STUDY OF VPN APPLICATIONS IN 3G

ANITA NAIR

SRCEM GWALIOR

, *M.TECH SCHOLAR(COMP.SC)*

anita.nair24@gmail.com

ABSTRACT

This paper represents the VPN technology for new wireless 3G networks, in this paper architecture and mechanisms of VPN in the 3G.With the new view Parallel Server Cluster and MPLS-VPN-based algorithm and the principles of VPN technology, the current vulnerability of VPN technology in the 3G network and prospect its application in the 3G network. We are contacting cloud computing and VPN to study cloud security with VPN. This will be closely integrated VPN security with the clouds, to discover the new applications of VPN security in the cloud computing .

***Keywords*-VPN, 3G (Third Generation)**

I INTRODUCTION

“A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.”

“A VPN is a group of two or more computer systems, typically connected to a private network (a network built and maintained by an organization solely for its own use) with limited public-network access that communicates "securely" over a public network.”

With the advent of 3G networks, a variety of technologies to meet the 3G network will be mature. 3G network is high-speed, wireless and mobility, providing a fiber optic line, ADSL broadband access cannot match the convenience, so it is gradually becoming indispensable to the current broadband access in a complementary manner. In some non-fixed location, cable broadband cannot reach there, but they require high-bandwidth access to the environment play a unique role. For such a nascent Internet age, the network speed will remain the focus of attention. We had a lot of trial operation to increase network access speed, with mixed success. However, presentation and application of VPN (Virtual Private Network) in the 3G network has brought the gospel. In fact, cable network VPN has existed for long time, but accessing to 3G networks later, instead of the VPN routing, VPN hardware firewalls, etc. are based on the radio and there. Except wireless Internet, in the application layer, because passing through the operator's public network, so security must be taken into account, and because the tense of the current global IPV4 address, generally the ip address from 3G network can not directly access the internet ,but VPN can create their own virtual local area network business, just from the security and accessibility are two aspects of a good solution to both problems. In recent years, VPN technology has been widely used .For business, VPN's biggest attraction is price. It is estimated that, if an enterprise abandon the leased-line and use VPN, the cost of their entire network can save 21% -45% . Thus, VPN in the 3G network have great commercial prospects, therefore, there are a lot of third-party vendor for VPN.

II Types of VPN

There are three different VPN connectivity models that can be implemented over a public network Remote-access VPNs: It provides remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Deploying a remote-access VPN enables corporations to reduce communications expenses by leveraging the local dial up infrastructures of internet service providers. At the same time VPN allows mobile workers, telecommuters, and day extenders to take advantage of broadband connectivity. Access VPNs impose security over analog, dial, ISDN, digital subscriber line (DSL), Mobile IP, and cable technologies that connect mobile users, telecommuters, and branch offices.

Intranet VPNs: It links enterprise customer headquarters, remote offices, and branch offices in an internal network over a shared infrastructure. Remote and branch offices can use VPNs over existing Internet connections, thus providing a secure connection for remote offices. This eliminates costly dedicated connections and reduces WAN costs. Intranet VPNs allow access only to enterprise customer's employees.

Extranet VPNs: It links outside customers, partners, or communities of interest to an enterprise customer's network over a shared infrastructure. Extranet VPNs differ from intranet VPNs in that they allow access to uses outside the enterprise.

III VPN Security Features

The main purpose of VPN is to ensure security and connectivity (tunnel) over a public network and this cannot be done without some key activities being performed and policies set up. For VPNs to provide a cost–effective and better way of securing data over an insecure network it applies some security principles/measures. Data sent over the internet using the TCP/IP rule are called packets. A packet consists of the data and an IP header. The first thing that happens to a data being sent across a VPN is that it gets encrypted at the source endpoint and decrypted at the destination endpoint. Encryption is a method of protecting information from unauthorised persons by coding the information that can only be read by the recipient. The method, encryption, is done by using an algorithm which generates a key that allows information to be coded as unreadable by all and only readable to the recipient. The larger the number of data bits used to generate the key, the stronger the encryption and the harder it can be broken by intruders. Data encryption can be done in two ways; it can either be encrypted by transport mode or tunnel mode. These modes are process of transmitting data securely between two private networks.

In transport mode, the data part (otherwise known as the payload) of the IP packet is encrypted and decrypted but not the header by both endpoint hosts. While in the tunnel mode both the data part and header of the IP packet are encrypted and decrypted between the gateways of the source computer and the destination computer.

Another security measure implemented by VPN on data is IP Encapsulation. The VPN uses the principle of IP encapsulation to protect packets from being intercepted on the network by intruders by enclosing the actual IP packet in another IP packet having the source and destination address of the VPN gateways, therefore hiding the data being sent and the private networks IP address which "does not conform to internet addressing standards".

The third security measure is Authentication. This is a method of identifying a user by proving that the user is actually authorized to access and use internal files. Authenticating a, host, user or a computer that uses the VPN depends on the tunneling protocol established and also encryption for added security. The tunneling protocols that are widely used for authentication over a network are IPSec, PPTP, LT2P and SSL but the most commonly used is the IPSec. The hosts using VPN establish a Security Association (SA) and authenticate one another by exchanging keys which are generated by an algorithm (mathematical formula). These keys can either be symmetric key which is a private key that are exactly the same and only known by the hosts to verify the identity of one another or asymmetric key where each hosts has a private key that can be used to generate a public key. The sending host uses the other's public key to encrypt information that can only be decrypted by the receiving host private key. The Point-to-Point Tunneling Protocol uses the Microsoft Challenge/Response Authentication Protocol (MS-CHAP) to authenticate computers using VPN by exchanging authentication packets to one another. Also the users connecting to VPN can be authenticated by what the user knows- a password (shared secret), what the user has – a smart card and what the user is – biometrics e.g. finger prints.

IV VPN TECHNOLOGY IN THE 3G NETWORK

VPN Routing Traditional VPN transmited private network data flow In the public Internet with GRE, L2TP, PPTP tunneling protocol, LSP tunnel itself is in a public Internet. So, to achieve the VPN using MPLS has a natural advantage. MPLS VPN is a private network through the LSP to the different branches of banded together to form a unified network. MPLS VPN also supports interoperability between different VPN control. MPLS VPN supports the reuse of IP addresses among different branches, and support interoperability between different VPN. Compared with traditional routing, VPN routing needs to increase the branching and VPN-identifying information, which needs to extend BGP protocol to carry VPN routing informations.

V . NEW VPN APPLICATION IN THE 3G NETWORK

A. The 3G Network-based VPN

Access to Image Data VPN is based on the existing network to establish a virtual LAN, which means the equipment in the network or server has two ip addresses, one is pre-wired ip address, it is wired ,such as the server's ip address 212.25.4.1 is public network IP addresses, the scope of VPN network segment address we program is 192.168.2.1-255, assuming that we assign to the VPN server, the ip address of 192.168.2.1, when a device-side firstly get an ip address 118.34 .2.15 by 3G wireless network, but the ip address can not take the initiative to access from the outside , and then the device have an establishment of the VPN server's virtual connection by the built-in PPTP VPN client. It is like the device have two network cards and establish direct connection to the network server.The VPN server will assign the virtual links an ip address of 192.168.2.2 , so that it can visit the device 192.168.2.2 by using 192.168.2.1 .At this time if we need a remote watching for an image data from the device , first we have a computer which could access to the Internet , and then have an establishment of the VPN server,that is to say ,the client get the ip address of 192.168.2.3 which is from the VPN server , so that the client and the central VPN server and the device just like in a real LAN, you can access each other. Clients can monitor remote image with the vendor-supplied client software or the ip address 192.168.2.2 in the IE browser[4-6].

B. New VPN Architecture In 3G Network

The current most prominent feature of 3G networks are not subject to geographical constraints, the stability and the speed of wireless transmission are the most important indicator.

1. First, in the wireless router , we need to have a powerful processing chip and its function should be a fast process data and fast forwarding, for example, I recommend TI davinci chip, the overall use of "ARM + DSP "architecture,.Namely, it associated the use of ARM Embedded Technology with DSP-processing structure.

2.Second, there must be the VPN-based server. Because the ip address of wireless Internet is not the real ip address which can be routed on the internet, so the client cannot link point to point with video servers and you must transit with the central VPN server.

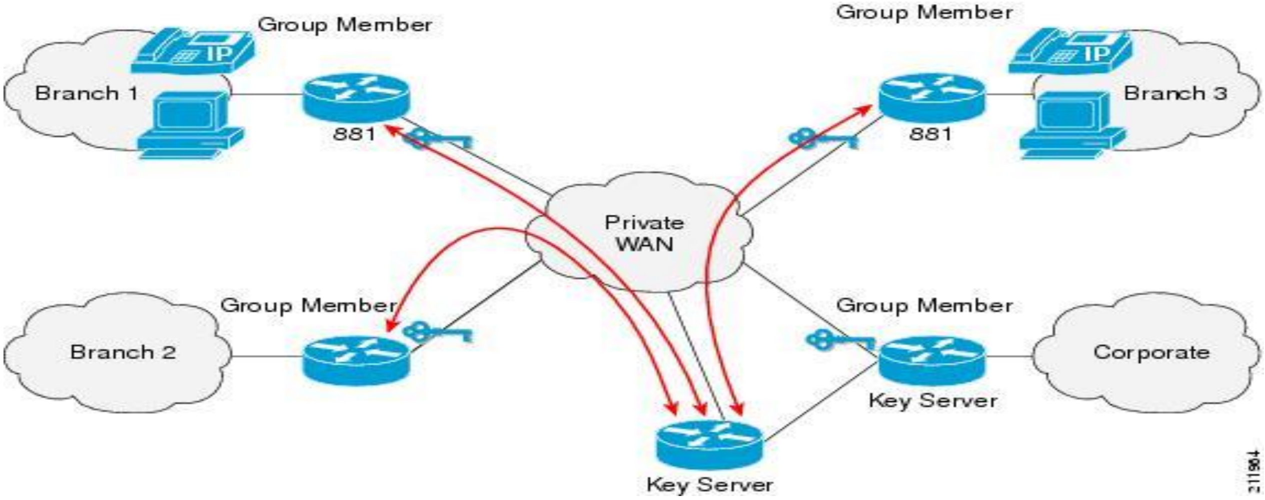

Figure 1.0

VPN ARCHITECTURE

3. The third is to build a virtual network tunnels. In the VPN, using PPP (Point to Point Protocol) packet stream is from a router on the LAN issue, through a shared IP network to transmit encrypted tunnel, and then to another router on the LAN,

C .New VPN Mechanism In 3G

3G network has just been put into practice, to some extent,a variety of mechanisms are not perfect. On the mainland ,most of PPPoE dial-up mechanism was used to access to the network environment, the operators change IP address frequently, which led to the instability of the network data transmission, however, in the 3G network, VPN have some new mechanisms to ensure the stability of its data transmission, they are: DPD (Dead Peer Detection) to detect VPN disconnection mechanism and to clear to see that whether online, in order to ensure that the VPN disconnected, it can make a first response and management; Keep-Alive mechanism, to continue to maintain a VPN line to help businesses automatically attempt to reach the first line of VPN to work to further ensure the VPN the stability of the quality of services are not dropped; NATT (NAT Traversal), ensure that the VPN device compatible with the mechanism, which is the mechanism for converting the packet format can be issued by the ESP Enterprise IPSec packet format into the UDP format, and then through the office management the Center's core router, VPN information can flow to achieve the purpose; VPN guaranteed bandwidth mechanism DDNS redundant VPN increase stability mechanism, which can help two dynamic IP-VPN gateways to find each other.

VI. CONCLUSION

In the emerging 3G networks ,using VPN technology, we can have a good access speed, especially if we join cluster parallel technology in this paper to the VPN server, because this technology include the parallel machine and parallel algorithm ,with which effectively the world's 3G networks all nodes are utilized, and even more effectively improve the performance of VPN access to the network itself. In addition, VPN's new architecture and mechanisms put forward, it also breaks the traditional framework of constraints, give full play to the 3Gnetwork.

REFERENCES

[1] Haiying Gao, VPN Technology[M],Machinery Industry Press,2004,pp.72-99. (in chinese)

[2] (US) Lucas . Firewall Policy and VPN Configuration . Water Resources and Hydropower Press,2008,pp.321-444.

[3] Zhiying Lv. On the VPN Technology .《Management and Technology》Journals, 2008 No. 3.pp.34-77.

[4] Dengguo Feng . Network Security Principles and Technology. Science Press , 2003.pp.65-87.(in chinese).

[5] Elizabeth D.Zwicky,Simon Cooper,Tsinghua University Press,2003,pp.54-77.

[6] Carasic-Hengmu.Firewall Core Technology Intensive Solution . Hydropower Press . 2005 . 4.pp..99-102

[7] Mei Zhang.SSL VPN Key Technology Research and System Design[D].PLA Information Engineering University Press,2006,pp.89-99.

[8] Jiazhen Xu,Comparison and Analysis of IPSec-based and SSL-based VPN[J],Computer Engineering and Design