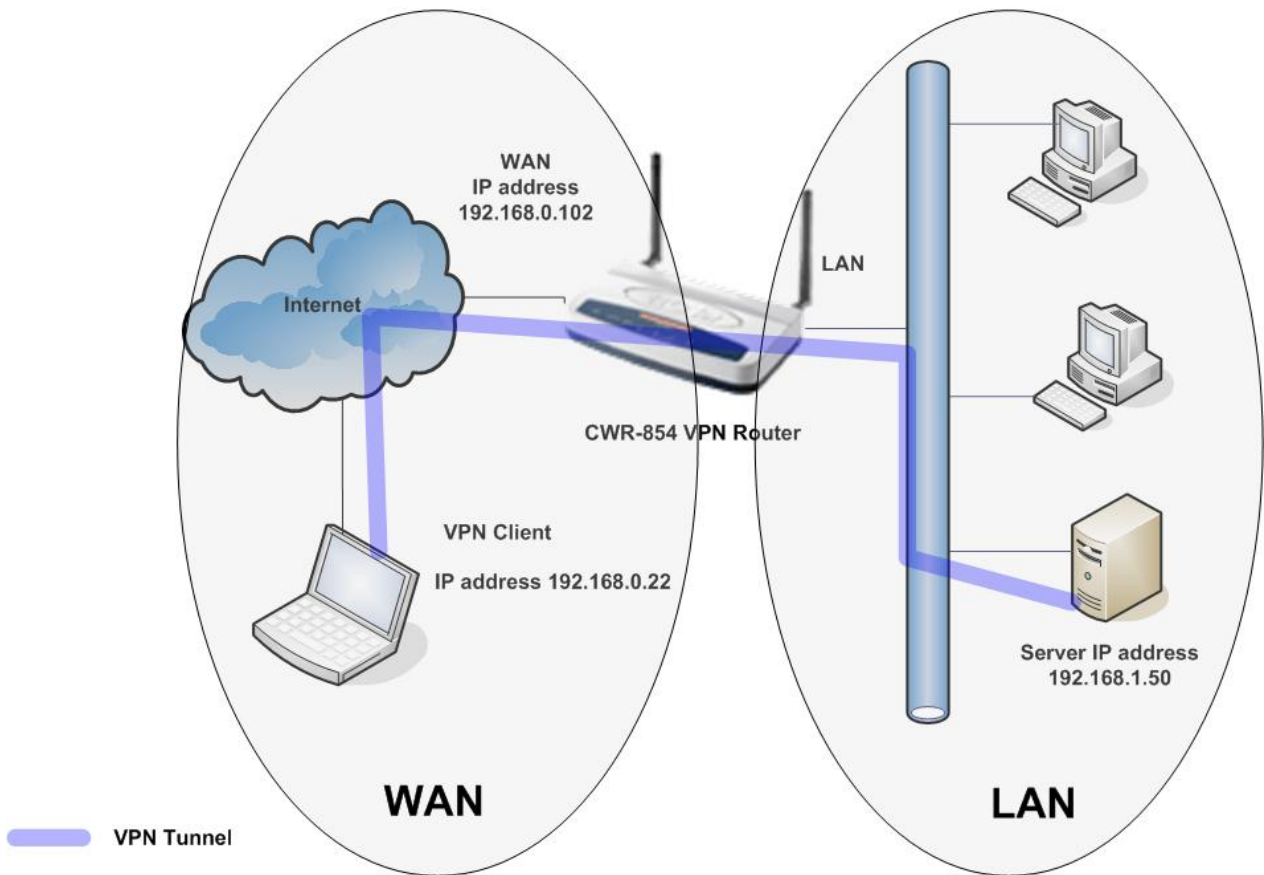


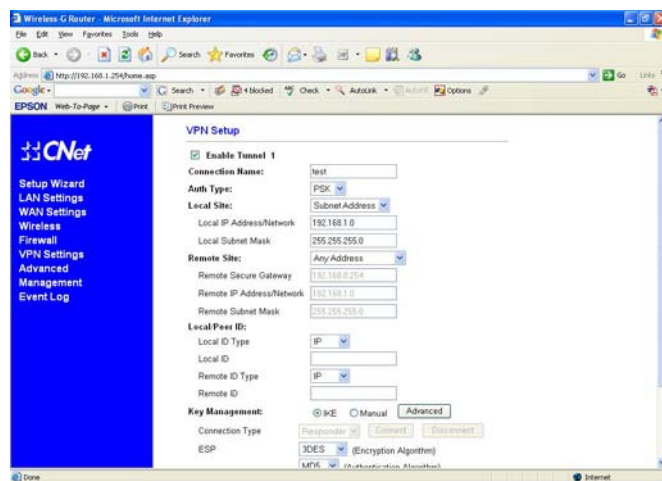
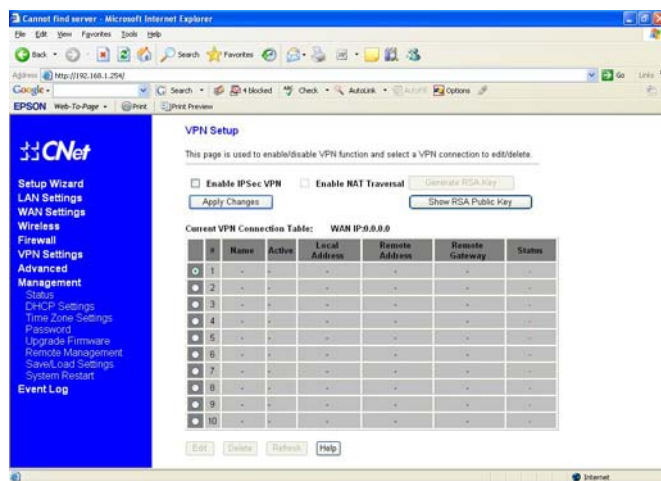
Establishing a VPN tunnel to CNet CWR-854 VPN router using WinXP IPsec client

Generally speaking, remote users need to use a VPN client software for establishing a VPN connection to their home/work router and access the network behind that router. Windows XP and 2000 have a built-in IPsec client that while difficult to configure, will actually work for building a VPN tunnel and connecting to the network behind a VPN router. The picture below shows the network that we'll use for setting up and testing the WinXP IPsec client.

VPN setup using WinXP IPsec client



The first step is to configure the router and enable IPsec VPN. Please use a computer connected to one of the LAN ports on CWR-854 for configuration. Default IP address of CWR-854 is 192.168.1.254, username and password are “root” and “1234” respectively. After accessing the web configuration page, select VPN Settings from the left menu and enable IPsec VPN and NAT Traversal. CWR-854 supports 10 different VPN profiles, click edit to configure profile # 1.



In the VPN setup page, “Local Site” is the network on the LAN side of the router and “Remote Site” is where the VPN client is. For the local site we can configure the VPN to provide access to a single computer or the subnet behind the router. If only a single computer is to be accessed we need to enter the IP address of that computer, otherwise the network IP address (LAN side) needs to be selected. The default network address is 192.168.0.1.

Remote site configuration is also similar. We can select VPN from a specific address, a subnet or any address. In this test we choose VPN from any address.

We are using PSK (pre shared key) for authentication and 3DES and MD5 are the “encryption” and “authentication” algorithms used.

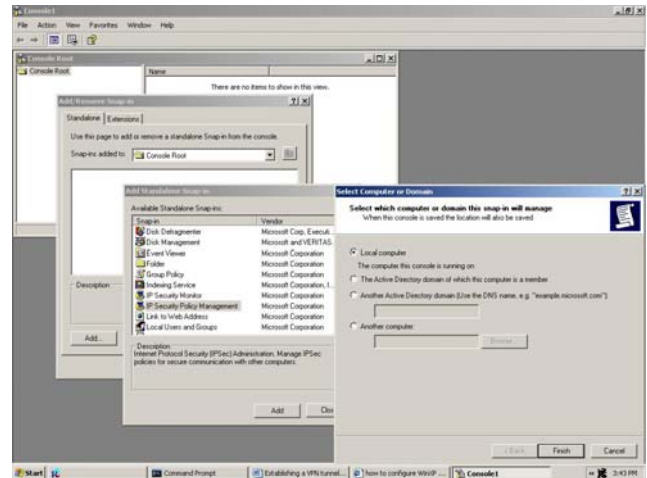
At this stage we need to enter a Pre Shared Key to finalize the VPN setup on the router. This same key we be used by VPN clients to establish the tunnel later on.

WinXP IPSec client configuration:

What we're doing is to configure/create an IPSec local security policy on the VPN client system so that it connects to the endpoint IPSec router and establishes a VPN tunnel. It must be noted that for WinXP IPSec client to work, the LAN clients behind the VPN router should have static IP addresses and the two ends of the VPN tunnel must be on different subnets. In our example the LAN subnet is 192.168.1.0 and the WAN subnet is 192.168.0.0.

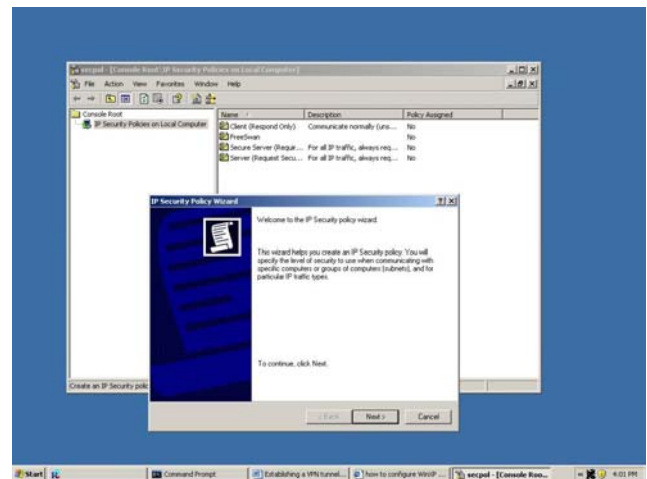
Adding a security policy Snap-in

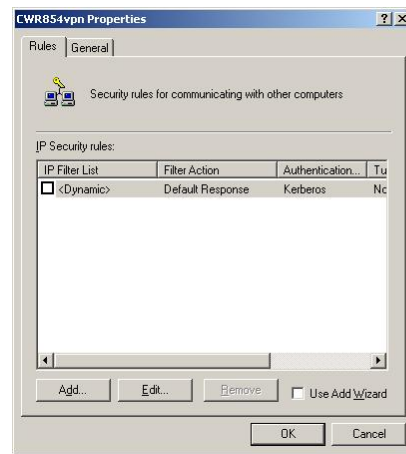
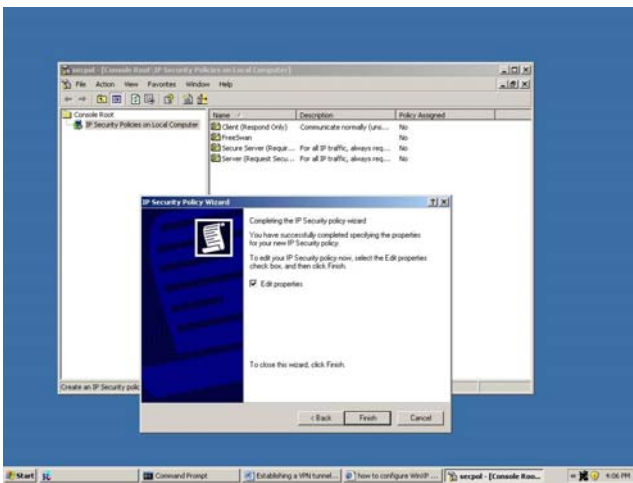
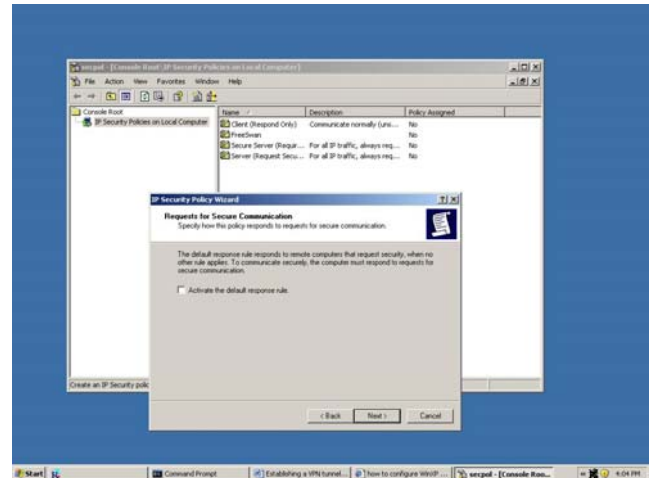
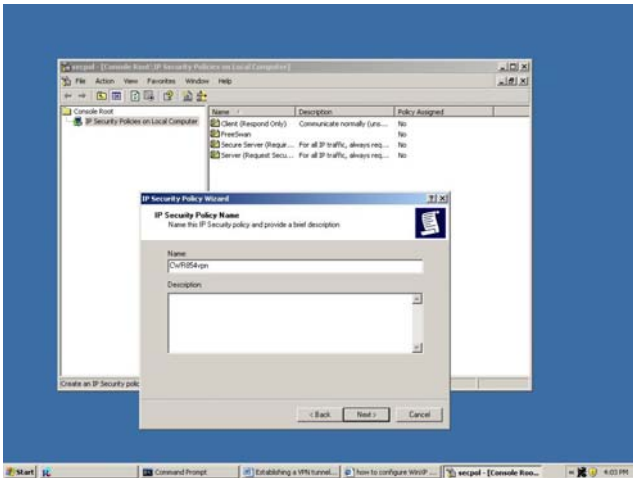
1. Go to start>>Run>> and type mmc and click OK
2. In console window choose file>>add/remove snap-in
3. Click add
4. Select IP Security Policy Management>> add
5. Select Local Computer and Finish
6. Close all windows
7. When closing the console window, save the settings to your desktop. Choose a file name of secpol.msc
8. You should now have a file called secpol.msc on the desktop



Creating an IPSec Policy

1. Double click the secpol.msc icon on the desktop
2. Right click on IP Security Policy on local computer and click Create IP Security Policy
3. Click next on the wizard page, enter a name for the policy (we use CWR854vpn) and click next
4. Deselect the Activate the default response rule check box and click next
5. Click the finish button making sure the Edit properties box is checked
6. The properties window of the new security policy will open up

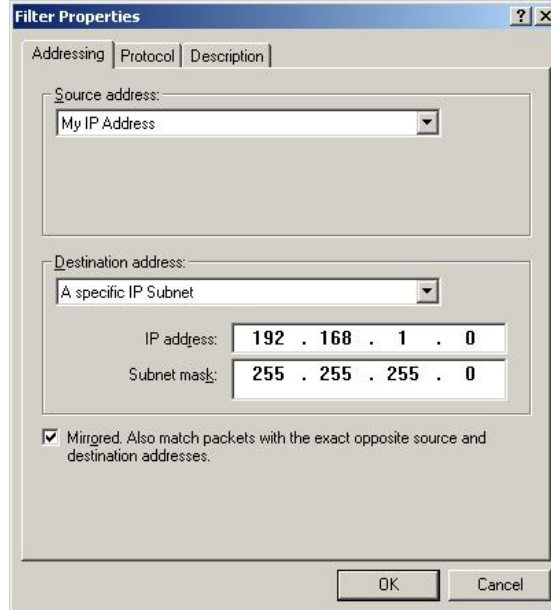
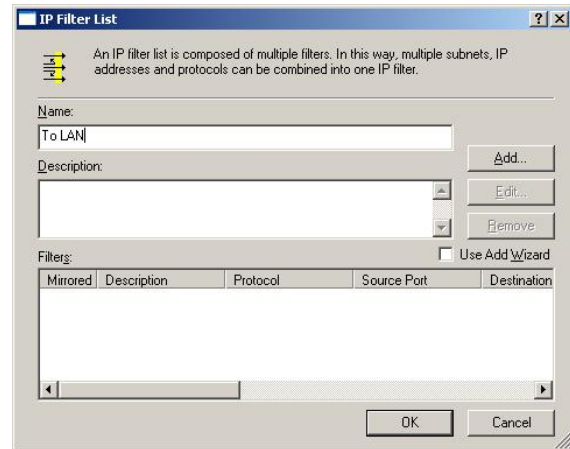
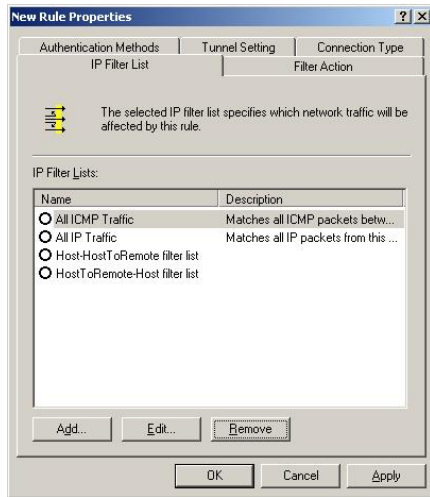




With the CWR854vpn properties window open, we're basically going to define two new security rules. One for traffic to the VPN router called **TO LAN** and one for traffic from the router called **From LAN**.

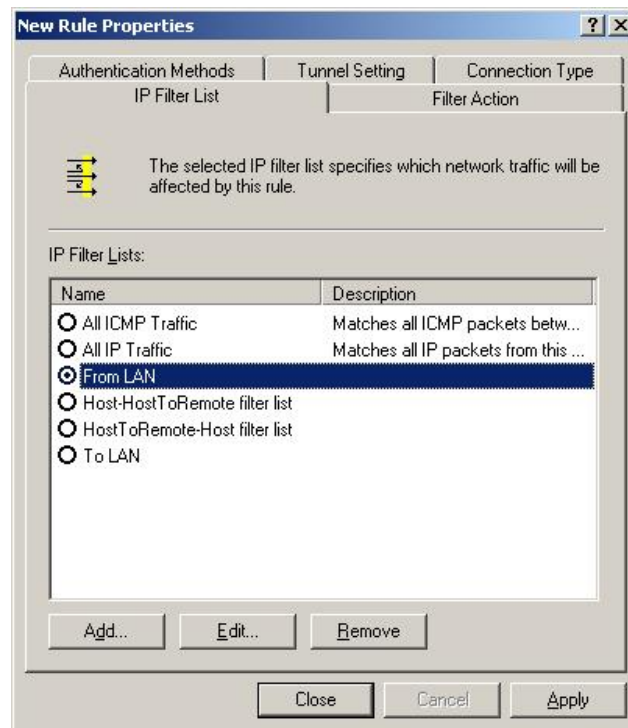
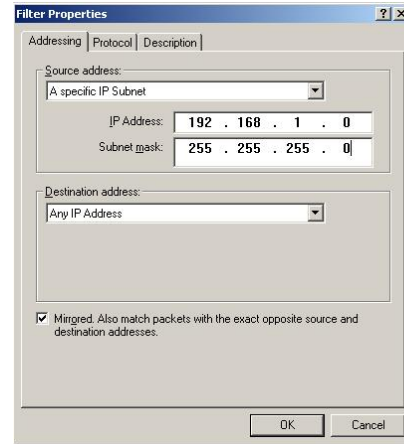
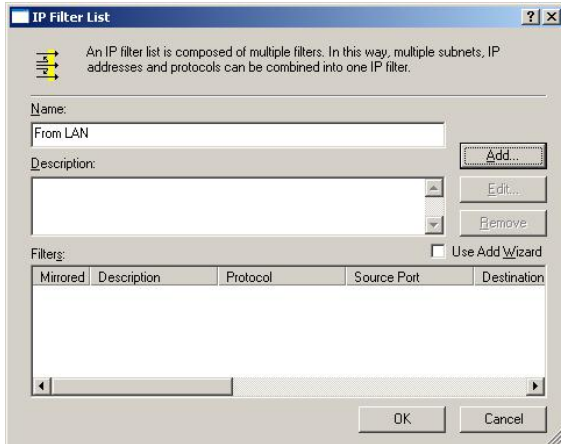
Creating the To LAN rule:

In the properties box make sure the Add Wizard box is unchecked and click on Add. In the New Rule Properties window, click on the Add button under the IP Filter list tab and then in the IP Filter list window type To LAN in the name box, deselect add wizard and click on Add.

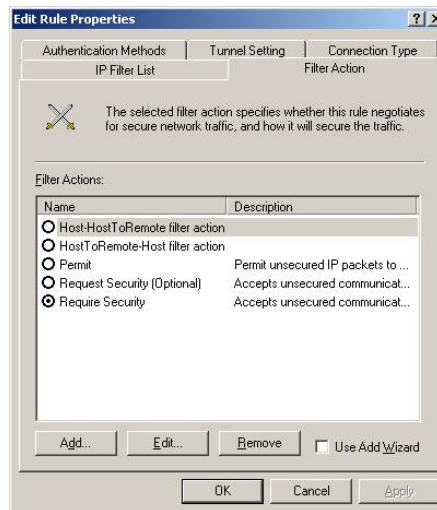
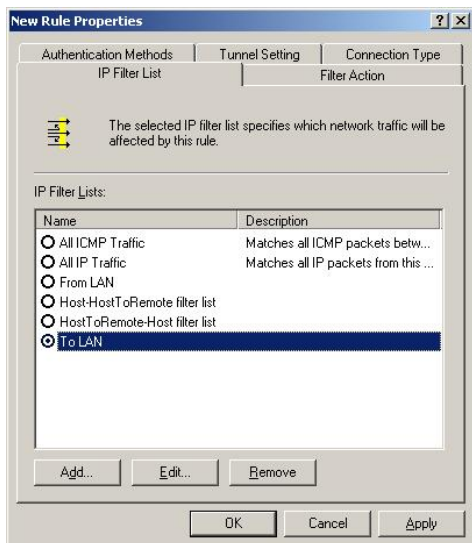


Creating the From LAN rule:

We're basically going to repeat the steps for To LAN rule except we will name the rule From LAN and have different source and destination IP addresses as figures below will indicate.

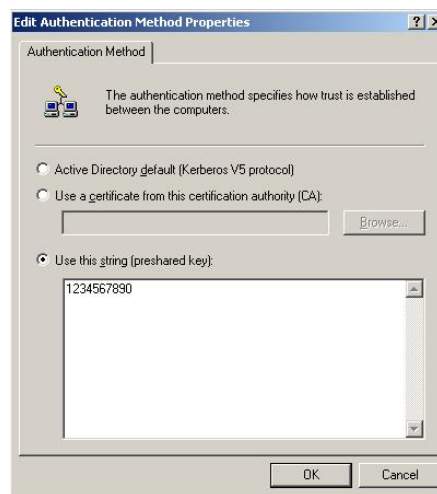
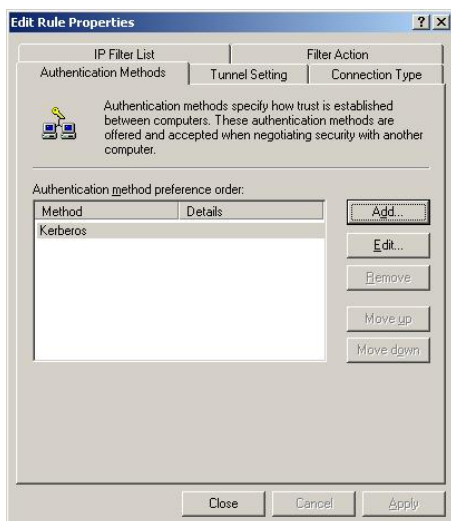


After the two new security rules are created, we need to edit and configure each rule. From the cwr854vpn, select the To LAN rule and make sure that its box is checked and click on edit. The new rule properties window should come up as below. Click on Filter Action tab and select require security and click the edit button.

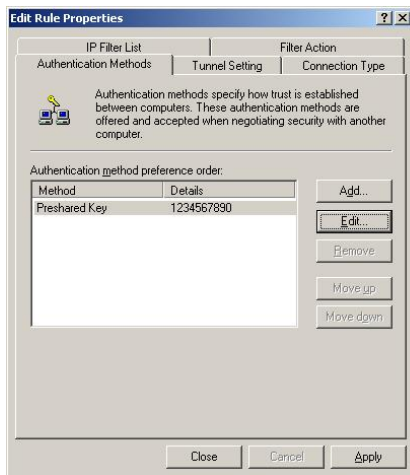


In the security properties window, make sure the settings are as figure below. Type should be Custom, AH integrity None, ESP confidentiality 3DES and ESP integrity MD5. Please note that we used the same authentication and encryption protocols when configuring VPN on CWR-854 router. If you need to change the security method, highlight it and click on edit. When done, click on OK to go back to edit rule properties window.

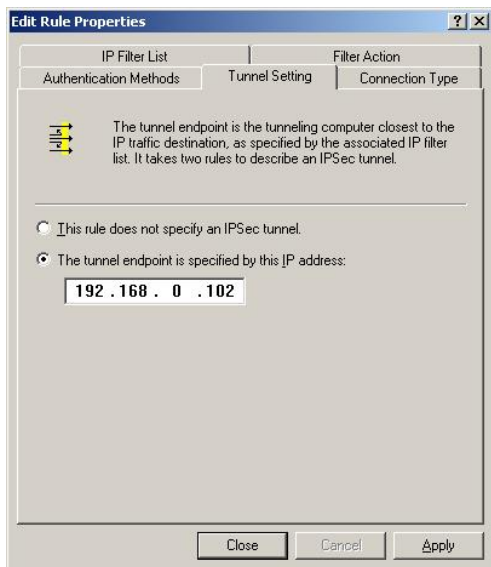
In the edit rule window, select the Authentication Methods tab and click the add button. In the Auth. Methode properties window select the box for preshared key and enter the key used in the router's VPN configuration.



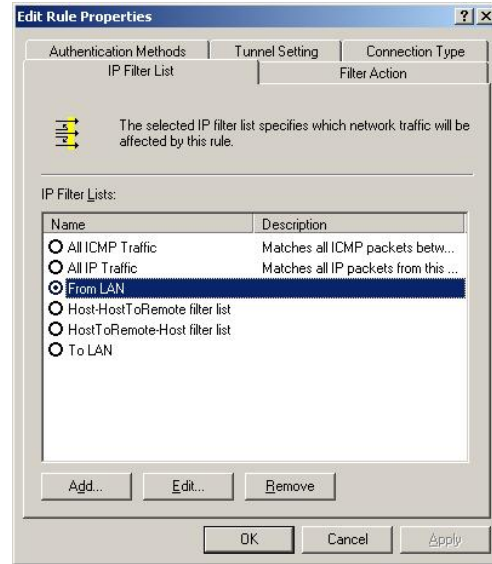
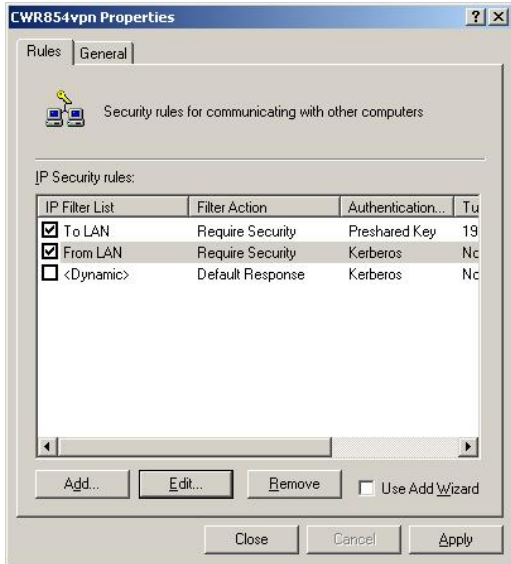
After entering the pre-shared key, the authentication methods tab should have pre-shared for method and the string you entered under details.



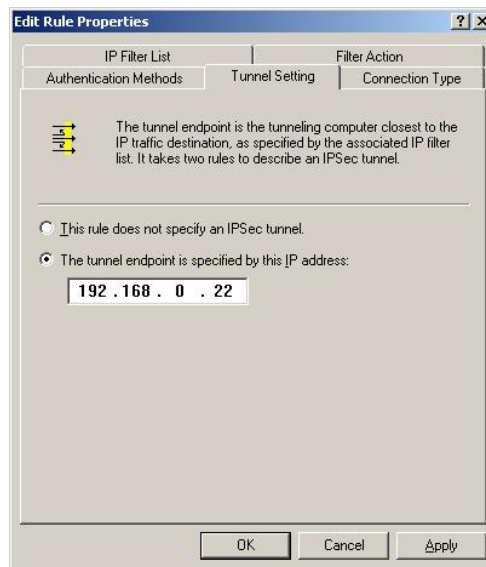
The next parameter to configure is the Tunnel Settings, select the Tunnel Settings tab and enter the WAN IP address of the remote VPN router. In our example the WAN IP of the router is 192.168.0.102. The last parameter for the To LAN rule is the connection type. Select the tab and make sure All network connections radio button is checked.



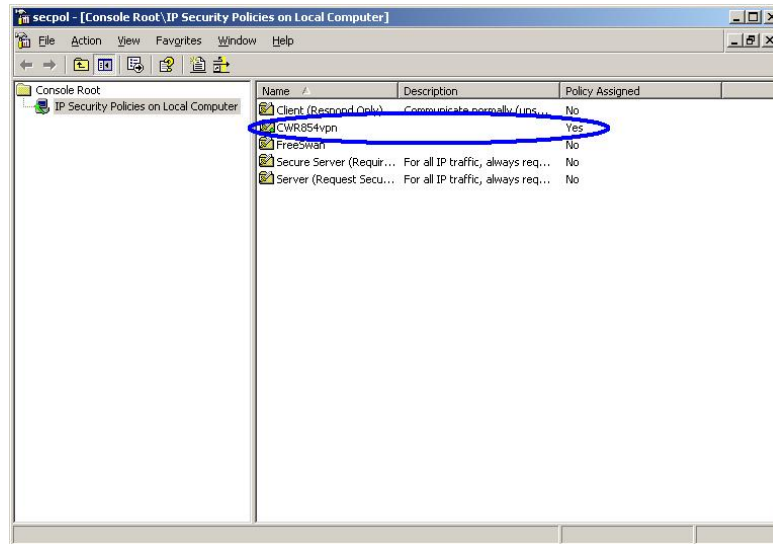
The To LAN rule configuration is complete. Click close to return the cwr854vpn properties page. Now the From LAN rule is to be configured. We basically have to set the same parameters as for the To LAN rule.



Select each tab as we did for To LAN rule starting with the filter action tab. All tabs are going to have the exact settings as To LAN except the Tunnel setting tab which needs the IP address of the client computer. In our example the address is 192.1680.22.



When all parameters are set click on OK and close to go the secpol window. Right click on cwr854vpn policy and choose assign. Make sure there is a **YES** in the policy assigned column for the cwr854vpn policy. This completes the IP security policy configuration on this computer. The policy will automatically start each time the computer is booted.



Testing the connection:

In situations that both the VPN router on the WAN side and VPN client have routable IP addresses, the configuration above should work. In situations that for example the VPN client has a private IP address (when it is behind another router), we might have to add a static route to the client system so it would know how to route packets to the LAN systems behind the VPN router. In order to add the static route, on the VPN client system open a Command Prompt window and enter the command below:

Route add 192.168.1.0 mask 255.255.255.0 192.168.0.102 , when added the client system will route packets destined for network 192.168.1.0 through the WAN IP address of the VPN router. To check the routing table on the system, issue the route print command:

```

C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 08 a1 7e 33 1a ..... Realtek RTL8139 Family PCI Fast Ethernet NIC #2
- Packet Scheduler Miniport
=====
Active Routes:
Network Destination     Netmask          Gateway          Interface        Metric
0.0.0.0                 0.0.0.0          192.168.0.50     192.168.0.22     20
127.0.0.0               255.0.0.0        127.0.0.1        127.0.0.1        1
192.168.0.0             255.255.255.0    192.168.0.22     192.168.0.22     20
192.168.0.22           255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.0.255         255.255.255.255  192.168.0.22     192.168.0.22     20
192.168.1.0            255.255.255.0    192.168.0.102    192.168.0.22     1
224.0.0.0              240.0.0.0        192.168.0.22     192.168.0.22     20
255.255.255.255       255.255.255.255  192.168.0.22     192.168.0.22     1
Default Gateway:       192.168.0.50
=====
Persistent Routes:
None
C:\>

```

Static route

Now when we ping the remote system behind the VPN router we will see the IPSec negotiations and finally VPN Tunnel creation between the client and the router.

```

C:\>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Negotiating IP Security. -----> client system negotiates IP security
Request timed out.
Reply from 192.168.1.100: bytes=32 time=5ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
VPN Tunnel created
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms
C:\>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:

```