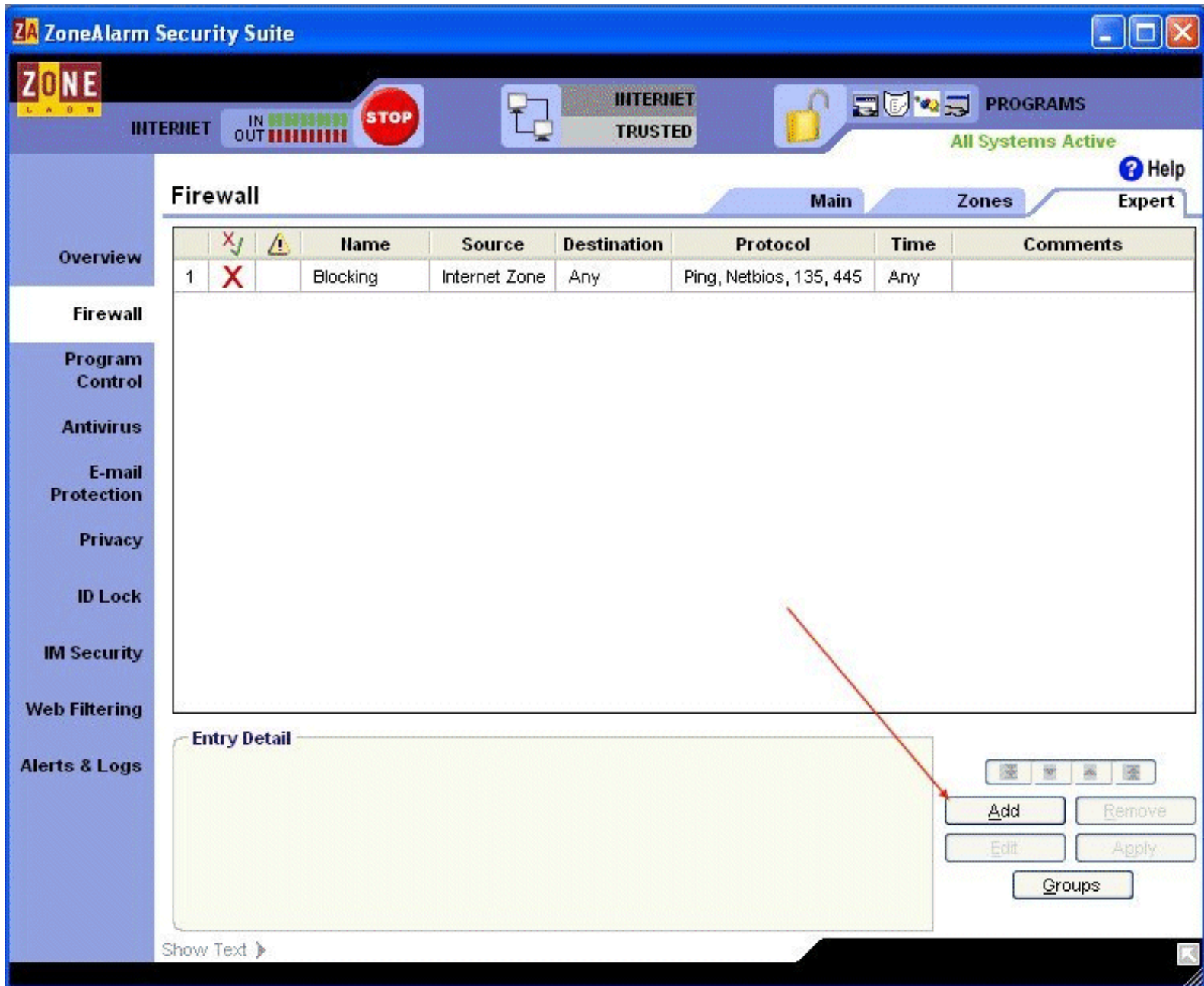


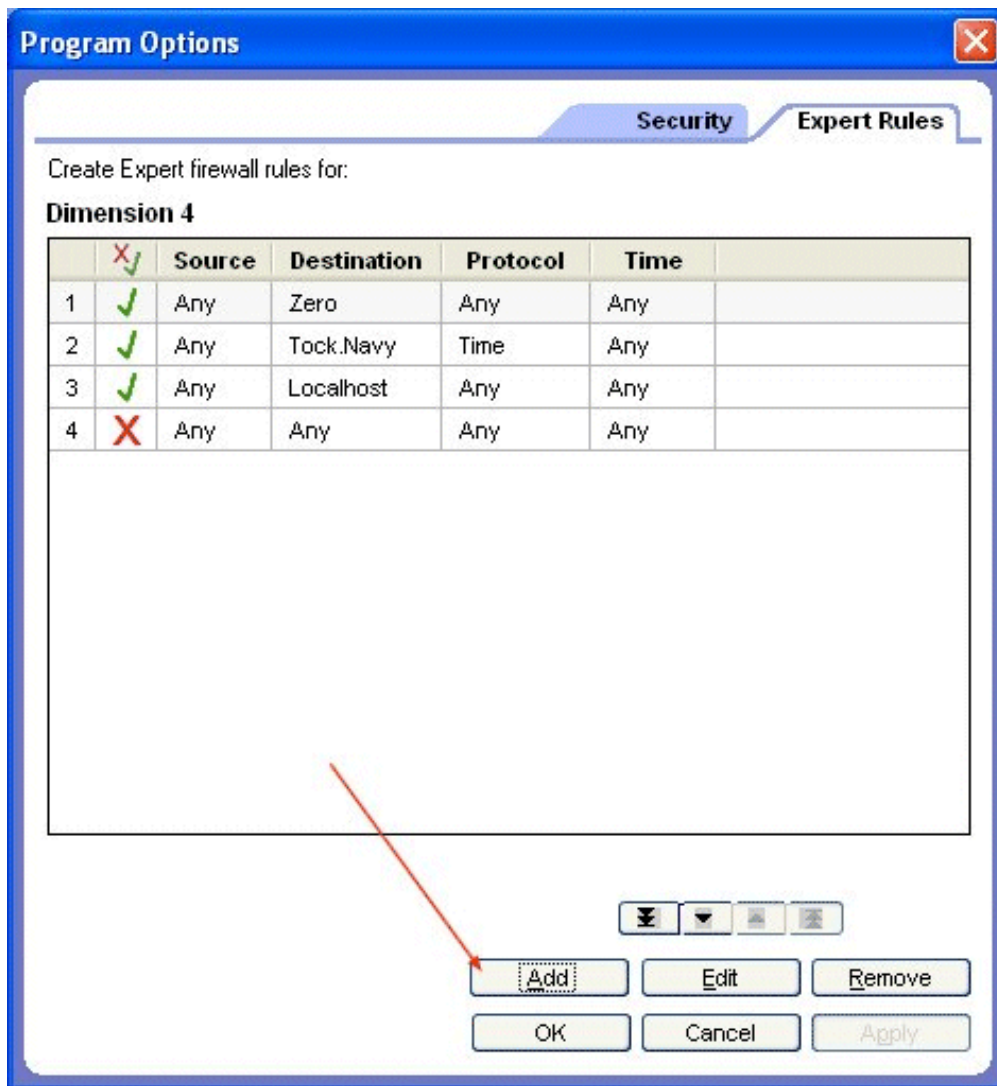
# Creating Expert Rules

First thing you need to do is to get to the kind of expert rule you want to create. First firewall expert rules are global in nature, they affect the entire connection



This is where you start adding expert firewall rules. Just click this add button.

Now for Program expert rules, go to the program list in ZA and right click on the program you want to add an expert rule to, and select options, then select the expert tab and this is what you will get.



And just like the firewall expert rules you click add.

## *General Area*

Once you get this far the rest of creating an expert rule is the same.

First thing you want to determine is rank. Now for Firewall expert rules this is a big deal. Each rule is enforced in the order listed, and only the first rule that matches will be enforced. But for program expert rules all the rules are enforced equally, so the order doesn't make any difference, except for the blocking rule (to be explained later)

The second thing you want to determine is the Name of the rule. This is required so give it a name that you will know what it means.

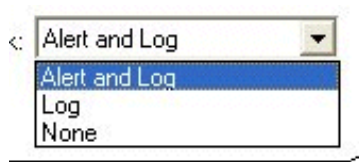
Next you can add any comments in that you need to help your figure out later why you did this rule.

Next you need to pick the state. Enabled means this rule will be checked, disabled means that the rule will be ignored. This comes in handy when first writing rules and you need to find out what the problem is or if the rule is doing what you want it to.

Next is the Action that you want. Allow means this rule allows a connection to go through. Block means this connection is blocked.

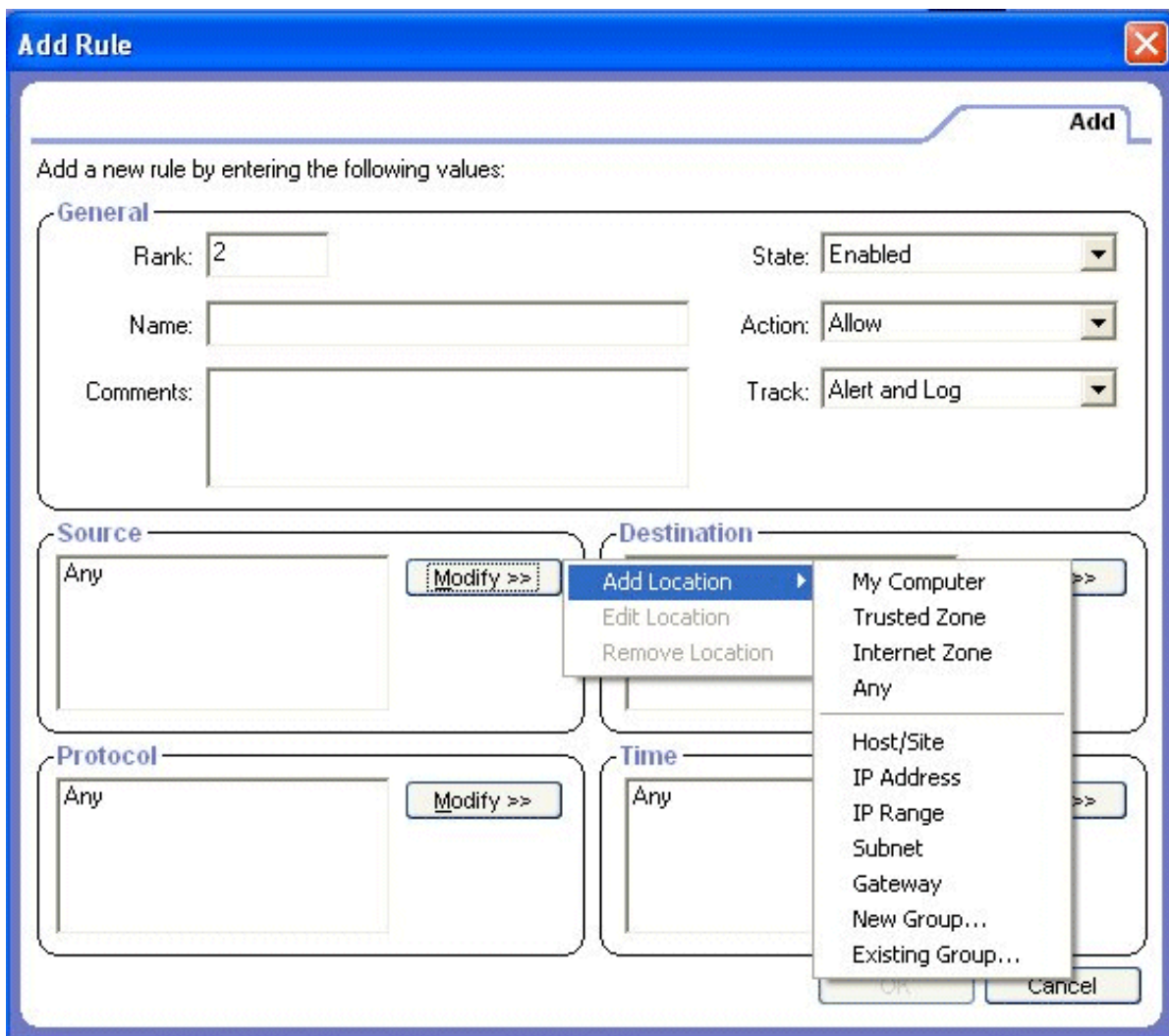
Next is the track options. Alert and log means you will get a popup and you will get an entry in the log that this rule was enforced. Not just that it was blocked, but that the conditions in the rule were met. Log will just give you a log entry, and then none means that

you will not be told when this rule is met.

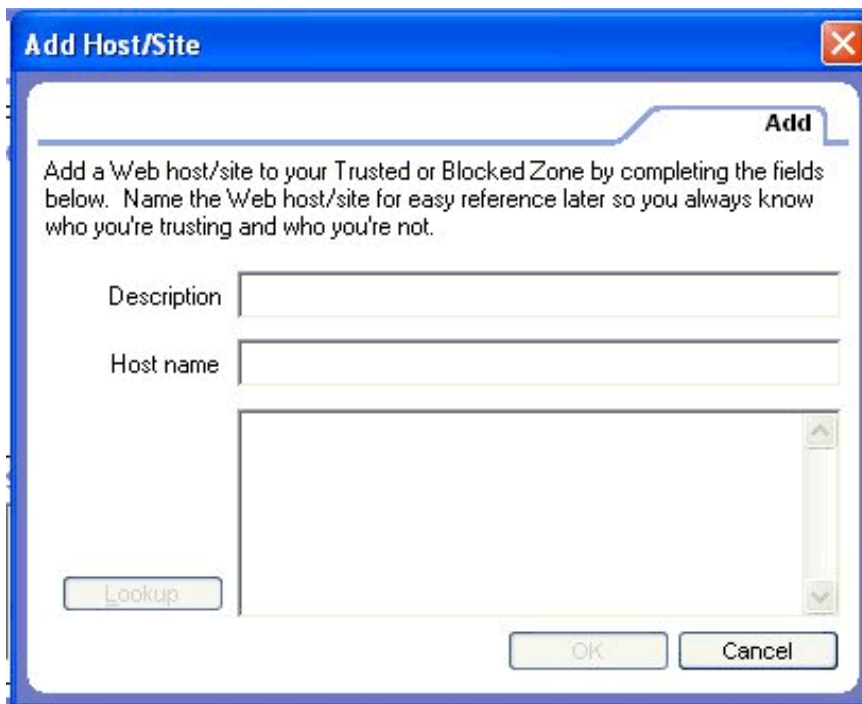


## Source Area

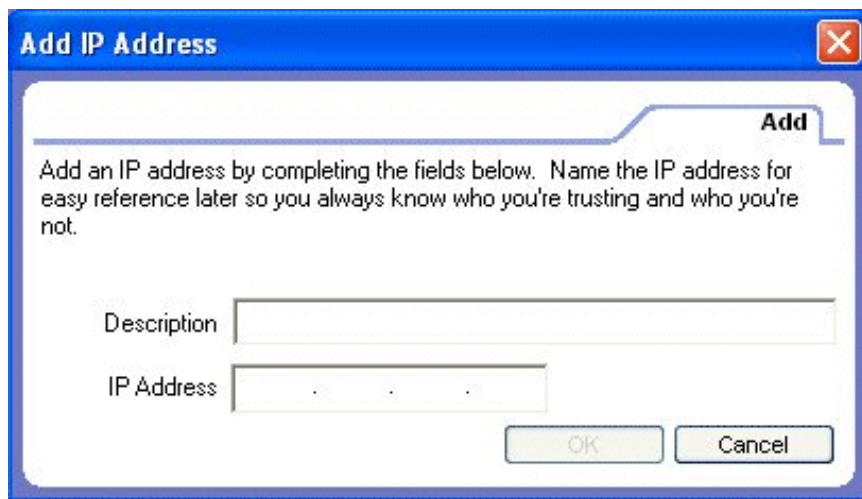
Next is figuring out the source. You have several selections you can choose from for your source. First is My computer is just that, your own computer, Trusted zone is your computer and any others that have been listed in the trusted zone. Internet zone is everything that is not your computer or trusted, and any is both internet and trusted zone.



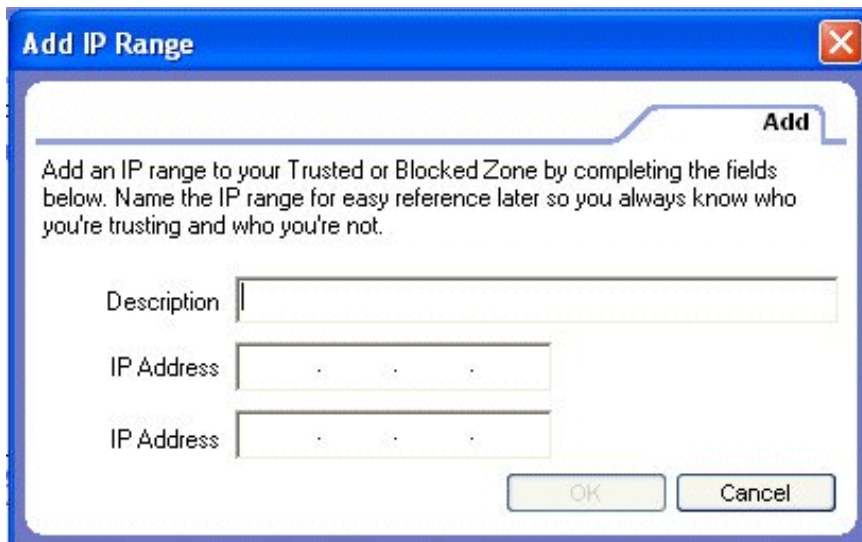
For Host or site you want to first give it a name, and then an web address, but don't enter in the http:// or ftp:// all you need is the web address. Then you need to click the lookup button to get the IP address.



Next is adding an IP address. Once again just give it a name and then enter in the IP address.



Next is adding an IP Range. Give it a name and then enter the first IP address and then the last IP address.



Next is a subnet. Again give it a name then enter in the base IP address, then enter in the subnet mask.

**Add Subnet**

**Add**

Add a subnet to your Trusted or Blocked Zone by completing the fields below. Name the subnet for easy reference later so you always know who you're trusting and who you're not.

Description:

IP Address:

Subnet Mask:

OK Cancel

Next is adding a gateway. This is if you want to just allow traffic from your gateway for this rule, and no place else.

**Add Gateway**

**Add**

Enter the following values for the new Gateway:

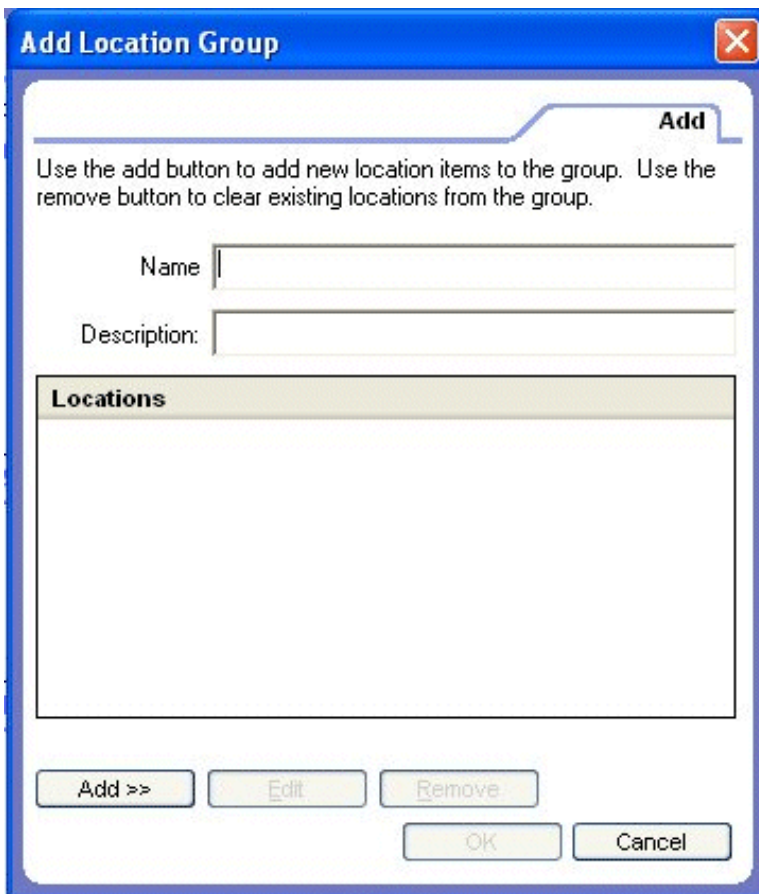
IP Address:

MAC Address:

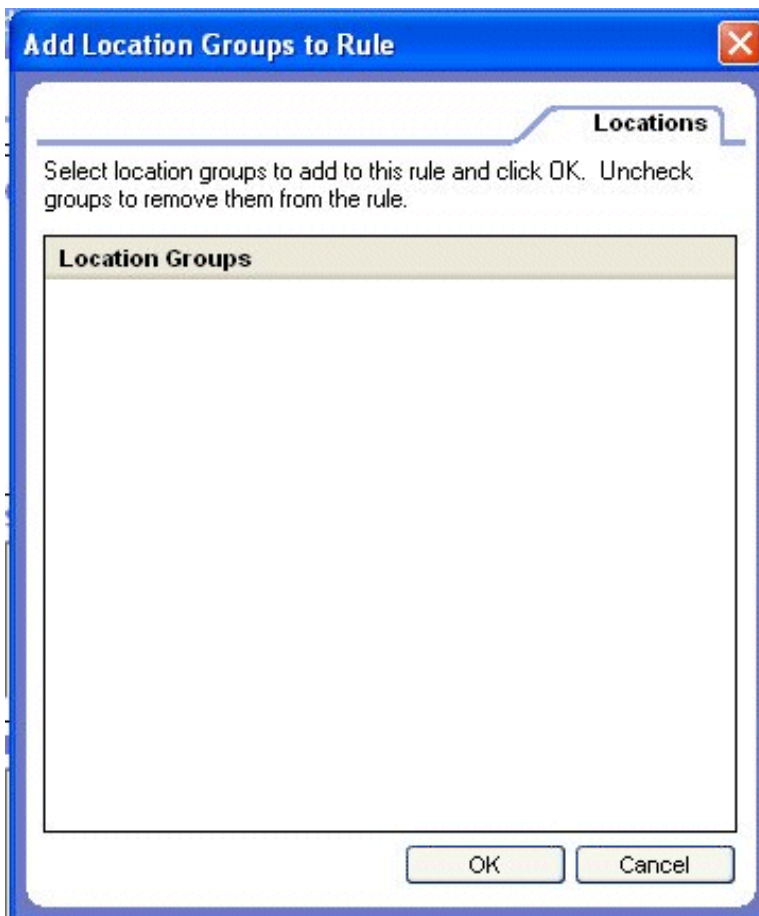
Description:

OK Cancel

Next is an area where you can create groups of locations. When doing this you the same choices to add as above, the host / site, IP address, IP Range and Subnet. And you add them they same way.



And next is used if you already have a group created that you want to add.

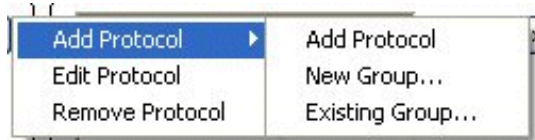


# Destination Area

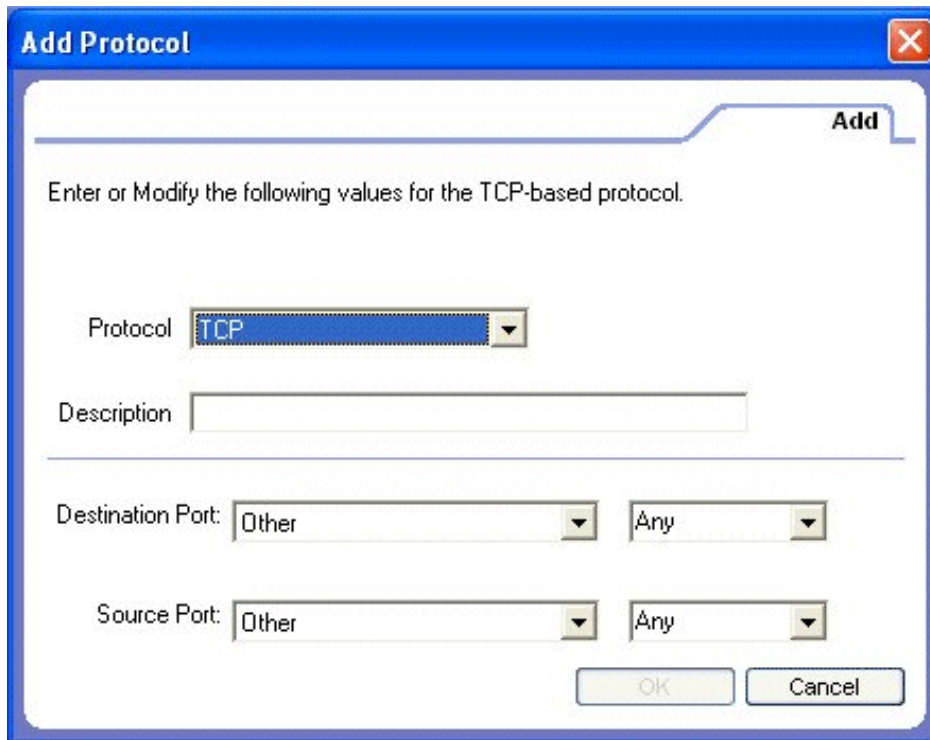
# Protocol Area

This section is identical to the Source area.

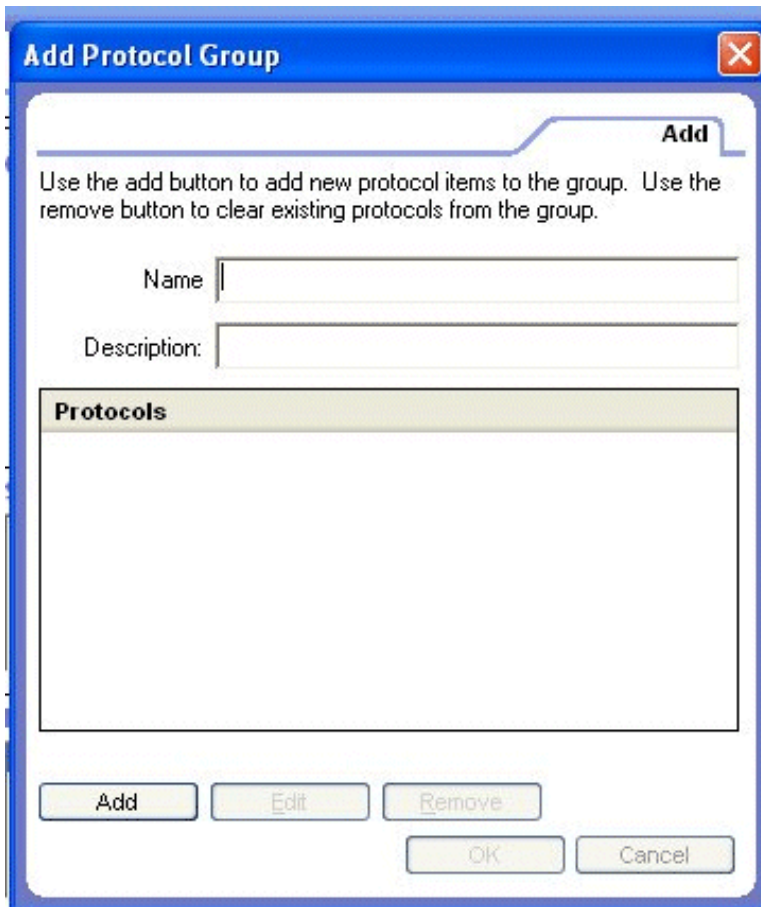
Here is where you enter the protocol or Port number that you want to use for the rule, and there are several ways to do this also. You can also click on a protocol that you have added and edit it or delete it.



First is adding a protocol. First you need to give it a name then if the name of the protocol isn't in the protocol drop down list then just click on ANY and enter in the port number.

The image shows a Windows-style dialog box titled 'Add Protocol'. At the top right is a close button (X). Below the title bar is a tab labeled 'Add'. The main area contains the text 'Enter or Modify the following values for the TCP-based protocol.' Below this are several input fields: a 'Protocol' dropdown menu with 'TCP' selected, a 'Description' text box, and two pairs of dropdown menus for 'Destination Port' and 'Source Port'. Each pair has 'Other' and 'Any' as options. At the bottom right are 'OK' and 'Cancel' buttons.

You can also add groups of protocols using this form,



**Add Protocol Group** [X]

**Add**

Use the add button to add new protocol items to the group. Use the remove button to clear existing protocols from the group.

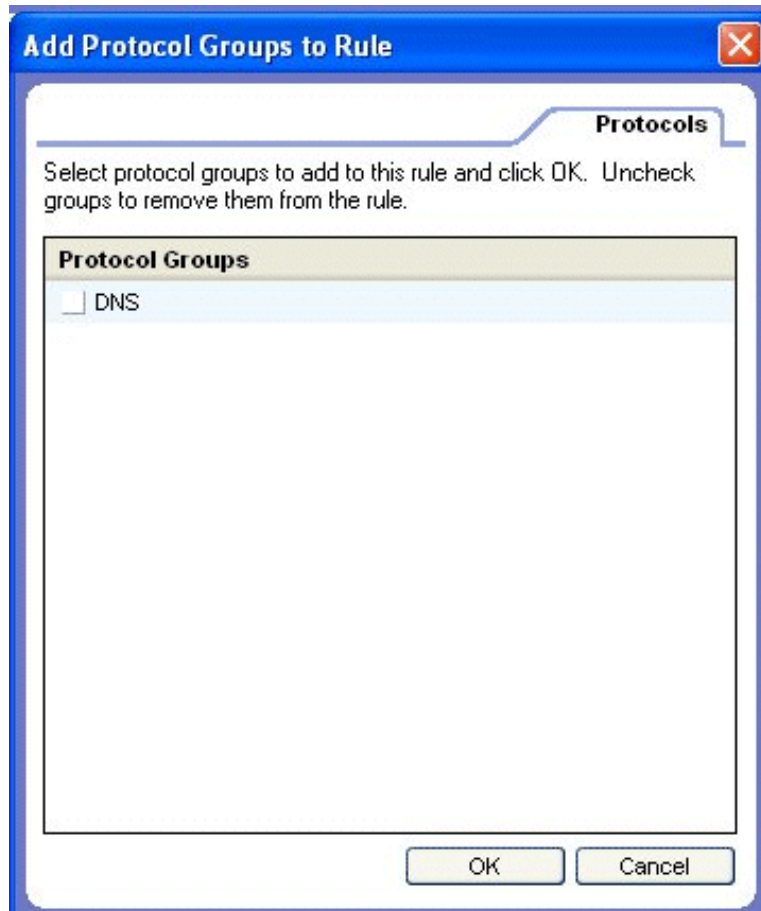
Name:

Description:

**Protocols**

--

And if you have an existing group you want to add tot he rule, use this form,



**Add Protocol Groups to Rule** [X]

**Protocols**

Select protocol groups to add to this rule and click OK. Uncheck groups to remove them from the rule.

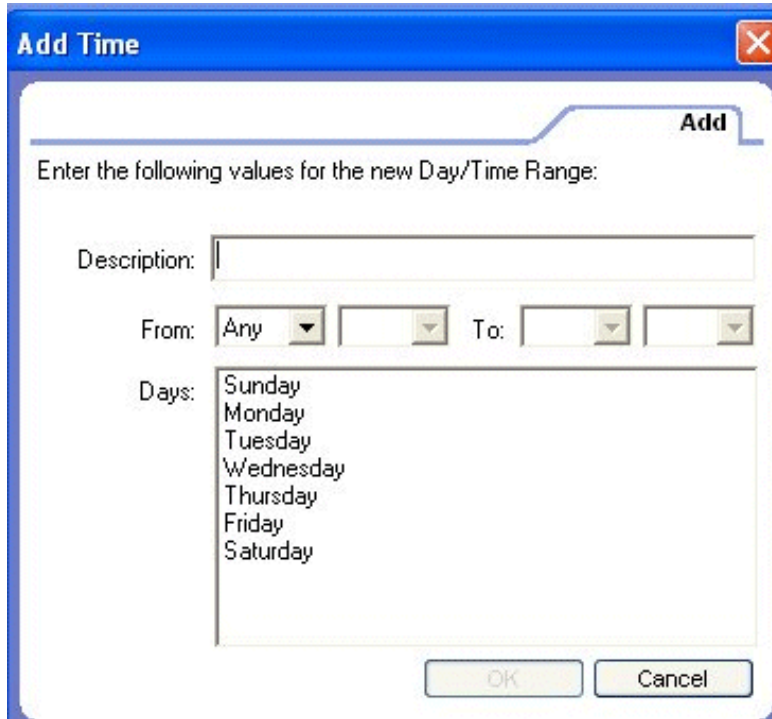
**Protocol Groups**

<input type="checkbox"/> DNS
------------------------------

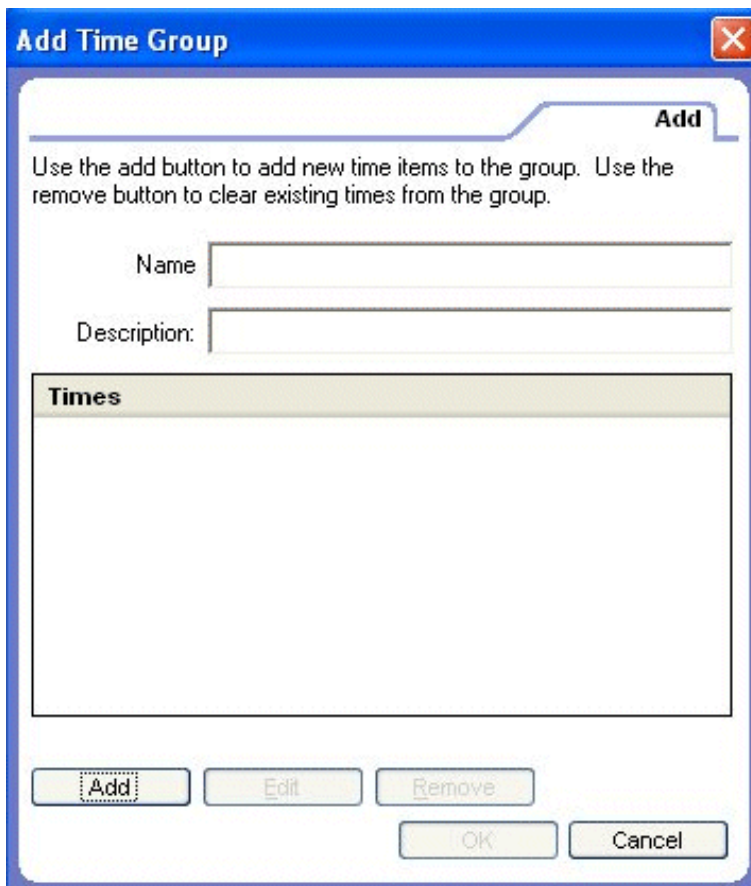
The last thing you can change for the expert rule is a time component. You can also click on an existing time component and edit it or remove it.



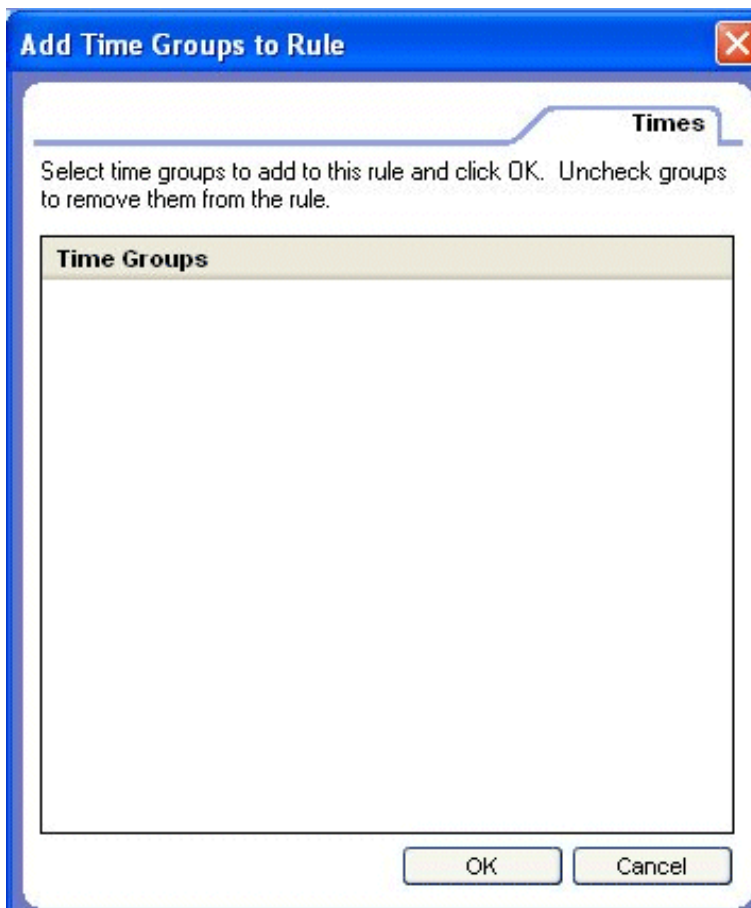
Again the first thing you do is give it a name, then select the times you want it to be in affect, then select the days you want it to be in affect. Use the ctrl and shft keys to select groups or add a day to the selection.



You can also create time groups to add.



And then if you have existing time groups you can then select those groups to add in.



# *Finishing The Expert Rules*

Now all you have to do is click OK and that expert rule is done.