INTERNET SECURITY: THE ROLE OF FIREWALL SYSTEM

Okumoku-Evroro Oniovosa
Lecturer, Department of Computer Science
Delta State University, Abraka, Nigeria
Email: *victorkleo@live.com*

ABSTRACT

Internet security has become a major issue in the current trend of things. And it's like an evil which if left to spread will in no time have effects on us all. This study thus examined internet security with a look at firewall and how it can help secure the internet. A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. The work descriptively identified packet fillters, circuit-level gateway and proxy server as the different types of firewall techniques. This paper observed that firewall has played a major role in Internet security and however advocates that it should be improved upon in order to assure the users of the Internet of security and unauthorizes access.

Keywords: *Firewall, computer traffic, network, packet filters.*

INTRODUCTION

Today, Internet has been dangerous place for the computer; there is no justification denying it. A few years ago you could happily go about your business on the web without any form of protection, and still face only a slim chance of being virus infested, hacked or otherwise interfered with. These days it is practically impossible. There are vast amounts of viruses and malware infections moving through the Internet, many of which need no prompting or permission to infect an unprotected computer. Gralla (2007) sees Internet security as a branch of computer security specifically related to the Internet. Its objective is to establish rules and measure to use against attacks over the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. A firewall is a hardware or software system that prevents unauthorized access to or from a network. They 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. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud (Rhee, 2003).

Generally, firewalls are configured to protect unauthenticated interactive logins from the outside world. This helps prevent hackers from logging into machines on your network. More firewalls that are sophisticated block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside. Firewalls are essential since they can provide a single block point where security and auditing can be imposed. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what type/volume of traffic has been processed through it. This is an important point since providing this block point can serve the same purpose (on your network) as an armed guard can (for physical premises). A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or 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.

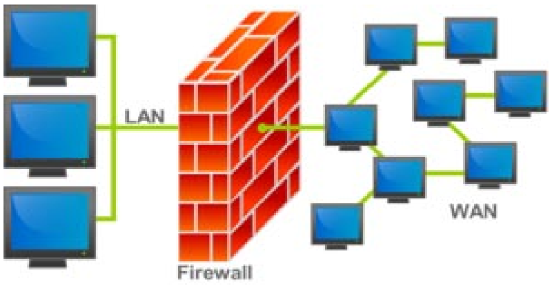

Figure 1: An illustration of how a firewall works.

In the illustration above the block in between represents the firewall, while the network at your left hand side Local Area Network (LAN) represent your home or office network and the one on your right side Wide Area network (WAN) represent all internet users.

TYPES OF FIREWALL TECHNIQUES

Packet filters: According to Kurose and Ross, (2007) a packet consists of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination addresses, error detection codes like checksums, and sequencing information. Typically, control information is found in packet headers and trailers, with user data in between.

Circuit-level gateway: Applies security mechanisms when a Transmission Control Protocol (TCP) or User datagram Protocol (UDP) connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

How Firewall Software has helped internet security

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. It is a hardware or software system that prevents unauthorized access to or from a network. A firewall helps protect computers inside a large company. Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make File Transfer Protocol (FTP) connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the Machine and exploit the hole. With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet. The firewall can implement security rules. For example, one of the security rules inside the company might be: Out of the 500 computers inside this company, only one of them is permitted to receive public FTP traffic. Allow File Transfer Protocol (FTP) connections only to that one computer and prevent them on all others.

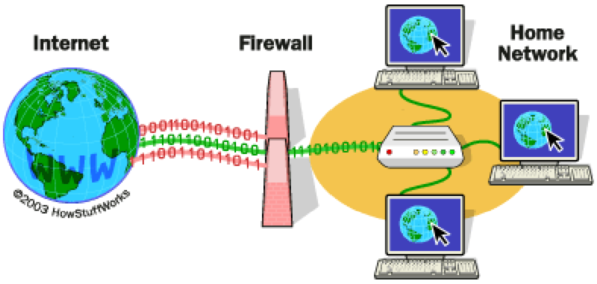

Figure 2: Firewall Protecting a Home Network

Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why it's called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next.

TYPES OF FIREWALLS

Firewalls are divided into five basic types: Packet filters, Stateful Inspection, Proxies, Dynamic, and Kernel. These divisions however are not well defined as most modern firewalls have a mix of abilities that place them in more than one of the categories shown above. To simplify the most commonly used firewalls, expert Chris (2009) breaks them into two categories: application firewalls and network layer firewalls. The International Standards Organization (ISO) Open Systems Interconnect (OSI) model for networking defines seven layers, where each layer provides services that higher-level layers depend on. The important thing to recognize is that the lower level the forwarding mechanism, the less examination the firewall can perform.

Network layer firewalls generally make their decisions based on the source address, destination address and ports in individual IP packets. A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from. Modern network layer firewalls have become increasingly more sophisticated, and now maintain internal information about the state of connections passing through them at any time. One important difference about many network layer firewalls is that they route traffic directly through them, which means in order to use one, you either need to have a validly-assigned IP address block or a private Internet address block. Network layer firewalls tend to be very fast and almost transparent to their use. Application layer firewalls defined are hosts running proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and gets out from the other side, after having passed through an application that effectively masks the origin of the initiating connection (Chris, 2009). However, run-of-the-mill network firewalls cannot properly defend applications. Application-layer firewalls offer Layer 7 security on a more granular level, and may even help organizations get more out of existing network devices. In some cases, having an application in the way may impact performance and may make the firewall less transparent. Early application layer firewalls are not particularly transparent to end-users and may require some training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

The future of firewalls sits somewhere between both networks: layer firewalls and application layer firewalls. It is likely that network layer firewalls will become increasingly aware of the information going through them, and application layer firewalls will become more and more transparent. The end result will be a fast packet-screening system that logs and checks data as it passes through.

FIREWALL CONFIGURATION

Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are:

Internet Protocol Addresses: Each machine on the Internet is assigned a unique address called an Internet Protocol address. Internet Protocol addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical Internet Protocol (IP) address looks like this: 216.27.61.137. For example, if a certain Internet Protocol address outside the company is reading too many files from a server, the firewall can block all traffic to or from that Internet Protocol address.

Domain Names: Because it is hard to remember the string of numbers that make up an Internet Protocol address, and because Internet Protocol addresses sometimes need to change, all servers on the Internet also have human-readable names, called domain names. For example, it is easier for most of us to remember www.yahoo.com than it is to remember 216.27.61.137. A company might block all access to certain domain names, or allow access only to specific domain names.

Protocols: The protocol is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation. The http in the Web's protocol. Some common protocols that firewall filters can be set for include:

IP (Internet Protocol)*:* The main delivery system for information over the Internet

TCP: (Transmission Control Protocol): Used to break apart and rebuild information that travels over the Internet

HTTP (Hyper Text Transfer Protocol): Used for Web pages

FTP (File Transfer Protocol): Used to download and upload files

UDP (User Datagram Protocol): Used for information that requires no response, such as streaming audio and video

ICMP (Internet Control Message Protocol): Used by a router to exchange the information with other routers

SMTP (Simple Mail Transport Protocol): Used to send text-based information (e-mail)

SNMP (Simple Network Management Protocol): Used to collect system information from a remote computer

Telnet: Used to perform commands on a remote computer

A company might set up only one or two machines to handle a specific protocol and ban that protocol on all other machines.

Ports: Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the internet. For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. A company might block port 21 access on all machines but one inside the company.

Specific Words and Phrases: The firewall will sniff (search through) each packet of information for an exact match of the text listed in the filter. For example, you could instruct the firewall to block any packet with the word "X-rated" in it. The key here is that it has to be an exact match. The "X-rated" filter would not catch "X rated" (no hyphen). But you can include as many words, phrases and variations of them as you need. Some operating systems come with in-built firewall. Otherwise, a software firewall can be installed on the computer in has an Internet connection. This computer is considered a gateway because it provides the only point of access between your home network and the Internet.

With a hardware firewall, the firewall unit itself is normally the gateway. A good example is the Linksys Cable/DSL router. It has an in-built Ethernet card and hub. Computers in your home network connect to the router, which in turn is connected to either a cable or DSL modem. You configure the router via a Web-based interface that you reach through the browser on your computer. You can then set any filters or additional information. Hardware firewalls are incredibly secure and not very expensive.

How To Switch ON/OFF Windows Firewall

To enable Windows Firewall, follow these steps:
Step1: Click Start; click Run, type Firewall.cpl, and then click OK.
Step 2. On the General tab, click On (recommended).
Step 3. Click OK.
To disable Windows Firewall, follow these steps:
Step 1. Click Start; click Run, type Firewall.cpl, and then click OK.
Step 2. On the General tab, click Off (not recommended).
Step 3. Click OK.

Note: These steps are only for Windows XP SP2 and Windows XP SP3. These steps are not for earlier versions of Windows XP.

Note: When you turn off the firewall, you leave your computer vulnerable to attack. Therefore, before you turn off your firewall, disconnect your computer from all networks. This includes the Internet.

CONCLUSION

Internet security has become a major concern as many businesses now make their transactions online. It therefore means that the internet must be secured for business to be done. The use of firewalls in our systems as a result cannot be over emphasized. Corporate bodies and companies can now prevent hackers and unrestricted access to their database or some vital information by the use of firewalls. Parents can monitor what their children and wards browse or watch on the internet even when they are not there by installing firewall into their system in order to bar them from unwholesome sites. Firewall has played a major role in internet security and its use should be encouraged and the software should be improved upon, in order to assure users of the Internet of security and unauthorized access.

REFERENCES

Chris, P. (2009). Introduction to firewalls, Retrieved 24th July 2009 From *http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci950168,00.html.*

Gralla, P. (2007). *How the Internet Works.* Indianapolis: Que Publication ISBN 0789721325.

Rhee, M. Y. (2003). Internet Security: Cryptographic Principles, Algorithms and Protocols. Chichester: Wiley. ISBN 0470852852.

Kurose, J. F. and **Ross, K. W.** (2007). Computer Networking: A Top-Down Approach ISBN 0-321-49770-8

Tyson, J. 24 October (2000). How Firewalls Work. Retrieved 22nd July 2009, from *www.howstuffworks.com*