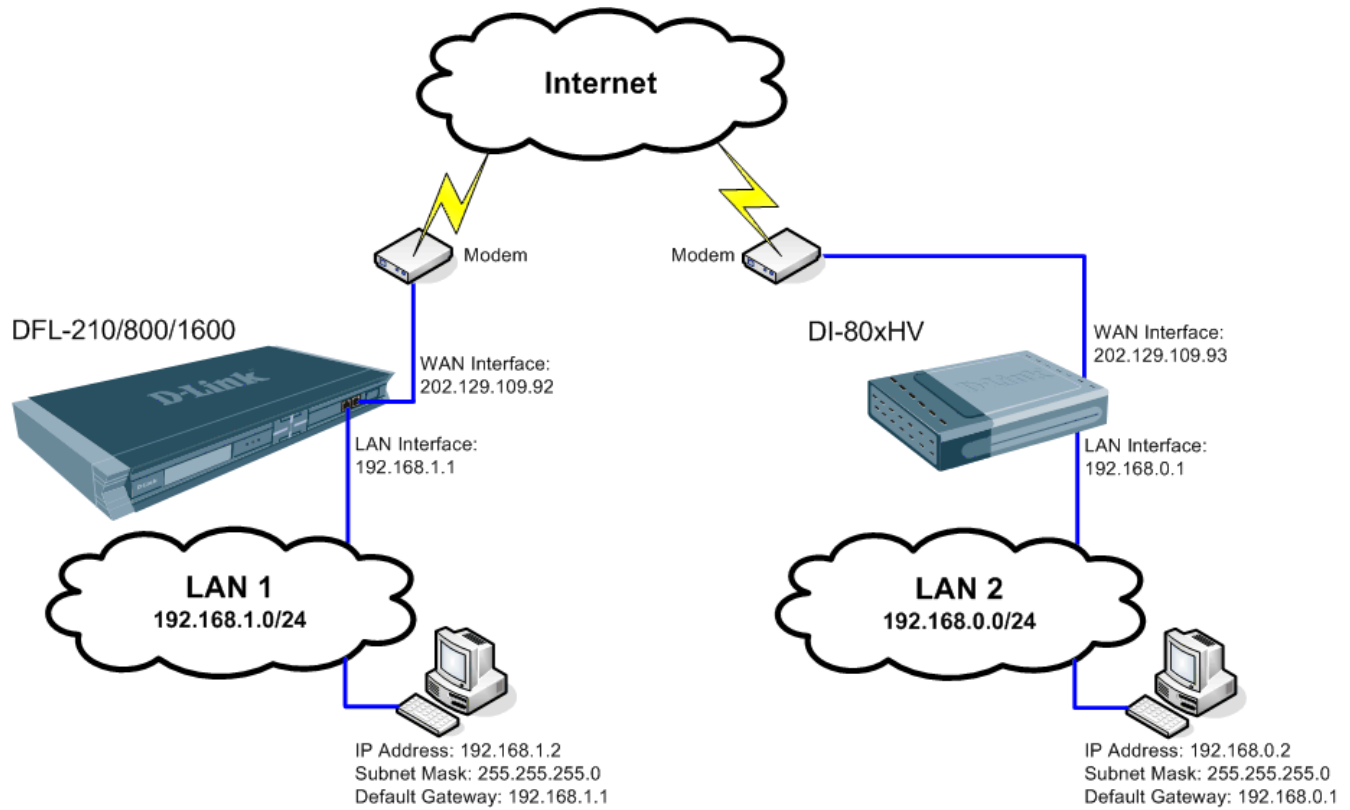


DFL-210, DFL-600, DFL-1600 How to setup IPSec VPN connection with DI-80xHV

This setup example uses the following network settings:

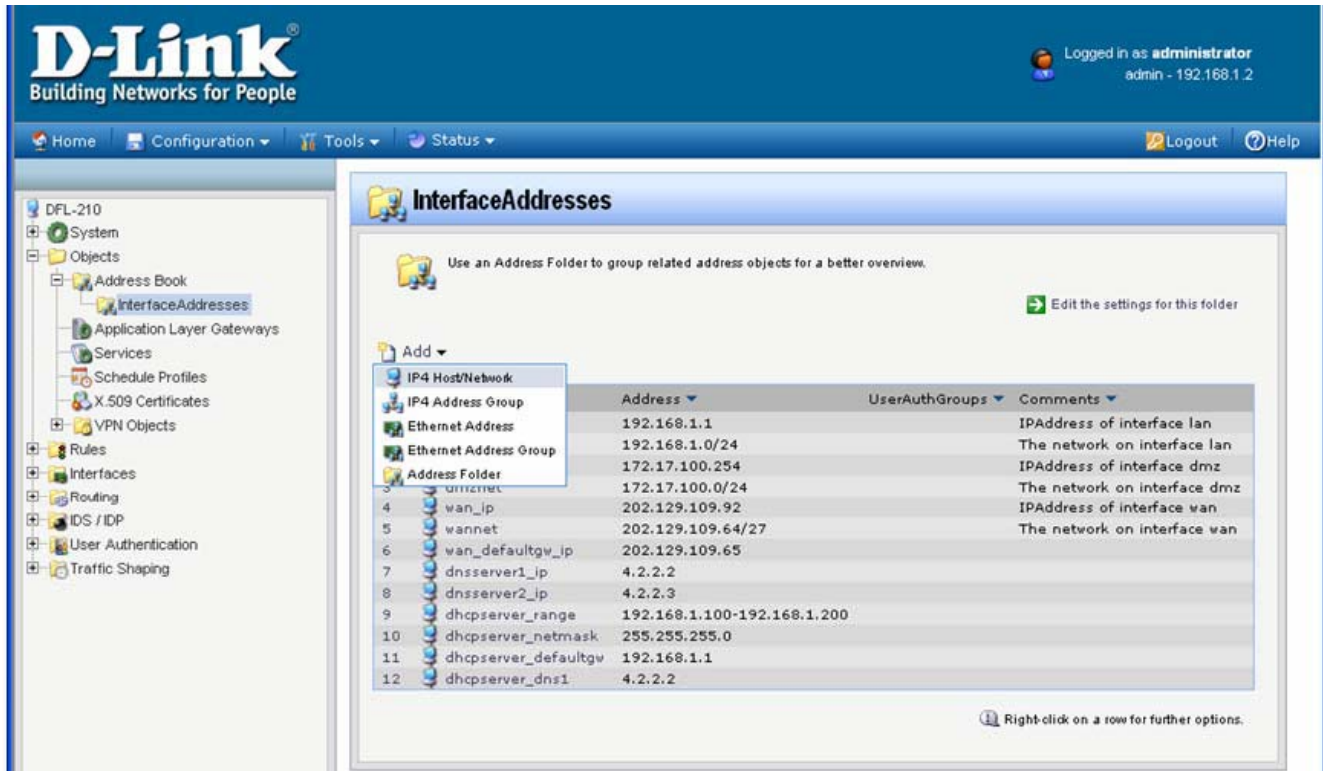


In our example the IPSec VPN tunnel is established between two LANs: 192.168.0.x and 192.168.1.x.
NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.

Configuration of the 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 configuration interface. The left sidebar contains a tree view with the following items: DFL-210, System, Objects, Address Book, InterfaceAddresses (selected), Application Layer Gateways, Services, Schedule Profiles, X.509 Certificates, VPN Objects, Rules, Interfaces, Routing, IDS / IDP, User Authentication, and Traffic Shaping. The main content area is titled 'InterfaceAddresses' and includes a sub-header: 'Use an Address Folder to group related address objects for a better overview.' Below this is an 'Add' dropdown menu with 'IP4 Host/Network' selected. A table lists existing address objects:

	Address	UserAuthGroups	Comments
1	192.168.1.1		IPAddress of interface lan
2	192.168.1.0/24		The network on interface lan
3	172.17.100.254		IPAddress of interface dmz
4	172.17.100.0/24		The network on interface dmz
5	202.129.109.92		IPAddress of interface wan
6	202.129.109.64/27		The network on interface wan
7	202.129.109.65		
8	4.2.2.2		
9	4.2.2.3		
10	192.168.1.100-192.168.1.200		
11	255.255.255.0		
12	192.168.1.1		
13	4.2.2.2		

At the bottom right of the table area, there is a note: 'Right-click on a row for further options.'

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 192.168.0.0/24.

Click on the OK button.

The screenshot displays the D-Link web management interface for a device named DFL-210. The user is logged in as administrator. The left sidebar shows a tree view of configuration objects, with 'VPN Objects' expanded. The main area shows the configuration for an 'Untitled' object, with the 'General' tab selected. The 'General' section includes a 'Name' field with the value 'VPN-Remote-LAN' and an 'IP Address' field with the value '192.168.0.0/24'. Below these fields is a 'Comments' section with a text area containing the text 'Remote VPN LAN'. At the bottom right of the configuration window are 'OK' and 'Cancel' buttons.

D-Link
Building Networks for People

Logged in as administrator
admin - 192.168.1.2

Home Configuration Tools Status Logout Help

DFL-210
System
Objects
Address Book
InterfaceAddresses
Application Layer Gateways
Services
Schedule Profiles
X.509 Certificates
VPN Objects
Rules
Interfaces
Routing
IDS / IDP
User Authentication
Traffic Shaping

Untitled

General User Authentication

General

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: VPN-Remote-LAN

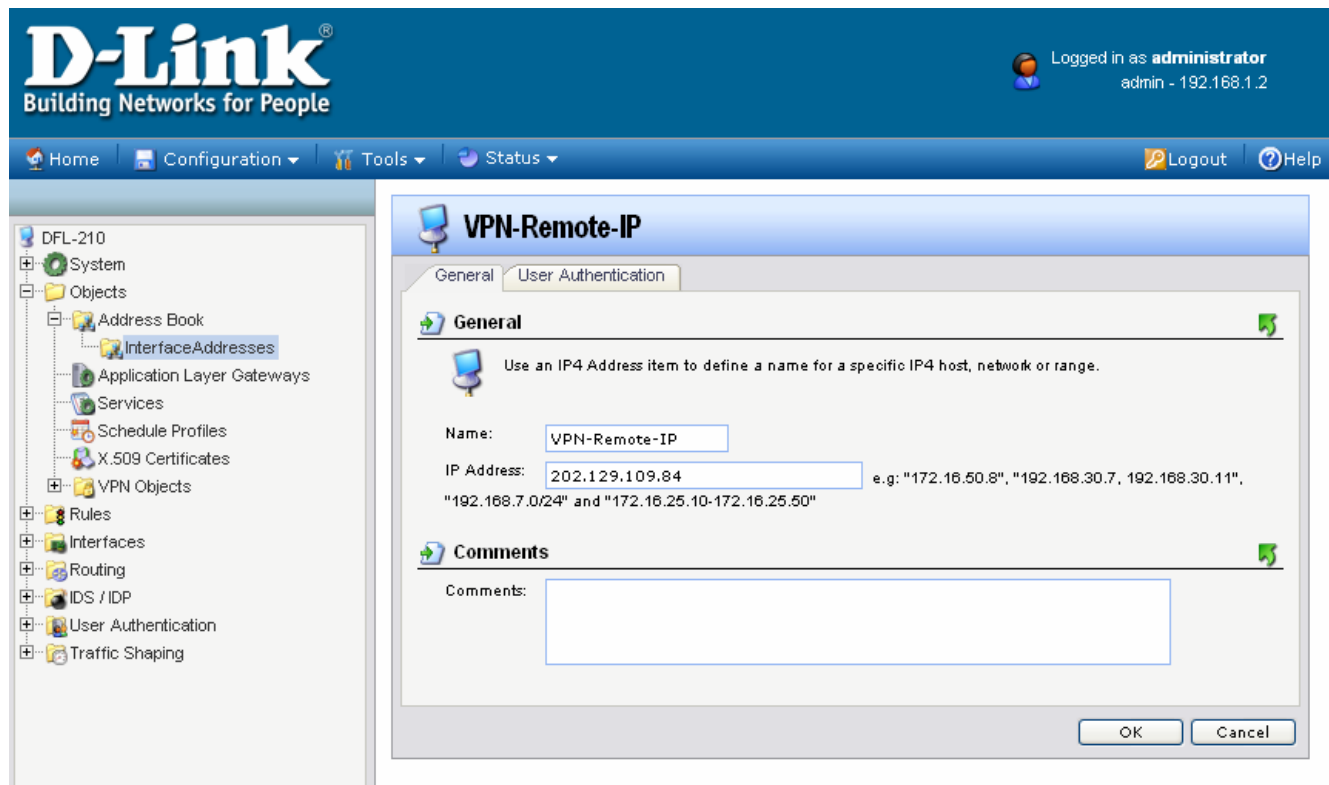
IP Address: 192.168.0.0/24 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

Comments: Remote VPN LAN

OK Cancel

Step 3. Add another "IP4 Host/Network". Enter the settings of the VPN endpoint, the public IP address of LAN 2. Under Name enter "VPN-Remote-IP". Under IP address specify the public IP address of the remote network (the IP address assigned 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.

The screenshot displays the D-Link web management interface for a device labeled 'DFL-210'. The top navigation bar includes 'Home', 'Configuration', 'Tools', and 'Status' menus, along with a 'Logout' button and a 'Help' icon. The user is logged in as 'administrator' with IP address '192.168.1.2'. The left sidebar shows a tree view of configuration categories, with 'VPN Objects' > 'Pre-Shared Keys' selected. The main content area is titled 'Pre-Shared Keys' and contains the following text: 'Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.' Below this text is an 'Add' dropdown menu with 'Pre-Shared Key' selected. A table with the following structure is visible:

#	Name	Type	Comments

A note at the bottom right of the table area reads: 'Right-click on a row for further options.'

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 DI-80xHV on the other end of the tunnel.

Click OK when done.

The screenshot shows the D-Link web management interface for a device named DFL-210. The user is logged in as administrator. The navigation menu on the left includes System, Objects, Rules, Interfaces, Routing, and User Authentication. The 'Objects' menu is expanded to show 'VPN Objects', with 'Pre-Shared Keys' selected. The main content area is titled 'Untitled' and contains the following configuration sections:

- General:** A key icon and text stating 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' The 'Name' field is set to 'Pre-Shared-Key'.
- Shared Secret:** Two radio buttons are present: 'Passphrase' (selected) and 'Hexadecimal Key'. Under 'Passphrase', there are two input fields for 'Shared Secret' and 'Confirm Secret', both containing seven asterisks. A 'Generate Random Key' button is located below the 'Passphrase' section. A warning icon and text state: 'Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.'
- Comments:** A text area containing the comment 'Pre-shared key for VPN connection'.

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

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

The screenshot shows the D-Link web management interface for a device (DFL-210). 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 configuration categories, with 'Interfaces' expanded and 'IPsec Tunnels' selected. The main content area is titled 'IPsec Tunnels' and contains the following text: 'Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.' Below this is an 'Add' button with a dropdown menu that has 'IPsec Tunnel' selected. A table with the following columns is visible: '#', 'Name', 'LocalNetwork', 'RemoteNetwork', 'RemoteEndpoint', 'AuthMethod', and 'Comments'. Below the table, there are instructions: 'Right-click on a row for further options.' and 'Modify advanced settings'.

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**).

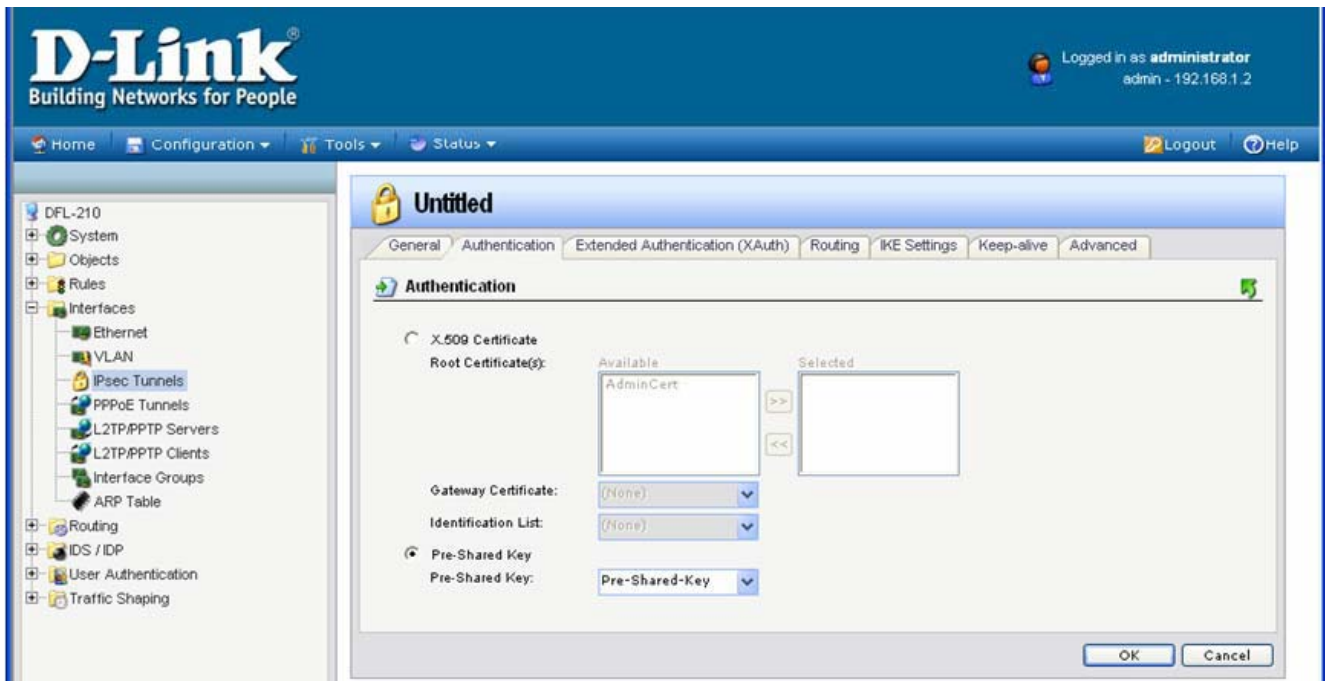
Under Remote Endpoint select "VPN-Remote-IP" (this is the public up of the remote network, see **Step 3**).

Encapsulation Mode should be set to Tunnel.

Under Algorithms 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.

The screenshot displays the D-Link web management interface for a device named 'DFL-210'. The user is logged in as 'administrator' with IP address '192.168.1.2'. The interface shows a navigation menu on the left with categories like System, Objects, Rules, Interfaces, Routing, and Traffic Shaping. The 'Interfaces' category is expanded, showing 'IPsec Tunnels' selected. The main content area is titled 'Untitled' and contains the configuration for a new IPsec tunnel. The 'General' tab is active, showing the following settings: Name: 'IPSec-tunnel', Local Network: 'lannet', Remote Network: 'VPN-Remote-LAN', Remote Endpoint: 'VPN-Remote-IP', and Encapsulation Mode: 'Tunnel'. The 'Algorithms' section is also visible, with IKE Algorithms set to 'Medium' (28800 seconds) and IPsec Algorithms set to 'Medium' (3600 seconds, 0 kilobytes). A 'Comments' field contains the text 'VPN tunnel'. 'OK' and 'Cancel' buttons are at the bottom right.

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**).

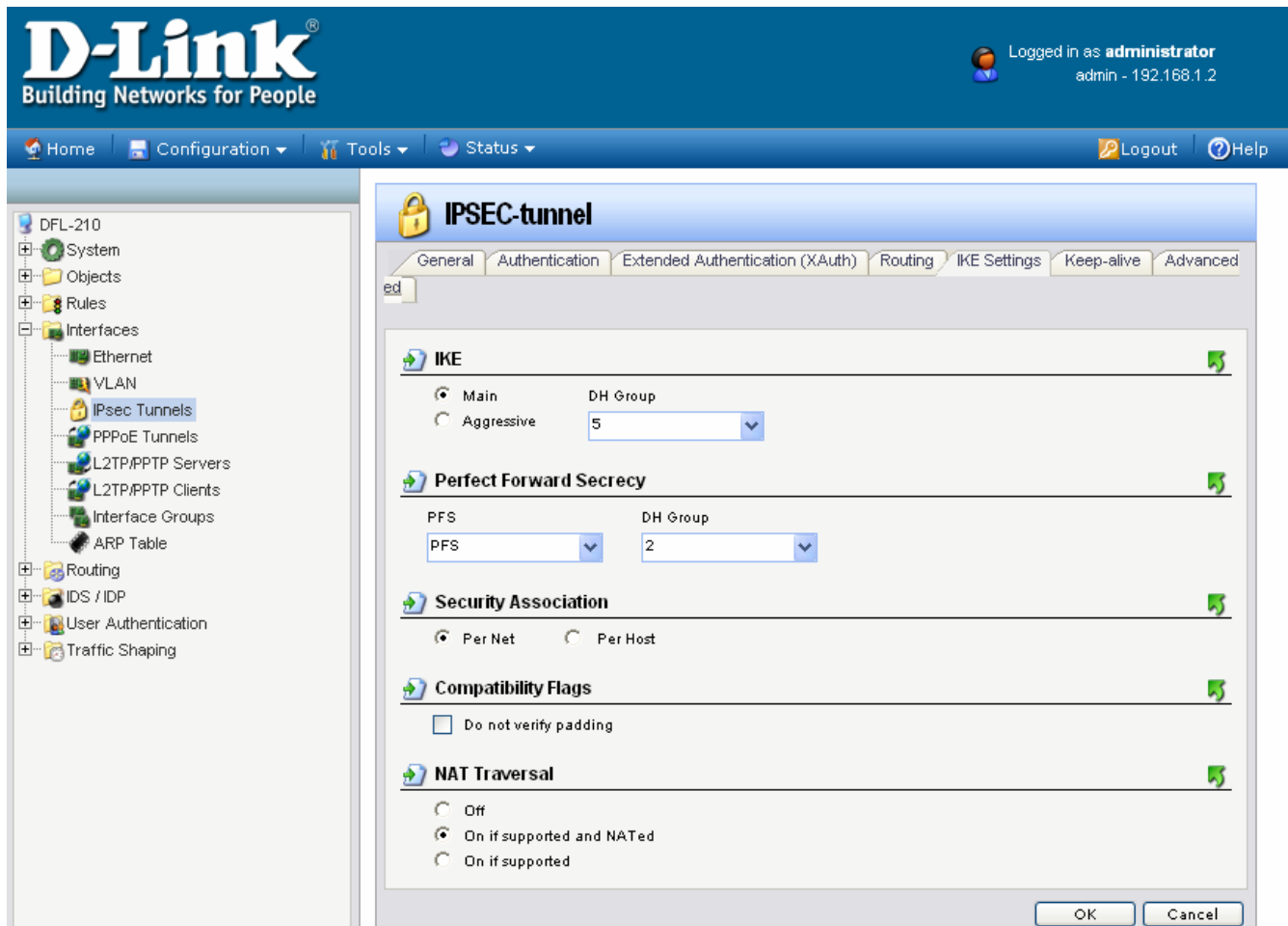


If the WAN port of the firewall is set with PPPoE authentication, select Advanced tab and change the Route Metric for the IPsec Tunnel to 80.



Click on IKE Settings tab. Under IKE change the DH Group to "5", Under Perfect Forward Secrecy select "PFS" from the drop down box and make sure the DH Group is "2".

Click on the OK button.



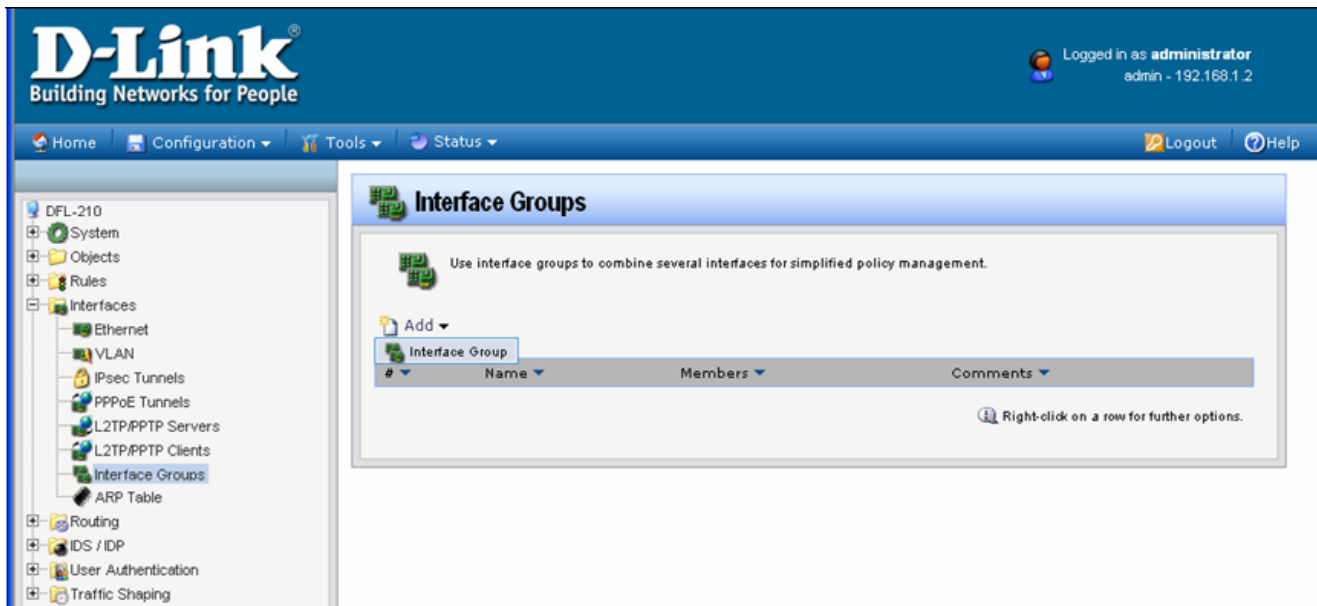
The screenshot displays the D-Link web management interface for configuring an IPSEC-tunnel. The interface includes a navigation menu on the left and a main configuration area on the right. The main area is titled "IPSEC-tunnel" and has several tabs: General, Authentication, Extended Authentication (XAuth), Routing, IKE Settings, Keep-alive, and Advanced. The "IKE Settings" tab is currently selected.

The configuration options are as follows:

- IKE:** Radio buttons for "Main" (selected) and "Aggressive". The "DH Group" dropdown menu is set to "5".
- Perfect Forward Secrecy:** A dropdown menu for "PFS" is set to "PFS". The "DH Group" dropdown menu 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 supported and NATed" (selected), and "On if supported".

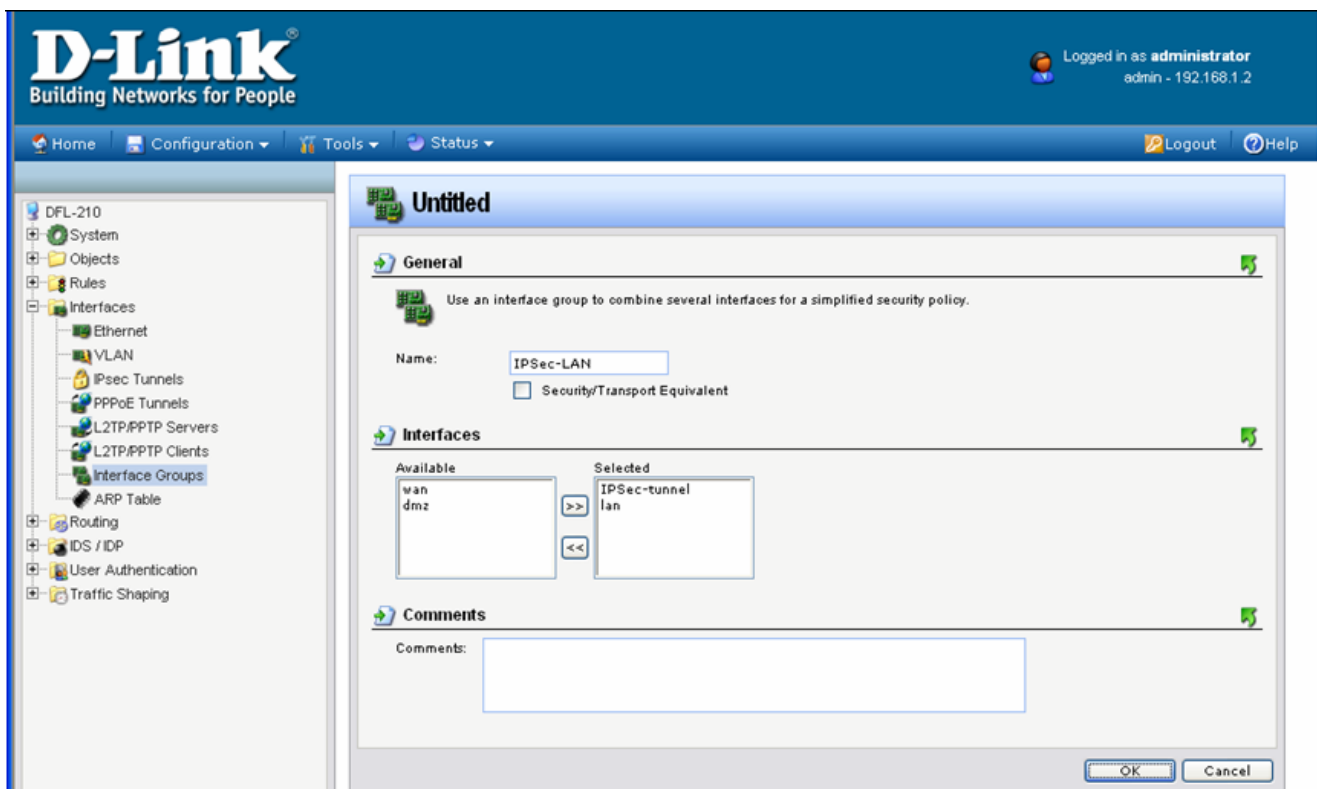
At the bottom right of the configuration area, there are "OK" and "Cancel" buttons.

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

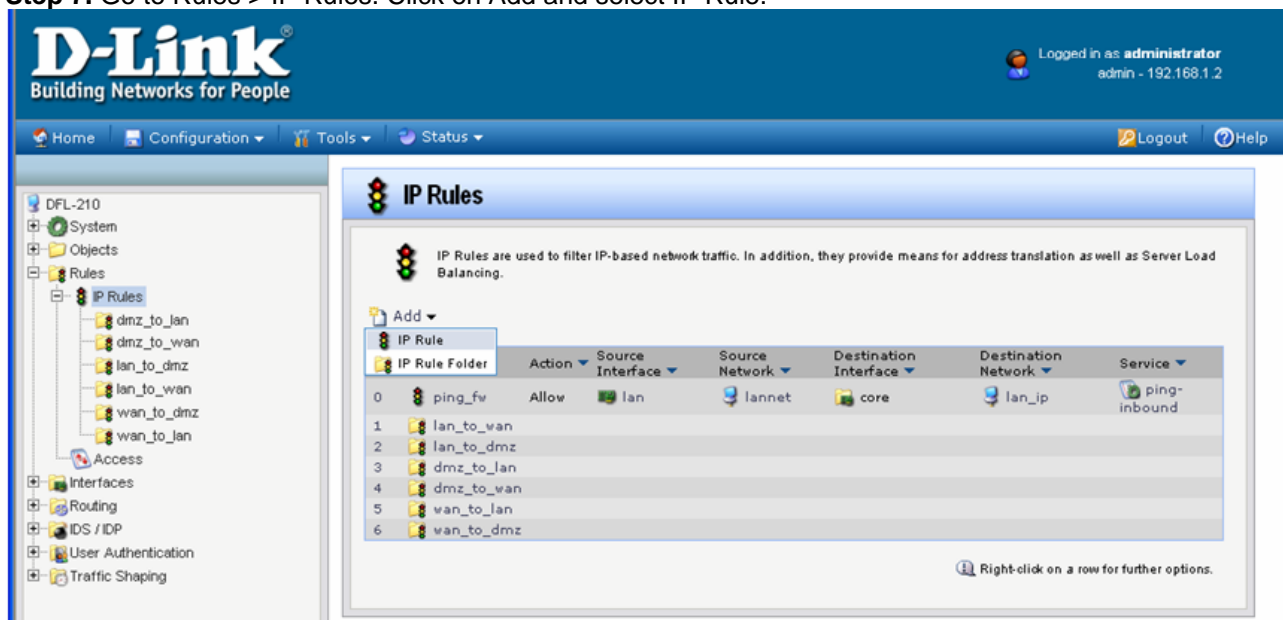


Create a group which has your IPsec tunnel and your LAN.
Under Name type IPsec-LAN.
Under Interfaces add "IPsec-tunnel" and "lan" into Selected field.

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".

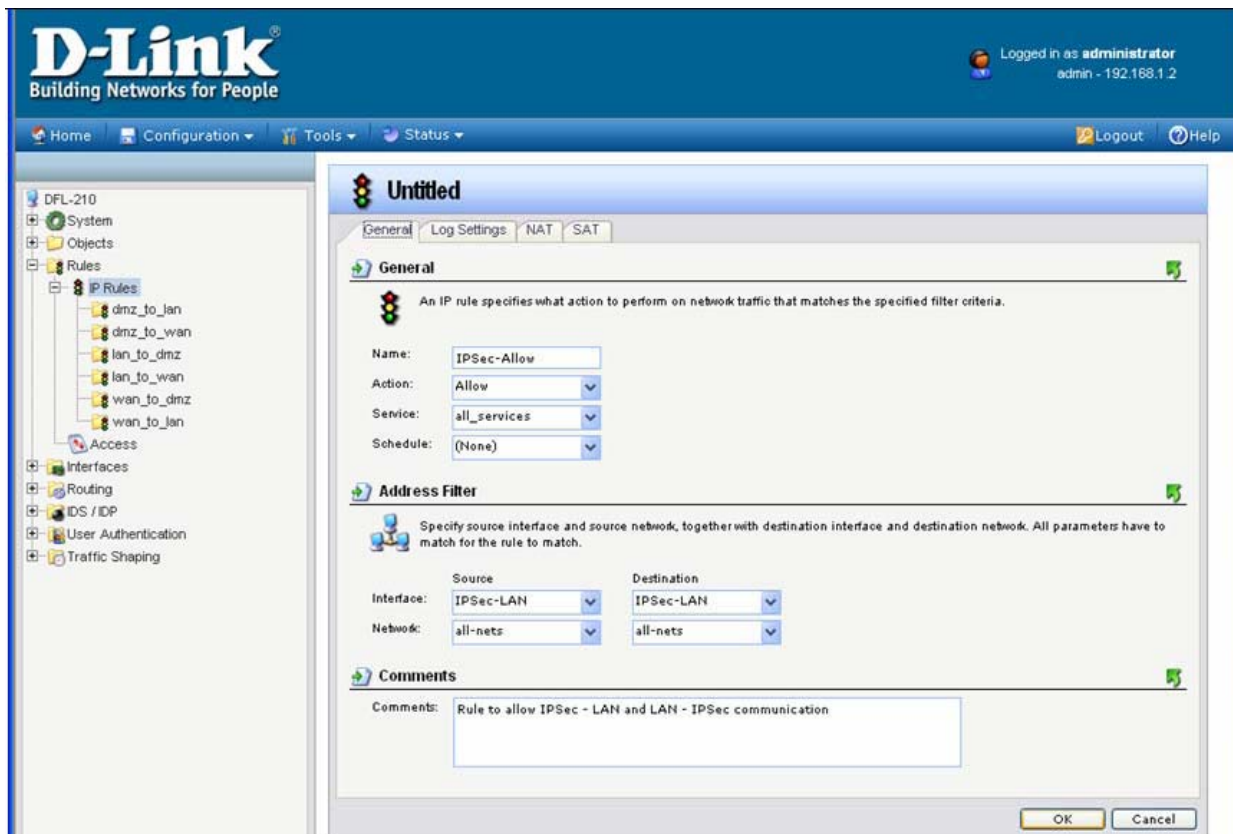
Under Action select "Allow".

Under Service select "all_services".

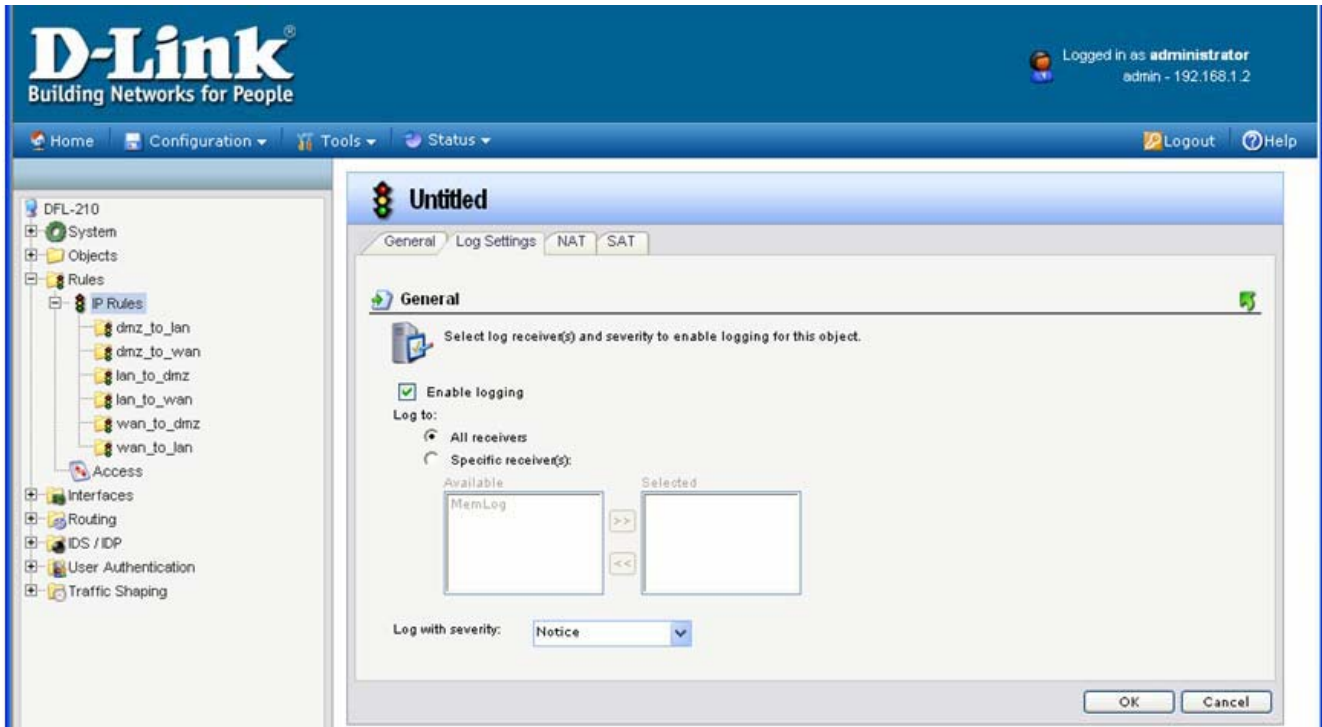
Under Address Filter specify the following:

Source and Destination Interfaces: "IPsec-LAN" (this is the group you created in Step 6).

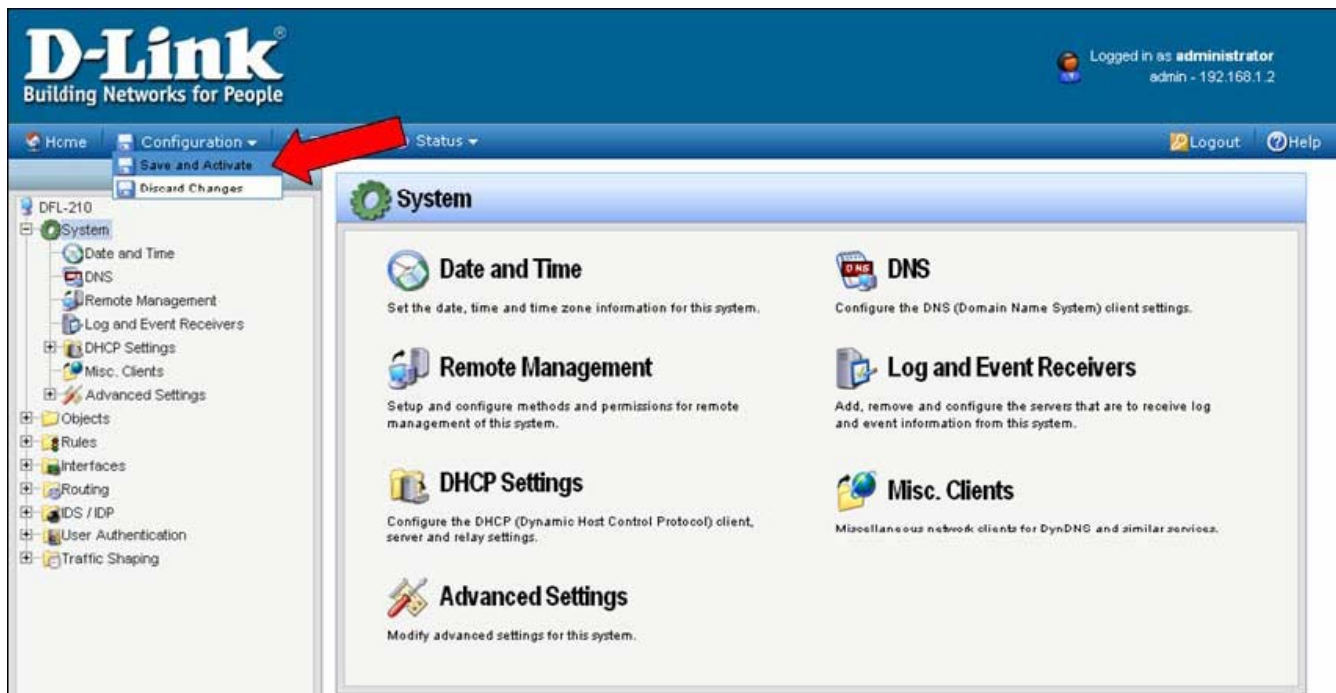
Source and Destination Network: select "all-nets".



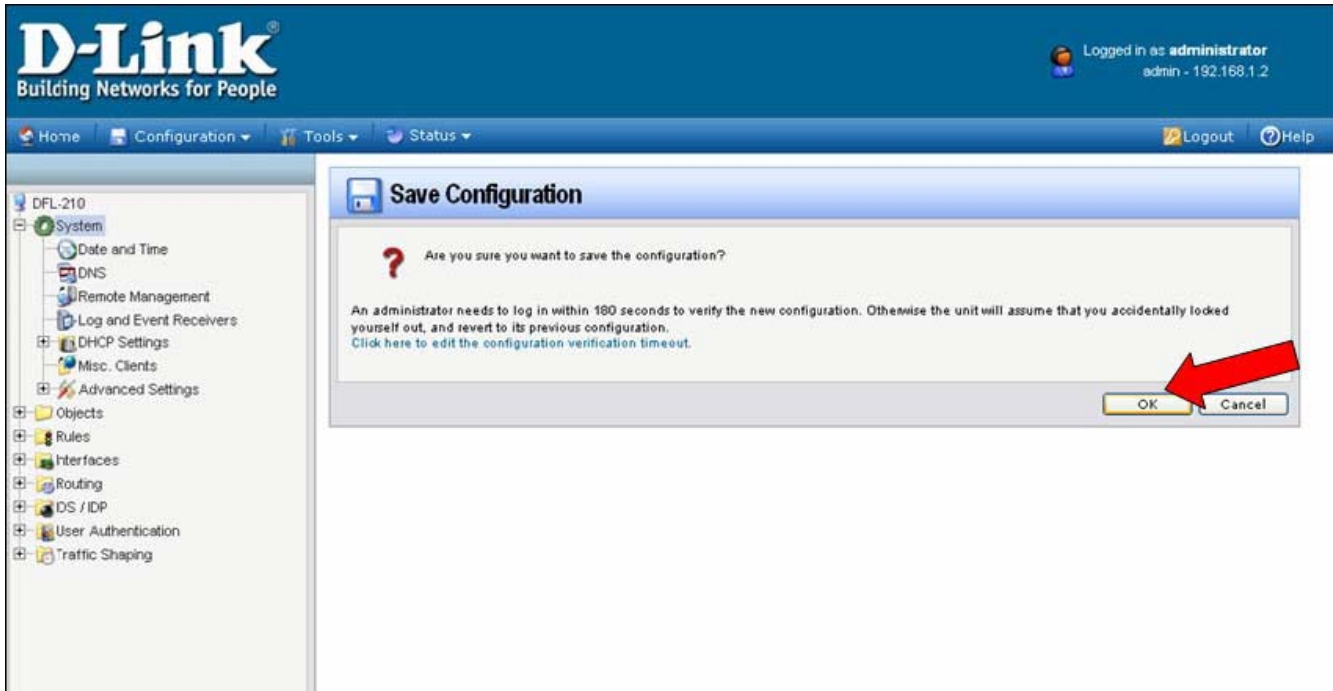
Click on Log Settings tab.
Select the Enable Logging option.
Click on the OK button when done.



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.

Configuration of the DI-80xHV router on LAN 2

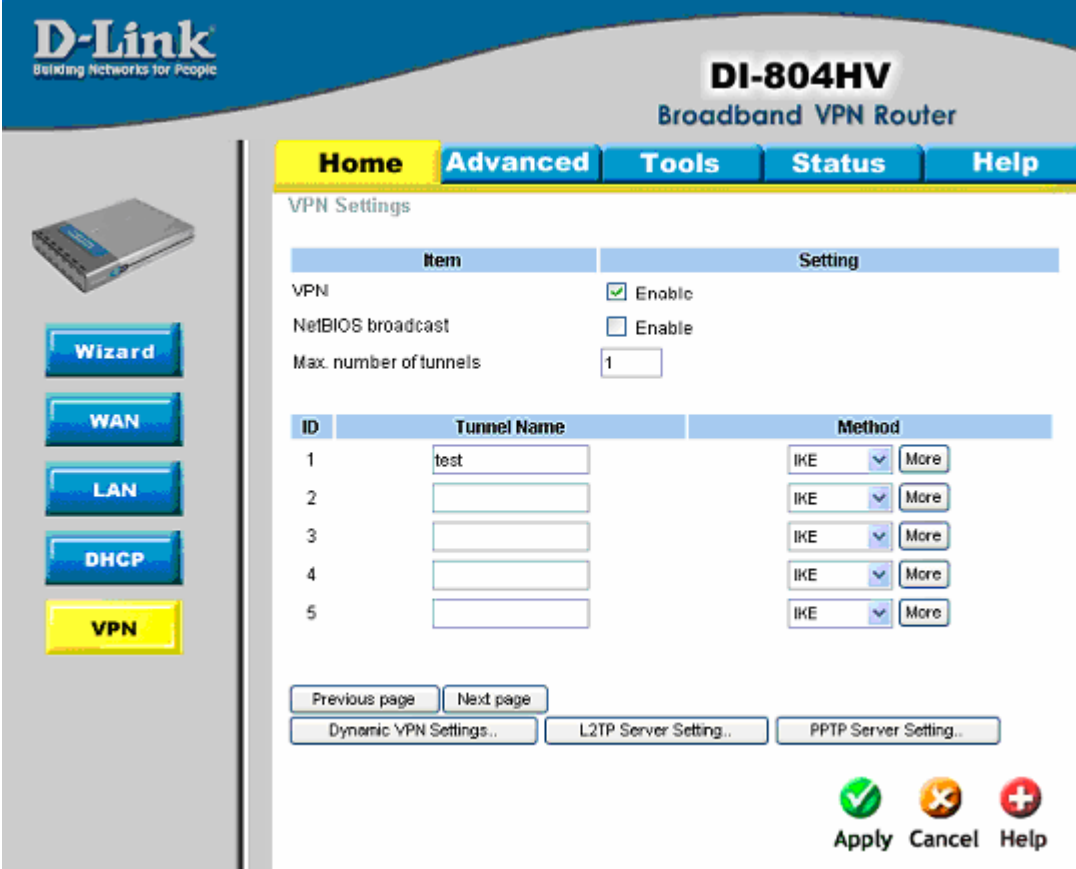
The steps to configure the second firewall will be almost identical to the steps for the firewall on the LAN 1. The only exception is the "Remote Network" and the "Remote Endpoint" settings. Note that the subnets on each LAN connecting through VPN should be different.

Login into the DI-80xHV configuration page, then go into Home > VPN.

Make sure you have VPN Enable box ticked.

Type in a name for the Tunnel Name, something related to the VPN connection would be a good idea, e.g. *Office, Home* etc...

Then click on "More" button to the right of the ID "1"



The screenshot shows the configuration interface for a D-Link DI-804HV Broadband VPN Router. The page has a blue header with the D-Link logo and the model name. A navigation bar includes tabs for Home, Advanced, Tools, Status, and Help. On the left, there is a sidebar with buttons for Wizard, WAN, LAN, DHCP, and VPN (highlighted in yellow). The main content area is titled "VPN Settings" and contains a table with columns "Item" and "Setting". Below this is a table with columns "ID", "Tunnel Name", and "Method". At the bottom, there are buttons for "Previous page", "Next page", "Dynamic VPN Settings..", "L2TP Server Setting..", and "PPTP Server Setting..". At the very bottom, there are three icons: a green checkmark for "Apply", an orange 'X' for "Cancel", and a red plus sign for "Help".

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	<input type="text" value="1"/>

ID	Tunnel Name	Method
1	<input type="text" value="test"/>	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>

Previous page Next page

Dynamic VPN Settings.. L2TP Server Setting.. PPTP Server Setting..

If the remote location does not have a static IP address please use **Dynamic VPN Settings** instead of the More button.

On the Tunnel 1 page enter the required information:

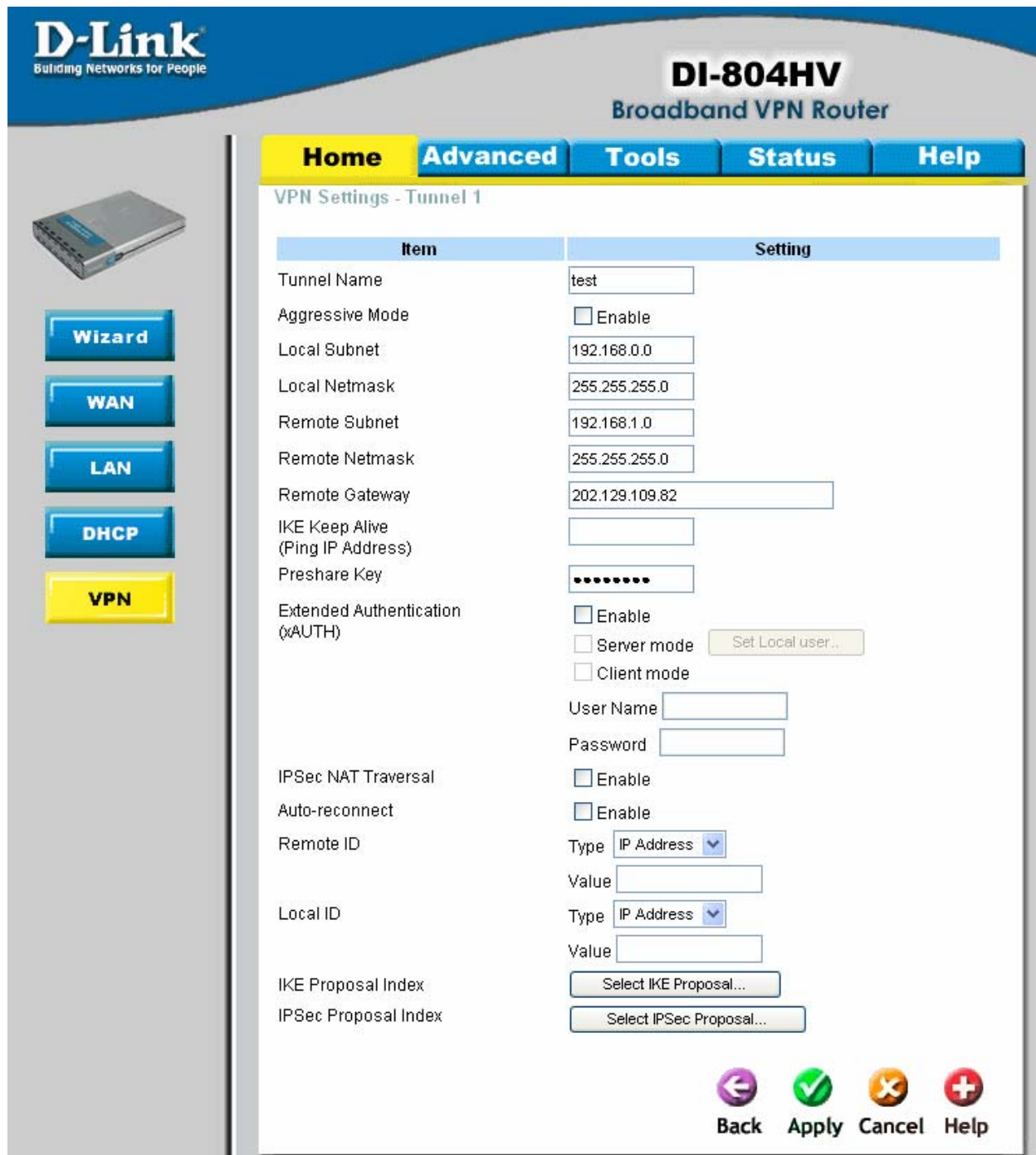
Local Subnet/Netmask are characteristics of the network where the Unit you are currently configuring is installed.

Remote Subnet/Netmask are for the network located on the other end of the VPN connection.

Make sure that you specify the Remote Gateway being public IP (the address Internet Provider assigns) of the remote network (WAN address on remote router).

Preshare Key: this can be anything up to 31 characters long (this is the same key that you used in the DFL-firewall configuration).

Then click Apply, then click on "Select IKE Proposal..."



D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home **Advanced** **Tools** **Status** **Help**

VPN Settings - Tunnel 1

Item	Setting
Tunnel Name	test
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.0
Remote Netmask	255.255.255.0
Remote Gateway	202.129.109.82
IKE Keep Alive (Ping IP Address)	
Preshare Key
Extended Authentication (XAUTH)	<input type="checkbox"/> Enable <input type="checkbox"/> Server mode Set Local user... <input type="checkbox"/> Client mode
User Name	
Password	
IPsec NAT Traversal	<input type="checkbox"/> Enable
Auto-reconnect	<input type="checkbox"/> Enable
Remote ID	Type: IP Address Value:
Local ID	Type: IP Address Value:
IKE Proposal Index	Select IKE Proposal...
IPsec Proposal Index	Select IPsec Proposal...

[Back](#) [Apply](#) [Cancel](#) [Help](#)

If you are using the Dynamic VPN option, the **Dynamic VPN Settings** page will look a bit different:

The screenshot shows the configuration interface for a D-Link DI-804HV Broadband VPN Router. The page title is "VPN Settings - Dynamic VPN Tunnel". The interface includes a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". On the left side, there is a sidebar with a router image and buttons for "Wizard", "WAN", "LAN", "DHCP", and "VPN". The main content area contains a table of settings for the Dynamic VPN Tunnel.

Item	Setting
Tunnel Name	<input type="text" value="Test"/>
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	<input type="text" value="192.168.0.0"/>
Local Netmask	<input type="text" value="255.255.255.0"/>
Preshare Key	<input type="password" value="....."/>
Extended Authentication (xAUTH)	<input type="checkbox"/> Enable Server mode <input type="button" value="Set Local user.."/>
IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>

At the bottom right of the settings area, there are four icons: a purple left arrow labeled "Back", a green checkmark labeled "Apply", an orange 'X' labeled "Cancel", and a red plus sign labeled "Help".

Below is the example how you can setup IKE Proposal.
 We used the following settings:
 ID 1, Name: test, Group 5, 3DES, SHA1, 300, Sec

The screenshot shows the configuration page for the D-Link DI-804HV Broadband VPN Router. The page is titled "VPN Settings - Tunnel 1 - Set IKE Proposal". On the left side, there is a navigation menu with buttons for Wizard, WAN, LAN, DHCP, and VPN (highlighted in yellow). The main content area has a navigation bar with Home, Advanced, Tools, Status, and Help. Below the navigation bar, there is a table with two columns: "Item" and "Setting". The "Item" column contains "IKE Proposal index" and the "Setting" column contains a text input field with "test" and a "Remove" button. Below this, there is a table with 7 columns: ID, Proposal Name, DH Group, Encrypt algorithm, Auth algorithm, Life Time, and Life Time Unit. The table contains 10 rows of configuration options. The first row (ID 1) has the following settings: Proposal Name: test, DH Group: Group 5, Encrypt algorithm: 3DES, Auth algorithm: SHA1, Life Time: 300, Life Time Unit: Sec. The remaining rows (IDs 2-10) have Proposal Name: (empty), DH Group: Group 1, Encrypt algorithm: 3DES, Auth algorithm: SHA1, Life Time: 0, Life Time Unit: Sec. Below the table, there is a "Proposal ID" dropdown menu set to "-- select one --", an "Add to" button, and a "Proposal index" dropdown menu. At the bottom right, there are four navigation buttons: Back (left arrow), Apply (checkmark), Cancel (X), and Help (plus sign).

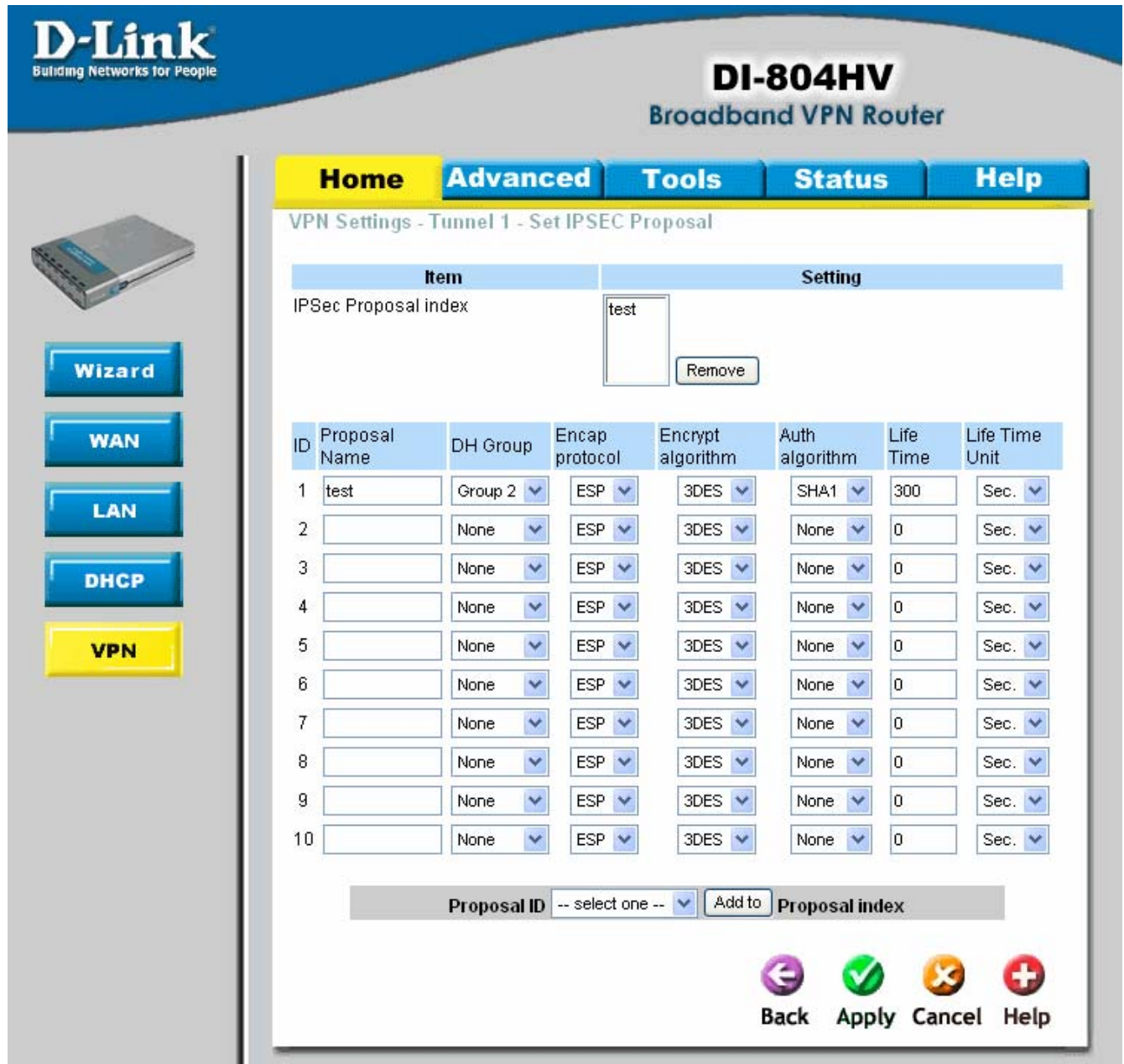
Once the settings have been changed click on the drop down box for "Proposal ID" and select "1". Then click on the Add to button.

This should move the Proposal name to the IKE Proposal Index at the top of the page.

NOTE: If you need to change the setting you do not need to click the Add to button the second time.

Click Apply, then click on Back.

Click on "IPSec Proposal". Configure it the same way as on the IKE Proposal page, then click Apply.



The image shows the web interface of a D-Link DI-804HV Broadband VPN Router. The top navigation bar includes Home, Advanced, Tools, Status, and Help. The current page is titled "VPN Settings - Tunnel 1 - Set IPSEC Proposal". On the left sidebar, there are buttons for Wizard, WAN, LAN, DHCP, and VPN (highlighted in yellow). The main content area features a table for IPsec proposals and a list of 10 proposal configurations.

Item	Setting
IPSec Proposal index	test <input type="button" value="Remove"/>

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 2	ESP	3DES	SHA1	300	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

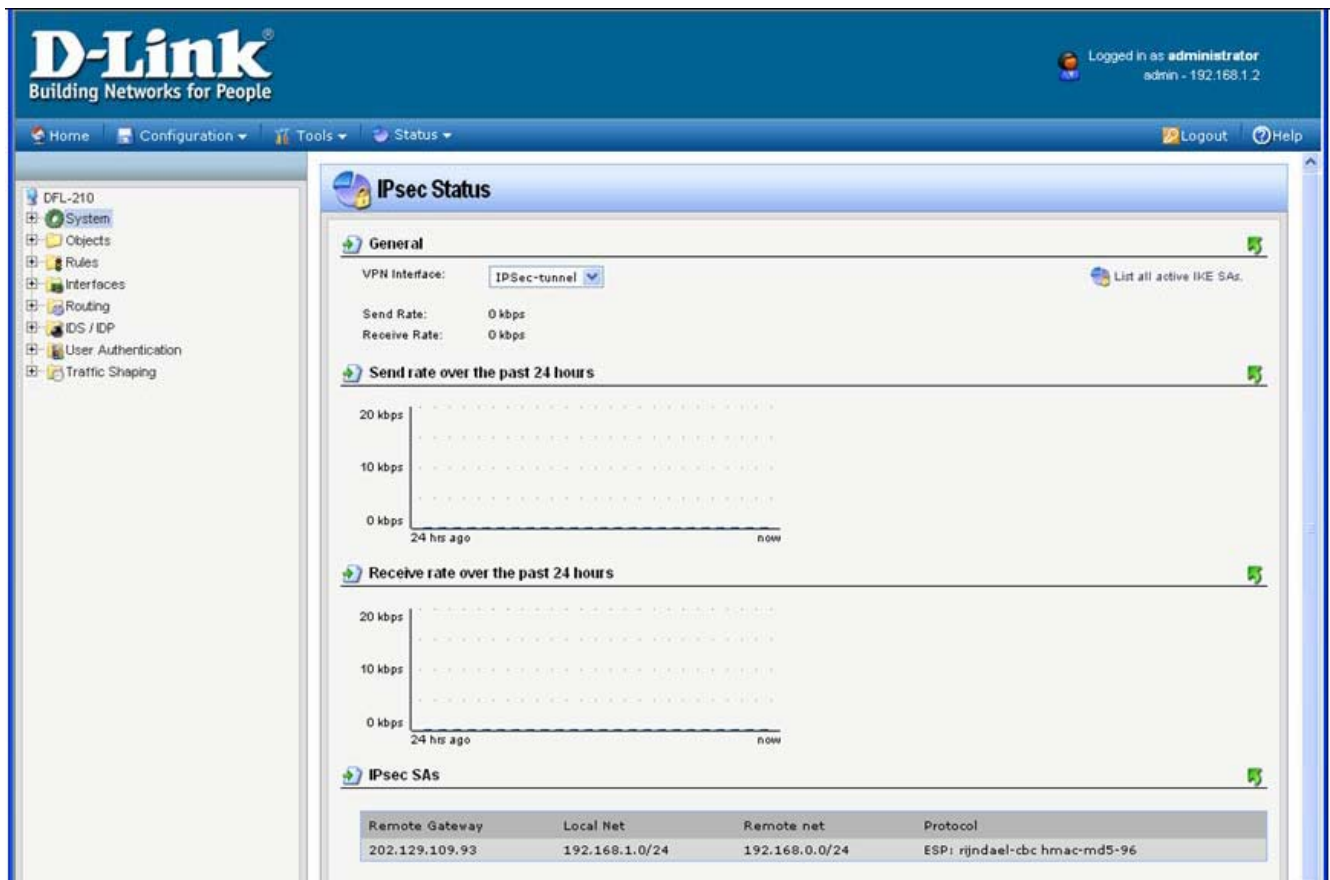
Proposal ID: -- select one -- Proposal index

Navigation icons: Back, Apply, Cancel, Help

This is all you need to do to configure the DI-80xHV VPN router.

Checking the 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.



The screenshot shows the D-Link web interface for the DFL-210 device. The user is logged in as 'administrator' with IP address '192.168.1.2'. The 'Status' menu is selected, and the 'IPsec Status' page is displayed. The 'General' section shows the VPN interface is 'IPSec-tunnel' and both send and receive rates are 0 kbps. Below this are two line graphs for 'Send rate over the past 24 hours' and 'Receive rate over the past 24 hours', both showing zero activity. At the bottom, the 'IPsec SAs' section contains a table with one entry.

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).

If VPN Tunnel can not be established:

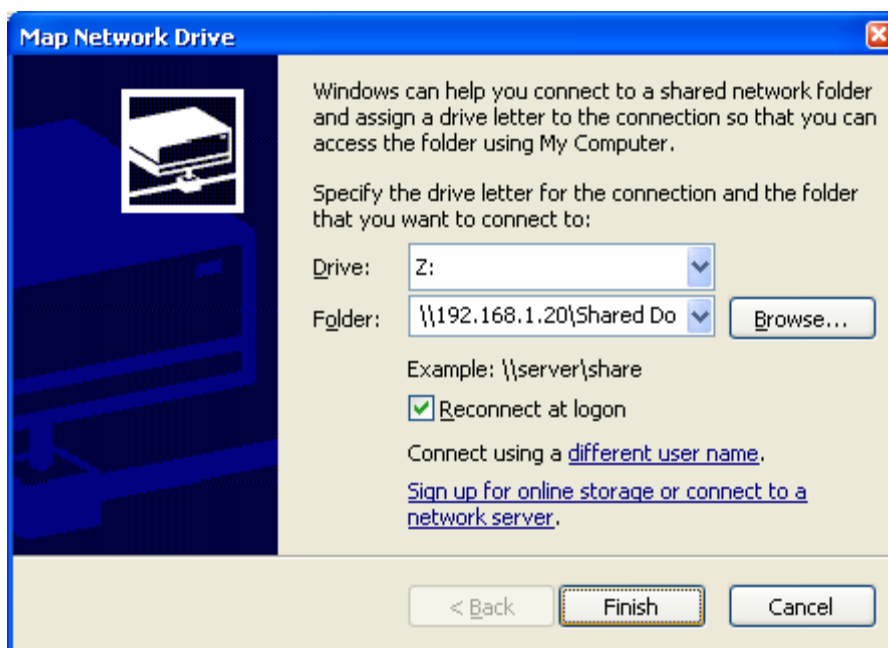
- Make sure that the modems in front of the firewalls support VPN passthrough.
- Check the Pre-shared keys, security algorithms and life times, make sure they match on both VPN firewalls.
- Restart both firewalls.

You can see the connection log under Status > Logging.

Log Status								
Internal Logging (1-45)								
Date	Severity	Category	Rule	Proto	SrcIf	Src/DstIP	Src/DstPort	Details
2006-05-19 00:36:33	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2	1030	connndestif=IPSec-tunnel
2006-05-19 00:36:29	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.243	connsrcid=512 connndestif=IPSec-tunnel connndestid=512 origsent=1680 termssent=1680
2006-05-19 00:36:12	Notice	CONN	IPsecBeforeRules	UDP	wan	202.129.109.93	500	connndestif=core origsent=7748 termssent=0
2006-05-19 00:35:53	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.149	connsrcid=512 connndestif=IPSec-tunnel connndestid=512
2006-05-19 00:35:35	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.1	connsrcid=512 connndestif=IPSec-tunnel connndestid=512 origsent=60 termssent=0
2006-05-19 00:35:26	Notice	CONN	IPSec-Allow	ICMP	lan	192.168.1.2	192.168.0.1	connsrcid=512 connndestif=IPSec-tunnel connndestid=512
2006-05-19 00:34:15	Notice	CONN	IPSec-Allow	UDP	lan	192.168.1.2	1028	connndestif=IPSec-tunnel
2006-05-19 00:33:59	Informational	IPSEC						SA ESP[b570dadf] 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	connndestif=IPSec-tunnel origsent=790 termssent=1136
2006-05-19 00:33:16	Notice	CONN	IPSec-Allow	TCP	IPSec-tunnel	192.168.0.149	3844	connndestif=lan origsent=168 termssent=404

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.