

IPSEC for Windows – Packet Filtering

David Taylor
SR Information Security Specialist
University of Pennsylvania
ltr@isc.upenn.edu
215-898-1236
(Revision Date: 14 October 2005)

NOTE

This document is going to be revised to remove the wizard function making it a little easier to read and implement. Also, REMOVE the ‘mirror’ settings for the ports you block. I will fix this in the near future.

Use at your own risk. This document is a guide to help you become familiar with IPSEC and how to setup basic filters to block traffic. You are responsible for proper testing of implementations in your own networks. Improper setup and lack of testing could cause disruptions in network communications.

Overview

IPSEC can be used to filter packets in a variety of scenarios. Successful implementation of IPSEC policies can significantly minimize the risk of unauthorized access to computers. The granularity of IPSEC filters makes it a desirable method of controlling access in lieu or in addition to built in firewalls. This would greatly enhance security of Windows 2000 machines that currently don’t come with a built-in firewall. Using IPSEC should be considered as an “added layer” of security. This could buy valuable time in the event a serious 0-Day exploit/worm is released. It will also buy a lot of quality “sleep time” at night for LSPs who suddenly find out they have less to worry about.

Logistics

IPSEC can be implemented via Active Directory Group Policies, Local Security Policies as well as command line tools such as IPSECPOL.EXE (Windows 2000) and IPSECCMD.EXE (Windows XP). Here we will focus mainly on the GUI interface. Since I don’t have direct access to a Domain Controller I will be using the Local Security Policy. This should look pretty much the same if you are using Group Policies from a Windows 2000+ Domain Controller.

Local Security Policy Editor

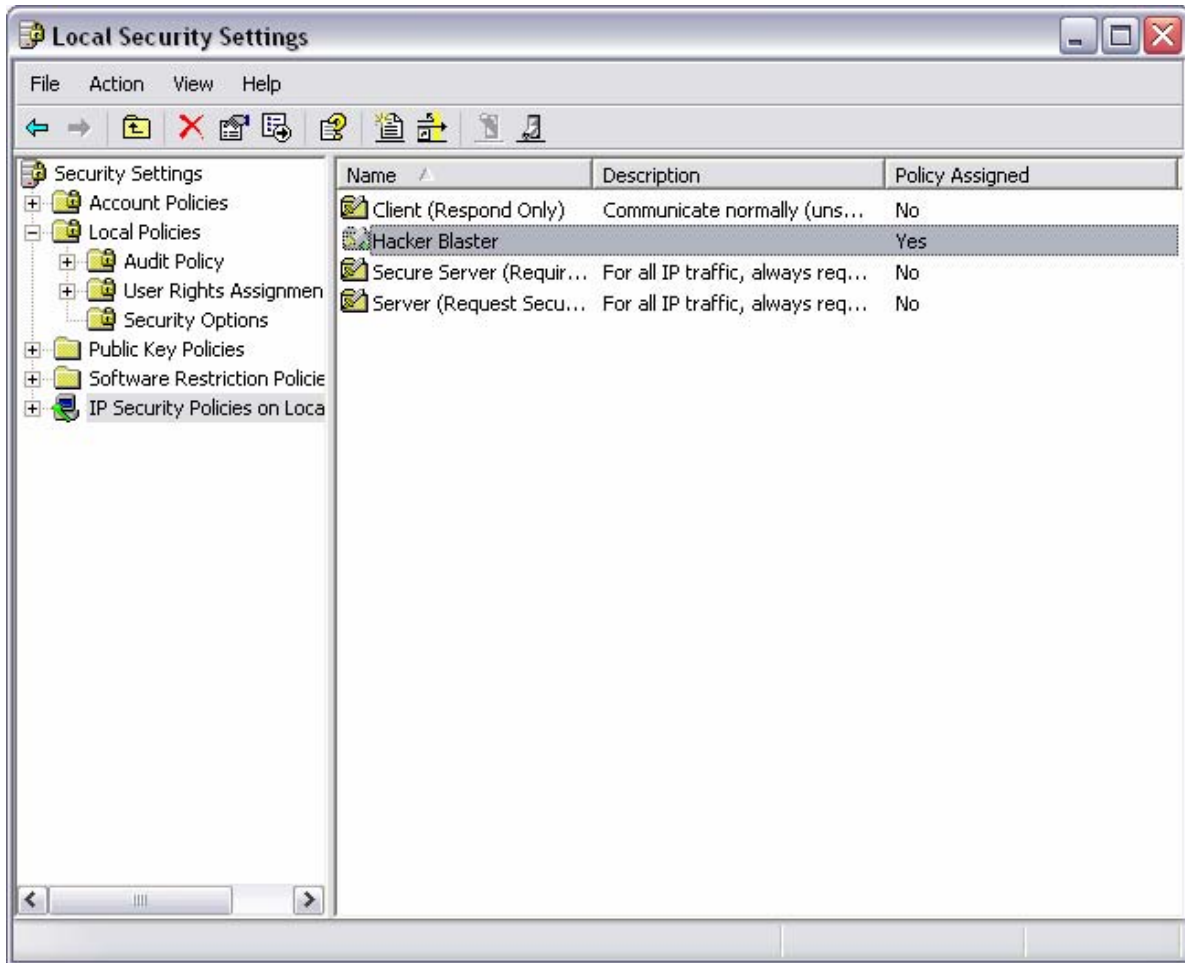
The editor can be started by going to the Control Panel and Opening the Administrative Tools folder and then clicking on “Local Security Policy”.

Once you have your Policy Editor opened click on the “IP Security Policies on Local Machine” choice (will be different on a Domain Controller but will be obvious which choice to make). As you can be in Figure #1 below I have created an IPSEC policy

named affectionately “Hacker Blaster”. Before a policy will take affect it must be “Assigned” which can be done by right-clicking on the policy and choosing “Assign”.

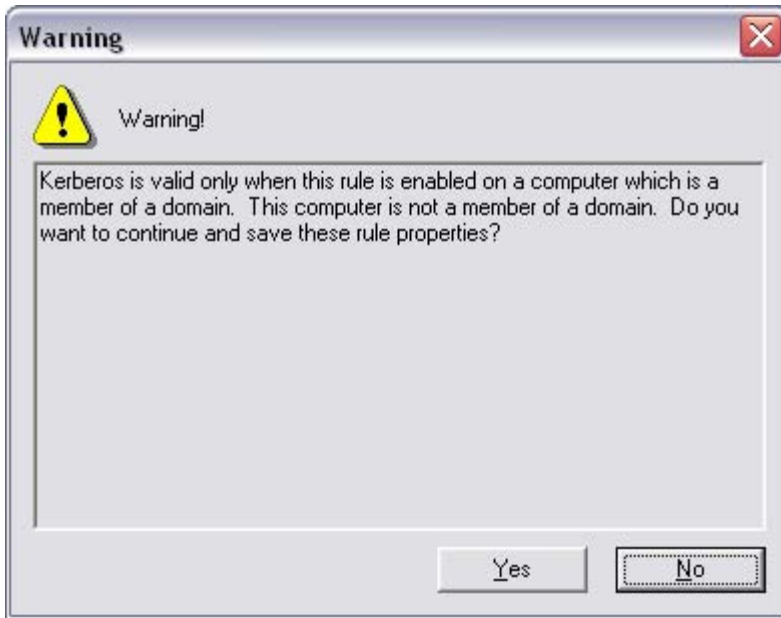
In this document we are going to setup IP and Port filters. There are going to be many wizards popping up asking you to set specific things. In this case we are only going to be filtering “Inbound” traffic to the computer.

Figure #1

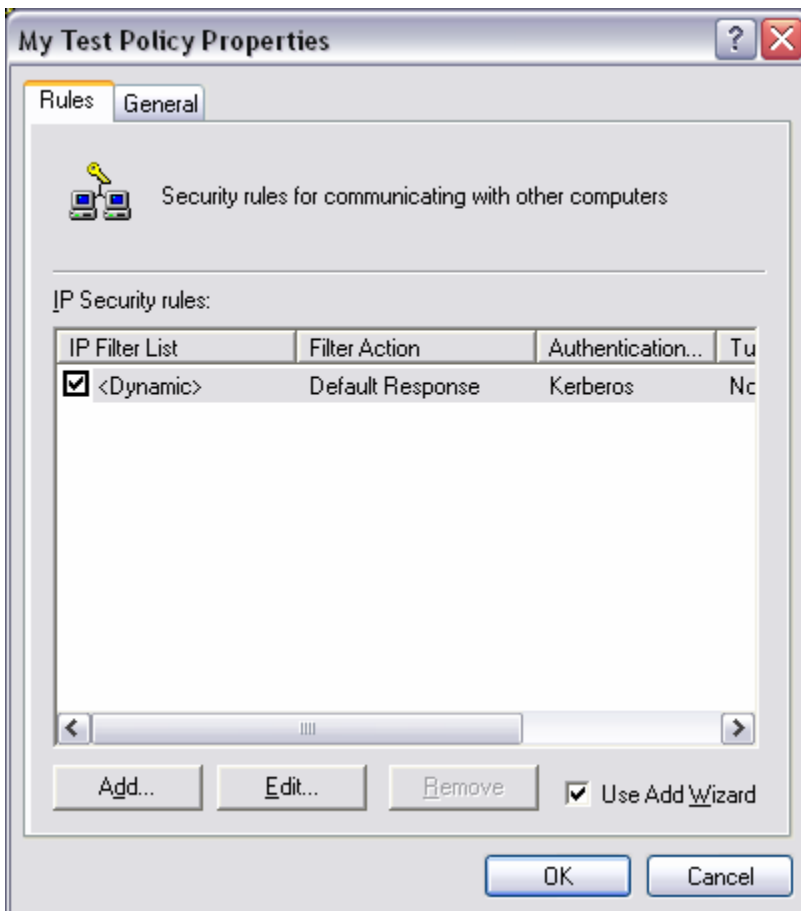


We are going to go ahead and create a new IPSEC Policy for this system.

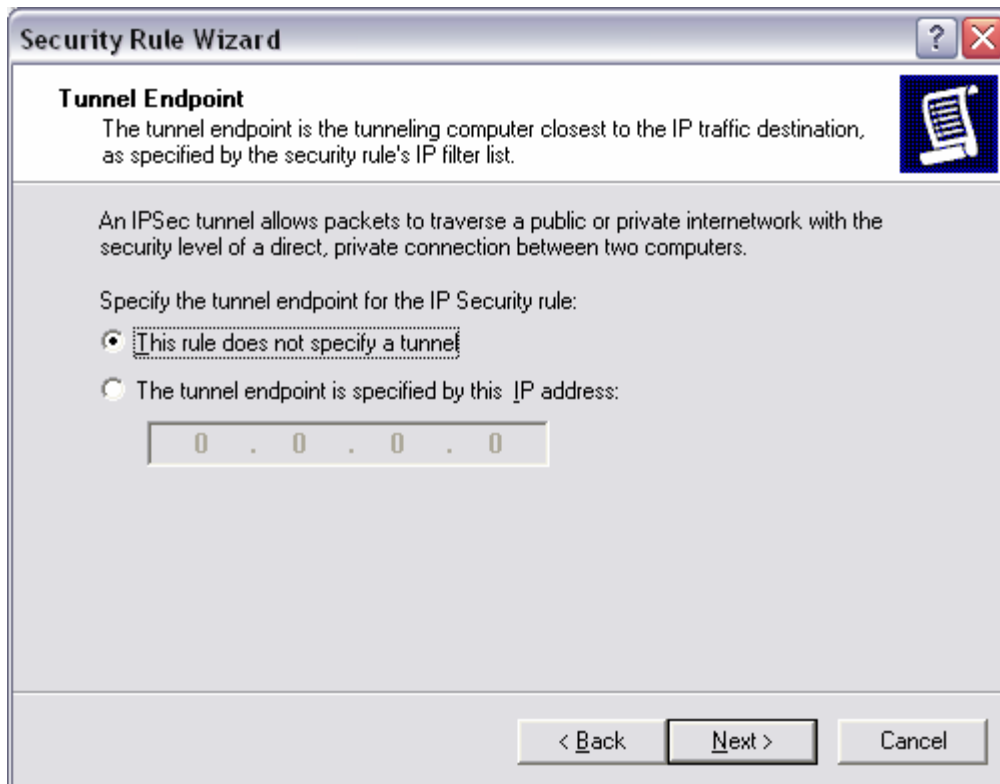
- 1) Right Click on IP Security Policies and choose “Create IP Security Policy”
- 2) A wizard will appear – Click “Next”
- 3) Give your policy a name – “My Test Policy”
- 4) Click “Next”
- 5) Leave “Activate the default response rule” checked and hit next
- 6) Leave current settings for next string as is and click “Next”
- 7) Ignore this warning on non-domain systems and click the “Yes” button



8) Click "Finish"- Policy properties will appear



9) Click "Add" where yet another wizard will appear – Click "Next"



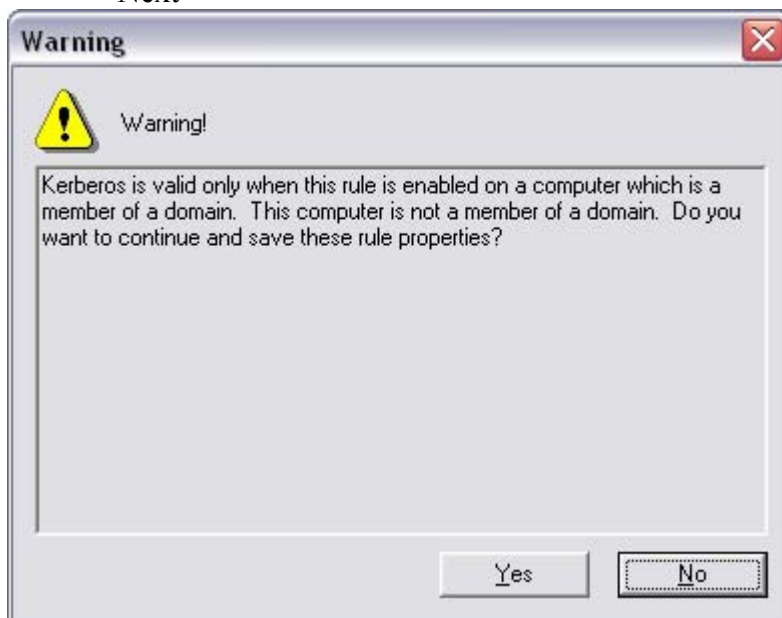
10) This rule will not apply to a tunnel – Hit “Next”



11) This will apply to “All network connections” – click “Next”



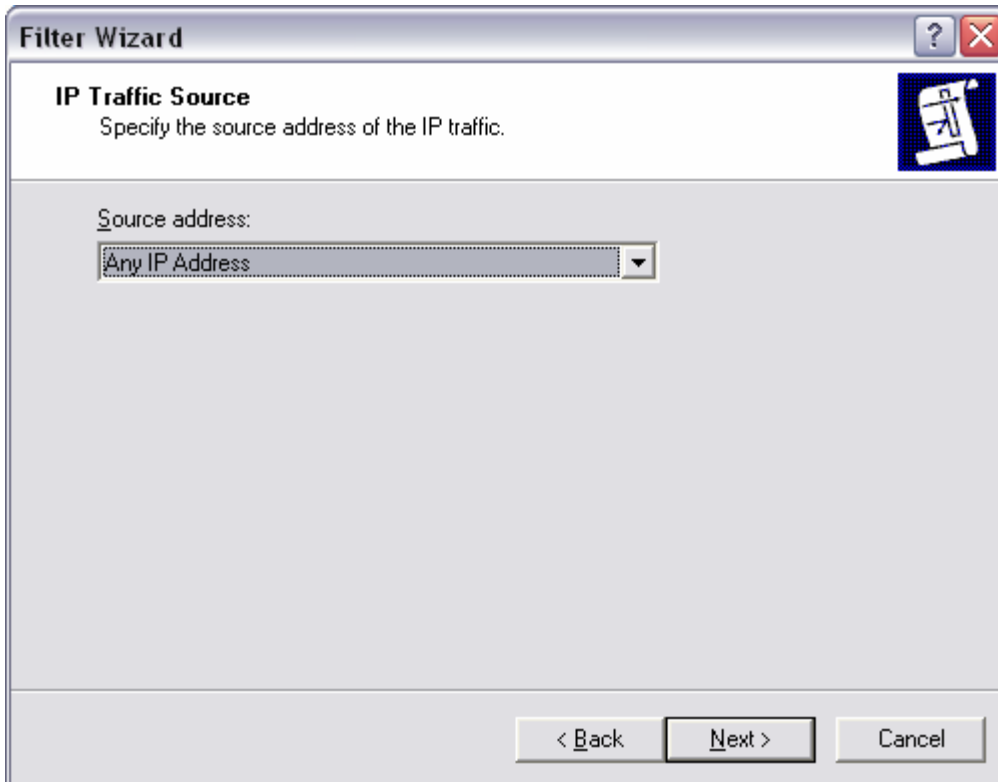
- 12) We are once again greeted with the same method as previously seen – Click “Next”



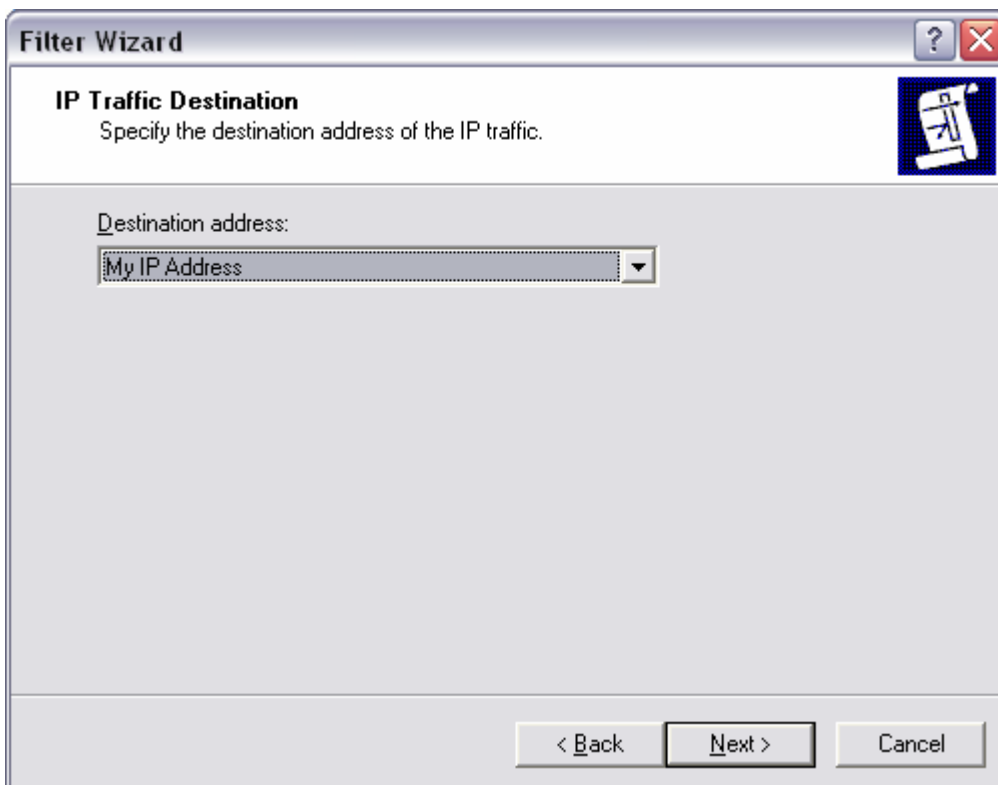
- 13) Once again click “Yes”



- 14) Finally we see something interesting. By default you will only see the first two entries. Ignore the other two for now. Here we are going to go ahead and create a new Filter for commonly attacked ports. Click the “Add” button now.
- 15) First we will create a Filter for the most attacked ports and call it “Evil Ports”. Next click the “Add” button
- 16) Great, another Wizard pops up. Hit “Next”



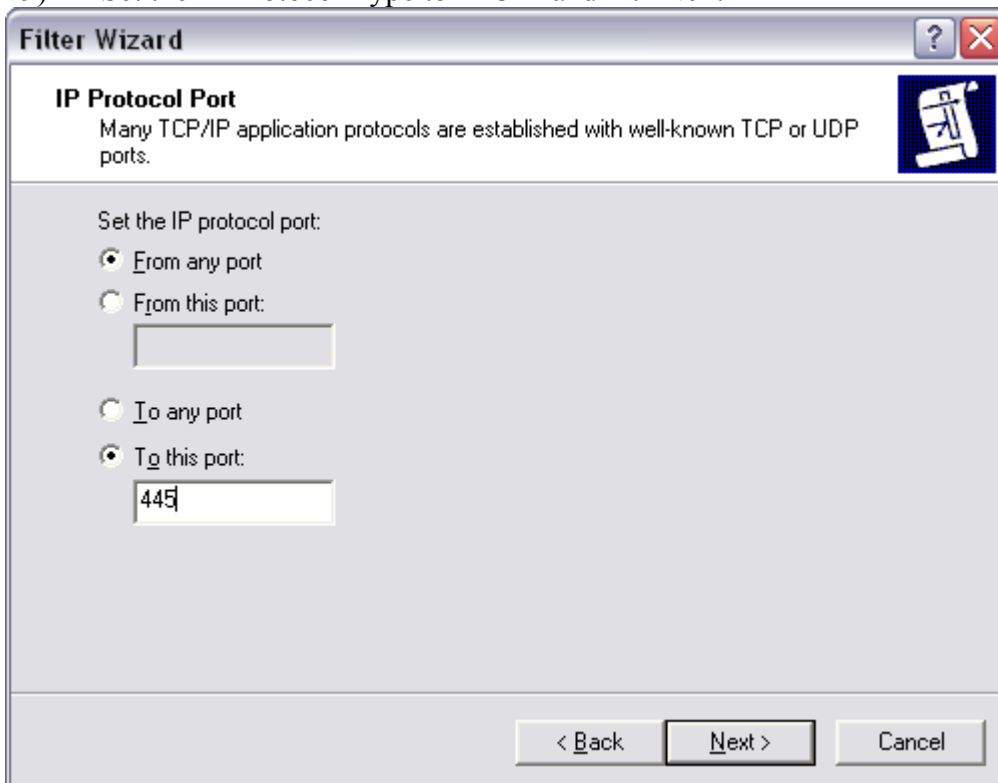
17) Set the IP Traffic Source to “Any IP Address” and click “Next”



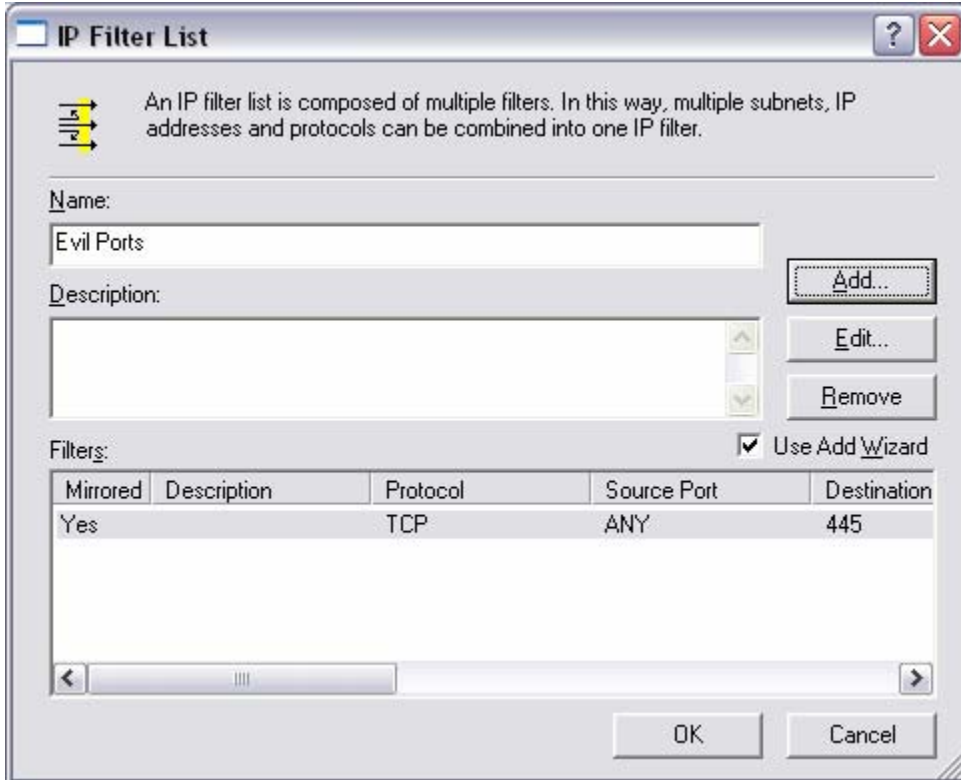
18) Set the IP Traffic Destination to “My IP Address” and hit “Next”



19) Set the IP Protocol Type to “TCP” and hit “Next”



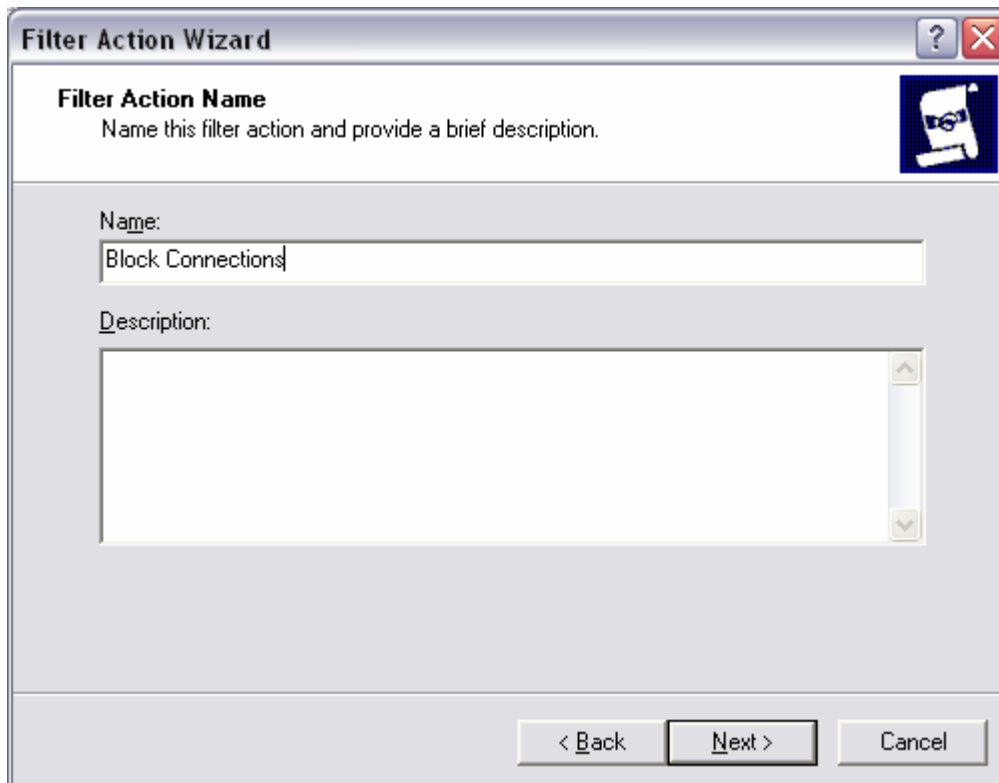
- 20) Leave the “From” port section blank and set the “To this port” to “445” and click “Next” – then click “Finish”



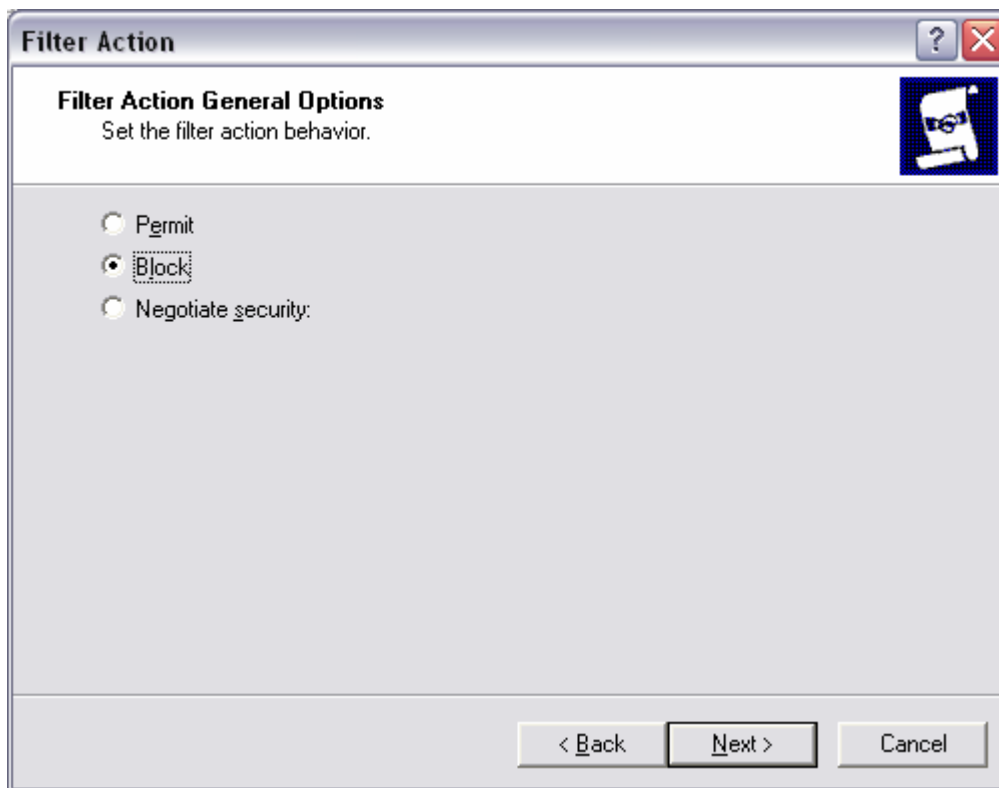
- 21) Now we have a port filter for port TCP/445. You can then click the “Add” button and add more ports. Refer to the list at the bottom of this page for a list I use.



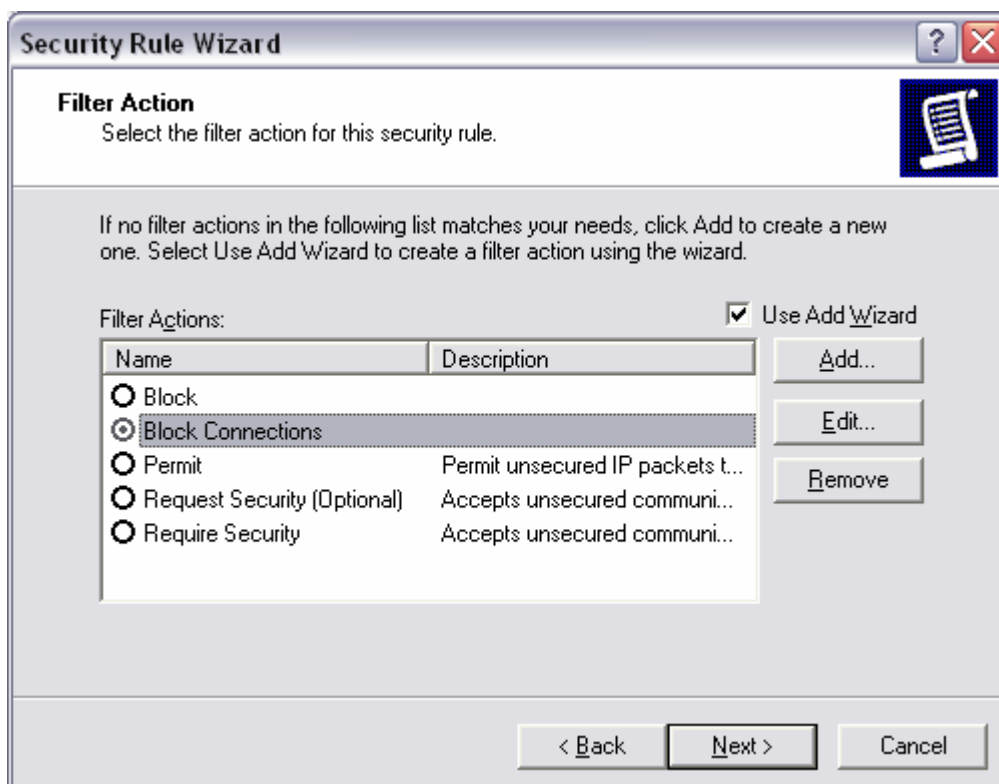
22) Make sure the radio button next to "Evil Ports" is selected and click "Next"



23) And of course we have another wizard popping up. Click "Next" and give your Filter Action a name. I chose "Block Connections" – Click "Next"



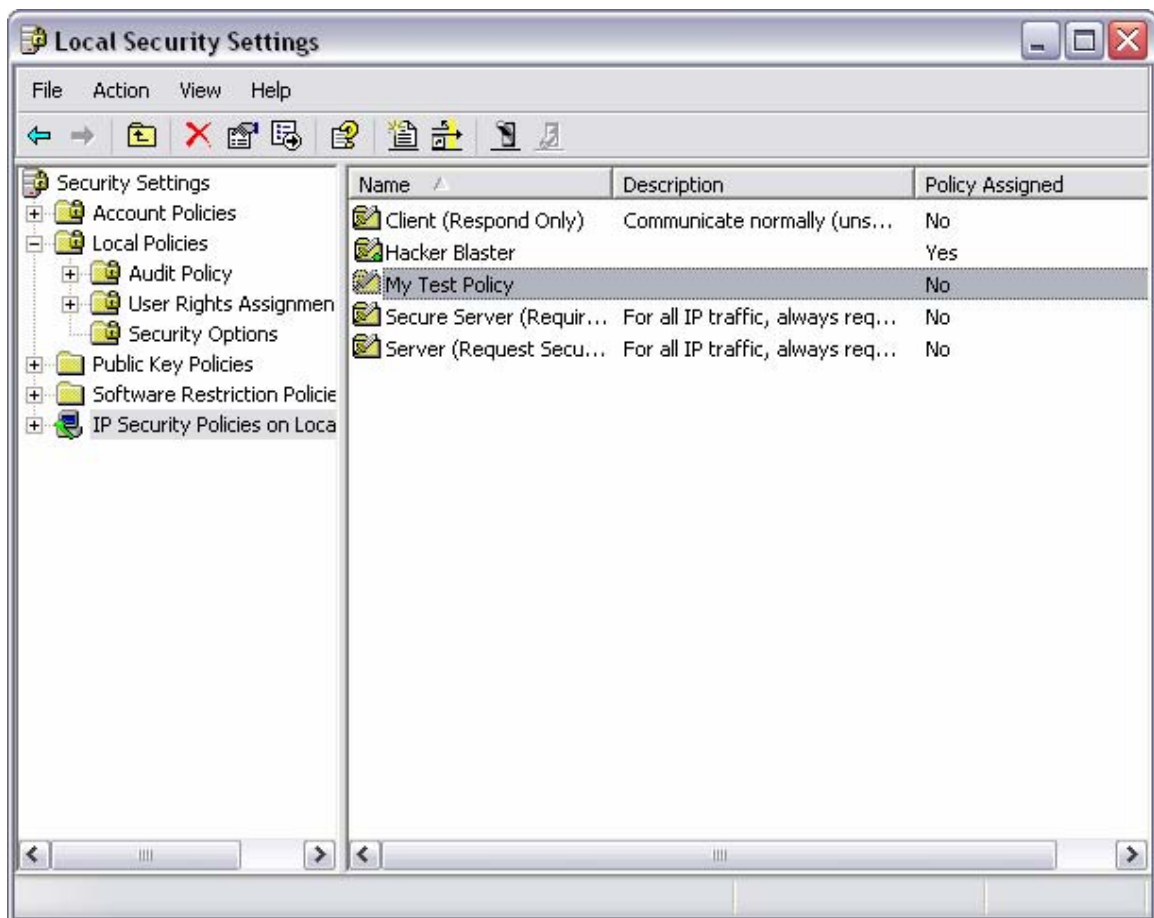
- 24) Make sure the “Block” radio button is highlighted and click “Next” then click “Finish”



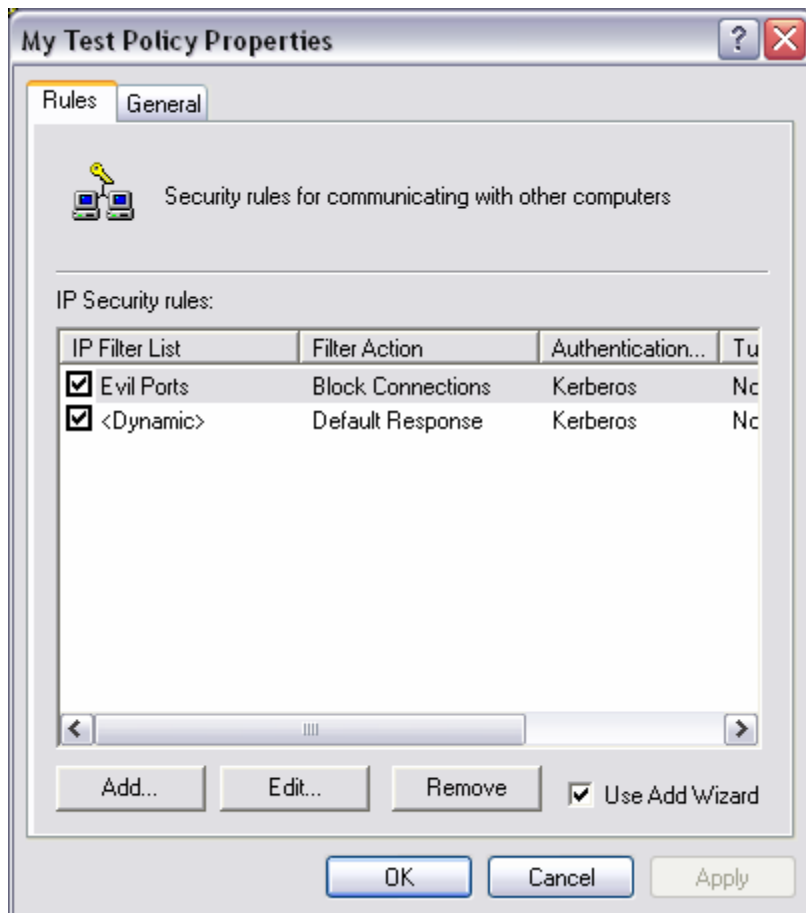
- 25) Make sure the radio button next to “Block Connections” is set and click “Next” - then click “Finish” – then click “OK”

At this point we have created a port filter which will drop all incoming connections to TCP 445. If other ports are added such as 139, 135 and 5000 this will remove most of the standard attack surface from the computer. Another huge benefit of this will be removing the ability for these systems on the network to attack each other in the even one does get infected by user intervention such as installing a pretty screen saver that has a backdoor installed.

Now, there may be systems that you want to have access to these “Evil Ports” such as a Domain Administrator’s workstation or an SMS server and the like. Here we will create a filter that allows these systems access. And yes, more wizards to click on.



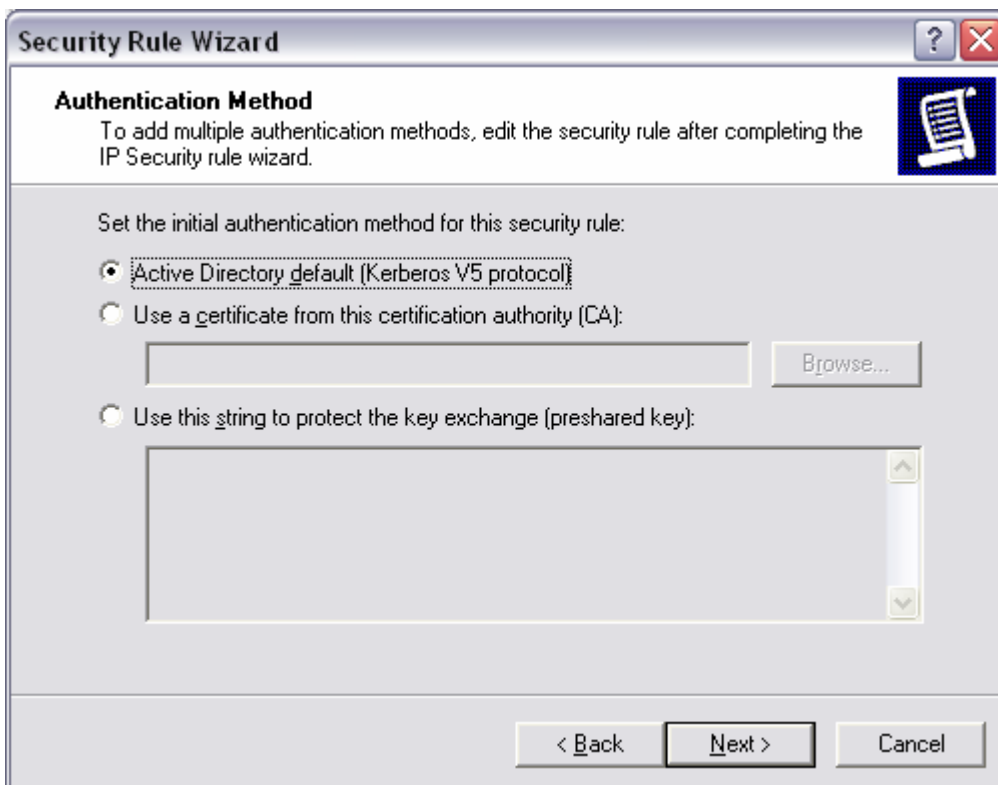
- 26) Double click on the “My Test Policy”



- 27) Click “Add” – then click “Next” and use the “This rule does not specify a tunnel” – Click “Next”



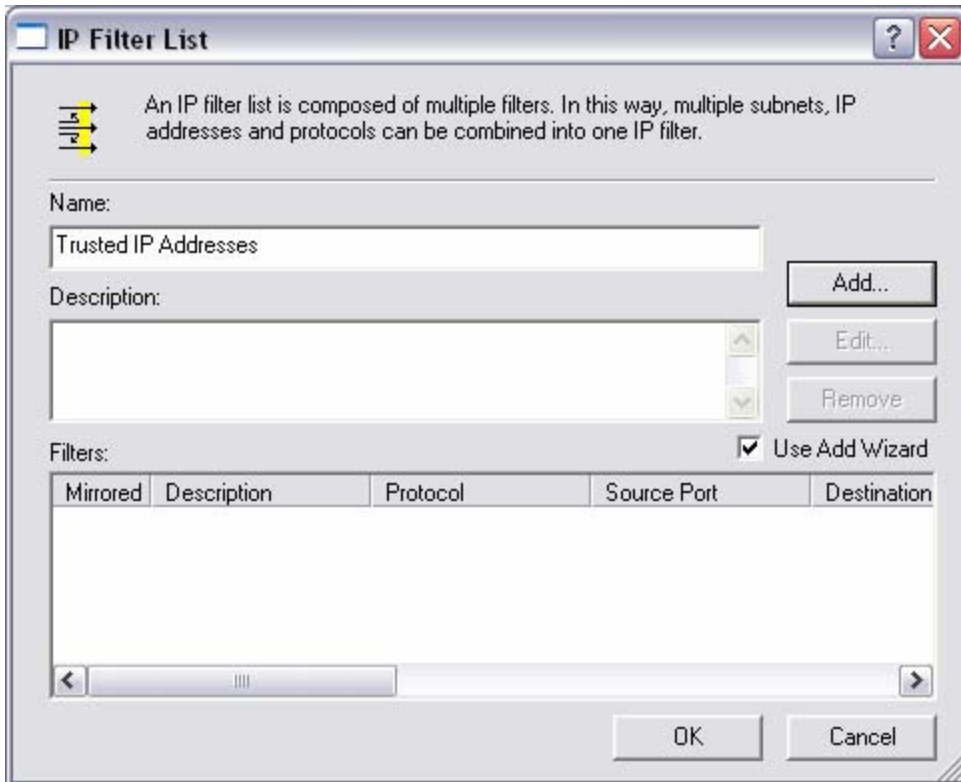
28) Choose "All network connections" and click "Next"



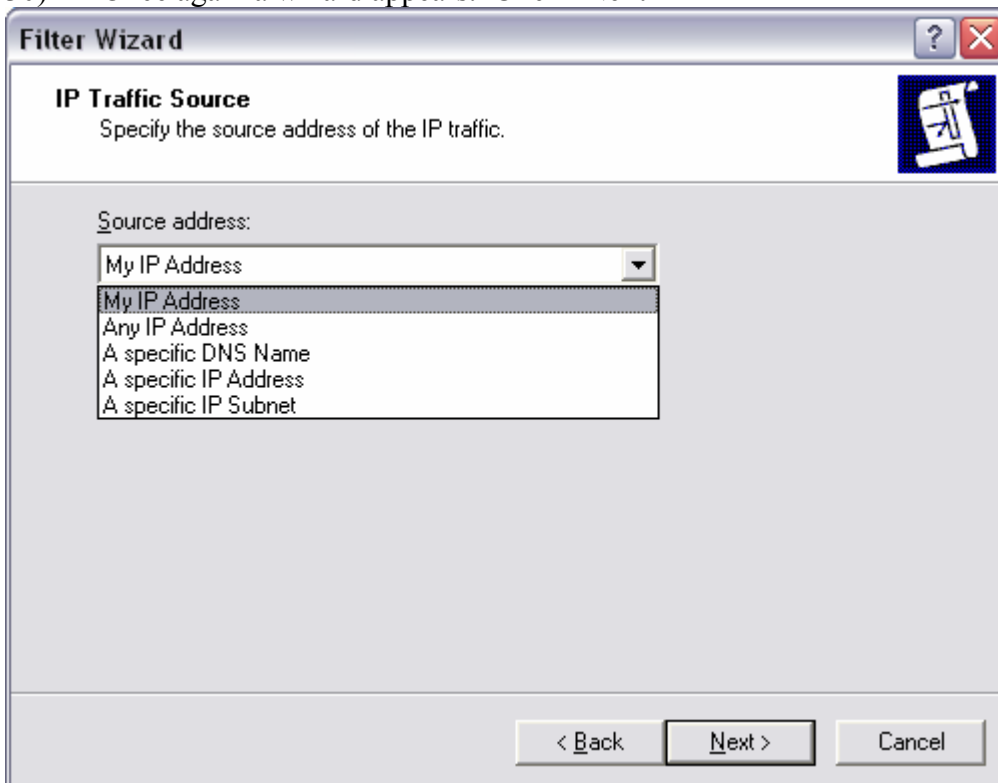
- 29) Use the default authentication method and click “Yes” on the warning if it pops up.



- 30) We are now going to create a “Trusted IP” filter list. Click “Add”



30) Once again a wizard appears. Click "Next"



- 31) Here we have several choices. In this example we are going to use an IP address. DNS names may be the best way to go in a Domain, however.

The screenshot shows the 'Filter Wizard' dialog box at the 'IP Traffic Source' step. The title bar reads 'Filter Wizard' with a help icon and a close button. The main heading is 'IP Traffic Source' with the instruction 'Specify the source address of the IP traffic.' Below this, there is a dropdown menu for 'Source address:' with the option 'A specific IP Address' selected. Underneath, there are two input fields: 'IP Address:' containing '130 . 91 . 75 . 101' and 'Subnet mask:' containing '255 . 255 . 255 . 255'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

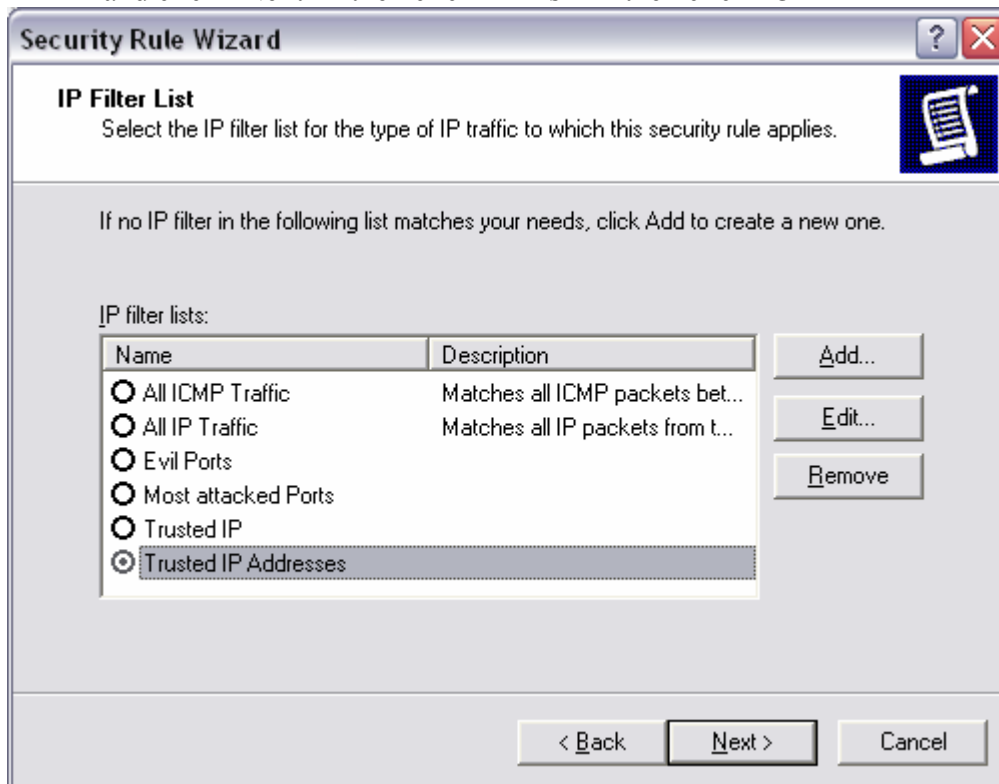
- 32) Here we enter in a specific IP address and click "Next"

The screenshot shows the 'Filter Wizard' dialog box at the 'IP Traffic Destination' step. The title bar reads 'Filter Wizard' with a help icon and a close button. The main heading is 'IP Traffic Destination' with the instruction 'Specify the destination address of the IP traffic.' Below this, there is a dropdown menu for 'Destination address:' with the option 'My IP Address' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

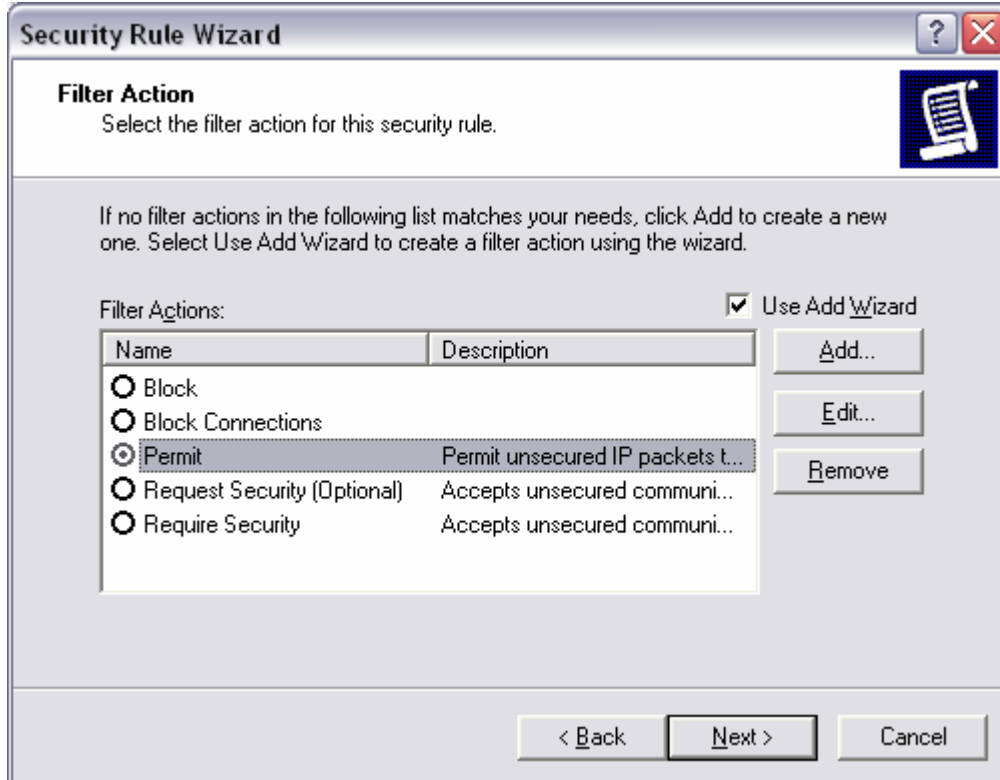
32) Choose “My IP Address” as the destination of the traffic and click “Next”



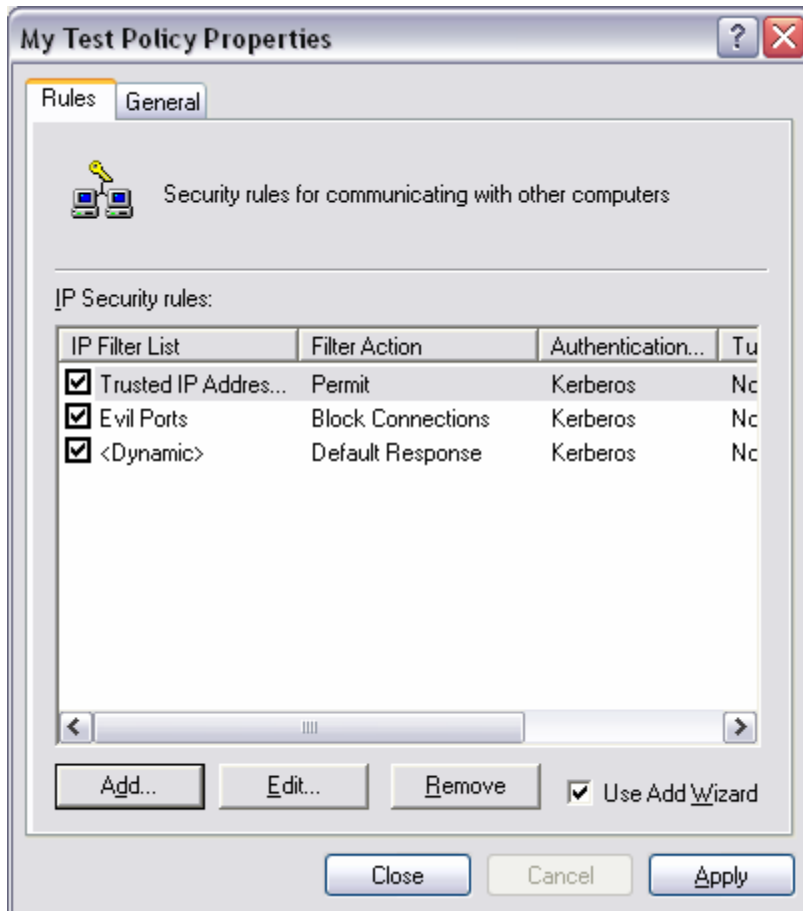
33) To allow all traffic from this trusted IP address leave protocol type to “Any” and click “Next” – then click “Finish” – then click “OK”



- 34) Make sure the radio button next to “Trusted IP Addresses” is set and click “Next”



- 35) Make sure the radio button next to “Permit” is set and click “Next” – then click “Finish”



36) Now we have our trusted IP filter in place. Click “Apply” then “OK”

37) Make sure the policy is “Assigned”

Using Active Directory Group Policies this is a pretty easy task to accomplish. You create your IPSEC policy and add it to a Group Policy and then apply to Organizational Units as appropriate. Using this method on stand-alone machines is somewhat tedious but much easier to do than having to rebuild the machines after a system compromise.

| Port | Description |
|------|---------------------|
| 445 | Netbios over TCP/IP |
| 139 | Netbios |
| 135 | Epmmap |
| 5000 | Plug and Play |
| | |

Some helpful links

How to block specific network protocols and ports by using IPSec

This is a great resource for using IPSECPOL.EXE and IPSECCMD.EXE

<http://support.microsoft.com/?id=813878>

Step-by-Step Guide to Internet Protocol Security (IPSec)

This shows how to use different authentication methods including certificates. There are also a lot of useful links on this page.

<http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp>

IANA assigned ports for reference

<http://www.iana.org/assignments/port-numbers>

David Taylor

SR Information Security Specialist

University of Pennsylvania

ltr@isc.upenn.edu

215-898-1236