Advanced Materials Research *Submitted: 2014-05-28*
ISSN: 1662-8985, Vols. 998-999, pp 1223-1226 *Revised: 2014-06-03*
doi:10.4028/www.scientific.net/AMR.998-999.1223 *Accepted: 2014-06-04*
 Online: 2014-07-30

Research on the Application of VPN Technology in the Computer Network

Xianguang Feng

Liaoning Electromechanical Polytechnic, Dandong 118000,China

fengxianguang@126.com

Key words: VPN, The computer network, Security

Abstract. VPN technology is a kind of common and mature data information sharing and exchange of technology. The technology can be very convenient to realize point-to-point transmission and guarantee process of information transmission security and integrity for the application of computer network. This paper introduces the principle of VPN technology and its advantages, and application of VPN technology in computer network is highlighted.

Introduction

Data are very vulnerable to security risks when it is transmitted in a public computer network without a specific encryption. In order to guarantee the security of data transmission and virtual private network technology, the VPN technology is widely used in public computer network resource sharing and data transmission [1-3]. VPN technology can be very convenient and efficient between the user and information server, it sets up a relatively hidden data transmission channel in the network to avoid the use of special network line, thus make sure the safety of data transmission. VPN technology is to use different ways to improve the security performance of the private network, the characteristics for enterprise information channel, digital libraries in colleges and universities and it has a very significant role in financial management of colleges and universities [4]. And VPN technology is very efficient and simplified; it reduces the laid in the traditional mode and the net inflow of special line and overcomes the difficult problems in the professional line laying.

Through the establishment of information access, VPN technology can reduce the cost of enterprises, schools and information carrier, and VPN technology equipment requirement is very low, and the advantages of equipment is simple, expansive and has very good performance, and school builds the core competitiveness for the enterprise as a technical support [5-6].

Casey Wilson and Peter Doak said in their book VPN is defined as a virtual channel, the channel can be used to connect two private networks with reliable technology and encryption method to ensure its safety, so it is special as a part of the public network.

We will discuss the application of VPN technology in computer network in the following article.

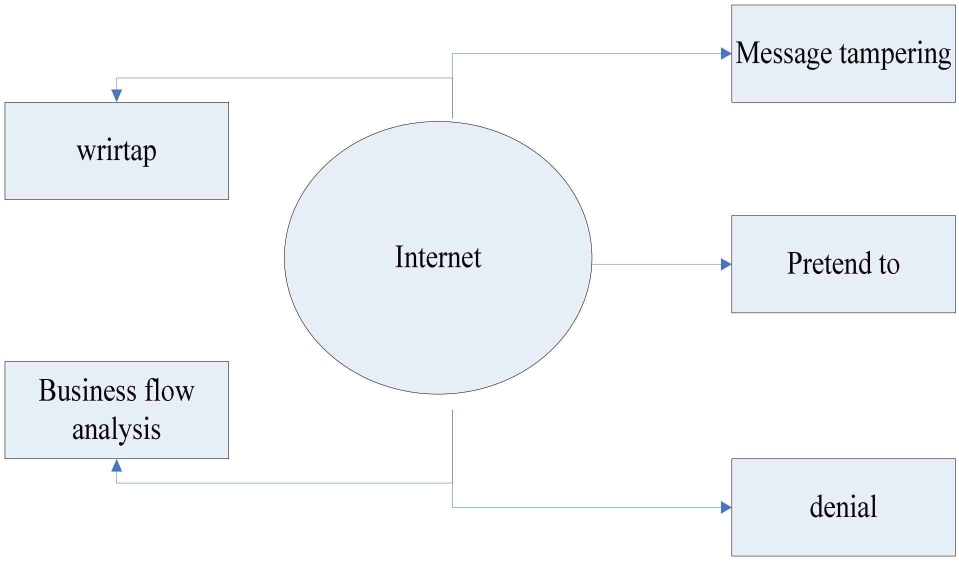

Fig.1 The common types of attack in data transmission

The principle of VPN technology and its advantages of analysis

The principle of the VPN technology. Fig.1 shows the common type of attack in data transmission. VPN through public IP network established private data transmission channel, branch offices, business partners, remote mobile office personnel, etc. Reduce the enterprise cost burden of remote access and save telephone expenses, and to provide the end-to-end data communications security [7]. To connect the VPN in the form of conventional direct dial-up connection and virtual private network connection. The network communication based on VPN technology can be roughly divided into four steps: First the terminal of network user to send transport channel to the VPN server build request; Then VPN server receives the request of the terminal of user authentication response; If users pass validation process, the VPN server will analyze the user's remote access under the condition of the authority authorized to set up a virtual private network for the user line; The communication between the user and the server data will be encrypted encapsulation process, and then through the established VPN tunnel transmission from the sender to the receiver.

Analysis advantages of VPN technology. First, the VPN technology has higher security, the high strength of encryption and authentication mechanisms is applied in VPN technology to ensure the security and privacy of data transmission, in particular, VPN technology can build a relatively independent and hidden safety communication channel, transmission of data in the tunnel to be effective in preventing malicious tampering and destruction from the network. Second, the VPN is easy to realize and has low cost. The VPN technology exists in the public network rely on the established virtual private network, also it doesn't need to set up a dedicated circuit for data transmission separately, the safe effect has no difference between a private network, so its cheaper, implementation structure is more simple[8-9]. The last, the VPN technology is efficient and convenient. Application of VPN technology to build virtual private networks (VPNS) just in the position of the public network node architecture proper VPN equipment can be realized the establishment of the virtual private line, its configuration to achieve more convenient and efficient.

The implementation of VPN technology in the protocol layer. According to the OSI model reference standard, the different VPN technology can be realized in different layers of the OSI protocol.Fig.2 shows the different layer and the types of VPN.

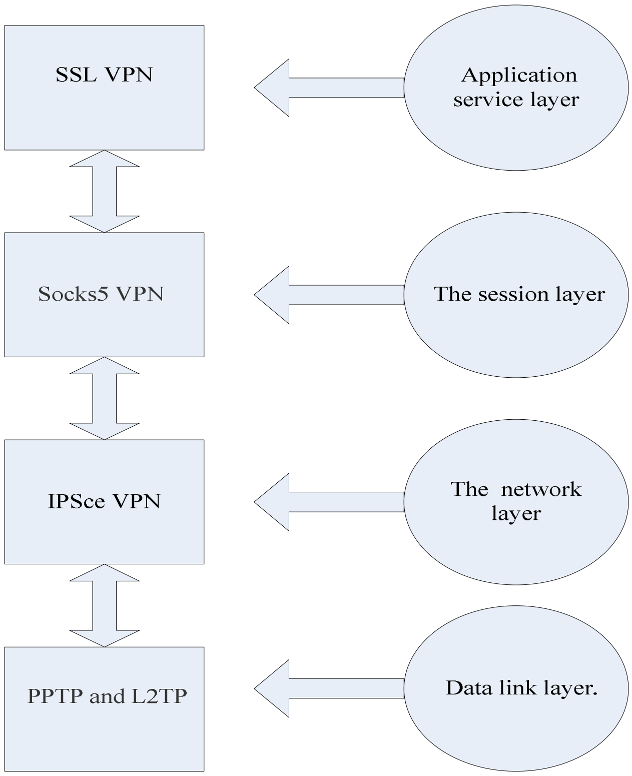

Fig.2 Frame structure chart

The application of VPN technology in the computer network

At present, the commonly application in computer network of VPN technology mainly includes three types including MPLS VPN technology. IPSece VPN technology and SSL VPN technology..

The application of MPLS VPN technology. MPLS VPN is mainly used in MPLS network data exchange equipment and routing equipment technology, the technology can effectively simplify the data transmission way of routing, to realize the establishment and application of IP virtual private network. The application mode is a mainstream trend of VPN technology**.** The MPLS VPN is realized through three steps. First, build LSP. Network can take advantage of the method of CR - the LDP among PE router, LSP usually contains a lot of business, there are two-layer VPN and three-layer VPN, at the same time these two steps also provide the key step in the MPLS network operators. Second, realize the VPN information on PE routers. This step is to control the VPN data transmission process, which is the key step to realize the VPN on the second floor. Third, we can realize the VPN data transmission.

Taken together, the application of MPLS VPN technology can realize smooth network expansion, to the operation of the network users with a transparent environment and don't let the user feel the difference between the VPN network and public network. If the corresponding is added in the MPLS VPN network management and control functions or superposition of related functions, is also can achieve high speed and efficient data transmission services.

The application of IPSece VPN technology. Virtual private networks (VPNS) is the most common way in IPSec protocol, the purpose of IPSec protocol is the IP address for the protection of the safety performance of VPN is in implementing the safety protection and produce a series of solutions, IPSec is a framework structure, basically has the following two kinds of protocol, the first kind of ESP protocol, the scope of this agreement to use widely, can provide a very complete data at the same time, with confidential data information and the characteristics of replay attacks, ESP use often have 3 des, AES encryption algorithm, using the MD5 algorithm to complete the integrity of the data to identify and analyze. IPSec VPN application scenario is divided into three kinds:

The application of SSL VPN technology. SSL VPN is a kind of network service in form of End to Site class type, its service implementation does not need the client's support, users can realize remote access more flexible and VPN technology is a kind of application layer. The SSL VPN can provide three work modes: the Web browser mode, the SSL VPN client mode, and LAN to LAN mode. The first kind of mode, the user can directly use the browser support SSL protocol to build virtual private network for remote access without considering relevant configuration, this model can effectively reduce the workload of VPN management and operation; The second pattern used to support the SSL protocol client makes a remote application server access, the encryption of data transmission between client and server is through a tunnel, which can effectively ensure the security of data transmission; The third kind of pattern is similar to IPSEC VPN application, it can support the data encryption transmission between different local area network (LAN).Virtual private network constructed based on SSL VPN can be very convenient to iterate through all the NAT devices also can effectively solve the problem of IP address conflicts. With respect to its application scenarios and development trends, SSL VPN is mainly used for remote access platform service, application gateway between platform and conversion service and unified authentication gateway service three aspects.

Conclusion

The application of VPN technology ensures the safety of the environment of computer network security and data transmission, at the same time in the realization of data sharing and exchange. It can provide a flexible, economic and efficient network deployment scheme to the enterprises or the users effectively, thus make enterprise build high security of network.

References

[1] I. Pepelnjak, J.Guichard: *MPLS VPN and Architecture* (Ciseo Press, USA 2008).

[2] H.J.Jin, H.Zhong:*Virtual Private Network VPN Security Practices Tutorial* (Tsinghua University Press, CN 2010).

[3] Z.J.Wang, L.N.Zhang, *VPN Network Technology and Business Applications* (National Defence Industry, CN, 2012)

[4] C.H.Wang, T.Song: *The VPN Network to Form a Case Record* (Science Press, CN, 2011)

[5] N.Zheng: China New Technologies and Products, Vol.2 (2009), p, 182.

[6]Y.L.Liu: Electronic Testing, Vol.15 (2013), p, 254.

[7]Z.G.Zhang: Shandong Transportation Technology, Vol, 1(2011), p, 169.

[8]Y.Liu,X.N.Liang: The Wealth of Network,Vol.6 (2008), p, 24.

[9]F.Bai: Information Communication,Vol.2 (2012), p, 216.