ATLANTIS PRESS

Advances in Engineering Research, volume 141

5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017)

Analysis of Wide Area Network Security Technology System

Yiyue Luo[1, a]

[1] Haikou College of Economics, Haikou, Hainan, China, 571127

[a]email,

Keywords: Wide Area Network; Network Security; Security Technology System

Abstract. In recent years, with the wide area network security attacks and threats gradually increased and how through the wide area network security technology system to effectively ensure the safety of the wide area network has become an important area of network security research. This paper mainly analyzes the importance of WAN security and the network security problems faced by wide area network (WAN), so as to solve the security problems of the network security technology system of the wide area network, strengthen the security early warning technology, analysis and research the public key infrastructure and the security management strategy.

Introduction

Wide Area Network, referred to as WAN, is a different area of the local area network or metropolitan area network connected to a computer communication remote network. Wide physical coverage of the wide area, from tens of kilometers to thousands of kilometers, can connect multiple cities or countries, and even across several continents can still provide long-distance communication of a remote network. In the world, all walks of life have a wide area network figure. The communication subnet of the WAN can connect the local area network or the computer system around the world by using the common packet switching network, the satellite communication network and the wireless packet switching network, so as to achieve the purpose of network resource sharing. Among them, the most common Internet is the world's largest WAN.

The Importance of WAN Network Security

With the continuous development of information science and technology, the construction of the wide area network is also constantly improving, from the national government agencies to various business units, are access to the wide area network through the realization of the sharing of information resources. However, people enjoy the sharing of resources at the same time, the wide area network security threats also increased, information leakage, information pollution and information is not easily controlled and other issues increasingly prominent.

WAN is the lifeblood of the world's information and the core control, because both at home and abroad, from the national defense communications facilities, scientific research, to the power control network, financial systems are using the wide area network for information exchange and sharing, once the wide area network of the network security problems, it may lead to many important institutions of the system suffered damage or even paralyzed. Therefore, we need to build a dynamic, sound, systematic WAN security technology system, ahead of monitoring, prevention and resolution of WAN network security may arise any problems, so as to further enhance the WAN network security initiative defense capabilities.

The Security Issues of the Wide Area Network

In the current information society environment, the computer Internet technology has become more and more flexible and open, network security problems are endless, different forms: network and computer system technology design loopholes, network and computer system password theft take, protocol error, authentication error, information disclosure and so on. Compared with the local area network, the WAN management and maintenance is more difficult, which led to the WAN network

security technology to strengthen the imminent. At present, the hidden danger of WAN security mainly exists in three aspects:

More Diversified Attack Channels. Due to the wide range of WAN access devices, which mainly include routers, switches, modems, communications servers, memory and so on. In addition, with the rapid development of modern mobile network technology, people have begun to use more and more mobile Internet, which increased the WIFI, 2G, 3G, 4G and other wireless access. WAN access channels from the past, the traditional PC, notebook computers, etc., gradually increased the mobile phone, tablet PCs, smart terminals and other more diversified access channels, but also makes the wide area network attack channel has become more diversified [1].

Network Security Threats Are More Intelligent. With the continuous development of network technology, the threat of network security is also more intelligent, from the flawed DDOS attacks, to ARP spoofing, DNS spoofing, DLL hijacking and 0day Hacker attacks. A variety of network attacks continue to upgrade technology, a variety of worms, viruses and Trojans hidden period is longer and longer, become more and more subtle, and some threats even make the current virus defense and killing software are powerless.

A Wider Range of Damage. Because WAN coverage is much wider than LAN (LAN) and MAN (MAN), which makes the scope of the wide area network damage is more extensive, a variety of different types of system management platform through SOA architecture, ESB technology Access to the WAN. In this case, if any of these systems are attacked, then the virus will be in a short period of time quickly spread to other sub-systems in the WAN, resulting in a wide range of damage.

The Security Technology System of Wide Area Network

At present, WAN network security technology research, mainly in a variety of different types of anti-virus and monitoring software, virtual private network, access control list. However, with the continuous development of modern network technology, WAN network security in a variety of attacks and threats become more intelligent and extensive, these single security tools cannot really make the WAN network security is protected, we It is necessary to introduce more advanced security defense technology, such as digital signature, IPSEC technology, DES encryption technology, through the construction of a complete WAN network security technology system, to enhance the WAN network security index. In addition, the security and protection of the wide area network security, in fact, is a dynamic process, the need to constantly study the wide area network security aspects of the characteristics of timely changes and adjustments in order to more effectively ensure that the WAN network security. To build complete and effective WAN security architecture, you need to consider the following aspects.

Network Layer Security. WAN communication technology is mainly located in the OSI model at the bottom of the three levels, namely: the physical layer, the data link layer and the network layer. The network layer is the most important level in the WAN security system, because the WAN layer of the network layer for each node in the exchange of information and data to provide a connection, so the network layer in the WAN network equipment may be data loss and leakage, As well as network equipment configuration attacks and other risks. Therefore, it is necessary to establish a complete and perfect management system for the network layer of the wide area network. Through the different levels of the network layer of the wide area network security distinction, the formation of a complete network layer protection standards and system requirements, with the WAN network security management Standardize the system, the WAN network layer of security continue to deepen and management [2].

System-Level Security. WAN system layer security issues, mainly focused on the network operating system, database and related products, security vulnerabilities and virus threats. WAN system layer security is the most basic security issues, once the WAN system layer of any security risks or vulnerabilities, will lead to the overall security of the entire information system has been destroyed. For example, hackers can through the Unicode, cache overflow and other means of the WAN system layer to destroy, and access to relevant information. And a large number of WEB

servers, database servers, mail servers, file servers, etc., are usually stored in the WAN system layer, once these servers are paralyzed or remote control, the consequences will be disastrous. Therefore, in the WAN system layer security, the primary measure is to take the defense, to prevent in the first place. First of all, through the provision of firewall, authentication technology, access control, virus prevention, intrusion detection and other traditional security system, followed by intrusion protection technology, honeypot and honeynet technology, forensics technology and other active security system defense measures, Two-pronged approach to ensure the information security of the WAN system layer.

Application Layer Security. The application layer in the WAN is mainly composed of a number of specific application service elements, and one or more common application service elements. Each specific application service element provides a specific application service. In fact, the WAN application layer is not as easy as the network layer invasion, WAN application layer is rarely able to be completely invaded; However, once the successful invasion of the application layer, destruction is fatal. Such as a variety of Java Applet or Active X applets, are likely to carry viruses or Trojans, and then the WAN application layer data and systems damage; damage depth and breadth of the network layer is more serious. In addition, in the WAN application layer, hackers can easily through the WEB, DNS, FTAM, MHS, VAP, E-mail, FTP and other WAN application layer security flaws to attack; for example, DNS service threats, identity vulnerabilities , E-mail system vulnerabilities, CGI script defects and so on. Therefore, for the WAN application layer of this security features, only through the firewall settings is not enough, but also the corresponding database files to hide, modify the format or encryption, to achieve more effective security [3].

Strengthen the Safety Early Warning Technology. For the characteristics of the network security technology system of the wide area network, it is necessary to strengthen the security warning technology of the wide area network to ensure the confidentiality, integrity and reliability of the system resources. Through the wide area network security early warning technology, you can network system to run the entire state of a comprehensive monitoring. According to the different sources of information, WAN security early warning technology can be divided into host-based security early warning, network-based security early warning and hybrid security early warning. According to different actual situation, use different WAN security early warning technology.

WAN security early warning technology, mainly through the data acquisition module for the system to provide raw data, the data source can be the host of the log information or change information, it can be on the network data or traffic changes. After the data extraction module obtains the data source, the data source is simply filtered, the data format is standardized and so on, and the processed data is stored in the database. Then, the event analysis module will analyze and classify the data in the database, So as to establish a data warehouse according to different protocols, discover the basic time change rules through data mining, and finally generate the early warning module to the security early warning system of the wide area network. Wait for a full monitoring of all threats and attacks that may occur in WAN security. Once the monitoring detects any problems, a security alert will be issued to indicate possible security vulnerabilities and security threats that will allow users to move faster and timely to take appropriate protective measures to avoid the security of the wide area network is further threatened. WAN network security technology through the network intrusion technology, detection model, audit analysis strategy for the construction of the WAN network security system, providing a powerful means of detection and protection [4]. WAN security early warning technology as a new type of wide area network security technology, to a large extent, to fill the past, the traditional dynamic solution to the problem of WAN security problems.

Public Key Infrastructure. Public Key Infrastructure technology is a technology commonly used in the wide area network security system. Public Key Infrastructure technology is actually an infrastructure which can provide services for network security through the use of public key technology. Public Key Infrastructure technology, it can be said that the modern WAN network information security core technology. It is through the transmission of data streams in the re-combination or encryption, so that only legitimate recipients or people with secret key energy

efficiency to open, this approach not only to ensure the confidentiality of data information, but also makes the data is difficult to be unidentified of the guest copy. Public Key Infrastructure technology can effectively solve the security problems such as confidentiality, authenticity and integrity of e-commerce, government affairs, affairs and other aspects. Therefore, it is widely favored by users. In addition, Public Key Infrastructure technology has a strong flexibility, economy, interoperability and scalability, can be in the WAN network security system play a vital role.

Security Management Strategy. In the wide area network security technology system, the implementation of security management strategy also has a very important position. Without a complete and effective WAN security management strategy, the entire WAN will show a chaotic network state. A complete set of WAN security management strategy must be for the information system security mechanism for effective security prevention and control, to ensure the normal operation of the entire information management system. For some of the inherent problems inherent, simply through the use of procedural patch method is difficult to solve, this time through the WAN network security management strategy to make up for human factors; for example, for computer information management system external equipment and related lines regular inspection and maintenance, and always ensure that the computer information system is in a good operating environment; the development of strict personnel management system to ensure that different authorities of the legitimate management of the system and so on. Through the implementation of the security management strategy of the wide area network security technology system, it can effectively improve the confidentiality of the system and avoid the leakage and destruction of the information.

Conclusion

In recent years, with the continuous development of WAN security technology, at home and abroad for the wide area network security system research is also more and more in-depth, how can effectively avoid, defense and solve the wide area network information disclosure, viruses, hacking and other A variety of security issues, the effective establishment of a wide area network security network technology system has become the most important development of information science and technology. In order to prevent and deal with the security threats in the wide area network in a timely and effective manner, we must fully understand the composition of the network security technology system of the wide area network, master the network security defense technology of the wide area network, and improve the wide area network security by adopting the advanced and effective wide area network security policy the defensive ability.

Acknowledgements

Fund Project: 1. Hainan Provincial Natural Science Foundation Project (Project Number: 617175, Project Name: simulation and cloud platform application based on adaptive load balancing algorithm). 2, Hainan Provincial Higher Education Research Project (Project No: Hnky2017-63, Project Name: Research and Practice of Constructing Nanhai More Road Culture Exhibition Platform Based on "Internet +" Mode)

References

[1] Wang Jing. Talking about the establishment of computer information system security mechanism strategy[J]. Technology Information, 2013 (1): 92.

[2] Li Ming. Dynamic complex threats require real-time network security defense [J]. Network Security Technology and Applications, 2013, 24 (5): 9-10.

[3] Chen Xiaosu, Lin Zhi, Xiao Daoju.Study on the Framework of Network Security Protection System Based on Policy [J]. Computer Engineering and Science, 2014, 29 (6): 7-9.

[4] Lu Linxin. Research on Computer Network Security Protection Measures and Countermeasures[J]. Science and Technology Innovation Guide, 2010 (4): 15-16.