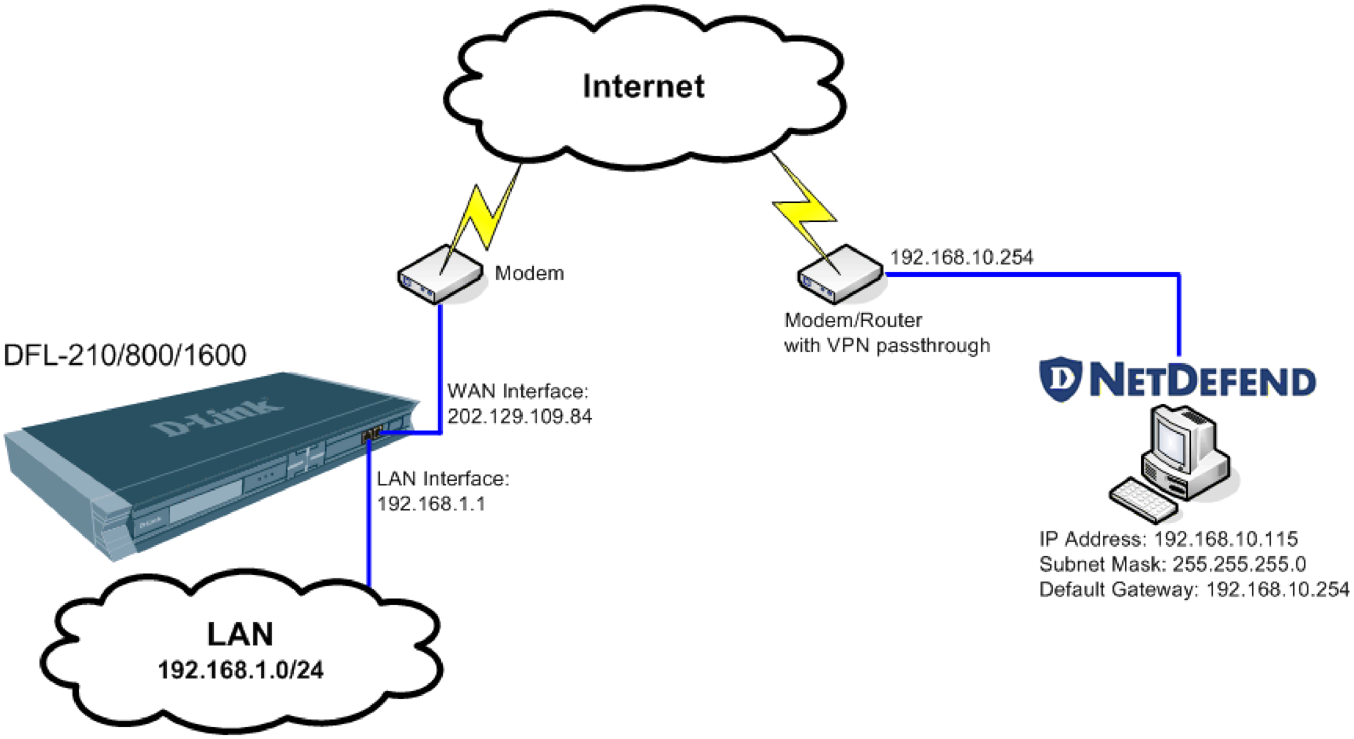
DFL-210, DFL-800, DFL-1600

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

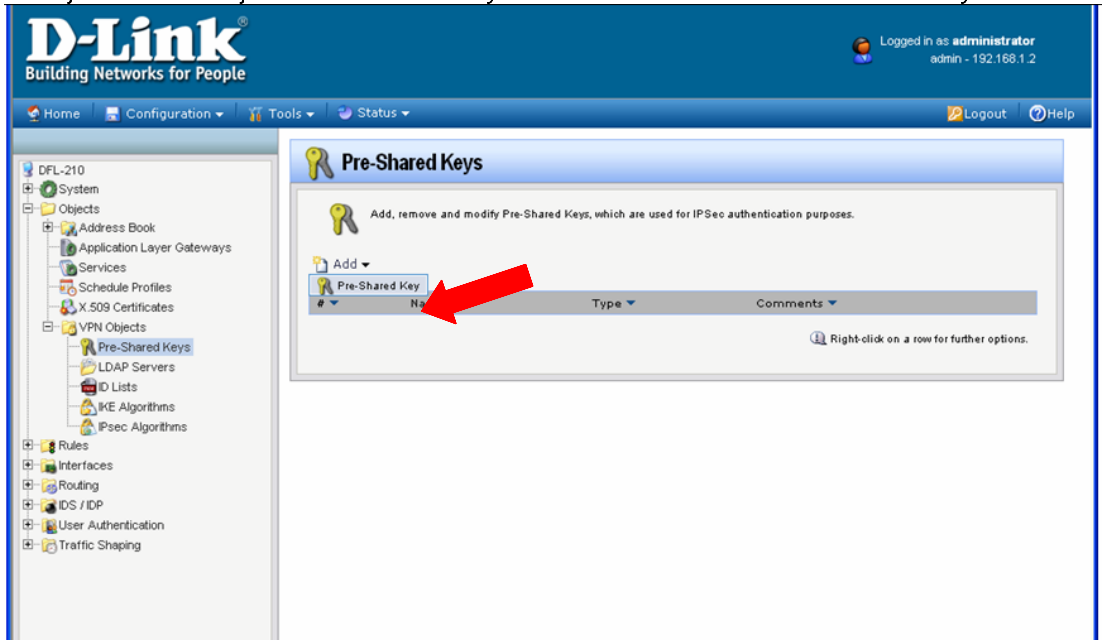
This setup example uses the following network settings:



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.

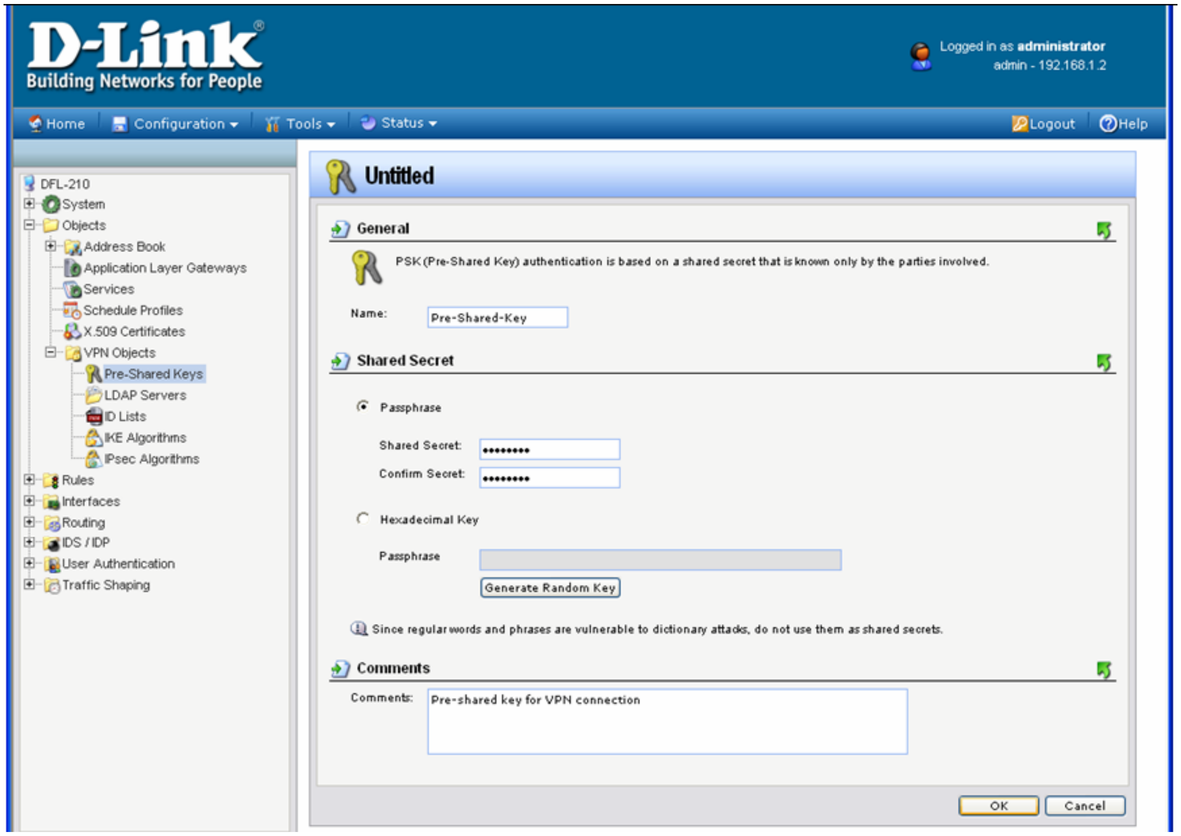
Step 2. Go to Objects > VPN Objects > Pre-Shared Keys. Click on Add and select Pre-Shared Key.



Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.

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 VPN Client. Click OK when done.



General

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name: Pre-Shared-Key

Shared Secret

● Passphrase

Shared Secret: ••••••••

Confirm Secret: ••••••••

○ Hexadecimal Key

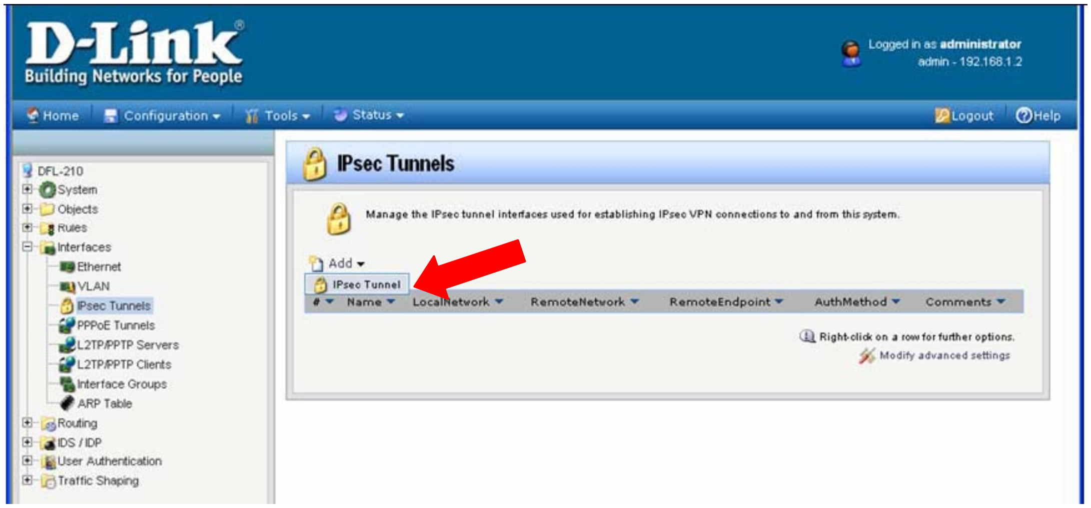
Passphrase

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments

Comments: Pre-shared key for VPN connection

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



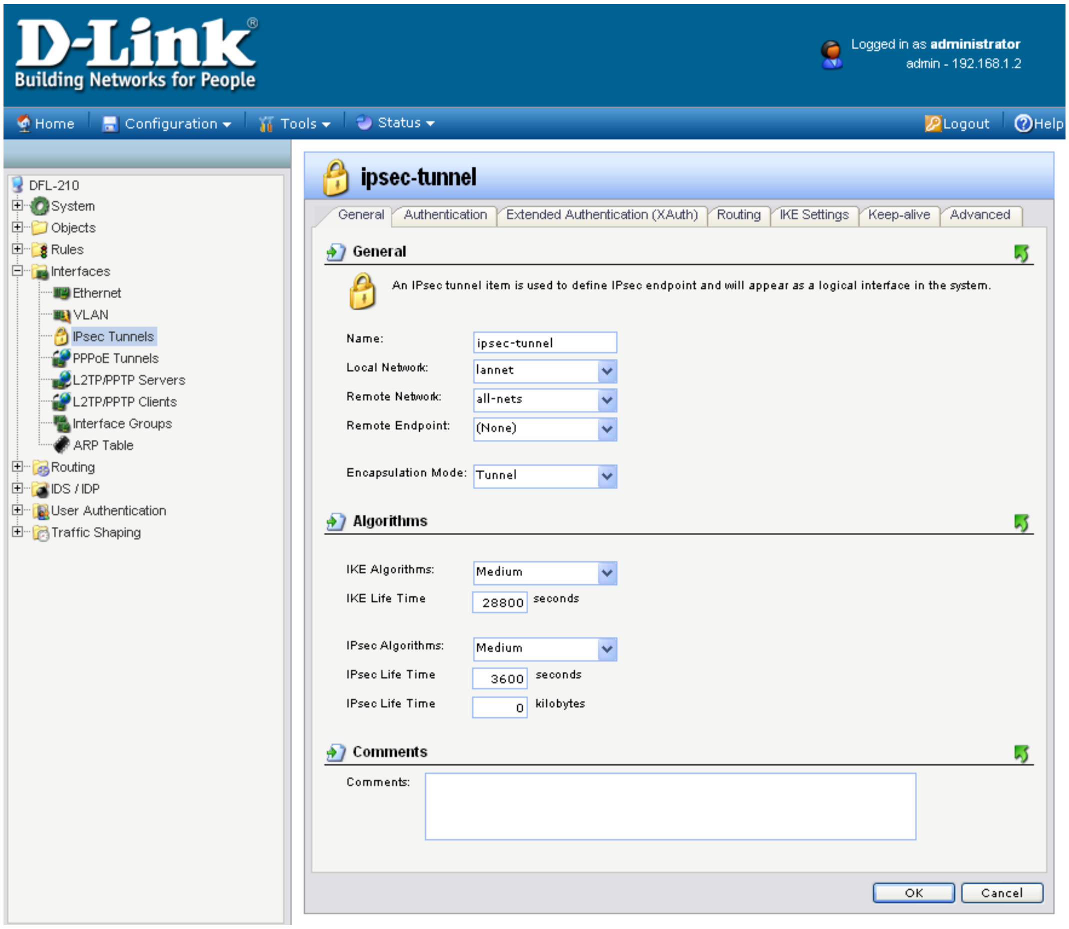
IPsec Tunnels

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	LocalNetwork	RemoteNetwork	RemoteEndpoint	AuthMethod	Comments

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.



ipsec-tunnel

General

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Name: ipsec-tunnel
Local Network: lannet
Remote Network: all-nets
Remote Endpoint: (None)

Encapsulation Mode: Tunnel

Algorithms

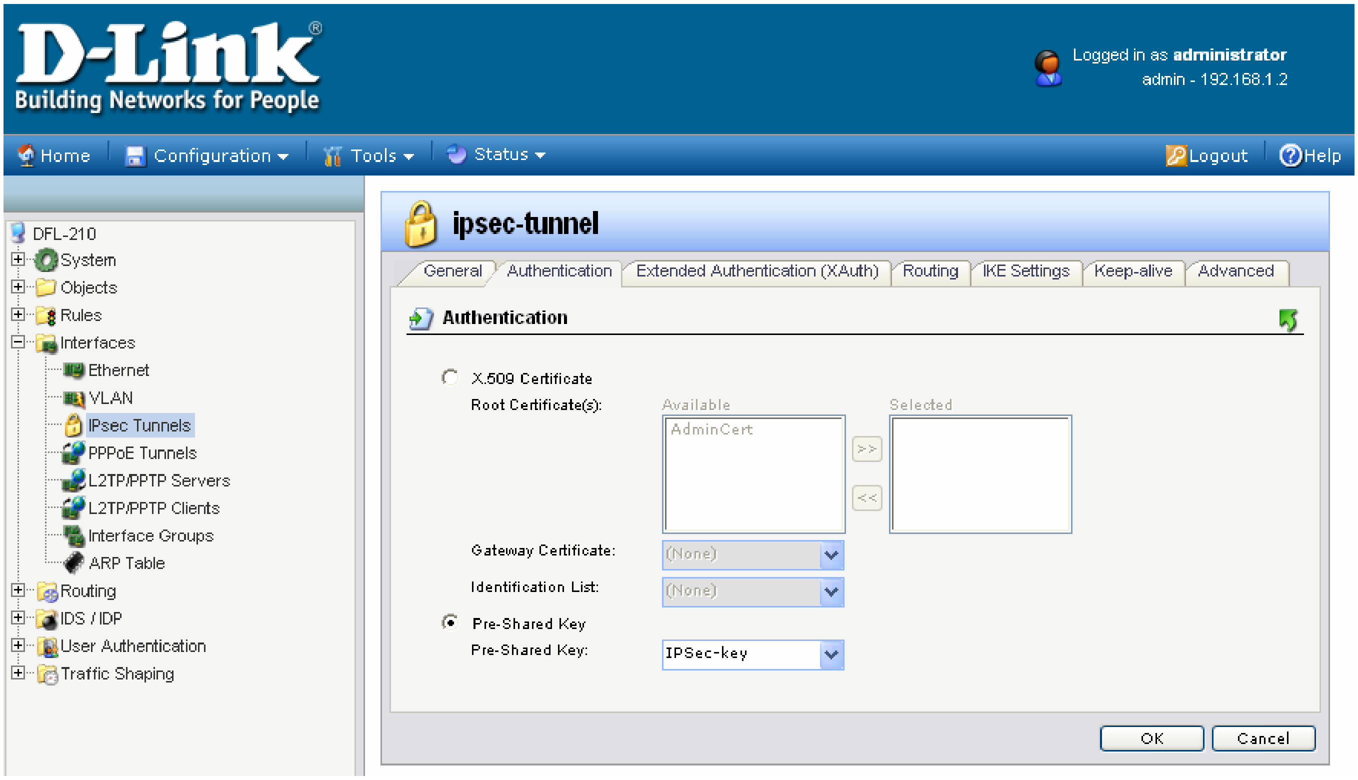
IKE Algorithms: Medium
IKE Life Time 28800 seconds

IPsec Algorithms: Medium
IPsec Life Time 3600 seconds
IPsec Life Time 0 kilobytes

Comments

Comments:

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**).



○ X.509 Certificate

Root Certificate(s):

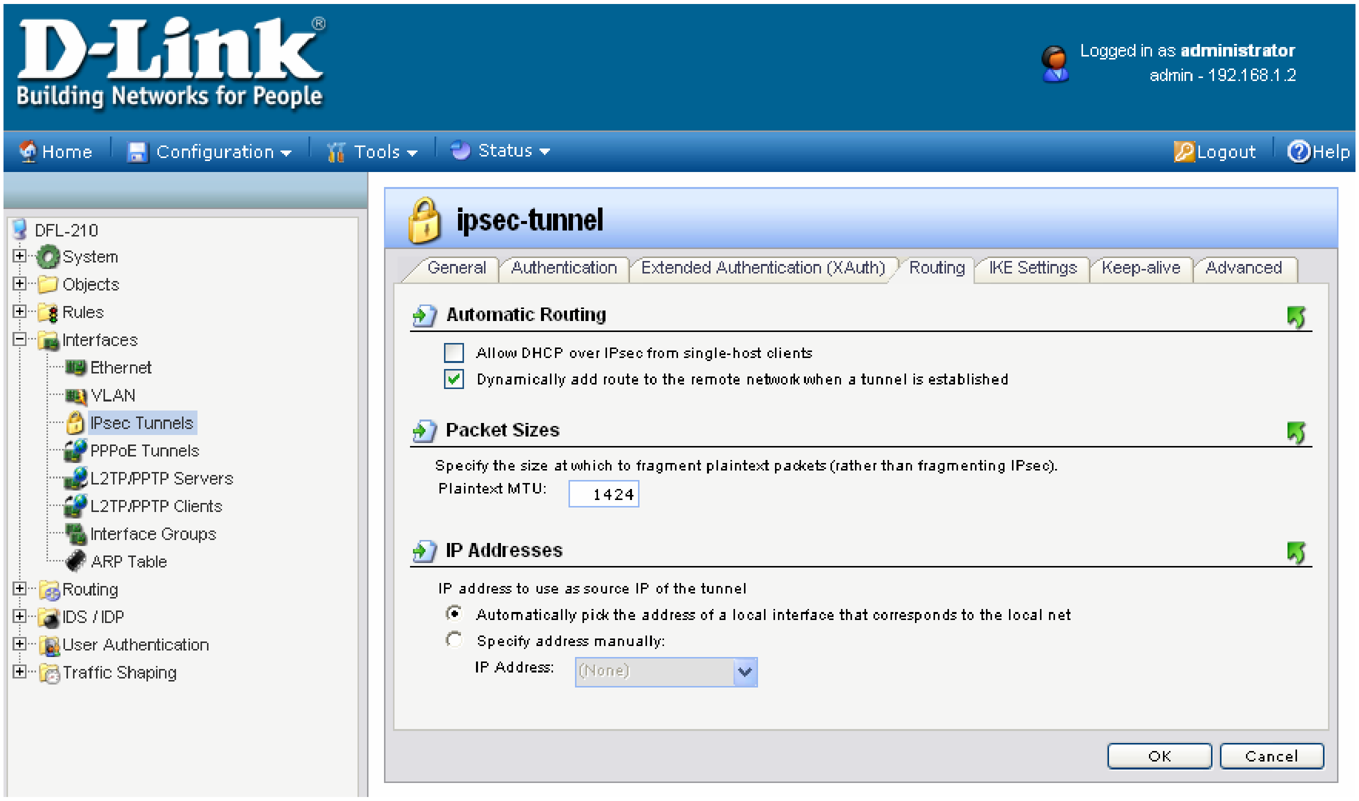
Gateway Certificate: (None)

Identification List: (None)

● Pre-Shared Key

Pre-Shared Key: IPSec-key

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



ipsec-tunnel

Automatic Routing

□ Allow DHCP over IPsec from single-host clients

☑ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1424

IP Addresses

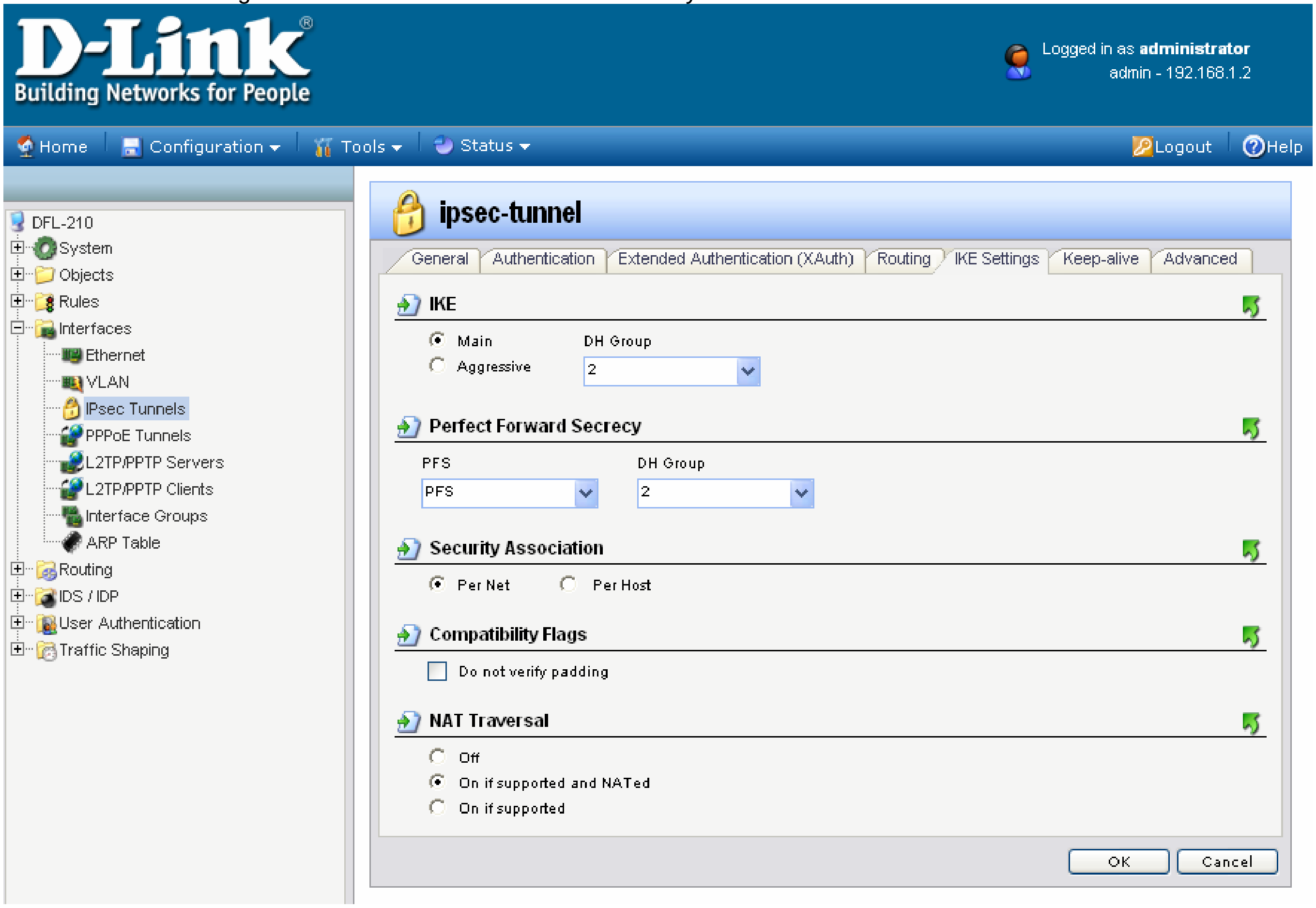
IP address to use as source IP of the tunnel

● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)

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



ipsec-tunnel

IKE

● Main
○ Aggressive

DH Group: 2

Perfect Forward Secrecy

PFS: PFS

DH Group: 2

Security Association

● Per Net ○ Per Host

Compatibility Flags

□ Do not verify padding

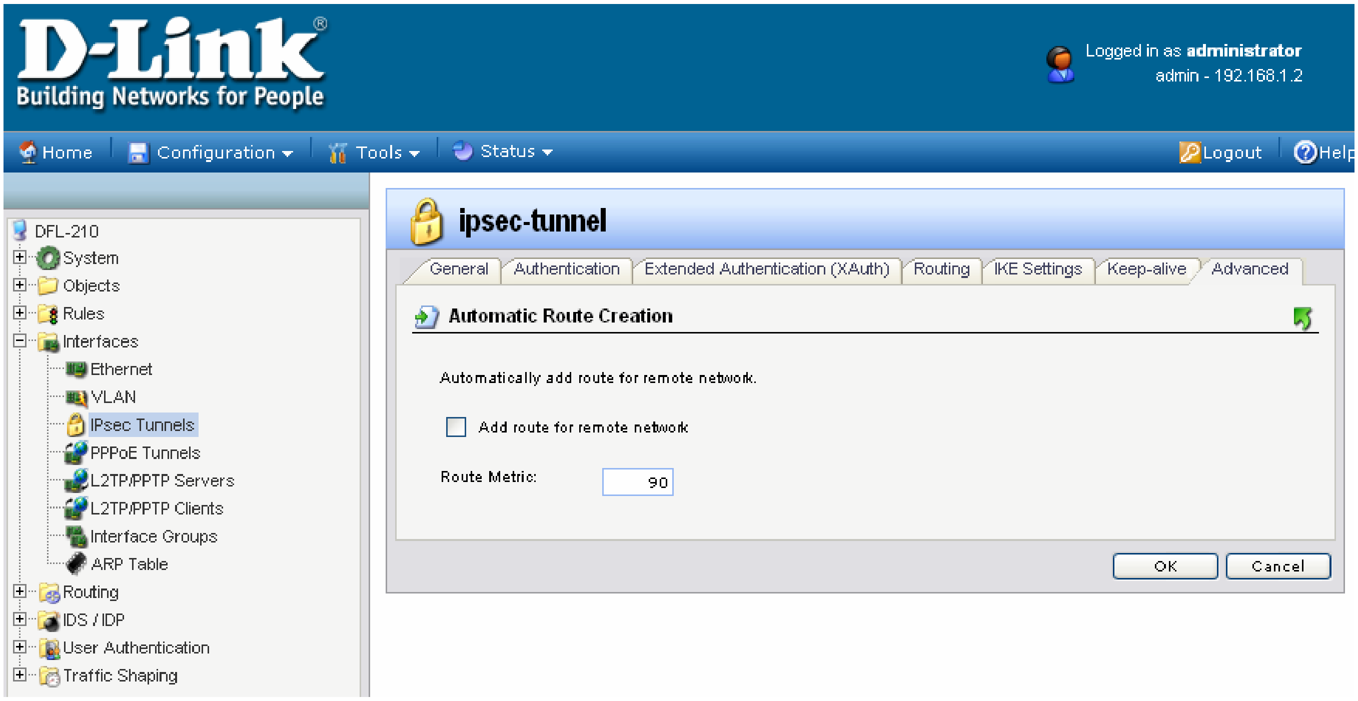
NAT Traversal

○ Off

● On if supported and NATed

○ On if supported

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



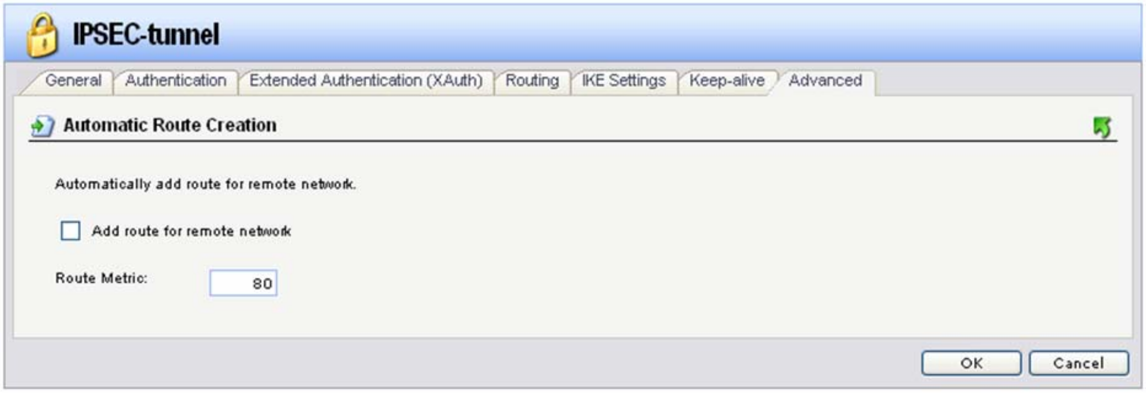
Automatic Route Creation

Automatically add route for remote network.

☐ Add route for remote network

Route Metric: 90

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



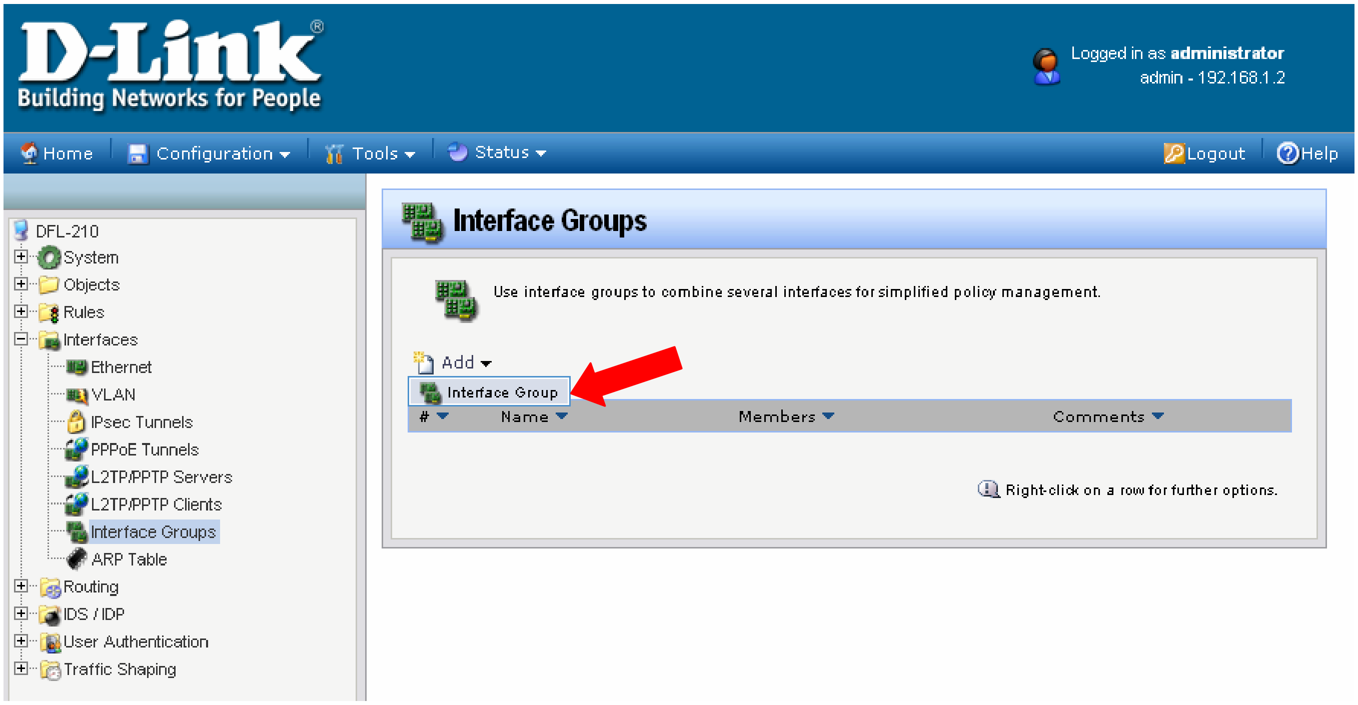
Automatic Route Creation

Automatically add route for remote network.

☐ Add route for remote network

Route Metric: 80

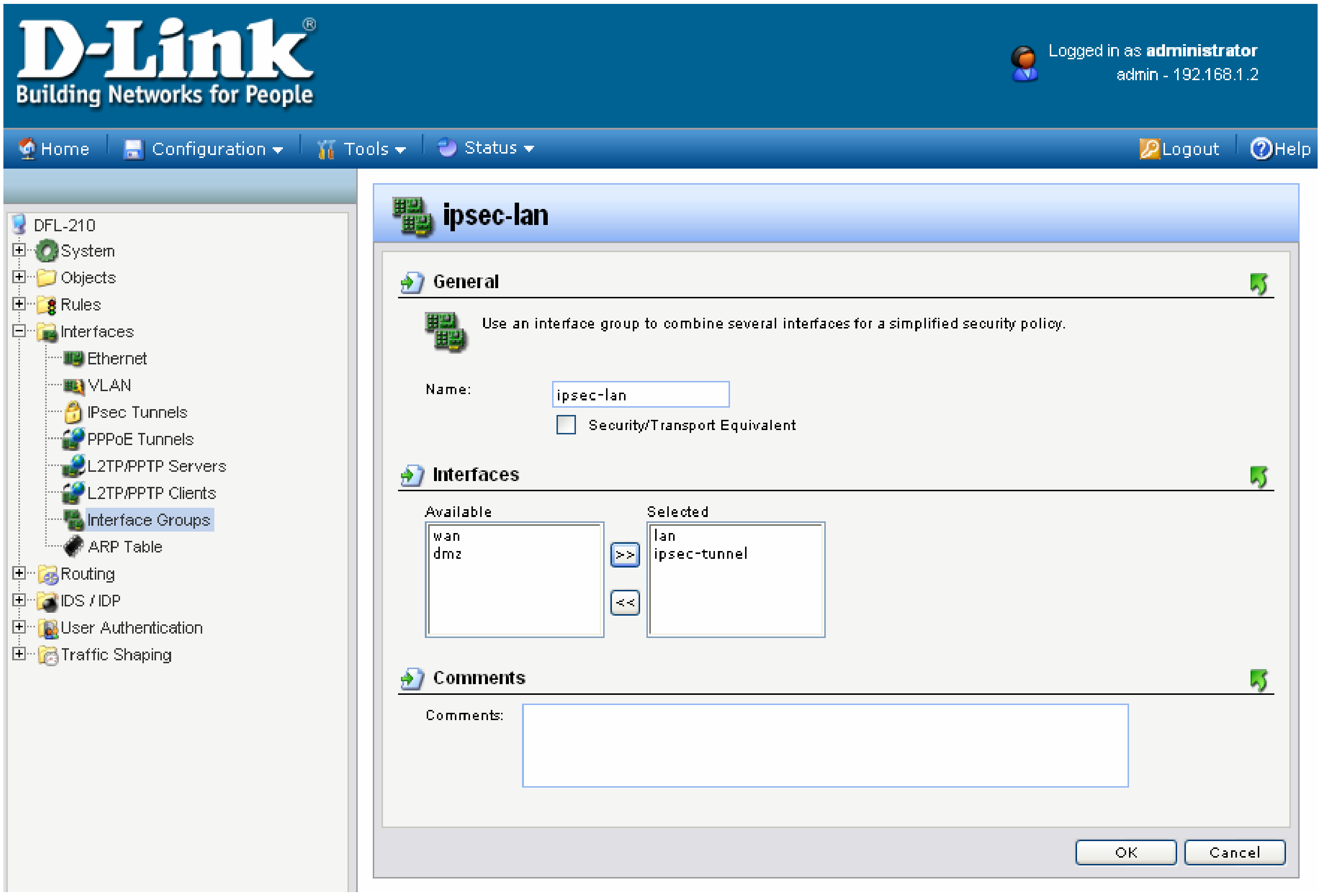
Step 4. Go to Interface > Interface Groups, Click on Add and then Interface Group.



Use interface groups to combine several interfaces for simplified policy management.

Right-click on a row for further options.

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.



Use an interface group to combine several interfaces for a simplified security policy.

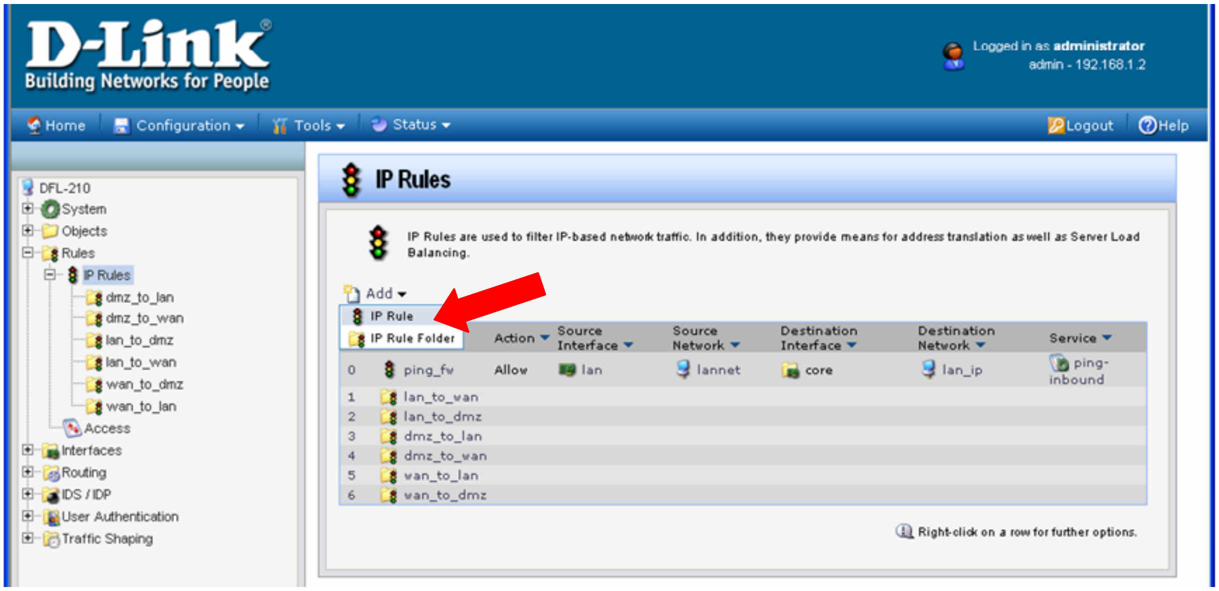
Name: ipsec-lan

□ Security/Transport Equivalent

Available	Selected
wan dmz	lan ipsec-tunnel

Comments:

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



IP Rules

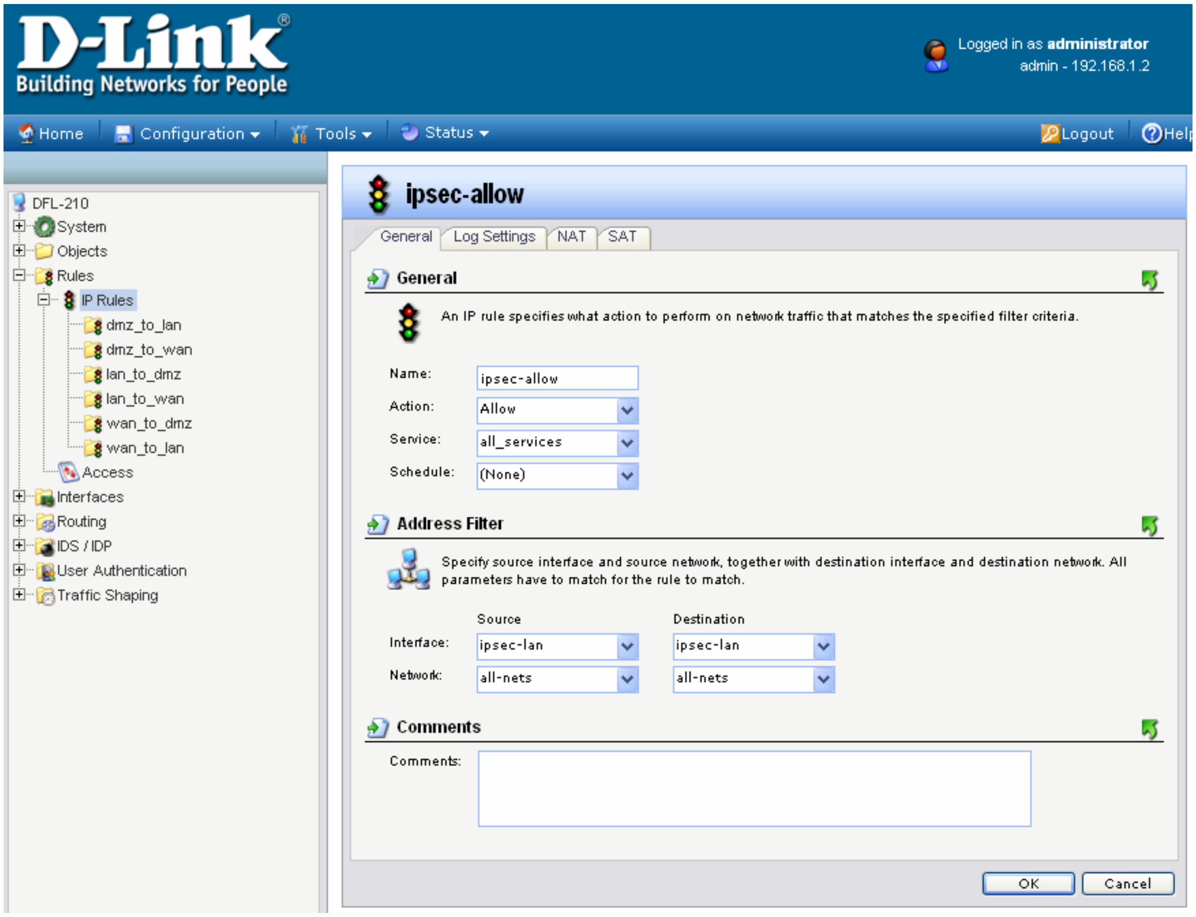
IP Rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

		Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
1	lan_to_wan						
2	lan_to_dmz						
3	dmz_to_lan						
4	dmz_to_wan						
5	wan_to_lan						
6	wan_to_dmz						

Right-click on a row for further options.

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".



ipsec-allow

General

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

Name: ipsec-allow
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

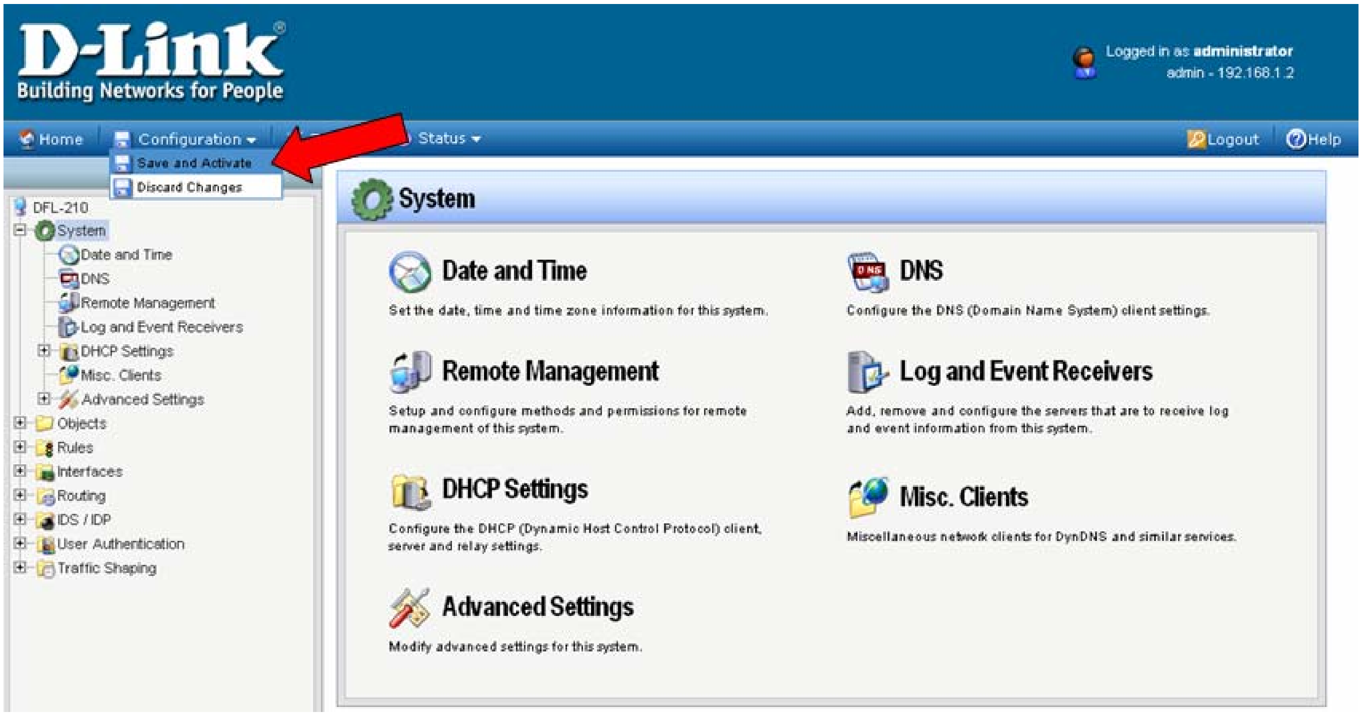
	Source	Destination
Interface:	ipsec-lan	ipsec-lan
Network:	all-nets	all-nets

Comments

Comments:

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”.



System

Date and Time

Set the date, time and time zone information for this system.

DNS

Configure the DNS (Domain Name System) client settings.

Remote Management

Setup and configure methods and permissions for remote management of this system.

Log and Event Receivers

Add, remove and configure the servers that are to receive log and event information from this system.

DHCP Settings

Configure the DHCP (Dynamic Host Control Protocol) client, server and relay settings.

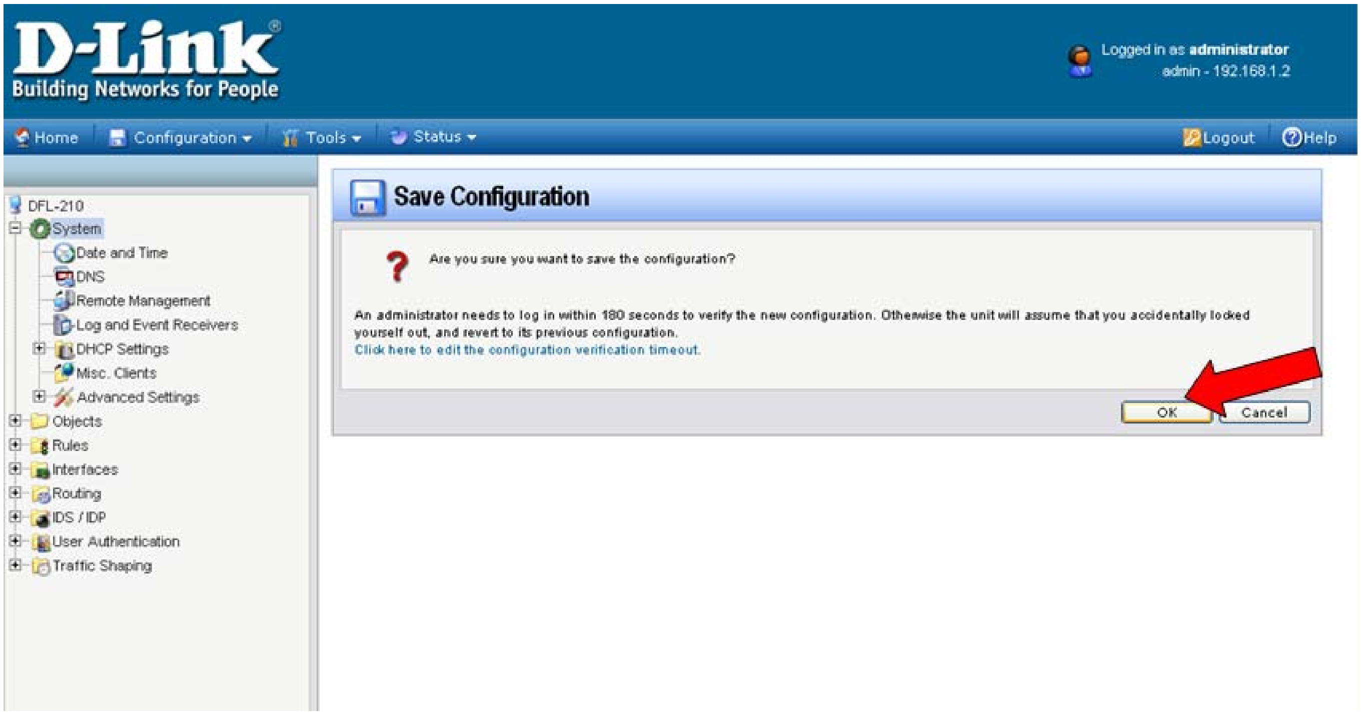
Misc. Clients

Miscellaneous network clients for DynDNS and similar services.

Advanced Settings

Modify advanced settings for this system.

Click on OK to confirm the new settings activation:



Save Configuration

Are you sure you want to save the configuration?

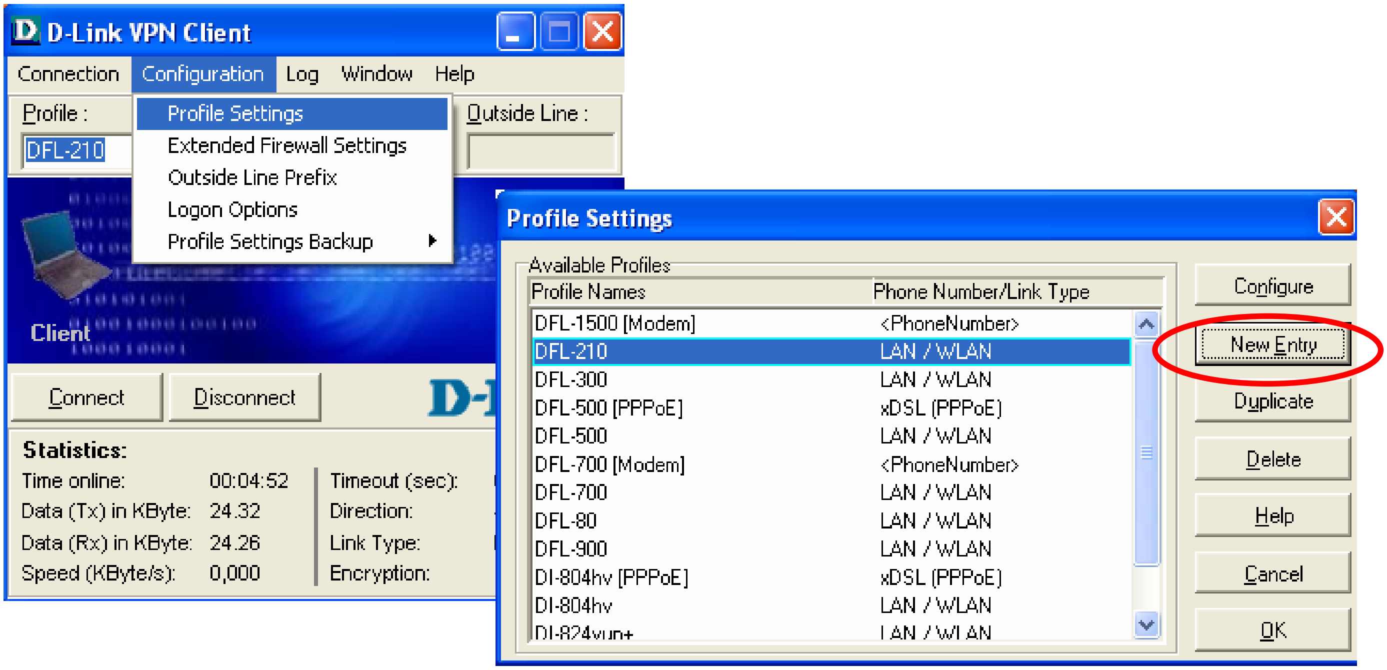
An administrator needs to log in within 180 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Click here to edit the configuration verification timeout.

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”.

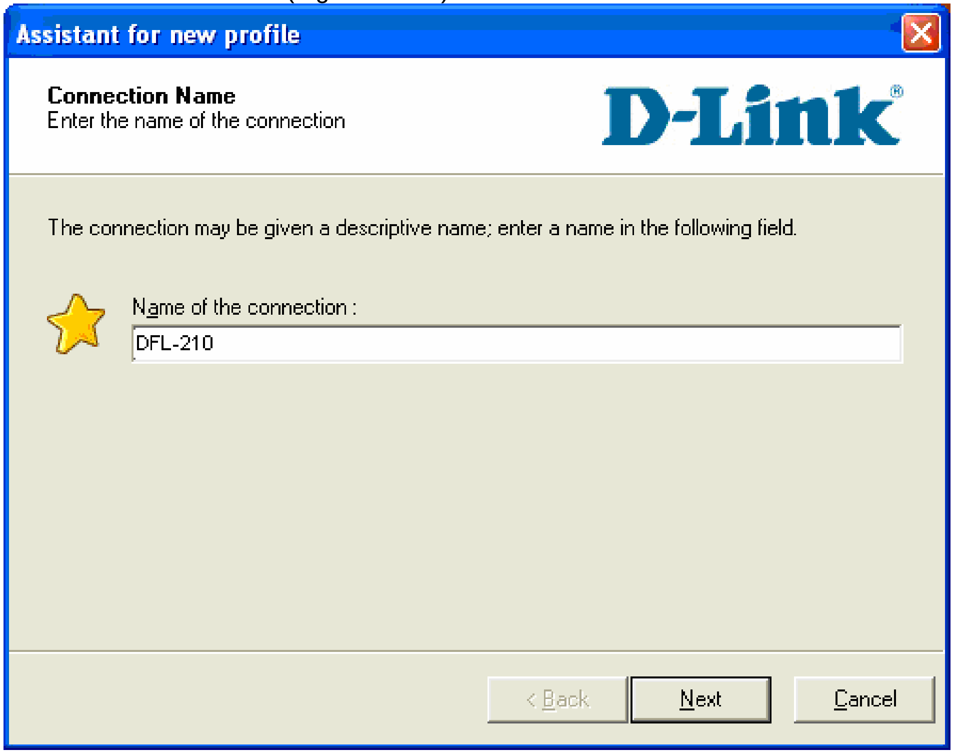


Statistics:

Time online: 00:04:52
Data (Tx) in KByte: 24.32
Data (Rx) in KByte: 24.26
Speed (KByte/s): 0,000
Timeout (sec):
Direction:
Link Type:
Encryption:

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-824vup+	LAN / WLAN

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

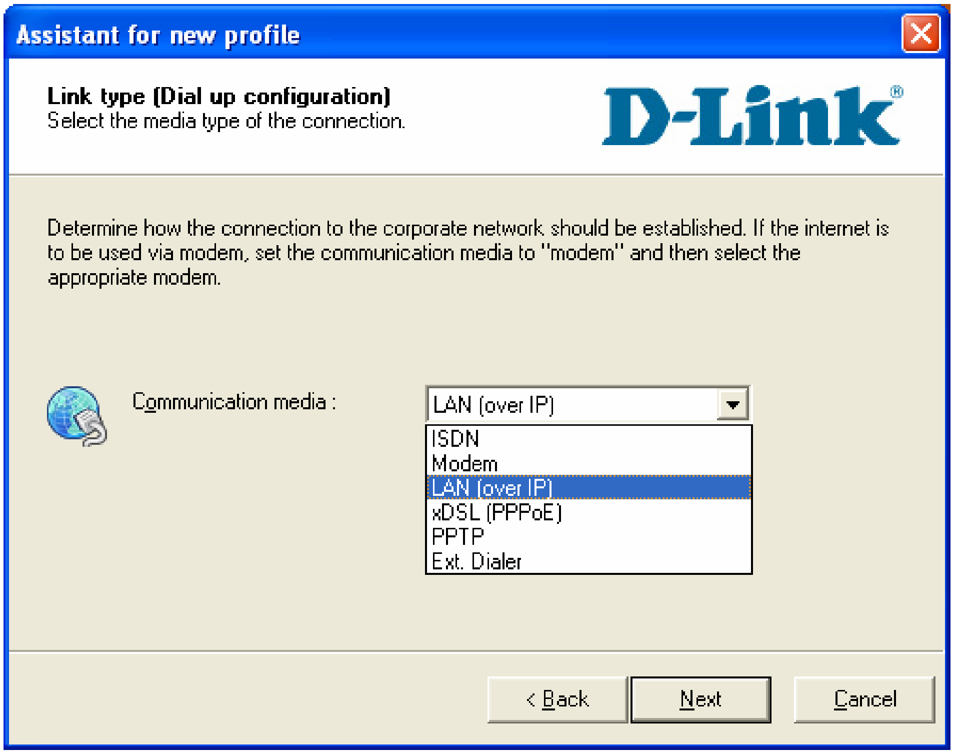


Connection Name
Enter the name of the connection

The connection may be given a descriptive name; enter a name in the following field.

Name of the connection : DFL-210

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



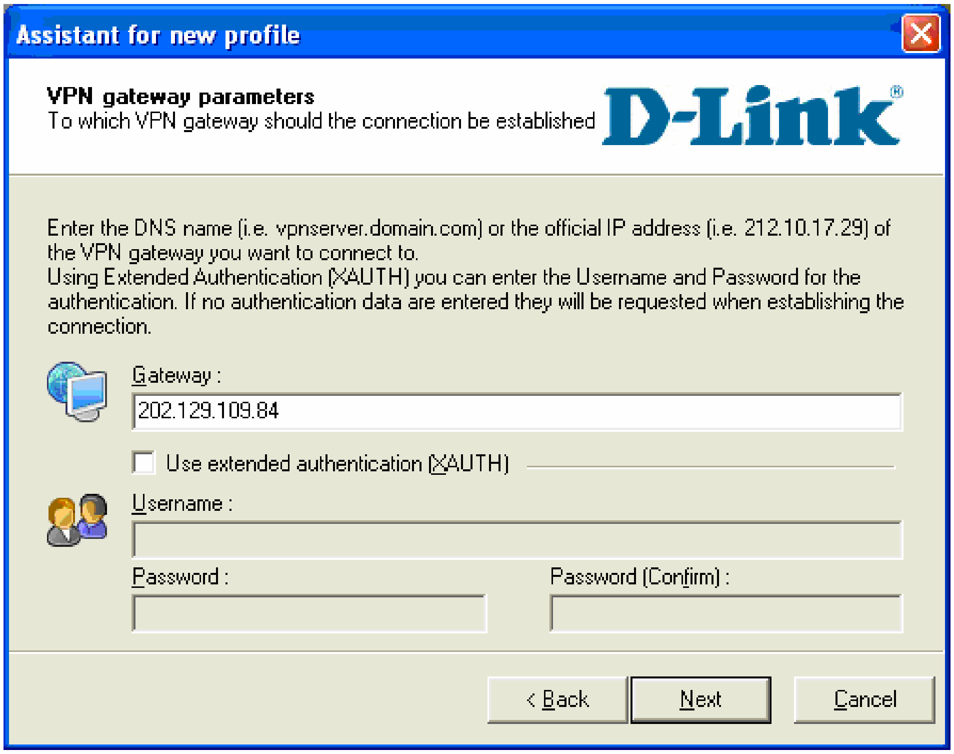
Assistant for new profile

Link type (Dial up configuration)
Select the media type of the connection.

Determine how the connection to the corporate network should be established. If the internet is to be used via modem, set the communication media to "modem" and then select the appropriate modem.

Communication media : LAN (over IP)

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.



Assistant for new profile

VPN gateway parameters
To which VPN gateway should the connection be established

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.
Using Extended Authentication (XAUTH) you can enter the Username and Password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway : 202.129.109.84

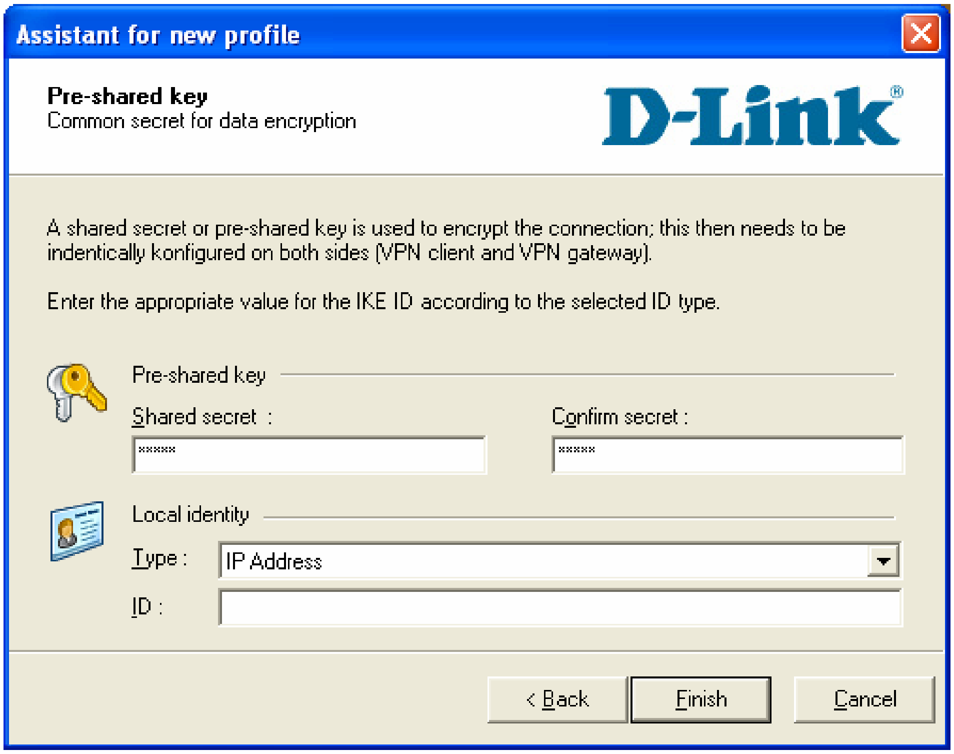
□ Use extended authentication (XAUTH)

Username :

Password :

Password (Confirm) :

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.



Assistant for new profile

Pre-shared key
Common secret for data encryption

A shared secret or pre-shared key is used to encrypt the connection; this then needs to be indentically konfigured 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

Shared secret : *****

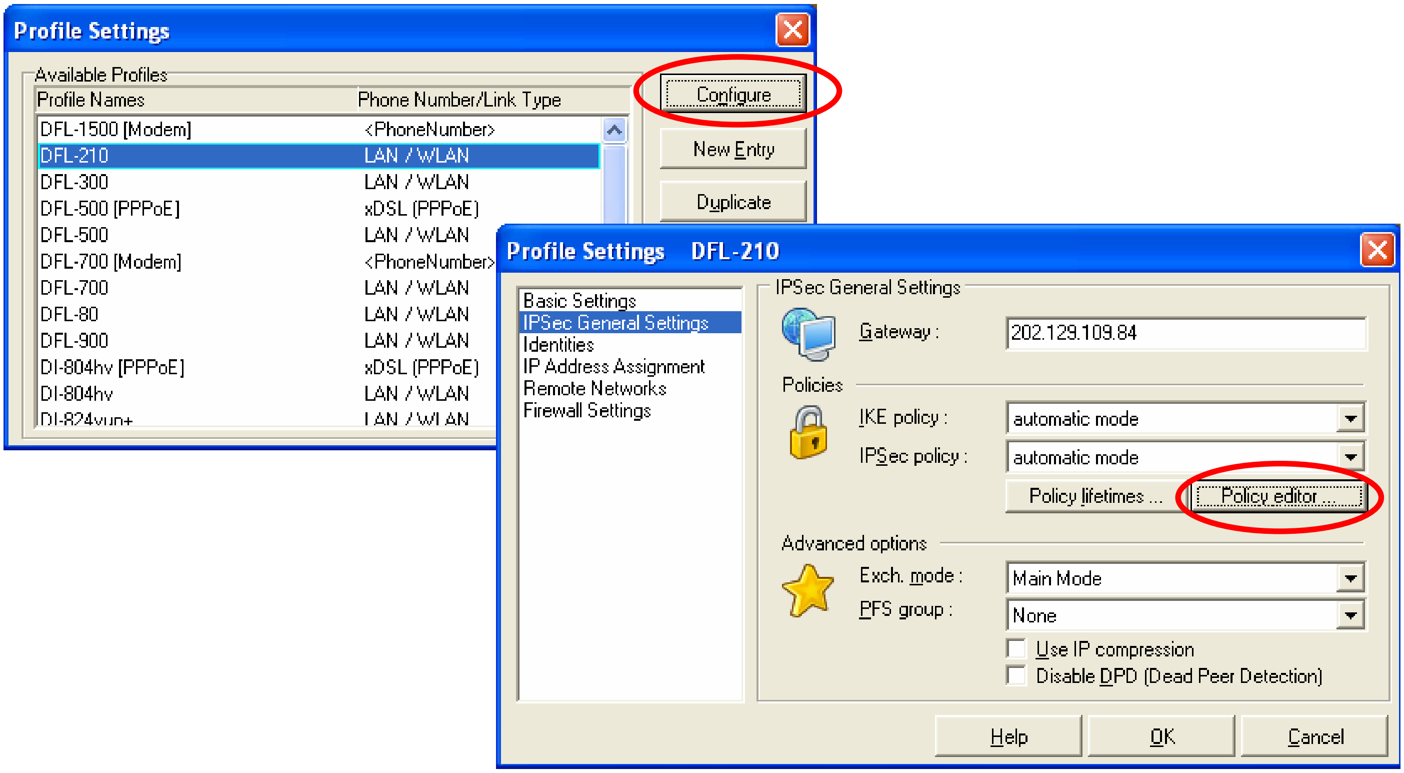
Confirm secret : *****

Local identity

Type : IP Address

ID :

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.



Profile Settings

Available Profiles

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-824vup+	LAN / WLAN

Profile Settings DFL-210

IPSec General Settings

Gateway : 202.129.109.84

Policies

IKE policy : automatic mode

IPSec policy : automatic mode

Advanced options

Exch. mode : Main Mode

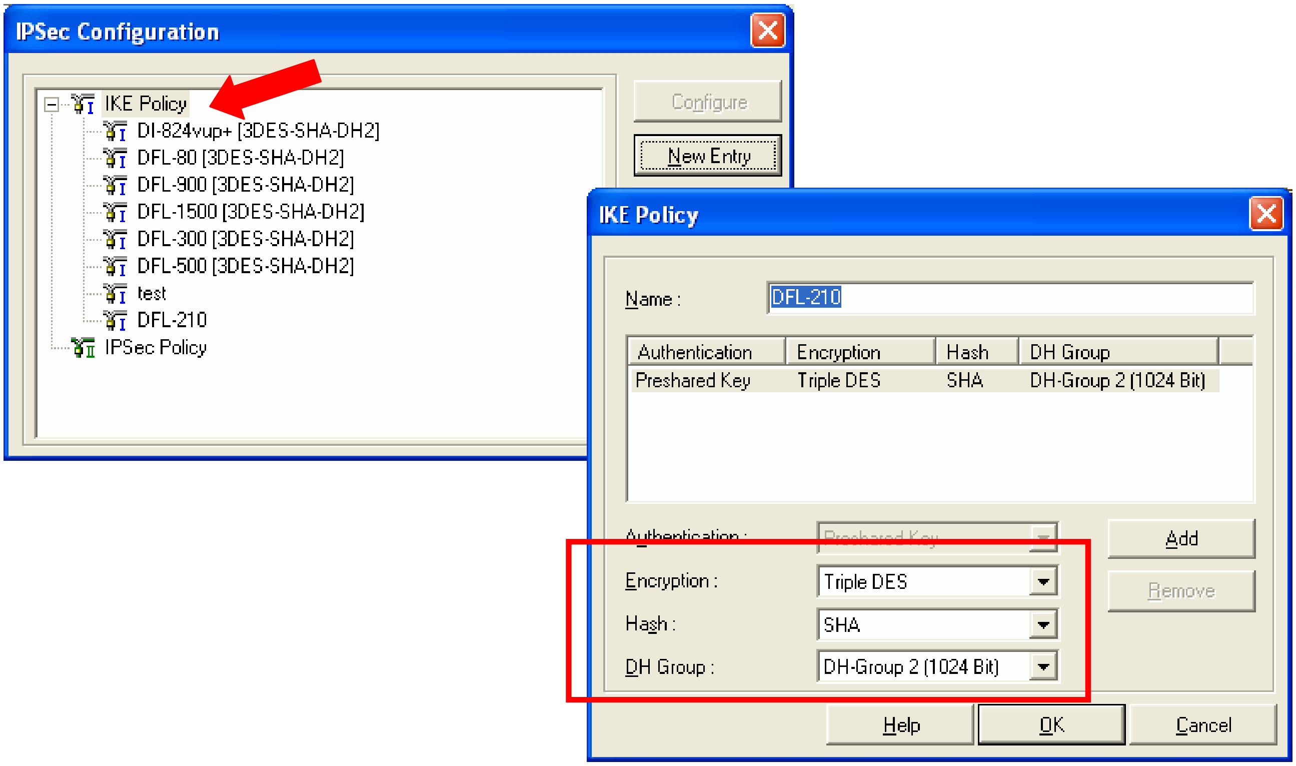
PFS group : None

□ Use IP compression

□ Disable DPD (Dead Peer Detection)

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.



IPSec Configuration

- IKE Policy
  - DI-824vup+ [3DES-SHA-DH2]
  - DFL-80 [3DES-SHA-DH2]
  - DFL-900 [3DES-SHA-DH2]
  - DFL-1500 [3DES-SHA-DH2]
  - DFL-300 [3DES-SHA-DH2]
  - DFL-500 [3DES-SHA-DH2]
  - test
  - DFL-210
- IPSec Policy

IKE Policy

Name : DFL-210

Authentication	Encryption	Hash	DH Group
Preshared Key	Triple DES	SHA	DH-Group 2 (1024 Bit)

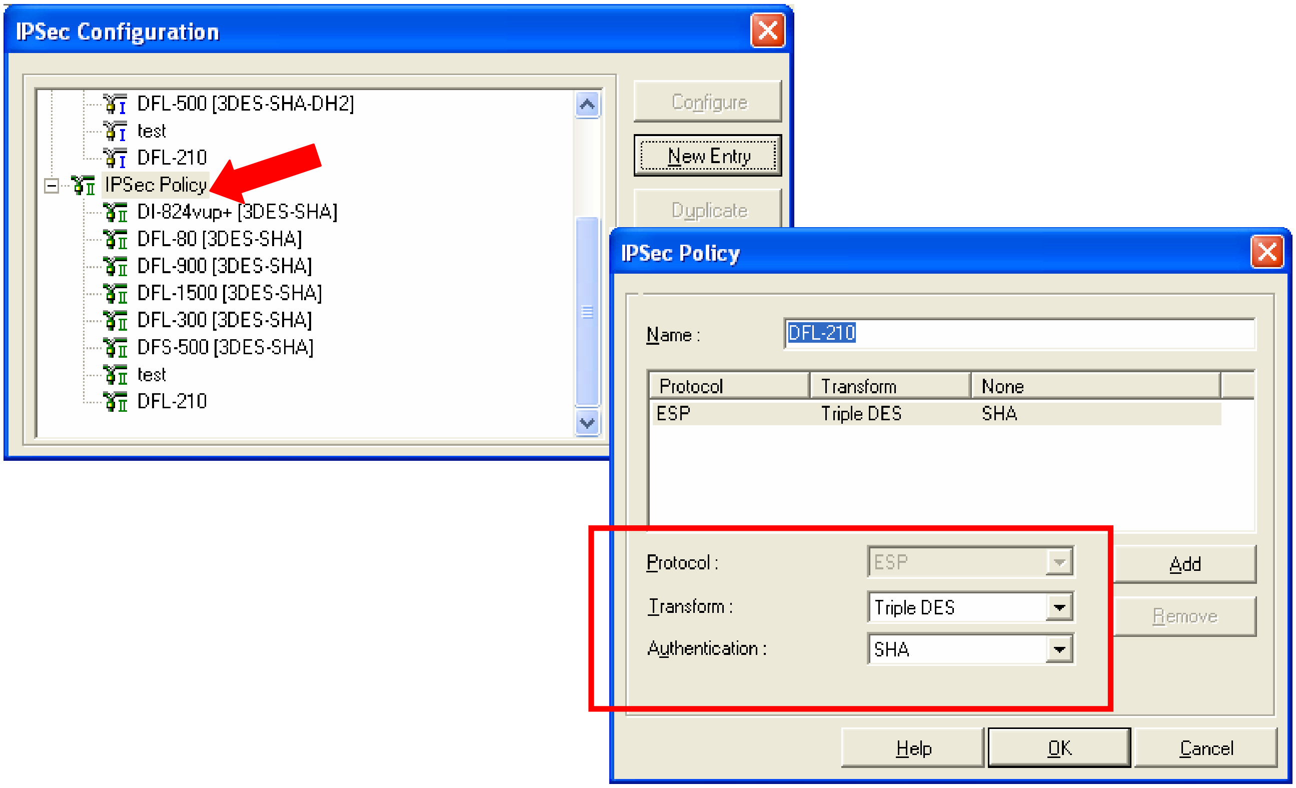
Authentication : Preshared Key

Encryption : Triple DES

Hash : SHA

DH Group : DH-Group 2 (1024 Bit)

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.



Name : DFL-210

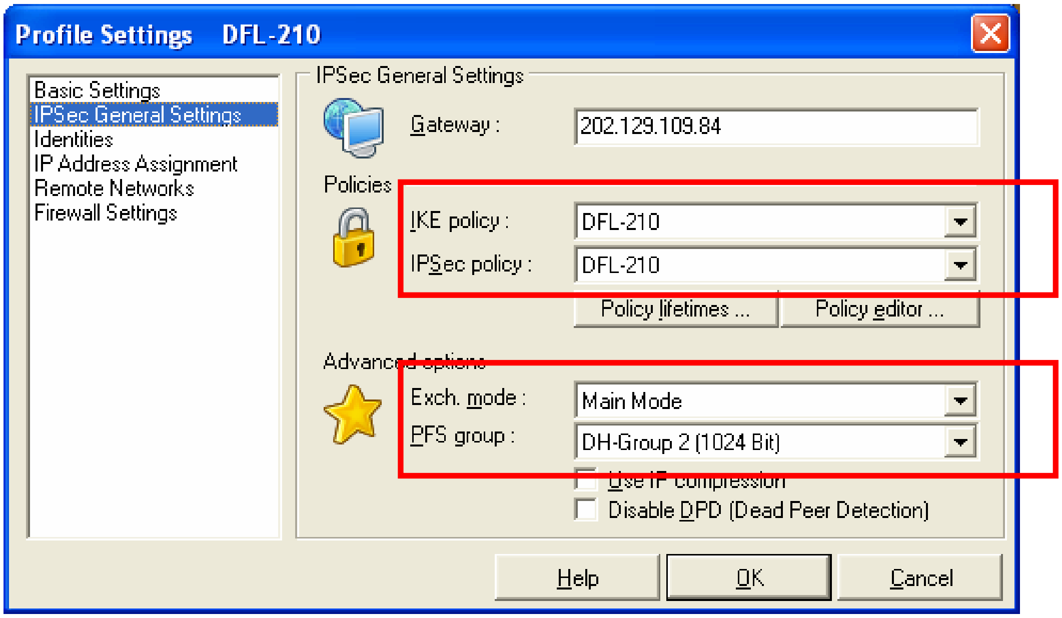
Protocol	Transform	None
ESP	Triple DES	SHA

Protocol : ESP

Transform : Triple DES

Authentication : SHA

Step 9. Back on the Profile Settings page, under the Polices 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.



Profile Settings DFL-210

- Basic Settings
- IPSec General Settings
- Identities
- IP Address Assignment
- Remote Networks
- Firewall Settings

IPSec General Settings

Gateway : 202.129.109.84

Policies

IKE policy : DFL-210

IPSec policy : DFL-210

Advanced options

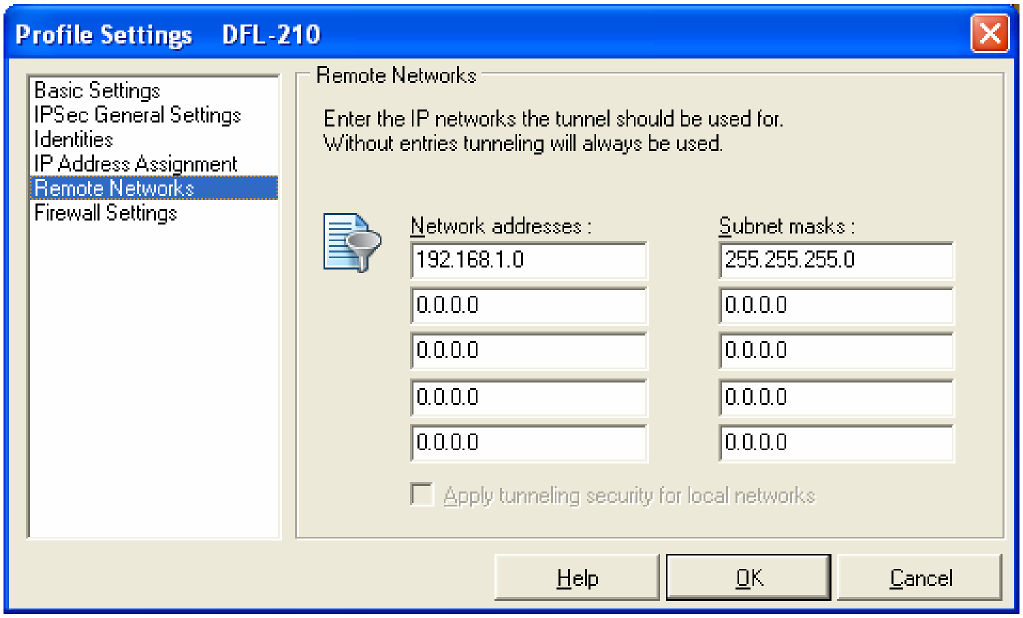
Exch. mode : Main Mode

PFS group : DH-Group 2 (1024 Bit)

□ Use IP compression

□ Disable DPD (Dead Peer Detection)

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.



Profile Settings DFL-210

- Basic Settings
- IPSec General Settings
- Identities
- IP Address Assignment
- Remote Networks
- Firewall Settings

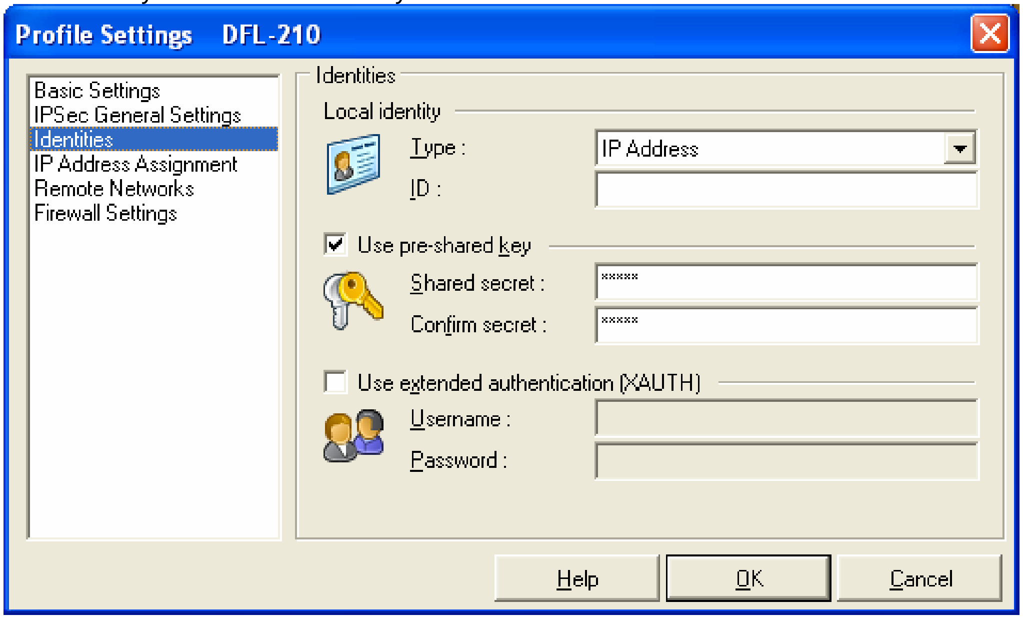
Remote Networks

Enter the IP networks the tunnel should be used for.
Without entries tunneling will always be used.

Network addresses :	Subnet masks :
192.168.1.0	255.255.255.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

□ Apply tunneling security for local networks

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.



Profile Settings DFL-210

Identities

Local identity

Type : IP Address

ID :

☑ Use pre-shared key

Shared secret : *****

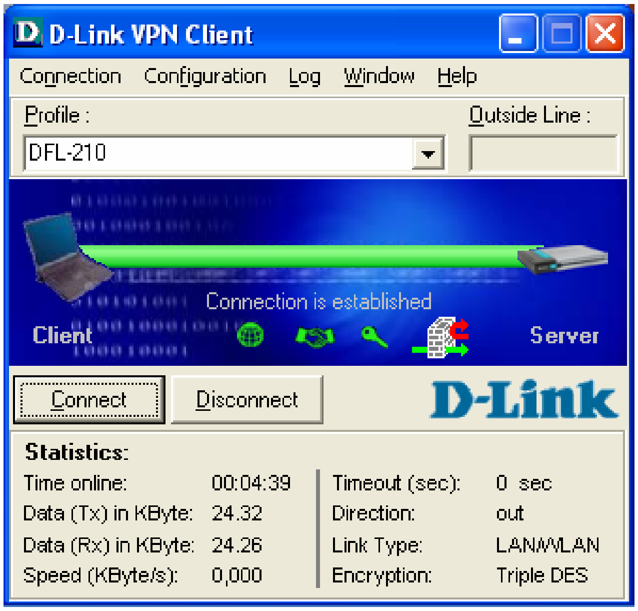
Confirm secret : *****

☐ Use extended authentication (XAUTH)

Username :

Password :

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



D-Link VPN Client

Profile : DFL-210

Outside Line :

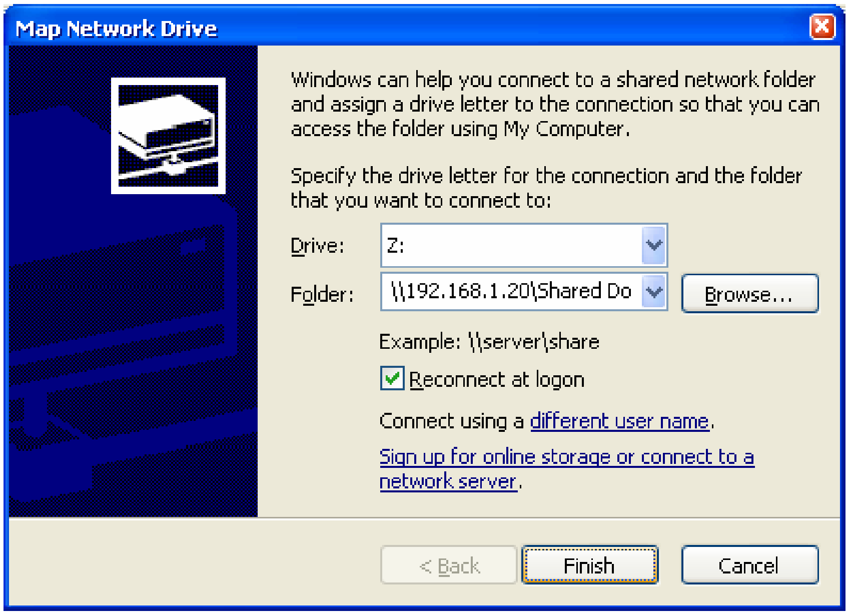
Connection is established

Statistics:

Time online:	00:04:39	Timeout (sec):	0 sec
Data (Tx) in KByte:	24.32	Direction:	out
Data (Rx) in KByte:	24.26	Link Type:	LAN/WLAN
Speed (KByte/s):	0,000	Encryption:	Triple DES

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):



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\192.168.1.20\Shared Do

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

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.