Advances in Computer Science Research (ACSR), volume 61
7th International Conference on Education, Management, Computer and Society (EMCS 2017)

Technical Analysis and Application of VPN

Shoubai Xiao

Nanchang Institute of Science & Technology, Jiangxi Nanchang 330108

Keywords: VPN; IPSec; Cross-regional; Networking

Abstract. With the development of current network communication technology and continuous expansion of the scale of enterprises, traditional network based on the fixed location of private line cannot meet the needs of modern enterprises, and large enterprises need to achieve effective, Safe and fast connection between business headquarters, branch and their partners. Enterprises want to achieve a connection can simultaneously realize the network communication among different regions of their subsidiaries and corporate headquarters, and the staff in different regions of the enterprise can easily exchange information, just like in the same local area network environment The VPN technology protect the privacy of communications through a variety of protocols, and fully guarantee the data security on the public network transmission.

Introduction

With the informationization degree of enterprise network system improving, cross-regional enterprises often choose to rent the operator's proprietary network to meet their own information needs. However, as time goes on, it is unbearable for the cost of this leasing method, and the security cannot be fully guaranteed. The use of VPN technology for cross-regional enterprises can make them reduce the cost of network to the minimum. In addition to the initial hardware equipment investment, the latter only the operator's public network royalties needs to be paid, so the cost will be greatly reduced. At the same time, the public network builds private networks on their own proprietary devices, and the security of communications is guaranteed. However, the traditional VPN usually refers to taking use of operator's public network for enterprises to provide dedicated services, the use of such communication has high cost, and maintenance is more difficult.

This paper achieves information resources sharing between the headquarter and member enterprises and providing timely and accurate information for the company's production, sales, management and other business activities through using VPN wide area network in the company, while providing pre-preparation for the future business development. In this time, VPN network construction is equipped with a dedicated hardware, VPN module router, with sufficient expansion slots to ensure that the needs of future Vo IP, remote management and other business.

VPN Principle of Realization

The most important reason why more and more enterprises choose VPN technology to set up the network is its low cost and connection security. VPN is built on the basis of tunneling technology, and it uses public networks (usually the Internet) to establish the connection between nodes through developing a number of secure protocols, virtual out of a common network running on the private network. So VPN is also a protected connection, and will not be exposed to the public network. Nowadays, under the IPv4 addressing rules, the public IP address is shortened as the number of users growing, so the enterprise uses the private address as the internal IP in building the internal network, and these private addresses cannot be routed on the public network. When different networks transfer data through the public network, if private addresses are used, it will not be linked normally, making access failure, as shown in Fig. 1 cross-regional network connection.

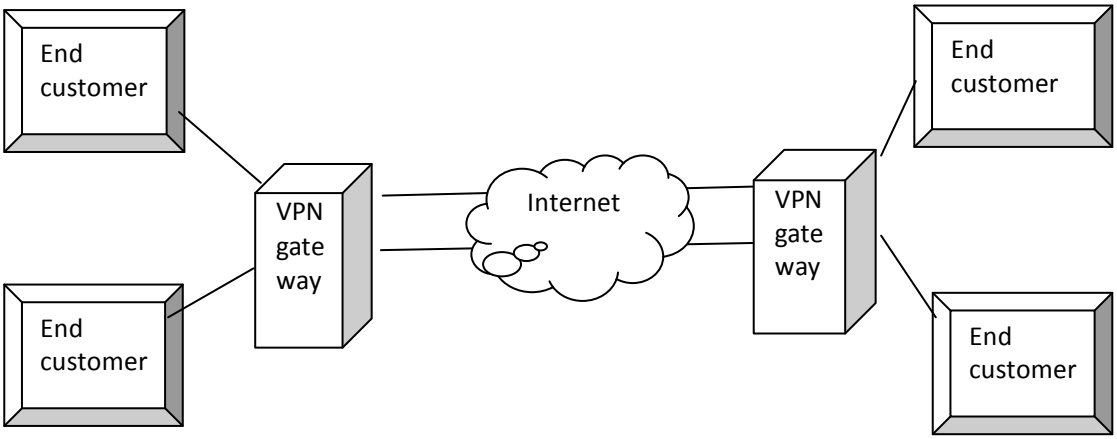

Figure 1. s-regional network connection

If the end user in the network wants to establish a connection with the end user of the network 2 through public network, the connection will fail if using private address, but there are two solutions:

NAT technology will be used to connect the Internet at both ends of the network; the private address of boundary router of network 1 and network 2 is translated into public address to achieve access. NAT conversion may make the connection of many applications of network 1 and network 2 ends be achieved complexly, and the user still wants to be able to connect directly with private address.

Both ends of network 1, 2 are set up dedicated connection, so that both ends can directly achieve the connection through private address. One way to achieve dedicated line is to build a private optical network of private enterprises, which is too costly and practically impossible to implement.

Based on the consideration of two networking modes above, people try to use tunnel technology based on the public Internet network to establish proprietary connections for remote network organizations. This is also the realization principle of VPN technology.

IPSec VPN

IPSec (Internet Protocol Security) is a set of standards that IETF RFC provides for Internet security communications, and IPSec is specifically designed to handle the transfer of sensitive data over insecure networks. IPSec components include security protocol authentication header (AH) and encapsulated security payload (ESP), key exchange (IKE), security association (SA), and encryption and authentication algorithms. IPSec is a network layer protocol that handles end-to-end network security issues such as data confidentiality, integrity, and data validation. IPSec supports DES, 3DES, and AES encryption algorithms to verify the integrity of a packet by using hash functions such as MD5 and SHA. The hash function is used to verify the identity of the sending identity of IPSec packet device. And the device verifying the user is to verify if the remote device is allowed to connect to the local device. IPSec supports pre-shared key, digital certificate and pre-shared key three device authentication methods. IPSec is a set of open standards, and it has been adopted by many network equipment manufacturers, so the current VPN application is the most common technology.

IPSec has different working modes under different application requirements, namely Transport Mode and Tunnel Mode.

Transmission mode

As shown in Fig. 2, the so-called IPSec VPN of transmission mode means that the data transferred between the two hosts can be encrypted. For example, when we use a portable computer to send a message back to the company's mail server via the POP3 protocol, an IPSec VPN of the

transport mode can be established between the Mail Server and the portable computer to ensure that the contents of the message are not stolen by others.

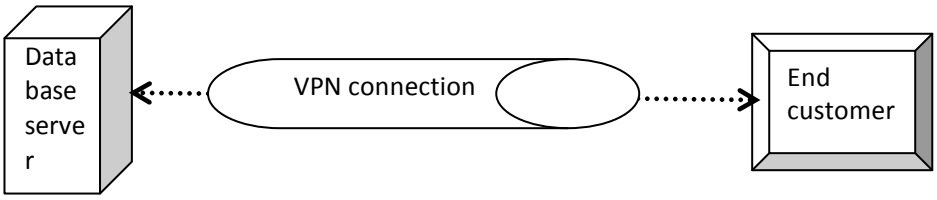

Figure 2. ec VPN of transmission mode

Tunnel mode

As shown in Fig. 3 below, if we need to encrypt the data content sent by two different network segments through the IPSec VPN, or need to use two private IP network segments through the IPSec VPN to cross the Internet connection, you will need to use Tunnel mode IPSec VPN.

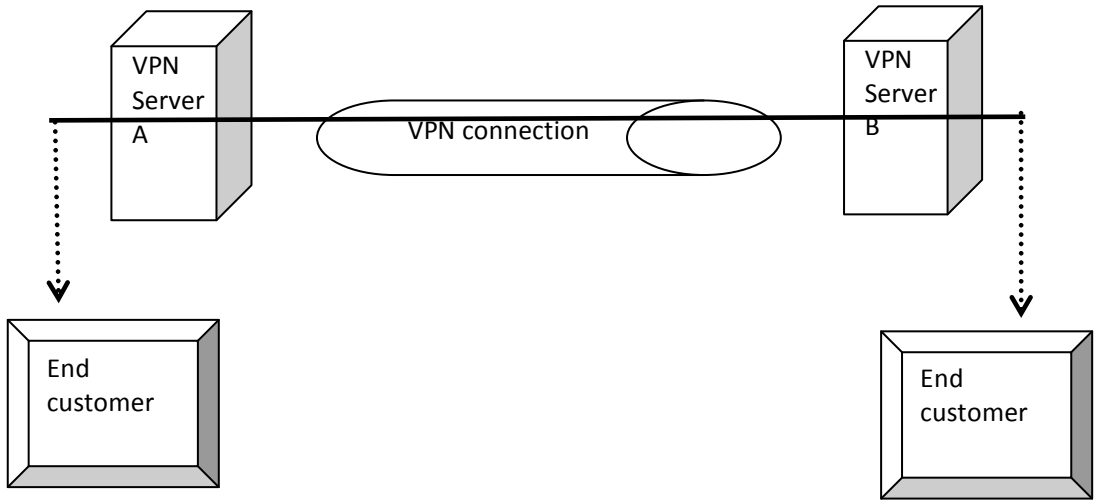

Figure 3. IPSec VPN of tunnel mode

Implementation Plan of VPN

The design of the Group headquarters network uses three-tier structure, namely the edge layer, the core layer and access layer, the specific network structure shown in Fig. 4 :

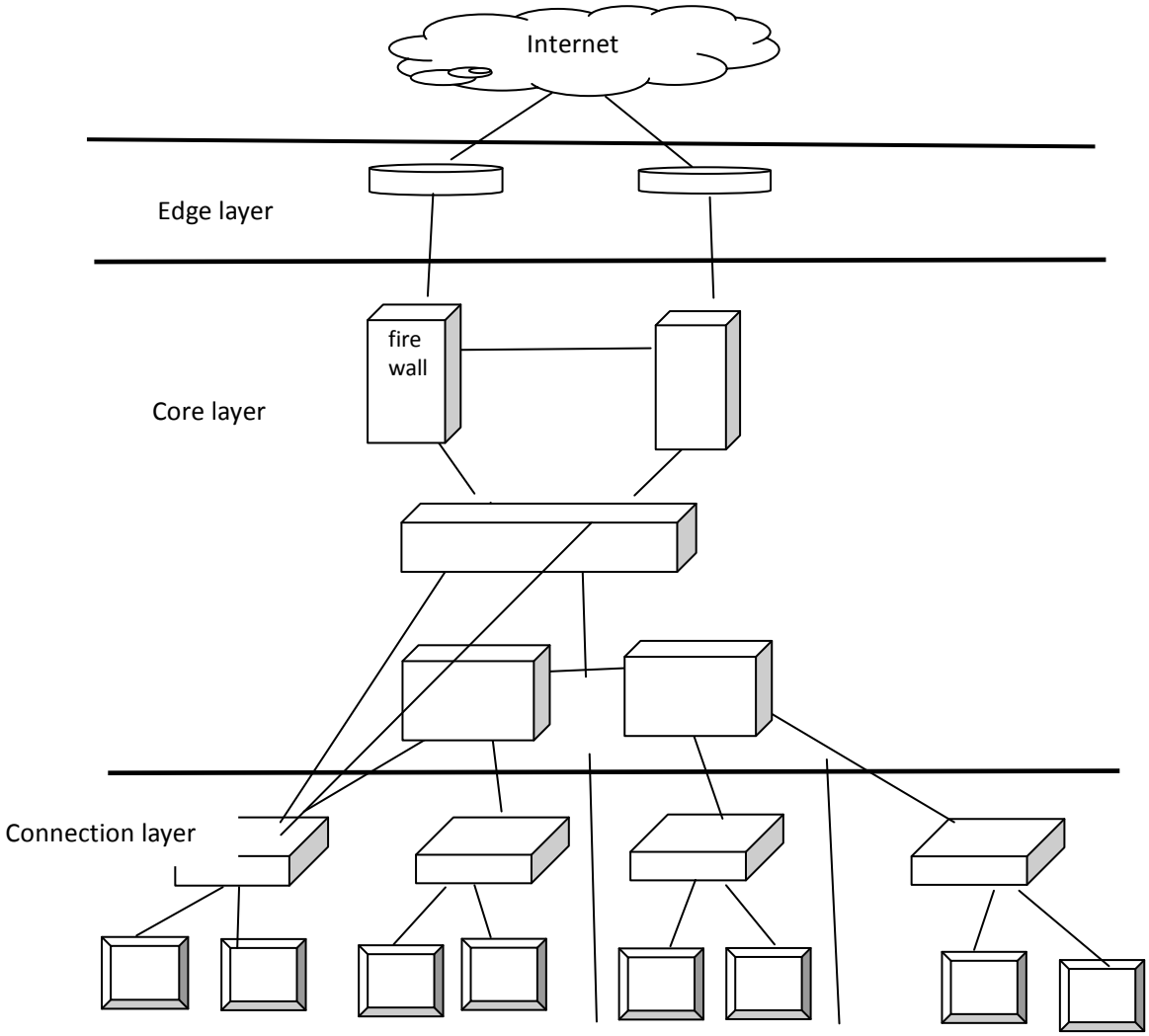

Figure 4. Network structure

The edge layer is responsible for IPSEC VPN tunnel termination and Internet access. Group headquarters Internet access links are provided by different operators, telecommunications 100M and Unicom 10M are all fiber access. Group headquarters network center is deployed with two IPSec VPN gateway, redundant for each other. The main VPN for Cisco 3745 connects the telecommunications 100M link, auxiliary with VPN equipment CISCO 3745, connecting Unicom 10M link up. Two VPN devices go down to the F5 equalization device to provide a redundant connection in load balancing. Once a VPN device fails, all VPN connections can be quickly and seamlessly switched to the second device to ensure that the WAN VPN Of usability.

Core Layer Group Headquarters LAN provides comprehensive routing and switching functions that provide a high-speed, broadband hub for the entire network and provide routing services to each information resource. The core layer consists of two CISCO Catalyst 6509 switches, through the HSRP for load balancing. Two CISCO Catalyst 6509 switches go up to the ALLOT bandwidth management device to ensure fair use of bandwidth resources for each application. ALLOT dually uplinks to the firewall, and two firewalls use hot standby mode working. Once a device failure, it can quickly and seamlessly switch to the second device, and the firewall device achieves different security areas isolation in the headquarters local area network.

The access layer is a layer that faces the user directly. It provides 10/100 / 1000M high-speed access for the majority of users, all switches go up to two core switches through the optical fiber dual-link to protect data redundancy. The DMZ service area of the Group's wide area network is

also located on the access network, which protects access restrictions by setting VLAN-based ACLs on the core switch.

Conclusion

VPN is a high-speed, reliable, secure, inexpensive remote network interconnection solution. The application of VPN technology reduces the operating cost of network and improves the efficiency of resource utilization, so it has obvious application value. With the acceleration of the informationization process in all walks of life, especially in e-commerce, e-government and distance education, remote office, management and other applications to promote, VPN technology will play a greater advantage and will become an important technology of future network security and ideal solution of remote network interconnection, with broad development and application prospects. In the formation of VPN network, companies need to analyze their own needs firstly, under the premise of understanding network size and capital investment, a set of suitable for their own business programs will be made, and then the required hardware equipments are selected. The selection of device not only refers to buying the appropriate VPN equipment or do the appropriate configuration, but also needs to take the future network expansion and equipment compatibility of different manufacturers into account.

★ Project Supported by: Nanchang Key Laboratory of Intelligent Building Network Engineering

References

[1] Qaddoumi N N, El-Hag A H, Saker Y. Outdoor Insulators Testing Using Artificial Neural Network-Based Near-Field Microwave Technique[J]. Instrumentation & Measurement IEEE Transactions on, 2014, 63(2):260-266.

[2] Caveney J E, Nordin R A, Doorhy M V, et al. Network managed device installation and provisioning technique[J]. 2012.

[3] W Xia, A Network Technique Based Feature Extraction Method For Remote Sensing Images[J]. 2015.

[4] W Xia, A Network Technique Based Feature Extraction Method For Remote Sensing Images[C]// International Conference on Environmental Engineering and Remote Sensing. 2015.

[5] Caldejon R I, Edwards D L, Fauerbach C H. Storing network bidirectional flow data and metadata with efficient processing technique[J]. 2016.

[6] R Huan,. Application of Computer Technology and Network Technique in Computer Room Management[J]. Value Engineering, 2011.

[7] Weiß M. Passive wireless local area network radar network using compressive sensing technique[J]. Iet Radar Sonar Navigation, 2014, 9(1):84-91.

[8] L Liu, Y Liu, The development strategy of the modern distance education based on network technique[J]. Technological Development of Enterprise, 2014.

[9] Said A M, Dominic D D, Faye I. Real-time network anomaly detection architecture based on frequent pattern mining technique[C]// International Conference on Research and Innovation in Information Systems. IEEE, 2013:392-397.

[10] Kersch P, Nemeth G, Toka L. Technique for projecting network load in a communication network[J]. 2017.

[11] C Lei, H.Q Zhang, D.H Ma, et al. Network Moving Target Defense Technique Based on Self-Adaptive End-Point Hopping[J]. 2017.

[12] Park J H, Jung Y H, Lee K H, et al. A New Privacy Scheme for Providing Anonymity Technique on Sensor Network[C]// International Conference on Ubiquitous Computing and Multimedia Applications. IEEE, 2011:10-14.