Design Scheme of Network Security based on Compound Policy Analysis

Xiaolei Zhang1,* and Bin Wang1
1Qingyuan Polytechnic, Qingyuan, China
*Corresponding author e-mail: 33937335@qq.com

Abstract. Network security refers to the protection of the hardware, software and data of the network system caused by accidental or malicious reasons caused by damage, change, leakage, so that the system can run continuously, reliably and normally, and the network service is not interrupted. Firewall technology is the main means to solve the network security problem. Firewall technology is an applied security technology based on modern communication network technology and information technology. By using audit records in intrusion detection system, intrusion detection system can identify any undesired activities, so as to limit these activities in order to protect the security of the system. Therefore, only by taking a variety of preventive measures and formulating strict confidentiality policies and clear security policies, can we ensure the confidentiality, integrity and availability of information in real time, and provide a strong security guarantee for the network.

Keywords: Intrusion detection technology, Firewall, Access control, Encryption, Security audit

1. Introduction
This section mainly introduces the current situation, characteristics and common network security threats. The management of critical equipment is a very important task [1]. This is because any failure of key devices in the network can cause network paralysis and irreparable damage to users.

As a kind of security service, entity authentication is particularly important. In an open distributed network environment, users on workstations want to access server resources distributed on the network. However, resources on the network only allow access to the specific permissions of authorized users, so in distributed networks; a mechanism must be provided to authenticate the identity of users.

Network security audit system is a kind of data acquisition, analysis, identification and resource audit blocking software based on information flow [2]. It is according to the security control policy set by the user, the activities of the controlled object are audited. It focuses on the "middle" stage. The system integrates the technical means based on the host computer, and can realize the control and management of the network by multi-level and multi-means.

A very important feature of a campus network is that the number of users is relatively large, there will be a lot of PC lack of effective virus prevention means, so, when users frequently access INTERNET, when sharing files through the local area network, through U disk, CD-ROMs copy files,
the system will be infected with the virus, when a student infected with the virus, he will send to every
corner of the campus network, sent to other users. Send it to the server.

The server used in the network is often the main object of attack because of its large amount of
information and strong processing ability. At present, the network of enterprises and organizations is
facing a variety of security threats, such as hacker attacks, malware, information disclosure, denial of
service, internal damage. Accordingly, we have taken many precautions, such as installing firewalls
and antivirus software, information encryption and access control, scanning technology and intrusion
detection technology. All kinds of network security defense measures are not isolated, but as a whole
to provide security for a network.

In order to prevent unauthorized users from using network resources and users deliberately destroy
the security of network system, security management should do a good job of security measures, such
as legitimate equipment access control and encryption, and so on..

2. Definition of attributes and threats in Network Security
For network equipment, operating system, database and application system, check whether the
password complexity of management account is not less than 8 bits and contains at least case and
lowercase letters, numbers and three categories of special characters (focusing on the existence of
weak password or default password), passwords should be changed periodically (such as quarterly) or
irregularly (such as before major festivals) [3].

The user logs in on the client. On the login interface, the user name User and password Password,
are displayed in normal characters, and the password is displayed as an asterisk. In order to prevent the
password from being obtained by the eavesdropper on the Internet, the password entered by the user
encrypts theEk (Password), on the client, so the encrypted user password Ek (Password). Is
transmitted on the Internet. Because the eavesdropper does not know the key K, even if they go to the
information Ek (Password), they cannot get the user's password Password server to receive the
information transmitted by the client and extract the user name User ciphertext, as is shown by
equation(1).

$$s_k^2 = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \overline{x}_k)$$  \hspace{1cm} (1)

Basically, where s is the sooner you update, the less risky you will be. Firewall data should also be
updated in a timely manner.

Install intrusion detection system detector on trunk switch; install NetHawk network security
monitoring and auditing system on trunk switch [4]. In this way, you can find out which port is closed.
Neither ICMP nor ICMP errors are guaranteed to reach, so the scanner must also be able to retransmit
when a packet appears to be lost.

The amount of log data is very large and growing, and when the limit is exceeded, it cannot be
simply discarded. Need a complete set of backup, recovery, processing mechanism. In the problem of
centralized analysis of log data, an attacker may attack servers in multiple networks at the same time.
If the log information on each server is analyzed individually, it is not only a heavy workload, but also
difficult to find attacks. How to associate the logs on multiple servers to discover the behavior of
attacks is an important problem faced by the security audit system.

The reason for the embezzlement of IP, MAC address: a campus network adopts static IP address
scheme. If there is no effective IP, MAC address management means, users can change the IP address
at will, and the MAC address can be changed at will in the advanced options of network card
properties. If the user intentionally or unintentionally changes his IP, MAC address, it will cause
multi-party conflicts, if the gateway address conflicts, all users in the same network segment can not a
large number of users' Internet packets fall into the hands of malicious users, resulting in ARP
spoofing attack.
Users send a lot of confirmation information to the server, so that the server is full of this useless information. All the information has false addresses to reply to, so that when the server tries to return it, it cannot find the user. So the server waits temporarily (sometimes for more than a minute) before cutting off the connection. When the server cuts off the connection, the hacker sends a new batch of information that needs to be confirmed again and again, a process that starts over and over again, resulting in the server unable to move and paralyzed to the ground.

3. Analysis of key Technologies and Strategies of Network Security

Today, TCP/IP protocol has become the de facto industrial standard, any workstation of TCP/IP network master needs a legitimate IP address to work properly. In the construction: when planning the computer network, we should do a good job in the investigation and statistics of the needs of each department within the organization for the Internet service, and determine the scale of the computer network. Whether the IP address is properly managed or not is the key to the efficient operation of the computer network. If the management method of IP address is not perfect, the network is prone to IP address conflict, which will lead to legitimate IP address users cannot enjoy the network resources normally, and even cause damage to some key data.

Vulnerabilities and backdoors is in network software. Any software has more or less vulnerabilities; The firewall is divided into 12 modules, each of which has a considerable amount of work to do, except for greater flexibility kernel module and firewall module [5]. Once it is opened, others can enter the system at will, and the consequences are unthinkable.

The deployment of the F5LTM at the front end of the transaction server and the portal server ensures that the client's requests are evenly distributed to different servers that provide the services normally, attack time and attack type of intrusion. Check whether the operating system, database, middleware and other third-party software update the latest patches [6].

The open UDP port does not need to send back the ACK packet, and the closed port does not require the return of the error packet (and the principle of this experiment is that those hosts will return the ICMP Port Unreachable error in the closed UDP port, so there is a good chance of misjudgment, because of the limitations of time reasons and their own knowledge cannot think of a better way), so it is very difficult to scan the UDP packet. Both the UDP packet and the ICMP packet are unreliable. The speed is slow (the speed of error message generation is limited), and root permission is required to read ICMP message, so the use of error message is very limited [7].

Intrusion detection is to use a variety of built-in correlation rules to analyze the correlation of log and alarm information generated by devices distributed in the network, so as to detect security events that are difficult to find in a single system. Automatically generating security analysis report is to analyze the security of network or system according to the log data recorded in log database, and output the security analysis report [8]. The output of the report can be automatically generated according to predefined conditions and submitted to the administrator. Real-time monitoring of network status can monitor the status of specific devices running agents, network devices, log content, network behavior and so on.

The common network attacks in campus network, such as stealing the administrator password of switch, sending a large number of broadcast messages, the existence of these attacks will disrupt the normal operation of the network and reduce the efficiency of campus network.

4. Design Scheme of Network Security based on Compound Policy Analysis

Illegal access is to access, use, or destroy certain resources without the authorization of the administrator. At present, there is a unified name for illegal intruders-hackers. They rely on their own technology to illegally obtain the control authority of the system, so as to steal user secret information and destroy data [9]. At present, there is still against cybercrime, so that the concealment of hacker attacks is strong, and the "lethal power" is strong.
For common viruses, such as shock wave, oscillatory wave and so on, the port of TCP, UDP used by these viruses can be prevented by deploying extended ACLs. Once a user is accidentally infected with ensure the reasonable use of network bandwidth in campus network.

It is link encryption. Encryption between network nodes, transmission of encrypted information between nodes, and it is decryption after transmission to nodes, different passwords between different nodes. 2, It is node encryption. Similar to link encryption, the difference is that when data is transmitted between nodes, it does not need to be transmitted in clear code format, but decrypts and encrypts with special encryption hardware, which is usually placed in a secure safe, as is shown by equation(2).

\[ P(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x - \mu)(x - \mu)^T}{2\sigma^2}\right) \]

The network management software adopts component structure design, where p is realizes the functions of equipment management [10]. Support a variety some is to achieve omni-directional network management from the device level to the network level.

As it is independent software, network security audit system and other security products (such as firewall, intrusion detection system, vulnerability scanning system, etc.) , there are independent of each other in function, but at the same time, they can coordinate with each other, and it is complement each other and protect the overall security of the network.

Combined with the characteristics of SAM system and switch embedded security protection mechanism, this design realizes network security from three aspects: accurate identity authentication in advance, real-time processing in the matter, and complete audit after the event.

Install an intrusion detection system gigabit detector on the local area network center switch, an 100 megabit detector on the DMZ area switch to detect the access of local area network users and external network users to the host in real time, install an intrusion detection system 100 megabit detector and intrusion detection system console in the security monitoring and backup center, and carry out unified management by the system console (unified event library upgrade, Unified security protection policy, unified report log generation report).

5. Conclusion
Access control is also an important means to maintain network system security and protect network resources. Access control technology mainly includes access control, network authority control, directory level security control, attribute security control, network server security control, network monitoring and locking control, network port and node security control.

Acknowledgments
This paper is supported by the Project of Qingyuan Network Security and Maintenance Skilled Master Studio.

References
[1] Miao Yan, Information Security, Network Security, cyberspace Security, Information and computer (theoretical Edition), 2016 (12):89-95.
[2] Joe Tian, Research on Network Security Management issues and Strategies, Communication World, 2017 (18):45-52.
[3] Zhang Xianqiu, problems and Protection Strategies in Enterprise Information Network Security Management, China Management Informatization, 2016 (01).
[4] Zhang Bin, Application of Virtual Machine Technology in computer Network Security Management, Electronic World, 2017 (10):102-108.
[5] Tang Xiuzhong, Liu Hoping, problems and Countermeasures of Network Security Management in Colleges and Universities, Journal of Chifeng University (Natural Science Edition), 2017
(09).

[6] Yang Yunjiang, computer Network Management Technology, Tsinghua University Press, 2010.3:500-509.
[7] Yu Dehai, Wang Liang, Wang Jinfu, computer Network Technology Foundation, China Water Conservancy and Hydropower Press, 2008.
[8] Zhang Yulin, computer network management and related security technology. Reading abstracts. 2015 (04):356-362.
[9] Jiao Yong, computer network management and related security technology exploration. China's new communications. 2016 (24).
[10] Zhang Jinying, computer network information security measures analysis. The world of communication. 2017 (02):470-479.