IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Security Network through High Quality Firewalls to Prevent Unauthorized Access

Menka Yadav[1], Dr. Anuranjan Mishra[2]

M. Tech Student, Department of CSE, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[1]

Professor, Department of CSE Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[2]

ABSTRACT*:* This paper presents a detailed study of firewall technologies which are commonly used for network security. A firewall cannot handle all the destructive threats which are coming from unauthorized networks. Therefore, to develop a secured network different types of firewall technologies are used. Lot of researches have been done considering technologies of firewalls. The main purpose of this paper is to apply firewall capacity along with other firewall technologies such as packet filtering, network address translation, virtual private network and proxy services in order to prevent unauthorized accesses. Due to lack of many researches, related to firewall capacity and firewall technologies together. The research group focuses to build a more protected network by combining both firewall capacity and firewall technologies. The experiment results show the proposed idea good enough to build a secured network.

KEYWORDS*:* firewall technologies, firewall capacity, packet filtering, network address translation, virtual private network, proxy services.

I. INTRODUCTION

Security is the most concerned topic for the networking and data communication. Data communication is made by the packet transaction where packet contains the data. There are different approaches are made for securing the network by imposing protection on the network terminologies[1]. One of the eligible approach to get secured network for the data transaction is the implication of Firewall technology. Firewall is the type of network monitor which scans the network and the packets while transaction. There are different protocol involves in the packet transaction through the network. When the data communication is taken place, Firewall check for each and every protocol for their incoming packet and also for the outgoing packet to certain ports. The ultimate objective of the Firewall is to filter the protocols and ports which seem to exhibit suspicious activities[2]. Suspicious activity is meant for the ports or protocol which carries malicious contents or data throughout the network. This is the concerned topic for the network security because the attackers generally penetrate into the user device through the network using those malicious activities. Those attackers or hackers tries to access the network in unauthorized way and without notifying the user also. Their objective is to steel the user data and the confidential information from the network or device or servers[3]. Thus, to protect network and to make it secure, those malicious activities is required to be prohibited from penetrating into the network.

Firewall is used to obstruct or avoid the malicious traffic using the packet filtering technology. This is one of the important technology that is done by firewall. This packet filtering can be done in different ways like virtual private network, Circuit-Level gateways, Application-Level gateway, Network addressing translation, Proxy service like Application proxies[1]. Those technologies are used in different field of applications but all those are implicated for the filtering of incoming and outgoing packets in the network. The integrated solution can be found by combining the Firewall application with those technologies which will allow the certain whitelisted traffic by disallowing the suspicious traffic. The degree of packet filtering depends upon the capacity of firewall but the high capacity firewall technology is much expensive and so, it cannot be used for general purpose[4]. If the security service is established with the low capacity firewall with a combination of the firewall technologies, that will be feasible to be used by user and can be published for user purpose. Many organizations use Virtual Private Network which enables them to connect to their private network securely[5].

This paper is focused on the design of the low capacity firewall with the firewall technologies to deploy the integrated security system using network Address Translation technology. Here, the static packet filtering is used for the filtering the incoming and outgoing network packets. On the other hand, the Network Address Translation or NAT service is used for the remapping of the Internet Protocol address into another protocol diagram. In this scenario, Circuit Level Gateway interacts in the session layer in the OSI model for the packet filtering technology[4]. Additionally, Proxy service is the security technology in the Firewall which allows the packet filtering at the application layer. The firewall will be deployed in the TCP/IP network model where TCP/IP stack is used to determine the legitimate packet in the session of transaction by handshaking the packets.

II. PREVIOUS WORK

There are many approaches are made for the creation of the secure network. This requires the network to be properly filtered. As different protocols are involved in the data transaction, so, one way to filter the packet is through tunneling. This is a technology through which one protocol and the containing data is encapsulated into another protocol. This is a process of transacting the encapsulated data throughout the network. This process is the backbone of Virtual Private Network through which most of the organizations use to connect to an unsecured public network in a secured way[5, 6]. Virtual Private Network is used to establish a secure connection between the data sender and receiver. The advantage of using Virtual Private Network is that the encapsulated data cannot be modified or even read by external agents without the detection of the registered user. So, by using the technology, the probability of unauthorized access to the confidential and sensitive documents in the user machine or in server is minimized. This has the direct impact on the security mechanism[6]. Some of the researches emphasizes on the Firewall mechanism using packet filtering technology which is used to prevent the unauthorized access to the network. Using its mechanism, it can prevent the suspicious packet to flow throughout the network. A firewall can be used for packet filtering to limit information at the network entry of the information which tends to move from one segment of another segment of network. Packet filtering generally uses Access Control Lists (ACLs) of that network that allow the firewall to accept or reject the access that is based on the type of packet or may be dependent upon other parameters related to the packet[7, 8]. It may be seen frequently that a packet is transacting from a unsecured network to a secured network. This may be dangerous for that secured or protected network. But with the implication of the packet filtering technology, such problems can be resolved. Those packets are generally dropped by the Packet filtering as those will not match the healthy criteria that are defined by ACL. That means, Packet filtering works with some predefined rules which is used to create the filter. When the flag is generated for an incoming packet, it indicates that the data may be inappropriate for acceptance. So, those packets are dropped and disallowed to flow through the network by those filters that is by the packet filtering process. Though this process works good in firewall but there are some drawbacks in packet filtering method[3]. Here arbitrary packet can be sent through the network which may pass the ACL criteria. So for many times, it passes without proper checking. Another issue is that the packets can be passed through the network filter without any fragmentation and additionally, some packet services cannot be checked and filtered which are not present in the ACL table. Higher security can be achieved through the complex ACL which is much expensive and thus it will not be commercial.Thus, by using these type of technology in firewall, basic but effective service can be achieved[1, 2].

Some researchershave focused on proxy server firewall. It is a type of firewall service that examines incoming packets at Application Layer of OSI model. As this Firewall operates at the Application layer, thus the mechanism is also known as Application Level Gateway[9]. Basically, these kind of firewall services are provided to the user through other proxy devices or it can be done through cloud platform. Proxy means to hide a data that will be communicated between two ports. Proxy device secure the network and the data transaction through hiding the confidential and even all the data being transacted. While the data transaction is taken place, the session is established between the sender and receiver by user authentication through authorization policy by the service. In this technology, the data communication is not established directly between the sender and receiver. Primarily, the connection is established with the sender or source of the packet. There, the incoming data packet is inspected and checked for consistency. In this process both the data and the underlying protocol is checked to determine whether any malware or suspicious activity is included in it[5]. As soon as the checking is done, the packet and the protocol gets the approval for further connection to the destination. At that time, this service will establish the connection of the proxy server with the destination by making the source communication turned off. Thus, here an extra layer, often called the Client, is created and hence it is anonymous. Thus, the source of the data cannot make a direct connection with the destination. Thus is can be considered as the secured service. Though it has also some problems. If any new service is proposed to be added with the existing one, it is difficult. Additionally, Proxy server responds slowly is the network traffic is dense[9].

There are different Security challenges can be observed while the time of the design [10]. They have investigated the challenges incorporated with the network traffic in different layers in TCP/IP model where the packet transaction is made. Different researchers and authors have proposed their approach for different type of firewall techniques in their research papers. Those includes challenges as it involves different layers of the model where the difficulties are seen. The mapping of the static rule of the network firewall behavior to their dynamic issues are discussed and focus in this research paper.

As observed from different type of firewall technologies, network can also be classified into different type in accordance with the network speed. In very recent era of data communication, new design of firewall is in the demand for securing enforcement for the network with high speed data service [11]. Two important architectures that exist for network parallelization which are the firewall for parallel data transaction and firewall for parallel functionality. for the first case, the packets are distributed through a set of similar type of firewalls which implement filtering policy. For the second type, every firewall creates a subset of the firewall policy with a fewer number of rules. But for the second type, the packets should be processed by all components and also duplicated by the firewalls. Thus, this becomes a new concept of the network firewall technology[6, 11].

Firewall technology is not only used in the corporate sectors or some organization related to Information Technology, but those are implied into the education and research service also[12]. With the immense digitization of technology, some of the educational service like the examination service are made online. In this case, there is a huge possibility to breach the examination data and the credentials. Thus, the underlying firewall technology is enhanced with different technology imposition in it. Thus, the integrated technology for the firewall is able to eradicate different possibilities of data breach by the invocating of malware into the educational and other organizations[13].

This paper focuses on the firewall technology with the implication of packet filtering and Network Address Translation or NAT. Network Address Translation is one of the comprehensive way to deploy security over the network for a computer of group of computer or alike devices. Network Address Translation makes the limit to the number of users who will access the system and web service. This is mostly used by the large or medium organization[14]. As the number of users are limited, it can be used for economic and security purpose as it will not be a public access. All the record of the access to the server is made by the known person like the employees of the organization. Thus the possibility of unauthorized access is minimized. So, there is a least possibility of theft of the network through malware or other suspicious activities[15].

III. FIREWALL TECHNOLOGY

Firewall specifically fall into four different categories like packet filters, application level gateways, full multilayer inspection firewalls and circuit level Gateways. Depending upon the platform, it can also be categorized to Hardware and Software Firewall. Hardware firewalls are considered as the superior and powerful firewall platform[14]. The main purposes of using it is the speed. Those are optimized using the ASIC configuration of the service and driven by machine code. Cisco offers the PIX hardware solution, a packet filtering firewall with state-full inspection. Though the speed of operation differs with the change in the technology behind it. As the speed differs, the capacity also changes for this reason. Recently, Software firewalls becomes the popular to protect the network for home users[8]. Those are basically the standalone configuration and are able to protect the system from malicious activity through the backend coding and use of tool. Software defined firewall is widely used with the implication of the Software Defined Network like the proxy service. Though there are different types of firewall available, those will be used in some particular purposes and those are pointing towards specific operations only. For example, proxy service always relies upon the virtual technology by using the remote server integration, whereas, packet filtering firewall can be used in the native server or machine as per the required rules imposed in it. So, not all those servers can exhibit all the functionalities but this can be achieved by making combination of those. There are different parameters are included for this selection like the capacity, technology, filtering rules etc. which helps to select the proper configuration of the firewall[10]. In the next section, the solution of the problem will be discussed with the proposed methodology and algorithm behind it.

IV. SOLUTION AND PROPOSED METHOD

As security is the most important factor in the security, it always relies upon the integrated and upgraded technology behind it. Every organization use to share their resources and the confidential information to their clients and employees. If the backend logic and algorithm for firewall technology is weak, the hackers can easily can access to the network and can access all the data and thus data breach occurs[4]. Thus, the technology behind the firewall service should be innovative and dynamic so that it cannot be well understood by the hackers. Thus, the probability of hacking will be lessening and the

network will be secured. Another important factor is the capacity of the firewall which acts as the primary role for detecting the suspicious activities.

This research thus, focuses of the firewall capacity with an integration of the firewall technologies like Network Address Translation, packet filtering etc. High capacity firewall is expensive but is able to protect the system from almost all types of threats by detecting their activity on the network monitor effectively[12]. If the capacity is decreased, the performance also will be decreased but the cost will be reduced. Thus, the effective firewall can be designed by the firewall by selecting specific type of technologies so that the firewall capacity and activity will be effective and cost will be moderate.

4.1 Considerable Technology

Every technology behind the firewall service has their own flavor and activity. Packet filtering can filter the packets by some defined rule in ACL which specifically filters the packets and protocols both. On the other hand, Network Address Translation technology secures the network by limiting the number of users in it[10]. Virtual private Network or VPN secures the network using proxy service which disallow the direct interaction between the sender and users. For this purposes, those kind of technologies are used to proposed the new system.

4.2 Proposed Algorithm

The discussed technologies are important to establish a new network and so, the proposed research is based on those technologies and obviously the capacity of firewall. This technique will check continuously for the server idle and busy time. When the capacity of the firewall become lower, it automatically time-out[11]. This is shown as follows:

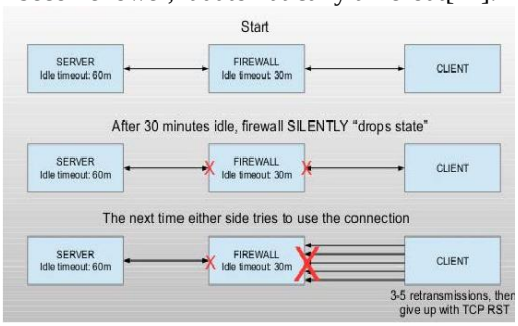

Fig-1: Time-Out

The proposed algorithm for the system is produced below:

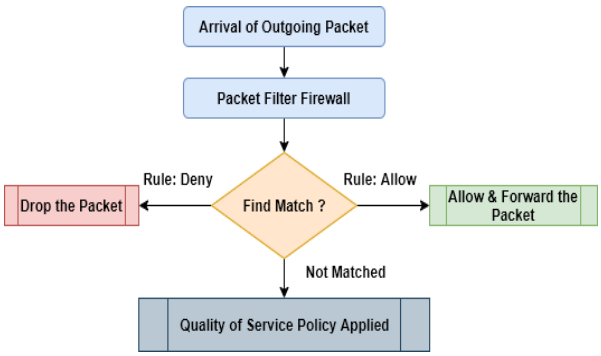

Fig-1: Proposed algorithm for packet filtering

This algorithm will check for each packer arrives at the gateway of the packet filter firewall where the filtering rules will be applied. This part is the heart of the algorithm. With the implied algorithm, the security certificate will be match[3]. If the check will be passed, then it either deny or accept as per the capacity of the firewall at that time. If the rule is not match, then the service will have checked for the Quality of Service(QoS).

4.3 Comparison

In the other technology focus of ideal time of the server is given so that firewall system can perform its task and in time of low capacity it gives time out. This is not generally followed in the current system and there can be security concern when the firewall server becomes lower or inactive.

V. FUTURE WORK

The proposed method is the combination of the firewall capacity and the selected technology which together performs better for the security service. Thus, the threat of the network can be reduced effectively and cam ensure the security is a better way. So, it can be applied in the cyber threat detection and organization firewall services.

VI. CONCLUSION

In this paper, the discussion is made on the basis of firewall technologies and their capacity. The proposed method shows the service with a combination of these two to make the service more effective and to secure the network well. The algorithm proposed can be used in the cyber security detection by making it dynamic with the implication of integrated rule for packet filtering.

REFERENCES

[1] R. S. S. S. S. S. K. L. A. A. S.C. Tharaka, "High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies," International Journal of Scientific and Research Publications, vol. 6, no. 4, pp. 504-508, 2016.

[2] S. a. P. K. Taluja, "Network Security Using IP," International Journal of Advanced Research in Computer, vol. 2, no. 8, 2012.

[3] Tharaka, S. C. et al. 'High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies', International Journal of Scientific and Research Publications, 6(4), p. 504.(2016)

[4] Vishwakarma, A. 'Virtual private networks', Network Security Attacks and Countermeasures, 2(10), pp. 78–114.(2016)

[5] Yusuf Haider, M. and Selvan, S. 'Confidentiality Issues in Cloud Computing and Countermeasures : A Survey', Conference: National Conference On Emerging Computer Paradigms 2016, At NMAMIT, Nitte, 1(July), pp. 1–5.(2016)

[6] S. M. B. a. W. R. Cheswick, "Network Firewalls," IEEE Communications Magazine September, pp. 50-56, 1994.

[7] R. R. H. K. Dhaval Satasiya, "Enhanced SDN security using firewall in a distributed scenario," Advanced Communication Control and Computing Technologies (ICACCCT) 2016 International Conference, pp. 588-592, 2016.

[8] C. D. H. W. Peng Zhichao, "A Load-Balancing and State-Sharing Algorithm for Fault-Tolerant Firewall Cluster," Information Science and Control Engineering (ICISCE) 2017 4th International Conference, pp. 34-37, 2017.

[9] P. D. G. R. B. Miss. Shwetambari G. Pundkar, "ANALYSIS OF FIREWALLTECHNOLOGY IN COMPUTERNETWORK SECURITY," International Journal of Computer Science and Mobile Computing, p. 841 – 846, 2014.

[10] u. K. Sharma, H. K. Kalita and B. Issac, "Different firewall techniques: A survey," Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2016.

[11] R. T. A. B. R. K. Taha Elamine Hadjadj, "Optimization of Parallel Firewalls Filtering Rules," Software Telecommunications and Computer Networks (SoftCOM) 2019 International Conference, pp. 1-6, 2019.

[12] S. R. Sing D., "Enhancement of Firewall Filtering," International Journal of Emerging Trends and Technology in, vol. 2, no. 4, 2013.

[13] D. Satasiya and R. Rupal, "Analysis of Software Defined Network firewall (SDF)," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016.

[14] S.-d. Krit and E. Haimoud, "Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically," 2017 International Conference on Engineering & MIS (ICEMIS), 2017.

[15] S. A. Md Fahad Monir, "Comparative Analysis of UDP Traffic With and Without SDN-Based Firewall," RoboticsElectrical and Signal Processing Techniques (ICREST), pp. 85-90, 2019.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details