Research of Financial Informationization Construction system based on VPN Technology

Jun Zheng
Finance Department, Hebei United University, Tangshan, China
mycw1015@163.com

Jiantao Gu
College of Sciences, Hebei United University, Tangshan, China
gujiantaolg@126.com

Jiansheng Gao
Jitang College, Hebei United University, Tangshan, China

Abstract—With the continuous deepening of China's educational reform, “multi-campus” school system has become a common phenomenon in China colleges. It is a burning question that how to improve the efficiency of the financial management. Not only is VPN (Virtual Private Network) technology provide effective solutions for “isolated island” of financial information among campus but also VPN is a safe, reliable and cost saving new garrison networking. Through analysis of current university financial information systems status, based on MPLS (Multi Protocol Label Switching) and technology principles of VPN (Virtual Private Network) and combined with practical, financial information systems construction solutions are provided under multi-campus school conditions.

Index Terms—Financial Management, VPN Technology, Educational Recourse, Informationization Construction

I. INTRODUCTION

With the development of “multi-campus” school system, the scale of income and expenditure has gradually increased and financial accounting management has continually expanded. Currently, due to geographical isolation, most colleges in the financial management between campus and campus, accounting between first and second account is out of joint.

The problems which financial data is unable to achieve a unified real-time processing, real-time summary, daily data calling, etc. have made the difficulties and pressure increasing gradually. Financial informationization construction is urgent to further enhance and to realizing unified, effective off-site financial management and ensuring safe and reliable financial data off-site transmission through technical means to solve the problem of financial system data synchronization in the multi-campus school system, see [1-2]. This paper provides a VPN technology used in the construction of the university's financial informationization program through researching Vpn technologies and combining with the practical situation of multi-campus school system [3-7].

II. THE CURRENT PROBLEMS IN THE FINANCIAL INFORMATIONIZATION CONSTRUCTION OF CHINESE COLLEGES

In recent years, the new mega university superintendence of the financial management system shall operate under the principle of unified leadership and decentralized administration, that is, colleges, various campuses and other branch schools are grading management, but still faces many problems and difficulties that are manifest in the following aspects:

A. Application of information networking management methods is not enough.

With the improving of consciousness in safeguarding their legal rights, the clamor of faculty and students for financial information publicity grew louder. From the standpoint of financial work, to acquaint departments, faculty and students with the major issues in the immediate interests by appropriate discoursing of financial information is one of the core contents in financial services.

From the standpoint of management, the information management requires financial data to achieve high degree of sharing and "seamless" link with the data management systems (accounts, assets, budget and project funding, fees, wages, academic, students, and logistics), to meet the needs of schools and departments in querying financial data.

As the campus location relative dispersion, we need to carry out the construction of the campus network vigorously, public necessary financial information online and take full advantages of VPN technology to enhance the financial management efficiency.

B. The Differences of Accounting Model

Schools in size, management system is different, also accounting mode is not the same before merging. Schools in large-scale and large volume of business may implement the "centralized management, decentralized
accounting" or "decentralized management, decentralized accounting", and has achieved computerized accounting.

Schools in small-scale and few volume of business may implement the "centralized management, centralized accounting" and even stay at the stage of hand-made account. It is a common phenomenon that financial management is inefficiency as complex and task hard of financial management. Improve efficiency, that is make all resources are fully utilized.

Through the VPN, financial management tends to standard, informational and scientific. Standard working process of finance management staff makes the overall financial management systematic and comprehensive.

C. The number of campuses is large and they distribute in different territory. The overall business volume is large, but the workload was unbalanced.

The phenomenon that campuses distribute in different territory is common in combined school increased the difficulty of unified accounting. All levels accounting offices implement the "self-contained, fragmented, decentralized accounting" financial management model. The financial system policies in accounting, financial expenses, income and other aspects were made by different departments.

There is no clear division of the responsibility and authority of all levels accounting offices in the financial work. There is no reasonable run mechanism of the fund use and calculation, which make the property movement out of joint.

D. The quality of staff in accounting offices is uneven and they have formed a certain way of thinking and "inertia" of accounting treatment under the influence of the existing accounting system and policies.

In addition to their original campus, some accounting staff is unfamiliar with other cases. In such circumstances, some staff begin to work would lead the obtained accounting information is difficult to reflect the financial situation truly.

Also the actual conditions that coordination between every position is poor and internal control weaken are not conducive to the financial sector implement effective, comprehensive supervision to the overall financial; The actual conditions that the financial district offices are far from each other and business processing tools are lag, it can not pass a real and effective accounting information are not conductive to the school leaders operate, deploy and control the funds cause the precipitation and waste of money.

E. Financial data is not fully utilized.

From the standpoint of manage tools, part of the financial management work is still in the manual or computer-aided stage. In the artificial management stage, administrative tasks are accomplished mainly depend on manual and information feedback lags behind the financial management activities in the process of financial activities.

In the artificial management stage, Information exchange and preservation with paper media as the carrier, the scope of information gathering is limited by the time and space, information transfer methods are obsolete, slow and lagging, financial data information is out of date and financial data is not fully utilized.

III. VPN CONSTRUCTION

A. The Background of VPN

In the information economy period, a growing number of organizations and users is a great convenience from the Internet. But at the same time, people have to face the brought challenge of data security from the open Internet. If the data transmitted over Internet was not protected effectively, a large number of important data will be exposed to the public, which would result in severe loss to the user if exposed data are stolen by criminals and used for illegal purposes.

Under this circumstance, research institutions and schools were engaged in computer information security put forward a lot of solutions. And one of the best solutions for computer network security requirements is the VPN technology.

It is a new network concept that using VPN to build the public network which will bring a lot of benefits for Internet service provider (ISP) and VPN users. For users, the special line cost can be reduced to a small fee and Internet costs by setting up a private network using Internet.

In related reports analysis, only the LAN interconnection costs can be reduced by 20% to 40%, while the remote access costs can be reduced 60% to 80%; For internet service providers, can establish closer cooperation with users and make full use of existing network resources and increase business volume through providing the value-added services for VPN users.

B. System Design Overview

Virtual Private Network (VPN) is a "service that giving users a feeling of direct connection to the private LAN based on public data network." VPN reduces the cost of the user significantly and provides stronger security and reliability than traditional methods.

VPN system is the filter driver that commonly used application layer VPN technology based on the network protocol stack, increased security subsystem between the TDI layer and protocol stack in the system and accomplished key management, negotiation, data encryption and decryption.

C. VPN technology principle and function

Virtual Private Network (VPN) is a technology using public network to build private network can be used to build the VPN public networks including Internet, Frame Relay, ATM and so on. "Virtual" concept is opposed to, "Virtual" is a new concept compared to the traditional way in terms of building a private network. For WAN connection, the traditional connection is achieved through remote dial-up networking, but VPN use the public network provided by the ISP to achieve remote WAN connections.
Users can connect remote secondary institutions, other partners at a lower cost with VPN. VPN technology has the security, reliability, manageability and scalability characteristics.

The main purpose of VPN technology is to protect the transmission data: protect the information flow which transfer from one endpoint to another in the channel. The main purpose of VPN technology is to protect the transmission data: protect the information flow which transfer from one endpoint to another in the channel. Normally VPN uses packet encapsulation (tunneling) technology.

VPN can imitate the point to point connection technology and make the data packet transmission through the private tunnel which built rely on ISP and NSP in the public network. They can be opened separately to different tunnels for different sources of information.

Rely on the public network facilities; tunnel is a data transmission method in the special “network” of the network. Tunneling protocol encapsulated frame with the additional header and the additional header provided routing information, so the encapsulated package can pass the middle public network.

The logical path that encapsulated package passed the public network is called "tunnel." Once the encapsulated frame reached the destination of the public Internet, the frame would be lifted encapsulation and continue to send to the final destination. Data transfer through the tunnel can be 1 different protocol packets. Tunnel protocol re-packaged these packets in a new header and new header provides routing information so that the encapsulated data can be transmitted through the Internet network.

- **The main purpose of VPN technology is to protect the transmission data: protect the information flow which transfer from one endpoint to another in the channel.** Normally VPN uses packet encapsulation (tunneling) technology. VPN can imitate the point to point connection technology and make the data packet transmission through the private tunnel which built rely on ISP and NSP in the public network. They can be opened separately to different tunnels for different sources of information. Rely on the public network facilities; tunnel is a data transmission method in the special “network” of the network. Tunneling protocol encapsulated frame with the additional header and the additional header provided routing information, so the encapsulated package can pass the middle public network.

- **Tunneling Protocol:** PPTP (Point to Point Tunneling Protocol) is a point to point secure tunneling protocol developed by the PPTP and is the expansion of PPP. PPTP adds a new level of security which supports establishing the on-demand and multi-protocol virtual private network through the public network. VPN transfer data by enabling PPTP is as safe as in the unit LAN. In addition, the dedicated LAN to LAN network can be established with PPTP. SSL (Secure Sockets Layer) is a security protocols based on Web application suggested by Netscape user. SSL provides data connection security between HTTP and TCP/IP, data encryption, server authentication, optional client authentication and message integrity verification. SSL is regarded as the Internet Web browser and server security standards. “IPSec” (IP Security) is the general name for widely used, open protocols. IPSec applied in the network data of IP layer and provided security architecture including network security protocols AH and ESP, key exchange protocol IKE and algorithms used for network authentication and encryption. MD5 and SHA-1 are most commonly used of AH standards, MD5 uses up to 128-bit keys and SHA-1 up to 160-bit keys provide stronger protection, DES up to 56-bit key and IPSec also supports 3DES, so the password algorithm has high security. IPSec set how to choose security protocol between the peer layers, to determine the security algorithms and key exchange, to provide upwardly access control, data origin authentication, data encryption and other network security services.

- **Information Verification and Identification:** Strict user authentication VPN system used in CA certified system (asymmetric key certificate system), that is to establish a unified authentication and authorization system in the information center VPN control platform. When user accessed VPN gateway through VPN client, the client authenticated user’s two-factor, that is to say user has a user digital certificate and the password of it. VPN Client used digital certificates technology based on PKI technology to complete the mutual authentication of VPN gateway server and user’s identity. The client also supports two-factor authentication. Every entry will have a strict log for audit in the future. Also, VPN system increased user's digital signature, that is, non-repudiation of transactions data, this technology is generally used to protect sensitive financial information. Therefore, compared with the normal line, the mandatory certification measures of VPV system ensured the security of the units network service accessing and auditing.

- **Data Encryption:** The perfect VPN system should not only improve the user's identity
authentication, but also certificate the transmission data to ensure that the message has been sent and there is no distortion. VPN generally provides more than 128-bit symmetric-key encryption (asymmetric-key algorithm uses 1024-bit), uses application layer VPN technology of the network protocol stack and one-time password system, data security is extremely high. Meanwhile, VPN uses the data MD5 digest algorithm to protect the integrity of the data transmission process. The common line does not provide any encryption measure. VPN technology, although it built on the Internet, its high-strength encryption make data transmission security is much higher than the normal line. VPN technology effectively prevents the transmission of data intercepted and tampered by others.

- **Provide Access Control:** People always pay attention to the security of financial information, security is controlled access. Therefore, the process of implementation the security is the process of access control. Password and firewall can help us to realize the access control of information reading and writing permission. VPN technology requires different users have different access rights. School organize inner parts to exchange important information with VPN network, which requires schools’ VPN system must have strict access control mechanisms. VPN technology uses Accessing Components List (ACL), administrators can easily assign different access privileges for each user. ACL based on the user identity, and its management is not relevant to technical maintenance of the VPN system. Schools can give function departments the work of make and manage the ACL, which both facilitate the management of schools and effectively prevent the network maintenance personnel stealing school confidentiality. There are two types of VPN communication: Remote Access VPN (Access VPN) and Router to Router VPN, which also includes Intranet VPN (Intranet VPN) and Extranet VPN (Extranet VPN).

### Table 1. PPTP Control Connection Packet Format

<table>
<thead>
<tr>
<th>Data-link Header</th>
<th>IP</th>
<th>TCP</th>
<th>PPTP Control Message</th>
<th>Data-link Trailer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data-link Header</td>
<td>IP</td>
<td>GRE Header</td>
<td>PPP Header</td>
<td>Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)</td>
</tr>
</tbody>
</table>

Fig.1. Resulting Packet Structure

A VPN is a private network that uses a public network such as the Internet to connect users or remote sites together in a secure manner. VPN direct-connect solutions are extremely popular, due to their low cost to deploy. Instead of using a dedicated connection, such as leased-line direct circuits, the VPN option uses tunnels routed over the Internet from the company’s private network to the Verizon Wireless network operations center. VPN tunnels are terminated by the Verizon Wireless VPN gateway.

This approach uses a business’s existing connection to the Internet and requires IP Security (IPSec)-compliant VPN gateway equipment at the enterprise location. The Verizon Wireless VPN option secures the communication path between the enterprise location and the Verizon Wireless network operations center. Unlike a client-to-server solution, it does not secure the complete path from the mobile device to the enterprise’s VPN gateway. A VPN solution also does not offer the typical reliability and controlled redundancy of leased-line direct connections.

Mobile terminals

Verizon Wireless network

VPN connection via Internet

Enterprise network

Fig.2. A customer VPN connection diagram
VPN technology, modern financial management tools, led a new, profound changes in financial management. First, VPN technology accomplished work coordination and data sharing and optimized the school public resources.

Second, VPN technology accomplished the integration between information system and the concept of financial management and enhanced the overall capabilities of modern financial management.

Third, VPN technology accomplished the integration between information system and the mode of financial management, greatly pushed the development of deepening teaching reform and further improved the modern quality of finance staff and training quality of talent.

---

IV. DATA ENCRYPTION TECHNOLOGY

Encryption technology as an active means of defence. General data encryption model showed in Figure 4. Plaintext X used encryption algorithm E and encryption key K to get the cipher text

\[ Y = E_k(X) \]  

There may have the ciphertext capturer in the transmission process. At the receiver, it decrypts the received ciphertext

\[ D_k(Y) = D_k(E_k(X)) = X \]  

by using the decryption algorithm D with the decryption key K'. In the above model, encryption keys K and decryption keys K' may be the same or different. Key is usually provided by the Key distribution center (KDC). When transmitted to the remote, the key must pass another secure channel.

So far, published encryption algorithms were up to hundreds. The encryption algorithm can be divided into counter key algorithm and public key algorithm according to whether encryption and decryption keys are the same or equivalent.

---

(a) Symmetric key algorithm

Encryption key can be derived from decryption key in the Symmetric key encryption algorithm, in turn, it is also established. Symmetric key algorithms require the sender and receiver to decide a key before secure communication. As the symmetric key algorithm is public, so the security depends on the key security.

Well-known symmetric key algorithm: DES and its variants of the United States such as Triple, GDES and New DES; IDEA of Europe; FEAL-N of Japan, LOEI-91, Skipjack, RC4, RC5, classical rotary password represented by the substitution cipher and rotor cipher. The greatest influence in symmetric key algorithm was DES algorithm.

Encryption and decryption of symmetric key algorithms can be expressed as:

Encryption: \[ E_k(X) = Y \]  
Decryption: \[ D_k(Y) = X \]  

Symmetric key algorithm has the advantage of strong security strength and fearlessness of the test of time and attack, but its key must be transmitted through secure channels. Therefore, the key management becomes an important factor in system security.

DES (Data Encryption Standard) algorithm which was a kind of symmetric key algorithms and developed by IBM and considered as the Federal Information Standards of the United States in 1977, has become a world-wide standard 20 years.

DES algorithm is 64-bit key length, but only 56 bits has the actual work, 8 bits are used for each parity, can be ignored.

DES is a Block Encryption Algorithm. The entire plaintext was classified before encryption, each group is 64 bit. After the initial permutation IP, divided each 64-bit plaintext group X and key K into left-L_0 and right-R_0 which is 32-bit. After 16 rounds, the left and right get together and the final permutation IP\(^{-1}\) then get the ciphertext \( Y \):

\[ Y = IP^{-1} \circ I_{16} \circ I_{15} \circ ... \circ I_1 \circ IP(X) \]  

---

© 2012 ACADEMY PUBLISHER
In each iteration (See figure 5), the 56 key bits are shifted, in two halves, by one or two bits, and 48 bits selected by a "compression permutation", to form a sub-key for the round. The right half of the text is expanded to 48 bits using an "expansion permutation", and XORed with the sub-key for the round. The result is sent through a set of 8 fixed "S-boxes", which map 6-bit substrings to 4-bit outputs. These are concatenated to obtain a new 32 bit string. The S-boxes effectively implement a variable substitution operation on a 4-bit (16 character) alphabet. The new string is permuted using a fixed permutation. This completes the application of the f function to the right half. The new 32 bit string f(Ri) is XORed with the old left half, and the new 64 bit string (Ri, L XOR f(Ri)) is sent to the next round, except for after the last stage, when the swap is not performed, and (L XOR f(Ri), R) is sent to the last step.

\[ L_i = R_{i-1} \]
\[ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \]  
where \( i = 1, 2, \ldots, 16 \). And \( K_i \) is the 48-bit key (\( K_i \) was derived through several transformations of the original 64-bit key).

![Fig.5. The i-th round iterative process](image)

(b) Public Key Algorithm

In this algorithm, the key used for encryption is different from decryption and encryption key can not be derived based on the decryption key (at least within the reasonable assumption time). Encryption key which called public key (Public Key) can be expose, decryption key which called the private key (Private Key) must be kept confidential.

Strangers can use the public key encrypted information, the one who held the private key correspond with the public key can decrypt. Encryption algorithm and decryption algorithm of symmetric key are public, so the private key must not be compromised. Well-known public key algorithm: RSA, Knapsack Algorithm, McEliece, Diffie-Hellman, Rabin, Elliptic Curve Algorithm and so on. The greatest influence algorithm was RSA, which can resistant to all attack from known password.

Encryption and decryption of public key algorithms can be expressed as:

Encryption: \( E_{PK}(X) = Y \)

Decryption: \( D_{SK}(Y) = X \)

Public key algorithm can adapt to the requirements of network opening and key management problem is simple, in particular, which can realize digital signature and verification. But the algorithm of public key is complex and the rate of encrypted data is lower. However, with the development of modern electronic technology and cryptography technology, public key algorithm is a promising network security encryption system.

RSA algorithm was proposed in 1976 and published in 1978 by American scientists Rivest, Shamir and Adleman. According to the knowledge of number theory, it was simple to select two big prime numbers, while it was extremely difficult to factorize product form. The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation: RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:
1. Choose two distinct prime numbers \( p \) and \( q \). For security purposes, the integers \( p \) and \( q \) should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute \( n = pq \). \( n \) is used as the modulus for both the public and private keys.
3. Compute \( \phi(n) = (p-1)(q-1) \), where \( \phi \) is Euler's totient function.
4. Choose an integer \( e \) such that \( 1 < e < \phi(n) \) and \( \gcd(e, \phi(n)) = 1 \), i.e. \( e \) and \( \phi(n) \) are coprime.
5. Determine \( d = e^{-1} \mod \phi(n) \); i.e. \( d \) is the multiplicative inverse of \( e \mod \phi(n) \).

The public key consists of the modulus \( n \) and the public (or encryption) exponent \( e \). The private key consists of the modulus \( n \) and the private (or decryption) exponent \( d \) which must be kept secret.

Encryption: Computing the ciphertext \( c \) corresponding to \( c = m^e \mod n \). This can be done quickly using the method of exponentiation by squaring.

Decryption: Recovering \( m \) from \( c \) by using private key exponent \( d \) via computing \( m = c^d \mod n \).

For the details see [11-13].

V. THE APPLICATION CASE OF VPN TECHNOLOGY IN THE FINANCIAL MANAGEMENT

Taking a university financial VPN network system as an example, the paper illustrates the application of VPN technology in the financial management under the multi-campus educational model.
A. Needs analysis

Taking a university as an example, currently consists of five parts: Xinhua Road Campus, Jianshe Road South Campus, Jianshe Road North Campus, Fengnan Campus and Qian'an campus, Xinhua Road is the main campus and Jianshe Road South Campus is about 30 kilometers apart from the main campus. Five campuses linked financial server and charged students’ tuition fees and external reimbursement, the financial computer room set on the main campus.

Construction of financial core data server and remote accessing of other campuses take into account that other campuses financial sectors access the financial core data server of the main campus, the number of prospects are more complicated than the original number and increase more than two times.

In order to ensure that the financial core data server's normal, safe operation, especially to ensure data security and disk read and write performance, special requests were made in the technical parameters of server hardware. The original server used as a data-sharing server, provided a WEB inquiry service separately, such data accessing mode will not bring additional financial load and insecurity to the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.

Comprehensive information searching platform provide real-time, convenient, and fast information query for staff and middle sectors. In order to ensure security of data backup, another PC configured as a dedicated data backup server for storing the copy of financial core backup, preventing the financial data losing because of the sudden fault of the core data server. Such data accessing mode provided integrated information searching platform, but also effectively ensured high-efficiency of the normal financial systems and security of financial core data.
the TOPSEC class network guards firewall NGFW4000 series with the VPN module and powerful functions.

The configuration of TOPSEC NGFW4000 series firewall is very convenient. And mobile client need to install TOPSEC VPN remote client (VPN Remote Client). VRC client software can be used to establish a VPN encrypted tunnel with financial network, which is an IPSec-based security link.

So the security link can provide reliable, flexible security guarantees to the IP and upper layer protocols and allow clients access the financial network resources safely and quickly. Established firewall certificates in VPN management and exchanged to enable VPN tunnel connection, and import the client certificate for VRC users to access the financial resources.

With the growing popularity of computers and networks, the network environment has been beset with crises, the data may be destroyed at any time and we must back up system and data in time.

Especially the financial data is extremely important for any unit, once data loss would cause incalculable damage and restore the data you need to pay a high price. Therefore, we must optimize the storage system architecture to ensure financial data security and reduce the data losing risk to the minimum.

VI. CONCLUSIONS

Under the multi-campus school mode, geographical isolation led the financial information is not data synchronization and management unification. VPN technology provides remote access, extranet and intranet security link, which is suitable for the financial network construction that requires high reliability and security of data.

Financial private network based on hardware VPN technology provides a good infrastructure network platform for achieving computer information unified management and maintenance and provides strong technical support for financial information construction.

ACKNOWLEDGMENT

The research was supported by Projects of Hebei Province Education Department (cwzx201145 and cwzx201129).