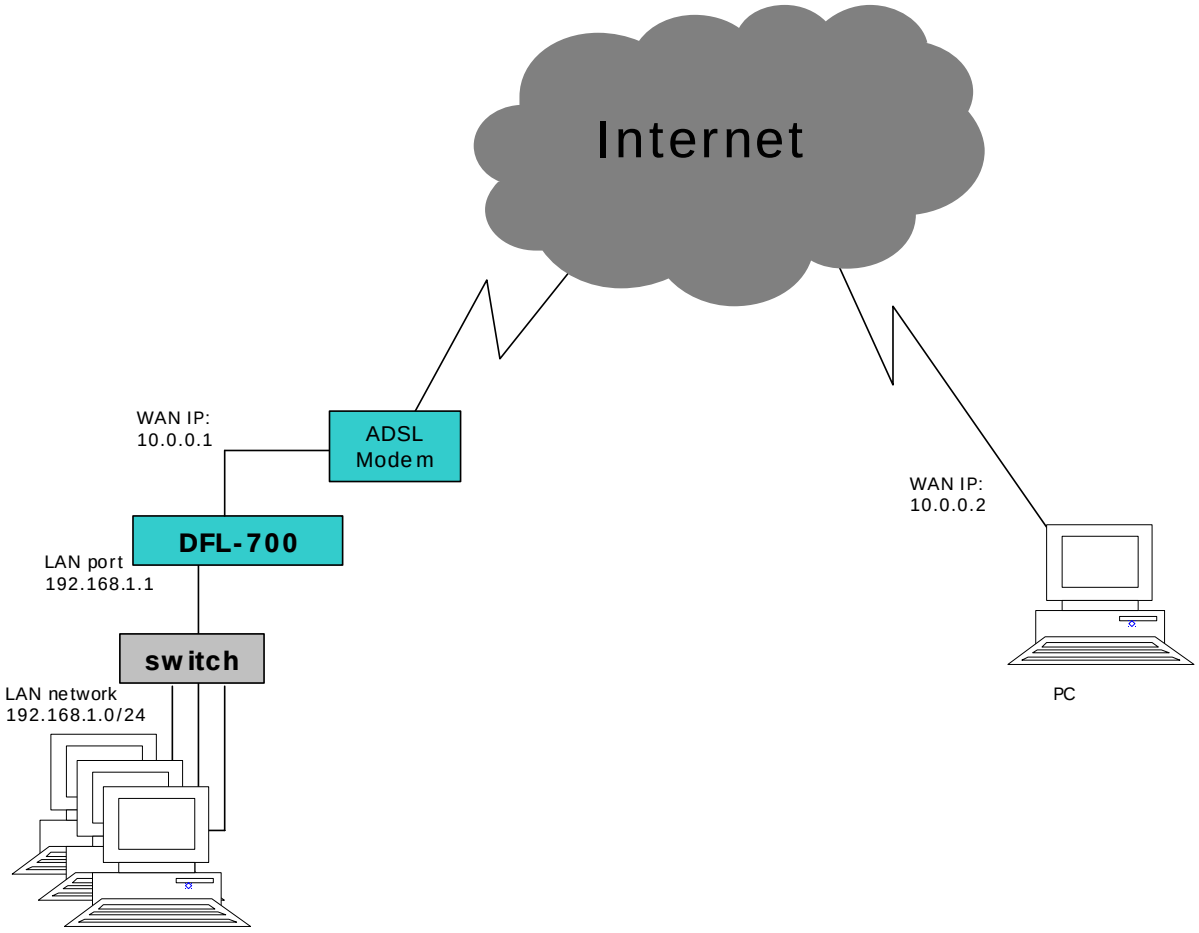
DFL-700 with Windows 2000/XP IPsec VPN Configuration Guide

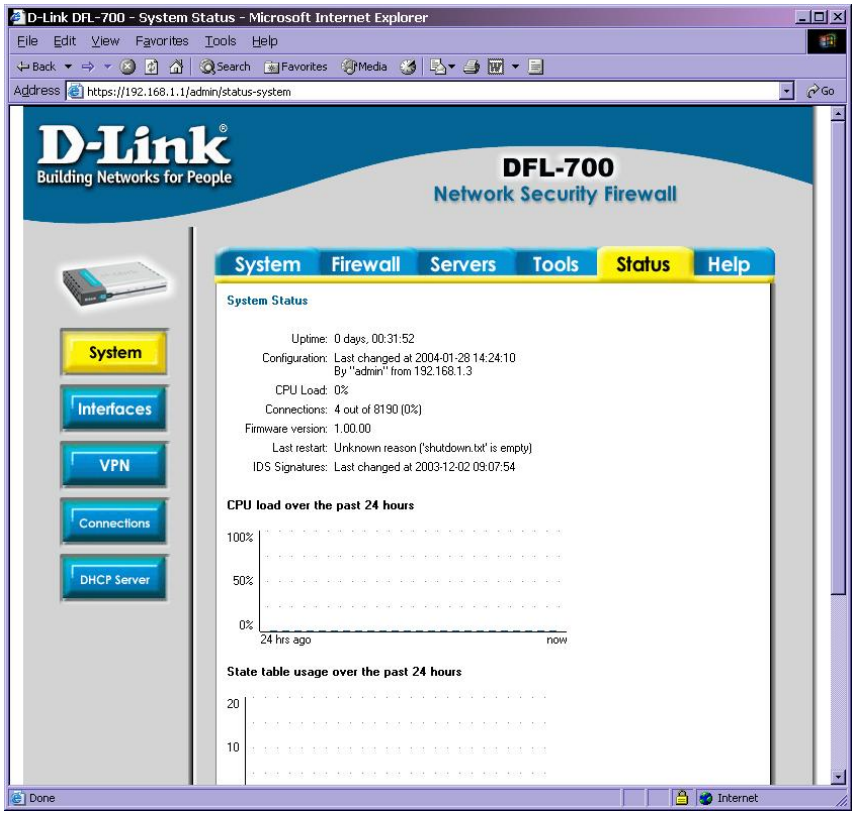
This guide will show how to configure a Windows 2000/XP machine to make an IPsec VPN Tunnel connection to a DFL-700. Below is the example network that this document is based on.

Technical Requirement: Customer is required to understand their network and Windows 2000/XP well for this configuration. Please consult a Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences that may arise from it.

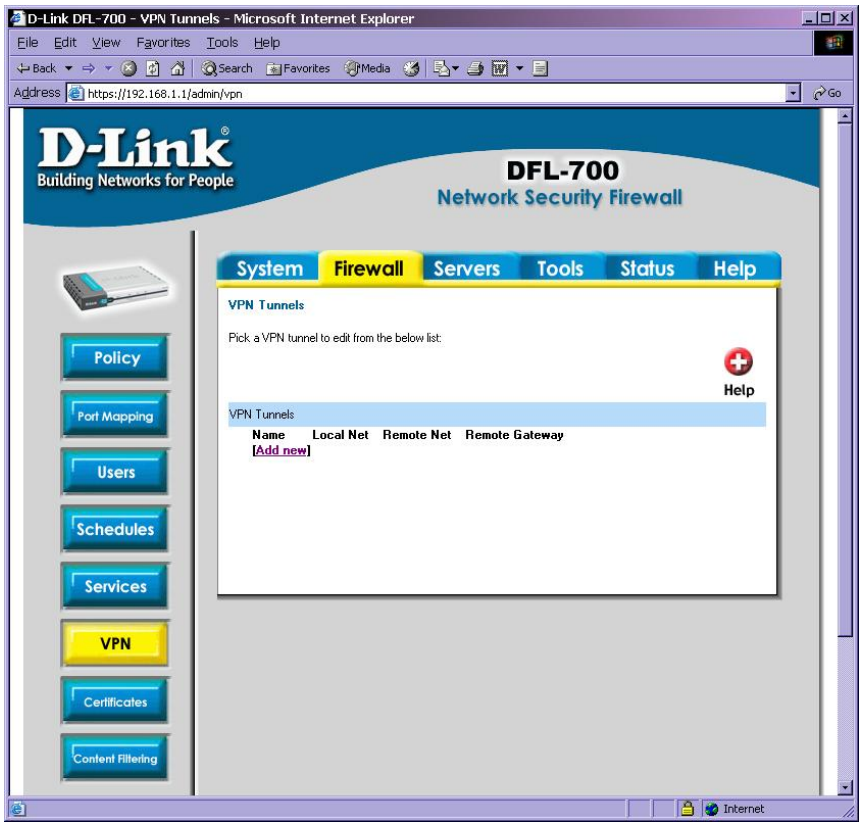


-

1. Logon to the DFL-700.



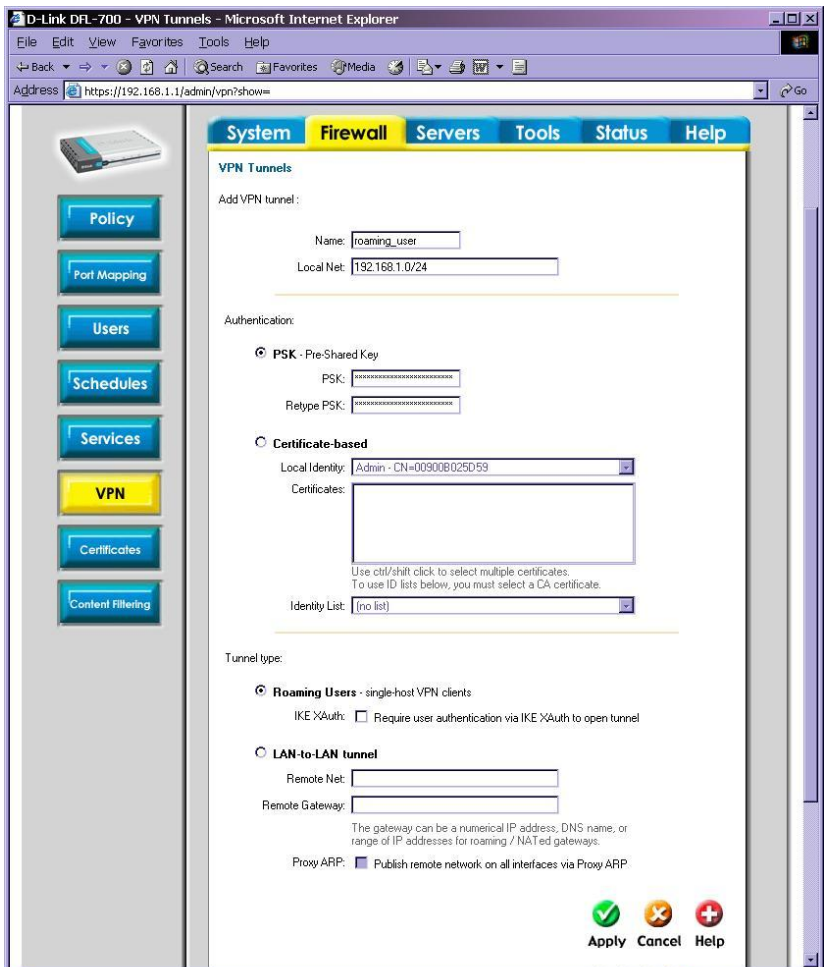
2. Click on **Firewall→ VPN→ Add New**



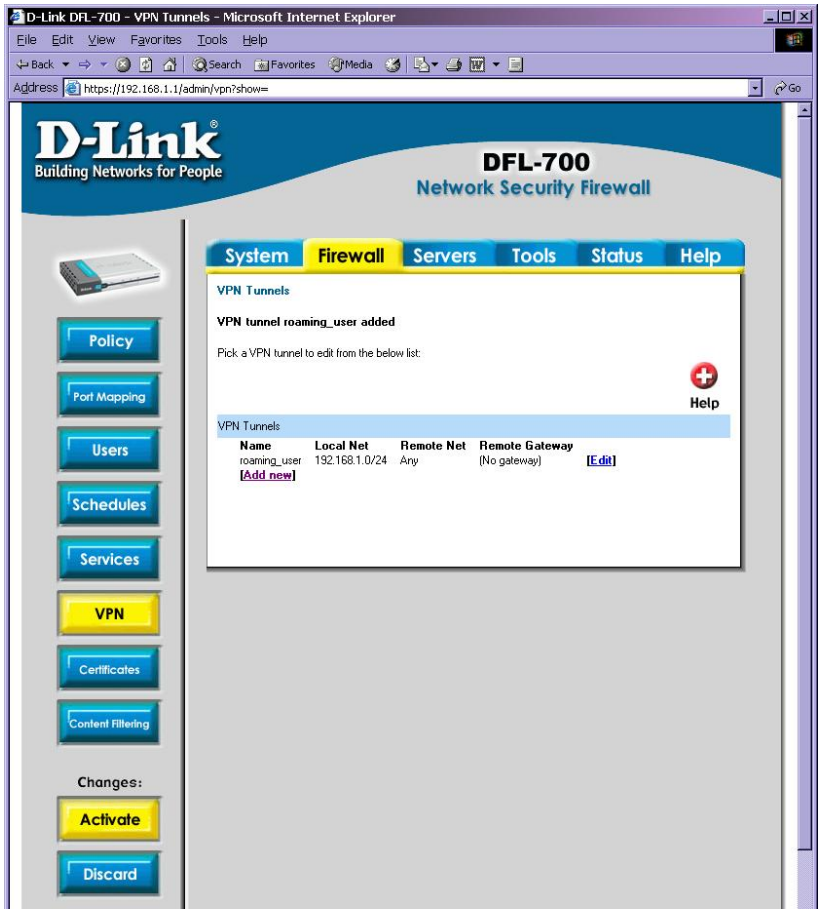
3. Enter the following details:

   Name: roaming_user
   Local Net: 192.168.1.0/24
   Authentication:
   PSK-Preshared Key: 'type in your preshared key'
   Tunnel Type: Roaming Users

   Click on Apply

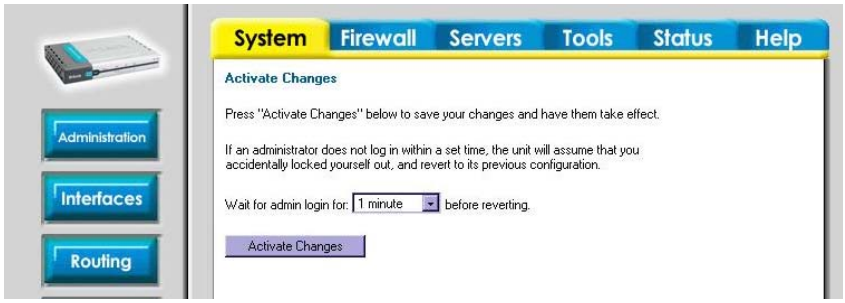


4. The new VPN profile will now be added

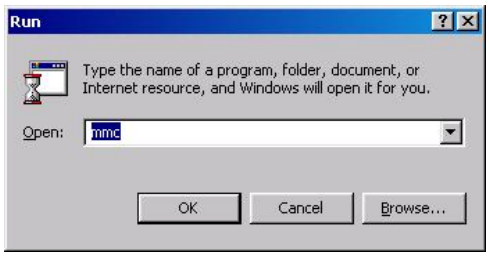


5. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.

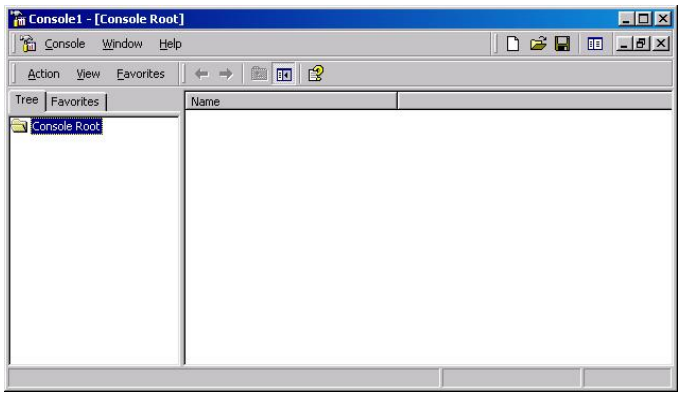
6. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.



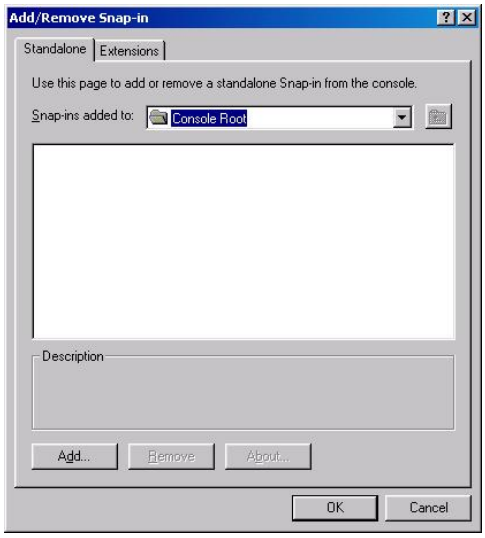
7. Go into Start→ Run→ and the type in MMC to bring up the Console.



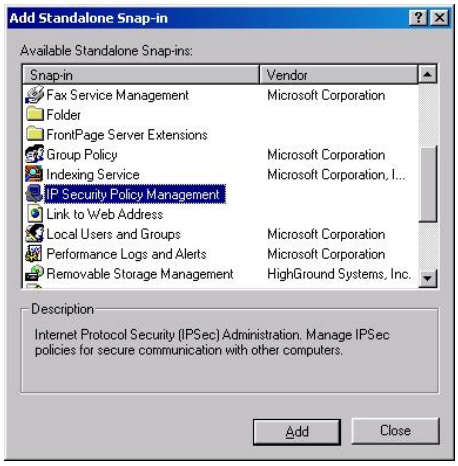
8. Click on Console→ and then Click on Add/Remove Snap In.



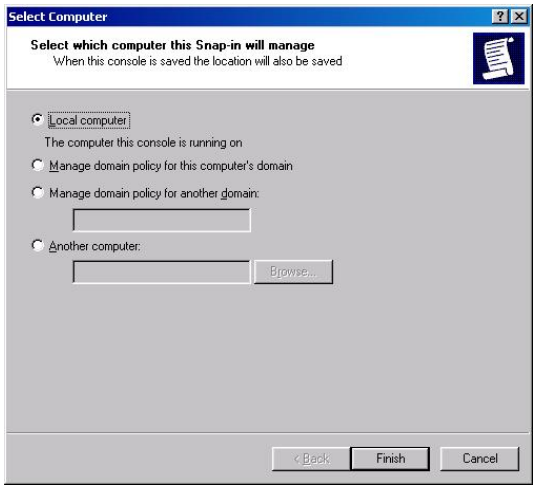
9. Click on the 'Add' Button.



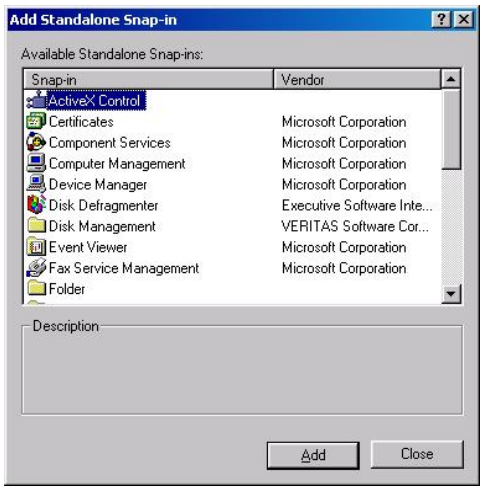
10. Select ‘IP Security Policy Management’ and then Click on ‘Add’.



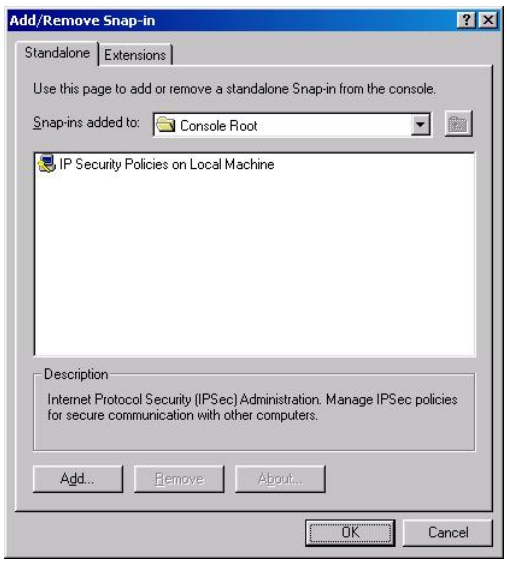
11. Select ‘Local computer’ and then click on Finish.



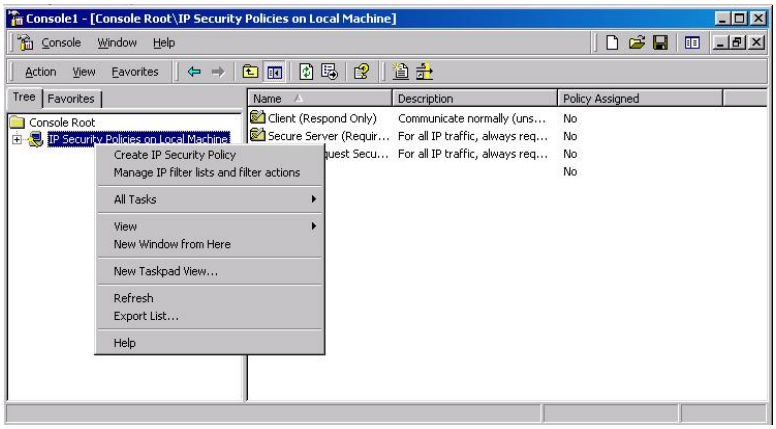
12. Click on ‘Close’ on the Add Standalone Snap-in window.



13. Click on OK in the 'Add/Remove Snap-in'.

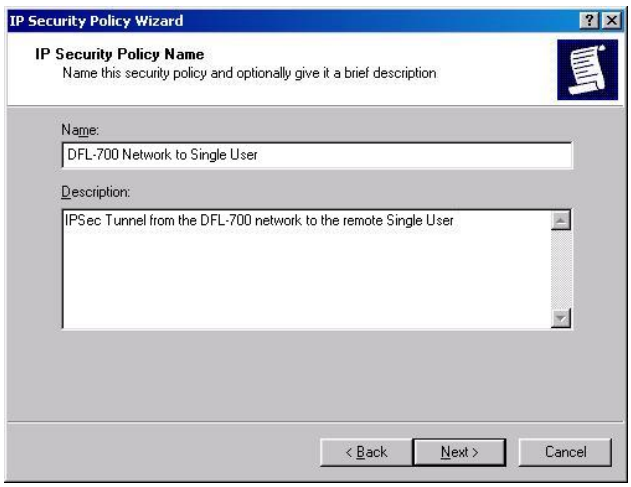


14. Right-Click on IP Security Policies on Local Machine. Select 'Create IP Security Policy'.

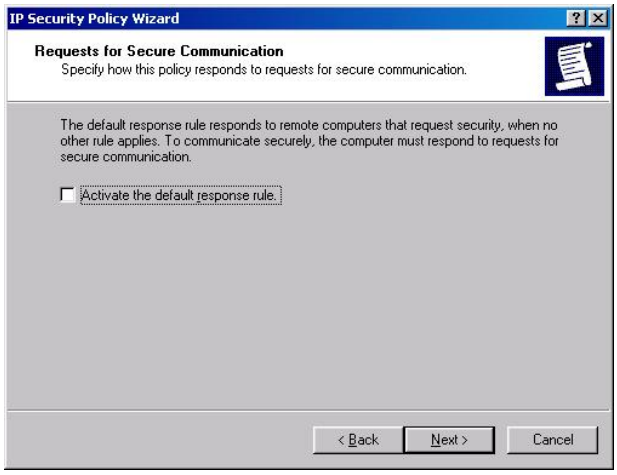


15. The wizard should then come up. Click 'Next' to continue.

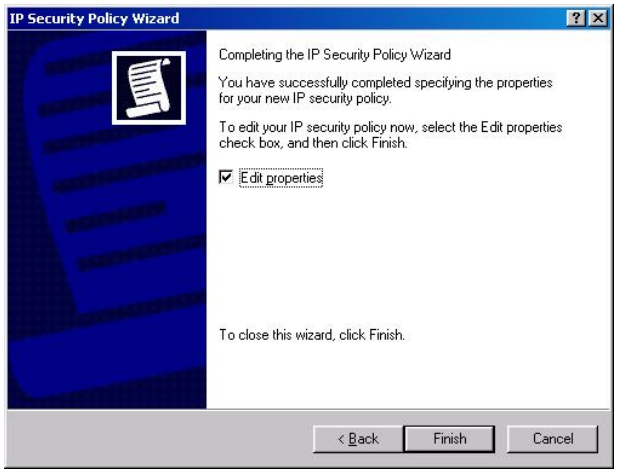
16. Enter the name for the Policy as well as the description. Click 'Next'.



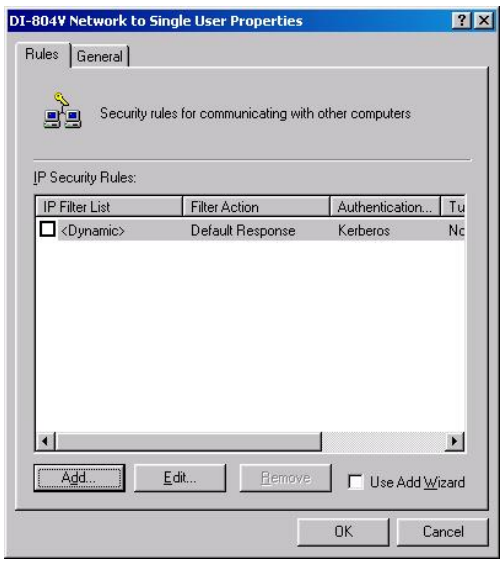
17. Uncheck 'Activate the default response rule'. Click 'Next'.



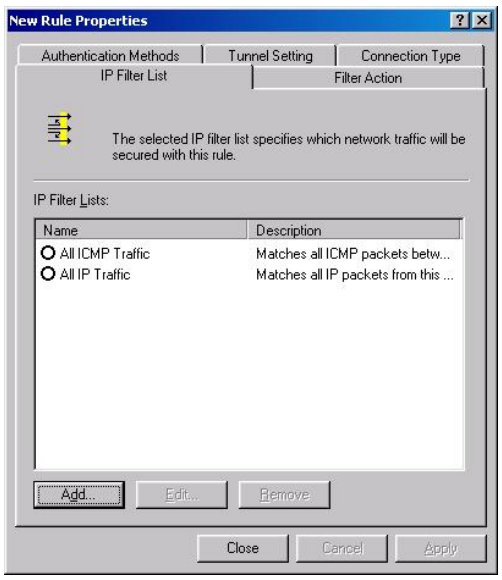
18. Click on 'Finish'.



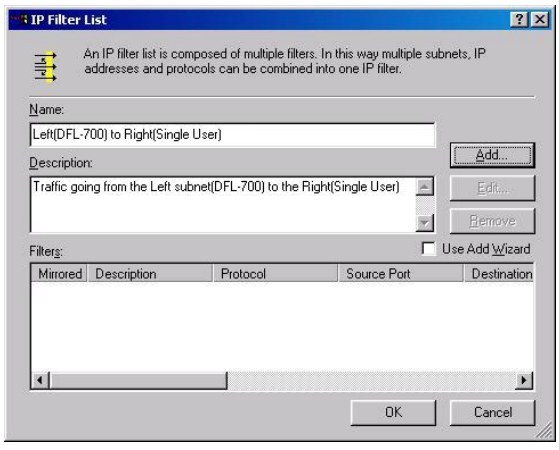
19. The Properties window for the newly created policy should then come up. Click on 'Add'.



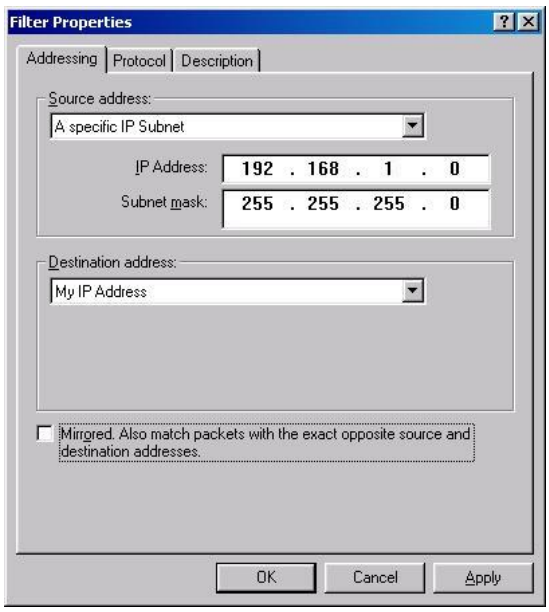
20. Click on 'Add' under IP Filter List.



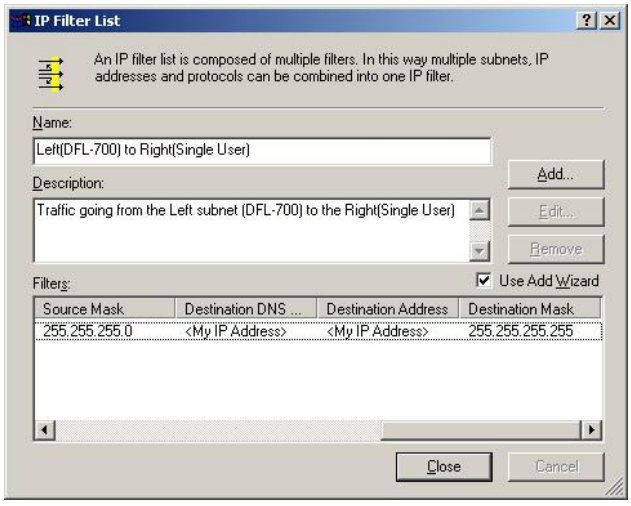
21. Enter the name and the description for the New IP Filter List. Uncheck the 'Use Add Wizard'. Click on 'Add'.



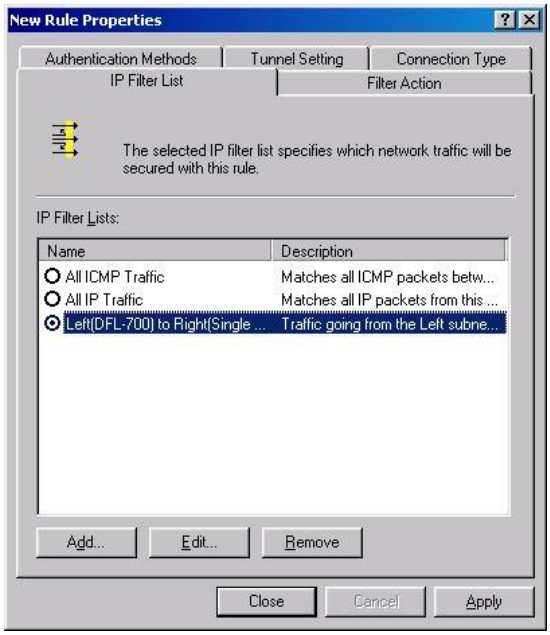
22. Select ‘A specific IP subnet’ for the ‘Source address’ and enter the Internal LAN range on the DFL-700 side. Select ‘My IP Address’ for the ‘Destination address’. Uncheck the ‘Mirrored….’ Option at the bottom of the screen. Click ‘OK’.



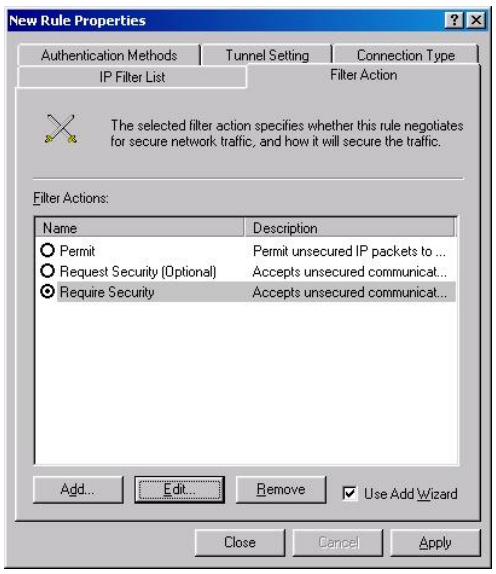
23. Click ‘Close’.



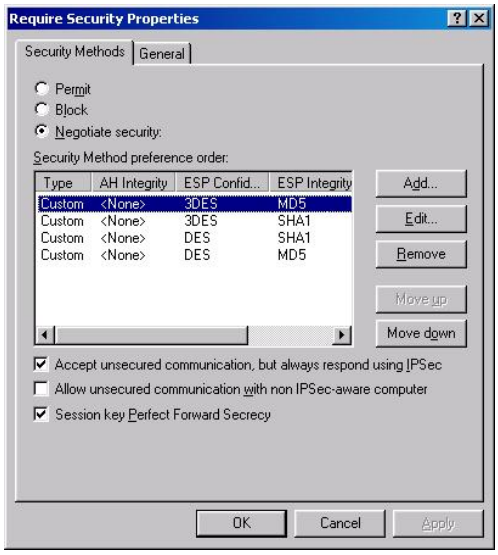
24. Select the newly created IP Filter.



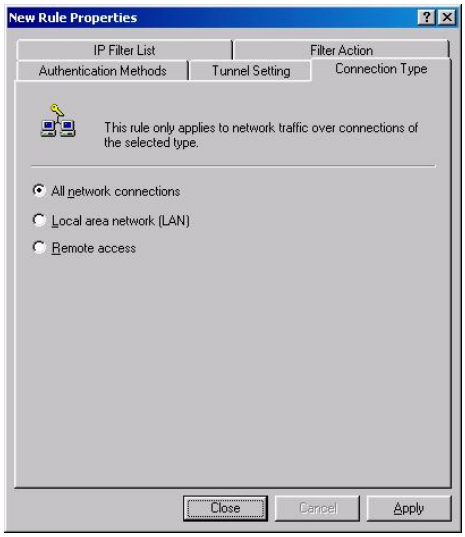
25. Click on the 'Filter Action' Tab. Select 'Require Security'. Click on 'Edit'.



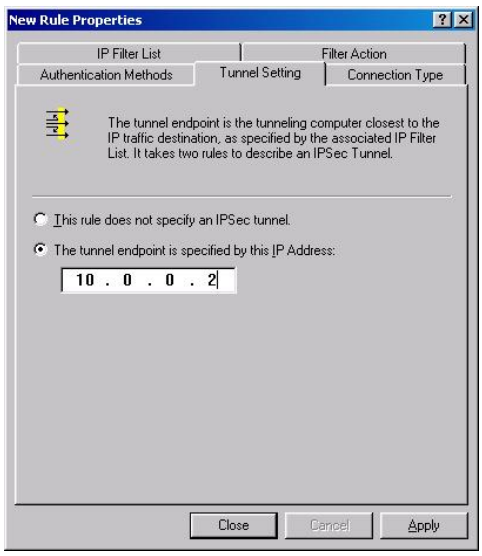
26. Move the 3DES/MD5 security method to the top. Check the 'Session key Perfect Forward Secrecy'. Click 'OK'.



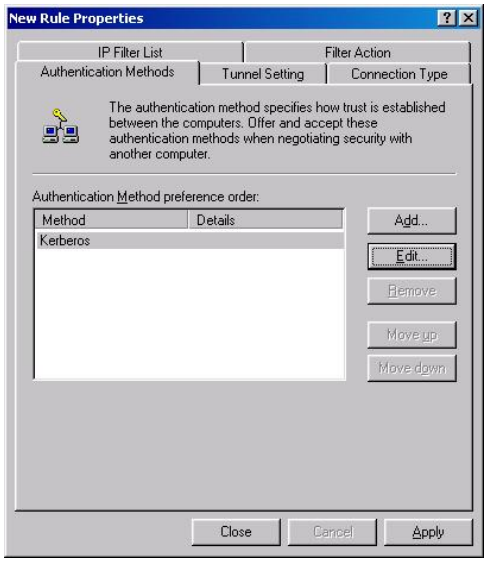
27. Click on 'Connection Type' Tab. Select 'All network connections'.



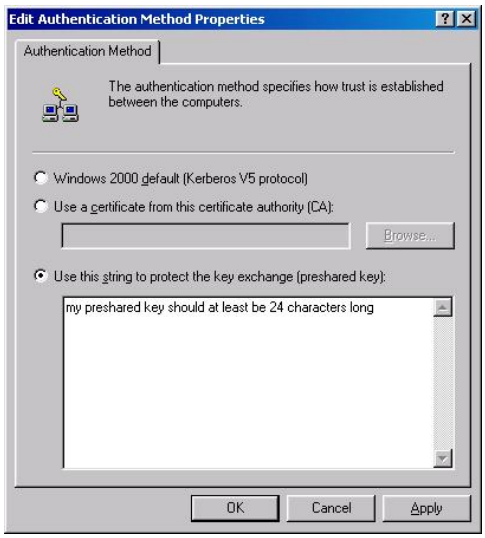
28. Click on 'Tunnel Setting' Tab. Specify the tunnel endpoint as the W2K Pro client IP address (10.0.0.2 in this example).



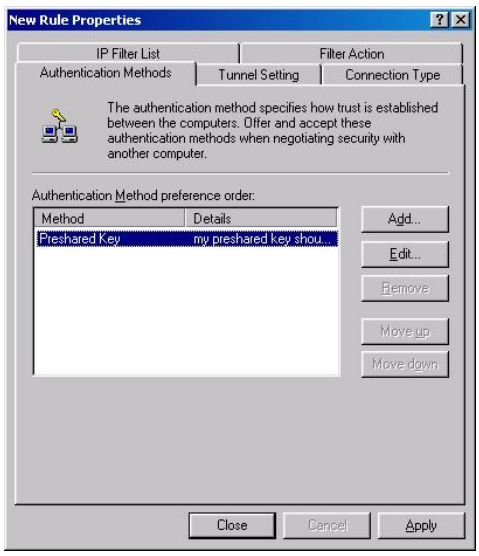
29. Click on 'Authentication Methods' Tab. Click on 'Kerberos' and then Click on 'Edit'.



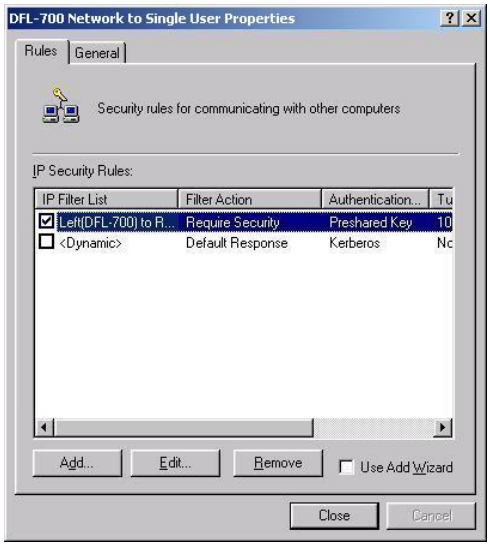
30. Select 'Use this string to protect the key exchange (preshared key)'. Type in the Preshared key. Click 'OK'.



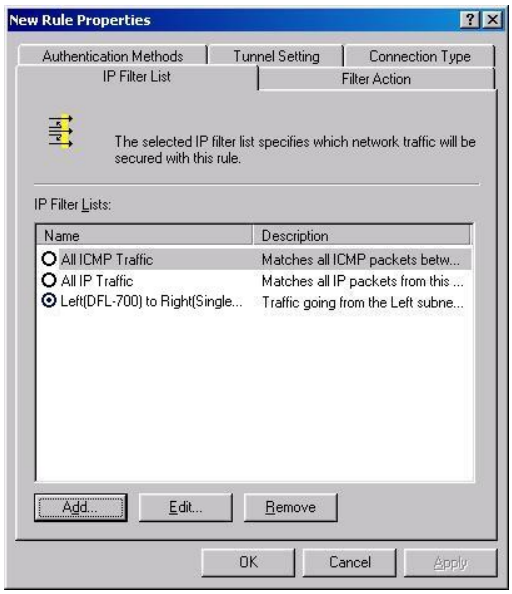
31. Click ‘Close’.



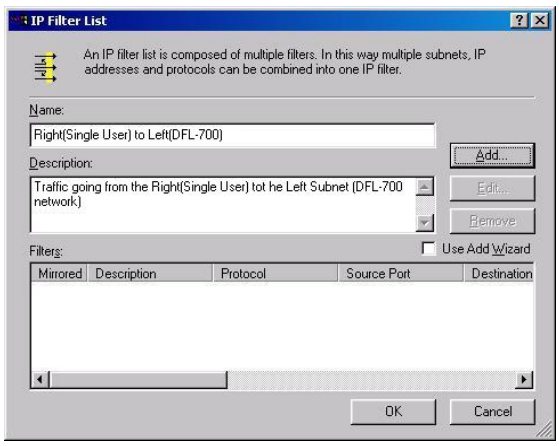
32. Select the newly created rule. Click on ‘Add’.



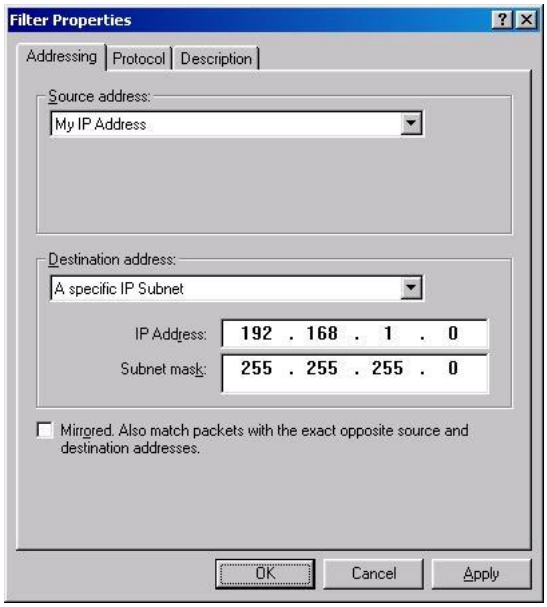
33. Click on ‘Add’ under IP Filter List.



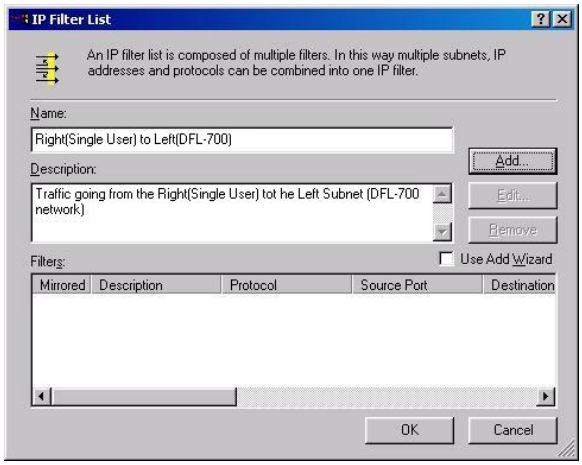
34. Enter the name and the description for the New IP Filter List. Uncheck the 'Use Add Wizard'. Click on 'Add'.



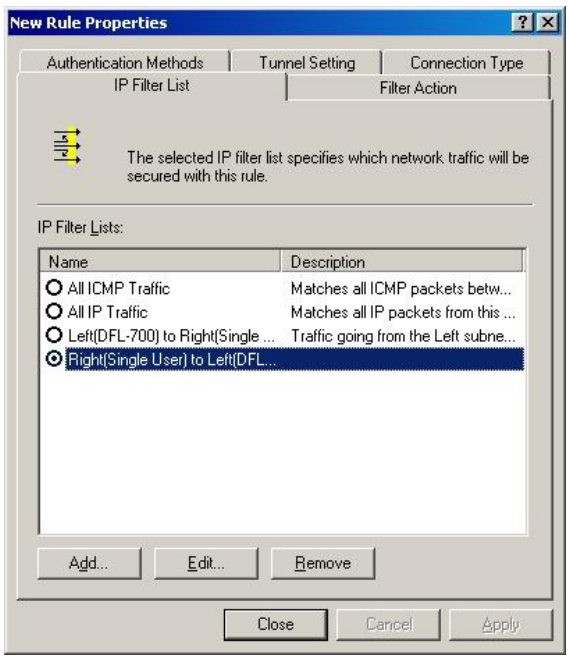
35. Select 'My IP Address' for the 'Source address'. Uncheck the 'Mirrored….' Option at the bottom of the screen. Select 'A specific IP subnet' for the 'Destination address' and enter the Internal LAN range on the DFL-700 side. Click 'OK'.



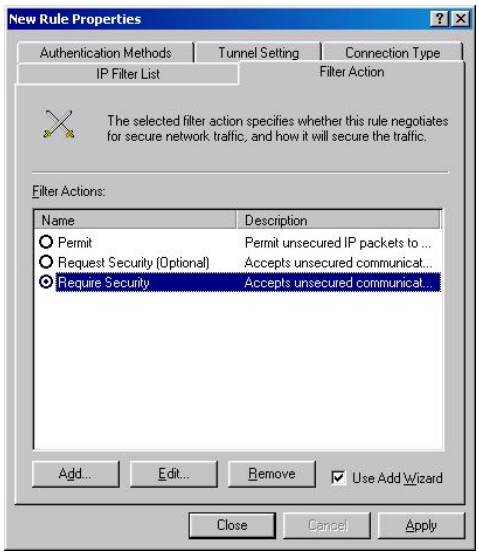
36. Click on 'Close'.



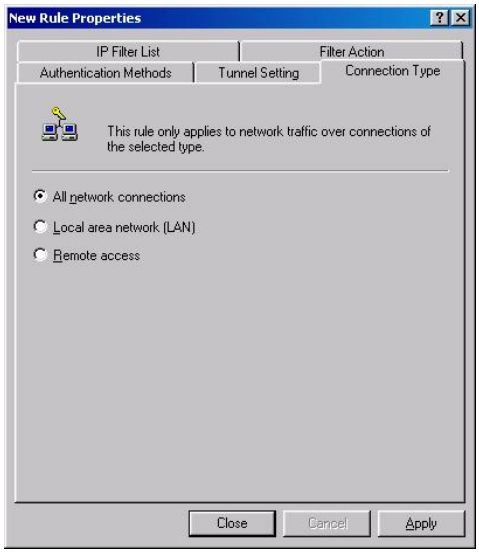
37. Select the newly created IP Filter 'Right (Single User) to Left(DFL-700…)'.



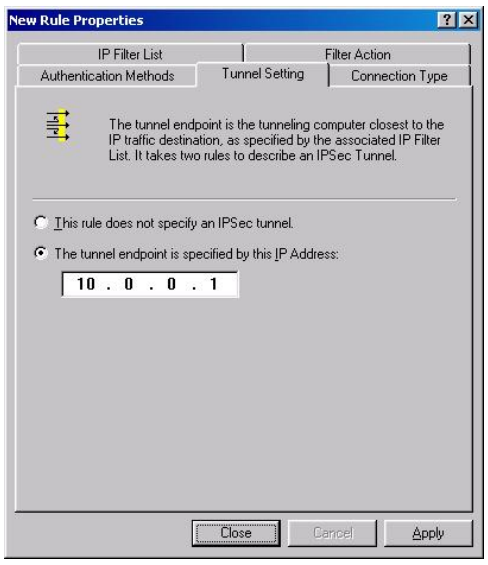
38. Click on the 'Filter Action' Tab. Select 'Require Security'. You don't need to click on Edit.



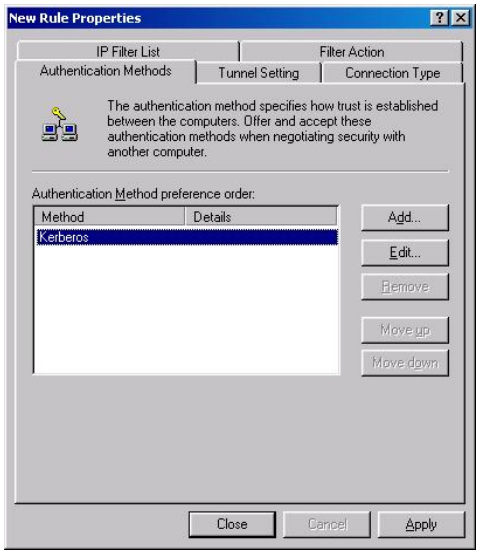
39. Click on 'Connection Type' Tab. Select 'All network connections'.



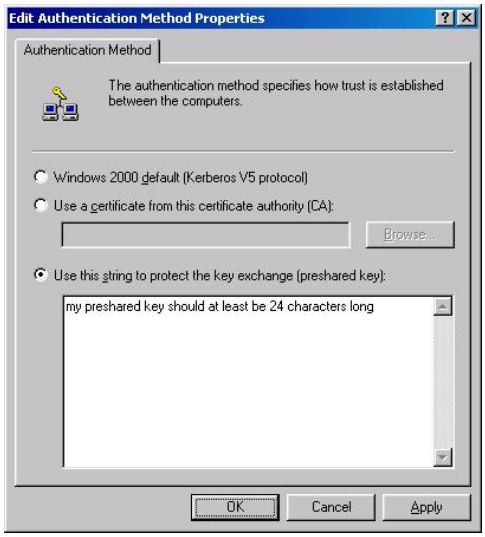
40. Click on 'Tunnel Setting' Tab. Specify the tunnel endpoint as the WAN IP address of the DFL-700.



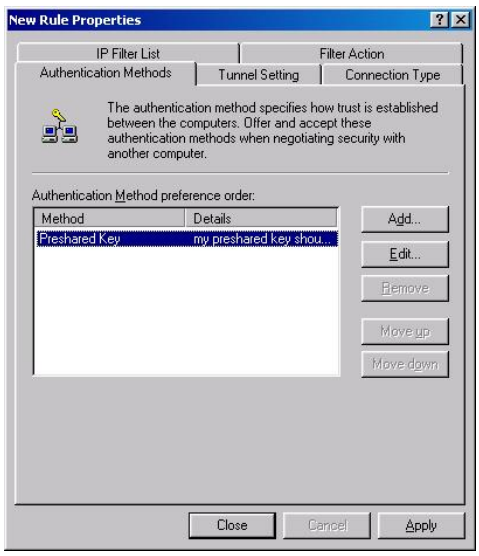
41. Click on 'Authentication Methods' Tab. Click on 'Kerberos' and then Click on 'Edit'.



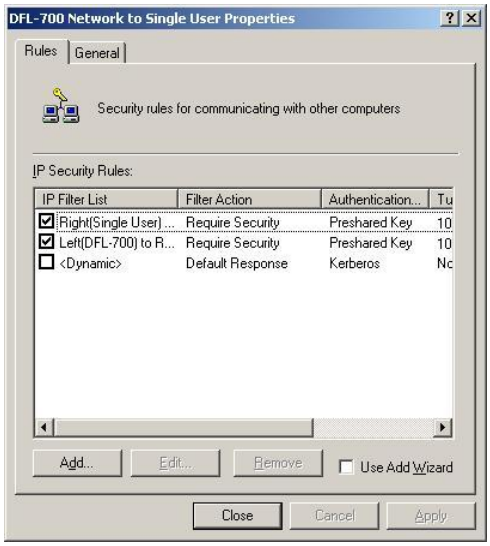
42. Select 'Use this string to protect the key exchange (preshared key)'. Type in the Preshared key. Click 'OK'.



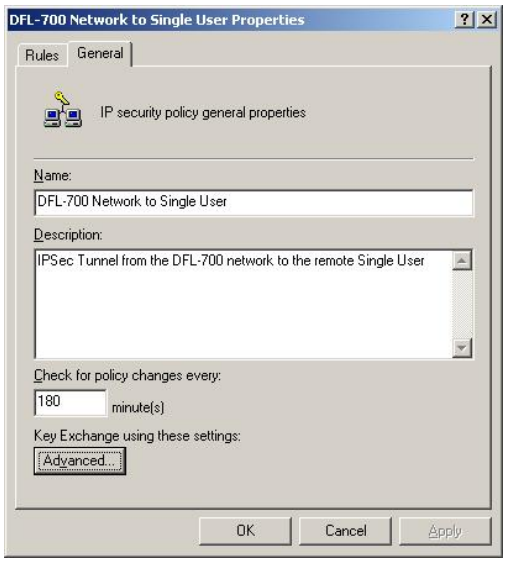
43. Click ‘Close’.



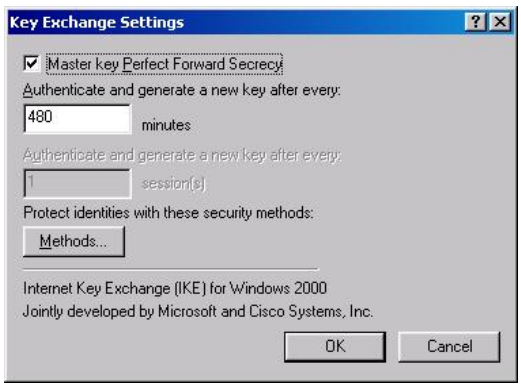
44. Select the newly created rule ‘Right (Single User)….’. Click ‘Close’.



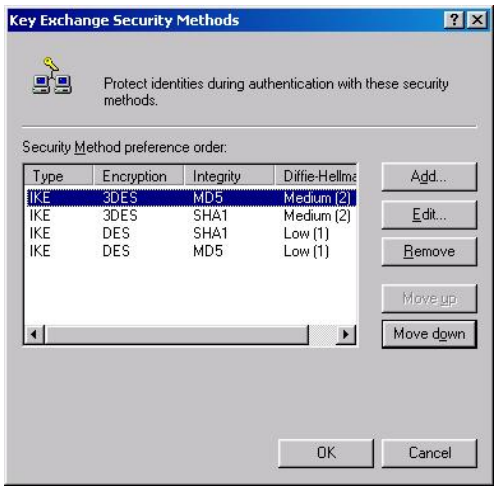
45. Click on General. Click on the ‘Advanced’ Button.



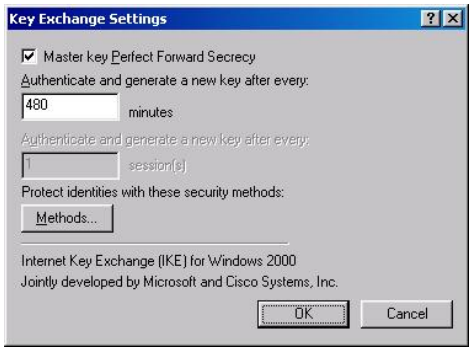
46. Check the 'Master key Perfect Forward Secrecy'. Click on the 'Methods' button.



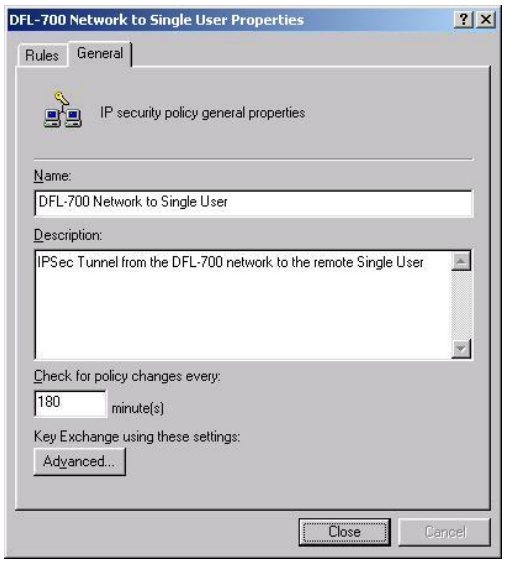
47. Move the IKE/3DES/MD5 to the top. Click 'OK'.



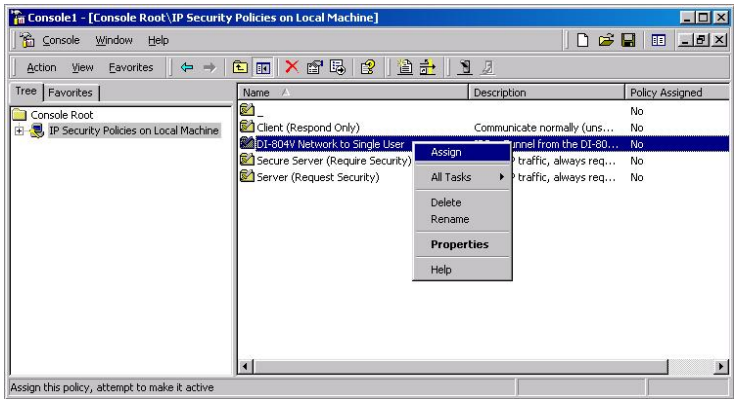
48. Click 'OK'.



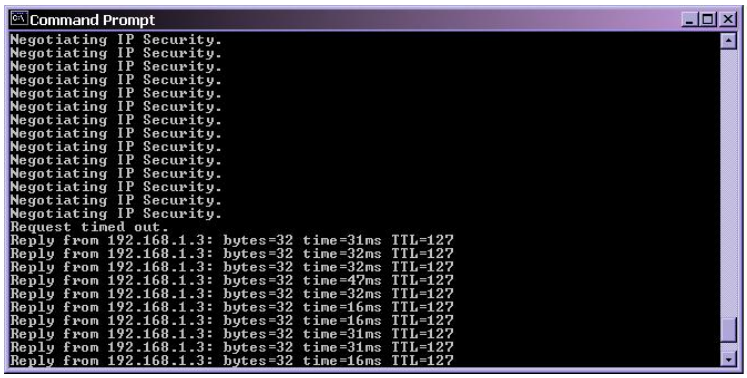
49. Click 'Close'.



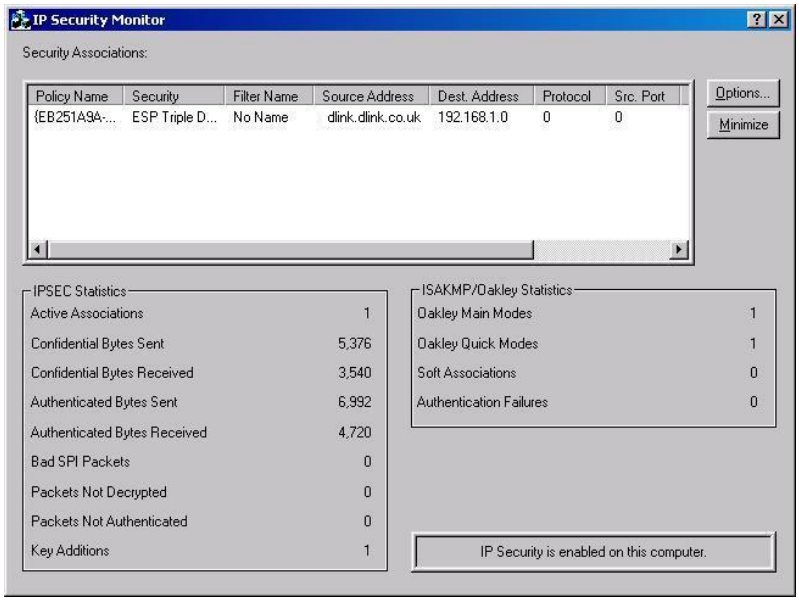
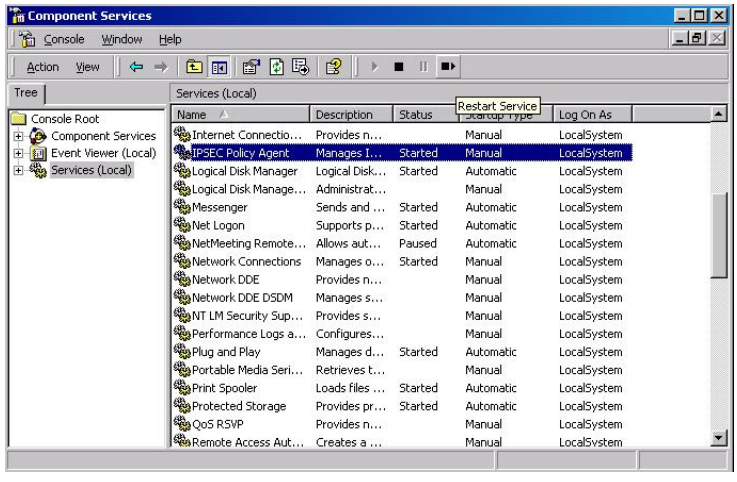
50. Right-click on the new policy and select 'Assign' to activate the policy.



51. You can then ping an Internal LAN IP address on the DFL-700 side (i.e. 192.168.1.3 in this example) in the DOS prompt. It will then start Negotiating IP security and eventually you will get a reply.



52. In Windows 2000 Professional, you can monitor the Ipsec tunnels that you have by running 'IPSECMON.EXE' in Start→ Run. In Windows XP, you can add a snap-in in the MMC called 'IP Security Monitor'.



53. Please note that if you make any changes to the Ipsec policy, you will need to Restart the 'Ipsec Policy Agent' in order for the changes to take effect.