tab for the policy list containing the policy to edit.
- Choose the policy to edit and select Edit  .
- Edit the policy settings as required.
You can change any of the policy settings.
- Select OK to save your changes.

Ordering policies in policy lists

The DFL-500 matches policies by searching for a match starting at the top of the policy list and moving down until it finds the first match. You must arrange policies in the policy list from more specific to more general.

For example, the default policy is a very general policy because it matches all connection attempts. To create exceptions to this policy, they must be added to the policy list above the default policy. No policy below the default policy will ever be matched.

Policy matching in detail

When the DFL-500 receives a connection attempt at an interface, it must match the connection attempt to a policy in either the Int to Ext or Ext to Int policy list. The DFL-500 starts at the top of the policy list for the interface that received the connection attempt and searches down the list for the first policy that matches the connection attempt source and destination addresses, service port, and time and date at which the connection attempt was received. The first policy that matches is applied to the connection attempt. If no policy matches, the connection is dropped.

The default policy accepts all connection attempts from the internal network to the Internet. From the internal network, users can browse the web, use POP3 to get email, use FTP to download files through the DFL-500 and so on. If the default policy is at the top of the Int to Ext policy list, the firewall allows all connections from the internal network to the Internet because all connections match the default policy.

A policy that is an exception to the default policy (for example, a policy to block FTP connections), must be placed above the default policy in the Int to Ext policy list. Then, all FTP connection attempts from the internal network would match the FTP policy and be blocked. Connection attempts for all other kinds of services would not match with the FTP policy but they would match with the default policy. So the firewall would still accept all other connections from the internal network.

Changing the order of policies in a policy list

To rearrange policies:

- Go to *Firewall > Policy* .
- Select the tab for the policy list that you want to rearrange.
- Choose a policy to move and select Move To  to change its order in the policy list.
- Type a number in the Move to field to specify where in the policy list to move the policy and select OK.
- Select Delete  to remove a policy from the list.

Adding addresses

All policies require source and destination addresses. To be able to add an address to a policy between two interfaces, you must first add addresses to the address list for each interface. These addresses must be valid addresses for the network connected to that interface.

By default the DFL-500 includes two addresses that cannot be edited or deleted:

- Internal_All on the internal address list represents the IP addresses of all of the computers on your internal network
- External_All on the external address list represents the IP addresses of all of the computers on the Internet

You can add, edit, and delete all other addresses as required.

This section describes:

- [Adding addresses](#)
- [Editing addresses](#)
- [Deleting addresses](#)

Adding addresses

To add an address using the web-based manager:

- Go to *Firewall > Address* .
- Select the interface to which to add the address.
The list of addresses added to that interface is displayed.
- Select New to add a new address to the selected interface.
- Enter an Address Name to identify the address.
The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and other special characters are not allowed.
- Add the IP Address.
The IP Address can be the IP address of a single computer (for example, 192.45.46.45) or the address of a subnetwork (for example, 192.168.1.0).
The address must be a valid address for one of the networks or computers connected to the interface.
- Add the NetMask.
The Netmask should correspond to the address. The Netmask for the IP address of a single computer should be 255.255.255.255. The Netmask for a subnet should be 255.255.255.0.
- Select OK to add the address.

Example address

The screenshot shows a web-based manager interface with two tabs: 'Internal' and 'External'. The 'Internal' tab is selected. A dialog box titled 'New Internal Address' is open, containing three input fields: 'Address Name' (Web_Server), 'IP Address' (192.168.2.3), and 'NetMask' (255.255.255.250). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Editing addresses

Edit an address to change its IP address and Netmask. You cannot edit the address name. If you need to change an address name, you must delete the address and then re-add it with a new name.

Using the web-based manager:

- Go to *Firewall > Address* .
- Select the interface with the address you want to edit.
- Choose an address to edit and select Edit  .
- Make the required changes and select OK to save your changes.

Deleting addresses

Delete an address to make it unavailable for use by policies. If an address is included in any policy, it cannot be deleted unless it is first removed from the policy. See [Editing policies](#).

- Go to *Firewall > Address* .
- Select the interface list containing the address you want to delete.
- Choose an address to delete and select delete  .
- Click OK to delete the address.

Adding virtual IPs

NAT mode security policies hide the addresses in more secure networks from less secure networks. To allow connections from a less secure network to a more secure network, you must make an association between a destination address in the less secure network and an actual address in the more secure network. This association is called a virtual IP.

By default virtual IPs are required for Ext to Int NAT mode policies.

Example virtual IP

Your web server has an IP address on the Internet, but the computer hosting your web server is located on your internal network with a private IP address. To get packets from the Internet to your web server, you must create a virtual IP that associates the Internet address of your web server with its actual IP address. The actual address of the web server is called the mapping IP.

Once you have created a virtual IP, you can add policies to allow access to the mapping IP by adding the virtual IP to the destination address of the Ext to Int policy that provides users on the Internet with access to the web server.

Adding Virtual IPs

To add a virtual IP:

- Go to *Firewall > Virtual IP* .
- Select New to add the virtual IP.
- Enter a Name for the virtual IP.
The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- In the IP Address field, enter the IP address of the server on the internal network.

For example, if the virtual IP is for a web server the IP address must be a static IP address obtained from your ISP for your web server and must not be the same as the external address of the DFL-500. However, your ISP must route this address to the external interface of the DFL-500.

- In the Map to IP field, enter the actual IP address of the web server.
- Select OK to save the Virtual IP.
- Repeat these steps to add Virtual IPs as needed.

Adding a Virtual IP

Services

Use services to control the types of communication accepted or denied by the firewall. You can add any of the pre-configured services listed in [DFL-500 pre-defined services](#) to a policy. You can also create your own custom services and add services to service groups.

This section describes:

- [Pre-defined services](#)
- [Providing access to custom services](#)
- [Grouping services](#)

Pre-defined services

The DFL-500 pre-defined firewall services are listed in [DFL-500 pre-defined services](#). You can add these services to any policy.

DFL-500 pre-defined services				
Service name	Description	Protocol	Source Port	Destination port
ANY	Match connections on any port.	all	1-65535	all
DNS	Domain name servers for looking up domain names.	tcp	1-65535	53
		udp	1-65535	53
FINGER	Finger service.	tcp	1-65535	79
FTP	FTP service for transferring files.	tcp	1-65535	20-21
GOPHER	Gopher communication service.	tcp	1-65535	70
HTTP	HTTP service for connecting to web pages.	tcp	1-65535	80

HTTPS	SSL service for secure communications with web servers.	tcp	1-65535	443
IMAP	IMAP email protocol for reading email from an IMAP server.	tcp	1-65535	143
IRC	Internet relay chat for connecting to chat groups.	tcp	1-65535	6660-6669
NFS	Network file services for sharing files.	tcp	1-65535	111 2049
		udp	1-65535	111 2049
NNTP	Protocol for transmitting Usenet news.	tcp	1-65535	119
NTP	Network time protocol for synchronizing a computer's time with a time server.	tcp	1-65535	123
		udp	1-65535	123
PING	For testing connections to other computers.	icmp	1-65535	0 8
POP3	POP3 email protocol for downloading email from a POP3 server.	tcp	1-65535	110
		udp	1-65535	110
QUAKE	For connections used by the popular Quake multi-player computer game.	udp	1-65535	26000 27000 27910 27960
RAUDIO	For streaming real audio multi-media traffic.	udp	1-65535	7070
RLOGIN	Rlogin service for remotely logging into a server.	tcp	1-65535	513
SMTP	For sending mail between email servers on the Internet.	tcp	1-65535	25
SNMP	For communicating system status information.	tcp	1-65535	161-162
		udp	1-65535	161-162
SSH	SSH service for secure connections to computers for remote management.	tcp	1-65535	22
		udp	1-65535	22
TELNET	Telnet service for connecting to a remote computer to run commands.	tcp	1-65535	23
VDOLIVE	For VDO Live streaming multimedia traffic.	udp	1-65535	7000
WAIS	Wide Area Information Server. An Internet search protocol.	tcp	1-65535	210
X-WINDOWS	For remote communications between an X-Window server and X-Window clients.	tcp	1-65535	6000

Providing access to custom services

Add a custom service if you need to create a policy for a service that is not in the predefined services list.

To add a custom service:

- Go to *Firewall > Service > Custom* .
- Select *New*.
- Enter a Name for the service. This name appears in the service list used when you add a policy.

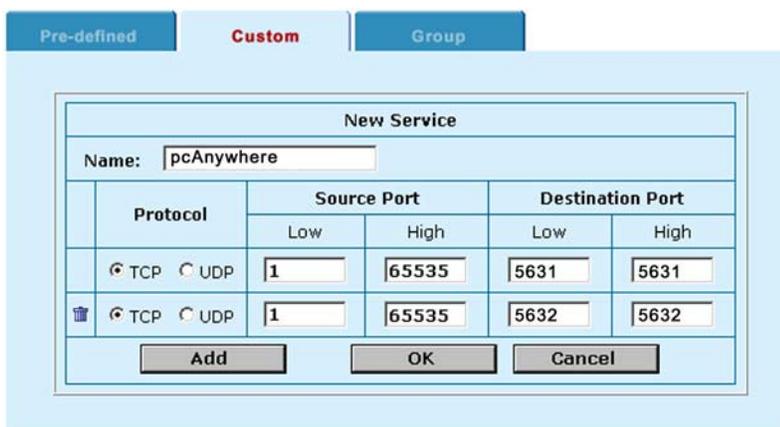
The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

- Select the protocol (either TCP or UDP) used by the service.
- Specify a port number range for the service by typing in the low and high port numbers. If the service uses one port number, type this number into both the Low and High fields.
- If the service has more than one port range, select Add to specify additional protocols and port ranges.

If you mistakenly add too many port range rows, select delete  to remove the extra row.

- Select OK to add the custom service.
You can now add this custom service to a policy (see [Adding policies](#)).

Sample pcAnywhere custom service



New Service				
Name: <input type="text" value="pcAnywhere"/>				
Protocol	Source Port		Destination Port	
	Low	High	Low	High
<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text" value="1"/>	<input type="text" value="65535"/>	<input type="text" value="5631"/>	<input type="text" value="5631"/>
 <input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text" value="1"/>	<input type="text" value="65535"/>	<input type="text" value="5632"/>	<input type="text" value="5632"/>

Example custom service

The custom service shown in [Sample pcAnywhere custom service](#) can be added to a policy to allow pcAnywhere, a popular program for allowing users remote control access to a PC, connections to be accepted by the DFL-500. Adding this service to an Ext to Int policy would allow a user on the Internet to use pcAnywhere to connect to one or more computers on the internal network.

The pcAnywhere server program uses TCP port 5631 and UDP port 5632 for communication.

If you have security concerns about adding a policy for a custom service such as pcAnywhere, you can configure the policy to restrict the source and destination addresses of the connection. This will restrict the users that can connect through the firewall using pcAnywhere, and will also restrict the addresses that they can connect to.

Grouping services

To make it easier to add policies, you can create groups of services and then add one policy to provide access to or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. You cannot add service groups to another service group.

To add a service group using the web-based manager:

- Go to *Firewall > Service > Group* .
- Select New.
- Enter a Group Name to identify the group. This name appears in the service list used when you add a policy.

The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

Adding a service group



- To add services to the service group, select a service from the Available Services list and select the right arrow to copy it to the Members list.
- To remove services from the service group, select a service from the Members list and select the left arrow to remove it from the group.
- Select OK to add the service group.

Schedules

Use scheduling to control when policies are active or inactive. You can create one-time schedules and recurring schedules. You can use one-time schedules to create policies that are effective once for the period of time specified in the schedule. Recurring schedules repeat weekly. You can use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.

This section describes:

- [Creating one-time schedules](#)
- [Creating recurring schedules](#)
- [Adding a schedule to a policy](#)

Creating one-time schedules

You can create a one-time schedule that activates or deactivates a policy for a specified period of time. For instance, your firewall may be configured with the default Internal to External policy that allows access to all services on the Internet at all times. You can add a one-time schedule to block access to the Internet during a holiday period. The following procedure describes how to create a one-time schedule with a start date at the start of the holiday and an end date at the end of the holiday.

To create a one-time schedule using the web-based manager:

- Go to *Firewall > Schedule > One-time* .
- Select New.
- Type in a name for the schedule.

The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.

- Set the Start date and time for the schedule.
Set start and stop times to 00 for the schedule to cover the entire day.
- Set the Stop date and time for the schedule.



Note: One-time schedules use the 24-hour clock.

- Select OK to add the One-time schedule.

Sample one-time schedule

New One-time Schedule					
Name	Holiday				
	Year	Month	Day	Hour	Minute
Start	2002	04	03	00	00
Stop	2002	04	05	00	00
OK			Cancel		
Notes: start time should be earlier than stop time.					

Creating recurring schedules

You can create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For instance, you may wish to prevent internet use outside of working hours by creating a recurring schedule.

If you create a recurring schedule with a stop time that occurs before the start time, the schedule will start at the start time and finish at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. You can also create a recurring schedule that runs for 24 hours by setting the start and stop times to the same time.

To add a recurring schedule:

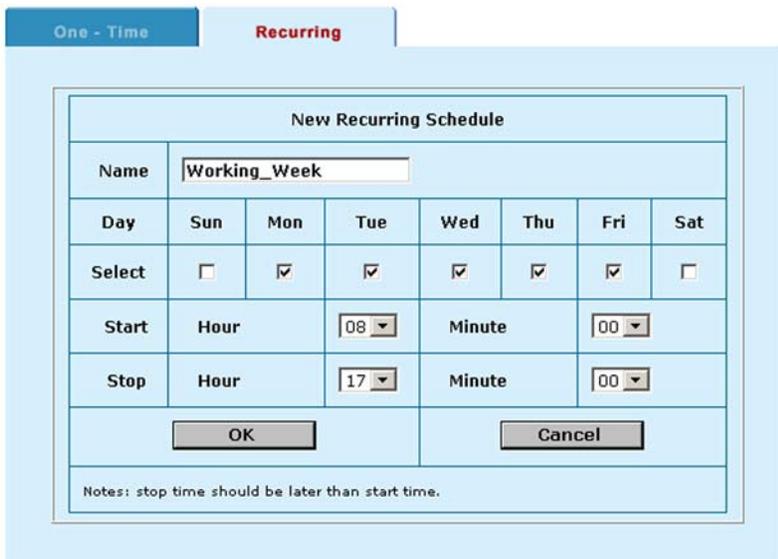
- Go to **Firewall > Schedule > Recurring**.
- Select New to create a new schedule.
- Type in a name for the schedule.
The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- Select the days of the week that are working days.
- Set the Start Hour and the End Hour to the start and end of the work day.



Note: Recurring schedules use the 24-hour clock.

- Select OK.

Sample recurring schedule



New Recurring Schedule							
Name	Working_Week						
Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Select	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Start	Hour		08	Minute		00	
Stop	Hour		17	Minute		00	
OK				Cancel			
Notes: stop time should be later than start time.							

Adding a schedule to a policy

Once you have created schedules, you can add them to policies to schedule when the policies are active. You can add the new schedules to policies when you create the policy or you can edit existing policies and add a new schedule to them.

To add a schedule to a policy:

- Go to *Firewall > Policy* .
- Select the tab corresponding to the type of policy to add.
- Select New to add a policy or select Edit  to edit a policy to change its schedule.
- Configure the policy as required.
- Add a schedule by selecting it from the Schedule list.
- Select OK to save the policy.
- Arrange the policy in the policy list to have the effect that you expect.

For example, to use a one-time schedule to deny access to a policy, add a policy that matches the policy to be denied in every way. Choose the one-time schedule that you added and set Action to Deny. Then place the policy containing the one-time schedule in the policy list above the policy to be denied.

Arranging a one-time schedule in the policy list to deny access

Order	Source	Dest	Schedule	Service	Action
1	Internal_All	External_All	Always	FTP	DENY
2	Internal_All	External_All	Always	ANY	ACCEPT

Users and authentication

You can configure the DFL-500 to require users to authenticate (enter a user name and password) to access HTTP, FTP, or Telnet services through the firewall. To configure authentication you need to add user names and passwords to the firewall and then add policies that require authentication. When a connection attempt is

matched by a policy requiring authentication, the user requesting the connection must enter a valid user name and password to be allowed to connect through the firewall.

 **Note:** Authentication is not supported in Transparent mode.

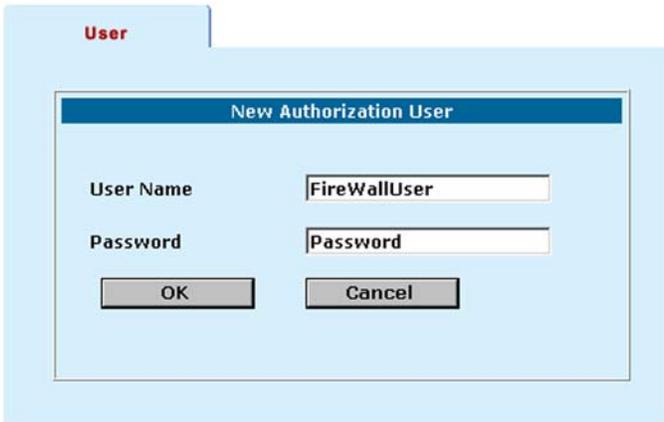
This section describes:

- [Adding user names and passwords](#)
- [Setting authentication time out](#)
- [Adding authentication to a policy](#)

Adding user names and passwords

- Go to *Firewall > Users* .
- Select New.

Adding a user name and password



- Enter a User Name and Password.
The user name and password should be at least six characters long. The user name and password can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Select OK.

Setting authentication time out

To set authentication time out:

- Go to *System > Config > Options* .
- Set Auth Timeout to control how long authenticated connections can remain idle before users have to authenticate again to get access through the firewall.

The default authentication time out is 15 minutes.

Adding authentication to a policy

Once you have added users and passwords to the firewall, you can include authentication in policies. You can add authentication when you create the policy or you can edit existing policies and change action to AUTH.

To add authentication to a policy:

- Go to *Firewall > Policy* .

- Select the tab corresponding to the type of policy to which to add authentication.
- Select New to add a policy or select Edit  to edit a policy to add authentication.
- Configure the policy as required.
- Set Action to AUTH.
- Set Service to HTTP, FTP, or Telnet.
- Select OK to save the policy
- Arrange the policy in the policy list to have the effect that you expect.

Policies that require authentication must be added to the policy list above matching policies that do not, otherwise the policy that does not require authentication is selected first.

Port forwarding

Port forwarding routes packets that are received by the DFL-500 external interface according to the packet's destination service port. When the packet is intercepted, the firewall changes the packet's destination address to an address on the network connected to the internal interface. The DFL-500 then forwards the packet to the server at that address.

You can also configure port forwarding to change the packet's destination service port.

Use port forwarding to provide Internet users with access to web, mail, ftp or other servers behind your DFL-500. When you use the setup wizard for internal server settings, you are configuring port forwarding for the services that you select.

Firewall policies take precedence over port forwarding. If you have configured port forwarding for a service, you can add a policy to deny access to this service.



Note: Port Forwarding is not supported in Transparent mode.

Port forwarding example

Configure port forwarding for the external interface so that all FTP packets (using port 20) have their destination IP address changed from an Internet IP address to the IP address of an FTP server on your internal network:

- FTP packets received by the external interface could have the following settings:
Source: 163.158.1.2/7890, Dest: 194.160.1.1/20
- FTP port forwarding could change the settings to:
Source: 163.158.1.2/7890, Dest: 192.168.1.2/20
- Replies from the FTP server would have the following settings:
Source: 192.168.1.2/20, Dest: 163.158.1.2/7890
- The DFL-500 would change these addresses to:
Source 194.160.1.1/20, Dest: 163.158.1.2/7890

Adding port forwarding

- Go to *Firewall > Port Forward* .
- Select New.
- In the External Service Port list, select the service for which to configure port forwarding.
For a list of common services and their port numbers, see [DFL-500 pre-defined services](#). You can add custom services using the procedure [Providing access to custom services](#).

- Set the Forwarded IP to the IP address of the server to which to send the packets.
- In the Forwarded Service Port list, select the service used by the packets when they are forwarded to the server. Usually you would select the same service as you selected in the External Service Port list, but you can select a different service port to have the DFL-500 change the destination port of packets before they are forwarded to the server.
- Select OK to save your changes.

Port forwarding configuration example

The screenshot shows a 'New Forward IP' dialog box. It contains three fields: 'External Service Port' (dropdown menu with 'FTP' selected), 'Forward IP' (text box with '10.10.10.5' entered), and 'Forward Service Port' (dropdown menu with 'FTP' selected). Below the fields are 'OK' and 'Cancel' buttons.

IP/MAC binding

IP/MAC binding protects the DFL-500 from IP Spoofing attacks. IP Spoofing attempts to use the IP address of a trusted computer to access the DFL-500 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.

You can enter the IP addresses and corresponding MAC addresses of trusted computers into the DFL-500 firewall configuration. When a packet arrives from a trusted IP address, it is checked to determine whether the MAC address that the packet originated from matches the MAC address in the table. The DFL-500 checks all packets received by the DFL-500 external interface. This includes packets addressed to the external interface and packets passing through the firewall.

 **Note:** IP/MAC binding is not supported in Transparent mode.

You can configure IP/MAC binding so that the DFL-500 lets traffic with a source address not found in the IP/MAC binding table pass through the firewall. Any traffic with a source address that is defined in the IP/MAC binding table must have the correct MAC address or it is blocked. You can also configure the DFL-500 to block all traffic with a source address that is not found in the IP/MAC binding table, and to only allow traffic with a source address in the IP/MAC binding table if the IP address and MAC address pair matches an entry in the table.

MAC addresses are only carried on the local network where they originate, and are not passed from one network to another.

This section describes:

- [Adding IP/MAC binding addresses](#)
- [Enabling IP/MAC binding](#)

Adding IP/MAC binding addresses

- Go to *Firewall > IP/MAC Binding > IP MAC* .
- Select New to add an IP address/MAC address pair.
- Add the IP address and the MAC address.
- Select Enable to enable IP/MAC binding for this address pair.
- Select OK to save the IP/MAC binding pair.

Enabling IP/MAC binding

- Go to *Firewall > IP/MAC Binding > Setting* .
- Select Enable IP/MAC.
- Select one of the following.

Allow traffic when not defined in the table

The DFL-500 lets traffic with a source address not found in the IP/MAC binding table pass through the firewall. Any traffic with a source address that is defined in the IP/MAC binding table must have the correct MAC address or it is blocked.

Block traffic when not defined in the table

The DFL-500 blocks all traffic with a source address that is not found in the IP/MAC binding table. Any traffic with a source address that is defined in the IP/MAC binding table must have the correct MAC address or it is also blocked.

- Select Apply to save your changes.

Traffic shaping

Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the DFL-500. For example, the policy for the corporate web server might be given higher priority than the policies for most employees' computers. An employee who needs unusually high speed Internet access could have a special outgoing policy set up with higher bandwidth.

You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth to make sure that there is enough bandwidth available for a high-priority service.

You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.

Adding traffic shaping to a policy

You can add traffic shaping to any type of policy. To add traffic shaping:

- Go to *Firewall > Policy* .
- Select the tab containing the policy to which you want to add traffic shaping.
- Choose a policy to which to add traffic shaping and select Edit  .
- Select traffic shaping.
- Configure traffic shaping for the policy:

Guaranteed bandwidth

Available in a future release.

Maximum bandwidth

Available in a future release.

Traffic Priority

Select high, medium, or low. Select traffic priority so that the DFL-500 manages the relative

priorities of different types of traffic. For example, a policy for connecting to a secure web-server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low priority connections only when bandwidth is not needed for high priority connections.

- Select OK to save your changes to the policy.

Example policies

- [NAT mode policy for public access to a server](#)
- [Route mode policy for public access to a server](#)
- [Transparent mode policy for public access to a server](#)
- [Denying connections from the Internet](#)
- [Denying connections to the Internet](#)
- [Adding policies that accept connections](#)
- [Requiring authentication to connect to the Internet](#)

NAT mode policy for public access to a server

The following example NAT mode policy to accept connections from the Internet and forward them to the internal network is similar to any NAT mode policy for connections from the external network to the internal network.

To add a NAT mode Ext to Int policy:

- Add a virtual IP that maps the public IP address of the server to the actual address of the server. See [Adding virtual IPs](#).
- Go to **Firewall > Policy > Ext to INT**.
- Select New to add a new policy.
- Configure the policy.

Source	External_All
Destination	The virtual IP added in Step Add a virtual IP that maps the public IP address of the server to the actual address of the server .
Schedule	Always
Service	Select a service to match the Internet server For a web server, select HTTP
Action	ACCEPT
Reverse NAT	Select Reverse NAT

- Select OK to save the policy.

Route mode policy for public access to a server

The following example route mode policy to accept connections from the Internet and forward them to the internal network is similar to any route mode policy. In this example, the DFL-500 is running in NAT/Route mode and the mode for connections between the external and internal interfaces has been changed to route mode. You can use route mode policies for connections from the Internet to the internal network if addresses on the internal network are routable from the Internet.

To add a route mode Ext to Int policy:

- Add an address for the server to the internal address list. See [Adding addresses](#).
- Go to **Firewall > Policy > Ext to Int**.

- Select New to add a new policy.
- Configure the policy.

Source	External_All
Destination	The address added in step Add an address for the server to the internal address list.
Schedule	Always
Service	Select a service to match the Internet server For a web server, select HTTP
Action	Select ACCEPT

- Select OK to save the policy.

Transparent mode policy for public access to a server

The following example policy to accept connections at the external interface and forward them to the internal interface is similar to any Transparent mode policy.

To add a Transparent mode policy between the external interface and the internal interface:

- Add an address for the server to the internal interface address list.
See [Adding addresses.](#)
- Go to **Firewall > Policy > Ext to Int** .
- Select New to add a new policy.
- Configure the policy.

Source	External_All
Destination	The address added in step 1.
Schedule	Always
Service	Select a service to match the Internet server For a web server, select HTTP
Action	Select ACCEPT.

- Select OK to save the policy.

Denying connections from the Internet

Policies that deny connections from the Internet can control access to policies that accept connections from the Internet.

You can deny connections:

- From specific Internet addresses
- To specific internal addresses
- To specific services
- According to a one-time or recurring schedule

Using a schedule to deny access

The following example procedure to periodically deny access to a public web server to allow for regular maintenance is similar to any procedure to deny a connection that would otherwise be accepted by an existing policy. In this example, the DFL-500 is running in NAT/Route mode.

To use a schedule to deny access:

- Add a schedule for the time period during which you want to deny access.
See [Schedules](#).
- Go to **Firewall > Policy**.
- Select the tab containing the policy to which you want to deny access.
- Select Insert Policy Before  for the policy to block.
- Configure the new policy to match the policy to block with the following exceptions:
 - Select the schedule that you added in step [Add a schedule for the time period during which you want to deny access](#).
 - Set Action to DENY.
- Select OK to save the policy.

You must add the deny policy above the accept policy in the policy list. For more information, see [Policy matching in detail](#) and [Ordering policies in policy lists](#).

Example policy to use a schedule to deny access



#	Source	Dest	Schedule	Service	Action	Config
1	External_All	Internal_Server	Always	ANY	DENY	
2	External_All	Internal_Server	Always	ANY	ACCEPT	

New

Denying connections to the Internet

Policies that deny connections to the Internet from the internal network restrict the full access to the Internet granted by the default policy.

You can deny connections:

- From addresses on the internal network
- To addresses on the Internet
- To specific services
- According to one-time or recurring schedules

The following example procedure to prevent all users on the internal network from using POP3 to connect to an email server on the Internet is similar to any procedure to deny a connection that would otherwise be accepted by the default policy. In this example, the DFL-500 is running in NAT/Route mode.

To deny a connection to the Internet:

- Go to **Firewall > Policy > Int to Ext**.

If it has not been removed, the default policy should be in this policy list.

- Select Insert Policy Before  to add a new policy above the default policy.
 - Configure the policy to match the default policy with the following exceptions:
 - Set Service to POP3
 - Set Action to DENY
 - Select OK to save the policy.
- You must add the deny policy above the default policy in the policy list. For more information on arranging policies in policy lists, see [Policy matching in detail](#) and [Ordering policies in policy lists](#).

Policy to deny POP3 connections to the Internet from the internal network



Adding policies that accept connections

Policies that accept connections can be used in the following ways:

- As exceptions to policies that deny connections

For example, if a policy denies connections from a subnet, you can add a policy that accepts connections from one of the computers on the subnet. Such policies must be added to the policy list above the connections that they are exceptions to.
- As a replacement for the default policy to accept only the connections that you want the firewall to accept

You can limit access to the Internet to that allowed in the policies that you create. You must delete the default policy. If the default policy remains in the policy list, all connections that do not match a policy will be accepted by the default policy.

The following example procedure to accept connections from the internal network to the Internet is similar to any procedure to accept connections. In this example, the DFL-500 is running in NAT/Route mode.

To accept a connection to the Internet:

- Add addresses, services, or schedules as required.
- Go to **Firewall > Policy > Int to Ext**.
- Select New to add a policy.

You can also select Insert Policy Before  on a policy in the list to add the new policy above a specific policy. You would do this if you were adding an accept policy as an exception to a deny policy.

- Configure the policy to match the type of connection to accept.
Set Action to ACCEPT.

- Select OK to save the policy.

If you are using accept policies to restrict access, you must remove all general access policies, such as the default policy, that could be matched by a connection that you do not want. For more information, see [Policy matching in detail](#) and [Ordering policies in policy lists](#).

Requiring authentication to connect to the Internet

To require authentication, you must add users to the firewall configuration, see [Users and authentication](#). Then you can add policies to require users to enter a user name and password to access HTTP, FTP, or Telnet services through the DFL-500.

You can require user authentication for:

- Int to Ext and Ext to Int policies
- To selected addresses on the Internet
- Using HTTP, FTP, or Telnet services
- According to a schedule

The following example procedure requiring users on the internal network to authenticate to access HTTP servers on the Internet is similar to any procedure requiring authentication. In this example, the DFL-500 is running in NAT/Route mode.

To require authentication:

- Add user names and passwords to the firewall.

See [Users and authentication](#).

- Go to **Firewall > Policy > Int to Ext**.
- Select New to add a new policy.

You can also select Insert Policy Before  on a policy in the list to add the new policy above a specific policy.

- Configure the policy to match the type of connection for which to require authentication.

Set Service to HTTP.

Set Action to AUTH.

- Select OK to save the policy.

You must add the policy requiring authentication above the default policy and above any matching accept policies in the policy list. For more information, see [Policy matching in detail](#) and [Ordering policies in policy lists](#).

IPSec VPNs

Using IPSec Virtual Private Networking (VPN), you can join two or more widely separated private networks together through the Internet. For example, a company that has two offices in different cities, each with its own private network, can use VPN to create a secure tunnel between the offices. In addition, remote or travelling workers can use a VPN client to create a secure tunnel between their computer and an office private network.

The DFL-500 is an excellent choice for connecting a satellite office or a telecommuter to a main office VPN. Usually the main office would be protected by a high-capacity product such as the DFL-500-300. The small office requires the same security and functionality but the smaller user base makes the DFL-500 the product of choice for protecting smaller networks.

The secure IPSec VPN tunnel makes it appear to all VPN users that they are on physically connected networks. The VPN protects data passing through the tunnel by encrypting it to guarantee confidentiality. In addition, authentication guarantees that the data originated from the claimed sender and was not damaged or altered in transit.

IPSec is an internet security standard for VPN and is supported by most VPN products. DFL-500 IPSec VPNs can be configured to use Autokey Internet Key Exchange (IKE) or manual key exchange. Autokey key exchange is easier to configure and maintain than manual key exchange. However, manual key exchange is available for compatibility with third party VPN products that require it.



IPSec VPN is not supported in Transparent mode.

This chapter describes:

- [Compatibility with third-party VPN products](#)
- [Autokey IPSec VPN between two networks](#)
- [Autokey IPSec VPN for remote clients](#)
- [Viewing VPN tunnel status](#)
- [Dial-up monitor](#)
- [Manual key IPSec VPN between two networks](#)
- [Manual key IPSec VPN for remote clients](#)
- [Testing a VPN](#)
- [IPSec pass through](#)

Compatibility with third-party VPN products

Because the DFL-500 supports the IPSec industry standard for VPN, you can configure a VPN between a DFL-500 and any third party VPN client or gateway/firewall that supports IPSec VPN. To successfully establish the tunnel, the VPN settings must be the same on the DFL-500 and the third party product.

DFL-500 IPSec VPNs support:

- IPSec Internet Protocol Security standard
- Automatic IKE based on Pre-shared Key
- Manual keys that can be fully customized
- ESP security in tunnel mode
- 3DES (TripleDES) encryption
- HMAC MD5 authentication/data integrity or HMAC SHA authentication/data integrity

Autokey IPSec VPN between two networks

Use the following procedures to configure a VPN that provides a direct communication link between users and computers on two different networks. [Example VPN between two internal networks](#) shows an example VPN between the main office and a branch office of a company. Users on the main office internal network can connect to the branch office internal network and users on the branch office internal network can connect to the main office internal network. Users on the branch office network can also connect to services such as an email server running on the main office network.

Communication between the two networks takes place in an encrypted VPN tunnel that connects the two DFL-500 IPSec VPN gateways across the Internet. Users on the internal networks are not aware that when they connect to a computer on the other network that the connection runs across the Internet.

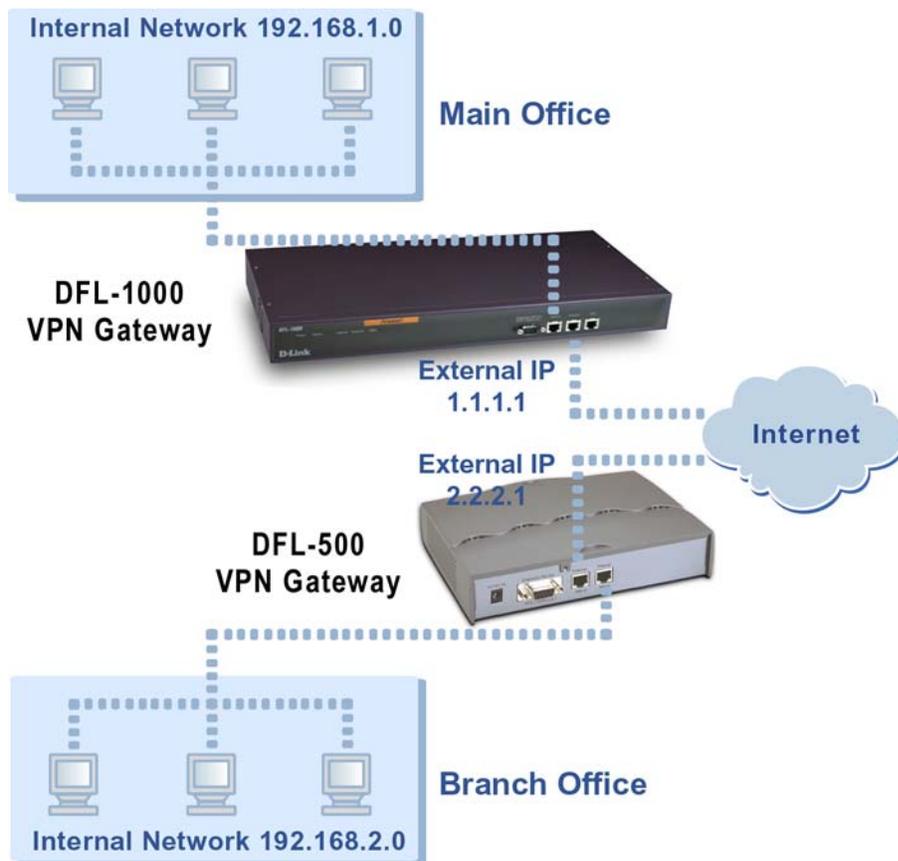
As shown in [Example VPN between two internal networks](#), the DFL-500 is designed to connect a telecommuter or small branch office network to the Internet. You can use DFL-500 IPSec virtual private networking to connect the branch office network to a main office network protected by a DFL-500 product that supports more users, such as the DFL-500-300.

You can also use the DFL-500 to connect to a network protected by a third-party VPN gateway that supports IPSec and Autokey IKE.

Use the following procedures to configure an IPSec Autokey IKE VPN between two internal networks:

- [Creating the VPN tunnel](#)
- [Adding source and destination addresses](#)
- [Adding an IPSec VPN policy](#)

Example VPN between two internal networks



Creating the VPN tunnel

A VPN tunnel consists of a name for the tunnel, the IP address of the VPN gateway at the opposite end of the tunnel, the keylife for the tunnel, and the authentication key to be used to start the tunnel. You must create complementary VPN tunnels on each of the VPN gateways. On both gateways the tunnel should have the same name, keylife, and authentication key.

[Example IPSec Autokey VPN Tunnel configuration](#) shows the information required to configure the VPN tunnel for the VPN in [Example VPN between two internal networks](#).

Example IPSec Autokey VPN Tunnel configuration			
	Description	Main Office	Branch Office
Tunnel Name	Enter a name for the tunnel. The name can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.	Branch_Office_VPN	Main_Office_VPN
Remote Gateway	The External IP address of the VPN gateway at the other end of the VPN tunnel.	2.2.2.1	1.1.1.1
P1 Proposal	Select the Encryption algorithms to propose for Phase 1 of the IPSec VPN connection. See About P1 and P2 proposals .	DES and 3DES	DES and 3DES
	Select the Authentication algorithms to propose for Phase 1 of the IPSec VPN connection.	MD5	MD5
	Specify the Keylife for Phase 1. The keylife is the amount of time in seconds before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service.	600	600
P2 Proposal	Select the encryption and authentication algorithms to propose for Phase 2 of the IPSec VPN connection. See About P1 and P2 proposals .		
	Select Enable replay detection to prevent IPSec replay attacks. See About replay detection	Select	Select
	Select Enable perfect forward secrecy (PFS) to improve the security of Phase 2 keys. See About perfect forward secrecy (PFS) .	Select	Select
	Specify the Keylife for Phase 2. The keylife is the amount of time in seconds before the phase 2 encryption key expires. When the key expires, a new key is generated without interrupting service.	600	600
	Specify the IKE Identity (also called the proxy ID) to use for the tunnel. The identity labels all IPSec packets associated with a specific tunnel so that the VPN gateway can associate IPSec packets that it receives with the correct tunnel. The default identity is IP Subnet, which means the IPSec packets associated with this tunnel are identified using the subnet IP address. You can also set Identity to IP address.	IP Subnet	IP Subnet
Authentication Key	Enter up to 20 characters. The key must be the same on both VPN gateways and should only be known by network administrators.	ddcHH01887d	ddcHH01887d
Incoming NAT	Select Incoming NAT if you require Network address translation for VPN packets.	Select	Select

About P1 and P2 proposals

IPSec VPNs use a two-phase process for creating a VPN tunnel. During the first phase (P1) the VPN gateways at each end of the tunnel negotiate to select a common algorithm for encryption and another one for authentication. When you select a P1 Proposal, you are selecting the algorithms that the DFL-500 proposes during Phase 1 negotiation. You can choose two encryption and two authentication algorithms. Usually you would choose both to make it easier for P1 negotiation, but you can restrict the choice to one if required. For negotiation to be successful, each VPN gateway must have at least one encryption algorithm and one authentication algorithm in common.

During the second phase (P2) the VPN gateways negotiate to select a common algorithm for data communication. When you select algorithms for the P2 Proposal, you are selecting the algorithms that the DFL-500 will propose during Phase 2 negotiation. Again, during P2, each VPN gateway must have at least one algorithm in common.

About replay detection

IPSec tunnels can be vulnerable to replay attacks. A replay attack occurs when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel. The attacker can use this technique to cause a denial of service (DoS) attack by flooding the tunnel with packets. The attacker could also change and then replay intercepted packets to attempt to gain entry to a trusted network.

Enable replay detection to check the sequence number of every IPSec packet to see if it has been received before. If packets arrive out of sequence, the DFL-500 discards them.

About perfect forward secrecy (PFS)

Perfect Forward Secrecy (PFS) improves the security of a VPN tunnel by making sure that each key created during Phase 2 is not related to the keys created during Phase 1 or to other keys created during Phase 2. PFS may reduce performance because it forces a new Diffie-Hellman key exchange when the Phase 2 tunnel starts and whenever the keylife ends and a new key must be generated. As a result, using PFS may cause minor delays during key generation.

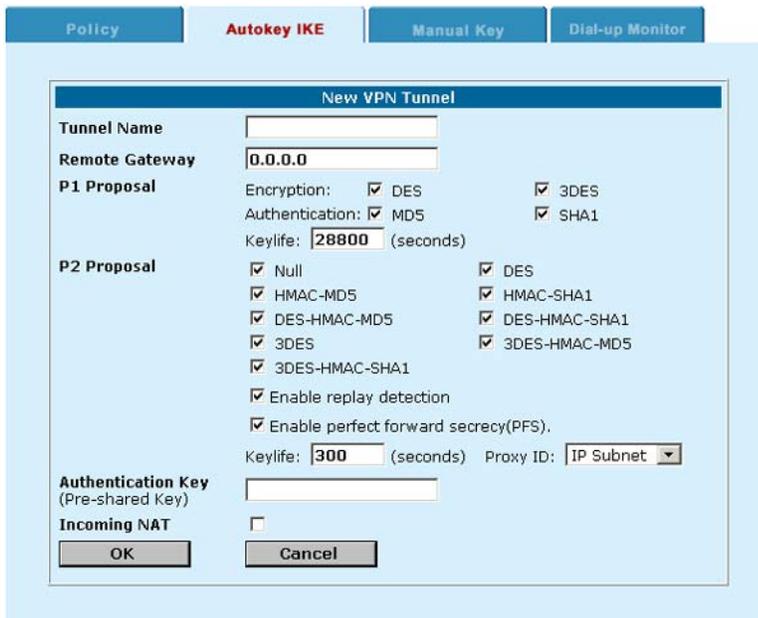
If you do not enable PFS, the VPN tunnel creates all Phase 2 keys from a key created during Phase 1. This method of creating keys is less processor intensive, but also less secure. If an unauthorized party gains access to the key created during Phase 1, all of the Phase 2 encryption keys can be compromised.

Creating the VPN tunnel

Complete the following procedure on both VPN gateways to configure a VPN tunnel that uses Autokey IKE key exchange:

- Go to *VPN > IPSEC > Autokey IKE* .
- Select New to add a new Autokey IKE VPN tunnel.
- Enter the VPN Tunnel Name, Remote Gateway, and Keylife.
- Select the P1 Proposal and P2 Proposal algorithms.
- Enter the Authentication Key.
- Select OK to save the Autokey IKE VPN tunnel.

Example Main office Autokey IKE VPN tunnel



Adding source and destination addresses

The next step in configuring the VPN is to add the addresses of the networks that are to be connected using the VPN tunnel. These address will be added to the VPN policy. On each VPN gateway, you must add two addresses:

- Source, the IP address of the network behind the local VPN gateway
The source address is an address on your internal network.
- Destination, the IP address of the network behind the other VPN gateway
The destination address is the IP address of one or more internal networks behind the destination VPN gateway.

[IPSec Autokey VPN addresses](#) shows the source and destination addresses required for the VPN in [Example VPN between two internal networks](#). In the example, both IP addresses are for internal networks.

IPSec Autokey VPN addresses			
	Description	Main office (VPN gateway 1)	Branch office (VPN gateway 2)
Source Address			
Address Name	The name to assign to the source address to be connected using the VPN. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.	Main_Office	Branch_Office
IP address	The source IP address and netmask of the network at the near end of the VPN tunnel.	192.168.1.0	192.168.2.0
Netmask		255.255.255.0	255.255.255.0
Destination Address			
Address Name	The name to assign to the destination address to be connected to using the VPN.	Branch_Office	Main_Office
IP address	The destination IP address and netmask of the network at the far	192.168.2.0	192.168.1.0

Netmask	end of the VPN tunnel.	255.255.255.0	255.255.255.0
----------------	------------------------	---------------	---------------

Complete the following procedures on both VPN gateways to add the source and destination addresses.

Adding a source address

To add the source address to the internal address list:

- Go to *Firewall > Address > Internal* .
- Select New to add a new address.
- Enter the Address Name and the IP Address and NetMask of the network that can connect to the near end of the VPN.

Example internal source address for VPN gateway 1

- Select OK to save the source address.

Adding a destination address

To add the destination address to the external address list:

- Go to *Firewall > Address > External* .
- Select New to add a new external address.
- Enter the Address Name and the IP Address and NetMask of the network behind the other VPN gateway at the far end of the VPN tunnel.
- Select OK to save the external address.

Adding an IPSec VPN policy

Add a VPN policy to associate the source and destination addresses with the VPN tunnel.

[Example IPSec Autokey VPN policy configuration](#) shows the VPN policy configuration for the VPN in [Example VPN between two internal networks](#).

Example IPSec Autokey VPN policy configuration			
	Description	Main office (VPN gateway 1)	Branch office (VPN gateway 2)
Source Address	The source address that you added for the VPN (See IPSec Autokey VPN addresses).	Main_Office	Branch_Office
Destination Address	The destination address that you added for the VPN (See IPSec Autokey VPN addresses).	Branch_Office	Main_Office
VPN Tunnel	The name of the VPN tunnel that you created for the VPN (See Example IPSec Autokey VPN	Branch_Office_VPN	Branch_Office_VPN

	Tunnel configuration).		
Incoming NAT	Select Incoming NAT if you require Network address translation for VPN packets.	Select	Select

Complete the following procedure on both VPN gateways to add the VPN policy:

- Go to *VPN > IPSEC > Policy* .
- Select New to add a new IPSec VPN policy.
- Select a Source address.
- Select a Destination address.
- Select the VPN Tunnel Name.
- Select OK to save the VPN policy.

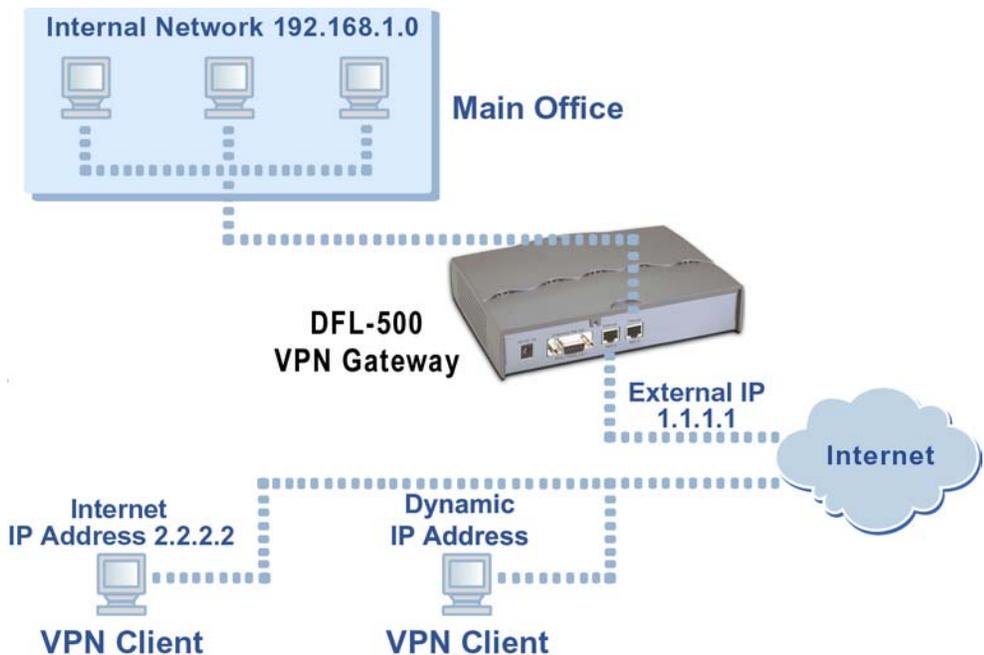
Example Main office VPN policy

Autokey IPSec VPN for remote clients

Use the following procedures to configure a VPN that allows remote VPN clients with static IP addresses to connect to users and computers on a main office internal network ([See Example VPN between an internal network and a remote client](#)). A remote VPN client can be any computer connected to the Internet with a static IP address and running VPN client software that uses IPSec and Autokey IKE.

Communication between the remote client and the internal network takes place over an encrypted VPN tunnel that connects the remote client to the DFL-500 VPN gateway across the Internet. Once connected to the VPN, the remote client computer seems to be installed on the internal network.

Example VPN between an internal network and remote clients



Use the following procedures to configure an IPsec Autokey IKE VPN that allows VPN clients to connect to an internal network:

- [Configuring the network end of the VPN tunnel](#)
- [Adding source and destination addresses](#)
- [Adding an IPsec VPN policy](#)
- [Configuring the IPsec VPN client](#)

Configuring the network end of the VPN tunnel

A VPN tunnel consists of a name for the tunnel, the remote gateway IP address (in this example, the IP address of the client), the keylife for the tunnel, and the authentication key to be used to start the tunnel.

You can either create one VPN tunnel for each VPN client, or you can create one VPN tunnel with a remote gateway address set to 0.0.0.0. This VPN tunnel can accept IPsec connections from any Internet address.

You must create complementary VPN tunnels on the VPN gateway and the clients. On both, the tunnel must have the same name, keylife, and authentication key.

[Example VPN Tunnel configuration](#) shows the information required to configure the VPN tunnel for the VPN in [Example VPN between an internal network and remote clients](#).

Example VPN Tunnel configuration		
	Description	Example Setting
Tunnel Name	Enter a name for the tunnel. The name can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.	Client_VPN
Remote Gateway	To accept connections from a client at a static IP address (for example, 2.2.2.2).	2.2.2.2
P1 Proposal	Select the Encryption algorithms to propose for Phase 1 of the IPsec VPN connection. See About P1 and P2 proposals .	DES and 3DES

	Select the Authentication algorithms to propose for Phase 1 of the IPsec VPN connection.	MD5
	Specify the Keylife for Phase 1. The keylife is the amount of time in seconds before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service.	600
P2 Proposal	Select the encryption and authentication algorithms to propose for Phase 2 of the IPsec VPN connection. See About P1 and P2 proposals .	
	Select Enable replay detection to prevent IPsec replay attacks. See About replay detection	Select
	Select Enable perfect forward secrecy (PFS) to improve the security of Phase 2 keys. See About perfect forward secrecy (PFS) .	Select
	Specify the Keylife for Phase 2. The keylife is the amount of time in seconds before the phase 2 encryption key expires. When the key expires, a new key is generated without interrupting service.	600
	Specify the IKE Identity (also called the proxy ID) to use for the tunnel. The identity labels all IPsec packets associated with a specific tunnel so that the VPN gateway can associate IPsec packets that it receives with the correct tunnel. The default identity is IP Subnet, which means the IPsec packets associated with this tunnel are identified using the subnet IP address. You can also set Identity to IP address.	IP Subnet
Authentication Key	Enter up to 20 characters. The VPN gateway and clients must have the same key and it should only be known by network administrators.	ddcHH01887d
Incoming NAT	Select Incoming NAT if you require Network address translation for VPN packets.	Select

Complete the following procedure on the DFL-500 VPN gateway:

- Go to *VPN > IPSEC > Autokey IKE* .
- Select New to add a new Autokey IKE VPN tunnel.
- Enter the VPN Tunnel Name, Remote Gateway, Keylife, and Authentication Key.
- Select the P1 Proposal and the P2 Proposal algorithms.
- Select OK to save the Autokey IKE VPN tunnel.

Adding source and destination addresses

The next step in configuring the DFL-500 VPN gateway is to add the source and destination addresses for the VPN policy. For each client VPN tunnel you require two addresses:

- Source, the IP address of the network behind the DFL-500 VPN gateway
The source address is an address on your internal network.
- Destination, the IP address of the VPN client
For VPN clients with static IP addresses, the destination address is the IP address of the client.

[See Example VPN gateway IP addresses for a client with a static IP address](#) shows the internal and external addresses required to create the VPN shown in [See Example VPN between an internal network and a remote client](#) if the client has a static IP address.

Example VPN gateway IP addresses for a client with a static IP address		
	Description	Example Setting
Source Address		
Address	The name to assign to the source address that the VPN client can connect to. The name	Main_Office

Name	can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.	
IP address	The IP address and netmask of the source address that the VPN client can connect to.	192.168.1.0
Netmask		255.255.255.0
Destination Address		
Address Name	The name to assign to the VPN client address.	VPN_Client
IP address	The IP address and netmask of a VPN client with a static IP address (for example, 2.2.2.2).	2.2.2.2
Netmask		255.255.255.255

Complete the following procedures on the DFL-500 VPN gateway to add the source and destination addresses.

Adding a source address

To add the source address to the internal address list:

- Go to *Firewall > Address > Internal* .
- Select New to add a new internal address to the list.
- Enter an Address Name, the IP Address, and the NetMask of the network to connect to the VPN.
- Select OK to save the new internal address.

Adding a destination address

To add the destination address to the external address list:

- Go to *Firewall > Address > External* .
- Select New to add the address of the client.
- Enter an Address Name, the static IP Address, and the Netmask of the client.
- Select OK to save the destination address.

Adding an IPSec VPN policy

The VPN policy associates the source and destination address with the VPN tunnel. The VPN gateway then starts up the VPN tunnel whenever it receives packets from the VPN client.

Example VPN gateway policy configuration		
	Description	Example setting
Source	The source address that you added for the VPN (See Example VPN gateway IP addresses for a client with a static IP address).	Main_Office
Destination	The destination address that you added for the client (See Example VPN gateway IP addresses for a client with a static IP address).	VPN_Client
VPN Tunnel Name	The name of the VPN tunnel to be created between the VPN gateway and the VPN client (See Example VPN Tunnel configuration).	Client_VPN
Incoming NAT	Select Incoming NAT if you require Network address translation for VPN packets.	Select

Complete the following procedure on the DFL-500 VPN gateway to add the VPN policy:

- Go to *VPN > IPSEC > Policy* .
- Select New to add a new IPSec VPN policy.
- Select a Source address.

- Select a Destination address.
- Select the VPN Tunnel.
- Select OK to save the VPN policy.

Configuring the IPSec VPN client

The VPN client PC must be running industry standard IPSec Autokey IKE VPN client software. D-Link recommends the SafeNet/Soft-PK client from IRE, Inc.

Configure the client as required to connect to the DFL-500 VPN gateway using an IPSec VPN configuration. Make sure the client configuration includes the settings in [VPN client configuration](#). These settings should match the VPN gateway configuration.

VPN client configuration		
	Description	Example Setting
Tunnel Name	Should correspond to the VPN tunnel name used on the DFL-500 VPN gateway.	Client_VPN
Remote Gateway	The External IP address of the DFL-500 VPN gateway.	1.1.1.1
Keylife	The Client key life should match the DFL-500 VPN gateway key life.	100
Authentication Key	The Client authentication key should match the DFL-500 VPN gateway authentication key.	ddcHH01887d

Dial-up VPN

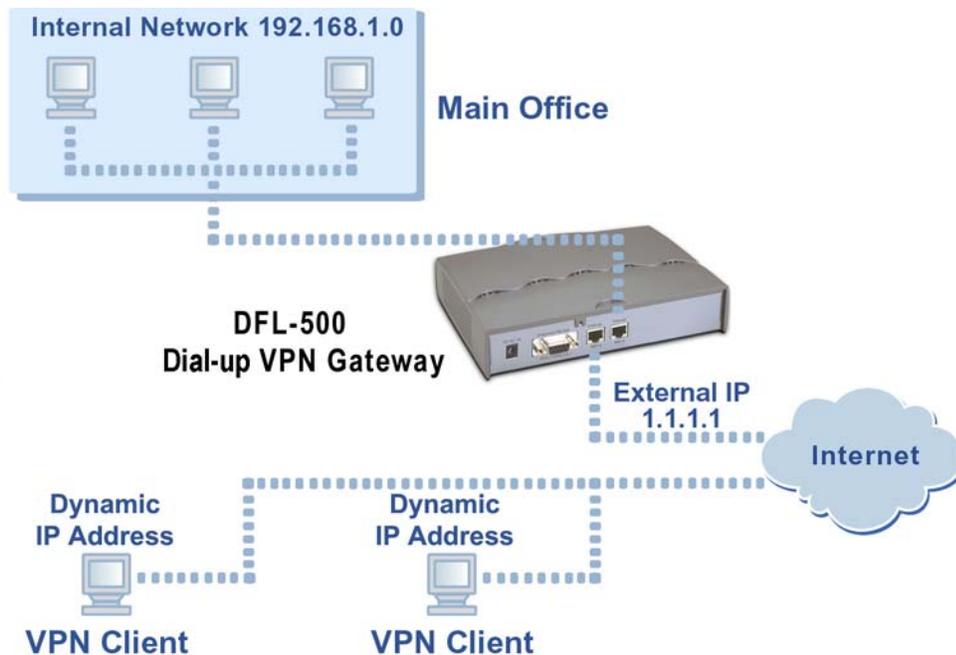
Use the following procedures to add a dial-up VPN configuration so that your VPN gateway accepts IPSec VPN connections from any IP address. A dial-up VPN configuration is most often used to allow clients with dynamic IP addresses to connect to the VPN gateway. Clients with dynamic IP addresses can be home or travelling users who dial into the Internet and are dynamically assigned an IP address by their ISP (using PPPoE, DHCP, or a similar protocol).

To configure a dial-up VPN gateway, add a dial-up VPN tunnel. A dial-up VPN tunnel is an IPSec Autokey IKE VPN tunnel with its remote gateway address set to 0.0.0.0. VPN policies and addresses are not required on the dial-up VPN gateway.

Any remote IPSec VPN client or gateway that can match the dial-up VPN tunnel's authentication key can connect to the dial-up VPN tunnel. The remote client or gateway must have a normal IPSec VPN tunnel configuration. For example, a remote DFL-500 IPSec VPN gateway must be configured with a VPN tunnel, VPN addresses, and VPN policies. Each remote client or gateway must have their VPN remote gateway set to the external address of the dial-up VPN gateway.

Each client or gateway that connects to the dial-up VPN gateway negotiates with the dial-up VPN gateway to create its own VPN tunnel. As these connections are made and the dial-up tunnels are created, they are added to the Dial-up Monitor list (see [Dial-up monitor](#)).

Example dial-up VPN configuration



Use the following procedures to create a dial-up VPN configuration:

- [Adding a dial-up VPN tunnel](#)
- [Configuring remote IPSec VPN clients](#)
- [Configuring remote IPSec VPN gateways](#)

Adding a dial-up VPN tunnel

[Dial-up VPN tunnel configuration](#) shows the information required to add a dial-up VPN tunnel to a dial-up VPN gateway.

Dial-up VPN tunnel configuration		
	Description	Example Setting
VPN Tunnel Name	The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.	Dial-up_VPN
Remote Gateway	To accept connections from any Internet address.	0.0.0.0
P1 Proposal	Select the Encryption algorithms to propose for Phase 1 of the IPSec VPN connection. See About P1 and P2 proposals .	DES and 3DES
	Select the Authentication algorithms to propose for Phase 1 of the IPSec VPN connection.	MD5
	Specify the Keylife for Phase 1. The keylife is the amount of time in seconds before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service.	600
P2 Proposal	Select the encryption and authentication algorithms to propose for Phase 2 of the IPSec VPN connection. See About P1 and P2 proposals .	
	Select Enable replay detection to prevent IPSec replay attacks. See About replay detection	Select

	Select Enable perfect forward secrecy (PFS) to improve the security of Phase 2 keys. See About perfect forward secrecy (PFS) .	Select
	Specify the Keylife for Phase 2. The keylife is the amount of time in seconds before the phase 2 encryption key expires. When the key expires, a new key is generated without interrupting service.	600
	Specify the IKE Identity (also called the proxy ID) to use for the tunnel. The identity labels all IPSec packets associated with a specific tunnel so that the VPN gateway can associate IPSec packets that it receives with the correct tunnel. The default identity is IP Subnet, which means the IPSec packets associated with this tunnel are identified using the subnet IP address. You can also set Identity to IP address.	IP Subnet
Authentication Key	Enter up to 20 characters. The VPN gateway and clients must have the same key and it should only be known by network administrators.	ddcHH01887d
Incoming NAT	Select Incoming NAT if you require Network address translation for VPN packets.	Select

Complete the following procedure on the DFL-500 dial-up VPN gateway:

- Go to *VPN > IPSEC > Autokey IKE* .
- Select New to add a new Autokey IKE VPN tunnel.
- Enter the VPN Tunnel Name, Remote Gateway, Keylife, and Authentication Key.
- Select the P1 Proposal and the P2 Proposal algorithms.
- Select OK to save the Autokey IKE VPN tunnel.

Configuring remote IPSec VPN clients

The remote VPN clients must be running industry standard IPSec Autokey IKE VPN client software. D-Link recommends the SafeNet/Soft-PK client from IRE, Inc.

Configure the client as required to connect to the dial-up VPN gateway using an IPSec VPN configuration. Make sure the client configuration includes the settings in [Remote IPSec VPN client configuration](#).

Remote IPSec VPN client configuration		
	Description	Example Setting
Tunnel Name	Should correspond to the dial-up VPN tunnel name used on the DFL-500 dial-up VPN gateway.	Dial-up_VPN
Remote Gateway	The External IP address of the dial-up VPN gateway.	1.1.1.1
Authentication Key	The client authentication key should match the dial-up VPN gateway tunnel authentication key.	ddcHH01887d

Configuring remote IPSec VPN gateways

The remote IPSec VPN gateways must be DFL-500 IPSec VPN gateways or third-party IPSec VPN gateways running industry standard IPSec Autokey IKE VPN software.

Configure the VPN gateway as required to connect to the dial-up VPN gateway using an IPSec VPN configuration. Make sure the gateway configuration includes the settings in [Remote IPSec VPN gateway configuration](#).

Remote IPSec VPN gateway configuration		
	Description	Example Setting
Tunnel Name	Should correspond to the dial-up VPN tunnel name used on the DFL-500	Dial-up_VPN

	dial-up VPN gateway.	
Remote Gateway	The External IP address of the dial-up VPN gateway.	1.1.1.1
Authentication Key	The Client authentication key should match the dial-up VPN gateway tunnel authentication key.	ddcHH01887d
VPN policies and addresses	Add as required to configure the remote gateway to connect to the dial-up VPN gateway.	

Viewing VPN tunnel status

You can use the IPSec VPN tunnel list to view the status of all IPSec Autokey IKE VPN tunnels. For each tunnel, the list shows the status of each tunnel as well as the tunnel time out.

To view VPN tunnel status:

- Go to *VPN > IPSEC > Autokey IKE*.

The Status column displays the status of each tunnel. If Status is Up, the tunnel is active. If Status is Down the tunnel is not active.

The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

Autokey IKE tunnel status

Tunnel Name	Remote Gateway	Keylife(mins)	Pre-shared Key	Status	Timeout	Modify
Client_VPN	2.2.2.2	100	ddcHH01887d	Up	87	
Branch_Office_VPN	2.2.2.1	100	ddcHH01887d	Down	0	

New

Dial-up monitor

The IPSec VPN dial-up monitor displays all of the active dial-up tunnels. A dial-up tunnel is an IPSec VPN tunnel created when a remote IPSec VPN gateway or client connects to the Autokey IKE VPN Tunnel with the IP address 0.0.0.0. This VPN tunnel accepts VPN connections from any remote IPSec VPN gateway or client as long as the remote gateway or client can match the VPN tunnel's Authentication Key.

To view the status of active dial-up tunnels:

- Go to *VPN > IPSEC > Dial-up Monitor*.

The Local IP column is always set to 0.0.0.0/0.0.0.0.

The Local Gateway column displays the IP address of the DFL-500 external interface.

The Remote Gateway column displays the IP address of the remote VPN gateway or remote IPSec VPN client connected to the tunnel.

The Remote IP column displays the IP address of the computer on the internal network behind the remote gateway.

For MD5 encryption algorithms, enter two hexadecimal numbers of 16 digits each. Use the same authentication key at both ends of the tunnel.

For SHA1 encryption algorithms, enter two hexadecimal numbers one of 16 digits and one of 20 digits. Use the same authentication key at both ends of the tunnel.

- Select OK to save the manual key VPN tunnel.

Example manual key VPN tunnel

The screenshot shows a 'New VPN Tunnel' dialog box with the following fields and values:

Field	Value
VPN Tunnel Name	Branch_Office_VPN
Local SPI	bb8ff83d (Hex)
Remote SPI	de66df78 (Hex)
Remote Gateway	2.2.2.1
Encryption Algorithm	ESP-3DES-HMAC-MD5
Encryption Key (Hex, 24 bytes)	125db62ffeac3367
	22678fbac8733672 - 38276fbaced62a33
Authentication Key (Hex, 16 bytes)	23f54a78e98d7838
	235dfbffd445433

Buttons: OK, Cancel

Adding source and destination addresses

Use the procedure [Adding source and destination addresses](#) to configure the source and destination addresses used by the VPN policy.

Adding an IPSec VPN policy

Use the procedure [Adding an IPSec VPN policy](#) to configure the VPN policy that associates the source and destination addresses with the VPN tunnel.

Manual key IPSec VPN for remote clients

Use the following procedures to configure a VPN that allows remote VPN clients to connect to computers on a Main office internal network ([See Example VPN between an internal network and remote clients](#)).



Manual key exchange VPNs do not support VPN clients with dynamic IP addresses.

The VPN client PC must have industry standard IPSec VPN client software installed. The DFL-500 VPN is based on the industry standard IPSec implementation of VPN making it interoperable with other IPSec VPN products (see [Compatibility with third-party VPN products](#)). D-Link recommends SafeNet/Soft-PK from IRE, Inc.

This section describes:

- [Configuring the VPN tunnel](#)
- [Adding internal and external addresses](#)
- [Adding an IPSec VPN policy](#)

Configuring the VPN tunnel

You can either create multiple VPN tunnels, one for each VPN client, or you can create one VPN tunnel with a remote gateway address set to 0.0.0.0. This VPN tunnel accepts connections from any Internet address.

You must create complementary VPN tunnels on the VPN gateway and the clients. On both, the tunnel must have the same name, keylife, and authentication key.

Complete the following procedure on the DFL-500 VPN gateway.

- Go to *VPN > IPSEC > Manual Key* .
- Select New to add a new manual key VPN tunnel.
- Configure the VPN tunnel as described in [See Configuring the manual key VPN tunnel](#).
- In the Remote Gateway field, enter the static IP address of the VPN client.

For the example network shown in [See Example VPN between an internal network and remote clients](#), you would use 2.2.2.2 as the remote gateway. To accept connections from more than one client, set the Remote Gateway address to 0.0.0.0.

- Select OK to save the manual key VPN tunnel.

Adding internal and external addresses

Use the procedure [See Adding source and destination addresses](#) to configure the internal and external addresses used by the VPN policy.

Adding an IPSec VPN policy

Use the procedure [See Adding an IPSec VPN policy](#) to add a VPN policy that associates the source and destination addresses of the VPN client with the VPN tunnel.

Testing a VPN

To confirm that a VPN between two networks has been configured correctly, use the ping command from one internal network to connect to a computer on the other internal network. The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the DFL-500.

To confirm that a VPN between a network and one or more clients has been configured correctly, start a VPN client and use the ping command to connect to a computer on the internal network. The VPN tunnel initializes automatically when the client makes a connection attempt. You can start the tunnel and test it at the same time by pinging from the client to an address on the internal network.

IPSec pass through

Configure IPSec pass through so that users on your internal network can connect to an IPSec VPN gateway on the Internet. IPSec pass through allows IPSec connections to pass through your DFL-500 and connect to the destination IPSec VPN gateway. The DFL-500 performs address translation on the connection, so that it seems to the destination VPN gateway that the connection to its VPN is originating from the external interface of your DFL-500.



IPSec pass through is only supported in NAT mode.

Use IPSec pass through so that:

- A visitor using your internal network can connect through your DFL-500 to their organization's VPN

- A subnet on your internal network, protected by an IPSec VPN gateway, can connect through your DFL-500 to an IPSec VPN gateway on the Internet

Other than enabling IPSec pass through, no special configuration is required for the DFL-500 that will be passed through. The VPN tunnel configuration of the VPN gateway on the Internet (or remote side) must be changed to accept connections from the IP address of the external interface of the DFL-500 that will be passed through.

This section describes how to create two IPSec pass through configurations:

- [IPSec client to network pass through](#)
- [IPSec network to network pass through](#)

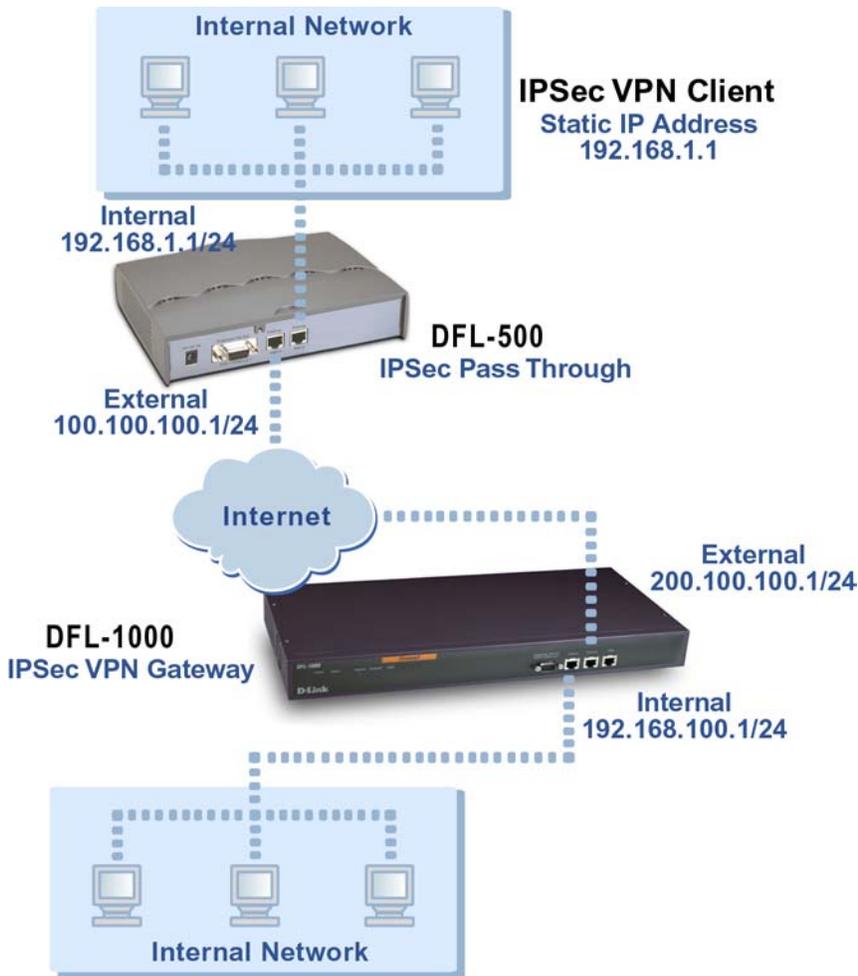
IPSec client to network pass through

In the configuration shown in [IPSec client connecting to a VPN on the Internet using VPN pass through](#), the PC on your internal network runs IPSec VPN client software and connects to a VPN gateway on the Internet. The DFL-500 is configured to pass through IPSec traffic and a DFL-500-300 functions as the remote IPSec VPN gateway.

You can substitute any suitable DFL-500 product for the IPSec VPN gateway. This gateway could also be a third-party VPN gateway.

Use the following procedures to configure the VPN client, the IPSec VPN gateway, and the DFL-500 that will be passed through.

IPSec client connecting to a VPN on the Internet using VPN pass through



Configure the IPSec VPN client

- Configure the IPSec VPN client to connect to the IPSec VPN gateway as if the client computer is connected directly to the Internet.
- Set the default gateway of the IPSec VPN client computer to 192.168.1.1, which is the IP address of the internal interface of the DFL-500 to be passed through.

Configure the IPSec VPN gateway

The administrator of the remote IPSec VPN gateway creates a standard VPN gateway configuration. However, the remote gateway address of the VPN tunnel is set to the external address of the DFL-500 to be passed through, rather than the IP address of the VPN client. Using the example in [IPSec client connecting to a VPN on the Internet using VPN pass through](#), the IP address of the remote gateway would be set to 100.100.100.1 with a netmask of 255.255.255.0.

Configure the DFL-500 for IPSec pass through

To enable IPSec pass through on the DFL-500:

- Go to *Firewall > Policy* .
- Select IPSEC Pass Through and select Apply.

When the IPsec client connects to the IPsec VPN gateway, the DFL-500 accepts IPsec VPN connections from the internal network and performs network address translation on them. The VPN packets are forwarded to the destination IPsec VPN gateway with a source address of the external interface of the DFL-500.

IPsec network to network pass through

In the configuration shown in [IPsec network to network VPN pass through](#), the DFL-500 that is configured for IPsec pass through allows the DFL-500 internal IPsec VPN gateway to connect to the DFL-500-400 Internet IPsec VPN gateway.

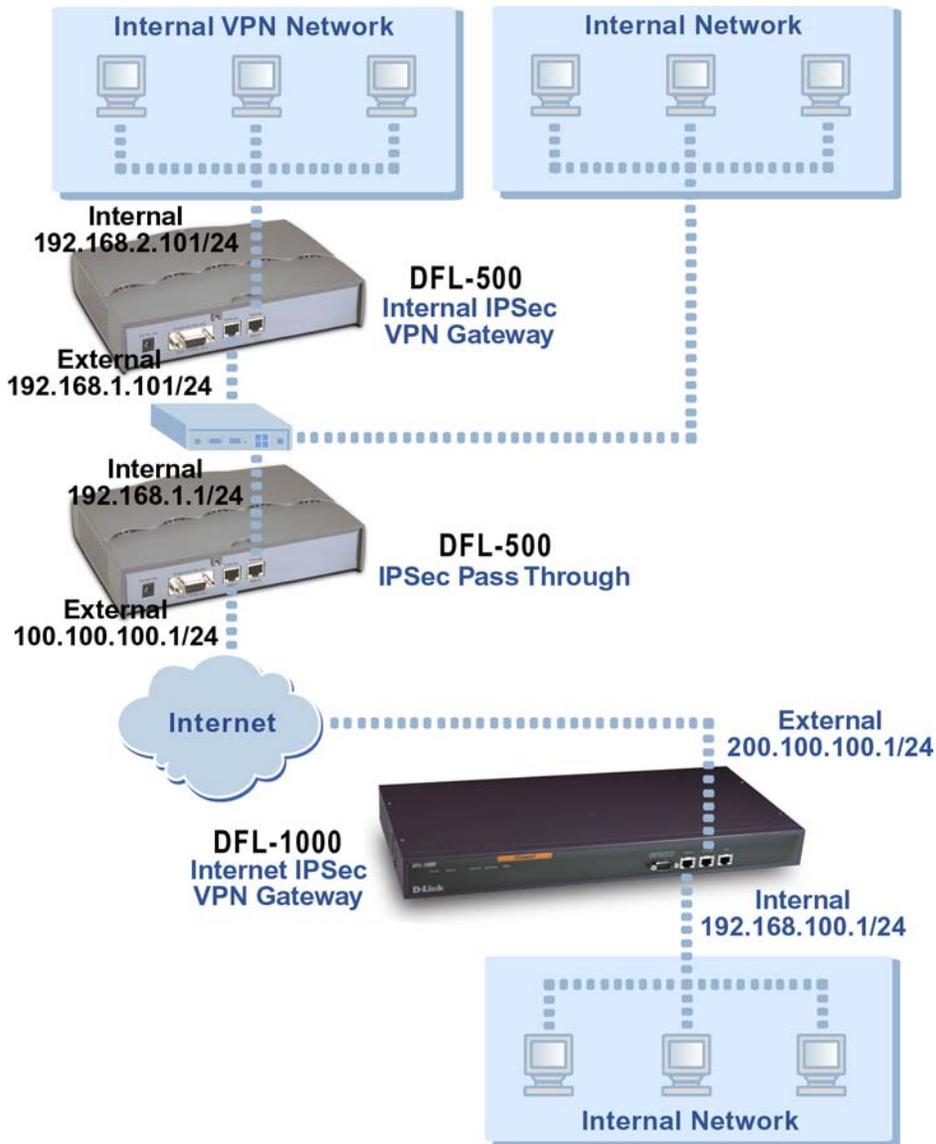
You can substitute any suitable DFL-500 product for the IPsec VPN gateways. One or both of these IPsec VPN gateways could also be a third-party VPN gateway.

Use the following procedures to configure the internal IPsec VPN gateway, the Internet IPsec VPN gateway, and the DFL-500 that will be passed through.

Configure the internal IPsec VPN gateway

Create the following configuration on the internal IPsec VPN gateway:

- Configure the internal IPsec VPN gateway to connect to the Internet IPsec VPN gateway as if the internal gateway is connected directly to the Internet. For more information, see [Autokey IPsec VPN between two networks](#). or [Manual key IPsec VPN between two networks](#)
- Go to **System > Network > IP Address** and set the default gateway of the internal IPsec VPN gateway to 192.168.1.1, which is the IP address of the internal interface of the DFL-500 to be passed through.



Configure the Internet IPsec VPN gateway

The administrator of the remote IPsec VPN gateway creates a standard VPN gateway configuration. The destination address of the VPN policy is set to the address of the internal network behind the internal IPsec VPN gateway. Using the example in [IPsec network to network VPN pass through](#), the destination address would be set to 192.168.2.0 with a netmask of 255.255.255.0.

The remote gateway address of the VPN tunnel is set to the external address of the DFL-500 to be passed through, rather than the external IP address of the internal IPsec VPN gateway. Using the example in [IPsec network to network VPN pass through](#), the IP address of the remote gateway would be set to 100.100.100.1 with a netmask of 255.255.255.255.

Configure the DFL-500 for IPsec pass through

To enable IPsec pass through on the DFL-500:

- Go to *VPN > IPSEC* .
- Select IPSEC Pass Through and select Apply.

No special VPN configuration is required. When a computer on the internal IPsec VPN network connects to the internal network behind the Internet IPsec VPN gateway, the DFL-500 accepts IPsec VPN connections from the internal network and performs network address translation on them. The VPN packets are forwarded to the destination IPsec VPN gateway with a source address of the external interface of the DFL-500.

PPTP and L2TP VPNs

Using DFL-500 PPTP and L2TP Virtual Private Networking (VPN), you can create a secure connection between a client computer running Windows and your internal network.

PPTP is a Microsoft Windows VPN standard. You can use PPTP to connect computers running Microsoft Windows to a DFL-500-protected private network without using third party VPN client software.

L2TP combines Windows PPTP functionality with IPSec security. L2TP is supported by most recent versions of MS-Windows.

VPNs protect data passing through the secure tunnel by encrypting it to guarantee confidentiality. In addition, authentication guarantees that the data originated from the claimed sender and was not damaged or altered in transit. Once connected to the VPN tunnel, it seems to the user that the client computer is directly connected to the internal network.



PPTP and L2TP VPNs are only supported in NAT mode.

This chapter describes:

- [PPTP VPN configuration](#)
- [PPTP pass through](#)
- [L2TP VPN configuration](#)
- [RADIUS authentication for PPTP and L2TP VPNs](#)

PPTP VPN configuration

You configure your DFL-500 to support PPTP by adding PPTP users and specifying a PPTP address range. You can also require PPTP VPN users to authenticate to your RADIUS server. Finally, to connect to the PPTP VPN, your remote Windows clients must be configured for PPTP.

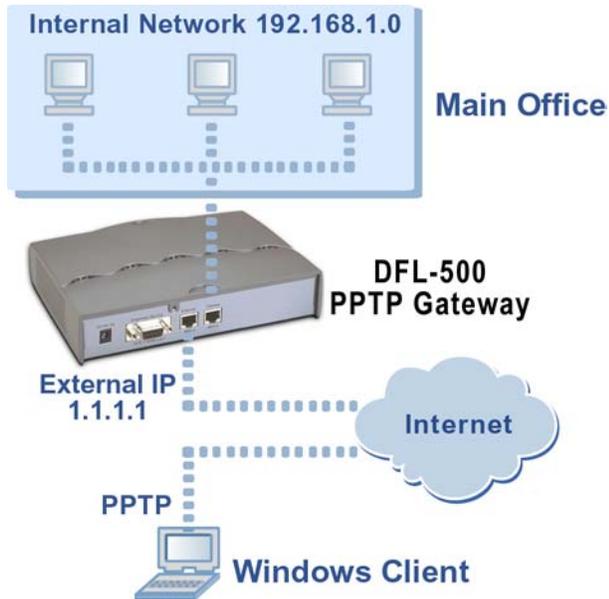


Make sure that your ISP supports PPTP connections.

This section describes:

- [Configuring the DFL-500 as a PPTP gateway](#)
- [Configuring a Windows 98 client for PPTP](#)
- [Configuring a Windows 2000 Client for PPTP](#)
- [Configuring a Windows XP Client for PPTP](#)

PPTP VPN between a Windows client and the DFL-500



Configuring the DFL-500 as a PPTP gateway

Use the following procedure to configure the DFL-500 to be a PPTP gateway:

- Go to **VPN > PPTP > PPTP User** .
- Select New to add a PPTP user name and password.
- Enter a user name and password.
The user name can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
The password must be at least 6 characters long and can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
A client can connect to the PPTP VPN with this user name and password.
- Repeat steps [Go to VPN > PPTP > PPTP User](#) . to [Enter a user name and password](#) . to add more PPTP user names and passwords as required.
- Go to **VPN > PPTP > PPTP Range** .
- Select Enable PPTP.
- Type in the Starting IP and the Ending IP for the PPTP address range.
The PPTP address range is the range of addresses on your internal network that must be reserved for remote PPTP clients. When a remote client connects to the internal network using PPTP, the computer is assigned an IP address from this range. The PPTP address range cannot overlap the L2TP address range.
- If you are planning on using RADIUS for authentication, select Enable RADIUS.
To turn on RADIUS support, see [RADIUS authentication for PPTP and L2TP VPNs](#) .
- Select Apply to enable PPTP through the DFL-500.

Sample PPTP range configuration

The screenshot shows a configuration window for PPTP. The 'PPTP Range' tab is selected. The 'Enable PPTP' radio button is chosen. The 'Starting IP' is set to 192.168.1.200 and the 'Ending IP' is set to 192.168.1.220. The 'Enable RADIUS' checkbox is checked. An 'Apply' button is located at the bottom of the configuration area.

Configuring a Windows 98 client for PPTP

Use the following procedure to configure a client machine running Windows 98 so that it can connect to a DFL-500 PPTP VPN. To configure the Windows 98 client, you must install and configure windows dial-up networking and virtual private networking support.

Installing PPTP support

- Go to *Start > Settings > Control Panel > Network* .
- Select Add.
- Choose Adapter.
- Select Add.
- Select Microsoft as the manufacturer.
- Select Microsoft Virtual Private Networking Adapter.
- Select OK twice.
- Insert diskettes or CDs as required.
- Restart the computer.

Configuring a PPTP dial-up connection

- Go to *My Computer > Dial Up Networking* .
- Double-click Make New Connection.
- Name the connection and select Next.
- Enter the external IP address or hostname of the DFL-500 to connect to and select Next.
- Select Finish.

An icon for the new connection appears in the Dial-up networking folder.

- Right-click the new icon and select Properties.
- Go to Server Types.
- Uncheck IPX/SPX Compatible.
- Select TCP/IP Settings.
- Turn off Use IP header compression.
- Turn off Use default gateway on remote network.

- Select OK twice.

Connecting to the PPTP VPN

- Start the dial-up connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Select Connect.

Configuring a Windows 2000 Client for PPTP

Use the following procedure to configure a client machine running Windows 2000 so that it can connect to a DFL-500 PPTP VPN.

Configuring a PPTP dial-up connection

- Go to *Start > Settings > Network and Dial-up Connections* .
- Double-click Make New Connection to start the Network Connection Wizard. Select Next.
- For Network Connection Type, select Connect to a private network through the Internet and select Next.
- For Destination Address, enter the external address of the DFL-500 to connect to and select Next.
- Set Connection Availability to Only for myself and select Next.
- Select Finish.
- Select Properties in the Connect window.
- Select the Security tab.
- Uncheck Require data encryption.
- Select OK.

Connecting to the PPTP VPN

- Start the dial-up connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Select Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP Client for PPTP

Use the following procedure to configure a client machine running Windows XP so that it can connect to a DFL-500 PPTP VPN.

Configuring a PPTP dial-up connection

- Go to *Start > Control Panel* .
- Select Network and Internet Connections.
- Select Create a Connection to the network of your workplace and select Next.
- Select Virtual Private Network Connection and select Next.
- Name the connection and select Next.
- If the Public Network dialog box appears, choose the appropriate initial connection and select Next.

- In the VPN Server Selection dialog, enter the external IP address or hostname of the DFL-500 to connect to and select Next.
- Select Finish.

Configure the VPN connection

- Right-click the icon that you have created.
- Select **Properties > Security** .
- Select Typical to configure typical settings.
- Select Require data encryption.
- Select Advanced to configure advanced settings.
- Select Settings.
- Select Challenge Handshake Authentication Protocol (CHAP).
- Make sure none of the other settings are selected.
- Select the Networking tab.
- Make sure the following are selected:
 - TCP/IP
 - QoS Packet Scheduler
- Make sure the following options are not selected:
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks
- Select OK.

Connecting to the PPTP VPN

- Connect to your ISP.
- Start the VPN connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Select Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

This user name and password is not the same as your VPN user name and password.

PPTP pass through

You can configure PPTP pass through so that a PPTP VPN client on your internal network can connect to a PPTP VPN gateway on the Internet. PPTP pass through allows the PPTP connection to pass through your DFL-500 and connect to the destination PPTP gateway. The DFL-500 performs address translation on the connection, so that it seems to the destination PPTP VPN gateway that the connection to its VPN is originating from the external interface of your DFL-500.

Turning on PPTP pass through is the only change you have to make to your DFL-500 configuration. No configuration changes are required for the PPTP VPN client and gateway.

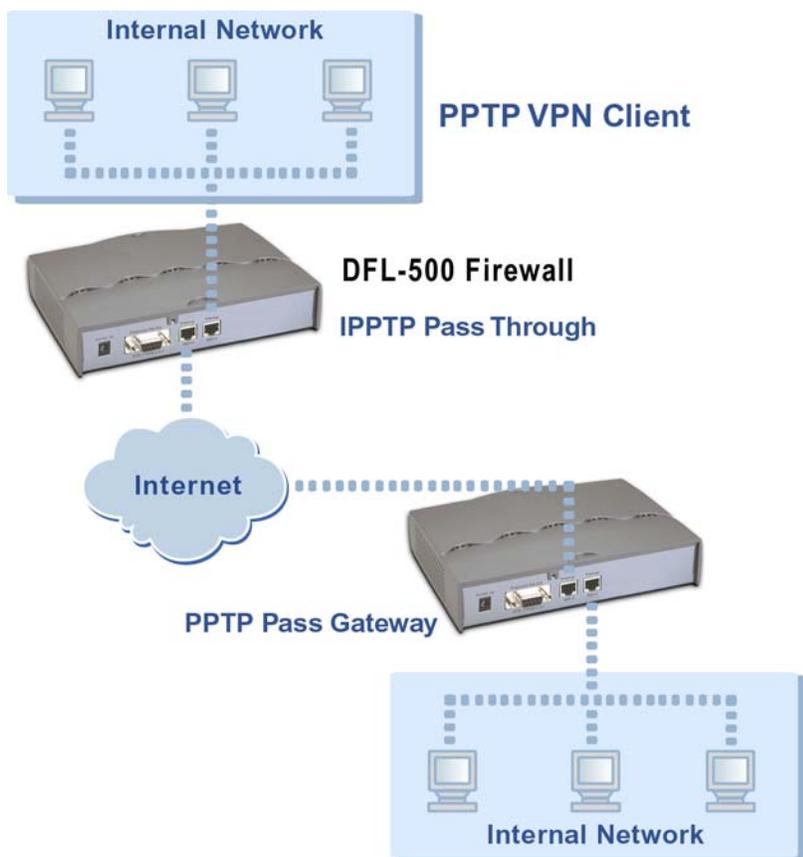
 PPTP pass through is only supported in NAT mode.

PPTP client to network pass through

In the configuration shown in [PPTP client connecting to a VPN on the Internet using PPTP pass through](#), the DFL-500 is configured for PPTP pass through. The PPTP VPN client on your internal network runs PPTP VPN client software to connect to the DFL-500-100 PPTP VPN gateway on the Internet.

You can substitute any suitable DFL-500 product for the PPTP VPN gateway. This gateway could also be a third-party PPTP VPN gateway.

PPTP client connecting to a VPN on the Internet using PPTP pass through



- Configure the PPTP VPN client to connect to the destination PPTP VPN gateway as if the client computer is connected directly to the Internet.

See the following client configuration sections:

[Configuring a Windows 98 client for PPTP](#)
[Configuring a Windows 2000 Client for PPTP](#)
[Configuring a Windows XP Client for PPTP](#)

- Set the default gateway of the PPTP VPN client computer to the internal interface of the DFL-500 to be passed through.
- Configure the PPTP VPN gateway. See [Configuring the DFL-500 as a PPTP gateway](#).
- On the DFL-500 to be passed through, go to **Firewall > Policy**.
- Select PPTP Pass Through and select Apply.

No special VPN configuration is required. When the PPTP client connects to the destination PPTP VPN gateway, the DFL-500 accepts PPTP packets from the internal network. The DFL-500 performs network address translation to change the source address of these packets to the IP address of the external interface of the DFL-500. The DFL-500 then forwards the PPTP packets to the PPTP VPN gateway.

L2TP VPN configuration

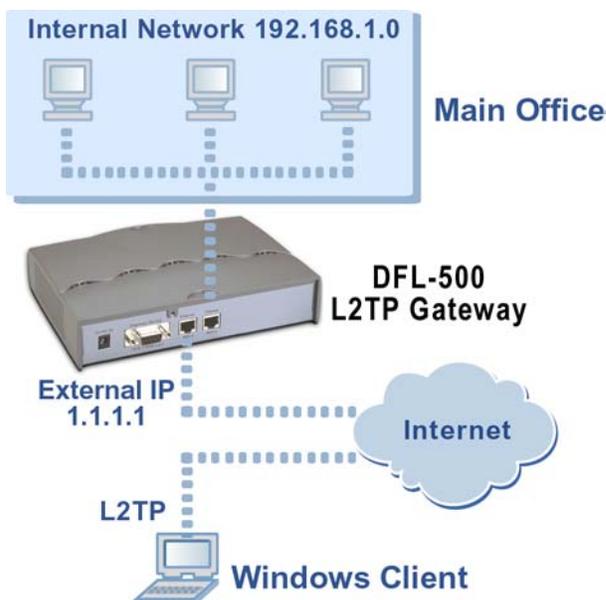
Configuring L2TP is similar to configuring PPTP. You configure the DFL-500 to support L2TP by adding L2TP users and specifying an L2TP address range. You can also require L2TP VPN users to authenticate to your RADIUS server. Finally, to connect to the L2TP VPN, your remote Windows clients must be configured for L2TP.

 Make sure that your ISP supports L2TP connections.

This section describes:

- [Configuring the DFL-500 as an L2TP gateway](#)
- [Configuring a Windows 2000 Client for L2TP](#)
- [Configuring a Windows XP Client for L2TP](#)

L2TP VPN between a Windows client and the DFL-500



Configuring the DFL-500 as an L2TP gateway

Use the following procedure to configure the DFL-500 to be an L2TP gateway:

- Go to *VPN > L2TP > L2TP User* .
- Select New to add an L2TP user name and password.
- Enter a user name and password.

The user name can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.

The password must be at least 6 characters long and can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

A client can connect to the L2TP VPN with this user name and password.

- Select OK.
- Repeat steps [Go to VPN > L2TP > L2TP User.](#) to [Select OK.](#) to add more L2TP user names and passwords as required.
- Go to **VPN > L2TP > L2TP Range .**
- Select Enable L2TP.
- Type in the Starting IP and the Ending IP for the L2TP address range.
The L2TP address range is the range of addresses on your internal network that must be reserved for remote L2TP clients. When a remote client connects to the internal network using L2TP, the computer is assigned an IP address from this range. The L2TP address range cannot overlap the PPTP address range.
- If you are planning on using RADIUS for authentication, select Enable RADIUS.
To turn on RADIUS support, see [RADIUS authentication for PPTP and L2TP VPNs.](#)
- Select Apply to enable L2TP VPNs through the DFL-500.

Sample L2TP range configuration

The screenshot shows the 'L2TP Range' configuration window. It features two tabs at the top: 'L2TP User' and 'L2TP Range'. The 'L2TP Range' tab is selected. The main area contains three radio buttons: 'Enable L2TP' (selected), 'Disable L2TP', and 'Enable RADIUS' (checked). Below these are two text input fields: 'Starting IP' with the value '192.168.1.220' and 'Ending IP' with the value '192.168.1.240'. At the bottom of the window is an 'Apply' button.

Configuring a Windows 2000 Client for L2TP

Use the following procedure to configure a client machine running Windows 2000 so that it can connect to a DFL-500 L2TP VPN.

Configuring an L2TP dial-up connection

- Go to *Start > Settings > Network and Dial-up Connections .*
- Double-click Make New Connection to start the Network Connection Wizard.
- Select Next.
- For Network Connection Type, select Connect to a private network through the Internet and select Next.
- For Destination Address, enter the external address of the DFL-500 to connect to and select Next.
- Set Connection Availability to Only for myself and select Next.
- Select Finish.
- Select Properties in the Connect window.

- Select the Security tab.
- Make sure Require data encryption is checked.
- Select the Networking tab.
- Set VPN server type to Layer-2 Tunneling Protocol (L2TP).
- Save your changes and continue with the following procedure.

Disabling IPsec

- Select the Networking tab.
- Select Internet Protocol (TCP/IP) properties.
- Double-click the Advanced tab.
- Go to the Options tab and select IP security properties.
- Make sure Do not use IPSEC is checked.
- Select OK and close the connection properties window.



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.

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

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

- Start the dial-up connection that you configured in the previous procedure.
- Enter your L2TP VPN User Name and Password.
- Select Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP Client for L2TP

Use the following procedure to configure a client machine running Windows XP so that it can connect to a DFL-500 L2TP VPN.

Configuring an L2TP VPN dial-up connection

- Go to *Start > Settings* .
- Select Network and Internet Connections.

- Select Create a connection to the network of your workplace and select Next.
- Select Virtual Private Network Connection and select Next.
- Name the connection and select Next.
- If the Public Network dialog box appears, choose the appropriate initial connection and select Next.
- In the VPN Server Selection dialog, enter the external IP address or hostname of the DFL-500 to connect to and select Next.
- Select Finish.

Configuring the VPN connection

- Right-click the icon that you have created.
- Select **Properties > Security**.
- Select Typical to configure typical settings.
- Select Require data encryption.
- Select Advanced to configure advanced settings.
- Select Settings.
- Select Challenge Handshake Authentication Protocol (CHAP).
- Make sure none of the other settings are selected.
- Select the Networking tab.
- Make sure the following are selected:
 - TCP/IP
 - QoS Packet Scheduler
- Make sure the following options are not selected:
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Disabling IPsec

- Select the Networking tab.
- Select Internet Protocol (TCP/IP) properties.
- Double-click the Advanced tab.
- Go to the Options tab and select IP security properties.
- Make sure Do not use IPSEC is checked.
- Select OK and close the connection properties window.



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

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

You must add the *ProhibitIpSec* registry value to each Windows XP-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 XP-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

- Connect to your ISP.
- Start the VPN connection that you configured in the previous procedure.
- Enter your L2TP VPN User Name and Password.
- Select Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

This user name and password is not the same as your VPN user name and password.

RADIUS authentication for PPTP and L2TP VPNs

If you have RADIUS servers installed, you can configure the DFL-500 to use RADIUS for authenticating PPTP and L2TP users. To configure RADIUS authentication, you must add the IP addresses of your RADIUS servers to the DFL-500 VPN configuration and then turn on RADIUS support for PPTP and L2TP.

If you have added PPTP and L2TP user names and passwords and configured RADIUS support, when a PPTP or L2TP user connects to a DFL-500, the user name and password is checked against the DFL-500 PPTP or L2TP user name and password list. If a match is not found locally, the DFL-500 contacts the RADIUS server for authentication.



RADIUS authentication is not supported by Windows 98 clients.

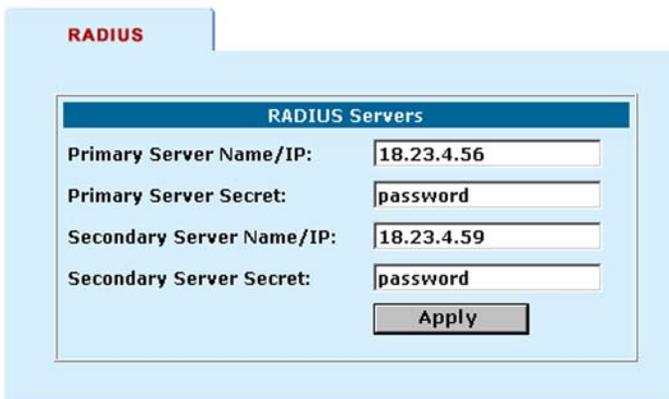
Adding RADIUS server addresses

You can install your RADIUS server on the Internet or on the internal network. No special DFL-500 configuration is required for RADIUS support for PPTP and L2TP other than what is described below. If you want non-VPN users to be able to connect to a RADIUS server installed on your internal network, you must add firewall policies to grant access to the server from the Internet.

To configure the DFL-500 for RADIUS authentication:

- Go to **VPN > RADIUS**.
- Enter the server name or IP address of your primary RADIUS server.
- Enter the primary RADIUS server secret.
- Optionally enter the server name or IP address and secret for your secondary RADIUS server.
- Select Apply.

Example RADIUS configuration



The screenshot shows a configuration window titled "RADIUS" with a sub-section "RADIUS Servers". It contains four input fields: "Primary Server Name/IP" with the value "18.23.4.56", "Primary Server Secret" with the value "password", "Secondary Server Name/IP" with the value "18.23.4.59", and "Secondary Server Secret" with the value "password". An "Apply" button is located at the bottom right of the form.

Turning on RADIUS authentication for PPTP

RADIUS authentication can be turned on separately for PPTP and L2TP. To turn on RADIUS authentication for PPTP users:

- Go to *VPN > PPTP > PPTP Range* .
- Check Enable RADIUS.
- Select Apply.

Turning on RADIUS authentication for L2TP

RADIUS authentication can be turned on separately for PPTP and L2TP. To turn on RADIUS authentication for L2TP users:

- Go to *VPN > L2TP > L2TP Range* .
- Check Enable RADIUS.
- Select Apply.

Network Intrusion detection system (NIDS)

The DFL-500 NIDS is a real-time network intrusion detection sensor that can identify a wide variety of suspicious network traffic including direct attacks, and take action as required. The NIDS uses attack signatures, stored in the attack database, to identify common attacks. In response to an attack, the NIDS protects the DFL-500 and the networks connected to it by:

- Dropping the connection
- Blocking packets from the location of the attack
- Blocking network ports, protocols, or services being used by an attack

To notify system administrators of the attack, the NIDS sends alert e-mails to up to three system administrators.

The attack database functions in a similar manner to an antivirus database. D-Link updates the attack database periodically. You can download and install attack database updates manually (see [Manual attack database updates](#)). You can also configure the DFL-500 to automatically check for and download attack database updates (see [Automatic antivirus and attack database updates](#)).

This chapter describes:

- [NIDS features](#)
- [Configuring NIDS detection](#)
- [Viewing the attack list](#)
- [Configuring NIDS responses](#)

NIDS features

The NIDS protects the DFL-500 and the networks connected to it from the attacks described below:

- [Denial of Service \(DoS\) attacks](#)
- [Reconnaissance](#)
- [Exploits](#)
- [NIDS evasion](#)

Denial of Service (DoS) attacks

Denial of service attacks attempt to deny access to a service or a computer by overloading network links, overloading the CPU, or filling up disks. The attacker is not trying to gain information, but is simply acting as a vandal to prevent users from accessing their network resources. The DFL-500 NIDS protects against the following common DoS attacks:

- Packet floods including Smurf flood, TCP SYN flood, UDP flood, and ICMP flood
- Incorrectly formed packets including Ping of Death, Chargen, Tear drop, land, and WinNuke

Reconnaissance

Reconnaissance attacks attempt to gain information about a computer network in preparation for an attempt to break into it. Using the information gained, an attacker can identify and attack specific vulnerabilities. The DFL-500 NIDS protects against the following common reconnaissance attacks:

- Fingerprinting
- Ping Sweeps
- Port Scans

- Buffer overflows including SMTP VRFY and SMTP EXPN
- Account Scans
- OS Identification

Exploits

Exploits are attempts to take advantage of features or bugs to gain unauthorized access to a computer or network. The DFL-500 NIDS protects against the following common exploits:

- Brute Force Attack
- CGI Scripts including Phf, EWS, info2www, TextCounter, GuestBook, Count.cgi, handler, webdist.cgi,php.cgi, files.pl, nph-test-cgi, nph-publish, AnyForm, and FormMail
- Web Server Attacks
- Web Browser Attacks including URL, HTTP, HTML, JavaScript, Frames, Java, and ActiveX
- SMTP (SendMail) Attack
- IMAP/POP
- Buffer Overflow
- DNS Attacks including Bind and Cache
- IP Spoofing
- Trojan Horse attacks including BackOrifice 2K, IniKiller, Netbus, NetSpy, Priority, Ripper, Striker, and SubSeven

NIDS evasion

As attackers become more sophisticated, they are developing techniques to evade NIDS systems. The DFL-500 NIDS can detect and evade the following NIDS evasion techniques:

- Signature spoofing
- Signature encoding
- IP fragmentation
- TCP/UDP disassembly

Configuring NIDS detection

To select the interface for which the NIDS monitors network traffic and to set whether or not the NIDS verifies checksums:

- Go to **NIDS > Detection > General** .
- For Monitored Interface, select the interface the NIDS monitors for network attacks. You can select only one interface. Selecting none stops NIDS monitoring.
- For Checksum Verification, check the type of traffic on which to run checksum verifications.
Checksum verification verifies that files passing through the DFL-500 have not been altered. The NIDS can run checksum verifications on IP, TCP, UDP, and ICMP traffic. For maximum protection, you can turn on checksum verification for all types of traffic. However, if the DFL-500 does not need to do checksum verification, you can turn it off for some or all types of traffic to improve performance. You may not need to run checksum verifications if your DFL-500 is installed behind a router that also does checksum verification.
- Select Apply to save your changes.

NIDS detection configuration



General Attack List

Monitored Interface: none internal external

Checksum Verifications: IP TCP UDP ICMP

Apply

Viewing the attack list

Use the following procedure to display the attacks in the current attack database:

- To display the virus list, go to *NIDS > Detection > Attack List* .
- Scroll through the virus list to view the names of all of the viruses in the list.

Configuring NIDS responses

Use the following procedures to configure NIDS responses:

- [General NIDS responses](#)
- [NIDS Alerts](#)

General NIDS responses

To configure when the NIDS sends alert messages in response to detecting an attack:

- Go to *NIDS > Responses > General* .
- Set the assurance mode for alerts:

- | | |
|----------------|--|
| All | The NIDS sends alerts for all attacks found in traffic received at the monitored interface. |
| TCP | The NIDS sends alerts only for attacks found in connections accepted by a firewall policy at the monitored interface. Select TCP Session to reduce the number of alerts generated by the NIDS. |
| Session | |

- Select Apply to save your changes.

NIDS Alerts

To configure how the NIDS reports alerts to the system administrator:

- Go to *NIDS > Responses > Alerts* .
- Check the channel to use for reporting alerts. In this release, you can select Log to record alerts on the attack log and Email to send alerts in Alert emails. SNMP will be available in a future release.
- For Message, select Summary or Full.

Summary Record a brief summary message stating the name of the attack and the source and destination addresses.

Full Record a more detailed message about the attack with details about the attack and the NIDS response.

- For Address Obfuscation, check source address, destination address, or both. When sending an alert message, the NIDS replaces the checked IP addresses of attacks with xxx.xxx.xxx.xxx.
- Select Apply to save your changes.

NIDS alerts configuration

General Alerts Logging

Channel: Log Email

Message: Summary Full

Address Obfuscation: Source IP Destination IP

Apply

Virus protection

DFL-500 antivirus protection screens the information found in web (HTTP protocol) and email content (SMTP, POP3, and IMAP protocols) as it passes through the DFL-500. The content can be contained in normal network traffic that is allowed to pass between DFL-500 interfaces as well as in IPsec VPN traffic.

Antivirus protection screens content traffic for the following types of target files that can contain viruses:

- Executable files (exe, bat, and com)
- Visual basic files (vbs)
- Compressed files (zip, gzip, tar, hta, and rar)
- Screen saver files (scr)
- Dynamic link libraries (dll)
- MS Office files that contain macros

You can configure antivirus protection to:

- Block target files

The DFL-500 removes target files and attachments that can contain viruses from content protocol data streams. You can configure antivirus protection to remove all target files or only selected target file types. You can also configure antivirus protection to remove different target file types from each content protocol. Block target files to remove all content that poses a potential threat and provide the best protection from active computer virus attacks. Blocking target files is also the only protection available from a virus that is so new that no effective virus scanner protects against it. You would not normally run the DFL-500 with blocking turned on. However, it is available for extremely high risk situations where there is no other way to prevent viruses from entering your network.

- Scan all target files for viruses

The antivirus scanning engine performs signature and macro virus scanning on all target files. If a virus is found in a file, the virus scanner deletes the file and replaces it with an alert message that is forwarded to the user. If a virus is not found, the file is forwarded unchanged to the user. Virus scanning prevents known viruses from passing through the DFL-500 and does not affect virus-free HTTP downloads and email attachments.

- Identify and remove files known to be used by worms

For each of the content protocols, you can configure antivirus protection separately for different DFL-500 traffic streams. You can configure the DFL-500 to scan all email from the Internet for viruses and worms before it is received on your internal network, while providing less protection for traffic between other more protected networks.

DFL-500 virus and worm protection is transparent to the end user. Client and server programs require no special configuration, and DFL-500 high-performance hardware and software ensure there are no noticeable download delays.

This chapter describes:

- [Configuring antivirus protection](#)
- [Worm protection](#)
- [Customize antivirus messages](#)
- [Updating your antivirus database](#)
- [Displaying virus and worm lists](#)

Configuring antivirus protection

To begin configuring antivirus protection you:

- Select the content protocol (HTTP, SMTP, POP3 or IMAP)

- Select the connection type to configure for that protocol

For each connection type you can select to protect:

- Firewall traffic
- IPSec VPN traffic

For each protocol and connection type you can turn on virus scanning or turn on and configure file blocking.

This section describes:

- [Antivirus connection types](#)
- [Configuring antivirus protection](#)

Antivirus connection types

You can configure virus protection separately for 2 traffic streams. These 2 traffic streams correspond to the 2 firewall policy types.

Antivirus protection connection types	
Connection Type	Description
Int to Ext	To protect users and servers installed on your internal network from downloading viruses from the Internet: Configure Int to Ext HTTP virus protection to prevent users on your internal network from downloading viruses from web pages Configure Int to Ext SMTP virus protection to prevent an SMTP email server on your internal network from receiving email containing viruses Configure Int to Ext POP3 and IMAP virus protection to prevent users from receiving email containing viruses when they download email from their POP3 or IMAP accounts
Ext to Int	To protect users and servers on the Internet from downloading viruses from your internal network: Configure Ext to Int HTTP virus protection if you have a web server on your internal network that can be accessed from the Internet, to prevent this web server from distributing viruses to users on the Internet Configure Ext to Int SMTP virus protection if you have an SMTP server on your internal network that can be accessed from the Internet by other SMTP servers Configure Ext to Int POP3 and IMAP virus protection if you have a POP3 or IMAP server on your internal network that is accessed by users on the Internet, to prevent these servers from distributing viruses to your remote POP3 or IMAP users

Configuring antivirus protection

To configure virus scanning:

- Go to *Anti-virus* .
- Select a content protocol (HTTP, SMTP, POP3, or IMAP) for which to configure antivirus protection.
- Select a connection type.
- Configure antivirus protection for the selected protocol and connection type.

Enable Firewall Protection

Enable antivirus protection for firewall traffic that matches the antivirus connection type that you are configuring. See [Antivirus protection connection types](#) for information about the relationship between firewall traffic and antivirus connection types.

Enable IPSEC Protection

Enable antivirus protection for IPSec VPN traffic that matches the antivirus connection type that you are configuring.

Settings

Select Scan or Block.

Scan

DFL-500 antivirus protection extracts the following files from the protocol data stream and scans

them for viruses:

- Executable files (exe, bat, and com)
- Visual basic files (vbs)
- Compressed files (zip, gzip, tar, hta, and rar)
- Screen saver files (scr)
- Dynamic link libraries (dll)
- MS Office files containing macros

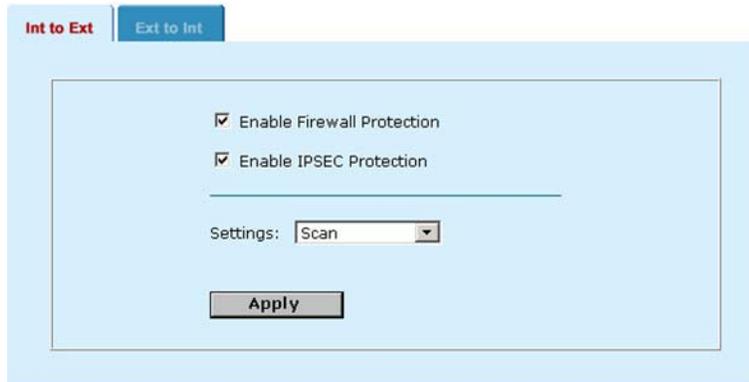
If the virus scanner finds a virus, the file is deleted from the data stream and replaced with a message informing the user that a virus was found and the file was deleted. To customize this message, see [Customize antivirus messages](#).

Block Block deletes target files from the protocol data stream. By default selecting block causes the DFL-500 to delete all target files. Configure file blocking by selecting Detail.

Detail Select Detail to configure the file types to block. You can block any of the file types listed above.

- Select OK to save your changes.

Sample antivirus configuration



Worm protection

When configured for worm protection, the virus scanning engine checks HTTP requests by scanning their originating web page for known worm patterns. For example, Code Red attempts to gain entry to MS IIS servers by trying to exploit a known buffer overflow bug in these servers.

To scan SMTP, POP3, and IMAP email attachments for worms, the virus scanning engine looks for filenames known to be used by worms. For example, the Nimda worm uses files named readme.exe and sample.exe.

To configure worm protection, choose the connection type and then turn on worm protection. You can turn on worm protection for the 2 connection types that correspond to the 2 firewall policy types.

Worm protection settings

From	To	Description
Internal	External	To protect users and servers installed on your internal network from downloading worms from the Internet.
External	Internal	To protect users and servers on the Internet from downloading worms from your internal network.

To configure worm protection:

- Go to *Anti-Virus > Config > Worm Protection*.
- Select Protection Status for each of the connection types to turn on worm protection for that connection type.

Customize antivirus messages

Use the following procedures to customize the message that appears when DFL-500 antivirus protection removes a file from a content protocol stream.

- [Customizing messages added to email](#)
- [Customizing messages added to web pages](#)

Customizing messages added to email

To configure the messages added to email:

- Go to *Anti-Virus > Config > Message*.
- Under Email, select Block Message to customize the message that appears when antivirus file blocking deletes a file from an email message.

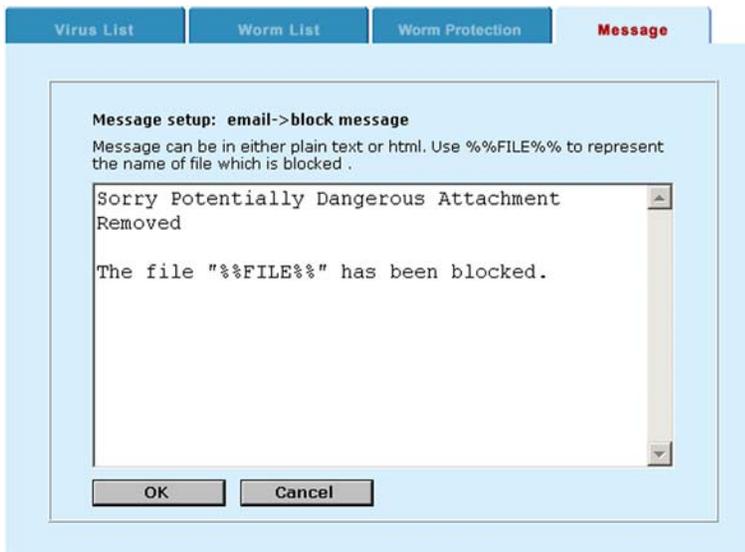
You can change the message as required. The messages can be in plain text or include html coding. Include `%%FILE%%` in the message to include the name of the file that was deleted.

- Select OK to save your changes.
- Under Email, select Infected Message to customize the message that appears when antivirus scanning detects a virus in a file contained in an email and deletes the file from the email message.

You can change the message as required. The messages can be in plain text or include html coding. Include `%%FILE%%` in the message to include the name of the file that was deleted. Include `%%VIRUS%%` in the message to include the name of the virus that was found to be infecting the file.

- Select OK to save your changes.

Default email block message



Customizing messages added to web pages

To configure the messages added to web pages:

- Go to *Anti-Virus > Config > Message*.
- Under HTTP, select Block Message to customize the message that appears when antivirus file blocking deletes a file that a user has attempted to download from a web page.

You can change the message as required. The messages can be in plain text or include html coding. Include `%%FILE%%` in the message to include the name of the file that was deleted.

- Select OK to save your changes.
- Under HTTP, select Infected Message to customize the message that appears when antivirus scanning detects a virus in a file that a user has attempted to download from a web page.
You can change the message as required. The messages can be in plain text or include html coding. Include %%FILE%% in the message to include the name of the file that was deleted. Include %%VIRUS%% in the message to include the name of the virus that was found to be infecting the file.
- Select OK to save your changes.

Updating your antivirus database

The antivirus database contains the information the virus scanning engine uses to scan files for viruses and worms. This database is continuously updated by D-Link as new viruses and worms are encountered and defined.

You should keep your antivirus database up to date so that the DFL-500 can protect your network from new viruses. You can configure the DFL-500 to update the antivirus database automatically, or you can update your antivirus database manually. See:

- [Automatic antivirus and attack database updates](#)
- [Manual antivirus database updates](#)

Displaying virus and worm lists

Use the following procedure to display the lists of viruses and worms in the current antivirus database:

- To display the virus list, go to *Anti-Virus > Config > Virus List* .
- Scroll through the virus list to view the names of all of the viruses in the list.
- To display the worm list, go to **Anti-Virus > Config > Worm List** .
- Scroll through the worm list to view the names of all of the worms in the list.

Web content filtering

Use DFL-500 Web content filtering to:

- [Block web pages that contain unwanted content](#)
- [Block access to Internet sites](#)
- [Remove scripts from web pages](#)

Block web pages that contain unwanted content

Block web pages that contain unwanted content by enabling content blocking and then creating a list of banned words and phrases. The DFL-500 blocks access to all web content that contains any of the banned words or phrases received at any interface.

You can add banned words to the list in many languages using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

This section describes:

- [Enabling the banned word list](#)
- [Changing the content block message](#)
- [Adding words and phrases to the banned word list](#)
- [Temporarily disabling the banned word list](#)
- [Temporarily disabling individual words in the banned word list](#)
- [Clearing the banned word list](#)
- [Backing up the banned word list](#)
- [Restoring the banned word list](#)

Enabling the banned word list

To turn on content blocking by enabling the banned word list:

- Go to *Web Filter > Content Block* .
- Select Enable Banned Word to turn on content blocking.
The DFL-500 is now configured to block web pages containing words and phrases added to the banned word list.

Changing the content block message

To customize the message that users receive when the DFL-500 blocks web content:

- Go to *Web Filter > Content Block* .
- Select Edit Prompt  to edit the content block message.
- Edit the text of the message. You can include HTML code in the message.
- Select OK to save your changes.
The DFL-500 will now display the message when content is blocked.

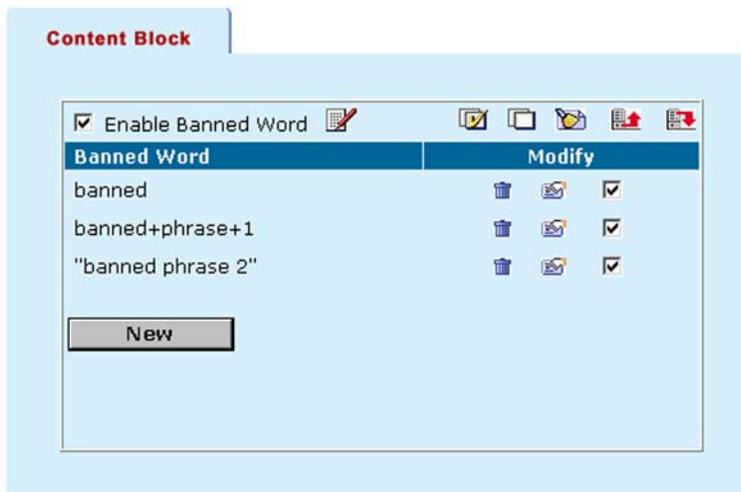
Adding words and phrases to the banned word list

To add words and phrases to the banned word list.

- Go to *Web Filter > Content Block* .

- Select New to add a word or phrase to the banned word list.
- Choose a language or character set for the banned word or phrase.
You can choose Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean.
Your computer and web browser must be configured to enter characters in the character set that you choose.
- Type a banned word or phrase.
If you type a single word (for example, *banned*), the DFL-500 blocks all web pages that contain that word.
If you type a phrase (for example, *banned phrase*), the DFL-500 blocks web pages that contain both of the words. When this phrase appears on the banned word list the DFL-500 inserts plus signs (+) in place of the spaces (*banned+phrase*).
If you type a phrase in quotes (for example, *"banned word"*), the DFL-500 blocks all web pages where the words are found together as a phrase.
Content filtering is not case-sensitive. You cannot include special characters in banned words.
- Select OK.
The word or phrase is added to the banned word list.
- Check the box beside the new entry in the banned word list so that the DFL-500 blocks web pages containing this word or phrase.
You can enter multiple banned words or phrases and then select Check All  to activate all of the entries in the banned word list.

Sample banned word list



Temporarily disabling the banned word list

- Go to *Web Filter > Content Block* .
- Uncheck Enable Banned Word to disable content blocking.

Temporarily disabling individual words in the banned word list

- Go to *Web Filter > Content Block* .
- Uncheck the box by individual entries in the banned word list.
- You can also select Uncheck All  to uncheck all of the items in the banned word list.

All unchecked items in the banned word list are not blocked by the DFL-500.

Clearing the banned word list

Use the following procedure to remove all of the entries from the banned word list.

- Go to *Web Filter > Content Block* .
- Select Delete  to remove all of the words in the banned word list.

Backing up the banned word list

If you make changes to the banned word list using the web-based manager, you can download the banned word list to a text file:

- Go to *Web Filter > Content Block* .
- Select Download Banned Word list  to download the banned word list to your management computer. The DFL-500 downloads the banned word list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Restoring the banned word list

You can restore a backed up banned word list by uploading it from your management computer to the DFL-500.

- Go to *Web Filter > Content Block* .
- Select Restore Banned Word list .
- Enter the path and filename of your banned word list text file or select Browse and locate the file.
- Select OK to upload the backed up banned word list text file.
- Select Return to display the restored list of banned words.

Block access to Internet sites

To block access to internet sites, enable URL blocking and then create a list of URLs to be blocked. The URLs in the list must include the complete domain name or IP address followed by the path and file name of the web page to block.

For example, you must specify *www.badsite.com/index.html* to block the index page of this example website. Entering *www.badsite.com* will not block the site.

Requiring the full path name means that you can choose specific parts of a web site to block. This allows you to fine tune blocking of unwanted parts of a web site without cutting off all access to otherwise useful content.

This section describes:

- [Enabling the URL block list](#)
- [Changing the URL block message](#)
- [Adding URLs to the URL block list](#)
- [Temporarily disabling the URL block list](#)
- [Temporarily disabling individual URL blocking](#)
- [Clearing the URL block list](#)
- [Downloading the URL block list](#)
- [Uploading a URL block list](#)

Enabling the URL block list

To turn on URL blocking by enabling the URL block list:

- Go to *Web Filter > URL Block* .
- Select Enable URL Block to turn on URL blocking.
The DFL-500 now blocks web pages added to the URL block list.

Changing the URL block message

To customize the message that users receive when the DFL-500 blocks web pages.

- Go to *Web Filter > URL Block* .
- Select Edit Prompt  to edit the URL block message.
- Change the text of the message. You can add HTML code to this message.
- Select OK to save your changes.
The DFL-500 will now display this message when a URL is blocked.

Adding URLs to the URL block list

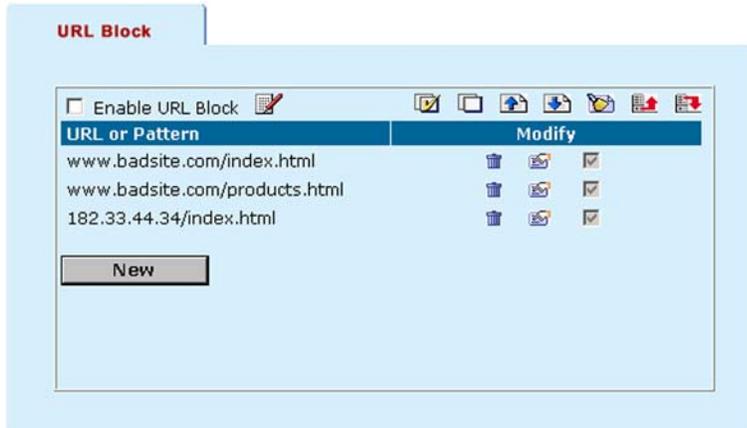
To add URLs to the URL block list:

- Go to *Web Filter > URL Block* .
- Select New to add an entry to the URL block list.
- Type the URL to block.
Enter a complete URL, including path, to block access to a page on a web site. For example, *www.badsite.com/index.html* blocks access to the main page of this example website. You can also add IP addresses, for example, *182.33.44.34/index.html* blocks access to the main web page at this address. Do not include *http://* in the URL to block.
- Select Enable to block the URL.
- Select OK to add the URL to the URL block list.
You can enter multiple URLs and then select Check All  to activate all of the entries in the URL block list.
Each page of the URL block list displays 100 URLs.
- Use Page Down  and Page Up  to navigate through the list.



You can add URLs to the URL block list by entering them into a text file and then uploading the text file to the DFL-500. See [Uploading a URL block list](#).

Sample URL block list.



Temporarily disabling the URL block list

- Go to *Web Filter > URL Block* .
- Uncheck Enable URL Block to disable URL blocking.

Temporarily disabling individual URL blocking

- Go to *Web Filter > URL Block* .
- Uncheck the box by individual URLs in the list.
- To page through the list, select Page Down or Page Up .
- You can also select Uncheck All to uncheck all of the items in the URL block list. All unchecked items in the URL block list are not blocked by the DFL-500.

Clearing the URL block list

To remove all of the URLs from the URL block list:

- Go to *Web Filter > URL Block* .
- Select Delete to remove all of the URLs from the URL block list.

Downloading the URL block list

If you make changes to the URL block list using the web-based manager, you can download the list to a text file using the following procedure:

- Go to *Web Filter > URL Block* .
- Select Download URL Block list to download the list to your management computer. The DFL-500 downloads the list to a text file on the management computer.

Uploading a URL block list

You can create a URL block list in a text editor and then upload the text file to the DFL-500. Add one URL to each line of the text file. You can follow the URL with a space and then a 1 to enable or a zero (0) to disable the URL. If you do not add this information to the text file, the DFL-500 automatically enables all of the URLs in the block list when you upload the text file.

Sample URL block list text file

```
www.badsite.com/index 1
www.badsite.com/products 1
182.63.44.67/index 1
```

You can either create the URL block list yourself, or add a URL list created by a third-party URL block or blacklist service. DFL-500 recommends downloading the squidGuard blacklists, available from <http://www.squidguard.org/blacklist/> as a starting point for creating your own URL block list. Three times a week, the squidGuard robot searches the web for new URLs to add to the blacklists. You can upload the squidGuard blacklists to the DFL-500, as a text file, with only minimal editing to remove comments at the top of each list, and to combine the lists that you want into a single file.



All changes made to the URL block list using the web-based manager are lost when you upload a new list. However, you can download your current URL list, add more URLs to it using a text editor and then upload the edited list to the DFL-500.

- In a text editor, create the list of URLs to block.
- Using the web-based manager, go to **Web Filter > URL Block**.
- Select Upload URL Block list
- Enter the path and filename of your URL block list text file, or select Browse and locate the file.
- Select OK to upload the file to the DFL-500.
- Select Return to display the updated URL block list.
Each page of the URL block list displays 100 URLs.
- Use Page Down and Page Up to navigate through the list.
- You can continue to maintain the URL block list by making changes to the text file and uploading it again.

Remove scripts from web pages

Use the following procedure to configure the DFL-500 to remove scripts from web pages. You can configure the DFL-500 to block Java Applets, Cookies, and ActiveX.

When the DFL-500 removes Java Applets, cookies, or ActiveX code from a web page, the DFL-500 writes a message to the Event log.



Blocking of any of these items may prevent some web pages from working properly.

- Go to **Web Filter > Script Filter**.
- Select the filtering options that you want to enable.
You can block Java Applets, Cookies, and ActiveX.
- Select Apply to enable script filtering.

Example script filter settings to block Java Applets and ActiveX

Script Filter

Filtering Options:

Java Applet

Cookie

ActiveX

Apply

Logging and reporting

You can configure the DFL-500 to record 3 types of logs:

- Traffic logs record all traffic that attempts to connect through the DFL-500
- Event logs record changes to the system configuration
- Attack logs record attacks intercepted by the NIDS

This chapter describes:

- [Configuring logging](#)
- [Log message formats](#)

Configuring logging

You can configure logging to record logs to one or more of the following locations:

- A computer running a syslog server
- A computer running a WebTrends firewall reporting server

You can also configure the kind of information that is logged.

- [Recording logs on a remote computer](#)
- [Recording logs on a WebTrends server](#)
- [Selecting what to log](#)

Recording logs on a remote computer

Use the following procedure to configure the DFL-500 to record logs onto a remote computer. The remote computer must be configured with a syslog server.

- Go to *Log&Report > Log setting* .
- Select Log to Remote Host to send the logs to a syslog server.
- Add the IP address of the computer running syslog server software.
- Select Apply to save your log settings.

Recording logs on a WebTrends server

Use the following procedure to configure the DFL-500 to record logs onto a remote WebTrends firewall reporting server for storage and analysis. DFL-500 log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with WebTrends Firewall Suite 4.1. Refer to the WebTrends Firewall Suite documentation for more information.

To record logs on a WebTrends server:

- Go to *Log&Report > Log setting* .
- Select Log to WebTrends.
- Add the IP address of the WebTrends firewall reporting server.
- Select Apply to save your log settings.

Example log settings

Log Setting

Log to Remote Host:

Log in WebTrends Enhanced Log Format:

Log All Internal Traffic To Firewall

Log All External Traffic To Firewall

Log All Events

Selecting what to log

Use the following procedure to configure the type of information recorded in DFL-500 logs.



When running in Transparent mode, the DFL-500 only supports Log All Events.

- Go to *Log&Report > Log setting* .
- Select Log All Internal Traffic To Firewall to record all connections to the internal interface.
- Select Log All External Traffic To Firewall to record all connections to the external interface.
- Select Log All Events to record all the changes made to the DFL-500 configuration.
- Select Apply to save your log settings.

Log message formats

The DFL-500 Traffic logs, Event logs, and Attack logs all have their own message format. All of these message formats are compatible with the WebTrends Enhanced Log Format (WELF).

Use the information in the following sections to interpret DFL-500 log messages:

- [Traffic log message format](#)
- [Event log message format](#)
- [Attack log message format](#)

Traffic log message format

When you select the Log Traffic policy option, traffic logs record sessions that match firewall policies. Each traffic log message records the date and time at which the session was started, the source and destination address of the session, and whether the session was accepted or denied by the firewall. Traffic logs do not record individual packets.

A sample traffic log message contains the following information:

```
<date> <time> src=<source IP> dst=<destination IP> proto=<destination port>  
msg="<protocol>, sport=<source port> <packet type> <action>"
```

Traffic log example messages

```
2002 Jun 19 15:35:09 src=192.168.2.1 dst=216.21.132.114 proto=80 msg="TCP, sport=3125, SYN, ACCEPT"
2002 Jun 19 16:35:09 src=192.1.1.2 dst=2.3.4.5 proto=25 msg="UDP, sport=UDP, sport=5214, ACCEPT"
```

Event log message format

Event logs record management events and activity events. Management events include changes to the system configuration as well as administrator and user logins and logouts. Activity events include system activities, such as VPN tunnel establishment, URL blocking, antivirus scanning or blocking, and so on.

Each event log message records the date and time of the event and a description of the event. For connections to the DFL-500 for management and for configuration changes, the event log message also includes the IP address of the management computer.

Management messages

All management event messages have a message type of *mgmt* , except messages that record VPN configuration changes which have the type *vpn, mgt* .

Management messages have the following format:

```
2002 Jun 19 15:35:10 type=mgmt,msg="User admin login successful at 192.168.2.2 by admin"
2002 Jun 21 20:35:09 type=mgmt,msg="Log&Report setting set successful at 192.168.100.111 by admin"
2002 Jun 19 15:23:09 type=mgmt,msg="Web-Filter banned-word add successful at 192.168.100.111 by admin"
2002 Jun 22 15:35:09 type=vpn,mgmt msg="VPN-ipsec_auto auto add successful at 192.168.100.111 by admin"
```

Antivirus messages

Antivirus event log messages record when the antivirus scanner blocks a file or detects a virus or worm in a file. Antivirus event log messages have the following format:

```
<date> <time> src=<source IP> dst=<destination IP> proto=<protocol>
msg="type=<Firewall event type> status=<status information> filename=<filename blocked/infected> virusname=<name of virus detected (infected status only)>"
```

Example antivirus event log messages:

```
2002 Jun 9 10:22:09 src=65.55.34.2 dst=192.168.100.105 proto=smtp
msg="type=Anti-Virus status=BLOCKED filename=readme.txt.vbs"
2002 Jun 11 12:35:09 src=65.55.34.2 dst=192.168.100.105 proto=http
msg="type=Anti-Virus status=INFECTED filename=readme.exe virusname=W32/Klez.h"
2002 Jun 12 10:35:09 src=65.55.34.2 dst=192.168.100.105 proto=pop3
msg="type=Anti-Virus status=INFECTED filename=readme.exe virusname=CodeRed"
2002 Jun 13 15:35:09 src=65.55.34.2 dst=192.168.100.105 proto=http
msg="type=Anti-Virus status=WORM virusname=CodeRed"
```

Content filtering messages

Content filtering messages record when content blocking or URL blocking deletes a web page from a content stream. Content filtering messages have the following format:

```
<date> <time> src=<source IP> dst=<destination IP> proto=<protocol>
msg="type=<Firewall event type> status=<status information> url=<url blocked>"
```

Example content filtering messages:

```
2002 Jun 19 23:35:09 src=25.155.34.2 dst=192.168.100.105 proto=http
msg="type=Web-Filter status=BANWORDBLOCK url=www.filtered.com/index.htm"
```

```
2002 Jun 12 15:35:02 src=23.11.34.2 dst=192.168.100.105 proto=http
msg="type=Web-Filter status=URLBLOCK url=www.filtered.com/index.htm"
```

NIDS messages

NIDS log messages record when the NIDS system detects an attack. NIDS messages have the following format:

```
<date> <time> src=<source IP> dst=<destination IP> msg="type=<Firewall event
type> attack=<description of intrusion detected>"
```

Example NIDS messages:

```
2002 Jun 22 15:23:09 src=65.55.34.2 dst=192.168.100.105 msg="type=Intrusion
attack='Tear Drop Attack' "
```

```
2002 Jun 13 12:35:09 src=65.55.34.2 dst=192.168.100.105 msg="type=Intrusion
attack='IP Spoof' "
```

```
2002 Jun 11 15:22:09 src=65.55.34.2 dst=192.168.100.105 msg="type=Intrusion
attack='SYN Flood' "
```



If the policy mode for connections in which attacks are detected is NAT, NIDS log messages contain reverse NAT IP addresses.

VPN tunnel monitor messages

VPN tunnel monitor log messages record when a VPN tunnel is started and stopped and also when keys are renegotiated. VPN tunnel monitor messages have the following format:

```
<date> <time> type=vpn, msg=<description of the VPN tunnel status event>
```

Example VPN tunnel monitor message:

```
2002 Jun 19 15:35:09 type=vpn, msg="Initiator: tunnel 172.18.0.1/172.16.0.1 main
mode phase I succeeded"
```

Attack log message format

Attack logs record attacks intercepted by the DFL-500 NIDS (see [Network Intrusion detection system \(NIDS\)](#)). Each attack log message records the date and time at which the attack was made, the type of attack, and the source and destination IP addresses of the attack. Attack log messages have the following format:

```
<date> <time> msg="<Attack type>:<protocol>, src=<source IP>, dst=<destination
IP>"
```

Example attack log message:

```
2002 Jun 19 15:35:09 msg="Sync Attack: TCP, src=1.1.1.1 dst=2.2.2.2"
```

Administration

This chapter describes how to use the DFL-500 web-based manager to administer and maintain the DFL-500. It contains the following sections:

- [Logging into the web-based manager](#)
- [System status](#)
 - [Upgrading the DFL-500 firmware](#)
 - [Manual antivirus database updates](#)
 - [Manual attack database updates](#)
 - [Displaying the DFL-500 serial number](#)
 - [Backing up system settings](#)
 - [Restoring system settings](#)
 - [Restoring system settings to factory defaults](#)
 - [Restarting the DFL-500](#)
 - [Shutting down the DFL-500](#)
 - [System status monitor](#)
- [Automatic antivirus and attack database updates](#)
- [Network configuration](#)
 - [Configuring the internal interface](#)
 - [Configuring the external interface](#)
 - [Configuring the management interface \(Transparent mode\)](#)
 - [Setting DNS server addresses](#)
 - [Configuring routing](#)
 - [Enabling RIP server support](#)
 - [Providing DHCP services to your internal network](#)
- [System configuration](#)
 - [Setting system date and time](#)
 - [Changing web-based manager options](#)
 - [Adding and editing administrator accounts](#)
 - [Configuring SNMP](#)
 - [Alert email](#)

Logging into the web-based manager

You require:

- A computer with an ethernet connection
- Internet Explorer version 4.0 or higher
- A crossover cable or an ethernet hub and two ethernet cables

To connect to the web-based manager:

- Make sure the computer from which you are going to connect to the web-based manager is correctly configured on the same network as the DFL-500 interface to which you are going to connect.
 - If the DFL-500 is running in NAT mode, connect to an interface that is configured for HTTPS management

- If the DFL-500 is running in Transparent Mode, connect to the management interface
- Start Internet Explorer and browse to the address **https://address** where **address** is the IP address of the interface to which you are connecting.

The DFL-500 login page appears.

DFL-500 login page



- Type an administrator name and password and select Login.

System status

If you log into the web-based manager using the admin administrator account you can go to **System > Status** to make any of the following changes to the DFL-500 system settings.

- [Upgrading the DFL-500 firmware](#)
- [Manual antivirus database updates](#)
- [Manual attack database updates](#)
- [Backing up system settings](#)
- [Restoring system settings](#)
- [Restoring system settings to factory defaults](#)
- [Restarting the DFL-500](#)
- [Shutting down the DFL-500](#)

If you log onto the web-based manager with any other administrator account you can go to **System > Status** to view the system settings including:

- [Displaying the DFL-500 serial number](#)

All administrative users can also go to **System > Status > Monitor** and view DFL-500 system status.

- [System status monitor](#)

Upgrading the DFL-500 firmware

D-Link releases new versions of the DFL-500 firmware periodically. You can download the upgrade from our Web site (<http://www.Dlink.com>). You can save this file on your management computer and then use one of the following procedures to upgrade the firmware on your DFL-500:

- [Upgrading the firmware using the web-based manager](#)
- [Upgrading the firmware from a TFTP server using the CLI](#)

Upgrading the firmware using the web-based manager

Using the web-based manager:

- Go to *System > Status* .
- Select Firmware Upgrade .
- Enter the path and filename of the firmware update file, or select Browse and locate the file.
- Select OK to upload the firmware update file to the DFL-500.
The DFL-500 uploads the file and restarts, running the new version of the firmware.
- Reconnect to the web-based manager.
- Go to **System > Status** and check the Firmware Version to confirm that the updated firmware has been installed successfully.

Upgrading the firmware from a TFTP server using the CLI

Use the following procedure to upgrade the DFL-500 firmware using the CLI. To run this procedure you must install a TFTP server and be able to connect to this server from the DFL-500 internal interface. The TFTP server should be on the same subnet as the internal interface. You can download a free TFTP server from: http://site.ifrance.com/freewares/P_tftpd32.htm.

 Installing new firmware using the CLI deletes all of the changes that you have made to the DFL-500 configuration and reverts the system to its default configuration, including resetting interface addresses. To keep your current settings, before installing new firmware, download your configuration file (see [Backing up system settings](#)), and your web content and URL filtering lists (see [Downloading the banned word list](#), and [Downloading the URL block list](#)).

 Installing new firmware using the CLI replaces your current antivirus database and attack database with the versions of these databases included with the firmware release that you are installing. Once you have installed new firmware see [Automatic antivirus and attack database updates](#) to make sure antivirus and attack databases are up to date.

Connecting to the DFL-500 CLI

You require:

- A computer with an available communications port
- A null modem cable with a 9-pin connector to connect to the DFL-500 Console port (RS-232 Serial connection) and to a communications port on your computer
- Terminal emulation software such as HyperTerminal for Windows

 The following procedure describes how to connect to the CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

- Connect the null modem cable to the communications port of your computer and to the DFL-500 Console port.
- Make sure the DFL-500 is powered on.
- Start HyperTerminal, enter a name for the connection, and select OK.
- Configure HyperTerminal to connect directly to the communications port on your computer into which you have connected the null-modem cable.
- Select OK.

- Select the following port settings and select OK:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- Press Enter to connect to the CLI.
The following prompt appears:
D-Link login:
- Type a valid administrator name and press Enter.
- Type the password for this administrator and press Enter.
The following prompt appears:
Type ? for a list of commands.

Upgrading the firmware

To install a firmware upgrade using the CLI:

- Make sure the TFTP server is running.
- Make sure the internal interface of the DFL-500 is connected to your internal network.
- To confirm that you can connect to the TFTP server from the DFL-500, start the DFL-500 CLI and use the following command to ping the computer running the TFTP server. If the TFTP server's IP address is 192.168.1.168:

```
> execute ping 192.168.1.168
```

- Copy the new firmware image file to the root directory of your TFTP server.
- Enter the following command to restart the DFL-500:

```
> execute reboot
```

As the DFL-500 reboots, messages similar to the following appear:

```
BIOS Version 2.2
Serial number: FGT-502801021075
SDRAM Initialization.
Scanning PCI Bus...Done.
Total RAM: 256M
Enabling Cache...Done.
Allocating PCI Resources...Done.
Zeroing IRQ Settings...Done.
Enabling Interrupts...Done.
Configuring L2 Cache...Done.
Boot Up, Boot Device Capacity=62592k Bytes.
Press Any Key To Download Boot Image.
...
```

- Quickly press any key to interrupt system startup.
The following message appears:
Enter TFTP Server Address [192.168.1.168]:

 You only have 3 seconds to press any key. If you do not press any key soon enough the DFL-500 reboots and you must log in and repeat the `execute reboot` command.

- Type the address of the TFTP server and press Enter.
The following message appears:
Enter Local Address [192.168.1.188]:

- Type the address of the internal interface of the DFL-500 and press Enter.
The following message appears:
Enter File Name [image.out]:
- Enter the firmware image file name and press Enter.
The TFTP server uploads the firmware image file to the DFL-500 and messages similar to the following appear:
*Total 7682959 Bytes Data Is Downloaded.
Testing The Boot Image Now.*

*Total 32768k Bytes Are Unzipped.
Do You Want To Save The Image ?[Y/n]*
- Type *Y*.
Programming The Boot Device Now.
.....
Read Boot Image 548405 Bytes.
Initializing Firewall ...

D-Link Login:
The installation can take a few minutes to complete.
You can then restore your previous configuration. Begin by changing the interface addresses if required. You can do this from the web-based manager or the CLI using the command:
set system interface
Once the interface addresses are changed, you can access the DFL-500 from the web-based manager and restore your configuration files and content and URL filtering lists. You should also download the most recent antivirus and attack databases (see [Automatic antivirus and attack database updates](#)).

Manual antivirus database updates

Use the following procedure to update your antivirus database manually:

 To configure the DFL-500 for automatic antivirus database updates, see [Automatic antivirus and attack database updates](#). You can also manually update your antivirus database by going to **System > Update** and selecting Update Now.

- Download the latest antivirus database from the D-Link update website at <http://www.Dlink.com> and copy it to the computer that you use to connect to the DFL-500 web-based manager.
- Start the DFL-500 web-based manager and go to **System > Status** .
- To the right of the Antivirus Database Version, select Database Update .
- Enter the path and filename for the antivirus database file, or select Browse and locate the file.
- Select OK to upload the antivirus database to the DFL-500.
The DFL-500 uploads the antivirus database. This takes about 1 minute.
- Go to **System > Status** to confirm that the Antivirus Database Version information has been updated.

Manual attack database updates

Use the following procedure to update your attack database manually:



To configure the DFL-500 for automatic attack database updates, see [Automatic antivirus and attack database updates](#). You can also manually update your attack database by going to **System > Update** and selecting Update Now.

- Download the latest attack database from the D-Link update website at <http://www.Dlink.com> and copy it to the computer that you use to connect to the DFL-500 web-based manager.
- Start the DFL-500 web-based manager and go to **System > Status** .
- To the right of the Attack Database Version, select Database Update .
- Enter the path and filename for the attack database file, or select Browse and locate the file.
- Select OK to upload the attack database to the DFL-500.
The DFL-500 uploads the attack database. This takes about 1 minute.
- Go to **System > Status** to confirm that the attack Database Version information has been updated.

Displaying the DFL-500 serial number

- Go to **System > Status** .
The Serial number is displayed in the Status window. The serial number is specific to your DFL-500 and does not change with firmware upgrades.

Backing up system settings



This procedure does not back-up the Web content and URL filtering lists. To back-up these lists see [Downloading the banned word list](#) and [Downloading the URL block list](#).

You can back-up system settings by downloading them to a text file on the management computer:

- Go to **System > Status** .
- Select System Settings Download.
- Select Download System Settings.
- Type in a name and location for the file.
The system settings file is downloaded to the management computer.
- Select Return to go back to the Status page.

Restoring system settings



This procedure does not restore the Web content and URL filtering lists. To restore these lists see [Uploading a URL block list](#) and [Creating the banned word list using a text editor](#).

You can restore system settings by uploading a previously downloaded system settings text file:

- Go to **System > Status** .
- Select System Settings Upload.
- Enter the path and filename of the system settings file, or select Browse and locate the file.
- Select OK to upload the system settings file to the DFL-500.
The DFL-500 uploads the file and restarts, loading the new system settings.
- Reconnect to the web-based manager and review your configuration to confirm that the uploaded system settings have taken effect.

Restoring system settings to factory defaults

Use the following procedure to restore system settings to the values set at the factory. This procedure does not change the DFL-500 firmware version or the Antivirus database.



This procedure deletes all of the changes that you have made to the DFL-500 configuration and reverts the system to its original configuration including resetting interface addresses.

- Go to *System > Status* .
- Select Restore Factory Defaults.
- Select OK to confirm.

The DFL-500 restarts with the configuration it had when it was first powered on.

- Reconnect to the web-based manager and review the system configuration to confirm that it has been reset to the default settings.

You can restore your system settings by uploading a previously downloaded system settings text file to the DFL-500.

Restarting the DFL-500

Use the following procedure to restart the DFL-500 using the web-based manager:

- Go to *System > Status* .
- Select Restart.

The DFL-500 restarts.

Shutting down the DFL-500

Use the following procedure to shutdown the DFL-500 using the web-based manager:

- Go to *System > Status* .
- Select Shutdown.

The DFL-500 shuts down and all traffic flow stops.

The DFL-500 can only be restarted after shutdown by turning the power off and on.

System status monitor

You can use the system status monitor to view system activity including the number of active connections to the DFL-500 and information about the connections. The connections list is divided into Route traffic connections and NAT traffic connections.

The system status monitor also displays system statistics such as CPU and memory usage.

To view system status:

- Go to *System > Status > Monitor* .
The system status monitor display appears.
- Select Refresh to update the information displayed.

System status monitor

CPU usage: 2.54% used, 97.46% idle, 0.00% interrupt.
Memory usage: 60.64% used.
Up time: 0 days, 0 hours, 55 minutes.

Protocol	From IP	From Port	To IP	To Port	Expire (secs)
Route traffic					
TCP	192.168.2.25	1110	66.88.222.131	80	897
UDP	192.168.2.25	137	206.191.0.140	53	245
TCP	192.168.2.25	1089	207.68.176.189	80	68
UDP	192.168.2.25	1086	206.191.0.140	53	247
UDP	192.168.2.25	1085	206.191.0.140	53	243
TCP	192.168.2.25	1107	205.138.3.220	80	93
TCP	192.168.2.25	1101	207.68.178.251	80	82
UDP	192.168.2.25	1098	206.191.0.140	53	258
TCP	192.168.2.25	1099	65.54.192.248	80	79
UDP	192.168.2.25	1096	206.191.0.140	53	257
UDP	192.168.2.25	1102	206.191.0.140	53	269

At the top of the display, the system status monitor shows:

CPU usage The current CPU usage statistics of the DFL-500.

Memory usage The percentage of available memory being used by the DFL-500.

Up time The number of days, hours, and minutes since the DFL-500 was last started.

Each line of the system status monitor displays the following information about each active firewall connection.

Protocol The service type or protocol of the connection.

From IP The source IP address of the connection.

From Port The source port of the connection.

To IP The destination IP address of the connection.

To Port The destination port of the connection.

Expire The time, in seconds, before the connection expires.

Automatic antivirus and attack database updates

You can configure the DFL-500 to automatically check the D-Link update center at update.Dlink.com to see if a new version of the antivirus database and a new version of the attack database are available. If it finds new versions, the DFL-500 automatically downloads and installs the updated databases.

You can specify the IP addresses of two update centers and configure the DFL-500 to check and download updated databases once a day, or once a week. You can specify whether the DFL-500 checks for and downloads the antivirus database, the attack database, or both.

The DFL-500 writes a message to the event log when it checks for database updates and when it downloads a new version of a database. You can also go to **System > Update** to see the date and time at which the antivirus and attack databases were last updated.

To configure antivirus and attack database updates:

- Go to **System > Update**.
- Enter the IP address or domain name of one or two antivirus and attack database update centers. The D-Link update center domain name is update.Dlink.com.

- Select Periodic Update to turn on the automatic database updates.
- Select whether to check for and download updates:

Daily Once a day. You can specify the time of day to check for updates.

Weekly Once a week. You can specify the day of the week and the time of day to check for updates.

- Select Virus Database Update to check for and download antivirus database updates.
- Select Attack Database Update to check for and download attack database updates.
- Select Apply to save your changes.



At any time, you can go to **System > Update** and select Update Now to check for and update your antivirus and attack databases.

Configuring automatic antivirus and attack database updates

Network configuration

Go to **System > Network** to make any of the following changes to the DFL-500 network settings:

- [Configuring the internal interface](#)
- [Configuring the external interface](#)
- [Setting DNS server addresses](#)
- [Configuring routing](#)
- [Enabling RIP server support](#)
- [Providing DHCP services to your internal network](#)

Configuring the internal interface

You can change the internal interface IP address and Netmask and configure the access method for the internal interface.

To configure the internal interface using the web-based manager:

- Go to **System > Network > Interface** .

- For the internal interface, select Modify .
- Change the IP address and Netmask as required.
- Select the management Access methods for the internal interface.

HTTPS To allow secure HTTPS connections to the web-based manager through the internal interface.

PING If you want the internal interface to respond to pings. Use this setting to verify your installation and for testing.

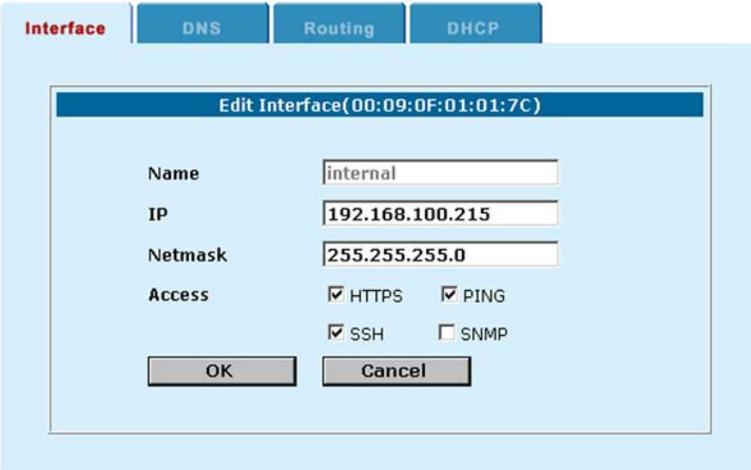
SSH To allow secure SSH connections to the CLI through the internal interface.

SNMP To allow a remote SNMP manager to request SNMP information by connecting to the internal interface. See [Configuring SNMP](#).

- Select OK to save your changes.

If you changed the IP address of the internal interface, you must reconnect to the web-based manager using the new internal interface IP address.

Configuring the internal interface



Configuring the external interface

Use the following procedures to configure the external interface:

- [Configuring the external interface with static IP addresses](#)
- [Configuring the external interface for DHCP](#)
- [Configuring the external interface for PPPoE](#)
- [Controlling management access to the external interface](#)
- [Changing external interface MTU size to improve network performance](#)

Configuring the external interface with static IP addresses

To configure the external interface using the web-based manager:

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Set Addressing Mode to Manual.
- Change the IP address and Netmask as required.
- Select OK to save your changes.

Configuring the external interface for DHCP

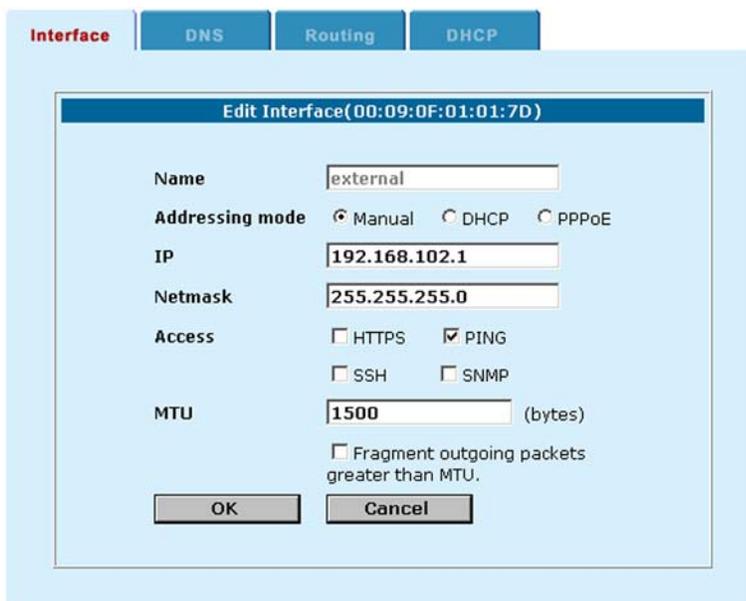
Use the following procedure to configure the DFL-500 external interface to use DHCP. This configuration is required if your ISP uses DHCP to assign the IP address of the DFL-500 external interface.

To configure the external interface to use DHCP:

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Set Addressing Mode to DHCP.
- Select Connect to DHCP server to automatically connect to a DHCP server.
- Select OK.

The DFL-500 attempts to contact a DHCP server from the external interface to set the external IP address, netmask, and default gateway IP address. When the DFL-500 gets this information from the DHCP server, the new addresses and netmask are displayed in the IP address and Netmask fields. These fields are colored grey to indicate that the addresses have not been assigned manually.

Configuring the external interface



The screenshot shows the 'Edit Interface' configuration window for the external interface. The window has tabs for 'Interface', 'DNS', 'Routing', and 'DHCP'. The 'DHCP' tab is selected. The window title is 'Edit Interface(00:09:0F:01:01:7D)'. The configuration fields are as follows:

Name	external
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP	192.168.102.1
Netmask	255.255.255.0
Access	<input type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP
MTU	1500 (bytes)
	<input type="checkbox"/> Fragment outgoing packets greater than MTU.

At the bottom of the window are 'OK' and 'Cancel' buttons.

Configuring the external interface for PPPoE

Use the following procedure to configure the DFL-500 external interface to use PPPoE. This configuration is required if your ISP uses PPPoE to assign the IP address of the external interface.

To configure the external interface to use PPPoE:

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Set Addressing Mode to PPPoE.
- Select OK.
- Enter your PPPoE account User Name and Password.
- Select OK.

The DFL-500 attempts to contact the PPPoE server to set the external IP address, netmask, and default gateway IP address. When the DFL-500 gets this information from the PPPoE server, the new addresses and netmask are displayed in the external IP address, netmask, and default gateway IP address fields. These fields are colored grey to indicate that the addresses have not been assigned manually.

Controlling management access to the external interface

Use the following procedure to control management access to the DFL-500 through the external interface. You can configure the DFL-500 so that you can access the web-based manager and CLI by connecting to the external interface. You can also control whether a remote SNMP manager can connect to the external interface to download management information from the DFL-500.

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Check or uncheck the following Access parameters for the external interface:
 - HTTPS** To allow secure HTTPS connections to the web-based manager through the external interface.
 - PING** If you want the external interface to respond to pings. Use this setting to verify your installation and for testing.
 - SSH** To allow secure SSH connections to the CLI through the external interface.
 - SNMP** To allow a remote SNMP manager to request SNMP information by connecting to the external interface. See [Configuring SNMP](#).

Checking HTTPS for the external interface allows remote administration of the DFL-500 using the web-based manager from any location on the Internet. Checking SSH for the external interface allows remote administration of the DFL-500 using the CLI from any location on the Internet. Checking SNMP for the external interface allows remote SNMP management of the DFL-500 from the Internet.

- Select OK.



You can control the IP addresses from which administrators can access the web-based manager. See [Adding and editing administrator accounts](#).

Changing external interface MTU size to improve network performance

To improve the performance of your internet connection, you can adjust the maximum transmission unit (MTU) of the packets that the DFL-500 transmits from its external interface. Ideally, you want this MTU to be the same as the smallest MTU of all the networks between the DFL-500 and the Internet. If the packets the DFL-500 sends are larger, they get broken up or fragmented, which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP or PPPoE, you might want to set the MTU size to 576. DSL modems may also have small MTU sizes. Most ethernet networks have an MTU of 1500.



If you connect to your ISP using DHCP to obtain an IP address for the external interface, you cannot set the MTU below 576 bytes due to DHCP communication standards.

To change the MTU size of the packets leaving the external interface:

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Select Fragment outgoing packets greater than MTU.
- Set the MTU size.

Set the maximum packet size in the range of 68 to 1500 bytes. The default MTU size is 1500. Experiment by lowering the MTU to find an MTU size for best network performance.

Configuring the management interface (Transparent mode)

You can configure the management interface for management access to the DFL-500 in transparent mode. To connect to the Management interface you must connect to the DFL-500 internal port.

To configure the management interface using the web-based manager:

- Go to *System > Network > Interface* .
- Change the IP and Netmask as required.
This must be a valid address for the network from which you will manage the DFL-500.
- Add a default gateway IP address if the DFL-500 must connect to a default gateway to reach the management computer.
- Select Apply to save your changes.

Setting DNS server addresses

Several DFL-500 functions, including sending alert emails and URL blocking, use DNS.

To set the DNS server addresses using the web-based manager:

- Go to *System > Network > DNS* .
- Change the primary and secondary DNS server addresses as required.
- Select Apply to save your changes.

Configuring routing

If there are multiple routers installed on your network, you can configure static routes to determine the path that data follows over your network before and after it passes through the DFL-500. You can also use static routing to allow different IP domain users to access the Internet through the DFL-500.

Use DFL-500 Routing to add, edit, and delete static routes:

- Go to **System > Network > Routing** .
- Select New to add a new route.
- Type the Destination IP address and Netmask for the route.
- Select the Interface for the route.
- Specify the default Gateway for the route.
- Select OK to save the new static route.
- To change a route, choose the route to change and select Edit  .
You can change any of the routing parameters.
- To delete a route, choose the route to delete and select Delete  .

Enabling RIP server support

Enable RIP server support to configure the DFL-500 to act like a RIP server. You can enable RIP support separately for the internal and external interfaces.

The RIP routing protocol maintains up-to-date dynamic routing tables between nearby routers. When you enable RIP server support, the DFL-500 acts like a RIP server broadcasting RIP packets to other nearby routers to:

- Request network updates from nearby routers
- Send its own routing tables to other routers
- Announce that the DFL-500 RIP is coming online (RIP server turned on) and requesting updates
- Announce that the DFL-500 RIP is shutting down and will stop sharing routing information

To enable RIP server support:

- Go to **System > Network > Routing** .
- Select Internal Interface to enable RIP server support from the internal interface.
- Select External Interface to enable RIP server support from the external interface.

Providing DHCP services to your internal network

If it is operating in NAT mode, you can configure the DFL-500 to be the DHCP server for your internal network:

- Go to **System > Network > DNS** .
- If they have not already been added, add the primary and secondary DNS server addresses provided to you by your ISP.



This step is not required if the external IP address of the DFL-500 is configured using DHCP or PPPoE.

- Select Apply.
- Go to **System > Network > DHCP** .
- Select Enable DHCP.
- Configure DHCP settings.

Starting IP Ending IP	If required, change the Starting IP and the Ending IP to configure the range of IP addresses that the DFL-500 can assign.
Netmask	Enter the Netmask that the DFL-500 assigns to the DHCP clients.
Lease Duration	Optionally type in the interval in seconds after which a DHCP client must ask the DHCP server for a new address.
Domain	Optionally type in the domain that the DHCP server assigns to the client.
DNS IP	Optionally type in the IP addresses of up to 3 DNS servers that the DHCP clients can use for looking up domain names.
Default Route	Optionally type in the default route assigned to DHCP clients.
Exclusion Range	Optionally type in up to 4 exclusion ranges of IP addresses within the starting IP and ending IP addresses that cannot be assigned to DHCP clients. If you have configured PPTP or L2TP, use the exclusion range to exclude the IP addresses assigned to PPTP or L2TP users. For more information, see PPTP and L2TP VPNs .

- Select Apply.
- Configure the IP network settings of the computers on your network to use DHCP. Use the address of the DFL-500 internal interface as the DHCP server address.

Sample DHCP settings

IP Address DNS Access Routing **DHCP**

Enable DHCP:

Starting IP:

Ending IP:

Netmask:

Lease Duration: (seconds)

Domain:

DNS IP:

Default Route:

Exclusion Range:

Range 1: -

Range 2: -

Range 3: -

Range 4: -

System configuration

Go to **System > Config** to make any of the following changes to the DFL-500 system configuration:

- [Setting system date and time](#)
- [Changing web-based manager options](#)
- [Adding and editing administrator accounts](#)
- [Configuring SNMP](#)
- [Automatic antivirus and attack database updates](#)

Setting system date and time

For effective scheduling and logging, the DFL-500 time should be accurate. You can either manually set the DFL-500 time, or you can configure the DFL-500 to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

For more information on NTP and to find the IP address of an NTP server that you can use, see <http://www.ntp.org>.

To set the date and time using the web-based manager:

- Go to **System > Config > Time** .
- Select Refresh to display the current DFL-500 date and time.
- Select your Time Zone from the list.
- Optionally select Set Time and set the DFL-500 date and time to the correct date and time.
- To configure the DFL-500 to use NTP, select Synchronize with NTP server.

By default, the DFL-500 is configured to connect to an NTP server at IP address 192.5.5.250, which is the IP address of an NTP server maintained by the Internet Software Consortium at Palo Alto, CA, USA.

- Optionally enter the IP address of a different NTP server.

- Specify how often the DFL-500 should synchronize its time with the NTP server. A typical Syn Interval would be 1440 minutes for the DFL-500 to synchronize its time once a day.
- Select Apply.

Example date and time setting

Changing web-based manager options

You can change the web-based manager idle timeout and firewall user authentication timeout. You can also change the language and character set used by the web-based manager.

To change web-based manager options:

- Go to *System > Config > Options* .
- Set the web-based manager idle time-out.
Set the idle time-out to control the amount of inactive time that the web-based manager waits before requiring the administrator to log in again.
The default idle time-out is 5 minutes. The maximum idle time-out is 480 minutes (8 hours).
- Set the firewall user authentication time-out.
For more information, see [Users and authentication](#). The default Auth time-out is 15 minutes. The maximum Auth time-out is 480 minutes (8 hours).
- Choose the character set and language that the web-based manager uses.



When the web-based manager language is set to use Simplified Chinese, you can change to English by selecting the English button that appears on the upper right of the web-based manager.

- Select Apply.
The options that you have selected take affect.

Adding and editing administrator accounts

When the DFL-500 is initially installed, it is configured with a single administrator account with the user name admin. From this administrator account, you can add and edit administrator accounts. You can also control the access level of each of these administrator accounts and, optionally, control the IP address from which the administrator can connect to the DFL-500.

There are three administration account access levels:

admin	Has all permissions. Can view, add, edit, and delete administrator accounts. Can view and change the DFL-500 configuration. There is only one admin level user.
Read & Write	Can view and change the DFL-500 configuration. Can view but cannot add, edit, or delete administrator accounts. Can change their own administrator account password.
Read Only	Can view the DFL-500 configuration.

Adding new administrator accounts

From the admin account, use the following procedure to add new administrator accounts to the DFL-500 and control their permission levels.

- Go to *System > Config > Admin* .
- Select New to add an administrator account.
- Type a login name for the administrator account.
The login name must be at least 6 characters long and can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Type and confirm a password for the administrator account.
The password must be at least 6 characters long and can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Optionally type in a trusted host IP address and netmask for the location from which the administrator can log into the web-based manager.
- Set the permission level for the administrator:

Read Only The administrator can access the web-based manager and the CLI to view the configuration but cannot change settings.

Read & Write The administrator can access, view and change settings.

- Select OK to add the administrator account.

Editing administrator accounts

The admin account user can change individual administrator account passwords, configure the IP addresses from which administrators can access the web-based manager, and change the administrator's permission level.

Administrator account users with Read & Write access can change their own administrator passwords.

To edit an administrator account:

- Go to *System > Config > Admin* .
- To change an administrator account password, select Change Password .
- Type a New Password and Confirm the new password.
The password must be at least 6 characters long and can contain numbers (0-9), and upper and lower case letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Select OK.
- To edit the settings of an administrator account, select Edit .

- Optionally type a trusted host IP address and wildcard mask for the location from which the administrator can log into the web-based manager.

If you want the administrator to be able to access the DFL-500 from any address, set the trusted host to 0.0.0.0 and the wildcard mask to 255.255.255.255.

To limit the administrator to only being able to access the DFL-500 from a specific network, set trusted host to the address of this network and set the wildcard mask to the netmask for this network. For example, to limit an administrator to accessing the DFL-500 from your internal network, set trusted host to the address of your internal network (for example, 192.168.1.0) and set wildcard mask to 255.255.255.0.

- Change the administrator's permission as required.
- Select OK.
- To delete an administrator account, choose the account to delete and select Delete .

Configuring SNMP

Configure SNMP for the DFL-500 so that the SNMP agent running on the DFL-500 can report system information and send traps. The DFL-500 agent supports SNMP v1 and v2c. System information can be monitored by any SNMP manager configured to get system information from your DFL-500. Your SNMP manager can use GET (GET-NEXT) SNMP operations to communicate with the DFL-500 agent.

DFL-500 MIBs

The DFL-500 agent supports the standard Internet MIB-II System Group (RFC-1213) for reporting basic system information. The agent also supports a DFL-500 MIB that reports firewall and VPN information. [DFL-500 MIB fields](#) shows the system and DFL-500 MIB fields.

You must compile the following MIBS into your SNMP manager to communicate with the DFL-500 agent:

- FN-SMI.mib
- FN-SYSTEM.mib
- FN-FIREWALL.mib

You can download copies of these MIB files from the D-Link web page (www.Dlink.com).

DFL-500 MIB fields		
Branch	Definitions	
System	Status	Operation Mode Firmware Version Antivirus database Version Serial Number
	Network	DNS Routing DHCP
	Configuration	
Firewall	Policy Address Service Schedule User Virtual IP IP/Mac Binding	



DFL-500 traps

The DFL-500 agent can send traps to up to 3 SNMP trap receivers on your network that are configured to receive traps from the DFL-500. The DFL-500 agent sends traps in response to the events listed in [SNMP traps](#).

SNMP traps	
Event	Description
System Startup	The DFL-500 starts or restarts.
Invalid Community	The SNMP agent has received an SNMP request with an invalid community string.
System Shutdown	The DFL-500 shuts down.
Agent Disabled	An administrator has disabled the SNMP agent from the web-based manager. The agent is also automatically disabled before a system shutdown, and a trap is sent when this occurs.
Agent Enabled	An administrator has enabled the SNMP agent from the web-based manager. The agent is also automatically enabled when the system starts up.

Configuring SNMP

To configure SNMP:

- Go to *System > Config > SNMP* .
- Select Enable SNMP.
- Configure SNMP settings:
- Select Apply.

Sample SNMP configuration

The screenshot shows a configuration window with tabs for Time, Options, Admin, and SNMP. The SNMP tab is active. The configuration fields are as follows:

Enable SNMP:	<input checked="" type="checkbox"/>
System Name:	Main Office Firewall
System Location:	Server room first floor
Contact Information:	ext. 3345
Get Community:	our_get_com
Trap Community:	trap_com
First Trap Receiver IP Address:	192.44.55.66
Second Trap Receiver IP Address:	145.23.66.77
Third Trap Receiver IP Address:	

An Apply button is located at the bottom of the configuration area.

System Name Type in a name for this DFL-500. The system name can be up to 31 characters long and can contain, numbers (0-9), upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the \ < > [] ` \$ % & characters are not allowed.

System Location Describe the physical location of the DFL-500. The system location description can be up to 31 characters long and can contain spaces, numbers (0-9), upper and lower case letters (A-Z, a-z), and the special characters - and _. The \ < > [] ` \$ % & characters are not allowed.

Contact Information Add the contact information for the person responsible for this DFL-500. The contact information can be up to 31 characters long and can contain spaces, numbers (0-9), upper and lower case letters (A-Z, a-z), and the special characters - and _. The \ < > [] ` \$ % & characters are not allowed.

Get Community Also called read community, get community is a password to identify SNMP get requests sent to the DFL-500. When an SNMP manager sends a get request to the DFL-500, it must include the correct get community string.

The default get community string is "public". Change the default get community string to keep intruders from using get requests to retrieve information about your network configuration. The get community string must be used in your SNMP manager to enable it to access DFL-500 SNMP information.

The get community string can be up to 31 characters long and can contain spaces, numbers (0-9), upper and lower case letters (A-Z, a-z), and the special characters - and _. The \ < > [] ` \$ % & characters are not allowed.

Trap Community The trap community string functions like a password that is sent with SNMP traps. The default trap community string is "public". Change the trap community string to the one accepted by your trap receivers.

The trap community string can be up to 31 characters long and can contain spaces, numbers (0-9), upper and lower case letters (A-Z, a-z), and the special characters - and _. The \ < > [] ` \$ % & characters are not allowed.

Trap Receiver IP Addresses Optionally type in the IP addresses of up to three trap receivers on your network configured to receive traps from your DFL-500. Traps are only sent to the configured addresses.

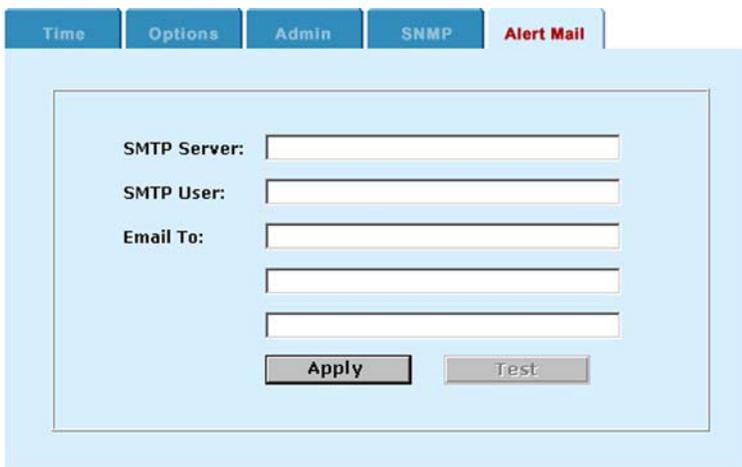
Alert email

You can configure the DFL-500 to send email alerts to up to three email addresses when the NIDS detects an attack.

Configuring alert email

- Go to System >Config > *Alert Mail* .
- In the SMTP Server field, enter the name of the SMTP server to which the DFL-500 should send email. The SMTP server can be located on any network connected to the DFL-500.
- In the SMTP User field, enter a valid email address (for example, warning@firewall.com). This address appears in the from heading of the alert email.
- Enter up to 3 destination email addresses in the Email To fields. These are the email addresses that the DFL-500 sends email alerts to.
- Select Apply to save the email alert settings.
- Make sure that the DNS server settings are correct for the DFL-500. See [Setting DNS server addresses](#). Because the DFL-500 uses the SMTP server name to connect to the mail server, it must be able to look up this name on your DNS server.

Example alert email settings



The screenshot shows a web interface with a navigation bar at the top containing tabs for Time, Options, Admin, SNMP, and Alert Mail. The Alert Mail tab is selected. Below the navigation bar is a light blue panel containing the configuration form. The form has three input fields: SMTP Server, SMTP User, and Email To. The Email To field has three stacked input boxes. At the bottom of the form are two buttons: Apply and Test.

Testing email alerts

You can test your email alert settings by sending a test email.

- Go to System >Config > *Alert Mail* .
- Select Test to send test email messages from the DFL-500 to the Email To addresses that you have configured.

Glossary

Connection : A link between machines, applications, processes, and so on that can be logical, physical, or both.

DNS, Domain Name Service : A service that converts symbolic node names to IP addresses.

Ethernet : A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

External interface : The DFL-500 interface that is connected to the Internet.

FTP, File transfer Protocol : An application and TCP/IP protocol used to upload or download files.

Gateway : A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

HTTP, Hyper Text Transfer Protocol : The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS : The SSL protocol for transmitting private documents over the Internet using a Web browser.

Internal interface : The DFL-500 interface that is connected to your internal (private) network.

Internet : A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

ICMP, Internet Control Message Protocol : Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

IKE, Internet Key Exchange : A method of automatically exchanging authentication and encryption keys between two secure servers.

IMAP, Internet Message Access Protocol : An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

IP, Internet Protocol : The component of TCP/IP that handles routing.

IP Address : An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

L2TP, Layer Two (2) Tunneling Protocol : An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

IPSec, Internet Protocol Security : A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

LAN, Local Area Network : A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

MAC address, Media Access Control address : A hardware address that uniquely identifies each node of a network.

MIB, Management Information Base : A database of objects that can be monitored by an SNMP network manager.

Modem : A device that converts digital signals into analog signals and back again for transmission over telephone lines.

MTU, Maximum Transmission Unit : The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

Netmask : Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

NTP , Network Time Protocol : Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

Packet : A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Ping, Packet Internet Grouper : A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POP3, Post Office Protocol : A protocol used to transfer e-mail from a mail server to a mail client across the Internet. Most e-mail clients use POP.

PPP, Point-to-Point Protocol : A TCP/IP protocol that provides host-to-network and router-to-router connections.

PPTP, Point-to-Point Tunneling Protocol : A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

Port : In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Protocol : An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

RADIUS , Remote Authentication Dial-In User Service : An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Router : A device that connects LANs into an internal network and routes traffic between them.

Routing : The process of determining a path to use to send data to its destination.

Routing table : A list of valid paths through which data can be transmitted.

Server : An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

SMTP, Simple Mail Transfer Protocol : In TCP/IP networks, this is an application for providing mail delivery services.

SNMP , Simple Network Management Protocol : A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SSH , Secure shell : A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

Subnet : A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Subnet Address : The part of the IP address that identifies the subnetwork.

TCP, Transmission Control Protocol : One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP, User Datagram Protocol : A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

VPN, Virtual Private Network : A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

Virus : A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

Worm : A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Troubleshooting FAQs

- [General administration](#)
- [Network configuration](#)
- [Firewall policies](#)
- [Schedules](#)
- [VPN](#)
- [Virus protection](#)
- [Web content filtering](#)
- [Logging](#)

General administration

Q: I am trying to set up some of the firewall options, but it keeps asking me for a password while I work.

Increase the web-based manager idle timeout. See [Changing web-based manager options](#).

Q: Administration from the Internet does not work.

Configure management access for the external, interface. See [Configuring the external interface](#).

Q: Everyone in the world knows the password.

Change the administrator password. See [Adding and editing administrator accounts](#).

Q: I have the DFL-500 configured the way I want it. Is there some way to save the configuration before making any more changes?

See [Backing up system settings](#) and [Restoring system settings](#).

Q: How can I get a warning when someone is attacking my network?

See [Network Intrusion detection system \(NIDS\)](#) and [Alert email](#).

Network configuration

Q: I am trying to set up the network connections, but I can't seem to ping the firewall.

Configure the interface to respond to pings. See [Configuring the internal interface](#).

Firewall policies

Q: When I set policies, all the computers on the network seem to be affected. The policy for a single machine is being applied to the entire network.

When adding the address of a single computer remember to change the netmask from 255.255.255.0 to 255.255.255.255.

Q: My policies are set correctly, but I still cannot connect to the Internet from one or more of the computers on my internal network.

Check the default gateway setting on that particular computer. Its default gateway must match the internal address of the DFL-500.

Q: I checked the default gateway and it matches, but I still cannot connect to the Internet.

Use the setup wizard to make sure that the external address and external gateway of the firewall have been properly set to your Internet Service Provider's (ISP) specifications. If there is no discrepancy, it would be a good idea to double check with your ISP that they have provided you with the correct information.

Q: I am having problems setting up my policies. I cannot add source or destination addresses to policies.

When setting up policies, it is important to remember that new addresses cannot be entered into the Destination or Source fields. New addresses must be added to the firewall address lists. The choices under the Destination and Source menus come directly from the address lists. See [Adding addresses](#).

Q: I want to set up an incoming policy for an FTP server on my internal network.

Providing access to servers on your internal network is explained in the following sections:

- [NAT mode policy for public access to a server.](#)
- [Route mode policy for public access to a server.](#)
- [Transparent mode policy for public access to a server.](#)

Q: I want to connect to a TELNET/FTP/WEB server across the Internet. If I set the outgoing policy service field to TELNET/FTP/HTTP, I can't connect.

Try setting the service to ANY. Settings for individual services assume that the standard port for that service is being used, and only traffic addressed to that port is allowed through. If you are using a non-standard port, setting individual services will not work. ANY allows traffic to go to all ports.

Schedules

Q: I need a schedule that will allow access to the Internet overnight, from 9:00 pm to 9:00 am. How can I do this?

Create a recurring schedule with a start time of 9:00 pm and a stop time of 9:00 am. If the stop time is set earlier than the start time, the stop time will be during next day.

VPN

Q: The client to subnet configuration was working, but now it has shut down and I can't recover it. How do I get it back again?

This happens when the tunnel is down and the client software thinks it is still connected. To recover you must disconnect at the client end.

Q. Why can't I bring up the connection in the case of subnet to subnet configuration?

First check that you have set up the proper IPsec policy for this connection. If you have, check that the authentication keys are the same on the local and remote IPsec gateways. Also check that the remote gateway address is correct.

Virus protection

Q: I am worried about viruses so I set the Antivirus options to block. Now people are complaining that some files that they need are blocked.

When antivirus protection for HTTP or any of the email protocols is set to block, potentially dangerous file types are blocked. Under normal conditions, antivirus protection can safely be set to scan. Block should only be used in extreme circumstances when a new virus has been found.

Q: A new virus is spreading through the Internet. What should I do?

Set virus protection to block. See [Configuring antivirus protection](#). Next contact D-Link and obtain an Antivirus database update which includes protection against the new virus. To install the new database, see [Automatic antivirus and attack database updates](#).

Web content filtering

Q: My employees are job hunting on the Internet when they should be working. Is it possible to block career sites.

See [Block access to Internet sites](#) and enter the names of the unwanted sites into the URL block list.

Q: I am worried about dangerous web content so I set the Script Filter options to block all scripts, Java Applets, ActiveX, and cookies. Now people are complaining that some web sites are inaccessible or don't work properly.

See [Remove scripts from web pages](#).

Logging

Q: Can I identify the attackers from the log?

The attack log does contain the IP address that the violating packets originated from, but since most Internet users do not have static IP addresses, these may not provide all of the information that you need.

Q: How can I find out which company employees are spending time on the Internet?

Select Log Traffic for all From Internal To External firewall policies the provide users on the Internal zone with access to the Internet.

Q: How can I record DFL-500 logs on a remote computer, such as an management computer?

You can send DFL-500 logs to a WebTrends server or a syslog server. To do this, configure one of these servers and go to **Log&Report > Log Setting** . Select Log to remote host and enter the IP address of the computer running the syslog server. Select Log to WebTrends and enter the IP address of the computer running the WebTrends server.

Technical Support

D-Link Offices

AUSTRALIA	D-LINK AUSTRALIA Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand) E-MAIL: support@dlink.com.au, info@dlink.com.au URL: www.dlink.com.au
BENELUX	D-LINK BENELUX Fellenoord 130, 5611 ZB Eindhoven, The Netherlands TEL: 31-40-2668713 FAX: 31-40-2668666 E-MAIL: info@dlink-benelux.nl, info@dlink-benelux.be URL: www.dlink-benelux.nl , www.dlink-benelux.be/
CANADA	D-LINK CANADA #2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5095 FREE CALL: 1-800-354-6522 E-MAIL: techsup@dlink.ca URL: www.dlink.ca FTP: ftp.dlinknet.com
CHILE	D-LINK SOUTH AMERICA Isidora Goyechea 2934 of 702, Las Condes, Santiago - Chile S.A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl URL: www.dlink.cl
CHINA	D-LINK CHINA 2F, Sigma Building, 49 Zhichun Road, Haidian District, 100080 Beijing, China TEL: 86-10-88097777 FAX: 86-10-88096789
DENMARK	D-LINK DENMARK Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL: 45-43-969040 FAX: 45-43-424347 E-MAIL: info@dlink.dk URL: www.dlink.dk
EGYPT	D-LINK MIDDLE EAST 7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt TEL: 202-2456176 FAX: 202-2456192 E-MAIL: support@dlink-me.com URL: www.dlink-me.com
FINLAND	D-Link FINLAND Thlil-ja Pakkahuone Katajanokanlaituri 5, FIN-00160 Helsinki, Finland TEL: 358-9-422-9166 FAX: 358-9-422-91661 E-MAIL: info@dlink-fi.com URL: www.dlink-fi.com
FRANCE	D-LINK FRANCE Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury France TEL: 33-1-302-38688 FAX: 33-1-3023-8689 E-MAIL: info@dlink-france.fr URL: www.dlink-france.fr
GERMANY	D-LINK Central Europe/D-Link Deutschland GmbH Schwabacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 INFO LINE: 00800-7250-0000 (toll free) HELP LINE: 00800-7250-4000 (toll free) REPAIR LINE: 00800-7250-8000 E-MAIL: info@dlink.de URL: www.dlink.de
IBERIA	D-LINK IBERIA Gran Via de Carlos III, 84, 3 ^o Edificio Trade, 08028 BARCELONA TEL: 34 93 4090770 FAX 34 93 4910795 E-MAIL: info@dlinkiberia.es URL: www.dlinkiberia.es
INDIA	D-LINK INDIA Plot No.5, Kurla-Bandra Complex Road, Off Cst Road, Santacruz (E), Bombay - 400 098 India TEL: 91-22-652-6696 FAX: 91-22-652-8914 E-MAIL: service@dlink.india.com URL: www.dlink-india.com
ITALY	D-LINK ITALIA Via Nino Bonnet No. 6/b, 20154 Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 E-MAIL: info@dlink.it URL: www.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 E-MAIL: kida@d-link.co.jp URL: www.d-link.co.jp
NORWAY	D-LINK NORWAY Waldemar Thranesgt. 77, 0175 Oslo, Norway TEL: 47-22-991890 FAX: 47-22-207039
RUSSIA	D-LINK RUSSIA Michurinski Prospekt 49, 117607 Moscow, Russia TEL: 7-095-737-3389, 7-095-737-3492 FAX: 7-095-737-3390 E-MAIL: vi@dlink.ru URL: www.dlink.ru
SINGAPORE	D-LINK INTERNATIONAL 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
S. AFRICA	D-LINK SOUTH AFRICA 102-106 Witchazel Avenue, Einetein Park 2, Block B, Highveld Technopark Centurion, South Africa TEL: 27(0)126652165 FAX: 27(0)126652186 E-MAIL: attie@d-link.co.za URL: www.d-link.co.za
SWEDEN	D-LINK SWEDEN P.O. Box 15036, S-167 15 Bromma Sweden TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 E-MAIL: info@dlink.se URL: www.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 E-MAIL: dssga@tsc.dlinktw.com.tw URL: www.dlinktw.com.tw
U.K.	D-LINK EUROPE 4 th Floor, Merit House, Edgware Road, Colindale, London, NW9 5AB, U.K. TEL: 44-20-8731-5555 FAX: 44-20-8731-5511 E-MAIL: info@dlink.co.uk URL: www.dlink.co.uk
U.S.A.	D-LINK U.S.A. 53 Discovery Drive, Irvine, CA 92618 USA TEL: 1-949-788-0805 FAX: 1-949-753-7033 INFO LINE: 1-800-326-1688 BBS: 1-949-455-1779, 1-949-455-9616 E-MAIL: tech@dlink.com, support@dlink.com URL: www.dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms _____
 Organization: _____ Dept. _____
 Your title at organization: _____
 Telephone: _____ Fax: _____
 Organization's full address: _____

 Country: _____
 Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____
 Telephone: _____ Fax: _____
 Reseller's full address: _____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

Home Office Travel Company Business Home Business Personal Use

2. How many employees work at installation site?

1 employee 2-9 10-49 50-99 100-499 500-999 1000 or more

3. What network protocol(s) does your organization use ?

XNS/IPX TCP/IP DECnet Others _____

4. What network operating system(s) does your organization use ?

D-Link LANsmart Novell NetWare NetWare Lite SCO Unix/Xenix PC NFS 3Com 3+Open
Banyan Vines DECnet Pathwork Windows NT Windows NTAS Windows '95
Others _____

5. What network management program does your organization use ?

D-View HP OpenView/Windows HP OpenView/Unix SunNet Manager Novell NMS
NetView 6000 Others _____

6. What network medium/media does your organization use ?

Fiber-optics Thick coax Ethernet Thin coax Ethernet 10BASE-T UTP/STP
100BASE-TX 100BASE-T4 100VGAnyLAN Others _____

7. What applications are used on your network?

Desktop publishing Spreadsheet Word processing CAD/CAM
Database management Accounting Others _____

8. What category best describes your company?

Aerospace Engineering Education Finance Hospital Legal Insurance/Real Estate Manufacturing
Retail/Chainstore/Wholesale Government Transportation/Utilities/Communication VAR
System house/company Other _____

9. Would you recommend your D-Link product to a friend?

Yes No Don't know yet

10. Your comments on this product?

PLEASE
PLACE STAMP
HERE

TO: _____

D-Link[®]

Limited Warranty

D-Link Systems, Inc. (“D-Link”) provides this 1-Year warranty for its product only to the person or entity who originally purchased the product from:

- D-Link or its authorized reseller or distributor.
- Products purchased and delivered with the fifty United States, the District of Columbia, US Possessions or Protectorates, US Military Installations, addresses with an APO or FPO.

1-Year Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below (“Hardware”) will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type (“Warranty Period”).

1-Year Limited Warranty for the Product(s) is defined as follows

- Hardware (excluding power supplies and fans)
- Power Supplies and Fans One (1) Year.
- Spare parts and spare kits Ninety (90) days.

D-Link’s sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days (“Warranty Period”), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link’s sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration is conducted via a link on our Web Site (<http://www.dlink.com/>). Each product purchased must be individually registered for warranty service within ninety (90) days after it is purchased and/or licensed.

FAILURE TO PROPERLY TO REGISTER MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
- The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package.
- The customer is responsible for all shipping charges to and from D-Link (No CODs allowed). Products sent COD will become the property of D-Link Systems, Inc. Products should be fully insured by the customer and shipped to **D-Link Systems Inc., 53 Discovery Drive, Irvine CA 92618.**

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

This limited warranty provided by D-Link does not cover: Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE 1-YEAR LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This 1-Year Warranty shall be governed by the laws of the state of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright© 2001 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

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

Registration

Register the D-Link DFL-500 Office Firewall online at <http://www.dlink.com/sales/reg>