ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Role of Security in Virtual Private Network (VPN)

[1] Dr. Rizwan Patan
[1] Department Of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] patan.rizwan@Galgotiasuniversity.edu.in

Abstract- Virtual Private Network is a connectivity system that offers secure information propagation over an unprotected or media system using any technology blend.A digital link is made through globally distributed consumers and systems, such as the Web, over a private or shared channel.Although the information is disseminated via a public network, Virtual Private Network gives the impression that the information is conveyed via the private association. VPNs enable distant customers to safely store personal systems over the Web.Virtual private networks provide complex, minimal-cost, encrypted access to personal channels. Perhaps such connectivity would be feasible using a costly leased line approach or by plugging straight onto the local area network.The paper presents the Virtual Private Network idea that spreads a private network along with a corporate network, like the web.It allows a person to transmit information around the community's shared network as if the processing machines are directly linked to the local network.The VPN service is entirely devoted to smaller business firms.

Keywords-Authentication, Confidentiality, Security, Virtual Private Network (VPN).

INTRODUCTION

A Virtual Private Network is the collection of personal and corporate channels like the Web, and the sharing of information is safe.A virtual private network, like regional offices, may create encrypted virtual ties between different companies[1].It will not provide such an outside facility among them and will not permit interference by any entity.A VPN transmits over a corporate network among several networks in such a manner that the data going is invisible to other network-connected devices.Such openness is feasible in transmission of data because VPN imitates end to end connections between the two structures.End to End connection is given through data encapsulation.A VPN provides safe access to LAN assets via shared network technology, like the Web. It can be conceived as creating a tunnel from one area to the next, with encrypted files travelling via the tunnel before they are deciphered at their target.Distant consumers can link to the Local Area Network or other LAN within their organization. As if they were linked to the LAN as usual, they can reach services like email and files. The Term VPN specifies

Virtual-It implies a diverse association.Using the fault sensitive features of the Internet it can evolve and change to various conditions.If a link is needed it is developed and retained around nodes irrespective of the internet infrastructure.The link is discontinued when no longer needed, keeping costs down and the number of unnecessary networks[2].

Private- It implies that the information exchanged is always kept private and can be viewed only by approved users.This is essential since the initial standards of the internet-"TCP / IP (transmission control protocol/internet protocol)" are not intended to provide privacy standards.

Network- *It* is the entire system that holds the information around endpoints of customers, sites or access points. It is developed using the accessible personal, public, connected, connectionless, Web, or any other suitable system asset.

A VPN is a form of private telecommunications network used by the public. This allows remote access over the web to the systems of a company rather than using wires to interact. Through linking workplaces a VPN can be built, and individual users like mobile phone users to the closest service providers[3].VPN is not the first wireless connection-making innovation.Some years earlier, the use of a leased line was the most popular way of linking machines among different offices.VPN enables organizations to link via a corporate network to the remote offices or other businesses whilst preserving encrypted communications.Security is the most significant and crucial determinant for businesses around the world. Institutions expect their networks to provide reliable and efficient facilities to reduce the possibility of suspicious

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

activity from both externally and internally sites.The formation of Virtual Private Network is shown below in Fig. 1 Virtual Private Network.

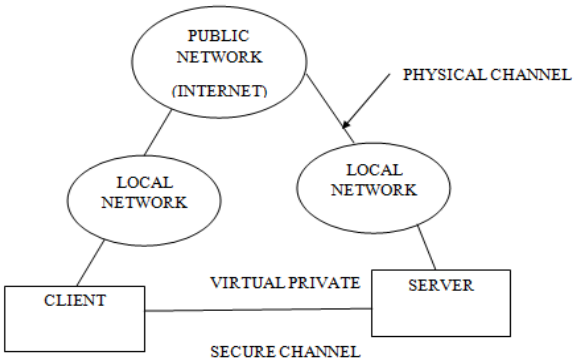

Fig.1: Virtual Private Network

TYPES OF VIRTUAL PRIVATE NETWORK

Remote Access VPN- A direct link to VPN is rendered through a remote access application. A remote access customer is a single client of the desktop which links from a remote place to a home network. The VPN provider gives access to the computing resources that are linked to the VPN server[4].The messages that are sent over the VPN connection come from the "VPN client". The VPN client verifies to the "VPN server" and the "VPN server" encrypts itself to the VPN client for shared encryption.Remote access, also known as "Virtual private dial-up network (VPDN)", is a Local Area Network link device.A perfect example of an organization needing a remote-access VPN will be bigger companies with thousands of marketing professionals in the field.It offers safe, authenticated communication via a third party supplier between such a firm's local network and mobile customers.It can be introduced by establishing a VPN portal or database, and it is possible to link to it from certain places using VPN client. The concept of Remote Access VPN is shown below in Fig. 2 Remote Access VPN

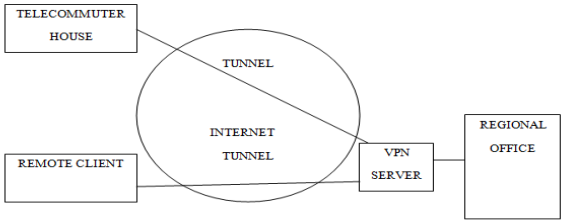

Fig.2: Remote Access VPN

Site to Site VPN-A VPN links from site to site links two parts of a local network or multiple local networks. It helps a company to have wired links over the Web, for instance, with different departments or with other organisations[5].Site-to-site VPN is the VPN link among several VPN access points residing over the Web in different networks so that machines of both channels can share data safely. Client machines don't need a VPN client.The VPN link between both VPN access points is built. All VPN routers must authenticate and decipher the information about the contact to make sure the security and privacy of information. "IPSec tunnel method, PPTP, L2TP over IPSectunnelling" procedures can promote the site-to-site VPN. The concept of Site to Site VPN is shown below in Fig. 3 Site to Site VPN

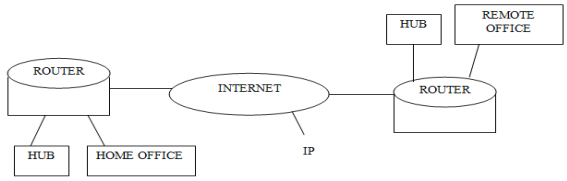

Fig.3: Site to Site VPN

Peer to Peer VPN-Peer to Peer VPN allows the participation of trustworthy peers. This can be accomplished using the main server to verify customers, including a connecting hub. Additionally, consumers can share credentials or encryption keys to create a distributed system with peers.Tunnelling is a network infrastructure that allows one form of protocol packet to be encapsulated within the packet headers of another guideline[6].For instance, Windows VPN links may use the Point-to-Point Tunnelling Protocol (PPTP) packets to encompass and submit cellular network congestion, such as TCP / IP congestion over a secure network like the Internet.

MPLS VPN-Multi-Protocol Label Switching (MPLS) VPN is a versatile approach for transporting and routing various kinds of internet traffic use a backend of the MPLS.MPLS VPNs merge the capacity of MPLS with dynamic routing Border Gateway (BGP).

VPN TECHNOLOGIES

Tunnelling-A digital point-to-point link that is made over a secure network.It holds the encoded datagram.Most VPN's

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

depend on tunnelling to develop an internet-wide home network.Basically, tunnelling is the method of putting whole packets into another and forwarding them over the system[7]. Tunnelling is of two types Voluntary Tunnelling and Compulsory Tunnelling. Voluntary Tunnelling is the method of tunnelling in which the VPN linkage is configured.It is the tunnelling method where VPN Network Configuration is managed by the carrier network service.Many VPNs depend on Tunnelling to establish an internet-wide home network.Tunnelling is basically the process of inserting a whole packet inside another packet and dispatching it over a system.

Authentication-By design, VPN does not provide good protection for compliance. An authorized User should create a VPN connection. Most VPN applications provide minimal forms of verification as PAP used in PPTP, storing login details in plain text.

Access Control-Rather than connecting directly to the system it moves to the network databases first. VPN involves two tunnelling techniques for connecting consumer to business.

Data Security-A well-defined VPN uses many tactics to keep the link and information safe for users: Firewall, Authentication, IPSec and Authorization database. Users can configure firewall to restrict the number of channels, which packet forms are transmitted through and which parameters are forced to pass through.

VPN provides a means to access a stable, private, entire network over insecure corporate networks like the Web.Although it is possible to open and tunnel an encrypted communication stream through VPN via an unstable network, client-side protection should not be ignored. Virtual Private Network provides information in a public network with data security.

SECURITY PROTOCOLS

VPN provides a number of security protocols for enhancing the security of the network. The various security protocols are-

Internet Protocol Security (IPSec) -IPSec is among the most comprehensive, safe and available systems based on the data transport procedures created.This functions in the layer of the network.IPSec includes specifications that help to develop shared identification at the start of the session between the two negotiating entities and negotiate the encryption keys to use during the conversation[8].IPSec is a collection of safety protocols allowing the machine to select suitable safety protocols throughout data transfer. IPSec could be used to secure transmission of data among two servers and between routers or adapters.It utilizes several key protocols, including “Authentication Header, Encapsulated Security Payload, and Internet Key Exchange, to securely create a link and data transfer”.

- *Authentication Header*- Authentication Header (AH) method offers source node verification and information integrity. It doesn't deliver data encoding. All IP bundles are bundled in Authentication Header format. AH includes "hashed data, number of sequences, index of safety parameters, etc". The IPSec AH Header is shown below in Fig. 4 IPSec Header

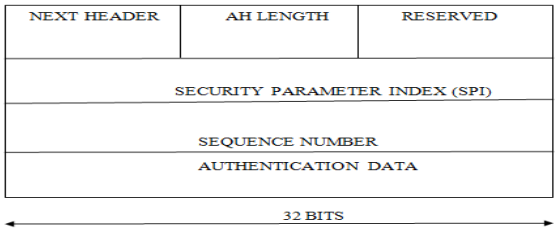

Fig.4: IPSEC AH Header

- *Encapsulated Security Payload (ESP)* - Encapsulated Security protocol offers several main features, including data privacy, data security, and source authentication. This utilizes techniques for key encryption to provide data protection and data security. The source and the recipient must use the same method for the encoding. All security protocols operate in two modes- Tunnel mode and Transport Mode.The function of the tunnel mode is also named as the end-to-end operating mode. A tunnel links two levels of a VPN around the backbone of the shared network. The tunnel parameters are growing VPN routers and the shared network framework in tunnel mode.The new IP header includes a "tunnel endpoint address."Once the encrypted data packet enters the endpoint of the tunnel, the location address is deciphered by the "endpoint of the tunnel”. The other term for transport mode is “host to host operation".
- *Point to Point Tunnel Protocol (PPTP)* -"Point to Point Tunnelling Protocol is a two-protocol OSI layer" built on top of the "Point to Point Protocol (PPP)".Through creating a virtual platform for each distant client, PPTP links to the target system[9].The PPTP control interface includes the PPTP request

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

command and monitoring communication used for the PPTP tunnel maintenance.Data packet encapsulation occurs in different levels in PPTP tunnelling.PPTP uses "Generic Routing Encapsulation (GRE)" to encompass PPP data blocks and communicates the embedded information like the Internet to the corporate network.In addition to data encapsulation, GRE also includes the traffic management and flow control frameworks.The "data frames" summed up with PPP are authenticated.Data packet formulation occurs in various levels in "PPTP tunnelling."The IP header includes the IP addresses for the source and the destination. When the PPTP data packet hits the PPTP database, the "IP header, GRE header, and PPP header are deleted from the data packet and the PPP data is decrypted". Fig.5 the figure shows the PPTP protocol.

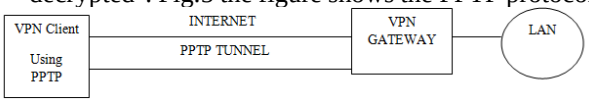

Fig.5: The Figure Portrays the PTPP Protocol

Layer 2 Tunnelling Protocols (L2TP) -L2TP is also run on the second layer of the Open System Interconnection model.One tunnel could permit multiple connections.The two layer tunnelling mechanism captures information in PPP layers and can distribute non-IP procedures over an IP system.L2TP links use the same methods of encryption as PPP links, like "EAP, CHAP and MSCHAP."In a PPP header and an L2TP header, the PPP information is embodied. A UDP header also encapsulates the embedded L2TP packet[10]. The final packet is encapsulated with an IP header containing the "VPN client and VPN server's" source and destination IP addresses.L2TP makes no private provision of information. It is therefore used in accordance with IPSec, and it is named "L2TP / IPSec".L2TP tunnelling is achieved by means of several encapsulation rates.The PPP information is embodied within the "PPP header and the L2TP header."

ADVANTAGES OF VPN

- VPN's have two major benefits, notably cost savings and usability.
- The lower price of the VPN by removing a need for costly brief-distance serviced lines.
- Regional serviced lines or even wireless connections are all you need to browse the web and use the public network to definitely tunnel the private association.
- Encrypted data exchanges.
- Low prices to incorporate.

DISADVANTAGES OF VPN

- VPN is slow to link.
- It is essential to have a strong understanding of information security problems and suitable measures before VPN deployment since the linkage moves across public routes.
- Stabilization of the VPN connection primarily controls the usability of the Web, factors beyond the power of the organisation.
- VPN technology differentiated. May not co-operate because of unintelligent norms.
- Bad equipment and small-speed user-end associations.

CONCLUSION

VPNs enable users or companies to communicate over a corporate network to individual computers, branches, or other businesses while retaining communications.In all such instances, the protected link acts as a secure communication channel to the user-despite the fact that this contact takes place over a shared internetwork.Virtual Private Network creates the information in a public network with safety and privacy.Institutions and multi-national companies make heavy use of such an innovation for their commercial activities.Virtual Private Network is expense-effective and offers powerful data transfer between networks.Virtual Private Network technology is created to solve problems surrounding the overall business pattern toward more enhanced remote working and broadly disseminated international operations, in which employees have to be able to link to central infrastructure and interact with each other. The paper gives a comprehensive overview on VPN, its types, various securities protocols, technologies enabling VPN followed by its advantages and disadvantages.

REFERNCES

[1] A. Vishwakarma, "Virtual private networks," in *Network Security Attacks and Countermeasures*, 2016.

[2] J. T. Harmening, "Virtual Private Networks," in *Computer and Information Security Handbook*, 2013.

[3] K. Lewis, "Virtual Private Cloud Security," in *Computer and Information Security Handbook*, 2017, pp. 937–942.

[4] K. K. Jyothi and B. I. Reddy, "Study on Virtual Private Network (VPN), VPN ' s Protocols And

Security," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 5, pp. 919–932, 2018.

[5] J. Gokulakrishnan, "A SURVEY REPORT ON VPN SECURITY & ITS TECHNOLOGIES," *Indian J. Comput. Sci. Eng.*, vol. 05, no. 4, p. 135, 2014.

[6] Z. Duan *et al.*, "Two-layer hybrid peer-to-peer networks," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 6, pp. 1304–1322, 2017.

[7] A. Alshalan, S. Pisharody, and D. Huang, "A Survey of Mobile VPN Technologies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016.

[8] D. Deshmukh and B. Iyer, "Design of IPSec virtual private network for remote access," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, 2017, vol. 2017-January, pp. 716–719.

[9] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta," *J. Matrik*, vol. 16, no. 2, p. 9, 2017.

[10] Y. qin Fan, C. Li, and C. Sun, "Secure VPN based on combination of L2TP and IPSec," *J. Networks*, vol. 7, no. 1, pp. 141–148, 2012.

[11] Gagandeep Singh Narula, Dr. Vishal Jain, Dr. S. V. A. V. Prasad, "Use of Ontology to Secure the Cloud: A Case Study", International Journal of Innovative Research and Advanced Studies (IJIRAS), Vol. 3 No. 8, July 2016, page no. 148 to 151 having ISSN No. 2394-4404.

[12] Gagandeep Singh Narula, Ritika Wason, Vishal Jain and Anupam Baliyan, "Ontology Mapping and Merging Aspects in Semantic Web", International Robotics & Automation Journal, having ISSN No. 2574-8092, Vol. 4, No. 1, January, 2018, page no. 01 to 05 .

[13] Gagandeep Singh Narula, Usha Yadav, Neelam Duhan and Vishal Jain, "Evolution of FOAF and SIOC in Semantic Web: A Survey", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under Big Data Analytics, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6619-1 page no. 253 to 263

[14] S. Balamurugan, K. Amarnath, J.Saravanan and S. Sangeeth Kumar, "Scheduling IoT on to the Cloud : A New Algorithm", European Journal of Applied Sciences 9 (5): 249-257, 2017.

[15] S.Balamurugan et.al., "Smart Healthcare: A New Paradigm", European Journal of Applied Sciences 9 (4), 212-218, 2017

[16] S.Balamurugan,R.Madhukanth,V.M.Prabhakaranand Dr.R.GokulKruba Shanker, "Internet of Health: Applying IoT and Big Data to Manage Healthcare Systems," International Research Journal of Engineering and Technology (IRJET), Volume 3 issue 10, pp.732-735,e-ISSN: 2395 -0056, p-ISSN: 2395-0072, 2016