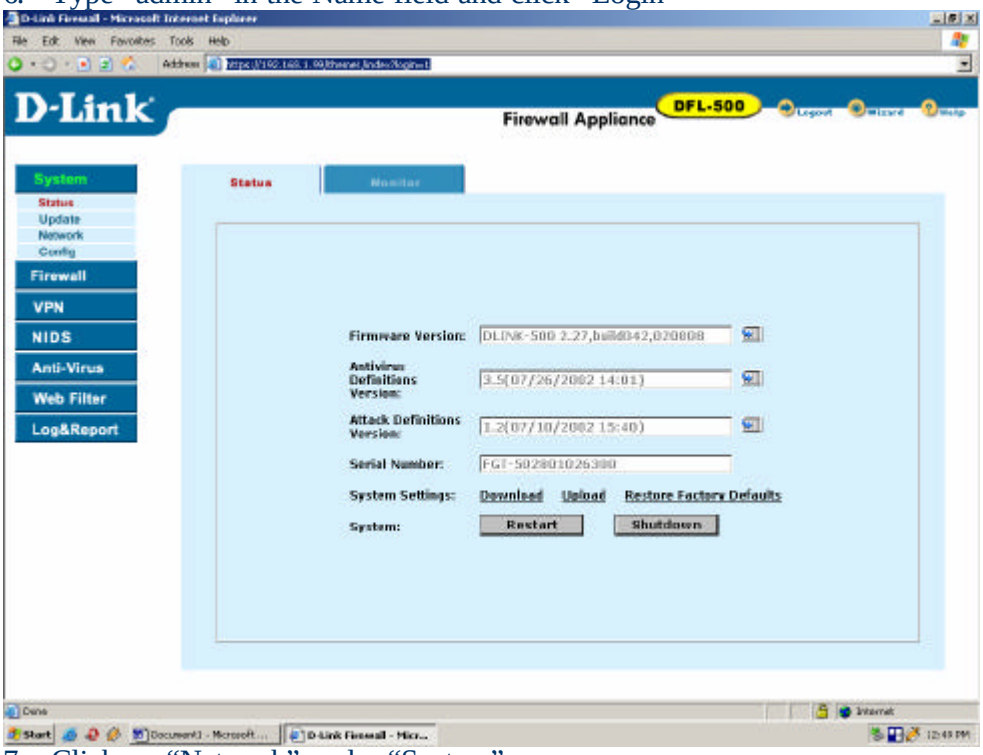
Configuring SSH Sentinel VPN client and D-Link DFL-500 Firewall

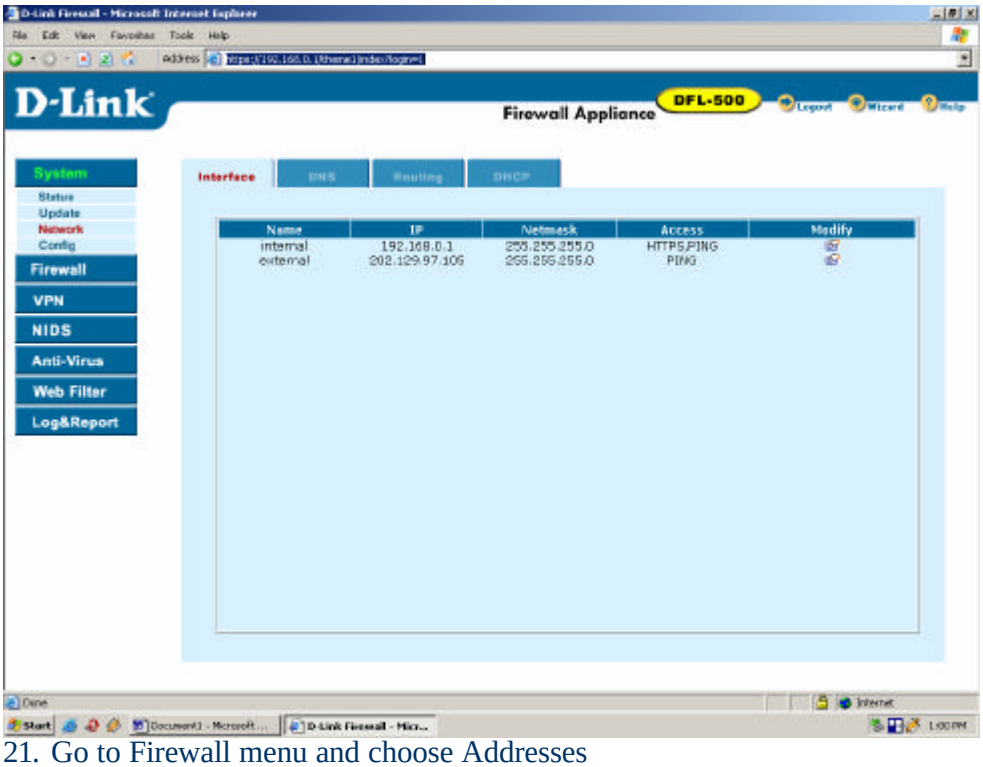
I. Configuring D-Link DFL-500 Firewall

1. Connect your computer to the internal port of the DFL-500 Firewall
2. Change the computer IP address to 192.168.1.100 255.255.255.0
3. In Internet Explorer address type: https://192.168.1.99
4. You will see the message with a Security Alert
5. Click “yes”, you are in the Web Base Interface (WBI)
6. Type “admin” in the Name field and click “Login”

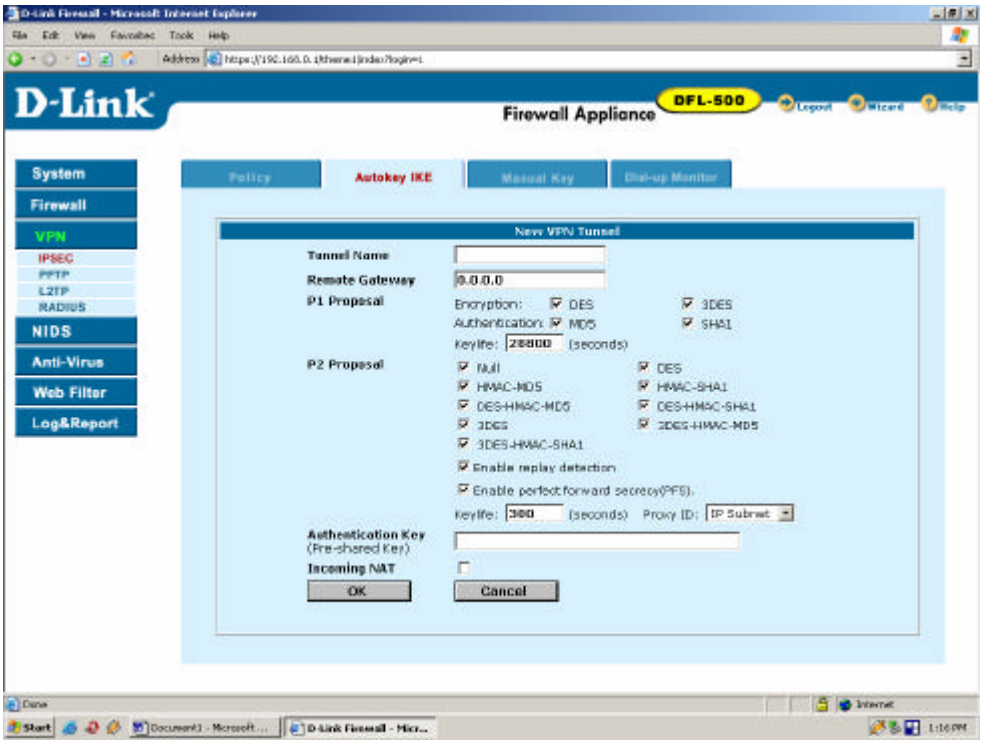


7. Click on “Network” under “System” menu
8. You will see “internal” and “external” interfaces
9. Click on Modify picture for “internal” interface
10. Put the ip address for the internal interface, for example 192.168.0.1 following the subnet mask 255.255.255.0 and press “OK”. You will loose the connection to the firewall after you press “OK”
11. Now you can connect your firewall to switch or hub and connect your computer to that switch or hub
12. Make sure all the stations in the network (including your own computer) have the default address of your internal firewall interface, for example 192.168.0.1
13. Change the ip address of your computer to 192.168.0.100 255.255.255.0
14. Change the ip address in your Internet Explorer to https://192.168.0.1
15. Go to Systems/Network again and choose “external” interface
16. Put the static IP address supplied by your internet provider, for example 202.129.97.105 255.255.255.0
17. Go to the Routing bookmark under System/Network and press “New”
18. Add the default router with the ip address supplied by your internet prover.

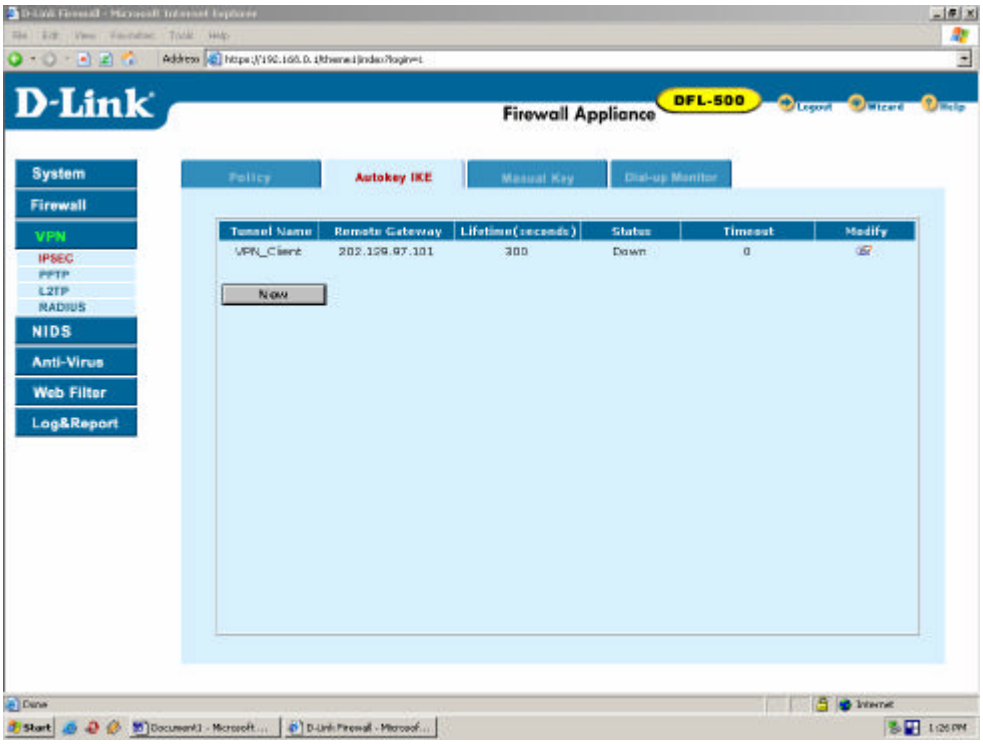
19. Go back to System/Network menu
20. You will get the following conf iguration:



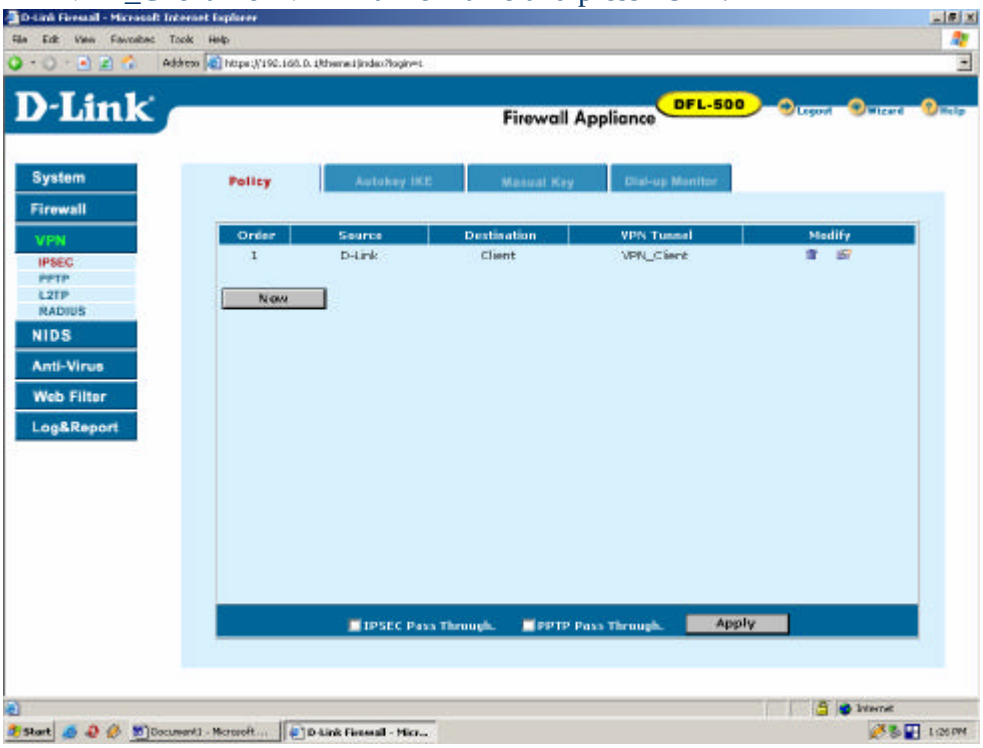
21. Go to Firewall menu and choose Addresses
22. In the Internal submenu press “New”
23. Type the name of your internal network, for example “D-Link” and put the ip address of the internal network, for example 192.168.0.0 255.255.255.0
24. Go to External submenu and press “New”
25. Type the name of the VPN client, for example “Client” and put the ip address of the client, for example 202.129.97.101 255.255.255.0. If you want to allow any VPN client to connect leave all 0s for the ip address
26. Go to VPN menu and choose IPSec submenu
27. Choose Autokey IKE bookmark and click “New”
28. You will see the following screen:



29. Put in the Tunnel Name, for example “VPN_Client”
30. In “Remote Gateway” field type the ip address of the client, for example 202.129.97.101 or leave it all zeros, if you want to allow any client to connect
31. Choose the encryption and authentication algorithms you would like to you or leave it as default
32. Put the “Authentication Key”, it can be any key, but it is better to use meaningless combination of digits and characters. Don’t forget the key, you will use it later.
33. Check “Incoming NAT” and press OK
34. You will get the following screen:



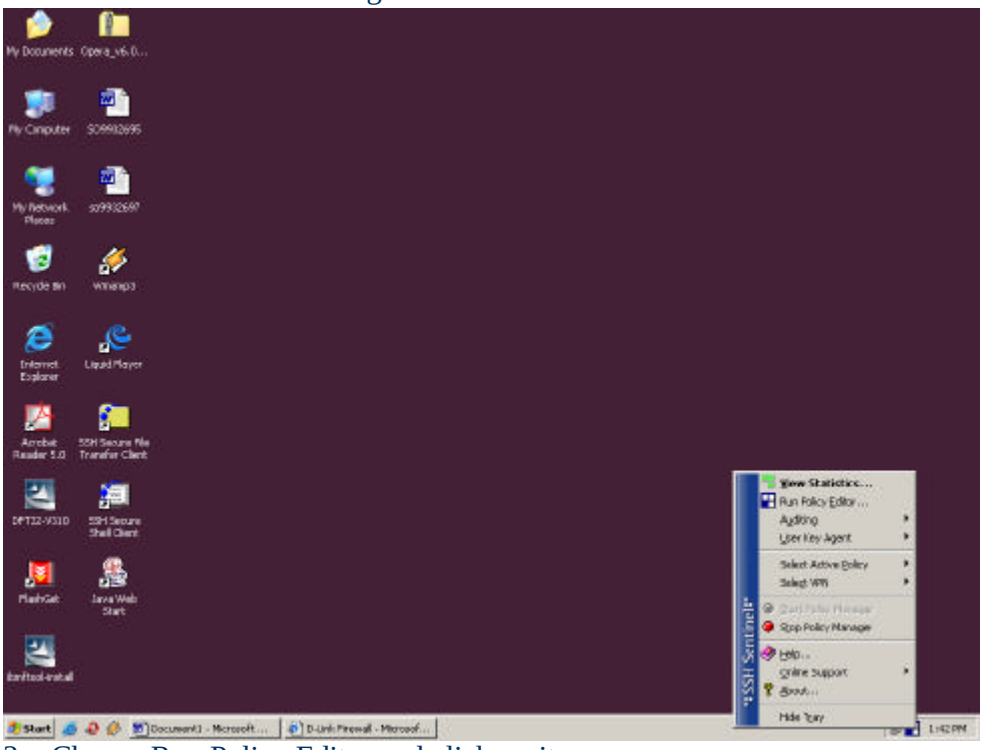
35. Choose “Policy” submenu in VPN/IPSec menu
36. Press “New” and choose “D-Link” for source, “Client” for destination and “VPN_Client” for VPN Tunnel name and press “OK”:



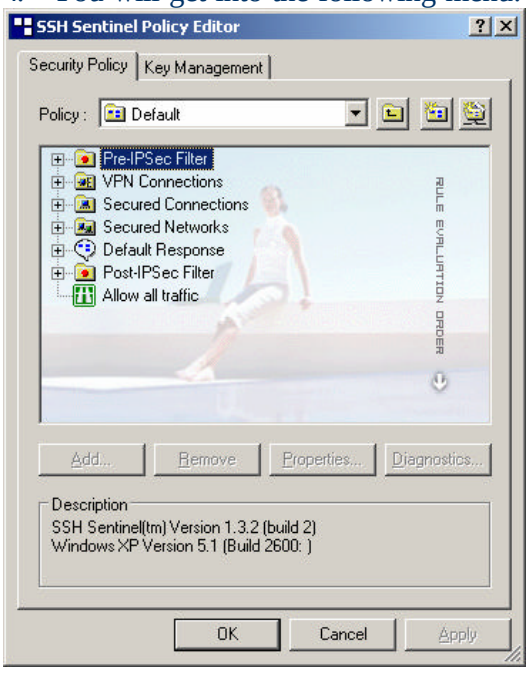
37. The DFL-500 Firewall configuration is finally ready.

II. Configuring SSH Sentinel Client

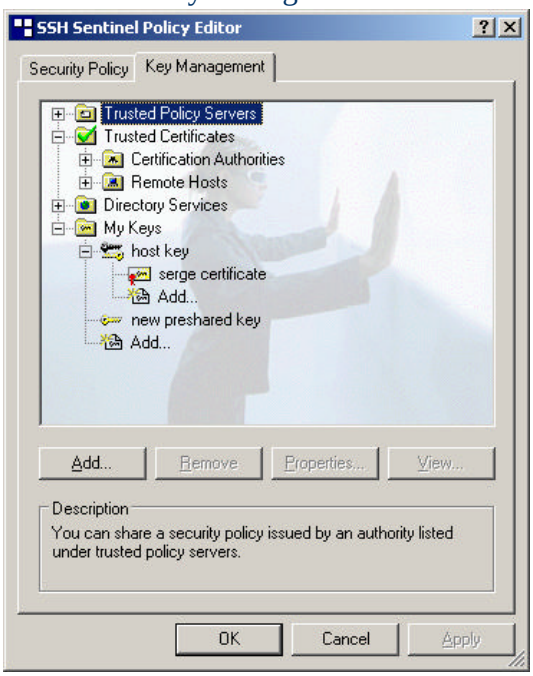
1. After you installed the SSH Sentinel client and restarted your computer, the client will start automatically, the SSH Sentinel taskbar sign will appear
2. Move your mouse to the SSH Sentinel sign at the taskbar and press the right mouse button
3. You will see the following menu:



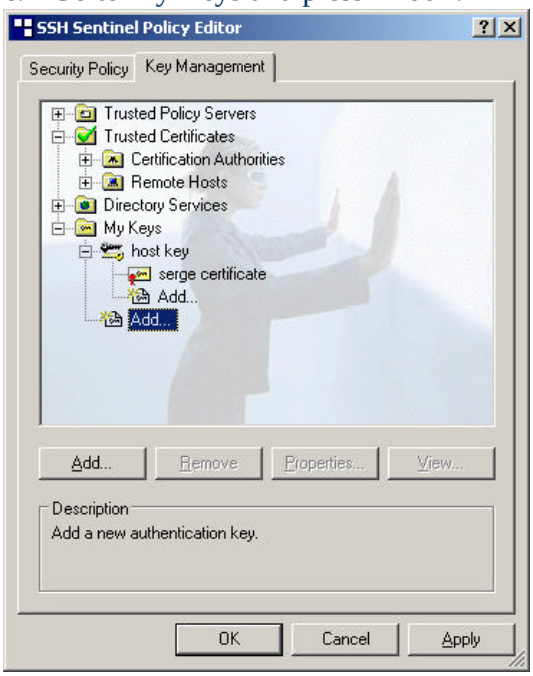
3. Choose Run Policy Editor and click on it
4. You will get into the following menu:



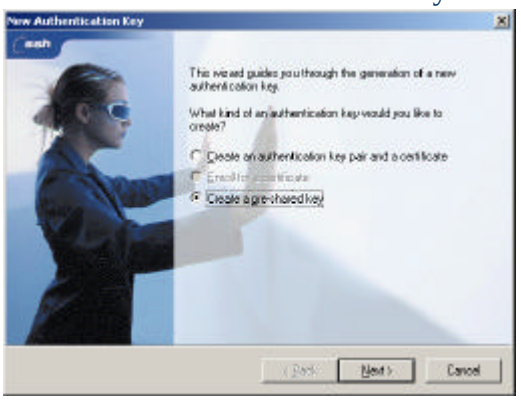
5. Choose Key Management bookmark:



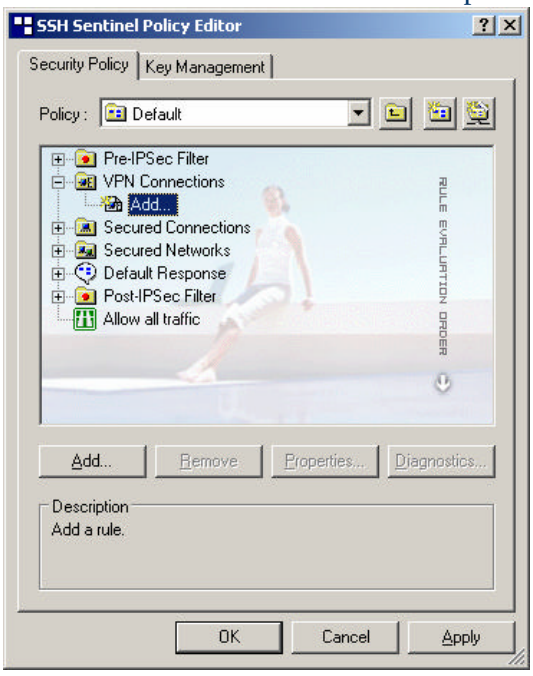
6. Go to My Keys and press “Add”:



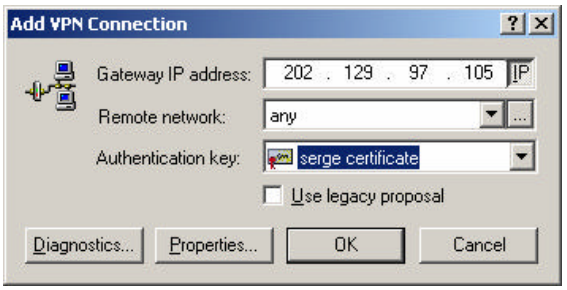
7. Choose “Create Pre-Shared Key” and click “Next”:



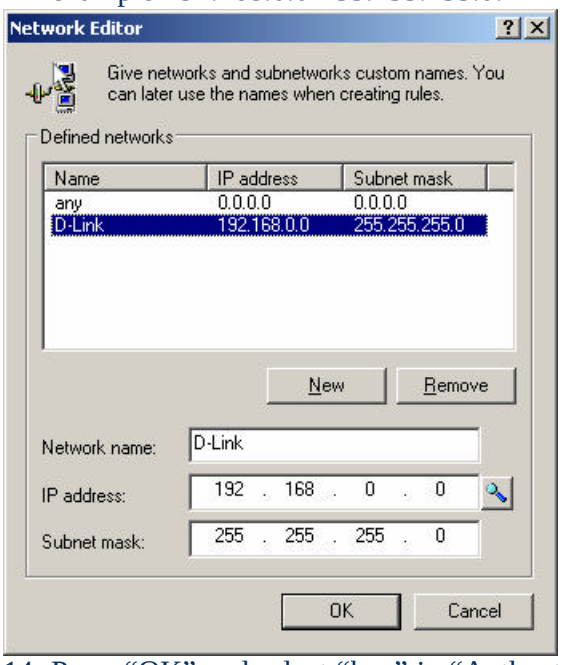
8. Give a name to the key and put exactly the same key you used in “Authentication Key” field of D-Link DFL-500 Firewall, press “Finish”
9. The key is now created and you can go back to the “Security Policy” bookmark
10. Choose “VPN Connections” and press “Add”:



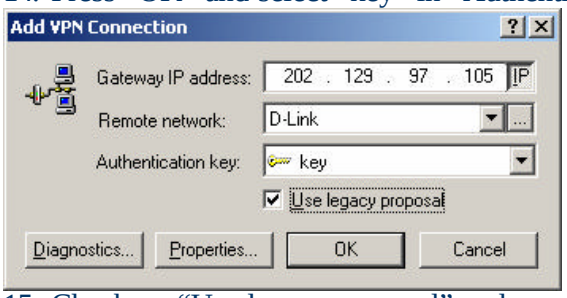
11. On the “Gateway IP address” field press “IP” and put the external ip address of your firewall, for example 202.129.97.105



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:

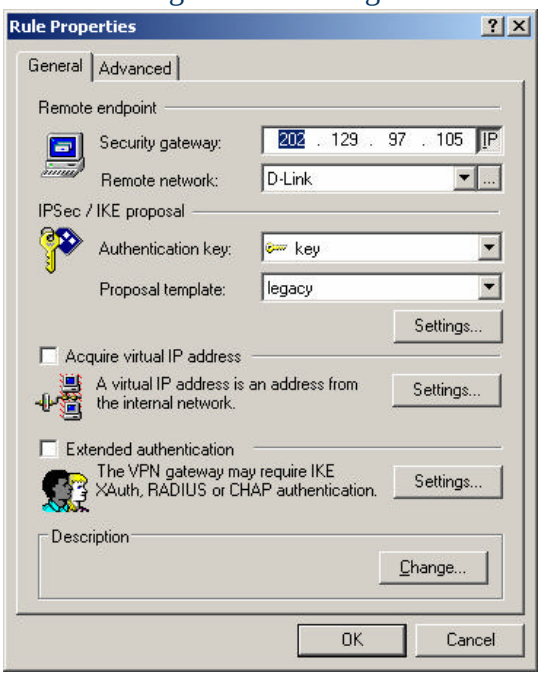


14. Press “OK” and select “key” in “Authentication Key” field:

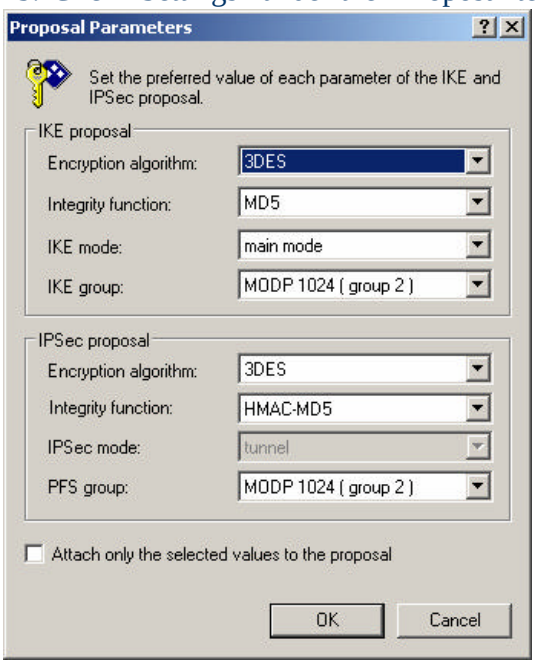


15. Check on “Use legacy proposal” and press “OK”
16. The VPN Connection is now created
17. Choose the VPN connection, we have just created and press “Properties”

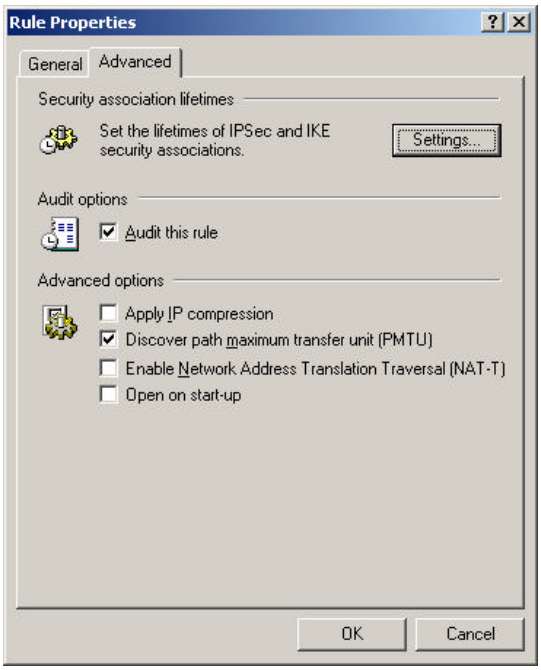
18. You will get the following menu:



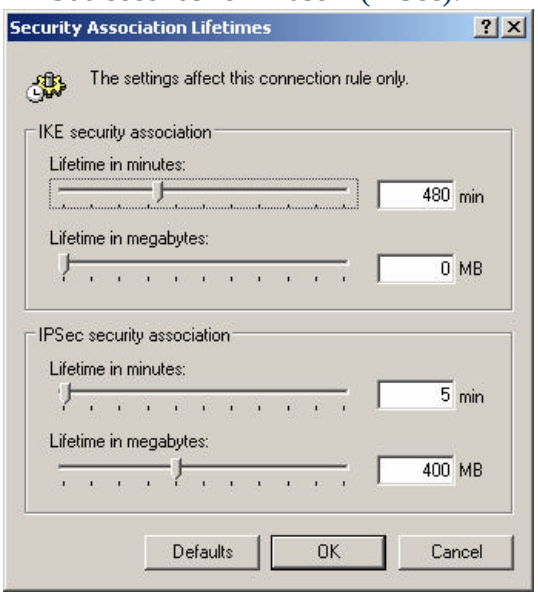
19. Click “Settings” under the “Proposal template” field, you will get this:



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



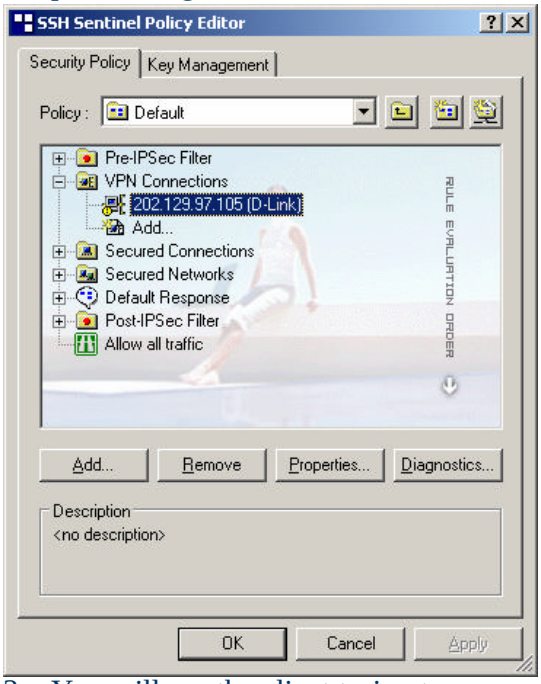
22. Choose lifetime, so it would correspond to the lifetime specified in DFL-500 configuration. The defaults for DFL-500 are 28800 seconds for Phase 1 (IKE) and 300 seconds for Phase 2 (IPSec):



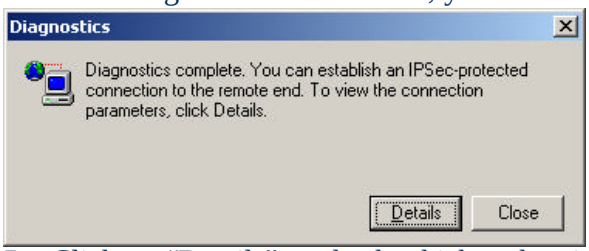
23. Go back to the main “Security Policy” window and press “Apply” and “OK” again. Don’t forget to “Apply” every time you change your VPN connection properties or security policy
24. The basic configuration of SSH Sentinel VPN client is now over
25. You can check you Pre-IPSec and Post-IPSec Filters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

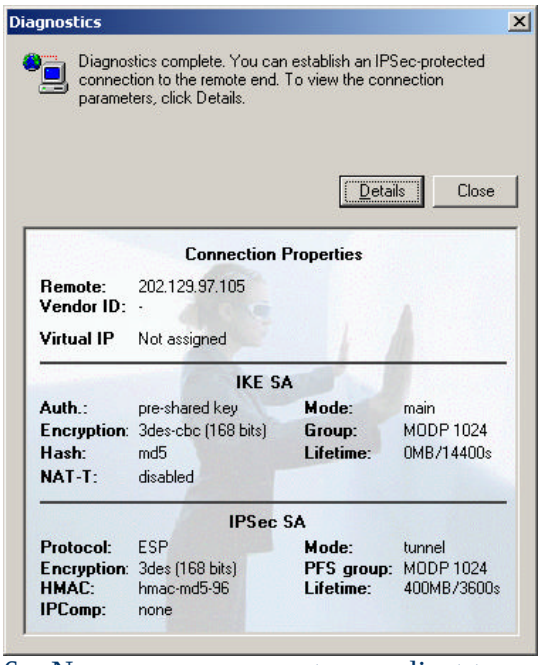
1. Make sure your client has a connection to internet
2. In SSH Sentinel Policy Editor choose the VPN connection you have created and press “Diagnostics”



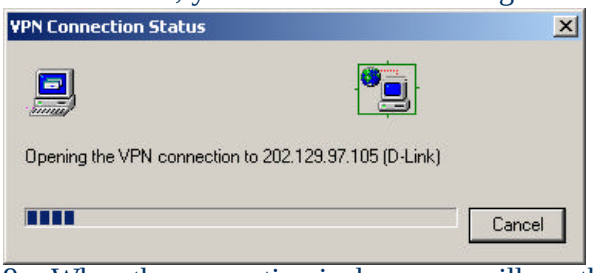
3. You will see the client trying to connect to D-Link DFL-500 Firewall
4. If the diagnostics is successful, you will see the following message:



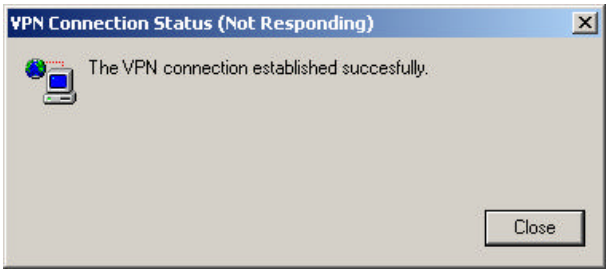
5. Click on “Details” to check which authentication and encryption modes are chosen for IKE and IPSec:



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:

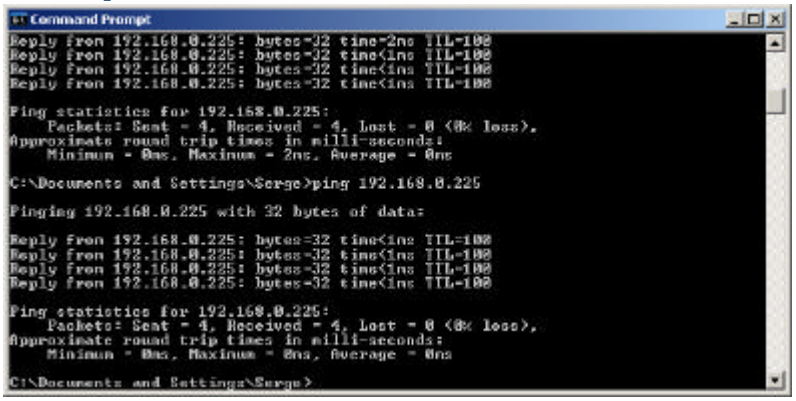


9. When the connection is done, you will see the follow message:



10. 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).

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!