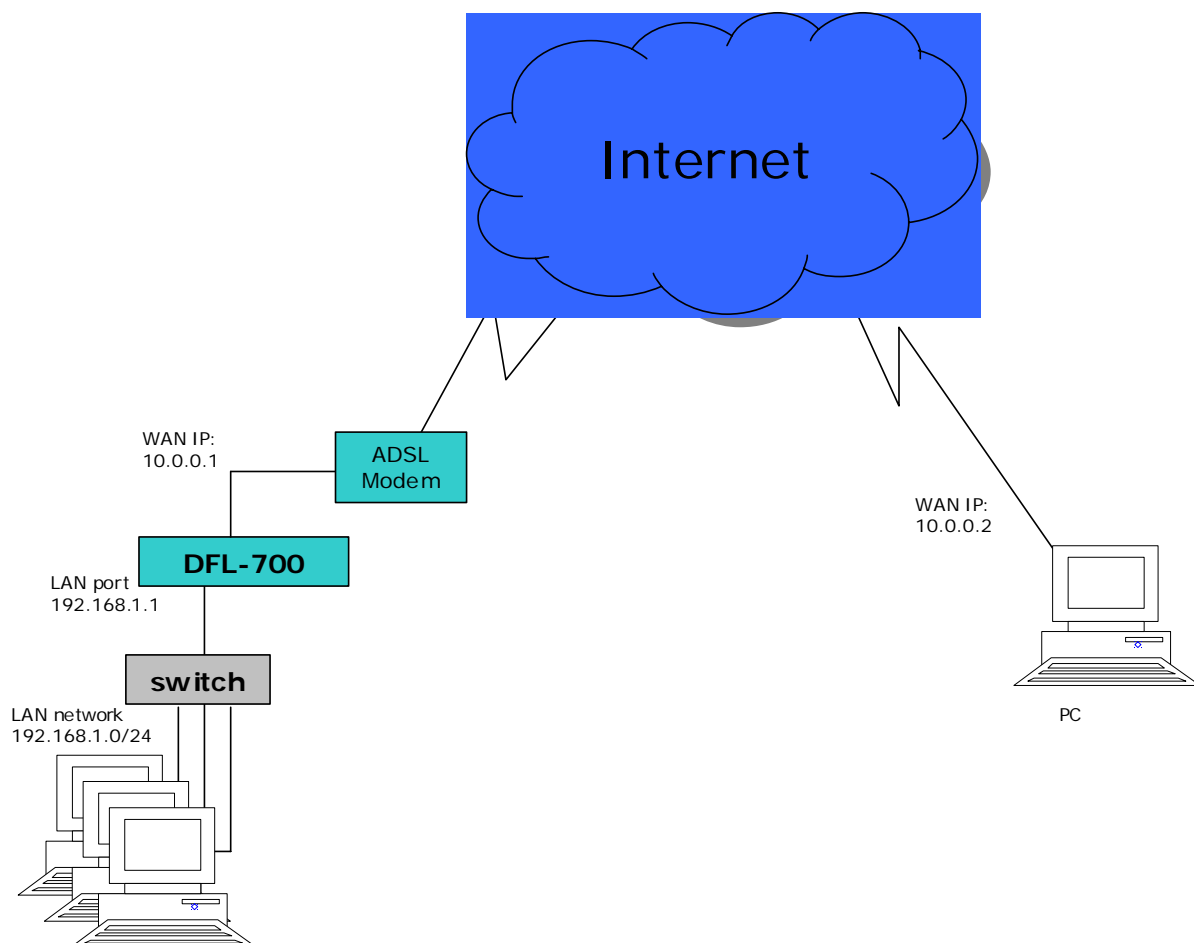


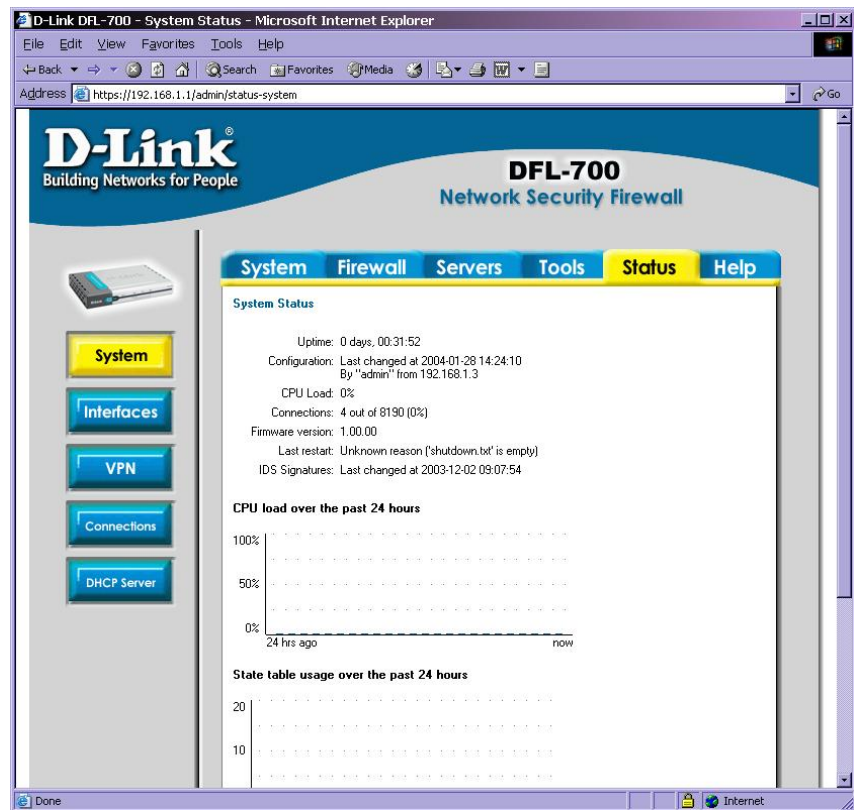
DFL-700 with Windows 2000/XP IPsec VPN Configuration Guide

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.

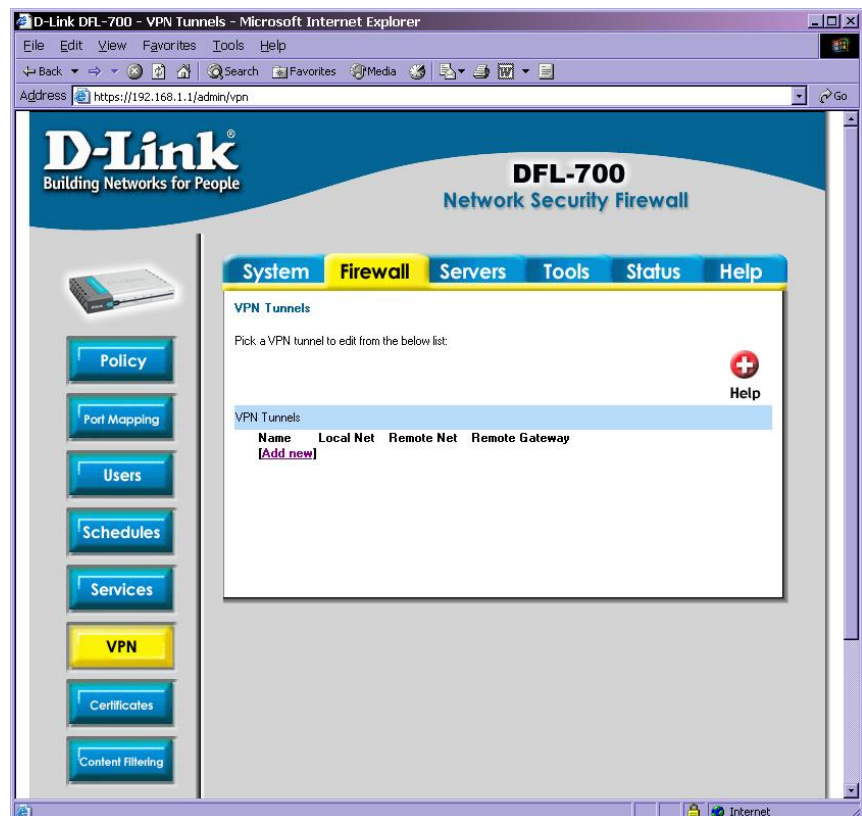
Technical Requirement: Customer is required to understand their network and Windows 2000/XP well for this configuration. Please consult a Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences that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

D-Link DFL-700 - VPN Tunnels - Microsoft Internet Explorer

Address: https://192.168.1.1/admin/vpn?show=

System Firewall Servers Tools Status Help

VPN Tunnels

Add VPN tunnel:

Name:

Local Net:

Authentication:

☒ **PSK - Pre-Shared Key**

PSK:

Retype PSK:

☐ **Certificate-based**

Local Identity:

Certificates:

Identity List:

Tunnel type:

☒ **Roaming Users** - single-host VPN clients

IKE XAuth: ☐ Require user authentication via IKE XAuth to open tunnel

☐ **LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Proxy ARP: ☐ Publish remote network on all interfaces via Proxy ARP

Apply Cancel Help

4. The new VPN profile will now be added

D-Link DFL-700 Network Security Firewall

System Firewall Servers Tools Status Help

VPN Tunnels

VPN tunnel roaming_user added

Pick a VPN tunnel to edit from the below list:

Name	Local Net	Remote Net	Remote Gateway	
roaming_user	192.168.1.0/24	Any	(No gateway)	[Edit]

[\[Add new\]](#)

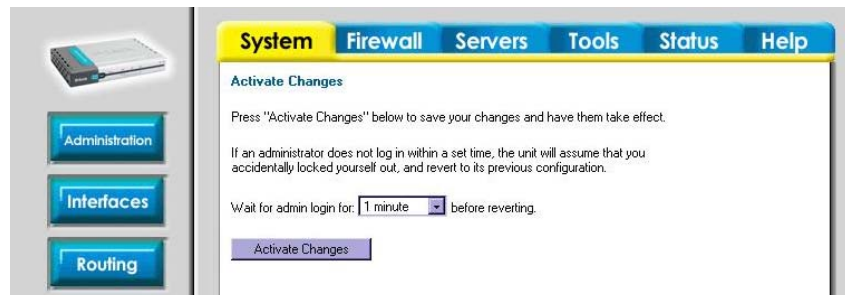
Changes:

Activate Discard

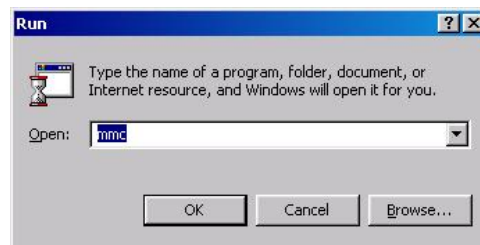
5. Click on '**Activate**' on the bottom left hand corner of the screen to Apply all changes.



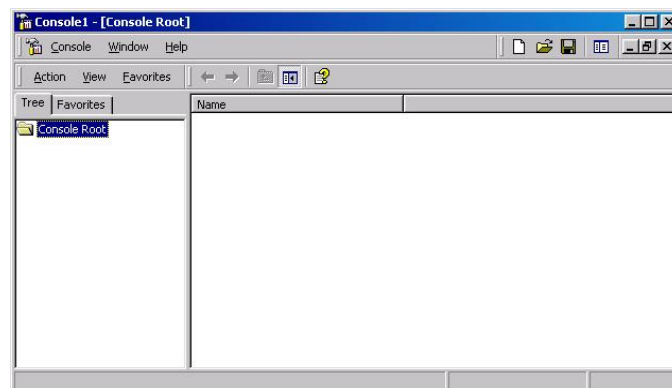
6. Click on '**Activate Changes**' to reboot the DFL-700 with the new settings.



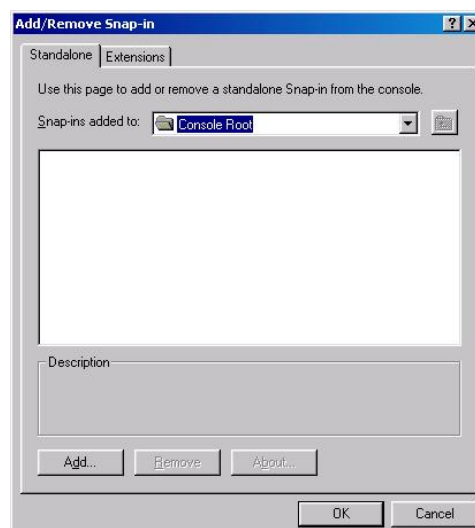
7. Go into Start → Run → and the type in MMC to bring up the Console.



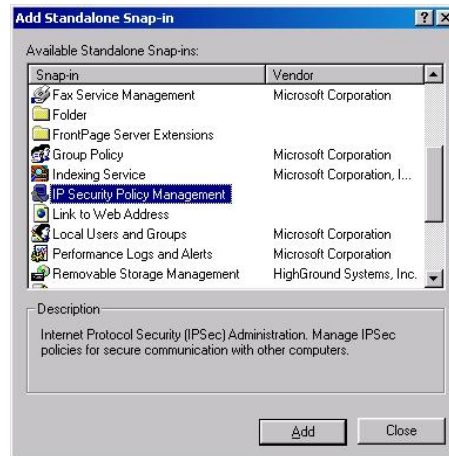
8. Click on Console → and then Click on Add/Remove Snap In.



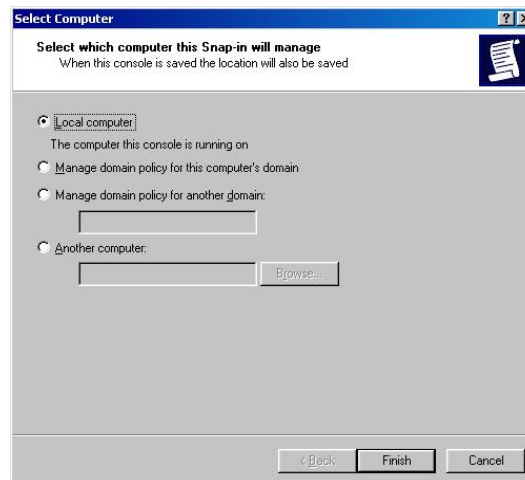
9. Click on the 'Add' Button.



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



11. Select 'Local computer' and then click on Finish.



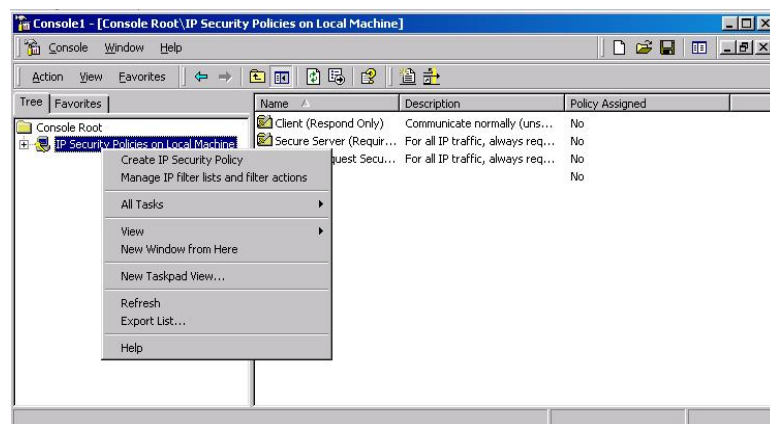
12. Click on 'Close' on the Add Standalone Snap-in window.



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



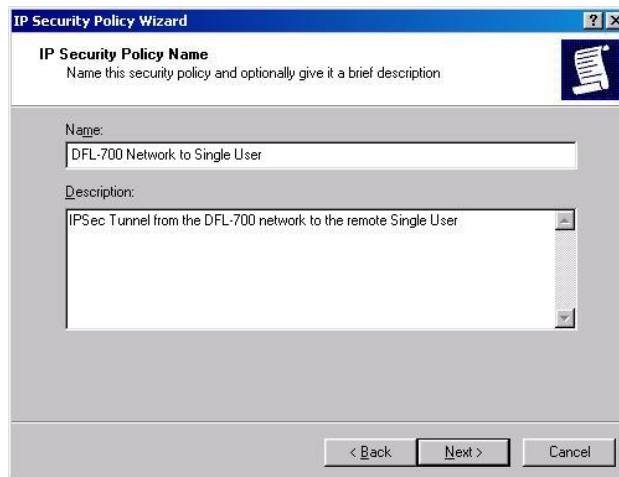
14. Right-Click on IP Security Policies on Local Machine. Select 'Create IP Security Policy'.



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'.



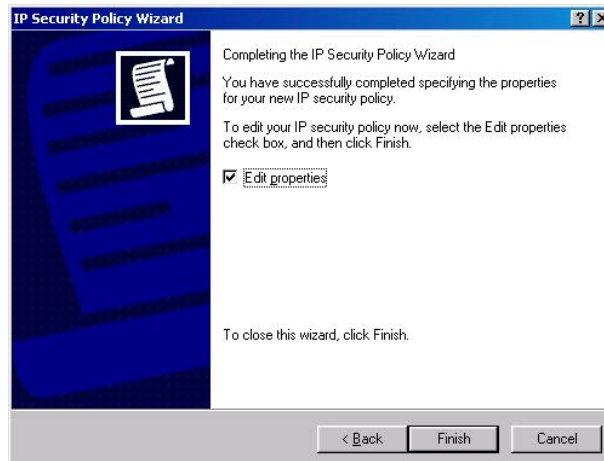
The screenshot shows the 'IP Security Policy Wizard' window, specifically the 'IP Security Policy Name' step. The title bar reads 'IP Security Policy Wizard'. Below the title, it says 'IP Security Policy Name' and 'Name this security policy and optionally give it a brief description'. There are two text input fields: 'Name:' with the text 'DFL-700 Network to Single User' and 'Description:' with the text 'IPSec Tunnel from the DFL-700 network to the remote Single User'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



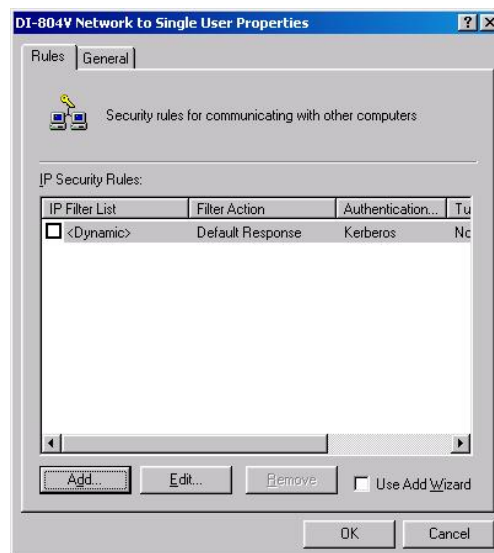
The screenshot shows the 'IP Security Policy Wizard' window, specifically the 'Requests for Secure Communication' step. The title bar reads 'IP Security Policy Wizard'. Below the title, it says 'Requests for Secure Communication' and 'Specify how this policy responds to requests for secure communication'. The main text area contains the following text: 'The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.' Below this text is a checkbox labeled 'Activate the default response rule.' which is currently unchecked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

18. Click on 'Finish'.

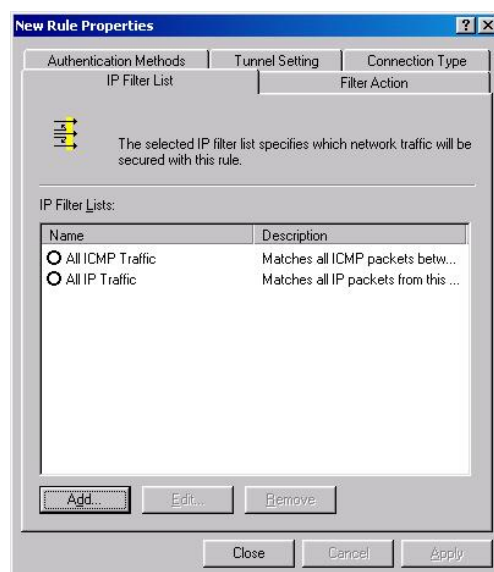


The screenshot shows the 'IP Security Policy Wizard' window, specifically the 'Completing the IP Security Policy Wizard' step. The title bar reads 'IP Security Policy Wizard'. The main text area contains the following text: 'Completing the IP Security Policy Wizard', 'You have successfully completed specifying the properties for your new IP security policy.', 'To edit your IP security policy now, select the Edit properties check box, and then click Finish.', and 'To close this wizard, click Finish.' There is a checkbox labeled 'Edit properties' which is currently checked. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

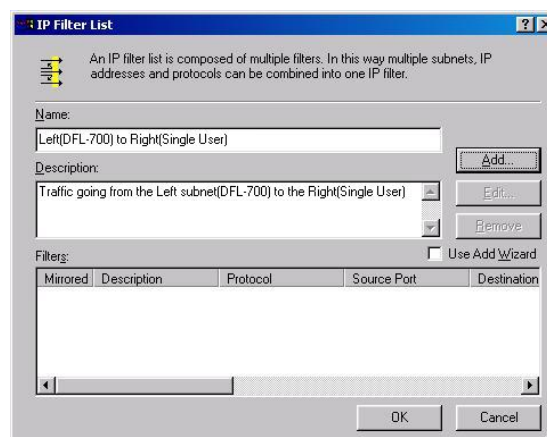
19. The Properties window for the newly created policy should then come up. Click on 'Add'.



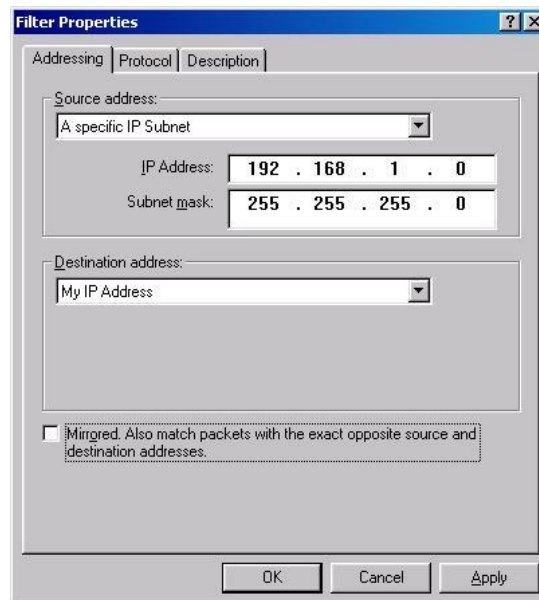
20. Click on 'Add' under IP Filter List.



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

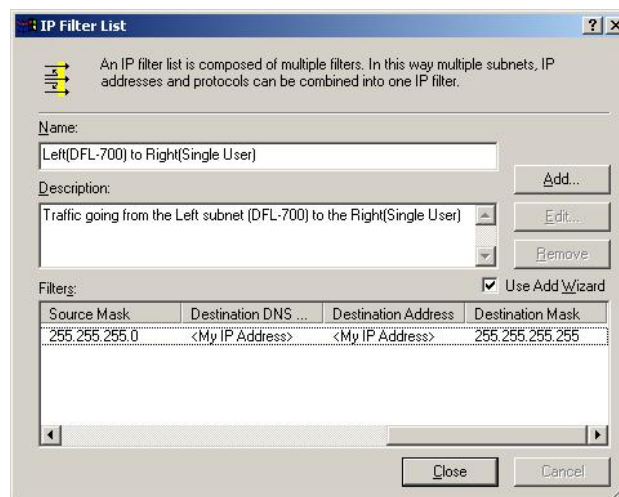


22. Select 'A specific IP subnet' for the 'Source address' and enter the Internal LAN range on the DFL-700 side. Select 'My IP Address' for the 'Destination address'. Uncheck the 'Mirrored....' Option at the bottom of the screen. Click 'OK'.



The 'Filter Properties' dialog box has three tabs: 'Addressing', 'Protocol', and 'Description'. The 'Addressing' tab is active. It contains two sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu is set to 'A specific IP Subnet'. Below it, the 'IP Address' field is '192 . 168 . 1 . 0' and the 'Subnet mask' field is '255 . 255 . 255 . 0'. In the 'Destination address' section, a dropdown menu is set to 'My IP Address'. At the bottom, there is a checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' which is unchecked. At the very bottom are 'OK', 'Cancel', and 'Apply' buttons.

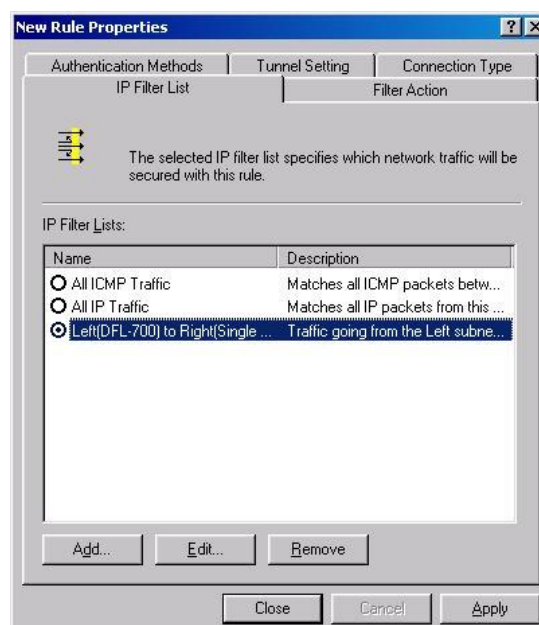
23. Click 'Close'.



The 'IP Filter List' dialog box contains a text area with the instruction: 'An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.' Below this are fields for 'Name' (containing 'Left(DFL-700) to Right(Single User)') and 'Description' (containing 'Traffic going from the Left subnet (DFL-700) to the Right(Single User)'). To the right of these fields are 'Add...', 'Edit...', and 'Remove' buttons. Below the description is a 'Filters:' section with a table. A checkbox 'Use Add Wizard' is checked. The table has four columns: 'Source Mask', 'Destination DNS ...', 'Destination Address', and 'Destination Mask'. It contains one row with values: '255.255.255.0', '<My IP Address>', '<My IP Address>', and '255.255.255.255'. At the bottom are 'Close' and 'Cancel' buttons.

Source Mask	Destination DNS ...	Destination Address	Destination Mask
255.255.255.0	<My IP Address>	<My IP Address>	255.255.255.255

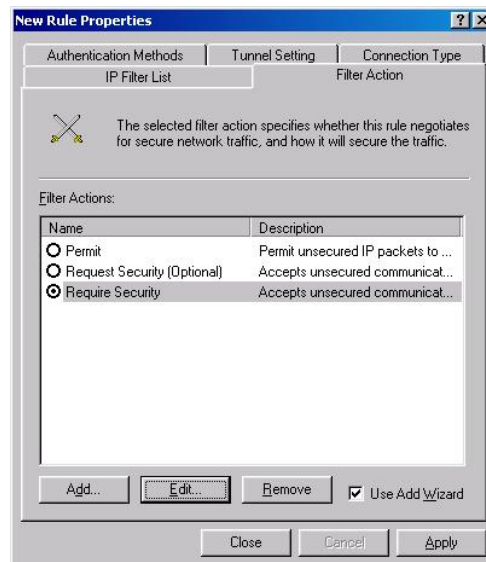
24. Select the newly created IP Filter.



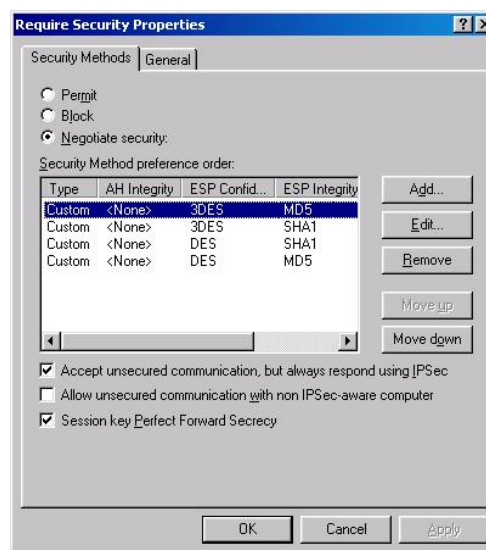
The 'New Rule Properties' dialog box has three tabs: 'Authentication Methods', 'Tunnel Setting', and 'Connection Type'. The 'Authentication Methods' tab is active. It has two sub-tabs: 'IP Filter List' and 'Filter Action'. The 'IP Filter List' sub-tab is active. It contains a text area with the instruction: 'The selected IP filter list specifies which network traffic will be secured with this rule.' Below this is a list box titled 'IP Filter Lists:' containing three items: 'All ICMP Traffic' (radio button), 'All IP Traffic' (radio button), and 'Left(DFL-700) to Right(Single ...)' (radio button, selected). Each item has a description to its right. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom are 'Close', 'Cancel', and 'Apply' buttons.

Name	Description
<input type="radio"/> All ICMP Traffic	Matches all ICMP packets betw...
<input type="radio"/> All IP Traffic	Matches all IP packets from this ...
<input checked="" type="radio"/> Left(DFL-700) to Right(Single ...	Traffic going from the Left subne...

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



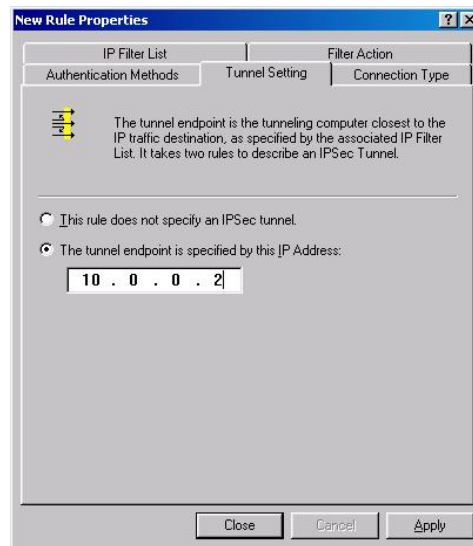
26. Move the 3DES/MD5 security method to the top. Check the 'Session key Perfect Forward Secrecy'. Click 'OK'.



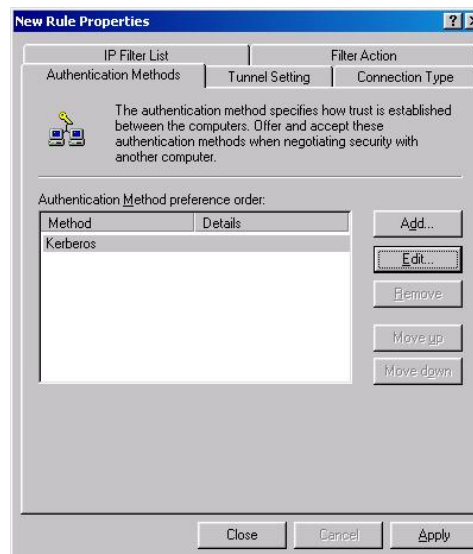
27. Click on 'Connection Type' Tab. Select 'All network connections'.



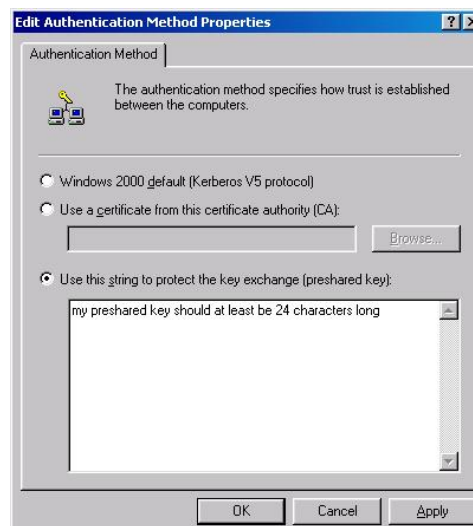
28. Click on 'Tunnel Setting' Tab. Specify the tunnel endpoint as the W2K Pro client IP address (10.0.0.2 in this example).



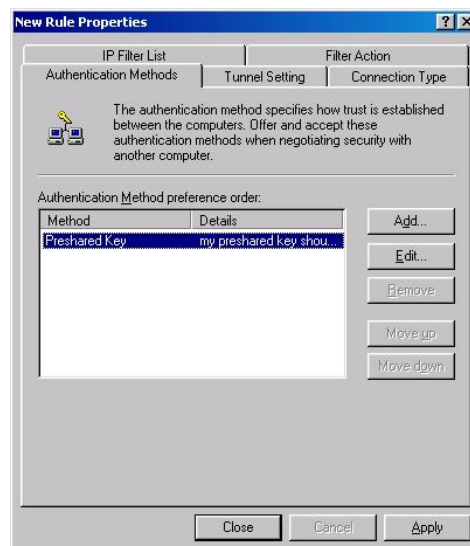
29. Click on 'Authentication Methods' Tab. Click on 'Kerberos' and then Click on 'Edit'.



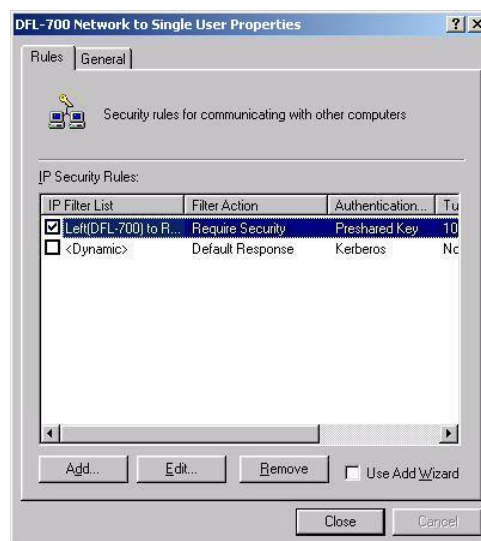
30. Select 'Use this string to protect the key exchange (preshared key)'. Type in the Preshared key. Click 'OK'.



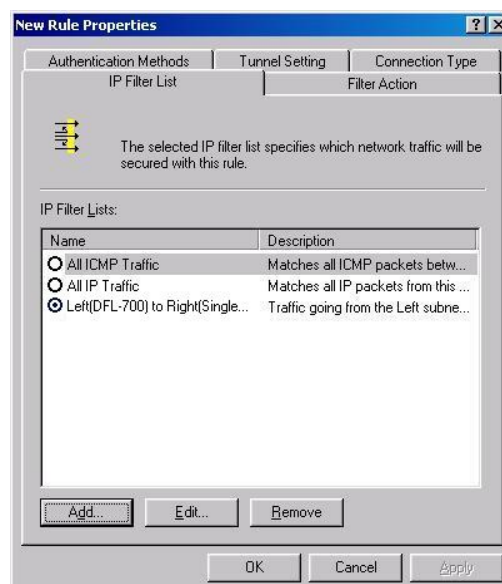
31. Click 'Close'.



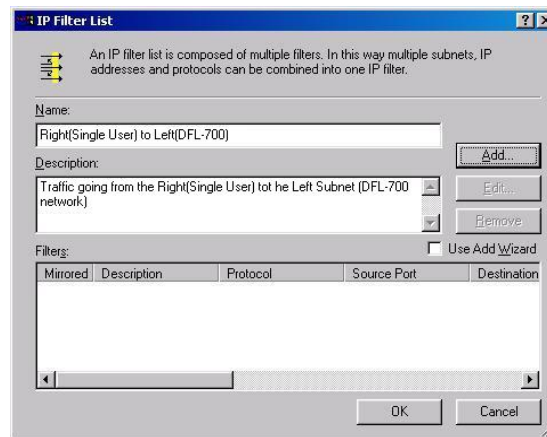
32. Select the newly created rule. Click on 'Add'.



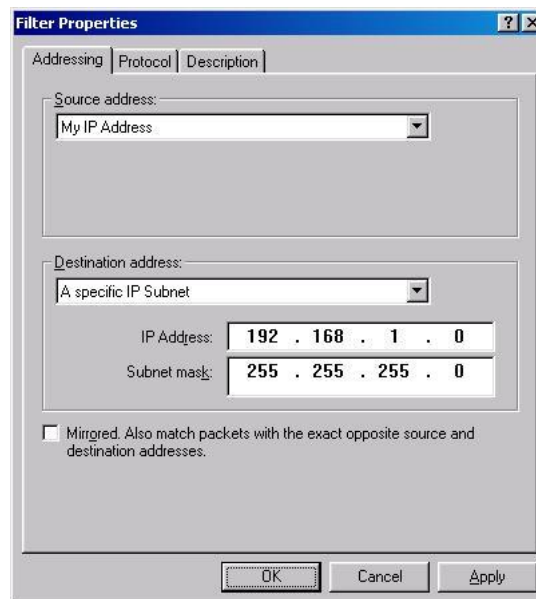
33. Click on 'Add' under IP Filter List.



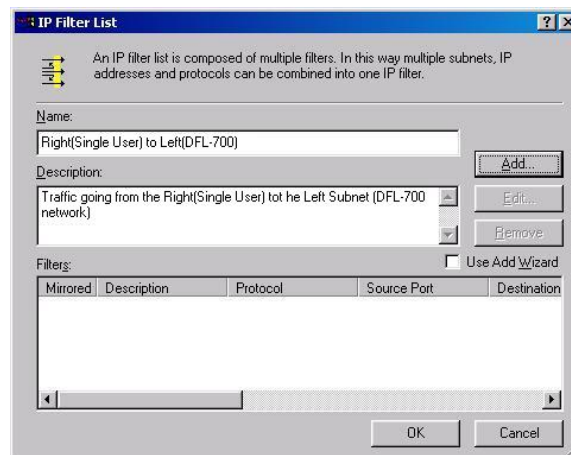
34. Enter the name and the description for the New IP Filter List. Uncheck the 'Use Add Wizard'. Click on 'Add'.



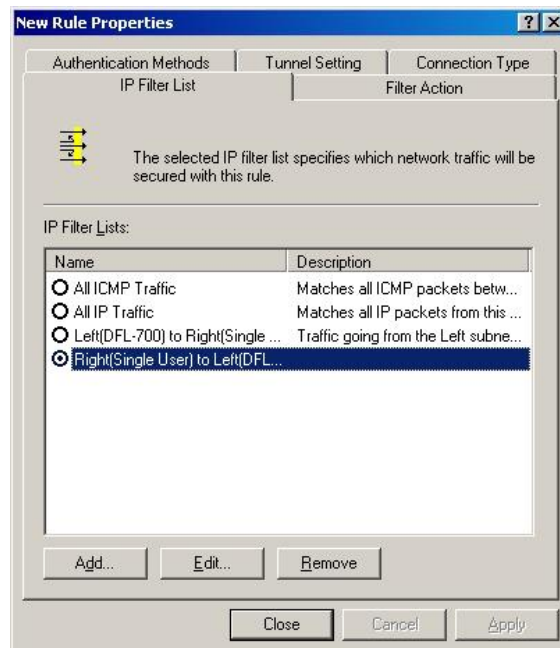
35. Select 'My IP Address' for the 'Source address'. Uncheck the 'Mirrored....' Option at the bottom of the screen. Select 'A specific IP subnet' for the 'Destination address' and enter the Internal LAN range on the DFL-700 side. Click 'OK'.



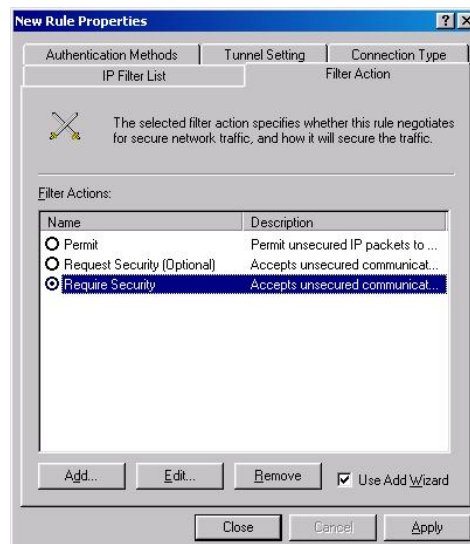
36. Click on 'Close'.



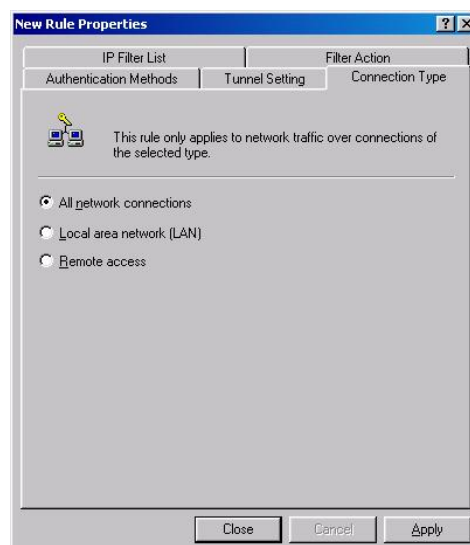
37. Select the newly created IP Filter 'Right (Single User) to Left (DFL-700...)'.



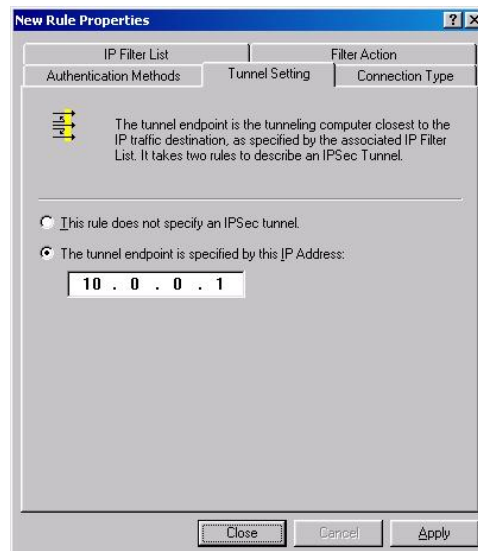
38. Click on the 'Filter Action' Tab. Select 'Require Security'. You don't need to click on Edit.



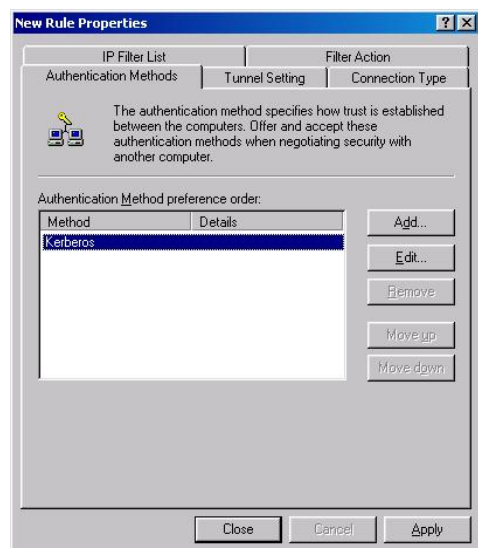
39. Click on 'Connection Type' Tab. Select 'All network connections'.



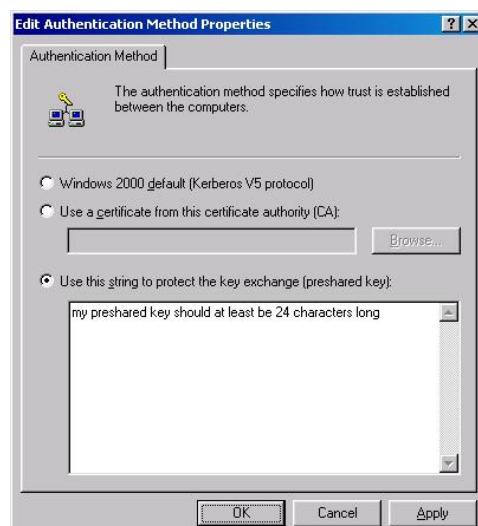
40. Click on 'Tunnel Setting' Tab. Specify the tunnel endpoint as the WAN IP address of the DFL-700.



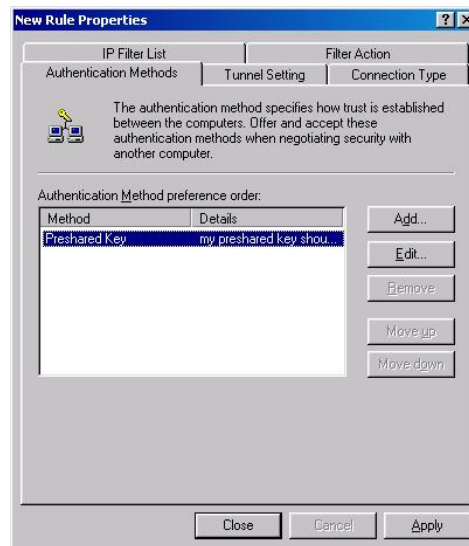
41. Click on 'Authentication Methods' Tab. Click on 'Kerberos' and then Click on 'Edit'.



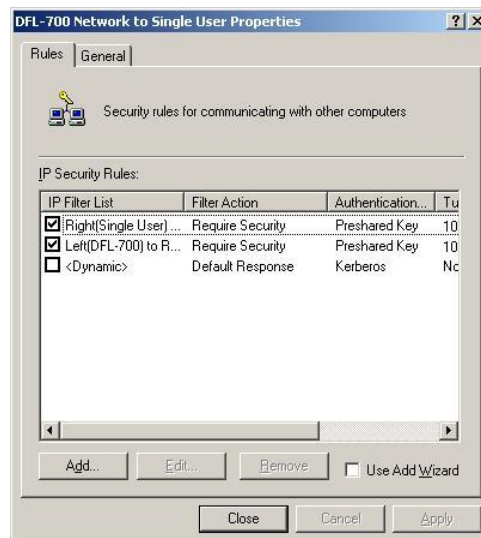
42. Select 'Use this string to protect the key exchange (presared key)'. Type in the Presared key. Click 'OK'.



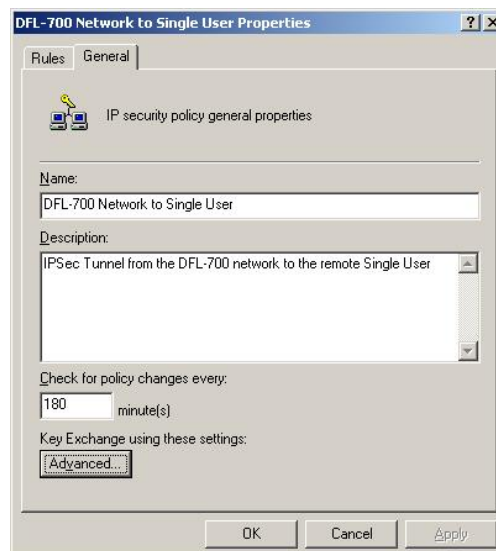
43. Click 'Close'.



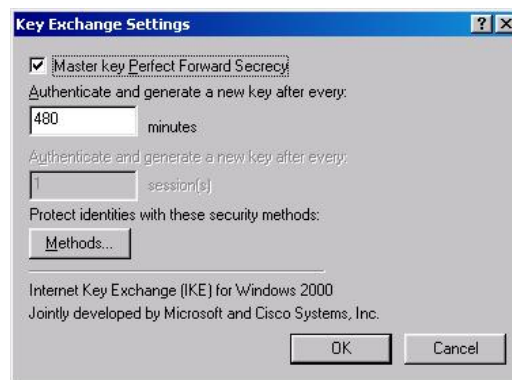
44. Select the newly created rule 'Right (Single User)....'. Click 'Close'.



45. Click on General.
Click on the 'Advanced' Button.



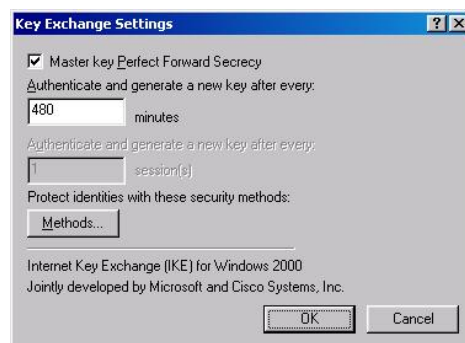
46. Check the 'Master key Perfect Forward Secrecy'. Click on the 'Methods' button.



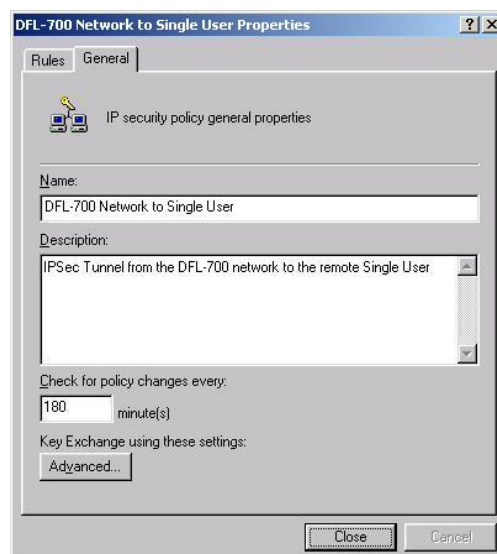
47. Move the IKE/3DES/MD5 to the top. Click 'OK'.



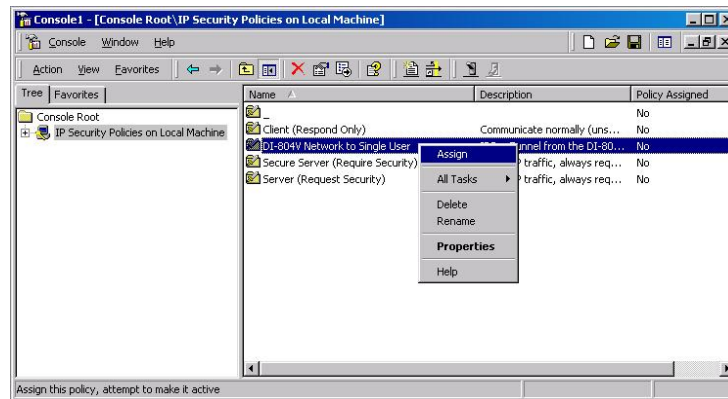
48. Click 'OK'.



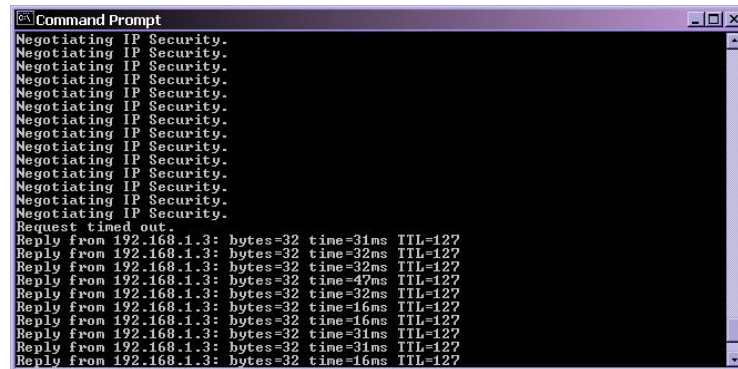
49. Click 'Close'.



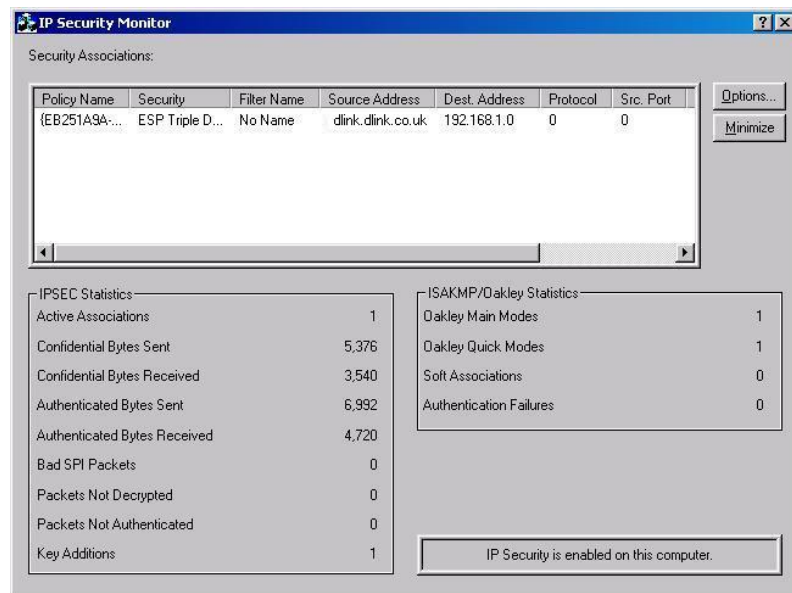
50. Right-click on the new policy and select 'Assign' to activate the policy.



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.

