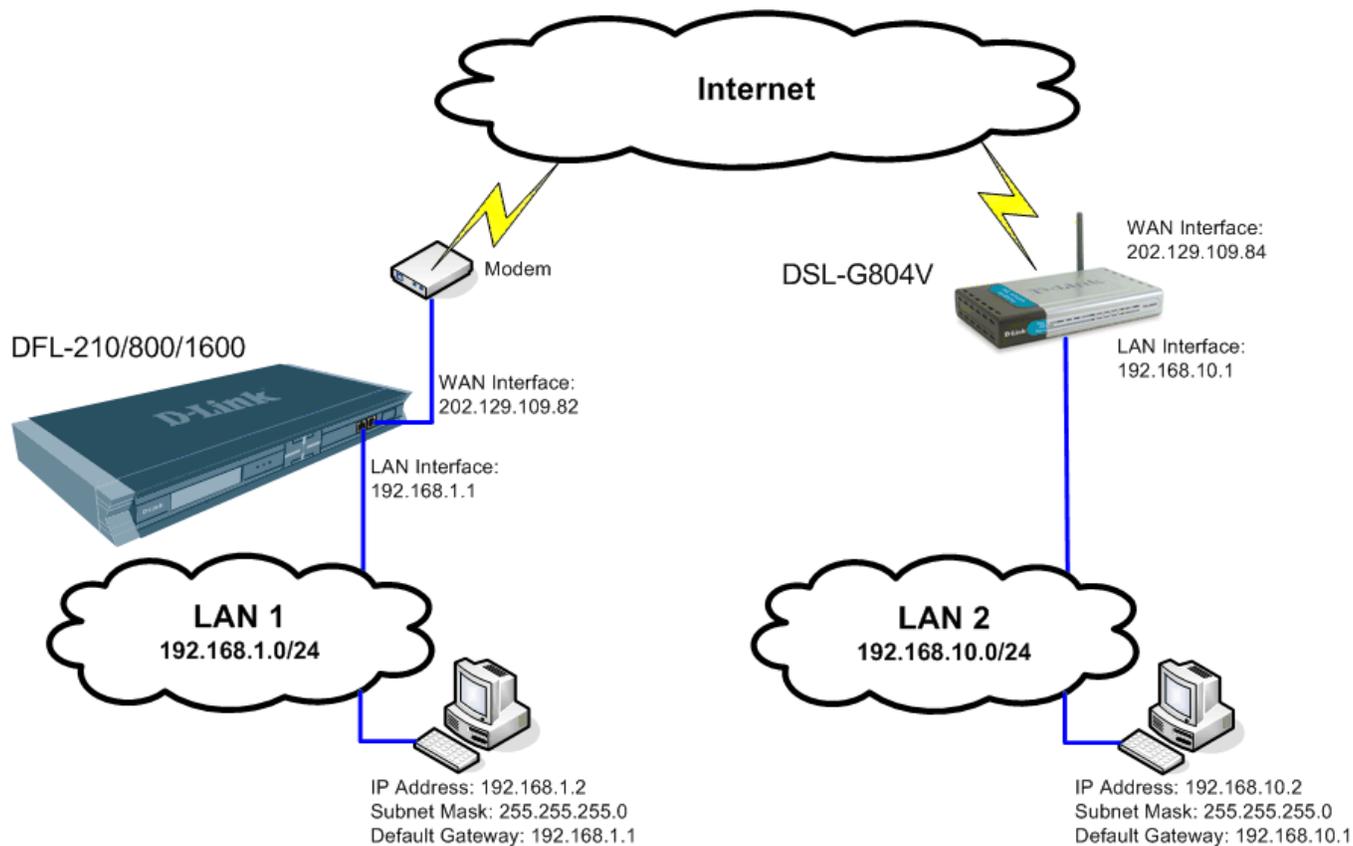


How to setup IPsec VPN connection between DSL-G804V and DFL-210/800/1600

This setup example uses the following network settings:



In our example the IPsec VPN tunnel is established between two LANs: 192.168.10.x and 192.168.1.x.

NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.

Configuration of the DSL-G804V router on LAN 2

Step 1. Log into the DSL-G804V configuration page, then go to Advanced > VPN and click on IPsec.

Step 2. Set “Enable after Apply” to “Yes”.

Connection Name - Enter a name for the tunnel.

Local Network - select “Subnet”.

IP Address - enter the IP Address of the local network. Note that it should be Subnet ID, not a single IP address (e.g. 192.168.10.0).

Netmask - enter the Subnet Mask of the local network.

Remote Secure Gateway IP - enter the public IP address of the remote VPN router.

Remote Network - select “Subnet”.

IP Address - enter the IP Address of the remote network. Note that it should be Subnet ID, not a single IP address (e.g. 192.168.1.0).

Netmask - enter the Subnet Mask of the remote network.

Proposal - select ESP.

Authentication Type - select MD5

Encryption - 3DES

Perfect Forward Secrecy - MODP 1024 (Group 2)

Pre-shared Key - enter the security key you want to use for your VPN connection. The same key will need to be specified in the VPN router on the other end (on remote network).

The screenshot shows the configuration page for a D-Link DSL-G804V router. The page is titled "Wireless ADSL VPN Router" and has a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". The "Advanced" tab is selected, and the "VPN" section is active. Under "VPN", the "IPSec" option is selected. The "Enable after 'Apply'" checkbox is checked and circled in red. The configuration fields are as follows:

Field	Value
Connection Name	Work
Local Network	Subnet
IP Address	192.168.10.0
Netmask	255.255.255.0
Remote Secure Gateway IP	202.129.109.82
Remote Network	Subnet
IP Address	192.168.1.0
Netmask	255.255.255.0
Proposal	ESP
Authentication Type	MD5
Encryption	3DES
Perfect Forward Secrecy	MODP 1024 (Group 2)
Pre-shared Key	test

At the bottom of the page, there are four buttons: "Back", "Apply", "Cancel", and "Help".

Click on the “Apply” button when done.

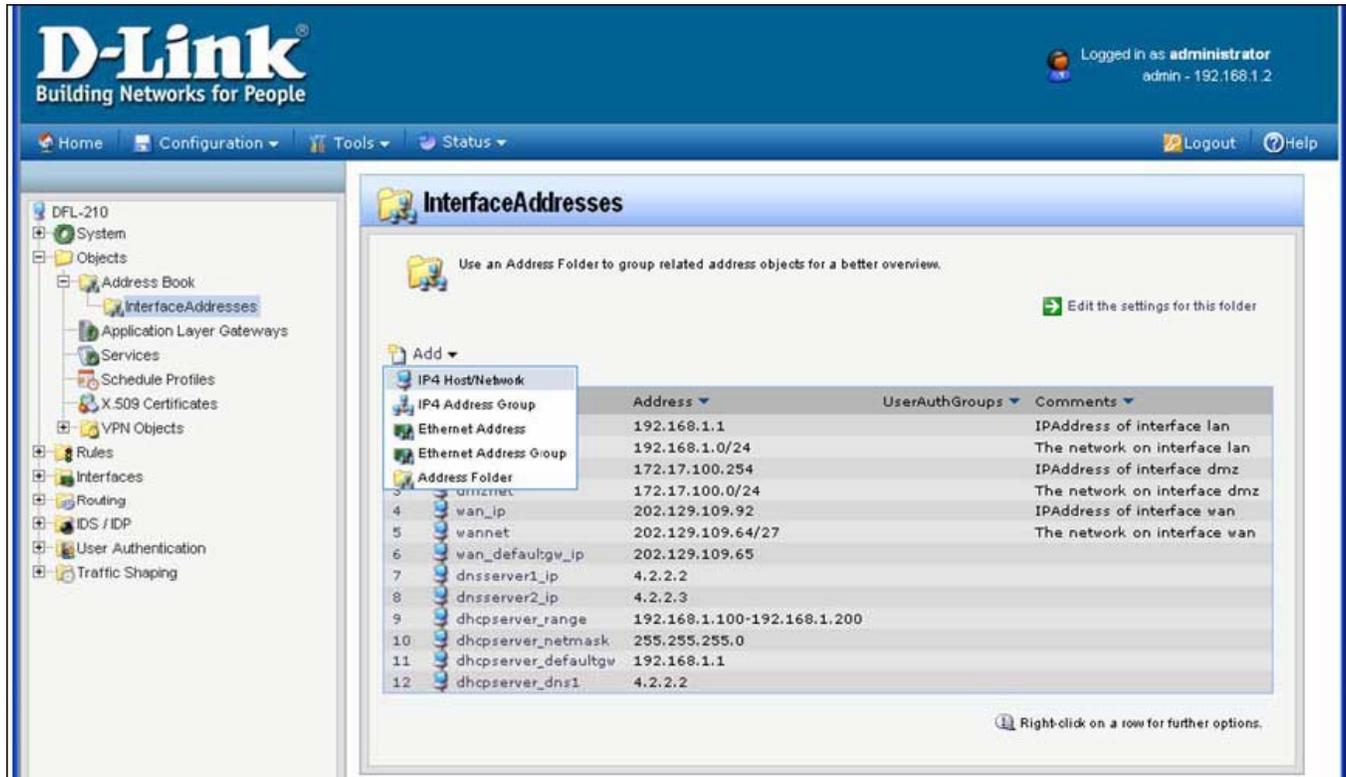
Step 3. Go to Tools > System. Click on the “Save” button. This will save the settings into the router’s memory.

The screenshot displays the web management interface for a D-Link DSL-G804V Wireless ADSL VPN Router. The interface is organized into a sidebar on the left and a main content area on the right. The sidebar contains a product image and a vertical menu of navigation buttons: Admin, Date & Time, System (highlighted in yellow), Firmware, Remote Access, and Logout. The main content area features a top navigation bar with tabs for Home, Advanced, Tools (selected), Status, and Help. Below the navigation bar, the 'System Settings' section is visible, containing options for saving and loading settings to a local hard drive. The 'Save Config to Device Memory' section includes a 'Save' button, which is highlighted with a red arrow. Below this, the 'Reboot Device' section offers options to restart the router with either current settings or factory defaults. A 'Help' icon is located in the bottom right corner of the main content area.

Configuration of the DFL-210/800/1600 VPN Firewall on LAN 1

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 > Address Book > Interface Addresses. Click on Add and select "IP4 Host/Network".

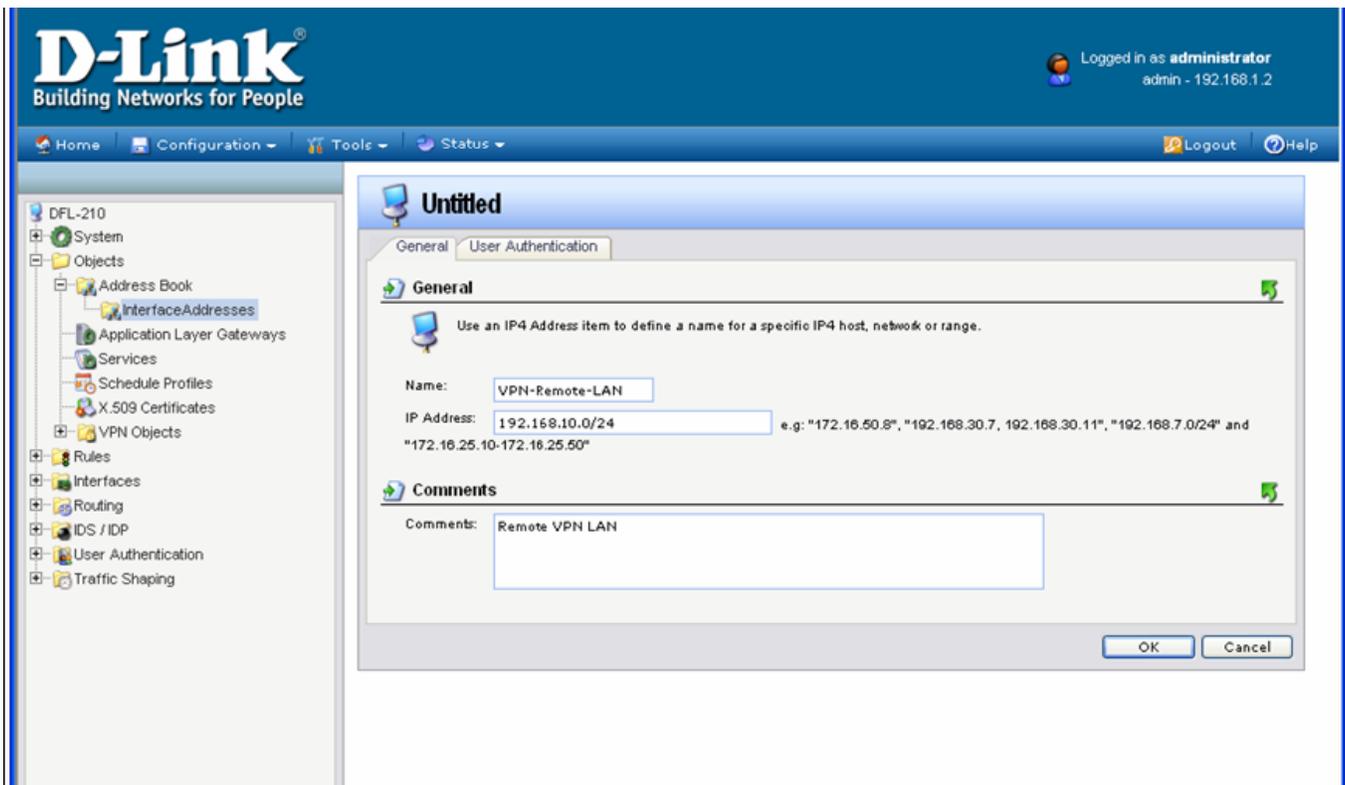


The screenshot shows the D-Link firewall web interface. The top navigation bar includes 'Home', 'Configuration', 'Tools', and 'Status'. The user is logged in as 'administrator' with IP 192.168.1.2. The left sidebar shows a tree view of the configuration, with 'InterfaceAddresses' selected under 'Address Book'. The main content area is titled 'InterfaceAddresses' and contains a table of address objects. A context menu is open over the 'Add' button, showing options like 'IP4 Host/Network', 'IP4 Address Group', 'Ethernet Address', and 'Address Folder'.

	Address	UserAuthGroups	Comments
IP4 Host/Network			
IP4 Address Group			
Ethernet Address	192.168.1.1		IPAddress of interface lan
Ethernet Address Group	192.168.1.0/24		The network on interface lan
Address Folder	172.17.100.254		IPAddress of interface dmz
3	172.17.100.0/24		The network on interface dmz
4	wan_ip	202.129.109.92	IPAddress of interface wan
5	wannet	202.129.109.64/27	The network on interface wan
6	wan_defaultgw_ip	202.129.109.65	
7	dnsserver1_ip	4.2.2.2	
8	dnsserver2_ip	4.2.2.3	
9	dhcpserver_range	192.168.1.100-192.168.1.200	
10	dhcpserver_netmask	255.255.255.0	
11	dhcpserver_defaultgw	192.168.1.1	
12	dhcpserver_dns1	4.2.2.2	

Specify the settings of the remote network on the other end of the VPN tunnel.
Under Name enter "VPN-Remote-LAN".

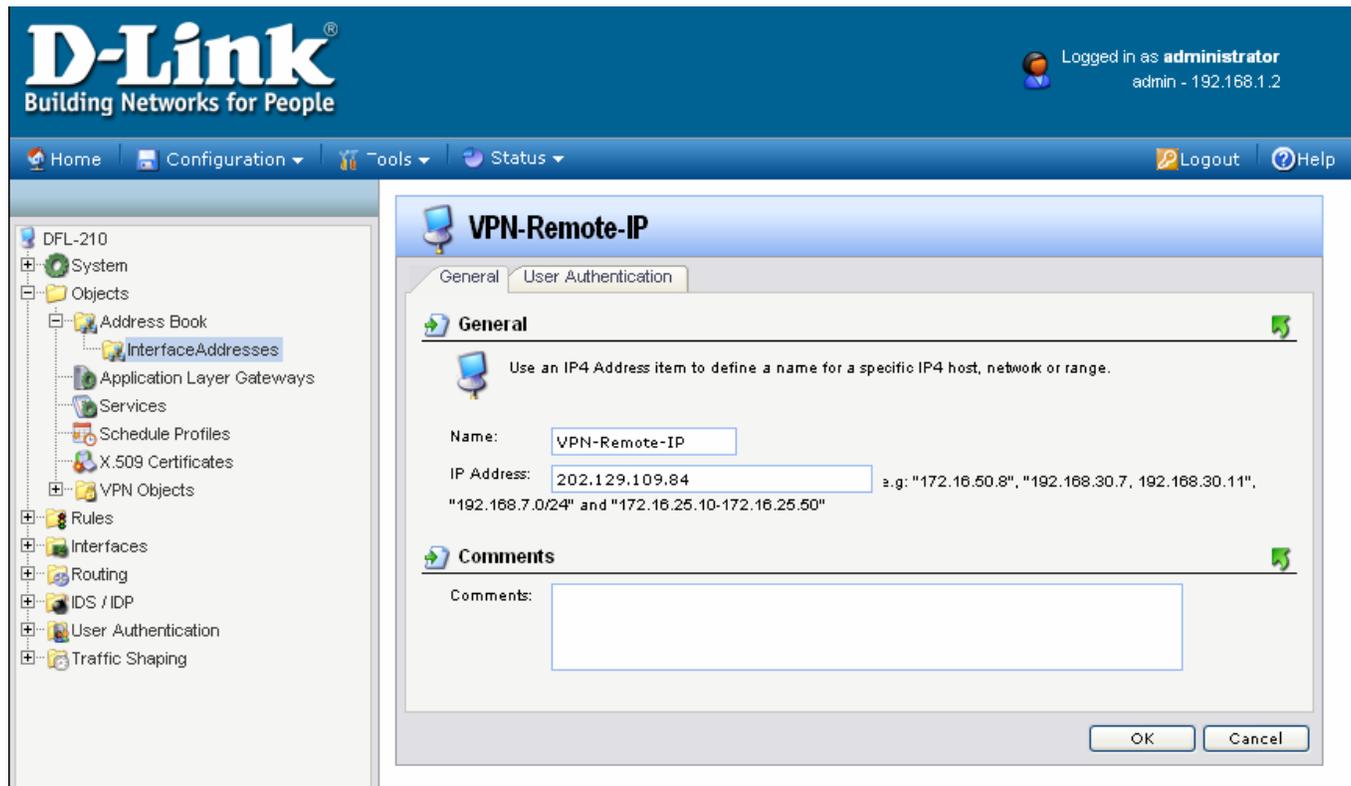
Under IP Address enter the Subnet ID and Mask Bits for the remote network: in our example it is 192.168.10.0/24.
Click on the OK button.



Step 3. Add another “IP4 Host/Network”. Enter the settings of the VPN endpoint, the public IP address of the router on LAN 2.

Under Name enter “VPN-Remote-IP”.

Under IP address specify the public IP address of the remote network (the IP address assigned to the DSL-G804V by the ISP).

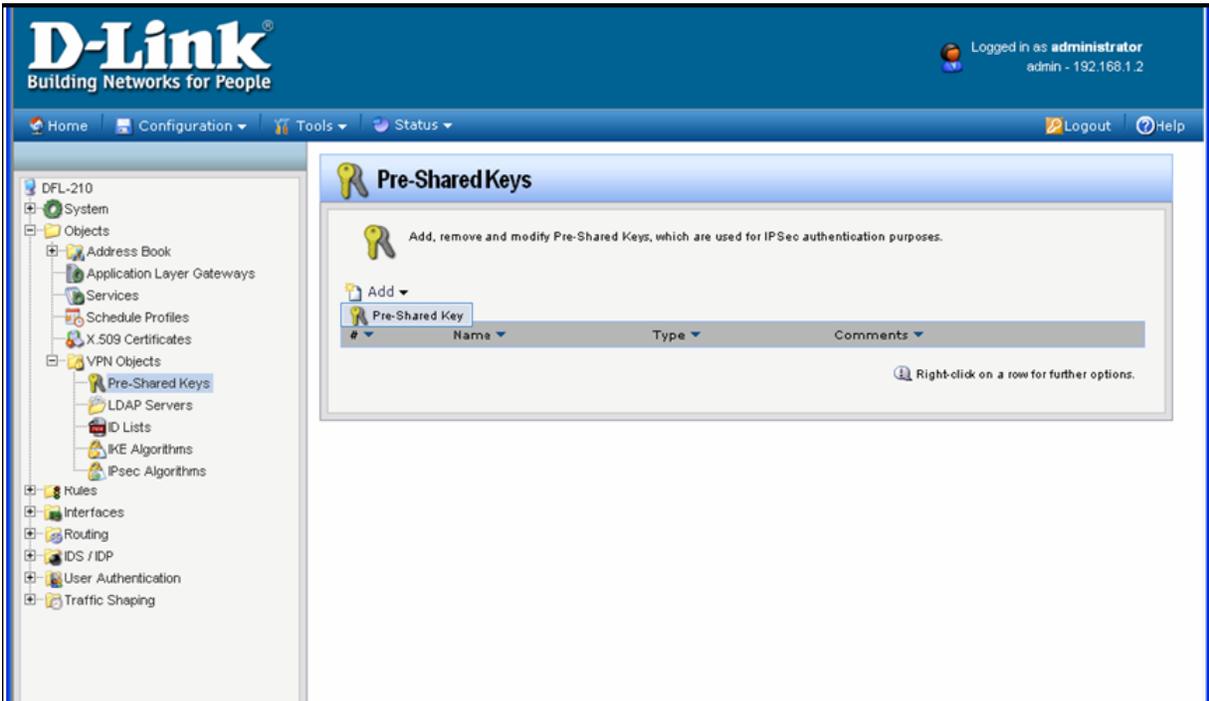


Dynamic IP Address: If remote network has dynamic public IP address, you can utilize one of the “Dynamic DNS” services available on the Internet. In this case the dynamic IP address of the remote site will be associated with a URL. To specify a URL as an address use this format: **dns:yoursite.dyndns.org**. Type the required URL under Interfaces > IPsec Tunnels > ‘your tunnel settings’ > Remote Endpoint (**Step 5**).

To configure the VPN firewall to update one of the Dynamic DNS services go to System > Misc. Clients > Add...

When setting up IPsec VPN Tunnel (**Step 5**) which connects to a site with dynamic IP address or accepts connections from roaming IPsec clients with dynamic IP addresses, set Remote Network as “Any” and Remote Endpoint as “None”.

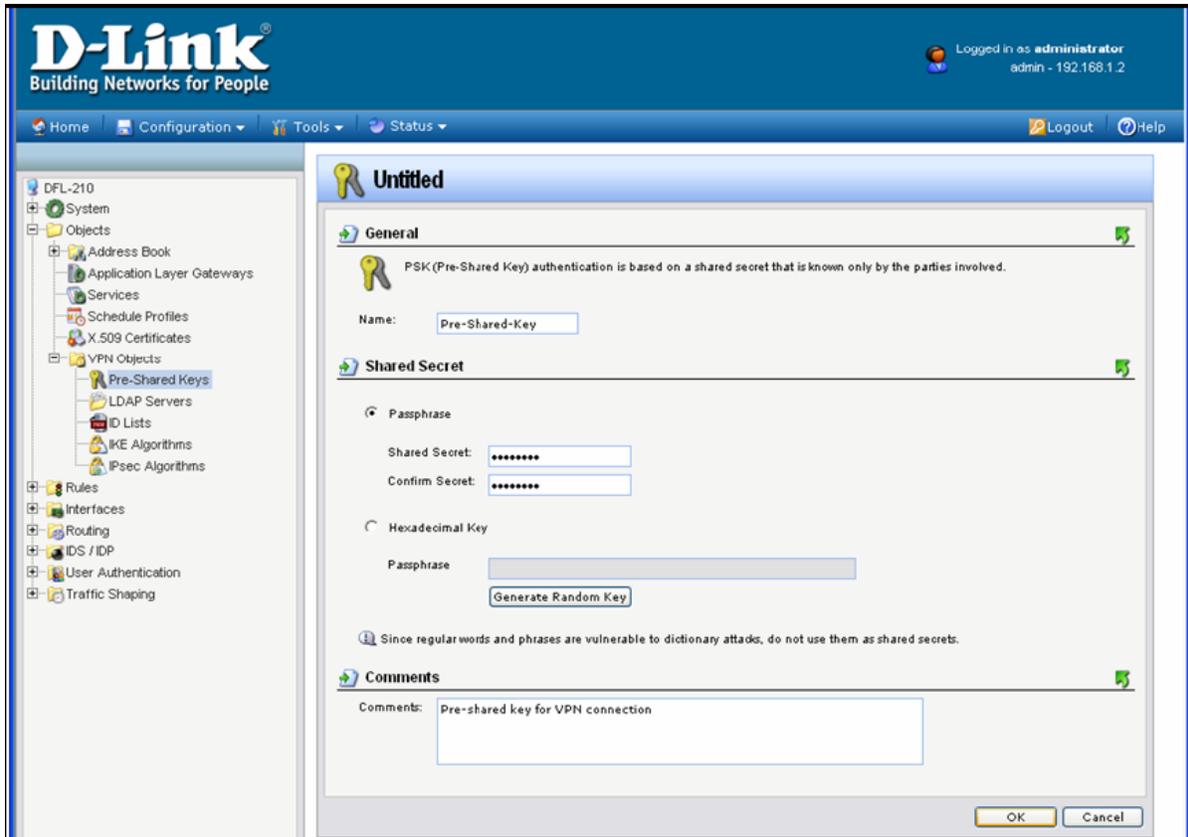
Step 4. Go to Object > VPN Objects > Pre-Shared Keys. Click on Add and select Pre-Shared Key.



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

Under Shared Secret select “Passphrase” and type in the key that you have entered when setting up the DSL-G804V.

Click OK when done.



Step 5. Go to Interfaces > IPsec Tunnels. Click on Add and select IPsec Tunnel.

Enter your IPsec tunnel settings.

Under Name enter "IPsec-tunnel".

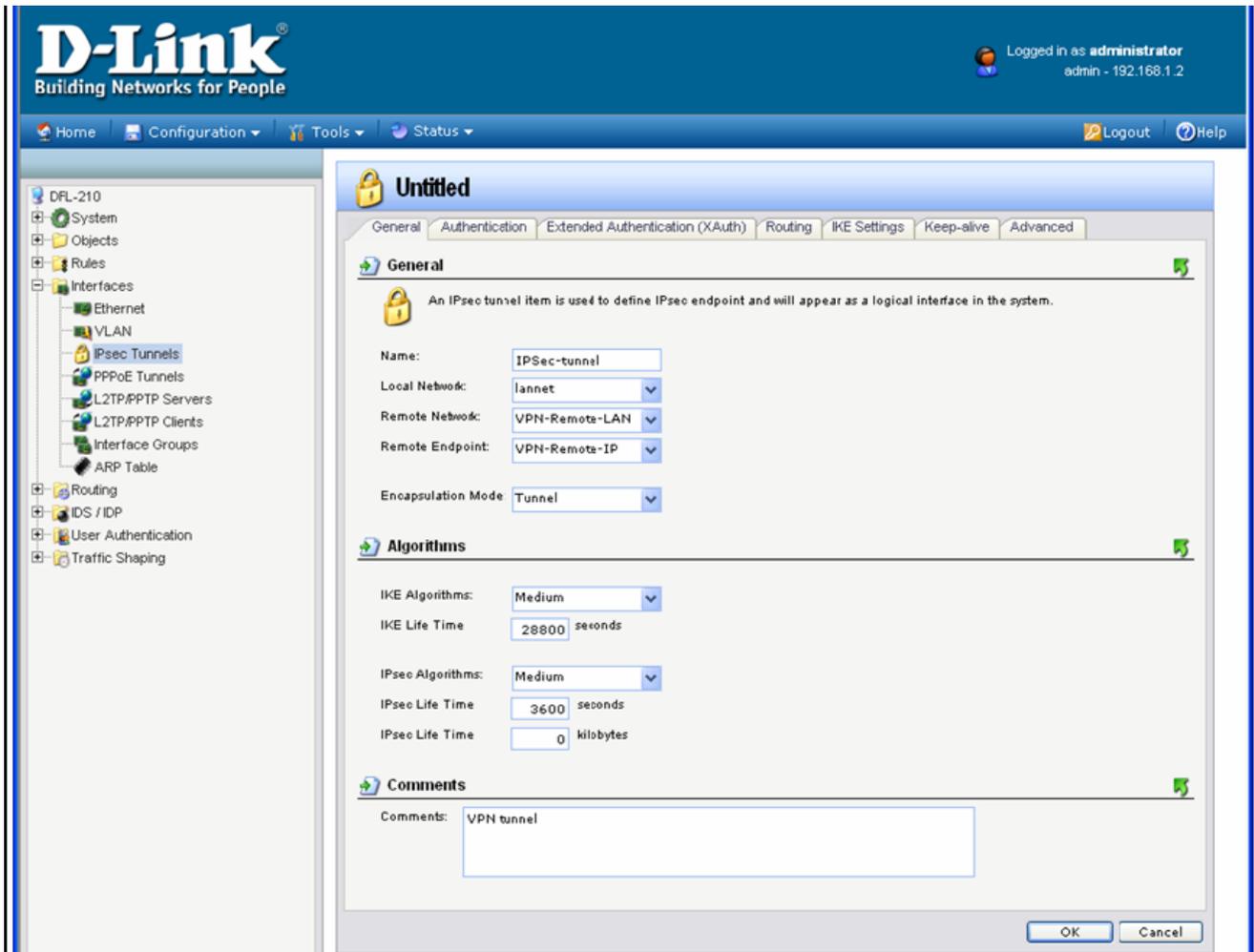
Under Local Network select "lanet" (this is the private network on this side of the VPN tunnel).

Under Remote Network select "VPN-Remote-LAN" (this is the private network on the other side of the VPN tunnel, see **Step 2**).

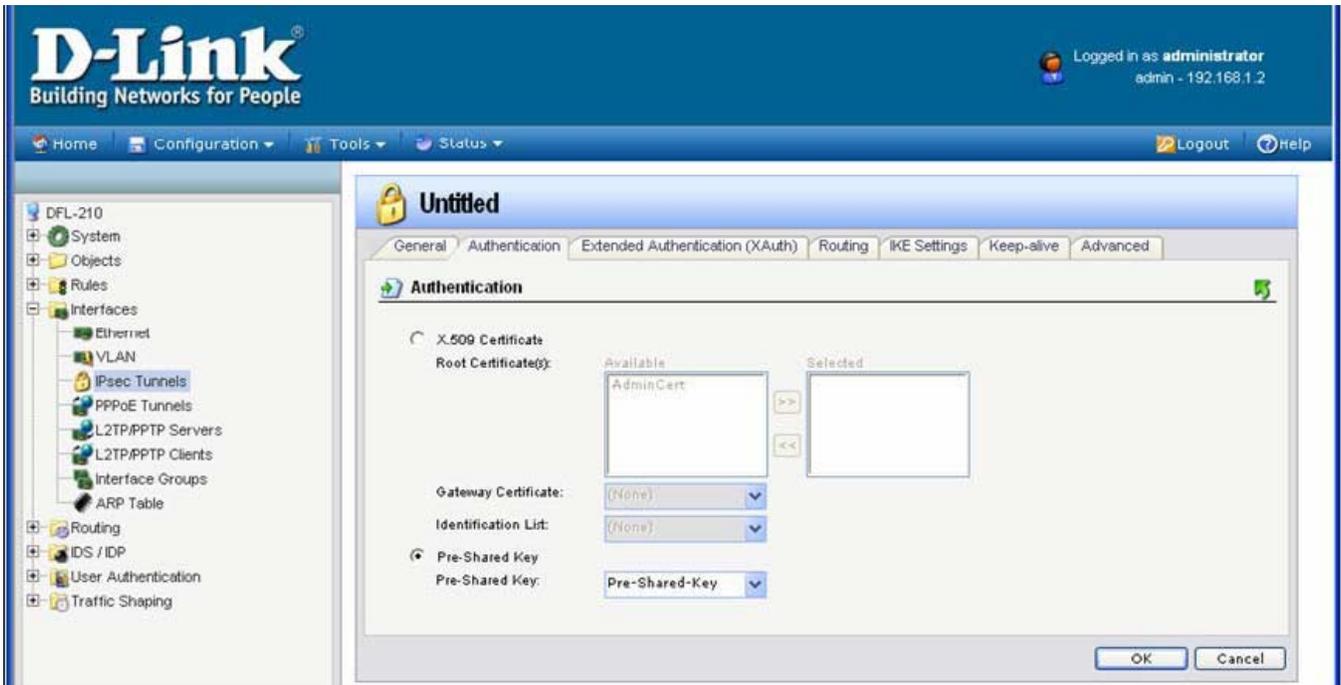
Under Remote Endpoint select "VPN-Remote-IP" (this is the public up of the remote network, see **Step 3**). Encapsulation Mode should be set to Tunnel.

Under Algorithms set IKE Algorithm to "Medium". Set IKE/IPsec lifetime to 28800 sec.
IPsec Algorithm - set to Medium. IPsec Lifetime - 3600 sec and 0 kilobytes.

Note: 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 4**).



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



Click on IKE Settings tab. Under IKE change the DH Group to “2”, Under Perfect Forward Secrecy select “PFS” from the drop down box and make sure the DH Group is “2”.

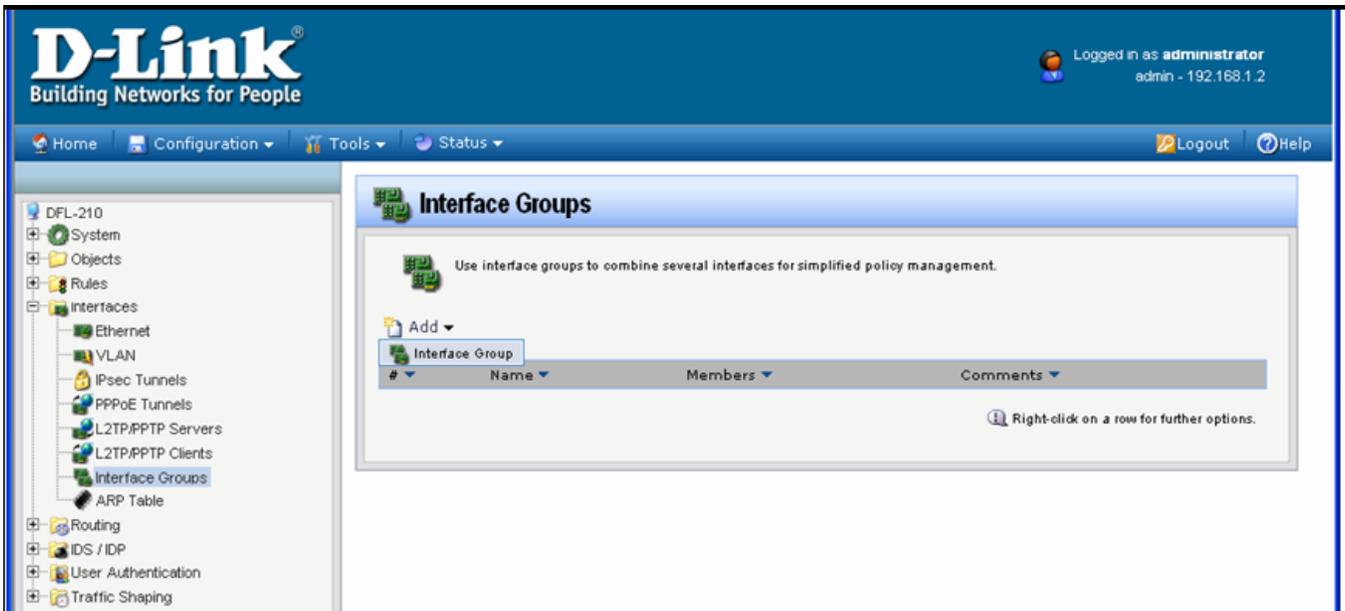
Click on the OK button.

The screenshot shows the D-Link web interface for configuring an IPSEC tunnel. The interface includes a navigation menu on the left with categories like System, Objects, Rules, Interfaces, Routing, and Traffic Shaping. The main content area is titled 'IPSEC-tunnel' and has several tabs: General, Authentication, Extended Authentication (X.Auth), Routing, IKE Settings, Keep-alive, and Advanced. The 'IKE Settings' tab is active, showing the following configuration options:

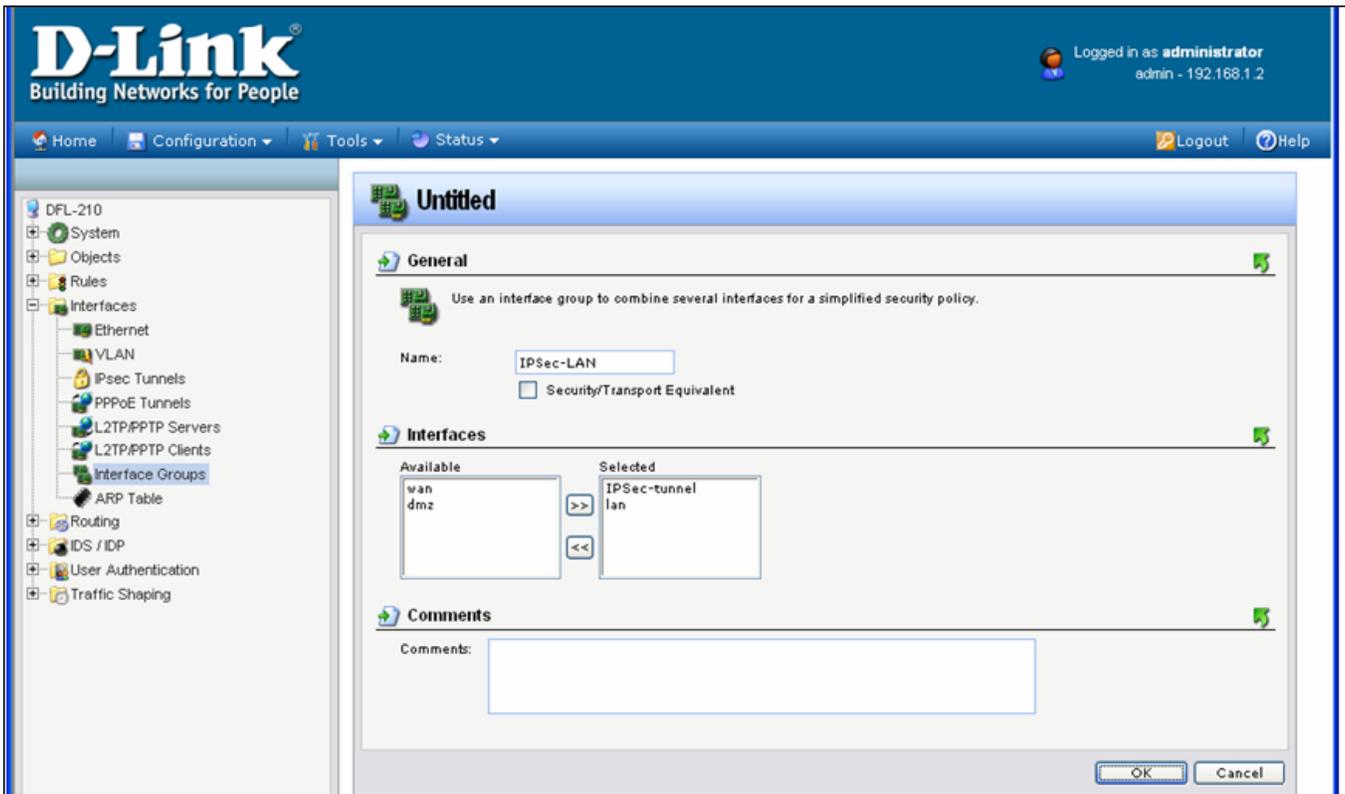
- IKE:** Radio buttons for 'Main' (selected) and 'Aggressive'. A dropdown menu for 'DH Group' is set to '2'.
- Perfect Forward Secrecy:** A dropdown menu for 'PFS' is set to 'PFS', and a dropdown menu for 'DH Group' is set to '2'.
- Security Association:** Radio buttons for 'Per Net' (selected) and 'Per Host'.
- Compatibility Flags:** A checkbox for 'Do not verify padding' is unchecked.
- NAT Traversal:** Radio buttons for 'Off', 'On if supportec and NATed' (selected), and 'On if supportec'.

At the bottom right of the configuration area, there are 'OK' and 'Cancel' buttons.

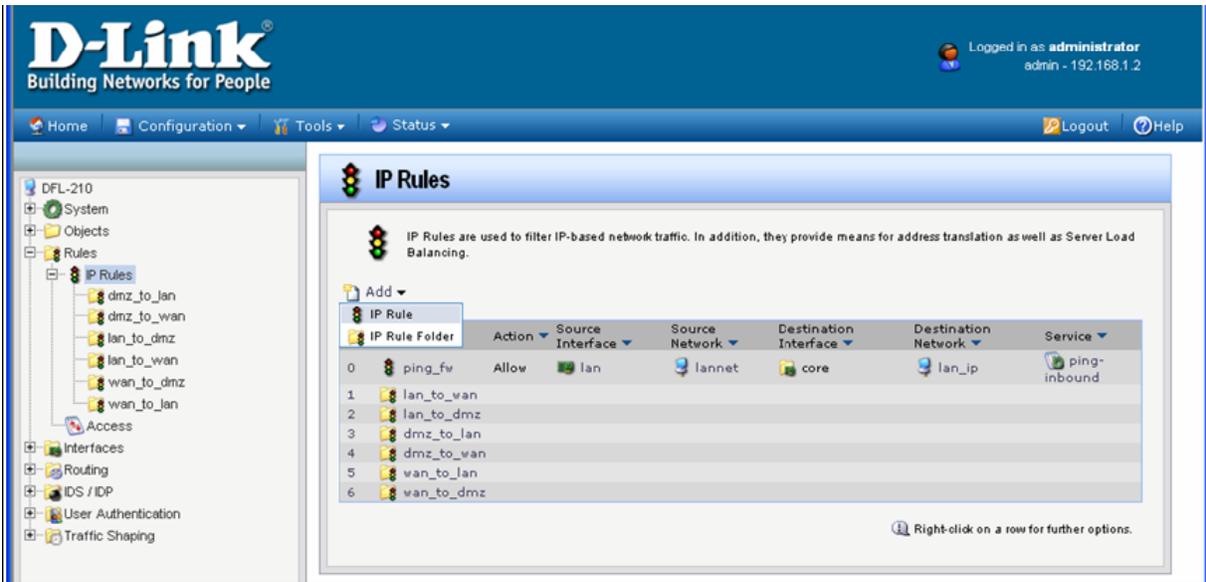
Step 6. Go to Interfaces > Interface Groups. Click on Add and select Interface Group.



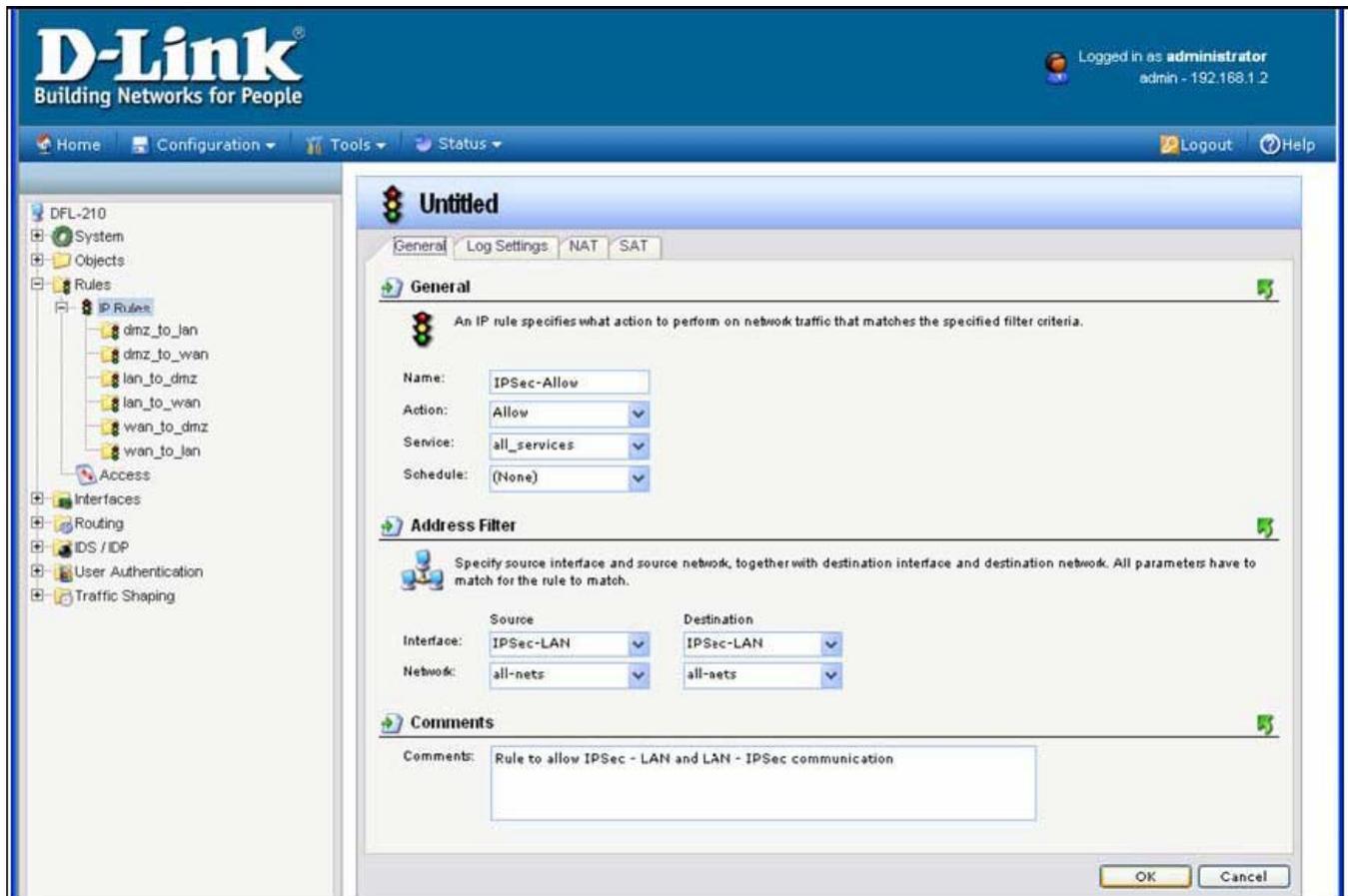
Create a group which has your IPsec tunnel and your LAN.
Under Name type IPsec-LAN.
Under Interfaces add "IPsec-tunnel" and "lan" into Selected field.
Click on the OK button.



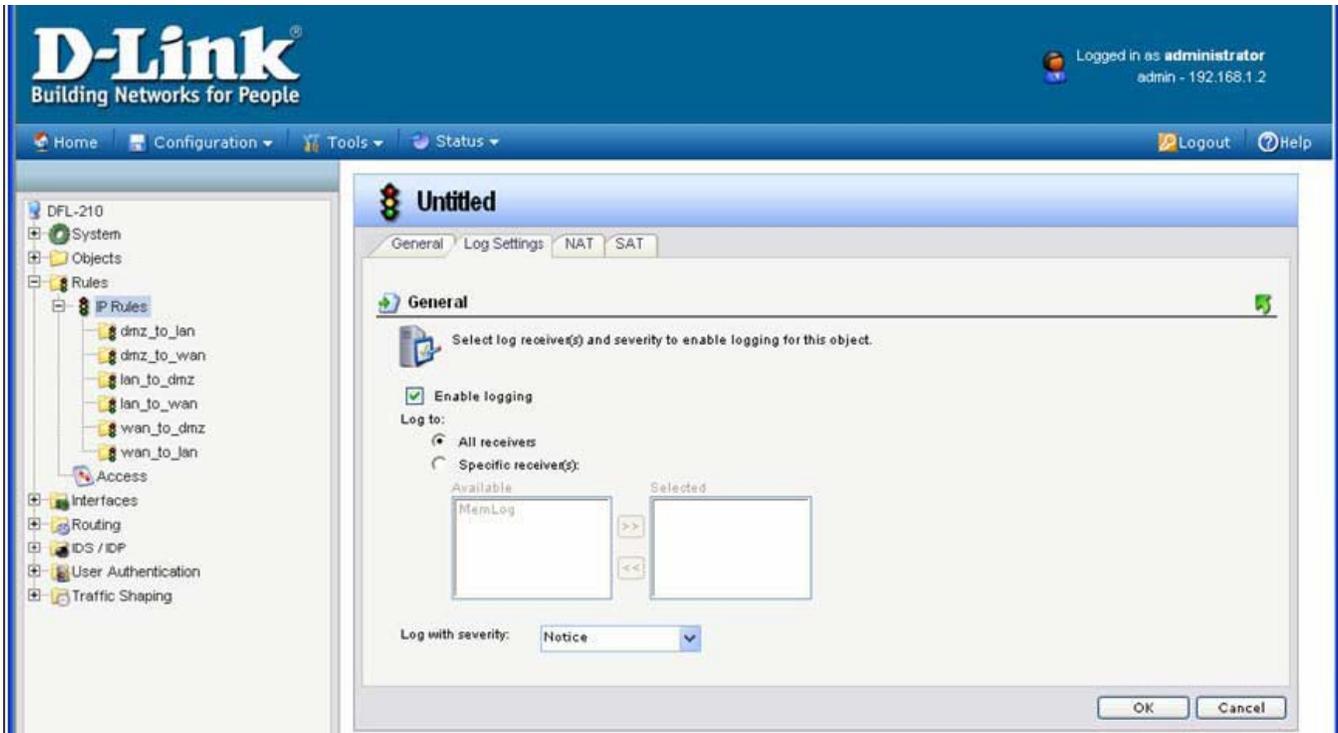
Step 7. Go to Rules > IP Rules. Click on Add and select IP Rule.



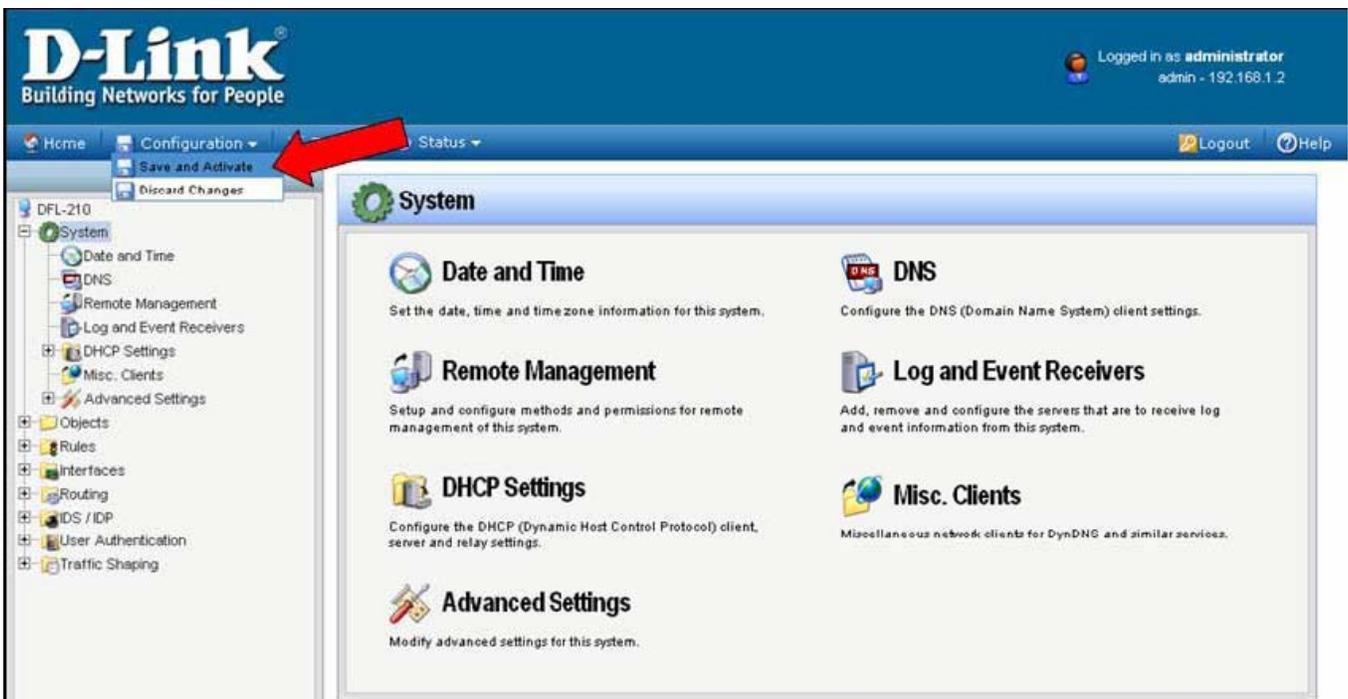
This rule will allow communication between the LAN and the IPSec tunnel.
Under Name type “IPSec-Allow”.
Under Action select “Allow”.
Under Service select “all_services”.
Under Address Filter specify the following:
Source and Destination Interfaces: “IPSec-LAN” (this is the group you created in **Step 6**).
Source and Destination Network: select “all-nets”.



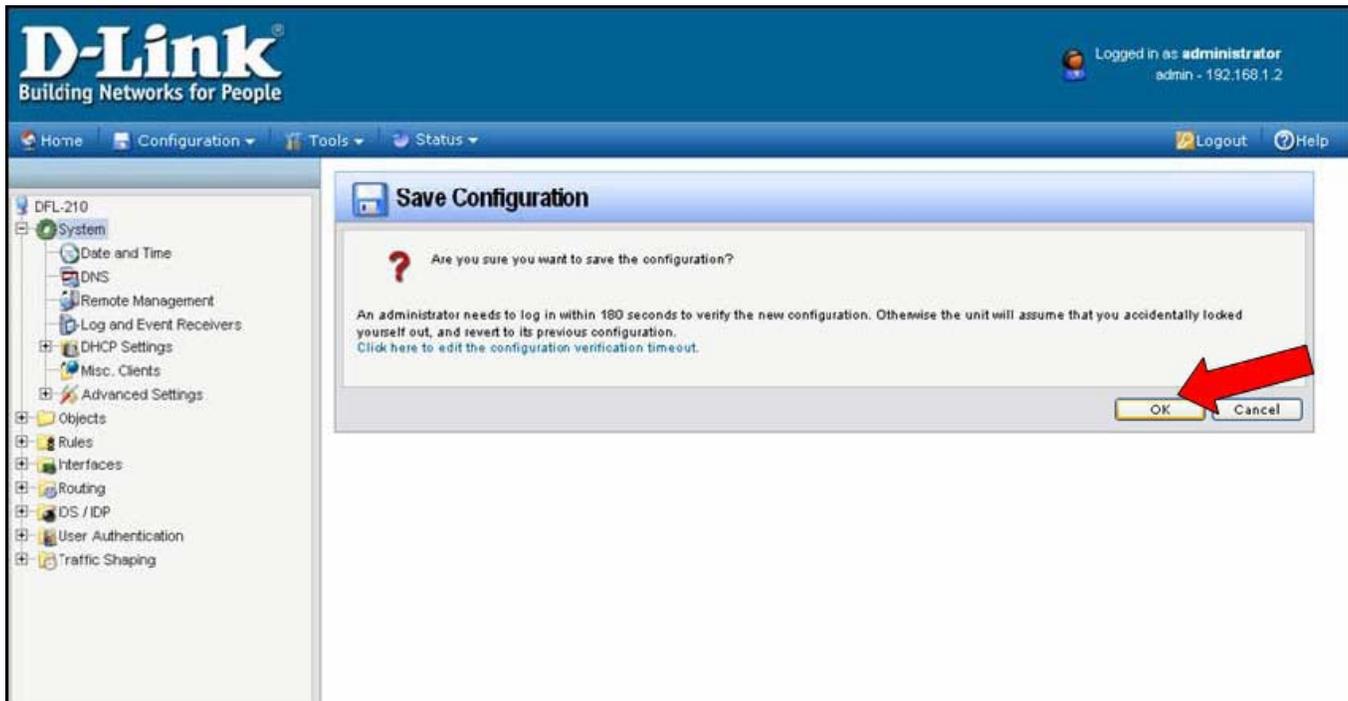
Click on Log Settings tab.
Select the Enable Logging option.
Click on the OK button when done.



Step 8. Save the new configuration. In the top menu bar click on Configuration and select “Save and Activate”.



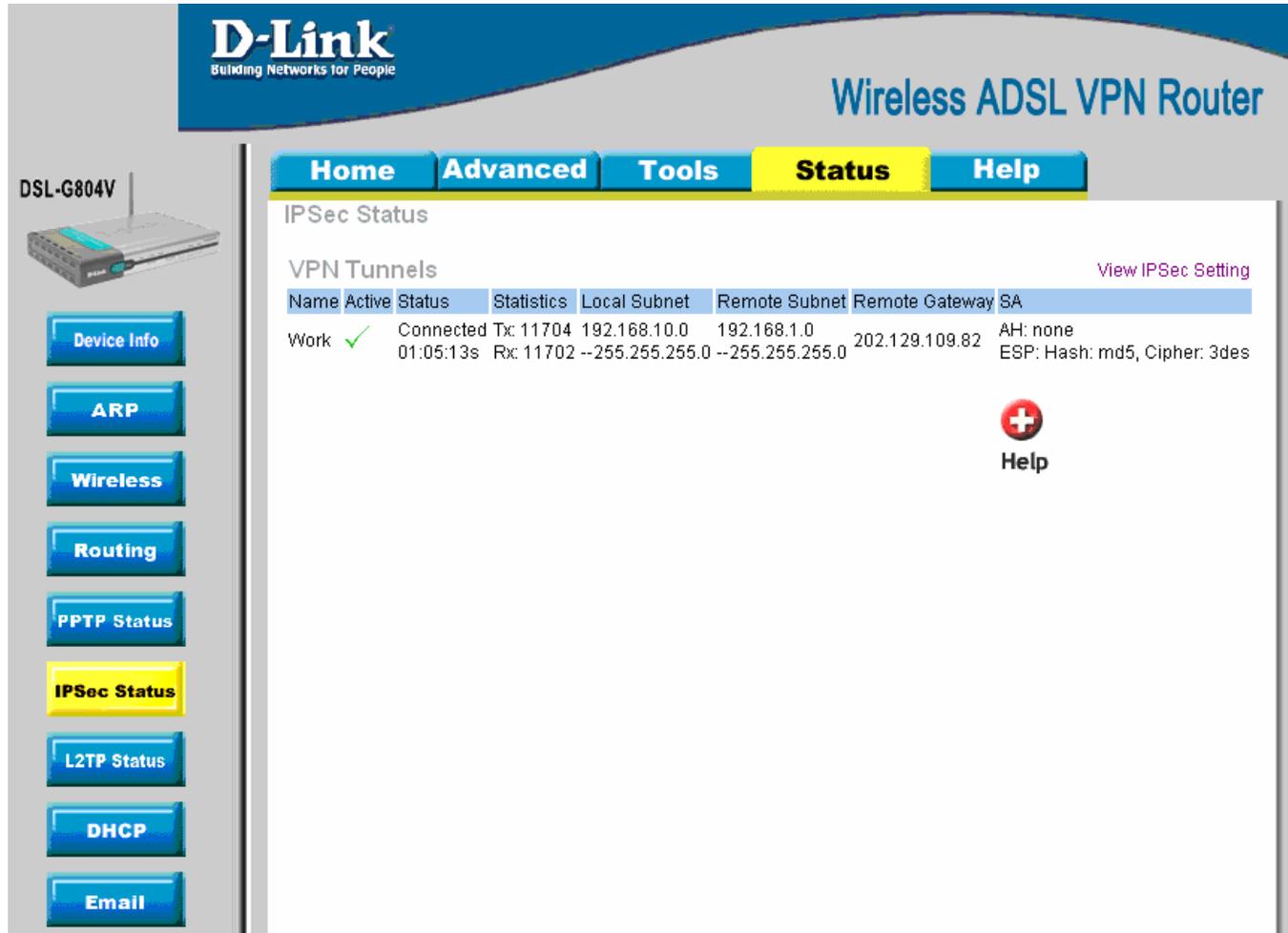
Click on OK to confirm the new settings activation:



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

How to check VPN connection status on the DSL-G804V

On the DSL-G804V click on Status > IPsec Status.
Under VPN Tunnels > Status it should say Connected.



The screenshot displays the web management interface of a D-Link DSL-G804V Wireless ADSL VPN Router. The interface is titled "D-Link Building Networks for People" and "Wireless ADSL VPN Router". The navigation menu includes Home, Advanced, Tools, Status (highlighted), and Help. On the left sidebar, there is a "DSL-G804V" label with an image of the router and a vertical menu of buttons: Device Info, ARP, Wireless, Routing, PPTP Status, IPsec Status (highlighted), L2TP Status, DHCP, and Email.

The main content area is titled "IPsec Status" and contains a "VPN Tunnels" section. A link "View IPsec Setting" is visible. Below the link is a table with the following data:

Name	Active	Status	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA
Work	✓	Connected	Tx: 11704 01:05:13s Rx: 11702	192.168.10.0 --255.255.255.0	192.168.1.0 --255.255.255.0	202.129.109.82	AH: none ESP: Hash: md5, Cipher: 3des

Below the table, there is a red plus icon and the text "Help".

How to check VPN connection status on the DFL-210

To check the status of your VPN connection, click on Status and select IPsec. If the VPN tunnel is up, you will see an active entry under IPsec SAs.

IPsec Status

VPN Interface: **IPSec-tunnel** [List all active IKE SAs.](#)

Send Rate: 0 kbps
Receive Rate: 0 kbps

Send rate over the past 24 hours

Receive rate over the past 24 hours

IPsec SAs

Remote Gateway	Local Net	Remote net	Protocol
202.129.109.93	192.168.1.0/24	192.168.0.0/24	ESP: rijndael-cbc hmac-md5-96

In order to trigger the VPN firewall to establish VPN tunnel try accessing any IP address on the remote private network (e.g. ping an IP address on remote LAN).

You can see the connection log under Status > Logging.

Log Status

Internal Logging (1-45) [Refresh Log](#) [Clear log](#)

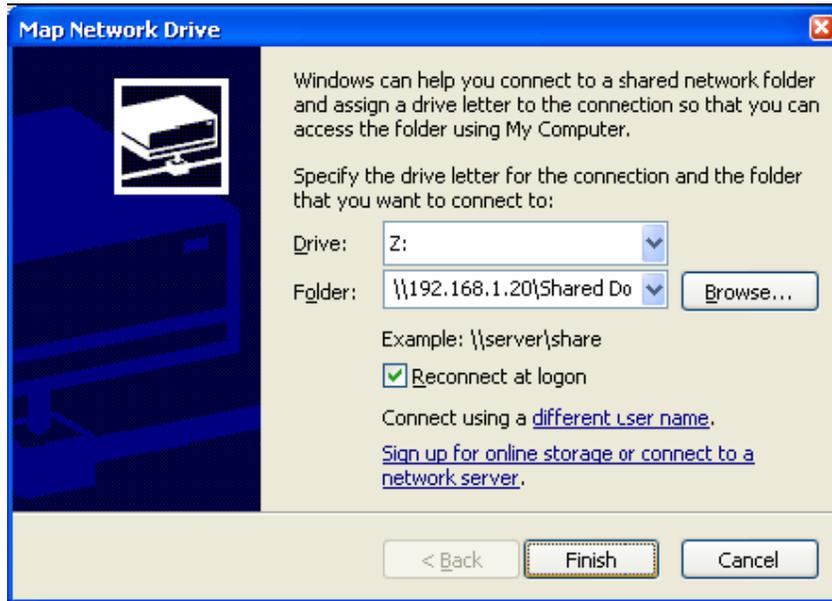
Date	Severity	Category	Rule	Proto	Src/If	Src/DstIP	Src/DstPort	Details
2006-05-19 00:36:33	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2	1030	conndestif=IPSec-tunnel
2006-05-19 00:36:29	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	53	connsrcid=512 conndestif=IPSec-tunnel conndestid=512 origsent=1680 termsent=1680
2006-05-19 00:36:12	Notice	CONN	IPSecBeforeRules	UDP	wan	202.129.109.93	500	conndestif=core origsent=7748 termsent=0
2006-05-19 00:35:53	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.149	connsrcid=512 conndestif=IPSec-tunnel conndestid=512
2006-05-19 00:35:35	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.1	connsrcid=512 conndestif=IPSec-tunnel conndestid=512 origsent=60 termsent=0
2006-05-19 00:35:26	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.1	connsrcid=512 conndestif=IPSec-tunnel conndestid=512
2006-05-19 00:34:15	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2	1028	conndestif=IPSec-tunnel
2006-05-19 00:33:59	Informational	IPSEC						SA ESP[b570dacf] alg [rijndael-cbc/16]+hmac[hmac-md5-96] bundle [4,0] pri 0 opts src=ipv4_subnet(any:0,[0..7]=192.168.0.0/24) dst=ipv4_subnet(any:0,[0..7]=192.168.1.0/24)
2006-05-19 00:33:59	Informational	IPSEC						SA ESP[9e022db6] alg [rijndael-cbc/16]+hmac[hmac-md5-96] bundle [4,0] pri 0 opts src=ipv4_subnet(any:0,[0..7]=192.168.1.0/24) dst=ipv4_subnet(any:0,[0..7]=192.168.0.0/24)
2006-05-19 00:33:59	Informational	IPSEC						Phase-2 [responder] done bundle 4 with 2 SA's by rule 1: 'ipsec ipv4_subnet(any:0,[0..7]=192.168.1.0/24)<->ipv4_subnet(any:0,[0..7]=192.168.0.0/24)(gw:ipv4(any:0,[0..3]=202.129.109.93))'
2006-05-19 00:33:45	Notice	CONN	IPSec-Allow	TCP	lan	192.168.1.2	4943	conndestif=IPSec-tunnel origsent=790 termsent=1136
2006-05-19 00:33:16	Notice	CONN	IPSec-Allow	TCP	IPSec-tunnel	192.168.0.149	3844	conndestif=lan origsent=168 termsent=404

If VPN Tunnel can not be established:

- Make sure that the modem in front of the DFL-firewall supports VPN passthrough.
- Make sure that both networks are using different IP subnets.
- Check the Pre-shared keys, security algorithms and life times, make sure they match on both VPN routers.
- Restart both firewalls.

Connecting to shared resources via VPN

To connect to shared resources via VPN 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.