Using the Windows XP VPN Client with SonicWALL Internet Security Appliances

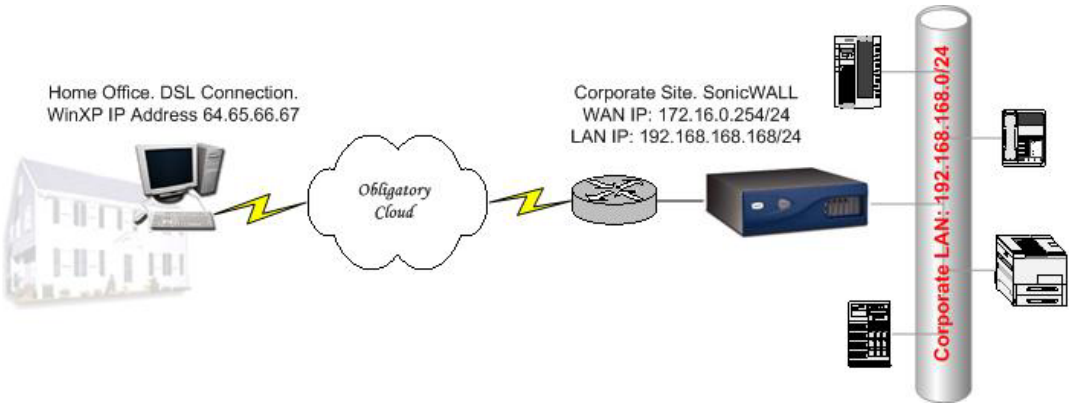
Prepared by SonicWALL, Inc.
01/03/2002

Introduction

Despite its many similarities to Windows 2000, Microsoft's Windows XP is very much a different product. Microsoft designed XP with security in mind, and among the implications of this focus was a redesign of the networking subsystem. Because of these changes, VPN clients that worked with Windows 2000 do not work with Windows XP. Most VPN client vendors, SonicWALL included, do not yet have available a VPN client that works with XP, causing some difficulty for those enterprises looking to deploy Microsoft's latest OS. Both Windows XP and its predecessor Windows 2000 have VPN support built in—PPTP and L2TP—but neither of these is compatible with standard IPSec VPN's, despite the fact that the latter is a subset of the IPSec standard. This precludes the better-known VPN capabilities from natively connecting to another *true* IPSec endpoint, such as that offered by a SonicWALL.

Fortunately, Microsoft also saw fit to include true IPSec capabilities in 2K and XP, but they did not wrap them in a friendly wizard. With a few minutes of configuration via the MMC, however, it is quite simple to set up Windows XP as a VPN client to a SonicWALL VPN. This will allow current XP clients to remotely and securely access their SonicWALL protected corporate networks, and will also allow those enterprises that have been delaying XP deployment because of VPN access considerations to deploy immediately.

Configuring an IPSec VPN between Windows XP and a SonicWALL requires no changes to the SonicWALL configuration. This document assumes the SonicWALL is configured with an existing GroupVPN, and it will illustrate step-by-step how to complete the Windows XP client side configuration.



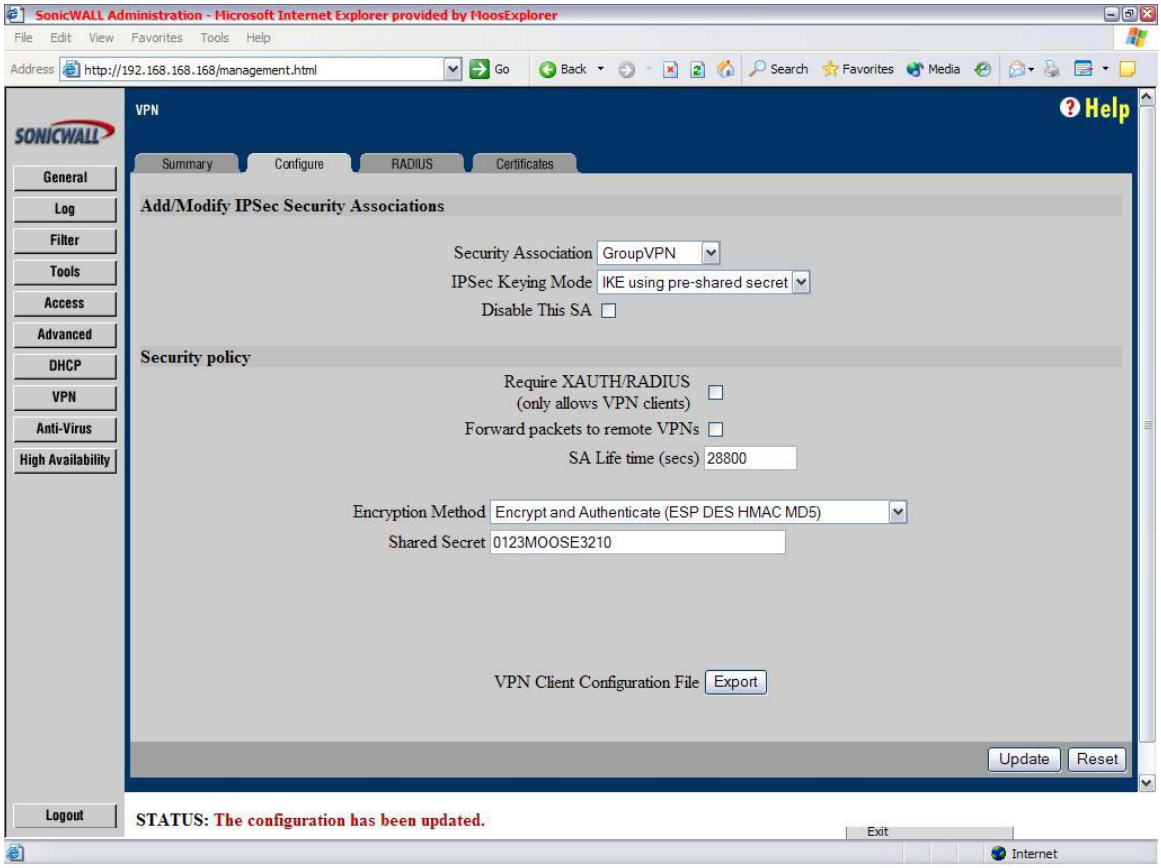


Figure 1. SonicWALL VPN Configuration Screen, GroupVPN.

Figure 1 shows the GroupVPN configuration screen. Any of the values on this page can be changed and the Windows XP client can be configured accordingly, but for the sake of this example, we will leave everything except the Shared Secret Key at its default value. The guide also assumes that the SonicWALL is fully configured and operational, and that VPN connectivity has been tested from a known-working client. The information we need from the existing SonicWALL configuration is:

- The WAN IP Address (assuming 172.16.0.254)
- The LAN Subnet (assuming 192.168.168.0/24)
- The IPSec Keying Mode (assuming default IKE Using Pre-Shared Secret)
- The Encryption Method (assuming default ESP DES HMAC MD5)

The component of Windows XP that we will use to configure our Client VPN is called ***secpol.msc***, a snap-in for the MMC, the Microsoft Management Console. You can launch ***secpol.msc*** a number of different ways, the easiest of which is to click start then select Run... and type ***secpol.msc*** and hit ***Enter***. This will launch the MMC:

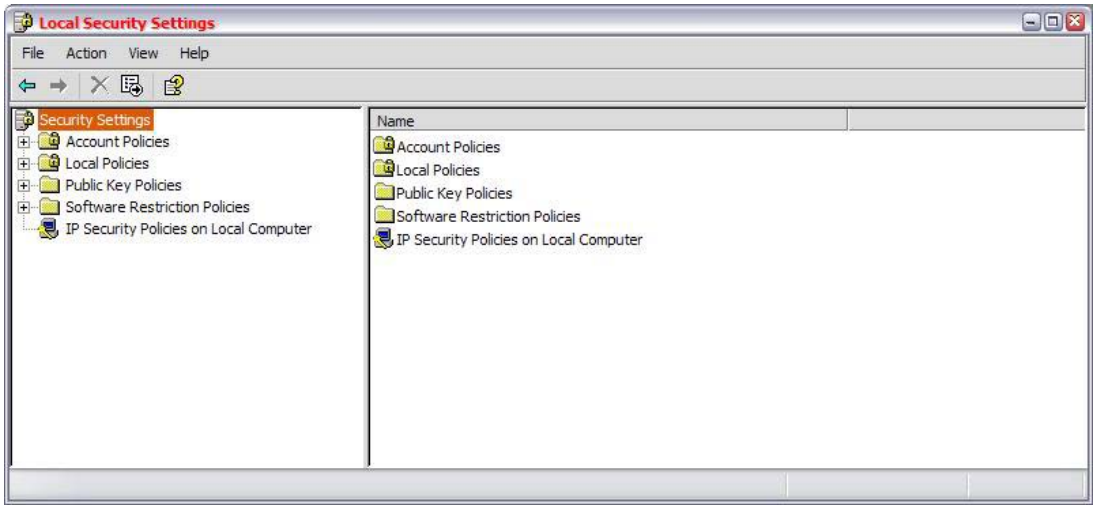


Figure 2. The Secpol.msc MMC Snap-In Main Screen.

From the default view, right click on “IP Security Policies on Local Computer” and select “Create IP Security Policy…”

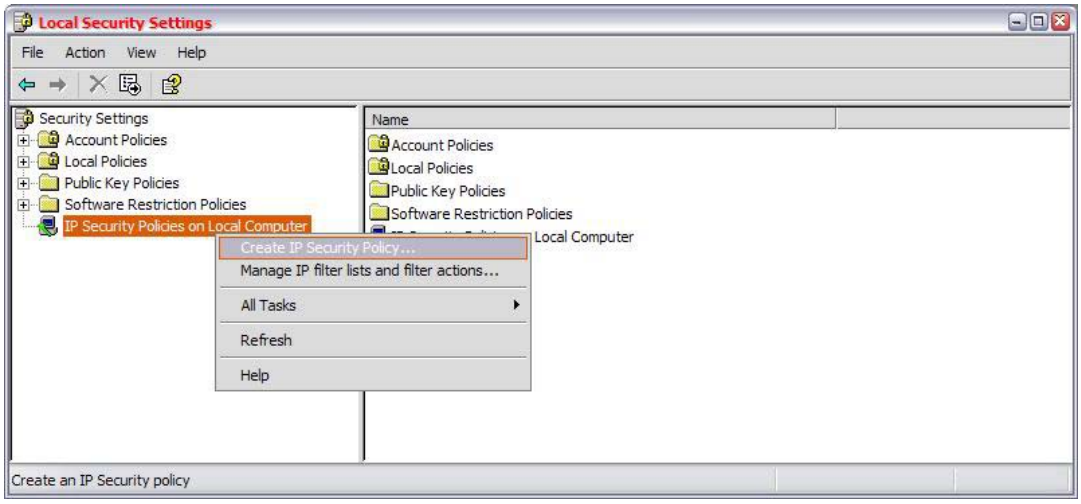


Figure 3. Creating a new IP Security Policy Step 1.

A wizard will appear. Click “Next” to bring up the following screen:

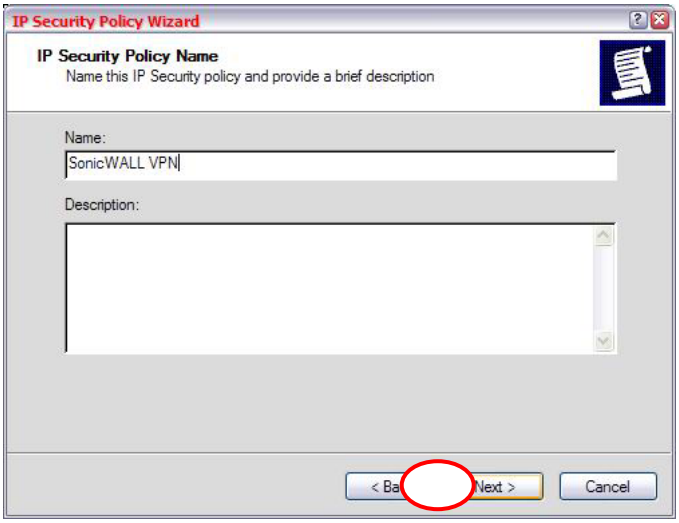


Figure 4. Naming the IP Security Policy.

Name the IP Security Policy "SonicWALL VPN" (or whatever you wish) and optionally enter a description. Click "Next". The next screen that appears will ask if you want to enable the "Default Response Rule." DESELECT this box, we do not wish to leave this rule enabled:

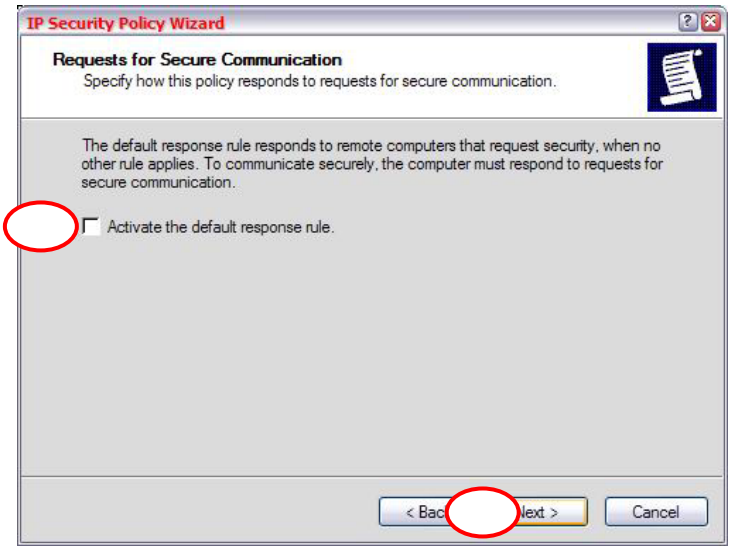


Figure 5. Deselecting the Default Response Rule.

After clearing the "Default Response Rule", click "Next". Leave the "Edit Properties" checkbox selected, and click "Finish".

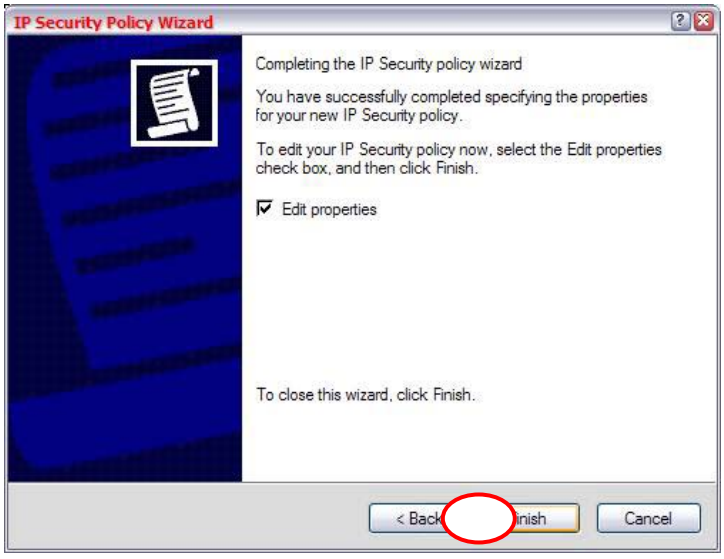


Figure 6. Completing the Policy Wizard.

The Properties page will appear and will include a default rule. We will leave this rule deselected, and will add two rules of our own: one for traffic from our client to the SonicWALL ("SNWL Filter"), and one for return traffic ("SNWL Filter Return"):

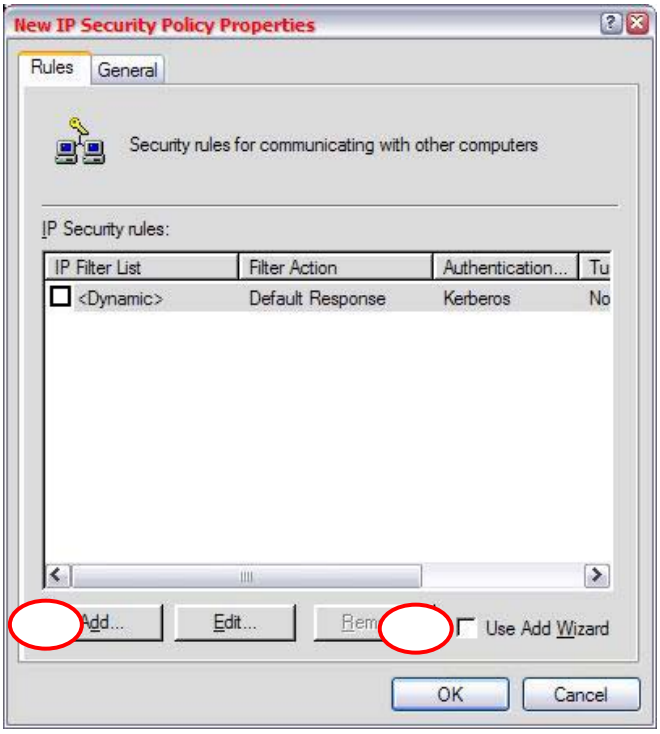


Figure 7. Adding Rules to the IP Security Policy.

Deselect the "Use Add Wizard" and click "Add" to add the first of our two Rules and Filters:

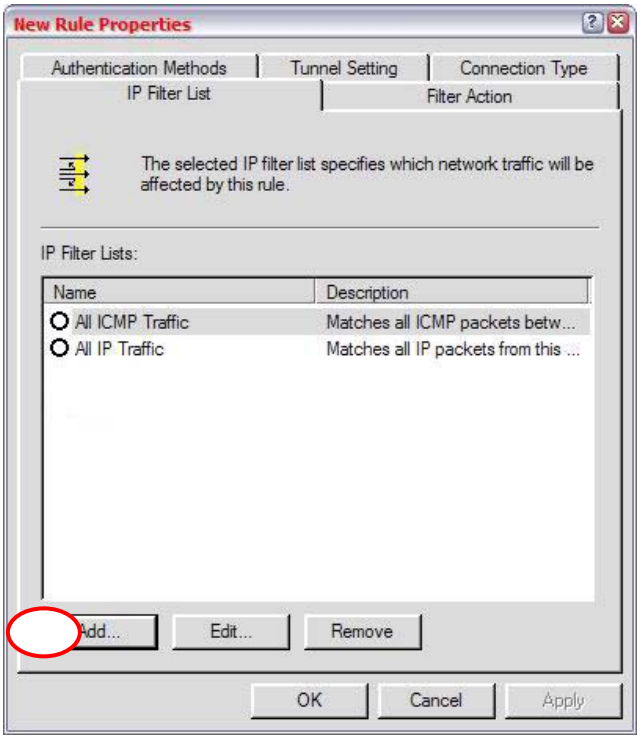


Figure 8. Default Rule/Filter List Page.

Click “Add”. We will define the outbound traffic Filter. Name the filter (“SNWL Filter”) and enter an optional description. Clear the “Use Add Wizard” button and click “Add”:

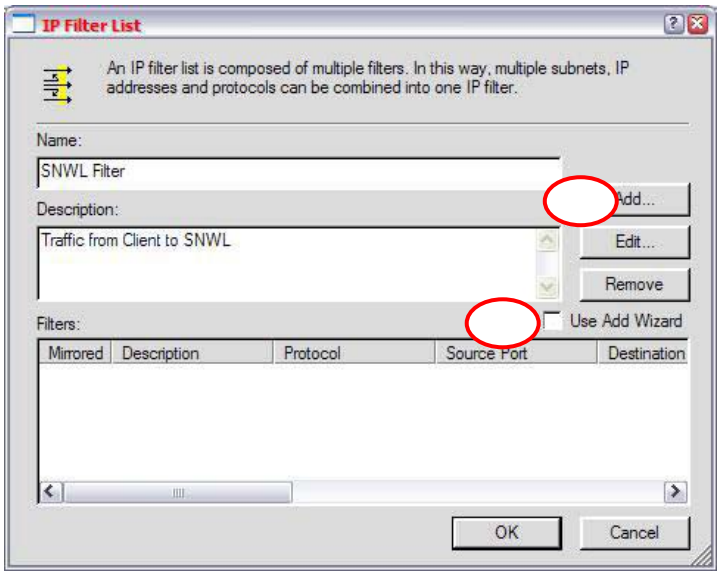


Figure 9. Adding the first Filter.

The “Filter Properties” page will appear (Figure 10). Deselect the “Mirrored” box. Enter the Source and Destination addresses for this Filter. For the source address we will select “Any IP Address”. This will allow for tunnel initiation from any network interface on your machine. (Note: If you only wish to allow initiation from a particular address, select “A Specific IP Address” and enter the address of the interface

you wish to allow.) The destination address will be the LAN segment of the remote/corporate network behind the SonicWALL (192.168.168.0 255.255.255.0):

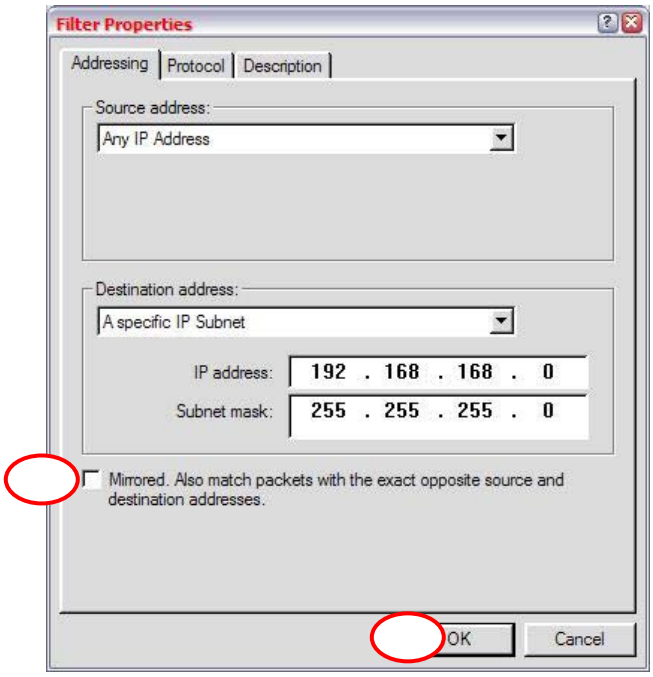


Figure 10. Adding Source and Destination Addresses to "SNWL Filter".

Click "OK" and select the "SNWL Filter" button. Select the "Filter Action" tab:

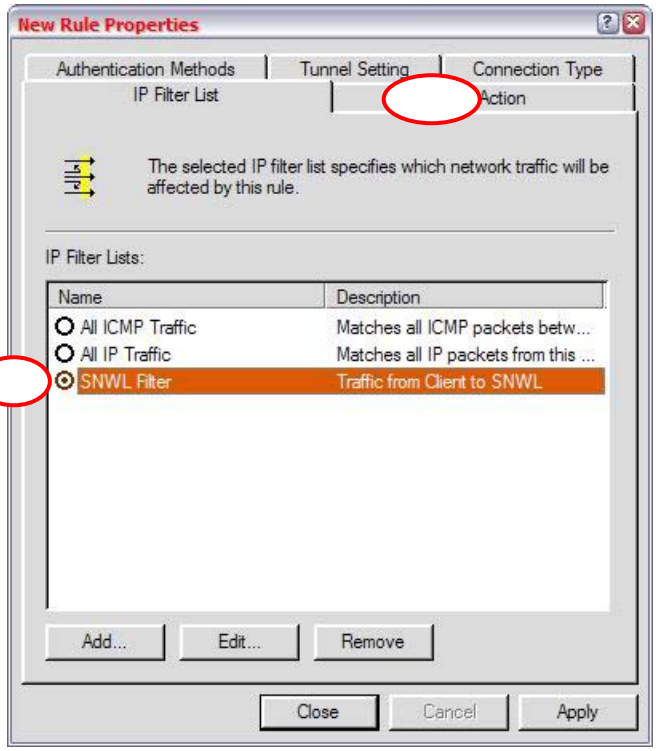


Figure 11. Selecting the Filter to Configure.

This will bring up the “Filter Action” screen with the three default actions. Leave these deselected. We will create a new action by clearing the “Use Add Wizard” and clicking the “Add” button, as illustrated in figure 12:

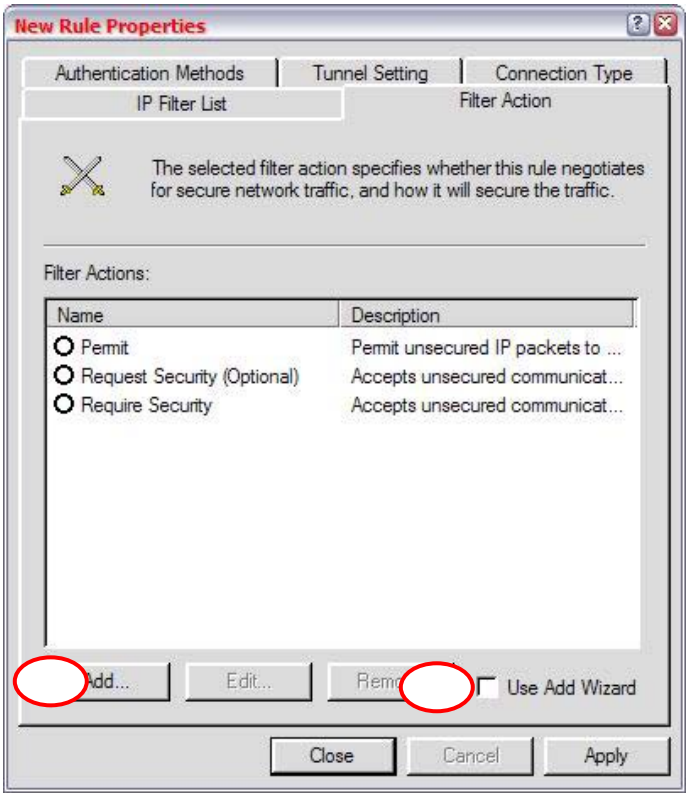


Figure 12. Adding a Filter Action for “SNWL Filter”.

On the Filter Action Properties screen (figure 13) clear the “…unsecured communication…” boxes toward the bottom, select “Negotiate Security” at the top, and click “Add”:

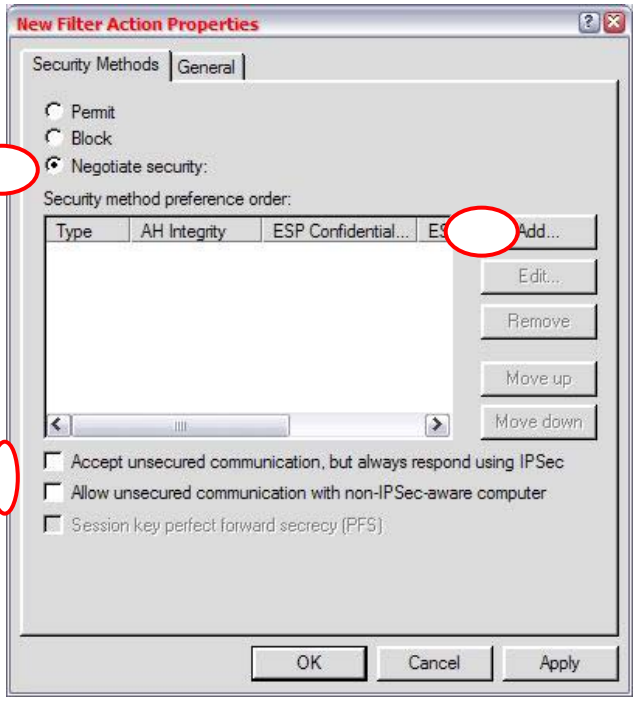


Figure 13. Defining Filter Action Properties

Under “Security Method” select “Custom” and then “Settings” (figure 14):

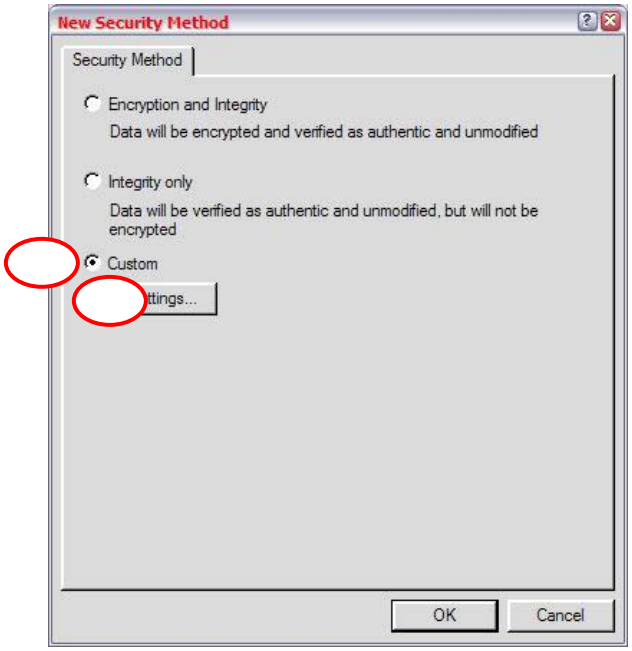


Figure 14. Selecting Custom Security Method.

We will now select a security method to match the configuration of our SonicWALL GroupVPN (ESP DES HMAC MD5). You can leave the Session Key settings at default (never timeout) or change them as you wish:

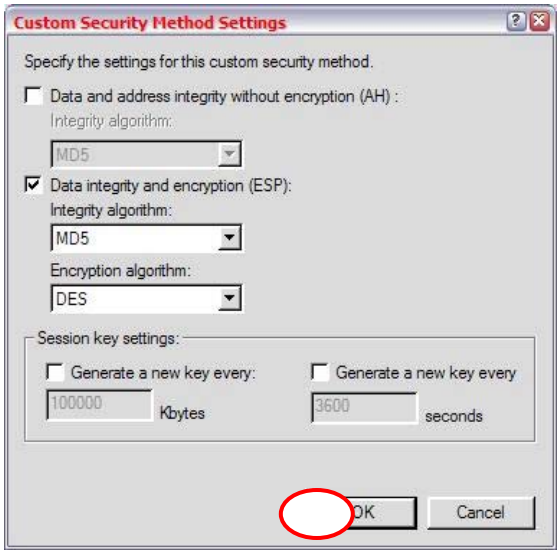


Figure 15. Defining a Custom Security Method.

Click “OK” a few times to return to the “New Rule Properties” screen. Select the filter action (“SNWL Filter”) you just created:

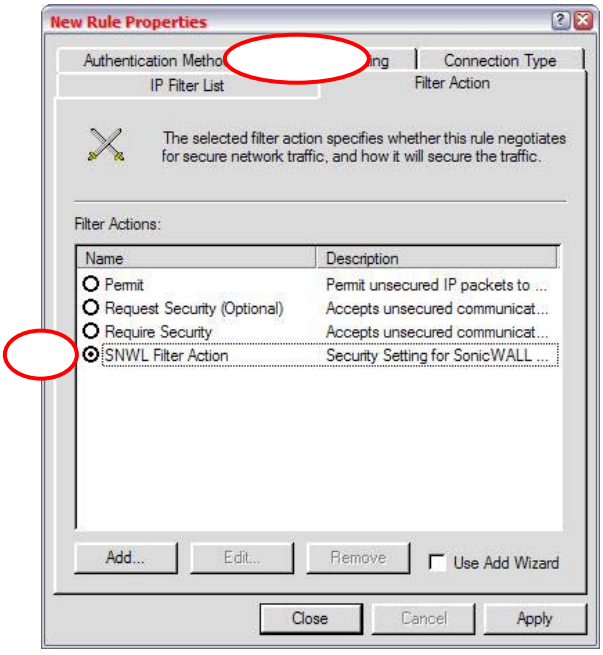


Figure 16. Selecting the Defined Filter Action.

Select the “Tunnel Settings” tab, and specify the WAN address of your SonicWALL:

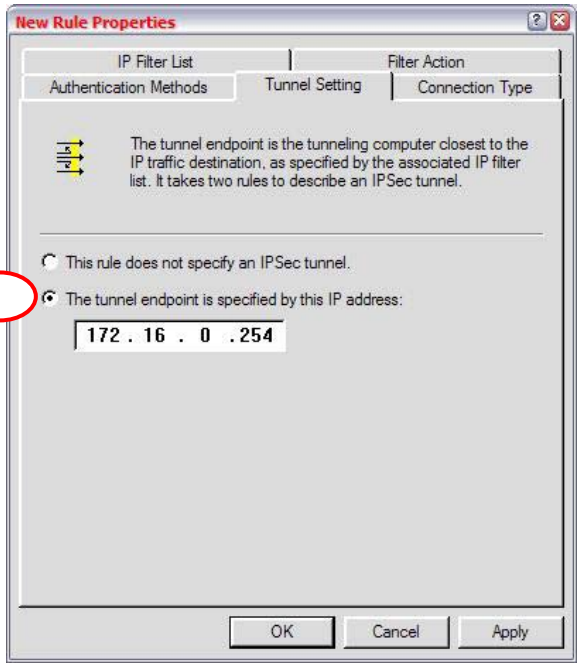


Figure 17. Set the Client to SonicWALL tunnel endpoint.

Select the “Authentication Methods” tab, highlight the default “Kerberos” method, and click edit, as illustrated in figure 18:

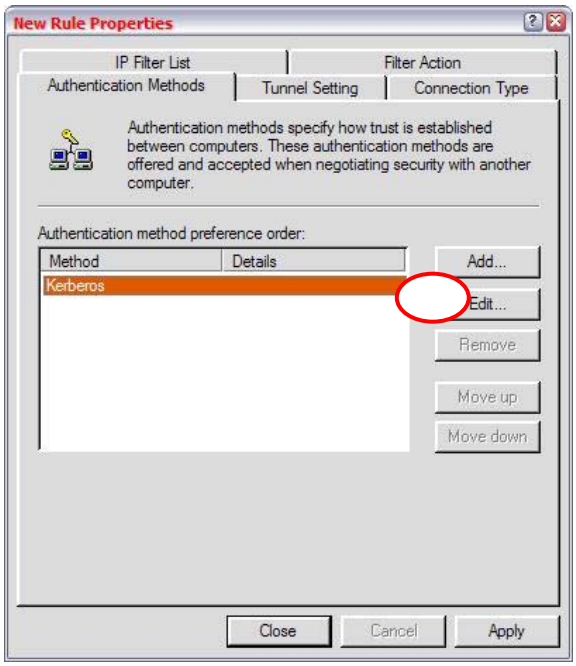


Figure 18. Editing the Authentication Method.

Selecting “Edit” will allow us to specify our shared-secret key (0123MOOSE3210) that we retrieved from the SonicWALL GroupVPN configuration:

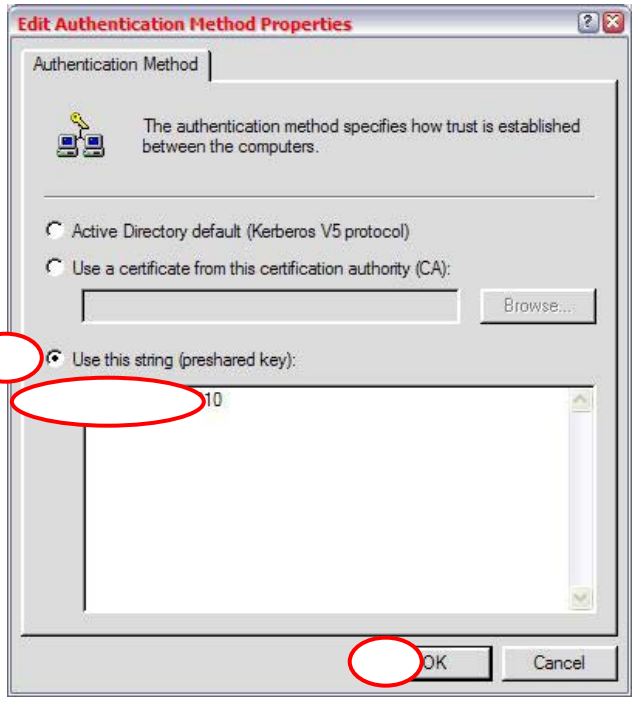


Figure 19. Entering the Preshared Secret Key.

Clicking “OK” will take you back to the “New Rules Property” page. We are now done with the first half of the configuration. The second half is considerably quicker, since most of our components are already defined. We will now build the Rule and Filters for traffic from the SonicWALL back to our Client.

Select the “IP Filter List” tab again, and click “Add”, as illustrated in figure 20:

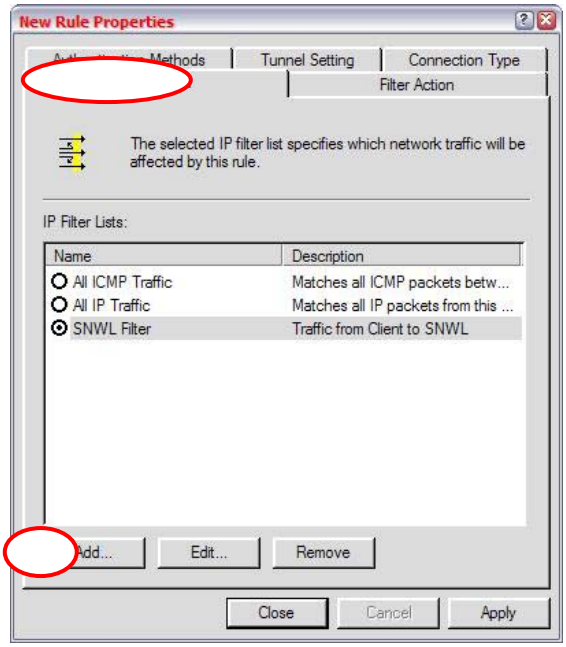


Figure 20. Adding a filter for return traffic.

This will bring up the now familiar “IP Filter List” screen. Name the filter list (“SNWL Filter Return”), enter an optional description, deselect “Use Add Wizard” and click “Add”. This will bring up the Filter Properties screen:

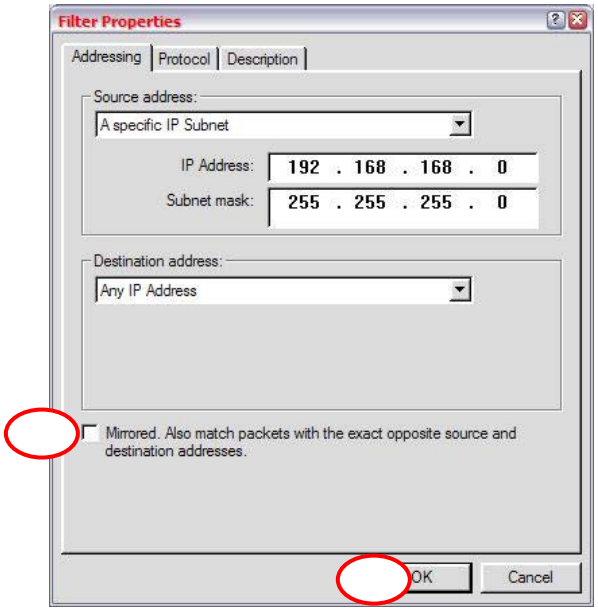


Figure 21. Setting the Return Filter properties

Just as we did before, we will define the properties of this IP Security filter, only this time, we will reverse the flow. The Source Address will become the remote/corporate subnet (192.168.168.0 255.255.255.0), and the Destination Address will be “Any Address” (or whatever option you wish to select, as described earlier). Be sure to again clear the “Mirrored” box, and click “OK” twice. You will return to the “IP Filter List” screen, and it should now look as follows:

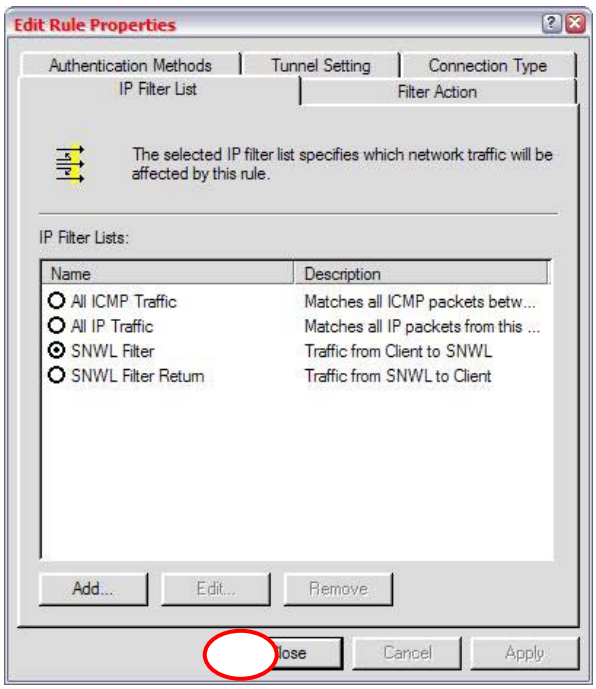


Figure 22. The IP Filter List with both filters defined.

Click “Close” to return to the “SonicWALL VPN Properties - Rules” page. It should look as follows:

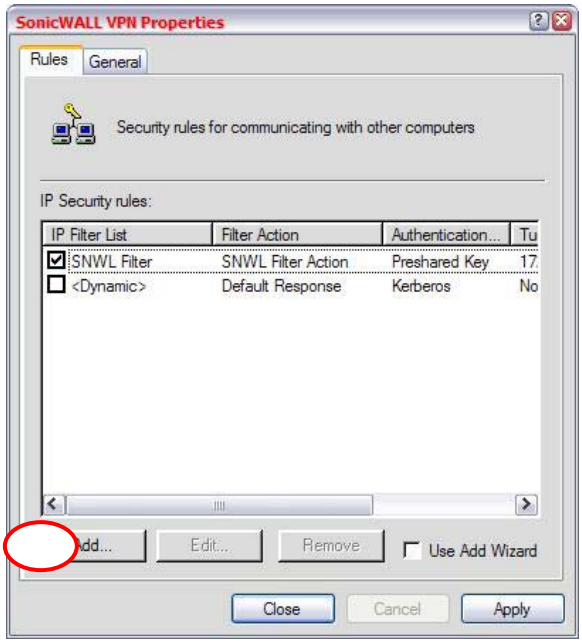


Figure 23. The “SonicWALL VPN Properties” Rules page.

Click “Add” and we will define the rule for return traffic. Figure 24 depicts the “New Rule Properties” view:

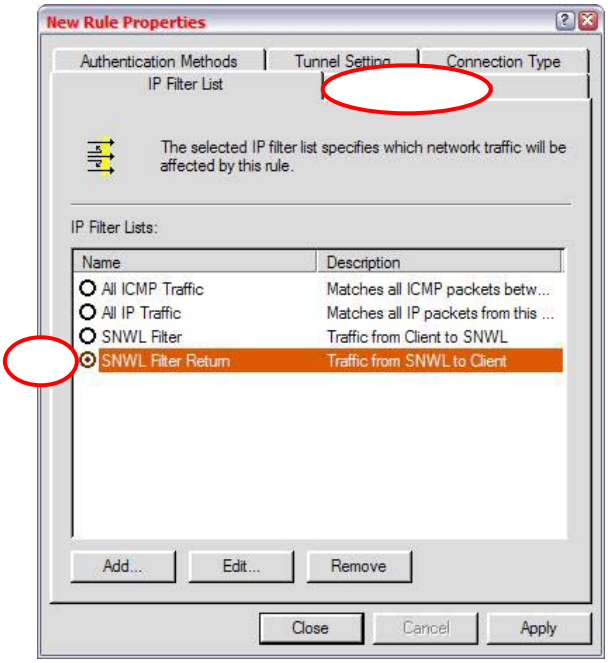


Figure 24. New Rule Properties.

Select the “SNWL Filter Return” button. Click on the “Filter Action” tab, and select the previously defined “SNWL Filter Action”:

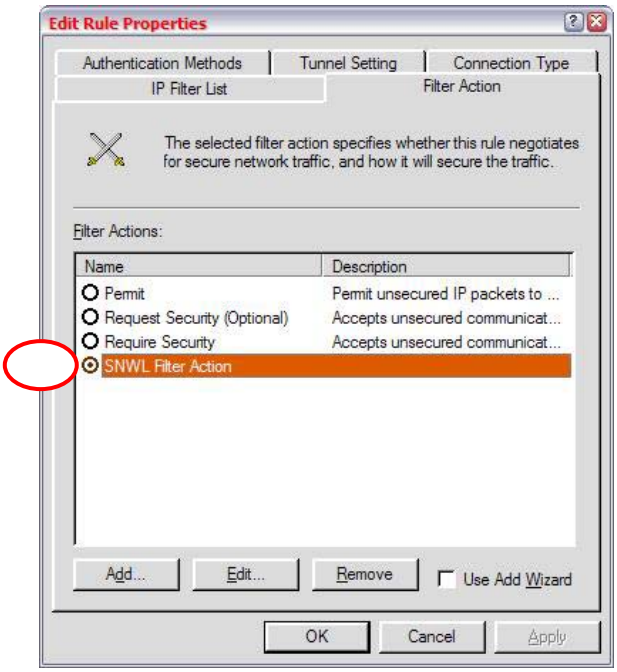


Figure 25. Selecting the "SNWL Filter Action".

Next, select the "Tunnel Setting" tab, and enter the Client's IP address (assume 64.65.66.67). This is the only parameter that must be unique to the client's configuration:

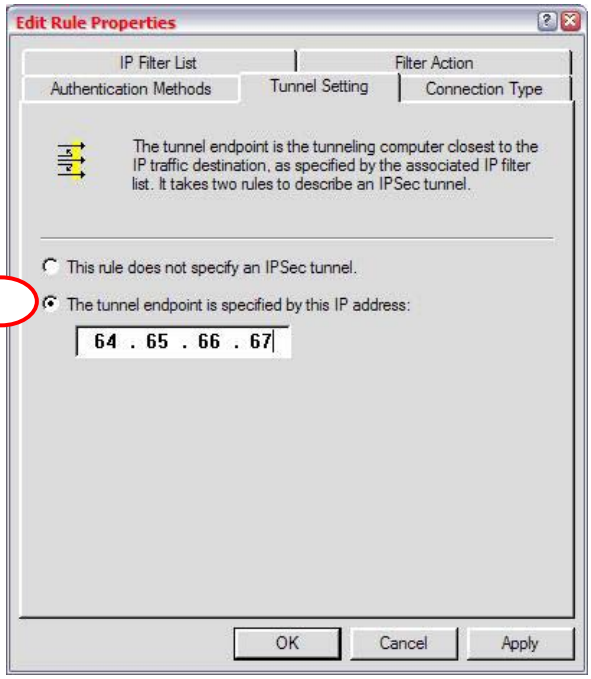


Figure 26. Setting the return tunnel endpoint.

Select the "Authentication Methods" tab, once again, highlight the default "Kerberos" method, and click edit, as illustrated in figure 27:

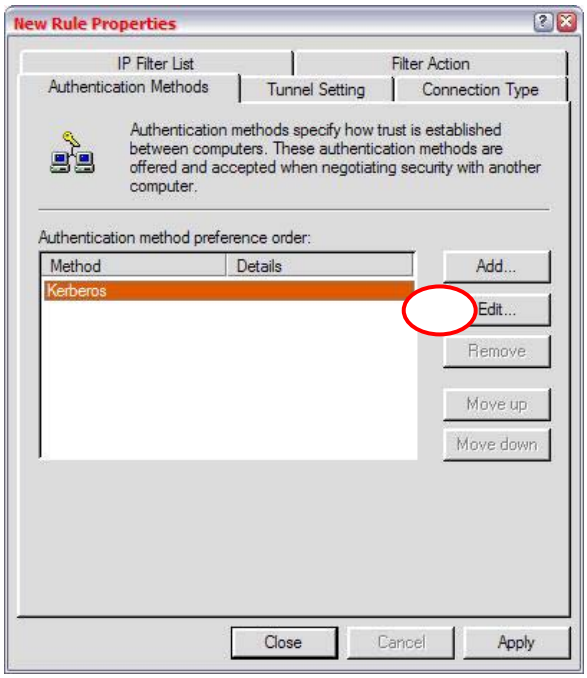


Figure 27. Editing the Authentication Method.

Selecting “Edit” will allow us to specify our shared-secret key (0123MOOSE3210) that we retrieved from the SonicWALL GroupVPN configuration:

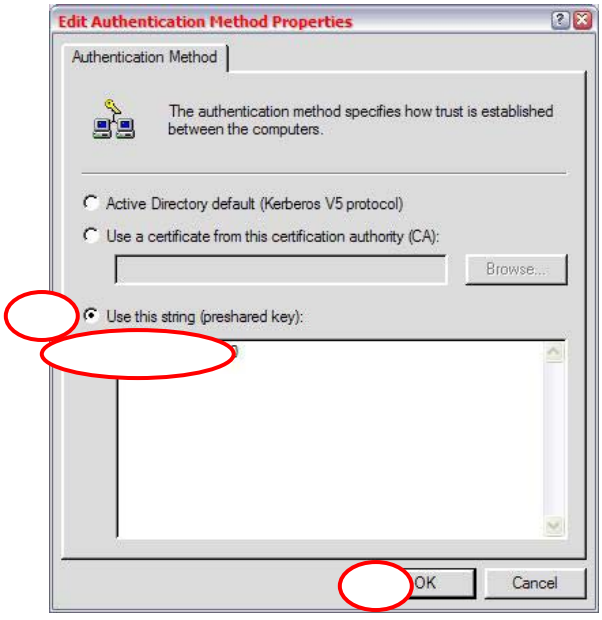


Figure 28. Entering the Preshared Secret Key.

Clicking “OK” will return you to the “SonicWALL VPN Properties” page. It should now look as follows:

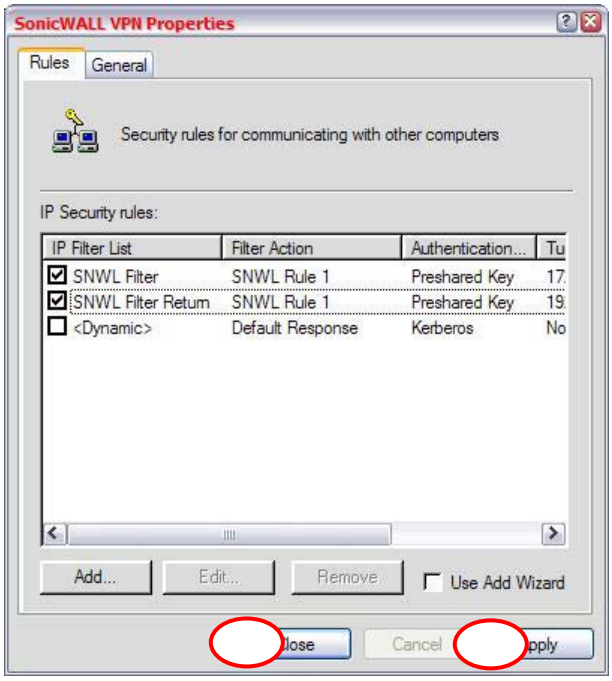


Figure 29. The completed Rules page.

Click “Apply” and “Close” to return to the “Local Security Settings” master page:

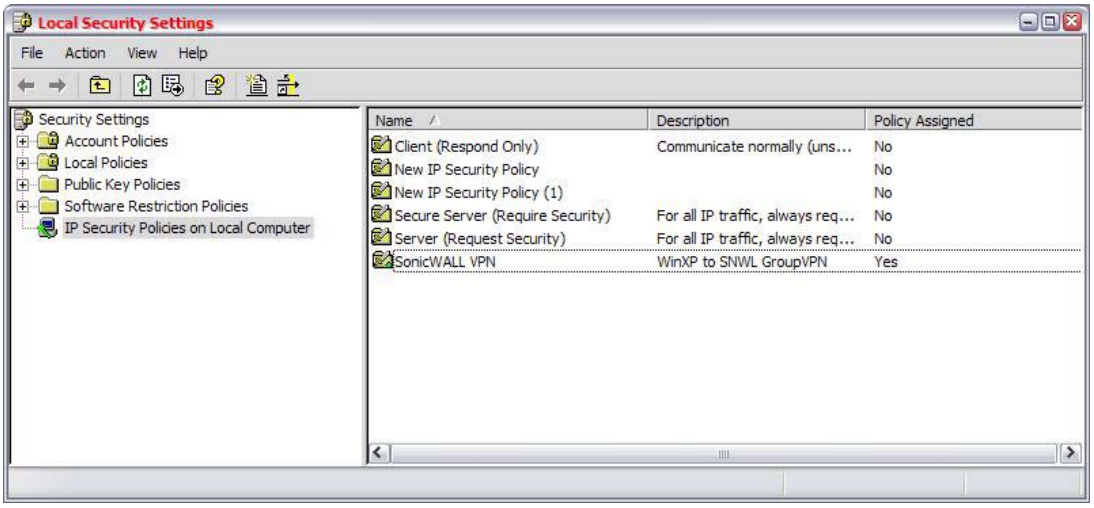


Figure 30. Completed Local Security Settings page.

Right Click on the “SonicWALL VPN” Security Policy, and select “Assign”. The policy is now active, and you should be able to bring up the VPN by initiating traffic to the 192.168.168.0 network; a ping should do. The first packet or few packets will initiate the VPN connection, and will display “Negotiating IP Security.” Depending on the speed of your connection, the tunnel should come up after 1 to 10 ping packets:

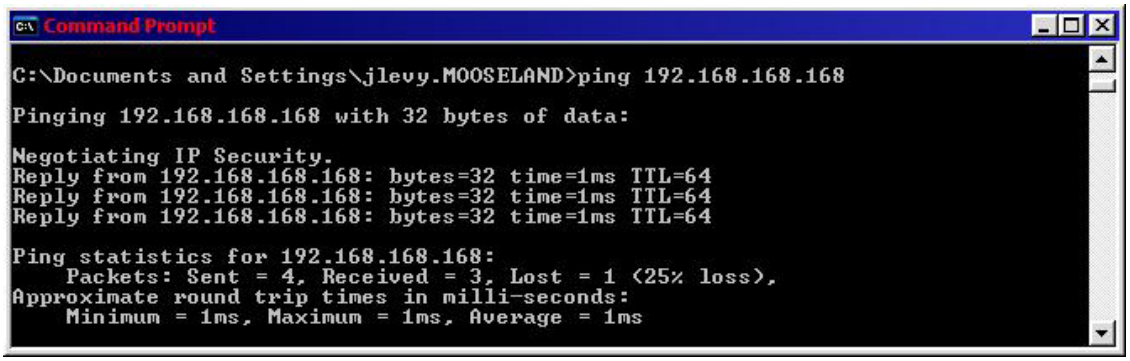


Figure 31. Negotiating the VPN with ICMP traffic.

You should now have VPN connectivity between you Windows XP client, and your SonicWALL VPN.

Supplement: Exporting and Importing the Windows XP Client VPN Settings

***NOTE**: Only use this option if there are no existing IP Security Policies defined on the export or import machines. Using this export/import method with other IP Security Policies present will yield unpredictable results. This method also assumes that Source and Destination addresses pertaining to the Client have been defined as "My IP Address" or "Any IP Address" and do not specifically define Client IP addresses.*

This section is offered to speed the deployment of Windows XP to SonicWALL VPN configurations. It allows an administrator to configure the settings described above one time on a single Windows XP client, and to export the registry values containing that configuration for easy import by clients. The information contained within the exported registry data contains all defined network information and your shared-secret key and should be considered VERY SENSITIVE information. Treat it with care.

secpol.msc has its own built in import and export facility. Using the integrated facility is no more secure than the method presented below, but it does require a bit more user intervention. With ease in mind, it has been excluded. You can use it, if you wish, but it requires that the client launch secpol.msc, import the policy, change a setting, and then activate it. The method presented below requires double clicking a .reg file and modifying a single setting.

After you have successfully configured a Windows XP client for VPN access to your SonicWALL, you can export the associated registry information with the following command:

C:\> regedit /e C:\VPN.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Micros
oft\Windows\IPSec\Policy\Local"

This will export the settings to the file VPN.reg (about 160KB) in the root of your C:\ drive. Carefully distribute this file to clients, and remind them to treat the file with similar care. They can import these settings onto their workstation by double-clicking on the VPN.reg file and selecting "Yes" at the "Are you sure you want to add…" prompt. This will import and activate the policy. Now all the client must do is change the "SNWL Filter Return: Tunnel Setting: IP Address" value.

[Start], [Run] and type ***cmd*** and hit ***Enter.*** Type ***ipconfig*** and hit ***Enter.*** This will offer a basic view of interfaces and addresses. Note the address through which you want the VPN to be established. Type ***secpol.msc*** and hit ***Enter***. This will launch the MMC. Double click the "SonicWALL VPN" Security Policy. Double click the "SNWL Filter Return" rule. Select the "Tunnel Setting" tab, and enter the correct IP address.

The client should then be able to bring the tunnel up by initiating traffic to the remote/corporate subnet.