International Journal of Control and Automation
Vol.9, No.1 (2016), pp.111-122
http://dx.doi.org/10.14257/ijca.2016.9.1.11

Study on Remote Access for Library Based on SSL VPN

Mei Zhang

Library, Linyi University, Shandong, 276000, China
zhangmei7596@163.com

Abstract

With the popularity of the Internet and improvement of information technology, digital information sharing increasingly becomes the trend. More and more universities pay attention to the digital campus, and the construction of digital library has become the focus of digital campus. A set of manageable, authenticated and secure solutions are needed for remote access to make the campus network be a transit point for the outside users. The VPN (Virtual Private Network) remote access solution of university library digital resources was proposed, two main ways to achieve the VPN were introduced, the realization of remote access to digital library resources based on SSL (Secure Sockets Layer) VPN system was elaborated. These measures can provide remote access to outside users, and can greatly improve the utilization of digital library resources.

Keywords*: Remote Access, Library, SSL, VPN*

1. Introduction

Digital library is a digital information resource which has a variety of media and rich content, and it can easily and quickly provide information service. Compared with the traditional library, digital library has some features, such as storage digitization, transmission networking, service knowledgeable, resource sharing and service globalization.

According to the statistics, the knowledge information today is mainly distributed in many Internet sites in the form of database, and it has 200 times the amount of website information. However, due to intellectual property protection and commercial involvement, domestic and foreign databases are mainly commercial. As database developers, they do not want their products to be open social resources. Similarly, as the database users, they do not want the database that they buy to be public resource entirely. Then, the digital library resource that can easily be shared and spread is limited in the local area network, becoming information islands artificially.

The law strictly restricts the use of digital library resource in the network. All the database providers add strict terms of intellectual property protection to the product sale contracts to prevent the digital resource unauthorized using and unlimited dissemination. The technology restricts the network use of digital library resource. The digital library resource in the form of mirror mode is often on the local area network, and cannot be accessed directly. The database in package repository approach generally only allows IP access in the local area network and rejects any other internet access.

In such context of intellectual property protection, the digital resources purchased by the university library have been set the access IP address range. The database providers only open access to the IP address within the unit. The method of IP limitation make the users cannot access the digital resources through dial-up or ADSL (Asymmetrical Digital Subscriber Loop) broadband, which causes great inconvenience, and also affects the utilization and benefits of the digital library.

Therefore, it is necessary for the university library to develop a set of manageable, authenticated and secure solutions to remote access, to make the campus network be a

ISSN: 2005-4297 IJCA

transit point for the outside users. Depending on the corresponding identity authentication, after entering the campus network, the outside users can visit corresponding electronic resource database. It allows the users to visit the digital resources without the limitation of time and space, and really play resource popularity and sharing role of university.

In this project, the VPN remote access solution of university library digital resources was proposed, two main ways to achieve the VPN were introduced, the realization of remote access to digital library resources based on SSL VPN system was elaborated, in order to provide remote access to outside users, which greatly improve the utilization of digital library resources.

2. Remote Access

2.1. Overview of Remote Access Technology

Remote access is a series of technology that can connect the particular computer located outside the workplace or in the remote location to the network. For the library digital resources, remote access, also known as off-campus access, means that it breaks physical limitations of IP addresses, and can use the library digital resources anywhere. There are two remote access ways, i.e. dial-up internet access and virtual private network connection.

Virtual private network is a technology that establishes a safe, temporary and dedicated data through a public network, and it is a safe and stable tunnel passing through the chaotic public network. Using the tunnel, it can encrypts the data several times to achieve using the Internet safely. In a virtual private network, there are no traditional end-to-end physical link between the two nodes, but dynamically composed using some kinds of public network resources.

2.2. Virtual Private Network

Virtual private network is a new network technology, and provides a safe connecting way of remote access between public network and the internal private network. VPN is a very useful technique. It can extend the library internal network, and allows the employees, customers and partners to access library network using Internet, which cost far less than traditional dedicated access.

VPN, an acronym of Virtual Private Network, is developed for corporate private use based on Internet. The network uses the lesser-reliability public Internet as the information medium, to achieve the safety performance similar as the private network through additional security tunnel, user authentication and access control technology.

VPN is to establish a virtual private network in Internet, so that the two long-distance network users can transmit data to each other in a dedicated network channel. The core of VPN is tunneling technology. The tunnel allows the data stream of VPN to pass through the IP network, regardless of the type of network or device. From this sense, the operation of VPN is independent of other network protocols, and the data flow inside the tunnel can be IP, IPX, AppleTalk, or other types of data packets.[1] Therefore, VPN is a secure private channel across the public network based on IP protocols to achieve private use of public network. Only need to connect to the Internet , customers can access to the internal network.

Working Process: Using VPN technology, library networks can communicate securely in the unreliable public Internet. VPN encrypts the transmission information using high-performance and complex algorithms, to ensure the need of information security for teachers and students.

(1) Non-campus network client users send information to the campus network VPN server, VPN server responses to the request, challenge to the client identity, and the client sends the encrypted identity information to the VPN server.

(2) VPN server checks the response according to the user database. If the account is valid, the VPN server will check whether the users have remote access rights. If the users have the rights, VPN server accepts the connection.

(3) If the user is legitimate, the VPN device will encrypt the entire packet and attach a digital signature, add new data header including security information of object client.

(4) The VPN server repackages the encrypted data, packet and originate IP address, and make the packet transmit in the Internet through a virtual channel.

(5) When the packet reaches the client outside the campus, it is de-capsulated and decrypted after checking the digital signature.

2.3. Security Technology of Virtual Private Network

VPN users are more concerned about data security because of its private information. Currently, VPN mainly uses four techniques to ensure safety, i.e. tunneling technology, encryption and decryption technology, key management technology and user and device authentication technology.[2]

(1) Tunneling

Tunneling technology is a basic technique of VPN, similar to point-to-point technology, creates a data channel in the public network and allows the data packet to pass through the tunnel. The tunnel is formed by tunneling protocols, and is divided to layer two and layer three tunneling protocol. The layer two tunneling protocol packages a variety of network protocols into the PPP, and then packages the entire data packet to the tunneling protocol. The package formed by double-layer encapsulation method transmit based on the layer two protocol. The layer two tunneling protocol has L2F, PPTP, L2TP and so on. L2TP protocol is the IETF standard, and formed by the fusion of PPTP and L2F.

The layer three tunneling protocol directly packages a variety of network protocols into the tunneling protocols, and the formed data packet transmits based on the layer three protocol. The layer three tunneling protocol has VTP, IPSec, etc. IPSec, short for IP Security, is composed of a group of RFC documents, defines a system to provide security protocol selection, security algorithms and determine the key needed by the service, so as to provide security at the IP layer.

(2) Encryption and decryption technologies

Encryption and decryption is the more mature technology in the data communication, and VPN can directly use the existing technology. Encryption is a process that transforms a piece of meaningful text or data into a messy arrangement and literally meaningless text or data.[3] The transformed information is referred as plaintext, and the changed information is ciphertext. Decryption is the reverse process of encryption, which is to revert the ciphertext to the plaintext.

The common VPN encryption algorithms have symmetric encryption and asymmetric encryption, i.e. private key and public key.

Symmetric encryption, or private key, shares a secret key by the communicating parties. The sender encrypts the plaintext into ciphertext by the key, and the recipient reverts the ciphertext into plaintext by the same key. RSA RC4 algorithm, the Data Encryption Standard, International Data Encryption Algorithm and Skipjack all belong to the symmetric encryption.

Asymmetric encryption, or public key, refers that the communication parties use two different keys, one is the private key only known by the sender, the other is the corresponding public key, and anyone can obtain the public key. The private key and the public key associates with each other, the former is used for data encryption and the latter is for data decryption.

The public key cryptography allows the information to digitally sign. The digital signature uses the private key of the sender to encrypt a part of the information. After

receiving the message, the recipient decrypts the digital signature by the public key, to verify the identity of the sender.

Since the data all transmits through the Internet, the data encryption and integrity must be protected. VPN generally provides more than 128-bit symmetric encryption, and asymmetric encryption algorithm uses 1024 bit, and uses application-layer VPN technology on the network protocol stack and one-time password system. Meanwhile VPN uses MD5 encryption algorithm to protect the data integrity in the transfer process.

(3) Key management technology

The main task of key management technology is how to safely pass the key in the public data network without being stolen. The existing key management technology have SKIP and ISAKMP / OAKLEY. SKIP mainly uses Diffie-Hellman algorithm to transmit the key. In ISAKMP, both parties have two keys for public and private use respectively.

(4) User and device authentication technology

User and device authentication technology commonly uses the user name and password or card authentication. When VPN client requests for communication, it must be authenticated by the other end of the VPN tunnel, the communication path can be considered safe and can communicate. There are two peer authentication methods.

Pre-Shared Key. It is the shared key between the two sides through a secure channel before use. PSK uses a symmetric key encryption algorithm, and it entered into each peer manually to verify the identity of the peer. At each end, PSK combines with other information to form the authentication key.

RSA signature. It uses digital certificates exchange to verify the peer identity. The local device obtains the hash value and encrypts it with the private key, the encrypted hash value i.e. digital signature, is attached to the message, and forwards to the remote side.[4] At the remote terminal, it uses the local public key to decrypt the encrypted hash value. If the decrypted hash value and the re-calculated hash value are the same, it indicates that the signature is authentic.

2.4. Advantages of Virtual Private Network

(1) Low cost

By constructing VPN through a public network, the companies do not have to hire long-distance dedicated line to construct private network, and do not need a lot of maintenance personnel and equipment investment.

(2) Security

VPN uses tunneling technology, encryption and decryption technology, key management and authentication technology to ensure the safety of the network and data transmission, which avoid eavesdrop, forgery and modification in the plain text form.

(3)Scalability and flexibility

VPN access is flexible, supports most types of library data flow, easy to add new nodes, supports multiple types of transmission media, and can meet the demand of voice, video and data transmission and bandwidth addition.

(4) Manageability

On the management side, VPN requires libraries to seamlessly extend network management functions from the LAN to the public network, and even customers and partners. Some minor network management tasks can be given to the service provider, but some important work, such as identification, access, network address, security and network change management must be responsible by itself.

(5) Quality of service guarantees

VPN can provide different levels of service quality assurance for user data. It allocates bandwidth resources according to the priority through traffic prediction and flow control strategy, all types of data can be reasonably sent, so that it prevents network congestion.

3. Two Main Ways to Achieve VPN

IPSec VPN, short for IP Security and SSL VPN, short for Secure Socket Layer, are two popular Internet remote secure access technology, and they both have overlapping points and complementarity.

3.1. IPSec VPN

IPSec VPN is a VPN technology that uses IPSec protocol to achieve remote access, and it is the security standards framework defined by Internet Engineering Task Force (IETF), in order to provide end-to-end encryption and authentication services for public and private networks. IPSec is not a separate protocol, but gives a set of architecture applied to network data security of the IP layer. The architecture includes Authentication Header protocol (referred to as AH), Encapsulating Security Payload protocol (referred to as ESP), Internet Key Exchange protocol (referred to as IKE) and some algorithms of network authentication and encryption. IPSec defines how to choose security protocol, determine safe algorithms and key exchange between peers, and provide access control, data origin authentication, data encryption and other network security services upwards.

IPSec has two modes, tunneling mode and transport mode. The tunneling mode can establish a secure tunnel between the two security gateway, and the transmission through the two gateway proxy are carried out in the tunnel. The IPsec packets in the tunnel mode will be segmentation and reassembly operations, and it can reach the destination host after going through multiple security gateways. In the tunnel mode, in addition to the source and destination hosts, the special gateway will also perform cryptographic operations.[5] In this mode, many tunnel are generated in the series form among the gateways, which achieve gateway to gateway security.

The transport mode has less encryption part, no additional IP header, and has relatively better efficiency, but less safe than the tunnel mode. In the transport mode, the source and destination hosts must perform all cryptographic operations directly. The encrypted data is sent through the single tunnel generated by using L2TP Layer Two Tunneling Protocol.

3.2. SSL VPN

IPSec VPN and SSL VPN are the two different VPN architecture. IPSec VPN is working at the network layer, and providing all the data protection and security communication at the network layer. SSL VPN is working between the application layer based on the HTTP protocol and the TCP layer. From the overall security level, both can provide secure remote access. IPSec VPN technology is designed to connect and protect data stream in the trust network, so it is better suited to providing communication security for different networks, and SSL VPN is more suitable for secure access of remote dispersed mobile users.

SSL (Secure Sockets Layer protocol) protocol is developed by Netscape. It is a set of common protocol ensuring the sending information safety in the network, and has been widely used for authentication and encrypted data transmission between the Web browser and the server. SSL is in the application layer, and it works with public key encryption through the transmission data. SSL protocol specifies the security mechanism for the data exchange between the application protocol and TCP/IP, in order to provide data encryption, server authentication and optional client authentication. The advantage of the SSL protocol is that it is independent of the application layer protocol. High-level application layer protocols, e.g. HTTP, FTP, can be transparently built on the top of SSL protocol. [6] SSL protocol has completed encryption algorithms, consultations of

communication key and server certification before the communication of application layer protocol. After that, the transmitted data of application layer protocol will be encrypted to ensure privacy of communications.

SSL protocol is mainly to provide privacy and reliability between two communicating applications. The process is completed through three elements:

(1) Handshake Protocol. This protocol is responsible for the parameter encryption of session between the client and the server. When an SSL client firstly starts communicating to the server, they reach an agreement on a protocol version, select the encryption algorithms and authentication, and generate a shared key using public key technology.

(2) Record Protocol. The protocol is used to exchange application data. The application message is divided into manageable data blocks. It can be compressed, generates a MAC (Message Authentication Code), and then the result is encrypted and transmitted.[7] The recipient accepts the data and decrypts, checks the MAC, unpacks, reassembles, and provides the result to the application protocol.

(3) Warning Protocol. It transmits alarms associated with SSL for peers, including three different levels, i.e. warnings, serious and major categories. This protocol is used to indicate when the error occurs and when the two hosts stop conversation.

3.3. Comparison of IPSec VPN and SSL VPN

(1) Safety

a) Secure channel. The main advantage of IPSec security protocol is only to create channels between customers and network resources. It merely protects secure from customers to the company network edge. All the data running on the internal work is transparent, including any passwords and sensitive data in transmission. SSL secure channel is established between the client and the accessed resource, to ensure end to end security. The data both on the internal network and the Internet is not transparent. Every operation of the customer needs secure authentication and encryption.

b) Application system attack. If the remote user uses IPSec VPN to establish connection with the internal network, hackers are able to detect the application systems connected to the internal network, which provides attack opportunity for hackers. If the user takes SSL VPN connection, because it directly opens the application system, and did not connect on the network layer, hackers are not easy to detect the internal network settings of application system. At the same time, hackers only attack VPN server, but unable to attack the background application server, and the attack opportunity comparatively reduced.

c) Viruses. The business generally take appropriate measures of antivirus detection in the Internet online portal. Whether IPSec VPN or SSL VPN connectivity, the effect is the same for the entrance virus detection, but it will be different from the possibility of remote client invasion. For IPSec connection, if the client computer is infected, the virus has chance to infect every computer connected to the internal network. For SSL VPN connection, the virus spread will be limited to the host, and the virus must aim at the type of application systems, different types of viruses cannot infect with the host.[8] So the possibility of infection by the external virus greatly reduced through SSL VPN connection.

(2) Application scope

IPSec works at the network layer, and it protects all the transmitted data of both communications. IPSec VPN is suitable for almost all applications, and the remote user and the LAN user feel exactly the same when it accesses the local resources. SSL protocol is located in the socket layer, and has close contact with the application layer, therefore, it can only access the sources that support SSL or Web browser. Accordingly, its application scope is e-mail systems, file sharing and Web applications.

(3) Deployment and management

As a traditional network endpoint security technology, IPSec VPN has relatively large dependence on the underlying hardware. When deploying IPSec VPN system, we need to re-plan the existing network hardware equipment, add related hardware facilities, and install corresponding software in the client hosts according to the specific platform. If the access control strategy of users changes long term, the configuration and operation is extremely complicated, and the personnel cost is large. When using SSL VPN system , as long as the client owns the digital certificate of relevant authority or other recognizable identity authentication method, the user can access the internal network information safely through Internet.[9] SSL VPN saves labor costs and material costs in the system deployment, development and maintenance of client software and hardware facilities. In simplicity, compared with the IPSec VPN system, SSL VPN has considerable advantages. Firstly, SSL VPN server does not require overly complex configuration and operations or install additional hardware facilities. Secondly, it does not need to install additional software in the client, and users can access through the own network browser supporting SSL protocol generally. Additionally, because no additional client software support, SSL VPN has stronger compatibility, and does not require the specified operating system for the client.

(4) Scalability

IPSec VPN system often couples to the gateway device, so when deploying IPSec, companies VPN should consider the topology of the entire network. If add new equipment, the network structure will be changed, which results in relatively poor scalability of IPSec VPN. In contrast, SSL VPN not only can be used as network devices, but also can be used as a single VPN server deploying on other internal network nodes. Therefore, it does not need to consider the network structure, does not need major changes and redeploying for the VPN server when adding internal network server, so it has stronger scalability.

(5) Controllability

IPSec VPN is constructed based on the network layer, so it is impossible to distinguish the request of visitors depending on the application. Therefore, the authentication visitors through IPSec VPN can access to any internal network resources without any restrictions. From this perspective, IPSec VPN just created a virtual transmission network, which is not enough for the access control function. In this way there is a big risk for the application of distinguishing data types and access levels. Unlike IPSec VPN, SSL VPN does not just create a virtual transmission network. while encrypting to the transmission data, SSL VPN will limit the accessed internal resources according to different visitors.[10] On this approach, SSL VPN distinguish the private data for different users, and greatly enhances the flexibility of access control.

(6) Economy

When add an accessed branch, IPSec VPN needs to add a hardware device. With the expansion of IT construction scale, the company needs to keep buying new equipment to meet the company's development. The SSL VPN only needs to place a hardware device in the central node, it can achieve secure remote access control for all users. After deployment in the system, a general administrator with basic IT knowledge will complete the daily management work, so SSL VPN is more economical than IPSec VPN.

4. Construction of Library Remote Access System Based On VPN

4.1. Design Principles of Establishing VPN for Library

For the security of network, when building a library VPN business network on the public network, it must follow the networking principles.

(1) Security: By constructing a library VPN business network on the public network, physical isolation of internal and external network, tunneling and encryption technology, it develops a unified security policy of library network, and considers the whole safety of the library network platform.

(2) High reliability: The stability and reliability of the network is key to ensure the normal operation of the library management system. In the library network design, it must prioritize high reliability network product, rationally design network product architecture and formulate a reliable network backup strategy in order to ensure self-healing capabilities of network fault.

(3) Advancement and practicality of technology: While guarantee to meet the library management system, it must reflect the nature of the network system.[11] In the network design, it should combine advanced technology with existing mature technologies and standards, and fully consider the applications and future trends of library business.

High performance: Backbone network performance is the foundation of running every business well for the library. In the design, it should guarantee high throughout capability of network and equipment to ensure high-quality transmission of various data and information.

(4) Standard openness: It is helpful for ensuring a smooth connection among the network and future expansion if it supports universal standard network protocols, such as TCP / IP, and large dynamic routing protocols of international standard

(5) Manageability: It carries out centralized monitoring, decentralized management for the network and uniform distribution of bandwidth resources. It uses advanced network management platform, with management and traffic statistics analysis for the devices and ports, and provides automatic fault alarm.

4.2. Network Structure

Network system is an important guarantee for SSL VPN system, and it is the basis and prerequisite for SSL VPN system operation. Network exports bandwidth is the success guarantee for the remote access, which relates to the possibility of establishing VPN connection and the access speed after successful establishing. A good university library network system should have at least two net export of educational network and public network. Education net exports should normally be more than 1,000M and the public should be more than 10M, to ensure transmission of network streaming media, so that the users can visit the library network and use the resources taking advantage of the public network. The network topology of remote access to the library resources is shown in Figure 1.

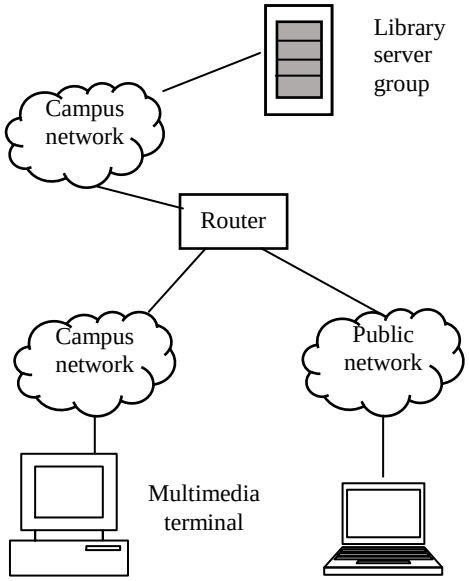


Figure 1. The Network Topology of Remote Access to the Library Resources

4.3. VPN Application Mode

SSL VPN system can be classified to SSL VPN server and SSL VPN clients according to their functions. SSL VPN server is a bridge between the public network and the private LAN, which protects the topology information in the LAN. SSL VPN client is a program running on a remote computer, which provides a secure channel for the remote computer access to the private LAN through the public network, so that the remote computer can access resources within the private LAN securely.

SSL VPN server is equivalent to a gateway router with two NIC and two IP addresses. One is the IP address that directly connected with the LAN, the other is the legitimate IP address that directly connected with the public network, which can ensure normal communication between the LAN and the public network.[12] The VPN solutions based on SSL include three modes, Web Browser mode, SSL VPN client mode and LAN / LAN mode.

(1) Web browser mode: The mode is the main advantage of SSL VPN. Because the wide deployment of the Web browser in Internet, and the built-in SSL protocol in the Web browser, therefore, in the access mode, users only need to centralized configure security policy without any configuration in the client. The remote user can access any resource in the digital library. In this mode, the SSL VPN server is equivalent to a data transfer server. When the user Web browser access to Web server, it will be authenticated, and then forwards to the Web sever. All the data from the Web server to the client will be encrypted by the SSL VPN server, and then be transferred to the Web browser of the user. The whole access process of the user is from the Web browser to the Web server, and pass through the SSL VPN server to construct a secure channel by the SSL protocol.

(2) SSL VPN client mode: In the SSL VPN client mode, its structure is basically the same as the Web browser mode, but the users need to achieve SSL VPN client program for the application, and will install and configure the program in the remote computer of customers. In this mode, SSL VPN client program is equivalent to a proxy client. When the application needs to access resources on the LAN, it will send a request to the SSL VPN server through the client, establish a secure channel and communicate with the LAN.

(3) LAN / LAN mode: The LAN / LAN mode mainly protects communication between the LAN transmission. This mode does not require any client installation and configuration for the client, and only need installation and configuration accordingly in the SSL VPN sever on the LAN. When the computer within a network access to the remote application sever of another LAN, it will go through the secure transmission between the SSL VPN sever of the two networks.

4.4. Remote Services Based on SSL VPN

Digital library system based on SSL VPN can provide a variety of services for readers.

(1) E-mail: For digital library system, e-mail is a basic function. IPSec VPN can protect the security of the mail system, but it needs to install the client software and connect to the system network of digital library, and then readers can use the internal mail system. If the staff use other people's computer or other network, he will faces address translation of the other firewall and obstacles brought by security policies, which cannot connect the digital library system, and cannot use the internal mail system.[13] It is a problem for the outward staff that it cannot connect to the internal system of digital library. SSL VPN provides a better solution, the staff can access Web-based e-mail system by any computer with a browser, and send and receive mail through SSL VPN secure channel. SSL VPN can also hide all the domain names and server addresses in the internal system, to improve the security of the system network of digital library.

(2) The internal network access of digital library system: Even out of office, readers also need to use some documents in the internal network of digital library, but under normal circumstances, the digital library system will not open the entire internal network to achieve file access. SSL VPN enable readers to access specific internal resources using any access device connected to internet with a browser anywhere.

(3) Network resources for the digital library system: In order to improve efficiency and strengthen partnerships, the digital library systems usually open the internal site and network resources. Considering confidentiality of the digital library system information, it has become an important problem how to ensure intended reader to access the corresponding resources and the information not to be intercepted in transmission. SSL VPN digital library can restrict a digital library or a reader to visit some pages and folders of a site, and does not need to modify its security policy, as long as the partners are able to access the Internet.

5. Conclusions

Compared to traditional IPSec VPN, SSL makes more remote users to access in different locations, visit network resources, and have low requirement for the client device, so it reduces the cost of configuration and operation. SSL VPN technology can access to important library database through a standard Web browser, improve the efficiency of the library, and solve the security problem. SSL VPN is to ensure that users can access to library information, therefore it is a remote access of low cost, high security and easy. VPN solutions are ideally suited to the users of Web-based applications and a lot of clients, which makes uses and readers access to digital resources without the limitations of time and space. It solves the technical problems of knowledge sharing and resource sharing, and really plays the library role in the sharing and popularity of knowledge and resources in the whole society.

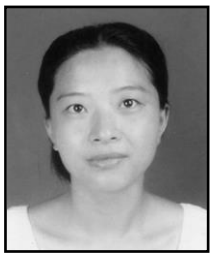
Acknowledgements

This study is supported by the Social Science Research Project of Linyi, Shandong Province, P. R. China (No. 2013SKL189).

References

[1] D. Wu, G.S. Chen and X.Z. Chen, "Study on Mode of Digital Library Resources Remote Access", Library Tribune, vol. 29, no. 3, **(2009)**, pp. 72-74.
[2] T.Y. Chen, M. Xing and X.Q. Pan, "Study on the Remote Access of Digital Resource of University Library", Modern Information, vol. 29, no. 11, **(2009)**, pp. 96-98.
[3] A.K. Zhang and C. Zeng, "Comparative Research of IPSec VPN and SSL VPN," Network and Computer Security, vol. 9, **(2009)**, pp. 98-100.
[4] Y.J. Li, H.C. Zhang and C.Q. Bi, "Digital Resource Remote Access of Library based on VPN", China CIO News, vol. 6, **(2011)**, pp. 124-124.
[5] Z.B. Du, "Library Digital Resources Visit Research Based on SSL VPN Technology", Digital Library Forum, vol. 4, **(2008)**, pp. 69-72.
[6] Q.J. Dong, "Research on user access mode of Digital Library based on SSL Protocol", Researches in Library Science, vol. 12, **(2005)**, pp. 16-18.
[7] B. Zhao, "Comparison and Choice between IPSec VPN and SSL VPN", Electric Power Information Technology, vol. 5, no. 9, **(2007)**, pp. 43-45.
[8] B.C. Liang, and M.Y. Li, "Applications of VPN Technology in the University Library Remote Access", Modern Information, vol. 28, no. 4, **(2008)**, pp. 82-84.
[9] S.C. Lin, "Comparative Study of IPSec and SSL VPN", Fujian Computer, vol. 29, no. 8, **(2013)**, pp. 11-13.
[10] Z.Q. Lin, "Research on Remote Access System Implementation of the University Library", Researches in Library Science, vol. 5, **(2009)**, pp. 43-46.
[11] W.Z. Zhu, "Using VPN to Realize Resource Share of University Library", Information Science, vol. 25, no. 7, **(2007)**, pp. 1058-1061.
[12] M.Y. Pan, "Applying SSL VPN Technology in the Digital Resources of Academic Libraries", Library Work in Colleges and Universities, vol. 30, no. 5, **(2010)**, pp. 74-76.
[13] A.V. Gerbessiotis and S.Y. Lee, "Remote memory access: A case for portable, efficient and library independent parallel programming Library", Science programming, vol. 12, no. 3, **(2004)**, pp. 169-183.

Authors



Mei Zhang, She received the Master's Degree of Arts from Qufu Normal University with the major of Foreign Linguistics and Applied Linguistics in 2009. She is a librarian of Linyi University, China. Her current research interests are focused on digital watermark image retrieval and remote access.