International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

APPLICATION OF FIREWALL SYSTEM TO INTERNET SECURIT

OKUMOKU-EVRORO, ONIOVOSA
M.Sc Candidate
Department of information technology
National open university of Nigeria, Benin City study centre
Email: victorkleo@live.com

Abstract

Almost Every business today use an internet enabled facility for better communication, from individuals to corporate organization, this has raised a lot of concern on the security of every network or a single computer connected to the internet. 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 how firewall can be applied to internet security with a look at the various techniques and types of firewall and how it can help to secure the internet. The configuration procedure for firewall and how they could be turned ON or OFF were also discussed. It was observed that the application of firewall has played a significant role in curbing security threats that have increased on the internet and the need to proffer solutions to the situation and make the internet a safer place. However through this study, I advocate that internet security be improved upon in order to assure the users of the Internet of security and unauthorized access denied or set to self destroy any potential or anticipated threat.

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

INTRODUCTION

Interest and knowledge about computer and network security is growing along with the need for it. This interest is, no doubt, due to the continued expansion of the Internet and the increase in the number of businesses that are migrating sales and information channels to the Internet. The growth in the use of networked computers in business, especially for e-mail, has also fuelled this interest. Many people are also presented with the post-mortems of security breaches in high-profile companies in the nightly news and are given the impression that some bastion of defence had failed to prevent some intrusion. One result of these influences is that many people feel that Internet security and Internet firewalls are synonymous. Although we should know that no single mechanism or method will provide for the entire computer and network security needs of an enterprise, many still put all their network security eggs in one firewall basket.

Computer networks may be vulnerable to many threats along many avenues of attack, including:

- Social engineering, wherein someone tries to gain access through social means (pretending to be a legitimate system user or administrator, tricking people into revealing secrets, etc.)
- War dialling, wherein someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network
- Denial-of-service attacks, including all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it
- Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services
- Host attacks, which attack vulnerabilities in particular computer operating systems or in how the system is set up and administered
- Password guessing
- Eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection.

Internet firewalls have been around for a hundred years-in Internet time. Firewalls can help protect against some of these attacks, but certainly not all. Firewalls can be very effective at what they do. The

ISSN 2304-0777 www.jitbm.com

people who set up and use them must have the knowledge of how they work, and also be aware of what they can and cannot protect. In this article, we examine the Internet firewall, touch on its history, see how firewalls are used today, and discuss changes that are in place for the next hundred years.

Firewall History

We are used to firewalls in other disciplines, and, in fact, the term did not originate with the Internet. We have firewalls in housing, separating, for example, a garage from a house, or one apartment from another. Firewalls are barriers to fire, meant to slow down its spread until the fire department can put it out. The same is true for firewalls in automobiles, segregating the passenger and engine compartments. Cheswick and Bellovin,(1994) in the definitive text on Internet firewalls said an Internet firewall has the following properties: it is a single point between two or more networks where all traffic must pass (choke point); traffic can be controlled by and may be authenticated through the device, and all traffic is logged. In a talk, Bellovin later stated, "Firewalls are barriers between 'us' and 'them' for arbitrary values of 'them.'" The first network firewalls appeared in the late 1980s and were routers used to separate a network into smaller LANs as stated by Avolio, F. & Ranum, M (1996). In these scenarios and using Cheswick, W. & Bellovin, S. (1994) definition, above "us" might be well, "us." And "them" might be the English Department. Firewalls like this were put in place to limit problems from one LAN spilling over and affecting the whole network. All this was done so that the English Department could add any applications to its own network, and manage its network in any way that the department wanted. The department was put behind a router so that problems due to errors in network management, or noisy applications, did not spill over to trouble the whole campus network. The first security firewalls were used in the early 1990s. They were IP routers with filtering rules. Avolio, F. & Ranum, M (1996) opined that the first security policy was something like the following: allow anyone "in here" to access "out there." Also, keep anyone (or anything I don't like) "out there" from getting "in here." These firewalls were effective, but limited. It was often very difficult to get the filtering rules right, for example. In some cases, it was difficult to identify all the parts of an application that needed to be restricted. In other cases, people would move around and the rules would have to be changed.

The next security firewalls were more elaborate and more tuneable. There were firewalls built on so called bastion hosts. Probably the first commercial firewall of this type, using filters and application gateways (proxies), was from Digital Equipment Corporation, and was based on the DEC corporate firewall. Brian Reid and the engineering team at DEC's Network Systems Lab in Palo Alto originally invented the DEC firewall. The first commercial firewall was configured for and delivered to the first customer, a large East Coast-based chemical company, on June 13, 1991 Avolio, F. and Ranum, M. (1996). During the next few months, Marcus Ranum at Digital invented security proxies and rewrote much of the rest of the firewall code. The firewall product was produced and dubbed DEC SEAL (for Secure External Access Link). The DEC SEAL was made up of an external system, called Gatekeeper, the only system the Internet could talk to, a filtering gateway, called Gate, and an internal Mailhub (see Figure 1).

In this same time frame, Cheswick and Bellovin at Bell Labs were experimenting with circuit relay-based firewalls. Raptor Eagle came out about six months after DEC SEAL was first delivered, followed by the ANS InterLock.

International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

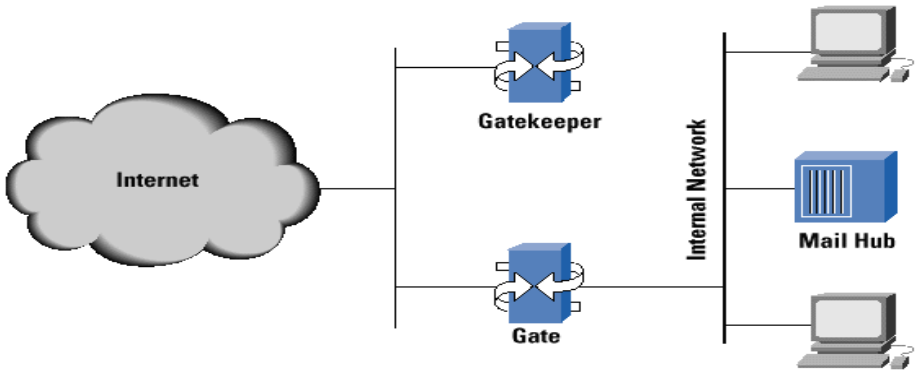

Figure 1: DEC SEAL-First Commercial Firewall (http://www.avolio.com/papers/isoc.html)

A firewall is a hardware or software system that prevents unauthorized access to or from a network. It controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should allowed through or not, based on a rule set. 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. 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.

Generally, firewalls are configured to protect against 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.

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.

International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

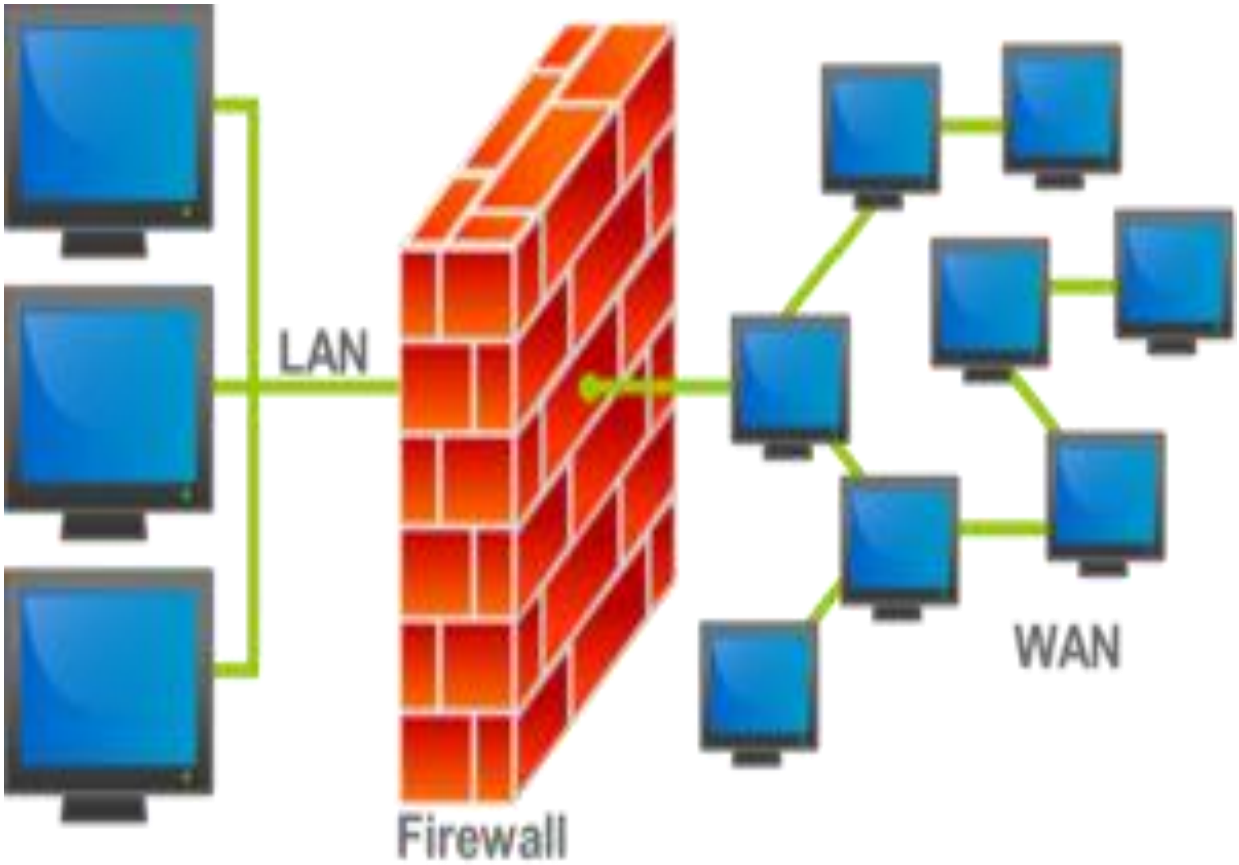

Figure 2: An illustration of how a firewall works.
(http://www.ijcsi.org/papers/IJCSI-Vol-9-Issue-1-No-3.pdf)

In the illustration above the red block represent the firewall, while the network at your left hand side (LAN) represent your home or office network and the one on your right side (WAN) represent all internet users.

Types of firewall techniques

1. 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.
2. Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.
3. 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.

International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

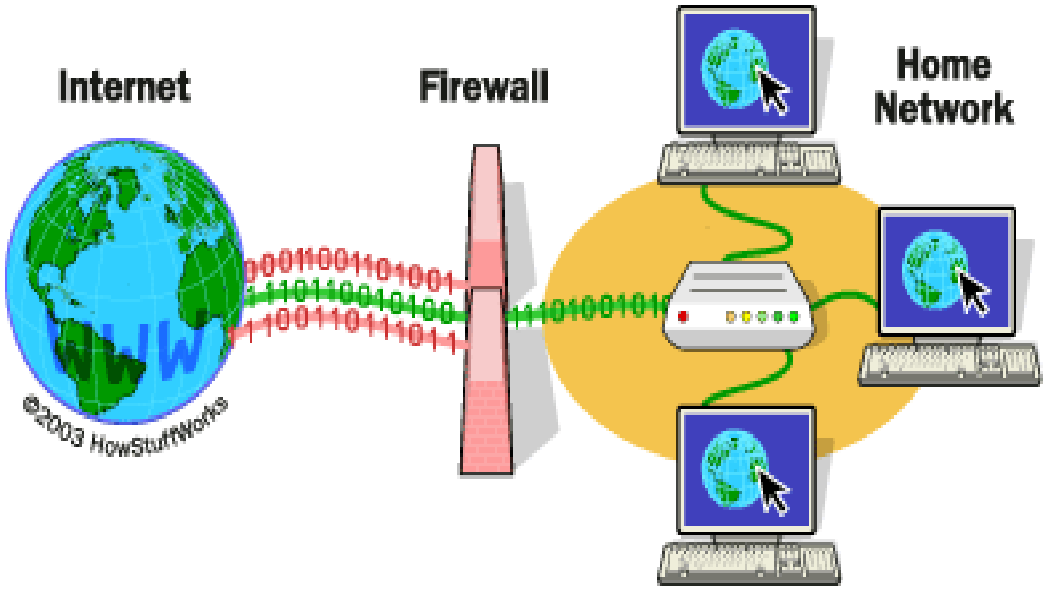

Figure 3: Firewall Protecting a Home Network
(http://www.ijcsi.org/papers/IJCSI-Vol-9-Issue-1-No-3.pdf)

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 quite 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 Partsenidis breaks them down 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. According to Chris Partsenidis (2009), application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection.

In some cases, having an application in the way may impact performance and may make the

International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

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 network 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 kind of a fast packet-screening system that logs and checks data as it passes through.

How Firewall ensures internet security

A firewall intercepts and controls traffic between networks with differing levels of trust. It is part of the network perimeter defence of an organization and should enforce a network security policy. By Cheswick's and Bellovin's definition, it provides an audit trail. A firewall is a good place to support strong user authentication as well as private or confidential communications between firewalls. As pointed out by Chapman and Zwicky, firewalls are an excellent place to focus security decisions and to enforce a network security policy. They are able to efficiently log internetwork activity, and limit the exposure of an organization.

The exposure to attack is called the "zone of risk." If an organization is connected to the Internet without a firewall (Figure IV), every host on the private network can directly access any resource on the Internet. Or to put it as a security officer might, every host on the Internet can attack every host on the private network. Reducing the zone of risk is better. An internetwork firewall allows us to limit the zone of risk. As we see in Figure v, the zone of risk becomes the firewall system itself. Now every host on the Internet can attack the firewall. With this situation, we take Mark Twain's advice to "Put all your eggs in one basket and watch that basket."

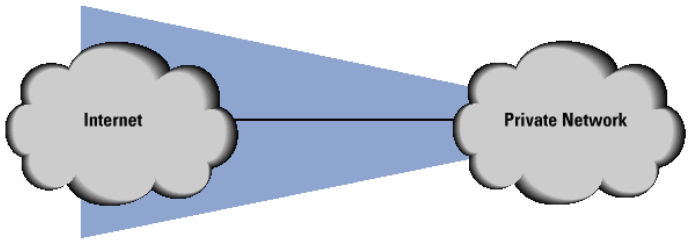

Figure 4: Zone of Risk for an Unprotected Private Network (http://www.avolio.com/papers/isoc.html)

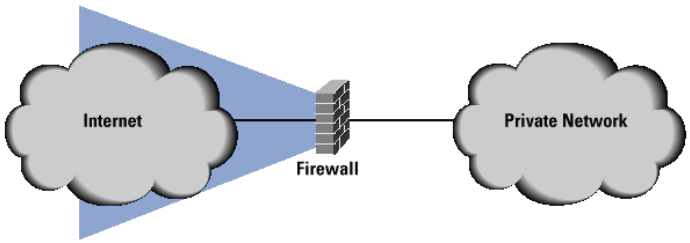

Figure 5: Zone of Risk with a Firewall (http://www.avolio.com/papers/isoc.html)

International Journal of Information Technology and Business Management
29th December 2015. Vol.15 No.1

ISSN 2304-0777 www.jitbm.com

Firewall Configuration

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

- IP addresses - Each machine on the Internet is assigned a unique address called an IP address. IP addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical IP address looks like this: 216.27.61.137. For example, if a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address, Okumoku E.O (2011).
- Domain names - Because it is hard to remember the string of numbers that make up an IP address, and because IP 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 you can set firewall filters 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. 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, Okumoku E.O (2011).
- Specific words and phrases - This can be anything. 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 a firewall built in. Otherwise, a software firewall can be installed on the computer in your home that 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 a built-in Ethernet

ISSN 2304-0777 www.jitbm.com

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 ON/OFF Windows Firewall
To enable Windows Firewall, follow these steps:

1. Click Start; click Run, type Firewall.cpl, and then click OK.
2. On the General tab, click On (recommended).
3. Click OK.

To disable Windows Firewall, follow these steps:

1. Click Start; click Run, type Firewall.cpl, and then click OK.
2. On the General tab, click Off (not recommended).
3. Click OK.

Note:

These steps are only for Windows XP SP2, Windows XP SP3 windows Vista and window 7. These steps are not for earlier versions of Windows XP.
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 and this includes the Internet.

Summary

This study has been able to show how firewall system can be applied to internet security. And not just how, but the various steps to take to achieve this. The study also has been able to outline how firewall can be configured and enabled in a computer system. The study was able to make internet users realize that turning off their firewall while on the internet is not safe at all.

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 upon. Corporate bodies and companies can now prevent hackers and unrestricted access to their database or some vital information by the use 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 in internet security and its use should be encouraged and the software should be improved upon, such that a time will come when people can rest assured that the internet is now safe from potential treat as a result of unauthorised access.

Reference

1. Umukoro, A. U. (2005). Introduction to: Network, Internet & World wide Web. *Gift prints associates Benin City.*
2. Avolio, F. and Ranum, M.(1996) "A Network Perimeter with Secure External Access," *Proceedings of the ISOC NDSS Symposium*, (http://www.avolio.com/papers/isoc.html)
3. Chapman, D. B. & Zwicky, E.(*1995.*). Building Internet Firewalls, *ISBN 1-56592-124-0, O'Reilly and Associates,*
4. Cheswick, W. & Bellovin, S. (1994). Firewalls and Internet Security: Repelling the Wily Hacker, *ISBN 0201633574, Addison-Wesley*.
5. Chris P (2009). Introduction to firewalls
   a. *http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci950168,00.html. Retrieved 24th July*, 2009
6. Tyson, Jeff.(2000) "How Firewalls Work." *www.howstuffworks.com. Retrieved 22nd July 2009.*
7. Okumoku E.O (2011). Internet security: the role of firewall system. *Readings in Education, Development and Globalization 65-70*