Application of VPN in e-Business

LIU Shuang-ying(刘爽英), LI Bo(李　博)
(*College of Electronics and Computer Science and Technology*, *North University of China*, *Taiyuan 030051*, *China*)

Abstract: With the development of Internet, e-Business has gradually become a new model for business activity, however, the security of e-Business is a major bottleneck restricting the development of e-Business. Network with virtual private network(VPN) can reduce network costs and communication costs, increase flexibility and provide safe and smooth network for the corporations that do e-Business across regions. This article introduces the definition and the technological core of VPN, and researches and analyzes the VPN application in e-commerce.

Key words: e-business; Internet security; virtual private network(VPN); tunnel

CLD number: TP393.08 **Document code:** A
Article ID: 1674-8042(2012)03-0248-03 **doi:** 10.3969/j.issn.1674-8042.2012.03.010

E-Business is a kind of business activities carried out according to some certain criteria with the platform of computer network, including activities that government and enterprises connect directly with their staff, customers, suppliers and partners by Intranet, Extranet and Internet when they do their main business.

When network is connected by a private channel, it is easier to control the reliability and security of network, but network's connection charge is high and its scalability is limited; when network is connected by public Internet, the charge is low and scalability is better, but the security and reliability is at risk. Virtual private network(VPN) technology emerges at the right moment. It can encrypt data point to point, which provides security and ensures that data clustering in the composition of routing has not been modified to keep data integrity, and ensures clustering come from the right source by providing certification. Moreover, VPN is cheap and its management is flexible. Because VPN can compensate previous defects, it has become a common network connection used in the e-Business.

1 Definition of VPN

VPN is "virtual private network". The "virtual" refers to the dynamic link between two remote nodes of public network, that is, a logical link between two routers of the public network. "Private" refers to the network limited to specific people or organizations. The "network" refers to the computer network. There are no end-to-end physical links which are needed in traditional private network, but dynamic links by using some public network resource according to actual needs between any two nodes in VPN. Enterprise private network can be built by public network such as Internet[1]. When needed, VPN can be exclusive part of the broadband from the public network as private network, and when communication finishes this part of broadband is returned to the public network. The connection of VPN is shown in Fig.1.

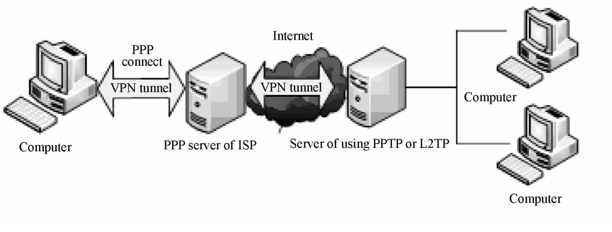

Fig.1 Connection of VPN

2 VPN security technology

2.1 Tunneling technology

Tunneling technology is to establish a data path in the public network, so that data can transmit through this tunnel. Its basic principle is that, in the interface of the original local area network (LAN) and the public network, data, as load, is encapsulated in a data format which can be transmitted in the public network, and is decapsulated

* **Received data:** 2012-04-18
Foundation item: The 2012 Development Plan of Science and Technology of Shanxi Province (No.20120321032)
Corresponding author: LIU Shuang-ying(liushuangying@nuc.edu.cn)

and taken out the interface of the destination LAN and the public network. The data format of packets was shown in Fig. 2. In this way, the logic path that encapsulates data packets passing through in the Internet is called "Tunnel". In order to make data in VPN tunnel more secure, VPN technology is generally realized in the second and third-level of IP protocol. At present, VPN tunneling protocol is mainly IPSec protocol[2].

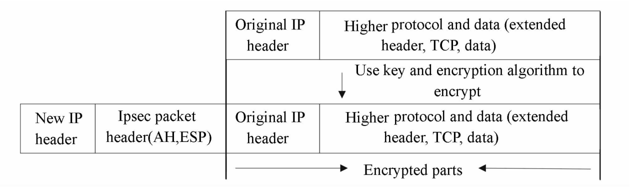
Original IP header
Higher protocol and data (extended header, TCP, data)
Use key and encryption algorithm to encrypt
New IP header
Ipsec packet header(AH,ESP)
Original IP header
Higher protocol and data (extended header, TCP, data)
Encrypted parts

Fig. 2 Data format of packets

2.2 Encryption and decryption technology

Encryption and decryption is a relatively more mature technology in the data communication, and VPN can directly realize encryption and decryption by using the existing technology. IPSec uses triple data encryption standard (DES) algorithm for data encryption. Triple DES algorithm is safer deformation of DES algorithm, and it provides three encryption processes for ciphertext, which encrypts the exchange information (such as electric data interchange (EDI) data) with three independent 56-bit keys to make its effective key length 168 bits. IPSec uses encapsulating security payload (ESP) and encryption algorithm to provide source authentication and ensure data integrity. IPSec also alone uses authentication header (AH) to ensure data integrity. The structure of IPSec security technology is shown in Fig. 3.

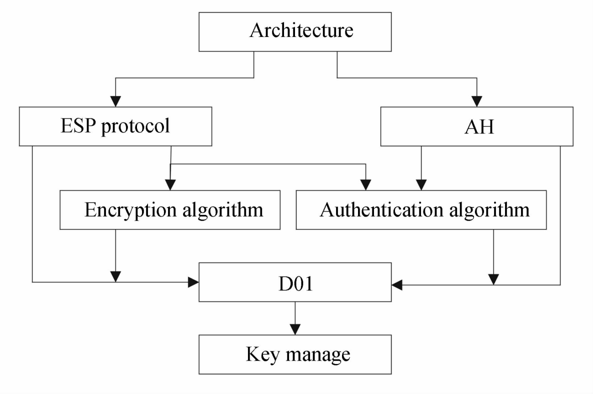

Fig. 3 Structure of IPSec security technology

2.3 Key management technology

The main task of key management technology is to safely transmit the key without being stolen in the public data network. The key technologies used in VPN are ISAKMP and OAKLEY. ISAKMP is internet security association and key management protocol, which provides support for Internet key management architecture and specific protocol. In ISAKMP, there are two keys for the communication parties, of which one is public and the other is private. OAKLEY is a key protocol based on Diffle-Hellman algorithm.

2.4 Authentication technology

High-strength password authentication protocol technology is used in VPN for identity recognition, which is mainly digital signature and public key. Digital signature is that, when A and B e-mail each other (two parties let the opposite's public key be known), A encrypts his own signature with his private key, then encrypts the message text with B's public key and sends out; when B receives letters he decrypts the message with his private key and uses A's public key to decrypt signature to ensure the mail is sent from A and not forged by the third-party. Digital signature technologies in VPN mainly are RSA, and iKey. In addition, VPN also can use Kerberos authentication mechanism for identity recognition of transaction parties. Kerberos is an authentication mechanism providing the service of the trusted third party facing open system for network communication. Kerberos depends on neither the terminal of user login nor security mechanism of user requiring services, which itself provides authentication server to complete the certification of users.

3 Application of VPN in e-Business

With the emergence of electronic commerce (e-commerce), the application of VPN in e-Business becomes more and more wider. Generally speaking, there are three solutions in e-commerce for VPN, and they are remote access virtual net (Access VPN) plan, enterprise's internal virtual network (Intranet VPN) plan and business expansion virtual network (Extranet VPN) plan respectively[3].

3.1 Access VPN

Access VPN refers to the VPN established between enterprise remote terminal and headquarters. If enterprise's internal staff often need to travel or telecommute, it is best to consider using Access VPN. Access VPN provides remote access for internal or external network by a shared infrastructure which has similar strategies with the private network. Access VPN allows users to get access to enterprise's resources anywhere, anytime in a desired way. Access VPN includes analog, dial-up, integrated services digital network (ISDN), asymmetric digital subscriber line (ADSL), mobile IP and cable technology, which can safely connect mobile users, remote workers or branches. Access VPN is best suited for those companies whose staff need frequent movement and telecommuting. Traveling users can connect the private tunnel established by VPN gateway of their company by using the VPN service provided by local Internet service provider (ISP). ISP server can certify and authorize users to ensure safety of connection, at the same time, the telephone bill incurred is reduced greatly.

3.2 Intranet VPN

Intranet VPN is a VPN connection between enterprise division and headquarters[4]. If you want to connect between all branches within company, Intranet VPN is a good method. More and more companies need to set up all kinds of offices, branch companies, research institutes and so on within the country or all over the world, and the network connection between all branches is generally the traditional leased-line mode. It is obvious that when branches increase and business develop, the network structure tends to be more complex and the cost is more expensive. World-wide Intranet VPN can be established on the Internet by use of VPN. Using the line of Internet can ensure network connectivity, and using the features of VPN such as tunneling, encryption and so on can ensure that information can be transmitted in Intranet safely. Intranet VPN connects headquarters, remote offices and branches through a shared infrastructure of private connection. Enterprises have the same policies as the private network, including safety and service quality, manageability and reliability.

3.3 Extranet VPN

Extranet VPN is a VPN connection between corporate headquarters and its partners. If enterprise network needs to construct a dynamic network system with the network of its associated corporative partners, the Extranet VPN is the best option. Its attractiveness to the users lies in: it is convenient to deploy and manage the external networks, and the connection of external network can use the same architecture and protocol with that of internal network and remote access VPN. Using this solution, customers, suppliers and distribution partners can get more resources[5].

4 Conclusion

In e-Business applications, VPN, which can reduce the operating costs of remote services and equipment, has highly extensible connection methods and cheap support of management and technology, and it has become the hot application platform of e-Business market. As solutions of remote access, high efficiency and low price of network interconnection, safety and reliability, VPN combines flexibility, security, economy and scalability into one, which can fully meet the requirements of branch offices of enterprises, mobile work and safe communication.

References

[1] HONG Yi. Analysis of application of VPN on electronic business security. Computer Knowledge and Technology, 2009, 5(8): 1855-1856.

[2] ZHANG Han-fang, WU Jun-sheng. The research and application of VPN in e-business. Microprocessors, 2008 (3): 59-62.

[3] GUO Li-chun, HUANG Jin-bo. Three design scenarios of VPN system suitable for electronic commerce. Networks Security, 2008, 11: 33-34.

[4] XIAO Zhong-liang. Establishment of network through VPN technology. Technological Development of Enterprise, 2011, 30(11): 21-23.

[5] MU Dong-zhou, YU Ben-cheng. Small and medium enterprise VPN network planning and design. Network Security Technology & Application, 2011(7): 72-73.