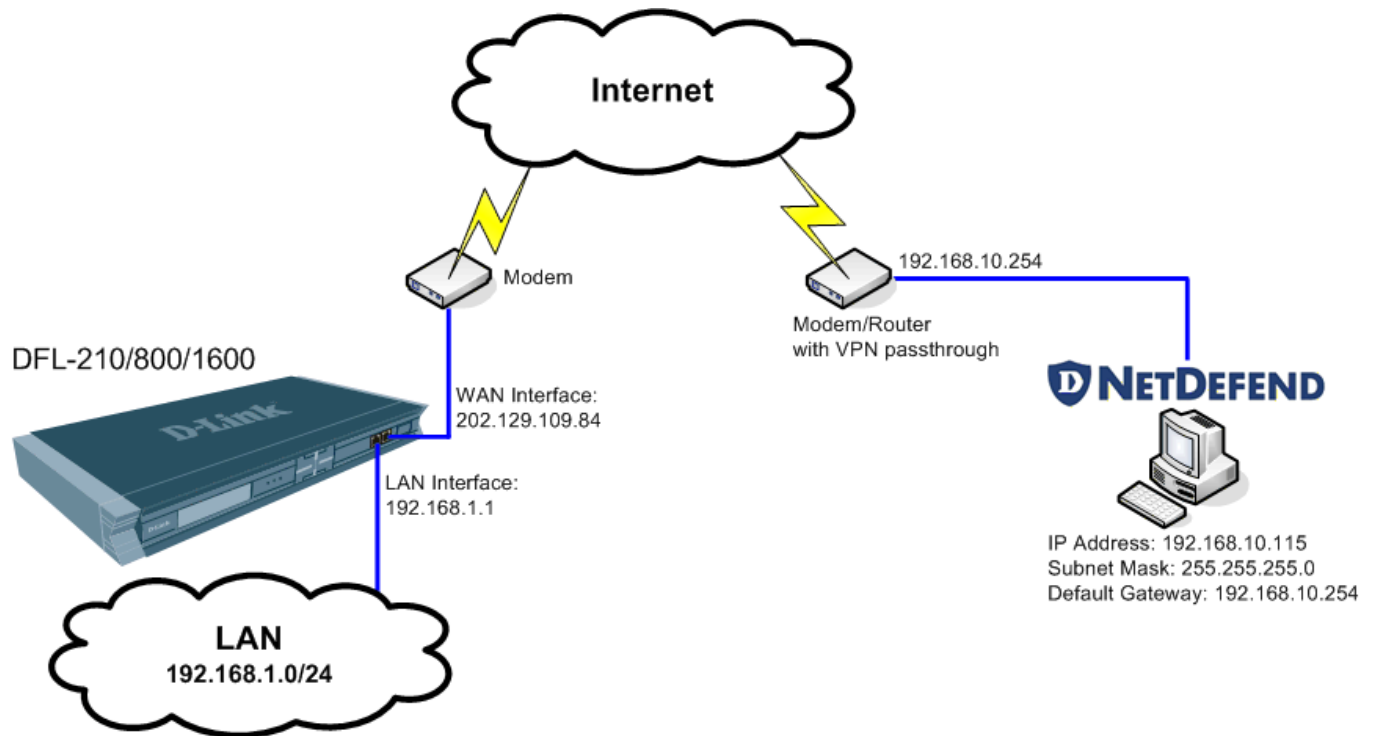


## DFL-210, DFL-600, DFL-1600

### How To Setup IPsec VPN Between D-Link Net Defend Client And The Firewall.

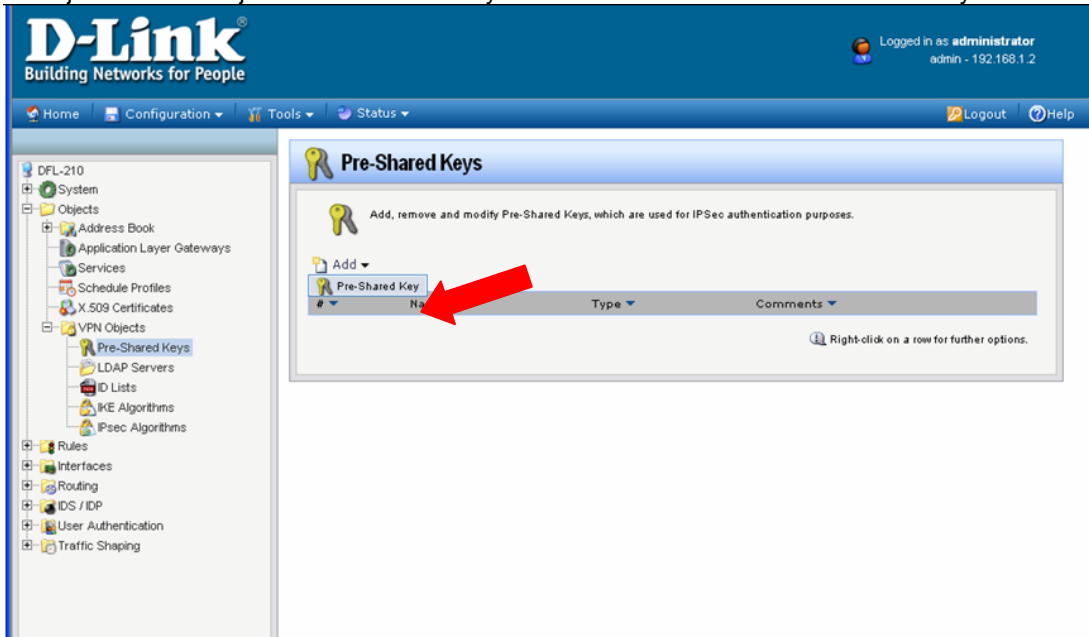
This setup example uses the following network settings:



## Firewall Setup

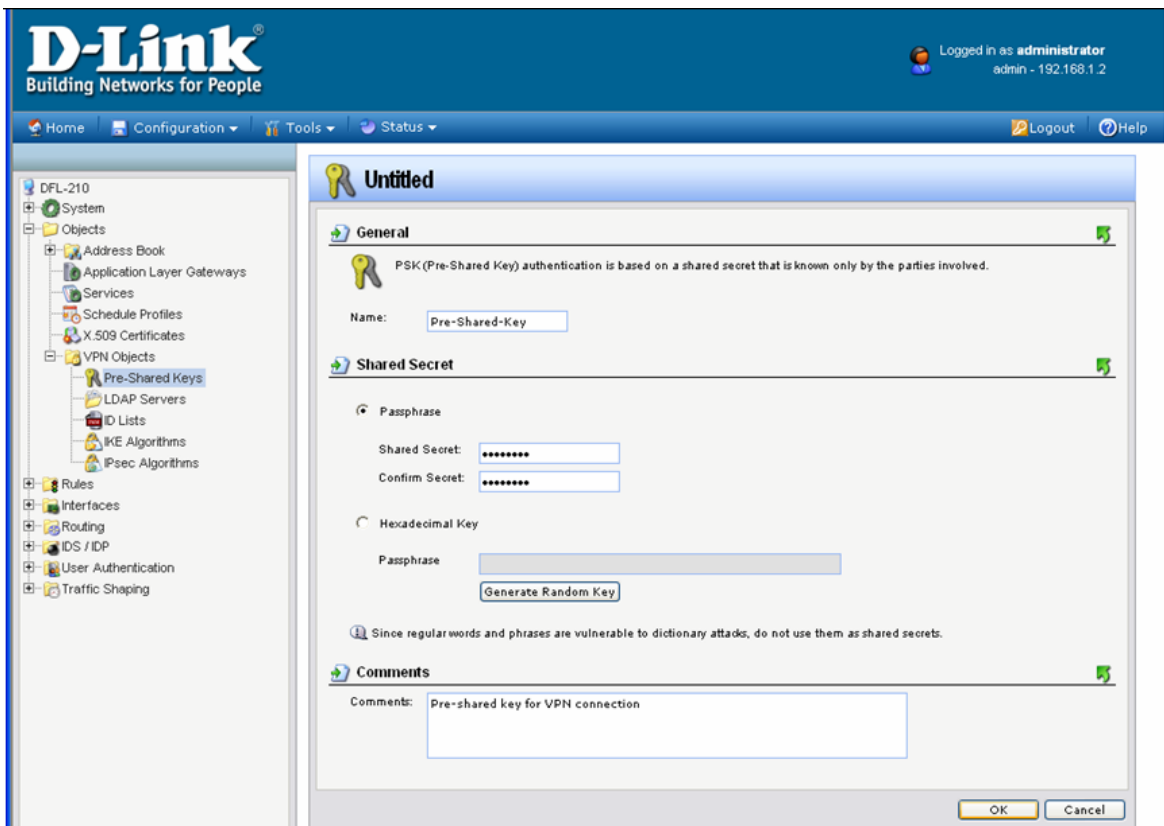
**Step 1.** Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. In our example we are using the default 192.168.1.1. Enter Username and Password which you specified during the initial setup of the Firewall.

**Step 2.** Go to Objects > VPN Objects > Pre-Shared Keys. Click on Add and select Pre-Shared Key.

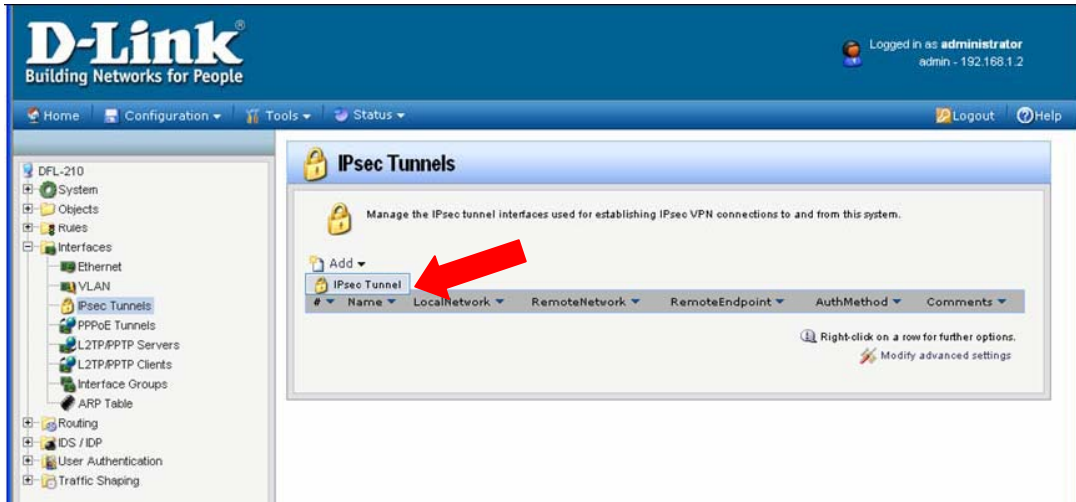


Enter the Pre-Shared Key settings for your VPN tunnel.  
Under Name type "Pre-Shared-Key".

Under Shared Secret select the type of key you want to use and type in the key. In our example we are using ASCII key (passphrase). Note that you will need to use exactly the same key when setting up the VPN Client. Click OK when done.



**Step 3.** Go to Interfaces > IPsec Tunnels. Click on Add and select IPsec Tunnel.



Enter your IPsec tunnel settings.

Under Name enter "IPSec-tunnel".

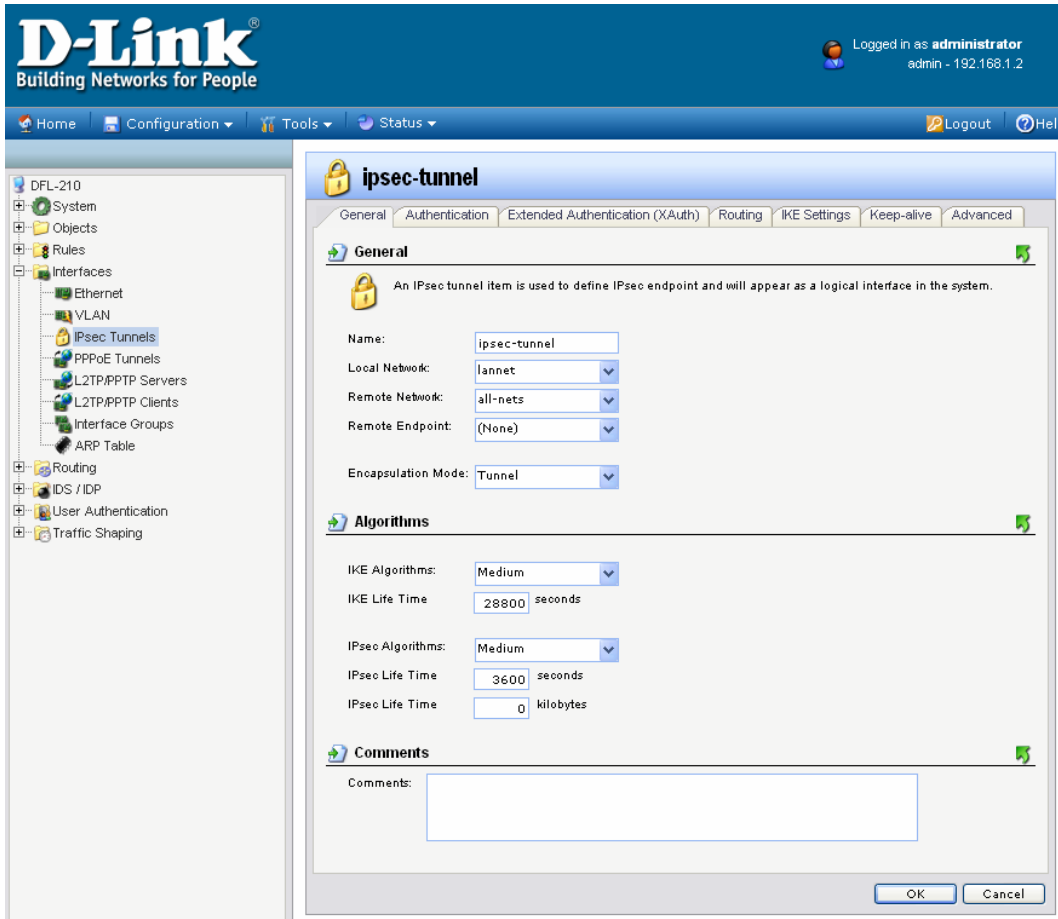
Under Local Network select "lannet" (this is the private network on this side of the VPN tunnel).

Under Remote Network select "all-nets".

Encapsulation Mode should be set to Tunnel.

Under Algorithms select the desired algorithms and IKE/IPsec lifetime. In our example we are using "Medium" settings.

You can modify or add your own set of security algorithms under Objects > VPN Objects > IKE Algorithms and IPsec Algorithms.



Click on Authentication tab. Make sure the Pre-Shared Key option is enabled. Select the “Pre-Shared-Key” in the dropdown menu (see **Step 2**).

The screenshot shows the D-Link NetDefend web interface. At the top left is the D-Link logo with the tagline "Building Networks for People". At the top right, it says "Logged in as administrator" with the IP address "admin - 192.168.1.2". Below the header is a navigation bar with "Home", "Configuration", "Tools", and "Status" menus, along with "Logout" and "Help" buttons.

The left sidebar contains a tree view of the configuration hierarchy: DFL-210, System, Objects, Rules, Interfaces (Ethernet, VLAN, IPsec Tunnels, PPPoE Tunnels, L2TP/PPTP Servers, L2TP/PPTP Clients, Interface Groups, ARP Table), Routing, IDS / IDP, User Authentication, and Traffic Shaping.

The main content area is titled "ipsec-tunnel" and has several tabs: "General", "Authentication", "Extended Authentication (XAuth)", "Routing", "IKE Settings", "Keep-alive", and "Advanced". The "Authentication" tab is active.

Under the "Authentication" tab, there are two radio button options: "X.509 Certificate" (unselected) and "Pre-Shared Key" (selected). Under "X.509 Certificate", there is a "Root Certificate(s):" section with two lists: "Available" (containing "AdminCert") and "Selected" (empty), with arrows between them. Below this are "Gateway Certificate:" and "Identification List:" dropdown menus, both set to "(None)". Under "Pre-Shared Key", there is a "Pre-Shared Key:" dropdown menu set to "IPSec-key".

At the bottom right of the configuration area are "OK" and "Cancel" buttons.

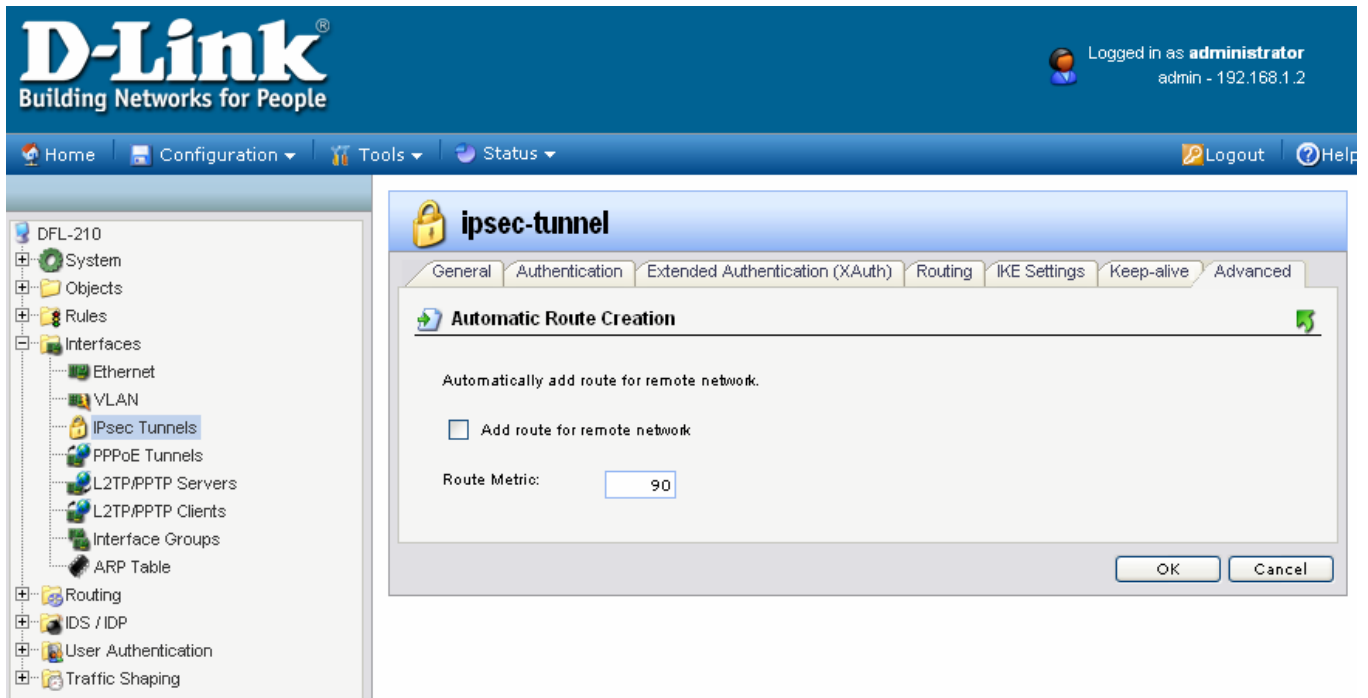
Click on Routing tab. Under Automatic Routing, tick the “Dynamically add route to the remote network when a tunnel is established” option.

The screenshot shows the D-Link NetDefend web interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', and 'Status'. The user is logged in as 'administrator' with IP '192.168.1.2'. The left sidebar shows a tree view with 'Interfaces' expanded to 'IPsec Tunnels'. The main content area is titled 'ipsec-tunnel' and has several tabs: 'General', 'Authentication', 'Extended Authentication (XAuth)', 'Routing', 'IKE Settings', 'Keep-alive', and 'Advanced'. The 'Routing' tab is selected, showing the 'Automatic Routing' section with the option 'Dynamically add route to the remote network when a tunnel is established' checked. Other sections include 'Packet Sizes' with 'Plaintext MTU' set to 1424, and 'IP Addresses' with 'Automatically pick the address of a local interface that corresponds to the local net' selected.

Go into the IKE Settings tab. Under the Perfect Forward Secrecy make sure PFS is selected.

The screenshot shows the D-Link NetDefend web interface with the 'ipsec-tunnel' configuration page. The 'IKE Settings' tab is selected, showing the 'IKE' section with 'Main' selected and 'DH Group' set to 2. The 'Perfect Forward Secrecy' section has 'PFS' selected and 'DH Group' set to 2. The 'Security Association' section has 'Per Net' selected. The 'Compatibility Flags' section has 'Do not verify padding' unchecked. The 'NAT Traversal' section has 'On if supported and NATed' selected.

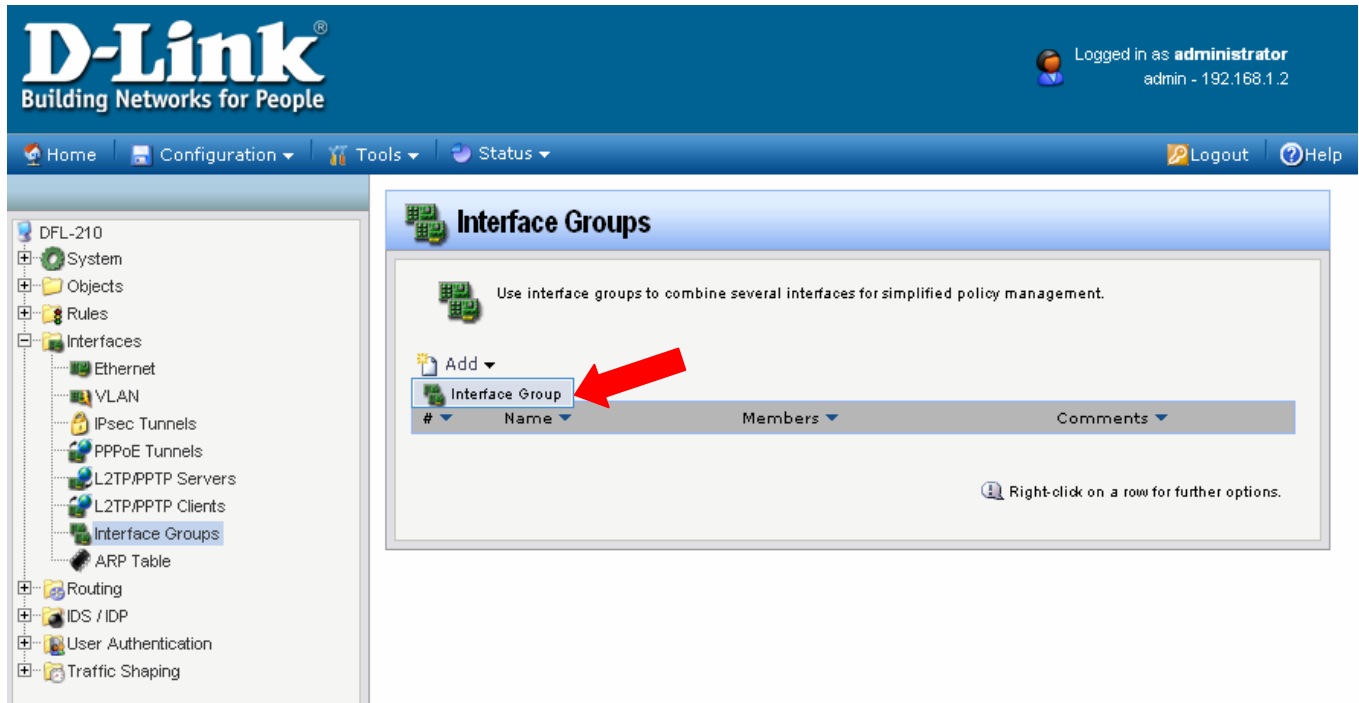
Last go into the Advanced tab and deselect the “Add route for remote network” option. Click on the OK button.



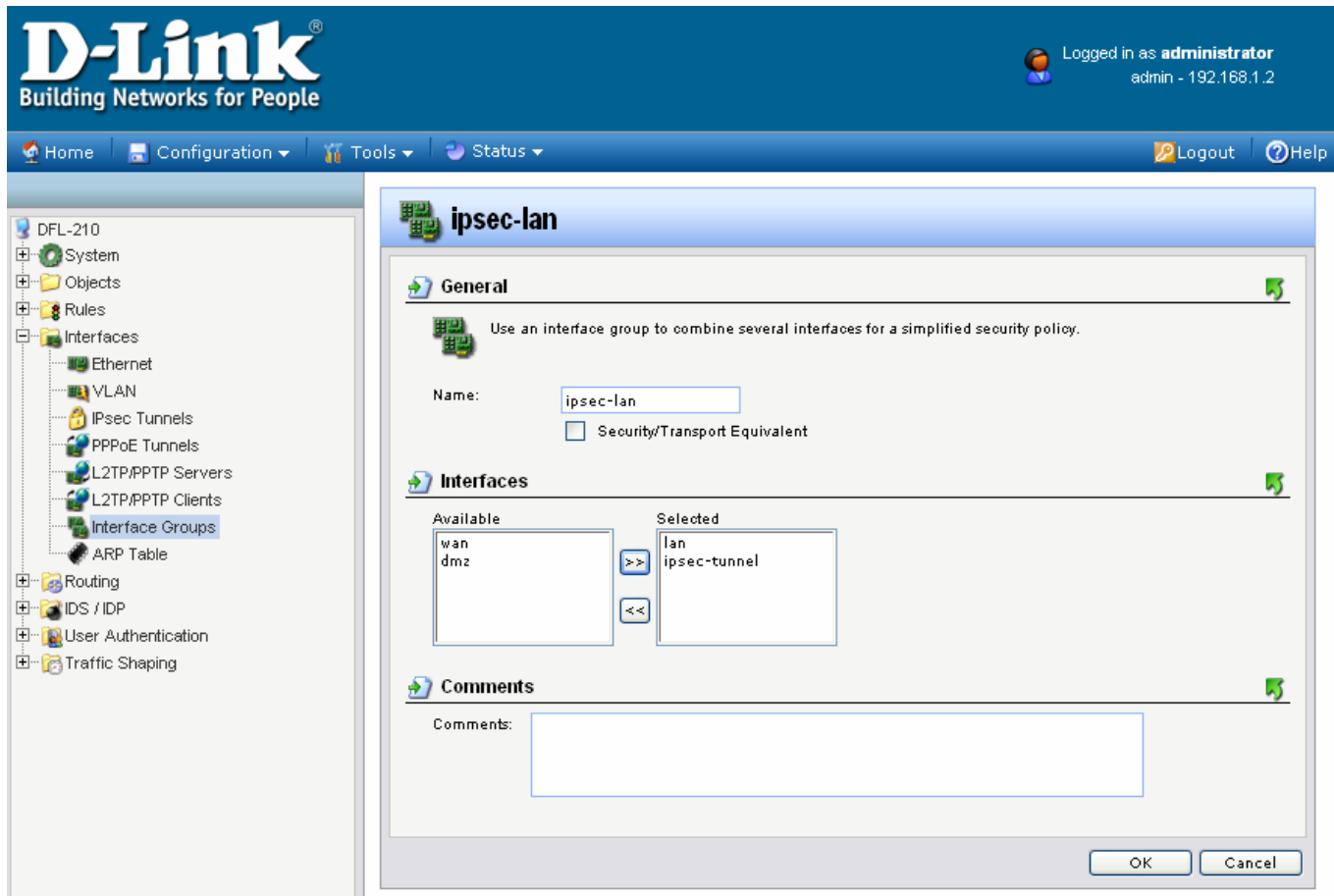
If the WAN port of the firewall is set with PPPoE authentication, change the Route Metric for the IPsec Tunnel to 80.



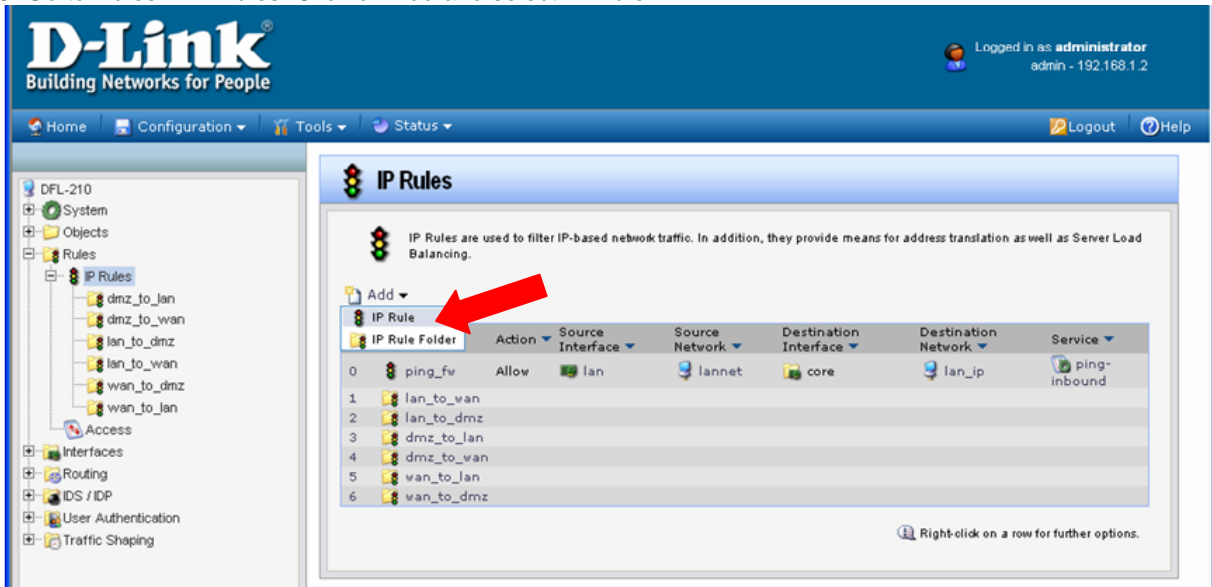
**Step 4.** Go to Interface > Interface Groups, Click on Add and then Interface Group.



Create a group which has your IPsec tunnel and your LAN.  
Under Name type IPsec-LAN.  
Under Interfaces add "IPsec-tunnel" and "lan" into the Selected field.  
Click on the OK button.



Step 5. Go to Rules > IP Rules. Click on Add and select IP Rule.



This rule will allow communication between the LAN and the IPsec tunnel.

Under Name type "IPSec-Allow".

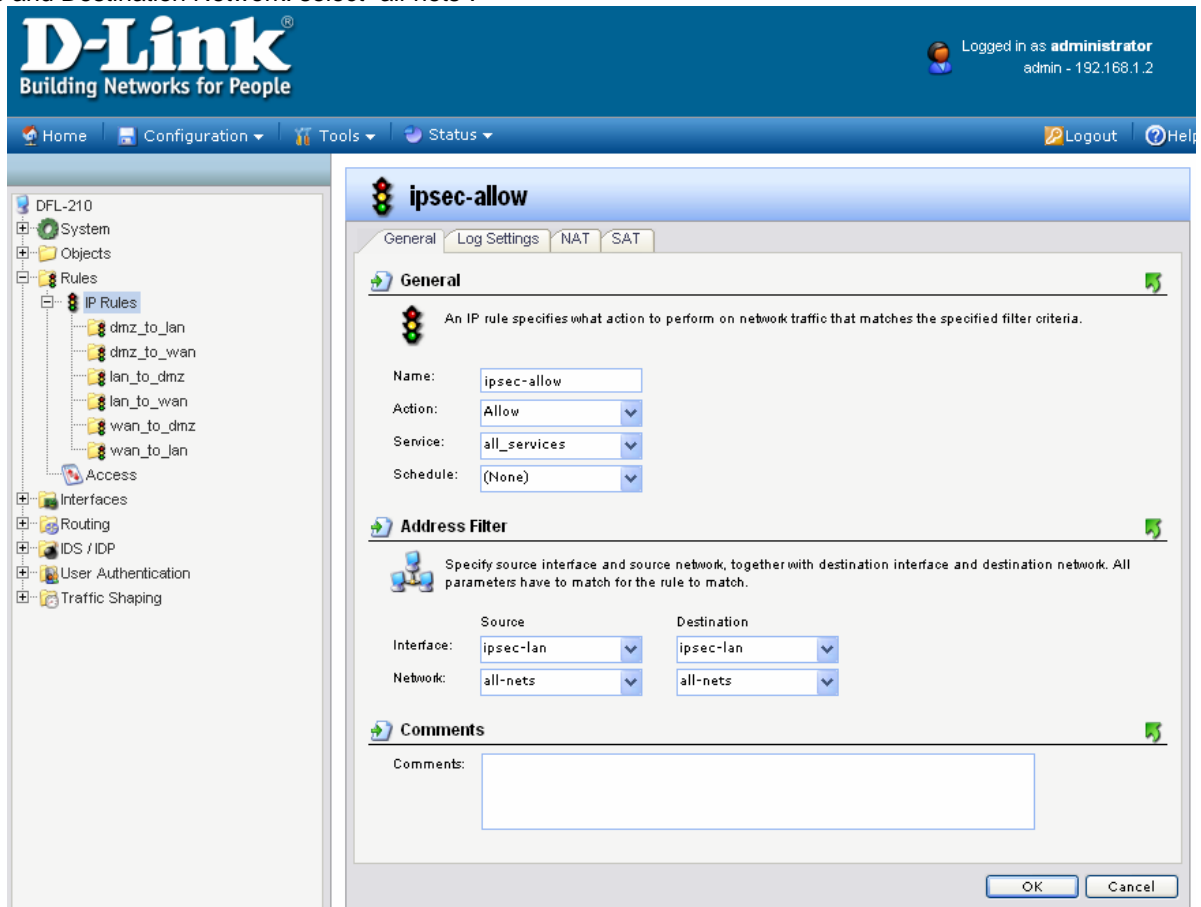
Under Action select "Allow".

Under Service select "all\_services".

Under Address Filter specify the following:

Source and Destination Interfaces: "ipsec-lan" (this is the group you created in Step 4).

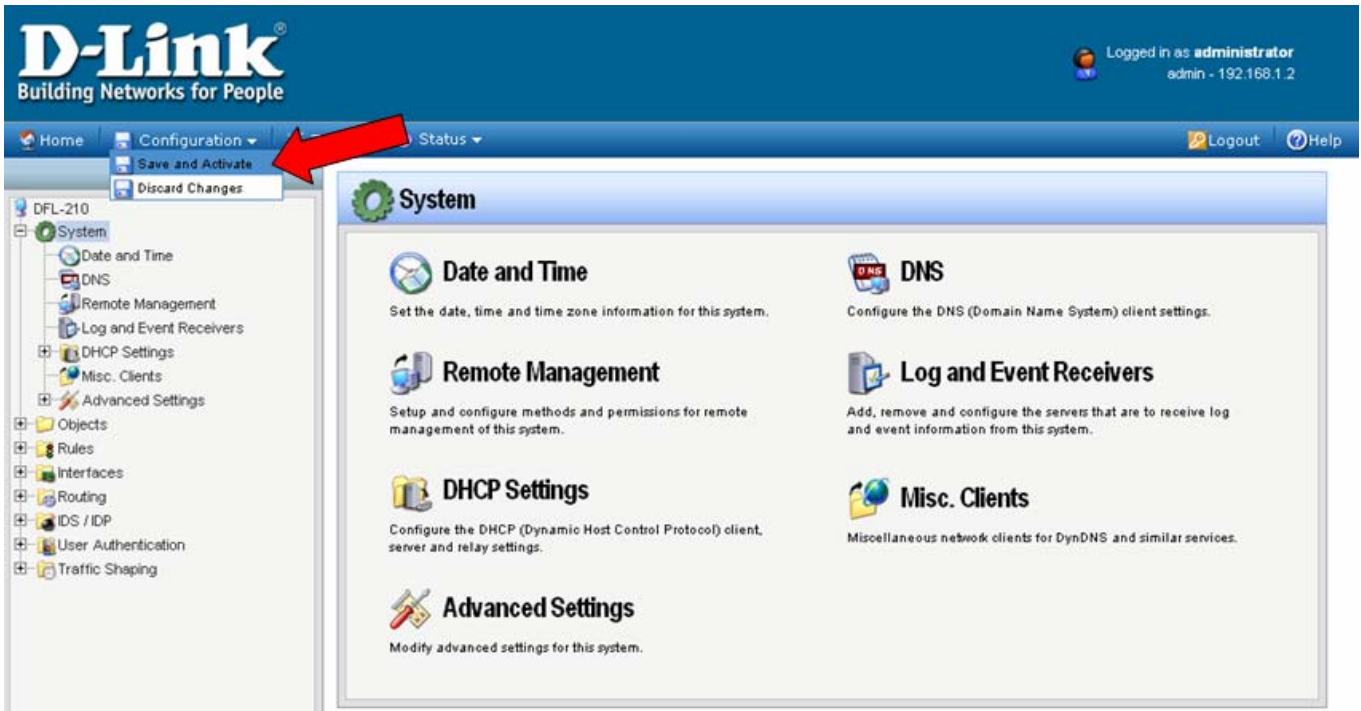
Source and Destination Network: select "all-nets".



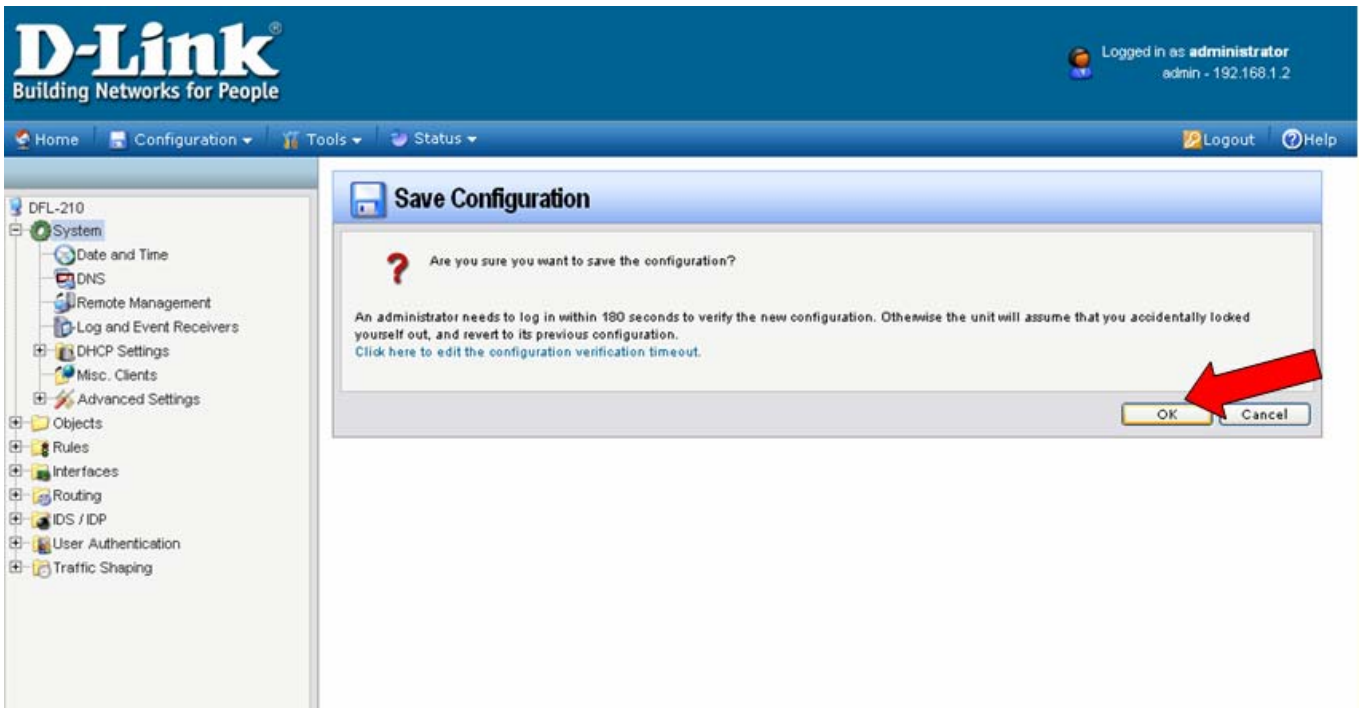
Click on the OK button when done.



**Step 6.** Save the new configuration. In the top menu bar click on Configuration and select “Save and Activate”.



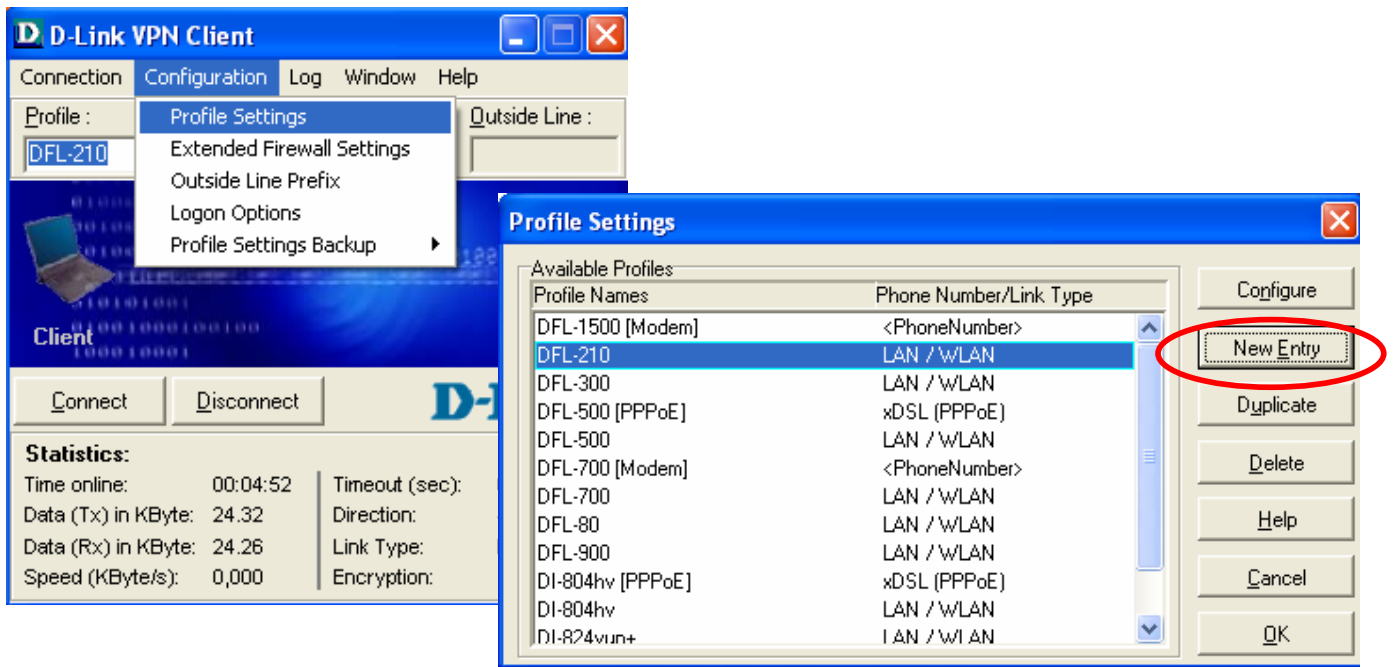
Click on OK to confirm the new settings activation:



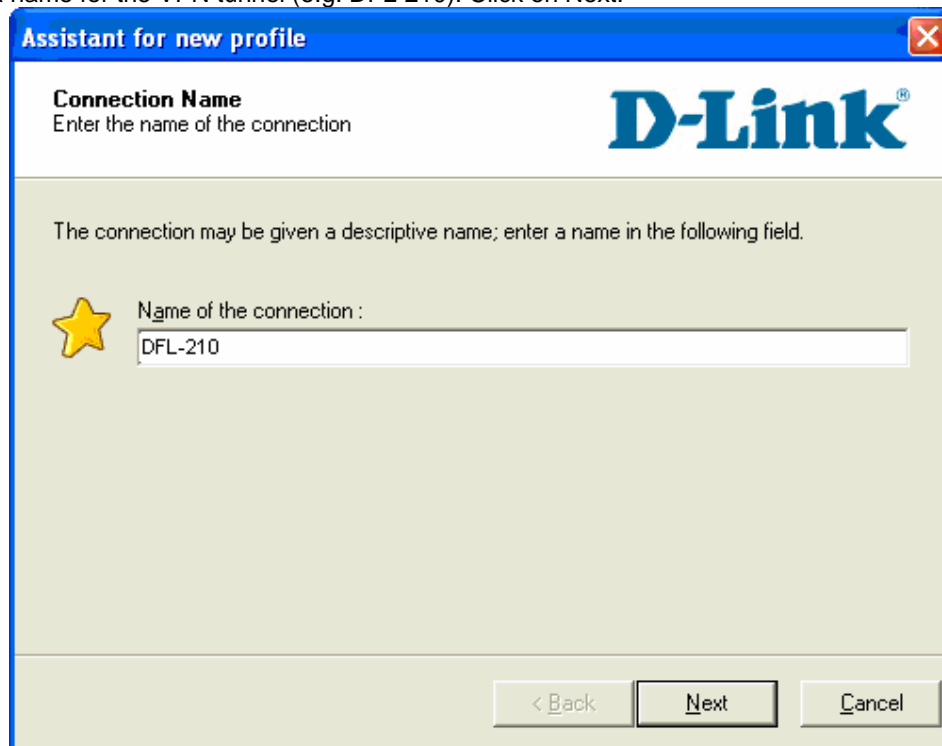
Wait 15 seconds for the Firewall to apply the new settings.

## NetDefend VPN Client Setup

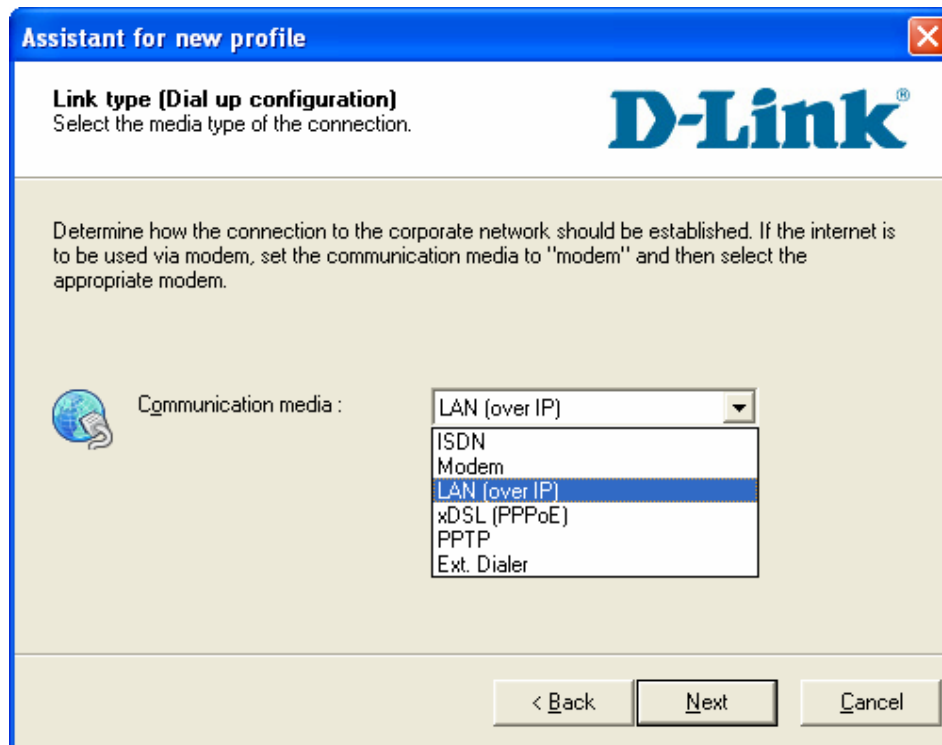
**Step 1.** Launch D-Link VPN Client (NetDefend). Select Configuration > Profile Settings. Click on “New Entry”.



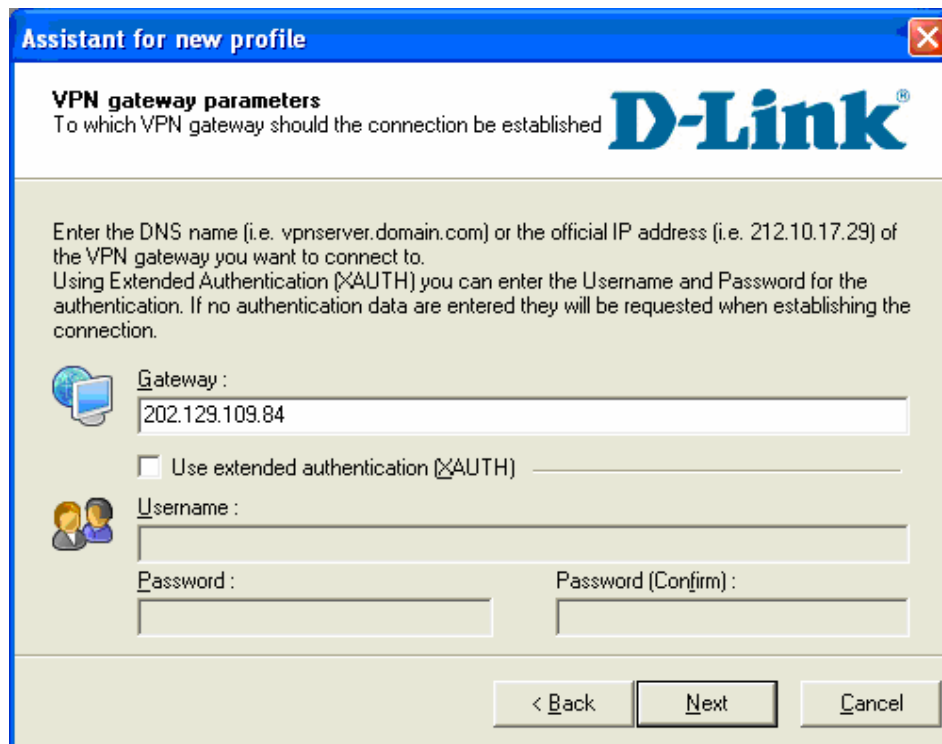
**Step 2.** Enter in a name for the VPN tunnel (e.g. DFL-210). Click on Next.



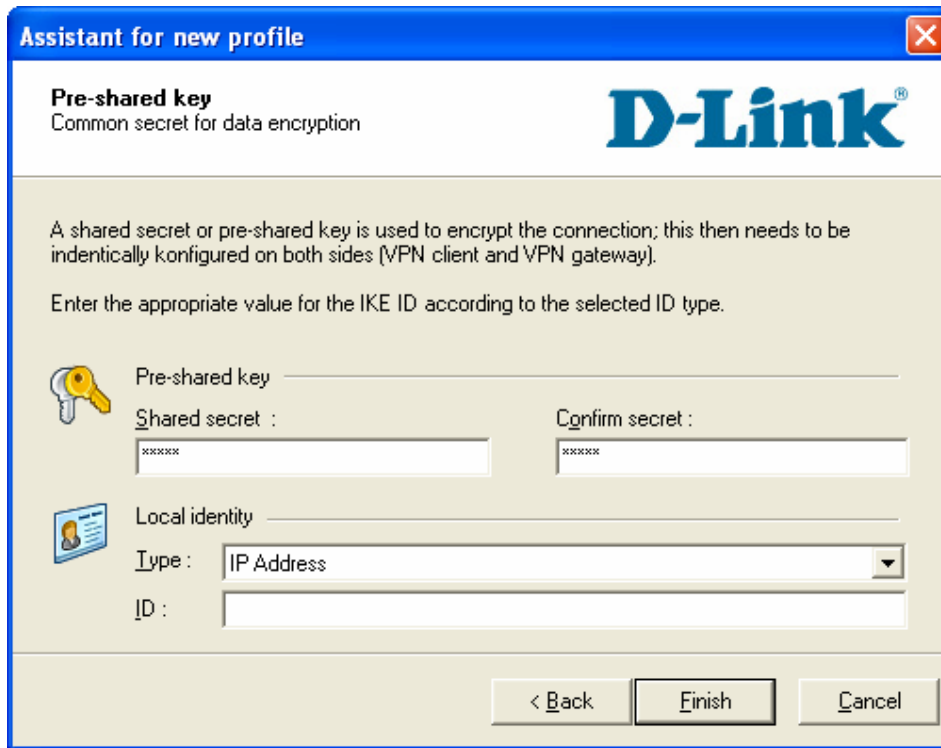
**Step 3.** Change the communication media to “LAN (over IP)”. Click on Next.



**Step 4.** In the Gateway section enter in the public IP address of the site you are going to connect to (the WAN IP of the VPN Firewall). Click on Next.



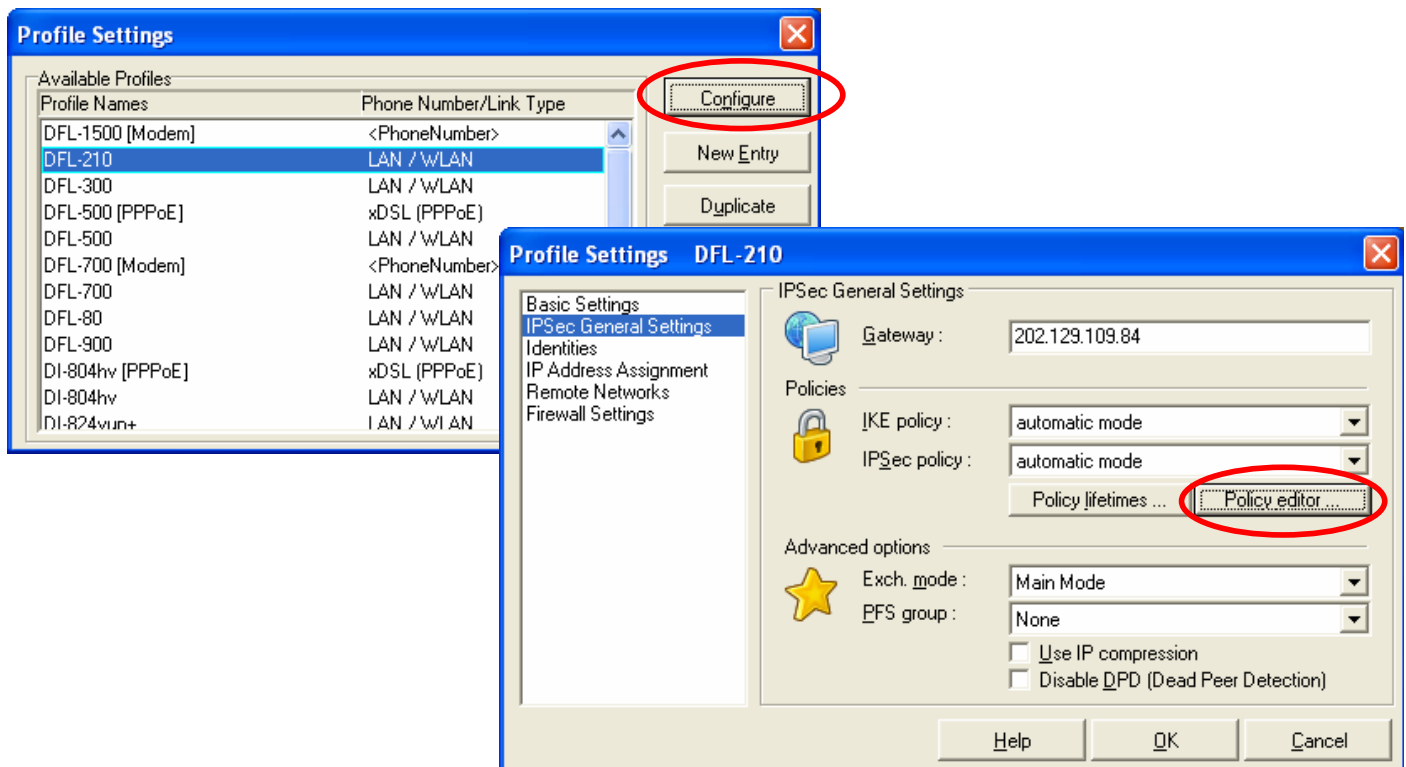
**Step 5.** Enter in the Pre-shared key (it should be exactly the same key you entered when configuring the VPN Firewall, Step 2). Click on Next.



The dialog box is titled "Assistant for new profile" and features the D-Link logo. It contains the following fields and instructions:

- Pre-shared key:** Common secret for data encryption.
- Instructions:** A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically configured on both sides (VPN client and VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type.
- Pre-shared key input:** A key icon followed by a text field.
- Shared secret:** A text field with "xxxxxx" as a placeholder.
- Confirm secret:** A text field with "xxxxxx" as a placeholder.
- Local identity:** A person icon followed by a text field.
- Type:** A dropdown menu currently set to "IP Address".
- ID:** A text field.
- Buttons:** "< Back", "Finish", and "Cancel".

**Step 6.** Once finished click on the newly created tunnel and then click on the "Configure" button. In the menu on the left select "IPSec General Setting" and then click on the "Policy editor" button.



The image shows two overlapping dialog boxes. The background one is "Profile Settings" and the foreground one is "Profile Settings DFL-210".

**Profile Settings (Background):**

Profile Names	Phone Number/Link Type
DFL-1500 [Modem]	<PhoneNumber>
DFL-210	LAN / WLAN
DFL-300	LAN / WLAN
DFL-500 [PPPoE]	xDSL [PPPoE]
DFL-500	LAN / WLAN
DFL-700 [Modem]	<PhoneNumber>
DFL-700	LAN / WLAN
DFL-80	LAN / WLAN
DFL-900	LAN / WLAN
DI-804hv [PPPoE]	xDSL [PPPoE]
DI-804hv	LAN / WLAN
DI-824vun+	LAN / WLAN

Buttons: "Configure" (circled in red), "New Entry", "Duplicate".

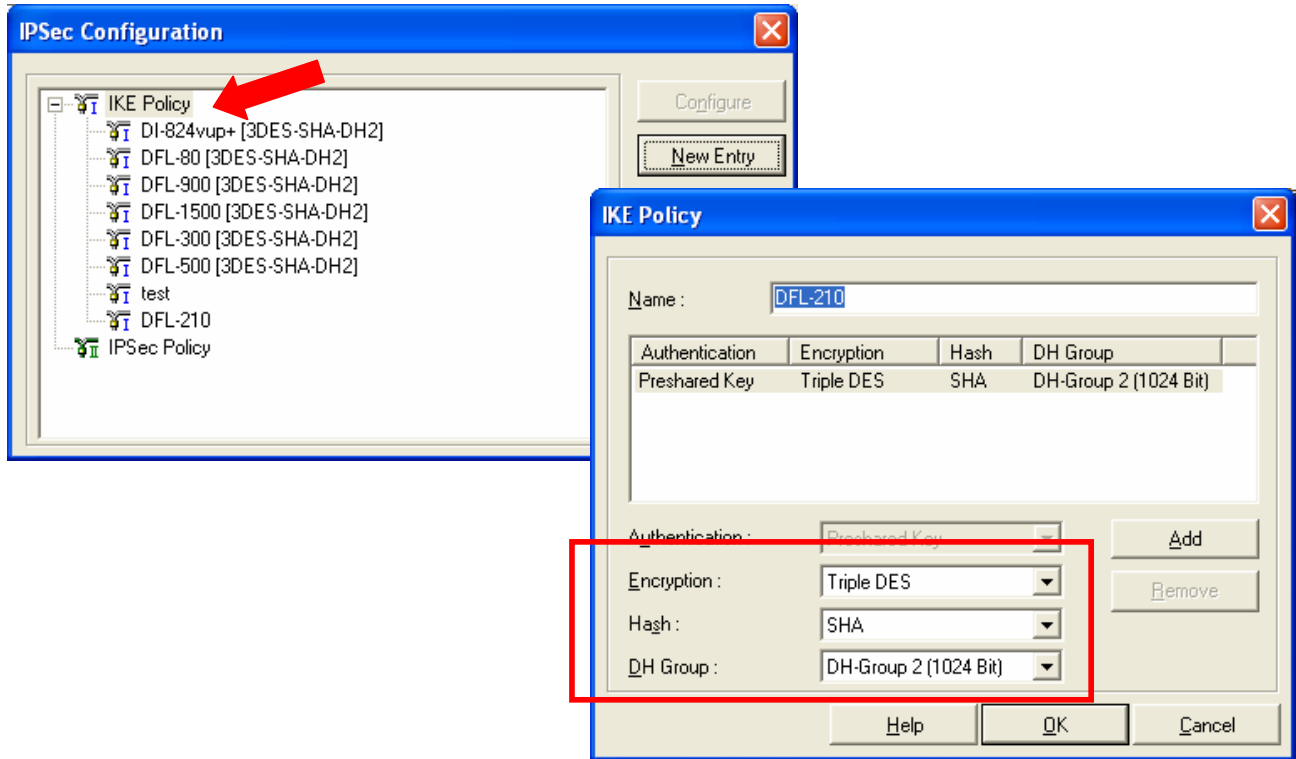
**Profile Settings DFL-210 (Foreground):**

- Basic Settings:** Selected in the left menu.
- IPSec General Settings:**
  - Gateway: 202.129.109.84
  - Policies:
    - IKE policy: automatic mode
    - IPSec policy: automatic mode
    - Policy lifetimes ...
    - Policy editor ... (circled in red)
  - Advanced options:
    - Exch. mode: Main Mode
    - PFS group: None
    - Use IP compression
    - Disable DPD (Dead Peer Detection)
- Buttons: "Help", "OK", "Cancel".

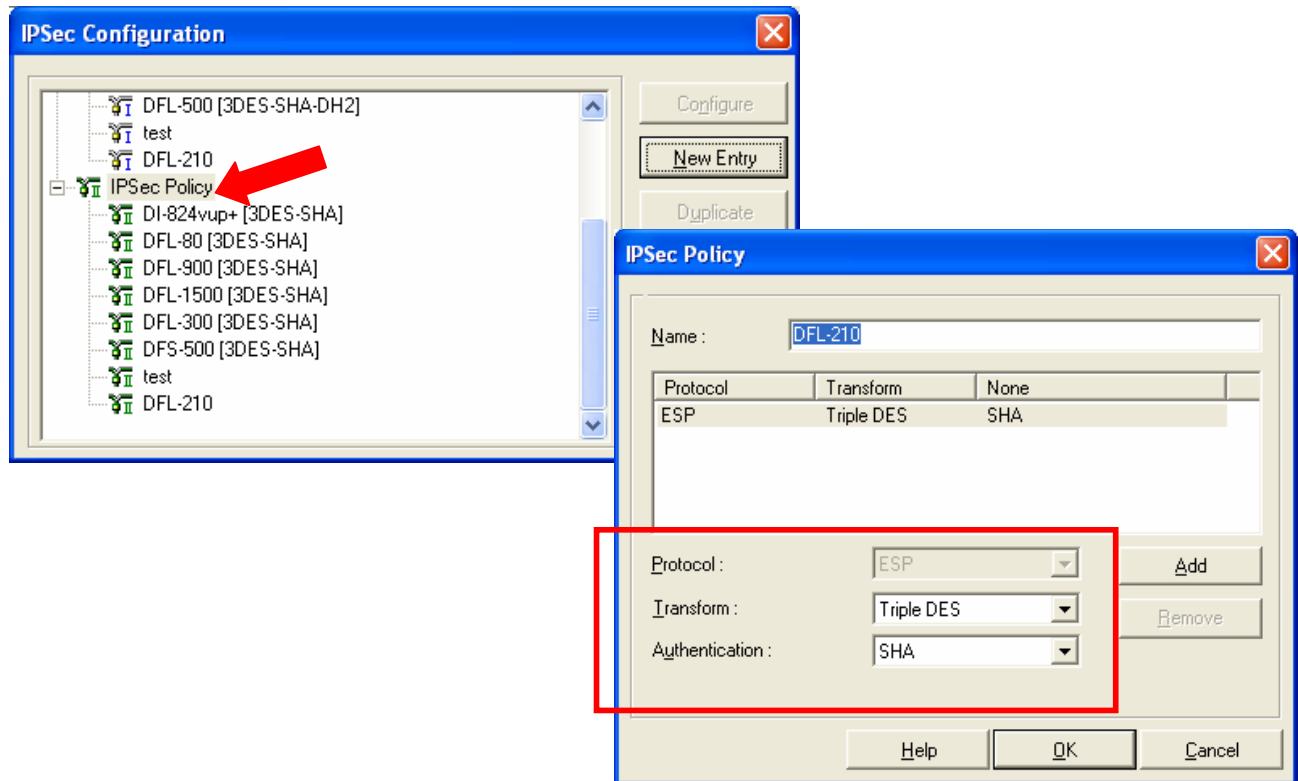
**Step 7.** Click on “IKE Policy” then click on “New Entry”.

Enter in a Name for the new policy, change the Encryption to “Triple DES”, Hash to “SHA” and DH Group to “DH-Group 2”. Click on OK when done.

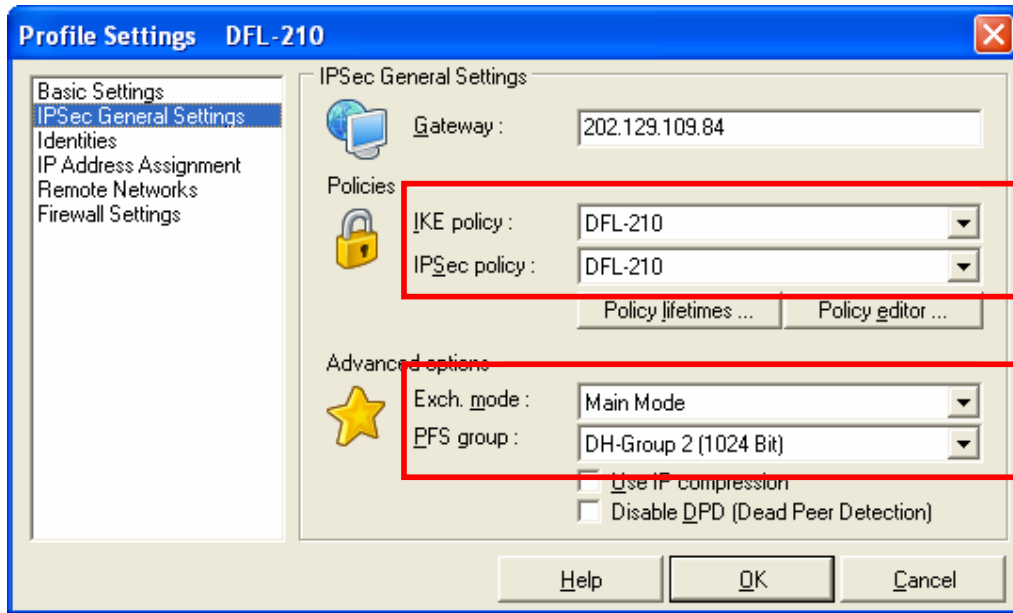
*NOTE: It would be a good idea to give your policy a name which describes its settings, e.g. “DFL-210 3DES SHA G2”. This may make it easier to see what the settings are later.*



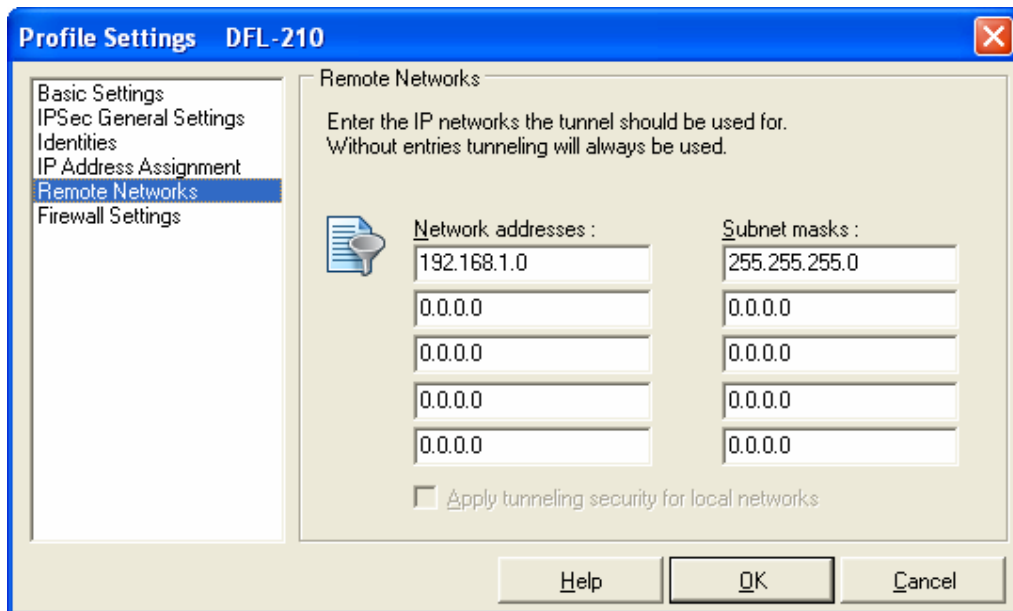
**Step 8.** Next highlight “IPSec Policy” and click on “New Entry”. Enter in a name. Set Transform as “Triple DES”, Authentication as “SHA”. Click OK.



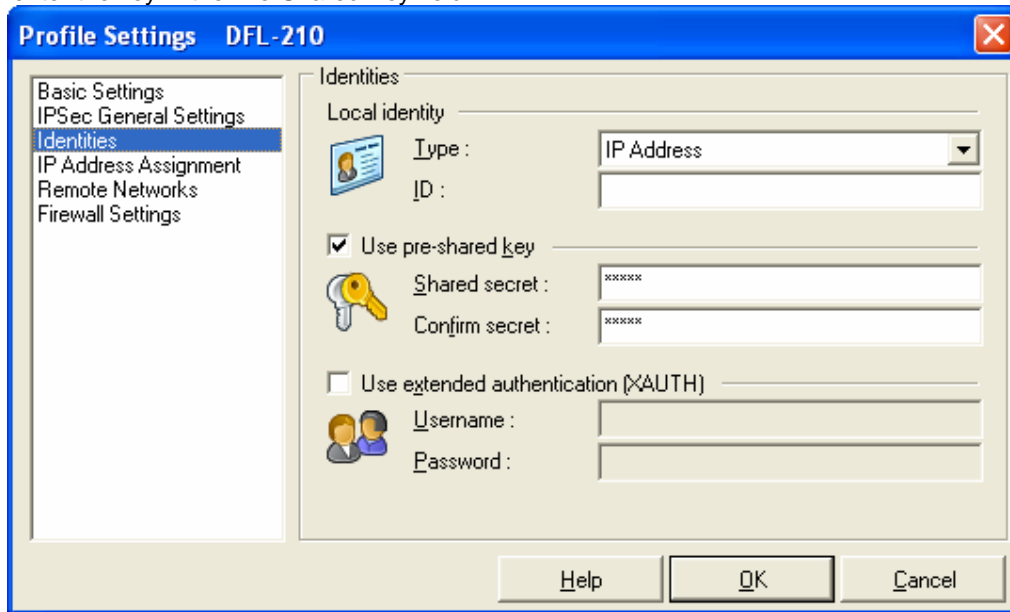
**Step 9.** Back on the Profile Settings page, under the Policies section select the policies that you've just created for both IKE policy and IPSec policy.  
Under Advanced options select "DH-Group 2" for the PFS group.



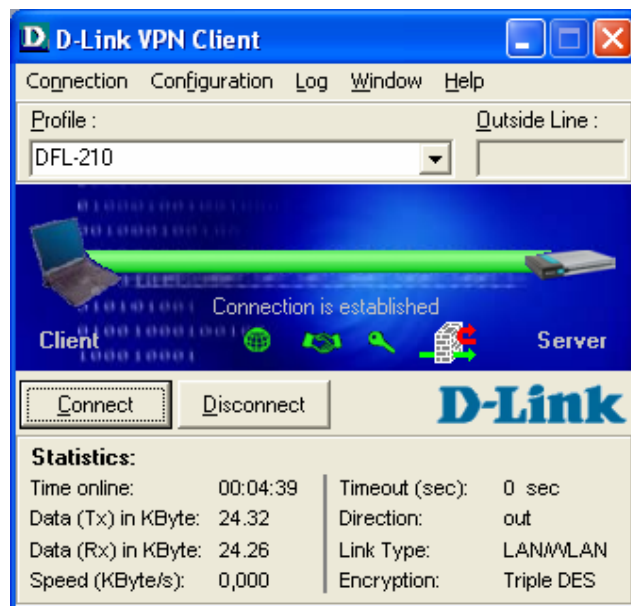
**Step 10.** In the menu on the left highlight the Remote Networks option. Under Network Addresses enter the private network which you will be connecting to (the best hint would be the LAN address of the VPN Firewall, e.g. if the LAN IP of the VPN Firewall is 192.168.1.1 enter 192.168.1.0 as Network address). Then enter the Subnet mask of the remote private network (e.g. 255.255.255.0). Click on "OK" when done.



**Step 11.** If you need to re-enter or modify the Pre-Shared Key for your VPN connection, in the menu on the left highlight “Identities” and enter the key in the Pre-Shared Key field.



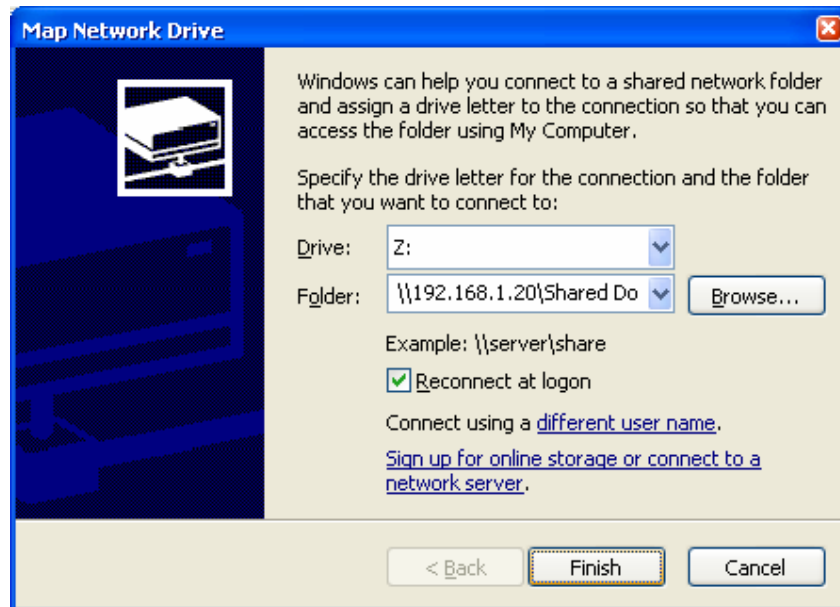
**Step 12.** To establish a VPN connection, click the “Connect” button. If connection is successful, you should see “Connection is established” message.





## Notes

In order to connect to shared resources via a VPN tunnel you can map remote computers' drives and folders by opening Windows Explorer and going to Tools > Map Network Drive (you need to specify the IP address of the computer on remote network and the name of the shared folder):



Alternatively you can do Search > Computers or People > Computer on Network > specify the IP address of the computer you are trying to connect to.

If you do not see computers in My Network Places or My Network Neighbourhood you may need to enable NetBIOS over TCP/IP in Windows.

Note that firewall/antivirus software installed on your or remote computer may stop you from accessing remote network.