Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment

Shaneel Narayan, Samad S. Kolahi, Kris Brooking, Simon de Vere
UNITEC New Zealand
snarayan@unitec.ac.nz

Abstract

Virtual Private Network (VPN) is a technology that provides secure communication for data as it transits through insecure regions of information technology infrastructure. With prolific development of the Internet, businesses nowadays implement VPN tunnels using different protocols that guarantee data authenticity and security between multiple sites connected using public telecommunication infrastructure. VPN provides a low-cost alternative to leasing a line to establish communication between sites. In this research we empirically evaluate performance difference between three commonly used VPN protocols, namely Internet Protocol Security (IPSec), Point-to-Point Tunneling Protocol (PPTP) and Secure Socket Layer (SSL). We compare performance differences in these protocols by implementing each using different algorithms in a Windows Server 2003 environment. Results obtained indicate that throughput in a VPN tunnel can range from approximately 40 to 90Mbps depending on the choice of protocol, algorithm and window size. These three attributes also govern CPU utilization of VPN servers.

Keywords
VPN, tunneling, IPSec, PPTP, L2TP, Windows 2003, performance evaluation.

1. Introduction

Internet has become the default communication channel for businesses and it continues to grow exponentially. However the protocol used to create the Internet infrastructure (TCP/IP) was originally not designed to provide data security. That is, TCP/IP can transmit data to different parts of a network, but the contents of the data packets are vulnerable to unauthorized access. To circumvent this problem, several solutions have been developed, but VPN is the most widely and trusted technology used to secure communication links that transit through unknown networks. VPN is cost effective and can work with common software and hardware vendor products. There are several VPN products that are widely available, all with different capabilities and features [1]. They all enable businesses to implement VPN tunnels (figure 1) to create organization wide secure networks between multiple sites. To create these tunnels, there are several protocols – three commonly used are: IPSec, PPTP, and SSL.

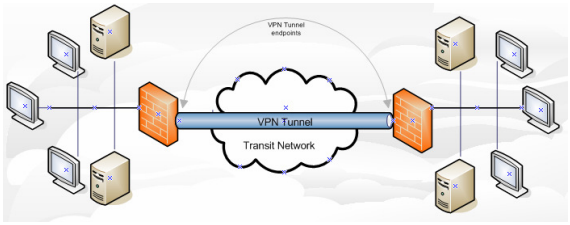

Figure 1: VPN Tunneling

VPN protocols provide encryption and integrity to data in transition. A VPN protocol is usually designed to be implemented with various compatible encryption and integrity algorithms. Common encryption protocols used include Triple Data Encryption Standard (3DES) and Blowfish (BF). And common data integrity protocols used includes Message-Digest 5 (MD5) and Secure Hash Algorithm (SHA1). PPTP was designed to only use a certain type of encryption, Microsoft Point to Point Encryption (MPPE). The encryption algorithms are simulated and compared in [2].

Since information technology infrastructure nowadays need high bandwidth, the study of the parameters affecting the VPN bandwidth is very important. In [3], the VPN technologies have been compared in Linux environment and in [4], the VPNs have been compared in Novell Netware and Windows 2000. Open-Source Linux based VPN solutions have been empirically evaluated in [5] and [6]. In this paper Windows 2003 is used and the VPN protocols are compared in terms of bandwidth, window size and CPU usage time. Because the TCP transit data packets at a time up to the size of the window size, the window size has an impact on overall number of bits transferred in a second. In [7, 8] the influence of windows size on capacity of some communication systems are discussed.

The rest of the paper is organized as follows: Section 2 discusses the three VPN protocols that will be tested for performance in this research, and Section 3 describes the experimental setup that was used. We present the results and discuss the findings in Section 4.

Finally, conclusions from the research are drawn in Section 5.

2. VPN Protocols

In this section three VPN Protocols (IPSec, PPTP and SSL) are discussed. These protocols are widely used in the industry, both in commercial products and open-source implementations, and are a common subject for research.

2.1 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. IPSec is an OSI Layer 3 protocol that supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality and replay protection. 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, but leaves the header untouched. This mode is commonly used to secure communication within a network. The more secure tunnel mode encrypts both the header and the payload and is generally used for securing communication that traverses unknown third party networks. That is, tunnel mode is used for network-to-network communication. IPSec has two protocols that is enables it to provide packet level security: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is intended to guarantee connectionless integrity and data origin authentication of the IP datagrams. It may optionally protect against replay attacks. ESP provides origin authenticity, integrity and confidentiality protection of a packet. It also supports encryption-only and authentication-only implementations.

2.2 PPTP

PPTP was developed by a vendor consortium of Microsoft, Ascend Communications and 3COM [9] and is an OSI Layer 2 protocol. PPTP is an extension of point-to-point protocol (PPP) and its popularity is attributed to the ease with which it can be configured. 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 datagrams containing encrypted PPP packets which are transported through the tunnel. Thus, by design PPTP has a very simple mechanism.

2.3 SSL

SSL is a VPN technology (developed by Netscape) that is commonly used with Web browsers to give users a seamless secure connection. However 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, which determine 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.

3. Experimental Setup

A VPN test network with TCP/IP protocol is set-up using Windows 2003 network operating systems (Figure 2) with no domain installed. All computers and servers are Pentium 4 with 3.0GHz CPU and 1GB of memory. They are connected to a 10/100 Ethernet switch with 100Mbps UTP links. The network consists of three subnets joined by two routers. Two VPN servers act as software routers and VPN tunnel end-points. A 10/100 switch is used to connect two VPN servers. To each VPN server, a client computer is connected and that is the point the data is generated and travels through the tunnel.

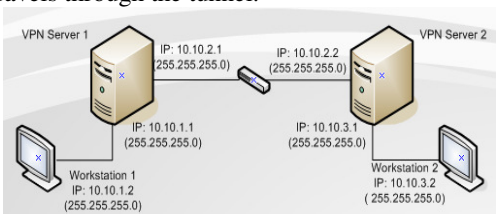

Figure 2: Testbed Setup

The traffic generation and monitoring tools used was *Iperf* and CPU usage data was collected by the Windows 2003 Server performance counter. These tools have been proven to be reliable and robust from previous research in network measurements. *Iperf* is a command line oriented software used to create and measure maximum TCP bandwidth [3].To ensure high data accuracy, all tests were executed with multiple runs for sufficient duration. Standard deviation for data generated for each windows size was calculated and if the results fell outside 95% confidence interval, the experiment was rerun. The metric used in the experiment is throughput (measured in Mbps).

4. Experimental Results

We present the findings of this research in this section. Each VPN Protocol was implemented with different algorithms on the experimental testbed and window size was gradually increased for TCP traffic and resulting throughput and CPU utilization values were recorded.

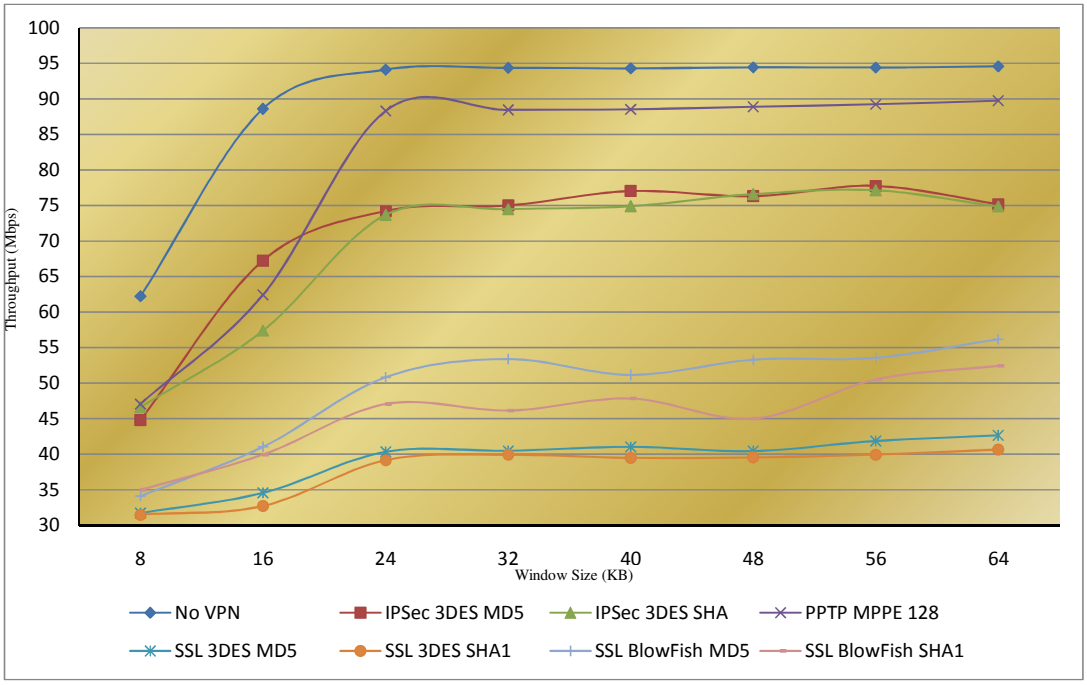

Figure 3: Graph of Throughput Values of the VPN Algorithms

The throughput results obtained from the experiments in this research are shown in Figures 2. These throughput results indicate that the bandwidth can change from anywhere between 30Mbps (SSL windows size 8KB) to 95Mbps (no VPN). As the windows size increases more data is transferred, therefore the graphs show high throughput values for higher window sizes. The most impact is when changing the window size from 8 to 16 to 24KB, where there is a steep incline in the graphs. The window sizes have little impact from this point onward (24KB to 64KB) as the VPN tunnels reach their capacity limit, evident in the flatness of the graphs.

The results indicate that the PPTP MPPE provides up to 90Mbps (the highest bandwidth) while SSL 3DES SHA1 is at 40Mbps (the least bandwidth). If no VPN is used the bandwidth can be increased up to 95Mbps. The differences between the protocols is less noticeable at low window size of 8KB (range from 32Mbps to 48Mbps and with 62Mbps for no VPN) but as the window size increases, the gap widens at the window size of 64Kbytes (range from 41Mbps to 90Mbps and with 95Mbps for no VPN). SSL BF MD5 appears to have up to 15Mbps bandwidth above other SSL protocols (BF SHA1, 3DES SHA1, 3DES MD5) especially at higher windows size of 32KB to 64KB. However IPSec protocols (3DES, MD5 and 3DES SHA1) has similar bandwidth for various window sizes. It is seen that there are significant difference between throughput values for SSL, IPSec and PPTP. All SSL algorithm throughput values are banding together around an average of approximately 40Mbps for larger window sizes. For the same windows sizes, IPSec values are averaging approximately 75Mbps while PPTP has the highest bandwidth of around 90Mbps.

It should be noted that this research purely evaluates performance difference between the different tunneling algorithms and does not investigate security differences resulting from different implementations. CPU utilization values of VPN servers are presented next.

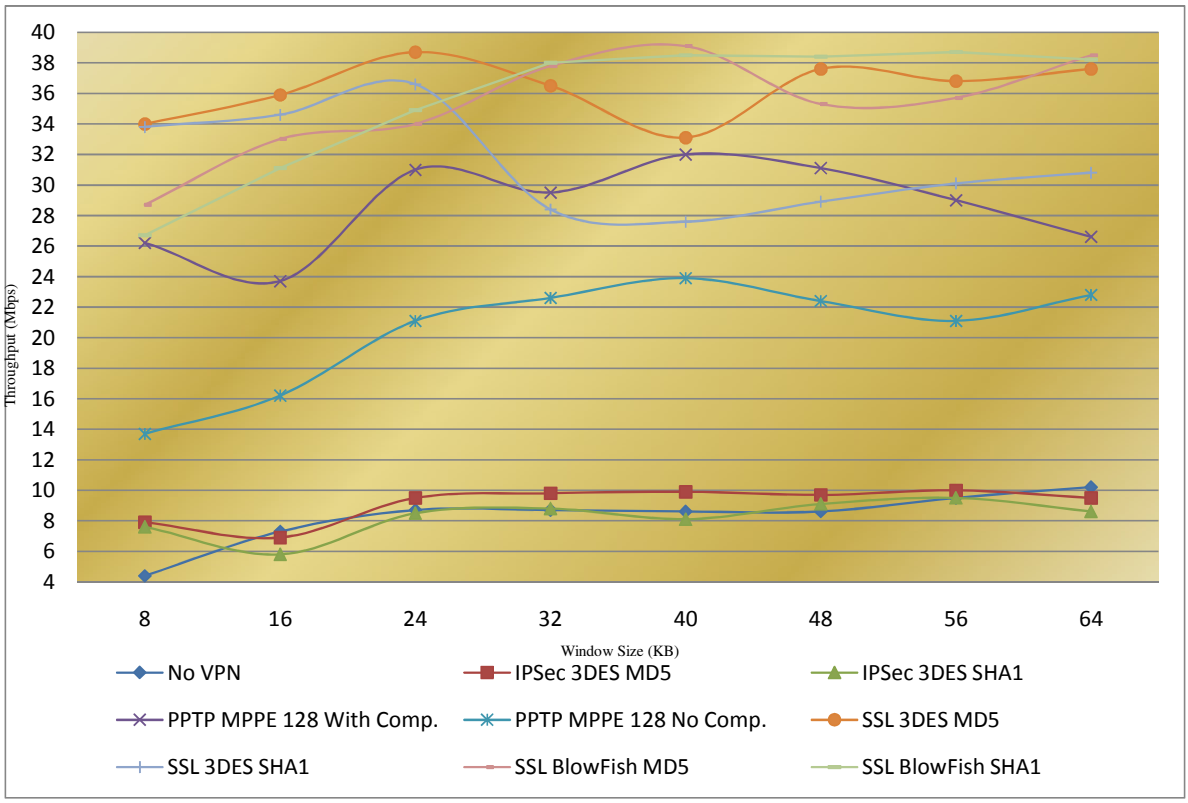

Figure 4: Graph of CPU Utilization of the VPN Algorithms

The measurement of CPU utilization at router 1 (VPN Server 1 in Figure 2) is shown in Figure 4. Since these values were very similar to the ones obtained at the other VPN router, only one set is shown.

Generally as the window size increases the CPU usage has increased with all changes between 8KB to 24KB. The CPU usage does not changed much for window sizes from 24 to 64KB for most algorithms. At small window size of 8KB, SSL 3DES uses the highest CPU of 32% and no VPN only uses 5% CPU. SSL BF SHA1 appear to use most CPU of all at higher window sizes (up to 42%) while no VPN uses approximately 7% at higher window sizes. IPSec appears to use considerably less CPU when compared to other protocols (between 5% to 12% depending on window size). Second least CPU usage is by PPTP (17% to 30%). From the graphs it is seen that SSL uses the most CPU of the VPN servers.

5. Conclusions and Future Work

In this paper we have empirically evaluated performance of IPSec, PPTP and SSL tunneling protocols in a Windows 2003 environment. The metrics considered were bandwidth and CPU usage time. The results indicate that throughput of VPN tunnel and CPU utilization of VPN servers are dependant on the choice of tunneling protocol, algorithm, and window size used in data transmission. We conclude that:

- VPN tunnel implemented in Windows 2003 environment has the best network performance when PPTP is used as the tunneling protocol (average value =90Mbps). The values obtained indicate that throughput for PPTP is very close to that of a network without VPN. IPSec is the second best performer while SSL depicts the lowest values (average value =40Mbps).
- Choice of a particular tunneling protocol algorithm can affect network performance significantly.

In case of SSL, throughput values vary by almost 30% depending on the choice of algorithm.

- CPU utilization of the VPN server is dependant on the tunneling protocol and the algorithm. While IPSec used the least resource and SSL the most, it is evident the various SSL algorithms consumed CPU resources differently.

This work will be extended to include more tunneling protocols with a wider selection of algorithms. Performance of VPN tunnel in Windows 2003 environment will also be compared with other network operating systems.

10. References

[1] S. Khanvilkar, and A. Khokhar, 'Virtual Private Networks: An Overview with Performance Evaluation", in IEEE Communications Magazine, October 2004, pp 146 – 154.

[2] A. Nadeem, and M. Y. Javed, "A Performance Comparison of Data Encryption Algorithms," in First International Conference on Information and Communication Technologies, *2005. ICICT 2005*, pp. 84 - 89.

[3] T. Berger, "Analysis of current VPN technologies", in The First International Conference on Availability, Reliability and Security, *2006. ARES 2006.*, 2006, p. 8.

[4] S. Al-Khayatt, S. A. Shaikh, B. Akhgar, and J. Siddiqi, "A study of encrypted, tunneling models in virtual private networks.," in Proceedings of the International Conference on Information Technology: Coding and Computing, 2002, pp. 139 - 143.

[5] S. Khanvilkar, and A. Khokhar, 'Experimental Evaluations of Open-Source Linux-bases VPN Solutions", 2004, pp 181 – 186.

[6] C. J. C. Pena, and J. Evans, "Performance Evaluation of Software Virtual Private Networks (VPN)', 2000, pp 522 – 523.

[7] W. Ge, Y. Shu, L. Zhang, L. Hao, and O. W. W. Yang, "Measurement and Analysis of TCP Performance in IEEE 802.11 Wireless Network", in Canadian Conference on Electrical and Computer Engineering, 2006, pp. 1846 - 1849.

[8] D. J. Choi and N. S. Kim, "Performance measure and analysis of large TCP window effect in broadband network including GEO satellite network", in 5th IEEE International Conference on High Speed Networks and Multimedia Communications, 2002, pp. 388 - 391.

[9] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, "Point to Point Tunneling Protocol (PPTP)", RFC 2637, 1999.