JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Firewall Technology and their Role in Enhancing Computer Network Security

Rashmi P. Dagde
Assistance Professor
Computer Science and Engineering
Priyadarshini Bagwati College of Engineering
Nagpur, India

Pooja G. Thakare
Research Scholar
Computer Science and Engineering
Priyadarshini Bagwati College of Engineering
Nagpur, India

Roshni G. Nerkar
Research Scholar
Computer Science and Engineering
Priyadarshini Bagwati College of Engineering
Nagpur, India

Abstract : The traffic that passes through network infrastructure, such as routers, is controlled by firewalls, which can be designed as hardware, software, or a hybrid of the two. By doing this, firewalls prevent against unauthorised entry from inside as well as outside sources in the boundaries of the local area network (LAN), which comprises external sites as the Internet. In this research, many firewall types with various approaches and methodologies are examined. The discussion focuses on the operation of each kind as well as the pros and cons that they present when deciding on network security strategy. Organisations may make wise decisions to create robust safeguards for their networks while improving overall network protection by being aware of the capabilities that different firewall systems.

IndexTerms **- Firewall, Local Area Network(LAN), Security.**

I. INTRODUCTION

Firewalls are indispensable tools for network security, playing a crucial role in safeguarding the perimeter of a computer network. Their primary function is to prevent unauthorized users or entities, both internal and external, from intruding into the network. This security measure encompasses various methods and technologies that regulate incoming and outgoing network traffic, ensuring the network's protection.

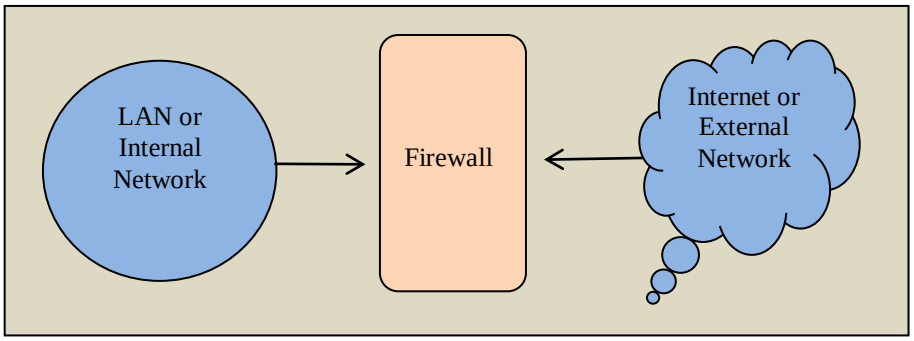

Figure 1.1. Packet Filtering Firewall

Controlling network traffic can be accomplished through diverse approaches, utilizing either hardware or software solutions. This paper will delve into the fundamental technologies and methods employed in different types of firewalls, analyzing their respective advantages and disadvantages. By exploring these aspects, organizations can make informed decisions when implementing firewall systems to fortify their network security.

II. FIREWALL TECHNOLOGY ENHANCES COMPUTER NETWORK SECURITY

In order to protect computer networks from various cyber threats, firewall technology serves as the first line of defence. Its main goal is to defend internal networks from unauthorised access, harmful activity, and subsequent cyber-attacks from outside sources like the internet.Access Administration Firewalls manage the flow of data across networks using pre-set security rules. They can allow or deny communication depending on factors like source/destination IP addresses, port numbers, and protocols by analysing incoming and outgoing packets. By preventing possible dangers, this access control makes sure that only legal and authorised connections are permitted.

The conventional method packet filtering firewalls look at each distinct data packet and determine whether to allow it or garbage it based on predefined criteria. This helps in preventing certain types of attacks, such as Denial of Service (DoS) attacks, by filtering out harmful packets before they can reach the network.Modern firewalls often incorporate stateful inspection, which tracks the state of active connections. This allows firewalls to understand the context of network traffic, making them more effective in distinguishing between legitimate sessions and malicious attempts, including packet-level anomalies and suspicious behaviors.

Advanced firewalls can operate at the application layer, allowing them to analyze application-specific protocols and data. This enables them to detect and block sophisticated threats, such as certain types of malware and intrusion attempts that may exploit vulnerabilities in specific applications.Some firewalls include intrusion detection and prevention capabilities, which monitor network traffic for signs of suspicious or unauthorized activities. When detected, these firewalls can take proactive measures to block the malicious traffic and prevent potential breaches. Firewalls often support Virtual Private Networks, providing secure encrypted tunnels for remote users and branch offices to connect to the main network. This ensures data confidentiality and integrity, especially when accessing the network over untrusted networks like the internet.

III. CHARACTERISTICS OF COMPUTER NETWORK SECURITY IN FIREWALL TECHNOLOGY

Network security in firewall technology involves several key characteristics that help protect a network from unauthorized access, data breaches, and other potential threats. Below are some of the essential characteristics of network security in firewall technology:

3.1.Packet Filtering : Firewalls use packet filtering to inspect individual data packets as they enter or exit a network. Based on predefined rules, the firewall allows or denies packets to pass through. The regulations often depend on factors like source/destination IP addresses, port numbers, and protocols.

3.2.Stateful Inspection : Stateful inspection, also known as dynamic packet filtering, goes beyond classical packet filtering. It monitors the data carried across active connections and tracks their states. This enables firewalls to make better informed judgements and recognise genuine packets associated with established connections.

3.3.Application Layer Filtering : Firewalls can operate at the application layer of the OSI model, which enables them to understand and control specific applications and protocols. This allows administrators to create rules based on application-specific behaviors, providing more granular control.

3.4.Proxy Services : Firewalls can act as proxies for certain services, such as web or FTP (File Transfer Protocol). When a user requests data from an external server, the firewall fetches the information on behalf of the user, shielding the internal network from direct external connections.

3.5.Network Address Translation (NAT) : Firewalls often use NAT to map private IP addresses to a single public IP address. This technique adds an extra layer of security by keeping internal IP addresses hidden from external entities.

3.6.Content Filtering : Some firewalls support content filtering, which allows administrators to block access to specific websites or content categories, helping enforce acceptable use policies and preventing access to malicious or inappropriate content.

IV. MEAN FUNCTION OF FIREWALLS TECHNOLOGY

The primary role of firewall technology is to operate as a protective barrier between trusted internal networks and untrusted external networks. Its function in improving computer network security includes access control, traffic filtering, and detecting/preventing cyber crimes. Firewalls play an important role in preventing possible attacks and data breaches by enforcing security regulations and protecting network integrity.

V. CLASSIFICATION OF FIREWALL TECHNOLOGY

5.1.Packet Filtering Firewalls

Role : The network layer, or Layer 3 of the OSI model, is where packet filtering firewalls function. As data packets move through the firewall, they are examined individually and established rules are used to decide whether the packet should be permitted or banned.

Enhancement : Packet filtering firewalls offer fundamental network perimeter security by obstructing traffic based on source/destination IP addresses, port numbers, and protocols. Although they lack the more sophisticated inspection capabilities of other firewall kinds, they are effective for high-speed network traffic.

5.2.Stateful Inspection Firewalls (Stateful Firewalls)

Role : Stateful inspection firewalls operate at the transport layer (Layer 4) of the OSI model. They maintain a state table of active connections and use this information to intelligently allow or deny incoming packets based on the context of established connections.

Enhancement : Stateful firewalls provide improved security by understanding the context of network connections. They can differentiate legitimate packets belonging to established sessions from potentially malicious packets, offering better protection against various types of attacks.

5.3.Proxy Firewalls

Role : Proxy firewalls have a role at the OSI model's application layer (Layer 7). Instead of directly transmitting traffic between networks, they function as mediators, making requests to external servers on behalf of inside clients.

Enhancement : Proxy firewalls give an extra certificate of protection by concealing the internal network's information and shielding it from direct external connections. They can conduct content filtering, data inspection, and protocol validation, making them useful in avoiding application-layer assaults.

5.4.Next-Generation Firewalls (NGFW)

Role : Traditional firewalls primarily examine packet headers to allow or restrict traffic based on IP addresses, ports, and protocols. NGFWs go beyond these basic firewall functions. NGFWs are responsible for implementing cutting-edge security measures into their operations.

Enhancement : Next-Generation Firewalls (NGFWs) have transformed network security by providing a more comprehensive means of defence.

5.5.Cloud Firewalls

Role : Cloud firewalls are designed specifically for cloud environments, providing security for virtualized networks and cloud-based applications.

Enhancement : Cloud firewalls offer scalability, flexibility, and centralized management, ensuring consistent security policies across distributed cloud infrastructures.

5.6.Application-Aware Firewalls

Role : Application-aware firewalls focus on understanding and controlling specific applications and their associated behavior.

Enhancement : By enforcing policies based on application characteristics, these firewalls improve security and enable administrators to implement more granular access controls.

5.7.Unified Threat Management (UTM) Firewalls

Role : UTM firewalls integrate multiple security features into a single platform, including firewall, antivirus, anti-spam, content filtering, VPN, and more.

Enhancement : UTM firewalls provide a holistic and streamlined approach to network security, simplifying management and reducing the complexity of deploying multiple security solutions.

VI. APPLICATION OF COMPUTER NETWORK SECURITY IN FIREWALL TECHNOLOGY

Firewall technology plays a vital role in enhancing computer network security by providing a first line of defense against potential threats. Here are some key applications of firewall technology and their roles in improving network security:

6.1. Network Perimeter Protection : Firewalls are commonly deployed at the network perimeter, acting as a barrier between the internal trusted network and the untrusted external network (usually the internet). They analyze incoming and outgoing traffic, blocking unauthorized access attempts and malicious data packets.

6.2.Access Control : Firewalls implement access control policies based on predefined rules, allowing or denying traffic based on factors such as source/destination IP addresses, port numbers, protocols, and application data. This ensures that only legitimate and authorized connections are allowed.

6.3.Traffic Filtering and Packet Inspection : Firewalls inspect packets passing through them to detect and block potentially harmful data packets. They can filter traffic based on packet headers, content, and behavior, identifying and thwarting common attack patterns like DDoS attacks, port scanning, and malicious payloads.

6.4.Application Control : Firewalls with application-layer filtering capabilities can identify and control specific applications and protocols. This helps in enforcing policies related to the use of certain applications and blocking potentially risky or unauthorized ones.

6.5.Prevention of Malware and Intrusions : Firewalls equipped with Intrusion Prevention Systems (IPS) and malware detection capabilities can identify and block known malicious signatures, preventing malware and unauthorized intrusions from entering the network.

VII. LITERATURE SURVEY

[1] The paper proposes a network firewall stateful detection model that incorporates a trust mechanism. The primary objective of the model is to enhance the effectiveness and efficiency of network firewall systems. The trust mechanism plays a significant role in assessing the trustworthiness of various entities within the network, such as devices, users, and network segments.

[2] The paper likely focuses on the application of computer network information security and firewall technology in the context of the new environment. The "new environment" could refer to the latest developments in networking, emerging technologies, or changing cyber security challenges.

[3] The paper likely focuses on the integration of Firewall and IPSec (Internet Protocol Security) technologies to establish a Layer 3 (L3) and Layer 2 (L2) integrated Virtual Private Network (VPN) solution. The authors may discuss the technical aspects and benefits of combining these security mechanisms to enhance the security and performance of VPNs.

[4] The paper likely focuses on the practical application and research of Virtual Private Networks (VPNs) based on the IPSec (Internet Protocol Security) protocol within the context of a firewall environment. The authors may explore how the integration of VPN and firewall technologies enhances network security, privacy, and remote access capabilities.

[5] The dissertation likely focuses on the collaborative strategy between IPSec (Internet Protocol Security) and firewall technologies, with a specific emphasis on the IPv6 protocol. The author may investigate how IPSec and firewall can work together in a coordinated manner to enhance network security and protect IPv6-based communication.

[6] The paper likely focuses on the study of technology used in firewall systems. The author might explore various aspects related to firewall technology, including its features, capabilities, configuration, and effectiveness in providing network security.

VIII. CONCLUSION

A network's security begins with effective protection against external access, and firewalls serve as a critical perimeter defense to achieve this goal. Over the years, firewall systems have evolved from simple packet filtering methods to sophisticated packet inspectors capable of making decisions based on traffic purpose, sources, and destinations. Among the various firewall technologies, dynamic inspection packet methods have proven to be the most effective in protecting network traffic.

However, a firewall system's effectiveness goes beyond its chosen methodology or technology. The best firewall system should also offer robust logging and reporting features. These features enable comprehensive recording of all actions taken by the firewall system and provide valuable insights into any intrusions that may occur within the computer network. By staying informed through detailed logs and reports, network administrators can promptly respond to potential threats and continuously enhance the network's overall security.

Lastly, a well-implemented firewall system, equipped with dynamic inspection packet technology and comprehensive logging/reporting capabilities, serves as a strong defense against unauthorized access and potential intrusions, safeguarding the integrity and security of the network.

REFERENCES

[1] Li Hongying, Zhang Xiaoman and Zhang Tianrong, "Network firewall stateful detection model based on trust mechanism[J]", Computer Simulation, vol. 39, no. 4, pp. 428-431, 4 2022.

[2] Luo Xiao, "Research on the application of computer network information security and firewall technology in the new environment[J]", China Computer & Communication, vol. 8, pp. 215-217, 2022.

[3] Shen Lingyu and Zhu Zhenqian, "Firewall and IPSec cooperate to realize L3/L2 integrated VPN [J]", Communication Technology, vol. 53, no. 09, pp. 2334-2337, 2020.

[4] Cao Yaqun and Zhu Jun, "Application Research of VPN Based on IPSec Protocol in Firewall [J]", Software Engineer, vol. 18, no. 3, pp. 37-38, 2015.

[5] Pan Pingjiang, Research and design of collaborative strategy between IPSec and firewall based on IPv6 [D], Guangdong:South China University of Technology, pp. 5, 2015.

[6] Bin Hamid Ali, F. A., "A study of technology in firewall system," Business, Engineering and Industrial Applications (ISBEIA), 2011 IEEE Symposium on, vol., no., pp. 232,236, 25-28 Sept. 2011.

[7] Zhang Yu, "The Program Design of Network Firewall Based on Windows," Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference on, vol., no., pp. 553,556, 24-25 April 2010.

[8] Xiang-Dong Hu and Wei Qinfang, Applied Cryptography Tutorial, Beijing:Electronic Industry Press, pp. 25-47, 2005.

[9] Guo Jikun, Firewall and intrusion detection technology information technology, Beijing:China Electric Power Press, vol. 27, no. 3, pp. 10-12, 2003.

[10] LI Tao, Introduction to network security, Beijing Electronic Industry Press, pp. 107-111, 2003.

[11] Xin Huang, Shen Chuan-Ning and Fallujah Wu, Attacks and prevention, Beijing China Electric Power Press, pp. 22-37, 2002.

[12] ZHU Ge-Mei, Zhou Chuan-Hua and ZHAO Bao-hua, Network security and new firewall technology. Beijing Electronic Industry Press, pp. 92-201, 2001.