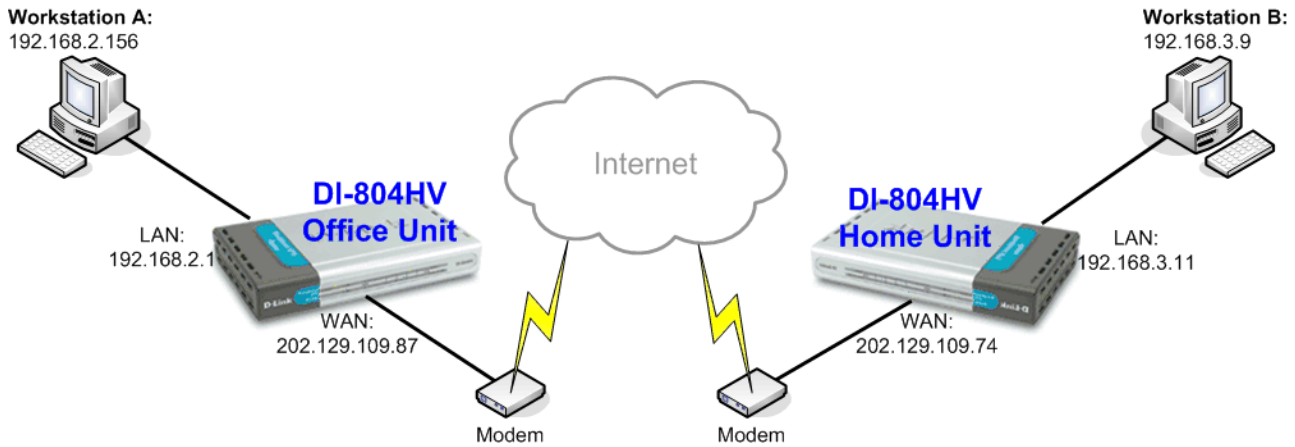


Setting up VPN connection: SSH to DI-804HV

Date: 28 Nov 2003

Doc version: 3.0

Author: Neil Stent



Client router: DI-624+ (Firmware 1.01)

LAN IP: 192.168.0.1 Subnet Mask: 255.255.255.0

WAN IP: 202.129.109.87 Subnet Mask: 255.255.255.224

Default Gateway: 202.129.109.65

Workstation A:

IP: 192.168.0.156 Subnet Mask: 225.255.255.0

Default Gateway: 192.168.0.1

Office: DI-804HV (firmware 1.34)

LAN IP: 192.168.3.11 Subnet Mask: 255.255.255.0

WAN IP: 202.129.109.74 Subnet Mask: 255.255.255.224

Default Gateway: 202.129.109.65

Workstation B:

IP: 192.168.3.157 Subnet Mask: 225.255.255.0

Default Gateway: 192.168.3.11

Please note:

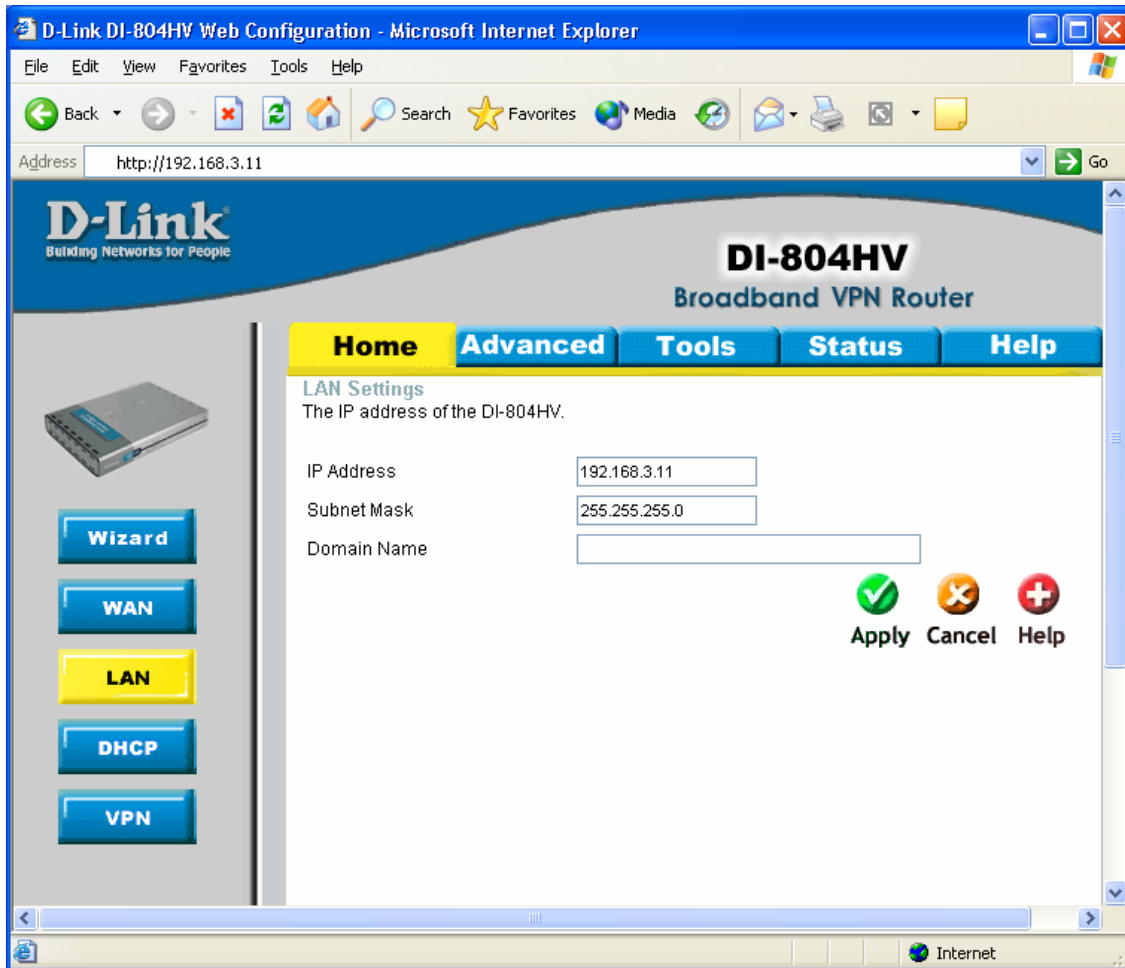
For any IPsec VPN connection you need to make sure that the LAN IP subnets on each location are different. As you can see in the above example the LAN IP of the Office DI-804HV is 192.168.2.1 and the Home DI-804HV is 192.168.3.1. If you had a third location it should be 192.168.4.x, etc... (where x is any number from 1 to 254).

If you are using DSL-300, DSL-300+, DSL-302G modem or DSL-500, DSL-504, DSL-604+ router please see **Appendix 3** at the end of this document.

Office DI-804HV Settings:

Log into the router's WEB interface and go to Home > LAN. Change the IP address of the LAN port of the router to required IP.

Once you have changed the LAN IP address on the router, make sure your PC has an IP address from the same subnet (192.168.3.x in this example), you may just need to renew IP on your PC or reboot.



Next go to the Home > WAN page, choose the type of connection your ISP requires. In our example it is Static IP Address.

You need to have a static IP address the on WAN port of at least one unit out of two participating in VPN connection. Some PPPoE connections have a static IP as well (in most of such cases you do not have to specify the IP – your ISP will be providing you with the same IP every time you connect).

After setting up the WAN port click on Apply to save settings.

The screenshot displays the D-Link DI-804HV Broadband VPN Router web configuration interface. The browser window title is "D-Link DI-804HV Web Configuration - Microsoft Internet Explorer" and the address bar shows "http://192.168.3.11". The page features a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". The "Home" tab is active, and the "WAN" button in the left sidebar is highlighted. The "WAN Settings" section prompts the user to select a connection type. The "Static IP Address" option is selected, and the "Static IP Address" section contains the following fields:

IP Address	202.129.109.74
Subnet Mask	255.255.255.224
ISP Gateway Address	202.129.109.65
Primary DNS Address	202.129.64.198
Secondary DNS Address	139.134.5.51
MTU	1400
Auto-backup	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

At the bottom right, there are three buttons: "Apply" (with a green checkmark icon), "Cancel" (with a yellow 'X' icon), and "Help" (with a red '+' icon). The status bar at the bottom of the browser window shows "Done" and "Internet".

Next make sure you can access the Internet (that will confirm that you have set WAN settings correctly), then log back into the router and go into Home > VPN.

Make sure you have VPN Enable box ticked.

In the Max number of tunnels section, enter the number of tunnels needed (e.g. 2).

Then click on “Dynamic VPN Setting” button.

D-Link DI-804HV Web Configuration - Microsoft Internet Explorer

Address: http://192.168.3.11

DI-804HV Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	<input type="text" value="2"/>

ID	Tunnel Name	Method
1	<input type="text"/>	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

Apply Cancel Help

On the Dynamic VPN Tunnel page enter the required information:

Tunnel Name, this is the name to describe the tunnel.

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

Preshare Key: this can be anything up to 31 characters long (write down this key as you will need it when configuring the SSH Software).

Then click Apply, then click on “Select IKE Proposal...”

D-Link DI-804HV Web Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.3.11

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Dynamic VPN Tunnel

Item	Setting
Tunnel Name	test
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	192.168.3.0
Local Netmask	255.255.255.0
Preshare Key	test
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Back Apply Cancel Help

Done Internet

Below is the example how you can setup IKE Proposal.

We used the following settings:

ID 1, Name: test, Group 1, 3DES, SHA1, 3600, Sec

D-Link DI-804HV Web Configuration - Microsoft Internet Explorer

Address: http://192.168.3.11

D-Link Building Networks for People

DI-804HV Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 0 - Set IKE Proposal

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

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 1	3DES	SHA1	3600	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 -- select one --

Click Apply, then click on Back.

Click on "IPSec Proposal" and you should see a page similar to the one below. Configure it the same way as on the IKE Proposal page, then click Apply.

The screenshot shows the D-Link DI-804HV Web Configuration interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.3.11>. The page title is "D-Link DI-804HV Web Configuration - Microsoft Internet Explorer". The main header displays the D-Link logo and "DI-804HV Broadband VPN Router".

The navigation menu includes "Home", "Advanced", "Tools", "Status", and "Help". The "Advanced" tab is selected, and the sub-page is "VPN Settings - Tunnel 0 - Set IPSEC Proposal".

On the left sidebar, there are buttons for "Wizard", "WAN", "LAN", "DHCP", and "VPN" (highlighted in yellow). Above the "VPN" button is an image of the DI-804HV router.

The main content area shows the "IPSec Proposal index" with a text input field containing "test" and a "Remove" button. Below this is a table of IPsec proposals:

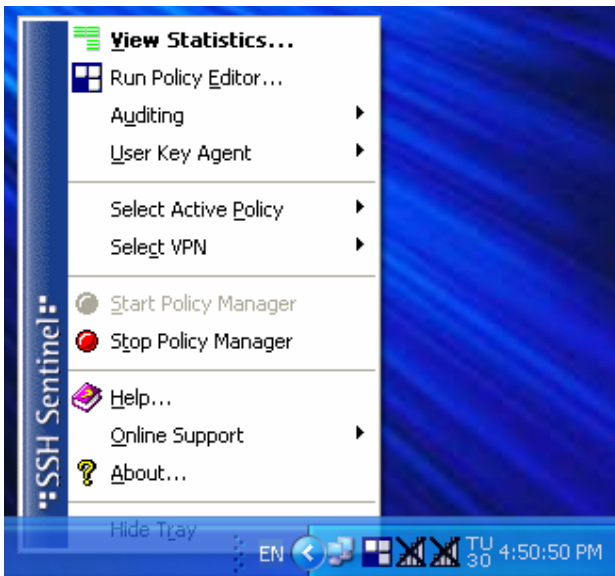
ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 1	ESP	3DES	SHA1	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

At the bottom of the table, there is a "Proposal ID" dropdown menu (set to "-- select one --") and an "Add to Proposal index" button. Below the table are four action buttons: "Back", "Apply", "Cancel", and "Help".

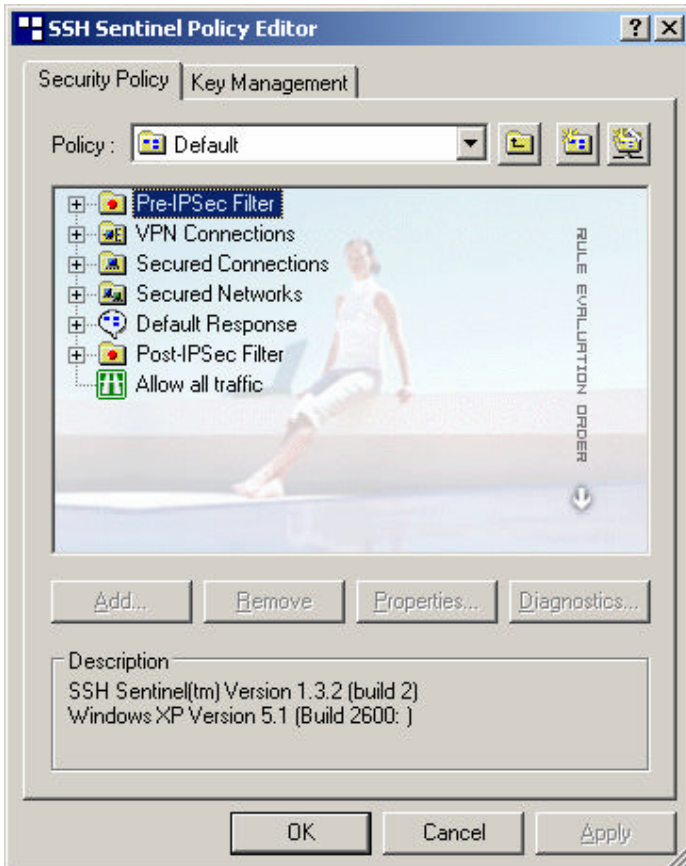
This is all you need to do to configure the Office Unit. Now you need to setup the Home Unit. The setup will be almost the same as on the DI-804HV Office Unit.

Home SSH VPN Connection settings:

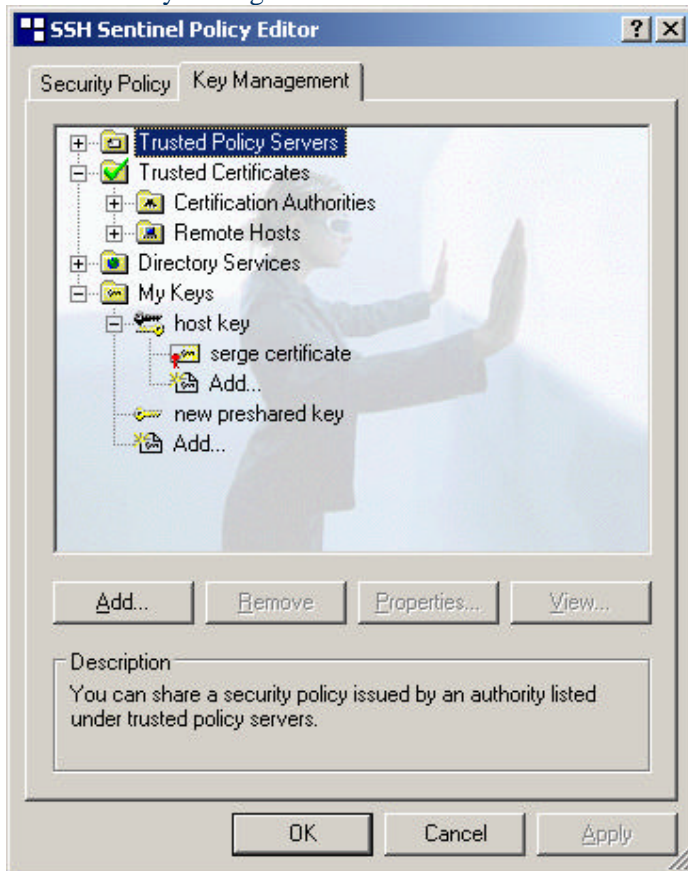
1. After you installed the SSH Sentinel client and restarted your computer, the client will start automatically, the SSH Sentinel taskbar sign will appear
2. Move your mouse to the SSH Sentinel sign at the taskbar and press the right mouse button
3. You will see the following menu:



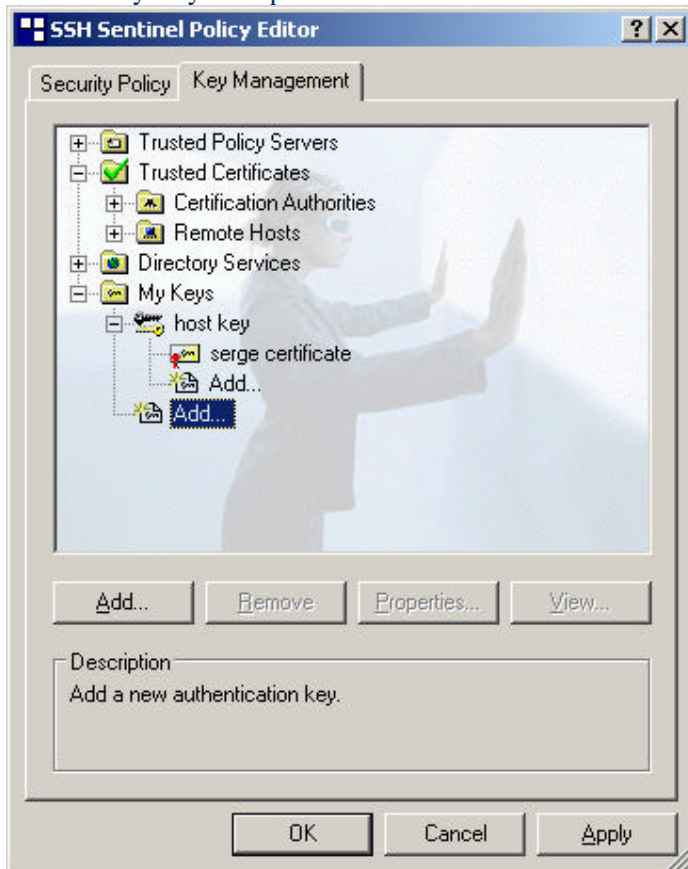
3. Choose Run Policy Editor and click on it
4. You will get into the following menu:



5. Choose Key Management bookmark:



6. Go to My Keys and press "Add" :



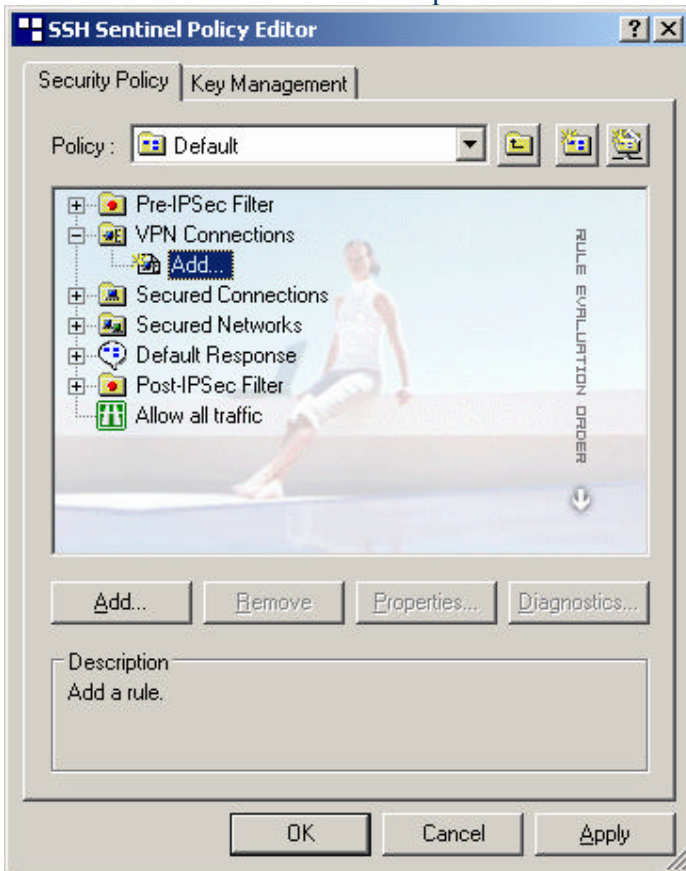
7. Choose “Create Pre-Shared Key” and click “Next”:



8. Give a name to the key and put exactly the same key you used in “Authentication Key” field of D-Link DFL-500 Firewall, press “Finish”

9. The key is now created and you can go back to the “Security Policy” bookmark

10. Choose “VPN Connections” and press “Add”:



11. On the “Gateway IP address” field press “IP” and put the external ip address of your firewall, for example 202.129.97.105

12. Press “...” button in “Remote Network” field

13. Press “New” and create a network with your internal network address, for example 192.168.0.0 255.255.255.0:

14. Press “OK” and select “key” in “Authentication Key” field:

15. Check on “Use legacy proposal” and press “OK”

16. The VPN Connection is now created

17. Choose the VPN connection, we have just created and press “Properties”

18. You will get the following menu:

19. Click “Settings” under the “Proposal template” field, you will get this:

20. Choose the IKE and IPSec modes you would like to use and click “OK”

21. Choose “Advanced” bookmark and press “Settings”:

22. Choose lifetime, so it would correspond to the lifetime specified in DFL -500 configuration. The defaults for DFL-500 are 28800 seconds for Phase 1 (IKE) and 300 seconds for Phase 2 (IPSec):

23. Go back to the main “Security Policy” window and press “Apply” and “OK” again. Don’t forget to “Apply” every time you change your VPN connection properties or security policy

24. The basic configuration of SSH Sentinel VPN client is now over

25. You can check you Pre-IPSec and Post-IPSec Filters to be sure that all the ports needed for your work are opened and the rest of the ports are closed. SSH Sentinel VPN client is actually working as a firewall on the client side

26. Now you are ready to connect your client to the office network

III. Connecting SSH Sentinel VPN Client to the Office network

1. Make sure your client has a connection to internet
2. In SSH Sentinel Policy Editor choose the VPN connection you have created and press “Diagnostics”
3. You will see the client trying to connect to D-Link DFL-500 Firewall
4. If the diagnostics is successful, you will see the following message:
5. Click on “Details” to check which authentication and encryption modes are chosen for IKE and IPSec:

6. Now you can connect your client to your office network

7. Click right mouse button on SSH Sentinel taskbar sign and choose "Select VPN"

8. Select the connection you have created, for example 202.129.97.105 (D-Link) and click on it, you will see the following window:

9. When the connection is done, you will see the following message:

10. The message disappears in a few seconds, that means that your VPN connection is now established (Not Responding is normal here, since Sentinel closes the window itself).

11. Now you can open Command Prompt from Start/Programs/Accessories menu in Windows
12. Check if you have a connection to your office network by “pinging” of the office computers:

13. If you get the replies from your office computer that means that the VPN connection to your office network works and you can start using the office network as you are connected directly to it
14. Congratulations! You have successfully created the VPN Connection from SSH Sentinel VPN Client to your Office network through D-Link DFL-500 Firewall!

Appendix 1.
How to test your VPN connection.

Make sure that computers on both locations can access the Internet.

To bring the VPN tunnel up you just need to try to access any IP address on the network at the remote location, pinging the other location is the easiest way.

To do this go to **Start > Run**, type *command* and click on OK.

Depending on what location you are at will depend on what you type in.

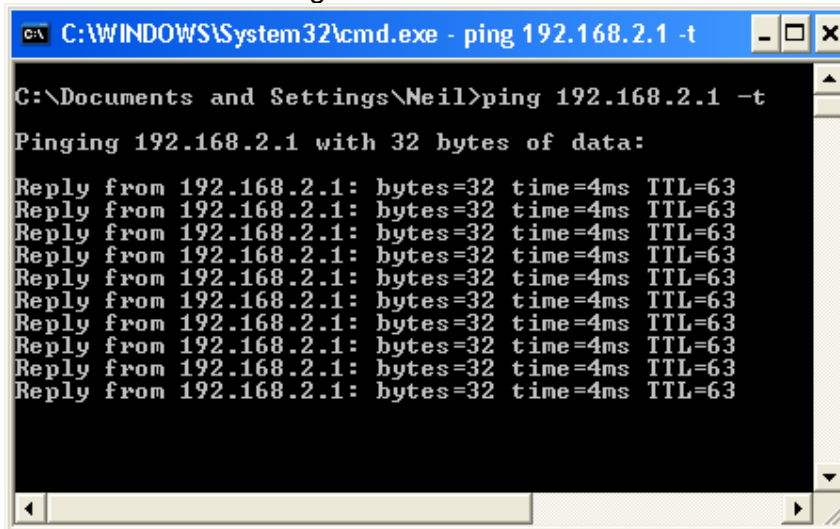
If you are located on the 192.168.2.x side (Office) type in the following and press Enter (this will ping the IP of the Home Unit):

```
ping 192.168.3.11 -t
```

Or if your location is network with 192.168.3.x (Home) type:

```
ping 192.168.2.1 -t
```

You should see messages similar to the ones below:



```
C:\WINDOWS\System32\cmd.exe - ping 192.168.2.1 -t
C:\Documents and Settings\Neil>ping 192.168.2.1 -t
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
Reply from 192.168.2.1: bytes=32 time=4ms TTL=63
```

If you see a message saying Reply from... that means that VPN tunnel has been established successfully and you can communicate with remote network via VPN.

If you now log into the DI-804HV and go into Status > Log you can see the VPN connection log.

The screenshot shows a Microsoft Internet Explorer browser window displaying the web management interface of a D-Link DI-804HV Broadband VPN Router. The address bar shows the URL `http://192.168.3.11/`. The interface features a navigation menu with tabs for Home, Advanced, Tools, Status, and Help. The 'Status' tab is selected, and the 'Log' sub-tab is active. The main content area displays the VPN connection log, which includes the following text:

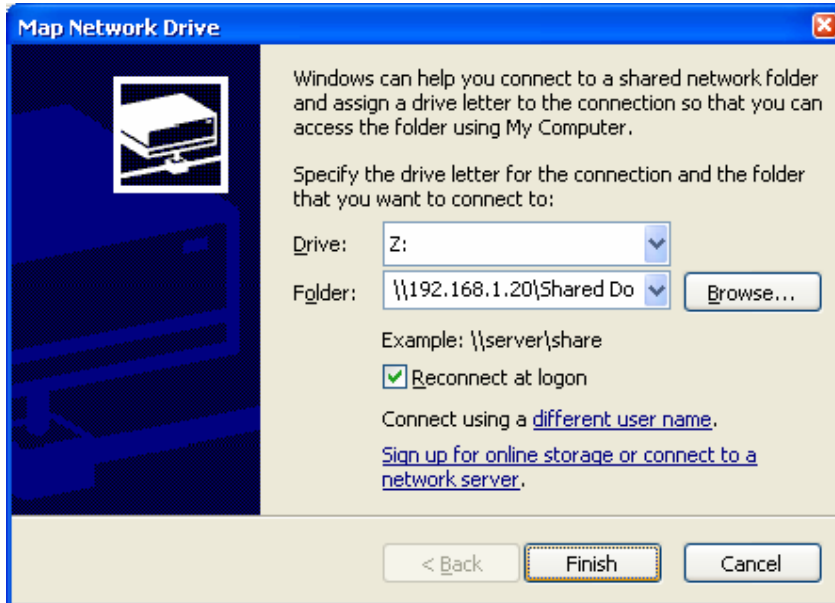
WAN Type: Static IP Address (V1.34)
Display time: Tue Oct 21 00:00:14 2003

*Send IKE M1(INIT) : 202.129.109.74 --> 202.129.109.87
Tuesday, 21 October 2003 12:00:01 AM Receive IKE M1(INIT) : 202.129.109.87 --> 202.129.109.74
Tuesday, 21 October 2003 12:00:01 AM Try to match with ENC:DES AUTH:PSK HASH:SHA1 Group:Group1
Tuesday, 21 October 2003 12:00:01 AM Send IKE M2(RESPI) : 202.129.109.74 --> 202.129.109.87
Tuesday, 21 October 2003 12:00:01 AM Receive IKE M3(KEYINIT) : 202.129.109.87 --> 202.129.109.74
Tuesday, 21 October 2003 12:00:01 AM Send IKE M4(KEYRESP) : 202.129.109.74 --> 202.129.109.87
Tuesday, 21 October 2003 12:00:01 AM Receive IKE M5(IDINIT) : 202.129.109.87 --> 202.129.109.74
Tuesday, 21 October 2003 12:00:01 AM Send IKE M6(IDRESP) : 202.129.109.74 --> 202.129.109.87
Tuesday, 21 October 2003 12:00:01 AM IKE Phase1 (ISAKMP SA) established : 202.129.109.74 <-> 202.129.109.87
Tuesday, 21 October 2003 12:00:02 AM Receive IKE Q1(QINIT) : [202.129.109.87]--> [202.129.109.74]
Tuesday, 21 October 2003 12:00:02 AM Requested routing is [192.168.2.0|202.129.109.87]<-> [202.129.109.74|192.168.3.0]
Tuesday, 21 October 2003 12:00:02 AM Try to match with MODE:Tunnel PROTOCOL:ESP-DES AUTH:SHA1 HASH:Others PFS(Group):Group1
Tuesday, 21 October 2003 12:00:02 AM Send IKE Q2(QRESP) : 192.168.3.0 --> 192.168.2.0
Tuesday, 21 October 2003 12:00:02 AM Receive IKE Q3(QHASH) : [192.168.2.0|202.129.109.87]--> [202.129.109.74|192.168.3.0]
Tuesday, 21 October 2003 12:00:02 AM IKE Phase2 (IPSEC SA) established : [192.168.2.0|202.129.109.87]<-> [202.129.109.74|192.168.3.0]
Tuesday, 21 October 2003 12:00:02 AM inbound SPI = 0x2000010, outbound SPI = 0x2000010

Appendix 2

Connecting to remote computers/drives via VPN

You can map remote computers' drives 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. Or use the methods described above. Note that firewall/antivirus software installed on your or remote computer may stop you from accessing shared folders.

Appendix 3

Note to DSL-300, DSL-300+, DSL-302G modems users and DSL-500, DSL-504, DSL-604+ users.

If you are using **DSL-300** to connect your DI-804HV to the Internet please avoid using **192.168.1.x** addresses on your networks as it is the temporary subnet used by the modem.

If you are using **DSL-300+** to connect your DI-804HV to the Internet please avoid using **192.168.0.x** addresses on your networks as it is the temporary subnet used by the modem. Also note that DSL-300+ links to the MAC address of the device connected to it directly. So if you configured the modem while it was connected to your PC directly or to another router, you will need to reconfigure it while it is connected to your DI-804HV. Here are the steps:

1. Connect the DSL-300+ modem to the WAN port of your DI-804HV.
2. Set WAN port on DI-804HV to "Dynamic IP" and set LAN port to subnet different from 192.168.0.x (e.g. 192.168.3.1)
3. Renew IP address on your computer so it will be on 192.168.3.x subnet and log into the DSL-300+ using your Internet browser: <http://192.168.0.1>
4. In the DSL-300+ interface select **Account Management**. Put a tick next to your account and click on **Delete**.
5. Select **Account Configuration** and reconfigure the modem according to your ISP requirements. Click on **OK** to save settings.

If you are using **DSL-500, DSL-504, DSL-604+** router to connect your DI-804HV to the Internet please avoid using **192.168.0.x** addresses on your networks as it is the default LAN subnet used by the routers. You may change it to a different subnet (e.g. 192.168.33.1) if you wish, under **Configuration > Ethernet IP**.

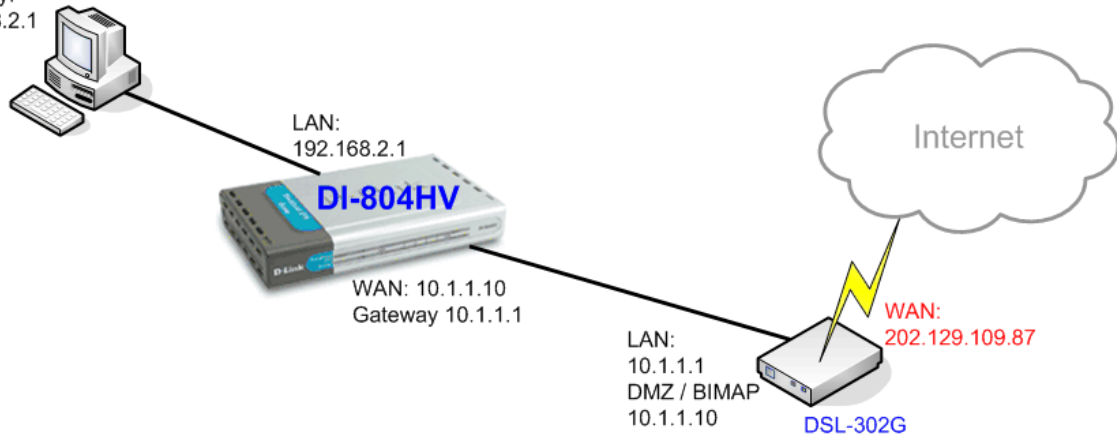
Note that you need to enable VPN passthrough on the router. Or go to **NAT Configuration** and enable **DMZ**: specify the IP address of the WAN port of DI-804HV there.

DI-804HV WAN port should be set with static IP from the same subnet as DSL-xxx LAN port. Default Gateway should be set as DSL-xxx LAN port IP address.

Please keep in mind that with DSL-xxx routers with NAT enabled your public IP address will be located on the WAN port of DSL-xxx router. WAN port of DI-804HV will have private IP address. When setting up **Remote Gateway** in VPN you will need to use public IPs on DSL-xxx routers' WAN ports, e.g. 202.129.109.87 (see example with DSL-302G below).

With **DSL-302G** the setup is similar. This modem uses **10.1.1.1** address on LAN.

Workstation A:
192.168.2.156
Gateway:
192.168.2.1



In order to enable VPN traffic passthrough in this modem you need to do the following:
Log into the modem's WEB interface and select **WAN > NAT**. Under **NAT Options** select **NAT Rule Entry**. Click on **Add** button.
Under **Rule Flavor** select **BIMAP**. Set **Rule ID** as next number in the rules table (in our case it is 2). **IF Name** = **ALL**. **Local Address** will be the IP on the WAN port of your DI-804HV which is connected to this modem. **Global address** leave as 0.0.0.0:

NAT Rule - Add

NAT Rule Information				
Rule Flavor:	BIMAP <input type="button" value="v"/>			
Rule ID:	2 <input type="text"/>			
IF Name:	ALL <input type="button" value="v"/>			
Local Address:	10	1	1	10
Global Address:	0	0	0	0

Copyright © 2002 D-Link, Inc. All rights reserved.

Then click on **Submit** to apply the settings.

When setting up **Remote Gateway** in **VPN** you will need to use public IP on DSL-302G's WAN port.

D-Link Australia & NZ Technical Support Team can be contacted on +61 2 88991800 or support@dlink.com.au

~ End of Document ~