Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

A survey on performance evaluation of VPN

Avani J. Patel[1], Ankita Gandhi[2],

[1] *Computer Engineering, Parul Institute of Engineering and Technology, Parul University*
[2] Assistant Professor, *Parul Institute of Engineering and Technology, Parul University*

Abstract — *Virtual Private Network (VPN) is commonly used in business situations to provide secure communication channels over public infrastructure such as Internet. Virtual Private Networks (VPNs) provide a secure encrypted communication between remote networks worldwide by using Internet Protocol (IP) tunnels and a shared medium like the Internet. 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.*

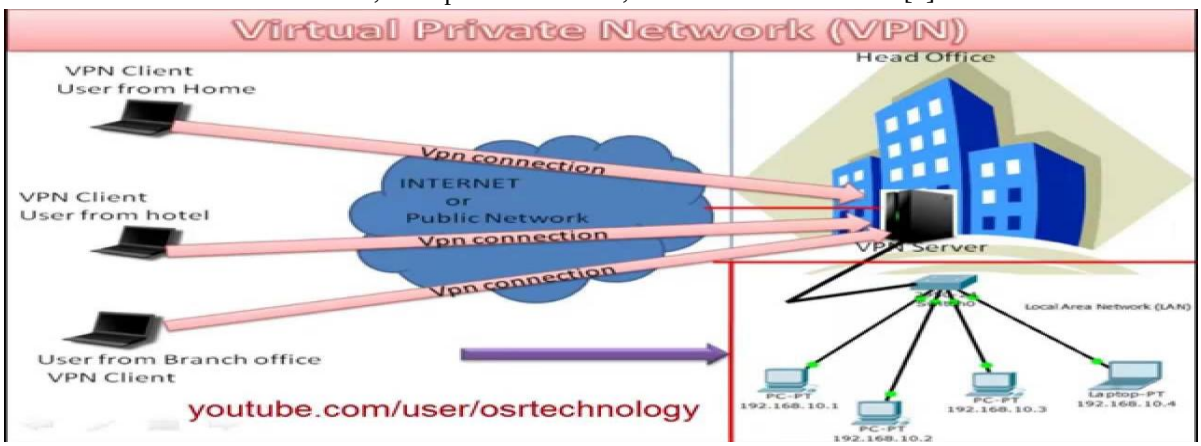
Keywords— *VPN, performance evaluation, IPSec, PPTP, SSL*

I. INTRODUCTION

In the 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] Direct connected VPN usually allows for a small scale of secure connections into a private network over the public network. [8] VPN is a concept that proven cost effective technology for securing data that traverses over large distances.[4] with the exponential growth of the Internet, telecommunications has changed and the Internet has become part of almost every aspect of the developed world including education, banking, business, and politics. Over the past two decades the public Internet has been found to be vulnerable to attackers seeking sensitive information. The most recent solution to this problem has been IP baseVPN.[1]VPN maintaining privacy through the protocols.[3].so To enable secure access to sensitive resources a virtual private network (VPN) is almost a required piece of technology.[9] To implement VPN, there are numerous protocols and products available on the market, each have their own capabilities and features. Three protocols that are frequently used with operating systems are IPSec, PPTP and SSL. These provide encryption and integrity to data in transition.[4]

II. VPN ARCHITECTURE

A Virtual Private Network (VPN) 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] 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. 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 tunneling protocols to encrypt and authenticate data as it moves between different locations.[5]

VPN DEVICES Devises in VPN are further divided into 3 categories as:

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 well designed VPN are several methods for keeping your connection and data secure. 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]

C. Software

The main advantage in software approach is that user's network does not change. No extra devices are 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 tunneling and encryption tasks will be carried out in software, taking CPU cycle from other processes.[6]

III. VPN SECURITY

VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission. VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission. By default, VPN does not provide or enforce 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. Nevertheless, VPN does support adds on authentication mechanisms, such as smart cards, tokens and RADIUS.

IV. VPN PROTOCOLS

A. PPTP

PPTP is a standard tunneling protocol developed by PPTP Forum which consists of Microsoft and some other remote access vendors. Basically, PPTP is an extension of PPP, 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]

B. L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the

PPP stream.L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The user has an L2 connection to an access concentrator, which then tunnels individual PPP frames to the NAS, so that the packets can be processed separately from the location of the circuit termination. This means that the connection can terminate at a local circuit concentrator, eliminating possible long-distance charges, among other benefits. From the user's point of view, there is no difference in the operation. [1]

C. IPSEC

IPSec is an open standard framework developed by Internet Engineering Task Force (IETF) that can be implemented for establishing VPN tunnels through the use of cryptographic security services.[2] It is for securing traffic on the network layer.[1] IPSec is an OSI Layer 3 protocol that supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality and replay protection.[2]. IPSec is a protocol suite for securing IP communications [12]. It does not specify the authentication and encryption protocol to use. This makes it flexible and able to support new authentication and encryption methods as they are developed [1] IPSec has a set of cryptographic protocols for two purposes: securing network packets and exchanging encryption keys. IPSec the preferred protocol [1] there are two encryption modes in which IPSec can be implemented: Transport and Tunnel. Transport mode encrypts only the data portion (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 (Encapsulating security protocol) 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 (MAC).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. BENEFITS OF VPN

- **Enhanced security.** When you connect to the network through a VPN, the data is kept secured and encrypted. In this way the information is away from hackers' eyes.
- **Remote control**. In case of a company, the great advantage of having a VPN is that the information
- **Share files** A VPN service can be accessed remotely even from home or from any other place. That's why a VPN can increase productivity within a company.
- **Share files**. A VPN service can be used if you have a group that needs to share files for a long period of time.
- **Online anonymity**. Through a VPN you can browse the web in complete anonymity. Compared to hide IP software or web proxies, the advantage of a VPN service is that it allows you to access both web applications and websites in complete anonymity.
- **Unblock websites & bypass filters**. VPNs are great for accessing blocked websites or for bypassing Internet filters. This is why there is an increased number of VPN services used in countries where Internet censorship is applied.
- **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.
- **Reduce costs**. Once a VPN network is created, the maintenance cost is very low. More than that, if you opt for a service provider, the network setup and surveillance is no more a concern.

VI. LIMITATIONS OF VPN

- VPN connection is slow.
- Because the connection travels over public lines, a strong understanding of network security issues and proper precautions before VPN deployment are necessary.

- VPN connection stability is mainly in control of the internet scalability, factors outside an organization control.
- Differing VPN technology. May not work together due to immature standards.
- 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.

VII. 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

CONCLUSION

In this paper we saw that what virtual private network is. It is very efficient to secure users private information. It securesusers information from the intruders. And it is a very cost effective technology. And also virtual private network technology is easy to use. In this paper the virtual private network protocols are defined. Their some protocols which are used in this technology. Protocols have own different strength. There are some VPN protocols like PPTP, L2TP, IPSec. Protocols use different ports. And also provide Encrption.VPN protocols have different speed. 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] Coonjah, Irfaan, Pierre Clarel Catherine, and K. M. S. Soyjaudah. "Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment." Computing, Communication and Security (ICCCS), 2015 International Conference on. IEEE, 2015.

[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.

