On the Relationship between Computer Firewall Technology and Network Security

Lan Jiang$^{1*}$

$^1$Wuhan Polytechnic, Wuhan, Hubei, China, 430074

*Corresponding author e-mail: 89788677@wtc.edu.cn

Abstract. The rapid development of The Internet brings convenience to people, but also brings some problems to people. The danger of information pollution and destruction is becoming more and more serious, in order to reduce the loss of confidence and security to people. People have studied firewall technology. The use of firewall technology provides a reliable guarantee for protecting the security of data and resources. This paper mainly discusses the application of firewall technology in computer network security from the aspects of network security, the general situation and types of firewall$^1$.

Keywords: Firewall Technology, Network Security, The Computer

1. The network security issues
With the rapid development of information technology, Internet technology has penetrated into many fields. The development of computer network technology not only changes people's life style and concept, but also has a certain influence on the ideology and appearance of the society. Virus attack, hacker attack and other serious impact on people's normal work and life. The causes of network security problems are people's careless mistakes and people's deliberate attacks on the network. The lack of security awareness or the inadvertent disclosure of information to others during the operation of operators can lead to network security threats. In addition, artificial malicious attack is also an important factor threatening network security, and it is also the biggest problem in network security. Therefore, whether it is the attack of the computer recidivism or the malicious attack of the rival party, it will pose a certain threat to the computer network security.

2. The contents and problems of firewall technology in computer network security
In the process of using the computer, in order to ensure the integrity and security of the data stored in the computer, the user is protected from tampering caused by external attacks. In order to keep the network operating environment in a safe and stable environment, isolation techniques similar to security barrier classes are needed. This "firewall" technology provides the means. Firewall technology can not only the access permissions between the network and the content control plays a good barrier role. At the same time, it also prevents the occurrence of some illegal behaviors and reduces the probability of harm to ordinary users due to hackers' illegal access to network information resources and other illegal behaviors. Although the computer network has brought great convenience
to people, but the network security problem is increasingly serious, such as the constant exposure of precision telecommunications fraud, Snowden prism, panda burning incense virus attack. The threats and challenges facing terminal equipment are increasing day by day. Therefore, it is very important to strengthen network security and firewall construction\(^2\).

There are also some problems in the current use of computer network technology, which are summarized as follows:

**Table 1.** Computer network technology problems.

| Data threat                  | When data is running, some vulnerabilities often appear. Attackers exploit vulnerabilities in the computer and start to invade the weak parts of the computer network. |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External force damage        | The problem of external damage in the computer can also adversely affect the operation of the data. The current external data destruction mainly refers to the use of mail virus, website virus way to attack the user's computer |
| Threatening issues in the network environment | Generally speaking, the closer the sharing is in the network environment, the more frequent and intense the attacks will be.                                                                                                                                 |

3. Specific analysis and application of firewall technology

3.1. Computer firewall technology related content

To ensure that the overall protection effect is positive and efficient, users need to understand the network security content they need to protect. Network security usually refers to the information security in the network transmission and storage. In practice, it can have a negative impact on network information security, which can be divided into information leakage and so on. Among them, information leakage, information tampering and software security vulnerability are the situations that users often encounter in their daily use\(^3\).

Firewall completes the network security maintenance main policy analysis can be divided into the following points: (1) To improve the security of the entire network environment, the data content should be encrypted first. The encrypted data plays an extremely effective role in preventing information data from being leaked, tampered and destroyed. (2) The link encryption method can also protect and encrypt the data of two adjacent nodes in the network. By ensuring the encrypted data in the link transmission to achieve the unique encryption of different data. (3) Node encryption refers to the protection of the link from the source node to the target node, which is similar to the link encryption method. The difference is that in the method of node encryption, the network node can complete the decryption of the received data content.

3.2. The concrete application of firewall technology

Firewall technology is the application of the whole access policy, which also occupies the main position in network security. To implement the configuration of network access, it is necessary to carry out the arrangement and calculation of packing and to deepen the whole information process running in the computer network, so as to ensure the formation of a scientific and reliable protection system. To complete the protection of the entire access process, specifically from the following aspects:

(1) firewall technology through the operation of different information is not divided In the same unit, and then in different units of the internal and external planning, in order to determine the significant value of circulation visits\(^4\).

(2) Firewall technology also accesses addresses in network operation through access policies. For example, according to the port address, destination address can also be the characteristics of the computer running, so as to plan the most secure way of protection.
(3) In the security protection of computer network, access policies correspond to different technologies, so as to generate policy tables. All activities in the access policy are then accessed. It is worth noting that policy table information is often not fully adapted to the needs of access policy adjustment. To achieve the best access results also need to firewall according to its own policy table in the order of strict execution, thus through a number of restrictive behavior to achieve the protection of the computer network.

(4) Some computer applications can also find valuable information from the protection log of firewall technology. Log monitoring in the protection of computer network should also occupy a large proportion and become the firewall technology to protect the object. When the user is analyzing the firewall log, there is no need to fully execute the operation content, thus avoiding the operation problem of critical information.

3.3. Configure the instance

Table 2. Configuration instructions.

| Demand                                                                 | Relying on the Internet to realize the non-secret LAN of two units and non-secret network of the group connection. |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Configuration instructions                                             | The router mainly realizes the address conversion between the public network and the private network to ensure the connection between the private network and the Internet. VPN is established between the internal interface of the Internet and the firewall to establish a virtual channel to ensure the peer-to-peer connection between the private network of secondary units and the non-secret network of the group. The external interface of the firewall and the internal interface set the relevant access policy, because the internal interface is directly connected to the non-dense network of the secondary unit. So set a number of rules that constrain access rules. IP qualification: access is controlled from the outside to the inside. Set any address as the source address and set all IP addresses of the secondary unit as the destination address. The source address is prohibited from accessing the destination address, and the external network is completely closed to access the private network of the secondary unit. The group non-secret network can be accessed from the inside out by setting the address object to restrict some addresses in the private network[^5]. |

4. Conclusion

The research on firewall technology can not only promote the network environment to be more secure and stable. Meanwhile, the exploration of firewall technology can also lay a more solid foundation for the healthy development of network and the prosperity of Internet market. Therefore, to do a good job in the research of firewall technology and its extensive use in practice, in order to promote the better development of the Internet[^6]. And then provide better service for each user. In order to make the firewall technology better meet the needs of network security, researchers also need to study a higher security and networking performance of the protection wall technology[^7].

References

[1] Wang Qi. Analysis of Computer Network Security Protection and Management [J]. Science and Technology Communication 2017(10).
[2] Liu Xuan. Internet Communication Network Security Protection [J] Coal Technology 2016 (09).
[3] Wang Ke. Analysis of Computer Network Fire Prevention Training Technology [J]. Enterprise Guide 2011(11).

[4] Wu Xiaodong. Analysis of Computer Network Information Security protection [J]. Modern Business 2019.

[5] Lausanne Wangdui. On the Security Management of Computer Network [J]. Information and Computer (Theoretical Edition). 2010(02).

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

[7] Xue Yifei discusses computer Network security and Firewall Technology [J] Information System Engineering, 2011(4): 63-64.