Journal of Computer Science and Frontier Technologies
ISSN Print: 3104-4204
ISSN Online: 3104-4212
CD ISSN: 3104-4220
https://doi.org/10.63313/JCSFT.9013

An Initial Exploration of Core Network Security Defense Technologies

Jiaxiang Ge[1]. Yaoxuan Guo[1] and Yuchen Xu[2]
[1]School of Computer Science and Technology, Zhejiang Normal University, Jinhua, China
[2]College of Physics and Electronic Information Engineering, Zhejiang Normal University, Jinhua, China

How to cite this paper: Ge, J., Guo, Y., & Xu, Y. (2025). An Initial Exploration of Core Network Security Defense Technologies. Journal of Computer Science and Frontier Technologies, 1(2), 30-38. ISSN Print: 3104-4204; ISSN Online: 3104-4212.
https://doi.org/10.63313/JCSFT.9013
Published: 2025-10-16

Abstract

With the rapid development of Internet technology, network security issues such as hacker attacks, ransomware, and DDoS attacks have gradually come into public view. This paper sorts out two core defense technologies—firewall technology and Intrusion Prevention System (IPS)—from the perspectives of technical principles, development trends, and application scenarios. Meanwhile, combined with current network security hotspots such as zero-day vulnerabilities and AI-driven attacks, it analyzes the challenges and development trends faced by the aforementioned defense technologies.

Keywords

Network Security; Defense Technology; Firewall; Intrusion Prevention System (IPS)

1. Introduction

1.1. Research Background

With the rapid development of Internet and artificial intelligence technologies, digital life has become an integral part of everyone’s daily life, and the Internet is closely intertwined with people’s daily routines. However, a wide variety of network attacks and data theft methods have emerged one after another, making network security threats increasingly severe. The Global Cybersecurity Index 2024 Edition points out that network security risk incidents occur frequently worldwide, especially the frequency and scale of ransomware attacks are on the rise. Statistics show that the annual growth rate of global network attack incidents reaches 35% . These threats not only undermine the stability of public network infrastructure but also directly endanger personal interests, commercial interests, and national interests.

1.2. Research Purpose and Significance

This paper aims to conduct an in-depth exploration of various "core defense technolo-

gies" in the field of network security, and analyze their technical principles, development trends, and application scenarios one by one. As the "first line of defense" in the network space security protection system, defense technologies are designed to block risks through their independent defense capabilities before an attack occurs, which is different from the "post-event discovery" feature of network security response and detection technologies. The significance of this research lies in systematically sorting out various core defense technologies, providing theoretical references for researchers and practitioners in the network security field, and promoting the further development of relevant defense technologies in the future.

2. Overview of Firewall Technology

2.1. Basic Concept

A firewall is a network security system composed of software and hardware. It is located between an internal network (usually secure) and an external network (usually with security risks) and serves as the "first line of defense" for network boundary protection. It filters data flows according to predefined security policies and access control rules, while preventing unauthorized access and data leakage, and effectively monitors network activities between the internal and external networks. Depending on the configured security policies, firewalls filter data flows in three ways: (1) allowing data flows to pass through the firewall into the internal network; (2) denying data flows access; (3) directly discarding the data flows. Its basic functions include filtering data and services entering and exiting the network, managing network access behaviors, recording all activities passing through the firewall, and detecting and alerting on network attacks. Generally, a firewall refers to one or a set of systems that implement access control policies between two networks, as shown in the figure below.

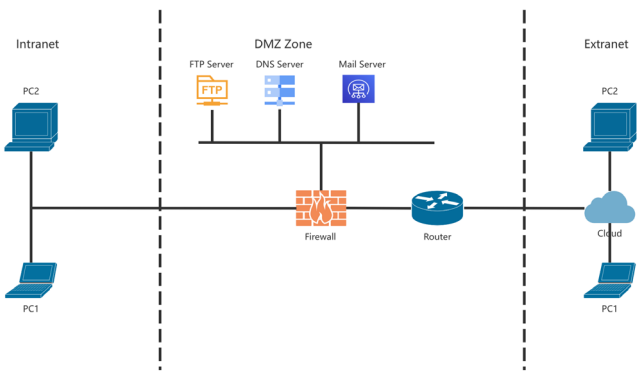

Figure 1. Schematic Diagram of a Firewall.

2.2. Core Principles of Firewall Technology

The basic working mechanism of a firewall is based on access control policies. It can

filter out prohibited protocols, ports, IP addresses, etc., and only allow legitimate traffic to pass through to protect the internal network [2]. Its core logic includes the following three steps: (1) Traffic Capture: Intercept all data packets entering and exiting the network boundary and extract key fields of the packets, such as source IP address, destination IP address, source port number, destination port number, and protocol type. (2) Rule Matching: Match the key fields of the data packets with the security policies and access control rules set by the administrator to determine the filtering action. (3) Action Execution: Based on the matching results, execute actions such as allowing access, denying access, or directly discarding the data flows to ensure that only permitted data flows enter the internal network.

3. Key Firewall Technologies

In practical applications, firewalls adopt a variety of mechanisms and technologies to implement access control, including packet filtering, stateful inspection, and application proxy. These mechanisms can be used independently or in combination to provide multi-level protection.

3.1. Packet Filtering Technology

Packet filtering is the most basic technology of firewalls. It filters data packets at the network layer based on a combination of information such as the source IP address, destination IP address, port number, and protocol type of the data packets. Packet-filtering firewalls process data packets according to a preset set of rules, which are usually implemented based on Access Control Lists (ACLs).

Its main advantages are simple logic, fast processing speed, and little impact on network performance. However, it also has obvious limitations. First, unauthorized access can bypass the firewall, for example, by exploiting software and configuration vulnerabilities on the host. Second, the source address, destination address, and IP port number of the data packet are all in the header of the packet, which may be eavesdropped or spoofed.

3.2. Application Proxy Technology

An application proxy firewall operates at the application layer of the computer network. It acts as an "intermediary" to proxy communications between internal network users and external network servers. The proxy server can inspect incoming and outgoing data packets, copy and transmit data through the gateway, and prevent direct connections between trusted servers/clients and untrusted hosts.Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

Its advantages mainly include the ability to store detailed information about con-

nections and applications, and implement complex access control at the application layer. At the same time, it does not allow direct connections between internal network hosts and external network servers, which can hide internal addresses and improve security. However, it also has the following disadvantages: the proxy service may introduce high processing latency, as incoming packets need to be processed twice by the application program and its proxy, making it a network bottleneck. In addition, different proxy programs need to be written for different application services, resulting in poor adaptability and complex user configuration, which increases the workload of system management.

3.3. Deep Packet Inspection (DPI) Technology

Deep Packet Inspection (DPI) is the core technology of next-generation firewalls. It not only inspects the header information of data packets but also deeply extracts, matches, and analyzes the payload information of the packets to identify application-layer protocols and malicious code [4]. DPI is implemented through a variety of technologies, including protocol identification, pattern matching, behavior analysis, and machine learning. DPI technology enables firewalls to identify and control various applications regardless of differences in ports or protocols.

The implementation process of DPI technology is shown in the figure below. There are differences in layer definitions between the OSI model and the TCP/IP model. The detection object of traditional ordinary packet inspection technology mainly focuses on the first three layers, and it is usually more concerned with the information of the "five-tuple". In contrast, DPI is an extension of traditional ordinary packet inspection in both horizontal and vertical dimensions.

4. Typical Applications of Firewall Technology in Network Security

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your journal for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

4.1. Intrusion Detection

In network security, intrusion detection and blocking are important application areas of firewall technology. By using a firewall, potential security threats can be detected and addressed in a timely manner, preventing the network from unauthorized access and malicious attacks. Its main implementation technologies are as follows:

1) Signature Detection: Uses predefined signatures or pattern-matching rules based on known intrusion behaviors and attack patterns to detect and identify mali-

cious traffic.

2) Malformed Traffic Detection: Detects abnormal traffic patterns in network transmission, such as sudden frequent access or a large number of requests to a specific port, thereby identifying potential intrusion behaviors.

3) Anomaly Behavior Detection: Establishes a normal pattern based on system and user behaviors. Once activities that deviate significantly from the normal behavior are detected, they can be determined as intrusion behaviors.

4.2. Traffic Filtering

Traffic filtering helps organizations and administrators control and manage current local area network (LAN) traffic, and protect the security and integrity of internal network resources and user data.

It monitors data packets passing through the network and filters and controls the flow direction and content of data flows according to predefined rules and policies. These rules and policies can be set based on fields such as the source IP address, destination IP address, port number, and protocol type of the data packets. For example, it can block access from known malicious IP addresses, prevent inbound connections to specific ports, or restrict the use of certain protocols in the internal network.

4.3. Security Enhancement of Virtual Private Networks (VPNs)

1) Access Control: Restricts VPN access to only authorized users or networks, preventing unauthorized users from accessing the VPN and improving network security.

2) Data Encryption Enhancement: Strengthens the data encryption function of the VPN to ensure effective protection of data during transmission. By encrypting data using encryption protocols, the firewall ensures data confidentiality and prevents the leakage of sensitive information.

3) Secure Tunnel Protection: A VPN transmits data by establishing a secure tunnel over a public network. The firewall can verify, monitor, and protect this secure tunnel, ensuring the secure and reliable transmission of data in the tunnel, intercepting potential intrusion attacks, and improving the security of the VPN.

4) Network Auditing: The firewall can also perform network auditing functions by recording and monitoring network activities occurring on the VPN, including logins, data transmissions, and resource access. This helps network administrators detect and respond to potential security threats in a timely manner, ensuring the security of the VPN.

5. Overview of Intrusion Prevention Systems (IPS)

5.1. Basic Concept

The core function of an Intrusion Prevention System (IPS) is to comprehensively detect and effectively defend against potential malicious attacks and threats in network and system activities, with real-time threat detection and active defense capabilities. This system can not only deeply monitor network traffic but also gain insights into changes in system activities, enabling the detection of both known and unknown attack behaviors [8]. Once a potential threat is detected, it triggers its defense mechanism and takes various targeted measures to immediately block or mitigate the damage caused by the attack to the target network or system. Unlike various passive defense methods, it is committed to intercepting intrusion activities and attacks outside the network boundary before they cause substantial damage, thereby maximizing network security protection. Its technical architecture is shown in the figure below:

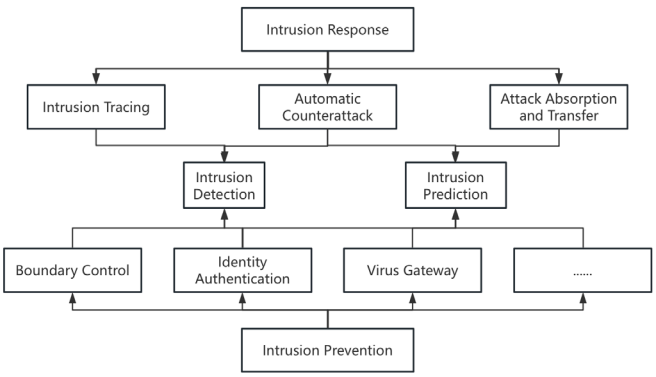

Figure 2. Architecture Diagram of Intrusion Prevention System

5.2. Core Technical Principles

The working principle of an IPS mainly lies in the real-time detection and interception of malicious attacks and threats in network traffic. The system is integrated into the network architecture and embedded in the network traffic path to inspect the data passing through. The IPS uses complex analysis algorithms and pattern-matching technologies to analyze data packets and identify abnormal activities and suspicious content. For data packets confirmed to have problems and other subsequent data packets from the same source, the IPS performs pre-filtering at the device level to effectively prevent the further spread of malicious attacks and threats. The IPS also has active protection capabilities, which can proactively detect and defend against malicious behaviors that are not explicitly listed in the blacklist but may cause damage to the network or data based on analysis and judgment.

5.3. Cooperative Relationship Between IPS and Firewall

As the first line of defense in network security, a firewall is responsible for controlling traffic entering and exiting the network. Its working principle is to filter data

packets based on preset security policies, only allowing legitimate and authorized network traffic to pass through, but it cannot identify and detect the specific content of the data payload of the packets. Its working method is relatively passive, mainly relying on a set of known rules to identify and block potential threats. It can provide effective protection against most known attacks but cannot identify and block unknown and complex attacks.

An IPS provides deeper security protection than a firewall. By real-time monitoring of network traffic and analyzing the content of the data payload of data packets, it detects and defends against potential network attacks, and has stronger initiative and defense capabilities. It can also identify and block unknown and complex attacks through methods such as behavior analysis and deep packet inspection.

In practical applications, firewalls and IPS are usually used in combination to achieve better defense effects. The firewall acts as the first line of defense to filter out a large amount of illegal and malicious traffic, and the IPS acts as the second line of defense to further conduct in-depth detection and defend against more hidden security threats.

6. Challenges and Future Trends of Network Security Defense Technologies

With the continuous iteration and development of network attack technologies, traditional network security defense technologies have become inadequate in coping with the complex network environment in the new era, and their future development faces many challenges.

6.1. Current Challenges

1. Difficulties in Zero-Day Vulnerability Defense. A zero-day attack is a network attack that exploits unknown vulnerabilities in computer systems or software applications, and these unpublicized vulnerabilities are called zero-day vulnerabilities. In recent years, zero-day attacks have become a hot issue in the field of network security. Attackers discover zero-day vulnerabilities through various means and develop malicious code and attack tools based on them. Then, they spread the malicious code to the target system through networks or physical media to infect it. After infection, attackers can obtain unauthorized system access rights to steal data or damage the system.

   Due to the lack of a known feature database for zero-day attacks, traditional IPS that rely on pattern matching cannot effectively detect them. Firewalls, on the other hand, lack behavior analysis capabilities and are difficult to identify abnormal behaviors, resulting in traditional defense technologies being unable to effectively, accurately, and efficiently respond to the above-mentioned attacks. Even next-generation firewalls (NGFW) based on signatures are difficult to cope with zero-day vulnerabilities and variant attacks. In particular, millions

of variants of vulnerabilities can currently only be identified through AI large models.

2. Inefficient Defense Against Advanced Persistent Threats (APT). APT attacks usually adopt multi-stage penetration strategies, such as implanting Trojans through spear-phishing and then using legitimate ports for lateral spread. Traditional firewalls lack behavior baseline analysis and threat chain correlation capabilities, and generally lack in-depth analysis modules, making them unable to identify abnormal behaviors in normal traffic.
3. Difficulties in Effective Detection of Encrypted Data Traffic. With the popularization of encryption technologies, statistics show that more than 90% of global network traffic has achieved encryption at different levels. Although encrypted traffic ensures the security of data transmission, it also leaves hidden channels for attackers. Attackers hide malicious code and malicious attacks in the traffic through encryption technologies, making it difficult for traditional IPS to conduct in-depth detection by parsing the content of the data payload of data packets.
4. Currently, IPS mainly detects network attacks indirectly by analyzing the characteristics of encrypted traffic, but the detection accuracy is relatively low. If the MITM (Man-in-the-Middle) decryption method is used to parse encrypted traffic, in-depth detection can be achieved, but it requires obtaining corresponding certificate authorization, which involves privacy compliance risks and is currently difficult to apply on a large scale.

7. Conclusion

This paper focuses on network security defense technologies—the first line of defense in network space security—and conducts research on two key technologies: firewalls and IPS. It comprehensively sorts out these technologies from the dimensions of concepts, principles, core technologies, and typical application scenarios.

Regarding firewall technology, this paper deeply elaborates on the characteristics of core technologies such as packet filtering, application proxy, and deep packet inspection, and clarifies its core role as the first line of defense for network boundaries in relevant fields. For IPS technology, it mainly highlights its significant advantages as an active defense barrier in identifying unknown attacks, and clarifies the complementary cooperative relationship between firewalls and IPS. The combination of the two constitutes a multi-level network security protection system.

At the same time, this paper also introduces the current challenges faced by network security defense technologies, such as zero-day vulnerabilities, APT attacks, and other complex network security risks in the new era, and demonstrates the limitations of traditional defense technologies in scenarios such as dynamic confrontation, complex environments, and unknown attacks. Against this background, AI-enabled intelligent firewalls and cloud-native distributed deployment of defense devices are

two major future trends, which can significantly improve the detection efficiency of unknown threats, and become the core idea to solve zero-day vulnerabilities and meet the security needs in complex network environments.

References

[1] International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024. Geneva: ITU Publishing.

[2] Masood, Z., Raja, M. A. Z., & Chaudhary, N. I. (2021). Fractional Dynamics of Stuxnet Virus Propagation in Industrial Control Systems. Mathematics, 2021, 9, 2160. https://doi.org/10.3390/math9172160

[3] Almohaimeed, A., & Asaduzzaman, A. (2019). A Novel Moving Target Defense Technique to Secure Communication Links in Software-Defined Networks. In 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ) (pp. 1 – 4). IEEE. https://doi.org/10.1109/MOBISECSERV.2019.8686530