Secure VPN Based on Combination of L2TP and IPSec

Ya-qin Fan  
College of Communication, Engineering, Jilin University  
Changchun 130012, china  
Suntianhang27@163.com

Chi Li  
College of Communication, Engineering, Jilin University  
Changchun 130012, china  
610516518@qq.com

Chao Sun  
College of Communication, Engineering, Jilin University  
Changchun 130012, china  
Sunchao.s.c@163.com

Abstract- This report is written to provide a method of building secure VPN by combination of L2TP and IPSec in order to meet the requirements of secure transmission of data and improve the VPN security technology. It remedies the secured short comes of L2TP Tunneling Protocol Tunneling Protocol and IPSec security. Simulation and analysis show that the construction method can improve the security of data transmission, and the simulation results of VPN is valuable for security professionals to refer.

Index Terms- L2TP, IPSec, VPN, tunneling

I. INTRODUCTION

Since the last century, 80 years, computer and data network as the theme of modern technology has made great breakthrough, and its application has been deep into every corner of society. In particular the emergence of the late 80s Internet, in just a few years the world will be tens of thousands of local area networks and even thousands of computers has become a transnational, trans-regional between the information superhighway. The rise of the global Internet data communications network as a single entity, information sharing, communication convenient and efficient, leading to the traditional information technology resources with a breakthrough capacity[1]. VPN (Virtual Private Network) as an important way for enterprises to use the Internet.

VPN: virtual private net can achieve different network components and connections between resources. Virtual private network to use internet or other public infrastructure of the Internet for users to create tunnels, and provide the same private network security and security features[2]. Throughout the VPN technology, you can see, security and service quality is the VPN technical support, the needs of business users to promote wider use of IPSec VPN's, carriers are great efforts to build MPLS VPN, VPN technology allows the development of China's future with more diverse , flexibility, technical services and demand trends closely.

VPN using a variety of security protocols, in the public network to establish a secure tunnel to provide private network capabilities. In ensuring quality of service at the same time, security is the primary VPN features.

In the current study VPN, L2TP and IPSec is the most widely used two kinds of tunneling protocol. L2TP supports multiple transfer protocols and remote access, but security is not strong. IPSec. IP layer can provide a strong security mechanism, but features such as multi-protocol support package deficient. Therefore, the integrated use of both, can both support each other to build a multi-protocol encapsulation, but also to provide authentication and encryption VPN[3]. L2TP and IPSec are on paper the two tunneling protocol to do a systematic exposition, and then each of the two tunneling protocol is proposed based on the principle of a combination of both to build a secure VPN approach, that is the first to use IPSec to encrypt data, and then data will be encrypted L2TP tunnel encapsulation. First introduced the model of this combined method to analyze structural model of the theory and obtained through the model structure to improve transport security, and then to write simulation software MATLAB source code of the program, the mode of data transmission speed the simulation, and finally by analyzing the simulation results show that the performance of this design

II. VPN MEANING

Virtual Private Network, VPN is in the public network (such as the Internet) to establish a dedicated data communication network technology. In the virtual private network, the connection between any two nodes do not need to end the traditional private network of physical links required, but to use the resources of a dynamic group of public networks, private network out, the user is good with a special way to pass. More simply, VPN is the use of shared public network to establish a specific user data transmission channel, the user's remote
branch offices, business partners, such as linking mobile workers to provide end to end, a certain security and service quality-assured data communications services network technology. VPN can be connected using the network, it can be a single point device. With the traditional use of shared resources for voice company dedicated voice messaging service similar to the idea, VPN want to use the shared data protected network resources to provide dedicated data services.

"Virtual" means a better understanding of: the establishment of tunnels or virtual circuits to different physical networks or devices and is no longer using the physical establishment of a long line proprietary data network, such as ATM / FR / IP network. "Virtual" is relative in terms of DDN, although it seems to yourself from the user network, and in fact the user is superimposed on the public network in a virtual dimension. Between VPN and non-VPN, shared between multiple VPN network infrastructure, is different from the private network VPN main difference, it is "virtual" lies.

In order to facilitate the "special" definition of the concept, first define the Closed User Group, CUG concept. Closed for the group that many users of the site-specific formation of a closed user groups, user-based "switch" during the network's business to ensure communications and to prevent unauthorized access to these sites to other sites[4-5]. Within a specific CUG can use private addresses, the address space between different CUG can be reused. CUG This feature prevents unauthorized packets to a specific CUG spread within the network to prevent fraud and tampering of data packets in transit and other security attacks, and can be of different types of packets different treatment, statistics and billing, etc.

The "private" at least two different ways of understanding:

1) CUG + QoS guarantee. The "special" as the circuit is connected to a closed user group or community, with QoS guarantee, but does not provide authentication and encryption and other security services. "Exclusive" means more emphasis on service performance in how not to consider security issues. Telecommunications experts and manufacturers generally are used to this understanding, such as ATM VPN, FR VPN, and the back will highlight the L2TP VPN.

2) CUG + security guarantees. The "special" as the connection is closed user group or community, but this time "dedicated" means more emphasis in the security services, in terms of performance only "best effort (best effort)" service, IP traffic between sites in the competing network resources. Computer experts and manufacturers generally prefer such an understanding, as will be described later IPSec VPN.

III. VPN CATEGORIES

According to protocol type, VPN is generally divided into two categories: Based on the Layer Two Tunneling Protocol Layer-based VPN tunneling protocol VPN.

1) Based on Layer Two Tunneling Protocol: Layer Two Tunneling Protocol OSI model corresponds to the data link layer, using the frame as a data exchange unit. Layer Two Tunneling Protocol commonly used are PPTP, L2F, L2TP.

2) Based on the third layer tunneling protocols: Layer Two Tunneling Protocol OSI model corresponds to the network layer, use the package as a data exchange unit. The third layer tunneling protocol used has PIsac, GRE. The second and third floor is the main difference between tunneling protocol user data in the first layers of network protocol stack is encapsulated.

Operators may participate in a variety of ways to a VPN to the management and implementation and, therefore, there are several types of VPN service, as shown in Figure 1, which is from the technical level (protocol stack) by the angle of the VPN type[6].

Figure 1 VPN service types

In the standard formulation, IETF, and more concerned about L3VPN L2VPN, research results are relatively more, IETF L1VPN although the research done, but the results much. ITU-T study in L1VPN put more effort to develop a large number of L1VPN standards.

IV. VPN TUNNELING

In order to have transparency in IP networks transmit data packets, and provide some security and service quality assurance, then all the VPN must use one or more tunneling protocol. Tunnel technology uses a protocol to another protocol technology transfer, through the tunnel protocol. Tunneling Protocol provides for the establishment of the tunnel, maintenance, and deletion rules and how to package the enterprise network data.
transmission in the tunnel, the following describes two commonly used tunneling protocol.

A. Layer 2 Tunneling Protocol (L2TP)

L2TP: Layer2 Tunneling Protocol PPTP and L2F protocols combines the advantages of a more comprehensive functional and technical[7]. It is also a PPP-based tunneling protocol, by IP, ATM, Frame Relay, and other public transport network to establish the tunnel to send the PPP packets.L2TP uses the client / server architecture, composed of two basic components, first, the client L2TP LAC (L2TP Access Concentrator), is used to initiate the call and the establishment of the tunnel; second server LNS (L2TP Network Server), provides a tunnel transmission services, but for all the end of the tunnel. In a traditional connection, the end user dial-up connection is the LAC, and the end of L2TP extends the PPP to the LNS.

B. IP Security (IPSec)

IPSec (IP Security) is the IETF IPSec working group in order to provide communication in IP layer security protocol developed by a family. It includes some security protocols, key agreement parts and security alliance. Section defines the security protocol for communications security protection mechanisms; key agreement part of the definition of how to protect the security protocol negotiation parameters, and how to communicate the identity of the entity identification; security alliance to store all the details of the consultations to be recorded.

Security protocol, including Encapsulation Security Payload, hereinafter referred to as ESP and the Authentication Header (AH) two. ESP protocol which provides for communication confidentiality, integrity protection; AH to provide integrity protection for the communications protocol[8]. The AH and ESP, has two operating modes: transport mode and tunnel mode. IPSec protocol typically used have been designed with the algorithm-independent. Algorithm selection in the Security Policy Database (SPD) is specified.

V. VPN SECURITY TECHNOLOGY MODEL

A. IPSec VPN Connection Models

In Figure 2, Site-to-site VPN configuration, each node is connected to separate networks, these networks are the other non-safety or public network isolation. As the security requirements of these networks partition, so unless otherwise deploy VPN client on the network node is not able to exchange data. This type of VPN configuration is "closed" Site-to-site network topology. Conversely, if connected to a network partition between the end nodes can freely exchange data and use other networks to forward and receive data. However, these non-secure data exchange. Therefore, IPSec can be used to guarantee some or all of the data exchange security. This type of VPN configuration is known as "open" Site-to-site network design. The key between the two is that, IPSec is used to implement data exchange gateway security. At the same time, more importantly, the realization of data exchange security safety net and connected to the security of end nodes is independent.

In the Client-to-Site VPN network topology (see Figure 3), "open" and "closed" model is applicable. Isolated from the IPSec gateway (or its near) the connection between the nodes may be or not to be limited. In the "open" the Client-to-Site network topology, in the end nodes and the network path between the IPSec gateway is secure. In the "closed" network topology, in the end node and the gateway between the network access is secure. However, the client node and the IPSec gateway adjacent to (or after) the data exchange between the nodes only connected to the IPSec gateway to proceed.

Both network topology, the client node and the IPSec gateway architecture is similar ties in the traditional PSTN remote access dial-up networking. End nodes first establish a connection to the gateway, then the two nodes to communicate as IPSec. In addition, the gateway provides IP as a client node, this status allows the client to work with the other nodes IP and IPSec gateway directly connected end nodes adjacent to the network access. Client communication between nodes and the
gateway is the same security is guaranteed by the IPSec. However, other IPSec client node and the gateway for communication between adjacent nodes are not safe.

B. GRE tunnel model

GRE tunnel is a traditional point to point connection. GRE as shown in Figure 4 applied to the enterprise network, you need the central node in the enterprise and between the various branches of the structure more than point to point GRE tunnels. When large enterprise branch offices, the allocation huge workload; and, if new branches, the central node on the need for additional configuration, an increase of the burden of network maintenance; In addition, branch offices with ADSL dial-up, etc., the branches of public Web address also increased the uncertainty of the center node configuration complexity. Although the dynamic VPN technologies, such as DVPN (Dynamic Virtual Private Network), can learn the public address branches and dynamically in the center tunnel between the nodes and branches, but the dynamic VPN technology is currently no uniform standard, various vendors private agreement with Dynamic VPN, can not communicate. Multipoint GRE tunnel solves the above problems, is ideal for branch offices of many corporate networks. Configuration in the central node multipoint GRE tunnels, the traditional branch-point GRE tunnel configuration, you can achieve a number of branches in the center between the node and dynamically created tunnel.

Multipoint GRE tunnels do not need to manually configure the tunnel destination address, but according to the received packet dynamic learning GRE tunnel destination address[9-11]. As shown below, the terminal device on the client device receives a GRE packet sent from the IP packet header to obtain the source address of the outer and inner payload (IP packet) source address, respectively, as the tunnel packet destination address and destination address (the branch network within the network address), the establishment of a tunnel entry. Among them, the packet destination address mask length can be manually configured. Forward through the multipoint GRE tunnel packet, the device according to the packet destination address, find the entry in the tunnel corresponds to the tunnel destination address, use this address as the external IP header encapsulation GRE destination address, as shown in Figure 5.

VI. L2TP AND IPSec VPN INTEGRATION

L2TP and IPSec have the following deficiencies: L2TP:

L2TP supports IP, IPX, Appletalk, and other network protocols, to support any of the wide area network technologies such as ATM, X.25 frame relay and any Ethernet technology. However, the L2TP protocol does not provide its own security mechanism, so the public network through the L2TP tunnel to transmit
PPP business, L2TP control messages and data packets are vulnerable to attack. L2TP protocol has the following security issues:

1) L2TP is only defined on the end of the tunnel to authenticate an entity, rather than flowing through the tunnel authentication data of each packet, so that the tunnel could not resist inserting and address spoofing attacks.

2) Since there is no integrity check for each packet, there may have been DoS attacks, and send some bogus control information, resulting in L2TP tunnel or the PPP connection closes.

3) L2TP itself does not provide any encryption means, when the data require encryption, you need other technical support.

4) Although the PPP packets can provide confidential, but the PPP protocol does not support automatic key generation and automatic updates, so that eavesdropping attacker is likely to eventually break the key, resulting in the transmitted data.

Because the L2TP protocol has security problems, so when the specific arrangements for L2TP, and other agreements to be combined to maximize the reduction of L2TP security risks.

IPSec:

IPSec is the IETF IPSec working group to provide communications to IP layer security protocol developed by a family. It includes some security protocols and key agreement part of the IP data can flow integrity, confidentiality, anti-replay protection, etc., can also provide flexible connectivity level, identify the source of the data packet level. Currently, the Internet often use the Internet in building LAN IPSec between VPN, but not used for building remote access type independent VPN, main reasons are:

1) IPSec, while providing a strong host-level authentication, but it can only support a limited user-level authentication. Type in the remote access VPN in a remote end user to enter the internal network must be strict authentication. IPSec protocol currently can not easily and effectively implement this feature.

2) in the IPSec security protocol, always assume that the packet is encapsulated IP packet, it is not yet support multi-protocol encapsulation.

3) the current IPSec support only a fixed IP address to find the corresponding pre-shared keys, certificates and other identifying information, does not yet support dynamic allocation of IP addresses. The company staff are often away on business use of the telephone dial-up access to Internet network, when users are using dynamically assigned IP address, so can not authentication, access to the internal network.

After the above analysis, it is natural to have such thoughts: the L2TP protocol and IPSec protocols combine to make up L2TP using IPSec security deficiencies at the same time make use of L2TP IPSec in the user-level authentication, authorization and other deficiencies.

A. L2TP and IPSec integration of design

The following building through the use of L2TP and IPSec-based VPN secure remote access example, to specific examples described. In this example, assume that the remote terminal and the internal network are using IP protocol, IPSec installed in the remote access terminal, the terminal used for remote access to internal network users to communicate with the internal IP packet before the IPSec security processing and then into PPP packet, L2TP encapsulation placed ISP access server-side, corporate intranets and the Internet connection protocol gateway that supports IPSec and L2TP protocol support.

First, the public network through a remote terminal access to dial-up ISP access server, PPP, PPP connection established between two points, ISP RADIUS server
using the tunnel completed by user identity authentication, if the user determine the user VPN, RADIUS server to the ISP access server provides the information needed to build the tunnel, the establishment of ISP and internal network access server gateway between the L2TP tunnel PPP connections through this tunnel extends from the remote terminal to the internal network gateway, the gateway receives a packet --- used for the control of user authentication information, the use of PPP protocol and improve user-level authentication function, the entrance to the internal network to the remote access user identity authentication, authentication is successful, the remote user and the gateway between the internal network --- transmission channel to set up, can be used for transparent transmission had already been dealt with IPSec security of user data, then the remote terminal and the gateway between the IPSec tunnel built in the IPSec security institutions under the protection of remote users and corporate intranets Users can secure data transmission. At this point the remote directly into the internal network as the internal users to use the internal network resources[12-13].

L2TP tunnel work in two modes: the voluntary tunnel (Voluntary Mode) tunnel mode and active mode (Mandatory Mode). The LAC will be installed in different L2TP position, gave rise to two different modes of L2TP.

The first mode is integrated into the remote L2TP client, then client computer acts as a LAC. In this mode, the user independently of the L2TP configuration and management. Another model is installed in the L2TP NAS, usually ISP. In this mode, the client computer can not serve as the tunnel endpoint, but by the remote access server (such as NAS) as the tunnel endpoint, the user can transparently be L2TP service.

Agreement by the combination of IPSec and L2TP VPN security to improve the basic idea is: to integrate remote users or LAC IPSec client software, while the LNS is also integrated IPSec. Service software (integrated IPSec protocol LNS called Sceuer Remote Access Server, SRAS), which use IPSec. To improve the security of remote access communications[14-15]. IPSec protocol integrated in two ways, one is to IPSec remote access integrated into the host, known as the L2TP protocol secure voluntary model; one is integrated into the LAC on the IPSec, L2TP protocol as a mandatory security model.

1). Based on combination of L2TP and IPSec tunnel mode forced

Shown in Figure 6, when operating in forced mode, L2TP, L2TP tunnel is established between the LAC and LNS, but according to the security before L2TP analysis shows, LAC - LNS security between can not be guaranteed. L2TP tunnels in order to ensure better transmission of data security, we can use IPSec to provide security. In the LAC (SIP) and the LNS at the realization of IPSec, such as the LAC and LNS two security gateways, the public packet transmission network to provide security services.

![Figure 6](image)

Figure 6 uses the IPSec tunnel mode force protection

2). Based on combination of L2TP and IPSec tunnel mode of the voluntary

Similarly, when the L2TP working in a voluntary mode, the client computer as LAC, the client computer at the realization of IPSec. Specific structure shown in Figure7.

![Figure 7](image)

Figure7 the voluntary use IPSec tunnel mode protection

B. L2TP and IPSec packet combining Encapsulation Format

The logical structure of the L2TP, L2TP tunnels to ensure security, you can achieve in the LAC and LNS at IPSec, so the LAC and LNS into two security gateways to public data transmission network to provide security services reported. Assumes that all tunnels and link have been established.

Specific data flow is as follows:

1) IPSec package

IPSec-based security policies, IP packet by adding the IPSec Encapsulating Security Payload ESP header, trailer, and IPSec authentication trailer (Auth trailer), the IPSec encryption package.

2) PPP Package

IPSec packet processing by the PPP protocol encapsulation into PPP packets.

3) L2TP encapsulation and IP encapsulation

L2TP encapsulates PPP in groups of form L2TP packet,
and then add the formation of UDP packet UDP header, and then the formation of IP packets transmitted via the Internet in the PI.

Since IPSec has two modes: transport mode and tunnel mode, so the combination of IPSec and L2TP

Figure 8 L2TP + IPSec transport mode encapsulation

package also has two modes, transport mode structures were shown in Figure 8.

C. L2TP a combination of VPN and IPSec works

Remote users to communicate with the VPN as follows:
1) the remote user initiates a local call, then start a PPP connection to the LAC, LAC determine the type of business is the standard Internet services (such as www) or to the internal network. If it is required to access the intranet to find the corresponding L2TP tunnel and IPSec tunnel. And LAC on the PPP encapsulation and L2TP packets IPSec processing to generate L2TP + IPSec packets[16].
2) Once the tunnel is established successfully, the call to assign a Call ID. LAC LNS also send a link to the logo, the logo contains all the parameters have been negotiated.
3) LNS receives the packet, the first in the PI layer IPSec decryption and authentication processing, and then to the L2TP software. L2TP L2TP software will first remove and then sent to a virtual PPP interface, the interface to the PPP to the PPP head again after the call to the IP layer. Finally, according to the internal PI PI layer header sent to the VPN destination address within the network server.

The design, the remote user access to integrated IPSec protocol LAC, established a PPP connection, L2TP tunnels and IPSec tunnels, and their different scope, PPP role of the physical connection between the remote user and the LAC; PPP logical connection on remote between the user and the LNS; L2TP tunnel between the role of the LAC and LNS; IPSec tunnel between the role of the LAC and LNS.

D. transmission time of three simulation packages

Let the maximum transmission unit 500 bit, data transfer speed 20 bit / s, use slice transmission. Transmission time through the simulation of Figure 9, Figure 10, Figure 11, we can clearly see the load of the same length the circumstances under which the method of combining L2TP and IPSec transmission time the system overhead. This shows that the more complex security protection, the greater the overhead, improve security, system performance will be reduced. However, the security of data transmission has been greatly improved. Repeat this at the expense of visible transmission rate of packages to improve security to nature, this method is a relatively time-consuming, but in today's information age, especially in emerging network security risk situation, transmission time to increase the cost of some Data security is very necessary[17].

Figure 9 Transmission mode of transmission time simulation of Figure

Figure 10 the tunnel mode of transmission time simulation of Figure

Figure 11 AH and ESP combined mode of transmission time simulation of Figure
VI. CONCLUSION

A secure VPN solution must be able to authenticate users and to strictly control that only authorized users can access VPN; be able to provide auditing and billing functions, show who and when to access what information; VPN solution must be able to assign a private network for users address and ensure the safety of the address; pass through the public Internet, data must be encrypted; VPN solution must be able to generate and update the client and the server's encryption key; On the integrated use of L2TP and IPSec, can only support each other to build a multi-protocol encapsulation, but also to provide authentication and encryption VPN. VPN solution must support the widespread use of the public on the Internet's basic protocols in ensuring quality of service at the same time, security is the primary VPN features.

REFERENCES


Ya-qin Fan female, was born in 1963 in Shulan city, JiLin Province, China. She received her Bachelor Degree in Changchun Institute of Posts and Telecommunications in 1985. Her directions of research include the broadband communications technology and wireless communication theory.Ya-qin Fan is an Associate Professor and also a Postgraduate Tutor, who is now working in Institute of Communications Engineering, Jilin University in China. Her lectures include the following specialized courses as "Modern Switching Technology" and "Computer Communication Networks", etc. Associate Professor Ya-qin Fan had been in charge of many research projects and participated in a number of scientific research items in her research field, and published a number of valuable research papers in domestic and international research fields.

Chi Li male, was born in 1991 in Jilin City, Jilin Province, China. he is an undergraduate of Communication Engineering in Communication Engineering College Jilin University. Being interested in the research of broadband communications and wireless communication theory, Chi Li has taken effort on studying professional knowledge and participated in various research projects with the help of teachers.

Chao Sun female, was born in 1987 in Baicheng city, Jilin Province, China.she is an undergraduate of Communication Engineering in Communication Engineering College Jilin University. Being interested in the research of broadband communications .

Project Title: Technology development plan project of jilin province china
Project number: 20090513