A SURVEY REPORT ON: - VPN

[1]Sneha A. Padhiar, [2]Karishma Chaudhary
[1]Assistant Professor, [2]Assistant Professor
[1]Computer Engineering
Charusat Unniversity, Nadiad,India

ABSTRACT- VPN [1] is a Proven Technology that does Provide Security Strong enough for transmission & business use. Virtual Private Network is a Communication Network Which provides Secure data transmission in an unsecured or public Network In VPN[1]. The Secure Connection across the Internet appears to the user as a Private Network Communication despite the fact that this Communication Occur over a Public Internetwork-hence the name Virtual Private Network [1]. This Paper Provides a Survey Report on Brief Introduction of VPN and its tunneling Protocols.

Index Terms- **VPN, Tunneling, IPsec, PPTP, SSL, L2TP**

I. INTRODUCTION

A Virtual Private Network(VPN)[1] is the Combination of Private and Public Networks. such as Internet. VPN Performs Secure data Transmission from one end to another end. Whenever we want to transfer our Important data Through a network, due to Security Concern for that data we leased a private network for transferring data in secure way because in Public network Proper Security features are not available which harms our data[1],[3]. Same way Secure transmission of data by using Private Network Charges very high. So VPN is a Best Solution to transfer our Data through secure as well as cheaper medium as compared to Private Network. The Secure Connection across the internet appears to the user as a Private Network Communication-despite the fact that this Communication occurs over a Public Internetwork- hence the name Virtual Private Network[1]. A VPN sends data between two Systems across a Public Network in such a way that the transmitted data is transparent to the other Systems Connected in the Network. VPN emulates Point to Point link between the two system so we get the transparency in data transmission. Point to Point link is Provided by Encapsulation is done by wrapping the data with a header, In header it Provides Routing Information. This Process is Known as Tunneling. To Provide Confidentiality to the encapsulated data, the data is Secured by Encryption.[1][2][3] When Data reaches to the end Point of Tunnel, the Process of Decryption is Performed on Encapsulated data and forwarded to its final Destination Point.[1]

Fig.1 Shows a Diagrammatic Representation of Virtual Private Network

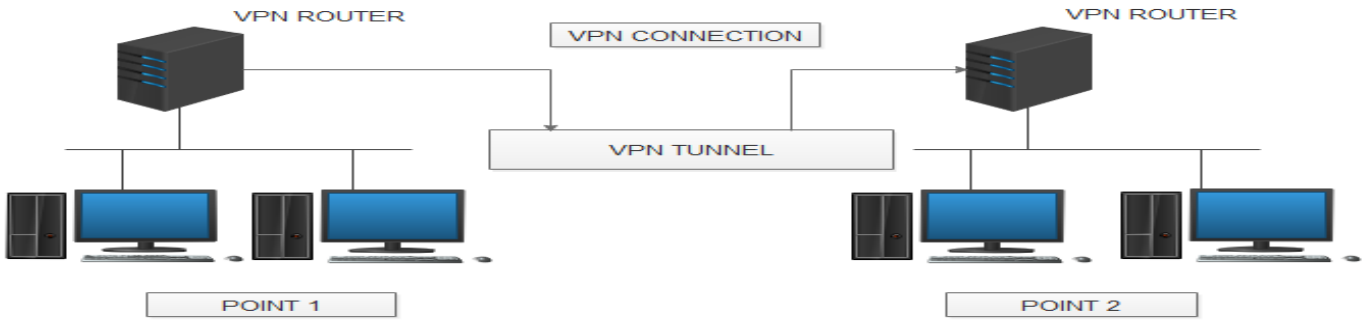

Fig. 1. Virtual Private Network Architecture

This Paper is Organized as Follows: Section I gives an Introduction to VPN. Section II Contains an Overview of VPN. Section III Contains Various Security Protocols Which are Used in VPN. Conclusion Is given in Section IV.

II. VPN-AN OVERVIEW

VPN allows Organizations to Connect to their Branch Office or to Other Companies Over a Public Network While Maintaining Secure Communications. Security is the most Important and Critical factor foe Organizations/Companies Worldwide.[1][2][4] Every Organizations need a Secure and reliable Infrastructure for their System to mitigate the risk of malicious activity from both external and Internal Sources.

major Security Concerns Which, every Organizations faces are[1]:-

- Data access from the Remote Site[1]
- Infection by Viruses[1]
- Intrusion by Hackers[1]
- Disruption in the Storage Network[1]

To Overcome the above Mentioned threats and Vulnerabilities in the network, VPN Provides Various Securing Measures.[1][1 2]
The Measures are Outlined Below[1]:

- Data Encryption and Authentication are Done into the VPN Network[1].

  Secure VPNS have more than one tunnels and each tunnels has two end points, Sender and Receiver Where Sender and Receiver accepts and agree upon the Security properties of the tunnel.[1]
- Security Properties of the VPN can't be change, modify by any external third party.[1]
- Routing Path of Data over a VPN can't be Change, add or delete by Outsides.[1]

III. VPN SECURITY PROTOCOLS

Various Security Protocols for Tunneling which are used in VPN are1]-[4]:

- Internet Protocol Security(IPsec)
- Layer2 Tunneling Protocol(L2TP)
- Point to Point Tunneling Protocol(PPTP)

All the Security Protocols Runs in Two Modes of Operations They are[1]-[4]:

- Tunnel Mode
- Transport Mode

Tunnel Mode[1]-[4] Operation is Called End-to -End Method of operation. It Interfaces two Purposes of a VPN Over the Common System. In the Passage mode, the end Purposes of the Passage are Regular hubs of the VPN and the Common System in. This Mode gives Information Security[1][2].

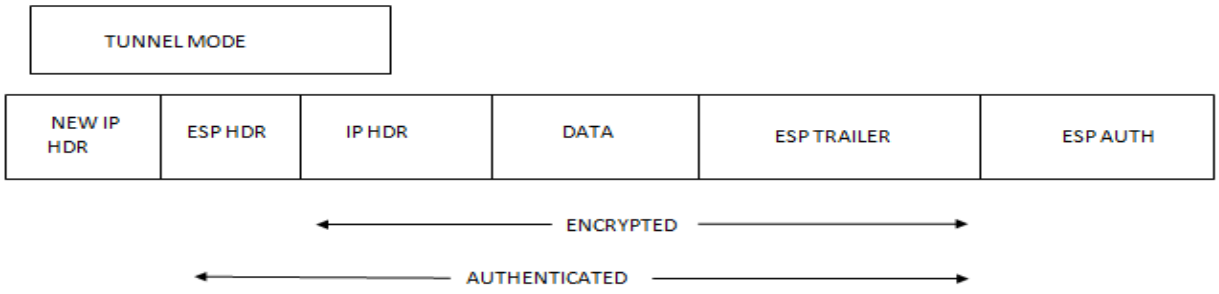

Fig.2. Tunnel Mode Packet Format

Transport Mode is Called host-to-host method of Operation[1]-[3]. The Information bundle Contains ESP header and Trailer, IP header, ESP verification and so on. IP header is not encoded. Thus there is Probability of Sniffing the location by the aggressors[1]-[4].

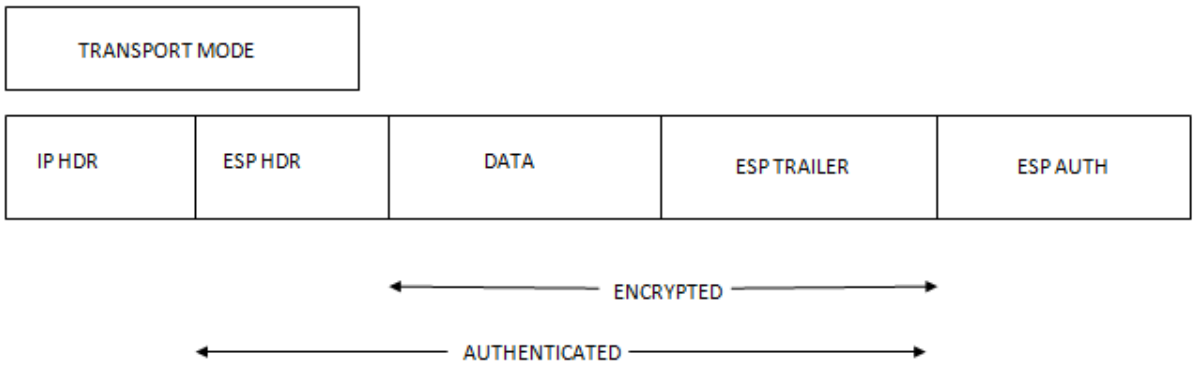

Fig.3. Transport Mode Packet Format.

IPSEC:

At time of data Transmission IPSEC Provides Authentication of Users, Encryption of data and data Integrity between Senders and Receivers[1]. It Uses three Primary Protocols which are Authentication Header(AH), Encapsulated Security Payload(ESP), And Internet Key Exchange (IKE)[1]-[5]. These protocols are used in establishing Connection and transmitting data in Secure way.

.

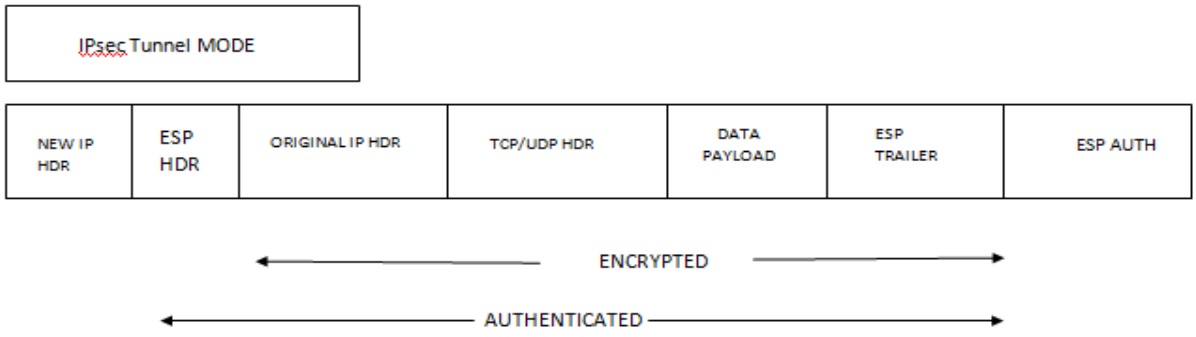

Fig.4. IPsec Packet Format

L2TP:

L2TP is additionally worked at the laye2 of OSI engineering[1][2]. One passage can Permit various associations. layer two tunneling tradition exemplifies data in PPP diagrams and is fit for transmitting non-IP traditions over an IP framework[1][3]. The PPP data is Exemplified inside a PPP header and a L2TP header. In this the typified L2TP bundle is again exemplified in a UDP header. The last Parcel is Exemplified with an IP header containing the source and destination IP locations of the VPN Server and VPN Client[1]-[4].

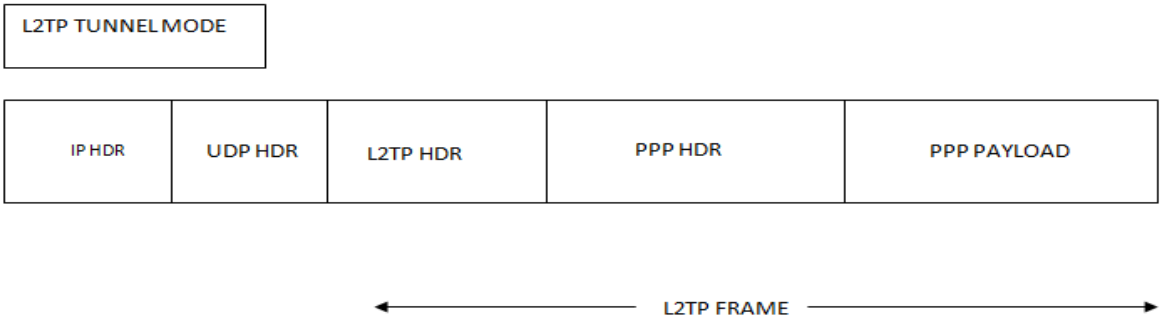

Fig.5. L2TP Packet Format

PPTP:

Point to Point Tunneling Protocol is layer two OSI tradition in light of top of the Point to Point Protocol[1]. It partners with the target framework by making a Virtual framework for each remote client. It allows a PPP Session, with non-TCP/IP traditions, to be tunneled through an IP Framework[1]-[3].

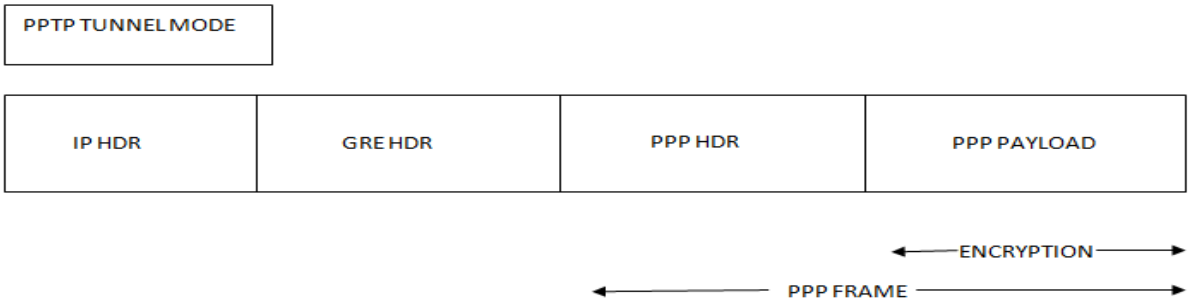

Fig.6. PPTP Packet Form

IV CONCLUSION

VPN is a Proven Secure technology. Through this survey we can concluded that ,VPN is Efficient and Effective technology for Secure transmission of data. VPN is Combination of Private and Public Network, where it provides Private and Secure transmission mode in our Public Networks Environment. [1]-[4]

REFERENCES

1]Jyanti Gokhul Krishan "A Survey Report on VPN technology and Its Issues", ,IJCSE,aug-sep 2014,ISSN 0976-5166

2]Dr.P.Rajamohan "Performance analysis and Special issues of VPN technologies in Communication", IIJCS,July 2014

3]Sneha Padhiar,Pranav Verma "A survey on Performance Evaluation of VPN on Various Operating Systems", IJEDR,vol-3,issue-4,2015

4]Shaneel Narayan, Samad S. kolahi, Kris Brooking, Simon De Vere, "Performance Evaluation of Virtual Private Network Protocols in windows 2003 Environment" ,© 2008 IEEE

5] Dr. S. S Riaz Ahamed, P rajmohan "comprehensive performance analysis and special issues of virtual private network strategies in the computer communication", IJEST, July 201.