

# Firewalls For Beginners

*Sunil Hazari* 2000-11-06

## Firewalls For Beginners

by *Sunil Hazari* ([Sunil@sunilhazari.com](mailto:Sunil@sunilhazari.com))

last updated Nov. 6, 2000

---

## Introduction

Access to e-mail and other Internet resources is very much a necessity for conducting business and accessing information. However, along with the convenience that network connectivity brings, it also raises serious security concerns. With [always-on connections](#) such as cable modems and [DSL lines](#), Internet users need to be increasingly vigilant of security issues, as network traffic coming into the computer can cause damage to files and programs even when the user is away from the computer and the computer is idle. In a system that is not protected with any security measures, [malicious code](#) such as [viruses](#) can infect systems and cause damage that may be difficult to repair. Unscrupulous characters on the Internet are always snooping around trying to find open computers from which they can steal personal files, personal information or create other forms of mischief. The loss of financial records, e-mail, customer files, can be devastating to a business or to an individual.

In conjunction with other security measures, [firewalls](#) can help to prevent this devastation.

## What are Firewalls?

Firewalls are tools that can be used to enhance the security of computers connected to a [network](#), such as a [LAN](#) or the Internet. A firewall separates a computer from the Internet, inspecting [packets](#) of data as they arrive at either side of the firewall ? inbound to, or outbound from, your computer ? to determine whether it should be allowed to pass or be blocked.

Firewalls act as guards at the computer?s entry points (which are called [?ports?](#)) where the computer exchanges data with other devices on the network. Firewalls ensure that packets that are requesting permission to enter the computer meet certain rules that are established by the user of the computer. Firewalls operate in two ways, by either denying or accepting all messages based on a list of designated acceptable or unacceptable sources, or by allowing or denying all messages based on a list of designated acceptable or unacceptable destination ports.

Although they sound complex, firewalls are relatively easy to install, setup and operate. This article will provide a brief introduction to firewalls. This is not intended to serve as a review of specific firewall products. Rather, it will serve as an overview of what firewalls are, how they work, the different types of firewall technology and their suitability for small office/ home office and personal computer users.

## TCP/IP

In order to understand how firewalls work it is important to understand the basics of [TCP/IP](#), the language or [protocol](#) which all computers on the internet use to communicate. If you are not at all familiar with concepts such as packets, ports and [IP addresses](#), please refer to the "Internet for Beginners" article at [LINK](#). If you are, the following section may seem elementary; however, it explains each of the aspects of TCP/IP as it relates specifically to firewalls.

Let's start by saying that TCP/IP is a "language" that allows different computers to communicate. On the Internet, this language is spoken and understood by all different types of computers, even those using different operating systems such as Windows, Macintosh, or Unix. In order for a computer to communicate on the Internet, it must "speak" TCP/IP.

## Packets

When messages are sent along the Internet, they are broken up into small "packets" that take different routes to get to the destination. On reaching the destination, the packets are re-assembled to form the complete original message. This method is similar to writing a letter, except the sentences that make up the letter are each sent in a separate envelope. With the large number of packets travelling the Internet, it is important that the content of the packets are transferred reliably and to the correct destination computer source information in the correct order - this is where TCP/IP comes in.

TCP/IP ensures that messages arrive at the proper computer in the proper order. Internet Protocol (IP) is used for addressing messages so they can be exchanged between the source computer and the destination computer. [Transmission Control Protocol \(TCP\)](#) is responsible for making sure the entire message is received in the correct format (this will be explained in more detail later in this section). These terms may seem technical but the main thing we have to remember is that TCP/IP makes information exchange over the Internet possible. And what

does this have to do with firewalls? Computers identify themselves using an IP address, which is similar to a street address. The IP address is a numerical translation of the web address. For example, the IP address of [www.securityfocus.com](http://www.securityfocus.com) is 207.126.127.69. When the message is in packet form, the destination address and the source address information are carried in the ? head? of the packet.

The IP address is an important concept in the discussion of firewalls because firewalls read the IP addresses in the head of the packets to determine the source of message. They then use part of that information to determine whether or not the message will be allowed access or not.

## Ports

We have talked about firewalls guarding the entry points of the computer system ? these entry points are known as ?ports?. Personal computers use TCP/IP ports to communicate with other computers. Simply put, a port is a point at which computers connect to networks and to other computers so that it can exchange information with networks and other computers. Personal computers have various types of ports, each of which provides a specific and unique service. Port numbers that are open indicate which applications or services that computer is currently running.

Each port has a specific number, and each one allows computers to exchange information related to a specific application. For instance, computers typically exchange information with the World Wide Web via port 80. The port number is held in the information in the packet header. This is important for firewalls, because by reading the packet the firewall can tell what application the message is trying to run. Firewalls can be configured to deny certain applications, which they determine by reading the port number of the incoming packet.

For example, one common service is [FTP, or file transfer protocol](#), which allows computers to exchange large files of text and graphics. The FTP server on a computer utilizes port #21. If the recipient computer is open to accepting FTP packets, it will accept packets that indicate that they are FTP packets by the inclusion of port #21 in their header. If, for instance, the recipient computer is not running FTP, it would not be open to receiving information that is addressed for port #21. Thus the firewall should be configured to deny access to any packets that are destined for that port number.

Some common TCP/IP ports and their corresponding numbers are:

- FTP (File Transfer Protocol) - #21
- SMTP (Simple Mail Transfer Protocol) - #25
- Login (Login Host Protocol) - #49
- HTTP (Hypertext Transfer Protocol) - #80
- Auth (Authentication service) - #113
- Audionews (Audio news multistream) - #114

## Port Scanners

[Hackers](#) often use software tools called [port scanners](#) to find services, such as the ones we just mentioned. Once the port scanner finds a service or an [application](#) that is running, the hacker then determines whether or not that specific service is vulnerable to attack. When they find vulnerable applications, the hacker may exploit them to gain entry into the system. Once inside the system, hackers proceed to attack the target and disrupt services by deleting or transferring critical files or by reading and/or stealing information that is stored on the computer.

There are 65,535 virtual ports on a typical personal computer that can be used to gain entry. The firewall has to keep an eye on each one of these ports. Talk about having a tough job!

## Types of Firewalls

We can think of firewalls as being similar to a bouncer in a nightclub. Like a bouncer in a nightclub, firewalls have a set of rules, similar to a guest list or a dress code, that determines if the packet should be allowed entry. Just as the bouncer places himself at the door of the club, the firewall is located at the point of entry where data attempts to enter the computer from the Internet. But, just as different night clubs might have different rules for entry, different firewalls have different methods of inspecting packets for acceptance or rejection.

## Packet Filtering

The most common firewall method is known as [packet filtering](#). Maintaining our bouncer analogy, some bouncers may only check ID's and compare this with the guest list before letting people in. Similarly, when a packet filter firewall receives a packet from the Internet, it checks information held in the IP Address in the header of the packet and checks it against a table of access control rules to determine whether or not the packet is acceptable.

In this case, a set of rules established by the firewall administrator serves as the guest list. These rules may specify certain actions when a particular source or destination IP address or port number is identified. For example, access to a pornographic web site can be blocked by designating the IP address of that site as a non-permitted connection (incoming or outgoing) with the user's computer. When the packet filter firewall encounters a packet from the porn site, it examines the packet. Since IP address of the porn site is contained in the header of the packet, it meets the conditions that specifically deny such a connection and the web traffic is not permitted to go through.

Although packet filters are fast, they are also relatively easy to circumvent. One method of getting around a packet filter firewall is known as [IP spoofing](#), in which hackers adopt the IP address of a trusted source, thereby fooling the firewall into thinking that the packets from the hacker are actually from a trusted source. The second fundamental problem with packet filter firewalls is that they allow a direct connection between source and destination computers. As a result, once an initial connection has been approved by the firewall, the source computer is connected directly to the destination computer, thereby potentially exposing the destination computer and all the computers to which it is connected to attack.

## Stateful Packet Inspection

A second method utilized by firewalls is known as [stateful packet inspection](#). Stateful packet inspection is a form of super-charged packet filtering. It examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. It is called a "stateful" packet inspection because it examines the contents of the packet to determine what the state of the communication is - i.e. it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, Stateful inspection firewalls also close off ports until connection to the specific port is requested. This allows an added layer of protection from the threat of port scanning.

## Application-Level Proxy

Other types of bouncers have stricter rules: they not only want to know who the guest is, but

what he or she will be doing once they are inside the club. In the world of firewalls, this type of bouncer is known as an [application-level proxy](#) because it determines if a connection to a requested application is permitted. Only connections for specified purposes, such as Internet access or e-mail, will be permitted. This allows system administrators to control what applications their system's computers will be used for.

For example, [hackers](#) can use the [Telnet](#) service (which in the early days of the Internet was developed to allow remote logins to computers) to gain unauthorized access to a network. However, a firewall can be setup to allow only web and e-mail applications to gain access. The firewall can be programmed to stop all packets with the destination port of 23, which is the standard port for Telnet. Any attempt by hackers to telnet into the user's computer will fail because the application level firewall will recognize this telnet connection as a non-web/e-mail application and reject the information trying to enter the user's computer.

This type of firewall is known as an application-level proxy because, in addition to screening packets for the type of application they want to run on the user's computer, they also serve as a [proxy server](#). A proxy can be thought of as a computer that sits between a computer and a web server and acts as a middleman between the computer and the web server.

An application-level proxy receives all communications requests from the computers behind it (or inside the firewall.) It then proxies the request; that is, it makes the requests on behalf of its constituent computers. What this does is to effectively hide the individual computers on the network behind the firewall. The targeted computers are protected from view because outside sources never make direct contact with the computers - every communication is conducted through the proxy server.

## Network Address Translation (NAT)

[Network Address Translation \(NAT\)](#), serves as a firewall by keeping individual IP addresses hidden from the outside world. Similar to a proxy server, Network Address Translation acts as an intermediary between a group of computers and the Internet. NAT allows an organization to present itself to the Internet with one address. NAT converts the address of each computer and device on a LAN into one IP address for the Internet and vice versa. As a result, people scanning the Internet for addresses cannot identify the computers on the network or capture any details of their location, IP address, etc. And if the bad guys can't find you, they can't hurt you.

## Drawbacks to Using Firewalls

Although firewalls have their strengths, and are an invaluable information security resource, there are some attacks that the firewalls cannot protect against, such as eavesdropping or interception of e-mail. Furthermore, whereas firewalls provide a single point of security and audit, this also becomes a single point of failure? which is to say, firewalls are a last line of defense. This means that if an attacker is able to breach the firewall, he or she will have gained access to the system, and may have an opportunity to steal data that is stored in that system, or to create other havoc within the system. Firewalls may keep the bad guys out, but what if the bad guys are inside? In the case of dishonest or disgruntled employees, firewalls will not provide much protection. Finally, as mentioned in the discussion of packet filtering, firewalls are not foolproof - IP spoofing can be an effective means of circumvention, for example.

For optimal protection against the variety of security threats that exist, firewalls should be used in conjunction with other security measures such as anti-virus software and encryption packages. As well, a well-thought out and consistently implemented security policy is vital to attaining optimal effectiveness of any security software.

## Selecting Firewalls

Firewall applications vary in sophistication and cost. For the small office or home user, the easiest and least expensive firewall solutions are personal firewalls, which are software programs that install on your computer. When selecting firewalls, the following considerations should be taken into account:

- Ease of installation/configuration
- Does the firewall run without user intervention?
- Are there parameters that have to be set, and is it easy to do?
- Is there online help or technical support available?
- Does the firewall provide audit reports identifying time, location and type of attack?
- Is the cost of the firewall appropriate to the size of your business/office?
- Are maintenance/ monitoring requirements suitable for the size and type of business?
- What will be the training requirements for the firewall?
- Will the firewall have a significant impact on the operation of the system as a whole?

There are a number of firewall products available with varying feature capabilities and costs.

Most of the vendors offer a free trial for evaluation purposes and SOHO users should select one based on their needs.

---

*Dr. Sunil Hazari is a faculty member in the Smith School of Business and Office of Information Technology at University of Maryland, College Park. His teaching and research interests are in the areas of E-commerce security, usability, and infrastructure. <http://sunil.umd.edu>.*

#### Relevant Links

##### [Shields Up!](#)

*By Steve Gibson, Gibson Research Corporation*

##### [What is a Firewall](#)

*By E-Labs*

##### [Turning Up The Heat On SOHO Firewalls](#)

*By Mike Fratto, Network Computing*

##### [Personal Firewalls](#)

*By Gary Flynn*

[Privacy Statement](#)

Copyright 2006, SecurityFocus