Global Information Assurance Certification Paper

ZoneAlarm – A free solution for home security

Curtis Elliott

October 1, 2001

Introduction:

In today's 'always online' environment home users are constantly faced with dangers and threats ranging from viruses that chew up system resources, destroy data, wipe out entire systems, and hackers trying to gain access to their personal data, at every turn. Security for home computers is becoming more of a necessity rather than a luxury. Home users need to secure their PC's and connections to the Internet to ensure that their data is safe and secure at all times. This is where ZoneAlarm comes in. ZoneAlarm is a personal firewall that is designed to guard a home user's PC against the threat of hackers and data thieves by allowing a user to control their computer's Internet traffic and the way applications access the Internet. ZoneAlarm is designed to protect DSL and/or cable connected PCs, and is also an invaluable tool for those with dial-up connections. After all, any computer connected to the Internet is at risk.

Operational Overview:

ZoneAlarm is a powerful and flexible security utility that provides ease of use without compromising security. To start with, ZoneAlarm's requirements are neither a system nor a resource hog and it supports just about all the version of Microsoft Windows.

ZoneAlarm's requirements are:

- Microsoft Windows 95
  Windows 98
  Windows NT 4.0
  Windows 2000
  Windows ME
- an 80386 or faster processor (486 recommended)
- 8 MB of system memory

A full installation only requires about 3 MB of hard disk space and it works with most types of TCP/IP connections, including Ethernet LAN, DSL, cable modem and dial-up connections.

ZoneAlarm is very easy to use. It protects automatically from the moment it is installed and no programming is needed to get the firewall and port blocking up and running. ZoneAlarm offers simplicity without compromising your security. To get a user up and running quickly ZoneAlarm provides nice tutorials that explain its controls and alerts. With color-coded alerts a user can easily and intuitively rate security risks in real time.

A core feature of ZoneAlarm is providing protection at the application layer, ensuring that dangerous applications such as Trojan horses and spyware are unable to achieve their purpose of reaching the Internet from a users computer.

ZoneAlarm includes four interlocking security services that are designed to protect a home user's 'always on' DSL or cable-connected PC as well as a typical dial-up connection. The four services are: a firewall, an Application Control, an Internet Lock feature and Zones.

The ZoneAlarm personal **firewall** is the main service of the four security services. ZoneAlarm provides a dynamic firewall, which allows a user to independently establish protection levels for both local and Internet zones. As soon as the firewall is installed it offers immediate and automatic blocking of dangerous Internet threats, both known and unknown, thereby guarding a user's PC against hackers and data thieves. The firewall does this in essence by acting like a bouncer at a nightclub or a doorman at a hotel in that it only allows traffic that the user understands and initiates to access the PC. ZoneAlarm's personal firewall offers complete port blocking. It is self-configuring and requires no need to learn about ports, protocols or firewall programming to be protected. It also runs in "stealth mode" which means the firewall hides all ports not currently in use by a program. The firewall only opens ports when an approved program requests them. In the Configuration Control Panel there is an Alerts icon. This icon monitors Internet traffic. It contains for small bars: two sets of up/down rows. These bars show graphical representations of all uploading and downloading. The top set of bars represent real time Internet traffic while the bottom set represent Internet traffic that has taken place over a period of time. A user may also click on the Alerts button to see a more detailed view of alerts along with two extra alert settings. The first option is to either

allow/disallow logging to a text file and the second option is show/hide the alert popup window.

The **Application Control** service allows the user to decide which applications can and cannot use the Internet. It consists of the Program Control Panel, which allows a user to see which programs have accessed the Internet and then restrict or broaden a program's ability to access the Internet. Software applications are automatically added to the Programs list the first time they attempt to access the Internet. There are four columns to the Programs Panel. The first column is the Programs List, which simply lists the program names that have tried to access the Internet. A user can highlight the program name for more information such as product version, location or name of file used to access the Internet. The second column is the Allow connect column. This column is divided into Local and Internet Zones. Each Zone allows a choice of three options each represented by a dot. A user can click on a dot to change the settings. The left most dot sets a checkmark, which allows access to the Internet. The middle dot sets an *X*, which denies access to the Internet. The right most dot sets a question mark, which means that ZoneAlarm will ask permission each time a program attempts to access the Internet. The third column is the Allow server section. It is setup the same as the Allow connect with options for both the Local and Internet Zones as well as the allow, deny and ask options. The fourth column is the Pass Lock column. A user may check the box in the Pass Lock column to allow Internet activity for applications that have been given rights to bypass the Internet Lock feature. Typically programs such as e-mail clients will be set to check for email while other applications are denied Internet Access. In the Configuration Control Panel there is an icon which provides a graphical look at which programs are currently connected to the Internet.

The **Internet Lock** feature blocks all Internet traffic during extended inactivity of a users PC. There are several options for setting up the lock feature. The Internet lock feature can automatically start when your screen saver is activated or after a period of Internet inactivity. If access is locked when the screen saver activates then it will be unlocked once the screen saver is deactivated. If the Lock is started by the period of inactivity option it will need to be deactivated by clicking the 'Lock' button in

the Configuration Control Panel. There are also two options to choose from while the automatic lock is engaged. The first is Pass lock, which allows programs that have been given rights to bypass the Lock feature. The second is High Security mode, which will stop all applications' Internet activity regardless of the program's access rights.

ZoneAlarm divides traffic into two separate zones: the **Local Zone** and the **Internet Zone**.
The purpose of the **Local Zone** is to allow those that a user trusts to access personal files and printers. Those users essentially have a "key" to access a users computer. A user may give anyone a "key" by entering his or her IP address into the Local Zone. This process enables ZoneAlarm to recognize what a user deems as permissible traffic. In a networked environment within your Local Zone enables connectivity to the Internet and to other computers on a local network. Most single PC users at home will not need to worry about including other domains, subnets and ip address, as they will probably have only one computer to secure. Three levels of security are available for the Local Zone: low, medium and high. *Low Security* is a minimal security setting and only enforces application privileges and the Internet lock settings. It allows local network access to Windows services and file/printer shares and leaves your computer and server applications visible to other on your local network. *Medium Security* is recommended for computers connected to the Internet through a local area network. It enforces application privileges and Internet lock blocks all traffic. It allows local network access to Windows services and shares and leaves your computer and servers visible to the local network. *High Security* is recommended for computers that are directly connected to the Internet or an untrusted network. It enforces applications privileges and Internet lock blocks all traffic. It blocks local network access to Windows services and shares. The firewall runs in "stealth mode" and hides all ports not in use by a program.

In keeping with the door and key analogy, the **Internet Zone** is treated as a locked door to those computers and web sites a user does not know or trust. So in other words the Internet Zone is defined as all computers and addresses not included in your trusted Local Zone. Three levels of security are available for the Internet Zone: low, medium and high. *Low Security* is not recommended for the Internet

Zone. It is a minimal setting that enforces application privileges and Internet lock setting only. It allows access to Windows services and shares and leaves your computer and server applications visible to others on the Internet. The firewall allows traffic to and from the Internet. *Medium Security* blocks only certain unsafe activity. It enforces application privileges and Internet lock blocks all traffic. It blocks Internet access to Windows services and file/printer shares but leaves your computer and servers visible to the Internet. *High Security* enforces application privileges and Internet lock blocks all traffic. It blocks Internet access to Windows services and file/printer shares. The firewall runs in "stealth mode" and hides all ports not in use by a program. In the Configuration Control Panel there is a Stop button. If any kind of trouble or malicious activity is suspected this button can be pushed to instantly stop ALL Internet traffic with no exceptions including not allowing any programs configured for Pass lock to function.

ZoneAlarm is also equipped with **MailSafe**. MailSafe is a service that guards a users PC against potentially harmful .vbs attachments that seem to be running rampart on the Internet today. MailSafe works with POP3 and IMAP, the most common Internet e-mail protocols. Keep in mind that MailSafe does not automatically delete files attached to e-mails and it is not a virus scanner. When an attachment is detected with a .vbs extension MailSafe quarantines it by changing the extension to .zl#, where the # is a number or letter. For example if e-mail were to be detected with a file attachment called please_open_me.vbs, that attachment would be quarantined and renamed to please_open_me.zl1 for ease of identification and removal.

ZoneAlarm also provides Mobile PC Protection, which allows a user to manually configure their security for a new network.

Conclusion:

Everything we do online leaves some sort of footprint that hackers can potentially use in some adverse way. Everyone wants to maximize their online Internet time and a good dose of common sense along with the use of ZoneAlarm's firewall and other powerful tools will help ensure that data and the PC's themselves are secure. ZoneAlarm's power, flexibility, easy of use and free price tag make it a highly recommended must have security tool for any home user whether they have

the 'always on' DSL/cable-connection or a standard dial-up Internet connection. ZoneAlarm's personal firewall blocks against Internet threats, both known and unknown, by making a home users PC invisible to the Internet. ZoneAlarm is the first to be tested as the only security software to make a computer invisible. (CNET test, August 2001) As the old saying goes: "Out of sight, out of mind" – if the hackers can't see a home users data then they can't attack it and cause destruction.

Zone Labs, Inc, "Installation Instructions". 5 September 2001
URL: http://www.zonelabs.com/sercices/support_install.htm

Zone Labs, Inc, 5 September 2001
URL: http://www.zonelabs.com/

ZDNet.com, ZDNet: Installing ZoneAlarm
URL: http://www.zdnet.com/products/stories/reviews/0,4161,2610364,00.html

CNET.com, Downloads.com.
URL:http://download.cnet.com/downloads/0-10105-100-6747047.html?tag=st.dl.10001-103-1.lst-7-1.6747047

Zone Labs, Inc, "Readme.txt File".
File: d:\program files\zonelabs\zonealarm\readme.txt

Marcus Goncalves, "Firewalls: A Complete Guide" 2000

John Chirillo, "Hack Attacks Denied" 2001