Global Information Assurance Certification Paper

An Example of Employing both a Hardware and a Software-based Personal Firewall in a Private Home

Barb Ann Kupiec
GIAC Security Essentials Certification (GSEC)
Practical Assignment ver 2.0

Abstract

The home PC owner who does Internet browsing and the employee who connects to their Corporate intranet should have basic security awareness. The home PC owner needs protection on their computer system to detect and stop attacks not only coming from the outside but also to prevent others from using their computer systems to launch attacks on other systems. The home PC probably contains sensitive information about finances and is used for Internet shopping. The employee who works from home may be involved in critical Company owned software code or project work. The home PC which is on the Internet should have a personal firewall that protects the home system from attacks coming from the Internet and prevents the PC from becoming a tool to launch an attack going out onto the Internet.

In this report I will state why computer security for the home owner is important and why use a personal firewall. I will explore how a PC and a personal firewall can be attacked and list a couple of Internet attacks the home user might expect. I will give justification why a double personal firewall that is both software and hardware based gives added protection over a single personal firewall. A brief overview of the two firewalls is given with their basic installation features. My own configuration using ZoneAlarm Pro 3.1 and the Linksys Router (or Linksys BEFSX41 EtherFast Cable/DSL Firewall Router) will be tested. As a conclusion, I will explore what other measures a home PC user might use to protect their PC security.

Reasons for Home Computer Security

Why should the home PC user be concerned about computer security? The home Internet user is just as vulnerable as major corporations in being attacked by hackers and viruses. A virus is a program that when runs inspects its environment and copies itself into other programs. In today's world, a antivirus scanner on the home PC is not enough. Unfortunately, many home users are not aware that their home PC is being attacked and many do not know what a firewall is. Their reliance on their Internet Service Provides (ISP) will not protect them in all cases and many home users are not aware of this.

Listed below are some Internet sites to help raise the security awareness for the home user. They are tailored to the home PC user.

1. www.cert.org (section for New & Home users; good articles in Home Computer Security and Tech Tip for Home Network Security)
2. www.microsoft.com/security (section for the home user)
3. your personal firewall home web site. In my case, it is the www.zonelabs.com and www.linksys.com sites.
4. your personal virus protection. In my case, it is the www.mcafee.com/ site.

The above CERT Home Network Security article answers questions and concerns for the home computer user. The article answers the question: What is computer security?

> "Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done."[1]

Computer security for the home owner is important The home internet user is a prime target for computer crime. Antivirus scanners are only one line of defense. The best defense is educating the home user.

Reasons for a Personal Firewall

Another line of defense is the personal or home firewall. The Microsoft Security web site (http://www.microsoft.com/security/) has an article on seven steps to help the home user in home computer security[2]:

1. assess your risk
2. use antivirus software
3. keep your software up-to-date
4. check your security settings
5. use a firewall
6. create strong passwords
7. conduct routine security maintenance

The article also states how a firewall helps protect your computer:

> "Firewalls help safeguard your computer by enforcing restrictions on incoming traffic. Firewalls can also help mask your computer's

> identity, so hackers' attempts to probe or scan your computer cannot return the type of information that makes it easy to invade."[2]

A search on the Internet on personal firewalls yields articles that give the home user opportunity to explore the advantages of a personal firewall:

Bahadur, Gary. "PERSONAL FIREWALLS: Personal Firewalls Under", July 2002, **http://www.infosecuritymag.com/articles/july01/cover.shtml** .

"Home PC Firewall Guide", http://www.firewallguide.com/ .

Nance, Barry. "Four Personal Firewalls Reviewed", May 28, 2001, **http://www.computerworld.com/securitytopics/security/story/0,10801,60821,00.html**

http://directory.google.com/Top/Computers/Security/Firewalls/Products/Personal_Firewalls/ (24 articles on Personal Firewalls).

There are also articles for the more knowledge-seeking user. Gary Smith's "A Brief Taxonomy of Firewalls – Great Walls of Fire"[3] covers in more technical detail how a firewall works. For instance, the design of the network operates around a layered model called the Open Systems Interconnection (OSI) model and is composed of seven layers beginning with layer 7: application, presentation, session, transport, network, data link, and physical. The network layer or layer 3 is the lowest layer at which a firewall operates.

> "At this level, a firewall can determine if a packet is from a permitted source but cannot be concerned with the contents of the packet. Firewalls that operate at the next layer, the transport layer, are able to make more sophisticated decisions about accepting or denying packets because they know more about a packet. At the application layer, firewalls have even more information available and can use even more stringent criteria to permit or deny packets."[3]

One definition of a firewall or network firewall[4] is a "system or combination of systems that enforces a boundary between two or more networks." Hackers seek information whether it be your credit number or if you connect to your company's intranet site. I can access my company's intranet through my high-speed cable modem using RoadRunner as my ISP. My multi-national company makes it mandatory to have a firewall installed on my home PC, and it recommends several firewall products. My company also does a port scan to ensure that I am complying to the terms of agreement stated in the user request form for cable modem intranet access. Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running or listening. For hackers, identifying listening ports is critical to determining

the type of operating system and applications in use.[5] However, it was still up to me to educate myself on the use and capabilities of my firewall.

Many home users don't have a clue as to what a 'port' refers to. Think of a port as the door to your PC. Each port has a number. Many of your favorite software packages have specific ports they use. FTP software usually connects to FTP servers using port 21. A firewall can block port 21 so your PC is protected from FTP attacks.[6]

A home/personal firewall will attract buyers if it is easy to install and configure. A home user should be able to install, go with the defaults of the firewall and forget about it. A minimal of user interaction is a desired trait. More than two dozen personal firewalls are on the market, some even free.

I looked at several basic features for a personal firewall.[7] I compared these features to the ZoneAlarm and Linksys firewalls I configured.

- The firewall should stop external attacks such as port scans, SYN floods, and IP spoofing. A SYN flood starts the TCP three-way handshake by the attacker sending a SYN packet to the victim, the victim responds with a SYN/ACK but instead of the attacker replying with an ACK, the attacker sends a new SYN to open a different connection. Within a short time the victim's memory is used up and the PC ceases to function. IP spoofing is the act of inserting a false sender IP address into an Internet transmission in order to gain unauthorized access to a computer.
  - The Linksys Router held its own against several online port scans.[8] It blocked SYN attacks, ping of death, and protects against IP spoofing. Note: Linksys issued a firmware fix (1.43.3) to correct a TCP SYN scan tests and this is available at the Linksys download site. Ping of death is an example of a fragmentation-based denial-of-service (DoS) attack. A large Internet Control Message Protocol (ICMP) packet that is fragmented into so many pieces is received and the OS reassembling them overflows and crashes.
  - ZoneAlarm blocked all port scans. I tested this with various port scanners and in every case I kept getting pop up alerts that access was blocked. ZoneAlarm's Program Control monitors all outbound traffic to prevent rogue programs from transferring valuable data to a hacker.

- Internal threats are stopped before other PCs on the network are infected. Malicious software (or malware) might attempt to make unauthorized external connections. Worms and Trojan horses are halted before they announce themselves that this PC has been infected. A worm is a program that copies itself over computer

networks infecting programs and machines in remote locations. A Trojan horse is an innocent looking program that does malicious work behind the scenes.

- The Linksys Router lacks application-specific controls. It can block incoming or outgoing traffic at scheduled times and filter content by URLs or keywords but this is not part of the default.
- ZoneAlarm's MailSafe protects the PC from malicious code and virus according to the E-mail Protection tab. MailSafe quarantines these attachments and prevents them from running on the PC.

- Firewalls should install easily and autoconfigure themselves with basic security. Checks for newer versions of the firewalls should be automatic. I had no problem in installing ZoneAlarm Pro and the Linksys Router. Both autoconfigured themselves with basic security.
  - The Linksys Router has no automatic scan for updates. The web site hosts a firmware update selection.
  - ZoneAlarm has a selection to automatically scan for updates.

- A personal firewall has some application control built into it. Applications that only the user and the firewall have approved can pass through the firewall. This trait can show the user either just the application filename or a list of application filenames contained in its database. Added to the list of applications in the database can be a checksum feature, which checks the application to see if it was legit or not. If the user accepts or a match in the database is found, a connection is made.
  - The Linksys Router has no application control built into it. It does have a port forwarding feature which is blank upon installation. Port forwarding can be used to set up public services on the internal network. When users from the Internet make certain requests on the router, they will be redirected to the specified IP.
  - In default medium setting, ZoneAlarm only allows Internet Explorer traffic onto the Internet; it prompts me for every other program. As I use applications, they get listed in a selection tab where I can add, delete or edit their security level.

- The firewall has a protection zone with different levels of security that the user can select.
  - The Linksys Router has no zones with different levels of security.
  - ZoneAlarm Pro has trusted, internet and block completely zones. I have HIGH for Internet Zone to protect my PC from the outside world; MEDIUM for the Trusted Zone so I can determine which PCs can see my resources; and a Blocked Zone where no communication is allowed.

- A log is kept recording the event's date and time and a brief description. A pop-up window should appear on the desktop signaling an attack.
  - The Linksys Router has a log where a user can see incoming connections (which lists source IP and destination port number) and outgoing (which lists LAN IP, destination URL/IP and service/port number). There is no popup window.
  - For each connection, ZoneAlarm's log gives me a security rating of high, medium or low, source/destination IPs, time/date, action taken and source/ destination DNS. It provides me with a popup window when an attack is made.

In summary, home firewalls cannot only protect the home user but their company as well. They can stop Internet attacks and protect the user's private information.

How to Attack a Firewall

There are different external attacks.

- A hacker seeks knowledge about a network before launching an attack. The hacker uses a port scan to figure out what services are running on a particular machine. It can be easy to detect this type of attack because few ports should be in active use by a remote computer at any given time. An effective port scan widely used is nmap (http://www.insecure.org/nmap/) by Fyodor.

- Network traffic flood overwhelms an individual PC by flooding it with tens of thousands of network packets. This flooding causes a Denial of Service (DoS) attack where the PC cannot accept any more information and hangs. The ZoneLabs' website (http://www.zonelabs.com/store/content/support) states for DoS: "ZoneAlarm stops generating new alerts after 500 in order to protect you from DoS attacks. It still keeps denying connections. Denial of Service occurs when packets arrive more rapidly than they can be processed. ZoneAlarm responds to the rapid arrival of large numbers of packets by limiting the rate at which alerts are generated."

- Trojan horse programs are used by hackers to trick the user into installing backdoor programs which can allow easy access to your PC. See http://www.cert.org/advisories/CA-1999-02.html. From this article: "A Trojan horse is an apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat."

- Unprotected Windows networking shares can be exploited by intruders. These shares can be leverage to propagate viruses or worms. See http://www.cert.org/incident_notes/IN-2000-03.html for an example of the 911 worm first seen in 2000.

- Another attack by viruses and malicious code can be found in email attachments. For one of the best known attachments, see information on W32/Sircam at http://www.cert.org/advisories/CA-2001-22.html. The McAfee web site states: "This mass-mailing virus attempts to send itself and local documents to all users found in the Windows Address Book and email addresses found in temporary Internet cached files (web browser cache)."[9]

As part of the home user's education process to enhance security awareness, several well-known attacks are listed.

- The Microsoft Security web site gives information about the Code Red II Worm (http://www.microsoft.com/security/): "A new variant of the Code Red Worm has been found on the Internet. As discussed in a new advisory from CERT, the new variant installs software that will allow a malicious user gain access to the system and execute commands on it. Clearly, this raises the stakes for infected systems, and reinforces the need for customers operating Windows NT 4.0 or Windows 2000 web servers to protect their systems." The Code Red Worm scans PCs for open port 80 which relates to HTTP (internet) traffic.

- A hacker can gain access to your PC through a program called Back Orifice which can be sent in an email to you and you open the email. "Because it is a Trojan horse, users must install Back Orifice themselves or be tricked into installing it. It can be disguised in a variety of ways and is ostensibly positioned as a 'remote administration tool.' Basically, Back Orifice works as a client-server program, with the intruder controlling the client. Once the Trojan horse is on the user's system, the client (which may be running anywhere on the Internet) can access the affected system with the privileges of the user who inadvertently installed it." (http://www.cert.org/vul_notes/VN-98.07.backorifice.html)

- The well-known Melissa macro virus propagates in the form of an email message containing an infected Word attachment. According to the www.cert.org web site: "Melissa was different from other macro viruses because of the speed at which it spread. The first confirmed reports of Melissa were received on Friday, March 26, 1999. By Monday, March 29, it had reached more than 100,000 computers."

Justification of a Double Personal Firewall

I selected the Linksys Router so I could have two PCs able to connect to the network with one IP address with the security of a firewall. From the articles below, I knew that adding a software firewall would be beneficial. For the home user, it is important to know that there are pros and cons to using just one type of firewall.

An PCMagazine article states: "With software, you must install a firewall on every PC that needs protection, whereas hardware firewalls centrally protect all machines in a network. Because software firewalls run locally, however, they have intimate knowledge of what's happening on systems. A hardware firewall will likely allow any e-mail traffic out over port 25; a software firewall can differentiate between Microsoft Outlook and Trojans."[10] This article also lists the pros and cons of hardware- and software-based firewalls:

Hardware PROs	Software PROs
Inexpensive	Inexpensive
Stops most hackers when used correctly	Stops most hackers when used correctly
Works at the port level	Works at the application level
Can protect multiple PCs	Ideal for one machine with many users
Uses a dedicated secure platform	Convenient for travelers
Nonintrusive	Analyzes incoming/outgoing traffic
Doesn't effect PC performance	
Hides PCs from the outside world	Easy to update
CONs	**CONs**
Can be complicated for beginners	Can be complicated for beginners
Difficult to customize	Doesn't hide PC from outside world
Ignores most outgoing traffic	Can be intrusive
Upgrades only via firmware	Affects PC performance
Creates a potential bandwidth bottleneck	Must be uninstalled in case of a conflict

Scot Finnie in his newsletter[8] stated: "I still believe that firewall software with application controls running on each PC behind NAT/DHCP-based hardware is your safest bet." Finnie reviewed and tested the hardware firewall Linksys BEFSRA1. He noted one drawback if a PC owner uses this as their only firewall—the Linksys router lacks application-specific controls. He suggested using an email-monitoring antivirus program like Norton AntiVirus 2003 and an anti-trojan horse protection software. I agree with his statement that a software firewall is far more configurable. He stateed: "If you're going to rely on hardware only to arm yourself

against hackers malware, you need to be more on the ball about security."[8]

There is interaction between the Linksys Router and ZoneAlarm Pro. The Linksys menu has a selection to incorporate the full version of ZoneAlarm Pro. A press release article[11] states the benefits of a software/hardware firewall involving Linksys®, Trend Micro Inc., and Zone Labs:

> As announced earlier this year, the three leaders joined forces to provide an easy, affordable, and comprehensive way to further protect broadband-connected PCs from Internet intruders and thieves. The result is a specially priced offering of Trend Micro's PC-cillin antivirus software and Zone Lab's ZoneAlarm Pro Internet security utility which enhances the security features of the Linksys broadband router and 802.11b wireless router solutions. The complete broadband solution is designed to strengthen the security of each PC connected to the Linksys Cable/DSL router against security threats including targeted hacker attacks, spyware, Internet-borne Trojan horses, viruses and other malicious code.

I am using a Linksys[R] BEFSRA1 EtherFast 4-port cable/DLS router with a built-in firewall and have purchased the full version of ZoneAlarm Pro 3.1. This provides me with an internal private LAN subnet using 192.168.x.x, and the router has a WAN IP supplied by my ISP RoadRunner. I have a firmware version 1.44.2 for the router in response to several articles testing it.

RoadRunner states clearly in their manual that the subscriber is held responsible for the security of their home network. RoadRunner encourages disabling file and print sharing, use of an antivirus program, and the use of a software firewall product.

ZoneAlarm Pro Overview

I purchased ZoneAlarm Pro 3.1 from Zone Labs as my software firewall. My workstation operating system is Windows 2000. From ZoneAlarm's datasheet on the ZoneLabs web site, some of the features are:

- Enhanced MailSafe which prevents email-borne viruses from opening and spreading to other computers
- Enhanced hacker tracking which pinpoints the origin of an intrusion
- Good logging, alerts
- Pop-up ad control which eliminates annoying pop-up ads
- Cookie control

- Automatic network detection with an easy 3-step wizard that instantly senses new networks for trusted networking and file sharing anywhere

The installation was user friendly and easy. For this initial test I went with the defaults. ZoneAlarm alerted me whenever it blocked Internet traffic. There are three firewall zones. Internet Zone Security is set at high or "stealth mode" where my computer is hidden from hackers; this setting is recommended for the Internet Zone. A setting of medium is recommended for the Trusted Zone where computers on my subnet can see my computer and share resources. The Blocked Zone contains computers and networks that I distrust; I can place data in these zone manually or at the time the alert popup windows comes on my desktop. At any time I can switch from one zone to another.

Another setting is Program Control. This is initially defaulted to medium; a program must ask for Internet access and server rights. ZoneAlarm recommends a medium setting for the first several days to learn and secure your programs. It recommends a high setting after you have used your browser, e-mail, chat and other Internet programs at least once. I am still in the learning mode because I haven't used all my programs for W2K yet. Program Control prevents unauthorized inbound plus outbound connections, stopping rogue applications from transferring your valuable data to a hacker. It keeps Trojan horses and other hacker malware from setting up shop on your computer. Alert Events is set at high to show all alerts and event logging is enabled. MailSafe Setting is enabled. MailSafe protects your computer from incoming e-mail attachments that may contain malicious code or viruses. It quarantines these attachments, preventing them from running without my permission. MailSafe examines the attachment's filename extension. If that extension (in the example at left, .BAT) is in MailSafe's quarantine list, ZoneAlarm Pro changes the filename extension to ".zl*" (where * is a number or letter.) Changing the filename extension quarantines the attachment by keeping it from running automatically.

Linksys Router Overview

I have installed a Linksys^{R} BEFSR41 Etherfast Cable/DLS Router on my home network consisting of two PCs with a connection to my RoadRunner Cable modem. Simply put, a router is a network device that connects two networks together. For this report, I only had one PC running. I installed the router with the default settings. The router uses an advanced stateful packet Inspection firewall. This means that it provides a high degree of security and does not introduce the performance hit that proxy firewalls introduce. Stateful firewalls make decisions on what packets to allow or disallow. The firewall maintains a state table that tracks each and every

communication channel. It is important for the home user because it makes it harder for an attacker to spoof a packet.

The router protects the PCs from ping of death, SYN flood, IP Spoofing and other denial of service attacks. It blocks Java, ActiveX and cookies. It provides a dedicated port for DMZ hosting and acts as the only externally recognized Internet gateway on my LAN. The demilitarized zones (DMZ) Hosting feature is an option. According to the Linksys knowledge web site (http://www.linksys.com/support/default.asp/), demilitarized zone (DMZ) allows one IP address (computer) to be exposed to the Internet. The user should disable file and printer sharing as well as get a software firewall with application rules for using DMZ. I did not enable the DMZ as this was not a default. One drawback is that the Linksys Router lacks application-specific controls, e.g. it will not protect the PC from Trojan horse malware.

The Linksys Router supports remote administration and IPSec Pass Through. The Internet Protocol security (IPSec) protocol is a method of setting up a secure channel for protected data exchange between two devices. IPSec is a widely accepted standard for secure network layer transport. It is usually used to establish virtual private networks (VPNs) between networks across the Internet.

The router has a Network Address Translation (NAT) firewall that protects my PCs from outside intruders and allows me to manage my own private network inside the firewall. NAT is used to masquerade traffic from private local area network to Internet and vise versa. The router configuration utility has a security tab that allows me to enhance security using ZoneAlarm Pro.

The Router uses stateful inspection which automatically detects denial-of-service (DoS) attacks.[12] Stateful packet inspection bumps the level of protection up a bit. "This method looks at some level 4 or presentation level data such as acknowledgment number and sequence number. This makes it harder for an attacker to spoof a packet, pretending it is a reply to an earlier request, and have it get past he firewall."[13]

Tests

I searched the web looking for how to test a firewall. One article from the CERT Security page states[14]: "The most common cause of firewall security breaches is a misconfiguration of your firewall system." For my site I went with all the defaults as one statement from the ZoneAlarm manual stated that changing the defaults could result in unexpected results. Another article listing the top 150 security tools[15] is a good place for a security minded system admin but may be beyond the

comprehension for the home user. I chose a couple of tools used by Scot Finnie[8] in his newsletter which included ShieldsUP, PCFlank, and AuditMyPC.

ShieldsUP. The first test I ran was ShieldsUP by Steve Gibson (http://www.grc.com).

I downloaded and ran the IP_Agent and selected the TEST MY SHIELDS. Both my ZoneAlarm and Linksys Router were operating. I was taken to the grc.com website. Since my IP belongs to the private network 192.168 which was set up by my Linksys Router, the results of the TEST MY SHIELDS test said that I was unreachable from the external public internet. The report stated that my computer is very secure against typical threats and discovery from passing Internet scanners. The port scan reported that port 113 IDENT was 'closed'; all other ports were 'stealth'. Port 113 provides the username/account ID associated with a given port in use on a system, allowing remote systems to detemine which user is responsible for a connection. It is associated with email servers.

PC Flank's Tests (http://www.pcflank.com/about.htm). I tried using the Stealth, Browser, Trojan, and Advanced Port Scanner Tests to test my PC and firewall. I had ZoneAlarm and the Linksys router enabled for all tests. The IP address pointed to my WAN address and not my true LAN IP. The web site states: "Commonly the test fails to determine your true IP address because of you are connected to the Internet through a proxy-server or your ISP uses Network Address Translation (NAT) to share IP addresses." So my Linksys Router would have prevented a hacker from gaining information.

AuditMyPC (http://www.auditmypc.com/). I used this test with both ZoneAlarm and the Linksys Router enabled. When I did the privacy check test from this web site, it showed not only my LAN IP address but also the WAN IP address assigned to me by the router. It also showed whatever was on my clipboard. If I had confidential information on my clipboard, e.g., credit card numbers, I could be in serious trouble. The Security Check did not find any opened ports.

NmapNT (http://www.eeye.com/html/Ressearch/Tools/nmapNT.html). Nmap, a reconnaissance too, gathers information about a PC. I downloaded the software and used it to perform a simple scan, a stealth scan, OS identification and an OS identification and service selection.[16] With both ZoneAlarm Pro and the Linksys Router enabled, I did a simple scan using nmapNT 127.0.0.1. My ZoneAlarm Pro immediately popped open an alert that the firewall has blocked Internet access to a loopback address (127.0.0.1)(ICMP Echo Request (ping) from your computer. This tells me that my system is blocking ping probes. ICMP is used primarily for

network troubleshooting purposes and operates at the network layer. Note: ZoneAlarm kept popping up alert messages all through the various tests. I used the nmapNT –P0 127.0.01 test and the results reported that all my ports are closed. I performed a stealth scan with nmap –sS –P0 –p135 127.0.0.1. The –sS option performs a SYN scan and the –p option specifies the port to scan which in this case is tcp. The test reported port 135/tcp is in a filtered state with loc-srv service. The test to perform an OS identification, nmapnt –sT –O 127.0.0.1, showed all my ports closed. The –O option attempts to perform OS fingerprinting by analyzing the predictability of the sequence numbers returned from the target device. The last test was for service selections can (nmapnt –sS –p143 –O [IP]. Again the ping probes were blocked.

Security Beyond the Firewall

I also took measures to use the security features built into W2K platform. I formatted my W2K partition using NTFS which gives me file level permissions. I disabled accounts like the Guest account. I set local policies to enforce a 7-character complexed password. I renamed the local administrator account. I disabled file and print sharing since I do not need to share my PC's resources beyond my Internet connection. I removed the Everyone group from both share and NTFS permissions. My lockout policy states a lockout after 3 attempts. I set up auditing to inform me of all failed attempts and successful logon attempts. My company provides its employees with a home version of an anti-virus program. I have installed it and I check for updates on a monthly basis. One article from PCMagazine[10] lists advice even a home user can utilize, such as:

- Check for patches
- Check for browser configuration by running Qualys's Free Browser Checkup (http://browsercheck.qualys.com). I ran this program and among other things, it discovered what OS I was running, my WAN IP address, and my host name.
- Try the Microsoft Baseline Security analyzer, a free download for windows users. This will scan for common system misconfigurations in such products as Windows 2000 and scan for missing security updates. I ran this, and the report showed what was scanned, result details, and how to correct. I had a number of findings listing updates that needed to be downloaded. Another finding is that it found that my C: drive was configured as FAT32; this is where my Windows 98 is located (my system is dual-booted).
- Turn off services you don't need
- Don't open e-mail attachments from strangers

Summary

I feel confident that having the Linksys Router with the NAT firewall and the ZoneAlarm software firewall along with my antivirus program is providing me with the most security protection. I have the ability to add more PCs to the router using a private network IP address scheme and have one IP address connecting to the Internet. It is still up to the individual home user to monitor for updates, keep abreast of major security attacks, carefully read and understand all alerts that pop up on the screen, and do a periodic check of the system.

References

1. CERT[R] Coordination Center, Software Engineering Institute, Carnegie Mellon University, "Home Computer Security", 2002, http://www.cert.org/homeusers/HomeComputerSecurity/.

2. "7 Steps to Helping Personal Computing Security", Security and Privacy for Home Users, April 2, 2002, http://www.microsoft.com/security/articles/steps_default.asp.

3. Smith, Gary. "A Brief Taxonomy of Firewalls – Great Walls of Fire", SANS Institute Information Security Reading Room, May 18, 2001, http://www.sans.org/rr/firewall/taxonomy.php/ .

4. NSA Glossary of Terms Used in Security and Intrusion Detection, http://www.sans.org/resources/glossary.php.

5. Scambray, Joel; McClure, Stuart; Kurtz, George. Hacking Exposed. Second Edition. New York: Osborne/McGraw-Hill, 2001, p 43-44.

6. Gralla, Preston. How the Internet Works, sixth edition, "How Personal Firewalls Work", Indianapolis: QUE, 2002, p 276.

7. Grimes, Roger A. "Personal Firewalls. A look at six popular firewall products for Windows machines," Security Administrator, July 2002, http://www.secadministrator.com/Articles/Index.cfm?ArticleID=25348&pg=1/ .

8. Finnie, Scot. "Review: Linksys's Firewall Router", vol. 2, issue no. 35, November 25, 2002, , http://www.scotsnewsletter.com/35.htm/ .

9. Virus Profile on W32/SirCam, http://vil.mcafee.com/dispVirus.asp?virus_k=99141&/ .

10. (Karagiannis, K.; Sarel, Matthew D. "Keep Hackers Out: Part One, Personal Edition, PCMagazine, November 19, 2002.

11. Press Release, "Linksys, Trend Micro and Zone Labs' Complete Broadband Internet Security Solution is Now Available For Home and Office Networks," September 26, 2001, http://www.linksys.com/press/press.asp?prid=53/ .

12. Senner, Lisa. "Anatomy of a Stateful Firewall," SANS Institute Information Security Reading Room, May 9, 2001, rr.sans.org/firewall/anatomy.php

13. Mallet, Fred. "Firewall Terminology", Win2000 Tips & Newsletters, July 23, 2001, http://searchwin2000.techtarget.com/tip/1,289483,sid1_gci787704,00.html?FromTaxonomy .

14. "Test the firewall system. A practice from the CERT^{R} Security Improvement Modules", http://www.cert.org/security-improvement/practices/p060.html/ .

15. TOP 50 Security Tools, March 22, 2002 http://www.insecure.org/tools.html .

16. Cole, Eric; Newfield, Mathew; Millican, John M. GSEC Security Essentials Tookit, SANS Press, 2002.

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
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
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
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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