Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment Version 1.2b
Protecting Your Corporate Laptops from Hackers, While they are on the Road
By Darrell Keller

Introduction

You have heard about firewall network appliances such as the Linksys box or the VelociRaptor Firewall Appliance for home use. You think 'that's great, but what about all of my laptop users who take their computer on business trips with them and plug them into conference networks and hotel networks? I can't have them all lug around a Linksys box and ask them to set it up before turning their computer on a new network.'

Maybe you are thinking: 'The computer is not on the corporate net and therefore no one would know it belongs to your company. For all a hacker knows it is someone's personal computer, why would they bother to hack into it?' Actually, hackers are looking for personal computers, too. According to SANS "the average home computer with a high-speed Internet connection gets scanned, usually by hackers looking for ways in, between five and 25 times a day." (Balint, p.6). Usually hackers are not targeting a specific person, they are just looking to see if they can get into the computer. There are a number of reasons they may want to try and get into the computer. Some are to steal your credit card numbers or other financial information, to use the hard drive to store pirated movies (which require lots of disk space) or WARZ files (pirated software), or to use the computer as a zombie to launch attacks on other sites. Sometimes it is just for the challenge of seeing whether they can hack into the computer. They may also be hoping to find a mobile computer that will eventually end up inside a corporate network. If they put the right tools on the computer, they will be able to bypass the corporate firewall and have nearly full access to all the corporate data.

Laptop computers that are on the road often are connected to the corporate network through remote network access. This opens your corporate network up to anyone on the network that a remote computer is attached to, and creates a backdoor into your company. So a large company with hundreds or thousands of remote users opens that many backdoors into the network. Using a VPN solution that employs onetime passwords or tokens such as SecurID is still vulnerable. The VPN creates an encrypted tunnel between the remote computer and the corporate network so no one can intercept and read the traffic, but once the tunnel is connected, any person with access to the remote system can access the internal network at the other end of the tunnel.

There are a lot more hackers in the world today, because of the increased access to computers and because of the scripts that have been made, allowing anyone with the desire to try to hack the ability to do so. It takes little real hacking knowledge for most attempts. Script Kiddies download their favorite hacking tool and start playing. Because most people don't protect their home network or their laptops when on the road, the Script Kiddies can have a field day. So what about personal firewalls? That is probably the best answer for these travelers and not a bad idea for home users, even if they have a Linksys box (defense in depth). A current anti-virus is also essential for defense in depth.

This paper will review two of the more popular personal firewalls, Black Ice Defender and ZoneAlarm.

PC World.com's Assessment

According to PCWorld.com,

> The perfect personal firewall would be inexpensive and easy to install and use, would offer clearly explained configuration options, would hide all ports to make your PC invisible to scans, would protect your system from all attacks, would track all potential and actual threats, would immediately alert you to serious attacks, and would ensure nothing unauthorized entered or left your PC. (Sengstack)

Both Black Ice and Zone Alarm come close to this definition. They each have their strengths and weaknesses making one more attractive over the other, depending on its user. PCWorld.com decided that both products should share the title of Best Buy in their evaluation of Personal Firewall products.

Both Black Ice and Zone Alarm offer layers of security settings- Zone Alarm has three (High, Medium, and Low), and Black Ice has four (Paranoid, Nervous, Cautious, and Trusting). This gives Black Ice the advantage of providing finer adjustments by the user. The lowest of these settings on both products provides very little to no security at all. The highest setting blocks almost all traffic. This layered approach is good for novice users. Both products also offer some ability to tweak some of the settings for the more advanced users. In this category, Black Ice offers more than Zone Alarm.

When it comes to reporting, Black Ice provides more information than Zone Alarm. Black Ice notes the source of any probe and can be set to automatically look up the IP addresses and provide contact information about the person who touched the PC. Zone Alarm, on the other hand offers real time alerts of potential threats with pop up alerts. A feature that is useful for paranoid users, however, most people will likely turn the feature off and rely on the logs. Black Ice offers a similar feature, by flashing an icon in the system tray when it detects a potential threat. However if the system tray is covered at that time, or you are not looking at the tray, you will not see the alert.

PC World.com tested Black Ice and Zone Alarm (among others). In their tests they evaluated the ability of each of the firewall products to see how they reacted with common applications that access the Internet, as well as how they reacted to various forms of attacks. The programs they used were MS Internet Explorer, NetMeeting, WS-FTP LE, ICQ, Napster, PC Anywhere, and Real Player. All of the programs were able to access the Internet. With Zone Alarm, you have to tell it that it is okay to allow the program to access the Internet. However, once you do that one time, it remembers. PC World.com then installed the freeware version of PKZip, which also installs TSAdbot, an advertisement conduit that behaves like Trojan horse programs. Zone Alarm alerted on TSAdbot and asked for authorization. "BlackICE did not recognize TSAbot's behavior

as harmful." (Sengstack) They then threw three simulated hacks at the boxes: Installing and accessing the Back Orifice Trojan horse, running a port scan, and conducting a denial-of-service attack. They ran these at the program's default security settings. Both Black Ice and Zone Alarm detect Back Orifice (at the time of their testing Black Ice did not detect it in it's default settings, but that has been corrected in the current version). The port scan turned up no useful information because both Black Ice and Zone Alarm put the ports into a stealth mode.

So from PC World.com's perspective Black Ice and Zone Alarm are their best buys:

> BlackICE Defender, from Network ICE ($40), worked well with programs that access the Internet, and it provided the clearest explanations of what was going on. It is easy to install--even for newbies--and it permits advanced users to fine-tune its features.
>
> Zone Labs' ZoneAlarm can be a bit cantankerous when dealing with applications, but it offered the tightest security in our simulated attack tests. And the price can't be beat: It's free for home users and nonprofit organizations. (Sengstack)

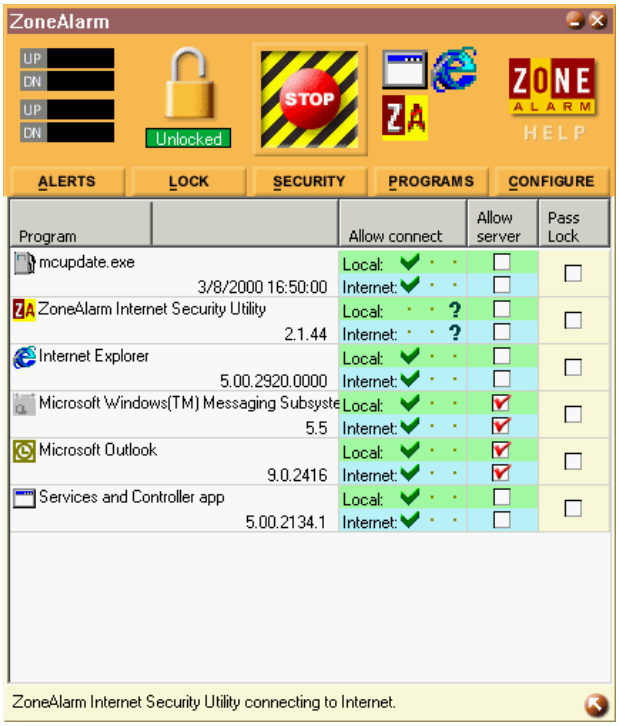
Now let's take a look at Zone Alarm and Back ICE:

Zone Alarm

Zone Alarm detects traffic both inbound and outbound from your computer. So if a Trojan happens to end up on your computer you will be notified when it tries to access the Internet. Their site claims that there is no need to learn about ports, protocols or firewall programming to be protected when using their software. This is because Zone Alarm watches network communications on a per-application basis and asks the user for permission each time an application wants to use the network. They also have a feature called MailSafe that is used "to stop email-borne Visual Basic Script worms, like the 'I Love You' virus, 'dead-in-its-tracks', thwarting its spread, and preventing it from wreaking havoc on your PC." (Zone Labs)

As mentioned before, Zone Alarm offers three levels of security; "low," "medium," and "high." These levels are available for both Internet connections and the local network. You can also add specific hosts to trust, however you can not specify the services to allow from those hosts.

By looking at an application's file header and directory location, Zone Alarm identifies the application that is requesting access to the Internet (or local network) and then checks its rule base to decide whether to allow it, deny it, or prompt the user. This rule base is kept in a file that is easily editable through the GUI. The user can use this to change the settings in order to allow, deny or prompt for permission to connect.



How effective is Zone Alarm when it comes to security? Security Portal ran some tests by running nmap on ZoneAlarm in "high security" mode. They state that Zone Alarm reported a single alert that "was not informative and nmap was able to identify a few services:" (Boran)

Port	State	Protocol	Service
17	open	tcp	qotd
19	open	tcp	chargen
135	open	tcp	loc-srv
139	open	tcp	netbios-ssn

No OS matches for host.

With no firewall installed, the test PC (Win2K SP1) presented nmap (nmap -sT -P0 -O IP_ADDR) with the following ports:

Port	State	Protocol	Service
7	open	tcp	echo
9	open	tcp	discard
13	open	tcp	daytime
17	open	tcp	qotd
19	open	tcp	chargen
23	open	tcp	telnet
135	open	tcp	loc-srv
139	open	tcp	netbios-ssn
445	open	tcp	microsoft-ds
1025	open	tcp	listen

No OS matches for host

Some of the advantages of Zone Alarm are:

- It is free for personal use.
- It shuts down all unused ports.
- If offers good intrusion detection.
- It has different rules for LAN (local) and Internet networks. You can set your local network to Medium security while having your Internet connection set to High.
- It asks for permission before an application can use the network. This can be set to ask for the first time or every time it attempts to access the network.
- It has the ability to block the network temporarily so no programs are allowed in or out of the computer while it is locked. There is also a way to set up specific programs to be able to pass through the lock (such as an email program that you want to still be able to check mail).

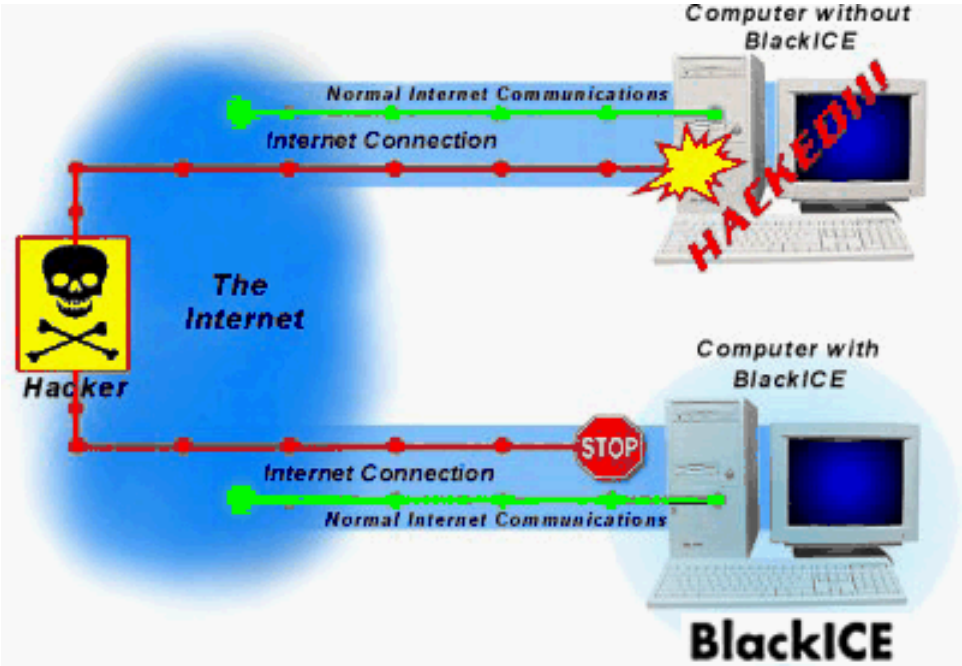
Some of the Disadvantages of Zone Alarm are:

- The more applications being used, the more pop-up questions appear. This may confuse or annoy the user, causing them to just click "allow" and then ending up with more applications trusted than expected.
- When it prompts to allow an application to access the network, it doesn't provide any information on what the application does.
- There is no way to allow or deny specific incoming or outgoing ports or protocols. This would be a useful feature for more advanced users.
- The attack logs (which are located in \winnt\Internet Logs\ZALog.txt on an NT system or \windows\Internet Logs\ZALog.txt on a 9x system) are not detailed enough. The logs give port numbers, but no reasons why packets are blocked; there are no packet headers or contents, or any state information.

Black Ice

Network Ice's web page explains Black Ice in the following way:

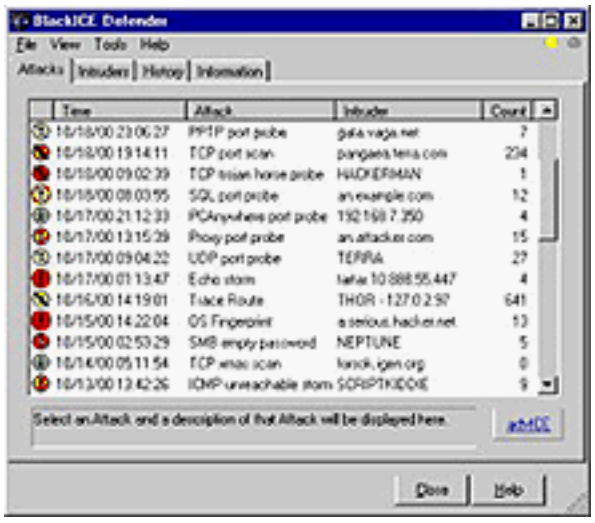
> BlackICE Defender scans your DSL, cable modem, or dial-up Internet connection looking for hacker activity. When it detects an attempted intrusion, it automatically blocks traffic from that source, keeping intruders from accessing your system.
>
> BlackICE is a way to detect, monitor, and block intrusions. BlackICE Defender analyzes, in real-time, ALL the communications from the Internet to your computer. Using an intelligent firewall combined with an intrusion detection engine, BlackICE can stop attacks while leaving normal Internet communications unaffected.
>
> ...BlackICE works continually to defend servers and workstations from over 200 hacker signatures including the Melissa Worm, "Slow Scans" and "Back Orifice." Even if hackers bypass firewalls or intrusion defenses, BlackICE bars entry at the desktop and server.



> The BlackICE engine uses a protocol analysis technology to detect attacks. This technology structurally analyzes and decodes the individual communications packets entering your computer. Because other security products use pattern-matching technology, BlackICE Defender is not only considerably more efficient and accurate, but it detects attacks other intrusion detection systems miss, such as fragmented attacks and NMAP scans. (Network Ice)

Black Ice sits in the taskbar and warns of incoming Network connections through the use of various colors of blinking icons (Yellow, Orange or Red depending on the level or urgency of the attack). It has four levels of protection: paranoid (don't allow any inbound TCP or UDP port connections), nervous (allow non-standard UDP port connections), cautious (allow non-standard TCP and UDP port connections), and trusting (don't block anything, however warn when something happens).

When an attack happens and the icon in the taskbar flashes, the user can click on the icon to get a list of attacks. Right clicking on the event allows the user to choose from four options: trust the address, block the address (for a period of time, or forever), ignore the attack by this intruder, or ignore this attack by anyone.



As we did with Zone Alarm, we must now ask, how effective is Black Ice when it comes to security? Once again Security Portal ran some tests by running nmap on Black Ice.

It did notice the nmap scans by flashing a red icon in the system tray. A closer look showed Black Ice reported a "TCP Port scan," "TCP port probe," "NMAP OS Fingerprint," "TCP Ace ping," "TCP OS Fingerprint," and "UDP Port Probe," among many others. Nmap returned a large list of "unfiltered" ports (false positives) and was unable to identify the OS.

Some of the advantages of Black Ice are:

- It has a simple GUI that is easy to use.
- It offers good intrusion detection.
- It offers a useful "attack history" and list of attacks in the GUI window, it informs immediately of an attack, and notes the attacker's IP address and, if the option is enabled, the attackers host name.
- Configuration, policy and alerting can be centralized on the corporate version.
- The firewall.ini can be manually edited to block or allow specific UDP and TCP ports.
- The program is fairly well documented.

Black Ice's disadvantages include:

- It is not free (and there is also no demo version available to download).
- In the firewall.ini there is no way to specify port ranges or wildcards or to filter state-based protocols.
- There is no GUI to edit the firewall.ini; it must be done through a text editor.
- It waits for a connection to be made before taking action rather than shutting down the system's ports so a connection can't be made in the first place.
- There is no way to block outgoing ports or applications.
- On a corporate LAN, there are a lot of false positives from SNMP servers, NetBIOS connection attempts, Exchange servers, etc.

Conclusion

What does all this mean? It means PCWorld.com was correct in stating that both products are nearly equal in their abilities and both do the job well. From a corporate stand point, I would choose Black Ice because it allows for centralized logging, and won't cause any user confusion by popping up boxes asking if a program should be allowed to access the network. The installer can also be configured so you can pre-set your corporate network IP's as a trusted net, before giving the installer to your users. For those who are more security cautious, I would recommend using both. What one may miss, the other will most likely catch.

References

Zone Labs Website
http://www.zonelabs.com (May 27, 2001)

Network Ice Website
http://www.networkice.com (May 27, 2001)

Breiling, Susanna; Andrew Plato, Kimi J. Winters. BlackICE Defender User's Guide – Version 2.5. Network ICE Corporation, 2001.

Balint, Kathryn. "Keeping Out the Bad Guys." The Computer Link, San Diego Union-Tribune. April 10, 2001: 6-7.

Andress, Mandy. "Personal Firewalls." TISC Insight. Volume 2, Issue 18
http://www.tisc2001.com/newsletters/218.html (May 27, 2001)

Sengstack, Jeff. "Make Your PC Hacker-Proof." PC World magazine (PC World.com). July 21, 2000
http://www.pcworld.com/hereshow/article.asp?aid=17759 (May 27, 2001)

Boran, Seán "Personal Firewalls/Intrusion Detection Systems." SecurityPortal. April 26, 2001
http://www.securityportal.com/articles/pf_main20001023.html (May 27, 2001)

Dolinar, Lou "Bolting the Windows Against Web Prowlers." Newsday.com. April, 26, 2000
http://www.newsday.com/plugin/99ld0426.htm (May 27, 2001)

Jssweb.net
http://jssweb.net/security.htm (May 27, 2001)

Seabold, Carl. "Security Program Testing"
http://www.msu.edu/~seaboldc/geek/security.html (May 27, 2001)

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event