Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 964-967
doi:10.4028/www.scientific.net/AEF.6-7.964

Construction and Exploration of Corporate Virtual Private Networks

Kai Peng

School of Science, Wuhan University of Technology, Wuhan 430070, China

E-mail: pengkaiwh@vip.qq.com

Key words: virtual private network; tunneling protocol; network security

Abstract. With the further development of Internet, VPN technology would provide high-quality and low-cost wide-area data network, and would be safer than the majority of corporate special network. Main purpose of VPN technology is to save communication expenses for enterprises, especially replace existing special lines of enterprises and reduce communication cost. With constant mergers and acquisitions of enterprises and the occurrence of new relationship between enterprises and employees, traditional corporate network mode faces challenges. One solution is to use virtual private network when constructing enterprise information environment. During network design, if only for simple point-to-point data transmission, making full use of transmission security is enough, security mechanisms such as encrypted tunnel, flows separating, packet authentication, user authentication, authorization system and access control etc have been taken to ensure the security. From perspective of engineering, comparison between the construction of corporate VPN and tunneling protocol that realizes VPN is made.

Introduction

The tide of global economic integration makes the mergers and acquisitions of enterprises become increasingly fierce, and there is an increasingly number of branches for each enterprise; cooperation among corporations and association between enterprises and customers is becoming increasingly close, and this kind of cooperation and association are dynamic, always in development and changes. The development of internet and continuous accelerating of access speed are changing people's working mode. However, the change of working mode makes mobile office employees and home office employee increase constantly, and the relationship between enterprises and employees is mainly maintained and strengthened by network. This kind of development trend makes traditional ways of dialup networks or leased lines difficult to adapt. Therefore, VPN technology emerges as the times require. VPN is the abbreviation of Virtual Private Network, which refers to building private data communication network technology in public network by relying on ISP (Internet service provider) and NSP (network service provider). VPN based on IP simulates a private WAN to use IP mechanism, and is a technology that simulates a point-to-point line on the public data network through private tunnel technology. VPN system makes private network distributed in different places communicate safely on unreliable public network (such as the Internet).

Realization of Corporate VPN

For enterprise users, VPN should meet the following requirements:

As VPN is mainly used to meet the demand of corporate customers, its availability requirement is not only about ensuring connectivity, but also should meet specific index requirements of customer service quality. For example, a user needs VPN service from Beijing to Shanghai, requiring to ensure that the bandwidth shall be not less than 512kbit/s, and time delay shall be less than 50ms. Then, when selecting bearer networks of VPN, it is essential to choose bearer networks with bandwidth guarantee, such as frame relay could be selected instead of public internet network. In addition, due to the requirement of time delay, it must be considered that when the network is interrupted, whether its alternate route meets the requirement of time delay. If not, other means must be taken such as ISDN etc to backup to meet the availability.

Networks combined by different business modes and technologies have different VPN management content. The management content of VPN provided by NSP to face connection should be equal to business network of NSP. The network transmission part of network that enterprise user has assigned is not known or protected by NSP, so its manageability is restricted by NSP. However, the following aspects would be involved: traffic monitoring, service level agreement (SLA), security policy guarantee and QoS policy. For traffic monitoring, it is required to have real-time observation and control the bandwidth application situation in all directions within the network, adjust network and use as the basis for network expansion through traffic monitoring prediction and flow control strategy. Service level agreement is mainly used for recording and tracking services that do not comply with application requirements or operator commitment timely. QoS policy allows network managers to allocate bandwidth resources in accordance with priority and realize bandwidth management, so that kinds of data could be sent one after another reasonably, and prevent blocking.

Expansibility includes physical network and business expansion. In the first place, a reasonable network structure is required to be built. For example, core nodes could be used to form mesh network, and then form small regional networks based on the nodes. In this way, lots of line resources could be saved, and in addition, it is also necessary to optimize IP routing system and IP address distribution principles within the network. Expansion for functions and applications should mainly consider the consistency of interface and relevant servo system, such as billing system and accounting system etc.

VPN security mainly involves two aspects of problems: one is the security in network transmission, this part is guaranteed by service providers through encryption, tunnel and other public technologies, and is already quite mature; on the other hand, when designing VPN, at the interface connected to public network, especially when there are strategic problems of internet business at the same time, for example, communication among internal primary machines of enterprise users could use private real address, while accessing to public network, network address translation is needed. During network design, if only for simple point-to-point data transmission, making full use of transmission security is enough, and if there is also requirement of mobile user remote access and guarantee the security of important data at the same time, security mechanisms such as encrypted tunnel, flows separating, packet authentication, user authentication, authorization system and access control etc should be taken to ensure the security.

Costs of VPN are mainly divided into two parts: initial network construction costs, network expansion, operation and maintenance costs. Among that, initial network construction and expansion costs are easier to calculate, and in most cases, there is not significant difference with the reality. Costs of operation and maintenance, network scale of enterprise users, requirements on network performance, business mode, and information technology personnel strength of the companies have great relationship with the degree of network management requirements.

Tunneling Protocol Based on VPN

To meet the above requirements, the realization of VPN must take tunneling mechanism in certain form. The so-called tunnel is actually a kind of encapsulation, transmit a type of protocol (protocol X) by encapsulating it in another type of protocol (protocol Y), and thus the transparency of protocol X on the public network. VPN protocol system structure realized by tunneling mechanism is shown in figure 1, where protocol X is called encapsulated protocol, and protocol Y is called encapsulation protocol, and generally specific tunneling control information should be added while encapsulating. Therefore, general encapsulation form of tunneling protocol is (protocol Y (tunnel head (protocol X))). As a type of network interconnection means, tunneling protocol is widely applied to various occasions, such as mobile IP and multi-point delivery etc. When we are realizing VPN based on Internet, the applied encapsulation protocol is IP protocol, and tunneling protocol that uses IP protocol as encapsulation protocol is called IP tunneling protocol. Existing IP tunneling protocols are: GRE, L2TP, IPSec and IP/IP etc.

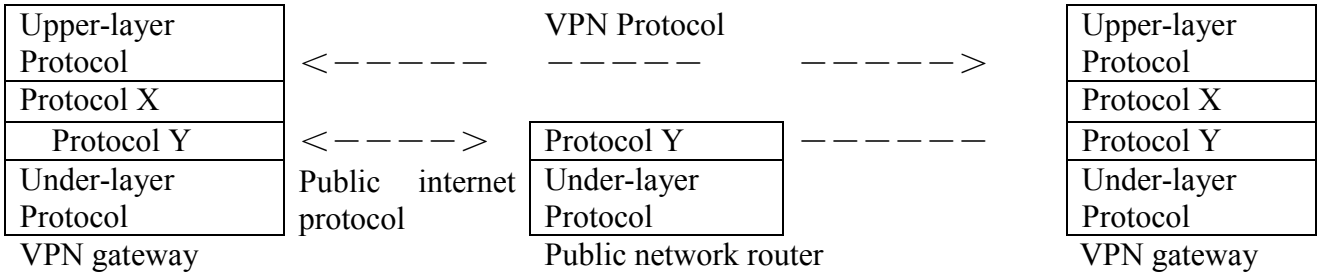

Fig.1 System Structure of VPN Protocol

GRE protocol is also known as general router encapsulation. It is a general encapsulation protocol proposed for some special encapsulation programs (such as IP encapsulation IPX, IP encapsulation X, 25 etc), and allows to use any types of network protocols to encapsulate any kinds of network protocols. The general encapsulation form of GRE is (protocol Y (GRE (protocol X))), and when the encapsulation protocol is IP protocol, its encapsulation form is (IP (GRE (protocol X))). The range of GRE application is very wide, including mobile IP, PPTP and other environment.

L2TP protocol is also known as layer 2 tunneling protocol. We classify it into the same category with Microsoft point-to-point tunneling protocol (PPTP) and Cisco layer 2 forwarding protocol (L2F), they are all tunneling protocol designed for using Internet as remote access infrastructure, and the work is in the layer 2 of OSI/RM system structure. The encapsulated form of L2TP is (IP (UDP (L2TP (Protocol X)))).

IPSec protocol, also known as IP layer security protocol, is a series of standards proposed by IPSec working group of IETF to introduce security mechanism to TCP/IP network, including security protocol (identification header AH and security encryption package ESP), security association, key management and security algorithm etc. The encapsulation form of IPSec that it works in "tunneling" mode is (IP (AH or ESP (IP))).

IP/IP protocol is proposed by IETF mobile IP working group that uses IP package to encapsulate IP package, and its purpose is to realize the communication between mobile host and other local agents in mobile IP environment. This working group also proposes tunneling establishment protocol (TEP) for establishing tunnels. The encapsulation form of IP/IP is (IP (tunnel head (IP))).

When constructing corporate VPN, while meeting the transparent transmission, security functions and service quality, IP tunneling protocol could be selected according to corporate network topology structure and practical situation. As IPSec has strong encryption and authentication function and supports multiplex and signaling protocol IKE, these are absent for other protocols. Therefore, IPSec protocol could be selected.

Conclusion

Main purpose of VPN technology is to save communication expenses for enterprises, especially replace existing special lines of enterprises and reduce communication cost. With the further development of Internet, VPN technology would provide high-quality and low-cost wide-area data network, and would be safer than the majority of corporate special network.

Acknowledgement

Finally, I would like to thank the Fundamental Research Funds for the Central Universities (2012-Ia-030) for providing funds to support this research.

References

[1] Zhang Dalu, Hu Xianfeng. Research on VPN Core Technology [J]. Computer Engineering, 2000,3(1):41-42.

[2] Zhao Equn, Ji Yi, Gu Guanqun. Research on Tunneling Techniques Supporting VPN [J]. Journal of China Institute of Communications, 2000,6(1):85-90.

[3] Sun Weiqing, Zhao Yiqun. VPN Tunneling Technology [J]. Application Research of Computers, 2000,8(1):55-57.

[4] Chu Kuang. Network Security and Firewall Technology. Posts & Telecom Press, 2000.

[5] Dai Chiyun. Virtual Private Network (VPN) Technology and Its Application in Enterprise WAN Connection. Modern Computer, 2000(8).

[6] Wang Lina, Yu Ge, Mei Zhe et al. Chaotic Encryption Method of Multimedia Information in Virtual Enterprise [J]. Journal of Northeastern University (Natural Science), 2001,22(4):381-384.

[7] Xiong Guixi, Wang Xiaohu. Computer Network [M]. Beijing: Tsinghua University Press, 2000.