Application of Big Data Technology in Three-dimensional Defense System of Digital Campus Information Security

Hongying Liu

Department of Computer Science and Engineering, Guangzhou College of Technology and Business, Guangzhou, China

*Corresponding author e-mail: liuhhying415@163.com

Keywords: Big data technology, digital campus, information security, defense system

Abstract: This article mainly takes the construction of big data technology digital campus as the background, through the research, analysis of various security problems in the construction and application of digital campus, and the feasibility study of solutions, it is proposed that digital campus construction can be used in digital campus construction. Refer to the reference security solutions to provide technical support and management suggestions for the construction of secure digital campus application systems. Through the deployment of security solutions, the information network security problems faced by digital campuses in universities can be solved to a certain extent, and the quality of digital campus construction can be improved.

1. Introduction

Under the background of big data, the construction of digital campus is an important work of colleges and universities at present [1]. It is an integral part of college construction and talent training. It is of great significance to improve the school's teaching, research, management and service level. With the development of computer technology and the popularization of the Internet, digital technology is changing the social environment on which human beings depend, making human living and working environments more digital, and has also brought about huge changes in the way people live and work. This new and more colourful and freer lifestyle brought by digital technology and digital products is habitually called "digital life". With the development of computer and communication technology, the digital campus construction of universities has also made great progress. Especially in the past ten years or more, driven by the national "211 Project", "985 Project" and related plans, universities have made great progress in the construction of network infrastructure and information systems. Taking Tsinghua University as an example, a good network environment has enabled the campus network application system and users to reach a considerable scale [2]. The network users include teachers, students, staff, workers and other types of people in the school and uncountable out-of-school visitors. Online office, online management, online teaching and online services.

2. Demand analysis

2.1. Business security and stable operation requirements

On the basis of meeting the basic security requirements of the network, the campus network itself and the services carried by it must be guaranteed to operate safely and stably. To ensure that each device runs normally and to detect and defend against various network attacks in a timely manner, these are the most basic network security requirements. At the same time, in order to fully manage the network, it is also necessary to effectively monitor and manage various online behaviours and traffic on the network. In general, there are the following [3]:

1) Requirements for the security of confidential information transmission. For the transmission of key data such as financial information, the security of data transmission must be considered, and encrypted transmission should be considered. 2) can effectively protect the campus network and its

key equipment and functional areas in the network, and effectively ensure that data and information can be safely transmitted. Can detect network viruses and take certain precautions, can record and analyse attack behaviours on the network, implement effective monitoring, information filtering, intrusion detection (and isolation control. 3) can effectively manage network traffic, online games, stocks, chats, Effective monitoring of P2P downloading, viewing of bad information, and posting of illegal speech. 4) Must have effective management and control capabilities for various illegal users to access the network and internal data of the network. 5) Develop effective network security management measures and unify security. Management and regulate network access behaviour.

2.2. Data security requirements

Considering the premise of improving the quality of teaching and services and optimizing the integration of various resources, data security issues in the construction of digital campuses are considered. The digital campus is driven by the school's business needs. Multiple business systems implement different service functions based on different permission policies to form a unified digital service platform. Therefore, it is required to consider the following factors in the construction of data security in the construction of digital campuses: 1) The data centre's demand for environmental security. Data centres should be built in areas that are relatively high and not vulnerable to the threat of floods, lightning strikes, and other natural disasters. The building design should meet the requirements of safety, energy conservation, environmental protection, etc., and meet national standards to ensure that it can provide stable and good data services for digital campus operations. 2) Equipment technical requirements. The requirements of digital campuses for data services determine that their data security depends to a certain extent on the advancement and stability of existing equipment technology. Based on security and stability considerations, and the need for large-capacity and high-speed transmission, the direct connection of digital campus data centres can be considered for the construction of digital campus data centres. Devices can use relatively advanced SAN storage systems.

3. Design ideas

To meet the needs of network security, it is necessary to focus on network security when designing the network. According to the security requirements of applications and services carried on the network, taking into account the long-term needs, the overall network is divided into different security areas and different security settings are made. Each area is securely isolated by means such as a firewall to achieve network design. At the beginning, it has the effect of strong security precautions. Can be divided into: WAN area, Internet service area, remote access area, network management area, data centre area, internal office area and so on. As shown in Figure 1.

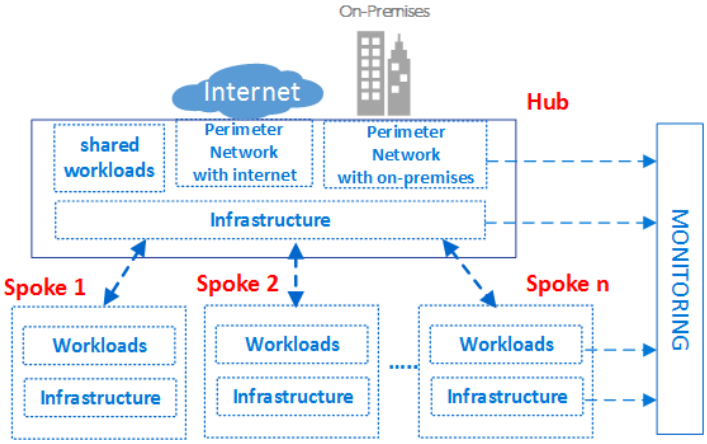

Figure 1. Schematic diagram of campus network security zone division.

4. System design and implementation

4.1. Network Security Solution Design and Implementation

Considering the current status of network security deployment in colleges and universities, combined with the aforementioned guiding ideology and design ideas, the digital campus network security system is designed according to the following 4 parts: 1) Design of remote access schemes. Because of the existence of multiple campuses, through the design of a remote access security scheme, the security of information transmission between campuses can be met, and the secure transmission of confidential data information between different campuses can be facilitated. 2) Border security scheme design. This solution aims to solve the regional border security precautions of the divided security areas. Depending on the security requirements of different regions, you can treat them differently and deploy corresponding security policies. 3) Intranet security scheme design. It is mainly aimed at network security prevention within the campus network, and focuses on solving internal network attacks, malicious access, and virus transmission. 4) Management plan design for monitoring network behaviour. It is mainly aimed at monitoring the online behaviour inside the network, limiting P2P traffic that occupies a lot of bandwidth, and can trace the source of illegal online behaviour.

4.1.1 Design and implementation of remote access security scheme.

The current technologies for remote access are: reverse proxy technology, VPN technology [4]. Among them, the reverse proxy is low in cost and easy to deploy, and has been adopted by some universities. However, it mainly uses user name and password verification to ensure security and weak security. VPN technology is widely recognized for its safety, reliability, efficiency, and stability. Based on comprehensive considerations, it was decided to adopt a mature, flexible and secure virtual private network (VPN) technology to meet the security needs of remote access between multiple campuses. Deploy online. At the exit of the campus network, deploying the SSLVPN gateway as shown in Figure 2 cannot only implement the remote access function of the network, but also solve the problem of security protection. The data transmitted in this way is transmitted through the VPN channel after being encrypted, which can effectively protect the information and data security of the core business of the network.

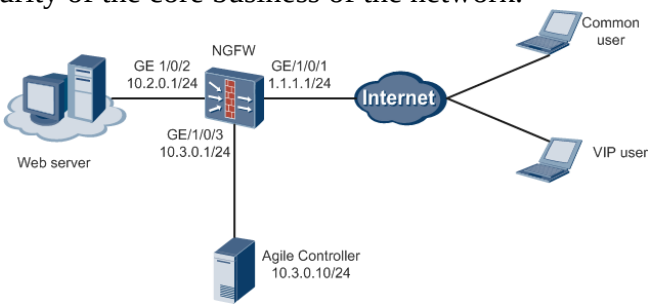

Figure 2. Campus Network SSLVPN Gateway.

To solve the network boundary security problem well, we cannot rely solely on a single technology. We must use a combination of multiple technologies to address the crux of the problem. Therefore, it was decided to adopt a border security design scheme combining firewalls, antivirus systems, and intrusion prevention systems (IPS). First, according to business characteristics, divide the network security area, deploy the above security system at the network boundary, form a comprehensive security defense system from the data link layer to the application layer, and implement deep and comprehensive network security protection that can be detected and controlled. It can effectively implement functions such as combating the spread of network worms, defending against network attacks, and limiting P2P traffic. The firewall is used to implement the function of dividing the network security zone. It provides access control based on the layer 3 network address and the service port of the transmission control layer, which effectively combats various security problems such as denial of service attacks and IP address spoofing [5]. Deploy the firewall at the

campus network exit, integrate the antivirus module, and deploy an intrusion prevention system (IPS). In the campus network, the Internet access area, intranet, and data centre can be divided by firewalls and isolated from each other. According to the security requirements of the business, the deployed security rules and policies must be different. To achieve different levels of security protection. As shown in Figure 3.

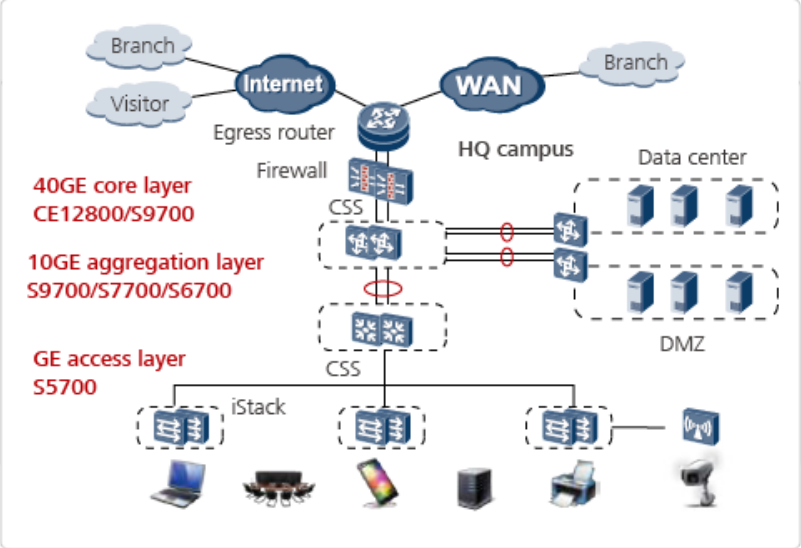

Figure 3. Design model of border security scheme.

4.1.2 Design and Implementation of Intranet Security Solution.

Adopt an endpoint admission defense mechanism to restrict or deny insecure terminals from accessing the network, and improve the active defense capability when the network accesses the terminal. By integrating terminal security measures and network security measures, a unified joint security system is formed, and a single-point passive defense and decentralized management network is upgraded to an overall active defense and centralized management network, which effectively improves network security defense capabilities. Adopt a firewall-centric internal network access control scheme, integrate the firewall module into the switching routing device, and accurately control access between different VLANs and ports through the firewall and the switch with port isolation. Therefore, data transmission security between terminals in the same security area is guaranteed. In addition, choose a switching device with port security features. This security feature mainly refers to access control technology, access security technology, preventing ARP spoofing, DHCP service protection, preventing intermediate attacks, routing protocol attack protection, and so on [6].

4.2. Data Security Solution Design and Implementation

1) Use firewalls for secure partitioning and access control. To achieve the security isolation of each partition, in addition to preventing the spread of security problems, different security policies can be implemented in different partitions. These characteristics are consistent with the characteristics of the aforementioned network security part. However, as the entrance of the data centre, the firewall can protect the data centre from illegal access and malicious attacks by formulating corresponding policies for access control. 2) Deploy an intrusion prevention system (IPS) to detect denial-of-service attacks, application-layer attacks, and illegal P2P traffic online in real time, and perform corresponding blocking operations to provide deep protection for the data centre.

For financial services, card services and other important business data services, we must consider the use of relatively more reliable dual-machine hot standby or even cluster load balancing technology to ensure the absolute security of data and fast recovery and uninterrupted service in the event of data loss. Machine hot standby deployment. Generally, dual-system hot backup can be implemented by using two servers sharing the same storage device. The two servers can work in

different ways such as one master, one slave, and mutual backup. They are assigned a virtual positive address. From the outside world's perspective, it is as if only one server is providing the service, and the two servers allocate service requests according to different deployment forms. The two servers usually use a private network to connect the heartbeat cable to detect the working condition of the other server.

5. Virtual system test

5.1. Virtual private network remote access function test

Test objective: To verify the function of external network users accessing internal network resources through the virtual private network in the solution. Test environment: Establish the experimental environment through the SSLVPN building software OpenVPN. One host in the campus network installs OpenVPN software and configures it to simulate a VPN server; the other host is outside the campus network and also installs OpenVPN software to configure as a VPN client; both hosts can be in their respective network environments Connect to the Internet normally. As shown in Figure 4.

Figure 4. Campus virtual private network test model.

Step 1: Install the OpenVPN software on the two hosts separately. Here we choose to use its 2.0 version. After installing the software according to the default steps, check the network equipment of the system. You will find that there is one more TAP-Win32AdapterV8 virtual network card. Disconnected when connected. Step 2: Configure the server and client and the security certification centre. Since OpenVPN sets the security certification centre on the server, you can configure the server and client respectively.

5.2. Firewall Security Zone Policy Function Test

Test results: By configuring a zone-based firewall policy, you can flexibly grasp the requirements for network access in different security zones, while effectively protecting the internal network from external intrusions, you can also achieve flexible inter-domain and intra-domain access control.

5.3. Intrusion Prevention System (IPS) Functional Test

First ping 172.18.1.1 through the host, and you can ping. Install SDM on the host and start it. Enter the router management address 172.18.1.1 as prompted and enter the username admin and password cisco to connect to the router, as shown in Figure 5.10. In SDM, through the visual configuration interface, create an IPS rule under the guidance of the IPS Rule Winzard wizard, and choose to set the port for IPS detection. Then, select the signature database file to set the types of network attacks that IPS recognizes and blocks. The name is selected here as the feature of ICMP Echo Req, and the defense behaviours for the feature are defined as alarm (issue an alarm) and drop (drop the packet). After the configuration is complete, it is applied to the router. Configuring corresponding behaviour characteristics to defend against different network attacks can effectively prevent network attacks. The rich signature database attached to IPS has defined many common attack behaviours. Through the continuous expansion of the signature database, various new network attack behaviours can be effectively blocked, which plays a good role in protecting campus network security. It shows that the deployment of IPS plays a vital role in campus network security

in the construction of digital campuses.

6. Conclusion

With the development of information technology, the speed of digital campus construction will become faster and faster. Informatized universities will surely be one of the concrete manifestations of the comprehensive strength of major universities in the future. A secure digital campus will play an important role in all its businesses. The role of security research and application of digital campus construction provides a good reference for the security construction of digital campus construction.

References

[1] Qi, J., & Lan, Y. Network financial fraud risk assessment system based on big data analysis. 13(12) (2016) 9335-9339.

[2] Lang Huang, Chao Wu, Bing Wang, & Qiumei Ouyang. Big-data-driven safety decision-making: a conceptual framework and its influencing factors. Safety Science, 109(2018) 46-56.

[3] Elaiw, A. From crowd modeling to safety problems. comment on "human behaviours in evacuation crowd dynamics: from modelling to "big data" toward crisis management" by nicola bellomo et al., 18(2016) 33-34.

[4] Jun Liu, Xin Wang, Asad J. Khattak, Jia Hu, & Jiaqi Ma. How big data serves for freight safety management at highway-rail grade crossings? a spatial approach fused with path analysis. Neurocomputing, 181(C) (2015) 38-52.

[5] Tiwari, V. S., & Arya, A. Horizontally scalable probabilistic generalized suffix tree (pgst) based route prediction using map data and gps traces., 4(1) (2017)23.

[6] Ruidong, Hitoshi, Asaeda, & Xiaoming. A distributed authentication and authorization scheme for in-network big data sharing., 3(4) (2017)226-235.