Analysis on the Application of Campus Network Firewall And Intrusion Detection System

Jinying Wang[1, a], Pengfei Yan[2, b]

[1]Department of Information Engineering, Qinhuangdao Institute of Technology

, Qinhuangdao, 066100, China

[2]Department of Information Engineering, Qinhuangdao Institute of Technology

, Qinhuangdao, 066100, China

[a]email: yammm2013@126.com, [b]email: lwdxdf3@126.com

Keywords: Network security; Firewall; Intrusion detection system; Campus network

Abstract. In recent years,when the ample network information, brought about by rapid developing network technology, is changing the campus's learning and living problems, network security problems, such as stealing data information and attack the network equipment of, is becoming more and more serious. As a part of the open network, campus network security can not be ignored. This paper first introduces the difference and connection of firewall and intrusion detection system, and then points out that the advantages of the combination of simple application, also analyzes the threats current campus network faces with, thus puts forward the combination application of firewall and intrusion detection system to guarantee the security of campus network, in order to protect the network security to the largest extent, and ultimately improve the safety protection level of the campus network system.

1. Introduction

For universities, campus network plays an irreplaceable role in teaching, scientific research, management and foreign exchange process. In recent years, with the unceasingly expands of development of campus network construction, the campus network safety problems also gradually highlights. From one hand, We are enjoying the convenience of network information resources, while form the other hand, we are also facing the trouble of network security.

Current network security technology includes two kinds:one is static security technology in firewall technology as an example, the other is a dynamic security technology to intrusion detection system technology as an example. The two kind of network security technology have different advantages and disadvantages. In order to realize the network security of campus network security effectively, the best way is to realize the combination application of firewall and intrusion detection system.

2. Firewall And Intrusion Detection System

2.1 Firewall Overview

A firewall is a piece of software or hardware that helps screen out hackers, virus, and worms that try to reach Intranet. It makes a protective structure between the internal network and external networks, private networks and public network. Thus a firewall is a communication channel, which in accordance with enterprise security policy to control (allow, refuse,monitor, record) the accessing network behavior.

As shown in Figure 1, Firewall filters the network information flow coming from internet. Only data stream which is consistent with firewall security policy can be allowed to pass through.

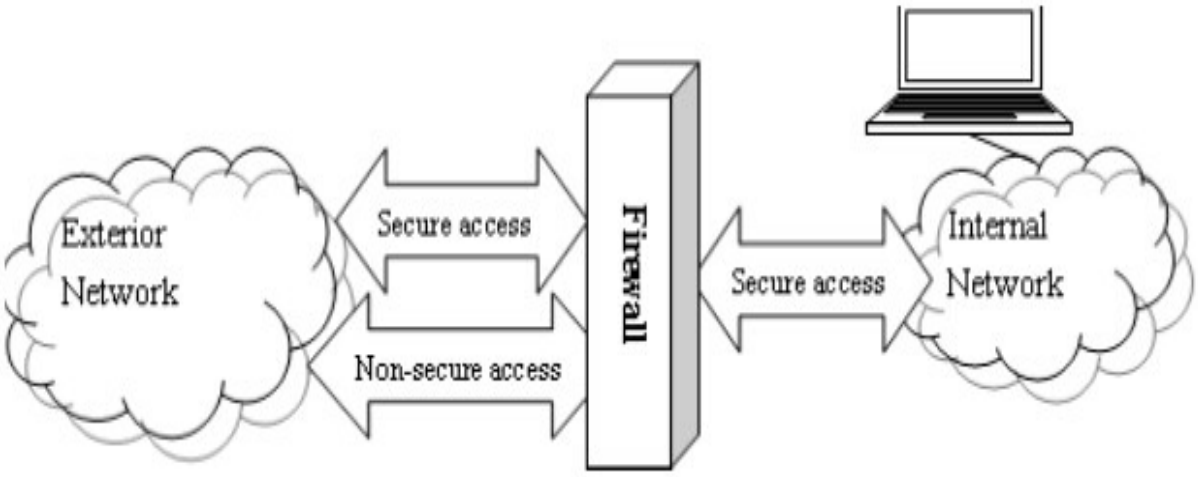

Fig 1. Firewall Filter Data Flow

2.2 Intrusion Detection System Overview

According to the current definition given by United States Agency for International Computer Security Association, Intrusion Detection checks whether there is any breach of network security strategy and the phenomenon of attacks, by collecting and analyzing information coming from the computer network and some key points in computer system. Intrusion Detection System (IDS) is composed of the software and the hardware. As shown in figure 2, based on characteristic description stored in characteristic description storehouse, IDS detect network intrusion and anomaly by analyzing network packets and system log. Therefore, a basic IDS needs to solve two aspect problems: First, how to extract the full and reliable description of behavioral characteristics of the data; second, how to determine the nature of a behavior efficiently and accurately, according to the existing characteristics.

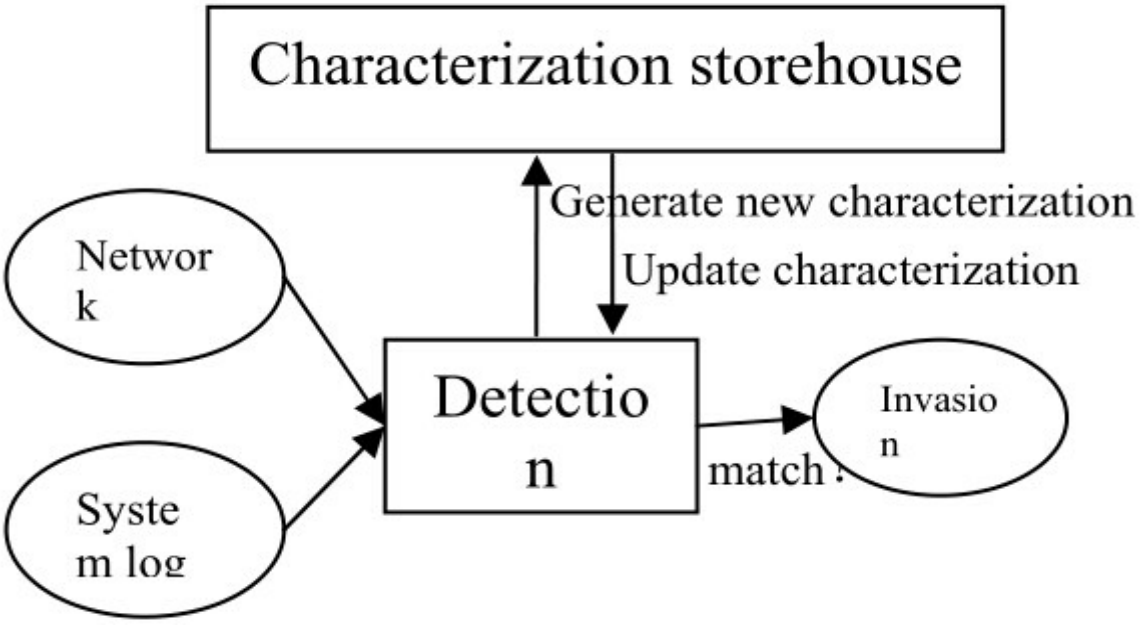

Fig 2. Intrusion Detection Model

3. Difference and Connection Between the Firewall And Intrusion Detection System

The firewall technology is the representative of network static security technology, and is also a kind of passive defense technology. The firewall technology is based on modern communication network technology and information security technology. As the only entry between different network and network security domain mouth, firewall technology is mainly used to control the access network data. But firewall technology cannot prevent illegal access behavior inside. In addition, the firewall technology has another defect that it can not take the initiative track to the intruders, while can only rely on artificial implementation and maintenance. Intrusion detection system, relative to the firewall technology, is representative of dynamic security technology. In network security it is a means of active defense, which actively detects the network vulnerable to threats and attacks the click of security vulnerabilities place, usually detection for dangerous behavior faster than the artificial. And instant analysis of the internal information and communication network, intrusion behavior.The intrusion behavior, attempting to real-time detection, and warning in advance, take early measures to deal with, to protect the security of network maximum.

4. Threat Faced with the Campus Network

At present, security problems of the campus network is confronted with three major threats:

4.1 Physical security

The premise of the campus network security is to ensure the physical security of all equipment of computer network system. The performance of data transmission, data storage and data access security is on the physical media layer. Network operating environment, such as temperature, humidity, power supply is a threat to the security of computer network. Physical security, network equipment, protection is the computer network facilities, and avoid other media in a natural disaster or that the damage in the accident. It is the protection of computer systems, servers, printers and other hardware.

4.2 Threat of Natural Factors

Natural threat faced with campus network refers to the security problems brought about by the nature cause, such as lightning, fires, floods, earthquakes and other natural disasters; positive for the use of the process in the case of damage of equipment; equipment operation and other aspects of the environment, damage hardware, network equipment, affecting the normal operation of the network, pose a threat to the security of campus network.

4.3 Threat of Human Factors

In campus network, human factors, facing network security threats, are divided into intentional and unintentional anthropogenic threats, both of which are a serious threat to the safety of computer network. Intentional threats cover wire connection access network data information, steal the password key to access to information resources, cutting the network communication cable, and the destruction of network equipment types. Unintentional anthropogenic threats refer to operating personnel, although have the legal and technical, have adverse effect on the safety of network or a major loss in the process of operation ,because of error or negligence.

5. Combined Application of Campus Network Firewall And Intrusion Detection System

First of all, select the location of the intrusion detection system. Intrusion detection systems can be put in inside the firewall, can also be placed on the outside of the firewall. But according to the different functional advantages of the two, intrusion detection can timely detect abnormal,

aggressive behavior, and control illegal intrusion by the firewall. The intrusion detection system is placed behind the firewall, and illegal information can be filtered by firewall technology, so that it can be protection for computer network to a certain degree. Internal intrusion detection system on the firewall, in maximum stop "childish script" attack at the same time, make the intrusion detection system to find attacks. Secondly, combining the firewall in campus network and intrusion detection system model design, the two are not just a simple superposition, but analysis of both specific function, advantages and disadvantages, after a study established by simple intrusion detection system assisted firewall technology security system. Finally, firewall and intrusion detection system interface. Both the realization of interactive in two ways. One is the intrusion detection system is embedded into the firewall technology, combining closely with the realization of the two. In this case, the intrusion detection system data from a data stream flows through the firewall. Firewall not only to verify the data, but also makes a judgment on whether the aggressive, thereby blocking on aggressive behavior. But intrusion detection system is a huge system, which brings certain difficulty for the implementation of. Another way is through the development of an interactive excuse to realize. Firewall technology, intrusion detection system, their open an interface, provide used to each other, both sides of transmission information according to the prior negotiation way. This interactive mode is flexible, and will not have impact on the performance of firewall technology and intrusion detection systems.

6. Conclusion

This paper combines static technology in firewall technology as the representative and the intrusion detection system as the representative of the dynamic of technology applications. It is not simple physical binding of the two system by setting the standard interface, but show the unique features of the two methods in the new system. It powerfully ensures safety of the campus network , and effectively improves the defense ability of the network. In future, combined application of firewall and intrusion detection system will provides a broad space for the development of the technology of computer network security. In the process of computer network security, combined application of the technology of firewall and intrusion detection system will learn from each other to add a heavy security for the protection of the security of computer network.

References

[1] Mo Zu-qin. Intrude Detecting Technique Summarizing. Metrology and Measurement Technique

[J] 2005,32(12):p.24-25

[2] Li Yu-jun. Firewall and Intrusion Detection Based on the Linkage Mode. Computer Knowledge and Technology [J] 2009-03-021 p.560-562,575

[3] Wang Lei. Research and Implementation of Interaction Response Strategy with Firewall and Intrusion Detection System [D] HARBIN Institute of technology.2008

[4] Wang Dei-zheng. Studies on Network Intrusion Detection Technology Based on Protocol Analysis. Popular Science & Technology [J] 2009-01:p.13-14

[5]MA Tong-wei; et al. On Invasion Detection Technology of Network Security. Journal of Henan Mechanical and Electrical Engineering College. 2007, 15(3):p.21-22