Journal of Applied Science and Engineering Innovation, Vol.4 No.1, 2017, pp. 36-38
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Application of SSL VPN Network Security Technology

Yan Yi[1], QingJiang Zhao [2]

[1] *Personnel division Kunming University, Kunming, 650214*
[2] *Assets and laboratory administration, Kunming University, Kunming, 650214*

Abstract: For that the current networks have brought us a lot of conveniences, but also the corresponding network risks. In this paper, the structure and application process of SSL VPN are briefly described, followed by the detailed analysis of the technical advantages and application of SSL VPN. Focus on the research object of SSL VPN and exploring the basic principles and applications of the technology, this paper aims at providing some references for the continuous improvements of China's network security. ..

Keywords SSL; VPN; Network security technology; Application.

INTRODUCTION

The core of SSL VPN technology is to construct an internal network with encryption and authentication functions in INTERNET public network, the internal network can not only ensure the connections within SSL VPN, but also can ensure the network information security by data encryption technology, as the same time can connect to the public network by router, and control the information transmission flowing to sensitive networks [Shan, *et. al.*, 2014]. Compared to the traditional VPN, SSL VPN is not limited in the information communication, and also management, control functions are also integrated into SSL VPN, so as to achieve the purpose of ensuring network security.

BASIC PRINCIPLES OF SSL VPN

SSL protocol

SSL VPN is a VPN technology built based on SSL secure socket protocol, the SSL protocol is mainly used for servicing WEB applications, including the user authentication, server and client authentication, data information encryption transmitting in SSL link, protection and other services in the WEB. Due to the technical characteristics of SSL, it has been widely used in a variety of browsers [Liu, *et. al.*, 2014].

VPN Technology

VPN technology is used to construct the virtual network, by this way realizes data security in VPN network, and the access control function with external network, now the internal networks of companies, campus interior networks generally adopt this technology. At the same time, VPN can also connect to the external INTERNET network by means of routers.

SSL VPN technology theory

VPN technology based on SSL combines VPN virtual network with encryption and authentication functions together, in SSL VPN, not only VPN internal network can browse external public INTERNET network, but also can authorize external networks to access the open part of the enterprise network by authentication and encryption, and control information transmission flowing to sensitive networks [Zheng, et. al., 2013]. The construction and operation cost of this kind of technology are much less than the previous special line access mode, and it has more advantages in the aspect of security protection.

THE STRUCTURE AND OPERATION PROCESS OF APPLICATION OF SSL VPN

The SSL VPN is mainly constructed by server, client, etc., the specific as shown in figure 1. SSL VPN server is the control core of the entire system [Liu, 2015]. When the client sends a visit request, the server will achieve the security protections of a number of WEB services by SSL VPN technology as the same as time. The server will convert the client's request address, the port into Web address, do the request sending of WEB service instead of the client, and wait for the response of WEB. Then the server will receive the data information the WEB responses, convert and control, and then send the conversion results to the client to complete interaction process of the network information.

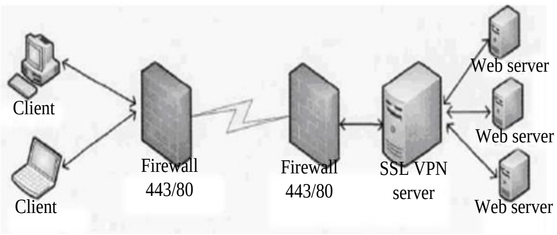

Figure 1: Structure diagram of SSL VPN

Corresponding Author: QingJiang Zhao,Assets and laboratory administration, Kunming University, Kunming, 650214

TECHNOLOGY ADVANTAGES OF SSL VPN

Wide application

SSL VPN is a kind of network security technology that can be applied to WEB services. With the comprehensive popularization of web browser, the application scope of SSL VPN has also expanded. As long as there is a WEB browser, application of SSL VPN technology could be achieved [Li, 2015]. The enterprise, customers, partners, suppliers, schools and families all can use SSL VPN technology to achieve network security protection. Its application advantages are especially suitable for commercial confidentiality of large and medium-sized enterprises, at the same time the costs of purchase and construction, management, operation, maintenance, etc., can significantly be reduced and the resources can be saved.

Strong security

Because that all of the information from the external network need to be dealt with by SSL VPN server, and then sent to the customer, in this process the viruses, worms from the external network and data from or to unreliable sites will be filtered. At the same time, the intermediary role of SSL VPN ensures the internal network won’t be exposed directly to hackers, reduce the risks from hackers effectively, at the same time because the SSL VPN server is not directly in the network layer, hackers will not detect internal supervision mechanism of SSL VPN easily, risks of being attacked by the hackers will be reduced greatly.

Economic

The traditional VPN virtual network needs additional hardware to increase the access branches, for the large and medium-sized enterprises which mostly use virtual networks, construction cost of VPN is very huge, maintenance workloads and costs of response are naturally a lot [Lin, 2015]. SSL VPN effectively solves this problem, as long as setting up a hardware device in headquarter, security of all internal users could be realized, each branch equipment only needs to use the WEB for remote access, greatly reducing the expenditure of construction and maintenance. At the same time, only a staff can complete related management and daily maintenance work, on the basis of strengthening the network security, it effectively realizes resource conservation of human resources, material and financial resources.

APPLICATION ANALYSIS OF SSL VPN

SSL VPN is a kind of security access technology, easy to be constructed, practical and effective, by encryption, authentication and other ways to realize the security protection in the application progress. With SSL VPN to achieve the communication between the user and the browser, with the compression and encryption, protection and other applications of data records in SSL VPN, the speed could be lifted on the basic of ensuring network security.

Encryption and verification

The key application technologies of SSL VPN are all kinds of protocols, such as the handshake protocol, recording protocol and warning protocol. The handshake protocol is one of the most basic SSL security control mechanisms, including algorithm negotiation, identity authentication, key, etc.

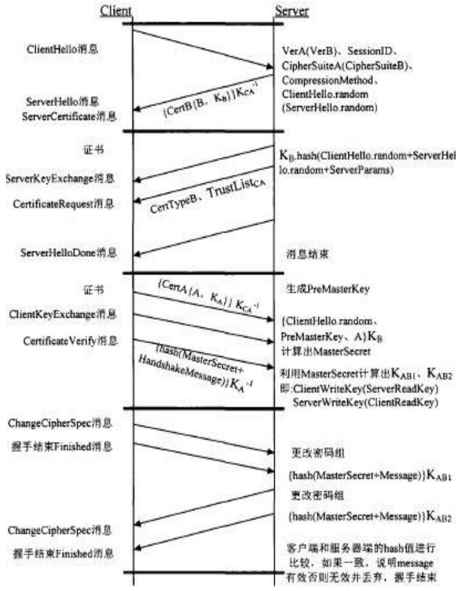

Figure 2: Process diagram of handshake protocol

In order to ensure the security of SSL VPN data network transmission, it is necessary to encrypt the data before transmission. By handshake protocol, protocol of modifying the password parameter, SSL VPN carries out the data encryption for client and server, and generates the encryption key for user's authentication. By the application of handshake protocol to achieve user confirmation, and according to the users to determine the transmission mode and the encrypted content, information security is greatly improved, and the user and server complete information transmission in communication security protocol. The specific operation process: 1. first server exchanges access information with client, after verification, to determine whether the information can be transmitted to the user [Yue, *et. al.*, 2015]. 2. The server sends security certificates and authentication information to the user. 3. Server verifies the user's access key, and determines whether the security certificate is valid. 4. After verification, by transferring the information received to the user to achieve the user's access. In practical application, not all constructions of SSL VPN need to verify the security certification and key at the same time, it also can be set to verify user information and key, or without verification and other forms, but without verification is very difficult to guarantee the network security, and therefore it is used less often.

Record, classification and compression of the data

This function is basic application service in SSL VPN, by recording protocol SSL VPN records, classifies, and compresses the data the server accepts, this application is to optimize the data transmission, and improve the response speed, is the most basic part of the whole SSL VPN. After classification, the recorded data needs to be divide into blocks and compressed, under the premise of ensuring the integrity is not damaged, each data packet has been compressed is controlled less than 214 bytes, and each packet's exclusive authentication codes are calculated, and marked. In this way, when SSL VPN browses and receives the same information, it can mobilize data compression, transmit the data very fast, and enhance the response speed.

Safety protection

The basic of SSL VPN is the user key and security authentication, the specific is shown in figure 3. In order to further enhance the effect of security protection, it also needs to add warning protocol on the basis of handshake protocol and the key, when the key and user security authentication fail, the user cannot obtain the required information, at the same time, the server will issue a warning, and feedback the result of failure to the manager and user, after receiving the feedback, it will promptly disconnect the error link to prevent more damage. At the same time because information of external network will go through SSL VPN server first, then users can accept, if viruses, worms and Trojans are found, it will issue a warning at the same time of filtering, if there are a large number of virus on a website, then the information interactions with this website will be terminated. According to the degree of harm, it can be divided into serious warning and general warning. For example, after the initial validation error, a general warning will be issued, the user can continue to operate and modify the key after receiving the feedback of verification failure. If mistakes repeat, it will issue a serious warning. As the same time of warning, the operation between the client and the user will be forced to suspend to prevent serious harm.

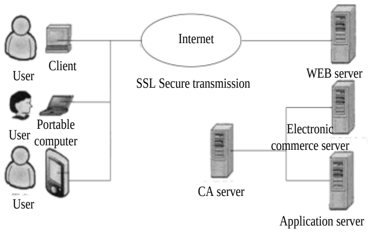

Figure 3: Diagram of network frame based on SSL security transmission protocol

Access control

In the traditional VPN virtual network, as long as passing the user authentication, it can browse all kinds of information in web without limitation. But in fact, even in internal network like an enterprise, campus, and not all information can be open to all staff, so the traditional VPN virtual network technology obviously is not suitable to the actual needs. The VPN technology based on SSL is an effective solution to this problem, through the security agreement to distinguish different users, and to give the appropriate authority. For example, the user authorities of company's leadership and employee are different, for the enterprise's confidential information data, ordinary employees do not have authority to access, so as to effectively protect the important information within the enterprise. At the same time, SSL VPN can also record by the recording protocol, record the users accessed, if the information is leaked, the records can also be used to track.

CONCLUSION

On the basis of network information communication, SSL VPN integrates management, control and other functions, and effectively ensures the network security. In summary, firstly the basic principles of SSL VPN are summarized, the basic framework, operation process and application advantages are made clear, finally respectively in the encryption and authentication, data recording and compression, security protection and access control and other aspects, the specific application of SSL VPN are explored, and I hope this research can provide some reference for related people.

REFERENCE

Li Ling, Li Chentao,2015, "The application analysis of SSL VPN technology in computer teaching resources network ",Telecom World, No.19,pp.261-262.

Lin Yongjing,2015, "The application of VPN technology in computer network",China Computer & Communication (THEORY EDITION), No.22,pp.14-16.

Liu Dong, Wang Shuang, Zhou Jing, Xu Manli, Chen Wei, Han Zhengfu,2014, "Application of quantum key in power grid SSL VPN", Power System Technology, No.2,pp.544-548.

Liu Shaogang,2015, "Research on SSL protocol-based VPN technology and its application in campus network", Practical Electronics, No.1,pp.85-86.

Shan Jialing, Xie Zhicheng, Zhao Chongjin, 2014, "Application of SSL technology-based VPN gateway in wireless network", Computer Systems & Applications ,No.2,pp.60-64.

Yue Ying, Sun Guangbo, Yang Min, Wang Hao, Yang Jin,2015, "Application of VPN technology in enterprise network construction", Mobile communications, No.21,pp.49-54

Zheng Huapu, Liu Shuai,2013, "Research on Key Technologies of SSL VPN network security ", Journal of Pingdingshan Institute of Technology, No.4,pp.69-72.