A REVIEW ON FIREWALL-BASED COMPUTER NETWORK SECURITY

Akash Devadiga *[1], Mr. Pradeep Nayak *[2], Adithya Tejaswi D *[3], Afiza A *[4], Aishwarya Salimath *[5]

[1] *Student, Information Science and Engineering, Alva's Institute of Engineering and Technology, Karnataka, India*
[2] *Assistant Professor, Information Science and Engineering, Alva's Institute of Engineering and Technology, Karnataka, India*
[3] *Student, Information Science and Engineering, Alva's Institute of Engineering and Technology, Karnataka, India*
[4] *Student, Information Science and Engineering, Alva's Institute of Engineering and Technology, Karnataka, India*
[5] *Student, Information Science and Engineering, Alva's Institute of Engineering and Technology, Karnataka, India*

ABSTRACT

The importance of firewall technology in maintaining computer network security is examined in this essay. It explores the fundamental ideas, guiding principles, traits, and primary purposes of firewalls. Furthermore, a variety of methods and strategies used in firewall technology are investigated. The study emphasises how important firewalls are for protecting network infrastructures from hostile activity, and it ends with predictions for future developments in this area. To protect sensitive data and maintain network integrity in today's computer networking environment, it is crucial to implement strong security measures. This essay explores how important firewall technology is to bolstering network security. The purpose of the abstract is to give a succinct summary of the main ideas, approaches, and conclusions covered in this study. It goes over the foundational ideas of firewall technology, clarifies how it operates, outlines its main purposes, and emphasises how important it is to modern network security paradigms. Through an examination of these facets, this study clarifies the vital function that firewalls provide in strengthening network security, reducing cyber risks, and guaranteeing the integrity of data transfer between networks.

Keyword:- *Firewall Technology, computer network security, network infrastructure, firewall technology, cybersecurity and malware.*

1. INTRODUCTION

In the linked digital world of today, computer network security is critical. The deployment of strong security measures is essential given the exponential increase in cyber threats. Firewall technology is a crucial component in strengthening network defences among these strategies. The purpose of this article is to clarify the role that firewall technology plays in maintaining the availability, confidentiality, and integrity of network resources. In the age of constant connection, when networks are the lifeblood of contemporary businesses, protecting confidential data and fending off cyberattacks become critical issues. Organisations face a wide range of sophisticated tactics, from denial-of-service strikes to malware penetration, as the cyber security environment continues to change. In this situation, firewall technology stands out as the mainstay of network security plans, offering a strong barrier against unwanted access attempts and malevolent assaults. By contextualising the importance of firewall technology in modern network security paradigms, the introduction sets the scene. It describes the main goals of this study, which are to clarify the underlying ideas, operational procedures, and essential roles of firewall technology. Moreover, it

emphasises how important it is for businesses to implement strong firewalls. This research intends to give insights into the effectiveness of firewalls in minimising cyber threats, maintaining regulatory compliance, and increasing the resilience of network infrastructures through an investigation of the fundamental ideas, operating principles, and features of firewall technology. By exploring these facets, the present study aims to add to the conversation about network security and support knowledgeable decision-making among those involved in the responsibility of protecting organisational resources in a more hostile cyber environment.

2. FUNDAMENTAL UNDERSTADING OF FIREWALLS

A firewall is a type of network security solution that keeps an eye on traffic and controls it according to pre-established security rules, enabling or prohibiting connection between networks within and outside the company. It functions as a barrier between private networks and the internet by analysing incoming and outgoing network traffic. Based on pre-established security criteria, firewalls determine whether to let, stop, or drop data packets, allowing only safe, authorised traffic to get through. They are essential to preserving the data and assets of an organization's digital safety. Firewalls use a variety of techniques and technologies to separate potentially harmful behaviour from acceptable network data. Stateful packet inspection, least privilege access, and traffic inspection against known threat signatures are some of these methods. Firewalls may successfully identify dangers that have not yet been discovered by regularly updating databases with new threat patterns and implementing policies that adhere to the concept of least privilege. Firewalls can be divided into groups according to the systems they safeguard, their configuration, where they are located in a network, or the way they filter data. Firewalls of the network, host-based, hardware, and software varieties are common varieties. Furthermore, there are next generation firewalls (NGFWs) that integrate sophisticated features like encrypted traffic inspection and intrusion prevention systems with more conventional capabilities. As gatekeepers, firewalls control data flow between internal and external networks, guaranteeing network traffic security and integrity and averting potential security breaches and unauthorised access.

3. FIREWALL OPERATONAL PRINCIPLE

3.1 Packet Filtering

The simplest type of firewall inspection is packet filtering. It looks over the packet headers and verifies that they match the rules on the firewall. The packet is either permitted or banned based on whether it meets a rule. Typically, undesirable traffic is filtered out of packet filtering firewalls using IP addresses and port numbers.

3.2 Stateful Inspection

To keep track of the status of open network connections, certain firewalls keep a state table updated. By comprehending the context of traffic flows, they are able to decide whether to admit or reject packets with more knowledge. Because stateful inspection firewalls can observe connection states and make judgements based on traffic context, they are considered more secure than packet filtering firewalls.

3.3 Network Address Translation (NAT) and proxying

Some firewalls carry out NAT or proxies. NAT converts internal IP addresses to external ones, whereas proxies intercept and forward traffic. This obscures the core network architecture, adding another degree of security. NAT and proxy firewalls are commonly employed for managing outgoing traffic and enforcing security regulations.

3.4 Application Layer Inspection

In the OSI model, advanced firewalls examine data at the application layer. This enables them to recognise and manage certain protocols or apps that are navigating the network. The most secure kind of firewalls are application layer inspection firewalls as they can examine the data that is really being sent. By recognising and managing certain apps or protocols, they may impose security controls with more granularity.

4. THE PRIMARY PURPOSE OF A FIREWALL

A firewall is a type of technology made especially to keep unauthorised users out of private networks. The firewall itself may be composed of software or hardware, or it may be a combination of the two. The concept of a firewall, or fire retaining wall, originated from a physical device known as a firewall, which is erected in buildings to stop fires from spreading from their origin. Many structures, including apartment complexes, have firewalls built. A barrier was erected between the two apartment buildings to prevent the rapid spread of fire from one unit to the next. A four-sided apartment unit, for example, has to construct a firewall at each of its four border points since the firewall acts as a barrier to the outside world. It will be ineffective to try to contain the fire that will spread swiftly if one side is unrestricted by a firewall while the other three are. This also applies to computer firewalls. A firewall needs to satisfy several requirements in order to perform properly. It also needs to be able to create a "security fence" around a private network and stop unwanted access as well as other disruptions to data or documents on the user's computer. There are many different firewall products available on the market, each with a unique set of features. The degree of security, the degree of access selectivity, and the extent of protection at different OSI (Open System Interconnection) levels are often where firewalls differ from one another.

5. FIREWALL OPERATION

A firewall serves as a security checkpoint that will inspect every traffic entering or leaving the network. The firewall will attempt to filter traffic each time it happens, taking into account the chosen level of protection. Stop important information from being secretly disclosed. Many File Transfer Protocol (FTP) firewalls are deployed just for this one purpose, allowing a firewall to regulate all data flow. In this instance, a firewall helps to stop network users from transferring important private files to unidentified third parties. Keep track of user behaviour. Network users must pass through a firewall each time they access data in order for it to be recorded as documentation (log files), which may then be used to create security systems. Firewall offers information on network usage and has access to log data. Adapting the Upcoming Data Set. NAT (Network Address Translation) is another name for it. NAT, often known as IP masquerading, is used to conceal an IP address so that users can access the internet without having a public IP address. Avoid altering data belonging to third parties. For instance, in business affairs, details about financial statements, product specifications, and other details that are proprietary to the corporation and would be detrimental to external parties' knowledge. To ensure its security, firewalls stop this data from being altered.

6. HOW A FIREWALL OPERATES

Firewalls essentially restrict personal computers' access to the internet. Similar to security guards stationed outside a home, firewalls identify and block unauthorised users from accessing personal computers. Firewalls function as the computer's first line of defence against any hacking attempts. The technology of firewalls is developing steadily. The firewall used to filter computer traffic based on protocols, port numbers, and IP addresses. As it has evolved, the firewall may now filter incoming data by first determining the message's content. One or more of the following techniques can be used by a firewall to control computer and internet data transfer traffic.

6.1 Filtering of packets

It functions as a firewall by keeping an eye on all incoming and outgoing packets and deciding whether to let them through or deny them depending on the protocol, port, and Internet Protocol (IP) address of each one. Using packet filtering to protect against LAN assaults is typically quite successful. Another name for packet filtering is a static firewall. Packets that arrive during communication with the internet network are filtered and compared to rules that have previously been created while constructing a firewall. If the data is appropriate, it will be accepted; if it doesn't comply with the regulations, it will be refused. The firewall verifies the IP address's source and destination when using the packet filtering mechanism. Because the sender of the packet may be using various programmes and apps, the packet filtering additionally verifies the source and destination of protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

6.2 State-approved examination

Stateful Inspection is frequently referred to as a dynamic firewall, as contrast to packet filtering. During stateful inspection, the connection's active status is tracked, and the data gathered is utilised to assess if a network packet can get past the firewall. Large-scale stateful inspection has taken the position of packet filtering. A hacker can obtain information over a firewall by simply indicating "reply" through the packet header on a static firewall, as only the packet header is verified. While security is tighter than packet filtering, a dynamic firewall analyses a packet into its levels by logging the IP address and port number. That concludes the conversation regarding firewall concepts, features, and operation. Could be beneficial. Here is a basic illustration of a firewall rule in IPTables, a well-liked Linux tool for packet filtering. BASH iptables -A INPUT -p tcp --dport 80 -j ACCEPT This rule blocks all other inbound traffic while permitting TCP communication on port 80 (HTTP). The rule would be more intricate under a stateful inspection firewall and would look like this: BASH iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT All other incoming traffic is blocked by this rule, except traffic that is connected to or a portion of an existing connection is permitted.

7. TECHNOLOGY USED IN FIREWALL

7.1 Technology of Composites

One well established and efficient way to use firewalls comprehensively is using composite technology. It is a group of firewalls, alarm systems, and anti-virus software that offers safe, dependable, and dependable security measures. Individuals and businesses alike may guarantee the security of their computer and internet usage by installing firewalls. Furthermore, in order to achieve a decent level of security, specialised firewall software systems might offer numerous levels of distinct defence techniques. Additionally, composite technology may actively conceal the computer's internal state, lowering the possibility of a breach and enhancing security overall.

8. The following is a step-by-step instruction for using composite technology

8.1 Select a Firewall

Pick a dependable firewall programme that can successfully prevent illegal access to your computer network. Norton Firewall, ZoneAlarm, and Windows Defender Firewall are a few examples of this type of software.

8.2 Install Anti-Virus Software

To safeguard your computer against harmful software, like viruses and worms, install anti-virus software. Software that fights viruses includes Avast, Norton, and McAfee.

8.3 Establish Firewall Rules

Set up the firewall rules to only permit inbound and outbound connections that are absolutely essential. This lessens the possibility of illegal users accessing your computer network.

8.4 Configure Intrusion Detection

To actively monitor your computer network, use intrusion detection software. This programme is capable of identifying and stopping illegal access to your computer network. Software for detecting intrusions includes Tripwire and Snort.

8.5 Put Alarm Systems in Place

Configure alarm systems to alert you to any possible dangers to your computer network. This enables you to safeguard your network right away. Alarm systems include, for instance, Alert Logic and LogRhythm. Below is an illustration of how to use Windows Defender Firewall to put up a firewall rule: Look for "Windows Defender Firewall" in the Start menu to launch the Windows Defender Firewall. Select "Turn Windows Defender Firewall on or off." Make your choice to "Turn on Windows Defender Firewall" and press "OK." Then select "Turn on Windows Defender Firewall" to activate it. To add a new rule, select "Restricted" or "Allow a programme through Windows Defender Firewall". Go to the programme that you wish to be able to run across the firewall, then select "Open." Click "OK" after choosing to "Allow the connection." This rule ensures safe connection between your computer and the internet by allowing the designated programme to get past the firewall.

9. USER ACCESS POLICIES

With separate access controls and reference pathways, intranet and extranet usage of the internet may be separated via firewall technology. For security purposes, this guarantees good data transfer, access, and interaction. Different types of protection are used by computer networks and access policies; firewall changes are optimised to increase the security of computer network protection. Rules known as access policies specify how users are allowed to access the network. These regulations may be based on information about the user, their location, and the time of day. By limiting access to network resources based on a user's location and identity, firewalls may enforce these regulations. Network administrators may guarantee that only authorised users have access to critical information and resources by implementing access policies. Additionally, by preventing unauthorised users from accessing the network, access restrictions can lower the likelihood of data breaches and other security events.

10. IDENTIFING INSTRUCTION

One crucial feature of computer internet use is intrusion detection. Computer antivirus software and firewalls can be used together to actively monitor computers. By using a variety of computer methods, the hidden difficulty investigation for computer network security may be finished from every angle. You can regularly utilize software for independent intrusion detection when users employ firewalls, in addition to passive detection. Systems known as intrusion detection systems (IDS) keep an eye on network traffic to spot unusual activity and notify network managers of any possible security risks. Malware infections, denial-of-service (DoS) assaults, and unauthorized access attempts are just a few of the security concerns that may be found using IDS. Intrusion detection systems fall into two primary categories: host-based IDS (HIDS) and network-based IDS (NIDS). While HIDS keeps an eye out for questionable activity on specific hosts, NIDS checks network traffic for it. IDS can give computer networks an extra degree of protection when used in tandem with firewalls. Network administrators can be informed of possible security concerns via intrusion detection systems (IDS), which can identify and stop unauthorized access attempts.

11. Firewall technology can defend against the following typical attacks

11.1 Backdoor programme

Malware of this kind that allows unwanted access to a network or machine.

11.2 Denial assault

An attack when a server or network is overloaded with traffic, rendering it inaccessible to authorised users.

11.3 Deception attack

An attack type in which users are tricked into divulging private information.

11.4Scan attack

This kind of attack looks for weaknesses in a system or network that may be taken advantage. By restricting access to network resources, keeping an eye out for unusual behaviour in network traffic, and warning network managers of any security risks, firewall technology can offer effective defence against these kinds of assaults. Network managers may make sure that their networks are safe and secure from a variety of security risks by combining firewall technology with access controls.

12. CONCLUSION

An essential part of network security, firewalls act as a first line of defence against malicious assaults and unauthorised access. They work by sifting incoming and outgoing network data according to pre-established security criteria. These rules may be based on protocols, port numbers, IP addresses, or other variables. Firewalls exist in several forms such as packet filtering, stateful inspection, application layer, proxy, and VPN firewalls, and can be implemented as hardware devices, software programmes, or a mix of both. Organisations may greatly improve their network security and lower the risk of data breaches and other cyber threats by putting firewalls in place and routinely upgrading their security policies.

13. REFERENCES

[1] The University of Perpetual Help System DALTA, Las Piñas Campus, Alabang–Zapote Rd, Las Piñas, 1740, Metro Manila, Philippines; Shuai Yang1,a,*, Xianfang Wang2,b a444288640@qq.com, b1025472846@qq.com 2Fushun County, Zigong, Sichuan, 643212, China *Author in correspondence

[2] The authors can be reached by email at daniele.bringhenti@polito.it, guido.marchetto@polito.it, riccardo.sisto@polito.it, and fulvio.valenza@polito.it. The authors' address is Dipartimento di Automatica e Informatica, Politecnico di Torino, Corso Duca degli Abruzzi, 24, 10129 Turin, Italy.

[3] Drs. Md. Golam Moazzam2, Dulal Hossain1, Shakil Ahmed1, Mohammed Asraf Uddin1, and Shamimul Islam1 1 Department of Computer Science, Jahangirnagar University, Bangladesh; 2 Institute of Computer Science, Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, Bangladesh Received January 17, 2022; revised December 21, 2022; accepted January 12, 2023; published January 31, 2023

[4] Shaanxi Xueqian Normal University No. 69, Xingshan Temple East Street, Yanta District, Xi'an, Shaanxi 710061, China Chunjuan Wang (Corresponding author: Chunjuan Wang) Email: miaotuichun788@126.com (Received September 22, 2019; First Online Dec. 13, 2022; Revised and Accepted December 5, 2022)

[5] Next Generation AI-Based Firewalls: A Comparative Analysis, Sina Ahmadi. 2023's 49(1) issue of International Journal of Computers (IJC), pages 245-262. hal 04456265 Id for HAL: hal-04456265 Haul.Science.com/hal-04456265 Sent on February 15, 2024