Strategy of Enterprise Network Security Protection Based on Cloud Computing

Qiang Wang
Center of Education Technology and network, Jilin Engineering Normal University, Changchun, China

*Corresponding author e-mail: wq@jlenu.edu.cn

Abstract. With the rapid development of science and technology in modern society, enterprises are developing in the direction of more openness, standardization and network interconnection. Although enterprises have realized the informationization of production and operation earlier, their network information security architecture is still not perfect, and the existing network information security model cannot be fully applied to some enterprises, which has made some enterprises unable to fully protect their network information security. Therefore, there is an urgent need for a more targeted network security model for enterprises to enhance the security strength of their network information systems. Based on the analysis of the security situation of the enterprise network information system, this thesis combines the security status of the enterprise information system and the main threats to construct a cloud computing-based enterprise network security model. This model is a classic network security model of dynamic closed-loop management consisting of four modules: protection, detection, response and recovery. On this basis, a risk-hardening security hardening scheme is designed and implemented, and the practicality and effectiveness of the improved enterprise network security model are verified. The research in this thesis proves that the improved enterprise network security model can make domestic companies 'network information systems more robust, and also provides a reference basis for the construction of other small and medium-sized enterprises' network information systems. Instead, it is developing in the direction of combining technical and management methods to effectively improve the level of enterprise network information security.

Keywords: Cloud Computing, Network Security, Information Security, Management Strategy

1. Introduction
The rapid development of global network technology and information technology has driven the development of informatization in Chinese enterprises. Compared with the traditional enterprise management model, modern information-based enterprises can reduce production and management costs, effectively improve business processing capabilities, mobilize enthusiasm for technological
innovation, improve overall management level, and greatly reduce the internal randomness of the enterprise. However, informatization is also a double-edged sword. Enterprise resources are subject to security risks such as tampering, forgery, and theft, which can easily lead to information loss, leaks, and even virus transmission, exposing enterprises to security threats, and adversely affecting enterprise information construction.

The development of Internet technology has spread all over the world. Data is playing an increasingly important role in people's lives, and it has become an indispensable thing in people's lives. The popularity of electronic devices such as mobile phones and computers has led to an explosive growth in data volume. The rapid growth of data volume and the different types of data have placed higher requirements on storage technology [1-2]. How to store such a large amount of data and manage it has become a difficult problem that people need to solve urgently. In this context, the concept of cloud computing is proposed. As a computing model, cloud computing is able to store and manage today's explosively growing amount of data, and distributed storage technology is indispensable [3]. Distributed storage technology in the cloud computing environment has a series of advantages such as strong scalability, high reliability, very practical, and affordable price. It can be said that the distributed storage technology in the cloud computing environment is the future trend of the development of storage technology. Occupy an important position in the Internet age. Combining with the definition given by many scholars to cloud computing, the author believes that cloud computing mainly refers to a new computer method based on network technology. By comprehensively using heterogeneous, autonomous and other services on the Internet, it can provide different users with corresponding services according to different needs. Computing services [4]. It can be seen that the computing power can also achieve the enterprise's network security protection. It uses network technology to achieve long-distance circulation, which is flexible, convenient, and simple to operate. For resource monitoring, cloud computing is a close combination of server management functions and related data, and extensively collects dynamically changing data information and fully integrates it, and then builds a more efficient and effective data service basis. Based on resource monitoring, cloud computing can also collect user information in a timely manner and provide timely feedback. This is beneficial to the subsequent integration of resources and enhances the accuracy and reliability of calculations [5-6].

With the application of cloud computing technology, enterprise network security protection is more efficient and reliable, especially with the help of cloud computing, it can generate information about network security at the first time, and accurately collect information content in the process of enterprise management. At the same time, through the use of perfect and refined data collection, scientific and efficient financial management of colleges and universities. In the process of enterprise modernization management, various departments can use the model proposed in this article to obtain a comprehensive and objective understanding of the network security status of each department of the enterprise, so as to ensure that the enterprise can operate in a secure network security environment.

2. Method

2.1 VLAN Topology Design
The core network, as the operating core of the local network system, determines the performance of the entire system network. According to statistics, in a well-functioning and full-service network, communication between subnets and internal communication within subnets each account for about 50%; and with the development of multimedia technology, multimedia homepages, video on demand (multicast) are widely used. These must occupy a large amount of backbone bandwidth; and the adoption of virtual network technology, the traditional subnet concept has changed, so that a subnet can be distributed throughout the network, resulting in the internal communication of the subnet also going through the backbone network; therefore, the traffic passing through the backbone network Will account for more than 80%, which requires the backbone network must have a very high transmission rate, to avoid congestion to the greatest extent. As the ultimate exit channel, the collapse of the
backbone core network means the collapse of the entire office network. Therefore, the backbone network design of this bureau must adopt a mature standardized scheme to ensure its stability. Based on the network design principles analyzed above, the new business requirements and characteristics of the Water Resources Bureau and the defects in the network design, the network core is upgraded, and a unified high-performance, high-availability platform is built on the platform of the network infrastructure. The absolute guarantee of operation prepares for the implementation of new business strategies in the future [7]. Upgrade the original core into a H3C S 7506E switch and configure two SalienceVI-Lite switching routing engines. The switch can provide up to 768Gbps backplane bandwidth and 492Mpps data forwarding rate, provide efficient data exchange communication capabilities, and build into an integration. It has a high-efficiency, low failure rate, high security, redundancy, and scalable network platform.

2.2 Enable Firewall
There are many user branches and frequent peripheral accesses, and remote network management is difficult to achieve. In order to ensure the security and efficiency of the core backbone network, firewalls are used here for boundary management [8]. At this time, we choose a firewall to provide high throughput, and there are no bottlenecks in border deployment. Dividing security domains on demand and clearly planning network boundaries: provide flexible packet filtering strategies to precisely control mutual access relationships; perform packet folding detection on VPN data packets. Ensure data communication security. The extremely high number of concurrency guarantees the effectiveness of the firewall. Without affecting the normal data transmission, the device can easily deal with millions of packets / second of DDoS attacks. Supports IPV6, guarantees the scalability of the equipment in the future, and makes a smooth transition for equipment upgrades. Five VPN types and secure encryption mechanisms ensure the security of the public Internet access to the internal network. Even outside, you can safely access internal network resources [9-10]. External threat defense: IPS intrusion prevention, AV gateway anti-virus, AS anti-spam, triple protection to ensure the security of the internal network.

2.3 Set up an Antivirus System
Network traffic monitoring computer information network systems have been widely used in enterprise systems. When users go online, they will exchange a variety of data, so they are vulnerable to various viruses[11]. Contact business often uses email. This process is susceptible to viruses and then spreads in the corporate LAN. Only by improving the prevention ability and strengthening control in all aspects of the information network can we prevent and control the virus effect [12]. Therefore, if an enterprise wants to realize the security protection of network security, it must strengthen the establishment of its antivirus system, monitor the operation of the system in real time, play the role of the antivirus system to prevent and control the spread of virus, and improve the protection ability of the network security of the enterprise. At the same time, when establishing an anti-virus system, enterprises can implement a distributed solution to unify anti-virus technology with other network virus protection systems and monitor various systems of the enterprise in real time. Once problems are found, they are analyzed in time and eliminated in time. To ensure the safe operation of enterprise systems.

3. Experiment
The first step is the collection and recording of data. This article collects network security data of major enterprises. The data mainly includes operational data, information data, and development data. In particular, the data of the new generation of information technology on the frequency of network attacks must be comprehensive in the development data collection, extract useful management technical characteristics from it, and accurately record their characteristics and original data.

The second step is to determine the correlation data and range of values as well through distributed computing in the cloud. The above-mentioned probability algorithm is used to search for the optimal
value and obtain the relevant features to realize the determination of the relevant data. Obtain the relevance of the data and determine whether the factor is related to the management mode. The value of obtaining the accuracy rate usually refers to the prediction result. It can indicate that when we make a prediction, the prediction result and the related probability can see the correctness of cloud computing for network security protection.

The third step is to use cloud computing for distributed computing to process network security data. By accurately understanding the current status of corporate network security, scientifically analyzing the problems and challenges of the management model, in-depth analysis of the main reasons affecting network security, and on this basis, exploring specific countermeasures to improve protection of network security.

4. Discuss

4.1 Security Analysis of Operating System
At present, the operating systems chosen by corporate users are mainly Unix operating systems, Linux operating systems, windows series operating systems, and Macintosh series operating systems. According to data from the 2008 National Network Security Survey Report, 7072 companies surveyed the use of enterprise information networks. The operating system is mainly the Windows operating system, of which WindowsME / 98 accounts for 4.3%, Windows XP accounts for 45.3%, Linux / Unix operating systems account for 29.6% and 15.6%, MacOS accounts for 2.4%, and other accounts for 2.8%, as shown in Figure 1:

![Figure 1. China's operating system usage](image)

These operating systems have their strengths in design and use. However, there are certain security vulnerabilities. Enterprises can decide which operating system to use according to the security level required by the actual computer system. Security level. For a computer system with only a simple client program, a lower security level but more friendly interface Windows XP series operating system can be used. No matter what operating system is used, it is impossible to achieve absolute security. Fortunately, various operating system developers will make timely corrections (patches) according to the vulnerabilities of their operating system products. Another effective way maintains computer
system security. On the basis of maintaining the stability of the operating system itself, as a system administrator, it should also formulate appropriate access policies for resources and files for the system, and through these policies, to deny malicious attacks and unauthorized access. The main policies in the operating system should include: account management policies, resource access policies, file access policies, audit policies, domain policies, group policies, log policies, etc., to develop a set of installed operating systems that meets actual requirements. Strategies can greatly enhance the security of the operating system and detect attacks against the operating system in a timely manner.

4.2 Enterprise Cyber Security

Computer network is the product of the development and combination of computer technology and communication technology. Group computers and other terminal equipment are connected to each other through communication subnets. To achieve mutual communication and resource sharing, such a system is a computer network. And the enterprise information system is based on the network foundation. According to the survey results, at present, the most widely used network security products in information systems in China are firewalls and computer virus prevention products, accounting for 82% and 98% of the users surveyed, respectively. The utilization rate of other security products is generally low, all below 30%, as shown in Figure 1:

Table 1. The use of security products in China

| Security Product Type       | Frequency |
|-----------------------------|-----------|
| antivirus software          | 98        |
| firewall                    | 89        |
| intrusion detection         | 22        |
| physical or logical isolation| 19        |
| identity products           | 38        |
| Access control              | 12        |

Most local area networks currently use the TCP/IP protocol. The protocol strives to be simple and efficient in its implementation. However, security factors have not been fully considered, because that would increase the complexity of the protocol, so TCP/IP itself is not secure by design. The sharing of the communication medium in the local area network and broadcast communication make the communication process in the local area network extremely easy to be monitored. If the sensitive information transmitted on the network, such as system login passwords, confidential files, etc. is illegally monitored and hijacked without the administrator's knowledge, it will bring unpredictable losses to the enterprise system.

5. Conclusion

The network security protection mode of the enterprise management is of great significance for the healthy development of the enterprise. Compared with the older and traditional network protection mode, this paper proposes that the network security protection mode based on cloud computing can more effectively protect the information security of the enterprise, and for enterprise management. In other words, the implementation of cloud computing construction is essentially an important demand based on the modern management innovation of the enterprise, and it is also the key to give play to the advantages of information technology and improve the management level of the enterprise. In the specific analysis and understanding of the status of corporate network security construction, it focuses on starting from various issues existing in the current process of corporate network security construction, and proposes targeted and practical solutions based on objective problems to truly improve the level of corporate management. And effectiveness serves the current enterprise reform and innovation.
References
[1] Benjamin Heintz, Abhishek Chandra, Ramesh K. Sitaraman. Optimizing Timeliness and Cost in Geo-Distributed Streaming Analytics[J]. IEEE Transactions on Cloud Computing, 2017, PP(99):1-1.
[2] Subhadeep Sarkar, Subarna Chatterjee, Sudip Misra. Assessment of the Suitability of Fog Computing in the Context of Internet of Things[J]. IEEE Transactions on Cloud Computing, 2018, 6(1):46-59.
[3] Rodrigo N. Calheiros, Enayat Masoumi, Rajiv Ranjan. Workload Prediction Using ARIMA Model and Its Impact on Cloud Applications' QoS[J]. IEEE Transactions on Cloud Computing, 2017, 3(4):449-458.
[4] Jianguo Chen, Kenli Li, Senior Member. A Parallel Random Forest Algorithm for Big Data in a Spark Cloud Computing Environment[J]. IEEE Transactions on Parallel & Distributed Systems, 2017, 28(4):919-933.
[5] Maria Alejandra Rodriguez, Rajkumar Buyya. A taxonomy and survey on scheduling algorithms for scientific workflows in IaaS cloud computing environments[J]. Concurrency & Computation Practice & Experience, 2017, 29(8).
[6] Tiago Gama Rodrigues, Katsuya Suto, Hiroki Nishiyama. Hybrid Method for Minimizing Service Delay in Edge Cloud Computing Through VM Migration and Transmission Power Control[J]. IEEE Transactions on Computers, 2017, 66(5):810-819.
[7] Muhammad Qasim Ali, Ehab Al-Sheer, Taghrid Samak. Firewall Policy Reconnaissance: Techniques and Analysis[J]. IEEE Transactions on Information Forensics & Security, 2017, 9(2):296-308.
[8] Yuzhu Cheng, Weiping Wang, Jianxin Wang. FPC: A new approach to firewall policies compression[J]. Tsinghua Science & Technology, 2019, 24(1):65-76.
[9] Cornelius Diekmann. Verified iptables Firewall Analysis and Verification[J]. Journal of Automated Reasoning, 2018, 61(2):191-242.
[10] Juntao Chen, Corinne Touati, Quanyan Zhu. A Dynamic Game Analysis and Design of Infrastructure Network Protection and Recovery[J]. Acm Sigmetrics Performance Evaluation Review, 2017, 45(2).
[11] Fernando Morales, Marc Ruiz, Lluís Gifre. Virtual Network Topology Adaptability Based on Data Analytics for Traffic Prediction[J]. IEEE/OSA Journal of Optical Communications & Networking, 2017, 9(1):A35.
[12] Barbara Barbé, Cedric P. Yansouni, Dissou Affolabi. Implementation of quality management for clinical bacteriology in low-resource settings[J]. Clinical Microbiology & Infection the Official Publication of the European Society of Clinical Microbiology & Infectious Diseases, 2017, 23(7):426