Application of Firewall Technology and Research

Xiaoping Feng and Qi Zeng

Jiangxi Technical College of Manufacturing, Department of Information Engineering

Keywords: Network Security; Firewall Technology; Packets Filtrating

Abstract. Our society will enter a comprehensive network era, which is mainly featured with electronic commerce. Our life will be more closely with the computer network. We can say that our life cannot go without computer network. So there is no doubt that network security is very important for us. We can't imagine how to survive in unsafe computer network, and how does the information be transmitted truly, completely, effectively and legally. So here we will discuss the topic of network security. This paper includes the meaning and characteristics of network security, the threats and attacks faced by computer network, security measures safeguarding network; network security technology introduction, classification and relationship; overview of firewall, firewall key technology; examples of firewall application construction; future development tendency of firewall technology and products, etc.

Introduction

Network security is a popular topic. It can be predicted that the society will enter a comprehensive network and information sharing era in the next few decades, Network security is very important, so only the network security can guarantee the network life can go orderly, the network system cannot be damaged, information cannot be stolen, and the network service will not be interrupted illegally, etc. On the other hand, the current network is suffering from a lot of threats and attacks, and there are many unsafe factors in the network, such as, hacking, information disclosure, etc. Even we can say arbitrarily that there is no absolutely secure network. To this end, we need to study and master more security technology.

A firewall is an important safeguard for network security. Currently, it plays an irreplaceable role in network security protection. A new generation of firewall technology has been greatly improved, such as multiple ports, NAT technology, security audit, encryption, anti-virus, etc., which increasingly make firewall play the vital role. The firewall technology has many shortcomings obviously, such as poor intelligence and so on. This paper mainly introduces the network security meaning, the characteristics of the ideal security network, threats and attacks faced by computer network and the general measures to protect the safety of network.

The Meaning of Network Security

Network security usually refers to the network system hardware, software and system data can be protected and will not be destroyed, changed, leaked because of accidental or malicious reasons, and the system can run continuously and reliably, web services will not be interrupted. There are many different interpretations of network security. Such as:

On the user’s (individual’s, enterprise’s, etc.) perspective, the definition of network security focuses on the protection of the confidentiality, integrity and authenticity of personal privacy or commercial information transmission, to avoid being tapped, pretended, tampered and suffered other invasion, at the same time when the information is stored on a computer system, it cannot be affected by illegal user unauthorized access and damaged.

On the perspective of network operation and management, the information access of local network and other operations is protected and controlled to avoid illegal use of network resources, illegal control, viruses, and denial of service and other threats, effectively defensing network "hackers" attack, etc., which is the content of network security.

For the security department, secured network should be able to filter and defend the illegal and harmful information involving state secrets, avoid the leakage through network and resulting harm to the society and the country's economic loss.

Threats and Attacks Faced by Computer Network

The current computer network system has a lot of weakness, such as data weakness, software weakness, physical weakness, etc. When the system is connected to the Internet, it will face a growing number of all kinds of security threats.

These threats can be divided into two categories: one is the threat of network information; Second, the threat to network equipment. These threats may be intentional, also may be unintentional, may be man-made, and also may not be man-made. We summarize the details as follows:

Human’s unintentional fault: some security vulnerabilities may be caused by human fault such as: configuring the system security improperly; user password is chosen carelessly; account is kept improperly or shared, etc.

Human’s malicious attack: human’s malicious attack, which is the biggest threat to computer network, including the enemy’s attack and computer crime.

Network software vulnerabilities and "back door": it’s impossible that the design of network software has no defects and loopholes, and these loopholes and defects are just the first choice for hackers to use for entrance. In the world, there is more than one case that the hackers entered network, which is mostly caused by incomplete security measures.

The Application Development of Firewall Technology

Firewall is a method separating LAN and wan, which can limit information access and exchange between the protected intranet and extranet. Firewalls can be used as the inlet and outlet for information exchange between different networks or network security domain. It can control the information flow in and out of the network according to the enterprise security policy and has strong ability to resist attacks, so it is the infrastructure to provide information security services, implementation of network and information security. Logically, a firewall is a separator, a limiter and also an analyzer, which can effectively control the activity between intranet and extranet, and ensure the safety of internal network.

Usually, firewall technology includes the following technologies:

Packet Filtering Technology. Packet filtering technology is a major safety technology of firewall, and it controls and operates the network data flow in and out through the firewall. The system administrator can set up a series of rules to allow specific types of packets inflow or outflow internal network and the types of data packets that should be intercepted. Now some packet filter firewall not only conducts access control according to the address, direction, protocols, services, port, access time and other information of IP packets, but also analyzes and monitors any network connection and current session state.

Proxy Technology. Proxy technology refers to the technology of application proxy or proxy server, which can be defined as the information exchange procedure surrogating internal network users and external web server program. It will deliver the request of the inner users to the external server after confirmation; at the same time bring the external server response back to the user.

Encryption Technology. The privacy, recognition and integrity of the transmitted information through internet can be solved by encryption technology. In the application, it should include three parts: the choice of encryption algorithm, choice of information confirmation algorithm, the key management agreement that produces and distributes key.

Complete Audit. Absolute safety is impossible, so what happened on the network must be recorded and analyzed; the sensitive information access of some protected network should be kept continuous record, and report to the system management personnel through a variety of different types of statements, alarm. For example, the real-time safety related information is displayed on the

firewall console, and the illegal user password, illegal access will be tracked dynamically, etc.

Conclusion

With the rapid development of firewall technology, it has become the focus of network technology development to strengthen the management of firewall system. The first is centralized management. The advantage of centralized management is able to provide manufacturers with minimal input to obtain the biggest benefit. At the same time, it also can ensure the consistency of the network security system. The monitoring and auditing function of firewall are strengthened. In the process of firewall technology research and development, we should not only pay attention to the governance after the problem, but also pay more attention to prevention, to kill the potential threat at the beginning. The last is to build a network security system taking firewall as the core. Because we found that in reality, it is difficult to meet the current needs only with the existing network security firewall technology. We should establish the security system taking firewall as the core, which deploy more security defense lines for internal network system, all kinds of security technologies performing their functions to defense foreign invasion from various aspects.

References

[1] Wang X Y. Based on Campus Net to Application and Research of Firewall Technology [J]. Computer Knowledge & Technology, 2009.

[2] Wu Q X. The Research and Application of Firewall based on Netfilter [J]. Physics Procedia, 2012, 25:1231-1235.

[3] Li J. The Research and Application of Multi-Firewall Technology in Enterprise Network Security [J]. International Journal of Software Engineering & Its Applications, 2015, 9(5):153-162.

[4] Win G, Wolman T A, Win G, et al. X Through the Firewall, and Other Application Relays [J]. Digital Equipment Corporation Cambridge Research Laboratory Crl, 1993.

[5] Li B L, He X B, Wang J. The Research and implementation of Key Technologies of Deep Packet inspection based on POP3 Protocol in Router Firewall [J]. Journal of Convergence Information Technology, 2013.

[6] Zheng L, Yue D, Cui S, et al. A research and model of host-firewall based on Windows Hook technology[C]// Multimedia Technology (ICMT), 2011 International Conference on. IEEE, 2011:2892 - 2895.

[7] Yuan W Y, Nie R H, Liang Z M, et al. Research and Application of Filtering Technology on IPv6 Firewall[J]. Computer Technology & Development, 2010.

[8] Dong B, Wang X M. The Study and Application of Electromagnetic Wave Absorption Materials Research [J]. Applied Mechanics & Materials, 2014, 651-653:65-71.

[9] Treese W, Wolman A. X Through the Firewall, and Other Application Relays," Cambridge Research Lab [J]. Digital Equipment Corporation Cambridge Research Laboratory Crl, 1993.

[10] Zhou Q. Solid Defense Architecture Research of Firewall and Intrusion Detection System [J]. Network Security Technology & Application, 2006.

[11] Zhang W. Research and Application of Firewall Technology Based on Linux Operating System [J]. Journal of Mianyang College of Economy & Technology, 2002.

[12] Shuang-Shuang L V, Liu P Y. An Improved Firewall Technology [J]. Application Research of Computers, 2001.