Network Security Policy

Lihua Han
School of Information, Linyi Normal University
Linyi, Shandong, China
E-mail: hlh1227@126.com

Abstract

The development of the Internet makes the rapid economy development of the whole society. Many enterprises form their own networks and connect to the Internet, in order to fully realize the sharing and use of data resources. With the development of the network, network security has become a growing concern in all sectors. This paper discusses the status of network security and several major network security technologies, and proposes several measures to realize the network security.

Keywords: Network security, Firewall, Encryption, Intrusion detection

1. Network and its status

1.1 The concept of networks and network security

The computer security is defined as "the establishment of a data processing system and the technical and management security to protect the computer hardware, software, data is not damaged, changed and disclosure due to accidental or malicious f reasons. " by International Standards Organization (ISO). The definition of computer security includes physical security and logical security. The logical security can be understood as information security, referring to the protection of the integrity, availability and reliability of the information. The network security is the meaning of information security, extended, or network security is the integrity of network information, availability, confidentiality and reliability of protection.

1.2 The necessity to realize the network security

As the development of the Internet, the world economy is rapidly integrating. Computer network are growing popular in all areas of economic and life, and the whole society is increasingly dependent on the network. Many enterprises, the education sectors, government departments and so form their own networks and connect to the Internet, in order to fully realize the sharing and use of data resources. However, with the rapid development of the network, a variety of issues are also produced, especially security issues. To understand the threats to the network to prevent and eliminate it, has become one of the most important things of the network development. Security is the Guarantee of the network's survival, and only security is guaranteed, the network can be more fully realized the value of application.

2. The main technology to realize the network security

The Network security involved a very wide scope with the development of the use of the network.

2.1 Firewall Technology

As the first barrier between internal network and external public network, the firewall is the first one of the products to pay attention to by people.

The firewall is a combination of computer hardware and software. The firewall can be established a security gateway between the Internet and the internal networks to prevent users outside to illegally enter the internal network accessing to internal network resources thereby protecting the internal network from the invasion of illegal users.

According to the technology used in different firewall, we can divide them into three basic types: packet filter-based, agent-based and monitoring-type.

2.1.1 Packet filter-based type

Packet filter-based types are primary products and its technology is based on sub-transmission technology of the network. Network data is packaged as a unit for transmission and the data divided into packets for a certain size. Each packet contains specific information, such as the source address, destination address of the data, source port and destination port of TCP / UDP and so on. The firewall determines if the "package" is from the trusted secure site by reading the address information of the data packets. The firewall will be shut out of these packets, once the packets are from the dangerous site. System administrators can also formulate the flexibility rules according

to the actual situation.

The advantage of packet filtering technology is simple and practical. It can be realized with the lower cost and simple environment.

However, the defect of packet filtering technology is obvious, which is wholly based on network layer security technology and only judge by the source of the data packet, destination of the data, port and other network information. It can not recognize the malicious invasion based on application layer, such as the malicious Java applet and the e-mail with the virus. Experienced hackers can easily forge IP addresses, fooling the packet filtering firewall.

2.1.2 Agent-based type

Agent-based firewall can also be called an agent server, which is more secure than packet filtering products, and has begun develop to the application layer. Agent server completely blocked the exchange of data between the client and server. From the client point of view, the agent server is equivalent to a real server. From the server point of view, the agent server is a real client. When clients need to use data on the server, the data request is firstly transferred to the agent server, then agent server request data to the server, then the data is transferred to the client by agent sever. As the external system and internal server has no direct data channels, it would be difficult that external malicious damage to the internal network.

Agent firewall has the advantage of higher security and can scan application layer to effectively detect and deal with the application layer-based intrusion and viruses. The drawback is that the system's overall performance has a greater impact and agent server must be set up one by one for all application types, which increases the complexity of the system management.

In fact, as the main trend of the current firewall products, most of the agent server (also named application gateway) integrated packet filtering. The mixture application of these two technologies is clearly greater than the one.

2.1.3 Monitoring type

Monitoring firewall is the new generation of products, the technology of which has gone beyond the actual definition of the original firewall. The types of firewalls can take the initiative and real-time monitoring for each layer of data. Monitoring firewall can effectively determine the illegal intrusion of levels, in an analysis of these data.

At the same time, the firewalls are generally detectors, which are placed in a variety of application server and other network nodes. It can detect attacks not only from outside the network, but also from the inside vandalism. According to authoritative statistics, a substantial proportion of attacks come from the inside network system. Therefore, the monitoring firewall is not only beyond the traditional definition of firewall, but also exceed the previous two generations in security.

2.2 Data Encryption

Computer network security mainly includes system security and data security. The system security generally use firewall technology, virus killing and other measures. And data security generally uses encryption technology. Encryption is a way confusing the information, so that unauthorized people can not understand it. There are two types of encryption, that is the private key encryption and public key encryption.

2.2.1 Private key encryption

Private key encryption uses a key to encrypt data, and the other receiving the data use the same key to decrypt. The advantage of this encryption method is very fast and very easy to achieve in hardware and software. But its main weakness is that, once the key disclosure, the information security is directly impact on.

2.2.2 Public key encryption

Private key encryption using the same key to encrypt and decrypt, and public key cryptography uses two keys, one of which is for the encryption, the other is for the decryption. The disadvantage of public key encryption system is slow, but if we combine the two, we can get a more complex system.

2.3 Intrusion Detection System

Intrusion detection technology is a research focus in network security and it is a proactive security technology. It provides real-time protection for internal intrusion, external intrusion and misuse operation to block invasion before the danger in the network. With the development of times the intrusion detection technology will develop to three directions, which are distributed intrusion detection, intelligent intrusion detection and comprehensive

security defense program.

Intrusion detection system (referred to as IDS) is the combination of software and hardware. Its main function is to collect and analysis information from the network or system to find if there is violating security policy behavior or attacking behavior. So that security administrators can promptly deal with the invasion to minimize the damage.

2.4 Virtual private network (VPN) technology

The full name of VPN in English is "Virtual Private Network". It is virtual dedicated or private network built on the public communications infrastructure and can be considered as a separate network from the public network. It can build a proprietary line through special encrypted communication protocol in two or many enterprises, which lie in the different places in the Internet. It is like a line set up the same, but it is not real physical lines.

VPN use four technologies to protect the safety. That is tunneling, encryption & Decryption technology, key management and and authentication technology. Several popular technologies of tunneling are PPTP, L2TP and IPSec.

3. Network security strategy

3.1 The concept of networks and network security

Network security is a systematic project, a social engineering. Network security measures are available from the following four aspects.

From a technical point of view, first of all, network managers must have the right mental preparation. The feature of network decides that network security is a constantly changing and updating field. The rapid development of network technology also means that network security is a "protracted war". Second, it is necessary to strengthen the technical level of network management to establish high-quality personnel. Currently in China, the scarce of talent is prominent problems, especially top-notch talent.

From the management to see, examining the safety of an internal network not only depends on its technical means, but more importantly, depends on the comprehensive measures taken for the network. This is mainly focuses management and safety is from management. Even the best technology, equipment, and no high-quality management, efficiency will be very low.

From the perspective of organizational systems and responsibilities, we should establish network security organization system as quickly as possible, clear responsibility at all levels within the organization, dedicate to safety oversight processes, such as logging and monitoring statistics, establish a scientific organization and management system, and so on.

Finally, strengthen network legislation as soon as. At the same time, we also continuously improve the moral standards of a vast of network users; enhance the safety awareness of each network user. We can fundamentally solve network security problems only in this way.

References

Cai Lijun. (2006). *Network security technology.* Beijing: Tsinghua University Press. 2006.9

Dai Yingxia, Lian Yifeng and Wanghang. (2002). *System security and intrusion detection.* Beijing: Tsinghua University Press. 2002.3

(U.S.A) Greg Holden, Wang Bin and Kong Lu. (2004). *Firewall and network security.* Beijing: Tsinghua University Press. 2004.6