The research on the application of SSL VPN technology on the digital campus

Chunyu li[1], Jianchun Cai[2]

[1]Department of Physical Science and Technology, Kunming University, Kunming 650214，China

[2]Department of Physical Science and Technology, Kunming University, Kunming 650214，China

Keywords: SSL VPN; universities; digital campus; network

Abstract. As a mature network technology, SSL VPN has strong scalability with low maintenance cost and it is easy to use. Furthermore, it can satisfy the remote office, branch office access and other discrete needs solving the remote access to data resources issue on university campus. This article describes the technologies related to SSL VPN, as well as SSL VPN technology in the digital campus. It has certain reference value in solving the remote access to data resources on university campus.

1. Introduction

With the development of digital campus network, the electronic networking of university information resources has progressively been realized. The digital campus has a variety of databases and different kinds of office software, such as: OA system, library resources systems, financial systems, E-learning systems and so on. But many data resources on campus are protected and can only access these resources at campus. Because of the expansion of the size of the universities, some have more than one campus. In addition to teachers, graduating students, traveling and training teachers, so some work must be completed outside the campus. Thus they can not access the on-campus resources while browsing the web outside the campus. A safe and effective way for users to access must be provided by the university to make sure that users can connect to the campus network anytime and anywhere. Considered as a mature network technology, SSL VPN is convenient to deploy and easy to use with scalability and low maintenance costs. It can satisfy the needs of telecommuting and branch discrete access. The problems the universities are facing can be effectively solved.

2. Technologies related to SSL VPN

2.1 VPN Overview

VPN is virtual dedicated network. Its meaning refers to the connection type provided remote access to the internal private network by using the public network infrastructure, the appropriate technology "tunnel" technology, authentication, encryption and access control [1]. It can connect different networks with each other between components and resources, create a tunnel for users to use the Internet or other public network, as well as provide the same security and protection features as dedicated network. Although VPN communications infrastructure is built on the public Internet, users feel they were using dedicated network when they use VPN.

2.2 SSL protocol description

SSL (Secure Sockets Layer, Secure Sockets Layer) protocol, is an application secure protocol based on web, which is proposed by Netscape. It uses data encryption technology to protect data on the internet transmission security, integrity, and to identify the web server and the identity of the client browser. It is widely used on the network. Besides, it is available for all web servers. So it is an internet security protocol. SSL protocol provides security support for data communications, and is used for encrypted data transmission and authentication between the web browser and the server. It is located in the protocol TCP/IP protocol and the various application layer protocol [2]. SSL session is divided into two parts: the connection and application. During the connection, the client

and server authenticate mutually and agree upon security parameters. The client server generates a master key based on authentication information. This master key will encrypt the contents of the communication that followed. During the application session, all kinds of information can be safely transported between the client and the server, including sensitive resources, classified data, etc [3].

2.3 SSL VPN Profile

SSL VPN is the virtual private network technology working on the application layer. It uses SSL technology and agent technology to provide secure access to HTTP resources, C/S resources and other services for remote users. It has a strong regulatory capacity in access control, application size, etc. Users can only access the application granted to him and can not access other resources without authorization, which effectively protect the security of information resources. Users can realize the goal of secure access to the universities' network anywhere and anytime through the application of this technology. At present, almost all major browsers support SSL protocol, so users do not need to install client software. It is more simple and convenient to use this kind of technology[4]. The costs of deployment and maintenance of the network in universities will surely be lowered.

SSL VPN has the advantage of platform independence. Any browser which supports SSL can access resources without fear of being dependent on the operating system. If the connection is not satisfying, there is no need for the user to troubleshoot the third-party VPN client. In addition, many organizations restrict most VPN traffic form (such as IPSec and PPTP) to go across its network. SSL VPN network can solve this problem. One major difference between SSL VPN and the performance of other remote access technologies lies in achieving the user's session. VPN client initiates a direct connection with the protected network server. In the SSL VPN Clientless Mode, SSL VPN gateway acts as a VPN agent between the client and internal resources. As shown in Figure 2.1, if the user wants to access the internal website jwc.kmu.edu.cn, the SSL VPN session is terminated at this gateway and then the gateway will initiate a new session to the internal server to represent the client.

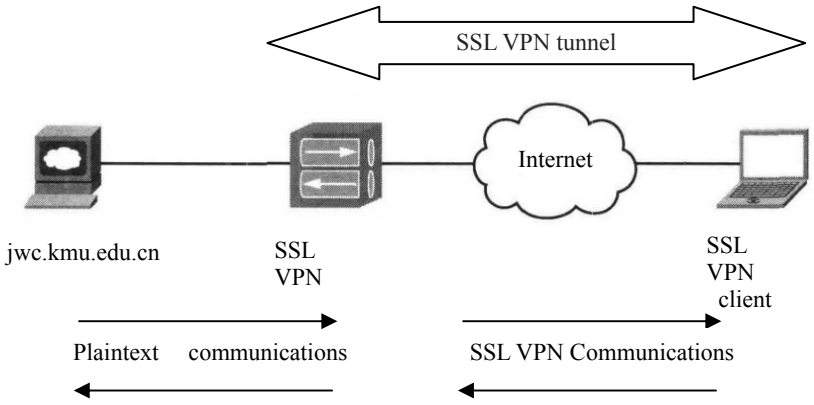

Fig2.1 SSL VPN gateway and connection broker

2.4 Deployment mode often used by SSL VPN

SSL VPN applications are typically placed on the edge of the internet of the campus network. Additional security devices are often deployed to protect the internal network from attacks at the edge of the network. There are three kinds of common deployment model SSL VPN gateway and firewall: Parallel Mode, Inline Mode and DMZ Mode [5], shown in Figure 2.2:

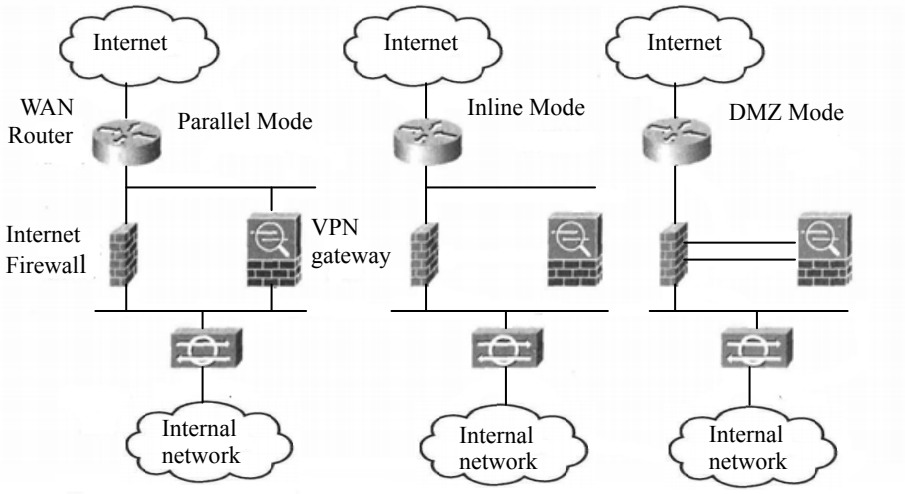

Fig.2.2 SSL VPN deployment model

(1) Parallel Mode

In the Parallel Mode, the internal and external network interfaces of the SSL VPN gateway and the firewall are divided in the same segment. This deployment is not really reliable because the SSL VPN gateway can not classify the appropriate security permissions for remote users and network users so that remote users can access the internal network resources without restriction through the SSL VPN gateway.

(2) Inline Mode

In the Inline Mode, the external network interface and firewall access SSL VPN gateway are in the same network segment, while its internal network interface connects to the access DMZ zone of the firewall. In this way the firewall will effectively isolate remote users and internal network users, control remote user access behavior by adopting appropriate security policies to prevent the internal network resources from being vandalized.

(3) DMZ Mode

In the DMZ Mode, the external and internal network interfaces of SSL VPN gateways are connected to two DMZ interfaces of the firewall. The firewall can control users' access to external network SSL VPN gateway. The extranet users secure access control can also be achieved through SSL VPN connection by its internal security policy.

3. SSL VPN applications in digital campus

3.1 Applications

This instance is a university, which ensures the staff, teachers and students outside the campus can access the network of the campus, SSL VPN architecture is adopted after studying and analyzing. The concrete frame is shown in Figure 3.1 .

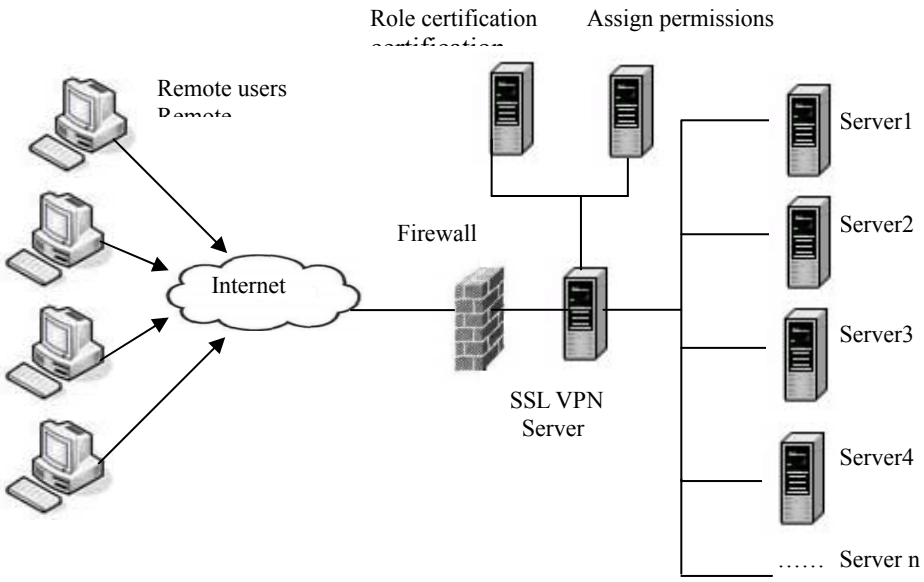

Fig. 3.1 SSL VPN architecture diagram

The university uses SSL VPN web-based system mode, building a secure messaging channel between the user and the application server. SSL VPN server is installed behind a firewall as a gateway, which has a dual identity. For users, it is a server, which is responsible for providing certificate-based identity authentication; for the application server, it belongs to the identity of the client and submits an access application to the server.

SSL VPN system uses role-based access control policies, including the interface for security authentication and the list of resources of users to access. The authentication of campus network system users and the access control can be implemented in the control protocol section. After external users open the web browser, without installing any software, enter the identity information in the login screen. SSL VPN device will get the connection and authenticate of the users. Then VPN access system determines the user's access rights on the basis of user's role properties, and then gives a list of resources that the user can access the information. The digital resources on campus can be accessed. This design adopts agent technology. All users outside the campus who can successfully access to SSL VPN will have a full access to digital resources available to the LAN port.

3.2 The advantages of using SSL VPN technology

SSL provides secure communications for application, and is transparent for the upper layer of applications. The most successful application running on SSL is HTTP because the web is very popular. All commercial web browsers are available by default on all operating systems supporting HTTPS (based on SSL/TLS for HTTP). For remote access, the technology advantages of VPN, SSL VPN are obvious, mainly in the following aspects:

1) Secure communications using encryption algorithms: providing confidentiality, integrity and authentication.

2) The prevalence: Because SSL/TLS is prevalent, it is possible for the VPN service users to have a remote access to corporate resources anywhere by using any PC without pre-installing a remote access VPN client.

3) Low management overhead: this type of remote access VPN deployment is almost free of charge because of no client access and so is the end-user. This is a huge benefit for IT managers. Otherwise, managers will spend a considerable sum of resources to deploy and maintain their remote access VPN solutions.

4) The efficient operation with a firewall and NAT : SSL VPN operates in the same port as HTTPS (TCP/43). The vast majority of Internet firewalls, proxy servers and NAT devices are used to handle TCP/443 data traffic. Therefore, there is no need to give special consideration to transfer

SSL VPN traffic in the network. Compared with the local IPsec VPN, this is an important advantage because IPsec VPN operation will be through IP type 50 (ESP) or 51 (AH). In most cases, the firewall or NAT devices need be specially considered to make them go through.

4. Conclusion

With the development of digital campus network, university teachers and students rely more on the growing data resources in universities, breaking through time and space constraints. It has become an urgent need for them to use internal resources in universities at any time. As an important security access and control system, the access of SSL VPN is easy and secure, with rich and effective rights management. The unique technical advantages and potential with cross-platform, free installation and maintenance have been widely used in universities. It can greatly meet the needs of low-cost and high cost-effective.

References

[1] Da Wang, A Virtual Dedicated Network (VPN) Fine Solution [M]. Beijing: Tsinghua University Press, 2004: 45-46

[2] Jiaqin JIN, Remoteaccess to E-resources of Public Library Based on SSL VPN [J]. Library Journal, 2009,28 (3): 62-63.

[3] Jing Yu, Research and Application of OpenVPN Based on SSL [D] Hubei: Hubei University Software Engineering, 2011

[4] Kui Ning, Safety Technology and Application of Access Control[M]. Beijing: Electronic Industry Press. 2005.

[5] Guanghui Zhou, Research and Implementation of USBKey User Authentication Platform [J] Information Security and Communications Privacy, 2009,9: 113-118