ISSN: 2321-8169
409 – 413

A Survey of VPN Performance Evaluation

Avani J.Patel
Dept. of Computer engineering
PIET, Parul University
Vadodara, India
anu301093@gmail.com

Ankita Gandhi
Assistant Prof.Dept.of.CSE
PIET, Parul University
Vadodara, India
anki.gandhi@gmail.com

***Abstract*—** Virtual Private Network (VPN) is commonly used in business situations to provide secure communication channels over public infrastructure such as Internet. A VPN operates by passing data over the Internet or corporate intranet through "tunnels" which are secure, encrypted virtual connections that use the Internet as the connection medium[13].The VPN establishes tunnels between servers in a site-to-site VPN, clients and servers in a client-to site VPN[13]. VPN is a technology that does provide security strong enough for business use. However, performance of these networks is also important in that lowering network and server resources can lower costs and improve user satisfaction.VPN have many protocols PPTP, L2TP, IPSec for the performance and security. In this research we evaluate performance of VPN using IPSec (Internet Protocol Security). IPSec is a framework for a set of protocols and algorithms for security at the network layer by authenticating and encrypting each packet between two IPSec gateways (GWs).So IPSec protocol is better than the other protocol it give better performance than the other protocol.

Keywords- *VPN; performance evaluation; IPSec; PPTP; L2TP; SSL*

*****

I. Introduction

In past, organizations would physically install cable over large distances to ensure secure data transfer. However, this system is impractical for every enterprise and everyday users due to the cost, space, and time required for such installations [1]. Most private networks have lack data security and allow hackers to have access to read and attack the data directly. A VPN shares a network that data can be passed through the private traffic in the way that only authorized users have access it [16].

A virtual private network (VPN) is a network that uses internet as its wan link. A VPN is a type of private network that uses public telecommunication. That provides remote access to an organization's networks via the internet instead of using lines to communicate [14]. VPN is a concept that proven cost effective technology for securing data that traverses over large distances[4].

A VPN operates by passing data over the Internet or corporate intranet through "tunnels" which are secure, encrypted virtual connections that use the Internet as the connection medium. The VPN establishes tunnels between servers in a site-to-site VPN, and between clients and servers. The VPN encrypts and encapsulates each IP packet before passing it through a tunnel. The encapsulated packet includes authentication information to ensure the authenticity of the data and source. The VPN also uses the authentication information to check that original data has not been corrupted during transmission, ensuring the integrity of the data [13]. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure [15].

II. VPN ARCHITECTURE

Virtual Private Network (VPN) is the traditional approach for an end-to-end secure connection between two endpoints [17]. And VPNs can be defined as a way to provide secure communication between members of a group through use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures [3].

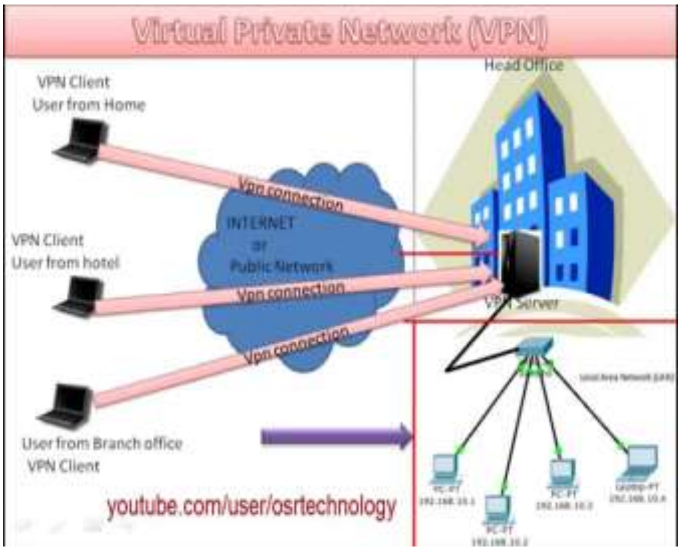

Fig. 1.VPN Architecture

Virtual Private Network (VPN) connections establish secure connections between a remote user and a home network by encrypting packets sent though the Internet rather than building a true private network [17].

The main purpose of a VPN is to give enterprises the same capabilities, or even better in some cases as the list below shows, as in private networks, but at a much lower cost[1].

Virtual Private Networks (VPN) has become an inexpensive methodology to secure connections between network sites that exist at different geographic locations. Virtual Private Network (VPN) is one of the most reliable technologies to provide data protection, confidentiality, integrity, data origin authentication, replay protection and access control [18]. It is an alternative to owning or leasing expensive communication lines and provides same capabilities as dedicated connections, but at a fraction of the cost. VPN technology may use shared public network infrastructure in part of its implementation and can use various tunnelling protocols to encrypt and authenticate data as it moves between different locations [5].

III. VPN DEVICES IN VPN ARE FURTHER DIIDED IN TO THREE CATEGORIES

A. Hardware

A hardware VPN is a virtual private network (VPN) based on a single, stand-alone devices. The device, which contains a dedicated processor, manages the authentication, encryption, and other VPN functions and provides hardware firewall. Hardware VPN's provides more and more security than compared to firewall programs for the small and home business computers. But hardware VPN is more expensive than software VPN. Because of the cost, hardware VPN's are a most realist option for large business than for small business or branch offices. Several vendors offer devices that can function as hardware VPN's.

B. Firewall

A firewall is a set of hardware and software that handles the access control to the company network [20]. You can set firewalls to restrict the number of open ports, what types of packets are passed through and which protocols are allowed through. A firewall approach is still relatively costly [6]. The function of a firewall is to allow a company's network to use the Internet while preventing intruders from accessing the network from the Internet. This allows companies to have secure networks that can interface with the more chaotic Internet. Firewalls used in the establishment of electronic commerce. There are two types of firewalls, packet level and application level firewalls [20].

C. *Software*

Software is collection of instruction that enables user to interact with the hardware. The most important advantage in software approach is that user's network doesn't change. Also extra devices are not needed to be installed, and management of the network remains the same. However, one point to consider when adding software to existing hardware is performance. VPN tunnelling and encryption tasks will be carried out in software, taking CPU cycle from other processes [6].

D.Tunnels

In tunnelling process wrap the data packets into other data packets and encrypt the package and sent through the tunnel. A VPN tunnel perform some operation known as encapsulation.Tunneling or encapsulation, is a technique of packaging one network packet inside another. The encapsulated packet is called the tunnelled packet and the outer, encapsulating the packet is called the transport packet.

IV. VPN SECURITY

Security is the most important and critical factor for companies worldwide. Organizations need a secure and reliable infrastructure for their systems to mitigate the risk of malicious activity from both external and internal sources [20].VPN provide encryption and data confidentiality. Once connected, the VPN use the tunnelling mechanism described above to encapsulate encrypted data into a secure tunnel.

Secure VPNs have more than one tunnels and each tunnel has two ends points, sender and the receiver. The sender and the receiver accept and agree upon the security properties of the tunnel [20]. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not changed in any way during transmission. It also provides a data integrity check. By default, VPN does not provide strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. So Outsider cannot change, add or delete data on a path in VPN[20]. Nevertheless, VPN does support adds on authentication mechanisms, such as smart cards, tokens and RADIUS.

V. VPN PROTOCOLS

A. PPTP

PPTP is a standard tunnelling protocol developed by PPTP Forum which consists of Microsoft and some other remote access vendors. The Point-to-Point Tunnelling Protocol (PPTP), developed by Microsoft, is the most widely supported VPN method among Windows users [19]. Basically uses the same types of authentication as PPP (PAP, SPAP, CHAP, MS-CHAP) [19] which encapsulates PPP frames in IP datagram for transmission over an IP-based network, such as the Internet or over a private intranet [1]. In the data link layer PPTP, which is used to make secure tunnel for exchanging information, is one way to implement the so called VPN [11].

The secure communication created using this protocol typically involves three stages; each has to be completed prior to the next. Firstly, a PPTP client uses a PPP type connection to establish a link through the transit network from the source to the destination. Once this is established, the PPTP protocol creates a control connection from the client to the PPTP server. This connection uses TCP to establish connection. And finally, PPTP protocol creates IP datagram containing encrypted PPP packets which are transported through the tunnel. Thus, by design PPTP has a very simple mechanism [4]. PPTP establishes the tunnel, but does not provide Encryption.PPTP has relatively low overhead, making it the fastest among the various VPN methods.

B.L2TP :

Asynchronous Transfer Mode, Frame Relay and X.25 networks use L2TP as tunnelling protocol for data transmission between the communicating nodes. L2TP is also operated at the layer 2 of OSI architecture.[20].Layer Two Tunnelling Protocol (L2TP) is an extension of the Point-to-Point Tunnelling Protocol (PPTP) used by an Internet service provider to enable the operation of a VPN over the Internet. One tunnel can allow multiple connections. Layer two tunnelling protocol encapsulates data in PPP frames and is capable of transmitting non-IP protocols over an IP network [20].

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The PPP data is encapsulated within a PPP header and an L2TP header. The encapsulated L2TP packet is further encapsulated in a UDP header. The final packet is encapsulated with an IP header containing the source and destination IP addresses of the VPN client and VPN server [20].

C.IPSEC:

IPSec is one of the most complete, secure, and accessible standards based on developed protocols for data transportation [20]. It operates in the network layer [20]. IPSec is an open standard framework developed by Internet Engineering Task Force that can be implemented for establishing VPN tunnels through the use of cryptographic security services [2]. IPSec is a collection of security protocols that allows the system to choose the appropriate security protocols during data transmission [20].

IPSec is an OSI Layer 3 protocol that supports network-level and provides authentication, data integrity, and data confidentiality and replay protection [2]. IPSec suite for securing IP communications [12].IPSec has a set of cryptographic protocols for two purposes: securing network packets and exchanging encryption keys. IPSec the preferred protocol [1].

IPSec have two encryption Transport and Tunnel. Transport mode encrypts payload of each packet. This mode is used to secure communication within a network. The more secure tunnel mode encrypts both the header and the payload. IPSec has two protocols that is enables it to provide packet level security: Authentication Header (AH) and Encapsulating Security Payload (ESP). IPSEC provides packet level data confidentiality through encryption via ESP and it also provide packet-by-packet host-level authentication via ESP or AH (Authentication header Protocol).

D.SSL: SSL is a VPN technology that is commonly used with Web browsers to give users a seamless secure connection. SSL can also be used to create VPN tunnels. It protects data using encryption and uses hashing to ensure integrity. Establishing a VPN using SSL involves three basics phases: firstly, SSL client and the server negotiate cipher suits. It determines the ciphers to be used, the key exchange and authentication algorithms, as well as the Message Authentication Codes .Then encryption keys are exchanged and client and the server are authenticated using the chosen algorithm, and finally encrypted message is created and sent between the two nodes involved. The MAC used in the process is made up from cryptographic hash functions [4].

V. SURVEY OF VPN PROTOCOLS

	PPTP	L2TP	IPSec
VPN encryption	128-bit	256-bit	256-bit
VPN app supported	Widows Mac ios	Windows Mac ios	Windows Mac ios android
VPN SPEED	Fast due to lower level of encryption.	Relatively slow as it requires more CPU processing.	Require more CPU processing to encapsulate data twice.
VPN security	Standard encryption. The security is minimum but better than doing without VPN.	Highest encryption. Verifies Data integrity by checking twice.	Highest encryption. Checks data and encapsulates the data twice.
Ports used	PPTP uses TCP port 1723 and GRE protocol 45	L2TP uses UDP ports 1701 and ESP protocol 50	UPD port 500

VI. BENEFITS OF VPN

- **Cost efficient** – VPNs reduce the cost of operation by eliminating the need for long-distanced leased lines. Cost cutting in telephone charges is also made possible by using VPN connection.
- **Enables easy inter-networking** – VPNs are also used to bridge different networks together. Creation of an extended intranet can be easily done using VPNs, by joining several different networks together.
- **Enhanced security:** By using theVPN data is kept secured and encrypted. In this way the information is away from hackers' eyes.
- **Accessing blocked websites and bypassing filters** – VPNs are known for bypassing internet filters. Blocked websites are easily accessible through a VPN. VPN's ability to bypass geographical filter and web restrictions has made it a preferred choice in countries where heavy censorship is practiced [20].
- **Better performance** – Some VPN providers provide you with better bandwidth and efficiency via your network. Some VPNs provide you the option to choose your preferred server location. Choosing a secure server located nearby, helps you to enhance the performance of the network as a whole [20].
- **Change IP address**. If you need an IP address from another country, then a VPN can provide you this.
- **Better performance**. Bandwidth and efficiency of the network can be generally increased once a VPN solution is implemented.

VII. LIMITATIONS OF VPN

- **Speed limitations** – The speed of a VPN is dependent upon the server location. If the server through which connection is being made is fast and reliable, then it ensures good speed. Unfortunately, most of the free servers are slow and sluggish.
- **Compatibility issues** – VPNs from different clients have compatibility issues due to which they may not work well together.
- **Complexity** – VPNs are complex compared to other methods of using a similar service. Using a VPN requires a certain level of technical knowledge. Knowledge about networks is also important to fully understand the way VPNs function.VPN connection is slow.
- **Performance and reliability** -Performance and reliability of the VPNs that are internet based will not be directly controlled by the organization. The solution will always rely on the ISP and the service quality offered [20].

VIII. PROPOSED WORK

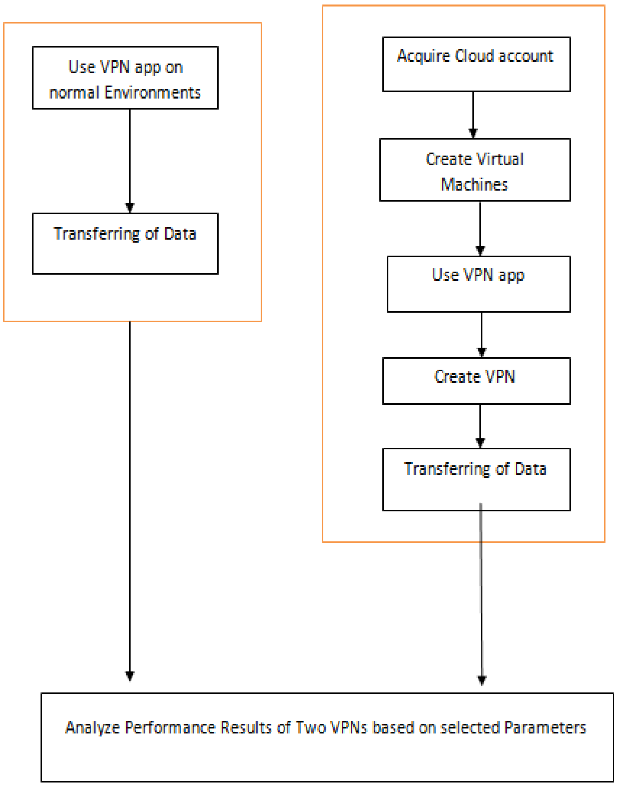

FIG 2. Propose work

- In our Proposed work we will going to do the following things:
- Implementation of VPN in normal LAN using various old and latest Operating Systems. Analyze data on different parameters.
- Implementation of VPN in cloud using various Operating Systems available on cloud. Analyze data on different parameters.
- Performance Analysis between VPN and VPN in CLOUD based on Parameters viz.
- Throughput
- With different OS
- Different Transmission speed
- Increased in Number of Devices

VIII. CONCLUSION

In this paper we saw virtual private network information. It is very efficient to secure users private information. It protects user's information from the intruders. And VPN technology is a very cost effective technology. And also this technology is easy to use. In this paper VPN protocols are defined. Defined protocols are used in this technology. Protocols have own different strength. There are some VPN protocols like PPTP, L2TP, IPSec and SSL. Protocols use different ports. And also provide Encrption.VPN protocols have different speed and security. By this survey we can say that the all protocol give different performance. Also we can say that the IPSec protocol is better than the other protocols.

References

[1] Joha, Ahmed A., Fathi Ben Shatwan, and Majdi Ashibani. "Performance evaluation for remote access VPN on windows server 2003 and fedora core 6." Telecommunications in Modern Satellite, Cable and Broadcasting Services, 2007. TELSIKS 2007. 8th International Conference on. IEEE, 2007.

[2] Narayan, Shaneel, et al. "Performance evaluation of virtual private network protocols in Windows 2003 environment." Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on. IEEE, 2008.

[3] Jaha, Ahmed A., Fathi Ben Shatwan, and Majdi Ashibani. "Proper virtual private network (VPN) solution." Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on. IEEE, 2008.

[4] Narayan, Shaneel, Kris Brooking, and Simon de Vere. "Network performance analysis of vpn protocols: An empirical comparison on different operating systems." *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on*. Vol. 1. IEEE, 2009.

[5] Narayan, Shaneel, Michael Fitzgerald, and Shiu Ram. "Empirical network performance evaluation of IPSec algorithms on windows operating systems implemented on a test-bed." Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on. IEEE, 2010

[6] Chowdhury, NM Mosharaf Kabir, and Raouf Boutaba. "A survey of network virtualization." *Computer Networks* 54.5 (2010): 862-876.

[7] AlZain, Mohammed A., et al. "Cloud computing security: from single to multi-clouds." System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, 2012.

[8] Liao, Wen-Hwa, and Shuo-Chun Su. "A dynamic VPN architecture for private cloud computing." Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on. IEEE, 2011.

[9] International Conference on. IEEE, 2012 Arshad, Fahad A., Gaspar Modelo-Howard, and Saurabh Bagchi. "To cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network." Network Protocols (ICNP), 2012 20th IEEE.

[10] International Conference on. IEEE, 2012 Arshad, Fahad A., Gaspar Modelo-Howard, and Saurabh Bagchi. "To cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network." Network Protocols (ICNP), 2012 20th IEEE.

[11] Shrivastava, Anupriya, and M. A. Rizvi. "External authentication approach for virtual private network using LDAP." Networks & Soft Computing (ICNSC), 2014 First International Conference on. IEEE, 2014

[12] Yu, Liang, et al. "An ipsec seamless switching mechanism with high availability and scalability by extending ikev2 protocol." (2011): 25-29.

[13] Ahamed, SS Riaz, and P. Rajamohan. "Comprehensive performance analysis and special issues of Virtual Private Network strategies in the computer communication: A novel study." International Journal of Engineering Science and Technology 3.7 (2011).

[14] Chowdhury, NM Mosharaf Kabir, and Raouf Boutaba. "A survey of network virtualization." Computer Networks 54.5 (2010): 862-876.

[15] Rajamohan, Dr P. "Performance analysis and special issues of VPN technologies in communication: Trusted vpns, secure vpns, and hybrid vpns." IIJCS, July (2014).

[16] Mohamed, M. A., M. E. A. Abou-El-Seoud, and A. M. El-Feki. "A Survey of VPN Security Issues." International Journal of Computer Science Issues (IJCSI) 11.4 (2014): 106.

[17] Alshalan, Abdullah, Sandeep Pisharody, and Dijiang Huang. "A Survey of Mobile VPN Technologies." IEEE Communications Surveys & Tutorials 18.2 (2016): 1177-1196.

[18] Uskov, Alexander V. "Information security of mobile VPN: Conceptual models and design methodology." In Electro/Information Technology (EIT), 2012 IEEE International Conference on, pp. 1-6. IEEE, 2012.

[19] Yadav, Aakanksha. "SECURITY STRUCTURE OF VPN: A SURVEY."

[20] GOKULAKRISHNAN, JAYANTHI, and DR V. THULASI BAI. "A SURVEY REPORT ON VPN SECURITY & ITS TECHNOLOGIES." Indian Journal of Computer Science and Engineering (IJCSE) 5.4 (2014): 3-5.

[21] http://vpngenic.com/pros-and-cons-of-using-a-vpn/