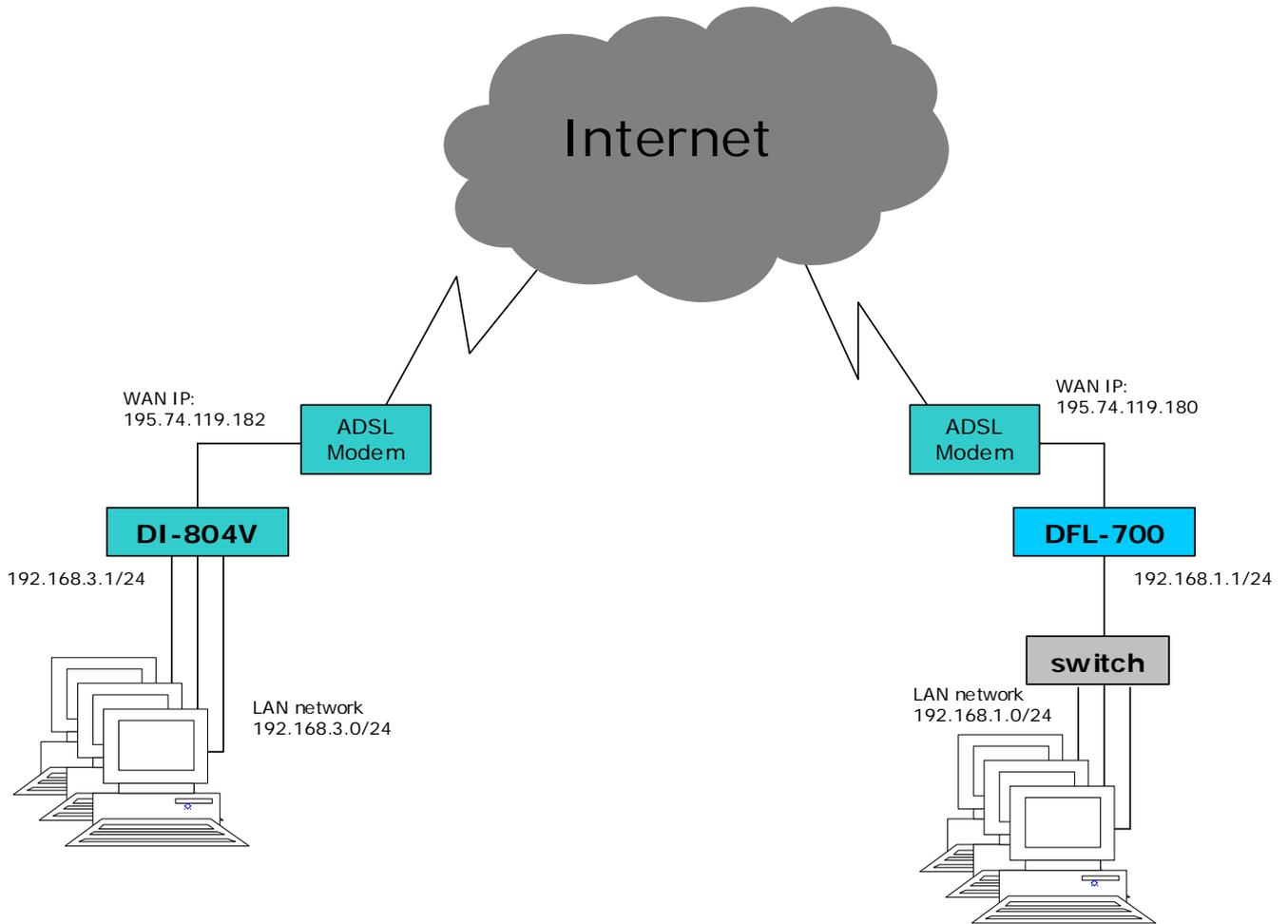


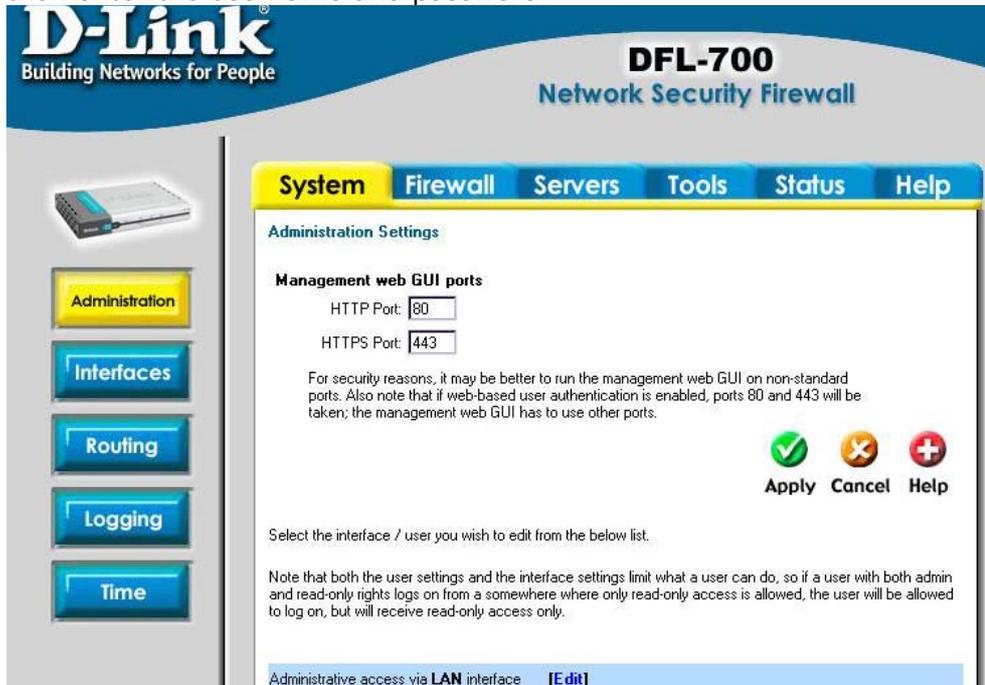
DFL-700 with DI-804V IPsec VPN Configuration Guide

This configuration shows how to connect a DFL-700 to a DI-804V with an IPsec tunnel. Please check the D-Link AUS FTP Site at <ftp://202.129.109.68> for updates on the firmware.



DFL-700 configuration

- 1) Log into the DFL-700 using its IP address (https://192.168.1.1 in this example) and then enter the username and password.



- 2) Click on **Firewall** → **VPN**. Click on **Add New**.



- 3) Enter the details for the Tunnel.

Name: DI-804V
 Local Net: 192.168.1.0/24
 Authentication: PSK – Pre-Shared Key
 Pre-shared key: dlinktest
 LAN-to-LAN tunnel

Remote Net: 192.168.3.0/24
Remote Gateway: 195.74.119.182

VPN Tunnels

Add VPN tunnel:

Name:

Local Net:

Authentication:

PSK - Pre-Shared Key

PSK:

Retype PSK:

Certificate-based

Local Identity:

Certificates:

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

Identity List:

Tunnel type:

Roaming Users - single-host VPN clients

IKE XAuth: Require user authentication via IKE XAuth to open tunnel

LAN-to-LAN tunnel

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Proxy ARP: Publish remote network on all interfaces via Proxy ARP

Click on **Apply** when done.

- 4) Click on **Edit** on the newly created **DI-804V** profile

VPN Tunnels

Changes to VPN tunnel DI-804V saved

Pick a VPN tunnel to edit from the below list:

Name	Local Net	Remote Net	Remote Gateway	
DI-804V	192.168.1.0/24	192.168.3.0/24	195.74.119.182	[Edit]

[\[Add new\]](#)

- 5) Click on **Advanced**. Set IKE mode to 'Main Mode' (default), IKE DH Group '1 – modp 768-bit'. Enable PFS by checking it. Set the PFS DH Group to '1 – modp 768-bit'. Set NAT traversal to 'Disabled'. Click on **Apply** when done.

The screenshot shows the D-Link DFL-700 Network Security Firewall configuration interface. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Firewall' tab is selected. On the left sidebar, the 'VPN' button is highlighted in yellow. The main content area is titled 'VPN Tunnels' and contains the following settings:

- Limit MTU: 1424
- IKE Mode: Main mode IKE, Aggressive mode IKE
- IKE DH Group: 1 - modp 768-bit
- PFS: Enable Perfect Forward Secrecy
- PFS DH Group: 1 - modp 768-bit
- NAT Traversal: Disabled, On if supported and needed (NAT detected between gateways), On if supported
- Keepalives: No keepalives, Automatic keepalives (works with other DFL-700/1100 units), Manually configured keepalives:
 - Source IP: []
 - Destination IP: []

Below the settings is the 'IKE Proposal List' section.

- 6) Click on '**Activate**' on the bottom left hand corner of the screen.

This screenshot shows the bottom left corner of the configuration page. It features a vertical sidebar with buttons for 'Certificates' and 'Content Filtering'. Below these is a 'Changes:' section containing three buttons: 'Activate' (highlighted in yellow), 'Discard', and 'Discard'.

- 7) Click on the '**Activate Changes**' button.

This screenshot shows the 'Activate Changes' page. The top navigation bar includes 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'System' tab is selected. The main content area is titled 'Activate Changes' and contains the following text:

Press "Activate Changes" below to save your changes and have them take effect.

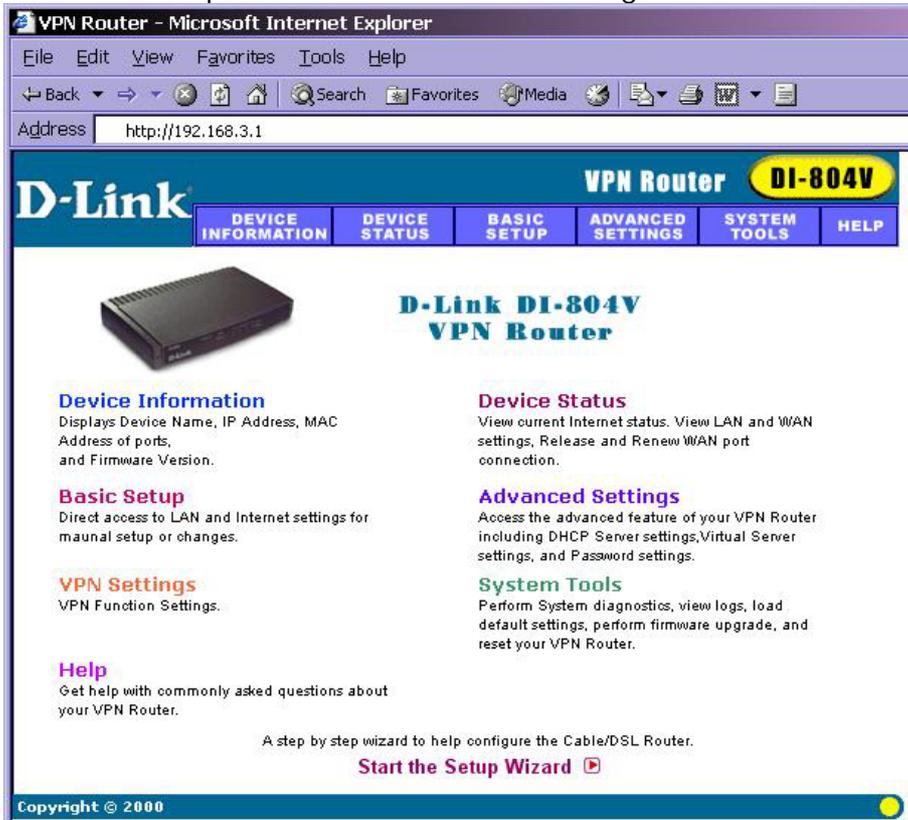
If an administrator does not log in within a set time, the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Wait for admin login for: 1 minute before reverting.

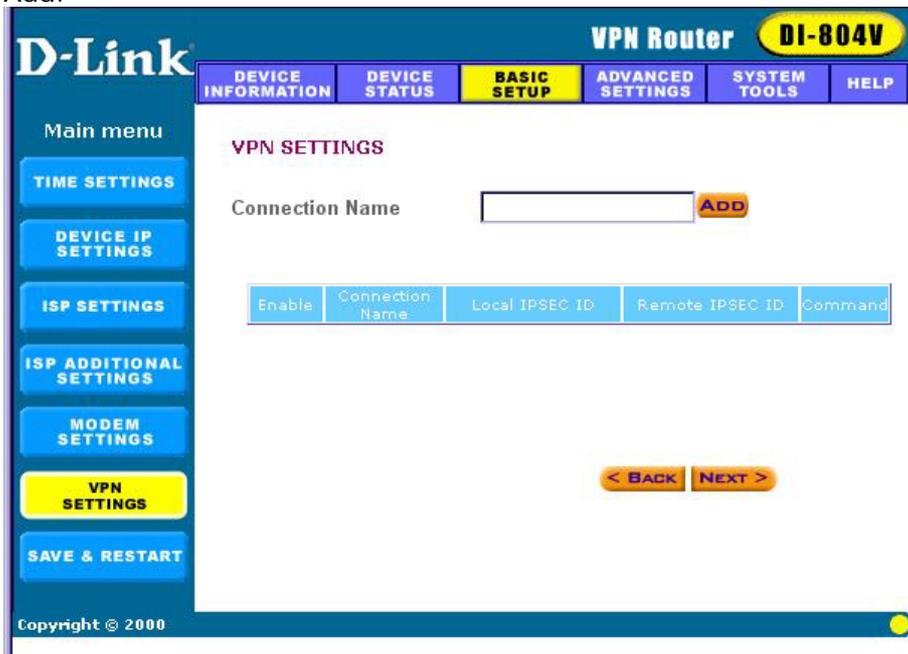
At the bottom, there is a button labeled 'Activate Changes'.

DI-804V configuration

- 1) Log on to the DI-804V using its IP address (<http://192.168.3.1>) and enter the username and password. Click on VPN Settings.



- 2) Under Connection Name, enter the name for the VPN tunnel (i.e. DFL-700). Click on Add.



- 3) Enter the following details. Click on **Save** when done.

Remote IP Network: 192.168.1.0

Remote IP Netmask: 255.255.255.0
 Remote Gateway IP: 195.74.119.180
 Network Interface: WAN ETHERNET

Secure Association: Main Mode
 Perfect Forward Secure: Enabled
 Encryption Protocol: 3DES
 Preshared Key: dlinktest
 Key Life: 3600
 IKE Life Time: 28800

The screenshot shows the 'VPN Router DI-804V' configuration interface. The 'BASIC SETUP' tab is selected. The 'VPN SETTINGS' section is active, showing the following configuration:

- Connection Name: dfl-700
- Enable UID (Unique Identifier String): Enable UID, Disable UID
- Local IPSEC Identifier: [Empty field]
- Remote IPSEC Identifier: [Empty field]
- Remote IP Network: 192.168.1.0
- Remote IP Netmask: 255.255.255.255
- Remote Gateway IP: 195.74.119.180
- Network Interface: WAN ETHERNET
- Enabled NetBIOS Broadcast:
- Secure Association: Main Mode, Aggressive, Manual
- Perfect Forward Secure: Enabled, Disabled
- Encryption Protocol: 3DES
- PreShared Key: dlinktest
- Key Life: 3600 Seconds
- IKE Life Time: 28800 Seconds

At the bottom, there is a table for managing connections:

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input type="checkbox"/>				

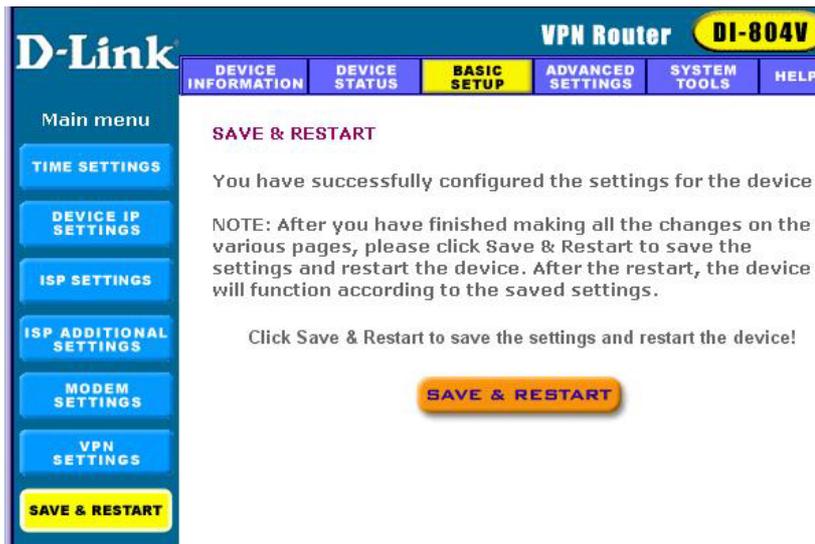
Buttons for '< BACK' and 'NEXT >' are visible. A 'SAVE' button is also present. A note at the bottom states: 'NOTE: Local IPSEC Identifier and Remote IPSEC Identifier are disabled for entering when Disable UID is checked.'

4) Click **Next**. Click **Save and Restart**.

The screenshot shows the 'VPN Router DI-804V' configuration interface after saving. The 'VPN SETTINGS' section now shows a table with one entry:

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input checked="" type="checkbox"/>	dfl-700			Edit Del

The 'ADD' button next to the 'Connection Name' field is now disabled. Buttons for '< BACK' and 'NEXT >' are visible. The 'SAVE & RESTART' button in the left sidebar is highlighted.



Testing the connection

From the DFL-700 side, you can initiate a ping to a machine on the LAN side of the DI-804V (i.e. 192.168.3.10, etc). The tunnel should then be generated and then you should get a response as shown below.

```
Command Prompt - ping 192.168.3.10 -t
Reply from 192.168.3.10: bytes=32 time=35ms TTL=128
Reply from 192.168.3.10: bytes=32 time=36ms TTL=128
Reply from 192.168.3.10: bytes=32 time=35ms TTL=128
Reply from 192.168.3.10: bytes=32 time=37ms TTL=128
Reply from 192.168.3.10: bytes=32 time=33ms TTL=128
Reply from 192.168.3.10: bytes=32 time=37ms TTL=128
Reply from 192.168.3.10: bytes=32 time=36ms TTL=128
Reply from 192.168.3.10: bytes=32 time=36ms TTL=128
```