Global Information Assurance Certification Paper

UNDERSTANDING & SELECTING A FIREWALL

BY: BARBARA MYSTKOWSKA

DATE: NOVEMBER 19, 2003

VERSION 1.4B

TABLE OF CONTENTS

OVERVIEW

Each system or network connected to the Internet is susceptible to unauthorized access. In order to protect ourselves, we have to understand how one can gain such access, called either an attack or hack. Firewalls provide the potential of stopping external attacks.

Once a computer is connected to the Internet, there are many ways an attacker can access the computer and retrieve information from the machine. The physical connection, Category 5 (CAT5) cable, allows the computer to be visible on the Internet. Once the machine is visible on the Internet, it can be accessed remotely using the Internet Protocol (IP) address and any open ports. Because there are different ways to get into a machine there are many counter measures that can be used to stop outside attacks.

All the possible access points can be easily shutdown by different methods. Physically disconnecting the cable connecting the computer to the Internet is a safe but not sufficient way to protect yourself. A burglar can still break into your house and access your machine. Many safety measures include the use of a firewall and password protecting the machine.

OBJECTIVE

The objective of this paper is to help users to better understand the mechanism behind the firewall of both personal computer (PC) and network. This paper will discuss firewalls and how hackers can potentially compromise a machine. Networking basics will be explained, including the OSI levels and TCP/IP. Following sections will explain the possible ways a system can be compromised, the mechanism of firewalls and how they can be used to stop different types of attacks. Commercial firewalls will be discussed and recommendations will be made on how to select the most compatible firewall.

NETWORKING BASICS

Prior to discussing firewalls, we need to understand how communications on a network take place. In order to block intruders, the basics of Transmission Communication Protocol/Internet Protocol (TCP/IP) and the structure of the Open Systems Interconnection (OSI) model should first be introduced. Note that machine, computer, system, and personal computer (PC) will all refer to an individual computer system.

TCP/IP BASICS

Two computers communicating with each other create a network. In fact, all computers connected to the Internet create one huge network (see Figure 1). The interactions between all machines are standard since each system may have different hardware and various configurations. This communication is governed by a set of rules, called protocols; common examples include the Transmission Communication Protocol/Internet Protocol (TCP/IP). TCP and IP are merely a few of the protocols.

Figure 1 – Basic TCP/IP connection

Protocols are a set of rules to direct machines on how to communicate. The form of data that is sent between machines is referred to as packets. As packets travel across a wire they need to know their destination and origin. This is done using an addressing scheme within each packet. Each machine is connected to a network using a network interface card (NIC). Each NIC has a unique Internet Protocol (IP) address.

An IP address is a 32-bit address in the form www.xxx.yyy.zzz, where each number xxx has the range of 0 – 255. This address is divided into two parts. First part of the IP address refers to the network address and the rest is the host address. Each network has a unique IP address range, e.g., 123.456.0.0, where each machine on that network has a unique address within that network, for example 123.456.0.24. The number of bits used for the network part and the host part vary from network to network. First part of the IP address refers to the

network and the rest is the host part. The number of bits representing the network is determined using a network mask (netmask) IP address. The bits that are set to 1 in the netmask show that those bits are the network bits in the corresponding IP address. Hence, each IP address identifies the exact address of the machine as well as the network that it belongs to.

However, each NIC has many access points for different types of traffic. These points are called ports. For example, all Internet traffic uses the Hyper Text Transfer Protocol (HTTP), which uses port 80 as a standard port for Internet. Hence, each packet contains the origin IP address and port number as well as the destination IP address and port number.

Knowing the basics that are used to communicate between computers we also need to understand what happens to these packets before leaving the origin NIC and after arriving at the destination NIC.

OSI MODEL

The Open Systems Interconnection (OSI) Reference Model describes network communications using a layered approach. It is a logical structure for network operations containing seven layers and is standardized within International Organization for Standardization (IOS)[1]. Each layer has a different responsibility, which are as follows:

Physical Layer	Includes hardware required to transmit data.
Data Link Layer	Provides a reliable means of transmitting data across the physical connection.
Network Layer	Manages connections across a network.
Transport Layer	Ensures ordered and reliable arrival of packets.
Session Layer	Handles connections between linked applications.
Presentation Layer	Presents data to applications using a standard format.
Application Layer	Applications interacting with the network.

[1] **[MSDN 2003]**

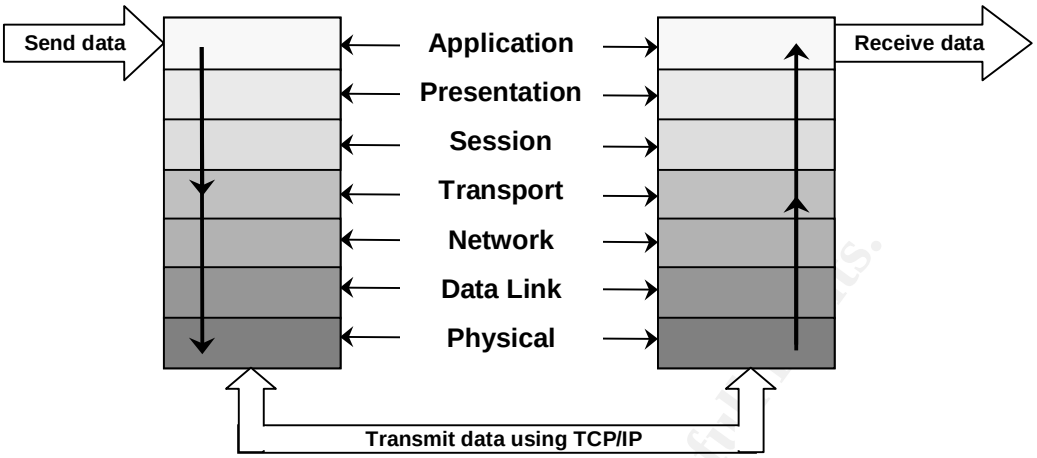

Figure 2 – OSI layers communications

Each piece of data entering a system must go through all the layers before it reaches the Application layer where the user decides what to do with the data. Similar but reverse process happens when a user wants to send data. The data starts at the Application layer and is transmitted through all the layers before it is released to the network. Each packet is modified in such a way that it knows its destination. Figure 2 shows a data packet travelling through all the OSI layers.

TYPES OF ATTACKS

In order to select a proper firewall to protect a network or machine, various types of attacks need to be understood. These attacks vary from minor to very severe, yet all are important in order to understand what a firewall can and cannot stop.

ATTACKS[1]

The following describes a selection of some common attacks. Many people do not protect themselves against them. The attack descriptions include simply the explanation of the attack and not the solution to protecting from it. The OSI layer that is affected by the attack will be discussed.

SOURCE ROUTING

Each packet moving across a network travels through different nodes. This path may vary from connection to connection if a particular node in the path is not working. Hence, there is typically more than one path between two machines. However, source routing is a way for the source to attach information to a packet that will direct it through a specific path. This allows the attacker to pretend their packets are coming from an internal network. The network layer recognizes the packets as internal and allows them through. On the way back, the packets take the reverse path, allowing the attacker to access these packets and possibly information about the target's machine.

DENIAL OF SERVICE

As the name suggests, service to a machine is refused in one form or another. Denial of service comes in many different forms; it can be as simple as shutting off the power. The machine may crash, the system might act really slowly, and certain services might simply be denied. This attack varies on the OSI layer it affects, starting with the physical layer if the power is shut off. The attack may appear in many different forms and the severity of the attack depends on the intruder, making it hard to detect.

[1] **[Curtin and Ranum 2000]**

VIRUSES

The most common threat that affects most Internet users is a small program that spreads itself from machine to machine. A virus spreads very quickly and effects many machines. Executed at application layer, a virus is treated as if another application has been opened. The threat level may vary and some users might not even know their machine is infected, which makes this attack very successful.

BUG EXPLOITATION

Many applications and operating systems contain bugs. Exploiting these bugs has become many hackers hobby. For example, such bugs as buffer overflow, can allow an attacker to gain access to a machine, which gives them a possibility to control the system. This type of attack influences different OSI layers; however, the application layer is where exploits take place. Exploiting bugs can give the attacker the opportunity to do various attacks, varying from crashing the operating system, infecting the machine with a virus, or creating a backdoor. Since not everyone keeps the operating system up to date, this is a popular attack, especially once the bug is published.

SPAMMING

If you have e-mail, you have most likely received e-mails advertising products. These types of e-mails are called spam. Although it appears harmless, spam mail may sometimes contain harmful links. Once the link is opened, a cookie may be accepted by the system, which could create a backdoor into the machine. Also, the website content may contain malicious code that could infect your machine. For the most part, spamming is annoying and it is hard to stop.

FIREWALLS

WHAT IS A FIREWALL?

A firewall is a tool used to improve system security. It provides counter measures for various types of attacks. As shown in Figure 3, a firewall stands between a trusted and the untrusted network, protecting the internal net. There are two types of firewalls, hardware and software. A software firewall is an application that runs on the system and monitors all the traffic coming in and out. A hardware firewall is a physical piece of hardware that stands between the machine and the Internet. It stops the bad traffic before it even reaches the system.

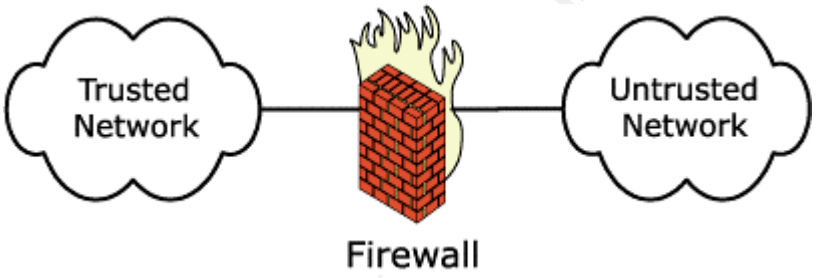

Figure 3 – Basic Firewall location[1]

HOW FIREWALLS WORK?

The mechanism behind a firewall is specific to each firewall, however since all firewalls have a similar goal, they work using comparable techniques. Every firewall examines each packet coming in and going out. The filter allows packets access based on a set of rules. The two extreme settings include: deny all incoming traffic or accept all incoming traffic. Obviously these are at the two extremes, secure versus vulnerable.

1 **[MOREnet 2003]**

FIREWALL TYPES

There are three types of firewalls: Packet Filters, Stateful Inspection, and Proxy System. Many firewalls are made of just one of these methods while some firewalls can contain up to all three of these methods. These types of firewalls protect the system on different OSI layers, concentrating mainly on the Network and Application layer. Figure 4 shows which layer is analyzed using each type of the firewall.

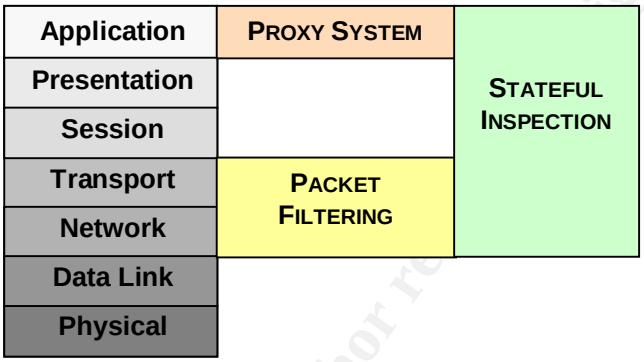

Figure 4 – Firewall types referencing OSI layers

PACKET FILTERS

The most common firewall method used on the Network Layer of the OSI model is called packet filtering. This method consists of monitoring traffic going in and coming out of the system. Each packet is examined based on its source IP address, destination IP address, source port number, and destination port number. The basic path of a packet is shown in Figure 5. The filters are set according to which packets should be allowed to come in and which ones are allowed to go out. For example, if the system only connects to the Internet using HTTP, then only port 80 should be open to external IP addresses.

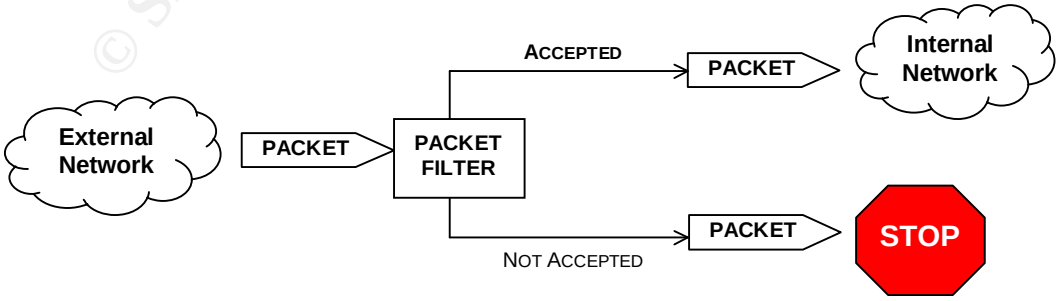

Figure 5 – Packet filter firewall type

The downside of the packet filter method is that the link between source and destination computer is still direct. All traffic coming through the packet filter is only examined based on their IP addresses and port numbers. However, what if someone tries to access a machine through a port that is not regularly used for a certain application like IE. There is no check for which application should be associated with the specific port, potentially creating a security hole.

Although not perfect, packet filter is still the most popular method used since it blocks out all IP addresses and then allows the user to specify one IP address at a time.

PROXY SYSTEMS

The Proxy System method operates at the Application layer of the OSI model. In this approach, the firewall acts as a gateway point between the internal and untrusted external network (see Figure 6). Typically two NIC cards are used: one to talk to the external network and the other to communicate with the internal machine. The gateway firewall changes the IP address of the internal system, thus hiding the real IP address from attackers. Most Digital Subscriber Line (DSL) and cable routers act to provide a hardware proxy firewall.

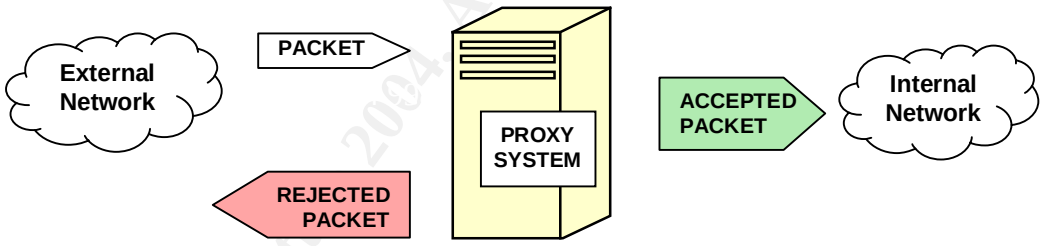

Figure 6 – Proxy System firewall type

The main weakness of a proxy system is the degradation in speed of communication. Each packet is examined, at the application layer, by looking at the whole packet, not just the IP addresses and port numbers. This method is much slower than packet filtering. As a result the proxy system requires more power, making it more expensive. Another drawback is the fact that a separate proxy must be used for each application. The complexity increases with each new application that is installed.[1]

Due to the separation between the internal network and the external network, a proxy system firewall is advantageous. Hiding the IP address alone gives one protection from untrusted networks.

[1] **[MOREnet 2003]**

STATEFUL INSPECTION

Stateful Inspection is an improved version of packet filtering and is acting fully on the Network and Application Layers. The packet headers are examined the same way a packet filter works, but the contents of the packet are also analysed. The contents of each packet give the communication state and determine whether communication had previously happened between these two machines. Figure 7 shows what happens to a packet when passing through a Stateful Inspection.

Figure 7 – Stateful Inspection firewall type

Since each packet maintains the IP address of the source and destination for application layer inspection, the IP address is exposed to the external network leaving it susceptible to attack. The complexity of stateful inspection makes maintenance difficult. Since each packet is accepted based on the source and destination IP address and port numbers, as well as the application that should be handling such packets, a separate set of rules need to be defined for each application.

However complex the rules may be, the degree of security and the speed of the Stateful inspection method makes it worthwhile to run this type of firewall.

SECURE VERSUS INSECURE[1]

While firewalls are meant to protect systems, they cannot stop all threats. There are many attacks that can be prevented using a firewall. However, a great deal of attacks cannot be stopped. Following are the firewall limitations.

WHAT IS SECURE?

A firewall allows for one point of access, simplifying the security management. Since each arriving packet has to go through the firewall, the packets may be monitored. The log of packets alone allows you to see what kind of traffic is coming in and out of the system. Even if the bad guys are not stopped, at least there is a record of their activities.

[1] **[Chapman and Zwicky 1995]**

There are many different services on a network. Some can be less secure than others. Firewalls have the capability to restrict access to some of these services, allowing the user to specify which services are admitted. Blocking harmful services minimizes the threat from the external networks.

Firewalls have the ability to hide the system its protecting from the external network altogether. The IP address of the machine will simply not respond to any attempts to establish a connection. Not only will a firewall not allow outsiders to connect but it can also block the user from connecting to unsafe systems.

VULNERABILITIES

However strong the firewall may be, it is still possible to attack a system. The following describes different methods for which a firewall is ineffective.

Regardless of how secure the system may be, if you have a vindictive friend it would be very simple for them to sabotage your machine. Once an e-mail attachment from this individual was opened, the system could have been infected with either a virus or a trojan. A firewall will not defend from applications or attachments that are allowed to execute.

Now, imagine you would like to download software from the Internet. It would seem that it is a trusted source, although it may not be. It is possible for some attackers to hack into a web server and pretend the original website is still legitimate while they substitute the files you download for their own Trojan code. Again, firewalls cannot protect from downloaded applications that are allowed to execute. Hence even trusted applications should be questioned whether they are completely safe.

Attackers are constantly coming up with new ways to attack systems. Firewalls are designed to protect only from known threats. If the firewall is set up to allow trusted services, such as Internet Explorer (IE), the attacker could come up with a new attack hiding behind IE. As a result, the attack could not be stopped by a firewall if IE was allowed to access the Internet.

A firewall cannot protect from what it does not know. Viruses are constantly being created. Firewalls can only look at the IP addresses and the applications associated with the specific packets. However, if the virus definition is unknown, a firewall will not detect that the application you are about to run is infected with a virus. The need to have up to date Anti-virus software running is essential since it contains a list of known virus definitions, which will be detected if a virus was about to be executed on a machine.

COMMERCIAL FIREWALLS

There are numerous firewalls on the market, each having very positive features, but how do we choose. Following is a table listing some of the available firewalls. Each is described in terms of which firewall type it is, does it block per executable, can you block selected TCP ports, UDP ports, does it block ping (ICMP) packets, does it contain Intrusion Detection, and does it have integrated Anti-virus software. These are many of the features that are useful in a firewall. Let us examine the commercial firewalls.

Product Name[1]	Firewall type*	Blocked on per executable basis	Blocks selected TCP ports	Blocks selected UDP port	Blocks ICMP	Intrusion Detection	Integrated Antivirus
Kerio Personal Firewall 2.1	PF, SPF	YES	YES	YES	YES	NO	NO
Outpost Personal Firewall Pro 2.0	PF, SPF	YES	YES	YES	YES	YES	Yes, with add-on product
Private Firewall	PF, SPF	YES	YES	YES	YES	YES	NO
BlackICE PC Protection	PF, SPF	YES	YES	YES	YES	YES	NO
ZoneAlarm 2.6	PF, SPF	YES	YES	YES	YES	NO	NO
ZoneAlarm Pro 3.0	PF, SPF	YES	YES	YES	YES	NO	NO
ZoneAlarm Pro 4.0	PF, SPF	YES	YES	YES	YES	YES	NO
ZoneAlarm Plus 3.1	PF, SPF	YES	YES	YES	YES	NO	NO
Symantec Client Security	PF	YES	YES	YES	YES	YES	Yes, with add-on product
Norton Internet Security 2004	PF, SPF	YES	YES	YES	YES	YES	YES
Norton Personal Firewall 2003	Proxy	YES	YES	YES	YES	YES	Yes, with add-on product

Product Name[1]	Firewall type*	Blocked on per executable basis	Blocks selected TCP ports	Blocks selected UDP port	Blocks ICMP	Intrusion Detection	Integrated Antivirus
Sygate Secur Enterprise 3.0	PF, SPF	YES	YES	YES	YES	YES	NO
Sygate Personal Firewall PRO 5.0	PF, SPF	YES	YES	YES	YES	YES	NO
PortsLock	PF	YES	YES	YES	YES	NO	NO
SG100	SPF	YES	YES	YES	YES	NO	NO
Desktop Firewall 7.5	PF	YES	YES	YES	YES	YES	Yes, with add-on product
RealSecure Desktop Protector 3.5	PF, SPF, Proxy	YES	YES	YES	YES	YES	NO
CyberArmor Suite 2.2	PF, SPF, Proxy	YES	YES	YES	YES	YES	Yes, with add-on product
Tiny Firewall 5.0	SPF	YES	YES	YES	YES	YES	YES

* SPF – Stateful Packet Filter
PF – Packet Filter

[1] **[Network Computing 2002]**

CONCLUSION

Having a firewall to protect a machine or network is as essential to network security as a front door is to a house. It is a fundamental tool for securing a system. Choosing a suitable firewall can provide quite a challenge, having to consider many different components that it might contain.

RECOMMENDATIONS

Before installing a firewall, the system should be prepared. To begin with the system and all the installed applications must be patched with most recent updates. This will close all the possible security holes that even a firewall might not be able to catch. Once the system is up to date, it is time to select a firewall.

First, in order to prepare the rules for a firewall, the applications that are being used need to be identified and which protocols are to be allowed access to the Internet. Using this information, the firewalls rules can be developed. Next, it must be decided whether more than a firewall is required to protect the system. Some firewalls include anti-virus software and some even have an intrusion detection system. If these already exist on the system, the firewall need not include these.

Most firewalls on the market are similar in functionality. In order to select a suitable firewall, the technical level of the user should be considered, as some of these firewalls require more technical knowledge than others. Some firewall rules are complex to set up and maintain, hence if not configured properly the machine might be exposed to more than it should. When selecting a firewall, verify that the maintenance will be manageable. If either anti-virus software or intrusion detection system is in place, the user must be able to maintain these.

Once a suitable firewall is selected, the set of rules need to be defined. The firewall should be set up in such a way that the least amount of traffic is allowed to go out or to come in. The applications that do not need to access the Internet should not be allowed to do so. The applications that do access the Internet should specify exactly which port they should be using and the protocol that they will be using. Lastly, to make sure all the rules are working and are up to date, the firewall should be tested. Of course it is not possible to completely test the firewall but at least this prevents most of the day-to-day attacks.

FINAL REMARKS

Choosing a firewall is not easy. Many users will try more than one firewall before settling on one they like. It is a preference and depends on the user. The most important thing about firewalls is to keep all the rules up to date and accurate. Start the rules with the default of blocking all traffic. As the machine is used and applications do not function properly, revisit the firewall rules and allow the appropriate packets to enter and exit the system. This approach will allow the user to constantly be aware of what type of activities are taking place on the system. Firewalls are one of the basic ways to defend against harmful hackers. Use them!

BIBLIOGRAPHY

[Chapman and Zwicky 1995] D.B. Chapman and E.D. Zwicky, "Building Internet Firewalls," *O'Reilly & Associates, Inc.* (November 1995). ISBN: 1565921240

[Clavister 2003] "Firewall Basics," *Clavister.com* (2003) http://www.clavister.com/manuals/ver8.1x/manual/introduction_to_network_security/firewall_basics.htm

[Curtin and Ranum 2000] M. Curtin and M.J. Ranum, "Internet Firewalls: Frequently Asked Questions," (December 2000) http://www.interhack.net/pubs/fwfaq

[Cutler, Pole, Wack 2002] K. Cutler, J. Pole, J. Wack, "Guidelines on Firewalls and Firewall Policy," *National Institute of Standards and Technology* (January 2002)

[Edwards 1997] M.J. Edwards, "Internet Security With Windows NT," *29th Street Press* (January 1997). ISBN: 1882419626

[Fonda and Postogna 1997] C. Fonda F. Postogna, "Computer Networking Basics," *Scientific Computers System of Trieste* (October 1997) http://www.ictp.trieste.it/~radionet/1997_workshop/networking/basics.html

[Hunt 1998] C. Hunt, "TCP/IP Network Administration," *O'Reilly & Associates, Inc.* (January 1998). ISBN: 1565923227

[MOREnet 2003] MOREnet "An Introduction to Network Firewalls and the Firewall Selection Process," *Missouri Research & Education Network* (March 2003) http://www.more.net/technical/netserv/tcpip/firewalls/

[MSDN 2003] Microsoft MSDN, "International Organization for Standardization (IOS)" (February 2003) http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/international_organization_for_standardization_ios__2.asp

[Network Computing 2002] "Complete Buyer's Guide: Desktop Firewalls", *Network Computing* (September 2002) http://ibg.networkcomputing.com/ibg/Chart?guide_id=3984