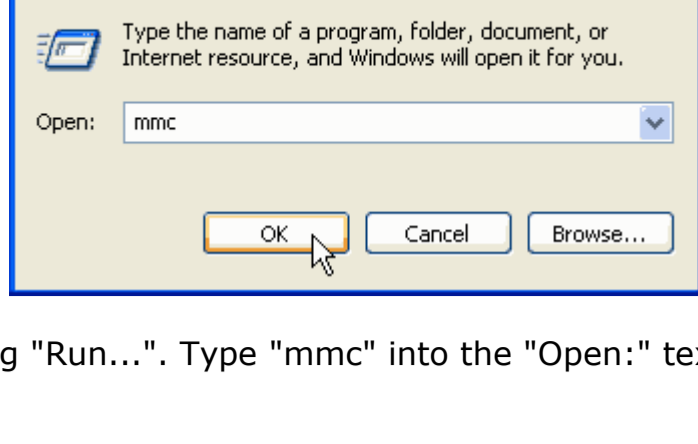


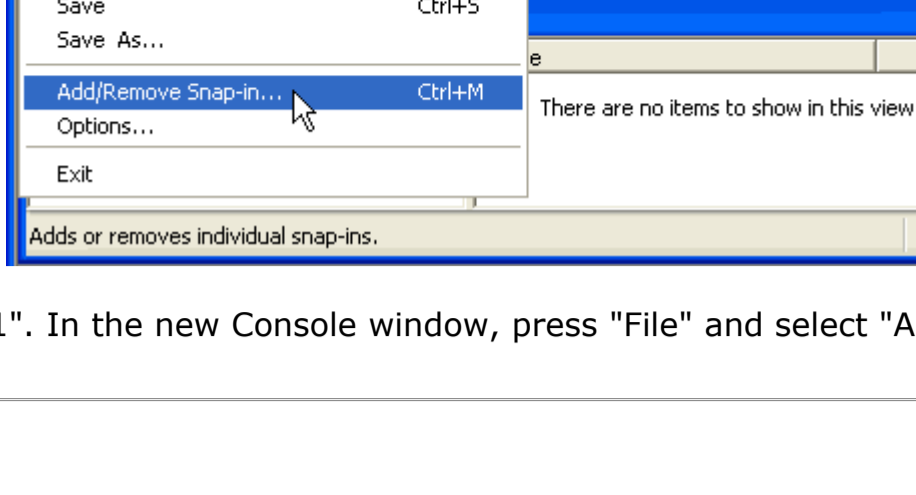
Windows XP IPsec

<http://www.treewalkdns.com/ipsec/ipsecxp.htm>

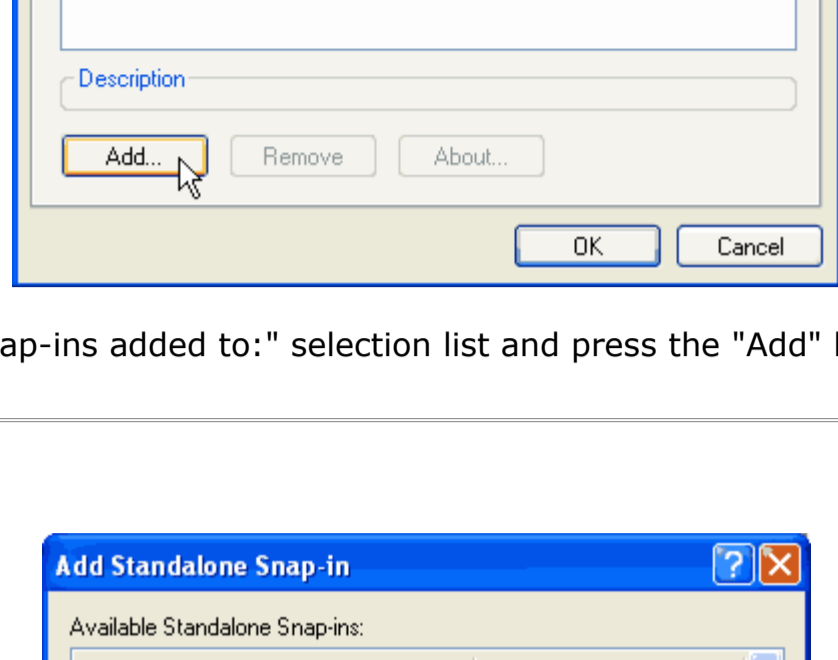
First, you'll need to download and extract the <http://www.treewalkdns.com/twtools/IpSecFilter.zip> from our site to your desktop (or any other suitable location) and rename the files if you wish. After that, just follow the steps below. (**NOTE: not all windows will be shown so in some cases you will need to use "Okay" or "Close" buttons to proceed to the next step.**)



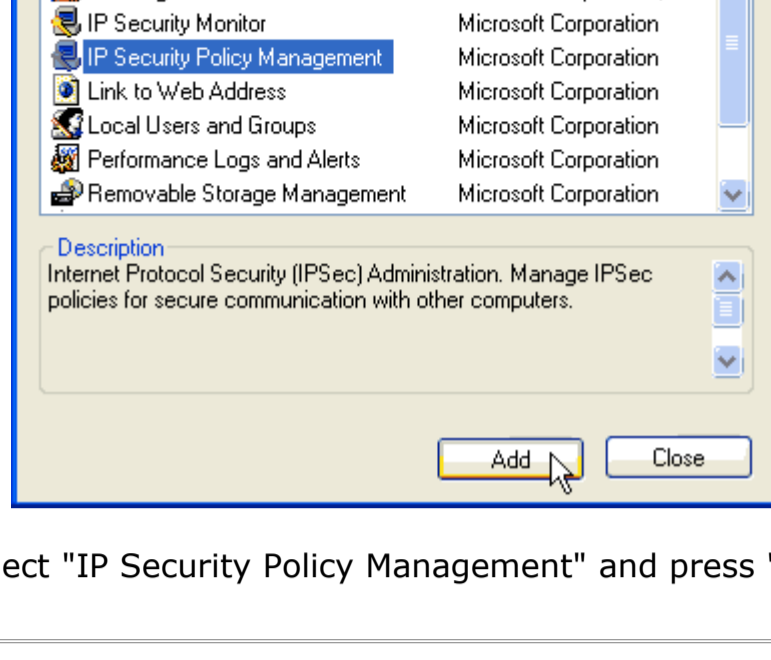
We begin by pressing the "Start" button and selecting "Run...". Type "mmc" into the "Open:" text box and press the "Okay" button to start a new Microsoft Management Console.



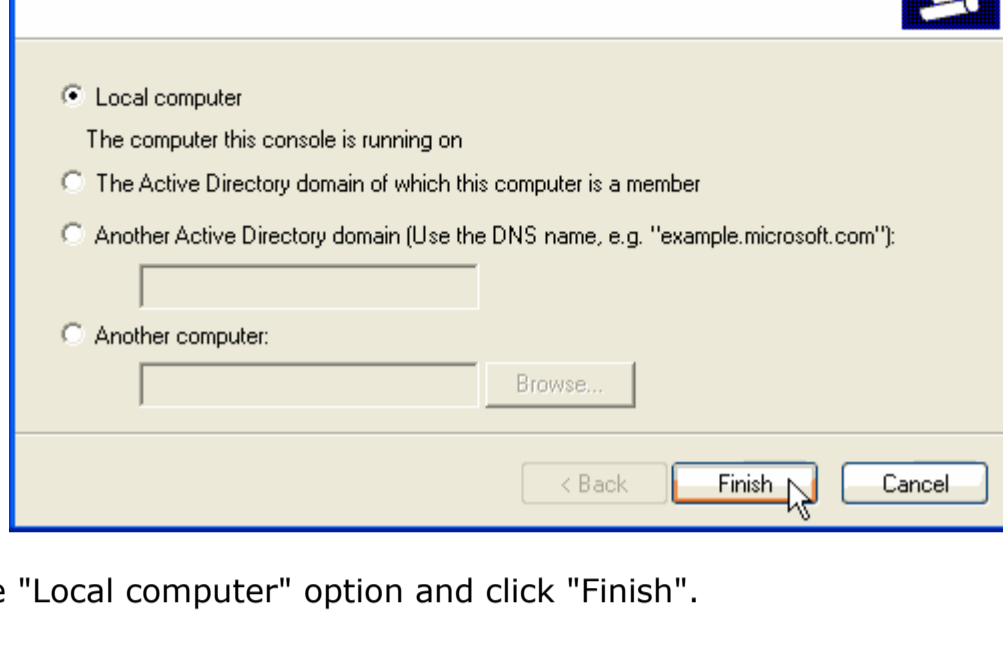
Our window in this example is titled "Console1". In the new Console window, press "File" and select "Add/Remove Snap-in...".



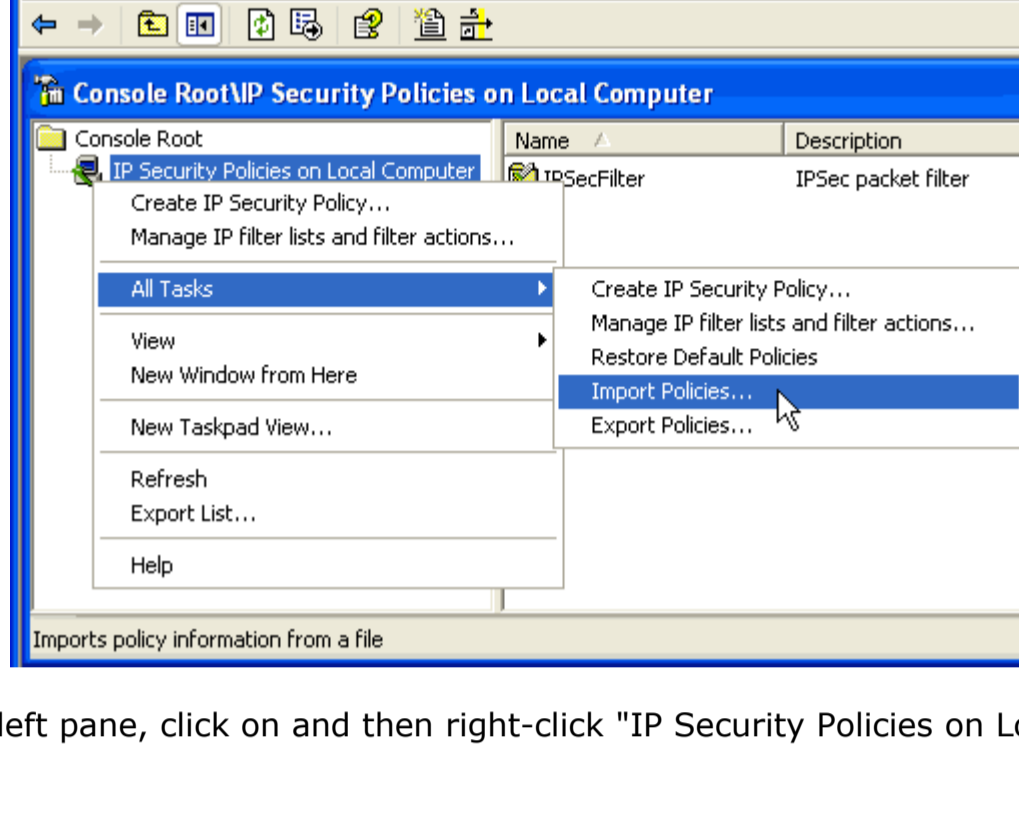
Ensure "Console Root" is displayed from the "Snap-ins added to:" selection list and press the "Add" button.



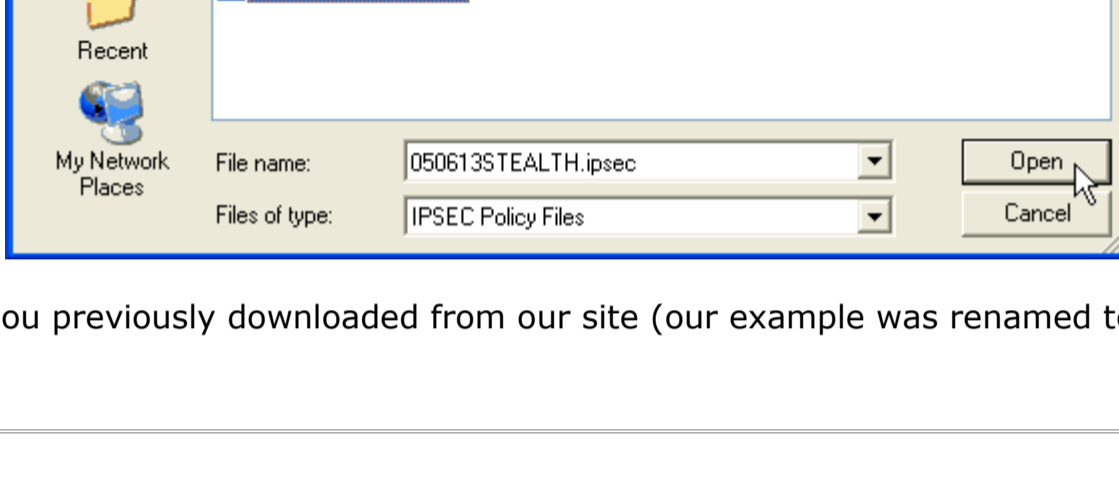
Scroll the "Add Standalone Snap-in" window to select "IP Security Policy Management" and press "Add".



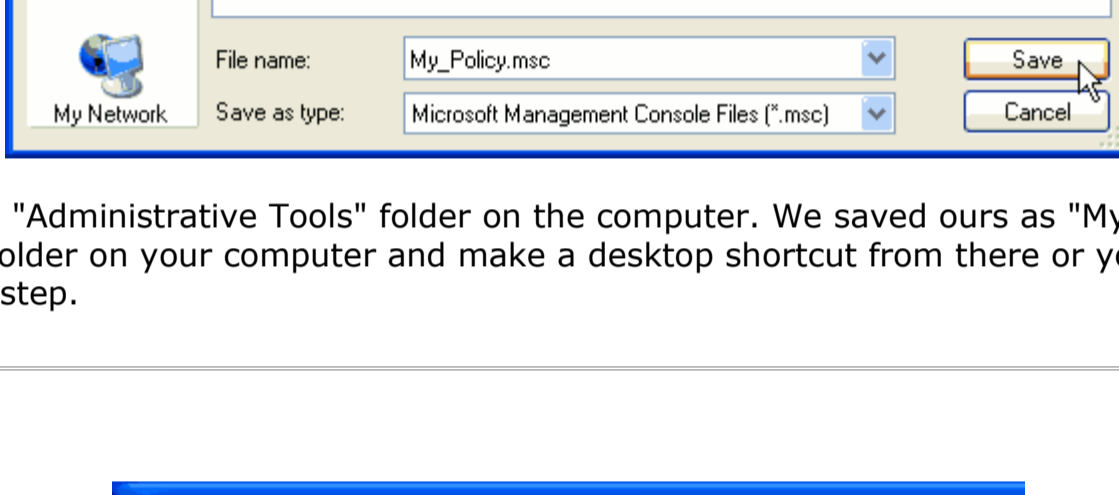
At "Select Computer or Domain", select the "Local computer" option and click "Finish".



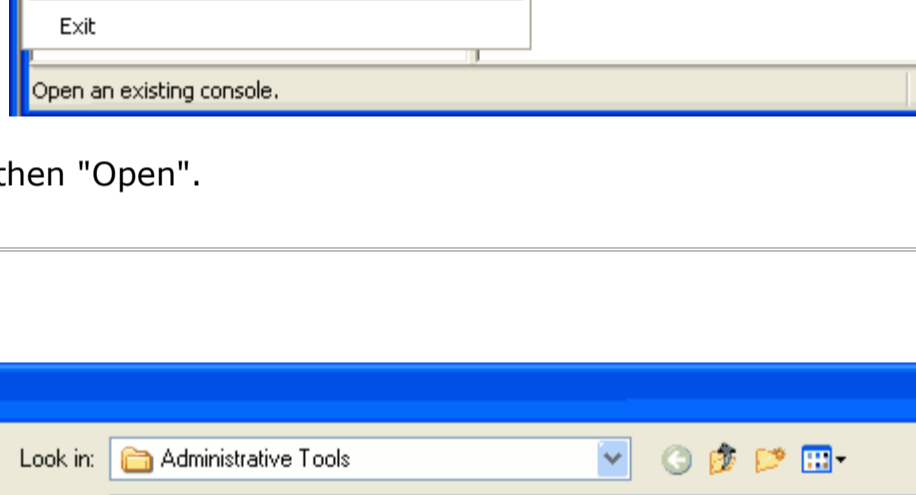
This brings us back to "Console1". On the left pane, click on and then right-click "IP Security Policies on Local computer", select "All Tasks" and select "Import Policies".



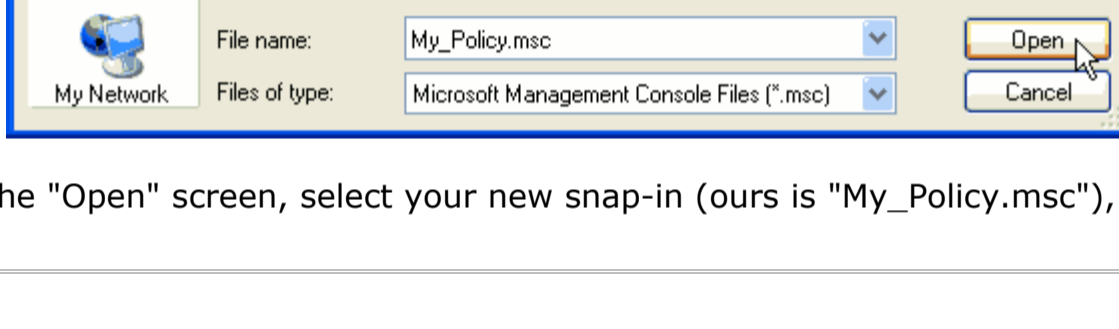
Navigate to where you saved the files you previously downloaded from our site (our example was renamed to "050613STEALTH.ipsec"). Select the file in the window and press "Open".



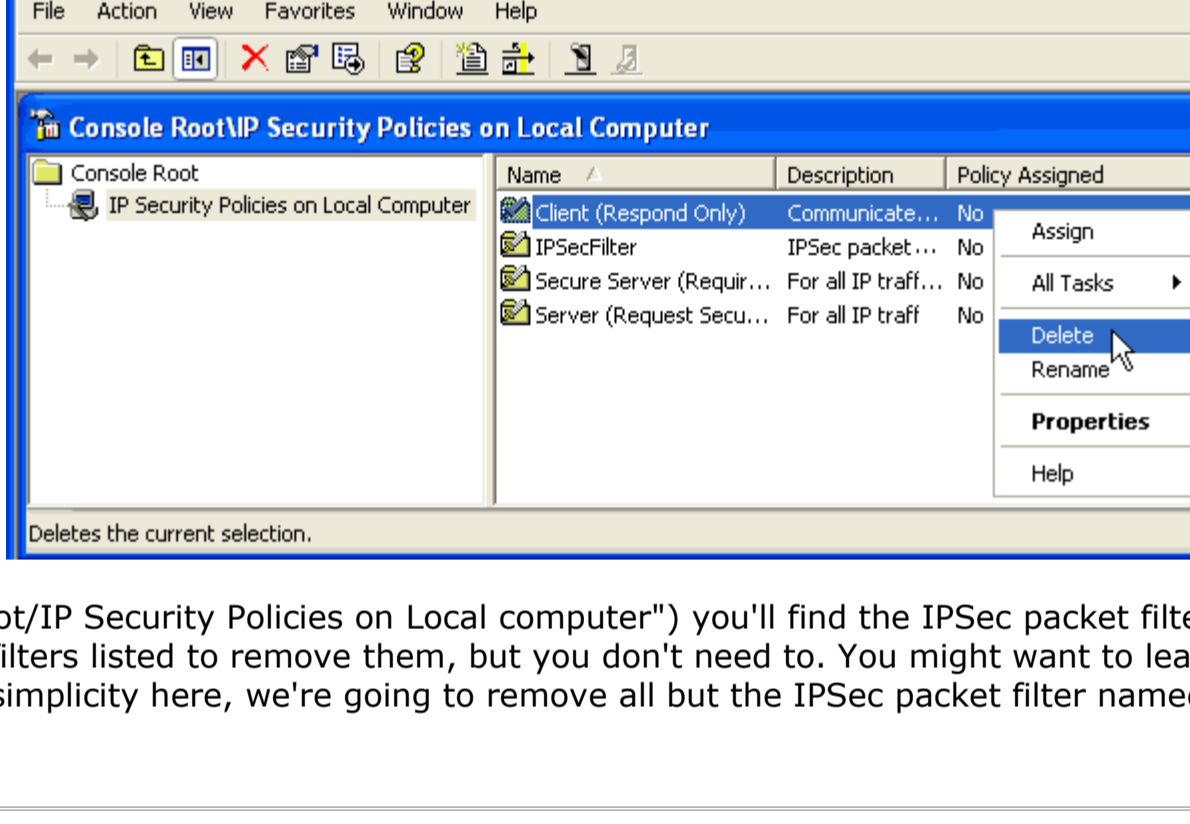
Next, we'll save the new Console to the "Administrative Tools" folder on the computer. We saved ours as "My_Policy.msc". At this point you could navigate to the "Administrative Tools" folder on your computer and make a desktop shortcut from there or you could simply type "mmc" into a Run box again, as we did to get to the next step.



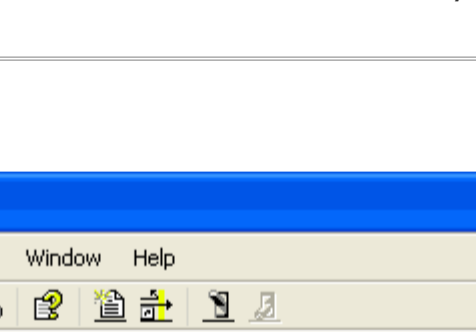
At the resulting console window select "File", then "Open".



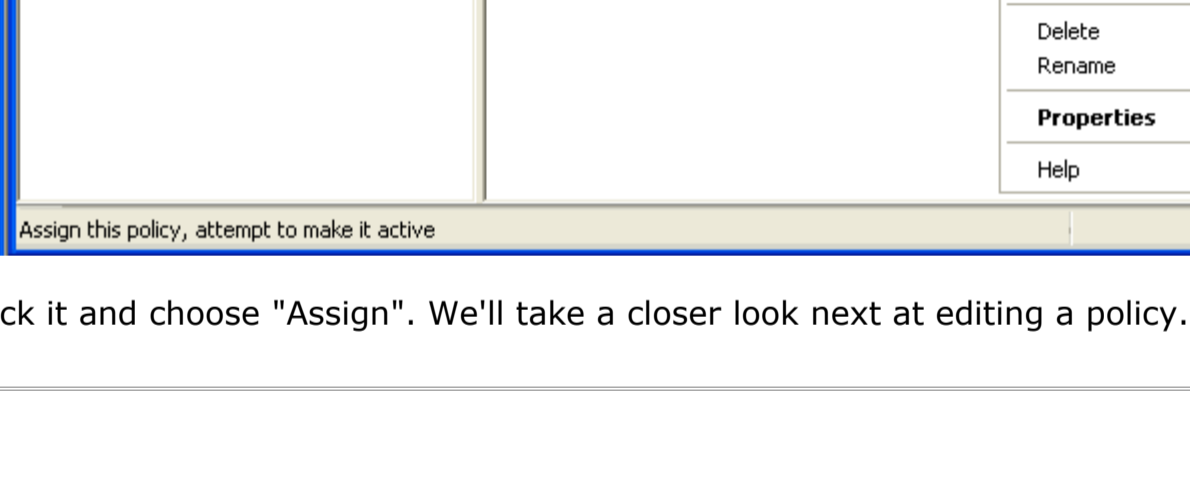
Now we'll take a look at our policy. At the "Open" screen, select your new snap-in (ours is "My_Policy.msc"), and click the "Open" button.



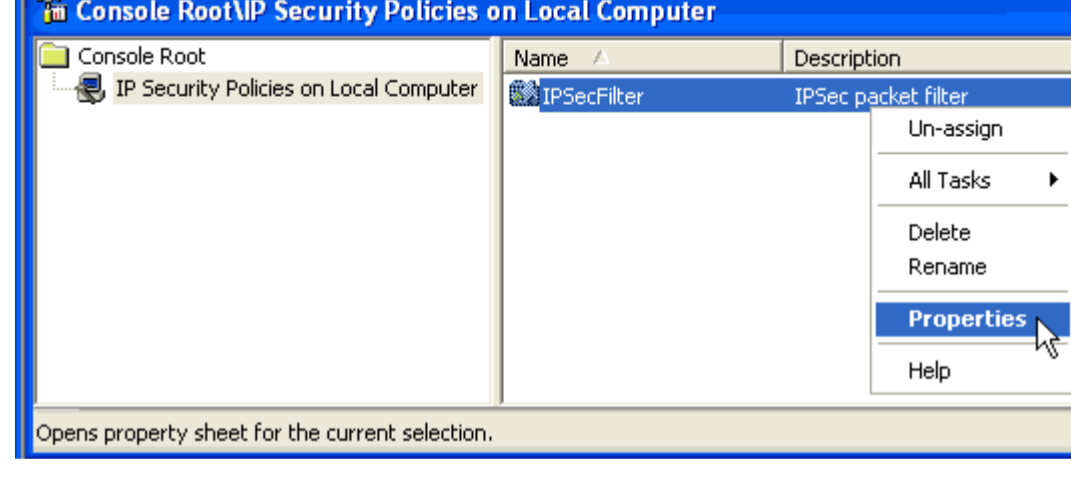
In the right pane (under "Console Root/IP Security Policies on Local computer") you'll find the IPsec packet filter we're focusing on. This is also where you can right-click any of the filters listed to remove them, but you don't need to. You might want to leave them in place and "Unassigned", for future reference. For the sake of simplicity here, we're going to remove all but the IPsec packet filter named "IPSecFilter" to demonstrate how to use this on a personal computer.



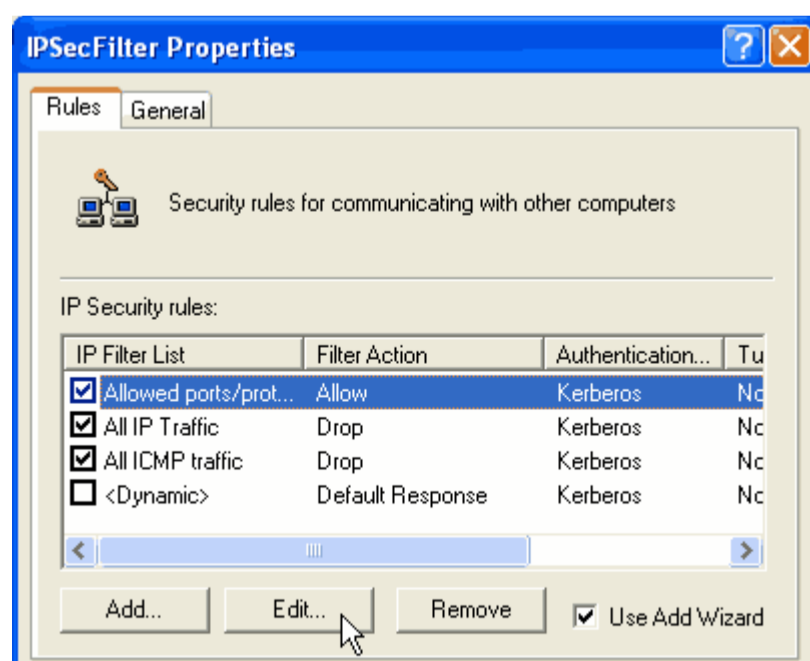
Each time you delete filters you'll be asked "Are you sure", so click "Yes" if that's what you want to do.



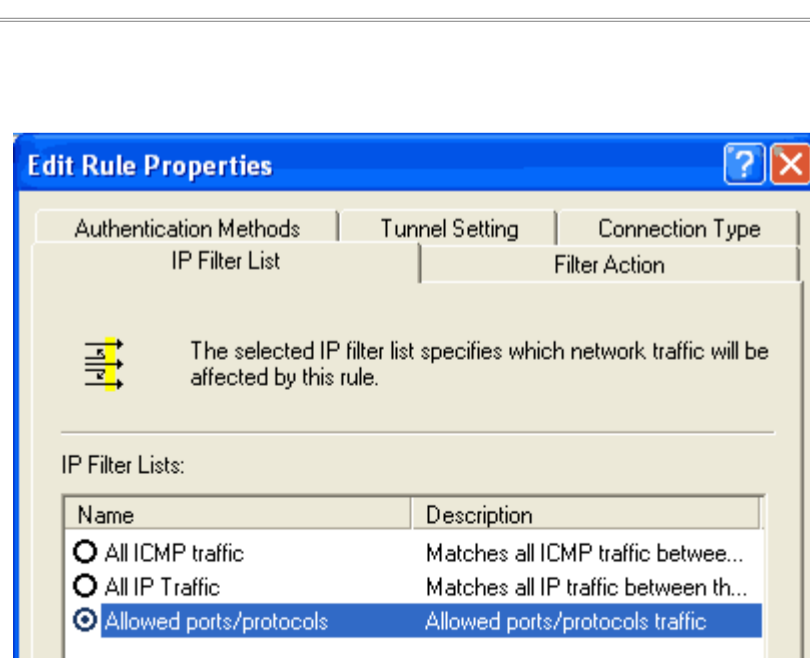
To activate a particular filter, right-click it and choose "Assign". We'll take a closer look next at editing a policy.



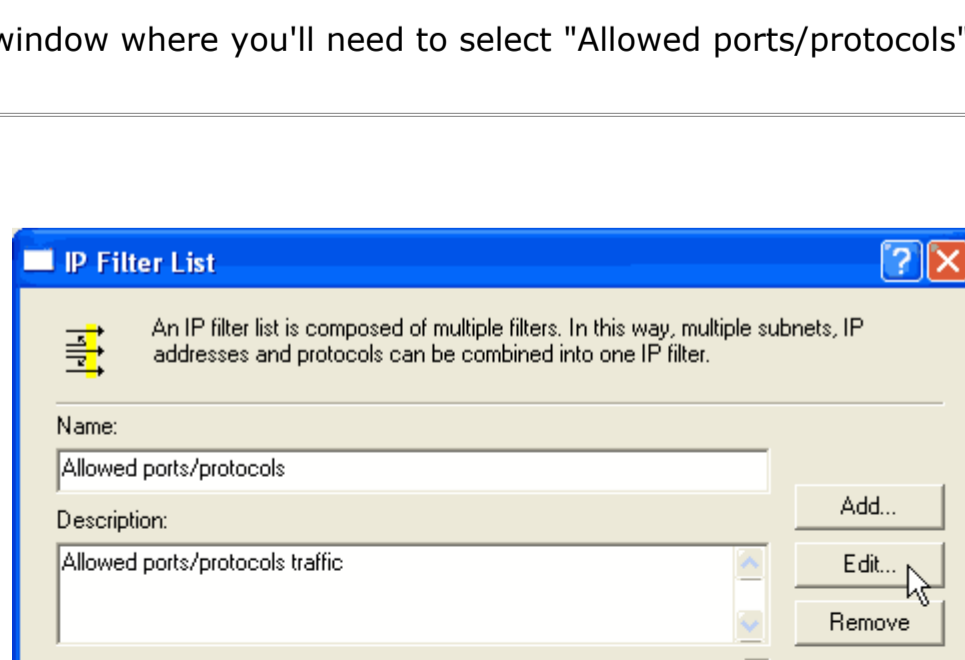
To edit or review the properties of a particular filter for an IPsec policy, right-click it in the right pane and choose "Properties".



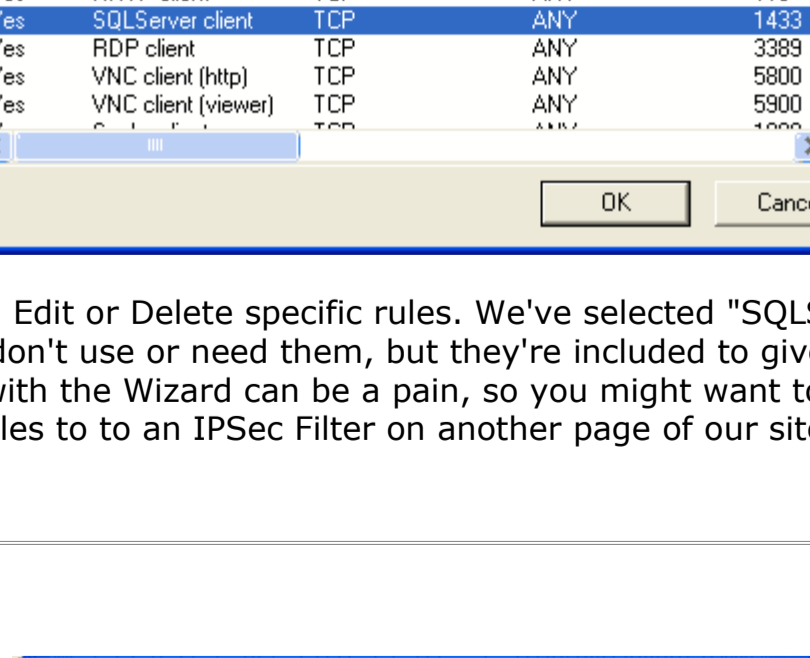
For our policy, you don't want to change any rules in the filter list except for the "Allowed ports/protocols" filter. Select it and choose "Edit".



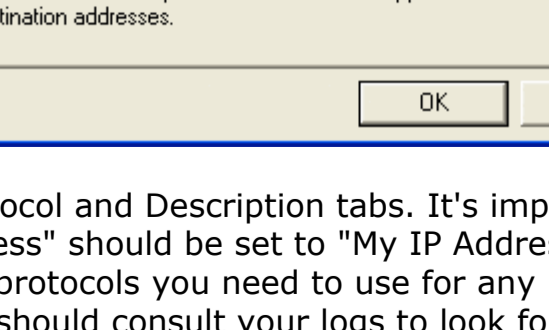
This brings us to the "Edit Rule Properties" window where you'll need to select "Allowed ports/protocols" again and choose "Edit" again.



The "IP Filter List" window is where you can Add, Edit or Delete specific rules. We've selected "SQLServer client" in our example and chose "Edit" again. You can remove certain rules here if you don't use or need them, but they're included to give you a pre-defined rule-set that should work in most (if not all) cases. (Note that adding filters with the Wizard can be a pain, so you might want to uncheck "Use Add Wizard" if you want to add a new filter and rules.) We look closer at adding rules to an IPsec Filter on another page of our site entitled "How To Create IPsec Rules" at <http://treewalkdns.com/ipsec/ipsecrule.htm>.



"Filter Properties" presents you with the Addressing, Protocol and Description tabs. It's important to note that for these filters the "Addressing" sheet should display a checkmark for "Mirrored". The "Source Address" should be set to "My IP Address" and the "Destination Address" should be "Any IP Address". The Protocol tab is where to set the ports and protocols you need to use for any rule and the "Description" tab is used to identify the filter. If you create a new filter and you find it doesn't work, you should consult your logs to look for any changes you might need to make. You can also review some of the other rules for more indications of how to properly set a filter.



If you do make any changes, you'll be prompted at the end to save them. Select "Yes"!

That's all there is to it! Happy surfing!