A New Method Of VPN Based On LSP Technology

HaiJun Qing[1, 2], ChaoXiang Liang[1, 2], LiPing Chen[3]

1 School of Information and Electronic Engineering,WuZhou University
2 Guangxi Colleges and Universities Key Laboratory of Professional Software Technology
3 First Middle School of WuZhou
WuZhou, 543000, China
qingnavy@qq.com, 420844683@qq.com, 393946674@qq.com

Keywords: Layered Service Provider, Virtual Private Network, data packet

Abstract

With the rapid development of mobile Internet and intelligent terminal, the demand of the remote access network is more intense than before. The virtual private network is a common solution to this problem, with its traditional technology realized by a security protocol and tunnel mechanism. But this is complicated and not flexible enough by the constraints of protocol. So it is a challenge for enterprises to adopt a more flexible and customized way to enable the employees to make remote access to the intranet. A new virtual private network based on layered service provider technology is proposed in this paper, by using layered service provider technology to intercept the network data packets, so the data packets can further receive their encrypted conversion and integrity check. The virtual private network system based on layered service provider technology doesn't need any security protocol, with its flexible security which caters to the needs of personalized and customized remote access.

1 Introduction

With the rapid development of mobile Internet and intelligent terminals, the virtual private network (VPN) technology is the most economical and secures solution for remote access network. VPN technology is a virtual private channel for users to access enterprise network. Its security features include encryption protection, integrity protection, and authentication and preventing malicious attacks and so on [1]. The traditional VPN technology is based on a specific security protocol, in fact, the essence of VPN is encrypted the private data by the public network, so that the connecting performance for a virtual line to external. So as long as the aforementioned security features can be achieved, the VPN technology can be more flexible.

The traditional VPN technology mainly employs the tunnel protocol with the two or three layers in the transmission control protocol/internet protocol (TCP/IP) architecture, with original data packets encapsulated by tunnel protocol, which has generic routing encapsulation (GRE), internet protocol security extensions (IPSEC), etc. [2-7]. There is also a remote access VPN based on secure sockets layer (SSL) protocol, which does not apply the tunnel technology to remote access and work in between the third and fourth layers in the architecture. Almost all of VPN technology design is based on the existing security protocols with different implementation technology, without enough flexibility. And it cannot meet personalized needs while its implementation mechanism is complex and huge. So how to achieve remote access to the intranet in a lightweight way is a valuable exploration. The VPN technology based on the layered service provider (LSP) do not depend on SSL, IPSEC protocol etc., so it can be customized according to the needs of enterprise development, and the client and server can be simplified as much as possible. It can also provide service for the hypertext transfer protocol (HTTP) and other applications, with its security freely controlled; the enterprise can choose encryption algorithm and key length according to their own security needs.

2. New method of VPN implementation based on LSP technology

2.1 LSP Technology

LSP is a layered service provider which is the implementation of Winsock 2 mechanism of Microsoft. The

Winsock 2 service provider interface (SPI) is implemented by network transport service providers and namespace resolution service providers [8]. Winsock 2 SPI can be used to extend an existing transport service provider by implementing a layered service provider. For example, Quality of Service (QOS) on Windows 98 and Windows 2000 is implemented as an LSP over the TCP/IP protocol stack [9]. The Winsock2 architecture diagram is shown in Figure 1 and LSP between

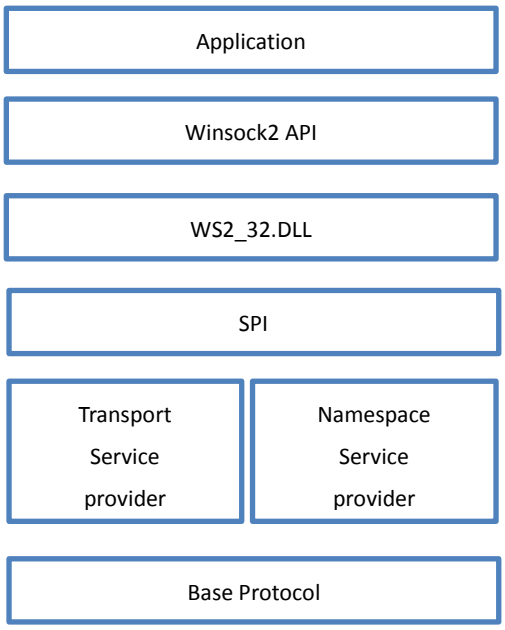

Fig 1 Winsock2 architecture diagram

WS2_32.DLL and base protocol, which plays a connecting role.

There are many applications which grab and process network data, such as firewall, security manager, bandwidth manager and data stream filtering. Various kinds of applications work on the network data flow at different levels, but they intercept and process the data at the places where the data must pass. The network data channel flows through different levels, such as network driver interface specification (NDIS), LSP, transport driver interface (TDI) and application programming interface (API) layer. The network data can be controlled, filtered and processed when it flows through in any layers. The lower level of the network is, the more transparent the user program is, and the more powerful the function is, and the more difficult it is to design and implement [10].

The LSP technology is to intercept and process data in the next layer of the API system. We implement VPN by LSP in this paper and its essence is to capture data packet and encrypt. Also we can use other methods to achieve VPN, such as NDIS, TDI and API etc. however, the LSP method can be used to achieve a good balance between difficulty and transparency.

2.2 The new method of VPN implementation based on LSP technology

2.2.1 The function structure design of VPN client and server

The VPN client functional structure design scheme is shown in Figure 2. The VPN client includes three modules such as data interception, parameter negotiation and identity authentication. Data interception module is responsible for intercepting encrypting decrypting verifying the data packet according to the parameters. The parameter negotiation module is responsible for the negotiation key, encryption and decryption algorithm and the integrity verification algorithm. The encryption and decryption algorithm suitable use symmetric encryption and it can reduce the complexity and improve the performance of the system. But the distribution and negotiation of the key suitable use asymmetric encryption. The identity authentication module is responsible for verifying the authenticity of the identity of the client, and it can use the password authentication method to authenticity. The parameter library mainly includes key, encryption and decryption algorithm and integrity verification algorithm parameters. The length of the key depends on the encryption and decryption algorithm and the actual needs. The encryption and decryption algorithm and the integrity verification can be selected from the backup algorithm. These parameters can be selected according to the settings of the front end and security level; generally speaking, a higher security will lead to a reduction in performance.

the server of VPN can adopt a similar architecture with the client of VPN, but the identity authentication module in the server is must to be changed into the verification module and the parameters library of the server must storage more parameter than the parameters library of client storage. The parameters library of client just save the parameters related to the client, and the parameters library of server must save all the parameters of all clients. The server can obtain different parameters to encryption decryption and integrity check according to different client. In addition, the server needs to

add a data packet forwarding agent module, so forwarding the

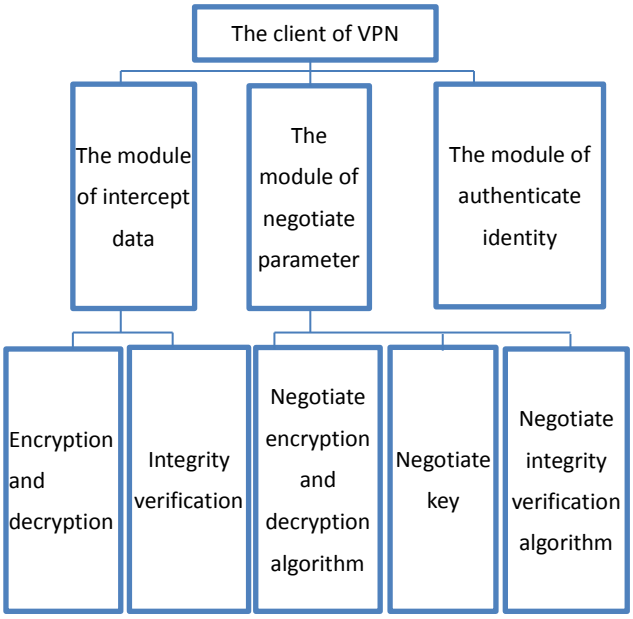

Fig 2 the VPN client functional structure diagram

data received from the remote access, at the same time, the data packet sent by internal network host transmitted to remote host. In order to the remote host achieve the final access to the internal network.

2.2.2 The process design of client and server

The client process design diagram is shown in Figure 3, where the two core steps are parameters negotiation and data interception. Parameter negotiation process includes negotiation of encryption and decryption algorithm, key and algorithm of integrity verification. The encryption and decryption algorithm can be selected according to the performance of the client machine and the safety requirements of the enterprise from the encryption and decryption algorithm list, and it is suitable to use the symmetric cryptography .The key can be generated by the server according to the request of the encryption and decryption algorithm, and then the client's public key can be used to encrypt the key and send the key to the client, so the client will receive the encrypted key and use the private key to decrypt it. Then the server and the client can use the key to carry out communication.

In the system, a special database is used to store all the information of LSP. When the application needs to create a Socket for communication, the system will search the database for matching LSP and load it so that the system can pass the communication requirements to the next. So the installation of the LSP is to configure the LSP information into the system database of Winsock 2, where the LSP will be packaged into dynamic link library (DLL). The specific process is as follows:

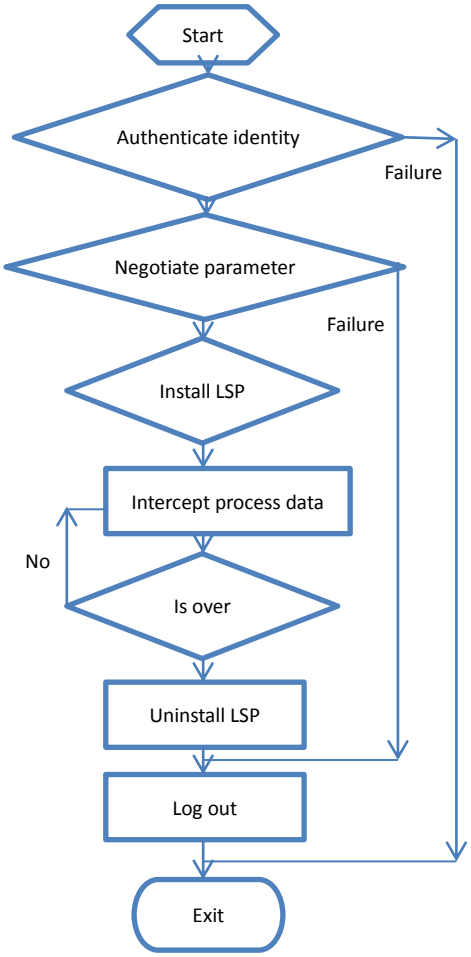

Fig 3 the client process design diagram

(1) Enumerate all the LSP directories, and find the first TCP, user datagram protocol (UDP) protocol chain directory, and save it.

(2) Call the WSCInstallProvider function to install the LSP of the client, once again enumerate all the LSP directories, and obtain the LSP directory's identification (ID).

(3) In the TCP and UDP protocol chain directory which is saved in the first step insert the ID of the second steps obtained

(4) Call the WSCInstallProvider function write the protocol chain directory which is rewritten at the third step to the Winsock 2 configure library.

(5) Call the WSCWriteProviderOrder function to resort the Winsock directory, and put our protocol chain directory in

front.

The process design for the client is mentioned above, and the server needs to load authentication module to verify the identity of the client followed by parameter negotiation between the client and the server. After negotiated successfully with the first client, then LSP for encrypted communication will be loaded, so the subsequent clients will only need to negotiate parameters with the server, and repeated loading LSP will no longer be needed, and the server parameter library will save all parameters which are unique to each customer, which will enable them to carry out encryption communication and integrity check. In addition, the server needs to increase the agent and forwarding process of remote host data packets, at the same time; it needs implement the process of package disassembly and re package.

2.2.3 The implementation of client and server LSP of intercept network packet

The LSP must be packed to DLL file, and the main work done in the DLL file includes two aspects. The first aspect is to load the next layer of LSP, and then the LSP is stacked to a hierarchy structure, with each layer filtering and processing the network data packet based on their needs. The second aspect of the work is to modify the function table, with the bottom of the function being replaced with their own functions, so as to filter and process the past network packet in their own functions. After filtering and processing the network data packet, the bottom of the function will be called to complete some basic receiving and sending work. These two aspects mentioned above will be discussed as follows.

Firstly, the process of loading the next layer of LSP is as follows:

(1) The ID of the lower level protocol will be found based on the parameter lpProtocolInfo of the WSP Startup function.

(2) To Enumerate all LSP based on the previous step of the ID to find the directory of the lower layer protocol.

(3) Find the next layer of LSP file directory by the directory at the second step.

(4) Call the Load Library function to load the DLL LSP, and get the address of the WSPStartup functions of next layer.

(5) Replace the corresponding function in the underlying function table with a custom function.

(6) Call the WSPStartup function of the lower level with the parameter of the upper function table, the lower level function table, and so on.

Secondly, modify the function table.

When the WSP Startup function of the lower level LSP is called, the bottom function table will be replaced with a custom function, and the following functions need to be replaced, such as RecvFrom, Send, Recv, and SendTo etc. After the function mentioned above being replaced, the custom function can be implemented. The Send function is used as an example to describe the process of the custom function WSPSend, and the same is true of other custom functions in terms of processing.

The processing of WSPSend functions is as follows:

(1) Check whether the destination address of the packet is specified for the enterprise intranet address.

(2) If the packet destination address is the intranet address of the enterprise, read the client key, encryption algorithm, integrity checking algorithm and other parameters from the parameter library.

(3) Replace the destination internet protocol (IP) address with the VPN server IP address, and the destination IP address is saved in a data packet some location.

(4) Encrypt the network data packet by using the specified encryption algorithm. HASH the encrypted data packet by the specified integrity check algorithm. Then write the verification code which obtained by integrity algorithm into the data packet.

(5) Call the Send function of the below layer with the parameter of the modified data packet.

For Recv, RecvFrom, SendTo and other functions, they can be carried out similar processing with send function. For the receiver function, the function is decryption and verification the integrity of the data packet, the operation is the opposite.

The implementation of the client LSP is discussed above, and the same is true of the server to load the next layer of LSP, with its similar custom functions, but what should be paid attention to is the definition parameter should cater to different clients.

3. Implementation of VPN system

We used the Visual C++ to achieve the VPN system of the client and server on the windows platform. Due to the

development of a complete set of VPN system workload is very large, so we just use LSP to catch the data packet and encrypt it and provide the proxy service. VPN system's client and server needs less code to implement with only more than 4000 and 5000 lines. We used the DES encryption algorithm to encrypt and decrypt the network data packets in the data interception module. Then we deploy VPN server program in the company's server and the client program is installed on the computer at home. The connectivity of the system and the speed of the network are tested. The connectivity of the system is verified. Due to the factors impact of the network speed is more, under the limit of the communication operator 4Mbps speed, we test its speed up to 3.2Mbps. Of course, the universality of the experiment and the completeness of the function need to be further improved.

4. Discussion

This method we presented in this paper has three main advantages over the traditional VPN implementation based on security protocol as follows: 1. Light weight. The traditional VPN implementation based on a security protocol is complex and large and requires hardware support in some cases. For example, The VPN system based on IPsec protocol designed by Wang is implementation by hardware, its cost is very high and it is a very complex technology [3]. The method used in this paper is not restricted to the security protocol, but it can realize the security characteristics of VPN system by simpler methods, which therefore simplifies the design of VPN system. 2. Freely controlled security. Mr. Liu pointed out the VPN system based on SSL protocol mainly use DES and RC4 etc. symmetric encryption algorithm to encrypt the network data packet which limit its flexibility [4]. The VPN implementation methods we presents in this paper doesn't restrict the algorithm of encryption and decryption as well as key length, so these parameters can be flexibly negotiated based on the need of actual security levels by enterprises. 3. Flexibility and convenience. While the traditional VPN implementation method bound to a certain protocol with its restrictions and standards. Mr. Yang pointed out installation and configuration the VPN system based on IPsec protocol is very complicated and not easy to flexible deploy in complex network environment [7]. The VPN implementation based on LSP technology is not limited to a particular application or application protocol, which provides a flexible processing method between application layer and transport layer.

Although the VPN implementation method we proposed have some advantages. But compared with the traditional method, there are three main problems. 1. The method proposed in this paper is more applicable to the case of remote access to internal network, for the case of intranet VPN and extranet VPN may have not good performance. 2. The method proposed in this paper need to be further verified. While the traditional VPN method is a more mature method. 3. The traditional implementation method has formed a certain standard with it has been widely accepted. The method proposed in this paper need to be further studied.

5. Summary

This paper presents a new VPN system implementation method compared with the traditional VPN implementation method without using existing security protocols to achieve VPN. Since the essence of the VPN communication is to provide identity authentication, confidentiality and integrity, LSP technology is artfully used to complete the function of the VPN, which can satisfy customized needs of some enterprises with its flexibility and personalized methods. Of course there is a deeper step to verify this method; next we will improve the function of the experimental system as well as the experiment in more scenes.

Acknowledgements

This article is supported by Young and middle-aged backbone teacher training program Of Wuzhou University.

References

[1] Yao Yonglei and Ma li, Network security of computer (the second edition), Beijing, Tsinghua University press, (2011)

[2] Zhang Kaixia, Research on the Design and Realization of VPN-Based Campus Mobile OA, Dissertation, Nanjing University of Posts and Telecommunications, (2013)

[3] Wang Yan, Design and Implementation of VPN System Based on IPSEC, Dissertation, University of Electronic Science and technology, (2013)

[4] Liu Hongqiang, Research and Implementation of SSL-based VPN, Dissertation, Shandong University, (2008)

[5] He Yahui, Xiao Lu, Chen Fengying, "Principle and

Application of IPSec-based VPN Technology", Journal of Chongqing Institute of Technology, vol:20, pp,114-117, (2006).

[6] Xu Kunliang, Wu Man, "Research on VPN application based on IPsec protocol", Computer knowledge and technology, vol:11, pp:52-53,(2015).

[7] Yang Wenkai, Research on security key technology of SSL VPN, Dissertation, Southwest Jiao Tong University, (2010).

[8] Hu Junhua, Wei Fang, "Online game acceleration based on LSP proxy" Computer applications and software, vol:29, pp:149-153,(2012).

[9] Wei Hua, Jim Ohlund, Barry Butterklee MSDN Home. http://www.microsoft.com/msj/0599/LayeredService/LayeredService.aspx. (1999).

[10] Leng Wei, Lu Yu, "Using LSP Technology to Build Simple Firewall", Journal of Institute of Command and Technology, vol:12, pp:169-172,(2001).