Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Research on Computer Network Security Based on Firewall Technology

To cite this article: Xinzhou He 2021 *J. Phys.: Conf. Ser.* **1744** 042037

View the article online for updates and enhancements.

ECS Toyota Young Investigator Fellowship
ECS TOYOTA
For young professionals and scholars pursuing research in batteries, fuel cells and hydrogen, and future sustainable technologies.
At least one $50,000 fellowship is available annually.
More than $1.4 million awarded since 2015!
Application deadline: January 31, 2023
Learn more. Apply today!

Research on Computer Network Security Based on Firewall Technology

Xinzhou He[1,*]

[1]Changjiang Polytechnic, Wuhan, Hubei, China, 430074

*Corresponding author e-mail: 343221@cjxy.edu.cn

Abstract. In the era of rapid network development. Its security has attracted much attention. In order to improve the security of computer network. Firewall as one of the most effective technologies. His development has also attracted people's attention. This article will further analyse firewall technology. I hope you can get some inspiration from it.

Keywords: Firewall Technology, Computer Network Security

1. Basic concept of firewall

Firewall is a security defense tool applied in the field of computer network security. It's used between the intranet and the extranet. The former is recognized as a secure network. The latter is identified as a relatively less secure network. The firewall consists of software and hardware. Connectivity between the intranet and the extranet must and can only pass through the firewall. Firewall is the basic service means to guarantee network information security. It's very protective. At the same time, the information flow in and out of the network can be released and intercepted by receiving the security policy control (permission, rejection, monitoring) and so on. The firewall is an analyzer. Be able to analyze the information flow through. And a separator, you can filter the analyzed information flow. It's also a limiter, restricting the flow of information that is screened as unsafe. Denying access to the intranet, authorize secure information flow into the intranet. Authorize secure information flow into the intranet. Therefore, it can effectively protect network security. Ensure the security of the intranet. Firewalls used to be partitions in buildings to prevent fire from spreading. Here is extended to protect the internal network security of a protective wall[1].

From a physical point of view. The physical implementation of each firewall can be different. But it is usually a combination of a set of hardware devices (routers, hosts) and software: Firewall is essentially a protective device. Be used to protect the reputation of network data, resources and users.

2. Working principle and characteristics of firewall

The working principle of a firewall. Fire walls work according to pre-defined configurations and rules. Monitor all data flows through the firewall. Only authorized data is allowed. Also records the relevant connection source, the communication display provided by the server and any attempt to break in. To facilitate administrator monitoring and tracking[2].

Figure 1. A wide connection to the Internet.

The characteristics of a firewall. A good firewall should have the following attributes: One is that all information must pass through the firewall; Secondly only in the security policy of the protected network is it allowed to pass through the firewall; The third is to record the information content and activities through the firewall; the fourth is to detect and alarm network attacks, Fourthly, the firewall itself is immune to all kinds of attacks.

3. Main functions of firewall

Dynamic packet filtering technology. It also became a state detection technology. Capable of intercepting packets through a firewall. Extracting Application Layer Information. To decide whether to refuse or allow, depending on the security of the information. The purpose of dynamic security network control can be realized. Firewalls can dynamically manage information flows through their ports. The premise is that you need to connect[3].

Control unsafe services. Firewalls can effectively control insecure services. Set up the policy of data entry and exit between trust domain and distrust domain in advance. You can deny unsafe services outside the intranet. Rule plans can also be defined. Automatically start and close when a startup and shutdown policy is required. It not only greatly increases the security of the intranet, but also has flexibility.

Figure 2. A global connection to the Internet.

Centralized security protection. Firewalls can centralize all the software needed to protect the intranet. Including all software changes and additions. Like an electronic password. Passwords and authentication. These security issues can be managed centrally by firewalls. It has high efficiency, it's easy to operate. Only the firewall as the center of the security scheme configuration can achieve centralized security protection. Compared to spreading security issues across every host. Centralized security management by firewalls is more efficient and economical. Strengthen the access control of network system. Firewalls can set up external network access services to the intranet. Access control, for example, specific services that are critical to network security can be shielded from external networks, make it inaccessible. For other services with less network security. The service allows external network access. The above points are some of the main protection functions that firewall should have. With the development of technology. Firewall protection features are more diversified. Reasonable application and management of firewall function can really play a protective role of fire wall.

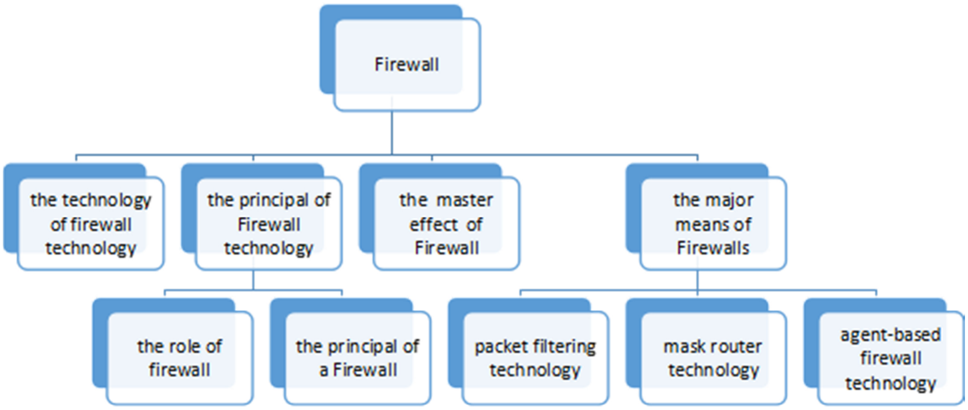
Firewall
the technology of firewall technology
the principal of Firewall technology
the master effect of Firewall
the major means of Firewalls
the role of firewall
the principal of a Firewall
packet filtering technology
mask router technology
agent-based firewall technology

Figure 3. The principle of computer security of firewall technology.

4. Means of firewall technology

4.1. Composite technology

Composite technology is one of the effective methods of comprehensive utilization of firewall. Composite technology is one of the effective methods of comprehensive utilization of firewall. Help to provide more stable, reliable and secure protective measures, reducing the malpractice in the use of firewalls. The composite ability of firewall technology is becoming more and more mature. At present, the composite ability of firewall technology is becoming more and more mature. The concentration of firewall technology embodies the characteristics of diversity, is a collection of anti-virus software, firewalls and alarm systems of a comprehensive technology. In the Internet, technology power is becoming more and more perfect today. Whether individual or enterprise users[4]. Good results can be achieved by installing firewalls. Ensure the safety of the use of computers and the Internet. Meanwhile, by installing special firewall software systems on computer networks, can achieve multiple layers of different defense mechanisms. Not only can the normal use of users have a good monitoring. At the same time, it can also protect the malicious attack of the external network. Composite technology can provide multiple encryption and protection. To have normal access, you have to go through multiple ports. So achieved a good purpose of protection. In addition, firewall composite technology can also actively hide the internal situation of the compute. Avoid malicious access by hackers or viruses，reduce the chance of being visited to improve the overall level of protection.

4.2. Use access policies

First, through the use of firewalls, the use of the Internet can be divided into intranet and extranet. Planning two different uses, reference paths. Achieve good data transmission, access and interaction security purposes. Second, firewall technology can be used before entering the system. Have a preliminary understanding of each other's systems and circumstances. To operate without exception, ensure safety factor. Finally, computer networks and access policies use different forms of protection. Access policies are based on the security requirements of computer networks. Optimizing firewall adjustments, in order to improve the security of computer network protection. Besides, based on the strategy sheet, access policy, detailed recording of all activities of the access policy. This table is used as the execution order to improve the efficiency of computer network security protection[5].

Intrusion detection is one of the most important functions in computer internet usage. The dynamic detection system can improve the stability of the computer protection system. To make up for the current failure of computers to check their own departments and external information. Firewall and computer antivirus software are combined. The ability to monitor computers.

Through the diversified computer way to complete the computer network security hidden trouble investigation.in all directions. Through the diversified computer way to complete the computer network security hidden trouble investigation[6].Meanwhile, When users use firewall software, in addition to passive detection, you can also use software for independent intrusion detection on a regular basis. Some viruses and Trojans lurk in computer systems for a certain period. The active detection can reduce the probability of this accident and improve the security of users. Reducing the chance of being visited to improve the overall level of protection. Hackers can be divided into non-destructive attacks and destructive attacks. Non-destructive attacks - in order to disrupt the operation of the system. A denial-of-service attack or information bomb is usually used; a destructive attack is an intrusion into someone else's computer system. The purpose of stealing confidential information of the system and destroying the data of the target system. Here are a few common attacks:

4.2.1. Backdoor program

Because programmers in the design of some complex functions of the program, the general use of modular programming ideas. Generally speaking after the completion of the program to remove the back door of each module. However, sometimes the back doors are not removed for various reasons, and some people with ulterior motives use exhaustive search methods to find and use these back doors, then enter the system and launch an attack.

4.2.2. Denial attack

There are many kinds of denial-of-service attacks. Their basic principle is to take advantage of the vulnerabilities of Windows operating system or TCP/IP protocol and send a large number of specific packets to the target host, which makes the host unable to provide normal services. At this point, the server has to wait - it doesn't close the connection until. The attacker's constant sending of such packets eventually caused the server to refuse to provide services because of overload.

4.2.3. Deception attack

Deception attack can be divided into IP deception, DNS deception, WEB deception. Below mainly explains the principle and process of IP deception attack. IP spoofing is a complex attack technique suitable for TCP/IP environments. First, the target host is selected; secondly, the trust mode is found and the host trusted by the target host is found. For IP deception, the trusted host is incapacitated. When the connection is successful, a system backdoor is placed for unauthorized operation.

4.2.4. Scan attack

Scanners are programs that automatically detect remote or local host security vulnerabilities [3] .Using scanners, hackers can discover the distribution of various TCP ports in remote servers without leaving a trace and can also collect a lot of useful information about the target host (for example, whether to log in anonymously, whether there is a writable FTP directory, whether TELNET services can be used, etc.

5. Concluding remarks

In short, through the above research, further improve the understanding of computer network firewall technology. As a technician, we should constantly carry out practical exploration and effectively summarize more scientific firewall technology in order to continuously improve the level of computer network security. Hope to combine the above elaboration, can provide effective reference for relevant technical personnel.

References

[1] Tang Xiao bin. Computer Network Security Research [J] Based on Firewall Technology Digital World, 2018(07): 38.

[2] Gu Kui ye, Liu Fa sheng. Analysis of Computer Network Security Governance and Firewall Technology [J].] in China Electronic Testing, 2016(22): 63-64.

[3] Wang Qiangqiang. Analysis on Application of Firewall-based Technology in Computer Security Construction [J] of China Digital World, 2019(08): 244.

[4] Road race. Countermeasure Research on Strengthening Computer Network Security Management in the Background of E-Commerce, SME Management and Technology (Mid-Year Journal), 2020 (08): 39-40.

[5] Peng Zhen yu. Based on computer network security and preventive countermeasures research, cyber security technology and application, 2020 (08): 3-4.

[6] Zhang Rui computer Network Security and Firewall Technology Analysis [J] Computer Knowledge and Technology, 2012(24): 5787-5788.