A Systematic Study of Network Firewall and Its Implementation

[1]Raed Alsaqour, [1]Ahmed Motmi, [2*]Maha Abdelhaq
[1]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia
[1]{r.alsaqor@seu.edu.sa , s180011676@seu.edu.sa}
[2*]{Corresponding Author: msabdelhaq@pnu.edu.sa}

Summary
This is an era of technology and with the rapid growth of the Internet, networks are continuously growing. Companies are shifting from simple to more complex networks. Since networks are responsible to transmit huge data which is often sensitive and a point of concern for hackers. Despite the sizes of the networks, all networks are subject to several threats. Companies deploy several security measures to protect their networks from unauthorized access. These security measures are implemented from the device level to the network level. Every security layer adds more to the security of the company's network. Firewalls are the piece of software that provides internal and external security of the network. Firewalls aim to enhance the device level as well as network-level security. This paper aims to investigate the different types of firewalls, their architecture, and vulnerabilities of the firewall. This paper improves the understanding of firewall and its various types of architecture.

Key words:
Firewall; Firewall issues; Firewall types; Firewall vulnerabilities; Firewall architecture.

1. Introduction

With the advent of the internet and fast-growing networks, threats are also increasing. These days networks are an essential part of every business's infrastructure. Networks are prone to cyber-attacks due to the latest tools used to breach security. There are different approaches deployed as cybersecurity in different businesses [1, 2]. All the defensive approaches aim to protect networks from hackers and reduce the chances of information stealing. A firewall is a protective layer that provides security from unauthorized access. It ensures that only legal users can get access to the network and illegal users will be blocked from that network. Firewalls are deployed at different levels such as device-level and network-level [3, 4].

Firewalls are equally beneficial for both businesses and home users. Companies use firewalls to protect their networks from intruders. Firewalls are also implemented to the outbound side to restrict employees from sending some specific kind of emails as well as to send sensitive data outside the network. While on the inbound side firewalls are configured to the inner side of the network. A company can allow one computer to share files while restricting other computers. Firewalls can work with several types of configurations which require a highly skilled IT specialist [5].

In contrast to the use of firewalls in companies, for homes firewall implementation is very simple. In this case, the major goal of a firewall is to protect computer and private networks from malicious actors and their activities. Malware is a major threat to the computer which can destroy the operating system and network. This type of malicious code is spread across computers to steal sensitive information and for illegal access. A firewall can protect these kinds of threats either preventing malicious packets or allow if packets to meet the set of rules [6].

This paper is divided into several subsections which describe different aspects of the firewall, types, architecture, and implementation of the firewall. The goal of this paper is to investigate firewall, its types, advantages and disadvantages of using firewalls as well as how firewalls are implemented. This paper provides a great understanding of the firewall and various aspects in the current time.

The rest of this paper is organized as follows. In Section 2, we provide a firewall background. In Section 3, we present the firewall mechanisms. In Section 4, we describe the firewall implementation. In Section 5, the firewall vulnerabilities are discussed. Advantages and disadvantages of firewall is presented in Section 6 and 7 respectively. In Section 8, we present recommendations to implement the firewall. Finally, the conclusion and possible directions for future work are in Section 9.

2. Firewall

A firewall is said to be a firmware or software that manages certain rules to make sure which type of data packets will pass or block through the network. The core function of a firewall is to reduce the risk of the flow of malicious packets passing through the network so that the security of the network users should not be compromised. The firewall

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.24

could be implemented as standalone software applications or could be integrated with several network devices [7].

The word firewall is a metaphor that could be compared to a physical barrier to protect fire, and a firewall in that case protects an internal or external network from cyberattacks. When a firewall is located at the corner of the network it provides low-level protection, auditing, and logging functions. It is revealed through literature that when companies shifted mainframe computers to the client-server model it became difficult to control the access to the server, so companies it as their priority. Before the emergence of the first firewall the only network security that was implemented at that time was an access control list (ACLs) that was included in routers [8]. ACLs were responsible to decide about the IP (internet protocol) addresses to be passed or blocked through the network. It was observed with the outstanding growth of the Internet and an increased number of networks that ACLs are not enough to protect networks from cyberattacks. So basically, that was the motivation behind the emergence of the firewall and its implementation across the networks [9]. Fig. 1 shows the basic implementation of the firewall within the network.

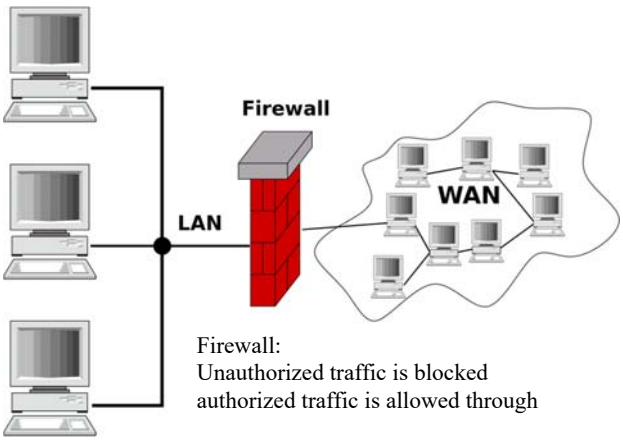

Fig.1 Firewall implementation within a network

It is worth knowing that why firewalls are important for network security. The core objective of the firewall is to eliminate or reduces the exposure to external hosts, networks, and protocols which are considered to be vectors for the major threats to networks. It sets out the foundation of the existing technologies for network security. Although networks and threats have evolving nature still firewall is important to be there. Firewall performs its major role which is to prevent unauthorized access to the networks. This could be done in several different ways based on the requirements of the user and the size of the network [8].

Firewalls could be divided into two major groups such as – host-based firewalls and network-based firewalls.

2.1 Host-based firewalls

These firewalls are installed on the individual's servers and these monitors every incoming and outgoing signal. In some cases, companies deploy host-based firewalls along with perimeter-based firewalls so that internal security could be ensured. For example, some malware attacks could be stopped now by using host-based firewalls. Fig. 2 shows a demonstration of the host-based firewall. A host-based firewall setup is simple to use for users since it could be configured to the user's computers and its settings could be changed anytime for its effective working [10].

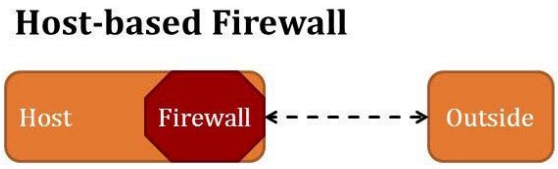

Fig .2 Host-based firewall

2.2 Network-based firewalls

These types of firewall are built in the cloud's infrastructure or could be delivered as a virtual firewall service. The basic purpose of these firewalls is to filter traffic from the Internet to the secured LAN and then vice versa. Fig. 3 shows an example of a network-based firewall.

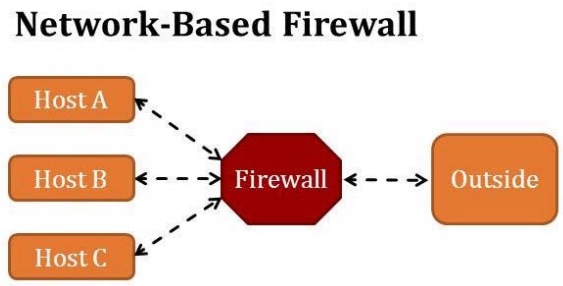

Fig. 3 Network-based firewall

Table 1 shows a comparison between host-based and network-based firewalls with various characteristics.

Table 1: Host-based versus network-based firewalls

Parameter	***Network-based***	***Host-based***
Functions at	Network-level	Host level
Hardware/software based	Hardware-based	Software-based

Placement	End of network	End of the host system
Mobility	Nor possible	Easy to move
Internal protection	End host to end-host communication is not protected in one VLAN	End host to end-host communication is protected in one VLAN
Network protection	Stronger defense	Limited defense
Scalability	Simple	Complex
Maintenance	Reduced	Dedicated
Skillset	Highly skilled resources	Basic skills
Cost	Lower for large companies	Higher for large companies

3. Firewall Mechanisms

There are four major mechanisms used by firewalls which are listed below:

3.1 Packet filtering

A packet filter captures the traffic that is going through the network as per its rules. Normally, a packet filter can have a source IP address, source port, destination IP address, and destination port. Based on these criteria, packets are filtered to be passed or blocked through the network at some specific points [11].

3.2 circuit-level gateway

A circuit-level gateway is a mechanism in which all the incoming traffic is blocked from any host by default. Basically, the client machine operates software to permit traffic to make a connection with the circuit-level gateway machine. Externally it looks like that all the communication is through an internal network but it is coming from a circuit level gateway [12].

3.3 Proxy server

A proxy server works to increase the network performance however it can work as a firewall. It hides the original IP addresses, and it seems like coming from the proxy server. It makes a cache of the requested pages [13].

3.4 Application gateway

An application gateway is somehow a type of proxy server. The internal client establishes a connection with the application gateway and then the application gateway decides either to establish a connection or not. Client to application gateway and application gateway to the destination is responsible for all communication. It keeps a check on all the traffic passing through it. Unlike a proxy server, the application gateway has only one address visible to the outer world so that the internal network is fully protected [3].

4. Firewall implementation

Based on the Firewall architectures, there are several types of firewalls which are described in detail in the following sections.

4.1 Packet filtering

This is the most basic and oldest type of firewall architecture which creates some checkpoints for the incoming and outgoing traffic as shown in Fig. 4. When a packet passes through the packet filtering firewall then its source and destination IP addresses along with protocol and the destination number are checked. If a packet does not comply with the rules of firewall, then it is dropped immediately [1]. For example, if a firewall is configured such that it blocks the Telnet access then firewall will discard the packets which are going to transmission control protocol (TCP) at port 23 [14].

Operations of a packet filtering firewall are very similar to the network layer of the OSI model. However, the transport layer is still getting port number for source and destination. It checks out every packet and does not have information about the packet to be part of a stream of traffic. Packet filter firewall is very effective but as it checks every packet individually which could be vulnerable to IP spoofing attacks so in most cases it is replaced by stateful inspection firewalls [15].

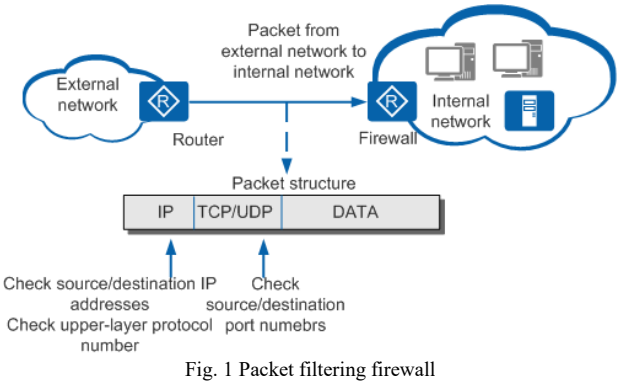

Fig. 1 Packet filtering firewall

4.2 Circuit level gateways

This is another simple firewall that does not consume too much computing resources and quickly passes or blocks the data packets. It works with the TCP handshake which is designed to ensure legitimate data packets. Although these are less resource-intensive but do not check the packets by

themselves. For example, a packet has a corrected TCP handshake but has malware, it will consider as the right packet and will pass through the network. Therefore, these firewalls are not enough at business levels [8]. Fig. 5 shows a circuit-level gateway.

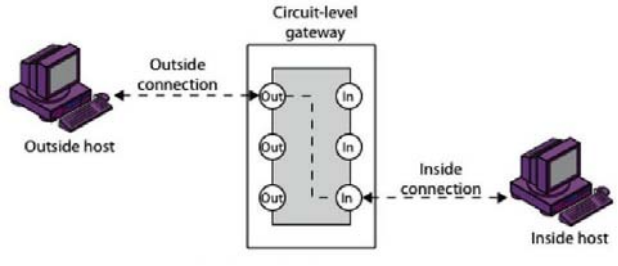

Fig .5 Circuit level gateway

4.3 Stateful inspection firewalls

Stateful inspection firewalls are also referred to as dynamic packet filtering firewall. These firewalls create a table in which all the information about open connections is maintained. On the arrival of the new packet, the firewall compares the packet header in the table to verify that this packet is included in the established connection. The packet is allowed if it is part of the existing connection else it is verified as per the rules of the new connection. These firewalls examine communication packets through incoming and outgoing traffic. Outgoing packets are tracked which requests for an incoming packet and only these packets are responsive across the firewall. Despite stateful firewalls are effective, these are suffered from denial of service attacks [7]. Fig. 6 a stateful inspection firewall.

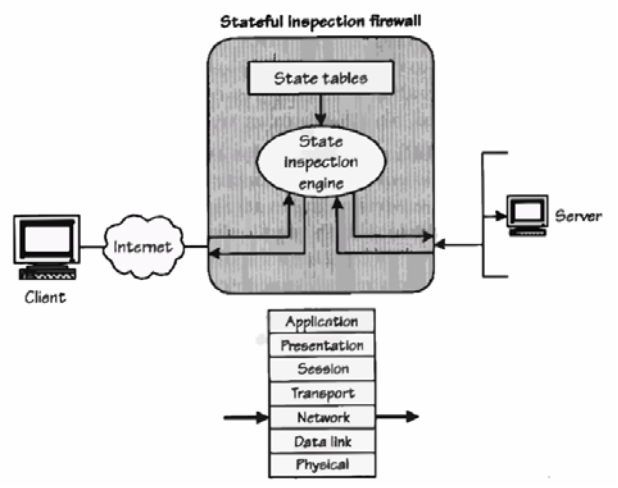

Fig. 6 Stateful inspection firewall

4.4 Application-level gateways or. proxy firewalls

With the increased number of attacks on the cyber server, it has become essential to protect the application layer of the networks. Unfortunately, packet filtering and stateful inspection firewalls are unable to distinguish the valid application layer protocol requests, malicious traffic, and data that is integrated into the valid protocol. In this situation, application firewalls are the more suitable option. These are also known as proxy-based or reserve proxy firewall (see Fig. 7) which could do filtration at the application layer and monitor the packet payload as well differentiate the valid requests and any malicious data within that request. Security engineers have rough control of the network traffic since these firewalls consider payload content to make decisions [11].

These firewalls do not allow hackers to connect directly with the network because it becomes very difficult for the attacker to find the actual place of the network when proxy firewalls are used. So basically, these act as an additional security layer. Proxy firewalls force both client and server to establish a connection through a proxy firewall so whenever an external client asks for a connection with an internal server or vice versa, a proxy server will be used to open a connection for the requested client [16].

Proxy firewalls can block certain content, websites, and malware. Moreover, their rules could be used to manage the execution files for an application [13].

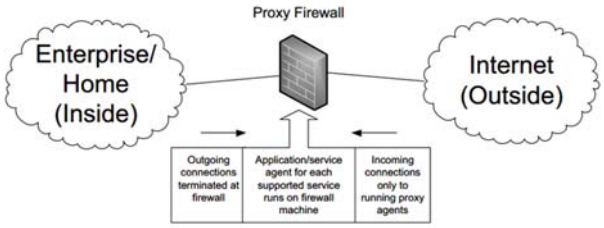

Fig. 7 Proxy firewall

4.5 Next-generation firewalls

These firewalls are the latest release although not clear completely that why these firewalls are known as next-gen firewalls. Deep-packet inspection, TCP handshake checks, and surface-level packet inspection are the most common features of these firewalls. Other technologies could also be incorporated into these firewalls like intrusion prevention systems (IPSs) which prevent attacks to the network automatically [16]. Fig. 8 shows the next-generation firewall framework.

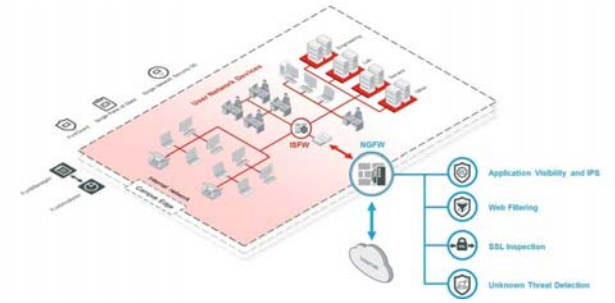

Fig. 8 Next-generation firewall

4.6 Software firewalls

All the firewalls installed on the local devices considered software firewalls. The major benefit of these firewalls is that they define endpoints by isolating networks from each other. Software firewalls are difficult to implement on each device and it may be possible that the device on the network is not compatible with the software firewall [7]. Fig. 9 shows the software and hardware firewall.

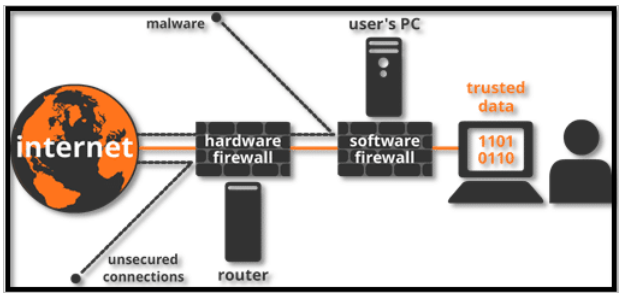

Fig. 9 Software and hardware firewall

4.7 Cloud firewalls

A Cloud firewall is a cloud solution, and these are considered another type of proxy firewall. A cloud server is also used in proxy firewall setup. These firewalls are easy to scale for the companies. More capacity could be added to the cloud to filter more traffic [1]. Fig. 10 shows the cloud firewall.

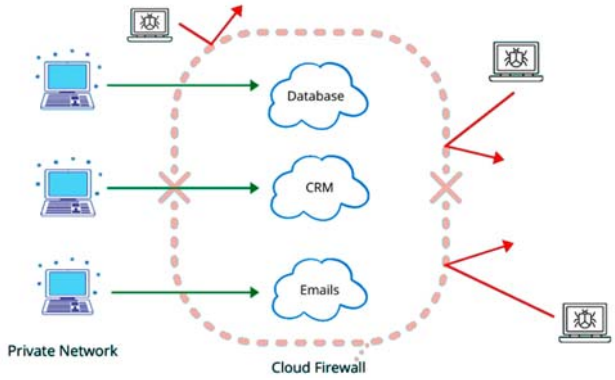

Fig. 10 Cloud firewall

4.8 Personal firewalls

Personal firewalls are beneficial for those users which have an open connection such as a digital subscriber line or cable model since these connections use a static IP address. Due to these characteristics, these networks become more vulnerable to hackers. Generally, the core function of all the firewalls is to filter incoming and outgoing traffic. However personal firewalls are more likely to act as antivirus applications [17]. Fig. 11 shows the personal firewall.

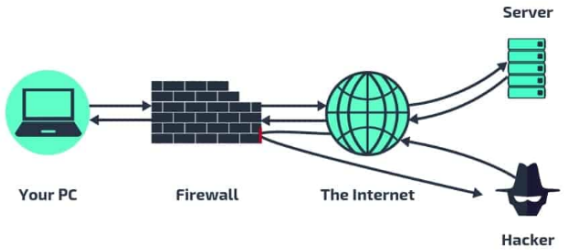

Fig. 11 Personal firewall

4.9 Hardware firewalls

Since a firewall could either be software-based or hardware-based or both depending on the needs of the users. A physical firewall device is more secure because physical access is required to modify it. While a hardware firewall device is not able to read content passing through it as it can only block the information source for example a device. Therefore, it is good to define restriction between home devices but not good for network devices because it cannot filter network based on the content type [13]

5. Firewall vulnerabilities

Firewalls are the most basic components of the cybersecurity architecture of any company. Although

firewalls are taken as security measures however these are not enough as a standalone security measure. Firewalls face some critical issues which are described in detail in the following section [7].

5.1 Insider Attacks

An outside firewall protects the user or network from any attack coming from the outside however inside attacks are also possible with the internal firewalls. The network could be protected if the internal firewall is on top of the outside firewall since internal firewalls divide the assets on the network which makes the attacker work more to get into the system of the user. That increases the break-out time of the hacker which allows more time for making any response against the attacker [13].

5.2 Misused Security Patches

This issue emerges due to a lack of proper management of network firewall software. Since every software has some vulnerabilities due to which software could be exploited. So, in the case of firewall software, it also happens. Generally, firewall vendors create a patch against these vulnerabilities to fix the issues. The existence of a patch does not guarantee that it will be implemented in the network firewall of the company. This patch needs to be applied to the software of the firewall and there are plenty of chances that a random attacker can exploit it [16].

5.3 Configuration Mistakes

This kind of vulnerability happens when there are some mistakes in the configuration of the firewall. It can cause a reduction in the performance of the company network. Poorly configured firewalls are just a waste of money, time, and effort that provides a space for hackers to attack the network [17].

5.4 Lack of Deep Packet Inspection

Deep packet inspection is a difficult inspection mode that is used in next-gen firewalls to check the content of a packet before it is accepted or denied passing the system. Basic firewalls check the data packet from its origin and destination before accept or reject a request which causes an attacker to spoof the firewall. A firewall with deep packet injection could be used to solve this issue since it can check packets that contain malware and then reject those packets [15].

5.5 DDoS Attacks

Distributed Denial of Service (DDoS) attacks are very common attacks because these could be done at a low cost. The objective of this attack is to overcome the resource of the target and shut down the delivery services. One such attack is a protocol attack in which the firewall is drained and the load balancer resource allows the valid traffic. Although a firewall can solve denial of service attacks however these are still vulnerable to DDoS and there is no simple solution for these attacks. There could be several types of attacks that could weaken the architecture of the network. Scrubbing services are provided by some cybersecurity services in which all the incoming traffic is sent away from the network and DDoS attacks could be reduced in this way [18].

6. Advantages of firewall

Some substantial benefits of firewalls are described below:

6.1 Traffic monitoring

A major function of the firewall is to monitor the incoming traffic and a two-way firewall monitors outgoing traffic as well. Data and information are transmitted in the form of packets that are checked by the firewall that either these should pass through the network or not. Even a legitimate sender could send the wrong data which necessitates the use of a firewall for the computers and the network [11].

6.2 Blocks Trojans

A firewall can prevent trojans from entering the network. This type of attack can damage the files on the computer as well as ride on the attachments which could spoil the destination as well [1]. Trojans are considered more harmful because they are disguised and create more serious infections to the files on the computer and server. Trojans remain to hide if something alarming does not happen. A firewall makes them unbale before they become active to exploit computers or networks [19].

6.3 Stops Hackers

A firewall keeps hackers away from the computer and if the firewall is not installed there are more chances that hackers will get hold of a computer or network. In that case, hackers will spread viruses. The firewall prevents these kinds of people and protects the computer and network [14].

6.4 Stops Keyloggers

Keylogger's threat could also be reduced by using firewalls. Keylogger is spyware that records keystrokes and aims to steal passwords as well as sensitive information. By using

this information hackers can access the private information and use it for illegal purposes. Other than these benefits, the firewall can provide security for more than one system. Firewalls not only block malicious packets coming from the network as well as block packets from the other computers within that network [17].

A firewall as a service offers similar benefits as a traditional firewall however it is based on the cloud. So it becomes available for all locations and on every device, in this case, the firewall is available as a virtual barrier instead of relying on a device [8]. Some major benefits of the firewall as a service are listed below:

6.5 Reliability

Firewall as a service is considered more reliable. It is obvious that physical appliances are more prone to attacks and securing these devices is the major concern of cybersecurity experts. Therefore, having an up-to-date firewall is very important. Firewall as a service provides more reliable services without the need for any physical device as well as provide required updates for the software keeping the system to match with the latest technologies [1].

6.6 Simplicity

Firewall management requires a well understanding of the technical aspects and knowledge about WAN otherwise it is difficult to understand firewall issues. Firewall as a service makes these things much simpler for users. Subscription to a firewall is like the CRM or cloud storage provider. Since default protocols are already implemented so even a normal user can manage the firewall with the help of a user interface [20].

6.7 External authority

Firewalls as a service represent the ability of a firewall to an external expert which is an important benefit. In this case, there is no need to hire someone to manage firewall maintenance. Besides, access to more skilled people in the firewall domain and if something goes wrong then the service provider will be accountable for it [12].

6.8 Remote Coverage

In contrast to a traditional firewall, a firewall as a service is more scalable since it makes a cloud. It is easy to implement to the remote locations with no interruptions along with required protocol as well as it makes sure that a similar level of protection is provided for each area. Firewall as a service is suitable for those businesses which have multiple offices at different locations [21].

6.9 Cost-Effectiveness

Firewall as a service is more cost-effective because it is implemented through the cloud. Service providers offer various levels of coverage and protection depending on the needs of the users, however, firewall as a service comes with many affordable packages which could be selected easily. Firewall as a service is much effective cheap and flexible as compared to traditional firewalls. Since a traditional firewall is not enough to provide firm security, therefore, adopting a firewall as a service is the best option for software companies and these should be included in the security plan of cybersecurity [1].

7. Disadvantages of firewall

System performance could be degraded due to the packet filtering software if the firewall is checking every packet as it is a time-consuming task. Configuration and maintenance of the firewall is a complicated task. Also, network firewalls can give users a wrong security sense and forces them to remove security at the machine level [1]. Therefore, if a network firewall is not at its place, it could lead to a disaster. If the firewall is not configured properly then there are chances that it will even block the legitimate software. Moreover, some firewalls slow down the system and distract users [1].

7.1 Real User Restriction

The Firewalls are developed to restrict access to certain networks and computers which can protect computers from any illegal activity. Despite this fact, these also create some issues for workers and employees of the company. Firewall policies could be too strict which can prevent employees to perform even legal actions. These restrictions limit productivity and may provide backdoors for attackers. These backdoors limit the functionality of the firewall and reduce the ability of the network to safeguard data and information [8].

7.2 Reduced Performance

Firewalls that are based on software can affect the performance of the computer. Since software firewalls are always running and consume a lot of power from processor and RAM to perform their functions. These firewalls occupy the resources which could be used in other operations. The level of reduction in performance could be different on the individual computers. In contrast, hardware firewalls do not face these kinds of issues as they are not dependent on the resources of the host computer [1].

7.3 Vulnerabilities

There are several types of vulnerabilities, for example, if strict policies are defined for firewall, then there could be numerous backdoors that could exploit the security plans. Firewalls do not provide features of anti-virus, anti-malware, and anti-spyware as these only restrict illegal traffic. Firewalls also become the point of concern for new hackers when they want to attack a certain network [3].

7.4 Internal Attack

Firewalls can protect the network from the attack, but these do not cover any damage if it happened as the result of an attack. It has been discovered that most attacks on the networks are happened due to the malicious activities of network users. Firewalls have no power to restrict or prevent these kinds of attacks because hackers are within the network [1].

7.5 Cost

Firewall selection should rely on the needs of the company. Software firewalls are more expensive although easy to implement and are very resource-intensive. While hardware firewalls are required purchase and installation for every node in the network. It becomes very expensive for large-scale companies which may have a large number of computers [17].

8. Recommendations

There are several different ways to implement a firewall however some basic steps and recommendations by security engineers and firewall developers for firewall implementation are given below.

8.1 Firewall security

Firewall security is the most important and mandatory practice to prevent an attacker to enter the network. It is extremely harmful to use a firewall that is not completely developed. Some important configuration actions could be:

- Updating firewall according to the latest firmware.
- Delete, disable, or rename any kind of user accounts as well as change all passwords. There must be more strong and complex passwords.
- Shared user accounts are harmful if multiple administrators are managing firewalls. Creating separate accounts for each could be helpful
- Do not use a simple network management protocol (SNMP) or configure it by using a secure community string [21].

8.2 Firewall zones and IP addresses

Before implementing any security, policy, or plan it is essential to define the important assets of the company. Next is to think about the network structure which is essential to group assets under network and decisions could be made that which level of security would be enough [12].

All the servers which provide services across the internet and VPN (a virtual private network) should be placed under a more dedicated group that needs more attention. This group will provide access to very limited inbound traffic coming from the internet. All those servers which do not need access to the Internet should be kept in the internal zone. Besides, some other components such as workstations, point of sale devices, and voice over Internet protocol (VOIP) systems could also be placed in the internal zone [1].

In other words, creating more zones in the network ensures a more secure network. Defining more zone is a time-consuming task and it requires more care. A network using IP version 4 should use internal IP addresses for all the internal computers while Network address translation (NAT) should also be configured so that internal devices could communicate on the Internet when required. After setting out the network zone and IP addresses, it becomes simple to define the firewall protection for each zone [20].

8.3 Creating access control lists

After deciding about the network zones and defining interfaces for those zones, the next step is to know about the traffic which will be passed from one zone to the other. All this traffic will be allowed to pass or stop based on the rules set by ACLs which apply to all interfaces as well as on sub-interfaces. It is important to specify ACLs to the correct source or destination IP addresses along with the port number. Deny all rules is also added to the end of every ACLs list for the restricted traffic. Both inbound and outbound ACLs should be applied on every interface as well as sub-interface. It is a wise approach to disable the firewall interfaces that involve administration roles from the public access to reduce possible threats from the outside world. All the protocols which are not encrypted should also be disabled at this level [8].

8.4 Firewall services and logging

Next is to configure the required services if the firewall can work as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion

prevention system (IPS). Firewall configuration support for all the logging servers is also required [14].

8.5 Testing of firewall configuration

The last step is to test the operations of firewalls in a testing environment. First thing is to think about the objectives for which firewall is deployed and then check the firewall's operations across those rules. Vulnerability scanning and penetration testing should also be done for the firewall. After testing the firewall, it should be able to operate and work on its own. It is also important to keep a backup of the firewall configuration so that recovery would be easy in case of any failure [19].

9. Conclusion

Cybersecurity is an important concern for companies these days since this is an era of the latest technologies and tools used for data transmission. Data and information are the two most important assets for companies. Despite the size of the company, hackers are always keen to steal sensitive information and get illegal access to someone else's computer. It is very difficult for companies to secure their network and user's data from such malicious access. Companies implement various mechanisms to provide defense for their network.

Firewalls are considered the most basic level of security in which all the traffic is filtered either at the devices or network level. All the data or information which do not comply with the rules of the firewall is stopped from entering the network. Firewalls could be software-based or hardware-based, and companies opt for these firewalls depending on their need and the level of security they want.

Firewalls use four mechanisms in their operations which are used in different architectures of firewalls. Firewalls are not considered to provide high-level security however firewall as a service improves security and is very cost-effective for any organization.

Firewalls provide several benefits, but these also have some drawbacks as these may be over restricted and some users may suffer from those rules. Firewalls require a step-by-step procedure for their implementation and companies must follow those steps to implement firewalls successfully. Also, firewalls could be better in terms of providing security if combined with other security measures used for cybersecurity.

References

[1] D. Appelt, C. D. Nguyen, A. Panichella, and L. C. Briand, "A machine-learning-driven evolutionary approach for testing web application firewalls," *IEEE Transactions on Reliability,* vol. 67, pp. 733-757, 2018.

[2] N. Altwaijry, "Identification of Network Attacks Using a Deep Learning Approach," *International Journal of Computer Science and Network Security (IJCSNS),* vol. 20, p. 201, 2020.

[3] T. Abbes, A. Bouhoula, and M. Rusinowitch, "Detection of firewall configuration errors with updatable tree," *International Journal of Information Security,* vol. 15, pp. 301-317, 2016.

[4] K. Kaur and D. Rao, "Automation the process of unifying the change in the firewall performance," *International Journal of Computer Science and Network Security (IJCSNS),* 2014.

[5] N. Ammari, A. A. El Mrabti, A. Abou El Kalam, and A. A. Ouahman, "Firewall anti-leak of sensitive data," *Procedia Computer Science,* vol. 83, pp. 1226-1231, 2016.

[6] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology,* vol. 1, pp. 32-74, 2017.

[7] K. Sattar, K. Salah, M. Sqalli, R. Rafiq, and M. Rizwan, "A Delay-Based Countermeasure Against the Discovery of Default Rules in Firewalls," *Arabian Journal for Science and Engineering,* vol. 42, pp. 833-844, February 01 2017.

[8] C. Diekmann, L. Hupel, J. Michaelis, M. Haslbeck, and G. Carle, "Verified iptables firewall analysis and verification," *Journal of automated reasoning,* vol. 61, pp. 191-242, 2018.

[9] S. Prabakaran and R. Ramar, "Stateful firewall-enabled software-defined network with distributed controllers: A network performance study," *International Journal of Communication Systems,* vol. 32, p. e4237, 2019.

[10] P. Cotret, G. Gogniat, and M. J. S. Flórez, "Protection of heterogeneous architectures on FPGAs: An approach based on hardware firewalls," *Microprocessors and Microsystems,* vol. 42, pp. 127-141, 2016.

[11] T. Kurek, M. Niemiec, and A. Lason, "Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality," *International Journal of Information Security,* vol. 15, pp. 235-250, June 01 2016.

[12] N. Ammari, A. A. E. Mrabti, A. A. E. Kalam, and A. A. Ouahman, "Firewall Anti-Leak of Sensitive Data," *Procedia Computer Science,* vol. 83, pp. 1226-1231, 2016.

[13] Y. Nomura and N. Salzetta, "Why firewalls need not exist," *Physics Letters B,* vol. 761, pp. 62-69, 2016.

[14] G. Hooft, "The Firewall Transformation for Black Holes and Some of Its Implications," *Foundations of Physics,* vol. 47, pp. 1503-1542, December 01 2017.

[15] M. Yeasmin, N. Akter, M. H. Kabir, J. Hossain, and K.-P. Shih, "Performance evaluation of multi-cloud compared to the single-cloud under varying firewall conditions," *Cogent Engineering,* vol. 5, 2018.

[16] R. Mohan, A. Yazidi, B. Feng, and J. Oommen, "On optimizing firewall performance in dynamic networks by invoking a novel swapping window–based paradigm," *International Journal of Communication Systems,* vol. 31, p. e3773, 2018.

[17] P. Cotret, G. Gogniat, and M. J. Sepúlveda Flórez, "Protection of heterogeneous architectures on FPGAs: An approach based on hardware firewalls," *Microprocessors and Microsystems,* vol. 42, pp. 127-141, 2016.
[18] S. Prabakaran and R. Ramar, "Stateful firewall-enabled software-defined network with distributed controllers: A network performance study," *International Journal of Communication Systems,* vol. n/a, p. e4237.
[19] A. Khoumsi, M. Erradi, and W. Krombi, "A formal basis for the design and analysis of firewall security policies," *Journal of King Saud University - Computer and Information Sciences,* vol. 30, pp. 51-66, 2018.
[20] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology,* vol. 1, pp. 32-74, 2016.
[21] M. Dunn Cavelty and A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemporary Security Policy,* pp. 1-28, 2019.