International Journal of New Developments in Engineering and Society
ISSN 2522-3488 Vol. 6, Issue 4: 58-62, DOI: 10.25236/IJNDES.2022.060408

Discussion on computer network security technology and firewall technology

Qi Yina

Wuhan University of Engineering, Wuhan, 430000, China

Abstract: *With the continuous development of computer technology, network technology is deeply integrated into all aspects of society, and people's daily work, study and life have undergone tremendous changes. However, people also gradually realize that with the development of network technology, there are more and more problems in network security. If these problems are not properly handled, they will inevitably become the bottleneck restricting the development of network technology.*

Keywords: *computer; Network security technology; Firewall technology*

1. Introduction

At present, the use of the Internet is becoming more and more extensive. People's daily work, study and life have undergone tremendous changes with the popularity of the Internet. While helping people improve their daily environment, the Internet also provides a large number of users with a wide range of resources and information. However, in recent years, network security has become a hot topic and is gradually being paid attention to. Various types of network security problems are constantly emerging. These problems remind people to take more efficient defense measures and use more advanced firewall technology. Only in this way can we protect the security of the Internet more efficiently. In the use of computers, network security refers to the principles that must be followed to ensure the security of information resources in a special network environment. Because computer network security is attacked by various external factors at any time, people need to strengthen network security awareness and continuously improve the protection system. As the network security protection adopts a complete set of network security strategies, various security technologies are required. Even though people continue to improve the network security protection system, there are still a large number of illegal intrusions, which have a negative impact on the network security and social security to a certain extent.

2. Network security

2.1 Definition of network security

The so-called "network security" refers to that in a computer system, all data can maintain a stable running state without being damaged, leaked or changed, and will not be interfered by any external factors. On the other hand, any confidentiality agreement, degree of integrity, controllable scope, real situation, etc. related to online information are all important issues facing current network security.

2.2 Factors affecting network security

In the process of computer use, if the system is invaded by hackers, the confidential information in the system will be disclosed or changed, and the information transmitted from the LAN to the public network will also be monitored or tampered with.

3. Current main network security strategies

Security policy refers to the principles to be followed in order to ensure a certain degree of security under a specific situation. Because the network often has security risks, people pay more and more attention to the implementation of network security policies. A set of security policies alone can not effectively protect the operation of the entire network security, so we must take a variety of means to carry out network security policies.

ISSN 2522-3488 Vol. 6, Issue 4: 58-62, DOI: 10.25236/IJNDES.2022.060408

3.1 Data encryption

In the network, if you want to implement high-end and effective protection of data, you need to encrypt the data. Its main role is to prevent intruders from tampering, leaking and damaging the information in the network. In general, data encryption technologies can be divided into the following categories:

The "link encryption" technology can link any two similar nodes in the network, so that the data between the two nodes can be transmitted in the link in the form of ciphertext. In the network system, the two nodes connected by each link can use random encryption passwords when transmitting or receiving information, and each link is an independent individual. When the user uses the "link encryption" technology, the message and header are encrypted by different passwords, so that the information of the output node and the receiving node is hidden in the transmission process. The "link encryption" technology can effectively prevent the eavesdropping of intruders, but the link encryption in the network does not protect the intermediate nodes, which makes the information of the intermediate nodes easy to leak, and cannot ensure the security of network communication [1].

The "end encryption" technology is to ensure the security of data transmission between the source node and the target node. During the whole transmission process, data can be transmitted in the form of ciphertext.

When encrypting data, the "node encryption" technology has many similarities with the "link encryption" technology, but the difference between the two is that when encrypting data, the nodes in the network must first decrypt the received data, and then encrypt the data within the node. This encryption form leads to the data being transmitted in clear text between nodes, Therefore, it is difficult to prevent intruders from parsing communication services.

"Hybrid encryption" technology is a combination of link encryption and end-to-end encryption, which can effectively protect sensitive information in the header, thus improving the network security [2].

3.2 Network access control

Network access control refers to the identification of users on the network to prevent data leakage and data damage caused by illegal visitors. Common access control methods are: ① identity authentication. In the network security system, identity authentication is the most basic function. This function can confirm the identities of both parties in a good way. When users need the system to provide services, they need to show relevant identity certificates, such as entering UserID and login password. Then, the system will check the user's identity according to the information provided by the user or the password entered. ② Digital signature. This kind of access control method is to sign and confirm the document or information in the form of electronic signature. This kind of signature can be completed by encryption and has high security. This kind of access control methods can be divided into two categories: "single key" and "double key". When digital signature is performed in the form of "single key", the password of the key cannot be disclosed because there is only one key. When digital signature is carried out in the form of "double key", two users need to register and use the public key for identity authentication, and the two users have their own encryption keys, thus ensuring the security of the transmission information. ③ Access control. The fundamental purpose of this operation is to prevent illegal users from invading and prevent legitimate users from abusing relevant system data. ④ Disaster recovery strategy. The most common form of this strategy is backup. Therefore, users need to back up the system on a regular basis on the server. You can choose to back up locally or online, keep the backed up data as far away from the server as possible, and put these data in different places to prevent the loss of backup data due to theft, fire and other reasons [3].

4. Firewall technology

4.1 Definition of firewall

Firewall is a method to isolate the internal LAN from the public network. When building the Internet security system, the firewall is the most important line of defense in the security system. Generally, a company will give priority to the security of the system firewall when purchasing network security products. Nowadays, firewall is the most widely used network security technology in the world.

ISSN 2522-3488 Vol. 6, Issue 4: 58-62, DOI: 10.25236/IJNDES.2022.060408

4.2 Classification of firewalls

The firewall can be divided into the following two categories according to its defense means and focus.

4.2.1 Packet filtering firewall

In the firewall, packet filtering technology is an important technology, which can filter and manage various information in the network efficiently.

4.2.2 Proxy firewall

Proxy firewall is a new type of firewall technology, which mainly acts on the proxy server, and the proxy server can provide users with connection requirements on the server. When the proxy server receives the connection intention of the customer, the server will first verify the customer's request, and at the same time use the proxy firewall application with high security to respond to the customer's request. After that, it will send the processed request to the real server, and then receive the response from the corresponding server. After further operations, it will send the response from the receiving end back to the source. In the external network, the proxy server transfers information, which can well isolate the internal and external networks. Therefore, this kind of firewall is called the proxy firewall [4].

4.3 Common architecture of firewall

In the work of network protection, the most common firewall structure is composed of "shielded router" and "proxy server". The so-called shielded router is an IP router with many ports. This kind of multi port router will classify and verify the data packets in the transmission process according to a set of set procedures to determine whether these data packets can continue to transmit. This kind of router has the advantages of simplicity and low (hardware) cost. However, its shortcomings are that the correctness of packet filtering is difficult to establish, the management of routers is expensive, and there is a lack of user level authentication. As a firewall with special performance, proxy firewall can replace network users to some extent to realize some TCP/IP functions. The proxy server is equivalent to the gateway of two networks, connecting the data transmission of the two networks[5].

In order to improve the security of the network, people usually use a composite firewall. At present, the most commonly used composite firewalls are "dual hole host gateway firewall", "shielded firewall" and "shielded subnet firewall".

4.3.1 Dual cave host gateway firewall

This structure uses a bastion host and two network cards. Each network card connects the protected network and the external network. Each network card has an independent IP address, so it is called a "dual hole host gateway firewall".

The dual cave host gateway is compared with the shielded router. Its advantage is that the bastion machine system can be used to maintain the normal operation of the network system. This will help the review of the following processes, but it cannot help the administrator to determine whether there are intranet hosts attacked by hackers. One of the fatal defects of the dual cave host gateway is that when an external hacker seizes the bastion host and makes the host capable of routing, all online users can enter the internal network at will.

4.3.2 Shielded host firewall

Such firewalls include shielded routers and application gateways. Among them, the shielded router plays the role of packet filtering, while the application gateway plays the role of proxy. This kind of firewall can set up a shielding router with data verification capability at the junction of the internal network and the external network to form a network security layer. At the same time, it can also set up a fortress host in the internal network to form an application security layer to achieve the effect of double-layer protection.

Compared with the dual cave host gateway, this type of firewall has superior protection performance and is more secure. However, since the two components need to work together, the firewall configuration is very cumbersome.

ISSN 2522-3488 Vol. 6, Issue 4: 58-62, DOI: 10.25236/IJNDES.2022.060408

4.3.3 Shielded subnet firewall

The structure of this type of firewall is "shield host gateway firewall+one router". Two routers can be placed at the head end and the end of the subnet respectively to check and filter the data entering and exiting the subnet. Both the intranet and the extranet can access the protected subnet, but cannot communicate through the protected subnet. In this network protection system, a total of three protective barriers can be formed. Therefore, it is extremely difficult for an intruder to invade the protected system. However, such firewalls require more equipment and software components, and their structure and configuration costs are extremely complex and expensive.

4.4 Firewall technology analysis

According to the differences of firewall technologies, firewalls can be divided into four types.

The first type is group filtering type. This kind of firewall is also known as the packet filtering firewall. Its main work place is at the network layer and the transport layer. This kind of firewall can check and filter the data by relying on the address information of the packet header, the address information of the target, the port number and the type of protocol, and transfer the data text that meets the filtering requirements to the corresponding target address. Other data text will be directly blocked outside the filtering process.

The second type is network location conversion. The conversion of network location is to temporarily convert the IP address to a temporary registered external IP address. Users need to register the IP address for each computer in the network.

The third type is application proxy firewall. This kind of firewall works in the application layer. This kind of firewall is characterized by "isolating" the communication flow of the whole network, and writing corresponding proxy programs for various application services, so as to achieve the purpose of monitoring the entire application layer.

The fourth type is state detection type. This type of firewall probes the data according to the connection state, regards each packet in a network as a complete collective, forms the connection state table, and uses the cooperation between the rule table and the state table to identify the connection factors in the table.

Such a dynamic data connection table will contain previous communication data or data of other related programs. Therefore, compared with several types of firewalls introduced earlier, this technology has the characteristics of high security, high efficiency, good scalability, wide application range, etc. The disadvantage is that these recording, testing and analysis work will cause network delay, especially when many connections are active or many filtering systems are required.

5. Conclusion

With the continuous development of computer technology and the Internet, the scope of its use has covered all aspects of mankind, bringing unprecedented convenience to people's daily work, study and life, but also causing many difficulties. Network security is a complex problem, which includes technology, application, maintenance and other aspects. People should adopt various security protection measures to ensure the security of the network. With the continuous progress of firewall technology, the security level of the network is gradually being improved. These new firewall technologies can not only achieve the filtering tasks of traditional firewalls, but also provide security guarantees for different application systems.

References

[1] Xiao Min, Wang Ying, Song Xiuli, Su Chang. Discussion on Network Management Course Teaching of Information Security Specialty [J]. Computer Education, 2009 (13): 110-112. DOI: 10.16512/j.cnki.jsjjy.2009.13.073.

[2] Huang Ruihua, Zhu Lixin, and Wen Xiangrong. On Technical and Administrative Regulations for Protecting Information Network Security [J]. Journal of Information Science, 2001 (05): 519-524.

[3] He Xinzhou. Research on Computer Network Security Based on Firewall Technology[J]. Journal of Physics: Conference Series, 2021, 1744(4) : 042037.

[4] Bai Lan. Computer Application Based on Network Information Security Technology Management [J]. Information System Engineering, 2012 (03): 83-84.

ISSN 2522-3488 Vol. 6, Issue 4: 58-62, DOI: 10.25236/IJNDES.2022.060408

[5] Liangying Chen. Discussion on Several Typical Computer Network Security Technologies in China[C]. Jinan, China, 2016.