Research on Application of Firewall Technology in Computer Network Security Based on Data Mining

Chenglong Du

Guangdong University of Science and Technology, Dongguan City, Guangdong Province, 523073, China

179074904@qq.com

Keywords: Data Mining, Firewall, Computer Network

Abstract: the Development of Computer Technology Has Greatly Promoted Social Progress. with the Continuous Popularization of Computer Technology, It Brings Convenience to People and Also Threatens People's Information Security. People's Dependence on the Network is Increasing Day by Day, and the Security of Computer Network Has Attracted Extensivel of Security Protection, But Also Creates a Safe and Reliable Operating Environment. Firewall Technology is an Effective Way to Maintain Computer Network Security, Making Computer Network Operation More Secure and Reliable. by Applying Firewall Technology in the Computer Network, the Firewall Settings Are Optimized, and the Application Advantages of the Firewall Technology Are Fully Utilized to Ensure the Security of the Computer Network.

1. Introduction

In the Information Age, Computer Networks Have Become an Indispensable Part of People's Lives and Work. At the Same Time, Computer Network Information Security Has Become the Most Concerned Issue [1]. Firewall Technology Can Effectively Avoid Various Infringements in Network Security and Ensure Network Information Security. It Embodies the Practical Role of Firewall Technology in Computer Network Security, and More Importantly, It Uses Firewall Technology to Maintain the Security of Computer Network and Strengthen the Reliability Control of Computer Network [2]. the Protection Principle of the Firewall is Information Isolation, Forming a Protective Barrier in the Process of Information Interaction, Filtering Dangerous Information on the One Hand, Improving the Security of Computer Network Protection on the Other Hand, and Strengthening the Defense Capability of the Computer Network System [3]. Prevent the Implantation of Viruses or Malicious Links, and Comprehensively Protect the Security of Computer Networks. All-Round Protection of the Operation of the Computer Network, Optimization of the Computer Network Environment, Reflecting the Practical Value of Firewall Technology, to Meet the Needs of Computer Network Security [4].

Computer Information Technology is Now Widely Used in All Kinds of Industrial Fields in Our Society. under the Synchronous Situation, More and More Strict Standard Demands Are Put Forward for the Quality of Network Security Maintenance Work [5]. among Them, the Network Security Problem Has Become the Focus of Concern for the Vast Number of Network Users and Researchers Due to Its Wide Range of Users, Serious Consequences and High Prevention Difficulty[6]. There Are Many Computer Network Security Protection Technologies, among Which Firewall Technology is the Most Widely Used. a Firewall is a Combination of a Series of Components Set Up between Different Networks or Network Security Domains [7]. It is the Only Gateway for Information between Different Networks or Network Security Domains. It Can Control the Flow of Information to and from the Network According to the Security Policy of the Enterprise, and It Has Strong Anti-Attack Capability [8]. There is an Inseparable Relationship between Computer Network Security and Firewall Technology. Firewall Technology Develops with the Demand of Computer Networks. under the Promotion of Network Security, Firewall Technology Reflects the Advantages of Security Protection [9].

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/ISMHI.2019.022

2. Firewall Technology in Computer Network Security

2.1 Overview of Firewall Technology

Firewall is a network protection and isolation technology. It is a system or a group of systems, including hardware and software, that execute access control policies between two networks. It is a passive defense control security technology, and its working method is to set up a separation wall between the public network and the private network, thus preventing illegal access to information resources and the entry of unauthorized users [10]. According to the protection principle and working mechanism of firewalls, firewalls can be roughly divided into the following two categories: packet filtering type and proxy service type. Different firewall types have different protection performance. Firewall technology is indeed widely used in computer network security, reflecting the high efficiency value of firewall technology. The proxy technology in the firewall has certain peculiarities. It can play a controlling role in various modules running on the computer network, and always reflects the powerful state. This technology plays a major role in the segmentation of the internal network and the external network, so as to eliminate the phenomenon of internal and external confusion, so the agency technology is also facing technical pressure in realizing the application value.

The firewall technology combines the hardware and software in the system to complete the filtering and screening of bad information. Once the bad information is filtered out, the firewall will intercept it in time to protect the computer network security. Only data flows that are consistent with firewall rules can pass through the firewall, and the firewall itself must have strong anti-attack and immunity. Users' various operations in the computer network environment will be recorded by the firewall, which uses real-time monitoring to effectively identify network information, thus realizing the security protection of user information data. Firewall technology can put forward available protection measures according to potential network security risks, avoid risk problems, protect the operation of computer network in all aspects, and optimize the computer network environment. The firewall will record the related information in detail to ensure that the specific sources of all kinds of information are properly verified and analyzed. As for, the status of some interactive information in the network system will be clarified as soon as possible so as to avoid the large-scale breeding of external attacks.

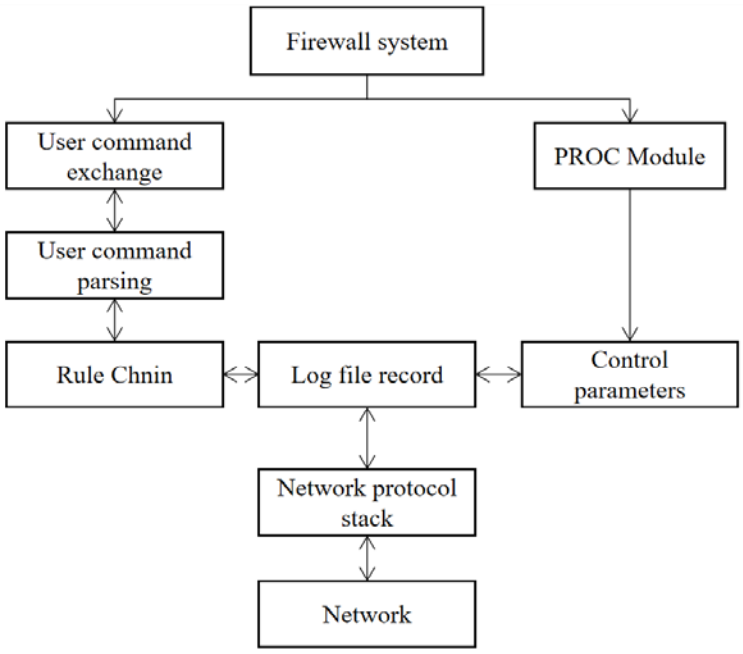

Fig.1 Firewall Network Data Processing Flow

2.2 Application of Firewall Technology in Computer Network Security

In the computer network security, the firewall can not only ensure the security of the server data, but also ensure the normal and safe operation of the computer network system. If a border router is

set in the LAN, the firewall can be combined with the filtering function of the router to focus on the intranet protection and firewall connection. The firewall technology in computer network security is based on encryption technology. In the early stage of sending messages in the computer network, the information encryption behavior is performed in advance, and the information transmission of the computer network is guaranteed, and the password is protected. Different users have different requirements for network services, and their chosen application proxy firewall has different isolation effects, so the security policies of application proxy firewall are also different. Access strategy is the application core of firewall technology, which occupies a dominant position in computer network security. Firewall technology plans access strategy according to the actual operation of computer network, so as to create a secure environment.

Composite technology in firewall is an important technology with comprehensive protection performance. It combines the advantages of packet filtering and proxy technology, fully embodies a more stable and reliable protection form, and effectively makes up for firewall defects. Authentication technology of computer network firewall refers to the operation of security protection by authorization and identity authentication in the process of safe transmission of computer network. The security scanning technology cooperates with the firewall and the intrusion detection system to effectively improve the security of the network. Through scanning, network administrators can understand the security configuration of the network and the application services running, identify security vulnerabilities in a timely manner, and objectively evaluate the network network level. The application proxy firewall itself also has the function of processing information. When bad information is found between the intranet and the extranet, it can be effectively isolated so that it cannot be circulated between the intranet and the extranet.

3. Firewall Technology Based on Data Mining

3.1 Data Mining Technology

With the rapid development of computer technology and database technology as well as the extensive application of database management system, information has accumulated over the years, forming a massive information base. How to extract useful knowledge from massive data has become a top priority. Data mining is a data processing technology developed to meet this need and is a key step in knowledge discovery. Data mining is to extract or “mine” knowledge. At present, data mining can be defined from statistics, database and machine learning. Data mining originates from the decision support problems faced by large retailers. It is the process of extracting hidden and potentially useful information and knowledge from a large amount of random data. The data description, organization and storage methods are different in different databases, and the data mining database is divided into relational, transactional, multimedia and heterogeneous databases.

From a database perspective, data mining is the process of discovering interesting knowledge from large amounts of data stored in databases or other information repositories. From a machine learning perspective, data mining is defined as extracting implicit, apparently unknown, and potentially useful information from the data. Data mining is a cross-disciplinary field that includes database technology, statistics, machine learning, visualization, and information science. Database type diversity, many data sets include complex data types such as relational data, semi-structured data, unstructured data, hypertext data, and multimedia data. The efficiency and scalability of data mining algorithms mean that in order to effectively extract useful knowledge from a large number of data in the database, knowledge discovery algorithms must be effective and scalable. The main functions of data mining include automatic prediction of trends and behaviors, association analysis, clustering, concept description and deviation detection. Compared with the traditional statistical methods, the data mining method has the advantages that it can discover unknown knowledge and laws from the data, and has the advantages of automatic and fast analysis process.

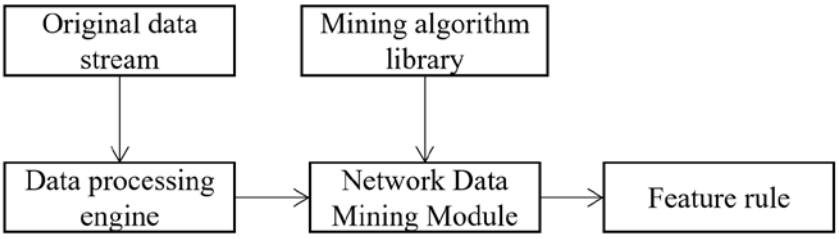

Fig.2 The Process of Establishing Feature Rules by Data Mining Technology

3.2 Application Value of Firewall Technology

Firewall technology is widely used in computer network security, reflecting the high value of firewall technology. The application value of firewall technology in computer network security mainly includes the application value of filtering technology, agent technology, detection technology and protocol technology. The firewall technology strictly plans the execution order according to the policy table. Therefore, the policy table restricts the protection behavior of the firewall technology, and the efficiency of the network security protection is largely provided. The quarantine area of firewall technology belongs to a separate local area network, which can become part of the internal network of the computer, but more importantly, it protects the information security inside the network server, and causes the computer to be in a safe and stable operating environment. The application of firewall in computer network security is mainly in packet filtering, deep detection, application gateway and distributed firewall. In computer network security, firewall technology also includes security service configuration, composite technology, application of access strategy and application of intrusion detection methods.

Among firewall application technologies, intrusion detection is an important application function in firewall technology. Through analyzing the stability and effectiveness of computer defense system, firewall uses relatively static defense methods to make up for the deficiencies of detection system. The application of data mining technology in firewall technology is mainly to discover the rules and patterns of intrusion, which are combined with pattern matching detection methods and used for anomaly detection to find out the normal behavior of users and create the normal behavior model of users. The firewall technology based on data mining is mainly intelligent and highly automated. The purpose of data mining technology is to establish a systematic and automated method for creating intrusion detection systems. This method uses a data-centric viewpoint and treats firewall technology as a data analysis process. Applying data mining to firewall technology can automatically generate accurate and applicable detection models from a large amount of audit data, making firewall technology suitable for any computing environment.

4. Conclusion

The development of firewall technology has a long history. The traditional knowledge-based firewall technology can no longer meet the needs of the rapid development of the network. It is appropriate and necessary to introduce data mining technology into firewall technology, which can improve the effectiveness, scalability and adaptability of firewall technology. Effectively respond to network information attacks and maintain network security. It is necessary to continuously improve firewall technology to overcome the existing drawbacks of firewalls and cope with network security under the new situation. Firewall technology is supported by advanced technology models and has obvious advantages in preventing information leakage and illegal user intrusion. On the basis of the computer network, optimize the use of firewall technology to ensure that the firewall technology can reflect the security protection actions in the computer network. Specifically, firewall technology plays a very important guiding role in the current computer network security management activities in our country. Applying data mining technology to firewall system can well solve the problem of massive data processing and mine unknown attack features, which is of great help to firewall system in finding unknown types of attacks.

References

[1] Bhardwaj, A.K., Singh, M. (2015). Data mining-based integrated network traffic visualization framework for threat detection. Neural Computing and Applications, vol. 26, no. 1, pp. 117-130.

[2] Xu, Hao, J. (2015). The Data Mining Application Research and Resolution Based on Network Information Retrieval. Applied Mechanics and Materials, no. 713-715, pp. 2491-2494.

[3] Zhou, W. (2016). Research and Application of Data Mining Algorithm Based on Fuzzy Neural Network for Nonlinear Problems in Large Data Environment. Journal of Computational & Theoretical Nanoscience, vol. 13, no. 7, pp. 4735-4738.

[4] Lee, S., Levanti, K., Kim, H.S. (2014). Network monitoring: Present and future. Computer Networks, vol. 65, no. 2, pp. 84-98.

[5] Vanikalyani, G., Avinash, P., Pandarinath, P., et al. (2014). Cross-Domain Search for Policy Anomalies in Firewall. International Journal of Computer Applications, vol. 104, no. 6, pp. 20-24.

[6] Ma Z. (2014). Android Application Install-time Permission Validation and Run-time Malicious Pattern Detection. Personal & Ubiquitous Computing, vol. 18, no. 8, pp. 1963-1976.

[7] Bao, N., Wang, Q., Jia, Y.J. (2017). Research of Characteristics of Stimulation Methods and Application of Acupoint in Auricular Needle Therapy Based on Data Mining. Zhen Ci Yan Jiu, vol, 42, no. 4, pp. 372-376.

[8] Suto, K., Nishiyama, H., Kato, N., et al. (2014). An Overlay-Based Data Mining Architecture Tolerant to Physical Network Disruptions. IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 3, pp. 292-301.

[9] Suto, K., Nishiyama, H., Kato, N., et al. (2014). An Overlay-Based Data Mining Architecture Tolerant to Physical Network Disruptions. IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 3, pp. 292-301.

[10] Wang, S.Q, Chen, H.Y. (2014). Research on ASIC Firewall Based on State Detection Technology. Applied Mechanics and Materials, no. 644-650, pp. 3283-3286.