Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

MANAGING ORGANISATION USING VPN's : A SURVEY

Aakanksha Pandey[1] , Saumyata Singh[2], Smriti Jaiswal[3]

[1]*Assistant Professor, Dept. of CSE, CEC Bilaspur (C.G.)*

[2]*BE Scholar, Dept. of CSE, CEC Bilaspur (C.G)*

[3]*BE Scholar, Dept. of CSE ,CEC Bilaspur (C.G)*

Abstract—The basic concept of a VPN is to connect networks in separate offices in such a way that makes them appear as a single network.The investigation of using peer-to-peer communication began due to the low performance of traditional, client-server based model. The bandwidth and latency of the communication between the connected clients , was improved by virtual private networks (VPN's). Thus a new peer-to-peer connection based VPN protocol was developed. It uses both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) communication to transfer Ethernet frames between the connected clients across IPv4 and IPv6 networks, and it makes direct communication for the clients possible. [1]

Keywords—TCP ,UDP ,LAN.

I. INTRODUCTION

The spread of VPN connections instead of direct dial-up or leased line connections is because of the now-a-days the high speed Internet connections became inexpensive and reliable and make corporate networks accessible for the employees anywhere using a single Internet connection by connecting offices in different parts of the world. They also help reserving the remaining IPv4 address space by making computers accessible without public IP addresses; they are still not practical for real-time, delay or speed sensitive applications. Like online games, video streaming, and file sharing services are just a few of the numerous protocols that through current point-to-point virtual private network protocols are not accessible; however, recently many applications of peer-to-peer technologies proved to be efficient, fast and reliable. It is possible to create faster VPN networks by combining peer-to-peer technologies with VPNs.

In a packet switching (packet-based) network, includes network resources made up of networked elements and customer premises equipment that are interconnected by one or more physical paths, a Virtual Private Network (VPN) is built above this underlying packet-based network and the selected portions of the packet-based network resources are included within it.

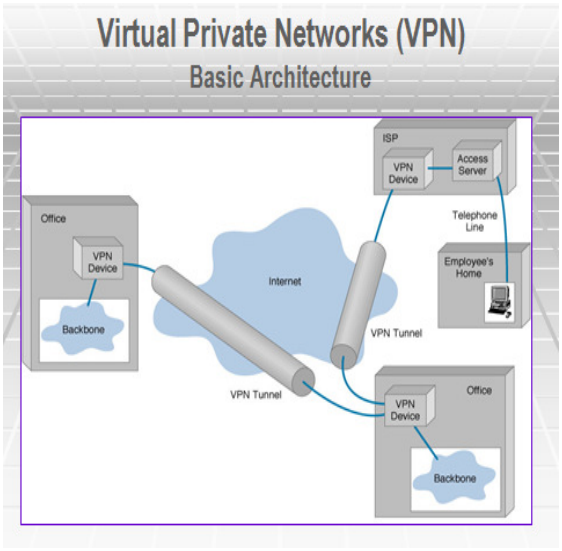

Fig. 1. Basic Architecture of VPN

Peer-to-Peer Communication

A peer-to-peer (P2P) network have equally privileged participants. The servers and clients are not clearly differentiated in the communication. They both provide and consume resources similarly. There are several uses of this type of network as Voice over IP, file sharing etc.

Two types of end points:

1. Remote Access
2. Site-to-Site

Remote Access

The connections between mobile or remote users and their corporate networks are encrypted and user in remote areas can easily make a local call to an ISP. VPN is ideal for a telecommuter or mobile sales people as it allows them to take advantage of broadband connectivity that is. DSL, Cable

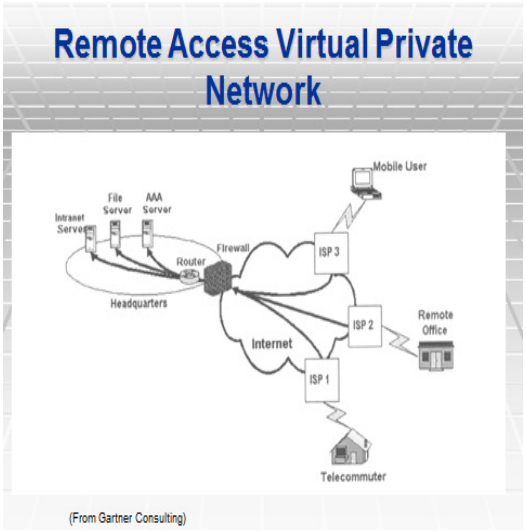

Fig. 2.Remote Access VPN

Site-to-Site VPNs

Site-to-Site VPNs are fixed sites such as remote offices and central offices. Network traffic is sent over their branchoffices and Internet connection .The company hardware and management expenses are saved upto some extent by this.

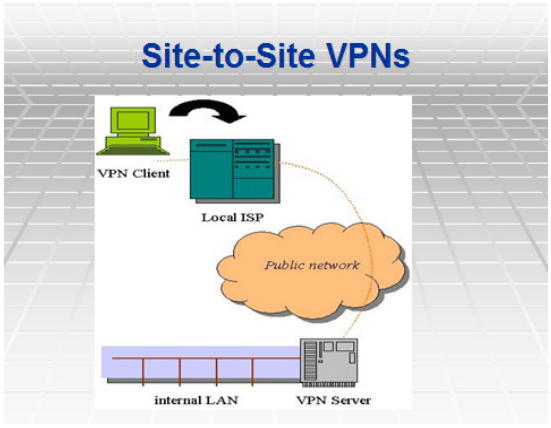

Fig. 3.Site-to-Site VPN

II. LITERATURE REVIEW

Computer networking has grown explosively. Since the 1970s, computer communication has changed from an esoteric research topic to an essential part of the infrastructure. The use of Networking is in every aspect of business, that includes advertising, production, shipping, planning, billing ,and accounting. Consequently, most corporations have multiple networks. Schools, at all grade levels are using computer networks from elementary through post-graduate, to provide students and teachers an instantaneous access to the online information. From Federal, state, and local government offices use networks, so as do military organizations. In short, computer networks are everywhere. [2]

By Modern computer networks data is handled in form of small data blocks that are called *packets*. The name of this method is *packet switching*. The data is moved towards its destination through different networks by using the address provided to it after encapsulating it in a packet. This method of Packet switching can be connection less and connection-oriented.

IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet every device including computers, smartphones and game consoles that connects to the Internet requires an address hence it is expected that the number of unused IPv4 addresses will eventually run out. [3]

The successor of IPv4 is IPv6, which is incompatible with the IPv4. IPv6 has a larger, 128b address space, and numerous new features compared to IPv4 ("RFC 2460", 1998). It drops the support for fragmentation. If a packet is simply dropped by the routers if it is too big to be transmitted through a network segment. It simplifies the routing process. IPv6 is also more secure, and provides better support for multicasting.

TCP is a connection oriented stream over an IP network. It guarantees transmission of all the packets to the destination in the correct order. This uses acknowledgement packets that are sent back to the sender, and automatic retransmission, which causes additional delays and a general less efficient transmission than UDP but TCP guarantees reliable transmission.

UDP is a connection-less protocol and communication through this is datagram oriented. The integrity is guaranteed only on the single datagram. Datagrams reaches to their destination and can arrive out of order or don't arrive at all. Since it uses non ACK IT is more efficient than TCP. Hence it does not guarantees a reliable transmission. It's generally used for real time communication, where quick transmission is required rather than reliable. [4]

Virtual Private Networks

The aim of a virtual private network is to provide a computer network that uses an existing computer network infrastructure and provides a secure access to a network. There are many different uses of VPNs;

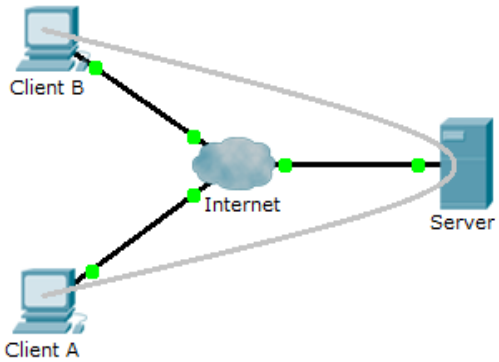

Fig.4. A typical VPN topology

A typical VPN topology is mentioned in which both of the clients are connected to the Internet, but all the VPN traffic is going through a single server. [1]

To satisfy the need for a less expensive way to interconnect corporate networks than leased or owned lines virtual private networks were created. This is because the original purpose of the VPN development was to replace leased or owned lines. Typically a point-to-point topology is used in VPN's; currently individual computers are also connected using VPN's.

There are various VPN Tunnelling Protocols that enables the encapsulation of a packet from one type of protocol into the datagram of a different type of protocol. Some of them are as follows:

1. PPTP VPN
This is the most common and widely used VPN protocol. By using the existing Internet connection this protocol enables the authorized remote users to connect to the VPN network and then log on to the VPN with the help of a password.
2. SITE-TO-SITE VPN
It allows different sites of the same organization to connect together to form a VPN with its own real network.
3. L2TP VPN
It provides data confidentiality and also data integrity. [5]

All the three protocol mentioned above depend heavily on the features originally specified for Point-to-Point Protocol (PPP) which was originally designed to send data across dial-up or dedicated point-to-point connections. PPP encapsulates IP packets within PPP frames and then those encapsulated PPP-packets are transmitted across a point-to-point link.

A frequently used protocol for VPNs is PPTP (Point-to-Point Tunneling Protocol), which encapsulates PPP (Point-to-Point Protocol) connections ("RFC 2637", 1999). For connecting a client to a VPN, at first we have to make PPTP connection and then this connection is used for creating the actual network connection by tunneling PPP through the PPTP connection. This protocol was simple to implement as PPP was already supported by most operating systems and devices. The PPTP is compatible with existing software and devices as any PPP traffic can be transferred transparently through a PPTP tunnel.

PPTP can be used with a variety of Microsoft clients such as Microsoft Windows 2000, Windows XP, Windows Vista, and Windows Server 2008. There is no use of a public key infrastructure (PKI) in PPTP. By using encryption, PPTP-based VPN connections provide data confidentiality (captured packets cannot be interpreted without the encryption key). PPTP-based VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user). [6]

PPTP has been the subject of many security analyses and serious security vulnerabilities have been found in the protocol. The known vulnerabilities relate to the underlying PPP authentication protocols used, the design of the MPPE protocol as well as the integration between MPPE and PPP authentication for session key establishment.[1]

III. CONCLUSION

At present the "Virtual Private Network (VPN)" has emerged as one of the leading technologies and many organizations looking to expand their networking capabilities and reducing their costs are attracting towards this technology. This project deals with the upcoming technology, VPN - Virtual Private Network and it has been proved that VPN provides reliable transferring of data between

remote places via a secured network hence it is paving the way for Data Security. The connection between the user (client) & the server of the organization not within the workplace itself but from home too is provided along with the data being transferred & received in a highly secured way with the help of creating VPN. The two parties exchanging information are really who they claim to be is guaranteed by Digital certificates that are used in Network Security. With the help of this certificate authority keeps a complete list of all the certificates issued by it along with the information on their status: valid, expired, or revoked.

REFERENCES

[1]. Daniel Kasza,"Virtual Private Network Using Peer-to-Peer Techniques".

[2]. Douglas E. Comer, " Introduction and Overview ", Computer Networks and Internets, Fifth Edition, Pearson Education, Upper Saddle River, New Jersey.2009

[3]. Traditional IP Network Address Translator (RFC 3022). (2001). Retrieved November 15, 2010, from http://datatracker.ietf.org/doc/rfc3022/

[4] . Managing Cisco networking security, Michael J. Wenstrom, Cisco Press, Indianapolis, IN 46290 USA

[5]. "www.techpp.com/Different types of protocals"Retrieved on 2 november 2014

[6]. P. Ruth, J. Rhee, D. Xu, R. Kennell, and S. Goasguen. Autonomic live adaptation of virtual computational environments in a multi-domain infrastruc-ture. In ICAC '06: Proceedings of the 2006 IEEE International Conference on Autonomic Computing, Washington, DC, USA, 2006.

[7]. "Microsoft says don't use PPTP and MS-CHAP"

[8]. P. Ruth, J. Rhee, D. Xu, R. Kennell, and S. Goasguen. Autonomic live adaptation of virtual computational environments in a multi-domain infrastruc-ture. In ICAC '06: Proceedings of the 2006 IEEE International Conference on Autonomic Computing, Washington, DC, USA, 2006.

[9]. Basics of VPN ,Retrieved on 2 November 2014, "www.topnettricks.com"

[10].How VPN works, Retrieved on 30 october 2014 , "www.howtogeek.com".

[11]. A primer for Implementing a Cisco Virtual Private Network. (1999). Cisco System. Retrieved October28,2002 http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm.

