Volume 8, No. 5, May-June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An approach to Virtual Private Networks and security

Dr. Himanshu Monga
Principal / Director, Engineering
Jan Nayak Ch.Devi Lal Vidyapeeth
Barnala Road, Sirsa, Haryana 125055

Abstract: To achieve the secure transmission of information from source to destination, concept of VPN(virtual private network) was introduced which ensures that the attacker cannot read the data but only the intended recipient can read it.VPN serves the functions of a private network with the difference that VPN works over a public network and occupies its own address space. These networks provide all the parameters that are required for security purposes like data confidentiality, data integrity and authenticity.

Keywords: VPN,Authentication,Encryption,Internet,Tunneling

I. INTRODUCTION

The use of internet is tremendously increasing and thus makes it difficult to send the secure data on a public network. security is a vital issue these days in practically every system. The need of secure and encrypted transmission of information between the parties by the big companies and organisations so that their confidential data cannot be publicized led to the concept of virtual private networks(VPN). Initially the concept of VPN was entirely developed for companies. However, the pros of VPN's made it available in the market to the end user's also. The demand of VPN's is enormously increasing from some years due to some reasons like ban implemented by government authorities on some websites, geo-blocking and ban on the use of public network (internet) in some countries. These reasons proved VPN's to be the veritable tool for accessing the public network privately. A number of security techniques like token authentication were incorporated from time to time in VPN's to make the technology more secure and confident[1]. Virtual Private Network is actually a private network within a public network. It is a means of transmitting information in a secure way over a publicly accessible network(internet) by creating a temporary virtual tunnel through an insecure public network[2].VPN can be best described as a a network which traverses a part of public network path and utilises the properties of private network. The network is maintained in such a way that the information that need to be protected can be decoded only by the sender and intended recipient[3]. One of the major asset of VPN's is that they are highly cost effective. An alternate way of using VPN is high speed leased line which are very costly ,hard to maintain and hard to administrate. Also, any failure in a leased line results in the failure of communication between two parties until it is repaired by some expert. On the other hand, in VPN, any failure of the nodes in the path between communicating devices when observed, a simple change in the logical path between two parties to a transparent user is made, The reliability of service is ensured by using a public network (internet) as a backbone of communication [3].

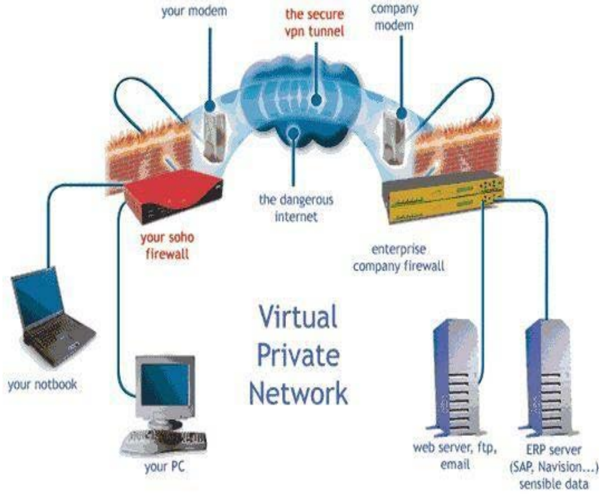

Fig 1. Virtual Private Network[4]

II. VPN WORKING

The use of public network as a private network demands the overcome of some hindrances that the companies and organisations may face while transmitting information in a secure way. The two hurdles that are needed to overcome are;

(i) The way of communicating in various networks depends on the use of different protocols. Since internet is also a communication network and supports only IP traffic, therefore ,there may be a need of providing non-IP protocols between the networks.

(ii) The second hurdle is that a clear text is used to transmit information over the internet and it can be read by anyone. Hence, lack of security can be a serious problem.

These hindrances are overcome by VPN's by using a technique called as Tunnelling in which data packet that is to be transmitted is first encoded and encapsulated in an IP package and is then securely tunnelled through the public network to the destination end[3].

The data packet to be transmitted is wrapped in a packet and header is attached to it. Header is attached for routing information so that the packet traverses the path of a public network and reaches the destination point of a tunnel. The Tunnel is actually a path that is traversed by an encapsulated packet while reaching the tunnel endpoint. On the destination end ,the packet is decapsulated (IP package is removed) and send to its intended recipient. The entire transmission is supported by protocols called as Tunnelling Protocols which run either at OSI(open system interconnection) layer or link layer or data link layer[5].

III. VPN SECURITY

Virtual Private Networks because of their property of providing secure transmission of information between two parties brought a revolution in the field of networking and communication. By establishing a VPN connection, a secure transmission of data is ensured by the features like data confidentiality, data integrity and data authentication to prevent the attackers by restricting all the traffic except desired data from intended locations or for an intended recipient[6].

To provide data confidentiality, VPN makes use of encryption technique. The encryption of data is performed by Tunneling mechanism in which encrypted data is encapsulated and attached with openly read headers and then securely enter a Tunnel(virtual path) so as to traverse a public network path and reach a destination end. Hence, data transmitted cannot be disclosed or changed by intruders. Thus, the data cannot be viewed or altered by the attackers.

Data integrity check is provided by VPN's to ensure that the data packet is not interfered or tampered by the attacker. A message digest is used to perform data integrity check.

As a matter of course, VPN's does not give or uphold strong user authentication. A simple username and password can enable the users to access an internal private network from home or some uncertain systems. Despite of that, add on authentication mechanisms such as token, smartcards and RADIANS are supported by VPN's [5].

IV. PROTOCOLS USED IN VPN

The protocols that are supported by VPN are called as Tunneling Protocols. The prime focus of these protocols is confidentiality, authentication and maintain data integrity and ensuring the data identity on the network(i.e. data should not be changed by the attacker)[4]. These protocols include

- IPSEC-Internet Protocol Security
- PPTP-Point to Point Tunneling Protocol
- L2tp-Layer Two Tunneling Protocol
- SOCKS- Socket Secure

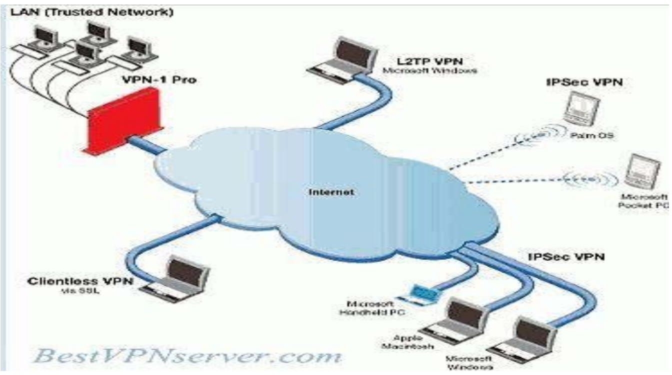

Fig 2. Protocols used in VPN[4]

These protocols are explained below;

1. IPSEC(Internet Protocol Security):

For transmitting information in a confidential way, IPSEC was developed by IETF (the Internet Engineering Task Force) at the third layer of OSI through an insecure public network (internet) to provide enhanced security features like authentication, data integrity and encryption services for preventing the unauthorised disclosure and alteration of data by intruders. AH (Authentication Header) and ESP(Encapsulated Security Payload) are two security protocols that are used for desired services. IPSEC is restricted to just sending the IP packets[5].

2.PPTP(Point to Point Tunneling Protocol):

It is the most commonly known security protocol from Microsoft. It is layer two OSI protocol i.e. works at the link layer of OSI model where a PPP is encapsulated with IP package [4].A multipoint, dial up protocol that has a function of making connection to the internet is a point to point protocol. In a PPTP based VPN connection, the authentication mechanism is same as used for PPP connection [5]. This mechanism includes EAP(Extensible Authentication Protocol), MS-CHAP(Microsoft challenge Handshake Authentication Protocol), CHAP, SPAP(Shiva Password Authentication Protocol) and PAP(Password Authentication Protocol).

3.L2TP (Layer Two Tunneling Protocol):

This protocol also functions at data link layer of OSI model and was basically implemented in CISCO protocols[4]. L2TP supports multiple connections through a single tunnel. PPTP is followed by L2TP and the authentication mechanisms that are used in PPTP(like EAP, CHAP,MS-CHAP,PAP and SPAP) are used in L2TP[5].

4.SOCKET:

It functions at layer five i.e. session layer of OSI model. Hence, access control by this is much finer than the above mentioned layers[3]. This protocol is used less as compared to above ones.

IV. SUPPORTING TECHNOLOGIES IN VPN

There are a number of underlying technologies that make a VPN connection possible. A VPN connection makes use of some or all of these technologies to transmit the information in a confidential manner between the two parties. The mechanisms include Tunnels, Firewalls and Proxy Servers. Tunnels are primarily used in every VPN system while as Firewall and Proxy Server are sometimes used in a VPN system[3].

(I) TUNNELS:

The technique of establishing a virtual path (tunnels) through a public network (internet) is called as Tunneling. Tunneling also refers to the establishment of virtual point –to-point connection across a public network[4].Tunneling also called as 'encapsulation' is a mechanism in which a packet is wrapped inside other packet where the wrapped packet is known as encapsulated packet and the external wrapping packet is known as transport packet. The packet is then made to pass through a tunnel. The encryption of the packet containing information is performed at the link layer of the OSI model[3]. The mechanism of tunneling simply involves encapsulating a data packet with its own header which gives information about the intended sender and recipient within an IP package to which header is also attached so as to specify the endpoints of the tunnel such that the confidential data that needs to be transmitted is between the two headers[3]. The protocols required to carry out tunneling process are passenger protocol, encapsulating protocol and carrier protocol[4].
Tunnels are classified in two classes; compulsory tunnels and voluntary tunnels.

(a) Compulsory tunnels:

These tunnels are also called as client-transparent tunnels. These type of tunnels establish a VPN connection. When the user sets up a connection, compulsory tunnels are initiated through ISP (internet service provider).The connection that needs to be tunnelled is identified when client dials into an ISP after which a tunnel to tunnel server is established by an ISP. This establishment of tunnel lets the client to form a connection through tunnel to the tunnel server. The whole connection appears as the direct connection between client and tunnel server. A simple username and password is entered for authentication process and hence there is no need of any special software for the client .However, compulsory tunnels ensure that there must be enabled access servers and may be routers for ISPs point of presence(pop). These tunnels are used for maintaining the connections for long sessions from the fixed location[3].

(b) voluntary tunnels:

This tunnel technique results in establishing and maintaining VPN connection by carrier network provider[4]. Such type of tunnels are initiated by the client . The tunnel is terminated by the ISP and hence there is no need of tunneling. It also provides authentication by simply entering username and password. These tunnels are beneficial for accessing distant, mobile computing[3].

(II) FIREWALLS:

To manage and control the access to the company network, a set of hardware and software is used called as firewall. The access to the public network(internet) for the company is provided by firewall which further restricts all other traffic from entering the network and hence ensures a secure connection [3]. Furthermore, to limit the number of open ports, the kind of packets crossing the network and the type of protocols to be used, firewall is used. Firewalls are classified in two classes[4]:

(a)Packet Level Firewall :

These firewalls have a complete control over incoming and outgoing traffic. The traffic is identified by software filters or router hardware . The software filters used for identification of message is called as packet filter and the firewalls using routers for message identification is called as router firewall[3].

(b) Application Level Firewall:

These firewalls have a complete control on a network access. And some special applications like Telnet or FTP are monitored by using these firewalls. However, these firewalls are hard to install and very costly[3].

(III) PROXY SERVERS:

A combination of of firewall and proxy cache gives proxy server where a proxy cache is used to enhance security performance. The network performance is enhanced by conserving the bandwidth of network. The property of providing security by the proxy server is mainly in directed VPNs[4]

V. TYPES OF VPN

VPN's are classified into different types and depending on the need and requirement ,customer will choose the kind of VPN accordingly. The different kinds of VPN are explained as;

(1) Remote Access VPN:

This kind of VPN being very easy and less costly removes the use of traditional dial-in-lines by eliminating the load of companies that have to manage large modem banks[3].
A user to LAN connection also known as virtual private dial-up network (VPDN) is a Remote Access VPN. This type of VPN is used by the big companies that have large number of sales people at the distant locations and need remote access VPN which results in the establishment of an encrypted and secure connection between the distant users and companies private network through a public network[4].

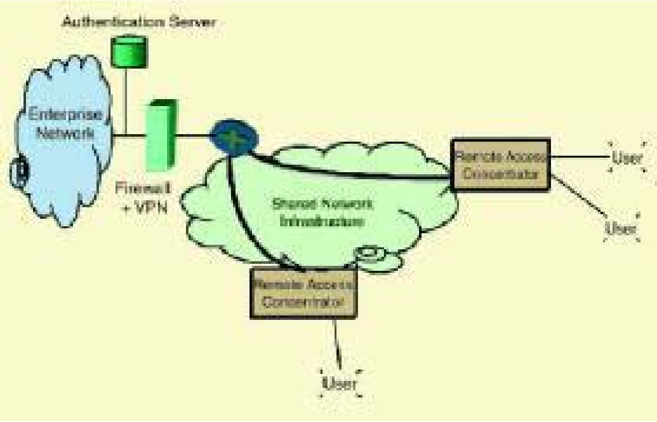
Authentication Server
Enterprise Network
Firewall + VPN
Shared Network Infrastructure
Remote Access Concentrator
User
User
Remote Access Concentrator
User

Fig 3.Remote Access VPN[3]

(2) Site –To-Site VPN (Intranet –Based):

This is a type of VPN in which a company having some remote locations are needed to connect in a single private network by establishing an intranet VPN for LAN to LAN connection[4].

In these VPNs, the two communicating devices share a high level of trust and both the tunnel endpoints are controlled by corporate office, hence, security needs like confidentiality is not of much importance[3].

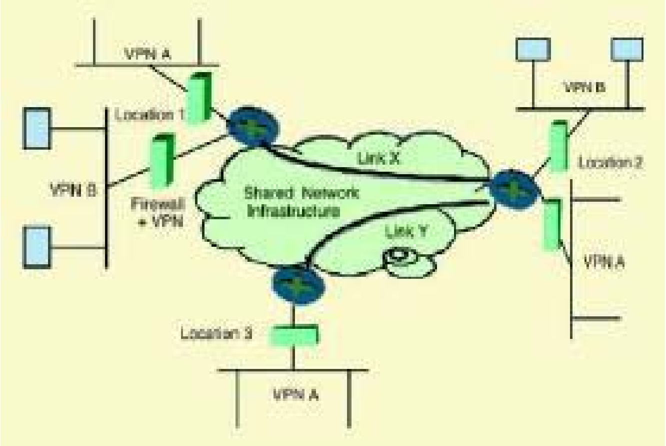

Fig 4. Site-To-Site VPN (Intranet-Based) [3]

(3) Site-To-Site VPN(Extranet –Based):

This VPN device is employed for set up of company to company connection. An extranet VPN connecting LAN to LAN is created by a company having close terms with other company (supplier, partner or customer)[4].

Extranet VPNs have the major contribution in providing versatility of the system [3]. A VPN proxy server resident behind a firewall constitutes an extranet VPN system[3].

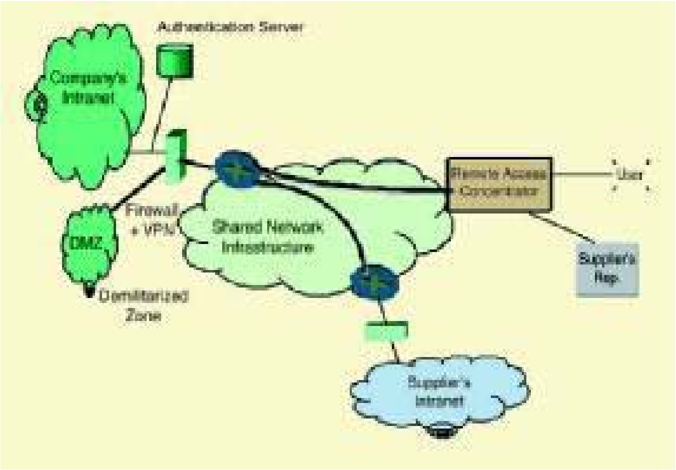

Fig 5. Site-To-Site VPN(Extranet-Based)[3]

VI. ADVANTAGES OF VPN

VPNs are having number of advantages and these advantages are the reason behind the popularity of VPNs in today's world full of challenges to privacy and information security. These benefits are explained below:

(A) SECURITY:
Security is of vital concern in almost every practical system. When an information is transmitted on any network, it is targeted by a number of intruders and hence, the information can be altered or read by an attacker. VPNs provide an encrypted and secure connection and cannot be decrypted by any attacker as a result of which the transmitted information is transmitted is read by the intended sender and recipient only.
When a VPN network is caught by an intruder, he wont be able to see the data, what he sees will be indecipherable characters shared between the two parties[7].

(B)PRIVACY PROTECTION:
When the user is not interested in disclosing his identity like name, address and location, VPN comes to play. By using VPN , the user can hide his identity and appears on the network with the identity of VPN provider like IP address, location etc. Web proxies are also used to hide the identity but they are inefficient as compared to VPNs.

(III) ACCESS TO RESTRICTED RESOURCES:
In some regions, access to some internet sites are restricted or access to some sites like facebook is prevented during working hours by the companies to their employees, VPN helps to evade these geographic restrictions.

(IV) BETTER CONNECTIVITY:
The poor web experience and slow browsing is overcome by use of VPNs[7]. VPN further routes the traffic of the user that results in same bandwidth to remote locations and between user and VPN provider.

(V) COST EFFECTIVE:
This is one of the major benefit of VPNs as per consumer point of view. Highly leased lines that can be used as an alternate are very costly, difficult to maintain and hard to administrate[3]. Furthermore, any failure in any node in leased line makes it to stop functioning, however, when any node fails in VPN system, the communication is changed to user. VPN systems are easy and cheaper to maintain. Besides decreasing the cost, VPN increases flexibility as the internet connections are established on demand[3].

VII. DISADVANTAGES OF VPN

(I) VPNs require a well knowledge of network security issues and careful installation is needed on deploying a VPN connection.

(II) The performance of VPN depends on ISP and its quality of service.

(III) Due to immature standards, VPN connections from different sales people may not function properly.

(IV) Additional protocols are required by VPNs other than IP and existing internal network technology [4].

VIII. APPLICATIONS OF VPN[8]

VPNs are used in a number of fields , some of which are described as:

(I) Access a Business Network While Travelling:

VPNs are used by the employees and businessmen to access their business networks without exposing to internet from their offices.

(II) Access Home Network While Travelling:

A VPN connection can be established for personal use to access ones own network while travelling for playing games over internet, sharing files etc as if the user is on the same LAN.

(III) Hide Browsing Activity From Local Network and ISP:

VPNs are used to hide identity or browsing activity over the network such that the user appears with identity of VPN provider like IP address, location etc.

(IV) Access Geo-Blocked Websites:

VPN is used to access geographical restricted sites.

(V) Bypass Internet Censorship:

Many sites in some regions like china are blocked by censorship government and VPNs help to gain access to the entire internet.

(VI) Downloading Files:

VPNs are used by many people to download files through Bit torrent.

IX. CONCLUSION

Since the use of public network (internet) does not ensure secure transmission of data, therefore, VPN system was established to access a secure, private, internal network over insecure public network (internet).VPNs provide a number of encryption, authentication and data integrity algorithms.

In this paper we observed some supporting technologies in VPN which cleared that no standard has been set yet for using VPN. VPN technology is still developing and is expected to be the promised technology in the coming years for secure communication using public network (internet)

REFERENCES

[1] http://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history

[2] Ekwe O.A, Iroegbu, “Virtual private network: A veritable tool”,international journal of research in engineering and technology,May 2014.

[3] Ayhan ERDOGAN,DZ.Yzb, “Virtual private networks: A survey”

[4] M krithikaaa, M priyadharsini, c.subha, “Virtual private networks-A survey”, International journal of trend in research and development,volume3(1),jan-feb 2016.

[5] http://www.infosec.gov.hk/english/technical/files/vpn.pdf

[6] https://vpntunnel.com/faqs/top-five-vpn-advantages-benefits/

[7] www.howtogeek.com/13380/htg-explains-what-is-a-vpn/