

D-Link DFL-1000

Network Security Firewall

Manual

D-Link[®]
Building Networks for People

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

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

DFL-1000 User Manual
Version 2.36
4 July 2003

Trademarks

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

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

Table of Contents

Introduction	10
Web content filtering	10
Firewall.....	10
NAT/Route mode	11
Transparent mode	11
VPN.....	11
Secure installation, configuration, and management	12
Web-based manager	12
Command line interface.....	12
Logging and reporting.....	13
What's new in Version 2.36	13
About this document	15
For more information	15
Customer service and technical support	15
Getting started.....	17
Package contents	17
Mounting	18
Powering on.....	18
Initial configuration.....	19
Connecting to the web-based manager.....	19
Connecting to the command line interface (CLI)	20
Next steps.....	21
NAT/Route mode installation	22
Preparing to configure NAT/Route mode	22
Advanced NAT/Route mode settings	22
DMZ interface	23
Using the setup wizard	23
Starting the setup wizard	23
Reconnecting to the web-based manager.....	23
Using the command line interface	24
Configuring the DFL-1000 NPG to run in NAT/Route mode	24
Connecting to your networks	25
Configuring your networks.....	25
Completing the configuration.....	26
Configuring the DMZ interface	26
Setting the date and time.....	26
Transparent mode installation.....	27
Preparing to configure Transparent mode.....	27

Using the setup wizard	27
Changing to Transparent mode.....	27
Starting the setup wizard.....	28
Reconnecting to the web-based manager.....	28
Using the command line interface	28
Changing to Transparent mode.....	28
Configuring the Transparent mode management IP address	28
Configure the Transparent mode default gateway	29
Setting the date and time.....	29
Connecting to your networks	29

Firewall configuration..... 31

NAT/Route mode and Transparent mode	32
NAT/Route mode.....	32
Transparent mode	32
Changing to Transparent mode.....	32
Changing to NAT/Route mode	32
Adding NAT/Route mode policies.....	32
Adding Transparent mode policies	35
Configuring policy lists	37
Policy matching in detail.....	37
Changing the order of policies in a policy list	38
Enabling and disabling policies	38
Disabling a policy.....	38
Enabling a policy	38
Addresses.....	38
Adding addresses.....	39
Editing addresses	40
Deleting addresses.....	40
Organizing addresses into address groups.....	40
Services	41
Predefined services	41
Providing access to custom services	43
Grouping services.....	43
Schedules	44
Creating one-time schedules.....	44
Creating recurring schedules.....	45
Adding a schedule to a policy.....	46
Virtual IPs	47
Adding static NAT virtual IPs.....	47
Adding port forwarding virtual IPs	49
Adding policies with virtual IPs	50
IP pools.....	51
IP/MAC binding.....	52

Configuring IP/MAC binding for packets going through the firewall	52
Configuring IP/MAC binding for packets going to the firewall	53
Adding IP/MAC addresses	53
Viewing the dynamic IP/MAC list.....	53
Enabling IP/MAC binding.....	54
Example policies	55
NAT policy for public access to a server	55
Routing policy for access to a server from the internal network.....	55
Transparent mode policy for public access to a server	56
Denying connections from the Internet.....	57
Using a schedule to deny access.....	57
Denying connections to the Internet.....	57
Adding policies that accept connections.....	58
Requiring authentication to connect to the Internet.....	59
Users and authentication	61
Setting authentication timeout	61
Adding user names and configuring authentication	61
Adding user names and configuring authentication	62
Deleting user names from the internal database	62
Configuring RADIUS support.....	63
Adding RADIUS servers	63
Deleting RADIUS servers	63
Configuring user groups	64
Adding user groups	64
Deleting user groups	65
IPSec VPNs	66
Interoperability with IPSec VPN products.....	67
Configuring AutoIKE key IPSec VPN	67
Configuring manual key IPSec VPN.....	68
Configuring dialup VPN	68
Configuring a VPN Concentrator for hub and spoke VPN.....	69
Configuring the VPN Concentrator.....	69
Configuring the member VPNs.....	70
Configuring IPSec redundancy.....	71
Adding a remote gateway	71
About dialup VPN authentication.....	73
About DH groups	75
About the P1 proposal	75
About NAT traversal	75
Adding an AutoIKE key VPN tunnel	76
About the P2 proposal	77
About replay detection.....	77

About perfect forward secrecy (PFS)	77
Adding a manual key VPN tunnel	78
Adding a VPN concentrator	79
Adding an encrypt policy.....	80
Viewing VPN tunnel status	82
Viewing dialup VPN connection status	83
Testing a VPN.....	83
IPSec VPN configuration examples.....	84
AutolKE key VPN between two networks.....	84
Configuring the remote gateway for a remote network	85
Configuring the AutolKE key tunnel for a remote network	86
Adding source and destination addresses for a network-to-network VPN.....	87
Adding an encrypt policy for a network-to-network VPN.....	87
AutolKE key VPN for remote clients.....	88
Configuring the remote gateway for remote clients.....	89
Configuring the AutolKE key tunnel for a remote client	89
Adding source and destination addresses for a remote client VPN.....	90
Adding a source address for the internal network.....	90
Adding an encrypt policy for a remote client	91
Configuring the IPSec VPN client.....	91
Dialup VPN	92
Adding a dialup remote gateway	93
Adding AutolKE key tunnels for dialup VPN.....	93
Adding source and destination addresses for dialup VPN	93
Adding encrypt policies for dialup VPN	94
Configuring remote IPSec VPN gateways for dialup VPN	94
Configuring remote IPSec VPN clients for dialup VPN	94
Manual key VPN between two networks	94
Configuring the manual key VPN tunnel	95
Adding source and destination addresses	95
Adding an encrypt policy	95
Manual key VPN for remote clients	96
Configuring the manual key tunnel.....	96
Adding internal and external addresses	97
Adding an encrypt policy	97
Configuring the IPSec VPN client.....	97
Hub and spoke VPN (VPN concentrator)	97
Configuring the hub	98
Configuring the spokes.....	98
Configuring the remote gateways.....	99
Configuring the AutolKE key tunnels.....	99
Configuring the VPN concentrator.....	100
Adding source and destination addresses	100

Adding encrypt policies.....	101
PPTP and L2TP VPNs	103
PPTP VPN configuration	103
Configuring the DFL-1000 NPG as a PPTP gateway	104
Configuring a Windows 98 client for PPTP	105
Configuring a Windows 2000 client for PPTP	106
Configuring a Windows XP client for PPTP.....	107
L2TP VPN configuration	108
Configuring the DFL-1000 NPG as an L2TP gateway	109
Configuring a Windows 2000 client for L2TP	110
Configuring a Windows XP client for L2TP	111
Web content filtering	113
Enabling web content filtering.....	113
Blocking web pages that contain unwanted content	113
Enabling the banned word list	114
Changing the content block message	114
Adding words and phrases to the banned word list	114
Temporarily disabling the banned word list.....	115
Temporarily disabling individual words in the banned word list	115
Clearing the banned word list.....	115
Backing up the banned word list	115
Restoring the banned word list.....	116
Blocking access to URLs.....	116
Enabling the URL block list.....	116
Changing the URL block message.....	116
Adding URLs to the URL block list	117
Temporarily disabling the URL block list	118
Temporarily disabling individual URL blocking.....	118
Clearing the URL block list	118
Downloading the URL block list.....	118
Uploading a URL block list	118
Removing scripts from web pages	119
Exempting URLs from content or URL blocking.....	119
Adding URLs to the Exempt URL list	120
Temporarily disabling entries in the Exempt URL list.....	121
Clearing the Exempt URL list	121
Downloading the Exempt URL list.....	121
Uploading an Exempt URL list	121
Logging and reporting.....	123
Configuring logging.....	123
Recording logs on a remote computer	123
Recording logs on a NetIQ WebTrends server	123

Recording logs on the DFL-1000 hard disk.....	124
Logging event log to memory	125
Selecting what to log	125
Viewing event log saved to memory.....	126
Viewing event log	126
Searching event log.....	126
Clearing event log messages	127
Viewing and maintaining logs saved to the hard disk.....	127
Viewing logs	127
Searching logs.....	128
Downloading a log file to the management computer	128
Deleting all messages in an active log	129
Deleting a saved log file	129
Configuring alert email.....	129
Configuring alert email.....	129
Testing alert emails	130
Enabling alert emails	130
Log message formats	130
Traffic log message format.....	130
Event log message format.....	131

Administration..... 132

System status	132
Upgrading the DFL-1000 firmware	133
Displaying the DFL-1000 NPG serial number	135
Backing up system settings.....	135
Restoring system settings	135
Restoring system settings to factory defaults.....	135
Changing to Transparent mode.....	136
Changing to NAT/Route mode	136
Restarting the DFL-1000 NPG	136
Shutting down the DFL-1000 NPG.....	136
System status monitor.....	137
Network configuration.....	138
Configuring the internal interface	138
Configuring the external interface	139
Configuring the dmz interface	142
Configuring the management interface (Transparent mode).....	142
Setting DNS server addresses	143
Configuring routing	143
Adding routing gateways	143
Adding a default route	144
Adding routes to the routing table	145
Configuring the routing table	145

Enabling RIP server support.....	146
Adding routes (Transparent mode)	146
Configuring the DFL-1000 NPG for multiple Internet connections	146
Providing DHCP services to your internal network.....	148
System configuration	150
Setting system date and time	150
Changing web-based manager options.....	151
Adding and editing administrator accounts	152
Configuring SNMP	153
Glossary.....	156
Troubleshooting FAQs	159
General administration.....	159
Network configuration	159
Firewall policies	159
Schedules	160
VPN.....	160
Web content filtering	160
Logging	161
Technical Support.....	162
Limited Warranty.....	165
Registration	168

Introduction

The DFL-1000 Network Protection Gateway (NPG) supports network-based deployment of application-level services—including and full-scan content filtering. DFL-1000 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-1000 NPG is a dedicated easily managed security device that delivers a full suite of capabilities that include:

- application-level services such as content filtering,
- network-level services such as firewall, VPN, and traffic shaping.

Your DFL-1000 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-1000 series complements existing solutions, such as host-based enables new applications and services while greatly lowering costs for equipment, administration and maintenance.



The DFL-1000 NPG is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office, home office, and branch office applications. The DFL-1000 installation wizard guides users through a simple process that enables most installations to be up and running in minutes.

Web content filtering

DFL-1000 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-1000 NPG blocks the web page. The blocked web page is replaced with a message that you can edit using the DFL-1000 web-based manager.

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

To prevent unintentional blocking of legitimate web pages, you can add URLs to an Exempt List that overrides the URL blocking and content blocking lists.

Web content filtering also includes a script filter feature that can be configured to block unsecure web content such as Java Applets, Cookies, and ActiveX.

Firewall

The DFL-1000 firewall protects your computer networks from the hostile environment of the Internet. After basic installation of the DFL-1000 NPG, the firewall allows users on the protected network to access the Internet while blocking Internet access to internal networks. You can modify this firewall configuration to place controls on access to the Internet from the protected networks and to allow controlled access to internal networks.

DFL-1000 policies include a complete range of options that:

- control all incoming and outgoing network traffic,
- control encrypted VPN 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 authenticate before gaining access,
- include traffic shaping to set access priorities and guarantee or limit bandwidth for each policy,
- include logging to track connections for individual policies,
- include Network address translation (NAT) mode and Route mode policies,
- include Mixed NAT and Route mode policies.

The DFL-1000 firewall can operate in NAT/Route mode or Transparent mode.

NAT/Route mode

In NAT/Route mode, you can create NAT mode policies and Route mode policies.

- NAT mode policies use network address translation to hide the addresses in a more secure network from users in a less secure network.
- Route mode policies accept or deny connections between networks without performing address translation.

Transparent mode

Transparent mode provides the same basic firewall protection as NAT mode. Packets received by the DFL-1000 NPG are intelligently forwarded or blocked according to firewall policies. The DFL-1000 NPG can be inserted in your network at any point without the need to make changes to your network or any of its components. However, VPN and some advanced firewall features are only available in NAT/Route mode.

VPN

Using DFL-1000 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-1000 VPN features include the following:

- Industry-standard and 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,
 - AutoIKE key based on pre-shared key tunnels,
 - Manual Keys tunnels,
 - Diffie-Hellman groups 1, 2, and 5,
 - Aggressive and Main Mode,
 - Replay Detection,
 - Perfect Forward Secrecy.
- 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.
- Firewall policy based control of IPSec VPN traffic.

- IPsec NAT traversal so that remote IPsec VPN gateways or clients behind a NAT can connect to an IPsec VPN tunnel.
- VPN hub and spoke using a VPN concentrator to allow VPN traffic to pass from one tunnel to another tunnel through the DFL-1000 NPG.
- IPsec Redundancy to create a redundant AutoIKE key IPsec VPN configuration to two remote VPN gateway addresses.

Secure installation, configuration, and management

Installation is quick and simple. When you initially power the DFL-1000 NPG up, it is already configured with default IP addresses and security policies. All that is required for the DFL-1000 NPG 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-1000 IP addresses for your network. From this foundation you can use the web-based manager to customize the configuration to meet your needs.

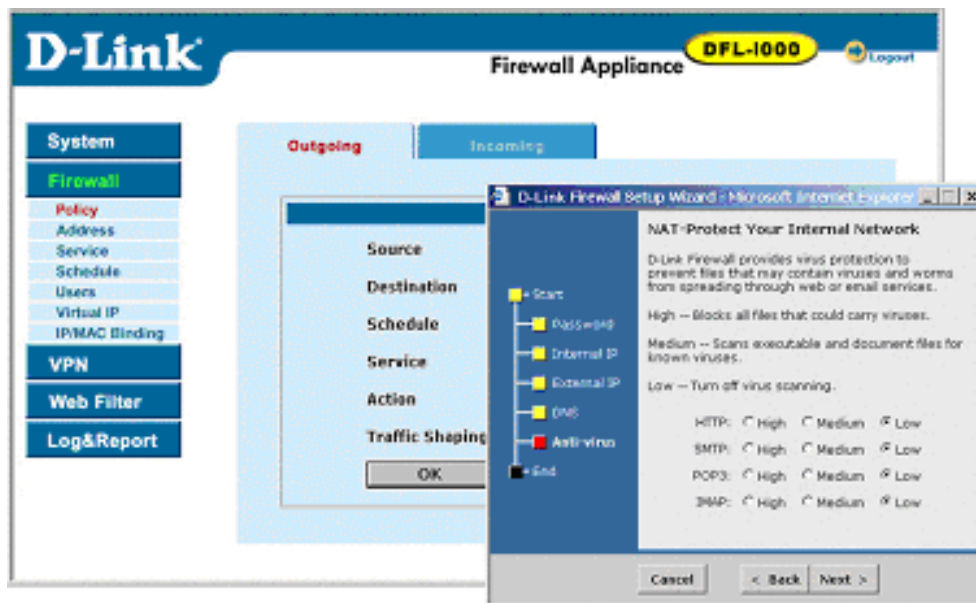
You can also create a basic configuration using the DFL-1000 command line interface (CLI).

Web-based manager

Using a secure HTTPS connection from any computer running Internet Explorer, you can configure and manage the DFL-1000 NPG. The web-based manager supports multiple languages. You can configure the DFL-1000 NPG for secure administration from any DFL-1000 interface, including secure remote management through the external interface from anywhere on the 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-1000 web-based manager and setup wizard



Command line interface

For troubleshooting and professional scripting, you can access the DFL-1000 command line interface (CLI) by connecting a management computer serial port to the DFL-1000 RS-232 serial Console connector. You can also use the SSH protocol to create a secure connection to the DFL-1000 CLI from

any network connected to the DFL-1000 NPG, including the Internet. Connecting to and using the DFL-1000 CLI is described in the *DFL-1000 CLI Reference Guide* .

Logging and reporting

The DFL-1000 NPG supports logging of various categories of traffic and of configuration changes. You can configure logging to:

- report traffic that connects to the firewall,
- 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, and web page blocking,
- send alert email to system administrators to report firewall or VPN events or violations.

Logs can be sent to a remote syslog server or to a WebTrends NetIQ Security Reporting Center and Firewall Suite server using the WebTrends enhanced log format. Some models can also save logs to an optional internal hard drive. If a hard drive is not installed, you can configure most DFL-1000 NPGs to log the most recent events to shared system memory.

What's new in Version 2.36

The following features are new in Version 2.36.

Policy-based NAT

When running the DFL-1000 NPG in NAT/Route mode, you can configure any firewall policy to be a NAT mode policy or a Route mode policy. See [Adding NAT/Route mode policies](#).

Multiple IP pools for each interface

You can add multiple IP pool address ranges to each DFL-1000 interface. When you select IP pool in a policy, the DFL-1000 NPG randomly changes the source address of packets to one of the addresses in the IP pools added to the destination of the policy. See [IP pools](#).

Configure port forwarding by configuring virtual IPs

Port forwarding is now configured by adding virtual IPs that route packets with a destination address that matches the IP address of the interface that receives the packets. See [Virtual IPs](#).

H.323 NAT traversal

By adding the H.323 server to firewall policies, DFL-1000 NPGs allow IP and other multi-media communications to connect through the firewall. See [Services](#).

IPSec VPN improvements

The following new IPSec VPN features have been added to v2.36:

- | | |
|----------------------------------|---|
| Encrypt firewall policies | Add IPSec firewall policies to control VPN traffic. Using IPSec VPN Firewall policies you can control the addresses of networks that can connect to a VPN tunnel and the direction of traffic flow through the VPN tunnel. See Adding an encrypt policy . |
| IPSec NAT traversal | Remote IPSec VPN gateways or clients behind a NAT can connect to an IPSec VPN tunnel. See About NAT traversal . |

Hub and spoke VPN using a VPN concentrator	You can add VPN tunnels to a VPN concentrator to create a VPN hub and spoke configuration. A hub and spoke configuration consists of two or more VPN tunnels that terminate at a DFL-1000 NPG. The VPN concentrator allows VPN traffic to pass from one tunnel to the other through a central DFL-1000 hub. See Configuring a VPN Concentrator for hub and spoke VPN .
Aggressive and normal mode	You can select aggressive mode for any IPSec VPN gateway configuration. In Aggressive mode, identifying information is exchanged before encryption is set up. Aggressive mode is less secure but establishes VPN tunnels faster. See Adding a remote gateway .
Dialup Monitor	You can monitor the status of dialup VPNs using the dialup monitor. The dialup monitor lists the dialup remote gateways and the VPN tunnels that are active for each remote gateway. For each tunnel, the dialup monitor lists the tunnel lifetime, timeout, Proxy ID source, and Proxy ID destination. See Viewing dialup VPN connection status .
IPSec Redundancy	IPSec redundancy allows you to create a redundant AutoIKE key IPSec VPN configuration to two remote VPN gateway addresses. See Configuring IPSec redundancy .

Local DFL-1000 user database

You can add user names to the local DFL-1000 user database. When you add a user name, you can specify a password or that the user can be authenticated using a RADIUS server. You can then add user names to user groups and make these user groups available for authenticating with firewall policies, dialup VPN, PPTP VPN, and L2TP VPN. See [Users and authentication](#).

Multiple WAN support

You can configure the DFL-1000 NPG to have multiple connections to the Internet. Using routing and policies the DFL-1000 multiple WAN feature supports:

- Redundancy, using link detection. If one WAN connection fails, the DFL-1000 NPG re-routes all traffic to and from the other WAN connection.
- Load balancing, to balance the amount of traffic routed to each WAN port.

For more information, see [Configuring the DFL-1000 NPG for multiple Internet connections](#).

Logging

The following logging features are new in v2.36 (see [Logging and reporting](#)):

- DFL-1000 logs are displayed with the last message at the top of the message list.
- Messages can be cleared from event log saved to memory.

Alert email

In v2.36 you configure alert email from Logging & Reporting. You can configure the DFL-1000 NPG to send alert email to report firewall or VPN events or violations. See [Configuring alert email](#).

Checksum to protect upgrade image from corruption

A Checksum added to the v2.36 firmware image guarantees its integrity during a firmware update.

New CLI commands

The command line interface has been extensively changed for v2.36. Command syntax has been changed to be easier to use and more effective, many command names and keywords have changed, and CLI help has been improved.

About this document

This user manual describes how to install and configure the DFL-1000 NPG. This document contains the following information:

- [Getting started](#) describes unpacking, mounting, and powering on the DFL-1000 NPG.
- [NAT/Route mode installation](#) describes how to install the DFL-1000 NPG if you are planning on running it in NAT/Route mode.
- [Transparent mode installation](#) describes how to install the DFL-1000 NPG if you are planning on running it in Transparent mode.
- [Firewall configuration](#) describes how to configure firewall policies to enhance firewall protection.
- [Example policies](#) contain some example firewall policies.
- [Users and authentication](#) describes how to add user names to the DFL-1000 user database and how to configure the DFL-1000 NPG to connect to a RADIUS server to authenticate users.
- [IPSec VPNs](#) describes how to configure DFL-1000 IPSec VPN.
- [IPSec VPN configuration examples](#) describe how to configure DFL-1000 IPSec VPN for a number of example VPN configurations.
- [PPTP and L2TP VPNs](#) describes how to configure PPTP and L2TP VPNs between the DFL-1000 NPG and a Windows client.
- [Web content filtering](#) describes how to configure web content filters to prevent unwanted Web content from passing through the DFL-1000 NPG.
- [Logging and reporting](#) describes how to configure logging and reporting to track activity through the DFL-1000 NPG.
- [Administration](#) describes DFL-1000 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-1000 User Manual*, you have access to the following DFL-1000 documentation:

- *DFL-1000 QuickStart Guide*
- *DFL-1000 CLI Reference Guide*
- DFL-1000 online help

Customer service and technical support

For firmware and 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.

You can register your DFL-1000 NPG by pointing your web browser to www.D-Link.com/support/register and following the directions. You can also modify your registration information by going to support.D-Link.com.

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-1000 NPG. When you have completed the procedures in this chapter, you can proceed to one of the following:

- If you are going to run your DFL-1000 NPG in NAT/Route mode, go to [NAT/Route mode installation](#).
- If you are going to run your DFL-1000 NPG in Transparent mode, go to [Transparent mode installation](#).

This chapter includes:

- [Package contents](#)
- [Mounting](#)
- [Powering on](#)
- [Initial configuration](#)
- [Connecting to the web-based manager](#)
- [Connecting to the command line interface \(CLI\)](#)
- [Next steps](#)

Package contents

The DFL-1000 package contains the following items:

- DFL-1000 NPG
- one orange crossover ethernet cable
- one gray regular ethernet cable
- one null modem cable
- DFL-1000 QuickStart Guide
- one power cable
- CD containing this *DFL-1000 User Manual* and the *DFL-1000 CLI Reference Guide*
- two 19-inch rack mount brackets

DFL-1000 package contents



Mounting

The DFL-1000 NPG can be installed on any stable surface. Make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

The DFL-1000 NPG can also be mounted on a standard 19-inch rack. It requires 1 U of vertical space in the rack.

Dimensions

- 16.8 x 10 x 1.75 in. (42.7 x 25.4 x 4.5 cm)

Weight

- 7.3 lb. (3.3 kg)

Power requirements

- Power dissipation: 50 W (max)
- AC input voltage: 100 to 240 VAC
- AC input current: 1.6 A
- Frequency: 50 to 60 H

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-1000 NPG:

- Make sure that the power switch on the back of the DFL-1000 NPG is turned off.
- Connect the power cable to the power connection at the back of the DFL-1000 NPG.
- Connect the power cable to a power outlet.
- Turn on the power switch.

The DFL-1000 NPG starts up. The Power and Status lights light. The Status light flashes while the DFL-1000 NPG is starting up and remains lit when the system is up and running.

Front and back view of the DFL-1000 NPG

DFL-1000 LED indicators		
LED	State	Description
Power	Green	The DFL-1000 NPG is powered on.
	Off	The DFL-1000 NPG is powered off.
Status	Flashing green	The DFL-1000 NPG is starting up.
	Green	The DFL-1000 NPG is running normally.

	Off	The DFL-1000 NPG is powered off.
Internal External DMZ (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 DMZ interfaces (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.

Initial configuration

When the DFL-1000 NPG is first powered on, it is running in NAT/Route mode and has the basic configuration listed in [DFL-1000 NPG initial power-on settings](#).

DFL-1000 NPG 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:	192.168.100.1
		Primary DNS Server:	207.194.200.1
		Secondary DNS Server:	207.194.200.129
DMZ interface		IP:	10.10.10.1
		Netmask:	255.255.255.0

Connecting to the web-based manager

The web-based manager is the primary tool for installing and configuring your DFL-1000 NPG. Configuration changes made with the web-based manager are effective immediately without the need to reset the firewall or interrupt service.

To connect to the web-based manager, you need:

- 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-1000 NPG to the computer ethernet connection.
- Start Internet Explorer and browse to the address <https://192.168.1.99>.
The DFL-1000 login appears.
- Type *admin* in the Name field and select Login.
The Register Now window appears. Use the information on this window to register your DFL-1000 NPG. Register your DFL-1000 NPG so that D-Link can contact you for firmware updates.

DFL-1000 login



Connecting to the command line interface (CLI)

As an alternative to the web-based manager, you can install and configure the DFL-1000 NPG using the CLI. Configuration changes made with the CLI are effective immediately without the need to reset the firewall or interrupt service.

To connect to the DFL-1000 CLI, you need:

- a computer with an available communications port,
- the null modem cable included in your DFL-1000 package,
- terminal emulation software such as HyperTerminal for Windows.



The following procedure describes how to connect to the DFL-1000 CLI using Windows HyperTerminal software. You can use any terminal emulation program.

- Connect the null modem cable to the DFL-1000 Console connector and to the available communications port on your computer.
- Make sure that the DFL-1000 NPG is powered on.
- Start HyperTerminal, enter a name for the connection, and select OK.
- Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable 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-1000 CLI.

The following prompt appears:

DFL-1000 login:

- Type *admin* and press Enter twice.

The following prompt appears:

Type ? for a list of commands.

For information on how to use the CLI, see the *DFL-1000 CLI Reference Guide* .

Next steps

Now that your DFL-1000 NPG is up and running, you can proceed to configure it for operation:

- If you are going to run your DFL-1000 NPG in NAT/Route mode, go to [NAT/Route mode installation](#).
- If you are going to run your DFL-1000 NPG in Transparent mode, go to [Transparent mode installation](#).

NAT/Route mode installation

This chapter describes how to install your DFL-1000 NPG in NAT/Route mode. If you want to install the DFL-1000 NPG 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 networks](#)
- [Configuring your networks](#)
- [Completing the configuration](#)

Preparing to configure NAT/Route mode

Use [NAT/Route mode settings](#) to gather the information that 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 servers	Web Server:	_____ . _____ . _____ . _____
	SMTP Server:	_____ . _____ . _____ . _____
	POP3 Server:	_____ . _____ . _____ . _____
	IMAP Server:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____
If you provide access from the Internet to a web server, mail server, IMAP 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-1000 NAT/Route mode settings](#) to gather the information that you need to customize advanced DFL-1000 NAT/Route mode settings.

Advanced DFL-1000 NAT/Route mode settings		
External interface	DHCP:	If your Internet Service Provider (ISP) supplies you with an IP address using DHCP, no further information is required.

	PPPoE:	User name:	<input type="text"/>
		Password:	<input type="text"/>
If your ISP supplies you with an IP address using PPPoE, record your PPPoE user name and password.			
DHCP server	<input type="text"/>	Starting IP:	<input type="text"/>
	<input type="text"/>	Ending IP:	<input type="text"/>
	<input type="text"/>	Netmask:	<input type="text"/>
	<input type="text"/>	Default Route:	<input type="text"/>
	<input type="text"/>	DNS IP:	<input type="text"/>
The DFL-1000 NPG contains a DHCP server that you can configure to automatically set the addresses of the computers on your internal network.			

DMZ interface

Use [DMZ interface \(Optional\)](#) to record the IP address and netmask of the DFL-1000 DMZ interface if you are configuring it during installation.

DMZ interface (Optional)	
DMZ IP:	<input type="text"/> Netmask: <input type="text"/>

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your DFL-1000 NPG. To connect to the web-based manager, see [Connecting to the web-based manager](#).

Starting the setup wizard

- Select Easy Setup Wizard (the middle button in upper-right corner 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.



If you use the setup wizard to configure internal server settings, the DFL-1000 NPG adds port forwarding virtual IPs and firewall policies for each server that you configure. For each server located on your internal network the DFL-1000 adds an Ext -> Int policy. For each server located on your DMZ network, the DFL-1000 NPG adds an Ext -> DMZ policy.

Reconnecting to the web-based manager

If you changed the IP address of the internal interface 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-1000 NPG, and you can proceed to connect the DFL-1000 NPG to your network using the information in [Connecting to your networks](#).

Using the command line interface

As an alternative to using the setup wizard, you can configure the DFL-1000 NPG using the command line interface (CLI). To connect to the CLI, see [Connecting to the command line interface \(CLI\)](#).

Configuring the DFL-1000 NPG 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

- Log into 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 static ip <IP address> <netmask>
```

Example

```
set system interface internal static 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 static ip <IP address> <netmask>
```

Example

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


To set the external interface to use DHCP, enter:

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


To set the external interface to use PPPoE, enter:

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

Example

```
set system interface external pppoe username user@domain.com password  
mypass connection enable
```
- Optionally set the IP address and netmask of the DMZ interface to the DMZ IP address and netmask that you recorded in [DMZ interface \(Optional\)](#). Enter:

```
set system interface dmz static ip <IP address> <netmask>
```

Example

```
set system interface dmz static ip 10.10.10.2 255.255.255.0
```
- Confirm that the addresses are correct. Enter:

```
get system interface
```

The CLI lists the IP address, netmask and other settings for each of the DFL-1000 NPG interfaces as well as the mode of the external interface (manual, DHCP, or PPPoE).
- Set the default route to the default gateway IP address that you recorded in [NAT/Route mode settings](#) (not required for DHCP and PPPoE). Enter:

```
set system route number <number> gw1 <IP address>
```

Example

```
set system route number 1 gw1 204.23.1.2
```

You have now completed the initial configuration of your DFL-1000 NPG, and you can proceed to connect the DFL-1000 NPG to your network using the information in [Connecting to your networks](#).

Connecting to your networks

When you have completed the initial configuration, you can connect the DFL-1000 NPG between your internal network and the Internet.

There are three 10/100Base-TX connectors on the DFL-1000 NPG:

- Internal for connecting to your internal network
- External for connecting to the Internet
- DMZ for connecting to a DMZ network



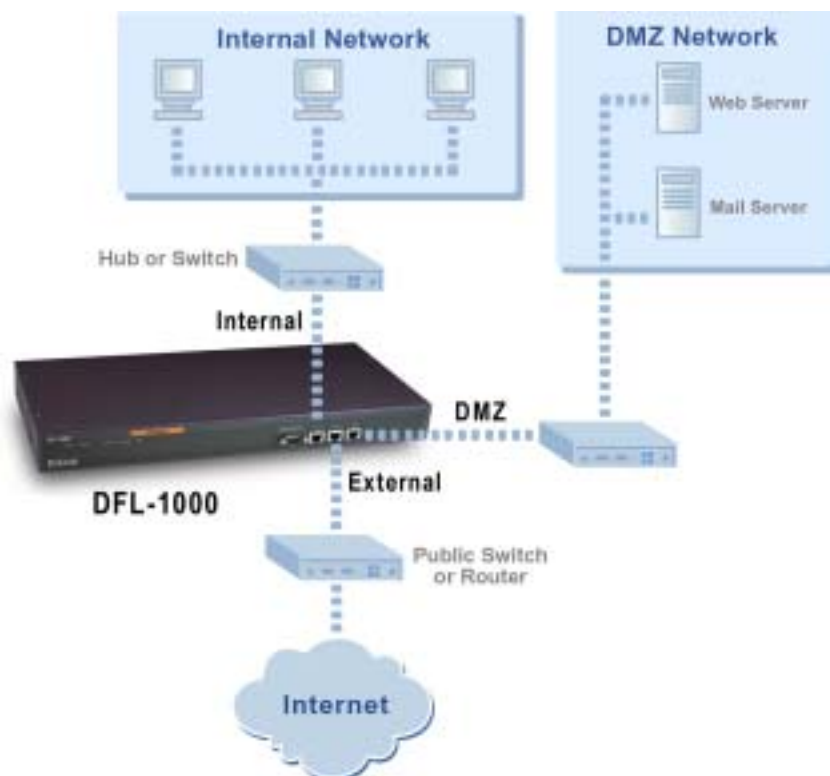
You can also connect both the external and DMZ interfaces to different Internet connections to provide a redundant connection to the Internet. See [Configuring the DFL-1000 NPG for multiple Internet connections](#).

To connect the DFL-1000 NPG:

- Connect the Internal interface to the hub or switch connected to your internal network.
- Optionally connect the DMZ interface to your DMZ network.

You can use a DMZ network to provide access from the Internet to a web server or other server without installing the servers on your internal network.

DFL-1000 NAT/Route mode connections



Configuring your networks

If you are running the DFL-1000 NPG in NAT/Route mode, your networks must be configured to route all Internet traffic to the IP address of the DFL-1000 NPG interface connected to that network. For your internal network, change the default gateway address of all computers and routers connected directly to

your internal network to the IP address of the DFL-1000 NPG internal interface. For your DMZ network, change the default gateway address of all computers and routers connected directly to your DMZ network to the IP address of the DFL-1000 DMZ interface. For your external network, route all packets to the DFL-1000 NPG external interface.

If you are using the DFL-1000 NPG as the DHCP server for your internal network, configure the computers on your internal network for DHCP.


When the DFL-1000 NPG is connected, make sure that 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-1000 NPG.

Configuring the DMZ interface

If you are planning to configure a DMZ network, you might want to change the IP address of the DMZ interface. Use the following procedure to configure the DMZ interface using the web-based manager.

- Log into the web-based manager.
- Go to **System > Network > Interface** .
- For the dmz interface, select Modify .
- Change the IP address and Netmask as required.
- Select Apply.

Setting the date and time

For effective scheduling and logging, the DFL-1000 NPG date and time should be accurate. You can either manually set the DFL-1000 NPG time or you can configure the DFL-1000 NPG to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the DFL-1000 NPG date and time, see [Setting system date and time](#).

Transparent mode installation

This chapter describes how to install your DFL-1000 NPG in Transparent mode. If you want to install the DFL-1000 NPG 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 networks](#)

Preparing to configure Transparent mode

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

Transparent mode settings			
Administrator Password:			
Management IP	<input type="checkbox"/>	IP:	_____ . _____ . _____ . _____
	<input type="checkbox"/>	Netmask:	_____ . _____ . _____ . _____
	<input type="checkbox"/>	Default Gateway:	_____ . _____ . _____ . _____
	The management IP address and netmask must be valid for the network from which you will manage the DFL-1000 NPG. Add a default gateway if the DFL-1000 NPG must connect to a router to reach the management computer.		
DNS Settings	<input type="checkbox"/>	Primary DNS Server:	_____ . _____ . _____ . _____
	<input type="checkbox"/>	Secondary DNS Server:	_____ . _____ . _____ . _____

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your DFL-1000 NPG. To connect to the web-based manager, see [Connecting to the web-based manager](#).

Changing to Transparent mode

The first time that you connect to the DFL-1000 NPG, it is configured to run in NAT/Route mode. To switch to Transparent mode using the web-based manager:

- Go to *System > Status* .
- Select Change to Transparent Mode.
- Select Transparent in the Operation Mode list.
- Select OK.

The DFL-1000 NPG changes to Transparent mode.

To reconnect to the web-based manager, change the IP address of your management computer to 10.10.10.2. Connect to the DFL-1000 NPG internal or DMZ interface and browse to https:// followed by

the Transparent mode management IP address. The default DFL-1000 NPG Transparent mode management IP address is 10.10.10.1.

Starting the setup wizard

- Select Easy Setup Wizard (the middle button in upper-right corner 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 you were using the setup wizard, you must reconnect to the web-based manager using the 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://10.10.10.1. If you connect to the management interface through a router, make sure that 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-1000 NPG using the command line interface (CLI). To connect to the CLI, see [Connecting to the command line interface \(CLI\)](#). Use the information that you gathered in [Transparent mode settings](#) to complete the following procedures.

Changing to Transparent mode

- Log into the CLI if you are not already logged in.
- Switch to Transparent mode. Enter:

```
set system opmode transparent
```

After a few seconds, the following prompt appears:

```
DFL-1000 login:
```
- Type `admin` and press Enter.
The following prompt appears:

```
Type ? for a list of commands.
```
- Confirm that the DFL-1000 NPG has switched to Transparent mode. Enter:

```
get system status
```

The CLI displays the status of the DFL-1000 NPG. The last line shows the current operation mode.

Configuring the Transparent mode management IP address

- Log into the CLI if you are not already logged in.
- Set the management IP address and netmask to the IP address and netmask that you recorded in [Transparent mode settings](#). Enter:

```
set system management ip <IP address> <netmask>
```

Example

```
set system management ip 10.10.10.2 255.255.255.0
```
- Confirm that the address is correct. Enter:

```
get system management
```

The CLI lists the management IP address and netmask.

Configure the Transparent mode default gateway

- Log into 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 route number <number> gateway <IP address>`

Example

```
set system route number 1 gateway 204.23.1.2
```

You have now completed the initial configuration of the DFL-1000 NPG, and you can proceed to the next section.

Setting the date and time

For effective scheduling and logging, the DFL-1000 NPG date and time should be accurate. You can either manually set the time or you can configure the DFL-1000 NPG to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the DFL-1000 NPG date and time, see [Setting system date and time](#).

Connecting to your networks

When you have completed the initial configuration, you can connect the DFL-1000 NPG between your internal network and the Internet. You can also connect a network to the DMZ interface.

There are three 10/100Base-TX connectors on the DFL-1000 NPG:

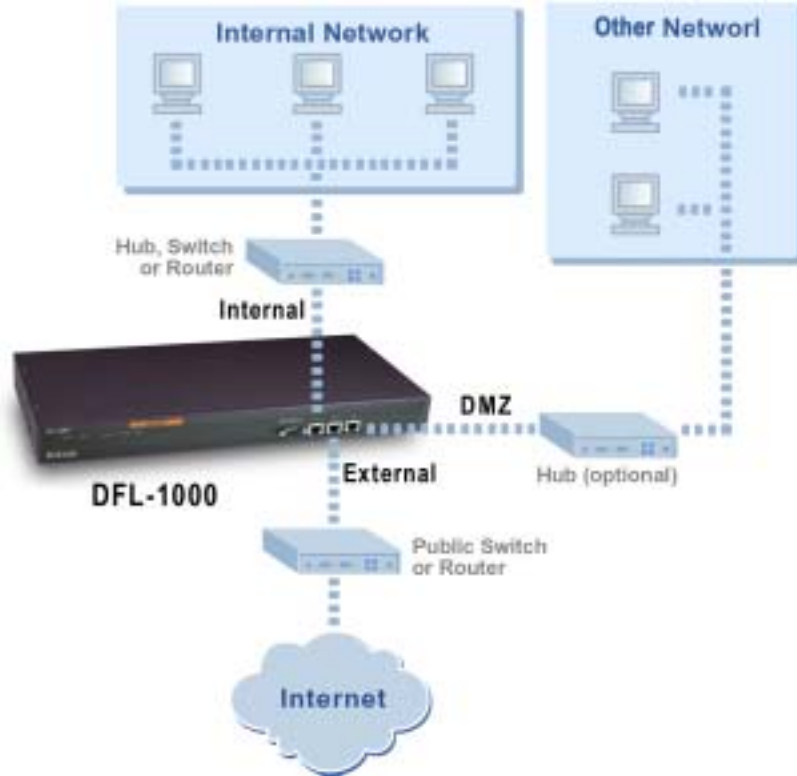
- Internal for connecting to your internal network
- External for connecting to the Internet
- DMZ for connecting to another network

To connect the DFL-1000 NPG running in Transparent mode:

Connect the Internal interface to the hub or switch connected to your internal network.

- Connect the DMZ interface to another network.

DFL-1000 Transparent mode connections



Firewall configuration

By default, the users on your internal network can connect through the DFL-1000 NPG to the Internet. The firewall blocks all other connections. The firewall is configured with a default policy that matches any connection request received from the internal network and instructs the firewall to forward the connection to the Internet.

Default policy



#	Source	Dest	Schedule	Service	Action	Enable	Config
1	Internal_All	External_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	

New

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-1000 NPG, you must have added a policy that matches 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, require authentication before the connection is allowed, or process the packet as an IPsec VPN packet.

You can enable and disable policies. You can add schedules to policies so that the firewall can process connections differently depending on the time of day or the day of the week, month, or year. You can also enable web content filtering for policies that control HTTP, SMTP, IMAP, or POP3 services.

Int -> Ext, Int -> DMZ, and DMZ -> Ext policies control connections from more secure to less secure networks. You can use these policies to apply web content filtering to protect users and servers on your internal network from downloading undesirable content from the Internet. You can also use these policies to control IPsec VPN connections through the firewall.

Ext -> Int, DMZ -> Int, and Ext -> DMZ policies control connections from less secure to more secure networks. You can use these policies to apply web content filtering to protect users and servers on the Internet from downloading undesirable content from your DMZ network. You can also use these policies to control IPsec VPN connections through the firewall and to allow remote users to connect to your internal or DMZ network using PPTP and L2TP VPN.

This chapter describes:

- [NAT/Route mode and Transparent mode](#)
- [Adding NAT/Route mode policies](#)
- [Adding Transparent mode policies](#)
- [Configuring policy lists](#)
- [Addresses](#)
- [Services](#)
- [Schedules](#)
- [Virtual IPs](#)
- [IP pools](#)
- [IP/MAC binding](#)

NAT/Route mode and Transparent mode

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

NAT/Route mode

Run the DFL-1000 NPG in NAT/Route mode to protect private networks from public networks. When the DFL-1000 NPG is running in NAT/Route mode, you can connect a private network to the internal interface, a DMZ network to the DMZ interface, and a public network, such as the Internet, to the external interface. Each of these networks must have a different subnet address. You create security policies to control how the firewall routes packets between DFL-1000 interfaces, and therefore between the networks connected to the interfaces.

In NAT/Route mode, you can create NAT mode policies and Route mode policies.

- NAT mode policies use network address translation to hide the addresses of a more secure network from users on a less secure network.
- Route mode policies control connections between networks without performing address translation.

Transparent mode

Run the DFL-1000 NPG in Transparent mode to provide firewall protection to a network with public addresses. The DFL-1000 NPG can be inserted in your network at any point without the need to make changes to your network or any of its components.

In Transparent mode, you add Transparent mode policies to accept or deny connections between interfaces. The firewall applies policies to control network traffic without modifying the packets in any way.

Changing to Transparent mode

Use the procedure [Changing to Transparent mode](#) to switch the DFL-1000 NPG from NAT/Route mode to Transparent mode.



Changing to Transparent mode deletes all NAT/Route mode policies and addresses. In addition, any routing set in NAT mode is also deleted. This includes the default route that is part of the default NAT configuration.

Changing to NAT/Route mode

Use the procedure [Changing to NAT/Route mode](#) to switch the DFL-1000 NPG from Transparent mode to NAT/Route mode.




Changing to NAT/Route mode deletes all Transparent mode policies and addresses. In addition, any routing set in NAT mode is also deleted. This includes the default route that is part of the default NAT configuration.

Adding NAT/Route mode policies

Add NAT/Route mode policies to control connections and traffic between DFL-1000 interfaces. If you have configured the DFL-1000 NPG for NAT/Route mode operation, you can use the following procedure to add NAT/Route mode policies.

- Go to *Firewall > Policy* .
- Select the policy list to which you want to add the policy.
- 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:

Source	Select an address or address group that matches the source address of the packet. Before you can add this address to a policy, you must add it to the source interface. To add an address, see Addresses .
Destination	Select an address or address group that matches the destination address of the packet. Before you can add this address to a policy, you must add it to the destination interface. To add an address, see Addresses . For a DMZ -> Int, Ext -> Int, or Ext -> DMZ NAT mode policy, the destination can also be a static NAT or port forwarding virtual IP that maps the destination address to a hidden destination address on the internal or DMZ network. See Virtual IPs .
Schedule	Select a schedule that controls when the policy is available to be matched with connections. See Schedules .
Service	Select a service that matches the service (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.
ACCEPT	Accept the connection. If you select ACCEPT, you can also configure NAT and Authentication for the policy.
DENY	Deny the connection.
ENCRYPT	Make this policy an IPsec VPN policy. If you select ENCRYPT, you can select an AutoIKE key or Manual Key VPN tunnel for the policy and configure other IPsec settings. For ENCRYPT policies, service is set to ANY and authentication is not supported. See IPsec VPNs .
NAT	Configure the policy for NAT. NAT translates the source address and the source port of packets accepted by the policy. If you select NAT, you can also select Dynamic IP Pool and Fixed Port.
Dynamic IP Pool	Select Dynamic IP Pool to translate the source address to an address randomly selected from an IP pool added to the destination interface of the policy. To add IP pools, see IP pools . You cannot select Dynamic IP Pool for Int -> Ext or DMZ -> Ext policies if the external interface is configured using DHCP or PPPoE.
Fixed Port	Select Fixed Port to prevent NAT from translating the source port. Some applications do not function correctly if the source port is changed. If you select Fixed Port, you must also select Dynamic IP Pool and add a dynamic IP pool address range to the destination interface of the policy. If you do not select Dynamic IP Pool, a policy with Fixed Port selected can only allow one connection at a time for this port or service.
VPN Tunnel	Select a VPN tunnel for an ENCRYPT policy. You can select an AutoIKE key or Manual Key tunnel.
Allow inbound	Select Allow inbound so that users behind the remote VPN gateway can connect to the source address.
Allow outbound	Select Allow outbound so that users can connect to the destination address behind the remote VPN gateway.
Inbound NAT	Select Inbound NAT to translate the source address of incoming packets to the DFL-1000 NPG internal IP address.
Outbound NAT	Select Inbound NAT to translate the source address of outgoing packets to the DFL-1000 NPG external IP address.
Traffic Shaping	Traffic Shaping controls the bandwidth available to and sets the priority of the traffic processed by the policy. Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the DFL-1000 NPG. 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.

Guaranteed Bandwidth	You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth (in kbps) to make sure that there is enough bandwidth available for a high-priority service.
Maximum Bandwidth	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.
Traffic Priority	Select High, Medium, or Low. Select Traffic Priority so that the DFL-1000 NPG 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.
Log Traffic	Select Log Traffic to write messages to the traffic log whenever the policy processes a connection.
Authentication	<p>Select Authentication and select a user group to require users to enter a user name and password before the firewall accepts the connection. Select the user group to control the users that can authenticate with this policy. To add and configure user groups, see Users and authentication. You must add user groups before you can select Authentication.</p> <p>You can select Authentication for any service. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt to connect through the firewall using this policy they are prompted to enter a firewall username and password.</p> <p>If you want users to authenticate to use other services (for example POP3 or IMAP) you can create a service group that includes the services for which you want to require authentication as well as HTTP, Telnet, and FTP. Then users could authenticate with the policy using HTTP, Telnet, or FTP before using the other service.</p> <p>In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or Telnet server using a domain name.</p>
Web filter	<p>Enable web filter content filtering for traffic controlled by this policy. You can select Web filter if Service is set to ANY, HTTP, SMTP, POP3, or IMAP, or to a service group that includes the HTTP, SMTP, POP3, or IMAP services.</p> <p>For web filter content filtering to take effect, you must configure web content filtering. See Web content filtering.</p> <p>You can select show settings to display the current web filter content filtering settings for the DFL-1000 NPG.</p>

- Select OK to add the policy.
- Arrange policies in the policy list so that they have the results that you expect. Arranging policies in a policy list is described in [Configuring policy lists](#).

Adding a NAT/Route Int -> Ext policy

The screenshot shows the 'New Policy' configuration window. The 'Int->Ext' tab is active. The configuration is as follows:

Source	Internal_Address1
Destination	External_All
Schedule	Always
Service	HTTP
Action	ACCEPT

Below the main configuration, there are several sections:

- NAT: Dynamic IP Pool Fixed Port
- Traffic Shaping: Guaranteed Bandwidth 100 (Kbytes/sec), Maximum Bandwidth 1000 (Kbytes/sec), Traffic Priority Medium
- Authentication: Firewall_User_Gro
- Log Traffic
- Web filter [show settings](#)

Buttons: OK, Cancel

Adding Transparent mode policies

Add Transparent mode policies to control the network traffic that is allowed to pass through the DFL-1000 NPG when you are running the firewall in Transparent mode.

- 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:

Source Select an address or address group that matches the source address of the packet. Before you can add this address to a policy, you must add it to the source interface. To add an address, see [Addresses](#).

Destination Select an address or address group that matches the destination address of the packet. Before you can add this address to a policy, you must add it to the destination interface. To add an address, see [Addresses](#).

Schedule A schedule that controls when this policy is available to be matched with connections. See [Schedules](#).

Service A service that matches the service (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 or DENY the connection. If you select ACCEPT, you can also configure Authentication for the policy.

Traffic Shaping Traffic Shaping controls the bandwidth available to and sets the priority of the traffic processed by the policy.

Log Traffic Select Log Traffic to write messages to the traffic log whenever the policy processes a connection.

Select Authentication and select a user group to require users to enter a user name and password before the firewall accepts the connection. Select the user group to control the users that can authenticate with this policy. To add and configure user groups, see [Users and authentication](#). You must add user groups before you can select Authentication.

Authentication You can select Authentication for any service. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt to connect through the firewall using this policy they are prompted to enter a firewall username and password.

If you want users to authenticate to use other services (for example POP3 or IMAP) you can create a service group that includes the services for which you want to require authentication as well as HTTP, Telnet, and FTP. Then users could authenticate with the policy using HTTP, Telnet, or FTP before using the other service.

In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or Telnet server using a domain name.

Enable web filter content filtering for traffic controlled by this policy. You can select Web filter if Service is set to ANY, HTTP, SMTP, POP3, or IMAP, or to a service group that includes the HTTP, SMTP, POP3, or IMAP services.

Web filter For web filter content filtering to take effect, you must configure web content filtering. See [Web content filtering](#).

You can select show settings to display the current web filter content filtering settings for the DFL-1000 NPG.

- Select OK to add the policy.
The policy is added to the policy list.
- Arrange policies in the policy list so that they have the results that you expect.
Arranging policies in a policy list is described in [Configuring policy lists](#).

Adding a Transparent mode Int -> Ext policy

The screenshot shows the 'New Policy' configuration window in a firewall interface. The window is titled 'New Policy' and has a tabbed interface with 'Int->Ext' selected. The configuration fields are: Source: Internal_Users, Destination: External_All, Schedule: Always, Service: POP3, Action: ACCEPT. Below these are sections for NAT (checked), Traffic Shaping (unchecked), Authentication (checked), and Log Traffic (checked). The Web filter is also checked with a 'show settings' link. Buttons for 'OK' and 'Cancel' are at the bottom.

Configuring policy lists

The firewall 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. When you create exceptions to this policy, you must add them to the policy list above the default policy. No policy below the default policy will ever be matched.

This section describes:

- [Policy matching in detail](#)
- [Changing the order of policies in a policy list](#)
- [Enabling and disabling policies](#)

Policy matching in detail

When the DFL-1000 NPG receives a connection attempt at an interface, it must select a policy list to search through for a policy that matches the connection attempt. Each interface has two policy lists (for example, the two external interface policy lists are Ext -> Int and Ext -> DMZ). The DFL-1000 NPG chooses the policy list based on the destination address of the connection attempt.

The DFL-1000 NPG then starts at the top of the selected policy list 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-1000 NPG, and so on. If the default policy is at the top of the Int -> 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 -> Ext policy list. In this example, all FTP connection attempts from the internal network would then 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. Therefore, the firewall would still accept all other connections from the internal network.



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.

Changing the order of policies in a policy list

- 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.

Enabling and disabling policies

You can enable and disable policies in the policy list to control whether the policy is active or not. The DFL-1000 NPG matches enabled policies but does not match disabled policies.

Disabling a policy

Disable a policy to temporarily prevent the firewall from selecting the policy.

- Go to *Firewall > Policy* .
- Select the tab for the policy list containing the policy to disable.
- Clear the check box of the policy to disable.

Enabling a policy

Enable a policy that has been disabled so that the firewall can match connections with the policy.

- Go to *Firewall > Policy* .
- Select the tab for the policy list containing the policy to enable.
- Select the check box of the policy to enable.

Addresses

All policies require source and destination addresses. 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 firewall includes two addresses that cannot be edited or deleted:

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

You can add, edit, and delete all other addresses as required. You can also organize related addresses into address groups to simplify policy creation.

This section describes:

- [Adding addresses](#)
- [Editing addresses](#)
- [Deleting addresses](#)
- [Organizing addresses into address groups](#)

Adding addresses

- 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), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Spaces and other special characters are not allowed.
- Enter 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.
- Enter 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.

Adding an internal address


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

Field	Value
Address Name	Web_Server
IP Address	192.168.1.34
Netmask	255.255.255.255

Buttons: OK, Cancel



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 add it again with a new name.

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

Deleting addresses

Deleting an address removes it from an address list. After the address is removed, it can no longer be added to policies. To delete an address that has been added to a policy, you must first remove the address from the policy.

- Go to *Firewall > Address* .
- Select the interface list containing the address that you want to delete.
You can delete any listed address that has a Delete Address icon .
- Choose an address to delete and select Delete .
- Select OK to delete the address.

Organizing addresses into address groups

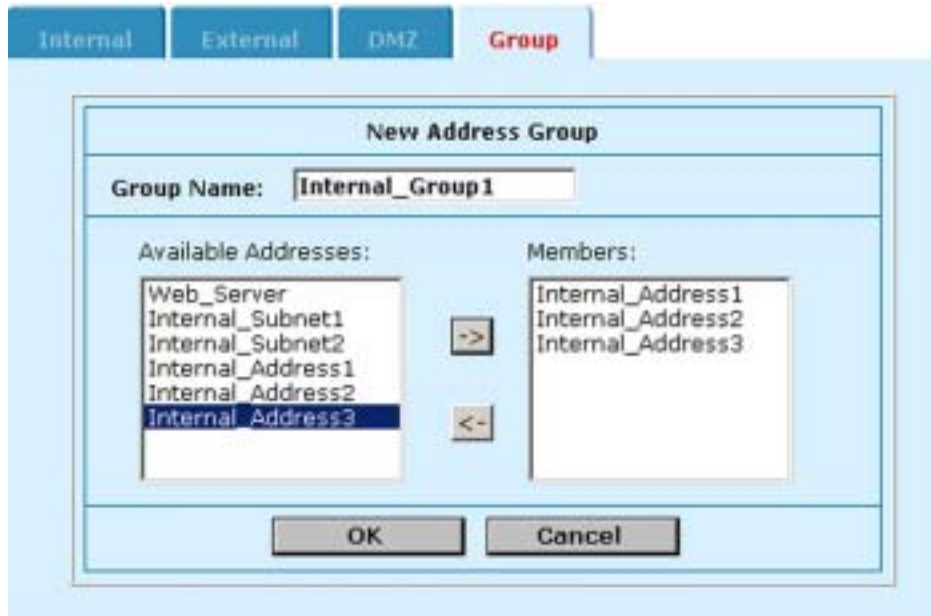
You can organize related addresses into address groups to make it easier to add policies. For example, if you add three addresses and then add them to an address group, you only have to add one policy for the address group rather than three separate policies, one for each address.

You can add address groups to any interface. The address group can only contain addresses from that interface. Address groups are available in interface source or destination address lists.

Address groups cannot have the same names as individual addresses. If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.

- Go to *Firewall > Address > Group* .
- Select the interface to which to add the address group: New Int. Group, New Ext. Group, or New DMZ Group.
- Enter a Group Name to identify the address group.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.
- To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.
- Select OK to add the address group.

Adding an internal address group



Services

Use services to control the types of communication accepted or denied by the firewall. You can add any of the predefined services to a policy. You can also create your own custom services and add services to service groups.

This section describes:

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

Predefined services

The DFL-1000 predefined firewall services are listed in [DFL-1000 predefined services](#). You can add these services to any policy.


DFL-1000 predefined services			
Service name	Description	Protocol	Port
ANY	Match connections on any port. A connection that uses any of the predefined services is allowed through the firewall.	all	all
GRE	Generic Routing Encapsulation. A protocol that allows an arbitrary network protocol to be transmitted over any other arbitrary network protocol, by encapsulating the packets of the protocol within GRE packets.		47
AH	Authentication Header. AH provides source host authentication and data integrity, but not secrecy. This protocol is used for authentication by IPSec remote gateways set to aggressive mode.		51
ESP	Encapsulating Security Payload. This service is used by manual key and AutoIKE VPN tunnels for communicating encrypted data. AutoIKE key VPN tunnels use ESP after establishing the tunnel using IKE.		50

AOL	AOL instant messenger protocol.	tcp	5190-5194
BGP	Border Gateway Protocol routing protocol.	tcp	179
DHCP-Relay	DHCP relay service.	udp	67
DNS	Domain name servers for looking up domain names.	tcp	53
		udp	53
FINGER	Finger service.	tcp	79
FTP	FTP service for transferring files.	tcp	21
GOPHER	Gopher communication service.	tcp	70
H323	H.323 multimedia protocol. Can be used for IP telephony through the firewall.	tcp	1720, 1503
HTTP	HTTP service for connecting to web pages.	tcp	80
HTTPS	SSL service for secure communications with web servers.	tcp	443
IKE	AutoIKE Internet key exchange service. You can add policies with service set to IKE to control IPSec connections through the firewall.	udp	500
IMAP	IMAP email protocol for reading email from an IMAP server.	tcp	143
Internet-Locator-Service	An LDAP-related service for locating user addresses.	tcp	389
IRC	Internet relay chat for connecting to chat groups.	tcp	6660-6669
L2TP	L2TP VPN service.	tcp	1701
LDAP	LDAP directory lookup service.	tcp	389
NetMeeting	NetMeeting multimedia conferencing service.	tcp	1720
NFS	Network file services for sharing files.	tcp	111, 2049
NNTP	Protocol for transmitting Usenet news.	tcp	119
NTP	Network time protocol for synchronizing a computer's time with a time server.	tcp	123
OSPF	Open Shortest Path First (OSPF) routing protocol.		89
PC-Anywhere	For remote access to a PC.	udp	5632
PING	For testing connections to other computers.	icmp	8
POP3	POP3 email protocol for downloading email from a POP3 server.	tcp	110
PPTP	PPTP VPN service.	tcp	1723
QUAKE	For connections used by the popular Quake multi-player computer game.	udp	26000, 27000, 27910, 27960
RAUDIO	For streaming real audio multimedia traffic.	udp	7070
RLOGIN	Rlogin service for remotely logging into a server.	tcp	513
RIP	Routing Information Protocol.	udp	520
SMTP	For sending mail between email servers on the Internet.	tcp	25
SNMP	For communicating system status information.	tcp	161-162
		udp	161-162
SSH	SSH service for secure connections to computers for remote management.	tcp	22

		udp	22
SYSLOG	Syslog service for remote logging.	udp	514
TALK	A protocol supporting conversations between two or more users.	udp	517-518
TCP	All TCP ports.	tcp	0-65535
TELNET	Telnet service for connecting to a remote computer to run commands.	tcp	23
TFTP	Trivial file transfer protocol, a simple file transfer protocol similar to FTP but with no security features.	udp	69
UDP	All UDP ports.	udp	0-65535
UUCP	Unix to Unix copy utility, a simple file copying protocol.	udp	540
VDOLIVE	For VDO Live streaming multimedia traffic.	tcp	7000-7010
WAIS	Wide Area Information Server. An Internet search protocol.	tcp	210
WINFRAME	For WinFrame communications between computers running Windows NT.	tcp	1494
X-WINDOWS	For remote communications between an X-Windows server and X-Windows clients.	tcp	6000-6063

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 service list.

- 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), uppercase and lowercase 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 Source and Destination Port number range for the service by entering the low and high port numbers. If the service uses one port number, enter this number in 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 each extra row.
- Select OK to add the custom service.
You can now add this custom service to a policy.

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.

- Go to *Firewall > Service > Group*.
- Select New.
- Enter a Group Name to identify the group.
This name appears in the service list when you add a policy and cannot be the same as a predefined service name.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

- 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.

Adding a 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 example, your firewall might 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.

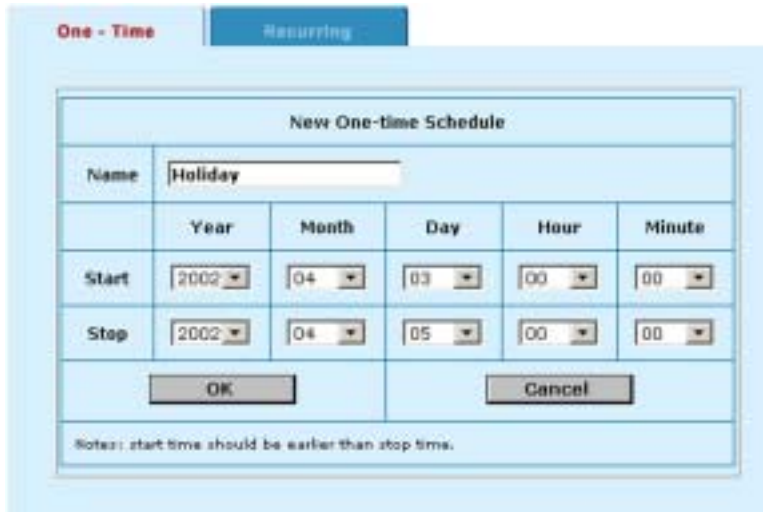


One-time schedules use the 24-hour clock.

- Go to *Firewall > Schedule > One-time* .

- Select New.

Adding a 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.					

- Enter a Name for the schedule.
The name can contain numbers (0-9), uppercase and lowercase 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 be active for the entire day.
- Set the Stop date and time for the schedule.
- Select OK to add the one-time schedule.

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 example, you might want 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.



Recurring schedules use the 24-hour clock.

- Go to *Firewall > Schedule > Recurring* .
- Select New to create a new schedule.

Adding a 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" 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.							

- Enter a Name for the schedule.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- Select the days of the week on which the schedule should be active.
- Set the Start and Stop hours in between which the schedule should be active.
- Select OK.

Adding a schedule to a policy

After 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.

- 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



Virtual IPs


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


For example, if the computer hosting your web server is located on your DMZ network, it could have a private IP address such as 10.10.10.3. To get packets from the Internet to the web server, you must have an external address for the web server on the Internet. You must then add a virtual IP that maps the external IP address of the web server to the actual address of the web server on the DMZ network. To allow connections from the Internet to the web server, you must then add an Ext -> DMZ firewall policy and set Destination to the virtual IP.

You can create two types of virtual IPs:

Static NAT Used in Ext -> Int, Ext -> DMZ, and DMZ -> Int policies to translate an address on a less secure network to a hidden address on a more secure network. Static NAT translates the source address of outbound packets to the address on the less secure network.

Port Forwarding Used in Ext -> Int, Ext -> DMZ, and DMZ -> Int policies to translate an address and a port number on a less secure network to a hidden address and, optionally, a different port number on a more secure network. Using port forwarding you can also route packets with a specific port number and a destination address that matches the IP address of the interface that receives the packets. This technique is called port forwarding or port address translation (PAT). You can also use port forwarding to change the destination port of the forwarded packets.

 If you use the setup wizard to configure internal server settings, the firewall adds port forwarding virtual IPs and policies for each server that you configure. For each server located on your internal network the firewall adds an Ext -> Int policy. For each server located on your DMZ network, the firewall adds an Ext -> DMZ policy.

 Virtual IPs are not required in Transparent mode.

This section describes:

- [Adding static NAT virtual IPs](#) See [Adding static NAT virtual IPs](#)
- [Adding static NAT virtual IPs](#) See [Adding port forwarding virtual IPs](#)
- [Adding static NAT virtual IPs](#) See [Adding policies with virtual IPs](#)

Adding static NAT virtual IPs

- Go to *Firewall > Virtual IP*.

- Select New to add a virtual IP.
- Enter a Name for the virtual IP.

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

- Select the virtual IP External Interface. You can select external or dmz.

external To map an Internet address to an internal or DMZ address. If you select external, the static NAT virtual IP can be added to Ext -> Int and Ext -> DMZ policies.

dmz To map a DMZ address to an internal address. If you select dmz, the static NAT virtual IP can be added to DMZ -> Int policies.

- Make sure Type is set to Static NAT.
- In the External IP Address field, enter the external IP address to be mapped to an address on the more secure network.

For example, if the virtual IP provides access from the Internet to a web server on your DMZ or internal network, the external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique address that is not used by another host and cannot be the same as the IP address of the External Interface selected in step [Select the virtual IP External Interface. You can select external or dmz.](#) However, this address must be routed to this interface.

- In the Map to IP field, enter the real IP address on the more secure network, for example, the IP address of a web server on your DMZ network.

If you enter an address on the same subnet as the internal interface, the virtual IP can be added to Ext -> Int or DMZ -> Int policies.

If you enter an address on the same subnet as the DMZ interface, the virtual IP can be added to Ext -> DMZ policies.



The firewall translates the source address of outbound packets from the host with the Map to IP address to the virtual IP External IP Address, instead of the firewall external address.

- Select OK to save the virtual IP.
You can now add the virtual IP to firewall policies.

Firewall policies to which you can add virtual IPs		
External interface	Map to IP	Firewall policy
external	Same subnet as the internal interface.	Ext -> Int
	Same subnet as the DMZ interface.	Ext -> DMZ
dmz	Same subnet as the internal interface.	DMZ -> Int

Adding a static NAT virtual IP

The screenshot shows a dialog box titled "Add New Virtual IP Mapping" with a "Virtual IP" tab. The dialog contains the following fields and options:

- Name:** Web_Server
- External Interface:** external
- Type:** Static NAT (selected), Port Forwarding
- External IP Address:** 173.87.26.89
- Map to IP:** 10.10.10.5

Buttons: OK, Cancel

Adding port forwarding virtual IPs

- Go to *Firewall > Virtual IP*.
- Select New to add a virtual IP.
- Enter a Name for the virtual IP.

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

- Select the virtual IP External Interface. You can select external or DMZ.

External To map an Internet address to an internal or DMZ address. If you select external, the port forwarding virtual IP can be added to Ext -> Int and Ext -> DMZ policies.

DMZ To map a DMZ address to an internal address. If you select DMZ, the port forwarding virtual IP can be added to DMZ -> Int policies.

- Change Type to Port Forwarding.
- In the External IP Address field, enter the external IP address to be mapped to an address in the more secure zone.

You can set the External IP Address to the address of external interface selected in step [Select the virtual IP External Interface. You can select external or DMZ.](#) or to any other address.

For example, if the virtual IP provides access from the Internet to a server on your internal network, the External IP Address must be a static IP address obtained from your ISP for this server. This address must be a unique address that is not used by another host. However, this address must be routed to the External Interface selected in step [Select the virtual IP External Interface. You can select external or DMZ.](#)

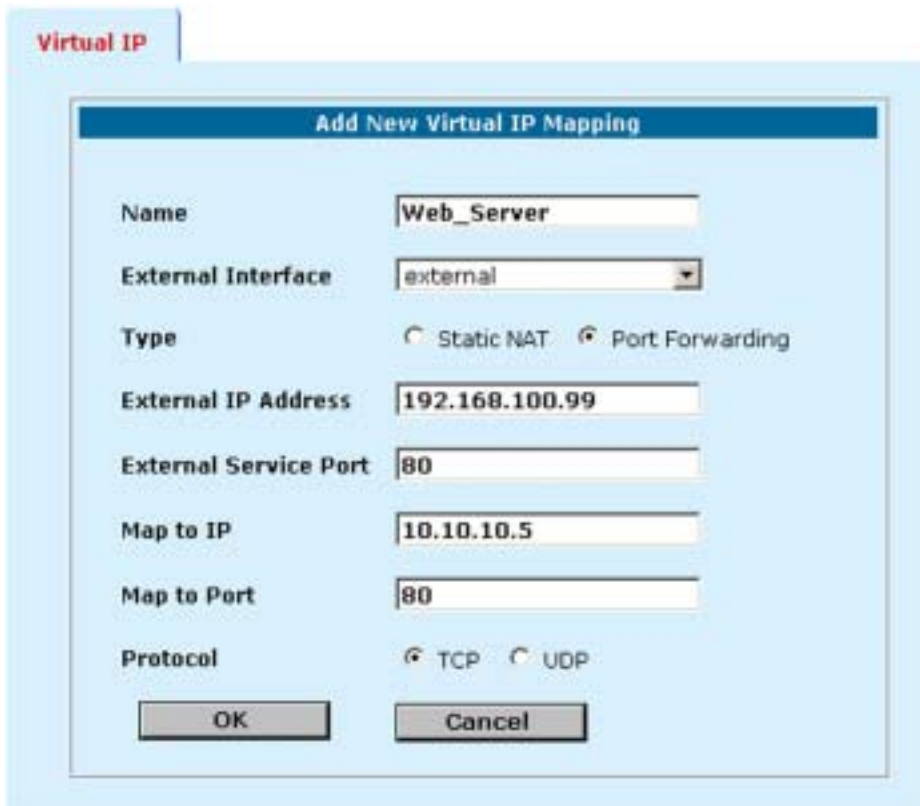
- Enter the External Service Port number for which to configure port forwarding.
The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides access from the Internet to a Web server on your DMZ or internal network, the external service port number would be 80 (the HTTP port).
- In Map to IP, enter the real IP address on the more secure network, for example, the IP address of a web server on your DMZ network.

If you enter an IP address on the same subnet as the internal interface, the virtual IP can be added to Ext -> Int or DMZ -> Int policies.

If you enter an IP address on the same subnet as the DMZ interface, the virtual IP can be added to Ext -> DMZ policies.

- Set Map to Port to the port number to be added to packets when they are forwarded.
If you do not want to translate the port, enter the same number as the External Service Port.
If you want to translate the port, enter the port number to which to translate the destination port of the packets when they are forwarded by the firewall.
- Select the protocol to be used by the forwarded packets.
- Select OK to save the port forwarding virtual IP.

Adding a port forwarding virtual IP



Adding policies with virtual IPs

Use the following procedure to add a policy that uses a virtual IP to forward packets.

- Go to *Firewall > Policy* .
- Select the type of policy to add.

Virtual IP settings and corresponding policy types		
External Interface	MAP to IP	Policy type
external	Internal network IP address.	Ext -> Int
external	DMZ network IP address.	Ext -> DMZ
dmz	Internal network IP address.	DMZ -> Int

- Use the following information to configure the policy.

Source	Select the source address from which users can access the server. For example, if you want to add a policy that allows all users on the Internet to access a server set Source to External_All.
Destination	Select the virtual IP.
Schedule	Select a schedule as required.
Service	Select the service that matches the Map to Service that you selected for the port-forwarding virtual IP.
Action	Set action to ACCEPT to accept connections to the internal server. You can also select DENY to deny access.
NAT	Select NAT if the firewall is protecting the private addresses on the destination network from the source network.
Authentication	Optionally select Authentication and select a user group to require users to authenticate with the firewall before accessing the server using port forwarding.
Log Traffic Web filter	Select these options to log port-forwarded traffic and apply web filter protection to this traffic.

- Select OK to save the policy.

IP pools

An IP pool (also called a dynamic IP pool) is a range of IP addresses added to a firewall interface. The addresses in the IP pool must be on the same subnet as the IP address of the interface. The addresses in the IP pool range cannot conflict with other addresses on the same network as the interface for which you are adding the IP pool. You can add multiple IP pools to any interface.

Add IP pools if you want to add NAT mode policies that translate source addresses to addresses randomly selected from a predefined range of IP addresses. For example, if the IP address of the internal interface is 192.168.1.99, a valid IP pool could have a start IP of 192.168.1.10 and an end IP of 192.168.1.20. This IP pool would give the firewall 11 addresses to select from when translating the source address.

If you add IP pools for an interface, you can select Dynamic IP Pool when you configure a policy with its destination set to this interface. For example, if you add IP pools for the internal interface, you can select IP pools for Ext → Int and DMZ → Int policies.

To add an IP pool:

- Go to Firewall > IP Pool.
- Select the interface to which to add the IP pool.
The list of IP pools added to that interface is displayed.
- Select New to add a new IP pool to the selected interface.
- Enter the Start IP and End IP addresses for the range of addresses in the IP pool.
The Start IP and End IP must define the start and end of an address range. The Start IP must be lower than the End IP. The Start IP and End IP must be on the same subnet as the IP address of the interface for which you are adding the IP pool.
If you have configured the external interface to use PPPoE or DHCP, you can only set the Start IP and End IP to the current IP address of the external interface.
- Select OK.

Adding an IP pool

The screenshot shows a 'New Dynamic IP Pool' dialog box. At the top, there are three tabs: 'Internal' (highlighted in red), 'External', and 'DMZ'. The dialog box contains two input fields: 'Start IP' with the value '192.168.1.50' and 'End IP' with the value '192.168.1.60'. Below the input fields are two buttons: 'OK' and 'Cancel'.

IP/MAC binding

IP/MAC binding protects the DFL-1000 NPG and your network from IP spoofing attacks. IP spoofing attempts to use the IP address of a trusted computer to connect to or through the DFL-1000 NPG 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 static IP addresses and corresponding MAC addresses of trusted computers in the Static IP/MAC table.

If you have trusted computers with dynamic IP addresses that are set by the DFL-1000 DHCP server, the DFL-1000 NPG adds these IP addresses and their corresponding MAC addresses to the Dynamic IP/MAC table. See [Providing DHCP services to your internal network](#). The dynamic IP/MAC binding table is not available in Transparent mode.

IP/MAC binding can be enabled for packets connecting to the firewall or passing through the firewall.



If you enable IP/MAC binding and change the IP address of a computer with an IP address or MAC address in the IP/MAC list, you must also change the entry in the IP/MAC list or the computer will not have access to or through the DFL-1000 NPG. You must also add the IP/MAC address pair of any new computer that you add to your network or this computer will not have access to or through the DFL-1000 NPG.

This section describes:

- [Configuring IP/MAC binding for packets going through the firewall](#)
- [Configuring IP/MAC binding for packets going to the firewall](#)
- [Adding IP/MAC addresses](#)
- [Viewing the dynamic IP/MAC list](#)
- [Enabling IP/MAC binding](#)

Configuring IP/MAC binding for packets going through the firewall

Use the following procedure to use IP/MAC binding to filter packets that would normally be matched with firewall policies to be able to go through the firewall.

- Go to **Firewall > IP/MAC Binding > Setting**.
- Select Enable IP/MAC binding going through the firewall.
- Go to **Firewall > IP/MAC Binding > Static IP/MAC**.
- Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets that would normally be matched with policies to be able to go through the firewall are first compared with the entries in the IP/MAC binding list. If a match is found, then the firewall attempts to match the packet with a policy.

For example, if the IP/MAC pair IP 1.1.1.1 and 12:34:56:78:90:ab:cd is added to the IP/MAC binding list:

- A packet with IP address 1.1.1.1 and MAC address 12:34:56:78:90:ab:cd is allowed to go on to be matched with a firewall policy.
- A packet with IP 1.1.1.1 but with a different MAC address is dropped immediately to prevent IP spoofing.
- A packet with a different IP address but with a MAC address of 12:34:56:78:90:ab:cd is dropped immediately to prevent IP spoofing.
- A packet with both the IP address and MAC address not defined in the IP/MAC binding table:
 - is allowed to go on to be matched with a firewall policy if IP/MAC binding is set to Allow traffic,
 - is blocked if IP/MAC binding is set to Block traffic.

Configuring IP/MAC binding for packets going to the firewall

Use the following procedure to use IP/MAC binding to filter packets that would normally connect with the firewall (for example, when an administrator is connecting to the DFL-1000 NPG for management).

- Go to *Firewall > IP/MAC Binding > Setting* .
- Select Enable IP/MAC binding going to the firewall.
- Go to **Firewall > IP/MAC Binding > Static IP/MAC** .
- Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets normally allowed to connect to the firewall are compared with the entries in the IP/MAC binding table. If a match is found in the IP/MAC binding table:

- If IP/MAC binding is set to Allow traffic, then IP/MAC binding allows the packet to connect to the firewall.
- If IP/MAC binding is set to Block traffic, then IP/MAC binding stops the packet from connecting to the firewall.

Adding IP/MAC addresses

- Go to *Firewall > IP/MAC Binding > Static IP/MAC* .
- Select New to add an IP address/MAC address pair.
- Enter the IP address and the MAC address.

You can bind multiple IP addresses to the same MAC address. You cannot bind multiple MAC addresses to the same IP address.

However, you can set the IP address to 0.0.0.0 for multiple MAC addresses. This means that all packets with these MAC addresses are matched with the IP/MAC binding list.

Similarly, you can set the MAC address to 00:00:00:00:00:00 for multiple IP addresses. This means that all packets with these IP addresses are matched with the IP/MAC binding list.

- Enter a Name for the new IP/MAC address pair.

The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- Select Enable to enable IP/MAC binding for the IP/MAC pair.
- Select OK to save the IP/MAC binding pair.

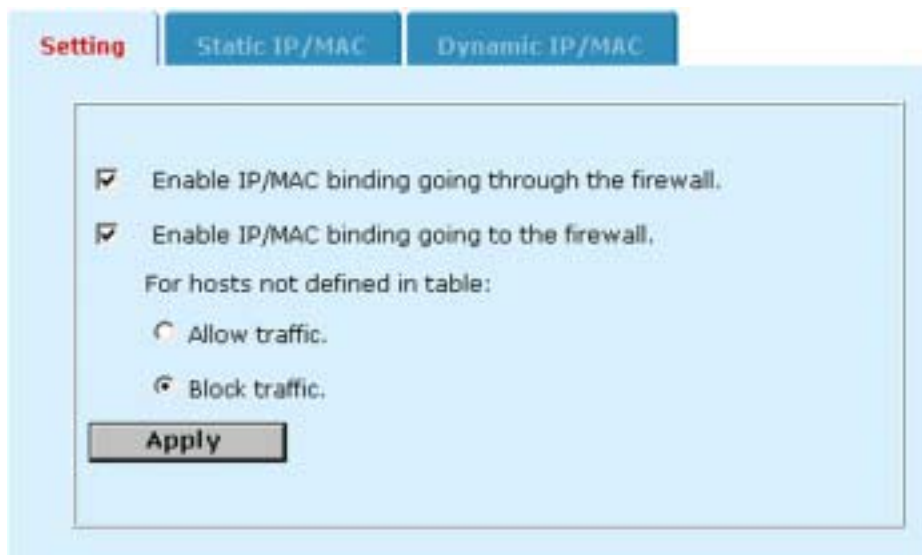
Viewing the dynamic IP/MAC list

- Go to *Firewall > IP/MAC Binding > Dynamic IP/MAC* .

Enabling IP/MAC binding

- Go to *Firewall > IP/MAC Binding > Setting* .
- Select Enable IP/MAC binding going through the firewall to turn on IP/MAC binding for packets that could be matched by policies.
- Select Enable IP/MAC binding going to the firewall to turn on IP/MAC binding for packets connecting to the DFL-1000 NPG.
- Configure how IP/MAC binding handles packets with IP and MAC addresses that are not defined in the IP/MAC list.
Select Allow traffic to allow all packets with IP and MAC address pairs that are not added to the IP/MAC binding list.
Select Block traffic to block packets with IP and MAC address pairs that are not added to the IP/MAC binding list.
- Select Apply to save your changes.

IP/MAC settings



The screenshot shows a configuration window with three tabs: "Setting" (selected), "Static IP/MAC", and "Dynamic IP/MAC". The "Setting" tab contains the following options:

- Enable IP/MAC binding going through the firewall.
- Enable IP/MAC binding going to the firewall.
- For hosts not defined in table:
 - Allow traffic.
 - Block traffic.

An "Apply" button is located at the bottom of the configuration area.

Example policies

- [NAT policy for public access to a server](#)
- [Routing policy for access to a server from the internal network](#)
- [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 policy for public access to a server

The following example NAT policy, to accept connections from the Internet and forward them to the DMZ network, is similar to any NAT policy for connections between a less secure network and a more secure network.

To add a NAT Ext -> DMZ policy:

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

Source	External_All.
Destination	The Virtual IP added in Step 1.
Schedule	Always.
Service	Select a service to match the Internet server. For a web server, select HTTP.
Action	ACCEPT.
NAT	Select NAT.
Authentication	Select Authentication and select a user group if you want users on the Internet to authenticate with the firewall before accessing the server.
Web filter	Select Web filter if service is set to HTTP, SMTP, POP3, or IMAP to apply content filtering to the network traffic allowed by this policy.

- Select OK to save the policy.
- Arrange the policy in the policy list to produce the results that you expect. Arranging policies in a policy list is described in [Configuring policy lists](#).

Routing policy for access to a server from the internal network

The following example routing policy, to accept connections from the internal network and forward them to the DMZ network, is similar to any routing policy. In this example, the DFL-1000 NPG is running in

NAT/Route mode and you do not require NAT for connections between the internal network and the DMZ network. Configuring a routing policy is similar to configuring a NAT policy except that you do not select NAT when you configure the policy.

You can use routing policies for connections between two networks if addresses are routable between these two networks.

To add a routing Int -> DMZ policy:

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

Source	Internal_All.
Destination	The address added in step 1.
Schedule	Always.
Service	Select a service to match the server in the DMZ network. For a web server, select HTTP.
Action	Select ACCEPT.
NAT	Do not select NAT.
Authentication	Select Authentication and select a user group if you want users on the internal network to authenticate with the firewall before accessing the server.
Web filter	Select Web filter if service is set to HTTP, SMTP, POP3, or IMAP to apply content filtering to the network traffic allowed by this policy.

- Select OK to save the policy.
- Arrange the policy in the policy list to produce the results that you expect.
Arranging policies in a policy list is described in [Configuring policy lists](#).

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 [Addresses](#).
- Go to **Firewall > Policy > Ext -> 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.
- Authentication** Select Authentication and select a user group if you want users on the Internet to authenticate with the firewall before accessing the server.
- Web filter** Select Web filter if service is set to HTTP, SMTP, POP3, or IMAP to apply content filtering to the network traffic allowed by this policy.
- Select OK to save the policy.
 - Arrange the policy in the policy list to produce the results that you expect. Arranging policies in a policy list is described in [Configuring policy lists](#).

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 or DMZ 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-1000 NPG 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 policy list containing the policy to which you want to deny access.
- Select Insert Policy before  to insert the new policy before the policy to block. You must add the deny policy above the accept policy in the policy list. For more information, see [Policy matching in detail](#) and [Configuring policy lists](#).
- Configure the new policy to match the policy to block, with the following exceptions:
 - Set Schedule to 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.
 - The policy is added to the policy list above the policy to which you want to deny access.

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-1000 NPG is running in NAT/Route mode.

To deny a connection to the Internet:

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

You must add the deny policy above the default policy in the policy list so that the deny policy is matched before the default policy. For more information on arranging policies in policy lists, see [Policy matching in detail](#) and [Configuring policy lists](#).

- 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.
The policy is added to the policy list above the default policy.

Adding policies that accept connections

Policies that accept connections can be used:


- 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-1000 NPG 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 -> 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 and 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 [Configuring policy lists](#).

Requiring authentication to connect to the Internet

To require authentication, you must add users and user groups to the firewall configuration (see [Users and authentication](#)). You can then add policies to require users to enter a user name and password to access services through the firewall.

You can require authentication:

- for policies between any two interfaces,
- to connect to selected addresses,
- according to a schedule.


You can select authentication for any service. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate, you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt to connect through the firewall using this policy, they are prompted to enter a firewall user name and password.

If you want users to authenticate to use other services (for example, POP3 or IMAP), you can create a service group that includes the services for which you want to require authentication as well as HTTP, Telnet, and FTP. Users can then authenticate with the policy using HTTP, Telnet, or FTP before using the other service.

In most cases, you should make sure that users can use DNS through the firewall without authentication. If DNS is not available, users cannot connect to a web, FTP, or Telnet server using a domain name.

The following example procedure describes how to configure the firewall to require users on the internal network to authenticate to access POP3 servers on the Internet. In this example, the DFL-1000 NPG is running in NAT/Route mode, but the configuration would be the same for a DFL-1000 NPG running in Transparent mode.

To require authentication:

- Add at least one user group to the firewall.
See [Users and authentication](#).
- Go to **Firewall > Service > Group**.
- Select New to add a Service Group.
- Enter a Group Name for the New Service Group and add the POP3, HTTP, FTP, and Telnet services to the service group Members list.
- Go to **Firewall > Policy > Int->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 the service group that you added in step [Enter a Group Name for the New Service Group and add the POP3, HTTP, FTP, and Telnet services to the service group Members list](#).
Set Action to ACCEPT.
- Select Authentication and select the user group that you added in step [Add at least one user group to the firewall](#).
- 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 [Configuring policy lists](#).

You must also make sure that users can connect to DNS without requiring authentication. You can ensure access to DNS by making sure that the default policy is not removed from the policy list. You can also add a policy to the top of the Int -> Ext policy list that includes the DNS service, has action set to ACCEPT, and does not include authentication.

Users and authentication

DFL-1000 NPGs support user authentication to the DFL-1000 user database or to a RADIUS server. You can add user names to the DFL-1000 user database and then add a password to allow the user to authenticate using the internal database. You can also add the name of a RADIUS server and select RADIUS to allow the user to authenticate using the selected RADIUS server. You can also disable users so that they cannot authenticate with the DFL-1000 NPG.

To enable authentication, you must add user names to one or more user groups. You can also add RADIUS servers to user groups. You can then select a user group when you require authentication.

You can require authentication for:

- any firewall policy with Action set to ACCEPT (see [Adding NAT/Route mode policies](#) and [Adding Transparent mode policies](#))
- IPSec dialup user remote gateways (see [Adding a remote gateway](#))
- PPTP (see [PPTP VPN configuration](#))
- L2TP (see [L2TP VPN configuration](#))

When a user enters a user name and password, the DFL-1000 NPG searches the internal user database for a matching user name. If Disable is selected for that user name, the user cannot authenticate and the connection is dropped. If Password is selected for that user and the password matches, the connection is allowed. If the password does not match, the connection is dropped.

If RADIUS is selected and RADIUS support is configured and the user name and password match a user name and password on the RADIUS server, the connection is allowed. If the user name and password do not match a user name and password on the RADIUS server, the connection is dropped.

This chapter describes:

- [Setting authentication timeout](#)
- [Adding user names and configuring authentication](#)
- [Configuring RADIUS support](#)
- [Configuring user groups](#)

Setting authentication timeout

To set authentication timeout using the web-based manager:

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

The default authentication timeout is 15 minutes.

Adding user names and configuring authentication

Use the following procedures to add user names and configure authentication.

This section describes:

- [Adding user names and configuring authentication](#)
- [Deleting user names from the internal database](#)

Adding user names and configuring authentication

- Go to *User > Local* .
- Select New to add a new user name.
- Enter the user name.
The user name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Select one of the following authentication configurations:
 - Disable** Prevent this user from authenticating.
 - Password** Enter the password that this user must use to authenticate. The password should be at least six characters long. The password can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
 - Radius** Require the user to authenticate to a RADIUS server. Select the name of the RADIUS server to which the user must authenticate. You can only select a RADIUS server that has been added to the DFL-1000 RADIUS configuration. See [Configuring RADIUS support](#).
- Select Try other servers if connect to selected server fails if you want the DFL-1000 NPG to try to connect to other RADIUS servers added to the DFL-1000 RADIUS configuration.
- Select OK.


Adding a user name

The screenshot shows a 'New User' dialog box with the following fields and options:

- User Name:** Text input field containing 'User_2'.
- Disable:** Unchecked checkbox.
- Password:** Password input field with asterisks.
- Radius:** Dropdown menu showing 'Radius_1'.
- Try other servers if connect to selected server fails:** Unchecked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Deleting user names from the internal database

If you delete a user, the user is also removed from any user groups that it has been added to.

- Go to *User > Local* .
- Select Delete User  for the user name to delete.
- Select OK.



Deleting the user name deletes the authentication configured for the user.

Configuring RADIUS support

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the DFL-1000 NPG contacts the RADIUS server for authentication.



When using a RADIUS server for user authentication, PPTP and L2TP encryption is not supported and you should not select Require data encryption when configuring Windows clients for PPTP or L2TP.

This section describes:

- [Adding RADIUS servers](#)
- [Deleting RADIUS servers](#)

Adding RADIUS servers

To configure the DFL-1000 NPG for RADIUS authentication:


- Go to **User > RADIUS**.
- Select New to add a new RADIUS server.
- Enter the name of the RADIUS server.
You can enter any name. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- Enter the domain name or IP address of the RADIUS server.
- Enter the RADIUS server secret.
- Select OK.

Example RADIUS configuration

The screenshot shows a dialog box titled "RADIUS" with a sub-title "New RADIUS Server". It contains three input fields: "Name" with the value "Radius_1", "Server Name/IP" with the value "23.64.67.47", and "Server Secret" with the value "Secret_1". There are "OK" and "Cancel" buttons at the bottom.

Deleting RADIUS servers

You cannot delete RADIUS servers that have been added to user groups.

- Go to **User > RADIUS**.
- Select Delete  beside the RADIUS server name that you want to delete.

- Select OK.

Configuring user groups

To enable authentication, you must add user names and/or RADIUS servers to one or more user groups. You can then select a user group when you require authentication. You can select a user group to configure authentication for:

- Policies that require authentication (see [Adding NAT/Route mode policies](#) and [Adding Transparent mode policies](#)). Only users in the selected user group or that can authenticate with the RADIUS servers added to the user group can authenticate with these policies.
- IPSec VPN remote gateways for dialup users ([Configuring dialup VPN](#)). Only users in the selected user group can authenticate with these remote gateways.
- The DFL-1000 PPTP configuration ([PPTP VPN configuration](#)). Only users in the selected user group can use PPTP.
- The DFL-1000 L2TP configuration ([L2TP VPN configuration](#)). Only users in the selected user group can use L2TP.

This section describes:

- [Adding user groups](#)
- [Deleting user groups](#)

Adding user groups

Use the following information to add user groups to your DFL-1000 configuration. You can add user names and RADIUS servers to user groups.

To add a user group:

- Go to User > User Group.
- Select New to add a new user group.
- Enter a Group Name to identify the user group.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- To add users to the user group, select a user from the Available Users list and select the right arrow to add the name to the Members list.
- To add a RADIUS server to the user group, select a RADIUS server from the Available Users list and select the right arrow to add the RADIUS server to the Members list.

Adding a user group




- To remove users or RADIUS servers from the user group, select a user or RADIUS server from the Members list and select the left arrow to remove the name or RADIUS server from the group.
- Select OK.

Deleting user groups

You cannot delete user groups that have been selected in a policy or remote gateway, PPTP, or L2TP configuration.

To delete a user group:

- Go to User > User Group
- Select Delete  beside the user group that you want to delete.
- Select OK.

IPSec VPNs

Using IPSec Virtual Private Networking (VPN), you can join together two or more widely separated private networks across a wide area network (WAN) such as 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. Remote or travelling workers can use a VPN client to connect to their office private network.

The DFL-1000 NPG is an excellent choice for connecting a satellite office to a main office VPN. The main office would usually be protected by a high-capacity product such as the DFL-1000-400 NPG or DFL-1000-500 NPG. The small office requires the same security and functionality, but the smaller user base makes the DFL-1000 NPG 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-1000 IPSec VPNs support three VPN configurations:

- Auto Internet Key Exchange (IKE) key VPN
- Manual Key Exchange VPN
- Dialup VPN

Both AutoIKE key and manual key configurations are used to connect remote clients or VPN gateways that have static IP addresses to a DFL-1000 VPN gateway. Dialup VPN uses an AutoIKE key configuration that allows clients or remote gateways with dynamic IP addresses to connect to the DFL-1000 VPN gateway.



IPSec VPN is not supported in Transparent mode.

This chapter describes:

- [Interoperability with IPSec VPN products](#)
- [Configuring AutoIKE key IPSec VPN](#)
- [Configuring manual key IPSec VPN](#)
- [Configuring dialup VPN](#)
- [Configuring a VPN Concentrator for hub and spoke VPN](#)
- [Configuring IPSec redundancy](#)
- [Adding a remote gateway](#)
- [Adding an AutoIKE key VPN tunnel](#)
- [Adding a manual key VPN tunnel](#)
- [Adding a VPN concentrator](#)
- [Adding an encrypt policy](#)
- [Viewing VPN tunnel status](#)
- [Viewing dialup VPN connection status](#)
- [Testing a VPN](#)

Interoperability with IPSec VPN products

Because the DFL-1000 NPG supports the IPSec industry standard for VPN, you can configure a VPN between a DFL-1000 NPG and any client or gateway/firewall that supports IPSec VPN.

DFL-1000 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
- DES and 3DES (TripleDES) encryption
- Diffie-Hellman groups 1, 2, and 5
- HMAC MD5 authentication/data integrity or HMAC SHA1 authentication/data integrity
- Aggressive and Main Mode
- NAT Traversal
- Replay Detection
- IPSec Redundancy
- Perfect Forward Secrecy
- VPN Concentrator for hub and spoke configurations

To successfully establish an IPSec VPN tunnel, the DFL-1000 IPSec VPN configuration must be compatible with the third-party product IPSec VPN configuration. D-Link has tested DFL-1000 VPN interoperability with the following third-party products:

- NetScreen Internet security appliances
- SonicWALL PRO firewall
- Cisco PIX firewall
- Cisco IOS router
- Check Point NG firewall
- Check Point NG-1 firewall
- Check Point FP-1 firewall
- Check Point FP-2 firewall
- Check Point FP-3 firewall
- Linksys firewall router
- SafeNet IPSec VPN client
- Secure Computing Sidewinder
- SSH Sentinel

For more information about DFL-1000 VPN interoperability, contact D-Link technical support.

Configuring AutoIKE key IPSec VPN

An AutoIKE key VPN configuration consists of a remote gateway, an AutoIKE key VPN tunnel, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.



Normally an AutoIKE key VPN tunnel requires one remote gateway. This can be a gateway with a static IP address or a dialup gateway. For IPSec redundancy, you can add up to three remote gateways with static IP addresses to an AutoIKE key tunnel. For information about IPSec redundancy, see [Configuring IPSec redundancy](#).

To create an AutoIKE key VPN configuration:

- Add a remote gateway.
See [Adding a remote gateway](#).
- Add an AutoIKE key VPN tunnel that includes the remote gateway that you added in step 1.
See [Adding an AutoIKE key VPN tunnel](#).
- Add an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel.
See [Adding an encrypt policy](#).

For an example AutoIKE key configuration between two networks, see [AutoIKE key VPN between two networks](#).

For an example AutoIKE key configuration for remote clients, see [AutoIKE key VPN for remote clients](#).

Configuring manual key IPSec VPN

A manual key VPN configuration consists of a manual key VPN tunnel, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.

To create a manual key VPN configuration:

- Add a manual key VPN tunnel.
See [Adding a manual key VPN tunnel](#).
- Add an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel.
See [Adding an encrypt policy](#).

For an example manual key configuration between two networks, see [Manual key VPN between two networks](#).

For an example manual key configuration for remote clients, see [Manual key VPN for remote clients](#).

Configuring dialup VPN

Use a dialup VPN configuration to allow remote clients or VPN gateways with dynamic IP addresses to connect to a DFL-1000 VPN gateway. Clients or gateways 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).

A dialup VPN configuration consists of a remote gateway and one or more VPN tunnels for this remote gateway. For each VPN tunnel, you must add an encrypt policy to control access to the VPN tunnel.

Dialup VPN has several configurations for user authentication. For information about dialup VPN authentication, see [About dialup VPN authentication](#).

To create a dialup VPN configuration:

- Add a remote gateway and select Dialup User.
See [Adding a remote gateway](#).

When you configure the Remote Gateway, you can require users to authenticate before accessing the remote gateway by choosing a user group in the User Group field. Selecting a user group is optional. For information about user groups, see [Adding user groups](#).

- Add one or more AutoIKE key VPN tunnels that include the remote gateway added in step 1.
See [Adding an AutoIKE key VPN tunnel](#).
- Add an incoming encrypt policy with External_All as the source address to allow all dialup users to access the VPN tunnel.
See [Adding an encrypt policy](#).

For an example dialup VPN configuration, see [Dialup VPN](#).

Configuring a VPN Concentrator for hub and spoke VPN

A hub and spoke VPN consists of a VPN Concentrator on a central DFL-1000 NPG (the hub) and two or more VPN tunnels (the spokes). The spoke VPNs communicate with each other through the hub VPN Concentrator.

To create a hub and spoke configuration, you must create a VPN Concentrator on the central DFL-1000 NPG. You must configure encrypt policies from each VPN spoke network to the VPN Concentrator network and to the other VPN spoke networks.

For an example VPN hub and spoke configuration, see [Hub and spoke VPN \(VPN concentrator\)](#).

This section describes:

- [Configuring the VPN Concentrator](#)
- [Configuring the member VPNs](#)

Configuring the VPN Concentrator

On the VPN Concentrator network, you must create one VPN tunnel for each of the prospective VPN Concentrator members and then add these tunnels to a VPN concentrator. You can add both AutoIKE and manual key VPN tunnels to a VPN Concentrator.

Encrypt policies control the direction of traffic through the VPN Concentrator. You must create a separate encrypt policy for each VPN added to the Concentrator. These policies allow inbound and outbound VPN connections between the Concentrator and the member VPN tunnels. The encrypt policy for each member VPN tunnel must include the member VPN tunnel name.

To configure the VPN Concentrator:

- Add the required number of remote gateways.

Each AutoIKE key tunnel requires a remote gateway.

See [Adding a remote gateway](#).

- Add the required number of AutoIKE key VPN tunnels and include the remote gateways added in step 1.

See [Adding an AutoIKE key VPN tunnel](#).

- Add the required number of manual key VPN tunnels.

See [Adding a manual key VPN tunnel](#).

- Add a VPN concentrator that includes the tunnels added in steps 2 and 3.

See [Adding a VPN concentrator](#).

- Add one encrypt policy for each member VPN. Use the following configuration for each policy:

Source	VPN Concentrator address.
Destination	Member VPN address.

Action	ENCRYPT
VPN Tunnel	The member VPN tunnel name.
Allow inbound	Select allow inbound.
Allow outbound	Select allow outbound
Inbound NAT	Select inbound NAT if required.
Outbound NAT	Select outbound NAT if required.

See [Adding an encrypt policy](#).

Configuring the member VPNs

For each member VPN, you must create a VPN tunnel to the VPN Concentrator network. This tunnel can be an AutoIKE key or manual key tunnel.

You must create an encrypt policy that allows inbound and outbound VPN connections between the member VPN and the Concentrator.

You must create additional encrypt policies that allow inbound and outbound VPN connections between each of the member VPNs.

The policy between the member VPN and the Concentrator must be arranged in the policy list above the policies between member VPNs. Each encrypt policy must include the same tunnel name.

To configure each member VPN:

- Add a remote gateway if you are adding AutoIKE key tunnels.
See [Adding a remote gateway](#).
- Add an AutoIKE key VPN tunnel and include the remote gateway added in step 1.
See [Adding an AutoIKE key VPN tunnel](#).
Or, add a manual key VPN tunnel.
See [Adding a manual key VPN tunnel](#).
- Add one encrypt policy between the member VPN and the VPN Concentrator. Use the following configuration:

Source	Member VPN address.
Destination	VPN Concentrator address.
Action	ENCRYPT
VPN Tunnel	The VPN tunnel added in step 2.
Allow inbound	Select allow inbound.
Allow outbound	Select allow outbound.
Inbound NAT	Select inbound NAT if required.
Outbound NAT	Select outbound NAT if required.

See [Adding an encrypt policy](#).

- Add additional encrypt policies between the member VPNs. Use the following configuration:

Source	Local member VPN address.
Destination	Remote member VPN address
Action	ENCRYPT
VPN Tunnel	The VPN tunnel added in step 2.
Allow inbound	Select allow inbound.

- Allow outbound** Select allow outbound.
- Inbound NAT** Select inbound NAT if required.
- Outbound NAT** Select outbound NAT if required.

Configuring IPSec redundancy

IPSec redundancy allows you to create a redundant AutoIKE key IPSec VPN configuration to two remote VPN gateway addresses.

One use of IPSec redundancy is if you have configured your DFL-1000 with multiple internet connections (see [Configuring the DFL-1000 NPG for multiple Internet connections](#))



For IPSec redundancy to work, both Internet connections must have static IP addresses.

To configure IPSec redundancy:

- Add two remote gateways with the same settings (including the same authentication key) but with different remote gateway addresses.
See [Adding a remote gateway](#).
- Add two AutoIKE key tunnels with the same settings and add one of the remote gateways to each tunnel.
See [Adding an AutoIKE key VPN tunnel](#).
- Add two outgoing encrypt policies.
If you have multiple internet connections you can add an Int->Ext encrypt policy and an Int->DMZ encrypt policy.
The source and destination of both policies must be the same. Add a different AutoIKE key tunnel to each policy.
See [Adding an encrypt policy](#).

Adding a remote gateway

Add a remote gateway configuration to define the parameters that the DFL-1000 NPG uses to connect to and establish an AutoIKE key VPN tunnel with a remote VPN gateway or a remote VPN client. The remote gateway configuration consists of the IP address of the remote VPN gateway or client as well as the P1 proposal settings required to establish the VPN tunnel. To successfully establish a VPN tunnel, the remote VPN gateway or client must have the same authentication key and compatible P1 proposal settings.

You can add one remote gateway and then create multiple AutoIKE key tunnels that include the same remote gateway in their configurations. When the DFL-1000 NPG receives an IPSec VPN connection request, it starts a remote gateway that matches the connection request. The VPN tunnel that starts depends on the source and destination addresses of the IPSec VPN request, which the DFL-1000 NPG matches with an encrypt policy.

To add a remote gateway:

- Go to *VPN > IPSEC > Remote Gateway* .
- Select New to add a new remote gateway.
- Configure the remote gateway.

- Gateway Name** Enter a name for the gateway. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
- Remote Gateway** Select Static IP Address or Dialup User.
- IP Address** If you select Static IP Address, the IP Address field appears. Enter the IP address of the remote IPsec VPN gateway or client that can connect to the DFL-1000 NPG.
- User Group** If you select Dialup User, the User Group field appears. For authentication purposes, you can select the group of users that will have access to the remote gateway. For information about dialup VPN authentication, see [About dialup VPN authentication](#).
- Mode** Select Aggressive or Main (ID Protection) mode. Both modes establish a secure channel. Main mode offers greater security because identifying information is exchanged after encryption is set up. Aggressive mode is less secure because it exchanges identifying information before encryption is set up.
For both Static IP Address and Dialup User remote gateways, the mode at both ends of the gateway must be the same.
- P1 Proposal** Select up to three encryption and authentication algorithm combinations to propose for phase 1. Two are selected by default. To decrease the number of combinations selected, select the minus sign. To increase the number of combinations selected, select the plus sign. See [About the P1 proposal](#).
- DH Group** Select one or more Diffie-Hellman groups to propose for Phase 1 of the IPsec VPN connection. You can select DH group 1, 2, and 5. See [About DH groups](#).
- Keylife** 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. P1 proposal keylife can be from 120 to 172,800 seconds.
- Authentication (Pre-shared Key)** Enter an authentication key. The key can contain any characters and must be at least 6 characters in length. The pre-shared key must be the same on the server and on the remote VPN gateway or client and should only be known by network administrators. For information about the pre-shared key, see [About dialup VPN authentication](#).
- Local ID** Optionally enter a local ID if you set Remote Gateway to Dialup user and select Aggressive Mode. Enter the IP address of the dialup user or the domain name of the dialup user (for example, domain.com). If you do not add a local ID, the DFL-1000 external interface automatically becomes the Local ID. For information about authentication and the Local ID, see [About dialup VPN authentication](#).
- Nat-traversal** Select Enable if you expect the IPsec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal will have no effect. Both ends of the gateway must have the same NAT traversal setting. See [About NAT traversal](#).
- Keepalive Frequency** If you enable NAT-traversal, you can change the number of seconds in the Keepalive Frequency field. This number specifies, in seconds, how frequently empty UDP packets are sent through the NAT device to ensure that the NAT mapping does not change until P1 and P2 keylife expires. The keepalive frequency can be from 0 to 900 seconds.
- Select OK to save the remote gateway.

Adding a remote gateway (Dialup User selected)

The screenshot shows the 'New VPN Gateway' configuration window. The 'Remote Gateway' tab is selected. The 'Gateway Name' is 'Dialup_1'. The 'Remote Gateway' dropdown is set to 'Dialup User'. The 'User Group' is '---None---'. The 'Mode' has radio buttons for 'Aggressive' (unchecked) and 'Main (ID Protection)' (checked). The 'P1 Proposal' section has two entries: '1 - Encryption: 3DES Authentication: SHA1' and '2 - Encryption: 3DES Authentication: MD5'. The 'DH Group' has radio buttons for '1' (unchecked), '2' (unchecked), and '5' (checked). 'Keylife' is '28800 (Seconds)'. 'Authentication: (Pre-shared Key)' is empty. 'Local ID' and 'Peer ID' are empty with '(Optional)' labels. 'Nat-traversal' has an unchecked 'Enable' checkbox. 'Keepalive Frequency' is '5 (Seconds)'. 'OK' and 'Cancel' buttons are at the bottom.

About dialup VPN authentication

For dialup VPN authentication to work you must create compatible configurations on the DFL-1000 NPG that is the dialup server and its dialup clients. The configurations required for the server and the clients are different for different dialup gateway configurations. There are four possible dialup VPN authentication configurations:

- [Main mode with no user group selected](#)
- [Main mode with a user group selected](#)
- [Aggressive mode with no user group](#)
- [Aggressive mode with a user group selected](#)

For each variation, the remote gateway field of the dialup server remote gateway configuration must be set to dialup user and all of the clients must have their remote gateway or equivalent set to the static IP address of the remote gateway server.

The following sections describe how to configure authentication on the server and clients for each of these variations.



A dialup user must use the same mode as the VPN dialup server.



For information about user groups, see [Adding user groups](#).

Main mode with no user group selected

In this configuration, the server and the clients use main mode for key exchange. A user group has not been added to the server dialup remote gateway. Clients authenticate with the server using their authentication keys.

Main mode without user group		
Field	Server	Clients
User Group	None	None
Mode	Main (ID Protection)	Main (ID Protection)
Authentication Key	The server and the clients must have the same authentication key.	
Local ID	empty	Empty

Main mode with a user group selected

In this configuration, the server and the clients use main mode for key exchange. A user group has been selected in the server dialup remote gateway. Clients authenticate with the server using their authentication keys. The client authentication key can be one of the following:

- The same as the server authentication key.
- A username and password in the user group added to the dialup server remote gateway. In this configuration, the clients pre-shared key must be formatted with a ` + ' between the user name and password (*username+password*).

Main mode with a user group selected			
Field	Server	Client configuration 1	Client configuration 2
User Group	Select a user group	N/A	N/A
Mode	Main (ID Protection)	Main (ID Protection)	Main (ID Protection)
Authentication Key	Server authentication key	Server authentication key	username+password
Local ID	empty	Empty	empty

Aggressive mode with no user group

In this configuration, the server and the clients use aggressive mode for key exchange. A user group has not been selected in the server dialup remote gateway. Clients authenticate with the server using their authentication keys.

Aggressive mode with no user group		
Field	Server	Clients
User Group	None	N/A
Mode	Aggressive	Aggressive
Authentication Key	The server and the clients must have the same authentication key.	
Local ID	empty	Empty

Aggressive mode with a user group selected

In this configuration, the server and the clients use aggressive mode for key exchange. A user group is selected in the server dialup remote gateway. The format of the authentication key depends on the information in the Local ID field.

Aggressive mode with a user group selected				
Field	Server	Client configuration 1	Client configuration 2	Client configuration 3
User Group	Select a user group	N/A	N/A	N/A
Mode	Aggressive	Aggressive	Aggressive	Aggressive
Authentication Key	Server authentication key	Server authentication key	Server authentication key	Client's password. This password must be added to the server user database.
Local ID	Empty	Client IP address	Client domain name	Other information in a different format.

About DH groups

The Diffie-Hellman (DH) algorithm creates a shared secret key that can be created at both ends of the VPN tunnel without communicating the key across the Internet.

You can select from DH group 1, 2, and 5. DH group 5 produces the most secure shared secret key and DH group 1 produces the least secure key. However, DH group 1 is faster than DH group 5.

About the P1 proposal

AutoIKE key 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 configure the remote gateway P1 proposal, you are selecting the algorithms that the DFL-1000 NPG proposes during phase 1 negotiation. You can select up to three different encryption and authentication algorithm combinations. Choosing more combinations might make it easier for P1 negotiation, but you can restrict the choice to one if required. For negotiation to be successful, both ends of the VPN tunnel must have at least one encryption algorithm and one authentication algorithm in common.

- Select DES to propose to encrypt packets using DES encryption.
- Select 3DES to propose to encrypt packets using triple-DES encryption.
- Select MD5 to propose to use MD5 authentication.
- Select SHA1 to propose to use SHA1 authentication.

About NAT traversal

NAT (Network Address Translation) converts private IP addresses into routable public IP addresses. The DFL-1000 NPG uses NAT (Network Address Port Translation), in which both IP addresses and ports are mapped. Mapping both components allows multiple private IP addresses to use a single public IP address.

Because a NAT device modifies the original IP address of an IPsec packet, the packet fails an integrity check. This failure means that IPsec VPN does not work with NAT devices.

NAT traversal solves this problem by encapsulating the IPsec packet within a UDP packet. Encapsulating the IPsec packet allows NAT to process the packet without changing the original IPsec packet.



Both ends of a gateway must have the same NAT traversal setting. Each end can have different keepalive frequencies.

Adding an AutoIKE key VPN tunnel

Add an AutoIKE key tunnel to specify the parameters used to create and maintain a VPN tunnel that has been started by a remote gateway configuration.

To add an AutoIKE key VPN tunnel:

- Go to *VPN > IPSEC > AutoIKE Key* .
- Select New to add a new AutoIKE key VPN tunnel.
- Configure the AutoIKE key VPN tunnel.

Tunnel Name	Enter a name for the tunnel. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
Remote Gateway	Select a STATIC or a DIALUP remote gateway to associate with the VPN tunnel. Select a static remote gateway if you are configuring IPsec redundancy. See Configuring IPsec redundancy . If you select a static gateway, you can select up to three remote gateways. To decrease the number of remote gateways, select the minus sign. To increase the number of remote gateways, select the plus sign.
P2 Proposal	Select up to three encryption and authentication algorithm combinations to propose for phase 2. Two are selected by default. To decrease the number of combinations selected, select the minus sign. To increase the number of combinations selected, select the plus sign. See About the P2 proposal .
Enable replay detection	Select Enable replay detection to prevent IPsec replay attacks during phase 2. See About replay detection .
Enable perfect forward secrecy (PFS)	Select Enable perfect forward secrecy (PFS) to improve the security of phase 2 keys. See About perfect forward secrecy (PFS) .
DH Group	Select the Diffie-Hellman group to propose for phase 2 of the IPsec VPN connection. You can select one DH group. Select 1, 2, or 5. See About DH groups .
Keylife	Specify the keylife for phase 2. The keylife causes the phase 2 key to expire after a specified amount of time, after a specified number of kbytes of data have been processed by the VPN tunnel, or both. If you select both, the key does not expire until both the time has passed and the number of kbytes have been processed. When the key expires, a new key is generated without interrupting service. P2 proposal keylife can be from 120 to 172800 seconds or from 5120 to 99999 kbytes.
Autokey Keep Alive	Enable Autokey Keep Alive to keep the VPN tunnel running even if no data is being processed.
Concentrator	Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration. If you use the procedure, Adding a VPN concentrator to add the tunnel to a concentrator, the next time you open the tunnel, the Concentrator field displays the name of the concentrator to which you have added the tunnel.

- Select OK to save the AutoIKE key VPN tunnel.

Adding an AutoIKE key VPN tunnel

The screenshot shows the 'New VPN Tunnel' configuration window. The 'AutoIKE Key' tab is active. The 'Tunnel Name' is 'IKE_Tunnel'. The 'Remote Gateway' is 'Remote_Gateway_1'. Under 'P2 Proposal', '1-Encryption' is '3DES' and 'Authentication' is 'SHA1'. '2-Encryption' is '3DES' and 'Authentication' is 'MD5'. Both 'Enable replay detection' and 'Enable perfect forward secrecy (PFS)' are checked. The 'DH Group' has radio buttons for '1', '2', and '5'. The 'Keylife' section shows 'Seconds' set to '1800' and '(Seconds)' set to '4608000'. The 'Autokey Keep Alive' checkbox is unchecked. The 'Concentrator' is set to 'None'. 'OK' and 'Cancel' buttons are at the bottom.

About the P2 proposal

During tunnel negotiation, 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-1000 NPG proposes during phase 2 negotiation. For phase 2 to be completed successfully, each VPN gateway must have at least one encryption and one authentication algorithm in common.

- Select DES to propose to encrypt packets using DES encryption.
- Select 3DES to propose to encrypt packets using triple-DES encryption.
- Select MD5 to propose to use MD5 authentication.
- Select SHA1 to propose to use SHA1 authentication.
- Select NULL to propose that the VPN packets not be encrypted or that a hash is not made for authentication.

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. An attacker can use this technique to cause a denial of service (DoS) attack by flooding the tunnel with packets. An 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 previously been received. If packets arrive out of sequence, the DFL-1000 NPG discards them.

The DFL-1000 NPG sends an alert email when replay detection detects a replay packet. To receive the alert email, you must configure alert email and select "Enable alert email for critical firewall/VPN events or violations". For information about alert email, see [Configuring alert email](#).

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 might 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 might 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 the phase 2 encryption keys can be compromised.

Adding a manual key VPN tunnel

Configure a manual key tunnel to create an IPSec VPN tunnel between the DFL-1000 NPG and a remote IPSec VPN client or gateway that is also using manual key. A manual key VPN tunnel consists of a name for the tunnel, the IP address of the VPN gateway or client at the opposite end of the tunnel, and the encryption algorithm to use for the tunnel. Depending on the encryption algorithm, you must also specify the encryption keys and optionally the authentication keys used by the tunnel. Because the keys are created when you configure the tunnel, no negotiation is required for the VPN tunnel to start. However, the VPN gateway or client that connects to this tunnel must use the same encryption algorithm and must have the same encryption and authentication keys.

To create a manual key VPN tunnel:

- Go to *VPN > IPSEC > Manual Key* .
- Select New to add a new manual key VPN tunnel.
- Configure the VPN tunnel.

VPN Tunnel Name	Enter a name for the tunnel. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
Local SPI	Security Parameter Index. Enter a hexadecimal number of up to eight digits (numbers (0-9) and/or letters (a-f)). The hexadecimal number must be added to the Remote SPI at the opposite end of the tunnel. The Local SPI value must be greater than bb8.
Remote SPI	Enter a hexadecimal number of up to eight digits. The hexadecimal number must be added to the Local SPI at the opposite end of the tunnel. The Remote SPI value must be greater than bb8.
Remote Gateway	Enter the external IP address of the DFL-1000 NPG or other IPSec gateway at the opposite end of the tunnel.
Replay Detection	Select Replay Detection to prevent IPSec replay attacks. See About replay detection .
Encryption Algorithm	Select an algorithm from the list. Make sure that you use the same algorithm at both ends of the tunnel. Required for encryption algorithms that include ESP-DES or ESP-3DES.
Encryption Key	For all DES encryption algorithms, enter one hexadecimal number of up to 16 digits. Use the same encryption key at both ends of the tunnel. For all 3DES encryption algorithms, enter three hexadecimal numbers of up to 16 digits each. Use the same encryption key at both ends of the tunnel. Required for encryption algorithms that include MD5 or SHA1 authentication.
Authentication Key	For MD5 authentication, enter two hexadecimal numbers of 16 digits each. Use the same authentication key at both ends of the tunnel. For SHA1 authentication, enter two hexadecimal numbers, one of 16 digits and one of 20 digits. Use the same authentication key at both ends of the tunnel.
Concentrator	Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration. See Adding a VPN concentrator .

- Select OK to save the manual key VPN tunnel.

Adding a manual key VPN tunnel

The screenshot shows the 'New VPN Tunnel' dialog box with the 'Manual Key' tab selected. The configuration fields are as follows:

- VPN Tunnel Name: Manual_Tunnel
- Local SPI: bb8 (Hex)
- Remote SPI: bb8 (Hex)
- Remote Gateway: 1.0.0.1
- Replay Detection:
- Encryption Algorithm: ESP-3DES-HMAC-SHA1
- Encryption Key (Hex, 24 bytes): Two masked input fields separated by a hyphen.
- Authentication Key (Hex, 20 bytes): Two masked input fields separated by a hyphen.
- Concentrator: None

Buttons: OK, Cancel

Adding a VPN concentrator

You can add VPN tunnels to a VPN concentrator grouping to create a hub and spoke configuration. The VPN concentrator allows VPN traffic to pass from one tunnel to the other through the DFL-1000 NPG.

To add a hub and spoke configuration:

- Go to VPN > IPsec > Concentrator.
- Select New to add a VPN Concentrator.
- Enter the name of the new concentrator in the Concentrator Name field.
- To add tunnels to the VPN Concentrator, select a VPN tunnel from the Available Tunnels list and select the right arrow.
- To remove tunnels from the VPN Concentrator, select the tunnel in the Members list and select the left arrow.
- Select OK to add the VPN concentrator.

Adding a VPN Concentrator



Adding an encrypt policy

Add encrypt policies to connect users on your internal network to a VPN tunnel. Encrypt policies are always outgoing policies. For example, if you have users on your internal network that should be able to connect to a network behind a remote DFL-1000 NPG VPN gateway on the Internet, you must add an Int -> Ext encrypt policy. The source of this policy must be an address on your internal network. The destination of this policy must be the address of the network behind the remote DFL-1000 NPG gateway.

The policy must also include the VPN tunnel that you created to communicate with the remote DFL-1000 NPG VPN gateway. When users on your internal network attempt to connect to the internal network behind the remote DFL-1000 NPG gateway, the encrypt policy intercepts the connection attempt and starts the VPN tunnel added to the policy. The tunnel uses the remote gateway added to its configuration to connect to the remote DFL-1000 NPG VPN gateway and the DFL-1000 NPGs use their remote gateway and VPN tunnel configurations to establish a VPN tunnel between them.

Using encrypt policies, you can control:

- the direction of traffic flow through the VPN,
- the addresses that can connect to the VPN tunnel.

The source and destination addresses that you specify when you add an encrypt policy identify the computers or networks that can connect using the VPN. Users connecting from either the source or destination address will be able to connect to the other address securely using VPN.



The destination address can be a VPN client address on the Internet or the address of a network behind a remote VPN gateway.

To add an encrypt policy:

- Add the source address for the policy.

The source address is the IP address of the local network, usually on your internal network, that can connect to the VPN.

For information about adding addresses, see [Adding addresses](#).

- Add the destination address for the policy.
The destination address is the IP address of the remote network behind the remote VPN gateway. If you are adding an encrypt policy for a VPN with a remote VPN client connected to the Internet, the destination address should be the Internet address of the client computer.
- Go to **Firewall > Policy** .
- Select the policy list to which you want to add the policy.
- Select New to add a new policy.
- Set Source to the source address added in step 1.
- Set Destination to the destination address added in step 2.
- Set Action to ENCRYPT.
Service is set to ANY and cannot be changed.
- Configure the ENCRYPT parameters.

VPN Tunnel Select an AutoIKE key or Manual Key tunnel for this encrypt policy. For information about adding VPN tunnels, see [Adding an AutoIKE key VPN tunnel](#) and [Adding a manual key VPN tunnel](#).

Allow inbound Select Allow inbound to enable inbound users to connect to the source address.

Allow outbound Select Allow outbound to enable outbound users to connect to the destination address.

Inbound NAT The DFL-1000 NPG translates the source address of incoming packets to the IP address of the DFL-1000 interface connected to the source address network.

Outbound NAT The DFL-1000 NPG translates the source address of outgoing packets to the IP address of the DFL-1000 interface connected to the destination address network.

Use the information in [Adding NAT/Route mode policies](#) to configure the remaining policy settings.

- Select OK to save the encrypt policy.
- To make sure that the encrypt policy is matched for VPN connections, arrange the encrypt policy above other policies with similar source and destination addresses in the policy list.

Adding an encrypt policy

Int->Ext | Int->DMZ | DMZ->Int | DMZ->Ext | Ext->Int | Ext->DMZ

New Policy

Source: Local_VPN_net
Destination: Remot_VPN_net
Schedule: Always
Service: ANY
Action: ENCRYPT

VPN Tunnel: AutoIKE_tunnel1
 Allow inbound Inbound NAT
 Allow outbound Outbound NAT

Traffic Shaping
Guaranteed Bandwidth: 0 (kbytes/sec)
Maximum Bandwidth: 0 (kbytes/sec)
Traffic Priority: High

Log Traffic
 Web filter [show settings](#)

OK Cancel

Viewing VPN tunnel status

You can use the IPsec VPN tunnel list to view the status of all IPsec AutoIKE key 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 > AutoIKE Key*.

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.

AutoIKE key tunnel status

Tunnel Name	Remote Gateway	Lifetime(sec/kb)	Status	Timeout	Modify
AutoIKE_tunnel_1	66.34.23.78	300/10240	Down	0	
AutoIKE_tunnel_2	55.66.77.88	1800/NA	Down	0	

New

Viewing dialup VPN connection status

You can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway. The monitor also lists the tunnel lifetime, timeout, proxy ID source, and proxy ID destination for each tunnel.

To view dialup connection status:

- Go to VPN > IPsec > Dialup.

The Lifetime column displays how long the connection has been up.

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.

Dialup monitor

Remote gateway	Lifetime	Timeout	Proxy ID Source	Proxy ID Destination
192.168.100.124	1800 sec	79	14.14.14.0/255.255.255.0	192.168.100.124/255.255.255.255
192.168.100.40	1800 sec	3585	14.14.14.0/255.255.255.0	192.168.100.40/255.255.255.255

The Proxy ID Source column displays the actual IP address or subnet address of the remote peer.

The Proxy ID Destination column displays the actual IP address or subnet address of the local peer.

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-1000 NPG.

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 VPN configuration examples

This chapter describes the following IPSec VPN configuration examples:

- [AutoIKE key VPN between two networks](#)
- [AutoIKE key VPN for remote clients](#)
- [Dialup VPN](#)
- [Manual key VPN between two networks](#)
- [Manual key VPN for remote clients](#)
- [Hub and spoke VPN \(VPN concentrator\)](#)

AutoIKE key VPN between two networks

[Example VPN between two internal networks](#) shows that you can use the DFL-1000 NPG to protect a branch office and a small main office. Both of these DFL-1000 NPGs can be configured as IPSec VPN gateways to create the VPN that connects the branch office network to the main office network.

You can use any DFL-1000 NPG configured as an IPSec VPN gateway to protect the branch office or main office, depending on the capacity that you require. Alternatively, one of the networks can be protected by a third-party VPN gateway that supports IPSec and AutoIKE key.

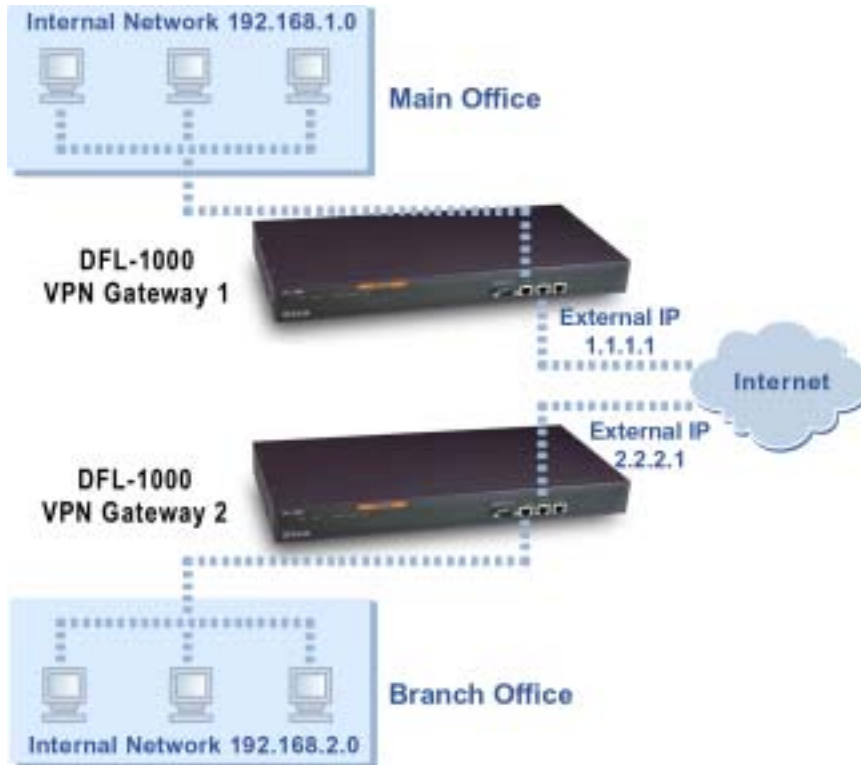
The example shows a VPN between two internal networks, but you can also create VPNs between an internal network behind one VPN gateway and a DMZ network behind another or between two DMZ networks. The networks at the ends of the VPN tunnel are selected when you add source and destination addresses to the encrypt policy.

The example also shows the two DFL-1000 NPGs connecting to each other through their external interfaces and across the Internet. However, the DFL-1000 NPGs can connect to each other either through their external or their DMZ interfaces. The interfaces through which the DFL-1000 NPGs communicate are selected when you add destination addresses to the encrypt policy.

The following procedures show an example of how to configure an IPSec AutoIKE key VPN between two internal networks:

- [Configuring the remote gateway for a remote network](#)
- [Configuring the AutoIKE key tunnel for a remote network](#)
- [Adding source and destination addresses for a network-to-network VPN](#)
- [Adding an encrypt policy for a network-to-network VPN](#)

Example VPN between two internal networks



Configuring the remote gateway for a remote network

Use the following procedure to configure the remote gateway for the example VPN in [Example VPN between two internal networks](#).

[Example remote gateway configuration](#) shows the information required to configure the remote gateway.

Example remote gateway configuration		
Field name	Main Office information	Branch Office information
Gateway Name	Branch_Office_gw	Main_Office_gw
Remote Gateway	Static IP Address	Static IP Address
IP Address	2.2.2.1	1.1.1.1
Mode	Main (ID Protection)	Main (ID Protection)
P1 Proposal		
1- Encryption	3DES	3DES
Authentication	SHA1	SHA1
DH Group	5	5
Keylife	28800 seconds	28800 seconds
Authentication (Pre-shared Key)	ddcHH01887d	ddcHH01887d
Local ID	Blank	Blank
NAT-traversal	Enable	Enable
Keepalive Frequency	5	5



You can use any characters for the authentication key. The authentication key must be the same on both gateways.



For more information about remote gateway settings, see [Adding a remote gateway](#).

To configure the remote gateways for the Main Office and Branch Office:

- Go to *VPN > IPSEC > Remote Gateway*.
- Select New to add a remote gateway.
- On the Main Office DFL-1000 NPG configure the remote gateway using the Main Office information in [Example remote gateway configuration](#).
- On the Branch Office DFL-1000 NPG configure the remote gateway using the Branch Office information in [Example remote gateway configuration](#).
- Select OK to save the remote gateway.

Configuring the AutoIKE key tunnel for a remote network

Use the following procedure to configure the AutoIKE key tunnel for the example VPN in [Example VPN between two internal networks](#).

[Example AutoIKE key tunnel configuration](#) shows the information required to configure the tunnel.

Example AutoIKE key tunnel configuration		
Field name	Main Office information	Branch Office information
Tunnel Name	Branch_Office_VPN	Main_Office_VPN
Remote Gateway	Branch_Office_gw	Main_Office_gw
P2 Proposal		
1- Encryption	3DES	3DES
Authentication	SHA1	SHA1
Enable replay detection	Select	Select
Enable perfect forward secrecy (PFS)	Select	Select
DH Group	5	5
Keylife	300 seconds	300 seconds
Autokey Keep Alive	Enable	Enable
Concentrator	Not selected	Not selected



For more information about AutoIKE key tunnel settings, see [Adding an AutoIKE key VPN tunnel](#).

To configure the AutoIKE key tunnel for the Main Office and Branch Office VPN gateways:

- Go to *VPN > IPSEC > AutoIKE Key*.
- Select New to add an AutoIKE key tunnel.
- On the Main Office DFL-1000, configure the AutoIKE key tunnel using the Main Office information in [Example AutoIKE key tunnel configuration](#).
- On the Branch Office DFL-1000, configure the AutoIKE key tunnel using the Branch Office information in [Example AutoIKE key tunnel configuration](#).
- Select OK to save the AutoIKE key tunnel.

Adding source and destination addresses for a network-to-network VPN

Use the following procedures to add the network addresses to the AutoIKE key tunnel shown in [Example VPN between two internal networks](#). You must add a source and a destination address to both gateways. [IPSec VPN source and destination addresses](#) shows the information required to add the source and destination addresses to the AutoIKE key tunnel.

IPSec VPN source and destination addresses		
Field name	Main Office information	Branch Office information
Source Address		
Address Name	Main_Office	Branch_Office
IP address	192.168.1.0	192.168.2.0
Netmask	255.255.255.0	255.255.255.0
Destination Address		
Address Name	Branch_Office	Main_Office
IP address	192.168.2.0	192.168.1.0
Netmask	255.255.255.0	255.255.255.0

To add the Main Office and Branch Office source addresses:

- Go to *Firewall > Address > Internal*.
- Select New to add an address.
- On the Main Office DFL-1000 NPG, enter the Address Name, IP Address, and NetMask, using the Main Office source address information in [IPSec VPN source and destination addresses](#).
- On the Branch Office DFL-1000 NPG, enter the Address Name, IP Address, and NetMask, using the Branch Office source address information in [IPSec VPN source and destination addresses](#).
- Select OK to save the source address.
- Repeat these steps (this time selecting the External address list) to add the Main office and Branch Office destination addresses.

Adding an encrypt policy for a network-to-network VPN

Use the following procedure to add an encrypt policy that allows IPSec VPN traffic through the firewall. The encrypt policy associates the tunnel with the source and destination address.

[Example encrypt policies](#) show Main Office and Branch Office encrypt policies for the VPN in [Example VPN between two internal networks](#).

Example encrypt policies		
Field name	Main Office information	Branch Office information
Source	Main_Office	Branch_Office
Destination	Branch_Office	Main_Office
Service	ANY	ANY
Action	ENCRYPT	ENCRYPT
VPN Tunnel	Branch_Office_VPN	Main_Office_VPN
Allow Inbound	Select	Select
Allow Outbound	Select	Select
Inbound NAT	Do not select.	Do not select.

Outbound NAT	Do not select.	Do not select.
---------------------	----------------	----------------

To add the encrypt policy:

- Go to *Firewall > Policy* .
- Select Int -> Ext.
- Select New to add a new policy.
- On the Main Office DFL-1000 NPG set Source and Destination to the Main Office Source and Destination shown in [Example encrypt policies](#).
- On the Branch Office DFL-1000 NPG set Source and Destination to the Branch Office Source and Destination shown in [Example encrypt policies](#).
- Set Action to ENCRYPT.
Service is set to ANY and cannot be changed.
- On the Main Office DFL-1000 NPG set VPN Tunnel to Branch_Office_VPN.
- On the Branch Office DFL-1000 NPG set VPN Tunnel to Main_Office_VPN.
- Select Allow Inbound and Allow Outbound to allow two-way communication through the VPN.
- You can also select Log Traffic and Web filter for encrypt policies.
- Select OK to save the policy.

AutoIKE key VPN for remote clients

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 AutoIKE key. The following procedures show an example configuration for an IPSec AutoIKE key VPN between an internal network and a remote VPN client.

Example VPN between a main office internal network and a remote client



The example shows a remote client on the Internet using IPSec VPN to connect to an address on the internal network. You can also configure an encrypt policy so that:

- a client on the Internet can connect to an address on the DMZ network,
- a client on the DMZ network can connect to an address on the internal network.

This section describes:

- [Configuring the remote gateway for remote clients](#)
- [Configuring the AutoIKE key tunnel for a remote client](#)
- [Adding source and destination addresses for a remote client VPN](#)
- [Adding an encrypt policy for a remote client](#)
- [Configuring the IPsec VPN client](#)

Configuring the remote gateway for remote clients

[Example remote gateway configuration](#) shows the information required to configure the remote gateway for the example VPN in [Example VPN between a main office internal network and a remote client](#).

Example remote gateway configuration	
Field name	Gateway information
Gateway Name	Client_gw
Remote Gateway	Static IP Address
IP Address	2.2.2.2
Mode	Main (ID Protection)
P1 Proposal	
1- Encryption	DES
Authentication	MD5
DH Group	5
Keylife	600 seconds
Authentication (Pre-shared Key)	ddcHH01887d
Local ID	Blank
Nat-traversal	Enable
Keepalive Frequency	5 seconds



You can use any characters for the authentication key. The authentication key must be the same on both the gateway and the client.



For more information about remote gateway settings, see [Adding a remote gateway](#).

To configure the remote gateway:

- Go to *VPN > IPSEC > Remote Gateway*.
- Select New to add a remote gateway.
- Configure the remote gateway using the information in [Example remote gateway configuration](#).
- Select OK to save the remote gateway.

Configuring the AutoIKE key tunnel for a remote client

[Example AutoIKE key tunnel configuration](#) shows the information required to configure the AutoIKE key tunnel for the example VPN in [Example VPN between a main office internal network and a remote client](#).

Example AutoIKE key tunnel configuration	
Field name	Tunnel information
Tunnel Name	Client_VPN

Remote Gateway	Client_gw
P2 Proposal	
1- Encryption	DES
Authentication	MD5
Enable replay detection	Select
Enable perfect forward secrecy (PFS)	Select
DH Group	5
Keylife	1800 seconds
Autokey Keep Alive	Enable
Concentrator	None



For more information about AutoIKE key tunnel settings, see [Adding an AutoIKE key VPN tunnel](#).

To configure the VPN tunnel:

- Go to *VPN > IPSEC > AutoIKE Key*.
- Select New to add an AutoIKE key tunnel.
- Configure the tunnel using the information in [Example AutoIKE key tunnel configuration](#).
- Select OK to save the AutoIKE key tunnel.

Adding source and destination addresses for a remote client VPN

Use the following procedures to add the network and client addresses to the AutoIKE key tunnel. The source address is the IP address of the network behind the local VPN gateway, and the destination address is the IP address of the remote VPN client.

Example source and destination addresses for a client with a static IP address	
Field name	Address information
Source Address	
Address Name	Main_Office
IP address	192.168.1.0
Netmask	255.255.255.0
Destination Address	
Address Name	VPN_Client
IP address	2.2.2.2
Netmask	255.255.255.255

Use the following procedures to add the example source and destination addresses.

Adding a source address for the internal network

- Go to *Firewall > Address > Internal*.
- Select New to add an address.
- Enter the Address Name, IP Address, and NetMask, using the Source Address information in [Example source and destination addresses for a client with a static IP address](#).
- Select OK to save the source address.
- Repeat these steps (this time selecting the External address list) to add destination address.

The destination address is the Internet IP address of the remote client.

- Select OK to save the destination address.

Adding an encrypt policy for a remote client

Use the following procedure to add an encrypt policy for the remote client shown in [Example VPN between a main office internal network and a remote client](#).

Example VPN gateway policy configuration	
Field name	Policy information
Source	Main_Office
Destination	VPN_Client
Service	Any
Action	Encrypt
VPN Tunnel Name	Client_VPN
Allow Inbound	Select
Allow Outbound	Do not select
Inbound NAT	Do not select.
Outbound NAT	Do not select.

To add the encrypt policy:

- Go to *Firewall > Policy* .
- Select Int -> Ext.
- Set Source and Destination to Source and Destination shown in [Example VPN gateway policy configuration](#).
- Set Action to ENCRYPT.
Service is set to ANY and cannot be changed.
- Set VPN Tunnel to Client_VPN.
- Configure the ENCRYPT parameters using the information in [Example VPN gateway policy configuration](#).
- Select Allow Inbound to allow the client to connect to the source address.
Only select Allow Outbound if you want users at the destination address to be able to connect to the client.
- You can also select Log Traffic and Web filter for encrypt policies.
- Select OK to save the policy.

Configuring the IPSec VPN client

The VPN client must be running industry-standard IPSec AutoIKE key VPN client software, such as the D-Link Remote VPN Client.

Configure the client as required to connect to the DFL-1000 VPN gateway using an IPSec VPN configuration. Make sure that the client configuration matches the DFL-1000 remote gateway and VPN tunnel configuration, including the settings in [Example remote VPN client configuration](#).

Example remote VPN client configuration		
Field name		Client information
Remote Gateway	The external IP address of the DFL-1000 VPN gateway.	1.1.1.1

DH Group	Should match the VPN tunnel DH Group.	5
Authentication Key	The client authentication key should match the DFL-1000 VPN gateway authentication key.	ddcHH01887d

Dialup VPN

Use a dialup VPN configuration to allow remote VPN gateways or clients with dynamic IP addresses to connect to a DFL-1000 VPN gateway. Gateways or 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).

Example dialup VPN configuration



This example describes creating a dialup VPN configuration by adding a remote gateway. This example also describes how to create VPN tunnels, source and destination addresses, and VPN policies so that remote VPN gateways and clients with dynamic IP addresses can connect to the DFL-1000 dialup VPN gateway.

A remote IPsec VPN gateway or client requires the following IPsec parameters to connect to the dialup VPN gateway:

- a matching authentication key,
- a remote gateway IP address set to the IP address of the DFL-1000 NPG configured for dialup VPN.

You can view the status of a dialup VPN configuration using the dialup monitor.



For more information about dialup authentication, see [About dialup VPN authentication](#).

Use the following procedures to create the example dialup VPN configuration:

- [Adding a dialup remote gateway](#)
- [Adding AutoIKE key tunnels for dialup VPN](#)
- [Adding source and destination addresses for dialup VPN](#)
- [Adding encrypt policies for dialup VPN](#)

- [Configuring remote IPSec VPN gateways for dialup VPN](#)
- [Configuring remote IPSec VPN clients for dialup VPN](#)

Adding a dialup remote gateway

Use the information in [Example dialup remote gateway](#) to configure the remote gateway.

Example dialup remote gateway

Field name	Remote gateway information
Gateway Name	Dialup_gw
Remote Gateway	Dialup User
User Group	None
Mode	Main (ID Protection)
P1 Proposal	
1 Encryption	3DES
Authentication	SHA1
DH Group	5
Keylife	28800 seconds
Authentication (Pre-shared Key)	ddcHH01887d
Local ID	Blank
Nat-traversal	Not Selected
Keepalive Frequency	Blank

To configure the example remote gateway:

- Go to *VPN > IPSEC > Remote Gateway*.
- Select New to add a remote gateway.
- Configure the remote gateway using the information in [Example dialup remote gateway](#).



For information about remote gateway settings, see [Adding a remote gateway](#).

- Select OK to save the dialup VPN remote gateway.

Adding AutoIKE key tunnels for dialup VPN

If you are configuring dialup VPN for a network-to-network VPN, use the procedure in [Configuring the AutoIKE key tunnel for a remote network](#). Use the information in [Example AutoIKE key tunnel configuration](#), but set the AutoIKE key tunnel remote gateway to the Dialup_gw gateway that you created.

If you are configuring dialup VPN for a remote client, use the procedure in [Configuring the AutoIKE key tunnel for a remote client](#). Use the information in [Example AutoIKE key tunnel configuration](#), but set the AutoIKE key tunnel remote gateway to the Dialup_gw gateway that you created.

Adding source and destination addresses for dialup VPN

If you are configuring dialup VPN for a network-to-network VPN, use the procedures in [Adding source and destination addresses for a network-to-network VPN](#). Use the information in [IPSec VPN source and destination addresses](#).

If you are configuring dialup VPN for a remote client, use the procedures in [Adding source and destination addresses for a remote client VPN](#). Use the information in [Example source and destination addresses for a client with a static IP address](#).

Adding encrypt policies for dialup VPN

If you are configuring dialup VPN for a network-to-network VPN, use the procedure in [Adding an encrypt policy for a network-to-network VPN](#). Use the information in [Example encrypt policies](#).

If you are configuring dialup VPN for a remote client, use the procedure in [Adding an encrypt policy for a remote client](#). Use the information in [Example VPN gateway policy configuration](#).

Configuring remote IPSec VPN gateways for dialup VPN

The remote IPSec VPN gateways must be DFL-1000 IPSec VPN gateways or third-party IPSec VPN gateways running industry-standard IPSec AutoIKE key VPN software.

Configure the VPN gateway as required to connect to the dialup VPN gateway using an IPSec AutoIKE key VPN configuration. Use the information in [Example remote IPSec VPN gateway configuration](#) to configure the gateway.

Example remote IPSec VPN gateway configuration		
Field name	DFL-1000 VPN gateway information	Client information
Remote Gateway	The external IP address of the dialup VPN gateway.	1.1.1.1
Authentication Key	The gateway authentication key must match the dialup VPN gateway tunnel authentication key.	ddcHH01887d

Configuring remote IPSec VPN clients for dialup VPN

The VPN client must be running industry-standard IPSec AutoIKE key VPN client software, such as the D-Link Remote VPN Client.

Configure the client as required to connect to the dialup VPN gateway using an IPSec AutoIKE key VPN configuration. Use the information in [Example remote IPSec VPN client configuration](#) to configure the client.

Example remote IPSec VPN client configuration		
Field name	DFL-1000 VPN gateway information	Client information
Remote Gateway	The external IP address of the dialup VPN gateway.	1.1.1.1
DH Group	Should match the VPN tunnel DH Group.	5
Authentication Key	The client authentication key must match the dialup VPN gateway tunnel authentication key.	ddcHH01887d

Manual key VPN between two networks

In this example, you configure a manual key VPN between two internal networks. [Example VPN between two internal networks](#) shows this configuration.

Use the following procedures to configure the manual key VPN:

- [Configuring the manual key VPN tunnel](#)
- [Adding source and destination addresses](#)
- [Adding an encrypt policy](#)

Configuring the manual key VPN tunnel

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

Example manual key tunnel configuration		
Field name	Main Office information	Branch Office information
VPN Tunnel Name	Branch_Office_VPN	Main_Office_VPN
Local SPI	100000	200000
Remote SPI	200000	100000
Remote Gateway	2.2.2.1	1.1.1.1
Replay Detection	Select	Select
Encryption Algorithm	ESP-3DES-HMAC-SHA1	ESP-3DES-HMAC-SHA1
Encryption Key	1234567890abcdef 1234567890abcdef 1234567890abcdef	1234567890abcdef 1234567890abcdef 1234567890abcdef
Authentication Key	1234567890abcdef 1234567890abcdef12345678	1234567890abcdef 1234567890abcdef12345678
Concentrator	None	None



The Local and Remote SPI values for both gateways should complement each other. You can use any HEX characters for the Local and Remote SPI. The Local SPI on the Main Office gateway should match the Remote SPI on the Branch Office gateway. The Remote SPI on the Main Office gateway should match the Local SPI on the Branch Office gateway. Both the Local SPI and the Remote SPI values must be greater than BB8.



You can use any HEX characters for the encryption and authentication keys. However, they must be the same on both VPN gateways.



For more information about manual key tunnel settings, see [Adding a manual key VPN tunnel](#).

To configure the manual key tunnel on both VPN gateways:

- Go to *VPN > IPSEC > Manual Key* .
- Select New to add a manual key tunnel.
- Configure the manual key tunnel using the Main Office information in [Example manual key tunnel configuration](#).
- Select OK to save the manual key tunnel.
- Repeat steps [Select New to add a manual key tunnel](#). to [Select OK to save the manual key tunnel](#). on the appropriate DFL-1000 NPG, using the Branch Office information in [Example manual key tunnel configuration](#).

Adding source and destination addresses

Use the procedure [Adding source and destination addresses for a network-to-network VPN](#).

Adding an encrypt policy

Use the procedure [Adding an encrypt policy for a network-to-network VPN](#).

Manual key VPN for remote clients

In this example, you configure a manual key VPN between an internal network and a remote VPN client. [Example VPN between a main office internal network and a remote client](#) shows this configuration.

Use the following procedures to configure the manual key VPN:

- [Configuring the manual key tunnel](#)
- [Adding internal and external addresses](#)
- [Adding an encrypt policy](#)
- [Configuring the IPsec VPN client](#)

Configuring the manual key tunnel

[Example DFL-1000 VPN gateway and client manual key tunnels](#) shows the information required to configure the manual key tunnel for the example VPN in [Example VPN between a main office internal network and a remote client](#).

Example DFL-1000 VPN gateway and client manual key tunnels		
Field name	DFL-1000 VPN gateway information	Client information
VPN Tunnel Name	Client_VPN	Gateway_VPN
Local SPI	100000	200000
Remote SPI	200000	100000
Remote Gateway	2.2.2.2	1.1.1.1
Replay Detection	Select	Select
Encryption Algorithm	ESP-3DES-HMAC-SHA1	ESP-3DES-HMAC-SHA1
Encryption Key	1234567890abcdef 1234567890abcdef 1234567890abcdef	1234567890abcdef 1234567890abcdef 1234567890abcdef
Authentication Key	1234567890abcdef 1234567890abcdef 12345678	1234567890abcdef 1234567890abcdef 12345678
Concentrator	None	None



The Local and Remote SPI values for the DFL-1000 VPN gateway and the client should complement each other. You can use any HEX characters for the Local and Remote SPI. The Local SPI on the DFL-1000 VPN gateway should match the Remote SPI on the client. The Remote SPI on the DFL-1000 VPN gateway should match the Local SPI on the client. Both the Local SPI and the Remote SPI value must be greater than BB8.



You can use any HEX characters for the encryption and authentication keys. However, they must be the same on the DFL-1000 VPN gateway and on the client.



For more information about manual key tunnel settings, see [Adding a manual key VPN tunnel](#).

To configure the manual key tunnel on the DFL-1000 VPN gateway:

- Go to *VPN > IPSEC > Manual Key*.
- Select New to add a manual key tunnel.
- Configure the manual key tunnel using the DFL-1000 VPN gateway information in [Example DFL-1000 VPN gateway and client manual key tunnels](#).

- Select OK to save the manual key tunnel.
- Repeat steps [Select New to add a manual key tunnel.](#) to [Select OK to save the manual key tunnel.](#) on the appropriate DFL-1000 NPG, using the client information in [Example DFL-1000 VPN gateway and client manual key tunnels.](#)

Adding internal and external addresses

Use the procedure [Adding source and destination addresses for a remote client VPN.](#)

Adding an encrypt policy

Use the procedure [Adding an encrypt policy for a remote client.](#)

Configuring the IPsec VPN client

The VPN client must be running industry-standard IPsec AutoIKE key VPN client software, such as the SafeNet/Soft-PK client from SafeNet, Inc.

Configure the client as required to connect to the DFL-1000 VPN gateway using an IPsec VPN configuration. Use the information in [Example DFL-1000 VPN gateway and client manual key tunnels](#) to configure the client.

Hub and spoke VPN (VPN concentrator)

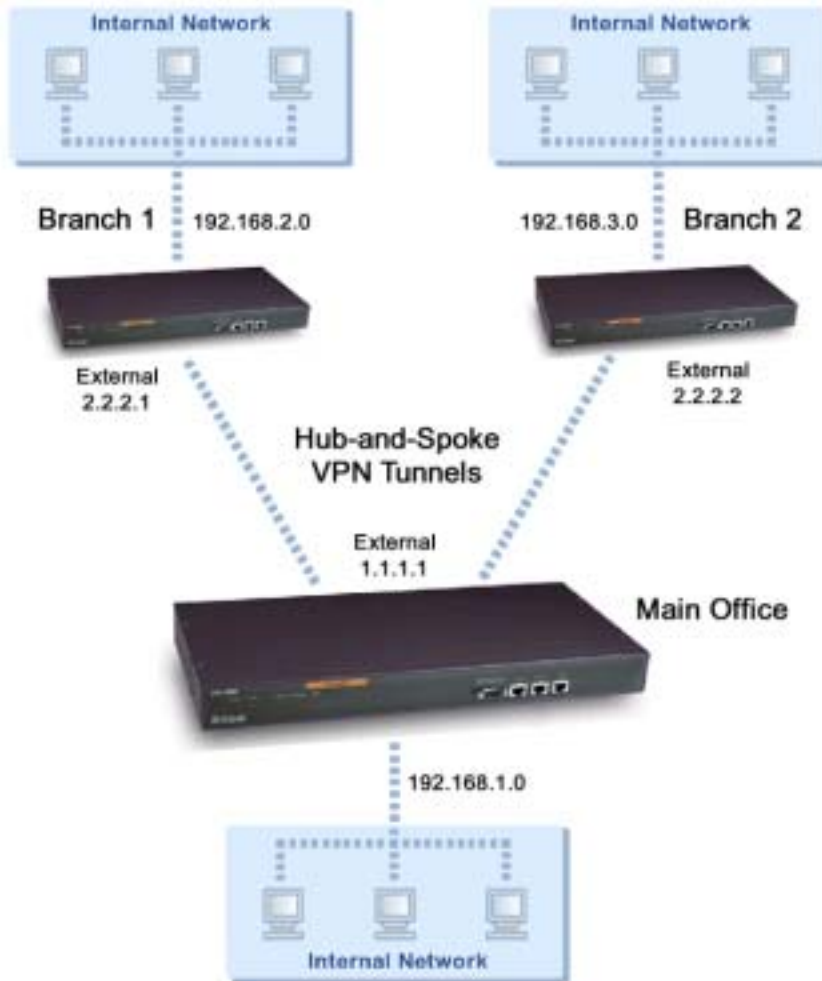
Using a VPN concentrator you can create a hub and spoke VPN configuration to direct traffic through a central DFL-1000 NPG from one VPN tunnel to another VPN tunnel. You create the hub and spoke configuration by adding a VPN concentrator to the central (or hub) DFL-1000 NPG and then adding VPN tunnels to the concentrator. Each VPN tunnel provides connectivity to a different remote VPN gateway. All of the VPN concentrator member tunnels can establish VPN connections with any of the other member VPN tunnels.

In this example, a company with a main office and two branch offices communicates using a hub and spoke VPN configuration. The Main Office is the hub where the VPN tunnels terminate, while Branch Office 1 and Branch Office 2 are the spokes. The Main Office has a VPN tunnel to each branch office. Branch 1 and Branch 2 each has its own VPN tunnel to the hub.

The Main Office hub needs two encrypt policies, one policy to Branch 1 and one policy to Branch 2. Each spoke also needs two encrypt policies, one policy to the Main Office (the hub) and one policy to the other spoke. The two policies at each spoke use the same tunnel. In the policy list for each spoke, the policy to the hub must be arranged in the policy list above the policy to the other spoke.

[Example hub and spoke VPN configuration](#) shows the example configuration. Each branch office has a VPN tunnel that terminates at the Main Office, where the DFL-1000 NPG directs the traffic between the VPN tunnels.

Example hub and spoke VPN configuration



This section contains examples for:

- [Configuring the hub](#)
- [Configuring the spokes](#)

Configuring the hub

For the Main Office (the hub), you create a remote gateway and an AutoIKE key tunnel. You also create a VPN concentrator and add tunnels to it as members. You then add policies to direct the VPN traffic.

Use the following procedures to create the Main Office hub:

- [Configuring the remote gateways](#)
- [Configuring the AutoIKE key tunnels](#)
- [Configuring the VPN concentrator](#)
- [Adding source and destination addresses](#)
- [Adding encrypt policies](#)

Configuring the spokes

For Branch 1 and Branch 2, you create remote gateways and AutoIKE key tunnels and then add the tunnels to the VPN concentrator. You then add policies to direct the VPN traffic.

Use the following procedures to create Branch 1 and Branch 2:

- [Configuring the remote gateways](#)
- [Configuring the AutoIKE key tunnels](#)
- [Adding source and destination addresses](#)
- [Adding encrypt policies](#)

Configuring the remote gateways

Use the procedure [Configuring the remote gateway for remote clients](#).

Use the information in [Example remote gateway configuration](#) to configure remote gateways for the Main Office, Branch 1, and Branch 2.

Example remote gateway configuration

Field name	Main Office information		Branch 1 information	Branch 2 information
Gateway Name	Branch1_gw	Branch2_gw	Main_Office_gw	Main_Office_gw
Remote Gateway	Static IP Address	Static IP Address	Static IP Address	Static IP Address
IP Address	2.2.2.1	2.2.2.2	1.1.1.1	1.1.1.1
Mode	Main (ID Protection)	Main (ID Protection)	Main (ID Protection)	Main (ID Protection)
P1 Proposal				
1- Encryption	3DES	3DES	3DES	3DES
Authentication	SHA1	SHA1	SHA1	SHA1
DH Group	5	5	5	5
Keylife	28800 seconds	28800 seconds	28800 seconds	28800 seconds
Authentication (Pre-shared Key)	ddcHH01887d	ddcHH01887d	ddcHH01887d	ddcHH01887d
Local ID	Blank	Blank	Blank	Blank
NAT-traversal	Not selected	Not selected	Not selected	Not selected
Keepalive Frequency	Blank	Blank	Blank	Blank

Configuring the AutoIKE key tunnels

Configure a separate AutoIKE key tunnel for the hub and for each spoke. These tunnels will use the remote gateways that you created in the procedure [Configuring the remote gateways](#).

Use the procedure [Configuring the AutoIKE key tunnel for a remote client](#).

Use the information in [Example AutoIKE key tunnel configuration](#) to configure the AutoIKE key tunnels.

Example AutoIKE key tunnel configuration

Field name	Main Office information		Branch 1 information	Branch 2 information
Tunnel Name	Branch1_VPN	Branch2_VPN	Main_Office_VPN	Main_Office_VPN
Remote Gateway	Branch1_gw	Branch2_gw	Main_Office_gw	Main_Office_gw
P2 Proposal				
1- Encryption	3DES	3DES	3DES	3DES
Authentication	SHA1	SHA1	SHA1	SHA1
Enable replay detection	Select	Select	Select	Select

Enable perfect forward secrecy (PFS)	Select	Select	Select	Select
DH Group	5	5	5	5
Keylife	300 seconds	300 seconds	300 seconds	300 seconds
Autokey Keep Alive	Enable	Enable	Enable	Enable
Concentrator	Not selected	Not selected	Not selected	Not selected

Configuring the VPN concentrator

For the Main Office (the hub), create the VPN concentrator and add the appropriate members to it. Add all the tunnels that are part of the same hub and spoke configuration to the same VPN concentrator.

If you add a spoke to the configuration after you create the VPN concentrator, you can add the new VPN tunnel to the VPN concentrator by selecting the concentrator name while you are configuring the tunnel.

[Example VPN concentrator configuration](#) shows the information required to configure the VPN concentrator.

Example VPN concentrator configuration

Field name **VPN concentrator information**

Concentrator Name Main_Office_Concentrator

Members Branch1_VPN
Branch2_VPN

To add a VPN concentrator:

- Go to VPN > IPSec > Concentrator.
- Select New to add a VPN concentrator.
- Enter the name of the new VPN concentrator in the Concentrator Name field.
- Select Branch1_VPN in the Available Tunnels list and select the right arrow.
The tunnel moves to the Members list.
- Select Branch2_VPN in the Available Tunnels list and select the right arrow.
The tunnel moves to the Members list.
- Select OK to add the VPN concentrator.

Adding source and destination addresses

Add source and destination addresses for the Main Office, Branch 1, and Branch 2.

Use the procedure [Adding source and destination addresses for a remote client VPN](#).

Use the information in [Example IPSec source and destination address information](#) to add the source and destination addresses. You need to add the addresses for each location individually.

Example IPSec source and destination address information

Field name	Main Office information	Branch 1 information	Branch 2 information
Source Address			
Address Name	Main_Office	Branch1	Branch2
IP address	192.168.1.0	192.168.2.0	192.168.3.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.0
Destination Address			
Address Name	Branch1	Branch2	Main_Office
IP address	192.168.2.0	192.168.3.0	192.168.1.0

Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
----------------	---------------	---------------	---------------	---------------

Adding encrypt policies

Use the information in tables below to add the encrypt policies.

Use the procedure [Adding an encrypt policy for a remote client](#).

The Main Office requires one policy to each branch office. Each branch office requires two policies on the same tunnel. At the branch offices, the policy for the hub must be arranged in the policy list above the policies for the spokes.

Main office encrypt policies	
Field name	Policy information
Main Office to Branch 1	
Source	192.168.1.0
Destination	192.168.2.0
Action	Encrypt
VPN Tunnel Name	Branch1_VPN
Main Office to Branch 2	
Source	192.168.1.0
Destination	192.168.3.0
Action	Encrypt
VPN Tunnel Name	Branch2_VPN

Branch Office 1 encrypt policies	
Field name	Policy information
Branch 1 to Main Office (policy for hub)	
Source	192.168.2.0
Destination	192.168.1.0
Action	Encrypt
VPN Tunnel Name	Main_Office_VPN
Branch 1 to Branch 2	
Source	192.168.2.0
Destination	192.168.3.0
Action	Encrypt
VPN Tunnel Name	Main_Office_VPN

Branch Office 2 encrypt policies	
Field name	Policy information
Branch 2 to Main Office	
Source	192.168.3.0
Destination	192.168.1.0
Action	Encrypt
VPN Tunnel Name	Main_Office_VPN

Branch 2 to Branch 1	
Source	192.168.3.0
Destination	192.168.2.0
Action	Encrypt
VPN Tunnel Name	Main_Office_VPN

PPTP and L2TP VPNs

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

PPTP is a Windows VPN standard. You can use PPTP to connect computers running Windows to a DFL-1000 NPG-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 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. When the client computer is 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/Route mode.

This chapter describes:

- [PPTP VPN configuration](#)
- [L2TP VPN configuration](#)

PPTP VPN configuration

PPTP clients must be able to authenticate with the DFL-1000 NPG to start a PPTP session. To support PPTP authentication, you must add a user group to the DFL-1000 NPG configuration. This user group can contain users added to the DFL-1000 NPG user database, RADIUS servers, or both.

After you have added a user group, configure your DFL-1000 NPG to support PPTP by enabling PPTP and specifying a PPTP address range. The PPTP address range is the range of addresses that must be reserved for remote PPTP clients. When a remote PPTP client connects to the internal network using PPTP, the client computer is assigned an IP address from this range. The PPTP address range can be on any subnet.

Add firewall policies with an external source address to control the access that PPTP clients have through the DFL-1000 NPG.

Add the addresses in the PPTP address range to the external interface address list. To make policy configuration easier, you can create an address group for PPTP that contains the IP addresses that can be assigned to PPTP clients from the PPTP address range.

Add addresses to the destination interface address list to control the addresses to which PPTP clients can connect.

The destination interface can be either the Int or DMZ interface. For example, if the destination address is on the internal network, you would create an Ext -> Int policy to control the access that PPTP users have through the DFL-1000 NPG.

Set the service for the policy to the traffic type inside the PPTP VPN tunnel. For example, if you want PPTP clients to be able to access a web server, set service to HTTP.



Make sure that your ISP supports PPTP connections.

This section describes:

- [Configuring the DFL-1000 NPG 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-1000 NPG



Configuring the DFL-1000 NPG as a PPTP gateway

Create a user group for the PPTP clients.

See [Users and authentication](#).

- Go to **VPN > PPTP > PPTP Range** .
- Select Enable PPTP.
- Enter the Starting IP and the Ending IP for the PPTP address range.
- Select the User Group that you added in step [Create a user group for the PPTP clients](#).
- Select Apply to enable PPTP through the DFL-1000 NPG.

Example PPTP Range configuration



PPTP Range

Enable PPTP

Starting IP:

Ending IP:

User Group:

Disable PPTP

- Add the addresses from the PPTP address range to the external interface address list. The addresses can be grouped into an external address group.
- Add the addresses to which PPTP users can connect to the interface connected to the destination network. The addresses can be grouped into an address group.
- Add a policy to allow PPTP clients to connect through the DFL-1000 NPG.
Configure the policy as follows:

Source The address group that matches the PPTP address range.

Destination The address to which PPTP users can connect.

Service The service that matches the traffic type inside the PPTP VPN tunnel. For example, if PPTP users can access a web server, select HTTP.

Action ACCEPT

NAT Select NAT if address translation is required.

You can also configure traffic shaping, logging, and web filter settings for PPTP policies.

For information about adding firewall policies, see [Adding NAT/Route mode policies](#).

Configuring a Windows 98 client for PPTP

Use the following procedure to configure a client computer running Windows 98 so that it can connect to a DFL-1000 PPTP VPN. To configure the Windows 98 client, you must install and configure Windows dialup networking and virtual private networking support.

Installing PPTP support

- Go to *Start > Settings > Control Panel > Network* .
- Select Add.
- Select 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 dialup connection

- Go to *My Computer > Dial-Up Networking > Configuration* .
- Double-click Make New Connection.
- Name the connection and select Next.
- Enter the IP address or host name of the DFL-1000 NPG 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.
- Uncheck Use IP header compression.
- Uncheck Use default gateway on remote network.
- Select OK twice.

Connecting to the PPTP VPN

- Start the dialup 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 computer running Windows 2000 so that it can connect to a DFL-1000 PPTP VPN.

Configuring a PPTP dialup connection

- Go to *Start > Settings > Network and Dial-up Connections* .
- Double-click Make New Connection to start the Network Connection Wizard and select Next.
- For Network Connection Type, select Connect to a private network through the Internet and select Next.
- For Destination Address, enter the IP address or host name of the DFL-1000 NPG to connect to and select Next.
- Set Connection Availability to Only for myself and select Next.
- Select Finish.
- In the Connect window, select Properties.
- Select the Security tab.
- Uncheck Require data encryption.
- Select OK.

Connecting to the PPTP VPN

- Start the dialup 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 that you use to connect to your dialup 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 computer running Windows XP so that it can connect to a DFL-1000 PPTP VPN.

Configuring a PPTP dialup 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 IP address or host name of the DFL-1000 NPG to connect to and select Next.
- Select Finish.

Configuring the VPN connection

- Right-click the Connection icon that you created in the previous procedure.
- Select **Properties > Security** .
- Select Typical to configure typical settings.
- Select Require data encryption.



If a RADIUS server is used for authentication do not select Require data encryption. PPTP encryption is not supported for RADIUS server authentication.

- Select Advanced to configure advanced settings.
- Select Settings.
- Select Challenge Handshake Authentication Protocol (CHAP).
- Make sure that none of the other settings are selected.
- Select the Networking tab.
- Make sure that the following options are selected:
TCP/IP
QoS Packet Scheduler
- Make sure that 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 that you use to connect to your dialup network connection.

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

L2TP VPN configuration

L2TP clients must be able to authenticate with the DFL-1000 NPG to start a L2TP session. To support L2TP authentication, you must add a user group to the DFL-1000 NPG configuration. This user group can contain users added to the DFL-1000 NPG user database, RADIUS servers, or both.

After you have added a user group, configure your DFL-1000 NPG to support L2TP by enabling L2TP and specifying a L2TP address range. The L2TP address range is the range of addresses that must be reserved for remote L2TP clients. When a remote L2TP client connects to the internal network using L2TP, the client computer is assigned an IP address from this range. The L2TP address range can be on any subnet.

L2TP VPN between a Windows client and the DFL-1000 NPG



Add firewall policies with an external source address to control the access that L2TP clients have through the DFL-1000 NPG.

Add the addresses in the L2TP address range to the external interface address list. To make policy configuration easier, you can create an address group for L2TP that contains the IP addresses that can be assigned to L2TP clients from the L2TP address range.

Add addresses to the destination interface address list to control the addresses to which L2TP clients can connect.

The destination interface can be either the Int or DMZ interface. For example, if the destination address is on the internal network, you would create an Ext -> Int policy to control the access that L2TP users have through the DFL-1000 NPG.

Set the service for the policy to the traffic type inside the L2TP VPN tunnel. For example, if you want L2TP clients to be able to access a web server, set service to HTTP.



Make sure that your ISP supports L2TP connections.

This section describes:

- [Configuring the DFL-1000 NPG as an L2TP gateway](#)
- [Configuring a Windows 2000 client for L2TP](#)
- [Configuring a Windows XP client for L2TP](#)

Configuring the DFL-1000 NPG as an L2TP gateway

- Create a user group for the L2TP users.
See [Users and authentication](#).
- Go to **VPN > L2TP > L2TP Range**.
- Select Enable L2TP.
- Enter the Starting IP and the Ending IP for the L2TP address range.
- Select the User Group that you added in step [Create a user group for the L2TP users](#).
- Select Apply to enable L2TP through the DFL-1000 NPG.

Sample L2TP address range configuration

L2TP Range

Enable L2TP

Starting IP:

Ending IP:

User Group:

Disable L2TP

- Add the addresses from the L2TP address range to the external interface address list. The addresses can be grouped into an external address group.
- Add the addresses to which L2TP users can connect to the interface connected to the destination network. The addresses can be grouped into an address group.
- Add a policy to allow L2TP clients to connect through the DFL-1000 NPG.

Configure the policy as follows:

Source	The address group that matches the L2TP address range.
Destination	The address to which L2TP users can connect.
Service	The service that matches the traffic type inside the L2TP VPN tunnel. For example, if L2TP users can access a web server, select HTTP.
Action	ACCEPT
NAT	Select NAT if address translation is required.

You can also configure traffic shaping, logging, and web filter settings for L2TP policies. For information about adding firewall policies, see [Adding NAT/Route mode policies](#).

Configuring a Windows 2000 client for L2TP

Use the following procedure to configure a client computer running Windows 2000 so that it can connect to a DFL-1000 L2TP VPN.

Configuring an L2TP dialup connection

- Go to *Start > Settings > Network and Dial-up Connections*.
- Double-click Make New Connection to start the Network Connection Wizard and select Next.
- For Network Connection Type, select Connect to a private network through the Internet and select Next.
- For Destination Address, enter the address of the DFL-1000 NPG to connect to and select Next.
- Set Connection Availability to Only for myself and select Next.
- Select Finish.
- In the Connect window, select Properties.
- Select the Security tab.
- Make sure that Require data encryption is selected.



If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

- 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 that Do not use IPSEC is selected.
- 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. See 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 dialup 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 that you use to connect to your dialup 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 computer running Windows XP so that it can connect to a DFL-1000 L2TP VPN.

Configuring an L2TP VPN dialup 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 IP address or host name of the DFL-1000 NPG 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.



If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

- Select Advanced to configure advanced settings.
- Select Settings.

- Select Challenge Handshake Authentication Protocol (CHAP).
- Make sure that none of the other settings are selected.
- Select the Networking tab.
- Make sure that the following options are selected:
TCP/IP
QoS Packet Scheduler
- Make sure that 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 that Do not use IPSEC is selected.
- 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. See 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 that you use to connect to your dialup network connection.
This user name and password is not the same as your VPN user name and password.

Web content filtering


Use DFL-1000 web content filtering for:

- [Enabling web content filtering](#)
- [Blocking web pages that contain unwanted content](#)
- [Blocking access to URLs](#)
- [Removing scripts from web pages](#)
- [Exempting URLs from content or URL blocking](#)

Enabling web content filtering

Enable web content filtering by selecting the Web filter option in firewall policies that allow HTTP connections through the DFL-1000 NPG. Next, configure web content filtering settings to control how the DFL-1000 NPG applies web content filtering to the HTTP traffic allowed by policies.

To enable web content filtering:

- Go to *Firewall > Policy*.
- Select a policy list that contains policies for which you want to enable web content protection.
- Select New to add a new policy, or choose a policy to edit and select Edit .
The policy must have Service set to ANY, HTTP, or a service group that includes HTTP.
See [Adding NAT/Route mode policies](#) or [Adding Transparent mode policies](#).
- Select Web filter to enable web content filtering protection for this policy. Select show settings to view the current web content filtering configuration.
- Select OK to save the policy.
- Repeat this procedure for any HTTP policies for which to enable web content filtering.

Blocking web pages that contain unwanted content

Block web pages that contain unwanted content by selecting Web Filter in firewall policies, enabling content blocking, and then creating a list of banned words and phrases. When the DFL-1000 NPG blocks a web page, the user who requested the blocked page receives a block message and the DFL-1000 NPG writes a message to the event log.

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

- Go to *Web Filter > Content Block* .
- Select Enable Banned Word to turn on content blocking.
The DFL-1000 NPG 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-1000 NPG 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-1000 NPG displays the message when content is blocked.

Adding 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, Chinese Simplified, Chinese Traditional, 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-1000 NPG blocks all web pages that contain that word.
If you type a phrase (for example, *banned phrase*), the DFL-1000 NPG blocks web pages that contain both words. When this phrase appears on the banned word list, the DFL-1000 NPG inserts plus signs (+) in place of spaces (for example, *banned+phrase*).
If you type a phrase in quotes (for example, "*banned word*"), the DFL-1000 NPG blocks all web pages in which 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.
- In the Modify column, check the box beside the new entry in the banned word list so that the DFL-1000 NPG blocks web pages containing this word or phrase.
You can enter multiple banned words or phrases and then select Check All  to activate all entries in the banned word list.



Enable Banned Word must be selected at the top of the banned word list for web pages containing banned words to be blocked.

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*.
- In the Modify column, uncheck the box beside an individual entry in the banned word list.
- You can also select Uncheck All to uncheck all entries in the banned word list. All unchecked items in the banned word list are not blocked by the DFL-1000 NPG.

Clearing the banned word list

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

- Go to *Web Filter > Content Block*.
- Select Clear Banned Word List to remove all entries in the banned word list.

Backing up the banned word list

You can back up the banned word list by downloading it to a text file on the management computer:

- Go to *Web Filter > Content Block*.
- Select Backup Banned Word list .

The DFL-1000 NPG 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 create or edit a banned word list in a text file and upload it from your management computer to the DFL-1000 NPG.


Each banned word or phrase must appear on a separate line in the text file. Use ASCII and western language characters only.

All words are enabled by default. You can optionally follow the word with a space and a 1 another space and a 0 (zero) to enable it and to indicate western language characters.

Sample banned word list text file

```
Banned 1 0
Banned+phrase+1 1 0
“banned phrase 2” 1 0
```

To restore the banned word list:

- 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 banned word list backup text file.
- Select Return to display the restored banned word list.

Blocking access to URLs

To block access to URLs, enable URL blocking and then create a list of URLs to be blocked. You can block all pages on a website by adding its top-level URL or IP address. Alternatively, you can block individual pages on a website by including the the full path and filename of the web page to block.

When the DFL-1000 NPG blocks a web page, the user who requested the blocked page receives a block message and the DFL-1000 NPG writes a message to the event log.

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

- Go to *Web Filter > URL Block* .
- Select Enable URL Block to turn on URL blocking.
The DFL-1000 NPG 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-1000 NPG 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-1000 NPG will now display this message when a URL is blocked.

Adding 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 top-level URL or IP address to block access to all pages on a website. For example, *www.badsite.com* or *122.133.144.155* blocks access to all pages at this website.




Enter a top-level URL followed by the path and filename to block access to a single page on a website. For example, *www.badsite.com/news.html* or *122.133.144.155/news.html* blocks the news page on this website.

Do not include *http://* in the URL to block.

To block all pages with a URL that ends with *badsite.com* , add *badsite.com* to the block list. For example, adding *badsite.com* blocks access to *www.badsite.com* , *mail.badsite.com* , *www.finance.badsite.com* , and so on.



URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to *ftp://ftp.badsite.com* . Instead, you can use firewall policies to deny FTP connections.

- 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 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 URL block list.

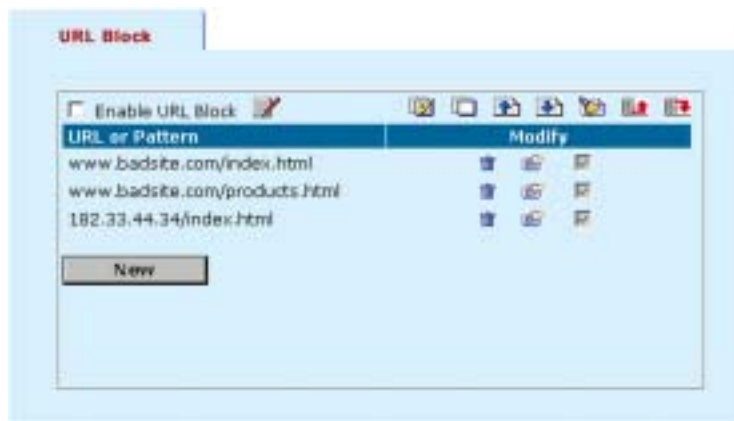


Enable URL Block must be selected at the top of the URL block list for web pages with banned URLs to be blocked.



You can add URLs to the URL block list by adding them to a text file and then uploading the text file to the DFL-1000 NPG. 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* .
- To page through the URL block list to find a URL, select Page Down  or Page Up .
- To disable a URL, select Edit  in the Modify column.
- Uncheck Enable.
- Select OK to save your changes.
- You can also select Uncheck All  to uncheck all items in the URL block list.
All unchecked items in the URL block list are not blocked by the DFL-1000 NPG.

Clearing the URL block list

- Go to *Web Filter > URL Block* .
- Select Clear URL Block List  to remove all 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 .

The DFL-1000 NPG 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-1000 NPG. 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-1000 NPG automatically enables all 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
182.33.44.34/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. For example, you can download the squidGuard blacklists available at <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-1000 NPG 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-1000 NPG.

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-1000 NPG.
- 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 URL block list.
- You can continue to maintain the URL block list by making changes to the text file and uploading it again.

Removing scripts from web pages

Use the following procedure to configure the DFL-1000 NPG to remove scripts from web pages. You can configure the DFL-1000 NPG to block Java applets, cookies, and ActiveX.



Blocking of any of these items might 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



Exempting URLs from content or URL blocking

Add URLs to the Exempt URL list to allow legitimate traffic that might otherwise be blocked by content or URL blocking. For example, if content blocking is set to block pornography-related words and a reputable

website runs a story on pornography, web pages from the reputable website would be blocked. Adding the address of the reputable website to the Exempt URL list allows the content of the website to bypass content blocking.

This section describes:

- [Adding URLs to the Exempt URL list](#)
- [Temporarily disabling entries in the Exempt URL list](#)
- [Clearing the Exempt URL list](#)
- [Downloading the Exempt URL list](#)
- [Uploading an Exempt URL list](#)

Adding URLs to the Exempt URL list




- Go to *Web Filter > Exempt URL* .
- Select New to add an entry to the Exempt URL list.
- Type the URL to exempt.


Enter a complete URL, including path and filename, to exempt access to a page on a website. For example, *www.goodsite.com/index.html* exempts access to the main page of this example website. You can also add IP addresses; for example, *122.63.44.67/index.html* exempts access to the main web page at this address. Do not include *http://* in the URL to exempt.

Exempting a top-level URL, such as *www.goodsite.com*, exempts all requested subpages (for example, *www.goodsite.com/ badpage*) from all content and URL filtering rules.

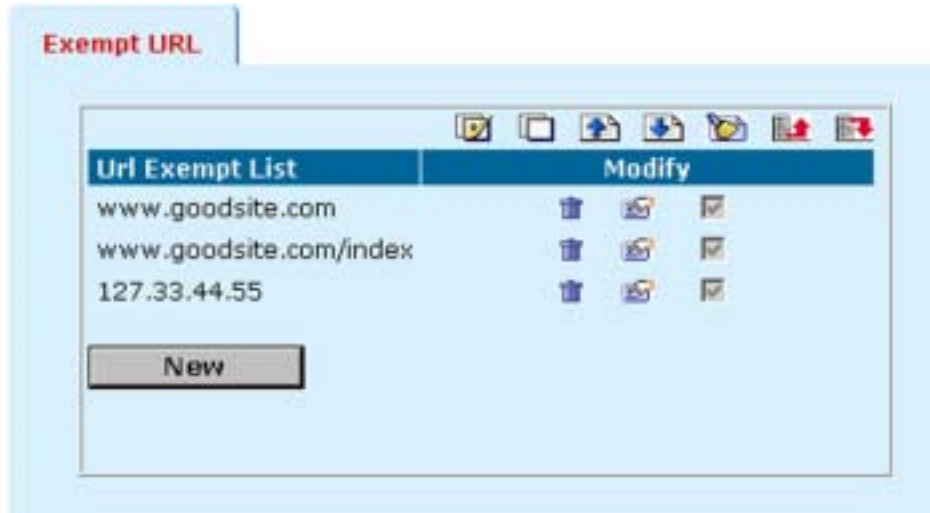


Exempting a top-level URL does not exempt pages such as *mail.goodsite.com* from all content and URL filtering rules unless *goodsite.com* (without the *www*) is added to the Exempt URL list.





- Select Enable to exempt the URL.
- Select OK to add the URL to the Exempt URL list.
You can enter multiple URLs and then select Check All  to activate all entries in the Exempt URL list.
Each page of the Exempt URL list displays 100 URLs.
- Use Page Down  and Page Up  to navigate through the Exempt URL list.

 You can add URLs to the Exempt List by adding them to a text file and then uploading the text file to the DFL-1000 NPG. See [Uploading an Exempt URL list](#).


Sample Exempt URL list



Temporarily disabling entries in the Exempt URL list


- Go to *Web Filter > Exempt URL* .
- To page through the Exempt URL list to find a URL, select Page Down  or Page Up .
- To disable a URL, select Edit  in the Modify column.
- Uncheck Enable.
- Select OK to save your changes.
- You can also select Uncheck All  to uncheck all URLs in the Exempt URL list.
All unchecked items in the Exempt List can be blocked by the DFL-1000 NPG according to other content blocking lists.

Clearing the Exempt URL list

- Go to *Web Filter > Exempt URL* .
- Select URL Exempt List  to remove all URLs from the Exempt URL list.

Downloading the Exempt URL list

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

- Go to *Web Filter > Exempt URL* .
- Select Download Exempt URL List  .

The DFL-1000 NPG downloads the list to a text file on the management computer.

Uploading an Exempt URL list

You can create a Exempt URL list in a text editor and then upload the text file to the DFL-1000 NPG. 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-1000 NPG automatically enables all URLs in the Exempt List when you upload the text file.

Sample Exempt URL list text file

```
www.goodsite.com/index 1
www.goodsite.com/products 1
127.33.44.55/index 1
```

You can either create the Exempt URL list yourself or add a URL list created by a third-party exempt or whitelist URL service.



All changes made to the Exempt URL list using the web-based manager are lost when you upload a new list. However, you can download your current Exempt URL list, add more URLs to it using a text editor, and then upload the edited list to the DFL-1000 NPG.

- In a text editor, create the list of URLs to exempt.
- Using the web-based manager, go to **Web Filter > Exempt URL** .
- Select Upload Exempt URL List
- Enter the path and filename of your Exempt URL list text file, or select Browse and locate the file.
- Select OK to upload the file to the DFL-1000 NPG.
- Select Return to display the updated Exempt URL list.
Each page of the Exempt URL list displays 100 URLs.
- Use Page Down and Page Up to navigate through the Exempt URL list.
- You can continue to maintain the Exempt URL list by making changes to the text file and uploading it again.

Logging and reporting

You can configure the DFL-1000 NPG to record three types of logs:

- Traffic logs record all traffic that attempts to connect through the DFL-1000 NPG.
- Event logs record management and activity events.

You can also use Log & Report to configure the DFL-1000 NPG to send alert emails for:

- Critical firewall or VPN events or violations (also recorded by the event log)

This chapter describes:

- [Configuring logging](#)
- [Viewing event log saved to memory](#)
- [Viewing and maintaining logs saved to the hard disk](#)
- [Configuring alert email](#)
- [Log message formats](#)

Configuring logging

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

- a computer running a syslog server,
- a computer running a WebTrends firewall reporting server,
- the DFL-1000 hard disk (if your DFL-1000 NPG contains a hard disk),
- the DFL-1000 system memory (if your DFL-1000 NPG does not contain a hard disk).



Logging to system memory is not available on all DFL-1000 models. The optional hard disk is not available for all DFL-1000 models.

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

This section describes:

- [Recording logs on a remote computer](#)
- [Recording logs on a NetIQ WebTrends server](#)
- [Recording logs on the DFL-1000 hard disk](#)
- [Logging event log to memory](#)
- [Selecting what to log](#)

Recording logs on a remote computer

Use the following procedure to configure the DFL-1000 to record log messages on 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.
- Enter the IP address of the remote computer running syslog server software.
- Select Apply to save your log settings.

Recording logs on a NetIQ WebTrends server

Use the following procedure to configure the DFL-1000 to record logs on a remote NetIQ firewall reporting server for storage and analysis. DFL-1000 log formats comply with WebTrends Enhanced Log Format

(WELF) and are compatible with WebTrends NetIQ Security Reporting Center 2.0 and Firewall Suite 4.1. See the Security Reporting Center and Firewall Suite documentation for more information.

To record logs on a NetIQ WebTrends server:

- Go to *Log&Report > Log Setting* .
- Select Log in WebTrends Enhanced Log Format.
- Enter the IP address of the NetIQ WebTrends firewall reporting server.
- Select Apply to save your log settings.

Example log settings with optional hard disk

Log Setting

Log to Remote Host: 192.168.1.20 (IP)

Log in WebTrends Enhanced Log Format: (IP)

Log to Local

The log file will rotate when either the file size or log time is reached.

Log file size: 10 (M)

Log time: 10 (day)

Log options when disk is full

Overwrite Block traffic Do not log

Log All Internal Traffic To Firewall

Log All External Traffic To Firewall

Log All DMZ Traffic To Firewall

Log All Events

Apply

Recording logs on the DFL-1000 hard disk

You can record log files on the DFL-1000 hard disk if one is installed on your system. If you do not have a hard disk installed, see [Recording logs on a remote computer](#) or [Recording logs on a NetIQ WebTrends server](#). On most DFL-1000 models you can record logs to memory only if no hard disk is installed.

To record logs on the DFL-1000 hard disk:

- Go to *Log&Report > Log Setting* .
- Select Log to Local.
- Type a maximum log file size (in Mbytes).

When the log file reaches this size, the current log file is closed and saved and a new active log file is started. The default maximum log size is 10 Mbytes.



The maximum allowed log file size is 2 Gbytes. If a log file reaches this size, it is closed and a new log file is opened.

Example log settings with no optional hard disk

Log Setting

Log to Remote Host: (IP)

Log in WebTrends Enhanced Log Format: (IP)

Log to memory (event and attack log only)

Log All Internal Traffic To Firewall

Log All External Traffic To Firewall

Log All DMZ Traffic To Firewall

Log All Events

- Type a log time interval (in days).
After the specified time interval, the current log file is closed and saved and a new one is started. The default log time interval is 10 days.
- Set Log options when disk is full to:

Overwrite Delete the oldest log file when the hard disk is full. Overwrite is the default option.

Block Traffic Block all network traffic when the hard disk is full.

Do not log Stop logging messages when the hard disk is full.

- Select Apply to save your log settings.

Logging event log to memory

If your DFL-1000 does not contain a hard disk, you can use the following procedure to configure the DFL-1000 to reserve some system memory for storing current event log messages. The DFL-1000 can store a limited number of messages in system memory. Once all available memory is used, the DFL-1000 deletes the oldest messages.

To record logs to memory:

- Go to *Log&Report > Log Setting* .
- Select Log to memory.
- Select Apply to save your log settings.

Selecting what to log

Use the following procedure to configure the type of information recorded in DFL-1000 logs.

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 DMZ Traffic To Firewall to record connections to the DMZ interface.



Traffic logs are also recorded when you select Log Traffic for a firewall policy.

- Select Log All Events to record management and activity events in the event log. 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 and URL blocking.
- Select Apply to save your log settings.




Viewing event log saved to memory

If the DFL-1000 is configured to save event log messages to memory, you can use the web-based manager to view, search, and clear the event log messages. This section describes:

- [Viewing event log](#)
- [Searching event log](#)
- [Clearing event log messages](#)

Viewing event log

Log messages are listed with the most recent message at the top. Use the following procedure to view event log messages saved in system memory:


- Go to *Log&Report > Logging* .
- Select **Event Log**.
The web-based manager lists the event log messages saved to system memory.
- Scroll through the log messages to view them.
- To view a specific line in the log, type a line number in the Go to line field and select .
- To navigate through the log message pages, select Go to Next Page  or Go to Previous page .



See [Log message formats](#) for a description of log message formats.

Searching event log

Use the following procedure to search event log messages saved in system memory:

- Go to *Log&Report > Logging* .
- Select **Event Log**.
- Select  to search the messages in the selected log.
- Select AND to search for messages that match all the specified search criteria.
- Select OR to search for messages that match one or more of the specified search criteria.
- Select one or more of the following search criteria:

Keyword To search for any text in a log message. Keyword searching is case-sensitive.

Time To search log messages created during the selected year, month, day, and hour.


- Select OK to run the search.
The web-based manager displays the messages that match the search criteria. You can scroll through the messages or run another search.



After running a search, to display all log messages again, run another search but leave all the search fields blank.

Clearing event log messages

Use the following procedure to clear the event log:

- Got to Log & Report > Logging.
- Select Event Log.
- Select  to clear all messages in the selected log.
- Select OK.

Viewing and maintaining logs saved to the hard disk

If your DFL-1000 contains a hard disk for recording logs, you can use the following procedures to view, search and maintain traffic and event logs:

- [Viewing logs](#)
- [Searching logs](#)
- [Downloading a log file to the management computer](#)
- [Deleting all messages in an active log](#)
- [Deleting a saved log file](#)





Viewing logs






Log messages are listed with the most recent message at the top. You can view the active or saved traffic, or event logs using the following procedure:

- Go to *Log&Report > Logging* .
- Select **Traffic Log** , or **Event Log**.

The web-based manager lists all saved logs of the selected type, with the active log at the top of the list. For each log, the list shows the date and time at which an entry was last added to the log, the size of the log file, and its name.

Sample event log list

Traffic Log		Event Log		
Last access time	Size	File name	Action	
Tue Jun 10 10:58:05 2003	40704	ellog		
Tue Jun 10 10:58:05 2003	40704	ellog.1		



- To view a log file, select View .
- The web-based manager displays the messages in the selected log.
- You can set the number of log messages to view on a single page to 30, 50 or All. You can scroll through the log entries.
- To view a specific line in the log file, type a line number in the Go to line field and select .
- To navigate through the log message pages, select Go to Next Page  or Go to Previous Page .
- To search the messages in the log file that you are viewing, select .



See [Log message formats](#) for a description of the log message formats.

Searching logs

Use the following procedure to search the active log or any of the saved log files:

- Go to *Log&Report > Logging* .
- Select **Traffic Log** , or **Event Log**.
- To view a log file, select View .
- Select  to search the messages in the log file that you are viewing.

Traffic Log Search



- Select AND to search for messages that match all the specified search criteria.
- Select OR to search for messages that match one or more of the specified search criteria.
- Select one or more of the following search criteria:

Keyword To search for any text in a log message. Keyword searching is case-sensitive.

Source To search for any source IP address (traffic log only).

Destination To search for any destination IP address (traffic log only).

Time To search log messages created during the selected year, month, day, and hour.

- Select OK to run the search.
The web-based manager displays the messages that match the search criteria. You can scroll through the messages or run another search.




After running a search, to display all log messages again, run another search but leave all the search fields blank.

Downloading a log file to the management computer

You can download traffic, or event log files to the management computer as plain text files. After downloading, you can view the log file with any text editor. Use the following procedure to download log files:

- Go to *Log&Report > Logging* .
- Select **Traffic Log** , or **Event Log**.

The web-based manager lists all saved logs of the selected type, with the active log at the top of the list. For each log, the list shows the date and time at which an entry was last added to the log, the size of the log file, and its name.


- To download a log file to the management computer, select Download .
- Select Save to download the log messages to a text file on the management computer.

Deleting all messages in an active log

Use the following procedure to delete all messages from the active traffic, or event log:

- Go to *Log&Report > Logging* .
- Select **Traffic Log** , or **Event Log**.

The web-based manager lists all saved logs of the selected type, with the active log at the top of the list. For each log, the list shows the date and time at which an entry was last added to the log, the size of the log file, and its name.


- To delete all messages in the active log file, select Empty Log .
- Select OK to delete the messages.

Deleting a saved log file

Use the following procedure to delete a saved traffic, or event log file:

- Go to *Log&Report > Logging* .
- Select **Traffic Log** , or **Event Log**.

The web-based manager lists all saved logs of the selected type, with the active log at the top of the list. For each log, the list shows the date and time at which an entry was last added to the log, the size of the log file, and its name.

- To delete a saved log file, select Delete .
- Select OK to delete the log file.

Configuring alert email

You can configure the DFL-1000 NPG to send alert emails to up to three email addresses. You can enable sending alert emails for firewall or VPN events or violations. If you have configured the DFL-1000 NPG to write log messages to an internal hard disk, you can enable sending an alert email when the disk is almost full.

This section describes:

- [Configuring alert email](#)
- [Testing alert emails](#)
- [Enabling alert emails](#)

Configuring alert email

- 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.
Because the DFL-1000 uses the SMTP server name to connect to the mail server, it must be able to look up this name on your DNS server.
- Select Apply.
- Go to **Log&Report > Alert Mail > Configuration**.

- In the SMTP Server field, enter the name of the SMTP server to which the DFL-1000 should send email.
The SMTP server can be located on any network connected to the DFL-1000.
- In the SMTP User field, enter a valid email address in the format user@domain.com.
This address appears in the From heading of the alert email.
- Enter up to three destination email addresses in the Email To fields.
These are the actual email addresses that the DFL-1000 sends alert email to.
- Select Apply to save the alert email settings.

Testing alert emails

You can test your alert email settings by sending a test email.

- Go to *Log&Report* > Alert Mail > Configuration.
- Select Test to send test email messages from the DFL-1000 NPG to the Email To addresses that you have configured.

Enabling alert emails

You can configure the DFL-1000 NPG to send alert email in response for firewall or VPN events. Use the following procedure to enable alert emails. If you have configured logging to a local disk, you can enable sending an alert email when the hard disk is almost full. Use the following procedure to enable alert emails:

- Go to *Log&Report* > Alert Mail > Categories .
- Select Enable Alert Email for Critical Firewall/VPN events or violations to have the DFL-1000 send an alert email when a critical firewall or VPN event occurs.
Critical firewall events include failed authentication attempts.
Critical VPN events include when replay detection detects a replay packet. Replay detection can be configured for both manual key and AutoIKE Key VPN tunnels.
- Select Send alert email when disk is full to have the DFL-1000 send an alert email when the hard disk is almost full.
- Select Apply.

Log message formats

The DFL-1000 traffic logs and event logs all have their own message format. All these message formats are compatible with the WebTrends Enhanced Log Format (WELF).

Use the information in the following sections to interpret DFL-1000 log messages:

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

Traffic log message format

The DFL-1000 records traffic log messages when:

- you configure logging to log all internal, external, or DMZ traffic to the firewall.
- you select Log Traffic for a firewall policy.

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=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 and URL blocking.

Each event log message records the date and time of the event and a description of the event. For connections to the DFL-1000 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 the message type *mgmt* except for messages that record VPN configuration changes, which have the type *vpn,mgmt*.

```
<date> <time> type=mgmt,msg="<management message>"
```

```
<date> <time> type=vpn,mgmt,msg="<vpn management message>"
```

Example management event log messages:

```
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 22 15:35:09 type=vpn,mgmt msg="VPN-ipsec_auto auto add successful at
192.168.100.111 by admin"
```

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 22 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"
```

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"
```

Administration

This chapter describes how to use the web-based manager to administer and maintain the DFL-1000 NPG. It contains the following sections:

- [System status](#)
- [Upgrading the DFL-1000 firmware](#)
- [Displaying the DFL-1000 NPG serial number](#)
- [Backing up system settings](#)
- [Restoring system settings](#)
- [Restoring system settings to factory defaults](#)
- [Changing to Transparent mode](#)
- [Changing to NAT/Route mode](#)
- [Restarting the DFL-1000 NPG](#)
- [Shutting down the DFL-1000 NPG](#)
- [System status monitor](#)
- [Network configuration](#)
- [Configuring the internal interface](#)
- [Configuring the external interface](#)
- [Configuring the dmz interface](#)
- [Configuring the management interface \(Transparent mode\)](#)
- [Setting DNS server addresses](#)
- [Configuring routing](#)
- [Adding routing gateways](#)
- [Adding a default route](#)
- [Adding routes to the routing table](#)
- [Configuring the routing table](#)
- [Enabling RIP server support](#)
- [Adding routes \(Transparent mode\)](#)
- [Configuring the DFL-1000 NPG for multiple Internet connections](#)
- [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](#)

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 DFL-1000 NPG system settings:

- [Upgrading the DFL-1000 firmware](#)
- [Backing up system settings](#)

- [Restoring system settings](#)
- [Restoring system settings to factory defaults](#)
- [Changing to Transparent mode](#)
- [Changing to NAT/Route mode](#)
- [Restarting the DFL-1000 NPG](#)
- [Shutting down the DFL-1000 NPG](#)

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

- [Displaying the DFL-1000 NPG serial number](#)

All administrative users can also go to **System > Status > Monitor** and view DFL-1000 NPG system status:


- [System status monitor](#)

Upgrading the DFL-1000 firmware

D-Link releases new versions of the DFL-1000 firmware periodically. You can save the firmware file on your management computer and then use one of the following procedures to upgrade the firmware on your DFL-1000 NPG:

- [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

- 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-1000 NPG.
The DFL-1000 NPG 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-1000 firmware using the CLI. To use this procedure, you must install a TFTP server and be able to connect to this server from the internal interface. The TFTP server should be on the same subnet as the internal interface.



Installing new firmware using the CLI deletes all changes that you have made to the 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 [Backing up the banned word list](#), [Downloading the URL block list](#), and [Downloading the Exempt URL list](#)).

Upgrading the firmware

To install a firmware upgrade using the CLI:

- Connect to the CLI.
- Make sure that the TFTP server is running.
- Copy the new firmware image file to the root directory of your TFTP server.

- Make sure that the internal interface of the DFL-1000 NPG is connected to the same network as the TFTP server.

- To confirm that you can connect to the TFTP server from the DFL-1000 NPG, use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- Enter the following command to restart the DFL-1000 NPG:

```
execute reboot
```

As the DFL-1000 NPG reboots, messages similar to the following appear:

```
BIOS Version 2.2
Serial number: FGT2002801012243
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-1000 NPG 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-1000 NPG 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-1000 NPG 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...
```

```
DFL-1000 login:
```

The installation might 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
```

When the interface addresses are changed, you can access the DFL-1000 NPG from the web-based manager and restore your configuration files and content and URL filtering lists.

Displaying the DFL-1000 NPG serial number

- Go to *System > Status* .

The serial number is displayed in the Status window. The serial number is specific to your DFL-1000 NPG 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 [Backing up the banned word list](#), [Downloading the URL block list](#), and [Downloading the Exempt URL 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 Backup.
- Select Backup System Settings.
- Type a name and location for the file.
The system settings file is backed up 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 [Restoring the banned word list](#), [Uploading a URL block list](#), and [Uploading an Exempt URL list](#).

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

- Go to *System > Status* .
- Select System Settings Restore.
- Enter the path and filename of the system settings file, or select Browse and locate the file.
- Select OK to restore the system settings file to the DFL-1000 NPG.
The DFL-1000 NPG 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 firmware version.



This procedure deletes all changes that you have made to the DFL-1000 NPG 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-1000 NPG restarts with the configuration that 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-1000 NPG.

Changing to Transparent mode

Use the following procedure if you want to switch the DFL-1000 NPG from NAT/Route mode to Transparent mode.



Changing to Transparent mode deletes all NAT/Route mode policies and addresses. In addition any routing set in NAT mode is also deleted. This includes the default route that is part of the default NAT/Route mode configuration.

- Go to *System > Status* .
- Select Change to Transparent Mode.
- Select Transparent in the operation mode list.
- Select OK.

The DFL-1000 NPG changes operation mode.

- To reconnect to the web-based manager, connect to the interface configured for Transparent mode management access and browse to https:// followed by the Transparent mode management IP address.

By default in Transparent mode, you can connect to the internal or DMZ interface. The default Transparent mode management IP address is 10.10.10.1. See [Configuring the management interface \(Transparent mode\)](#).

Changing to NAT/Route mode

Use the following procedure if you want to switch the DFL-1000 NPG from Transparent mode to NAT/Route mode.



Changing to NAT/Route mode deletes all Transparent mode policies and addresses. In addition any routing set in Transparent mode is also deleted. This includes the default route that is part of the default Transparent mode configuration.

- Go to *System > Status* .
- Select Change to NAT Mode.
- Select NAT/Route in the operation mode list.
- Select OK.

The DFL-1000 NPG 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.

Restarting the DFL-1000 NPG

Use the following procedure to restart the DFL-1000 NPG:

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

The DFL-1000 NPG restarts.

Shutting down the DFL-1000 NPG

Use the following procedure to shut down the DFL-1000 NPG:

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

The DFL-1000 NPG shuts down and all traffic flow stops.





The DFL-1000 NPG can only be restarted after shutdown by turning the power off, then on.

System status monitor

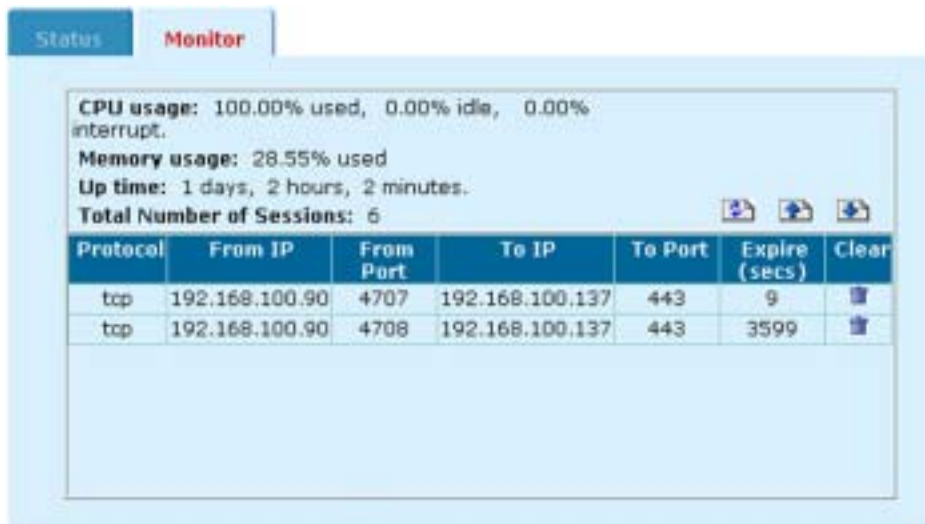
You can use the system status monitor to view system activity, including the number of active communication sessions and information about each session.

The system status monitor also displays DFL-1000 NPG CPU usage, memory usage, and system up-time statistics.

To view system status:

- Go to *System > Status > Monitor* .
The system status monitor appears.
- To page through the list of connections, select Page Up  or Page Down .
- Select Refresh  to update the information displayed.
- You can select Clear  to stop any active communication session.

System status monitor



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

CPU usage The current CPU usage statistics of the DFL-1000 NPG.

Memory usage The percentage of available memory being used by the DFL-1000 NPG.

Up time The number of days, hours, and minutes since the DFL-1000 NPG was last started.

Total Number of Sessions The total number of active communication sessions to and through the DFL-1000 NPG.

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.
- Clear** Stop and active communication session.


Network configuration

Go to **System > Network** to make any of the following changes to the DFL-1000 NPG network settings:

- [Configuring the internal interface](#)
- [Configuring the external interface](#)
- [Configuring the dmz interface](#)
- [Configuring the management interface \(Transparent mode\)](#)
- [Setting DNS server addresses](#)

Configuring the internal interface

To configure the internal interface:

- 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 and you are connecting to the internal interface to manage the DFL-1000 NPG, you must reconnect to the web-based manager using the new internal interface IP address.

Configuring the internal interface

The screenshot shows a configuration window titled "Edit Interface(00:50:C2:08:65:54)". The window has a tabbed interface with "Interface" selected. The configuration fields are as follows:

Name	internal
IP	192.168.100.137
Netmask	255.255.255.0
Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP


At the bottom of the window are two buttons: "OK" and "Cancel".

Configuring the external interface

Use the following procedures to configure the external interface:

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

Configuring the external interface with a static IP address

- 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 with a static IP address

The screenshot shows the 'Edit Interface' configuration window for the external interface. The window has tabs for 'Interface', 'DNS', 'Routing Table', 'Routing Gateway', and 'DHCP'. The 'Interface' tab is active. The title bar reads 'Edit Interface(00:50:C2:08:65:55)'. The configuration fields are: Name: 'external'; Addressing mode: 'Manual' (selected), 'DHCP', 'PPPoE'; IP: '5.5.5.5'; Netmask: '255.255.255.0'; Access: 'HTTPS' (unchecked), 'PING' (checked), 'SSH' (unchecked), 'SNMP' (unchecked); MTU: '1500' (bytes); and a checkbox for 'Fragment outgoing packets greater than MTU.' (unchecked). 'OK' and 'Cancel' buttons are at the bottom.

Configuring the external interface for DHCP

Use the following procedure to configure the external interface to use DHCP. This configuration is required if your ISP uses DHCP to assign the IP address of the 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 and select OK to change to DHCP mode. Both the IP address and Netmask change to 0.0.0.0.
- Select Enable Connect to DHCP server if you want the DFL-1000 NPG to automatically connect to a DHCP server when it starts up.
- Select OK.
The DFL-1000 NPG 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-1000 NPG gets this information from the DHCP server, the new addresses and netmask are displayed in the IP address and Netmask fields.

Configuring the external interface for PPPoE

Use the following procedure to configure the 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 and select OK to change to PPPoE mode.


- Enter your PPPoE account User name and Password.
- Select OK.

The DFL-1000 NPG attempts to contact the PPPoE server to set the external IP address, netmask, and default gateway IP address. When the DFL-1000 NPG gets this information from the PPPoE server, the new addresses and netmask are displayed in the external IP address and netmask fields. If the PPPoE connection with your ISP is dropped, the DFL-1000 NPG automatically attempts to re-establish the connection.

- Select Enable Connect to PPPoE server if you want the DFL-1000 NPG to automatically connect to a PPPoE server when it starts up.

Controlling management access to the external interface

Use the following procedure to control management access to the DFL-1000 NPG through the external interface. You can configure the DFL-1000 NPG 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-1000 NPG.

- Go to *System > Network > Interface* .
- For the external interface, select Modify .
- Select the management Access methods 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](#).

Selecting HTTPS for the external interface allows remote administration of the DFL-1000 NPG using the web-based manager from any location on the Internet. Selecting SSH for the external interface allows remote administration of the DFL-1000 NPG using the CLI from any location on the Internet. Selecting SNMP for the external interface allows remote SNMP management of the DFL-1000 NPG 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 the 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-1000 NPG 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-1000 NPG and the Internet. If the packets that the DFL-1000 NPG 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 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.



If the external interface is configured using PPPoE, MTU may be negotiated by the PPPoE protocol. If this is the case, the system may override manual MTU settings.

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 dmz interface

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

To configure the dmz interface:

- Go to *System > Network > Interface* .
- For the dmz interface, select Modify
- Change the IP address and Netmask as required.
- Select the management Access methods for the dmz interface.

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

PING If you want the dmz 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 dmz interface.

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

- Select OK to save your changes.

Configuring the management interface (Transparent mode)

In Transparent mode, you can configure the management interface for management access to the DFL-1000 NPG.

- Go to *System > Network > Management* .
- Change the Management IP and Mask as required.
These must be valid addresses for the network from which you will manage the DFL-1000 NPG.
- Select the management Access methods for each interface.
By default in Transparent mode, you manage the DFL-1000 NPG by connecting to the internal or dmz interface. However, you can configure the management interface so that you can manage the DFL-1000 NPG by connecting to any interface.

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

PING If you want this 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 this interface.

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

- Select Apply to save your changes.

Configuring the management interface (Transparent mode)

Management IP:

IP Mask

Access:

internal	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
external	<input type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
dmz	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP

Setting DNS server addresses

Several DFL-1000 NPG functions, including sending email alerts and URL blocking, use DNS.

To set the DNS server addresses:

- Go to *System > Network > DNS*.
- Change the primary and secondary DNS server addresses as required.
- Select Apply to save your changes.

Configuring routing

This section describes how to configure DFL-1000 NPG routing. You can configure routing to add static routes from the DFL-1000 NPG to local routers. You can also use routing to add multiple routing gateways and create a multiple WAN configuration that supports redundancy and load sharing between two Internet connections.

- [Adding routing gateways](#)
- [Adding a default route](#)
- [Adding routes to the routing table](#)
- [Configuring the routing table](#)
- [Enabling RIP server support](#)
- [Adding routes \(Transparent mode\)](#)
- [Configuring the DFL-1000 NPG for multiple Internet connections](#)

Adding routing gateways

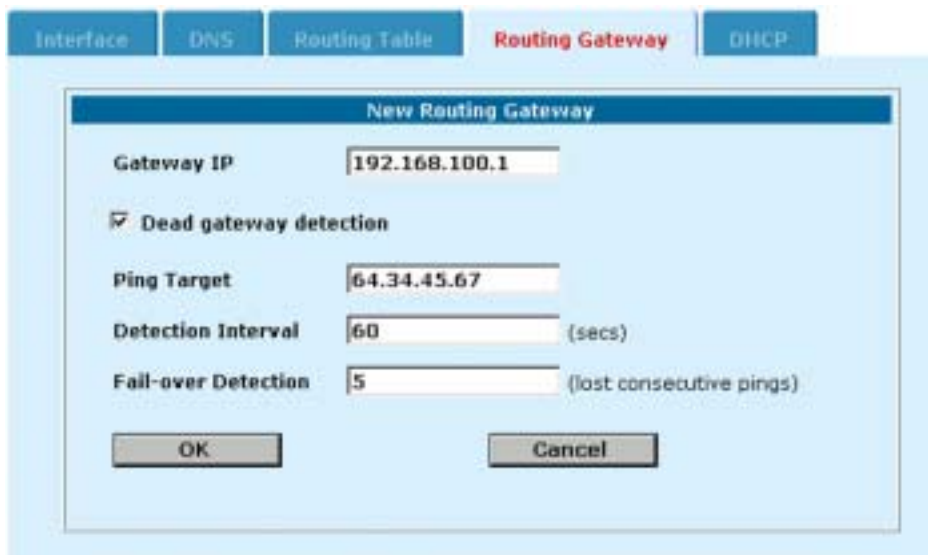
The first step in configuring DFL-1000 NPG routing is to add routing gateways. Routing gateways are the gateways on your network that you want to route DFL-1000 NPG traffic to. You can add the IP address of each routing gateway, and you can also optionally configure the DFL-1000 NPG to ping the routing

gateway at a specified time interval to make sure that the DFL-1000 NPG can communicate with the routing gateway.

To add a routing gateway:

- Go to *System > Network > Routing Gateway* .
- Select New to add a new routing gateway.
- Enter the IP address of the routing gateway.
This IP address should be on the same subnet as the DFL-1000 NPG interface that connects to this gateway.
- Select Dead gateway detection if you want the DFL-1000 NPG to confirm connectivity with the gateway.
If you select dead gateway detection you can also configure ping target, detection interval, and fail-over detection for the routing gateway.

Adding a routing gateway



- Set Ping Target to the IP address that the DFL-1000 NPG should ping to test connectivity with the gateway.
The ping target could be the IP address of the gateway, but it is more useful if it is the IP address of a server on the other side of the gateway that will respond to pings in a reliable manner.
- Set Detection Interval to specify how often the DFL-1000 NPG tests the connection to the ping target.
- Set Fail-over Detection to the number of times that the connection test fails before the DFL-1000 NPG assumes that the gateway is no longer functioning.
- Select OK to save the routing gateway.
- Repeat this procedure to add all the routing gateways that you require.

Adding a default route

Use the following procedure to add a default route for network traffic leaving the external interface.

- Go to **System > Network > Routing Table** .
- Select New to add a new route.
- Set the Source IP and Netmask to 0.0.0.0.
- Set the Destination IP and Netmask to 0.0.0.0.
- Set Gateway 1 to the IP address of the routing gateway that routes traffic to the Internet.



If you are adding a default route (source and destination IPs and netmasks set to 0.0.0.0), you do not have to use the procedure [Adding routing gateways](#) to add this routing gateway.

- Select OK to save the default route.

Adding routes to the routing table

When you have added routing gateways, you can use the following procedure to add routes to them. Add routes to determine the path that data follows from the DFL-1000 NPG to routing gateways and other networks.

- Go to **System > Network > Routing Table** .
- Select New to add a new route.
- Type the Source IP address and Netmask for the route.
- Type the Destination IP address and Netmask for the route.
- Add the IP addresses of up to four gateways.



The IP addresses that you add must match the IP addresses of the routing gateways added using the procedure [Adding routing gateways](#).

If you are adding a static route from the DFL-1000 NPG to a single destination router, only specify one gateway.

You can add multiple gateways if you have multiple gateways connecting to the same network. You might have multiple gateways for redundancy or for load sharing.

- Select OK to save the new route.





Arrange routes in the routing table from more specific to more general. To arrange routes in the routing table, see [Configuring the routing table](#).

Configuring the routing table

As you add routes, they appear on the routing table. The routing table shows the source and destination addresses of each route as well as the gateways added to the route. For each gateway, the routing table displays the gateway connection status. A green check mark indicates that the DFL-1000 can connect to the gateway; a red X means that a connection cannot be established. A blue question mark means that the connection status is unknown.

The DFL-1000 NPG assigns routes by searching for a match starting at the top of the routing table and moving down until it finds the first match. You must arrange routes in the routing table from more specific to more general. The default route is the most general route. If you add a default route, it should be at the bottom of the routing table.

- Go to **System > Network > Routing Table** .
- Choose a route to move and select Move to  to change its order in the routing table.
- Type a number in the Move to field to specify where in the routing table to move the route and select OK.
- Select Delete  to remove a route from the routing table.

Routing table

Source IP/Mask	Destination IP/Mask	Gateway #1	Gateway #2	Gateway #3	Gateway #4	Modify
10.10.10.1/255.255.255.0	0.0.0.0/0.0.0.0	192.168.100.1				
192.168.1.1/255.255.255.0	0.0.0.0/0.0.0.0	192.168.100.1	192.168.100.3			
0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	192.168.100.1				

Enabling RIP server support

Enable routing information protocol (RIP) server support to configure the DFL-1000 NPG to act like a RIP server. The RIP routing protocol maintains up-to-date dynamic routing tables between nearby routers. When you enable RIP server support, the DFL-1000 NPG 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 RIP server is going online (RIP server turned on) and requesting updates,
- announce that the RIP server is shutting down and will stop sharing routing information.

To enable RIP server support:

- Go to **System > Network > Routing Table**.
- Select Enable RIP Server.

Adding routes (Transparent mode)

Use the following procedure to add routes when running the DFL-1000 NPG in Transparent mode.

- Go to **System > Network > Routing**.
- Select New to add a new route.
- Enter the Destination IP address and Netmask for the route.
- Enter the Gateway IP address for the route.
- Select OK to save the new route.
- Repeat these steps to add more routes as required.

Configuring the DFL-1000 NPG for multiple Internet connections

You can use routing to configure the DFL-1000 NPG with two Internet or WAN connections. Using this multiple WAN configuration, if one of these WAN connections fails, the DFL-1000 NPG routes all packets to the other WAN connection.

Example multiple Internet connection configuration



For example, your main connection to the Internet could be a T1 or broadband connection to the external interface. To make sure that problems with this Internet connection do not affect your access to the Internet, you could add a second T1 or broadband connection, perhaps with a different ISP. You can connect this second Internet connection to the DMZ interface. You can then configure routing so that incoming and outgoing traffic is automatically routed to the WAN connection that is running. You can also configure routing to balance the traffic between both connections if both are running.

Example configuration

This example configuration consists of a T1 WAN connection to the external interface and a broadband WAN connection to the DMZ interface. The WAN networks have the following IP addresses:

Example multiple Internet connection configuration	
External interface	15.1.2.99
T1 gateway connected to external interface	15.1.2.1
DMZ interface	16.1.2.99
Broadband gateway connected to DMZ interface	16.1.2.1
Internal interface	192.168.1.99

Configuring routing for multiple Internet connections

- Configure the external, DMZ, and internal interface addresses as listed in [Example multiple Internet connection configuration](#).
- Use the procedure [Adding routing gateways](#) to add the T1 gateway and the broadband gateways to the routing gateway list.
- Use the procedure [Adding routes to the routing table](#) to add routes to the routing table. You can add routes to support redundancy and load balancing.

Adding a route for redundancy

Add the route listed in [Adding routes for redundancy](#) to support redundancy between the two example WAN connections. This route includes two destination gateways.

Adding routes for redundancy			
Source IP/MASK	Destination IP/MASK	Gateway 1	Gateway 2
192.168.1.1/255.255.255.0	0.0.0.0/0.0.0.0	15.1.2.1	16.1.2.1

When the first gateway is running (the T1 gateway, IP address 15.1.2.1), the DFL-1000 NPG routes all traffic from the internal network (IP address 192.168.1.1) to this gateway. If the first gateway goes down, the DFL-1000 NPG routes all traffic to the second gateway (the broadband gateway, IP address 16.1.2.1).

Adding routes for load balancing

You can add routes to the routing table to define routing based on the source and destination IP address and netmask. Using this technique, you can add routes that send traffic from some source addresses to one gateway, and traffic from other source addresses to the other gateway.

Using the routing configuration in [Adding routes for load balancing](#), if both gateways are running, traffic from IP addresses 192.168.1.1 to 192.168.1.7 goes to the T1 gateway (IP address 15.1.2.1). All other traffic from the 192.168.1.0 subnet goes to the broadband gateway (16.1.2.1). In both routes, if gateway 1 goes down, the DFL-1000 NPG re-routes the traffic to gateway 2.

Adding routes for load balancing			
Source IP/MASK	Destination IP/MASK	Gateway 1	Gateway 2
192.168.1.1/255.255.255.248	0.0.0.0/0.0.0.0	15.1.2.1	16.1.2.1
192.168.1.1/255.255.255.0	0.0.0.0/0.0.0.0	16.1.2.1	15.1.2.1

Providing DHCP services to your internal network

If the DFL-1000 NPG is operating in NAT/Route mode, you can configure it to be the DHCP server for your internal network:

- Go to *System > Network > DHCP*.
- Select Enable DHCP.
- Configure the DHCP settings:

Starting IP Enter Starting IP and the Ending IP to configure the range of IP addresses that the DFL-1000 NPG can assign to DHCP clients. The addresses must be addresses on your internal network.

Ending IP Enter the Ending IP to configure the range of IP addresses that the DFL-1000 NPG can assign to DHCP clients. The addresses must be addresses on your internal network.

Netmask Enter the Netmask that the DFL-1000 NPG assigns to the DHCP clients.

Lease Duration Enter the interval in seconds after which a DHCP client must ask the DHCP server for a new address. The lease duration must be between 300 and 604800 seconds.

- Domain** Optionally enter in the domain that the DHCP server assigns to the DHCP clients.
- DNS IP** Enter the IP addresses of up to 3 DNS servers that the DHCP clients can use for looking up domain names.
- Default Route** Enter the default route to be assigned to DHCP clients. The default route should be on the same subnet as the Starting and Ending IP addresses.
- Exclusion Range** Optionally enter up to 4 exclusion ranges of IP addresses within the starting IP and ending IP addresses that cannot be assigned to DHCP clients.

- Select Apply.
- Configure the IP network settings of the computers on your network to obtain an IP address automatically using DHCP.

Example DHCP settings

The screenshot shows the DHCP configuration page with the following settings:

- Enable DHCP:**
- Starting IP:** 192.168.100.1
- Ending IP:** 192.168.100.98
- Netmask:** 255.255.255.0
- Lease Duration:** 1140 (seconds)
- Domain:** Fortinet.com
- DNS IP:** 192.168.100.5, 192.168.100.98
- Default Route:** 192.168.100.1
- Exclusion Range:**
 - Range 1: 192.168.100.5 - 192.168.100.10
 - Range 2: (empty)
 - Range 3: (empty)
 - Range 4: (empty)

Buttons for 'Dynamic IP List' and 'Apply' are visible.

Viewing the dynamic IP list

If you have configured your DFL-1000 NPG as a DHCP server, you can view a list of IP addresses that the DHCP server has added, their corresponding MAC addresses, and the expiry time and date for these addresses. The DFL-1000 NPG adds these addresses to the dynamic IP/MAC list and if IP/MAC binding is enabled, the addresses in the dynamic IP/MAC list are added to the list of trusted IP/MAC address pairs. For more information about IP/MAC binding, see [IP/MAC binding](#).

To view the dynamic IP list:

- Go to *System > Network > DHCP* .
- Select Dynamic IP List.
The dynamic IP list appears.

Example date and time setting

The screenshot shows the 'Time' configuration page in the DFL-1000 NPG web-based manager. The page has a navigation bar with 'Time', 'Options', 'Admin', and 'SNMP' tabs. The 'Time' tab is active. The configuration area includes:

- System Time:** A text field showing 'Thu Jul 3 11:34:19 2003' and a 'Refresh' button.
- Time Zone:** A dropdown menu set to '(GMT-8:00)Pacific Time(US&Canada)'.
- Daylight Saving Time:** An unchecked checkbox.
- Set Time:** A radio button that is selected, followed by dropdown menus for Hour (11), Minute (34), Second (19), Month (Jul), Day (3), and Year (2003).
- Synchronize with NTP Server:** An unchecked radio button.
- Server:** A text field containing '132.246.168.148'.
- Syn Interval:** A text field containing '60' with '(mins)' next to it.
- Apply:** A button at the bottom.

- To configure the DFL-1000 NPG to use NTP, select Synchronize with NTP Server. By default, the DFL-1000 NPG 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-1000 NPG should synchronize its time with the NTP server. A typical Syn Interval would be 1440 minutes for the DFL-1000 NPG to synchronize its time once a day.
- Select Apply.

Changing web-based manager options

You can change the web-based manager idle time out and firewall user authentication time out. 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 Idle Timeout 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 Timeout is 15 minutes. The maximum Auth Timeout is 480 minutes (8 hours).
- Choose the character set and language that the web-based manager uses.
You can choose from English, Simplified Chinese, Japanese, Korean, or Traditional Chinese.



When the web-based manager language is set to use Simplified Chinese, Japanese, Korean, or Traditional Chinese, you can change to English by selecting the English button on the upper right of the web-based manager.

- Select Apply.

The options that you have selected take effect.

Adding and editing administrator accounts

When the DFL-1000 NPG 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-1000 NPG.

There are three administration account access levels:

admin	Has all permissions. Can view, add, edit, and delete administrator accounts. Can view and change the configuration. The admin user is the only user who can go to System > Status and manually update firmware, download or upload system settings, restore the DFL-1000 NPG to factory defaults, restart the DFL-1000 NPG, and shut down the DFL-1000 NPG. There is only one admin-level user.
Read & Write	Can view and change the configuration. Can view but cannot add, edit, or delete administrator accounts. Can change own administrator account password. Cannot make changes to system settings from the System > Status page.
Read Only	Can view the configuration.

Adding new administrator accounts

From the admin account, use the following procedure to add new administrator accounts to the DFL-1000 NPG 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), uppercase and lowercase 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), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . Other special characters and spaces are not allowed.
- Optionally type a Trusted Host IP address and netmask 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-1000 NPG 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 be able to access the DFL-1000 NPG from a specific network, set the trusted host to the address of the network and set the wildcard mask to the netmask for the network. For example, to limit an administrator to accessing the DFL-1000 NPG from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the wildcard mask to 255.255.255.0.
- Set the Permission level for the administrator.
- 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 permission levels.

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 the Old 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), uppercase and lowercase 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 netmask 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-1000 NPG 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 be able to access the DFL-1000 NPG from a specific network, set the trusted host to the address of the network and set the wildcard mask to the netmask for the network. For example, to limit an administrator to accessing the DFL-1000 NPG from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the wildcard mask to 255.255.255.0.
- Change the administrator's permission level as required.
- Select OK.
- To delete an administrator account, choose the account to delete and select Delete .

Configuring SNMP

Configure SNMP for the DFL-1000 NPG so that the SNMP agent running on the DFL-1000 NPG can report system information and send traps. The DFL-1000 agent supports SNMP v1 and v2c. System information can be monitored by any SNMP manager configured to get system information from your DFL-1000 NPG. Your SNMP manager can use GET (GET-NEXT) SNMP operations to communicate with the DFL-1000 agent.

Configuring the DFL-1000 NPG for SNMP connections

Before a remote SNMP manager can connect to the DFL-1000 SNMP agent, you must configure one or more interfaces to accept SNMP connections. For information about how to do this, see [Configuring the internal interface](#) and related interface configuration sections.

Configuring SNMP

- Go to *System > Config > SNMP* .
- Select Enable SNMP.
- Configure SNMP settings:

System Name	Type a name for this DFL-1000 NPG. The system name can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase 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-1000 NPG. The system location description can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase 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-1000 NPG. The contact information can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _ . The \ < > [] ` \$ % & characters are not allowed.

Also called read community, get community is a password to identify SNMP get requests sent to the DFL-1000 NPG. When an SNMP manager sends a get request to the DFL-1000 NPG, it must include the correct get community string.

Get Community

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-1000 NPG SNMP information.

The get community string can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and the \ < > [] ` \$ % & characters are not allowed.

The trap community string functions like a password that is sent with SNMP traps.

Trap Community

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 numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and the \ < > [] ` \$ % & characters are not allowed.

Trap Receiver IP Addresses

Type the IP addresses of up to three trap receivers on your network that are configured to receive traps from your DFL-1000 NPG. Traps are only sent to the configured addresses.

- Select Apply.

Example SNMP configuration

The screenshot shows a web-based configuration interface for SNMP. At the top, there are four tabs: "Time", "Options", "Admin", and "SNMP" (which is highlighted in red). Below the tabs is a light blue box containing the configuration fields. The 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:	192.33.44.55
Second Trap Receiver IP Address:	143.44.52.78
Third Trap Receiver IP Address:	

At the bottom of the configuration box is an "Apply" button.

DFL-1000 MIBs

The DFL-1000 agent supports the standard Internet MIB-II System Group (RFC-1213) for reporting basic system information. The agent also supports a DFL-1000 MIB that reports firewall and VPN information. [Example DFL-1000 MIB fields](#) shows the system and DFL-1000 MIB fields.

You must compile the following MIBs in your SNMP manager to communicate with the DFL-1000 agent:

- FN-FIREWALL.mib** D-Link firewall MIB that collects all firewall policy information.
- FN-SMI.mib** Defines the private UCD SNMP MIB extensions.
- FN-SYSTEM.mib** D-Link system MIB that collects all system information.
- FN-VPN.mib** D-Link VPN MIB that collects all VPN configuration information.

You can download copies of these MIB files from D-Link.

Example DFL-1000 MIB fields	
Branch	Definitions
Firewall	Policy Address Service Schedule User Virtual IP IP/Mac Binding
System	Status Operation Mode Firmware Version Serial Number
	Network DNS Routing DHCP
	Configuration
VPN	IPSEC PPTP L2TP

DFL-1000 traps

The DFL-1000 agent can send traps to up to three SNMP trap receivers on your network that are configured to receive traps from the DFL-1000 NPG. The DFL-1000 agent sends traps in response to the events listed in [SNMP traps](#).

SNMP traps	
Event	Description
System Startup	The DFL-1000 NPG starts or restarts.
Invalid Community	The SNMP agent has received an SNMP request with an invalid community string.
System Shutdown	The DFL-1000 NPG 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.

Glossary

Connection : A link between machines, applications, processes, and so on that can be logical, physical, or both.

DMZ, Demilitarized Zone : Used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

DMZ interface : The DFL-1000 interface that is connected to your DMZ network.

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-1000 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-1000 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.

Troubleshooting FAQs

- [General administration](#)
- [Network configuration](#)
- [Firewall policies](#)
- [Schedules](#)
- [VPN](#)
- [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 internal interface](#).

Q: Everyone in the world knows the password.

Change the administrator password. See [Adding and editing administrator accounts](#).

Q: I have the DFL-1000 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](#).

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-1000.

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 [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 policy for public access to a server](#)
- [Routing policy for access to a server from the internal network](#)
- [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.

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 [Blocking access to URLs](#) 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 [Removing scripts from web pages](#).

Logging

Q: Our web site is on a computer on the DMZ network. How can I tell how many people look at it?

Select Log Traffic for all Ext to DMZ firewall policies that provide access to the web site.

Q: How can I find out which company employees are spending time on the Internet?

Select Log Traffic for all Int -> Ext firewall policies that provide users on the internal network with access to the Internet.

Q: How can I record DFL-1000 logs on a remote computer, such as a management computer?

You can send DFL-1000 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 Fellensord 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://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 Thli-ja Pakkahuone Katajanokanlaituri 5, FIN-00160 Helsinki, Finland TEL: 358-9-622-91660 FAX: 358-9-622-91661 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 Schwalbacher 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, 3º 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: kjda@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: vl@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: dssng@tse.dlinktw.com.tw URL: www.dlinktw.com.tw
U.K.	D-LINK EUROPE 4th 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: 1-949-789-0805 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>
