

# **D-Link DFL-700**

**Network Security Firewall**

**Manual**

**D-Link<sup>®</sup>**

**Building Networks for People**

(05/18/2004)

# Contents

<b>Introduction .....</b>	<b>6</b>
Features and Benefits .....	6
Introduction to Firewalls .....	6
Introduction to Local Area Networking .....	7
LEDs .....	8
Physical Connections .....	8
Package Contents .....	9
System Requirements .....	9
<b>Managing D-Link DFL-700 .....</b>	<b>10</b>
Resetting the DFL-700 .....	10
<b>Administration Settings .....</b>	<b>11</b>
Administrative Access .....	11
Add ping access to an interface .....	12
Add Admin access to an interface .....	12
Add Read-only access to an interface .....	13
Enable SNMP access to an interface .....	13
<b>System .....</b>	<b>14</b>
Interfaces .....	14
Change IP of the LAN or DMZ interface .....	14
WAN Interface Settings – Using Static IP .....	15
WAN Interface Settings – Using DHCP .....	15
WAN Interface Settings – Using PPPoE .....	16
WAN Interface Settings – Using PPTP .....	17
WAN Interface Settings – Using BigPond .....	18
Traffic Shaping .....	18
MTU Configuration .....	19
Routing .....	20
Add a new Static Route .....	21
Remove a Static Route .....	21
Logging .....	22
Enable Logging .....	23
Enable Audit Logging .....	23
Enable E-mail alerting for IDS/IDP events .....	23
Time .....	24
Changing time zone .....	25
Using NTP to sync time .....	25

Setting time and date manually.....	25
-------------------------------------	----

## **Firewall..... 26**

Policy.....	26
Policy modes.....	26
Action Types.....	26
Source and Destination Filter.....	27
Service Filter.....	27
Schedule.....	27
Intrusion Detection / Prevention.....	27
Traffic Shaping.....	28
Add a new policy.....	29
Change order of policy.....	30
Delete policy.....	30
Configure Intrusion Detection.....	30
Configure Intrusion Prevention.....	31
Port mapping / Virtual Servers.....	32
Add a new mapping.....	32
Delete mapping.....	33
Administrative users.....	34
Add Administrative User.....	34
Change Administrative User Access level.....	35
Change Administrative User Password.....	35
Delete Administrative User.....	36
Users.....	37
The DFL-700 RADIUS Support.....	37
Enable User Authentication via HTTP / HTTPS.....	38
Enable RADIUS Support.....	38
Add User.....	39
Change User Password.....	39
Delete User.....	40
Schedules.....	41
Add new recurring schedule.....	41
Add new one-time schedule.....	42
Services.....	43
Adding TCP, UDP or TCP/UDP Service.....	43
Adding IP Protocol.....	44
Grouping Services.....	44
Protocol-independent settings.....	45
VPN.....	46
IPSec VPN between two networks.....	47
Creating a LAN-to-LAN VPN Tunnel.....	47
IPSec VPN between client and an internal network.....	48
Creating a Roaming Users Tunnel.....	48
VPN – Advanced Settings.....	49
Limit MTU.....	49

IKE Mode .....	49
IKE DH Group .....	49
PFS – Perfect Forward Secrecy .....	49
NAT Traversal .....	49
Keepalives.....	49
Proposal Lists.....	50
IKE Proposal List.....	50
IPSec Proposal List.....	50
Certificates .....	51
Trusting Certificates .....	51
Local identities .....	51
Certificates of remote peers.....	51
Certificate Authorities .....	51
Identities.....	52
Content Filtering .....	53
Edit the URL Global Whitelist.....	53
Edit the URL Global Blacklist .....	54
Active content handling.....	55
<b>Servers.....</b>	<b>56</b>
DHCP Server Settings.....	56
Enable DHCP Server .....	57
Enable DHCP Relay.....	57
Disable DHCP Server/Relayer.....	57
DNS Relay Settings .....	58
Enable DNS Relay.....	58
Disable DNS Relay.....	59
<b>Tools.....</b>	<b>60</b>
Ping .....	60
Ping Example.....	60
Dynamic DNS.....	61
Add Dynamic DNS Settings .....	61
Backup .....	62
Exporting the DFL-700's Configuration.....	62
Restoring the DFL-700's Configuration.....	62
Restart/Reset .....	63
Restarting the DFL-700.....	63
Restoring system settings to factory defaults .....	63
Upgrade .....	65
Upgrade Firmware .....	65
Upgrade IDS Signature-database.....	65
<b>Status .....</b>	<b>66</b>

System .....	66
Interfaces .....	67
VPN .....	68
Connections .....	69
DHCP Server .....	70

**How to read the logs..... 71**

USAGE events .....	71
DROP events .....	71
CONN events .....	71

**Appendixes..... 73**

Appendix A: ICMP Types and Codes .....	73
Appendix B: Common IP Protocol Numbers .....	75

# Introduction

The DFL-700 provides three 10/100M Ethernet network interface ports, which are (1) Internal/LAN, (1) External/WAN, and (1) DMZ port. It also provides easily operated software WebUI that allows users to set system parameters or monitor network activities using a Web browser.

## Features and Benefits

- **Firewall Security**
- **VPN Server/Client Supported**
- **Content Filtering**
- **Bandwidth Management**  
The DFL-700 features an extensive Traffic Shaper for bandwidth management.
- **Web Management**  
Configurable through any networked computer's Web browser using Netscape or Internet Explorer.
- **Access Control supported**  
Allows you to assign different access rights for different users, such as Admin or Read-Only User.

## Introduction to Firewalls

A firewall is a device that sits between your computer and the Internet that prevents unauthorized access to or from your network. A firewall can be a computer using firewall software or a special piece of hardware built specifically to act as a firewall. In most circumstances, a firewall is used to prevent unauthorized Internet users from accessing private networks or corporate LAN's and Intranets.

A firewall monitors all of the information moving to and from your network and analyzes each piece of data. Each piece of data is then checked against a set of criteria configured by the administrator. If any data does not meet the criteria, that data is blocked and discarded. If the data meets the criteria, the data is passed through. This method is called packet filtering.

A firewall can also run specific security functions based on the type of application or type of port that is being used. For example, a firewall can be configured to work with an FTP or Telnet server. Or a firewall can be configured to work with specific UDP or TCP ports to allow certain applications or games to work properly over the Internet.

## **Introduction to Local Area Networking**

Local Area Networking (LAN) is the term used when connecting several computers together over a small area such as a building or group of buildings. LANs can be connected over large areas. A collection of LANs connected over a large area is called a Wide Area Network (WAN).

A LAN consists of multiple computers connected to each other. There are many types of media that can connect computers together. The most common media is CAT5 cable (UTP or STP twisted pair wire.) On the other hand, wireless networks do not use wires; instead they communicate over radio waves. Each computer must have a Network Interface Card (NIC), which communicates the data between computers. A NIC is usually a 10Mbps network card, or 10/100Mbps network card, or a wireless network card.

Most networks use hardware devices such as hubs or switches that each cable can be connected to in order to continue the connection between computers. A hub simply takes any data arriving through each port and forwards the data to all other ports. A switch is more sophisticated, in that a switch can determine the destination port for a specific piece of data. A switch minimizes network traffic overhead and speeds up the communication over a network.

Networks take some time in order to plan and implement correctly. There are many ways to configure your network. You may want to take some time to determine the best network set-up for your needs.

## LEDs



**Power:** A solid light indicates a proper connection to the power supply.

**Status:** A System status indicator that flashes to indicate an active system. If the LED has a solid light, the unit is defective.

**WAN, LAN, & DMZ:** Ethernet port indicators that light green. The LED flickers when the ports are sending or receiving data.

## Physical Connections



**COM Port:** Serial access to the firewall software, 9600, 8bit, None Parity, 1Stop bit.

**DMZ Port:** Use this port to connect to the company's server(s), which needs direct connection to the Internet (FTP, SNMP, HTTP, DNS).

**Internal Ports (LAN):** Use this port to connect to the internal network of the office.

**External Port (WAN):** Use this port to connect to the external router, DSL modem, or Cable modem.

**Reset:** Use to reset the DFL-700 to the original default settings.

**DC Power:** Connect one end of the power supply to this port, the other end to the electrical wall outlet.

## Package Contents



Contents of Package:

- **D-Link DFL-700 Firewall**
- Manual and CD
- Quick Installation Guide
- 5V/3A AC Power adapter
- Straight-through CAT-5 cable

*Note: Using a power supply with a different voltage rating than the one included with the DFL-700 will cause damage and void the warranty for this product.*

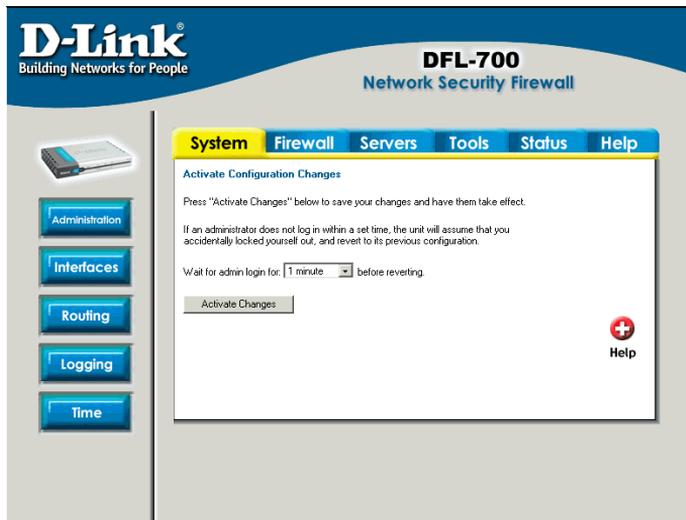
If any of the above items are missing, please contact your reseller.

## System Requirements

- Computer with a Windows, Macintosh, or Unix based operating system with an installed Ethernet adapter.
- Internet Explorer or Netscape Navigator, version 6.0 or above, with JavaScript enabled.

# Managing D-Link DFL-700

When a change is made to the configuration, a new icon named **Activate Changes** will appear. When all changes made by the administrator are done, the changes need to be saved and activated to take effect by clicking on the Activate Changes button on the Activate Configuration Changes page. The firewall will save the configuration and reload it, making the new changes take effect. In order to make the changes permanent, the administrator must login again. This has to be done before a configurable timeout has been reached. This can be set on the Activate Configuration Changes page, by choosing the time from the dropdown menu.



This has to be done before a configurable timeout has been reached. This can be set on the Activate Configuration Changes page, by choosing the time from the dropdown menu.

## Resetting the DFL-700

To reset the DFL-700 to factory default settings you must hold the reset button down for at least 15 seconds after powering on the unit. You will first hear one beep, which will indicate that the firmware is being restored. Keep the button pressed in until you hear two short consecutive beeps. After this you can release the reset button and the DFL-700 will continue to load and startup in default mode, i.e. with 192.168.1.1 on the LAN interface.

# Administration Settings

## Administrative Access

### Administration Settings

Select the interface / user you wish to edit from the below list.

Note that both the user settings and the interface settings limit what a user can do, so if e.g. a full admin user logs on via an interface that only allows "read-only" access, the user will be allowed to log on, but will receive read-only access only.

#### Administrative users

**Admin:** [admin](#) [\[Add\]](#)

**Read-only:** [auditor](#) [\[Add\]](#)

#### Administrative access via LAN interface [\[Edit\]](#)

**Ping:** 1.0.0.0 - 223.255.255.255

**Admin:** 1.0.0.0 - 223.255.255.255 (HTTPS only)

**Read-only:** 1.0.0.0 - 223.255.255.255 (HTTP + HTTPS)

**SNMP:** 1.0.0.0 - 223.255.255.255  
Read Community: "MySecretCommunity"

#### Administrative access via DMZ interface [\[Edit\]](#)

**Ping:** 1.0.0.0 - 223.255.255.255

**SNMP:** 1.0.0.0 - 223.255.255.255  
Read Community: "public"

#### Add administrative access via:

**Interface:** [WAN](#)

**VPN Tunnel:** [lantolan1](#), [lantolan2](#), [roaminusers](#)

**Ping** – If enabled, it specifies who can ping the IP interface of the DFL-700. Enabling Default allows anyone to ping the interface IP.

**Admin** – If enabled, it allows all users with admin access to connect to the DFL-700 and change configuration; this can be **HTTPS** or **HTTP and HTTPS**.

**Read-Only** – If enabled, it allows all users with read-only access to connect to the DFL-700 and look at the configuration; this can be **HTTPS** or **HTTP and HTTPS**. If there is no Admin access specified on an interface and only read-only, admin users can still connect but will be in read-only mode.

**SNMP** – Specifies if SNMP should or should not be allowed on the interface. The DFL-700 only supports read-only access.

## Add ping access to an interface

To add ping access click on the interface you would like to add it to.

Follow these steps to add ping access to an interface.

**Step 1.** Click on the interface you would like to add it to.

**Step 2.** Enable the **Ping** checkbox.

**Step 3.** Specify which networks are allowed to ping the interface, for example 192.168.1.0/24 for a whole network or 172.16.0.1 – 172.16.0.10 for a range.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

Example:

**Ping** - standard ICMP echo to the IP address of the interface

Networks:

## Add Admin access to an interface

To add admin access, click on the interface you would like to add it to. Only users with administrator rights can login on interfaces where there is only admin access enabled.

Follow these steps to add admin access to an interface.

**Step 1.** Click on the interface you would like to add it to.

**Step 2.** Enable the **Admin** checkbox.

**Step 3.** Specify which networks are allowed to access the interface, for example 192.168.1.0/24 for a whole network or 172.16.0.1 – 172.16.0.10 for a range.

**Step 4.** Specify protocol used to access the DFL-700 from the dropdown menu, either HTTP and HTTPS (Secure HTTP) or only HTTPS.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

Example:

**Admin** - Full access to web-based management

Networks:

Protocol:

## Add Read-only access to an interface

To add read-only access, click on the interface you would like to add it to. Note that if you only have read-only access enabled on an interface, all users will only have read-only access, even if they are administrators.

Follow these steps to add read-only access to an interface.

**Step 1.** Click on the interface you would like to add it to.

**Step 2.** Enable the **Read-only** checkbox.

**Step 3.** Specify which networks are allowed read-only access to the interface, for example 192.168.1.0/24 for a whole network or 172.16.0.1 – 172.16.0.10 for a range.

**Step 4.** Specify protocol used to access the DFL-700 from the dropdown menu, either HTTP and HTTPS (Secure HTTP) or only HTTPS.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

Example:

**Read-only** - Read-only access to web-based management

Networks:

Protocol:

## Enable SNMP access to an interface

Follow these steps to add read-only SNMP access to an interface.

**Step 1.** Click on the interface you would like to add it to.

**Step 2.** Enable the **Read-only** checkbox.

**Step 3.** Specify which networks are allowed to receive SNMP traps, for example 192.168.1.0/24 for a whole network or 172.16.0.1 – 172.16.0.10 for a range.

**Step 4.** Specify the community string used to authenticate the DFL-700.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

Example:

**SNMP** - Simple Network Management Protocol (read-only access)

Networks:

Community:

# System

## Interfaces

Click on **System** in the menu bar, and then click **interfaces** below it.

### Change IP of the LAN or DMZ interface

Follow these steps to change the IP of the LAN or DMZ interface.

#### Interface Settings

Edit settings of the **LAN** interface:

IP Address:

Subnet Mask:  - 256 hosts (/24)

**Step 1.** Choose which interface to view or change under the Available interfaces list.

**Step 2.** Fill in the IP address of the **LAN** or **DMZ** interface. These are the addresses that will be used to ping the firewall, remotely control it, and used as the gateway for the internal hosts or DMZ hosts.

**Step 3.** Choose the correct Subnet mask of this interface from the drop down menu.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## WAN Interface Settings – Using Static IP

If you are using **Static IP**, you have to fill in the IP address information provided to you by your ISP. All fields are required except the Secondary DNS Server. Note: Do not use the numbers displayed in these fields, they are only used as an example.

- **IP Address** – The IP address of the **WAN** interface. This is the address that may be used to ping the firewall, remotely control it, and be used as the source address for dynamically translated connections.
- **Subnet Mask** – Size of the external network.
- **Gateway IP** – Specifies the IP address of the default gateway used to access the Internet.
- **Primary and Secondary DNS Server** – The IP addresses of your DNS servers; only the Primary DNS is required.

### Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type:

Static WAN interface configuration is most commonly used in dedicated-line internet connections. Your ISP usually provides this information to you.

IP Address:

Subnet Mask:  .256 hosts (/24)

Gateway IP:

Primary DNS Server:

Secondary DNS Server:  (optional)

## WAN Interface Settings – Using DHCP

If you are using **DHCP**, there is no need to complete any fields.

### Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type:

Regular ethernet connection with DHCP-assigned IP addresses is used in many DSL and cable modem networks. Everything is automatic.

## WAN Interface Settings – Using PPPoE

Use the following procedure to configure the DFL-700 external interface to use PPPoE (Point-to-Point Protocol over Ethernet). This configuration is required if your ISP uses PPPoE to assign the IP address of the external interface. You will have to fill in the username and password provided to you by your ISP.

- **Username** – The login or username supplied to you by your ISP.
- **Password** – The password supplied to you by your ISP.
- **Service Name** – When using PPPoE some ISPs require you to fill in a Service Name.
- **Primary and Secondary DNS Server** – The IP addresses of your DNS servers; these are optional and are often provided by the PPPoE service.

**Interface Settings**

Edit settings of the **WAN** interface:

Change WAN Type:

PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.

Username:

Password:

Retype Password:

Service Name:

(Some ISPs require the Service Name to be filled out.)

Most PPPoE services provide DNS server information. A few do not. If this is the case, you can fill out their IP addresses yourself.

Primary DNS Server:  (optional)

Secondary DNS Server:  (optional)

## WAN Interface Settings – Using PPTP

PPTP over Ethernet connections are used in some DSL and cable modem networks.

You need to enter your account details, and possibly also IP configuration parameters of the actual physical interface that the PPTP tunnel runs over. Your ISP should supply this information.

- **Username** – The login or username supplied to you by your ISP.
- **Password** – The password supplied to you by your ISP.
- **PPTP Server IP** – The IP of the PPTP server that the DFL-700 will connect to.

### Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type:

PPTP over Ethernet connections are used in some DSL and cable modem networks. You need account details, and possibly also IP configuration parameters of the actual physical interface that the PPTP tunnel runs over. Your ISP should supply this information.

#### PPTP tunnel parameters:

Username:

Password:

Retype Password:

PPTP Server IP:

#### Physical interface parameters:

**DHCP** - automatic configuration

Everything is automatic.

**Static IP** - manual configuration

Your ISP should provide this information to you.

IP Address:

Subnet Mask:  - 256 hosts (/24)

Gateway IP:

This may or may not be necessary, depending on the ISP.

Before PPTP can be used to connect to you ISP, the physical (WAN) interface parameters need to entered. You can use either **DHCP** or **Static IP**, depending on the type of ISP used. Your ISP should supply this information.

If using static IP, this information needs to be filled in.

- **IP Address** – The IP address of the **WAN** interface. This IP is used to connect to the PPTP server.
- **Subnet Mask** – Size of the external network.
- **Gateway IP** – Specifies the IP address of the default gateway used to access the Internet.

## WAN Interface Settings – Using BigPond

The ISP Telstra BigPond uses BigPond for authentication; the IP is assigned with DHCP.

- **Username** – The login or username supplied to you by your ISP.
- **Password** – The password supplied to you by your ISP.

### Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type:

Regular ethernet connection with DHCP-assigned IP address, plus authentication via a special protocol. Used by the ISP Telstra BigPond.

Username:

Password:

Retype Password:

## Traffic Shaping

### Traffic shaping - interface speed limits

In order to do traffic shaping beyond simple limits, such as guarantees and priorities, the traffic shaper needs to know what the maximum bandwidth is. Throughput through this interface will be limited to these speeds. If the limits are set too high, traffic shaping will not work.

Upstream bandwidth:  kbit/s

Downstream bandwidth:  kbit/s

When **Traffic Shaping** is enabled and the correct maximum up and downstream bandwidth is specified, it is possible to control which policies have the highest priority when large amounts of data are moving through the DFL-700. For example, the policy for the Web server might be given higher priority than the policies for most employees' computers.

You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth to make sure that there is enough bandwidth available for a high-priority service. You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.

**Note:** If the limit is set too high, i.e. higher than your Internet connection, the traffic shaping will not work at all.

## MTU Configuration

**Manual Interface MTU Configuration** - maximum size of packets sent via this interface

Normally, you do not need to change the MTU settings. By default, the interface uses the maximum size that the physical media supports.

MTU:  bytes. Upper limit:

To improve the performance of your Internet connection, you can adjust the maximum transmission unit (MTU) of the packets that the DFL-700 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-700 and the Internet. If the packets the DFL-700 sends are larger, they get broken up or fragmented, which could slow 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 PPPoE, you may want to set the MTU size to this value. DSL modems may also have small MTU sizes. Most ethernet networks have an MTU of 1500.

**Note:** 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.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Routing

Click on **System** in the menu bar, and then click **Routing** below it; this will provide a list of all configured routes, and it will look something like this:

Routing table				
Interface	Network	Gateway	Additional IP	Proxy ARP
WAN	194.1.2.0/24			<a href="#">[Edit]</a>
LAN	192.168.1.0/24			<a href="#">[Edit]</a>
WAN	0.0.0.0/0	194.1.2.254		<a href="#">[Edit]</a>
LAN	192.168.5.0/24		192.168.5.1	<a href="#">[Edit]</a>
VPNTunnel1	192.168.2.0/24			Yes <a href="#">[Edit]</a>
<a href="#">[Add new]</a>				

The Routes configuration section describes the firewall's routing table. The DFL-700 uses a slightly different method of describing routes compared to most other systems. However, we believe that this method of describing routes is easier to understand, making it less likely for users to cause errors or breaches in security.

**Interface** – Specifies which interface packets destined for this route shall be sent through.

**Network** – Specifies the network address for this route.

**Gateway** – Specifies the IP address of the next router hop used to reach the destination network. If the network is directly connected to the firewall interface, no gateway address is specified.

**Local IP Address** – The IP address specified here will be automatically published on the corresponding interface. This address will also be used as the sender address in ARP queries. If no address is specified, the firewall's own interface IP address will be used.

**Proxy ARP** – Specifies that the firewall shall publish this route via Proxy ARP.

One advantage with this form of notation is that you can specify a gateway for a particular route, without having a route that covers the gateway's IP address or despite the fact that the route that covers the gateway's IP address is normally routed via another interface.

The difference between this form of notation and that most commonly used, is that you do not specify the interface name in a separate column. Instead, you specify the IP address of each interface as a gateway.

**Note:** The firewall does not Proxy ARP routes on VPN interfaces.

## Add a new Static Route

Follow these steps to add a new route.

**Step 1.** Go to **System** and **Routing**.

**Step 2.** Click on **Add new** in the bottom of the routing table.

**Step 3.** Choose the interface that the route should be sent through from the dropdown menu.

**Step 4.** Specify the Network and Subnet mask.

**Step 5.** If this network is behind a remote gateway, enable the checkbox **Network is behind remote gateway** and specify the IP of that gateway.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Remove a Static Route

Follow these steps to remove a route.

**Step 1.** Go to **System** and **Routing**.

**Step 2.** Click the **Edit** corresponding to the route you would like to remove.

**Step 3.** Check the checkbox named **Delete this route**.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

# Logging

Click on **System** in the menu bar, and then click **Logging** below it.

Logging, the ability to audit decisions made by the firewall, is a vital part in all network security products. The D-Link DFL-700 provides several options for logging activity. The D-Link DFL-700 logs activity by sending the log data to one or two log receivers in the network.

The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'System' tab is selected, and the 'Logging' sub-tab is active. On the left sidebar, there are buttons for 'Administration', 'Interfaces', 'Routing', 'Logging', and 'Time'. The main content area is titled 'Logging Settings' and contains the following options:

- Syslog** - send log data via the syslog protocol to one or two servers  
If both servers are configured, logs will be sent to both at the same time.  
Syslog server 1:   
Syslog server 2:  (optional)  
Syslog facility:
- Enable audit logging**  
The firewall normally logs denied packets. With audit logging enabled, it will also log when allowed connections open and close.
- Enable E-mail alerting for IDS/IDP events**  
Sensitivity:   
SMTP Server:   
Sender:   
E-Mail Address 1:   
E-Mail Address 2:   
E-Mail Address 3:

At the bottom right of the settings area, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a red plus icon).

All logging is done to Syslog recipients. The log format used for syslog logging is suitable for automated processing and searching.

The D-Link DFL-700 specifies a number of events that can be logged. Some of these events, such as startup and shutdown events, are mandatory and will always generate log

entries. Other events, for instance to log when allowed connections are opened and closed, are configurable. It is also possible to have E-mail alerting for IDS/IDP events to up to three email addresses.

## Enable Logging

Follow these steps to enable logging.

**Step 1.** Enable syslog by checking the **Syslog** box.

**Step 2.** Fill in your first syslog server as **Syslog server 1**. If you have two syslog servers, you have to fill in the second one as **Syslog server 2**. You must fill in at least one syslog server for logging to work.

**Step 3.** Specify what facility to use by selecting the appropriate syslog facility. Local0 is the default facility.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Enable Audit Logging

To start auditing all traffic through the firewall, follow the steps below. This is required for running third party log analyzers on the logs and to see how much traffic different connections use.

Follow these steps to enable auditing.

**Step 1.** Enable syslog by checking the **Enable audit logging** box.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Enable E-mail alerting for IDS/IDP events

Follow these steps to enable E-mail alerting.

**Step 1.** Enable E-mail alerting by checking the **Enable E-mail alerting for IDS/IDP events** checkbox.

**Step 2.** Choose the sensitivity level.

**Step 3.** In the **SMTP Server** field, fill in the SMTP server to which the DFL-700 will send the e-mail alerts.

**Step 4.** Specify up to three valid email addresses to receive the e-mail alerts.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

# Time

Click on **System** in the menu bar, and then click **Time** below it. This will give you the option to either set the system time by syncing to an Internet Network Time Server (NTP) or by entering the system time manually.

The screenshot shows the configuration interface for a D-Link DFL-700 Network Security Firewall. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The left sidebar contains buttons for 'Administration', 'Interfaces', 'Routing', 'Logging', and 'Time' (which is highlighted in yellow). The main content area is titled 'Time Settings' and is divided into three sections:

- Current time and date:** Contains a checkbox for 'Set the system time'. Below it are date pickers for 'Date' (19 Oct 2003) and 'Time' (12:34:56) with a '(24 hour time)' label.
- Time zone and daylight saving time settings:** Features a 'Time zone' dropdown menu set to '(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'. Below are radio buttons for 'No daylight saving time' and 'Apply daylight saving time from: Mar 28 ... to: Oct 28'.
- Automatic time synchronization:** Includes a checkbox for 'Enable NTP'. Below are input fields for 'Primary NTP Server:' and 'Secondary NTP Server:' (optional).

At the bottom right of the configuration area are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with an orange 'X' icon), and 'Help' (with a red plus icon).

## Changing time zone

Follow these steps to change the time zone.

**Step 1.** Choose the correct time zone in the drop down menu.

**Step 2.** Specify the dates to begin and end daylight saving time or choose no daylight saving time by checking the correct box.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Using NTP to sync time

Follow these steps to sync to an Internet Time Server.

**Step 1.** Enable synchronization by checking the **Enable NTP** box.

**Step 2.** Enter the Server IP Address or Server name with which you want to synchronize.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Setting time and date manually

Follow these steps to manually set the system time.

**Step 1.** Check the **Set the system time** box.

**Step 2.** Select the correct date.

**Step 3.** Set the correct time using the 24-hour format.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

# Firewall

## Policy

The Firewall Policy configuration section is the "heart" of the firewall. The policies are the primary filter that is configured to allow or disallow certain types of network traffic through the firewall. The policies also regulate how bandwidth management, traffic shaping, is applied to traffic flowing through the WAN interface of the firewall.

When a new connection is being established through the firewall, the policies are evaluated, top to bottom, until a policy that matches the new connection is found. The Action of the rule is then carried out. If the action is Allow, the connection will be established and a state representing the connection is added to the firewall's internal state table. If the action is Drop, the new connection will be refused. The section below will explain the meanings of the various action types available.

## Policy modes

The first step in configuring security policies is to configure the mode for the firewall. The firewall can run in NAT or No NAT (Route) mode. Select NAT mode to use DFL-700 network address translation to protect private networks from public networks. In NAT 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. Then you can create NAT mode policies to accept or deny connections between these networks. NAT mode policies hide the addresses of the internal and DMZ networks from users on the Internet. In No NAT (Route) mode you can also create routed policies between interfaces. Route mode policies accept or deny connections between networks without performing address translation. To use NAT mode select **Hide source addresses (many-to-one NAT)** and to use No NAT (Route) mode choose **No NAT**.

## Action Types

**Drop** – Packets matching Drop rules will immediately be dropped. Such packets will be logged if logging has been enabled in the Logging Settings page.

**Reject** – Reject works basically the same way as Drop. In addition to this, the firewall sends an ICMP UNREACHABLE message back to the sender or, if the rejected packet was a TCP packet, a TCP RST message. Such packets will be logged if logging has been enabled in the Logging Settings page.

**Allow** – Packets matching Allow rules are passed to the stateful inspection engine, which will remember that a connection has been opened. Therefore, rules for return traffic will not be required as traffic belonging to open connections is automatically dealt with before it reaches the policies. Logging is carried out if audit logging has been enabled in the Logging Settings page.

## Source and Destination Filter

**Source Nets** – Specifies the sender span of IP addresses to be compared to the received packet. Leave this blank to match everything.

**Source Users/Groups** – Specifies if an authenticated username is needed for this policy to match. Either make a list of usernames, separated by a comma (,) or write **Any** for any authenticated user. If it is left blank there is no need for authentication for the policy.

**Destination Nets** – Specifies the span of IP addresses to be compared to the destination IP of the received packet. Leave this blank to match everything.

**Destination Users/Groups** – Specifies if an authenticated username is needed for this policy to match. Either make a list of usernames, separated by a comma (,) or write Any for any authenticated user. If it is left blank there is no need for authentication for the policy.

## Service Filter

Either choose a predefined service from the dropdown menu or make a custom service.

The following custom services exist:

**All** – This service matches all protocols.

**TCP+UDP+ICMP** – This service matches all ports on either the TCP or the UDP protocol, including ICMP.

**Custom TCP** – This service is based on the TCP protocol.

**Custom UDP** – This service is based on the UDP protocol.

**Custom TCP+UDP** – This service is based on either the TCP or the UDP protocol.

The following is used when making a custom service:

**Custom source/destination ports** – For many services, a single destination port is sufficient. The source port used most often are all ports, 0-65535. The http service, for instance, uses destination port 80. A port range can also be used, meaning that a range 137-139 covers ports 137, 138, and 139. Multiple ranges or individual ports may also be entered, separated by commas. For instance, a service can be defined as having source ports 1024-65535 and destination ports 80-82, 90-92, and 95. In this case, a TCP or UDP packet with the destination port being one of 80, 81, 82, 90, 91, 92 or 95, and the source port being in the range 1024-65535, will match this service.

## Schedule

If a schedule should be used for the policy, choose one from the dropdown menu. These are specified on the **Schedules** page. If the policy should always be active, choose Always from the dropdown menu.

## Intrusion Detection / Prevention

The DFL-700 Intrusion Detection/Prevention System (IDS/IDP) is a real-time intrusion detection and prevention sensor that identifies and takes action against a wide variety of suspicious network activity. The IDS uses intrusion signatures, stored in the attack database, to identify the most common attacks. In response to an attack, the IDS protects the networks behind the DFL-700 by dropping the traffic. To notify of the attack the IDS sends an e-mail to

the system administrators if e-mail alerting is enabled. D-Link updates the attack database periodically. There are two modes that can be configured, either **Inspection Only** or **Prevention**. Inspection Only will only inspect the traffic, and if the DFL-700 detects anything it will log, e-mail an alert (if configured), and pass on the traffic. If Prevention is used the traffic will be dropped and logged and if configured, an e-mail alert will be sent.

## Traffic Shaping

The simplest way to obtain quality of service in a network, seen from a security as well as a functionality perspective, is to have the components in the network, not the applications, be responsible for network traffic control in well-defined choke points.

Traffic shaping works by measuring and queuing IP packets, in transit, with respect to a number of configurable parameters. Differentiated rate limits and traffic guarantees based on source, destination, and protocol parameters can be created, much the same way firewall policies are implemented.

There are three different priorities when configuring the traffic shaping, **Normal**, **High**, and **Critical**.

**Limit** works by limiting the inbound and outbound traffic to the specified speed. This is the maximum bandwidth that can be used by traffic using this policy. Note however that if you have other policies using limit, which in total is more than your total Internet connection, and have configured the traffic limits on the WAN interface, this limit is sometimes lowered to allow traffic with higher priorities to have precedence.

By using **Guarantee**, you can control traffic using a policy with a minimum bandwidth. This will only work if the traffic limits for the WAN interface are configured correctly.

## Add a new policy

Follow these steps to add a new outgoing policy.

**Step 1.** Choose the **LAN->WAN** policy list from the available policy lists.

**Step 2.** Click on the **Add new** link.

**Step 3.** Fill in the following values:

**Name:** Specifies a symbolic name for the rule. This name is used mainly as a rule reference in log data and for easy reference in the policy list.

**Action:** Select **Allow** to allow this type of traffic.

**Source Nets:** – Specifies the sender span of IP addresses to be compared to the received packet. Leave this blank to match everything.

**Source Users/Groups:** Specifies if an authenticated username is needed for this policy to match. Either make a list of usernames, separated by a comma (,) or write **Any** for any authenticated user. If it is left blank there is no need for authentication for the policy.

**Destination Nets:** Specifies the span of IP addresses to be compared to the destination IP of the received packet. Leave this blank to match everything.

**Destination Users/Groups:** Specifies if an authenticated username is needed for this policy to match. Either make a list of usernames, separated by a comma (,) or write **Any** for any authenticated user. If it is left blank there is no need for authentication for the policy.

**Service:** Either choose a predefined service from the dropdown menu or make a custom service.

**Schedule:** Choose which schedule should be used for this policy to match. Choose Always for no scheduling.

**Step 4.** If using Traffic shaping, fill in the required information. If not, skip this step.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Change order of policy

Follow these steps to change the order of a policy.

**Step 1.** Choose the policy list for which you would like to change the order from the available policy lists.

**Step 2.** Click on the **Edit** link corresponding to the rule you want to move.

**Step 3.** Change the number in the **Position** to the new line. This will occur after the apply button is clicked and will move the policy to the new row and move the old policy and all following policies one step down.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Delete policy

Follow these steps to delete a policy.

**Step 1.** Choose the policy list from which you would like do delete the policy in from the available policy lists.

**Step 2.** Click on the **Edit** link corresponding to the rule you want to delete.

**Step 3.** Enable the **Delete policy** checkbox.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Configure Intrusion Detection

Follow these steps to configure IDS on a policy.

**Step 1.** Choose the policy you would like to have IDS on.

**Step 2.** Click on the **Edit** link corresponding to the rule you want to configure.

**Step 3.** Enable the **Intrusion Detection / Prevention** checkbox.

**Step 4.** Choose **Intrusion Detection** from the mode drop down list.

**Step 5.** Enable the alerting checkbox for e-mail alerting.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Configure Intrusion Prevention

Follow these steps to configure IDP on a policy.

- Step 1.** Choose the policy you would like have IDP on.
- Step 2.** Click on the **Edit** link corresponding to the rule you want to configure.
- Step 3.** Enable the **Intrusion Detection / Prevention** checkbox.
- Step 4.** Choose **Prevention** from the mode drop down list.
- Step 5.** Enable the alerting checkbox for e-mail alerting.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Port mapping / Virtual Servers

The Port mapping / Virtual Servers configuration section is where you can configure virtual servers like Web servers on the DMZ or similar servers. It is also possible to regulate how bandwidth management, traffic shaping, is applied to traffic flowing through the WAN interface of the firewall. It is also possible to use Intrusion Detection / Prevention and Traffic shaping on Port mapped services. These are applied in the same way as with policies. See the previous chapter for more information.

Mappings are read from top to bottom, and the first matching mapping is carried out.

### Add a new mapping

Follow these steps to add a new mapping on the WAN interface.

**Step 1.** Choose the **WAN** policy list from the available policy lists.

**Step 2.** Click on the **Add new** link.

**Step 3.** Fill in the following values:

**Name:** Specifies a symbolic name for the rule. This name is used mainly as a rule reference in log data and for easy reference in the policy list.

**Source Nets:** Specify the source networks, leave blank for everyone (0.0.0.0/0).

**Source Users/Groups:** Specifies if an authenticated username is needed for this mapping to match. Either make a list of usernames, separated by a comma (,) or write **Any** for any authenticated user. If it is left blank there is no need for authentication for the policy.

**Destination Nets:** Leave empty for the interface's own IP or enter a new IP if using Virtual IP.

**Service:** Either choose a predefined service from the dropdown menu or make a custom service.

**Pass To:** The IP of the server that the traffic should be passed to.

**Schedule:** Choose which schedule should be used for this mapping to match. Choose Always for no scheduling.

**Step 4.** If using Traffic shaping, fill in the required information. If not, skip this step.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## **Delete mapping**

Follow these steps to delete a mapping.

**Step 1.** Choose the mapping list (WAN, LAN, or DMZ) you would like to delete the mapping from.

**Step 2.** Click on the **Edit** link corresponding to the rule you want to delete.

**Step 3.** Enable the **Delete mapping** checkbox.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Administrative users

Click on **Firewall** in the menu bar, and then click **Users** below it. This will display all the users. The first section lists the administrative users.



The first column show the access levels, *Administrator* and *Read-only*. An *Administrator* user can add, edit and remove rules, change settings of the DFL-700, and so on. The *Read-only* user can only look at the configuration. The second column displays the users in each access level.

## Add Administrative User

Follow these steps to add a new administrative user.

**Step 1.** Click on **add** corresponding to the type of user you would like to add, Admin or Read-only.

**Step 2.** Fill in the **User name**; make sure you are not trying to add one that already exists.

**Step 3.** Specify the password for the new user.

A screenshot of a web form titled "Administration Settings". The form is for "Add new user:" and contains four input fields: "User name:" with the value "newuser", "Access level:" with a dropdown menu set to "Administrator", "Password:" with masked characters "xxxx", and "Retype password:" with masked characters "xxxx". At the bottom right of the form are three buttons: "Apply" (green checkmark), "Cancel" (orange X), and "Help" (red plus sign).

Click the **Apply** button below to apply the settings or click Cancel to discard changes.

**Note:** The user name and password should be at least six characters long. The user name and password can contain numbers (0-9) and upper and lower case letters (A-Z, a-z). Special characters and spaces are not allowed.

## Change Administrative User Access level

To change the access level of a user click on the user name and you will see the following screen. From here you can change the access level by selecting the appropriate level from the drop-down menu.

### Access levels

- **Administrator** – The user can add, edit and remove rules, and change all settings.
- **Read-only** – The user can only look at the configuration of the firewall.
- **No Admin Access** – The user is only used for user authentication.

**Administration Settings**

Edit administrative user **admin**:

User name:

Access level:

**Change password**

Password:

Retype password:

**Delete user**

Follow these steps to change Administrative User Access level.

**Step 1.** Click on the user you would like to change level of.

**Step 2.** Choose the appropriate level from the drop-down menu.

Click the **Apply** button below to apply the settings or click Cancel to discard changes.

## Change Administrative User Password

To change the password of a user click on the user name and you will see the following screen.

Follow these steps to change Administrative User password.

**Step 1.** Click on the user for which you would like to change the password.

**Step 2.** Enable the **Change password** checkbox.

**Step 3.** Enter the new password twice.

**Administration Settings**

Edit administrative user **admin**:

User name:

Access level:

**Change password**

Password:

Retype password:

**Delete user**

Click the **Apply** button below to apply the settings or click Cancel to discard changes.

**Note:** The password should be at least six characters long. The password can contain numbers (0-9) and upper and lower case letters (A-Z, a-z). Special characters and spaces are not allowed.

## Delete Administrative User

To delete a user click on the user name and you will see the following screen.

Follow these steps to delete an Administrative User.

**Step 1.** Click on the user you would like to delete.

**Step 2.** Enable the **Delete user** checkbox.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

**Note:** Deleting a user is irreversible; once the user is deleted, it cannot be undeleted. Do not delete the user you are currently logged in as.

**Administration Settings**

Edit administrative user **admin**:

User name:

Access level:

**Change password**

Password:

Retype password:

**Delete user**

Apply Cancel Help

## Users

User Authentication allows an administrator to grant or reject access to specific users from specific IP addresses, based on their user credentials.

Before any traffic is allowed to pass through any policies configured with username or groups, the user must first authenticate him/her-self. The DFL-700 can either verify the user against a local database or pass along the user information to an external authentication server, which verifies the user and the given password, and transmits the result back to the firewall. If the authentication is successful, the DFL-700 will remember the source IP address of this user, and any matching policies with usernames or groups configured will be allowed. Specific policies that deal with user authentication can be defined, thus leaving policies that not require user authentication unaffected.

The DFL-700 supports the RADIUS (Remote Authentication Dial In User Service) authentication protocol. This protocol is heavily used in many scenarios where user authentication is required, either by itself or as a front-end to other authentication services.

### The DFL-700 RADIUS Support

The DFL-700 can use RADIUS to verify users against, for example, Active Directory or Unix password-file. It is possible to configure up to two servers, if the first one is down it will try the second IP instead.

The DFL-700 can use CHAP or PAP when communicating with the RADIUS server. **CHAP** (Challenge Handshake Authentication Protocol) does not allow a remote attacker to extract the user password from an intercepted RADIUS packet. However, the password must be stored in plaintext on the RADIUS server. **PAP** (Password Authentication Protocol) may be defined as the less secure of the two. If a RADIUS packet is intercepted while being transmitted between the firewall and the RADIUS server, given time, the user password can be extracted. The advantage to this is that the password does not have to be stored in plaintext in the RADIUS server.

The DFL700 uses a shared secret when connecting to the RADIUS server. The shared secret enables basic encryption of the user password when the RADIUS-packet is transmitted from the firewall to the RADIUS server. The shared secret is case sensitive, can contain up to 100 characters, and must be typed exactly the same on both the firewall and the RADIUS server.

## Enable User Authentication via HTTP / HTTPS

Follow these steps to enable User Authentication.

**Step 1.** Enable the checkbox for User Authentication.

**Step 2.** Specify if HTTP and HTTPS or only HTTPS should be used for the login.

**Step 3.** Specify the idle-timeout, the time a user can be idle before being logged out by the firewall.

**Step 4.** Choose new ports for the management WebUI to listen on as the user authentication will use the same ports as the management WebUI is using.

**Enable User Authentication via HTTP / HTTPS**  
HTTP Security:  HTTP as well as HTTPS  
 HTTPS only  
Idle Timeout:  hour

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Enable RADIUS Support

Follow these steps to enable RADIUS support.

**Step 1.** Enable the checkbox for RADIUS Support.

**Step 2.** Enter information for up to two RADIUS servers.

**Step 3.** Specify which mode to use, PAP or CHAP.

**Step 3.** Specify the shared secret for this connection.

**Enable RADIUS Support**  
Primary Server:  port   
Secondary Server:  port   
Mode:   
Shared Secret:   
Retype Secret:   
RADIUS retry:  seconds

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Add User

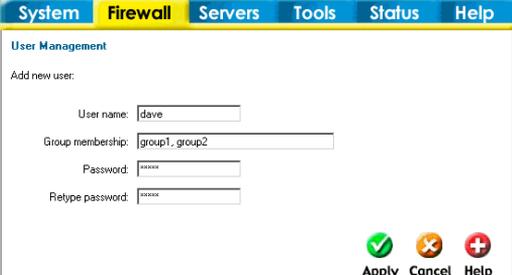
Follow these steps to add a new user.

**Step 1.** Click on **add** corresponding to the type of user you would like to add, Admin or Read-only.

**Step 2.** Fill in **User name**; make sure you are not trying to add one that already exists.

**Step 3.** Specify which groups the user should be a member of.

**Step 3.** Specify the password for the new user.



The screenshot shows the 'User Management' window with a menu bar containing 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The main content area is titled 'User Management' and contains the text 'Add new user:'. Below this are four input fields: 'User name:' with the value 'dave', 'Group membership:' with the value 'group1\_group2', 'Password:' with masked characters, and 'Retype password:' with masked characters. At the bottom right, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a red plus icon).

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

**Note:** The user name and password should be at least six characters long. The user name and password can contain numbers (0-9) and upper and lower case letters (A-Z, a-z). Special characters and spaces are not allowed.

## Change User Password

To change the password of a user click on the user name and you will see the following screen.

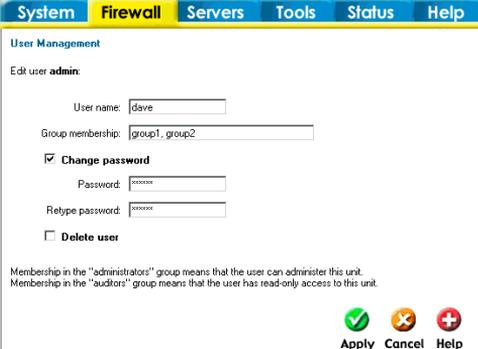
Follow these steps to change a users password.

**Step 1.** Click on the user for which you would like to change the password.

**Step 2.** Enable the **Change password** checkbox.

**Step 3.** Enter the new password twice.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.



The screenshot shows the 'User Management' window with a menu bar containing 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The main content area is titled 'User Management' and contains the text 'Edit user admin:'. Below this are four input fields: 'User name:' with the value 'dave', 'Group membership:' with the value 'group1\_group2', 'Password:' with masked characters, and 'Retype password:' with masked characters. There is a checked checkbox labeled 'Change password' and an unchecked checkbox labeled 'Delete user'. At the bottom, there is a small text block: 'Membership in the "administrators" group means that the user can administer this unit. Membership in the "auditors" group means that the user has read-only access to this unit.' At the bottom right, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with a red X icon), and 'Help' (with a red plus icon).

**Note:** The password should be at least six characters long. The password can contain numbers (0-9) and upper and lower case letters (A-Z, a-z). Special characters and spaces are not allowed.

## Delete User

To delete a user click on the user name and you will see the following screen.

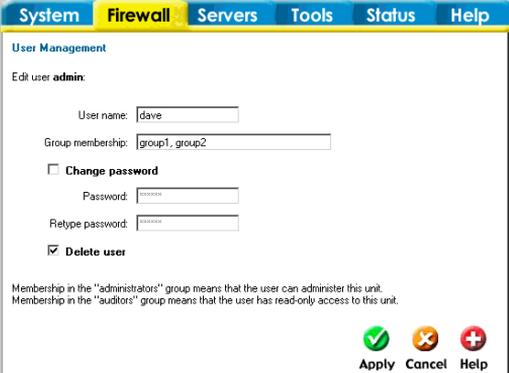
Follow these steps to delete a user.

**Step 1.** Click on the user you would like to delete.

**Step 2.** Enable the **Delete user** checkbox.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

**Note:** Deleting a user is irreversible; once the user is deleted, it cannot be undeleted.



The screenshot shows a web interface for 'User Management'. At the top, there is a navigation bar with tabs for 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. Below the navigation bar, the page title is 'User Management'. The main content area is titled 'Edit user: admin:'. It contains several input fields: 'User name:' with the value 'dave', 'Group membership:' with the value 'group1\_group2', 'Password:' and 'Retype password:' both with masked characters. There are three checkboxes: 'Change password' (unchecked), 'Delete user' (checked), and a third checkbox that is not clearly labeled. At the bottom of the form, there is a small text block explaining group memberships: 'Membership in the "administrators" group means that the user can administer this unit. Membership in the "auditors" group means that the user has read-only access to this unit.' At the bottom right of the form, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with an orange 'X' icon), and 'Help' (with a red plus icon).

## Schedules

It is possible to configure a schedule for policies to take effect. By creating a schedule, the DFL-700 allows the firewall policies to be used only at those designated times. Any activities outside of the scheduled time slot will not follow the policies and therefore will not likely be permitted to pass through the firewall. The DFL-700 can be configured to have a start time and stop time, as well as 2 different time periods in a day. For example, an organization may only want the firewall to allow the internal network users to access the Internet during work hours. Therefore, one may create a schedule to allow the firewall to allow traffic Monday-Friday, 8AM-5PM only. During the non-work hours, the firewall will not allow Internet access.

The screenshot shows the D-Link DFL-700 Network Security Firewall configuration interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Firewall' tab is selected, and the 'Schedules' sub-tab is active. The interface displays the 'Manage Schedules' section, where a schedule named 'OfficeHours' is being edited. The 'Active from' date is set to 01 Jan 2003, and the 'Active to' date is 01 Jan 2038. The 'Recurring scheduling' checkbox is checked, and the schedule is configured for Monday through Friday, 06:00 to 18:00. Below the schedule configuration, there is a table of 'Defined schedules' with columns for Name, Start, Stop, and Recurring. The table lists 'OfficeHours' and 'TempAccess'.

Name	Start	Stop	Recurring
OfficeHours			Mon-Fri 08-17 <a href="#">[Edit]</a>
TempAccess	2003-10-15 00	2003-10-21 00	<a href="#">[Edit]</a>

### Add new recurring schedule

Follow these steps to add a new recurring schedule.

- Step 1.** Go to Firewall and Schedules and choose Add new.
- Step 2.** Enable the checkbox named Recurring scheduling.
- Step 3.** Use the checkboxes to set the times this schedule should be active.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## **Add new one-time schedule**

Follow these steps to add a new one-time schedule.

**Step 1.** Go to Firewall and Schedules and choose Add new.

**Step 2.** Choose the starting and ending date and hour when the schedule should be active.

**Step 3.** Use the checkboxes to set the times this schedule should be active inside the specified timeframe.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Services

A service is basically a definition of a specific IP protocol with corresponding parameters. The service http, for instance, is defined as using the TCP protocol with destination port 80.

Services are simplistic, in that they cannot carry out any action in the firewall on their own. Thus, a service definition does not include any information whether the service should be allowed through the firewall or not. That decision is made entirely by the firewall policies, in which the service is used as a filter parameter.

### Adding TCP, UDP or TCP/UDP Service

For many services, a single destination port is sufficient. The http service, for instance, uses destination port 80. To use a single destination port, enter the port number in the destination ports text box. In most cases, all ports (0-65535) have to be used as source ports. The second option is to define a port range; a port range is inclusive, meaning that a range 137-139 covers ports 137, 138, and 139.

Multiple ranges or individual ports may also be entered, separated by commas. For instance, a service can be defined as having source ports 1024-65535 and destination ports 80-82, 90-92, and 95. In this case, a TCP or UDP packet with the destination port being one of 80, 81, 82, 90, 91, 92 or 95, and the source port being in the range 1024-65535, will match this service.

Follow these steps to add a TCP, UDP, or TCP/UDP service.

**Step 1.** Go to Firewall and Service and choose add new.

**Step 2.** Enter a Name for the service in the name field. This name will appear in the service list when you add a new policy. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and \_. No other special characters and spaces are allowed.

**Step 3.** Select TCP/UDP Service.

**Step 4.** Select the protocol (either TCP, UDP, or both TCP/UDP) used by the service.

**Step 5.** Specify a source port or range for this service by typing in the low and high port numbers. Enter 0-65535 for all ports, or a single port like 80 for only one source port.

**Step 6.** Specify a destination port or range for this service by typing in the low and high port numbers. Enter 0-65535 for all ports, or a single port like 80 for only one destination port.

**Step 7.** Enable the Syn Relay checkbox if you want to protect the destination from SYN flood attacks.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Adding IP Protocol

When the type of the service is IP Protocol, an IP protocol number may be specified in the text field. To have the service match the GRE protocol, for example, the IP protocol should be specified as 47. A list of some defined IP protocols can be found in the appendix named “IP Protocol Numbers.”

IP protocol ranges can be used to specify multiple IP protocols for one service. An IP protocol range is similar to the TCP and UDP port range described previously. The range 1-4, 7 will match the protocols ICMP, IGMP, GGP, IP-in-IP, and CBT.

Follow these steps to add a TCP, UDP, or TCP/UDP service.

**Step 1.** Go to Firewall and Service and choose new.

**Step 2.** Enter a Name for the service in the name field. This name will appear in the service list when you add a new policy. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and \_. No other special characters and spaces are allowed.

**Step 3.** Select IP Protocol.

**Step 4.** Specify a comma-separated list of IP protocols.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Grouping Services

Services can be grouped in order to simplify configuration. Consider a Web server using standard http as well as SSL encrypted http (https). Instead of having to create two separate rules allowing both types of services through the firewall, a service group named, for instance, Web, can be created, with the http and the https services as group members.

Follow these steps to add a group.

**Step 1.** Go to Firewall and Service and choose new.

**Step 2.** Enter a Name for the service in the name field. This name will appear in the service list when you add a new policy. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and \_. No other special characters and spaces are allowed.

**Step 3.** Select Group.

**Step 4.** Specify a comma-separated list of existing services.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## Protocol-independent settings

**Allow ICMP errors from the destination to the source** – ICMP error messages are sent in several situations: for example, when an IP packet cannot reach its destination. The purpose of these error control messages is to provide feedback about problems in the communication environment.

However, ICMP error messages and firewalls are usually not a very good combination; the ICMP error messages are initiated at the destination host (or a device within the path to the destination) and sent to the originating host. The result is that the ICMP error message will be interpreted by the firewall as a new connection and dropped, if not explicitly allowed by the firewall rule-set. It is generally not a good idea to allow any inbound ICMP message to be able to have those error messages forwarded.

To solve this problem, the DFL-700 can be instructed to pass an ICMP error message only if it is related to an existing connection. Check this option to enable this feature for connections using this service.

**ALG** – Like other stateful inspection based firewalls, the DFL-700 filters only information found in packet headers, for instance in IP, TCP, UDP, and ICMP headers.

In some situations though, filtering only header data is not sufficient. The FTP protocol, for instance, includes IP address and port information in the protocol payload. In these cases, the firewall needs to be able to examine the payload data and carry out appropriate actions. The DFL-700 provides this functionality using Application Layer Gateways, also known as ALGs.

To use an Application Layer Gateway, the appropriate Application Layer Gateway definition is selected in the dropdown menu. The selected Application Layer Gateway will thus manage network traffic that matches the policy using this service.

Currently, the DFL-700 supports two Application Layer Gateways, one is used to manage the FTP protocol and the other one is a HTTP Content Filtering ALG. For detailed information about how to configure the HTTP Application Layer Gateway, please see the Content Filtering chapter.

## VPN

This chapter introduces IPSec, the method, or rather set of methods used to provide VPN functionality. IPSec, Internet Protocol Security, is a set of protocols defined by the IETF, Internet Engineering Task Force, to provide IP security at the network layer.

An IPSec based VPN, such as DFL-700 VPN, is made up by two parts:

- Internet Key Exchange protocol (IKE)
- IPSec protocols (ESP)

The first part, IKE, is the initial negotiation phase, where the two VPN endpoints agree on which methods will be used to provide security for the underlying IP traffic. Furthermore, IKE is used to manage connections, by defining a set of Security Associations, SAs, for each connection. SAs are unidirectional, so there will be at least two SAs per IPSec connection. The other part is the actual IP data being transferred, using the encryption and authentication methods agreed upon in the IKE negotiation. This can be accomplished in a number of ways; by using the IPSec protocol ESP.

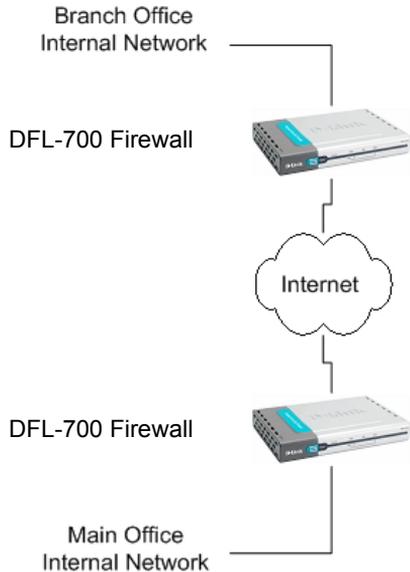
To set up a Virtual Private Network (VPN), you do not need to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet (Local Net), Destination Gateway (If LAN-to-LAN), Destination Subnet (If LAN-to-LAN), and Authentication Method (Pre-shared key or Certificate). The firewalls on both ends must use the same Pre-shared key or set of Certificates and IPSec lifetime to make a VPN connection.

## IPSec VPN between two networks

In the following example users on the main office internal network can connect to the branch office internal network and vice versa. Communication between the two networks takes place in an encrypted VPN tunnel that connects the two DFL-700 Network Security Firewalls across the Internet. Users on the internal networks are not aware that when they connect to a computer on the other network that the connection runs across the Internet.

As shown in the example, you can use the DFL-700 to protect a branch office and a small main office. Both of these DFL-700s can be configured as IPSec VPN gateways to create the VPN that connects the branch office network to the main office network.

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 configure the VPN policy.



## Creating a LAN-to-LAN VPN Tunnel

Follow these steps to add a LAN-to-LAN Tunnel.

**Step 1.** Go to Firewall and VPN and choose **Add new**.

**Step 2.** Enter a Name for the new tunnel in the name field. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and \_. No other special characters and spaces are allowed.

**Step 3.** Specify your local network, or your side of the tunnel, for example 192.168.1.0/255.255.255.0, in the Local Net field.

**Step 4.** Choose authentication type, either PSK (Pre-shared Key) or Certificate-based. If you choose PSK, make sure both firewalls use exactly the same PSK.

**Step 5.** For Tunnel Type, choose LAN-to-LAN tunnel and specify the network behind the other DFL-700 as Remote Net. Also specify the external IP of the other DFL-700, this can be an IP or a DNS name.

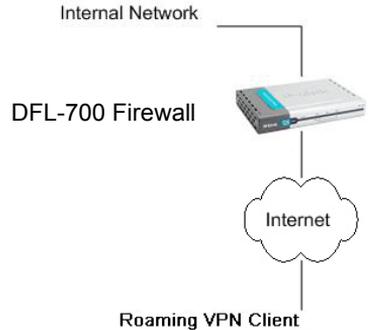
Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

Repeat these steps with the firewall on the other site.

## IPSec VPN between client and an internal network

In the following example users can connect to the main office internal network from anywhere on the Internet. Communication between the client and the internal network takes place in an encrypted VPN tunnel that connects the DFL-700 and the roaming users across the Internet.

The example shows a VPN between a roaming VPN client and the internal network, but you can also create a VPN tunnel that uses the DMZ network. The networks at the ends of the VPN tunnel are selected when you configure the VPN policy.



## Creating a Roaming Users Tunnel

Follow these steps to add a roaming users tunnel.

**Step 1.** Go to Firewall and VPN and choose **Add new**.

**Step 2.** Enter a Name for the new tunnel in the name field. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and \_. No other special characters and spaces are allowed.

**Step 3.** Specify your local network, or your side of the tunnel, for example 192.168.1.0/255.255.255.0, in the Local Net field. This is the network your roaming VPN clients should be allowed to connect to.

**Step 4.** Choose authentication type, either PSK (Pre-shared Key) or Certificate-based. If you choose PSK, make sure the clients use exactly the same PSK.

**Step 5.** For Tunnel Type, choose Roaming User.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

## **VPN – Advanced Settings**

Advanced settings for a VPN tunnel is used when the user needs to change some characteristics of the tunnel to, for example, try to connect to a third party VPN Gateway. The different settings per tunnel are:

### **Limit MTU**

With this setting it is possible to limit the MTU (Max Transferable Unit) of the VPN tunnel.

### **IKE Mode**

Specify if Main mode IKE or Aggressive Mode IKE should be used when establishing outbound VPN Tunnels. Inbound main mode connections will always be allowed. Inbound aggressive mode connections will only be allowed if this setting is set to aggressive mode.

### **IKE DH Group**

Here it is possible to configure the Diffie-Hellman group to 1 (modp 768-bit), 2 (modp 1024-bit), or 5 (modp 1536-bit).

### **PFS – Perfect Forward Secrecy**

If PFS, Perfect Forwarding Secrecy, is enabled, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. While this is slower, it makes sure that no keys are dependent on any other previously used keys; no keys are extracted from the same initial keying material. This is to make sure that, in the unlikely event that some key was compromised, no subsequent keys can be derived.

### **NAT Traversal**

Here it is possible to configure how the NAT Traversal code should behave.

**Disabled** - The firewall does not send the Vendor ID's that include NAT-T support when setting up the tunnel.

**On if supported and need NAT** - Will only use NAT-T if one of the VPN gateways is NATed.

**On if supported** - Always tries to use NAT-T when setting up the tunnel.

### **Keepalives**

**No keepalives** – Keep-alive is disabled.

**Automatic keepalives** - The firewall will send ICMP pings to IP Addresses automatically discovered from the VPN Tunnel settings.

**Manually configured IP addresses** - Configure the source and destination IP addresses used when sending the ICMP pings.

## Proposal Lists

To agree on the VPN connection parameters, a negotiation process is performed. As the result of the negotiations, the IKE and IPSec security associations (SAs) are established. As the name implies, a proposal is the starting point for the negotiation. A proposal defines encryption parameters, for instance encryption algorithm, life times etc, that the VPN gateway supports.

There are two types of proposals, IKE proposals and IPSec proposals. IKE proposals are used during IKE Phase-1 (IKE Security Negotiation), while IPSec proposals are using during IKE Phase-2 (IPSec Security Negotiation).

A Proposal List is used to group several proposals. During the negotiation process, the proposals in the proposal list are offered to the remote VPN gateway one after another until a matching proposal is found.

### IKE Proposal List

**Cipher** – Specifies the encryption algorithm used in this IKE proposal. Supported algorithms are AES, 3DES, DES, Blowfish, Twofish, and CAST128.

**Hash** – Specifies the hash function used to calculate a check sum that reveals if the data packet is altered while being transmitted. MD5 and SHA1 are supported algorithms.

**Life Times** – Specifies in KB or seconds when the security associations for the VPN tunnel need to be re-negotiated.

### IPSec Proposal List

**Cipher** – Specifies the encryption algorithm used in this IPSec proposal. Supported algorithms are AES, 3DES, DES, Blowfish, Twofish, and CAST128.

**HMAC** – Specifies the hash function used to calculate a check sum that reveals if the data packet is altered while being transmitted. MD5 and SHA1 are supported algorithms.

**Life Times** – Specifies in KB or seconds when the security associations for the VPN tunnel need to be re-negotiated.

## Certificates

A certificate is a digital proof of identity. It links an identity to a public key in a trustworthy manner. Certificates can be used to authenticate individual users or other entities. These types of certificates are commonly called end-entity certificates.

Before a VPN tunnel with certificate based authentication can be set up, the firewall needs a certificate of its own and that of the remote firewall. These certificates can either be self-signed certificates, or issued by a CA.

### Trusting Certificates

When setting up a VPN tunnel, the firewall has to be told whom it should trust. When using pre-shared keys, this is simple. The firewall trusts anyone who has the same pre-shared key.

When using certificates, on the other hand, you tell the firewall that it can trust anyone whose certificate is signed by a given CA. Before a certificate is accepted, the following steps are taken to verify the validity of the certificate:

- Construct a certification path up to the trusted root CA.
- Verify the signatures of all certificates in the certification path.
- Fetch the CRL for each certificate to verify that none of the certificates have been revoked.

### Local identities

This is a list of all the local identity certificates that can be used in VPN tunnels. A local identity certificate is used by the firewall to prove its identity to the remote VPN peer.

To add a new local identity certificate, click Add new. The following pages will allow you to specify a name for the local identity, and upload the certificate and private key files. This certificate can be selected in the Local Identity field on the VPN page.

This list also includes a special certificate called Admin. This is the certificate used by the Web interface to provide HTTPS access.

Note: The certificate named Admin can only be replaced, not deleted or renamed. This is used for HTTPS access to the DFL-700.

### Certificates of remote peers

This is a list of all certificates of individual remote peers.

To add a new remote peer certificate, click Add new. The following pages will allow you to specify a name for the remote peer certificate and upload the certificate file. This certificate can be selected in the Certificates field on the VPN page.

### Certificate Authorities

This is a list of all CA certificates. To add a new Certificate Authority certificate, click Add new. The following pages will allow you to specify a name for the CA certificate and upload the certificate file. This certificate can be selected in the Certificates field on the VPN page.

Note: If the uploaded certificate is a CA certificate, it will automatically be placed in the Certificate Authorities list, even if Add New was clicked in the Remote Peers list. Similarly, a non-CA certificate will be placed in the Remote Peers list even if Add New was clicked from the Certificate Authorities list.

## **Identities**

This is a list of all the configured Identity lists. An Identity list can be used on the VPN page to limit inbound VPN access from this list of known identities.

Normally, a VPN tunnel is established if the certificate of the remote peer is present in the Certificates field in the VPN section, or if the remote peer's certificate is signed by a CA whose certificate is present in the Certificates field in the VPN section. However, in some cases it might be necessary to limit who can establish a VPN tunnel even among peers signed by the same CA.

The Identity list can be selected in the Identity List field on the VPN page.

If an Identity List is configured, the firewall will match the identity of the connecting remote peer against the Identity List, and only allow it to open the VPN tunnel if it matches the contents of the list.

If no Identity List is used, no identity matching is done.

# Content Filtering

DFL-700 HTTP 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 the DFL-700 blocks the Web page.

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

The HTTP content filtering can also be configured to strip contents like ActiveX, Flash, and cookies.

There is also a URL whitelist for URLs that should be excluded from all Content Filtering.

**Note:** For HTTP URL filtering to work, all HTTP traffic needs to go through a policy using a service with the HTTP ALG.

## Edit the URL Global Whitelist

Follow these steps to add or remove a URL.

**Step 1.** Go to Firewall and Content Filtering and choose Edit global URL whitelist.

**Step 2.** Add/edit or remove the URL that should never be checked with the Content Filtering.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.



## Edit the URL Global Blacklist

Follow these steps to add or remove a URL.

**Step 1.** Go to Firewall and Content Filtering and choose Edit global URL blacklist.

**Step 2.** Add/edit or remove the URL that should be checked with the Content Filtering.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.

**Note:** For HTTP URL filtering to work, all HTTP traffic needs to go through a policy using a service with the HTTP ALG.

The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Firewall' tab is active. On the left sidebar, there are buttons for 'Policy', 'Portmapping', 'Users', 'Schedules', 'Services', 'VPN', 'Certificates', and 'Content Filtering' (highlighted in yellow). The main content area is titled 'HTTP Content Filtering' and contains the following text:

Edit Destination URL GlobalBlacklist:

The URL blacklist can be used to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

Blank lines are ignored. Lines beginning with "#" are also ignored.

# Deny access to potentially dangerous file types:

- #
- #
- # Malicious executables can be downloaded by exploits
- \*.exe
- \*.com
- \*.scr
- \*.cpl
- \*.pif
- # Malicious scripts can be downloaded by exploits
- \*.vb
- \*.vbd
- \*.vbe
- \*.vbs
- \*.vbx
- \*.bat
- \*.cmd
- \*.wsc
- \*.wsf
- \*.wsh
- \*.set
- # Shell scripts can contain executables and invoke nearly any command

At the bottom right, there are three buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with an orange X icon), and 'Help' (with a red plus icon).

## **Active content handling**

Active content handling can be enabled or disabled by checking the checkbox before each type you would like to strip. For example to strip ActiveX and Flash, enable the checkbox named Strip ActiveX objects. It is possible to strip ActiveX, Flash, Java, JavaScript, and VBScript. It is also possible to block cookies.

**Note:** For HTTP URL filtering to work, all HTTP traffic needs to go through a policy using a service with the HTTP ALG.

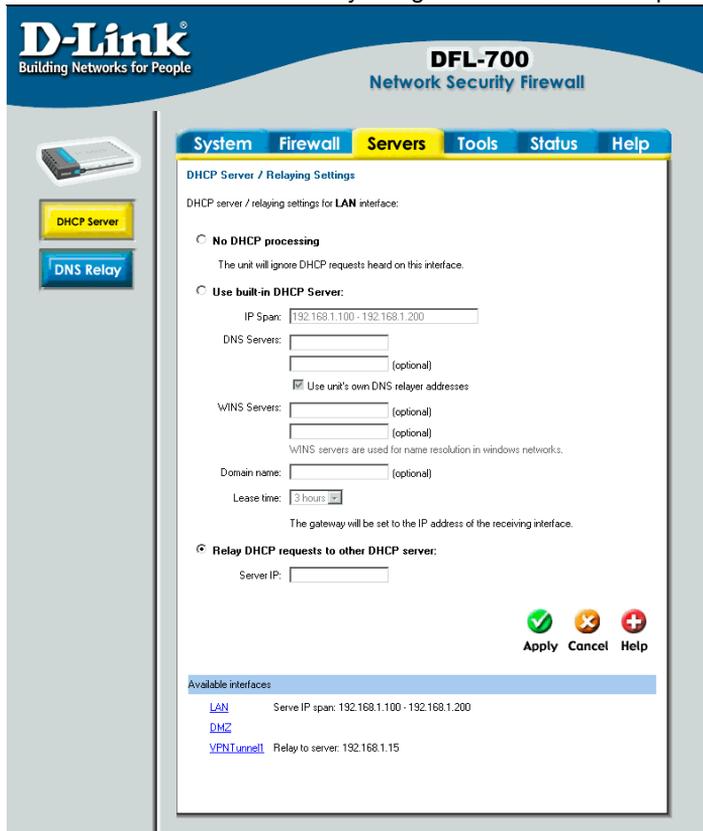
# Servers

## DHCP Server Settings

The DFL-700 contains a DHCP server. DHCP (Dynamic Host Configuration Protocol) is a protocol that allows network administrators to automatically assign IP numbers to computers on a network. The DFL-700 DHCP Server helps to minimize the work necessary to administer a network, as there is no need for another server running DHCP Server software.

The DFL-700 DHCP Server only implements a subset of the DHCP protocol necessary to serve a small network; these are:

- IP address
- Netmask
- Subnet
- Gateway address
- DNS Servers
- WINS Servers
- Domain name



The DFL-700 DHCP Server assigns and manages IP addresses from specified address pools within the firewall to the DHCP clients.

**Note:** Leases are remembered over a re-configure or reboot of the firewall.

The DFL-700 also includes a DHCP Relayer. A DHCP Relayer is a form of gateway between a DHCP Server and its users. The relayer intercepts DHCP queries from the users and forwards them to a DHCP server while setting up dynamic routes based on leases. This enables the firewall to keep an accurate routing table based on active users and protects the DHCP server to some degree.

**Note:** There can only be one DHCP Server or DHCP Relay configured per interface.

## Enable DHCP Server

To enable the DHCP Server on an interface, click on **Servers** in the menu bar, and then click **DHCP Server** below it.

Follow these steps to enable the DHCP Server on the LAN interface.

**Step 1.** Choose the LAN interface from the Available interfaces list.

**Step 2.** Enable by checking the **Use built-in DHCP Server** box.

**Step 3.** Fill in the IP Span, the start and end IP for the range of IP addresses that the DFL-700 can assign.

**Step 4.** Fill in the DNS servers the DHCP server will assign to the clients; at least one should be provided. If the DNS Relay is configured, the DHCP server can assign those.

**Step 5.** Optionally type in the WINS servers the DHCP server will assign to the clients.

**Step 6.** Optionally type in the domain that the DHCP server will assign to the clients.

**Step 7.** Choose the length of time the DHCP server will give out leases before the client has to renew them.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Enable DHCP Relay

To enable the DHCP Relay on an interface, click on **Servers** in the menu bar, and then click **DHCP Server** below it.

Follow these steps to enable the DHCP Relay on the LAN interface.

**Step 1.** Choose the LAN interface from the Available interfaces list.

**Step 2.** Enable by checking the **Relay DHCP Requests to other DHCP server** box.

**Step 3.** Fill in the IP of the DHCP Server; note that it should be on another interface than where the DHCP request is coming from, i.e. a server on the DMZ.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Disable DHCP Server/Relayer

To disable the DHCP Server on an interface, click on **Servers** in the menu bar, and then click **DHCP Server** below it. Here click on the interface that you want to disable the DHCP server or relay on.

Follow these steps to disable the DHCP Server or Relay on the LAN interface.

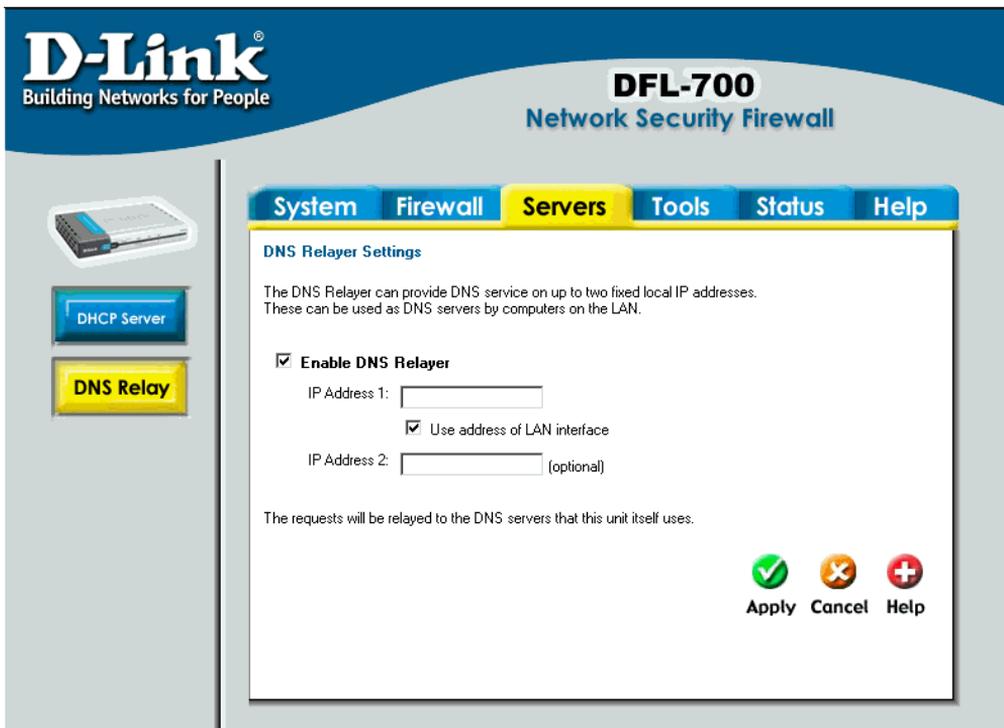
**Step 1.** Choose the LAN interface from the Available interfaces list.

**Step 2.** Disable by checking the **No DHCP processing** box.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## DNS Relay Settings

Click on **Servers** in the menu bar, and then click **DNS Relay** below it. The DFL-700 contains a DNS Relay that can be configured to relay DNS queries from the internal LAN to the DNS servers used by the firewall itself.



The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Servers' tab is selected. On the left sidebar, there are icons for 'DHCP Server' and 'DNS Relay'. The main content area is titled 'DNS Relay Settings' and contains the following text: 'The DNS Relay can provide DNS service on up to two fixed local IP addresses. These can be used as DNS servers by computers on the LAN.' Below this is a checked checkbox for 'Enable DNS Relay'. There are two input fields for 'IP Address 1' and 'IP Address 2' (optional). A checked checkbox 'Use address of LAN interface' is positioned between the two IP address fields. At the bottom right of the settings area are three buttons: 'Apply' (green checkmark), 'Cancel' (orange X), and 'Help' (red plus sign).

### Enable DNS Relay

Follow these steps to enable the DNS Relay.

**Step 1.** Enable by checking the **Enable DNS Relay** box.

**Step 2.** Enter the IP numbers that the DFL-700 should listen for DNS queries on.

**Note:** If “Use address of LAN interface” is checked, you do not have to enter an IP in IP Address 1, as the firewall will know what address to use.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## **Disable DNS Relay**

Follow these steps to disable the DNS Relay.

**Step 1.** Disable by un-checking the **Enable DNS Relay** box.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

# Tools

## Ping

Click on **Tools** in the menu bar, and then click **Ping** below it. This tool is used to send a specified number of ICMP Echo Request packets to a given destination. All packets are sent in immediate succession rather than one per second. This method is the best suited for diagnosing connectivity problems.

**Ping**

IP Address:

Number of packets:

Packet size:

**Apply** **Cancel** **Help**

- **IP Address** – Target IP to send the ICMP Echo Requests to.
- **Number of packets** – Number of ICMP Echo Request packets to send, up to 10.
- **Packet size** – Size of the packet to send, between 32 and 1500 bytes.

## Ping Example

In this example, the **IP Address** is 192.168.10.1 the **Number of packets** is five. After clicking on **Apply** the firewall will start to send the ICMP Echo Requests to the specified IP. After a few seconds the result will be displayed. In this example, only four out of five packets were received back, a 20% packet loss, and the average time for the packets to travel to and from the specified IP was 57 ms.

Results of pinging 192.168.10.1

Seq	Roundtrip	TTL
1	50 ms	236
2	70 ms	236
3	60 ms	236
5	50 ms	236

5 packets transmitted, 4 packets received, **20%** packet loss.  
Round trip time average: **57 ms**.

## Dynamic DNS

The **Dynamic DNS** (requires Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by a specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.

Click DynDNS in the Tools menu to enter Dynamic DNS configuration.

The firewall provides a list of a few predefined DynDNS service providers. Users must register with one of these providers before trying to use this function.

### Add Dynamic DNS Settings

Follow these steps to enable Dynamic DNS.

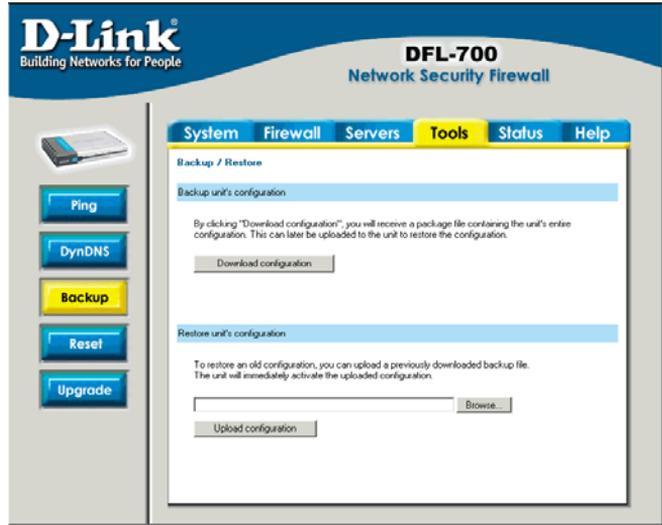
**Step 1.** Go to Tools and DynDNS.

**Step 2.** Choose what Dynamic DNS service you would like to use, and fill in the required information, username and password in all cases and domains in all but cjb.net.

Click the **Apply** button below to apply the settings or click **Cancel** to discard changes.

## Backup

Click on **Tools** in the menu bar, and then click **Backup** below it. Here an administrator can backup and restore the configuration. The configuration file stores system settings, IP addresses of the firewall's network interfaces, address table, service table, IPSec settings, port mapping, and policies. When the configuration process is completed, a system administrator can download the configuration file onto a local disc as a backup. System Administrators



can restore the firewall's configuration file with the one stored on disc.

## Exporting the DFL-700's Configuration

Follow these steps to export the configuration.

**Step 1.** Under the **Tools** menu and the **Backup** section, click on the Download configuration button.

**Step 2.** When the File Download pop-up window appears, choose the destination place in which to save the exported file. The Administrator may choose to rename the file if preferred.

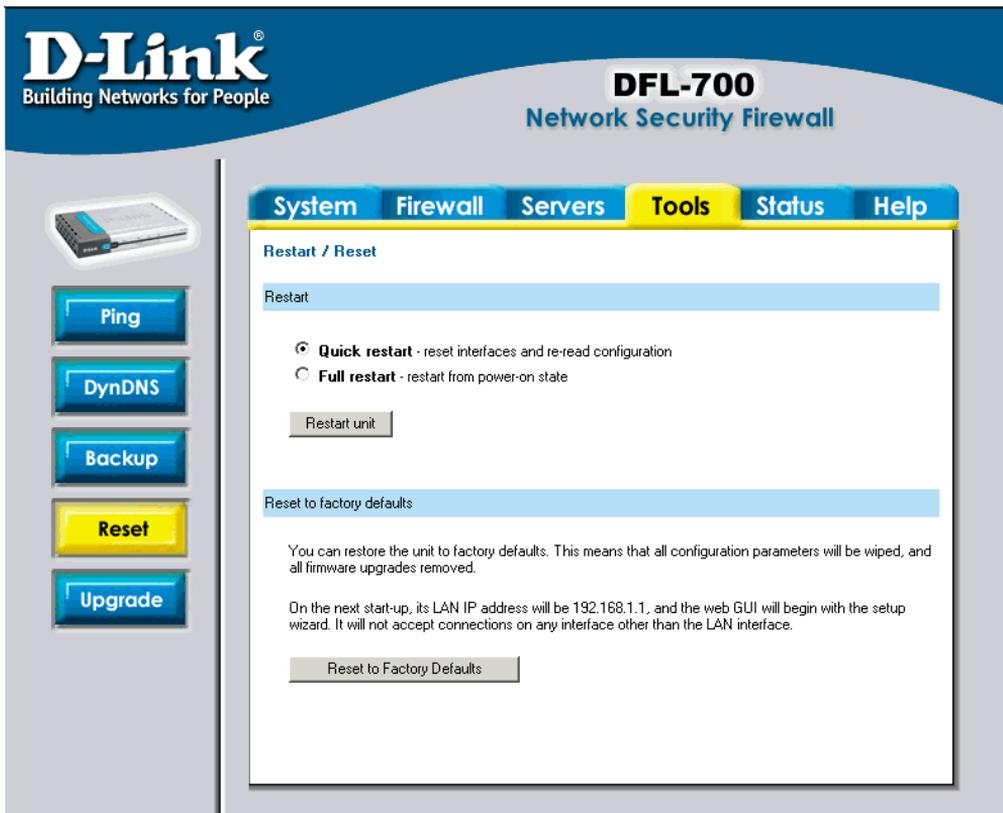
## Restoring the DFL-700's Configuration

Follow these steps to restore the configuration.

**Step 1.** Under the **Tools** menu and the **Backup** section, click on the **Browse** button next to the empty field. When the **Choose File** pop-up window appears, select the file that contains the saved firewall settings, then click **OK**.

**Step 2.** Click **Upload Configuration** to import the file into the firewall.

## Restart/Reset



**D-Link**  
Building Networks for People

**DFL-700**  
Network Security Firewall

System Firewall Servers **Tools** Status Help

Restart / Reset

Restart

**Quick restart** - reset interfaces and re-read configuration

**Full restart** - restart from power-on state

Restart unit

Reset to factory defaults

You can restore the unit to factory defaults. This means that all configuration parameters will be wiped, and all firmware upgrades removed.

On the next start-up, its LAN IP address will be 192.168.1.1, and the web GUI will begin with the setup wizard. It will not accept connections on any interface other than the LAN interface.

Reset to Factory Defaults

### Restarting the DFL-700

Follow these steps restart the DFL-700.

**Step 1.** Choose if you want to do a quick or full restart.

**Step 2.** Click **Restart Unit** and the unit will restart.

### Restoring system settings to factory defaults

Use the following procedure to restore system settings to the factory defaults. This procedure will possibly change the DFL-700 firmware version to a lower version if it has been upgraded.

This procedure deletes all of the changes that you have made to the DFL-700 configuration and reverts the system to its original configuration, including resetting interface addresses.

Follow these steps to reset the DFL-700 to factory default settings.

**Step 1.** Under the **Tools** menu and the **Reset** section, click on the **Reset to Factory Defaults** button.

**Step 2.** Click **OK** in the dialog to reset the unit to factory defaults, or press **Cancel** to cancel.

You can restore your system settings by uploading a previously downloaded system configurations file to the DFL-700 if a backup of the device has been done.

## Upgrade

The DFL-700's software, IDS signatures, and system parameters are all stored on a flash memory card. The flash memory card is re-writable and re-readable.

## Upgrade Firmware

To upgrade the firmware, first download the correct firmware image from D-Link. After downloading the newest version of the software, please store it on the hard disk. Then connect to the firewall's WebUI, enter **Upgrade** on the **Tools** menu, click **Browse**, and choose the file name of the newest version of the firmware. Then click **Upload firmware image**.



The screenshot displays the D-Link DFL-700 Network Security Firewall WebUI. The interface features a top navigation bar with the D-Link logo and the product name. Below the navigation bar, there are several menu items: System, Firewall, Servers, Tools (highlighted in yellow), Status, and Help. On the left side, there is a vertical sidebar with buttons for Ping, DynDNS, Backup, Reset, and Upgrade (highlighted in yellow). The main content area is titled 'Upgrade' and contains two sections: 'Upgrade unit's firmware' and 'Upgrade unit's signature-database'. Each section includes instructions on how to upgrade and a form with a 'Browse...' button and an 'Upload' button. A red cross icon labeled 'Help' is located in the bottom right corner of the main content area.

The updating process will not overwrite the system configuration. Though it is not necessary, it is a good idea to backup the system configuration before upgrading the software.

## Upgrade IDS Signature-database

To upgrade the signature-database first download the newest IDS signatures from D-Link. After downloading the newest version of the software, connect to the firewall's WebUI, enter **Upgrade** on the **Tools** menu, click **Browse** in the **Upgrade Unit's signature-database** section, and choose the file name of the newest version of the IDS signatures. Then click **Upload signature database**.

# Status

In this section, the DFL-700 displays the status information about the Firewall.

Administrator may use Status to check the System Status, Interface statistics, VPN, connections, and DHCP Servers.

## System

Click on **Status** in the menu bar, and then click **System** below it. A window will appear providing some information about the DFL-700.

**Uptime** – The time the firewall has been running, since the last reboot or start.

**CPU Load** – Percentage of cpu used.

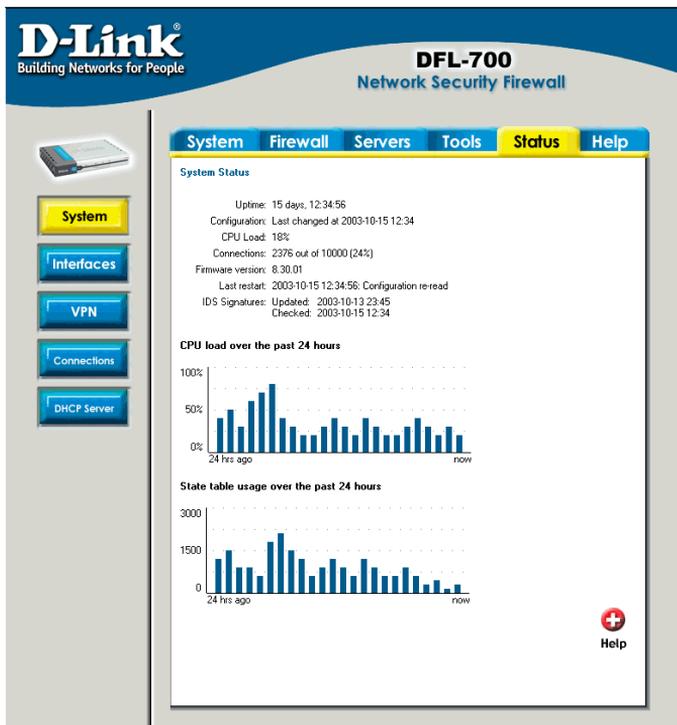
**Connections** – Number of current connections trough the firewall.

**Firmware version** – The firmware version running on the firewall.

**Last restart** – The reason for the last restart.

**IDS Signatures** – The IDS signature versions.

There are also two graphs on this page; one shows the CPU usage during the last 24 hours. The other shows the state table usage during the last 24 hours.



## Interfaces

Click on **Status** in the menu bar, and then click **Interfaces** below it. A window will appear providing information about the interfaces on the DFL-700. By default, information about the **LAN** interface will be displayed. To see another one, click on that interface (**WAN** or **DMZ**).

**Interface** – Name of the interface shown, LAN, WAN, or DMZ.

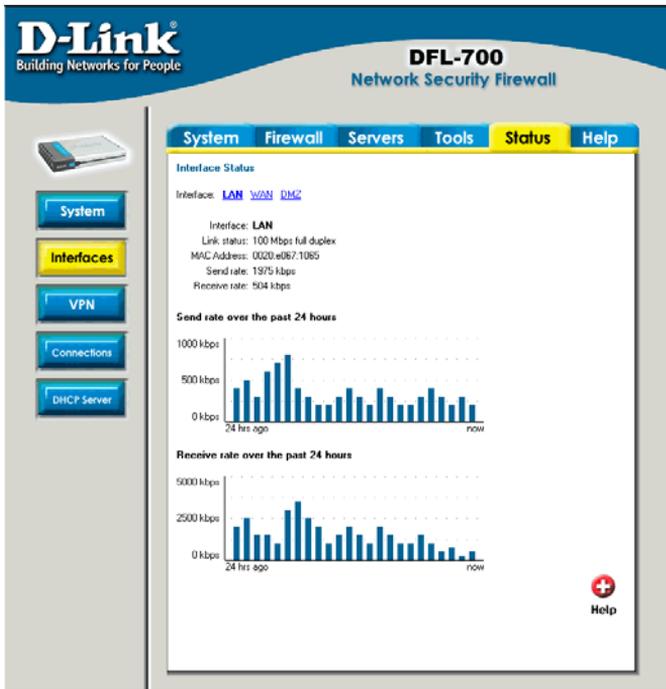
**Link status** – Displays what link the current interface has. The speed can be 10 or 100 Mbps and the duplex can be Half or Full.

**MAC Address** – MAC address of the interface.

**Send rate** – Current amount of traffic sent through the interface.

**Receive rate** – Current amount of traffic received through the interface.

There are also two graphs displaying the send and receive rate through the interfaces during the last 24 hours.



# VPN

Click on **Status** in the menu bar, and then click **Interfaces** below it. A window will appear providing information about the VPN connections on the DFL-700. By default information about the first VPN tunnel will be displayed. To see another one, click on that VPN tunnels name.

The two graphs display the send and receive rate trough the selected VPN tunnel during the last 24 hours.

In this example, a tunnel named **RoamingUsers** is selected. This is a tunnel that allows roaming users. So under the IPsec SA listing each roaming user connected to this tunnel is shown.

The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes System, Firewall, Servers, Tools, Status (highlighted), and Help. On the left, a sidebar contains buttons for System, Interfaces, VPN (highlighted), Connections, and DHCP Server. The main content area is titled 'VPN Status' and shows 'VPN Tunnels: vportunnel1 vportunnel2 **RoamingUsers**'. Below this are two bar charts: 'Send rate over the past 24 hours' (0-500 kbps) and 'Receive rate over the past 24 hours' (0-200 kbps). At the bottom, a table lists IPsec SAs for the selected tunnel 'RoamingUsers'.

Gateway	Local Net	Remote Net	
172.16.0.7	192.168.1.0/24	172.16.0.7	<a href="#">[Close]</a>
172.16.0.11	192.168.1.0/24	172.16.0.11	<a href="#">[Close]</a>
172.16.0.15	192.168.1.0/24	172.16.0.15	<a href="#">[Close]</a>
172.17.0.23	192.168.1.0/24	172.17.0.23	<a href="#">[Close]</a>

## Connections

Click on **Status** in the menu bar, and then click **Connections** below it. A window will appear providing information about the content of the state table.

The state table shows the last 100 connections opened through the firewall. Connections are created when traffic is permitted to pass via the policies.

Each connection has two timeout values, one in each direction. These are updated when the firewall receives packets from each end of the connection. The value shown in the **Timeout** column is the lower of the two values.

Possible values in the **State** column include: TCP\_CLOSE, TCP\_OPEN, SYN\_RECV, FIN\_RECV, and so on.

The **Proto** column can have:

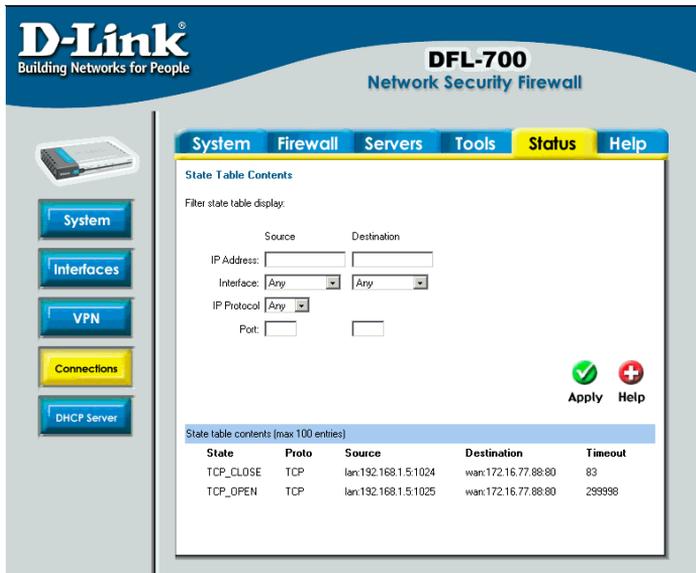
**TCP** - The connection is a TCP connection.

**PING** - The connection is an ICMP ECHO connection.

**UDP** - The connection is a UDP connection.

**RAWIP** - The connection uses an IP protocol other than TCP, UDP, or ICMP.

The **Source** and **Destination** columns show which IP and port on the source interface the connection is coming from, and which interface and port number the connection is going to.



The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Status' tab is selected. On the left sidebar, there are buttons for 'System', 'Interfaces', 'VPN', 'Connections', and 'DHCP Server'. The main content area is titled 'State Table Contents' and includes a 'Filter state table display:' section with input fields for 'Source' and 'Destination' (IP Address, Interface, IP Protocol, Port). Below the filter section is a table showing the state table contents (max 100 entries).

State	Proto	Source	Destination	Timeout
TCP_CLOSE	TCP	lan:192.168.1.5:1024	wan:172.16.77.88:80	83
TCP_OPEN	TCP	lan:192.168.1.5:1025	wan:172.16.77.88:80	293998

## DHCP Server

Click on **Status** in the menu bar, and then click **DHCP Server** below it. A window will appear providing information about the configured DHCP Servers. By default, information about the **LAN** interface will be displayed. To see another one, click on that interface.

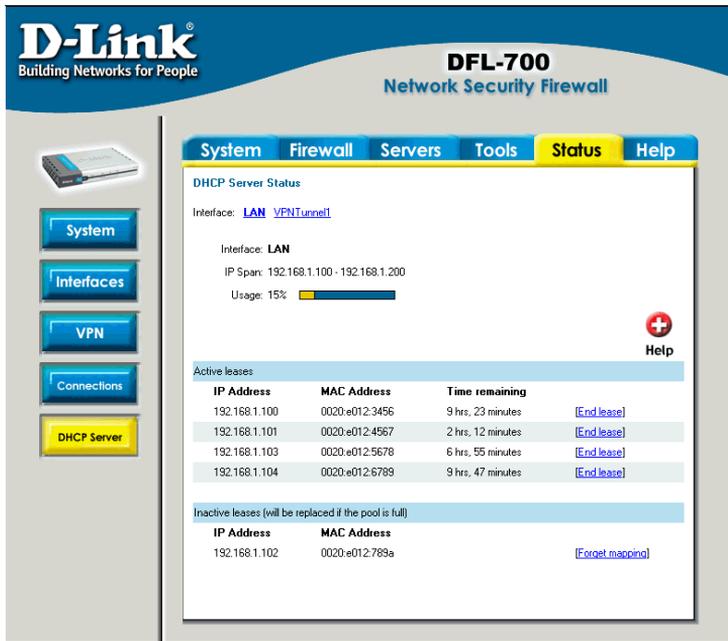
**Interface** – Name of the interface the DHCP Server is running on.

**IP Span** – Displays the configured ranges of IP's that are given out as DHCP leases.

**Usage** – Displays how much of the IP range is give out to DHCP clients.

**Active leases** are the current computers using this DHCP server. It is also possible to end a computers lease on this screen by clicking on **End lease** corresponding to that IP.

**Inactive leases** are leases that are not currently in use but have been used by a computer before. That computer will get the lease the next time it is on the network. If there is no free IP in the pool these IP's will be used for new computers.



**D-Link**  
Building Networks for People

**DFL-700**  
Network Security Firewall

System Firewall Servers Tools **Status** Help

DHCP Server Status

Interface: [LAN](#) [VPN Tunnel](#)

Interface: **LAN**

IP Span: 192.168.1.100 - 192.168.1.200

Usage: 15%

**Active leases**

IP Address	MAC Address	Time remaining	
192.168.1.100	0020:e012:3456	9 hrs, 23 minutes	<a href="#">[End lease]</a>
192.168.1.101	0020:e012:4567	2 hrs, 12 minutes	<a href="#">[End lease]</a>
192.168.1.103	0020:e012:5678	6 hrs, 55 minutes	<a href="#">[End lease]</a>
192.168.1.104	0020:e012:6789	9 hrs, 47 minutes	<a href="#">[End lease]</a>

**Inactive leases (will be replaced if the pool is full)**

IP Address	MAC Address	
192.168.1.102	0020:e012:789a	<a href="#">[Forget mapping]</a>

# How to read the logs

Although the exact format of each log entry depends on how your syslog recipient works, most are very similar. The way in which logs are read is also dependent on how your syslog recipient works. Syslog daemons on UNIX servers usually log to text files, line by line.

Most syslog recipients preface each log entry with a timestamp and the IP address of the machine that sent the log data:

```
Oct 20 2003 09:45:23 gateway
```

This is followed by the text the sender has chosen to send. All log entries from the DFL-700 are prefaced with "EFW:" and a category, e.g. "DROP:"

```
Oct 20 2003 09:45:23 gateway EFW: DROP:
```

Subsequent text is dependent on the event that has occurred.

## USAGE events

These events are sent periodically and provide statistical information regarding connections and amount of traffic.

### Example:

```
Oct 20 2003 09:45:23 gateway EFW: USAGE: conns=1174 if0=core ip0=127.0.0.1  
tp0=0.00 if1=wan ip1=192.168.10.2 tp1=11.93 if2=lan ip2=192.168.0.1 tp2=13.27 if3=dmz  
ip3=192.168.1.1 tp3=0.99
```

The value after "conns" is the number of open connections through the firewall when the usage log was sent. The value after "tp" is the throughput through the firewall at the time the usage log was logged.

## DROP events

These events may be generated by a number of different functions in the firewall. The most common source is the policies.

### Example:

```
Oct 20 2003 09:42:25 gateway EFW: DROP: prio=1 rule=Rule_1 action=drop recvif=wan  
srcip=192.168.10.2 destip=192.168.0.1 ipproto=TCP ipdatalen=28 srcport=3572 destport=135  
tcphdrLen=28 syn=1
```

In this line, traffic from 192.168.10.2 coming from the WAN side of the firewall, connecting to 192.168.10.1 on port 135 is dropped. The protocol used is TCP.

## CONN events

These events are generated if auditing has been enabled.

One event will be generated when a connection is established. This event will include information about the protocol, receiving interface, source IP address, source port, destination interface, destination IP address, and destination port.

**Open Example:**

*Oct 20 2003 09:47:56 gateway EFW: CONN: prio=1 rule=Rule\_8 conn=open  
connipproto=TCP connrecvif=lan connsrcip=192.168.0.10 connsrcport=3179 conndestif=wan  
conndestip=64.7.210.132 conndestport=80*

In this line, traffic from 192.168.0.10 on the LAN interface is connecting to 64.7.210.132 on port 80 on the WAN side of the firewall (internet).

Another event is generated when the connection is closed. The information included in the event is the same as in the event sent when the connection was opened, with the exception that statistics regarding sent and received traffic is also included.

**Close Example:**

*Oct 20 2003 09:48:05 gateway EFW: CONN: prio=1 rule=Rule\_8 conn=close  
connipproto=TCP connrecvif=lan connsrcip=192.168.0.10 connsrcport=3179 conndestif=wan  
conndestip=64.7.210.132 conndestport=80 origsent=62 termsent=60*

In this line, the connection in the other example is closed.

# Appendixes

## Appendix A: ICMP Types and Codes

The Internet Control Message Protocol (ICMP) has many messages that are identified by a "type" field; many of these ICMP types have a "code" field. Here we list the types with their assigned code fields.

Type	Name	Code	Description	Reference
0	Echo Reply	0	No Code	RFC792
3	Destination Unreachable	0	Net Unreachable	RFC792
		1	Host Unreachable	RFC792
		2	Protocol Unreachable	RFC792
		3	Port Unreachable	RFC792
		4	Fragmentation Needed and Don't Fragment was Set	RFC792
		5	Source Route Failed	RFC792
		6	Destination Network Unknown	RFC792
		7	Destination Host Unknown	RFC792
		8	Source Host Isolated	RFC792
		9	Communication with Destination Network is Administratively Prohibited	RFC792
		10	Communication with Destination Host is Administratively Prohibited	RFC792
		11	Destination Network Unreachable for Type of Service	RFC792
12	Destination Host Unreachable for Type of Service	RFC792		
13	Communication Administratively Prohibited	RFC1812		
14	Host Precedence Violation	RFC1812		
15	Precedence cutoff in effect	RFC1812		
4	Source Quench	0	No Code	RFC792
5	Redirect	0	Redirect Datagram for the Network (or subnet)	RFC792

		1	Redirect Datagram for the Host	RFC792
		2	Redirect Datagram for the Type of Service and Network	RFC792
		3	Redirect Datagram for the Type of Service and Host	RFC792
8	Echo	0	No Code	RFC792
9	Router Advertisement	0	Normal router advertisement	RFC1256
		16	Does not route common traffic	RFC2002
10	Router Selection	0	No Code	RFC1256
11	Time Exceeded	0	Time to Live exceeded in Transit	RFC792
		1	Fragment Reassembly Time Exceeded	RFC792
12	Parameter Problem	0	Pointer indicates the error	RFC792
		1	Missing a Required Option	RFC1108
		2	Bad Length	RFC792
13	Timestamp	0	No Code	RFC792
14	Timestamp Reply	0	No Code	RFC792
15	Information Request	0	No Code	RFC792
16	Information Reply	0	No Code	RFC792
17	Address Mask Request	0	No Code	RFC950
18	Address Mask Reply	0	No Code	RFC950
30	Traceroute			RFC1393
31	Datagram Conversion Error			RFC1475
40	Photuris			RFC2521
		0	Bad SPI	RFC2521
		1	Authentication Failed	RFC2521
		2	Decompression Failed	RFC2521
		3	Decryption Failed	RFC2521
		4	Need Authentication	RFC2521
		5	Need Authorization	RFC2521

Source: <http://www.iana.org/assignments/icmp-parameters>

## Appendix B: Common IP Protocol Numbers

These are some of the more common IP Protocols. For a list of all protocols, follow the link after the table.

Decimal	Keyword	Description	Reference
1	ICMP	Internet Control Message	RFC792
2	IGMP	Internet Group Management	RFC1112
3	GGP	Gateway-to-Gateway	RFC823
4	IP	IP in IP (encapsulation)	RFC2003
5	ST	Stream	RFC1190, RFC1819
6	TCP	Transmission Control	RFC793
8	EGP	Exterior Gateway Protocol	RFC888
17	UDP	User Datagram	RFC768
47	GRE	General Encapsulation	Routing
50	ESP	Encapsulation Payload	Security RFC2406
51	AH	Authentication Header	RFC2402
108	IPComp	IP Payload Compression Protocol	RFC2393
112	VRRP	Virtual Router Redundancy Protocol	
115	L2TP	Layer Two Tunneling Protocol	

Source: <http://www.iana.org/assignments/protocol-numbers>

## LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor.

**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”) if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

<b><i>Product Type</i></b>	<b><i>Warranty Period</i></b>
Product (excluding power supplies and fans)	One (1) Year
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 may 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 Card.** The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. **FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD 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 claim must include 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 packaged product shall be insured and shipped to D-Link, 17595 Mt. Herrmann Street Fountain Valley, CA 92708 USA, with all shipping costs prepaid. 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 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 Limited 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.

### **Wichtige Sicherheitshinweise**

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.

13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  - a – Netzkabel oder Netzstecker sind beschädigt.
  - b – Flüssigkeit ist in das Gerät eingedrungen.
  - c – Das Gerät war Feuchtigkeit ausgesetzt.
  - d – Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  - e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  - f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Reparatur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm<sup>2</sup> einzusetzen.

## **Trademarks**

Copyright ©2002 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 B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

## **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum 20cm between the radiator and your body.

The Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la class B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

# International Offices

## U.S.A

17595 Mt. Herrmann Street  
Fountain Valley, CA. 92708  
TEL: 714-885-6000  
Fax 866-743-4905  
URL: www.dlink.com

## Canada

2180 Winston Park Drive  
Oakville, Ontario, L6H 5W1  
Canada  
TEL: 1-905-8295033  
FAX: 1-905-8295223  
URL: www.dlink.ca

## Europe (U. K.)

4<sup>th</sup> Floor, Merit House  
Edgware Road, Colindale  
London NW9 5AB  
U.K.  
TEL: 44-20-8731-5555  
FAX: 44-20-8731-5511  
URL: www.dlink.co.uk

## Germany

Schwalbacher Strasse 74  
D-65760 Eschborn  
Germany  
TEL: 49-6196-77990  
FAX: 49-6196-7799300  
URL: www.dlink.de

## France

Le Florilege #.2, Allee de la Fresnerie  
78330 Fontenay le Fleury  
France  
TEL: 33-1-30238688  
FAX: 33-1-30238689  
URL: www.dlink-france.fr

## Netherlands

Weena 290  
3012 NJ Rotterdam  
Netherlands  
Tel: +31-10-282-1445  
Fax: +31-10-282-1331  
URL: www.dlink-benelux.com

## Belgium

Rue des Colonies 11  
B-1000 Brussels  
Belgium  
Tel: +32(0)2 517 7111  
Fax: +32(0)2 517 6500  
URL: www.dlink-benelux.com

## Italy

Via Nino Bonnet n. 6/b  
20154 – Milano,  
Italy  
TEL: 39-02-2900-0676  
FAX: 39-02-2900-1723  
URL: www.dlink.it

## Sweden

P.O. Box 15036, S-167 15 Bromma  
Sweden  
TEL: 46-(0)8564-61900  
FAX: 46-(0)8564-61901  
URL: www.dlink.se

## Denmark

Naverland 2, DK-2600  
Glostrup, Copenhagen,  
Denmark  
TEL: 45-43-969040  
FAX: 45-43-424347  
URL: www.dlink.dk

## Norway

Karihaugveien 89  
1086 Oslo  
Norway  
TEL: 47-22-309075  
FAX: 47-22-309085  
URL: www.dlink.no

## Finland

Pakkalankuja 7A  
01510 Vantaa,  
Finland  
TEL : +358-9-2707 5080  
FAX: + 358-9-2707 5081  
URL: www.dlink.fi

## Iberia

C/Sabino De Arana,  
56 Bajos  
08028 Barcelona  
TEL: 34 93 4090770  
FAX: 34 93 4910795  
URL: www.dlinkiberia.es

## Singapore

1 International Business Park  
#03-12 The Synergy  
Singapore 609917  
TEL: 65-6774-6233  
FAX: 65-6774-6322  
URL: www.dlink-intl.com

## Australia

1 Giffnock Avenue,  
North Ryde, NSW 2113  
Australia  
TEL: 61-2-8899-1800  
FAX: 61-2-8899-1868  
URL: www.dlink.com.au

## India

D-Link House, Kurla Bandra Complex Road,  
Off CST Road, Santacruz (East), Mumbai -  
400098.  
India  
TEL: 91-022-26526696/56902210  
FAX: 91-022-26528914  
URL: www.dlink.co.in

## Middle East (Dubai)

P.O.Box: 500376  
Office No.:103, Building:3  
Dubai Internet City  
Dubai, United Arab Emirates  
Tel:+971-4-3916480  
Fax:+971-4-3908881  
URL: www.dlink-me.com

## Turkey

Regus Offices  
Beybi Giz Plaza, Ayazaga Mah. Meydan Sok.  
No:28  
Maslak 34396, Istanbul-Turkiye  
TEL: +90 212 335 2553  
FAX: +90 212 335 2500  
URL: www.dlink.com.tr

## Egypt

19 El-Shahed Helmy, El Masri  
Al-Maza, Heliopolis  
Cairo, Egypt.  
TEL: +202 414 4295  
FAX: +202 415 6704  
URL: www.dlink-me.com

## Israel

11 Hamanofim Street  
Ackerstein Towers, Regus Business Center  
P.O.B 2148, Hertzelia-Pituach 46120.  
Israel  
TEL: +972-9-9715700  
FAX: +972-9-9715601  
URL: www.dlink.co.il

## LatinAmerica

Isidora Goyechea 2934 of 702,  
Las Condes  
Santiago – Chile S.A.  
TEL: 56-2-232-3185  
FAX: 56-2-232-0923  
URL: www.dlink.cl

## Brasil

Av das Na--es Unidas, 11857,  
cj 132 - Brooklin Novo  
S-o Paulo - SP - Brazil  
04578-000  
TEL: (55 11) 550 39320  
Fax: (55 11) 550 39321

## South Africa

Einstein Park II  
Block B  
102-106 Witch-Hazel Avenue  
Highveld Technopark  
Centurion  
Gauteng  
Republic of South Africa  
TEL: 27-12-665-2165  
FAX: 27-12-665-2186  
URL: www.d-link.co.za

## Russia

Grafsky per., 14, floor 6  
Moscow  
129626 Russia  
TEL: 7-095-744-0099  
FAX: 7-095-744-0099 #350  
URL: www.dlink.ru

## China

Room 507/508, Tower W1,  
The towers Oriental Plaza NO.1,  
East Chang An Ave.,  
Dong Cheng District Beijing ,  
100738, China.  
TEL +86-010-85182533  
FAX: +86-010-85182250  
URL: www.dlink.com.cn

## Taiwan

2F, No. 119, Pao-Chung Rd.  
Hsin-Tien, Taipei  
Taiwan  
TEL: 886-2-2910-2626  
FAX: 886-2-2910-1515  
URL: www.dlinktw.com.tw

## Headquarters

2F, No. 233-2, Pao-Chiao Rd.  
Hsin-Tien, Taipei  
Taiwan  
TEL: 886-2-2916-1600  
FAX: 886-2-2914-6299  
URL: www.dlink.com.tw

# 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®**