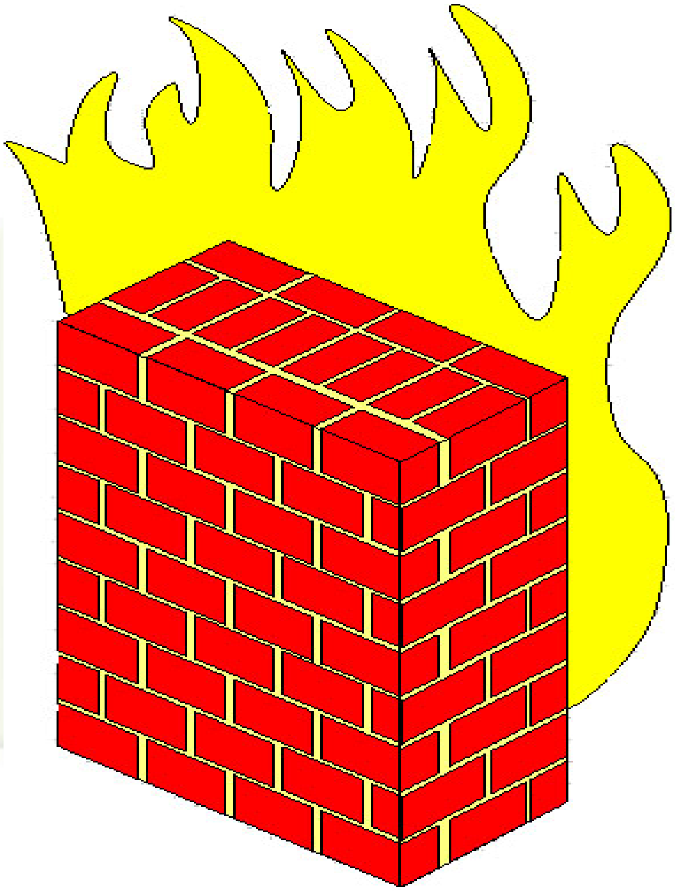
5.3.1

PERSONAL FIREWALLS

(ZoneAlarm Pro)



June 2008

Laboratory Overview

Objective

At the end of this lab students will be able to configure and test a firewall.

Information for Laboratory

A. Students will utilize ZoneAlarm Pro Firewall software

Student Preparation

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

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that ZoneAlarm Pro is installed and working on each student computer.

Estimated Completion Time

60 Minutes

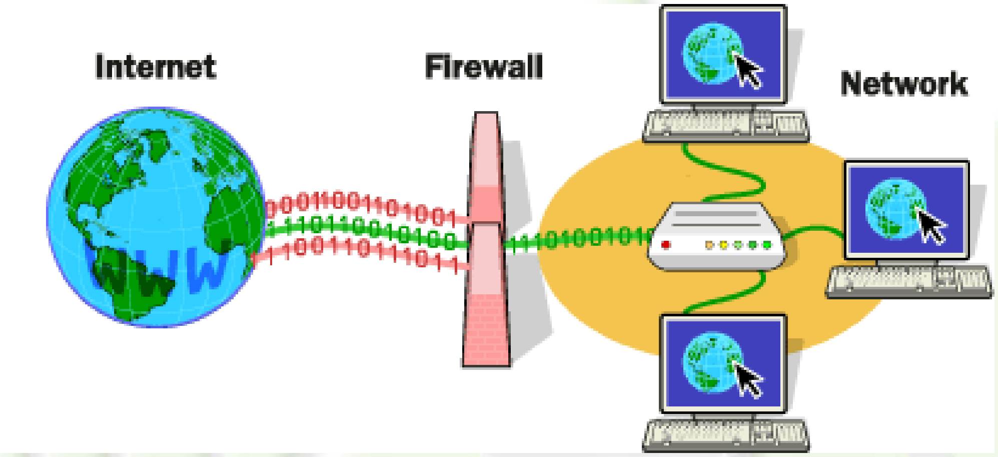
Firewalls

A firewall is simply a program or hardware device that filters data passing into or out of a network. Firewalls use different methods to control traffic flowing in and out of the network:

Packet filtering - Packets (small chunks of data) are analyzed against a set of filters, or rules. Packets that make it through the filters are sent to the requesting system and all others are discarded.

Stateful inspection - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

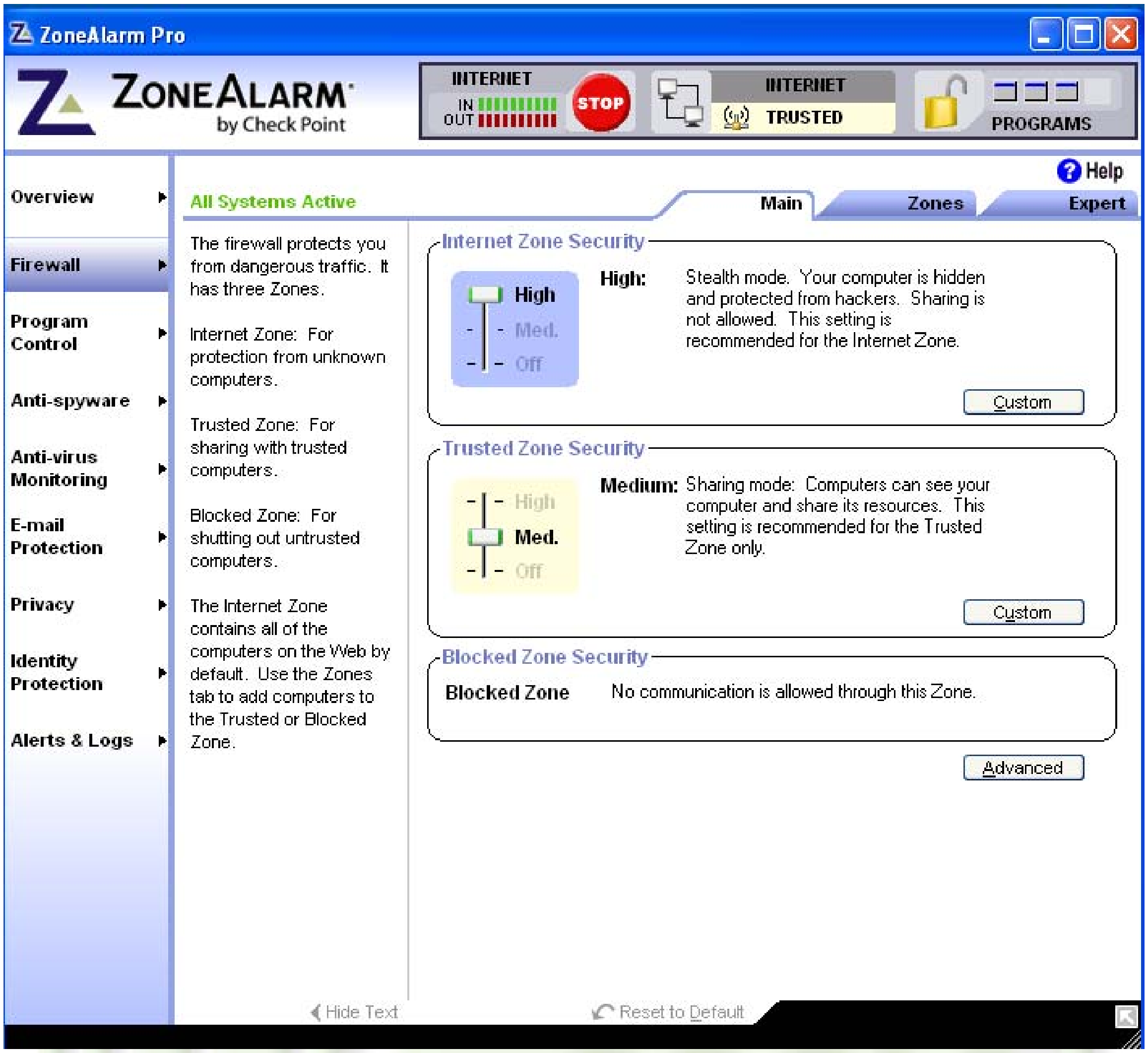
Most firewall configurations are setup to block access from outside or public networks, like the Internet.



Step 1: Basic Configuration of ZoneAlarm Pro

Open ZoneAlarm by double clicking the ZA icon on the taskbar

When open, Click on Firewall on the left side



All Systems Active

The firewall protects you from dangerous traffic. It has three Zones.

Internet Zone: For protection from unknown computers.

Trusted Zone: For sharing with trusted computers.

Blocked Zone: For shutting out untrusted computers.

The Internet Zone contains all of the computers on the Web by default. Use the Zones tab to add computers to the Trusted or Blocked Zone.

Internet Zone Security

High / Med. / Off

High: Stealth mode. Your computer is hidden and protected from hackers. Sharing is not allowed. This setting is recommended for the Internet Zone.

Trusted Zone Security

High / Med. / Off

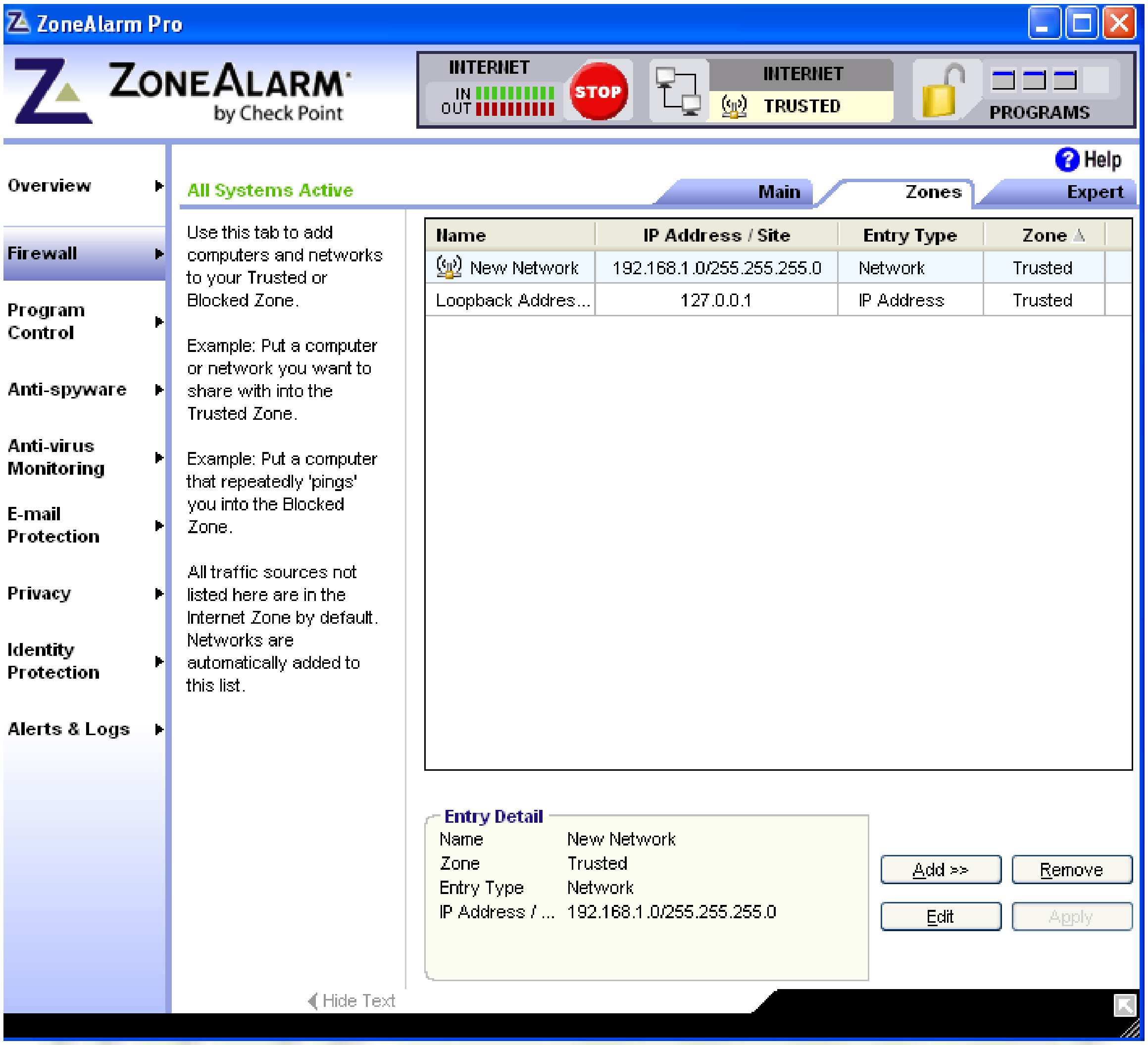
Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone only.

Blocked Zone Security

Blocked Zone No communication is allowed through this Zone.

Click on the Main tab on the top from the firewall menu. Set the Internet Zone Security on High.

Next click on the Zones tab from the firewall menu.



Use this tab to add computers and networks to your Trusted or Blocked Zone.

Example: Put a computer or network you want to share with into the Trusted Zone.

Example: Put a computer that repeatedly 'pings' you into the Blocked Zone.

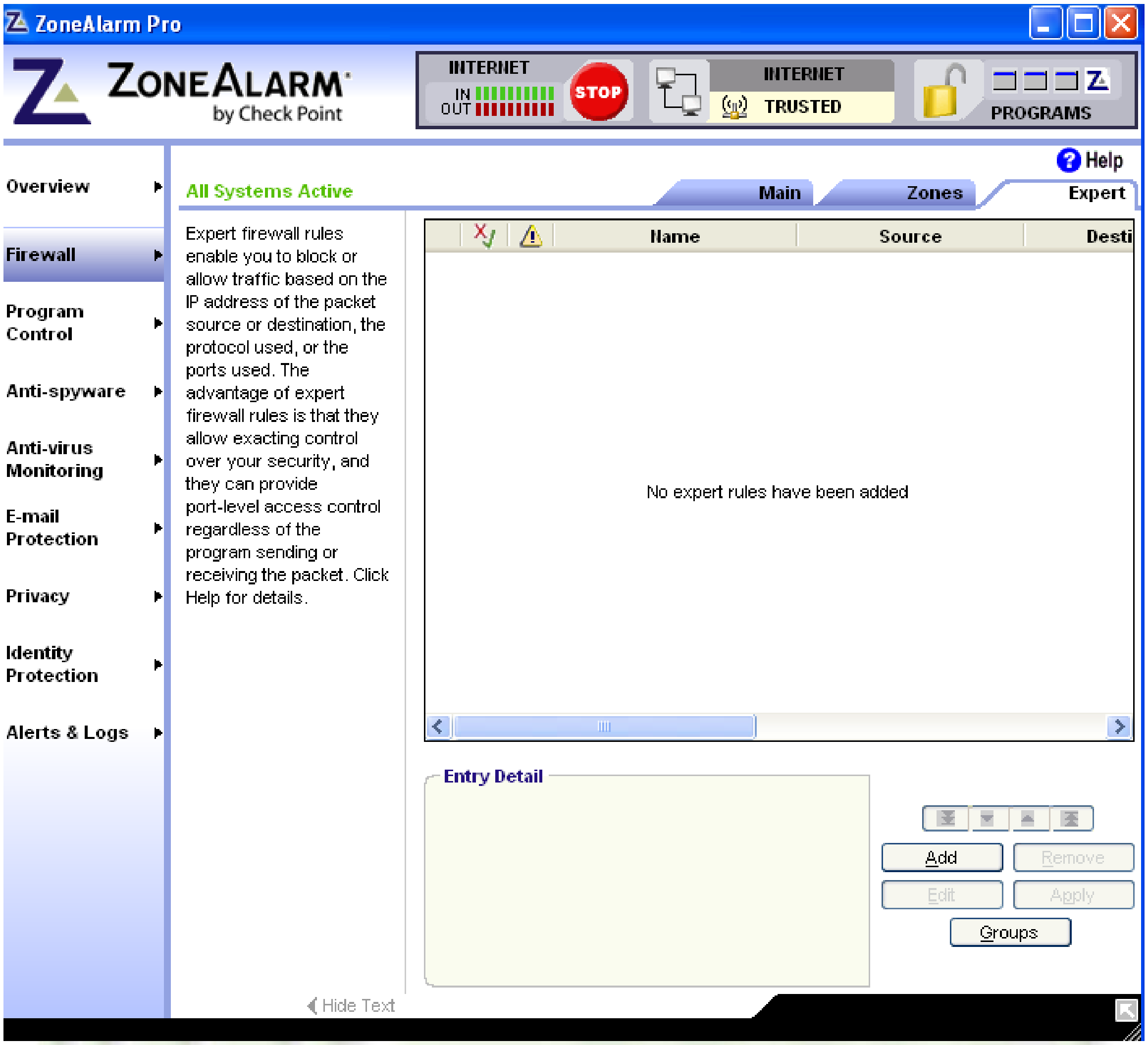
All traffic sources not listed here are in the Internet Zone by default. Networks are automatically added to this list.

Name	IP Address / Site	Entry Type	Zone
New Network	192.168.1.0/255.255.255.0	Network	Trusted
Loopback Addres...	127.0.0.1	IP Address	Trusted

Entry Detail

Name	New Network
Zone	Trusted
Entry Type	Network
IP Address / ...	192.168.1.0/255.255.255.0

Make sure that the local network is listed, and set in the Trusted Zone. Next, click on the expert tab from the firewall menu.

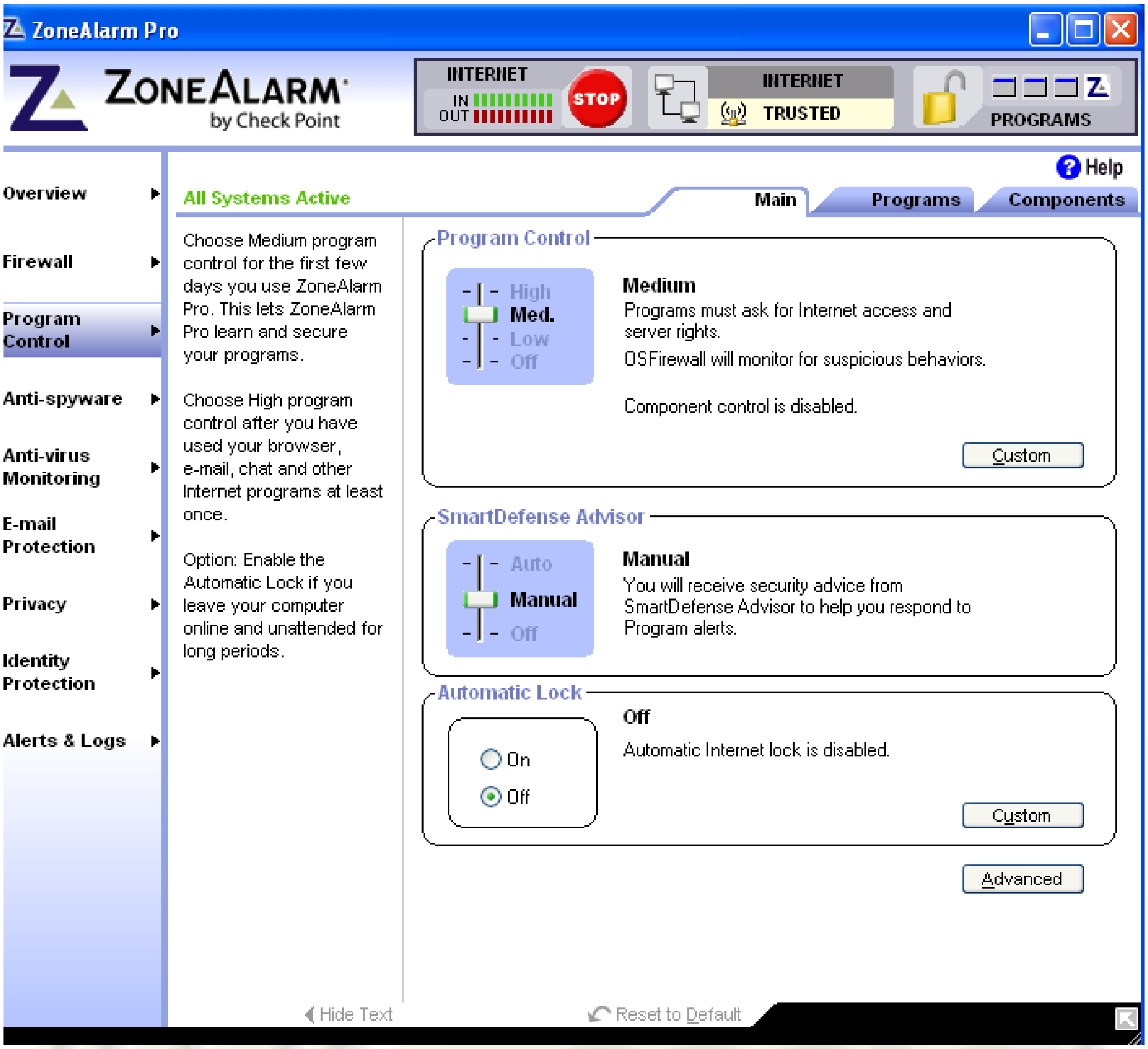


All Systems Active

Expert firewall rules enable you to block or allow traffic based on the IP address of the packet source or destination, the protocol used, or the ports used. The advantage of expert firewall rules is that they allow exacting control over your security, and they can provide port-level access control regardless of the program sending or receiving the packet. Click Help for details.

No expert rules have been added

Make sure that no expert rules have been added. Next, Click on the Program Control menu on the left.



All Systems Active

Choose Medium program control for the first few days you use ZoneAlarm Pro. This lets ZoneAlarm Pro learn and secure your programs.

Choose High program control after you have used your browser, e-mail, chat and other Internet programs at least once.

Option: Enable the Automatic Lock if you leave your computer online and unattended for long periods.

Program Control

Medium
Programs must ask for Internet access and server rights.
OSFirewall will monitor for suspicious behaviors.

Component control is disabled.

SmartDefense Advisor

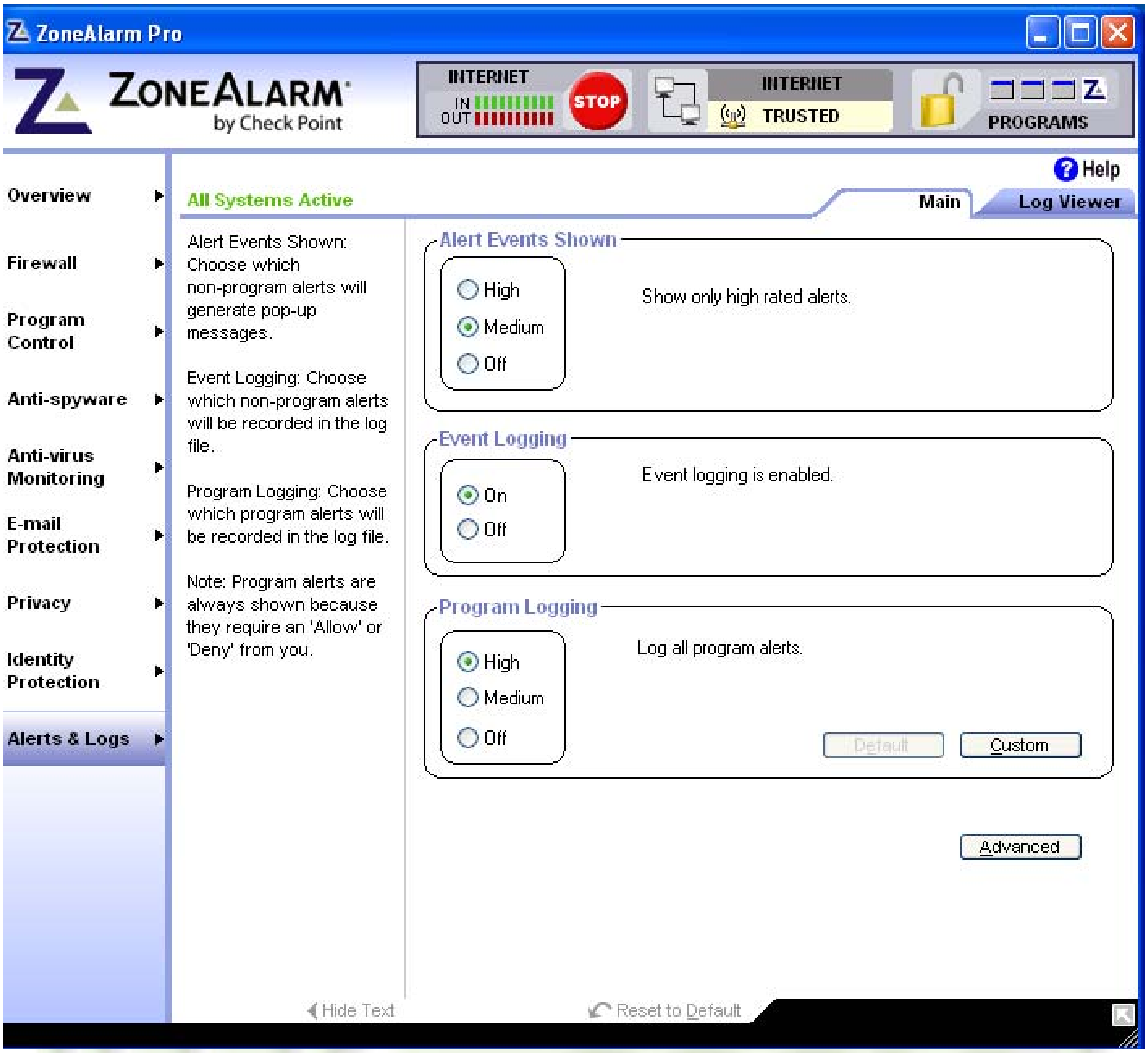
Manual
You will receive security advice from SmartDefense Advisor to help you respond to Program alerts.

Automatic Lock

○ On
● Off

Off
Automatic Internet lock is disabled.

Set the Program Control to OFF. Next, click on the Alerts & Logs menu on the left.



All Systems Active

Alert Events Shown: Choose which non-program alerts will generate pop-up messages.

Event Logging: Choose which non-program alerts will be recorded in the log file.

Program Logging: Choose which program alerts will be recorded in the log file.

Note: Program alerts are always shown because they require an 'Allow' or 'Deny' from you.

Alert Events Shown

○ High
● Medium
○ Off

Show only high rated alerts.

Event Logging

● On
○ Off

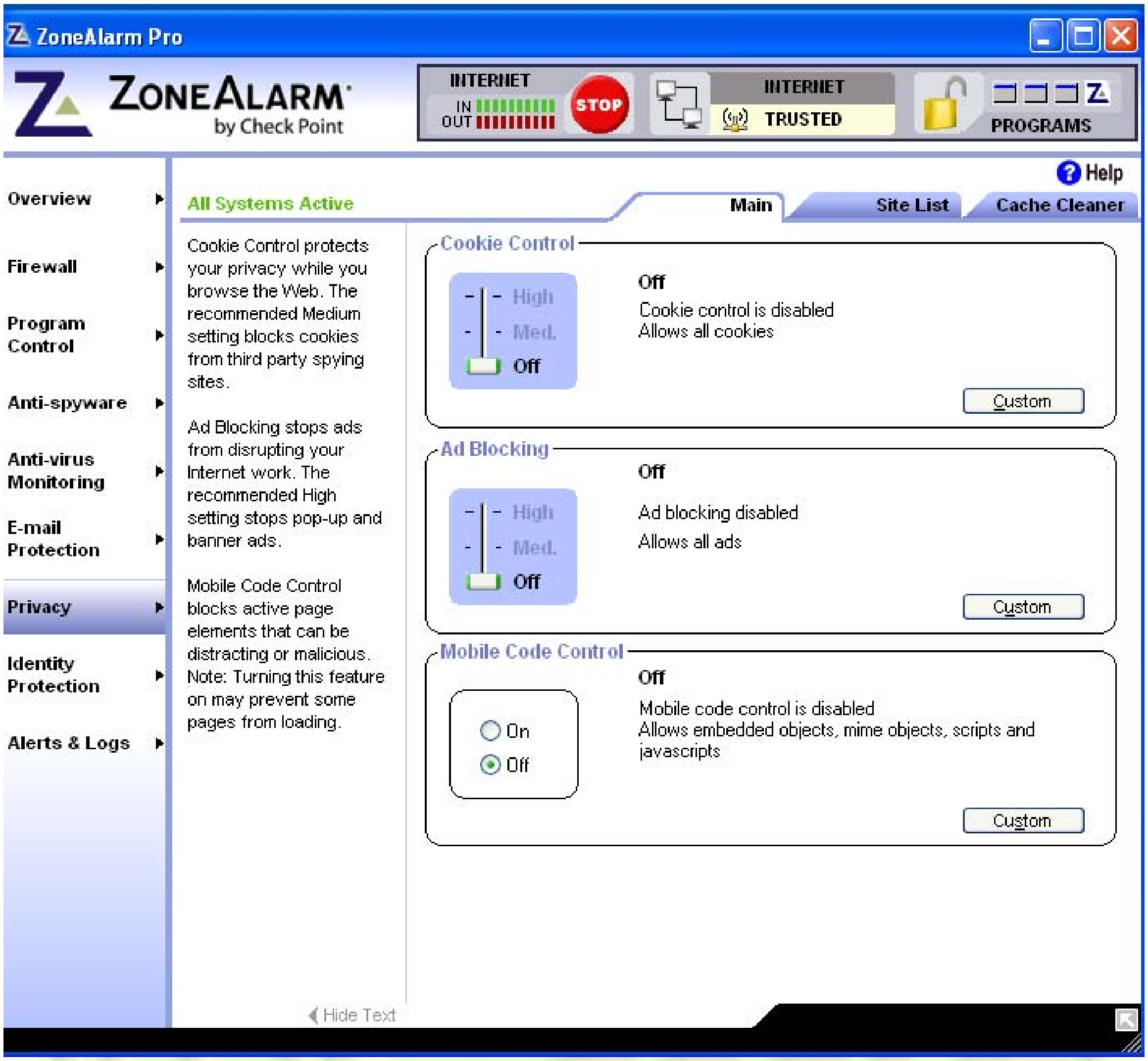
Event logging is enabled.

Program Logging

● High
○ Medium
○ Off

Log all program alerts.

Set Alert Events Shown, Event Logging, and Program Logging to OFF. Next, click on the Privacy menu on the left.



All Systems Active

Cookie Control protects your privacy while you browse the Web. The recommended Medium setting blocks cookies from third party spying sites.

Ad Blocking stops ads from disrupting your Internet work. The recommended High setting stops pop-up and banner ads.

Mobile Code Control blocks active page elements that can be distracting or malicious. Note: Turning this feature on may prevent some pages from loading.

Cookie Control

High / Med. / Off

Off
Cookie control is disabled
Allows all cookies

Custom

Ad Blocking

High / Med. / Off

Off

Ad blocking disabled

Allows all ads

Custom

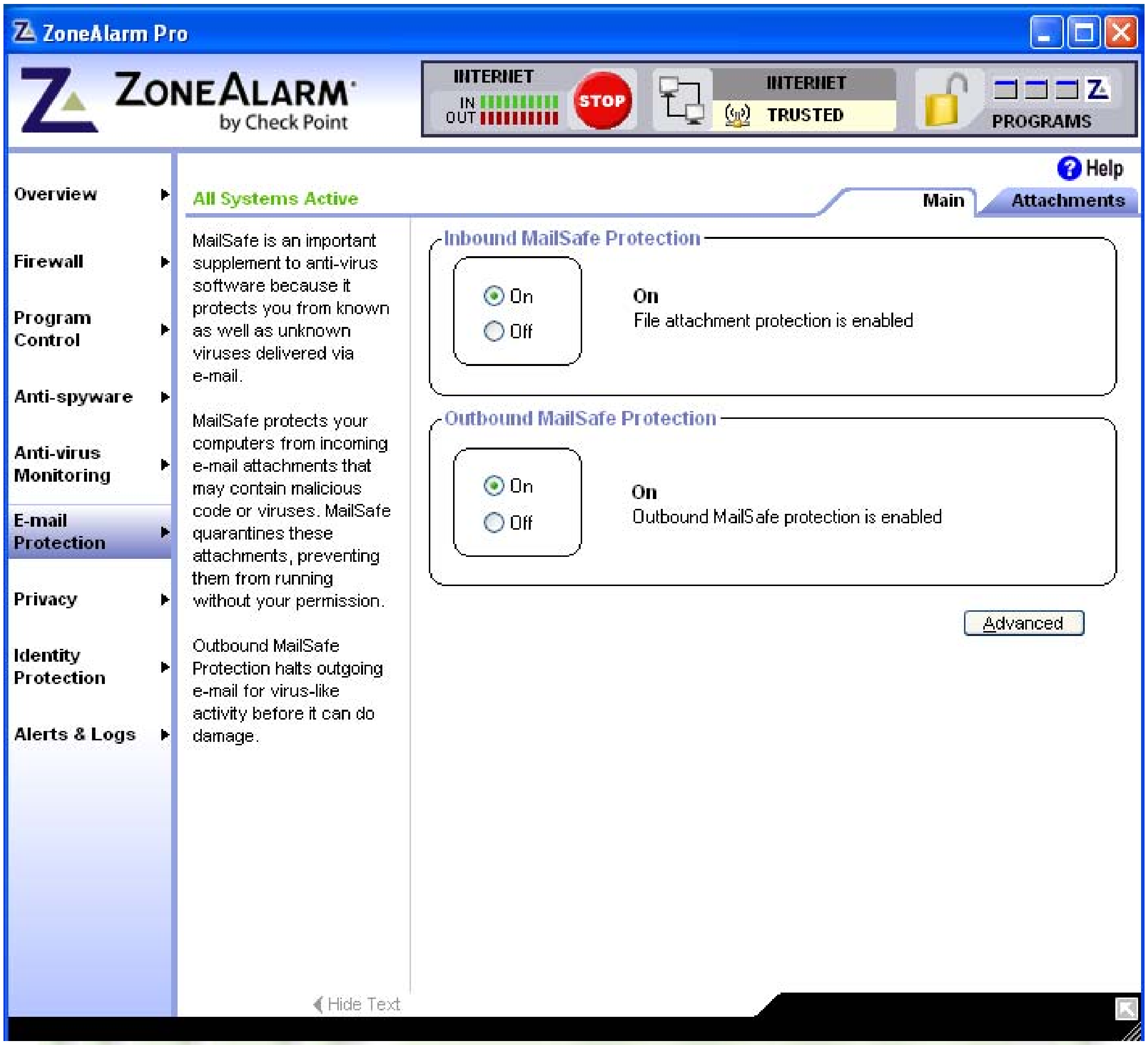
Mobile Code Control

○ On
● Off

Off
Mobile code control is disabled
Allows embedded objects, mime objects, scripts and javascripts

Custom

Set Cookie Control, Ad Blocking, and Mobile Code Control to OFF. Next, click on the E-mail Protection menu on the left.



All Systems Active

MailSafe is an important supplement to anti-virus software because it protects you from known as well as unknown viruses delivered via e-mail.

MailSafe protects your computers from incoming e-mail attachments that may contain malicious code or viruses. MailSafe quarantines these attachments, preventing them from running without your permission.

Outbound MailSafe Protection halts outgoing e-mail for virus-like activity before it can do damage.

Inbound MailSafe Protection

● On
○ Off

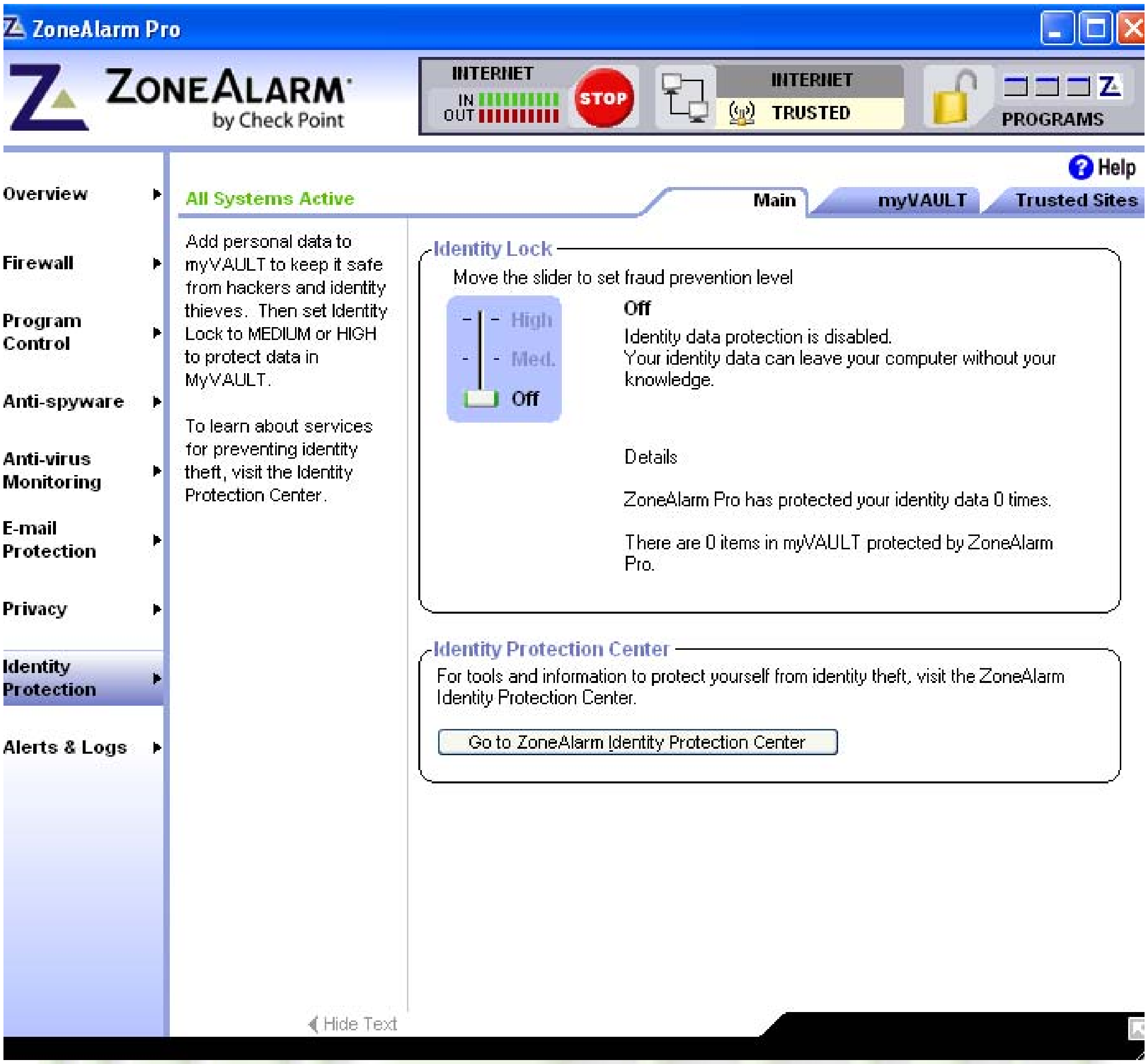
On
File attachment protection is enabled

Outbound MailSafe Protection

● On
○ Off

On
Outbound MailSafe protection is enabled

Set Inbound and Outbound MailSafe Protection to OFF. Next, click the Identity Protection on the left.



Add personal data to myVAULT to keep it safe from hackers and identity thieves. Then set Identity Lock to MEDIUM or HIGH to protect data in MyVAULT.

To learn about services for preventing identity theft, visit the Identity Protection Center.

Identity Lock

Move the slider to set fraud prevention level

High

Med.

Off

Off

Identity data protection is disabled.
Your identity data can leave your computer without your knowledge.

Details

ZoneAlarm Pro has protected your identity data 0 times.

There are 0 items in myVAULT protected by ZoneAlarm Pro.

Identity Protection Center

For tools and information to protect yourself from identity theft, visit the ZoneAlarm Identity Protection Center.

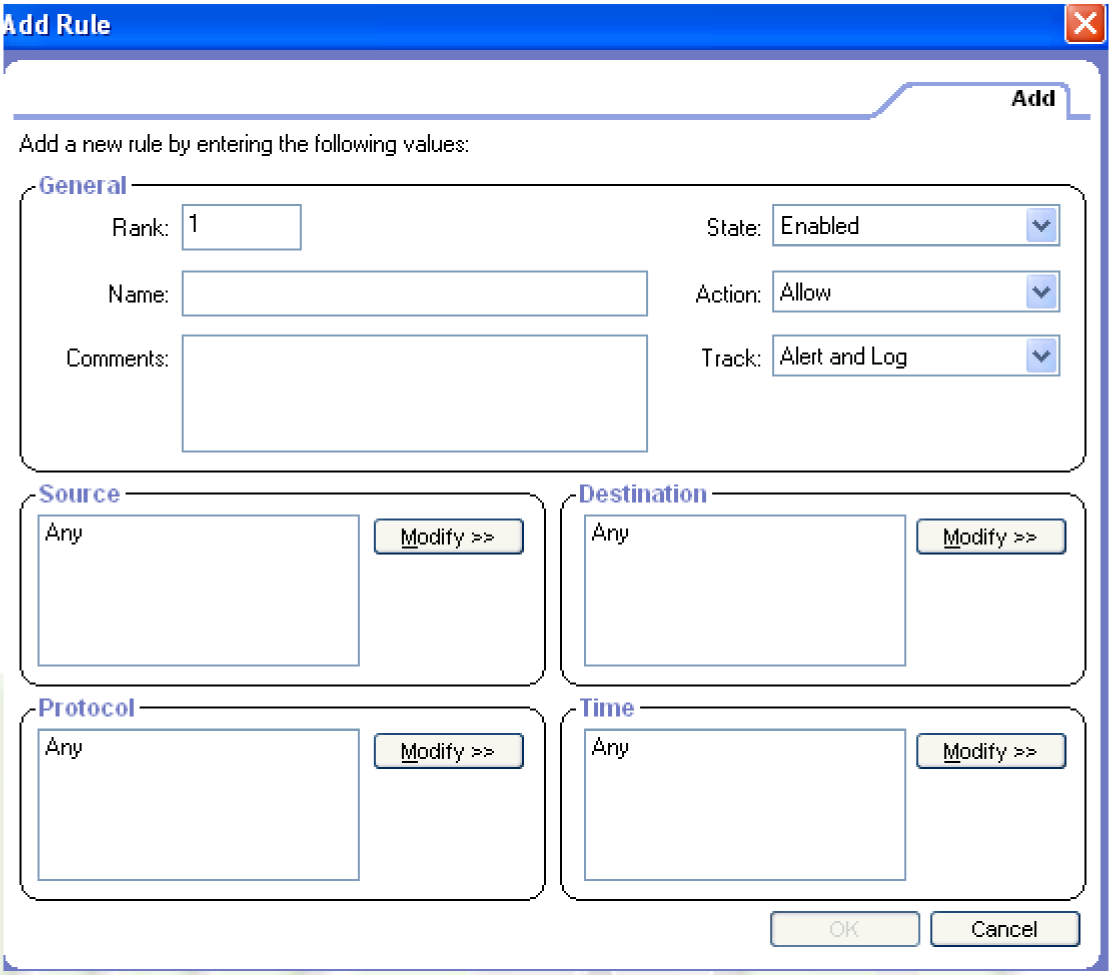
Go to ZoneAlarm Identity Protection Center

Set ID Lock to OFF.

STEP 2: Blocking web traffic

Open Internet Explorer, and make sure that your web access is working properly. You should be able to navigate to any web page, such as www.yahoo.com or www.google.com as a test.

Once you have verified that web access is working, From the Firewall menu, Click on Expert, and click Add on the bottom right. See sample screen shot below



Add a new rule by entering the following values:

General

Rank: 1
Name:
Comments:
State: Enabled
Action: Allow
Track: Alert and Log

Source: Any

Destination: Any

Protocol: Any

Time: Any

In the General Box, set the following…

Rank:	1
Name:	Block HTTP
State:	Enabled
Action:	Block
Track:	None

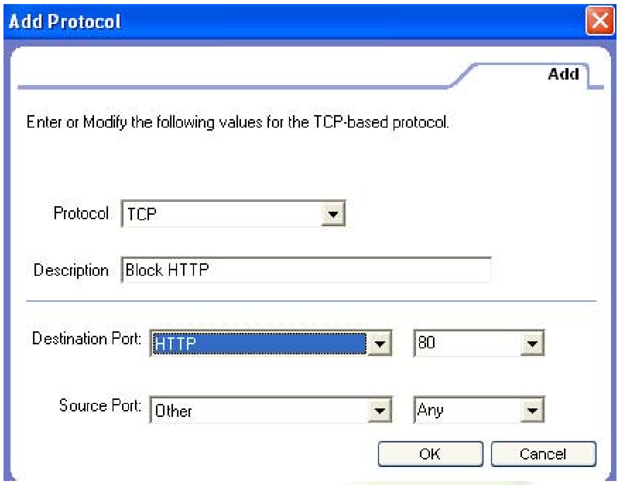
In the Source, Destination, and Time Boxes, leave the default setting ANY.

In the Protocol box, click Modify, add protocol, and add protocol.

Configure as below…

Protocol: TCP

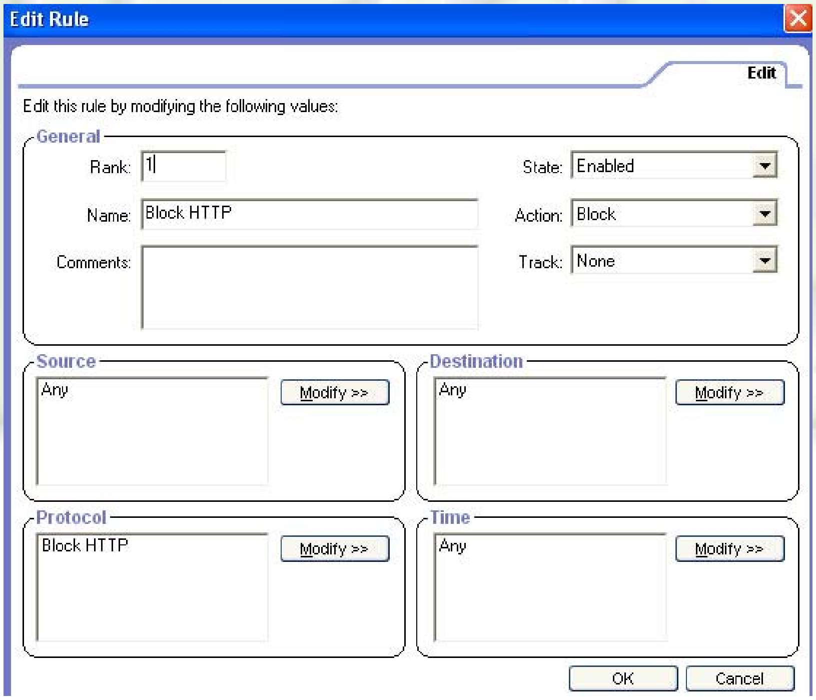
Description: Block HTTP
Destination Port: HTTP: 80
Source Port: Other: Any



Enter or Modify the following values for the TCP-based protocol.

Protocol: TCP
Description: Block HTTP
Destination Port: HTTP 80
Source Port: Other Any

Compare your rule as below…

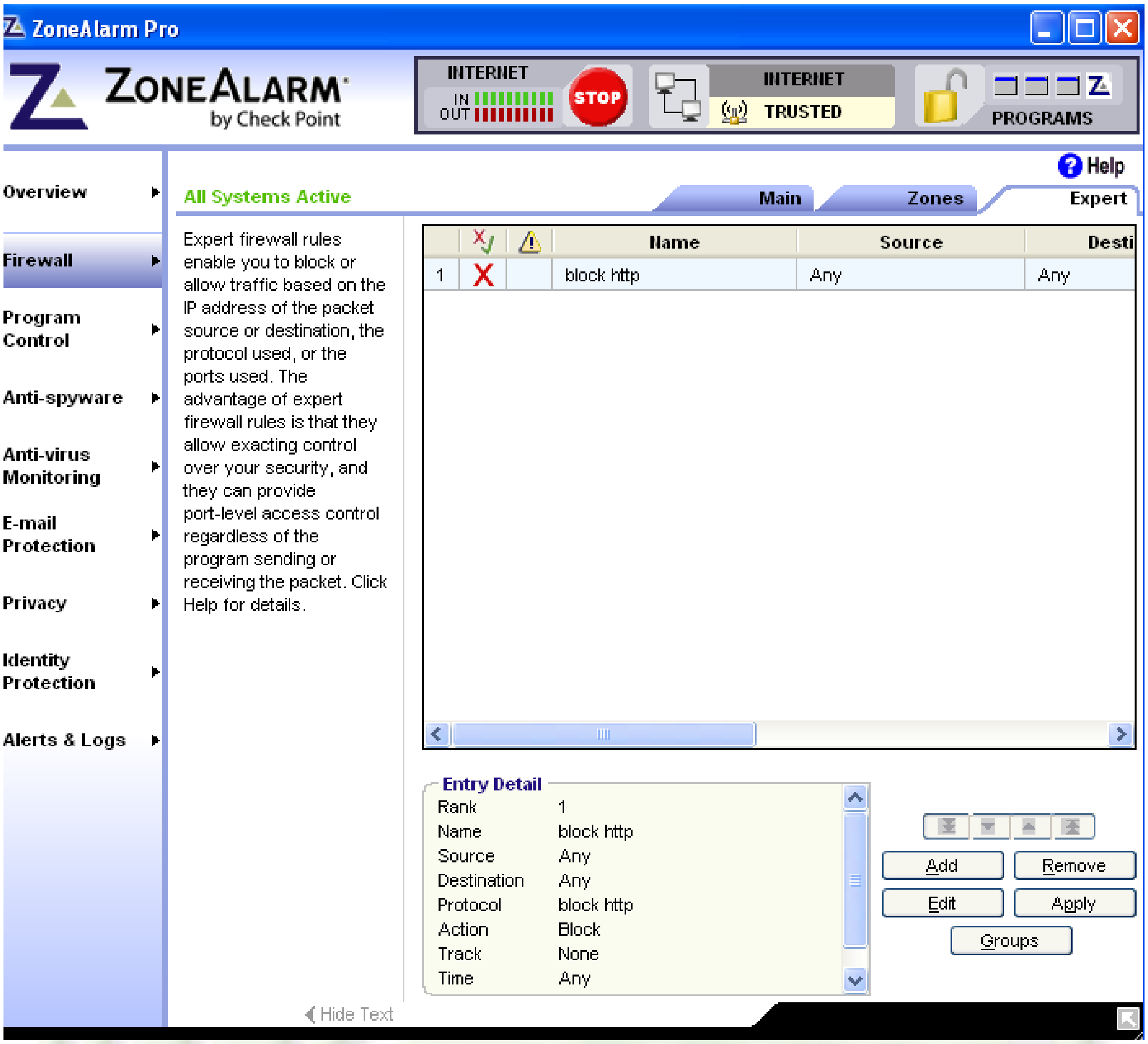


Edit this rule by modifying the following values:

General
Rank: 1
Name: Block HTTP
Comments:
State: Enabled
Action: Block
Track: None

Source: Any
Destination: Any
Protocol: Block HTTP
Time: Any

Click OK to set the rule, it should be listed as below…



Expert firewall rules enable you to block or allow traffic based on the IP address of the packet source or destination, the protocol used, or the ports used. The advantage of expert firewall rules is that they allow exacting control over your security, and they can provide port-level access control regardless of the program sending or receiving the packet. Click Help for details.

			Name	Source	Desti
1	✗		block http	Any	Any

Entry Detail

Rank	1
Name	block http
Source	Any
Destination	Any
Protocol	block http
Action	Block
Track	None
Time	Any

Click on the Zones Tab, and you should be automatically prompted to save your settings. Click YES.

Step 3: Testing HTTP rule

To test your new firewall rule, open Internet Explorer and try to open any web pages, www.yahoo.com, or www.google.com for test.

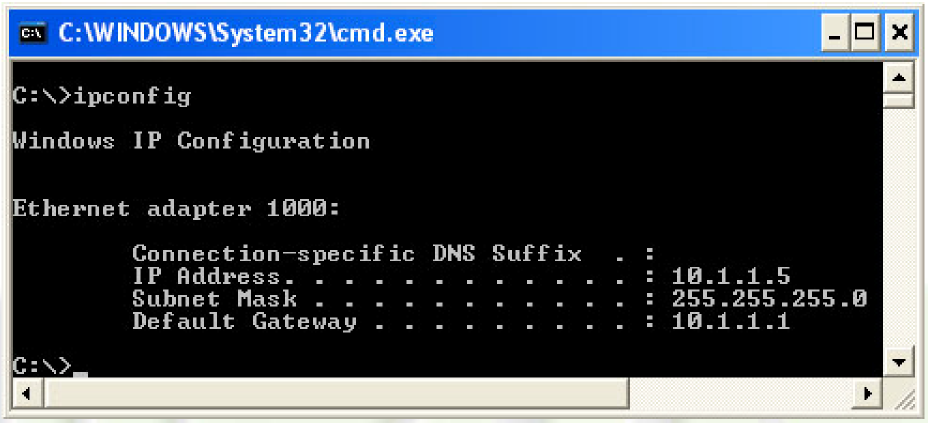
If the rule was configured properly, you should not be able to view any web pages. Were you able to access any web pages?

Step 4:

Take a screen shot of the failed web page and save to a Word document. Make sure your name is within the document. We will use this document again so do not print off or close.

Step 5: Block ICMP traffic

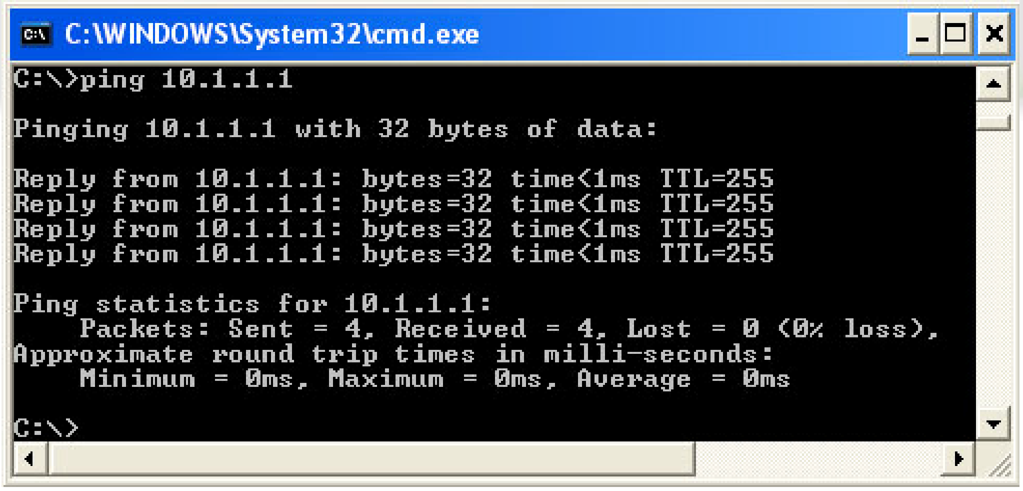
From START, Run, type cmd in the Open box and click OK. This will open a command prompt window. At the c:\> type ipconfig and press enter. This will show your current TCP/IP configuration.



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter 1000:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.5
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.1.1

C:\>_
```

Note your Default Gateway address

From the c:\> type ping [space] [ip address of your default gateway] and press enter. As below…
Ex. ping 10.1.1.1



```
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
Reply from 10.1.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

You should be able to successfully ping your gateway.

Click on the Expert tab from the Firewall menu. Click on Add on the bottom right.

In the General Box, set the following…

Rank:	2
Name:	Block ICMP
State:	Enabled
Action:	Block
Track:	None

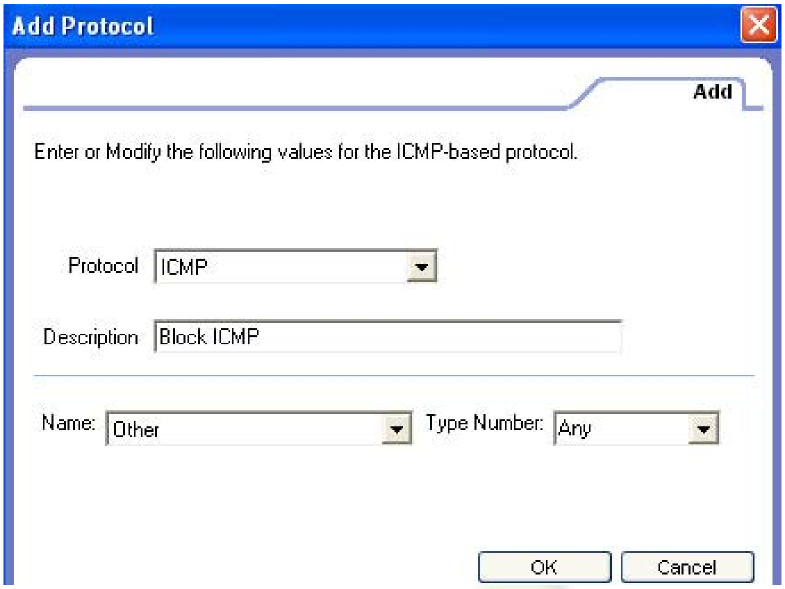
In the Source, Destination, and Time Boxes, leave the default setting ANY.

In the Protocol box, click Modify, add protocol, and add protocol.

Configure as below…

Protocol:	ICMP
Description:	Block ICMP
Name:	Other
Type Number:	Any

Click on the down arrow on name to view the different types of ICMP messages, but select Other, Any to choose them all.



Add Protocol

Enter or Modify the following values for the ICMP-based protocol.

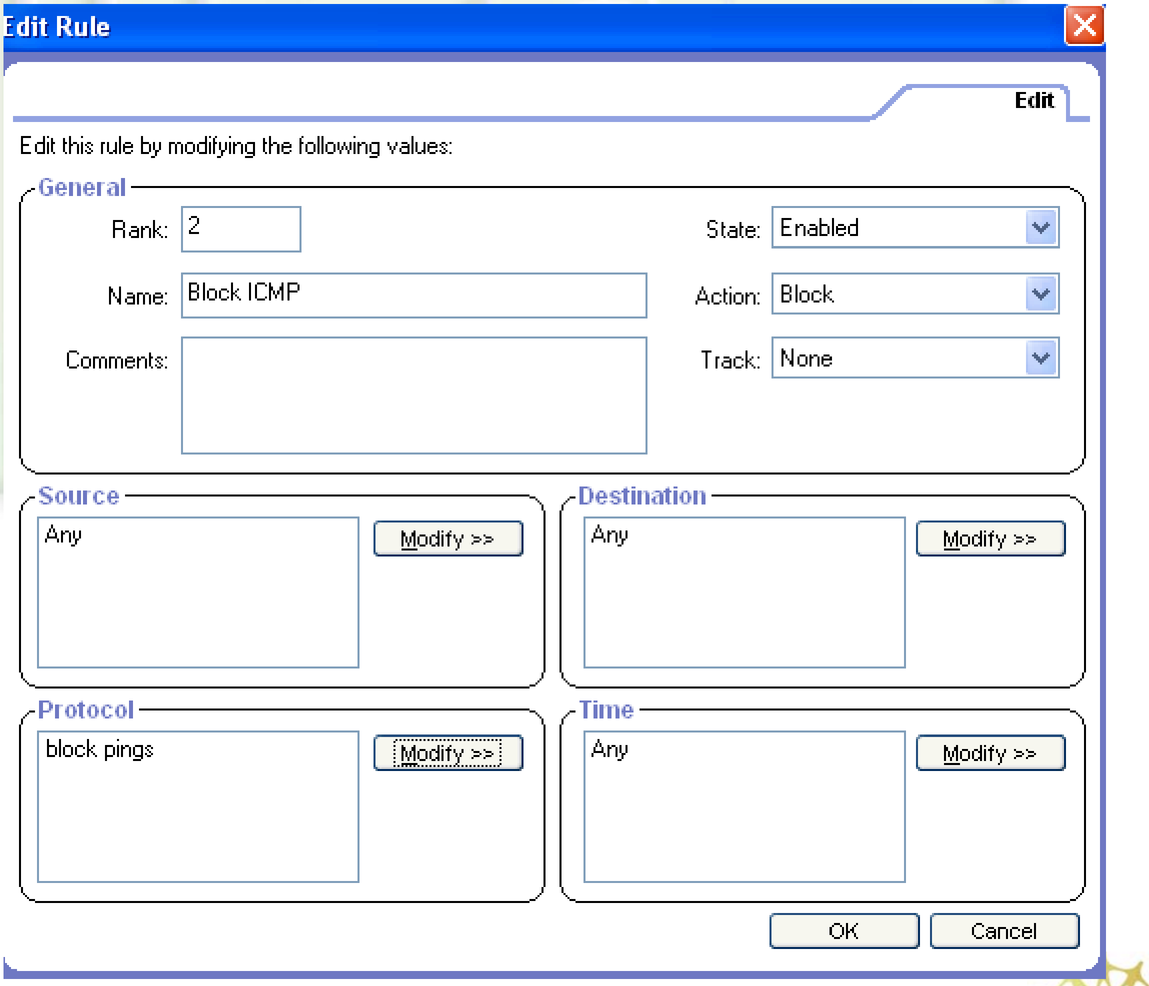
Protocol: ICMP

Description: Block ICMP

Name: Other

Type Number: Any

Compare your Rule as below…



Edit Rule

Edit this rule by modifying the following values:

General

Rank: 2

State: Enabled

Name: Block ICMP

Action: Block

Comments:

Track: None

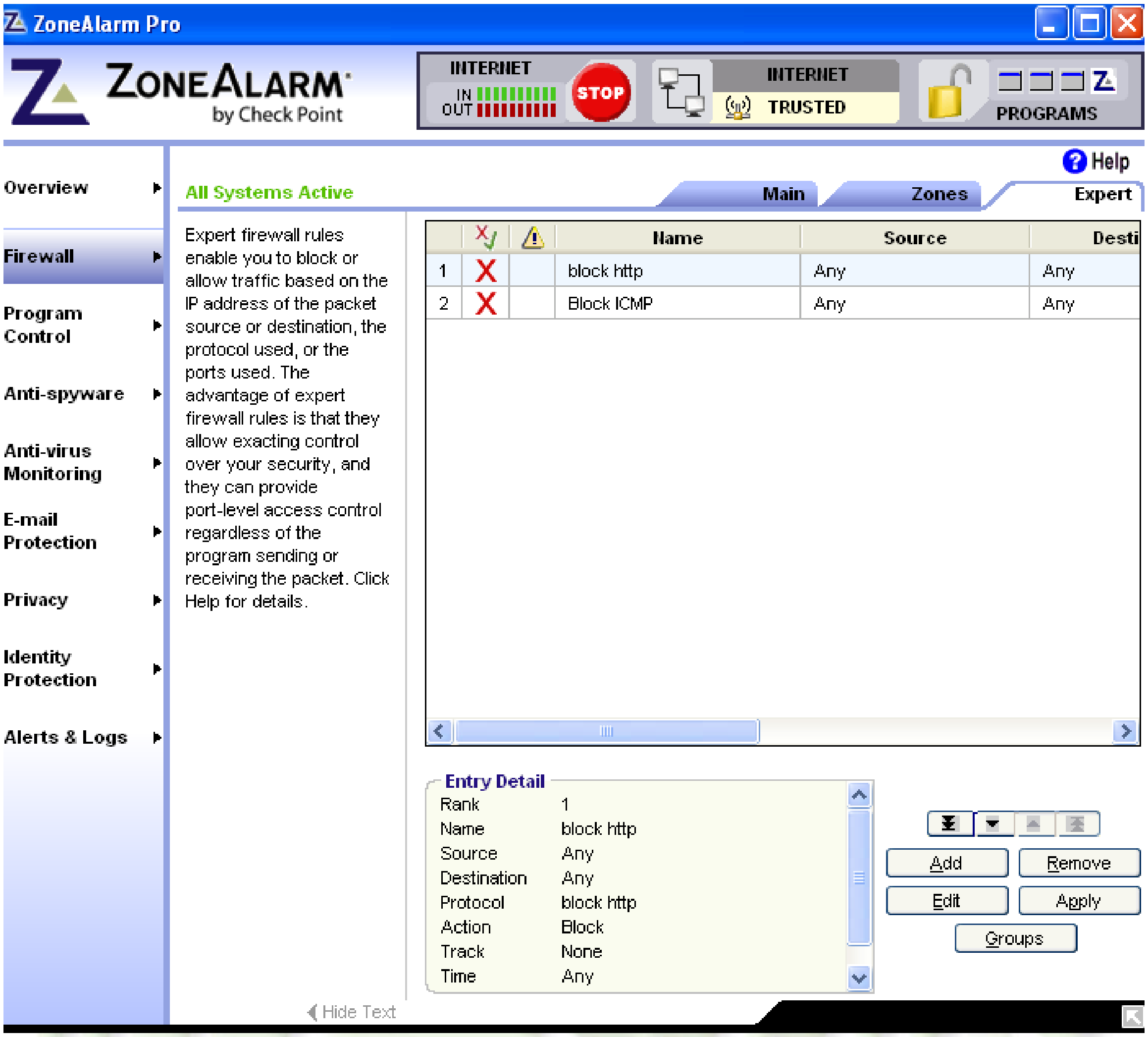
Source: Any

Destination: Any

Protocol: block pings

Time: Any

Compare your Firewall Rule list as below…



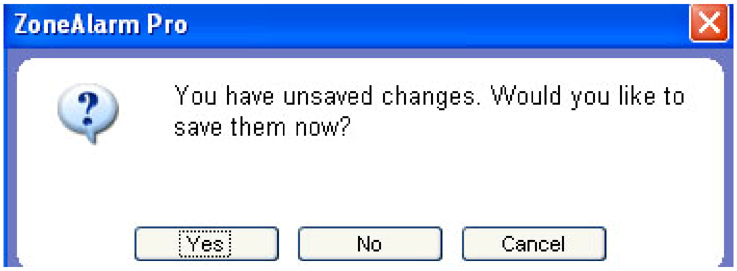
Expert firewall rules enable you to block or allow traffic based on the IP address of the packet source or destination, the protocol used, or the ports used. The advantage of expert firewall rules is that they allow exacting control over your security, and they can provide port-level access control regardless of the program sending or receiving the packet. Click Help for details.

			Name	Source	Desti
1	X		block http	Any	Any
2	X		Block ICMP	Any	Any

Entry Detail

Rank	1
Name	block http
Source	Any
Destination	Any
Protocol	block http
Action	Block
Track	None
Time	Any

Click on the Zones Tab, and you should be automatically prompted to save your settings. Click YES.



You have unsaved changes. Would you like to save them now?

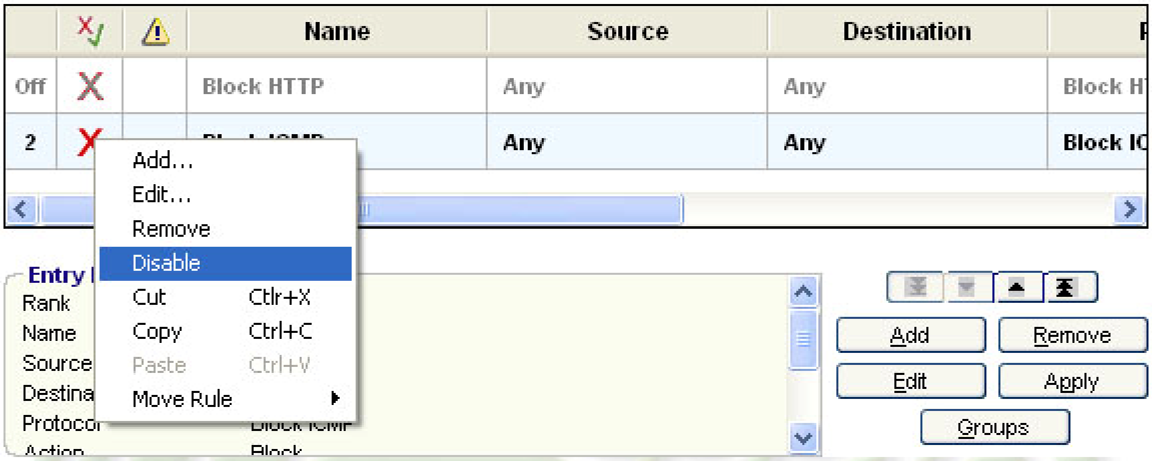
Step 6: Test ICMP rule

To Test your Firewall Rule, ping your default gateway address again. If the rule was setup correctly, you should not be able to ping anything, all ICMP traffic should be blocked. Was the ping successful? (It should not be successful!)

Step 7
Take a screen shot of failed ping screen and save to same Word document file that you used earlier. Print off this document for your instructor.

Step 8: Disable Firewall Rules

From the Firewall menu, click on Expert. Right click on each rule and click disable.



	✗✓	⚠	Name	Source	Destination	P
Off	✗		Block HTTP	Any	Any	Block H
2	✗			Any	Any	Block IC

When both rules are disabled, click on the Zones tab. You should be prompted to save your settings, Click Yes to save. Once you settings are saved, both rules disabled, try to ping you default gateway again. Was it successful? Open Internet Explorer, Navigate to a webpage such as www.yahoo.com or www.google.com. Were you able to? Enable the rules and save, test again. What was the outcome?

Step 9: Analysis

1) Should a product like this be placed on every PC within a network at a large business? (500 PCs)

2) If you answered yes to question 1, discuss ramifications of your answer. Think in terms of setup, support, configuration, etc.

3) Why should you setup a firewall on a computer that is connected to the Internet?

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.

Appendix:

This lab was developed using ZoneAlarm Pro, Trial Version 7.0.473.000, which can be obtained from:

http://www.zonealarm.com/store/content/home.jsp

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).