Global Information Assurance Certification Paper

Resubmission
SANS Security Essentials GSEC Practical Assignment (Version 3.1)
Diane Berens
February 15, 2002
TITLE: Firewalls: Protecting Your Personal Information

INTRODUCTION

When deciding on a firewall for your personal computer, many factors come into play. Most users are not aware of the questions that need to be answered before selecting the right firewall. For example, why are firewalls so important, why personal computers need firewalls, what to look for in purchasing a firewall, what is a firewall, hacking trends, requirements of a firewall, will my firewall protect my computer against viruses, and what ports are safe to pass through a firewall. Users should shop around and look at the firewalls that are available for their personal computer. There are many good firewalls on the market. Two of the best selling firewalls are BlackICE Defender 2.9 and ZoneAlarm Pro Firewall Version 2.6. Considering all the pros and cons of both firewalls, ZoneAlarm would be my choice because of the password-protection capability. But Freeware and Shareware should also be considered in the ever-growing firewall market.

Corporate and personal information stored on computer systems that are in any way connected to a communications network is information at risk of being stolen, corrupted, or compromised. In today's electronic commerce era, security is a concern for every person using data communications whether private, public, intranet, or internet. Nothing is safe any longer. The Internet has opened up opportunities and possibilities for personal users, small businesses, and large companies that were unheard of a few years back. The explosion of on-line business is a good thing; but there are negative drawbacks, primarily private information is no longer secure. Companies and individuals are constantly looking for ways to keep their private data away from the prying eyes of others. There will always be a market for applications to guard the personal computer from a hacker's intent on breaking into a computer. In my opinion, the proper and consistent use of a firewall is essential in today's information dominant environment.

WHY DO I NEED SECURITY ON MY PERSONAL COMPUTER?

Security is a "must" for the protection of your data. If not properly protected, this data may be accessible by cyber-intruders. The data, stored on your computer, contains sensitive information about yourself and your computer. The following lists examples of personal information that may be stored on your personal computer

- Documents and databases stored on your system – checkbook balancing, documents with your Social Security Numbers, personal correspondence, etc.
- Passwords transmitted across your network – on-line banking; internet services, such as American On Line, HotMail, etc.

- Electronic mail stored in your mailbox – mail from mail order companies, credit card numbers, personal correspondence, etc.
- System files stored in queues and mailboxes – contacts through e-mail, information given to vendors, personal inventory data bases, etc.
- System logs that keep your system running smoothly – firewall logs, anti-virus logs, system administration logs, etc.

Hopefully, the above list provides insight into just how dependent we have become on computers. More importantly, hopefully the reader is more aware of the types of personal information that may be at risk. And perhaps take a closer look at the types of information you store on your personal computer.

The following may happen if your personal computer is unprotected:

- Unauthorized dissemination of information – illegal use of social security numbers, use of your credit cards, etc.
- Changing your data – making changes to your checkbook by using on-line banking, manipulating personal correspondence/databases, changing your passwords, etc.
- Deleting your data – changing your system files, deleting financial information, etc.

WHAT IS A FIREWALL?

The firewall is one of the best security products that you can purchase to protect your personal computer. It is your first line of defense. A firewall is a product that controls access between two networks. The firewall monitors the data flow in and out of the thousands of communication ports that are resident on every computer. By comparing the on-going data flow with known or expected data flow characteristics for a given port, the firewall identifies suspicious activity. It blocks unauthorized users from entering your network while allowing those who do have access to enter. Firewalls are becoming as important as anti-virus protection. And, much like anti-virus software, firewalls require frequent updates as attacks become more sophisticated. Vendors of firewall software make available, through the internet, warnings about flaws in their software and how to update your current versions of the software to make it more secure. Firewalls are no longer cost prohibitive (some can be downloaded from the internet at no cost) and are becoming easier to set up. BlackICE Defender 2.9, which is discussed in this paper, is menu driven by a Wizard that walks you through all the steps in setting up your firewall and takes approximately five minutes to install. By installing a firewall on your personal computer, users have fewer worries about intrusion and damage caused by hackers.

REQUIREMENTS OF A FIREWALL

There are important features that should be on your list of "must haves", when looking for a firewall for your personal computer. The list does not stop here, there are many important features. And as technology and the abilities of the hacker increases, the list will continue to grow.

- Packet flow control - All Internet Protocol packets between two networks cannot be forwarded unless the packets use the firewall system as their destination or original address. In other words, all internet traffic is diverted through the firewall for content/characteristics monitoring.

- A good User ID and password authentication scheme -- The most basic system protection starts with a sound user ID and password scheme. This is also true of firewalls. To ensure continued proper configuration, a solid user ID/password scheme is essential.

- The firewall must eliminate the telnet "open" command. The internet tool known as *telnet* allows connection to another computer on the internet, just as if it were sitting on your desk. Most of the time, registration on the other computer is required, but a few remote hosts allow everyone to have access. If not firewall protected, the telnet port becomes a primary target for the hacking community.

- The firewall must NOT allow an external user to login as root. Logging on as root allows the intruder full access to all the files on your system, to include your system files. Root access means the intruder "owns" your system.

- The firewall should protect the integrity of the audit trail. This should include all successful and unsuccessful attempts to use your system. The audit record also needs to include user's name, type of event, the event's success or failure, and the origin (Internet Protocol) address of event, including the date and time.

- Automated system monitoring -- Automated procedures verify the firewall's integrity. The firewall must be able to detect tampering. Automated system monitoring provides this capability.

- System compatibility -- Applications on your personal computer should remain the same after your firewall has been installed. Firewalls should enhance your system, not detract from its performance.

- User recognition -- The firewall should be able to differentiate between a user coming from an external unprotected system or an internal protected system.

- FTP (file transfer protocol) blocking – FTP allows the exchange of files between computers. FTP activity should only be allowed if it is specifically authorized by the system owner and then only for short periods of time.

- Adequate thru-put – System performance should be limited by the LAN speed, not by the firewall. If the firewall is too slow, users will bypass the firewall, and system integrity is forfeited.

WILL MY FIREWALL PROTECT MY COMPUTER AGAINST VIRUSES?

A virus is a piece of software designed and written to negatively affect your computer by changing the way it works without your knowledge or permission. Technically, a virus is a segment of program code that inserts itself to one of your executable files and spreads from one file to another. Viruses are most commonly propagated through e-mail attachments. Because the infected e-mail attachment contains a normally accepted data packet structure, firewalls do not normally identify them. A growing number of firewall vendors are beginning to package anti-virus software along with the firewall operating system. However, these anti-virus programs are not normally as reliable as the better known packages. For example, ZoneAlarm Pro Firewall Version 2.6, which is described later on in this paper, includes viruses detecting software with their firewall. Norton and McAfee, two of the most popular computer vendors, market virus scanning software for the personal computer. The anti-virus package, supplied along with ZoneAlarm Pro Firewall Version 2.6, is better than no package at all. Still, I would highly recommend one of the better known packages such as McAfee or Norton.

WHAT TO LOOK FOR WHEN SELECTING A FIREWALL

The software-based standalone firewalls are the most common when choosing a firewall for your personal computer. They can easily be installed as programs and are available for most operating systems, including Windows 95/98/ME/NT, and sometimes Windows 2000. This type of firewall protects only a single device, and the owner of the computer ensures the loading of updates. Users can find most of the features needed for personal use for less than $50.00. The applications, BlackICE Defender 2.9 and ZoneAlarm Pro Firewall 2.6 discussed in this paper were advertised for $39.95. The internet also offers many good products that are available for downloading free-of-charge from the vendor's websites. Freeware is software that is free, but may ask for registration. Even though the software is free the vendor of the software is the sole owner of the copyright, and often has rules surrounding its use, for example it can only be used for individual use, and cannot be repackaged, resold, or redistributed and you will probably be charged for all updates. Adobe Acrobat Reader 5.01 and ZoneAlarm Firewall 2.6.88 are excellent examples of freeware. Another option for the user is shareware. Shareware is software that can be downloaded and used for a limited amount of time like a demo, and then if the user likes the product it can purchased. Two examples of this type of software are JASC Paint Shop Pro 7.02 and WinZip Pro 8.0. For the first time user of a firewall, this would be an excellent way to find out what features are suited for you.

Regardless of which type of firewall you purchase, these are the features to look for:

- Easy-to-use configuration utility. If a product is difficult to use and configure, chances of continuously using the product are very slim.
- Frequent updating of new hacking techniques. If the vendor does not update its software, it will be become outdated and unable to prevent the "bad" from accessing your personal computer.
- Proven track record.
- Password-protection capability.

HACKING TRENDS

The definition of a "hacker" is: an individual who, via a modem or some other computer communications device, goes around computer security and breaks into a computer system. Hackers are no longer breaking into systems just for fun or just to look around your system. There are three different types of hackers: the ones doing it for fun, the ones that trash the website and tell their friends; and the criminals who steal things, such as credit cards, passwords, etc. Today, more malicious acts are being committed. Hacking tools that anyone can use and be proficient at, in a small amount of time, are easily accessible on the internet. Hacking tools are even showing up on e-bay.com and amazon.com. Just by initiating a search of "hacking", many applications show up. The advertising on these sites promotes protecting yourself against hackers. However, if you dig a little deeper, you will find a "how to" section dedicated to hacking. These will also normally be a selection of downloadable tools. Realistically speaking, new hackers are born on an hourly basis.

WHAT PORTS ARE SAFE TO PASS THROUGH A FIREWALL?

A computer port is an interface that provides computer-to-computer paths of communication. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting models, printers, and peripheral devices. Without ports, connection to the internet would be impossible. Port numbers are divided into three group: the Well Known Ports (0-1023), The Registered Ports (1024-49151), and the Dynamic and/or Private Ports (49152-65535). The Well Known Ports are controlled and assigned by the Internet Assigned Names Authority (IANA) and on most systems can only be used by system (or root) processes or by programs executed by privileged users.

When a port on a computer is being used, the computer is listening through that port for appropriately addressed packets. For example, a server listens through port 80 for Hypertext Transfer Protocol (HTTP) packets and routes them to an e-mail server application. An open port becomes a security issue, because hackers can gain access to a

computer when these ports are in the open mode. A personal firewall will protect your personal computer from unauthorized users when these ports are open.

Remote Procedures Calls (RPCs) are made by using either TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP/IP (User Datagram Protocol/Internet Protocol) as the network transport. TCP, a connection-oriented protocol is more reliable than the UDP. UDP makes no attempt to detect dropped or out-of-sequence packets, whereas TCP has sophisticated error-correcting techniques to prevent data loss. Port security depends on what application you will reach through that port, so it really doesn't matter what port you use.

There are many ports connected to your computer, but to help explain the definition of a port, I chose to define five of the most common ports are:

- Port 23 Telnet – Internet Standard protocol for remote login from one host to another.

- Port 25 Simple Mail Transfer Protocol (SNMP) – A protocol that governs network management and the monitoring of network devices

- Port 50 Remote Mail Checking Protocol – This protocol queries the server in order to find out whether new mail has arrived for a specified user.

- Port 53 Domain Name Server – The way internet domain names are located and translated into Internet Protocol addresses.

- Port 80 World Wide Web Hypertext Transfer Protocol (HTTP) - The protocol used to transport hypertext documents across the internet.

All ports are vulnerable to intrusion. But with some precaution, the risk of computer break-in can be reduced. The firewall is one way to protect your system; another example is disabling file and printer sharing options. The easiest and cheapest way to protect your computer is by turning off your printer when it is not used for long periods of time.

REMARKS ABOUT AVAILABLE FIREWALLS

BlackICE Defender 2.9 (cost $39.95)
Platforms: Windows 95/98, Windows ME, Windows NT, Windows 2000

BlackICE Defender 2.9, a software application, catches the hacker by logging the evidence, which includes the hacker's IP address and computer name. When an attack occurs, BlackICE flashes an icon and plays a sound. By clicking on the icon, one can display a list of all intrusion events, with the most recent attack highlighted. Detailed

information can be obtained on the intruder by logging into Network ICE's website. BlackICE consists of two main parts:

- The intrusion-detection system (IDS).
- The uncomplicated firewall.

The BlackICE IDS uses patent-pending protocol-analysis techniques that will analyze network traffic. It has the capability to detect over 700 patterns of activity associated with hacking, including port scans and Trojan horses.

The firewall blocks all levels of access from detected intruders and blocks general network traffic depending on which security level you choose. BlackICE lets the user choose between four different levels of security:

- Paranoid level -- blocks all unsolicited incoming Transfer Control Protocol (TCP) and User Datagram Protocol (UDP) traffic to the system and to applications.
- Nervous level -- permits incoming UDP access for applications.
- Cautious level -- adds incoming TCP.
- Trusting level -- permits all four types of traffic.

Sophisticated computer users who are familiar with firewall settings can fine-tune the application to permit or block specific combinations of IP addresses, protocols, and ports.

Some of the selling points of BlackICE are the simplicity of the installation, multiple security levels that can be defined, a detailed advICE database available on the company's website, the real-time attack alerting feature, and out-of-the box security enabled with the default "Cautious" settings. BlackICE markets its product for all levels of expertise, from the novice user to the sophisticated user. Like most reliable companies it has a website with downloads so the firewall application can stay up-to-date.

Some of the disadvantages of BlackICE are it has a limited filtering capability, attack signatures are not always correct resulting in false positives, no password protection, and not useful in setting up a DMZ (DeMilitarized Zone). The DMZ is the area that is outside the firewall. A DMZ is described as the front yard of your house, it belongs to you and you have some of personal belongings there, but you put the most valuable possession into the house where they can be properly secured. If you have multiple computers, you can choose to place one of the computers between the Internet connection and the firewall. Most of the software firewalls available will allow you to designate a directory on the gateway computer as a DMZ. Unfortunately, BlackICE does not facilitate DMZ utilization. BlackICE has some features that aren't desirable, but in the long run the pros outnumber the cons.

ZoneAlarm Pro Firewall Version 2.6 (cost $39.95)
Platforms: Windows 95/98, Windows NT, Windows 2000

Setting up ZoneAlarm Firewall Version 2.6, also a software application, is a little more time consuming than other firewall products. But to make installation easier, a nine-screen wizard guides you through the installation process. The next step is a quick start guide, which highlights important features. At this time you can create a password and configure Internet Connection Sharing/Network Address Translation (ICS/NAT), which protects the gateway and client machines on your network. With a password, only the administrator can make changes to the program, a great security feature for preventing unauthorized access to your personal computer. After installation, rebooting is not necessary, unlike other firewall programs. It informs you when setup is finished, and gives the option of whether or not to create an icon, which indicates the firewall's operating status. This icon also allows you to access different control panels available with ZoneAlarm.

Where as BlackICE had four different security settings, ZoneAlarm has three different zones to define access restrictions. The three zones are: Local Zone, Internet Zone, and Restricted Zone. But like BlackICE, depending on the level of expertise, zones settings can be customized.

ZoneAlarm has the following selling points: a built-in virus detection capability, out-of-the box security enabled, includes the password-protection capability, outbound traffic is easy to monitor, real-time alerting of blocked traffic and new processes, and can block unknown attacks. The password-protection capability that ZoneAlarm provides makes this product more appealing.

The disadvantages of purchasing ZoneAlarm are: cannot easily setup a DMZ (like BlackICE), not capable of remote administration, and the user may not understand what an alert means when an unknown attack is launched.

Most of the features of ZoneAlarm are similar to BlackICE. And both applications provide comprehensive security that will keep your personal computer safe from known and unknown attacks. But the password-protection capability would be a selling point for me. If BlackICE were to add to this feature, the decision of which application to buy, would be a difficult one.

CONCLUSION

A firewall may be your first line of defense, but other security features must be considered. Some of the most important security practices include the protection of passwords; checking audit file; virus scanning software; and, if you have a firewall on your computer, keeping up with current advisories from the firewall vendor.

The demand for improved security standards will always exist. Technology will always need that continuous and ongoing update to provide more durability and strength against a hacker's intent of breaking into a network. Installing a firewall is only one way to protect yourself from a hacker, but it is a very important step in protecting your private information.

References:

1. "To Protect and to Surf", by Troy Dreier, February 26, 2002
http://www.pcmag.com/article/0,2997,s%253D1474%2526a%253D22020,00.asp

2. "How It Works: Personal Firewalls", by Robert L. Hummel, June 5, 2000
http://www.pcworld.com/howto/article.asp?aid=17012

3. "Insurance for Your Home PC", January 29, 2002
http://pcworld.com/howto/article/0,aid,17012,pg,2,00.asp

4. "Getting Personal With Firewalls", By Curtis Dalton, January 5,2001
http://networkmagazine.com/article/NMG20010103S0010/1

5. "BlackICE Defender 2.9", by Neil J. Rubenking, February 26, 2002
http://www.pcmag.com/article/0,2997,s%253D1474%2526a%253D21994,00.asp

6. "Review: ZoneAlarm Pro Firewall V2.6. ", by Walter Arellano and Vincent Wong
http://www.8wire.com/articles/?AID=2572

7. "Sending Firewalls Home", by Barry Nance, May 28, 2001
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60879,00.html

8. Advisories, February 4, 2002
http://www.iss.net/security_center/alerts/advise109.php

9. "Personal Firewalls", by Gary Bahadur, July 2001
http://www.infosecuritymag.com/articles/july01/cover.shtml

10. Personal Firewalls
http://www.infosecuritymag.com/articles/july01/charts/cover_story_chart.pdf

11. "Internet Firewalls, Frequently Asked Questions", by Matt Curtin and Marcus J. Ranum, December 1, 2000
http://www.interhack.net/pubs/fwfaq/#SECTION000410000000000000000

12. Firewall Requirements
http://www.lsli.com/tut27.html

13. TCP or UDP?
http://www.transarc.ibm.com/Support/dce/general/tcp_and_udp.html

14. Port Numbers
http://www.iana.org/assignments/port-numbers

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor