ISSN : 0974 - 7435 Volume 10 Issue 21

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(21), 2014 [12810-12815]

Study on application of computer network security system in modern enterprises

Liping Niu[1], Xinzhi Guo[2]

[1]School of Computer & Information Engineering, Henan Normal University, Xinxiang, 453007, (CHINA)

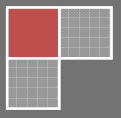
[2]School of Continuing Education, Anyang Institute of Technology, Anyang, 455000, (CHINA)

ABSTRACT

With the rapid development of society, technology and economy, the economic circumstance in China has undergone great changes, for it has entered into a world with more intense competition. The development and application of computer in economic field has led to major changes in the world economic system. Computer technology, contributing a lot for the rapid growth of China's economy, gains the most rapid development with the most beneficial economic structure since China's reform and opening up. Now, computers occupies a very important position in all walks of life, and have changed the operating mode of modern enterprises, such as the company information storage, transmission, data analysis etc., greatly improving the efficiency of enterprises, increasing the global competition of enterprises. However, there follows the network security issue with the application of computer, how to ensure the safety of the internal data in modern enterprise is the foremost issue. This study analyses the current status of application of computer network system in the modern enterprise, introduces the application of various computer network technologies in enterprise and network security issues, and the way to ensure corporate computer network security, such as the protection of transferred data from malicious tampering, deletion, theft, etc. Only with the establishment of a healthy and harmonious enterprise network environment can the development of modern enterprise get promoted. And the insurance of security technology in modern enterprises' computer network will provide staffs more professional, complete service, with a rather high feasibility and reliability. Thus not only can the development goals of modern enterprise network security system be achieved, the effectiveness of modern enterprises can be largely promoted too.

KEYWORDS

Internet security systems; Computer technology; Enterprise; Security management; Security safeguard system of information systems.



INTRODUCTION

With the continuous development and expansion of modern enterprise, and the gradually increased business in recent years, the former model and size of corporate computer network security systems has been unable to meet the needs of nowadays enterprises' development. Therefore, a new, advanced corporate computer network security system is needed. Conforming to the needs of the times, by the use of computer technology, a more modern management model can be created. This model will achieve combination of scientific management, and informationization and intelligence, will form a platform for complete, intelligent planned enterprise management and service, thus enabling enterprises to enhance efficiency.

Star network topology is the main network platform applied by enterprise, cored on Ethernet technology of rapid exchange. Depending on the needs of their own development and management modes, enterprises have the network dispatched into many application subnets, and entitle users of different layers with the corresponding permissions, thus to realize the reasonable configuration of resources and coordinate schedule, providing a good foundation for rational analysis for enterprise decision-making. The high-tech equipments in internal service center such as database server, GPRS servers, video surveillance etc. are mainly to provide access to data and information and communication services for the stable operation of the enterprise. The central portion is connected with its affiliated parts by virtual network for remote connections[1], which ensures the development of enterprise infrastructure business as well as the communication among various businesses to a certain extent. Web services platform contributes to the rapid development of enterprises, but in order to ensure the safety and stable operation of the enterprise network systems, a very reliable network security support platform is needed. Only with effective security measures can the enterprise resist the illegal network data attacks and ensure high confidentiality and integrity of enterprise. However, enterprise network security system is a very complex and challenging project. It requires careful and reasonable arrangement of structure of the enterprise network, together with advanced network security technology to create a reliable, secure enterprise network system.

KEY TECHNOLOGY OF NETWORK SECURITY SYSTEM IN ENTERPRISE

The network security system is the key to modern digital management and efficient operation for enterprises, so it is necessary to take all measures and security technologies to set up enterprise network security systems from all aspects, to avoid the risk of loss of business because of network security systems. In addition, building a secure network security system can secure information protection system to ensure the security and integrity of internal information resources. Secured corporate networks can provide better, more professional service functions for the company, reduce the risk to a minimum, and achieve the balance between security and effective investment.

Concept of network security

Computer network security involves many scientific fields, such as computer science, network technology, coding theory, etc. With the further development of modern information technology, advancement in network technology, the application of network security technology gradually expanded, and gradually turned into a structure of multiple levels of network security system. Despite the various definitions in computer network security, there is one the ultimate goal which is mainly to establish a secure protection system for enterprise data systems to secure the safety of infrastructure of hardware and software, to protect various data from malicious attacks, damage, and disclosure. In China, there is a particular emphasis on a confidential, complete, available and controllable network security of computer network. Network security model is shown in Figure 1 as below.

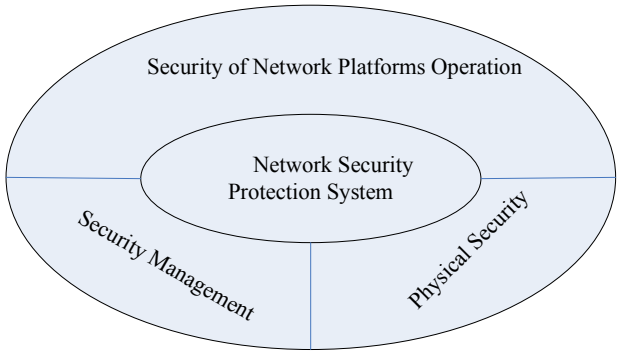


Figure 1 : Model of network security protection system

Computer network security is realized through a variety of security technologies and technology management methods, in order to achieve a safe and smooth transfer of information within the system, to ensure transmission, reception, processing

and storage of internal data. Among the various features of computer network security, the ultimate aim is to ensure the security of network data. The availability feature of network security ensures entitled users to access data in the network databases, even in case of malicious damages or other failures, the system are still able to provide normal services, avoiding issues of data loss, or data cannot be shared. So it is necessary to establish a reliable, complete network information platform for sharing of resources, and to increase network controllability. Network security system has integrity to ensure that data won't be lost or destroyed in the process of transmission, and only authorized users can modify the data, and check whether the data has been modified successfully. Enterprise network security must be with a high degree of confidentiality, so only authorized users can access to the data while unauthorized visitors are blocked. VPN technology is applied in network security to encrypt confidential data. In addition, the reliability of network security is also very important, and only secure and reliable network security system can provide high-quality service, if the network system has function of recoverable data backup, the reliability of network system will get greatly improved.

Introduction of key technologies of network security

In order to ensure the safety of the enterprise network system, a variety of network security technologies are needed for an establishment of multi-assurance, realizing the enterprise network security maintenance ultimately, and providing better technical services for the development of enterprises.

(1) Firewall Technology

Firewall technology[2] establishing a security protection system in the present corporate intranet and extranet, is a safe isolation technology, can effectively control access mechanism. By separating the enterprise's internal network and its external network, it sets restriction on user access, which can effectively guarantee the safety of data on the network. Firewall can be divided into several basic types of filtering firewall, hybrid firewall and proxy services. Firewall technology can effectively prevent some users without granted access; can effectively circumvent attacks from the hackers on database information and networking equipment. Generally firewall technology is only available for the boundary of the internal network and the Internet, so it can effectively protect the internal security of the database, even if the internal danger can be effectively filtered out. Firewall technology in the future can further concern about application security, and user security, and can make configuration easier and more convenient, so as to set up a network security mechanism. As shown in Figure 2 is the firewall deployment diagram.

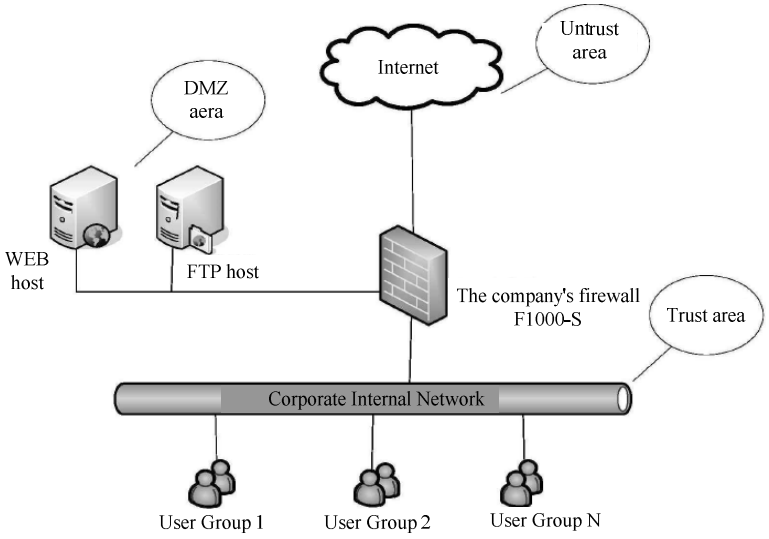


Figure 2 : Firewall deployment diagram

(2) Virtual local area network

The application of VLAN (Virtual Local Area Network, VLAN)[3] technology makes the topology of the network more diverse and flexible. VLAN separates network devices into multiple logical subnets, thereby achieving exchange function of virtual local area network data. VLANs can be divided in different ways, which represent different forms of implementation of virtual local area network, such as the port-based division which is a relatively simple way of division, MAC-based division which divides the VLAN mainly according to the physical address in the network card, network-based division which is mainly applied in large-scale networks, policy-based division which is a more flexible division. VLAN is able to control broadcast storms, improve overall network performance, increase network performance and security, and easy, intuitive in network management. Figure 3 is an enterprise's virtual local area network (VLAN) configuration diagram.

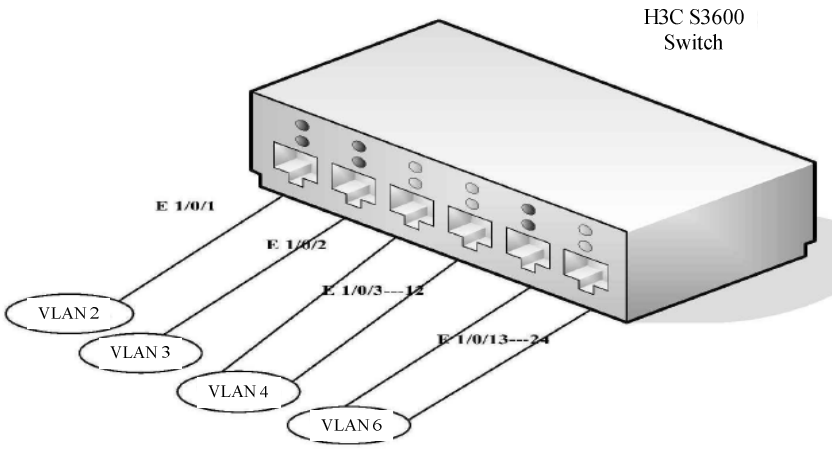


Figure 3 : Enterprise VLAN configuration diagram

(3) Intrusion detection and prevention technologies

Intrusion Detection and Prevention System[4] can compensate firewall technology. It makes network intrusion detection and feedback mainly based on certain security monitoring strategy for the entire computer system or network system. It ensures the integrity and confidentiality of safety of network resources, expands the capacity of the network security monitoring and identifying attacks. IPS technology is an active, intelligent anti-intrusion detection system.

ANALYSIS OF ENTERPRISE NETWORK SECURITY SYSTEMS

IP security protocol

Network is a relatively complex environment with many dangerous problems, such as Trojan viruses. In order to ensure the safety of the network system, the network security protocols play an important role in the creation of a secure network system.

(1) L2TP Protocol

Based on industry standard IETE, Microsoft and Cisco proposed the L2TP security protocol[5], whose block diagram is showed in Figure 4. L2TP offers legal definitions of data frame, supports transmission of data frame in PPP link layer, also supports a variety of protocols, including IP, AppleTalk, etc.

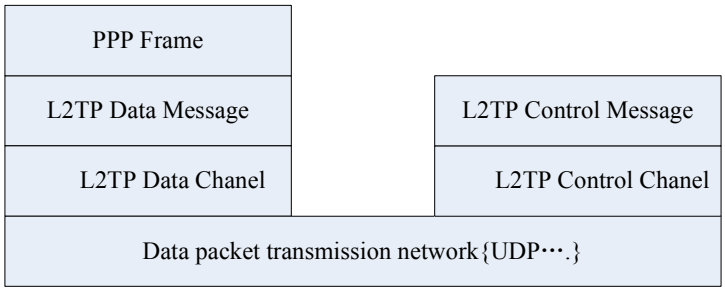


Figure 4 : Block diagram of L2TP protocol

L2TP protocol is widely used in virtual private network. The agreement describes the relationship among PPP data frame of the network, the data channel and channel control. PPP data frames can be on unreliable data channel, but the control message can only be transmitted over a reliable data channel, and data in secure data channel cannot be modified.

(2) IP security protocol

IPSEC (IP Security) protocol suite[6] is a security protocol developed by the Internet Engineering Task Force, is to provide high quality, workable, safe and reliable data transmission based on cryptography for both ends of the communication, to ensure integrity, flexibility and authenticity of data transmitted over the network. IPSEC protocol consists of two operating modes, one is transport mode when AH or SEP is placed between the header and transport protocol; the other is tunnel mode[7] when AH or SEP is placed in front of the header and regenerate a new IP header, with the original data encrypted for higher security and smaller occupation of transmission bandwidth, so a better transmission performance. Figure 5 is a package comparison of transport mode and tunnel mode.

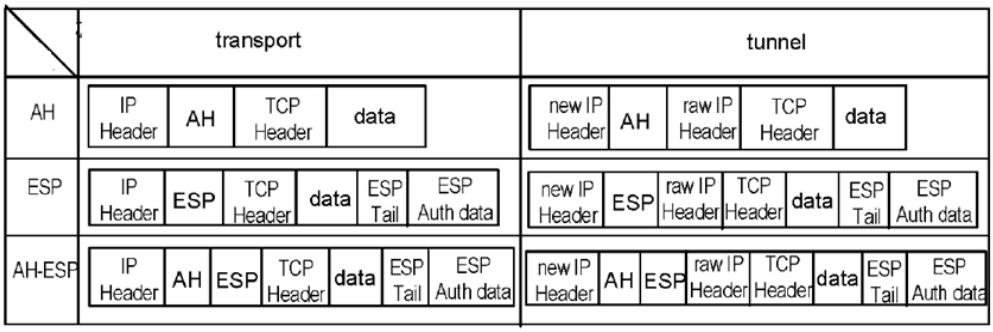


Figure 5 : package comparisons of transport mode and tunnel mode

(3) SSL Protocol

SSL (Secure Sockets Layer) protocol[8], widely used in between the browser and the server, is mainly for identity authentication, and to provide encryption of data for the data link, authentication, and other functions. Secure Sockets Layer protocol is applied between sequence protocol and TCP / IP, mainly composed by the record protocol, the handshake protocol, warnings, and key change agreement protocols. SSL protocol workflow includes two aspects, first server authentication phase, followed by user authentication stage, providing a variety of services including authentication, anti-theft, anti-tampering.

Situation analysis of enterprise network security

The development of computer network applications also brings some problems such as the invasion of illegal users, the enterprise's internal data theft, hackers using virus spread to destroy data on the corporate network, installing listening devices in enterprises' communications link to intercept corporate information, etc., which increases the risk of network application as well as results great loss for the development of enterprises.

Thus it is necessary to have a detailed understanding of enterprise network topology as well as the characteristics of business and enterprise security needs. Enterprise network security can be realized with VLAN technology used to achieve security isolation between different networks within the enterprise, rational distribution of firewall technology, deployment of intrusion prevention system to make up for lack of firewall technology, and network-virus solutions in addition to backup and analysis of and enterprise data network[9]. To solve the network risk, overall complementation and system construction including application, management, network even in physical layer, then can ultimately reduce the potential risk, develop a viable, useful security network. The design and solutions of enterprise network security depend on scientific technology, and analysis of physical layer, network layer analysis, management analysis according to the security needs of the network, full realization of the increased flow of data while saving bandwidth resources, protection of the internal network resources and users' system. This will ensure the reasonableness and usability of the enterprise network system.

CONCLUSION

With the progress of computer network application level, network scale is also gradually expanded, and the number of web-users is dramatically increasing. Along with the convenience computer network bringing to the enterprise, the network security issues cannot be ignored. More and more factors threaten to enterprise security and development. So the enterprise network security has become more important issue, and the foundation for smooth running of various companies. Once suffered a virus infection or hacker attacks, the entire enterprise network systems might be affected, which leads to paralysis of larger enterprise networks, resulting in economic losses of enterprises. In this paper, through analysis in the key technologies and protocols in computer networks, existing problems in enterprise and solutions, a conclusion has been made that the design and management of enterprise network security is dependable on scientific planning and security needs analysis, so as to establish a more secure computer network security system.

ACKNOWLEDGEMENT

Project supported by Technology Research Project of Henan Province (Grant No. 122102210505, 132102210434); Key Projects of Scientific Technological Research of Henan Province (Grant No.12A520026, 14A520086).

REFERENCE

[1] Jiang Bin; Analysis of application of computer network security system in the meteorological communications [J], Software, **01**, 96-97 **(2014)**.

[2] Shen Zhiling; Discussion on security technology of computer network [J], Journal of Henan Science and Technology, **17**, 13-14 **(2014)**.

[3] Xu Yan; On the application of computer network security systems in meteorological communication [J], Telecom World, **18**, 3-4 **(2014)**.
[4] Cheng Youwang; Analysis on establishment of computer network information security system [J], Science & Technology Information, **24**, 19 **(2014)**.
[5] Han Chao; Analysis of enterprise network security management [J], Digital Technology and Application, **07**, 181 **(2014)**.
[6] Chen Ning, Li Zhilei; Analysis of application of computer network security system in the meteorological communications [J], Information & Communications, **06**, 98 **(2013)**.
[7] Wang Weiping; Research on application of network security technology in an enterprise network [D], University of Electronic Science and Technology of China, **(2010)**.
[8] Song Guohua; On the design and implementation of computer network security system in a certain corporate [D], University of Electronic Science and Technology of China, **(2012)**.
[9] Shen Zhiling; Discussion on security technology of computer network [J], Journal of Henan Science and Technology, **17**, 13-14 **(2014)**.