Performance Analysis of SSL VPN: On Cloud Environment

Sneha Padhiar
ME Research Scholar

Abstract— VPN is a Proven technology that does provide Security Strong enough for business use. However, Performance of these network is also Important. In this Research we evaluate Performance of Operation System available on Cloud (Windows Server 2012R2, Windows Server 2013 trial, Windows Server 2008R2) on a test-bed set-up and observe their network Performance with SSL VPN Protocol. It is found that the three Operating System give different Performance Values.

Key words: VPN, SSL-VPN, throughput, Virtual machine

I. INTRODUCTION

A. VPN:

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)

B. 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].

C. 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].

D. 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].

E. 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].

F. Cloud Computing:

1) Deployment Models [7][8]:

2) Public Cloud:

In this cloud infrastructure is made available to a large industry group or the general public and is owned by an organization selling cloud services.

3) Private Cloud:

The cloud infrastructure is operated by particular organization. It may be managed by a third party or the organization and may exist on premise or off premise.

4) Hybrid Cloud:

In this cloud infrastructure is a composition of clouds (public, private, community) that remain same entities but are bound together by standardized technology that enables data and application portability.

5) Community Cloud:

The cloud infrastructure is shared by some organizations and supports a particular community that has shared concerns (e.g., security requirements, mission, compliance consideration and policy). It may be managed by a third party or the organization and may exist off premise or on premise.

G. Service Models [7][8]:

1) Software as A Service (Saas):

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

2) Platform as A Service (Paas):

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

3) Infrastructure as A Service (Iaas):

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

The rest of paper is organized as follows: In Section II Experimental finding results are given. Conclusion is discussed in Section III. Future work are described in section IV.

II. EXPERIMENTAL FINDINGS

To Evaluate the Performance of SSL-VPN on Cloud based Operating System first the SSL-VPN has been created using Cloud Infrastructure where Cloud Infrastructure as a Service is Provided by Windows Azure. After Creation of SSL-VPN using Azure portal Transmission of Data is Carried out on Selected Operating systems.

We Presents the findings of this Research in this Section. Connection of VPN using Azure gateway are shown in Fig a and Fig b. Throughput Values of Virtual Machines Operating System :Windows Server 2008 and windows Server 2012 R2 with different size of File are shown in Fig c and Fig d. Graph shows that Windows Server 2012 gives the higher throughput Values than Windows server 2008 with different Combination of sender and receiver Operation system.

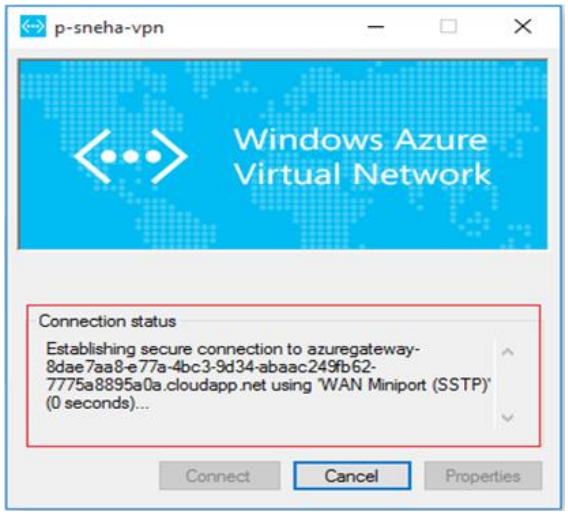

Fig. 1: Secure connection to Azure Gateway

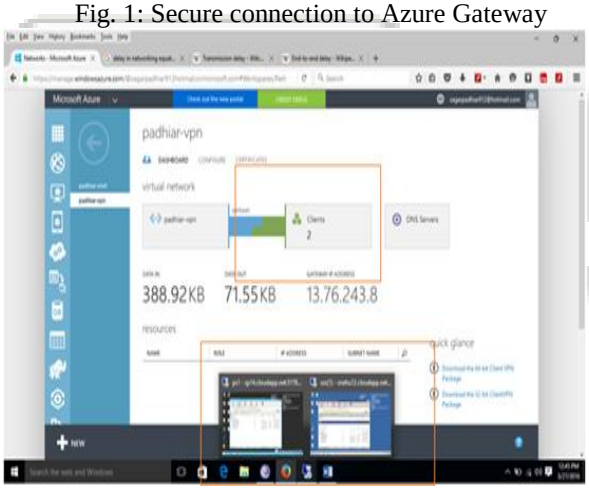

Fig. 2: Two Virtual Machines Are Connected on Created VPN(Padhiar-VPN)

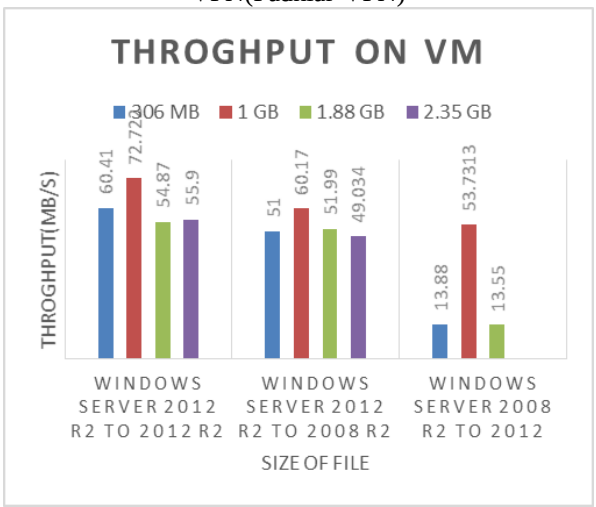

Fig. 3: performance comparison by transferring data on different OS

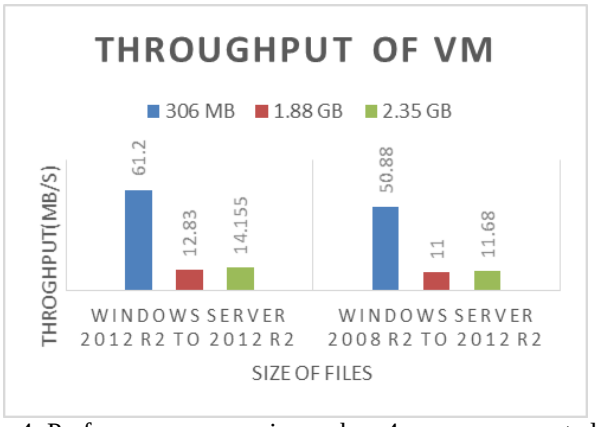

Fig. 4: Performance comparison when 4vms are connected

III. Conclusion

In this research, network Performance of SSL-VPN were tested on Different Operating Systems. In Windows Server 2012 R2 SSL shows the Highest throughput. So from the findings it is evident that network performance of VPN tunnel is dependent on the choice of the Operating System, VPN Protocol, Algorithm.

IV. Future Work

This work can be extended by including new operating systems. 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] Rahul Bhoyar, Prof. Nitin Chopde, "Cloud Computing: Service models, Types, Database and issues",IJARCSSE Volume 3, Issue 3, March 2013
[8] Zhengping Liang, SongsongJia, Jianyong Chen , Pengfu Chen, "Security of Virtual Working on Cloud Computing Platform" , © 2012 IEEE
[9] Sneha Padhiar,Pranav Verma, "A Survey on Performance Evaluation of VPN on Various Operating Systems", s © 2015 IJEDR

