Configuring VPN connection using SSH Sentinel VPN Client and D-Link DI-804V VPN Router

I. Configuring D-Link DI-804V VPN Router

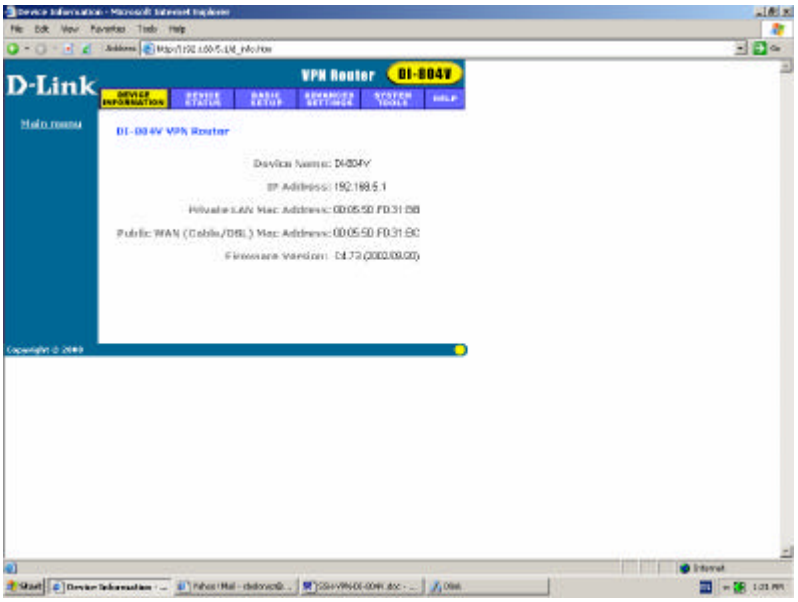
First of all you should login into your D-Link VPN Router. Please connect your PC to any of the Ethernet ports of the VPN Router.

By default the IP address of DI-804V is 192.168.0.1 255.255.255.0, thus you should configure your PC, so it would be in the same subnet as VPN router, for example you can configure it for the IP address of 192.168.0.2 255.255.255.0 and default gateway of 192.168.0.1. The default gateway should always point to VPN Router. You can also use the dynamic IP settings on your PC, so VPN Router will give you the address automatically.

Try to ping the VPN Router to check if your PC can communicate with VPN Router. If ping is unsuccessful, that probably means that your VPN Router is configured with some other IP address. In order to get the Router back to default settings press Factory Reset button on the back of unit. After resetting, the IP address of the unit will be 192.168.0.1 255.255.255.0.

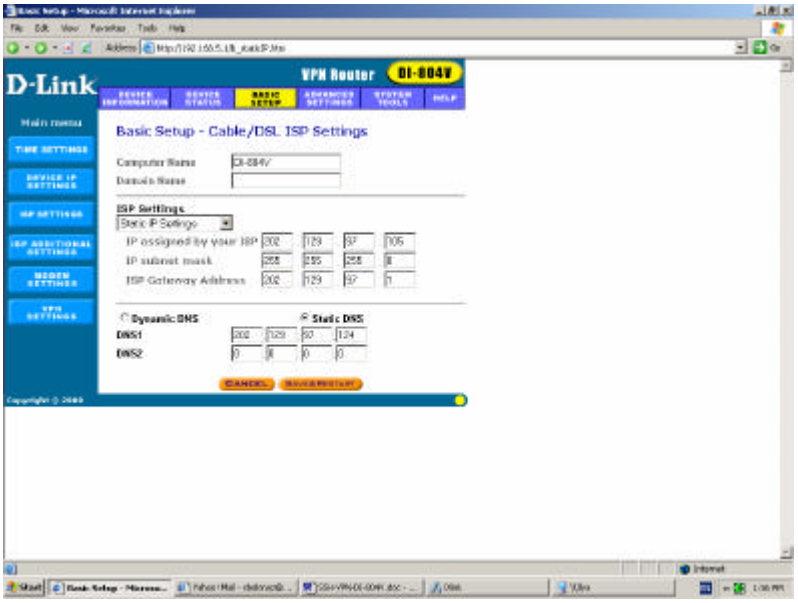
Now you should open your Internet Explorer and type http://192.168.0.1 in the Address bar. The login prompt will appear. You should use the login name “admin” and leave the password blank. You can set up the password later on. If you cannot log into the Router with blank password, that means that the password was changed. You should Factory Reset the unit in order to login into it. After you have logged in, you will see the following screen:

Now, let's go to the Device Information. You will see the following screen there:

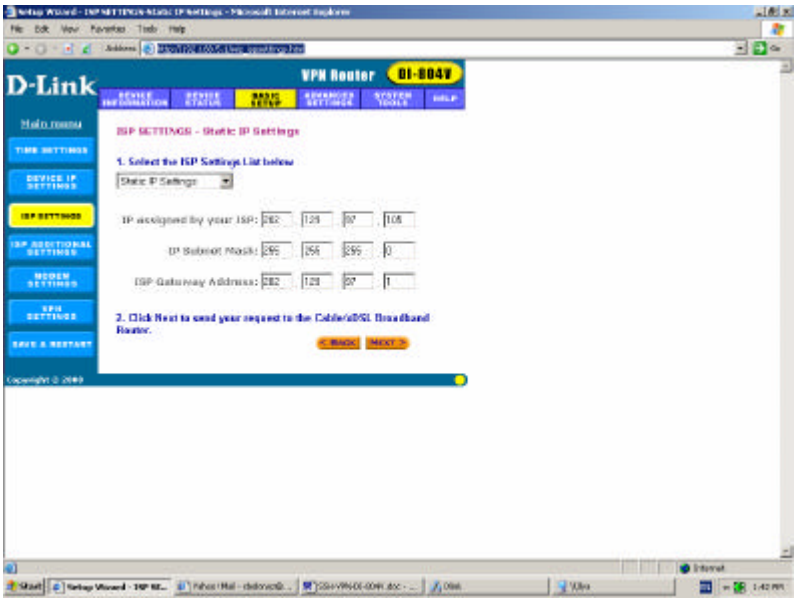


You will see the device name, IP address of the unit, Private and Public MAC addresses as well as firmware version. It is always recommended that you use the latest firmware available. By the time of this writing the latest firmware version available is 4.73.

Now you should go to the Basic Setup menu and configure Cable/DSL ISP Settings. It can be a Static IP, PPPoE, PPTP or Telstra. For PPPoE, PPTP and Telstra you must specify the user name and the password. Let's configure a static IP for our example. We will use the IP address of 202.129.97.105 255.255.255.0 for our WAN interface and the default gateway of 202.129.97.1 255.255.255.0. For DNS server we use 202.129.97.124. Your Internet service provider must give your IP address, default gateway address and DNS server address. When you are done with Static IP configuration, you will see the following screen:

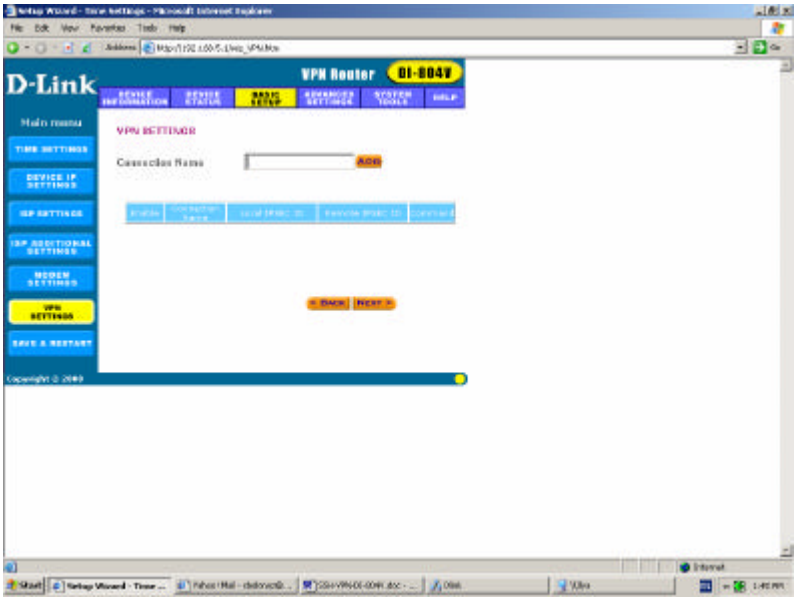


Click Save & Restart, so the unit will save the new ISP settings. After the unit is restarted, go to the Basic Setup again. Choose ISP Settings, you will see the following screen:



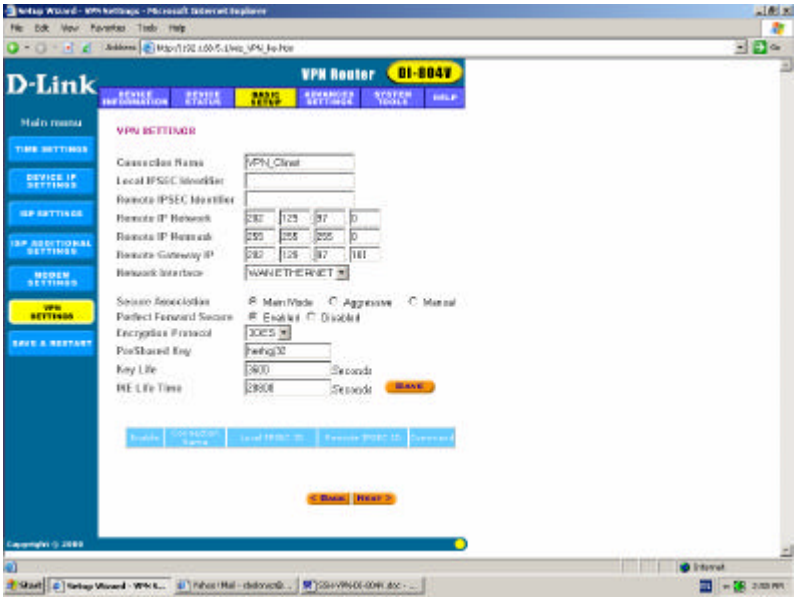
Click Next, so your VPN Router will to access Cable/xDSL Broadband Router. The connection is established now and we can go to the next step. If you have problems with the connection, check the IP (PPPoE, PPTP, Telstra) settings with your Internet service provider.

Let's go to VPN settings menu now:



Type the name of your new VPN connection and click Add. We will use VPN_Client for our example. In the next menu, you will be asked for Remote IP settings. Put the IP address of Remote Network, i.e. the network from which the clients will be connecting. If you want many clients from the same network to connect to your VPN Router, then leave Remote Gateway field blank. Otherwise, you must specify the static IP address of your client. If your client gets the IP dynamically, than you should also leave this field blank.

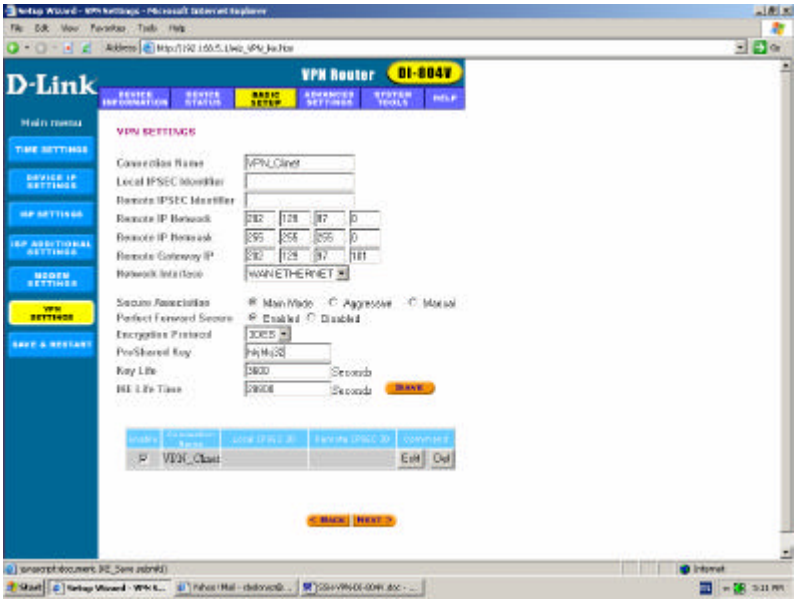
Let's look at what we have got:



You should type in the PreShared Key, which is going to be used by remote Client as well. So, don't forget the key, you will use it later, while configuring the remote Client. Be sure to remember the Key Life and IKE Life Time settings as well, they must be the same on your VPN Router and VPN Client. You may change them to whatever amount is suitable for you, but be sure to use equal settings for your client.

You can use Main, Aggressive and Manual modes for Secure Association, but be sure to use the same mode on the VPN Client. The default mode is a Main mode for VPN Router as well as for VPN Client. You have two choices for the Encryption Protocol: 3DES or DES in Main mode, you can choose Key Group in Aggressive mode and Authentication protocol in Manual mode, as well as Encryption and Authentication Keys. Once again, make sure to use equal settings for you VPN Client and VPN Router.

Now, when we are done with VPN settings, you may safely click on Save.



You will see the Connection at the bottom on the screen. This is the connection we have just created. You can add more connections if you would like a client with another IP address or from the other remote network to access your internal network. The maximum amount of clients, which are supported by D-Link DI-804V VPN Router is 8.

Now you can either click on Save & Restart in the left bottom corner of the screen, or you can click Next and the system will offer you to Save & Restart the router itself. Now your VPN Router is ready to get the VPN Client request.

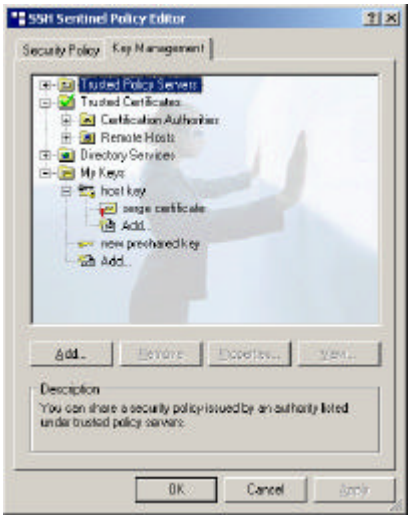
II. Configuring SSH Sentinel Client[1]

Please install the SSH Sentinel to your system. Please you the official SSH Sentinel Manual if you have problems while installing it. If you installed the SSH Sentinel client successfully and restarted your computer, the client would start automatically, the SSH Sentinel taskbar sign would appear in your taskbar in the right bottom corner of your Desktop. Move your mouse to the SSH Sentinel sign at the taskbar and press the right mouse button. Choose Run Policy Editor and click on it.

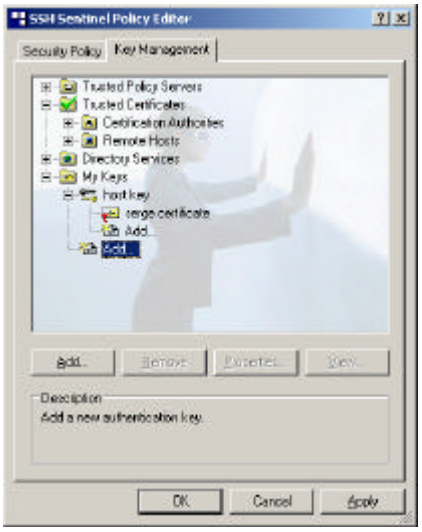
You will get into the following menu:

[1] The SSH Sentinel official manual can be found at www.ssh.com. The material, which is presented in this chapter is not an official SSH manual. D-Link does NOT guarantee that the configuration changes you make to SSH Sentinel according to this manual are correct and has no responsibilities for any misconfiguration or misuse of SSH products.

Choose Key Management bookmark:



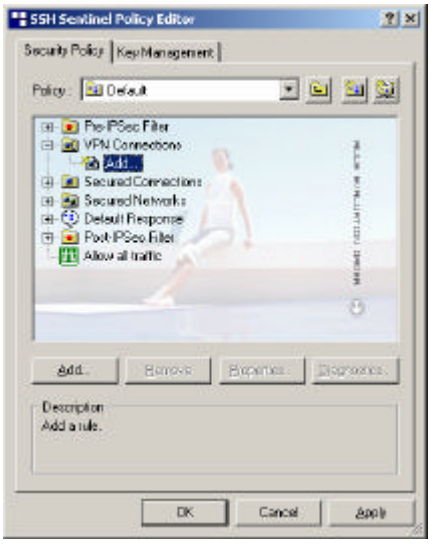
Go to My Keys and press “Add”:



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

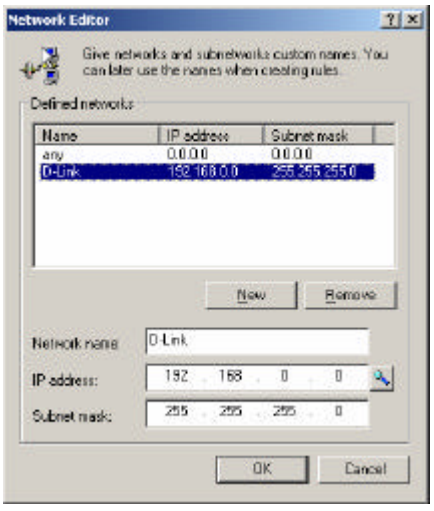
Give a name to the key and put exactly the same key you used in “Authentication Key” field of D-Link DI-804V VPN Router, press “Finish”. The key is now created and you can go back to the “Security Policy” bookmark.

Choose “VPN Connections” and press “Add”:

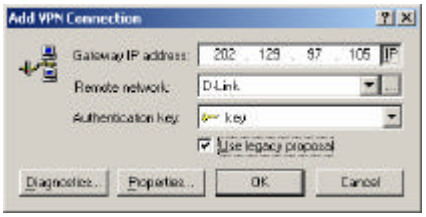


On the “Gateway IP address” field press “IP” and put the external IP address of your VPN Router, for example 202.129.97.105:

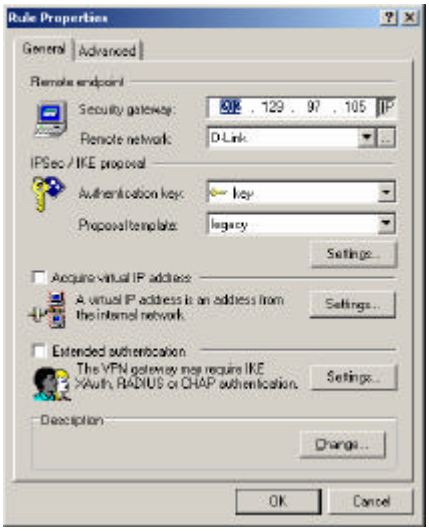
Press “...” button in “Remote Network” field. Press “New” and create a network with your internal network address, for example 192.168.0.0 255.255.255.0:



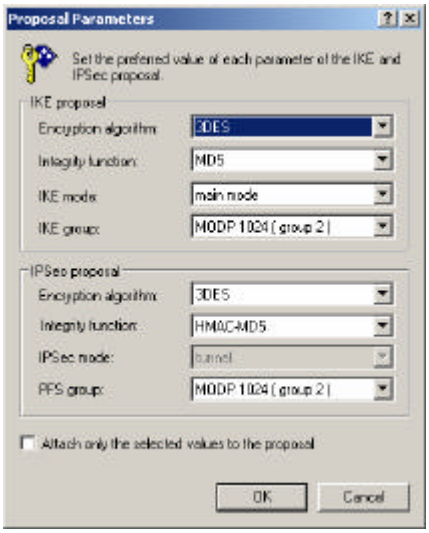
Press “OK” and select “key” in “Authentication Key” field:



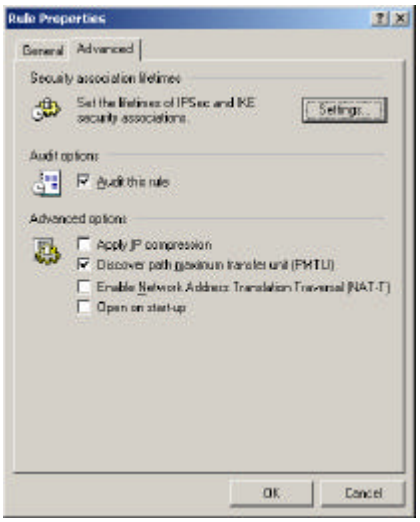
Check on “Use legacy proposal” and press “OK”. The VPN Connection is now created. Choose the VPN connection, we have just created and press “Properties”. You will get the following menu:



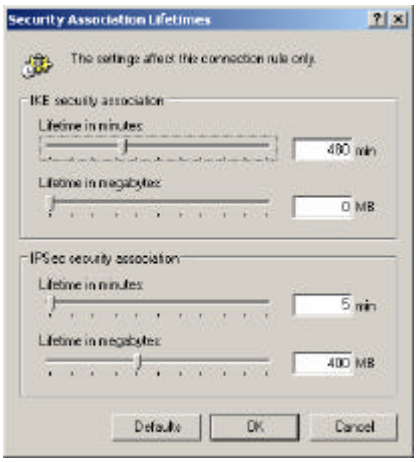
Click “Settings” under the “Proposal template” field, you will get this:



Choose the IKE and IPSec modes you would like to use and click “OK”. Choose “Advanced” bookmark and press “Settings”:



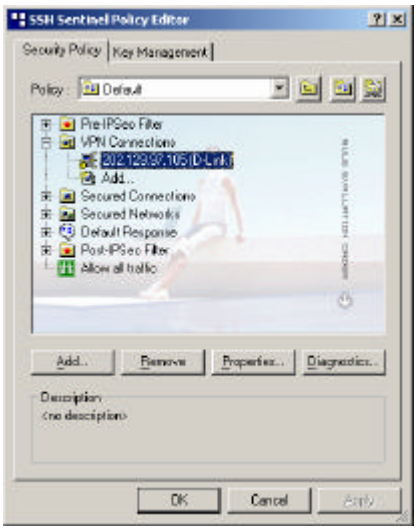
Choose lifetime, so it would correspond to the lifetime specified in DI-804V configuration. The defaults for DI-804V are 28800 seconds for Phase 1 (IKE) and 3600 seconds for Phase 2 (IPSec):



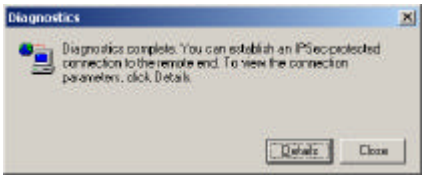
Go back to the main “Security Policy” window and press “Apply” and “OK” again. Don’t forget to “Apply” every time you change your VPN connection properties or security policy. The basic configuration of SSH Sentinel VPN client is now over. You can check you Pre-IPSec and Post-IPSec Filters to be sure 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. Now you are ready to connect your client to the office network.

III. Connecting SSH Sentinel VPN Client to the Office network

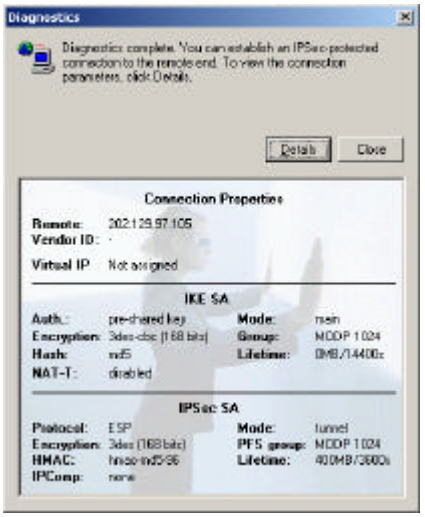
Make sure your client has a connection to the Internet. In SSH Sentinel Policy Editor choose the VPN connection you have created and press “Diagnostics”.



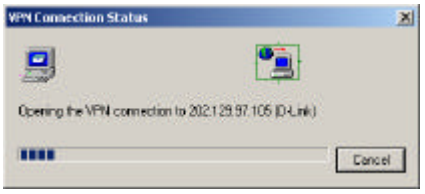
You will see the client trying to connect to D-Link DI-804V VPN Router. If the diagnostics is successful, you will see the following message:



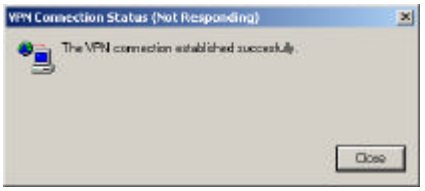
Click on “Details” to check which authentication and encryption modes are chosen for IKE and IPSec:



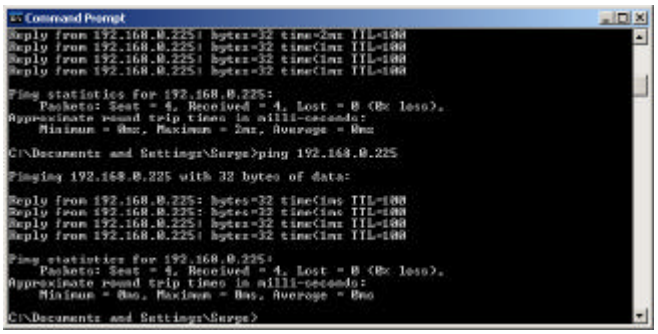
Now you can connect your client to your office network. Click right mouse button on SSH Sentinel taskbar sign and choose “Select VPN”. Select the connection you have created, for example 202.129.97.105 (D-Link) and click on it, you will see the following window:



When the connection is done, you will see the follow message:



The message disappears in a few seconds, that means that you VPN connection is now established (Not Responding is normal here, since Sentinel closes the window itself). Now you can open Command Prompt from Start/Programs/Accessories menu in Windows. Check if you have a connection to your office network by “pinging” of the office computers:



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.

Congratulations! You have successfully created the VPN Connection from SSH Sentinel VPN Client to your Office network through D-Link DI-804V VPN Router!