American Journal of Multidisciplinary Research in Africa
Vol. 1(3), pp. 1-6, December, 2021
AJMRA-21-007

ISSN: 2769-0504
https://www.mprijournals.com/

Full Length Research

Firewall Technology's Importance in the Fight against Internet Security

Saheed Tunde Zubair[1]
[1]Faculty of Computer Science,
School of Computer Science & Information Technology,
Skyline University, Nigeria, Nigeria,
[1]Email: saheedtzubair@gmail.com

Oluwatosin Islamiyat Yusuf[2] **and Abdulrahman Muhammed Bello**[3]
[2, 3]Faculty of Computer Science,
School of Computer Science & Information Technology,
Kano state university of Technology,
Wudil - Nigeria
[2]Email: oluwatosinyusuf85@gmail.com
[3]Email: dzabdul@gmail.com

Lateefat Saheed, Yusuf[4] **and Samiha Sani Sammani**[5]
[4, 5]Department of Computer Science & Information Technology,
Federal College of Education,
Kano, Kano State - Nigeria
[4]Email: lateefat4sta@gmail.com
[5]Email: sssani2003@gmail.com

Accepted 25th November, 2021

Abstract: The ubiquity of online vulnerability and fraud throughout the world is posing a major threat to the internet's and information technology's benefits. There have been considerable initiatives and investigations to tackle this hydra-headed challenge of internet vulnerability, with one of them being the discovery of firewall. A firewall is a network security device that monitors and restricts internet traffic based on predefined security rules. It creates an obstacle between a trusted and secure internal network and an untrusted and insecure external network. The firewall security technology was thoroughly examined in this study by the use of secondary data, and it was discovered that it is still extremely important in countering system network vulnerability through the use of Prescriptive Analysis. This study concluded that firewall technology is essential for any sort of computer usage that is connected to the internet. It has been discovered to be an effective counter measure in countering the various security threats that affect internet users for a variety of reasons, including business. This is due to the fact that firewalls have evolved through time to the generations indicated in this article, with each generation being properly prepared to tackle the security risks of that generation. That is to say, while hackers advance in their wicked research to deliver more damaging security threats to internet users, firewall research has far surpassed them in order to deal with such threats as they arise. Hence, the study proposed that computer users install a firewall, whether it is independent, a personal network, or an office network.

Keywords: Confidentiality: Firewall: Internet: Network
Cite This Article As: Zubair, T. S., Yusuf, O, I., Bello, M. A., Sani, S. S. & Yusuf, L. (2021). Firewall Technology's Importance in the Fight against Internet Security. American Journal of Multidisciplinary Research in Africa, 1(3): 1-6.

1.0 Introduction of the Study

On a day where the amount of transactions in networked computers (internet) is growing by the day, it is only natural that the type of data entering and exiting computers be thoroughly inspected to assure its security. Firewalls are computer security systems that keep invaders, hackers, and harmful code out of your workplace computer, personal computer, and networked computers (Funel, 2005). It safeguards your computer from malicious software that may be installed by unscrupulous cybercriminals and intruders. When utilizing your computer system, particularly when linked to the online world (internet) without any protection measures in place, such as a firewall, you are taking a significant risk. An efficient firewall protects your computer from the internet by enforcing a blockage that inspects each data packet sent or received by your computer system to decide if it should be permitted to pass or not.

A firewall is a network security device that detects and regulates inbound and outbound traffic according to pre-set security criteria (Palo, 2013). A firewall is used to act as a barrier between a recognized, protected internal network and an external network; such as the internet, that is considered insecure and untrustworthy. Even a single personal computer or a network of interconnected machines may identify harmful software and unethical hackers when connected to the internet. Every connection towards the internet is protected by a firewall, which ensures that all data flows are carefully monitored. It may also be programmed to follow certain rules.

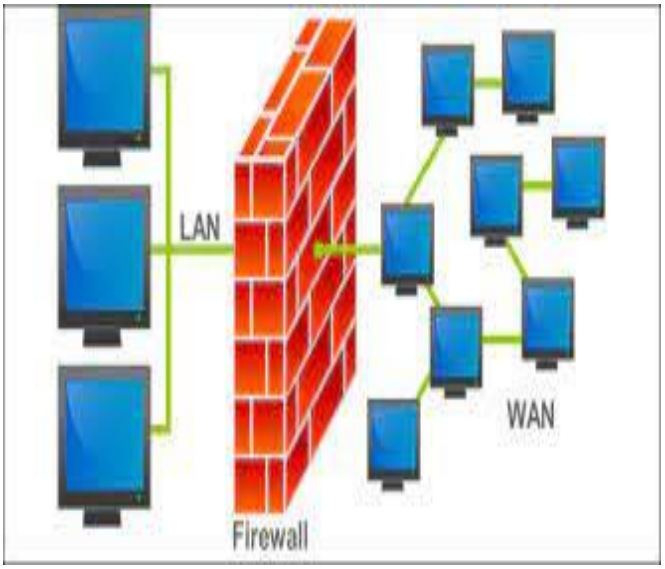

Fig.1: Firewalls in network system

The graphic above depicted the existence of firewalls in all network elements at the intersection to the outside world. According to the middle section of the network above, a solo computer linked to the internet requires a firewall. To avoid any security breaches, the firewall guarantees that traffic flow is regulated in and out. Protection is one of the most pressing concerns for computer system users and owners in the Era of the internet, and previous decades have demonstrated that the challenge is growing in both scope and expense (Duhigg, 2003). Computer privacy violations have resulted in significant financial losses, but accurately quantifying costs is challenging. The harm produced by malware such as system viruses like the Code Red worm has been estimated in the billions of dollars, however such figures may be overstated.

Many losses, as well as those inflicted by the theft of credit card details, are more clearly quantifiable, and they're still significant, as evidenced by the millions of victims of cybercrime each year in a variety of countries, as well as the tremendous suffering placed on each victim. Those who have been infected with spyware or malware are likely to go through a costly and time-consuming computer cleaning process. Spyware and malware are thought to be an issue unique to Microsoft's Windows operating systems. Nevertheless, the reality that Microsoft owns a significant PC share is partially an explanation of this and therefore the most important objective (Peltier *et al*, 2007).

Many studies and discoveries have been done to combat the threat of computer vulnerability, such as user account access control, which provides specific keys that are concealed from other system users. Intrusion Detection Systems (IDS) are intended to identify network assaults in process and aid in post-attack forensics, whilst audit trails and logs serve a similar purpose for individual systems. In his study on firewall security, Rocky Chang (2002) stated that firewalls are by far the most prevalent network security prevention systems because they may (when correctly configured) protect access to internal network services and stop certain types of assaults through packet filtering.

2.0 Types of Firewall

The three main kinds of firewalls are: firewalls filtering packets, firewalls for state-of-the-art inspection and firewalls proxy. Frequently, the phrase gateways server firewall refers to:

i) **Packet filters and stateful inspection firewalls:** Each of these three techniques builds on the preceding approach(s), giving a company network more safety. This is how they function:

The much more basic firewall technique is packet filtering firewalls. To assess if a network packet is permitted to travel through the firewall, it is analyzed based on its source, destination IP address, and port William Stallings (2003). Because the firewall has no knowledge about active connections, it must make this choice every time a packet is received. Packet filter firewalls are uncommon, and most people who use them write rules that operate on their routers.

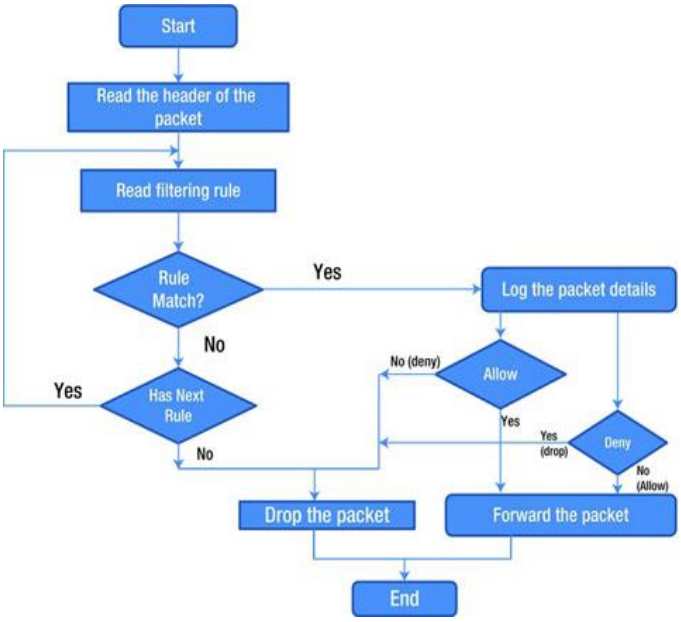

Fig 2: Packet filtering firewall flow diagram

ii) **Filtering firewalls:** The most widely used firewalls in businesses today are packet - filtering firewalls. They extend packet filters by requiring the firewall to keep track of the state of each bonding relationship. When a new packet is received at the firewall, the filtering algorithm checks to see if it is part of a local (and previously approved) connection. The firewall only checks the packet against its rule base if it is not in the list of active connections. Stateful inspection firewalls are often used for a reason: They are the most efficient and cost-effective firewalls, and they are good for most network perimeter protection.

iii) Static firewall inspection: Internet gateway firewalls go one step farther than stateful inspection firewalls, because they do not allow packages to flow directly across appropriate conditions. Instead, a proxy on a target node is created by the firewall and traffic goes through that proxy connection. Proxy firewalls generally feature comprehensive app scan abilities that enable complex application layer cyber attacks such as buffer overflow attempts and SQL injection attacks to be detected Zacker (2001). They are nonetheless a tad more costly than state-

of-the-art inspection firewalls and are usually exclusively used to safeguard data Centers and other public server networks.

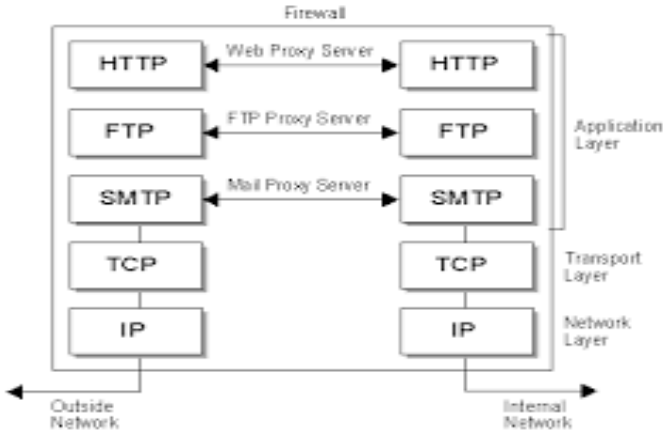

Fig 3: Application proxy firewall

3.0 Configuration Policies for Firewalls

The actions of packet filters integrated in firewalls resulted in the primary setting guidelines of firewalls. A packet filter has three parts: a dirty port, a set of rules, and a clean port. The filthy port is open to the internet and serves as the entry point for all traffic. The traffic that arrives the filthy port is routed via the firewall as shown in a set of rules or policies Bauer (2001). The firewall will either allow the packet to reach the network over the clean port or refuse it based on the decided action resulting from the rule defined. Below are set rules for filtering packets.

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

Rule2: This rule permits inbound traffic on port 80, which is often used for HTTP traffic. The domain's web server is located at 129.1.5.154. Because it is impossible to foresee who would wish to visit the website, there are no restrictions on the originating IP address.

Rule 3: Inbound SMTP traffic is allowed by this rule. The firm will have one or more records in its Domain Name System (DNS) that specify its SMTP mail servers. MX records are the name for these records. The organization's DNS MX record resolves to the IP address 129.1.5.150 in the example network perimeter. Any host on the internet wishing to send email to a host in this domain will attempt to connect to this IP address using the SMTP protocol. This is because any host on the internet may potentially try a connection, and the transaction's originating IP address could be any IP address. Some system on the internet would be unable to deliver mail to users in this domain if a subnet of IP addresses was specified here.

Table 1: Firewall Security Rule Set Illustrations

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Rule 4 and 5: The Domain Name Service servers for this domain are 129.1.5.152 and 129.1.5.153, respectively. Only UDP is necessary in all cases for effective DNS services. TCP is required in two situations: when a DNS zone transfer is necessary, and when the response is too big to fit inside a single UDP packet.

Rule 6: This rule clearly bans all packets that do not fit any of the preceding rules' requirements.

4.0 Generations of Firewalls

Firewalls have gone through various stages of security transformation, all of which are presently in use. This idea arose from a need to plug any security gaps that may arise as a result of a system attacker creating a more hazardous technique. The generations are as follows:

4.1 First generation (Packet filters): This type of firewall examines the network by looking at the packets' network addresses and ports to see if they should be permitted or banned. Depending on whether a packet meets the packet filter rules defined on the host server, it is discarded or forwarded. If it matches, the packet is permitted; if it doesn't, the packet is quietly discarded (Deraison, 2004). Firewall security firewalls mostly operate on the first three levels of the OSI reference model, which implies that the majority of the work is done between the network and physical layers, with a little amount of peering into the network layer to determine source and destination port numbers.

4.2 Second generation (Circuit level gateway): This checks the handovers of the packet switching (TCP) between the local and distant hosts to see if the session being formed is genuine. That is, this sort of firewall wants to make sure that the distant computer attempting to connect to the dedicated server system for the purpose of exchanging packets is trustworthy. It does not examine the packet on its own.

4.3 Third generation (Stateful filters): This improves packet inspection by examining each packet and keeping track of whether or not it is part of an established TCP session. This is accomplished by keeping packets until enough data is available to make a decision regarding their status. This works on the OSI model's fourth layer (transport layer).

4.4 Fourth generation (Application level): This job is completed at the software level of the TCP/IP stack (i.e. all browser traffic, telnet, and FTP traffic) and may intercept all packets sent to or from a program. Without acknowledging the sender, they block additional transmissions. It can limit or prevent the spread of networked computer worms and Trojans by scanning all packets for inappropriate information. This firewall generation is known for its ability to execute socket calls and socket filtering (Firkhan, 2005). This is just a careful and comprehensive examination of the program and the OSI model's lowest levels. This is accomplished by the application of a well-established rule set.

4.5 Fifth generation (Multi-layer inspection): Combine deep packet inspection with circuit surveillance while allowing direct, network transparent communications between the local and distant hosts. You achieve this through the use of algorithms to detect which service is accessed instead of just providing a proxy for each secured service. They work by keeping each firewall component, which allows you to pass the status (state) of a packet by following the stacking protocol. This allows the user to exercise full control over the packets that can reach their final destination but impacts network performance, albeit not as significantly as proxies do in general.

4.6 The next generation firewall (NGF): Modern dangers such as online malware assaults, targets, app-layer attacks and others have had a substantially detrimental impact on the threat environment. In fact, over 80% of all new malware and intrusion efforts leverage apps' flaws, as opposed to communication weaknesses in features and functionality (Funel, 2005). NGF is an integrated network platform, part of a 3rd generation firewall technology, integrating a standard firewall and additional network device filter features like a DPI software firewall, a threat detection system (IPS).

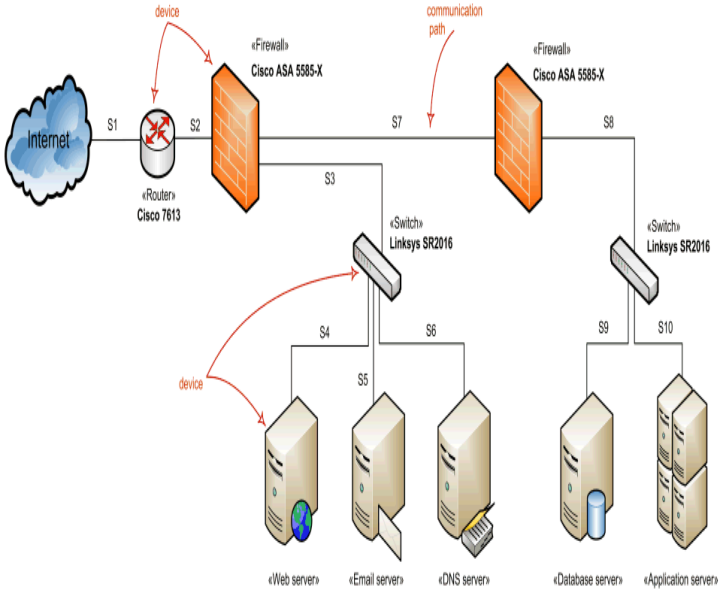

Fig 4 Network security Architecture

5.0 Conclusion of the Study

Firewall technology is essential for any sort of computer usage that is connected to the internet. It has been discovered to be an effective countermeasure in countering the various security threats that affect internet users for a variety of reasons, including business. This is due to the fact that firewalls have evolved through time to the generations indicated in this article, with each generation being properly prepared to tackle the security risks of that generation. That is to say, while hackers advance in their wicked research to deliver more damaging security threats to internet users, firewall research has far surpassed them in order to deal with such threats as they arise. As a result, the study proposed that computer users install a firewall, whether it is independent, a personal network, or an office network.

6.0 Reference of the Study

Boudriga, N. (2010). Security Of Mobile Co-Mmunications. Boca Raton: CRC Press

Chang, R. (2002). Defending Against Flooding-Based Distributed Denial-Of-Service Attack. A Tutorial. IEEE Communication Magazine, 40(10): 37-49.

Duhigg, C. (2003). Virus May Elude Computer Defenses: More Struggle In The Data Storehouse Rodenny Press, Washinton Post.

Elizabeth, D., Zwicky, S. C. & 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, A. (2013). Next Generation Firewalls: Restoring Effectiveness Through Application Visibility And Control.

Peltier, J. & 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

William, S. (2003). Mcryptography And Network Securityn, 3rd Edition, Prentice Hall,2003.

Bauer, M. (2001). Mparanoid Penguin: Seven Top Security Tools llinux Journal, 29(118) (February, 2004).

Deraison, R., Haroon, M., Temmingh, R., Walt, C., Raven A., Alderson, J., Johnston, A. & Theall, G. A. (2004). Mnessus Network Auditing.N Syngress.

Firkhan, H. A. (2005). An Analysis Of Possible Exploits In The Computernetwork_S Security M In ISC: Proceedings Of The International Science Congress 2005. PWTC, Kuala Lumpur, 2005. Pp.338.

Zacker, C. (2001). Networking: The Complete Reference, Osborne/Mcgraw-Hill