Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

Firewall Approach to Computer Network Security: Functional Viewpoint

[1*]OLOYEDE A.O., [1]YEKINI N.A., [2*]AKINWOLE A.K., [2]OJO O
[1]Computer Engineering Department, [2]Computer Technology Department
[1, 2, & 3]Yaba College Of Technology, Lagos Nigeria

ABSTRACT

In today's modern world, most businesses, regardless of size believes that access to the internet is essential to compete effectively in the industry. Yet, connecting a personal or corporate computers to the internet could expose personal or confidential data to malicious attack from anywhere since unprotected connections to the internet makes computer users vulnerable to attacker, hacker, virus, and other internet threats. Therefore, firewall is introduced to provide high degree of protection to the network and network users. This work is concerned with the design and implementation with firewall approach to network security as a means of protecting both individual and corporate network from hostile intrusion coming through internet connectivity. Conclusively, this system proposed is built based on the packet filtering mechanism to control or filter all the packets coming in and leaving the protected site using IP address, and port number of the TCP/IP packet. It was discovered that firewall approach is more robust as it combined capability of other methods like packet filtering, port scanning etc.

Keywords**: Attacker, Firewall, Hacker, Virus, Internet threats, TCP/IP Packet, Packet Filtering, Network users.**

Date of Submission: Oct 23, 2021 Date of Acceptance: Dec 18, 2021

1. INTRODUCTION

A. Background to the Study

Information security has become indispensable because of the distinguishing value that data has gained in the last decades. Unarguably, the way organizations operate have changed significantly with the help of high technology computing systems. At the same time, the world has adapted interconnecting along with the fast development and wide spread of the internet.

Yekini N.A., Oloyede A.O., & Akinwowle A.K. (2020) in a paper entitled Cybernetic Communication Roles in Managing Corona Virus Pandemic Risk: Nigeria Case opined that Computer and Internet-Based Communication Technologies aka Cybernetic Communication play important role in communication over a distance.

Along with this enormous spread of networks, came the issue of security. Many people are only concern on protection of data on network with focus on how to provide confidentiality, authenticity, integrity, and non-repudiation of the information transmitted through the online communication network.

Yekini N. A., Aigbokhan E. E., & Okikiola F. M. (2014) opined that security of information/data from sender to receivers in an online communication could be utilize better using cryptography system. Apart from securing a personal computer, as a stand-alone machine, a new security concept should be invented and developed to conceal a whole network (Deah et al., 2017). Communications via terminals of network have become increasingly easy making interactions among networks quite vulnerable since one could have access to networks from a computer and a dial up modem wired with a telephone cable. Network security has become even more open with the existence of the internet where users have secured access not only to varieties of information but to opportunities for mean use of computer inter connectivity(Abhisek, 2017). The network, as an effective tool is based on the foundations of the seven-layered reference model of open system interconnected model (ISO/OSI). In relation to this model, many attacks as well as threats have been developed and constantly updated to cause operational problems on a network or penetrate to gain administrative right or nab data. By taking into consideration these potential attacks as well as the organization's services and requirements. A firewall is a network security device, that could be in computer hardware or software forms, and helps in protecting network by filtering traffic and banning an unauthorized access to the private data in your computers. There are different methods of securing networked system which includes packet filtering, port scanning, firewall etc, firewall approach is more robust compared to other methods because it combined capability of other methods because apart from blocking traffic, a network firewall stops any malicious software like virus, trojans from infecting the computers as well. Firewalls widely provide certain degrees of network protection based on personal or business needs. The firewall is the most common defense mechanism used in network security (Mihalos et al., 2019). The firewalls force restrictions on packets coming in or exiting the private network. All traffic from the inside out, and vice versa, must go through the firewall, but only authorized traffic will be allowed to pass. Packets are not allowed through unless they conform to a filtering specification, or unless there is negotiation involving some sort of authentication. The firewall itself must be immune to penetration. Firewalls create checkpoints (or choke points) between an internal private network and an untrusted Internet. Once the choke points have been

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

clearly established, the device can monitor, filter, and verify all inbound and outbound traffic. The firewall may filter based on IP source and destination addresses and TCP port number. Firewalls may obstruct packets from the Internet perspective that claim a source address of a system on the intranet, or they may need the use of an access negotiation and encapsulation protocol like SOCKS to gain access to the internet. Firewalls is required to provide high level of defence against illegitimate activities (Rehman et al., 2016). Network security is any designed program with the primary aim of protecting the integrity and usability of your data and network. This includes both software and hardware technologies. It is a designed program to stop a variety of threats and prevent them from spreading or entering your network**.**

There are different types of firewalls, although they differ in their approach but can be characterized as firewalls, which block traffic, and firewall which permit traffic. Then each one of them differ than the other in ways they behave but they all share the same point that they do as a shield to protect the private network users.

A host-based firewallis thetype of firewall thatis used on a personal computer to shield malicious activity from occurring on the network. The policy could have impact on what traffic the pc takes from the web, from the native network, or maybe from itself

A network-based firewall is the type that is implemented at a specified point in the network path and protects all computers users on the “internal” side of the firewall from all computers on the “external” side of the firewall through a set of rules.

Network-based firewalls may be installed at the around any perimeter of a network to guide/protect a corporation from hosts on the Internet, or internally to protect one fragment of the community from another, such as separating corporate and residential systems, or research systems from marketing systems (Solomon, 2021). A network-based firewall cannot defend one computer from the other on the same network orprotect any computer from itself.

B. Firewall Limitations

Although firewalls can strengthen a local network security policy, they also introduce some flaws. The first issue that rises when installing a firewall, is that a significant amount of time must be invested to properly configure the security policy of the local network. Another critical issue that firewalls must solve is the increase in protocol complicated type of traffic. Although the point of a firewall can thoroughly examine all incoming and outgoing traffic it is a fact that firewall’s operation could turn to be slow on a large amount of traffic. Furthermore, another problem that arises is the wireless infrastructure of a local network. In this case, there are vulnerabilities which come up since the points of connection cannot be as enforced as the wired network. Some other vulnerabilities of firewalls include encryption issues. Encrypted packets include non-transparent headers, but firewalls show difficulties in recognizing and trafficking packets (Heukelom, 2018). Last, but not least, firewalls don’t seem to fully collaborate with protocols that include sophisticated handshake mechanisms. FTP for example works by initiating connections from client to server and vice versa. Firewalls are familiar with handling these protocols, but some operations remain vulnerable and unsafe.

C. Classification of Firewalls

Firewalls can be classified regarding the ISO/OSI network layer model into two main categories: network layer and application layer operating firewalls (Kyriakos, 2021). A more detailed description of network and application layer firewalls follows. Network layer firewalls in network layer firewalls traffic is routed directly through the network layer. Packet filters have a simple philosophy of operation that lies on the IP packet characteristics (Michail et al., 2021). If the packet complies with the rules defined by the local security policy, its trespassing is being allowed. In any other case the packet is being discarded and its entrance on the local network is being blocked. IP packet headers inspection includes the examination of the following characteristics: Source IP Address, Destination IP Address, Protocol inspection, TCP and UDP port enforcement and finally, TCP flag examination.

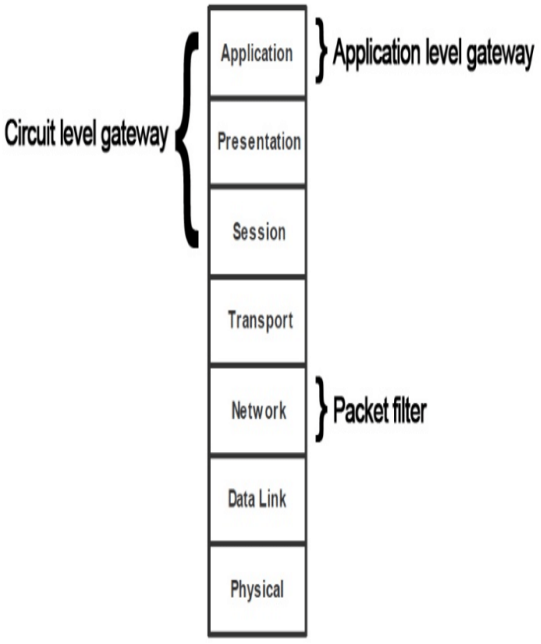

Figure 1. Classification of firewall on the OSI /ISO network layer

Packet filters can be also divided into two categories of filtering, stateless and stateful. In stateless packet filtering the firewall decides whether to allow or discard a packet by examining all the packet characteristics. Stateful packet filtering on the other hand is an enhanced version of the stateless filtering mechanism. The main difference is that it maintains specific characteristics of the TCP/IP protocol as sessions, thus, storing packet’s active connections while any other packet which doesn’t belong to any of these connections is being blocked. Stateful packet filtering also comes with dynamic packet filtering, a service where the

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

firewall can ping the source IP of the packet that is under examination and examine its integrity.

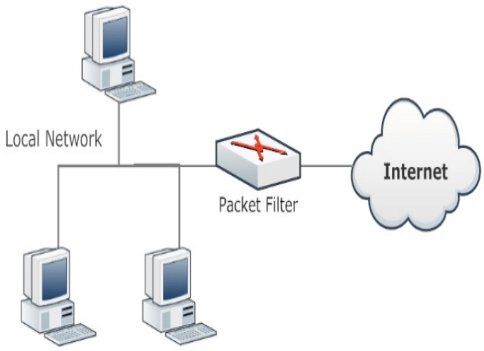

Figure 2. Packet filter firewall topology

D. Statement of Problem

Analyzing the traditional firewall comes with varieties of loopholes which this report work will highlight. All the four different types of firewalls namely Packet filters, circuit level gateways, application-level gateways and stateful multilayer inspection firewalls are all having their own setbacks. Few of them are also specified below:

a) Packet filtering firewall which only works on network level of OSI model, does not support sophisticated rule-based models.
b) Circuit level firewall gateways works at session layer of OSI model, though they stash the information about protected networks, but they do not strain distinct packets.
c) Application-level firewall gateways famously known as proxies are very much analogous to the circuit level gateways except that they are application specific. They also pitch a very high level of security but have a momentous impingement on network performance.
d) Dynamic Packet Filter Firewall or Stateful multilayer inspection firewalls are the amalgamation of above three firewalls, but they are supremely costly and due to their complexity are potentially less secured than simpler firewalls.

E. Objective

The main objective of firewall as a hardware device or software system or group of systems (router, proxy, or gateway) is to permit or deny network transmission based upon set of security rules and regulations to enforce control of hardware device or a software between two networks to protect “inside” network from “outside” network. A firewall could also be a program which might be running on a secured host computer. Firewall must have two network interfaces, one for the network it is intendedto protect, and one for the network it is exposed to. A firewall protects a local system or network systems from all the network-based security threats while at the same time it same provides access to the outside network through WAN and internet (Avolio, 2016).All traffic from inside out, and vice versa through the main entry, must pass through the firewall. This is achieved by physically blocking all access to the site except via the firewall. Various configurations are possible. Only authorized traffic, as defined by the local policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies. In general, firewall is one of the famous types of intruder detection. Firewall effective against worms because it is much difficult for a worm to authenticate itself to a firewall operating a tight exclusive policy than to a general, widely used system.

2. LITERATURE REVIEW

In late 1980s came the first network firewalls designed by Cisco Systems and digital equipment corporation & those were the routers used to divide network into smaller LANs (Michail et al., 2021). Such type of firewalls was put in place to impede obstacles from one LAN to unveil & affect the entire network. In 1990s, first security firewall was used. These were IP routers with filtering rules/refining rules. This security policy allowed “anyone in” Organization to access data “outside” the organization. Also, it does not allow anyone who is “outside of the organization” (who is not trusted) to get access to “inside” data of an organization. The Advantage of this firewall was that they were effective from the security point of view, but they were limited (Sylvester, 2018). The major drawbacks of this firewall were firstly, it was difficult to get filtering rules right. Secondly, it was difficult to identify all the parts of an application thatshould be restricted in some cases. Next security firewall was built on the concept of Bastion Host(which is a special purpose computer on a network specifically designed and configured to withstand attacks). These were more refined and more efficient and were likely the first commercial firewalls of this type. They used filters and application gateways (proxies) from Digital Equipment Corporation and were based on DEC corporate firewall.
Later Marcus Ranum at DEC invented security proxies and that product was called DEC SEAL(Secure External Access Link). The DEC SEAL System was made up of an external system, called Gatekeepera filtering gateway called gate &an internal system Mail. Gatekeeper is the only system the internet could talk to. The Mail Hub is used to denote a message Transfer Agent(MTA) or MTAs used to route email but it does not act as a mail server(having no end-user emailstore) since there is no Mail User Agent(MUA) access.Around 1992, Bell Labs experimented with Circuit-Relay Based firewalls, it is a type of security firewall (proxy firewall) that provides a controlled network connection between internal & external systems (Bellovin et al., 2018).Eagle came after DEC SEAL and was delivered, followed by the ANS Interlock.in Oct 1, 1993. Trusted Information System (TIS) Firewall Toolkit (FWTK) was released in source code from the internet community. It was later named “Gauntlet”. This is still used by experimenters as well as in the industry as a basis for internet security. In 1994, Check Point followed with the Firewall-1 product which introduced “user-friendliness” to the world of internet security. Check points introduced icons, colors & mouse-

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

driver's tools etc. The firewalls before Firewall-1 required editing of ASCII files with ASCII editors.

3. METHODOLOGY & DESIGN

The sections gives the analysis of implementation of firewall approach to network security through the designs and how the software works while implementing it tasks.
The first part of firewall is based on packet filtering mechanism which provides the best isolate between Internet and protected network (Dosal, 2019). The packet filtering is used because it is the basic rule to construct all types of firewall mechanisms are using the packets in it work. While the second part of firewall uses other security mechanisms like log file, authentication, and auditing to the user. This part is used to identify the manager or employee and to display the private information that specified to manager or employee. This firewall system works by receiving packet from the first LAN card that connects to the Internet and from the ports that the system scans it. Then it sends the packet to a buffer, the system will be examining each packet in the buffer by compare the IP address of the source computer and destination computer of packet with authorized IPs table. Therefore, the number of ports and the IP of source and destination computer determine the level of security. Whereas the IP of the source or destination computer is unauthorized the packet is rejected, access is denied and sends message to the request owner (source computer) about this situation (Eric, 2019). When the IP of the source and destination address is authorized, the firewall system will ask the user about his name and password to login inside the protected network. If the name and password is not true, the firewall system will reject his request until the user enter the true name and password or cut the connection. But when the user enters the true name and password, the firewall system sends the packet to the second LAN card connected to the protected network.

A. Software Design

The following algorithm is used when receiving packet from LAN card. This algorithm explains the operation of packet sending after checking the IP address and port number. The firewall program will check the IP's and ports that come from a packet. If the received packet comes from an authorized IP and port is authorized, then allow packet to transfer normally if it is unauthorized then block the connection (Dave, 2013). The software design is divided into 2 categories.

1. Send/Receive Packet from LAN Card

Input: Packets
Output: Scan packet for passing.
Step 1: Get packet from LAN card.
Step 2: Store incoming packet in a buffer.
Step 3: Check the IP address and port number of the sender.
Step 4: Check the IP address and port number of the receiver.
Step 5: If the IP address and port number are authorized, then allow packet to Send/Receive,else block the connection
Step 6: End

2. Checking/Adding IP Address

The following algorithm is used to check the IP address for database when the administrator of the proposed firewall system inserts IP address, examine the database if it is found or not. The first step in this algorithm is used if the administrator adds new IP address to the database. The second step check if this IP address found in the database, if found then message "IP is found" will be displayed, if not then store IP address in the database.
Check IP Address
Input: IP Address
Output: Scan IP address.
Step 1: Get IP address from administrator.
Step 2: Search the IP value in database, if found. Then display message "IP address is found" Else store the IP address in database
Step 3: End

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

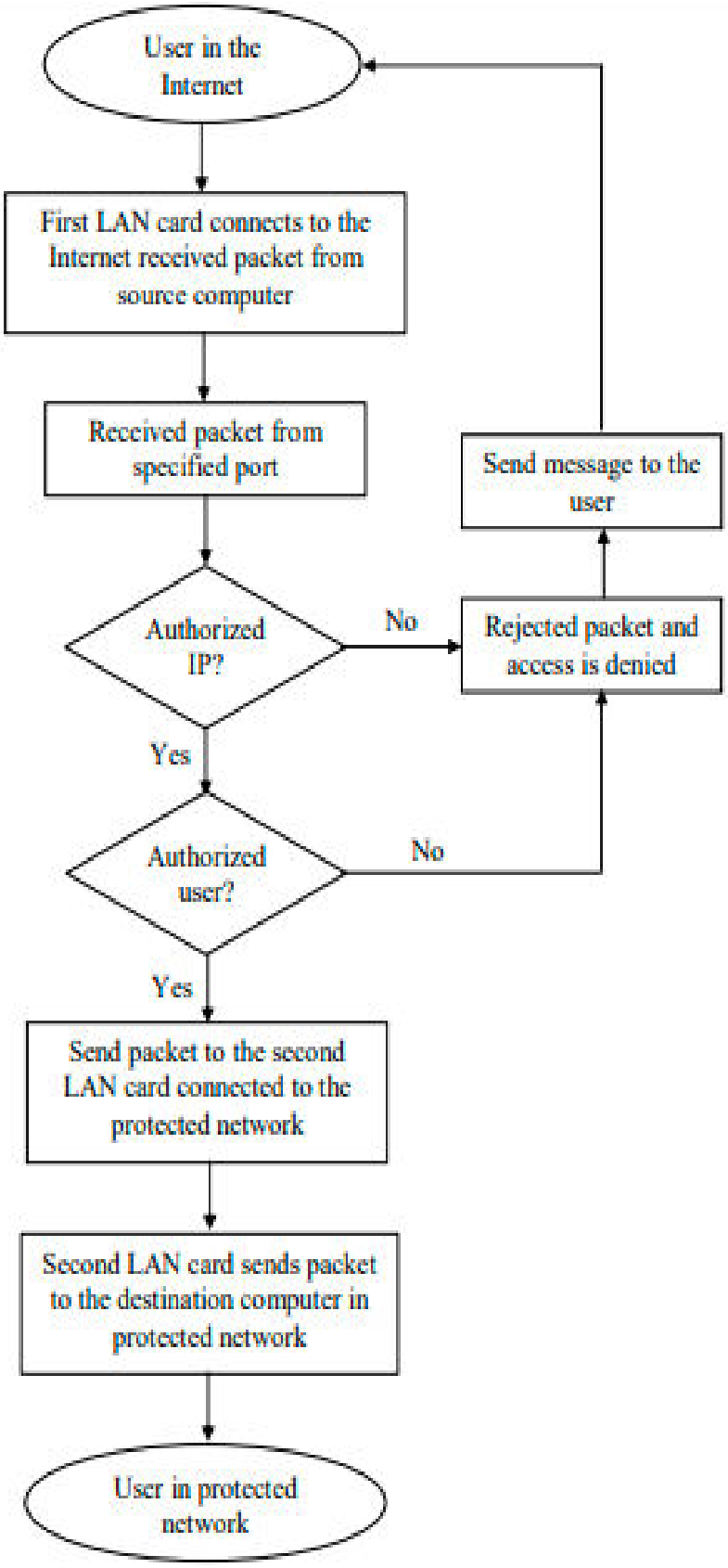

Figure 3. Algorithm for Send/Receive Packet from LAN Card

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

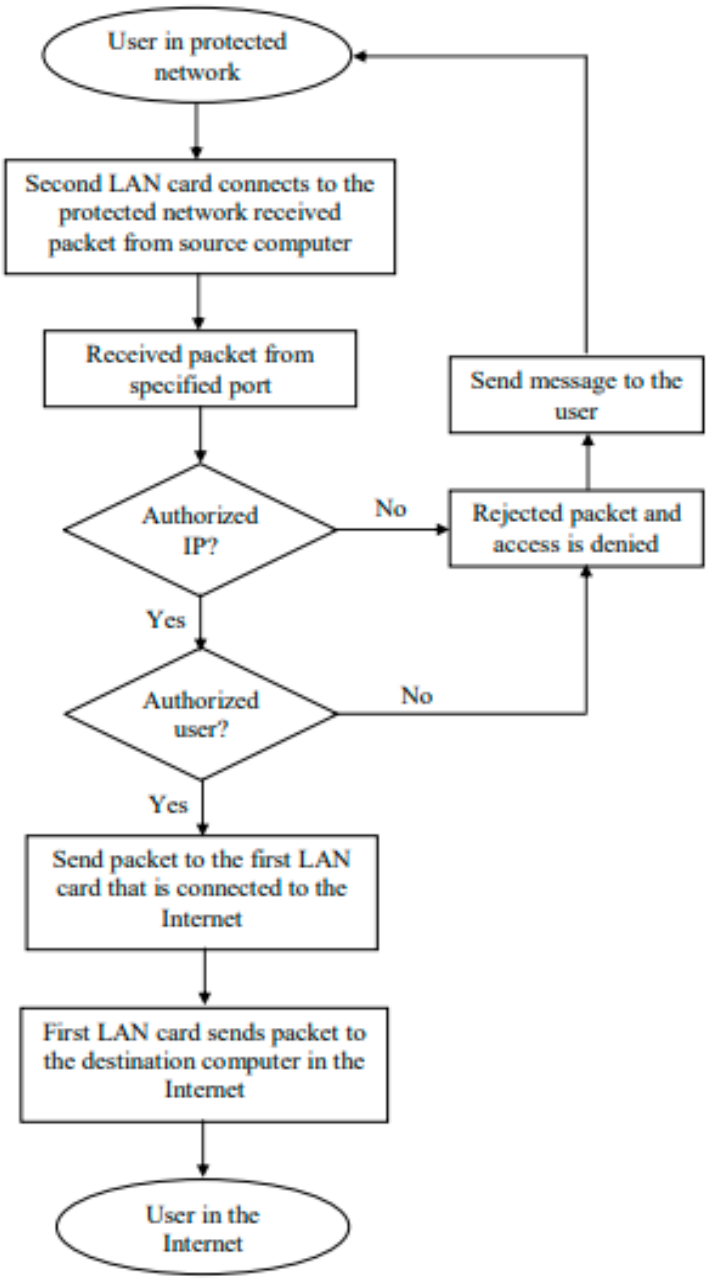

Figure 4. Algorithm for Checking/Adding IP Address

3. IMPLEMENTATION AND TESTING

This section presents the implementation of the firewall system using Sophos as an example which had been built using algorithms discussed in previous sections. Like any firewall system, the firewall system consists of many parts, this section presents and explains how the firewall system's windows works and the relationship among other windows.The proposed firewall system contains more than one window to display the parts of the system; the following sections will describe these parts with its job in firewall system work.

The figures below shows the main window of the firewall system, that displays the public parts of the system. The main form of the network firewall program, which has a screen monitoring of all the connections associated with the computer that this program is working and have a filter screen that represents the filter contents preventing any incoming packets by blocking three types of locations (Local port and Remote port).

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

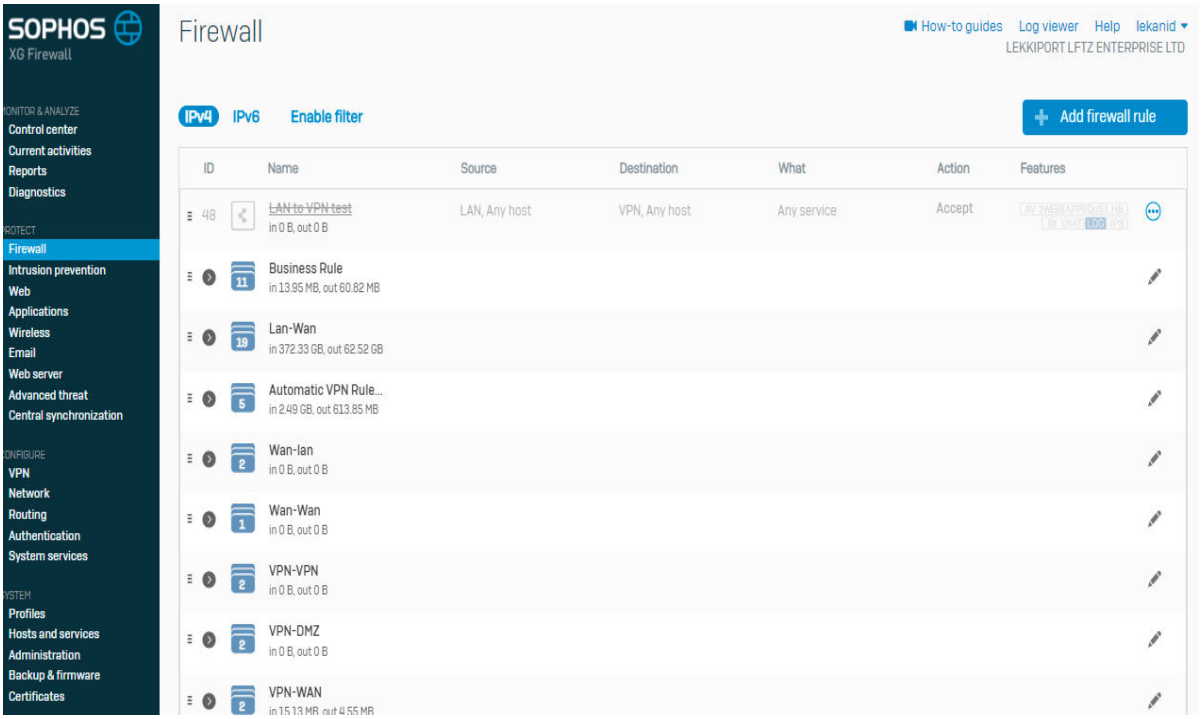

Figure 5. `Sophos interface for rules creation

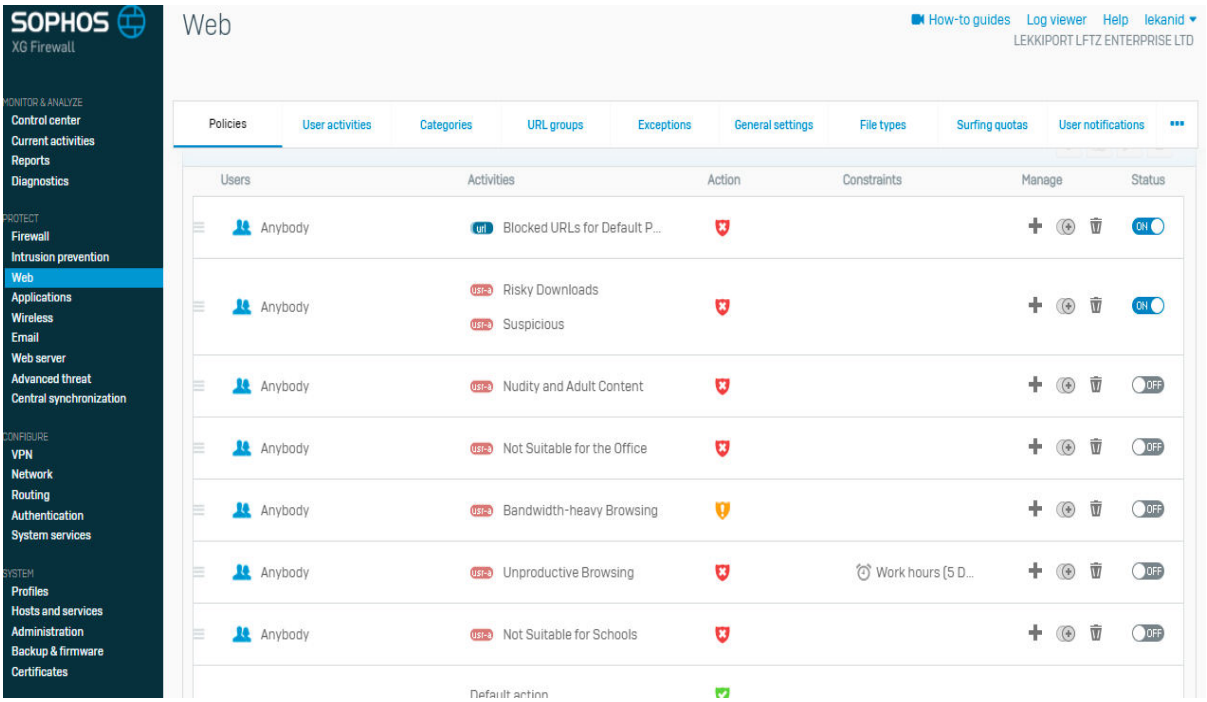

Figure 6. Sophos interface for rules creation for a software traffic

This is the interface in the Sophos firewall environment where rules are created for a specific traffic entering or leaving the network. It allows administrator to specify a particular rule for a traffic. Note, the filter can be enabled and disabled by clicking on enable, disable Filter button at the middle of the main window as shown in figure 6. So public address or IP address, local port and remote port can be added to filter them from accessing through the Internet.

4. FINDING AND RESULT

Findings made us better understand the benefits of firewall security as the first step in helping business grow safely in the ever-changing digital age. Even if business only relies on technology and networks for a small piece of your operations, it is still equally important that you take proactive steps to keep things protected. Firewalls serve as a first line of defence to external threats, malware, and hackers trying to gain access to your data and systems. The implementation of the design revealed that Firewall

Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290

Monitors Network Traffic; Stops Virus Attacks; Prevents Hacking; Stops Spyware; Promotes Privacy. Also firewall approach to the network security is more robust as it discovered that capability of other methodslikepacket filtering, port scanning etc has been utilized through firewall approach.

5. CONCLUSION AND RECOMMENDATIONS

Computer networks are prone to attacks from a wide range of sources. There are different types of internet attackers like hackers, deceitful vendors, or bad employees of an organization that could initiate the attack. It is not necessary that attacks always comes from extrinsic(external) parties but can also be caused by lack of intrinsic (internal) information security, and due to bad policies and procedures. Also, new security risks could arise from evolving attack methods or newly detected holes and bugs in existing software & hardware. Social engineering, Denial-of-service attacks, Protocol based attacks, Host attacks, password guessing, eavesdropping. Back doors, exploiting known security vulnerabilities, hijacking, social engineering, spoofing, Trojan Horses, Viruses, Impersonation, Exploits, Transitive Trust, are many internet attacks which could also fool conventional firewall and harm individual computer or entire networks like anything. To avoid this impact of internet attacks and the later consequences, the use of firewall is highly recommended.

REFERENCES

Aaron B. (2017). Introduction to Firewalls. [White Paper]. Retrieved from http://routeralley.com/.

Avishai W. (2017). Packet Filtering and Stateful Firewalls. School of Electrical Engineering, Tel Aviv University, unpublished

Bhovare, S. R., & Chaudhari, B. K. (2015). A Survey on Data Security Provided in Local Network Using Distributed Firewall. International Journal of Research in Advent Technology, Vol. 2, No. 4, April 2014, E-ISSN: 2321-9637, pp: 169-171.

Chenghua T. et al., (2018). Assessment of Network Security Policy Based on Security Capability. Proceedings of the 2008 International Conference on Computer Science and Software Engineering. December 12 – December 14, Wuhan, China.

David W. (2014). Network Firewall Technologies. Proceedings of the NATO Advanced Networking Workshop on Advanced Security Technologies in Networking, September 15 – September 18, Bled, Slovenia.

Escamilla T. (2018) "Intrusion Detection Network Security Beyond the Firewall", John Wiley & Sons Inc, pg 63-71

Matt W. (2005). An Evaluation of Firewall Technologies. Coursework paper, University of Virginia, USA

Rathod R. et al., (2016). Role of Distributed Firewalls in Local Network for Data Security. International Journal of Computer Science and Applications, Vol.3

Warade S. Et al., (2016). Data Security in Local Network using Distributed Firewall: A Review. International Journal of Computer Applications (0975-8887), National Conference on Emerging Trends in Computer Technology (NCETCT-2016), pp: 19-21

Warlock M. (2019). Evaluation of Firewall Technologies in Network Security. Coursework paper, University of Virginia, USA.

Yekini N. A., Aigbokhan E. E., & Okikiola F. M. (2014). Cryptography System for Online Communication Using Polyalphabetic Substitution Method. Int. J. Advanced Networking and Applications 2151 Volume: 6 Issue: 1 Pages: 2151-2157 (2014) ISSN: 0975-0290

Yekini N.A., Oloyede A.O., & Akinwowle A.K. (2020): Cybernetic Communication Roles in Managing Corona Virus Pandemic Risk: Nigeria Case. Int. J. Advanced Networking and Applications Volume: 11 Issue: 06 Pages: 4471-4477 (2020) ISSN: 0975-0290

Zwiky E et al., (2016)"Building Internet Firewalls", Second Edition, O'relly & Association, pg 14-19