International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 363-365
Published Online May 2020 in IJEAST (http://www.ijeast.com)

A SURVEY ON THE DIFFERENT FIREWALL TECHNOLOGIES

Padma Priya Mukkamala
Dept. of ECE
RV College of Engineering,
Bengaluru, India. 560059

Sindhu Rajendran,
Assistant Professor, Dept. of ECE
RV College of Engineering,
Bengaluru, India. 560059

***Abstract*— Given the importance of internet in our day to day lives in today's world, network security is of utmost importance. A firewall acts as a barrier that provides security by filtering traffic. However, traditional firewalls are no longer capable of overcoming new security threats. In this paper, the different types of firewalls, their functionalities and their drawbacks are discussed. This paper talks about the advantages that the different types of firewalls offer. This is a systematic study of the different research work that has been carried out in the different Firewall technologies over the last few years. The firewall types which are discussed mainly are Packet filtering, Circuit level gateways, Stateful inspection, Proxy firewalls, Next Generation firewalls and Cloud based firewalls.**

Keywords— **Proxy firewalls, Next Generation firewalls, Cloud based firewalls**

I. INTRODUCTION

Firewalls are an important part of the security of any network. Firewalls can be of two types namely, network firewalls or host-based firewalls. Network firewalls are those that help to provide security between networks and these run on network hardware. Host-based firewalls are those that help to filter traffic to the end devices or the hosts [1].
Firewalls traditionally worked on rules that were configured statically like access policy lists. Over the years, with increasing threats they have evolved to dynamically detect and react to threats to the network [2]. The different types of Firework technologies work at different layers of the TCP/IP model. This paper studies the different firewall technologies that have evolved over the years.

II. METHODOLOGY OF DIFFERENT FIREWALL TECHNIQUES

The different types of firewall technologies as well as the research conducted is outlined. The advantages and the drawbacks of these technologies are:

- Packet-filtering firewalls

The oldest and most basic type of network firewall is the packet filtering firewall. A packet filter acts as a firewall by creating checkpoints at a network node like a router or switch. The filter has a set of configured rules based on destination and source IP address, port number, and other information. If a packet does not match any of these rules, it is either discarded silently, or an ICMP message is generated notifying the source of the dropped packet.

Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers. Since most of the TCP or UDP based communication uses well known ports for specific applications it is convenient to block packets based on port numbers. Thus, this type of firewall does not look into the contents of the packet [3] to make the decision of rejecting or allowing it.

The types of firewalls are simple in terms of complexity and do not consume much of the resources. However, they are not the most effective firewalls as they are easy to bypass. Another drawback of this method is that there may be conflicting rules which need to be resolved for some packets.

There has been research conducted to develop methods to resolve these conflicts. The firewall may use the IP addresses, port number, or protocol to filter the packets. A 1-tuple filter uses only the destination IP address while a 3-tuple filter uses source IP, destination IP as well as the port number. The complexity further increases when the protocol and packet type is specified. In such cases there may be a conflict of rules. When such an overlap occurs a higher priority filter may be chosen to either allow or reject the packet. A method of adding new resolve filters that can be used to break the conflict is proposed [4]. The resolve filter is added based on the two conflicting rules. This is important because conflicts can lead to security vulnerabilities.

- Circuit-level gateways

This is another simple firewall that does not consume much of the resources. It either approves or denies the traffic based on the TCP handshake. It does not check the content of the packet itself and thus it is not the most effective way of preventing malware from entering your network. However, it is a relatively simple firewall that can be used in certain situations.

The TCP handshake is a three-way handshake technique that helps to establish a secure connection that is full duplex [5]. The SYN and the ACK flags are exchanged between the two communicating entities. This exchange is done in three steps as SYN, SYN+ACK, and ACK. An improved handshake can be used to prevent initial eavesdropping [6] by using

asymmetric key exchange. The challenges of the traditional methods are overcome by optimizing the public parameters. This method is more secure and has lower overhead.

- Stateful inspection firewalls

This type of firewall combines the previously discussed technologies, Packet filtering as well as TCP handshake to provide greater security. This is more computationally complex compared to either of those technologies. It may slow down the rate of transfer of packages.

Stateful firewall uses session tables to maintain a flow of the state of connections. The accuracy of the working of this type of firewall depends on these processing of these tables as well as the packet filtering mechanism. These firewalls are susceptible to DoS attacks.

The packet filtering time can be reduced [7] by rejecting the packets to be denied with the use of a splay tree firewall. This helps to save time as well as memory space. The session state and the timeout data are divided into different data structures. In the case of a Denial-of-Service attack the data can be compared with a splay tree and can be rejected early. Thus, excess computational overhead can be avoided.

- Application-level gateways (proxy firewalls)

As the name suggests these firewalls operate at the application level. They filter the traffic between the network and the source at this level. These are delivered using a proxy device. The proxy firewall establishes connection with the source and then inspects the content of the packet. It looks at the packet as well as the TCP handshake protocol. It also checks the content of the packet to check for the presence of malware.

Only if the data is approved it is sent to the destination. Thus, proxy servers add a layer of protection by providing anonymity to the devices within the network. These proxy devices are generally present at the edge of a network. However, there may a slowdown in the rate of transfer due to the additional security measures. This is one of the drawbacks of this technology.

A proxy firewall obstructs a request from a system on the internal network [8] before sending it to the destination. It behaves as a server while communicating with the client host and as a client when sending or receiving data from the server host. In this manner, the server and the client never have a direct connection. Proxy firewalls function at the application layer and they inspect the content of the data. The decision to either permit or deny data transmission is based on the application protocol headers or payloads. Thus proxy firewalls it offer a greater level of security.

- Next-generation firewalls

The recent firewall technologies combine methods like Deep packet inspection, Intrusion Prevention System, Bandwidth management, URL filtering Antivirus, Malware detection etc. along with the older packet filtering and TCP handshakes based firewalls. These can prevent threats to the network and provide a higher level of security. There is no fixed definition of a next generation firewall. Next generation firewalls inspect the contents of the data and flag potentially harmful data by using signature based methods or machine learning based methods.

There has been research conducted to study of effectiveness of the Next Generation Firewall [9] in the IoT in a smart house and a company. The firewall is tested with various attacks like DDoS, phishing and SQL Injection on the different networks. The results show that the next generation firewall performs better against threats while compared to older firewall technologies.

String matching is one of the methods that can be used for deep packet inspection while scanning for viruses or while filtering content from the internet. There has been [10] a discussion about using string matching and accelerating packet flow as well as using higher level semantics for string matching.

The use of traffic classification techniques by Next generation firewalls is studied [11]. This helps to identify the application level protocols. Machine learning can be used to identify encrypted traffic. A time varying Logistic Regression model that is embedded with traffic pattern is proposed. There is an improvement in accuracy in this model compared to previous models. Many machine learning models can be exploited to study the data traffic.

- Cloud firewalls

A cloud firewall as the name suggests is one that is implemented with the help of a cloud solution. These are considered to be a type of proxy firewall since the cloud server can be thought of as a proxy server. These are easy to scale as traffic loads continue to grow.

When cloud data centers have to be protected the traditional firewalls fail and thus it is necessary to have a technology that can perform anomaly detection. A framework that combines event detection and dynamic resource allocation can be used [12]. A mathematical model is established for this framework.

Software-Defined Networking has been emerging as a structure that can save resources that the corporates and service providers spend on security. This is because it provides centralized management and allows programmability. The benefits of using a cloud based firewall along with a software defined network have been studied [13]. The firewall protects the network from application layer traffic and other attacks.

III. CONCLUSION

The Next Generation firewall is the most suitable while working with emerging unknown threats. It provides operability across the different layers of the network model. While compared to traditional methods, Next Generation firewalls offer the advantage of being dynamic. They use

machine learning methods to identify previously unknown threats by recognizing the behavioral patterns. This is more suitable to be used in an ever changing situation like the current day internet. Cloud based firewalls can be used effectively in Software Defined networks. They can be managed easily and can provide protection from different types of attacks.

IV. REFERENCE

[1] Sheth, C and Thakker, R. (2011) Performance Evaluation and Comparative Analysis of Network Firewalls, *2011 International Conference on Devices and Communications (ICDeCom)*, Mesra. (pp. 1-5)

[2] Vinay T. Patil et al. (2018) Performance and information security evolution with firewalls, *International Science and Technology Journal*, Volume 7, Issue 2. (pp. 33- 38)

[3] I. Mothersole and M. J. Reed. (2011) Optimising Rule Order for a Packet Filtering Firewall, *2011 Conference on Network and Information Systems Security*, La Rochelle. (pp. 1-6)

[4] A. Hari, S. Suri and G. Parulkar. (2000) Detecting and resolving packet filter conflicts, *Proceedings IEEE INFOCOM 2000, Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064), Tel Aviv, Israel*. (pp. 1203-1212)

[5] M. Jadin, G. Tihon, O. Pereira and O. Bonaventure. (2017) Securing multipath TCP: Design & implementation, *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, Atlanta, GA, (pp. 1-9)

[6] D. Kim and H. Choi. (2016) Efficient design for secure multipath TCP against eavesdropper in initial handshake, *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. (pp. 672-677)

[7] Z. Trabelsi, S. Zeidan, K. Shuaib and K. Salah. (2018) Improved Session Table Architecture for Denial of Stateful Firewall Attacks, *IEEE Access, vol. 6*. (pp. 35528-35543)

[8] M. Z. Abdul Aziz et al. (2012) Performance analysis of application layer firewall, *2012 IEEE Symposium on Wireless Technology and Applications (ISWTA), Bandung*. (pp. 182-186)

[9] B. Soewito and C. E. Andhika. (2019) Next Generation Firewall for Improving Security in Company and IoT Network, *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia*. (pp. 205-209)

[10] P. Lin, Y. Lin, Y. Lai and T. Lee. (2008) Using String Matching for Deep Packet Inspection, in *Computer*, vol. 41, no. 4. (pp. 23-28)

[11] Y. Shao, L. Zhang, X. Chen and Y. Xue. (2014) Towards time-varying classification based on traffic pattern, *2014 IEEE Conference on Communications and Network Security, San Francisco, CA*. (pp. 512-513)

[12] S. Yu, R. Doss, W. Zhou and S. Guo. (2013) A general cloud firewall framework with dynamic resource allocation, *2013 IEEE International Conference on Communications (ICC), Budapest*. (pp. 1941-1945)

[13] A. Mahesh et al. (2017), Cloud based firewall on OpenFlow SDN network, *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai*. (pp. 1-6)