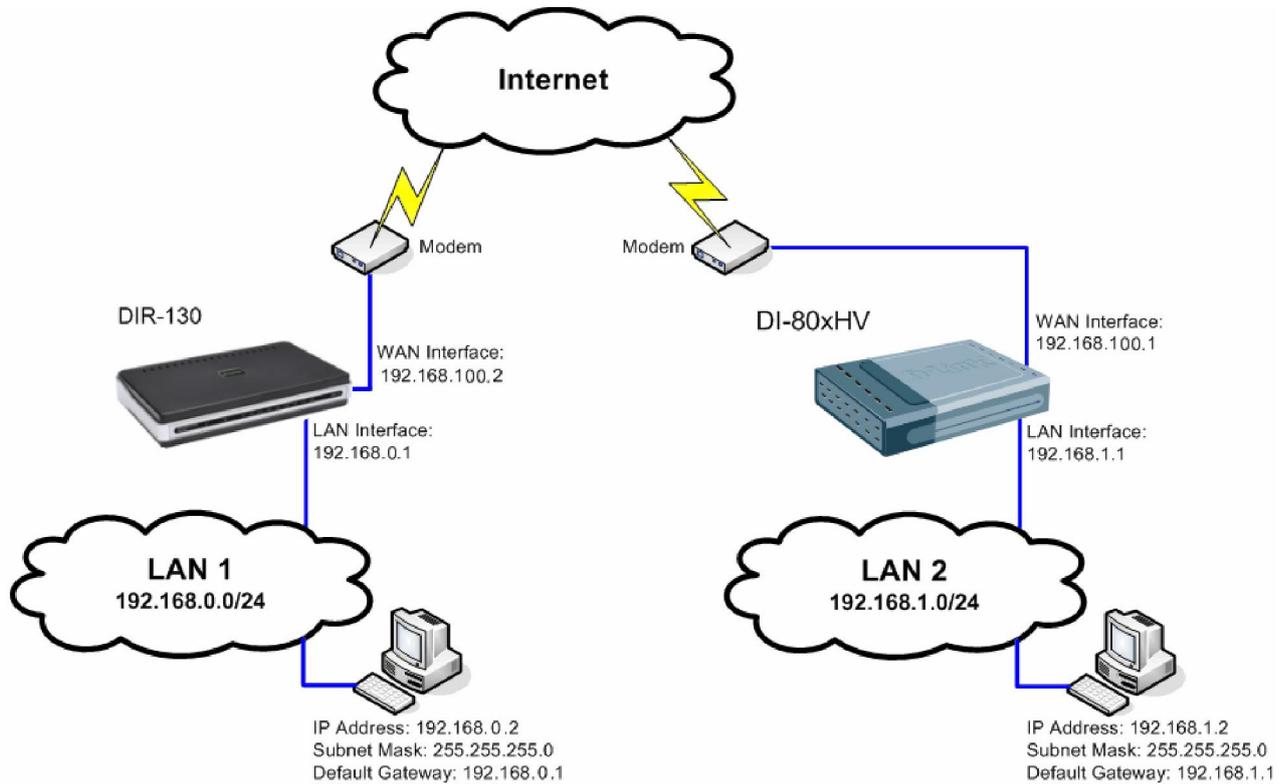


How to setup an IPSec VPN connection between a DIR-130 and DI-80xHV

This setup example uses the following network settings:



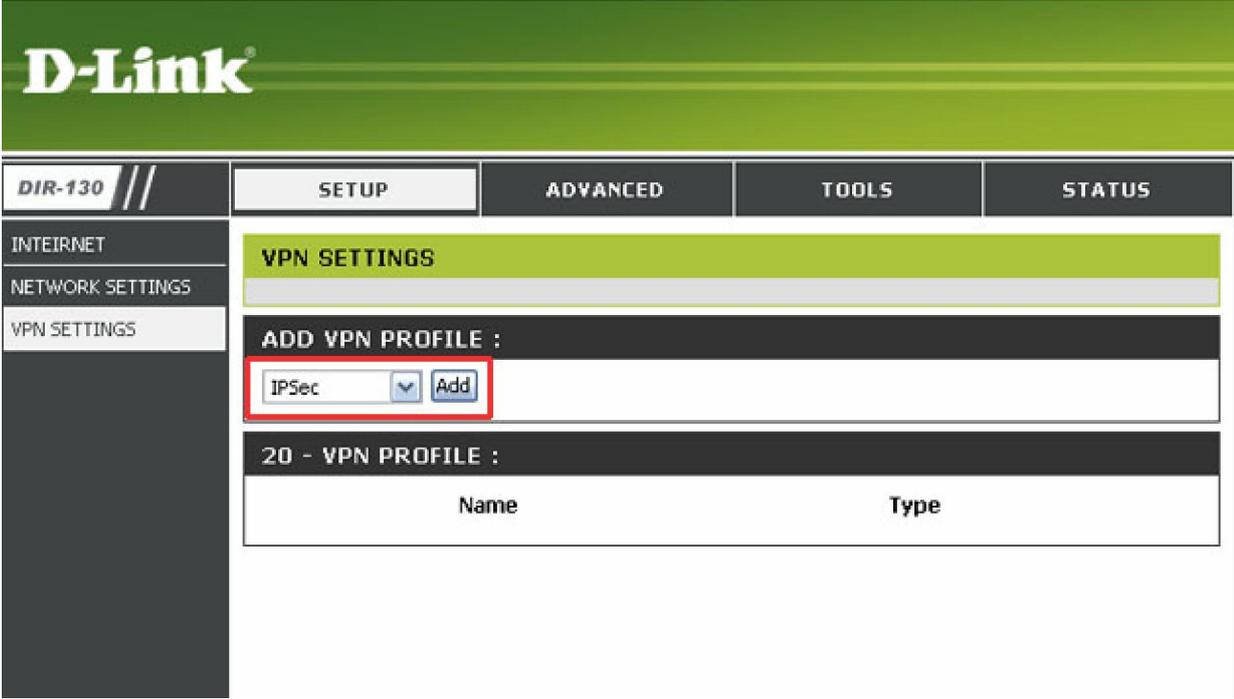
In our example the IPSec VPN tunnel is established between two LANs: 192.168.0.x and 192.168.1.x.

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

Configuration of the DIR-130

Step 1. Log into the DIR-130 by opening Internet Explorer and typing the LAN address of the device. In our example we are using the default 192.168.0.1. Enter Username and Password which you specified during the initial setup of the Firewall.

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



The screenshot displays the D-Link DIR-130 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for 'DIR-130', 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. The 'SETUP' tab is active, and the left sidebar shows 'VPN SETTINGS' selected. The main content area is titled 'VPN SETTINGS' and contains the following elements:

- ADD VPN PROFILE :** A dropdown menu showing 'IPSec' and an 'Add' button, both highlighted with a red rectangular box.
- 20 - VPN PROFILE :** A table with two columns: 'Name' and 'Type'.

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

IPSEC SETTING

- **Enable:** check box to enable
- **Name:** enter a name for the VPN
- **Encapsulation Mode::** Tunnel
- **Remote IP:** select Site to Site and enter the remote gateway
- **Remote Local LAN Net /Mask:** enter the remote network and remote subnet mask

Authentication: enter a Pre-shared Key (Pre-share key must match remote side)

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

- **IKE Proposal List:** leave at default (*3DES, SHA1*)

PHASE 2

- **IPSec Proposal List:** leave at default (*3DES, SHA1*)

Click **Save Settings**.

PHASE 1 :

Main mode Aggressive mode

NAT-T Enable:

Keep Alive / DPD: none Keep Alive DPD (Dead Peer Detection)

DH Group : 2 - modp 1024-bit ▼

IKE Proposal List :

Cipher

#1: 3DES ▼

#2: 3DES ▼

#3: 3DES ▼

#4: 3DES ▼

Hash

MD5 ▼

MD5 ▼

MD5 ▼

MD5 ▼

IKE Lifetime : 28800 Seconds

PHASE 2 :

PFS Enable: Perfect Forward Secrecy PFS

PFS DH Group : 2 - modp 1024-bit ▼

IPSec Proposal List :

Cipher

#1: 3DES ▼

#2: 3DES ▼

#3: 3DES ▼

#4: 3DES ▼

Hash

MD5 ▼

MD5 ▼

MD5 ▼

MD5 ▼

IPSec Lifetime : 3600 Seconds

Configuration of DI804HV/808HV

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**.

In our setup we changed the IP of the unit to 192.168.1.1 (NOTE both routers can not be on the same subnet).

Step 2: Click on the **Home** tab and select the **VPN** button and configure as followed:

- **VPN:** check to enable
- **Max. number of tunnels:** enter the number of tunnels
- **ID 1**
- **Tunnel Name:** enter a name of the VPN
- **Method:** select IKE

Click **Apply** to save the settings.

The screenshot displays the D-Link VPN configuration page. On the left sidebar, the 'VPN' button is highlighted in yellow. The main panel shows the 'VPN Settings' section with the following configuration:

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

ID	Tunnel Name	Method
1	test	IKE [More]
2		IKE [More]
3		IKE [More]
4		IKE [More]
5		IKE [More]

At the bottom of the interface, there are navigation buttons: 'Previous page', 'Next page', 'Dynamic VPN Settings..', 'L2TP Server Setting..', 'PPTP Server Setting..', and 'View VPN Status..'. At the bottom right, there are three action buttons: 'Apply' (with a green checkmark icon), 'Cancel' (with an orange 'X' icon), and 'Help' (with a red plus icon).

Step 3: Click on **More** under **Method** and configure as followed:

Tunnel Name: the name of the tunnel should already be entered if done in the previous step

- **Local Subnet:** enter the local subnet (192.168.0.0 in this example)
- **Local Netmask:** enter the local subnet mask(255.255.255.0 in this example)
- **Remote Subnet:** enter the remote subnet (192.168.1.0 in this example)
- **Remote Netmask:** enter the remote subnet mask(255.255.255.0 in this example)
- **Remote Gateway:** enter the remote gateway (172.68.140.140 in this example)
- **IKE Keep Alive (Ping IP Address):** enter an IP address of a client on the remote side (192.168.1.100 in this example)
- **Preshare Key:** enter preshare key as desired (*Pre-share key* must match remote side)
- **IPSec NAT Traversal:** check to enable
- **Auto-reconnect:** check to enable

Click **Apply** to save the settings and click **Continue** when prompted.

Item	Setting
Tunnel Name	test
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.0.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.100.2
IKE Keep Alive (Ping IP Address)	192.168.0.1
Preshare Key
Extended Authentication (xAUTH)	<input type="checkbox"/> Enable <input type="checkbox"/> Server mode <input type="button" value="Set Local user..."/> <input type="checkbox"/> Client mode
User Name	<input type="text"/>
Password	<input type="text"/>
IPSec NAT Traversal	<input type="checkbox"/> Enable
Auto-reconnect	<input type="checkbox"/> Enable
Remote ID	Type: IP Address Value: <input type="text"/>
Local ID	Type: IP Address Value: <input type="text"/>
IKE Proposal Index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal Index	<input type="button" value="Select IPSec Proposal..."/>

Back Apply Cancel Help

Step 4: Click on **Select IKE Proposal** and configure as followed:

- **Proposal Name:** enter a name for the *Proposal ID Number 1*
- **DH Group:** *Group 2*
- **Encrypt algorithm:** *3DES*
- **Authentication Algorithm:** *SHA1*
- **Life Time:** *28800*
- **Life Time Unit:** *Sec*
- **Proposal ID:** select *1* and click on **Add To** to add to the **IKE Proposal index**

Click **Apply** and then click **Back**.

D-Link
Building Networks for People

DI-808HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1 - Set IKE Proposal

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

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE	Group 2	3DES	SHA1	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Proposal ID 1 Proposal index

Step 5: Click on **Select IPSec Proposal** and configure as followed:

- **Proposal Name:** enter a name for *Proposal ID Number 1*
- **DH Group:** *Group 2*
- **Encapsulation Protocol:** *ESP*
- **Encryption Algorithm:** *3DES*
- **Authentication Algorithm:** *SHA1*
- **Life Time:** *3600*
- **Life Time Unit:** *Sec.*
- **Proposal ID:** select *1* and click on **Add To** to add to the **IPSec Proposal index**

Click **Apply** and then click **Continue** when prompted.

D-Link
Building Networks for People

DI-808HV
Broadband VPN Router

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

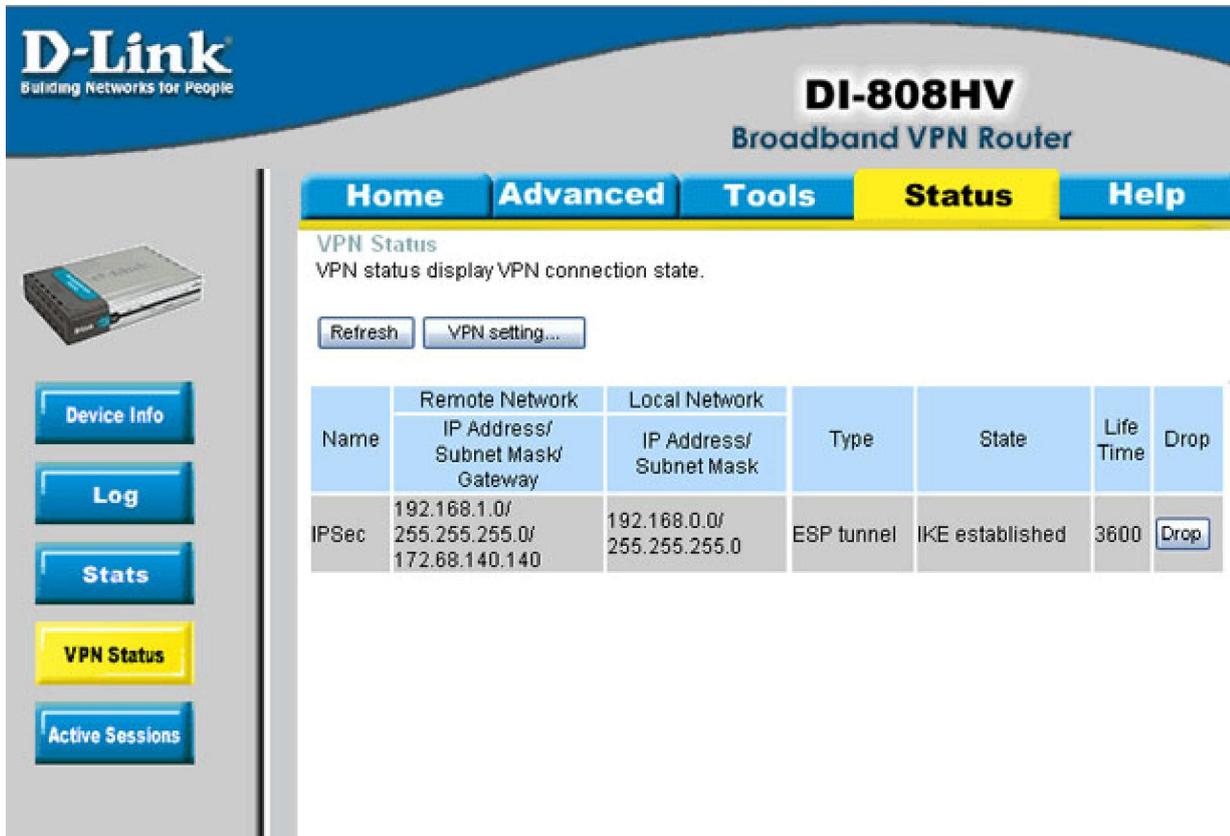
VPN Settings - Tunnel 1 - Set IPSEC Proposal

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

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IPSec	Group 2	ESP	3DES	SHA1	3600	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 1 Proposal index

Step 6: Click on the **Status** tab and select the **VPN Status** button. The VPN should be established. If the tunnel has not been established, click on the **Refresh** button or ping to an IP address on the remote side. When replies are sent back, the tunnel has been established.



D-Link
Building Networks for People

DI-808HV
Broadband VPN Router

Home Advanced Tools **Status** Help

VPN Status
VPN status display VPN connection state.

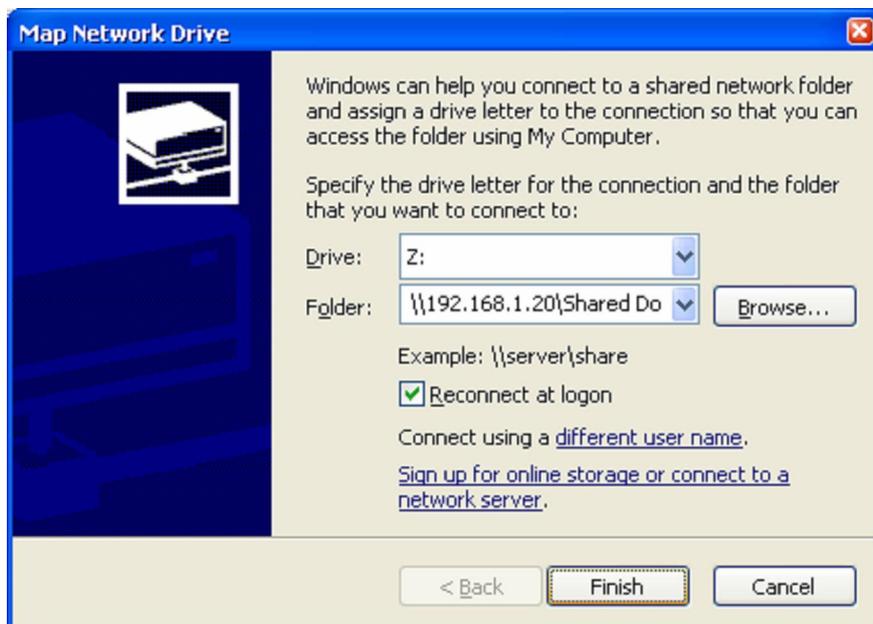
Refresh VPN setting...

Name	Remote Network	Local Network	Type	State	Life Time	Drop
	IP Address/ Subnet Mask/ Gateway	IP Address/ Subnet Mask				
IPSec	192.168.1.0/ 255.255.255.0/ 172.68.140.140	192.168.0.0/ 255.255.255.0	ESP tunnel	IKE established	3600	Drop

Device Info
Log
Stats
VPN Status
Active Sessions

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.