An Overview of Firewall Types, Technologies, and Functionalities

Aftab Ul Nabi
School of Electronics and Information Engineering, South China University of Technology, Guangzhou 510061, China

E-mail: aftabshahani644@yahoo.com

Mushtaque Ahmed
Department of Computer Science, ILMA University, Karachi, Sindh, Pakistan

E-mail: engrmushtaque@hotmail.com

Dr. Ahad Abro
Department of Computer Engineering, Ege University, Izmir, Turkey

E-mail: abdulahadabro1@gmail.com

Submission: 11th June 2022; Revised: 28th June 2022; Published: 1st July 2022

***Abstract*:** The networks are increasing day by day and their complexity is also increasing every passing second. The businesses are going online; the payments are done online. Hence the user wants their data to be highly secured and the internet is a public network, no one is safe from threats on the internet, hence the networks must be guarded perfectly so that people can trust the internet and they will continue to work online. One of the protective mechanisms under serious consideration is the firewall [1]. A firewall secures the network at its entry points, it checks all the traffic which passes through the entry point. The allowed IPs are called trusted while disapproved IPs are called untrusted in firewall terminologies. This paper provides an overview of firewall types, functionalities, and technologies.

Index Terms: Firewall technologies, Network Security, Access Control, Security Policy, Firewall Techniques.

1. INTRODUCTION

Nowadays, Internet has become so common and it is used in almost every field. Banking, e-commerce, engineering, social studies, research, Information technology, history, etc. [2] Internet has become the most essential part of our lives and we cannot even perform our daily routine work without using the internet and its usage and importance are increasing every passing second. As there is so much use of the internet, there is a big risk to security because all the banking systems are working on the internet, and all the transactions are being made on the internet. So, the network security can never be ignored, it has to be highly secured so that more and more users can work freely on the internet. A device that is used for the security of the network interface is called Firewall [3]. As well as, the Firewall works better on Computers and other communication devices just like routers. Which can protect from the suspicious activity of unwanted users. On the other hand, the firewall is a known component or, A System that is placed among two network devices and carries these two properties.

- Public and Private traffic will be passed through firewall policies.
- In this policy system, approved security can easily allow passing through Firewall settings.

Whenever we have seen that a firewall cannot change its built-in features. Because firewall known as security barrier inside the computer and it is designed for unauthorized accessed or suspicious activity from private network. After that, firewall can easily access over the hardware and software where it known as combination of both things [4]. Firewall works continuously on computers which are connected over the internet and it protect us from unauthorized activity or access. So it stops to other user which are trying to connect without permission [5]. As it is shown that data can travel through internet which is in packet form. Firewall has authority to scan such type of packets and analysis them that those packets are right or wrong. Therefore, private and public network have filtered mechanism, where it can be seen through traffic passing system and prevent from unauthorized activity. As well as, firewall protect from suspicious activity over internet. Such kind of things has been defined in filtering policy [6]. The network administrator can develop the polices of firewall and those policies can check step by step to know that those policies are implemented perfectly or not. As it is well-known that firewalls mostly connected on first match method that means if first policy has been matched with match field of packet transferring, so it can be stopped and removed from the given policy manual. Because all policies make the rules for packet moving [7]. Figure 1 shows the firewall schematics and the packet matching involves on field from the TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and IP (Internet Protocol) Packet header [8]. Some of the categories has been shown below:

- Basic-Packet-Filtering
- Stateful-Packet-Filtering

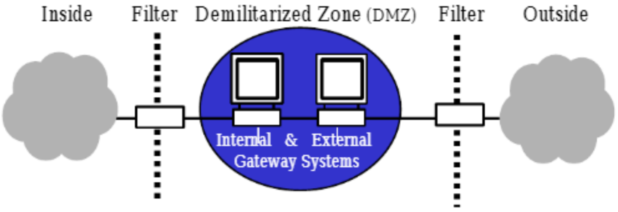

Fig. 1 Firewall Schematics

2. LITERATURE REVIEW

Recent research shows better understanding and improvement of firewall technologies and functionalities Solicits that: Firewalls are one of the most used devices for the safety of the Network, but it has limitations and can be misused by hackers. For example, it can protect the network from outside threats but it is not supposed to protect it if the threat/hacker is from the inside of the network. Anyhow, it can be used for internal safety but it will eventually decrease the efficiency level of the network speed. Firewalls are categorized in different parts which are:

- Packet Filter Firewall
- Application Gateway Firewall
- Stateful Inspection Firewall
- Circuit Level Gateway-Firewall
- Next-Gen Firewalls

Whenever we designed Firewall inside the network than it must provide safety against unwanted activity including Denial of Services (DoS) attacks. DoS attacks occur when users want to attack their victim and that person can harm their victim with their virus or any other soft-type activity using the network. The attacker easily breaks computer security, if the firewall is not working as policies has been designed for their network. Similarly, Yue [9] has analyzed the computer network security features and the main threat, discussed the firewall technology for domestic and international use, they also analyzed the advantages and shortcomings of the firewall device. Likewise, Bishop [10] has also discussed different types of attacks users face on the internet. Correspondingly, Greve [11] has discussed the functionalities and mechanisms of the firewalls, i.e. Access control, etc. Moreover, Burns [12] has argued about the enhancement of firewall technologies for the future.

In starting days, the Firewall has the ability to filter out the network packets and routing-based protocols. After all, they created boundaries inside the network over the world such as connected networks and their secured boundaries within networks. These firewalls were effective for small businesses and computers and networks etc. but there was still a risk [13]. Of course, attackers don't stand putting their hands on their hands, many of the advanced attacks can easily destroy the Firewall settings: such type of attacking activity in the vulnerability of the application servers. Social engineering activity can easily gain access to their inside network through spam emails and such type of website can easily have compromised. In this digital world firewall technology can be advanced too. As well as, firewall technology is going too advanced on the basis of OSI layers. Where it can be identified easily and traffic controlled on the basis of user applications. If the deep inspection of the threats inside the computer, then it must occur in applications traffic [14]. After that, it shifts from ports and protocols where users have a new category which is network protection as well as it called like Next-Generation firewalls. It includes deep packet inspections of encrypted and unencrypted traffic of user-based policies [15]. As we have noticed the efficiency of advanced firewall products can be operated in a difficult way and their weakness/ limitations. If you approved any activity or any message, then the firewall cannot responsible for their loss.

1. The most important thing in Firewall setting, it cannot stop social engineering attacks which is being accept by user, with their approval setting.
2. Inside network administrative setting firewall cannot be responsible for their poor administrative setting and their security policies.
3. When the amount traffic increase then firewall cannot work or process efficiently.
4. It may be efficient, when rules are enforced properly as their need.

Modern Firewalls must:

1. It shows malicious activity from unwanted resources or any other behavior of records that are collected during network connectivity.
2. Security systems work better; it provides better solutions in modified network architecture and they can implement in one operating system so it can easily detect unwanted activity inside the computer. As well as, it responds to advance security threats efficiently.
3. Inside the computer, the usage of dynamic applications which control the new technical service and it manage malicious activity which can occur during the usage of unauthorized software.
4. Threat protection technologies can easily integrate into the full suite any protected software. So the security administrator can easily maintain and protect against security issues.

3. METHODOLOGY

Firewalls contain policies that are used for security purposes and in network terminologies, we can say Trust/Un-Trust. We assign policies for the different networks of IPs through the firewall. Internet is the most un-trusted network because anybody can access our network if we assign the internet as a trusted network. Hence, the firewall comes with a built-in functionality having the internet marked as an un-trust network. The firewall series has become so advanced nowadays as it can perform deep content filtering. Older firewalls were only used to filter a complete IP as a whole, so there was a great risk of policy violations because anyone could access under the roof of that particular IP and the firewall couldn’t detect the malicious particle. But now, firewalls have advanced a lot.

1.1. Firewall Architecture

Firewall Architecture is liable for the standards framework and associated with Sub-Network systems. So it can be divided into sub-network systems just IP or TCP which can easily expose those companies which are responsible for it. Figure 2, which are a subdivision of an IP or TCP/IP network that exposes the company's services to a larger untrusted network, such as the Internet. Let us summarize the different types/technologies of firewalls [16].

Packet Filtering Firewall: Also known as static packet filtering. It was the very first firewall that worked on the network layer of an OSI model, it examines packet headers which included the IP addresses, ports, and protocols of the source and destination [17]. On the basis of these headers, it used to allow or block traffic to pass through it.

Stateful-inspection Firewall: Also known as Dynamic packet filtering. it had access up to the application layer of an OSI model. It was much better in performance than the previous firewall which checked just headers to allow or block the traffic. This firewall is used to store information like port numbers, IP addresses, etc. of the visiting network. It records information intelligently of both incoming packets and outgoing packets, by using these records the administrator can set parameters to meet specific needs [18].

Circuit-level Gateway: These firewalls provided UDP and TCP connection security. It works between the application and transport layer of an OSI model and basically works on a session layer of an OSI model [19].

Application Gateway: Also known as a proxy firewall. It is an application program that runs on a firewall system. This basically creates a secured tunnel between a client and a destination network and when a client or a destination network desires to communicate with each other than all the traffic will be passed through this proxy securely. Although this is considered as one of the highly secured methods of firewall protection, it requires a large amount of storage and processor as compared to other firewalls like static packet firewalls, etc [20].

Next-Gen Firewall: These firewalls are the most recent and advanced firewalls in the current era. These are the 3rd generation of the firewalls which have gone pass through all the traditional security methods like headers checking, port/protocol checking, etc. Instead, it does deep packet inspection, application-level inspection, and Intrusion prevention, and also brings intelligence to the outer of the firewall. Most organizations which are having sensitive data are taking complete advantage of next-gen firewalls and it is their go-to choice nowadays for securing their network [21].

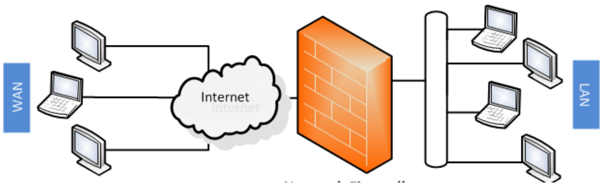

Fig. 2 Shows Network Firewall

Be it on the intranet of any organization or internet. In both these, there has to be some security device that can be used for the security of the organization either from outside networks or from the inside network. A firewall is designed to perform this job [22]. However, principally, the philosophy behind a firewall can be thought of as a pair of mechanisms such as:

- It exists to block traffic
- It exists to permit traffic.

Figure 3, the most important feature of the firewall is that it is at the entry of the network and also at the exit point of the network which eventually means that every traffic that comes inside the network will pass through the firewall first and also every packet of data that leave the network has to go through the firewall [23]. The logic is simple: a firewall must be positioned in a network to control all incoming and outgoing traffic.

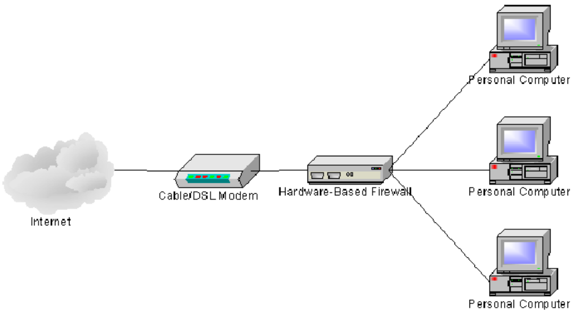

Fig. 3 Illustrate the structure of the Internet

IPsec

IPsec (IP SECURITY) is a protocol that was developed for the security of data communication between networks. It has two modes of operation, the transport mode, and the tunnel mode.

IDS and IPS

Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. This system, it shows various technical things where cyber-attacks cannot enforce the system. Intrusion Prevention Systems (IPS) also analyze packets, but can also stop the packet from being delivered based on what kind of attacks it detects — helping stop the attack [24].

4. PROPOSED FIREWALL MODEL

In this model, figure 4 the firewall compares the connection within internet parameters and it matches the call permit.

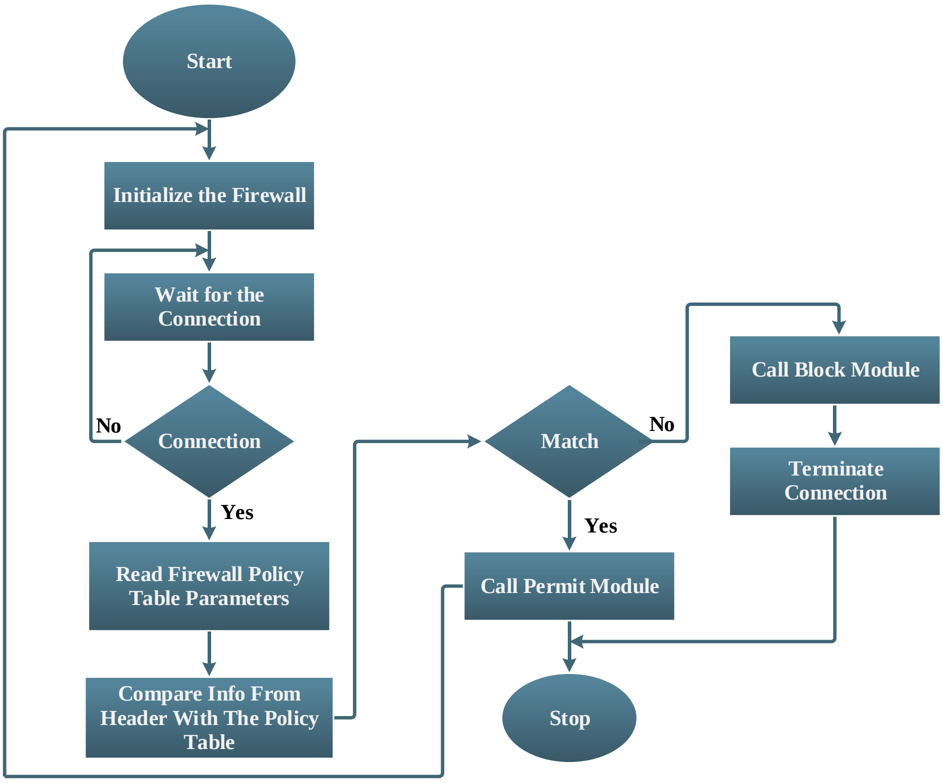

Fig. 4 Proposed Model for Firewall

5. CONCLUSION

This paper examined how the firewall works, and what are different firewall techniques. The paper also gives a brief introduction to the types and technologies of firewalls with diagrams and a working packet filtering firewall flowchart. Also, this paper concluded that a firewall is no doubt the best device for network security purposes but it has some limitations which are mentioned in this paper. This paper also contains reviewed data from some of the previous papers related to this topic i.e. firewalls.

I. References

[1] Abie, H. (2000). An overview of firewall technologies. Telektronikk, 96(3), 47-52.

[2] Liu, A. X. (2008). Formal verification of firewall policies. In 2008 IEEE International Conference on Communications (pp. 1494-1498). IEEE.

[3] Mothersole, I., & Reed, M. J. (2011). Optimising rule order for a packet filtering firewall. In 2011 Conference on Network and Information Systems Security (pp. 1-6). IEEE.

[4] Papadaki, M., & Furnell, S. (2004). IDS or IPS: what is best?. Network Security, 2004(7), 15-19.

[5] Sheth, C., & Thakker, R. (2011, February). Performance evaluation and comparative analysis of network firewalls. In 2011 International Conference on Devices and Communications (ICDeCom) (pp. 1-5). IEEE.

[6] Trabelsi, Z., Masud, M. M., & Ghoudi, K. (2015). Statistical dynamic splay tree filters towards multilevel firewall packet filtering enhancement. Computers & Security, 53, 109-131.

[7] Solanki, V. K., Singh, K. P., Venkatcsan, M., & Raghuwanshi, S. (2013, April). Firewalls policies enhancement strategies towards securing network. In 2013 IEEE Conference on Information & Communication Technologies (pp. 32-36). IEEE.

[8] Kashefi, I., Kassiri, M., & Shahidinejad, A. (2013). A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities. Internationla Journal of Engineering Researh and Applications (IJERA), 3(2), 585-591.

[9] Yue, X., Chen, W., & Wang, Y. (2009, November). The research of firewall technology in computer network security. In 2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA) (Vol. 2, pp. 421-424). IEEE.

[10] Bishop, M. (2003). What is computer security?. IEEE Security & Privacy, 99(1), 67-69.

[11] Greve, D., Wilding, M., & Vanfleet, W. M. (2003, July). A separation kernel formal security policy. In Proc. Fourth International Workshop on the ACL2 Theorem Prover and Its Applications.

[12] Burns, J., Cheng, A., Gurung, P., Rajagopalan, S., Rao, P., Rosenbluth, D., ... & Martin, D. M. (2001). Automatic management of network security policy. In Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01 (Vol. 2, pp. 12-26). IEEE.

[13] Hu, H., Ahn, G. J., & Kulkarni, K. (2012). Detecting and resolving firewall policy anomalies. IEEE Transactions on dependable and secure computing, 9(3), 318-331.

[14] Anderson, B. M., Bunn, W. C., Karnes, M., Lieberman, S. M., & Wilczek, M. E. (2014). U.S. Patent No. 8,701,177. Washington, DC: U.S. Patent and Trademark Office.

[15] Golnabi, K., Min, R. K., Khan, L., & Al-Shaer, E. (2006, April). Analysis of firewall policy rules using data mining techniques. In 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006 (pp. 305-315). IEEE.

[16] Markham, T., & Payne, C. (2001). Security at the network edge: A distributed firewall architecture. In Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01 (Vol. 1, pp. 279-286). IEEE.

[17] Hamed, H., & Al-Shaer, E. (2006). Taxonomy of conflicts in network security policies. IEEE Communications Magazine, 44(3), 134-141.

[18] Eronen, P., & Zitting, J. (2001, November). An expert system for analyzing firewall rules. In Proceedings of the 6th Nordic Workshop on Secure IT Systems (NordSec 2001) (pp. 100-107).

[19] Zhang, B., Al-Shaer, E., Jagadeesan, R., Riely, J., & Pitcher, C. (2007, June). Specifications of a high-level conflict-free firewall policy language for multi-domain networks. In Proceedings of the 12th ACM symposium on Access control models and technologies (pp. 185-194). ACM.

[20] Guttman, J. D., Herzog, A. L., & Thayer, F. J. (2000, October). Authentication and Confidentiality via IP sec. In European Symposium on Research in Computer Security (pp. 255-272). Springer, Berlin, Heidelberg.

[21] Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 18(3), 1617-1655.

[22] Li, X., Ji, Z. Z., & Hu, M. Z. (2005, April). Stateful Inspection firewall session table processing. In International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II (Vol. 2, pp. 615-620). IEEE.

[23] Lanzisera, S., Weber, A. R., Liao, A., Pajak, D., & Meier, A. K. (2014). Communicating power supplies: Bringing the internet to the ubiquitous energy gateways of electronic devices. IEEE Internet of things journal, 1(2), 153-160.

[24] Hamed, H. H., El-Atawy, A., & Al-Shaer, E. (2006, April). Adaptive Statistical Optimization Techniques for Firewall Packet Filtering. In INFOCOM (Vol. 6, pp. 1-12).

Authors' Profiles

Author 1st Aftab UL Nabi received his BC(CS) from the University of Sindh Jamahoro and Master's degree from south china university of technology in 2013 and 2018. During his MS studies, Mr. Aftab ul nabi currently working as a lecturer and deputy director incubation Center at ILMA university. Aftab Ul Nabi has published over 6 Research articles in scientific journals including IoT and WSNs.

Author 2nd Mushtaq Ahmed received his Bachelors degree BE (Telecommunication) from Hamdard university, Karachi 2007-2011. Master's degree ME (Telecommunication) NED university of Engineering Science and Technology, Karachi 2014- 2016. Mr. Mushtaq Ahmed currently working as lecturer at ilma university. Mushtaq Ahmed has published over 5 Research articles in different fields

Author 3rd Abdul Ahad Abro was born in 1988. He received the BS degree from the University of Sindh, MSc degree from Mohammad Ali Jinnah University and PhD degree from Ege University, Computer Engineering Department, Izmir, Turkey. From 2020 to 2021, he was an Associate Professor at ILMA University Pakistan. He has been reviewing numerous indexed journals & conferences paper. His research interests are artificial intelligence, machine learning, deep learning, Natural Language Processing and computer vision