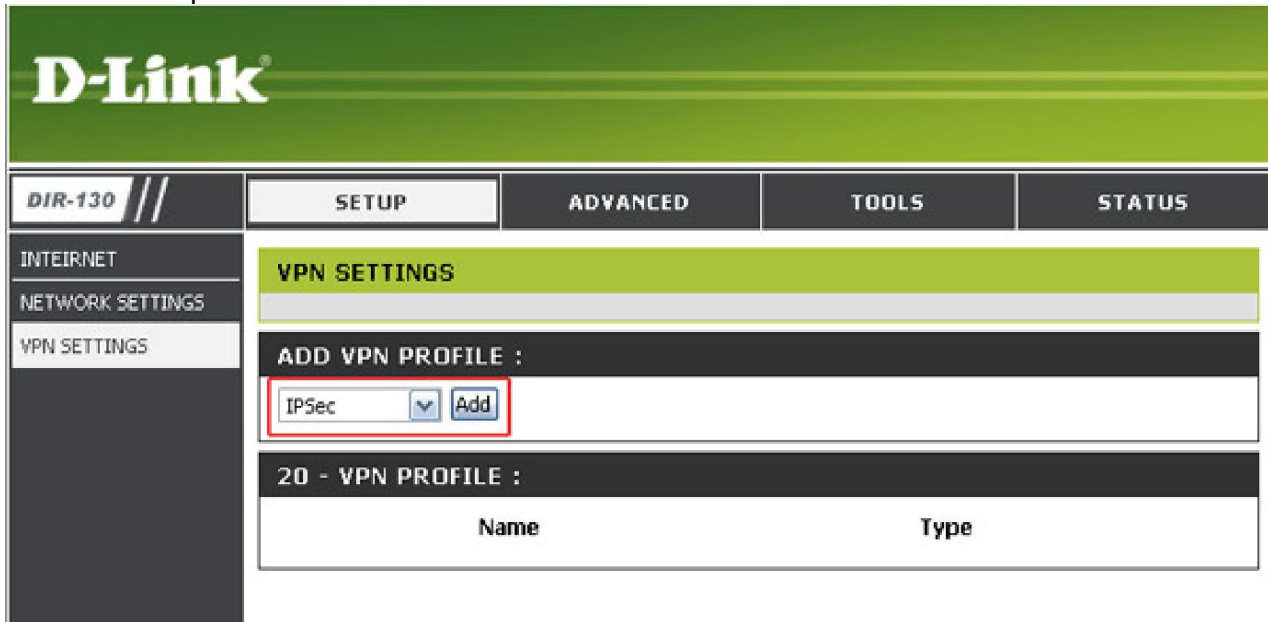


DS-60x VPN to DIR-130

Configuration of DIR-130

Step 1: Open your web browser and type in the IP address of the router (192.168.0.1 by default). Enter the username (*admin* by default) and password (blank by default), and then click **OK**.

Step 2: Click on **SETUP** and select **VPN SETTINGS**. Choose **IPSec** from the **ADD VPN PROFILE** dropdown menu and click **Add**.



The screenshot displays the D-Link DIR-130 web interface. The top navigation bar includes 'DIR-130', 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. The left sidebar shows 'INTERNET', 'NETWORK SETTINGS', and 'VPN SETTINGS'. The main content area is titled 'VPN SETTINGS' and contains the 'ADD VPN PROFILE' section. In this section, a dropdown menu is set to 'IPSec' and the 'Add' button is highlighted with a red box. Below this is a table titled '20 - VPN PROFILE' with columns 'Name' and 'Type'.

Name	Type
------	------

Step 3: Configure the *IPSec VPN* as followed:

- **Enable:** check box to enable
- **Name:** enter a name for the VPN
- **Local Net / Mask:** enter the local network and subnet mask
- **Remote IP:** select Remote User
- **Authentication:** enter your desired Pre-shared Key
- **Local ID:** leave as Default
- **Remote ID:** leave as Default
-
- **Phase 1 Main Mode:** selected
- **NAT-T Enable:** untick the box
- **Keep Alive / DPD:** select **none**
- **DH Group:** select **2-modp 1024-bit**
- **IKE Proposal List:**
- **Cipher #1:** select **3DES**
- **Hash: #1:** select **SHA**
- **IKE Lifetime:** enter **28800** (default)
-
- **Phase 2:**
- **PFS Enable:** tick the box (default)
- **PFS DH Group:** select **2-modp 1024-bit**
- **IPSec Proposal List:**
- **Cipher #1:** select **3DES**
- **Hash #1:** select **SHA1**
- **IPSec Lifetime:** enter **3600** (default)
- Click **Save Settings** then **Continue**



DIR-130	SETUP	ADVANCED	MAINTENANCE	STATUS
---------	-------	----------	-------------	--------

Internet
Network Settings
VPN Settings

VPN - IPSEC

User this section to create and configure your VPN-IPSec page.

IPSEC SETTING :

☒ Enable
Name :
Local Net /Mask :
Remote IP : ☒ Remote User ☐ Site to Site
Remote Local LAN Net /Mask :
Authentication : ☒ Pre-shared Key
☐ X.509 Certificate
Local Identity
Certificates
☐ XAUTH
☒ Server mode
Authentication database
☐ Client mode
User Name
Password
Local ID :
Remote ID :

PHASE 1 :

☒ Main mode ☐ Aggressive mode
NAT-T Enable: ☐
Keep Alive / DPD: ☒ none ☐ Keep Alive ☐ DPD (Dead Peer Detection)
DH Group :
IKE Proposal List :

Cipher	Hash
#1: 3DES	SHA
#2: 3DES	MD5
#3: 3DES	MD5
#4: 3DES	MD5

IKE Lifetime : Seconds

PHASE 2 :

PFS Enable: ☒ Perfect Forward Secrecy PFS
PFS DH Group :
IPSec Proposal List :

Cipher	Hash
#1: 3DES	SHA1
#2: 3DES	MD5
#3: 3DES	MD5
#4: 3DES	MD5

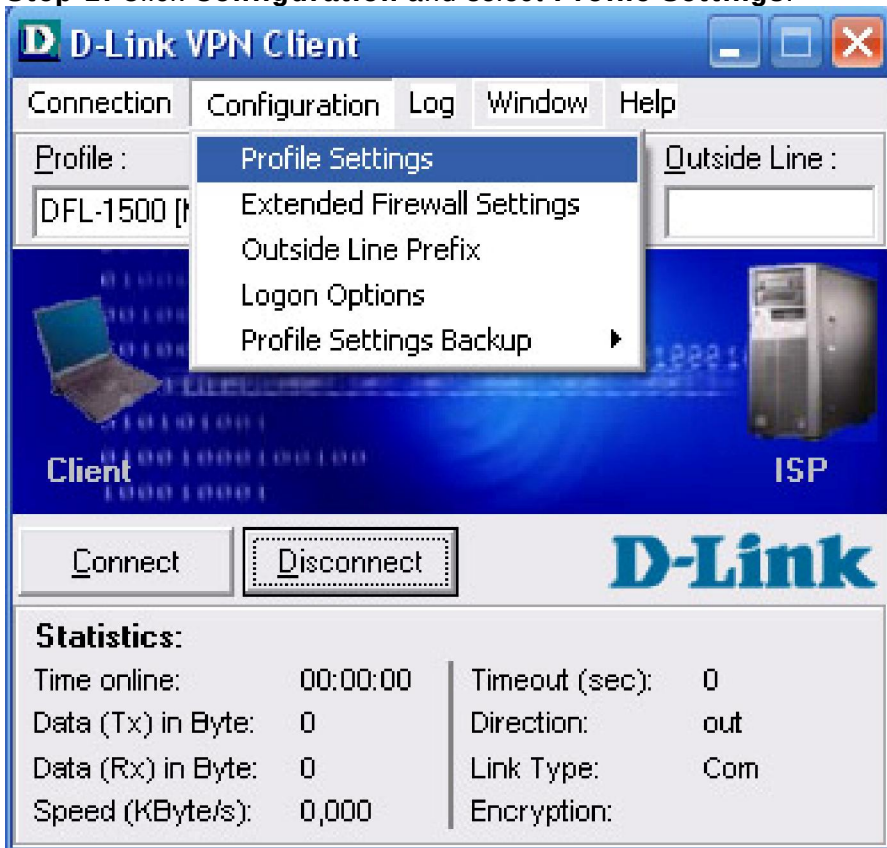
IPSec Lifetime : Seconds

The IPSec Tunnel should now appear in the **VPN PROFILE** list below.

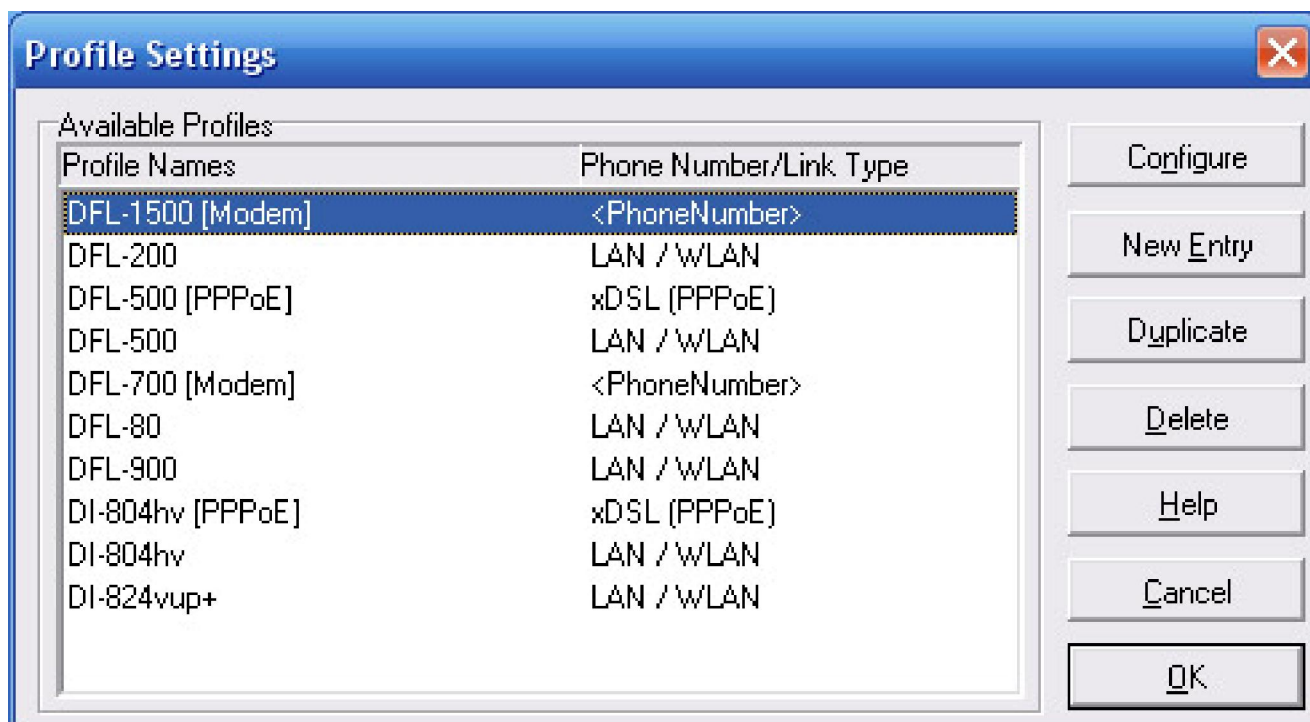
DIR-130	SETUP	ADVANCED	MAINTENANCE	STATUS								
Internet	VPN SETTINGS Use this section to create and configure your VPN settings.											
Network Settings	ADD VPN PROFILE : Select a type Add											
VPN Settings	25 - VPN PROFILE : <table border="1"> <thead> <tr> <th>Enable</th> <th>Name</th> <th>Type</th> <th></th> </tr> </thead> <tbody> <tr> <td>☒</td> <td>DIR-130_IPSec</td> <td>IPSEC</td> <td> </td> </tr> </tbody> </table>				Enable	Name	Type		☒	DIR-130_IPSec	IPSEC	 
Enable	Name	Type										
☒	DIR-130_IPSec	IPSEC	 									

Configuration of DS-601/605 client VPN software

Step 1: Click **Configuration** and select **Profile Settings**.



Step 2: Click **New Entry** to create a profile for the *DIR-130*.



Step 3: Name the profile *DIR-130* and click **Next**.



Assistant for new profile

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 :
DIR-130

< Back Next > Cancel

Step 4: Select the type of *Communication media* for the Local side and click **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)

< Back Next > Cancel

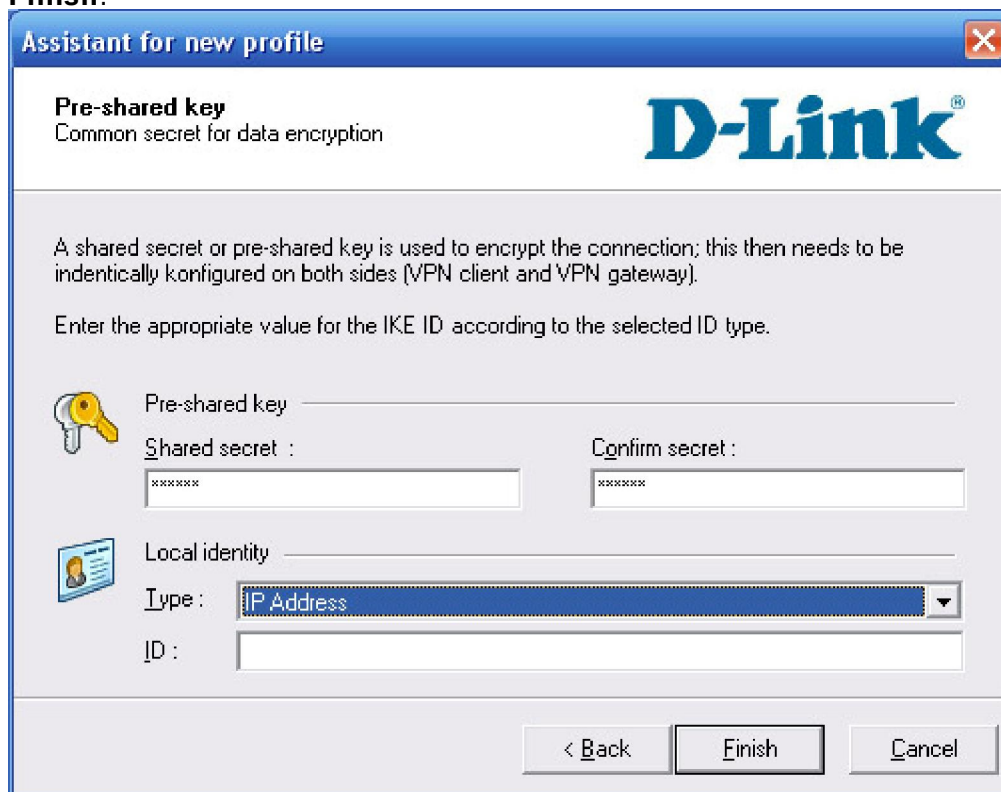
Step 5: Enter the *Remote Gateway* and click **Next**.

The IP can normally be found in the Status page of the DIR-130.



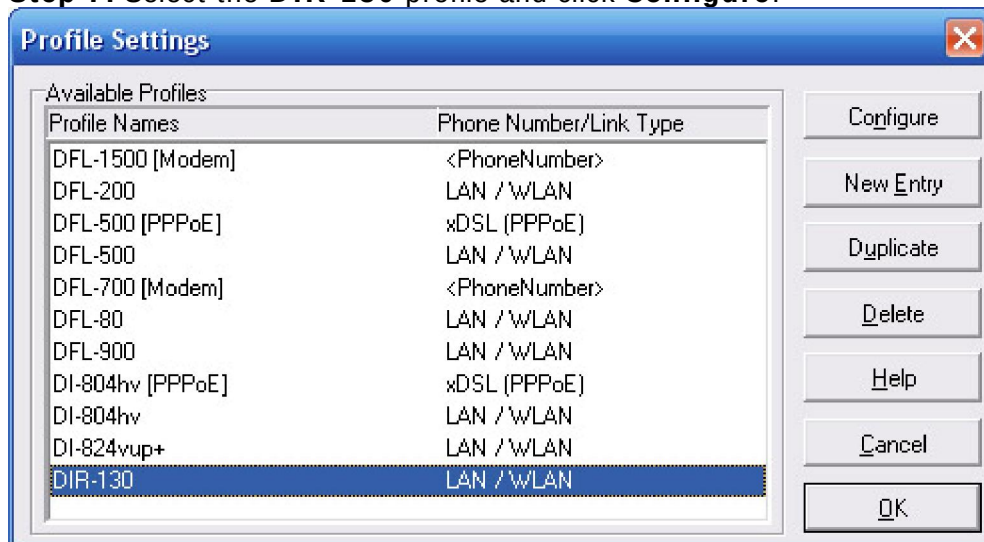
The screenshot shows a Windows-style dialog box titled "Assistant for new profile" with a close button (X) in the top right corner. The main heading is "VPN gateway parameters" with the subtext "To which VPN gateway should the connection be established". The D-Link logo is in the top right. Below the heading, there is instructional text: "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." The form includes a "Gateway:" label with a computer icon, a text box containing "68.140.140.140", a checkbox for "Use extended authentication (XAUTH)", a "Username:" label with a user icon, a text box, a "Password:" label, a text box, a "Password (Confirm):" label, and a text box. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Step 6: Enter the *Pre-shared Key* in both the **Shared secret** and **Confirm secret** and click **Finish**.

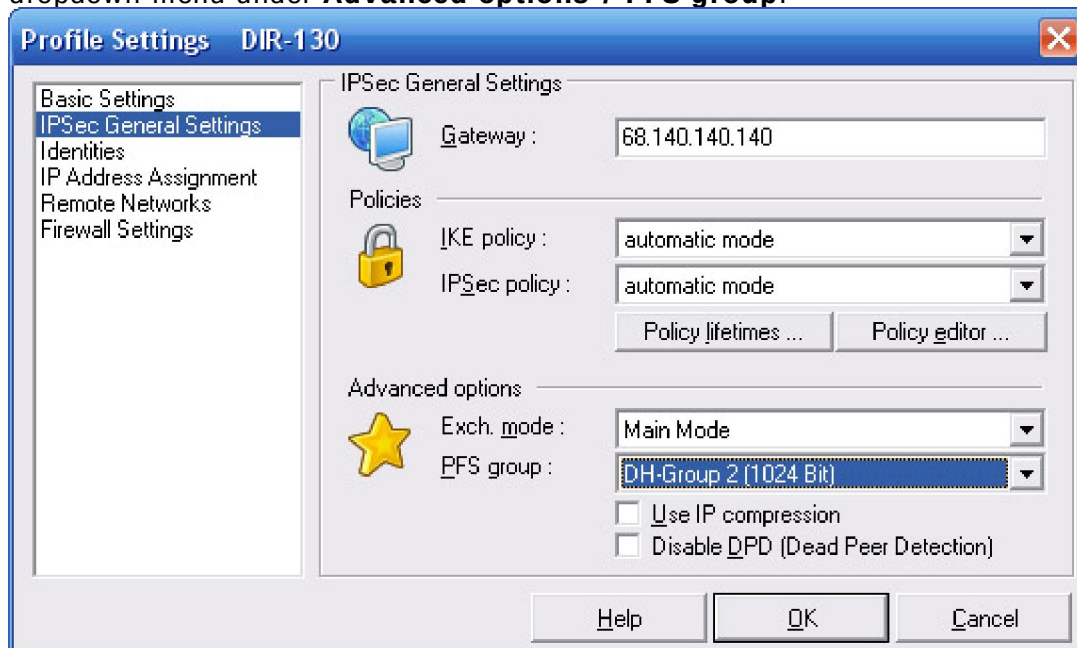


The screenshot shows the same "Assistant for new profile" dialog box, now at Step 6: "Pre-shared key" with the subtext "Common secret for data encryption". The D-Link logo is in the top right. Below the heading, there is instructional text: "A shared secret or pre-shared key is used to encrypt the connection; 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." The form includes a "Pre-shared key" label with a key icon, a text box, a "Shared secret:" label, a text box with "xxxxxx", a "Confirm secret:" label, and a text box with "xxxxxx". Below this is a "Local identity" label with a user icon, a "Type:" label, a dropdown menu showing "IP Address", and an "ID:" label with a text box. At the bottom are three buttons: "< Back", "Finish", and "Cancel".

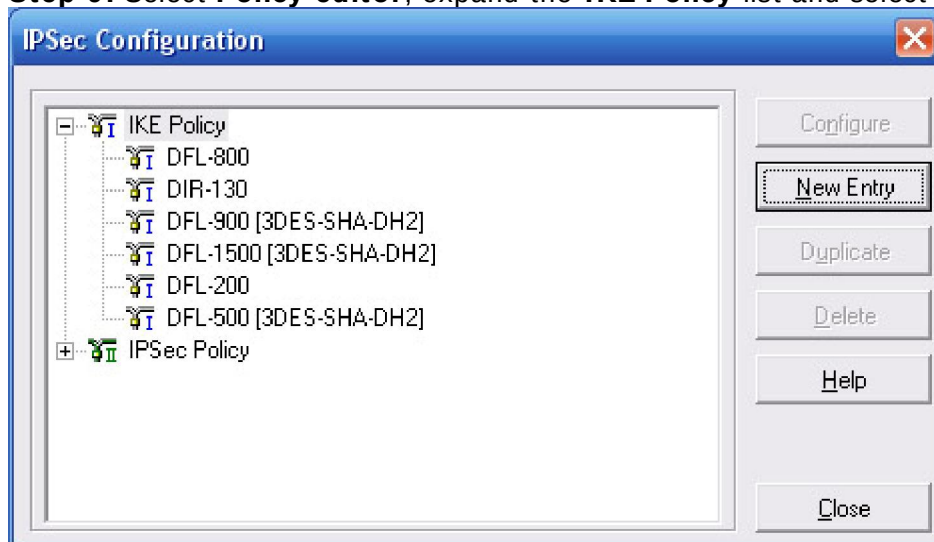
Step 7: Select the **DIR-130** profile and click **Configure**.



Step 8: Select **IPSec General Settings** and select **DH-Group 2 (1024 Bit)** from the dropdown menu under **Advanced options / PFS group**.



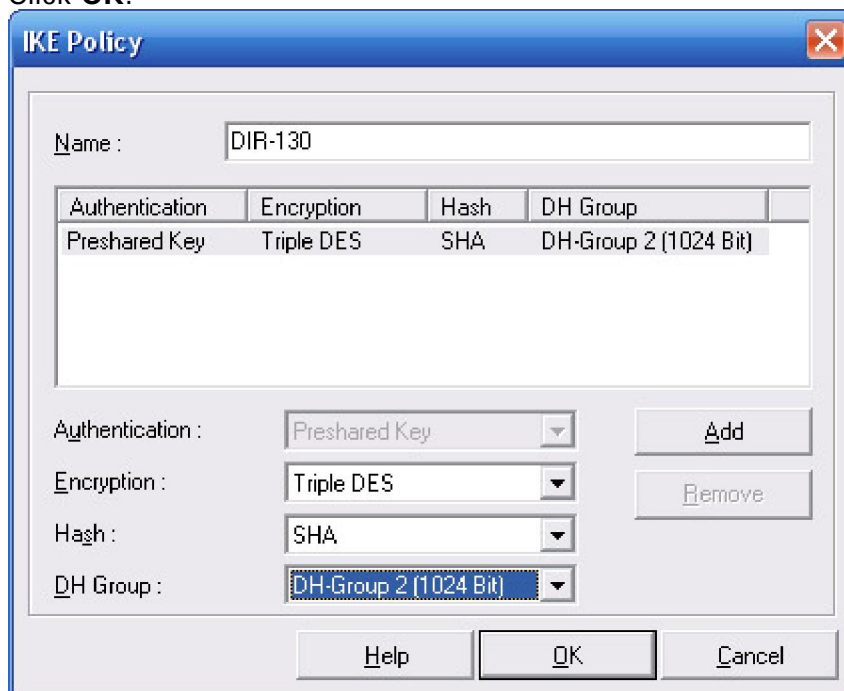
Step 9: Select **Policy editor**, expand the **IKE Policy** list and select **New Entry**.



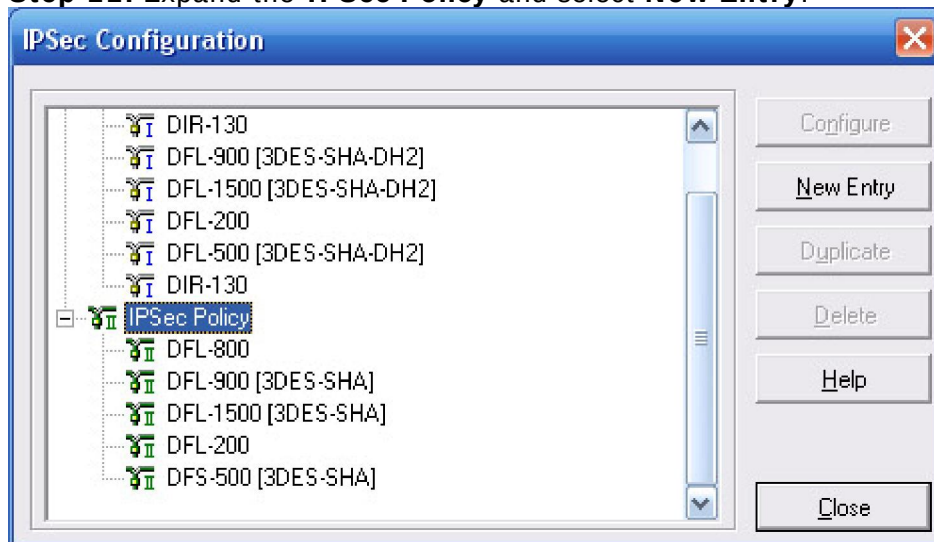
Step 10: Configure the *IKE Policy* as followed:

- **Name:** enter a name for the policy (*DIR-130* in this example)
- **Encryption:** *Triple DES*
- **Hash:** *SHA*
- **DH Group:** *DH-Group 2 (1024 Bit)*

Click **OK**.



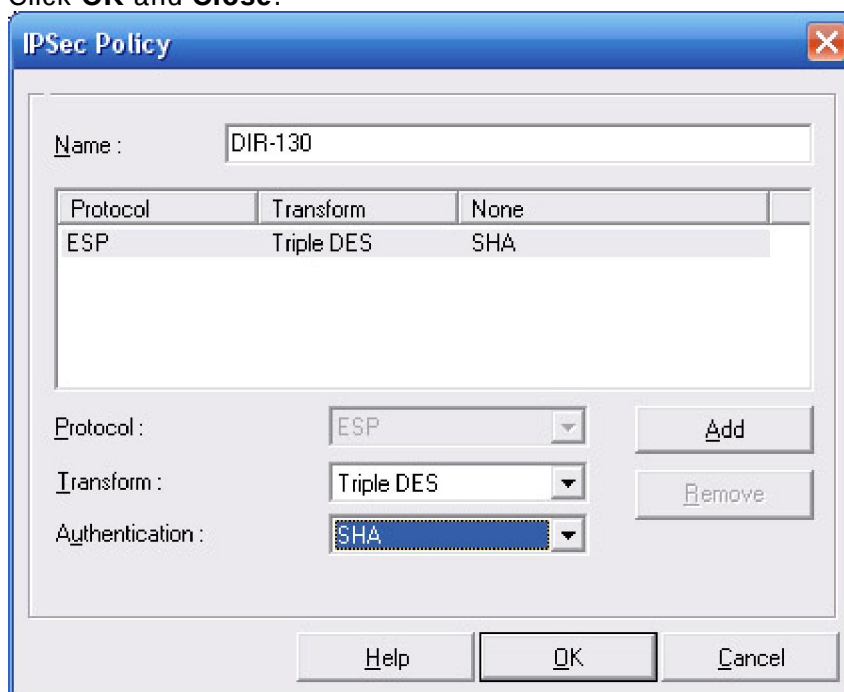
Step 11: Expand the **IPSec Policy** and select **New Entry**.



Step 12: Configure the *IPSec policy* as followed:

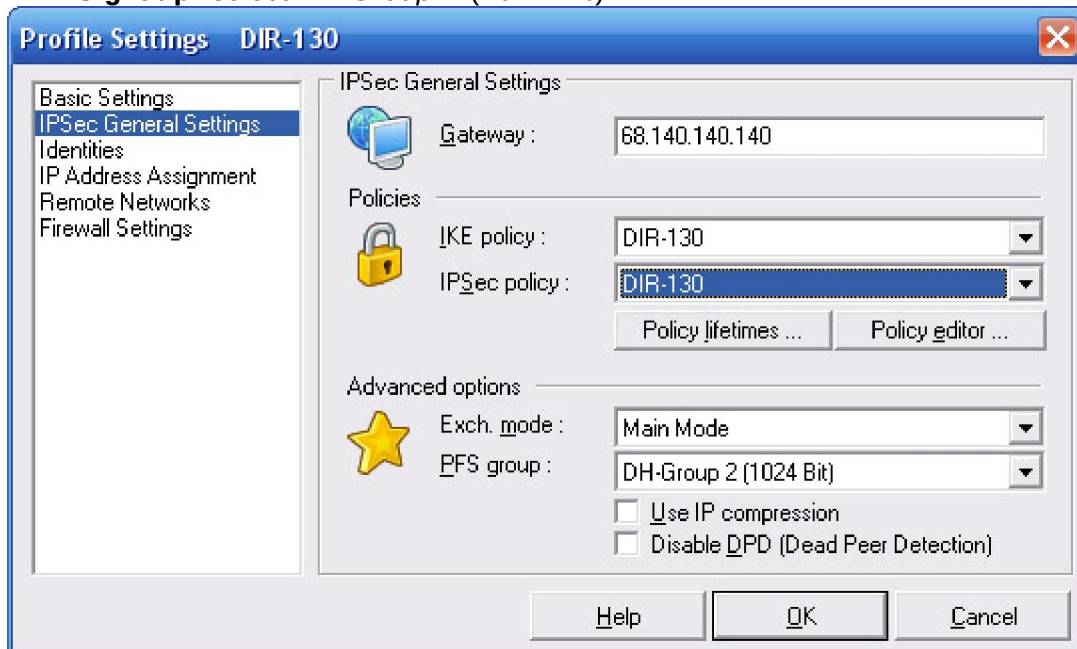
- **Name:** entry a name for the policy(*DIR-130* in this example)
- **Transform:** *Triple DES*
- **Authentication:** *SHA*

Click **OK** and **Close**.



Step 13: The **IPSec General Settings** should be configured as followed:

- **Gateway:** WAN IP address of the remote router
- **IKE policy:** select *DIR-130* from the dropdown menu
- **IPSec policy:** select *DIR-130* from the dropdown menu
- **Exch. mode:** select *Main mode*
- **PFS group:** select *DH-Group 2 (1024 Bit)*



The screenshot shows the 'Profile Settings' window for 'DIR-130'. The 'IPSec General Settings' tab is selected in the left sidebar. The main area contains the following settings:

- Gateway:** 68.140.140.140
- Policies:**
 - IKE policy:** DIR-130
 - IPSec policy:** DIR-130
 - Buttons: Policy lifetimes ..., Policy editor ...
- Advanced options:**
 - Exch. mode:** Main Mode
 - PFS group:** DH-Group 2 (1024 Bit)
 - ☐ Use IP compression
 - ☐ Disable DPD (Dead Peer Detection)

Buttons at the bottom: Help, OK, Cancel.

Step 14: Select **Identities** and enter the *pre-shared key* next to **Shared secret** and **Confirm secret**.



The screenshot shows the 'Profile Settings' window for 'DIR-130'. The 'Identities' tab is selected in the left sidebar. The main area contains the following settings:

- Local identity:**
 - Type:** IP Address
 - ID:** (empty field)
- ☒ **Use pre-shared key:**
 - Shared secret:** (masked with asterisks)
 - Confirm secret:** (masked with asterisks)
- ☐ **Use extended authentication (XAUTH):**
 - Username:** (empty field)
 - Password:** (empty field)

Buttons at the bottom: Help, OK, Cancel.

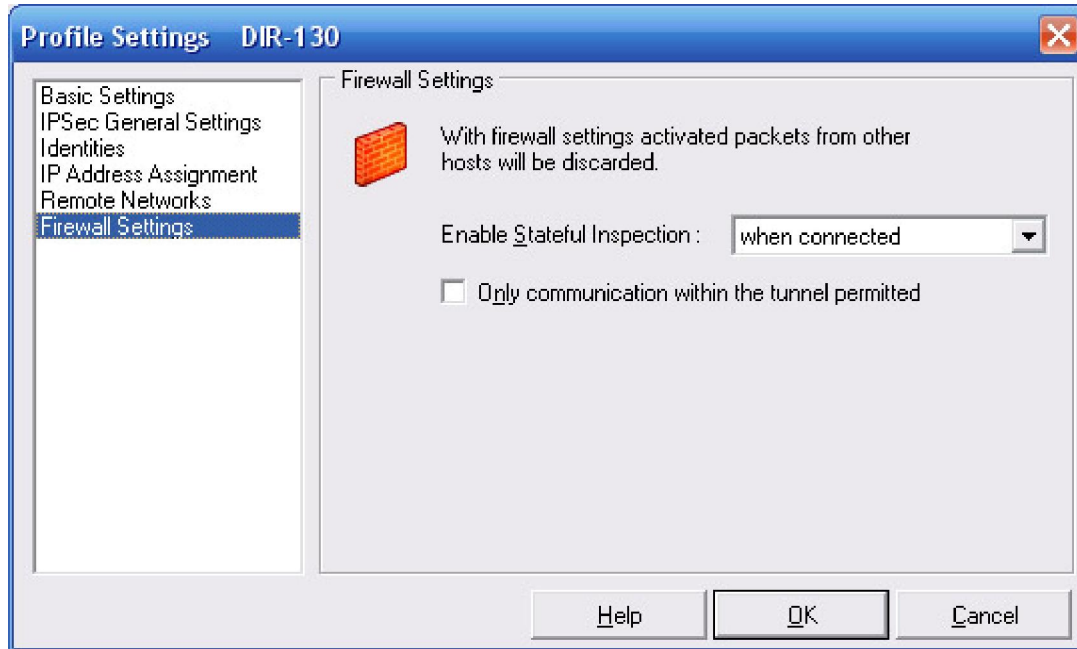
NOTE: The Preshared Key must be identical to the one configured on the router.

Step 15: Select **IP Address Assignment** and configure it according to your settings. It is recommended to keep the default settings.

Step 16: Select **Remote Networks** and configure as followed:

- **Network addresses:** enter the remote network (192.168.0.0 in this example)
- **Subnet masks:** enter the remote subnet mask (255.255.255.0 in this example)

Step 17: Select **Firewall Settings** and set the *Enable Stateful Inspection* to **when connected**. Click **OK** to save the settings and then click **OK** again to go back to the connection screen.



Step 18: Click **Connect** to establish the VPN connection to the router.

