Research and analysis on hierarchical management balancing strategy of intelligent VPN in colleges and universities under hierarchical protection 2.0 background

Yunjia Li[a], Xinxiang Xiao[b*], Zhiyong Zhang[c], Zhixin Chen[c]
[a] Business College, Hunan Normal University, Changsha, Hunan, China; [b] Department of Principal's Office, Hunan Normal University, Changsha, Hunan, China; [c] Department of Information Center, Hunan Normal University, Changsha, Hunan, China

ABSTRACT

With the rapid development of information technology, online office and study has been applied by more and more colleges and universities, but the convenient off-campus access has brought a great threat to the network security. In order to solve this problem, this paper proposes an efficient hierarchical management balancing strategy for complex VPN under hierarchical protection 2.0. Through the process design of VPN, unified identity authentication and reverse proxy, the practical case of this strategy has been realized. The network security level of users has been significantly enhanced. In 2021, our school won the title of excellent defensive unit in the offensive and defensive exercises held by Hunan Provincial Public Security Department.

Keywords: VPN, network security, level protection 2.0, balancing strategy

1. INTRODUCTION

At present, the construction of key systems such as graduate management, financial management, educational administration management and one-card has begun to take shape. With the further development of office automation (OA), more and more staff put forward the need to operate office computers on the Internet. There are also many software vendors that require remote operation of application system servers. Therefore, secure remote access is an urgent problem to be solved. After investigation, most colleges and universities have built VPN system to provide convenience for teachers and students to access the Intranet system outside the campus. However, complicated operation, repeated login and low efficiency are common. In recent years, there are also some schools to improve the user experience of remote access by teachers and students. The construction of WEBVPN remote access system allows users to access the school system after authentication in the browser. This measure does facilitate the remote access of users. However, the problems of too large scope of authority and weak security are more prominent.

How to make teachers and students access the campus system quickly and conveniently under the premise of ensuring safety and reliability and clear authority, remote operation of office computers and servers is a hot issue in the field of remote access resources in colleges and universities. Under the background of the formal implementation of network security level protection 2.0, this paper investigates the Internet access technology of domestic universities. Combining with the strong demand of teachers and students in practical work, the paper puts forward a balanced strategy of intelligent VPN hierarchical management in colleges and universities. This is used to resolve the imbalance between user experience and network security during VPN use.

2. NETWORK SECURITY LEVEL PROTECTION 2.0

At present, the information construction of all walks of life is in full swing, and the application of network information system in enterprises is more and more extensive. The state introduced the system of information security work, the strategy of network security level protection regulations, it aims to standardize the information security protection market, improve the level of information security protection. In 1999, China put forward the information system security protection grade standard. After that, it successively issued relevant information system security regulations. In 2007, "Information security

* 790975278@qq.com

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 125064S
 · 0277-786X · doi: 10.1117/12.2662581

level protection management measures" established level protection 1.0. In recent years, with the rapid development of information technology, big data, cloud computing, artificial intelligence and other new technologies have developed rapidly. The existing level of protection 1.0 no longer meets the requirements of the work. Therefore, in 2019, China officially released the network security level protection system 2.0, which marks China's network security level protection into the 2.0 era.

Compared with equal-insurance 1.0, equal-insurance 2.0 focuses more on active defense. The whole process of passive defense is safe and reliable, dynamic perception and comprehensive audit have realized the full coverage of traditional information system, basic information network, cloud computing, big data, Internet of things, mobile Internet and industrial control information system level protection objects. In addition to technical specifications, level protection 2.0 emphasizes the importance of network security management from five levels, including security management system, security management organization, security management personnel, security construction management, security operation and maintenance management.

3. THE CONCEPT OF VPN

Virtual Private Network (VPN) is a virtual private network[1-3]. It can create a channel on a public network, after layers of encryption and authentication, this channel can guarantee the security of virtual space on the network. It is VPN technology[4-6]. VPNs originate from business requirements, requiring large amounts of data to be transferred between the headquarters and branches. Each branch needs access to the resources of the head office. Important data is not suitable for transmission over the Internet. If the physical dedicated line is set up, the cost is extremely expensive, and the line is easy to be destroyed, thus, VPN technology arises at the historic moment[7]. The network virtual channel established by VPN technology can be encrypted during information transmission[8]. This also ensures data privacy to a certain extent. VPNS do not require the re-establishment of specialized physical networks[9]. It requires very little investment and has very significant safety effects.

4. OAUTH2.0 UNIFIED IDENTITY AUTHENTICATION TECHNOLOGY

OAuth (Open Authorization) protocol is an open standard. It is a complement to OpenID. It allows users to do so without providing a user's name and password. Third-party applications can access their resources on a website, such as user nicknames, profile pictures and other information. OAuth2.0 authentication and authorization technology are based on OAuth protocol. It focuses on version upgrades for ease of development. Oauth2.0 authorized login allows users managed by the platform to securely log in to third-party applications or websites. User authentication (showing passwords or other authentication methods) is completed by the Oauth2.0 system without the intervention of third-party applications. After a user is authenticated, a third party can obtain the user's interface invocation certificate (access_token). By using access_token, we can obtain the basic information of the current login user, the functions related to the user are implemented. The authorization process is shown in Figure 1.

(1) The application sends an authentication and authorization request. The user can navigate to the login authentication page. After the user authorizes the third-party application. The system redirects to the callback address specified by the application and takes the authorization temporary ticket code parameter.

(2) The system uses the API to exchange the access_token using code, client ID, and client secret.

(3) It can obtain basic user information and help users perform basic operations by the access_token interface.

5. REVERSE PROXY SERVICE

A reverse proxy is a server that accepts connection requests from users on the network[10]. The request is then forwarded to the corresponding application service on the network and the results obtained from the application service are returned to the requesting user client on the network. In this case, the server acts as a reverse proxy server[11-13]. Users accessing web applications through proxy servers do not need to change any configuration. It just needs to visit the website normally. Common reverse proxy tools include HAProxy, Fikker, Squid, Nginx, etc. This paper mainly uses Nginx as a reverse proxy tool for research[14]. It identifies the target address status through user-defined configuration and dynamically directs Intranet sites.

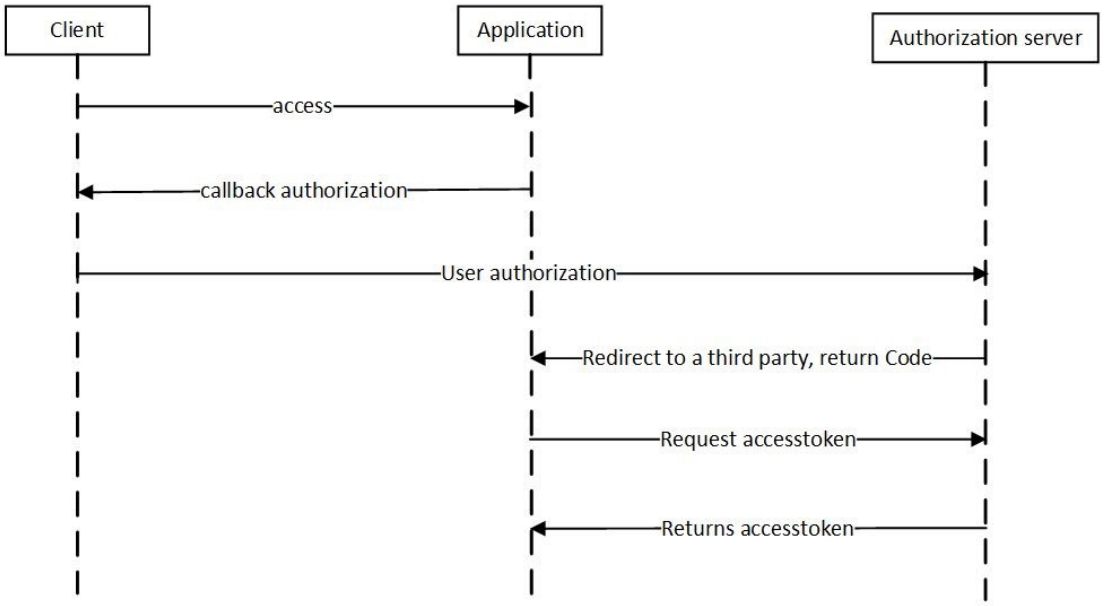

Figure 1. Authorization sequence diagram Oauth2.0.

6. THE BALANCING STRATEGY OF COMPLEX VPN HIERARCHICAL MANAGEMENT IS PROPOSED

According to the application requirements, a hierarchical management balancing strategy of intelligent VPN in colleges and universities is proposed under the condition of ensuring network security. This leads to solving the imbalance between user experience and network security guarantee in VPN use. The workflow is shown in Figure 2.

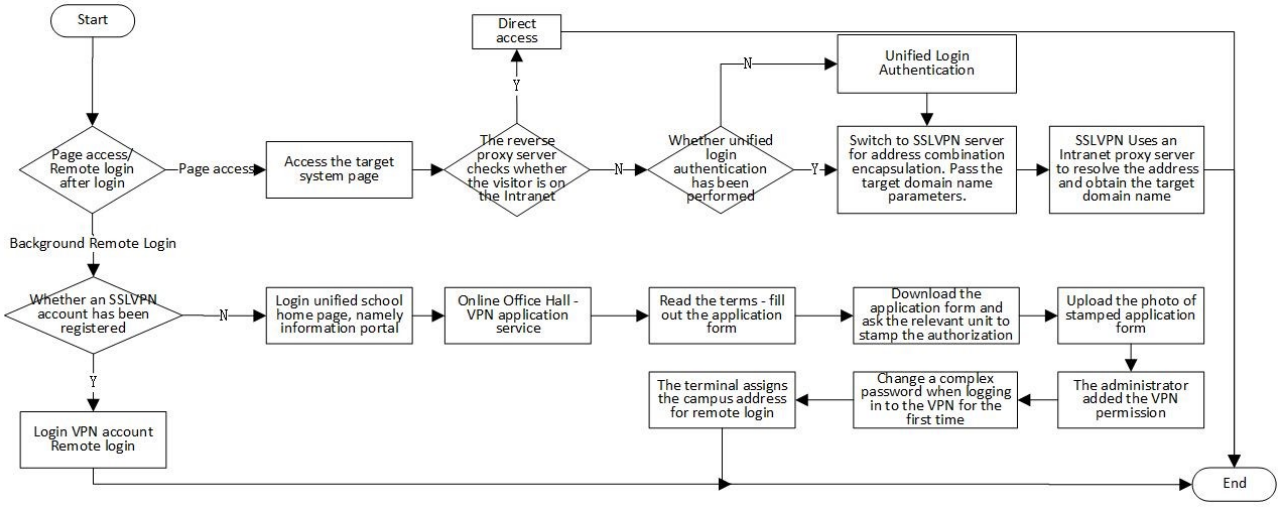

Figure 2. Flow chart of balancing strategy for complex VPN hierarchical management.

It can be divided into client SSLVPN and WEBVPN according to VPN demand and crowd. The former has higher permissions and can remotely log in to an IP server or PC. The latter accesses campus resources directly through the web.

6.1 WEBVPN workflow

(1) Log in sites of school. The reverse proxy server checks whether the visitor is on the Intranet. The visitor accesses the

Intranet directly.

(2) If the visitor is outside the campus, it determines whether the login has been authenticated (no second login is required). Otherwise, unified login authentication is required, and only the faculty and staff on campus can access restricted sites on the Internet.

(3) This switchs to the VPN server after you have logged in unified authentication. Through address combination encapsulation, the target domain name parameters are transmitted to the reverse proxy.

(4) The VPN server connects to the Intranet proxy server using a public IP address. It can access the Intranet directly by resolving the address and obtaining the target domain name.

6.2 Client VPN workflow

(1) If do not have an SSLVPN account, log in the school home page information portal module to apply for an SSLVPN account. Fill in the application form and submit it to the Information Center after being authorized and approved by the department.

(2) The information Center opens specific addresses, allocates permissions and manages them accurately according to needs. This prevents too many open permissions.

(3) If an SSLVPN account is available, it directly logs in to the client to perform remote working.

7. CONCLUSION

At present, the rapid development of information technology has put forward new requirements for our school's information work. With the continuous expansion of enrollment and teaching scale, the multi-campus and multi-teaching site management mode is implemented through the implementation of intelligent VPN hierarchical management scheme. On the premise of ensuring network security, the problem of multi-campus access in campus network is solved. This enables campus users and users outside the campus to access various resources on the campus network through VPN channels anytime and anywhere, and ensures user identity authentication and data encryption transmission between campuses. The application of intelligent VPN hierarchical management balance strategy in campus network promotes the development of smart campus in our school. It has positive and beneficial significance in the process of school internal management and teaching activity management.

ACKNOWLEDGEMENT

This research was financially funded by the Project of Hunan Development and Reform Commission (XFGTZ [2019] No. 412) and Industry-university-research Innovation Fund of China Universities, No.2020ITA07018.

REFERENCES

[1] Tang, P. Y., Li, G. C., Yu, G., et al., "Network communication security based on QS-KMS and VPN," *Computer Engineering* 44(12), 13-7(2018).
[2] Wang, L., Feng, H. M., Liu, B., et al., "Research on SSL VPN encrypted traffic identification based on hybrid method," *Computer Applications and Software,* 36(2), 315-22(2019).
[3] Du, L. M., "Design and research of wireless campus Network based on SSL VPN technology," *Journal of Jining Normal University,* (3), 30-3(2017).
[4] Chen, H. Q., Zhang, L. J., Lai, Y., Y., et al., "Design and implementation of power security gateway based on SSL VPN technology," *Electronic Design Engineering,* 28(13), 97-100(2020).
[5] Muc, A., Muchowski, T., Murawski, L., et al., "Providing the ability of working remotely on local company server via VPN," *Multidiplinary Aspects of Production Engineering,* 3(1), 195-205(2020).
[6] VPN technology and application based on SSL protocol, *Information & Computer,* (3), 146-8(2013).
[7] Wang, Z. Y., [Wireless Interconnection Technology], 21-2(2019). (in Chinese)
[8] He, Y., "Application of VPN technology in local area network," *Computer Products and Circulation,* (05), 42(2019).
[9] Chen, Q. S., "Application analysis of virtual private network technology in computer network security," Science and Technology Innovation and Application, (019), 177-8(2018).

[10] Wang, Y. and Kong, C., “Application of reverse proxy Technology in Digital Campus,” Information and Computers: Theoretical Edition, (11), 195-196(2019).
[11] Tan C., Tan, X., Hu, L., et al., “Dynamic weight load balancing algorithm based on nginx in cloud center,” Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 33(6), 991-998(2021).
[12] Huang, C. and Teng J., “Performance optimization of web-based course selection system based on reverse proxy server,” Microcomputer Applications, 36(10), 132-134(2020).
[13] Liu, S. and Zhong, L., “A Load Balancing Algorithm for Web Cluster Based on Service Type,” Journal of Wuhan University of Technology, 31(19), 134-136+159(2009).
[14] Wei, M. and Wei, Y., “Load balancing of streaming media in network system,” Journal of Wuhan University of Technology: Information and Management Engineering, (4), 529-532+536(2008).