Firewall: Software and Hardware Implementations

Dhiraj Kumar Banwal, Sanjay Kumar, Indresh Singh Rawat
1Dept. of IT, Govt. Polytechnic, Narendra Nagar (TG), UK, India
2Dept. of CE, Govt. Polytechnic, Narendra Nagar (TG), UK, India
3Technical Support Manager, Tula’s Institute (The Engineering & Management College), Dehradun, UK, India

Abstract
A firewall is simply a program or hardware device that filters the information coming through the Internet connection into the private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. In this research paper we mainly focus on the working of the firewall along with its software and hardware type.

Keywords
Software Firewall, Hardware Firewall, Security, Antivirus

I. Introduction
A Firewall is defined as any device (Hardware) or software used to filter or control the flow of traffic. Firewall are typically implemented on the network parameter and function by defining trusted and untrusted zones.

Fig. 1: Firewall

Firewalls are mostly used to consist of simple mechanisms to controlling access into and out of the company or a firm. Traditional firewall techniques such as port blocking and NAT (Network Address Transition) still play a massive part; however on their own they do not have the in depth power to stopping today’s threats. The primary job of a firewall is to protect the company’s network from internet threats and to enforce company security policies. The security policy will dictate what applications, services, ports and IP addresses are allowed and disallowed via the firewall. Companies are in need of firewall’s that do not only consist of advanced protection tools, but also have other built in advanced capabilities for other uses, such as VPN’s, WAN optimization. Failover and high availability, VLAN support, Dynamic routing, logging and reporting and other very handy utilities.

Now a days the firewall releases are becoming easier to use and offer user-friendly interface. There are essentially two forms of firewall that typical home user will frequently encounter. The first is a hardware or firmware firewall, which is usually found in a home router. This type of firewall is pre-configured from the factory to prevent unauthorized access of a wireless or wired network from intruders. It can be further customized by the user to block specific ports, which will prevent certain programs from accessing the Internet. Sometimes it is forced to customize the router firewall to allow certain programs access to the Internet. PC games sometimes conflict with router firewalls.

Another common form of firewall is a software firewall. A software firewall monitors Internet traffic going into and out of a specific PC. Should suspicious activity be noticed, it will be blocked, and in most cases a pop-up notice will alert whoever is using the PC. A software firewall can also be used to block or enable Internet access for specific programs, and the process of doing so is often easier than doing so via a router. The downside is that access will only be shut down for the PC that the software firewall is installed on.

II. Benefits of a Firewall
The Internet has made a large amount of information available to us. People of all ages enjoy browsing websites for different purposes, whether it is for education, entertainment, for business or any other reason. But connecting a computer or a private network to the Internet is always a security risk. A computer connected to the web has to be willing to accept information from outside sources and send information back to them. While there are rules for how this information must be sent, those rules can be bent or broken.

Fig. 2: Implementation of Firewall

That is why we need a Firewall. Anyone who connects to the Internet, as a single computer or whole network, should use a firewall. A Firewall can protect both individual computers and corporate networks from security threats such as worms, which attempt to exploit networking protocol to access a remote PC. A firewall can also log all attempts to enter private network or an individual computer and set an alarm when suspicious or hostile activity is attempted. Some firewalls can also monitor and log all outbound data traffic and prevent unauthorized access to resources on external networks.

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing
private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques. It includes:

A. Packet Filters
Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

B. Application Gateway
Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

C. Circuit-Level Gateway
Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

4. Proxy Server
Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses. In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. Small business firewall software is one method used to protect computers against hacker attacks and other Internet threats. Another method is to deploy a hardware firewall (which also uses software). The following is a guide to understanding the differences between small business firewall software and hardware firewalls.

III. Software Firewalls
Small business firewall software and hardware solutions are both designed to block unauthorized access to computers. Firewalls help prevent hackers from intercepting private data or planting Trojan horses or other Internet threats on your networked computers. A small business firewall software program is installed on each individual PC it's meant to protect. To safeguard all your company's computers, however, each one must have a software firewall installed. This can become expensive and difficult to maintain and support. In addition, small business firewall software may require each individual user to make decisions about allowing or denying a program's requested access to the Internet which helps prevent malware from sending proprietary information from your computer over the Internet, among other things. Users without much computer or security experience may be uncomfortable handling the requests and alerts that small business firewall software presents to them.

For individual home users, the most popular firewall choice is a software firewall. Software firewalls are installed on your computer like any software and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system. Additionally, software firewalls may also incorporate privacy controls, web filtering and more. The downside to software firewalls is that they will only protect the computer they are installed on, not a network, so each computer will need to have a software firewall installed on it. A good software firewall will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer. The differences between a software and hardware firewall are vast, and the best protection for your computer and network is to use both, as each offers different but much needed security features and benefits. Updating your firewall and your operating system is essential to maintaining optimal protection, as is testing your firewall to ensure it is connected and working correctly.

IV. Hardware Firewalls
Hardware-based firewalls protect all the computers on your network. A hardware-based firewall is easier to maintain and administer than individual software firewalls. The ideal solution for small businesses is a hardware firewall integrated into a comprehensive security solution. In addition to a firewall, the solution should include Virtual Private Network (VPN) support, antivirus, anti-spam, antispyware, content filtering, and other security technologies.

Hardware firewalls can be purchased as a standalone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available. A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped. As with any electronic equipment, a computer user with general computer knowledge can plug in a firewall, adjust a few settings and have it work. To ensure that your firewall is configured for optimal security and protect however, consumers will no doubt need to learn the specific features of their hardware firewall, how to enable them, and how to test the firewall to ensure its doing a good job of protecting your network.

V. Conclusion
Hardware firewall security as well as software firewall is the efficient technique to protect our computer system or network. But before implementing it we have to ensure its reliability that can be obtained by purchasing third-party test software or search the Internet for a free online-based firewall testing service. Firewall testing is an important part of maintenance to ensure the system is always configured for optimal protection.

References


Mr. Dhiraj Kumar Banwal is working as Lecturer in Department of IT in Govt. Polytechnic, Narendra Nagar (TG) Under the Department of Technical Education, Govt. of Uttarakhnd, India. He have Nine year Experience of teaching in Govt. as well as Private Engg. College and he also worked as examination controller in Engg. College And he had external practical examiner of IGNOU.

Mr. Sanjay Kumar Is working as HOD in Department of CSE in Govt. Polytechnic, Narendra Nagar(TG)Under the Department of Technical Education , Govt. of Uttarakhnd. (India), He have Eleven year Experience of teaching in Govt. as well as Private Engg. College and he also worked as examination controller in Uttarakhnd Board of Technical Education, Roorkee.
Indresh Singh Rawat is working as Technical Support Manager in the Tula’s Institute (The Engineering & Management College), Dehradun, UK, India.