D-Link DFL-700

NETDEFEND™

Network Security Firewall

Manual

D-Link®

Building Networks for People

(04/18/2005)

Contents

Introduction

The DFL-700 provides three 10/100Mbps Ethernet network interface ports, which are (1) Internal/LAN, (1) External/WAN, and (1) DMZ port. In addition the DFL-700 also provides a user-friendly Web UI that allows users to set system parameters or monitor network activities using a Web browser supporting Java.

Features and Benefits

- **Firewall Security**

- **VPN Server/Client Supported**
  Supports IPSec LAN-to-LAN or Roaming user tunnels with AES encryption in addition to PPTP and IPSec over L2TP

- **Content Filtering**
  Strip ActiveX objects, Java Applets, JavaScript, and VBScript from HTTP traffic

- **Bandwidth Management**
  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 assignment of 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. Firewalls are also deployed to prevent sensitive information about your network from leaking out of your network.

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 occasionally to indicate a functional, active system. Solid illumination of the Status LED indicates a hardware/software critical failure.

WAN, LAN, & DMZ: Bright Green illumination indicates a valid Ethernet Link on that respective port. Each LED will flicker when that respective port is sending or receiving data.

Physical Connections

COM Port: Serial Read-Only access to the firewall software from a PC equipped with a Serial COM port (9600 baud, 8 data bits, No Parity, 1 Stop bit, No Flow Control).

LAN Port: Use this port to connect to a Fast Ethernet Switch to service more than 1 client PC on the internal office network.

DMZ Port: Use this port to service an additional physically segmented Private or Transparent Network to be occupied by WAN accessible servers (FTP, HTTP, DNS).

WAN Port: Use this port to connect to an external network, such as a WAN or a modem provided by an ISP.

Reset: Use this switch to reset the DFL-700 to factory default settings. Refer to page 67 for further instructions.

DC Power: Use the included 5VDC 3A switching power supply to connect to an 110/120VAC electrical receptacle. Do not use less than 5VDC 3A to power the device, doing so will damage the unit.

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
- RS-232 Null Modem Cable

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

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

System Requirements

- Computer running Microsoft Windows, Macintosh OS, or a UNIX based operating system with an installed Ethernet adapter configured to communicate using TCP/IP.
- 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 complete, those 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, otherwise the DFL-700 will revert to the previous configuration. The timeout 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 first press and hold the reset button. Power on the unit, and continue to hold the reset button for at least 15 seconds. You will first hear one beep, which indicates that the default configuration restoration has started. Keep the button pressed in until you hear two consecutive beeps shortly after each other. 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

Management web GUI ports

HTTP Port: 80

HTTPS Port: 443

For security reasons, it may be better to run the management web GUI on non-standard ports. Also note that if web-based user authentication is enabled, ports 80 and 443 will be taken; the management web GUI has to use other ports.

Apply   Cancel   Help

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 a user with both admin and read-only rights logs on from a somewhere where only read-only access is allowed, the user will be allowed to log on, but will receive read-only access only.

Administrative access via **LAN** interface   [Edit]

Ping:	Any address
Admin:	Any address (HTTPS only)
Read-only:	Any address (HTTPS only)
SNMP:	Any address
	Read Community: "public"

Administrative access via **WAN** interface   [Edit]

Ping:	Any address
Admin:	Any address (HTTPS only)

Administrative access via **IPSec_tunnel** vpn tunnel   [Edit]

Ping:	Any address
Admin:	Any address (HTTPS only)

Add administrative access via:

Interface:	DMZ
VPN Tunnel:	

Management UI Ports – The ports for the DFL-700's Web Server Management UI (HTTP and HTTPS) can be customized if so desired. These values must change if User Authentication is enabled (User Authentication uses 80 and 443 to accomplish user login).

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**. In the case where Read-Only access is the only type allowed on a specific interface, all users that log in to that interface 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 network addresses should be allowed to ping the interface, for example 192.168.1.0/24 for a whole class C network or 172.16.0.1 – 172.16.0.10 for a range of IP addresses.

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: 192.168.1.0/24

Add Admin access to an interface

To add admin access, click on the interface you would like to add it to. Only users with administrative 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 network addresses should be allowed to access the administrative interface, for example 192.168.1.0/24 for a whole class C network or 172.16.0.1 – 172.16.0.10 for a range of IP addresses.

Step 4. Specify protocol to be used to access the DFL-700 via the dropdown menu. Select **HTTP and HTTPS** (Secure HTTP) or **HTTPS only**.

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

Example:

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

Networks: 1.0.0.0 - 223.255.255.255

Protocol: HTTPS only

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 network addresses should be allowed read-only access to the interface, for example 192.168.1.0/24 for a whole class C network or 172.16.0.1 – 172.16.0.10 for a range of IP addresses.

Step 4. Specify protocol to be used to access the DFL-700 via the dropdown menu. Select **HTTP and HTTPS** (Secure HTTP) or **HTTPS only**.

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: `172.16.0.1 - 172.16.0.10`

    Protocol: `HTTP and HTTPS ▼`

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 network addresses should be allowed to receive SNMP traps, for example 192.168.1.0/24 for a whole class C network or 172.16.0.1 – 172.16.0.10 for a range of IP addresses.

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: `192.168.1.10`

    Community: `MySecretCommunity`

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: 192.168.0.1

Subnet Mask: 255.255.255.0   - 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. This configuration will determine the IP addresses that can communicate with this interface.

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

Please keep in mind that the DHCP scope will also need to be changed to correspond with the new LAN IP. If the computer through which the DFL-700 is being configured is a DHCP client, you will need to manually release and renew the IP address after applying changes and restarting. Failure to follow these directions will result in the firewall configuration reverting back to the state prior to changing the LAN IP.

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.

Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type: [Static IP ▼]

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

IP Address: [192.168.10.2]
Subnet Mask: [255.255.255.0] - 256 hosts (/24) ▼
Gateway IP: [192.168.10.1]
Primary DNS Server: [10.0.0.1]
Secondary DNS Server: [10.0.0.2] (optional)

- **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.

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: [DHCP ▼]

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.

Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type: PPPoE

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)

- **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.

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.

Interface Settings

Edit settings of the **WAN** interface:

Change WAN Type: [PPTP ▼]

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: [255.255.255.0   - 256 hosts (/24) ▼]
   Gateway IP: [   ]
   This may or may not be necessary, depending on the ISP.

- **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.

Before PPTP can be used to connect to your ISP, the physical (WAN) interface parameters must be input. 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 L2TP

L2TP 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 L2TP 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.

- **L2TP Server IP** – The IP of the L2TP server that the DFL-700 will connect to.

Before L2TP can be used to connect to your ISP, the physical (WAN) interface parameters must be input. 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 L2TP server.

- **Subnet Mask** – Size of the external network.

- **Gateway IP** – Specifies the IP address of the default gateway used to access the Internet. Contact your ISP if you are unsure of the necessity of this information.

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: Big Pond ▾

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's possible to control whichever 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 then 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: 1500   bytes.   Upper limit: 1500

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				[Edit]
LAN	192.168.1.0/24				[Edit]
WAN	0.0.0.0/0	194.1.2.254			[Edit]
LAN	192.168.5.0/24		192.168.5.1		[Edit]
VPNTunnel1	192.168.2.0/24			Yes	[Edit]
[Add new]					

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.

Additional 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 interface IP address of the firewall 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 major difference between this form of notation and the form most commonly used is there is no need to specify the interface name in a separate column. Instead, you specify the IP address of each interface as a gateway.

Note: Proxy ARP will publish the remote network on all interfaces (except WAN) if enabled on the VPN tunnel.

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.

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, are mandatory and will always generate log entries. Other events, for instance 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 when running third party log analyzers on the logs or to see how much traffic specific connections account for.

Follow these steps to enable auditing.

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 synchronizing with an Internet Network Time Server (NTP) or by entering the system time manually.

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. Simply make a list of usernames separated by commas (,), specify an entire user group, or write **Any** to indicate all authenticated users to enable authentication on this policy. 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 **–** 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 uses both the TCP and UDP protocols.

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 will protect the networks behind the DFL-700 by dropping the traffic. To notify responsible parties of the malicious attack, the IDS will send e-mails to the system administrators if e-mail alerting is enabled and configured. 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 then 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 traffic using a policy 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.

Position: Moves before given position.

Action: Select **Allow** to allow the specified service traffic to traverse the firewall. Choose **Deny** to drop all traffic matching the criteria of the specified service.

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.

Note: *Refer to Appendix C of the manual for details on mapping Public IP addresses to Internal Servers.*

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 **Inspection Only** 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 (such as a LAN Web server) on the LAN or DMZ Interfaces to be accessible through the WAN. One may also regulate how bandwidth management (traffic shaping) is applied to traffic flowing through the WAN interface of the firewall to the LAN or DMZ. It is also possible to use Intrusion Detection / Prevention 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. Click on the **Add new** link.

   Step 2. 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 IP: Leave empty to use the WAN IP of the firewall, or enter an additional IP address to be forwarded to the specified Pass To address.

   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.

   Note: *Refer to Appendix C of the manual for details on mapping Public IP addresses to Internal Servers.*

Delete mapping

Follow these steps to delete a mapping.

Step 1. Choose the mapping list (WAN, LAN, or DMZ) you would like do 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 show all the users, and the first section is the administrative users.

Administrative users		
Admin:	admin	**[Add]**
Read-only:	auditor	**[Add]**

The first column shows 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 shows the users in each access level.

Add Administrative User

Follow these steps to add a new administrative user.

Step 1. Click on **add** after 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 the password for the new user.

User Management

Edit user **admin**:

User name:	admin
Group membership:	administrators
☐ **Change password**	
Password:	‖‖‖
Retype password:	‖‖‖

Click the **Apply** button below to apply the setting 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 lever of a user click on the user name and you will see the following screen. From here you can change the access level by entering the appropriate level in the **Group Membership** field.

User Management

Edit user **admin**:

User name:	admin
Group membership:	administrators

☐ **Change password**

Password:	‖‖‖
Retype password:	‖‖‖

L2TP/PPTP settings:

Static client IP: _____ If empty, the IP address will be taken from the server's IP pool

Networks behind user: _____

☐ **Delete user**

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.

Apply   Cancel   Help

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.

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 by entering into the Group **Membership Field**.

Click the **Apply** button below to apply the setting 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 you would like to change level of.

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

Step 3. Enter the new password twice.

User Management

Edit user **admin**:

User name:	admin
Group membership:	administrators

☐ **Change password**

Password:	‖‖‖
Retype password:	‖‖‖

Click the **Apply** button below to apply the setting 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.

User Management

Edit user **admin**:

User name:	admin
Group membership:	administrators

☐ **Change password**

Password:	|||||
Retype password:	|||||

L2TP/PPTP settings:

Static client IP: [   ]
If empty, the IP address will be taken from the server's IP pool

Networks behind user: [   ]

☐ **Delete user**

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.

Apply   Cancel   Help

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

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

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 do 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 DFL-700 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 web-based management GUI to listen on since enabling user authentication requires the default ports for user login purposes (80 and 443).

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.

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.

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

User Management

Add new user:

User name:

Group membership:

Password:

Retype password:

L2TP/PPTP settings:

Static client IP: If empty, the IP address will be taken from the server's IP pool

Networks behind user:

Apply   Cancel   Help

Select a user to edit from the below list, or select "Add new":

Administrative users
Admin: admin   [Add]
Read-only: [Add]

Users in local database
User name   Groups   Client IP
ange
[Add new]

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 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.

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

User Management

Edit user **Todd**:

User name: Todd

Group membership: NetDefend

☑ **Change password**

Password:

Retype password:

☐ **Delete user**

Apply   Cancel   Help

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.

User Management

Edit user **Todd**:

User name: Todd

Group membership: NetDefend

☐ **Change password**

Password: |||||

Retype password: |||||

☑ **Delete user**

Apply Cancel Help

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

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.

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.
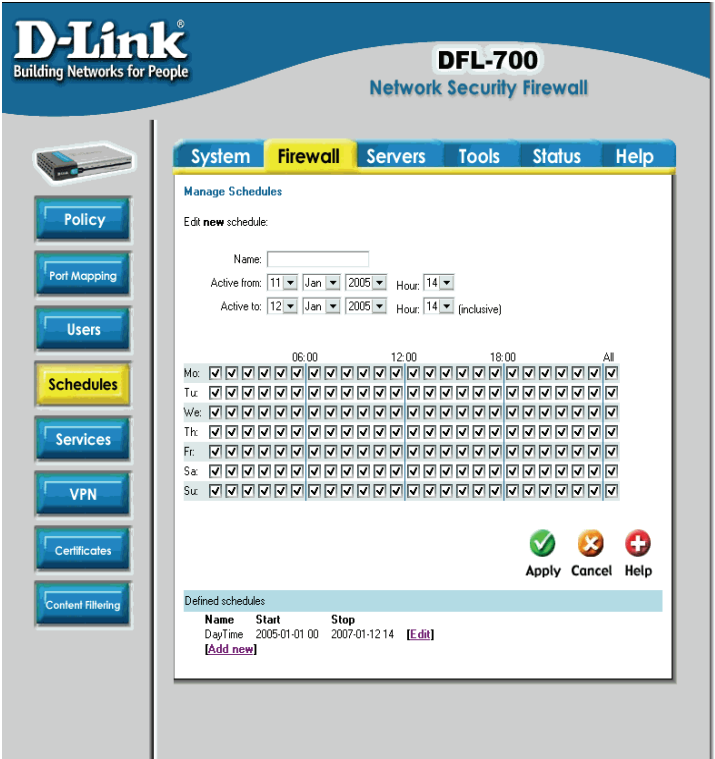
Add new one-time schedule

Follow these steps to create and 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 (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 – Similar to the way most stateful inspection firewalls behave, the DFL-700 filters only information found in packet headers, such as IP, TCP, UDP, or 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 (ALG).

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

Introduction to IPSec

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 that of the DFL-700, is made up of two basic parts:

- Internet Key Exchange security protocol (IKE)

- IPSec protocol (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 (SA), for each connection. Each SA is unidirectional, so there will be at least two SA 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 an IPSec 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.

Introduction to PPTP

PPTP, Point-to-Point Tunneling Protocol, jointly developed by Microsoft, US Robotics, and various other remote access companies known collectively as the PPTP Forum, is used to provide IP security at the network layer.

A PPTP based VPN is made up by these parts:

- Point-to-Point Protocol (PPP)

- Authentication Protocols (PAP, CHAP, MS-CHAP v1, MS-CHAP v2)

- Microsoft Point-To-Point Encryption (MPPE)

- Generic Routing Encapsulation (GRE)

PPTP uses TCP port 1723 for it's control connection and uses GRE (IP protocol 47) for the PPP data. PPTP supports data encryption by using MPPE.

Introduction to L2TP

L2TP, Layer 2 Tunneling Protocol, a combination of Microsoft's PPTP and Cisco's L2F (Layer 2 Forwarding), is used to provide IP security at the network layer.

An L2TP based VPN is made up by these parts:

- Point-to-Point Protocol (PPP)
- Authentication Protocols (PAP, CHAP, MS-CHAP v1, MS-CHAP v2)
- Microsoft Point-To-Point Encryption (MPPE)

L2TP uses UDP to transport the PPP data, this is often encapsulated in IPSec for encryption instead of using MPPE.

Point-to-Point Protocol

PPP (Point-to-Point Protocol) is a standard for transporting datagram's over point-to-point links. PPP is used to encapsulate IP packets for transport between two peers.

PPP consists of these three components:

- Link Control Protocols (LCP) to negotiate parameters, test and establish the link.
- Network Control Protocol (NCP) to establish and negotiate different network

  layer protocols (DFL-700 only supports IP)
- Data encapsulation to encapsulate datagram's over the link.

To establish a PPP tunnel, both sides send LCP frames to negotiate parameters and test the data link. If authentication is used, at least one of the peers has to authenticate itself before the network layer protocol parameters can be negotiated using NCP. During the LCP and NCP negotiation optional parameters such as encryption, can be negotiated. When LCP and NCP negotiation is done, IP datagram's can be sent over the link.

Authentication Protocols

PPP supports different authentication protocols, PAP, CHAP, MS-CHAP v1 and MSCHAP v2. The authentication protocol to be used is decided during LCP negotiation.

PAP

PAP (Password Authentication Protocol) is a simple, plaintext authentication scheme, which means that both user name and password are sent over the tunnel plaintext. PAP is therefore not considered a secure authentication protocol.

CHAP

CHAP (Challenge Handshake Authentication Protocol) is a challenge-response authentication protocol specified in RFC 1994. CHAP uses an MD5 one-way encryption scheme to hash the response to a challenge issued by the DFL-700. CHAP is superior to PAP in that the password is never sent over the link. Instead the password is used to create the one-way MD5 hash. This does however mean that CHAP requires passwords to be stored in a reversibly encrypted form.

MS-CHAP v1

MS-CHAP v1 (Microsoft Challenge Handshake Authentication Protocol version 1) is similar to CHAP; the main difference is that with MS-CHAP v1 the password only needs to be stored as an MD4 hash instead of a reversibly encrypted form. Another difference is that MSCHAP v1 uses MD4 Hashing as opposed to MD5 used in CHAP.

MS-CHAP v2

MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 1) is more secure then MS-CHAP v1 as it provides two–way authentication. MS-CHAPv2 is not backwards compatible with MS-CHAP v1. Both the Remote Access Server and the client must prove they have knowledge of the password via two-way Challenge response messages.

MPPE, Microsoft Point-To-Point Encryption

MPPE is used is used to encrypt Point-to-Point Protocol (PPP) packets. MPPE uses the RSA RC4 algorithm to provide data confidentiality. The length of the session key to be used for the encryption can be negotiated. MPPE currently supports 40-bit, 56-bit and 128-bit RC4 session keys.

L2TP/PPTP Clients

Settings for L2TP/PPTP Client Configuration

Name – Specifies a friendly name for the PPTP/L2TP Client tunnel.

Username – Specify the username for this PPTP/L2TP Client tunnel.

Password/Confirm Password – The password to use for this PPTP/L2TP Client tunnel.

Interface IP - Specifies if the L2TP/PPTP Client tunnel should use a Static IP or obtain a dynamic IP from the server.

Remote Gateway - The IP address of the remote PPTP/L2TP Server.

L2TP/PPTP Clients

Add **PPTP** Client :

Name:

Basic settings:

Username:
Password:
Retype Password:
Interface IP: Blank = get IP from server
Remote Gateway:

☑ Use primary DNS server from tunnel as primary DNS
☐ Use secondary DNS server from tunnel as secondary DNS
Hint: Use Servers -> DNS Relayer to easily make DNS servers available to internal clients.

☐ **Dial on demand**

Idle timeout: 60 minutes

○ Count sending as activity
○ Count receiving as activity
○ Count both as activity

Dial on demand – If enabled the tunnel will only be initiated when needed. If disabled the tunnel will be persistent (always on).

Authentication protocol – Specify which authentication protocol to use (if any). Refer to the **Authentication Protocols** section for more information about each type.

MPPE encryption – If MPPE encryption is to be used, select the desired level of encryption key (MPPE is used with PPTP). A selection of **None** means that data will be sent over the PPP link unencrypted.

Require IPSec encryption – If configuring for L2TP, you most likely will be using IPSec instead of MPPE for data encryption. To use IPSec enable the checkbox and select PSK or Certificate.

Authentication:

Protocol:
☐ No auth
☑ PAP
☑ CHAP
☑ MSCHAP (MPPE encryption possible)
☑ MSCHAPv2 (MMPE encryption possible)

MPPE encryption:

☑ None
☑ 40 bit
☑ 56 bit
☑ 128 bit
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

☐ **Use IPsec encryption**

○ **PSK** - Pre-Shared Key
Key:
Retype key:

○ **Certificate based**
Local Identity: Admin - CN=000F3D10FC27
Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)

L2TP/PPTP Servers

Settings for L2TP/PPTP Server Configuration

Name – Specifies a name for this PPTP/L2TP Server.

Outer IP - Specifies the IP that the PPTP/L2TP server should listen on, leave it Blank for the WAN IP.

Inner IP - Specifies the internal IP of the VPN tunnel. Leave this field Blank for the LAN IP.

IP Pool and settings – Information related to client IP assignment.

Client IP Pool – An IP range, group or entire network that the PPTP/L2TP Server will use as an IP address pool to assign dynamic IP addresses to clients.

Primary/Secondary DNS – IP addresses of the primary and secondary DNS servers. If utilizing the DNS Relay function, be sure to enable the check box to ensure proper DNS info.

Primary/Secondary WINS - IP of the Windows Internet Name Service (WINS) servers that are used in Microsoft environments which uses the NetBIOS Name Servers (NBNS) to assign IP addresses to NetBIOS names.

Authentication protocol – Specify which authentication protocol to use, if any (not necessary). Refer to the **Authentication Protocols** section for more information about each type.

MPPE encryption – If MPPE encryption is to be used, select the desired level of encryption key (MPPE is used with PPTP). A selection of **None** means that data will be sent over the PPP link unencrypted.

Require IPSec encryption – If configuring for L2TP, you most likely will be using IPSec instead of MPPE for data encryption. To use IPSec enable the checkbox and select PSK or Certificate.

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 IPSec VPN tunnel that connects the two DFL-700 NetDefend 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 a VPN tunnel that connects the branch office network to the main office network.

The example shows an IPSec VPN between two internal networks. One may also create VPN tunnels between an internal network behind one VPN gateway and a DMZ network behind another or between two remote DMZ networks. The networks at the ends of the VPN tunnel are selected when you configure the VPN policy.
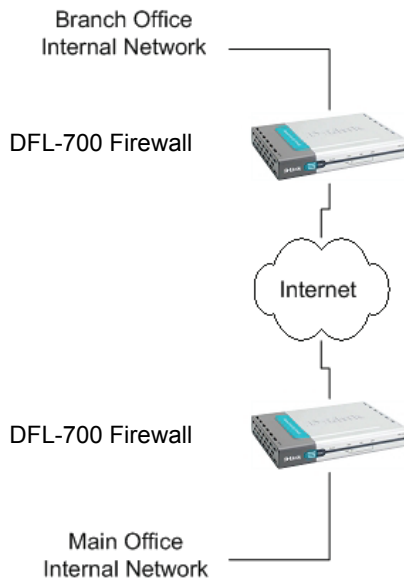
Creating a LAN-to-LAN IPSec VPN Tunnel

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

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

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, either 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.

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.
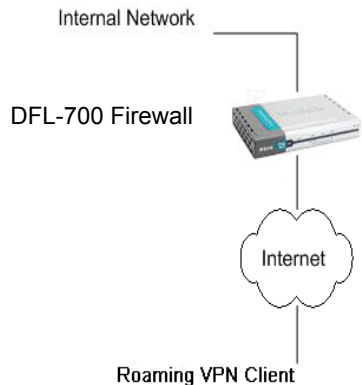
Creating a Roaming Users IPSec Tunnel

Follow these steps to add a roaming user tunnel.

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

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.

Adding an L2TP/PPTP VPN Client

Follow these steps to add an L2TP or PPTP VPN Client configuration.

Step 1. Go to Firewall and VPN and choose **Add new PPTP client** or **Add new L2TP client** in the L2TP/PPTP Clients section.

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 or spaces are allowed.

Step 3. Enter the username and password for the PPTP or L2TP Client.

Step 4. Specify if the IP should be received from the server or if a static one should be used. This field should be left blank in most scenarios.

Step 5. Specify the **Remote Gateway**; this should be the IP of the L2TP or PPTP Server you are connecting to.

Step 6. If you are using IPSec encryption for the L2TP or PPTP Client, choose the appropriate authentication type, either PSK (Pre-shared Key) or Certificate-based.

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

Adding an L2TP/PPTP VPN Server

Follow these steps to add an L2TP or PPTP VPN Server configuration that listens on the WAN IP.

Step 1. Go to Firewall and VPN and choose **Add new PPTP server** or **Add new L2TP server** in the L2TP/PPTP Server section.

Step 2. Enter a Name for this 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 or spaces are allowed.

Step 3. Specify the **Client IP Pool**; this should be a range of unused IP's on the LAN interface that will be handed out to L2TP or PPTP Clients.

Step 4. If you are using IPSec encryption for the L2TP or PPTP Client choose authentication type, either PSK (Pre-shared Key) or Certificate-based.

Click the **Apply** button below to apply the change 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. PFS is used to ensure that in the unlikely event an encryption key is compromised, no subsequent keys could be derived from that compromised key.

NAT Traversal

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

Disabled - The firewall will not send the necessary Vendor ID's to indicate 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 behind a NAT device.

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 (SA) 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 by another certificate. It cannot be 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 those 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 performed.

Content Filtering

DFL-700 HTTP content filtering may be configured to scan all HTTP protocol streams for URLs or for potentially dangerous Web page content. If a match is found between the requested URL and the URL Blacklist the DFL-700 will block the Web page.

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

HTTP content filtering may also be configured to strip potentially dangerous content such as ActiveX objects, Flash objects, Java, and cookies.

There is also a URL Whitelist to explicitly define URLs that should be excluded from all Content Filtering (URLs in this list will not be stripped of ActiveX, Java, Flash, or cookies).

Note: For HTTP URL filtering to work, all HTTP traffic needs to go through a policy using a service with the HTTP ALG. Content Filtering rules will not apply to HTTPS streams. A pre-defined "HTTP-outbound TCP: All -> 80   ALG: "http-cf", max 100" service is provided to simplify the configuration of HTTP Content Filtering.

Refer to Appendix D for more detailed information on configuration of HTTP Content Filtering.

Edit the URL Global Whitelist

Follow these steps to add or remove a URL.

Step 1. Navigate to Firewall / Content Filtering and choose Edit global URL Whitelist.

Step 2. Add or edit a URL that should always be allowed. Remove any URL that you do not want to always allow.

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.** Navigate to Firewall / Content Filtering and choose Edit global URL Blacklist.

> **Step 2.** Add or edit a URL that should be filtered and blocked. File extensions may also be defined to block download of specified file types.

Click the **Apply** button below to apply the changes or click **Cancel** to discard changes.
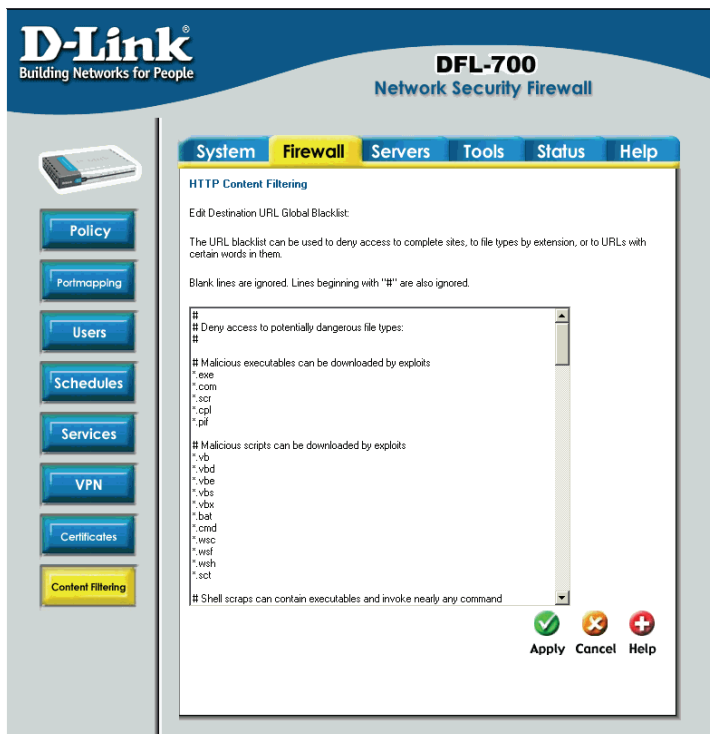
Note: For HTTP URL filtering to work, all HTTP traffic needs to go through a policy using a service with the HTTP ALG. A pre-defined "HTTP-outbound TCP: All -> 80 ALG: "http-cf", max 100" service is provided to simplify the configuration of HTTP Content Filtering.

Refer to Appendix D for more detailed information on configuration of HTTP Content Filtering.

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. A pre-defined "HTTP-outbound TCP: All -> 80 ALG: "http-cf", max 100" service is provided to simplify the configuration of HTTP Content Filtering.

Refer to Appendix D for more detailed information on configuration of HTTP Content Filtering.

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 DHCP enabled 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 DHCP server.

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 Relay function. A DHCP Relay allows the DFL-700 to receive DHCP requests and forward those requests to a specified DHCP server. The relay function allows the use of existing DHCP servers in conjunction with the DFL-700 to ensure all users on all interfaces receive IP addresses when requested. The DFL-700 will also configure dynamic routes based on those DHCP 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.
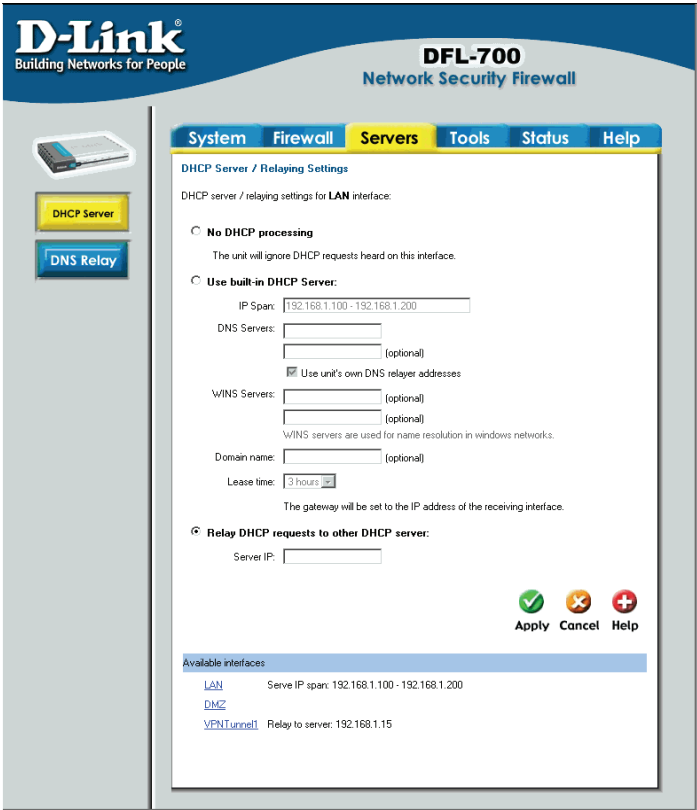
Enable DHCP Server

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 function is configured, the DHCP server will assign those addresses.

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/Relay

To disable the DHCP Server on an interface, click on **Servers** in the menu bar, and then click **DHCP Server** below it. Select the interface on which you wish to disable the DHCP server or relayer.

Follow these steps to disable the DHCP Server or Relayer 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 function that can be configured to relay DNS queries from the internal LAN to the DNS servers used by the firewall itself.

Enable DNS Relayer

Follow these steps to enable the DNS Relayer.

Step 1. Enable by checking the **Enable DNS Relayer** 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 Relayer

Follow these steps to disable the DNS Relayer.

Step 1. Disable by un-checking the **Enable DNS Relayer** 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: [1 ▼]

Packet size: [64 ▼]

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.
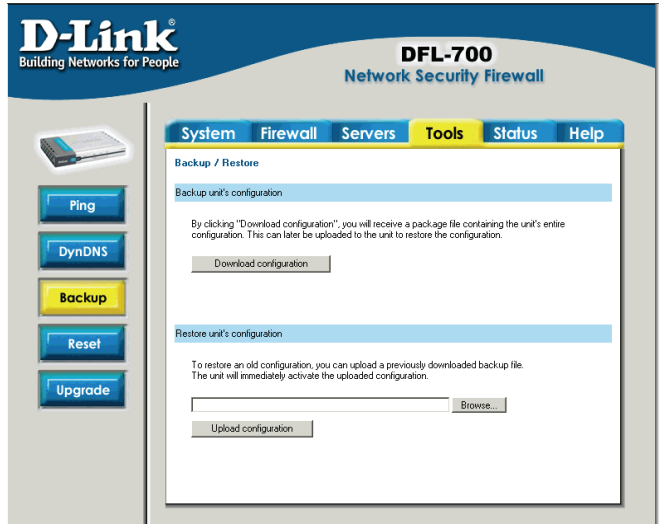
Exporting the DFL-700's Configuration

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, click **OK**.

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

Restart/Reset
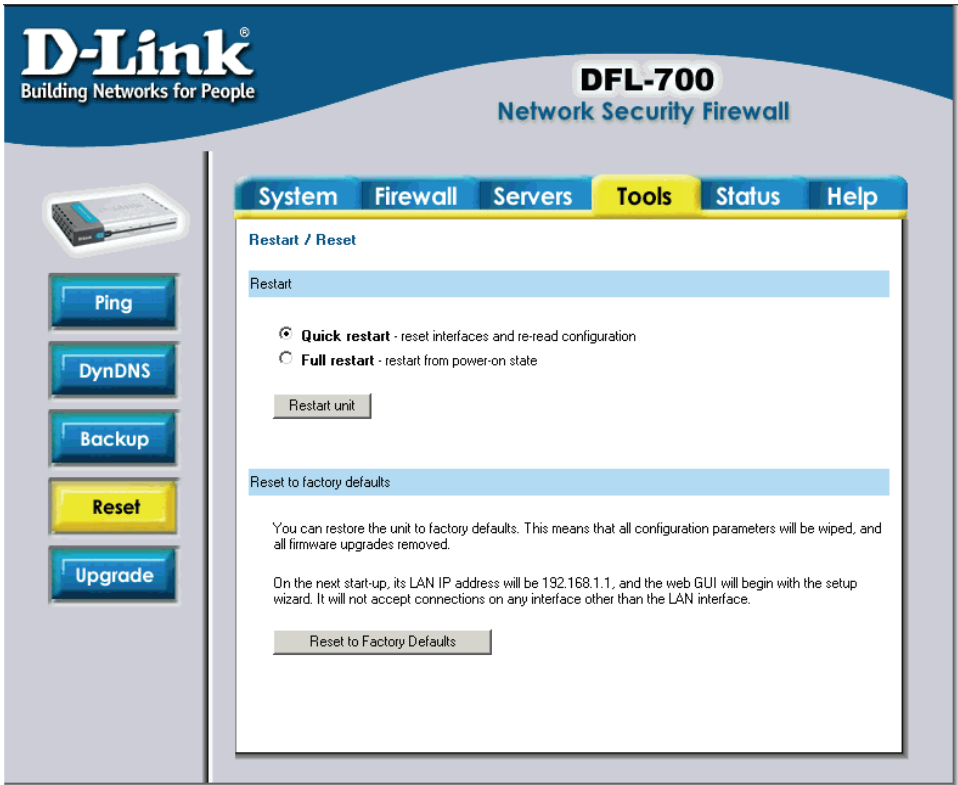
Restarting the DFL-700

Follow these steps to 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. Make sure you have the current firmware file available for upload to the device in the case where the firmware version is defaulted to an older version.

The factory reset procedure erases all configuration changes that have been made to the DFL-700 and reverts the system to its original configuration, including resetting of all interface addresses.

Follow these steps to reset the DFL-700 to factory default settings through the Web-based Configuration:

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.

Follow these steps to reset the DFL-700 to factory default settings using the Reset button located at the rear of the device:

Step 1. Using a paperclip or some other rigid small diameter object push in and hold the Reset button with the unit powered off.

Step 2. Continue to hold the reset button for 15 seconds while the DFL-700 is powered on. The Firewall should beep to indicate the default configuration restore procedure has initiated.

Step 3. Hold the reset button until the Firewall again beeps twice. Release the reset button following the two beeps. At this point the Firewall is loading the factory default configuration.

Step 4. Allow at least 1 minute for the Firewall to completely restart. At this point the firewall can be accessed via its default LAN IP (192.168.1.1) through a web browser. The first login will require the use of the Wizard to complete basic connectivity configurations.

You can restore your system settings by uploading a previously generated system configuration file to the DFL-700 if a backup of the device has been downloaded to your Local Machine Prior to reset.

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 of the DFL-700, obtain the latest version from support.dlink.com (US). Make sure the firmware file is stored on the PC connected to the firewall. Connect to the web-based GUI, navigate to the **Upgrade** / **Tools** menu, click **Browse**, and choose the file name of the newest version of firmware you wish to load. Click **Upload firmware image** to load the new firmware and restart the device.

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 Web-based configuration GUI, 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**.

Beginning with firmware version 1.30, the IDS Signature database will automatically update itself once enabled on a policy.

Status

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

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

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.

Time – The current time and date.

Configuration – Shows when the last administrative configuration change was activated as well as the originating IP.

Firmware version – The firmware version running on the firewall.

Last restart – The reason for the last restart.

IDS Signatures – The IDS signature database versions.

Resources – Displays CPU load, RAM usage, Connections, VPN Tunnels and Rules configured.

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. Useful for plotting usage trends for your application.
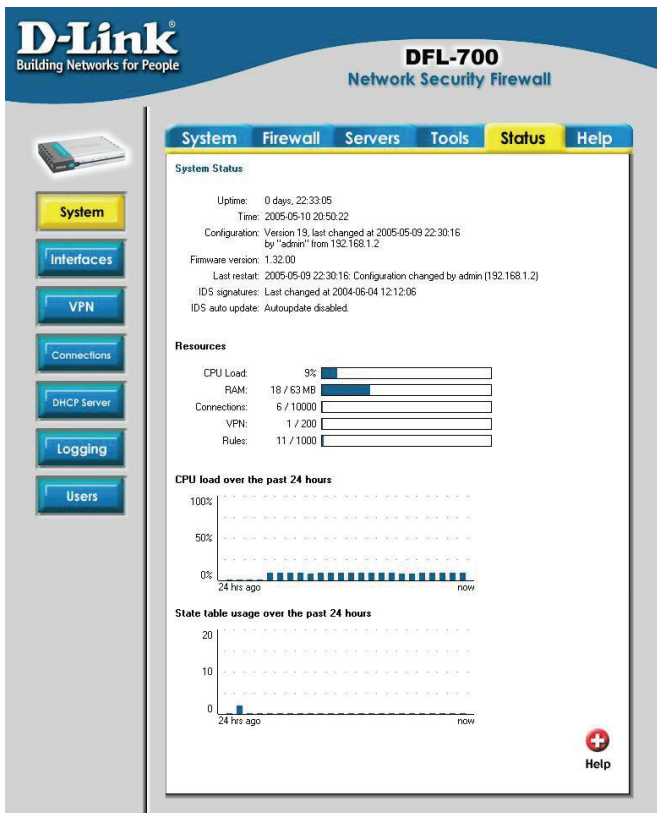
Interfaces

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. Click on **WAN** or **DMZ** for more information about the respective interface.

**Interface** – Name of the interface being viewed, 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.
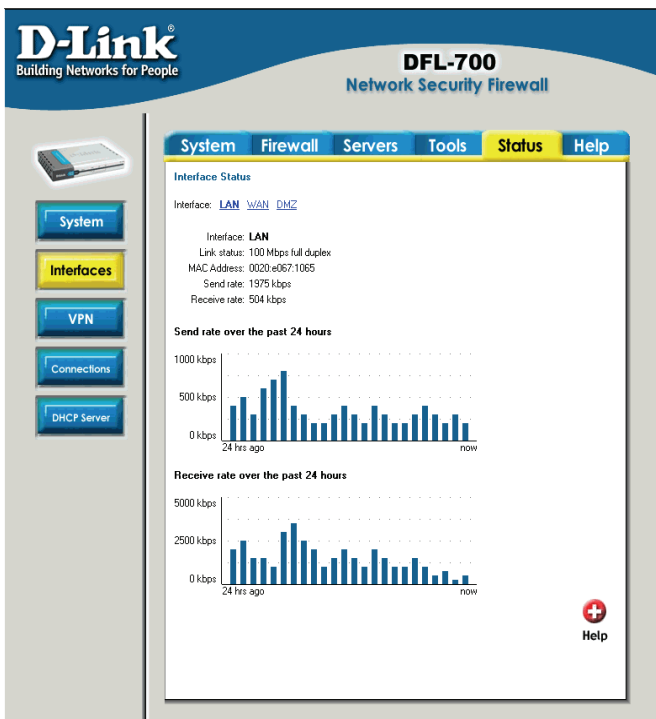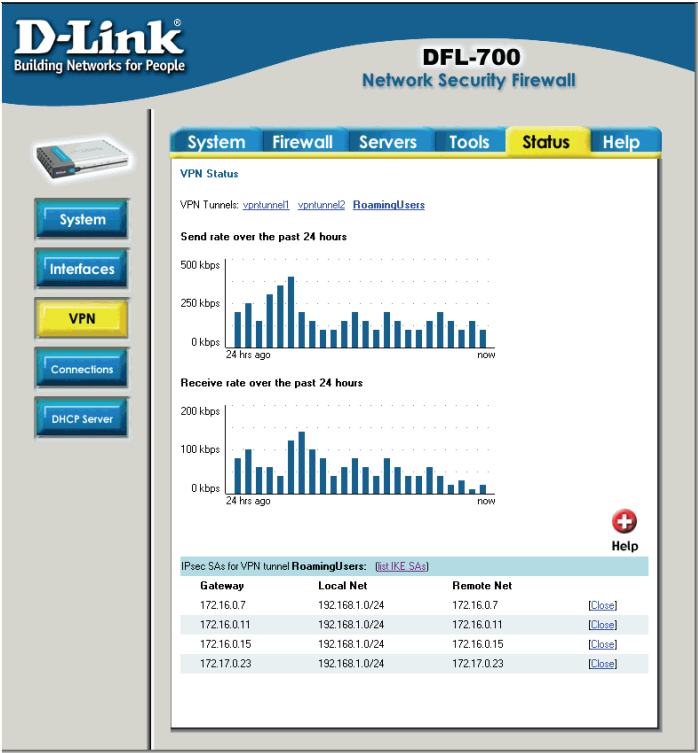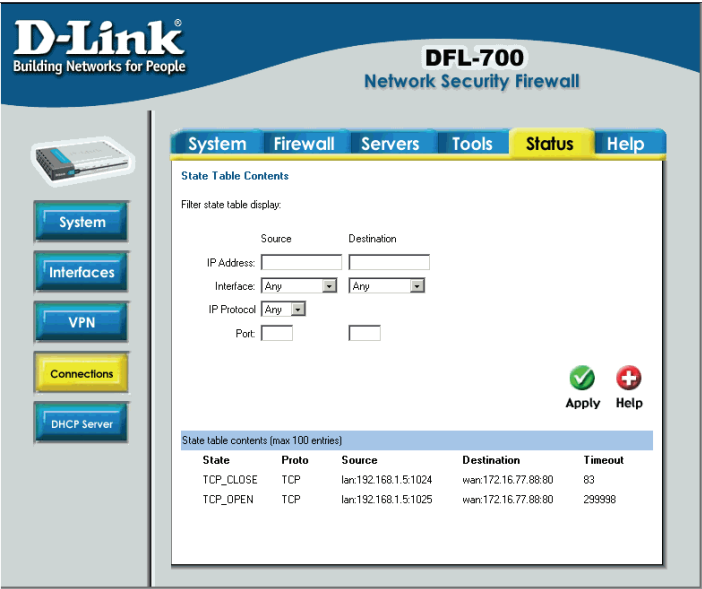
VPN

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 through 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.

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.

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 range of IP addresses 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.

Users

Click on **Status** in the menu bar, and then click **Users** below it. A window will appear providing user information.

Currently authenticated users – users logged in using HTTP/HTTPS authentication, users logged in on PPTP and L2TP servers will be listed here. Users can be forced to log out by clicking logout.

Currently recognized privileges – all users and groups that are used in policies are listed here. These users and groups will be able to use HTTP and HTTPS authentication.
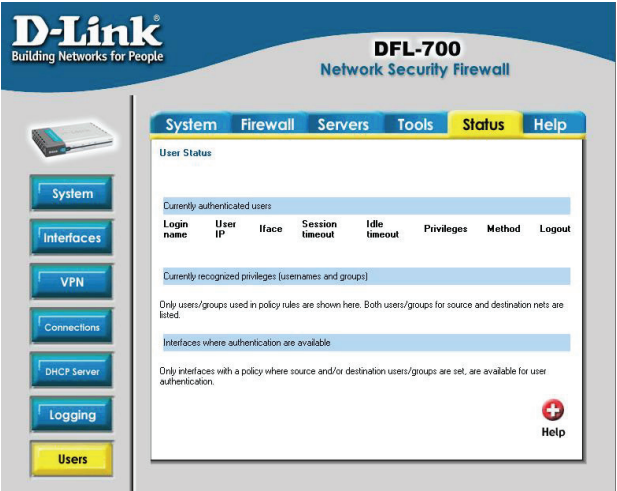
Interfaces where authentication are available – here all interfaces where HTTP and HTTPS authentication is possible is listed.

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.

Step by Step Guides

The following guides make use of example IP Addresses, users, sites and passwords. You will have to exchange the example information with your own values. Passwords used in these examples are not recommended for real life use. Strong passwords and keys should be chosen making use of symbols, letters, and numbers to decrease the likelihood of a brute force dictionary attack success.

In these guides for example *Firewall->Users* will mean that the **Firewall** tab should first be selected from the menu at the top of the screen,
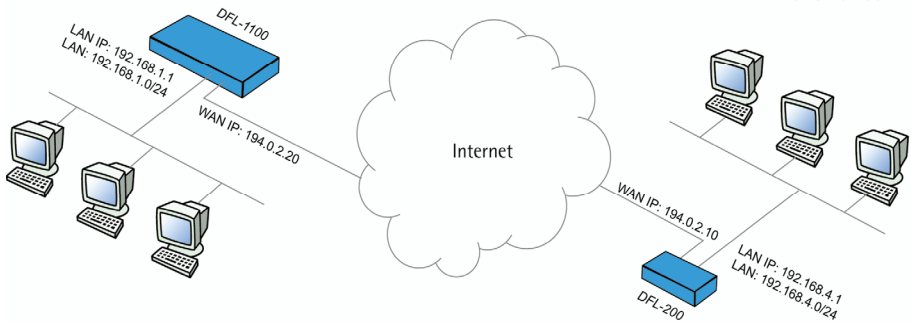

followed by the **Users** button to the left of the screen should be selected.
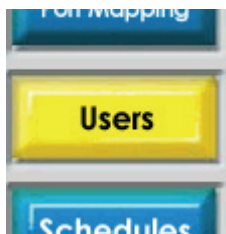
LAN-to-LAN VPN using IPSec

Main office

Settings for Branch office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.10**

LAN IP: **192.168.4.1**, Subnet mask: **255.255.255.0**

2. Setup IPSec tunnel, *Firewall->VPN:*

Under IPSec tunnels click *Add new*

Name the tunnel **ToMainOffice**

Local net: **192.168.4.0/24**

VPN Tunnels

Add IPsec tunnel :

Name: toMainOffice

Local Net: 192.168.4.0/24

Authentication:

PSK - Pre-Shared Key

PSK: **********

Retype PSK: **********

PSK: **1234567890** (Do not use this as your PSK)

Retype PSK: **1234567890**

Select Tunnel type: **LAN-to-LAN tunnel**

Remote Net: **192.168.1.0/24**

Remote Gateway: **194.0.2.20**

Enable **Automatically add a route for the remote network**

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click *Apply*

4. Click *Activate* and wait for the firewall to restart

Settings for Main office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.20**

LAN IP: **192.168.1.1**, Subnet mask: **255.255.255.0**

2. Setup IPSec tunnel, *Firewall->VPN:*

Under IPSec tunnels click *add new*

Name the tunnel **ToBranchOffice**

Local net: **192.168.1.0/24**

PSK: **1234567890** (Note! You should use a key that is hard to guess)

Retype PSK: **1234567890**

Select Tunnel type: **LAN-to-LAN tunnel**

Remote Net: **192.168.4.0/24**

Remote Gateway: **194.0.2.10**

Enable "Automatically add a route for the remote network"

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click *Apply*

4. Click *Activate* and wait for the firewall to restart

This example will allow *all* traffic between the two offices. To get a more secure solution read the **A more secure LAN-to-LAN VPN solution** section of this user guide.

LAN-to-LAN VPN using PPTP

Main office
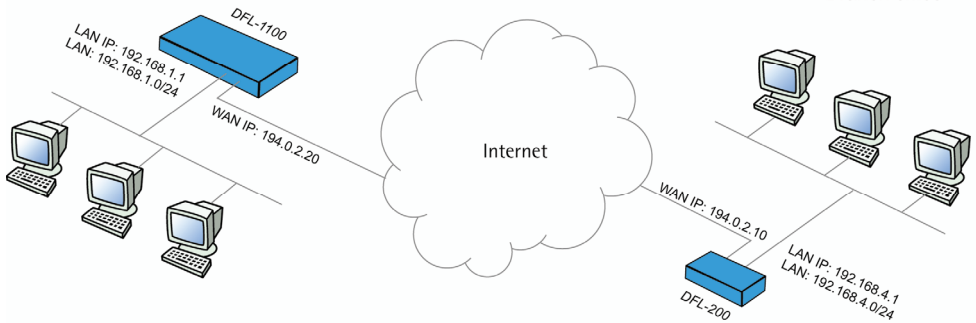
Settings for Branch office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.10**

LAN IP: **192.168.4.1**, Subnet mask: **255.255.255.0**

2. Setup PPTP client, *Firewall->VPN:*

Under PPTP/L2TP clients click *Add new PPTP client*

Name the tunnel **toMainOffice**

L2TP/PPTP Clients

Add **PPTP** Client :

Name: toMainOffice

Basic settings:

Username: BranchOffice

Password: ***********

Retype Password: ***********

Interface IP: [blank]   Blank = get IP from server

Remote Gateway: 194.0.2.20

Remote Net: 192.168.1.0/24

Proxy ARP ☐ Publish remote network on all interfaces via Proxy ARP.

☐ Use primary DNS server from tunnel as primary DNS

☐ Use secondary DNS server from tunnel as secondary DNS

Hint: Use Servers -> DNS Relayer to easily make DNS servers available to internal clients.

☐ **Dial on demand**

Username: **BranchOffice**

Password: **1234567890** (Note! You should use a password that is hard to guess)

Retype password: **1234567890**

Interface IP: leave blank

Remote gateway: **194.0.2.20**

Remote net: **192.168.1.0/24**

Dial on demand: leave unchecked

Authentication:

Protocol: ☐ No auth

☐ PAP

☐ CHAP

☐ MSCHAP (MPPE encryption possible)

☑ MSCHAPv2 (MMPE encryption possible)

Under authentication **MSCHAPv2** should be the only checked option.

MPPE encryption:

- ☐ None
- ☐ 40 bit
- ☐ 56 bit
- ☑ 128 bit

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

☐ **Use IPsec encryption**

Under MPPE encryption **128 bit** should be the only checked option.

Leave **Use IPSec encryption** unchecked

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Firewall Policy

Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL: 3

VPN: ☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

Click *Apply*

4. Click *Activate* and wait for the firewall to restart.

Settings for Main office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.20**

LAN IP: **192.168.1.1**, Subnet mask: **255.255.255.0**

2. Setup PPTP server, *Firewall->VPN:*

Under L2TP / PPTP Server click **Add new PPTP server**

L2TP/PPTP Servers

Add **PPTP** tunnel :

Name: pptpServer

Outer IP: Blank = WAN IP

Must be WAN IP if IPsec encryption is required

Inner IP: Blank = LAN IP

IP Pool and settings:

Client IP Pool: 192.168.1.100 - 192.168.1.199

☑ Proxy ARP dynamically added routes

Primary DNS: (Optional)

Secondary DNS: (Optional)

☑ Use unit's own DNS relayer addresses

Primary WINS: (Optional)

Secondary WINS: (Optional)

Name the server **pptpServer**

Leave Outer IP and Inner IP blank

Set client IP pool to **192.168.1.100 – 192.168.1.199**

Check **Proxy ARP dynamically added routes**

Check **Use unit's own DNS relayer addresses**

Leave WINS settings blank

Authentication:

Protocol:
- ☐ No auth
- ☐ PAP
- ☐ CHAP
- ☐ MSCHAP (MPPE encryption possible)
- ☑ MSCHAPv2 (MMPE encryption possible)

MPPE encryption:
- ☐ None
- ☐ 40 bit
- ☐ 56 bit
- ☑ 128 bit

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

☐ **Use IPsec encryption**

Under authentication **MSCHAPv2** should be the only checked option.

Under MPPE encryption **128 bit** should be the only checked option.

Leave **Use IPsec encryption** unchecked

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Firewall Policy

Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL: 3

VPN: ☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click *Apply*

4. Set up the authentication source, *Firewall->Users*:

Authentication source:

⦿ **Local database**

◯ **RADIUS server**

Select **Local database**

Click *Apply*

5. Add a new user, *Firewall->Users*:

Under **Users in local database** click *Add new*

Name the new user **BranchOffice**

User Management

Add new user:

User name:	BranchOffice
Group membership:	
Password:	**********
Retype password:	**********

L2TP/PPTP settings:

Static client IP:	
	If empty, the IP address will be taken from the server's IP pool
Networks behind user:	192.168.4.0/24

Enter password: **1234567890**

Retype password: **1234567890**

Leave static client IP empty (could also be set to 192.168.1.200. If no IP is set here the IP pool from the PPTP server settings are used).
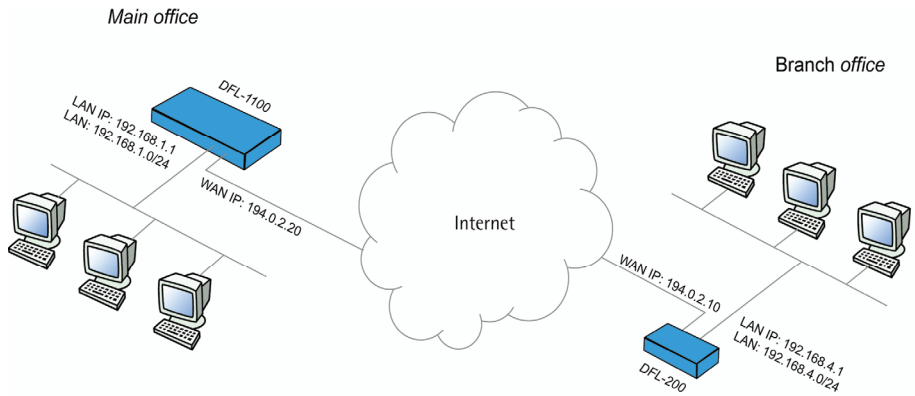
Set Networks behind user to **192.168.4.0/24**

Click *Apply*

6. Click **Activate** and wait for the firewall to restart.

This example will allow *all* traffic between the two offices. To get a more secure solution read the **A more secure LAN-to-LAN VPN solution** section.

LAN-to-LAN VPN using L2TP

Settings for Branch office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.10**

LAN IP: **192.168.4.1**, Subnet mask: **255.255.255.0**

2. Setup L2TP client, *Firewall->VPN:*

Under L2TP / PPTP client click **Add new L2TP client**

Name the server **toMainOffice**

L2TP/PPTP Clients

Add **L2TP** Client:

Name: toMainOffice

Basic settings:

Username: `BranchOffice`

Password: `**********`

Retype Password: `**********`

Interface IP: `                    ` Blank = get IP from server

Remote Gateway: `194.0.2.20`

Remote Net: `192.168.1.0/24`

Proxy ARP ☐ Publish remote network on all interfaces via Proxy ARP.

☐ Use primary DNS server from tunnel as primary DNS

☐ Use secondary DNS server from tunnel as secondary DNS

Hint: Use Servers -> DNS Relayer to easily make DNS servers available to ir clients.

☐ **Dial on demand**

Username: **BranchOffice**

Password: **1234567890** (Note! You should use a password that is hard to guess)

Retype password: **1234567890**

Interface IP: leave blank

Remote gateway: **194.0.2.20**

Remote net: **192.168.1.0/24**

Dial on demand: leave unchecked

Authentication:

Protocol: ☐ No auth

☐ PAP

☐ CHAP

☐ MSCHAP (MPPE encryption possible)

☑ MSCHAPv2 (MMPE encryption possible)

Under authentication only **MSCHAPv2** should be checked

MPPE encryption:

- ☑ None
- ☐ 40 bit
- ☐ 56 bit
- ☐ 128 bit

Encryption is only possible when using MSCHAP or MSCHAPv2 as authenti protocol

☑ **Use IPsec encryption**

    ⦿ **PSK** - Pre-Shared Key

        Key: `**********`

    Retype key: `**********`

    ◯ **Certificate based**

Under MPPE encryption only **None** should be checked

Check **Use IPsec encryption**

Enter key **1234567890** (Note! You should use a key that is hard to guess)

Retype key **1234567890**

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Firewall Policy

Edit global policy parameters:

Fragments:	☐ Drop all fragmented packets	
Minimum TTL:	3	
VPN:	☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.	

Click *Apply*

4. Click **Activate** and wait for the firewall to restart

Settings for Main office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.20**

LAN IP: **192.168.1.1**, Subnet mask: **255.255.255.0**

2. Setup L2TP server, *Firewall->VPN:*

Under L2TP / PPTP Server click **Add new L2TP server**

Name the server **l2tpServer**

L2TP/PPTP Servers

Add **L2TP** tunnel :

Name:	l2tpServer
Outer IP:	Blank = WAN IP
	Must be WAN IP if IPsec encryption is required
Inner IP:	Blank = LAN IP

IP Pool and settings:

Client IP Pool:	192.168.1.100 - 192.168.1.199
	☑ Proxy ARP dynamically added routes
Primary DNS:	(Optional)
Secondary DNS:	(Optional)
	☑ Use unit's own DNS relayer addresses
Primary WINS:	(Optional)
Secondary WINS:	(Optional)

Leave Outer IP and Inner IP blank

Set client IP pool to **192.168.1.100 – 192.168.1.199**

Check **Proxy ARP dynamically added routes**

Check **Use unit's own DNS relayer addresses**

Leave **WINS** settings blank

Authentication:

Protocol:
- ☐ No auth
- ☐ PAP
- ☐ CHAP
- ☐ MSCHAP (MPPE encryption possible)
- ☑ MSCHAPv2 (MMPE encryption possible)

Under authentication **MSCHAPv2** should be the only checked option.

Under MPPE encryption **None** should be the only checked option.

MPPE encryption:
- ☑ None
- ☐ 40 bit
- ☐ 56 bit
- ☐ 128 bit

Encryption is only possible when using MSCHAP or MSCHAPv2 as authenti
protocol

☑ **Use IPsec encryption**

⦿ **PSK** - Pre-Shared Key

Key: `**********`

Retype key: `**********`

○ **Certificate based**

Check **Use IPSec encryption**

Enter key **1234567890** (Note! You should not use this key)

Retype key **1234567890**

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Firewall Policy

Edit global policy parameters:

Fragments:	☐ Drop all fragmented packets
Minimum TTL:	3
VPN:	☑ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

Click ***Global policy parameters***

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click ***Apply***

4. Set up authentication source, *Firewall->Users*:

Authentication source:

◉ **Local database**

○ **RADIUS server**

Select **Local database**

Click ***Apply***

5. Add a new user, *Firewall->Users*:

Under **Users in local database** click *Add new*

User Management

Add new user:

User name:	BranchOffice
Group membership:	
Password:	**********
Retype password:	**********

L2TP/PPTP settings:

Static client IP:	
	If empty, the IP address will be taken from the server's IP pool
Networks behind user:	192.168.4.0/24

Name the new user **BranchOffice**

Enter password: **1234567890**

Retype password: **1234567890**

Leave static client IP empty (could also be set to eg 192.168.1.200. If no IP is set here the IP pool from the L2TP server settings are used).

Set Networks behind user to **192.168.4.0/24**

Click *Apply*

6. Click **Activate** and wait for the firewall to restart.

This example will allow *all* traffic between the two offices. To get a more secure solution read the **A more secure LAN-to-LAN VPN solution** section in this chapter.

A more secure LAN-to-LAN VPN solution

In order to establish a more secure LAN-to-LAN VPN connection, traffic policies should be created instead of allowing all traffic between the two private Networks. The following steps show how to enable some common services allowed through the VPN tunnel. In this example we have a mail server, ftp server and a web server (intranet) in the main office that we want to access from the branch office.

Settings for Branch office

1. Setup policies for the new tunnel, ***Firewall->Policy:***

Click ***Global policy parameters***

Firewall Policy

Edit global policy parameters:

Fragments: ☐ Drop all fragmented packets

Minimum TTL: 3

VPN: ☐ Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN.

Disable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click ***Apply***

2. Now is it possible to create policies for the VPN interfaces. Select from **LAN** to **toMainOffice** and click ***Show***.

- LAN->DMZ policy - 3 rules
- DMZ->LAN policy - 0 rules

- WAN->DMZ policy - 0 rules
- DMZ->WAN policy - 4 rules, NAT enabled

Custom policy:

LAN -> toMainOffice Show

3. Click ***Add new*** to create the first rule

4. Setup the new rule:

Name the new rule: **allow_pop3**

Select action: **Allow**

Select service: **pop3**

Select schedule: **Always**

Firewall Policy

Show policy: LAN->WAN   LAN->DMZ   WAN->DMZ
WAN->LAN   DMZ->LAN   DMZ->WAN

Show custom policy: LAN ▾ -> toMainOffice ▾   Show

Edit **new** rule:

Name: allow_pop3

Position: [   ] Moves before given position. Blank = last.

Action: Allow ▾

Source Nets: [   ]

... Users/Groups: [   ] "Any" = Any authenticated

Destination Nets: [   ]

... Users/Groups: [   ] "Any" = Any authenticated

Leave source and/or destination blank to match everything.

Service: pop3 ▾

Custom source ports: [   ] Blank = any port

... destination ports: [   ]

Schedule: - Always - ▾

We don't want any Intrusion detection for now, so leave this option unchecked.

Click *Apply*

5. The first policy rule is now created. Repeat step 4 to create services named **allow_imap**, **allow_ftp** and **allow_http**. The services for these policies should be **imap**, **ftp_passthrough** and **http** respectively.

The policy list for **LAN->toMainOffice** should now look like this.

LAN->toMainOffice Policy						
Name	**Action**	**Source**	**Destination**	**Service**	**Move**	
#1 allow_pop3	Allow	Any	Any	pop3	⬇	[Edit]
#2 allow_imap	Allow	Any	Any	imap	⬆⬇	[Edit]
#3 allow_ftp	Allow	Any	Any	ftp-passthrough	⬆⬇	[Edit]
#4 allow_http	Allow	Any	Any	http	⬆	[Edit]
[Add new]						

Order of evaluation

If no rule matches, the connection will be denied and logged.

6. Click *Activate* and wait for the firewall to restart.

Settings for Main office

1. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Disable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click *Apply*

2. Now it is possible to create policies for the VPN interfaces. Select from **toBranchOffice** to **LAN** and click *Show*.

- LAN->DMZ policy - 3 rules
- DMZ->LAN policy - 0 rules
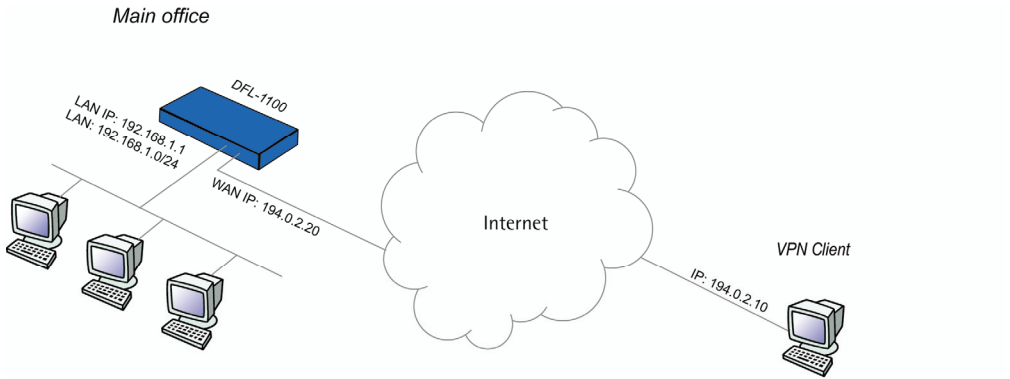
- WAN->DMZ policy - 0 rules
- DMZ->WAN policy - 4 rules, NAT enabled

Custom policy:

toBranchOffice ▾ -> LAN ▾ Show

3. Create the same 4 policy rules that were created on the branch office firewall (**allow_pop3**, **allow_imap**, **allow_ftp** and **allow_http**).

4. Click *Activate* and wait for the firewall to restart.

Windows XP client and PPTP server

Settings for the Windows XP client

1. Open the control panel (Start button -> Control panel).

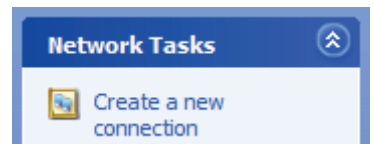**2.** If you are using the Category view, click on the **Network and Internet Connections** icon. Then click **Create a connection to the network on your workplace** and continue to step 6.

If you are using the Classic view, click on the **Network Connections** icon.

3. Under Network task, click **Create a new connection**

4. The **New connection wizard** window opens up. Click *next*.

New Connection Wizard

Network Connection Type
What do you want to do?

○ **Connect to the Internet**

Connect to the Internet so you can browse the Web and read email.

◉ **Connect to the network at my workplace**

Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**

Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**

Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

[< Back] [Next >] [Cancel]

5. Select **Connect to the network at my workplace** and click *Next*

New Connection Wizard

Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

◉ **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

[< Back] [Next >] [Cancel]

6. Select **Virtual Private Network connection** and click *Next*

New Connection Wizard

Connection Name
  Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

MainOffice

For example, you could type the name of your workplace or the name of a server you will connect to.

[< Back] [Next >] [Cancel]

7. Name the connection **MainOffice** and click *Next*

New Connection Wizard

Public Network
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

○ Do not dial the initial connection.

○ Automatically dial this initial connection:

[< Back] [Next >] [Cancel]

8. Select **Do not dial the initial connection** and click *Next*

New Connection Wizard

VPN Server Selection
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

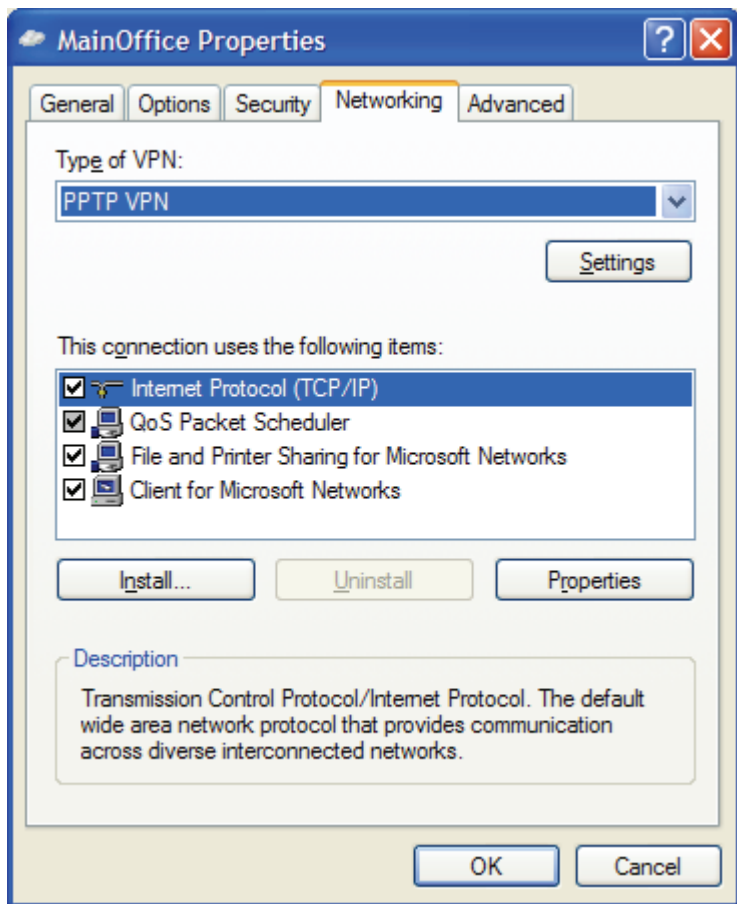194.0.2.20

< Back   Next >   Cancel

9. Type the IP address to the server, **194.0.2.20**, and click *Next*

10. Click *Finish*
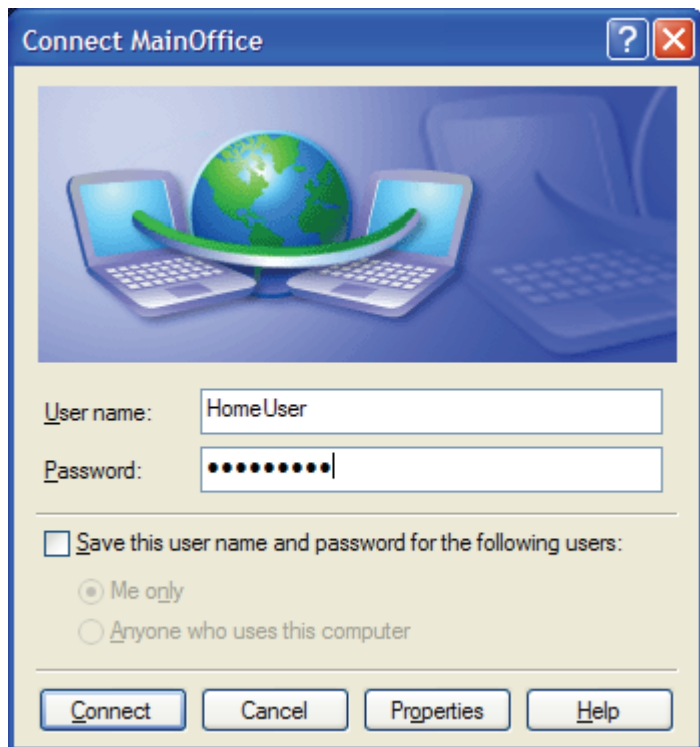
11. Type user name **HomeUser** and password **1234567890** (Note! You should use a password that is hard to guess)

12. Click *Properties*

13. Select the **Networking tab** and change **Type of VPN** to **PPTP VPN**. Click *OK*.

All settings needed for the XP client are now complete. Once we have configured the server on the firewall you should be able to click **Connect** to establish the connection to the Main office.

Settings for Main office

1. Setup interfaces, *System->Interfaces*:

   WAN IP: **194.0.2.20**

   LAN IP: **192.168.1.1**, Subnet mask: **255.255.255.0**

2. Setup PPTP server, *Firewall->VPN:*

    Under L2TP / PPTP Server click **Add new PPTP server**

    Name the server **pptpServer**

    Leave Outer IP and Inner IP blank

    Set client IP pool to **192.168.1.100 – 192.168.1.199**

    Check **Proxy ARP dynamically added routes**

    Check **Use unit's own DNS relayer addresses**

    Leave WINS settings blank

    Under authentication **MSCHAPv2** should be the only checked option.

    Under MPPE encryption **128 bit** should be the only checked option.

    Leave **Use IPSec encryption** unchecked

    Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

    Click *Global policy parameters*

    Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

    Click *Apply*

4. Set up authentication source, *Firewall->Users*:

    Select **Local database**

    Click *Apply*

5. Add a new user, *Firewall->Users*:

    Under **Users in local database** click *Add new*

    Name the new user **HomeUser**

    Enter password: **1234567890**

   Retype password: **1234567890**

    Leave static client IP empty (could also be set to eg 192.168.1.200. If no IP is set here the IP pool from the PPTP server settings are used).

    Click *Apply*

6. Click *Activate* and wait for the firewall to restart.

This example will allow *all* traffic from the client to the main office network. To get a more secure solution read the **Settings for the Main office** part of the **A more secure LAN-to-LAN VPN solution** section.
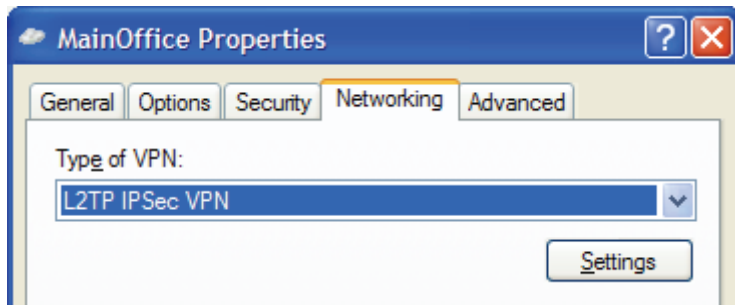
Windows XP client and L2TP server
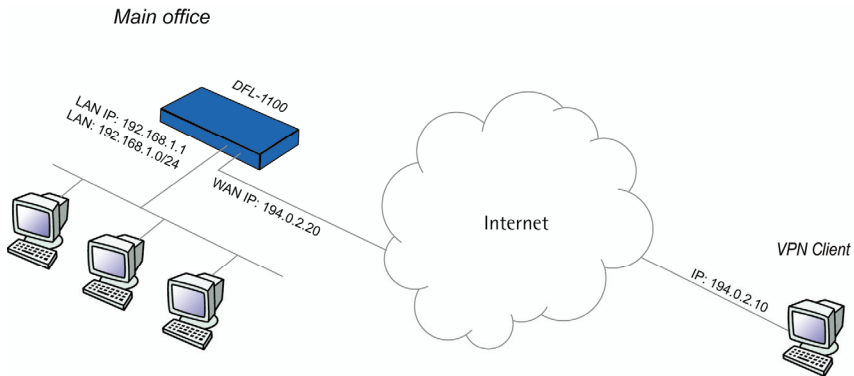
The Windows XP client to L2TP server setup is quite similar to the PPTP setup above.
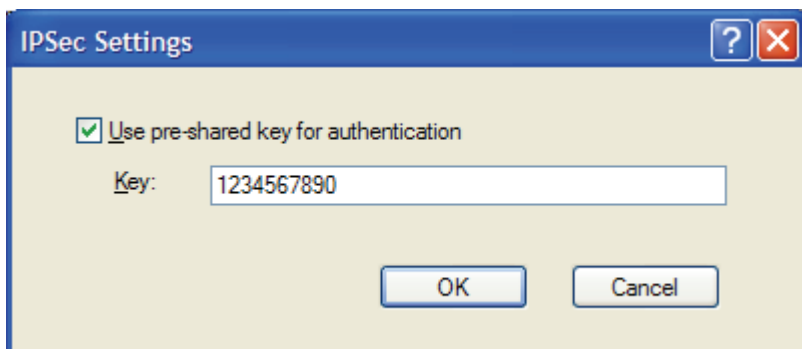
Settings for the Windows XP client

To setup a L2TP connection from Windows XP to the Main office firewall, please follow the steps in the PPTP guide above for the client side. The only changes to the PPTP guide are:

1. In step 13, change the **Type of VPN** to **L2TP IPSec VPN**.
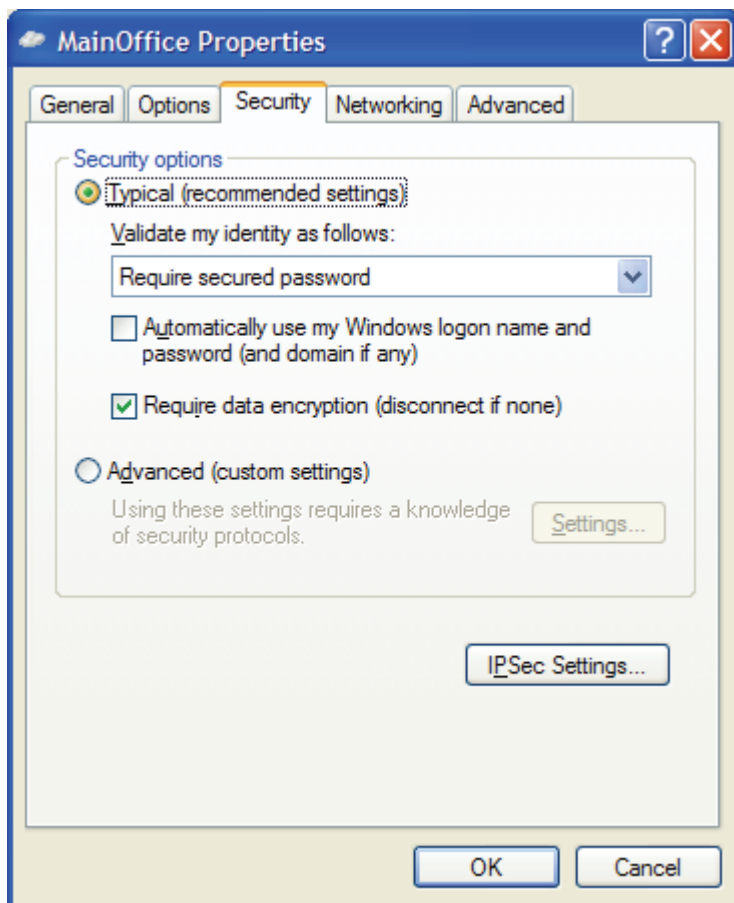
2. Select the **Security** tab and click **IPSec Settings**

3. Check **Use pre-shared key for authentication**, type the key and click *OK*

Settings for Main office

1. Setup interfaces, *System->Interfaces*:

WAN IP: **194.0.2.20**

LAN IP: **192.168.1.1**, Subnet mask: **255.255.255.0**

2. Setup L2TP server, *Firewall->VPN:*

Under L2TP / PPTP Server click **Add new L2TP server**

Name the server **l2tpServer**

Leave Outer IP and Inner IP blank

Set client IP pool to **192.168.1.100 – 192.168.1.199**

Check **Proxy ARP dynamically added routes**

Check **Use unit's own DNS relayer addresses**

Leave WINS settings blank

Under authentication **MSCHAPv2** should be the only checked option

Under MPPE encryption **None** should be the only checked option

Check the **Use IPSec encryption** box

Enter the pre-shared key, **1234567890**, and retype same pre-shared key

Click *Apply*

3. Setup policies for the new tunnel, *Firewall->Policy:*

Click *Global policy parameters*

Enable **Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**

Click *Apply*

4. Set up authentication source, *Firewall->Users*:

Select **Local database**

Click *Apply*

5. Add a new user, *Firewall->Users*:

      Under **Users in local database** click *Add new*

      Name the new user **HomeUser**

      Enter password: **1234567890**

      Retype password: **1234567890**

      Leave static client IP empty (could also be set to eg 192.168.1.200. If no IP is set here the IP pool from the PPTP server settings are used).

      Click *Apply*

6. Click *Activate* and wait for the firewall to restart.

This example will allow *all* traffic from the client to the main office network. To get a more secure solution read the **Settings for the Main office** part of the **A more secure LAN-to-LAN VPN solution** section.

Intrusion Detection and Prevention
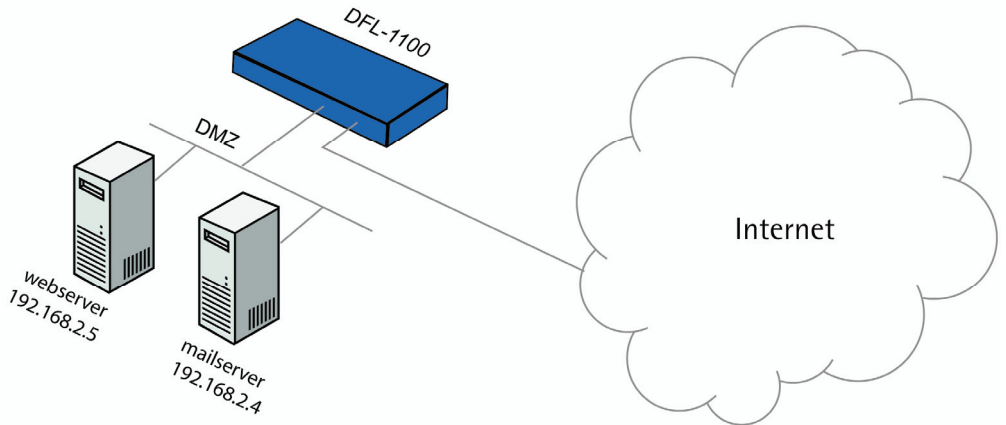
     Intrusion detection and prevention can be enabled for both policies and port mappings. In this example we are using a port mapping. The policy setup is quite similar.

     In this example a mail server with IP 192.168.2.4 and a web server with IP 192.168.2.5 are connected to the DMZ interface on the firewall.

     To set up intrusion detection and prevention to a web server on the DMZ net, follow these steps:

1. Create a Port mapping for the web server, **Firewall->Port Mapping**:

     Under **Configured mappings**, click **Add new**

2. Set up the newly created port mapping:

Port Mapping / Virtual Servers

Edit **new** mapping :

Name: map_www

Source Nets: [   ]   Blank = everyone
... Users/Groups: [   ]   "Any" = Any authenticated
Destination IP: [   ]   Blank = WAN interface IP address

Service: http-in-all ▼

Custom source ports: [   ]   Blank = any port
... destination ports: [   ]
... pass to port: [   ]   ... and up. Blank=no change.

Pass To: 192.168.2.5

Schedule: - Always - ▼

☑ **Intrusion Detection / Prevention:**

Mode: Prevention ▼

Alerting: ☑ Enable IDS/IDP alerting via email for this rule

Name the rule **map_www**

Select service **http-in-all**

Enter pass to IP: **192.168.2.5** (the IP of the web server)

Check the **Intrusion detection / prevention** option

Select mode **Prevention**

Enable email alerting by checking the **Alerting** box

Click *Apply*

The new mapping is now in the list.

Name	Source	Destination	Service	Pass to
map_www	Any	WAN IP	http-in-all	192.168.2.5

Configured mappings:

[Add new]

3. Setup email server and enable alerting, *System->Logging*:

☑ **Enable E-mail alerting for IDS/IDP events**

Sensitivity:	Normal ▼
SMTP Server:	192.168.2.4
Sender:	idsalert@examplecompany.com
E-Mail Address 1:	webmaster@examplecompany.co
E-Mail Address 2:	steve@examplecompany.com
E-Mail Address 3:	

Check **Enable E-mail alerting for IDS/IDP events**

Select sensitivity **Normal**

Enter SMTP server IP (email server): **192.168.2.4**

Enter sender: **idsalert@examplecompany.com**

Enter E-mail address 1: **webmaster@examplecompany.com**

Enter E-mail address 2: **steve@examplecompany.com**

Click *Apply*

4. Click *Activate* and wait for the firewall to restart.

When attacks are stopped by the firewall it will listed in the logs. Since we enabled email alerting in this example, emails will also be sent to the users **webmaster** and **steve**.

In this example we used the **prevention** mode. This means that the firewall will block all attacks. In **Inspection only** mode nothing will be blocked, the firewall will only log the attacks and send email alerts (if that is enabled).

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	RFC792

			Network (or subnet)	
		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

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 Routing Encapsulation	
50	ESP	Encapsulation Security Payload	RFC2406
51	AH	Authentication Header	RFC2402
108	IPComp	I 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

Appendix C: Multiple Public IP addresses

Mapping of a Public IP address other than that of the Firewall to a Server located on either internal interface can be accomplished in two basic steps (order does not matter): add a Port Mapping/Virtual Server rule that forwards specified services to a single LAN or DMZ host to be accessible through a WAN IP not used by the DFL-700; add a static route in the firewall's routing table indicating the internal interface to which the Public IP should be mapped. For an increased level of protection from Network Intrusions or malicious attacks, isolation of servers accessible to the public from the Private network is recommended. This will ensure that if one of those servers happens to become compromised through vulnerabilities related to software, an attacker would not be able to directly access the private internal Network. The DFL-700 provides a physical DMZ network interface specifically for this purpose. This can be accomplished with NAT disabled or enabled on the DMZ interface.

Example Scenario using NAT:

The firewall is configured using the following scheme in order to allow Internet hosts access to web services running on either the internal LAN or DMZ Network
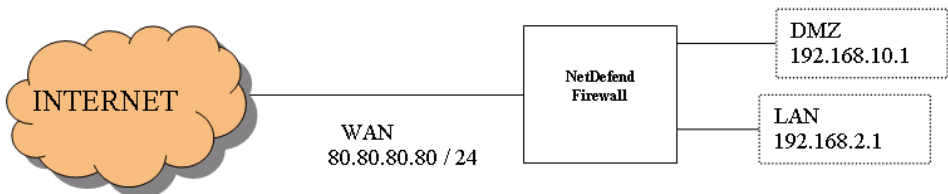
The goal is to map two internal web servers (port 80) to two Public IP addresses provided by our ISP.

Host Interface	Private IP	Public IP
Firewall LAN	192.168.2.1	80.80.80.80
Firewall DMZ	192.168.10.1	80.80.80.80
Web Server on LAN	192.168.2.50	80.80.80.81
Web Server on DMZ	192.168.10.100	80.80.80.82
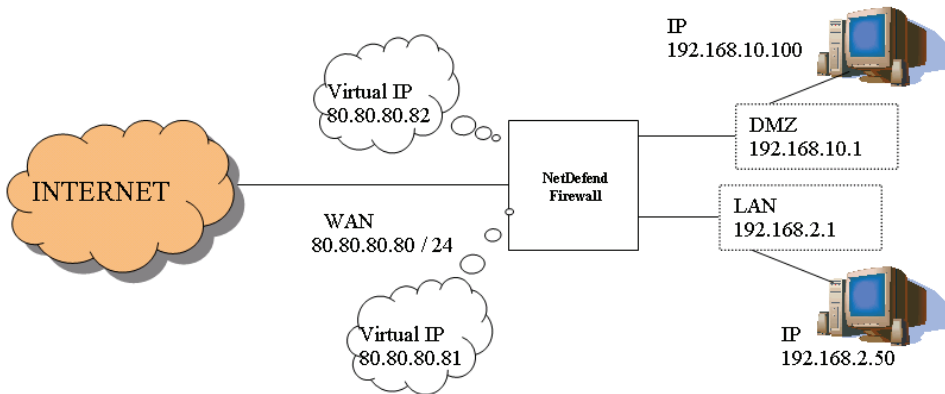
To accomplish this we need to create the following firewall settings:

- Configure two static routes (one for each public IP we wish to forward)
- Create two port mappings (one for each public IP mapping to each private Server)

Routing configuration:

Static Route Configuration for a Server on the LAN:

Navigate to the **SYSTEM** tab, then the **ROUTING** page of the Web-based configuration.

Select the **Add New** link to create the first static route.

Select the Interface that the Internal Server is connected to (**LAN** or **DMZ**).

Specify the Public IP to be forwarded in the **Network** field.

The **Subnet Mask** should be set to 255.255.255.255 (1-host).

Enable the **Proxy ARP** feature.

The above static route configuration explicitly defines the interface that the additional Public IP address should be forwarded to.

Routing Table

Edit **new** route:

Interface: DMZ ▾

Network: 80.80.80.82

Subnet Mask: 255.255.255.255 · 1 host (/32) ▾

Gateway: ☐ Network is behind remote gateway

0.0.0.0

Proxy ARP: ☑ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:

0.0.0.0

Static Route Configuration for a Server on the DMZ:

Navigate to the **SYSTEM** tab, then the **ROUTING** page of the Web-based configuration.

Select the **Add New** link to create the second static route.

Select the **Interface** that the Internal Server is connected to (LAN or DMZ).

Specify the Public IP to be forwarded in the **Network** field.

The **Subnet Mask** should be set to 255.255.255.255 (1-host).

Enable the **Proxy ARP** feature.

The above static route configuration explicitly defines the interface that the additional Public IP address should be forwarded to.

NOTE: Be sure to enable Proxy ARP for both routes or the Firewall will not forward traffic destined for the specified Public IP addresses to Internal servers.

Configure Port Mapping/Virtual Server Rules for LAN Server:

Virtual Server Configuration for a Server on the LAN:

Navigate to the **FIREWALL** tab, **PORT MAPPING** page of the Web-based configuration.

Click the **Add New** link to create a new Port Mapping.

Input the Public IP address to be forwarded in the **Destination IP** field.

Select the **Service** to be forwarded to the Internal Server (pre-defined or custom).

Enter the Private IP of the Server in the **Pass To** field.

Configure Scheduling, IDS/IDP, and/or Bandwidth Management if desired.

Click **Apply** to save the configuration.

Configure Port Mapping/Virtual Server Rules for DMZ Server:

Virtual Server Configuration for a Server on the DMZ:

    Navigate to the **FIREWALL** tab, **PORT MAPPING** page of the Web-based configuration.

    Click the **Add New** link to create a new Port Mapping.

    Input the Public IP address to be forwarded in the **Destination IP** field.

    Select the **Service** to be forwarded to the Internal Server (pre-defined or custom).

    Enter the Private IP of the Server in the **Pass To** field.

    Configure Scheduling, IDS/IDP, or Bandwidth Management if desired.

    Click **Apply** to save the configuration.

    Click **Activate Changes** to apply changes and restart.

Similar steps can be taken to configure other services to be mapped to Internal Servers for access from Public Hosts. Keep in mind that this configuration uses Network Address Translation. Not all Protocols will work through NAT, so be aware of the type of service in use.

Example Scenario using DMZ w/out NAT:

An alternative method to that described in the preceding pages is to isolate publicly accessible servers to the DMZ interface with NAT disabled. This configuration requires multiple (at least 2) Public IP addresses to function, as the Firewall will assume one IP and the Server(s) will use the other(s).

Configure the Static Routes:

Routing Table

Edit **192.168.10.234/255.255.255.255** route:

Interface: DMZ

Network: 192.168.10.234

Subnet Mask: 255.255.255.255 - 1 host (/32)

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☑ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

☐ **Delete this route**

Apply Cancel Help

A new route must be added to inform the firewall on which interface the Public IP will reside.

Navigate to **SYSTEM** > **ROUTING** in the web-based configuration of the DFL-700.

Click on **Add New** to create a new static route.

Select **DMZ** as the Interface. Enter the IP Address (WAN Network) you wish to forward to a server on the **DMZ** interface in the **Network** field.

Select a 32-bit subnet mask from the **Subnet Mask** dropdown box.

Be sure to have **Proxy ARP** enabled by checking the checkbox.

Click **Apply** to save any changes.

Modify Existing WAN Route:

Routing Table

Edit **192.168.10.0/255.255.255.0** route:

Note that this is the local network route for the interface; you can only change the Proxy ARP setting.

Interface: WAN ▾

Network: 192.168.10.0

Subnet Mask: 255.255.255.0   - 256 hosts (/24) ▾

Gateway: ☐ Network is behind remote gateway
0.0.0.0

Proxy ARP: ☑ Publish network on all other interfaces via Proxy ARP

Additional IP: ☐ Additional firewall IP address that hosts can use as gateway:
0.0.0.0

Apply   Cancel   Help

The default WAN route must be modified to enable **Proxy ARP**. The default route for any interface cannot be deleted or modified other than to enable the Proxy ARP feature.

From the **SYSTEM** > **ROUTING** page select **WAN** to edit the default route of the WAN interface.

Enable the **Proxy ARP** feature by checking the checkbox.

After making configuration changes, be sure to click **Apply** to save those changes to RAM.

Disable NAT on the DMZ Interface:

Firewall Policy

Show policy: LAN->WAN   LAN->DMZ   WAN->DMZ
               WAN->LAN   DMZ->LAN   **DMZ->WAN**

Settings for DMZ->WAN policy:

NAT: ○ Hide source addresses (many-to-one NAT)

       ◉ No NAT - requires public IP addresses on DMZ network.

✓ **Apply**   ✗ **Cancel**   ✚ **Help**

Select "Add New" below, or select a rule from the list to edit it:

By default the DFL-700 is enabled to perform NAT on both LAN and DMZ interfaces. Disable NAT on the DMZ interface.

Navigate to **Firewall > Policy** in the web-based configuration. Click on **DMZ->WAN** to modify the behavior of the DMZ interface.

Select the **No NAT – requires public IP addresses on DMZ network** radio button.

After making configuration changes click on the **Apply** button to save those changes.

To allow services on the DMZ interface to be accessible from the WAN, incoming policies must be defined to allow those services. This can be done through the **WAN->DMZ** section in the Firewall Policy configuration section.

Once all changes are final, those changes must be activated. Click on the **Activate** button under the left-hand-side menu. Follow the on-screen instructions to finalize your configuration.

Appendix D: HTTP Content Filtering

HTTP Content Filtering Global Policy

Protection from malicious or improper web content is a must for Business owners and concerned parents alike. There are numerous vehicles for hackers to damage or take control of one's PC or even Network. Malicious code may be delivered in deviously crafted ActiveX controls, Java Scripts, cookies, or tainted file downloads. Many times executable (*.exe) files are laced with spy-ware or viral programs that become active and take over after the program is run for the first time.

To help reduce the likelihood of malicious software reaching the PCs on the LAN or DMZ of the NetDefend Firewall, filtering of HTTP traffic can be customized and enabled. This filter can be configured to strip ActiveX objects (including flash), Java Applets, Visual Basic/Java Scripts, and or block cookies. In addition, a Whitelist is configurable to define URLs that will always be allowed. Conversely a Blacklist is provided to allow customizable filtering of websites, domains, and even file types based on file extension. All of the aforementioned filters function simultaneously (if enabled/configured) when HTTP content filtering is enabled. In order for HTTP content filtering to be performed, all HTTP traffic must pass-through an outbound policy utilizing the HTTP ALG. Due to this behavior content filtering can be applied to either LAN or DMZ interface simultaneously or independent of one another. Keep in mind that the content filtering specifications are global and will apply to every instance of a rule using the HTTP ALG.

Two configurations need to be made in order to use HTTP Content Filtering:

- The Whitelist and Blacklist must be customized to suit the desired filtering requirements.

- HTTP traffic on an interface (LAN or DMZ) must be bound to a rule using the HTTP ALG.

The Whitelist

Items entered in the Whitelist will always be allowed through the firewall, assuming HTTP content filtering is enabled. This section should only be used to allow essential domains and servers, such as Microsoft.com and DLink.com to ensure the ability to locate and download critical updates or firmware is not hindered. Domains or websites entered in the Whitelist will not be subject to any of the content filtering functions.

Edit Destination URL Global Whitelist:

To allow access to a whole domain, use e.g. "*.safesite.com/*". Note the ending slash, which protects against someone setting up e.g. "www.safesite.com.dyndnsprovider.net" as an alias for an otherwise disallowed site.

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

```
# Access to sites that are important for software updates and
# require cookies / scripts:

d-link.com/*
*.d-link.com/*

dlink.com/*
*.dlink.com/*

d-link.com.tw/*
*.d-link.com.tw/*

dlink.com.tw/*
*.dlink.com.tw/*

microsoft.com/*
*.microsoft.com/*
```

Apply   Cancel   Help

Navigate to the **Firewall** tab, **Content Filtering** section of the web-administration.

Click on **Edit URL Black** List to modify or append the contents of the filtering database.
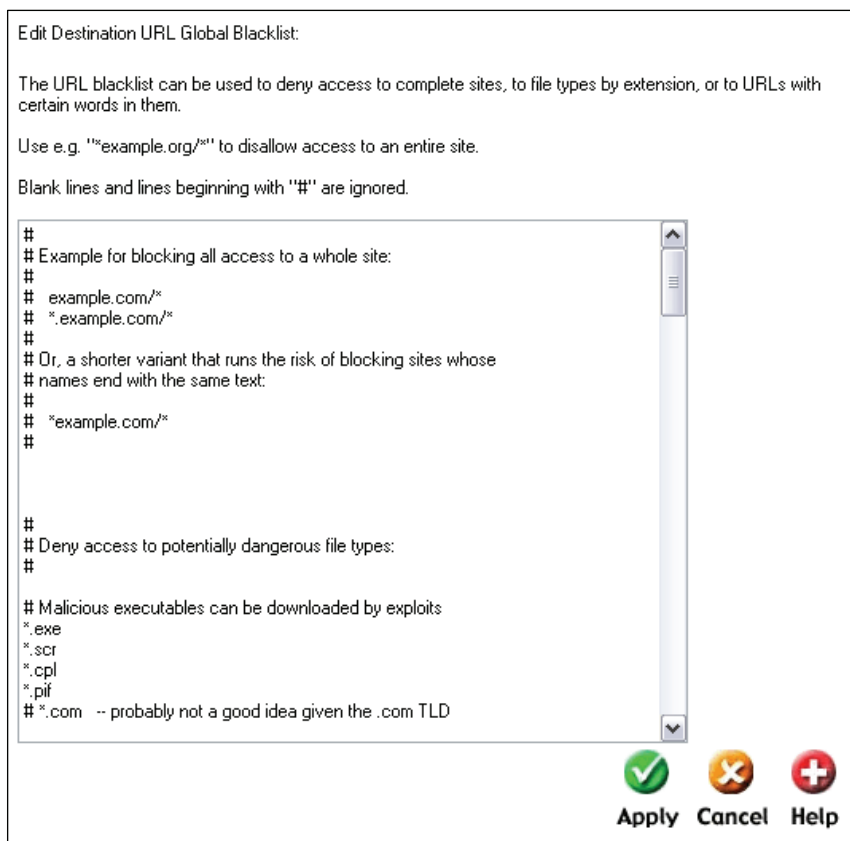
To allow an entire domain and all sub-domains use the following syntax

    dlink.com/*   # Allows access to the domain dlink.com

    .dlink.com/   # Allows access to all sub-domains in dlink.com

Once finished editing the Whitelist, click **Apply** to save changes or **Cancel** to clear.

The Blacklist

Blacklist configuration is not limited to domain names. File extensions may be specified to block the download of said file types. Be sure to evaluate the type of files that may be traversing the firewall out of necessity on a regular basis to ensure no loss in productivity due to invalid network configurations or network outages. Domains and/or file types defined in the Blacklist will be denied upon request.

```
Edit Destination URL Global Blacklist:

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.

Use e.g. "*example.org/*" to disallow access to an entire site.

Blank lines and lines beginning with "#" are ignored.

#
# Example for blocking all access to a whole site:
#
#   example.com/*
#   *.example.com/*
#
# Or, a shorter variant that runs the risk of blocking sites whose
# names end with the same text:
#
#   *example.com/*
#



#
# Deny access to potentially dangerous file types:
#

# Malicious executables can be downloaded by exploits
*.exe
*.scr
*.cpl
*.pif
# *.com   -- probably not a good idea given the .com TLD
```

✅ **Apply** ❌ **Cancel** ➕ **Help**

Navigate to the **Firewall** tab, **Content Filtering** section of the web-administration.

Click on **Edit URL Black** List to modify or append the contents of the filtering database.

To block an entire domain and all sub-domains use the following syntax

    casino.com/*   # Blocks access to the domain casino.com

    .casino.com/   # Blocks access to all sub-domains under casino.com

To block specific file types from download through HTTP use the following syntax

    *.exe   # Blocks executable downloads

Once finished editing the Blacklist, click **Apply** to save changes or **Cancel** to clear.

Additional Content Filters

The Firewall can also filter Java Applets, Java/VB Script, ActiveX objects, and/or cookies from reaching the PCs behind the NetDefend Firewall. These content categories do not require configuration other than enable or disable.

Active content handling:

☑ Strip ActiveX objects (including Flash)

☑ Strip Java applets

☑ Strip Javascript/VBScript

☑ Block Cookies

Navigate to the **Firewall** tab, **Content Filtering** section of the web-administration.

Click the check box next to each filter you would like to enable.

Once finished selecting additional filters, click **Apply** to save changes or **Cancel** to clear.

HTTP Rule using the HTTP ALG

Now that the content to be filtered has been decided on, a rule needs to be configured for each interface that this filtering should be applied to utilizing the HTTP ALG. This will require a rework of the default outbound policy to eliminate the chance of unfiltered HTTP traffic passing through the Firewall. The idea is to remove the most general allow rule and configure rules to allow essential services such as DNS as well HTTP to pass the Firewall.

Edit **allow_standard** rule (#4):

Name:	allow_standard
Position:	4 Moves before given position. Blank = last.
Action:	Allow

Source Nets:

... Users/Groups: "Any" = Any authenticated

Destination Nets:

... Users/Groups: "Any" = Any authenticated

Leave source and/or destination blank to match everything.

Service: All

Custom source ports: Blank = any port

... destination ports:

Schedule: - Always -

☐ **Intrusion Detection / Prevention:**

Mode: Inspection only

Alerting: ☐ Enable IDS/IDP alerting via email for this rule

☑ **Delete this rule**

Apply   Cancel   Help

To disable the default general allow all rule -

Navigate to the **Firewall** tab, **Policy** section of the web-administration.

Select the appropriate policy based on desired effect (**LAN->WAN** or **DMZ->WAN**).

Click **Edit** next to the default allow all rule.

Check the check box next to **delete this rule**.

Click **Apply**.

To allow DNS queries to pass through

Navigate to the **Firewall** tab, **Policy** section of the web-administration.

Select the appropriate policy based on desired effect (**LAN->WAN** or **DMZ->WAN**).

Click **Add New** at the bottom of the list.

Give the rule a friendly name, such as **dns_out**.

Position does not matter, leave blank or choose a position.

Choose **Allow** as the Action.

For service choose **dns_all**.

Select a schedule and enable IDS/IDP if desired.

Click **Apply** to save the changes, or click **Cancel** to disregard.

```
Edit new rule:

              Name: [ http_cntnt_fltr ]
           Position: [ 1 ]    Moves before given position. Blank = last.
            Action: [ Allow            v ]

        Source Nets: [                              ]
     ... Users/Groups: [                              ]   "Any" = Any authenticated
    Destination Nets: [                              ]
     ... Users/Groups: [                              ]   "Any" = Any authenticated
                     Leave source and/or destination blank to match everything.

           Service: [ http-outbound  v ]
                     Custom source ports: [              ]  Blank = any port
                      ... destination ports: [              ]

          Schedule: [ - Always - v ]

    [ ] Intrusion Detection / Prevention:
              Mode: [ Inspection only  v ]
           Alerting: [ ] Enable IDS/IDP alerting via email for this rule

                                              Apply   Cancel   Help
```

To configure the HTTP Content Filtering rule -

Navigate to the **Firewall** tab, **Policy** section of the web-administration.

Select the appropriate policy based on desired effect (**LAN->WAN** or **DMZ->WAN**).

Click **Add New** at the bottom of the list.

Give the rule a friendly name, such as **http_cntnt_filtr**.

Position does not matter, leave blank or choose a position.

Choose **Allow** as the Action.

For service choose **http_outbound** (already configured to use the HTTP ALG).

Select a schedule and enable IDS/IDP if desired.

Click **Apply** to save the changes, or click **Cancel** to disregard.

After clicking Apply, click the **Activate** button on the left-hand menu.

Select **Activate Changes Now** to save the configuration to flash and restart.

When the firewall has finished restarting, the HTTP Content Filtering Function will be enabled and active. Keep in mind that depending on the type of activities your LAN participates in, more services may need to be specified as rules in the Firewall Policy configuration to allow said services to pass the firewall. The steps should be similar to the DNS and HTTP configuration if there is a default service configured. Custom services can also be created to accommodate most any service needed to run through the firewall.

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

D-Link or its authorized reseller or distributor and

Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

1-Year Limited Warranty for the Product(s) is defined as follows:

Hardware (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 during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. 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 have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. 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 retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that 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 or to refund at D-Link's sole discretion. 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. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. 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.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

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, if in D-Link's judgment, 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; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER 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.

FCC Statement: **This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in an industrial 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 communication. 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.

For detailed warranty outside the United States, please contact corresponding local D-Link office.

CE Mark Warning: This is a Class A product. In an Industrial environment, this product may cause radio interference, in which case the user may be required to take adequate measures.