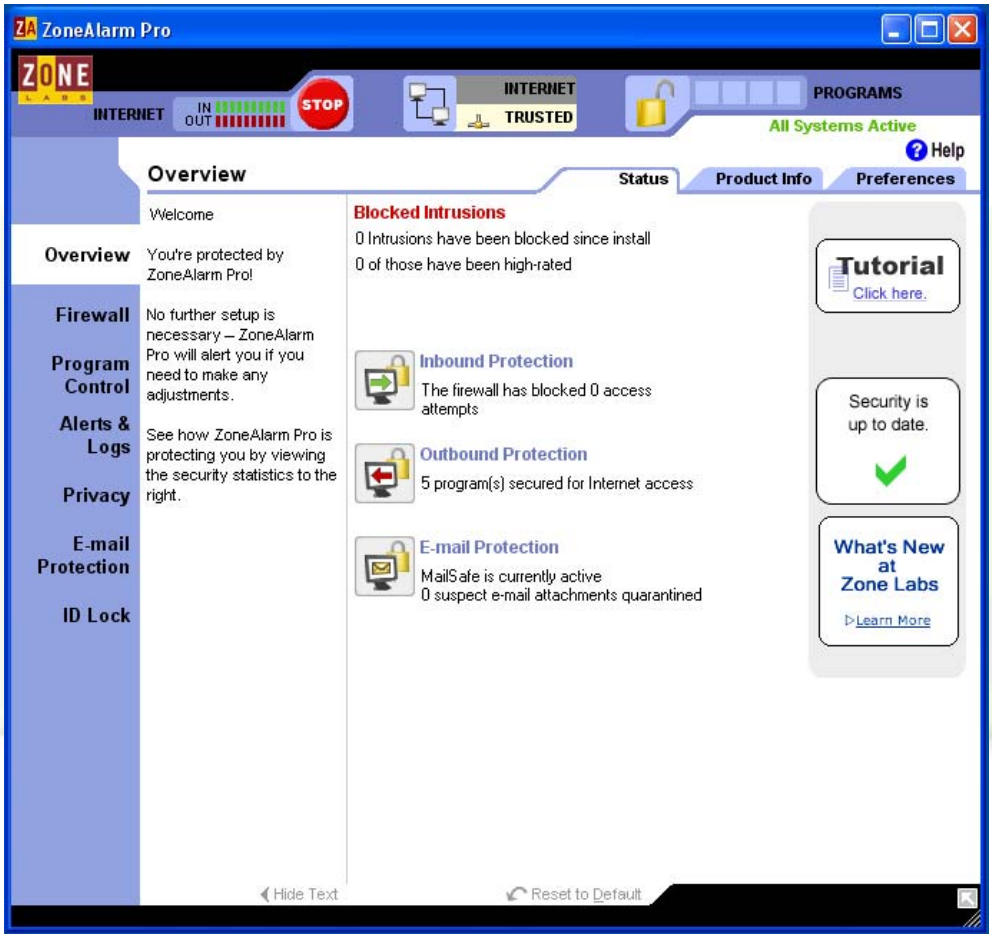
5.9.1

INTRUSION DETECTION

(ZoneAlarm)



March 2005

Laboratory Overview

Objective

At the end of this lab students will be able to install and configure ZoneAlarm Pro. They will also be able to customize the settings within ZoneAlarm Pro and tailor alerts for both interactive and log file settings.

Information for Laboratory

A. Students will utilize Zone Alarm Pro Firewall software

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Warning[s]

Once ZoneAlarm Pro is configured with the standard settings, almost any program accessed will set off an alarm. It is recommended that you uninstall ZoneAlarm Pro after this lab.

Estimated Completion Time

35 Minutes

Intrusion Detection Systems

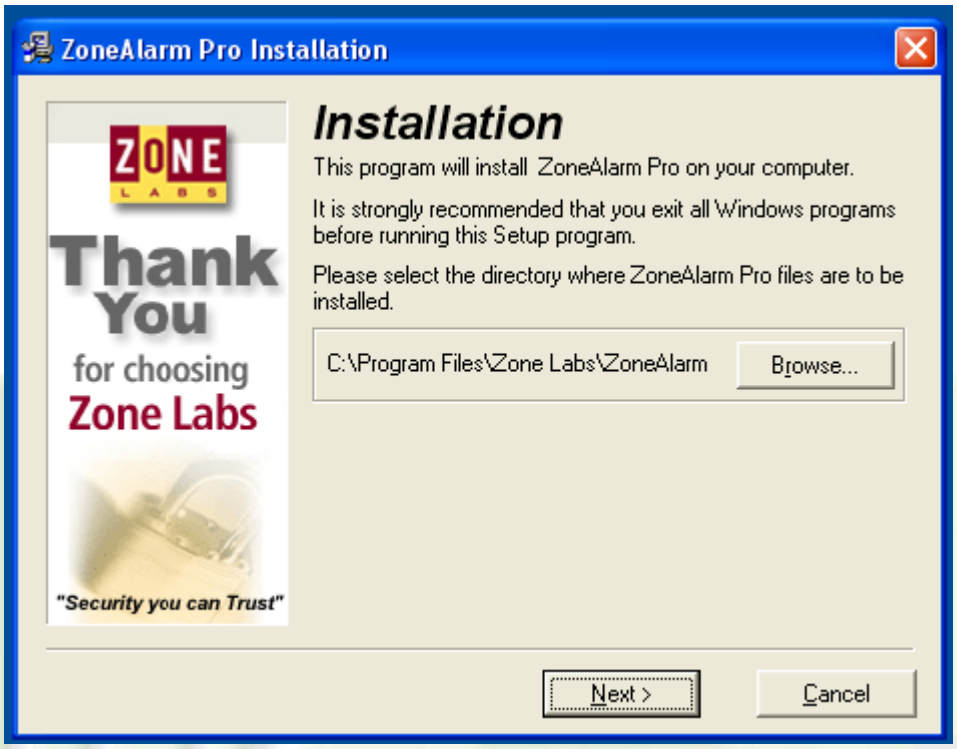
Intrusion Detection Systems come in two basic varieties: enterprise and personal PC-based. Enterprise IDS's are usually quite expensive, (upwards of $20K), but are very flexible in both configuration and reporting. IDS's are usually used in *conjunction* with a firewall product, not as a replacement for one. An Intrusion Detection System can give a network manager immediate feedback on what is happening on their network at that point in time.

ZoneAlarm Pro

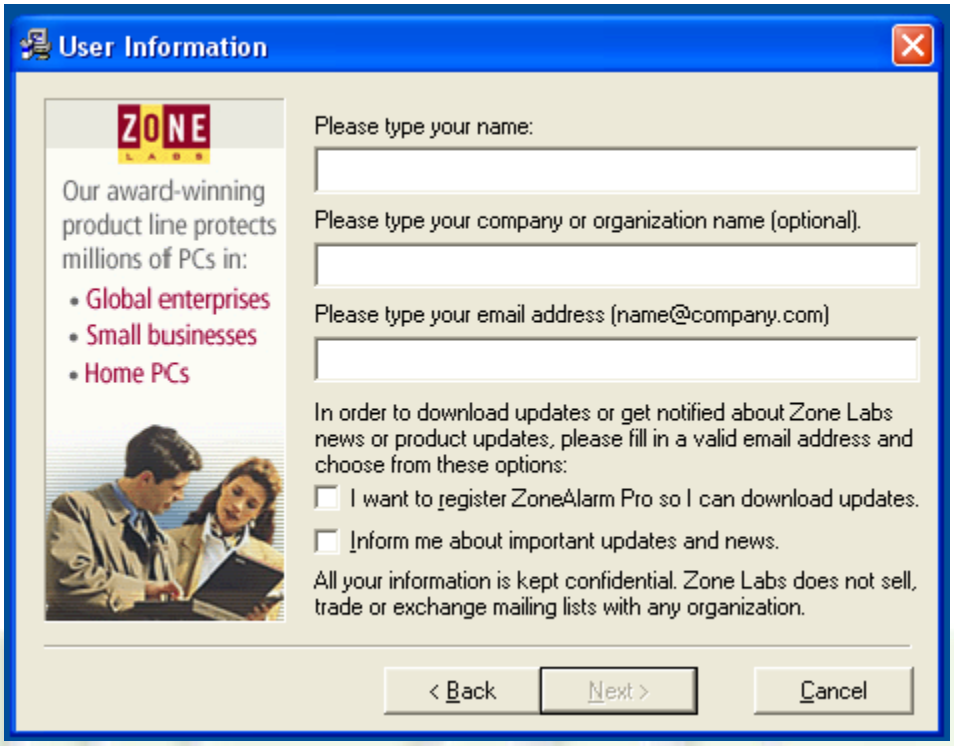
ZoneAlarm comes in three flavors: ZoneAlarm Pro, ZoneAlarm Plus and ZoneAlarm. Trial versions of all three products can be downloaded from Zone Labs web site, which makes the product.

Step 1:

This lab assumes that the ZoneAlarm Pro setup file is stored on a directory on this computer. Have your instructor point you to the appropriate directory to install ZoneAlarm Pro. Double-click the setup icon to begin. You will see the screen shown below.



Click the Next > button to continue. Use the default installation directory. It will bring you to a "registration" screen similar to the one shown on the next page.

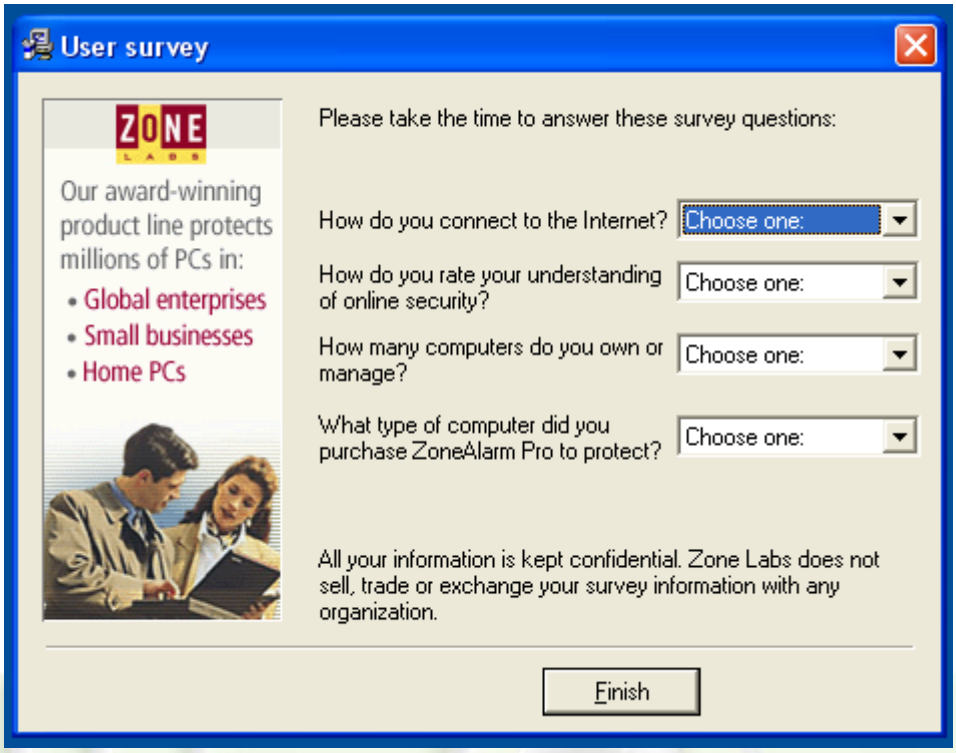


Step 2:

Fill out the registration screen with your name, the Name of your school and your e-mail address. Click Next > to continue. You will see a screen similar to the one shown on the next page.

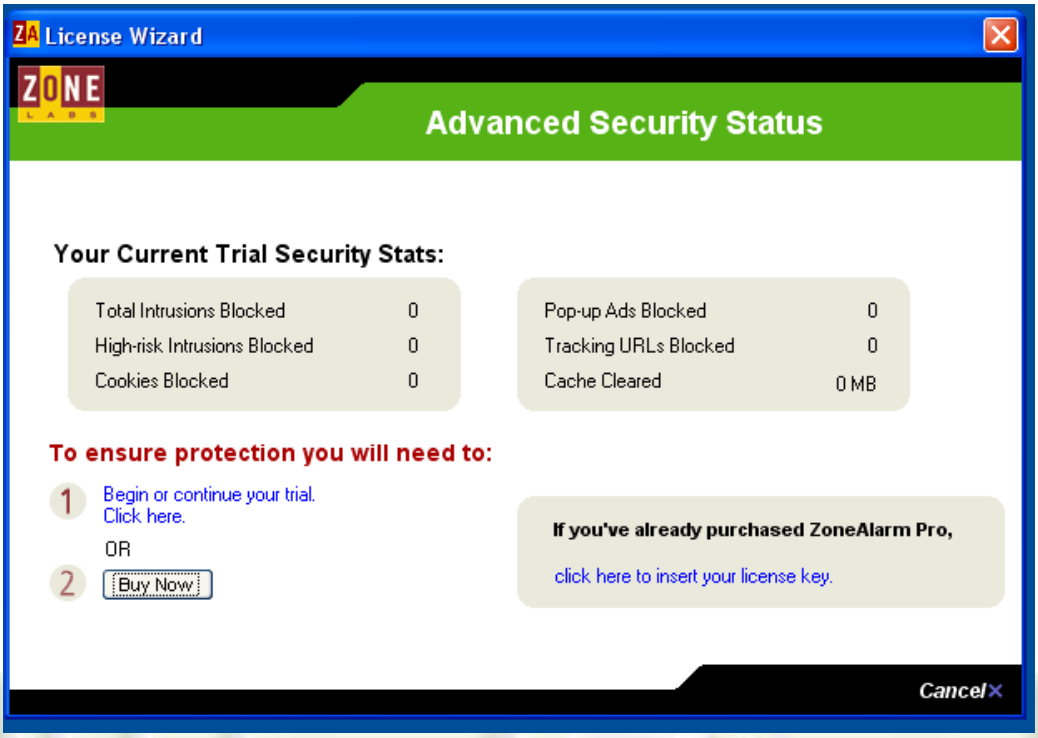
Step3:

Click the Accept terms of agreement box and click Install. Wait a bit (be patient) and then the program will install. At the conclusion of the installation you will see a screen similar to the one shown on the next page.



Step 4:

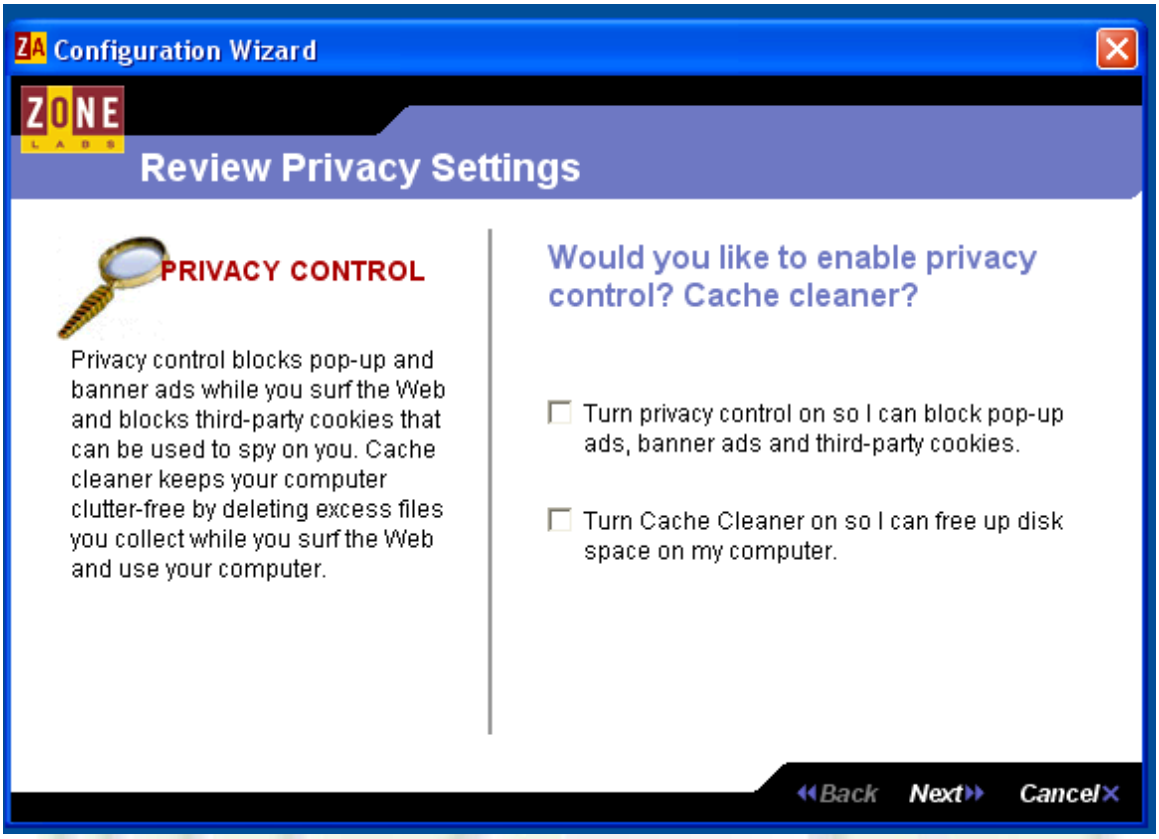
Fill out the survey and click the Finish button. It will then ask if you wish to Run Zone Alarm. Say yes. You will see a screen like the one shown on the next page.



Step 5:

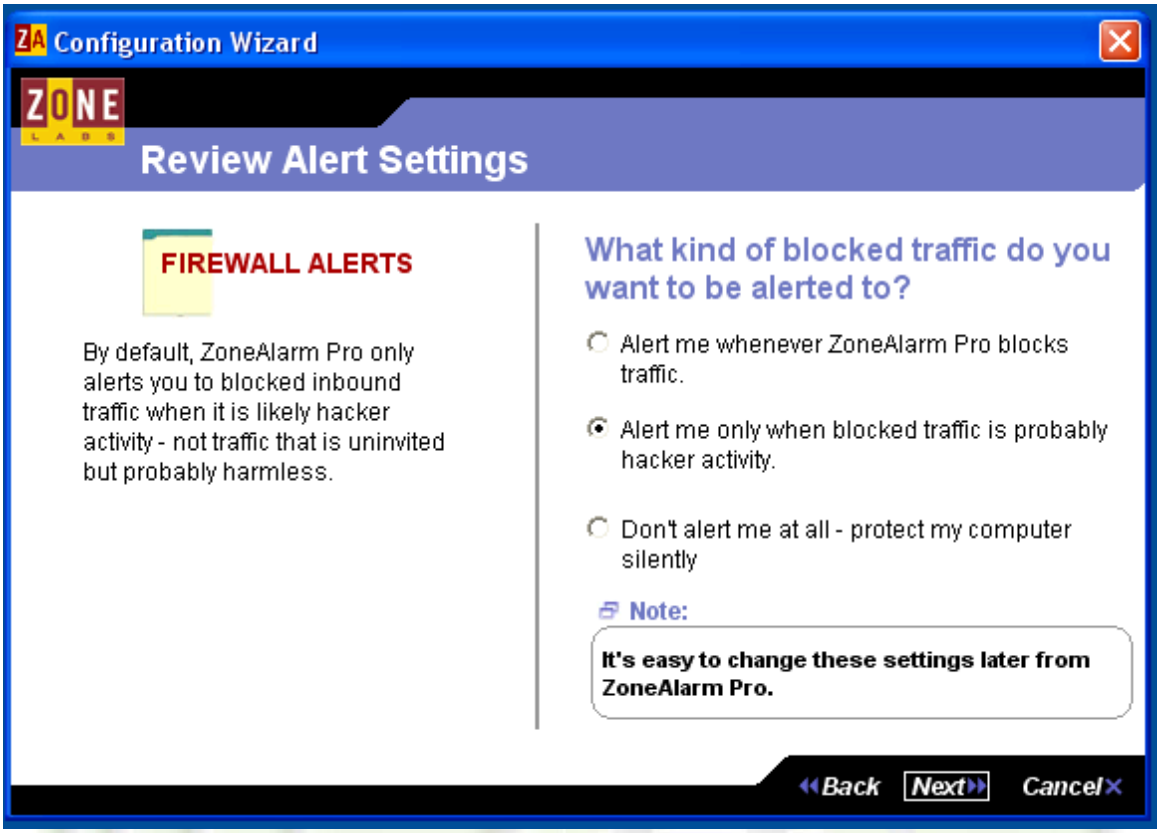
Click on Begin or continue your trial. Click here. After you do this you will see the screen shown below.

Click Next to continue.



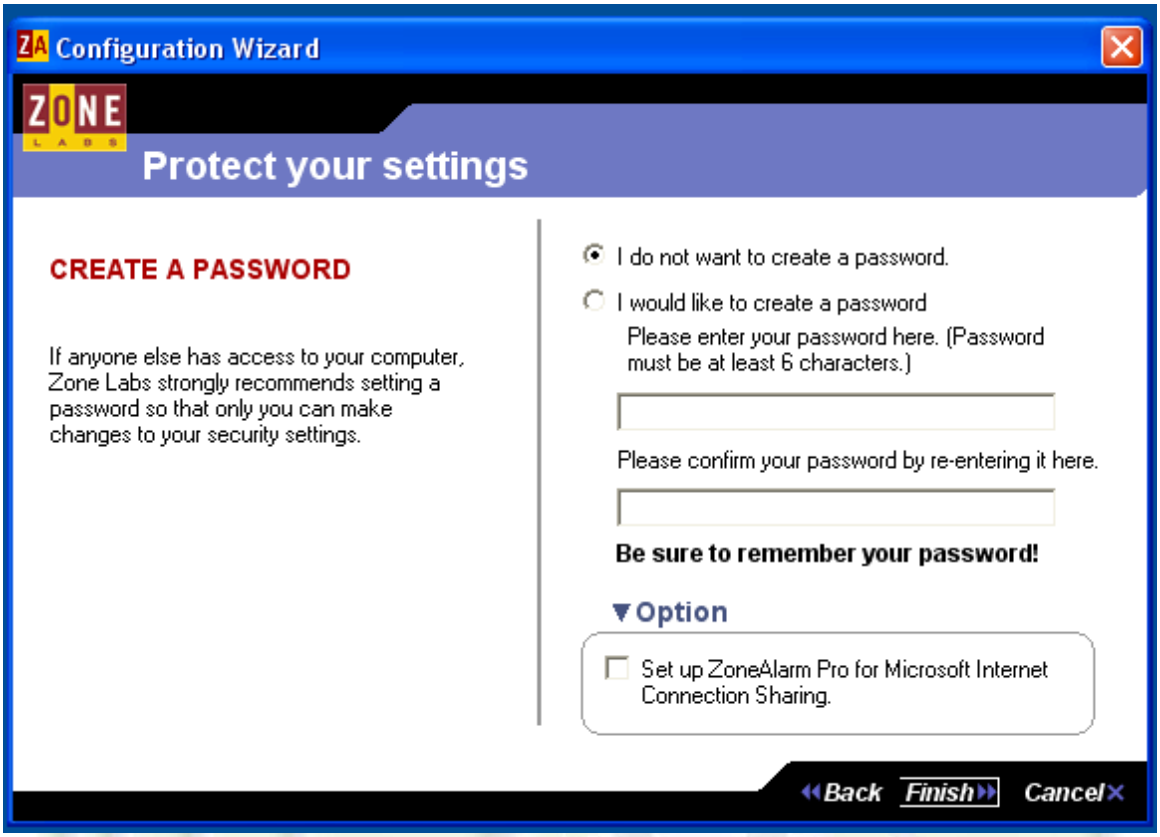
Step 6:

For now, only click the box for Privacy control. Click Next to continue. You will see a screen similar to the one shown on the next page.

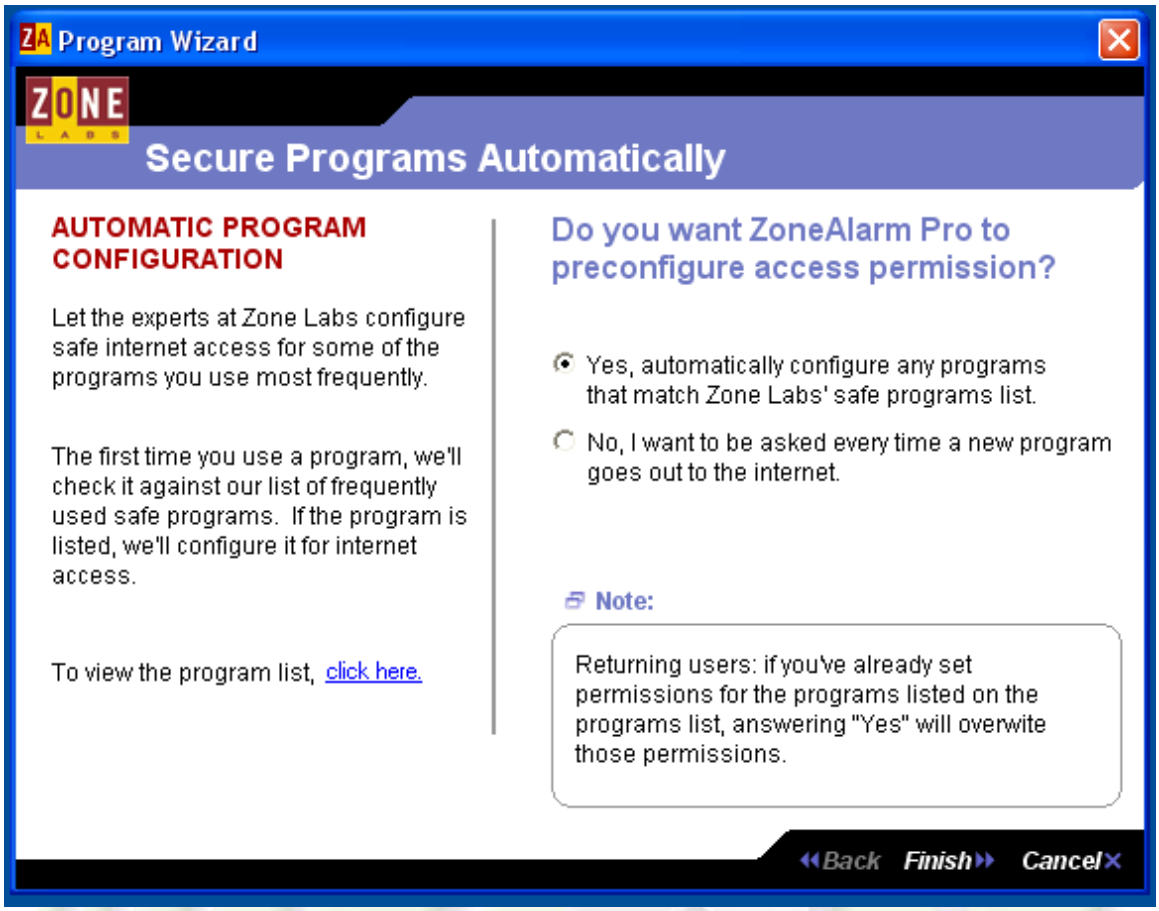


Step 7:

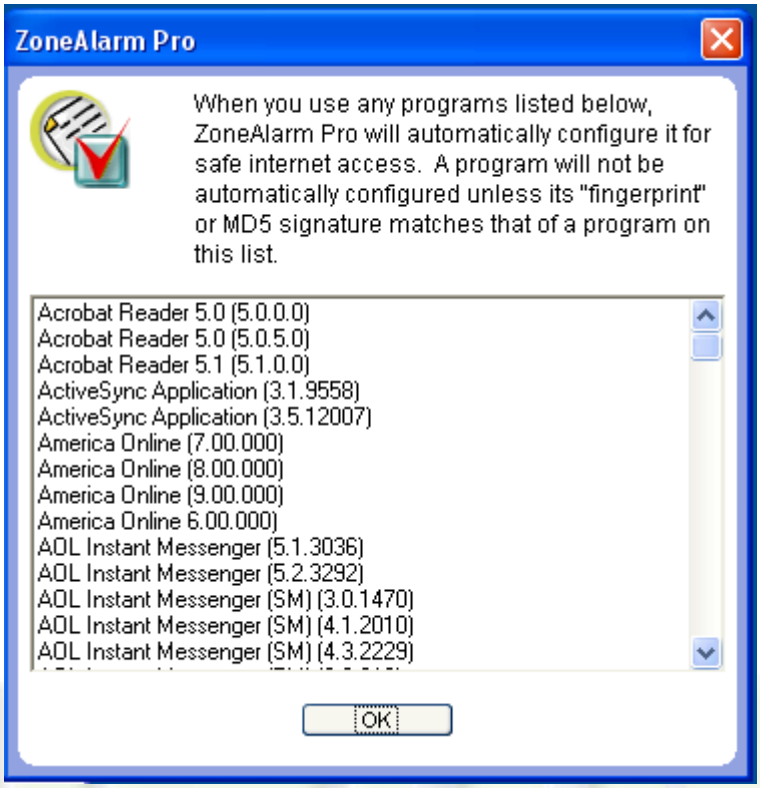
Change the Radio Button setting shown above to Alert me whenever ZoneAlarm Pro blocks traffic. Click Next to continue. You will see a screen similar to the one showing on the next page.



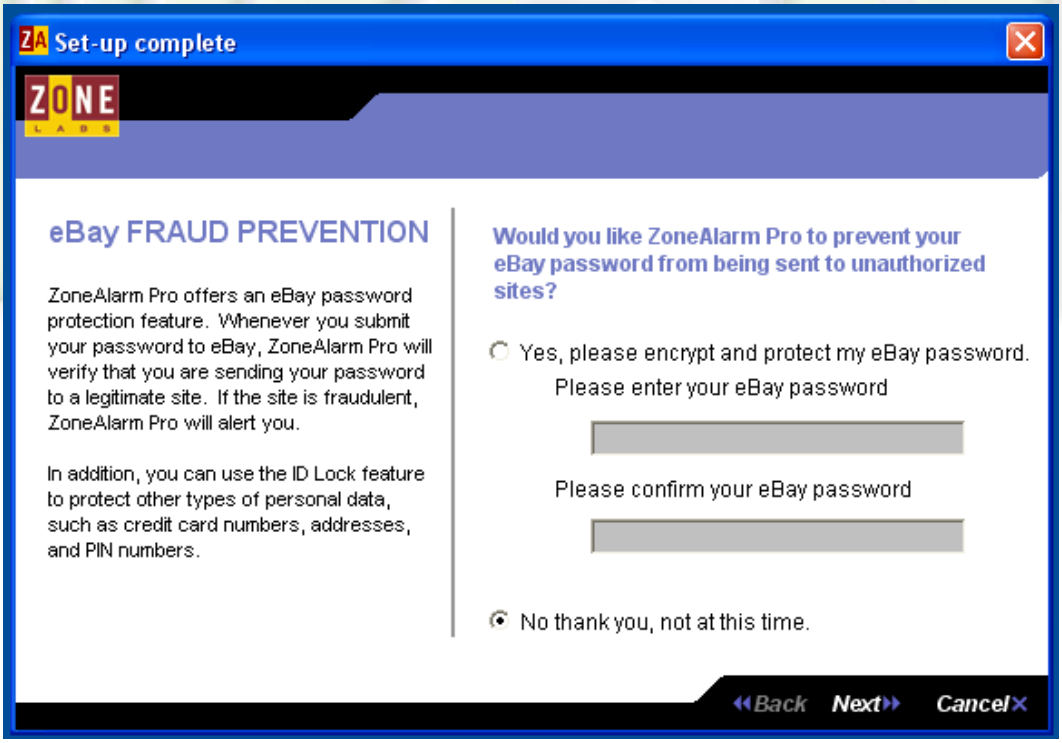
Use the default setting, do not create a password. Click Finish. After quite a while, the screen showing on the next page will appear.



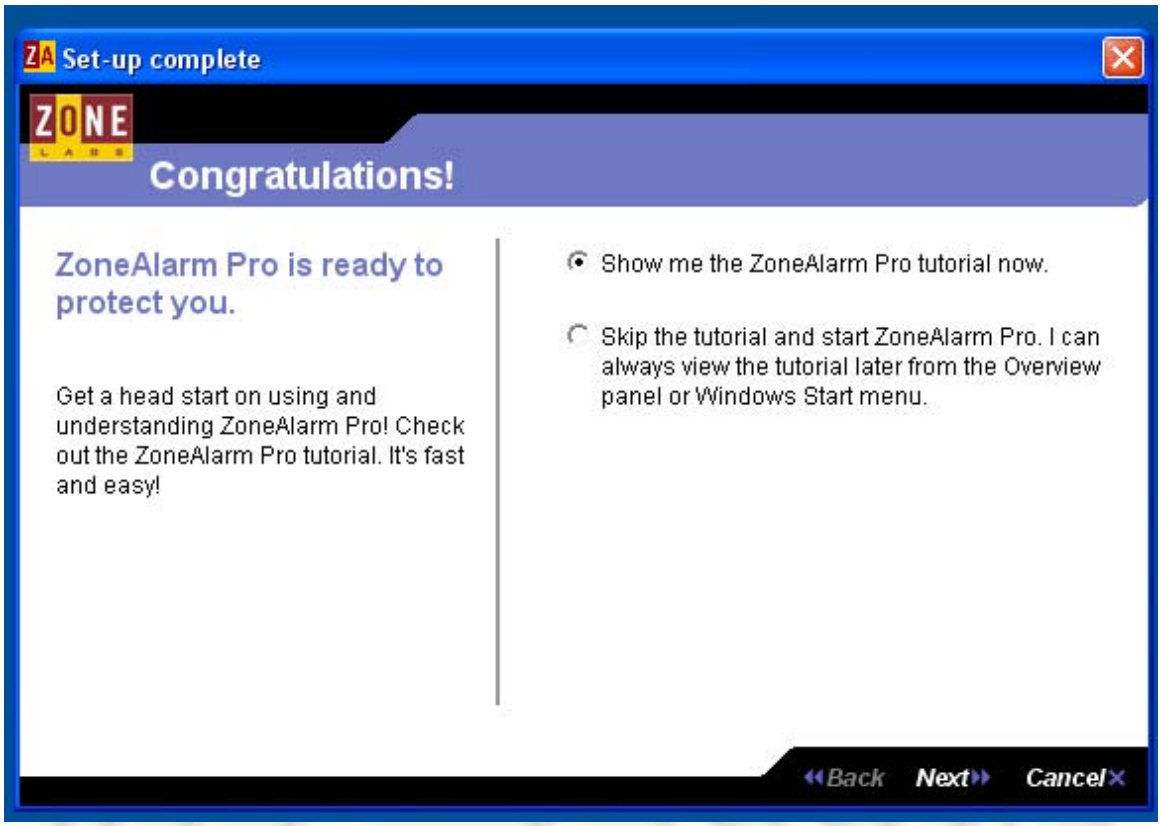
The program list contains well-known programs that are “safe” to access the Internet. Click on the click here link to see a list of them. You will see a list similar to the one shown on the next page.



Click on OK. You will then be shown the screen below.

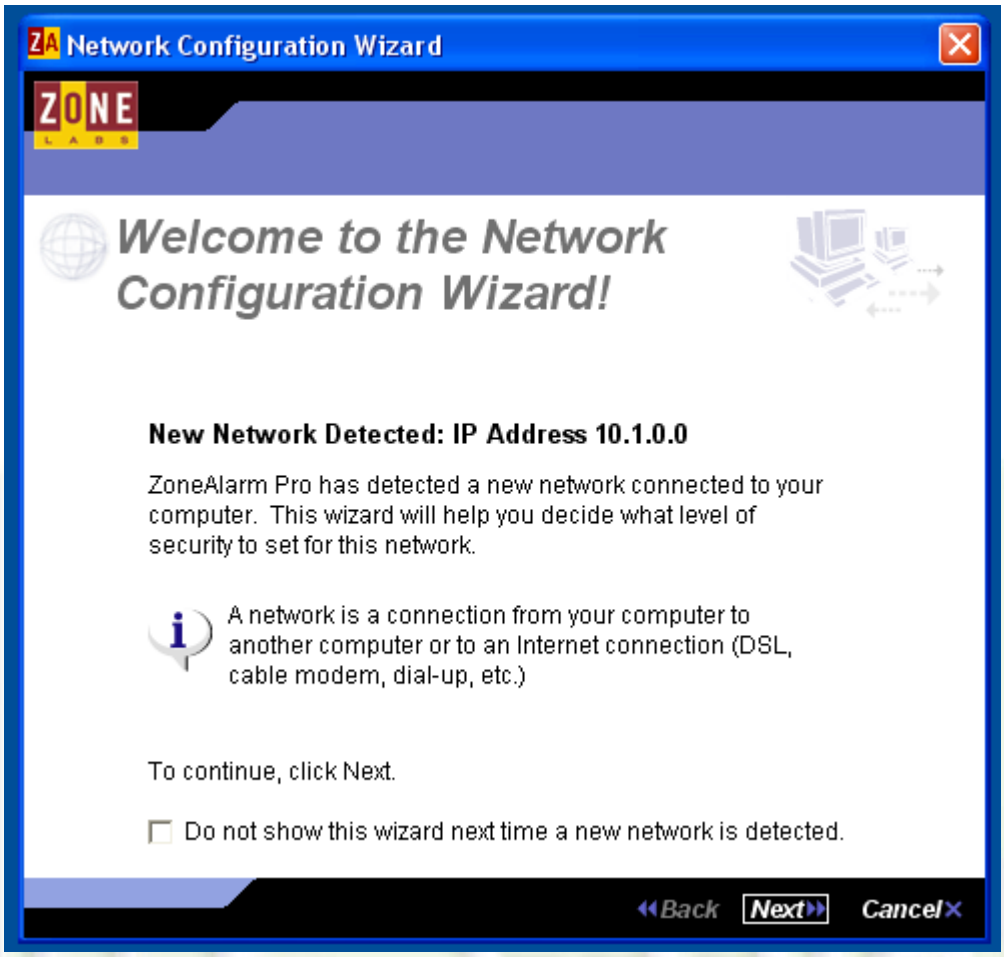


Use the default Radio button (No thank you, not at this time.), and click Next to continue. You will then see the screen shown below.

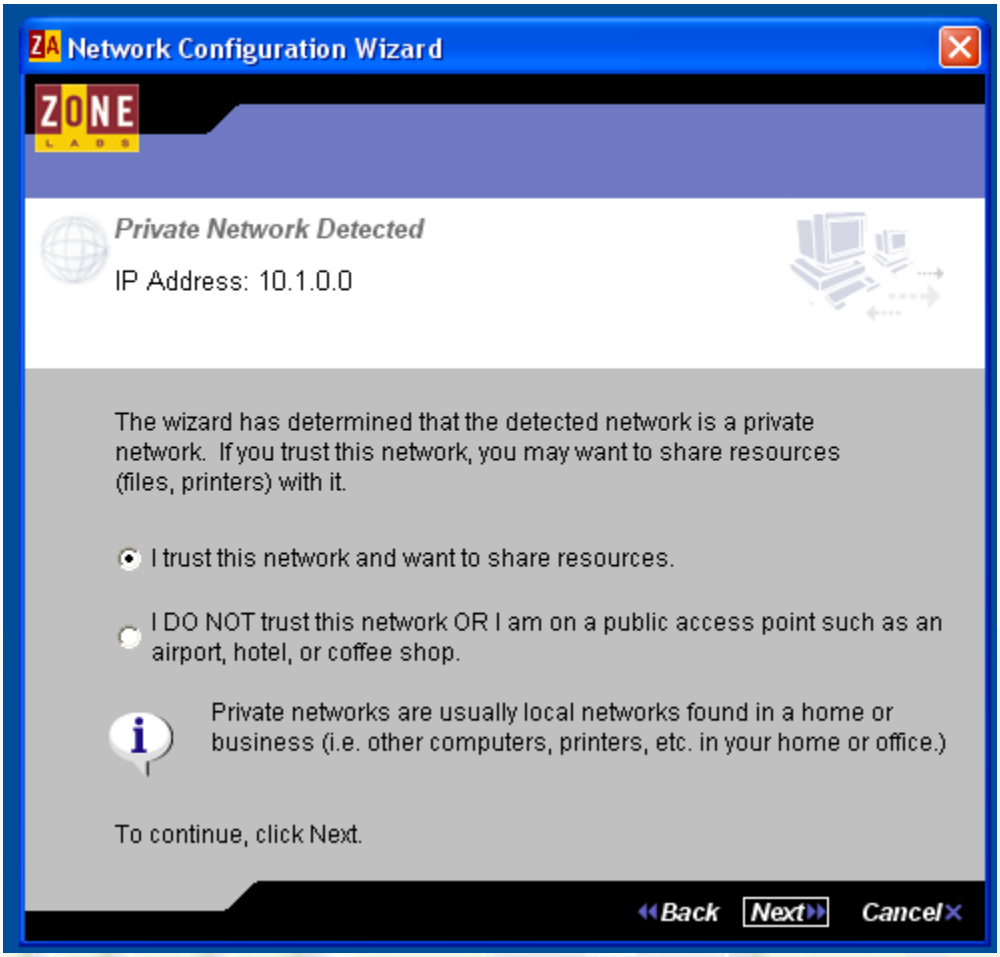


Select the Radio button which skips the tutorial for now and click Next. ZoneAlarm will then bring you to the Network Configuration Wizard.

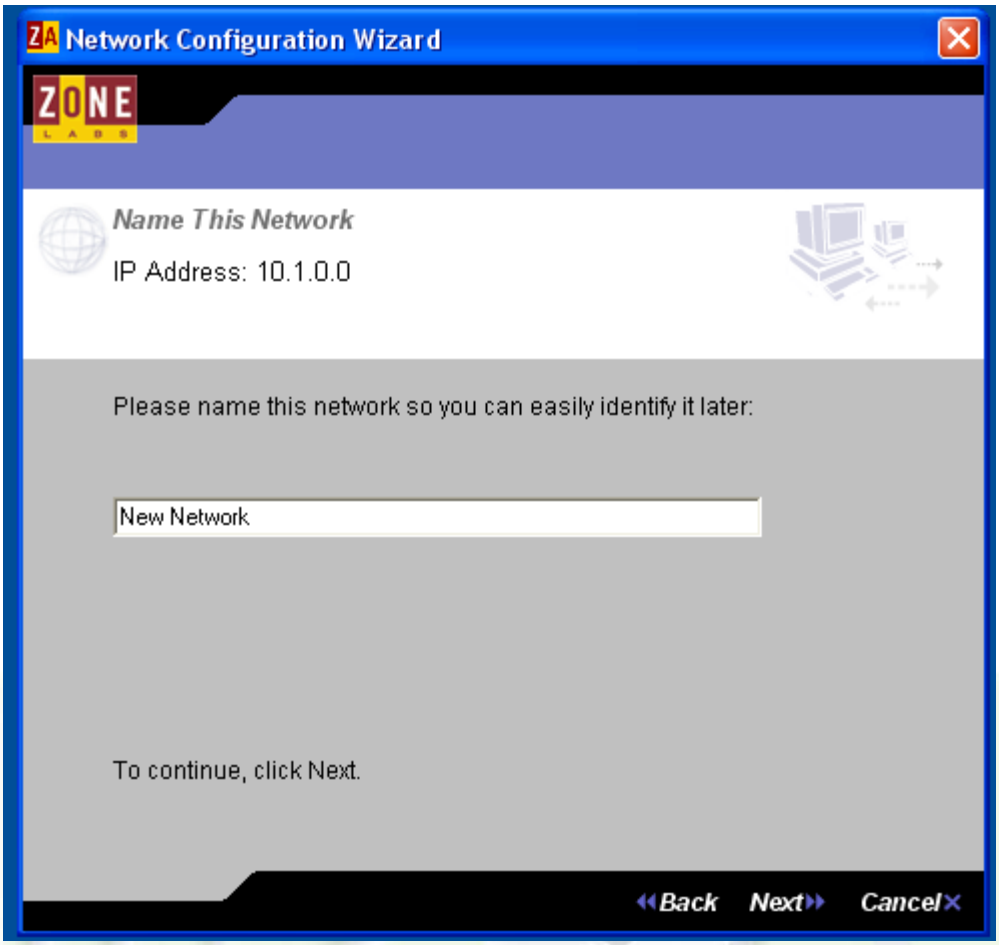
A screen shot of the Network Configuration Wizard is shown below.



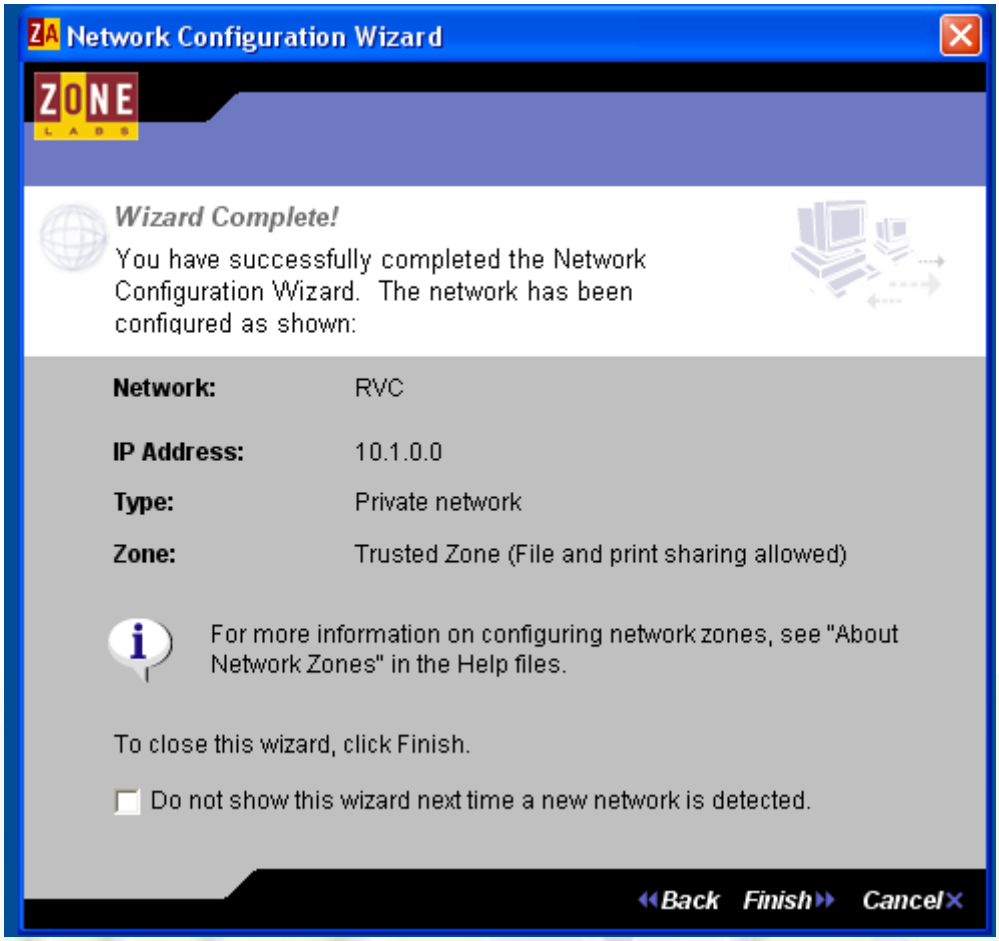
Click Next to continue. Depending upon your network configuration, you will see a screen something like the one shown on the next page.



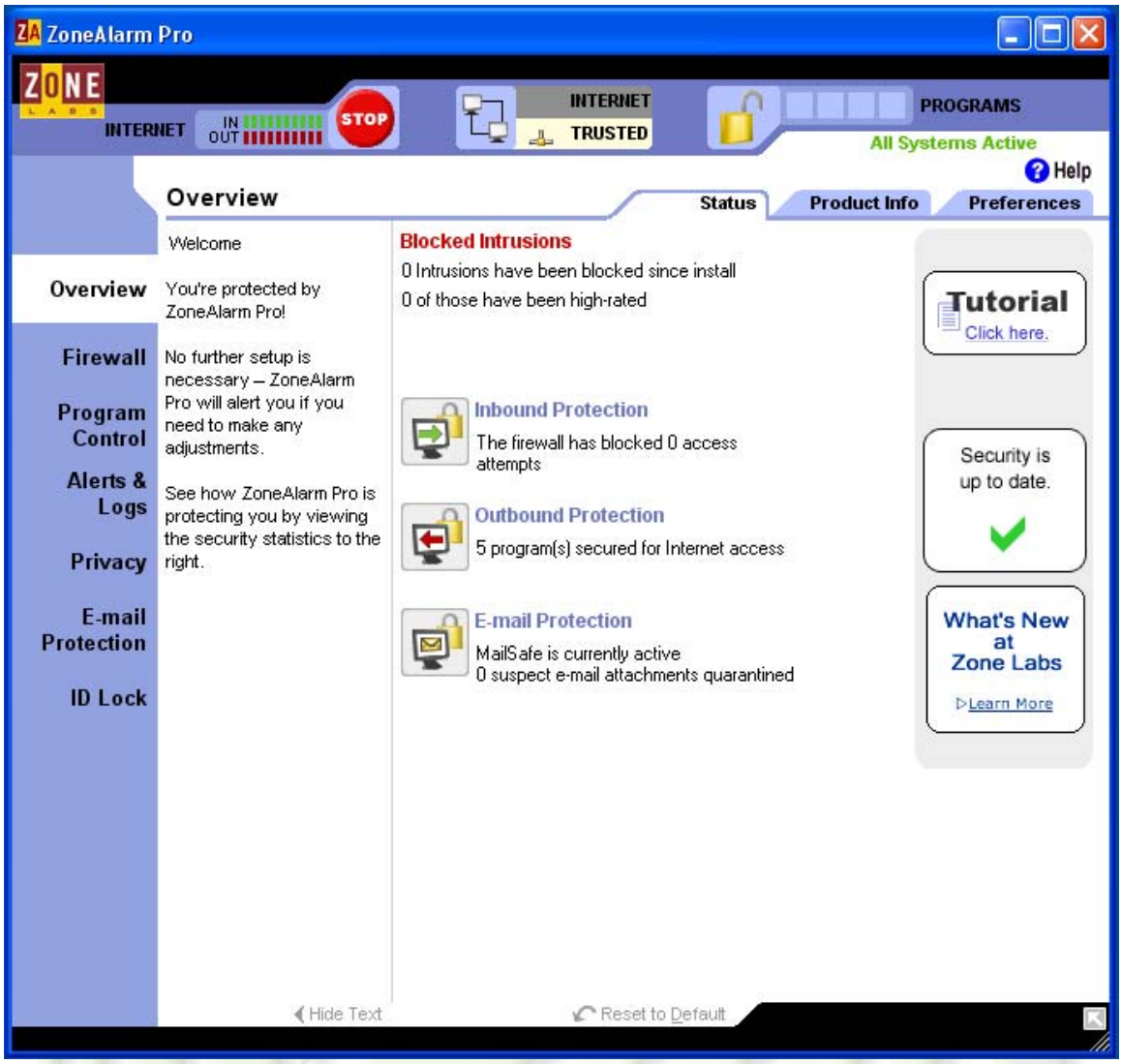
The network shown in this example, 10.1.0.0 is a Private network used internally on a campus LAN. If you were to run this program at home behind a LinkSys router for example, it would show a Private IP network of 192.168.1.0 For this lab, we will trust this network. Make sure the Radio button is on the Trust option and click Next to continue. You will then see a screen similar to the one shown on the next page.



You will want to pick a name for this network. Since this is your internal network, you should probably name it the same as your school name. Highlight the New Network dialog box and put in the name of your school. You will see a screen similar to the one shown on the next page.



Click Finish. You will then be brought to a screen like the one shown on the next page.



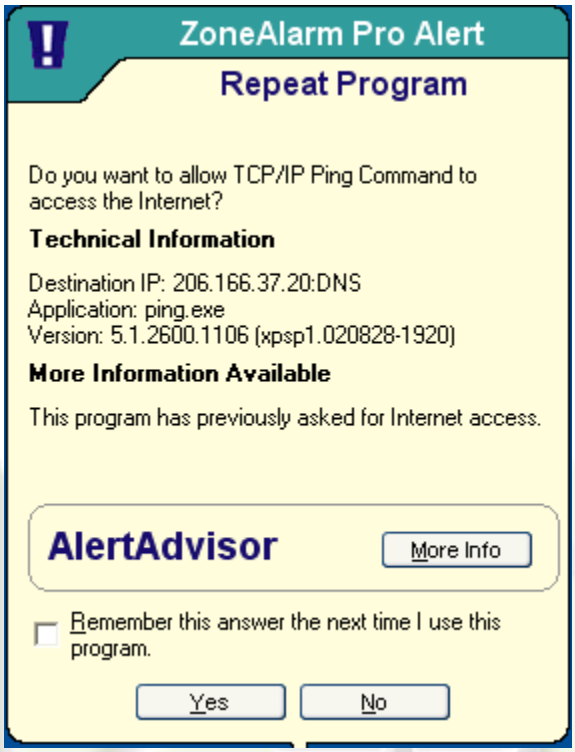
Step 8:

An IDS system typically has both an interactive flavor (immediate notification) as well as a batch-oriented flavor such as log files. You will see both of these demonstrated in this lab.

To demonstrate the interactive nature of ZoneAlarm Pro, we will ping an external web site.

Click on Start, Run, and type in *command* to get to a command prompt.

At the command prompt, type in ping www.google.com and press Enter. You will see a message from ZoneAlarm that looks like the screen shown below.



If you click on the More Info button, it will give you information on what this particular command or program is trying to do. By clicking on the Technical Info tab on the screen shown on the next page, it will give you detailed information on the ping.exe command.

TCP/IP Ping Command is trying to connect to the Internet or your local network

ZoneAlarm Pro is asking you whether to allow the connection. No breach in your security has occurred. **Your computer is safe.**

Inside the program alert

Alert property	Alert property value	Technical explanation
Program Name	TCP/IP Ping Command	A program running on your computer, which either attempted to send an IP packet over the Internet or is waiting for an incoming packet.
Filename	ping.exe	The filename of the program that ZoneAlarm Pro found on your computer.
Program Version	5.1.2600.1106 (xpsp1.020828-1920)	The version of TCP/IP Ping Command running on your computer.
Program Size	16384	The size of the program executable file in bytes.

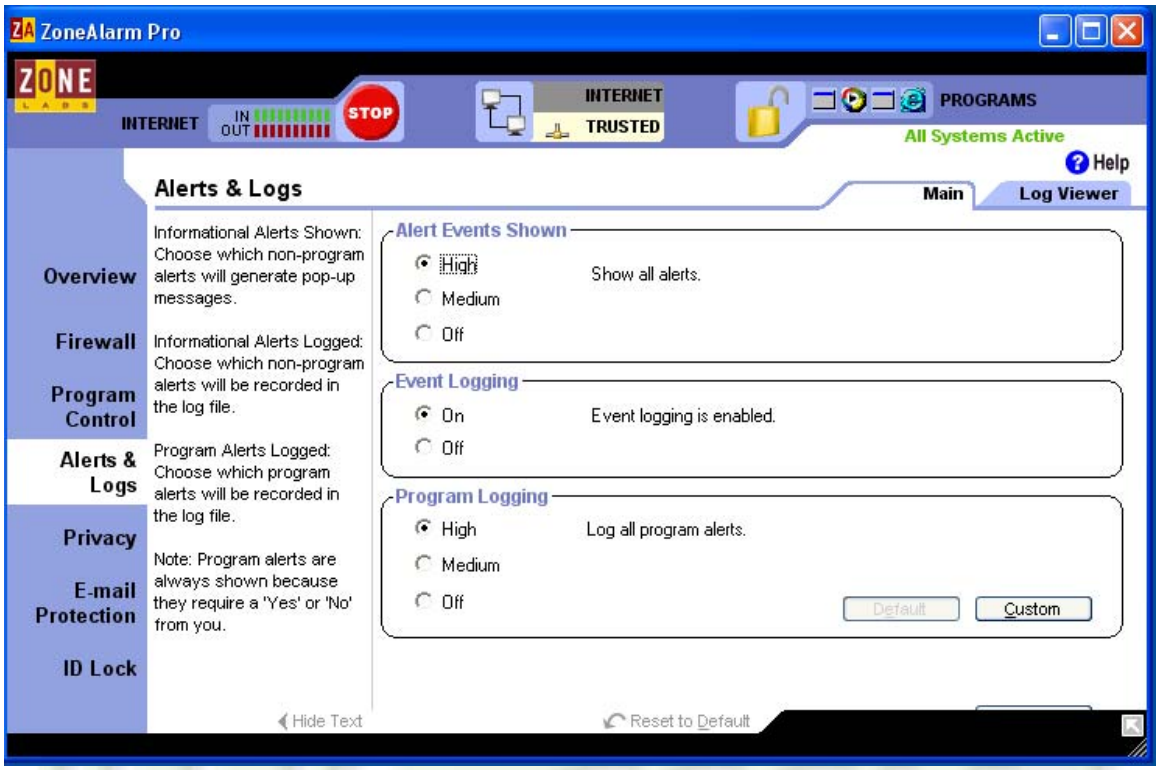
Click on Yes to allow the ping request to go through. ZoneAlarm may bring up another popup which asks if you will allow a DNS request to go through. Click on OK and you should get a reply back from google.

If you have e-mail access, start your email program. ZoneAlarm will ask you if you will allow this program to access the Internet. Click on Yes. ZoneAlarm may then ask another question about accepting a service request. Click Yes.

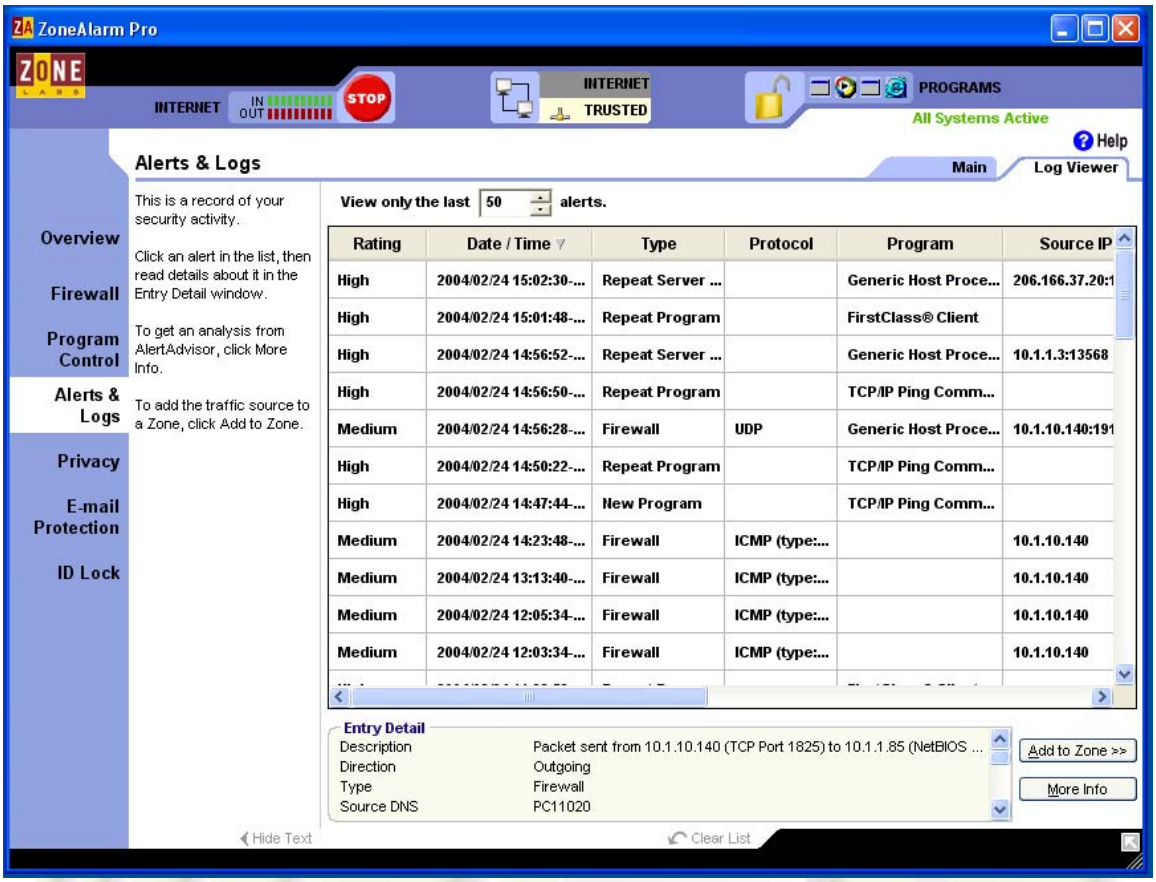
The popup windows for ZoneAlarm are the interactive feedback portion of ZoneAlarm. While interactive is nice because it is immediate, constant interruptions can be disrupting and annoying. Log files can also be created that a network security administrator could then review later instead of in real time.

Step 9:

Let's view the log file to see the activity. You should see an Icon for ZoneAlarm on your taskbar. You can either double-click or right-click and choose Restore ZoneAlarm Control Center. You will see a screen similar to the one shown below.



Click on the Log Viewer Tab. You will see a screen similar to the one shown on the next page.



By clicking on any of the rows, you can see details of each "transaction" and what it was attempting to do.

Analysis

1) For which applications is ZoneAlarm best suited?

2) After working with the ZoneAlarm utility, what features do you feel you should study further? Why?

3) Why should you use a product like this?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Research software with similar functionality such as Norton Internet Security or Snort.

Appendix

This lab was done using Microsoft Windows XP Professional operating system version 2002 Service Pack 2. ZoneAlarm Pro was downloaded from www.zonelabs.com. The lab should be done with PCs connected into an active working LAN and internet connectivity.