

## 1

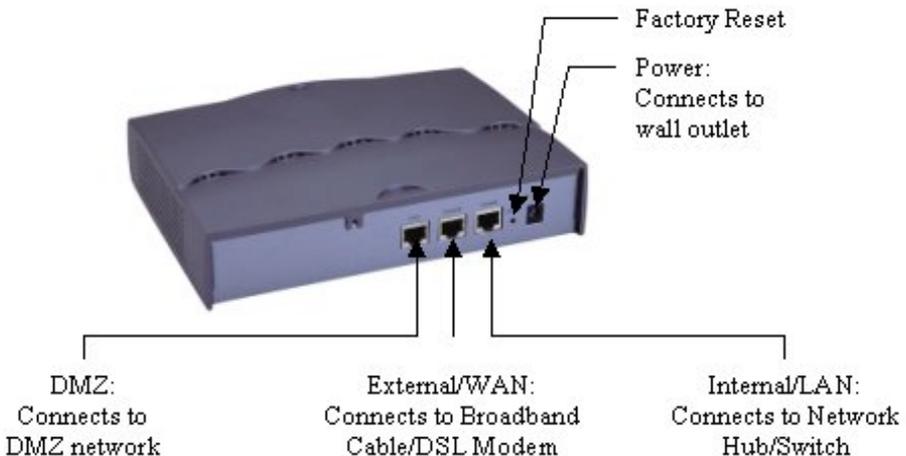
### Review Package Contents

Make sure that the package contains the following items. If any items are missing, contact the reseller.

- DFL-300 Firewall
- Manual
- Quick Install Guide
- AC Power Adapter

## 2

### Connecting the DFL-300



## 2

## Connecting the DFL-300 *continued...*

To setup the DFL-300, begin by connecting the AC adapter to a power source. The Power LED on the front of the DFL-300 should now be on.

Connect one end of the Ethernet cable to the Internal/LAN port of the DFL-300 and the other end of the cable into a hub or switch on your network. If the cable connection is good, a green LED on the front of the DFL-300 should come on for Internal Link.

Now with another Ethernet cable, connect one end to the External/WAN port of the DFL-300 and the other end to your Broadband modem. The External Link LED on the front should now also come on.

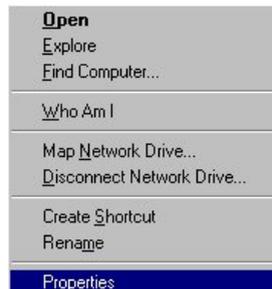
## 3

## Setting Up the Computer

By default, the DFL-300 firewall is a DHCP Server. You can set your computer to obtain an IP address. Follow the below steps to do so. If you prefer, you can set your computer up with a static IP address in the range of 192.168.1.2 ~ 192.168.1.254.

Right-Click the **Network Neighborhood** (Win 98/98SE) or **My Network Places** (Win ME/2K/XP) icon on your desktop.

Select **properties**

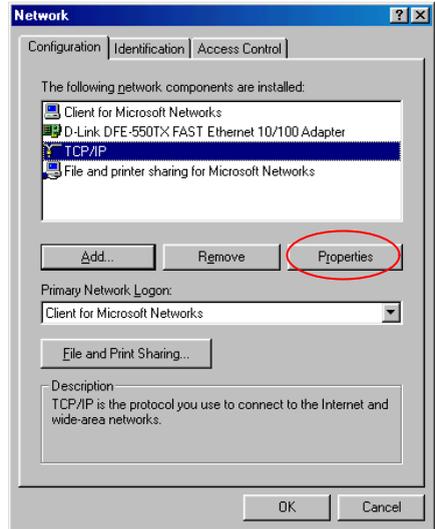


# 3

## Setting Up the Computer *continued...*

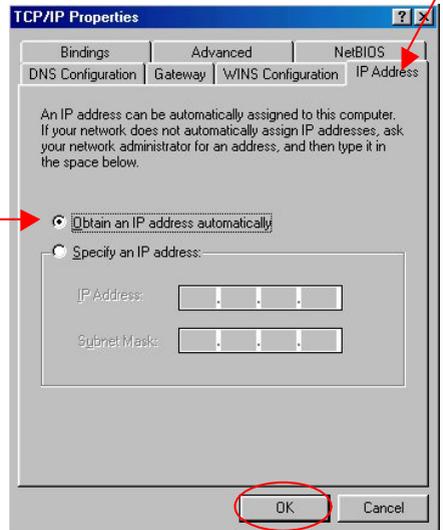
Highlight the **TCP/IP** setting for the installed Ethernet Network Adapter.

**Click Properties**



At this screen, select the IP address tab. Select Obtain an IP Address Automatically.

**Click OK**



If you are prompted to restart your computer, please do so. When the computer restarts, it will automatically receive an IP address from the DFL-300 firewall.

# 4

## Configuring the DFL-300

*Note: The DFL-300 requires Internet Explorer 4.0 or higher, or Netscape Communicator 4.0 or higher.*

Please open your Web Browser and enter this URL:

<http://192.168.1.1>

This will launch the DFL-300's integrated web-based management system.



This **Enter Network Password** pop-up screen will appear.

The default User Name is **admin** and the default Password is also **admin**. Click **OK**



Once the D-Link DFL-300 screen appears, click **Configuration** on the left side menu. Then click **Interface** below it. (See left)

You will now need to choose the External Interface option that your Broadband connection uses.

# 4

## Configuring the DFL-300 *continued...*

If your ISP requires you to enter a username/password for a PPPoE connection, choose **PPPoE (ADSL User)**

**D-Link** Office Firewall **DFL-300**

**Internal Interface**  
IP Address: 192.168.1.1  
Netmask: 255.255.255.0

**External Interface**  
 PPPoE (ADSL User)  
 Dynamic IP Address (Cable Modem User)  
 Static IP Address

Current Status: Disconnected  
IP Address: 0.0.0.0  
User Name:   
Password:   
IP Address provided by ISP:  Dynamic  
 Fixed   
 Service-On-Demand  
Auto Disconnect if idle: 0 minutes (0 : means not disconnect)  
Enable:  Ping  WebUI

**DMZ Interface**  
IP Address:   
Netmask:   
Enable:  Ping  WebUI

Fill in your PPPoE username and password provided by your ISP. Click **Ok** at the bottom when done.

# 4

## Configuring the DFL-300 *continued...*

If your ISP assigns you a dynamic IP address, choose **Dynamic IP Address (Cable Modem User)** (Cable Modem User)

**D-Link** Office Firewall **DFL-300**

**Internal Interface**

IP Address	<input type="text" value="192.168.1.1"/>
Netmask	<input type="text" value="255.255.255.0"/>

**External Interface**

PPPoE (ADSL User)

**Dynamic IP Address (Cable Modem User)**

Static IP Address

IP Address	<input type="text" value="10.50.1.46"/>
MAC Address	<input type="text" value="00:90:0b:01:11:a2"/>
Hostname	<input type="text" value="DFL-300"/>
Domain Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> WebUI

**DMZ Interface**

IP Address	<input type="text"/>
Netmask	<input type="text"/>
Enable	<input type="checkbox"/> Ping <input type="checkbox"/> WebUI

Fill in the Hostname if provided by your ISP.

Click **Ok** at the bottom when done.

# 4

## Configuring the DFL-300 *continued...*

If your ISP assigns you a static IP address, choose **Static IP Address**

**D-Link** Office Firewall **DFL-300**

**Configuration**

- Administration
- Configuration**
- Interface
- Hacker Alert
- Route Table
- DHCP
- DNS Proxy
- URL Blocking
- Address
- Service
- Schedule
- Policy
- VPN
- Virtual Server
- Log
- Alarm
- Statistics
- Status

**Internal Interface**

IP Address: 192.168.1.1  
Netmask: 255.255.255.0

**External Interface**

PPPoE (ADSL User)  
 Dynamic IP Address (Cable Modem User)  
 **Static IP Address**

IP Address:    
Netmask:    
Default Gateway:    
Domain Name Server:    
Enable:  Ping  WebUI

**DMZ Interface**

IP Address:   
Netmask:   
Enable:  Ping  WebUI

Fill in the static IP information provided by your ISP. Click **Ok** at the bottom when done.

## D-Link

**Administration**

- Configuration**
- Address
- Service
- Schedule
- Policy**
- Outgoing**
- Incoming
- External To DMZ
- Internal To DMZ
- DMZ To External
- DMZ To Internal
- VPN
- Virtual Server
- Log
- Alarm
- Statistics
- Status

Now set up the Outgoing Policy. Click on **Policy** on the left menu. Then click **Outgoing** below it.

# 4

## Configuring the DFL-300 *continued...*

Click on **New Entry** and enter the following:

**Source Address:**

Inside\_Any

**Destination Address:**

Outside\_Any

**Service:** Any

**Action:** Permit

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Click **Ok**

There should now be an Outgoing Policy created. This policy will allow all computers in the Internal network to access the Internet.

**D-Link** Office Firewall **DFL-300**

No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove To	1

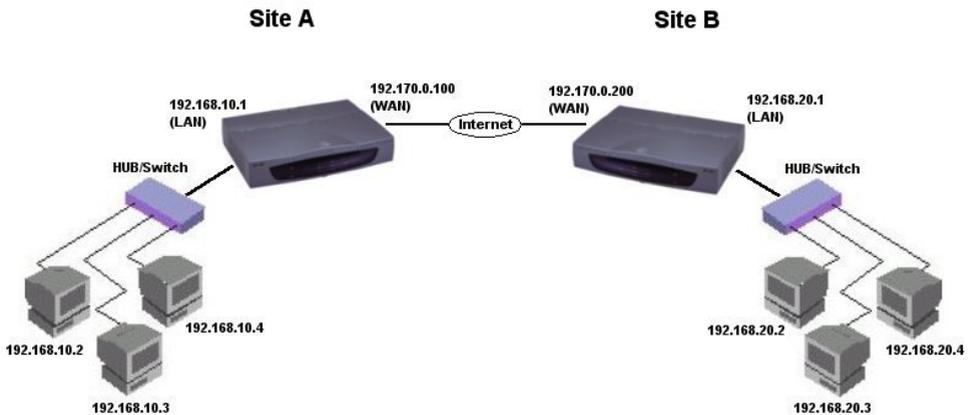
*Note:* You do not need to manually restart the DFL-300 Firewall. The changes will take place immediately once you click **Ok**. Once you are finished with the installation, you should be able to access the Internet.

# Appendix

## Creating a VPN IPsec Tunnel

This example will demonstrate how to create a Virtual Private Network (VPN) between two remote locations through the Internet. The VPN policy will use IPsec to securely send/receive encrypted data over the Internet. This example will consist of two DFL-300 Office Firewalls with a simple setup to enable VPN.

The two remote locations in this example will be call Site A and Site B. Both firewalls must already be set up and able to access each other.



*Please note the differences in the IP addresses for each site.*

We will begin by configuring the DFL-300 at Site A . Start by going into the web configuration. Once in, go to the **VPN** menu. You should now be under **VPN>Autokey IKE**.



Click **New Entry**

Please fill in the appropriate information for Site A.

**Name:** Site\_A

**From Source:** Internal

**Subnet/Mask:**

192.168.10.0/255.255.255.0

**Remote Gateway – Fixed**

**IP:** 192.170.0.200

**Subnet/Mask:**

192.168.20.0/255.255.255.0

**Authentication Method:**

Preshare

**Preshare Key:** 123456

**Encapsulation:** Encryption

(ESP)

Click **OK**

VPN Auto Keyed Tunnel	
Name	Site_A
From Source	<input checked="" type="radio"/> Internal <input type="radio"/> DMZ
Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP	192.170.0.200
Subnet / Mask	192.168.20.0 / 255.255.255.0
<input type="radio"/> Remote Gateway -- Dynamic IP	Subnet / Mask
<input type="radio"/> Remote Client -- Fixed IP or Dynamic IP	
Authentication Method	Preshare
Preshare Key	123456
Encapsulation	
<input checked="" type="radio"/> Encryption (ESP)	
<input type="radio"/> Authentication	
<input type="checkbox"/> Perfect Forward Secrecy	
IPSec Lifetime	28800 Seconds
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

*Note: 123456 is an example of a preshare key, please fill in any secret preshare key you desire. Keep in mind that both sites require the same preshare key.*

There should now be a VPN Policy created for Site A.

Name	Gateway IP	Destination Subnet	PSK/RSA	Status	Configure
Site_A	192.170.0.200	192.168.20.0	psk	Disconnect	<a href="#">Modify</a> <a href="#">Connect</a> <a href="#">Disconnect</a> <a href="#">Remove</a>

New Entry

Site A is now complete, we will now configure Site B with the other DFL-300. Follow the same steps previously with Site A to create a VPN policy. Please change the appropriate IP information.

**Name:** Site\_B

**From Source:** Internal

**Subnet/Mask:**

192.168.20.0/255.255.255.0

**Remote Gateway – Fixed IP:**

192.170.0.100

**Subnet/Mask:**

192.168.10.0/255.255.255.0

**Authentication Method:**

Preshare

**Preshare Key:** 123456

**Encapsulation:** Encryption (ESP)

Click **OK**

VPN Auto Keyed Tunnel

Name: Site\_B

From Source:  Internal  DMZ

Subnet / Mask: 192.168.20.0 / 255.255.255.0

To Destination

Remote Gateway -- Fixed IP: 192.170.0.100

Subnet / Mask: 192.168.10.0 / 255.255.255.0

Remote Gateway -- Dynamic IP

Subnet / Mask: / 255.255.255.0

Remote Client -- Fixed IP or Dynamic IP

Authentication Method: Preshare

Preshare Key: 123456

Encapsulation

Encryption (ESP)

Authentication

Perfect Forward Secrecy

IPSec Lifetime: 28800 Seconds

OK Cancel

There should now be a VPN policy created for Site B.

Name	Gateway IP	Destination Subnet	PSK/RSA	Status	Configure
Site_B	192.170.0.100	192.168.10.0	psk	Disconnect	<a href="#">Modify</a> <a href="#">Connect</a> <a href="#">Disconnect</a> <a href="#">Remove</a>

New Entry

After the VPN policies have been created for the two remote locations, click **Connect** at both Sites to enable the VPN policy. The two remote locations will authenticate and the VPN status should now say **Connected**. Congratulations, you have created a simple IPSec VPN tunnel. Site A and Site B should now be able to communicate with each other securely over the Internet. All IP traffic from the two Sites are now encrypted strongly with 168-bit 3DES encryption.

## **Technical Support**

D-Link provides free technical support for customers within the United States during the warranty period. U.S. customers can contact D-Link Technical Support through our web site, by e-mail or by phone.

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

(949) 790-5290

6 a.m. to 6 p.m. Monday thru Friday

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

[www.dlink.com](http://www.dlink.com)

*If you are a customer residing outside of the United States, please refer to the list of D-Link locations that is included in the User's Manual.*

**D-Link<sup>®</sup>**  
Building Networks for People