Internet Firewalls

Robert D. Henson; University of Alabama at Birmingham; Birmingham, AL

Keywords: Internet Firewalls, Firewalls, Network Security, Personal Computer Security, Proxies, Packet filters, Application-level gateways, BlackICE Defender

ABSTRACT

In recent years, network security and personal computing security have become major topics for all types of computer users. Attacks on large corporations, intermediate to small businesses, and private, non-commercial systems have increased each year. Since attacks have become widespread and sensationalized by the media, numerous computer users have started to search for ways to secure their computers. One way that has started to gain popularity is the Internet firewall. An Internet firewall helps to secure and defend a host system from possible intruders, malicious or otherwise. If a user implements and maintains a firewall correctly, numerous attacks can be avoided and the system can be somewhat protected. With security being such a hot topic, hackers and crackers are looking for easy-to-penetrate, unprotected systems. Implementing and maintaining an Internet firewall saves users valuable time, money, and resources and provides adequate means to stop attacks.

1. INTRODUCTION

Increasing attacks and overall uneasiness of the Internet have lead many computer users to seek methods to secure their computer systems. One way of securing a computer system is by installing and maintaining an Internet firewall. By utilizing software or a combination of hardware and software, a person or business can implement a successful firewall.

Firewalls come in many different forms. Most firewalls are broken down into two different types that include network-layer firewalls, in which IP packets are examined by the firewall, and proxy firewalls, in which the firewall is a “middle-man” or intermediate between a host computer and a computer on the Internet [1]. Firewalls, no matter the type, provide basic functions, which include blocking and preventing intrusion attempts, isolating a host computer from Internet users, and the logging of all attempts, malicious or not, made on the system [2].

Internet Firewalls for personal and business use can be purchased from commercial vendors and can be downloaded free from different Internet sites. Two examples of firewalls available today are examined in this paper. These examples are BlackICE Defender, a commercially bought firewall, from Network ICE and Zone Alarm, a free downloadable firewall, from Zone Labs, Inc. Both of the examples given are explained in detail. Various features of each example and their relation to the paper are explained.

1.1. Acronyms and notation

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>Global Internet</td>
</tr>
<tr>
<td>Firewall</td>
<td>Internet firewall</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transfer Control Protocol</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>SYN</td>
<td>Synchronization Flag</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement Flag</td>
</tr>
<tr>
<td>Admin</td>
<td>Administrator</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>ME</td>
<td>Millennium</td>
</tr>
<tr>
<td>BID</td>
<td>BlackICE Defender</td>
</tr>
<tr>
<td>ZA</td>
<td>Zone Alarm</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
</tbody>
</table>

2. WHAT IS AN INTERNET FIREWALL

An Internet firewall is basically just a barrier or barricade placed between a host computer and unknown computers on the Internet. A firewall, in most cases, is specialized software developed to protect and defend a system from unauthorized use and to prevent unsolicited attacks on a system [3, 4]. Many publications today use a castle analogy to describe firewalls [1]. Since castles seem to be a bit outdated, a more recent description might be more appropriate. To give a twenty-first century example, a firewall is comparable to a bouncer at a nightclub. The bouncer’s job is to protect and defend a certain access point to the nightclub. The bouncer only allows people to enter if they meet his appropriate standards, which might include age, dress, attitude, name on a guest list, someone he personally knows, etc… The bouncer has the ultimate responsibility in choosing who is allowed in and who is not. The same thing might be said about a firewall. Just like the bouncer, a firewall has certain standards that it must follow and it has the responsibility of allowing or disallowing traffic into the host computer [1, 2].
3. WHY HAVE A FIREWALL

There are many reasons for installing a firewall on a host computer. One reason is to block intrusions made on the host system. The firewall monitors Internet traffic on a host computer. If any suspicious activity occurs, the firewall blocks the suspicious incoming traffic and prevents it from entering the system [3]. Another reason for using a firewall is to stealth or conceal the host computer from unknown or un-trusted sources. This is accomplished by stealthing the ports of the host computer. The ports on the computer can be open – the port is accessible, closed – the port is not accessible, but can be seen by outside port scans, and stealthed – the port is not accessible and is invisible to outside scans. If the computer is invisible, then it is much harder to attack [5]. Another reason for having an Internet firewall is to control any access or activities that occur on the host computer. By properly configuring the firewall software and or hardware, the firewall can allow or disallow any internal application or program from accessing the Internet and can also allow or disallow incoming Internet traffic [3, 4]. A firewall also provides a record of intrusion attempts, successful or unsuccessful, made on the system. These log files can be used to gather information on the attacker and can be used as evidence against the attacker once the attacker is arrested and prosecuted [2, 3]. In my own experience, the reason I have a firewall is for piece of mind. With so many attacks occurring each day, it makes me feel better and safer having a firewall. Personally, I think most people feel the same.

4. TYPES OF FIREWALLS

Various forms of firewalls exist, but generally, firewalls are broken into two categories. These two categories are network-layer firewalls and proxy firewalls [1]. Out of these two categories, most firewalls are developed. Both types serve to protect a user’s computer, but each type uses different means to maintain this protection.

4.1. Network-layer firewall

The first type of firewall is the network-layer firewall. This type of firewall examines actual IP packets and derives its name because of this [3]. The network layer is the third layer in the ISO 7-layer reference model and is the layer associated with IP [6]. A commonly used type of network-layer firewall is the packet filter [4, 7].

Packet filters. Packet filters examine the contents of incoming IP packets and determine whether to accept or drop the packet based on the rule set of the packet filter. The rule set (a more comprehensive description is given in a later section) is a set of policies the filter follows in order to maintain a secure system. The rule set determines the level of strictness or scrutiny the packet filter operates at and is defined by the user, owner, or administrator of the packet filter [2, 3].

Packet filters can either be stateless, each packet is treated as a separate packet having no connection with any other packets, or stateful, information about recent connections and activities is stored and compared as new packets come in [4].

Stateless or traditional packet filters are very simple filters that examine the IP headers, and only the IP headers, of the incoming IP packets. Source address, destination address, and total length are some of the fields examined and checked by the rule set of this type of filter. A common example of a stateless packet filter is a router [1].

Stateful packet filters are far more complex than stateless packet filters. Stateful packet filters examine not only the fields of the IP header, but also the IP datagram itself. Different messages such as UDP, TCP, and ICMP are carried in the payload of the IP datagram [6]. Stateful packet filters examine the header of each message encapsulated in the datagram. With UDP and TCP, the source and destination ports are checked. With ICMP, the source address, destination address, and the type are checked and examined [2, 4]. Stateful packet filters store information relating to received packets and use that information to remove or disallow packets further entry if suspicious activity is seen [4].

4.2. Proxy Firewalls

The next type of firewall is the proxy firewall. A proxy firewall works by creating a proxy or substitute application to act as an intermediate connection between a host computer and the Internet [2]. Once created, the proxy relays information form source to source. Depending on which source is receiving and which source is sending, the proxy represents itself as either the host computer or the Internet or outside source [2]. Traffic flows from source to source through the proxy. Once a packet arrives at the proxy, it is examined and checked to see if it complies with the established rule set. If the packet is acceptable, it is forwarded on to the end source. If the packet is not acceptable, it is dropped by the proxy [1].

Even though each source has a separate connection to the proxy, each source thinks it is connected to the other source directly [2]. Since no direct connection is established, the proxy firewall is able to control exactly what is allowed in and out of the host computer [1].

An important feature of a proxy firewall is that it provides for network address translation (NAT) [3]. Network address translation allows a computer to mask its IP address with the IP address of the firewall. By doing this, the outside source never knows the exact IP address of the host computer. Since only the IP address of the firewall is known, the outside source can only travel as far as the proxy firewall [1].

Many types of proxy firewalls are used today. The most common proxy firewalls used are application-level gateways and circuit-level gateways.

Application-level gateways. An application-level gateway is a proxy firewall that deals with specific applications. Each proxy created is designed for a specific individual applications or group of applications [2]. In an application-level gateway, a specific proxy is used when a host computer
or outside source tries to establish a connection through a specified application. If no proxy exists for the application, a new proxy must be coded for it [2]. FTP, SMTP, HTTP, are some of the applications used with application-level gateways [1, 7].

Circuit-level gateways. A circuit-level gateway is a proxy firewall in which the firewall itself (called a gateway) establishes a connection between the host computer and an outside source. The connection used is a TCP or UDP port connection [7].

Like application-level gateways, the circuit-level gateway acts as an intermediate connection between a host computer and an Internet source. When a host computer wants to establish a connection to an outside source, it connects to the TCP or UDP port of the circuit-level gateway [7]. The gateway then establishes a connection to the TCP or UDP port of the outside source. Once the connection is established, the gateway allows data to be transferred and received freely from each source [7]. The circuit-level gateway then becomes just a connection to send data.

5. RULE SET

As described early in the paper, the rule set or security policy determines anything and/or everything allowed or disallowed in and, depending on what type of firewall is in use, out of the firewall. The user, owner, or administrator determines the appropriate rule set for the firewall [2, 3]. Many software firewalls available today have predefined or default rule sets configured by the manufacturer. Even though the rule sets have default configurations, users and administrators still have some ability to create custom configurations so that their particular system or network is more secure [1]. Also, each specific type of firewall (stateless packet filters, stateful packet filters, application-level gateways, etc...) may have a different configuration for its respective rule set [1, 4].

A rule set can consist of various rules. These rules might include specific IP addresses, various TCP and/or UDP ports, particular applications (FTP, Telnet, SMTP, HTTP, etc...), specific network protocols (IP, ICMP, ARP, etc), certain flags (SYN, ACK flags) set in the TCP header field, and many others [4,7]. According to the user or admin, the rule set can allow or disallow any number of these things [3].

Even though a variety of rule sets may exist, many firewalls include default configurations to deal with anything the user or admin has not included. Default configurations usually are in two forms. The first form specifies anything that is not specifically blocked by the firewall to be allowed by default [1]. The second form is the more paranoid form. The second form specifies anything that is not specifically allowed by the firewall to be blocked by default [1, 4]. The second default configuration allows the user or admin to protect the system or network from random attacks such as DOS attacks, SYN floods and IP spoofing [7].

6. POPULARITY OF PERSONAL INTERNET FIREWALLS

The popularity and availability of personal firewalls has grown tremendously in recent years. Now days numerous firewall packages are sold or freely distributed. Within the last few years, retail stores have started carrying more and more brand name software packages that include firewalls. For example, I went to Wal-Mart the other day to buy a computer game. While I was looking for the game, I noticed many different firewalls for sale. McAfee, Norton, and Zone Labs were some of the companies that had firewall products for sale at the retail giant. Since these firewalls were being sold at a retail store, they were reasonably priced. When examining some of the different firewall products, I noticed that each firewall had several specific features not included with other firewalls. It seems the market for personal firewalls has become very competitive. With the increasing popularity, firewalls are no longer for tech-minded people. The increase in online shopping and online banking has created demand for competitive, cost-effective firewalls.

7. TWO EXAMPLES OF PERSONAL INTERNET FIREWALLS

Personal Internet firewalls have become very popular among computer users today. Firewalls can either be purchased through commercial vendors or downloaded free from websites. Many types of firewalls exist today. The two examples examined and detailed in this paper are BlackICE Defender 2.5, a commercially sold firewall developed by Network ICE, and Zone Alarm version 2.6.362, a free downloadable firewall from Zone Labs, Inc. Both of these firewalls are installed and used on the author’s personal laptop computer. The aforementioned laptop is a Gateway Solo with Windows ME running on it. Both firewalls support Windows ME operating system.

7.1. BlackICE Defender 2.5

BlackICE Defender 2.5 is a firewall/intrusion detection system developed by Network ICE. This firewall was purchased from Wal-Mart for $39.95. The firewall has been running on the aforementioned laptop for over two years. Many times BlackICE Defender has blocked intrusion attempts made on the host system and, in doing so, has become an invaluable piece of software. Attempts such as port scans, scans for Trojan horses (Sub-seven, Back Orifice, Netbus), and ping requests have all been blocked by the BlackICE Defender software. BID has been a valuable tool in learning the many aspects of the Internet and the different attacks that hackers use to infiltrate systems.

BlackICE Defender is composed of not just a firewall, but a firewall and an intrusion detection system [8]. These two components work together to secure the system from malicious and unwanted Internet traffic. In the author's opinion, BID’s intrusion detection system closely resembles a stateful packet filter. Just as a stateful packet filter examines and keeps up with information on current packets, BID’s
intrusion detection system does the same. The detection system examines each packet that tries to access the system and determines the legitimacy of the packet according to the information (the datagram payload encapsulated within the packet and other state information) collected by the BlackICE Defender software [8]. Depending on the legitimacy of the packet, the intrusion detection system relays information to the firewall to allow or disallow the packet access to the system [8].

BlackICE Defender includes many features. These features include differing levels of security, an easy-to-use user interface that includes an attack display screen and a graphical representation of attacks, allowing/disallowing of suspect IP addresses, the blocking of protocol ports, a desktop alert icon, and logging of attacks. BID allows these features to be configurable so that the user can determine how the software responds to various attacks [8].

BlackICE Defender has four levels of protection. These levels include trusting – trust all incoming information no matter what, cautious – block some unwanted incoming traffic, nervous – block most unwanted incoming traffic, and paranoid – block all unwanted incoming traffic (the current setting on the author’s system). These security levels allow the user the ability to determine how strict the system’s security policy is [9].

Another aspect included with the level of protection is port blocking within each level. As the level of protection increases, the number of ports blocked also increases. Within the first level of protection (the trusting level), all protocol ports are open. As the level of protection increase, the well-known ports for both TCP and UDP are blocked, then the random ports for TCP are blocked, and finally all ports for both transfer protocols are blocked [8].

An interesting feature of BlackICE Defender is the attack display screen. The attack display screen, illustrated in figure 1 (screen capture from the author’s computer), shows the type of attack that occurred, the intruder’s name or IP address, the time the attack occurred, and the number of times an intruder tried to make an attempt on the system. All attempts made on the system are recorded and displayed here.

![Figure 1. Attack Display Screen](image)

When an attack (successful or not) occurs, the attack display is updated and two things, besides those mentioned above, are added to the entry. The two things are a severity level and an action overlay. The severity level, represented by different colors, informs the user how bad the situation is. The action overlay, placed on top of the severity level, indicates the action (blocked, not blocked, successful attack, etc…) the firewall performed or tried to perform to prevent the possible intrusion [9].

In order to give users a better grasp of when attacks occur, BlackICE Defender presents a graphical representation of attacks and network activity. BID provides this graphical representation of all network activity that has occurred for up to ninety days. The representation is split into two graphs, one graph for attacks and a second graph for all network traffic. The graphs can show activity for the last ninety minutes, ninety hours, or ninety days. The attacks graph displays suspicious activity (yellow line) and critical activity (red line) for the selected time interval. The network traffic graph displays all network activity in terms of the number of packets that has traversed the system. For each time interval, the total number of critical and suspicious attacks is displayed and total traffic in number of packets is displayed. In addition, the high traffic minute, hour, or day (according to the interval) is displayed [8]. By utilizing these graphs, the user can establish when attacks are more likely to occur and possibly use it to help protect the system more.

BlackICE Defender also includes features that allow IP addresses to be allowed (trusted) or blocked according to the user’s preference. When an IP address is blocked, a time limit can be placed on how long it remains blocked. Depending on what the user specifies, the IP address can be blocked for varying amounts of time, which include a specific hour, day, month, or permanently [8, 9]. This feature allows the user the ability to customize the rule set and to disallow attackers access to the system permanently if so chosen. This feature is very important because IP spoofing has become very prominent. Since an address can be spoofed, the user may allow an IP address to be forgiven after the specified time limit expires. If the address remains a problem, the user then can block it forever [8].

The last feature discussed is the evidence logging techniques and activities performed by BlackICE Defender. Unlike other firewalls, BID has an interesting feature called Back Trace. Back Trace allows the user to trace the attack back to the originating machine or trace the route the attacker used to send the malicious traffic. By using Back Trace, the user can discover information such as the IP address, hardware address, and the DNS name of the attacking system [8].

BlackICE Defender features logs that record system information and intrusion attempts. BID includes two logs, a packet log and an evidence log. The packet log records all traffic that traverses the system. The evidence log records all
intrusion attempts made on the system and any suspicious traffic encountered by the system [8].

### 7.2. Zone Alarm version 2.6.362

Zone Alarm version 2.6.362 is a free downloadable firewall developed by Zone Labs, Inc. Zone Alarm is a very interesting firewall in the sense that it monitors both incoming and outgoing traffic from the host system. Zone Alarm also monitors all internal applications that try to access the Internet. All traffic, incoming and outgoing, is routed through the firewall before it is allowed to enter or exit the host system [5]. Since all traffic is routed through the firewall, ZA can be classified, in the author's opinion, as a proxy firewall.

Zone Alarm has many features. These features include an Internet lock, an emergency all-stop button, varying levels of security, popup alert windows, a detailed list of all applications and programs that are allowed to access the Internet, and event logs that capture suspicious activity [5].

One of the main features of ZA is the detailed program list of all applications and programs that are allowed to access the Internet. The list maintains information that allows the user to know specific details about each program found there. The list includes the name of the program, the version number, the date created, the full path name of the program, and the size. This information can be used to inform the user if any suspicious activity has occurred. Suspicious activity might include the size of the file changing or the application residing in a different folder than previously specified [5].

The program list also includes a set of permissions for each program. These permissions include Internet access, acting as a server, and passing through the Internet lock. For each permission, the user can specify whether the program is allowed without asking permission, disallowed, or must ask permission each time [5].

Another feature of Zone Alarm is varying levels of security. As with BlackICE Defender, Zone Alarm has different degrees of protection. The levels include low – local area network connections and many trusted sources, medium – smaller amount of trusted source and Intranet/Internet connections, and high – Internet connections, high level of danger. The user can determine the amount of Internet and network activity for the system and set the level of security accordingly [5].

Another feature shared by BlackICE Defender and Zone Alarm is the blocking of protocol ports by level of protection. Zone Alarm is similar to BID, but it takes an extra step in blocking the ports. In order to completely hide the host computer, ZA not only blocks the ports, but stealth’s the ports also. By stealing the ports, attackers cannot find or access the host computer [5].

When suspicious activity is suspected or detected, Zone Alarm alerts the user with popup alert windows. The alert windows are used to grab or get the user’s attention. When a popup alert window appears, it will stay open until the user closes it. This helps to guarantee that the user is notified and aware of what ZA is doing [5].

When an alert window does popup, many things are displayed. Figure 2 [5] illustrates the various parts of the alert window.

![Sample Popup Alert Window](image)

**Figure 2. Sample Popup Alert Window**

Things displayed here can include the action the firewall has taken, the host’s transfer protocol and port, the DNS name and/or the IP address of the attacker, the attacking system’s transfer protocol and port, and the suspicious application or activity the attacking system is trying to use [5].

If alert windows start to popup frequently, the user has the option to stop Internet traffic. Zone Alarm includes a feature called the Stop button that kills all Internet connections to all applications. When the button is pushed, all connections are terminated without delay. This feature is useful when a user suspects Trojan horse applications are connecting to the Internet [5].

In order to keep users aware of specific system and firewall activity, Zone Alarm logs activities pertaining to the firewall and internal applications to an Internet log. This log records all, incoming or outgoing, traffic that has been blocked by the firewall. Also, any internal application that tries to access the Internet is recorded to the log [5].

As activity takes place, new entries are added to the log. ZA classifies each entry as one of three types. These types include FWIN – blocked incoming traffic, FWOUT – blocked outgoing traffic, and PE – internal application trying to connect to the Internet. Once the type is determined, the IP addresses and protocol ports for both the source and destination computers are added. The time the activity occurred, the date the activity occurred, and any other prevalent information (name of applications, transfer protocol used, etc…) are also included [5].

### 8. CONCLUSIONS

As more computers continue to go online and access the Internet, the threat of attacks increases. Numerous hackers scan the Internet daily looking for unprotected computers. One way of preventing intentional and random malicious attacks is by installing an Internet firewall. Firewalls not only prevent attacks, but also provide the user with a better sense of security. Users across the board have incorporated firewalls into their business networks and home systems.
Firewalls have become so popular that retail giants such as Wal-Mart have begun stocking their shelves with different brands of firewall software. Internet firewalls have become a valued resource in today’s Internet society.

REFERENCES

7. W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, 1994; Addison-Wesley

BIOGRAPHY

Robert D. Henson
3010 Old Birmingham Hwy.
Jasper, AL 35501 USA

e-mail: rdh@uab.edu

Robert Henson is a student at the University of Alabama at Birmingham. He is currently pursuing a Bachelor’s Degree in Computer and Information Sciences. Mr. Henson is currently employed with Wal-Mart Super Center #287 in Jasper, Alabama. Mr. Henson has worked on several in-class projects. He was a member of the software quality assurance team that helped develop an online database application for a fictitious company. Mr. Henson is a member of the Association for Computing Machinery and a member of the Golden Key International Honor Society.