A Survey on Performance Evaluation of VPN on various Operating System

[1]Sneha Padhiar, [2]Pranav Verma
[1]ME Research Scholar, [2]Assistant Professor
[1] Department of Computer Engineering,
[1] SOCET, Ahmedabad. INDIA

***Abstract* - VPN is a proven technology that does provide security strong enough for transmission use. However, performance of VPN networks is also important because, the choice of VPN protocol and algorithm affect the network performance of different Operating Systems by different amounts. This paper provides a survey report on performance of three operating systems viz. Windows 2003, Windows Vista, Linux Fedora; on a test-bed set-up and observation of their network performance with different VPN tunnel protocols and algorithms. It is found that the all operating systems give different performance metrics values. We will see various experimental implementations and discuss their results in conclusion.**

***Keywords* - VPN, Tunneling, IPsec, PPTP, SSL, L2TP, Performance evaluation**.

I. INTRODUCTION

Internet has become the default communication channel for businesses, therefore the ultimate challenge for network designers is to provide IT infrastructure that guarantees efficient and secure delivery of data. A Virtual Private Network (VPN) is a private data network which uses the public telecommunication infrastructure, it maintains privacy through the use of tunneling protocol and security procedure [1]. Idea behind VPN is providing secure connection between organization and its branches via low-cost lines using internet [1][2]. A VPN operates by passing data over the internet through “Tunnels” which are secure ,encrypted virtual connections [1]-[5]. VPN uses various security protocols for Tunneling they are:-

- Internet Protocol Security(IPSEC)
- Layer2 Tunneling Protocol(L2TP)
- Point to point tunneling Protocol(PPTP)
- Secure Sockets Layer(SSL)

IPSEC:

IPsec provides authentication of users, encryption of data and data integrity during the data transmission between senders and receivers [2]. It uses three primary protocols which are Authentication Header (AH), Encapsulated Security Payload (ESP), and Internet Key Exchange (IKE). These are used in establishing connection and transmitting data in secure way [2]. There are two encryption modes in which IPsec can be implemented [2]-[4].

- Transport Mode
- Tunnel Mode

Transport mode encrypts only data portion (Payload) of packets. Tunnel mode is more secure which encrypts both header and payload [2][3].

L2TP:

L2TP tunneling is accomplished through multiple levels of encapsulation. PPP data is encapsulated within a PPP header and an L2TP header. Then L2TP packet is further encapsulated in a UDP header. Final packet is encapsulated within IP header [2][3][6].

PPTP:

PPTP is an OSI Layer2 protocol which is an extension of point-to-point protocol (PPP).It creates IP datagrams which containing encrypted PPP packets. which are transported through the tunnel. By design PPTP has a very simple mechanism [2][3].

SSL:

SSL is used with web browsers to give users a seamless Connection. It protects data using encryption and uses hashing to ensure Integrity [3][4].

The rest of paper is organized as follows: Section II is dedicated to the related work of literature. In section III Experimental finding results are given. Conclusion is discussed in Section IV. Future scope are described in section V.

II. RELATED WORK

The purpose of a VPN is to give an organization the same capabilities as private leased lines at much lower cost by using the shared infrastructure.

Rajamohan [1] has presented a detail terminology and technologies of VPN. There are three important VPN technologies. Trusted VPNs, Secure VPNs, Hybrid VPNs [1] [2]. **Trusted VPNs**: VPN customer trusted the VPN provider to maintain the integrity of the circuits and to use the best available business practices to avoid snooping of the network traffic. **Secure VPNs**: Networks are constructed using encryption even if an attacker is able to sniff from the traffic, he cannot read it. **Hybrid VPNs**: New type of trusted VPN in which a secure VPN can be run as part of a trusted VPN [1][2].

VPN is a proven technology that does provide security strong enough for business use. However, performance of these network is also important. Shaneel Narayan et al. [3] evaluate performance of window 2003 operating system on a test-bed setup and shows their network performance with different VPN tunnel protocols and algorithms. Metrics used for comparative study are throughput, CPU usage, window size.

In [5] Shaneel Narayan et al. extends their study by jointly considering new operating systems like Windows Vista, Windows Server 2003 and Linux Fedora core 6 which is not considering in [3]. In this, metrics used for comparisons are bandwidth, window size and CPU usage time [3] [5].

In [7] authors evaluated performance of VPN IPsec methods. In their research AES, DES, and 3DES each implemented with various algorithm. In this paper tests were conducted on Linux Fedora and windows operating system Combination, with one node as Linux Fedora router and other with Window 7, Windows Vista.

Paper [8] presents study of popular open-source Linux based VPN solutions and comparisons with respect to network performances and security. Performances are measured with metrics, which are bandwidth, delay and jitter.

In paper [9], they shows the performance of encryption algorithm for text files, it uses AES, DES and RSA algorithm and is evaluated from the following parameters like computation time, memory usage. By Comparing these three algorithms they conclude that, RSA takes more time for computational process.

Paper [10] had been introduced for, study of different VPN encryption techniques. The selected algorithms in [10] are RC4, Data Encryption Standard (DES), Advanced Encryption standard (AES), Blowfish.

III. EXPERIMENTAL FINDINGS

To evaluate the performance of different operating system, a test network with TCP/IP is setup [3] [5] [7] [8]. Where each VPN protocol was implemented with different algorithm on the experimental test-bed with various operating systems and the measurement were taken. The traffic generation and monitoring tool used was IPref [3] [5] [7].

Windows Server 2003 throughput values are presented in Figure 1. SSL with different algorithm portray the lowest values around 40Mbps while PPTP shows the highest.

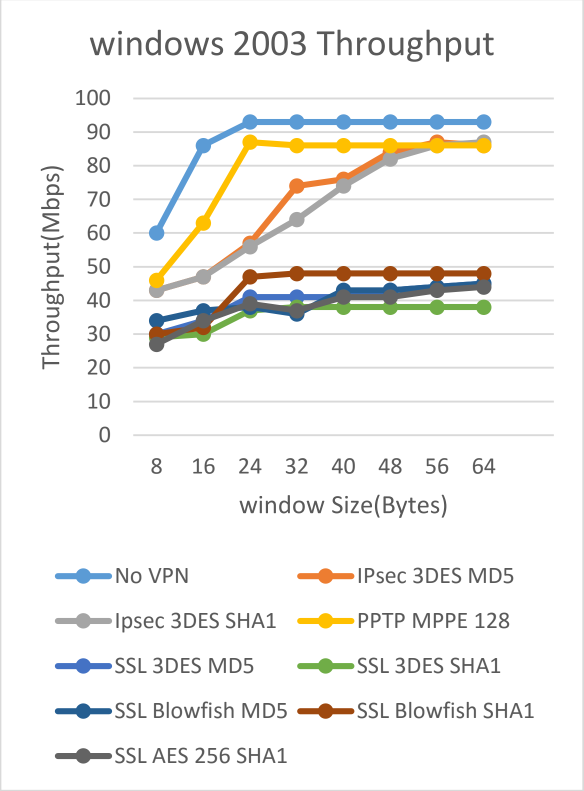

Figure 1. windows 2003 Throughput[3]

Windows Vista throughput values are presented in Figure 2. SSL values are lower than Windows Server 2003 around 25Mbps.

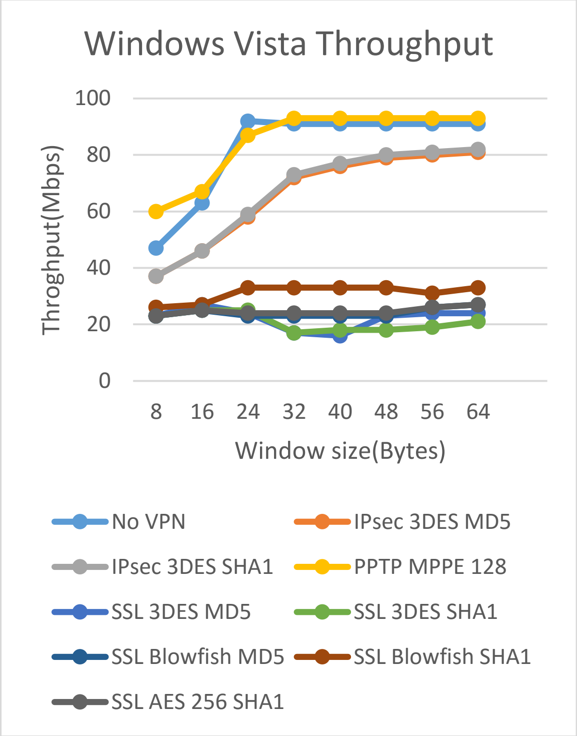

Figure 2.windows vista throughput [5]

Linux throughput values are presented in Figure 3. SSL is a better performer than IPsec in this environment. IPsec values are comparatively lower than that on Windows platforms.

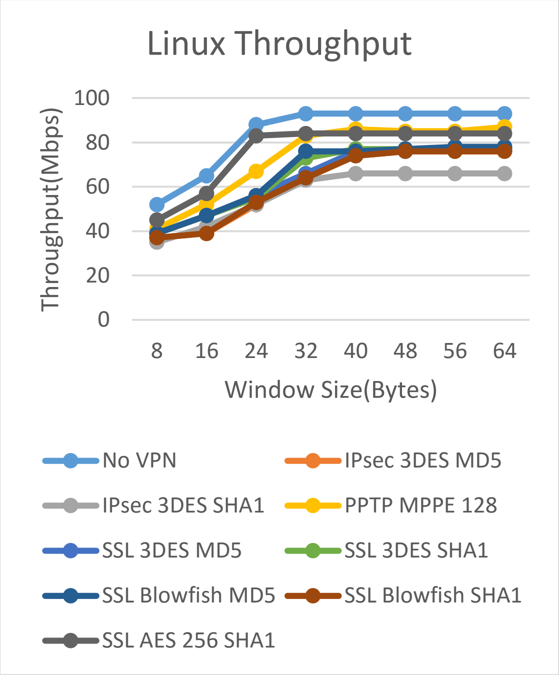

Figure 3.Linux Throughput[5]

IV. CONCLUSION

Virtual Private Network provides security and privacy to data in a public network. This technology is cost effective and efficient transmission of data among the network. In this survey, network performance of VPN protocols were tested on different operating systems. In Window 2003 PPTP shows the highest throughput while SSL shows the lowest. In Linux SSL shows the better throughput than IPsec. IPsec values are comparatively lower than that on Windows platform. So from the findings it is evident that network performance of VPN tunnel is dependent on the choice of the operating system, VPN protocol, and VPN algorithms.

V. FUTURE WORK

This work can be extended by including new operating systems like windows 8, windows 8.1, and windows 10, Mac OS-X. We can also compare the performance of normal VPN and VPN in cloud infrastructure, so this work can be further extended to calculate the performance of VPN in cloud with different Operating Systems, Protocols and algorithms with various parameters.

REFERENCES

[1] Dr. P. Rajamohan “Performance analysis and special issues of VPN technologies in communication: Trusted vpns, secure vpns, and hybrid vpns”,IIJCS,July 2014.

[2]Jayanthi Gokulakaeishnan, Dr. V. Thulasi Bai “a survey report on vpn security & its technologies”, IJCSE, aug-sep 2014

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

[4] Su Hua Sun, “The advantages and the implementation of SSL VPN”, ©2011 IEEE.

[5]Shaneel Narayan, Kris Brooking, Simon De Vere “network performance analysis of vpn protocols:an empirical comparison on different operating system” , © 2009 IEEE.

[6] Dr. S. S Riaz Ahamed, P rajmohan “comprehensive performance analysis and special issues of virtual private network strategies in the computer communication”, IJEST, July 2011.

[7]Shaneel Narayana, Michael Fitzgeralda, “empirical network performance evaluation of security protocols on operating systems”,I.J.wireless and microwave Technologies,2012.

[8]Shashank Khanvikar, Ashfaq Khokhar, “Experimental evaluation of open-source Linuxbased vpn solutions”.

[9]S. Pavithra, Mrs. E. ramadevi, “study and performance analysis of cryptography algorithms”, international journal of advanced research in computer engineering & technology, July 2012.

[10] M.A. Mohamed, M.E.A. Abou-El-Seoud, A.M. El-Feki , “A Survey of VPN Security Issues” , IJCSES Vol. 11, Issue 4, No 1, July 2014.

[11] Mohd Nazri Ismail , “Study the Best Approach for Virtual Private Network Implementation: CPU and Memory Usage Performance” , IJCSES , NOVEMBER 2010.

[12] Fahad A. Arshad, gaspar modelo-howard, saurabh bagchi “to cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network” , © 2012 IEEE.

[13] Siddeeq Y. Ameen, Shayma Wail Nourildean , “Firewall and VPN Investigation on Cloud Computing Performance” , IJCSES, April 2014.

[14] Dayananda M S , Ashwin Kumar , “Architecture for inter-cloud services using IPsec VPN” , © 2012 IEEE.