

# DFL-1100

## INSTALLATION GUIDE



## Package Contents

- D-Link<sup>®</sup> DFL-1100 NETDEFEND<sup>™</sup> Network Security Firewall
- CAT5 UTP Straight-Through Ethernet Cable
- CAT5 UTP Crossover Cable
- RS-232 Console Interface Cable
- CD-ROM (Containing Manual)
- Power Cord

## System Requirements

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

# Hardware Overview

## Front Panel



LED	Function
<b>Link</b>	Solid green indicates a good connection on the associated port number.
<b>Act</b>	The Act LED flashes during data transmission on the associated port number.
<b>Power</b>	A solid light indicates a proper connection to the power supply.
<b>Status</b>	LED should flash to indicate an active system. (If the status LED is lit solid and not flashing, please contact D-Link® Technical Support.)

Port	Description
<b>Console</b>	Direct connection to your computer's serial port using an RS-232 cable for firewall configuration. (The console settings are: Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1)
<b>WAN</b>	Attaches to your external router, DSL modem, or cable modem.
<b>LAN</b>	Connects to your internal network.
<b>DMZ</b>	Connects to internal servers that will be visible from the Internet (FTP, SNMP, HTTP, and DNS).
<b>ETH4/Sync</b>	Can be used as an extra LAN port, DMZ port, or Sync interface when using High Availability.

## Rear Panel



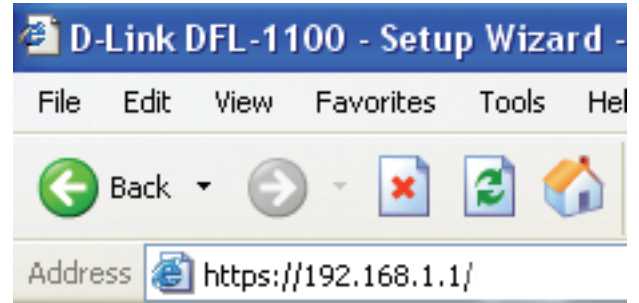
Item	Description
<b>Power Connector</b>	The power cord attaches here.
<b>Power Switch</b>	Powers the unit off and on.
<b>Cooling Fans</b>	Be sure to keep the unit in a well ventilated area and do not block the cooling fan vents.

# Hardware Installation

1. Connect the power cord to the power connector on the rear panel of the DFL-1100. Plug the other end of the power cord to a wall outlet or power strip.
2. Turn on the power switch on the rear panel of the DFL-1100. The Power LED will illuminate.
3. Power off your broadband modem. Some modems may not have an on/off switch and will require you to unplug the power adapter.
4. Connect an Ethernet cable to the Ethernet jack of your broadband modem and then connect the other end of the Ethernet cable to the WAN port on the front panel of the DFL-1100.
5. Power on the broadband modem. It may take a few seconds for your modem to initialize but then the WAN port LED should illuminate to indicate a proper connection.
6. Connect an Ethernet cable to the LAN port on the front panel of the DFL-1100. Connect the other end of the Ethernet cable to your network hub or switch. The LAN port LED should illuminate to indicate a proper connection.
7. Connect the computer that you will use to configure the DFL-1100 to the network hub or switch (if it isn't already connected). Be sure that the configuration PC is setup to obtain an IP address automatically. It may be necessary to release and renew the IP address.

# The Setup Wizard

The DFL-1100 provides Web based configuration. You can configure your DFL-1100 using Internet Explorer or Netscape Navigator version 6.0 or above with JavaScript enabled. To access the configuration screen, launch your Web browser and enter the IP address of the DFL-1100 in the address field and press enter. If using the DFL-1100's default IP address, you would enter **https://192.168.1.1** (Note: Include the "s" at the end of **https** to ensure a secure connection).

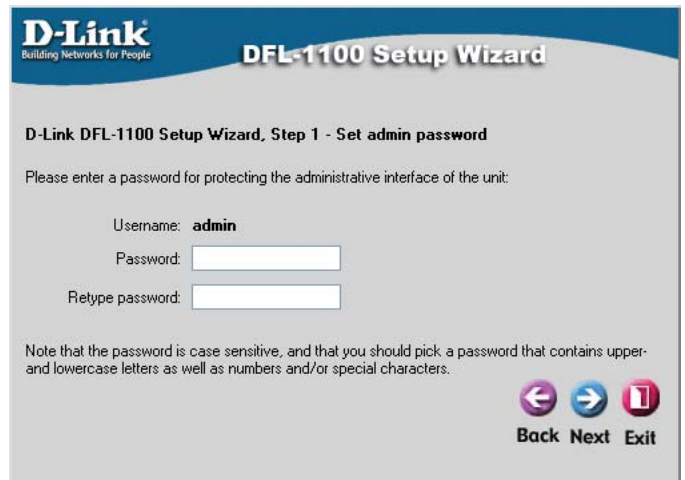


Once you've connected to the DFL-1100, the Setup Wizard automatically begins. It is recommended that you connect to the DFL-1100 using secure HTTP only. To do so, select **Secure HTTP (HTTPS) only** and click **Next**.



## Step 1 - Set admin password

Enter a password for the admin account and retype it for confirmation. Click **Next** to continue.



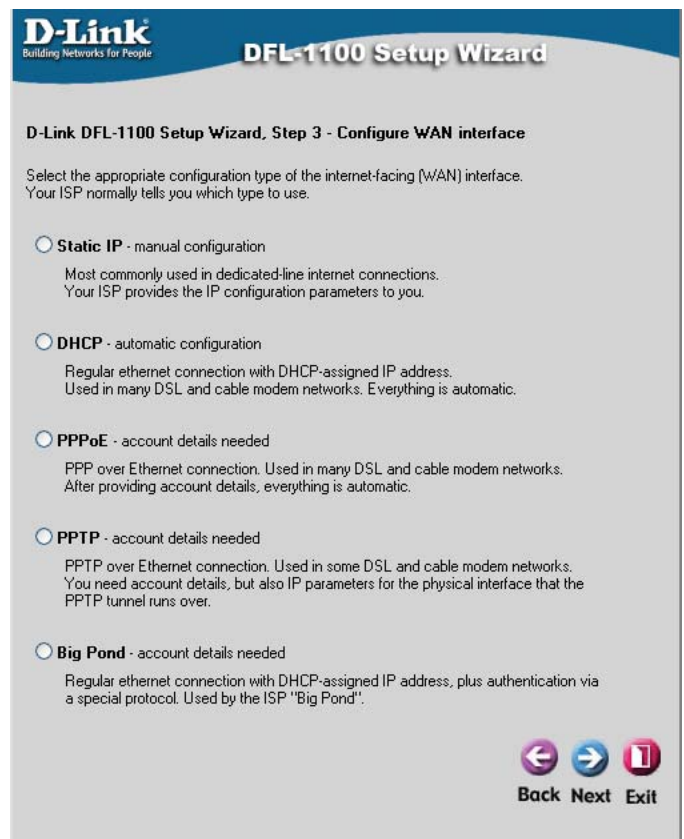
## Step 2 - Set timezone

Select your time zone and daylight savings time settings. Click **Next** to continue.



## Step 3 - Configure WAN interface

Select the type of Internet connection that you have. If you are unsure of which to select, please contact your Internet Service Provider. Click **Next** to continue. If you selected DHCP, proceed to step 4 on page 8.



### Step 3 - Static IP

If you selected Static IP, enter the IP address information provided by your Internet Service Provider. You must complete all of the fields except for Secondary DNS Server. Click **Next** and continue to Step 4 on page 8.

The screenshot shows the 'D-Link DFL-1100 Setup Wizard' interface for 'Step 3 - Configure WAN interface'. The title bar includes the D-Link logo and the text 'Building Networks for People' and 'DFL-1100 Setup Wizard'. Below the title bar, the text reads 'D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface'. A descriptive paragraph states: 'Static WAN interface configuration is most commonly used in dedicated-line internet connections. Your ISP usually provides this information to you.' The form contains the following fields: 'IP Address:' with a text input box; 'Subnet Mask:' with a dropdown menu showing '255.255.255.0 - 256 hosts (/24)'; 'Gateway IP:' with a text input box; 'Primary DNS Server:' with a text input box; and 'Secondary DNS Server:' with a text input box and '(optional)' text to its right. At the bottom right, there are three buttons: a left arrow labeled 'Back', a right arrow labeled 'Next', and a red square with a white 'I' labeled 'Exit'.

### Step 3 - PPPoE

If you selected PPPoE, you will have to fill out the user name and password provided by your Internet Service Provider. Leave the PPPoE Service Name field blank unless instructed by your Internet Service Provider. Click **Next** and continue to Step 4 on page 8.

The screenshot shows the 'D-Link DFL-1100 Setup Wizard' interface for 'Step 3 - Configure WAN interface'. The title bar includes the D-Link logo and the text 'Building Networks for People' and 'DFL-1100 Setup Wizard'. Below the title bar, the text reads 'D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface'. A descriptive paragraph states: 'PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.' The form contains the following fields: 'Username:' with a text input box; 'Password:' with a text input box; 'Retype Password:' with a text input box; and 'Service Name:' with a text input box and '(Some ISPs require the Service Name to be filled out.)' text below it. At the bottom right, there are three buttons: a left arrow labeled 'Back', a right arrow labeled 'Next', and a red square with a white 'I' labeled 'Exit'.

### Step 3 - PPTP

If you selected PPTP, you will need to specify both the tunnel parameters and the physical interface parameters. Click **Next** and continue to Step 4 on page 8.

**D-Link** Building Networks for People **DFL-1100 Setup Wizard**

**D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface**

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.

### Step 3 - Big Pond

If you selected Big Pond, fill out the username and password and then retype the password. This information is provided to you from your Internet Service Provider. Click **Next** to continue.

**D-Link** Building Networks for People **DFL-1100 Setup Wizard**

**D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface**

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

Username:

Password:

Retype Password:

## Step 4 - Set up built-in DHCP Server

- **Disable DHCP Server:** If this option is disabled, then LAN clients must be configured with an IP address manually.
- **Enable DHCP Server:** When enabled, this allows the DFL-1100 to automatically provide the necessary IP information to all LAN clients configured for DHCP. The IP range defines the beginning and ending addresses to provide the clients.

*Be sure the IP range does not conflict with any manually configured network devices or the IP address of the DFL-1100.*

**D-Link**  
Building Networks for People

### DFL-1100 Setup Wizard

D-Link DFL-1100 Setup Wizard, Step 4 - Set up built-in DHCP server

You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.

Disable DHCP Server

Enable DHCP Server

Enter a range of IP addresses to hand out to DHCP clients:

IP Range:

Back Next Exit

## Step 5 - Configure helper servers

- **Time Servers:** When enabled, the firewall time will be synchronized with the NTP servers entered here.
- **Syslog Servers:** When enabled, the DFL-1100 will log data to the specified servers.

**D-Link**  
Building Networks for People

### DFL-1100 Setup Wizard

D-Link DFL-1100 Setup Wizard, Step 5 - Configure helper servers

**Time servers** - for automatically keeping the unit's time accurate

Primary NTP Server:

Secondary NTP Server:  (optional)

**Syslog servers** - for receiving log data from the unit

If both servers are configured, logs will be sent to both at the same time.

Syslog server 1:

Syslog server 2:  (optional)

Back Next Exit

## Setup Wizard Complete

Click on **Restart** to finalize the configuration.

**D-Link**  
Building Networks for People

### DFL-1100 Setup Wizard

D-Link DFL-1100 Setup Wizard Complete

Click Restart to finalize the configuration.

After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.

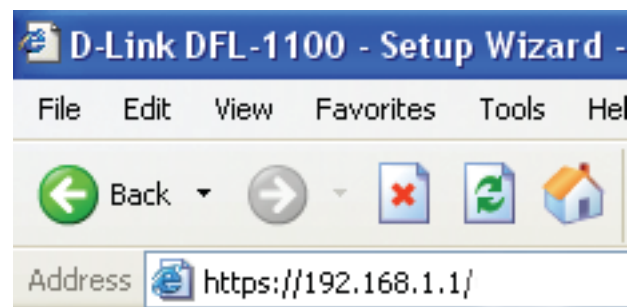
Back Restart Exit



A message will appear indicating that the unit is restarting.



After you've configured the unit, you will need to reconnect to the web browser interface. Type in **https://192.168.1.1**. Be sure to include the "s" in **https**.

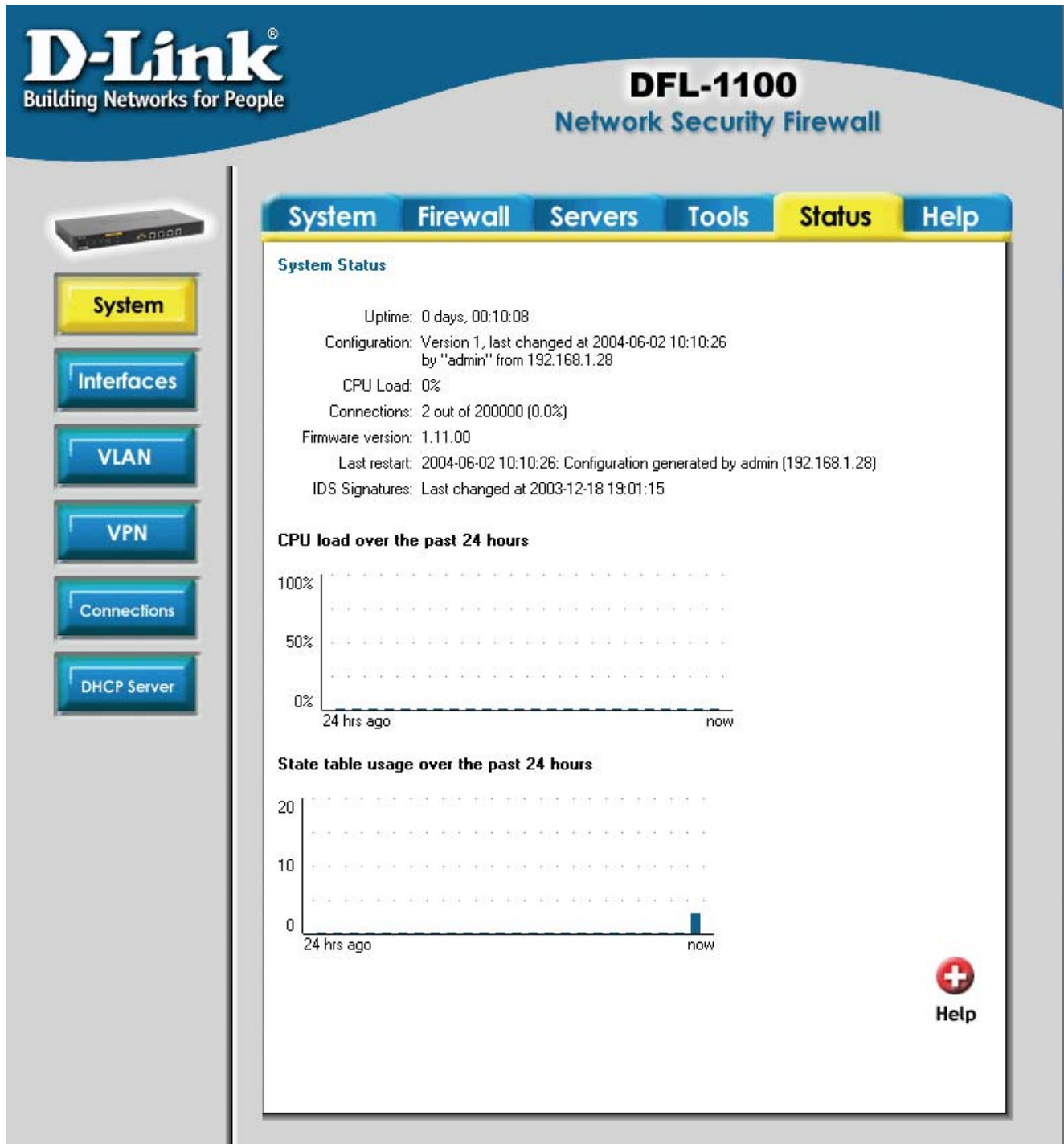


Type in the admin username and the password that you defined during the Setup Wizard.



## Installation is complete!

You should see the System Status screen after reconnecting to the DFL-1100.



**D-Link**  
Building Networks for People

**DFL-1100**  
Network Security Firewall

System | Firewall | Servers | Tools | **Status** | Help

**System Status**

Uptime: 0 days, 00:10:08  
Configuration: Version 1, last changed at 2004-06-02 10:10:26 by "admin" from 192.168.1.28  
CPU Load: 0%  
Connections: 2 out of 200000 (0.0%)  
Firmware version: 1.11.00  
Last restart: 2004-06-02 10:10:26; Configuration generated by admin (192.168.1.28)  
IDS Signatures: Last changed at 2003-12-18 19:01:15

**CPU load over the past 24 hours**


100%  
50%  
0%

24 hrs ago now

**State table usage over the past 24 hours**

20  
10  
0

24 hrs ago now

 Help

# Activating Changes to the D-Link® DFL-1100

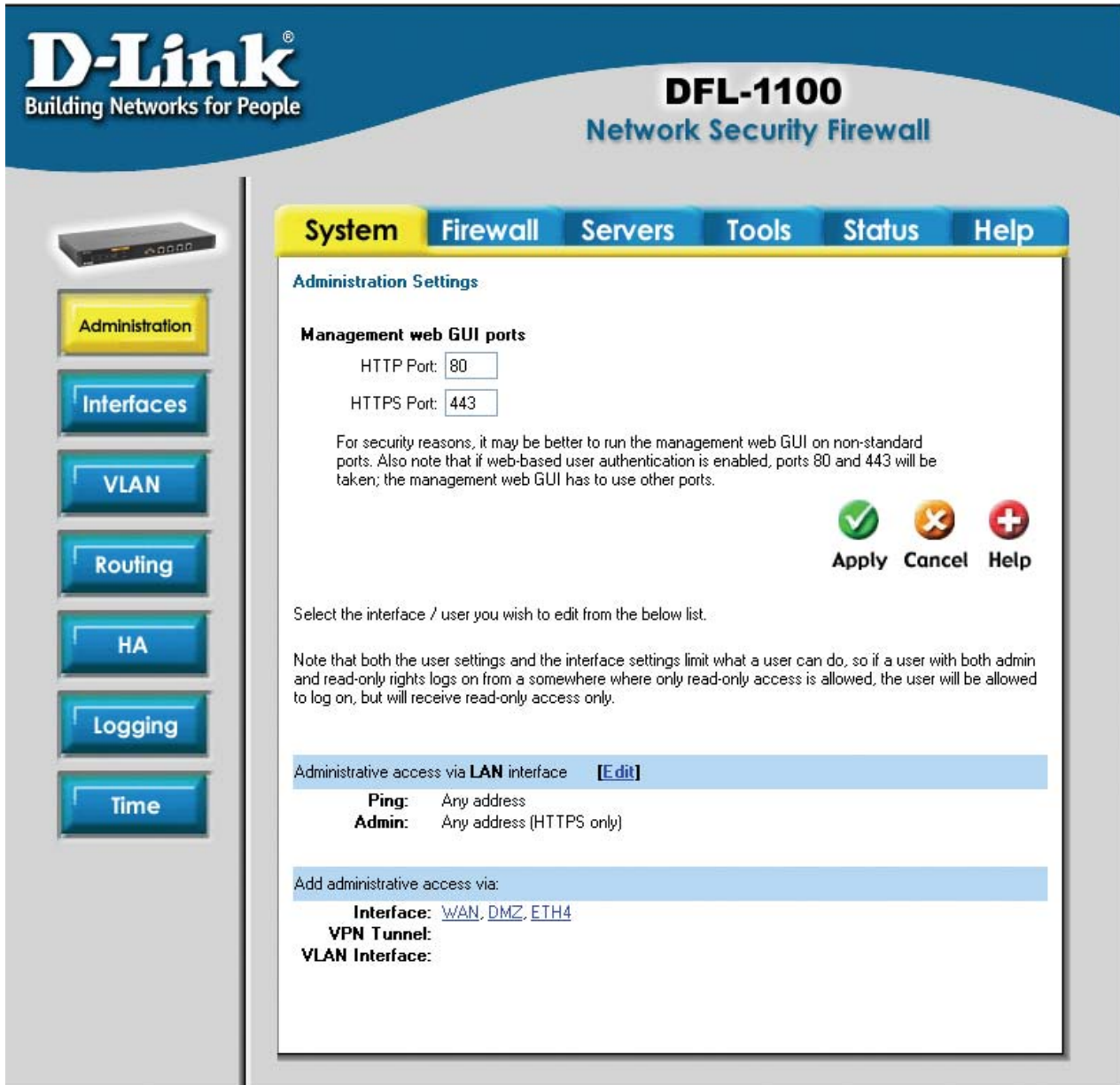
When changes are made to the configuration of the DFL-1100, two new buttons appear below the existing menu buttons. Once all changes to the configuration of the DFL-1100 have been made, click on the **Activate** button to go to the Activate Changes window. Once the changes are activated, the admin account must login within the timeout period configured on this page. If not, the changes will be discarded and the previous configuration will be used. Once you've set the desired timeout period, click the **Activate Changes** button to activate the configuration changes. The DFL-1100 will save the configuration, reload it, and the new changes will take effect. To ensure the configuration changes are permanent, you must login with the admin account within the established time period.






# Administration Settings

The Administration settings screen can be found by clicking on the **System** tab and selecting the **Administration** button. By default, administrative access is limited to the **LAN** interface. The selection you made during the Setup Wizard determines whether you can access the DFL-1100 via **HTTP and HTTPS** or only via **HTTPS**. Additional interfaces can be configured for administrative access by selecting the appropriate interface ([WAN](#), [DMZ](#), or [ETH4](#)).

**Management web GUI ports:** These are the HTTP and HTTPS ports being utilized by the DFL-1100 for web-based configuration. The default settings are the standard port 80 for HTTP and port 443 for HTTPS. For security reasons, you may want to use non-standard port numbers.



The screenshot shows the D-Link DFL-1100 Network Security Firewall web interface. The top navigation bar includes tabs for System, Firewall, Servers, Tools, Status, and Help. The left sidebar contains buttons for Administration, Interfaces, VLAN, Routing, HA, Logging, and Time. The main content area is titled "Administration Settings" and contains the following sections:

- Management web GUI ports:** HTTP Port: ; HTTPS Port:
- 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.
- Buttons:  **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)
- Add administrative access via:
- Interface:** [WAN](#), [DMZ](#), [ETH4](#)
- VPN Tunnel:**
- VLAN Interface:**

You may selectively add administration features to any of the interfaces. To do so, click on the desired interface ([WAN](#), [DMZ](#), or [ETH4](#)) under the heading titled **Add administrative access via:** or click on [Edit](#) next to an interface that has already been configured.

**Note: User settings and interface settings limit what a user can do. So if a full admin user logs on via an interface configured with read-only access, the user will only receive read-only access.**

Any of the settings below can be limited to specific IP addresses (192.168.0.0/24, 10.0.0.5 - 10.0.0.9) by entering the ranges in the **Networks:** field. When left blank there are no IP address restrictions.

**Ping:** If enabled, specifies the IP addresses/range that can ping the interface of the DFL-1100. The default setting allows everyone to ping the interface IP.

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

Networks:  Blank = Any

**Admin:** If enabled, allows users with admin rights to access the specified interface with full access to the web-based configuration. Configuration via **HTTP and HTTPS** or only **HTTPS** can also be configured.

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

Networks:  Blank = Any

Protocol:

**Read-Only:** If enabled, allows users to view but not modify the DFL-1100 configuration from the specified interface. Viewing via **HTTP and HTTPS** or only **HTTP** can also be configured.

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

Networks:  Blank = Any

Protocol:

**SNMP:** Specifies if SNMP should be allowed or not for the specified interface. The DFL-1100 supports read-only access.

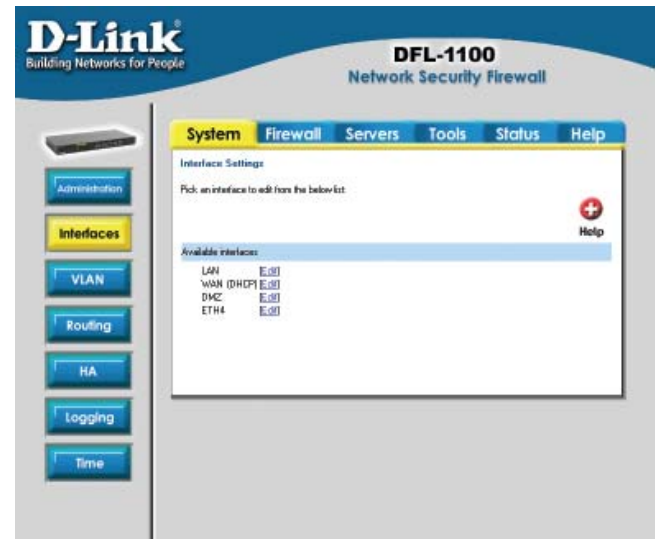
**SNMP** - Simple Network Management Protocol (read-only access)

Networks:  Blank = Any

Community:

# WAN Interface Settings

When you first connect to the DFL-1100, the Setup Wizard guides you through configuring the basic firewall settings. Your WAN settings are configured at that time. Should you need to modify these settings, go to the **System** tab and click on the **Interfaces** button. Click on the [Edit](#) option next to WAN.



## Static IP

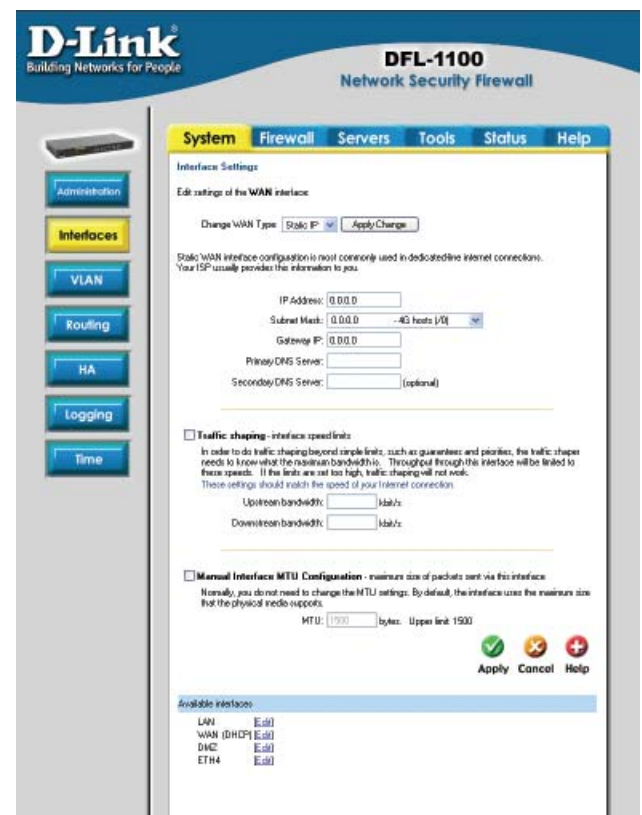
If your Internet connection uses a Static IP Address, this information is provided to you by your Internet Service Provider. All fields are mandatory except for the Secondary DNS Server.

**IP Address:** The IP Address of the WAN interface. This is the address that is used to ping the firewall, remotely control it, and as a source address for dynamically translated connections.

**Subnet Mask:** Network and subnet identifier.

**Gateway IP:** Specifies the IP address of the default gateway used to reach the Internet.

**Primary and Secondary DNS Server:** The IP address(es) of your DNS Server(s). Only the Primary DNS Server is required.



## DHCP

If using DHCP, there is no need to enter any values.



## PPPoE

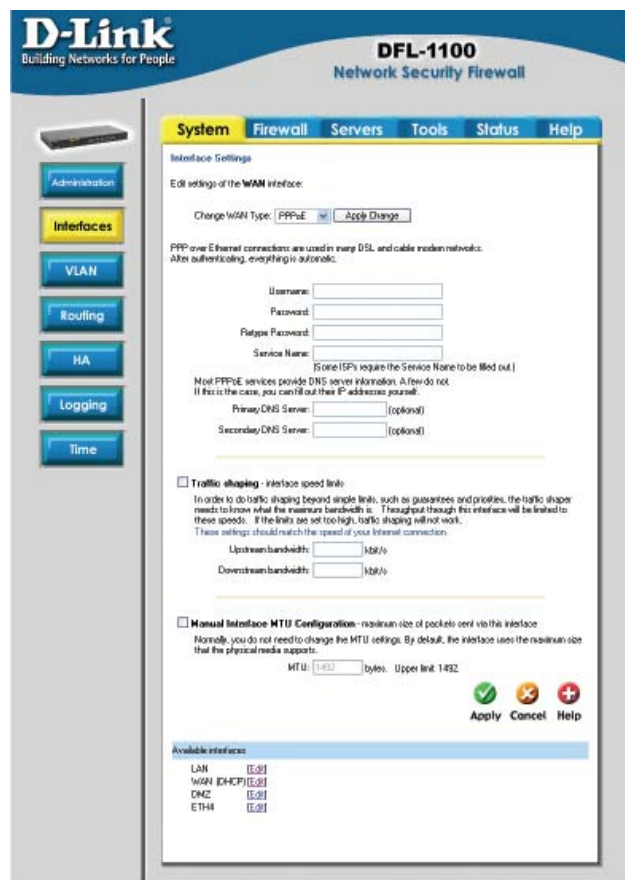
If you are using a PPPoE connection, you must enter the username and password, retype the password, and enter any other information your Internet Service Provider (ISP) requires.

**Username:** The login or username supplied by your ISP.

**Password:** The password associated with the login or username.

**Service Name:** Only use this option if required by your ISP. They will provide you the Service Name to enter.

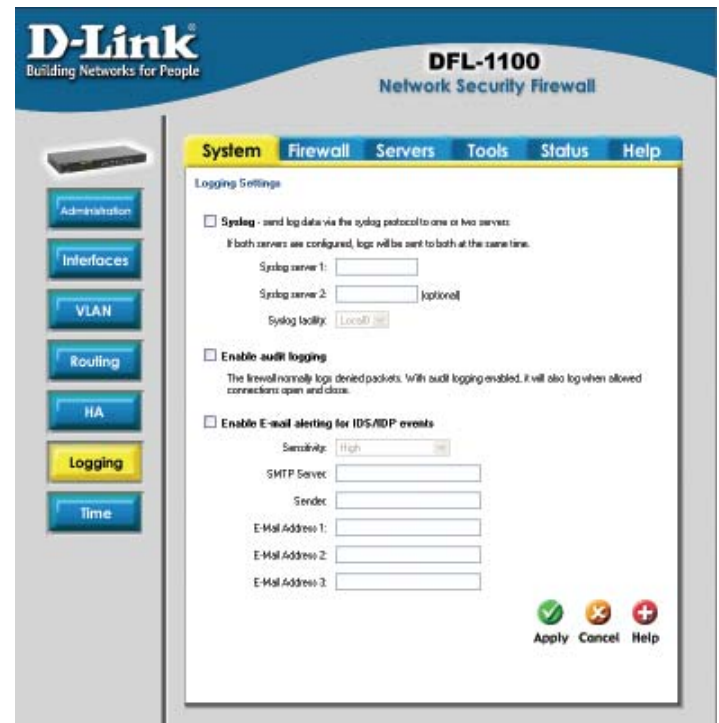
**Primary and Secondary DNS Server:** The IP addresses of your DNS servers. These are optional and often provided by the PPPoE service.



# Logging

To go to the logging configuration screen, select the **System** tab and click on the **Logging** button.

Logging allows you to track events such as startup, shutdown, and the opening and closing of connections. The startup and shutdown events are always logged. Events such as the opening and closing of allowed connections are user configurable. The DFL-1100 sends the log data to one or two Syslog servers. An e-mail alert for IDS/IDP events can be generated for up to three e-mail addresses.



## To Enable Logging

1. Place a checkmark in the Syslog box.
2. Enter the name of your first Syslog server in the **Syslog server 1** text box. If you have a second Syslog server, enter the server name in the Syslog server 2 text box. At least one Syslog server must be entered for logging to work.
3. Specify what facility to use by selecting the appropriate Syslog facility. The Syslog facility is a label to identify where a message originated from. The facility value is used by the PC running the Syslog Daemon to sort messages. **Local0** is the default value, as this is the usual value assigned to a firewall.
4. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

## To Enable Audit Logging

To start auditing all firewall traffic, simply place a checkmark in the **Enable audit logging** box. Be sure to click **Apply** to apply the setting or click **Cancel** to discard the changes.

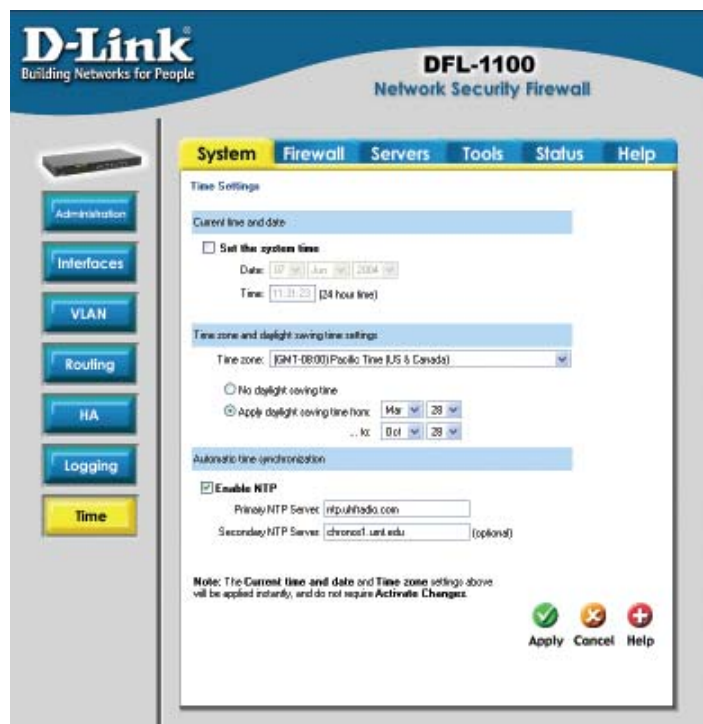
## To Enable E-mail alerting for IDS/IDP events

1. Place a checkmark in the **Enable E-mail alerting for IDS/IDP events** box.
2. Select a Sensitivity level. There are five levels of sensitivity for IDS/IDP e-mail reporting. Very High (top level) will issue an e-mail alert for any type of attack in the IDS signature file. Lower sensitivity settings will reduce the amount of e-mail alerts but will not reduce the level of IDS protection.
3. In the SMTP Server field, type in the address of the SMTP server that the DFL-1100 should use to send e-mail.
4. The DFL-1100 will send out e-mail alerts to up to 3 valid e-mail addresses. Enter the e-mail addresses in the appropriate textbox.
5. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.



# Time

The time configuration screen can be found by selecting the **System** tab and then clicking on the **Time** button. The time can be set manually or synchronized to an Internet Network Time Server.



## Changing the Time Zone

1. Select the correct time zone from the dropdown menu.
2. Specify your daylight savings time or select no daylight savings time by selecting the appropriate radio button.
3. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

## Using NTP to Sync Time

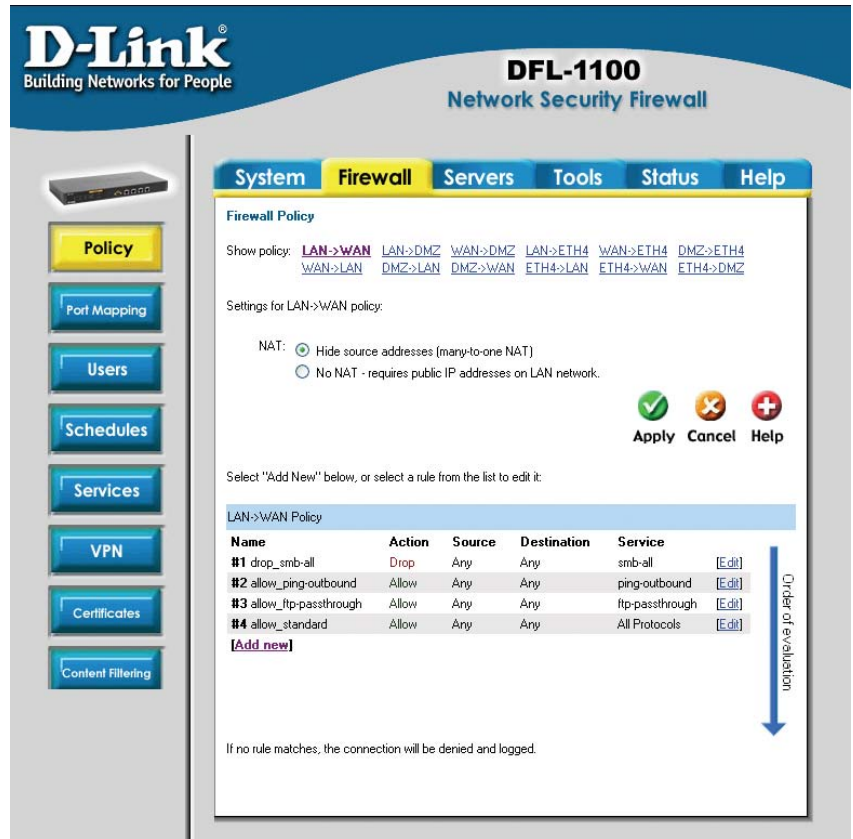
1. Enable synchronization by checking the Enable NTP box.
2. Enter the server IP address or server name with which you want to synchronize.
3. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

## Setting the Time and Date Manually

1. Place a checkmark in the **Set the system time** box.
2. Select the correct date from the dropdown boxes.
3. Enter the correct time in 24-hour format.
4. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

# Firewall Policy

The DFL-1100 allows you to configure policies to handle data being transmitted and received via the various interfaces. The policy configuration window can be found by going to the **Firewall** tab and the **Policy** button is the default selection.



## Adding a New Policy

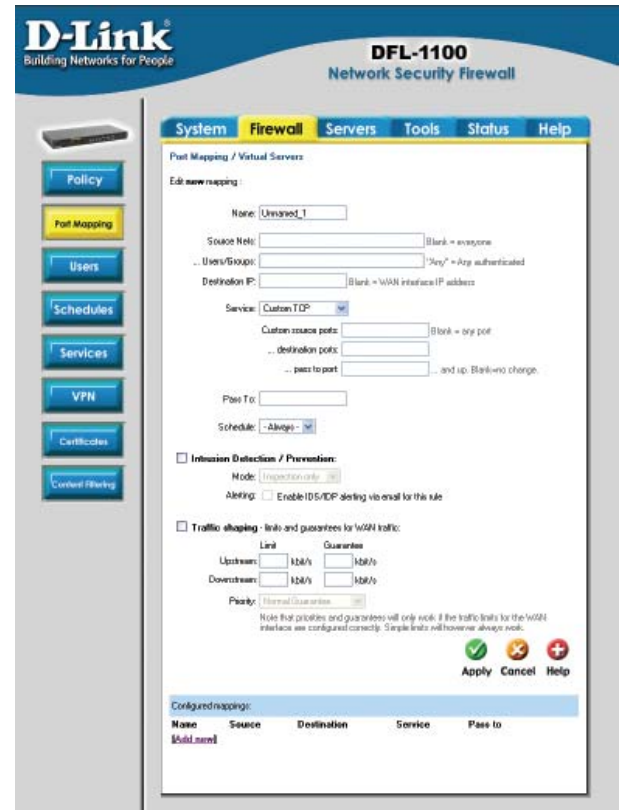
1. Select the desired interfaces to create a policy for. For instance, **LAN > WAN** would create a policy for data from the internal LAN to the Internet.
2. Click on the **Add new** link.
3. Fill in the appropriate values for the following options:

<b>Name</b>	Create a name for the policy. This name is used mainly as a rule reference in log data and for easy reference in the policy list.
<b>Action</b>	Select the action to be performed with the specified data.
<b>Source Nets</b>	Specifies the sender span of IP addresses to be compared to the received packet. Leave this blank to match everything.
<b>Source Users/Groups</b>	Here you can specify that a username, group, or any authenticated user must be the source for the action to occur. A list of usernames can be entered, separated by a comma, or write Any to represent any authenticated user. If it's left blank there is no need for authentication for this policy.
<b>Destination Nets</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet. Leave this blank to match everything.
<b>Destination Users/Groups</b>	A specific username can be specified for this policy to match. A list of usernames can be entered, separated by a comma, or write Any for any authenticated user. If it's left blank there is no need for authentication for this policy.
<b>Service</b>	A predefined service can be selected from the dropdown menu or a custom service can be created.
<b>Schedule</b>	Select what schedule should be used for this policy to match. Choose Always for no scheduling.

4. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

# Port Mapping / Virtual Servers

The Port Mapping / Virtual Servers configuration section allows you to configure virtual servers such as Web servers. Mappings are read from top to bottom. The first matching mapping is carried out. The Port Mapping / Virtual Servers configuration screen can be found by going to the **Firewall** tab and clicking on the **Port Mapping** button.



## Adding a New Mapping

1. Click the **Add new** link.
2. Fill in the following values:

<b>Name</b>	Create a name for the policy. This name is used mainly as a rule reference in log data and for easy reference in the policy list.
<b>Action</b>	Select the action to be performed with the specified data.
<b>Source Nets</b>	Specifies the sender span of IP addresses to be compared to the received packet. Leave this blank to match everything.
<b>Source Users/Groups</b>	Here you can specify that a username, group, or any authenticated user must be the source for the action to occur. A list of usernames can be entered, separated by a comma, or write Any to represent any authenticated user. If it's left blank there is no need for authentication for this policy.
<b>Destination Nets</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet. Leave this blank to match everything.
<b>Destination Users/Groups</b>	A specific username can be specified for this policy to match. A list of usernames can be entered, separated by a comma, or write Any for any authenticated user. If it's left blank there is no need for authentication for this policy.
<b>Service</b>	A predefined service can be selected from the dropdown menu or a custom service can be created.
<b>Schedule</b>	Select what schedule should be used for this policy to match. Choose Always for no scheduling.

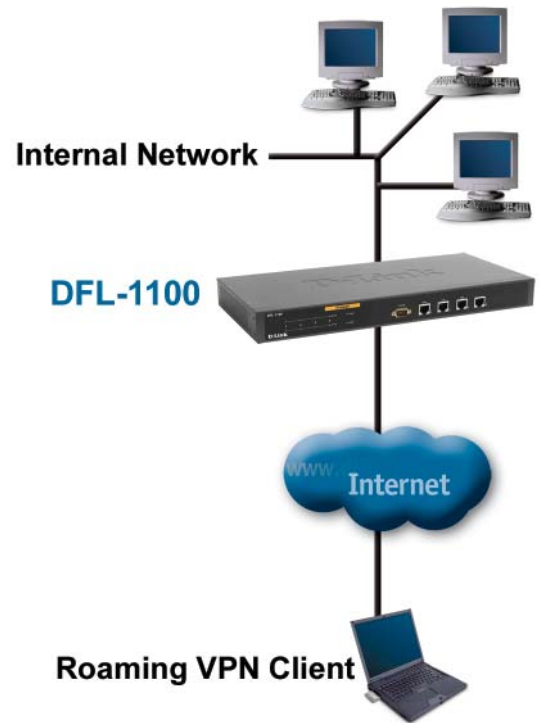
4. If using Traffic Shaping, fill in the appropriate information. If not, skip this step.
5. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.

# IPSec VPN Configuration

The VPN configuration screen can be found by going to the **Firewall** tab and selecting the **VPN** button.

## IPSec VPN Between a Client and an Internal Network

Users can connect to the main office internal network from any Internet connection. Communication between the client and the internal network takes place in an encrypted VPN tunnel that connects the DFL-1100 and the roaming users across the Internet. The client can connect to an internal network or the DMZ network.



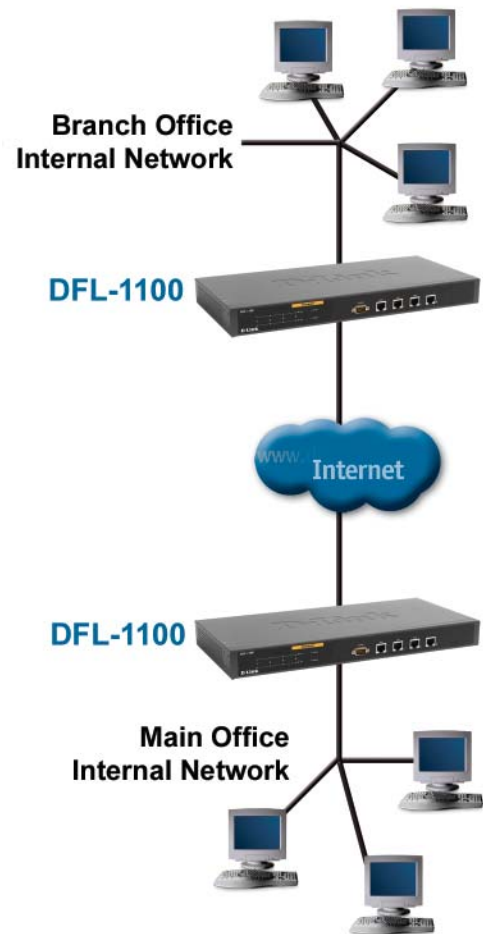
## Creating a Roaming Users VPN Tunnel

1. Click on the [Add new](#) link.
2. Enter a name for the new tunnel in the name field. The name can contain numbers (**0-9**), upper and lower case letters (**A-Z, a-z**), dash (-), or underscore (\_).
3. In the Local Net field, enter the local network that your roaming VPN clients will be connecting to.
4. Choose the authentication type, either PSK (Pre-shared Key) or Certificate-based. If you select PSK, be sure the clients use exactly the same PSK.
5. Select **Roaming Users** as the Tunnel Type.
6. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.



## IPSec VPN Between Two Networks

Users can connect from an internal network at one location to an internal network at another location via the Internet. Communication between the two networks takes place in an encrypted VPN tunnel that connects two DFL-1100 units across the Internet. Users of the internal networks are not aware that when they connect to a computer on the other network, the connection runs across the Internet. The connections can be made to the internal LAN connections or to the DMZ connections.



## Creating a LAN-to-LAN VPN Tunnel

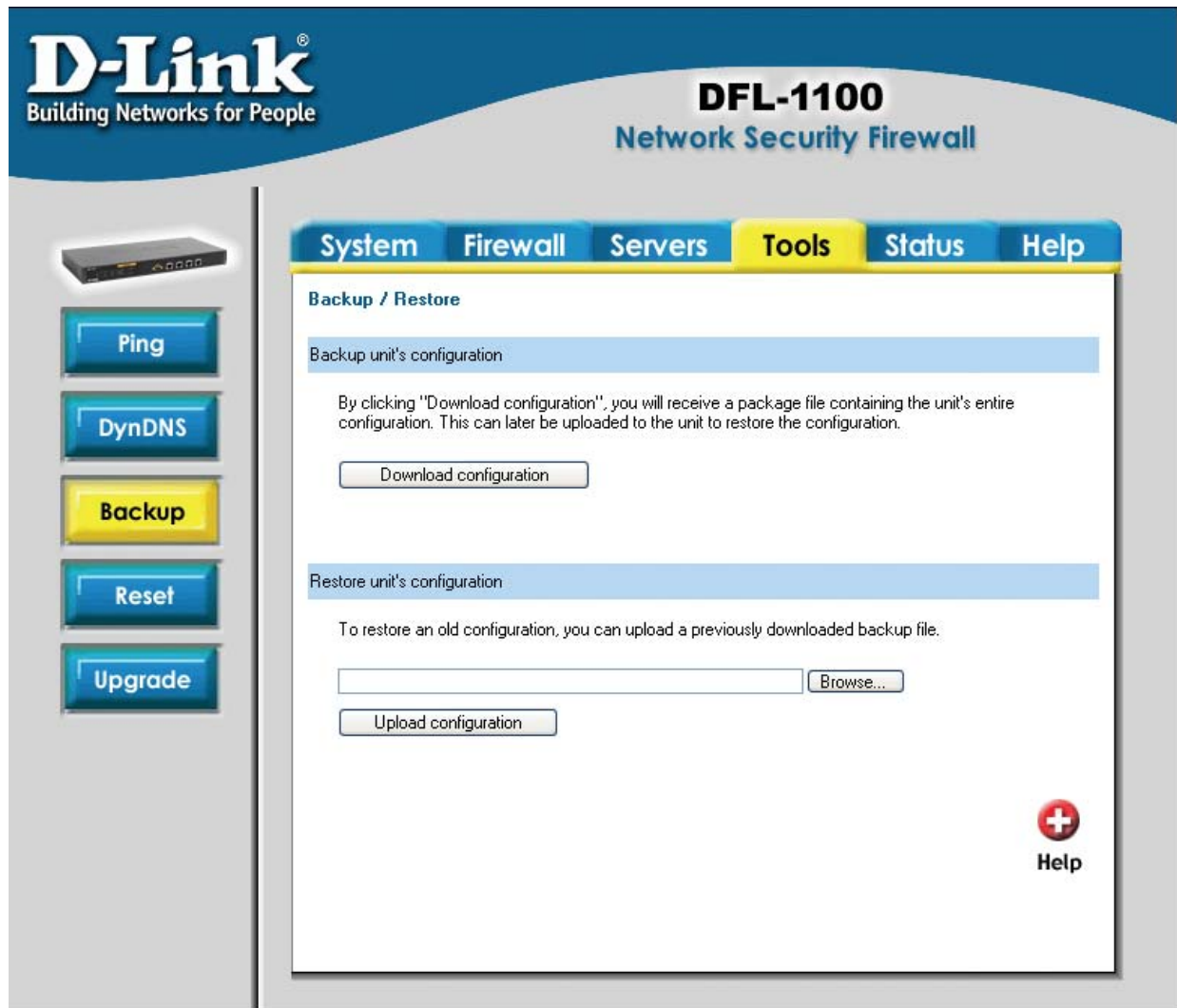
**Note:** These steps should be performed on both DFL-1100 units.

1. Click on the [Add new](#) link.
2. Enter a name for the new tunnel in the name field. The name can contain numbers (**0-9**), upper and lower case letters (**A-Z, a-z**), dash (-), or underscore (\_).
3. In the Local Net field, enter the local network that the LAN-to-LAN tunnel will be using.
4. Choose the authentication type, either PSK (Pre-shared Key) or Certificate-based. If you select PSK, be sure both DFL-1100's are configured to use exactly the same PSK.
5. Select LAN-to-LAN as the tunnel type and specify the network behind the other DFL-1100 as Remote Net. Specify the external IP of the other DFL-1100 with an IP address or DNS name.
6. Click **Apply** to apply the settings or click **Cancel** to disregard the changes.



# Backup

To reach the Backup screen, go to the **Tools** tab and select the **Backup** button. The Backup option allows the administrator the ability to backup and restore the configuration of the DFL-1100. The configuration file stores system settings, IP addresses, address tables, service tables, IPSec settings, port mappings, and policies. When your DFL-1100 is fully configured, you can save the configuration file to a local drive. The configuration can be restored from the configuration file on the local drive at any time.



## To Export the Configuration File:

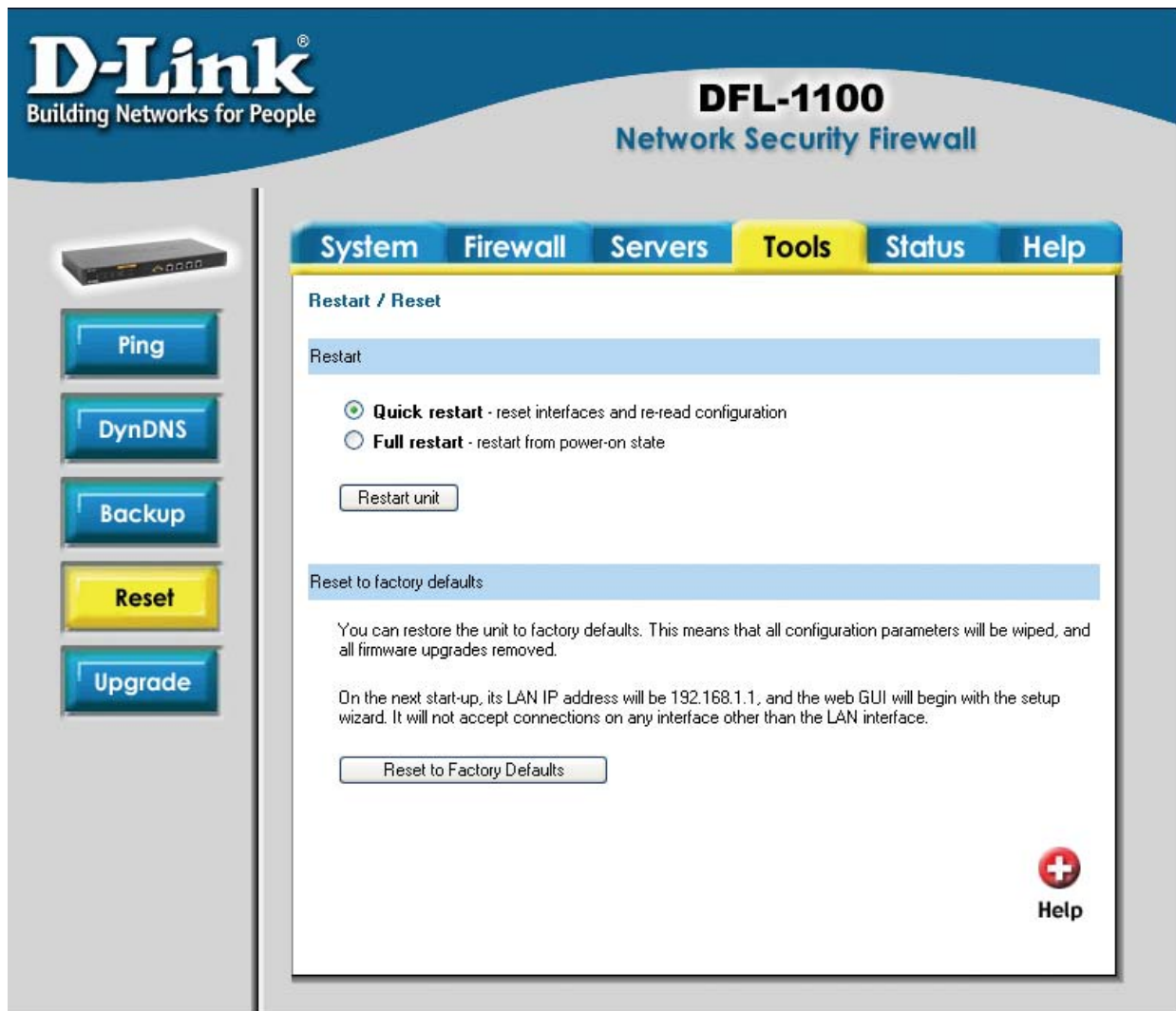
1. Click on the **Download Configuration** button.
2. Choose a destination location for saving the configuration file. The administrator may rename the file if desired.

## To Load a Previously Saved Configuration File:

1. Click on the **Browse** button and locate and select a previously saved configuration file.
2. Click the **Upload Configuration** button to import the file into the firewall.

# Restart / Reset

The Restart / Reset window can be found by going to the **Tools** tab and clicking on the **Reset** button.



## Restarting the DFL-1100

1. Select quick or full restart. A quick restart will reset the interfaces and re-read the configuration. A full restart is the same as starting up after the unit has been powered off.
2. Click on the **Restart Unit** button and the unit will restart.

## Reset System Settings to Factory Defaults

If you reset the system settings to the factory defaults, **you will lose all changes that you've made to the DFL-1100 configuration.** The system reset will also revert to the original firmware version if the unit's firmware has been upgraded. To reset the factory default settings, click the **Reset to Factory Defaults** button.

# TECHNICAL SUPPORT

You can find software updates and user documentation on the D-Link® support website.

D-Link® provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link® Technical Support through our website or by phone.

## Tech Support for customers within the United States:

### *D-Link® Technical Support over the Telephone:*

(877) 453-5465

6am-6pm PST, Mon-Fri.

### *D-Link® Technical Support over the Internet:*

<http://support.dlink.com>

email:[support@dlink.com](mailto:support@dlink.com)

## Tech Support for customers within Canada:

### *D-Link® Technical Support over the Telephone:*

(800) 361-5265

Monday to Friday 8:30am to 9:00pm EST

### *D-Link® Technical Support over the Internet:*

<http://support.dlink.ca>

email:[support@dlink.ca](mailto:support@dlink.ca)