Global Information Assurance Certification Paper

Protecting your Home Computer from the Internet, Can You Keep the Heat Out?

Robert Ashworth

December 9, 2000

Introduction:

Whenever someone mentions computer security or network security most people immediately think of either viruses or hackers (crackers) or both. As emerging technologies gain footholds in the global information infrastructure, they often come with a price. This price is the new technical vulnerabilities that often emerge from upgrades and service packs. One of the key technologies used to protect internal trusted networks from crackers, and to some extent malicious software (e.g., viruses), is a firewall. Corporate enterprises can afford top-of-the-line robust firewall systems guarding Internet accesses for their entire network at known entry points. These separate the important corporate equipment from the Internet using bastion hosts, inner screening routers, and outer perimeter routers, often in addition to other security tools. Meanwhile, the individual at home connecting through his Internet Service Provider once was all alone and vulnerable while browsing the Internet. However, when home access speeds increased with the introduction of Integrated Services Digital Network lines, Digital Subscriber Lines, and cable modems, so did the potential interest a cracker might have in accessing an unsuspecting home system. Today, various vendors have come up with low-cost and even no-cost solutions to aid the home user with both high and low speed communications lines to monitor electronic traffic to allow use of the Internet, yet protect the individual's home systems. This is accomplished with personal firewalls that run on home computers. This paper explores some of the more popular personal firewalls, features that set them apart from the rest, and summarizes some published test comparisons. Although there are some hardware appliances available, this paper considers only the more popular software personal firewall choices available at the time of this writing.

What are they?

A network firewall is basically a method of protecting the internal (trusted) network resources from detrimental electronic threats originating from the external (untrusted) network by disallowing all network traffic from entry that was not pre-defined as "allowed access". However, there are other uses that firewalls can employ. For example the firewall could be placed to protect a single important host instead of a "trusted" network, and can hide the internal configuration with network address translation. This example may be implemented by the home user through employment of personal firewalls. While it is possible for home users to employ bastion hosts to protect the key computer resources in their home, most users will likely use cost-effective software solutions that actually run on their main home host computer that serve to mitigate risk enough to provide them adequate protection. Personal firewalls do just that, but can be configured to only allow explicitly permitted traffic, just like their more robust (network) cousins. Most personal firewalls do sense, alert, and halt attempted Internet connections that were not explicitly permitted. In this monitoring some are considered basic intrusion detection systems, as they do look for certain malicious things, such as Virtual Basic Script. However, they are not full "intrusion detection systems" as they do not watch for anomalous conditions or identify intrusion signatures, but rather analyze traffic against a rule-set by identifying what traffic is specifically permitted to come in and what traffic is allowed out. The "what traffic" analyzed can be based on specific Internet Protocol addresses, certain services or ports, or certain application data.

Imagine going away for the weekend, or turning in at night. Locking your front door while leaving your back door unlocked and ajar is not very secure. Similarly, implementing a firewall at an electronic entry point and leaving another open is also not very secure. Most home users, though, have a single electronic entry point that is connected directly to their computer. Therefore, companies have come up with low-cost software solutions to monitor communications to and from those home workstations and to provide a degree protection from unauthorized electronic communications. Just as the robust enterprise firewalls are not foolproof, these low-cost solutions are far from perfect. Imagine a door with many keyholes (ports), any of which can open the door, but each is normally used for a specific purpose. The main problem with this is that intelligent people work hard to find ways to beat the mechanism. One way is by testing all the key holes in the lock while jiggling the doorknob, eventually it is possible for unauthorized visitors to gain access by simply locating the right accessible keyhole (port) with the right pick to access a flaw in the tumblers to gain them access. This is especially true since upgrades to the door sometimes create unknown changes to the "tumblers".

What's the difference?

The cost of the products varies from no-cost for personal home use up to $300. This paper will take a brief look at features of a dozen offerings that are all below $60. We will start with 4 that are free for home use.

"Freeware" Personal Firewalls

Alladin's e-Safe Desktop was found by Sean Boran to not stop attacks during the initial 14-day learning period. He also felt that the wizard questions were very too technical for the average user. It comes with a sandbox anti-vandal capability for active content/mobile code issues and providing a basic access control list. It can also filter for certain words, allowing it to be used somewhat as a parental "guard". Beta version 3 is out with enhancement to the existing features; however, both versions 2.2 or the 3.0 Beta are 10 Megabytes, which is a long download for a dial-up connection.

Nukenabber is also readily available as freeware. However, as Personal Firewalls go, it is limited in its capabilities, allowing only 50 ports to be selected for monitoring and logging.

Tiny Software advertises that their Tiny Personal Firewall has simple setup and configuration. It contains an application filter to help protect against Trojan Horse "spyware" (e.g., BackOrifice2000, NetBus, or Sub7). Additionally, the optionally password-protected audit log information can be sent to a remote "syslog" server to protect it from deletion or modification, and allows address-based filtering rules to be created by the user.

ZoneLabs' Zone Alarm provides three security levels (the highest is recommended) for each of 2 "zones" (Local and Internet). The system is "stealth" (cannot be detected) when the Internet level is set "High". This is the product that I use, as it returns much more than the cost and is easy to install. It works by allowing external communication only to applications that the user has specifically permitted. Each time a new application requires Internet access, ZoneAlarm asks the user if it is permitted, and also allows you to avoid being asked again for that application with a checkbox that makes your decision semi-permanent (until you modify this in the rule list). Thus, firewall rules are created as you go. It allows sharing of specific files and provides application-level filters to thwart Trojan Horse spyware. It also has an emergency "Stop" that can lock out all traffic, as well. To combat e-mail attachments it also has a feature to protect the user from Virtual Basic script files (like the IloveYou virus and its copy-cats).

Low-Cost Commercial Personal Firewalls

BlackICE Defender advertises that it has simple setup and configuration, this was seconded in various independent articles. It comes with easy-to-understand color-coded alerts, can do comprehensive back-trace and identification of the attacker, has evidence logging, and using their advice feature, it can do a web-lookup of an attack signature. Although it is very popular, both Michael Bensimon (2) and Warren Ernst (12) reported in their articles that it's drain on system resources and throughput was inadequate in comparison to its competitors.

ConSeal PC Firewall. Similar to many of its competitors, this system allows you to insert Firewall rules as you encounter new access requirements, or you can configure them manually; however, the optionally password-protected rule-set is more specific, allowing the user to create rules on IP addresses, services, devices, or any resource or source.

McAfee Firewall 2.11. This was originally released as "ConSeal Private Desktop" from Signal 9. Application communications rules are set up as they appear, similar to ZoneAlarm. However, this system is very flexible and difficult to manage and thus, like eSafe, is considered not appropriate for the inexperienced user. Monitoring both inbound and outbound traffic, it can identify and thwart Trojan Horse "spyware". The resource drain was found by Bensimon (2) to be minimal, and thus adequate.

Symantec's Norton Personal Firewall 2000 2.0 is quoted to have a low CPU utilization and throughput reduction, as well as good overall capabilities. This Firewall faired very well in the rankings, although was not considered as adjustable as its competitors. This software can block active content (mobile code) such as ActiveX controls and Java applets. Additionally, unlike ZoneAlarm in its "High" security setting, by default Norton Personal Firewall 2000 remains visible to the Internet. Warren Ernst's (12) tests resulted in a very good performance rating.

Symantec's Norton Internet Security 2000 Family Edition 2.0 is more robust than Norton Personal Firewall 2000. Bundled with anti-virus software, it includes password-protected parental and privacy configuration features for an all-around Home "Internet Security 2000" protection package.

Sharp Technology HackTracer advertises easy installation, which was agreed upon by independent reviewers. It creates evidence logs upon an attack, and the provided "NeoTrace" software can trace back to an intruder. Michael Bensimon's (2) efficiency tests of this system resulted in very low system resource draw.

Sygate Secure Desktop 2.1 comes with many of the key features found in competitors; however it appears that it is not as powerful in certain features as many others. However, it does have some features that are reminiscent of

much more robust Firewalls. You can create an access list of trusted IP addresses. It has 5 configurable levels of security from "Off" to "Ultra High Security". It permits the user to set different protection modes during particular times of the day or due to inactivity. It also allows the user to set up e-mail alerts to any address. Additionally the Sygate Online Scan service allows you to see which ports are open.

ZoneLabs' ZoneAlarm Pro comes with all the features of the freeware version. In Michael Bensimon's (2) article, it was found it to have a minimal draw on system throughput and resources. In addition, it comes with a Network Address Translation capability, password protection for your settings, and more enhanced configuration features as well as much more robust e-mail attachment review.

Analysis of Research:

Both Tiny Personal Firewall and ZoneAlarm freeware Personal Firewalls include prompts when they detect unknown activity, allowing the user to set up firewall rules list as he/she continues to use the device online. Employing too much security isn't always a good thing, as I found out when I loaded ZoneAlarm and Tiny Personal Firewall in tandem. I had installed them both with the hopes that some exploit that made it through one would be thwarted by the other. The result was a system fully electronically secure from remote threat agents (i.e., one that did not communicate at all).

Almost all of the products did have some good strong capability according to the research, much of which was similar throughout. ZoneAlarm Pro 1.0 was ranked the top of those tested by Warren Ernst (12), and also was given top kudos by Steve Gibson (13) and Jube Shiver (18) in their articles. Michael Bensimon (2) gave top rankings to three products, ZoneAlarm Pro, BlackICE Defender and HackTracer. From the results of the published comparisons and tests that were reviewed, ZoneAlarm Pro appears to be the overall contender of choice, although most seemed to have useful features. I would surmise that since ZoneAlarm Pro doesn't offer too much in addition to its freeware brother, that of the freeware Personal Firewall contenders ZoneAlarm is the likely welterweight champion.

References:

(1) Armstrong, Larry. "Back Off, Hacker." 28 February 2000. URL: http://www.businessweek.com:/2000/00_09/b3670174.htm (31 Nov 2000).

(2) Bensimon, Michael. "Review: Software Firewalls for Personal Protection." 17 November 2000. URL: http://www.8wire.com/headlines/?AID=1384 (6 Dec 2000).

(3) Boran, Sean. "An Analysis of Mini-Firewalls for Personal Use." 28 August 2000. URL: http://www.securityportal.com/cover/coverstory20000717.html (31 Nov 2000).

(4) Boran, Sean. "Personal Firewalls Test: BlackICE Defender." 29 October 2000. URL: http://securityportal.com/articles/pf_blackice20001023.printerfriendly.html (31 Nov 2000)

(5) Boran, Sean. "Personal Firewalls Tests: Tiny Personal Firewall." 14 November 2000. URL: http://securityportal.com/articles/pf_tiny20001114.printerfriendly.html (31 Nov 2000)

(6) Boran, Sean. "Personal Firewalls Test: McAfee Firewall." 29 November 2000. URL: http://securityportal.com/articles/pf_mcafee20001011.printerfriendly.html (31 Nov 2000)

(7) Boran, Sean. "Personal Firewalls Tests: Sygate Personal Firewall." 29 November 2000. URL: http://securityportal.com/articles/pf_sygate20001112.html (31 Nov 2000).

(8) Boran, Sean. "Personal Firewalls Test: PGP7." 30 November 2000. URL: http://securityportal.com/articles/pf_esafe20001023.printerfriendly.html (31 Nov 2000).

(9) Boran, Sean. "Personal Firewalls Tests: ZoneAlarm Pro." 30 November 2000. URL: http://securityportal.com/articles/pf_zonealarmpro20001108.printerfreindly.html (31 Nov 2000).

(10) Bowen, Eric. "Windows 2000 SP1 Thwarts ZoneAlarm and BlackICE Defender." 14 August 2000. URL: http://www8.zdnet.com/zdhelp/stories/main/0%2C5594%2C2614038%2C00.html (31 Nov 2000)

(11) Dvorak, John. "Paranoia and Personal Firewalls." 31 March 1997. URL: http://www.zdnet.com/pcmag/insides/dvorak/jd970331.htm (31 Nov 2000).

(12) Ernst, Warren. "Seven Solutions for Safe Systems." 21 September 2000. URL: http://www.winmag.com/reviews/software/2000/09/0921_b.htm (6 Dec 2000).

(13) Gibson, Steve. "Shields Up! Internet Connection Security for Windows Users." (date unknown). URL: http://grc.com/su-reginding9x.htm (6 Dec 2000).

(14) Hummel, Robert. "It's dangerous out there. A firewall can protect your data from hackers." 5 June 2000. URL: http://www.pcworld.com/hereshow/article.asp?aid=17012 (31 Nov 2000).

(15) Sengstack, Jeff. "Insulate your PC from hackers." 10 August 2000. URL: http://www.cnn.com/2000/TECH/computing/08/10/diy.hacker.proofing.idg/ (31 Nov 2000).

(16) Sheldon, Leemon. "Personal Firewalls." 22 August 2000. URL: http://www5.zdnet.com/products/stories/reviews/0%2C4161%2C2615071%2C00.html (31 Nov 2000). (Includes sub-pages with individual reviews).

(17) Strauch, Joel. "Personal Firewalls Keep Intruders at Bay." 14 July 2000. URL: http://www.pcworld.com/resource/printable/article.asp?aid=17637 (31 Nov 2000).

(18) Shiver, Jube. "Don't Get Burned, Surfers; Personal Firewalls Are Here". 7 September 2000. URL: http://www.latimes.com/business/columns/ereview/20000907/t000084154.html (6 Dec 2000).

Vendor Sites:

Alladin: http://www.ealaddin.com/esafe/desktop/index.asp (9 Dec 2000)

ConSeal: http://www.consealfirewall.com/ (6 Dec 2000)

McAffee: http://www.mcafee.com/myapps/firewall/ov_firewall.asp? (6 Dec 2000)

Network ICE: http://www.networkice.com/ (2 Dec 2000)

Nukenabber: http://www.dynamsol.com/puppet/ (2 Dec 2000)

Sharp Technology: http://www.sharptechnology.com/ (9 Dec 2000)

Symantec: http://www.symantec.com/sabu/nis/npf/ (2 Dec 2000)

Sygate: http://www.sygate.com/ (2 Dec 2000)

Tiny Software: http://www.tinysoftware.com/ (31 Nov 2000)

ZoneLabs: http://www.zonelabs.com/ (31 Nov 2000)