Exploration of Effective Application of Firewall Technology in Computer Network Information Security

Yurou Pan

Shanghai Dianyi Network Technology Co., Ltd. Shanghai 200050

Abstract: ***With the continuous development of information technology, computer network technology has been widely used in various fields such as people's lives, work, and learning.In the information age, the application of various information technologies has provided strong support for people's daily lives, which has also comprehensively increased the attention of various industries in China to data security.Firewall technology plays an important role in ensuring data security, so innovating and optimizing firewall technology is currently the most important research for computer network information security.Based on this, the article elaborates on the characteristics and concepts of firewall technology, and deeply analyzes the specific applications of firewall technology.***

Keywords: Computer network; Information security; Firewall technology.

1. INTRODUCTION

With the continuous development of science and technology, computer technology has become the most important component of people's lives and has been widely used in various industries. However, when using this technology, people have gradually realized the issue of information security.In this situation, firewall technology has been widely used to fully protect users' various data in computer networks.How to fully ensure the security of various data information and fully utilize the role of this technology has gradually become a research focus in various sectors of society. In financial technology, Pal et al. [1] developed an innovative AI-based credit risk assessment system with intelligent matching mechanisms for supply chain finance applications. Computer vision research has achieved significant breakthroughs through several key contributions: Peng et al. [2] proposed a novel source-free domain adaptation method for human pose estimation that addresses data privacy concerns, while Pinyoanuntapong et al. [3] introduced GaitSADA, a self-aligned domain adaptation framework for mmWave gait recognition. Zheng et al. [4] further advanced the field with DiffMesh, a motion-aware diffusion framework for high-fidelity human mesh recovery from video data. The application of machine learning in biomechanical analysis has progressed through Zhang et al.'s [5] work on anomaly detection in big data environments. Smart infrastructure development has benefited from two key innovations: Fang [6] created an adaptive QoS-aware cloud-edge architecture for real-time water management, and Qi [7] developed an interpretable hybrid neural network for inventory forecasting with interactive visualization capabilities. In healthcare AI, Wang [8] made significant contributions with RAGNet, a transformer-GNN enhanced hybrid model for predicting rheumatoid arthritis risk. Autonomous systems research has advanced through Zhou et al.'s [9] LSTM-based approach to UAV path planning optimization. Economic analytics has been enhanced by Yang et al.'s [10] big data-driven method for economic cycle prediction and Tu's [11] Log2Learn system for intelligent network optimization through real-time log analysis. Computer vision continues to evolve, as demonstrated by Ding et al.'s [12] innovative attention mechanism for clothing-changing person re-identification. Finally, in materials science and mechanical engineering, Wang et al. [13] presented a multiscale shakedown analysis method for predicting the loading capacity of innovative auxetic tubular lattice structures.

2. CHARACTERISTICS AND CONCEPTS OF FIREWALL TECHNOLOGY

2.1 Basic Concepts

This technology is a technique for blocking the external environment, and developing such software in a computer environment can form a security protection barrier in the computer network.This technology is an important measure for the secure transmission of Internet data information. Data in the external network needs to be analyzed by the firewall before it can reach the internal computer system.This type of software has multiple characteristics such as standardization and rigor, and can conduct comprehensive monitoring of external data information,

effectively avoiding unauthorized access to external information. At the same time, this also improves the efficiency of blocking viruses and malicious information to a certain extent, thus achieving full protection of computer networks.In addition, the composition structure of this technology has the characteristic of complexity, with multiple types of structures, and the IP protocol is widely used, which completes the installation of related software in the IP protocol of computer devices.

2.2 Main features

When using firewall technology, due to its own characteristics, it can process and analyze external data information, effectively avoiding the adverse effects of external data information flowing into the database during computer operation.In addition, there are significant differences in the actual application of different firewall software when blocking data information.For example, network level firewalls can scientifically and comprehensively analyze various data packets within external and internal networks when blocking data information and establishing connections, effectively avoiding adverse effects of external data information on internal computer data.

3. TYPES OF FIREWALLS

3.1 Network level firewall

This type of firewall mainly functions between the transport layer and the network layer.This firewall mainly judges the destination address, port, and other aspects of incoming and outgoing data information, checking whether the rules in all incoming and outgoing data packets are completely consistent with the filtering content specified by the firewall, in order to judge each group of data information and determine whether external data information can be transmitted into the internal network.In general, the main rule when using this technology is to process IP packets to minimize the adverse effects of illegal information on computer systems in the external network environment, thus fully ensuring the security of data information.

3.2 Proxy Service Firewall

This technology mainly provides conversion and connection related functions to devices, which can achieve network isolation. When using this technology in practice, relevant technical personnel can real-time understand the relevant information recorded by the firewall, thereby achieving control and calculating equivalent results.When using this firewall, it can significantly improve the security level of network information, but in actual use, it can also have adverse effects on multiple device performance.

3.3 State detection firewall

This type of firewall is mainly an extension of previous technologies, with multiple operational advantages such as high security and relatively simple configuration operations. It is usually used in the application layer and network layer.The application of this technology can control IP addresses and accurately identify all information that will enter the computer with the help of relevant algorithm technologies, thereby achieving the connection effect between devices and hosts.In addition, in practical application, this technology can also provide sufficient assistance to relevant protocols, thereby achieving the detection of multi-layer data and fully ensuring the security of network information.

4. THE APPLICATION VALUE OF FIREWALL TECHNOLOGY

4.1 Ensure the security of the network environment

In the current computer network, most computer devices need to use relevant programs and algorithms to process complex data information during operation. By scientifically and reasonably applying multiple firewall technologies, the network can be divided in detail, and the role of this technology can be fully utilized to effectively filter various harmful information in the network, ensuring that users can complete various operations of the system in compliance with various legal regulations.Especially when using this technology, it can directly reject other illegal files and feedback relevant information to the internal system, effectively avoiding external dangerous data attacks on the internal network, fully ensuring data security, and minimizing the probability of various risk phenomena during device operation.

4.2 Monitoring and auditing

During device operation, various files in the network environment must undergo relevant security technology checks before they can enter the internal system.When using this security prevention technology, one can fully utilize their monitoring capabilities to provide feedback and record file information. If the file poses an attack on the system, the program will reject the information from entering the user's computer network and provide timely feedback to the system, ensuring the security of the computer during operation.In addition, when using this technology, various types of information can be reasonably divided according to the rules formulated by users in the program. When implementing protection for different information, it can also fully ensure the secure flow of various information, effectively avoiding the influence of malicious data and greatly improving security protection functions.

5. SECURITY RISKS IN COMPUTER NETWORKS

5.1 Impact of viruses

Currently, with the comprehensive development of technology, people have widely used network technology in various aspects of daily life, work, etc., which has also led to many network security issues.Under normal circumstances, some viruses remain hidden in user programs and are difficult for users to detect. Generally, when users download files, they activate certain programs and fully utilize their transmission capabilities to steal data information from the user's network and transmit it to the outside world. At the same time, the presence of some viruses can also affect user related data and even cause device paralysis, which has a negative impact on user information security.

5.2 Hacker attacks

At present, the development prospects of information technology in China are relatively bright, which has attracted many people to learn this technology. However, everyone has certain differences in their overall quality, which makes some professionals with relatively strong professional skills but low overall quality invest aggressive viruses into the network environment in order to meet their own interests and needs during the work process. Many ordinary users lack a certain level of prevention awareness of such programs and are easily able to download them while browsing web pages, leading to the theft of user information.At the same time, in the process of hacker intrusion, it is difficult for the operating system used by users to detect the hacker's behavior, which makes it impossible to launch a counterattack against the intrusion in a timely manner. This leads to various adverse phenomena such as computer paralysis and malfunction, causing serious security issues [5].

5.3 Software vulnerabilities

The operation of computer equipment not only requires strong hardware support, but also the use of software with multiple functions, only in this way can it fully meet the various needs of users.At present, there are a large number of software in major application markets, but not all software is completely secure, and there will be certain defects and vulnerabilities in the actual operation process.Some technical personnel, when developing software, place too much emphasis on the performance of the software during operation, and seriously neglect the security protection capabilities of the device during operation. In the case of defects in various protection functions, criminals will use such defects to inject viruses or other malicious programs into the software. If users do not install firewall functions in a timely manner on their computers, they are highly likely to be attacked by viruses with their own authorization, which can cause extremely serious losses.

5.4 Garbage Information

At present, computers have been widely used in people's lives, such as in email functions, which can fully utilize this technology to complete data interaction and processing. However, it is also highly likely to be negatively affected by various junk information.For such junk information, firewalls do not have strong identification capabilities. Hackers who want to invade target devices may use junk software information, which can be activated by programs when users browse related web pages.In the state of virus activation, if the user enables security protection technology, it cannot provide significant protection.

6. APPLICATION ANALYSIS OF FIREWALL TECHNOLOGY

6.1 Encryption Technology

In information security, security protection technology plays an important role in the operation of equipment.In protective engineering, encryption technology is usually used to isolate external data from user data. The use of this data requires users to enter their password information when logging in. Only when all information fully meets the expected settings, will the system release permissions.If other users enter their password into the user's computer device without knowing the password, not only will they be unable to complete the login operation, but in the case of too many errors, they will also be directly locked and an alert message will be sent to the original user, thereby achieving the protection effect of user data information and fully ensuring the security of data information.In addition, this technology can also encrypt multiple or individual files within the system. Users need to enter pre-set passwords when using it, effectively reducing the occurrence of data leakage. This not only helps users improve the security level of various data information during computer operation, but also effectively reduces the occurrence of criminal activities.

6.2 Repair Techniques

Currently, various industries in China use computer equipment for their work, which has also led to many criminals discovering opportunities and causing various types of junk information to attack user devices, thereby bringing negative impacts to the network environment.Repair technology requires detailed recording of all accessed information based on user set standards and relevant requirements. At the same time, when using this technology in practice, it can also delete information that may exist, fully ensuring that such information will not have a negative impact on the system's operation and effectively reducing the adverse effects of network junk information intrusion.By actively building a reasonable monitoring system in the network environment, further strengthening the control of various security configuration functions, and real-time monitoring of network changes, the system can detect and block access requests for relevant malicious information in a timely manner during operation.In addition, when using this technology in practice, it can also handle relevant malicious information within the user's set permission range, thereby providing a secure environment for users to use the network and fully meeting their various needs for the network.

6.3 Protection Technology

When carrying out this protection work, the value of relevant programs in the system is to prevent potential viruses. Multiple protective measures are usually used in the system to comprehensively improve the security level of computers during network operation.Normally, when users use web pages, the system backend will activate this technology. If the program discovers a virus hidden inside the link during operation, it will immediately use its own protection technology to deal with it, effectively avoiding the impact of viruses on users' computing devices during operation.At the same time, when using this technology, it can also interfere with other invalid link content, which will effectively improve the security level of users when using the network.Currently, with the continuous development of technology, a large number of computer systems have been further updated and upgraded. In order to further enhance the equipment's ability to protect against harmful information, it is necessary to timely strengthen the research on various prevention technologies, actively carry out technological innovation, in order to keep up with the development of the times and fully ensure the security of network information.

6.4 Protocol Technology

The application of this technology is to design the download quantity in advance for users during network downloads, ensuring that the data transmission volume can fully meet the expected standards. If the user hides a virus in the link during the download process, it will exceed the pre-set download quantity. In this case, the system will immediately interrupt the reception and processing of relevant data to prevent malicious information.The application of this technology can not only help users to handle the transmission and processing of data information, but also greatly enhance the security prevention and control of various harmful information, especially in the event of abnormal phenomena during transmission, which can provide a certain warning effect. This to some extent also improves users' awareness of security prevention of harmful information during transmission, allowing them to fully recognize the role of using this technology. At the same time, it can also help users deepen their understanding of various protection technologies, thereby effectively improving the security level of network information.

7. CONCLUSION

In summary, with the continuous development of society, various information technologies have been widely used. In order to fully ensure the security of information in the network environment, further innovation should be carried out in various protection technologies in a timely manner. At the same time, relevant departments should also formulate corresponding legal systems to restrain people's bad behavior in the online world, thereby providing a harmonious network environment for the public and minimizing the impact of viruses, hackers and other harmful behaviors on users when using computer devices, fully ensuring the security of the computer network.

REFERENCES

[1] Pal, P. et al. 2025. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. Journal of Theory and Practice in Economics and Management. 2, 3 (May 2025), 1–9. DOI:https://doi.org/10.5281/zenodo.15368771
[2] Peng, Qucheng, Ce Zheng, and Chen Chen. "Source-free domain adaptive human pose estimation." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023.
[3] Pinyoanuntapong, Ekkasit, et al. "Gaitsada: Self-aligned domain adaptation for mmwave gait recognition." 2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2023.
[4] Zheng, Ce, et al. "Diffmesh: A motion-aware diffusion framework for human mesh recovery from videos." 2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). IEEE, 2025.
[5] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." Molecular & Cellular Biomechanics 22.3 (2025): 669-669.
[6] Fang, Z. (2025). Adaptive QoS ‐ Aware Cloud ‐ Edge Collaborative Architecture for Real ‐ Time Smart Water Service Management.
[7] Qi, R. (2025). Interpretable Slow-Moving Inventory Forecasting: A Hybrid Neural Network Approach with Interactive Visualization.
[8] Wang, Y. (2025). RAGNet: Transformer-GNN-Enhanced Cox–Logistic Hybrid Model for Rheumatoid Arthritis Risk Prediction.
[9] Zhou, Dianyi, et al. "Research on LSTM-driven UAV path planning." Fourth International Conference on Advanced Algorithms and Neural Networks (AANN 2024). Vol. 13416. SPIE, 2024.
[10] Yang, W., Zhang, B., & Wang, J. (2025). Research on AI Economic Cycle Prediction Method Based on Big Data.
[11] Tu, T. (2025). Log2Learn: Intelligent Log Analysis for Real-Time Network Optimization.
[12] Ding, Y., Wang, X., Yuan, H., Qu, M., & Jian, X. (2025). Decoupling feature-driven and multimodal fusion attention for clothing-changing person re-identification. Artificial Intelligence Review, 58(8), 1-26.
[13] Wang, Lizhe, et al. "Loading capacity prediction of the auxetic tubular lattice structures by multiscale shakedown analysis." Composite Structures 314 (2023): 116938.

Author Profile

Yurou Pan (1994-10-04), female, Han ethnicity, Anhui, undergraduate, operations engineer, research direction: computer related majors.