International Journal of Basic, Applied and Innovative Research

IJBAIR, 2017, 6(1): 10 - 17

ISSN: 2315 - 5388

www.arpjournals.com; www.antrescentpub.com

E-ISSN: 2384 - 681X

RESEARCH PAPER

THE RELEVANCE OF FIREWALL TECHNOLOGY IN COMBATING INTERNET INSECURITY

***[1]Ume, L.E. and [2]Ibebuogu, C.C.**

Department of computer science, Ebonyi State University, Abakaliki; Department of computer science Imo State University, Owerri

Correspondence: kristychynwe@yahoo.com; leo.manuels@gmail.com

Published: 31st March, 2017

***Endorsed By**: Innovative Science Research Foundation (**ISREF**) and International Society of Science Researchers (**ISSCIR**).*

***Indexed By**: African Journal Online (AJOL); Texila American University; Genamics; Scholarsteer; EIJASR; CAS-American Chemical Society; and IRMS Informatics India (J-Gate)*

ABSTRACT

The prevalence of internet insecurity and fraud all over the world is seriously contending with the gains of internet and information technology. They had being serious attempts and researches to combat this hydra-headed problem of internet insecurity and one of which is the discovery of firewall. A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a trusted and secure internal network and another outside network. This paper extensively analyzed the firewall security technology and made a discovery that this technology is still very much relevant in combating system network insecurity.

Keyword: Firewall, insecurity, internet, network

INTRODUCTION

In an era when the volume of transaction in networked computers (internet) is increasing by the day, it is not out of place that the type of data coming in and out of computers should be properly scrutinized to ensure the safety of such data. Firewalls are computer security systems that protect your office personal computer, home personal computer and networked computers from intruders, hackers and malicious codes (Funel, 2005). It protects your system from offensive software that may come to reside on your computer from prying hackers and intruders. It will amount to a serious risk when using your computer system especially when connected to the information super high way (internet) without any protective measure like firewall. An effective firewall isolates your computer from the internet using a code that set up a blockade to inspect each packet of data, from or to your computer system to determine whether it could be allowed to pass or blocked.

A firewall is generally seen as a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules (Palo, 2013). A firewall typically establishes a barrier between a trusted, secure internal network and another outside network such the internet that is assumed not to be secured or trusted. When connected to the internet, even a standalone personal computer or a network of interconnected computers make it easy to detect malicious software and unscrupulous hackers. Firewalls are setup at every connection to the internet, therefore subjecting all data flow to careful monitoring. It can also be tuned to follow rules. These rules are simply security rules that can be set up by the network administrator to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owner or administrator immense control over the traffic that flows in and out of their system networks (Zwicky, *et al*, 2000).

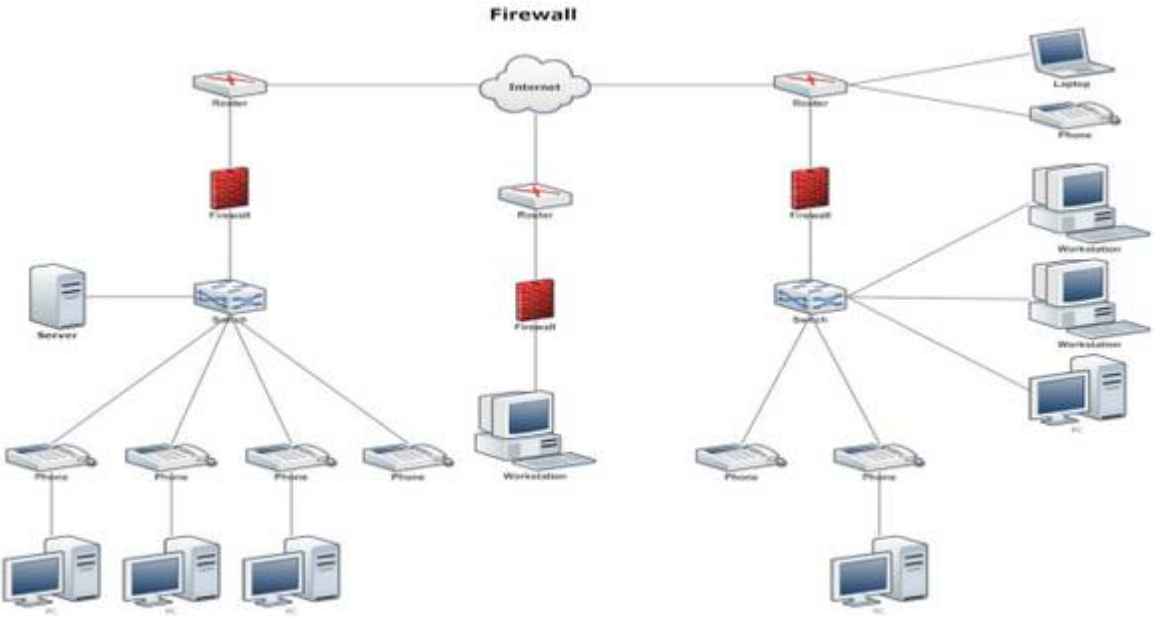

Fig.1: Firewalls in network system

The figure above showed the presence of firewall in all the segments of the network at the point of connection outside the internal network. The middle segment of the network above indicates that a standalone computer that is connected to the internet needed to have firewall. The firewall ensures that network traffic is monitored in and out to prevent any security compromise.

Security is one of the most significant issues facing the owners and users of computer systems in the Internet age, and recent years have convincingly illustrated that the problem is increasing in both scale and cost (Duhigg, 2003). Serious financial damage has been caused by computer security breaches, but reliably estimating costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm, but such estimates may be exaggerated. However, other losses, such as those caused by the compromise of credit card information, can be more easily determined, and they have been substantial, as measured by millions of individual victims of identity theft each year in each of several nations, and the severe hardship imposed on each victim. Individuals who have been infected with spyware or malware likely go through a costly and time-consuming process of having their computer cleaned. Spyware and malware is considered to be a problem specific to the various Microsoft Windows operating systems; however this can be explained somewhat by the fact that Microsoft controls a major share of the PC market and thus represent the most prominent target (Peltier *et el*, 2007).

There are a lot of research and discovery made towards fighting the menace of computer insecurity such as users account access control which provide special keys hidden from other system users. The Intrusion Detection Systems (IDS's) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems. Rocky, Chang (2002) in his research on firewall security opined that firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.

Types of firewall

There are three basic categories of firewalls: packet filtering firewalls, stateful inspection firewalls and application proxy firewalls. Often, people refer to packet filtering firewalls and stateful inspection firewalls using the term gateway server

firewall. Each of these three approaches builds upon the previous one(s), offering greater protection to an enterprise network. Here's how they work:

1. Packet filtering firewalls are the most basic firewall technology available. Each network packet reaching the firewall is evaluated based upon its source, destination IP address and port to determine whether it is allowed to pass through the firewall. The firewall does not have any information about active connections, so it makes this decision each time it receives a packet. Packet filter firewalls are not common and users of this technology are typically writing rules that run on their routers.

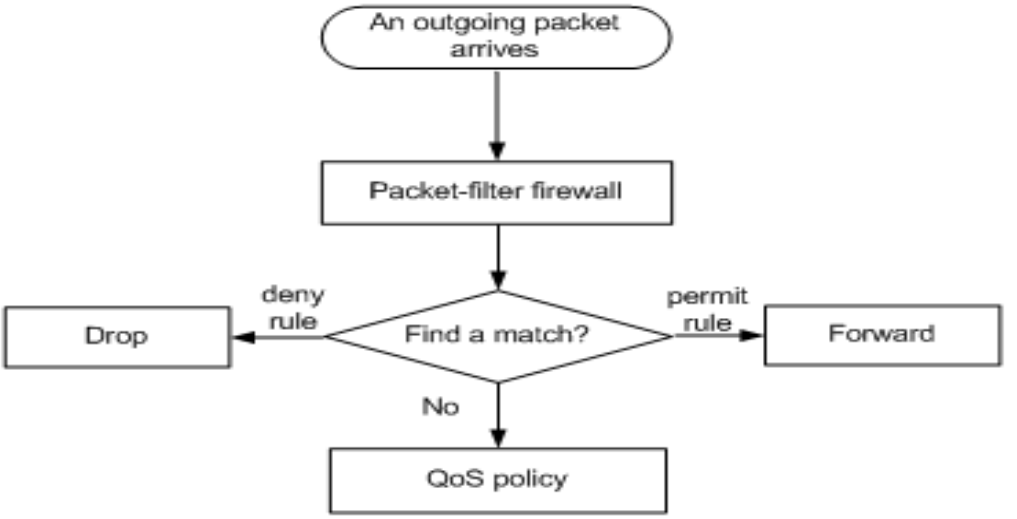

Fig 2: Packet filtering firewall flow diagram

2. Stateful inspection firewalls are the most commonly deployed firewalls in enterprises today. They build upon packet filters by having the firewall maintain information about the state of each active connection. When a new packet arrives at the firewall, the filtering mechanism first checks to determine whether the packet is part of a currently active (and previously authorized) connection. Only if it doesn't appear on the list of active connections does the firewall evaluate the packet against its rulebase. There's a reason stateful inspection firewalls are so common: They're the most efficient and cost-effective firewalls, and are generally suitable for protecting most network borders.

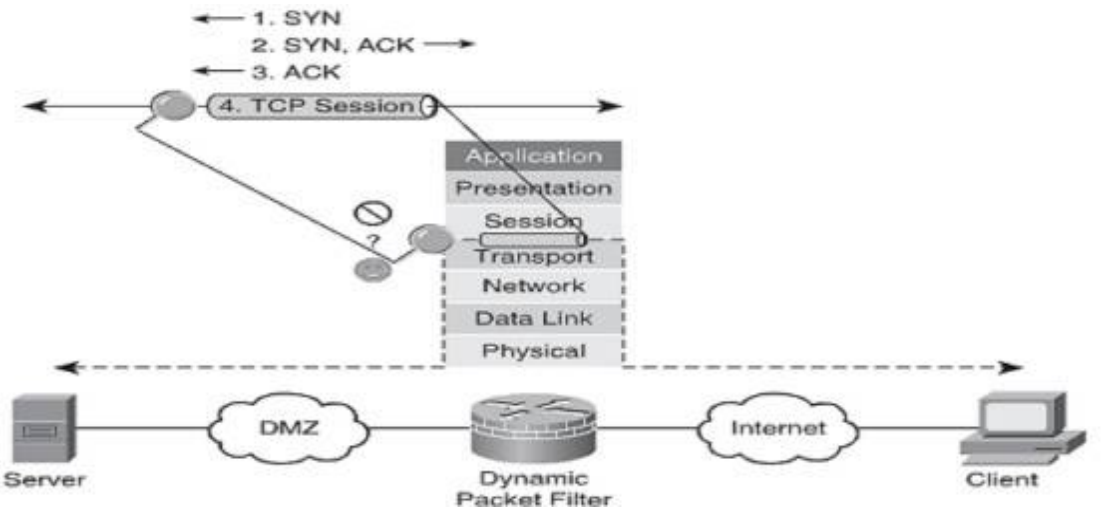

Fig 3: Stateful inspection firewall Application proxy firewalls go a step beyond stateful inspection firewalls in that they don't actually allow any packets to directly pass between protected systems. Instead, the firewall creates a proxy connection on the destination network and then passes traffic through that proxied connection. Proxy firewalls often contain advanced application inspection capabilities, allowing them to detect sophisticated application-layer attacks, such as buffer overflow attempts and SQL injection attacks. They're much more expensive than stateful inspection firewalls, however, and are normally only used to protect data centers and other networks containing publicly accessible, high-value servers.

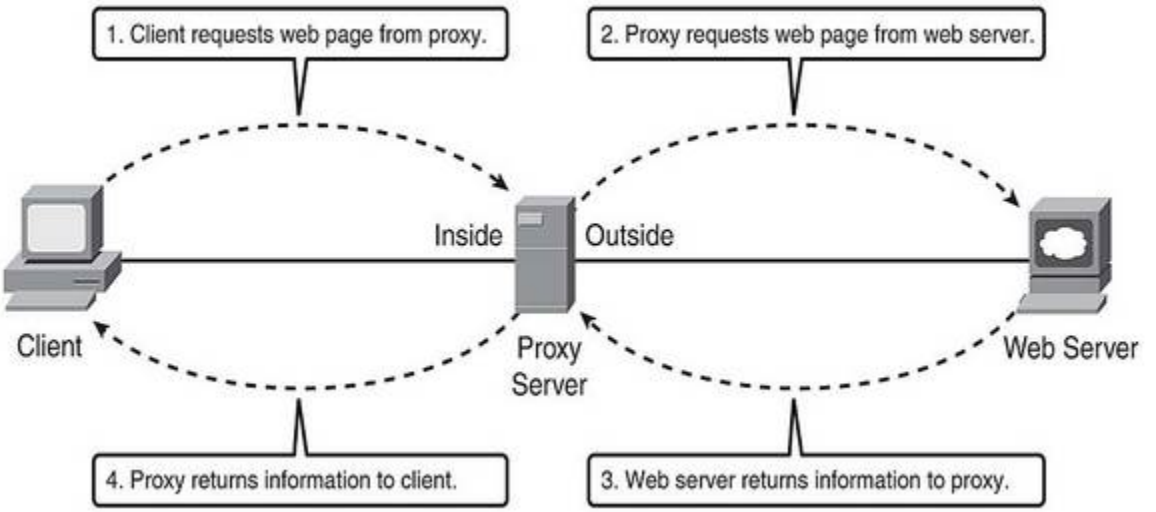

Fig 4: Application proxy firewall

Firewalls configuration policies

The major configuration policies of firewalls were derived as a result of the activities of packet filters embedded in firewalls. Essentially a packet filter has a dirty port, a set of rules and a clean port. The dirty port is exposed to the internet and is where all traffic enters. The traffic that enters the dirty port is processed according to a set of rules or policies configured for the firewall. Based on the determined action derived from the rule set, the firewall will either let the packet enter through the clean port into the trusted network or deny it from entering.

Creating Rule set for packet filtering

A typical firewall packet filtering rule set constitute of the following parameters- type of protocol, source address, destination address, source port, destination port and the action the firewall should take when the rule set is matched. The table 1 below presents the set of rules that will act as the policy guideline that the firewall will utilize to determine whether a packet is allowed to enter into the trusted network.

Rule 1: This rule permits inbound access from a single IP subnet on the internet to a single host in the network for secure shell (SSH).

Rule2: This rule allows inbound access on port 80, which is typically used for HTTP traffic. The host is 129.1.5.154 is the web server for the domain. Such arrangement cannot predict who will want to access the website, so there is no restriction on the source IP address.

Rule 3: The rule allows inbound SMTP traffic. Within a Domain Name System (DNS) the company will have one or more records that indicate its SMTP mail servers. These records are called MX records. In the example network perimeter, the

organization's DNS MX record resolves to the IP address 129.1.5.150. Any host on the internet that wishes to send e-mail to a host in this domain will attempt an SMTP connection to this IP address. This is because any host on the internet can conceivably attempt a connection; the source IP address for the transaction must be any IP address. If a subnet of IP addresses were listed here, some network on the internet would not be able to send mail to users in this domain.

Table 1: Sample of packet filtering rule set

Rule	Protocol Type	Source Address	Destination Address	Source Port	Destination Port	Action
1	TCP	128.5.6.0/24	129.1.5.155	>1023	22	Permit
2	TCP	Any	129.1.5.154	>1023	80	Permit
3	TCP	Any	129.1.5.150	>1023	25	Permit
4	UDP	Any	129.1.5.152	>1023	53	Permit
5	UDP	Any	129.1.5.1.153	>1023	53	Permit
6	Any	Any	Any	Any	Any	Deny

Rules 4 and 5: The two servers IP addresses 129.1.5.152 and 129.1.5.153 are the Domain Name Service servers for this domain. In every case, only UDP is required for proper DNS services. The two cases in which TCP is required are when support is needed for a DNS zone transfer and when the reply is so large that it cannot fit inside a single UDP packet.

Rule 6: This rule explicitly blocks all packets that have not matched any of the criteria in the previous rules.

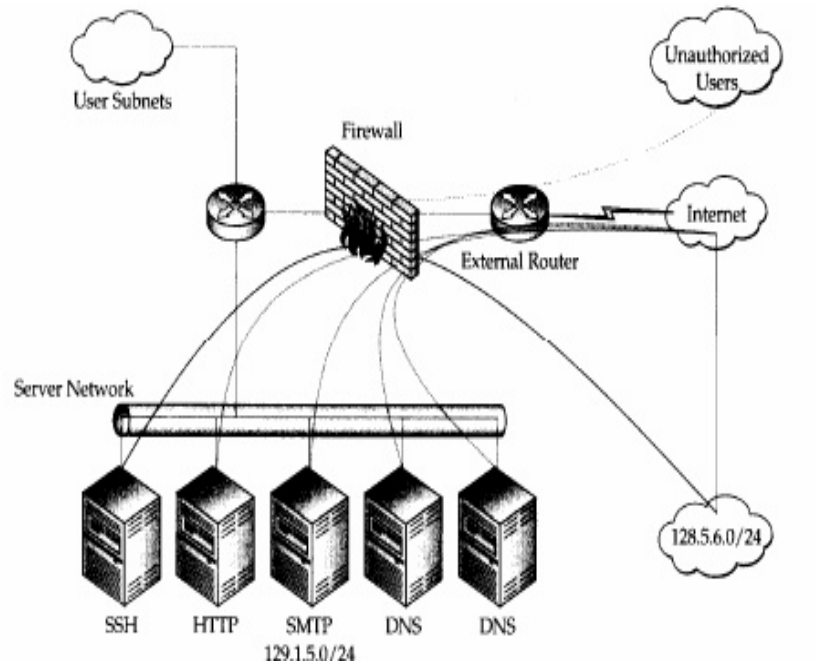

Fig 5: The flow of packet filtering example

The above depicts overall packet filtering for the example given above.

Generations of firewalls

The development of firewalls went through several stages of security metamorphosis which are now in use. This development came about in trying to seal off every security loopholes that may result as a result of the system attacker devising more dangerous strategy. The generations include:

1) **First generation (Packet filters):** This generation of firewall monitors the network through the network addresses and ports of the packets to determine if the packets should be allowed or blocked. A packet is dropped or forwarded depending whether it matches with the packet filter rules set on the host server. If it matches, the packet is allowed and if does not match, the packet is dropped silently. Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between network and physical layers with little bit of peeking into the transport layer to figure out source and destination port numbers.

2) **Second generation (Circuit level gateway):** This monitors the transmission control protocol (tcp) handshaking going on between local and remote host to determine whether the session being established is legitimate. That is to say that this type of firewall want to ensure that the remote computer seeking to establish contact with the host computer for the purpose of exchange of packets is trusted. It does not inspect the packet by itself.

3) **Third generation (Stateful filters):** This deepens the packet inspection by not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This is achieved by retaining packets until enough information is available to decide about its state. This operates on layer four of OSI model (transport layer).

4) **Fourth generation (Application level):** This work on the application level of the TCP/IP stack (that is all browser traffic, all telnet of FTP traffic) and may intercept all packets travelling to or from an application. They block other packets without acknowledgement to the sender. On inspecting all packets for improper content, it can restrict or prevent outright the spread of networked computer worms and Trojan. This generation of firewall is reputed for its ability to perform socket calls or socket filter. This is simply a deliberate and thorough inspection between the application and the lower layers of OSI model. This is done by the use of well established rule set. The set of rules in this generation is more complex compared to the one in first generation because of the varieties of software application in this layer of OSI model.

5.) **Fifth generation (Multi-layer inspection):** combine packet filtering with circuit monitoring, while still enabling direct connections between the local and remote hosts, which are transparent to the network. They accomplish this by relying on algorithms to recognize which service is being requested, rather than by simply providing a proxy for each protected service. They work by retaining the status (state) assigned to a packet by each firewall component through which it passes on the way up the protocol stack. This gives the user maximum control over which packets are allowed to reach their final destination, but again affects network performance, although generally not so dramatically as proxies do.

6.) **The next generation firewall (NGF):** Modern threats like web-based malware attacks, targeted attacks, application-layer attacks, and more have had a significantly negative effect on the threat landscape. In fact, more than 80% of all new malware and intrusion attempts are exploiting weaknesses in applications, as opposed to weaknesses in networking components and services (Funel, 2005). NGF is an integrated network platform that is a part of the third generation of firewall technology, combining a traditionalfirewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection and third-party identity management integration

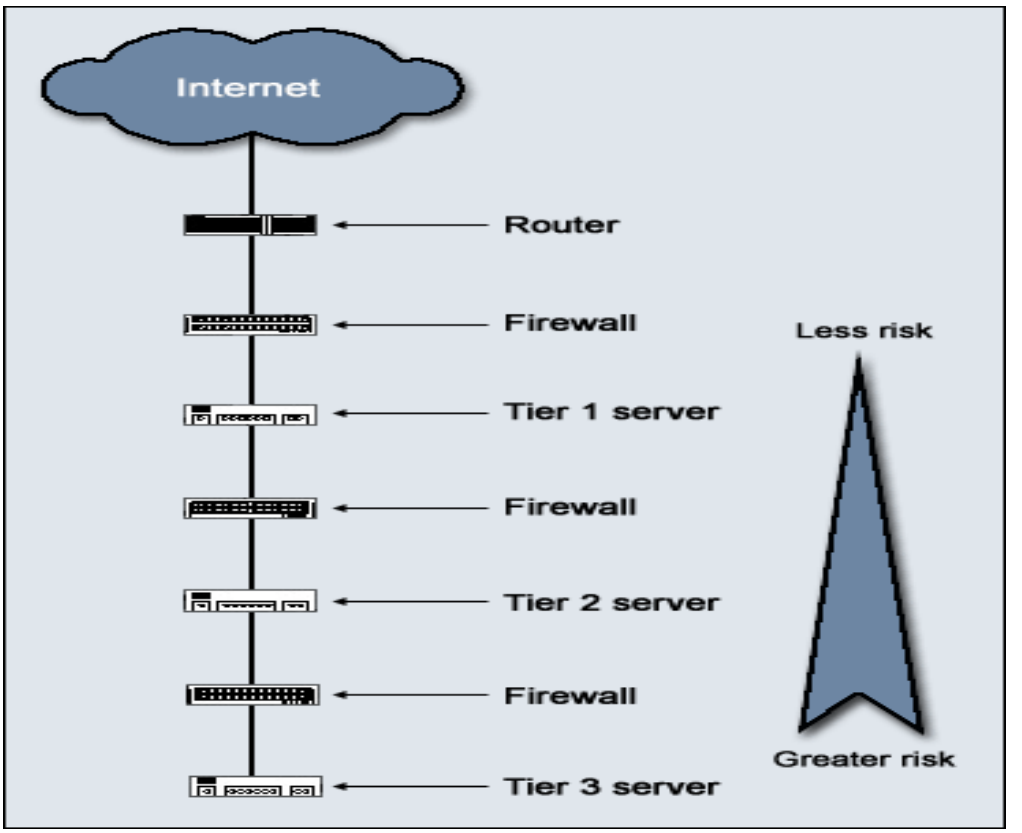

Fig 6: Multi-layer firewall architecture

CONCLUSION

Firewall technology is a must have for any type of computer usage that go online. It has being found to be a good counteracting measure in combating the numerous security menaces that threatens users of internet for different purposes including business. This is because firewalls had over the years evolved to these generations outlined in this paper with each generation adequately poised to handle security threats of that generation. That is to say that as hackers are advancing in their wicked research to bring more harmful security threat to computer users, firewall research has far go beyond them to handle such threat as they come. I therefore recommend installation of firewall to system users be it standalone, home network or an office network.

ACKNOWLEDGEMENT

We wish to acknowledge the efforts of our postgraduate students (Euphemia Osigwe, Edmund Ezennorom, Bisong John Bisong) for their useful contributions in the literature search. Members of our families are not left out especially MrsUcheIbe who gave birth to a baby at the course of this research.

REFERENCE

Boudriga, N. (2010). Security of mobile communications. Boca Raton: CRC press

Chang, R. (2002). Defending against flooding-based distributed denial-of-service attack. A tutorial. IEEE communication magazine 40(10).

Duhigg, Charles (2003). Virus may elude computer defenses: more struggle in the data storehouse. Rodenny press, Washinton post

Elizabeth, D., Zwicky, S.C. and Chapman, B.D. (2000). Building internet firewalls. 2nd Edition. O'Rally publishers

Funnel, S.M. (2005). Computer insecurity: Risking the system. Springer-Verlag, London

Palo, Alto (2013). Next generation firewalls: Restoring effectiveness through application visibility and control.

Peltier, J. and Thomas, R. (2007). Complete guide to CISM certification. CRS Press

Zwicky, R. and Giberson, F. (2000). Parallel computing security. Retrieved from http://www.worktanksolutions.com

AUTHOR'S CONTRIBUTIONS

Ume, L.E and Ibebuogu, C.C contributed immensely in various stages of this research to ensure that it sees the light of the day.

.