Performance Evaluation of IPSEC-VPN on Debian Linux Environment

A. A. Ajiya
Computer Science Department
Federal University Gashua,
Yobe State, Nigeria

U. S. Idriss
Computer Science Department
Federal University Gashua,
Yobe State, Nigeria

Jerome M. G.
Computer Science Department
Federal University Gashua,
Yobe State, Nigeria

ABSTRACT

Cyberspace has gotten a great favour from the general public in recent times. Affordability of infrastructure and globalization are believed to be the main drivers. This development resulted to lots of business enterprises to conceive a secure Virtual Private Network (VPN). Internet Protocol Security (IPSEC) which is one of the most widely used and deployed VPN tunneling Protocol in today's networks. However, it is extremely difficult for one to find out the information about its performances comparatively with different encryption algorithms. In this research, the performance differences were evaluated through empirical observation. The experimental analysis was done on Debian Linux environment by implementing IPsec tunneling protocol with different encryption algorithms. Encryption algorithms are used to encrypt data so it cannot be read or modify by a third-party while in transit. Triple Data Encryption Standard (TDES/3DES) and Advance Encryption Standard (AES) are the encryption algorithms used in this research. The study concluded that IPSec AES-sha1 provides fair and reasonable performance compare to IPSec 3DES-sha1. Also, the research indicated that encryption/decryption of VPN UDP (User Datagram Protocol) traffic requires large amount of CPU and memory and that contributed to performance degradation.

General Terms

Cyberspace, Protocol, Algorithms, Linux, Datagram, Memory.

Keywords

Virtual Private Network (VPN), User Datagram Protocol (UDP), Internet Protocol Security (IPSEC), Advance Encryption Standard (AES), Data Encryption Standard (3DES).

1. INTRODUCTION

VPN is usually employed in business sectors with the intention to allow for guaranteed secure connection or access over untrusted public network infrastructure such as cyberspace /Internet [12]. VPN is a tested technology that adequately does offers security strengths, for business enterprises usage [12]. Nevertheless, analysing the networks' performance is also of great significant, since reducing the available network reserved resources could reduce monetary values and ameliorate business enterprises or remote client's self-contentment and network efficiency.

VPN applied encryption to offer data confidentiality, information integrity and client authentication because data is passing through the public network [13]. Confidentiality is achieved at a time when packets that passed through the public network are unreadable [4]. Similarly, that insured that information is not exposed or altered in whatsoever fashion throughout the duration of the transmission. Additionally, VPN offers information integrity by exploiting a message digest to assure that the information or data has not been manipulated with time during of the transmission [15]. Normally, VPN does not offer effective client or user authentication, because client or users can gain access to a private internet through insecure networks by simply entering a simple username and password. However, VPN exercise to support authentication applications like smart cards. In this research, 3DES and AES are used for encryption and Secure Hash Algorithm (SHA1) for integrity [15]. Choice of the encryption algorithms can impact the performance of different operating system environment [12]. In this study we have used the VPN cryptographic concepts and empirically evaluated the network performance of the most commonly used VPN tunnelling protocol IPSEC and encryption algorithms on Debian Linux operating system. The encryption algorithms used are AES and 3DES. Moreover, in an end-to-end communication quality of services (QoS) factors/parameters are taken into considerate. The research focused upon analysing UDP generated traffic and measuring the throughput, latency, packets Loss and jitter with respect to frame sizes. At the same time, the study measured the CPU utilization of the VPN server machine.

This study is useful to the router's or computer systems manufacturers and the general public, introducing VPN accelerator cards (VACs) built with cryptographic functionalities on routers (or software routers) will enhance performance. These additional routing capabilities on VPN accelerators will improve the routers operation performance [1]. The significant issue in this research is on the performance of IPsec-VPN tunnelling protocol, but this research added additional VPN scopes that will help us understand more about the generally IPsec-VPN tunnelling protocol performance issues on the internet. These additional scopes are formulated in the research questions. The investigation of these questions was made and finally the study came up with accurate answers to them. The research questions are as follows:

Which encryption algorithm is better, between IPsec-AES-Sha1 and IPsec-3DES-Sha1on Debian Linux operating system environment with respect to quality of service parameters such as throughput, jitter, packet Loss, CPU usage and latency?

(i) Does encryption and decryption of VPN traffic requires large amount of CPU and memory?

2. VIRTUAL PRIVATE NETWORK (VPN) AND IP SECURITY (IPSEC)

This section discussed the principle of how VPN and IPsec work considering their security features.

2.1 Overview of Virtual Private Network (VPN)

There is a raising needs and involvement nowadays to link to internet networks from remote locations. VPNs has been found and proved to be that effective to substitute old system of lease lines to produce private network in an organisations and business establishments [12]. VPNs generally exploited by organisations and administrations to link central office/Head-office with subdivision office, main office for distant employees or roaming users, business collaborator sites and remote teleworkers of their join network [10][3]. VPN is a general terminal figure used to identify a communication channel network that uses any collection of technologies e.g. IPsec to insure and guarantee a connection tunnelled via an unsecured network, e.g. Public Network like internet [4]. Implemented VPNs add a manner of transmitting data as if it were moving through private network connections. VPN carries information through the act of “tunnelling”. At first, VPN encapsulate (wrapped) a packet to be transmitted into a new packet on a new header before its transmission take place [5]. Similarly, the header is responsible for the provision of routing information, these routing information aids transmitting packets to transverses the public network before reaching their tunnel endpoint. Subsequently, when these packets arrives at the tunnel endpoint, VPN decapsulate them and forward to its final destination [5]. This logical route that these packets pass through is called a VPN tunnel. These two VPN tunnel endpoints need to endure and support identical tunnelling protocol effectively before VPN can establishes connection.

2.2 Overview of IP Security

IPsec is a cryptographic protocol designed by Internet Engineering Task Force (IETF) to offers security on IP packets in the internet [12]. This security provision involves creating a secure connection or tunnel between two endpoints (client and server). To create this tunnel, IPsec has to use a handshake protocol called Internet Key Exchange (IKE) to establish the connection so that endpoints can securely send IP packets [7]. IPsec significantly provide information integrity, authentication and data encryption [17]. These significant provisions prevent unauthorized user from data modification and disclosure. Moreover, for IPsec to achieve these functionalities it requires using two protocols; Authentication Header (AH) and Encapsulating Security Payload (ESP) [1][15]. IPsec is client/server protocol that set to only ship data between VPN endpoints [7]. IPsec is used in two fashions, tunnel mode or transport mode and each IPsec security protocol has a transport mode and tunnel mode. Transport mode is used to only secure (encrypt or authenticate) the carried data itself, and tunnel mode, only encrypt or authenticate the IP header of the packets [1].

3. METHODOLOGY

This section provided a detailed description on the methodological analysis used to explain which encryption algorithm performs better between AES and 3DES, including the Steps followed to establish the VPN secure connections.

3.1 Experimental Setup

This research used four network nodes (Linux computer systems) to create a VPN network. The experimental test was carried out through generating and monitoring network traffics across the VPN connection. The evaluated final result finalized after latency, throughput, package Loss, CPU usage and jitter values are elapsed, based on those results the research determined the performance of IPsec-VPN considering IPsec-AES-Sha1 and IPsec-3DES-Sha1. At the same time, we plotted graphs to represent the distribution differences graphically.

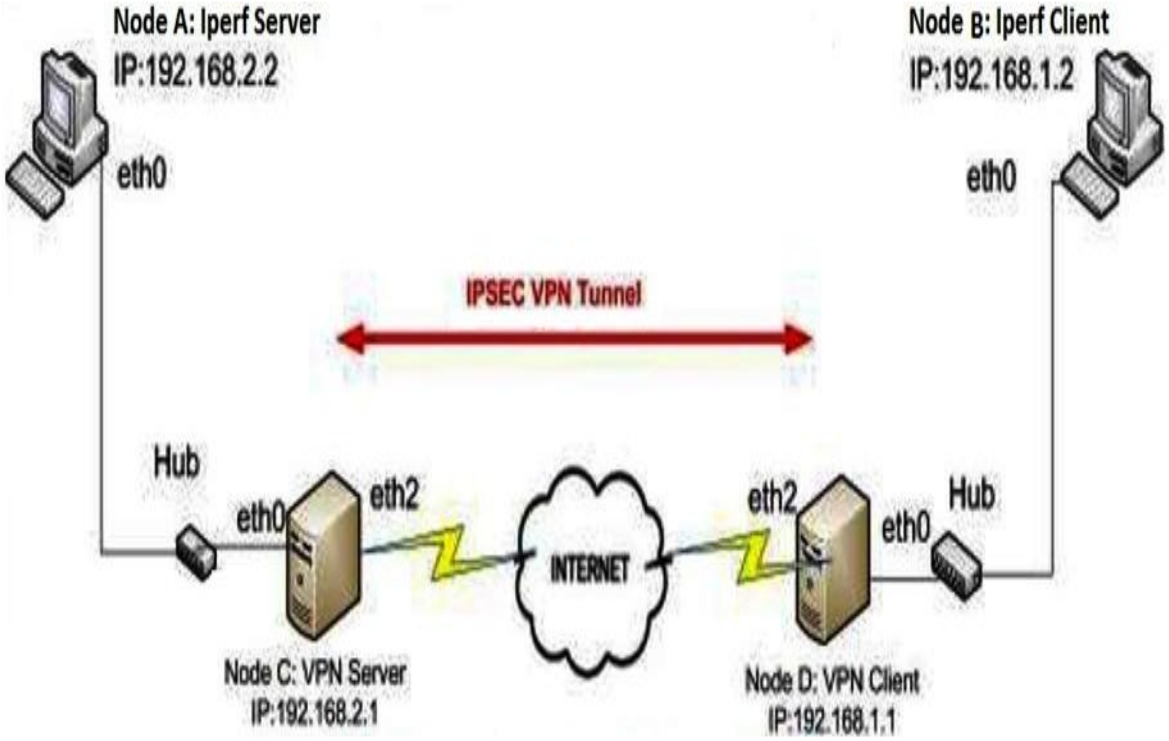

Figure 1 – Experimental Test-bed

The major goal of this research is to evaluate the performance of IPsec VPN protocol on Debian 6.0.5 Linux environment. To measure and analyses the performance of IPsec VPN protocol, this study employed Open swan [9], is a free open sources software application for IPsec VPN implementation. It is installed to evaluate different aspects of the IPsec protocol performance scenarios. This research also used the following Measurement tools. Iperf 2.0.0 is installed as the network traffic generator and monitoring tool, tcpdump tool is used to measure the packet loss of the UDP traffics generated by Iperf and ping tool is used to measure round-trip latency.

3.2 Steps followed to established the VPN secure connections

Before analysing the performance of any VPN protocol, a VPN secure connection or tunnel has to be established. This section discussed the steps followed by this research to create the VPN tunnel (IPsec-VPN tunnel).

Step 1 – Make Interfaces file: These file contain instructions that are responsible for allocating the internet protocol address, broadcast address, network address and the network mask address. Each computer or node holds one interface file and all the addresses are assign statically.

Step 2 – Install VPN application software (Openswan - IPSec): This step involved choosing the type VPN tunnel to use after having the interfaces files ready [16]. In this research, Openswan 2.0 is chosen and is installed successfully on the gateway machines (Node C and Node D).

Step 3 – Produce IP forwarding files: The file contains NAT traversal instructions that are responsible for specifying the internet protocol forwarding capabilities. Contain all the rules to forward the UDP traffic packets across the networks. Similarly, it is used to provide security and firewall functionality to the network.

Step 4 – Setting up the IPSec configuration files: Configuration file is the main effective file among all the files mentioned above, it contain instructions and information about the VPN tunnelling session. These instructions are security properties that specify the tunnelling requirements (VPN security parameters) to use throughout the established VPN tunnelling session.

Step 5 – Adding route between VPN endpoints: The next important thing is adding communication routes between VPN endpoints in to the routing table.

Step 6 – establishing VPN connection: This is the last steps we followed to creating a VPN secure connection between Node C and Node D. IPSec VPN connection established using the command “ipsec auto – up net-to-net” on system command prompt.

4. EXPERIMENTAL FINDINGS AND ANALYSIS

This section described all the test results found. The results were obtained from the experimental test-bed above. Each test scenario was repeated for several number times in order to get an average performance and effective result. Microsoft excel was used to graphically represent the performance results on a different graphs based on the performance matrix (Quality of service parameters). The description of these results is as follows:

4.1 Throughput

Throughput is the range at which information can be transferred from one endpoint to another over long period time duration. The UDP throughput is measured using Iperf and analysed for UDP generated traffic for differed frame size. Figure 2, indicated that UDP throughput get increases when frame size increases for all VPN scenarios. Throughput increases with increase in frame size because, when sending information with bigger frame site the maximum overhead for sending the data as a result of frame header decreases compare to transmitting data with small frame sizes [8]. The result of this experiment clearly from the graphs indicated that, IPsec/AES is the best to choose over IPsec/3DES in accordance with UDP throughput, because VPN protocol with the higher throughput has the best performance [8].

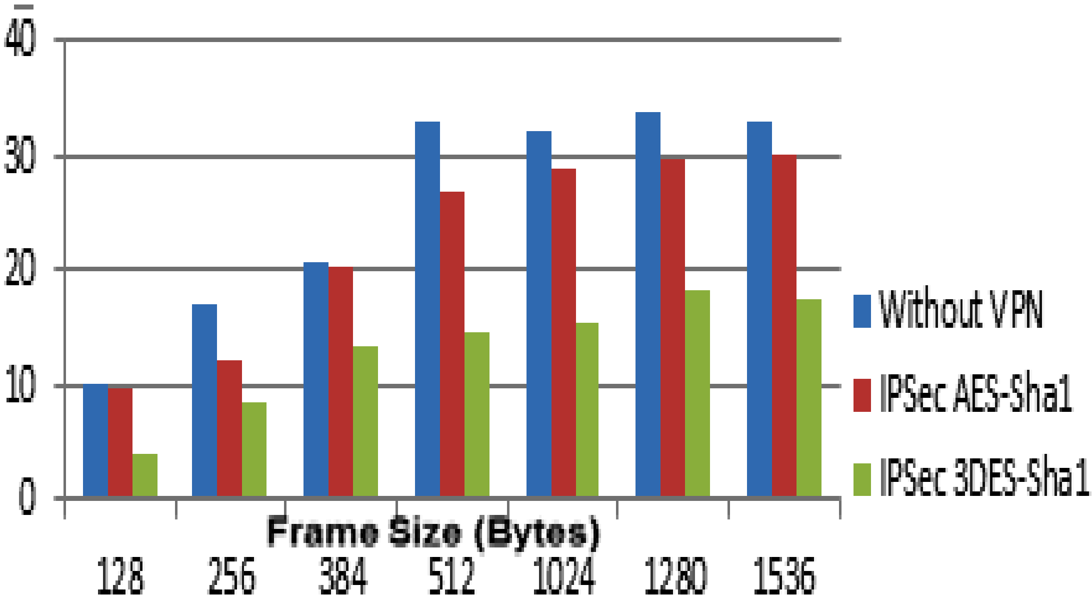

Figure 2 – IPsec VPN throughput results

4.2 Packet Latency

Latency is also known as round trip time (rtt), is total time it takes for a packet to transverses the network from one source to destination and back to the source [6]. The packet latency is measured using ping tool and analysed for generated traffic for differed frame size. Figure 3, indicated that latency values get increases when the frame size increases for all VPN protocols. Also, it showed that the latency without VPN is less than all the latency values for IPSec AES-sha1 and IPSec 3DES-sha1 and it happened because of the traffic load with encrypted packets over packets without encryption [1]. The result indicated that, IPsec/AES win, because it has the highest maximum latency then followed by IPsec/3DES as the second.

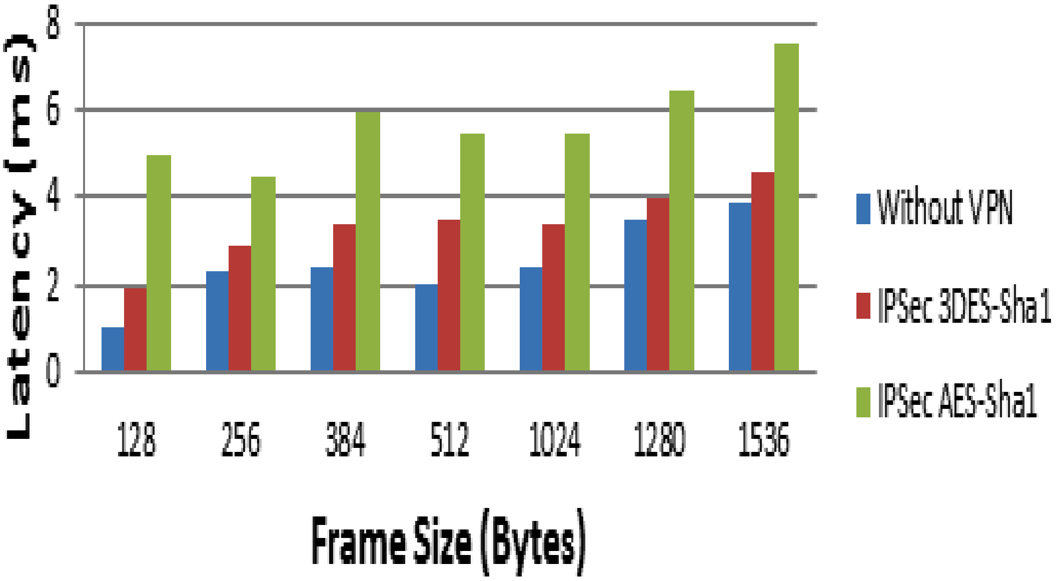

Figure 3 – IPsec VPN packet latency results

4.3 Packet Delay Variation (Jitter)

Packet delay variation (jitter) is the variation in the sample latency received by the destination host. Jitter has strong impacts on the quality of service or performance when it is high. This research obtained all the jitters values from calculation, by taking the differences between latency samples obtain from using the ping tool and divide by number of latency samples minus 1. This mechanism or formula [11] used is shown below. Where, Ln is the number of latency samples obtained.

$$\text{Jitter} = \frac{|L1-L2| + |L2-L3| + |L3-L4| +\ldots+ |(Ln-1)- Ln|}{n - 1}$$

The packet delay variation is measured from calculating the variation different of latency values obtained from using the ping tool. The overall jitter results of this experiment are shown in figure 4. It indicated that the jitter values almost moves in the same manner and does not pass 1ms both for IPsec/AES and IPsec/3DES. Eventually, figure 4 depicted that, IPsec/3DES has the highest jitter and IPsec/AES has the lowest. In that case, it is shown that IPsec/AES is better than IPsec/3DES.

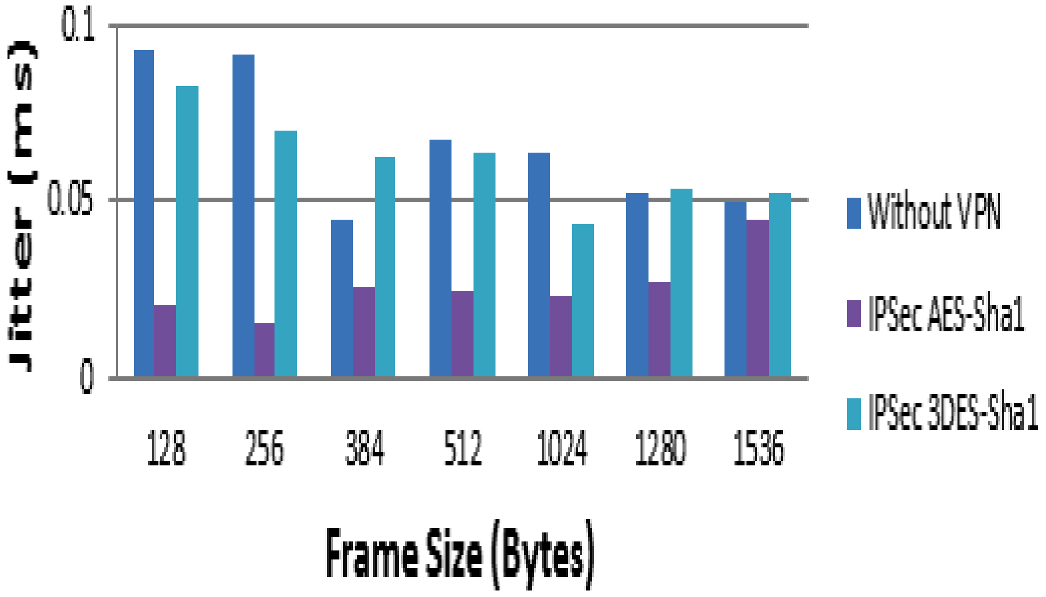

Figure 4 – IPsec VPN packet delay variation (jitter) results

4.4 Packet Loss

Packet loss is the amount of packet transferred but not received at the destination compare to the total number of packet sent at the source (sender) [6]. The packet loss is measured using tcp dump and the percentage packet loss calculated using the packet loss formula [11] below.

$$\text{Packet Loss} = \frac{\text{Number of lost packet}}{\text{Number of lost packet + Number of packet received.}}$$

The overall percentage packet loss results of this experiment are shown in figure 5. It indicated that IPsec/3DES has the highest packet loss and followed by IPsec/AES, it has the lowest packet loss values. Evidently, because of the packet loss prominence for IPsec/3DES, IPsec/AES win over IPsec/3DES. Clearly, the graph shown that IPsec/AES is the first and IPsec/3DES is the second.

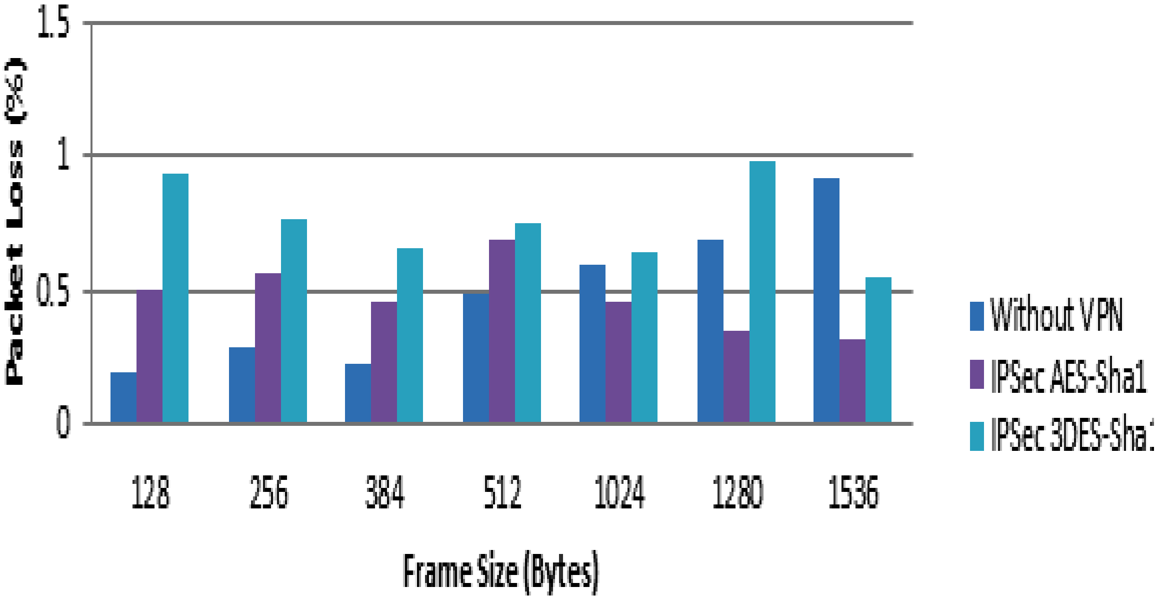

Figure 5 – IPsec VPN packet loss results

4.5 CPU Usage

CPU usage is affected in the time of encapsulation and de-capsulation of VPN packets and Monitoring the CPU usage provides us with bottleneck in the VPN network connection [1]. The CPU usage is measured from the VPN client system. This experiment is repeated many number of time to find the average CPU usage for various frame size. The overall percentage CPU usage results of this experiment are shown in figure 6. It clearly showed that IPsec/3DES and IPsec/AES have the same CPU utilization (performance) because they literally fall in the same range. In this scenario any IPsec/3DES or IPsec/AES could be used to create a VPN connection when CPU utilization is considered. Also, figure 6 showed that without VPN has the lowest percentage CPU usage. Using encryption algorithms to create a VPN tunnel to protect data reduce the transmitting rate and could cause CPU demanding [2]. This is because encryption demands more time to encrypt and decrypt transmitted packets which lead CPU throughput reduction and high CPU consumption [1].

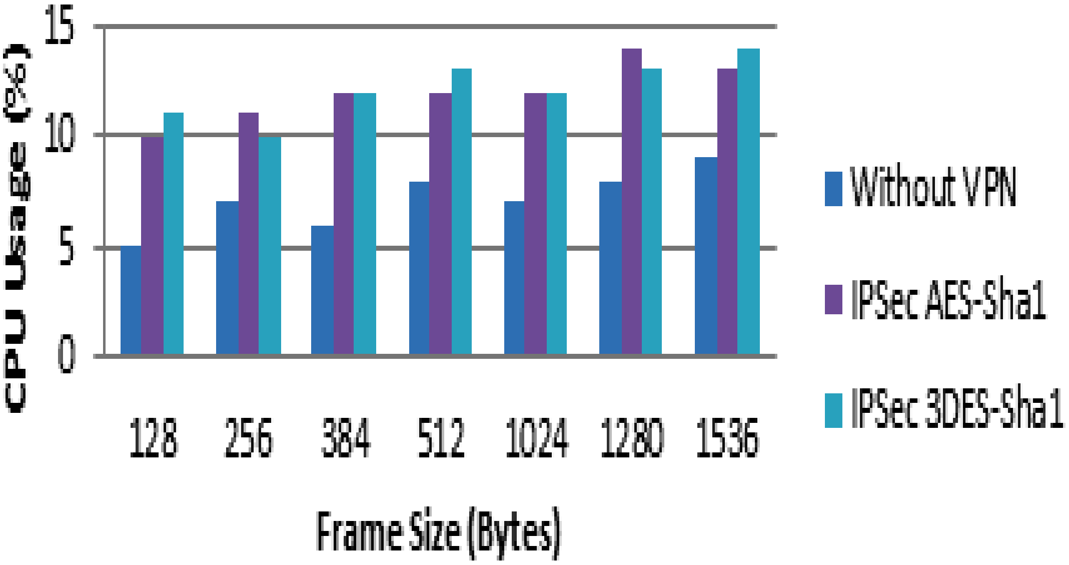

Figure 6 – IPsec VPN CPU usage results

5. SUMMARY AND CONCLUSION

In this study, through empirical observation, it examined the performance of IPsec-VPN tunnelling protocols configured with AES and 3DES cryptographic algorithms. This protocol is well examined towards network performance on Linux Debian operating system. The measurement parameters used in this relative study are throughputs, latency, jitter, packet loss and CPU usage. From the experimental results and findings it clearly indicated that, the performance of VPN secure connection is reliant to the type of tunnelling protocol and encryption algorithms selected for the VPN session. The study found the following conclusions and they served as the answers to our research questions. IPsec configure with AES provide high UDP throughout performance compare to IPsec/3DES. IPsec configured with AES offers best latency performance for UDP packets, followed by IPsec/3DES which offered the lowest performance. IPsec/3DES gave the greatest effect on jitter and packet loss compared to IPsec/AES. IPsec/AES provided the lowest jitter and packet loss values. In this case IPsec/AES wins over IPsec/3DES. IPsec/AES and IPsec/3DES almost consume similar CPU memory (system memory/*RAM)*. It also indicated VPN traffic demands large amount of CPU memory and decryption of transmitted VPN packets that lead CPU throughput reduction and high CPU consumption.

6. REFERENCES

[1] Adeyinka, O. (2008). Analysis of IPsec VPNs Performance in a Multimedia Environment. *Association for Computing Machinery*.

[2] Alshamsi, A. and Saito, T. (2005) A technical comparison of IPSec and SSL. *IEEE: 19th International Conference for Advanced Information Networking and Applications*, 2 p.395 - 398.

[3] Boulanger, J. and Bailly, B. (2009) Performance Analysis of Two Secure tunneling mechanisms: IPSec VPN versus SSL VPN. *Ensimag Grenoble*, p.1 - 13.

[4] GovHK (2008). The Government of the Hong Kong Special Administrative Region: *VPN Security*.

[5] Jaha, A., Fathi B. S. and M. A. (2007) Performance Evaluation for Remote Access VPN on Windows Server 2003 and Fedora Core 6. *IEEE: TELSIKS*, p.587 - 592.

[6] Jaha, A., Fathi B. S. and M. A. (2008) Performance Evaluation for Remote Access VPNs on Windows Server 2003. *IEEE Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, p.582 - 587.

[7] Kotuliak, I., P. Rybár and P. Trúchly. (2011) Performance Comparison of IPsec and TLS Based VPN Technologies. 9th IEEE International Conference on Emerging eLearning Technologies and Applications, p.217 - 221.

[8] Likhar, P., Ravi Y. and Keshava M. R. (2011) Performance Evaluation of Transport Layer VPN on IEEE 802.11g WLAN. *Journal of Institute of Electrical and Electronics Engineers*, (197) p.407 - 415.

[9] Linuxplayer.org (2011) Openswan – Use the KLIPS stack. [Online] Available at: http://www.linuxplayer.org/2011/02/openswan-use-the-klips-stack [Accessed: 31 Jul 2012].

[10] Mazlan Zaharuddin, M., Ruhani Ab Rahman and Murizah Kassim. (2010). Technical Comparison Analysis of Encryption Algorithm on Site-to-Site IPSec VPN. International Conference on Computer Applications and Industrial Electronics, p.641 - 645.

[11] Malik, R. and Syal, R. (2010) Performance Analysis of IP Security VPN. *International Journal of IP Security VPN*, 8 (4), p.5 - 8.

[12] Narayan, S., Kris B. and Simon de Vere. (2009).Network Performance Analysis of VPN Protocols. *IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing*, (367), p.645 - 648.

[13] Narayan, S., Michael F. and S. R.. (2010). Empirical Network Performance Evaluation of IPSec Algorithms on Windows Operating Systems Implemented on a Test-bed. *Journal of Institute of Electrical and Electronics Engineers*.

[14] Nessoft.com (2011).What is Jitter?. [Online] Available at: http://www.nessoft.com/kb/article/what-is-jitter-57.html [Accessed: 31 Jul 2012].

[15] O. Elkeelany, M.M. Matalgah, K.P. Sheikh, M. Thaker, G. Chaudhry, D. Medhi and J. Qaddour. (2002). Performance analysis of IPSec protocol: Encryption and authentication. IEEE International Conference.

[16] Scribd.com (2009). *Openswan Installation and Configuration Tutorial*. [Online] Available at: http://www.scribd.com/doc/15585156/Openswan-Installation-and-Configuration-Tutorial [Accessed: 30 Jul 2012].

[17] Shue, C., Youngsang S., M. Gupta and Jong Youl Choi. (2005) Analysis of IPSec Overheads for VPN Servers. 1st IEEE ICNP Workshop on Secure Network Protocols.