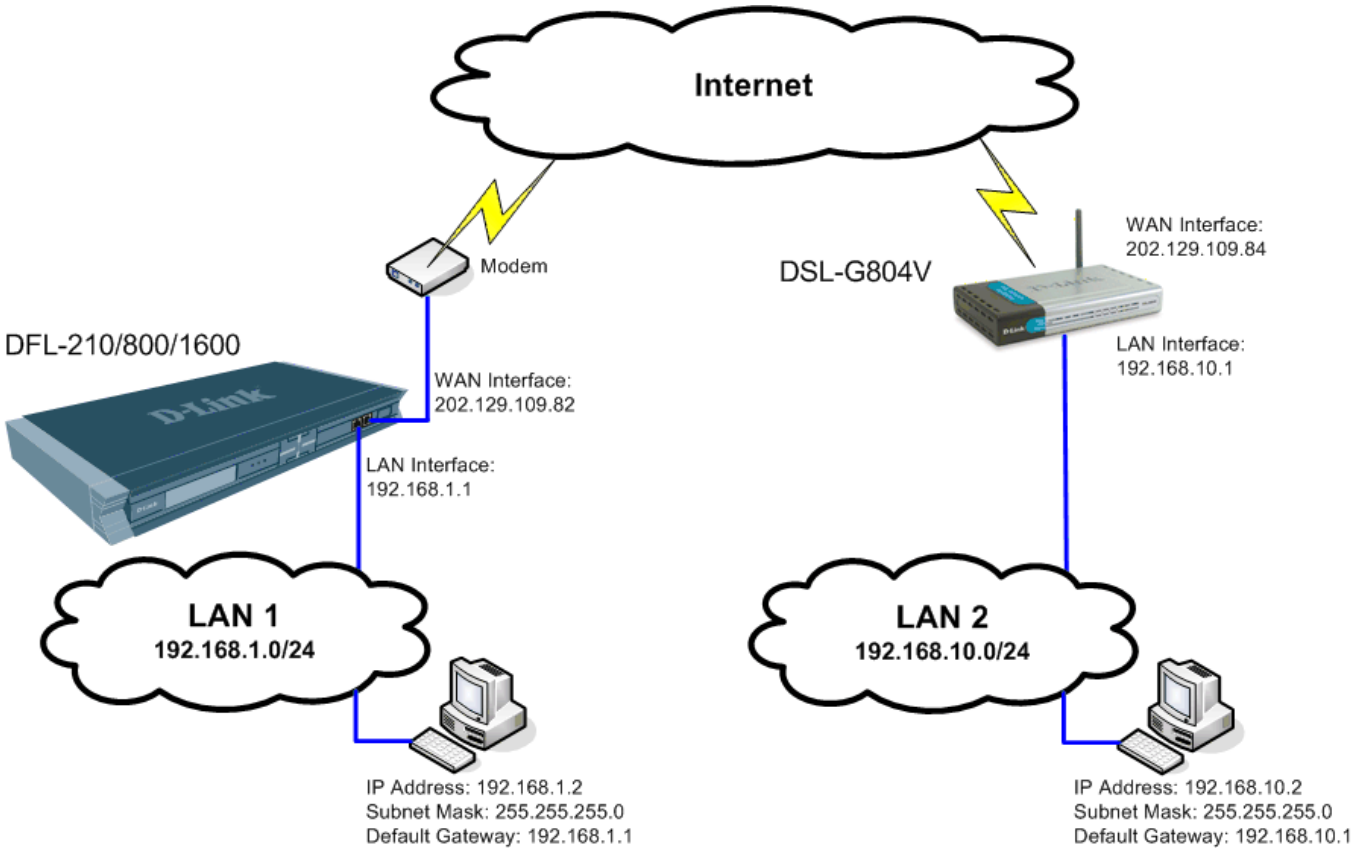
How to setup IPSec VPN connection between DSL-G804V and DFL-210/800/1600

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.

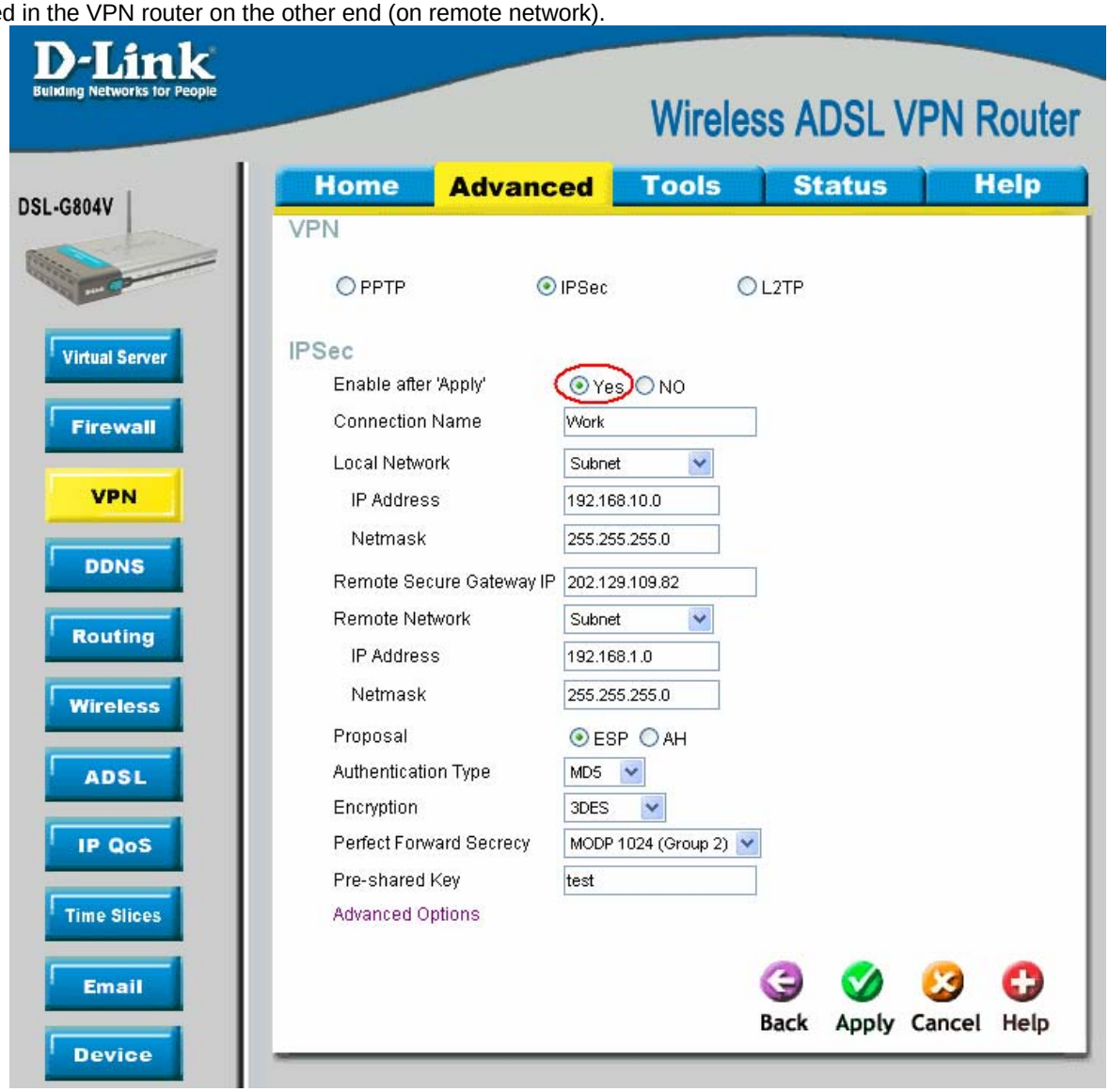
Configuration of the DSL-G804V router on LAN 2

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.

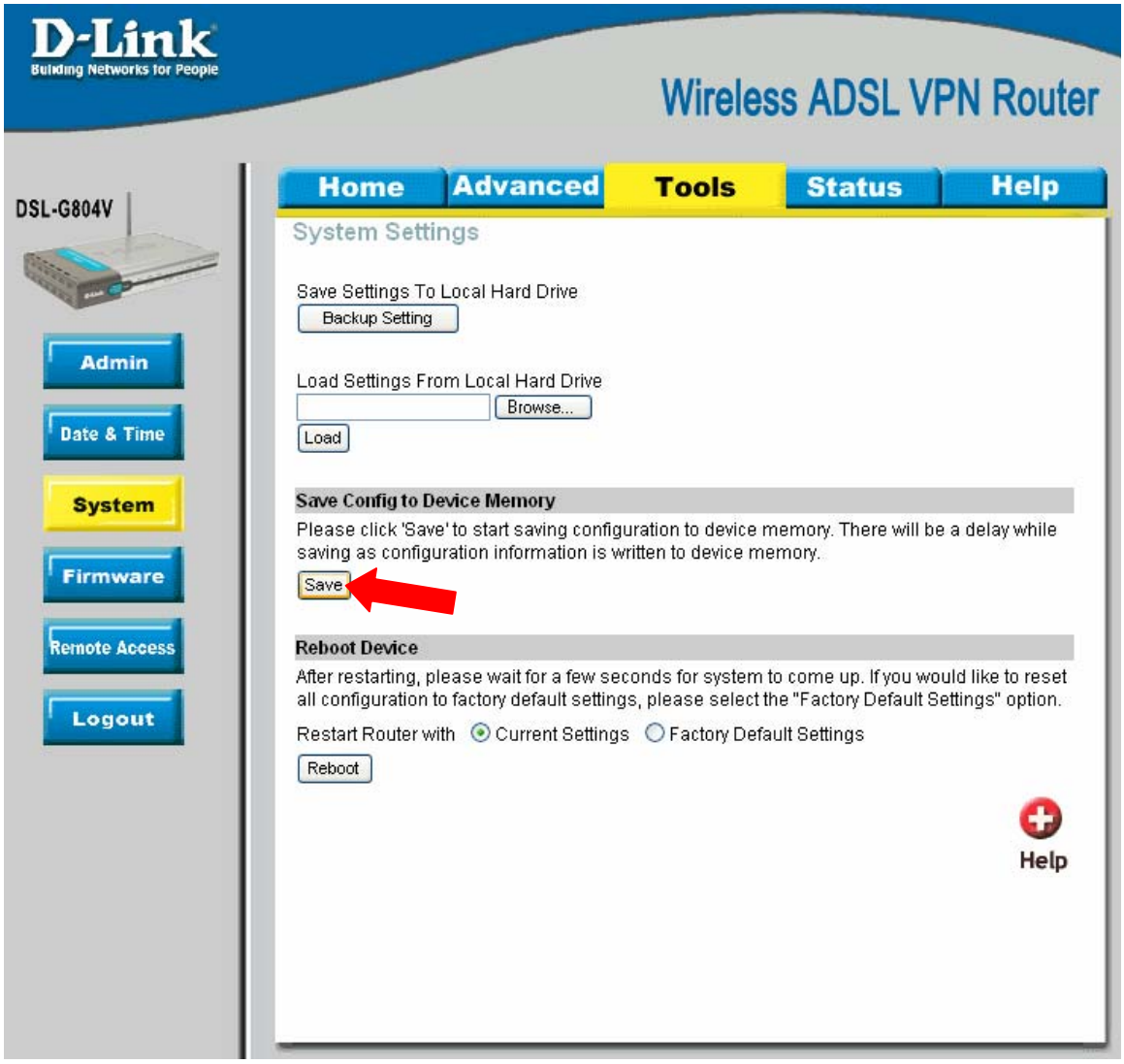
Remote Secure Gateway IP - enter the public IP address of the remote VPN router.
Remote Network - select "Subnet".
IP Address - enter the IP Address of the remote network. Note that it should be Subnet ID, not a single IP address (e.g. 192.168.1.0).
Netmask - enter the Subnet Mask of the remote network.

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).



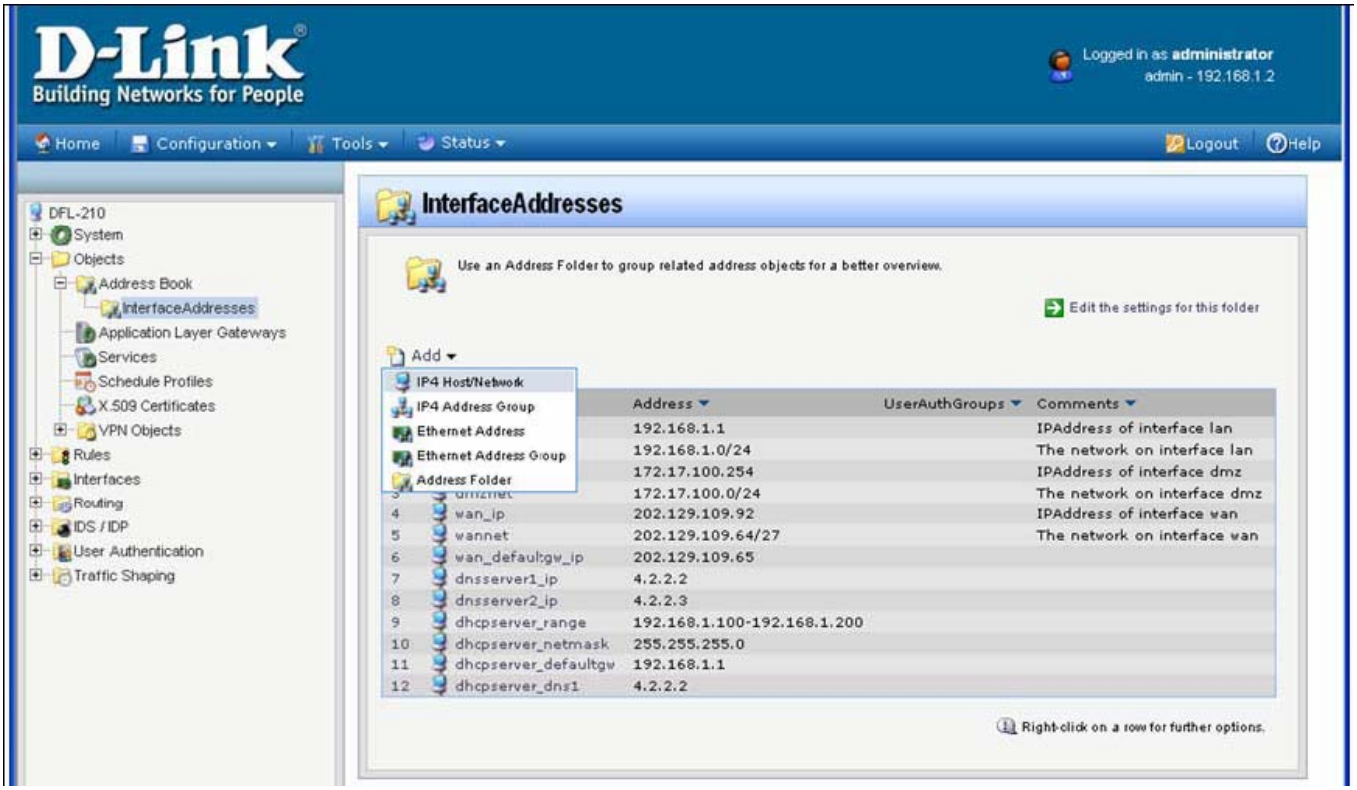
Click on the "Apply" button when done.

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



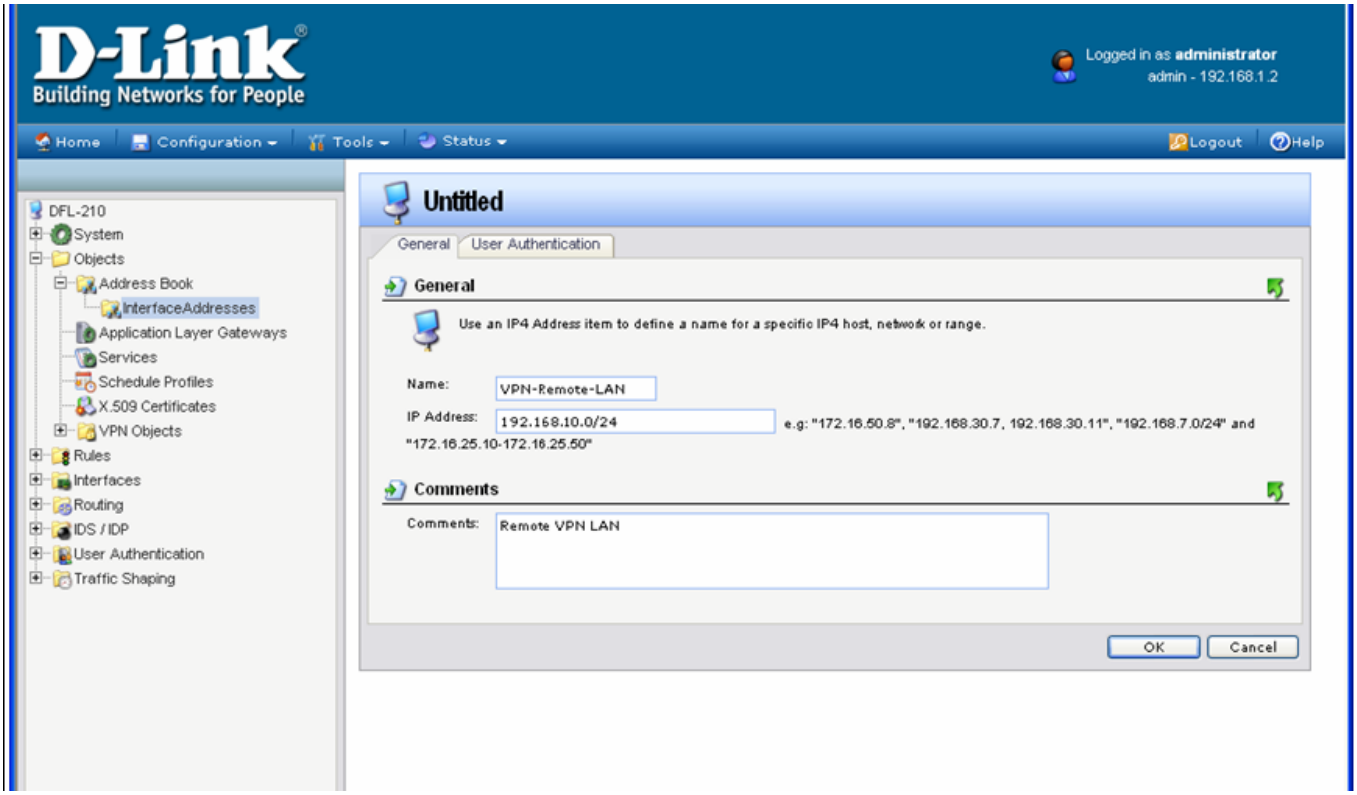
Configuration of the DFL-210/800/1600 VPN Firewall on LAN 1

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”.



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”.

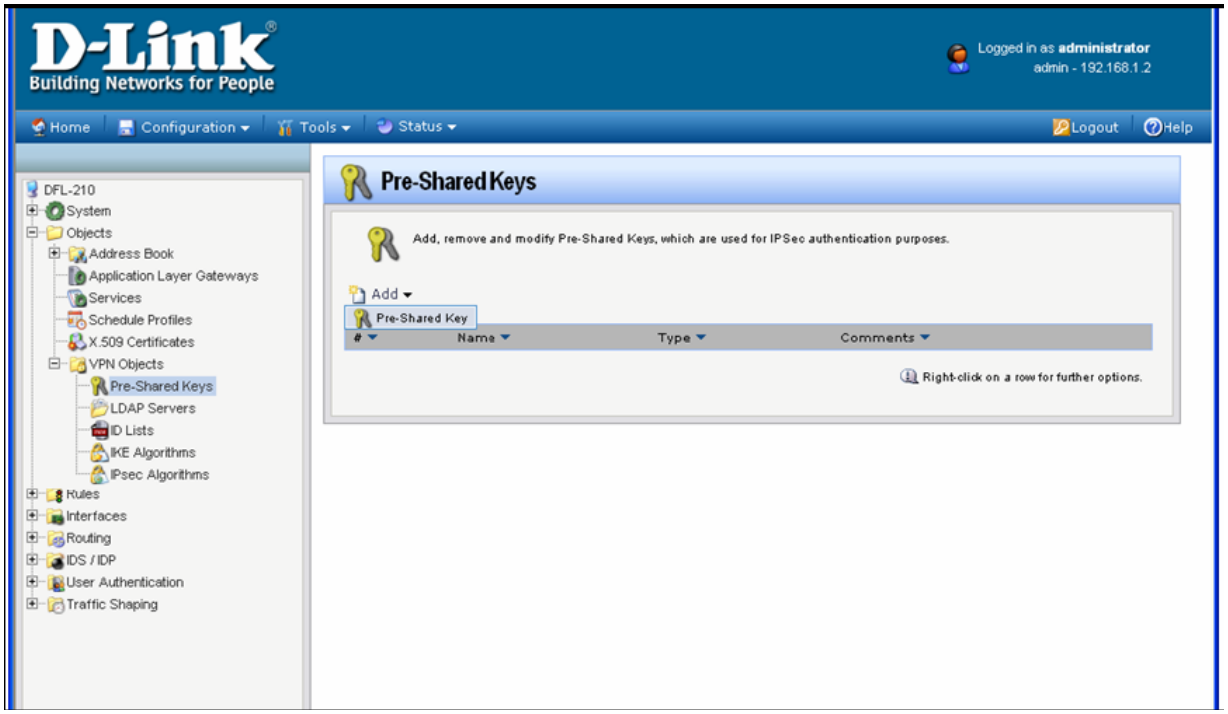
Under IP address specify the public IP address of the remote network (the IP address assigned to the DSL-G804V by the ISP).

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”.*

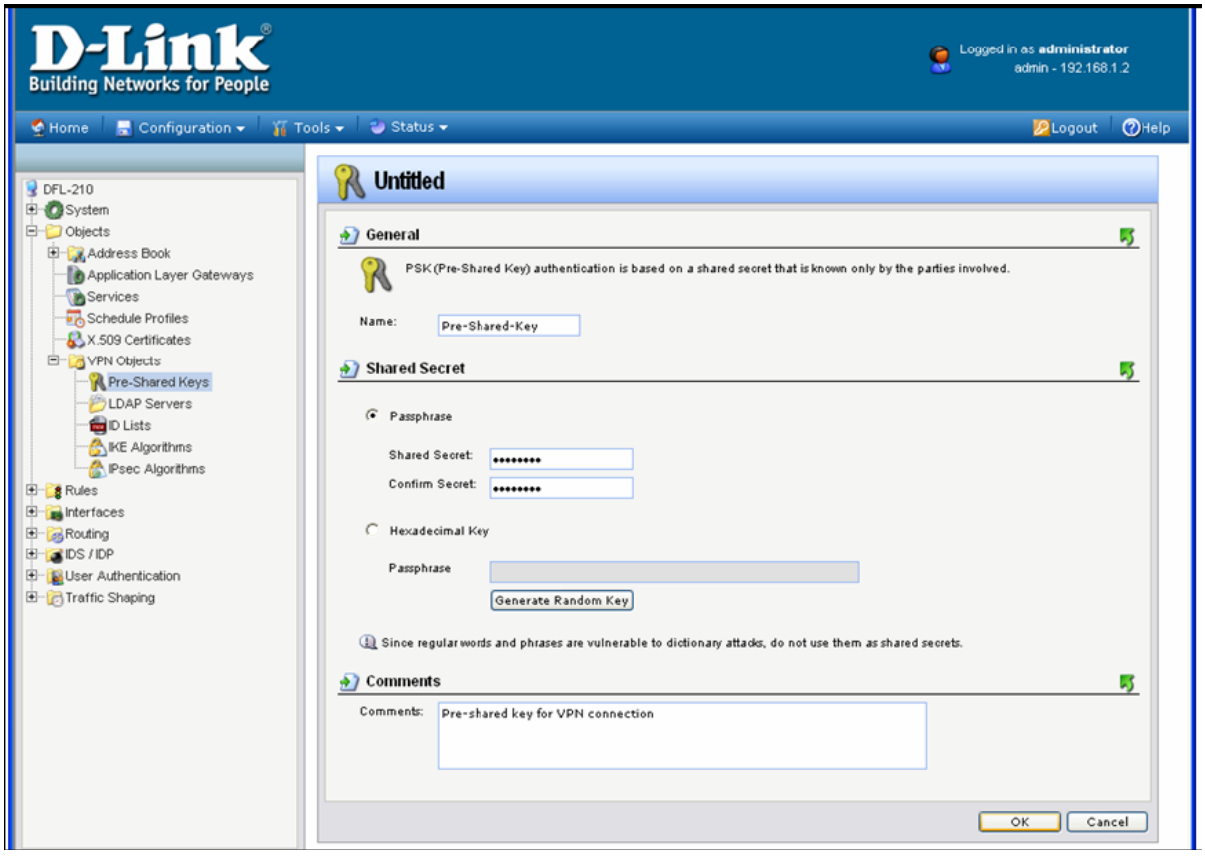
Step 4. Go to Object > VPN Objects > Pre-Shared Keys. Click on Add and select Pre-Shared Key.



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.



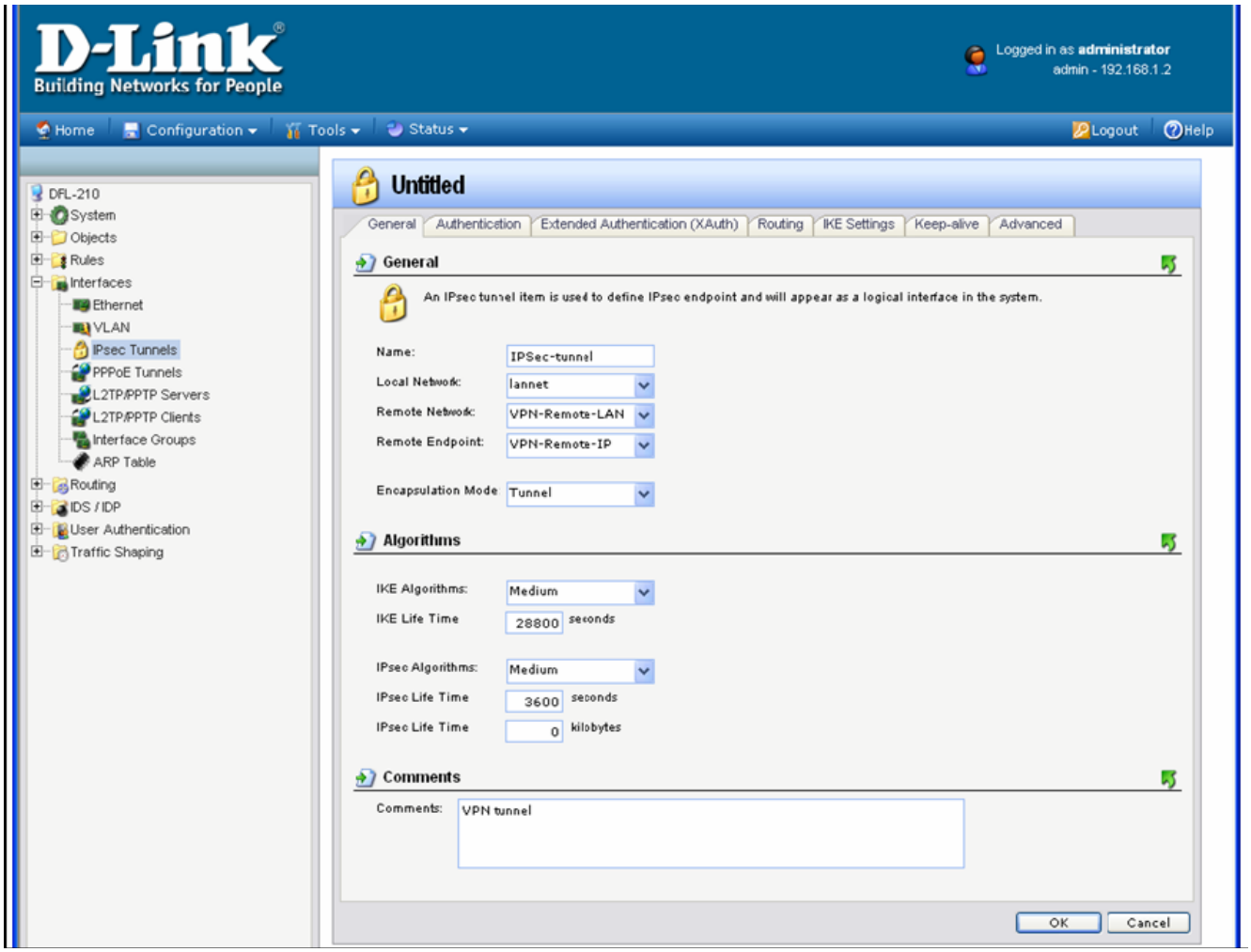
Step 5. Go to Interfaces > IPSec Tunnels. Click on Add and select IPSec Tunnel.

Enter your IPSec tunnel settings.
Under Name enter “IPSec-tunnel”.
Under Local Network select “lannet” (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**).

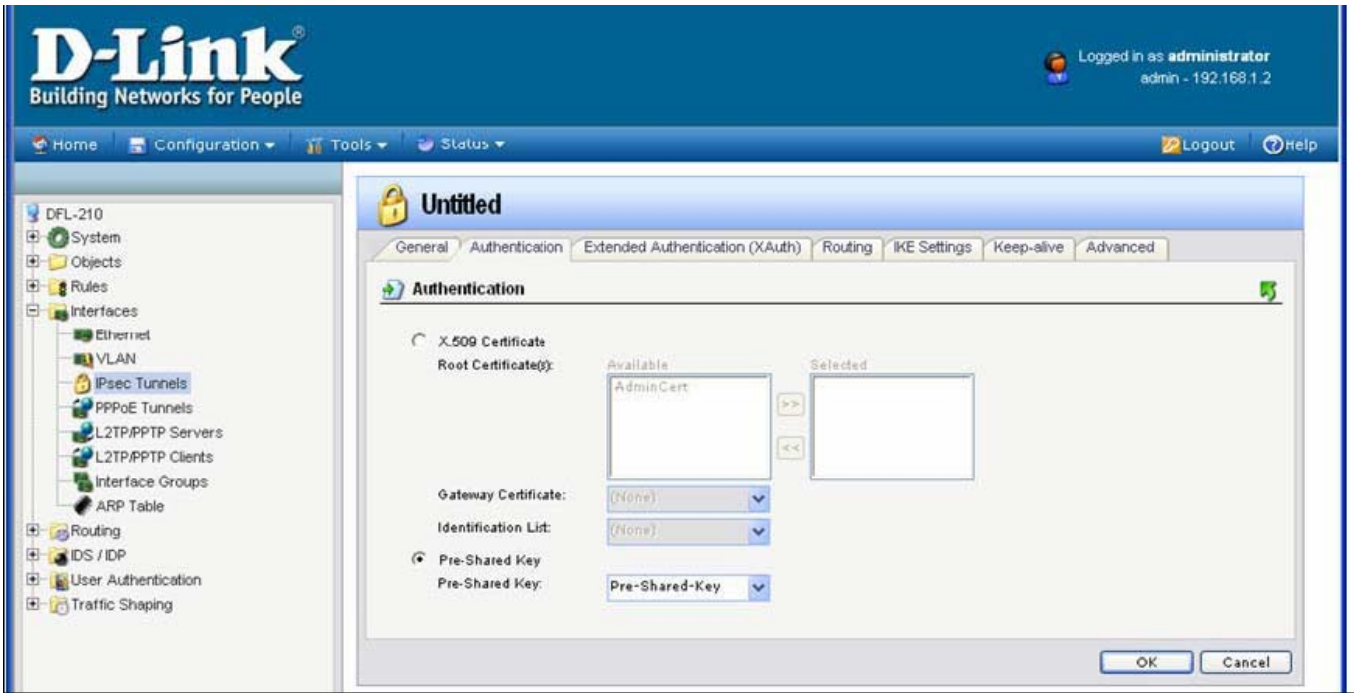
Under Remote Endpoint select “VPN-Remote-IP” (this is the public up of the remote network, see **Step 3**).
Encapsulation Mode should be set to Tunnel.

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.



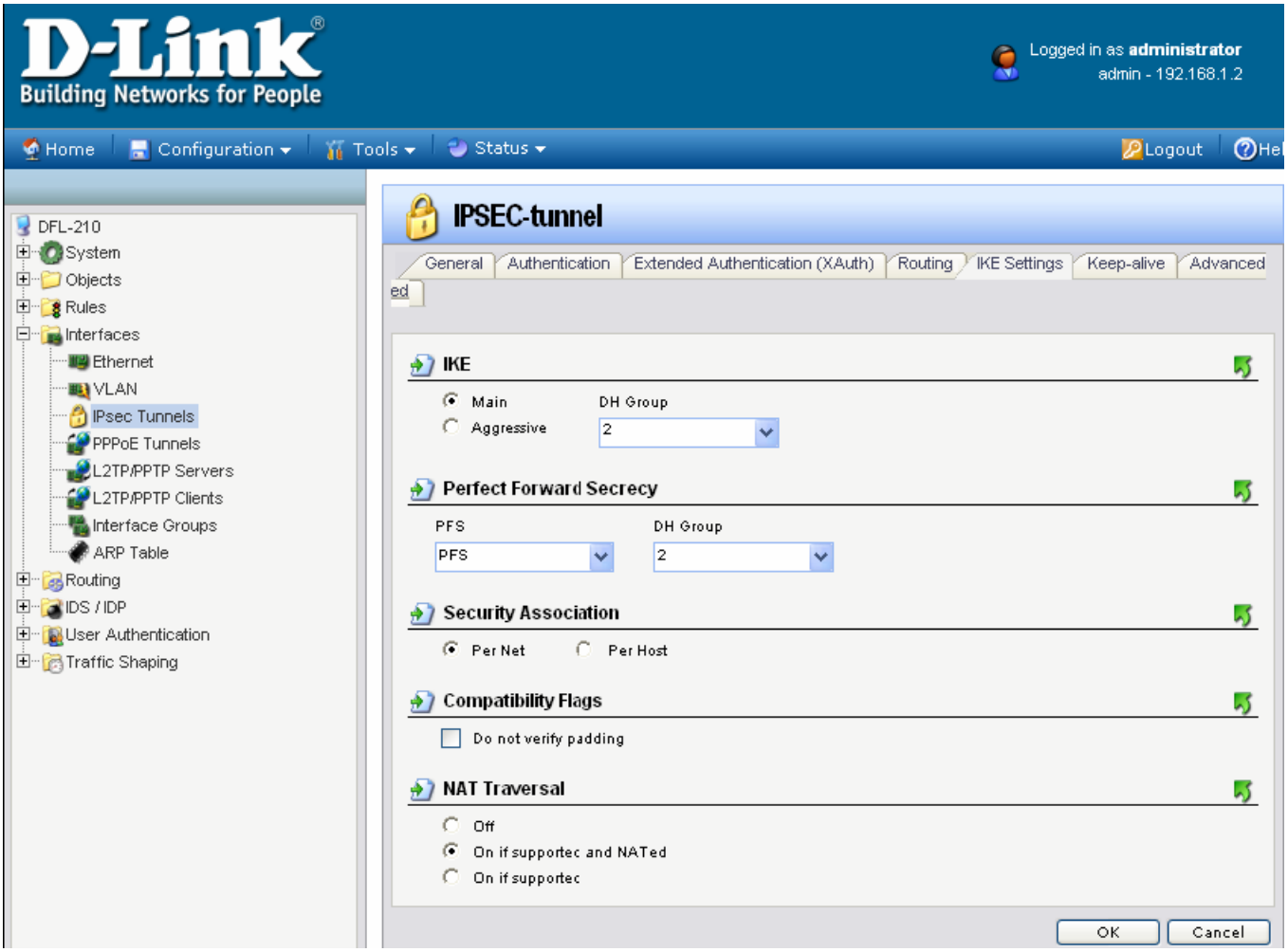
Click on Authentication tab. Make sure the Pre-Shared Key option is enabled. Select the “Pre-Shared-Key” in the dropdown menu (see **Step 4**).



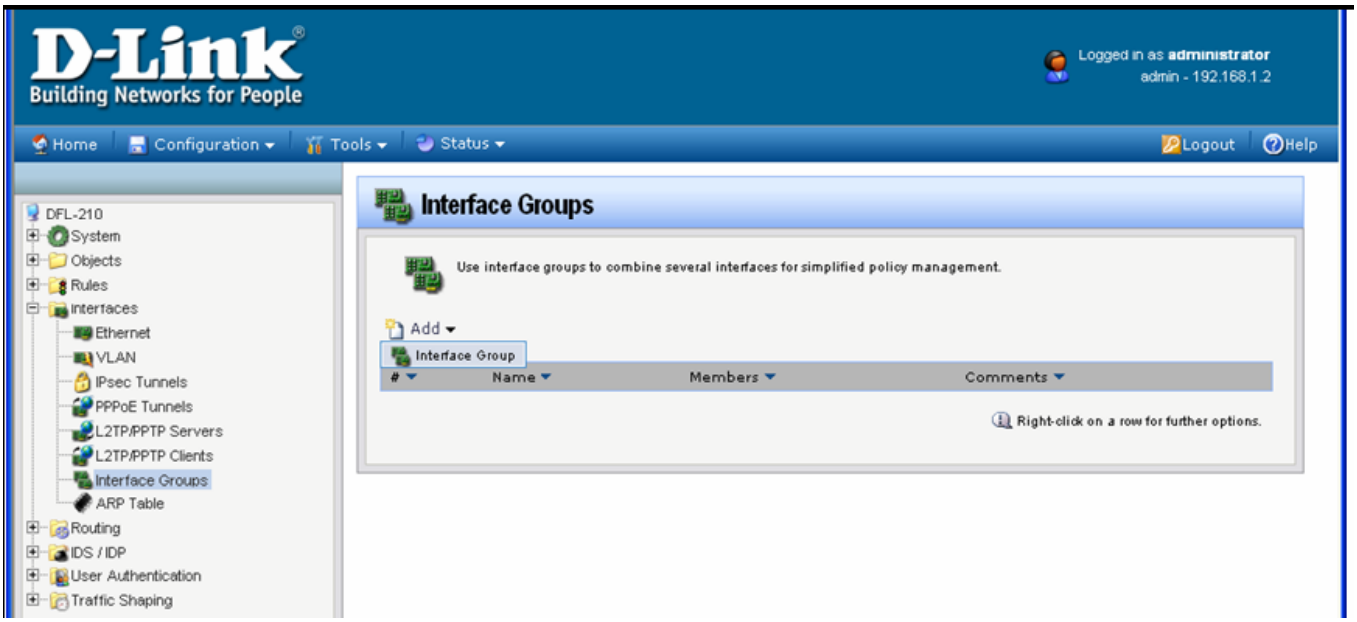
If the WAN port of the VPN firewall is set with PPPoE authentication, select Advanced tab and change the Route Metric for the IPSec Tunnel to 80.

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”.

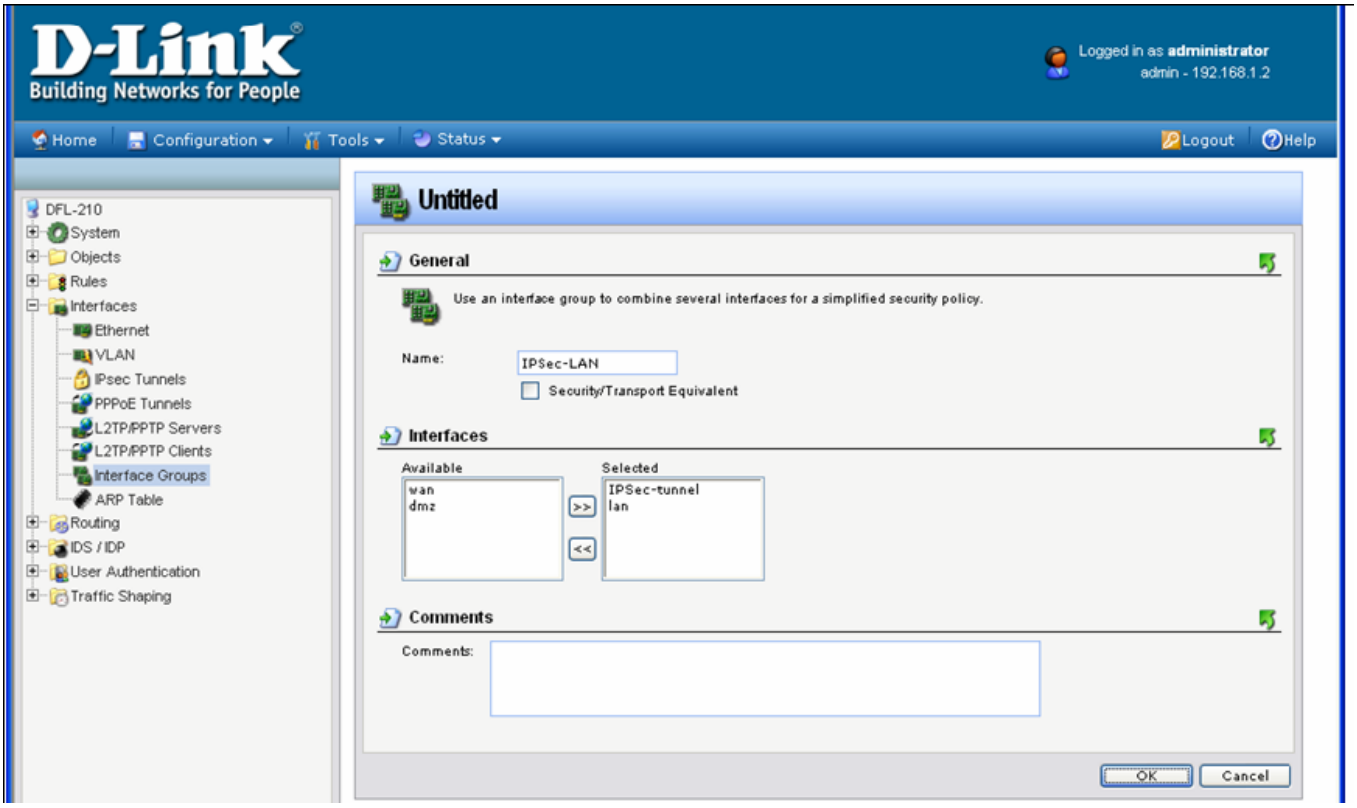
Click on the OK button.



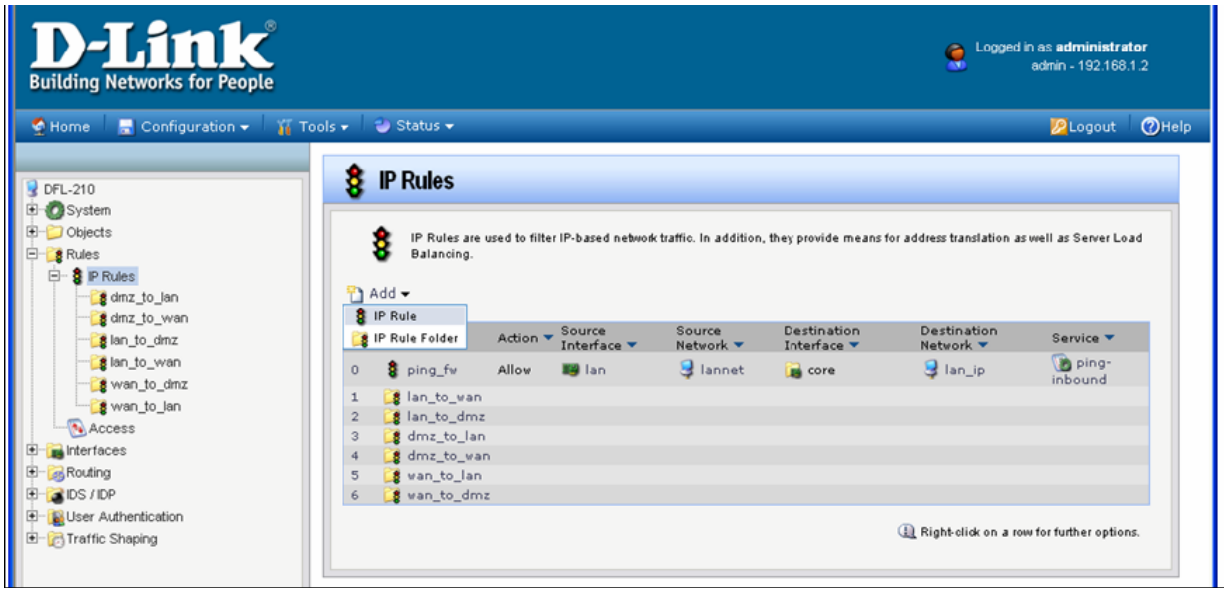
Step 6. Go to Interfaces > Interface Groups. Click on Add and select Interface Group.



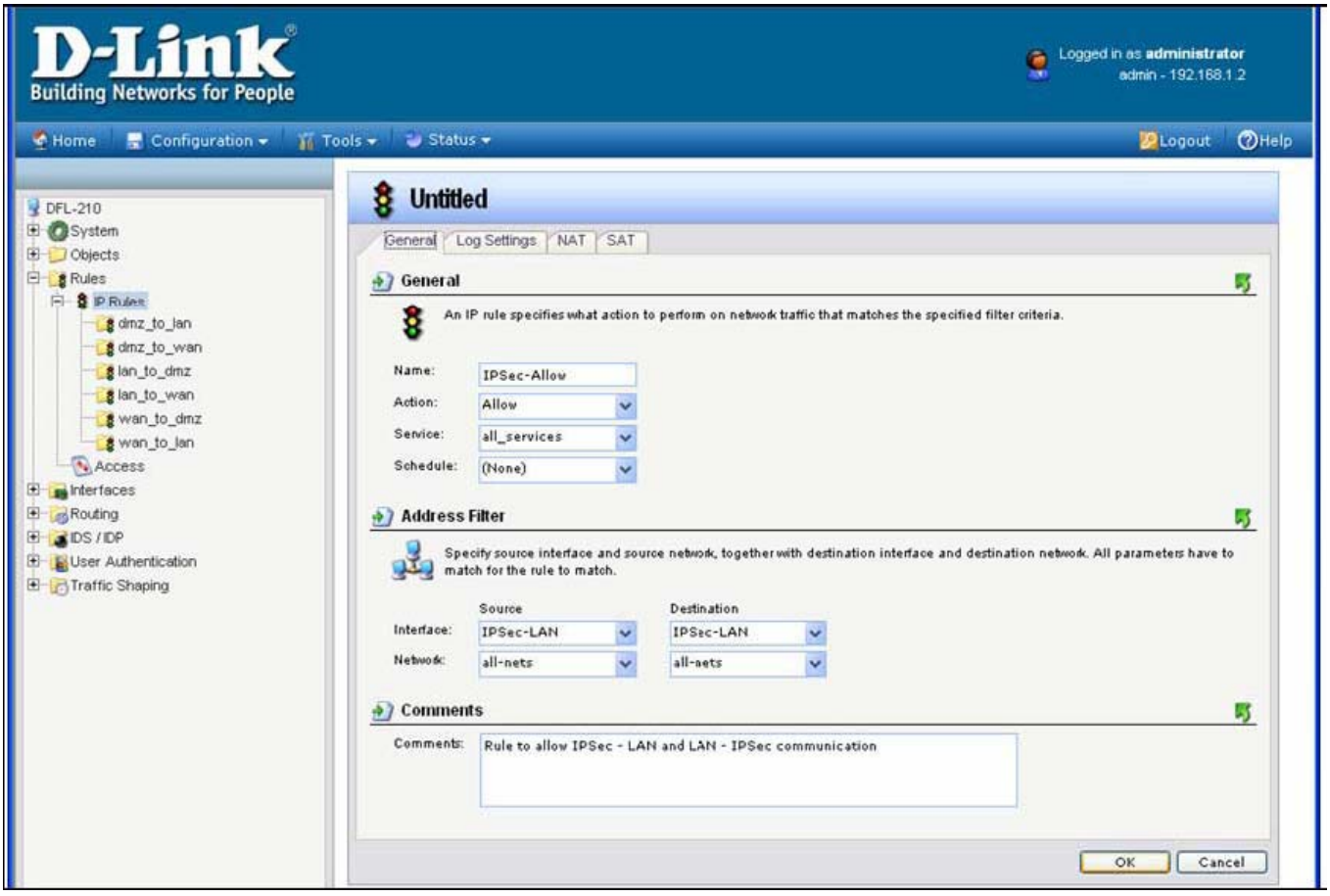
Create a group which has your IPSec tunnel and your LAN.
Under Name type IPSec-LAN.
Under Interfaces add “IPSec-tunnel” and “lan” into Selected field.
Click on the OK button.



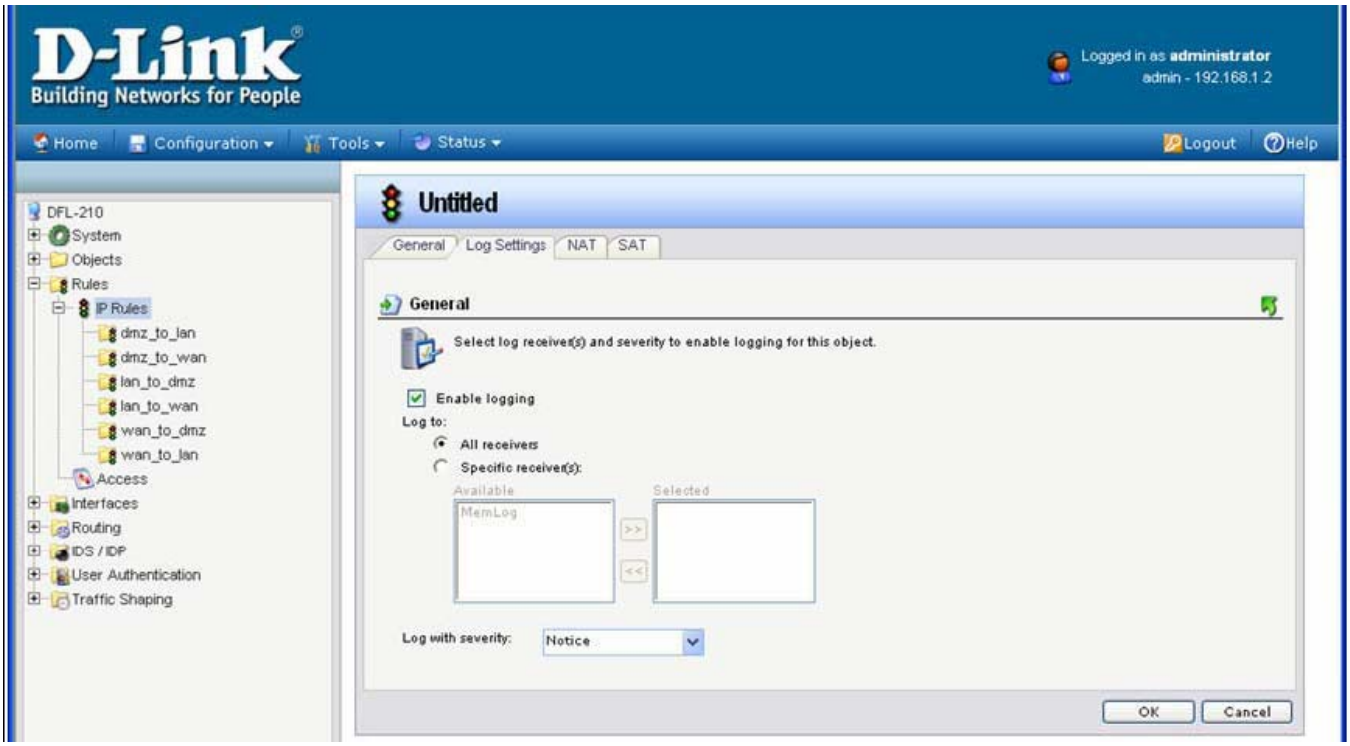
Step 7. Go to Rules > IP Rules. Click on Add and select IP Rule.



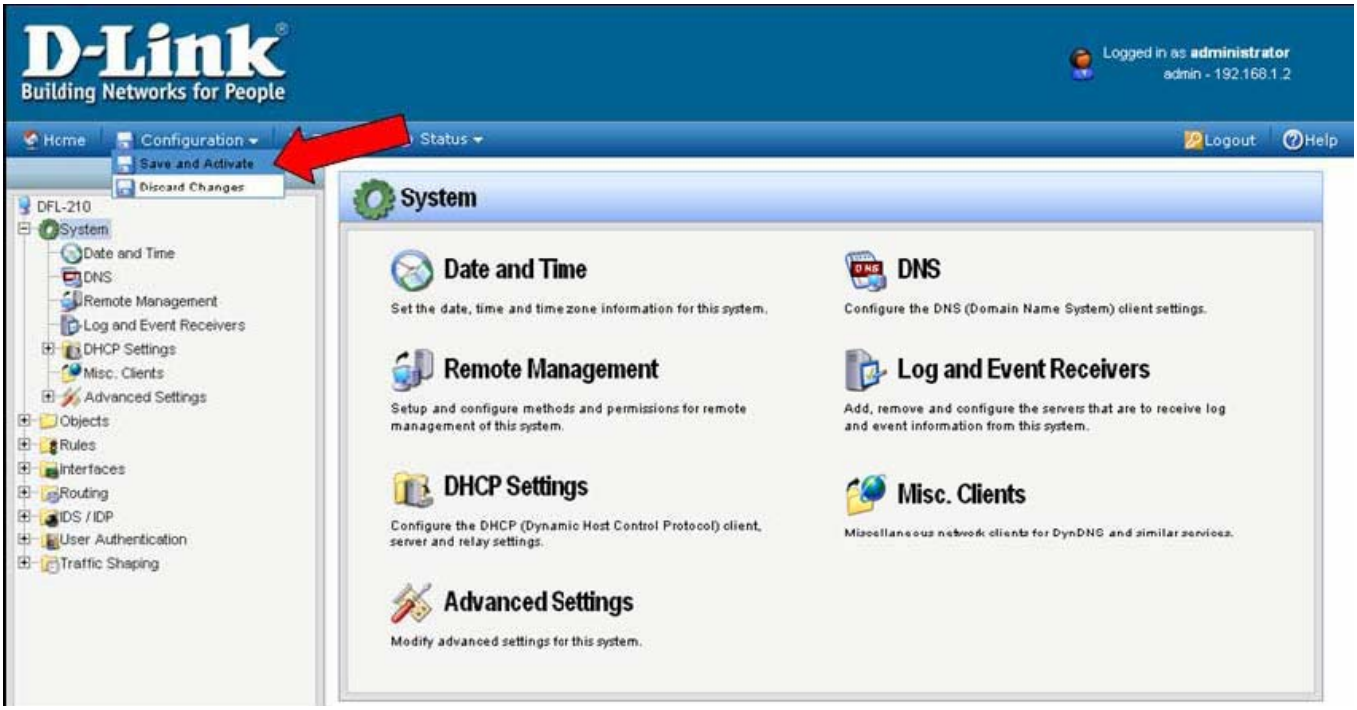
This rule will allow communication between the LAN and the IPSec tunnel.
Under Name type “IPSec-Allow”.
Under Action select “Allow”.
Under Service select “all_services”.
Under Address Filter specify the following:
Source and Destination Interfaces: “IPSec-LAN” (this is the group you created in **Step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



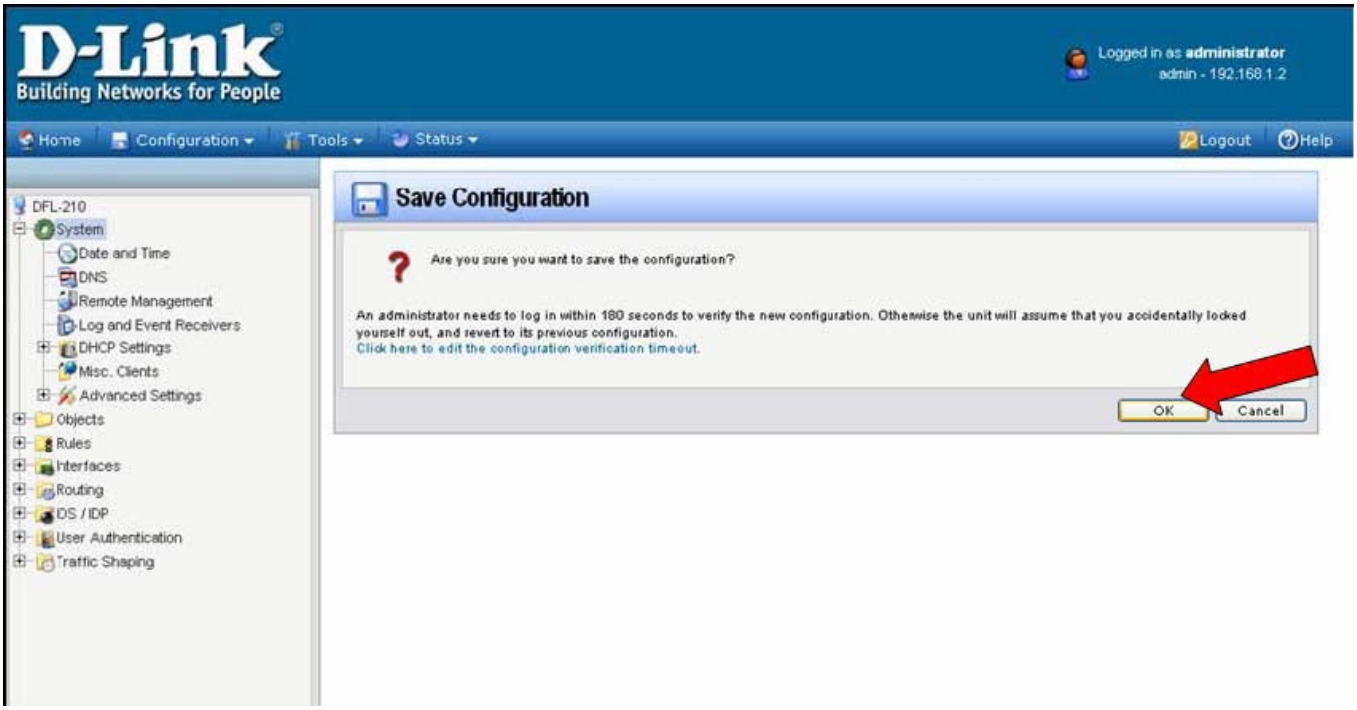
Click on Log Settings tab.
Select the Enable Logging option.
Click on the OK button when done.



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



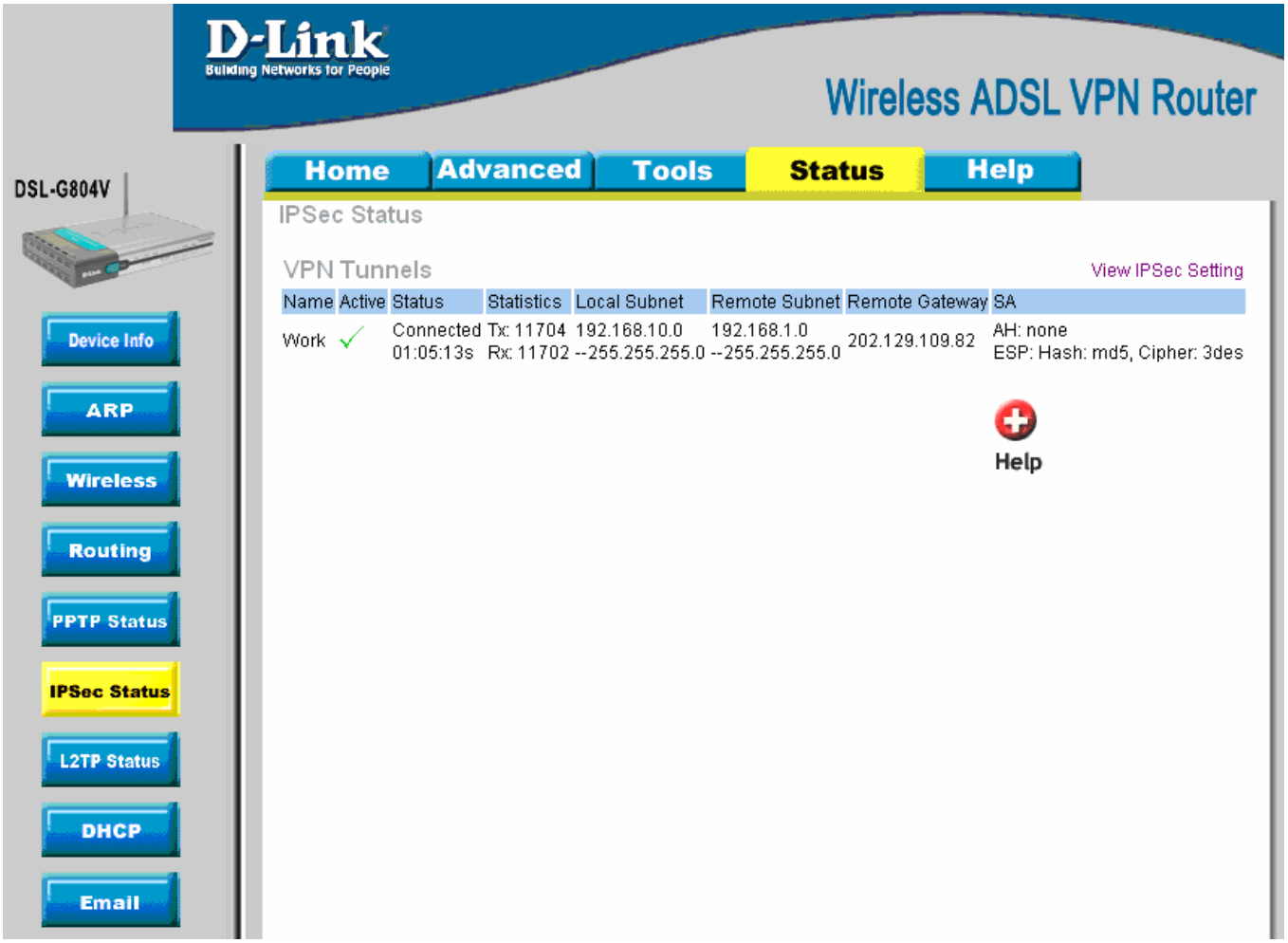
Click on OK to confirm the new settings activation:



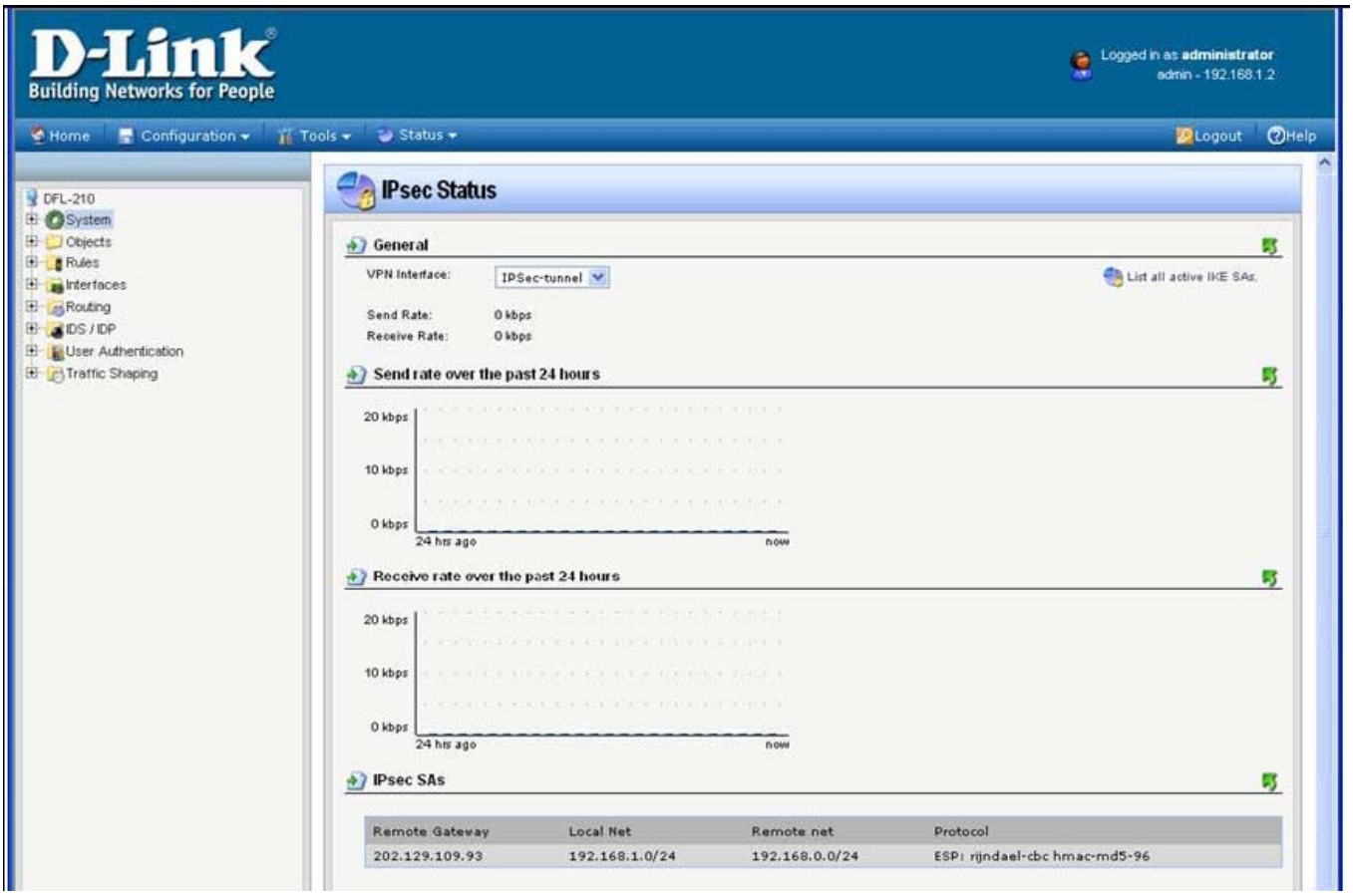
Wait 15 seconds for the Firewall to apply the new settings.

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.

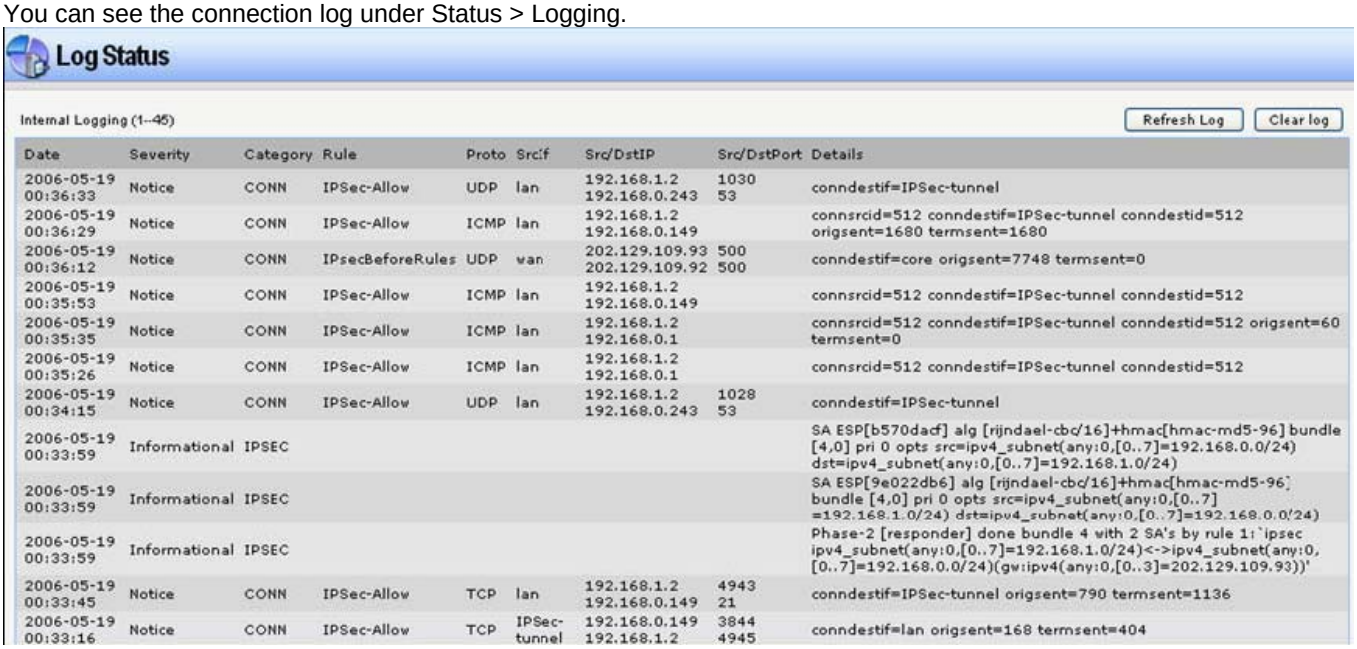


How to check VPN connection status on the DFL-210
To check the status of your VPN connection, click on Status and select IPSec. If the VPN tunnel is up, you will see an active entry under IPSec SAs.



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).

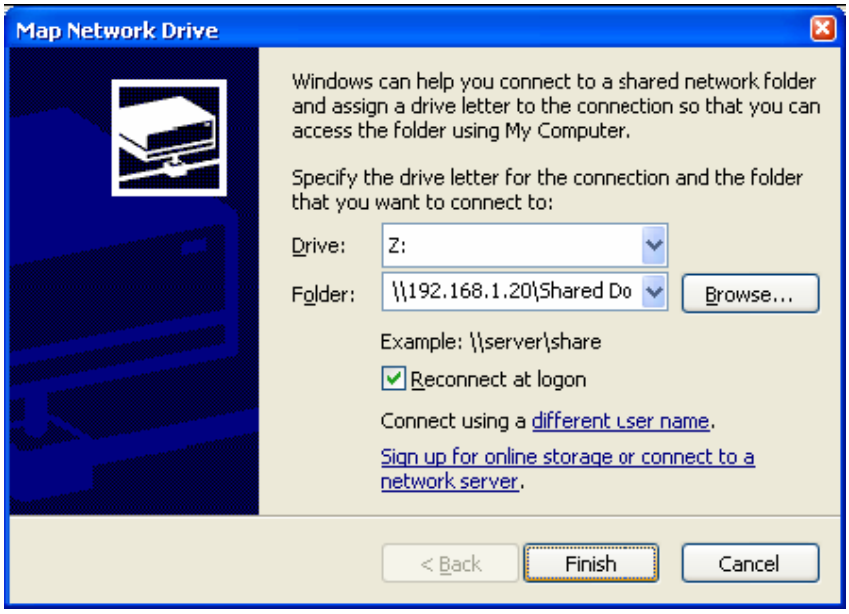
You can see the connection log under Status > Logging.



Date	Severity	Category	Rule	Proto	Src:f	Src/DstIP	Src/DstPort	Details
2006-05-19 00:36:33	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2 192.168.0.243	1030 53	conndestif=IPSec-tunnel
2006-05-19 00:36:29	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2 192.168.0.149		connsrcid=512 conndestif=IPSec-tunnel conndestid=512 origsent=1680 termsent=1680
2006-05-19 00:36:12	Notice	CONN	IPsecBeforeRules	UDP	wan	202.129.109.93 202.129.109.92	500 500	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	192.168.1.2 192.168.0.243	1028 53	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	192.168.1.2 192.168.0.149	4943 21	conndestif=IPSec-tunnel origsent=790 termsent=1136
2006-05-19 00:33:16	Notice	CONN	IPSec-Allow	TCP	IPSec-tunnel	192.168.0.149 192.168.1.2	3844 4945	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.