Firewalls

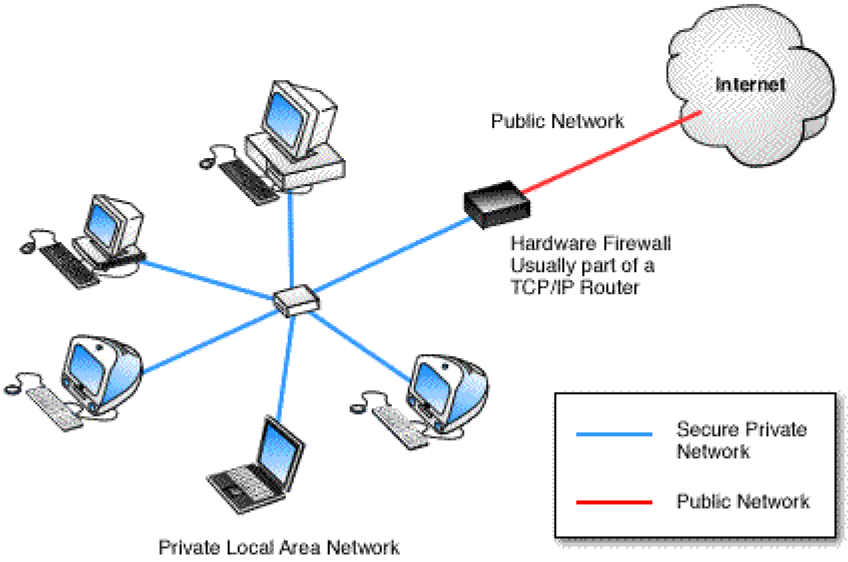
Alexander Khodenko

May 01, 2003

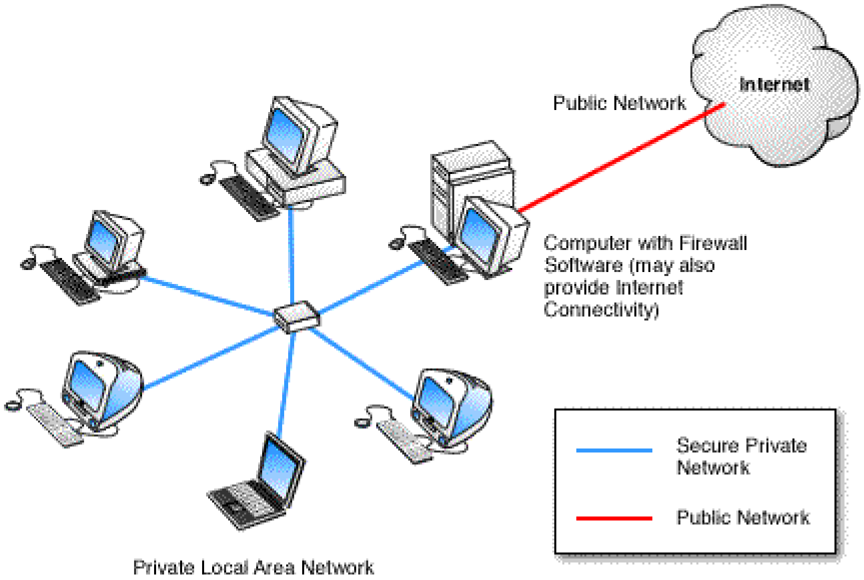
Firewalls

Firewall is defined as a linkage in a network, which relays only those data packets that are clearly intended for and authorized to reach the other side. Firewalls are helpful in keeping computers safe from intentional cracker attacks and hardware failures occurring elsewhere.

The performance of a firewall is similar to that of a physical wall that helps to keep fire from spreading. A firewall is a program or a hardware device that filters the incoming pockets of information (Figure1hardware device, & Figure 2 software program).



(Figure 1; Vicomsoft, 2003.)


Internet
Public Network
Computer with Firewall Software (may also provide Internet Connectivity)
Secure Private Network
Public Network
Private Local Area Network

(Figure 2; Vicomsoft, 2003.)

If certain types of packets are marked by firewall filters, they will not be permitted to go through the firewall into the system. The major two functions of a firewall:

1. It permits traffic
2. It blocks traffic

If a computer user does not have a firewall, his computer can be easily accessed by anyone on the Internet. Crackers can probe unprotected computers by establishing FTP and Telnet connections. **FTP (**File Transfer Protocol) defines rules according to which files can be transferred from one computer to another on the Internet and TCP/IP networks. **Telnet** is a command that allows the user to use his computer as a terminal through a network. Usually, the Telnet program provides a direct path so that the remote computer is able to communicate directly with the terminal computer.

Firewalls allow establishment of security rules for FTP, Telnet, and network connections. Firewalls use from one to three methods of traffic control:

- **Packet Filtering**-when data packets are analyzed against a set of filters.

- **Proxy Service**-when the information from the Internet is retrieved by the firewall and then is sent to the system.
- **Stateful Inspection**-occurs when certain key parts of packets are compared to a database of trusted information.

Protection by Firewalls

Generally speaking, firewalls protect against unauthorized interactive logins. There are many malicious intruders on the Internet who will not miss their chance to break into someone's computer in order to get information and/or disrupt computer's work.

Firewalls have different security levels:

- **Block all** – blocks all the traffic, thus preventing all information entering and/or leaving one's computer from any outside sources. The user is capable of defining which programs or information is allowed to enter or leave his computer.
- **Normal level** – is usually a configurable setting that blocks any application until the user grants a permission for an access.
- **Allow all** – is the least secure level that permits transmission of all traffic including the Internet, but still, logs are created.

In addition, a firewall can be used as an effective tracing tool. Through the security logs, the user is capable to trace intruders. Unfortunately, often the source that has been traced is not the hacker's computer, but the public router that was used by the hacker to initiate an attack.

Even though firewalls are helpful in protecting against attacks, there are many other important for security factors that may play a role. Having firewalls in an organization does not ensure that there will not be treacherous activities within the organization. For this reason, the overall organizational security must be assured. Firewall policies have to reflect the level of security in the entire network. For an organization with top security data, it might be appropriate to isolate this data from the rest of the network instead of having a firewall with liberal access to the data. Firewalls will not protect organizations against traitors who work inside the network. Firewalls do not prevent information leakage. Information can be leaked through phones, fax machines, CD and floppy disks, and by other means of communication. Firewalls cannot replace security-consciousness of users.

In addition, it is hard for firewalls to protect from:

- **Remote Login –** when someone connects to a computer of another and takes control of it in some form.
- **Application Backdoors** – some programs have special features that allow for remote access. Other programs may contain bugs that allow for hidden access.
- **SMTP Session Hijacking – SMTP** stands for Simple Mail Transport Protocol and is used to send text-based information such as e-mails. By gaining access to a list of e-mail addresses, one can send spam to thousands of users.
- **Operating System Bugs –** Operating systems have backdoors as well as some program applications. Experienced crackers may take advantage of them.
- **Denial of Service –** occurs when a cracker sends multiple session requests to a server. As a result, users are unable to access it; server slows down and even may eventually crash.
- **E-Mail Bombs** – occur when somebody sends the same e-mail hundreds and even thousands of times until no more messages can be accepted.
- **Macro Viruses** – viruses written using the macro language of a particular application. Generally, macros are used by many applications to simplify complicated procedures.

Crackers create their own scripts that are able to destroy the data on one's computer, or even crash it.

- **Computer Viruses** – small programs that copy themselves and disrupt the operation of one's computer. They are capable of destroying data and/or play different kinds of tricks.
- **Spam** – junk mail, but in electronic form. Often, letters contain links to web sites. By clicking on a link, one's computer may accept a cookie thus providing for an access to his computer through a backdoor.

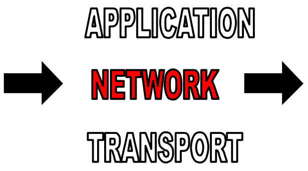
Types of Firewalls

Firewalls can be classified by technology and by intended application. There are four types of firewalls classified by technology:

1. Packet Filtering
2. Circuit Gateways
3. Application Proxies
4. Hybrid

Packet Filtering

Packet filtering firewalls are functioning at the IP packet level. All the pockets are inspected against the firewall rules. If they meet requirements, they might be allowed to go through, if not, then they are blocked (Figure 3).



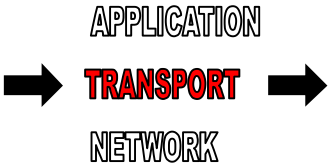
(Figure 3)

Filtering firewalls can be classified according to types of filtering:

- **Static Filtering** – is being implemented by most routers. Rules of filters are adjusted manually.
- **Dynamic Filtering** – allows filtering rules to change depending on responses to outside processes.
- **Statefull Inspection** – filtering is similar to dynamic filtering. The difference is that in addition to dynamic filtering, packets are inspected more carefully.

Circuit Gateways

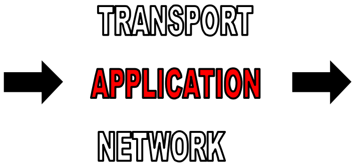
Circuit gateways firewalls function at the network transport layer (Figure 4). They allow or deny connections based on addresses and prevent direct connection between networks.



(Figure 4)

Application Proxies

Application proxy-based firewalls function at the application level (Figure 5) where all the data passes through an application server and is examined as the entire stream, and not per-packet.



(Figure 5)

Hybrid Firewalls

Hybrid firewalls as the name suggests, represent a combination of technologies. A hybrid firewall may consist of a pocket filtering combined with an application proxy firewall, or a circuit gateway combined with an application proxy firewall.

The following types of firewalls are classified by intended application:

1. PC Firewalls
2. SOHO Firewalls
3. Firewall Appliances
4. Large Enterprise Type Firewalls

PC Firewalls – are known as firewalls for personal use and are designed in such a way as to provide a satisfactory level of protection to users of single computers.

SOHO Firewalls – Small Office/Home Office firewalls are designed for small businesses with no dedicated information technology personnel. These type of firewalls offer simple configuration and sophisticated security levels. Usually SOHO firewalls are hardware appliances.

Firewall Appliances – aimed at meeting requirements of small businesses and remote offices of large enterprises. Firewall appliances are specialized systems with fewer option configuration in comparison to those of a large enterprise firewalls. The distinction between firewall appliances and large enterprise level firewalls is identified in lesser amount of functionality, and absence of unnecessary security levels.

Large Enterprise Type Firewalls – are usually hardware devices with extra features required for protection of a large business. These features typically include centralized administration, multi-firewall administration, and support for Internet, Intranet, and Extranet services.

Firewall Components

A typical firewall consists of:

- Console
- Logs
- Application List
- Configurable Options
- Advanced Rules

Console – Provides constant updates on one's computer network traffic, status of security level and status of applications. The user is able to navigate anywhere else within the console. Many firewalls have an alert mode that alerts the user when an attack is in progress.

Logs – Typically, there are three types of logs:

1. Security Log
2. System Log
3. Traffic and Pocket Logs.

The Security Logs – record potentially threatening activities directed at one's computer network. These can be port scanning, or denial of service attacks. Usually, logged events are arranged in such a way as to provide information about the date and time of the event, number of attacks, their severity, and direction (inbound or outbound). Most attacks are incoming, but if a user downloaded Trojan Horses to his computer, they might become outgoing.

System Logs – record operational changes such as software execution errors, software modifications, and beginning and ending of services. The system logs are especially useful for troubleshooting because they carry information about errors and warnings.

Traffic and Pocket Logs – allow to capture and record all the data that enters or leaves one's computer. It gives information about the type of traffic that passed through the firewall, and the kind that was blocked. It might display protocol types by the use of which the traffic moved, the date and time, the number of events that occurred during a certain period, the IP address of the attempted attack, the name of the host computer, and even IP address of the user.

Application List – is a list of the running applications. It displays all applications and services that are accessing or attempting to access one's network. The user is usually able to make changes to the list by restricting access to some applications and giving permission to others.

Configurable Options – allow the user to set up:

1. notification for attacks against one's computer
2. log files
3. network browsing rights
4. password protection

E-Mail Notification – function allows to have an e-mail sent immediately and/or at regular intervals to the administrator of the network, investigative authorities, or anybody whose address was pre-programmed.

Log Files – can be configured according to preferences of the firewall administrator. Typical configuration allows setting the size of logs and log days.

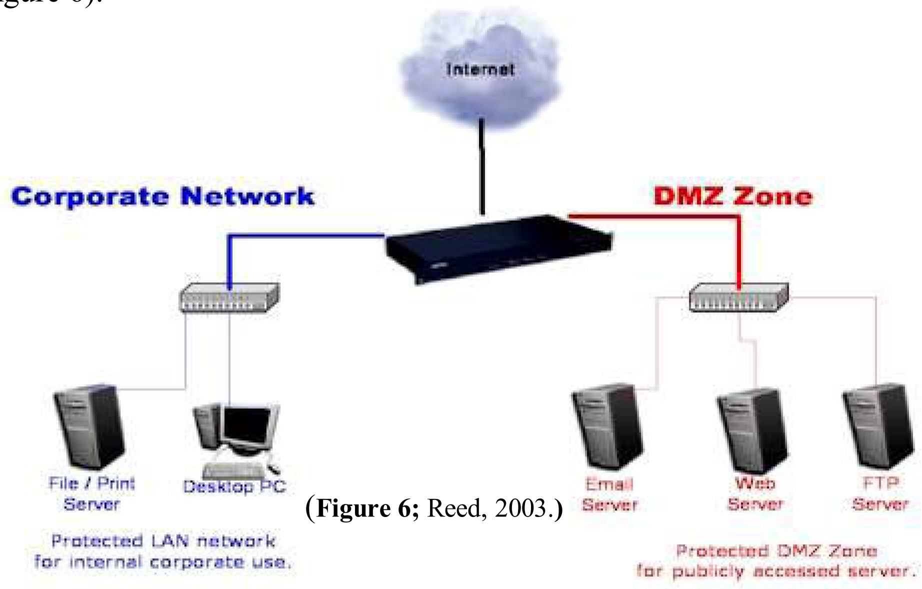
Network Browsing Rights – allow adjusting settings to network interface. The administrator can decide whether to allow or limit access to certain files on the computer and hardware devices.

Password Protection – plays an important role in a firewall administration. It allows protecting the settings from being changed by another user. At the prompt, the user is required to enter a password every time he tries to access firewall's settings.

Advanced Rules – are usually rules that apply to all applications. Such a configuration is useful to those administrators who wish to create universal settings for the firewall they use. Since there are different characteristics of traffic, the administrator can specify the kind of traffic he wants to have controlled. Some firewalls allow to schedule the time for rules to be applied. For example, the administrator may set the rule to block all the traffic after 00:00 hours and have it resumed after 06:00 hours.

DMZ

"DMZ" is an abbreviation for Demilitarized Zone. "DMZ" is an area outside the firewall. It is not a part of the network or the Internet, but an area that is between the end points (Figure 6).


Internet
Corporate Network
DMZ Zone
File / Print Server
Desktop PC
Email Server
Web Server
FTP Server
Protected LAN network for internal corporate use.
Protected DMZ Zone for publicly accessed server.

(**Figure 6;** Reed, 2003.)

The “DMZ” enhances safety by keeping malicious outsiders on the Internet from accessing the private network. The safety and security of networks can significantly be enhanced through the proper combinatorial use of firewalls and demilitarized zones.

Summary

Firewalls are software or hardware devices that help to keep computers safe and secure from intentional attacks of crackers.

The major two functions of a firewall are to permit or block the traffic depending on the needs, rules, and policies of an organization or individuals.

Firewalls can be classified by technology and intended application. There are four types of firewalls classified by technology: Packet Filtering, Circuit Gateways, Application Proxies, and Hybrid. Firewalls classified by intended application are PC firewalls, SOHO firewalls, Firewall Appliances, and Large Enterprise Type firewalls.

Demilitarized Zone is a good addition to a firewall that makes a network safer. It is very important to understand and remember that a firewall by itself will not make a network safer and more secure without the proper combination and use of all known security measures.

Address your comments and/or questions to:

Alexander Khodenko

Khodenko@MSN.com

Publication Notice

Bibliography

Curtin, C. Matthew (2001, July 02). Internet Firewalls: Frequently Asked Questions [Message – ID: 9hpldl$3r2$1@news.cis.ohio-state.edu]. Message posted to http://www.faqs.org/faqs/firewalls-faq/

Downing, D., Covington, M., & Covington M. M. (2000). Dictionary of Computer Internet Terms. New York: Barron's Educational Series, Inc.

How Stuff Works. (1998-2003). How Firewalls Work. Retrieved February 02, 2003, from http://computer.howstuffworks.com/firewall.htm/printable

ICSA Lab. (2003). Types of Firewalls. Retrieved March 30, 2003, from http://www.icsalabs.com/html/communities/firewalls/buyers guide2001/chap 2.shtml

ICSA Lab. (2003). Common Pitfalls of Firewall Deployment and How to Avoid Them. Retrieved March 30, 2003, from http://www.icsalabs.com/html/communities/firewalls/buyers guide2001/chap 5.shtml

Reed, B.A. (2003). The DMZ Zone Explained. Retrieved April 17, 2003, from http://www.firewalls.com/document-dmz.asp

Sygate Technologies. (2003). Sygate Product Documentation. Retrieved March 13, 2003, from http://soho.sygate.com/support/documentation.htm

Vicomsoft. (2003). KnowledgeShare-White Papers. Retrieved February 16, 2003, from http://www.vicomsoft.com/knowledge/reference/firewalls.html