Global Information Assurance Certification Paper

Security Essentials Level I Practical
Washington, DC July 5-7, 2000

Host based intrusion detection systems

Personal Firewalls: What are they, how do they work?

Tina Zych
August 22, 2000

Introduction

A firewall was originally considered necessary only on a network system to prevent undesirable access at the perimeter. With the advent of increased home computing, cable and DSL modems, a personal firewall now is prudent for the sensible user.

Cable and DSL modems are "on" 24x7 unless the computer owner "turns off" the computer. This constant connection often has a static Internet Protocol (IP) address that can be found time after time once discovered by a hacker. A computer without a firewall in this environment is an easy target wherein to leave a Trojan behind. Some Trojans allow a hacker to take remote control of that computer to launch attacks against other targets. The February 2000 Distributed Denial of Services attack was aided by the lack of defensive tools on computers.

The likelihood of success is increased when the average user either does not patch vulnerabilities in their operating system and applications or uses anti-virus software or lets it expire. Another contributor to successful hacking exploits is the File and Printer Sharing feature on Microsoft products. Each of these can be dealt with but I will discuss only personal firewalls in this paper.

Many companies now permit "road warriors," staff in the field or working at home, to access the company network. If the employee's home pc is vulnerable due to a high speed, always open connection a firewall will help. Personal firewalls may be installed on desktops, PCs and laptops adding an additional layer of protection to the home user or telecommuter's business LAN connection. Ed Pardo's *Cable Modems and Corporate Security* discusses this further. The cost of personal firewalls makes them more affordable than its big brother network firewall.

This reduced cost, in conjunction with ease of use, make personal firewalls an attractive addition at the workplace. A personal firewall can provide host-based protection on a desktop or server that contains highly sensitive or confidential information.

The Tools

A personal firewall should monitor, once configured, without much additional user input. Firewalls should block ports and allow only those services necessary to the business mission. Personal firewalls are pre-configured upon installation and vary with regard to additional configuration functionality. There are currently two types of personal firewall on the market to provide protection. One is an application level firewall that monitors

inbound and outbound Internet traffic and alerts the user that an application is attempting access his/her pc or his/her machine is trying to access something on the Internet. The other firewall monitors at the IP level reading data that is contained in the TCP/IP header for approved protocols or suspicious packet contents. It too alerts the user when malicious activity is detected.

Examples of application level firewalls include: Symantec's "Norton Personal Firewall," McAfee's "GuardDog," Zone Labs' "ZoneAlarm" and Signal9's "Conseal Private Desktop." Note that NAI does not advertise "GuardDog" on their site although it is available in stores. McAfee announced the purchase of Signal9 in January 2000.

Firewalls that monitor at the IP level include: Dynamic Solutions, Inc. "NukeNabber," Network Flight Recorder "BackOfficer Friendly," NetworkICE "BlackICE Defender" and Signal9 (McAfee) "Conseal PC Firewall." This paper will describe the similarities and differences between three of the more popular products in the market today: Symantec's "Norton Personal Firewall v2.0," NetworkICE "BlackICE Defender v2.1" and Zone Labs "ZoneAlarm v2.1.25."

John Broughton mentions in *Cable modem and DSL security issues and solutions* that NetBarrier is available for Macintosh OS 7.5.5 and later versions as well as DoorStop Firewall, Personal Edition for MacOS 8.1 and later. LinuxIP Firewalling Chains is a packet filter firewall for Linux.

But which should you use? Computer magazine publications run tests frequently on firewall products to determine "best buy" and "best product." Any one of the three in this paper currently holds the title of best depending on which magazine you read and what month it is. Your selection may depend on what you want it to do and what information you want it to provide. Some prefer an IP level firewall that provides more information about the attacker. Others prefer an application level firewall that focuses more on inbound and outbound traffic than tracing the attacker. Others want highly configurable applications. What's your preference?

Application Level Firewall

Let's start with two popular application firewalls. These firewalls monitor connections attempted by applications to or from the user's pc. Symantec's Norton Personal Firewall offers extensive configuration if you know how. Zone Lab's ZoneAlarm also allows configuration but to a lesser degree.

Norton Personal Firewall v2.0

Symantec released this firewall originally as part of their "Internet Security 2000" software package in early 2000. By the summer, it was available as a separate product. It works at the application level and monitors inbound and outbound activity. The Personal Firewall contains security and privacy applications less the parental control, anti virus and ad blocking of the larger Internet Security 2000 product. It has multiple settings ranging from the recommended "medium" to user dictated configuration at every alert. This makes the software easy to use for novices and provides more customization for the

knowledgeable analyst. Norton's firewall can be set to interactive learning whereby the firewall updates its rules as the user determines.

Alerts

The screen print below displays the alert. An "ALERT" window appears each time the Firewall Rule Assistant detects an attempt to connect through the Internet. It will announce inbound and outbound connection attempts. The user must then choose to block or permit the communication one time or to configure a new rule. For the firewall expert configuring new rules allows more control over the connections being attempted. For the novice, this proves more challenging since limited information is provided about the attempt being requested. For example, Norton recognizes "Umgr3.exe," Back Orifice's filename but not the application name. Unless the user recognizes the filename, he/she will not know whether to permit it or not. The Event Log will display the connection's application or the attack name, but the user cannot access the log until after he/she has made a decision to permit or block.

This research discovered that there appears to be several complaints that when the Alert icon flashes, it freezes the screen and a reboot is needed. I have experienced this too so I wrote to Symantec and was told to "Try deselecting the show icon option on the Norton Internet Security options screen. Does this help the problem?" by the support technician. This change may stop the problem but I no longer will see a visual alert. These discussions can be found on Symantec's support web page.

How it Works

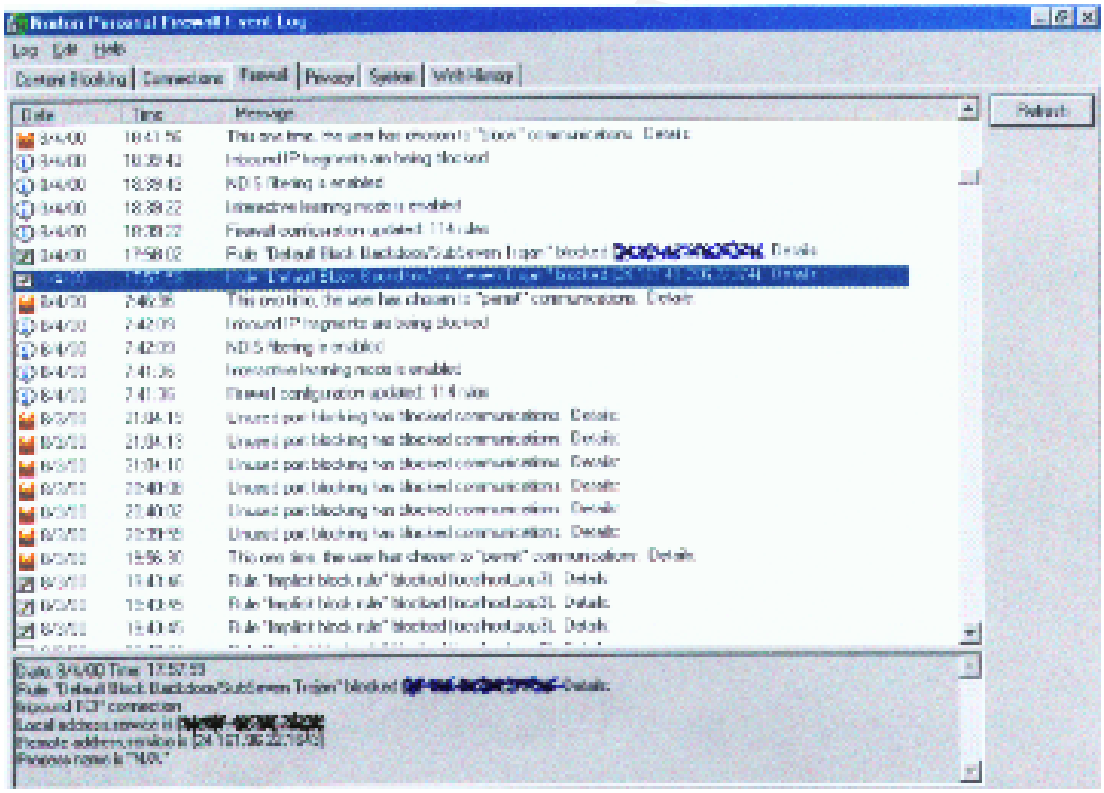
This firewall claims to work in stealth mode. The unblocked ports are invisible to anyone looking for them on the Internet. Any ports left open for necessary services are assigned a rule and are not stealth. The default installation provides this level of protection but be warned that if the user configures the firewall differently, he/she may change the stealth capability and unknowingly open a port. Symantec also claims that if a Trojan is hidden on a computer before the user installs their product, the hacker owning the Trojan cannot access it since the port is not seen. Stealth is also intended to protect against port scans.

Additionally, the firewall works on implicit rules. It protects any inbound or outbound connection that does have a rule. The screen print example that follows shows these actions in the event log.

Event Log

The Norton firewall also provides content blocking, connection, privacy, system and web history information in the Event Log. Norton's Event Log file captures activity without disturbing the user. The firewall tab has a timestamp and message that tells the user the attack used. In the screen print below "Rule 'Default Block Backdoor/SubSeven Trojan' blocked (my.IP). Details" is highlighted. The details are provided at the bottom of the screen for the highlighted attack. The date (mo/day/yr), time (hr/min/sec), the action "Inbound TCP connection," local address is the user's IP address and the remote IP address of the attacker; in this case "24.161.96.22.1643" are displayed. There are no further instructions or assistance for a user to automatically trace the attacker's address.

Other icons in the firewall log display the decisions made by the user when the alert box prompts a decision. The silent blocking done by Norton is also logged here indicating, "Unused port blocking has blocked communications." Further information is displayed such as inbound TCP but not always with the port scanned or attacked. The remote IP address is displayed with the port. The user can see that an "implicit block rule" occurred. Logs can be copied to a text file. Norton does not detect Trojans; it only reports them in the log. It is not an intrusion detection product.



The actual text log for other dates show:

8/19/00 14:26:09 Unused port blocking has blocked communications. Details: Inbound TCP connection Remote address, local service is (207.71.92.221,finger)

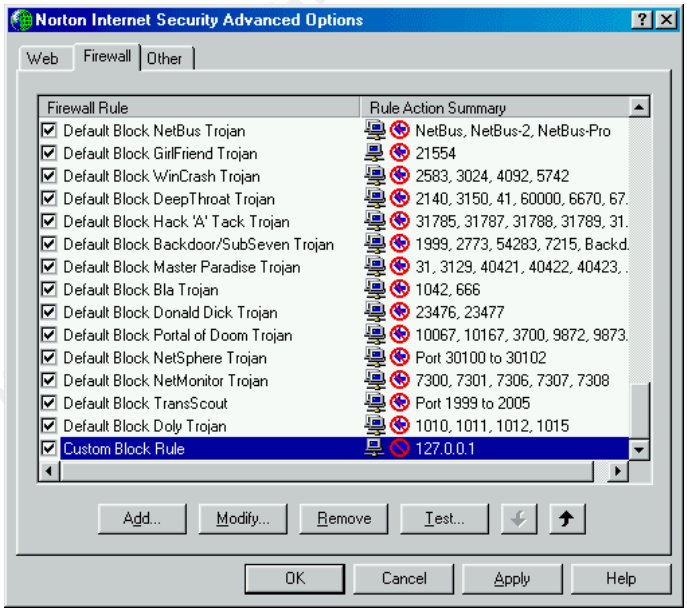
8/19/00 14:25:20 Unused port blocking has blocked communications. Details: Inbound TCP connection Remote address, local service is (207.71.92.221,smtp)

8/19/00 14:24:18 Unused port blocking has blocked communications. Details: Inbound TCP connection Remote address, local service is (207.71.92.221,telnet)

8/19/00 14:38:36 Unused port blocking has blocked communications. Details: Inbound TCP connection Remote address, local service is (207.71.92.221,ftp)

Configuration

The firewall rule screen is shown here. By clicking on the boxes and add/modify/remove the changes are adopted. Norton allows configuration by adding or removing ports to block and changing the rules for the firewall. Symantec technical support advises that the user document any changes made to the default configuration to be able to undo any unanticipated problems. Change control is necessary for this application. Additional ports can be blocked manually. Configuring this firewall can be difficult for the novice to understand. More documentation is found in HELP than in the manual and in a file off Symantec's web page.



Benefits

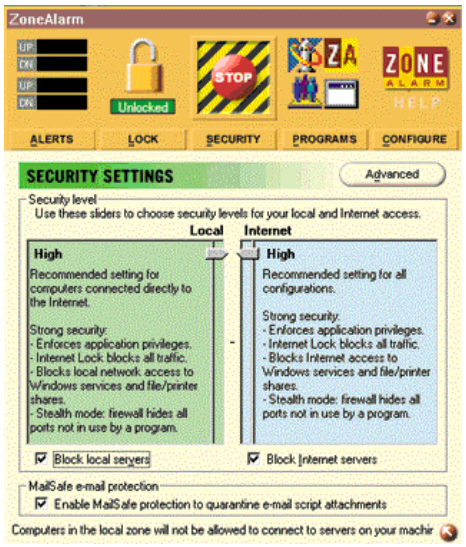
- Highly configurable for the expert user.
- Good firewall rule window.
- Easy to access logs.

Problems

- A "blinking" alert icon tends to freeze up the screen that is open.
- Learning about configuring the settings on one's own is time consuming.
- Configuration changes can reduce the effectiveness of the firewall.

ZoneAlarm v2.1.25

Another popular application level firewall is Zone Labs' ZoneAlarm, which is a free download from their site. Zone Labs take the firewall out of the box and into a panel. There are five panels that provide the user with information about security settings, Internet alerts, lock status, configuration and programs. ZoneAlarm monitors inbound and outbound traffic.

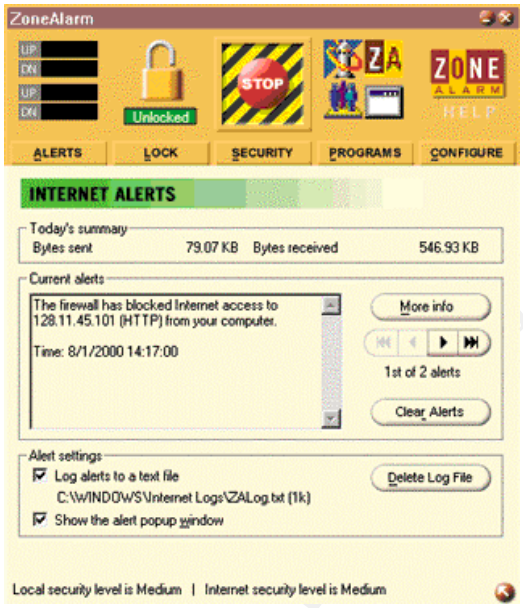


Security Settings

ZoneAlarm provides settings of "high" the default setting, "medium" and "low" to protect the pc. The "high" setting stealths all ports not in use.

This application differs from Norton in that it allows the user to choose settings for both local and Internet servers individually and if to block them. The "Advanced" button allows the user to designate any other computers or subnets on the in the local area.

The enabled "MailSafe" protects against .vbs attachments in incoming email.



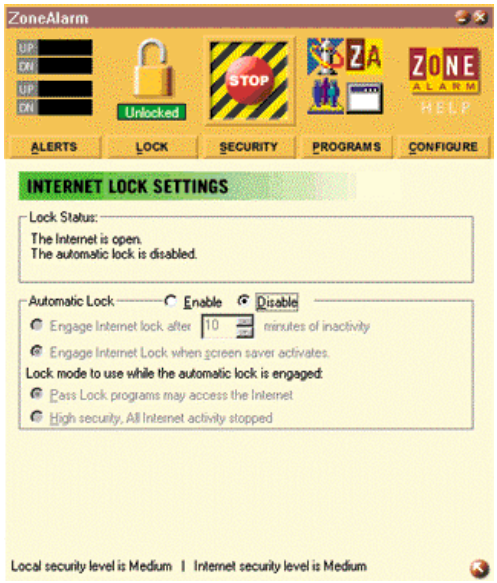
Alerts

The alert to an application trying to access the Internet from your pc or from the Internet to the pc is not a sole icon in the task bar. ZoneAlarm can be configured in the Configure panel to create a "desk band" instead. The desk band will be discussed later. Like Norton the Internet Alert panel will open if enabled, to tell the user what connection is being attempted. This is also where the option to log alerts to a text file if enabled.

ZoneAlarm offers simple configuration for the novice. Experts may find it less interesting than Norton. The panels on ZoneAlarm take a different approach than Norton as described further.

This is the Internet Lock Settings panel. Unlike Norton, the user can enable a lock that activates after a set time of inactivity or when a screen saver comes on to automatically block all inbound and outbound traffic. Programs can be identified to work around the block preventing the lock to activate in the midst of long downloads. The "high security" button is recommended.

Locking a pc after a period of activity allows one more layer of security if the user is pulled



away from the pc unexpectedly. This firewall also lets a user choose to lock the pc manually by clicking on the "Stop" or "Lock" icon.

The fourth panel is the Program panel. ZoneAlarm records applications attempting access from the local and Internet areas on the in this panel. Network access privileges for each of those applications are then set in this panel. In this example, Eudora was detected and the user must decide whether a connection should be permitted to or from the Internet and local pc and if the lock should be enabled for it.

Once an application is stored here, ZoneAlarm will reference these settings to permit or deny a connection. The user can change the settings as needed from this panel.

The Configure panel (not shown) allows the user to enable the "desk band" on the user's window so the "lock" and "Stop" icons are always visible. This panel also provides an enable box to check automatically for updates.

Logs
A sample of ZoneAlarm's logs shows timestamp, GMT, application, intruder IP address, and port:

PE, 2000/05/20,19:03:02 -5:00 GMT, KVTekyiPost, 38.153.36.65:80,N/A

FWIN, 2000/05/21,13:53:20 -5:00 GMT, 63.15.231.22:31337,24.161.3.127:31337,UDP

PE, 2000/05/21,14:01:54 -5:00 GMT, Distributed COM Services, 0.0.0.0:0,N/A

Benefits

- Allows configuration by user.
- Lock feature allows user to block Internet after a timeout.
- Checks each application that does not have a rule.
- Free download.

Problems

- Alerts do not easily identify the application that is trying to connect.
- Configuration capability could be better for the expert.
- No manual.

IP Level Firewall

At the IP layer, the personal firewall checks packets for fragmentation, corruption and other problems and blocks those. It reads IP protocol headers like TCP, ICMP and UDP for malicious activity. It monitors ports and services for intrusions and provides stealth protection.

BlackICE v2.1cm

An interesting bit of trivia. Founded in April 1999 by former product development and management executives at Network Associates, NetworkICE takes its name from the fiction novel, Neuromancer by William Gibson. It is about a hacker who must find a way to get into an artificial intelligence network protected by intrusion detection software "Corporate Ice."

BlackICE v2.1 protects and detects suspicious connections both inbound and outbound at the IP level. If the firewall detects a match to its attack signatures it alerts the user, logs the action and can if configured, collect trace evidence in a special log. The trace will contain the source IP address' MAC, DNS and node if available. NetworkICE claims that if two firewalls are running on one system, the one set to block will block the connection even if the other firewall is set to permit it. They also claim this product is compatible with other firewalls.

Settings

Similar to Norton, BlackICE allows the user to set a level of protection. Its default setting is "cautious" but if left at that will not protect against all Trojans; Back Orifice has gotten through. The user must set it at "paranoid" to provide full security.

Alerts

BlackICE will alert you to inbound and outbound scans, attacks and probes with this version**.** Upon installation, an icon appears in the task bar that blinks different colors depending on the detection: red for an intrusion, yellow for minor alerts. Simply click on the icon and the attack list will open in a window allowing the user to see the attack immediately. The decision to block or permit the intruder does not require immediate attention. BlackICE automatically blocks and logs the attack and intruder. The user can open the intruder list at a later date and determine whether to block or trust the IP address in the future.

Configuration

This firewall is less configurable, reducing the holes that an unskilled user may create by writing new firewall rules. (Norton Personal Firewall v2.0 cautions their users about this problem.) BlackICE's configuration allows the user to enable packet and evidence logs and trace settings.

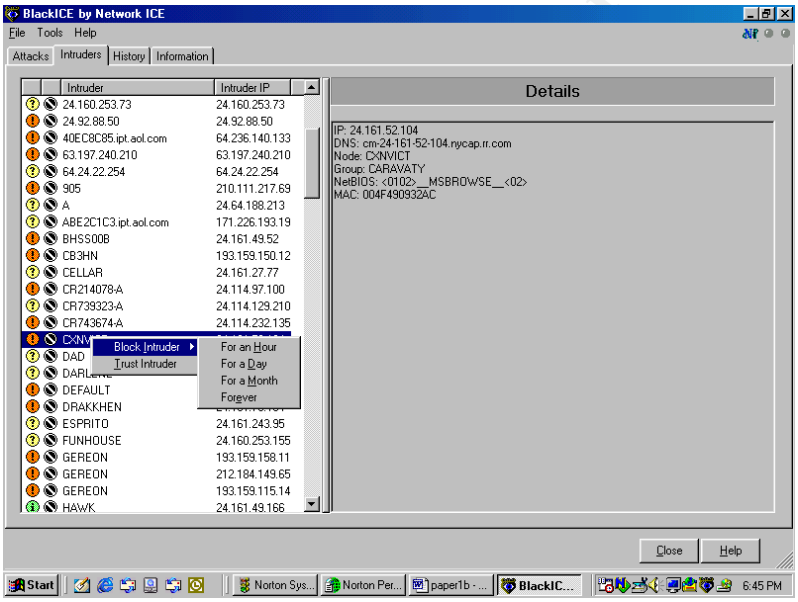
Attack Details

BlackICE captures the source IP address, the timestamp GMT (mo/day/yr, hr/min/sec), the port being attacked or probed, the DNS of the attacker, the name of the attack, the destination IP address, the parameters of the attack (port, attack and whether a password

was sought) and when identifiable the MAC, Group and Node information of the attacker. This facilitates report of the attack or abuse to the ISP in question. BlackICE also provides an "Advice" button that connects to their web page where the selected attack is further described in general terms.

Let's take a look at an example. In the screen print below, the "Intruder" is "CXNVICT" and the information captured is:

IP: 24.161.52.104,
DNS: cm-24-161-52-104.nycap.rr.com,
Node: CXNVICT,
Group: CARAVATY,
Netbios <0102. >
MSBROWSE<02>,
MAC: 004F490932AC



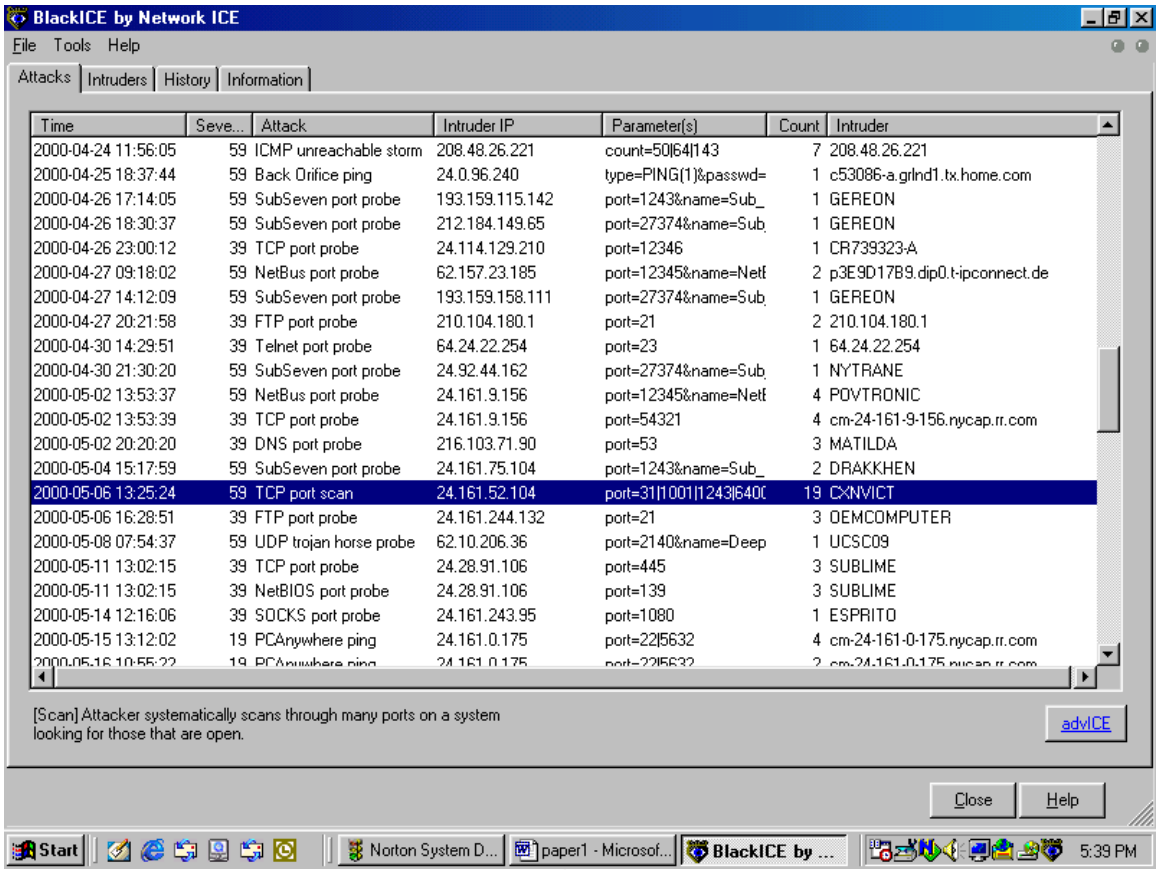
BlackICE successfully blocked these attacks and the application can be configured to block future attacks from these intruders from an hour to forever. The user may set the firewall to trust an IP address here.

With the addition of the information in the next screen shot it is possible to contact abuse@nycap.rr.com to report the attack. If writing to report an abuse to an ISP, please read Donald McLachlan and the GIAC Community paper Contacting Host Owners v 2.0 (4/8/00) before making a mistake or a wrongful accusation.

There is also a history tab that shows in graphic format the flow of packets and attacks in the last minute/hour/day.

Attack Screen

The "Attacks" screen is pre-configured but the user may determine which columns to show in each tab displaying several pieces of information. In the example below, it shows the timestamp, severity as rated by BlackICE, the intruder's source IP, the attack, the parameters, number of attempts and intruder's name. Following the example above, "CXNVICT" used a TCP scan 19 times against ports 31, 1001, 1234, 6400, 6670, 7547, 12345-12346, 20000, 2003, 2734,30100 and 31337 using NetBus, NetSphere, Sub_7_2 and Sub_7. (Only part of the parameters is seen in the screen shot.)



Attack Logs

BlackICE's attack logs are in Microsoft Excel spreadsheets with the same information contained within the attack screen. The spreadsheet allows the user to sort on each column to seek repeat attacks in text format. A sample of some attack logs is below.

	Time	Attack	Intruder IP	Intruder	Parameter	
59	2000-07-16 00:42:36	TCP OS fingerprint	216.2.176.162	www.hitb.co.za	port=53&flags=SF&options=	1
39	2000-07-08 15:46:15	TCP port probe	207.96.220.14	ppp207.ivic.qc.ca	port=6346	4
59	2000-06-25 07:05:07	SubSeven port probe	63.197.240.210		port=1243&name=Sub_7	2
39	2000-06-25 05:38:37	UDP port probe	24.161.48.240	cm-24-161-48-240.nycap.rr.com	port=1051	5

Benefits

- Provides intrusion detection.
- Requires little technical knowledge.
- Provides back trace of intruder if necessary.
- Very good documentation.

Problems

- There is an on-going debate as to whether it interfaces with Norton Personal Firewall on the same desktop.
- Evidence Logs require a third party vendor product to access them.

Comparison of these products

All three products provide secure firewall protection for the home and road warrior user. Each vendor continues to update current products and produce new ones. It is important to note the version reviewed by any magazine or author to truly understand the capabilities of each firewall when making comparisons. Some articles state that BlackICE only monitors inbound traffic, true of older versions.

I tested BlackICE with *ShieldsUP!,* a port probe, with Norton Personal Firewall disabled on the same pc. Then I tested just Norton with BlackICE disabled and finally with both running. The results showed that BlackICE protected with stealth all ten tested ports but one, port 113, while Norton resulted in three ports showing "closed" instead of "stealth." Running together, the results mirrored those of the BlackICE test results. BlackICE put two of Norton's "closed" ports under "stealth" protection.

While writing this paper, I noticed that Zone Labs now offers another firewall product called ZoneAlarm Pro. This product was not reviewed here. Zone Labs claims this firewall provides complete, customizable control. It does not replace ZoneAlarm v2.1.

The true value of configuration ability is tied to the user's skills. There is a product for everyone on the market today. Norton Personal Firewall is an expert's friend and BlackICE a novice's, ZoneAlarm suites a middle audience.

Logs come in various forms across these three firewalls. Norton and ZoneAlarm provide easy text logs but do not provide more information for tracing an attack. BlackICE traces well and if the user is not using WIN9x, has easy access, with use of a third party product, to evidence logs. BlackICE does provide its attack log in text through Microsoft Excel.

	Norton Personal Firewall 2.0	ZoneAlarm 2.1	BlackICE 2.1
Price	Approximately $50	Free download to individuals and non-profits	Approximately $40
Type of firewall	Application level	Application level	IP level
Configurability	High	Medium	Minimal
Settings	High, Medium (default) and Minimal	High (default), Medium and Low	Paranoid, Nervous, Cautious (default) and Trusting
Updates	Uses Symantec's	User may enable checking for	User can enable checking for automatic updates.

	"Live Update"	automatic updates	Icon lights to indicate available.
Log access	In text format	In text format	Event logs in text format Evidence logs require third party software
"How to use manual"	Comes with a manual. More information within application.	Online FAQ	Downloadable pdf format very informative
Accepts a "Trusted" IP Address	Yes through firewall rule	Yes in the security settings panel	Yes in intruder screen
Alert window for *immediate* rule configuration	Yes	Yes	No
Compatible OS	Windows 2000, Windows NT, Win9x	Windows 2000, Windows NT, Win9x	Windows 2000, Windows NT, Win9x
Stealth mode	Yes it claims, *ShieldUp!* test scan for this paper showed otherwise.	Yes (default) (not tested by *ShieldsUp!*)	Yes (click on box)

Bibliography

Angelica, Amara D. "Who's Probing Your Ports?" Techweek. 24 July 2000. URL: http://www.techweek.com/articles/7-24-00/beta.htm 17 August 2000.

Boran, Sean. "Personal Firewalls/Intrusion Detection Systems: An analysis of mini-firewalls for personal use." SecurityPortal. 17 July 2000. URL: http://www.securityportal.com/cover/coverstory20000717.html (17 July 2000).

Boyle, Padriac. "ZoneAlarm." ZDNet. 19 May 2000. URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2571337,00.htm 17 August 2000.

Broughton, John. "Cable modem and DSL security issues and solutions." April-May 2000. URL: http://istpub.berkeley.edu:4201/bcc/Apr_May2000/sec.dsl.html 12 August 2000.

Gibson, Steve. ShieldsUp. 2000. URL: http://www.grc.com 19 August 2000.

Hess, Donald, Trish et al. Symantec Service and Support. "Internet Security detects ME trying to hack ME." 9 August 2000. URL: http://servicenews.symantec.com/cgi-

bin/displayArticle.cgi?article=8540&group=symantec.support.win9x.nis.security&mini_version=npf%2D2&next=150&product=npf&product_name=Norton+Personal+Firewall&version_name=2.0& 12 August 2000.

Hess, Donald and Morris Joseph. Symantec Service and Support. "Distinction between two kinds of blocks?" 24 July 2000. URL: http://servicenews.symantec.com/cgi-bin/displayArticle.cgi?article=7552&group=symantec.support.win9x.nis.security&mini_version=npf%2D2&next=450&product=npf&product_name=Norton+Personal+Firewall&version_name=2.0& 12 August 2000.

Keizer, Gregg. CNET Review. "Norton Internet Security 2000." 3 May 2000. URL: http://www.cnet.com/software/0-3752-7-1773453.html?tag=st.sw3752-7-1773431.txt.3752-7 (13 August 2000).

McAfee. 31 January 2000 URL: http://www.mcafee.com/aboutus/press_room/press_releases/pr01310002.asp 22 August 2000.

McLachan, Don and the GIAC Community. "Contacting Host Owners v2.0." SANS Institute. 8 April 2000. URL: http://www.sans.org/y2k/contacting.htm 12 August 2000.

Mcpherson, James. "Network security for the small office." TechRepublic. 3 August 2000. URL: http://www.techrepublic.com/article.jhtml?id=column/r00220000803jim02.htm 17 August 2000.

Network Flight Recorder. URL: http://www.nfr.net/ 22 August 2000.

NetworkICE Intrusions and Vulnerabilities Reference Guide v2.01 June 2000 ed. http://www.networkice.com/Docs/Issue_Reference_Guide_21.pdf 19 August 2000.

Pardo, Ed. "Cable Modems and Corporate Security." SANS Institute. 21 March 2000. URL: http://sans.org/infosecFAQ/cable.htm 9 Aug 2000.

Puppet's Place. URL: http://www.dynamsol.com/puppet/nukenabber.html 22 August 2000.

Raikow, David. "Installing ZoneAlarm.' ZDNET. 2 August 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2610364.htm?chkpt=zdnnp1ms 17 August 2000.

Rattfnk1. "Possible Bug." Symantec Service and Support. 17 August 2000. URL: http://servicenews.symantec.com/cgi-bin/displayArticle.cgi?article=9098&group=symantec.support.win9x.nis.security&mini_ 20 August 2000.

Schultz, Beth. Ten top companies to watch." Network World. 24 April 2000. URL: http://www.nwfusion.com/nw200/2000/nw200-tencompanies.html?nf 19 August 2000.

Sengstack, Jeff. "Make Your PC hacker-proof." PCWORLD. September 2000. URL: http://www1.pcworld.com/heres_how/article/0,1400,17759,00.html 12 August 2000. Signal 9 Solutions. URL: http://www.signal9.com 22 August 2000.

Symantec Service and Support. Knowledge Base. "How to block a specific computer from accessing yours." 29 June 2000. URL: http://service1.symantec.com/SUPPORT/nip.nsf/docid/2000012114041136&src=w 12 August 2000.

Symantec. "Norton Personal Firewall Users Guide Online" 23 May 2000. URL: http://www.symantec.com/techsupp/files/nis/nis2000.html 12 August 2000.

Symantec Service and Support. Knowledge Base. "How Norton Internet Security protects your computer from attack." 27 June 2000. URL: http://service1.symantec.com/SUPPORT/nip.nsf/docid/2000011014313436 12 August 2000.

Symantec Service and Support. Knowledge Base. "How to "stealth" a port with Norton Internet Security or Norton Personal Firewall." 11 August 2000. URL: http://service1.symantec.com/SUPPORT/nip.nsf/5a5e9c8a8ac2ec3c882568f60060f23a/2d50a9f9d1f4b3fa882569290064a60a?OpenDocument&Highlight=0,how,to,stealth 12 August 2000.

Symantec Service and Support. Knowledge Base. "NIS statistics show Trojans were permitted to your system." 11August 2000. URL: http://service1.symantec.com/SUPPORT/nip.nsf/5a5e9c8a8ac2ec3c882568f60060f23a/62e885a2c6d6856d852568af0052aff3?OpenDocument&Highlight=0,NIS,statistics 12 August 2000.

Waring, Becky. "Zone Labs ZoneAlarm 2.1" cnet. 1 August 2000. URL: http://www.cnet.com/software/0-3752-7-2342093.html?st.sw.3752-7-2342092.txt.3752-7-2342093 17 August 2000.

Zone Labs. 1999, 2000. URL: http://www.zonelabs.com/zonealarmnews.htm 17 August 2000.

Zone Labs. "FAQ." 2000.
URL: http://www.zonelabs.com/faq.htm 19 August 2000.

Zone Labs. "General questions about Zone Labs and our products." 1999, 2000. URL: http://www.zonelabs.com/faq_gen.htm 19 August 2000.

Zone Labs. " Quick Support." 1999, 2000. URL: http://www.zonelabs.com/support_quick.htm 19 August 2000.

Zone Labs. " How to use ZoneAlarm and how it protects." 1999, 2000. URL: http://www.zonelabs.com/zonealarm/za_faq_using.htm 19 August 2000.

Zone Labs. "Details on how ZoneAlarm and our technology works." 1999, 2000. URL: http://www.zonelabs.com/zonealarm/za_faq_details.htm 19 August 2000.

Zone Labs. "Configuring and installing ZoneAlarm." 1999, 2000. URL: http://www.zonelabs.com/zonealarm/za_faq_config.htm 19 August 2000.

Zone Labs. "New ZoneAlarm Pro." August 2000. URL: http://www.zonelabs.com/zap.htm 19 August 2000.